LCOS 10.94

R&S®LANCOM WLC-60

Zentrales, unkompliziertes Management für 6 bis 60 Access Points

Der R&S®LANCOM WLC-60 ist ein zentraler WLAN-Controller für die Verwaltung von Installationen mit bis zu 60 Access Points. Durch Zero-touch Deployment werden Access Points mit geringem Aufwand automatisiert in ein Netzwerk aufgenommen und mit ihnen zugewiesenen Konfigurationen versorgt. Mit vielen nützlichen Funktionen vereinfacht der WLC-60 das Management von WLAN-Installationen: die integrierte Public Spot Option verschlankt den Arbeitsprozess bei der Erstellung von öffentlich zugänglichen Hotspots, automatische Firmware-Updates sparen Zeit und sichern jederzeit den neuesten Stand der Software und der integrierte RADIUS-Server erleichtert die Verwaltung der WLAN-Nutzer. Gerade in mittelgroßen komplexen Netzwerken ist der WLC-60 das passende Produkt, um ein optimal ausgelastetes WLAN-Netz aufzubauen.

- Zentraler Firmware Rollout, Monitoring & Management von 6 bis zu 60 Access Points
- Zero-Touch Deployment von angeschlossenen APs
- Optimiertes Roaming-Verhalten von WLAN-Clients durch IEEE 802.11r und OKC
- Umfangreiche VLAN-, RADIUS- und IEEE 802.1X/EAP-Funktionen
- Integrierte Public Spot Option

R&S®LANCOM WLC-60

Zentraler Firmware Rollout, Monitoring & Management

Mit dem R&S®LANCOM WLC-60 können bis zu 60 Access Points und WLAN-Router lokal und zentral vollautomatisch konfiguriert und gesteuert werden - eine massive Zeitersparnis und Arbeitserleichterung für den Netzwerkadministrator. Damit bietet der WLAN-Controller eine einheitliche Netzwerk-Kontrolle, Sicherheit und Zuverlässigkeit.

Zero-Touch Deployment

Schnelle und einfache Netzwerkintegration neuer Access Points sowie automatische Konfigurationsvergabe - ohne manuelle Konfiguration. Nach Netzwerkauthentifizierung vergibt der R&S®LANCOM WLC-60 unmittelbar die geeignete Konfiguration an den Access Point.

Optimiertes Roaming-Verhalten von WLAN-Clients

R&S®LANCOM WLAN-Controller stellen die Kommunikation unter den verwalteten Access Points sicher. Somit werden Clients beim Wechsel zwischen zwei Funkfeldern effizient vom einen an das andere WLAN-Gerät übergeben - ohne Verbindungsabbrüche.

VLAN-, RADIUS- und IEEE 802.1X/EAP-Funktionen

Dank umfangreicher Virtualisierungs- und Sicherheitsfunktionen lassen sich WLAN-Netze sehr effizient und gemäß der firmeneigenen Security Policies gestalten. Die integrierte VLAN-Funktion ermöglicht die Trennung mehrerer sicher getrennter WLAN-Netze in nur einer Infrastruktur. Professionelle Sicherheitsfunktionen erlauben dem Administrator darüber hinaus, den Netzwerkzugriff nur für autorisierte Clients zu erlauben.

Integrierte Public Spot Option

Dank der integrierten Hotspot-Funktion eignet sich der R&S®LANCOM WLC-60 ideal für die Bereitstellung eines öffentlichen Internetzugangs. Der Benutzer profitiert von einem sicheren und komfortablen Hotspot und der Hotspot-Anbieter hat die Sicherheit, dass sein eigenes Netzwerk sicher getrennt bleibt.

Maximale Zukunftssicherheit

R&S®LANCOM Produkte sind grundsätzlich auf eine langjährige Nutzung ausgelegt und verfügen daher über eine zukunftssichere Hardware-Dimensionierung. Selbst über Produktgenerationen hinweg sind Updates des R&S®LANCOM Operating Systems – LCOS – mehrmals pro Jahr kostenfrei erhältlich, inklusive "Major Features".

R&S®LANCOM WLC-60

WLAN Profileinstellungen*	
Funkkanäle 6 GHz	Bis zu 24 nicht überlappende Kanäle (EU; 20 MHz Kanalbreite)
Funkkanäle 5 GHz	Bis zu 26 nicht überlappende Kanäle (verfügbare Kanäle je nach landesspezifischer Regulierung und mit automatischer, dynamischer DFS-Kanalwahl verbunden)
Funkkanäle 2,4 GHz	Bis zu 13 Kanäle, max. 3 nicht überlappend (landesspezifische Einschränkungen möglich)
Gleichzeitige WLAN Clients	Je nach verwendeten Access Points
IEEE 802.11u	Gemanageten R&S®LANCOM Access Points ermöglicht der WLAN-Standard IEEE 802.11u (Hotspot 2.0) einen vom mobilen Benutzer unbemerkten Übergang vom Mobilfunknetz zu WLAN Hotspots. Authentifizierungsmethoden mit SIM-Kartendaten, Zertifikaten oder Benutzername und Passwort ermöglichen eine automatische, verschlüsselte Anmeldung an Hotspots von Roaming-Partnern - ganz ohne aufwändige Eingabe von Login-Daten.
Roaming	Wechsel zwischen Funkzellen (seamless handover), IAPP-Support mit optionaler Zuordnung eines ARF-Kontextes, IEEE 802.11d Support
Opportunistic Key Caching	Opportunistic Key Caching ermöglicht schnelle Roaming-Vorgänge zwischen Access Points. Bei Controller-basierten WLAN-Installationen mit IEEE 802.1X-Authentifizierung werden die Zugangsschlüssel der Clients zwischengespeichert und vom WLAN-Controller automatisch an alle verwalteten Access Points weitergegeben
Protected Management Frames	Absicherung von WLAN Management Frames, basierend auf dem Standard IEEE 802.11w, gegen Man-in-the-Middle-Angriffe durch Message Ingegrity Codes (MIC)
Sicherheit	WPA3-Personal, IEEE 802.11i / WPA2 mit Passphrase (WPA2-Personal) oder IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise) mit hardwarebeschleunigtem AES, Closed Network, WEP64, WEP128, WEP152, User Authentication, IEEE 802.1X /EAP, WPA1/TKIP, LEPS-MAC, LEPS-U
Zeitsteuerung	WLAN-Netze können zeitbasiert aktiviert und deaktiviert werden.
RADIUS Accounting pro SSID	Pro SSID kann der RADIUS Server individuell festgelegt werden
Quality of Service	Priorisierung entsprechend der Wireless Multimedia Extensions (WME, Bestandteil von IEEE 802.11e)
Background Scanning	Erkennung von fremden Access Points ("Rogue Access Points") und der Kanaleigenschaften auf allen WLAN-Kanälen während des normalen Access-Point-Betriebes. Das Background-Scan-Intervall gibt an, in welchen zeitlichen Abständen ein Wireless Router oder Access Point nach fremden WLAN-Netzen in Reichweite sucht. Mit der Zeiteinheit kann ausgewählt werden, ob die eingetragenen Werte für Millisekunden, Sekunden, Minuten, Stunden oder Tage gelten
Client Detection	Erkennung von fremden WLAN Clients ("Rogue Clients") anhand von Probe-Requests
Space Time Block Coding (STBC)*	Codierverfahren nach IEEE 802.11n. Bei der STBC-Codierung wird ein Datenstrom zur Übertragung in Datenblöcke codiert, so dass in einem MIMO-System Verbesserungen der Empfangsbedingungen entstehen.
Low Density Parity Check (LDPC)*	Low Density Parity Check (LDPC) ist eine Methode zur Fehlerkorrektur. IEEE 802.11n nutzt als Standardmethode zur Fehlerkorrektur Convolution Coding (CC) und optional die effektiviere Methode Low Density Parity Check (LDPC).
***) Hinweis**	Je nach verwendeten Access Points

