

LCOS 10.94

# R&S® LANCOM 1650E

**Sicherer Internetzugang über Gigabit Ethernet**



Kleine und mittelgroße Unternehmen benötigen oftmals nur eins: einen sicheren und zuverlässigen Zugang zum Internet sowie die Anbindung mobiler Mitarbeitender oder Filialen an die Firmenzentrale. Mit dem R&S® LANCOM 1650E und ausgezeichnetem R&S® LANCOM IPSec- und WireGuard-VPN vernetzen Sie Ihre Standorte problemlos miteinander. Der Anschluss an beliebige DSL-, Kabel- und Glasfasermodems bietet größtmögliche Flexibilität bezüglich der am Standort verfügbaren Internetleitungen. Die SD-WAN-Funktionen des Filialrouters in Kombination mit der R&S® LANCOM Management Cloud (R&S® LMC) vereinfachen nicht nur Ihr Netzwerkmanagement, sondern beschleunigen und automatisieren die Verwaltung, das Monitoring und den Rollout Ihrer Netzwerkkomponenten.

- ▶ Secure SD-WAN – zentrale Cloud-Verwaltung mit sicherer Netztrennung, automatisierter Bereitstellung und intelligenter Pfadsteuerung
- ▶ Flexibler Anschluss externer Modems über Gigabit Ethernet
- ▶ 3 integrierte VPN-Kanäle
- ▶ Netzvirtualisierung mit 2 Netzen auf einem Gerät (ARF)
- ▶ Erweiterter Schutz mit dem Content Filter der R&S® LANCOM Security Essentials Option

# R&S® LANCOM 1650E

## **WAN-Anbindung über Gigabit Ethernet**

Der Internet Access Router ermöglicht den flexiblen Anschluss externer Provider-Modems über Gigabit Ethernet und bietet damit größtmögliche Unabhängigkeit hinsichtlich der am Standort verfügbaren Internetanschlüsse.

## **Sichere, intelligente Standortvernetzung mit Secure SD-WAN**

R&S® LANCOM Secure SD-WAN ermöglicht die zentral gesteuerte und sichere Vernetzung aller Standorte. In Kombination mit der R&S® LANCOM Management Cloud (R&S® LMC) lassen sich unternehmensweite Sicherheits- und Zugriffsrichtlinien umsetzen sowie Rollouts, Konfigurationen und Updates automatisiert beschleunigen. Verschlüsselte Auto-VPNs, High Scalability & Advanced Mesh VPNs, Dynamic Path Selection sowie Active/Active-WAN mit Load Balancing sorgen für resiliente, ausfallsichere Verbindungen.

## **Mehrschichtige Sicherheit – automatisch integriert**

Ab Werk ist eine SPI-Firewall im LCOS-Betriebssystem integriert (Built-in Security). Sichere Netzwerksegmentierung erfolgt über ARF und VLAN, während PQ-PSKs vor „Store-now-decrypt-later“-Angriffen schützen und auf Quantenresistenz vorbereiten.

## **Verschlüsselte Kommunikation über VPN**

Das Gateway ermöglicht geschützte Internetverbindungen für mobile Mitarbeitende, Home-Offices und Standorte über 3 integrierte VPN-Kanäle (IPsec und WireGuard).

## **Individuell erweiterbare Sicherheit mit Content Filter**

Die R&S® LANCOM Security Essentials Option erweitert den Router um einen cloudbasierten Web- und Content-Filter gegen Phishing, Ransomware und schädlichen Webseiten und ist dank unbegrenzter Nutzeranzahl optimal für wachsende Netzwerke.

