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

LANCOM OAP-321-3G

Outdoor 3G router with WLAN for mobile broadband connectivity under extreme conditions

- Connection of stationary and temporary outdoor applications via HSPA+ (UMTS/EDGE/GPRS)

- GPS positioning secures the device even for mobile applications

- IP-66 housing and extended temperature range from -33°C to +70°C

- For highest performance networks: 802.11n WLAN, Multi SSID, Gigabit Ethernet and VLAN

- VPN site-to-site connectivity with 5 simultaneous IPSec VPN channels (25 channels optional)

- IPSec-over-HTTPS for secure VPN connections via cellular networks

- Flexible input voltage from 10 to 28 V, power supply LANCOM OAP-320 PSU optionally available

The outdoor router LANCOM OAP-321-3G has a built-in HSPA+ module and 802.11n wireless LAN. On cellular networks the router achieves data rates of up to 21 Mbps downstream and 5.76 Mbps upstream. Its rugged outdoor housing makes the device ideal for connecting outdoor applications where wired broadband access is not available: Applications include the video surveillance of open areas by IP video camera, or the provision of network connectivity to remote locations such as wind turbines or construction sites. The built-in GPS function makes the LANCOM OAP-321-3G ideal for mobile applications. The device features a Gigabit Ethernet port and numerous features such as IPSec VPN, Multi-SSID and VLAN support.

More flexibility.

The LANCOM OAP-321-3G offers exceptional flexibility for providing connectivity to remote areas. Thanks to the high coverage of cellular networks, the device guarantees Internet connectivity almost everywhere. Where HSPA+ is not available, the cellular modem is backwards compatible to the standard UMTS, EDGE and GPRS. The wireless LAN radio module can operate in the 2.4- and 5-GHz frequency ranges.

More security.

The stateful-inspection firewall in the LANCOM OAP-321-3G protects the network with intrusion prevention, denial-of-service protection, and access control by means of MAC or IP address. Flexible bandwidth management guarantees the availability of all network applications as these can be prioritized with a comprehensive range of Quality-of-Service features. The VPN gateway in the LANCOM OAP-321-3G with its 5 simultaneous IPSec channels and high-security encryption by 3-DES or AES provides optimal security for VPN connections. Thanks to IPSec-over-HTTPS (based on the NCP VPN Path Finder technology) secure VPN connections are also available through firewalls and in cellular networks. For mobile applications and installation in public places, the LANCOM OAP-321-3G features an integrated GPS module to determine the position of the device. This can function as an anti-theft measure: for example, the router can transmit its current position via email or stop operating if its location is changed.

More management.

LCMS, the LANCOM Management System, is a free software package for the LANCOM OAP-321-3G. It caters for the configuration of the device, remote maintenance and network monitoring. The central component of LCMS, LANconfig, is used to configure the LANCOM OAP-321-3G and other LANCOM devices on the network. 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. Other functions in LCMS include the firewall GUI for object-oriented setup of the firewall, automatic backup of configurations and scripts, and the intuitive folder structure with convenient search function.

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 safeguarding of your investment.

