LANCOM
Systems

LANCOM 1781EW

LANCOM 1781EW

High-performance VPN router with 802.11n WLAN for professional site connectivity

■ Versatile professional router with Gigabit WAN port for VDSL, cable or SHDSL modems

■ Energy-efficient Gigabit switch as per IEEE 802.3az

■ Secure 300-Mbps dualband wireless LAN as per IEEE 802.11n with WPA2 and up to 8 WLAN SSIDs

■ VPN site connectivity with 5 simultaneous IPsec VPN channels (25 channels optional)

■ Network virtualization with up to 16 virtual networks on one device (ARF)

■ Stateful-inspection firewall with intrusion detection/denial-of-service protection

■ High availability with optional 3G backup via USB

LANCOM
Systems

The LANCOM 1781EW professional VPN router is ideal for setting up modern corporate networks: This versatile device connects to various types of modems and, with its integrated dualband WLAN module, it provides wireless networking for clients as per IEEE 802.11 a/b/g/n. Thanks to the longer ranges available from 802.11n technology, additional access points often become unnecessary. An extensive range of VPN functions enable branch offices and mobile workers to access the company network securely and at high speeds. The four ports of the integrated Gigabit Ethernet switch ensure maximum performance and are also energy-efficient as per IEEE 802.3az: If no data is transmitted over an interface, the power consumption shuts down automatically. The LANCOM 1781EW supplies everything that a modern enterprise network needs, such as comprehensive Quality-of-Service capabilities and an object-oriented firewall.

More performance.

The LANCOM 1781EW provides a balanced and modern hardware platform for reliable operation of enterprise networks around the clock. As a professional business router, the device meets with high standards in the areas of network virtualization, security and VPN networking. At the same time its computing power, storage capacity and the high-speed interfaces ensure excellent network performance even with heavy data traffic. And the integrated 300-Mbps wireless LAN module takes this performance to wireless clients as well.

More security.

For connecting to home offices or setting up multi-national branch networks: VPN specialist LANCOM stands for fast, secure and cost-effective communications. The LANCOM 1781EW is ideal for offices or small businesses that want to set up a secure VPN: The router's VPN gateway supports five simultaneous IPSec channels, with support for 25 channels as an optional extra. Secure wireless LAN with the LANCOM 1781EW is assured by its support of a wide range of security standards such as IEEE 802.1i (WPA2), 802.1X and WEP encryption. Thanks to multi-SSID, the wireless LAN supports multiple networks that are securely separated from one another. Optionally available, the LANCOM Content Filter protects up to 100 users effectively while surfing the World Wide Web. Flexible bandwidth management guarantees the availability of all applications (also in local networks) as these can be prioritized with a comprehensive range of Quality- of-Service features.

More management.

LCMS, the LANCOM Management System, is a free software package for the LANCOM 1781EW. 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 1781EW and other LANCOM devices on the network. The extensive range of features and the configuration wizards make the router quick to set up. 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 GUI for firewall setup, automatic backup of configurations and scripts, and the intuitive folder structure with convenient search function.

More virtualization.

The LANCOM 1781EW helps you to use your IT resources more effectively and to save costs. The device simultaneously supports multiple independent networks. This is made possible by the powerful technology Advanced Routing and Forwarding (ARF). The ARF function on the LANCOM 1781EW provides up to sixteen virtual networks, each with its own settings for DHCP, DNS, routing and firewall. ARF allows multiple separate networks for different groups and applications to be operated on a single physical infrastructure.

More reliability for the future.

LANCOM products are designed for a product life of several years and 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 1781EW

