LANCOM Operating System (LCOS)

LCOS 10.40

Top performance and efficiency for your SD-WAN

- Next-generation SD-WAN – LANCOM High Scalability VPN (HSVPN) greatly improves efficiency as it requires fewer VPN tunnels
- A fresh look & feel – WEBconfig has been completely redesigned for an intuitive and modern appearance
- Multicast routing – new possibilities with multimedia applications in LANCOM infrastructures

LANCOM Systems

LCOS LANCOM Operating System

General Feature Overview		
Firewall	IPv4/IPv6 Stateful inspection, IP packet filter with port ranges, object-oriented rule definition. IPv4 Masking (NAT/PAT) of TCP, UDP, ICMP, FTP, PPTP, H.323, Net-Meeting, IRC and IPSec; DNS forwarding. Extended port forwarding and N:N mapping. Support for up to 256 contexts with individual IP networks, VLANs and interfaces, bandwidth management, QoS and VLAN prioritization for VoIP and VoWLAN	
Operating modes	LAN protocols	ARP, Proxy ARP, IPv4, ICMP, UDP, TCP, TFTP, RIP-1, RIP-2, DHCP, DNS, SNMP, HTTP, HTTPS, SSH, Telnet and SIP, BOOTP, NTP/SNTP, NetBIOS, RADIUS, TACAS+, LANCAPI, VRRP, STP/RSTP, IGMP, IPv6, DHCPv6, SLAAC, MLD, NDP, ICMPv6
	WAN protocols (Ethernet)	PPPoE, PPTP (PAC or PNS) and Plain Ethernet (with and without DHCP), RIP-1, RIP-2, IPv6CP, 6to4 Tunnel, 6in4 Tunnel, 6rd Tunnel, DHCPv6, SLAAC, L2TPv3 for Ethernet Pseudowires
	Multiprotocol router	IPv4/IPv6 router, NAT/Reverse NAT (IP- masquerading), DHCPv4/DHCPv6 server, DHCPv4/DHCPv6 client, DHCPv4/DHCPv6 relay server, DNS server, PPPoE client / Multi-PPPoE, ML-PPP, PPTP (PAC and PNS), NetBIOS proxy, DynDNS client, GnuDIP client, N:N address mapping and port mapping.
	ISDN gateway	ISDN gateway ISDN S0 bus, point-to-point and point-to-multipoint configuration, I.430, (Autosen sing);D channel: 1TR6, DSS1 (Euro-ISDN); B channel: PPP (asynchronous/synchronous), X.75, HDLC, MLPPP for channel bundling, CAPI 2.0 via LANcapi, Stac data compression
IPsec	Encryption algorithms	DES (56 bit), 3-DES (168 bit), AES, Blowfish (128-448 bit), CAST (128 bit), MD-5 or SHA-1 Hashes IKE with X.509 digital certificates or preshared keys, SCEP, IKE Config Mode, NAT-T, IPCOMP, up to 16 redundant VPN gateways for high availability and load balancing, Dynamic VPN
	IPSec clients	LANCOM Advanced VPN client for Windows Vista, Windows 7, Windows 8, Windows 10, Windows 2008 Server, Windows Server 2011 (all 32- and 64-bit versions) and Windows Server 2012 & Windows Server 2012 R2 incl. firewall, automatic connection-establishment tools, profiles for UMTS/GRPS/ Wi-Fi, analog, ISDN and DSL/PPPoE, X.auth/Config Mode, IPCOMP, Seamless Roaming
Dynamic VPN	Dial up to dynamic IP addresses: Transmission of dyn. IP address via ISDN B or D channel, IKE main mode. Dial up dynamic to static IP addresses: Transmission of dyn. IP address via ICMP- or UDP packet, IKE main mode. Trigger by ISDN data call, N:N address mapping for connecting locations with identical subnets	
IPSec over HTTPS	Transport of IPsec over TCP (port 443, like HTTPS) to pass through VPN filters (e. g. blocking of port 500 for IKE). IPSec over HTTPS is based on the VPN Path Finder technology from NCP	
Voice Call Manager	SIP-PBX	PBX functions for exchange between local analog, ISDN and SIP subscribers (depending on device's interfaces) as well as with upstream PBXs or external analog, ISDN and SIP subscribers
	Call router	Central routing of incoming/outgoing Calls, number mapping, digit replacement, number concatenation, configuration of several alternative target lines (line backup)
	SIP proxy and registrar	Management of local SIP users, inclusion of public SIP provider accounts as lines for common use, connection to upstream SIP PBXs including line backup.
	SIP gateway	Transparent conversion of analog (DTMF dialing) or ISDN (Euro ISDN/DSS1) calls to SIP and vice versa (depending on device's interfaces)
	VoIP Media Proxy	Termination and interconnection of multiple media streams. Control of media sessions resulting from SIP connections. IP address and port translation for media stream packets between different networks. Connection of parties at media stream level where a call transfer in SIP (REFER) is not possible
	Auto QoS	Automatic dynamic bandwidth reservation per SIP connection. Voice packet prioritization (CoS), DiffServ marking, traffic shaping (incoming/outgoing) and packet-size management of non-prioritized connections compared to VoIP
	Other functions	SIP over IPSec, SIP trunk, SIP link, SIP remote gateway, Media Proxy, ISDN with MSN/DDI and point-to-multipoint/point-to-point ISDN even with 1TR6 (only at external landline connections), support for G.722 in ISDN and SIP, SIP DTMF support according to RFC 2976 (SIP Info), RFC 2833 (RTP Payload Type/outband), echo cancellation (G.168), automatic adaptive de-jitter buffer, inband tone signaling (EU standard and country specific), fax transmission with G.711 or T.38 in LAN and WAN
Wireless LAN	Wi-Fi access point	Up to 255 Clients
	Wi-Fi client	Client Mode for connecting printers or PCs by Ethernet
	Wi-Fi bridge	Point-to-Point links with up to 16 Point-to-Point clients
	Frequency band	2400 – 2483.5 MHz (ISM) or 5150 – 5850 MHz
	Super A/G	108 Mbps Turbo Mode (channel bundling), bursting and hardware data compression (IEEE 802.11a/g)
	Wi-Fi standards	IEEE 802.11a/b/g/h/i with 54 Mbps, 802.11n with up to 450 Mbps, or 802.11ac with up to 1733 Mbps
	Radio channels	Up to 23 non-overlapping channels (5 GHz Band) with automatic dynamic channel selection (DFS), or up to 11 channels, max. 3 non-overlapping (2.4 GHz Band)
	Roaming	Seamless handover, IAPP-Support, IEEE 802.11d support, Spanning Tree
	VLAN	802.1p/q VLANs with 4094 IDs and 8 priorities, dynamic VLAN assignment by MAC/SSID/BSSID
	Multi SSID	Up to 8 independent Wi-Fi networks per radio module
	Security	802.11i with hardware AES encryption, WPA/TKIP, WEP, LEPS, 802.1x, access control lists, protocol filters, IP redirect
	QoS	WMM (part of 802.11e), APSD
	Rogue AP detection	Background scanning and client detection to identify rogue APs and clients on all Wi-Fi channels
	Fast roaming	PMK caching, pre-authentication for 802.1x and fast client-mode roaming via background scanning, Opportunistic Key Caching
	CAPWAP mode	Mode as managed access point with LANCOM WLAN Controller via CAPWAP protocol
	Spectral Scan	Analysis of the wireless spectrum directly at the Access Point
	Band Steering	Steering of Wi-Fi clients to a specific frequency band
	Adapt. Noise Immunity	Cut out sources of interferences in the radio field
	Hotspot 2.0	Automatic roaming from cellular networks to Wi-Fi hotspots
IP Quality of Service	Dynamic bandwidth management with IP traffic shaping, dynamic bandwidth reservation, TOS or DiffServ priority queuing, globally or per session, individually per send and receive direction, automatic packet size adjustment with PMTU reduction or fragmentation, layer 2/3 tagging (copying of 802.1p to DiffServ and back to 802.1p for end-to-end QoS)	
Diagnosis	Diagnostics Extensive LOG and TRACE possibilities, globally or per remote site. Integrated PING and TRACEROUTE to check connections, LANmonitor status display and protocol, internal logging buffer for SYSLOG and firewall events, monitor mode for Ethernet ports, partial RTTMON MIB for QoS monitoring. Graphical user interface for TRACE in LANmonitor	

LCOS LANCOM Operating System

General Feature Overview	
Management	LANconfig including Setup Wizards for Internet access, security, firewall, dynamic DNS, remote access and LAN-LAN coupling; 1-Click VPN via drag&drop; group configurations; WLANmonitor, LANmonitor status display, RADIUS user administration for dial-in access and Wi-Fi access control, EAP server, remote maintenance via ISDN, Telnet/SSL, SSH, WEBconfig (http/https) and HTTPS/TFTP configuration/scripting and firmware upload, SNMP management via SNMPv2 (MIB II, 802.11, 802.1d, 802.3, private MIB), Individual configuration of access rights for all local and remote access methods, individual access rights for up to 16 administrators, simultaneous remote configuration and version management of multiple devices, alerts from SNMP traps, SYSLOG or e-mail, scheduled control of commands with CRON service, TFTP client and server with variable file names (name, MAC/IP address, serial number), SSH client to access third-party devices. Scripting function for batch-programming of all command-line parameters for transferring (partial) configurations, irrespective of software versions and device types, incl. test mode for parameter changes. Support for TACACS+ protocol for authentication, authorization and accounting (AAA) with reliable connections and encrypted payload. Authentication and authorization are separated completely.

LCOS LANCOM Operating System

Feature Overview up to LCOS 10.40

New Features as of LCOS 10.40	
LANCOM vRouter	LANCOM High Availability Clustering Option (>=vRouter 500) and Public Spot PMS Accounting Plus Option for all vRouters
MLD Snooping	Support for MLD Snooping
LANCOM High Scalability VPN (HSVPN)	High scalability VPN significantly improves the extensibility and efficiency of your SD-WAN architecture. Previously each individual application needed its own individual VPN tunnel, but HSVPN now transports any number of networks on a single VPN tunnel to the remote site. Networks remain secure and strictly separated from one another. The advantage for your business: Significantly fewer VPN tunnels are required and faster recovery times in case of failover.
New WEBconfig	You can look forward to the completely new look and feel of LANCOM WEBconfig. Based on the modern and bright design of the LANCOM Management Cloud, WEBconfig has been completely redesigned to offer you an attractive and fresh appearance.
Multicast routing	Multicast data such as IPTV is now transmitted efficiently to multiple devices. Previously, separate data packets had to be sent to each recipient, whereas multicast routing now allows an IP stream to be transmitted to multiple recipients. This reduces the load on the router and makes better use of available routing capacity. Supported are PIM (Protocol Independent Multicast), IGMP-Proxy, and MLD-Proxy.
SD-WAN zero-touch deployment for DSL routers	Automatic installation of DSL routers at BNG Telekom connections with the LANCOM Management Cloud—without the laborious configuration of DSL access data on the router.
Netflow	With Netflow, network analysis information about the router's incoming and outgoing IP traffic (source, destination, ports, etc.) can be sent to a central server for processing.
IKEv2 VPN with Windows login	Mobile VPN clients using IKEv2 EAP can now authenticate against a central database such as Microsoft Active Directory or RADIUS without having to store VPN credentials on the LANCOM router.
More flexibility with backup scenarios	Route prioritization offers new levels of flexibility for backup scenarios.
New SD-WAN functions for the load balancer	On central-site gateways, VPN load balancers can be generated automatically with the help of RADIUS. Furthermore, multiple VPN channels are aggregated into tunnel groups, so that even in the case of failover, the VPN connects to a common gateway.
WLAN scheduling	Enables time-based activation and deactivation of SSIDs in the wireless LAN. Ideal for WLAN networks that should only be available at specific times, such as hotspots or Wi-Fi in educational institutions.
More security in the VPN	Support for new and modern encryption algorithms such as Chacha20-Poly 1305, digital signature with ECDSA, and new Diffie-Hellmann groups.
TLS 1.3 client mode	Support for the new TLS 1.3 protocol improves security for router accessing web services.
New filters for individual notifications	Configurable filter lists for SNMP traps and SYSLOG enable individualized monitoring notifications to be received.
New Features as of LCOS 10.32	
Wireless ePaper USB	The module LANCOM Wireless ePaper USB enables routers, access points or wireless LAN controllers (WLC-4006+) to wireless ePaper functionality. Supplement your devices with modern digital signage applications - without much effort.
ThinAP 2.0 protocol	Support for the ThinAP 2.0 protocol for connecting wireless ePaper access points to a central wireless ePaper server
New Features as of LCOS 10.30	
SD-WAN – Application Routing	Enjoy significant performance gains when you operate modern business applications in the cloud (e.g. Office 365, SalesForce, etc). SD-WAN Application Routing detects cloud-based applications and routes them directly to the Internet (local break-out). This relieves the VPN path to the headquarters as well as the headquarters' Internet line.
SD-WAN – Layer-7 Application Control in the firewall	Keep control of which applications can operate on your network. Defining application-related rules in the firewall allows you to decide which Internet applications are allowed, blocked, limited or prioritized.
WLC functions in the vRouter (vWLC)	You decide which role your LANCOM vRouter should play: VPN gateway or WLAN controller. The LANCOM vRouter now supports the role of a virtual WLC (vWLC). This fully virtualizes the functions of a WLAN controller on virtualization platforms such as VMWare ESXi or Microsoft Hyper-V. The number of managed access points depends on the vRouter license category.
TLS 1.3	Support of the new TLS 1.3 protocol increases the security of device access via WEBconfig.
Elliptic Curve Digital Signature Algorithm (ECDSA)	IKEv2 now supports the Elliptic Curve Digital Signature Algorithm (ECDSA) authentication method. Shorter keys combined with high-efficiency encryption provide the same security.
IKEv2 split DNS	Split DNS allows DNS to resolve specific internal domains to a VPN tunnel, with other DNS requests using a public DNS server.
IKEv2 fragmentation	Fragmentation of IKEv2 messages (per RFC 7383) is handled by the VPN router itself, eliminating the need for the transport network to fragment IKE packets.
Enhanced client reservations in the DHCPv6 server	In the DHCPv6 server, client addresses or prefixes can now be assigned either by means of DUID, MAC address, interface ID (as per RFC 3315) or remote ID (as per RFC 4649).
Double the number of Public Spot users	For particular routers of the LANCOM 178x and 179x series with the Public Spot Option, the number of users is increased from 64 to 128.
New Features as of LCOS 10.20	
WPA3	The latest generation of Wi-Fi encryption - WPA3 (Wi-Fi Protected Access) - now offers you more security for your Wi-Fi infrastructure. As the successor to WPA2, WPA3 offers important extensions and security features for small („WPA3-Personal") and large networks („WPA3-Enterprise"). With LCOS 10.20, all LANCOM access points and Wi-Fi routers support the new Wi-Fi security standard.
LEPS-U & LEPS-MAC	Keep control of who is in your Wi-Fi. With LEPS-U (LANCOM Enhanced Passphrase Security – User), individual clients or entire groups each receive a unique Wi-Fi password for an SSID. Using LEPS-MAC, you additionally authenticate the clients by their MAC address—ideal for secure corporate networks.

LCOS LANCOM Operating System

Client Management	Client Management steers Wi-Fi clients to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes—whether they operate stand-alone or orchestrated by the LANCOM Management Cloud. The popular Band Steering and Client Steering, which so far were separate features, have now been combined and even operate without a WLAN controller.
Auto Updater	The Auto Updater keeps your installations up-to-date automatically: If desired, LANCOM devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install only security updates, release updates, or all updates automatically. If automatic updates are not desired, the feature can still be used to check for new updates, which can then be installed with a single click.
WAN Policy-Based NAT	WAN Policy-Based NAT allows an easy assignment of static WAN IPv4 addresses to desired services. Due to a NAT action in the firewall rules internal addresses are masked behind a WAN address from the Internet access provider. Ideal for scenarios e.g. for the operation of mail servers and web servers with different WAN addresses.
DSL bridge mode	VDSL routers now operate optionally in DSL bridge mode. This allows a device to work purely as a DSL modem. Ideal for scenarios where multiple DSL connections are operated on one router.
LANCOM vRouter	Managing the vRouters is now even easier, because firmware updates are easy to import as a UPX file.
Layer-3 tunneling	As an alternative to the WLAN controller, layer-3 tunnels can now be established from the access point to a router (based on L2TPv3). This allows traffic to be directed through an existing infrastructure (routers, switches) without the use of complex VLANs.
OCSP responder	Maximum security with VPN access: Smart Certificate is the easy way to create digital certificates with your LANCOM device—without any need for an external certificate authority. This feature has now been extended to include the OCSP (Online Certificate Status Protocol) network protocol, which enables clients to automatically and efficiently query the integrated CA for the status of X.509 certificates.
LISP (Locator / ID Separation Protocol) support	The Locator / ID Separation Protocol (LISP) is a new routing architecture. LISP allows the implementation of highly scalable networks with an integrated routing protocol, tunneling, and overlays. Ideal for service providers or enterprise networks.
Public Spot CSV import	Public Spot management is now even easier: Hotspot users are easily imported and exported by text file (CSV).
Enhanced Open	Thanks to the introduction of additional data encryption, Enhanced Open improves the security of clients in open Wi-Fis such as hotspots in cafés or hotels.
New Features as of LCOS 10.12	
VPN IKEv2	More VPN performance and security › Support of AES-GCM for IKEv2 › Support of the elliptic curve Diffie-Hellmann groups (ECDH) 19, 20, 21, and the ECC Brainpool curves 28, 29, and 30 for IKEv2 › Support of RADIUS CoA for IKEv2 › Load balancer for IKEv2 for even load distribution in large enterprise scenarios › Additional backup mechanics for VPN › VPN setup wizard for IKEv2, incl. 1-click configuration of the LANCOM Advanced VPN Client for IKEv2 connections
IPv6 DHCPv6	Freely configurable DHCPv6 options
LACP	LACP (Link Aggregation Control Protocol) offers a huge added value in terms of reliability. LACP allows bundling of Ethernet connections to a virtual link. Ideal for the installation of redundant connections: If a physical link fails, data traffic will still be transmitted over the other cable. In addition, the possible transmission speed of redundantly connected devices is increased.
VoIP	With overlap dialing you are able to significantly reduce the idle time between dialing the telephone number and call establishment: already during the dialing process, telephone number parts will be sent to the agency.
IPv6	Variables for IPv6 LAN address and prefix in the action table
ICMPv4 und ICMPv6	Rate limiting for ICMPv4 and ICMPv6 is available
NTP	› Support of MD5 in NTP client and server › NTP server for each ARF net available
OSPF	Efficient, dynamic routing for internal networks: The routing protocol OSPF (Open Shortest Path First) provides the best path selection for all connected internal routers due to the exchange of their best paths from their routing table.
OCSP	OCSP check in the TLS / Rollout agent
TACACS	Support for TACACS shell authorization
Content Filter	An extension of selectable categories to block web contents grants you now even more security against unwanted Internet misuse in your network. Furthermore, the LANCOM Content Filter now enables to filter web content from IPv6 addresses.
WLAN	The automatic conversion option from Multicast to Unicast data streams enables multiple Wi-Fi clients to stream judder-free, high-resolution video applications. For applications, e.g. Multicast IPTV services, you benefit from an improved performance and a significant quality improvement.
Public Spot Smart Ticket	More security for the Smart Ticket functionality in the Public Spot: Having already been able to allow and block country codes, you can now do the same with individual area codes. This way the abuse of expensive value-added numbers when requesting access to your Public Spot is prevented.
New Features as of LCOS 10.0	
Support for the LANCOM Management Cloud	The LANCOM Management Cloud is the world's first hyper-integrated management system for the intelligent organization, optimization, and control of your entire network architecture. State-of-the-art software-defined networking technology drastically simplifies the provision of integrated networks – the manual configuration of individual devices is now a thing of the past.
Bonjour proxy	The Bonjour protocol offers Wi-Fi clients the fast and automatic discovery of network devices, so that printing and streaming applications (such as Airprint, Airplay, etc.) work without prior manual configuration. This is even better when it functions across networks: The Bonjour proxy allows the Bonjour protocol to operate across layer-2 boundaries. In this way you can implement ZeroConf services even in scenarios that operate with network virtualization (ARF).

LCOS LANCOM Operating System

Layer-7 application detection	Layer-7 application detection gives you the opportunity to comfortably track used applications and services (e.g. Netflix, Youtube, etc.) within the complete network via LANmonitor or the LANCOM Management Cloud – a real benefit for a widespread monitoring.
Support for Radius CoA (change of authorization) in the Wi-Fi	RADIUS CoA operates on the wireless LAN to throttle the bandwidth available to associated clients even for current sessions, and can even log the client off. This gives administrators more control, for example if data-volume budgets are exceeded.
WLC Skript rollout depending on LCOS version	WLC-controlled script rollouts for particular LCOS versions can be defined, thus configurations of different LCOS versions can be migrated to a Wi-Fi installation.
Public Spot E-Mail request on login	The Public Spot usage can be made conditional on a user registration by requesting the user's e-mail address.
Public Spot Multi-language login page	The title of the Public Spot login page can be stored in six different languages. You can choose between German, English, Italian, Spanish, and Dutch. The language of the Public Spot login page's title depends on the user-defined browser language.
Public Spot PMS module	The PMS module gives the opportunity to let the user accept the Public Spot's terms of use on the PMS login page, too. Additionally, the maximum transmit- and receive bandwidth can be configured for each tariff.
RADIUS Configurable WAN access	The access to the RADIUS service over an IPv4 connection can be limited.
RADIUS New attributes	The LANCOM RADIUS server supports the attributes „Tunnel password" and „LCS routing tag", which can be defined within the user accounts. This gives the opportunity to store user data centralized on the company's own RADIUS server, and thus minimize the configuration efforts for VPN scenarios.
VoIP / SIP Voice Call Manager with IPv6 support	As of LCOS 10.0 the Voice Call Manager supports the IPv6 protocol.
VoIP / SIP VoIP +10 option	Besides the general SIP lines upgrade within the Voice Call Manager from 20 to 25, you can add further lines with the LANCOM VoIP +10 option (up to 55).
VoIP / SIP LAN encryption	LCOS 10.0 provides an extension for the Session Border Controller: Thanks to new encryption facilities for VoIP data within the local network, SIP client communication is maximum secure within the LAN, too.
VoiP / SIP LAN SIP trunk	Using the internal SIP trunk termination, SIP PBXs can be operated at external VoIP lines via Session Border Controller.
VoIP / SIP SIPS and SRTP	The Voice Call Manager gives the opportunity to configure SIPS (Session Initiation Protocol Security) as well as SRTP (Secure Real-Time Transport Protocol) for encrypted SIP user authentication data transmission.
VoIP / SIP UDP packet processing	The processing of incoming UDP packets can be controlled if the provider line uses UDP for the communication with the registrar.
New Features as of LCOS 9.24	
DECT Extension for LANCOM All-IP Solutions	The base station LANCOM DECT 510 IP is the ideal solution for the integration of Gigaset DECT handsets in small and medium companies. Connected to the LANCOM router, LCOS 9.24 supports the automatic setup and configuration of the base station with up to 6 DECT handsets. So they can be easily registered with individually allocated call numbers. Thereby, LANCOM DECT 510 IP combines wireless telephony with outstanding HD voice quality.
Integration of AiRISTAFLOW RTLS systems	As of now, LCOS 9.24 allows the integration of AiRISTAFLOW Real Time Location Systems into LANCOM infrastructures. Hence, from now on persons, objects, and devices can be positioned professionally and reliably within their Wi-Fi environment. Positioning of patients in medical centers, tracking of mobile machines in a warehouse or even tracing of work tools–the compatibility between LANCOM and AiRISTAFLOW offers you realtime localization for any business or application field.
MWI (Message Waiting Indicaton)	The MWI extension of the LANCOM Voice Call Manager enables signalling of voice- and text messages on your provider's mailbox on the Internet (if supported by the provider). If there is a message left, the recipient will be informed automatically via message indication on the SIP device.
Call Forking	The Call Forking extension of the LANCOM Voice Call Manager enables simultaneous call signalling for incoming calls on one single line to multiple assigned extensions. If a call is answered by an extension, the other extensions will recognize that, so there is no notification about a missed call.
Support for RADIUS CoA (Change of Authorization) within Public Spot	In scenarios with external hotspot servers, RADIUS CoA is able to throttle the available bandwidth of a registered client or even log it off. So the hotspot provider gains better control for asserting his terms of use, e.g. when data volume is exceeded.
New Features as of LCOS 9.20	
SNMPv3	LANCOM customers now benefit from improved security in network monitoring thanks to SNMPv3 (Simple Network Management Protocol version 3). This protocol combines user-friendly device monitoring with strong security thanks to its encrypted data communications. And since it is enabled automatically, there is no need for you to make any configuration changes.
Maximum Wi-Fi quality	Noticeable improvements in the performance, reliability, and range of LANCOM access points, Wi-Fi routers, and WLAN controllers: As of LCOS 9.20, all Wi-Fi devices support the highlight features Airtime Fairness, Adaptive RF Optimization, the Wireless Intrusion Detection System, and many others. What's more, substantial quality improvements give LANCOM users and administrators the best ever Wi-Fi experience.
IKEv2	IKEv2 ensures that VPN tunnel establishment is faster and more secure. For the first time, encrypted VPN networking is now possible between IPv6-based sites, including those using mixed operation with IPv4.
IKEv1 with IPv6 support	As well as supporting IKEv2, LCOS 9.20 also supports IKEv1 for negotiating VPN connections between IPv6 networks.
BGP	Efficient VPN-based site connectivity thanks to dynamic routing in medium to large-scale networks. BGP (Border Gateway Protocol) ensures that all networked routers communicate effectively by sharing the best paths from their routing tables.
Logging of DNS queries	Client-side DNS requests are optionally sent to an external SYSLOG server for logging and analysis.
Performance measurement with iPerf	iPerf, a tool integrated into LCOS, allows you to precisely measure the maximum and momentary TCP and UDP throughputs between two devices on the network. The bandwidth losses derived from this can be used to identify and correct bottlenecks on the network.
Higher complexity for device passwords	Improved security with a new password policy requiring at least eight characters consisting of letters, digits and special characters.

LCOS LANCOM Operating System

Wi-Fi Adaptive RF Optimization	Dynamic selection of the best available Wi-Fi channel: Optimized wireless LAN throughput in case of interference as the access point dynamically selects the best Wi-Fi channel.
Wi-Fi Airtime Fairness	Improved exploitation of the Wi-Fi bandwidth: The fair sharing of wireless transmission times between all of the active clients uses the available bandwidth to maximum effect and improves Wi-Fi performance.
Wi-Fi Wireless IDS	Detection of attacks or unusual behavior of clients in the wireless LAN infrastructure by permanently monitoring the radio field. If attack-like events occur with a certain frequency within a set period of time, alerts are sent via e-mail, SYSLOG message, SNMP, or LANmonitor.
Wi-Fi Adaptive Transmission Power	Ideal for professional backup scenarios in wireless environments: If an access point fails, the transmission power of the remaining access points is increased automatically, so that full Wi-Fi coverage is assured at all times.
Wi-Fi Configurable data rates per SSID	Communication data rates between the access point and Wi-Fi clients can now be tightly controlled for a genuine gain in flexibility. For instance, data rates made unusable by environmental conditions can be excluded from use.
Wi-Fi Flexible access models for Public Spot accounts	The bandwidth that was booked for the Public Spot can now be displayed on vouchers. Also the validity period (time of expiry) of vouchers can be set with shorter time units (days, hours, minutes), which is ideal for scenarios with higher customer frequencies and shorter linger times.
Wi-Fi Controller-less Wi-Fi-Management	LANCOM Management Cloud and LANCOM Large Scale Rollout & Management (LSR) offer automatic setup and configuration allocation („Zero-touch Deployment“), as well as LANCOM access point management, even without WLAN controller.
Support for the LANCOM Battery Pack	The LANCOM Battery Pack allows up to two connected LANCOM routers or access points to remain powered up for at least two hours if the normal power supply should fail.
Assigning VLAN per ISP	VLANs can be defined per Internet Service Provider. They are tested for corresponding WAN connections and used if the test was successful.
Features as of LCOS 9.10	
Smart Certificate	LANCOM sets a milestone for security Maximum security for VPN accesses: As of now, all users benefit from the user-friendly functionality to create digital certificates - an external certificate authority (CA) is no longer necessary. VPN connections can be set up and securely encrypted with self-produced certificates. This maximum of security is included in all LANCOM central site VPN gateways, WLAN controllers, and all current LANCOM routers with the LANCOM VPN 25 Option.
High Availability Clustering	Grouping and central management of multiple WLAN controllers and central site VPN gateways: Group several WLAN controllers or central site VPN gateways to a high-availability cluster! With the LANCOM High Availability Clustering Options you can combine several devices to one cluster. As a consequence, there are many advantages like the central management and convenient configuration alignment (Config Sync) of all cluster devices. This is particularly beneficial for setting up intelligent backup scenarios since only one WLAN controller or central site VPN gateway has to be configured – an enormous time saver for administrators. Furthermore, you benefit from an automatic load balancing and the enrollment of cluster certificates.
GRE tunnel	With Generic Routing Encapsulation (GRE) packages are embedded and transported between two end points via a tunnel
Ethernet over GRE tunnel	The “virtual Ethernet cable” – ideal for the connection of two networks via layer-2 tunnel e.g. with encrypted IPSec VPN
TR-069 support	‚Zero-touch management‘ - The TR-069 protocol allows automated provisioning and secure remote management of a router in provider environment.
Public Spot	› The current and maximum number of Public Spot users is displayed in the LANmonitor with an additional notification at 90 % used capacity › You can set more than 4 GB data volume limit in the Public Spot volume budget and additionally print the defined budget per user on the voucher › Vastly simplified access for the generation of Public Spot vouchers due to an automatic forwarding to the respective interface › Input set of passwords for Public Spot users can be configured › The CSV export function of the Public Spot wizard can be configured › The Public Spot XML interface now supports advanced VLAN handling
Wi-Fi	› The usable bandwidth per SSID (download and upload) can be granted to each client equally › 16 individual SSIDs can be configured per Wi-Fi radio module - 15 SSIDs for IEEE 802.11ac modules › PPPoE-Intermediate-Agent for PPPoE-Snooping, to process PPPoED packets.
Wireless Quality Indicators	Visual display of transmit and receive quality of the Wi-Fi for an easy classification of the signal quality.
IEEE 802.11ac	Support for point to point connections (up to 1 km) and the client mode for all IEEE 802.11ac devices
WLAN Controller	› The automatic assignment of configurations by a WLAN controller to new access points via a WAN connection can be configured › Shows the certificate status of new access points › Wireless ePaper and iBeacon configuration can be set via the WLC › The LEDs of administrated Wi-Fi devices can be centrally deactivated via the WLAN controller › The table for centralized firmware management has been extended by a date entry › Channel and frequency display per client › WLAN controllers profiles were split in Wi-Fi profiles and advanced profiles for better usuability
SCEP	More security for using certificates: › The SCEP algorithms AES192 and AES256 for encryption and SHA256, SHA384, and SHA512 for signature control are supported › Wizard for certificate revocation › Configurable One Time Password for SCEP
SSL / TLS	The cipher suite for SSL and TLS can be set to always prefer PFS instead of using the client preferences.
Load Balancer - Client Binding	Conntected sessions, as seen in online banking are being recognized and then bundled and maintained on a single WAN line.

LCOS LANCOM Operating System

RADIUS	› Support for additional RADIUS attributes › Additional methods to determine realms out of user names › Comments field for RADIUS clients › RADIUS client may use additional source ports on demand › Accounting-On and Accounting-Off packages are being sent for each start and shutdown of an SSID
DHCPv6	Support for the PD-Exclude option in the DHCPv6 client
L2TP	Configurable loopback address for L2TP
RIP	Configurable loopback address for RIP
Content Filter	Content Filter notifications per e-mail can now be sent directly or daily.
Encrypted configuration for LANconfig	Configuration files of LANconfig can be encrypted and saved securely while being password protected. In addition, communication protocols have been set to encrypted protocols only by default.
Monitoring of configuration changes	Simple monitoring of configuration changes thanks to an easy view based on hash values, time stamps, and change counters.
Increased character limit for device name	The character limit for the device names has been increased to support 64 characters.
TACACS+	The command 'passwd' has been modified and allows a change of the local user passwords.
WAN	Automatic detection of VDSL connections by Deutsche Telekom and therefore usage of VLAN-ID 7 for the WAN connection.
VoIP	A proactive configuration of the All-IP Option is now possible, due to automated increases of the time intervals of repeated registration attempts. Therefore, a lockout based on false registration attempts can be prevented and a seamless migration from ISDN to All-IP is the result.
Features as of LCOS 9.04	
Wireless ePaper management	Management and monitoring for LANCOM E series access points and LANCOM Wireless ePaper Displays integrated in LANconfig.
All-IP Option	Upgrades routers (LANCOM 1781 series, 1631E, 831A) with telephony functions. Ensuring that existing ISDN terminal devices and ISDN PBX systems can continue to be used without replacement with IP-based phone functions when using an All-IP connection.
iBeacon support	iBeacon is a radio standard for indoor positioning. The iBeacon radio module, integrated in the LANCOM access points of the E series, continuously sends radio signals which can be received by smart phones and tablet PCs with Bluetooth Low Energy support (version 4.0). If there is a suitable end device in the operating range of the iBeacon, various location-based services can be realized with a corresponding app.
Listen before Talk	Conformance according to EN 300328 V1.8.1 in all Wi-Fi devices
Clearmode support	Support for the clearmode protocol for ISDN data applications
Features as of LCOS 9.00	
Client Steering	Wi-Fi clients are directed actively to the best available access point to provide the best overall load balancing and the highest possible bandwidth for each client. Client Steering can be based on client number, frequency band, and signal strength.
Auto WDS	Auto WDS allows wireless integration of access points in existing Wi-Fi infrastructure, including managment via WLAN controller.
Fast Roaming	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 Wi-Fi installations, which save the access keys temporarily and distribute them to the managed access points.
Protected Management Frames	Protection of Wi-Fi Management Frames, based on the standard IEEE 802.11w, against man-in-the-middle attacks by using Message Ingegrity Codes (MIC)
Bandwidth limitation per SSID	The bandwidth available to Wi-Fi clients can be configured for each SSID individually.
RADIUS Accounting per SSID	A RADIUS server can be set for each individual SSID.
Public Spot XML Interface	The bandwidth of connected Public Spot users can be changed during the session. In addition, the VLAN ID can be transmitted during the login process.
Public Spot	The Public Spot user can be redirected to advertisement websites of the provider at configurable time intervals.
WLC 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.
WLC 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 breaks down the access points are redistributed among the remaining WLAN controllers automatically. Once it is restored they are redistributed again.
WLC 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.
PRP	Packet loss of point-2-point connections can be reduced by using the Parallel Redundancy Protocol with dual radio access points due to parallel data transmissions. Supported devices: › IAP-322 › OAP-322 › OAP-382
L2TPv2	Support for the Layer 2 Tunneling Protocol version 2
DHCP	Support for DHCP option 82 to differentiate between Wi-Fi user groups by marking the DHCP messages resulting in different IP address pools.
Content Filter	Extracting the domain name from the HTTPS server certificate or using reverse DNS lookup of the IP address offers additional options to filter HTTPS websites.

LCOS LANCOM Operating System

VDSL Vectoring	Support for VDSL Vectoring in the respective devices
IPv6	The enhancements for IPv6 include: › RAS connection via IPv6 › Dual Stack Lite (IPv4-in-IPv6-tunnel) › IPv6 support for RADIUS server and client › Additional loopback addresses › Lightweight DHCPv6 Relay Agent › RA Guard › DHCPv6 Guard
LANconfig	The ports of the different management protocols (HTTP, HTTPS, TELNET, SSL, SNMP) can be configured via a single menu entry in LANconfig.
LANmonitor	All Public Spot clients are clearly marked in LANmonitor
SSL/TLS	Eliptic Curve Cryptography (ECC) for SSL und TLS, the algorithms can be chosen freely
SSH	Eliptic Curve Cryptography (ECC) for SSH. Additionally, special commands can sent via SSH (i.e. restart device, activate software option, set time).
WWAN	The SIM PIN can be changed via LANconfig and CLI.
Features as of LCOS 8.84	
Wi-Fi	The base data rate used to send multicast and broadcast packets is not fixed anymore. Instead it is determined dynamically according to the data rates of the clients currently logged in. This way the best available data rate can be used. To increase the reliability of DHCP responses in the Wi-Fi broadcast packets can be changed into unicast packets.
Adaptive Noise Immunity	By using adaptive noise immunity an access point can cut out sources of interferences in the radio field and focusses on clients with a sufficent signal strength. Therefore, Wi-Fi clients profit by having a higher data throughput available due to less interferences.
Opportunistic Key Caching	Opportunistic key caching allows fast roaming processes between access points. Wi-Fi 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 manan-ged access points.
RADIUS	RADIUS authentication can be used to log in to a device. In addition, users can be deactivated in the internal RADIUS server without deleting them.
Public Spot	The numerous novelties in the public spot consist of: › display of an error page when the Internet connection is inactive › additional default languages in the public spot: German, English, Spanish, Italian, French and Dutch › the option to set language specific texts for different parameters for the public spot › integration of a specifc logout URL to allow an easy logout of the public spot › the acceptance of the terms of service can be demanded for all public spot modes › the ticket page may contain conditional HTML code that is used only with specific users or administrators › optional caching of templates can increase the performance of the public spot › new variables for LAN MAC, gateway IP and client IP used when forwarding to an external hotspot gateway
Public Spot Smart Ticket	Templates for the smart ticket login can be generated and configured in the LANCOM public spot on HTML basis.
IPv6	The IPv6 WAN address can be used as a script variable in the LANconfig action table. This allows the usage of dynamic IPv6 addresses, for example dynamic DNS services. Furthermore, the IPv6 prefix can be delegated from the WWAN into the LAN, al-lowing the Clients to use the /64 prefix of the WWAN in the LAN. Meaning, a router can be operated in an IPv6 celluar network without DHCPv6 prefix delegation and neighbor discovery proxy (ND-Proxy).
SMTP Client	The LCOS SMTP Client now supports the following authentication methods and protocols: SMTP over TLS, STARTTLS, CRAM-MD5 for a SSL based encryption of the login credentials of an email server.
LCMS	Additional wizard for VoIP provider.
LCMS Quick Config Rollback	Quick and easy rollback to previous configurations is possible thanks to an automated backups of the configuration files in LANconfig.
Hotspot 2.0	Hotspot 2.0 can now be configured on LANCOM WLAN controllers.
LTE	The available frequency bands for LTE connections can be set manually.
SSH	LANCOM devices will generate an individual SSH key after a reset. The generation can be triggered via the CLI, too.
SMS	Cellular routers can now send and receive SMS. The management can be comfortably conducted via LANmonitor. Additionally, notifications can be sent by SMS at defined network events. SMS can be sent via HTTP with URL parameters, too. Therefore, a cellular router can be utilized as an SMS gateway. Automated dispatch of SMS for smart ticket. Sending the public spot login credentials for smart ticket can be done directly via the celluar router - without the need of an external SMS gateway. Suitable for installations with a maximum throughput of 10 SMS per minute.
SYSLOG	SYSLOG has been expanded to cover extensive information about the process of connecting to cellular networks, DSL synchroni-sation, and the start-up of plain IP connections.
LANCOM CC Router	After running the CC start-up wizard the fingerprint of the used SSH keys can be saved.

LCOS LANCOM Operating System

Volume Budget	The used data volume of WAN connections can be monitored and different actions can be triggered once certain thresholds are passed. This feature is only available for the following devices: › 1781er series › L-45x series › 1780EW-3G, 1780EW-4G › 9100+ VPN, 7100+ VPN, 9100 VPN, 7100 VPN › WLC-4006+ › IAP-321, IAP-321-3G, IAP-3G › OAP-322, OAP-321, OAP-321-3G, OAP-3G › 831A, 1631E
Rollout Wizard	A default rollout wizard is now available on all LANCOM devices which can be used to obtain rollout configurations.
Features as of LCOS 8.82	
Hotspot 2.0	The new Wi-Fi standard IEEE 802.11u (Hotspot 2.0) allows for a seamless transition from the cellular network into Wi-Fi hotspots. Authentication methods using SIM card information, certificates or username and password, enable an automatic, encrypted login to Wi-Fi hotspots of roaming partners - without the need to manually enter login credentials.
Wi-Fi	The ARP/NDP handling of Access Points was improved to allow storing of multiple IPv6 address per MAC address. In addition, broadcasts and multicasts can be deactivated for a radio cell. Furthermore, band steering can be configured in profiles of a WLAN controller.
Public Spot	One of the improvements is an easy login to a Public Spot by just accepting the terms of service. A temporary user with limited bandwidth or online time is created in the background. Additionally, the source VLAN and the NAS port ID can be transmitted in the Public Spot URL to allow different welcome pages based on the information given. Additionally, a VLAN can be assigned to a Public Spot user dynamically after a successful login.
Public Spot Re-Login	The Public Spot identifies known Wi-Fi clients for an automatic authentication. After an initial authentication, the hotspot stores the relevant client information so that there is no need for an additional manual entering of login credentials - signifi-cantly increased comfort for regular guests.
Public Spot Bandwidth Management	The available bandwidth for Public Spot user groups (e.g. “gold”, “silver”, “bronze”) can be individually configured: An ideal functionality for preferring “premium users” and for limiting the bandwidth for standard accounts.
Public Spot WISPr	Wireless Internet Service Provider roaming allows smart clients to connect to a Public Spot without the need of manual input of login credentials on a website.
RADIUS	The maximum length of the realm entry for RADIUS forwarding was increased to 64 characters. Additionally, a bandwidth limitation can be set for all clients connected via LAN or Access Points directly connected to the LAN.
SYSLOG	The amount of stored entries in the internal SYSLOG server was increased to over 20,000. The maximum age of entries can now be defined in hours, days, and months.
ARF per DNS	DNS forwarding can be configured separately for each ARF network.
DHCPv6	The DHCPv6 server of LANCOM devices includes the ‘reconfigure’ feature, which is used by the DHCPv6 server to force clients to renew various information, such as IP addresses, prefixes or DNS server.
LANconfig with SSH	SSH can be used as an additional protocol in LANconfig to configure or to upload firmwares or files to a device.
WWAN	A login that was denied by the cellular provider, is clearly communicated to the user via LCOS, LANmonitor and SYSLOG.
Firewall	The source routing tag can be used in the firewall to set up rules for different ARF contexts independently from each other.
Public Spot PMS Accounting Plus	This option simplifies the charging of hotspot fees. The LANCOM Public Spot option is an add-on extra that can be installed on LANCOM devices. In combination with a property management system (PMS), it enables guests to register and pay for Internet guest access. This is carried out via the FIAS interface, which provides direct communication between a LANCOM device and FIAS-based systems such as Micros Fidelio.
Features as of LCOS 8.80	
IPv6 Dual Stack	IPv6 functionality can be enabled and disabled globally. IPv6 functions can be used additionally to IPv4. Operation modes: IPv4, IPv4/IPv6, IPv6 Supported IPv6 address types: link local, global unicast. unique local
IPv6 Router	Possible step-by-step migration of the network configuration by using the seperated IPv6 router with a designated routing table.
IPv6 Internet connection	Available methods to establish an IPv6 internet connection: › IPv6 tunnel using an IPv4 network › Native IPv6 over PPP (IPv6CP) with address configuration by the autoconfiguration and with multi link PPP support › Native IPv6 over IPoE with either static automatic address configuration, autoconfiguration or DHCPv6 (DSLoL only with native IPv6 in exclusive mode available)
IPv6 Tunnel technologies	The following IPv6 tunnel technologies are available to realize an IPv6 internet connection by using an IPv4 connection. › 6to4 tunnel › 6in4 tunnel › 6rd tunnel with either static configuration or dynamic configuration by DHCPv4
IPv6 over PPP (IPv6CP)	IPv6 can be used at a single IPv6 PPP session or in a dual stack IPv4/IPv6 session.
IPv6 DHCPv6 Server	Supports stateless and stateful mode. Supported options: IPv6 address (IA_NA), Prefix Delegation (IA_PD), DNS Server, DNS Search List, and Rapid Commit
IPv6 DHCPv6 Client	Supports stateless and stateful mode. Supported options: IPv6 address (IA_NA), Prefix Delegation (IA_PD), DNS Server, DNS Search List, FQDN, Rapid Commit, and Reconfigure.
IPv6 DHCPv6 Relay Agent	Forwarding of DHCPv6 messages between DHCPv6 clients and DHCPv6 servers in different networks.

LCOS LANCOM Operating System

IPv6 Stateless Address Autoconfiguration (SLAAC)	Automatic configuration of an IPv6 address by using the MAC address of received router advertisements according to EUI-64.
IPv6 Neighor Discovery Protocol (NDP)	Responsible for automatic detection of network devices and the corresponding IPv6 addresses in the same network segment. Possible configuration of multiple subnets by using router advertisements according to the delegated prefix of the provider. Operation modes: Router, Host
IPv6 Firewall	Fully configurable stateful inspection firewall.
IPv6 LCOS applications	Supported applications to date: WEBconfig, SSH, Telnet, DNS, TFTP Additional applications will be supported with further development.
IPv6 LANconfig support	IPv6 support for LANconfig consists of the search and configuration of devices over IPv6. Operating modes: IPv4, IPv4/IPv6, IPv6
Band Steering	Band Steering allows dual radio Access Point to assign a preferred frequency band to a client (2.4 GHz or 5 GHz). This allows to suppress probe responses in the non-preferred band to clients that are already known to be able to operate in the preferred band.
Spectral Scan	Using Spectral Scan (via WEBconfig) allows a spectral analysis of the wireless medium directly at the Access Point. This can be used to identify and analyse interferences. The feature is available for the following devices: › L-45x series › L-32x series › 1781AW, 1781EW › 1780EW-3G
DFS	Conformance to DFS as of ETSI 301 893 version 1.6.1 - DFS 4
UUID info element for Wi-Fi APs	Access Points can include a UUID element in their beacons which identifies them as a LANCOM Access Point. The UUID element is dependent on the device, so an Access Point with two Wi-Fi modules will send the same UUID on both modules.
RADIUS server per SSID	An individual RADIUS server can be assigned to each SSID profile in the WLC configuration.
Alternative WLC via DNS	Managed Access Poins can obtain addresses of alternative WLCs via DNS.
Public Spot	Funktionality of the Public Spot was improved by adding a setup wizard and the option to let users request the login credentials via e-mail or mobile with the Smart Ticket system. A new set of rules for specific users has been implemented which allows the administration of the user management. Furthermore, the new user wizard allows to set the number of multiple logins and if the user name is case-sensitive or not. In Addition, the free network table was expanded and supports now wildcards and domains that can be reached via multiple IP addresses. Furthermore, an XML interface is available for communication with an external hotspot gateway.
SYSLOG, boot log, and event log	SYSLOG, boot log and event log can be saved boot persistent. This feature is only available for the following devices: › 1781 series › 1681 series › L-45x series › 1780EW-3G › 9100 VPN, 7100 VPN › WLC-4100, WLC-4025+ › IAP-321, IAP-321-3G, IAP-3G › OAP-321, OAP-321-3G, OAP-3G
Logging of configuration changes	Configuration changes done by command line interface on a LANCOM device can now be logged via SYSLOG.
Packet capture in WEBconfig	Possibility to generate packet dumps by remote on a LANCOM device and to save them locally. These can be later analyzed by Wireshark or similar tools.
VPN	Additions in the VPN area include the support for Diffie Hellman Group 14 and intelligent pre-calculation of DH keys for faster connecting.
IPSec	Replay Detection according to the IPSec standard to protect against replay attacks.
SSH / SCP	SSH / SCP can be used to upload certificates and configuration files to a LANCOM device. Furthermore, the crypto protocols and key lengths used by SSH can be configured.
LANCOM myVPN	Additional configuration options are available for optaining a VPN profile. Optaining a VPN profile via the WAN connection can be prohibited and in the brute force protection it can be set how many unsuccessful attempts are allowed.
Fast roaming for Wi-Fi APs in client mode	Wi-Fi Access Points operating in client mode now support PMK caching and preauthentication according to 802.1x to speed up roaming. In addition, dual radio Access Points in client mode coordinate now the roaming procedure of the Wi-Fi module to ensure that at least one will stay connected at all times.
LLDP	LLDP is used to automatically detect devices and their topology in the network.
Scripting	The TAB command used for scripting was extended. Now, an unknown column will not cause a syntax error but will be ignored instead. This allows to use the same script for devices with a different feature set.
GPS Time	The GPS transmitted time can be used to set the system time.
Content Filter	The LANCOM Content Filter is using a Concurrent User Model, which checks how many user are using the content filter at any given time and not how many user are allowed overall.
LANmonitor	LANmonitor now shows the active ethernet ports and IPv6 addresses. In addition the DHCP Server is displayed, including the leases with time stamp.
LANconfig	LANconfig uses the built-in web browser to open WEBconfig by default. Furthermore, the usability of LANconfig has been enhanced by including the Quickfinder in selection menus and the structure is easier accessible due to the new overview tables. Generating secure passwords in LANconfig has been improved.

LCOS LANCOM Operating System

Features as of LCOS 8.62	
LANCOM myVPN	LCOS now supports the LANCOM myVPN app. The myVPN app for iOS devices allows the complete configuration of IPSec VPN on your device in just a few steps. Afterwards, the integrated VPN client can establish a secure VPN connection to a LANCOM router. In the process of the configuration the app will download the VPN profile from the LANCOM router via HTTPS and will automatically enter the profile data in the VPN client of the iOS device. (Availability via the Apple AppStore)
WLC-6 Option	The WLC-6 option allows to use the LANCOM WLAN controller functions on a LANCOM router. Up to six LANCOM access points and Wi-Fi routers can be managed centrally. Supported routers: 1781EF, 1781A, 1781A-3G, 1781-4G
Public Spot	Multi-login for new public spot users can now be set via the wizard or an URL command while generating it. This way a user can use the same access information on multiple devices. Furthermore, additional information is shown in the user management wizard: online-time, traffic, status, MAC address, and IP address.
VoIP	The default value regarding WAN access by SIP users has been changed to 'denied'. In addition, the wizard for adding new SIP users has been updated and will now ask if access via WAN is wanted.
IKE and IPSec	The default proposal lists for IKE and IPSec have been revised. AES-256 bit was added to improve security when using default settings.
Wi-Fi	The additional value 'tightened' was added to the selection of the setting supress SSID broadcast. If chosen, the access point will only send probe responses to clients which use the correct SSID.
Features as of LCOS 8.60	
LCMS Flexible Group Configuration	The flexible group configuration of LANconfig offers easy generation of configuration templates for groups of LANCOM devices. With these templates it is possible to configure multiple parameters on devices that share them and only individual parameters have to be configured manually on each single device.
LCMS CSV Import	By using the CSV import of LANconfig, multiple devices can be added at once. In addition, the CSV import can also be used to create multiple configuration files for further usage.
Public Spot	New and improved wizards for user management simplify generating, administrating and deleting user accounts. One of those is the voucher wizard with which it is possible to generate and print a whole batch of vouchers. In addition, export of the user list of the public spot in the CSV format is available. Further improvements of the public spot are an extension of the forwarding URL which can now consist of 251 characters and the option to set the size of the public spot station-table-limit manually.
Wi-Fi P2P Links	Up to 16 point to point links can now be configured for each WiFi module.
WLAN Controller	The RF field optimization was improved by using a new method to determine interferences.
Wi-Fi Security	Clients which were assigned different VLANs by the 802.1x authentication are now unable to decrypt broadcasts and multicasts meant for different VLANs due to VLAN specifc group keys.
Wi-Fi 40 MHz mode	The 40 MHz modus in the 2,4 GHz frequency band was extended by a "good neighbor" funcionality, which is used as the new default setting. This ensures the reduction of the channel bandwidth to 20 MHz in case of overlapping in the frequency band when using 40 MHz channels.
PPTP	A PPTP tunnel can be encrypted by using an MPPE encryption. This allows mobile devices using the android operating system to connect to the company's network via secured access.
SYSINFO	SYSINFO was expanded to show and transmit location and the first comment.
TLS 1.1 / 1.2	TLS 1.1 and 1.2 are supported to provide better security. The TLS protocol is used by LCOS in the following modules: HTTP over SSL, Telnet over SSL, RADSEC, CAPWAP/DTLS, EAP-TLS/PEAP/TTLS.
Command Line Enhancements	To ease the work with large tables using the command line it is now possible to jump into the table rows as if you would jump into a new directory to get a list of the parameters. Additionally, various show and dir/ls commands can now be filtered similar to traces.
DHCP Vendor Class	The DHCP vendor class identifier can now be set manually to increase compatibility to various ISPs.
PPPoA / IPoA Support	The LANCOM 1781router series with integrated modem support now PPPoA and IPoA as WAN protocols.
IPSec	Unified and recommended default IPSec lifetimes are now being used.
LCOSCAP	LCOSCAP offers the possibility to generate packet dumps by remote on a LANCOM device and to save them locally. These can be later analyzed by Wireshark or similar tools.
Advanced VPN Client Seamless Roaming	By using a LANCOM Advanced VPN Client (Version 2.3) a VPN connection to a LANCOM router (LCOS 8.6) will be established again without asking for new credentials after an internet connection loss. The new connection can even be established over a different medium. Seamless roaming is especially interesting if one time passwords or RSA token are used for authentication.
Feature and License Activation	Extensions of the content filter license does not require a reboot of the device.
SIP ALG	The SIP ALG (Application Layer Gateway) acts as a proxy for SIP communication. For SIP calls the ALG opens the necessary ports on the firewall for the corresponding media packets. By using automatic address translation for devices inside the LAN, the use of STUN is no longer needed. Available for the following devices: LANCOM 1781 series, 1780EW-3G, 1681V, 1631E, 831A, 7100 VPN, 9100 VPN, WLC-4006, WLC-4025+, WLC-4100, IAP-3G, IAP-321-3G, OAP-3G, OAP-321-3G
Features as of LCOS 8.50	
LANCOM QuickFinder	Search filter in LANconfig, including device configurations, LANmonitor and WLANmonitor. In a configuration you can search for units, values and descriptions (selectable). All hits will be highlighted and the menu will be reduced to pages which contain hits. When searching in WLANmonitor or the device list in LANconfig, views will be shortened to lines with hits. In LANmonitor you can flick through the different hits easily.
Layer-3 Tunneling	Layer-3 Tunneling in conformity with the CAPWAP standard allows the bridging of Wi-Fis 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.
Content Filter	Filtering of HTTPS requests. New and easier to use override function requires just one click. Possible number of users is doubled on all supported devices. Enhanced performance by software optimization.

LANCOM Systems

LCOS LANCOM Operating System

Programmable Rollout Wizard	Allows the programming of a customized wizard to simplify the rollout in projects. Support for customized templates and logos provide a way to generate a brand specific look. Available for LANCOM 1681V, 1711+ VPN, 1721+ VPN, 1751 UMTS, 1811n Wireless, 1821n Wireless.
OCSP Client	Check X.509 certifications by using OCSP (Online Certificate Status Protocol) in real time as an alternative to CRLs.
Public Spot Option	The Public Spot Option (max. 64 users) is now available for the routers 1711+ VPN and 1721+ VPN, too.
WLC Public Spot Option	The WLC Public Spot Option (unlimited number of users) is now available for the central site gateways 7100 VPN and 9100 VPN, too.
SYSINFO	SYSINFO provides additional information. Hash value for the current configuration, time stamp of the last configuration change, a persistent counter of the number of configuration changes and the output of the value CONFIG_STATUS.
Load Commands	LoadFirmware, LoadConfig and LoadScript can now be executed conditionally in case certain requirements are met. For example, the command LoadFirmware could be executed on a daily basis and check each time if the current firmware is up to date or if a new version is available. In addition, LoadFile was implemented and allows the upload of files including certificates and secured PKCS-12 containers. HTTP and HTTPS are now supported by all commands as well.
SSL/TLS	HTTPS client authentication by certificate.
HTTPS Server	Option to choose if an uploaded certificate or the default certificate is used by the HTTPS server.
Configuration Dialog	Any viewed page of a configuration is saved in a history. It can be easily accessed by a drop down menu or by simply flicking through it.
Trace Application	The trace window can be opened in LANconfig from the ‚device' menu for the selected device.
Automatic Software Update	Voluntary automatic updates for LCMS. Search online for LCOS updates for devices managed by LANconfig on the myLANCOM download server (myLANCOM account mandatory). Updates can be applied directly after the download or at a later time.
Features as of LCOS 8.00	
Content filter (Option)	Optional content filter for web surfing through an HTTP proxy. Configuration of filter profiles for different categories and category groups. Allocation of time profiles. Customization with your own black and white lists, which also work with wildcards. Optional override mechanisms per category/category group make it easy to handle exceptions. Filter profiles can be applied flexibly with the aid of firewall actions. Individual adaptation to show blocking/error in each language, or by linking to a separate web server. Convenient configuration and organization of filter profiles with LANconfig. Preset profiles for standard applications. E-mail/Syslog/SNMP notification of license expiry. Wizard for quick and easy setup of the content filter function in standard environments. Statistical reports of content filter usage (category hitlist and allocation, top ten of visited web sites, maximum and average response times, etc.) in LANmonitor
IPSec over HTTPS	New item for VPN tunnels; this alternative transmits VPN data via TCP over port 443 (like HTTPS). Encapsulates IPSec VPN in TCP over port 443 which can go through firewalls in networks where e. g. port 500 for IKE is blocked. Suitable for client-to-site connections (with LANCOM Advanced VPN Client 2.22 or later) and site-to-site connections (LANCOM VPN gateways or routers with LCOS 8.0 or later). With the function "IPSec over HTTPS" activated, a LANCOM Advanced VPN Client initially attempts to establish a conventional IPSec tunnel (low overhead). If this doesn't work, IPSec is encapsulated in TCP over port 443. IPSec over HTTPS is based on the VPN Path Finder technology from NCP
WLC/load balancing	LANCOM Wireless LAN controllers now also support load balancing for WAN connections, allowing multiple connections to be bundled for better performance
WLC/802.1X	RADIUS accounting as per IEEE 802.1X can be configured for any SSID individually managed by a Wireless LAN controller
WLC/channel load display	WLANmonitor displays the load on each channel where LANCOM access points are managed by wireless LAN controllers
Wi-Fi/DFS	Recognition of new radar patterns in Wi-Fi according to ETSI 301 893 v. 1.5
Wi-Fi/Broken link detection	If the link of a chosen LAN interface breaks down, a Wi-Fi module can be deactivated to let the associated clients search for a new base station
DHCP	DHCP forwarding to multiple (redundant) DHCP servers
Alternative boot configuration	During rollout devices can be preset with project- or customer-specific settings. Up to two boot- and reset-persistent memory spaces can store customized configurations for customer-specific standard settings (memory space „1") or as a rollout configuration (memory space „2"). A short reset (more than 5 seconds) loads the customer-specific standard settings from memory space 1 (if programmed; otherwise LANCOM factory settings). A long reset (more than 15 seconds) loads the rollout configuration from memory space 2 (if programmed; otherwise LANCOM factory settings). A further option is the storage of a persistent standard certificate for the authentication of connections during rollouts
USB setup	Automtatic upload of appropriate firmware and configuration files on insertion of USB memory (FAT filesystem) into USB interfaces of LANCOM routers with factory settings. The function can be activated to be used during operation of configured devices. The router checks the files' dates and versions against the current firmware before upload
Internal HTTP/HTTPS file server	HTML pages, images and templates for Public Spot pages, vouchers, information pages of the Content Filter can be stored on a USB memory (FAT file system) in a specific folder as an alternative for the limited internal LANCOM router memory
SNMP/MIB	New concept for a single, unified LANCOM enterprise MIB for new LANCOM products with LCOS (initially for LANCOM L-32x series and LANCOM Wireless LAN controllers); simplifies the integration into third-party management and monitoring solutions based on SNMP. Central provision of the MIB via LANCOM
SSL/TLS	Improved security for all services with TLS negotiation (e.g. HTTPS configuration, CAPWAP, load commands via HTTPS) as per RFC 5746. Provides protection from potential weaknesses in TLS key renegotiation
SSH & Telnet client	SSH client functionality compatible to OpenSSH under Linux and Unix operating systems for accessing third-party components from a LANCOM router. Also usable when working with SSH to login to the LANCOM device. Support for certificate- and password-based authentication. Generates its own key with sshkeygen. SSH client functions are restricted to administrators with appropriate rights. Telnet client function to access/administer third-party devices or other LANCOM devices at the command line
Internet Access Setup Wizard	Additional setup of IPTV settings for non-VDSL connections offering T-Entertain
LANconfig/(W)LANmonitor	Program windows are displayed in the style used by the operating system. New full-color icons in high resolution. Tree view of the settings pages in the configuration window provides quick access to all settings. Interactive full-text filter for the device list in LANconfig that allows a quick selection of/restriction to relevant entries. New password fields which optionally display the password in plain text and can generate complex passwords. Editing of meta parameters in configuration file headers for automatic configuration upload from USB storage. New application help for LANconfig (W)LANmonitor and Trace

LCOS LANCOM Operating System

Features as of LCOS 7.80	
XAUTH with RADIUS connection	Connection of XAUTH to RADIUS servers provides the central management of the control over VPN-client access on a per-connection basis. Authentication of VPN-client access additionally by OTP token
VPN/certificates	Simultaneous support for multiple certification authorities with the management of up to nine parallel certificate hierarchies, each with a CA certificate and with reference to CRLs. Indices for simplified addressing of individual certificates, especially when working with the command-line prompt. Wildcards for certificate checks of parts of the identity in the subject, enabling the economical authentication of remote sites in large installations with parallel certificate hierarchies
VPN/PPTP	Revised algorithms multiply the performance of central-site VPN gateways working with multiple remote stations, especially for VPN and PPTP connections. Up to 32 alternative remote stations, each with its own routing tag, can be defined as a backup for PPTP and VPN connections. Automatic selection may be sequential, or dependant on the last connection, or random (load balancing)
DoS	Threshold for half-opened connections for central site devices raised to 1,000
DHCP cluster	Depending on the routing context, DHCP servers can be switched into cluster mode if different DHCP servers are active in the context's network. All DHCP negotiations carried out by other DHCP servers are monitored, enabling DNS requests to be resolved independently of the DHCP server which was originally used for DNS registration
Routing	Packets sent in response to LCOS service requests (e.g. for Telnet, SSH, SNTP, SMTP, HTTP(S), SNMP, etc.) via Ethernet can be routed directly to the requesting station (default) or to a target determined by ARP lookup
ARF	Support for up to 16 ARF contexts (networks) for the 1700 and 1800 series. The routing tag for a packet arriving from a local router is determined by a series of comparisons (in descending order): If the tag matches with a defined network, then the tag is retained; if only one network is defined for the interface where the packet arrived, then the interface tag is taken; if a reverse ARP lookup finds a next hop belonging to a defined network, then its tag is used; alternatively, the tag can be determined from the routing table
ARF/Wi-Fi	Allocation to a special ARF context for IAPP to enable the exchange of roaming information between access points, instead of transmitting to all ARF contexts defined for an access point (default)
Wi-Fi profiles in client mode	For access points and Wi-Fi routers in client mode, different Wi-Fi profiles can be defined which are independent of the SSID. The profile can be selected depending on signal strength (default) or in a pre-defined sequence of profiles which are independent of signal strength
Voice Call Manager	Independent settings for DiffServ marking of signaling (SIP) and media streams (RTP)
COM-port forwarding	Data can be forwarded from devices connected via the serial port either with newline conversion for detection and normalization of line breaks (default), or in a binary mode which ignores line breaks. TCP keepalive as per RFC 1122, keepalive interval, retransmission timeout and count are configurable
Ethernet interfaces	Ethernet interfaces can be set to idle when not in use or, additionally, they can be completely electrically disabled
SNMP optimization	Optimization of SNMP processing and communication with LAN/WLANmonitor. Information for LANmonitor is transmitted only in the form of SNMP traps, which avoids having to repeatedly transmit large tables
TACACS+	CRON, action-table and script processing can be diverted to avoid TACACS+, so relieving TACACS+ servers of these exceptional actions when rolling-out large installations
Management in general	Extended management information relating to device configuration; 8 commentary fields for storing project-specific identities
CPU load display	The time period for averaging the CPU load can be set to 1s, 5s, 60s or 300s. The default value is 60s according to the HOST-RESOURCES-MIB
LANconfig	Firmware updates and the saving/uploading of configurations for LANCOM managed switches can be directly initiated by LANconfig. The DHCP server supports DHCP options with ARF context-specific types and values. These values can now be set with LANconfig as well. The automatic cleanup of the RADIUS server's user table can be set in LANconfig
LANmonitor/WLANmonitor	In the tree view for large tables (e.g. for VPN and PPTP connections), LANmonitor only displays the most recent changes. The full scope of entries are accessed and viewed in a separate table view. The processing and display of large tables in LANmonitor and WLANmonitor has been optimized
Features as of LCOS 7.70	
VPN/hardware acceleration	With LCOS 7.7 the VPN hardware accelration in routers of 1700 and 1800 series is activated, even without VPN-25 Option. The limit of simultaneous VPN connections, however, stays the same (depending on device model and VPN-25 Option)
Public Spot	Re-Design of the Public Spot wizard to optimize printing of vouchers. New parameters for time and traffic budgets as well as the start of accounting for flexible tariffs with Wi-Fi vouchers
TACACS+	Support for 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 for 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. 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
BFWA	Support for Broadband Fixed Wireless Access in 5.8 GHz band with up to 4 Watts transmitter power for Wi-Fi point-to-point links according to IEEE 802.11n. (The use of BFWA is subject to country specific regulation.)
Outdoor Wi-Fi	Enhanced DFS pattern matching and performance for IEEE 802.11n. New profile for Ireland in 5.8 GHz band with 2 Watts transmitter power without DFS

LCOS LANCOM Operating System

LANmonitor	Graph with timeline for Tx and Rx rates of WAN or point-to-point links, Rx and link signal strength as well as throughput of point-to-point links, CPU usage, free memory and temperature (not available for all devices) in a separate window. Icon to mark parameters in the LANmonitor view that can be displayed with a graph. Selection of sequences in the tracked timeline and comparison table with minimum, maximum and average. Acoustic indication tones for signal strength played in the dialog for point-to-point link antenna setup. DHCP table with manual refresh to view current DHCP leases, available in device's context menu. Trace icon in toolbar. Trace with dual view for comparison of trace logs. Additional display of radio band and channel at Wi-Fi interfaces
U-APSD/WMM Power Save	Extension of power saving according to IEEE 802.11e by Unscheduled Automatic Power Save Delivery (equivalent to WMM Power Save). U-APSD supports the automatic switch of clients to a doze mode between predicted voice packet arrival due to the previous negotiation of a service profile (for supporting terminal devices, especially for Voice over WLAN). Display of U-APSD capability per SSID in status menu and display of negotiated category for each client in the station table in status menu
IGMP Snooping	Support for Internet Group Management Protocol (IGMP) in the Wi-Fi bridge for Wi-Fi SSIDs and LAN interfaces for specific switching of multicast packets (devices with integrated Wi-Fi only). Multicast groups of ports (SSIDs, LAN interfaces) and router ports to route multicast packets over layer-3-networks. Detailled configuration of request, request-reply and advertisement interval as well as robust-ness. Automated detection of multicast groups. Configurable action for multicast packets without registration (router-ports-only, flood, discard). Configuration of static multicast group members per VLAN Id. Configuration of query simulation for multicast membership per VLAN Id
Draeger Validation	Suitability of LANCOM devices with Wi-Fi and IGMP snooping for wireless patient data transmission in medical environments
RADIUS Accounting	Command to reset all counters of active accounts, e. g. for accurate billing of periods by resetting with a CRON job
RADIUS Server	Extension of user accounts with switchable multi-login, expiration at realtive or absolute date, time and traffic budgets as well as restriction to service type
Enlarged temperature ranger for L-305/310	Limiting of interface speed to Fast Ethernet when the temperature exceeds the allowed limit (+35°C) to extend the temperatur range to +45°C
Telnet/SSH (CLI)	Extension of ‚mailto' command to execute commands and attach their output at specific events (connection up/down, CRON job)
UMTS/LANconfig	Upload of firmwares provided as upx files for UMTS modules in LANCOM 1751 UMTS within LANconfig, even for a group of multiple uploads
Voice Call Manager	In case of call forwarding the Caller ID can be set to the internal number of the user or to the original Caller ID where the provider line supports this or to an individual number per each subscriber
Features as of LCOS 7.60	
Router / ARF	Automatic learning of routing tags for ARF contexts from the routing table
Firewall	New trigger for firewall rules depending on backup status, e.g. simplified rule sets for low-bandwidth backup lines
QoS / session limits	Limitation of the number of session per remote site (ID). Setting relative bandwidth limits for QoS in percent. Bandwidth control and QoS also for UMTS connections
RIP	The names of RIP sources can use wildcards, which simplifies the configuration in large installations
PPP	Setting of the protocol for PPP authentication. MS-CHAPv2 support. Optional connection to RADIUS server for MS-CHAPv1 and MS-CHAPv2
COM-port server and forwarding	COM-port server for DIN and USB interfaces on LANCOM routers and access points. For multiple serial devices connected to it, the server also manages its own virtual COM ports via Telnet (RFC 2217) for remote maintenance (works with popular virtual COM-port drivers compliant with RFC 2217)
IPSec VPN backup	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)
Certificates	New OpenSSL implementation with FIPS-140-certified algorithms. Secure Key Storage protects a private key (PKCS12) from theft
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
WLC monitoring & management	Standardized and combined monitoring view of WLAN Controller clusters. Internal storage of up to three script files (max. 64K) for provisioning access points without a separate HTTP server. Automatic monitoring of all devices in a cluster simply by selecting one controller in the cluster
Public Spot	Support for public certificates and certificate chains from positions of trust for Public Spots. This allows popular browsers to access trustworthy login pages with secure access (HTTPS) without warnings from LANCOM devices.
SIP registrar	Configurable registration (with/without) and line monitoring (inactive, automatic, with re-registration, with OPTIONS requests) for SIP trunk, link, remote gateway and SIP-PBX line
SIP proxy	Switchable support for privacy/call screening (call number suppression) per line compliant with RFC 3325 or with remote party ID. Implementation depending on subscriber settings (CLIR). Support for Request URI (RFC 3261)
New WEBconfig	Completely reworked Web interface for LANCOM router and access point configuration. Similar to LANconfig with a system overview, syslog and events display, symbols in the menu tree, quick access with side tabs. WEBconfig now also features new Wizards for basic configuration, security, Internet access, LAN-LAN coupling + online help
HTTPS client	For downloading firmware and configuration files from an HTTPS server, e.g. for roll-out management
New firewall GUI	New 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)
Simplified config management	Exchange of configuration files between similar devices, e.g. for migrating existing configurations to new LANCOM products. New, non-modal help window that can dock with the configuration window. Context-sensitive help display. Configurable tool bar (add/remove symbols, size settings, show/hide subtitles) with new symbols for storage and properties.
LANmonitor	Optimized, sorted display of VPN connections. Display and storage of internal Syslog buffer (events) from LANCOM devices
Trace Wizard / diagnosis files	Improvement of graphical TRACES with Wizards for standard diagnostics. Export of diagnostic files for support purposes (including bootlog, sysinfo and device configuration without passwords)

LCOS LANCOM Operating System

Features as of LCOS 7.50	
WLAN controller 802.11n access point support	Direct support for the LANCOM L-300 series Access Points via LANCOM WLAN Controller (without additional licenses)
WLAN Controller firmware deployment	Central firmware distribution to multiple LANCOM wireless routers and LANCOM access points by the WLAN Controller (firmware provision from web server required). 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
WLAN Controller script distribution	Enables the complete configuration of non-Wi-Fi specific functions such as redirects, protocol filter, ARF etc.
WLAN Controller 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 which 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 LED, e-mail, SYSLOG and SNMP traps
Wi-Fi Public Spot	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 adapted to the hotel or clinic by uploading the individual logo. Function works without external RADIUS and accounting servers
LANconfig	Revised wizards for basic settings, Internet and Wi-Fi. Preferences for LANconfig can be saved and restored per user or globally for several users or per project. The new multi-column view allows for immediate overview of core device information (name, description, address, device status, progress, device type, hardware release, serial number, MAC address, firmware version, FirmSafe, 1. image version, 2. image version). Columns can be hidden and the view can be sorted by each column. From LCOS 7.54: Automatic storage of the current configuration before firmware updates, detection and display of the new LANCOM ES-2126/ES-2126P managed switches.
LANmonitor	Advanced diagnostic functionality with TRACES directly from within LANmonitor. Convenient dialog windows for configuration and filter settings for output. Revocation of certificates within LANmonitor. Sorted view of VPN connections. From LCOS 7.54: Search function within TRACE tasks. Monitoring of the new managed switches LANCOM ES-2126/ES-2126P
WEBconfig	New setup wizards for Internet configuration, Wi-Fi and Public Spot Management rollout wizard Rollout support for LANCOM devices in large scale projects.
Management Rollout Wizard	Support for large project rollouts. After pre-configuration with basic settings, the LANCOM device is provisioned with a project- and location specific configuration when installed on location
VoIP Media Proxy	Termination and interconnection of multiple media streams. Control of SIP-connection media sessions. IP address and port translation for media stream packets. Connection of parties at media stream level where a call transfer in SIP (REFER) is not possible.
Dynamic routing	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
Specific DNS forwarding	Separate entry for backup DNS servers per forwarding rule
VPN certificates	Support for digital, multi-level X.509 certificates, compatible with Microsoft Server/Enterprise Server and OpenSSL. Now certificate hierarchies are supported when the certificates are uploaded in a single PKCS#12 file via WEBconfig (HTTPS) or LANconfig
RADSEC	Secure communication between RADIUS server and client with certificate based authentication
Wi-Fi point-to-point connections	Radio modules with assigned names (radio ID). Now the configuration of point-to-point connections allows to use the radio IDs as references instead of MAC addresses
Wi-Fi background scanning	Custom adjustment of scanning time/filter for faster roaming decisions
DFS	Conformance to DFS as of ETSI 301 893 version 1.3 for all Wi-Fi devices with 5 GHz radio brought to market from April 2008 on 5-GHz radio modules
Dynamic DNS update with GnuDIP client	As of LCOS 7.54, the GnuDIP protocol is supported for updating DNS servers with dynamic IP addresses. The protocol offers security that is superior to DynDNS (Salt and MD5 Digest). The GnuDIP server with self-signup functions and DNS Dynamic Update Protocol for DNS servers is available as open-source software
Firmware compression	A new compression algorithm improves the use of flash ROM for firmware storage with LCOS 7.54
SIP proxy	Support for early and late initiation of SDP negotiation (as of LCOS 7.56)
ADSL multi-mode	New ADSL line code and support for various line codes for ADSL, ADSL2 and ADSL2+ in one firmware (as of LCOS 7.56)
Features as of LCOS 7.20	
VoIP PBX	PBX functions integrated into all LANCOM VoIP routers: Hold call, transfer call, connect call to and from any internal and external subscriber (SIP, analog, ISDN); call forwarding immediately, on busy or after a wait time for all internal subscribers; suppression of second calls (busy-on-busy); group calls with parallel or sequential ringing (group cascading); FAX over with T.38; multi-login to reach a subscriber via multiple terminal devices using one telephone number
1-Click-VPN	"1-Click VPN" for VPN-connection configuration between LANCOM routers by drag&drop in LANconfig. "1-Click VPN Client" for simple configuration of VPN-client dial-in, including automatic generation of an import profile for LANCOM Advanced VPN Client by LANconfig
Advanced Routing and Forwarding (ARF)	Virtualized LANCOM routing engine: Depending on the device, up to 64 independent routing contexts can be provided, each with independent interfaces, IP networks, VLANs, rules for routing, firewall and QoS, DHCP server, DNS settings, etc. Dedicated firewall rules can allow a controlled transition between these (normally strictly separated) contexts for shared use of IP infrastructure (server, printer, etc.).
SCEP	Automatic creation, rollout and renewal of certificates via SCEP (Simple Certificate Enrollment Protocol). In combination with LANCOM Pro-Adaptive VPN, self-configuring certificate-based networks can be rolled out fully automatically.

LCOS LANCOM Operating System

Integrated RADIUS/EAP server	Integrated RADIUS/EAP server for self-sufficient 802.1x authentication with EAP-TLS, EAP-TTLS, PEAP, MSCHAP and MSCHAPv2.
Rapid Spanning Tree	Support for rapid spanning tree for fast path resolution in case of redundant layer 2 connections.
Wi-Fi client roaming improvements	New expert settings for fine tuning the roaming behavior when in Wi-Fi client mode
WLAN Controllers	As of LCOS 7.20, all LANCOM Wi-Fi access points and Wi-Fi routers support operations with LANCOM WLAN Controllers.
Uninterrupted 5 GHz Wi-Fi connections with DFS	As of LCOS 7.20, the limitation requiring 5-GHz outdoor radio paths operated with DFS to be interrupted for one minute every 24 hours no longer applies. The connection can now be operated for any length of time on the channel selected by the DFS algorithm until a radar signal is detected.
Extended port forwarding	Inverse masking can now be defined for multiple IP addresses and can be bound to TCP and/or UDP.
HTTP tunnel for remote-maintenance access	A TCP/HTTP tunnel can be used to access LAN devices after authentication.
Extended VLAN support	Support for Ethernet frames with multiple VLAN tags (Q-in-Q) and support for VLAN over (V)DSL WAN connections
Fuzzy CRON actions	Timed control can be varied, for example, for the staggering of time-controlled connections to multiple devices.
New UMTS cards	Support for UMTS cards “Option GT 3G CDMA - HSDPA 7.2 Ready” and “web ‘n’ walk ExpressCard II (Option GE0201)”
Configurable reset button	The behavior of the reset button is configurable (reset & boot, boot only, or ignore) for the protection of devices in public areas.
Bridge groups	Interfaces such as Ethernet ports, SSIDs or point-to-point connections can now be individually connected to one another through multiple bridges.
Features as of LCOS 6.24	
WLANmonitor	The new WLANmonitor detects and displays rogue Wi-Fi access points. Displayed information includes: channel occupied, network name, Wi-Fi MAC address, encryption method and signal strength at the access points which detected the rogue AP or client.
Wi-Fi background scanning	The detection or rogue access points and channel properties is carried out almost unnoticeably (few ms) for all Wi-Fi channels during normal AP operation. .
Wi-Fi client detection	Rogue Wi-Fi client detection based on probe requests.
Fast client roaming	With background scanning, mobile access points in client mode can switch to alternative access points which offer a better signal before the connection to the first access point fails.
WPA2 fast roaming	Pre-authentication and PMK caching for fast 802.1x authentication
LED display for signal quality	In addition to the standard display (the number of associated clients), devices can now directly display the signal strength of a Wi-Fi client or over a point-to-point connection. This can be of help when setting up transmission paths, for example.
802.1x supplicant	Authentication of an access point in Wi-Fi client mode at another access point via 802.1x (EAP-TLS, EAP-TTLS and PEAP).
Automatic daylight-saving time	Although the NTP module internally works with UTC, the local time can automatically be adjusted for daylight-saving time.
Accounting snapshot	Snapshot function for regular exact read-outs of values (connection time, online time, transfer volumes per station) at the close of a billing period.
Public key SSH	Certificate-based SSH authentication (alternative to PSK)
Proadaptive VPN	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.
VPN certificate requests	Extended Cisco interoperability in certificate-based IPSec installations by supporting an optional “CERTREQ” request.
New VoIP codecs	Optimal voice coding with G.729 as a low-bitrate codec, for example for WAN connections over ADSL, and with the G.722 high-quality codec between ISDN and SIP. The codecs are available for all “VoIP integrated” devices and for “VoIP ready” devices with the Advanced VoIP option.
DTMF tone dialing	Tone dialing (DTMF) by means of RFC 2976 (SIP INFO) or RFC 2833 (RTP payload for DTMF digits).
AOC support	Transmission of AOC (advice of charge) information between the internal and external ISDN interfaces with appropriate “VoIP integrated” products. Two types are supported: AOC-D for advice of charge during a call, and AOC-E for advice of charge at the end of a call.
Features as of LCOS 6.10	
ISDN point-to-point connection	In addition to the support for ISDN point-to-multipoint connections, LANCOM now also supports ISDN point-to-point connections. Multiple connections can be collected together under a root number and extensions
SIP trunking	By using SIP trunking (ITU Q.1912), an appropriate SIP account can be used by multiple subscribers, each of which has an individual extension number.
SIP remote gateway	The ISDN interface of a LANCOM router with VoIP functions can be used as a local dial-in or dial-out point, for instance by a central VoIP PBX.
Layer 2 / Layer 3 tagging	The prioritization information in 802.1p VLAN frames on Ethernet (layer 2) can be set as layer 3 attributes (DiffServ), enabling prioritization information to be transmitted from end to end along routes. Terminal devices emitting packets with 802.1p-tagged frames will be answered with 802.1p frames.
802.11e / WME	Support for wireless LAN Quality of Service according to Wireless Multimedia Extensions (WME) for prioritization in Wi-Fis.
RADIUS server	A Wi-Fi access point with integrated RADIUS server can make its access control list (MAC address filter) available to further access points.
Certificate Revocation Lists	With a revocation list, certificates can be revoked prior to their expiry date. LANCOM VPN gateways with CRL support can query certificate authority CRLs via HTTP, either at regular intervals or briefly before a certificate is due to expire.
RAS user template	All certificate-controlled VPN client connections in Config Mode can now be operated via a single configuration setting (RAS user template). It is no longer necessary to create configuration files on a per-client basis.
USB printer port	Enables USB printers to act as network printers. Support for RAW and LPR protocols. Bidirectional data exchange, for example to send messages about toner level. Parallel print jobs are saved on the PCs and processed in sequence.
ISDN leased lines	As of this version, the formerly optional leased-line support is now a standard feature in all devices featuring ISDN.
Extended UMTS support	In combination with the UMTS/VPN option, the “HSDPA-ready” UMTS cards Option GT Fusion+ and Option GT max are supported. (Update: This option is activated as standard on all LANCOM 3550 Wireless models as of LCOS 6.14.)

LCOS LANCOM Operating System

Features as of LCOS 6.02	
SIP proxy	Management of local SIP users with optional automatic registration/authentication. Mapping of public SIP-provider accounts for shared use. Connection to up to four upstream SIP PBXs including line backup. SIP connections from/to internal subscribers, SIP providers and SIP PBXs with automatic login of SIP users at SIP providers/ upstream SIP PBXs. Optional shared/individual password for authentication at an upstream SIP PBX. Automatic bandwidth management and automatic configuration of the firewall for SIP connections. Backup connections via ISDN if the SIP line is unavailable; set in the Voice Call Manager (VCM). Default DNS entry for the local SIP domains, support for service location records (SRV) especially for SIP.
SIP/ISDN gateway	Operation direct at ISDN exchange lines or at ISDN extension lines of existing PBXs. Local ISDN subscribers register as local SIP users, and local ISDN subscribers automatically register as SIP users at upstream SIP PBXs. Number translation between internal numbers and MSN and automatic adaptation of caller numbers and called numbers at the transition. ISDN supplementary services CLIP, CLIR, en-block dial, individual dialing with adjustable wait time until completion.
Voice Call Manager (VCM)	Central switching of all incoming and outgoing calls. Number translation by mapping, numeral replacement and number supplementation. Configuration of line and route selection, entry of multiple alternative routes (line backup). Routing based on calling and called number, SIP domain and line. Manual routing by the user ("outside-line access codes"); routing with line-selection keys on telephones or telephone number prefixes; targeted routing for individual telephone numbers (e.g. emergency calls via local ISDN); separate routes for internal, local, long-distance or international calls; blocking of telephone numbers or blocks of telephone numbers; inclusion of local SIP and ISDN subscribers into the number range of upstream SIP PBXs; internal standard telephone number for undeliverable calls; supplement/remove line-related dialing prefixes or trunk numbers.
VoIP Setup Wizard	Installation Wizard in LANconfig for connections to SIP providers, SIP PBXs, SIP subscribers, ISDN subscribers and ISDN PBXs, and VCM configuration.
VoIP monitoring	Status display for VoIP subscribers, lines and connections; VoIP trace in the command-line interface.
VoIP processing	G.168 echo cancellation, adaptive de-jitter buffer, inband tone signaling to the German standard, transparent pass-through for negotiated codecs, interaction on codec negotiation between subscribers (filtering, optimization for quality or bandwidth), voice coding to G.711 (a-law, u-law, 64 kbps) or G.726 (16, 24, 32, 40 kbps).
VoIP Quality of Service	QoS adapted for voice connections with dynamic bandwidth reservation per connection and automatic selection of the voice compression method. Prioritization (CoS), and DiffServ marking of voice packets, traffic shaping (incoming/outgoing) and packet-size management of non-prioritized connections compared to VoIP
Extended UMTS support	In combination with the UMTS/VPN option, the "HSDPA-ready" UMTS cards Option GT 3G+ are supported (e.g. T-Mobile "Mobile DSL Card").
Features as of LCOS 5.20	
ADSL2+	ADSL2+ A downstream speed of up to 24 Mbps can be achieved with the ADSL2+ standard, compliant with ITU G.992.5. A software update to LCOS 5.20 featuring new ADSL line code makes the following products ADSL2+ compliant; LANCOM 821+, LANCOM 1721 VPN and LANCOM 1821 Wireless ADSL (1821 from hardware release E).
VRRP	VRRP (Virtual Router Redundancy Protocol) provides a manufacturer-independent redundancy protocol according to RFC 3768. Multiple VRRP-capable devices can be combined to form a standby group, generally with one device acting as master and maintaining the connections. With this VRRP master set as the default gateway and reachable via virtualized MAC and IP addresses, redundant routers provide network backup without the need to make manual changes in the LAN. As standard the LANCOM VRRP function is triggered by device failure, although this can also be linked with the availability of individual remote stations, or with the function of connections or interfaces. Another option is the parallel load-balancing operation of multiple devices, which then act to back each other up. The short propagation time (standard 1s) and the virtualization of the default gateway provides an extremely fast and transparent failover.
NAT-T	NAT-Traversal allows IPSec VPN applications to operate over connections using routers that do not support VPN pass-through. The consistency of the TCP/IP header in ESP packets is automatically checked during the IKE negotiation. Where necessary, these ESP packets are encapsulated in an additional IP header, so preventing VPN connections from being interrupted by devices which don't carry out IPSec masquerading
New UMTS cards	With LCOS 5.20 and an activated UMTS/VPN option, the LANCOM 3550 Wireless now supports the following UMTS data cards: Novatel Wireless U530 and U630, Option GT 3G Fusion and Option GT 3G Quad.
IEEE 802.11h	In Europe, compliance with the ETSI standard is a prerequisite for operating 5-GHz Wi-Fi connections with the maximum approved transmission power of 1000mW, and LANCOM has supported the necessary mechanisms (e.g.TPC and DFS) for some considerable time already. We have now supplemented this with improved channel swapping according to IEEE 802.11h.
HTTPS remote configuration	LANconfig now additionally supports encrypted remote configuration via HTTPS. This offers AES 256-bit protection when updating configurations or when uploading scripts and firmware. For remote maintenance without encryption (e.g. when using ISDN direct dial-in, or inside a VPN), HTTP can be used as an alternative to TFTP, thus enabling faster data transmission during remote management.
PPPoE Server	Layer-2 authentication of users or user groups with PPPoE clients is now supplemented by a PPPoE server function.
Wi-Fi bandwidth limitation	The maximum allowable Wi-Fi transmit and receive data rates can be limited on a per-client basis.
LAN / DMZ intrusion prevention	The IP address checks of the intrusion detection module can now be applied to LAN and DMZ interfaces and allocated network zones. The "strict" setting only accepts IP addresses allocated to the interface.
Spanning Tree	The Spanning Tree protocol helps Ethernet devices in any meshed network to establish redundant paths without undesirable loops.
Per client VLAN-ID	A separate VLAN-ID can be allocated to each Wi-Fi client.
DHCP client IDs	When acting as a DHCP client, a LANCOM can supplement transmitted DHCP requests with a device name in the form of a vendor class identifier. User-specific information can be transmitted as a user class ID.
WAN RIP propagation	Dynamic routing entries learned by RIP can now be propagated over the WAN, too. A masquerading method and a routing tag can optionally be defined for each remote site.