LANCOM OAP-321-3G

WLAN	
Frequency band 2.4 GHz or 5 GHz	2400-2483.5 MHz (ISM) or 5150-5825 MHz (depending on country-specific restrictions)
Data rates 802.11b/g	54 Mbps to IEEE 802.11g (fallback to 48, 36 , 24, 18, 12, 9, 6 Mbps, Automatic Rate Selection) compatible to IEEE 802.11b (11, 5.5, 2, 1 Mbps, Automatic Rate Selection), 802.11 b/g compatibility mode or pure g or pure b
Data rates 802.11a/ h	54 Mbps (fallback to 48, 36 , 24, 18, 12, 9, 6 Mbps, Automatic Rate Selection), fully compatible with TPC (adjustable power output) and DFS (automatic channel selection, radar detection) according to EN 301 893 and EN 302 502
Range (outdoor / P2P)	More than 20 km in 5 GHz. See our LANCOM Antenna Distance Calculator under www.lancom.de
Output power at radio module, 5 GHz	802.11a/h: 17 dBm @ 6 bis 24 Mbit/s, 15 dBm @ 36 Mbit/s, 13 dBm @ 54 Mbit/s, 802.11n: 17 dBm @ 6,5/13/30 Mbit/s (MCS0/8), 13 dBm @ 65/130/300 Mbit/s (MCS7/15)
Minimum transmission power	Transmission power reduction in software in 1 dB steps to min. 0.5 dBm
Receiver sensitivity 2.4 GHz	802.11b: -89 dBm @ 11 Mbit/s, -94 dBm @ 1 Mbit/s 802.11g: -93 dBm @ 6 Mbit/s, -79 dBm @ 54 Mbit/s 802.11n: -93 dBm @6,5 Mbit/s (MCS0/8), -75 dBm @ 65 Mbit/s (MCS7/15)
Receiver sensitivity 5 GHz	802.11a/h: -93 dBm @ 6Mbit/s, -75 dBm @ 54 Mbit/s 802.11n: -93 dBm @ 6,5 Mbit/s (MCS0/8), -71 dBm @ 65 Mbit/s (MCS7/15)
Radio channels 2.4 GHz	Up to 13 channels, max. 3 non-overlapping (depending on country-specific restrictions)
Radio channels 5 GHz	Up to 26 non-overlapping channels (available channels and further obligations such as automatic DFS dynamic channel selection depending on national regulations)
Roaming	Seamless handover between radio cells, IAPP support with optional restriction to an ARF context, IEEE 802.11d support
WPA2 fast roaming	Pre-authentication and PMK caching for fast roaming
Fast client roaming	With background scanning, moving LANCOM 'client mode' access points pre-authenticate to alternative access points which offer a better signal before Roaming fails
VLAN	VLAN ID definable per interface, WLAN SSID, point-to-point connection and routing context (4094 IDs) IEEE 802.1q
Dynamic VLAN assignment	Dynamic VLAN assignment for target user groups based on MAC addresses, BSSID or SSID by means of external RADIUS server.
Q-in-Q tagging	Support of layered 802.1Q VLANs (double tagging)
Multi-SSID	Simultaneous use of up to 8 independent WLAN networks per WLAN interface
IGMP snooping	Support for Internet Group Management Protocol (IGMP) in the WLAN bridge for WLAN SSIDs and LAN interfaces for specific switching of multicast packets (devices with integrated WLAN only). Automated detection of multicast groups. Configurable action for multicast packets without registration. Configuration of static multicast group members per VLAN ID. Configuration of query simulation for multicast membership per VLAN ID
Security	IEEE 802.11i / WPA2 with passphrase (WPA2-Personal) or 802.1X (WPA2-Enterprise) and hardware-accelerated AES, closed network, WEP64, WEP128, WEP152, user authentication, 802.1x /EAP, LEPS, WPA1/TKIP
EAP Types	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-SIM, EAP-AKA, EAP-AKA Prime, EAP-FAST
RADIUS server	Integrated RADIUS server for MAC address list management
EAP server	Integrated EAP server for authentication of 802.1X clients via EAP-TLS, EAP-TTLS, PEAP, MSCHAP or MSCHAPv2
Quality of Service	Prioritization according to Wireless Multimedia Extensions (WME, subset of IEEE 802.11e)
U-APSD/WMM Power Save	Extension of power saving according to IEEE 802.11e by Unscheduled Automatic Power Save Delivery (equivalent to WMM Power Save). U-APSD supports the automatic switch of clients to a doze mode. Increasmed battery lifetime for telephone calls over VoWLAN (Voice over WLAN)
Bandwidth limitation	Maximum transmit and receive rates and an individual VLAN ID can be assigned to each WLAN client (MAC address)
Broken link detection	If the link of a chosen LAN interface breaks down, a WLAN module can be deactivated to let the associated clients search for a new base station
Background scanning	Detection of rogue AP's and the channel information for all WLAN channels during normal AP operation. The Background Scan Time Interval defines the time slots in which an AP or Router searches for a foreign WLAN network in its vicinity. The time interval can be specified in either milliseconds, seconds, minutes, hours or days
Client detection	Rogue WLAN client detection based on probe requests
802.1X supplicant	Authentication of an access point in WLAN client mode at another access point via 802.1X (EAP-TLS, EAP-TTLS and PEAP)
Layer-3 Tunneling	Layer-3 Tunneling in conformity with the CAPWAP standard allows the bridging of WLANs per SSID to a separate IP subnet. Layer-2 packets are encapsulated in Layer-3 tunnels and transported to a LANCOM WLAN controller. By doing this the access point is independent of the present infrastructure of the network. Possible applications are roaming without changing the IP address and compounding SSIDs without using VLANs.
IEEE 802.11u	The WLAN standard IEEE 802.11u (Hotspot 2.0) allows for a seamless transition from the cellular network into WLAN hotspots. Authentication methods using SIM card information, certificates or username and password, enable an automatic, encrypted login to WLAN hotspots - without the need to manually enter login credentials.

