LANCOM Release Notes

LCOS

10.32 RU2

LANCOM Systems GmbH
Adenauerstraße 20 / B2
52146 Würselen
Germany

Internet: http://www.lancom-systems.de

15.10.2019, CBuersch

Inhaltsübersicht

LANCOM Systems

1. Einleitung

LCOS („LANCOM Operating System“) ist das bewährte LANCOM Betriebssystem für Router, Access Points und WLAN-Controller. Im Rahmen der von den Produkten vorgegebenen Hardware ist die jeweils aktuelle LCOS-Version für LANCOM Produkte verfügbar und wird von LANCOM Systems kostenlos zum Download angeboten.

Dieses Dokument beschreibt die Neuerungen der LCOS Software Release 10.32 RU2 sowie die Änderungen und Verbesserungen zur Vorversion.

Beachten Sie vor der Durchführung des Firmware-Update unbedingt die Hinweise im Kapitel 6 „Allgemeine Hinweise“ dieses Dokumentes.

Aktuelle Support-Hinweise und sowie Informationen über bekannte Einschränkungen zur aktuellen LCOS-Version finden Sie im Support-Bereich unserer Webseite
https://www.lancom-systems.de/service-support/soforthilfe/aktuelle-support-hinweise/

2. Gerätespezifische Kompatibilität zu LCOS 10.32 / 10.30

Grundsätzlich werden alle LANCOM Produkte über die gesamte Lebenszeit regelmäßig mit Major Releases bedient, welche neue Features und Bugfixes beinhalten.
Auch für Geräte, die keine aktuelle LCOS-Version unterstützen, werden in regelmäßigen Abständen LCOS Release Updates inklusive Bugfixes und allgemeinen Verbesserungen bereitgestellt. Eine Übersicht über die aktuell unterstütze LCOS-Version für Ihr Gerät finden Sie unter
https://www.lancom-systems.de/produkte/firmware/lifecycle-management/produkttabellen/

Mit LCOS 10.30 entfällt die Unterstützung für folgende Geräte

- LANCOM 831A
- LANCOM IAP-322
- LANCOM L-451agn
- LANCOM L-452agn
- LANCOM L-460agn
- LANCOM OAP-3G

3. Hinweise zu LCOS 10.32

Informationen zu Werkseinstellungen

Geräte, die mit LCOS 10.00 oder größer ausgeliefert werden, kontaktieren automatisch die LANCOM Management Cloud (LMC). Diese Funktionalität ermöglicht eine Zero-Touch-Inbetriebnahme von neuen Geräten. Falls die LMC nicht verwendet werden soll, kann diese Funktionalität über den Grundeinstellungs-Wizard bei der Erstinstallation oder im LANconfig jederzeit unter Management > LMC deaktiviert werden. Eine spätere Verwendung der LMC ist jederzeit wieder manuell aktivierbar.

4. Feature-Übersicht LCOS 10.30

4.1 Feature-Highlights

SD-WAN – Application Routing

Profitieren Sie von einem deutlichen Performance-Gewinn bei der Nutzung moderner Cloud-Anwendungen (z.B. Office 365, SalesForce, etc.). SD-WAN Application Routing kann Cloud-basierte Anwendungen erkennen und leitet diese direkt ins Internet (Local Break-out). Dies entlastet die VPN-Strecke zur Zentrale als auch die Internetleitung in der Zentrale.

SD-WAN – Layer-7-Applikationskontrolle in der Firewall

Bewahren Sie die Kontrolle über die Nutzung der Anwendungen in Ihrem Netzwerk. Durch die Definition anwendungsbezogener Regeln in der Firewall liegt es in Ihrer Entscheidung, welche Internet-Anwendungen erlaubt, gesperrt, limitiert oder priorisiert werden.

WLC-Funktionen im vRouter (vWLC)

Entscheiden Sie selbst und flexibel, welche Rolle Ihr LANCOM vRouter übernehmen soll: VPN-Gateway oder WLAN-Controller. Der LANCOM vRouter unterstützt ab sofort die Rolle eines virtuellen WLCs (vWLC). Damit können die WLAN-Controller-Funktionalitäten vollständig auf einer Virtualisierungsplattform wie VMWare ESXi oder Microsoft Hyper-V virtualisiert werden. Die Anzahl verwalteter Access Points ist abhängig von der Lizenzkategorie des vRouters.

4.2 Weitere Features

TLS 1.3

Die Unterstützung des neuen Protokolls TLS 1.3 erhöht die Sicherheit beim Gerätezugriff über WEBconfig.

IKEv2 Elliptic Curve Digital Signature Algorithm (ECDSA)

IKEv2 unterstützt ab sofort die Authentifizierungsmethode Elliptic Curve Digital Signature Algorithm (ECDSA). Dies ermöglich deutlich kleinere Schlüssellängen und somit höhere Verschlüsselungs-Effizienz bei gleichem Sicherheitsniveau.

IKEv2 Split-DNS

Split-DNS ermöglicht die DNS-Auflösung bestimmter interner Domänen über einen VPN-Tunnel, während für alle anderen DNS-Anfragen ein öffentlicher DNS-Server verwendet wird.

IKEv2 Fragmentierung

Ermöglicht die effiziente Fragmentierung von IKEv2-Nachrichten (nach RFC 7383) vom VPN-Router selbst, so dass IKE-Pakete vom Transportnetz nicht mehr fragmentiert werden müssen.

Erweiterung bei Client-Reservierungen im DHCPv6-Server

Im DHCPv6-Server können ab sofort Client-Adressen bzw. Präfixe wahlweise anhand von DUID, MAC-Adresse, Interface-ID (nach RFC 3315) oder Remote-ID (nach RFC 4649) zugewiesen werden.

Doppelte Anzahl an Public Spot-Usern

Für die LANCOM 178x- und 179x-Serie mit Public Spot Option erhöht sich die Anzahl der User von 64 auf 128.

Weitere Features finden Sie in den Abschnitten zu den einzelnen Builds im Kapitel 5 „Historie LCOS 10.32 / 10.30“.

