Release Notes

LCOS
10.80 RU11

Table of contents

1. Preface

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

This document describes the innovations within LCOS software release 10.80 RU11, 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
www.lancom-systems.com/service-support/instant-help/common-support-tips

2. The release tag in the software name

Release Candidate (RC)
A Release Candidate has been extensively tested by LANCOM 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 LANCOM 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 LANCOM 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 10.80

LANCOM products regularly receive major firmware releases throughout their life-time 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 under www.lancom-systems.com/products/firmware/lifecycle-management/product-tables

LANCOM devices without support as of LCOS 10.80

→ LANCOM LN-1700
→ LANCOM LN-1702
→ LANCOM LN-830acn
→ LANCOM L-822acn
→ WLC-4006+

4. Advices regarding LCOS 10.80

Changing the attribute for e-mail addresses when using certificates
As of LCOS 10.80, the ‘E’ attribute for email addresses is no longer supported when using certificates (e.g. for IKEv2). Instead, the ‘emailAddress’ attribute must be used. This change must be made before updating to LCOS 10.80.

Example:
“/E=test@lancom.de” has to be changed to “/emailAddress=test@lancom.de”.

Further information can be found in the KB article
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=36449459

Important notes on extending the input length of the main device password
As of LCOS 10.80, the input option for the number of possible characters for the main device password and the other administrators has been extended from 16 to 128 characters. If more than 16 characters are used in LCOS 10.80, a downgrade to versions lower than 10.80 is no longer possible or supported. It is no longer possible to log on to a device after the downgrade.

Special attention must be paid to the WLC with managed access points in the case of password synchronization. If the longer password is used on the WLC, all managed access points must also be operated with LCOS 10.80. In this case, local logon is no longer possible on APs with LCOS lower than 10.80.
The above instructions apply only in case the new option of more than 16 characters is used for the password.

Information on default settings

Devices delivered with LCOS 10.00 or higher automatically connect to the LANCOM Management Cloud (LMC). This functionality provides zero-touch installation for new devices. In case you do not want to use the 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 LMC whenever you want.

Omission of VPN rules in the IPv4 firewall

As of LCOS 10.70, VPN rules for generating network relationships (SAs) are no longer supported in the IPv4 firewall and are replaced by the 'Network rules' configuration option in the VPN menu.
This mainly concerns scenarios with IKEv1 connections.

For more details see:
https://support.lancom-systems.com/knowledge/pages/viewpage.action?pageId=85885727

5. Feature overview LCOS 10.80

5.1 Feature highlights 10.80

Let's Encrypt for WEBconfig and the LANCOM Public Spot

Let's Encrypt is a certificate authority that offers free HTTPS certificates to standardize encrypted connections. WEBconfig and also the LANCOM Public Spot now support Let's Encrypt. This means that free and trusted certificates can be created, integrated via the gateway, and automatically renewed with just a few one-time and simple steps.

5.2 Further features 10.80

Zero-touch rollout for cellular routers

With the support of Zero-touch, the setup of LANCOM cellular routers is now even easier and faster. Where previously manual configuration of the cellular access point was required, it is now sufficient to insert a PIN-free SIM card into the device. Zero-touch rollout enables an automatic connection to the Internet and subsequently to the LANCOM Management Cloud to retrieve the appropriate configuration of the gateway.

LANCOM vRouter available via Google Cloud

With LCOS 10.80, you can now operate the LANCOM vRouter on demand with the cloud computing provider Google Cloud. This means that in addition to Microsoft Azure, VMware ESXi, Hyper-V, and AWS, you can now also use Google Cloud to move your own infrastructure to the cloud. The LANCOM vRouter guarantees a secure connection and handles encrypted communication between your site and your virtualized infrastructure in the Google Cloud. Furthermore, the virtualization of headquarters is also possible: the vRouter in the Google Cloud simply replaces the central hardware gateway.

WEBconfig in new corporate design

If you manage your devices via the web browser, LANCOM provides you with a graphical user interface via WEBconfig, which is directly integrated into LCOS and from now on shines with a new coat of paint in a modern design and maximum clarity.

You can find further features within the individual builds sections in chapter 6 "History LCOS 10.80".

6. History LCOS 10.80

LCOS improvements 10.80.1023 RU11

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.

→ It could happen with the following routers that the TCP checksums were calculated incorrectly. This led to timeouts of TCP sessions that were initiated by the router and transmitted via VPN.

- 1800EF
- 1800EFW
- 1800EF-4G
- 1800EF-5G

→ Access points with LCOS LX were assigned a default profile even though the option ‘Automatically assign APs a default configuration’ was disabled in the WLAN controller.

→ If a device of the LANCOM 1800EF series in the path ‘Setup/Public-Spot-Module/Free-Networks’ used a netmask for a subnet that was not equal to ‘255.255.255.255’ (e.g. ‘255.255.255.230’), the entry did not work.

→ It could happen that an outgoing call from a SIP client could not be established if the SIP provider repeated its “407 Proxy Authentication Required” because the Voice Call Manager (VCM) did not observe the command sequence ‘CSeq’. If the provider also sent a ‘To’ tag in the “407 Proxy Authentication Required”, the VCM did not send back a ‘To’ tag in its ‘ACK’.

→ Up to and including LCOS 10.80, it is possible to assign two xDSL interfaces to an Internet remote station on routers of the 1900 series with two xDSL modems. The Internet connection is then established via the xDSL modem for which the DSL sync has taken place.
If the Internet connection was established via the xDSL-2 interface in such a scenario, the router did not delete the QoS reservations created by the Voice Call Manager for the Internet connection. As a result, more and more bandwidth was reserved and was therefore no longer available for Internet communication.

