LANCOM SYSTEMS

lancom-systems.de

LCOS 10.80

LANCOM vRouter

Virtualisierte Performance für beste Skalierbarkeit

vRouter

Der LANCOM vRouter ist ein Software-basierter Router für den Betrieb in einer virtualisierten Umgebung basierend auf einem Hypervisor wie VMware ESXi, Amazon Web Services (AWS), Hyper-V oder Microsoft Azure. Mit seinem umfassenden Funktionsspektrum und den zahlreichen Sicherheitsfeatures basierend auf dem Betriebssystem LCOS ist er die beste Grundlage für modernste Infrastrukturen. Ob als virtueller VPN-Router (vCPE), als Central Site VPN-Gateway (vGateway) oder WLAN-Controller (vWLC) eignet er sich insbesondere für Systemhäuser, Service Provider sowie im Einsatz in mittleren und großen Unternehmen.

- → Virtueller, Software-basierter Router für den Betrieb mit VMware ESXi, Amazon Web Services (AWS), Hyper-V oder Microsoft Azure
- → Einsetzbar als Filial-Router (vCPE), Central Site VPN-Gateway (vGateway) oder WLAN-Controller (vWLC)
- → IPSec-VPN-Funktionalität für bis zu 3.000 VPN-Kanäle sowie WLAN-Controller-Funktion für bis 1.500 WLAN-Geräte
- → Einfaches Management über die LANCOM Management Cloud oder LANtools
- → Radikale Vereinfachung der Konfiguration mit SD-WAN
- → Instant & anywhere Deployment: Dramatische Reduktion der Bereitstellungszeiten wo immer der Router benötigt wird
- → Erhältlich als vRouter 50, 250, 1.000 und unlimited für verschiedene Leistungsstufen
- → Integrierte Public Spot Option (inkl. PMS-Accounting-Plus)
- → Integrierte HA-Clustering-Funktion

LANCOM SYSTEMS

lancom-systems.de

LCOS 10.80

LANCOM vRouter

Network Function Virtualization

Der LANCOM vRouter bietet Ihnen hinsichtlich Geschwindigkeit und Netzwerkgröße höchste Flexibilität und damit eine ideale Anpassung auf Ihre individuelle Infrastruktur. Er ersetzt Hardwarekomponenten in klassischen Infrastrukturen und ermöglicht dank Virtualisierung von Netzwerkfunktionen (NFV) eine optimal skalierbare Vernetzung.

Bewährtes Betriebssystem virtualisiert

Der LANCOM vRouter ist ein Produkt, das die LANCOM Kernwerte Sicherheit, Zuverlässigkeit und Zukunftsfähigkeit kompromisslos vereint. Sicher, weil er auf dem jahrelang erprobten und bewährten Betriebssystem LCOS basiert. Zuverlässig, weil das langjährige Knowhow unserer Mitarbeiter in die Produktentwicklung eingeflossen ist. Zukunftsfähig, weil er fortschrittlichste Technologien wie SD-WAN, modernste Virtualisierung und das Management über die LANCOM Management Cloud unterstützt.

Virtualisierte WLAN-Controller-Funktionalität

Der LANCOM vRouter unterstützt die Rollen VPN-Router (vCPE), Central Site VPN-Gateway (vGateway) und auch die Rolle eines virtuellen WLAN-Controllers (vWLC). Damit können WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi, Amazon Web Services (AWS), Hyper-V oder Microsoft Azure virtualisiert werden. Die Anzahl verwalteter Access Points ist dabei abhängig von der Lizenzkategorie des vRouters.

Instant & anywhere Deployment

Die Bereitstellung von Routern erfolgt mit wenigen Klicks innerhalb von Sekunden statt bisher Stunden: An jedem Ort weltweit, wo immer der Router benötigt wird, kann ein LANCOM vRouter automatisiert erzeugt werden - ganz ohne den Versand und die Installation von Hardware! Egal ob in einer Laborumgebung, im eigenen Server-Raum, im Rechenzentrum oder in der Cloud.

Radikale Vereinfachung der Konfiguration mit SD-WAN

In Kombination mit der LANCOM Management Cloud eröffnet der LANCOM vRouter den Weg für automatisiertes Management. Mit Software-defined WAN (SD-WAN) ermöglicht er die automatische Einrichtung sicherer VPN-Verbindungen zwischen Standorten, inklusive Netzwerkvirtualisierung auch über die Weitverkehrsstrecken: Die VPN-Funktionalität wird per Mausklick aktiviert und die gewünschten VLANs werden für den jeweiligen Standort ausgewählt. Die aufwändige Konfiguration der einzelnen Tunnelendpunkte entfällt vollständig.

State-of-the-art Security

Der LANCOM vRouter unterstützt aktuellste Sicherheitsfunktionenen wie IPSec-VPN basierend auf IKEv2, elliptische Kurven und AES-GCM - selbstverständlich für IPv4 und IPv6. Mit dieser fortschrittlichen Technologie werden Standorte sicher miteinander vernetzt, mobile Mitarbeiter sicher in das Netzwerk integriert und unternehmensinterne Daten bestens geschützt. Und das alles bei garantierter Backdoor-Freiheit und IT-Security Made in Germany.

