

Releasenotes MC Firmware

Firmware 2.04b --> 2.04d (11. Mai 2015)

1. Linux Kernel 4.0.0-rc5+ --> 4.0.0+
2. Änderung in der Roaming Strategie. Das Roaming wurde bei der 2.04b von der Bridge-Applikation gesteuert. Mit der 2.04e wird das Roaming komplett dem WLAN-Treiber des Linux-Kernels überlassen.
3. auf der Home-Webseite werden in der Accesspointliste Parameter rot angezeigt, wenn sie eine Verbindung mit dem Client verhindern.

Firmware 2.04d --> 2.04r (28. Juli 2015)

1. DHCP-Server mit Löschfunktion für die Reservierungen.
2. MWLC Bridge-Mode hinzugefügt
3. (Wireless --> Roaming) Lower SNR Threshold Parameter entfernt.
4. (Wireless --> Roaming) Im AP Denisty Modus : "Auto detect" Mode wird das Roamingverhalten doch wieder etwas von der Application gesteuert. Der Schwerpunkt wurde hier wieder mehr auf die Signalstärke des AP's gelegt und nicht so sehr auf die potentiell mögliche Übertragungsgeschwindigkeit. Es wird von uns empfohlen, den AP Denisty Modus wenn möglich immer auf "Auto detect" zu stellen.

Firmware 2.04r --> 2.06d (09. September 2015)

1. neuer Linux-Kernel 4.1.5+
2. DHCP-Problem im "Level 2 Pseudo-Bridge" Mode behoben
3. DHCP-Server überarbeitet. Dadurch gibt es eine bessere Verarbeitung der Reservierungen.
4. neuer Parameter "Stay connected" im "LAN Client Cloning" - Mode
5. Verbesserte Verarbeitung von Zertifikatsdateien.
6. NTP RTC Config --> es kann jetzt ein Datum und eine Zeit definiert werden mit der der MC1 startet.
7. unter Admin kann jetzt der HTTPS - Port konfiguriert werden.

Firmware 2.06d --> 2.06f (04. Oktober 2015)

1. Mit der Firmware 2.06d darf man kein Downgrade auf Firmware-Versionen 2.04x durchführen. Das Gerät startet danach nicht mehr und muss zur Reparatur eingeschickt werden. Die 2.06f behebt diesen Fehler!
2. Einige überflüssige Parameter in der Config wurden entfernt.

Firmware 2.06f --> 2.06k (18. November 2015)

1. SCEP (Simple Certificate Enrollment Protocol) Funktion hinzugefügt („Wireless --> SCEP“)
2. „MWLC Master“ Mode korrigiert

Firmware 2.06k --> 2.06p (17. Dezember 2015)

1. Fehler bei der Firmware 2.06k im Bridge-Modus „Single Client NAT“ beseitigt. Dieser Fehler führte zu einem Neustart des Geräts. Dieser Zustand kann nur durch einen Default-Reset per Resettaster beseitigt werden.
2. Änderungen, damit die neuen MC Varianten MC2 + MC4 mit der gleichen Firmware wie der MC1 arbeiten können.
3. Zusatzfunktion zur WLAN-Status Mitteilung des MC-Adapters an einen LAN-Client durch UDP - Datagramm. Diese Funktion wird unter „Configuration“ -> „Wireless“ -> „Main Parameter“ gesetzt.

4. Zusatzfunktion bei der Definition der Portweiterleitungen (Bridge-Mode:NAT):
In der Regeldefinition können jetzt mit einer Regel mehrere Ports zur Weiterleitung für eine IP-Adresse angegeben werden.
5. Das MC-Config-Programm kann jetzt von der LAN-Seite per Unicast auf den MC-Adapter zugreifen. Dies beschleunigt den Firmware-Update von der LAN-Seite erheblich.

Firmware 2.06p --> 2.06q (07. Januar 2016)

1. Änderung im USB-Printerserver: bisher wurde der Hersteller und das Produkt abgefragt wenn ein Drucker verbunden wurde. Ohne diese Information wurde der PrinterServer nicht gestartet. Manche Drucker liefern diese Information aber anscheinend nicht. Die Firmware wurde so geändert, dass trotz fehlender Info der MC den Printerserver trotzdem startet.
2. Kleinere Änderungen auf der Webseite.

Firmware 2.06q --> 2.06s (04. Februar 2016)

1. Bug im Modul zum Betrieb der seriellen Schnittstelle: Bei bestimmten Zeichenfolgen konnte eine Verfälschung der seriell empfangenen Daten auftreten, wenn die Einstellung „no Parity“ aktiv war.
2. Änderung im Roaming-Modul: Bei der Bewertung der Wahl des besten AP's wird berücksichtigt ob von dem betreffenden AP auch innerhalb der letzten 10 Sekunden ein „Probe response“ empfangen wurde.

Firmware 2.06s --> 2.06u (19. Februar 2016)

1. Handshake-Behandlung im seriellen COMSERVER Modus korrigiert.
2. Fehler bei der Verarbeitung der NAT-Regeln korrigiert.

Firmware 2.06u --> 2.07b (22. März 2016)

1. Unter „Roaming“ wurde die Pingfunktion überarbeitet.
2. Fehler im Timer-Modul behoben. Dieser Fehler konnte unter Umständen zu einem Neustart des WLAN-Clients führen oder einen manuellen Reset erforderlich machen.
3. Serielle Schnittstelle: XON - XOFF Protokollbehandlung verbessert

Firmware 2.07b --> 2.07c (12. April 2016)

1. Der Zustand der LAN-Ports wird jetzt zum MConfig-Programm übermittelt und kann dort dargestellt werden
2. Fehler bei der Zustandsanzeige an den LAN-Stecker-LED's beseitigt.
3. optionaler Temperatursensor wurde in die Firmware aufgenommen.

