## Für sichere und zukunftsfähige Netzwerke

# LCOS

# 11.00

Mit LCOS 11.00 RC1 profitieren Sie von einem wichtigen Meilenstein für die zukunftsfähige Absicherung Ihrer Netzwerke. So bereiten moderne Post-Quantum-Mechanismen beim Schlüsselaustausch IKEv2-VPN-Verbindungen bereits heute auf zukünftige Bedrohungen durch Quantencomputer vor und bieten zusätzlichen Schutz vor potenziellen Angriffen. Darüber hinaus profitieren Sie in der VoIP-Telefonie von noch mehr Ausfallsicherheit: Dank der VRRP-Unterstützung des Voice Call Managers lassen sich mit den R&S®LANCOM SD-WAN VoIP Gateways nun auch Redundanzkonzepte für eine hochverfügbare Telefonie realisieren.

- Zukunftssichere VPN-Verschlüsselung mit Post-Quantum-Kryptografie
- VRRP für hochverfügbare VoIP-Umgebungen

| Neue Features LCOS 11.00 | |
|---|---|
| Zukunftssichere VPN-Verschlüsselung mit Post-Quantum-Kryptografie | Mit diesem Update lassen sich IKEv2-VPN-Verbindungen bereits heute auf zukünftige Bedrohungen durch leistungsfähige Quantencomputer vorbereiten. Dafür setzt LCOS auf moderne Post-Quantum-Mechanismen beim Schlüsselaustausch. Klassische Verschlüsselungsverfahren können mit dem quantenresistenten Verfahren ML-KEM kombiniert werden. So entsteht ein hybrider Ansatz, der etablierte Sicherheitsmechanismen mit zusätzlichem Schutz für die Zukunft verbindet. Verfügbar sind die ML-KEM-Gruppen DH35, DH36 und DH37. |
| VRRP für hochverfügbare VoIP-Umgebungen | Um die Ausfallsicherheit von Telefonie-Infrastrukturen zu erhöhen lässt sich nun auch der Voice Call Manager in R&S®LANCOM SD-WAN VoIP Gateways über VRRP (Virtual Router Redundancy Protocol) redundant betreiben. Mehrere physische R&S®LANCOM SD-WAN VoIP Gateways treten dabei als ein gemeinsames virtuelles Gateway auf, sodass ein Standby-Gerät bei Ausfall des aktiven Geräts die Netzwerkkommunikation übernehmen kann. Der Voice Call Manager wird dazu gezielt an das entsprechende virtuelle Netzwerk gebunden. SIP-Endgeräte registrieren sich über die virtuelle IP-Adresse des Gateways und können sich nach einem Wechsel auf das neue Master-Gerät erneut anmelden. So werden Telefonie-Funktionen auch bei einer Störung schnell wieder verfügbar. |

| Neue Features LCOS 10.94 | |
|---|---|
| eSIM: Die clevere Mobilfunklösung direkt im R&S®LANCOM Router | Mit der integrierten eSIM-Technologie verbinden sich R&S®LANCOM SD-WAN Gateways ganz unkompliziert mit dem Mobilfunknetz. Statt physischer SIM-Karten, die verwaltet und manuell ausgetauscht werden müssen, lassen sich Mobilfunkverträge und -profile einrichten und managen. Die fest im Gerät verbaute eSIM (Consumer-Variante) wird per Software mit dem Profil des Mobilfunkanbieters programmiert. So können Verträge oder Tarife schnell digital aufgespielt, gewechselt, aktualisiert und verwaltet werden – ganz ohne aufwändigen Kartenwechsel oder kostenintensive Vor-Ort-Einsätze. Neue Geräte sind sofort einsatzbereit; Rollouts an verschiedenen Standorten oder für viele Geräte lassen sich in kürzester Zeit durchführen. Gleichzeitig steigt die Sicherheit, da keine Karten verloren gehen oder missbräuchlich genutzt werden können. Ob für mobile Arbeitsplätze, Filialnetze oder als Backup-Lösung – eSIM ermöglicht die einfache Verwaltung der Mobilfunk-Konnektivität und bietet dabei ein Maximum an Flexibilität und Zeitersparnis. |
| WireGuard | Gerade in kleinen und überschaubaren Vernetzungsszenarien – etwa im Homeoffice oder in Unternehmen mit nur wenigen VPN-Anbindungen – bietet die Unterstützung von WireGuard eine schnell eingerichtete und zugleich flexible Lösung für eine sichere VPN-Verbindung. Dank seiner klaren Struktur und intuitiven Handhabung bietet das moderne Protokoll eine sichere und gleichzeitig unkomplizierte Lösung für einfache Vernetzungsszenarien. Moderne Kryptografie-Algorithmen sorgen dabei für eine zuverlässige Absicherung. WireGuard ermöglicht einen breiten Einsatz auf allen gängigen Betriebssystemen – ideal für heterogene IT-Umgebungen. |
| Zwei-Faktor-Authentifizierung (2FA) | Mit der neuen Zwei-Faktor-Authentifizierung (2FA) wird das lokale Gerätemanagement unter LCOS nochmals deutlich sicherer. Neben der gewohnten Passworteingabe kann künftig ein zusätzlicher Sicherheitscode angefordert werden, der bequem über eine gängige Authenticator-App generiert wird. So bleibt der Zugriff selbst dann zuverlässig geschützt, wenn Ihr Passwort in falsche Hände geraten sollte. Die Einrichtung erfolgt unkompliziert mit Standard-Apps und bietet zusätzlich wirksamen Schutz vor Brute-Force-Attacken. Auf diese Weise erhöhen Sie Ihre Sicherheitsstandards, indem unerwünschte Gerätezugriffe abgewehrt werden. |
| | Unterstützung von Hybrid-Post-Quantum-Verfahren: Erweiterung der Verschlüsselung im Gerätemanagement (SSH und TLS) |
| | Mit den Software-Optionen WLC Basic und WLC Upgrade kann der R&S®LANCOM 2100EF nun bis zu 60 Access Points verwalten. |
| | Erweiterte Konfigurationsmöglichkeiten von Wi-Fi 7 Access Points über R&S®LANCOM WLAN-Controller |
| | Vollständig transparente Datenweiterleitung von Mobilfunkverbindungen dank Unterstützung des WWAN-Bridge-Mode |
| **Neue Features LCOS 10.92** | |
| Netzwerksicherheit aus der Cloud mit der R&S®LANCOM Security Essentials Option | Mit LCOS 10.92 erfüllen Sie alle Voraussetzungen, um Ihre Geräte mit der R&S®LANCOM Security Essentials Option aufzurüsten. Die R&S®LANCOM Security Essentials Option bietet eine effiziente und zuverlässige Lösung, um Netzwerke vor Bedrohungen wie Ransomware, Phishing, Malware oder Diebstahl von Zugangsdaten zu schützen. Durch den integrierten Content Filter werden unerwünschte und illegale Internetinhalte gezielt blockiert – so bleibt die Integrität des Unternehmens gewahrt und das Haftungsrisiko wird deutlich reduziert. Gleichzeitig schützt das BPjM-Modul der Bundeszentrale für Kinder- und Jugendmedien-schutz (BzKJ) Minderjährige zuverlässig vor jugendgefährdenden Inhalten. Die zugrunde liegende Datenbank zur Überprüfung der Webseiteninhalte wird DSGVO-konform in einer vertrauenswürdigen Cloud des europäischen Security-Spezialisten Bitdefender gehostet. Für beste Skalierbarkeit ist die Nutzung der Option nicht auf eine bestimmte Nutzeranzahl begrenzt – ideal für wachsende Netzwerke.<br><br>**Hinweis:** Die R&S®LANCOM Security Essentials Option ist als Upgrade-Option für R&S®LANCOM SD-WAN Gateways, SD-WAN Central Site Gateways und WLAN-Controller verfügbar und das Nachfolgeprodukt des R&S®LANCOM Content Filter. |
| **Neue Features LCOS 10.90** | |
| Sicherstellung geschäftskritischer Anwendungen dank Unterstützung von acht QoS-Queues | Dieses Feature ermöglicht es Ihnen, bis zu acht verschiedene Queues (Serviceklassen) mit entsprechenden Prioritätsstufen für Anwendungen im Netzwerk festzulegen (z. B. „VoIP", „Gold", „Silber" oder „Best Effort"). Ihre Datenpakete werden mithilfe von DSCP-Markierungen oder durch Firewallregeln der entsprechenden Quality of Service (QoS)-Klasse zugeordnet. Das Gateway sortiert anschließend die Pakete in die richtige Prioritätsstufe und stellt sicher, dass die entsprechenden Dienste nur so viel Upload-Bandbreite nutzen, wie für ihre Klasse zuvor von Ihnen in Prozent oder MBit/s konfiguriert wurde. Auf diese Weise wird sichergestellt, dass wichtige Dienste wie VoIP oder Videoanrufe stets ausreichend Bandbreite erhalten, selbst bei hoher Netzwerkauslastung. |
| MOBIKE im VPN für einen beschleunigten Netzwerkwechsel | Mit der MOBIKE-Erweiterung für IKEv2 können VPN-Clients nahtlos zwischen verschiedenen Netzwerken wechseln (z. B. von WLAN zu Mobilfunk), ohne den VPN-Tunnel neu aufbauen zu müssen. Der R&S®LANCOM Advanced VPN Client oder R&S®LANCOM Trusted Access Client sendet beim Netzwechsel eine Aktualisierungsnachricht mit seiner neuen IP-Adresse an das SD-WAN-Gateway. Für Sie bedeutet das: Keine Unterbrechung beim VPN-Roaming, die Verbindung bleibt stabil. |
| Proaktiv gegen Quantencomputer: Zukunftssichere VPNs mit Post-Quantum Preshared Keys | Die fortschreitende Entwicklung von Quantencomputern stellt traditionelle Verschlüsselungstechnologien wie VPNs vor grundlegende Herausforderungen. Umso wichtiger ist es, sich darauf vorzubereiten. Mit Post-Quantum Preshared Keys (PQ-PSK oder PPK) für IKEv2 ergreifen Sie erste Sicherheitsmaßnahmen. Diese Technologie fügt zusätzliche Schutzmechanismen hinzu, um die Verschlüsselung von VPNs schon jetzt gegen potenzielle Angriffe durch Quantencomputer zu sichern.<br>Darüber hinaus werden wir Ihnen in zukünftigen LCOS-Versionen sukzessive weiterer Funktionen zur Absicherung Ihrer Netzwerke zur Verfügung stellen, sodass Sie vollumfänglich geschützt sind – selbst wenn Quantencomputer in der Lage sein sollten, traditionelle Verschlüsselungsmethoden zu brechen. |
| Höchste Ausfallsicherheit mit VRRPv3 für Dual-Stack-Netzwerke | VRRPv3 für IPv6 ermöglicht es Ihnen, Router-Redundanz auch in Netzwerken mit IPv6 oder in Dual-Stack-Umgebungen (gleichzeitige Nutzung von IPv4 und IPv6) zu implementieren. Dies erhöht die Betriebssicherheit, da bei einem Ausfall eines Routers ein anderer automatisch die Funktion übernehmen kann. Diese Funktion ist ideal für moderne Netzwerke, die sowohl IPv4 als auch IPv6 unterstützen, da sie eine nahtlose Redundanz in beiden Protokollen gewährleistet. |
| | Mit LCOS 10.90 kann der Router im LAN dynamisch VLANs per RADIUS an IEEE 802.1X-Clients zuweisen. Eine aufwendige physische Infrastruktur, wie dedizierte Switches, wird nicht benötigt, um eine VLAN-Trennung und -Zuordnung durchzuführen. Da der Router die gesamte LAN-Sicherheitsstruktur übernimmt, ist dieses Feature ideal für kleine Standorte. |
| | Viele weitere Verbesserungen für die Administration und den Betrieb moderner Netzwerke |

| Neue Features LCOS 10.80 | |
|---|---|
| Unterstützung des R&S®LANCOM Trusted Access Client | Der R&S®LANCOM Trusted Access Client ist die vertrauenswürdige Network Access Security-Lösung für Unternehmensnetzwerke. Er ermöglicht einen sicheren und skalierenden Zugriff auf Unternehmensanwendungen für Mitarbeitende im Büro, zu Hause oder unterwegs und schützt damit modernes hybrides Arbeiten von überall und jederzeit. Die R&S®LANCOM Trusted Access-Lösung passt sich an steigende Sicherheitsanforderungen in Ihrer Organisation an und ermöglicht sowohl Cloud-managed VPN-Client-Vernetzung für den Zugriff auf ganze Netze als auch den Umstieg auf eine Zero-Trust-Sicherheitsarchitektur für eine umfassende Netzwerksicherheit. Dabei erhalten Benutzer auf Basis granularer Zugriffsrechte ausschließlich Zugangsberechtigung auf Anwendungen, die ihnen zugewiesen wurden (Zero-Trust-Prinzip). Bestehende Systeme zur Verwaltung von Benutzern und Benutzergruppen (Active Directory) lassen sich vollständig in die R&S®LANCOM Management Cloud (LMC) integrieren. Für kleinere Netzwerke bietet die LMC alternativ eine interne Benutzerverwaltung. R&S®LANCOM Trusted Access 100% DSGVO-konform und skaliert für Kleinunternehmen genauso wie für sehr große Netzwerke mit mehreren tausend Benutzern. |
| Let's Encrypt für WEBconfig und den R&S®LANCOM Public Spot | Let's Encrypt ist eine Zertifizierungsstelle, die kostenlose HTTPS-Zertifikate anbietet, um verschlüsselte Verbindungen zu standardisieren. WEBconfig und auch der R&S®LANCOM Public Spot unterstützen nun Let's Encrypt. So lassen sich mit wenigen einmaligen und einfachen Handgriffen kostenlose und vertrauenswürdige Zertifikate erstellen, über das Gateway einbinden und automatisch verlängern. |
| Zero-touch Rollout für Mobilfunk-Router | Mit der Unterstützung von Zero-touch ist die Einrichtung von R&S®LANCOM Mobilfunk-Routern nun noch einfacher und schneller. Wo zuvor eine manuelle Konfiguration des Mobilfunk-Zugangspunktes erforderlich war, genügt nun das Einsetzen einer PIN-freien SIM-Karte in das Gerät. Zero-touch Rollout ermöglicht eine automatische Verbindung mit dem Internet und darauf folgend mit der R&S®LANCOM Management Cloud, um die passende Konfiguration des Gateways abzurufen. |
| R&S®LANCOM vRouter über Google Cloud verfügbar | Mit LCOS 10.80 betreiben Sie den R&S®LANCOM vRouter auf Wunsch nun auch mit dem Cloud-Computing-Anbieter Google Cloud. So können Sie neben Microsoft Azure, VMware ESXi, Hyper-V und AWS nun auch Google Cloud nutzen, um die eigene Infrastruktur in die Cloud zu verlagern. Der R&S®LANCOM vRouter garantiert dabei die sichere Anbindung und übernimmt die verschlüsselte Kommunikation zwischen Ihrem Standort und Ihrer virtualisierten Infrastruktur in der Google Cloud. Darüber hinaus ist auch die Virtualisierung von Zentralen möglich: Der vRouter in der Google Cloud ersetzt ganz einfach das zentralseitige Hardware-Gateway. |
| WEBconfig im neuen Corporate Design | Managen Sie Ihre Geräte über den Webbrowser, stellt Rohde & Schwarz Networks and Cybersecurity Ihnen über WEBconfig eine grafische Benutzeroberfläche bereit, die direkt in das LCOS integriert ist und ab sofort in neuem Anstrich mit modernem Design und maximaler Übersichtlichkeit glänzt. |
| | R&S®LANCOM High Availability Clustering Option L für die 1900er-Serie |
| | Router können Traces und Wireshark-Captures direkt auf einem USB-Stick aufzeichnen und speichern. |
| | Einträge in der Aktionstabelle können durch ein CLI-Kommando getestet bzw. ausgeführt werden. |
| **Neue Features LCOS 10.72** | |
| Advanced Mesh VPN | Bei klassischen, sternförmigen VPN-Standortvernetzungen, in denen alle Filialen lediglich über die Zentrale und nicht direkt untereinander verbunden sind, wird die Internetleitung der Zentrale schnell zum Flaschenhals der gesamten Kommunikation. Mit Advanced Mesh VPN kommunizieren die Zweigstellen nun auf direktem Weg miteinander und sorgen so in der Zentrale für deutlich weniger Traffic und einhergehend für höhere Performance. Die VPN-Tunnel werden hierbei bei Bedarf dynamisch aufgebaut, sobald Datentraffic von einer zur anderen Filiale transportiert wird. Findet keine Kommunikation mehr statt, wird die VPN-Verbindung ebenso dynamisch wieder abgebaut. |
| Jugendschutz nach BPjM-Vorgaben | Mit LCOS 10.72 Rel maximieren Sie jetzt den Schutz von minderjährigen Nutzern z. B. in Schulen oder Jugendeinrichtungen. So ist die offizielle Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) nun auch Teil der R&S®LANCOM Content Filter Option oder separat über die Software-Erweiterung R&S®LANCOM BPjM Filter Option erhältlich. Damit sind URLs, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine stetige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet. |
| Zwei-Faktor-Authentifizierung – Doppelte Sicherheit für Ihr VPN | Immer dann, wenn ein hohes Sicherheitslevel für Ihre sensiblen Daten erforderlich ist oder z. B. auch Compliance-Richtlininen in Ihrem Unternehmen es vorsehen, ist die doppelte Absicherung des Netzwerk-Zugangs über den R&S®LANCOM Advanced VPN Client ideal. Dank Zwei-Faktor-Authentifizierung (IKEv2 EAP-OTP) schützen Sie jetzt den VPN-Zugang und damit auch Ihr Netzwerk vor unbefugten Zugriffen. So kann festgelegt werden, dass sich User ausschließlich über den R&S®LANCOM Advanced VPN Client einwählen können, sofern sie beim Login die Zwei-Faktor-Authentifizierung nutzen. Hierbei wird das VPN-Passwort um ein zeitbasiertes Einmalpasswort ergänzt, welches in einer Authentifizierungs-App (z.B. Google Authenticator) auf dem Mobiltelefon generiert werden kann. Nutzbar ist dieses Feature mit allen Geräten, die mindestens 25 VPN-Tunnel besitzen (entweder bereits integriert oder aber mit R&S®LANCOM VPN Option aufgerüstet). |
| **Neue Features LCOS 10.70** | |
| Advanced Mesh VPN | Bei klassischen, sternförmigen VPN-Standortvernetzungen, in denen alle Filialen lediglich über die Zentrale und nicht direkt untereinander verbunden sind, wird die Internetleitung der Zentrale schnell zum Flaschenhals der gesamten Kommunikation. Mit Advanced Mesh VPN kommunizieren die Zweigstellen nun auf direktem Weg miteinander und sorgen so in der Zentrale für deutlich weniger Traffic und einhergehend für höhere Performance. Die VPN-Tunnel werden hierbei bei Bedarf dynamisch aufgebaut, sobald Datentraffic von einer zur anderen Filiale transportiert wird. Findet keine Kommunikation mehr statt, wird die VPN-Verbindung ebenso dynamisch wieder abgebaut. |
| Jugendschutz nach BPjM-Vorgaben | Mit LCOS 10.70 RC2 maximieren Sie jetzt den Schutz von minderjährigen Nutzern z. B. in Schulen oder Jugendeinrichtungen. So ist die offizielle Webseiten-Liste der Bundesprüfstelle für jugendgefährdende Medien (BPjM) nun auch Teil der R&S®LANCOM Content Filter Option oder separat über die Software-Erweiterung R&S®LANCOM BPjM Filter Option erhältlich. Damit sind URLs, deren Inhalte offiziell als jugendgefährdend eingestuft werden, für die entsprechende Zielgruppe in Deutschland nicht erreichbar. Eine stetige Aktualisierung und Erweiterung dieser Auflistung ist dabei gewährleistet. |
| Zwei-Faktor-Authentifizierung – Doppelte Sicherheit für Ihr VPN | Immer dann, wenn ein hohes Sicherheitslevel für Ihre sensiblen Daten erforderlich ist oder z. B. auch Compliance-Richtlininen in Ihrem Unternehmen es vorsehen, ist die doppelte Absicherung des Netzwerk-Zugangs über den R&S®LANCOM Advanced VPN Client ideal. Dank Zwei-Faktor-Authentifizierung (IKEv2 EAP-OTP) schützen Sie jetzt den VPN-Zugang und damit auch Ihr Netzwerk vor unbefugten Zugriffen. So kann festgelegt werden, dass sich User ausschließlich über den R&S®LANCOM Advanced VPN Client einwählen können, sofern sie beim Login die Zwei-Faktor-Authentifizierung nutzen. Hierbei wird das VPN-Passwort um ein zeitbasiertes Einmalpasswort ergänzt, welches in einer Authentifizierungs-App (z.B. Google Authenticator) auf dem Mobiltelefon generiert werden kann. Nutzbar ist dieses Feature mit allen Geräten, die mindestens 25 VPN-Tunnel besitzen (entweder bereits integriert oder aber mit R&S®LANCOM VPN Option aufgerüstet). |