LANCOM vRouter

WLAN Profileinstellungen*	
Funkkanäle 5 GHz	Bis zu 26 nicht überlappende Kanäle (verfügbare Kanäle je nach landesspezifischer Regulierung und mit automatischer, dynamischer DFS-Kanalwahl verbunden)
Funkkanäle 2,4 GHz	Bis zu 13 Kanäle, max. 3 nicht überlappend (landesspezifische Einschränkungen möglich)
Gleichzeitige WLAN Clients	Je nach verwendeten Access Points
IEEE 802.11u	Gemanageten LANCOM Access Points ermöglicht der WLAN-Standard IEEE 802.11u (Hotspot 2.0) einen vom mobilen Benutzer unbemerkten Übergang vom Mobilfunknetz zu WLAN Hotspots. Authentifizierungsmethoden mit SIM-Kartendaten, Zertifikaten oder Benutzername und Passwort ermöglichen eine automatische, verschlüsselte Anmeldung an Hotspots von Roaming-Partnern - ganz ohne aufwändige Eingabe von Login-Daten.
Roaming	Wechsel zwischen Funkzellen (seamless handover), IAPP-Support mit optionaler Zuordnung eines ARF-Kontextes, IEEE 802.11d Support
Opportunistic Key Caching	Opportunistic Key Caching ermöglicht schnelle Roaming-Vorgänge zwischen Access Points. Bei Controller-basierten WLAN-Installationen mit IEEE 802.1X-Authentifizierung werden die Zugangsschlüssel der Clients zwischengespeichert und vom WLAN-Controller automatisch an alle verwalteten Access Points weitergegeben
Fast Roaming	Basierend auf WLAN-Standard IEEE 802.11r, ermöglicht schnelle Roaming-Vorgänge zwischen Access Points. Dies wird in Controller-basierten WLAN-Installationen mit IEEE 802.1X-Authentifizierung oder Pre-Shared Key realisiert, indem die Zugangsschlüssel der Clients zwischengespeichert und automatisch an die verwalteten Access Points weitergegeben werden.
Sicherheit	WPA3-Personal, IEEE 802.11i / WPA2 mit Passphrase (WPA2-Personal) oder IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise) mit hardwarebeschleunigtem AES, Closed Network, WEP64, WEP128, WEP152, User Authentication, IEEE 802.1X /EAP, WPA1/TKIP, LEPS-MAC, LEPS-U
Zeitsteuerung	WLAN-Netze können zeitbasiert aktiviert und deaktiviert werden.
Quality of Service	Priorisierung entsprechend der Wireless Multimedia Extensions (WME, Bestandteil von IEEE 802.11e)
Background Scanning	Erkennung von fremden Access Points ("Rogue Access Points") und der Kanaleigenschaften auf allen WLAN-Kanälen während des normalen Access-Point-Betriebes. Das Background-Scan-Intervall gibt an, in welchen zeitlichen Abständen ein Wireless Router oder Access Point nach fremden WLAN-Netzen in Reichweite sucht. Mit der Zeiteinheit kann ausgewählt werden, ob die eingetragenen Werte für Millisekunden, Sekunden, Minuten, Stunden oder Tage gelten
Client Detection	Erkennung von fremden WLAN Clients ("Rogue Clients") anhand von Probe-Requests
Auto-WDS*	Auto-WDS ermöglicht die kabellose Integration von Access Points in die vorhandene WLAN-Infrastruktur, inklusive Verwaltung durch WLAN-Controller.
Space Time Block Coding (STBC)*	Codierverfahren nach IEEE 802.11n. Bei der STBC-Codierung wird ein Datenstrom zur Übertragung in Datenblöcke codiert, so dass in einem MIMO-System Verbesserungen der Empfangsbedingungen entstehen.
Low Density Parity Check (LDPC)*	Low Density Parity Check (LDPC) ist eine Methode zur Fehlerkorrektur. IEEE 802.11n nutzt als Standardmethode zur Fehlerkorrektur Convolution Coding (CC) und optional die effektivere Methode Low Density Parity Check (LDPC).
*) Hinweis	Je nach verwendeten Access Points

LCOS 10.80

LANCOM vRouter

WLAN-Sicherheit	
Sicherheitsverfahren	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)
Verschlüsselungsalgorithmen	AES-CCMP, AES-GCMP, TKIP, RC4 (nur bei WEP)
EAP-Typen (Authenticator)	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-FAST
Radius/EAP-Server	Benutzerverwaltung von MAC-Adressen, Bandbreitenbegrenzung, Passphrase, VLAN je Benutzer, Authentisierung von IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP, MS-CHAPv2, Dynamic Peer Discovery
Sonstiges	WLAN-Protokollfilter (ACL), IP-Redirect von empfangenen Paketen aus dem WLAN, IEEE 802.1X Supplicant, Background Scanning, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS)
Sonstiges	IEEE 802.11X Supplicant, Background Scanning, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS)

LANCOM Active Radio Control	
Client Management	Steuerung von WLAN Clients auf den sinnvollsten Access Point unter Verwendung von 802.11k und 802.11v
Band Steering	Steuerung von 5 GHz Clients auf dieses leistungsstarke Frequenzband
Managed RF Optimization*	Auswahl optimaler WLAN-Kanäle durch den Administrator
Adaptive Noise Immunity	Immunität vor Störsignalen im WLAN
Spectral Scan	Überprüfen des WLAN-Funkspektrum auf Störquellen
Adaptive RF Optimization	Dynamische Auswahl des besten WLAN-Kanals
Airtime Fairness	Verbesserte Ausnutzung der WLAN-Bandbreite
*) Hinweis	Je nach verwendeten Access Points. Band-/Client-Steering ist in der US-Variante nicht verfügbar.

WLAN-Controller	
Anzahl gemanagter Geräte*	Bis zu 1500 LANCOM Access Points und WLAN-Router können - auch in beliebiger Kombination - durch den LANCOM WLAN-Controller zentral gemanagt werden. Weitere Kapazitätserweiterungen sind über das Clustering mehrerer Controller möglich.
Smart Controller Technologie	Der LANCOM WLAN-Controller unterstützt pro Funkzelle / SSID die unterschiedliche Auskopplung der Nutzdaten: – direkt in das LAN gebridged (maximale Performance z.B. für IEEE 802.11n-basierte Access Points) – per VLAN strikt vom LAN separiert (z.B. für WLAN-Gastzugänge) – zentral zum Controller getunnelt (Layer-3-Tunneling über IP-Netze hinweg)

