



. . . c o n n e c t i n g   y o u r   b u s i n e s s

## LANCOM 1722 VoIP

Business VoIP Router with integrated IP PBX for ISDN and SIP telephony at sites with up to 2 ISDN exchange lines

- IP PBX for ISDN and 8 SIP subscribers (up to 32 with VoIP-32 Option)
- SIP proxy for registration with providers and upstream VoIP PBXs
- SIP gateway with transparent transition between SIP and ISDN
- Intelligent call routing and number translation
- Two ISDN ports (NT/TE) with life-line support
- Stateful-inspection firewall and VPN gateway

The LANCOM 1722 VoIP is the innovative all-round solution providing integrated data and voice networking. It provides an IP PBX, SIP gateway, VPN router, access router and professional firewall in one compact device. The Business VoIP Router LANCOM 1722 VoIP seamlessly switches between ISDN telephones, existing ISDN PBXs, SIP subscribers and central VoIP PBXs. By enabling the continued use of existing ISDN technology, the LANCOM 1722 VoIP offers investment protection and cost savings with Voice over IP for smaller sites, small offices and subsidiaries.

#### **More than just a new PBX.**

The combination with ISDN or SIP telephones makes a separate PBX completely superfluous. Basic functions of the traditional telephone system are provided by the LANCOM router's VoIP Call Manager. At the same time, the professional security, routing and network functions, including VPN, provide everything that modern companies need for their data networks. Even Voice over VPN or Voice over WLAN (with separate Access Points) can be used in parallel with data networking. Free updates to the solution provide savings through consolidation for true protection of this future-proof investment.

#### **More telephony.**

Telephone calls can be automatically directed over existing VPN connections between company sites. Not only are these calls secured from interception; by using flatrate connections, there are no additional costs, either. LANCOM opens up a cost-effective migration path between technologies of the 'old and new world' because existing ISDN telephones and PBXs can be integrated and operated side by side with VoIP terminal equipment. Two ISDN ports can be freely configured as internal or external connections and offer four parallel voice channels. This allows, for example, an existing ISDN PBX to be additionally equipped with SIP and connected to an upstream VoIP PBX. Subscribers can simultaneously make calls via ISDN telephones, SIP equipment, or softphones to other SIP or ISDN subscribers, both internally and externally. The transition between SIP and ISDN is automatic and invisible to the user. With life-line support and power relay to the internal ISDN port, it is still possible to telephone with ISDN even in case of a power outage. ISDN backup, load balancing and VRRP combined with up to three Ethernet ports as WAN interfaces provide SIP connections with redundancy and high reliability. This ensures that telephony is just as reliable as ever, even with VoIP.

#### **More security.**

The integrated firewall with the latest security functions such as stateful inspection, Intrusion Detection and Denial-of-Service protection is supplemented by dynamic bandwidth management and comprehensive functions for backup, high-availability and redundancy. The integrated VPN gateway that fulfills the IPSec standard, and the optional hardware accelerator provide optimal security for connecting telecommuters and branch offices thanks to the high-security 3-DES or AES encryption and support of digital certificates.

#### **More management.**

LCMS, the LANCOM Management System, is a free software package for the Microsoft Windows operating system for the configuration, remote maintenance and real-time monitoring of all LANCOM routers, central-site gateways, access points, WLAN controllers and managed switches. LANconfig is an application for remote configuration via HTTP, HTTPS, TFTP or ISDN dial-up. It offers easy-to-use wizards that cater for everything from the basic setup to the configuration of VPN connections, but it can also handle the fine-tuning of individual device parameters. A single LCMS installation can handle the monitoring and maintenance of any of the various LANCOM devices. LANmonitor offers detailed, real-time monitoring of parameters, it provides access to log files and statistics, and it can carry out a detailed trace-protocol analysis. Along with convenient functions such as the firewall GUI for object-orientated firewall programming, a range of professional functions help with the administration of projects, including the automatic configuration backup, saving and uploading scripts, a folder-based organization, and a dynamic search filter. Service providers benefit from the broad range of scripting methods and professional access with individual access rights for administrators via SSH, HTTPS, TFTP, telnet and ISDN dial-in. Rollouts and operations are assisted by the automatic upload of configurations and firmware from USB data media and the option of storing project-specific boot configurations in place of the standard factory settings—all of which offers big potential savings on expensive manual maintenance.

**More benefits.**

The versatile functions for address translation and routing allow completely different networks to be connected over common infrastructure. Existing networks at partner companies, home-office workstations or subsidiaries can be integrated into the VPN without problem. The management software (LANconfig and LANmonitor) is included and offers not only cost-effective remote maintenance of entire installations along with highly convenient setup wizards, but also full real-time monitoring and logging. What's more, service providers benefit from the broad range of scripting methods and professional access with individual access rights for administrators via SSH, HTTPS, TFTP and ISDN dial-in.