Firmware 2.07c --> 2.07g (13. Mai 2016)

1. Statusmeldungen an das MConfig-Programm über den Zustand der seriellen Schnittstelle und des USB-Ports hinzugefügt
2. Es werden jetzt bis zu 16 DNS-Server-IP-Adressen vom DHCP-Client (WLAN - Seite) verarbeitet.
3. Es können jetzt 2 NTP-Server angegeben werden.
4. Für den DHCP-Server (LAN- Seite) kann die IP-Adressenvergabe über Regeln festgelegt werden. In diesen Regeln kann eine IP entweder über die MAC oder über den Gerätenamen zugeordnet werden.
5. Unter Roaming kann man jetzt in einer Liste Accesspoints BSSID's angeben, die entweder bevorzugt oder ausgeschlossen werden, wenn es darum geht, mit welchem AP eine Verbindung aufgebaut werden soll.
6. Es ist jetzt im Zusammenhang mit dem MConfig-Programm (Vers. 2.0.2.11) möglich, eine vorläufige Konfiguration an ein MC-Gerät zu schicken. Erst wenn die Konfiguration nach

dem Neustart über das MCCConfig-Programm innerhalb einer vorgegebenen Zeit bestätigt wird, wird diese Konfiguration als permanent gekennzeichnet. Damit kann verhindert werden, dass durch eine fehlerhafte Eingabe eines Parameters der Zugriff über WLAN auf ein MC-Gerät dauerhaft verloren geht.

Firmware 2.07g --> 2.07k (01. Juni 2016)

1. Im LAN-Client-Cloning Mode können jetzt DNS Server IP Adressen angegeben werden. Dies ist dann wichtig, wenn der LAN-Client eine statische IP-Adresse hat und der MC dadurch keine DNS Informationen erhält. In diesem Zustand kann der MC keine per Namen vorgegebene Dienste erreichen (z.B. NTP oder SCEP)
2. Die Anzahl der Einträge für bestimmte Tabellen wurde variable gestaltet. Unter den Tabellen befinden sich „Add“ und „Remove“ Tasten, die Einträge hinzufügen oder entfernen. Dadurch können die Konfigurationsseiten übersichtlicher gestaltet werden.
3. Fehler im seriellen Modul im UDP-Modus gefixt. Wenn keine IP-Adresse des Kommunikationspartners angegeben war, wurden die Verbindungsdaten des ersten eintreffenden Pakets von diesem nicht richtig verarbeitet, sodass eine Wiederholung notwendig war.

Firmware 2.07k --> 2.07v (25. August 2016)

1. Fehler im Pingtest-Modus (Roaming) behoben. Durch eine fehlerhafte Auswertung der Sequenznummern kommt es nach mehreren Tagen Betrieb (abhängig von den Intervall-Parametern) dazu, dass die Funktion unwirksam ist.
2. Erweiterung der Wireless-Dump-Funktion:
 - Es kann festgelegt werden, was geschehen soll, wenn der verfügbare Flash-Speicher voll geschrieben ist:
 - 1) Stop der Aufzeichnung
 - 2) Löschen der ältesten Aufzeichnung
3. Änderung im DHCP-Client-Modul. Bei manchen DHCP-Server funktionierte die Anforderung einer IP Adresse nicht korrekt. Mit der Änderung sollte es besser funktionieren.

Firmware 2.07v --> 2.08a (20. September 2016)

1. Überarbeitung der Dump-Funktion (Wireless + Ethernet) zur besseren Abspeicherung der WLAN- und Ethernet-Mitschnitte.
2. SNMP-Funktion wurde wesentlich erweitert. Die MIB-Datei des MC Geräts kann jetzt von der **Webseite** des MC (--> Admin --> SNMP) heruntergeladen werden.
3. Fehler bei der HTTPS Funktion. Wenn die initiale Generierung des selbst signierten Zertifikats aus irgendeinem Grund nicht komplett abgeschlossen wurde, konnte der HTTPS Zugang auf die MC Webseite nicht genutzt werden. Mit der 2.08a wird die Generierung erneut gestartet, wenn ein fehlerhaftes Zertifikat erkannt wird.

Firmware 2.08a --> 2.09d (14. Dezember 2016)

1. neu: Multi-SSID. Es können jetzt mehrere (bis zu 8) WLAN Profile konfiguriert werden.
2. Die Anzahl der Instanzen für die seriellen Schnittstellen werden jetzt auch dynamisch im MC-Config Programm und auf der Webseite angezeigt

3. Die Funktion zur Beschränkung der verwendeten Sendebitraten wurde überarbeitet. Mit der Firmware 2.09d können zunächst aber nur die Bitraten für den Modus 802.11 b/g eingestellt werden.
4. In manchen WLAN-Systemen kommt es vor, dass der WLAN-Controller BSSID's vergibt, die doppelt vorkommen, wobei eine BSSID im 2.4GHz existiert und die gleiche BSSID auch im 5GHz Band benutzt wird. Die Firmware 2.09d berücksichtigt dies und führt beide BSSID's getrennt in der Accesspoint-Liste.
5. Es gibt jetzt die Möglichkeit im MWLC-Modus den Datenverkehr durch den Tunnel zu priorisieren.
6. Unter „Realtime Clock“ kann jetzt die Zeitzone konfiguriert werden, wo der MC betrieben wird. Damit kann jetzt in den Debuglog-Dateien die lokale Zeit richtig angegeben werden.

