LANCOM SYSTEMS

lancom-systems.com

LCOS 10.90

LANCOM vRouter

Virtualized performance for best scalability

vRouter

The LANCOM vRouter is a software-based router for operation in virtualized environments based on a hypervisor like VMware ESXi, Amazon Web Services (AWS), Hyper-V, or Microsoft Azure. With its comprehensive range of functions and the numerous security features based on the operating system LCOS, it offers the best basis for modern infrastructures. Be it as a virtual VPN router (vCPE), as central-site VPN gateway (vGateway), or as WLAN controller (vWLC), it is ideally suited for systems integrators, service providers, and for operation in medium-sized and large enterprises.

- → Virtual, software-based router for operation with VMware ESXi, Amazon Web Services (AWS), Hyper-V, or Microsoft Azure
- → Applicable as branch router (vCPE), central-site VPN gateway (vGateway) or WLAN controller (vWLC)
- → IPSec-VPN functionality for up to 3,000 VPN channels and WLAN controller function for up to 1,500 WLAN devices
- → Easy management via the LANCOM Management Cloud or LANtools
- → Radical simplification of the configuration with SD-WAN
- → Instant deployment anywhere: Dramatic reduction of deployment times wherever the router is required
- → Available as vRouter 50, 250, 1,000, and unlimited for different performance requirements
- → Integrated Public Spot Option (incl. PMS accounting plus)
- → Integrated HA clustering function

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.90

LANCOM vRouter

Network Function Virtualization

The LANCOM vRouter offers you maximum versatility in terms of performance and network size, and thus ideal adaptation to your individual infrastructure. It replaces hardware components in classic infrastructures and enables optimally scalable networking thanks to the virtualization of network functions (NFV).

Proven operating system virtualized

The LANCOM vRouter is a product that uncompromisingly unites the LANCOM core values of security, reliability and sustainability. Secure because it is based on the tried-and-trusted operating system LCOS. Reliable because the long-standing know-how of our employees has been incorporated into the product development. Sustainable because it supports advanced technologies such as SD-WAN, the latest virtualization technologies, and management via the LANCOM Management Cloud.

Virtualized WLAN controller functionality

In addition to a VPN router (vCPE) and a central-site VPN gateway (vGateway), the LANCOM vRouter now also supports the role of a virtual WLAN controller (vWLC). This allows full virtualization of WLAN controller functionalities on a virtualization platform such as VMWare ESXi, Amazon Web Services (AWS), Hyper-V or Microsoft Azure. The number of managed access points depends on the license category activated on the vRouter.

Instant deployment anywhere

The routers are deployed with just a few clicks and within seconds instead of hours: At any location around the world, wherever a router is required, the LANCOM vRouter is created automatically—without any shipping or hardware installation! Be it in a lab environment, in your own server room or data center, or in the cloud.

Radical simplification of the configuration with SD-WAN

In combination with the LANCOM Management Cloud, the LANCOM vRouter opens the way for automated management. The software-defined WAN (SD-WAN) enables the automatic setup of secure VPN connections between sites, including network virtualization across the wide-area network: A few mouse clicks is all it takes to enable the VPN function and select the required VLANs for each site. The laborious configuration of individual tunnel endpoints is no longer required at all.

State-of-the-art security

The LANCOM vRouter supports the very latest security functions including IPSec-VPN based on IKEv2, elliptic curves, and AES-GCM—for IPv4 and IPv6 networks. This advanced technology ensures that remote sites and mobile workers are securely integrated into the network and that corporate data remains well protected. All of this comes guaranteed backdoor-free thanks to IT security Made in Germany.