| Neue Features LCOS 10.50 | |
|---|---|
| Performance-Upgrade für den R&S®LANCOM ISG-8000 | In großen SD-WAN- oder Standortvernetzungsszenarien mit einer Vielzahl an IPSec-VPN-Kanälen und hohem Datenaufkommen ist der Einsatz des Central Site VPN-Gateways R&S®LANCOM ISG-8000 nun noch effizienter. Durch die intelligente Verteilung der Datenlast auf mehrere Kerne (Multicore) wird die Gesamtperformance der VPN-Verbindungen auf 10 GBit/s erhöht. So können bei der Nutzung vieler VPN-Kanäle deutlich mehr Daten in kürzerer Zeit ausgetauscht werden. |
| Schnelles Failover für höchste Betriebssicherheit | In Infrastrukturen mit Anforderungen an höchste Betriebssicherheit sind schnelle Failover-Zeiten essenziell wichtig. Bei Einsatz von Dynamic Path Selection (DPS) oder BGP gelingt das Umschalten von einer IPSec-VPN-Verbindung zur anderen nun in weniger als einer Sekunde. Somit führt in einem Active-Active-Betrieb der Ausfall einer Verbindung zu keiner merklichen Downtime, beispielsweise bei geschäftskritischen Prozessen wie Zahlungsvorgängen mit EC-Cash-Terminals. |
| Erweiterung der IPv6-Funktionalität | Profitieren Sie jetzt von noch mehr Zukunftsfähigkeit Ihrer IPv6-Standortvernetzung: Ab LCOS 10.50 werden Funktionen wie 464XLAT bei IPv6-only im Mobilfunk, NAT bei IPv6 (NPTv6), Load Balancing mit IPv6 sowie IPv6-Polling unterstützt. |
| Plattformerweiterung für den R&S®LANCOM vRouter | Für einen noch flexibleren Einsatz unterstützt der R&S®LANCOM vRouter neben den Hypervisor-Plattformen Hyper-V, ESXi und Azure jetzt auch KVM (Kernel-based Virtual Machine). |
| BFD | Unterstützung von Bidirectional Forwarding Detection (BFD) für BGP |
| **Neue Features LCOS 10.42** | |
| Dynamic Path Selection | Mit dem neuen Highlight-Feature Dynamic Path Selection routen Sie in Ihrem SD-WAN geschäftskritische Business-Anwendungen stets über die qualitativ beste Leitung. |
| Dynamic DNS Service für die Public Cloud | Die R&S®LANCOM Management Cloud (Public) wird zum DynDNS-Provider! Weisen Sie in den Standort-Einstellungen den dort eingesetzten Gateways einfach eine feste, selbstgewählte Domain zu (mycompany.dyndns-lmc.de). Diese Domain kann daraufhin beispielsweise in VPN-Gegenstellen wie dem R&S®LANCOM Advanced VPN Client hinterlegt werden. Somit bleiben mit der neuen LCOS 10.42 auch Gateways mit dynamischen WAN-IP-Adressen jederzeit über diesen Domain-Namen erreichbar. |
| Cloud-managed Hotspot | Erstellen Sie mit wenigen Klicks einen einfachen WLAN-Hotspot – direkt aus der LMC heraus. Ein zusätzliches Gateway oder ein WLAN-Controller mit R&S®LANCOM Public Spot Option sind hierfür nicht erforderlich. Über ein intuitiv zu bedienendes Menü individualisieren Sie Ihren Hotspot-Begrüßungsbildschirm mit Ihrem Logo sowie Ihren Unternehmensfarben und integrieren wichtige Informationen wie Impressum und Nutzungsrichtlinien für Ihre Hotspot-Benutzer. Anschließend weisen Sie das neue Hotspot-Netz den gewünschten Standorten zu und schon steht er Ihren Besuchern zur Verfügung. |
| BLE API für die Realisierung innovativer Location-based Services | Ob für die Innenraumlokalisierung von Patienten in Krankenhäusern, die Auswertung von Kundenaufkommen im Einzelhandel oder Asset Tracking im Logistik-Bereich: Für alle R&S®LANCOM Access Points mit Bluetooth Low Energy-Modul (BLE) steht nun eine neue API-Schnittstelle (REST) für die Einbindung ortsbezogener Dienste zur Verfügung. In Zusammenarbeit mit Drittanbietern ermöglicht diese die Realisierung einer Vielzahl ortsbezogener Dienste (Location-based Services, LBS) und innovativer IoT-Anwendungen. |
| 802.1X-Authenticator | Der 802.1X-Authenticator für Ethernet-Ports ist nun in allen Geräten enthalten und kann nun optional statt einer 802.1X-Verhandlung sofort eine Prüfung der MAC-Adresse des angeschlossenen Ethernet-Geräts mit einem RADIUS-Server durchführen. |
| Wireless ePaper | Für die Verbindung mit einem Wireless ePaper Server kann nun das ThinAP2.0/TLS-Protokoll verwendet werden. |
| **Neue Features LCOS 10.40** | |
| R&S®LANCOM vRouter | Erweiterung des R&S®LANCOM vRouters um die Funktionen der R&S®LANCOM High Availability Clustering Option (ab vRouter 500) und der Public Spot PMS Accounting Plus Option |
| MLD-Snooping | Unterstützung von MLD-Snooping |
| R&S®LANCOM High Scalability VPN (HSVPN) | High Scalability VPN verbessert deutlich die Skalierbarkeit und Effizienz Ihrer SD-WAN-Architektur. Wo zuvor für jede Anwendung ein einzelner VPN-Tunnel benötigt wurde, transportiert HSVPN beliebig viele Netze in einem einzigen VPN-Tunnel gesammelt an die Gegenstelle – dabei bleibt jedes Netz sicher und strikt voneinander getrennt. Der Vorteil für Ihr Business: deutlich weniger benötigte VPN-Tunnel sowie schnellere Wiederherstellungszeiten bei Failover. |
| Neue WEBconfig | Erfreuen Sie sich nun an einem ganz neuen Look & Feel in der R&S®LANCOM WEBconfig. Angelehnt an das moderne und helle Design der R&S®LANCOM Management Cloud wurde die WEBconfig komplett neu überarbeitet und bietet Ihnen eine attraktive und frische Optik. |
| Multicast Routing | Ab sofort werden Multicast-Daten, wie z. B. IPTV, effizient an verschiedenen Endgeräte übertragen. Während bislang an jeden Empfänger separate Datenpakete verschickt werden mussten, ermöglicht Multicast-Routing die parallele Übertragung eines IP-Stroms an mehrere Empfänger. Dadurch wird die Last für den Router verringert und die verfügbare Routing-Kapazität besser genutzt. Unterstützt werden PIM (Protocol Independent Multicast), IGMP-Proxy sowie MLD-Proxy. |
| SD-WAN Zero-touch Deployment für DSL-Router | Automatische Inbetriebnahme von DSL-Routern an BNG-Telekom-Anschlüssen mit der R&S®LANCOM Management Cloud – ohne die aufwändige Konfiguration von DSL-Zugangsdaten auf dem Router. |
| Netflow | Mit Netflow können Informationen zur Netzwerkanalyse über eingehenden bzw. ausgehenden IP-Datenverkehr (u.a. Quelle, Ziel, Ports) im Router an einen zentralen Server zur Auswertung gesendet werden. |
| IKEv2-VPN mit Windows-Login | Mobile VPN-Clients können jetzt mittels IKEv2 EAP gegen eine zentrale Datenbank wie Microsoft Active Directory oder RADIUS authentifiziert werden, ohne dass die VPN-Zugangsdaten auf dem R&S®LANCOM Router gespeichert werden müssen. |
| Mehr Flexibilität bei Backup-Szenarien | Die Priorisierung von Routen bietet neue Möglichkeiten für flexible Backup-Szenarien. |
| Neue SD-WAN-Funktionen für den Loadbalancer | Auf zentralseitigen Gateways können VPN-Loadbalancer durch RADIUS automatisch erzeugt werden. Zudem werden mehrere VPN-Kanäle zu Tunnel-Gruppen zusammengefasst, sodass auch im Fall eines Failovers der VPN-Aufbau zu einem gemeinsamen Gateway erfolgt. |
| WLAN-Zeitsteuerung | Ermöglicht das zeitgesteuerte Aktivieren und Deaktivieren von SSIDs im WLAN. Ideal für WLAN-Netze, die nur zu bestimmten Zeiten zur Verfügung stehen sollen, wie beispielsweise Hotspots oder WLAN in Bildungseinrichtungen. |
| Mehr Sicherheit im VPN | Unterstützung von neuen und modernen Verschlüsselungs-Algorithmen wie Chacha20-Poly 1305, Digital Signature mit ECDSA sowie neue Diffie-Hellmann-Gruppen. |
| TLS 1.3 Client Mode | Die Unterstützung des neuen Protokolls TLS 1.3 erhöht die Sicherheit beim Zugriff des Routers auf Webdienste. |
| Neue Filter für individuelle Meldungen | Konfigurierbare Filterlisten für SNMP-Traps und SYSLOG ermöglichen den Erhalt individualisierter Monitoring-Meldungen. |

| Neue Features LCOS 10.32 | |
|---|---|
| Wireless ePaper USB | Das Modul R&S®LANCOM Wireless ePaper USB erweitert USB-fähige Router, Access Points oder WLAN Controller (WLC-4006+) um Wireless ePaper Funktionalität. Damit erweitern Sie Ihre Bestandsgeräte ohne großem Aufwand um moderne Digital Signage Anwendungsmöglichkeiten. |
| ThinAP 2.0-Protokoll | Unterstützung des ThinAP 2.0-Protokolls zur Anbindung von Wireless ePaper-Access Points an einen zentralen Wireless ePaper-Server |
| **Neue Features LCOS 10.30** | |
| SD-WAN – Application Routing | Profitieren Sie von einem deutlichen Performance-Gewinn bei der Nutzung moderner Cloud-Anwendungen (z.B. Office 365, SalesForce, etc.). SD-WAN Application Routing kann Cloud-basierte Anwendungen erkennen und leitet diese direkt ins Internet (Local Break-out). Dies entlastet die VPN-Strecke zur Zentrale als auch die Internetleitung in der Zentrale. |
| SD-WAN – Layer-7-Applikationskontrolle in der Firewall | Bewahren Sie die Kontrolle über die Nutzung der Anwendungen in Ihrem Netzwerk. Durch die Definition anwendungsbezogener Regeln in der Firewall liegt es in Ihrer Entscheidung, welche Internet-Anwendungen erlaubt, gesperrt, limitiert oder priorisiert werden. |
| WLC-Funktionen im vRouter (vWLC) | Entscheiden Sie selbst und flexibel, welche Rolle Ihr R&S®LANCOM vRouter übernehmen soll: VPN-Gateway oder WLAN-Controller. Der R&S®LANCOM vRouter unterstützt ab sofort die Rolle eines virtuellen WLCs (vWLC). Damit können die WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi oder Microsoft Hyper-V virtualisiert werden. Die Anzahl verwalteter Access Points ist abhängig von der Lizenzkategorie des vRouters. |
| TLS 1.3 | Die Unterstützung des neuen Protokolls TLS 1.3 erhöht die Sicherheit beim Gerätezugriff über WEBconfig. |
| IKEv2 Elliptic Curve Digital Signature Algorithm (ECDSA) | IKEv2 unterstützt ab sofort die Authentifizierungsmethode Elliptic Curve Digital Signature Algorithm (ECDSA). Dies ermöglicht deutlich kleinere Schlüssellängen und somit höhere Verschlüsselungs-Effizienz bei gleichem Sicherheitsniveau. |
| IKEv2 Split-DNS | Split-DNS ermöglicht die DNS-Auflösung bestimmter interner Domänen über einen VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird. |
| IKEv2 Fragmentierung | Ermöglicht die effiziente Fragmentierung von IKEv2-Nachrichten (nach RFC 7383) vom VPN-Router selbst, so dass IKE-Pakete vom Transportnetz nicht mehr fragmentiert werden müssen. |
| Erweiterung bei Client-Reservierungen im DHCPv6-Server | Im DHCPv6-Server können ab sofort Client-Adressen bzw. Präfixe wahlweise anhand von DUID, MAC-Adresse, Interface-ID (nach RFC 3315) oder Remote-ID (nach RFC 4649) zugewiesen werden. |
| Doppelte Anzahl an Public Spot-Usern | Für ausgewählte Router der R&S®LANCOM 178x- und 179x-Serie mit Public Spot Option erhöht sich die Anzahl der User von 64 auf 128. |
| **Neue Features LCOS 10.20** | |
| WPA3 | Mehr Sicherheit für Ihre WLAN-Infrastruktur bietet Ihnen ab sofort die jüngste Generation der WLAN-Verschlüsselung - WPA3 (Wi-Fi Protected Access). Als Nachfolger von WPA2 bietet WPA3 wichtige Erweiterungen und Sicherheits-Features für kleine („WPA3-Personal") und große Netze („WPA3-Enterprise"). Mit LCOS 10.20 unterstützen alle R&S®LANCOM Access Points und WLAN-Router den neuen WLAN-Sicherheitsstandard. |
| LEPS-U & LEPS-MAC | Bewahren Sie die Kontrolle darüber, wer sich in Ihrem WLAN befindet. Mit LEPS-U (R&S®LANCOM Enhanced Passphrase Security - User) vergeben Sie einzelnen Clients oder ganzen Gruppen ein individuelles WLAN-Passwort für eine SSID. Über LEPS-MAC authentifizieren Sie die Clients noch zusätzlich anhand ihrer MAC-Adresse - ideal für sichere Unternehmensnetzwerke! |
| Client Management | Mit Client Management werden WLAN-Clients stets auf den für sie idealen Access Point sowie das beste Frequenzband gesteuert. Dieses Feature steigert somit die Qualität drahtloser Netzwerke jeder Größenordnung - egal ob im stand-alone-Betrieb oder orchestriert über die R&S®LANCOM Management Cloud. Die beliebten, aber bislang getrennten Funktionen Band Steering und Client Steering werden hiermit kombiniert und auch ohne den Betrieb mit einem WLAN-Controller bereitgestellt. |
| Auto Updater | Der Auto Updater hält Ihre Installationen automatisch immer auf dem aktuellen Stand: R&S®LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Dabei wählen Sie, ob Sie nur Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden, die Sie anschließend mit einem Klick manuell installieren können. |
| WAN Policy-Based NAT | WAN Policy-Based NAT ermöglicht die einfache Zuordnung von statischen WAN-IPv4-Adressen zu gewünschten Diensten. Durch eine NAT-Aktion in den Firewall-Regeln werden dabei interne Adressen hinter einer vom Provider zugewiesenen WAN-Adresse maskiert. Ideal für Szenarien z.B. für den Betrieb von Mailservern und Webservern mit verschiedenen WAN-Adressen. |
| DSL-Bridge-Mode | Ab sofort können alle VDSL-Router in einen DSL-Bridge-Modus versetzt werden. Dies ermöglicht den Einsatz der Geräte als reines DSL-Modem. Ideal für Szenarien, in denen mehrere DSL-Zugänge an einem Router betrieben werden sollen. |
| R&S®LANCOM vRouter | Das Management des vRouters wird nun noch einfacher, denn Firmware-Updates können fortan einfach via UPX-Datei eingespielt werden. |
| Layer-3-Tunneling | Alternativ zum WLAN-Controller ist nun der Aufbau von Layer-3-Tunneln vom Access Point zu einem Router auf Basis von L2TPv3 möglich. Ohne den Einsatz von komplexen VLANs wird der Datenverkehr so bequem über eine existierende Infrastruktur (Router, Switches) geleitet. |
| OCSP-Responder | Maximale Sicherheit bei VPN-Zugriffen: Dank Smart Certificate profitieren Sie von der in R&S®LANCOM Geräten integrierten Funktion zur komfortablen Erstellung digitaler Zertifikate - ganz ohne externe Zertifizierungsstelle! Erweitert wurde diese Funktion nun um das Netzwerkprotokoll OCSP (Online Certificate Status Protocol), welches Clients ermöglicht, den Status von X.509-Zertifikaten bei der integrierten CA automatisch und effizient abzufragen. |
| Unterstützung von LISP (Locator/ID Separation Protocol) | Das Locator/ID Separation Protocol (LISP) ist eine neue Routing-Architektur. Mit LISP können hochskalierbare Netzwerke mit integriertem Routing- und Tunnel-bzw. Overlay-Protokoll realisiert werden. Ideal für Service Provider oder Enterprise-Netzwerke. |
| Public Spot CSV-Import | Public Spot-Management noch einfacher: Benutzer können nun bequem per Textdatei (CSV) für den Hotspot-Zugriff importiert und exportiert werden. |
| Enhanced Open | Dank Einführung einer zusätzlichen Datenverschlüsselung verbessert Enhanced Open die Sicherheit von Clients in offenen WLANs wie z.B. Hotspots in Cafés oder Hotels. |

| Neue Features LCOS 10.12 | |
|---|---|
| VPN<br>IKEv2 | Mehr Performance und Sicherheit im VPN<br>Unterstützung von AES-GCM bei IKEv2<br>Unterstützung der elliptischen Diffie-Hellmann-Gruppen (ECDH) 19, 20 und 21 sowie der ECC Brainpool-Kurven 28, 29 und 30 bei IKEv2<br>Unterstützung für RADIUS CoA bei IKEv2<br>Loadbalancer für IKEv2 für gleichmäßige Lastverteilung in großen Szenarien<br>Erweiterte VPN-Backup-Mechanismen<br>VPN-Einrichtungsassistent für IKEv2, inkl. 1-Click-Konfiguration des R&S®LANCOM Advanced VPN Clients für IKEv2-Verbindungen |
| IPv6<br>DHCPv6 | Frei konfigurierbare DHCPv6-Optionen |
| LACP | LACP ermöglicht die Bündelung von Ethernet-Verbindungen zu einer virtuellen Einheit. Ideal für die Einrichtung redundanter Verbindungen, denn falls eine physikalische Leitung ausfällt, wird der Datenverkehr über das andere Kabel weiterhin übertragen. Zudem wird die mögliche Übertragungsgeschwindigkeit redundant angeschlossener Geräte erhöht. |
| VoIP | Mittels Overlap Dialing können Sie die Wartezeit zwischen gewählter Rufnummer und Rufaufbau deutlich verkürzen: Bereits während des Wählvorgangs werden bereits Rufnummernteile an die Vermittlungsstelle gesendet. |
| WLAN | Die automatische Umwandlungsmöglichkeit von Multicast- in Unicast-Datenströme ermöglicht mehreren WLAN-Clients ruckelfreies Streaming hochauflösender Videoanwendungen. Bei Anwendungen, wie z.B. IPTV-Diensten, profitieren Sie so von gesteigerter Performance und einer deutlich spürbaren Qualitätsverbesserung. |
| IPv6 | Für die Aktionstabelle sind Variablen für die IPv6-LAN-Adresse und Präfix verfügbar |
| ICMPv4 und ICMPv6 | Rate-Limiting für ICMPv4 und ICMPv6 ist verfügbar. |
| NTP | Unterstützung von MD5 im NTP-Client und Server<br>NTP-Server pro ARF-Netz schaltbar |
| OSPF | Unterstützung von OSPFv2 |
| OCSP | OCSP-Prüfung im TLS/Rollout-Agent |
| TACACS | Unterstützung für TACACS Shell-Autorisierung |
| Content Filter | Eine Erweiterung der auswählbaren Kategorien zum Einschränken von Webinhalten gewährt Ihnen jetzt noch mehr Sicherheit vor unerwünschtem Internet-Missbrauch in Ihrem Netzwerk.<br>Darüber hinaus ermöglicht der R&S®LANCOM Content Filter nun auch das Filtern von Webinhalten, die über IPv6 erreicht werden. |
| Public Spot<br>Smart Ticket | Mehr Sicherheit für die Nutzung der Smart-Ticket-Funktionalität im Public Spot: Nutzen Sie die Möglichkeit, über die von Ihnen erlaubten Ländervorwahlen hinaus, auch einzelne Rufnummer-Vorwahlen innerhalb des Landes zu gewähren bzw. auszuschliessen. Der Missbrauch von teuren Mehrwert-Rufnummern beim Anfordern der Zugangsdaten für Ihren Public Spot ist somit ausgeschlossen. |
| **Neue Features LCOS 10.0** | |
| Unterstützung der<br>R&S®LANCOM Management Cloud | Die R&S®LANCOM Management Cloud ist das weltweit erste hyper-integrierte Management-System, das Ihre gesamte Netzwerkarchitektur intelligent organisiert, optimiert und steuert. Mittels hochmoderner „Software-defined Networking-Technologie" wird die Bereitstellung eines integrierten Netzwerks drastisch vereinfacht, die manuelle Einzelgerätekonfiguration entfällt. |
| Bonjour-Proxy | Das Protokoll Bonjour ermöglicht Ihren WLAN-Clients ein schnelles und automatisches Auffinden von Geräten im Netzwerk, um z.B. Druck- und Streaming-Anwendungen (wie Airprint, Airplay, etc.) ohne vorherige manuelle Konfiguration durchzuführen. Der Bonjour Proxy erlaubt die Nutzung des Protokolls Bonjour über Layer-2-Grenzen hinweg. So lassen sich ZeroConf-Dienste auch in Szenarien mit Netzwerkvirtualisierung (ARF) umsetzen. |
| Layer-7-Anwendungserkennung | Mit der Layer-7-Anwendungserkennung können Sie genutzte Anwendungen und Dienste (z.B. Netflix, Youtube, etc.) im gesamten Netzwerk via LANmonitor oder R&S®LANCOM Management Cloud komfortabel nachvollziehen – ein echter Mehrwert für ein umfassendes Monitoring. |
| Unterstützung für Radius CoA im WLAN | Im WLAN kann durch RADIUS CoA die Bandbreitenverfügbarkeit eines eingebuchten Clients während einer laufenden Sitzung gedrosselt oder der Client abgemeldet werden. Der Administrator erhält damit eine verbesserte Kontrolle, zum Beispiel bei Überschreitung des Datenvolumens. |
| WLC<br>Skript-Rollout nach LCOS-Version | Es können WLC-gesteuerte Skript-Rollouts für bestimmte LCOS-Versionen festgelegt und somit abweichende Konfigurationen unterschiedlicher LCOS-Versionen in eine WLAN-Installation integriert werden. |
| Public Spot<br>E-Mail-Abfrage bei Login | Die Nutzung des Public Spots kann von einer Benutzerregistrierung abhängig gemacht werden, in der eine E-Mail-Adresse der Nutzer abgefragt wird. |
| Public Spot<br>Mehrsprachiger Titel der Login-Seite | Der Titel der Public Spot Login-Seite kann in sechs verschiedenen Sprachen abgelegt werden. Hierbei stehen Deutsch, Englisch, Französisch, Italienisch, Spanisch und Niederländisch zur Verfügung. Der Titel des Public Spot Login-Seite wird in Abhängigkeit der vom Benutzer eingestellten Browsersprache ausgegeben. |
| Public Spot<br>PMS-Modul | Das PMS-Modul bietet die Möglichkeit, den Benutzer die Nutzungsbedingungen des Public Spots auch auf der PMS-Login-Seite bestätigen zu lassen. Zusätzlich können für jeden Tarif die maximale Sende- und Empfangsbandbreite konfiguriert werden. |
| RADIUS<br>Konfigurierbarer WAN-Zugriff | Der Zugriff auf den RADIUS-Dienst über eine IPv4-WAN-Verbindung kann eingeschränkt werden. |
| RADIUS<br>Neue Attribute | Der R&S®LANCOM RADIUS-Server unterstützt die Attribute „Tunnel-Password" und „LCS-Routing-Tag", welche Sie in den Benutzerkonten definieren können. Daraus ergibt sich die Möglichkeit, die Benutzerdaten innerhalb eines Unternehmens zentral im RADIUS-Server zu speichern und den Konfigurationsaufwand für VPN-Szenarien zu minimieren. |
| VoIP / SIP<br>IPv6-Unterstützung im<br>Voice Call Manager | Der Voice Call Manager unterstützt mit LCOS 10.0 auch das Internet-Protokoll IPv6. |