IEEE 802.11n Features	
MIMO	MIMO technology is a technique which uses multiple transmitters to deliver multiple data streams via different spatial channels. Depending on the existing RF conditions the throughput is multiplied with MIMO technology.
40 MHz Channels	Two adjacent 20 MHz channels are combined to create a single 40 MHz channel. Depending on the existing RF Conditions channel bonding doubles the throughput.
20/40MHz Coexistence Mechanisms in the 2.4GHz Band	Support of coexisting accesspoints with 20 and 40MHz channels in 2.4GHz band.
MAC Aggregation and Block Acknowledgement	MAC Aggregation increase the 802.11 MAC efficiency by combining MAC data frames and sending it out with a single header. The receiver acknowledges the combined MAC frame with a Block Acknowledgement. Depending on existing RF conditions, this technique improves throughput by up to 20%.
Maximal Ratio Combining (MRC)	Maximal Ratio Combining (MRC) enables the receiver (access point), in combination with multiple antennas, to optimally combine MIMO signals to improve the client reception at long-range.
Short Guard Interval	The guard interval is the time between OFDM symbols in the air. 802.11n gives the option for a shorter 400 nsec guard interval compared to the legacy 800 nsec guard interval. Under ideal RF conditions this increases the throughput by upto 10%
BFWA*	Support for Broadband Fixed Wireless Access in 5.8 GHz band with up to 4 Watts EIRP for WLAN point-to-point links according to the national regulations of your country, special antennas required
*) Note	The use of BFWA is subject to country specific regulation

WLAN operating modes	
WLAN access point	Infrastructure mode (autonomous operation or managed by LANCOM WLAN Controller)
WLAN bridge	Point-to-multipoint connection of up to 16 Ethernet LANs (mixed operation optional), broken link detection, blind mode, supports VLAN When configuring Pt-to-Pt links, pre-configured names can be used as an alternative to MAC Adresses for creating a link. Rapid spanning-tree protocol to support redundant routes in Ethernet networks
WLAN router	Use of the LAN connector for simultaneous DSL over LAN, IP router, NAT/Reverse NAT (IP masquerading) DHCP server, DHCP client, DHCP relay server, DNS server, PPPoE client (incl.Multi-PPPoE), PPTP client and server, NetBIOS proxy, DynDNS client, NTP, port mapping, policy-based routing based on routing tags, tagging based on firewall rules, dynamic routing with RIPv2, VRRP
WLAN client	Transparent WLAN client mode for wireless Ethernet extensions, e.g. connecting PCs or printers by Ethernet; up to 64 MAC addresses. Automatic selection of a WLAN profile (max. 8) with individual access parameters depending on signal strength or priority