WLAN-Sicherheit	
Sicherheitsverfahren	WPA3-Personal, IEEE 802.1X (WPA3-Enterprise, WPA2-Enterprise), IEEE 802.11i (WPA2-Personal), Wi-Fi Certified™ WPA2™, WPA, WEP, IEEE 802.11w (Protected Management Frames), LEPS-MAC (R&S®LANCOM Enhanced Passphrase Security MAC), LEPS-U (R&S®LANCOM Enhanced Passphrase Security User)
Verschlüsselungsalgorithmen	AES-CCMP, AES-GCMP, TKIP, RC4 (nur bei WEP)
EAP-Typen (Authenticator)	EAP-TLS, EAP-TTLS/MSCHAPv2, PEAPv0/EAP-MSCHAPv2, PEAPv1/EAP-GTC, EAP-FAST
Radius/EAP-Server	Benutzerverwaltung von MAC-Adressen, Bandbreitenbegrenzung, Passphrase, VLAN je Benutzer, Authentisierung von IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP, MS-CHAPv2, Dynamic Peer Discovery
Sonstiges	WLAN-Protokollfilter (ACL), IP-Redirect von empfangenen Paketen aus dem WLAN, IEEE 802.1X Supplicant, Background Scanning, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS)
Sonstiges	IEEE 802.11X Supplicant, Background Scanning, Client Detection ("Rogue WLAN-Client Detection"), Wireless Intrusion Detection System (WIDS)

R&S®LANCOM WLC-60

R&S®LANCOM Active Radio Control	
Client Management	Steuerung von WLAN Clients auf den sinnvollsten Access Point unter Verwendung von 802.11k und 802.11v
Band Steering	Steuerung von 5 GHz Clients auf dieses leistungsstarke Frequenzband
Managed RF Optimization*	Auswahl optimaler WLAN-Kanäle durch den Administrator
Adaptive Noise Immunity	Immunität vor Störsignalen im WLAN
Spectral Scan	Überprüfen des WLAN-Funkspektrum auf Störquellen
Adaptive RF Optimization	Dynamische Auswahl des besten WLAN-Kanals
Airtime Fairness	Verbesserte Ausnutzung der WLAN-Bandbreite
***) Hinweis**	Je nach verwendeten Access Points. Band-/Client-Steering ist in der US-Variante nicht verfügbar.
WLAN-Controller	
Anzahl gemanagter Geräte	Ab Werk können bis zu 6 R&S®LANCOM Access Points und WLAN-Router durch den R&S®LANCOM WLC-60 gemanaged werden. Mit der optionalen R&S®LANCOM WLC AP Upgrade +6 Option können bis zu 60 R&S®LANCOM WLAN Access Points und WLAN-Router gemanagt werden. Falls das Netzwerk erweitert werden soll und mehr als 60 Geräte verwaltet werden müssen, können weitere Controller hinzugefügt werden.
Anzahl gemanagter SSIDs	Bis zu 16 SSIDs können durch den R&S®LANCOM WLAN-Controller verwaltet werden.
Smart Controller Technologie	Der R&S®LANCOM WLAN-Controller unterstützt pro Funkzelle / SSID die unterschiedliche Auskopplung der Nutzdaten: – direkt in das LAN gebridged (maximale Performance z.B. für IEEE 802.11n-basierte Access Points) – per VLAN strikt vom LAN separiert (z.B. für WLAN-Gastzugänge) – zentral zum Controller getunnelt (Layer-3-Tunneling über IP-Netze hinweg)
Auto Discovery	Automatisches Finden der WLAN-Controller durch die R&S®LANCOM Access Points oder WLAN-Router anhand von IP-Broadcasts, einstellbaren DNS-Namen oder IP-Adressen. Auch Geräte in entfernten Außenstellen oder Home Offices, die nicht direkt einen zentralen Controller erreichen, können in das zentrale Management eingebunden werden.
Authentifizierung und Autorisierung	Access Points können manuell oder automatisch authentifiziert werden. Signalisierung neuer Access Points durch LED-Anzeige, E-Mail-Benachrichtigung, SYSLOG und SNMP-Traps. Manuelle Authentisierung über grafisches Benutzerinterface in LANmonitor oder WEBconfig. Halbautomatische Authentifizierung anhand von Access Point Listen im Controller ("Bulk-Modus"). Vollautomatischer Modus mit einstellbarer Default-Konfiguration (separat an- und abschaltbar, z.B. während der Rollout-Phase). Eindeutige Identifikation authorisierter Access Points anhand digitaler Zertifikate, Zertifikatserstellung durch integrierte CA (Certificate Authority), Zertifikatsverteilung mittels SCEP (Simple Certificate Enrollment Protocol). Sperrung von Access Points mittels CRL (Certificate Revocation List)
Management-Kommunikationsprotokoll	CAPWAP (Control and Provisioning Protocol for Wireless Access Points). Zur Kommunikation zwischen Controller und Access Points genügt eine beliebige IP-Verbindung, so dass auch ein netzwerksegment- und standortübergreifendes WLAN-Management möglich ist.
Layer-3-Tunneling	Layer-3-Tunnel gemäß CAPWAP-Standard, um WLANs pro SSID zu einem IP-Subnetz zu verschalten (Bridge). Die Layer-3-Tunnel transportieren Layer-2-Pakete gekapselt durch Layer-3-Netze zu einem R&S®LANCOM WLAN-Controller, so dass der Datenverkehr gemanagter Access Points unabhängig von der bestehenden Netzinfrastruktur aggregiert werden kann. Dies ermöglicht Roaming ohne einen Wechsel der IP-Adresse und das logische Zusammenfassen von SSID, ohne den Einsatz von VLANs
Verschlüsselung	DTLS-Verschlüsselung des Kontrollkanals zwischen WLAN-Controller und Access Point (256 bit AES Verschlüsselung mit digitalen Zertifikaten, inkl. Hardware-Krypto-Beschleuniger, Verschlüsselung zu Diagnosezwecken abschaltbar)
Firmware Management	Konfiguration von mehreren R&S®LANCOM Wireless Routern und R&S®LANCOM Access Points wird vom Controller aus vorgenommen. Einrichten eines Webservers erforderlich. Eine Automatisierung der Firmware Updates ist möglich. Der WLAN-Controller prüft einmal täglich oder aufgrund einer entsprechenden Benutzeraktion die aktuell verfügbaren Dateien und vergleicht sie mit den Versionen in den Geräten. Dieser Vorgang kann auch z. B. nachts durch einen Cron-Job ausgelöst werden. Wenn auf dem Access Point nicht die gewünschte Version läuft, lädt der WLAN-Controller diese vom Webserver herunter und spielt sie in die entsprechenden Wireless Router und Access Points ein.
Skriptverteilung	Ermöglicht die vollständige Konfiguration von nicht WLAN-spezifischen Funktionen wie Redirects, Protokollfilter, ARF etc. Interner Speicher für bis zu drei Skript-Dateien (max. 64 kByte) zur Provisionierung von Access-Points ohne separaten HTTP-Server