Firmware 2.09d --> 2.10c (16. März 2017)

1. Neue Linux Kernel Version 4.9.13+ integriert
2. Verbesserte Reaktion des MC bei Störungen während der Authentifizierungsphase
3. Fehler bei der Behandlung mehrerer aktiver WLAN-Profiles behoben.
4. Die Behandlung der Dateien für die Trace-Mitschnitte (WLAN + LAN) wurde verbessert, sodass jetzt über das MC-Config-Programm einzelne Dateien zum Download selektiert werden können. Diese Dateien können im internen Flash und auf einem aufgesteckten USB-Stick gespeichert sein.
5. Es werden jetzt zusätzliche Informationen auf der „Home“ Seite des MC in der Liste der AP's angezeigt. Soweit der AP diese Informationen liefert, wird folgendes zusätzlich in der Spalte „Extra Information“ angezeigt:
 - Anzahl der eingebuchten Clients
 - Auslastung (%)
 - TPC Vorgabe vom AP
 Diese Angaben werden jetzt auch beim Roaming herangezogen um den am besten geeigneten AP zu ermitteln.
6. Fehler beim NTP Client behoben. Wenn die IP des Timerservers über DNS ermittelt werden musste und der erste Versuch dieser Adressenauflösung nicht gelang, wurde der Versuch nicht erneuert. Somit wurde keine Zeit über einen NTP-Server bezogen.

Firmware 2.10c --> 2.10i (02. Mai 2017)

1. Neue Kernelversion 4.9.25 integriert.
2. Fehler im Roaming-Modul bei der Zusammenstellung der zu scannenden Kanäle beseitigt.
3. Einführung eines neuen Parameters „Hostname“ im DHCP-Client-Modul. Damit kann unabhängig von dem Parameter „Device Name“ die Angabe „Hostname“ festgelegt werden, die der DHCP-Client an den DHCP-Server übermittelt.
4. Fehler bei der Überprüfung der Zertifikatsgültigkeit behoben. Ein Datum über das Jahr 2038 hinaus wurde als ungültig bewertet.
5. „Wireless Status Information Service“ um einige Statusabfragen erweitert (siehe Handbuch)

Firmware 2.10i --> 2.10k (18. Mai 2017)

1. Scanverhalten im 5 GHz Band verändert, sodass jetzt auch „hidden“ SSID's erkannt werden.
2. Im Pseudo-Level-2-Bridge Mode die Durchleitung von Broadcast Paketen verbessert. Diese Pakete werden von manchen WLAN Systemen als Unicast (Level 2) verschickt.

Firmware 2.10k --> 2.10n (12. Juni 2017)

1. Mit der 2.10k Firmware kam es vereinzelt zu Reboots beim Roaming, wenn die Signalwerte (SNR) nur relativ schwach waren. Es konnte ermittelt werden, dass diese Reboots durch zu intensive Debugmeldungen des Linux-Kernels ausgelöst wurden. Nach der Abschaltung dieser Meldungen konnte dieses Verhalten nicht mehr beobachtet werden.
2. Bei der SNMP Funktion kann man jetzt den Parameter „Community Name“ festlegen, sodass auch ein anderer Wert als „public“ eingestellt werden kann.
3. Im Bridge-Modus „Level 2 Pseudo-Bridge“ kann man jetzt einen DHCP-Relay-Agent aktivieren.

Firmware 2.10n --> 2.10r (04. August 2017)

1. Einführung einer Überwachungsfunktion die sicherstellt, dass nach einem ungewollten Abbruch des Bridge-Prozesses dieser neu gestartet wird.
2. Ein „memory leak“ führte dazu, dass der freie Arbeitsspeicher aufgebraucht wurde. Dies geschah insbesondere dann, wenn der LAN-Client sehr oft neue TCP-Verbindungen auf- und wieder abbaute. Je nach Intensität konnte das zu einem Stillstand der Bridge-Funktion führen und einen manuellen Reboot erforderlich machen.
3. Die Config der seriellen Schnittstelle hat eine neue Option erhalten, die bestimmt, wie mit Daten umgegangen wird, die bei einer noch nicht vorhandenen WLAN-Verbindung empfangen werden.

Firmware 2.10r --> 2.10s (01. September 2017)

1. Es wurde ein Fehler gefunden, der in Situationen mit schlechten Signalverhältnissen und somit mit vielen erfolglosen Sendeversuchen, zu einem Stop des Bridge-Prozesses geführt hat.
2. Linux Kernel Version 4.9.46+ integriert.

Firmware 2.10s --> 2.11a (10. Oktober 2017)

1. In den Debuglog-Meldungen wird im Zeitstempel jetzt auch das Datum angegeben.
2. Korrektur im SNMP-Modul. Einige als 64bit Werte definierte Zähler wurden zuvor nur als 32bit Werte geliefert.
3. Zusätzliche Option im NAT & Single Client NAT Mode:
Mit aktiver „Forward DNS requests“ Option werden die DNS Anfragen, die über die LAN-Seite auf der lokalen LAN-IP eintreffen, an den DNS-Server weitergeleitet, der auf der WLAN-Seite definiert ist.
4. Bei wiederholten Fehlversuchen während der Authentifizierung hat der WPA-Supplikant die betroffene SSID für 10 Sekunden blockiert. Die daraus resultierende Unterbrechung ist aber in einigen Anwendungen sehr störend. Daher wurde ein Algorithmus eingebaut, der diese Sperre schon sehr bald nach der Aktivierung wieder aufhebt. Die Unterbrechung wird damit auf ca. 3 Sekunden begrenzt.
5. Linux Kernel Version 4.9.53+ integriert.