LCOS 10.80

LANCOM vRouter

WLAN-Controller	
Auto Discovery	Automatisches Finden der WLAN-Controller durch die LANCOM Access Points oder WLAN-Router anhand von IP-Broadcasts, einstellbaren DNS-Namen oder IP-Adressen. Auch Geräte in entfernten Außenstellen oder Home Offices, die nicht direkt einen zentralen Controller erreichen, können in das zentrale Management eingebunden werden.
Authentifizierung und Autorisierung	Access Points können manuell oder automatisch authentifiziert werden. Signalisierung neuer Access Points durch LED-Anzeige, E-Mail-Benachrichtigung, SYSLOG und SNMP-Traps. Manuelle Authentisierung über grafisches Benutzerinterface in LANmonitor oder WEBconfig. Halbautomatische Authentifizierung anhand von Access Point Listen im Controller ("Bulk-Modus"). Vollautomatischer Modus mit einstellbarer Default-Konfiguration (separat an- und abschaltbar, z.B. während der Rollout-Phase). Eindeutige Identifikation authorisierter Access Points anhand digitaler Zertifikate, Zertifikatserstellung durch integrierte CA (Certificate Authority), Zertifikatsverteilung mittels SCEP (Simple Certificate Enrollment Protocol). Sperrung von Access Points mittels CRL (Certificate Revocation List)
Management-Kommunikationsprotokoll	CAPWAP (Control and Provisioning Protocol for Wireless Access Points). Zur Kommunikation zwischen Controller und Access Points genügt eine beliebige IP-Verbindung, so dass auch ein netzwerksegment- und standortübergreifendes WLAN-Management möglich ist.
Layer-3-Tunneling	Layer-3-Tunnel gemäß CAPWAP-Standard, um WLANs pro SSID zu einem IP-Subnetz zu verschalten (Bridge). Die Layer-3-Tunnel transportieren Layer-2-Pakete gekapselt durch Layer-3-Netze zu einem LANCOM WLAN-Controller, so dass der Datenverkehr gemanagter Access Points unabhängig von der bestehenden Netzinfrastruktur aggregiert werden kann. Dies ermöglicht Roaming ohne einen Wechsel der IP-Adresse und das logische Zusammenfassen von SSID, ohne den Einsatz von VLANs
Verschlüsselung	DTLS-Verschlüsselung des Kontrollkanals zwischen WLAN-Controller und Access Point (256 bit AES Verschlüsselung mit digitalen Zertifikaten, inkl. Hardware-Krypto-Beschleuniger, Verschlüsselung zu Diagnosezwecken abschaltbar)
Firmware Management	Konfiguration von mehreren LANCOM Wireless Routern und LANCOM Access Points wird vom Controller aus vorgenommen. Einrichten eines Webservers erforderlich. Eine Automatisierung der Firmware Updates ist möglich. Der WLAN-Controller prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion die aktuell verfügbaren Dateien und vergleicht sie mit den Versionen in den Geräten. Dieser Vorgang kann auch z. B. nachts durch einen Cron-Job ausgelöst werden. Wenn auf dem Access Point nicht die gewünschte Version läuft, lädt der WLAN-Controller diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und Access Points ein.
Skriptverteilung	Ermöglicht die vollständige Konfiguration von nicht WLAN-spezifischen Funktionen wie Redirects, Protokollfilter, ARF etc. Interner Speicher für bis zu drei Skript-Dateien (max. 64 kByte) zur Provisionierung von Access-Points ohne separaten HTTP-Server
RF Management und automatische Funkfeld-Optimierung	Die Kanalzuteilung erfolgt wahlweise statisch oder automatisch. Bei Aktivierung der Funkfeld-Optimierungs-Funktion suchen sich die APs im 2,4 GHz-Band automatisch die optimalen Kanäle. Diese Kanalwahl wird an den Controller übermittelt und der Controller speichert sie für die jeweiligen APs. Funkfeld-Optimierung kann auch für einzelne APs (wiederholt) durchgeführt werden. Sendeleistungseinstellung statisch 0 bis -20 dB. Alarmierung bei Ausfall eines Access Points über LED, E-Mail, SYSLOG und SNMP-Traps
Konfigurationsmanagement	Definition und Gruppierung aller logischen und physikalischen WLAN-Parameter mittels WLAN-Konfigurationsprofilen. Vollautomatische oder manuelle Zuweisung von Profilen zu WLAN Access Points, automatische Konfigurationsübermittlung und -prüfung (Policy Enforcement)
Vererbung von Konfigurationsprofilen	Unterstützung hierarchischer WLAN-Profilgruppen inklusive konfigurierbarer Parameter-Vererbung zur Ableitung abweichender standortspezifischer WLAN-Konfigurationen
Management-Betriebsmodi	Einstellbarer Betriebsmodus "managed" oder "unmanaged" pro Radio-Modul. Bei LANCOM WLAN-Routern wird ausschließlich der WLAN-Teil vom Controller aktiv verwaltet (Split-Management).

LCOS 10.80

LANCOM vRouter

WLAN-Controller	
Autarker Weiterbetrieb	Im "managed"-Modus kann festgelegt werden, ob der Access Point seine WLAN-Konfiguration nicht persistent erhält (keine Speicherung von Konfigurationsdaten, Normalfall im Betrieb mit Controller) und bei Verlust der Verbindung zum Controller sofort den Betrieb einstellt oder ob für eine einstellbare Zeit ein autarker Weiterbetrieb im Rahmen der technischen Möglichkeiten gestattet ist (z.B. Weiterbetrieb von Funkzellen mit WPA2 / PSK bei Ausfall der Controller-Verbindung oder nach Stromausfall). Nach Ablauf der optionalen Weiterbetriebszeit wird die WLAN-Konfiguration im WLAN AP gelöscht. Der autarke Weiterbetrieb ist pro SSID einstellbar.
VLAN und IP-Kontexte	Pro SSID kann ein festes VLAN vorgegeben werden. Der WLAN-Controller kann eigenständig bis zu 64 separate IP-Netze zur Verfügung stellen, die jeweils individuell auf VLANs und damit auch auf SSIDs abgebildet werden können (Advanced Routing and Forwarding, ARF). Der Controller kann unter anderem individuelle DHCP-, DNS-, Routing-, Firewall- und VPN-Funktionen für diese Netze übernehmen.
Dynamische VLAN-Zuweisung	Dynamische VLAN-Zuweisung für bestimmte Benutzergruppen anhand von MAC-Adressen, BSSID oder SSID mittels externem RADIUS-Server
RADIUS-Server	Integrierter RADIUS-Server zur Verwaltung von MAC-Adress-Listen. Unterstützung von RADSEC (Secure RADIUS) zur sicheren Anbindung an RADIUS-Server
EAP-Server	Integrierter EAP-Server zur Authentisierung von IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP oder MS-CHAP v2
RADIUS/EAP Proxy pro SSID	Proxy-Betriebsart für externe RADIUS/EAP-Server (Forwarding und Realm Handling) pro SSID konfigurierbar
Redundanz, Controller-Backup und Lastverteilung	Jedem gemanagten LANCOM Access Point können mehrere alternative WLAN-Controller zugewiesen werden. Innerhalb dieser Gruppen wird auslastungsabhängig ein passender Controller ausgewählt, so dass sich bei größeren Installationen auch im Backup-Fall automatisch eine Gleichverteilung auf alle Controller ergibt.
LED Steuerung	LEDs der verwalteter WLAN-Geräte lassen sich über Profile abschalten
CA-Hierarchie	Die Certificate Authority (CA) kann bei WLAN-Controllern hierarchisch strukturiert werden. Somit können Access Points zwischen den verschiedenen WLAN-Controllern wechseln, ohne dass es zu Zertifaktskonflikten kommt. Certifcate Revocation Lists (CRLs) können untereinander ausgetauscht werden
Load Balancing	Bei der Nutzung von mehreren WLAN-Controllern werden die Access Points gleichmässig auf die verschiedenen WLAN-Controller verteilt um eine optimale Lastverteilung zu gewährleisten. Bei Ausfall eines WLAN-Controllers verteilen sich die Access Points automatisch neu, ist er wieder verfügbar wird auch die Rückverteilung automatisch durchgeführt
Backup	WLAN-Controllern kann eine Priorität zugewiesen werden, was einen Betrieb im Hot-Standby ermöglicht. Access Points wechseln automatisch zu dem WLAN-Controller mit der höchsten Priorität
Fast Roaming	Die Access Points unterstützen PMK-Caching und Pre-Authentication für schnelles Roaming. Im WPA2- und WPA2-PSK-Modus beträgt die Roaming-Zeit unter 85 ms (Voraussetzungen: Ausreichende Signalqualität, hinreichende Überlappung von Funkzellen sowie Clients mit geeignet eingestelltem, niedrigen Roaming-Threshold).
QoS	IEEE 802.11e / WME: Automatisches VLAN-Tagging (IEEE 802.1p) in den Access Points. Umsetzung auf DiffServ-Attribute im WLAN-Controller, sofern dieser als Layer-3-Router zum Einsatz kommt