R&S®LANCOM WLC-60

WLAN-Controller	
RF Management und automatische Funkfeld-Optimierung	Die Kanalzuteilung erfolgt wahlweise statisch oder automatisch. Bei Aktivierung der Funkfeld-Optimierungs-Funktion suchen sich die APs im 2,4 GHz-Band automatisch die optimalen Kanäle. Diese Kanalwahl wird an den Controller übermittelt und der Controller speichert sie für die jeweiligen APs. Funkfeld-Optimierung kann auch für einzelne APs (wiederholt) durchgeführt werden. Sendeleistungseinstellung statisch 0 bis -20 dB. Alarmierung bei Ausfall eines Access Points über LED, E-Mail, SYSLOG und SNMP-Traps
Konfigurationsmanagement	Definition und Gruppierung aller logischen und physikalischen WLAN-Parameter mittels WLAN-Konfigurationsprofilen. Vollautomatische oder manuelle Zuweisung von Profilen zu WLAN Access Points, automatische Konfigurationsübermittlung und -prüfung (Policy Enforcement)
Vererbung von Konfigurationsprofilen	Unterstützung hierarchischer WLAN-Profilgruppen inklusive konfigurierbarer Parameter-Vererbung zur Ableitung abweichender standortspezifischer WLAN-Konfigurationen
Management-Betriebsmodi	Einstellbarer Betriebsmodus "managed" oder "unmanaged" pro Radio-Modul. Bei R&S®LANCOM WLAN-Routern wird ausschließlich der WLAN-Teil vom Controller aktiv verwaltet (Split-Management).
Autarker Weiterbetrieb	Im "managed"-Modus kann festgelegt werden, ob der Access Point seine WLAN-Konfiguration nicht persistent erhält (keine Speicherung von Konfigurationsdaten, Normalfall im Betrieb mit Controller) und bei Verlust der Verbindung zum Controller sofort den Betrieb einstellt oder ob für eine einstellbare Zeit ein autarker Weiterbetrieb im Rahmen der technischen Möglichkeiten gestattet ist (z.B. Weiterbetrieb von Funkzellen mit WPA2 / PSK bei Ausfall der Controller-Verbindung oder nach Stromausfall). Nach Ablauf der optionalen Weiterbetriebszeit wird die WLAN-Konfiguration im WLAN AP gelöscht. Der autarke Weiterbetrieb ist pro SSID einstellbar.
VLAN und IP-Kontexte	Pro SSID kann ein festes VLAN vorgegeben werden. Der WLAN-Controller kann eigenständig bis zu 16 separate IP-Netze zur Verfügung stellen, die jeweils individuell auf VLANs und damit auch auf SSIDs abgebildet werden können (Advanced Routing and Forwarding, ARF). Der Controller kann unter anderem individuelle DHCP-, DNS-, Routing-, Firewall- und VPN-Funktionen für diese Netze übernehmen.
Dynamische VLAN-Zuweisung	Dynamische VLAN-Zuweisung für bestimmte Benutzergruppen anhand von MAC-Adressen, BSSID oder SSID mittels externem RADIUS-Server
RADIUS-Server	Integrierter RADIUS-Server zur Verwaltung von MAC-Adress-Listen. Unterstützung von RADSEC (Secure RADIUS) zur sicheren Anbindung an RADIUS-Server
EAP-Server	Integrierter EAP-Server zur Authentisierung von IEEE 802.1X Clients mittels EAP-TLS, EAP-TTLS, EAP-MD5, EAP-GTC, PEAP, MS-CHAP oder MS-CHAP v2
RADIUS/EAP Proxy pro SSID	Proxy-Betriebsart für externe RADIUS/EAP-Server (Forwarding und Realm Handling) pro SSID konfigurierbar
Redundanz, Controller-Backup und Lastverteilung	Jedem gemanagten R&S®LANCOM Access Point können mehrere alternative WLAN-Controller zugewiesen werden. Innerhalb dieser Gruppen wird auslastungsabhängig ein passender Controller ausgewählt, so dass sich bei größeren Installationen auch im Backup-Fall automatisch eine Gleichverteilung auf alle Controller ergibt.
LED Steuerung	LEDs der verwalteter WLAN-Geräte lassen sich über Profile abschalten
CA-Hierarchie	Die Certificate Authority (CA) kann bei WLAN-Controllern hierarchisch strukturiert werden. Somit können Access Points zwischen den verschiedenen WLAN-Controllern wechseln, ohne dass es zu Zertifaktskonflikten kommt. Certifcate Revocation Lists (CRLs) können untereinander ausgetauscht werden
Load Balancing	Bei der Nutzung von mehreren WLAN-Controllern werden die Access Points gleichmässig auf die verschiedenen WLAN-Controller verteilt um eine optimale Lastverteilung zu gewährleisten. Bei Ausfall eines WLAN-Controllers verteilen sich die Access Points automatisch neu, ist er wieder verfügbar wird auch die Rückverteilung automatisch durchgeführt
Backup	WLAN-Controllern kann eine Priorität zugewiesen werden, was einen Betrieb im Hot-Standby ermöglicht. Access Points wechseln automatisch zu dem WLAN-Controller mit der höchsten Priorität
Fast Roaming	Die Access Points unterstützen PMK-Caching und Pre-Authentication für schnelles Roaming. Im WPA2- und WPA2-PSK-Modus beträgt die Roaming-Zeit unter 85 ms (Voraussetzungen: Ausreichende Signalqualität, hinreichende Überlappung von Funkzellen sowie Clients mit geeignet eingestelltem, niedrigen Roaming-Threshold).
QoS	IEEE 802.11e / WME: Automatisches VLAN-Tagging (IEEE 802.1p) in den Access Points. Umsetzung auf DiffServ-Attribute im WLAN-Controller, sofern dieser als Layer-3-Router zum Einsatz kommt
Background Scanning, Rogue AP und Rogue Client Detection	Während des normalen Betriebs kann ohne Unterbrechung des Funkbetriebes im Hintergrund ein Background-Scan gefahren werden, so dass auf allen Kanälen Informationen über alle Funkkanalauslastungen sowie über alle sichtbaren Access Points und Clients gesammelt werden können (Hintergrundbetrieb als "Probe" bzw. "Sensor"). Fremde Access Points und Clients werden zentral an die Rogue AP Detection des WLANmonitor gemeldet.