**More virtualization.**

Advanced Routing and Forwarding (ARF) from LANCOM is a unique technology for network virtualization. It enables different logical networks, each with their own settings for DHCP, DNS, routing and firewall, to operate on a single device and share the same physical infrastructure. For example, networks in the LAN can be assigned to different VLANs, tagged in the WAN or assigned to different RAS connections. The innovative Tunnel-in-Tunnel technology for VPN allows different networks between LANCOM routers to be completely isolated even over a shared IPsec-VPN connection—even with overlapping IP-address ranges. ARF is suitable for the cross-site separation of logical networks, for example where different applications or service providers work on shared infrastructure. Conflicts can be completely avoided. Incursions from one logical network to another, either intentionally or by accident, are effectively prevented by ARF. In particular for companies located at multiple sites, ARF enables the switch to a purely IP-based infrastructure, so offering considerable potential savings in operations.

**More reliability for the future.**

From the very start, LANCOM products are designed for a product life of several years. They are equipped with hardware dimensioned for the future. Even reaching back to older product generations, updates to the LANCOM Operating System—LCOS—are available several times a year, free of charge and offering major features. LANCOM offers unbeatable protection of your investment!

Firewall	
Stateful inspection firewall	Incoming/Outgoing Traffic inspection based on connection information. Trigger for firewall rules depending on backup status, e.g. simplified rule sets for low-bandwidth backup lines. Limitation of the number of sessions per remote site (ID)
Packet filter	Check based on the header information of an IP packet (IP or MAC source/destination addresses; source/destination ports, DiffServ attribute); remote-site dependant, direction dependant, bandwidth dependant
Extended port forwarding	Network Address Translation (NAT) based on protocol and WAN address, i.e. to make internal webservers accessible from WAN
N:N IP address mapping	N:N IP address mapping for translation of IP addresses or entire networks
Tagging	The firewall marks packets with routing tags, e.g. for policy-based routing; Source routing tags for the creation of independent firewall rules for different ARF contexts
Actions	Forward, drop, reject, block sender address, close destination port, disconnect
Notification	Via e-mail, SYSLOG or SNMP trap
Quality of Service	
Traffic shaping	Dynamic bandwidth management with IP traffic shaping
Bandwidth reservation	Dynamic reservation of minimum and maximum bandwidths, totally or connection based, separate settings for send and receive directions. Setting relative bandwidth limits for QoS in percent
DiffServ/TOS	Priority queuing of packets based on DiffServ/TOS fields
Packet-size control	Automatic packet-size control by fragmentation or Path Maximum Transmission Unit (PMTU) adjustment
Layer 2/Layer 3 tagging	Automatic or fixed translation of layer-2 priority information (IEEE 802.11p-marked Ethernet frames) to layer-3 DiffServ attributes in routing mode. Translation from layer 3 to layer 2 with automatic recognition of IEEE 802.11p-support in the destination device
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
URL blocker	Filtering of unwanted URLs based on DNS hitlists and wildcard filters. Extended functionality with Content Filter Option
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
Anti-theft	Anti-theft ISDN site verification over B or D channel (self-initiated call back and blocking)
Adjustable reset button	Adjustable reset button for 'ignore', 'boot-only' and 'reset-or-boot'
High availability / redundancy	
VRRP	VRRP (Virtual Router Redundancy Protocol) for backup in case of failure of a device or remote station. Enables passive standby groups or reciprocal backup between multiple active devices including load balancing and user definable backup priorities
FirmSafe	For completely safe software upgrades thanks to two stored firmware versions, incl. test mode for firmware updates
ISDN backup*	In case of failure of the main connection, a backup connection is established over ISDN. Automatic return to the main connection
Analog/GSM modem backup	Optional operation of an analog or GSM modem at the serial interface
Load balancing	Static and dynamic load balancing over up to 4 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 (with LANCOM Advanced VPN Client 2.22 or later) and site-to-site connections (LANCOM VPN gateways or routers with LCOS 8.0 or later). IPSec over HTTPS is based on the NCP VPN Path Finder technology
Number of VPN tunnels	Max. number of concurrent active IPSec, PPTP (MPPE) and L2TPv2 tunnels: 5 (25 with VPN 25 Option). Unlimited configurable connections. Configuration of all remote sites via one configuration entry when using the RAS user template or Proadaptive VPN.
Hardware accelerator	Integrated hardware accelerator for 3DES/AES encryption and decryption
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	IPSec key exchange with Preshared Key or certificate
Certificates	X.509 digital multi-level certificate support, compatible with Microsoft Server / Enterprise Server and OpenSSL, upload of PKCS#12 files via HTTPS interface and LANconfig. Simultaneous support of multiple certification authorities with the management of up to nine parallel certificate hierarchies as containers (VPN-1 to VPN-9). Simplified addressing of individual certificates by the hierarchy's container name (VPN-1 to VPN-9). Wildcards for certificate checks of parts of the identity in the subject. Secure Key Storage protects a private key (PKCS#12) from theft
Certificate rollout	Automatic creation, rollout and renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) per certificate hierarchy
Certificate revocation lists (CRL)	CRL retrieval via HTTP per certificate hierarchy
OCSP Client	Check X.509 certifications by using OCSP (Online Certificate Status Protocol) in real time as an alternative to CRLs
XAUTH	XAUTH client for registering LANCOM routers and access points at XAUTH servers incl. IKE-config mode. XAUTH server enables clients to register via XAUTH at LANCOM routers. Connection of the XAUTH server to RADIUS servers provides the central authentication of VPN-access with user name and password. Authentication of VPN-client access via XAUTH and RADIUS connection additionally by OTP token
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 (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 or SHA-1 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)
LANCOM Dynamic VPN*	Enables VPN connections from or to dynamic IP addresses. The IP address is communicated via ISDN B- or D-channel or with the ICMP or UDP protocol in encrypted form. Dynamic dial-in for remote sites via connection template
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
VPN throughput (max., AES)	
1416-byte frame size UDP	46 Mbps
256-byte frame size UDP	8 Mbps
IMIX	14 Mbps
Firewall throughput (max.)	
1518-byte frame size UDP	65 Mbps
256-byte frame size UDP	17 Mbps
Content Filter (optional)	
Demo version	Activate the 30-day trial version after free registration under <a href="http://www.lancom.eu/routeroptions">http://www.lancom.eu/routeroptions</a>
URL filter database/rating server*	Worldwide, redundant rating servers from IBM Security Solutions for querying URL classifications. Database with over 100 million entries covering about 10 billion web pages. Web crawlers automatically search and classify web sites to provide nearly 150,000 updates per day: They use text classification by optical character recognition, key word searches, classification by word frequency and combinations, web-site comparison of text, images and page elements, object recognition of special characters, symbols, trademarks and prohibited images, recognition of pornography and nudity by analyzing the concentration of skin tones in images, by structure and link analysis, by malware detection in binary files and installation packages
URL check*	Database based online check of web sites (HTTP/HTTPS). HTTPS websites are checked based on DNS names of HTTPS server certificates or based on "Reverse DNS lookup" of IP addresses.