5. Historie LCOS 10.32 / 10.30

LCOS-Änderungen 10.32.0092 RU2

Neue Features

- Die IPv4-Firewall unterstützt jetzt eine automatische Weiterleitung / NAT eines GRE-Tunnels zwischen lokalem Netzwerk und einer WAN-Verbindung.

Korrekturen / Anpassungen

Allgemein

- Wenn in der Firewall des LANCOM Routers eine „Deny all"-Regel konfiguriert, und für die Kommunikation zwischen dem VPN-Client und dem lokalen Netzwerk eine „Allow"-Regel in der Firewall angelegt war, in welcher als Quelle der Name der VPN-Gegenstelle hinterlegt wurde, konnte über den VPN-Tunnel keine Kommunikation stattfinden.
- Der Konfigurationsbaum „/Setup/SIP-ALG" fehlte bei den Geräten ISG-1000 und ISG-4000.
- In einem Szenario mit BGP, in dem eine Route von einem LANCOM Router gelernt und an einen weiteren Router weitergegeben werden sollte, wurde die AS-Nummer des ursprünglichen Routers nicht durch die eigene AS-Nummer ersetzt. Stattdessen waren im AS_PATH beide AS-Nummern enthalten.
- Bei der Verwendung der Routen-Redistribution in OSPF werden jetzt die folgenden Routenquellen von verbundenen Netzwerken nicht mehr propagiert: Local LAN, Local WAN, DCHP, /32 Connected LAN, /32 Connected WAN.
- In einem OSPF-Szenario mit aktiver Routen-Redistribution konnte es vorkommen, dass die LSAs aus der Datenbank herausalterten und nicht erneuert wurden, wenn einem LANCOM Router seine eigenen LSAs zugewiesen wurden (dies kann etwa nach einem Neustart vorkommen).
  Dies führte dazu, dass nach einiger Betriebszeit alle per OSPF gelernten Routen nicht mehr vorhanden waren und somit keine Kommunikation mehr möglich war.
- Fragte die interne SMS-Verwaltung den Netzwerkzustand genau in dem Moment ab, in dem das Mobilfunk-Modul deaktiviert wurde, führte dies zu einem unvermittelten Neustart.
- Bei Empfang eines DHCP Server Identifiers (DHCP-Option 54) muss ein DHCP-Client ein RENEW und ein REBIND an den DHCP Server Identifier senden statt an den Server, von dem das ACK empfangen wurde. Der LANCOM Router sendete bei der Erneuerung der IP-Adresse das RENEW an den Server, von dem das ACK empfangen wurde, weshalb keine IP-Adresse bezogen werden konnte.
  Dies führte zu Verbindungsabbrüchen der Internet-Verbindung, wenn der DHCP-Lease ausgelaufen war.
- In einem Szenario mit einer /31 Subnetzmaske (RFC 3021), bei dem die IP-Adresse des Routers gleichzeitig auch die Broadcast-Adresse darstellte, funktionierten diverse Dienste nicht (u.A. ARP und DNS).
- Bei der Bearbeitung des Feldes „Backupliste" im WEBconfig-Menü „Kommunikation/Ruf-Verwaltung/Backup-Tabelle" wurde beim Eintrag mehrerer Gegenstellen als Trennzeichen ein Komma verwendet. Dieses Zeichen war jedoch für die Backupliste im LCOS nicht zulässig. In der Folge wurde der Eintrag nicht in die Konfiguration übernommen.

- Erfolgte über die LANCOM Management Cloud ein Zugriff auf einen LANCOM Router oder Access Point über die Funktion „Secure Terminal Access“, wurde im Event-Log des Gerätes als Zugriffs-Typ „Outband“ ausgegeben statt „LMC“.
- Wurden zwei OSPF-Instanzen mit dem gleichen Routing-Tag angelegt, konnte es zu einem unerwarteten Neustart kommen.
  In einem OSPF-Trace wird jetzt eine Fehlermeldung ausgegeben, dass es je Routing-Tag nur eine OSPF-Instanz geben darf.

VPN

- VPN-Zertifikate wurden bei deaktiviertem VPN-Modul nicht initialisiert.
  Dies führte dazu, dass die VPN-Verbindung nach Aktivieren des VPN-Moduls nicht aufgebaut werden konnte.

WLAN

- Wurde auf einem WLAN-Router oder Access Point mit dem Setup-Assistenten eine WLAN-Punkt-zu-Punkt-Verbindung im exklusiven Modus erstellt und anschließend der Setup-Assistent zur Einrichtung des Public Spot gestartet und ein WLAN erstellt, führte dies zu einem unvermittelten Neustart des Gerätes.
- Sendete ein WLAN-Endgerät fehlerhafte Parameter im DSSS Set, konnte sich dieses nicht mit einer versteckten SSID eines LANCOM WLAN-Routers oder Access Points verbinden. Diese Parameter werden jetzt ignoriert.
- Wurde in einem WLAN-Punkt-zu-Punkt-Szenario mit Geräten mit 802.11ac WLAN-Modulen das WLAN-Modul des Masters deaktiviert (etwa durch einen Neustart), kam die Punkt-zu-Punkt-Verbindung nicht mehr zustande, bis das WLAN-Modul des Slaves neugestartet wurde.
- Es konnte keine WLAN-Punkt-zu-Punkt-Verbindung per Auto-WDS aufgebaut werden.

VoIP

- Eine verzögerte Anrufweiterschaltung funktionierte nicht, da der Weiterleitungs-Timer zu früh angehalten wurde.
- Empfing der LANCOM Router nach einem INVITE auf einen nicht mehr existierenden Anruf die Meldung „200 OK“, antwortete der Voice Call Manager mit der Meldung „481 Call/Transaction Does Not Exist“.
  Der Voice Call Manager antwortet jetzt mit einem ACK und sendet anschließend ein BYE.
- Es konnte zu einem unvermittelten Neustart des Router kommen, wenn ein SIP-Client einen angenommen, über den SIP-Provider eingegangenen Ruf an einen weiteren externen Teilnehmer vermittelte.