→ After a failure of the mobile network infrastructure of a mobile network provider, the used APN may be placed on a blacklist. However, on routers with Sierra MC7421, EM7421, and MC7455 cellular modems, the assigned timer for the entry in the blacklist was not interpreted correctly, so that the timer sometimes did not expire or expired very late. As a result, it was not possible to dial in to the mobile phone provider during the blocking state.

→ In the OSPF route redistribution with configured metric source ‘Protocol’ it could happen that routes of type LSA 5 were not propagated.

→ 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 destination, 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.

LCOS improvements 10.80.0966 RU10

New features

→ Wildcards can now also be used for remote stations in the WAN MTU list table.

Bug fixes

General

→ When calling the actions ‘Delete-History’ and ‘Retrain’ via WEBconfig (menu path ‘Extras / LCOS menu tree / Status / xDSL / xDSLx’), the submenu for executing the commands was not loaded and the error message “Not Found” was displayed instead.

→ If IPv6 was active on a router, the router could restart immediately when Netflow analyzed an FTP data session that was transmitted via IPv6.

→ If the command “find vrrp” was entered in the command line, the path information output did not contain any line breaks.

→ If DNS addresses were specified as IPv4/IPv6 target addresses instead of IP addresses in a VPN load balancer configuration, the table in the path ‘Status/VPN/Load-Balancer/Peer-Status/’ was filled with an infinite number of entries.

→ On cellular routers with Quectel 4G and 5G modules, the field for the RSRP (Reference Signals Received Power) and RSRQ (Reference Signal Received Quality) was skipped when calculating the signal values. This resulted in incorrect and sometimes physically impossible values being output for the RSRP and RSRQ.

The following mobile routers were affected by this behavior:

- 1800EF-4G
- 1800EF-5G as of HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

→ A plain Ethernet remote station with a dynamically generated MAC address (‘MAC address type’ set to ‘Local’) of a vRouter operated in Hyper-V was not established, so that the Internet connection could not be established. Furthermore, in such a scenario, several plain Ethernet remote stations with dynamic MAC addresses created in the vRouter could not exchange ICMP packets (ping) with each other.

→ For cellular routers with Quectel 4G and 5G modules, the provider name in the ‘Network’ status field (console path ‘Status/Modem-Mobile/’) was limited to 16 characters. This could cause the name to be truncated.
The following LANCOM cellular routers were affected by this behavior:
- 1800EF-4G
- 1800EF-5G as of HW Rel C
- 1803VA-5G
- 1800VA-5G
- 750-5G
- IAP-5G

→ After a firmware update of LANCOM L-322agn (Hardware Rev. 2) managed by the LMC, a sudden restart could occur due to a lack of memory.

→ The table for listing open services in the ‘Status/Config/Services’ path displayed incorrect values.

→ Due to two security vulnerabilities, OpenSSL has been updated to version 3.0.16 (see also CVE-2024-13176 & CVE-2024-9143).

→ If the route to the BGP neighbor was changed multiple times to a different interface, it could happen that the router tried to establish the BGP connection via an incorrect interface. As a result, the BGP connection was not established.

→ If the WAN IP address of the LANCOM router changed (e.g. after a forced disconnection by the provider), existing firewall sessions were not removed. As a result, the outdated WAN IP address continued to be used, which meant that existing VPN connections could no longer be used. Only after a restart of the LANCOM router was the new WAN IP address used and the misbehavior thus resolved.

→ The LANCOM 1930EF has six Ethernet interfaces, but only four virtual LAN interfaces. As there were six LAN interfaces for this device in LANconfig and the LMC, this meant that the configuration could not be written or rolled out to the router via LANconfig and the LMC.
Six virtual LAN interfaces are now available.

→ When using the vRouter in Proxmox, it could happen that an incorrect value was displayed for the assigned RAM.

→ If a default route is operated unmasked with an Internet connection, the DNS server can be reached from the WAN. In the ‘Status/Config/Services’ service table, however, only the default route with the tag 0 was taken into account, so that the status ‘No’ was incorrectly displayed for unmasked default routes with a routing tag other than 0.

→ If the assignment of the PON module was changed from ‘LAN-1’ to ‘DSL-1’, for example, the PON management remained in the ‘Working’ status. This could only be resolved by restarting the router.

→ If the router received an ARP packet for an invalid LAN interface (e.g. in the event of a faulty configuration with DNS forwarding to its own IP address), this led to an immediate restart of the router.
In such a scenario, the entry in the ARP cache becomes invalid and the packet is therefore discarded.

→ When using XLAT with masking, embedded ICMP headers were not masked by the XLAT. As the sender and destination addresses were therefore the same, the packets were blocked by IDS detection.

VPN

→ If a VPN connection with the same name was created as both an IKEv1 and an IKEv2 connection, the router could restart unexpectedly when a configuration was written back.

Wi-Fi

→ The mechanism for cleaning up the Wi-Fi ARP table did not work correctly, which could result in multiple entries for wireless clients. As a result, ARP packets for these wireless clients were not forwarded and communication was severely restricted.

VoIP

→ SIP-ALG set the media endpoint for outgoing INVITEs in RTP to 0.0.0.0. As a result, no RTP session could be established and no voice transmission was possible.

LCOS improvements 10.80.0833 RU9

Bug fixes

General

→ The LANCOM SFP-GPON-1 module was not recognized by the LANCOM 1930EF. The status of the module remained in the console path “Status/PON” at “Module in Waiting”.

→ After the maximum number of half-open connections for a connection source or connection destination was reached, the DoS (Denial of Service) detection dropped these packets until the runtime of all half-open connections for this source or destination expired and they were deleted. This could lead to desired data traffic also being discarded.
DoS detection now allows communication after the maximum number of half-open connections has been exceeded, when the threshold has fallen below half again.

