RELEASE NOTES

LCOS
10.92 RU8

Table of contents

02 **1. Preface**

02 **2. The release tag in the software name**

03 **3. Device-specific compatibility to LCOS 10.92**
03 R&S®LANCOM devices without support as of LCOS 10.92

03 **4. Advices regarding LCOS 10.92**
03 General notes on the update
03 Information on default settings

04 **5. Feature overview LCOS 10.92**

04 **5.1 Feature highlights**
04 Cloud-based network security with the R&S®LANCOM Security Essentials Option

05 **6. History LCOS 10.92**
05 LCOS improvements 10.92.0473 RU8
06 LCOS improvements 10.92.0413 RU7
07 LCOS improvements 10.92.0346 RU6
08 LCOS improvements 10.92.0325 RU5
10 LCOS improvements 10.92.0278 RU4
12 LCOS improvements 10.92.0227 RU3
14 LCOS improvements 10.92.0167 RU2
15 LCOS improvements 10.92.0098 RU1
17 LCOS improvements 10.92.0018 Rel

19 **7. General advice**
19 Disclaimer
19 Backing up the current configuration
19 Using converter firmwares to free up memory

ROHDE&SCHWARZ
Make ideas real

1. Preface

The LCOS family of operating systems—LCOS, LCOS SX, LCOS LX, and LCOS FX—forms the trusted basis for the entire R&S®LANCOM range of products. Within the scope of the hardware specified by the products, the latest firmware version is available for all R&S®LANCOM products and is offered by Rohde & Schwarz Networks and Cybersecurity for download free of charge.

Rohde & Schwarz Networks and Cybersecurity keeps program libraries used in LCOS firmware up to date with the latest security patches and fixes security vulnerabilities even if they cannot be exploited in the firmware.

This document describes the innovations within LCOS software release 10.92 RU8, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 7 „General advice“ of this document.

Latest support notes and known issues regarding the current LCOS version can be found in the support area of our website.

2. The release tag in the software name

Release Candidate (RC)

A Release Candidate has been extensively tested by Rohde & Schwarz Networks and Cybersecurity and includes new LCOS featurses. It is suitable for testing and is not recommended for use in productive environments.

Release Version (REL)

The release version has been extensively and successfully tested in practice. It contains new features and improvements over previous operating system versions and is therefore recommended for use in productive environments.

Release Update (RU)

A release update is a further development of an initial release version in productive environments and contains minor improvements, security fixes, bug fixes and smaller features.

Security Update (SU)

Contains important security fixes for the respective operating system version and ensures that your security level remains very high on an ongoing basis in your productive environment.

3. Device-specific compatibility to LCOS 10.92

R&S®LANCOM products regularly receive major firmware releases throughout their lifetime which provide new features and bugfixes.
LCOS release updates including bugfixes and general improvements are available on a regular basis for devices which do not support the latest LCOS version. You can find an overview of the latest supported LCOS version for your device here.

R&S®LANCOM devices without support as of LCOS 10.92

- R800V
- LN-630acn
- 1781VA
- 1906VA-4G
- L-322agn (R2)
- LN-862
- LN-860
- OAP-830
- OAP-1700B
- OAP-821
- OAP-822
- IAP-1781VAW(+)

4. Advices regarding LCOS 10.92

General notes on the update

As of LCOS 10.90, the CLI menu for VRRP has been moved from '/Setup/IP-Router/VRRP/' to '/Setup/VRRP/'. The table structure and the associated OID path have also changed due to the support for VRRPv3 and IPv6.
Please note that add-ins for the R&S®LMC and any existing scripts for VRRP must be adapted for LCOS 10.90 and higher. Existing scripts for VRRP are not compatible with LCOS 10.90 and higher.

Information on default settings

Devices delivered with LCOS 10.00 or higher automatically connect to the R&S®LANCOM Management Cloud (R&S®LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the R&S®LMC, this feature can be disabled while running the default setup wizard for the initial configuration, or at any time from within LANconfig under Management > LMC. You can manually re-enable the usage of the R&S®LMC whenever you want.