Firmware 2.11a --> 2.11b (17. Oktober 2017)

1. Update des WPA-Supplikanten wegen der unter dem Namen KRACK ("Key Reinstallation Attack") bekannt gewordenen Schwachstelle im Sicherheitsstandard WPA2.

Firmware 2.11b → 2.11c (01. Februar 2018)

1. Linux kernel version 4.9.61+ integriert.
2. Null-Pointer Fehler im DHCP Client behoben.
3. Fehler in der Logserver Funktion behoben.
4. NTP – Server auf der LAN-Seite implementiert. Dieser NTP-Server ist nur im NAT oder Single-Client-NAT Mode aktiv und übermittelt die Daten, die der NTP-Client auf der WLAN-Seite erhalten hat.

Firmware 2.11c → 2.11m (14. Juni 2018)

1. Linux kernel version 4.9.105+ integriert.
2. Speicherfehler beim „Level2 Bridge Mode“ gefixt. Wenn der LAN-Client häufig offline ging, wurde Speicher reserviert, der nicht wieder freigegeben wurde. Das konnte dazu führen, dass der MC nach einer längeren Zeit nicht mehr kommunizieren konnte.
3. Zusätzlicher Parameter „AP Scoring“ unter Roaming.
Mit diesem Parameter kann festgelegt werden, ob bei der Bewertung eines AP's alle Informationen wie Sendeleistung, Kanalauslastung, Bandbreite (20 oder 40 Mhz) und die Signalstärke (SNR) herangezogen werden oder ob allein das stärkere Signal bewertet wird.
4. Zusätzliche Funktion „Connection Watchdog“ unter „Roaming“ eingeführt:
Damit kann eine Funktion aktiviert werden, die beobachtet, ob Daten vom aktuell verbundenen AP empfangen werden. Wenn diese Daten für die eingestellte Zeit ausbleiben, wird ein Neu-Scan durchgeführt. Der aktuelle AP wird beim folgenden „scoring“ niedriger bewertet, sodass es wahrscheinlich zu einem Wechsel des AP's kommt.
5. Extra-Parameter im „LAN Client Cloning Mode“:
Mit „MAC to Clone“ kann eine MAC-Adresse festgelegt werden, die über WLAN-kommunizieren soll.

Firmware 2.11m → 2.11p (13. August 2018)

1. „Logging“ → WLAN Dump Event Funktion deaktiviert. Es zeigte sich, dass diese Funktion in der Praxis keinen Nutzen hat.
2. Unter Roaming → „Preferred / avoided access points“ gibt es jetzt die Option „strictly avoid“ mit der ein Accesspoint gesperrt werden kann.
3. Fehler in der Relaisfunktion im UDP-Mode behoben.

Firmware 2.11p → 2.11p1 (24. August 2018)

1. Fehler bei der Bewertung der AP's im 2.4GHz Band behoben.

Firmware 2.11p1 → 2.12a (28. November 2018)

1. Neuen Kernel 4.9.140 integriert
2. Die Schnittstellen über die das MC-Config-Programm auf den MC zugreifen kann, können jetzt eingeschränkt werden:
 - LAN + WLAN (default)
 - LAN
 - Zugriff gesperrt
3. Unterstützung für AC-Funkkarten integriert
4. Der Schaltzustand des Relais kann jetzt auch über die WLAN-Info vom LAN-Client abgefragt werden.
5. Wenn WLAN- oder LAN-Mitschnitte auf einem MC aktiv sind (→ Logging), wird dieser Zustand im MConfig unter Status angezeigt (MConfig ab Version 2.0.2.42)
6. Experimentelle Power-Save-Funktion implementiert. Damit kann der MC für eine bestimmte Zeit in einen Schlafmodus versetzt werden. In diesem Zustand wird der Energiebedarf auf ~30% des Normalverbrauchs gesenkt.
7. Port-MAC-Authentication für LAN-Clients im NAT-Mode implementiert
8. Schnellerer Start bei gleichem Standort (Zuerst letzte WLAN-Frequenz testen)
9. Bei Default-Reset über den Resettaster wird geprüft, ob ein USB-Stick am MC aufgesteckt ist, auf dem die Datei "Default.cfg" vorliegt. Wenn ja, wird diese Config intern gespeichert und aktiviert.
10. LAN-Cloning: Verbesserte und korrigierte Prozedur für das Handling von ARP-Paketen

Firmware 2.12a → 2.12f (25. März 2019)

1. Neuen Kernel 4.9.164 integriert
2. Pseudo Level 2 Bridge Mode:
Unterstützung für passive Clients implementiert.
Mit der Aktivierung dieser Funktion werden LAN-Clients, die von sich aus keine Daten senden, im WLAN „bekannt“ gemacht, indem der MC Pings mit der IP des passiven LAN-Clients über WLAN an eine bestimmte IP verschickt.
3. Home Webseite:
Neben dem SNR wird jetzt auch die Signalstärke und der Geräuschpegel des Empfangssignals angezeigt.
4. Relais Funktion:
Dem Kommando zum Ausschalten des Relais kann man jetzt eine Sequenz anhängen, die

eine Verzögerungszeit angibt mit das Relais ausgeschaltet werden soll. Die Verzögerungszeit wird so definiert <xx> (xx = Zeit in Sekunden)

5. Bugfix: Spezielles Zertifikatsformat kann jetzt wieder importiert werden.
6. Feature: Bridge-Mode
Wenn die Bridge-Funktion deaktiviert wird, gibt es jetzt die Möglichkeit die IP-Einstellungen auf der LAN-Seite zu definieren (incl. DHCP-Client-Funktion).
7. Antennen-Gewinn kann jetzt als Parameter angegeben werden. Damit kann der Funksender die Sendeleistung so anpassen, dass die gesetzlichen Bestimmungen eingehalten werden.