UMTS modem	
Supported standards	UMTS, HSPA+ (HSPA+ with up to 21 Mbps, HSUPA with up to 5.76 Mbps), Edge, and GPRS support
UMTS and HSxPA bands	850/900/1900/2100 MHz
EDGE/GPRS bands	850/900/1800/1900 Mhz (EDGE up to max. 236kbps)
Diversity support	Receive diversity on the aux antenna

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. Bandwidth control and QoS also for UMTS connections
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

Quality of Service	
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 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
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	EAP-TLS, EAP-TTLS, PEAP, MS-CHAP, MS-CHAPv2 as EAP authentication mechanisms, PAP, CHAP, MS-CHAP and MS-CHAPv2 as PPP authentication mechanisms
GPS anti-theft	Network protection via site verification by GPS positioning, device stops operating if its location is changes
WLAN protocol filters	Limitation of the allowed transfer protocols, source and target addresses on the WLAN interface
IP redirect	Fixed redirection of any packet received over the WLAN interface to a dedicated target address

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
UMTS backup	In case of failure of the main connection, a backup connection is established over the internal UMTS modem; automatic return to the main connection
Load balancing	Static and dynamic load balancing over up to 2 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 and PPTP tunnels (MPPE): 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
Realtime clock	Integrated, buffered realtime clock to save the date and time during power failure. Assures timely validation of certificates in any case
Random number generator	Generates real random numbers in hardware, e. g. for improved key generation for certificates immediately after switching-on
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

LANCOM OAP-321-3G

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 (128, 192 or 256 bit), Blowfish (128 bit), RSA (128 or -448 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 LZS or 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 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
IPv4 VPN over IPv6 WAN	Enables the use of IPv4 VPN over IPv6 WAN connections

VPN throughput (max., AES)	
1418-byte frame size UDP	82 Mbps
256-byte frame size UDP	16 Mbps
IMIX	25 Mbps

Firewall throughput (max.)	
1518-byte frame size UDP	110 Mbps
256-byte frame size UDP	20 Mbps

Content Filter (optional)	
Demo version	Activate the 30-day trial version after free registration under http://www.lancom.eu/routeroptions
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
HTTPS filter	Additional filtering of HTTPS requests with separate firewall entries
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

Content Filter (optional)	
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 traffic for a maximum of 100 different IP addresses in the LAN

VoIP	
SIP ALG	The SIP ALG (Application Layer Gateway) acts as a proxy for SIP communication. For SIP calls the ALG opens the necessary ports on the firewall for the corresponding media packets. By using automatic address translation for devices inside the LAN, the use of STUN is no longer needed.

Routing functions	
Router	IP 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
Dynamic routing	Dynamic routing with RIPv2. Learning and propagating routes; separate settings for LAN and WAN. Extended RIPv2 including HopCount, Poisoned Reverse, Triggered Update for LAN (acc. to RFC 2453) and WAN (acc. to RFC 2091) as well as filter options for propagation of routes. Definition of RIP sources with wildcards
DHCPv6	DHCPv6 client, DHCPv6 server, DHCPv6 relay, stateless- and stateful mode, IPv6 address (IA_NA), prefix delegation (IA_PD), DHCPv6 reconfigure (server and client)

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, SNTP, SMTP, HTTP(S), SNMP, etc.) via Ethernet can be routed directly to the requesting station (default) or to a target determined by ARP lookup
LLDP	Automatic discovery of network topology in layer 2 networks (Link Layer Discover Protocol).