| | |
|---|---|
| VoIP / SIP<br>VoIP +10 Option | Neben der generellen Aufrüstung von SIP-Leitungen im Voice Call Manager von 20 auf 25 können additiv mit der R&S®LANCOM VoIP +10 Option weitere Leitungen hinzugefügt werden (bis maximal 55). |
| VoIP / SIP<br>Verschlüsselung im LAN | LCOS 10.0 bietet eine Erweiterung des Session Border Controllers: Dank der neuen Verschlüsselungsmöglichkeit von VoIP-Daten im internen Netz unterliegt der Austausch von SIP-Clients damit auch innerhalb des LANs maximaler Sicherheit. |
| VoiP / SIP<br>SIP-Trunk im LAN | Über die interne SIP-Trunk-Terminierung können SIP-TK-Anlagen über den Session Border Controller an externen VoIP-Leitungen betrieben werden. |
| VoIP / SIP<br>SIPS und SRTP | Der Voice Call Manager bietet die Möglichkeit, zur verschlüsselten Übertragung der Authentifizierungsdaten von SIP-Benutzern sowohl SIPS (Session Initiation Protocol Security) als auch SRTP (Secure Real-Time Transport Protocol) zu konfigurieren |
| VoIP / SIP<br>Verarbeitung von UDP-Paketen | Die Verarbeitung eingehender UDP-Pakete kann gesteuert werden, sofern die Providerleitung UDP zur Kommunikation mit dem Registrar verwendet. |
| **Neue Features LCOS 9.24** | |
| DECT-Erweiterung für R&S®LANCOM All-IP-Lösungen | Die Basisstation R&S®LANCOM DECT 510 IP ist die ideale Lösung zur Einbindung von Gigaset DECT-Mobilteilen in kleinen und mittleren Unternehmen. Angeschlossen an den R&S®LANCOM Router ermöglicht LCOS 9.24 eine automatische Einrichtung und Konfiguration der Basisstation mit bis zu 6 DECT-Mobilgeräten. So können diese einfach registriert und Rufnummern individuell zugewiesen werden. Dabei kombiniert die R&S®LANCOM DECT 510 IP kabellose Telefonie mit außergewöhnlicher HD-Voice-Sprachqualität. |
| Einbindung von AiRISTAFLOW RTLS-Systemen | LCOS 9.24 ermöglicht ab sofort die Einbindung von AiRISTAFLOW Real Time Location Systems in R&S LANCOM Infrastrukturen. Damit können Personen, Gegenstände und Geräte fortan professionell und zuverlässig in Ihrer WLAN-Umgebung lokalisiert werden. Von der Positionsbestimmung von Patienten im Krankenhaus, über Wegeverfolgung mobiler Maschinen in der Lagerhalle, bis hin zur Nachverfolgung von Arbeitsgeräten, die Kompatibilität von R&S LANCOM und AiRISTAFLOW ermöglicht Ihnen Echtzeit-Lokalisierung für jegliche Branchen und Anwendungsgebiete. |
| MWI (Message Waiting Indicaton) | Die Erweiterung des R&S LANCOM Voice Call Managers um MWI ermöglicht die Signalisierung von hinterlassenen Sprach- und Textnachrichten auf Ihrer Provider Mailbox im Netz (sofern vom Provider unterstützt). Ist dort eine Nachricht hinterlassen worden, wird der Empfänger automatisch über die Benachrichtigungsfunktion des SIP-Endgerätes informiert. |
| Call Forking | Die Erweiterung des R&S LANCOM Voice Call Managers um Call Forking ermöglicht die gleichzeitige Rufsignalisierung von eingehenden Anrufen über eine Rufnummer auf mehreren zugewiesenen Nebenstellen. Wird ein Anruf an einer Nebenstelle entgegengenommen, wird dies von den weiteren Nebenstellen erkannt, sodass keine Benachrichtigung über einen entgangenen Anruf erfolgt. |
| Unterstützung für RADIUS CoA (Change of Authorization) im Public Spot | In Szenarien mit externen Hotspot-Servern kann durch RADIUS CoA die Bandbreitenverfügbarkeit eines eingebuchten Clients gedrosselt oder der Client abgemeldet werden. Der Hotspot-Provider erhält damit eine verbesserte Kontrolle zur Durchsetzung seiner Nutzungsbedingungen, zum Beispiel bei Überschreitung des Datenvolumens. |
| **Neue Features LCOS 9.20** | |
| Voice over Secure IP (VoSIP) | Der in der R&S LANCOM All-IP Option integrierte Voice Call Manager mit Session Border Controller-Funktionalität unterstützt ab sofort Voice over Secure IP (VoSIP). Die Verschlüsselung von Signalisierungs- und Sprachdaten (SIPS/SRTP) ermöglicht abhörsichere Telefonie an IP-basierten Amtsanschlüssen. |
| SNMPv3 | Ab sofort profitieren alle Rohde & Schwarz Networks and Cybersecurity Kunden von mehr Sicherheit bei der Netzwerküberwachung durch die Unterstützung von SNMPv3 (Simple Network Management Protocol Version 3). Dieses Protokoll vereint komfortables Geräte-Monitoring mit hoher Sicherheit dank verschlüsselter Datenkommunikation - ganz ohne Konfigurationsänderungen, da automatisch aktiviert. |
| WLAN-Qualität | Spürbar mehr Performance, Robustheit und Reichweite für R&S LANCOM Access Points, WLAN-Router und WLAN-Controller: Ab LCOS 9.20 unterstützen alle WLAN-Geräte die Highlight-Features Airtime Fairness, Adaptive RF Optimization, Wireless Intrusion Detection System und viele weitere Funktionen. Darüber hinaus genießen R&S LANCOM User und Administratoren dank umfangreicher Qualitätsverbesserungen das beste WLAN-Erlebnis aller Zeiten. |
| IKEv2 | IKEv2 ermöglicht einen schnelleren und sichereren Verbindungsaufbau von VPN-Tunneln. Erstmals wird darüber hinaus die VPN-verschlüsselte Vernetzung von IPv6-basierten Standorten möglich - auch im Mischbetrieb mit IPv4. |
| IKEv1 mit IPv6-Unterstützung | Neben der Unterstützung von IKEv2 lassen sich ab LCOS 9.20 auch über IKEv1 VPN-Verbindungen zwischen IPv6-Netzwerken aushandeln. |
| BGP | Effiziente VPN-Vernetzung von Standorten dank dynamischem Routing in mittleren bis großen Netzen. BGP (Border Gateway Protocol) sorgt für eine optimale Wegwahl aller vernetzten Router durch den Austausch ihrer besten Pfade aus ihren Routing-Tabellen. |
| Erweiterte Telefonie-Funktionen | Der in der R&S LANCOM All-IP Option integrierte Voice Call Manager (VCM) unterstützt zahlreiche zusätzliche Funktionen wie gleichzeitige Anrufsignalisierung über mehrere interne ISDN-Busse, integrierte DTMF-Umwandlung für eine zuverlässige Übertragung von Wähltönen über All-IP-Leitungen sowie die Unterstützung von SIP-Paketen über TCP-Verbindungen. |
| Logging von DNS-Anfragen | Client-seitige DNS-Anfragen können zur Protokollierung und Auswertung an einen externen SYSLOG-Server gesendet werden. |
| Performance-Messung über iPerf | Mit dem im LCOS integrierten Tool iPerf messen Sie exakt den maximalen, sowie den aktuellen TCP- und UDP-Durchsatz zwischen zwei Geräten im Netzwerk. Daraus ableitbare Bandbreitenverluste können so als Engpass im Netzwerk aufgedeckt und behoben werden. |
| Höhere Komplexität bei Gerätepasswörtern | Höhere Sicherheit bei der Verwendung von Passwörtern durch neue Vergaberichtlinie für mindestens acht Zeichen bestehend aus Buchstaben, Ziffern und Sonderzeichen. |
| WLAN<br>Adaptive RF Optimization | Dynamische Auswahl des besten WLAN-Kanals - Höherer WLAN-Durchsatz im Funkfeld dank dynamischer Auswahl des besten WLAN-Kanals durch den Access Point bei Kanalstörungen. |
| WLAN<br>Airtime Fairness | Verbesserte Ausnutzung der WLAN-Bandbreite - Bessere WLAN-Performance durch effiziente Ausnutzung der zur Verfügung stehenden Bandbreite dank einer fairen Aufteilung der WLAN-Übertragungszeiten unter den aktiven Clients. |

| | |
|---|---|
| WLAN<br>Wireless IDS | Erkennung von Angriffen oder auffälligem Verhalten von Clients in der WLAN-Infrastruktur durch dauerhafte Überwachung des Funkfeldes. Tritt ein angriffsähnliches Ereignis mit einer bestimmten Häufigkeit in einem definierten Zeitraum auf, wird eine Warnung via E-Mail, SYSLOG-Nachricht, SNMP oder LANmonitor ausgegeben. |
| WLAN<br>Adaptive Transmission Power | Ideal für professionelle Backup-Szenarien in WLAN-Umgebungen: Bei Ausfall eines Access Points wird die Sendeleistung der verbleibenden Access Points automatisch erhöht, sodass eine vollständige WLAN-Abdeckung stets sichergestellt ist. |
| WLAN<br>Konfigurierbare Datenraten je SSID | Für die vorgegebenen Datenraten, welche zur Kommunikation zwischen Access Point und WLAN Clients genutzt werden, stehen nun detaillierte Konfigurationsmöglichkeiten zur Verfügung - ein echter Zugewinn an Flexibilität. So können z.B. Datenraten, die aufgrund der Umgebungsbedingungen nicht sinnvoll nutzbar sind, von der Verwendung ausgeschlossen werden. |
| WLAN<br>Flexible Gültigkeit von Public Spot-Zugängen | Ab sofort kann die gebuchte Bandbreite auf den Public Spot Vouchern dargestellt werden. Zudem kann die Gültigkeit (Ablaufzeitpunkt) von Vouchern mit kürzeren Zeiteinheiten (Tage, Stunden, Minuten) gestaltet werden - ideal für Szenarien mit hoher Kundenfrequenz bei gleichzeitig kurzer Verweildauer. |
| WLAN<br>Controller-less WLAN-Management | Die R&S LANCOM Management Cloud sowie das Management-System R&S LANCOM Large Scale Rollout & Management (LSR) ermöglichen die automatische Inbetriebnahme und Konfigurationsvergabe („Zero-touch Deployment") sowie das Management von R&S LANCOM Access Points auch ohne WLAN-Controller. |
| Unterstützung R&S LANCOM Battery Pack | Das R&S LANCOM Battery Pack ermöglicht bei Stromunterbrechungen den Betrieb von maximal zwei angeschlossenen Routern oder Access Points über einen Zeitraum von mehr als zwei Stunden. |
| VLAN-Zuweisung pro ISP | Es können pro Internet-Service-Provider mögliche VLANs definiert werden, welche bei entsprechenden WAN-Verbindung getestet und bei Erfolg verwendet werden. |
| **Neue Features LCOS 9.10** | |
| Smart Certificate | LANCOM setzt einen Meilenstein im Bereich Sicherheit!<br>Maximale Sicherheit bei VPN-Zugriffen: Profitieren Sie ab sofort von der in LANCOM Geräte integrierten Funktion zur komfortablen Erstellung digitaler Zertifikate - ganz ohne externe Zertifizierungsstelle! VPN-Verbindungen lassen sich somit mit selbst erstellten Zertifikaten sicher verschlüsselt einrichten. Dieses Maximum an Sicherheit ist enthalten in allen LANCOM Central Site VPN Gateways, WLAN-Controllern sowie in allen LANCOM Routern mit LANCOM VPN 25 Option. |
| High Availability Clustering | Gruppierung und zentrales Management von mehreren WLAN-Controllern und Central Site VPN Gateways<br>Gruppieren Sie mehrere WLAN-Controller oder Central Site VPN Gateways zu einer hochverfügbaren Gerätegruppe (High Availability Cluster). Über die LANCOM High Availability Clustering Optionen lassen sich mehrere Geräte zu einem Cluster zusammenfassen. Somit ergeben sich viele Vorteile, wie das zentrale Management und der komfortable Konfigurationsabgleich (Config Sync) aller Cluster-Geräte. Hiervon profitieren Sie insbesondere beim Aufbau von intelligenten Backup-Szenarien, da nur ein WLAN-Controller oder Central Site VPN Gateway im Cluster konfiguriert werden muss - für den Administrator eine enorme Zeitersparnis. Darüber hinaus ermöglicht High Availability Clustering eine automatische Lastverteilung sowie die Vergabe von Cluster-Zertifikaten. |
| GRE-Tunnel | Maximale Flexibilität bei der Kopplung von entfernten Netzwerken: Mit Generic Routing Encapsulation (GRE) werden Pakete eingekapselt und in Form eines Tunnels zwischen zwei Endpunkten transportiert. |
| Ethernet over GRE-Tunnel | Das „virtuelle Ethernet-Kabel" - ideal zur Verbindung zweier Netze via Layer-2-Tunnel z.B. per IPSec-VPN. |
| TR-069-Unterstützung | „Zero-touch Management" - Das Protokoll TR-069 ermöglicht die automatische Provisionierung und ein sicher verschlüsseltes Remote-Management eines Routers in Provider-Umgebungen. |
| Public Spot | Im LANmonitor wird die aktuelle sowie die maximal mögliche Anzahl verwendeter Public Spot-Benutzer angezeigt und zudem ein Hinweis bei 90% Lizenzauslastung ausgegeben.<br>Im Public Spot-Volumenbudget kann nun mehr als 4 GB Datenvolumen als Limit angelegt und zusätzlich das festgelegte Budget pro Nutzer auf dem Voucher gedruckt werden.<br>Stark vereinfachter Zugang zur Erstellung von Public Spot-Vouchern durch automatische Weiterleitung auf die entsprechende Seite.<br>Das Inputset für die Passwörter von Public Spot-Benutzern ist konfigurierbar.<br>Die Option des CSV-Exports im Public Spot-Assistenten ist schaltbar.<br>Das Public Spot XML Interface wurde um erweitertes VLAN Handling erweitert. |
| WLAN | Die maximale Client-Bandbreite kann pro SSID konfiguriert werden.<br>Pro WLAN-Funkmodul sind ab sofort 16 individuelle SSIDs konfigurierbar, bei IEEE 802.11ac-Modulen 15 SSIDs.<br>PPPoE-Intermediate-Agent für PPPoE-Snooping, um PPPoED-Datenpakete zu be- und verarbeiten. |
| Wireless Quality Indicators | Grafische Darstellung von Empfangs- und Signalstärke im WLAN zur schnellen Identifizierung der Signalqualität |
| IEEE 802.11ac | Unterstützung von Point-to-Point-Verbindungen (bis zu 1 km) und des Client-Modus für alle IEEE 802.11ac-Geräte |
| WLAN-Controller | Die automatische Konfigurationsvergabe durch einen WLAN-Controller an neue Access Points über eine WAN-Verbindung ist konfigurierbar.<br>Anzeige des Zertifikatsstatus bei neuen Access Points<br>Wireless ePaper- und iBeacon-Konfiguration über den WLC<br>LEDs der Access Points über den WLC abschaltbar<br>Erweiterung der Tabelle des zentralen Firmware-Managements um Datumsangabe<br>Kanal- und Frequenzanzeige von Clients<br>Die Profile des WLAN-Controllers wurden zur Übersichtlichkeit in WLAN-Profile und Erweiterte Profile aufgeteilt |
| SCEP | Mehr Sicherheit bei Zertifikaten:<br>Unterstützung der SCEP-Algorithmen AES192 und AES256 zur Verschlüsselung sowie SHA256, SHA384 und SHA512 zur Signaturprüfung<br>Assistent zum Widerrufen von Zertifikaten<br>Konfigrierbares One-Time-Password für SCEP |
| SSL / TLS | Die Auswahl der Cipher-Suite für SSL und TLS kann insofern gesteuert werden, dass immer PFS bevorzugt wird, unabhängig von der Präferenz des Clients. |
| Load Balancer - Client Binding | Neue Anwendungsmöglichkeiten in Load Balancing-Szenarien - In anspruchsvollen Anwendungen wie Online-Banking werden zusammenhängende Sessions auf einer WAN-Leitung erkannt und aufrechterhalten |

| | |
|---|---|
| RADIUS | Unterstützung von weiteren RADIUS-Attributen<br>Zusätzliche Schemata zur Ermittlung von Realms aus Benutzernamen<br>Kommentarfeld für RADIUS Clients<br>RADIUS Client kann bei Bedarf weitere Source Ports nutzen.<br>Accounting-On- und Accounting-Off-Pakete werden für jeden Start und Shutdown einer SSID versendet. |
| DHCPv6 | Unterstützung der PD-Exclude-Option im DHCPv6 Client. |
| L2TP | Konfigurierbare Loopback-Adresse für L2TP |
| RIP | Konfigurierbare Loopback-Adresse für RIP |
| Content Filter | Benachrichtigungen per E-Mail bei Content Filter-Ereignissen werden auf Wunsch sofort oder täglich ausgelöst. |
| Verschlüsselte Konfiguration in LANconfig | In LANconfig lassen sich Konfigurationsdateien per Passwort verschlüsseln und sicher speichern. Des weiteren wurden die Protokolle im Default auf verschlüsselte Protokolle eingeschränkt. |
| Überwachung von Konfigurationsänderungen | Einfache Überprüfung von Konfigurationsänderungen dank der Darstellung von Hash-Werten, Zeitstempeln und Change-Countern. |
| Erweiterte Zeichenanzahl für Gerätenamen | Die mögliche Zeichenanzahl zur Vergabe von Gerätenamen wurde auf 64 erweitert. |
| TACACS+ | Der Befehl „passwd" wurde erweitert und ermöglicht so eine Änderung des lokalen Passworts von Benutzern. |
| WAN | Automatische Erkennung von VDSL-Anschlüssen der Deutschen Telekom und entsprechendes Nutzen von VLAN-ID 7. |
| VoIP | Eine proaktive Einrichtung der All-IP Option wird ermöglicht, indem die Zeitintervalle der Registrierungsversuche von Seiten des LANCOM Routers in geregelten Abständen steigen. Dies verhindert im Falle eines noch nicht umgestellten Anschlusses das ungewollte Sperren des Zugangs und sorgt für einen nahtlosen Übergang zum All-IP-Betrieb. |
| T.38-Unterstützung | LANCOM Router mit aktivierter All-IP Option unterstützen das IP-basierte Faxprotokoll T.38. Somit lassen sich Faxe mit sehr hoher Zuverlässigkeit über an den LANCOM Router angeschlossene Faxgeräte versenden und empfangen. Ideal zur Migration von ISDN/analog zu All-IP: Unterstützt die Gegenstelle oder der Provider kein T.38, wird das Fax wie bisher als Audiosignal mittels Codec G.711 versendet. |
| **Neue Features LCOS 9.04** | |
| Wireless ePaper-Verwaltung | In LANconfig integriertes zentrales Management und Monitoring für LANCOM Access Points der E-Serie und LANCOM Wireless ePaper Displays. |
| All-IP Option | Die All-IP Option rüstet Router der 1781er-Serie und den 1631E sowie den 831A mit IP-basierten Telefoniefunktionen aus. Somit wird der Weiterbetrieb von vorhandenen ISDN-Endgeräten und ISDN-TK-Anlagen mit einem ISDN-BUS nach Umstellung auf All-IP ermöglicht. |
| iBeacon-Unterstützung | iBeacon ist ein Funkstandard zur Innenraumlokalisierung. Das in den LANCOM Access Points der E-Serie integrierte iBeacon-Funkmodul sendet kontinuierlich Funksignale, die von Smartphones und Tablet PCs mit Bluetooth Low Energy-Unterstützung (Version 4.0) empfangen werden können. Befindet sich ein geeignetes Endgerät in Reichweite des iBeacons, können mit einer entsprechenden App vielfältigste ortsbezogene Dienste realisiert werden. |
| Listen before Talk | Unterstützung der Norm EN 300328 V1.8.1 in allen WLAN-Geräten |
| Clearmode-Unterstützung | Unterstützung des Clearmode-Protokolls für ISDN-Datenanwendungen |
| **Neue Features LCOS 9.00** | |
| Client Steering | WLAN Clients werden aktiv zu den für sie sinnvollsten Access Point gelenkt um eine ideale Lastverteilung zu erreichen und den einzelnen Clients die best mögliche Übertragungsrate zu bieten. Das Client Steering kann von der Client-Anzahl, dem Frequenzband und der Signalstärke abhängig gemacht werden. |
| Auto-WDS | Auto-WDS ermöglicht die kabellose Integration von Access Points in die vorhandene WLAN-Infrastruktur, inklusive Verwaltung durch WLAN-Controller. |
| Fast Roaming | Fast Roaming, basierend auf WLAN-Standard IEEE 802.11r, ermöglicht schnelle Roaming-Vorgänge zwischen Access Points. Dies wird in Controller-basierten WLAN-Installationen mit IEEE 802.1x-Authentifizierung oder Pre-Shared Key realisiert, indem die Zugangsschlüssel der Clients zwischengespeichert und automatisch an die verwalteten Access Points weitergegeben werden. |
| 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) |
| Bandbreitenlimitierung pro SSID | Die, den WLAN Clients zur Verfügung stehende Bandbreite kann pro SSID individuell konfiguriert werden. |
| RADIUS Accounting pro SSID | Pro SSID kann der RADIUS Server individuell festgelegt werden. |
| Public Spot XML-Schnittstelle | Eingebuchte Public Spot-Benutzer können während der Session durch Änderung der erlaubten Bandbreite (Bandbreitenlimit) gedrosselt werden. Zusätzlich kann die VLAN-ID beim Anmeldevorgang übergeben werden. |
| Public Spot | In konfigurierbaren Zeitabständen kann der Public Spot-Benutzer auf Werbe-Webseiten des Betreibers umgeleitet werden. |
| WLC 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. |
| WLC 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. Beim Auswahl eines WLAN-Controllers verteilen sich die Access Points automatisch neu, ist er wieder verfügbar wird auch die Rückverteilung automatisch durchgeführt. |
| WLC 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. |