Firmware 2.12f → 2.12k (19. September 2019)

1. Neuen Kernel 4.9.193 integriert
2. Mögliche Verwendung von TLS zur Verschlüsselung der Kommunikation mit dem MCConfig bei Firmware-Upgrades oder Logdatei Abruf
3. Bugfix zu Abstürzen bei der Verwendung von SNMP mit SNMPWalk. Korrekturen bei der Abfrage von Unsigned-Werten.
4. Relais-Funktion: Fehler bei fehlender Nullterminierung beseitigt.
Jetzt ist auch ein verzögertes **Einschalten** des Relais möglich.
5. Seriell-Funktion mit RS485: Korrektur bei der Ansteuerung des Treiber-IC's
6. WPA3 Modi erweitert. Jetzt ist auch der Modus WPA/WPA2/WPA3 auswählbar.
7. Wireless: DHCP-Renew jetzt auch beim Wechsel des Accesspoints einstellbar.
8. Webseite arbeitet jetzt auch mit TLS 1.2
9. Wireless-Info liefert jetzt nicht nur über das eingestellte Intervall Informationen.
Jetzt können auch per Request Statusinformationen angefordert werden. (nur über die LAN-Seite)
10. Ein aufgesteckter USB-Stick mit FAT-Dateisystem kann über die Webseite auf EXT4 formatiert werden. Damit ist er besser zur Aufzeichnung von Debugdaten (Logs oder Dumps) geeignet.

Firmware 2.12k → 2.12m (16. Oktober 2019)

1. Neuen Kernel 4.9.196 und Openssl 1.0.2t integriert
2. Überwachung der Nutzung des internen Flashspeichers:
Es ist mittlerweile zu Fällen gekommen, bei denen die (W)LANDump-Funktion (siehe Logging) vom Anwender dauerhaft eingeschaltet geblieben ist.
Durch diese damit verbundene intensive Nutzung über Monate wird nach einiger Zeit der Flashspeicher in seiner Funktion als Filesystem durch den starken „Verbrauch“ von Reserve-Sektoren stark eingeschränkt.
Mit der Firmware-Version 2.12m wird die (W)LANDump-Funktion in Bezug auf die

geschriebene Datenmenge, die Zeit, die die Dump-Funktion aktiv ist, und auf die Menge der noch vorhandenen Reserve-Sektoren ggf. automatisch abgeschaltet.

3. Auch im 5GHz Bereich kann man jetzt die Mindest-Bitrate einstellen.
4. Berücksichtigung von Sonderzeichen im Zertifikatspasswort

Firmware 2.12m → 2.12o (16. Januar 2020)

Funktionelle Änderungen:

1. Neuen Kernel 4.9.209 integriert
2. AUX-Input: Im Modus „Relay ON“ kann jetzt auch eigener Timeout für die Relais-Funktion angegeben werden.
3. Im Modus LANClient-Cloning werden redundante Netzwerkinformationen jetzt nicht mehr doppelt auf der Startseite angezeigt.
4. Die Wireless-Funktionalität kann jetzt ohne Neustart aktiviert/deaktiviert werden!
5. Für Zertifikate werden jetzt auch pkcs8-Keys ohne Passphrase-Encryption akzeptiert.

Bugfixes:

1. Eine mögliche Bitraten-Einstellung für 11bg und 11a war bisher falsch (11MBit statt 12MBit)
2. Die Serielle RS422-Schnittstelle hatte aufgrund eines anderen Patches zwischenzeitlich nicht funktioniert.
3. WEP-LEAP funktionierte bisher nicht.
4. DHCP-Client ändert jetzt das Gateway nach Re-Priorisierung oder Änderung korrekt.
5. Beim LANClient-Cloning wurden bisher ARP-Request von unserem Modul mit der IP des geclonten Clients an die LAN-Schnittstelle gesendet. Das konnte beim Client zu IP-Konflikten führen.
6. Ein zu schnelles Aktualisieren der Webseite in Verbindung mit Änderung der Konfiguration konnte zum Absturz führen.
7. Der DHCP-Client ist jetzt deaktiviert in Modikombinationen wo dies keinen Sinn macht.
8. Beendete interne Prozesse konnten bisher weiterhin Systemressourcen belegen.
9. Bei Nutzung des Relay-Ports wurde die Verbindung nicht richtig beendet, was dazu führen konnte, dass das Gerät nicht mehr richtig funktionierte.

Sicherheits-Updates:

1. Verbesserungen des Webservers um CSS-Attacken zu verhindern. (OWASP-Header & Cookie-Handling)
2. DoS-Attacken und andere ungewöhnliche Zugriffe werden jetzt erkannt, verhindert und geloggt.
3. HTTPS-Zugriffe auf die Website sind nur noch mit anerkannt sicheren Ciphers möglich.
4. HTTPS und HTTP Zugriffe klar getrennt.
5. Überlange Konfigurations-Variablen werden jetzt schon bei der Eingabe verworfen.