R&S®LANCOM WLC-60

WLAN-Controller	
WLAN Visualisierung	Das Management-Programm WLANmonitor dient als zentrales Monitoring-Programm für den WLAN-Controller und visualisiert die Zuordnung und Performance von allen WLAN-Controllern, Access Points, SSIDs und Clients.
WLAN-Gastzugänge	Statisches Mapping von Gast-SSIDs in VLANs, Zugriffsbeschränkungen und VLAN-Routing mittels ARF (Advanced Routing and Forwarding)
Public-Spot-Funktion	Funktion im Lieferumfang enthalten (max. 256 gleichzeitige Benutzer). Einfaches Einrichten von Zugangsdaten mit nur 2 Maus-Klicks über den Voucher-Druck-Assistenten möglich. Die Voucher lassen sich über PC-Standard-Drucker ausdrucken. Anpassung des Voucher-Druck-Assistenten an das Unternehmen durch Einbindung des individuellen Firmenlogos. Funktioniert auch ohne externen RADIUS- oder Accounting-Server. Einstellung von Zeit- und/oder Volumenbudgets sowie Kriterium für Start der Abrechnung. Unterstützung von öffentlichen Zertifikaten und Zertifikats-Ketten von Trust Centern für Public Spot. Somit sind für gängige Internet-Browser vertrauenswürdige Login-Seiten mit gesichertem Zugriff (HTTPS) ohne Warnungen möglich
WLAN Client Limiting	Zur gleichmäßigen Auslastung mehrerer Access Points kann pro Access Point und pro SSID die maximale Anzahl der unterstützen WLAN Clients vorgegeben werden. Darüber hinausgehende Assoziierungsanfragen werden abgelehnt.
Management Software	LANconfig, LANmonitor, WLANmonitor
Unterstützte Access Points und WLAN-Router	
Indoor	▶ R&S®LANCOM L-151gn Wireless, R&S®LANCOM L-151E Wireless, R&S®LANCOM L-54g Wireless, R&S®LANCOM L-54ag Wireless, R&S®LANCOM L-54 dual Wireless ▶ R&S®LANCOM L-305agn Wireless, R&S®LANCOM L-310agn Wireless, R&S®LANCOM L-315agn dual Wireless ▶ R&S®LANCOM L-320agn Wireless, R&S®LANCOM L-320agn Wireless (white), R&S®LANCOM L-321agn Wireless, R&S®LANCOM L-322agn dual Wireless, R&S®LANCOM L-322E Wireless, R&S®LANCOM L-330agn dual Wireless ▶ R&S®LANCOM L-451agn Wireless, R&S®LANCOM L-452agn dual Wireless, R&S®LANCOM L-460agn dual Wireless ▶ R&S®LANCOM LN-630acn dual Wireless, R&S®LANCOM LN-830acn dual Wireless, R&S®LANCOM LN-830E Wireless, R&S®LANCOM L-822acn dual Wireless, R&S®LANCOM LN-830U, R&S®LANCOM L-1302acn dual Wireless, R&S®LANCOM L-1310acn dual Wireless, R&S®LANCOM LN-860, R&S®LANCOM LN-862 ▶ R&S®LANCOM LN-1700, R&S®LANCOM LN-1702 ▶ R&S®LANCOM LN-1700B, R&S®LANCOM LN-1702B, R&S®LANCOM LN-1700UE ▶ R&S®LANCOM LW-500, R&S®LANCOM LW-600, R&S®LANCOM LW-700 ▶ R&S®LANCOM LX-6200, R&S®LANCOM LX-6200E ▶ R&S®LANCOM LX-6400, R&S®LANCOM LX-6402, R&S®LANCOM LX-6500, R&S®LANCOM LX-6500E ▶ R&S®LANCOM LX-7000-Serie
Outdoor	▶ R&S®LANCOM OAP-321, R&S®LANCOM OAP-321-3G ▶ R&S®LANCOM OAP-382, R&S®LANCOM OAP-322 ▶ R&S®LANCOM OAP-821, R&S®LANCOM OAP-822, R&S®LANCOM OAP-830 ▶ R&S®LANCOM OAP-1700B, R&S®LANCOM OAP-1702B ▶ R&S®LANCOM OW-602 ▶ R&S®LANCOM OW-702 ▶ R&S®LANCOM OX-6400, R&S®LANCOM OX-6402
Industrial	▶ R&S®LANCOM IAP-321, R&S®LANCOM IAP-321-3G, R&S®LANCOM IAP-322 ▶ R&S®LANCOM IAP-821, R&S®LANCOM IAP-822 ▶ R&S®LANCOM IAP-1781VAW+
UMTS/HSPDA	▶ R&S®LANCOM 1780EW-4G, R&S®LANCOM 1780EW-3G, R&S®LANCOM 1780EW-4G+
WLAN-Router und IADs	▶ R&S®LANCOM 1781VAW, R&S®LANCOM 1781AW, R&S®LANCOM 1781EW(+) ▶ R&S®LANCOM 1783VAW, R&S®LANCOM 883 VoIP ▶ R&S®LANCOM 1793VAW, R&S®LANCOM 1790VAW ▶ R&S®LANCOM 1800VAW, R&S®LANCOM 1800VAW-4G, R&S®LANCOM 1800EFW
Public Spot - Technische Details	
Anzahl unterstützter User	256 gleichzeitig aktive Benutzer

R&S®LANCOM WLC-60

Public Spot - Technische Details	
Anmeldung über Webportal (Captive Portal)	Anmeldung am Hotspot nach Eingabe von Benutzername und Passwort über ein Webportal (frei konfigurierbar)
Selbstständige Benutzeranmeldung am Hotspot (Smart Ticket)	Zugangsdaten zum Public Spot-Netz werden dem Nutzer per E-Mail oder SMS zugesandt. Die E-Mail wird dabei vom Gerät via SMTP verschickt. Der SMS-Versand erfolgt über das integrierte Mobilfunk-Modem, ein E-Mail-2-SMS-Gateway oder einen nachgeschalteten Mobilfunk-Router
Voucher-Ausgabe	Mit wenigen Mausklicks können bis zu 256 Tickets mit Zugangsdaten für den Hotspot generiert und über einen beliebigen Office-Drucker ausgedruckt werden. Der Voucher lässt sich individuell gestalten.
Einfacher Public Spot-Login mit einem Klick	Nach Akzeptierung der allgemeinen Nutzungsbedingungen erhält der Benutzer für einen definierbaren Zeitraum Gastzugang
WISPr	Wireless Internet Service Provider roaming erlaubt es SmartClients, sich an einem Public Spot anzumelden, ohne dass der Benutzer Zugangsdaten auf einer Webseite eintragen muss.
Re-Login	Der Public Spot erkennt bekannte Clients und authentifiziert sie automatisch. Nach der erstmaligen Authentifizierung speichert der Hotspot die Client-Informationen (MAC-Adresse) für einen konfigurierbaren Zeitraum, so dass für den Benutzer keine erneute manuelle Eingabe der Zugangsdaten mehr nötig ist - ein deutlicher Komfortgewinn für regelmäßige Gäste.
Walled Garden-Funktion	Ermöglicht, ausgewählte Websites auch ohne Freischaltung des Gastzugangs zugänglich zu machen (z. B. Websites von Sponsoren oder des Hotels)
Bandbreitenmanagement	Die verfügbare Bandbreite für Public Spot-Benutzergruppen lässt sich individuell konfigurieren und steht im Assistenten zum Anlegen eines neuen Benutzers zur Verfügung, z. B. zur Unterscheidung von normalen und Premium-Usern
Unterstützung von volumen- und zeitbasierten Accounts	Gültigkeit eines Hotspot-Zugangs kann über Begrenzung des Download-Volumens der Nutzer oder über die Zeit festgelegt werden
Umleitung auf Werbe-Webseiten	In konfigurierbaren Zeitabständen kann der Public Spot-Benutzer auf Werbe-Webseiten des Betreibers umgeleitet werden
Dynamische VLAN-Zuweisung	Zuweisung von Public Spot-Benutzern zu individuell konfigurierbaren Netzen
Idle time out basierter Disconnect	Verbindung wird nach einer konfiguerierbaren Zeit ohne Internetzugriff getrennt
Disconnect bei WLAN Logout	Automatische Abmeldung vom Hotspot, wenn Client nicht mehr im WLAN gesehen wird, Funktion nur möglich bei Geräten mit WLAN
Mehrfach-Login	Gestattet Public Spot-Benutzern, sich mit mehreren Geräten gleichzeitig auf einem Account an einem Hotspot anzumelden
Public Spot - Externe Datenschnittstellen	
RADIUS-Server-Schnittstelle	Standardmäßig speichert der Public Spot sitzungsrelevante Daten für spätere Abrechnungen auf einem internen RADIUS-Server. Bei Bedarf kann auf einem Gerät mit Public Spot die Weiterleitung auf einen externen RADIUS-Server konfiguriert werden
SYSLOG	R&S®LANCOM Geräte verfügen über einen integrierten SYSLOG-Speicher. Alternativ können R&S®LANCOM Geräte an externe SYSLOG-Server angebunden werden
XML	Um neben der Anmeldung über Benutzername/Passwort noch weitere Authentifizierungsszenarien zur Verfügung zu stellen, kann die R&S®LANCOM Public Spot-Lösung mit externen Servern über die XML-Schnittstelle angebunden werden
FIAS (optional)	Ermöglicht direkte Kommunikation zwischen dem R&S®LANCOM Public Spot und einem Property Management System (PMS), welches das von Micros Fidelio verwendete FIAS-Protokoll unterstützt. Schnittstelle ist nur in Kombination mit der R&S®LANCOM Public Spot PMS Accounting Plus Option nutzbar
Layer 2-Funktionen	
VLAN	4.096 IDs nach IEEE 802.1q, dynamische Zuweisung
Quality of Service	WME nach IEEE 802.11e, Wi-Fi Certified™ WMM®
Bandbreitenlimitierungen	pro SSID, pro WLAN-Client
Multicast	IGMP-Snooping, MLD-Snooping
Protokolle	Ethernet über GRE-Tunnel (EoGRE), L2TPv3, ARP-Lookup, LLDP, DHCP Option 82, IPv6-Router-Advertisement-Snooping, DHCPv6-Snooping, LDRA (Lightweight DHCPv6 Relay Agent), Spanning Tree, Rapid Spanning Tree, ARP, Proxy ARP, BOOTP, DHCP, LACP