LANCOM vRouter

WLAN-Controller	
Background Scanning, Rogue AP und Rogue Client Detection	Während des normalen Betriebs kann ohne Unterbrechung des Funkbetriebes im Hintergrund ein Background-Scan gefahren werden, so dass auf allen Kanälen Informationen über alle Funkkanalauslastungen sowie über alle sichtbaren Access Points und Clients gesammelt werden können (Hintergrundbetrieb als "Probe" bzw. "Sensor"). Fremde Access Points und Clients werden zentral an die Rogue AP Detection des LANCOM WLANmonitor gemeldet.
WLAN Visualisierung	Das Management-Programm LANCOM WLANmonitor dient als zentrales Monitoring-Programm für den WLAN-Controller und visualisiert die Zuordnung und Performance von allen WLAN-Controllern, Access Points, SSIDs und Clients.
WLAN Client Limiting	Zur gleichmäßigen Auslastung mehrerer Access Points kann pro Access Point und pro SSID die maximale Anzahl der unterstützen WLAN Clients vorgegeben werden. Darüber hinausgehende Assoziierungsanfragen werden abgelehnt.
*)	Um bis zu 1500 Geräte zu managen wird LCOS 10.50 RU3 oder höher benötigt. Bei vorherigen LCOS Versionen beträgt die maximale Geräteanzahl 1000.

Public Spot - Technische Details	
Anmeldung über Webportal (Captive Portal)	Anmeldung am Hotspot nach Eingabe von Benutzername und Passwort über ein Webportal (frei konfigurierbar)
Selbstständige Benutzeranmeldung am Hotspot (Smart Ticket)	Zugangsdaten zum Public Spot-Netz werden dem Nutzer per E-Mail oder SMS zugesandt. Die E-Mail wird dabei vom Gerät via SMTP verschickt. Der SMS-Versand erfolgt über das integrierte Mobilfunk-Modem, ein E-Mail-2-SMS-Gateway oder einen nachgeschalteten Mobilfunk-Router
Voucher-Ausgabe	Mit wenigen Mausklicks können beliebig viele Tickets (abhängig von der aktivierten Lizenz) mit Zugangsdaten für den Hotspot generiert und über einen beliebigen Office-Drucker ausgedruckt werden. Der Voucher lässt sich individuell gestalten.
Einfacher Public Spot-Login mit einem Klick	Nach Akzeptierung der allgemeinen Nutzungsbedingungen erhält der Benutzer für einen definierbaren Zeitraum Gastzugang
WISPr	Wireless Internet Service Provider roaming erlaubt es SmartClients, sich an einem Public Spot anzumelden, ohne dass der Benutzer Zugangsdaten auf einer Webseite eintragen muss.
Re-Login	Der Public Spot erkennt bekannte Clients und authentifiziert sie automatisch. Nach der erstmaligen Authentifizierung speichert der Hotspot die Client-Informationen (MAC-Adresse) für einen konfigurierbaren Zeitraum, so dass für den Benutzer keine erneute manuelle Eingabe der Zugangsdaten mehr nötig ist - ein deutlicher Komfortgewinn für regelmäßige Gäste.
Walled Garden-Funktion	Ermöglicht, ausgewählte Websites auch ohne Freischaltung des Gastzugangs zugänglich zu machen (z. B. Websites von Sponsoren oder des Hotels)
Bandbreitenmanagement	Die verfügbare Bandbreite für Public Spot-Benutzergruppen lässt sich individuell konfigurieren und steht im Assistenten zum Anlegen eines neuen Benutzers zur Verfügung, z. B. zur Unterscheidung von normalen und Premium-Usern
Unterstützung von volumen- und zeitbasierten Accounts	Gültigkeit eines Hotspot-Zugangs kann über Begrenzung des Download-Volumens der Nutzer oder über die Zeit festgelegt werden
Umleitung auf Werbe-Webseiten	In konfigurierbaren Zeitabständen kann der Public Spot-Benutzer auf Werbe-Webseiten des Betreibers umgeleitet werden

LCOS 10.80

LANCOM vRouter

Public Spot - Technische Details	
Dynamische VLAN-Zuweisung	Zuweisung von Public Spot-Benutzern zu individuell konfigurierbaren Netzen
Idle time out basierter Disconnect	Verbindung wird nach einer konfiguerierbaren Zeit ohne Internetzugriff getrennt
Mehrfach-Login	Gestattet Public Spot-Benutzern, sich mit mehreren Geräten gleichzeitig auf einem Account an einem Hotspot anzumelden

