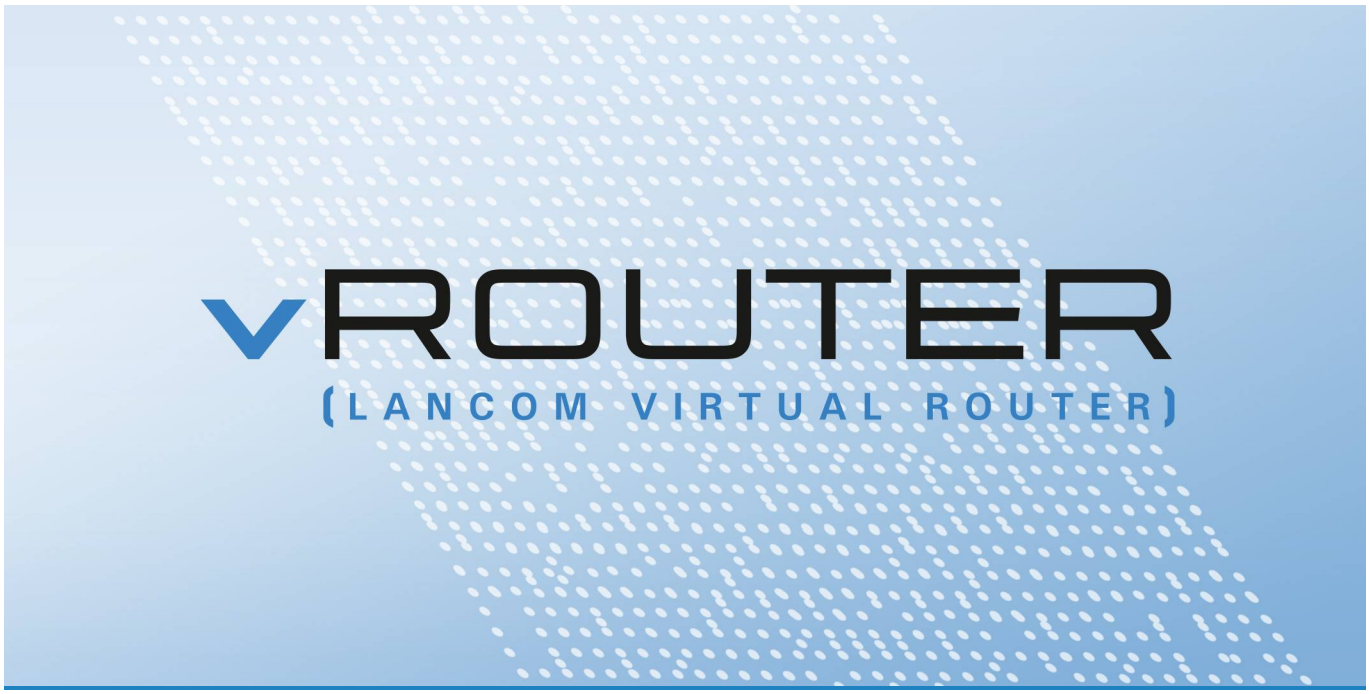

LANCOM vRouter

The best router may not be a normal router

The LANCOM vRouter is a virtual router for operation in virtualized environments based on the hypervisor VMware ESXi. Based on the longstanding, tried-and-trusted operating system LCOS (LANCOM Operating System), it works just like a hardware router to offer the same security and the same comprehensive range of functions. The LANCOM vRouter virtualizes a wide variety of networking functions, and it can optionally be deployed and monitored either with the LANCOM Management Cloud using software-defined networking, or with the LANtools. Be it as a router for medium-scale scenarios or as a central-site VPN gateway, the LANCOM vRouter is the right basis for modern networks.

- Virtual, software-based routers for operation with VMware ESXi
- Tried-and-trusted operating system LCOS as a high-performance basis
- 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
- Secure site connectivity thanks to advanced IPSec-VPN for up to 1,000 channels
- Support for up to 5 ethernet ports
- Network virtualization with up to 256 networks (ARF)

LANCOM Systems

LANCOM vRouter

Software-based router for virtualized environments

The LANCOM vRouter is a software-based router for operation in virtualized environments based on the hypervisor VMware ESXi. 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 or as a central-site VPN gateway, it is ideally suited for systems vendors, service providers, and for operation by medium-sized and large companies.

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.

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.

Fast recovery

The LANCOM vRouter is easily and completely backed up to any storage medium at any time. This means that even in the event of server hardware failure, your router can be restarted immediately on another machine, so avoiding any lengthy network outages.