R&S®LANCOM WLC-60

Layer 2-Funktionen	
OAM	Ethernet Link OAM 802.3ah, IEEE 802.1ag CFM
Layer 3-Funktionen	
Firewall	Stateful Inspection Firewall mit Paketfilterung, erweitertem Port-Forwarding, N:N IP-Adressumsetzung, Paket-Tagging, Unterstützung von DNS-Zielen, unterschiedlichen Aktionen und unterschiedlichen Benachrichtigungen
Quality of Service	Traffic Shaping, Bandbreitenreservierung, DiffServ/TOS, Paketgrößensteuerung, Layer 2-in-Layer 3-Tagging, Unterstützung von 8 QoS Queues (davon 6 frei konfigurierbar)
Sicherheit	Intrusion Prevention, IP-Spoofing, Access-Control-Listen, Denial-of-Service Protection, detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung, URL-Blocker, Passwortschutz, programmierbarer Reset-Taster
PPP-Authentifizierungsmechanismen	PAP, CHAP, MS-CHAP und MS-CHAPv2
Hochverfügbarkeit/Redundanz	VRRP (Virtual Router Redundancy Protocol)
Router	IPv4-, IPv6-, IPv4/IPv6 Dual Stack
SD-WAN Application-Routing	SD-WAN Application Routing in Verbindung mit der R&S®LANCOM Management Cloud
SD-WAN Dynamic Path Selection	SD-WAN Dynamic Path Selection in Verbindung mit der R&S®LANCOM Management Cloud
Router-Virtualisierung	ARF (Advanced Routing und Forwarding) mit bis zu 16 Kontexten
IPv4-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DNS-Client, DNS-Server, DNS-Relay, DNS-Proxy, Dynamic DNS-Client, DHCP-Client, DHCP-Relay und DHCP-Server mit Autodetection, NTP-Client, SNTP-Server, Policy-based Routing, Bonjour-Proxy, RADIUS
IPv6-Dienste	HTTP- und HTTPS-Server für die Konfiguration per Webinterface, DHCPv6-Client, DHCPv6-Server, DHCPv6-Relay, DNS-Client, DNS-Server, Dynamic DNS-Client, NTP-Client, SNTP-Server, Bonjour-Proxy, RADIUS
Dynamische Routing-Protokolle	RIPv2, BGPv4, OSPFv2, LISP (Locator/ID Separation Protocol)
IPv4-Protokolle	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, PPPoE (Server), RADIUS, RADSEC (Secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3
IPv6-Protokolle	NDP, Stateless Address Autoconfiguration (SLAAC), Stateful Address Autoconfiguration (mit DHCPv6), Router Advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, BGP, LISP, Syslog, SNMPv1,v2c,v3, MLDv2, PIM, NPTv6 (NAT66), VRRPv3
Multicast Routing	PIM (Protocol Independent Multicast), IGMP-Proxy, MLD-Proxy
WAN-Betriebsarten	VDSL, ADSL1, ADSL2 oder ADSL2+ jeweils auch mit externem Modem an einem ETH-Port (auch simultan zum LAN-Betrieb)
WAN-Protokolle	PPPoE, Multi-PPPoE, ML-PPP, GRE, EoGRE, PPTP (PAC oder PNS), L2TPv2 (LAC oder LNS), L2TPv3 mit Ethernet-Pseudowire, IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 und IPv4/IPv6 Dual Stack Session), IP(v6)oE (Autokonfiguration, DHCPv6 oder Statisch)
Tunnelprotokolle (IPv4/IPv6)	6to4, 6in4, 6rd, Dual Stack Lite, 464XLAT
VPN	
IPSec over HTTPS	Ermöglicht IPSec VPN durch Firewalls in Netzen, für die z. B. Port 500 für IKE gesperrt ist, auf Basis von TCP über Port 443. Geeignet für Client-to-Site und Site-to-Site-Verbindungen. IPSec over HTTPS basiert auf der NCP VPN Path Finder Technology
Anzahl der VPN-Tunnel	5 Tunnel gleichzeitig aktiv bei Kombination von IPSec- mit PPTP-(MPPE) und L2TPv2-Tunneln, unbegrenzte Anzahl konfigurierbarer Gegenstellen.
Hardware-Beschleuniger	Integrierter Hardwarebeschleuniger für die 3DES/AES-Ver- und -Entschlüsselung
1-Click-VPN Site-to-Site	Erzeugen von VPN-Verbindungen zwischen R&S®LANCOM-Routern per "Drag and Drop" mit einem Klick in LANconfig
IKE, IKEv2	IPSec-Schlüsselaustausch über Preshared Key oder Zertifikate (RSA-Signature, ECDSA-Signature, Digital-Signature)
Smart Certificate	Komfortable Erstellung von digitalen X.509 Zertifikaten mittels einer eigenen Zertifizierungsstelle (SCEP-CA) via Weboberfläche oder SCEP.