LCOS-Änderungen 10.32.0023 RU1

Korrekturen / Anpassungen

VoIP

- Es wurde ein VoIP-Problem behoben, bei dem in bestimmten Konstellationen mit analogen Telefonen einseitige Sprachverbindungen oder keine Verbindung zustande kommen konnte. Für folgende Geräte wird das Update bereitgestellt:
  LANCOM 1783VA, 1783VAW, 1783VA-4G
  LANCOM 1793VA, 1793VAW, 1793VA-4G
  LANCOM 1906VA, 1906VA-4G
  LANCOM 883 VoIP

LCOS-Änderungen 10.32.0021 Rel

Neue Features

Allgemein

- Unterstützung für die SSH-Hostkey-Verfahren rsa-sha2-256 und rsa-sha2-512 (RFC 8332).
- Für SNMPv3-Passwörter kann eine vordefinierte Passwort-Richtlinie nun optional mittels eines Schalters erzwungen werden.

VPN

- Für IKEv2-Pre-Shared-Keys kann eine vordefinierte Passwort-Richtlinie nun optional mittels eines Schalters in der allgemeinen IKEv2-Konfiguration erzwungen werden.

Wireless ePaper

- Unterstützung des ThinAP 2.0-Protokolls zur Anbindung von Wireless ePaper-Access Points an einen zentralen Wireless ePaper-Server
- Unterstützung des LANCOM Wireless ePaper USB

Korrekturen / Anpassungen

Allgemein

- In der Konfiguration der Geräte LANCOM 1790-4G, 1790VA-4G und 1793VA-4G war ein Print-Server enthalten, obwohl diese Geräte keine USB-Schnittstelle zum Anschluss eines Druckers besitzen.
- Bei der Paketprüfung im DNS-Server kam es zu Fehlermeldungen und nicht funktionierenden DNS-Anfragen, wenn die Paketlänge der DNS-Anfrage durch eine andere Netzwerkkomponente verändert wurde.

- Wenn Gegenstellen in einem iBGP-Umfeld anhand gelernter Routen auf- bzw. abgebaut werden sollten, funktionierte dies nur beim ersten Mal. Bei allen weiteren Vorgängen wurde kein Abbau der Gegenstelle mehr durchgeführt.
- Waren bei einer als Backup verwendeten Mobilfunk-Verbindung die Namen von Mobilfunkprofil, Kommunikationslayer und Gegenstelle nicht identisch, konnte die Mobilfunk-Gegenstelle im Backup-Fall nicht aufgebaut werden.

VPN

- Bei IKEv2-Verbindungen enthielten UDP-Pakete für ein NAT-Keepalive einen nicht benötigten „Non ESP-Marker". In der Folge wurden diese Pakete von VPN-Produkten anderer Hersteller verworfen, was jedoch keinen negativen Einfluss auf die Qualität der VPN-Verbindung hatte.
- Wenn zwei zertifikatsbasierte VPN-Verbindungen existierten und beide Zertifikate den gleichen „Common Name (CN)" besaßen, konnte von diesen beiden Verbindungen nur die Verbindung aufgebaut werden, welche zuerst angelegt wurde.
- Bei VPN-Verbindungen mit IPSec-Encapsulation konnte es dazu kommen, dass der Router einen unvermittelten Neustart durchführte.

WLAN

- Nach der Aktivierung der LANCOM WLC Basic Demo-Option auf einem kompatiblen Gerät wurde die Zertifizierungsstelle (CA) nach dem obligatorischen Neustart des Gerätes als nicht auswählbar angezeigt und konnte in der Konfiguation nicht aktiviert werden.
- Bei der Vergabe von IP-Parameter-Profilen über den vWLC wurden die IP-Adressen aus den Profilen in umgekehrter Reihenfolge an die Access Points übermittelt. In der Folge war kein Zugriff auf die Access Points möglich.
- Bei der Konfiguration von statischen WLAN Controllern im Menü „Wireless LAN / WLC / WLAN Controller" konnte es vorkommen, dass trotz der Angabe einer Absende-Adresse ein anderes lokal konfiguriertes IP-Netzwerk verwendet wurde. Somit konnte bei der Kommunikation über einen VPN-Tunnel aufgrund fehlender Netzbeziehungen (SAs) keine Verbindung zum WLAN Controller aufgebaut werden.
- Wenn eine Public Spot-Anmeldung per HTTPS (TLS 1.3) durchgeführt wurde, erhielt der Benutzer anstatt einer Login-Seite eine Information des Browsers mit einer nicht irnorierbaren Sicherheitswarnung. In der Folge konnte sich ein Benutzer nicht am Public Spot anmelden.

VoIP

- Es konnte vorkommen, dass ein eingehender Anruf nach 30 Minuten beendet wurde, wenn die anrufende Gegenseite keine Session Timer verwendete. Dies führte dazu, dass der Timer auf dem LANCOM Router auslief und die Verbindung terminiert wurde, ohne dass die Gegenseite dies bemerkte.
- Bei einem ausgehenden Anruf, bei welchem im „To"-Feld des Parameters „Call is Being Forwarded" ein Tag angegeben war, antwortete der LANCOM Router mit einem PRACK ohne Tag im „To"-Feld. In der Folge wurde der Rufaufbau abgebrochen. Dies konnte dazu führen, dass bestimmte Rufnummern nicht erreicht werden konnten.

LCOS-Änderungen 10.30.0167 RU1

Neue Features

Allgemein

- Unterstützung für SD-WAN Application Routing in der LMC
- Für den Alive-Test ist nun eine Loopback-Adresse / Absende-Adresse konfigurierbar.
- Die Größe der Tabelle „Status / Config / Event-Log“ wurde auf 256 Zeilen erweitert.
- LISP: Das Akzeptieren von Paketen von unbekannten ITRs ist jetzt konfigurierbar.