→ After deactivating the IPv6 interface and deleting the delegation addresses for an IPv6 interface with statically configured delegation addresses, the delegation addresses were still present after activating the IPv6 interface.

→ An IPv6 interface should only not be set up if the DAD (IPv6 Duplicate Address Detection) is not successful for the primary link-local address. However, the IPv6 interface was also not set up if the DAD was not successful for a statically assigned IPv6 address that was checked before the primary link-local address.

→ Activated demo licenses were not displayed in the WEBconfig dashboard of a LANCOM vRouter.

→ An Ethernet interface was only monitored by the BGP for state changes if the connection to the BGP neighbor was successfully established. If the Ethernet interface had not yet been successfully established (e.g. after a router restart) before the router attempted to resolve the source address for the BGP neighbor, the BGP connection could not be established.
In such a case, status monitoring is now started so that the BGP recognizes changes to the interface.

→ After a hardware reset of an R883+ or R903 managed by the LMC, the LMC certificate was not deleted.

→ If the LMC client of a device was waiting for data from the LMC after a rollout, but none arrived (e.g. due to connection problems), this led to an immediate restart of the device.

→ If there were more than 32 entries in the port forwarding table, this led to an immediate restart of the device when writing the configuration via LANconfig.

→ If the SIM card was replaced on a mobile router with an active mobile

connection, the mobile module could no longer establish a connection.

→ When inserting a non-activated SIM card, the error code 10 was displayed on the console (Mode) and in LANmonitor (Mode) instead of the error message “Limited Service”.

→ If a router with a configured backup connection was switched back to the main connection after the backup case, it could happen that data traffic from a downstream router was still routed via the backup connection and the data could therefore not be transmitted.

→ If SMS packets arrived on a mobile router in the wrong order, the triggers could not be processed correctly by the action table. This meant that the stored action could not be executed (e.g. rebooking data volume).

VPN

→ In individual cases, when setting up / rekeying a Child_SA (ESP SA) on a LANCOM ISG-4000 / ISG-5000 / ISG-8000 and the vRouter, it could happen that a non-functional Child_SA was created. As a result, no data could be transferred via the VPN tunnel.

→ When using the load balancer, it could happen in individual cases that the connection was not automatically established by the keepalive (hold time 9999) after a VPN connection was terminated.

LCOS improvements 10.80.0742 SU8

Bug fixes

General

→ A security vulnerability in the web interface has been fixed, which allowed unauthenticated attackers to cause an unexpected device restart (DoS attack) by sending a manipulated packet. This affected administrative access via WEBconfig from the LAN and the WAN (if management access via HTTP/HTTPS from the WAN was enabled), as well as the web services IPSec-over-HTTPS, SCEP, OCSP server/responder, and the Public Spot. In the default configuration, access to the router from the WAN is disabled, meaning the router was not affected by this vulnerability in such cases. The TR-069 protocol was also not affected by the vulnerability.

LCOS improvements 10.80.0741 RU7

New features

→ When using the LANCOM SFP-GPON-1 module on Deutsche Telekom gigabit connections, the BNG sets the achievable data rate to 1.1 Gbps. As a result, the download performance in Internet speed tests, for example, was only between 700 and 800 Mbps instead of approx. 930 Mbps due to bursts. The buffers in the GPON module have been enlarged and are now adjusted accordingly by LCOS for this case. This setting is automatically activated after the LCOS update. The behavior can be switched on the CLI. In certain cases, it may be necessary for the new settings to only take effect after a new LCOS restart once the Internet connection has been successfully established.

→ After a device reset, the SFP port of the LANCOM 1800EF series is now predefined as a WAN port instead of a LAN port. This also enables zero-touch commissioning on fiber optic connections via SFP.

Bug fixes

General

→ In the WEBconfig dashboard of a LANCOM vRouter, activated demo licenses were not displayed.

→ After a forced disconnect of the WAN connection by the ISP, it could happen that BGP remained in IDLE status and no longer worked.

→ In the configuration of a RADIUS server, it was not possible to use an existing backup server in a profile. After saving the profile, the selection was no longer available.

→ It could happen that the CRL client had no CRL for a short period of time because it had already expired and a new CRL had not yet been obtained.

→ If the connection to a BGP neighbor was not possible when BGP was started, the BGP connection was not established after the BGP neighbor could be reached again. As a result, communication with the affected BGP neighbor was not possible.

→ If the target interface to a BGP neighbor was in the ‘down’ state, the router still tried to establish the connection and switched to the ‘active’ or ‘connect’ state.

→ When importing the *.ova file of a vRouter into VMWare, it is possible to set the IP address and the subnet mask for a network via a field in VMWare. The IP address and the subnet mask should be separated by a space. However, a space was not allowed and could therefore not be entered. As a result, it was not possible to enter the IP parameters in VMWare. The IP address and the subnet mask can now be separated from each other by a comma (,).
→ After deleting the ACS URL by an ACS (Auto Configuration Server) via TR-069, the router continued to respond incorrectly to requests via TR-069 and continued to try to contact the ACS.
→ In individual cases, the router may restart immediately when the VPN module is activated / deactivated if many firewall sessions are established or terminated in the meantime.

Wi-Fi

→ In scenarios where 802.1X authentication was used for SSIDs, clients with Windows 11 operating system could not connect to the SSID because the authentication failed.
→ In the RADIUS table of a LANCOM WLC-60, only a maximum of 128 entries could be created for Public Spot users. A maximum of 256 entries are now possible.