R&S®LANCOM WLC-60

VPN	
Zertifikate	Unterstützung von X.509 digitalen mehrstufigen Zertifikaten, kompatibel z.B. zu Microsoft Server / Enterprise Server und OpenSSL. Secure Key Storage zur Sicherung eines privaten Schlüssels (PKCS#12) gegen Diebstahl.
Zertifikatsrollout	Automatisierte Erzeugung sowie Rollout und Verlängerung von Zertifikaten mit SCEP (Simple Certificate Enrollment Protocol) pro Zertifikatshierarchie
Certificate Revocation Lists (CRL)	Abruf von CRLs mittels HTTP pro Zertifikatshierarchie
OCSP Client	Prüfen von X.509-Zertifikaten anhand von OCSP (Online Certificate Status Protocol), in Echtzeit arbeitende Alternative zu CRLs
XAUTH	XAUTH-Client zur Anmeldung von R&S®LANCOM Routern und Access Points an XAUTH-Servern inkl. IKE-Config-Mode. XAUTH-Server, der die Anmeldung von Clients per XAUTH an R&S®LANCOM Routern ermöglicht. Anbindung des XAUTH-Servers an RADIUS-Server zur Authentisierung von VPN-Zugängen pro Verbindung über eine zentrale Benutzerverwaltung. Authentisierung für VPN-Client-Zugänge via XAUTH mit RADIUS-Anbindung auch mit OTP-Tokens
Proadaptive VPN	Automatisierte Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routing-Einträge anhand eines Default-Eintrags bei Site-to-Site Verbindungen.
Algorithmen	3DES (168 Bit), AES-CBC und -GCM (128, 192 und 256 Bit), RSA (1024-4096 Bit), ECDSA (P-256-, P-384-, P-521-Kurven) und Chacha20-Poly 1305. OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen. MD-5, SHA-1, SHA-256, SHA-384 oder SHA-512 Hashes
NAT-Traversal	Unterstützung von NAT-Traversal (NAT-T) für den VPN-Einsatz auf Strecken, die kein VPN-Passthrough unterstützen
MOBIKE	IKEv2 VPN-Clients können nahtlos zwischen verschiedenen Netzwerken wechseln (z. B. von WLAN zu Mobilfunk), ohne den VPN-Tunnel neu aufbauen zu müssen
Dynamic DNS	Ermöglicht die Registrierung der IP-Adresse bei einem Dynamic-DNS-Provider, falls keine feste IP-Adresse für den VPN-Verbindungsaufbau verwendet wird
Spezifisches DNS-Forwarding	DNS-Forwarding einstellbar pro DNS-Domäne, z.B. zur Auflösung interner Namen durch eigenen DNS-Server im VPN und Auflösung externer Namen durch Internet-DNS-Server. Eintrag für Backup-DNS pro DNS-Weiterleitung
Split-DNS	Ermöglicht für IKEv2 das selektive Weiterleiten von Datenverkehr abhängig von der angesprochenen DNS-Domäne.
IPv4 VPN	Kopplung von IPv4 Netzwerken
IPv4 VPN über IPv6 WAN	Nutzung von IPv4 VPN über IPv6 WAN-Verbindungen
IPv6 VPN	Kopplung von IPv6 Netzwerken
IPv6 VPN über IPv4 WAN	Nutzung von IPv6 VPN über IPv4 WAN-Verbindungen
RADIUS	RADIUS Authorization und Accounting, Auslagerung von VPN-Konfigurationen in externem RADIUS-Server bei IKEv2, RADIUS CoA (Change of Authorization)
High Scalability VPN (HSVPN)	Übertragung von mehreren, sicher getrennten Netzen innerhalb eines VPN-Tunnels
Advanced Mesh VPN	Dynamischer VPN-Tunnelaufbau zwischen beliebigen Filialen bei Bedarf
Content Filter (optional)	
Demo-Version	Aktivierung der 30-Tage Testversion nach kostenloser Produktregistrierung unter http://www.lancom-systems.de/routeroptions
URL-Filter-Datenbank/Ratingserver*	Weltweit redundante Ratingserver der IBM Security Solutions zur Abfrage von URL-Klassifizierungen. Datenbank mit über 100 Millionen Einträgen, die etwa 10 Milliarden Webinhalte abdeckt. Täglich fast 150.000 Aktualisierungen durch Webcrawler, welche automatisiert Webseiten untersuchen und kategorisieren: durch Textklassifizierung mit optischer Zeichenerkennung, Schlüsselwortsuche, Bewertung von Häufigkeit und Wort-Kombinationen, durch Webseitenvergleich hinsichtlich Text, Bildern und Seitenelementen, durch Objekterkennung von speziellen Zeichen, Symbolen, Warenzeichen, verbotenen Bildern, durch Erkennung von Erotik und Nacktheit anhand der Konzentration von Hauttönen in Bildern, durch Struktur- und Linkanalyse, durch Malware-Erkennung in Binärdateien und Installationspaketen
URL-Prüfung*	Datenbankbasierte Online-Prüfung von Webseiten (HTTP/HTTPS). HTTPS-Webseiten werden durch die Entnahme von angesteuerten DNS-Namen aus HTTPS-Serverzertifikaten oder durch “Reverse DNS lookup” der IP-Adresse geprüft und ggfs. blockiert.

R&S®LANCOM WLC-60

Content Filter (optional)	
Kategorien/Kategorie-Profile*	Definition von Filterregeln pro Profil durch Zusammenstellen von Kategorie-Profilen aus 58 Kategorien, z.B. zur Einschränkung der Internetnutzung auf geschäftliche Anwendungen (Unterbinden privater Nutzung) oder Schutz vor jugendgefährdenden oder gefährlichen Inhalten wie z.B. Malware-Seiten. Übersichtliche Auswahl durch Zusammenstellung thematisch ähnlicher Kategorien zu Gruppen. Inhalte pro Kategorie erlauben, blockieren oder für Override freigeben
Override**	Für Kategorien kann ein Override vergeben werden, der es Anwendern fallweise erlaubt, eigentlich gesperrte Seiten durch manuelle Bestätigung zu laden. Der Override kann zeitlich beschränkt für die Kategorie, die Domäne oder eine Kombination aus beidem ausgesprochen werden. Möglichkeit zur Benachrichtigung eines Administrators im Fall von Overrides
Black-/Whitelist	Manuell konfigurierbare Listen zum expliziten Erlauben (Whitelist) oder Verbieten (Blacklist) von Webseiten pro Profil, unabhängig von der Bewertung durch den Ratingserver. Platzhalter (Wildcards) zur Definition von Gruppen von Seiten oder Filtern von Unterseiten
Profile	Zusammenfassen von Zeitrahmen, Black-/Whitelists und Kategorie-Profilen zu getrennt aktivierbaren Profilen für Content Filter Aktionen. Werksseitig aktiviertes Default-Profil mit Standard-Einstellungen zum Blocken von rassistischen, pornografischen, kriminellen, extremistischen Inhalten sowie anonymen Proxies, Waffen/Militär, Drogen, SPAM und Malware
Zeitrahmen	Flexible Definition von Zeitrahmen, um Profile zur Filterung in Abhängigkeit von Tageszeiten oder Wochentagen zu definieren, z. B. für Lockerung während Pausenzeiten für privates Surfen
Flexibel anwendbare Firewall-Aktion	Anwendung des Content Filters durch Content Filter Aktionen mit Auswahl des gewünschten Profils in der Firewall. Firewall-Regeln ermöglichen die flexible Anwendung eigener Profile für verschiedene Clients, Netze oder Verbindungen zu bestimmten Servern
Individuelle Rückmeldungen (bei blockiert, Fehler, Override)	Antwortseiten des Content Filters für blockierte Seiten, Fehler und Override können individuell gestaltet und durch Variablen mit aktuellen Informationen zu Kategorie, URL und Kategorisierung des Ratingservers versehen werden. Sprachabhängige Definition von Antwortseiten, je nach vom Anwender ausgewählter Anzeigesprache des Webbrowsers
Umleitung zu externen Webseiten	Alternativ zur Anzeige der geräteinternen Antwortseiten für blockierte Seiten, Fehler oder Override können auch Seiten von externen Webservern aufgerufen werden (Redirect)
Lizenzmanagement	Automatische Benachrichtigung vor Ablauf der Lizenz per E-Mail, LANmonitor, SYSLOG und SNMP-Trap. Aktivierung der nächsten Lizenz-Verlängerung zu beliebigem Zeitpunkt vor dem Ablauf der aktuellen Lizenz (Start des neuen Lizenzzeitraumes passend zum Ablauf der aktuellen Lizenz)
Statistiken	Anzeige der Anzahl der geprüften und gesperrten Webseiten je Kategorie in LANmonitor. Logging aller Content-Filter-Events in LANmonitor; tägliches, wöchentliches oder monatliches Anlegen einer Protokolldatei. Hitliste der meist aufgerufenen Seiten und Ratingergebnisse. Auswertung der Verbindungseigenschaften, minimalen, maximalen und durchschnittlichen Antwortzeiten des Ratingservers
Alarmierungen	Benachrichtigung bei Content-Filterung einstellbar via E-Mail, SNMP, SYSLOG sowie LANmonitor
Assistent für Standard-Konfigurationen	Assistent zur Einrichtung des Content Filters für typische Anwendungsszenarien in wenigen Schritten, inklusive Erzeugung der nötigen Firewall-Regeln mit entsprechender Aktion
Maximale Benutzeranzahl	Gleichzeitige Prüfung des HTTP(S)-Verkehrs für maximal 100 unterschiedliche IP-Adressen im LAN
***) Hinweis**	Die Kategorisierung erfolgt durch IBM. Die jederzeitige Richtigkeit der Kategorisierungen können weder IBM noch R&S®LANCOM garantieren.
****) Hinweis**	Die Override-Funktionalität steht nur für HTTP-Seiten zur Verfügung.
VoIP	
SIP ALG	SIP ALG (Application Layer Gateway) agiert als Proxy für SIP. Automatische Öffnung der notwendigen Ports für Sprachdaten. Automatische Adressumsetzung (STUN unnötig).
Schnittstellen	
WAN: Ethernet	10/100/1000 MBit/s Gigabit Ethernet
Ethernet Ports	4 individuelle Ports, 10/100/1000 MBit/s Gigabit Ethernet, im Auslieferungszustand als Switch geschaltet. Bis zu 3 Ports können als zusätzliche WAN-Ports geschaltet werden. Ethernet-Ports können in der LCOS-Konfiguration elektrisch deaktiviert werden. Unterstützung von Energiesparfunktionen nach IEEE 802.3az
SFP-Einschub	Steckplatz für Small Form-factor Pluggable Gigabit-Ethernet-Transceiver ("mini-GBIC"). Kompatibel mit optionalen R&S®LANCOM SFP-Modulen für Glasfaseranschlüsse über kurze Distanzen (SX) oder lange Distanzen (LX). Im Auslieferungszustand als weiterer LAN-Port geschaltet, kann als WAN-Port konfiguriert werden