WLAN

- Hinzufügen einer Konfigurationsmöglichkeit zur Reduzierung der Empfindlichkeit für empfangene WLAN-Pakete.
- In der Public Spot-Benutzerverwaltung sind nun die Passwörter für bereits angelegte Nutzer editierbar.
- Ist eine Kanalbevorzugung im 5 GHz-Band konfiguriert, kehrt der Access Point nach einer Radar-Erkennung und Ablauf der damit verbundenen Sperrzeit wieder auf den bevorzugten Kanal zurück.
- Unterstützung von IEEE 802.11r (Fast Roaming) im WLAN-Client-Modus.

VoIP

- Erweiterung des Telekom All-IP-Assistenten um die Angabe des Rufnummernblocks.
- Für SIP-zu-SIP-Rufe kann die Transkodierung nach T.38 abgeschaltet werden.

Korrekturen / Anpassungen

Allgemein

- Bei einigen Geräten der 1781x-Serie war es nicht möglich, die Zertifizierungsstelle (CA) im WEBconfig zu aktivieren, obwohl das Gerät über die dafür benötigte Voraussetzung (aktivierte VPN25-Option) verfügte.
- Bei LANCOM Geräten der 179x- und der R88x-Serie, welche über mehrere Internetverbindungen verfügten (1x VDSL-Modem, 2x WAN über ETH-Schnittstelle), startete das integrierte VDSL-Modem nicht. In der Folge konnte die WAN-Verbindung über das integrierte Modem nicht aufgebaut werden.
- Ein LANCOM vRouter mit abgelaufener Lizenz konnte im LANmonitor nicht mehr überwacht werden, da die initiale SNMP-Abfrage des LANmonitors vom vRouter nicht verarbeitet wurde.
- Aufgrund eines falschen Formats des SOAP-Headers im LANCOM Router wurde die TR-069-Aushandlung vom Auto Configuration Server (ACS) abgelehnt. In der Folge war eine automatische Konfiguration sowie ein Firmware-Update durch den ACS nicht möglich.
- Beim Verwenden eines Loadbalancers als Default-Route konnte es zu Problemen beim Verbindungsaufbau zur LANCOM Management Cloud (LMC) kommen.
- Bei Verwendung von IPv6-Only LTE-Verbindungen, d.h. PDP-Kontext IPv6, erhielt der LANCOM Router keine IPv6-Adresse, da der Router den DHCPv4-Client gestartet hatte. In der Folge kam die LTE-Verbindung nicht zustande.

- Wenn ein Dienst (z.B. E-Mail) von einem lokalen Client über das Port-Forwarding aufgerufen wurde (Hairpin-NAT), konnte es zu Paketverlusten auf der Internetverbindung kommen. In der Folge war die Internetverbindung für alle neu aufgebauten Sessions gestört.
- Bei den LANCOM Routern der 179x-Serie und beim LANCOM R883+ konnte es zu Einbrüchen und/oder Schwankungen der Downstream-Datenraten kommen, wenn das integrierte Modem an einem Supervectoring-Anschluss betrieben wurde und mit ADSL2+ synchronisiert war.
- Wurde eine Konfiguration über die LANCOM Management Cloud (LMC) auf ein Gerät ausgerollt, während ein gleichzeitiger TFTP-Zugriff auf das Gerät erfolgte, führte dies zu einem unvermittelten Neustart des Gerätes.
- In einem Backup-Szenario, welches zwei konfigurierte Mobilfunkverbindungen besaß, konnte ein LANCOM 1906VA-4G kein Backup auf die Mobilfunkverbindung herstellen, in welcher der SIM-Karten Slot 2 genutzt wurde, wenn für die SIM-Karte in Slot 1 eine inkorrekte PIN hinterlegt war. Das System blieb im Status „PIN invalid“ stehen.
- In einem Szenario mit eingesetztem PMS-Server sprachen die LANCOM Geräte ISG-1000, ISG-4000 und WLC-1000 anstatt der IP-Adresse des PMS-Servers die Adresse 0.0.0.0 an, da die Loopback-Adresse für das Netzwerk nicht korrekt erkannt wurde. In der Folge war die Kommunikation mit dem PMS-Server nicht möglich.
- L2TPv3 unterstützte in Verbindung mit VLAN kein MSS Clamping und Path MTU Discovery. Dies führte zu einem Performance-Verlust, da Pakete mehrfach übertragen werden mussten. Teilweise konnten Daten auch gar nicht übertragen werden.
- Bei einem LANCOM Router, welcher durch die LANCOM Management Cloud (LMC) verwaltet wurde, konnte es vorkommen, dass dieser nach einem Neustart oder nach dem Ausrollen einer Konfiguration als „Offline“ angezeigt wurde, obwohl das Gerät funktionsfähig und erreichbar war.
- Der Router in einer LISP-Konfiguration antwortete nicht auf Ping-Anfragen von unbekannten ITRs.
- Wenn der RADIUS-Server des LANCOM als Weiterleitungsziel von einem Windows NPS (Network Policy Server) angegeben wurde, konnte es vorkommen, dass keine Authentifizierung möglich war. Hier wurde ein Proxy-State-Attribut hinzugefügt, welches der NPS erwartet, damit die Kommunikation funktioniert.
- Bei der Kommunikation eines LANCOM Routers mit einem Serversystem, welches switchunabhängiges NIC Teaming verwendet, konnte es zu Problemen kommen. Hierbei war sowohl der Zugriff auf die Konfiguration des LANCOM Routers als auch die Erreichbarkeit des Servers bei einem Port Forwarding aus dem Internet gestört.
  Damit die Kommunikation zwischen dem Server und dem LANCOM Router bei switchunabhängigem NIC Teaming funktioniert, muss zudem unter „IP-Router / Pakete von internen Diensten über den Router senden“ aktiviert werden.
- Ein eingerichtetes Loopback-Interface für den LISP-ETR wurde nicht ausgerollt.