Firmware 2.12o → 2.12p (24. Januar 2020)

Bugfixes:

1. Es konnte unter Umständen passieren, dass bei statischer IP-Einstellung die Gateway-IP und der DNS Server nicht richtig gesetzt wurden.

Firmware 2.12p → 2.12r (26. Mai 2020)

Funktionelle Änderungen:

- 1) Neuen Kernel 4.9.223 integriert
- 2) WPA3 funktioniert jetzt auch mit FT (802.11r)
- 3) Ein optionales benutzerdefiniertes Zertifikat für den MC internen Webserver kann jetzt hochgeladen werden.
- 4) Rest-API liefert unter /API/Status jetzt mehr Informationen zur seriellen Schnittstelle und zum Relais.
Unter /API/Status/Device wird jetzt auch die Kernelversion angegeben.
- 5) BridgeMode NAT: Wenn die WLAN-Schnittstelle kein DHCP macht und kein Gateway definiert ist, kann jetzt auf der LAN-Seite ein Gateway definiert werden.
- 6) Optimierung der LTE Variante für LTE Campus-Netze
- 7) Roamingoptimierung auf der Basis von **IEEE 802.11k** mit Konfigurationsoptionen unter "Roaming".

Sicherheits-Updates:

- 1) jQuery Bibliothek auf Version 3.5.1 aktualisiert
- 2) Maßnahmen gegen SYN und PING Floods.

Firmware 2.12r → 2.12s (30. Oktober 2020)

Funktionelle Änderungen:

- 1) Neuen Kernel 4.9.240 integriert
- 2) Verbesserung beim Zertifikatsimport
- 3) Wireless: Bugfix für den Adhoc-Mode
- 4) Seriell: Anstatt einer IP-Adresse kann man jetzt auch einen Hostnamen angeben
- 5) Rest-API: Import von Zertifikaten und Statusabfrage der geladenen Zertifikate ist jetzt möglich
- 6) Langzeitaufzeichnung der WLAN-Signalwerte und Roamingvorgänge ist jetzt möglich
- 7) Relais: Statusanzeige des aktuellen Zustands auf der Webseite korrigiert

Firmware 2.12s → 2.12u (05. Januar 2021)

Funktionelle Änderungen:

- 1) Neuen Kernel 4.9.253 integriert
- 2) Möglicher Deadlock beim Starten behoben.
- 3) In der AP-Liste auf der "Home"-Seite wird jetzt auch die minimale Bitrate des AP's angegeben. Damit kann man ggf. Einstellungen bezüglich der minimalen Bitrate auf der "Wireless -> Main Parameter" Seite vornehmen.
- 4) Die Funktion zur Überwachung der WLAN-Verbindung konnte beim ersten Authentifizieren (EAP) zu früh ein Neuaufsetzen der WLAN-Verbindung erzeugen. Dies wurde korrigiert.
- 5) Die Statusabfrage per API liefert jetzt Informationen zur WLAN- und (oder) zur LTE-Funkkarte.
- 6) 802.11ac Option nur sichtbar wenn auch eine AC-Funkkarte vorhanden ist.
- 7) Maximale Ausschaltverzögerung bei der Relais-Funktion von 100 auf 3600 Sekunden abgehoben.

Firmware 2.12u → 2.12v (15. Januar 2021)

Funktionelle Änderungen:

- 1) Verkürzung der Zeit bis zum Aufbau einer WLAN-Verbindung nach einen Neustart, nur in dem Fall wenn die EAP - Authentifizierung aktiv ist.

Firmware 2.12v → 2.12w1 (28. Juli 2021)

Sicherheits-Updates:

- 1) Neuen Kernel 4.9.277 integriert:
Dieser Kernel schließt die Sicherheitslücke, die unter dem Stichwort „FragAttacks“ publik wurde.

Funktionelle Änderungen:

- 1) Admin:

Unter „Admin“ → „Securing Passwords“ kann man jetzt einstellen, dass die verschlüsselten Parameter (Passwörter, PSK, Zertifikatsschlüssel usw) beim Download der Config nicht exportiert werden.

2) NAT-Bridge-Mode:

Im NAT-Mode wird jetzt der Betrieb eines FTP-Servers am LAN-Port unterstützt. Durch die dynamischen Ports bei den FTP-Dateitransfers, war es bisher nicht möglich, dafür NATRegeln zu definieren. Man kann jetzt eine Port-Weiterleitungsregel mit der Eigenschaft „:ftp“ kennzeichnen, sodass mit Unterstützung des Linuxkernels die verwendeten Ports automatisch richtig weitergeleitet werden.

Im NAT-Mode kann jetzt eine DMZ-IP angegeben werden. Dadurch kann man eine IP definieren, an die alle Datenpakete, für die es keine passende Weiterleitungsregel gibt, weitergeleitet werden.

3) SCEP:

Verbesserungen im Ablauf. (Verbesserungen für Nexus SCEP-Service) Zertifikat wird erst bei erfolgreichem Ablauf ersetzt (Initiales generisches Zertifikat für SCEP möglich). Auch bei einem Renewal wird jetzt ein Challenge-Password mit übertragen.

Renewal/Enrollment kann per Konfigurationswert getriggert werden. Für den gesamten Renewal/Enrollmentprozess wird wenn möglich eine HTTP-Session verwendet (Nötig für Loadbalancing des SCEP-Service)

4) Statistics→Network:

Bitraten und übertragene Bytes/Frames werden lesbarer dargestellt.