Public Spot - Externe Datenschnittstellen	
RADIUS-Server-Schnittstelle	Standardmäßig speichert der Public Spot sitzungsrelevante Daten für spätere Abrechnungen auf einem internen RADIUS-Server. Bei Bedarf kann auf einem Gerät mit Public Spot die Weiterleitung auf einen externen RADIUS-Server konfiguriert werden
SYSLOG	LANCOM Geräte verfügen über einen integrierten SYSLOG-Speicher. Alternativ können LANCOM Geräte an externe SYSLOG-Server angebunden werden
XML	Um neben der Anmeldung über Benutzername/Passwort noch weitere Authentifizierungsszenarien zur Verfügung zu stellen, kann die LANCOM Public Spot-Lösung mit externen Servern über die XML-Schnittstelle angebunden werden
FIAS	Ermöglicht direkte Kommunikation zwischen dem LANCOM Public Spot und einem Property Management System (PMS), welches das von Micros Fidelio verwendete FIAS-Protokoll unterstützt.

Layer 2-Funktionen	
VLAN	4.096 IDs nach IEEE 802.1q, dynamische Zuweisung
Multicast	IGMP-Snooping, MLD-Snooping
Protokolle	ARP-Lookup, LLDP, ARP, Proxy ARP, BOOTP, DHCP

Layer 3-Funktionen	
Firewall	Stateful Inspection Firewall mit Paketfilterung, erweitertem Port-Forwarding, N:N IP-Adressumsetzung, Paket-Tagging, Unterstützung von DNS-Zielen, unterschiedlichen Aktionen und unterschiedlichen Benachrichtigungen
Quality of Service	Traffic Shaping, Bandbreitenreservierung, DiffServ/TOS, Paketgrößensteuerung, Layer 2-in-Layer 3-Tagging
Sicherheit	Intrusion Prevention, IP-Spoofing, Access-Control-Listen, Denial-of-Service Protection, detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung, URL-Blocker, Passwortschutz, programmierbarer Reset-Taster
PPP-Authentifizierungsmechanismen	PAP, CHAP, MS-CHAP und MS-CHAPv2
Hochverfügbarkeit/Redundanz	VRRP (Virtual Router Redundancy Protocol), Analog/GSM-Modem-Backup
Router	IPv4-, IPv6-, NetBIOS/IP-Multiprotokoll-Router, IPv4/IPv6 Dual Stack
SD-WAN Application-Routing	SD-WAN Application Routing in Verbindung mit der LANCOM Management Cloud

LCOS 10.80

LANCOM vRouter

Layer 3-Funktionen	
SD-WAN Dynamic Path Selection	SD-WAN Dynamic Path Selection in Verbindung mit der LANCOM Management Cloud
Router-Virtualisierung	ARF (Advanced Routing und Forwarding) mit bis zu 4096 Kontexten (abhängig von der aktivierten Lizenz)
IPv4-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DNS-Client, DNS-Server, DNS-Relay, DNS-Proxy, Dynamic DNS-Client, DHCP-Client, DHCP-Relay und DHCP-Server mit Autodetection, NetBIOS/IP-Proxy, NTP-Client, SNTP-Server, Policy-based Routing, Bonjour-Proxy, RADIUS
IPv6-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DHCPv6-Client, DHCPv6-Server, DHCPv6-Relay, DNS-Client, DNS-Server, Dynamic DNS-Client, NTP-Client, SNTP-Server, Bonjour-Proxy, RADIUS
Dynamische Routing-Protokolle	RIPv2, BGPv4, OSPFv2, LISP (Locator/ID Separation Protocol)
IPv4-Protokolle	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, NetBIOS, PPPoE (Server), RADIUS, RADSEC (Secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3
IPv6-Protokolle	NDP, Stateless Address Autoconfiguration (SLAAC), Stateful Address Autoconfiguration (mit DHCPv6), Router Advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, LISP, Syslog, SNMPv1,v2c,v3, MLDv2, PIM, NPTv6 (NAT66)
Multicast Routing	PIM (Protocol Independent Multicast), IGMP-Proxy, MLD-Proxy
WAN-Betriebsarten	VDSL, ADSL1, ADSL2 oder ADSL2+ mit externem Modem an einem ETH-Port (auch simultan zum LAN-Betrieb)
WAN-Protokolle	PPPoE, Multi-PPPoE, ML-PPP, GRE, EoGRE, PPTP (PAC oder PNS), L2TPv2 (LAC oder LNS), L2TPv3 mit Ethernet-Pseudowire, IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 und IPv4/IPv6 Dual Stack Session), IP(v6)oE (Autokonfiguration, DHCPv6 oder Statisch)
Tunnelprotokolle (IPv4/IPv6)	6to4, 6in4, 6rd (statisch und über DHCP), Dual Stack Lite (IPv4-in-IPv6-Tunnel), 464XLAT

Sicherheit	
Intrusion Prevention	Überwachung und Sperrung von Login-Versuchen und Portscans
IP-Spoofing	Überprüfung der Quell-IP-Adressen auf allen Interfaces: nur die IP-Adressen des zuvor definierten IP-Netzes werden akzeptiert
Access-Control-Listen	Filterung anhand von IP- oder MAC-Adresse sowie zuvor definierten Protokollen für den Konfigurationszugang und LANCAPI
Denial-of-Service Protection	Schutz vor Fragmentierungsfehlern und SYN-Flooding
Allgemein	Detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung
Passwortschutz	Passwortgeschützter Konfigurationszugang für jedes Interface einstellbar
Alarmierung	Alarmierung durch E-Mail, SNMP-Traps und SYSLOG
Authentifizierungsmechanismen	PAP, CHAP, MS-CHAP und MS-CHAP v2 als PPP-Authentifizierungsmechanismen