LANCOM vRouter

WLAN profile settings*	
Radio channels 6 GHz	Up to 24 non-overlapping channels (EU; 20 MHz channel width)
Radio channels 5 GHz	Up to 26 non-overlapping channels (available channels and further obligations such as automatic DFS dynamic channel selection depending on national regulations)
Radio channels 2.4 GHz	Up to 13 channels, max. 3 non-overlapping (depending on country-specific restrictions)
Concurrent WLAN clients	Depends on the access points in operation
IEEE 802.11u	Managed LANCOM Access Points support the WLAN standard IEEE 802.11u (Hotspot 2.0) which allows mobile clients a seamless transition from the cellular network into WLAN hotspots. Authentication methods using SIM card information, certificates or username and password, enable an automatic, encrypted login to WLAN hotspots of roaming partners - without the need to manually enter login credentials
Roaming	Seamless handover between radio cells, IAPP support with optional restriction to an ARF context, IEEE 802.11d support
Opportunistic Key Caching	Opportunistic key caching allows fast roaming processes between access points. WLAN installations utilizing a WLAN controller and IEEE 802.1X authentication cache the access keys of the clients and are transmitted by the WLAN controller to all mananged access points
Fast roaming	Based on IEEE 802.11r, allows fast roaming procedures between access points. This is possible by using IEEE 802.1X authentication or pre-shared keys in controller based WLAN installations, which save the access keys temporarily and distribute them to the managed access points.
Security	WPA3-Personal, IEEE 802.11i / WPA2 with passphrase (WPA2-Personal) or IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise) and hardware-accelerated AES, closed network, WEP64, WEP128, WEP152, user authentication, IEEE 802.1x /EAP, WPA1/TKIP, LEPS-MAC, LEPS-U
Time Control	time-based activation and deactivation of WLAN networks
Quality of Service	Prioritization according to Wireless Multimedia Extensions (WME, subset of IEEE 802.11e)
Background scanning	Detection of rogue AP's and the channel information for all WLAN channels during normal AP operation. The Background Scan Time Interval defines the time slots in which an AP or Router searches for a foreign WLAN network in its vicinity. The time interval can be specified in either milliseconds, seconds, minutes, hours or days
Client detection	Rogue WLAN client detection based on probe requests
Auto WDS*	Auto WDS allows wireless integration of access points in existing WLAN infrastructure, including managment via WLAN controller.
Space Time Block Coding (STBC)*	Coding method according to IEEE 802.11n. The Space Time Block Coding improves reception by coding the data stream in blocks.
Low Density Parity Check (LDPC)*	Low Density Parity Check (LDPC) is an error correcting method. IEEE 802.11n uses convolution coding (CC) as standard error correcting method, the usage of the more effective Low Density Parity Check (LDPC) is optional.
*) Note	Depends on the access points in operation

LCOS 10.90

LANCOM vRouter

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

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

WLAN-Controller	
Number of managed devices*	Up to 1,500 LANCOM Access Points and WLAN routers can be centrally managed by the WLAN controller. Capacities can be expanded even further by clustering multiple controllers.
Smart Controller technology	The WLAN controller can switch user data per AP Radio or per SSID in the following ways: – Direct switching to the LAN at the AP (for maximum performance, e.g. for IEEE 802.11n-based access points) – Logical seperation of user data into VLANs (e.g. for WLAN guest access accounts) – Central tunneling to the Controller* (layer 3 tunneling between different IP Subnets)
Auto Discovery	LANCOM access points and WLAN routers automatically discover the WLAN controller by means of DNS name or IP addresses. Even AP's at remote sites or in home offices with no direct access to the Controller can be integrated into the central Controller