VoIP

→ If all TCP SIP servers that were resolved via NAPTR failed, the voice call manager sent several new TCP SYN packets per second to all servers. If all UDP SIP servers that were resolved via NAPTR failed, the voice call manager sent too many new REGISTER packets in a specified period of time.
In the event of unavailability, an exponential backoff is used to repeat a failed request at regular intervals with increasing delays between requests.
→ In scenarios where the same SIP server was used for registration via UDP, TCP, and TLS, the voice call manager prioritized the NAPTR records incorrectly if the DNS responses received were in a different order than the DNS responses sent.

LCOS improvements 10.80.0665 RU6

New features

→ When delivered ex works, or after a configuration reset with LCOS 10.80.0664 PR, a new default remote site with the name ‘GPON-Default’ for telecom fiber optic connections is available, which enables zero-touch commissioning with the LMC and automatically establishes a Telekom PPPoE connection at the WAN / SFP port (device-dependent). This remote site is available for all devices of the 1800EF-x series, 180xVA series, and 19xx series.

→ A new configuration parameter has been introduced for IPv4 firewall sessions, which can be used to limit the number of concurrent firewall sessions. By default, the parameter is ‘0’, i.e. not limited. The parameter must be set manually for the individual scenario.

→ Additional counters for monitoring the number of IPv4 firewall sessions have been introduced.

Bug fixes

General

→ In scenarios with multiple WAN connections, the DNS service used the line classified as ‘MOST_USED’ by default when DPS was active. This meant that DNS queries were not answered if the internet connection was poor. The ‘ROUND_ROBIN’ method is now used again by default.

→ When installing a vRouter with LCOS 10.80 on Hyper-V, the installation routine froze. As a result, the installation could not be completed.

→ Netflow occupied CPU resources even when Netflow was deactivated.

→ If Netflow had to clean up a large number of sessions, it could happen that the job took too long. This led to an immediate restart of the router.

→ If a USB stick was connected to a router of the LANCOM 1800EF series, to the LANCOM 1650E or to the LANCOM WLC-60, it could happen that it was not recognized correctly. This led to an immediate restart of the device. It could also happen that the immediate restart occurred when reading the console path ‘Status/USB/Devices’ with the USB stick inserted.

→ With the LANCOM devices ISG-5000 / ISG-8000 and WLC-2000 the meta information for the LMC was not stored boot persistent. As a result, the information was not displayed correctly in LMC monitoring when using Dynamic Path Selection.

→ In individual cases, it could happen that configured BGP neighbors were created twice. The first connection remained permanently in the ‘Established’ status. However, the router repeatedly tried to establish the second connection, which led to a collision with the existing connection and thus to the connection being terminated. This was acknowledged by the error message “Connection collision resolution”.

→ If an SSH client tried to establish a connection to an access point or router with the outdated and insecure encryption algorithm ‘arcfour128’, this led to an immediate reboot of the device.

VPN

→ In scenarios with multiple VPN load balancers (e.g. with Dynamic Path Selection), the VPN licenses were not counted correctly. With correct licensing, this meant that too few VPN licenses were available in such a scenario and therefore not all VPN tunnels could be established.

→ The parameter ‘Remote-Auth’ can only be set to EAP for IKEv2 in the console path ‘Setup/VPN/IKEv2/Auth/Parameter/<VPN-Name>’ if at least 25 VPN licenses are available on the router (Central Site Gateway, router of the 19xx series or router with VPN-25 option). However, no error message was displayed, so the cause was not immediately apparent.
In such a case, the error message “Missing EAP license.” is now displayed.

→ When using an IKEv2 load balancer, it could happen that the load balancer was no longer set up if a setup and teardown overlapped.
Furthermore, sessions were not deleted from the statistics when switching to a different interface, so that the number of sessions was displayed incorrectly.

LCOS improvements 10.80.0594 RU5

New features

→ For multi-core devices, the CPU utilization of multiple CPU cores is now also displayed in the status menu or as SNMP OID.

→ For RADIUS scenarios, a new switch has been introduced in multiple modules that defines whether the presence of the 'Message Authenticator attribute' in RADIUS messages is enforced on the client side (i.e. the side that receives a 'RADIUS Accept / Fail').

→ The 802.1X authenticator in LCOS no longer accepts responses without an EAP message.

→ For dynamic path selection / load balancer scenarios, a new parameter has been added that places sessions on the most utilized channel.

→ In TR-069, you can configure which WAN connections should not be used by the TR-069 client for the connection to the ACS.

→ The performance when displaying the IPv4 firewall connection list for large tables has been improved.

→ Stability improvement in the output or display of the IPv4 router connection list and open port list in scenarios with a large number of entries under high load.

→ Improved performance when automatically cleaning up the IPv4 router connection list in scenarios with a large number of entries.

→ Stability improvements and optimizations in ARP, especially in scenarios under load.

Bug fixes

General

→ The SFP+ interfaces of a LANCOM ISG-5000 or ISG-8000 could not be permanently set to '10 Gbps fiber'. An error message was displayed when writing back.

→ When using the accounting function, it could happen that the LANCOM router performed a sudden restart during a firmware update.

→ When using VRRP on routers of the 1800 series (except 1800EF, 1800EFW and 1800EF-5G), the VRRP address could only be addressed if a bridge group was assigned to the Ethernet port used instead of a LAN interface.

→ In individual cases, routers with multicore CPUs could cause the scheduler not to assign any work to the TCP job. As a result, SSH connections to the affected router were very slow and routers managed by the LMC repeatedly lost the connection to the LMC.

→ If a router managed by the LMC was disconnected from the Internet via the WEBconfig tunnel in the LMC, this led to an immediate restart of the router.
→ The use of more than one plugged-in SFP module of the type ‘SFP-CO10MG’ could lead to an immediate reboot of the LANCOM router.
→ Some syslog assignments between log level and source were incorrect. For example, the log level ‘Info’ was assigned to the source ‘Emergency’.
→ When using Mesh VPN, it could happen in individual cases that several processes processed the same variables at the same time. This led to an immediate restart of the router.
→ A background image uploaded for Public-Spot was cut off at a size of 1500 x 999 pixels on the displaying device because the associated variable only had a length of 16 bits.
→ With a LANCOM ISG-5000 managed via LMC, a maximum of 128 Public Spot users could be created.

VPN

→ The VPN data throughput was calculated incorrectly for the LANCOM ISG-5000 and ISG-8000 devices. As a result, a value that deviated from reality was displayed on the console, in LANmonitor and the LMC.
→ If more than 1000 VPN connections were established simultaneously, the ‘VPN-IKE’ process occupied all free CPU resources and the CPU load of the router increased to 100%. As a result, the establishment of VPN connections stopped and some connections were terminated again due to a DPD timeout. As a result, a large number of VPN connections could not be established.

Wi-Fi

→ On the LANCOM 1800EF and 1800VA devices, a high value for the number of connected 6 GHz Wi-Fi clients was displayed in the ‘Status / WLAN Management’ path, although no WLC Basic option for routers was activated on these devices.

VoIP

→ If the Voice Call Manager received an error message in the SIP that belonged to a SIP call that no longer existed, this led to an immediate restart of the router.

LCOS improvements 10.80.0450 SU4

Bug fixes

General

→ A security vulnerability has been fixed which caused the password of the administrator ‘root’ to be reset - and thus deleted - after writing a complete configuration (e. g. an *.lcf file) with another administrator with supervisor authorization.

LCOS improvements 10.80.0448 RU3

New Features

→ New configuration option for data roaming in third-party networks for mobile routers on the CLI. Data roaming is activated by default.

→ New configuration option for the PDP context (IPv4/IPv6) in the event of data roaming in third-party networks for mobile routers on the CLI. IPv4 is used by default when roaming in third-party networks.

→ The ICMP SLA monitor now automatically generates a syslog message for measurements or threshold values in the result evaluation in the case of 'Critical' and 'Warning'.

→ If a running trace consumes too much free memory, it is automatically terminated by the system so that the device is protected from restarting due to insufficient free memory.

→ IPsec performance improvement in the event that the device has established the VPN connection (initiator)

→ IPsec performance improvements for 1800 / 1900 series devices

→ The syslog filter is now also supported for messages from the internal syslog server.

Bug fixes

General

→ After a configuration rollout via the LMC, it could happen in certain situations that the changes were transmitted again by the LMC. This meant that the configuration generated by the LMC was incorrect and an inconsistent configuration was created when it was rolled out again.

→ If the 'Address Family Transition Router' (AFTR) of the provider was changed for a Dual Stack Lite connection, it could happen that the new DNS address of the AFTR could not be reached because the DNS address of the previous AFTR was still being used due to a problem with the DNS cache.

→ If a service in the LANCOM router (e.g. DynDNS) was still using TLS 1.0 or 1.1, this led to an immediate restart.

→ Due to a too large DMA buffer, the image of a LANCOM vRouter could not be installed under Microsoft Azure.

→ LANCOM routers of the 1700 series with permanently configured Internet access data, which were subsequently connected to the ACS server of Deutsche Telekom, sent an incorrect provisioning code.

→ Because the required value was not stored in the transmission mode for SFP connections, the value ‘Auto’ was automatically stored. As a result, a configuration rollout via the LMC was prevented by the lack of the parameter.

→ If the SMTP server of an email provider only allowed the encryption algorithm ‘secp384r1’ during TLS negotiation, the TLS handshake could not be completed. As a result, the email transmission failed.

→ If an add-in script was rolled out via LMC, which incorrectly set the line index to 0 (only numbers from 1 may be used as an index), this led to an immediate restart of the device.

When using Dynamic Path Selection in conjunction with a load balancer at the head office, if a VPN connection failed, data traffic initiated from the central site for an existing session continued to be routed via the terminated connection. This meant that the packets could not be answered by the branch office and it was therefore not possible to switch to the other VPN connection (passive switchover).

In such a scenario, the head office now routes all existing sessions via the other VPN connection (active switchover).

→ The load score for Dynamic Path Selection has been set to the maximum value of 250 instead of 0 for connections that have not yet been established.

→ If an IPv6 interface was activated for an EoGRE tunnel, it could happen that the EoGRE tunnel was constantly activated and deactivated again (flapping).

→ Due to the introduction of the ‘Japanese Unicode Conversion’ in LCOS 10.80, more special characters had to be taken into account, which significantly increased the load on the DNS service. In large scenarios, this could lead to the DNS service permanently utilizing 100% of the CPU, resulting in restrictions during operation.

VPN

→ It could happen that VPN connections were not established automatically by the keepalive mechanism. Instead, the establishment was only triggered by a data transfer.

→ When using tunnel groups in the VPN, it could happen that the remaining connections of the group were also disconnected when a VPN connection was terminated.

→ After disconnecting several VPN connections within a tunnel group, it could happen that the newly established connections were not established to the same gateway as the remaining connections. This meant that communication via the load balancer was not possible.

Wi-Fi

→ In a Public Spot scenario, when using self-created welcome pages and using the authentication method “Login after declaration of consent”, an error message could appear during the first login to the system, claiming a missing e-mail address.

VoIP

→ In the WEBconfig configuration dialog for adding a new DECT handset, the field for assigning the handset ID was missing.

LCOS improvements 10.80.0345 RU2

New features

→ The ping command can be executed via WEBconfig under ‘Extras / Execute ping’.

→ The Internet setup wizard for mobile radio has been expanded to include providers from France, the USA and the Netherlands.

→ The broadcast bit for the DHCP client can now be switched. To do this, there is the parameter ‘B-DHCP’ in the selection for layer 3 in the WAN layer table on the console or in the LCOS menu tree.

→ Adjustments to the QinQ VLAN on the WAN: The scenario is now supported that both Ethernet types (e.g. 0×8100) are identical, but only one tag is included, or is ‘0’.

→ Additional status parameters for mobile radio are supported in the TR-069 data model TR-181.

→ Support for displaying the WWAN firmware version in the LMC.

→ With the LANCOM ISG-8000, parameters such as backlighting for the device display can be configured on the console.

→ The interface or WAN connection used for SIP registration is now also displayed in the VCM status table ‘Line’.

Bug fixes

General

→ With a high volume of IPSec data, enqueue errors could occur if packets were to be added to a queue that had already been released. In individual cases, this could lead to an immediate restart of the router in connection with further encrypted data traffic (e.g. HTTPS).

→ The vRouter only supports one CPU core. However, it could happen that the vRouter assigned jobs to several virtual CPU cores, which then led to an immediate restart.

→ A security vulnerability in the SSH protocol has been fixed (‘Terrapin’ security vulnerability/CVE-2023-48795).

→ In a scenario with config sync, it could happen that no synchronization of the configurations was carried out due to a failed TLS handshake.

→ With a TACACS+ login, it was not possible to use user names with more than 16 characters. User names can now contain up to 32 characters.

→ In a VRRP scenario in which ICMP line polling was used for a remote station, it could happen that a switch back from the backup device to the master device failed.
→ After disconnecting from the Internet, it could happen that the MAC address of the router was used instead of the stored user-defined MAC address.
→ The ‘Layer 7 application detection’ could not resolve packets with QUIC, as a result of which the corresponding data traffic was not listed in the statistics.
→ When using the Safari browser under iOS / macOS, the configuration could not be saved via WEBconfig.
→ In a scenario with DPS (Dynamic Path Selection), switching the session to a better line (passive switchover for DPS) for UDP packets did not work on central devices.
→ On 5G routers with an IPv6-only mobile connection, an IPv4 context is set up in addition to the IPv6 context. The IPv4 context reports a ‘link down’ after two minutes due to inactivity. This incorrectly led to the entire mobile connection being terminated.
→ When using the test mode (flash no), it could happen in individual cases that the complete device configuration was deleted after writing a configuration.

VPN

→ The ICMP polling function used an incorrect routing tag during the polling process, which could cause the connection setup to fail for IKEv2 connections for which a routing tag was specified in the routing table.
→ In individual cases, the router could restart unexpectedly if a large number of VPN operations were carried out in quick succession.

Wi-Fi

→ After an update to LCOS 10.80, PoE negotiation via LLDP no longer worked. As a result, access points that require PoE according to 802.3at for full functionality were only supplied with PoE according to 802.3af. This limited the functionality of the access points.
→ When using the Public Spot mode ‘Login data is sent via SMS’, no country code could be selected on the landing page.

VoIP

→ If the Voice Call Manager routed an incoming call to an internal user with multiple registrations (SIP user with multiple SIP registrations or ISDN user with activated parallel call), who forwarded the call to another subscriber, the Voice Call Manager did not send a source phone number. As a result, the phone number of the original caller was not sent to the other subscriber.

→ The Voice Call Manager does not support RTP extensions. If the Voice Call Manager received an incoming call with RTP extensions, it also sent the RTP extensions in the ‘SDP Answer’. This meant that the called party could not hear the caller.
The Voice Call Manager no longer sends RTP extensions in the ‘SDP Answer’.

→ If the encryption function was activated in the settings of a SIP line, an IPv6 registration with the registrar forced in the ‘SIP domain/realm’ field with the suffix ‘?6’ did not work.

→ During a call via the Voice Call Manager, it could happen that reserved memory was overwritten. This led to an immediate restart of the router.

→ If the Voice Call Manager in INVITE received two alternative media streams (m=audio) with different ports from the SIP provider, the router only responded with one media stream in the “200 OK” to the provider. This resulted in the call being terminated by the SIP provider.

→ In a scenario with a connected SIP PBX, the Voice Call Manager incorrectly sent a CANCEL to the SIP PBX after forwarding an incoming call to an external subscriber via SIP302.

LCOS improvements 10.80.0233 RU1

New features

→ Support of Zero Touch commissioning for the LANCOM 1800 Blackline series and LANCOM 1900 series on the WAN Ethernet port. For this purpose, the device must be delivered with LCOS 10.80 RU1 or higher or a reset must be performed after the update to LCOS 10.80 RU1.

→ The operating mode for the rollout agent is now ‘Off’ by default.

→ If a connection is terminated, extended information is now displayed in the syslog for WWAN.

→ When displaying tables with many entries in WEBconfig, the entries are now displayed on several pages by pagination.

Bug fixes

General

→ Using WEBconfig, a maximum value of 2147483647 could be entered in the ‘Remote AS’ field in the ‘Configuration / Routing protocols / BGP / Neighbors’ menu, although higher values were also possible via the console and LANconfig.

→ If several ARF networks were configured on a router with the same IP address (separated by VLAN), a configuration change in the ARF networks triggered ‘gratuitous ARP flooding’ in each network. In scenarios with a large number of identical ARF networks, this could lead to severe packet loss and also to an immediate restart of the router.
After changing the configuration of the ARF networks, only one ‘gratuitous ARP’ is now sent for each network.

→ If there were a large number of routing entries on a router (e.g. learned via BGP) and all interfaces were read out by a monitoring tool via SNMP (SNMP path 1.3.6.1.2.1.4.24.4, RFC 2096), the router’s CPU was fully utilized. The router was then restarted immediately.

→ The 4G LED of the LANCOM 1800VA-4G was permanently lit blue, even if the cellular module was not active.

→ A faulty BGP base attribute could cause the BGP connection to be terminated (VU#347067).

→ If the remote destination (such as an access point) confirmed several packets with an ACK in an L2TP tunnel to a router, this meant that the sessions on the router were not deleted when the connection was terminated. As a result, the L2TP connections could not be re-established.
→ OpenSSL has been updated to version 3.0.12.

Wi-Fi

→ For access points with a fixed frequency band on a WiFi6 WLAN module, different frequency bands could be selected via WEBconfig.
→ In LCOS 10.80 Rel, the Public Spot templates no longer worked due to changes to the paths for the jquery libraries.
There are now new variables for the jquery libraries and new Public Spot templates. If you want to use your own templates with LCOS from version 10.80 RU1, you must use the new versions.

VPN

→ If the router received an 'Informational request' with a DELETE(CHILD_SA) message followed by a DELETE(IKE_SA) message when an IKEv2 connection was established, this led to an immediate restart of the router.
→ IDS blocked the keepalive packets of a GRE tunnel because the firewall expected at least 2 bytes of user data in GRE packets after the protocol field. As a result, the GRE tunnel was repeatedly taken down.
→ No certificate containers (PKCS12) could be uploaded to one of the VPN certificate slots via WEBconfig. The process was always acknowledged with the messages "Upload failed" and "Incorrect password or invalid file type".

VoIP

→ If the Voice Call Manager received a duplicate 'Connection Information' with different IP addresses during an incoming call in a dialog ("180 Ringing", "183 Session Progress" or "200 OK"), it could happen that the Voice Call Manager sent the answer to the wrong IP address. This led to a one-sided voice transmission.

LCOS improvements 10.80.0155 Rel

New features

→ Support of the re-init function for 5G modules
→ Support for N:N NAT for multicast data packets (not for SSM)
→ Support for WWAN status values RSRP, RSRQ and SINR and display in WEBconfig dashboard
→ Improvement of the hard disk performance of the LANCOM vRouter

Bug fixes

General

→ If an incorrect APN was entered on a mobile router with a 5G module, this led to an immediate reboot of the router after a few minutes.
→ If an SFP-GPON-1 module with activated 'Dying Gasp' function was plugged into the LANCOM router, no automatic configuration change with subsequent restart of the module took place. As a result, the PON management connection did not start and remained in the 'Opening management connection' state.
→ After an undefined time (it could be several weeks), the WWAN module switched itself off and was then in the 'Deactivated' state. As a result, an Internet connection was disconnected.
→ With mobile routers, it could happen that an error was displayed in the connection information of the mobile connection (Status/Modem-Mobile/Connect-Info), although the connection was established.
→ On a serial device connection, an active session was not disconnected when using the 'passwd -n' command in a script.
→ The value specification for memory usage was incorrectly output on the display page for LANCOM devices with LCOS.
→ When forwarding to an external RADIUS server, the specified IP address was entered in reverse order in the configuration at the LANCOM 1800EFW.
→ As soon as a new configuration was imported into a LANCOM 1900EF-5G via script, the WWAN modem remained in the 'Device Removal/Deactivated' state. The WWAN modem could only be set to active mode by restarting the device.
→ On some LANCOM mobile routers, the built-in WWAN module did not provide a network identifier in text form. As a result, the 'Network' field remained empty after a query (e.g. via CLI with 'ls /Status/Modem-Mobile').

VPN

→ If a LANCOM router received an ‘INVALID_SPI notification’ from another router, the LANCOM router deleted the child SA of the associated IKEv2 connection. It could happen that the memory of the deleted child SA was occupied twice. This led to an immediate reboot of the router.

→ In individual cases, it could happen that the ‘Security Associations’ of a VPN connection were not terminated when switching to a backup connection. As a result, the VPN connection could no longer be established. In such a case, the message “VPN: local reconnect lock active” was displayed in a VPN status trace.

Wi-Fi

→ UDP traffic could also be transmitted without logging into the Public Spot, allowing some applications to communicate with their servers on the Internet.

→ A managed access point did not use the VLAN ID entered in the SSID in the WLAN controller, but always the VLAN ID available in its local configuration in the group key index. This meant that broadcasts and multicasts could not be decrypted and thus could not be transmitted.

→ The source VLAN check (Setup/Public Spot modules/Check origin VLAN) in the Public Spot only worked for VLANs that were assigned via RADIUS. If the VLAN was assigned via another method (e.g., via circuit ID), the WLAN client was not logged out of the Public Spot and could communicate in other existing Public Spot SSIDs.

→ If a framing error occurred on the serial bus to the ePaper radio module, the connection to the ePaper displays was lost and the displays could no longer be updated. In such a case, the error messages “AccessPoint - An error occurred, need to restart WePaper Access-Point” and “SerialInterface - Error in communication with RF-Module!” were output in the syslog of the access points.

The connection between the ePaper radio module and the ePaper displays is now re-established even without a restart of the access point.

VoIP

→ In a SIP trunk scenario with gateway line to a SIP PBX, when the router received a ‘RE-INVITE’ from the SIP provider on the SIP trunk with ‘refresher’ in the ‘Session-Expires’ header (in this case ‘refresher=uas’), the Voice Call Manager changed the ‘refresher’ in the “200 OK” to the SIP provider (to ‘refresher=uac’), which is not allowed. This caused the call to be disconnected by the SIP provider.

→ If analog or ISDN devices were connected to the router, the Voice Call Manager always sent the codecs PCMA (G.711-a) and PCMU (G.711-u) in the SDP offer as soon as one of the two codecs was contained in the SDP offer. Now all codecs except PCMA and PCMU are deleted from the SDP-Offer and the first codec is taken over into the SDP-Answer. If PCMU is used, the Voice Call Manager transcodes this to PCMA, since ISDN and analog devices only support PCMA. If there is no SDP-Offer in the INVITE, the Voice Call Manager answers with PCMA and PCMU in the SDP-Answer.

LCOS improvements 10.80.0124 RC2

New features

→ The DHCPv4 client supports the MTU option.

Bug fixes

General

→ On a LANCOM 1793VA-4G, the SIM card remained offline when the router was without power or a cold boot was performed via the command line.

→ Running a script with the ‘beginscript’ and ‘exit’ commands sporadically caused existing BGP connections to be disconnected.

→ The IPv6 firewall used a non-existent content filter profile ‘CF-PARENTIAL-CONTROL-PROFILE’ instead of ‘CF-PARENTAL-CONTROL-PROFILE’.

→ Deprecated SSL/TLS default settings were used in the ‘Setup/Mail’ path. The following default values are now used:

- at least TLS 1.2
- no MD5/SHA1
- no 3DES
- exclusively Key Agreement with PFS

→ A newly added ‘Virtual link’ was not automatically detected with OSPF enabled. OSPF had to be globally deactivated and reactivated for this.

→ The TR-069 service sent its requests with the IP address instead of the DNS name of the ACS server. This caused the TLS connection to be terminated on a strictly configured ACS server with SNI because the URI and the name in the certificate did not match.

VoIP

→ When DNS resolving SRV records via NAPTR, the output of the console command ‘show vcm dns’ always displayed one SRV record more than was actually resolved.

LCOS improvements 10.80.0075 RC1

New features

→ Support for Let's Encrypt certificates (ACME client) for WEBconfig and the LANCOM Public Spot
→ Zero-touch rollout for mobile routers together with the LMC
→ WEBconfig in new corporate design
→ Support for Google Cloud (GCP) for the LANCOM vRouter.
→ Support for High Availability Clustering Option L for the LANCOM 1900 series.
→ Routers can record and store traces and Wireshark captures directly on a USB stick.
→ Entries in the action table can be tested or executed by a CLI command.
→ Support for the 'Automatic APN' feature on cellular routers.
→ Access to RPCap and LCOScap via WAN can be configured.
→ The GPON status can be displayed on the WEBconfig dashboard.
→ The GPON password can now also be entered in HEX format (20 characters).
→ Accounting in the router has been reworked and can now also be used to display the throughput of current sessions of stations in the analysis case.
→ Support for configurable responses to incoming SMS messages on cellular routers, e.g. sending reply SMS messages for re-billing when data volume is used up.
→ Support for cold standby on cellular routers
→ The input option for the main device password and additional administrators has been extended to a maximum of 128 characters. When using the new password length, a downgrade to older LCOS versions is no longer possible.
→ The status table 'Protocol-Table' under '/ Status / IP-Router' is omitted.
→ The 'LTE-Delayed-Attach' switch on cellular routers is omitted.
→ The 'Stack Errors' status counter of the IP router is omitted.
→ The 'Establish-Table' status table is omitted.
→ The 'Tx-normal', 'Tx-urgent' and 'Tx-reliable' columns in the '/ Status / WAN / Packet Transport' table are omitted.
→ Support for SSL 3.0 and ciphers with 56 bits or less has been removed.
→ Support for 3G (USB) WWAN modems has been removed completely.
→ WEBconfig certificates generated by LCOS now only have a maximum validity of 365 days.
→ 464XLAT and DS-Lite can be used as backup.
→ Support of the operating switch for SMS

→ Disabling syslog now also disables the regular writing of the syslog backup to the internal flash memory.
→ DHCP and DHCPv6 servers are displayed in WEBconfig under ‘Services’.
→ The ‘(VLAN) Priority Bit’ can be set for WAN connections.
→ Additional DHCP options can be configured on the DHCP client.
→ Additional DHCPv6 options can be configured on the DHCPv6 client.
→ Support for interim accounting in Netflow
→ Netflow now uses 64 bit counters internally.
→ Support for dual stack (IPv4 / IPv6) in Config Mode with IKEv2 against the LANCOM Advanced VPN Client.

Bug fixes / improvements

General

→ For routers with multi-core CPU (e.g. LANCOM 1800 series), only the utilization for CPU core 0 was displayed in the console path ‘Status / Hardware info’. Now the average value of all CPU cores is displayed.
→ After activating a VPN-25 option on a router (no reboot required), the device certificate could not be downloaded in WEBconfig via the ‘Download current CA certificate’ option when the CA was activated. The process was acknowledged with the error message ‘Not found’. The download of the certificate was only possible after a restart.

VoIP

→ If the Voice Call Manager received both the P-Asserted-Identity (PAI) and the P-Preferred-Identity (PPI) in an INVITE from a SIP PBX, the Voice Call Manager then used the phone number in the PAI. If this phone number was not known to the SIP provider in a scenario with CompanyFlex connection (e.g. due to a missing digit), the call was disconnected and acknowledged with the error message “403 Forbidden”.
There is now an additional parameter ‘Prefer-Identity-Field’ in the path ‘Setup / Voice-Call-Manager / Users / SIP-Users / Users’. This can be used to select whether the PAI (Prefer-PAI) or the PPI (Prefer-PPI) should be preferred (default setting is PAI as before).

7. General advice

Disclaimer

LANCOM Systems GmbH does not take any guarantee and liability for software not developed, manufactured or distributed by LANCOM Systems GmbH, especially not for shareware and other extraneous software.

Backing up the current configuration

Before upgrading your 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 LANCOM Systems.

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 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 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.