5) LANCloning:

Parse des Hostnamens aus dem DHCP-Request und Anzeige auf der Statusseite

6) Seriell → Special Options → Resend unacknowledged :

Über die serielle Schnittstelle empfangene Daten, die per TCP weitergeleitet werden, gelten erst dann als bestätigt, wenn diese von der Gegenseite per TCP als korrekt empfangen bestätigt werden. Wenn eine TCP-Verbindung unterbrochen und neu wieder hergestellt wird, werden die als unbestätigt gespeicherten Daten über die neue Verbindung erneut gesendet. Das kann ggf. zu Wiederholungen beim Empfänger dieser Daten führen.

7) Network → IP Address:

Man kann jetzt zusätzlich spezielle Routen definieren, wenn bestimmte IP-Adress-Bereiche über spezielle Gateways erreicht werden sollen.

Bugfixes:

1. Seriell → Comserver Mode

Im Comserver Mode funktionierte der Hardware-Handshake Modus (RTS/CTS oder DTR/DSR) nicht richtig

2. Kernel

Problem mit der Sende-Bitratenvahl in 802.11b/g Netzwerken behoben. Dieses Problem ist ab der Firmware 2.12u aufgetreten.

Firmware 2.12w1 → 2.12x (29. Nov 2021)

Sicherheits-Updates:

Neuen Kernel 4.9.290 integriert

Funktionelle Änderungen:

1. Startdatum:
Der MC startet jetzt nicht mehr ab dem Jahr 2000, sondern startet mit dem Jahr in dem die Firmware compiliert wurde.
2. Json:
UTF-8 und ISO8859-1 escaping korrigiert.
3. LTE:
Delta-Upgrade-Funktion für Firmware von EC25 und RM500Q
4. TLS1.2:
NULL-Ciphers deaktiviert
5. Wireless:
Bei der Verbindung mit Accesspoints wird eine Warnung ausgegeben, wenn die Kanalnutzung besonders hoch ist. Die Kanalnutzung für 2.4GHz und 5GHz wird auf der Webseite besser angezeigt.
6. SNMP:
Der Status der einzelnen LAN-Ports kann jetzt abgefragt werden.
7. NAT:
Konfiguration für +Hairpinning (NAT-Loopback) hinzugefügt.
8. SCEP:
Längere CA-/SCEP-Server URL möglich.
Option für HTTP-Redirect ("Location: ...") hinzugefügt
Option für HTTP-Proxy hinzugefügt

Bugfixes:

1. Wireless:
802.11k - Anzahl der Nachbar-APs limitiert. Wenn der AP eine Liste mit mehr als 31 Nachbar-AP's lieferte konnte es zu einem Absturz kommen.
2. Wireless:
Wurde der MC bei ausgeschaltetem WLAN und aktivem DHCP eingeschaltet, wurde der DHCP-Client nicht richtig gestartet wenn das WLAN anschliessend per API eingeschaltet wurde.

Firmware 2.12x → 2.14b (04.07.2022)

Sicherheits-Updates:

Update der Linux Kernel Version von 4.9.290 → 5.4.202

Funktionelle Änderungen:

1. MWLC:
PAE (Port Access Entity) Weiterleitung im MWLC-Mode implementiert.
MWLC-Master kann jetzt auch als Hostname definiert werden.
2. Print Server:
Adaptive Erkennung ob ein angeschlossener Drucker als lp0 oder lp1 erkannt wird.
3. Web-Interface:
Zusätzliche Seite unter „Device“ → „Network Test“
Dort können ausgehend vom MC Netzwerkverbindungen getestet werden.

Homepage: zusätzliche Informationen zu den angeschlossenen LAN Clients im NAT-Mode
4. Default Reset (Clear Dumps and Log):
jetzt werden auch evt. vorhandene Coredump-Dateien gelöscht.
5. SNMP:
neue Info zur IP-Adresse des WLAN-Interfaces (1.3.6.1.4.1.29456.3.15.0)
6. AUX-IN:
Ein- und Ausschalten der AUX-IN Funktion per Config führt nicht mehr zum Reboot des MC
7. NAT-Mode: snat Option eingeführt.
Damit sieht der LAN-Client die IP des LAN-Interfaces vom MC als Quelle.
8. ARP-Probe: bei dem ARP-Probe-Test des MC werden jetzt eingehende Antworten besser ausgewertet. Dadurch wird vermieden, dass vom AP gesendete Wiederholungen der ARP-Probes als solche erkannt und nicht als IP-Konflikt gewertet werden.
9. LTE:
Auswahl von Authentifizierungsarten „ PHP+CHAP,PAP,CHAP“ hinzugefügt.
OpenVPN: Import von Client-Config verbessert.
OpenVPN-Client: Korrektur im TUN-Modus. Masquerading und NAT-Support.
OpenVPN-Server/-Client: Neue Version: OpenVPN 2.5.6.
Upgrade der LTE-Firmware nur ausführen, wenn diese nicht schon die aktuelle ist.
Anzeige der IMEI (International Mobile Equipment Identity) in der Statusabfrage
5G: Kampus-Netz Korrekturen (5G-SA)

Firmware 2.14b → 2.14c (10.10.2022)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.202 → 5.4.215

Funktionelle Änderungen:

- 1) neue REST-API Funktion: LAN-Port Status + OpenVPN Server Abruf für CA-Cert und Client-Config
- 2) MQTT-Client für Seriell, Relais und AUX-Eingang

Bugfix:

- 1) Relais: Der Relais-Timeout, der über den Input gestartet werden kann, wurde nicht zurückgesetzt, wenn während der Ablaufzeit dieses Timers, das Relais über das Netzwerk angesteuert wurde.
- 2) Seriell: Fehler beim RTS/CTS Handshake behoben.