LANCOM vRouter

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

LCOS 10.90

LANCOM vRouter

WLAN-Controller	
VLAN and IP contexts	A fixed VLAN can be set for each SSID. The WLAN controller can independently provide up to 64 separate IP networks, and each of these can be individually mapped to VLANs and, consequently, to SSIDs (Advanced Routing and Forwarding, ARF). The Controller can provide, among others, individual DHCP, DNS, routing, firewall and VPN functions for these networks.
Dynamic VLAN assignment	Dynamic VLAN assignment for target user groups based on MAC addresses, BSSID or SSID by means of external RADIUS server.
RADIUS server	Integrated RADIUS server for MAC address list management. Support for RADSEC (Secure RADIUS) for secure communication with RADIUS servers.
EAP server	Integrated EAP server for authentication of IEEE 802.1X clients via EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MSCHAP or MSCHAPv2
RADIUS/EAP proxy per SSID	Proxy mode for external RADIUS/EAP servers (forwarding and realm handling) per SSID
Redundancy, Controller backup and load balancing	Every managed LANCOM AP can be assigned to a group of alternative WLAN controllers. A suitable Controller is selected within this group depending on AP load. This ensures that also in backup state the load of larger installations remains equally distributed.
LED control	The LEDs of administrated WLAN devices can be centrally deactivated via the WLAN controller
CA hierarchy	The Certificate Authority (CA) can be structured hierarchically when using multiple WLAN controllers. This allows access points to swap between different WLAN controllers without certificate conflicts. The Certificate Revocation Lists (CRL) can be shared between the different devices
Load balancing	When using multiple WLAN controllers the access points are distributed evenly among the different WLAN controllers to offer the best load balancing. In case one WLAN controller is unavailable the access points are edistributed among the remaining WLAN controllers automatically. Once it is restored they are redistributed again.
Backup	A priority can be set for the WLAN Controller which allows operating in hot standby mode. Access points switch automatically to the WLAN controller with the highest priority
Fast roaming	VoWLAN devices require seamless roaming for ensuring optimal speech quality. The Access Points support PMK caching and Pre-authentication for such demanding applications. WPA2 and WPA2-PSK operate with sub-85 ms roaming times (requirements: adequate signal quality, sufficient RF overlap, clients with a low roaming threshold).
QoS	IEEE 802.11e / WME: Automatic VLAN tagging (IEEE 802.1p) in the Access Points. Mapping to DiffServ attributes in the WLAN controller if this is deployed as a layer-3 router
Background scanning, rogue-AP and rogue-client detection	Background scanning does not interupt normal AP operation and collects information on the radio channel load (AP acts as a 'Probe' or 'Sensor' by going off-channel). Foreign Access Points and clients is sent to the Rogue AP Detection in LANCOM WLANmonitor.
WLAN visualization	The management tool LANCOM WLANmonitor acts as a central monitoring program for the WLAN controller and visualizes the performance of all WLAN controllers, Access Points, SSIDs and clients.
WLAN client limiting	To ensure that load is evenly balanced between multiple Access Points, each one can be set with a maximum number of allowable WLAN clients.

LANCOM vRouter

WLAN-Controller	
*)	In order to manage up to 1500 devices LCOS 10.50 RU3 or higher is required. For previous LCOS versions the maximum number of devices is 1000.

Public Spot - Technical details	
Login via web portal (Captive Portal)	Login to the hotspot after entry of username and password via a web portal (freely definable)
Self-service login to the hotspot (Smart Ticket)	Login credentials to the public spot network are sent to the user through SMS or e-mail. The e-mail is sent via SMTP. The sms is transmitted via the integrated 3G/4G modem, an e-mail-2-SMS gateway or a 3G/4G router in the network
Voucher print	With just a few mouseclicks a ticket with login credentials for the hotspot can be generated and be printed with any office printer. The voucher can be individually designed.
Easy Public Spot login with one click	After accepting the terms of use, the user gets a WLAN guest access for a definable period
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.
Re-login	The Public Spot identifies known WLAN 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 - significantly increased comfort for regular guests.
Walled Garden functionality	Enables a free access to selected websites, even without activation of the guest access (e.g. sponsoring, corporate or hotel websites)
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 of standard accounts
Support of volume- and time-based accounts	Validity of a hotspot access can be defined with regard to download volume limitation per user or to a limited time period
Redirection to advertisment websites	The Public Spot user can be redirected to advertisement websites of the provider at configurable time intervals
Dynamic VLAN allocation	Allocation of Public Spot users to individually configurable networks
Idle timeout-based disconnect	Connection will be disconnected after x minutes without Internet access
Multi login	Allows Public Spot users to login to one hotspot account with multiple devices