LCOS 10.80

LANCOM vRouter

Hochverfügbarkeit / Redundanz	
VRRP	VRRP (Virtual Router Redundancy Protocol) zur herstellerübergreifenden Absicherung gegen Geräte- oder Gegenstellenausfall.
HA-Clustering	Durch die Zusammenfassung mehrerer Einzelgeräte zu einer Gerätegruppe (Cluster) können Konfigurationsänderungen, die an einem Gerät vorgenommen werden, automatisch auf die anderen Cluster-Geräte übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss (Config Sync - integriert ab vRouter 500 oder höher).
Load-Balancing	Statische und dynamische Lastverteilung auf bis zu 3 WAN-Strecken; Kanalbündlung durch Multilink-PPP (sofern vom Netzbetreiber unterstützt)
VPN-Redundanz	Backup von VPN-Verbindungen über verschiedene Hierarchie-Stufen hinweg, z.B. bei Wegfall eines zentralen VPN-Konzentrators und Ausweichen auf mehrere verteilte Gegenstellen. Beliebige Anzahl an Definitionen für VPN-Gegenstellen in der Konfiguration (Tunnel-Limit gilt nur für aktive Verbindungen). Bis zu 32 alternative Gegenstellen mit jeweils eigenem Routing-Tag als Backup oder zur Lastverteilung pro VPN-Gegenstelle. Die automatische Auswahl kann der Reihe nach, aufgrund der letzten erfolgreichen Verbindung oder zufällig (VPN-Load-Balancing) erfolgen
Leitungsüberwachung	Leitungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling

VPN	
IPSec over HTTPS	Ermöglicht IPSec VPN durch Firewalls in Netzen, für die z. B. Port 500 für IKE gesperrt ist, auf Basis von TCP über Port 443. Geeignet für Client-to-Site und Site-to-Site-Verbindungen. IPSec over HTTPS basiert auf der NCP VPN Path Finder Technology
Anzahl der VPN-Tunnel	Bis zu 3.000 Tunnel gleichzeitig aktiv (abhängig von der aktivierten Lizenz) bei Kombination von IPSec- mit PPTP-(MPPE) und L2TPv2-Tunneln, unbegrenzte Anzahl konfigurierbarer Gegenstellen. Konfiguration aller Gegenstellen über einen einzigen Eintrag möglich bei Nutzung von RAS User Template oder Proadaptive VPN.
1-Click-VPN Client-Assistent	Erstellung von VPN-Client-Zugängen mit gleichzeitiger Erzeugung von Profilen für den LANCOM Advanced VPN Client mit einem Klick aus LANconfig heraus
1-Click-VPN Site-to-Site	Erzeugen von VPN-Verbindungen zwischen LANCOM-Routern per "Drag and Drop" mit einem Klick in LANconfig
IKE, IKEv2	IPSec-Schlüsselaustausch über Preshared Key oder Zertifikate (RSA-Signature, ECDSA-Signature, Digital-Signature)
Smart Certificate*	Komfortable Erstellung von digitalen X.509 Zertifikaten mittels einer eigenen Zertifizierungsstelle (SCEP-CA) via Weboberfläche oder SCEP.
Zertifikate	Unterstützung von X.509 digitalen mehrstufigen Zertifikaten, kompatibel z.B. zu Microsoft Server / Enterprise Server und OpenSSL. Secure Key Storage zur Sicherung eines privaten Schlüssels (PKCS#12) gegen Diebstahl.
Zertifikatsrollout	Automatisierte Erzeugung sowie Rollout und Verlängerung von Zertifikaten mit SCEP (Simple Certificate Enrollment Protocol) pro Zertifikatshierarchie
Certificate Revocation Lists (CRL)	Abruf von CRLs mittels HTTP pro Zertifikatshierarchie
OCSP Client	Prüfen von X.509-Zertifikaten anhand von OCSP (Online Certificate Status Protocol), in Echtzeit arbeitende Alternative zu CRLs

LANCOM SYSTEMS

lancom-systems.de

LCOS 10.80

LANCOM vRouter

VPN	
OCSP Server/Responder*	Bereitstellen von Gültigkeits-Informationen zu mittels Smart Certificate ausgestellten Zertifikaten via OCSP
XAUTH	XAUTH-Client zur Anmeldung von LANCOM Routern und Access Points an XAUTH-Servern inkl. IKE-Config-Mode. XAUTH-Server, der die Anmeldung von Clients per XAUTH an LANCOM Routern ermöglicht. Anbindung des XAUTH-Servers an RADIUS-Server zur Authentisierung von VPN-Zugängen pro Verbindung über eine zentrale Benutzerverwaltung. Authentisierung für VPN-Client-Zugänge via XAUTH mit RADIUS-Anbindung auch mit OTP-Tokens
RAS User Template	Konfiguration aller VPN-Client-Verbindungen im IKE-Config-Mode über einen einzigen Konfigurationseintrag
Proadaptive VPN	Automatisierte Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routing-Einträge anhand eines Default-Eintrags bei Site-to-Site Verbindungen.
Algorithmen	3DES (168 Bit), AES-CBC und -GCM (128, 192 und 256 Bit), RSA (1024-4096 Bit), ECDSA (P-256-, P-384-, P-521-Kurven) und Chacha20-Poly 1305. OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen. MD-5, SHA-1, SHA-256, SHA-384 oder SHA-512 Hashes
NAT-Traversal	Unterstützung von NAT-Traversal (NAT-T) für den VPN-Einsatz auf Strecken, die kein VPN-Passthrough unterstützen
Dynamic DNS	Ermöglicht die Registrierung der IP-Adresse bei einem Dynamic-DNS-Provider, falls keine feste IP-Adresse für den VPN-Verbindungsaufbau verwendet wird
Spezifisches DNS-Forwarding	DNS-Forwarding einstellbar pro DNS-Domäne, z.B. zur Auflösung interner Namen durch eigenen DNS-Server im VPN und Auflösung externer Namen durch Internet-DNS-Server. Eintrag für Backup-DNS pro DNS-Weiterleitung
Split-DNS	Ermöglicht für IKEv2 das selektive Weiterleiten von Datenverkehr abhängig von der angesprochenen DNS-Domäne.
IPv4 VPN	Kopplung von IPv4 Netzwerken
IPv4 VPN über IPv6 WAN	Nutzung von IPv4 VPN über IPv6 WAN-Verbindungen
IPv6 VPN	Kopplung von IPv6 Netzwerken
IPv6 VPN über IPv4 WAN	Nutzung von IPv6 VPN über IPv4 WAN-Verbindungen
RADIUS	RADIUS Authorization und Accounting, Auslagerung von VPN-Konfigurationen in externem RADIUS-Server bei IKEv2, RADIUS CoA (Change of Authorization)
High Scalability VPN (HSVPN)	Übertragung von mehreren, sicher getrennten Netzen innerhalb eines VPN-Tunnels
Advanced Mesh VPN	Dynamischer VPN-Tunnelaufbau zwischen beliebigen Filialen bei Bedarf
IKEv2-EAP*	VPN-Clients können mit IKEv2-EAP gegen eine zentrale Datenbank wie Microsoft Windows Server oder RADIUS-Server authentifiziert werden
*) Hinweis	verfügbar ab der Lizenzstufe "vRouter 250"

Schnittstellen	
Ethernet Ports	5 individuelle Ports, 10/100/1000/10.000 MBit/s Ethernet. Bis zu 3 Ports können als zusätzliche WAN-Ports geschaltet werden. Ethernet-Ports können in der LCOS-Konfiguration deaktiviert werden.