# R&S® LANCOM 1650E

Layer 2-Funktionen	
<b>VLAN</b>	4.096 IDs nach IEEE 802.1q, dynamische Zuweisung
<b>Multicast</b>	IGMP-Snooping, MLD-Snooping
<b>Protokolle</b>	ARP-Lookup, LLDP, ARP, Proxy ARP, BOOTP, DHCP
Layer 3-Funktionen	
<b>Firewall</b>	Stateful Inspection Firewall mit Paketfilterung, erweitertem Port-Forwarding, N:N IP-Adressumsetzung, Paket-Tagging, Unterstützung von DNS-Zielen, unterschiedlichen Aktionen und unterschiedlichen Benachrichtigungen
<b>Quality of Service</b>	Traffic Shaping, Bandbreitenreservierung, DiffServ/TOS, Paketgrößensteuerung, Layer 2-in-Layer 3-Tagging, Unterstützung von 8 QoS Queues (davon 6 frei konfigurierbar)
<b>Sicherheit</b>	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
<b>PPP-Authentifizierungsmechanismen</b>	PAP, CHAP, MS-CHAP und MS-CHAPv2
<b>Hochverfügbarkeit/Redundanz</b>	VRRP (Virtual Router Redundancy Protocol)
<b>Router</b>	IPv4-, IPv6-, IPv4/IPv6 Dual Stack
<b>SD-WAN Application-Routing</b>	SD-WAN Application Routing in Verbindung mit der R&S® LANCOM Management Cloud
<b>SD-WAN Dynamic Path Selection</b>	SD-WAN Dynamic Path Selection in Verbindung mit der R&S® LANCOM Management Cloud
<b>SD-WAN Zero Touch Deployment</b>	Zero Touch Inbetriebnahme des Geräts in Verbindung mit der R&S® LANCOM Management Cloud
<b>Router-Virtualisierung</b>	ARF (Advanced Routing und Forwarding) mit bis zu 2 Kontexten
<b>IPv4-Dienste</b>	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
<b>IPv6-Dienste</b>	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
<b>Dynamische Routing-Protokolle</b>	RIPv2
<b>IPv4-Protokolle</b>	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, PPPoE (Server), RADIUS, RADSEC (Secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3
<b>IPv6-Protokolle</b>	NDP, Stateless Address Autoconfiguration (SLAAC), Stateful Address Autoconfiguration (mit DHCPv6), Router Advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, Syslog, SNMPv1,v2c,v3, MLDv2, NPTv6 (NAT66), VRRPv3
<b>WAN-Betriebsarten</b>	VDSL, ADSL1, ADSL2 oder ADSL2+ mit externem Modem an einem ETH-Port (auch simultan zum LAN-Betrieb)
<b>WAN-Protokolle</b>	PPPoE, Multi-PPPoE, GRE, PPTP (PAC oder PNS), L2TPv2 (LAC oder LNS), L2TPv3 mit Ethernet-Pseudowire und 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)
<b>Tunnelprotokolle (IPv4/IPv6)</b>	6to4, 6in4, 6rd, Dual Stack Lite, 464XLAT
Sicherheit	
<b>Intrusion Prevention</b>	Überwachung und Sperrung von Login-Versuchen und Portscans
<b>IP-Spoofing</b>	Überprüfung der Quell-IP-Adressen auf allen Interfaces: nur die IP-Adressen des zuvor definierten IP-Netzes werden akzeptiert
<b>Access-Control-Listen</b>	Filterung anhand von IP- oder MAC-Adresse sowie zuvor definierten Protokollen für den Konfigurationszugang
<b>Denial-of-Service Protection</b>	Schutz vor Fragmentierungsfehlern und SYN-Flooding
<b>Allgemein</b>	Detailliert einstellbares Verhalten bzgl. Re-Assemblierung, Session-Recovery, PING, Stealth-Mode und AUTH-Port-Behandlung
<b>Passwortschutz</b>	Passwortgeschützter Konfigurationszugang für jedes Interface einstellbar