Full integration into the LANCOM Management Cloud

The LANCOM vRouter is effortlessly managed and monitored by the LANCOM Management Cloud. The LMC is the world's first management system for the intelligent organization, optimization and control of your entire network. This radically simplifies the management of installations, from small to very large scenarios. What's more, the virtual router can be managed with all of the tried-and-tested methods.

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.

Advanced Routing & Forwarding

The LANCOM vRouter provides up to 256 securely isolated IP contexts, each of which has its own separate routing. This is an elegant way of operating IP applications via one central router. Be it in small networks or enterprise environments: The various communication channels remain securely isolated from one another and are easily configured with the LANCOM Management Cloud.

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 Systems

LANCOM vRouter

LCOS 10.12

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
Layer 2 features	
VLAN	4.096 IDs based on IEEE 802.1q, dynamic assignment, Q-in-Q tagging
Multicast	IGMP-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, user-defined rules and notifications
Quality of Service	Traffic shaping, bandwidth reservation, DiffServ/TOS, packetsize control, layer-2-in-layer-3 tagging
Security	Intrusion Prevention, IP spoofing, access control lists, Denial of Service protection, detailed settings for handling reassembly, session-recovery, PING, stealth mode and AUTH port, URL blocker, password protection, programmable reset button
PPP authentication mechanisms	PAP, CHAP, MS-CHAP, and MS-CHAPv2
High availability / redundancy	VRRP (Virtual Router Redundancy Protocol), analog/GSM modem backup
Router	IPv4-, IPv6-, NetBIOS/IP multiprotokoll router, IPv4/IPv6 dual stack
Router virtualization	ARF (Advanced Routing and Forwarding) up to separate processing of 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, NetBIOS/IP proxy, NTP client, SNTP server, policy-based routing, Bonjour-Proxy, RADIUS
IPv6 services	HTTP and HTTPS server for configuration by web interface, DHCPv6 client, DHCPv6 server, DHCPv6 relay, DNS client, DNS server, dynamic DNS client, NTP client, SNTP server, Bonjour-Proxy, RADIUS

LANCOM vRouter

LCOS 10.12

Layer 3 features	
IPv6 compatible LCOS applications	WEBconfig, HTTP, HTTPS, SSH, Telnet, DNS, TFTP, firewall, RAS dial-in
Dynamic routing protocols	RIPv2, BGPv4, OSPFv2
IPv4 protocols	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, NetBIOS, PPPoE (server), RADIUS, RADSEC (secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+
IPv6 protocols	NDP, stateless address autoconfiguration (SLAAC), stateful address autoconfiguration (DHCPv6), router advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, Syslog, SNMPv1,v2c,v3
WAN operating mode	VDSL, ADSL1, ADSL2 or ADSL2+ additional with external DSL modem at an ETH port
WAN protocols	PPPoE, Multi-PPPoE, ML-PPP, GRE, EoGRE, PPTP (PAC or PNS), L2TPv2 (LAC or LNS) and IPoE (using DHCP or no DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 and IPv4/IPv6 dual stack session), IP(v6)oE (autokonfiguration, DHCPv6 or static)
Tunneling protocols (IPv4/IPv6)	6to4, 6in4, 6rd (static and over DHCP), Dual Stack Lite (IPv4-in-IPv6-Tunnel)
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) for backup in case of failure of a device or remote station.
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)
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 1000 (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, 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

LANCOM vRouter

LCOS 10.12

VPN	
XAUTH	XAUTH client for registering LANCOM routers and access points at XAUTH servers incl. IKE-config mode. XAUTH server enables clients to register via XAUTH at LANCOM routers. Connection of the XAUTH server to RADIUS servers provides the central authentication of VPN-access with user name and password. Authentication of VPN-client access via XAUTH and RADIUS connection additionally by OTP token
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. Propagation of dynamically learned routes via RIPv2 if required
Algorithms	3DES (168 bit), AES-CBC and -GCM (128, 192 or 256 bit), Blowfish (128 bit), RSA (1024-4096 bit) and CAST (128 bit). OpenSSL implementation with FIPS-140 certified algorithms. MD-5, SHA-1, SHA-256, SHA-384 or SHA-512 hashes
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough
IPCOMP	VPN data compression based on Deflate compression for higher IPSec throughput on low-bandwidth connections (must be supported by remote endpoint)
Dynamic DNS	Enables the registration of IP addresses with a Dynamic DNS provider in the case that fixed IP addresses are not used for the VPN connection
Specific DNS forwarding	DNS forwarding according to DNS domain, e.g. internal names are translated by proprietary DNS servers in the VPN. External names are translated by Internet DNS servers
IPv4 VPN	Connecting private IPv4 networks
IPv4 VPN over IPv6 WAN	Use of IPv4 VPN over IPv6 WAN connections
IPv6 VPN	Connecting private IPv6 networks
IPv6 VPN over IPv4 WAN	Use of IPv6 VPN over IPv4 WAN connections
Radius	RADIUS authorization and accounting, outsourcing of VPN configurations in external RADIUS server in IKEv2, RADIUS CoA (Change of Authorization)
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
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
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))