Content Filter (optional)	
Categories/category profiles*	Filter rules can be defined in each profile by collecting category profiles from 58 categories, for example to restrict Internet access to business purposes only (limiting private use) or by providing protection from content that is harmful to minors or hazardous content (e.g. malware sites). Clearly structured selection due to the grouping of similar categories. Content for each category can be allowed, blocked, or released by override
Override**	Each category can be given an optional manual override that allows the user to access blocked content on a case-by-case basis. The override operates for a limited time period by allowing the category or domain, or a combination of both. Optional notification of the administrator in case of overrides
Black-/whitelist	Lists that are manually configured to explicitly allow (whitelist) or block (blacklist) web sites for each profile, independent of the rating server. Wildcards can be used when defining groups of pages or for filtering sub pages
Profiles	Timeframes, blacklists, whitelists and categories are collected into profiles that can be activated separately for content-filter actions. A default profile with standard settings blocks racist, pornographic, criminal, and extremist content as well as anonymous proxies, weapons/military, drugs, SPAM and malware
Time frames	Timeframes can be flexibly defined for control over filtering depending on the time of day or weekday, e.g. to relax controls during break times for private surfing
Flexible firewall action	Activation of the content filter by selecting the required firewall profile that contains content-filter actions. Firewall rules enable the flexible use of your own profiles for different clients, networks or connections to certain servers
Individual display pages (for blocked, error, override)	Response pages displayed by the content filter in case of blocked sites, errors or overrides can be custom designed. Variables enable the inclusion of current information such as the category, URL, and rating-server categorization. Response pages can be issued in any language depending on the language set in the user's web browser
Redirection to external pages	As an alternative to displaying the device's own internal response pages to blockings, errors or overrides, you can redirect to external web servers
License management	Automatic notification of license expiry by e-mail, LANmonitor, SYSLOG or SNMP trap. Activation of license renewal at any time before expiry of the current license (the new licensing period starts immediately after expiry of the current license)
Statistics	Display of the number of checked and blocked web pages by category in LANmonitor. Logging of all content-filter events in LANmonitor; log file created daily, weekly or monthly. Hit list of the most frequently called pages and rating results. Analysis of the connection properties; minimum, maximum and average rating-server response time
Notifications	Messaging in case of content-filter events optionally by e-mail, SNMP, SYSLOG or LANmonitor
Wizard for typical configurations	Wizard sets up the content filters for a range of typical scenarios in a few simple steps, including the creation of the necessary firewall rules with the corresponding action
Max. users	Simultaneous checking of HTTP(S) traffic for a maximum of 50 different IP addresses in the LAN
*) Note	Categorization is maintained by IBM. Neither IBM or LANCOM can guarantee full accuracy of the categorization.
***) Note	The Override function is only available for HTTP websites.
VoIP	
Number of local subscribers	max. 8 (upgradable to 32 with LANCOM VoIP-32 Option)
PBX functionality	Switching between local ISDN, SIP subscribers and upstream SIP PBXs or external ISDN and SIP subscribers. E.g. support for: Hold/Request, Swap, Transfer, Call Forwarding (CFU, CFB, CFNR), settings per subscriber for original, local subscriber or user defined calling party ID in case of Call Forwarding, number display/suppression (CLIP, CLIR), named internal subscribers, suppression of second call (Busy on Busy), immediate outgoing line, AOC (at internal ISDN), hunt groups, call diversion ISDN or SIP subscriber initiated actions: - Hold/Consultation, Swap, Transfer - Call Forwarding unconditional (CFU), on busy (CFB), on no reply (CFNR)
Hunt groups	Hunt group cascades with groups as group members. Call diversion to all members simultaneously or sequentially. Automatic forwarding to target number or hunt group after timeout or when busy/unreachable
Multi login	Registration of several SIP terminal devices with the same number/ID. Signaling like with a single subscriber, e.g. tabletop telephone, softphone and mobile handset at the same time
Call router	Central switching of all incoming and outgoing calls. Number translation by mapping, numeral replacement and number supplementation. Configuration of line and route selection, entry of multiple alternative routes (line backup). Routing based on calling and called number, SIP domain and line. Manual routing by the user ('outside-line access codes'). Routing with line-selection keys on telephones or telephone number prefixes. Targeted routing for individual telephone numbers (e.g. emergency calls via local ISDN). Separate routes for internal, local, long-distance or international calls. Blocking of telephone numbers or blocks of telephone numbers. Inclusion of local subscribers into the number range of an upstream SIP PBX. Internal standard telephone number for undeliverable calls. Supplement/remove line-related prefixes or switchboard numbers
SIP registrar	Management of local SIP users with optional automatic registration/authentication at SIP providers/upstream SIP PBXs. Optional shared/individual password for authentication at an upstream SIP PBX. Default DNS entry for the local SIP domains, service location (SRV) support. Configurable registration (with/without) and line monitoring (inactive, automatic, with re-registration, with OPTIONS requests) for SIP trunk, link, remote gateway and SIP PBX line