LCOS 10.80

LANCOM vRouter

Schnittstellen	
Port-Konfiguration	Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus). Als WAN-Port können zusätzliche, externe DSL-Modems oder Netzabschlussrouter inkl. Load-Balancing und Policy-based Routing betrieben werden. DMZ-Ports können mit einem eigenen IP-Adresskreis ohne NAT versorgt werden
Management und Monitoring	
Management	LANCOM Management Cloud, LANconfig, WEBconfig, LANCOM Layer 2 Management (Notfall-Management)
Management-Funktionen	Individuelle Zugriffs- und Funktionsrechte für bis zu 16 Administratoren, RADIUS- und RADSEC-Benutzerverwaltung, Fernwartung (über WAN oder (W)LAN, Zugangsrechte (lesen/schreiben) separat einstellbarüber) SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, alternative Steuerung der Zugriffsrechte durch TACACS+, Scripting, zeitliche Steuerung aller Parameter und Aktionen durch CRON-Dienst
Automatisches Firmware-Update	Konfigurierbare automatische Prüfung und Installation von Firmware-Updates
Monitoring	LANCOM Management Cloud, LANmonitor
Monitoring-Funktionen	Geräte-SYSLOG, SNMPv1,v2c,v3 inkl. SNMP-TRAPS, sehr umfangreiche LOG- und TRACE-Möglichkeiten, PING und TRACEROUTE zur Verbindungsüberprüfung, interne Loggingbuffer für SYSLOG und Firewall-Events
Monitoring-Statistiken	Umfangreiche Ethernet-, IP- und DNS-Statistiken, SYSLOG-Fehlerzähler, Accounting inkl. Export von Accounting-Informationen über LANmonitor und SYSLOG, Layer-7-Anwendungserkennung inkl. anwendungsbezogenes Erfassen des verursachten Traffics
IPerf	IPerf ermöglicht es den Datendurchsatz von IP-Netzwerken zu testen (integrierter Client und Server)
SLA-Monitor (ICMP)	Performance-Überwachung von Verbindungen
Netflow	Export von Informationen über eingehenden bzw. ausgehenden IP-Datenverkehr
SD-LAN	SD-LAN - Automatische LAN-Konfiguration über die LANCOM Management Cloud
SD-WAN	SD-WAN - Automatische WAN-Konfiguration über die LANCOM Management Cloud
Lieferumfang	
Bedienungsanleitung	Gedruckte Bedienungsanleitung (DE, EN)
Mindestanforderungen	
Unterstützte Hypervisor	→ VMWare ESXi 6.0 oder höher (auf Intel XEON-Prozessor mit AES-Befehlssatzerweiterung (Intel AES-NI) und HW-Virtualisieurng (Intel VT-x)) → Hyper-V auf Microsoft Windows Server 2016 / 2019 oder Windows 10 (auf Intel XEON-Prozessor mit AES-Befehlssatzerweiterung (Intel AES-NI) und HW-Virtualisieurng (Intel VT-x))
Unterstützte Cloud-Plattformen	→ Microsoft Azure

LCOS 10.80

LANCOM vRouter

Mindestanforderungen	
Mindestanforderungen an virtuelle Maschine	→ 1 virtuelle x86 CPU → RAM: • 2 GB (empfohlen für vRouter 50, vRouter 250) • 4 GB (empfohlen für vRouter 500, vRouter 1000) • 8 GB (empfohlen für vRouter Unlimited) → 512 MB Festplattenplatz (SSD empfohlen) → 1-5 Netzwerkinterfaces (vmxnet3 oder Hyper-V Synthetic NIC) → Hinweis: Für die vRouter Modelle 250, 500, 1000 und insbesondere für den vRouter Unlimited wird eine möglichst hohe CPU Taktung empfohlen

Support	
Software-Updates	Während der Lizenz-Laufzeit regelmäßige, kostenfreie Updates (LCOS Betriebssystem und LANtools) via Internet
LANcare Direct 24/7	Direkter, priorisierter 10/5-Hersteller-Support inkl. 24/7-Notfall-Hotline und Security Updates für das Gerät, zugesicherte Erstreaktionszeiten (SLA) von max. 30 Minuten bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre. vRouter 50 und vRouter 250: LANcare Direct 24/7 S (Art.-Nr. 10752, 10753 oder 10754) vRouter 500: LANcare Direct 24/7 M (Art.-Nr. 10755, 10756 oder 10757) vRouter 1000: LANcare Direct 24/7 L (Art.-Nr. 10758, 10759 oder 10760) vRouter unlimited: LANcare Direct 24/7 XL (Art.-Nr. 10761, 10762 oder 10763)
LANcare Direct 10/5	Direkter, priorisierter 10/5-Hersteller-Support und Security Updates für das Gerät, zugesicherte Erstreaktionszeiten (SLA) von max. 2 Stunden bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre. vRouter 50 und vRouter 250: LANcare Direct 10/5 S (Art.-Nr. 10740, 10741 oder 10742) vRouter 500: LANcare Direct 10/5 M (Art.-Nr. 10743, 10744 oder 10745) vRouter 1000: LANcare Direct 10/5 L (Art.-Nr. 10746, 10747 oder 10748) vRouter unlimited: LANcare Direct 10/5 XL (Art.-Nr. 10749, 10750 oder 10751)