Public Spot - External data interfaces	
RADIUS server interface	By default the Public Spot records session-specific data for later billing on an internal RADIUS server. The forwarding to an external RADIUS server can be configured on a device with Public Spot, if required
SYSLOG	LANCOM devices are equipped with an integrated SYSLOG. Alternatively, LANCOM devices can be connected to external SYSLOG servers
XML	In order to provide further authentication szenarios apart from login with username and password, the LANCOM Public Spot solution can be connected to external servers via an XML interface

LCOS 10.90

LANCOM vRouter

Public Spot - External data interfaces	
FIAS	Enables a direct communication between the LANCOM Public Spot and a Property Management System (PMS) which supports the FIAS protocol as supported by Micros Fidelio.
Layer 2 features	
VLAN	4.096 IDs based on IEEE 802.1q, dynamic assignment
Multicast	IGMP-Snooping, MLD-Snooping
Protocols	ARP-Lookup, LLDP, ARP, Proxy ARP, BOOTP, DHCP
Layer 3 features	
Firewall	Stateful inspection firewall including paket filtering, extended port forwarding, N:N IP address mapping, paket tagging, support for DNS targets, user-defined rules and notifications
Quality of Service	Traffic shaping, bandwidth reservation, DiffServ/TOS, packetsize control, layer-2-in-layer-3 tagging, support for 8 QoS queues (6 free configurable)
Security	Intrusion Prevention, IP spoofing, access control lists, Denial of Service protection, detailed settings for handling reassembly, session-recovery, PING, stealth mode and AUTH port, URL blocker, password protection, programmable reset button
PPP authentication mechanisms	PAP, CHAP, MS-CHAP, and MS-CHAPv2
High availability / redundancy	VRRP (Virtual Router Redundancy Protocol), analog/GSM modem backup
Router	IPv4-, IPv6-, IPv4/IPv6 dual stack
SD-WAN Application Routing	SD-WAN Application Routing in connection with the LANCOM Management Cloud
SD-WAN dynamic path selection	SD-WAN dynamic path selection in connection with the LANCOM Management Cloud
Router virtualization	ARF (Advanced Routing and Forwarding) up to separate processing of 4096 contexts (depending on installed vRouter license)
IPv4 services	HTTP and HTTPS server for configuration by web interface, DNS client, DNS server, DNS relay, DNS proxy, dynamic DNS client, DHCP client, DHCP relay and DHCP server including autodetection, NTP client, SNTP server, policy-based routing, Bonjour-Proxy, RADIUS
IPv6 services	HTTP and HTTPS server for configuration by web interface, DHCPv6 client, DHCPv6 server, DHCPv6 relay, DNS client, DNS server, dynamic DNS client, NTP client, SNTP server, Bonjour-Proxy, RADIUS
Dynamic routing protocols	RIPv2, BGPv4, OSPFv2, LISP (Locator/ID Separation Protocol)
IPv4 protocols	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, PPPoE (server), RADIUS, RADSEC (secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3

LCOS 10.90

LANCOM vRouter

Layer 3 features	
IPv6 protocols	NDP, stateless address autoconfiguration (SLAAC), stateful address autoconfiguration (DHCPv6), router advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, LISP, Syslog, SNMPv1,v2c,v3, MLDv2, PIM, NPTv6 (NAT66), VRRPv3
Multicast Routing	PIM (Protocol Independent Multicast), IGMP proxy, MLD proxy
WAN operating mode	VDSL, ADSL1, ADSL2 or ADSL2+ additional with external DSL modem at an ETH port
WAN protocols	PPPoE, Multi-PPPoE, ML-PPP, GRE, EoGRE, PPTP (PAC or PNS), L2TPv2 (LAC or LNS), L2TPv3 with Ethernet-Pseudowire, IPoE (using DHCP or no DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 and IPv4/IPv6 dual stack session), IP(v6)oE (autokonfiguration, DHCPv6 or static)
Tunneling protocols (IPv4/IPv6)	6to4, 6in4, 6rd, Dual Stack Lite, 464XLAT