LANCOM vRouter

LCOS 10.12

Minimum requirements	
Minimal requirements virtualization hardware	> 1 virtual x86 CPU > 512 MB of RAM > 512 MB of disk space > 1-5 network interfaces (VMXnet3)
Support	
Software updates	During the term of a valid license - regular free updates (LCOS operating system and LANtools) via Internet
LANCOM Management Cloud	
LANCOM LMC-A-1Y LMC License	LANCOM LMC-A-1Y License (1 Year), enables the management of one category A device for one year via the LANCOM Management Cloud, item no. 50100
LANCOM LMC-A-3Y LMC License	LANCOM LMC-A-3Y License (3 Years), enables the management of one category A device for three years via the LANCOM Management Cloud, item no. 50101
LANCOM LMC-A-5Y LMC License	LANCOM LMC-A-5Y License (5 Years), enables the management of one category A device for five years via the LANCOM Management Cloud, item no. 50102
LANCOM LMC-B-1Y LMC License	LANCOM LMC-B-1Y License (1 Year), enables the management of one category B device for one year via the LANCOM Management Cloud, item no. 50103
LANCOM LMC-B-3Y LMC License	LANCOM LMC-B-3Y License (3 Years), enables the management of one category B device for three years via the LANCOM Management Cloud, item no. 50104
LANCOM LMC-B-5Y LMC License	LANCOM LMC-B-5Y License (5 Years), enables the management of one category B device for five years via the LANCOM Management Cloud, item no. 50105
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
LANCOM LMC-D-1Y LMC License	LANCOM LMC-D-1Y License (1 Year), enables the management of one category D device for one year via the LANCOM Management Cloud, item no. 50109
LANCOM LMC-D-3Y LMC License	LANCOM LMC-D-3Y License (3 Years), enables the management of one category D device for three years via the LANCOM Management Cloud, item no. 50110
LANCOM LMC-D-5Y LMC License	LANCOM LMC-D-5Y License (5 Years), enables the management of one category D device for five years via the LANCOM Management Cloud, item no. 50111
Accessories	
VPN Client Software	LANCOM Advanced VPN Client for Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, single license, item no. 61600
VPN Client Software	LANCOM Advanced VPN Client for Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, 10 licenses, item no. 61601
VPN Client Software	LANCOM Advanced VPN Client for Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10, 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)
LANCOM vRouter 50 (3 Years)	59001 (10 VPN channels, 50 Mbps bandwith, 8 ARF contexts, 128 Public Spot users)
LANCOM vRouter 250 (1 Year)	59002 (50 VPN channels, 250 Mbps bandwith, 16 ARF contexts, 256 Public Spot users)
LANCOM vRouter 250 (3 Years)	59003 (50 VPN channels, 250 Mbps bandwith, 16 ARF contexts, 256 Public Spot users)
LANCOM vRouter 500 (1 Year)	59008 (100 VPN channels, 500 Mbps bandwith, 64 ARF contexts, unlimited Public Spot users)
LANCOM vRouter 500 (3 Years)	59009 (100 VPN channels, 500 Mbps bandwith, 64 ARF contexts, unlimited Public Spot users)
LANCOM vRouter 1000 (1 Years)	59004 (200 VPN channels, 1000 Mbps bandwith, 128 ARF contexts, unlimited Public Spot users)

LANCOM vRouter

LCOS 10.12

Item number(s)	
LANCOM vRouter 1000 (3 Years)	59005 (200 VPN channels, 1000 Mbps bandwith, 128 ARF contexts, unlimited Public Spot users)
LANCOM vRouter unlimited (1 Year)	59006 (1000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users)
LANCOM vRouter unlimited (3 Years)	59007 (1000 VPN channels, unlimited bandwith, 256 ARF contexts, unlimited Public Spot users)
*) Note	Licenses can not be used additively and can not be combined