VPN

- Bei einem EoGRE-Tunnel, welcher durch einen IPSec-Tunnel aufgebaut wurde, sorgte ein Abbruch des IPSec-Tunnels dafür, dass der EoGRE-Tunnel nicht mehr funktionsfähig war.
- Wenn ein VPN-Client über das IKEv1-Protokoll mit dem LANCOM Router verbunden war und dieser per Config-Mode eine IP-Adresse vom Router erhielt, wurde die Adresse nicht in die RIB/FIB-Tabelle des Routers übernommen. Wenn zudem unter ‚IP-Router / Allgemein' die Option „Pakete von internen Diensten über den Router senden" aktiviert waren, führte dies dazu, dass keine Kommunikation vom LANCOM Router in Richtung des Clients möglich war. Die Kommunikation vom VPN-Client in das lokale Netzwerk war jedoch nicht betroffen.
- Wurde einem WAN-Interface ein IPv6-Kontext zugewiesen, obwohl die Internet-Verbindung kein IPv6 unterstützte, dauerte der VPN-Verbindungsaufbau sehr lange, da jeder Verbindungsaufbau mit einer IPv6-Adresse erst nach 30 Sekunden abgebrochen wurde. Weiterhin versuchte der Router die VPN-Verbindung über eine Link Local Adresse aufzubauen.
- L2TP unterstützt Endpunkt-Bezeichner mit maximal 16 Zeichen. Wird ein längerer Bezeichner verwendet, wird dieser intern ungekürzt verwendet, nach außen aber auf 16 Zeichen gekürzt (etwa in einer Status-Tabelle). Da beim Kürzen ein Byte zuviel kopiert wurde, konnten die Informationen einer L2TPv3-Verbindung nicht in den Status-Tabellen aktualisiert werden.
- Unicast-Pakete wurden bei Verwendung eines L2TPv3-Tunnels verworfen, wenn keine zugehörige Session mehr existierte, die Adresse aber noch in der ARP-Tabelle enthalten war. Dies führte dazu, dass Geräte im Netzwerk, welche selten Broad- und Multicast-Pakete senden, über den L2TPv3-Tunnel nicht mehr erreichbar waren.
  L2TPv3 sendet jetzt alle Unicast-Pakete in die Bridge, auch wenn keine zugehörige Session existiert.
- Bei VPN-Einwahlzugängen mit einem übergeordneten VPN-Benutzer (Authentifizierung per RADIUS-Server oder Zertifikatseinwahl) werden die Gegenstellen-Namen z.B. durch die Key-ID oder den RADIUS-Benutzer gebildet. Damit der Gegenstellen-Name eine Länge von 16 Zeichen nicht überschreitet, werden intern nur die ersten 12 Zeichen verwendet, gefolgt von einem Hash-Wert mit 4 Zeichen.
  Es konnte vorkommen, dass einer VPN-Gegenstelle der gleiche Hash-Wert zugewiesen wurde. Waren die ersten 12 Zeichen der Key-ID gleich, führte dies dazu, dass es mehrere Gegenstellen mit dem gleichen Namen gab. Dadurch kam es zu einem Auf- und Abbau der VPN-Tunnel, weil die VPN-SAs nicht eindeutig zugeordnet werden konnten.
- Nach einem Re-keying war keine Kommunikation über eine IKEv1-VPN-Verbindung möglich, wenn den Lifefetimes der Phase-1 und Phase-2 der gleiche Wert zugewiesen wurde.
- Bei IKEv2 VPN-Verbindungen mit HTTPS-Encapsulation konnte es aufgrund von Speicherverlusten zu einem unvermittelten Neustart des LANCOM Routers kommen.

WLAN

- Nach Bezug des WLAN-Profils samt Passwort wird bei erstmaligem Aufrufen des Access Points in WEBconfig der Ersteinrichtungs-Assistent geöffnet. Wurde dieser vom Benutzer abgebrochen, konnten im WEBconfig beliebige Konfigurationsänderungen am Access Point vorgenommen werden, ohne dass zuvor eine Passwort-Abfrage für den Zugriff auf die Konfiguration erfolgte.
- Der Idle-Timeout nicht mehr angemeldeter WLAN-Clients verblieb dauerhaft auf 900 Sekunden. In der Folge wurden die WLAN-Clients nicht aus der WLAN-Stations-Tabelle gelöscht, wenn die Anmeldung im WLAN vorher abgelehnt wurde.
- Verringerung der Fehlerkennungen von Radar-Ereignissen (DFS) für IEEE 802.11ac Wave1- und Wave2-WLAN Module

VoIP

- Wenn ein externer Anruf von einer ISDN-TK-Anlage angenommen und dieser Anruf an eine externe Rufnummer umgeleitet wurde, scheiterte die Rufumleitung. Der Voice-Call-Manager verarbeitete diesen sogenannten REDIRECT nicht korrekt, sodass nach der Bearbeitung die Leitungszuordnung nicht stimmte.
- Es konnte zu Gesprächsabbrüchen nach ca. 15 Minuten kommen, da der Voice-Call-Manager auf eine UPDATE-Anfrage des VoIP-Providers nach 15 Minuten mit der Meldung ‚200 OK' antwortete und in dieser Antwort keine ‚Require:timer' Header enthalten waren. In der Folge sendete der VoIP-Provider ein BYE und der Anruf wurde beendet.
- Bei Verwendung eines Telekom DeutschlandLAN IP Voice/Data-Anschlusses und aktiviertem VoSIP konnten keine eingehenden Faxe von einem analogen Faxgerät empfangen werden. Dies wurde dadurch verursacht, dass der LANCOM Router auf T.38 wechselte und dafür ein Re-INVITE sendete. Da die Verschlüsselungs-Einstellungen im Re-INVITE des Routers fehlerhaft waren, lehnte der VoIP-Provider das Re-INVITE mit der Meldung „403 Forbidden" ab.
- Eine Mehrfachverwendung von internen Rufnummern in verschiedenen Rufgruppen, die kaskadiert nacheinander gerufen werden sollen, war nicht möglich. Der interne Teilnehmer wurde nur beim ersten Mal signalisiert. Beim Auflösen der nächsten Gruppen, in welcher der interne Teilnehmer ein weiteres Mal eingetragen war, wurde dieser nicht beachtet.
- Wenn ein bestehendes Telefonat über den Voice Call Manager beendet wurde, während z.B. LANconfig eine Konfigurationsänderung in den LANCOM Router übertrug, konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.
- Erhält ein SIP-Teilnehmer ein INVITE mit einem zu kleinen Session Timer, quittiert dieser das INVITE mit der Meldung ‚422 Session Interval Too Small'. In einem Szenario mit einer Rufgruppe mit mehreren SIP-Teilnehmern wurde die Meldung ‚422 Session Interval Too Small' aber nicht an den Anrufer gesendet. Dadurch kam das Telefonat nicht zustande.
- Sendete ein LANCOM Router bei einem bestehenden Telefonat im RE-INVITE den Parameter Require: timer, konnte es vorkommen, dass die Gegenseite dies mit der Meldung ‚420 Bad Extension' mit dem Parameter Unsupported: timer ablehnte, obwohl im initialen INVITE der Gegenseite der Parameter Supported: timer enthalten war. Dadurch brachen Telefonate nach 10 Minuten ab.
  Der Parameter Require: timer wird jetzt in einem RE-INVITE nicht mehr übertragen, da dieser nicht erforderlich ist.