VoIP	
SIP proxy	Mapping of up to 16 public SIP-provider accounts as telephone lines for shared use. Connection to up to four upstream SIP PBXs including line backup. SIP connections from/to internal subscribers, SIP providers and SIP PBXs. Automatic bandwidth management and automatic configuration of the firewall for SIP connections. Support of early and late initiation of SDP negotiation (SDP offer in INVITE or OK). Switchable support of privacy/call screening (call number suppression) per line compliant with RFC 3325 or with remote party ID when set for subscriber (CLIR). Support of Request URI (RFC 3261)
SIP gateway	Transparent conversion of ISDN telephone calls to SIP calls, and vice versa. Local ISDN subscribers register as local SIP users, and local ISDN subscribers automatically register as SIP users at upstream SIP PBXs/with SIP providers. Number translation between internal numbers and MSN/DDI (including telephone number blocks), plus automatic adaptation of calling numbers and called numbers
SIP trunk	Outgoing call switching and incoming call reception based on extension numbers to/from SIP PBXs/SIP providers (requires support of the SIP-DDI functions compliant with ITU-T Q.1912.5 at the central exchange) with a registration of the switchboard number or without any registration (fixed configuration on both sides). Mapping of entire SIP telephone number blocks
SIP link	Outgoing call switching and incoming call reception of any numbers to/from SIP PBXs/SIP providers (requires support of this function at the central exchange) with a single registration or without registration (fixed configuration on both sides). Mapping of entire SIP telephone number blocks
SIP remote gateway	Local break-in/out of calls with any telephone number to/from upstream VoIP PBXs/SIP providers with telephone number mapping, independent of local users
Media proxy	Termination and interconnection of multiple media streams. Control of media sessions resulting from SIP connections. IP address and port translation for media stream packets. Connection of parties at media stream level where a call transfer in SIP (REFER) is not possible
Number of simultaneous connections	2 - 16 depending on code conversion, echo canceling and load
Signaling	VoIP: SIPv2, ISDN: DSS1 (Euro-ISDN), point-to-point/point-to-multipoint; 1TR6 (only at an external ISDN connector in TE mode)
Media protocols	RTP
ISDN features	Operation directly at ISDN exchange lines or at ISDN extension lines of existing PBXs. Provision of exchange lines or extension lines. ISDN supplementary services CLIP, CLIR, en-block dial and individual dialing with adjustable wait-time until completion. Transparent pass-through of data services and ISDN facilities to control switching exchanges (in case of default ISDN interface configuration). ISDN-UDI calls with G.722. Pass-through of service identifiers (BC, HLC, LLC) for ISDN-to-ISDN connections. PCM bit-transparent coupling. Support for keypad facilities. Advice of charge (AOC-D, AOC-E). 'DSS1 NT reverse' and 'DSS1 NT point-to-point reverse' for ISDN clock synchronization with suitable PBXs. ISDN 50 buses can be collected into hunting groups. Parallel operation of point-to-point and point-to-multipoint connections
Audio properties	Echo canceling (G.168), automatic adaptive de-jitter buffer. Inband tone signaling compliant with EU standards and country-specific. DTMF support compliant with RFC 2976 (SIP info), RFC 2833 (RTP payload type/outband). Transparent pass-through for negotiated codecs. Interaction on codec negotiation between subscribers (filter, quality/bandwidth) Voice encoding with G.711 -law/A-law (64 kbps), G.722 high-quality codec (payload is passed through, no conversion of different G.722 encoding variants), G.729 Annex A
Fax transmission	Transmission of fax via SIP on the LAN side with T.38 or G.711, on the WAN/Internet side with T.38. Conversion of SIP fax with T.38 and break-in/break-out at the outside line to ISDN G.711 with service signalisation. Connection and conversion to SIP T.38 or G.711 for ISDN fax machines
Auto QoS	Automatic dynamic bandwidth reservation per SIP connection. Automatic selection of compression method depending upon available bandwidth. Voice packet prioritization (CoS), DiffServ marking, traffic shaping (incoming/outgoing) and packet-size management of non-prioritized connections compared to VoIP. Independent settings for DiffServ marking of signaling (SIP) and media streams (RTP)
VoIP management	VoIP Setup Wizard and configuration with LANconfig. Configuration and tracing with command line interface (remote or locally)
VoIP monitoring	Reporting of Call Data Records (CDR) via SYSLOG or e-mail. Status display of subscribers, lines, and connections. Logging of VoIP Call Manager events in LANmonitor. SYSLOG and TRACE for voice connections. Active monitoring even of ISDN interface states with SNMP
Routing functions	
Router	IP, IPX and NetBIOS/IP multi-protocol router
Advanced Routing and Forwarding	Separate processing of 16 contexts due to virtualization of the routers. Mapping to VLANs and complete independent management and configuration of IP networks in the device, i.e. individual settings for DHCP, DNS, Firewalling, QoS, VLAN, Routing etc. Automatic learning of routing tags for ARF contexts from the routing table
HTTP	HTTP and HTTPS server for configuration by web interface
DNS	DNS client, DNS server, DNS relay, DNS proxy and dynamic DNS client
DHCP	DHCP client, DHCP relay and DHCP server with autodetection. Cluster of several LANCOM DHCP servers per context (ARF network) enables caching of all DNS assignments at each router. DHCP forwarding to multiple (redundant) DHCP servers
NetBIOS	NetBIOS/IP proxy
NTP	NTP client and SNTP server, automatic adjustment for daylight-saving time
Policy-based routing	Policy-based routing based on routing tags. Based on firewall rules, certain data types are marked for specific routing, e.g. to particular remote sites or lines