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
Data rates 802.11n	300 Mbps according to IEEE 802.11n with MSC15 (Fallback to 6,5 Mbps with MSC0)
Range 802.11a/b/g *	Up to 150 m (up to 30 m in buildings) *
Range 802.11n	Up to 250 m @ 6.5 Mbps (up to 20 m @ 300 Mbps indoor)*
Output power at radio module, 2.4 GHz	802.11b: +18 dBm @ 1 and 2 Mbps, +18 dBm @ 5,5 and 11 Mbps 802.11g: +18/19 dBm @ 6 up to 36 Mbps, +18 dBm @ 48 Mbps, +17 dBm @ 54 Mbps 802.11n: +19 dBm @ 6,5 and 13 Mbps (MCS0/8, 20 MHz), +13 dBm @ 65 and 130 Mbps (MCS7/15, 20 MHz), +17 dBm @ 15/30 Mbps (MCS0/8, 40 MHz), +13 dBm @ 150/300 Mbps (MCS7/15, 40 MHz)
Output power at radio module, 5 GHz	802.11a/h: +16 up to +17 dBm @ 6 up to 24 Mbps, +16 up to +17 dBm @ 36 Mbps, +9 up to +15 dBm @ 54 Mbps 802.11n: +14 up to +17 dBm @ 6,5/13 Mbps (MCS0/8, 20 MHz), +5 up to +9 dBm @ 65/130 Mbps (MCS7/15, 20 MHz), +12 up to +16 dBm @ 15/30 Mbps (MCS0/8, 40 MHz), +5 up to +9 dBm @ 150/300 Mbps (MCS7/15, 40 MHz)
Max. radiated power (EIRP), 2.4 GHz band	802.11b/g: Up to 20 dBm / 100 mW EIRP (transmission power control according to TPC)
Max. radiated power (EIRP), 5 GHz band	802.11a/h: Up to 30 dBm / 1000 mW or up to 36 dBm / 4000 mW EIRP (depending on national regulations on channel usage and subject to further obligations such as TPC and DFS)
Minimum transmission power	Transmission power reduction in software in 1 dB steps to min. 0.5 dBm
Receiver sensitivity 2.4 GHz	802.11b: -91 dBm @ 11 Mbps, -93 dBm @ 1 Mbps, 802.11g: -94dBm @ 6 Mbps, -80dBm @ 54 Mbps 802.11n: -94 dBm @ 6,5 Mbps (MCS0, 20 MHz), -77 dBm @ 65 Mbps (MCS7, 20 MHz), -94 dBm @ 13 Mbps (MCS 8, 20 MHz), -77 dBm @ 130 Mbps (MCS15, 20 MHz), -89 dBm @ 15 Mbps (MCS0, 40 MHz), -73 dBm @ 150 Mbps (MCS7, 40 MHz), -89 dBm @ 30 Mbps (MCS8, 40 MHz), -73 dBm @ 300 Mbps (MCS15, 40 MHz)
Receiver sensitivity 5 GHz	802.11a/h: -94 dBm @ 6 Mbps, -77 dBm @ 54 Mbps 802.11n: -93 dBm @ 6,5 Mbps (MCS0, 20 MHz), -74 dBm @65 Mbps (MCS7, 20 MHz), -93 dBm @ 13 Mbps (MCS8, 20 MHz), -74 dBm @ 130 Mbps (MCS15, 20 MHz), -90 dBm @ 15 Mbps (MCS0, 40 MHz), -72 dBm @ 150 Mbps (MCS7, 40 MHz), -90 dBm @ 30 Mbps (MCS8, 40 MHz), -72 dBm @ 300 Mbps (MCS15, 40 MHz)
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

LANCOM 1781EW

WLAN	
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.
*) Note	The effective distances and transmission rates that can be achieved are depending of the site RF conditions
**) Note	In preparation

LANCOM Spectral Scan	
RF spectrum scan	Up to 13 channels (2.4 GHz) or up to 26 channels (5 GHz) (depending on national regulations and manual configuration)
Signal strength of WLAN channels	Illustration of signal strength on individual WLAN channels at a certain point of time

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%.
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 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
Spectral Scan	By scanning the RF spectrum, non-WLAN intererences are automatically identified and graphically illustrated.

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

LANCOM 1781EW

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 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
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
Anti-theft	Anti-theft ISDN site verification over B or D channel (self-initiated call back and blocking)
WLAN protocol filters	Limitation of the allowed transfer protocols, source and target addresses on the WLAN interface
Adjustable reset button	Adjustable reset button for 'ignore', 'boot-only' and 'reset-or-boot'
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*	Operation of an external UMTS/HSDPA USB card at the USB host port
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
*) Note:	A UMTS USB modem is not supplied. Supported UMTS USB modem at www.lancom.eu/umts-support

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

VPN	
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 (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 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
IPv4 VPN over IPv6 WAN	Enables the use of IPv4 VPN over IPv6 WAN connections
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
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

LANCOM 1781EW

Content Filter (optional)	
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 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, LANCAPI, DHCP, DNS, HTTP, HTTPS, IP, ICMP, NTP/SNTP, NetBIOS, PPPoE (server), RADIUS, RIP-1, RIP-2, RTP, SIP, SNMP, TCP, TFTP, UDP, VRRP
Rapid Spanning Tree	802.1d Spanning Tree and 802.1w Rapid Spanning Tree support for dynamic path selection with redundant layer 2 connections
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	
IPv6 compatible LCOS applications	WEBconfig, HTTP, HTTPS, SSH, Telnet, DNS, TFTP, Firewall