- Erhielt ein LANCOM Router bei einem ausgehenden Anruf im ‚183 Session Progress' vom Provider den Parameter Require: 100rel, schickte der Router im ‚183 Session Progress' an den internen SIP-Teilnehmer den Parameter Supported: 100rel.
  Dadurch hörte der Anrufer keinen Klingelton und bei Annahme des Anrufes durch den Angerufenen wurden keine Sprachdaten übertragen. Weiterhin wurde das Telefonat nach 10 Sekunden abgebaut.
- Ein Voice over LTE (VoLTE) Teilnehmer bietet in seinem INVITE mehrere Codecs an sowie Abtastraten von 8 und 16 Khz für DTMF. Bei einem eingehenden Telefonat eines VoLTE Teilnehmers antwortete der LANCOM Router im ‚200 OK' mit einem falschen DTMF Payload Type. Weiterhin unterstützte der Voice Call Manager lediglich eine DTMF Abtastrate von 8 Khz.
  Dadurch konnten keine DTMF-Informationen übertragen werden. Teils führte dies auch dazu, dass keine Sprach-Übertragung möglich war.

LCOS-Änderungen 10.30.0075 Rel

Korrekturen / Anpassungen

Allgemein

- Bezog ein Router oder Access Point seine IP-Adresse per DHCP, kam es beim Empfang von IP-Paketen außerhalb des lokalen Netzwerkes auf dem DHCP-Interface zu einem Fehler beim Auflösen der Routen. In der Folge lehnte die Firewall des Gerätes die IP-Pakete mit der Meldung „Intruder detection" ab.
- Das Abfrage-Intervall für den Bezug von Zertifikaten über den SCEP-Client in dem Pfad /Setup/Certificates/SCEP-Client/Check-Pending-Requests-Interval wurde ignoriert und stattdessen ein fester Wert von 60 Sekunden verwendet. Es wird jetzt wieder der hinterlegte Wert herangezogen.
- Wenn ein LANCOM Router die IP-Parameter für die Gegenstelle INTERNET-DEFAULT von einem DHCP-Server bezog und ein vorgeschaltetes Gateway die IP-Adresse xx.xx.xx.254 besaß, kam es zu einem IP-Adresskonflikt, da der LANCOM Router sich selbst ebenfalls die IP-Adresse xx.xx.xx.254 vergab. Dies führte dazu, dass keine Kommunikation zum Internet und somit auch nicht zur LMC möglich war.
- Das Ausrollen einer Konfiguration von der LANCOM Management Cloud (LMC) an einen Router, welcher über einen IPv6 Dual Stack-Lite-Anschluss mit dem Internet verbunden war, konnte zu einem unvermittelten Neustart des Routers führen.
- Wurde ein DS-Lite-Tunnel in einem Load-Balancer hinterlegt (IP-Router / Routing / Load-Balancing), konnte es zu einem unvermittelten Neustart des LANCOM Routers kommen.
  Der DS-Lite-Tunnel kann jetzt im Load-Balancer nicht mehr ausgewählt werden.
- Wurde IKEv2 in Verbindung mit IPv6 im LAN verwendet, konnte der IKE-Config-Mode-Server einem VPN-Client keine IPv6-Default-Route zuweisen.
- Bezog ein LANCOM Router seine IP-Parameter für ein mit einem Schnittstellen-Tag versehenes Netzwerk per DHCP, wurde die automatisch generierte Default-Route Netzwerken mit anderen Schnittstellen-Tags zugewiesen.
- Dies führte dazu, dass Pakete aus den betroffenen Netzwerken falsch geroutet wurden, anstatt die Pakete zu verwerfen.

- Nach Ausführen des Befehls default -r auf der Root-Ebene zwecks Zurücksetzen der Konfiguration auf die Standard-Werte wurde die Tabelle „Setup/Firewall/DNS-Destinations“ nicht zurückgesetzt.
- Beim LANCOM vRouter fehlte die Funktion zur Ermittlung und Festlegung von Daten- und Zeit-Budgets.
- Bei den LANCOM Geräten ISG-4000 und WLC-1000 war es nicht möglich, eine alternative Boot-Konfiguration zu erstellen.
- Bei Webseiten-URLs, welche in der Konfiguration des Content Filters als Whitelist-Einträge angelegt waren, dauerte der Aufbau der Webseiten-Inhalte ungewöhnlich lange.
- Die Checksummen-Berechnung von Ethernet-Paketen funktionierte im vRouter nicht korrekt. Dies konnte zu Kommunikationsproblemen führen.