COM port server	
COM port forwarding	COM-port server for the DIN interface. For a serial device connected to it, the server manages its own virtual COM port 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

LAN protocols	
IP	ARP, proxy ARP, BOOTP, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (server), RADIUS, RIP-1, RIP-2, RTP, SIP, SNMP, TCP, TFTP, UDP, VRRP, VLAN
IPv6	NDP, stateless address autoconfiguration (SLAAC), stateful address autoconfiguration (with DHCPv6), router advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, TCP, UDP

IPv6	
Dual Stack	IPv4/IPv6 dual stack
IPv6 compatible LCOS applications	WEBconfig, HTTP, HTTPS, SSH, Telnet, DNS, TFTP, Firewall

LANCOM OAP-321-3G

WAN protocols	
Ethernet	PPPoE, Multi-PPPoE, ML-PPP, PPTP (PAC or PNS) and IPoE (with or without DHCP), RIP-1, RIP-2, VLAN, IP
IPv6	IPv6 over PPP (IPv6 and IPv4/IPv6 dual stack session), IPoE (autoconfiguration, DHCPv6 or static)
Tunneling protocols (IPv4/IPv6)	6to4, 6in4, 6rd (static and via DHCP)

WAN operating mode	
xDSL (ext. modem)	ADSL1, ADSL2 or ADSL2+ with external ADSL2+ modem
UMTS/HSPA+	GPRS, Edge, UMTS or HSPA+ with internal UMTS modem

Interfaces	
WAN: GSM/UMTS	UMTS, HSxPA, GPRS or Edge with integrated UMTS modem
ETH1	10/100/1000 Mbps, auto-sensing algorithm
ETH2	10/100 Mbps, auto-sensing algorithm
External antenna connectors	Four N connectors for external LANCOM AirLancer Extender antennas or for antennas from other vendors. Please respect the restrictions which apply in your country when setting up an antenna system. For information about calculating the correct antenna setup, please refer to www.lancom-systems.com

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 IP connection (HTTPS, HTTP, 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
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 to the command line interface of a 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
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 (PPP/PPTP). Support for RADSEC (Secure RADIUS) providing secure communication with RADIUS servers
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

Management	
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
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
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
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
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

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	
Dimensions	255 mm x 250 mm x 80 mm (LengthWidth/Height)
Weight	approximately 3 kg including pole mounting material
LED display	6 LEDs for Power, Ethernet 1, Ethernet 2, WLAN, 3G and VPN
Power supply	10-28 V DC input voltage, optionally available: 24 V DC power supply unit LANCOM OAP-320 PSU
Reset button	Configurable reset switch for resetting and booting the device
Environment	-33° C to +70° C at 95% max. humidity (non condensing)
Housing	Robust metal housing, IP 66 protection rating, ready for wall and pole mounting, 3 LEDs for status display, please note: device must not be mounted in salt water environments without a suitable protective housing
Power consumption (max)	max. 10 Watts

Declarations of conformity*	
CE	EN 60950-1, EN 301 489-1, EN 301 489-17, EN 301 489-24
2.4 GHz WLAN	EN 300 328
5 GHz WLAN	EN 301 893, EN 302 502
GSM 900, GSM 1800	EN 301 511
UMTS	EN 301 908-1, EN 301 908-2

LANCOM OAP-321-3G

Features as of: LCOS 8.82

Declarations of conformity*	
Notifications	Certifications notified in Germany, Belgium, Netherlands, Luxembourg, Austria, Switzerland, UK, Italy, Spain, France, Portugal, Czech Republic, Denmark
IPv6	IPv6 Ready Gold
*) Note	You will find all declarations of conformity in the products section of our website at www.lancom-systems.eu

Scope of delivery	
Manual	Hardware Quick Reference (EN, DE), Installation Guide (DE/EN/FR/ES/IT/PT/NL)
CD/DVD	Data medium with firmware, management software (LANconfig, LANmonitor, WLANmonitor) and documentation
Plug	5-pin plug to connect with power supply cable (Information which are necessary to design your individual power supply cable can be taken from the Quick Reference Guide of this product.)
Cable	Water-resistant, UV-resistant Ethernet PoE cable with water-resistant screw connector, 15m
Mounting Kit	Mounting kit for wall and pole mounting
Antennas	Two 4-5 dBi dipole antennas (Gain depends on frequency.)
Antennas	Two 2 dBi dipole UMTS/GPRS antennas (850-960 Mhz and 1700-2220 Mhz)
GPS antenna	Passive GPS antenna can be ordered free of charge with enclosed voucher