R&S®LANCOM WLC-60

Schnittstellen	
Port-Konfiguration	Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus). LAN Ports können als Switch oder isoliert betrieben werden. Als WAN-Port können zusätzliche, externe DSL-Modems oder Netzabschlussrouter inkl. Load-Balancing und Policy-based Routing betrieben werden. DMZ-Ports können mit einem eigenen IP-Adresskreis ohne NAT versorgt werden
USB 2.0 Host-Port	USB 2.0 Hi-Speed Host-Port zum Anschluss von USB-Druckern (USB-Druck-Server), seriellen Geräten (COM-Port-Server), USB-Datenträgern (FAT Dateisystem); bidirektionaler Datenaustausch möglich
Serielle Schnittstelle	Serielle Konfigurationsschnittstelle / COM-Port (USB-C): 9.600-115.000 Bit/s.
Management und Monitoring	
Management	LANconfig, WEBconfig, R&S®LANCOM Layer 2 Management (Notfall-Management)
Management-Funktionen	Alternative Boot-Konfiguration, automatisches Software-Update über LANconfig, individuelle Zugriffs- und Funktionsrechte für bis zu 16 Administratoren, RADIUS- und RADSEC-Benutzerverwaltung, Fernwartung (über WAN oder (W)LAN, Zugangsrechte (lesen/schreiben) separat einstellbarüber) SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, alternative Steuerung der Zugriffsrechte durch TACACS+, Scripting, zeitliche Steuerung aller Parameter und Aktionen durch CRON-Dienst
FirmSafe	Zwei speicherbare Firmware-Versionen im Gerät, inkl. Testmodus bei Firmware-Updates
Automatisches Firmware-Update	Konfigurierbare automatische Prüfung und Installation von Firmware-Updates
Monitoring	R&S®LANCOM Management Cloud, LANmonitor, WLANmonitor
Monitoring-Funktionen	Geräte-SYSLOG, SNMPv1,v2c,v3 inkl. SNMP-TRAPS, sehr umfangreiche LOG- und TRACE-Möglichkeiten, PING und TRACEROUTE zur Verbindungsüberprüfung, interne Loggingbuffer für SYSLOG und Firewall-Events
Monitoring-Statistiken	Umfangreiche Ethernet-, IP- und DNS-Statistiken, SYSLOG-Fehlerzähler, Accounting inkl. Export von Accounting-Informationen über LANmonitor und SYSLOG, Layer-7-Anwendungserkennung inkl. anwendungsbezogenes Erfassen des verursachten Traffics
IPerf	IPerf ermöglicht es den Datendurchsatz von IP-Netzwerken zu testen (integrierter Client und Server)
SLA-Monitor (ICMP)	Performance-Überwachung von Verbindungen
Netflow	Export von Informationen über eingehenden bzw. ausgehenden IP-Datenverkehr
Hardware	
Gewicht	450 g
Spannungsversorgung	12 V DC, externes Steckernetzteil (230 V/110 V bei US-Variante)
Gehäuse	Robustes Kunststoffgehäuse, Anschlüsse auf der Rückseite, für Wandmontage vorbereitet, Kensington-Lock; Maße 210 x 45 x 140 mm (B x H x T)
Anzahl Lüfter	1 leiser Lüfter
Leistungsaufnahme (max./Idle)	15 Watt / 6 Watt
Konformitätserklärungen*	
CE	EN 62368, EN 55022, EN 55024
Herkunftsland	Made in Germany
***) Hinweis**	Auf unserer Website www.lancom-systems.de finden Sie die vollständigen Erklärungen zur Konformität auf der jeweiligen Produktseite
Lieferumfang	
Handbuch	Quick Installation Guide (DE/EN)
Kabel	Ethernet-Kabel, 3 m
Netzteil	Externes Steckernetzteil (230 V), NEST 12 V/2,0 A DC/S, Hohlstecker 2,1/5,5 mm, Temperaturbereich -5 bis +45° C, R&S®LANCOM Art.-Nr. 111303

