LANCOM Systems

Information regarding

LCOS Software Release 7.82 RU6

LANCOM Systems GmbH
Adenauerstrasse 20 / B2
52146 Wuerselen
Germany

Internet: http://www.lancom.eu

01.07.2011, CBuersch

Table of contents

1. Preface

LCOS („LANCOM Operating System“) is the operating system for all Wireless LAN Access Points and Routers. 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 dowload from LANCOM Systems.

This document describes the innovations within LCOS software release 7.82 RU6, as well as the changes since release 7.72

Warning hint – Backing up the current configuration

Before upgrading the firmware to LCOS 7.82 it is essential to backup the configuration of your router. Due to extensive features it is not possible to downgrade to a previous firmware without using the backup configuration.
Please see the reference manual for instructions on how to backup the router configuration.

If you want to upgrade devices which are only accessible via router connections or WLAN bridges, please keep in mind to upgrade the remote device first and the local device afterwards.

Note – Upgrading central site components

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

Note – Using converter firmwares

You will need enough free memory to use a firmware 6.0 and newer in your LANCOM 15x1, 1611+, 821+ and DSL/I-10+.
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 firmsave 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.

Note – Dynamic VPN registration

By reason of patent you have to register the functionality „Dynamic VPN“ with IP address transmission over ISDN. This operating mode is usually required when you configure a VPN tunnel with dynamic IP addresses on both sides without dynamic DNS services.
Any other Dynamic VPN operation mode (e.g. transmitting the IP address via ICMP, provoking a callback etc.) does not require registration.
The registration process is fully anonymous - no personal or company data will be transmitted.

The registration of the Dynamic VPN option requires administrator rights on the LANCOM device.

Note – Using VoIP options

VoIP options for LANCOM 1821 Wireless ADSL are dicontinued with LCOS 7.20. The final version containing the VoIP Call Manager is LCOS 6.32.
As from LCOS 7.5x support for VoIP options for the devices LANCOM 1511 Wireless DSL and 1521 Wireless ADSL is discontinued. The final version containing the VoIP Call Manager is LCOS 7.30.
For the „VoIP ready“ routers LANCOM 1711 VPN, 1721 VPN and 1811 Wireless DSL support for the subsequently installed VoIP option will be discontinued with LCOS version 7.56. If you want to continue using your VoIP option, please do only use LCOS versions up to and including 7.54.
For T-Systems Business LAN R800+ VoIP functionality is discontinued in LCOS 7.60
LCOS 7.70 is the final version supporting VoIP options for the remaining „VoIP ready“ devices.

2. Known Issues

Latest support notes and known issues regarding the current LCOS version can be found in the download area of our website http://www.lancom-systems.eu/Common-Support-Hints.64.0.html

3. New Features, Changes and History

LCOS changes 7.82.0156 RU5 ► 7.82.0159 RU6

Bugfixes / Changes:

Network Connectivity:

- An NTP update does not extend the CRL update interval to one day if the CRL could not be successfully loaded before.
- If the CRL could not be loaded due to an error, there are continuous attempts to receive the CRL from the CA.
- If no valid CRL exists although CRL check is configured, certificates are marked as temporarily invalid

LCOS changes 7.82.0135 RU4 ► 7.82.0156 RU5

New Features:

Network Connectivity:

- A VPN remote station can be admitted to certificate- and preshared-key-connections by using a mixed proposal list. If the LANCOM device has no valid certificate for a VPN connection, the effectively used proposal list is limited to preshared-key proposals
- A routing tag from the PPTP table is evaluated for incoming connections, too

Bugfixes / Changes:

Network Connectivity:

- In case of repeatedly recurring backups the configured remote station connections are established in the configured order
- A lost TACACS+ connection will be closed after ten minutes, so the connection to the TACACS+ server can be re-established
- If an SSH connection is cancelled while reading a configuration/script, the connection is closed within the LANCOM device
- Fixed a memory leak which occured when the cellular radio modules of a LANCOM 1751 were reset (e.g. no SIM card inserted/recognized or no roaming coverage)
- The LANCOM device does no longer boot with an LCOS watchdog if no username is specified for TACACS+ login via WEBconfig
- The command „show dlyfnc“ does no longer lead to an LCOS watchdog
- Fixed a small memory leak on configuration changes with disabled TACACS+

LCOS changes 7.82.0121 RU3 ► 7.82.0135 RU4

Bugfixes / Changes:

Network Connectivity:

- Reassembling of fragmented data packets done by the LANCOM device can be used in combination with N:N NAT
- If a SYNACK is received with zero window size for a TCP connection which was established by the remote site, the connection is not abandoned. This modification works around a misbehaviour which occurred after a DynDNS.org server update
- DynDNS access for provider „DynAccess.de“ can be configured accurate via WEBconfig wizard
- Data packets which were sent from a loopback address will not be masked
- Correct checksum setting of reassembled data packets which had their addresses changed by N:N NAT
- Reconfiguration of the RIP RFC2091 mode is applied instantly
- If the default route is part of the LAN and terminates a further logical connection (e.g. VPN or PPTP), packets will be dropped by IDS if there exists no back route or rather was learned by RIP
- The initiator does no longer insist on RFC2091 if the remote site falls back to multicast RIP
- The switching status (sticky or conditional) of a routing table route is evaluated by RIP even if the gateway is part of the LAN
- Changes in the link state of an ARF network are reliably propagated via RIP
- Packet loss in RIP RFC2091 negotiation does now reliably lead to a fallback to Multicast-RIP

LCOS changes 7.82.0120 RU2 ► 7.82.0121 RU3

Bugfixes / Changes:

Network Connectivity:

- No more LCOS watchdog when checking a LANCOM without or with outdated TACACS+ password

LCOS changes 7.82.0105 RU1 ► 7.82.0120 RU2

Bugfixes / Changes:

Network Connectivity:

- Dynamic VPN packets are checked more strictly. This avoids LCOS restarts by reason of faulty memory structures
- Aborted UMTS connection establishments due to unknown failure will cause a UMTS module reset, too
- Fixed an LCOS-Watchdog when finishing the Public Spot wizard
- Entries changed per „add“ command are written to flash memory using the „flash yes“ command, if there was no “set” command used in the meantime
- Non-established calls on an external ISDN line do not lock up new calls
- Before restart an accounting-end is sent to the RADIUS server, so the accounting session is not closed by a timeout. Thus, Public Spot users can re-register immediately
- Corrected distribution of outgoing ISDN calls to the ISDN lines
- Not all firewall sessions are restarted after configuration upload. This fixes connection losses of time-critical applications
- Extended re-init cycle for the LANCOM 1751, so that the used UMTS modules 8780 and 8781 are completely reset, too
- RIP routes are always sent via the correct PPTP tunnel
- If an already negotiated VPN tunnel is disconnected due to a timeout, no more phantom entries (which would prevent a VPN reconnect) are generated in the VPN connection list,
- VPN connections which do remain in „incoming“ state are terminated via connection monitoring
- Connection monitoring timers are not terminated early on temporally overlapping VPN connection establishments or disconnects. In case of error, negotiated SAs are correctly terminated and thus do not prevent VPN tunnel re-establishment
- RIP metrics is set correctly after disconnecting a remote station

LCOS changes 7.82.0020 Release ► 7.82.0105 RU1

Bugfixes / Changes:

VoIP:

- If the registration of a SIP provider line was denied with a 423 response, the next registration can immediately take place

WLAN:

- After radar detection the channel list is furthermore respected
- WLC-communicated fixed IP addresses and VLAN settings are completely adopted, even if the management VLAN is not 1
- Using public spot wizard of a WLC doesn't restart the device anymore
- With DFS2 the complete channel choice is available.

Network Connectivity:

- During active PPTP tunnel establishment GRE packets are no longer sent as broadcasts, but are sent directly to the next router's MAC address
- An appropriate timeserver can be added in WEBconfig
- Simplified certificate dial-in can even be used if there are only single certificates (without PKCS#12 container) stored in the LANCOM
- A cancelled telnet session does no longer deny access
- Incoming PPTP connections can be established using DNS names
- A RADIUS authentication can happen through a PPTP tunnel
- Incoming VPN connections on tagged default routes are displayed correctly in the connection statistics
- If the firewall rule table is empty entries in the connection table do age, though
- If a configuration is written with an empty firewall rule table, this table is taken completely
- If a broken connection is forwarded to another router due to RIP, answer packets are no longer sent to the disconnected remote station
- Connection failures can be deleted via LANmonitor/SNMP
- Corrected change of route via WAN-RIP
- Corrected transfer of the XAUTH username length to the external RADIUS server
- Incoming PPTP connections are logged to PPTP statistics only after successful connection establishment
- Internal services do not trigger connection establishment if the VRRP device is in standby state
- Writing of huge configfiles / scripts to flash has been speeded up
- Better monitoring of boot process
- A monitoring job checks the UMTS module of he LANCOM 1751 UMTS. If the module isn`t available with all necessary COM ports it will be reset
- At 100 SNMP requests per second the device will not restart with an LCOS watchdog
- CRL requests can be allocated to a single ARF network
- Within a SCEP request several Organizational Units can be declared in Destinguished Name