| | |
|---|---|
| PRP | Durch das Parallel Redundancy Protocol können die Paketverluste bei Punk-zu-Punkt-Szenarien mit Dual Radio Access Points deutlich reduziert werden, da die Daten redundant übertragen werden.<br>Unterstützte Geräte:<br>IAP-322<br>OAP-322<br>OAP-382 |
| L2TPv2 | Unterstützung des Layer 2 Tunneling Protocols Version 2 |
| DHCP | Unterstützung der DHCP Option 82 zur logischen Unterscheidung von WLAN-Benutzergruppen mit Hilfe der Markierung von DHCP-Nachrichten zur Einteilung in unterschiedliche Adress-Pools. |
| Content Filter | Erweiterung des Content Filters zur Blockierung von HTTPS-Webseiten durch die Entnahme des Domain-Namens aus den HTTPS-Serverzertifikaten oder durch Reverse DNS Lookup der IP-Adresse. |
| VDSL Vectoring | Unterstützung von VDSL Vectoring in den entsprechenden Geräten. |
| IPv6 | Die Erweiterungen in IPv6 umfassen:<br>RAS-Einwahl per IPv6<br>Dual Stack Lite (IPv4-in-IPv6-Tunnel)<br>IPv6-Unterstützung für RADIUS Server und Client<br>Zusätzliche Loopback-Adressen<br>Lightweight DHCPv6 Relay Agent<br>RA Guard<br>DHCPv6 Guard |
| LANconfig | Die Ports der einzelnen Management-Protokolle (HTTP, HTTPS, TELNET, SSL, SNMP) können in LANconfig über einen Menüpunkt zentral konfiguriert werden. |
| LANmonitor | Alle Public Spot Clients werden im LANmonitor eindeutig gekennzeichnet |
| SSL/TLS | Eliptic Curve Cryptography (ECC) für SSL und TLS wird angeboten. Die genutzten Algorithmen können frei gewählt werden. |
| SSH | Eliptic Curve Cryptography (ECC) für SSH wird angeboten. Zudem können jetzt Sonderkommandos über SSH abgesetzt werden (z.B. Geräte neustarten, Software-Option aktivieren, Uhrzeit setzen) |
| Mobilfunk | Der SIM PIN kann sowohl über LANconfig als auch die CLI geändert werden. |
| **Neue Features LCOS 8.84** | |
| WLAN | Die Basisdatenrate, mit der Multicast- und Broadcast-Pakete versendet werden, ist nicht mehr festgelegt. Stattdessen wird sie dynamisch an die verfügbaren Datenraten der eingebuchten Clients angepasst, so dass die bestmögliche Datenrate verwendet werden kann.<br>Um die Zuverlässigkeit der Zustellung von DHCP-Antworten im WLAN zu steigern, können als Broadcast gesendete Datenpakete in Unicast-Datenpakete umgewandelt werden. |
| Adaptive Noise Immunity | Durch aktivierte Adaptive Noise Immunity blendet ein Access Point Störquellen im Funkfeld aus und fokussiert sich ausschließlich auf WLAN Clients mit ausreichender Signalstärke. WLAN Clients profitieren von deutlich mehr Datendurchsatz dank einer störungsfreien Funkabdeckung. |
| 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. |
| RADIUS | Die RADIUS-Authentifizierung kann auch zur Anmeldung an einem Gerät verwendet werden. Zusätzlich ist es möglich, Benutzer im internen RADIUS-Server zu deaktivieren, ohne sie direkt zu löschen. |
| Public Spot | Zahlreiche Neuerungen im Public Spot umfassen:<br>die Anzeige einer Fehlerseite bei inaktiver Internetverbindung<br>die Erweiterung der Default-Sprachen im Public Spot auf Deutsch, Englisch, Spanisch, Italienisch, Französisch und Niederländisch<br>die Möglichkeit, Texte in verschiedenen Sprachen für unterschiedliche Parameter im Public Spot in Tabellen abzulegen<br>die Integration einer spezifischen Logout URL, um den einfachen Logout aus dem Public Spot zu ermöglichen<br>bei allen Betriebsarten des Public Spots kann der Benutzer bei der Anmeldung dazu aufgefordert werden, die AGBs des Anbieters zu akzeptieren<br>auf der Voucher-Seite kann konditionaler HTML-Code eingefügt werden, den das Gerät nur bei bestimmten Benutzern bzw. Administratoren ausgibt<br>das optionale Caching von Templates kann die Performance des Public Spots verbessern<br>neue Variablen für LAN MAC, Gateway IP und Client IP zur Nutzung bei der Weiterleitung an ein externes Hotspot-Gateway |
| Public Spot<br>Smart Ticket | Auf Basis von HTML-Seiten lassen sich Anmeldeseiten für Smart Ticket im LANCOM Public Spot erstellen und konfigurieren. |
| IPv6 | Zur Nutzung dynamischer IPv6-Adressen kann die IPv6-WAN-Adresse als Skriptvariable in der LANconfig-Aktionstabelle eingerichtet werden, z.B. für Dynamic DNS-Dienste. Eine weitere Ergänzung zu IPv6 umfasst die IPv6-Präfix-Delegation vom WWAN ins LAN. Dies ermöglicht, dass Clients das auf der WAN-Mobilfunkseite zugewiesene /64-Präfix im LAN verwenden können. Damit ist ein Betrieb eines Routers in IPv6-Mobilfunknetzwerken ohne DHCPv6-Präfix-Delegation und Neighbor Discovery Proxy (ND-Proxy) möglich. |
| SMTP Client | Der SMTP Client im LCOS unterstützt die Authentifizierungsmethoden und -protokolle "SMTP über TLS", "STARTTLS" und "CRAM-MD5" für eine SSL-basierte Verschlüsselung der Anmeldedaten an einem E-Mail-Server. |
| LCMS | Ergänzung um einen Einrichtungs-Assistenten für VoIP-Provider. |
| LCMS<br>Quick Config Rollback | Die automatische Sicherung der Konfigurationsdateien in LANconfig erlaubt ein einfaches und schnelles Rollback auf vorherige Konfigurationen. |
| Hotspot 2.0 | Die Funktionalität von Hotspot 2.0 ist nun auch über LANCOM WLAN-Controller konfigurierbar. |

| | |
|---|---|
| LTE | Die zu nutzenden Frequenzbänder für LTE-Verbindungen können fest eingestellt werden. |
| SSH | Nach einem Reset erzeugen LANCOM Geräte automatisch einen individuellen SSH-Schlüssel. Des weiteren ist es möglich, die Erstellung eines neuen SSH-Schlüssels über die Kommandozeile auszulösen. |
| SMS | Mobilfunk-Router sind nun in der Lage, SMS zu versenden und zu empfangen. Die Verwaltung erfolgt komfortabel über den LANmonitor. Zusätzlich können Benachrichtigungen bei definierten Netzwerkereignissen, beispielsweisebei Störungen, per SMS versendet werden. Das Versenden von SMS kann auch über HTTP-Aufrufe mit URL-Parameter ausgelöst werden. Somit kann der Mobilfunk-Router als SMS Gateway eingesetzt werden.<br>Automatischer Versand von SMS für Smart Ticket. Der SMS-Versand von Public Spot-Zugangsdaten bei Smart Ticket kann direkt über einen Mobilfunk-Router erfolgen – ohne externes SMS-Gateway.<br>Geeignet für Installationen mit einem maximalen Durchsatz von 10 SMS/Minute. |
| SYSLOG | Die SYSLOG-Protokollierung wurde erweitert und beinhaltet ausführliche Informationen zum Aufbau von Mobilfunkverbindungen als auch zur DSL-Synchronisation und zu Einwahlvorgängen von Plain-IP-Verbindungen. |
| LANCOM CC Router | Nach der Ausführung des CC-Einrichtungsassistenten kann der Fingerprint des eingespielten SSH-Schlüssels gespeichert werden. |
| Volumen-Budget | Das genutzte Datenvolumen von WAN-Verbindungen kann überwacht werden und beim Erreichen von gesetzten Grenzwerten können verschiedene Aktionen ausgelöst werden.<br>Dieses Feature wird für folgende Produkte angeboten:<br>1781er Serie<br>L-45x Serie<br>1780EW-3G, 1780EW-4G<br>9100+ VPN, 7100+ VPN, 9100 VPN, 7100 VPN<br>WLC-4006+<br>IAP-321, IAP-321-3G, IAP-3G<br>OAP-322, OAP-321, OAP-321-3G, OAP-3G<br>831A, 1631E |
| Rollout Assistent | Ein Default Rollout-Assistent steht nun in LANCOM Geräten zur Verfügung, welcher zum Bezug von Rollout-Konfigurationen genutzt werden kann. |
| **Neue Features LCOS 8.82** | |
| Hotspot 2.0 | Der neue WLAN-Standard IEEE 802.11u (Hotspot 2.0) ermöglicht 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. |
| WLAN | Das ARP/NDP-Handling von Access Points wurde verbessert, so dass pro MAC-Adresse mehr als eine IPv6-Adresse gespeichert werden kann. Außerdem kann das Senden von Multicasts und Broadcasts in die Funkzelle deaktiviert werden. Eine zusätzliche Ergänzung ist die Möglichkeit, Band Steering über den WLAN Controller auf verwalteten Access Points zu aktivieren. |
| Public Spot | Die Erweiterung der Public Spot Funktionen umfasst ein einfaches Login, bei dem der Benutzer nicht mehr Zugangsdaten angeben, sondern nur die Nutzungsbedingungen des Hotspot-Betreibers bestätigen muss. Hierbei wird im Hintergrund ein temporärer Benutzer angelegt, der über ein limitiertes Zeit- oder Volumenbudget verfügt. Zusätzlich können nun sowohl das Quell-VLAN als auch die NAS-Port-ID in der Public Spot URL übergeben werden, um auf deren Basis unterschiedliche Willkommensseiten anzuzeigen. Außerdem kann einem Public Spot-Benutzer nun beim Login ein bestimmtes VLAN zugewiesen werden. |
| Public Spot<br>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. |
| Public Spot<br>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. |
| Public Spot<br>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. |
| RADIUS | Die maximale Zeichenanzahl für den Realm in der RADIUS-Weiterleitung wurde auf 64 Zeichen erhöht. Es kann über den RADIUS-Server eine Bandbreitenlimitierung für Public Spot Clients vorgegeben werden, welche über am LAN ausgekoppelte Access Points oder direkt über LAN angebunden sind. |
| SYSLOG | Die Anzahl der maximalen Einträge des internen SYSLOG-Servers von LANCOM Routern wurde auf über 20.000 erhöht. Zudem kann das maximale Alter von Nachrichten auch in Stunden, Tagen oder Monaten angegeben werden. |
| DNS pro ARF | DNS-Weiterleitungen können für jedes über ARF virtualisierte Netz individuell vergeben werden. |
| DHCPv6 | Der Funktionsumfang des DHCPv6 Servers von LANCOM Geräten wurde um die Option 'Reconfigure' erweitert. Somit kann der DHCPv6-Server seine Clients dazu auffordern, ihre IP-Adressen, Präfixe, DNS-Server oder andere Informationen zu erneuern. |
| LANconfig mit SSH | SSH steht als zusätzliches Protokoll in LANconfig zur Verfügung, um Firmwares und andere Dateien auf das Gerät hochzuladen oder es zu konfigurieren. |
| Mobilfunk | Wird die Einbuchung von Seiten des Mobilfunknetzes verweigert, kann dies über LCOS, LANmonitor und SYSLOG an den Benutzer transparent mitgeteilt werden. |
| Firewall | In der Firewall können über das Quell-Routing-Tag Regeln für verschiedene ARF-Kontexte unabhängig voneinander realisiert werden. |
| Public Spot<br>PMS Accounting Plus | Diese Option vereinfacht die Abrechnung von Hotspot-Gebühren. Sobald auf einem LANCOM Gerät die LANCOM Public Spot Option installiert ist, ermöglicht diese zusätzliche Option die Anmeldung und Abrechnung des Gastzugangs über das Property Management System (PMS). Dies geschieht über die FIAS-Schnittstelle, die eine direkte Kommunikation zwischen LANCOM Gerät und z. B. dem FIAS-basierten Micros Fidelio System erlaubt. |

| Neue Features LCOS 8.80 | |
|---|---|
| IPv6<br>Dual Stack | Die Unterstützung von IPv6 kann global aktiviert und deaktiviert werden. Hierbei können die IPv6-Funktionen zusätzlich zu den bestehenen IPv4-Funktionen verwendet werden.<br>Unterstützte Betriebsarten: IPv4, IPv4/IPv6, IPv6<br>Unterstützte IPv6-Adresstypen: Link Local, Global Unicast, Unique Local |
| IPv6<br>Router | Ein separater IPv6-Router mit eigener Routing-Tabelle ermöglicht die schrittweise Migration der Netzwerkkonfiguration. |
| IPv6<br>Internetzugang | Verfügbare Methoden, den IPv6-Internetzugang zu realisieren:<br>IPv6-Tunnel durch ein IPv4-Netzwerk<br>Natives IPv6 über PPP (IPv6CP) mit Adresszuweisung durch die Autokonfiguration und mit Unterstützung für Multi-Link-PPP<br>Natives IPv6 über IPoE mit statischer Adresszuweisung, durch Autokonfiguration oder DHCPv6<br>(DSLoL mit nativem IPv6 nur im Exklusiv-Modus möglich) |
| IPv6<br>Tunneltechnologien | Folgende Tunneltechnologien stehen zur Verfügung, um den IPv6-Internetzugang an einem IPv4-Anschluss zu realisieren:<br>6to4-Tunnel<br>6in4-Tunnel<br>6rd-Tunnel mit statischer Parameterkonfiguration oder über DHCPv4 |
| IPv6<br>over PPP (IPv6CP) | IPv6 kann sowohl in einer reinen IPv6-PPP-Verbindung, als auch in einer gemeinsamen IPv4/IPv6-Verbindung genutzt werden. |
| IPv6<br>DHCPv6-Server | Unterstützt Stateless- und Stateful-Modus. Unterstützte Optionen: IPv6-Adresse (IA_NA), Präfix-Delegierung (IA_PD), DNS-Server, DNS-Suchliste und Rapid Commit. |
| IPv6<br>DHCPv6-Client | Unterstützt Stateless- und Stateful-Modus. Unterstützte Optionen: IPv6-Adresse (IA_NA), Präfix-Delegierung (IA_PD), DNS-Server, DNS-Suchliste, FQDN, Rapid Commit, Reconfigure. |
| IPv6<br>DHCPv6-Relay-Agent | Weiterleitung von DHCPv6-Nachrichten zwischen DHCPv6-Clients und DHCPv6-Servern in unterschiedlichen Netzwerken. |
| IPv6<br>Stateless Address Autoconfiguration (SLAAC) | Automatische Konfiguration der IPv6-Adresse aus der MAC-Adresse nach EUI-64 aus empfangenen Router Advertisements. |
| IPv6<br>Neighbor Discovery Protocol (NDP) | Verantwortlich für das automatische Finden anderer Komponenten im gleichen Netzwerksegment und der zugehörigen IPv6-Adressen. Konfiguration mehrerer Subnetze über Router Advertisements möglich, sofern es das vom Provider delegierte Präfix zulässt.<br>Unterstützte Betriebsarten: Router, Host |
| IPv6<br>Firewall | Objektorientierte, voll konfigurierbare Stateful Inspection Firewall. |
| IPv6<br>LCOS-Anwendungen | Derzeit unterstützte Andwendungen: WEBconfig, SSH, Telnet, DNS, TFTP<br>Weitere Anwendungen werden in einer späteren Version IPv6 unterstützten. |
| IPv6<br>LANconfig Unterstützung | Die IPv6-Unterstützung von LANconfig umfasst das Suchen und Konfigurieren von Geräten über IPv6.<br>Mögliche Betriebsarten: IPv4, IPv4/IPv6, IPv6 |
| Band Steering | Durch das gezielte Unterdrücken von Probe Responses auf dem nicht bevorzugten Freuenzband kann ein Client, der bereits auf beiden Frequenzbändern wahrgenommen wurde, auf das bevorzugte gelenkt werden. |
| Spectral Scan | Der Spectral Scan bietet die Möglichkeit, über WEBconfig eine Spekralanalyse direkt am Access Point durchzuführen und grafisch darzustellen. Hiermit können Interferenzen und Störsignale erkannt und analysiert werden. Das Feature wird für folgende Geräte angeboten:<br>L-45x Serie<br>L-32x Serie<br>1781AW, 1781EW<br>1780EW-3G |
| DFS | Erfüllung der neuen DFS-Anforderungen nach ETSI 301 893 Version 1.6.1 - DFS4 |
| UUID Info Element für WLAN APs | WLAN Access Points können optional in den Beacons ein UUID Info Element senden, welches sie als einen LANCOM Access Point identifiziert. Ein Access Point mit zwei Funkmodulen sendet auf beiden Funkmodulen die gleiche UUID. |
| RADIUS Server pro SSID | Einer SSID kann nun in ihrem Profil im WLAN Controller ein spezifischer RADIUS Server zugewiesen werden, so dass mehrere SSIDs unterschiedliche RADIUS Server verwenden können. |
| Alternative WLC über DNS | Über DNS können managed Access Points Adressen alternativer WLAN Controller übermittelt werden. |
| Public Spot | Erweiterte Funktionalität des Public Spots, welche sowohl einen Assistenten zur Ersteinrichtung, als auch die Möglichkeit des Smart Tickets, der automatischen Authentifizierung von Benutzern über SMS oder E-Mail, beinhaltet. Zusätzlich wurde ein weiteres Funktionsrecht zur Administration der Benutzerverwaltung des Public Spots implementiert. Außerdem ist es möglich, die Anzahl der Mehrfach-Logins im Assistenten zu konfigurieren und festzulegen, ob ein Benutzer bei der Eingabe des Benutzernamens an Groß- und Kleinschreibung halten muss. Eine Ergänzung an der Tabelle der freien Netze erlaubt nun auch das Nutzen von Wildcards und Domains, die über mehrere IP-Adressen erreicht werden können. Des Weiteren wurde eine XML-Schnittstelle zur Kommunikation mit einem externen Hotspot Gateway implementiert. |
| SYSLOG, Bootlog und Eventlog | SYSLOG, Bootlog und Eventlog sind optional auch boot-persistent.<br>Dieses Feature wird für folgende Produkte angeboten:<br>1781er Serie<br>1681er Serie<br>L-45x Serie<br>1780EW-3G<br>9100 VPN, 7100 VPN<br>WLC-4100, WLC-4025+<br>IAP-321, IAP-321-3G, IAP-3G<br>OAP-321, OAP-321-3G, OAP-3G |