VPN

- Nahm ein Router eine VPN-Verbindung an, bei welcher die Authentifizierung per RADIUS-Server erfolgte, blieben die VPN-Regeln der Verbindung auch nach Deaktivierung des VPN-Moduls und Abbau der Verbindung in der SADB aktiv. Es wurden weiterhin DPD-Pakete versendet.
- Split-DNS soll DNS-Informationen über den IKE-Config-Mode übertragen. Hierbei wurden Domänen, die im DNS-Server als Subdomain hinterlegt wurden, nicht übertragen, sondern nur die, welche als eigene Domäne für den Router konfiguriert waren. Zusätzlich führte eine leerer Eintrag bei der Geräte-eigenen Domäne zu einem Anzeigefehler in der entsprechenden Status-Tabelle des empfangenden Gerätes.
- Bei der Verwendung der Split-DNS-Funktion in einer IKEv2-VPN-Verbindung wurde beim Übermitteln des DNS-Wildcard-Wertes „*“ im Client-Router der Wildcard-Wert „*.“ eingetragen. Somit wurde der Wildcard-Eintrag in der Außenstelle nicht korrekt verwendet.
- Bei Verwendung von IKEv2-Verbindungen besteht die Möglichkeit, die Authentifizierung über einen externen RADIUS-Server durchzuführen. Dabei wurden RADIUS-Anfragen vom LANCOM Router nicht wieder freigegeben, sodass nach längerem Betrieb keine weiteren RADIUS-Anfragen zur Authentifizierung mehr gestellt werden konnten. In der Folge konnten keine VPN-Verbindungen mehr aufgebaut werden.
- War für eine IKEv2-Verbindung ein Eintrag in der Polling-Tabelle hinterlegt und der IKE-Config Mode „Client“ definiert, damit die Pakete hinter der zugewiesenen IP-Adresse maskiert werden, so funktionierte der VPN-Verbindungsaufbau nicht.
- Wenn eine VPN-Gegenstelle (IKEv1), welche über eine IPv6-WAN-Verbindung aufgebaut werden sollte, und eine ISDN-Gegenstelle die gleiche Namensbezeichnung hatten, konnte die VPN-Gegenstelle nicht korrekt aufgebaut werden.
- Bei der Verwendung von GCM-Verschlüsselungs-Algorithmen trennte eine fehlerhafte VPN-Verbindung, die über einen externen RADIUS-Server authentifiziert werden sollte, alle aufgebauten VPN-Verbindungen, welche erfolgreich über den RADIUS-Server authentifiziert wurden.
- Wenn in einem Einwahl-Profil des LANCOM Advanced VPN Client im Menü „Erweiterte IPsec-Optionen / UDP-Encapsulation“ der Port 4500 fest eingestellt wurde, scheiterte eine IKEv1-Client-Einwahl mit der Fehlermeldung „IKE info: Phase-2 proposal failed“.
- Wenn eine VPN-Verbindung (manuell) getrennt und dann neu verbunden wurde (Reconnect), funktionierte das OSPF-Protokoll über diese VPN-Verbindung nicht mehr.

WLAN

- Wenn auf einem LANCOM Gerät sowohl ein WLAN als auch die Public Spot-Funktion betrieben wurde, hatte dies zur Folge, dass Public Spot-Benutzer nach Erreichen des standardmäßig definierten WLAN-Idle-Timeout nicht nur aus der WLAN-Stations-Tabelle, sondern auch aus der Public Spot-Auto-Relogin-Tabelle gelöscht wurden. Ein erneutes Anmelden am Public Spot mit den gleichen Benutzerdaten war somit nicht mehr möglich.

VoIP

- Empfing ein LANCOM Router ein codiertes T.38-Paket ohne Audio-Inhalte, so konnte dies zu einem unvermittelten Neustart des Routers führen.
- Sendete eine SIP-TK-Anlage ein INVITE mit einem sehr kleinen Session Timer, wurde dieser vom LANCOM Router übernommen. Wurde dieser Wert vom Provider mit der Meldung „422 Session Interval Too Small“ quittiert (mit Angabe des minimalen Session Timers), ignorierte der Router dies, wenn der Provider während der „Early Media Phase“ ein UPDATE sendete. In der Folge baute der Router das Gespräch nach Ablauf des ursprünglichen Session Timers mit einem BYE ab.
- In einem Szenario mit einem Telekom SIP-Trunk bzw. Telekom All-IP-Anschluss und einer per SIP-Trunk angebundenen NFON Cloud-TK-Anlage wurde ein eingehender Anruf über den Telekom-Anschluss von NFON mit der Meldung „404 Not Found“ abgelehnt.
  Die Ursache dafür war, dass NFON bei Verwendung eines SIP-Trunks die User-ID im Feld P-Asserted-Identity anstatt in der P-Preferred-Identity erwartet.
- Bei der Verwendung von ISDN-Endgeräten, welche bei einem ausgehenden Anruf keine Quellrufnummer sendeten (z.B. eine Türsprechanlage) konnten ausgehende Gespräche nicht geführt werden, wenn ein ein VoIP-Provider verwendet wurde, welcher das leere oder mit dem Wert „anonym“ gefüllte „Calling Party“-Feld nicht akzeptierte (z.B. SIPGATE).
- Bei einem eingehenden Telefonat über eine SIP-PBX-Leitung wurden DTMF-Signale nicht an die Teilnehmer weitergeleitet.
- Wurde vom SIP-Provider aufgrund einer aktiven Rufweiterleitung die Meldung „181 Call Is Being Forwarded“ auf einen ausgehenden Anruf empfangen, fehlten in der vom Provider geforderten Bestätigung (mittels PRACK) Informationen im To-Header. Dadurch baute der Provider den Anruf mit der Meldung „481 Call/Transaction Does Not Exist“ ab.
- Es konnte zu Gesprächsabbrüchen nach ca. 15 Minuten kommen, da der Voice-Call-Manager auf eine UPDATE-Anfrage des VoIP-Providers nach 15 Minuten mit der Meldung “200 OK“ antwortete und in dieser Antwort SDP-Informationen enthalten waren, welche der VoIP-Provider nicht verarbeiten konnte.
  In der Folge sendete der VoIP-Provider eine BYE-Nachricht, was dazu führte, dass das Telefonat beendet wurde.
- Sendete ein SIP-Teilnehmer ein REGISTER-Paket ohne Angabe des Ports im Contact-Header, hängte der Voice Call Manager im darauf folgenden 200 OK im Contact-Header den Port 0 an. In der Folge konnte es zu fehlender Sprachübertragung bei eingehenden Anrufen kommen.
- Bei eingehenden Anrufen konnte es bei der Umwandlung eines DTMF-Signals zu einem Fehler kommen, in Folge dessen alle RTP-Pakete verworfen und eingehende Sprachdaten nicht übertragen wurden.