5. Feature overview LCOS 10.92

5.1 Feature highlights

Cloud-based network security with the R&S®LANCOM Security Essentials Option

With LCOS 10.92, you fulfill all the requirements to upgrade your devices with the R&S®LANCOM Security Essentials Option. The R&S®LANCOM Security Essentials Option provides an efficient and reliable solution to protect networks against threats such as ransomware, phishing, malware, and credential theft. The integrated Content Filter effectively blocks unwanted and illegal internet content – preserving corporate integrity and significantly reducing liability risks. At the same time, the BPjM module of the German Federal Review Board for Media Harmful to Minors (BzKJ) reliably shields minors from harmful content. The underlying database used to verify website content is hosted in a GDPR-compliant cloud provided by European security specialist Bitdefender. For maximum scalability, use of the option is not limited to a specific number of users – making it ideal for growing networks.

Note: The R&S®LANCOM Security Essentials Option is available as an upgrade for R&S®LANCOM SD-WAN gateways, SD-WAN central site gateways, and WLAN controllers as the successor product to the R&S®LANCOM Content Filter.

You can find further features within the individual builds sections in chapter 6 „History LCOS 10.92".

6. History LCOS 10.92

LCOS improvements 10.92.0473 RU8

Note

- Since server-side service adjustments are being made, to ensure that the R&S®LANCOM Security Essentials Option continues to function properly, you must install an update to LCOS 10.92 RU8 (or later) or LCOS 10.94 RU5 (or later) by January 1, 2027.

Bug fixes

General

- When calculating the exact position of the 'Authentication Digest' in the OSPF extension, OSPF extensions with additional data fields (e.g., RFC 5613 Link-Local Signaling) were not taken into account, resulting in the 'Authentication Digest' being calculated incorrectly. If a router in the OSPF community used extensions with additional data fields, this caused authentication to fail on that router.
- If a router with two Internet connections (a primary connection using dual-stack and a backup connection using IPv4) switched to the backup connection, the router was unable to resolve DNS targets (e.g., for VPN connections) that could be resolved using both IPv4 (A) and IPv6 (AAAA).
- In WEBconfig, the # character could not be included in the name of a blacklist or whitelist, so it was not possible to configure blacklists or whitelists with names longer than 254 characters.
- The maximum number of blocks in the buffer memory for a QoS rule specifying a maximum bandwidth was set too low. This could cause downloads to be very slow or even to stop entirely.
- OpenSSL has been updated to version 3.0.23.

VPN

- When the Create-Routes-For-RAS-SAs function is used, the router automatically creates VPN rules (SAs) for RAS dial-in connections (enabled by default). If this function was enabled in a scenario with an IKEv2 RAS dial-in connection using RADIUS and BGP, the router withdrew the prefix for the RAS dial-in connection and reported this to the BGP peer ("withdrawn routes"), even though the prefix had not yet been advertised to the BGP peer. The router advertised the prefix immediately after establishing the VPN interface.
  Withdrawn prefixes are no longer reported to the BGP peer if they have not yet been sent to the peer.

LCOS improvements 10.92.0413 RU7

Note

- The 10.92 RU7 firmware for the R&S®LANCOM 1803VA-4G has build number 10.92.0414 instead of 10.92.0413.

Bug fixes

General

- If an xDSL connection had been established via the built-in xDSL modem, configuration changes to that interface were not applied.

VPN

- The router's VPN module terminated the accounting session of an IKEv2 connection with RADIUS authentication and RADIUS accounting (ACCOUNT-Stop) when a second connection attempt using the same login credentials was rejected (RADIUS-Reject), because a connection already existed and another one was not permitted (no multi-login). However, because the accounting session had been terminated, a second connection using the same login credentials could subsequently be established.
  The accounting session is no longer terminated after a failed connection attempt.

VoIP

- After a change to the SIP server, there were instances where the Voice Call Manager did not adopt the value for the ‚Min-Expires' header in the VoIP provider's ‚423 Interval Too Brief' message. This caused the SIP registration to fail.