LANCOM Management Cloud	
LANCOM Management Cloud	LANCOM LMC-C-1Y Lizenz (1 Jahr), ermöglicht für ein Jahr die Verwaltung eines Gerätes der Kategorie C mit der LANCOM Management Cloud, Art.-Nr. 50106
LANCOM Management Cloud	LANCOM LMC-C-3Y Lizenz (3 Jahre), ermöglicht für drei Jahre die Verwaltung eines Gerätes der Kategorie C mit der LANCOM Management Cloud, Art.-Nr. 50107
LANCOM Management Cloud	LANCOM LMC-C-5Y Lizenz (5 Jahre), ermöglicht für fünf Jahre die Verwaltung eines Gerätes der Kategorie C mit der LANCOM Management Cloud, Art.-Nr. 50108

Geeignetes Zubehör	
VPN-Client-Software	LANCOM Advanced VPN Client für Windows 7,8/8.1,10,11 - 1er Lizenz Art.-Nr. 61600
VPN-Client-Software	LANCOM Advanced VPN Client für Windows 7,8/8.1,10,11 - 10er Lizenz, Art.-Nr. 61601
VPN-Client-Software	LANCOM Advanced VPN Client für Windows 7,8/8.1,10,11 - 25er Lizenz, Art.-Nr. 61602
VPN-Client-Software	LANCOM Advanced VPN Client für Mac OS X (10.5 nur Intel, 10.6 oder höher), 1er Lizenz, Art.-Nr. 61606

LCOS 10.80

LANCOM vRouter

Geeignetes Zubehör	
VPN-Client-Software	LANCOM Advanced VPN Client für Mac OS X (10.5 nur Intel, 10.6 oder höher), 10er Lizenz, Art.-Nr. 61607

Artikelnummer(n)	
LANCOM vRouter 50 (1 Jahr)	59000 (10 VPN-Kanäle, 50 MBit/s Durchsatz, 8 ARF-Kontexte, 128 Public-Spot-Benutzer, Management von 10 Access Points/WLAN-Routern)*
LANCOM vRouter 50 (3 Jahre)	59001 (10 VPN-Kanäle, 50 MBit/s Durchsatz, 8 ARF-Kontexte, 128 Public-Spot-Benutzer, Management von 10 Access Points/WLAN-Routern)*
LANCOM vRouter 50 (5 Jahre)	59012 (10 VPN-Kanäle, 50 MBit/s Durchsatz, 8 ARF-Kontexte, 128 Public-Spot-Benutzer, Management von 10 Access Points/WLAN-Routern)*
LANCOM vRouter 250 (1 Jahr)	59002 (50 VPN-Kanäle, 250 MBit/s Durchsatz, 16 ARF-Kontexte, 256 Public-Spot-Benutzer, Management von 50 Access Points/WLAN-Routern)*
LANCOM vRouter 250 (3 Jahre)	59003 (50 VPN-Kanäle, 250 MBit/s Durchsatz, 16 ARF-Kontexte, 256 Public-Spot-Benutzer, Management von 50 Access Points/WLAN-Routern)*
LANCOM vRouter 250 (5 Jahre)	59013 (50 VPN-Kanäle, 250 MBit/s Durchsatz, 16 ARF-Kontexte, 256 Public-Spot-Benutzer, Management von 50 Access Points/WLAN-Routern)*
LANCOM vRouter 500 (1 Jahr)	59008 (100 VPN-Kanäle, 500 MBit/s Durchsatz, 64 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 100 Access Points/WLAN-Routern)*
LANCOM vRouter 500 (3 Jahre)	59009 (100 VPN-Kanäle, 500 MBit/s Durchsatz, 64 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 100 Access Points/WLAN-Routern)*
LANCOM vRouter 500 (5 Jahre)	59014 (100 VPN-Kanäle, 500 MBit/s Durchsatz, 64 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 100 Access Points/WLAN-Routern)*
LANCOM vRouter 1000 (1 Jahr)	59004 (200 VPN-Kanäle, 1000 MBit/s Durchsatz, 128 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 200 Access Points/WLAN-Routern)*
LANCOM vRouter 1000 (3 Jahre)	59005 (200 VPN-Kanäle, 1000 MBit/s Durchsatz, 128 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 200 Access Points/WLAN-Routern)*
LANCOM vRouter 1000 (5 Jahre)	59015 (200 VPN-Kanäle, 1000 MBit/s Durchsatz, 128 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 200 Access Points/WLAN-Routern)*
LANCOM vRouter unlimited (1000 Sites, 1 Jahr)	59006 (1000 VPN-Kanäle, unlimitierter Durchsatz, 256 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 1000 Access Points/WLAN-Routern)*
LANCOM vRouter unlimited (1000 Sites, 3 Jahre)	59007 (1.000 VPN-Kanäle, unlimitierter Durchsatz, 256 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 1000 Access Points/WLAN-Routern)*
LANCOM vRouter unlimited (1000 Sites, 5 Jahre)	59016 (1.000 VPN-Kanäle, unlimitierter Durchsatz, 256 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 1000 Access Points/WLAN-Routern)*
LANCOM vRouter unlimited (3000 Sites, 1 Jahr)	59022 (3.000 VPN-Kanäle, unlimitierter Durchsatz, 256 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 1500 Access Points/WLAN-Routern)*

LCOS 10.80

LANCOM vRouter

Artikelnummer(n)	
LANCOM vRouter unlimited (3000 Sites, 3 Jahre)	59023 (3.000 VPN-Kanäle, unlimitierter Durchsatz, 256 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 1500 Access Points/WLAN-Routern)*
LANCOM vRouter unlimited (3000 Sites, 5 Jahre)	59024 (3.000 VPN-Kanäle, unlimitierter Durchsatz, 256 ARF-Kontexte, unlimitierte Public-Spot-Benutzer, Management von 1500 Access Points/WLAN-Routern)*
DEMO Option	Die 30-tägige DEMO-Option (bestehend aus 10 MBit/s, 3 ARF-Netzen, 3 VPN-Tunneln und 128 Public Spot Usern) kann kostenlos über die LANCOM-Webseite unter "Service & Support" erzeugt werden.
*) Hinweis	Im unlizenzierten Zustand ist der Funktionsumfang auf 1 MBit/s, 3 ARF Netze, 1 VPN Tunnel und 128 Public Spot User begrenzt. Des Weiteren sind Lizenzen nicht additiv und können nicht kombiniert werden. Nach Ablauf der Lizenzoption kann der vRouter weiter genutzt werden, Firmwareupdates und Konfigurationsänderungen sind dann jedoch nicht mehr möglich.

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