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 +100 user, 1 year subscription
LANCOM Content Filter	LANCOM Content Filter +10 user, 3 year subscription
LANCOM Content Filter	LANCOM Content Filter +25 user, 3 year subscription
LANCOM Content Filter	LANCOM Content Filter +100 user, 3 year subscription
Advance Replacement	LANCOM Next Business Day Service Extension IAP & OAP, item no. 61412
Warranty Extension	LANCOM 2-Year Warranty Extension IAP & OAP, item no. 61415
Public Spot	LANCOM Public Spot Option (authentication and accounting software for hotspots, incl. Voucher printing through Standard PC printer), item no. 60642.

Accessories	
LANCOM WLC-4006+ (EU/UK/US)	LANCOM WLAN controller for central management of 6 (opt. up to 30) LANCOM access points and WLAN routers, item no. 62035 (EU), item no. 62036 (UK) and item no. 62037 (US)
LANCOM WLC-4006 (EU/UK)	LANCOM WLAN controller for central management of 6 or 12 LANCOM access points and WLAN routers, item no. 61367 (EU) and item no. 61368 (UK) - only stock devices, article is no longer available
LANCOM WLC-4025+ (EU/UK/US)	LANCOM WLAN controller for central management of 25 (opt. up to 100) LANCOM access points and WLAN routers, item no. 61378, item no. Art.-Nr. 61379 and item no. 61384 (US)
LANCOM WLC-4025 (EU/UK)	LANCOM WLAN controller for central management of 25 (opt. up to 100) LANCOM access points and WLAN routers, item no. 61550 (EU) and item no. 61551 (UK) - only stock devices, article is no longer available
LANCOM WLC-4100 (EU/UK)	LANCOM WLAN controller for central management of 100 (opt. up to 1000) LANCOM access points and WLAN routers, item no. 61369 (EU) and item no. 61377 (UK)
Adapter	AirLancer Adapter NP-NP 25 cm, connector for external LANCOM outdoor antennas, LANCOM item no. 61346
External antenna*	AirLancer Extender O-D80g 2.4 GHz 'dual linear' polarisation diversity outdoor sector antenna, item no. 61221
External antenna*	AirLancer Extender O-D60a 5 GHz 'dual linear' polarisation diversity outdoor sector antenna, item no. 61222
External antenna*	AirLancer Extender O-D9a 5 GHz 'dual linear' polarisation diversity outdoor antenna, item no. 61224
External antenna	AirLancer Extender O-360-3G 4 dBi omnidirectional GSM/GPRS/EDGE/3G outdoor antenna, item no. 61225

Accessories	
Antenna cable	AirLancer cable NJ-NP 3m antenna cable extension for connection with LANCOM outdoor antennas, item no. 61230
Antenna cable	AirLancer cable NJ-NP 6m antenna cable extension for connection with LANCOM outdoor antennas, item no. 61231
Antenna cable	AirLancer cable NJ-NP 9m antenna cable extension for connection with LANCOM outdoor antennas, item no. 61232
Surge arrestor (antenna cable)	AirLancer Extender SA-5L surge arrestor (2.4 and 5 GHz), to be integrated between Access Point and antenna, item no. 61553
Surge arrestor (LAN cable)	AirLancer Extender SA-LAN surge arrestor (LAN cable), item no. 61213
LAN cable (outdoor)	LANCOM OAP-320 Ethernet cable (30 m), item no. 61347
*) Note	The Polarization Diversity antennas require 2 cables and surge arrestors

Item number(s)	
LANCOM OAP-321-3G	61540
LANCOM OAP-320 PSU	61691 (UK), Power supply unit for LANCOM OAP-321-3G and LANCOM OAP-3G

www.lancom.eu

LANCOM
Systems