LCOS-Änderungen 10.30.0045 RC2

Neue Features

Allgemein

- Für das CLI-Kommando „ll2mdetect“ kann nun ein Ziel-Interface angegeben werden (Parameter „-i“).
- Das CLI-Kommando „show job“ gibt nun zusätzlich die gesamte CPU-Last aus.

Korrekturen / Anpassungen

Allgemein

- Nach einem Geräteneustart wurde die in der IPv4-Routingtabelle konfigurierte Distanz nicht mehr beachtet.

WLAN

- Bei Verwendung von WLAN-Routern oder Access Points, die ein 802.11n-WLAN-Modul verwenden, kam es zu Verbindungsabbrüchen mit Amazon Echo-Geräten.
- Der WLAN-Client-Modus unter Verwendung des WLAN-2-Funkmoduls bei den Access Points der LN-17xx-Serie funktionierte nicht.

VoIP

- Bei der Verarbeitung von eingehenden DTMF-Signalen konnte es zum Abbruch der Sprachübertragung kommen.

LCOS-Änderungen 10.30.0028 RC1

Neue Features

Allgemein

- Anpassung der Anzahl gleichzeitiger Public Spot-Benutzer auf Routern der 178x- und 179x-Serie auf 128.
- Die SSL/TLS-Version, die vom internen SMTP-Client verwendet wird, kann nun konfiguriert werden.
- Jitter-Anzeige im ICMP-SLA-Monitor
- „clear"-Kommando zum Leeren der aktuellen Konsolenausgabe
- Unterstützung von TLS 1.3 für WEBconfig
- Unterstützung des ThinAP 2.0-Protokolls zur Anbindung von Wireless ePaper Access Points an einen zentralen Wireless ePaper Server
- Unterstützung von IPv6 für TACACS+
- Unterstützung für RSA-PSS-Signierung in der SCEP-CA

Routing

- Application Routing und -Kontrolle in der IPv4- und IPv6-Firewall
- Auswertung von DSCP-Markierungen in der IPv6-Firewall
- IKEv2-IPv6-CFG-Mode-Adressen können an Clients basierend auf dem vom Provider zugewiesenen Präfix vergeben werden.
- Unterstützung von Adressreservierungen im DHCPv6-Server

VPN

- Unterstützung für IKEv2-Cookie-Notification
- Unterstützung für IKEv2-Split-DNS
- Unterstützung für IKEv2-Fragmentierung
- Unterstützung von ECDSA für die IKEv2-Authentisierung

WLAN

- Die E-Mail-Benachrichtigung für WLAN-Ereignisse kann nun über einen Schalter aktiviert und deaktiviert werden.
- Die Ratenadaption für 802.11n-WLAN-Module berücksichtigt nun bei der Ratenauswahl auch eine konfigurierte Sendeleistungsreduktion.
- Alternativ zur Sendeleistungsreduktion ist nun die Ziel-EIRP (Sendeleistung) im WLAN einstellbar.
- Unterstützung von 802.11k im WLAN-Client-Modus
- Unterstützung von 802.11v im WLAN-Client-Modus
- Unterstützung des Authentisierungsverfahrens SAE im WLAN-Client-Modus

6. Allgemeine Hinweise

Haftungsausschluss

Die LANCOM Systems GmbH übernimmt keine Gewähr und Haftung für nicht von der LANCOM Systems GmbH entwickelte, hergestellte oder unter dem Namen der LANCOM Systems GmbH vertriebene Software, insbesondere nicht für Shareware und sonstige Fremdsoftware.

Sichern der aktuellen Konfiguration

Bitte sichern Sie vor dem Update Ihrer LANCOM-Geräte auf eine neue LCOS-Version unbedingt Ihre Konfigurationsdateien!

Wegen umfangreicher Feature-Erweiterungen ist ohne eine Sicherung der Konfigurationsdaten eine Rückkehr auf die alte Firmware **nicht mehr automatisch möglich.**

Wenn Sie Geräte, die Sie über eine Router-Verbindung oder WLAN-Punkt-zu-Punkt-Verbindung erreichen können, aktualisieren möchten, bedenken Sie bitte, dass Sie zuerst das entfernte LANCOM Gerät und anschließend das lokale LANCOM Gerät aktualisieren. Eine Anleitung zur Firmware-Aktualisierung erhalten Sie im LCOS-Referenzhandbuch.

Wir empfehlen zudem, dass produktive Systeme vor dem Einsatz in der Kundenumgebung erst einem internen Test unterzogen werden, da trotz intensivster interner und externer Qualitätssicherungsmaßnahmen ggf. nicht alle Risiken durch LANCOM Systems ausgeschlossen werden können.

Verwendung einer Minimalfirmware zur Vergrößerung des Speicherplatzes

Durch zahlreiche neue Funktionen in der LCOS-Firmware ist es bei älteren LANCOM Geräten unter Umständen nicht mehr möglich, zwei vollwertige Firmware-Versionen gleichzeitig zu speichern. Um mehr Platz im Speicher zu schaffen, muss dann statt einer vollwertigen Firmware zunächst eine eingeschränkte, kleinere Firmware eingerichtet werden. Hierdurch steht für die andere Firmware im Gerät erheblich mehr Speicher zur Verfügung.

Diese Einrichtung ist nur einmalig erforderlich und wird mit einer „Minimalfirmware" durchgeführt.

Nach dem Einspielen der Minimalfirmware steht die Firmsafe-Funktion des LANCOM nur noch in eingeschränktem Umfang zur Verfügung. Das Update auf eine neuere Firmware ist weiterhin problemlos möglich.

Das LANCOM Gerät arbeitet nach einem fehlgeschlagenen Update jedoch mit einer Minimalfirmware, die Ihnen ausschließlich den lokalen Zugriff auf das Gerät erlaubt. Alle erweiterten Funktionalitäten, insbesondere die Remote Administration, sind nicht verfügbar, solange die Minimalfirmware aktiv ist.