# R&S® LANCOM 1650E

Sicherheit	
<b>Zwei-Faktor-Authentifizierung</b>	Zwei-Faktor-Authentifizierung (2FA) für das lokale Gerätemanagement über WEBconfig, SSH und Telnet mit externer Authenticator-App
<b>Alarmierung</b>	Alarmierung durch E-Mail, SNMP-Traps und SYSLOG
<b>Authentifizierungsmechanismen</b>	PAP, CHAP, MS-CHAP und MS-CHAP v2 als PPP-Authentifizierungsmechanismen
<b>Programmierbarer Reset-Taster</b>	Einstellbarer Reset-Taster für "ignore", "boot-only" und "reset-or-boot"
Hochverfügbarkeit / Redundanz	
<b>VRRP</b>	VRRP (Virtual Router Redundancy Protocol VRRPv2 und VRRPv3) zur herstellerübergreifenden Absicherung gegen Geräte- oder Gegenstellenausfall.
<b>FirmSafe</b>	Für absolut sichere Software-Upgrades durch zwei speicherbare Firmware-Versionen, inkl. Testmodus bei Firmware-Updates
<b>Load-Balancing</b>	Statische und dynamische Lastverteilung auf bis zu 2 WAN-Strecken; Kanalbündlung durch Multilink-PPP (sofern vom Netzbetreiber unterstützt)
<b>VPN-Redundanz</b>	Backup von VPN-Verbindungen über verschiedene Hierarchie-Stufen hinweg, z.B. bei Wegfall eines zentralen VPN-Konzentrators und Ausweichen auf mehrere verteilte Gegenstellen. Beliebige Anzahl an Definitionen für VPN-Gegenstellen in der Konfiguration (Tunnel-Limit gilt nur für aktive Verbindungen). Bis zu 32 alternative Gegenstellen mit jeweils eigenem Routing-Tag als Backup oder zur Lastverteilung pro VPN-Gegenstelle. Die automatische Auswahl kann der Reihe nach, aufgrund der letzten erfolgreichen Verbindung oder zufällig (VPN-Load-Balancing) erfolgen
<b>Leistungsüberwachung</b>	Leistungsüberwachung mit LCP Echo Monitoring, Dead Peer Detection und bis zu 4 Adressen für Ende-zu-Ende-Überwachung mit ICMP-Polling
VPN	
<b>IPSec over HTTPS</b>	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
<b>Anzahl der VPN-Tunnel</b>	3 Tunnel gleichzeitig aktiv bei Kombination von WireGuard- oder IPSec- mit PPTP-(MPPE) und L2TPv2-Tunneln, unbegrenzte Anzahl konfigurierbarer Gegenstellen.
<b>Hardware-Beschleuniger</b>	Integrierter Hardwarebeschleuniger für die 3DES/AES-Ver- und -Entschlüsselung
<b>Echtzeituhr</b>	Integrierte, gepufferte Echtzeituhr zur Speicherung der Uhrzeit bei Stromausfällen, sodass die zeitliche Validierung der Gültigkeit von Zertifikaten immer möglich ist
<b>Zufallszahlen-Generator</b>	Erzeugung echter Zufallszahlen in Hardware, z. B. zur Verbesserung der Generierung von Schlüsseln für Zertifikate direkt nach dem Einschalten
<b>1-Click-VPN Client-Assistent</b>	Erstellung von VPN-Client-Zugängen mit gleichzeitiger Erzeugung von Profilen für den R&S® LANCOM Advanced VPN Client mit einem Klick aus LANconfig heraus
<b>1-Click-VPN Site-to-Site</b>	Erzeugen von VPN-Verbindungen zwischen R&S® LANCOM-Routern per "Drag and Drop" mit einem Klick in LANconfig
<b>IKE, IKEv2</b>	IPSec-Schlüsselaustausch über Preshared Key oder Zertifikate (RSA-Signature, ECDSA-Signature, Digital-Signature)
<b>Zertifikate</b>	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.
<b>Zertifikatsrollout</b>	Automatisierte Erzeugung sowie Rollout und Verlängerung von Zertifikaten mit SCEP (Simple Certificate Enrollment Protocol) pro Zertifikatshierarchie
<b>Certificate Revocation Lists (CRL)</b>	Abruf von CRLs mittels HTTP pro Zertifikatshierarchie
<b>OCSP Client</b>	Prüfen von X.509-Zertifikaten anhand von OCSP (Online Certificate Status Protocol), in Echtzeit arbeitende Alternative zu CRLs
<b>XAUTH</b>	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
<b>RAS User Template</b>	Konfiguration aller VPN-Client-Verbindungen im IKE-Config-Mode über einen einzigen Konfigurationseintrag

# R&S® LANCOM 1650E

VPN	
<b>Proadaptive VPN</b>	Automatisierte Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routing-Einträge anhand eines Default-Eintrags bei Site-to-Site Verbindungen.
<b>Algorithmen</b>	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
<b>Post-Quantum-Sicherheit</b>	Post-quantum Preshared Keys (PPK) für IKEv2
<b>NAT-Traversal</b>	Unterstützung von NAT-Traversal (NAT-T) für den VPN-Einsatz auf Strecken, die kein VPN-Passthrough unterstützen
<b>MOBIKE</b>	IKEv2 VPN-Clients können nahtlos zwischen verschiedenen Netzwerken wechseln (z. B. von WLAN zu Mobilfunk), ohne den VPN-Tunnel neu aufbauen zu müssen
<b>WireGuard</b>	Unterstützung von WireGuard
<b>R&amp;S® LANCOM Dynamic VPN</b>	Ermöglicht den VPN-Verbindungsaufbau von oder zu dynamischen IP-Adressen. Die IP-Adresse wird verschlüsselt mittels ICMP- oder UDP-Protokoll übertragen. Dynamische Einwahl von Gegenstellen mittels Verbindungs-Template
<b>Dynamic DNS</b>	Ermöglicht die Registrierung der IP-Adresse bei einem Dynamic-DNS-Provider, falls keine feste IP-Adresse für den VPN-Verbindungsaufbau verwendet wird
<b>Spezifisches DNS-Forwarding</b>	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
<b>Split-DNS</b>	Ermöglicht für IKEv2 das selektive Weiterleiten von Datenverkehr abhängig von der angesprochenen DNS-Domäne.
<b>IPv4 VPN</b>	Kopplung von IPv4 Netzwerken
<b>IPv4 VPN über IPv6 WAN</b>	Nutzung von IPv4 VPN über IPv6 WAN-Verbindungen
<b>IPv6 VPN</b>	Kopplung von IPv6 Netzwerken
<b>IPv6 VPN über IPv4 WAN</b>	Nutzung von IPv6 VPN über IPv4 WAN-Verbindungen
<b>RADIUS</b>	RADIUS Authorization und Accounting, Auslagerung von VPN-Konfigurationen in externem RADIUS-Server bei IKEv2, RADIUS CoA (Change of Authorization)
<b>High Scalability VPN (HSVPN)</b>	Übertragung von mehreren, sicher getrennten Netzen innerhalb eines VPN-Tunnels
<b>Advanced Mesh VPN</b>	Dynamischer VPN-Tunnelaufbau zwischen beliebigen Filialen bei Bedarf
Performance	
<b>Routing-Performance</b>	Daten zur Routing-Performance finden Sie im R&S® NC Techpaper "Routing-Performance" <a href="#">hier</a> .
VoIP	
<b>SIP ALG</b>	SIP ALG (Application Layer Gateway) agiert als Proxy für SIP. Automatische Öffnung der notwendigen Ports für Sprachdaten. Automatische Adressumsetzung (STUN unnötig).
Schnittstellen	
<b>WAN: Ethernet</b>	10/100/1000 MBit/s Gigabit Ethernet
<b>Ethernet Ports</b>	3 individuelle Ports, 10/100/1000 MBit/s Gigabit Ethernet, im Auslieferungszustand als Switch geschaltet. Ein Port kann als zusätzlicher WAN-Port geschaltet werden. Ethernet-Ports können in der LCOS-Konfiguration elektrisch deaktiviert werden. Die Ports unterstützen Energiesparfunktionen nach IEEE 802.3az
<b>Port-Konfiguration</b>	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
<b>USB 2.0 Host-Port</b>	USB 2.0 Hi-Speed Host-Port zum Anschluss von USB-Druckern (USB-Druck-Server), USB-Datenträgern (FAT Dateisystem); bidirektionaler Datenaustausch möglich
<b>Serielle Schnittstelle</b>	Serielle Konfigurationsschnittstelle / COM-Port (USB-C): 9.600-115.000 Bit/s.

# R&S® LANCOM 1650E

Management und Monitoring	
<b>Management</b>	R&S®LANCOM Management Cloud, LANconfig, WEBconfig, R&S®LANCOM Layer 2 Management (Notfall-Management)
<b>Management-Funktionen</b>	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
<b>FirmSafe</b>	Zwei speicherbare Firmware-Versionen im Gerät, inkl. Testmodus bei Firmware-Updates
<b>Automatisches Firmware-Update</b>	Konfigurierbare automatische Prüfung und Installation von Firmware-Updates
<b>Monitoring</b>	R&S®LANCOM Management Cloud, LANmonitor, WLANmonitor
<b>Monitoring-Funktionen</b>	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
<b>Monitoring-Statistiken</b>	Umfangreiche Ethernet-, IP- und DNS-Statistiken, SYSLOG-Fehlerzähler, Accounting inkl. Export von Accounting-Informationen über LANmonitor und SYSLOG
<b>IPerf</b>	IPerf ermöglicht es den Datendurchsatz von IP-Netzwerken zu testen (integrierter Client und Server)
<b>SLA-Monitor (ICMP)</b>	Performance-Überwachung von Verbindungen
<b>Netflow</b>	Export von Informationen über eingehenden bzw. ausgehenden IP-Datenverkehr
<b>SD-LAN</b>	SD-LAN - Automatische LAN-Konfiguration über die R&S®LANCOM Management Cloud
<b>SD-WAN</b>	SD-WAN - Automatische WAN-Konfiguration über die R&S®LANCOM Management Cloud
Hardware	
<b>Gewicht</b>	450 g
<b>Umgebung</b>	Temperaturbereich 0–40° C; Luftfeuchtigkeit 0–95%; nicht kondensierend
<b>Gehäuse</b>	Robustes Kunststoffgehäuse, Anschlüsse auf der Rückseite, für Wandmontage vorbereitet, Kensington-Lock; Maße 210 x 45 x 140 mm (B x H x T)
<b>Anzahl Lüfter</b>	Keine; lüfterloses Design ohne rotierende Teile, hohe MTBF
<b>Abwärme (max.)</b>	48 BTU/h
<b>Leistungsaufnahme (max./Idle)</b>	12 Watt / 6 Watt
Konformitätserklärungen*	
<b>Europa/EFTA</b>	CE
<b>Herkunftsland</b>	Made in Germany
<b>*) Hinweis</b>	Der vollständige Text der jeweiligen Konformitätserklärung ist <a href="#">hier</a> verfügbar.
Lieferumfang	
<b>Handbuch</b>	Quick Installation Guide (DE/EN)
<b>Kabel</b>	Ethernet-Kabel, 3 m
<b>Netzteil</b>	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
Support	
<b>Gewährleistungsverlängerung</b>	Kostenfreie Gewährleistungsverlängerung auf 3 Jahre (Austausch-Service bei Defekt) Details finden Sie hier: <a href="#">Link</a> . Es finden die Service- und Supportbedingungen mit Stand vom 01.07.2026, abrufbar unter <a href="https://rs-nc.rohde-schwarz.com/fileadmin/pdf/LCS/ServiceSupportConditions/Rohde-Schwarz-Networks-and-Cybersecurity-GmbH-Service-und-Supportbedingungen-20260701.pdf">rs-nc.rohde-schwarz.com/fileadmin/pdf/LCS/ServiceSupportConditions/Rohde-Schwarz-Networks-and-Cybersecurity-GmbH-Service-und-Supportbedingungen-20260701.pdf</a> , Anwendung.
<b>Security Updates</b>	Bis 2 Jahre nach End of Sale des Gerätes (aber min. 3 Jahre, siehe <a href="#">Link</a> ), verlängerbar mit R&S®NC Support-Produkten

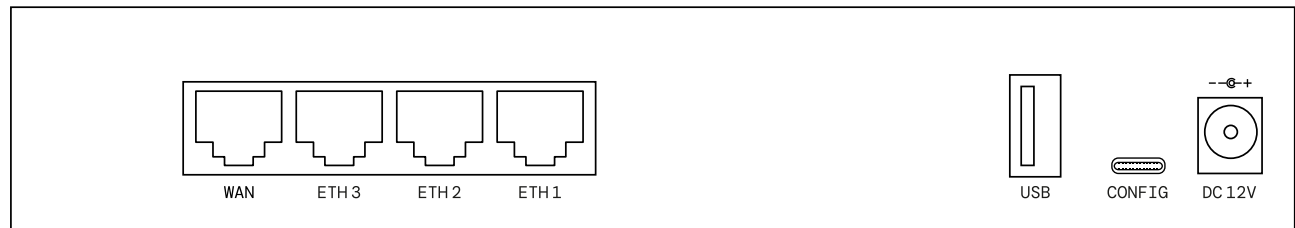
# R&S® LANCOM 1650E

Support	
<b>Software Updates</b>	Regelmäßig kostenfreie Updates inkl. neuer Features im Rahmen des R&S®NC Lifecycle Managements ( <a href="#">Link</a> )
<b>Angaben zum EU Data Act</b>	Details zu Produktdaten und Daten verbundener Dienste finden Sie unter: <a href="#">Link</a>
<b>Hersteller-Support</b>	Erhältlich mit R&S®NC-Produkten wie Support Access (nur für R&S®NC Community Partner), Direct oder Premium
<b>R&amp;S®NC Replacement Basic S</b>	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
<b>R&amp;S®NC Replacement Advanced S</b>	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
<b>R&amp;S®NC Support Direct 24/7 S</b>	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)
<b>R&amp;S®NC Support Direct Advanced 24/7 S</b>	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)
<b>R&amp;S®NC Support Direct 10/5 S</b>	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)
<b>R&amp;S®NC Support Direct Advanced 10/5 S</b>	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	
<b>Lifecycle Management</b>	Das Gerät unterliegt nach der Abkündigung (End of Sale) dem R&S®NC Lifecycle Management. Details dazu finden Sie unter: <a href="#">Link</a>
<b>IT-Security made in Germany</b>	Die Entwicklung und Qualitätssicherung erfolgen in Deutschland nach hohen Sicherheitsstandards. Das Qualitätszeichen „IT-Security made in Germany“ des Bundesverbands IT-Sicherheit belegt das erreichte Sicherheitsniveau.
Optionen	
<b>R&amp;S®LANCOM Security Essentials</b>	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
<b>R&amp;S®LANCOM Security Essentials</b>	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
<b>R&amp;S®LANCOM Security Essentials</b>	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
<b>R&amp;S®LANCOM BPjM Filter</b>	R&S®LANCOM BPjM Filter Option, 5 Jahre Laufzeit, Art.-Nr. 61418
<b>R&amp;S®LANCOM All-IP Lizenz Option</b>	Upgrade-Option zur Nutzung der R&S®LANCOM Router an All-IP-Anschlüssen, Unterstützung von TK-Anlagen und Telefoniegeräten sowie Sprach- & Faxdiensten, inkl. Voice Call Manager, Art.-Nr. 61419
<b>R&amp;S®LANCOM VoIP +10 Option</b>	Upgrade von R&S®LANCOM VoIP-Routern für 10 zusätzliche interne VoIP-Teilnehmer (additiv bis zu 40) und 10 externe SIP-Leitungen (additiv bis zu 55), Art.-Nr. 61423
R&S®LANCOM Management Cloud	
<b>R&amp;S®LANCOM Management Cloud</b>	R&S®LMC-A-1Y Lizenz (1 Jahr), ermöglicht für ein Jahr die Verwaltung eines Gerätes der Kategorie A mit der R&S®LANCOM Management Cloud, Art.-Nr. 50100
<b>R&amp;S®LANCOM Management Cloud</b>	R&S®LMC-A-3Y Lizenz (3 Jahre), ermöglicht für drei Jahre die Verwaltung eines Gerätes der Kategorie A mit der R&S®LANCOM Management Cloud, Art.-Nr. 50101
<b>R&amp;S®LANCOM Management Cloud</b>	R&S®LMC-A-5Y Lizenz (5 Jahre), ermöglicht für fünf Jahre die Verwaltung eines Gerätes der Kategorie A mit der R&S®LANCOM Management Cloud, Art.-Nr. 50102

LCOS 10.94

# R&S® LANCOM 1650E

Geeignetes Zubehör	
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Windows - 1er Lizenz Art.-Nr. 61600
VPN-Client-Software	R&S®LANCOM Advanced VPN Client für Mac OS X, 1er Lizenz, Art.-Nr. 61606
Artikelnummer(n)	
R&S®LANCOM 1650E (EU)	62163



Rohde & Schwarz Networks and Cybersecurity GmbH  
 Adenauerstr. 20/B2  
 52146 Würselen | Deutschland  
[info.rs-nc@rohde-schwarz.com](mailto:info.rs-nc@rohde-schwarz.com) | [www.rohde-schwarz.com/networks-and-cybersecurity](http://www.rohde-schwarz.com/networks-and-cybersecurity)

R&S und Rohde & Schwarz sind Marken der Rohde & Schwarz GmbH & Co. KG, die u.a. in Deutschland, EU, USA, China und weiteren Ländern eingetragen oder benutzt werden. Andere verwendete Namen oder Bezeichnungen können (registrierte) Marken von unterschiedlichen Firmen oder Inhabern sein. Dieses Dokument enthält zukunftsbezogene Aussagen zu Produkten und Produkteigenschaften. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen. 06/2026

**ROHDE & SCHWARZ**  
 Make ideas real