Routing functions	
Dynamic routing	Dynamic routing with RIPv2. Learning and propagating routes; separate settings for LAN and WAN. Extended RIPv2 including HopCount, Output Delay, Poisoned Reverse, Triggered Update for LAN (acc. to RFC 2453) and WAN (acc. to RFC 2091) as well as filter options for propagation of routes. Definition of RIP sources with wildcards
Layer 2 functions	
VLAN	VLAN ID definable per interface and routing context (4,094 IDs) IEEE 802.1q
ARP lookup	Packets sent in response to LCOS service requests (e.g. for Telnet, SSH, SNMP, SMTP, HTTP(S), SNMP, etc.) via Ethernet can be routed directly to the requesting station (default) or to a target determined by ARP lookup
COM port server	
COM port forwarding	COM-port server for DIN and USB interfaces. For multiple serial devices connected to it, the server also manages its own virtual COM ports via Telnet (RFC 2217) for remote maintenance (works with popular virtual COM-port drivers compliant with RFC 2217). Switchable newline conversion and alternative binary mode. TCP keepalive according to RFC 1122 with configurable keepalive interval, retransmission timeout and retries
USB print server	
Print server (USB 2.0)	Host port for connecting USB printers via RAW-IP and LPD; bi-directional data exchange is possible
LAN protocols	
IP	ARP, proxy ARP, BOOTP, LANCAP, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (server), RADIUS, RIP-1, RIP-2, RTP, SIP, SNMP, TCP, TFTP, UDP, VRRP
WAN protocols	
ADSL, Ethernet	PPPoE, PPPoA, IPoA, Multi-PPPoE, ML-PPP, PPTP (PAC or PNS), L2TPv2 (LAC or LNS) and IPoE (with or without DHCP), RIP-1, RIP-2, VLAN
ISDN	1TR6, DSS1 (Euro-ISDN), PPP, X75, HDLC, ML-PPP, V.110/GSM/HSCSD
WAN operating mode	
xDSL	ADSL1, ADSL2 or ADSL2+ with internal ADSL2+ modem
xDSL (ext. modem)	ADSL1, ADSL2 or ADSL2+ with external ADSL2+ modem
ISDN	ISDN data or voice usage via internal ISDN interface
Interfaces	
WAN: ADSL2+	ADSL2+ over ISDN compliant with ITU G.992.3, ITU G.992.5 Annex B (ADSL2+) with DPBO or ADSL2+ over POTS compliant with ITU G.992.3 and ITU G.992.5 Annex A (ADSL2+) with DPBO
WAN: ADSL	ADSL over ISDN compliant with ITU G.992.1 Annex B (compatible to Deutsche Telekom U-R2 connections) or ADSL over POTS compliant with ITU G.992.1 Annex A
Ethernet ports	4 individual 10/100-Mbps Fast Ethernet ports; up to 3 ports can be operated as additional WAN ports with load balancing. Ethernet ports can be electrically disabled within LCOS configuration
Port configuration	Each Ethernet port can be freely configured (LAN, DMZ, WAN, monitor port, off). LAN ports can be operated as a switch or separately. 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
USB 2.0 host port	USB 2.0 full-speed host port for connecting USB printers (USB print server), serial devices (COM port server) or USB data storage (FAT file system); bi-directional data exchange is possible (max. 12 Mbps)
ISDN	2 ISDN BRI ports (S0 bus), NT/TE mode with cross-over adapter, switchable termination, power relay and signaling pass-through (lifeline support) switchable to ISDN2
Serial interface	Serial configuration interface / COM port (8 pin Mini-DIN): 9,600 - 115,000 baud, suitable for optional connection of analog/GPRS modems. Supports internal COM port server and allows for transparent asynchronous transmission of serial data via TCP
LCMS (LANCOM Management System)	
LANconfig	Configuration program for Microsoft Windows, incl. convenient Setup Wizards. Optional group configuration, simultaneous remote configuration and management of multiple devices over ISDN dial-in or IP connection (HTTPS, HTTP, SSH, TFTP). A tree view of the setting pages like in WEBconfig provides quick access to all settings in the configuration window. Password fields which optionally display the password in plain text and can generate complex passwords. Configuration program properties per project or user. Automatic storage of the current configuration before firmware updates. Exchange of configuration files between similar devices, e.g. for migrating existing configurations to new LANCOM products. Detection and display of the LANCOM managed switches. Extensive application help for LANconfig and parameter help for device configuration. LANCOM QuickFinder as search filter within LANconfig and device configurations that reduces the view to devices with matching properties. Central configuration of each management port.



LCMS (LANCOM Management System)	
LANmonitor	Monitoring application for Microsoft Windows for (remote) surveillance and logging of the status of LANCOM devices and connections, incl. PING diagnosis and TRACE with filters and save to file. Search function within TRACE tasks. Wizards for standard diagnostics. Export of diagnostic files for support purposes (including bootlog, sysinfo and device configuration without passwords). Graphic display of key values (marked with an icon in LANmonitor view) over time as well as table for minimum, maximum and average in a separate window, e. g. for Rx, Tx, CPU load, free memory. Monitoring of the LANCOM managed switches. Flick easily through different search results by LANCOM QuickFinder
Firewall GUI	Graphical user interface for configuring the object-oriented firewall in LANconfig: Tabular presentation with symbols for rapid understanding of objects, choice of symbols for objects, objects for actions/Quality of Service/remote sites/services, default objects for common scenarios, individual object definition (e.g. for user groups)
Automatic software update	Voluntary automatic updates for LCMS. Search online for LCOS updates for devices managed by LANconfig on the myLANCOM download server (myLANCOM account mandatory). Updates can be applied directly after the download or at a later time
Management	
WEBconfig	Integrated web server for the configuration of LANCOM devices via Internet browsers with HTTPS or HTTP. Similar to LANconfig with a system overview, SYSLOG and events display, symbols in the menu tree, quick access with side tabs. WEBconfig also features Wizards for basic configuration, security, Internet access, LAN-LAN coupling. Online help for parameters in LCOS menu tree
LANCOM Layer 2 Management (emergency management)	The LANCOM Layer 2 Management protocol (LL2M) enables an encrypted access between the command line interfaces of two LANCOM device directly via a Layer 2 connection
Alternative boot configuration	During rollout devices can be preset with project- or customer-specific settings. Up to two boot- and reset-persistent memory spaces can store customized configurations for customer-specific standard settings (memory space '1') or as a rollout configuration (memory space '2'). A further option is the storage of a persistent standard certificate for the authentication of connections during rollouts
Automatic update from USB	Automatic upload of appropriate firmware and configuration files on insertion of USB memory (FAT filesystem) into USB interfaces of LANCOM routers with factory settings. The function can be activated to be used during operation of configured devices. The router checks the files' dates and versions against the current firmware before upload
Device SYSLOG	SYSLOG buffer in the RAM (size depending on device memory) to store events for diagnosis. Default set of rules for the event protocol in SYSLOG. The rules can be modified by the administrator. Display and saving of internal SYSLOG buffer (events) from LANCOM devices with LANmonitor, display only with WEBconfig
Access rights	Individual access and function rights for up to 16 administrators. Alternative access control on a per parameter basis with TACACS+
User administration	RADIUS user administration for dial-in access (PPTP/L2TP via PPP and ISDN CLIP). Support for RADSEC (Secure RADIUS) for secure communication with RADIUS servers. RADIUS authentication can be used to log in to a device. In addition, users can be deactivated in the internal RADIUS server without deleting them
Remote maintenance	Remote configuration with Telnet/SSL, SSH (with password or public key), browser (HTTP/HTTPS), TFTP or SNMP, firmware upload via HTTP/HTTPS or TFTP
TACACS+	Support of TACACS+ protocol for authentication, authorization and accounting (AAA) with reliable connections and encrypted payload. Authentication and authorization are separated completely. LANCOM access rights are converted to TACACS+ levels. With TACACS+ access can be granted per parameter, path, command or functionality for LANconfig, WEBconfig or Telnet/SSH. Each access and all changes of configuration are logged. Access verification and logging of SNMP Get and Set requests. WEBconfig supports the access rights of TACACS+ and choice of TACACS+ server at login. LANconfig provides a device login with the TACACS+ request conveyed by the addressed device. Authorization to execute scripts and each command within them by checking the TACACS+ server's database. CRON, action-table and script processing can be diverted to avoid TACACS+ to relieve TACACS+ servers. Redundancy by setting several alternative TACACS+ servers. Configurable option to fall back to local user accounts in case of connection drops to the TACACS+ servers. Compatibility mode to support several free TACACS+ implementations
RADIUS	Support of RADIUS protocol for authentication of configuration access. Administrative privileges can be assigned for each administrator.
Remote maintenance of 3rd party devices	A remote configuration for devices behind der LANCOM can be accomplished (after authentication) via tunneling of arbitrary TCP-based protocols, e.g. for HTTP(S) remote maintenance of VoIP phones or printers of the LAN. Additionally, SSH and Telnet client allow to access other devices from a LANCOM device with an interface to the target subnet if the LANCOM device can be reached at its command line interface
ISDN remote maintenance	Remote maintenance over ISDN dial-in with calling-number check
TFTP & HTTP(S) client	For downloading firmware and configuration files from a TFTP, HTTP or HTTPS server with variable file names (wildcards for name, MAC/IP address, serial number), e.g. for roll-out management. Commands for live Telnet session, scripts or CRON jobs. HTTPS Client authentication possible by username and password or by certificate
SSH & Telnet client	SSH-client function compatible to Open SSH under Linux and Unix operating systems for accessing third-party components from a LANCOM router. Also usable when working with SSH to login to the LANCOM device. Support for certificate- and password-based authentication. Generates its own key with sshkeygen. SSH client functions are restricted to administrators with appropriate rights. Telnet client function to login/administer third party devices or other LANCOM devices from command line interface
Basic HTTP(S) file server	HTML pages, images and templates for Public Spot pages, vouchers, information pages of the Content Filter can be stored on a USB memory (FAT file system) in a specific folder as an alternative for the limited internal memory
HTTPS Server	Option to choose if an uploaded certificate or the default certificate is used by the HTTPS server
Security	Access rights (read/write) over WAN or LAN can be set up separately (Telnet/SSL, SSH, SNMP, HTTPS/HTTP), access control list

Management	
Scripting	Scripting function for batch-programming of all command-line parameters and for transferring (partial) configurations, irrespective of software versions and device types, incl. test mode for parameter changes. Utilization of timed control (CRON) or connection establishment and termination to run scripts for automation. Scripts can send e-mails with various command line outputs as attachments
Load commands	LoadFirmware, LoadConfig and LoadScript can be executed conditionally in case certain requirements are met. For example, the command LoadFirmware could be executed on a daily basis and check each time if the current firmware is up to date or if a new version is available. In addition, LoadFile allows the upload of files including certificates and secured PKCS#12 containers
SNMP	SNMP management via SNMPv2, private MIB exportable by WEBconfig, MIB II
Timed control	Scheduled control of parameters and actions with CRON service
Diagnosis	Extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, LANmonitor status display, internal logging buffer for SYSLOG and firewall events, monitor mode for Ethernet ports
LANCAPI	Available for all LANCOM routers with integrated ISDN interface. LANCAPI provides CAPI 2.0 features for Microsoft Windows to utilize ISDN channels over the IP network
CAPI Faxmodem	Softmodem for Microsoft Windows that makes use of LANCAPI to send and receive faxes via ISDN
Statistics	
Statistics	Extensive Ethernet, IP and DNS statistics; SYSLOG error counter
Accounting	Connection time, online time, transfer volumes per station. Snapshot function for regular read-out of values at the end of a billing period. Timed (CRON) command to reset all counters at once
Export	Accounting information exportable via LANmonitor and SYSLOG
Hardware	
Power supply	12 V DC, external power adapter (230 V)
Environment	Temperature range 5–35° C; humidity 0–80%; non-condensing
Housing	Robust synthetic housing, rear connectors, ready for wall mounting, Kensington lock; 210 x 45 x 140 mm (W x H x D)
Fans	None; fanless design without rotating parts, high MTBF
Power consumption (max)	approx. 8.5 Watts
Declarations of conformity*	
CE	EN 60950-1, EN 55022, EN 55024
*) Note	You will find all declarations of conformity in the products section of our website at <a href="http://www.lancom-systems.eu">www.lancom-systems.eu</a>
Scope of delivery	
Manual	Printed User Manual (DE, EN) and Installation Guide (DE/EN/FR/ES/IT/PT/NL)
CD/DVD	Data medium with management software (LANconfig, LANmonitor, WLANmonitor, LANCAPI) and documentation
Cable	Serial configuration cable, 1.5m
Cable	1 Ethernet cable, 3 m
Cable	ADSL cable, 3m
Cable*	ISDN cable, 3m
Adapter	ISDN cross-over adapter for S0 bus
Power supply unit	12 V DC, external power adapter (230 V)
Support	
Warranty	3 years support via hotline and Internet KnowledgeBase
Software updates	Regular free updates (LCOS operating system and LANCOM Management System) via Internet
Options	
VPN	LANCOM VPN-25 Option (25 channels), item no. 60083
LANCOM Content Filter	LANCOM Content Filter +10 user, 1 year subscription
LANCOM Content Filter	LANCOM Content Filter +25 user, 1 year subscription
LANCOM Content Filter	LANCOM Content Filter +10 user, 3 year subscription

Options	
LANCOM Content Filter	LANCOM Content Filter +25 user, 3 year subscription
Advance Replacement	LANCOM Next Business Day Service Extension CPE, item no. 61411
Warranty Extension	LANCOM 2-Year Warranty Extension CPE, item no. 61414
VoIP extension	LANCOM VoIP-32 Option (Upgrade to 32 SIP users in total), item no. 61617
Fax Gateway	LANCOM Fax Gateway Option activates 'hardfax' within the router. Supports 4 parallel fax channels with LANCAPI ('fax group 3' without use of CAPI Faxmodem), item no. 61425
LANCOM Public Spot PMS Accounting Plus	Extension of the LANCOM Public Spot (XL) Option for the connection to hotel billing systems with FIAS interface (such as Micros Fidelio) for authentication and billing of guest accesses for 178x routers, WLCs, and current central-site gateways, item no. 61638
Accessories	
19" Rack Mount	19" Rackmount-Adapter, Art.-Nr. 61501
LANCOM Wall Mount	For simple, theft-proof mounting of LANCOM devices with plastic housings, item no. 61349
LANCOM Wall Mount (White)	For simple, theft-proof mounting of LANCOM devices with plastic housings, item no. 61345
Analog modem backup/serial adapter	LANCOM Serial Adapter Kit, item no. 61500
VPN Client Software	LANCOM Advanced VPN Client for Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, single license, item no. 61600
VPN Client Software	LANCOM Advanced VPN Client for Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, 10 licenses, item no. 61601
VPN Client Software	LANCOM Advanced VPN Client for Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1, 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 1722 VoIP (Annex B)	61350 (suitable for UR-2 standard ADSL connections in Germany)
LANCOM 1722 VoIP (Annex A)	61351
LANCOM 1722 VoIP (Annex A) UK	61352

LANCOM, LANCOM Systems and LCOS are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. Subject to change without notice. No liability for technical errors and/or omissions. 7/2014