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/HSDPA* (ext. module)	UMTS/HSDPA with external module at the USB interface
ISDN	ISDN data or voice usage via internal ISDN interface
Analog/GPRS (ext. modem)	Analog or GPRS operation via serial interface
*) Note:	A UMTS USB modem is not supplied. Supported UMTS USB modems at www.lancom.eu/umts-support

Interfaces	
WAN: Ethernet	10/100/1000 Mbps Gigabit Ethernet
Ethernet ports	4 individual 10/100/1000 Mbps 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. The ports support energy saving according to IEEE 802.3az
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 hi-speed host port for connecting USB printers (USB print server), serial devices (COM port server), USB data storage (FAT file system) or supported 3G USB modems; bi-directional data exchange is possible*
ISDN	ISDN BRI port (S0 bus)
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
External antenna connectors	Two reverse SMA 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
*) Note	A UMTS USB modem is not supplied. Supported UMTS USB modems at www.lancom.eu/umts-support

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, 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
WLANmonitor	Monitoring application for Microsoft Windows for the visualization and monitoring of LANCOM WLAN installations, incl. Rogue AP and Rogue Client visualization. LANCOM QuickFinder as search filter that reduces the view to devices with matching properties
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 1781EW

Management	
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
Automatic update from USB	Automtatic 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 (PPP/PPTP and ISDN CLIP). Support for RADSEC (Secure RADIUS) for 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
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
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 (W)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, new unified private MIB for all most current and future LANCOM devices with LCOS. Download link in WEBconfig
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
LANCOM WLAN Controller	Supported by all LANCOM WLAN Controller (separate optional hardware equipment for installation, optimization, operating and monitoring of WLAN networks, except for P2P connections)
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

LANCOM 1781EW

Management	
Programmable Rollout Wizard	Allows the programming of a customized wizard to simplify the rollout in projects. Support for customized templates and logos provide a way to generate a brand specific look

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) with bayonet cap to protect against accidentally unplugging
Environment	Temperature range 5–40° C; humidity 0–95%; 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)	12.5 Watts

Declarations of conformity*	
CE	EN 60950-1, EN 301 489-1, EN 301 489-17
Wi-Fi Alliance Certification	802.11a/b/g/n Wi-Fi Certified
2.4 GHz WLAN	EN 300 328
5 GHz WLAN	EN 301 893, EN 302 502
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, LANCAPI) and documentation
Cable	2 Ethernet cables, 3m
Cable	ISDN cable, 3m
Antennas	Two 3 dBi external dipole dual-band antennas, one internal 3dBi dipole dual-band antenna
Power supply unit	External power adapter (230 V), NEST 12 V/1.5 A DC/S, coaxial power connector 2.1/5.5 mm bayonet, temperature range from -5 to +45° C, LANCOM item no. 110723 (EU)/LANCOM item no 110829 (UK)

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 CPE, item no. 61411
Warranty Extension	LANCOM 2-Year Warranty Extension CPE, item no. 61414

Options	
Public Spot	LANCOM Public Spot Option (authentication and accounting software for hotspots, incl. Voucher printing through Standard PC printer), item no. 60642.
Fax Gateway	LANCOM Fax Gateway Option activates 'hardfax' within the router. Supports 2 parallel fax channels with LANCAPI ('fax group 3' without use of CAPI Faxmodem), item no. 61425

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)
External antenna	AirLancer Extender O-30 2.4 GHz outdoor antenna, item no. 60478
External antenna	AirLancer Extender O-70 2.4 GHz outdoor antenna, item no. 60469
External antenna	AirLancer Extender O-9a 5 GHz outdoor antenna, item no. 61220
External antenna	AirLancer Extender O-18a 5 GHz outdoor antenna, item no. 61210
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-360ag dual-band omnidirectional outdoor antenna, item no. 61223
External antenna	AirLancer Extender I-60ag dual-band indoor sector antenna, item no. 61214
External antenna	AirLancer Extender I-180 omnidirectional 2.4 GHz indoor antenna, item no. 60914
External antenna*	AirLancer Extender O-D9a 5 GHz 'dual linear' polarisation diversity outdoor antenna, item no. 61224
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
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
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, single license, item no. 61600
VPN Client Software	LANCOM Advanced VPN Client for Windows XP, Windows Vista, Windows 7, Windows 8, 10 licenses, item no. 61601
VPN Client Software	LANCOM Advanced VPN Client for Windows XP, Windows Vista, Windows 7, Windows 8, 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
*) Note	The Polarization Diversity antennas require 2 cables and surge arrestors

Item number(s)	
LANCOM 1781EW (EU)	62025
LANCOM 1781EW (UK)	62026