LCOS improvements 10.92.0346 RU6

Bug fixes

General

- If an SSH session or a CLI tunnel to a router (jump host) was started and an SSH session to another router was initiated from that router, transferring large amounts of data could result in the SSH client's received packets not being read on the jump host. This caused the SSH session to freeze, and no further data could be transferred.
  If the jump host remained in this state without the session being manually terminated, this led to an unexpected reboot of the router.
- OpenSSL has been updated to version 3.0.21.
- After creating a certificate using Smart Certificate, the wizard remains on the 'Create Certificate' page, allowing you to create another certificate immediately. However, when attempting to create another certificate, the session was terminated and the message "Access Forbidden" was displayed.
- The network chip in the SFP+ ports of the R&S®LANCOM ISG-8000 interpreted UDP packets without a checksum as if the checksum were invalid (packet checksum invalid). When TCP requests were sent to internal services of the ISG-8000 (e.g., via SSH) over a VPN connection using UDP (IPSec or WireGuard), the ISG-8000's TCP stack adopted the incorrect checksum (Bad TCP checksum). This resulted in no TCP communication being possible with the ISG-8000 over a VPN connection using UDP when data was transmitted via the SFP+ ports.
- In the 'Configuration / IP Router / VRRP' menu, WEBconfig allowed a maximum of 15 characters in the 'Virtual Link Local IPv6 Address' and 'Virtual Global IPv6 Address' fields.

Wi-Fi

- In rare cases, the WLAN controllers in a WLC cluster were unable to exchange packets used to manage the cluster. This caused synchronization within the WLC cluster to fail.
- In a Wi-Fi network using 802.1X with multiple RADIUS servers and active RADIUS pre-authentication (both standalone and LMC-managed), the access point was reading the wrong field in the encryption settings, which caused it to always use the first RADIUS server. If a different RADIUS server was required, this caused pre-authentication to fail.
  With pre-authentication enabled, the access point now uses the correct field in the encryption settings, ensuring that the correct RADIUS server is used.

VoIP

- After an incoming phone call followed by a successful transfer to another participant, the Voice Call Manager might have incorrectly assumed that the transfer destination was not answering. As a result, the Voice Call Manager terminated the call with a CANCEL after approximately 30 seconds.
- If UDP without encryption was selected for automatic signaling encryption (set to 'Automatic'), the Voice Call Manager would incorrectly send an INVITE with crypto attributes during an outgoing call.

LCOS improvements 10.92.0325 RU5

Bug fixes

General

- In LCOS 10.94, an update to OpenSSL 3.5 was implemented. This requires Certificate Signing Requests (CSRs) in version 1 and rejects CSRs with an incorrect version. Access points and Wi-Fi routers send CSRs in version 3 to the WLAN controller up to and including LCOS 10.92. As a result, newly added access points and Wi-Fi routers running LCOS up to and including version 10.92 could not obtain a certificate from a WLAN controller running LCOS 10.94 and therefore could not be managed by it (already connected access points and Wi-Fi routers are not affected).
- When configuring a RADIUS accounting server in a public hotspot scenario, an invalid value for 'Acct-Status-Type' was sent in the 'Accounting-On' message, which is responsible for enabling accounting.
  This affected the following R&S®LANCOM routers:
  - 1800EF
  - 1800EF-4G
  - 1800EF-5G
  - 1800EFW
  - 2100EF
  - vRouter
  - ISG-5000
  - ISG-8000
  - WLC-2000
- An SNMP user created via WEBconfig was not fully configured. As a result, it did not function properly and could not be used in LANmonitor or other SNMP monitoring software.
- When the router enters cold standby mode, power to the SIM card is cut off, which is why the PIN must be re-entered after the router returns to active mode. Although the router recognized that the SIM had already been unlocked, it did not reset the status when entering cold standby mode. As a result, the cellular connection could not be reestablished after the router returned from cold standby to active mode.
- To address CVE-2026-27171, the zLib library has been updated to version 1.3.2.

VPN

- If a R&S®LANCOM Unified Firewall initiated a rekey during an existing IKEv2 connection to a R&S®LANCOM router, the IKEv2 connection might have been disconnected.

Wi-Fi

- When using 802.11r, each WLAN controller set its own MAC address as the R0KH ID. In a WLC cluster scenario, this caused 802.11r to malfunction.
  The string "CAPWAP" is now always used for the R0KH-ID.
- In a WLAN controller scenario, changes made to the interfaces (e.g., switching from WLC tunnel to 'LAN on AP' or deleting or adding SSIDs) were not applied to the access points. This resulted in communication becoming impossible on some or even all SSIDs.

VoIP

- When switching SIP servers, the Voice Call Manager continued to use the 'REGISTER Expires' value negotiated with the first SIP server. This could result in the 'REGISTER Expires' value having to be renegotiated each time the device re-registered.

LCOS improvements 10.92.0278 RU4

Bug fixes

General

- When multiple service objects and a DNS target were used simultaneously in a firewall rule, the DNS target was not taken into account.
- In the syslog of a R&S®LANCOM 2100EF, messages about temperature incorrectly displayed a reference to a WLAN module: "Temperature is back to normal, wireless is turned on again".
- The status of the 'Remote Tables Last Change' info field in the 'Status/LLDP' console path was not processed correctly if it was empty (zero). When reading the 'Status/LLDP' console path, this caused the CPU load to permanently increase to 100%.
- If an IDS/DoS message was sent by the firewall after an IDS/DoS event, this could cause the router to restart unexpectedly.
- The parameter '-E' can be used to restrict the iPerf client on the console to a specific Internet peer. If this parameter was applied on a router with a configured load balancer, the iPerf client used all peers in the load balancer instead of restricting it to one connection. This led to incorrect measurements.
- Due to a change in the file name format, updates for the BPJM filter could be downloaded but not unzipped. The message "Info-Request-failed" was then displayed in the console path 'Status/Firewall/BPJM/Last-update-result'. This resulted in the BPJM filter not being functional.
- Communication between clients within the same network takes place natively via the switch. If clients in different networks connected via different Ethernet ports needed to communicate with each other, the MAC addresses of the clients were permanently assigned to the CPU port by the LAN bridge. If a client in one of the networks then needed to communicate with another client in the same network, this was no longer possible because the MAC address was still assigned to the CPU port. The packets were therefore discarded by the LAN bridge.

  This affected the following router models:

  - 1800EFW-5G
  - 1800EFW
  - 1800EF-5G
  - 1800EF
  - 1800VA
  - 1800VAW
  - 1800VAW-4G
  - 1800VAW-5G
  - 1800VA-4G
  - 1800VA-5G
  - 1803VAW
  - 1803VAW-5G
  - 1803VA-4G
  - 1803VA-5G
  - R903

- 1930EF
- 1930EF-5G
- 1936VAG
- 1936VAG-4G
- 1936VAG-5G

▶ To fix CVE-2025-15467, the OpenSSL library was updated to version 3.0.19.

▶ With IGMP and MLD snooping enabled, the backup router was incorrectly selected as the VRRP master in IPv6 mode because snooping blocked the VRRP multicast address ff02::12 (VRRP IPv6).

▶ When the maximum size of the RADIUS user table was reached, the Public Spot wizard returned an invalid page without an HTTP header instead of a meaningful error message when creating a new Public Spot user. The message "The Server provided an invalid message! Content Length: 0" was displayed in the web browser.

▶ In a BGP scenario, if there were two identical routes in the RIB table (a static route to a local LAN interface and one received from another BGP router), the received route was not removed when the local LAN interface was inactive.

Wi-Fi

▶ The major version LCOS 10.90 introduced the "Management Rate" feature, which can be used to influence the speed of management beacon frames. The default setting is 'Minimum', which means that the lowest speed for the Wi-Fi standard used (1 or 6 Mbit) is used. The value used for the 'Management Rate' was also included in the 'Basic Rate Set', i.e., the speed that clients must support in order to communicate with the wireless network. This resulted in Wi-Fi analysis software displaying the speed of the 'Management Rate' as the 'Minimum Basic Rate', which deviated significantly from the recommended value.

LCOS improvements 10.92.0227 RU3

Bug fixes

General

- The SFP trace “trace # SFP” could not be executed on the R&S®LANCOM R903, even though the device has an SFP port.
- When transferring data via an Internet connection with a low upstream data rate, a loop occurred in the active queue management of the Ethernet driver. This led to a significant increase in CPU load during the upload.
- When downloading the signature updates for the BPJM filter, the comparison of the local file header with the central directory record of the zip file containing the signature update failed. This meant that the signature update could not be downloaded. The error message “Zip extraction failed” was displayed in LANmonitor.
- In an OSPF scenario, if the VLAN of a network—and thus also the routing tag of the network and the OSPF instance—was changed, this resulted in the OSPF neighbor remaining in a ‘down’ state and the connection not being reestablished.
- To fix a security vulnerability (CVE-2025-9230), the OpenSSL library has been updated to version 3.0.18.
- The ‘jsPDF’ program library has been updated to version 3.0.2 to fix a security vulnerability (CVE-2025-57810).
- In the R&S®LANCOM 1800EF series, the default settings for the bridge groups of ports LAN-5 and LAN-6 were incorrect.
- In a scenario with active access management via RADIUS or TACACS+, if the configuration was uploaded with the RADIUS/TACACS+ user as an *.lcf file, the main device password for the user ‘root’ was empty in the backup case and login was only possible without a password.
- The accounting tables were not stored persistently on the following R&S®LANCOM router models and were therefore empty after a restart:
  - 180x series
  - 1936VAG / 1936VAG-5G
  - 2100EF
  - ISG-5000 / ISG-8000
  - vRouter
- If there is a change of VRRP master in a VRRP scenario, the new VRRP master sends a Gratuitous ARP (GARP) with the VRRP MAC address to the network. When VRRP and LACP were used simultaneously with a user-defined LACP MAC address and an active LAN bridge, the new VRRP master sent the LACP MAC address in the GARP instead of the VRRP MAC address. This resulted in severely restricted communication.
- As of LCOS 10.90, it was no longer possible to transfer data via DSLoL (DSL over LAN) on R&S®LANCOM access points with LCOS and WLAN routers of the R&S®LANCOM 1700 series.
- If the public spot user could not be created in the RADIUS user table when creating a new public spot voucher (for example, because the ‘Accounting-Total’ table was full), this led to an unexpected restart.
- Mobile routers may have restarted unexpectedly on occasion.

VPN

- After a failed connection attempt by a device with configured IKEv2-EAP to a router with unconfigured IKEv2-EAP, the established security association (SA) remained in the router's security association database (SADB) and was no longer deleted.
- An incoming VPN connection in a VRRP scenario without an active IKEv2 load balancer could not be established when the virtual VRRP address was used for the establishment.

LCOS improvements 10.92.0167 RU2

Bug fixes

General

- When TACACS+ was configured, opening the port forwarding table via WEBconfig could cause the router to restart unexpectedly.
- If the mobile network provider's network was in an error state, the router detected this and performed a reinitialization followed by a restart of the mobile modem in order to recover from the error state. This could take several minutes.
  In such a case, the mobile radio modem is now reattached, thus minimizing downtime.

VPN

- A newly created IKEv2 connection under iOS 26 could not be established because a new iOS feature was not compatible with LCOS.

Wi-Fi

- When using client steering (not recommended; client management should be used instead), the WLAN controller could suddenly restart in environments with a large number of logged-in wireless devices.

LCOS improvements 10.92.0098 RU1

New features

- When using Dynamic Path Selection (DPS), the ICMP identifier is now changed after every 4096 measurements (for the default interval of 1 second this means every 70 minutes).
- The backoff time for a failed VPN tunnel establishment can be configured on the CLI.
- SIP-ALG: PMTU reduction and fragmentation are only carried out if the MaxTxRate is less than 1 Mbps. If no bandwidth is configured, no reduction or fragmentation is performed.
- The default country code for the R&S®LANCOM DECT N610 IP is 'Europe' instead of 'undefined'.
- Content Filter: If an override is executed by a user, this applies to the entire domain and regardless of the protocol used. This means that a direct call after an HTTPS redirect also works.

Bug fixes

General

- If a mobile radio module restarted due to a hardware reset, it could happen that the internal PIN status in LCOS was not reset. As a result, LCOS could no longer unlock the SIM and the mobile radio module could no longer connect to the mobile radio network.
- If a timeout occurred when using the internal HTTP server (e.g. to provide certificates) via a slow connection, this led to an immediate restart of the router.
- If a configuration was rolled out several times via the LMC to a device that was in offline status, this resulted in TACACS+ authentication being deactivated.
- When using R&S®LANCOM Security Essentials, it could happen that applications that were allowed or classified as secure (e.g. Office 365) and categories were still blocked by the content filter.
- When reading the hexadecimal password of the GPON module, the router converted it to lowercase letters. If uppercase letters were used in the PON password (under Interfaces / WAN / PON), this led to a permanent boot loop of the GPON module.
- When deleting the ARP table after the 'ARP aging minutes' have expired, a request is made to the firewall for each deleted entry in order to delete the ARP resolution for affected sessions. In larger scenarios with many simultaneous sessions, this led to periodic short load peaks with every second deletion of the ARP table (i.e. every 30 minutes with the default 'ARP aging minutes' value of 15 minutes). This could lead to short-term connection problems.
  ARP aging now has an interval of 30 seconds. Furthermore, the number of ARP entries that can be deleted simultaneously is limited (can be adjusted via the console path 'Setup / TCP-IP / ARP-Max-Remove', default value is 25). If more ARP entries are to be deleted and the ARP aging limit is exceeded as a result, ARP aging is reduced to 10 seconds.
- On a vRouter operated in Hyper-V, the checksums for TCP and UDP were calculated incorrectly for a PPPoE connection. Depending on the network card used, this could lead to heavy packet loss, among other things.
- If the router was assigned an IP address with x.x.x.255 during PPP negotiation and the dial-in router of the Internet provider also claimed this IP address, the router rejected DNS responses. As a result, no Internet connection could be established via the router. Furthermore, the router could not establish a connection to the LMC.

- After updating the firmware of a R&S®LANCOM 1793VA-4G to LCOS 10.90, it could no longer establish a cellular connection with the default settings of the cellular profile 'WWAN-DEFAULT'. This meant that a zero-touch rollout was no longer possible.
- If an action with a large number of characters was stored in a firewall rule via WEBconfig, this led to an immediate restart of the router.
- If a vRouter operated in Proxmox with a VirtIO network card for the Internet connection routed data traffic with many simultaneous sessions via the Internet connection (such as a speed test), this led to heavy packet losses or even an interruption of the Internet connection.

Wi-Fi

- If a 4-digit VLAN ID was entered in the 'Set up WLC profile' setup wizard, this could cause the device to restart immediately after completing the wizard.

VoIP

- The Voice Call Manager did not forward a busy signal to ISDN and analog subscribers.
- After an update to LCOS 10.9x, it could happen that a SIP client could no longer log on to a SIP PBX (e.g. a Cloud PBX) via a SIP PBX line set up in the Voice Call Manager.
- On the WEBconfig interface of a R&S®LANCOM 1803VA it was not possible to configure or activate ISDN interfaces.
- If the Voice Call Manager received a 'Provisional Update' from the SIP PBX for an outgoing call, the Voice Call Manager then sent a PRAck with "RAck: 2 100 UPDATE" instead of "RAck: 2 100 INVITE" to the SIP provider. This resulted in the SIP provider terminating the connection with the message "481 Call/Transaction Does Not Exist".
- The Voice Call Manager could not process multi-part SDP messages and then sent the message "406 SDP Not Acceptable".
- If a SIP user established a call with a video and an audio stream to an ISDN or analog user, the Voice Call Manager removed the video stream and deactivated the audio stream (m=audio 0). This meant that no voice communication was possible.
  In such a scenario, the Voice Call Manager now deactivates the video stream and leaves the audio stream active.

LCOS improvements 10.92.0018 Rel

New features

- Support for the R&S®LANCOM Security Essentials Option
- Change of the Content Filter to Bitdefender

  Please note that some of the categories have changed and new categories have been added as a result of the change. It is recommended to check the configuration after the LCOS update. Please also refer to the notes on the update.
- Support for the backup/restore function of the device
- Support for Dynamic RADIUS Caching
- The behavior for inter-tunnel traffic can be configured in L2TPv3.

Bug fixes

General

- When using an unmasked default route for an IKEv2 connection, it was incorrectly displayed that the DNS server could be reached from the WAN.
- The DSL line code has been updated to version 12.9.1.2.0.7 for devices of the 180xVA and 1926/1936 series.
- The password change of a logged-in TACACS user was acknowledged in WEBconfig with the error message “Not Found”. As a result, the password change failed.
- When repeatedly reading out the console path ‘Status/VDSL/Line-Type’ (this also affected the higher-level path ‘Status/VDSL’) with the repeat command (e.g. “repeat 3 ls Status/VDSL/Line-Type”), the information was only output once.
- If no gateway was entered on the standby router in the DHCP network in a VRRP scenario (0.0.0.0), the standby router sent a DHCP offer without a gateway instead of using the VRRP IP address. If an end device first received the DHCP offer from the standby router instead of the master router, it did not accept the assigned IP address and communication was not possible.
- If the VLAN of a network - and thus also the routing tag of the network and the OSPF instance - was changed in an OSPF scenario, this resulted in the OSPF neighbor subsequently remaining in the ‘down’ status and the connection not being re-established.

VPN

- If a router with several active Internet connections and an IKEv2 connection with a specific routing tag received an IKE packet with the message type ‘Redirect’, the router changed the routing tag for the outgoing IKE_SA_INIT to 0 instead of retaining the previous routing tag. As a result, the VPN communication was then transmitted via the wrong Internet connection.

Wi-Fi

- The IAPP table can hold a maximum of 2048 entries. New access points can therefore no longer be added once the maximum has been reached.
  If an access point could no longer be added to the IAPP table and therefore could not be found in the table, this led to an immediate restart of the access point.
- If there was an IP address entry for a freely accessible web server in the 'Setup/Public-Spot-Module/Free-Server' table, an error message was displayed when an HTML page of this web server was called up due to a missing HTML header.

VoIP

- If communication with a particular destination was only possible via a specific, dynamically learned route with 'next hop' (e.g. via BGP), but a statically configured default route without 'next hop' was also configured for the same remote station, but with a different routing tag, and the router received a packet for the destination network before the dynamic route was learned, the router did not replace the static route with the dynamic route for the session (the static route was not invalidated). As a result, the static route continued to be used and the destination network could not be reached via it.

7. General advice

Disclaimer

Rohde & Schwarz Networks and Cybersecurity does not take any guarantee and liability for software not developed, manufactured or distributed by Rohde & Schwarz Networks and Cybersecurity, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your R&S®LANCOM devices to a new LCOS version it is essential to backup the configuration data!

Due to extensive features it is **not possible to downgrade** to a previous firmware without using the backup configuration.

If you want to upgrade devices which are only accessible via router connections or Wi-Fi bridges, please keep in mind to upgrade the remote device first and the local device afterwards. Please see the LCOS reference manual for instructions on how to upgrade the firmware.

We strongly recommend updating productive systems in client environment only after internal tests. Despite intense internal and external quality assurance procedures possibly not all risks can be eliminated by Rohde & Schwarz Networks and Cybersecurity.

Using converter firmwares to free up memory

Due to numerous new functions within the LCOS firmware it may not be possible in some circumstances for older devices to keep two fully-featured firmware versions at the same time in the device. To gain more free memory, a smaller firmware with less functionality has to be uploaded to the device first. As a result, significantly more memory will be available for a second firmware.

This installation has to be done only once by using a “converter firmware“.

After having installed the converter firmware, the firmsafe function of the R&S®LANCOM device is only available on a limited scale. The update to a new firmware is furthermore possible without any problems.

However, after a failed update the R&S®LANCOM device works with the converter firmware which only allows local device access. Any advanced functionality, particularly the remote administration, is not available as long as the converter firmware is active.

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

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions.

ROHDE&SCHWARZ
Make ideas real