LCOS changes 7.80.0081 Release ► 7.82.0020 Release

Bugfixes / Changes

VoIP:

- Modified ISDN bus self test timing for LANCOM 1823 VoIP
- After a WAN connection reconnect the overlying PBX line is reconnected, too
- The Advanced VoIP Client can be used again

WLAN:

- Individual configuration of the relation between all LAN- and WLAN interfaces for LAN link error detection

Network Connectivity:

- ADSL protocol switching works with established connections, too
- A firewall rule with a loadbalancer connection as target applies even if the actual target is one of the loadbalancer channels
- Corrected address allocation of an XAUTH client authenticated by RADIUS
- If the TACACS+ server requests a new password via SSH, the account will not be blocked if a password is entered which does not match the security guidelines
- Reverse DNS requests for multicast addresses are no longer answered with the LANCOM's IP address
- Modified range of values for the english WEBconfig version
- Accelerated screen display of the firewall filter list
- Packets of an active TCP connection are discarded if the necessary carrier connection is not established
- Before warmstart the public spot module sends an "accounting end" to all RADIUS servers, so that running sessions can be closed
- Improvements in locking internal VPN structures
- PPTP can be used on devices without VPN
- An administrator having read permission may use "show" commands
- KeepAlive of a VPN connection is only evaluated if KeepAlive is configured for the physical connection
- The UMTS module of the LANCOM 1751 UMTS has to be registered as USB device. If necessary the UMTS module will be reset

LCOS changes 7.80.0075 RC3 ► 7.80.0081 Release

Bugfixes / Changes

Network Connectivity:

- If the sleep command is executed from within a script, former configuration changes are applied to the current configuration
- Dynamic configuration tables can be completely filled via SNMP
- WLAN data packets without payload do not lead to error message „Too many beacon transmit failures"
- Fax option can be used with LANCOM 1724 Annex A
- Simplified VPN dial-in with certificates can be used again

LANCOM Systems

LCOS changes 7.80.0067 RC2 ► 7.80.0075 RC3

Bugfixes / Changes

VoIP:

- A SIP trunk is available even if it is polled using OPTION packets
- Configurable DSCP flags for SIP-/RTP packets
- If overlap dialing for an analog line is terminated with „#“, this character will no longer be transmitted as part of the calling number

Network Connectivity:

- A global disconnect can be used even if the connections were established via LAN interface
- If the configured amount of half-open connections is exceeded, there is no more packet loss with other connections
- If an ICMP error message is received for a forwarded port no additional entry in the masquerading table is generated, thus decreasing CPU load significantly
- Access with configurable “immediate” validity in the Public Spot Wizard
- VPN connections using AH do not decrease the throughput of all VPN tunnels
- If a connection can not be established in a backup chain, a further connection on the failed channel is no longer regarded as backup connection
- If protocol- and port-objects are declared mixed-up in a firewall rule, the firewall rule is created correctly
- If XAUTH is disabled for the Advanced VPN client, a connection can only be established if XAUTH is disabled for this connection on the LANCOM device, too

LANCOM Systems

LCOS changes 7.80.0058 RC1 ► 7.80.0067 RC2

Bugfixes / Changes

VoIP:

- When stripping the line prefix on incoming calls there is a check if the prefix is part of the destination number
- If the rport flag is set in the VIA header, the LANCOM sends its packets to the IP address and port number on which the packet was received

Network Connectivity:

- The firewall condition for physically sent/received packets refers to the trigger only if it is not equal to zero
- Port forwardings to the LANCOM's internet address are possible to (for example) use the print server via masked connections, too
- Undefined station objects used in a firewall are no longer merged to ‚ANYHOST'
- A DSL backup may be used through further DSL connections
- If NAT traversal was negotiated on a VPN connection, a phase one re-keying on port 4500 will not be decliend
- Fixed an LCOS watchdog which occured when using 4 ISDN B channels
- Bugfixes in PPP negotiation, if channel bundling is rejected by remote station