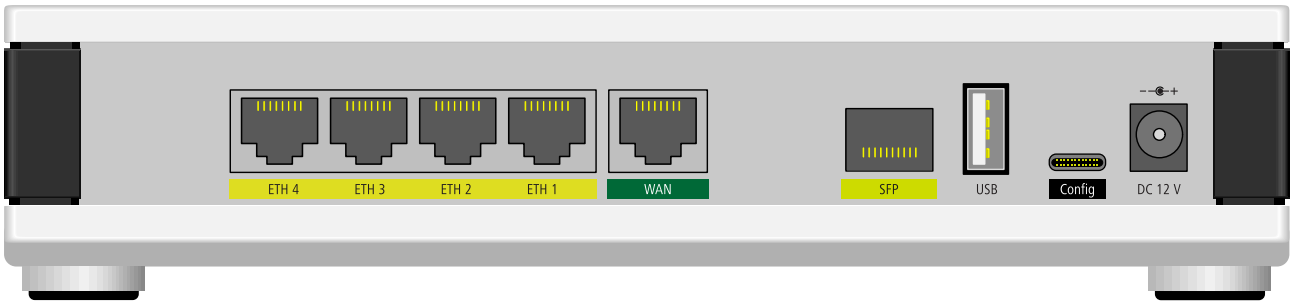
R&S®LANCOM WLC-60

Support	
Gewährleistungsverlängerung	Kostenfreie Gewährleistungsverlängerung auf 3 Jahre (Austausch-Service bei Defekt) Details finden Sie hier: Link. Es finden die Service- und Supportbedingungen mit Stand vom 01.07.2026, abrufbar unter rs-nc.rohde-schwarz.com/fileadmin/pdf/LCS/ServiceSupportConditions/Rohde-Schwarz-Networks-and-Cybersecurity-GmbH-Service-und-Supportbedingungen-20260701.pdf, Anwendung.
Security Updates	Bis 2 Jahre nach End of Sale des Gerätes (aber min. 3 Jahre, siehe Link), verlängerbar mit R&S®NC Support-Produkten
Software Updates	Regelmäßig kostenfreie Updates inkl. neuer Features im Rahmen des R&S®NC Lifecycle Managements (Link)
Angaben zum EU Data Act	Details zu Produktdaten und Daten verbundener Dienste finden Sie unter: Link
Hersteller-Support	Erhältlich mit R&S®NC-Produkten wie Support Access (nur für R&S®NC Community Partner), Direct oder Premium
R&S®NC Replacement Basic S	Security Updates bis EOL (min. 5 Jahre) und 5 Jahre Austausch-Service mit Versand des Ersatzgerätes innerhalb von 5 Tagen nach Eintreffen des defekten Gerätes (8/5/5Days), Art.-Nr. 10720
R&S®NC Replacement Advanced S	Security Updates bis EOL (min. 5 Jahre) und 5 Jahre NBD-Vorabaustausch mit Lieferung des Ersatzgerätes innerhalb eines Werktages (8/5/NBD), Art.-Nr. 10730
R&S®NC Support Direct 24/7 S	Direkter, priorisierter 10/5-Hersteller-Support inkl. 24/7-Notfall-Hotline und Security Updates für das Gerät, zugesicherte Erstreaktionszeiten (SLA) von max. 30 Minuten bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre(Art.-Nr. 10752, 10753 oder 10754)
R&S®NC Support Direct Advanced 24/7 S	Direkter, priorisierter 10/5-Hersteller-Support inkl. 24/7-Notfall-Hotline und Security Updates für das Gerät, NBD-Vorabaustausch mit Lieferung des Ersatzgerätes zum nächsten Werktag (24/7/NBD), zugesicherte Erstreaktionszeiten (SLA) von max. 30 Minuten bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre (Art.-Nr. 10776, 10777 oder 10778)
R&S®NC Support Direct 10/5 S	Direkter, priorisierter 10/5-Hersteller-Support und Security Updates für das Gerät, zugesicherte Erstreaktionszeiten (SLA) von max. 2 Stunden bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre.(Art.-Nr. 10740, 10741 oder 10742)
R&S®NC Support Direct Advanced 10/5 S	Direkter, priorisierter 10/5-Hersteller-Support und Security Updates für das Gerät, NBD-Vorabaustausch mit Lieferung des Ersatzgerätes zum nächsten Werktag (10/5/NBD), zugesicherte Erstreaktionszeiten (SLA) von max. 2 Stunden bei telefonischer Meldung massiver Betriebsstörungen (Priorität 1) und max. 4 Stunden für alle weiteren Anliegen (Priorität 2), laufzeitbasiert für 1, 3 oder 5 Jahre.(Art.-Nr. 10764, 10765 oder 10766)
Software	
Lifecycle Management	Das Gerät unterliegt nach der Abkündigung (End of Sale) dem R&S®NC Lifecycle Management. Details dazu finden Sie unter: Link
IT-Security made in Germany	Die Entwicklung und Qualitätssicherung erfolgen in Deutschland nach hohen Sicherheitsstandards. Das Qualitäts- zeichen „IT-Security made in Germany" des Bundesverbands IT-Sicherheit belegt das erreichte Sicherheitsniveau.
Optionen	
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 1 Jahr (für R&S®LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller R&S®LANCOM WLC-60), Art.-Nr. 62168
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 3 Jahre (für R&S®LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller R&S®LANCOM WLC-60), Art.-Nr. 62169
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 5 Jahre (für R&S®LANCOM SD-WAN Gateways der 700-, 800-, 1600-, 1700-, 1800-, IAP- und OAP-Serien sowie WLAN-Controller R&S®LANCOM WLC-60), Art.-Nr. 62170
R&S®LANCOM BPjM Filter	R&S®LANCOM BPjM Filter Option, 5 Jahre Laufzeit, Art.-Nr. 61418
R&S®LANCOM Public Spot PMS Accounting Plus	Erweiterung der R&S®LANCOM Public Spot (XL) Option für die Anbindung an Hotelabrechnungssysteme mit FIAS-Schnittstelle (wie Micros Fidelio) zur Authentifizierung und Abrechnung von Gastzugängen, für 178x-, 179x-, 19xx-Router, 2100EF, WLCs und aktuelle Central Site Gateways, Art.-Nr. 61638
R&S®LANCOM WLC AP Upgrade +6	R&S®LANCOM WLC AP Upgrade +6 Option, ermöglicht die Verwaltung von 6 weiteren Access Points/WLAN-Router (additiv bis zu 60) über den WLC, Art-Nr. 61629

LCOS 10.94

R&S®LANCOM WLC-60

Geeignetes Zubehör	
1000Base-BX20-U SFP-Modul	R&S®LANCOM SFP-AON-1, Art.-Nr.: 60200
GPON ONT SFP-Modul	R&S®LANCOM SFP-GPON-1, Kompatibel zum Betrieb an FTTH-Anschlüssen der Deutschen Telekom, Art.-Nr.: 60199
1000Base-BX20 SFP-Modul-Paar	R&S®LANCOM SFP-BiDi1550-SC1, Art.-Nr.: 60201
1000Base-SX SFP-Modul, 550 m	R&S®LANCOM SFP-SX-LC1, Art.-Nr.: 61556
1000Base-SX SFP-Modul, 550 m (10er Bulk)	R&S®LANCOM SFP-SX-LC1 (10er Bulk), Art.-Nr.: 60184
1000Base-SX SFP-Modul, 2 km	R&S®LANCOM SFP-SX2-LC1, Art.-Nr.: 60183
1000Base-LX SFP-Modul	R&S®LANCOM SFP-LX-LC1, Art.-Nr.: 61557
1000Base-LX SFP-Modul (10er Bulk)	R&S®LANCOM SFP-LX-LC1 (10er Bulk), Art.-Nr.: 60185
SFP-Kupfer-Modul 1G	R&S®LANCOM SFP-CO1, Art.-Nr.: 61494
SFP-Kupfer-Modul 1G (10er Bulk)	R&S®LANCOM SFP-CO1 (10er Bulk), Art.-Nr.: 60186
19"-Montage	19" Rackmount-Adapter, Art.-Nr. 61501
19"-Montage	19" Rack Mount Plus Adapter, Art.-Nr. 61644
Artikelnummer(n)	
R&S®LANCOM WLC-60	61719



Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Würselen | Deutschland
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity