

LANCOM Release Notes

LCOS 10.20 Rel

Copyright (c) 2002-2018 LANCOM Systems GmbH, Wuerselen (Germany)

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: <http://www.lancom-systems.com>

09.11.2018, CBuersch

Table of Contents

1. Preface	2
2. Device-specific compatibility to LCOS 10.20	2
3. Advices regarding LCOS 10.20	3
3.1 Information on default settings	3
3.2 Information on the LANCOM vRouter	3
4. Feature overview LCOS 10.20	4
4.1 Feature highlights	4
4.2 Further features	5
5. History LCOS 10.20	6
LCOS improvements 10.20.0145 RC2 > 10.20.0175 Rel	6
LCOS improvements 10.20.0097 RC1 > 10.20.0145 RC2	8
LCOS improvements 10.20.0097 RC1	10
6. General advice	13
Disclaimer	13
Backing up the current configuration	13
Using converter firmwares	13

1. Preface

LCOS ("LANCOM Operating System") is the operating system for all LANCOM routers, wireless LAN access points and Wi-Fi controllers. In the context of the hardware given by the products the at a time latest LCOS version is available for all LANCOM products and is available free of charge for download from LANCOM Systems.

This document describes the innovations within LCOS software release 10.20 Rel, as well as the improvements since the previous version.

Before upgrading the firmware, please pay close attention to chapter 6 „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

<https://www.lancom-systems.com/service-support/instant-help/common-support-tips/>

2. Device-specific compatibility to LCOS 10.20

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 under

<https://www.lancom-systems.com/products/lcos/lifecycle-management/product-tables/>

As from LCOS 10.20, support for the following devices is discontinued

- > LANCOM IAP-321
- > LANCOM IAP-321-3G
- > LANCOM OAP-321
- > LANCOM OAP-321-3G
- > LANCOM OAP-322
- > LANCOM IAP-3G
- > LANCOM 1781A-3G

3. Advices regarding LCOS 10.20

3.1 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 LAN-config under Management > LMC. You can manually re-enable the usage of the LMC whenever you want.

3.2 Information on the LANCOM vRouter

If you had initially installed a vRouter instance using LCOS 10.20 RC1 or LCOS 10.20 RC2, it is necessary to reinstall the vRouter with LCOS 10.20 Rel.

The LANCOM vRouter for Microsoft Hyper-V will be available with a future LCOS release update.

4. Feature overview LCOS 10.20

4.1 Feature highlights

WPA3 - State-of-the-art Wi-Fi security

The latest generation of Wi-Fi encryption - WPA3 (Wi-Fi Protected Access) - now offers you more security for your WLAN infrastructure. As the successor of WPA2, WPA3 offers important extensions and security features for small („WPA3-Personal“) and large networks („WPA3-Enterprise“). With LCOS 10.20, all LANCOM access points and WLAN routers support the new Wi-Fi security standard. Learn more in our [Whitepaper](#)

Auto Updater – always up-to-date

The Auto Updater keeps your installations up-to-date automatically: If desired, LANCOM devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install only security updates, release updates, or all updates automatically. If automatic updates are not desired, the feature can still be used to check for new updates, which can then be installed with a single click.

Client Management – for best-ever Wi-Fi

Client Management steers Wi-Fi clients to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes—whether they operate stand-alone or orchestrated by the LANCOM Management Cloud. The popular Band Steering and Client Steering, which so far were separate features, have now been combined and even operate without a WLAN controller.

LEPS-U & LEPS-MAC

Keep control of who is in your Wi-Fi. With LEPS-U (LANCOM Enhanced Passphrase Security – User), individual clients or entire groups each receive a unique Wi-Fi password for an SSID. Using LEPS-MAC, you additionally authenticate the clients by their MAC address—ideal for secure corporate networks.

WAN Policy-Based NAT

WAN Policy-Based NAT allows an easy assignment of static WAN IPv4 addresses to desired services. Due to a NAT action in the firewall rules internal addresses are masked behind a WAN address from the Internet access provider. Ideal for scenarios e.g. for the operation of mail servers and web servers with different WAN addresses.

4.2 Further features

Enhanced Open

Thanks to the introduction of additional data encryption, Enhanced Open improves the security of clients in open Wi-Fis such as hotspots in cafés or hotels.

DSL-Bridge-Mode

VDSL routers now operate optionally in DSL bridge mode. This allows a device to work purely as a DSL modem. Ideal for scenarios where multiple DSL connections are operated on one router.

Even more flexibility for the LANCOM vRouter

The LANCOM vRouter now supports the Microsoft Hyper-V virtualization platform. Furthermore: Managing the vRouters is now even easier, because firmware updates are easy to import as a UPX file.

OCSP responder – more power for Smart Certificate

Maximum security with VPN access: Smart Certificate is the easy way to create digital certificates with your LANCOM device—without any need for an external certificate authority. This feature has now been extended to include the OCSP (Online Certificate Status Protocol) network protocol, which enables clients to automatically and efficiently query the integrated CA for the status of X.509 certificates.

LISP (Locator / ID Separation Protocol) support

The Locator / ID Separation Protocol (LISP) is a new routing architecture. LISP allows the implementation of highly scalable networks with an integrated routing protocol, tunneling, and overlays. Ideal for service providers or enterprise networks.

Public Spot CSV import

Public Spot management is now even easier: Hotspot users are easily imported and exported by text file (CSV).

You can find further features within the individual builds sections in chapter 5 „Historie LCOS“.

5. History LCOS 10.20

LCOS improvements 10.20.0145 RC2 > 10.20.0175 Rel

New features

as from LCOS 10.20 the Voice Call Manager (VCM) is activated by default for the following devices:

- > LANCOM 1900EF
- > LANCOM ISG-1000
- > LANCOM ISG-4000

For the following devices the VCM can be activated using the All-IP Option:

- > LANCOM 1640E
- > LANCOM 1780EW-4G+
- > LANCOM 1790-4G
- > LANCOM 7100+ VPN
- > LANCOM 9100+ VPN

Bugfixes / improvements

General

- > The routing method „Obey DiffServ field“ did not work correctly due to packets marked with AFxx were not only allocated to the send queue „SAFE“, but also to the send queue „URGENT“. This resulted in QoS rules having no effect, because not only packets which had to be handled as preferred, but also subordinate packets were forwarded via URGENT queue.
- > With activated SNMP SNMPv1/2 as well as SNMPv3 was shown with active status in the service table under Status/Config/Services/, even if one of both protocols was not activated. The status is now shown separately for each protocol.
- > Due to a polling failure mobile connections with activated ICMP polling were disconnected right after connection establishment.
- > The mobile radio module MC7710 of the LANCOM 1781VA-4G stated faulty network name values for some providers, so that these values were shown in LCOS and LANmonitor. In such cases, now the numeric identifier of the provider network is shown.

VPN

- > When using IKEv2 with activated PFS it could happen that after a re-keying or immediately after connection establishment ESP tunnels could no longer be used for data communication, if the LANCOM router established a connection to a third-party provider.

Wi-Fi

- If a LANCOM device which is compatible to the LANCOM Public Spot XL Option was paired to the LANCOM Management Cloud, the Public Spot XL Option did not activate itself automatically on the device.

VoIP

- If a SIP domain which referenced to another alias name instead of the IP address (CNAME) was specified as SIP registrar, the SIP registration was not possible.

LCOS improvements 10.20.0097 RC1 > 10.20.0145 RC2

New features

- > LANCOM Auto Updater for automatic firmware updates
- > Support for WPA3
- > Enhanced Open for improved client security in open Wi-Fis
- > Redistribution of RIP routes in BGPBugfixes / improvements

Bugfixes / improvements

General

- > Obtaining DHCP addresses via WLC- or EoGRE tunnel could fail due to IP packet related processing problems. Rarely, this could lead to a sudden router restart, too.
- > Due to a faulty channel allocation on Wi-Fi routers an IPoE connection which was configured on a DSL interface (e.g. DSL-1) was allocated to an ISDN interface.
- > When using a backup connection via backup table, switching from the main to the backup connection caused TCP sessions to not being taken over to the backup connection or not being terminated accurately. Additionally, DNS requests were not using the established backup connection.
- > If the access to the management protocol „TFTP“ was forbidden from WAN side, the router answered a port scan with a „TFTP error (Access violation)“. The following „TFTP ack“ of the port scanner was answered with the message „Destination unreachable (Port unreachable)“. Now a port scan is immediately answered by the router with a „Port unreachable“message.
- > When executing a file system operation in the Layer 7 application detection (enabling an internal resource), a sudden LANCOM router restart could occur.
- > Due to a missing initialization during a LANCOM router start, all interfaces which were set disabled on startup were shown as active on an SNMP request.
- > If only one DSL remote station was configured and active, MLPPP packets did not contain a multilink header, which led to these packets always being sent on the first channel (master channel).
- > When using a LANCOM router as a VDSL modem the bridge stopped working after a short time. This caused a non-working Internet connection.
- > After disconnecting the ADSL connection (e.g. forced provider disconnect) the Internet connection was not re-established in some cases. This behavior occurred, if a VDSL remote site (with VDSL as layer 1) was used on an ADSL line.
- > When using a Plain Ethernet connection (IPoE or DHCPoE), ICMP polling failed if the sender address specified a network with an allocated, but unplugged Ethernet port. Due to this, the Plain Ethernet connection could not be established.

Routers & VPN

- › The speed of establishing VPN tunnels on central site VPN gateways has been improved in big scenarios.
- › The VPN status trace output used an IKEv2 technology term while negotiating a phase 2 SA of an IKEv1 connection.
- › Simultaneously disconnecting and connecting an IKEv2 connection with simplified dial-in could cause a sudden LANCOM router restart.

Wi-Fi

- › If the amount of "Max-Login-Tries" was set to "0" in the path "Setup / Public-Spot-Module / Brute-Force-Protection", and thus the brute force detection function was disabled, the function was still active and a Public Spot user could not log on to the system.
- › When using an access point with two 802.11ac Wi-Fi modules (IAP-822, OAP-822 and OAP-830), switching between the two modules by a Wi-Fi client caused a sudden router restart because a wrong interface pointer was allocated, if the Wi-Fi client did not log off or had not been logged off.

VoIP

- › After a router restart it could occasionally happen that incoming calls were not signaled on an IPv6 SIP provider line. The telephony worked only after disabling and re-enabling the Voice Call Manager.
- › In scenarios with routing tags for all IP networks and routing entries it could occur in certain constellations that telephony via Voice Call Manager led to a unidirectional communication. An option was implemented now to configure one loopback address (sender address) per SIP line. Using these lines, the outgoing path can now be explicitly defined.
- › The Voice Call Manager did not check the server name stored in the SIP domain/realm when using TLS authentication. This led to SIP registrations executed even if the server name in the SIP domain/realm did not match the certificate's server name.

LCOS improvements 10.20.0097 RC1

New features

General

- › LANCOM vRouter: Support for Microsoft Hyper-V
- › LANCOM vRouter: Support for firmware updates via UPX files
- › WEBconfig: Requests for the unencrypted site on port 80 are automatically redirected to the secure site (port 443). This behavior is activated automatically after a device reset.
- › 'Boot-Cause' is available as an environment variable.
- › The RADIUS server supports user-defined RADIUS attributes per RADIUS user.
- › A search on the CLI is possible via 'find' command.
- › Administrators from the table 'Further administrators' do no longer have read- or write permission within this table.
- › The readscript option '-o' suppresses the output of passwords within scripts.
- › The DSCP tag for internal services can now be configured.
- › Physical Ethernet ports are now enclosed within the lfx- and lf-tables of the SNMP-IF-MIB.