Miscellaneous:

- If HTTP(S) is used with console commands loadscript, loadfirmware and loadconfig, the specified sender address will be used
- The specified ping time interval is used correctly with higher times (> 65 sec.)
- WEBconfig's VPN configuration is again offered for VPN devices containing a VPN 25 license
- If a trace filter string contains syntax elements like ‚+' oder ‚-', these will be recognized as part of the string
- The LANCOM 1721+ VPN's DSL interface can be configured via WEBconfig

LANCOM Systems

LCOS changes 7.72.0066 RU3 ► 7.80.0058 RC1

New Features:

WLAN:

- Support for multiple profiles in WLAN client mode
- IAPP switching available per ARF network
- On authentication, a LANCOM in client mode utilizes an accesspoint reject
- When roaming, a LANCOM WLAN client transmits separate update packets for any VLAN

Network Connectivity:

- Extended number of 16 ARF networks for the 17xx and 18xx devices
- 32 alternatively configurable PPTP remote stations
- The DHCP server can retain negotiations with other DHCP servers in the network
- Packets from internal services can be sent via router module
- Support for 9 parallel multilevel certificate hierarchies
- A partly checking of the certificate subject is possible
- XAUTH is useable in common with an external RADIUS server
- Configurable CPU load display
- Extended amount of comment fields (8 fields)
- CR/FL conversion can be disabled in the COM port server when using the RFC2217 extension
- Disengageable ethernet ports for central site devices, e.g. LANCOM 9100 and WLC
- Local routes with no link on the associated LAN interface are no longer propagated via RIP
- Loopback addresses are analyzed prior to NAT
- No RIP entry is created if N:N-entry netmasks and network settings do not match
- Local ARF networks and RAS users, who have been assigned an address from the given address pool are recorded in the current routing table, too
- Routing tags are evaluated for local routes, too
- Increased DOS detection default value for central site devices
- Configurable DiffServ masquerading for SIP- and RTP packets

Bugfixes / Changes:

WLAN:

- With dynamic VLAN assignment, communication is furthermore possible between access point and WLAN client
- RADIUS accounting can be used via managed Accesspoints

VoIP:

- In WEBconfig, a „#“ character is possible as MSN for ISDN users
- DTMF signalizing works as configured
- Call forwarding can be used with Mobilkom Austria
- Unitymedia SIP lines can be registered

Network Connectivity:

- Tables containing many columns are configurable error-free using scripting
- No more VPN connection errors when certificates are renewed via SCEP
- Incoming packets via tagged WAN routes which get different routing tags within the firewall are no longer filtered by IDS
- Firewall: a rule can be used which is limited to a tagged default route
- The MAC address from the DHCP table (/Status/LAN-Bridge/DHCP-Table) can be read via SNMNP
- Improvements in VRRP stability

- Windows computers can get the system time via virtual VRRP-IP address
- DNS requests are answered on a tagged local default route, too
- The correct number of tunnels is communicated in the SNMP traps
- Portforwarding is possible for masked connections with protocols HTTP(S), Telnet and SSH
- No errors when loading scripts due to wrong object sequence
- VPN connections with extranet addresses are masked always, even if masquerading is disabled in the routing table
- The LANCOM device is accessible directly after activating the VLAN module
- TCP connection breaks do lead to syslog messages
- 6 characters available for up- and downstream rates in the configuration
- A RIP update while disconnecting with instant reconnection start propagates RIP metrics 16
- Improvements in RIP Poisoned Reverse
- Fixed LCOS watchdog in USB reinit
- Fixed LCOS watchdog when disconnecting TCP links
- Corrected ADSL bitswapping. This fxes amongst others ADSL sync problems in Irland
- An LS/DIR command with fully specified path (incl. menuepoint) can be inhibited selectively via TACACS+

4. Comments

If you want to upgrade the firmware of your device to a new version, please install the latest LCMS version first. **Before running the firmware-upload you should save the router configuration to a file**. After that you can use LANconfig to load the latest LCOS-version into the device.

In principle, we suggest upgrading the firmware of your device only if you are in need of the latest features.

Please note that different firmware files might be available for your device. Further information can be found in the file README.PDF in the download area of our homepage.