| | |
|---|---|
| Packet Capture in WEBconfig | Bietet die Möglichkeit, Paketmitschnitte remote auf einem LANCOM Gerät über WEBconfig ausführen zu lassen und sie lokal zu speichern. Diese können dann zum Beispiel mit Wireshark ausgewertet werden. |
| Logging von Konfigurationsänderungen | Konfigurationsänderungen auf der Kommandozeile können nun von einem LANCOM Gerät mit SYSLOG protokolliert werden. |
| VPN | Erweiterungen im VPN-Bereich umfassen die Unterstützung der Diffie Hellman Gruppe 14, sowie die intelligente Vorberechnung von DH-Schlüsseln für einen schnelleren Verbindungsaufbau. |
| IPsec | Implementation der Standard-konformen IPsec Replay Detection, die dazu dient, Replay Attacken zu verhindern, indem sie Pakete mit alten Sequenznummern verwirft. |
| SSH / SCP | Über SSH / SCP können jetzt Zertifikate und Konfigurationsdateien an ein LANCOM-Gerät übertragen werden. Zusätzlich ist es möglich, die von SSH benutzten Krypto-Protokolle und Schlüssellängen zu konfigurieren. |
| LANCOM myVPN | Es werden zusätzliche Konfigurationsoptionen zum Profilbezug angeboten. Zum einen kann der Bezug eines myVPN-Profils über das WAN unterbunden werden und zum anderen kann im Brute-Force-Schutz des Profilbezug angepasst werden, wie viele Fehlversuche erlaubt sind. |
| Fast Roaming<br>für WLAN APs im Client-Modus | WLAN Access Points im Client-Modus unterstützen nun PMK Caching und Preauthentication gemäß 802.1x, um Roaming-Vorgänge zu beschleunigen. Dual-Radio Access Points im Client Modus koordinieren nun die Roaming-Vorgänge der WLAN-Module, so dass bei zwei bestehenden Verbindungen zuerst ein Modul den Roaming-Vorgang abgeschlossen haben muss, bevor das andere beginnt. |
| LLDP | LLDP-Unterstützung zur automatischen Erkennung der im Netzwerk eingebundenen Geräte und deren Topologie. |
| Scripting | Um Scripting zu vereinfachen, wurde das TAB-Kommando in Skripten erweitert, so dass ein unbekannter Spaltenname keinen Syntaxfehler mehr meldet, sondern ignoriert wird. Dies ist dann relevant, wenn Geräte einen unterschiedlichen Funktionsumfang haben. |
| GPS Zeit | Die per GPS übermittelte Zeit kann zum Setzen der Systemzeit genutzt werden. |
| Content Filter | Der LANCOM Content Filter unterstützt nun ein Concurrent User Modell. Hierbei wird die Anzahl der gleichzeitigen Benutzer des Content Filters betrachtet und nicht mehr die Anzahl aller möglichen Benutzer. |
| LANmonitor | In LANmonitor werden die aktiven Ethernet-Ports und IPv6-Adressen angezeigt. Zusätzlich wird der DHCP-Server angezeigt, inklusive der Leases mit Zeitstempel. |
| LANconfig | Wird über LANconfig WEBconfig aufgerufen, wird per Default der in LANconfig integrierte Browser benutzt. Des Weiteren wurde die Bedienung von LANconfig überarbeitet, in Auswahlmenüs wurde der QuickFinder integriert und es wurden tabellarische Übersichten eingeführt, die Tiefenstrukturen übersichtlich darstellen. Die Möglichkeit sichere Passwörter generieren zu lassen wurde weiter verfeinert. |
| **Neue Features LCOS 8.62** | |
| LANCOM myVPN | Unterstützung der LANCOM myVPN App im LCOS. Die myVPN App für iOS-Geräte ermöglicht die vollständige IPSec-VPN-Konfiguration auf dem Endgerät in wenigen Schritten, um dann mit dem integrierten VPN-Client eine sichere VPN-Verbindung zu einem LANCOM Router aufzubauen. Hierzu wird das auf dem LANCOM Router angelegte VPN-Profil über HTTPS abgerufen und die notwendigen Einstellungen im VPN-Client des iOS-Gerätes automatisch vorgenommen. (Verfügbarkeit über den Apple AppStore) |
| WLC-6 Option | Mit der WLC-6 Option für Router ist es möglich, die Funktionalität eines LANCOM WLAN Controllers auch auf einem LANCOM Router zu nutzen. Es lassen sich bis zu sechs LANCOM Access Points und WLAN Router zentral verwalten.<br>Unterstützte Router: 1781EF, 1781A, 1781A-3G, 1781-4G |
| Public Spot | Die Funktionalität des Public Spots wurde erweitert, so dass nun über den Assistenten oder auch einen URL-Befehl ein Mehrfach-Login für Benutzer konfiguriert werden kann. So kann ein Benutzer den gleichen Zugang mit mehreren Endgeräten nutzen. Zusätzlich werden im Assistenten zur Benutzerverwaltung im Public Spot weitere Statusinformationen bereitgestellt: Online-Zeit, Traffic, Status, MAC-Adresse und IP-Adresse. |
| VoIP | Der Default-Wert für die WAN-Anmeldung eines neuen SIP-Benutzers wurde auf "Nicht erlaubt" geändert. Der Assistent zum Einrichten neuer SIP-Benutzer wurde um einen entsprechenden Dialog ergänzt. |
| IKE und IPSec | Die Default-Proposal-Listen in IKE und IPSec wurden überarbeitet und beinhalten nun auch AES-256 Bit, um per Default eine höhere Sicherheit zu gewährleisten. |
| WLAN | Die Einstellung SSID Broadcast unterdrücken wurde um den Wert "verschärft" erweitert. Ist diese Einstellung gewählt, wird nur an Clients, die die richtige SSID eingetragen haben, ein Probe-Response versendet. |
| **Neue Features LCOS 8.60** | |
| LCMS<br>Flexible Gruppenkonfiguration | Mit der flexiblen Gruppenkonfiguration können in LANconfig Konfigurationsvorlagen für Gruppen von LANCOM Geräten zusammengestellt werden. Diese Vorlage kann genutzt werden, um eine gemeinsame Basiskonfiguration an beliebig vielen Geräten vorzunehmen, so dass nur noch die individuellen Parameter für jedes Gerät einzeln konfiguriert werden müssen. |
| LCMS<br>CSV-Import | Mit Hilfe der Import-Möglichkeit von CSV-Dateien in LANconfig, können mehrere Geräte in einem Schritt angelegt werden. Zusätzlich können auch auf den Daten einer CSV-Datei Konfigurationsdateien erstellt werden, die dann zur weiteren Verwendung abgelegt werden. |
| Public Spot | Durch neue und erweiterte Assistenten im Benutzermanagement wurde das Anlegen, Ändern und Löschen von Benutzern optimiert. Hierzu zählt unter anderem der erweiterte Voucher-Druck-Assistent, mit dem es möglich ist, mehrere Voucher mit einem Klick zu drucken. Außerdem kann die Benutzerliste des Public Spots als CSV-Datei exportiert werden. Weitere Verbesserungen des Public Spot umfassen die Erweiterung der Weiterleitungs-URL auf bis zu 251 Zeichen und die Möglichkeit die Größe der Stationstabelle fest einzustellen. |
| WLAN P2P-Verbindungen | Bis zu 16 Gegenstellen können pro WLAN-Modul für P2P-Verbindungen genutzt werden. |
| WLAN Controller | Die Funkfeldoptimierung wurde durch ein neues Verfahren zur Interferenzmessung verbessert. |
| WLAN Sicherheit | Clients, denen über die Authentifizierung über 802.1x unterschiedliche VLANs zugeordnet wurden, können auf Grund von VLAN-spezifischen Gruppenschlüsseln nicht mehr die Broadcasts und Multicasts, die für andere VLANs bestimmt sind entschlüsseln. |

| | |
|---|---|
| WLAN 40 MHz Modus | Der 40 MHz Modus im 2,4 GHz Frequenzband wurde um eine “Good Neighbor” Funktionalität erweitert, welche als neue Standardeinstellung genutzt wird. Diese sorgt dafür, dass die Kanalbandbreite auf 20 MHz reduziert wird, sofern es durch den Einsatz von 40 MHz Kanälen zu Überlappungen im Frequenzband kommt. |
| PPTP | Ein PPTP-Tunnel kann nun auch mit einer MPPE-Verschlüsselung versehen werden, um so zum Beispiel mobile Geräte mit Android Betriebssystem sicher ins Unternehmensnetz einzubinden. |
| SYSINFO | SYSINFO wurde erweitert, so dass auch Standort und Kommentar angezeigt und übermittelt werden. |
| TLS 1.1 / 1.2 | TLS 1.1 und 1.2 werden unterstützt um eine bessere Sicherheit zu gewährleisten. Das TLS-Protokoll wird von LCOS in den folgenden Modulen verwendet: HTTP over SSL, Telnet over SSL, RADSEC, CAPWAP/DTLS, EAP-TLS/PEAP/TTLS. |
| Kommandozeilen-Verbesserung | Zur Vereinfachung der Arbeit mit großen Tabellen auf der Kommandozeile, ist es nun möglich in Tabellenzeilen zu wechseln und die Einträge der Zeile als Liste anzeigen zu lassen. Außerdem können die Show- und ls/dir-Kommandos äquivalent zu Traces gefiltert werden. |
| DHCP Vendor Class | Option den Vendor Class Identifier für DHCP-Anfragen zu ändern, um eine verbesserte Kompatiblität mit ISPs zu gewährleisten. |
| PPPoA / IPoA Unterstützung | Die LANCOM Router der 1781 Serie mit integriertem Modem unterstützen nun PPPoA und IPoA als WAN-Protokolle. |
| IPSec | Umstellung der Default-IPSec-Lifetimes auf einen einheitlichen und empfohlenen Wert. |
| LCOSCAP | LCOSCAP bietet die Möglichkeit Paketmitschnitte remote auf einem LANCOM Gerät ausführen zu lassen und sie lokal zu speichern. Diese können dann zum Beispiel mit Wireshark ausgewertet werden. |
| Advanced VPN Client Seamless Roaming | Mit dem LANCOM Advanced VPN Client (ab Version 2.3) ist es möglich, eine VPN-Verbindung mit einem LANCOM Router (ab LCOS 8.6) nach einem Verbindungsabbruch, der zugrunde liegenden Verbindung (z.B. UMTS oder ADSL), ohne erneute Anmeldung wieder aufzubauen. Die neue Verbindung kann hierbei auch über ein anderes Medium zu Stande kommen. Seamless Roaming ist insbesondere dann interessant, wenn One-Time-Passwords oder RSA-Token zur Authentifizierung zum Einsatz kommen. |
| Feature- und Lizenzaktivierung | Die Verlängerung der Content-Filter-Lizenz erfordert nicht mehr den Neustart des Gerätes. |
| SIP ALG | Das SIP ALG (Application Layer Gateway) agiert als Proxy für SIP-Kommunikation. Bei SIP-Telefonaten werden vom ALG automatisch die notwendigen Ports für die entsprechenden Medienpakete geöffnet. Durch automatische Adressumsetzung für Geräte im LAN entfällt der Einsatz von STUN.<br>Für folgende Geräte verfübar: LANCOM 1781-Serie, 1780EW-3G, 1681V, 1631E, 831A, 7100 VPN, 9100 VPN, WLC-4006, WLC-4025+, WLC-4100, IAP-3G, IAP-321-3G, OAP-3G, OAP-321-3G |
| **Neue Features LCOS 8.50** | |
| LANCOM QuickFinder | Suchfilter in LANconfig, auch innerhalb von Gerätekonfigurationen, LANmonitor und WLANmonitor. Bei der Suche in einer Konfiguration werden sowohl Beschreibungen als auch eingetragene Werte und Einheiten durchsucht (einstellbar). Fundstellen werden grafisch hervorgehoben und der Menübaum auf Seiten mit Treffern reduziert. Die Geräteliste in LANconfig, sowie Access Points, Controller, Profile und Clients in WLANmonitor werden bei Eingabe in LANCOM QuickFinder sofort auf Zeilen mit Treffern reduziert. In LANmonitor kann zwischen markierten Treffern geblättert werden. |
| 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 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. |
| Content Filter | Erweiterung um die Möglichkeit HTTPS-Anfragen zu filtern. Vereinfachte Override-Funktion, so daß nur noch ein Klick notwendig ist. Verdopplung der maximal unterstützten Benutzerzahl für den Content Filter bei allen unterstützten Geräten und Steigerung der allgemeinen Performance durch Softwareoptimierung. |
| Programmierbarer Rollout-Assistent | Ermöglicht die Programmierung von komplexen eigenen Assistenten, um eine vereinfachte Inbetriebnahme von Geräten je nach Projekt zu gewährleisten. Es werden eigene Templates und Logos unterstützt, um eine firmenspezifische Optik zu ermöglichen. Verfügbar für LANCOM 1681V, 1711+ VPN, 1721+ VPN, 1751 UMTS, 1811n Wireless, 1821n Wireless. |
| OCSP Client | Prüfen von X.509-Zertifikaten anhand von OCSP (Online Certificate Status Protocol), in Echtzeit arbeitende Alternative zu CRLs. |
| Public Spot Option | Die Public Spot Option (maximal 64 Benutzer) wird nun auch von LANCOM 1711+ VPN und 1721+ VPN unterstützt. |
| WLC Public Spot Option | Die WLC Public Spot Option (unlimitierte Zahl an Benutzern) wird nun auch von Central Site Gateways LANCOM 7100 VPN und 9100 VPN unterstützt |
| SYSINFO | Die Abfrage von SYSINFO stellt zusätzliche Informationen bereit: einen Hash-Wert für die aktuelle Konfiguration, einen Zeitstempel der letzten Konfigurationsänderung, einen persistenten Zähler für die Anzahl der Konfigurationsänderungen und die Anzeige des Wertes CONFIG_STATUS. |
| Load-Befehle | Die Befehle LoadFirmware, LoadConfig und LoadScript können nun konditional ausgeführt werden, um so automatische Ladevorgänge zu steuern. Zum Beispiel kann bei einer täglichen Ausführung von LoadFirmware geprüft werden, ob die aktuelle Firmware älter oder neuer ist als die angefragte Firmware. Anhand dieser Information wird dann entschieden, ob das Update durchgeführt werden soll. Der Befehl LoadFile wurde implementiert und erlaubt das Laden von Dateien auf ein Gerät, inklusive von Zertifikaten und gesicherten PKCS-12 Containern. Alle Befehle unterstützen nun zusätzlich zu TFTP auch HTTP und HTTPS. |
| SSL/TLS | HTTPS-Client-Authentifizierung auch per Zertifikat möglich. |
| HTTPS Server | Auswahl, ob ein hochgeladenes oder das Default-Zertifikat für den HTTPS Server verwendet werden soll. |
| Konfigurationsdialog | Die besuchten Einstellungsseiten einer Gerätekonfiguration werden in einer Historie abgelegt, der Zugriff erfolgt durch einfaches Vor- und Zurückblättern oder die Auswahl aus einer Ausklappliste. |
| Trace-Anwendung | Das Trace-Fenster kann nun auch aus dem Menü „Gerät“ in LANconfig heraus für das ausgewählte Gerät geöffnet werden. |
| Automatische Software Updates | Automatische Aktualisierung von LCMS nach Bestätigung. Suche von Updates, inklusive LCOS Versionen für verwaltete Geräte auf dem Downloadserver von myLANCOM (erfordert myLANCOM-Account). Wahlweise Aktualisierung ausgewählter Geräte bei heruntergeladenen Updates. |

| Neue Features LCOS 8.00 | |
|---|---|
| Content Filter (Option) | Optionaler Inhaltsfilter für das Websurfen mittels HTTP-Proxy. Individuelle Konfiguration von Filterprofilen aus verschiedenen Kategoriegruppen und Kategorien. Vergabe von Zeitprofilen. Zusätzliche Nutzung eigener Black- und Whitelisten mit Platzhaltern (Wildcards) in den Einträgen. Pro Kategorie-Gruppe/Kategorie schaltbarer Override-Mechanismus zur einfachen Behandlung von Ausnahmen. Flexible Anwendung der Filterprofile durch Aktionen in der Firewall. Individuelle Anpassung der angezeigten Seiten für Blockieren/Fehler pro Sprache oder Verweis auf Seiten auf separatem Webserver. Komfortable Konfiguration und Zusammenstellung von Filterprofilen in LANconfig. Vorgabe-Profile für Standardanforderungen. Benachrichtigung vor Ablauf von Lizenzen per E-Mail/ Syslog/SNMP. Assistent zur einfachen und schnellen Einrichtung des Content Filters für Standard-Anforderungen. Statistische Auswertung der Content Filter Nutzung (Kategorien-Hitliste und Verteilung, Top Ten der besuchten Webseiten, maximale und durchschnittliche Antwortzeiten, etc.) in LANmonitor |
| IPSec over HTTPS | Neue Auswahl für VPN-Tunnel zur alternativen Übertragung der VPN-Daten via TCP auf Port 443. Ermöglicht IPSec-VPN durch Firewalls in Netzen, für die z. B. Port 500 für IKE gesperrt ist. Geeignet für Client-to-Site- (mit LANCOM Advanced VPN Client 2.22 oder höher) und Site-to-Site-Verbindungen (LANCOM VPN Gateways oder Router mit LCOS 8.0 oder höher). Bei aktivierter Funktion "IPSec over HTTPS" versucht ein LANCOM Advanced VPN Client zunächst, einen klassischen IPSec-Tunnel (geringerer Overhead) aufzubauen, sollte dies nicht gelingen, wird die Kapselung von IPSec in TCP verwendet. IPSec over HTTPS basiert auf der VPN Path Finder Technologie von NCP |
| WLC/Load Balancing | LANCOM Wireless LAN Controller untersützten nun auch Loadbalancing für WAN-Anbindungen, sodass mehrere Leitungen für mehr Performance zusammengefasst werden können |
| WLC/802.1X | RADIUS-Accounting gemäß IEEE 802.1X kann für jede SSID individuell vom Wireless LAN Controller konfiguriert werden |
| WLC/Kanallastanzeige | Anzeige der Last pro Kanal in WLANmonitor bei Verwaltung von LANCOM Access Points über Wireless LAN Controller |
| WLAN/DFS | Unterstützung der neuen Anforderungen für die Erkennung von Radarimpulsen im WLAN gemäß ETSI 301 893 v. 1.5 |
| WLAN/Broken-Link-Detection | Das Fehlen eines Ethernet-Links an einem wählbaren LAN-Interface kann zum automatischen Deaktivieren eines WLAN-Moduls genutzt werden damit Clients sich an alternativen Basisstationen anmelden können |
| DHCP | DHCP Forwarding auch an mehrere (redundante) DHCP-Server |
| Alternative Boot-Konfiguration | Zur Vorgabe von projekt-/kunden-spezifischen Werten beim Rollout von Geräten können auf bis zu zwei boot- und reset-persistenten Speichplätzen individuelle Konfigurationen für kundenspezifische Standardeinstellungen (Speicherplatz "1") oder als Rollout-Konfiguration (Speicherplatz "2") abgelegt werden. Ein kurzer Reset (mehr als 5 Sekunden) lädt die kundenspezifischen Standardeinstellungen vom ersten Speicherplatz (falls vorhanden, sonst LANCOM Werkseinstellungen). Ein langer Reset (mehr als 15 Sekunden) lädt die Rollout-Konfiguration vom zweiten Speicherplatz (falls vorhanden, sonst LANCOM Werkseinstellungen). Zusätzlich ist die Ablage eines persistenten Standard-Zertifikats zur Authentifizierung für Verbindungen beim Rollout möglich |
| USB-Setup | Automatisches Laden von geeigneten Firmware- und Konfigurationsdateien nach dem Einstecken von USB-Datenspeichern (FAT Dateisystem) in LANCOM Router mit USB-Schnittstelle und Werkseinstelllungen. Die Funktionalität kann auch für den laufenden Betrieb aktiviert werden. Prüfung des Routers, ob die auf dem USB-Speichermedium vorliegenden Dateien zum Gerät passen und aktueller sind als bereits installierte |
| Interner HTTP/HTTP(S)-Fileserver | Ablegen von HTML-Seiten, Grafiken und Vorlagen für Public Spot Seiten, Voucher, Hinweisseiten des Content Filters auf einem USB-Datenträger (FAT Dateisystem) in vorgegebenem Ordner als Alternative zum begrenzten internen Speicher von LANCOM Routern |
| SNMP/MIB | Neues Konzept einer einzigen, vereinheitlichten LANCOM Enterprise MIB für neue LANCOM Produkte mit LCOS (erstmalig für LANCOM L-32x Serie und LANCOM WLAN Controller) zur einfachen Integration in Drittlösungen für Management und Monitoring auf Basis von SNMP. Bereitstellung der MIB zentral über LANCOM Systems |
| SSL/TLS | Verbesserte Sicherheit für alle Dienste mit TLS-Verhandlung (z. B. HTTPS-Konfiguration, CAPWAP, load-Kommandos via HTTPS) gemäß RFC 5746 zum Schutz vor potenziellen Schwächen von TLS in der Wieder-Aushandlung von Schlüsseln |
| SSH Client | SSH-Client-Funktionalität kompatibel zu OpenSSH unter Linux und Unix-Betriebssystemen zum Zugriff auf Drittkomponenten von einem LANCOM Router aus. Nutzung auch bei Verwendung von SSH zum Login auf dem LANCOM Gerät. Unterstützung von zertifikats- und passwort-basierter Authentifizierung. Erzeugung eigener Schlüssel mittels sshkeygen. Beschränkung der SSH-Client-Funktionalität auf Administratoren mit entsprechender Berechtigung |
| Setup-Assistent Internetzugang | Erweiterung des Assistenten zur Einrichtung von IPTV für Anschlüsse mit T-Entertain |
| LANconfig/(W)LANmonitor | Darstellung der Fensteransichten im Stil des jeweiligen Betriebssystems. Neue Icons mit hoher Auflösung. Baumansicht der Einstellungsseiten im Konfigurationsfenster zum schnellen Springen zwischen Einstellungen. Interaktiver Volltextfilter für Listen-Ansichten zur schnellen Auswahl/Einschränkung auf relevante Einträge (z. B. für Geräteliste in LANconfig, Accesspoints/Controller in WLANmonitor). Neue Passwortfelder mit optional einblendbarem Klartextpasswort sowie Erzeugung komplexer Passwörter. Editieren von Meta-Parametern im Header von Offline-Konfigurationen für das automatische Laden von Konfigurationen vom USB-Datenträger. Neue Anwendungshilfe für LANconfig (W)LANmonitor und Trace |
| **Neue Features LCOS 7.80** | |
| XAUTH mit RADIUS-Anbindung | Anbindung von XAUTH an RADIUS-Server zur Authentisierung von VPN-Client-Zugängen pro Verbindung über eine zentrale Benutzerverwaltung. Authentisierung für VPN-Client-Zugänge auch mit OTP-Tokens |
| VPN/Zertifikate | Gleichzeitige Unterstützung mehrerer Certification Authorities durch Verwaltung von bis zu neun parallelen Zertifikatshierarchien, jeweils mit CA-Zertifikat und Nutzung von CRL. Indizes zur einfachen Adressierung der einzelnen Zertifikate, insbesondere zur Arbeit auf der Kommandozeile. Platzhalter zur Prüfung von Zertifikaten auf Teile der Identität im Subject damit Gegenstellen in großen Umgebungen mit parallelen Zertifikatshierarchien auf ökonomische Weise authentifiziert werden können |
| VPN/PPTP | Überarbeitete Algorithmen vervielfachen die Performance von Central Site VPN Gateways bei vielen Gegenstellen, speziell für VPN- und PPTP-Verbindungen. Für PPTP- und VPN-Verbindungen können bis zu 32 alternative Gegenstellen mit jeweils eigenem Routing-Tag als Backup definiert werden. Die automatische Auswahl kann der Reihe nach, aufgrund der letzten erfolgreichen Verbindung oder zufällig (Load-Balancing) erfolgen |
| DoS | Erhöhung des Schwellwertes für halboffene Verbindungen bei Zentralgeräten auf 1.000 |

| | |
|---|---|
| DHCP-Cluster | Die DHCP-Server in LCOS können pro Routing-Kontext in den Cluster-Betrieb geschaltet werden, wenn in dem zum Kontext gehörenden Netz verschiedene DHCP-Server aktiv sind. Alle DHCP-Aushandlungen der anderen DHCP-Server werden mitverfolgt, sodass DNS-Anfragen unabhängig vom für die DNS-Registrierung verwendeten DHCP-Server aufgelöst werden können |
| Routing | Von Diensten im LCOS (Telnet, SSH, SNTP, SMTP, HTTP(S), SNMP etc.) über Ethernet versandte Antwortpakete auf Anfragen von Stationen können direkt zur anfragenden Station (Default) geleitet werden oder an ein durch ARP-Lookup ermitteltes Ziel |
| ARF | Unterstützung von bis zu 16 ARF-Kontexten (Netzen) für die 1700 und 1800 Serien. Das Routing-Tag für von lokalen Routern stammende Pakete wird durch eine Reihe von Vergleichen (in absteigender Folge) ermittelt: passt es zu einem definierten Netz, so wird dessen Tag verwendet, ist für die Schnittstelle, auf der es eingeht, nur ein Netz definiert, wird das Tag der Schnittstelle gewählt,, kann der per Reverse-ARP-Lookup ermittelte Next-Hop einem der definierten Netze zugeordnet werden, so wird dessen Tag gewählt, das Tag kann alternativ noch durch Vergleich mit der Routing-Tabelle bestimmt werden |
| ARF/WLAN | Zurodnung eines speziellen ARF-Kontextes für IAPP zum Austausch von Roaming-Informationen zwischen Accesspoints statt des Sendens in alle für einen AccessPoint definierten ARF-Kontexte (Default) |
| WLAN-Profile im Client-Modus | Für Accesspoins und WLAN-Router im Client-Modus können in Abhängigkeit von der SSID verschiedene WLAN-Profile definiert werden. Die Auswahl des zu verwendenden Profils erfolgt konfigurierbar anhand der Signalstärke (Default) oder der vorgegebenen Reihenfolge der Profile unabhängig von der Signalstärke |
| Voice Call Manager | Frei einstellbare Werte zur DiffServ-Markierung für Signalisierung (SIP) und Medienströme (RTP) |
| COM-Port-Forwarding | Bei Weiterleitung von Daten seriell angeschlossener Geräte kann neben Newline-Conversion zur Erkennung und Normalisierung von Zeilenumbrüchen bei zeilen-basierter Übertragung (Default) auch ein Binärmodus ohne Erkennung und Berücksichtigung von Zeilenumbrüchen verwendet werden. TCP-Keepalive nach RFC 1122, Keepalive-Intervall, Wiederholungs-Timeout und -Anzahl sind konfigurierbar |
| Ethernet-Schnittstellen | Über den ruhenden Modus, wenn Ethernet-Schnittstellen nicht verwendet werden, hinaus können diese vollständig elektrisch deaktiviert werden |
| SNMP-Optimierung | Optimierung der SNMP-Abarbeitung und Kommunikation mit LAN/WLANmonitor. Informationen für LANmonitor werden nur noch auf Basis von SNMP TRAPS übertragen und somit die wiederholte Übertragung großer Tabellen vermieden |
| TACACS+ | Schaltbare Umgehung von TACACS+ für CRON, Aktionstabelle und Script-Abarbeitung zur Entlastung zentraler TACACS+-Server in großen Installationen bei diesen Ausnahme-Aktionen speziell in der Phase von Rollouts |
| Management allgemein | Erweiterung der allgemeinen Management-Informationen der Geräte-Konfiguration auf acht Kommentarfelder zum Hinterlegen projektspezifischer Kennungen |
| CPU-Lastanzeige | Das Intervall zur Bildung des Mittelwerts der CPU-Last kann auf 1s, 5s, 60s oder 300s eingestellt werden. Ein Wert von 60s gemäß HOST-RESOURCES-MIB ist der Default |
| LANconfig | In LANCOM managed Switches können direkt von LANconfig aus neue Firmware-Dateien eingespielt sowie Konfigurationen gesichert und wieder hochgeladen werden.Der DHCP-Server unterstützt DHCP-Optionen mit Typ und Wert pro ARF-Kontext. Die Werte können nun auch in LANconfig eingestellt werden.<br>Das automatische Bereinigen der Benutzertabelle im RADIUS-Server kann nun auch in LANconfig gesetzt werden |
| LANmonitor/WLANmonitor | Bei großen Tabellen wie für VPN- und PPTP-Verbindungen zeigt LANmonitor nur die letzten Veränderungen in der Baumansicht. Alle Einträge können durch Aufruf einer separaten Tabellenansicht abgerufen und eingesehen werden. LANmonitor und WLANmonitor sind für die Verarbeitung und Anzeige von großen Tabellen optimiert |
| **Neue Features LCOS 7.70** | |
| VPN/Hardware-Beschleunigung | Mit dem Wechsel auf LCOS 7.7 wird auf VPN-Routern der 1700er, 1800er und 3000er Baureihe die Hardware-Beschleunigung auch ohne VPN-25 Option freigeschaltet. Die Anzahl der gleichzeitig möglichen Tunnel bleibt jedoch bestehen (abhängig vom Gerätemodell und der VPN-25 Option) |
| Public Spot | Umgestaltung des Public Spot-Assistenten zur Optimierung der Ausstellung von Vouchern. Neue Einstellparameter für Zeit- und Volumenbudgets sowie den Start des Accountings für flexible Tarifgestaltung bei WLAN Vouchern |
| TACACS+ | Unterstützung des Protokolls TACACS+ für Authentifizierung, Autorisierung und Accounting (AAA) mit verbindungsorientierter und verschlüsselter Übetragung der Inhalte. Authentifizierung und Authorisierung sind vollständig separiert. LANCOM Zugriffsrechte werden auf TACACS+-Berechtigungsstufen umgesetzt. Über TACACS+ können Zugriffsberechtigungen pro Parameter, Pfad, Kommando oder Funktionalität für LANconfig, WEBconfig oder Telnet/SSH gesetzt sowie alle Zugriffe und Änderungen der Konfiguration protokolliert werden. Berechtigungsprüfung und Protokollierung für SNMP Get- und Set-Anfragen. Das Berechtigungssystem wird auch in Webconfig mit Auswahl eines TACACS+-Servers bei der Anmeldung unterstützt. LANconfig unterstützt die Anmeldung über das gewählte Gerät am TACACS+-Server. Prüfung der Ausführung und jeden Kommandos innerhalb von Skripten gegen die Datenbank des TACACS+-Servers. Redundanz durch Konfiguration mehrerer TACACS+-Server. Konfigurierbare Möglichkeit zum Rückfall auf lokale Benutzerkonten bei Verbindungsfehlern zu den TACACS+-Servern. Kompatibilitätsmodus zur Unterstützung vieler freier TACACS+-Implementierungen |
| BFWA | Unterstützung von Broadband Fixed Wireless Access im 5,8 GHz-Band mit bis zu 4 Watt Sendeleistung für WLAN-Richtfunkstrecken nach IEEE 802.11n. (Die Nutzung von BFWA unterliegt landesspezifischen Vorgaben.) |
| Outdoor WLAN | Verbesserte DFS-Erkennung und Performance-Steigerung für IEEE 802.11n. Neues Profil für Irland im 5,8 GHz-Band mit 2 Watt Sendeleistung ohne DFS |
| LANmonitor | Grafische Darstellung mit zeitlichem Verlauf für Sende- und Empfangsrate von WAN- oder Punkt-zu-Punkt-Verbindungen, Empfangs-, Linksignalstärke und Durchsatz von Punkt-zu-Punkt-Verbindungen, CPU-Last, freiem Speicher und Temperatur (nicht für alle Geräte verfügbar) in separatem Fenster. Symbol zur Kennzeichnung grafisch darstellbarer Kenngrößen in der Ansicht des LANmonitors. Auswahl von Zeitabschnitten aus dem aufgezeichneten Zeitraum und tabellarische Gegenüberstellung der aufgezeichneten Kenngrößen mit Minimum, Maximum und Mittelwert. Akustische Wiedergabe der Signalstärke im Dialog zum Einrichten von Punkt-zu-Punkt-Verbindungen zur leichteren Ausrichtung von Antennen. DHCP-Tabelle mit manueller Aktualisierung zur Anzeige der aktuellen DHCP-Leases, erreichbar über das Kontextmenü des Gerätes. Trace-Symbol in der Symbolleiste. Gleichzeitige Betrachtung zweier Trace-Ergebnisse nebeneinander (dual view) im Trace-Modul. Anzeige von Funkband und Kanal pro WLAN-Schnittstelle |

| | |
|---|---|
| U-APSD/WMM Power Save | Erweiterung des Power Savings nach IEEE 802.11e um Unscheduled Automatic Power Save Delivery (entsprechend WMM Power Save) zum Umschalten von WLAN Clients in einen Stromsparmodus in erwarteten Gesprächspausen gemäß einer vorherigen Aushandlung des Anwendungsprofils (bei entsprechenden Endgeräten speziell für Voice over WLAN geeignet). Anzeige der Verfügbarkeit von U-APSD pro SSID im Statusmenü und Anzeige der pro Client ausgehandelten Kategorie in der Stationstabelle im Statusmenü |
| IGMP Snooping | Unterstützung des Internet Group Management Protocol (IGMP) in der WLAN-Bridge für WLAN SSIDs und LAN-Schnittstellen (nur für Geräte mit WLAN) zur gezielten Weiterleitung von Multicast-Paketen. Unterstützung von Multicast-Gruppen über Ports (SSIDs, LAN-Interfaces) und Router-Ports für das Routing von Multicast-Paketen über verschiedene Layer-3-Netze hinweg. Detaillierte Einstellung von Anfrage-, Anfrage-Antwort- und Werbe-Intervall sowie Robustheit. Automatisches Lernen von Multicast-Gruppen. Behandlung von Multicast-Paketen ohne Registrierung einstellbar (Nur-Router-Ports, Fluten, Verwerfen). Konfiguration statischer Mitglieder von Multicast-Gruppen pro VLAN-Id. Konfiguration simulierter Anfrager für Multicast-Mitgliedschaften pro VLAN-Id |
| Draeger Validierung | Eignung von LANCOM Geräten mit WLAN und IGMP Snooping zur Übermittlung von Patientendaten im medizinischen Umfeld per Multicast im WLAN |
| RADIUS Accounting | Kommando zum Zurücksetzen der Zähler alle aktuellen Konten, z. B. für exakte Abrechnung von Zeiträumen durch Zurücksetzen per CRON-Job |
| RADIUS Server | Erweiterung der Benutzerkonten um schaltbaren Mehrfach-Login, Ablauf zu relativem oder absolutem Zeitpunkt, Zeit- und Volumenbudgets sowie die Eingrenzung auf einen Service-Typ |
| Erweiterung Temperaturbereich L-305/310 | Erweiterung des Temperaturbereichs auf +45°C durch Begrenzung der Schnittstellengeschwindigkeit der Fast Ethernet-Ports bei Überschreiten einer Umgebungstemperatur von +35°C |
| Telnet/SSH (CLI) | Erweiterung des Kommandos „mailto“ zum automatisierten Ausführen von Kommandos und Versenden der Ausgaben als E-Mail-Anhang beim Eintreten von Ereignissen (Verbindungsauf-/abbau, CRON-Job) |
| UMTS/LANconfig | Upload von Firmwares, die in Form von upx-Dateien bereitgestellt werden, für UMTS-Module in LANCOM 1751 direkt aus LANconfig, auch für Gruppen von Routern |
| Voice Call Manager | In der automatischen Anrufweiterschaltung kann pro lokalem Benutzer gewählt werden, ob die interne Rufnummer, die originale Anrufernummer (sofern die Provider-Leitung dies ermöglicht) oder eine individuelle Rufnummer als Caller ID signalisiert wird |
| **Neue Features LCOS 7.60** | |
| Router / ARF | Automatisches Lernen von Routing-Tags für ARF-Kontexte aus der Routing-Tabelle |
| Firewall | Neue Trigger für Firewall-Regeln in Abhängigkeit vom Backup-Status, z.B. für vereinfachte Regelsätze bei schmalbandigen Backup-Leitungen |
| QoS / Session Limits | Limitierung der Session-Anzahl pro Gegenstelle (ID). Setzen von relativen Bandbreiten-Limits für QoS in Prozent. Bandbreiten-Steuerung und QoS auch für UMTS-Verbindungen |
| RIP | RIP-Quellen können zur Vereinfachung der Konfiguration in großen Installationen mit Platzhaltern (Wildcards) im Namen versehen werden |
| PPP | Einstellung der Protokolle zur Authentifizierung bei PPP. Unterstützung von MS-CHAPv2. Wahlweise Anbindung an RADIUS-Server für MS-CHAPv1 und MS-CHAPv2 |
| COM-Port-Server und -Forwarding | COM-Port-Server für DIN- und USB-Schnittstellen der LANCOM Router und Access-Points, der auch für mehrere seriell angeschlossene Geräte eigene virtuelle COM-Ports via Telnet (RFC 2217) zur Fernsteuerung verwaltet (nutzbar mit gängigen virtuellen COM-Port-Treibern gemäß RFC 2217) |
| IPSec VPN-Backup | 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) |
| Zertifikate | Neue OpenSSL-Implementierung mit FIPS-140 zertifizierten Algorithmen. Secure Key Storage zur Sicherung eines privaten Schlüssels (PKCS12) gegen Diebstahl |
| XAUTH | XAUTH-Client zur Anmeldung von LANCOM Routern und Access-Points an XAUTH-Servern inkl. IKE-Config-Mode. XAUTH-Server, der die Anmeldung von Clients per XAUTH an LANCOM Routern ermöglicht |
| WLC Monitoring & Management | Einheitliche und zusammengefasste Monitoring-Sicht auf WLAN-Controller-Cluster. Interner Speicher für bis zu drei Skript-Dateien (max. 64K) zur Provisionierung von Access-Points ohne separaten HTTP-Server. Automatisches Monitoring aller zu einem Cluster gehörenden Geräte bei Auswahl nur eines Controllers im Cluster |
| Public Spot | Unterstützung von öffentlichen Zertifikaten und Zertifikats-Ketten aus Vertrauensstellungen für Public Spot. Somit sind für gängige Internet-Browser vertrauenswürdige Login-Seiten mit gesichertem Zugriff (HTTPS) ohne Warnungen auf LANCOM Geräten möglich |
| SIP Registrar | Konfigurierbare Registrierung (mit/ohne) und Leitungs-Überwachung (inaktiv, automatisch, mit Re-Registrierung, mit OPTIONS-Requests) für SIP-Trunk, -Link, -Remote-Gateway und SIP-PBX-Leitung |
| SIP Proxy | Schaltbare Unterstützung von Privacy/Call Screening (Rufnummern-Unterdrückung) pro Leitung gemäß RFC 3325 oder mit Remote-Party-ID sowie Umsetzung in Abhängig von Teilnehmer-Einstellungen (CLIR). Unterstützung von Request-URI (RFC 3261) |
| Neues WEBconfig | Völlig neu überarbeitetes Web-Interface zur Konfiguration von LANCOM Routern und Access-Points in Anlehnung an LANconfig mit Systemübersicht, Syslog und Ereignis-Anzeige, Symbolen im Menübaum, Schnellzugriff über Seiten-Reiter. WEBconfig jetzt auch mit neuen Assistenten für Grundkonfiguration, Sicherheit, Internetzugang, LAN-LAN-Kopplung + Online Hilfe |
| HTTPS-Client | Zum Download von Firmware- und Konfigurations-Dateien von einem HTTPS-Server, z.B. für Roll-Out-Management |
| Neues Firewall GUI | Neue grafische Oberfläche zur Konfiguration der objekt-orientierten Firewall in LANconfig: Tabellenansicht mit Symbolen zum schnellen Erfassen von Objekten, Vergabe eigener Symbole für Objekte, Objekte für Aktionen/Quality-of-Service/Gegenstellen/Dienste, Default-Objekte für typische Anwendungsfälle, Definition individueller Objekte (z.B. für Anwendergruppen) |

| | |
|---|---|
| Vereinfachtes Config-Management | Austausch von Konfigurations-Dateien zwischen ähnlichen Geräten, z.B. zur Migration alter Konfigurationen auf neue LANCOM Produkte. Neues, nicht-modales Hilfefenster, das an das Konfigurationsfenster angedockt/gelöst werden kann, mit kontext-sensitiver Hilfe-Anzeige. Konfigurierbare Symbol-Leiste (hinzufügen/entfernen von Symbolen, Größeneinstellung, Beschreibungstexte ein-/ausblenden) mit neuen Symbolen für Speichern und Eigenschaften |
| LANmonitor | Optimierte und sortierte Anzeige der VPN-Verbindungen. Darstellung und Speichern des internen Syslog-Puffers (Ereignisanzeige) von LANCOM Geräten |
| Trace-Assistent / Diagnose Dateien | Erweiterung des grafischen TRACES um Assistenten für Standard-Diagnosen. Export von Diagnose-Dateien für Supportzwecke (enthalten Bootlog, Sysinfo und die Gerätekonfiguration ohne Passwörter) |
| **Neue Features LCOS 7.50** | |
| WLAN Controller 802.11n Access Point Unterstützung | Unterstützung der Access Points der LANCOM L-300er-Serie durch die LANCOM WLAN Controller (ohne zusätzliche Lizenzen) |
| WLAN Controller Firmware Management | Firmware-Verteilung für mehrere LANCOM Wireless Router und LANCOM Access Points zentral durch den WLAN Controller (Firmware-Bereitstellung durch Webserver erforderlich).<br><br>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 |
| WLAN Controller Skriptverteilung | Ermöglicht die vollständige Konfiguration von nicht WLAN-spezifischen Funktionen wie Redirects, Protokollfilter, ARF etc. |
| WLAN Public Spot | Einfaches Einrichten von Zugängen mit nur 2 Maus-Klicks über den Voucher-Druck-Assistenten. Die Voucher lassen sich über einen Standard-PC-Drucker ausdrucken. Anpassung des Voucher-Druck-Assistenten an das Unternehmen durch Einbindung des individuellen Firmenlogos. Funktioniert auch ohne externen RADIUS- oder Accounting-Server |
| LANconfig | Überarbeitete Assistenten für Grundkonfiguration, Internet und WLAN. Die Einstellungen von LANconfig können pro Benutzer oder global für mehrere Benutzer bzw. pro Projekt abgespeichert und geladen werden. Eine neue Multi-Spalten-Ansicht mit wichtigen Geräte-Informationen (Gerätename, Beschreibung, Adresse, Gerätestatus, Verlauf, Gerätetyp, Hardware-Release, Seriennummer, MAC-Adresse, Akt. Firmwareversion, Firmsafe, 1. Image Version, 2. Image Version) sorgt für sofortigen Überblick in Projekten. Spalten können ausgeblendet und es kann nach jeder Spalte sortiert werden. Ab LCOS 7.54: automatisches Speichern der aktuellen Konfiguration vor jedem Firmware-Update, Erkennen und Anzeige der neuen managed Switches LANCOM ES-2126/ES-2126P |
| LANmonitor | Umfangreiche Diagnose mit TRACES direkt aus LANmonitor mit komfortablen Dialogfenstern zum Einstellen und Filtern der Ausgabe. Zurückziehen von Zertifikaten in der LANmonitor-Ansicht. Sortierte Ansicht der VPN-Verbindungen. Ab LCOS 7.54: Suchfunktion innerhalb von TRACE-Ausgaben. Monitoring der neuen managed Switches LANCOM ES-2126/ES-2126P |
| WEBconfig | Neue Assistenten zur Einrichtung von Internet, WLAN und Public Spot |
| Management Rollout-Assistent | Unterstützung des Rollouts von LANCOM Geräten in großen Projekten durch Vorkonfiguration mit Basis-Einstellungen und automatisches Beziehen der individuelen Konfiguration anhand von Projekt und Standort beim Aufstellen des Gerätes |
| VoIP Media-Proxy | Definiertes Terminieren und Verschalten von multiplen Medienströmen. Kontrolle der Media Sessions, die aus SIP-Verbindungen resultieren. IP-Adress- und Port-Umsetzung für Pakete der Medienströme zwischen verschiedenen Netzen. Verschalten von Medienströmen zwischen Gegenstellen, die kein Verbinden (REFER) in SIP erlauben. |
| Dynamisches Routing | Extended RIPv2 mit HopCount, Poisoned Reverse, Triggered Update für LAN (nach RFC 2453) und WAN (nach RFC 2091) sowie Filtereinstellungen zum Propagieren von Routen |
| Spezifisches DNS-Forwarding | Eintrag eines Backup-DNS-Servers pro DNS-Weiterleitung |
| VPN Zertifikate | Unterstützung von digitalen, mehrstufigen X.509-Zertifikaten, kompatibel z.B. zu Microsoft Server/Enterprise Server und OpenSSL. Damit lassen sich auch Zertifikats-Hierarchien unterstützen. Das Hochladen erfolgt gesammelt in einer PKCS#12-Datei über WEBconfig (HTTPS) oder LANconfig |
| RADSEC | Sichere Kommunikation von RADIUS-Server und -Client mit zertifikats-basierter Authentifizierung |
| WLAN Punkt-zu-Punkt-Verbindungen | Zuweisung von Namen (Radio-ID) zu Funkmodulen und Referenzieren der Radio-IDs bei Konfigurationen für Punkt-zu-Punkt-Verbindungen anstelle von MAC-Adressen |
| WLAN Background Scanning | Individuelle Einstellung von Scan-Interval Filter für schnellere Roaming-Entscheidungen |
| DFS | Erfüllung der neuen DFS-Anforderungen nach ETSI 301 893 Version 1.3 für ab April 2008 in Verkehr gebrachte WLAN Geräte mit 5-GHz-Funkmodulen |
| Dynamic DNS Update mit GnuDIP-Client | Ab LCOS 7.54 wird das GnuDIP-Protokoll zum Update von DNS-Servern für dynamische IP-Adressen unterstützt. Das Protokoll bietet höhere Sicherheit (Salt und MD5 Digest) als DynDNS. Der GnuDIP-Server mit Self-Signup-Funktionen und DNS Dynamic Update Protocol für DNS-Server steht als Opensource-Software zur Verfügung |
| Firmware Kompression | Verwendung eines neuen Kompressions-Algorithmus zur besseren Ausnutzung das Flash-ROMs für Firmware-Speicherung mit LCOS 7.54 |
| SIP Proxy | Unterstützung von frühem und spätem Beginn der SDP-Aushandlung (ab LCOS 7.56) |
| ADSL Multi-mode | Neuer ADSL-Linecode und Unterstützung diverser Linecodes für ADSL, ADSL2 und ADSL2+ in einer Firmware (ab LCOS 7.56) |
| **Neue Features LCOS 7.20** | |
| VoIP TK-Anlage | Integration von TK-Anlagenfunktionen in alle LANCOM VoIP Router: Halten, Makeln, Verbinden von und zu allen internen und externen Teilnehmern (SIP, Analog, ISDN); Rufumleitung sofort, bei besetzt oder nach Wartezeit für alle internen Teilnehmer; Unterbinden von Zweitanrufen (busy-on-busy); Gruppenrufe mit parallelem oder sequentiellem Klingeln (Gruppen kaskadierbar); FAX over IP durch T.38; Multi-Login für komfortable Erreichbarkeit eines Teilnehmers mit mehreren Endgeräten unter einer Rufnummer |

| | |
|---|---|
| 1-Click-VPN | „1-Click-VPN“ zur Konfiguration von VPN-Verbindungen zwischen LANCOM Routern durch einfaches Drag & Drop in LANconfig. „1-Click-VPN Client“ zur einfachen Konfiguration einer VPN-Client-Einwahl incl. automatischer Erstellung eines Importprofils für den LANCOM Advanced VPN Client aus LANconfig heraus |
| Advanced Routing and Forwarding (ARF) | Die Virtualisierung der LANCOM Routing Engine: Je nach Gerät könnnen bis zu 64 unabhängige Routing-Kontexte bereitgestellt werden, die jeweils über unabhängige eigene Schnittellen, IP-Netze, VLANs, Routing-, Firewall- und QoS-Regeln, DHCP-Server, DNS-Einstellungen usw. verfügen. Ein kontrollierter Übergang zwischen diesen – in der Regel strikt getrennten – Kontexten kann zur Nutzung einer gemeinsamen IP-Infrastruktur (Server, Drucker etc.) über dedizierte Firewall-Regeln hergestellt werden. |
| SCEP | Unterstützung von SCEP (Simple Certificate Enrollment Protocol) zur automatischen Erzeugung, Verteilung und Verlängerung von digitalen Zertifikaten. In Verbindung mit LANCOM Pro-Adaptive VPN können so selbstkonfigurierende zertifikatsbasierte Netze vollautomatisch ausgerollt werden. |
| Integrierter RADIUS/EAP-Server | Integrierter Radius/EAP-Server für selbständige 802.1x Authentifizierung mit EAP-TLS, EAP-TTLS, PEAP, MSCHAP und MSCHAPv2. |
| Rapid Spanning Tree | Unterstützung von Rapid Spanning Tree zur schnellen Pfadauflösung bei redundanten Layer-2-Verbindungen. |
| WLAN Client Roaming-Verbesserung | Neue Experteneinstellungen zur Feinabstimmung des Roaming-Verhaltens im WLAN Client-Betrieb |
| WLAN Controller | Alle LANCOM WLAN Access Points und WLAN Router unterstützen ab LCOS 7.20 den Betrieb durch die LANCOM WLAN Controller. |
| Unterbrechungsfreie 5 GHz WLAN-Funkstrecken mit DFS | Ab LCOS 7.20 gilt nicht mehr die Einschränkung, daß beim Betrieb von 5 GHz Outdoor-Funkstrecken mit DFS die Verbindung alle 24 Stunden für eine Minute unterbrochen werden muß. Die Verbindung kann nun beliebig lange auf dem vom DFS-Algorithmus gewählten Kanal bestehen bleiben, bis ein Radarsignal erkannt wird. |
| Erweitertes Portforwarding | Die inverse Maskierung kann nun für mehrere IP-Adressen definiert und an TCP und/oder UDP gebunden werden. |
| HTTP Tunnel als Fernwartungszugang | Durch einen TCP/HTTP-Tunnel kann nach Authentifizierung auf Geräte im LAN zugegriffen werden. |
| Erweiterte VLAN Unterstützung | Unterstützung für mehrfach VLAN-getaggte Ethernet-Frames (‚Q-in-Q‘) sowie Unterstützung von VLAN auf (V)DSL WAN-Verbindungen |
| Unscharfe CRON-Aktionen | Die Zeitsteuerung kann mit einer Varianz versehen werden, so dass z.B. zeitgesteuerte Verbindungsaufbauten mehrerer Geräte zeitlich entzerrt werden. |
| Neue UMTS-Karten | Unterstützung der UMTS-Karten „Option GT 3G CDMA - HSDPA 7.2 Ready“ und „web ‘n’ walk ExpressCard II (Option GE0201)“ |
| Konfigurierbarer Reset-Taster | Das Verhalten des Reset-Tasters ist konfigurierbar (Reset & Boot, Boot only oder Ignore) zum Schutz von Geräten in öffentlich zugänglichen Bereichen |
| Bridge Gruppen | Schnittstellen wie Ethernet-Ports, SSIDs oder Punkt-zu-Punkt-Strecken können nun durch mehrere Bridges individuell miteinander verbunden werden. |
| **Neue Features LCOS 6.24** | |
| WLANmonitor | Neuer WLANmonitor mit Anzeige von allen in Funkreichweite befindlichen fremden Access Points (‘Rogue AP Detection’) und fremden Clients. Dargestellt werden unter anderem der verwendete Kanal, der Netzwerkname, die WLAN-MAC-Adresse, die Verschlüsselungsmethode sowie die Signalstärke bei denjenigen Access Points, von denen aus der fremde AP oder Client gesehen wurde. |
| WLAN Background Scanning | Die Erkennung von fremden Access Points und der Kanaleigenschaften erfolgt nahezu unmerklich durch einen kurzzeitigen Wechsel (wenige ms) auf alle anderen WLAN-Kanälen. Der normale Access Point Betrieb arbeitet dabei nahezu unbeeinflusst weiter. |
| WLAN Client Detection | Erkennung von fremden WLAN Clients (‘Rogue Clients’) anhand von Probe-Requests. |
| Fast Client Roaming | Durch das Background Scanning kann ein mobiler Access Point im Client-Betrieb bereits auf einen anderen Access Point mit stärkerem Signal wechseln, bevor die Verbindung zum aktuellen Access Point zusammenbricht. |
| WPA2 Fast Roaming | Pre-Authentication und PMK-Caching zur schnellen 802.1x Authentisierung |
| LED-Anzeige für WLAN-Signalqualität | Neben der Standardanzeige (Anzahl eingebuchter Clients) kann nun auch die Signalstärke einer Punkt-zu-Punkt-Strecke oder eines WLAN-Clients direkt am Gerät angezeigt werden, z.B. zum einfachen Einmessen einer Funkstrecke. |
| 802.1x Supplicant | Authentifizierung eines Access Points im WLAN-Client-Modus über 802.1x (EAP-TLS, EAP-TTLS und PEAP) bei einem anderen Access Point. |
| Automatische Sommerzeit | Die lokale Uhrzeit des intern mit UTC arbeitenden NTP-Moduls kann automatisch auf Sommerzeit gestellt werden. |
| Accounting Snapshot | “Snapshot”-Funktion zum regelmäßigen, exakten Auslesen der Werte (Verbindungs- und Onlinezeit sowie Übertragungsvolumen je Station) am Ende einer Abrechnungsperiode. |
| Public Key SSH | Zertifikatsbasierte SSH-Authentifizierung (alternativ zum PSK-Verfahren) |
| Proadaptive VPN | Automatische Konfiguration und dynamisches Anlegen aller notwendigen VPN- und Routingeinträge anhand eines Default-Eintrages bei Site-to-Site-Verbindungen. Das Propagieren der dynamisch gelernten Routen kann auf Wunsch per RIPv2 erfolgen. |
| VPN Certificate Requests | Erweiterte Cisco-Interoperabilität in zertifikatsbasierten IPSec-Installationen durch Unterstützung einer optionalen ‘CERTREQ’-Anfrage. |
| Neue VoIP Sprachcodecs | Optimale Sprachcodierung mit G.729a als “Low Bitrate Codec”, z.B. für WAN-Strecken über ADSL, sowie von G.722 als “High Quality Codec” zwischen ISDN und SIP. Diese neuen Codecs stehen für alle “VoIP integrated”-Geräte sowie für alle “VoIP ready”-Geräte mit “Advanced VoIP Option” zur Verfügung. |
| DTMF Tonwahl | Tonwahl-Unterstützung (DTMF) mittels RFC 2976 (SIP INFO) oder nach RFC 2833 (RTP Payload for DTMF Digits). |
| AOC Gebühreninformationen | Übertragung von Gebühreninformationen (AOC - ‘Advice of Charge’) zwischen den internen und externen ISDN-Schnittstellen bei den entsprechenden “VoIP integrated”-Produkten. Unterstützt werden zwei Varianten: AOC-D zur Übertragung während eines Gespräches, AOC-E zur Übertragung nach einem Gespräch. |

| Neue Features LCOS 6.10 | |
|---|---|
| ISDN-Anlagenanschluss | Zusätzlich zu den bisher unterstützen ISDN-Mehrgeräteanschlüssen (Punkt-zu-Mehrpunkt) werden nun auch ISDN-Anlagenanschlüsse (Punkt-zu-Punkt) unterstützt. Mehrere ISDN-Anlagenanschlüsse lassen sich zusammenfassen (Stammnummer und Durchwahlbereich). |
| SIP-Trunking | Mit SIP-Trunking (ITU Q.1912) kann ein entsprechender SIP-Account für mehrere Teilnehmer verwendet werden, die jeweils eine individuelle Durchwahl besitzen. |
| SIP Remote-Gateway | Die ISDN-Interfaces eines LANCOM-Routers mit VoIP-Funktion lassen sich als lokaler Ein- oder Auswahlpunkt, z.B. einer zentralen VoIP-TK-Anlage, zur Verfügung stellen. |
| Layer 2 / Layer 3 Tagging | Die Priorisierungsinformationen von 802.1p-VLAN-Frames auf dem Ethernet (Layer 2) können als Layer-3-Attribut (DiffServ) gesetzt werden, so dass eine Ende-zu-Ende-Übertragung von Priorisierungsinformationen über geroutete Strecken ermöglicht wird. Pakete von Endgeräten mit 802.1p-getaggten Frames werden automatisch mit 802.1p-Frames beantwortet. |
| 802.11e / WME | Unterstützung von Wireless LAN Quality-of-Service entsprechend den Wireless Multimedia Extensions (WME) für WLAN-Priorisierung. |
| RADIUS-Server | Die Access Control Liste (MAC-Adressfilter) eines WLAN-Access Points kann über den integrierten RADIUS-Server anderen Access Points zur Verfügung gestellt werden. |
| Certificate Revocation Lists | Zertifikate können über eine Sperrliste auch vor Ablauf gesperrt werden. LANCOM-VPN-Gateways mit CRL-Unterstützung können via HTTP die CRL einer Certificate Authority in regelmäßigen Abständen oder kurz vor Ablauf der Zertifikatslebensdauer abfragen. |
| RAS User Template | Alle VPN-Client-Verbindungen mit Zertifikaten und im Config-Mode können nunmehr über einen einzigen Konfiguratonseintrag (RAS User Template) bedient werden. Das Anlegen von Konfigurationsdaten pro Client entfällt. |
| USB-Druckerport | Zur Verwendung von USB-Druckern als Netzwerkdrucker. Unterstützung des RAW- und LDP-Protokolls. Bidirektionaler Datenaustausch z.B. zur Rückmeldung des Tonerstands. Parallele Druckaufträge werden auf den PCs gespeichert und der Reihe nach verarbeitet. |
| ISDN-Festverbindungen | Die bislang optionale Festverbindungsunterstützung ist ab dieser Version werksseitig für alle Geräte mit ISDN freigeschaltet. |
| Erweiterte UMTS-Unterstützung | In Verbindung mit der UMTS/VPN Option wird nun auch die “HSDPA-ready”-UMTS-Karte Option GT Fusion+ und Option GT max. unterstützt. (Nachtrag: Diese Option wurde mit LCOS 6.14 auf allen LANCOM 3550 Wireless standardmäßig aktiviert.) |
| **Neue Features LCOS 6.02** | |
| SIP-Proxy | Verwaltung lokaler SIP-Benutzer mit wahlweiser automatischer Registrierung/Authentisierung. Abbildung von Konten bei öffentlichen SIP-Providern zur gemeinsamen Nutzung. Anbindung an bis zu vier übergeordnete SIP-TK-Anlagen inklusive Leitungsbackup.<br>SIP-Verbindungen von/zu internen Teilnehmern, SIP-Providern und SIP-TK-Anlagen mit automatischer Anmeldung von SIP-Benutzern bei SIP-Providern/übergeordneten SIP-TK-Anlagen. Wahlweise gemeinsames/individuelles Passwort zur Authentifizierung an übergeordneter SIP-TK-Anlage. Automatisches Bandbreitenmanagement und automatische Konfiguration der Firewall für SIP-Verbindungen. Backup-Verbindungen über ISDN, wenn die SIP-Leitung nicht verfügbar ist, einstellbar im Voice Call Manager (VCM). Default DNS-Eintrag für die lokale SIP-Domäne, Unterstützung von Service Location Records (SRV) speziell für SIP. |
| SIP/ISDN-Gateway | Betrieb direkt an ISDN-Amtsleitungen oder an ISDN-Nebenstellenanschlüssen vorhandener TK-Anlagen. Anmeldung lokaler ISDN-Teilnehmer als lokale SIP-Benutzer sowie automatische Anmeldung lokaler ISDN-Teilnehmer als SIP-Benutzer an übergeordneten SIP-TK-Anlagen. Rufnummernumsetzung zwischen interner Rufnummer und MSN sowie automatische Anpassung der anrufenden und gewählten Rufnummer beim Übergang. ISDN-Dienstemerkmale CLIP, CLIR, Blockwahl und Einzelwahl mit einstellbarer Wartezeit für Nummernvervollständigung. |
| Voice Call Manager (VCM) | Zentrale Vermittlung für alle ankommenden und abgehenden Rufe. Rufnummernumsetzung mit Mapping, Ziffernsetzung und Nummernergänzung. Konfiguration der Leitungs- und Wegewahl, Angabe mehrerer alternativer Wege (Leitungs-Backup). Wegewahl abhängig von rufender und gewählter Rufnummer, SIP-Domäne und Leitung. Manuelle Wegewahl durch den Anwender (“Kennziffer für Amtsholung”), Wegewahl durch Leitungstasten an den Telefonen oder durch Rufnummern-Präfixe, gezielte Wegewahl für einzelne Rufnummern (z.B. Notrufe über lokalen ISDN-Anschluss), getrennte Wegewahl für interne, lokale, nationale oder internationale Anrufe, Sperrung von Rufnummern oder Rufnummernblöcken, Einbindung lokaler SIP- und ISDN-Teilnehmer in die Rufnummernkreise übergeordneter SIP-TK-Anlagen, Standard-Rufnummer für unzustellbare Anrufe, Ergänzung/Entfernung leitungsbezogener Wählpräfixe und Stammnummern. |
| VoIP Setup Assistent | Installations-Assistent in LANconfig für Anbindung an SIP-Provider, SIP-TK-Anlagen, SIP-Teilnehmern, ISDN-Teilnehmern und ISDN-TK-Anlagen und VCM-Konfiguration. |
| VoIP Monitoring | Zustandsanzeige der VoIP-Teilnehmern, Leitungen und Verbindungen; VoIP Trace auf dem Kommandozeileninterface. |
| VoIP Processing | G.168 Echo-Unterdrückung, adaptiver De-Jitter-Buffer, Inband Tone Signalling nach deutschem Standard, transparente Durchleitung ausgehandelter Codecs, Beeinflussung der Aushandlung von Codecs zwischen Teilnehmern (Filterung, Optimierung auf Bandbreite oder Sprachqualität), Sprachcodierung nach G.711 (a-law, u-law, 64 kBit/s) oder G.726 (16, 24, 32, 40 kBit/s). |
| VoIP Quality of Service | Angepasste QoS für Sprachverbindungen mit dynamischer Bandbreitenreservierung pro Verbindungn und automatischer Auswahl der Sprachkompression. Priorisierung (CoS) und DiffServ-Markierung von Sprachpaketen, Traffic-Shaping (eingehend/ausgehend) und Paketgrößenstuerung nicht-priorisierter Verbindungen gegenüber VoIP. |
| Erweiterte UMTS-Unterstützung | In Verbindung mit der UMTS/VPN Option wird nun auch die “HSDPA-ready”-UMTS-Karte Option GT 3G+ unterstützt (z.B. T-Mobile “Mobile DSL Card”) |
| **Neue Features LCOS 5.20** | |
| ADSL2+ | Bis zu 24 MBit/s Downstream-Geschwindigkeit ermöglicht der ADSL2+ Standard nach ITU G.992.5. Durch Software-Update auf den in LCOS 5.20 enthaltenen neuen ADSL-Linecode können die Produkte LANCOM 821+, LANCOM 1721 VPN und LANCOM 1821 Wireless ADSL (1821 ab HW Release E) entsprechend ADSL2+-fähig gemacht werden. |

| | |
|---|---|
| VRRP | Mit VRRP (Virtual Router Redundancy Protokoll) steht ein nach RFC 3768 herstellerübergreifend standarisiertes Redundanz-Protokoll zur Verfügung. Mehrere VRRP-fähige Geräte können zu einer Standby-Gruppe zusammengefasst werden, wobei i.d.R. ein Gerät als aktiver Master die Verbindungen hält. Durch die Virtualisierung der MAC- und IP-Adresse des VRRP-Masters als Default-Gateway können Netze mit redundanten Routern abgesichert werden, ohne dass Änderungen an im LAN notwendig sind. Neben Geräteausfall kann die VRRP-Funktion bei LANCOM auch an die Erreichbarkeit einzelner Gegenstellen bzw. an die Funktionlität von Leitungen oder Interfaces gebunden werden. Ferner können auch mehrere Geräte parallel aktiv im Load-Balancing betrieben werden, die sich jeweils gegeinseitig absichern. Durch die kurze Propagationszeit (Standardwert 1s) und die Virtualisierung des Default-Gateways wird eine extrem schnelles, transparentes Failover erreicht. |
| NAT-T | Durch NAT-Traversal wird das Einsatzgebiet von IPSec VPNs auch auf Strecken erweitert, wo Router ohne VPN Pass-Through-Funktion betrieben werden. Durch eine automatische Überprüfung im Rahmen der IKE-Verhandlung wird die Konsistenz des TCP/IP-Headers von ESP-Paketen geprüft. Im Bedarfsfall wird ein solches ESP-Paket mit einem weiteren, umgebenden IP-Header versehen, so dass die VPN-Verbindung nicht mehr durch Geräte ohne korrekte IPSec-Maskierung gestört werden kann. |
| Neue UMTS-Karten | Mit LCOS 5.20 und aktivierter UMTS/VPN-Option unterstützt der LANCOM 3550 Wireless nunmehr folgende UMTS-Datenkarten: Novatel Wireless U530 und U630, Option GT 3G Fusion und Option GT 3G Quad. |
| IEEE 802.11h | Zur Nutzung der maximal zuässigen Sendeleistung von 1000mW bei 5 GHz WLAN-Strecken unterstützt LANCOM bereits seit geraumer Zeit die dafür in Europa notwendigen Mechanismen TPC und DFS nach ETSI-Standard. Durch den IEEE-Standard 802.11h wird diesen Verfahren nun ein verbessertes Kanalwechselverhalten zur Seite gestellt. |
| HTTPS Fernkonfiguration | LANconfig unterstützt jetzt auch die verschlüsselte Fernkonfiguration über HTTPS. Dabei können Konfigurationsupdates oder der Upload von Scripten oder Firmwares mit einer AES 256 Bit Verschlüsselung geschützt werden. Für Fernwartung ohne Verschlüsselung (z.B. bei ISDN-Direkteinwahl oder innerhalb eines VPNs) kann nun ebenfalls HTTP alternativ zu TFTP als Kommunikationsprotokoll Verwendung finden, wodurch sich eine schnellere Datenübertragung beim Remote Management ergibt. |
| PPPoE Server | Zu zur Layer-2-Authentisierung von Benutzern oder Benutzergruppen mittels PPPoE-Clients steht nun auch eine PPPoE-Server-Funktion zur Verfügung. |
| WLAN Bandbreitenlimitierung | Die maximal zulässigen WLAN Sende- und Empfangsraten können pro WLAN Client limitiert werden |
| LAN / DMZ Intrusion Prevention | Die IP-Adressüberprüfung des Intrusion Detection Moduls kann nun auch auf LAN- und DMZ-Interfaces bzw. die zugeordnete Netzwerkzone angewendet werden. In der Einstellung “strict” werden nur dem Interface zugeordnete IP-Adressen akzeptiert. |
| Spanning Tree | Zum Einsatz von Ethernet-Geräten in beliebig vermaschten Netzen wird das Spanning Tree Protokoll unterstützt, so dass damit redundante Pfade ohne unerwünschte Schleifen gebildet werden können. |
| VLAN-ID pro Client | Pro WLAN-Client kann eine separate VLAN-ID zugewiesen werden. |
| DHCP-Client-IDs | Das LANCOM kann als DHCP-Client in den versendeten DHCP-Requests als Vendor-Class-Indentifier den Gerätenamen übermitteln. Als User-Class-ID können benutzerspezifische Informationen übermittelt werden. |
| WAN-RIP Propagierung | Über RIP gelernte dynamische Routing-Einträge können nun auch über das WAN propagiert werden. Pro Gegenstelle kann optional die Art der Maskierung vorgegeben werden sowie ein optionales Routing-Tag angegeben werden. |
| **Neue Features LCOS 5.00** | |
| X.509 Digitale Zertifikate | Mehr Sicherheit für IPSec VPNs: Ab sofort können digitale Zertifikate für LAN-LAN-Kopplung und VPN-Client-Einwahlzugänge verwendet werden. Unterstützt werden selbstsignierte PKCS#12 Softzertifikate, beispielsweise erstellt vom Microsoft Zertifikatsdienst (Server oder Enterprise Server) oder OpenSSL. Gegenüber dem Preshared-Key-Verfahren ergeben sich einige Vorteile:<br>VPN Clients können mit Zertifikaten im sichereren IKE Main Mode betrieben werden<br>Gegenseitige Verifikation der Zertifikate<br>Weitere Info-Elemente im Zertifikat möglich wie Firma, Organisationseinheit usw.<br>Zeitlich befristete Gültigkeit<br>Keine ‘simplen’ Passwörter mehr – Unterbindung von Wörterbuchangriffen<br>Unterstützung von Smartcards und Tokens – Auslesen von Passwörtern aus Notebooks/PCs verhindert<br>Integration in Active Directory Umgebungen – zentrales Rechtemanagement<br>Die PKCS#12-Dateien mit Root-Zertifikat, Geräte-Zertifikat und Private Key können mit WEBconfig über https in die Geräte eingespielt werden. Beim LANCOM Advanced VPN Client steht eine Importfunktion zur Verfügung. |
| AES-256 und IPCOMP | Die Bit-Tiefe bei der AES-Verschlüsselung kann jetzt neben 128 auch 192 oder 256 bit betragen. Die Hardware-AES-Beschleunigung der entsprechenden Modelle bleibt dabei erhalten. Die Blowfish Verschlüsselungstiefe kann nunmehr bis zu 448 bit betragen. IPCOMP dient zur Datenkompression im VPN-Tunnel. Der Datendurchsatz im VPN-Tunnel kann mit den Kompressionsalgorithmen LZS und Deflate beschleunigt werden. |
| Load Balancing | Je nach Modell können bis zu 4 externe DSL-Modems oder Netzabschlussrouter direkt an freie Switch Ports als zusätzliche WAN-Ports angeschlossen werden. Durch die automatische optimale Lastverteilung kann durch einfaches “Dazustecken” weiterer Breitbandanschlüsse die verfügbare Übertragungsleistung gesteigert werden. Ferner ergibt sich eine vollwertige Redundanz bei Ausfall einer oder mehrerer Leitungen. |
| ML-PPP | Bis zu 4 PPPoE-Strecken (z.B. Leitungen mit DSL-Modems) können per Kanalbündlung zusammengefasst werden. So steigt nicht nur die Übertragungskapazität, sondern auch die effektive maximale Geschwindigkeit. So können z.B. 4 PPPoE-basierte SHDSL-Anschlüsse mit je 2 Mbit zu einem 8 Mbit-Anschluss zusammengefasst werden. |
| Konfigurierbare Switch Ports | Die Verwendung der Switch Ports kann bei vielen Modellen jetzt frei programmiert werden. Zur Auswahl stehen die Betriebsarten ‘Aus’, LAN-Port, separater DMZ-Port, WAN-Port (für zusätzliche WAN-Ports beim Load Balancing) und Monitor-Port. Bei letzterem kann für Diagnosezwecke der Traffic aller Ethernet LAN- und WAN-Ports ausgegeben werden. |
| Policy-based Routing / Tags | Die Firewall kann mit beliebigen Triggern und Regeln ein sog. ‘Tag’ an bestimmte Datenpakete heften. Diese frei zuweisbaren Tags werden in der erweiterten Routing-Tabelle ausgewertet. Somit ergibt sich eine völlige Flexibilität des bislang rein auf Zieladressen basierenden Routings. Im Falle von Load Balancing ergibt sich z.B. die Möglichkleit, bestimmte Dienste wie VoIP, VPN oder Email nur über ganz bestimme Leitungen auszugeben. Ja nach Art der Daten können auch mehrere Default-Routen angesprochen werden, beispielsweise in Abhängigkeit von der Absenderadresse, der DiffServ-Markierung oder anhand des verwendeten Protokolls. |

| | |
|---|---|
| WLAN Gruppenkonfiguration | In LANconfig können zur einfachen Administration mehrere WLAN Access Points zentral konfiguriert werden. Einem Gruppenordner kann eine Gruppenkonfiguration zugewiesen werden, in der die für alle Geräte der Gruppe identischen WLAN-Parameter wie z.B. Verschlüsselung und Access Control Listen zentral definiert sind. Änderungen an der Gruppenkonfiguration werden an alle in der Gruppe befindlichen Geräte verteilt. Etwaige Abweichungen von den Gruppeneinstellungen werden erkannt und ein automatisches Update angeboten. Per Drag and Drop können einfach zusätzliche Geräte in eine Gruppe integriert werden oder aber von einem Gerät abgeleitet werden. |
| WLANmonitor | Die zentrale Überwachung von WLAN-Installationen wird mit dem neuen WLANmonitor zum Kinderspiel. Für alle WLAN Geräte werden die eingebuchten Clients angezeigt, ebenso wie die verwendeten Funkkanäle, die Verschlüsselungseinstellungen und die aktuelle Signalqualität und Übertragungsrate. Einfaches Clicken auf einen Client markiert den Access Point, auf dem der Client aktuell eingebucht ist. Nicht authentisierte Clients werden unter Angabe des Fehlergrundes rot markiert. |
| Scripting | Mit dem neuen Scripting-Interface können beliebige Kommandozeilenparameter in Script-Dateien übertragen werden.<br>Die Vorteile des Sptings sind:<br>Erstmals können auch Teilbereiche von Konfigurationen übertragen werden - z.B. nur Firewall-Einstellungen, Access Control Listen, VPN-oder DHCP/DNS-Einstellungen<br>Scripte können über SW-Versionen und unterschiedliche Gerätetypen übertragen werden<br>Batch-Programmierung aller LANCOM Funktionen erlaubt neue Anwendungen wie z.B. einen "Testmodus" für Parameter-änderungen mit Hilfe der "Flash off"- und "Sleep"-Befehle<br>Scripte sind einfach lesbar, übersichtlich und kompakt da nur vom Default abweichende Werte enthalten sind.<br>Scripte enthalten sind mit jedem Texteditor zu bearbeiten und enthalten LANCOM Kommandozeilenbefehle im Klartext.<br>Sogar Kommentare werden automatisch generiert.<br>Über Loadscript auf der Kommandozeile oder per LANconfig Kontextmenü können Scripte geladen werden. Über den neuen Readscript Befehle können alle zur Konfiguration getätigten Befehle unterhalb eines Menüpfades ausgegeben werden. |
| Lösch-Assistent | LANconfig verfügt nun über einen Assistenten zum vollständigen Entfernen nicht mehr benötigter Verbindungen und Gegenstellen inklusive aller zugehörigen Konfigurationseinträge. |
| ISDN Standortverifikation | Einbruchsschutz bei Gerätediebstahl – Router mit ISDN-Interface können sich selbst anrufen um festzustellen, ob sich der Router am vorgesehenen Standort befindet. Schlägt die Überprüfung fehl, so verharrt das Gerät im gesperrten Zustand, so dass keine Datenübertragung z.B. zu einem konfigurierten VPN-Firmenzugang möglich ist. |
| Wake-up on LAN | Unterstützung von Gerätefernaktivierung / Remote PC Wake-up mit entsprechender Broadcast-Verteilung der Aktivierungspakete. |
| Transparenter WLAN Client-Modus | Beim Betrieb eines LANCOM Access Points als WLAN Client steht ein MAC-transparenter Modus zur Verfügung.<br>Damit sind auch in der Client-Betriebsart MAC-Adressbasierte Authentisierungen möglich. |
| DFS Blacklists / Whitelists | In 5 GHz WLANs konnten die DFS-Kanalwechselzeiten durch Pflege von Listen geeigneter Kanäle optimiert werden. |
| TFTP Dateinamen mit Variablen | Für einfache Software-Verteilungen z.B. von individuellen Gerätekonfigurationen und Scripten können in den Dateinamen des integrierten TFTP Servers und Clients Variablen für die jeweilige MAC- oder IP-Adresse, die Seriennummer oder den Namen des Gerätes enthalten sein. |
| **Neue Features LCOS 4.12** | |
| UMTS-Unterstützung | Im externen Cardbus-Slot der Modelle LANCOM 3550 / 3050 Wireless kann in Verbindung mit der neuen LANCOM UMTS/ VPN Option eine UMTS-Datenkarte betrieben werden. Unterstützt werden derzeit ausschließlich die UMTS/GPRS-Datenkarten U-530 und U-630 des Herstellers Novatel Wireless. Damit können UMTS-basierte Breitbandzugänge realisiert werden oder ein 'mobiler Konferenzraum', wo über UMTS und VPN ein WLAN- oder LAN-Zugang zum eigenen Firmennetz überall realisiert werden kann. Ferner ist UMTS ideal als Backup geeignet, da es mehr Geschwindigkeit bei besserer Ausfallsicherheit und niedrigeren Bereitstellungskosten als eine klassische ISDN-Absicherung einer DSL-Strecke bietet. Im Rahmen der UMTS/VPN werden gleichzeitig 5 VPN Tunnel auf dem UMTS/WLAN-Router aktiviert. |
| **Neue Features LCOS 4.00** | |
| LEPS – Erweiterte WLAN-Sicherheit | Mit dem neuartigem LANCOM Enhanced Passphrase Security Verfahren (LEPS) besteht erstmals die Sicherheit Möglichkeit, auch ohne aufwändige 802.1x Infrastruktur jedem einzelnen WLAN-Nutzer eine separate WPA Passphrase zuzuordnen. Bisher musste entweder jedem WLAN-Client die gleiche Passphrase gegeben werden (einhergehend mit der Notwendigkeit, alle WLAN-Clients bei jedem Mitarbeiterwechsel manuell neu zu konfigurieren), oder aber zwingend eine 802.1x Infrastruktur mit einem EAP-fähigen (Extended Authentication Protokoll) RADIUS Server betrieben werden. LEPS ist einfach und genial zugleich:<br>Pro MAC-Adresse kann ein LANCOM Access Point jeweils eine individuelle Passphrase verwalten. Nur wenn die zur jeweiligen MAC-Adresse passende Passphrase verwendet wird, ist ein WLAN Zugang möglich. LEPS funktioniert mit allen WPA / 802.11i-fähigen WLAN Clients. Die Access Control Liste mit den zugelassenen MAC-Adressen und individuellen Passphrases kann im LANCOM Access Point hinterlegt werden, oder in einem beliebigen Standard RADIUS Server. |
| WLAN Hardware-Datenkompression | Alle 54 MBit LANCOM Access Points und 54 Mbit AirLancer Client-Adapter können ab sofort die integrierte Hardware-Daten-kompression nutzen. Dadurch steigt die effektive Datendurchsatzrate in Verbindung mit Bursting und Turbo Modus von 40 Mbit/s (Standard: 20 auf 30 Mbit/s) auf nunmehr bis zu 60 Mbit/s – auch bei gleichzeitiger AES-Verschlüsselung. |
| 802.11i für WLAN P2P-Strecken | Jetzt können auch Punkt-zu-Punkt WLAN-Funkstrecken die integrierte AES Hardwareverschlüsselung der LANCOM 54 Mbit Funk-module nutzen. In Verbindung mit dem WLAN Turbo-Modus und bis zu 1000mW Sendeleistung im 5 GHz Band (802.11a) können dank 802.11i abhörsichere Funkverbindungen bei bis zu 108 MBit/s über Entfernungen im Kilometerbereich betrieben werden. |
| Default-Verschlüsselung für WLAN | Im Auslieferungszustand und nach einem Reset ist eine gerätespezifische WLAN-Verschlüsselung aktiviert. Damit wird ein Mindest-schutz auch bei "vergessenem" Ausführen der Installations- und Sicherheitsassistenten sowie nach einem Reset geboten. Der 13-stellige Default WEP128-Schlüssel setzt sich aus der 12-stelligen MAC-Adresse des Gerätes und einem vorangestelltem "L" zusammen. |
| Redundante VPN Gateways | Ansteuerung mehrerer VPN-Endpunkte (i.d.R. gleich konfigurierte, parallel betriebene zentrale VPN Gateways) für Hochverfügbarkeit und zur gleichmäßigen Lastverteilung in größeren VPN-Installationen (VPN Load Balancing, High Availability). Sobald die Leitungsüberwachung (Dead-Peer-Detection oder ICMP Line Polling) fehlschlägt, kann nach verschiedenen Strategien (z.B. "Random") ein neuer VPN Endpunkt angesprochen werden. Zentralseitig wird eine neue "Outbound" Route und das lokale Default Gateway über dynamisches Routing (RIP V2) propagiert. |
| IKE Config Mode | Automatische Zuweisung von IP-Adressen an VPN-Gegenstellen, z.B. an den LANCOM Advanced VPN Client. |

| | |
|---|---|
| Mehrere Administrationszugänge | Mehrere Administratoren können mit individuellen Passwörtern und Rechten auf das Gerät zugreifen. Das bisherige Gerätepasswort bleibt als "Supervisor" erhalten. Unter WEBconfig, telnet, TFTP und SNMP stehen erweiterte Login-Funktionen zur Verfügung. Bis zu 16 Rollen mit unterschiedlichen Berechtigungen zur Gerätekonfiguration und zum Ausführen von Funktionen können definiert werden. |
| SSH Konfigurationszugang | Unterstützung des SSH-Protokolls als weiterem verschlüsseltem Zugangsweg zum Kommandozeileninterface, z.B. mit dem frei verfügbarem "PuTTY"-Tool (telnet über SSH-Client, für Windows- und Unix-Betriebssysteme). |
| Port-Mapping | Ermöglicht ein frei einstellbares Port-Remapping, z.B. um lokale Server auf nicht standardisierte Ports umzulegen. |
| Multi-PPPoE | An einem DSL-Zugang können jetzt auch mehrere Internetzugänge von unterschiedlichen Internet Sevice Providern betrieben werden. Mehrere PPPoE-Sessions können z.B. für ein ISP-Backup, oder für eine getrennte Abrechnung von geschäftlichem und privatem Internetzugang genutzt werden. |
| RIP via WAN | Die Propagierung von statischen oder dynamischen Routen mittels RIP V2 kann nun auch in das WAN erfolgen, beispielsweise zur Aktualisierung von Routen innerhalb geschlossener Netze wie z.B. MPLS-basierter VPNs. |
| Manuelle MTU-Definition | Zusätzlich zur automatischen Anpassung der maximalen Paketgröße auf einer bestimmten Übertragungsstrecke kann dieser Wert jetzt auch statisch überschrieben werden. Dies ist z.B. notwendig für bestimmte Internet Service Provider, die über getunnelte Verbindungen ein Reselling von DSL-Aschlüssen betreiben. In diesem Fall führt die automatische MTU-Aushandlung mit dem DSL Access Provider zu einem zu großen MTU Wert (z.B. 1492), da der Tunnel zum ISP u.U. zusätzlichen Overhead mit sich bringt. In solchen Fällen kann die MTU entsprechend manuell reduziert werden (z.B. auf 1400 Byte). |
| "Loopback" Adressen | Dem Gerät können bis zu 16 weitere IP-Adressen zugewiesen werden, unter denen das Gerät eindeutig angesprochen werden kann (z.B. zur Wartung von Geräten in mehreren Netzen mit gleichen IP Adresskreisen) |
| Internes Logging | Zusätzlich zum bereits vorhandenem Firewall Eventlog können jetzt auch beim aktiviertem SYSLOG Modul die letzten 100 SYSLOG Meldungen direkt im Gerät eingesehen werden, z.B. als "Fehlerspeicher" zur Ferndiagnose nach Verbindungsabbrüchen. |
| Software Versionsmanagement mit LANconfig | Einfaches Versionsmanagement durch Firmware-Archiv mit Update-Funktion. Entweder zum mit LANconfig komfortablen zentralen Update von Installationen mit unterschiedlichen Gerätetypen, oder auch zum gezielten "Rollback". |
| Neuer LANmonitor | Jetzt mit Button-Leiste zum direkten Funktionsaufruf und neuem Fenstermanagent zur Überwachung größerer Installationen. |
| Analog- und GPRS-Modem | Durch den Anschluss eines externen Analog- oder GSM/GPRS-Modems an der seriellen Schnittstelle ('Config/COM') steht ein zusätzlicher, vollwertiger WAN-Zugang bereit. Alle Funktionen wie Haltezeit, automatische Rückkehr zur Hauptverbindung beim Einsatz als Backup oder die Bereitstellung von Einwahlzugängen z.B. für Fernwartung können genutzt werden. Selbst Dynamic VPN Anwendungen mit Übermittlung von IP-Adressen per Anruf sind möglich. Individuelle Modem-Parameter können über AT-Befehlssätze konfiguriert werden. Leitungszustand und Connect-Raten werden übersichtlich im LANmonitor dargestellt. Aufgrund anderer Beschaltung als beim Einsatz als Konfigurationsschnittstelle ist das LANCOM Modem Adapter Kit zum Betrieb von externen Modems erforderlich. |
| Erweiterte Polling-Adresssen | Zur End-to-End Verbindungsüberwachung mittels ICMP-Polling ('ping') stehen nunmehr bis zu 4 Prüfadressen zur Verfügung. Der Backup-Fall wird nur dann ausgelöst wenn keine der zu prüfenden Adressen mehr erreicht werden kann. |
| WLAN P2P-Strecken mit 802.11i | Die integrierte AES-Verschlüsselung der WLAN-Funkmodule kann nun auch für WLAN Punkt-zu-Punk-Strecken verwendet werden. |
| N:N Mapping für alle Geräte | Vormals nur für VPN-fähige Geräte implementiert, steht nun auch die N:N IP-Adressumsetzung für Geräte ohne VPN zur Verfügung –beispielsweise um in MPLS-Netzten Standorte mit gleichen integrieren zu können. |
| CPU-Load- und Speicheranzeige | LANmonitor zeigt in den Systeminformationen unter 'Gerät' weitere Informationen wie CPU-Typ und -Geschwindigkeit, die Speicherausstattung sowie die momentane Speicherauslastung an. |
| Erweiterter Ping-Befehl | Die neue -a Option ermöglicht das Setzen einer dedizierten Absenderadresse (z.B. Intranet, DMZ oder frei einstellbar). Damit lässt sich bereits bei der Inbetriebnahme des Gerätes die korrekte Funktionsweise des Routers für alle zu routenden Netze vorab testen. |
| Erweiterte Kommentarfelder | Um die bisherigen allgemeinen Geräteinformationen wie Gerätename, Standort und Administrator beliebig erweitern zu können stehen nun vier frei definierbare Kommentarfelder zur Verfügung. |
| **Neue Features LCOS 3.50** | |
| WLAN | Mit LCOS 3.50 steht ein WLAN-Sicherheits-Update für alle LANCOM WLAN-Router, Access Points und AirLancer Client Adapter mit 54 Mbit/s Funkmodulen bereit. Die Verschlüsselung kann durch 802.11i/AES oder WPA/TKIP erfolgen, wobei mit AES eine Sicherheit nach Behördenstandard FIPS 140-2 gewährleistet werden kann. Die LANCOM 54 Mbit Funkmodule verfügen bereits über ein integriertes Hardware-Verschlüsselungsmodul, so dass die AES-Verschlüsselung ohne Performance-Einbußen genutzt werden kann. Durch die Verwendung von WPA-Passphrasen ergibt sich eine deutliche komfortablere Einrichtung im Vergleich zu WEP. |
| **Neue Features LCOS 3.42** | |
| Multi-SSID | Pro WLAN-Funkmodul können jetzt bis zu 8 unterschiedliche Funkzellen (SSIDs) aufgespannt werden. Pro SSID können individuell alle Sicherheits- und Zugangseinstellungen getrennt voneinander konfiguriert werden. So kann z.B. neben einem privaten WLAN Intranet gleichzeitig ein getrennter, öffentlicher WLAN Hot Spot-Zugang bereitgestellt werden. |
| Super A/G | Zur Steigerung der Übertragungsraten in 2.4 und 5 GHz WLANs. Der 108 Mbit Turbo Modus bündelt zwei freie WLAN-Kanäle und verdoppelt somit die effektive Bandbreite. Durch Bursting werden mehrere Pakete zusammengefasst. Für Punkt-zu-Punkt-Strecken zwischen zwei Access Points kann eine Hardware-Datenkompression eingesetzt werden. |
| VPN-Triggerruf | VPN-Verbindungsaufbauten zu einer festen Gegenstelle können nun auch über einen ISDN-Datenanruf getriggert werden. |
| ISDN-Backup für Dynamic VPN | Waren bislang ISDN-Backupfunktionen nur begrenzt in Verbindung mit Dynamic VPN nutzbar, so entfällt nunmehr diese Einschränkung vollständig. So kann jetzt auch eine Dynamic VPN Verbindung mit beidseitig dynamischen IP-Adressen mit einer ISDN-Direktwählverbindung abgesichert werden. |
| IP-Redirect | Zur Vorgabe dedizierter Übergangspunkte vom Wireless LAN zum drahtgebundenen LAN können pro SSID alle über das WLAN eingehenden Datenpakete zwangsweise auf genau eine einstellbare IP-Adresse umgeleitet werden |

| **Neue Features LCOS 3.32** | |
|---|---|
| VPN-Upgrade | Kostenfreies und rückwirkendes Upgrade auf 5 VPN-Kanäle für alle Geräte der 16xx und 18xx Serie! Aufwertung der bisherigen VPN-2 Option auf 5 Kanäle |
| QoS | Erweiterte Quality-of-Service-Funktionen z.B. für optimale Voice-over-IP Sprachqualität über VPN-Verbindungen. Zusätzlich zum sendeseitigen Bandbreitenmanagement stehen folgende Funktionen zur Verfügung:<br>Extended IP QoS<br>Dynamisches „Einbremsen" von Downloads:<br>Automatische Paketgrößenanpassung und einstellbare PMTU oder Fragmentierung zur Jitter-Reduzierung (insbesondere bei niedrigen ADSL Upstream-Bandbreiten)<br>DiffServ-Trigger im IP-Router und in der Firewall |
| Virtuelle LANs (VLANs) | Mit VLAN können auch getrennte Netzwerke eine gemeinsame Infrastruktur nutzen<br>VLAN-ID verbindet zusammengehörige Segmente<br>VLAN-Priorität für Quality-of-Service<br>VLAN-fähige Switche konvertieren normales Ethernet in das VLAN-Segment und zurück |
| N:N IP-Mapping | IP-Adressumsetzung eines Netzes auf einen anderen Adressbereich<br>VPN-Netzwerkkopplung auch mit identischen IP-Netzen<br>Zur Erzeugung eindeutiger Management-Adressen („Loopback-Adressen")<br>Zentrales Netzwerkmanagement mehrere Netze mit gleichen Adressbereichen |
| LANconfig/LANmonitor | Multitasking – bequeme Verwaltung ganzer Projekte (z.B. zentrales Firmware-Update), Zusammenfassen und Gruppieren von Geräten, Aufzeichnen der Änderungshistorie Echtzeit-Fernüberwachung per SNMP-Trap Überwachung aller relevanten VPN-, WLAN-, Verbindungs-, Security- und Geräte-Ereignisse Protokollieren aller Statusänderungen, Transfervolumina und Verbindungszeiten |

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

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 Produkteigenschaft. Der Herausgeber behält sich vor, diese jederzeit ohne Angaben von Gründen zu ändern. Keine Gewähr für technische Ungenauigkeiten oder Auslassungen. 11/2026

ROHDE&SCHWARZ
Make ideas real