Security	
Intrusion Prevention	Monitoring and blocking of login attempts and port scans
IP spoofing	Source IP address check on all interfaces: only IP addresses belonging to the defined IP networks are allowed
Access control lists	Filtering of IP or MAC addresses and preset protocols for configuration access and LANCAPI
Denial of Service protection	Protection from fragmentation errors and SYN flooding
General	Detailed settings for handling reassembly, PING, stealth mode and AUTH port
Password protection	Password-protected configuration access can be set for each interface
Alerts	Alerts via e-mail, SNMP traps and SYSLOG
Authentication mechanisms	PAP, CHAP, MS-CHAP and MS-CHAPv2 as PPP authentication mechanism

High availability / redundancy	
VRRP	VRRP (Virtual Router Redundancy Protocol VRRPv2 and VRRPv3) for backup in case of failure of a device or remote station.
HA-Clustering	Due to the grouping of several individual devices to one device group (cluster), configuration changes conducted for one device can be automatically synchronized with all cluster devices, without having to manage each device manually (Config Sync - integrated from vRouter 500 or higher.)
Load balancing	Static and dynamic load balancing over up to 3 WAN connections. Channel bundling with Multilink PPP (if supported by network operator)
VPN redundancy	Backup of VPN connections across different hierarchy levels, e.g. in case of failure of a central VPN concentrator and re-routing to multiple distributed remote sites. Any number of VPN remote sites can be defined (the tunnel limit applies only to active connections). Up to 32 alternative remote stations, each with its own routing tag, can be defined per VPN connection. Automatic selection may be sequential, or dependant on the last connection, or random (VPN load balancing)

LANCOM vRouter

High availability / redundancy	
Line monitoring	Line monitoring with LCP echo monitoring, dead-peer detection and up to 4 addresses for end-to-end monitoring with ICMP polling
VPN	
IPSec over HTTPS	Enables IPsec VPN based on TCP (at port 443 like HTTPS) which can go through firewalls in networks where e. g. port 500 for IKE is blocked. Suitable for client-to-site connections and site-to-site connections. IPSec over HTTPS is based on the NCP VPN Path Finder technology
Number of VPN tunnels	Max. number of concurrent active IPSec, PPTP (MPPE) and L2TPv2 tunnels: up to 3,000 (depending on installed vRouter license). Unlimited configurable connections. Configuration of all remote sites via one configuration entry when using the RAS user template or Proadaptive VPN.
1-Click-VPN Client assistant	One click function in LANconfig to create VPN client connections, incl. automatic profile creation for the LANCOM Advanced VPN Client
1-Click-VPN Site-to-Site	Creation of VPN connections between LANCOM routers via drag and drop in LANconfig
IKE, IKEv2	IPSec key exchange with Preshared Key or certificate (RSA signature, ECDSA-Signature, digital signature)
Smart Certificate*	Convenient generation of digital X.509 certificates via an own certifaction authority (SCEP-CA) on the webpage or via SCEP.
Certificates	X.509 digital multi-level certificate support, compatible with Microsoft Server / Enterprise Server and OpenSSL. Secure Key Storage protects a private key (PKCS#12) from theft.
Certificate rollout	Automatic creation, rollout and renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) per certificate hierarchy
Certificate revocation lists (CRL)	CRL retrieval via HTTP per certificate hierarchy
OCSP Client	Check X.509 certifications by using OCSP (Online Certificate Status Protocol) in real time as an alternative to CRLs
OCSP Server/Responder*	Offers validity information for certificates created with Smart Certificate via OCSP
XAUTH	XAUTH client for registering LANCOM routers and access points at XAUTH servers incl. IKE-config mode. XAUTH server enables clients to register via XAUTH at LANCOM routers. Connection of the XAUTH server to RADIUS servers provides the central authentication of VPN-access with user name and password. Authentication of VPN-client access via XAUTH and RADIUS connection additionally by OTP token
RAS user template	Configuration of all VPN client connections in IKE ConfigMode via a single configuration entry
Proadaptive VPN	Automated configuration and dynamic creation of all necessary VPN and routing entries based on a default entry for site-to-site connections.
Algorithms	3DES (168 bit), AES-CBC and -GCM (128, 192 or 256 bit), RSA (1024-4096 bit), ECDSA (P-256-, P-384-, P-521-curves) and Chacha20-Poly 1305. OpenSSL implementation with FIPS-140 certified algorithms. MD-5, SHA-1, SHA-256, SHA-384 or SHA-512 hashes
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.90