Routers & VPN

- › The configuration logic of the IPv6 WAN interfaces has been changed.
- › WAN Policy-Based NAT: WAN Policy-Based NAT allows address translation (masking) of connections based on firewall rules.
- › DSL bridge mode for all LANCOM VDSL routers: As of now, all VDSL routers can be set into a DSL bridge mode.
- › OCSP responder/server for online certificate check
- › Support for LISP (Locator/ID Separation Protocol)
- › Configurable target port for IKEv2 and switchable encapsulation (UDP, HTTPS)
- › Adaption of the IKEv1/IPSec default crypto algorithms to current standards
- › Adaption of the TLS default crypto algorithms to current standards
- › Adaption of the SCEP default crypto algorithms to current standards
- › BGP: Support for LISP route redistribution
- › BGP: The administrative routing distance can be configured per policy.
- › A particular sender address can be configured for DNS forwarding.
- › Besides the Rollout wizard another four programmable WEBconfig wizards can be uploaded.
- › The form for Dynamic VPN registration is no longer available
- › Enhanced support for DHCP option 43 in the DHCPv4 server
- › Support for DHCP option 82 in the DHCPv4 server
- › A sender address (loopback address) can be configured via the DHCP relay agent.
- › The function automatic WAN tag creation has been omitted, see knowledgebase article
- › [Option for automatic WAN tag generation omitted.](#)

- › The switch for configuring the building of the IPsec SAs is no longer available. IPsec SAs are now built combined.

Wi-Fi

› WLAN Client Management

WLAN Client Management permanently directs Wi-Fi clients to the ideal access point and frequency band. As a consequence, this feature improves the quality of wireless networks regardless of their dimension - whether or not in standalone operation or orchestrated via the LANCOM Management Cloud. The popular, but so far separated functions Band Steering and Client Steering are hereby combined and provided even without operating a WLAN controller.

› LEPS-U

LEPS-U (LANCOM Enhanced Passphrase Security - User) gives you the opportunity to specify an individual Wi-Fi password for an SSID for individual clients or whole groups.

- › Public Spot user accounts / RADIUS user accounts can be imported and exported via CSV files.
- › Public Spot with login after statement of agreement: The point of time for the the day account limits reset is now configurable.
- › Active Public Spot sessions are terminated when deleting the user via the 'Manage user' wizard.
- › The former Public Spot user list has been removed and is no longer supported. Existing configurations are converted to RADIUS entries automatically.
- › Support for a dynamic negotiation of the PoE power via LLDP instead of class-based
- › Support for DStoL over WLAN for all access points and Wi-Fi routers
- › The configuration item 'Transfer only unicasts, suppress broad- and multicast' is now available for LANCOM WLC devices.
- › The WLC-controlled automatic radio field optimization now considers DFS channels, too.

Bugfixes / improvements

General

- › In the LCOS path '/Setup/Certificates/SCEP-CA/Client-Certificates' the fields 'Challenge-Passwords' and 'General-challenge-password' were not defined as password fields.

Routers & VPN

- › When specifying an IKEv2 remote gateway, a maximum of 40 characters could be used. This value has been increased to 64 characters.

Known issues

- › Obtaining DHCP addresses via WLC- or EoGRE tunnel may fail due to IP packet related processing problems. Rarely, this may lead to a sudden router restart, too.

6. 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 use any firmware from version 8.8 in your LANCOM 1722, 1723, 1724, and in the L-320agn, L-321agn, and L-322agn (less than hardware release E), enough space must be available in the memory of your device.

Due to the implementation of several new features within the current build of the firmware, it is no longer possible to store two main firmware versions side by side. To gain more free space for the current version, it is now necessary to upload a converter firmware into your device. The converter-firmware has a much smaller size, so that it is now possible to store the main release of the firmware besides the converter-firmware.

This setup is only necessary once for a single device and is done with the so-called converter-firmware (see readme.pdf of the affected devices).

After having flashed the converter-firmware the firmsafe function of the LANCOM device is available only on a limited scale. The update to a newer firmware is furthermore possible. However, in case of an update failure the LANCOM will only work with a minimal-firmware which allows just local access to the device. Any extended functionality, in particular remote administration, is not possible when running the minimal-firmware.