LCOS LANCOM Operating System

Features as of LCOS 5.00	
X.509 digital certificates	Improved security for IPSec VPNs: Digital certificates can now be used for LAN-LAN coupling and VPN client dial-in connections. Supported are self-signed PKCS#12 soft certificates created by the Microsoft Certificate Services (Server or Enterprise Server) or OpenSSL. Digital certificates have numerous advantages over the pre-shared key method: › VPN clients can be operated in the more secure IKE main mode › Reciprocal certificate verification › Additional information can be integrated into certificates (e.g. company name, division, etc.) › Time-limited validity › No more 'simple' passwords – lower susceptibility to dictionary attacks › Support for Smartcards and tokens – prevents passwords being read from notebooks/PCs › Integration in Active Directory environments – central rights management The PKCS#12 files with root certificate, device certificate and private key can be uploaded to devices with WEBconfig via https. The LANCOM Advanced VPN Client features an import function.
AES-256 and IPCOMP	AES encryption now operates with bit depths of 128, 192 and 256 bits. Hardware AES acceleration can still be used with appropriate devices. The Blowfish encryption depth now operates with up to 448 bits. IPCOMP offers data compression in the VPN tunnel. Data throughput in the VPN tunnel can be accelerated with the compression algorithms LZS and Deflate.
Load balancing	Depending on the model, up to 4 external DSL modems or termination routers can be connected directly to the switch ports to provide additional WAN ports. Automatic load balancing means that extra broadband connections can simply be plugged in for an overall increase in performance. There is also complete redundancy in case of the failure of one or more lines.
ML-PPP	Up to 4 PPPoE connections (e.g. lines with DSL modems) can be combined with channel bundling. This increases not only the transfer capacity but the effective maximum speed as well. For example, 4 PPPoE-based SHDSL connections with 2 Mbps each can be unified to an 8-Mbps connection.
Configurable switch ports	Many models support the flexible programming of switch port functions. The operating modes are 'off', LAN port, separate DMZ port, WAN port (for additional WAN interfaces for load balancing), and monitor port. A monitor port can be used for diagnostics by outputting all of the traffic at the other Ethernet LAN and WAN ports.
Policy-based routing / tags	The firewall can attach a tag to a data packet after initiation by any trigger or rule. These tags are processed in the extended routing table. The result is fully flexible routing that was formerly based only on destination addresses. In combination with load balancing, certain services such as VoIP, VPN or e-mail can be directed exclusively through certain lines. Depending on the data type, one of a multitude of default routers can be addressed as determined by the sender address, DiffServ marking, or depending on the protocol used.
Wi-Fi group configuration	LANconfig makes administration easier with the central configuration of multiple grouped Wi-Fi access points. A group configuration can be assigned to a group folder to centrally define uniform Wi-Fi parameters (e.g. encryption, access control lists) for all of the devices in that group. Changes to the group configuration are carried out for all devices in the group. Discrepancies from the group configuration are detected and an update suggested automatically. Devices can be integrated into a group simply by drag and drop, and group parameters can be derived from a single device.
WLANmonitor	The new WLANmonitor makes child's play of the centralized surveillance of Wi-Fi installations. For each Wi-Fi device, the registered clients are displayed along with the frequency channel in use, the encryption settings, and the current signal quality, and data rate. Simply clicking on a client marks the access point that it is logged on to. Non-authenticated clients are shown in red along with the reason for the error.
Scripting	The new scripting interface allows command-line parameters to be transferred via script files. Scripting offers the following advantages: › For the first time, a portions of a configuration can be transferred to the device(s), such as firewall settings, access control lists, VPN or DHCP/DNS settings › Scripts can be transferred between different software versions and different types of device › Batch programming of all LANCOM functions realizes new applications, such as a ''test mode'' for changing parameters with the help of the ''Flash off'' and ''Sleep'' commands › Scripts are easy to read, clear and compact as only values that differ from the factory settings are listed › Scripts contain LANCOM commands in plain text and can be edited with any text program. Even comments are generated automatically. Scripts are uploaded with Loadscript at the command line or via a LANconfig context menu item. The new Readscript command allows the export of the commands executed for a configuration to a text file.
Delete Wizard	LANconfig now features a Wizard for the complete removal of unwanted connections and remote sites along with all related configuration settings.
ISDN site verification	Protection from break-ins with stolen devices—routers with an ISDN interface can call themselves back to establish if the router is still situated at its intended location. If this check fails, then the device locks up and no data transfers will be possible, for example over a VPN connection to the company.
Wake-up on LAN	Supports device remote activation /remote PC wake-up upon receipt of activation packets.
Transparent Wi-Fi client mode	A MAC-transparent mode is available when operating a LANCOM access point as a Wi-Fi client. This allows MAC address-based authentication in client mode as well.
DFS blacklists / whitelists	The DFS channel switching times in 5-GHz Wi-Fis can be optimized with lists of suitable channels.
TFTP file names with variables	The distribution of software, such as of individual device configurations and scripts, is aided by the inclusion of variables—i.e. the respective MAC or IP address, device serial number or identifier—in the file names of the integrated TFTP servers and clients.
Features as of LCOS 4.12	
UMTS support	A UMTS data card can be operated in the external card bus of the LANCOM 3550 / 3050 Wireless models in combination with the new LANCOM UMTS/VPN Option. Currently supported are the UMTS/GPRS data cards U-530 and U-630 from Novatel Wireless. UMTS-based broadband access can be realized, for example for a 'mobile conference room' allowing Wi-Fi or LAN access to the company's network from any location over UMTS and VPN. What's more, UMTS is an ideal backup as it offers more speed, better reliability, and lower long-term running costs than the typical DSL backups via ISDN. The UMTS/Wi-Fi router activates 5 VPN tunnels simultaneously for the UMTS/VPN.

LCOS LANCOM Operating System

Features as of LCOS 4.00	
LEPS—extended Wi-Fi security	The innovative LANCOM Enhanced Passphrase Security method (LEPS) is a new technology offering each and every Wi-Fi user a separate WPA passphrase without the need of complex 802.1x infrastructure. Until now, it was necessary to issue all Wi-Fi clients with the same password (i.e. if an employee departs from the company then all Wi-Fi clients have to be reconfigured) or to operate an 802.1x infrastructure featuring an EAP-capable (Extended Authentication Protocol) RADIUS server. LEPS is simple and yet ingenious. A LANCOM access point can manage an individual passphrase for each MAC address. Access to the Wi-Fi is only permitted with the combination of the MAC address and its associated passphrase. LEPS functions with all WPA / 802.11i-capable clients. The access control list with the approved MAC addresses and individual passphrases can be stored in the LANCOM access point or in any standard RADIUS server.
Wi-Fi hardware data compression	Effective immediately, all 54-Mbit LANCOM access points and 54-Mbit AirLancer client adapters can make use of their integrated hardware data compression. This increases the effective data throughput rate in combination with bursting and turbo mode from 40 Mbps (standard: 20 to 30 Mbps) to a value of 60 Mbps – even when using AES encryption at the same time.
802.11i for Wi-Fi P2P connections	Now point-to-point Wi-Fi connections can take advantage of the AES hardware encryption that is featured in the LANCOM 54 Mbit radio module. The combination of WLAN turbo mode and transmitting powers of up to 1000mW at 5 GHz (802.11a) allows the operation of wireless connections that are secure from interception (thanks to 802.11i) at up to 108 Mbps and over distances in excess of one kilometer.
Default encryption for Wi-Fi	Device-specific Wi-Fi encryption is activated by default in the settings from the factory and after resetting. This ensures that a minimum of security is provided even if the user forgets to run the installation and security wizards or following a reset. The 13-character default WEP128 key is made up of the device's 12-character MAC address preceded by an 'L'.
Redundant VPN gateways	Activation of multiple VPN end points (mostly identically configured central VPN gateways operated in parallel) for load balancing and high availability within large VPN installations. Should line polling (dead-peer detection, ICMP line polling) indicates a failure, then a variety of strategies (e.g. "random") can be used to enable communication to a different VPN end point. At the central headquarters, the new outbound router and the local default gateway are propagated by dynamic routing (RIP V2).
IKE config mode	Automatic allocation of IP addresses to VPN remote sites, for example to the LANCOM Advanced VPN Client.
Access for multiple administrators	Several administrators can access the device with individual passwords and access rights. The device password formerly in use is now exclusively for the supervisor. Extended login functions are now available under WEBconfig, telnet, TFTP and SNMP. Up to 16 roles can be defined with differing rights for configuring the device and running functions.
SSH configuration access	Support for the SSH protocol as an additional method for accessing the command-line interface, for example with the freely available "PuTTY" tool (telnet via SSH client, for Windows and Unix).
Port mapping	Enables freely definable port remapping, for example to divert local servers to non-standard ports.
Multi-PPPoE	Now one DSL access can be used to operate multiple Internet accesses to different Internet service providers. Multiple PPPoE sessions can be used, for example, as an ISP backup or for separate invoicing of business and private Internet access.
RIP via WAN	RIP via WAN The propagation of static or dynamic routes via RIP V2 can now take place over the WAN, for example for the updating of routes within closed networks (e.g. MPLS-based VPNs).
Manual MTU definition	In addition to the automatic adaptation of the maximum packet size over a certain transmission route, theses values can now also be statically overwritten. This is necessary, for example, for tunneled connections operated by Internet service providers who resell DSL connections. In these cases, the automatic MTU negotiation with the DSL access provider can cause an oversized MTU value (e.g. 1492) as the tunneling to the ISP can lead to additional overhead. In such cases, the MTU can be reduced manually (e.g. to 1400 bytes).
"Loopback" addresses	A device can be assigned up to 16 additional IP addresses so that the device can be uniquely identified (e.g. for the maintenance of devices in multiple networks using the same IP address range).
Internal logging	In addition to the existing firewall event log, the activated SYSLOG module stores the last 100 SYSLOG messages directly in the device; this is useful, for example, as an "error memory" for the remote diagnosis of interrupted connections.
Software version management with LANconfig	Simple version management with this firmware archive plus update function. Either for the convenient, centralized update of installations with different types of devices, or even for a specific rollback.
New LANmonitor	Now with button bar for direct access to functions and new windows management for supervising larger installations.
Analog and GPRS modem	Connecting an external analog or GSM/GPRS modem to the serial interface ('Config/COM') provides an additional fully-functional WAN connection. All functions are available including hold time, automatic return to the standard connection when using Backup, or dial-in connections (e.g. for remote maintenance). Even Dynamic VPN applications that rely on the exchange of IP addresses per telephone connection are possible. Individual modem parameters can be configured with AT commands. Line status and connect rates are displayed clearly in LANmonitor. Owing to the different circuitry, the LANCOM Modem Adapter Kit is necessary for the operation of external modems.
Additional polling addresses	End-to-end connection monitoring by ICMP polling ('ping') now has up to four polling addresses. The backup event is only triggered when contact is lost to all polling addresses.
Wi-Fi P2P connections with 802.11i	The integrated AES encryption in Wi-Fi radio modules can now be used for Wi-Fi point-to-point connections too.
N:N mapping for all devices	Formerly implemented for VPN devices only, N:N IP-address mapping is now available for devices without VPN—for example, for integrating locations with MPLS networks.
CPU-load and memory display	LANmonitor displays detailed information such as the CPU type and speed, total memory and current free memory in the system information under 'Device'.
Extended ping command	The new option '–a' enables the definition of a dedicated sender address (e.g. intranet, DMZ or any). As early as when commissioning the device, the router can be tested in advance for correct functioning in relation to other routed networks.
Extended comment fields	Four freely definable comment fields are now available to handle the general device information such as device name, location and administrator.
Features as of LCOS 3.50	
Wi-Fi	LCOS 3.50 provides a Wi-Fi security update for all LANCOM Wi-Fi routers, access points and AirLancer clients adapters with 54 Mbps radio modules. Supported encryption methods are 802.11i/AES and WPA/TKIP. 802.11i provides a security level according to FIPS 140-2. The AES encryption utilizes the integrated hardware encryption engines of the LANCOM 54 Mbps radio modules, which ensure a encryption at full speed. Additionally, the installation of WPA passphrases is much more comfortable than WEP.

LANCOM Systems

LCOS LANCOM Operating System

Features as of LCOS 3.42	
Multi SSID	Each Wi-Fi radio module now supports up to 8 different radio cells (SSIDs). All settings for security and access can be independently configured for each SSID. This, for example, enables a private Wi-Fi intranet to be operated parallel to a separate, public Wi-Fi hotspot.
Super A/G	Increases the transfer rates in 2.4 and 5 GHz Wi-Fis. The 108-Mbit Turbo Mode bundles two vacant Wi-Fi channels and so doubles the effective bandwidth. Bursting combines multiple packets to save overhead and uses the available bandwidth more effectively. Hardware data compression can be used for point-to-point connections between two access points.
VPN trigger call	VPN connections to a set remote station can now be triggered by an ISDN data call.
ISDN backup for Dynamic VPN	ISDN backup functions formerly suffered from limitations in combination with dynamic VPN: These limitations now no longer apply. It is now possible to use dynamic VPN to secure an ISDN direct-dial connection with dynamic IP addresses at both ends.
IP redirect	For each SSID, dedicated Wi-Fi-to-wired LAN transfer points can be defined so that data packets received from the Wi-Fi are forcibly redirected to just one set IP address
Features as of LCOS 3.32	
VPN upgrade	Upgraded VPN gateway functions: 5 VPN channels integrated (instead of 2 channels) for all products of the 1600 and 1800 series. Former VPN-2 Option upgraded to 5 channels
QoS	Extended Quality-of-Service features – optimum Voice-over-IP for voice quality via VPN connections. Also available to the already integrated (send-side) bandwidth management: › Extended IP QoS › Dynamic download „slow down“ › Automatic packages adaptation and PMTU setting or fragmentation (jitter reduction) (in particular for low ADSL upstream bandwidths) › DiffServ-Trigger in the IP-Router and the firewall
Virtual LANs (VLAN)	VLAN enables separate networks use common LAN or Wi-Fi infrastructures › VLAN-ID connecting segments › VLAN-Prio enabled Quality-of-Service › VLAN-capable switches convert normal Ethernet to the VLAN segment and back
N:N IP mapping	IP address mapping from one network to another address range › VPN network coupling also with identical IP networks › N:N address mapping on well-defined IP addresses („loopback-addresses“) › Central SNMP management for several networks with identical IP addresses
LANconfig/LANmonitor	Multitasking – project management and monitoring (e.g. centralized firmware update) Hardware integration and configuration, registration of change history Real-time remote monitoring per SNMP trap Monitoring of all relevant technical events (VPN, Wi-Fi, connections, security), recording of all changes.

Supported Devices

The information which devices are eligible for the current LCOS version can be found at the following link:
https://www.lancom-systems.com/products/firmware/version-overview/