LANCOM vRouter

VPN	
MOBIKE	IKEv2 VPN clients can seamlessly switch between different networks (e.g. from WLAN to mobile radio) without having to re-establish the VPN tunnel
Dynamic DNS	Enables the registration of IP addresses with a Dynamic DNS provider in the case that fixed IP addresses are not used for the VPN connection
Specific DNS forwarding	DNS forwarding according to DNS domain, e.g. internal names are translated by proprietary DNS servers in the VPN. External names are translated by Internet DNS servers
Split DNS	Allows the selective forwarding of traffic for IKEv2 depending on the addressed DNS domain.
IPv4 VPN	Connecting private IPv4 networks
IPv4 VPN over IPv6 WAN	Use of IPv4 VPN over IPv6 WAN connections
IPv6 VPN	Connecting private IPv6 networks
IPv6 VPN over IPv4 WAN	Use of IPv6 VPN over IPv4 WAN connections
Radius	RADIUS authorization and accounting, outsourcing of VPN configurations in external RADIUS server in IKEv2, RADIUS CoA (Change of Authorization)
High Scalability VPN (HSVPN)	Transmission of multiple, securely separated networks within a VPN tunnel
Advanced Mesh VPN	On demand dynamic VPN tunnel establishment between branches
IKEv2-EAP*	VPN clients can be authenticated with IKEv2-EAP against a central database like Microsoft Windows Server or RADIUS Server
*) Note	available for license "vRouter 250" or higher

Interfaces	
Ethernet ports	5 individual 10/100/1000/10.000 Mbps Ethernet ports; up to 3 ports can be operated as additional WAN ports with load balancing. Ethernet ports can be disabled within LCOS configuration.
Port configuration	Each Ethernet port can be freely configured (LAN, DMZ, WAN, monitor port, off). Additionally, external DSL modems or termination routers can be operated as a WAN port with load balancing and policy-based routing. DMZ ports can be operated with their own IP address range without NAT

Management and monitoring	
Management	LANCOM Management Cloud, LANconfig, WEBconfig, LANCOM Layer 2 management (emergency management)
Management functions	Individual access and function rights up to 16 administrators, RADIUS and RADSEC user management, remote access (WAN or (W)LAN, access rights (read/write) adjustable seperately), SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, access rights via TACACS+, scripting, timed control of all parameters and actions through cron job
automatic firmware update	configurable automatic checking and installation of firmware updates

LANCOM SYSTEMS

lancom-systems.com

LCOS 10.90

LANCOM vRouter

Management and monitoring	
Monitoring	LANCOM Management Cloud, LANmonitor
Monitoring functions	Device SYSLOG, SNMPv1,v2c,v3 incl. SNMP-TRAPS, extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, internal logging buffer for firewall events
Monitoring statistics	Extensive Ethernet, IP and DNS statistics; SYSLOG error counter, accounting information exportable via LANmonitor and SYSLOG, Layer 7 Application Detection including application-centric tracking of traffic volume
IPerf	IPerf is a tool for measurements of the bandwidth on IP networks (integrated client and server)
SLA-Monitor (ICMP)	Performance monitoring of connections
Netflow	Export of information about incoming and outgoing IP traffic
SD-LAN	SD-LAN – automatic LAN configuration via the LANCOM Management Cloud
SD-WAN	SD-WAN – automatic WAN configuration via the LANCOM Management Cloud
Scope of delivery	
Manual	Printed Installation Guide (DE/EN)
Minimum requirements	
Supported hypervisors	→ VMWare ESXi 6.0 or higher (on Intel XEON processor with AES instructions set (Intel AES-NI) and HW virtualization (Intel VT-x)) → Hyper-V on Microsoft Windows Server 2016 / 2019 oder Windows 10 (on Intel XEON processor with AES instructions set (Intel AES-NI) and HW virtualization (Intel VT-x))
Supported cloud platforms	→ Microsoft Azure
Minimal requirements virtualization hardware	→ 1 virtual x86 CPU → RAM: • 2 GB (recommended for vRouter 50, vRouter 250) • 4 GB (recommended for vRouter 500, vRouter 1000) • 8 GB (recommended for vRouter Unlimited) → 512 MB of disk space (SSD recommended) → 1-5 network interfaces (vmxnet3 or Hyper-V Synthetic NIC) → Note: When using vRouter 250, 500, 1000 or in particular vRouter unlimited a high cpu rate is recommended
Support	
Software updates	During the term of a valid license - regular free updates (LCOS operating system and LANtools) via Internet

LCOS 10.90

LANCOM vRouter

Support	
LANcare Direct 24/7	Direct, prioritized 10/5 manufacturer support incl. 24/7 emergency hotline and security updates for the device, guaranteed first response times (SLA) of max. 30 minutes for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years. vRouter 50 and vRouter 250: LANcare Direct 24/7 S (item no. 10752, 10753 or 10754) vRouter 500: LANcare Direct 24/7 M (item no. 10755, 10756 or 10757) vRouter 1000: LANcare Direct 24/7 L (item no. 10758, 10759 or 10760) vRouter unlimited: LANcare Direct 24/7 XL (item no. 10761, 10762 or 10763)
LANcare Direct 10/5	Direct, prioritized 10/5 manufacturer support and security updates for the device, guaranteed first response times (SLA) of max. 2 hours for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years. vRouter 50 and vRouter 250: LANcare Direct 10/5 S (item no. 10740, 10741 or 10742) vRouter 500: LANcare Direct 10/5 M (item no. 10743, 10744 or 10745) vRouter 1000: LANcare Direct 10/5 L (item no. 10746, 10747 or 10748) vRouter unlimited: LANcare Direct 10/5 XL (item no. 10749, 10750 or 10751)
LANCOM Management Cloud	
LANCOM LMC-C-1Y LMC License	LANCOM LMC-C-1Y License (1 Year), enables the management of one category C device for one year via the LANCOM Management Cloud, item no. 50106
LANCOM LMC-C-3Y LMC License	LANCOM LMC-C-3Y License (3 Years), enables the management of one category C device for three years via the LANCOM Management Cloud, item no. 50107
LANCOM LMC-C-5Y LMC License	LANCOM LMC-C-5Y License (5 Years), enables the management of one category C device for five years via the LANCOM Management Cloud, item no. 50108
Accessories	
VPN Client Software	LANCOM Advanced VPN Client for Windows 7,8/8.1,10,11 - single license, item no. 61600
VPN Client Software	LANCOM Advanced VPN Client for Windows 7,8/8.1,10,11 - 10 licenses, item no. 61601
VPN Client Software	LANCOM Advanced VPN Client for Windows 7,8/8.1,10,11 - 25 licenses, item no. 61602
VPN Client Software	LANCOM Advanced VPN Client for Mac OS X (10.5 Intel only, 10.6 or higher), single license, item no. 61606
VPN Client Software	LANCOM Advanced VPN Client for Mac OS X (10.5 Intel only, 10.6 or higher), 10 licenses, item no. 61607
Item number(s)	
LANCOM vRouter 50 (1 Year)	59000 (10 VPN channels, 50 Mbps bandwith, 8 ARF contexts, 128 Public Spot users, Management of 10 access points/WiFi routers)*
LANCOM vRouter 50 (3 Years)	59001 (10 VPN channels, 50 Mbps bandwith, 8 ARF contexts, 128 Public Spot users, Management of 10 access points/WiFi routers)*
LANCOM vRouter 50 (5 Years)	59012 (10 VPN channels, 50 Mbps bandwith, 8 ARF contexts, 128 Public Spot users, Management of 10 access points/WiFi routers)*

LCOS 10.90

LANCOM vRouter

Item number(s)	
LANCOM vRouter 250 (1 Year)	59002 (50 VPN channels, 250 Mbps bandwith, 16 ARF contexts, 256 Public Spot users, Management of 50 access points/WiFi routers)*
LANCOM vRouter 250 (3 Years)	59003 (50 VPN channels, 250 Mbps bandwith, 16 ARF contexts, 256 Public Spot users, Management of 50 access points/WiFi routers)*
LANCOM vRouter 250 (5 Years)	59013 (50 VPN channels, 250 Mbps bandwith, 16 ARF contexts, 256 Public Spot users, Management of 50 access points/WiFi routers)*
LANCOM vRouter 500 (1 Year)	59008 (100 VPN channels, 500 Mbps bandwith, 64 ARF contexts, unlimited Public Spot users, Management of 100 access points/WiFi routers)*
LANCOM vRouter 500 (3 Years)	59009 (100 VPN channels, 500 Mbps bandwith, 64 ARF contexts, unlimited Public Spot users, Management of 100 access points/WiFi routers)*
LANCOM vRouter 500 (5 Years)	59014 (100 VPN channels, 500 Mbps bandwith, 64 ARF contexts, unlimited Public Spot users, Management of 100 access points/WiFi routers)*
LANCOM vRouter 1000 (1 Years)	59004 (200 VPN channels, 1000 Mbps bandwith, 128 ARF contexts, unlimited Public Spot users, Management of 200 access points/WiFi routers)*
LANCOM vRouter 1000 (3 Years)	59005 (200 VPN channels, 1000 Mbps bandwith, 128 ARF contexts, unlimited Public Spot users, Management of 200 access points/WiFi routers)*
LANCOM vRouter 1000 (5 Years)	59015 (200 VPN channels, 1000 Mbps bandwith, 128 ARF contexts, unlimited Public Spot users, Management of 200 access points/WiFi routers)*
LANCOM vRouter unlimited (1000 Sites, 1 Year)	59006 (1000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users, Management of 1000 access points/WiFi routers)*
LANCOM vRouter unlimited (1000 Sites, 3 Years)	59007 (1,000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users, Management of 1000 access points/WiFi routers)*
LANCOM vRouter unlimited (1000 Sites, 5 Years)	59016 (1,000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users, Management of 1000 access points/WiFi routers)*
LANCOM vRouter unlimited (3000 Sites, 1 Year)	59022 (3,000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users, Management of 1,500 access points/WiFi routers)*
LANCOM vRouter unlimited (3000 Sites, 3 Years)	59023 (3,000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users, Management of 1,500 access points/WiFi routers)*
LANCOM vRouter unlimited (3000 Sites, 5 Years)	59024 (3,000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users, Management of 1,500 access points/WiFi routers)*
DEMO option	The 30 days DEMO option (containing 10 mbps of throughput, 3 ARF networks, 3 VPN tunnels, and 128 Public Spot users) can be created for free via the LANCOM webpage under "Service & Support".
*) Note	When unlicensed the vRouter is limited to 1 mbps throughput, 3 ARF networks, 1 VPN peer and 128 public spot users. Licenses can not be used additively and can not be combined. Once the lifetime of the license is exceeded the vRouter can be used as licenced, but firmware updates and configurations changes are not possible any longer.

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