Firmware 2.14c → 2.14d (16.10.2022)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.215 → 5.4.218

Fix für:

CVE-2022-41674

CVE-2022-42720

CVE-2022-42721

CVE-2022-42722

Firmware 2.14d → 2.14e (18.10.2022)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.218 → 5.4.219

Fix für:

CVE-2022-42719

Firmware 2.14e → 2.14f (04.01.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.215 → 5.4.228 BuildRoot 2022.08.3

Funktionelle Änderungen:

- 1) Mit der Firmware 2.14 wurde nach jedem AP-Wechsel die ARP-Tabelle der WLAN-Schnittstelle gelöscht, sodass folgend immer erst ARP-Request - Response ausgetauscht werden mussten, bevor die Kommunikation fortgesetzt werden konnte.
Mit der 2.14f gibt es die Option "Clear ARP" (->Roaming) mit der per Default das Löschen der ARP-Tabelle verhindert wird.
- 2) (Roaming) Der EAP Authentication Watchdog ist jetzt konfigurierbar. Bisher justierte sich dieser Timeout anhand der gemessenen Zeitdauer des letzten erfolgreichen EAP-Handshakes. Jetzt kann auch ein fester Timeout (1,2,3,4 Sekunden) eingestellt werden.
- 3) Zur Übertragung der Konfigurationsdatei findet jetzt eine Komprimierung der Daten statt. Das führt zu einer schnelleren Übertragung der Konfiguration.
- 4) (Logging) Es kann jetzt ein Trennzeichen zwischen den verschiedenen ausgegebenen Informationen angegeben werden. Damit lassen sich die Debugausgaben ggf. besser in eine Tabelle einfügen.
- 5) Erkennung von Replay-Paketen. Wenn diese zahlreich in kurzer Zeit registriert werden, wird die WLAN-Verbindung getrennt und neu aufgebaut.
- 6) Die Durchnummerierung der Debug-Dateien im USB-Stick wird jetzt mit führenden Nullen gemacht, sodass sich eine bessere Sortierung der Dateinamen ergibt.
- 7) MQTT-Broker: Die Maximallänge des Hostnamens wurde auf 256 erweitert.

Firmware 2.14f → 2.14g1 (10.02.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.228 → 5.4.231 BuildRoot 2022.08.3

Funktionelle Änderungen:

bei der REST-API Abfrage API/Status/Device wird jetzt auch der Device-Name angegeben.

Bugfix:

Ab der Version 2.14 führe eine Einstellung der AP-Density ungleich „autodetect“ zu einem schlechten Roamingverhalten.

Firmware 2.14g1 → 2.14h (02.03.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.231 → 5.4.233

Funktionelle Änderungen:

1. MQTT-Client: Der MQTT-Client kann jetzt Statuswerte senden, die man auch über die REST-API (Status) auslesen kann.
2. MQTT-Client: QoS für alle Publishes einstellbar.
3. MQTT-Client: Verbindungstimeout einstellbar (Vorher fest auf 60 Sekunden)
4. MQTT-Client: das LWT wird jetzt auch ausgelöst, wenn der MC gezielt neu gestartet wird.
5. Logging: WLAN-Dumps mit Filtermöglichkeit. So kann man z.B. nur den eigenen WLAN-Datenverkehr aufzeichnen. Damit wird in vielen Systemen der überwachte Zeitraum erheblich erweitert.

Bugfix:

Network-Dumps: Wenn bei vollem Speicher für die Dump-Dateien, viele Daten über (W)LAN sendet bzw. empfangen wurden, konnte es zum Systemabsturz (Reset) kommen. Dieser Fehler wurde behoben.

Firmware 2.14h → 2.14i (12.03.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.233 → 5.4.240

Funktionelle Änderungen:

1. EAP-Hanging und 4-Way-Handshake Timeout werden jetzt auch in die Verbindungsstatistik der verwendeten AP' aufgenommen.
2. EAP Authentifizierung: zusätzlich Option für die Aktivierung von TLS 1.2
TLS 1.2 war bisher nicht aktiv, weil es Probleme mit älteren RADIUS Servern gab.
Aus Kompatibilitätsgründen ist diese Option per Default nicht aktiv.
3. Ping-Test: Die Debug-Ausgaben wurden überarbeitet. Der Debug-Level für diese Funktion ist jetzt abhängig vom „Wireless Debug Level“.

Firmware 2.14i → 2.14k (16.05.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.240 → 5.4.242

Funktionelle Änderungen:

1. Das Relais ist jetzt auch über die REST-API und mit Hilfe von Anweisungssequenzen steuerbar.
2. Authentifizierung von einzelnen API/URLs:
Dadurch ist es möglich, Zugriffe auf bestimmte API-Funktionen mit einem separaten

User/Passwort abzusichern ohne das User/Passwort für die Gerätekonfiguration verwenden zu müssen.

3. Remote Capture Daemon:

Damit können z.B. per Wireshark Mitschnitte auf der (W)LAN Schnittstelle eines MCx remote abgerufen und live angezeigt werden.

Bugfix:

Segfault-Fehler in der MQTT Funktion behoben (TLS-Write)

Segfault-Fehler im Timermodul behoben (Blacklist + ConfigChange)

Firmware 2.14k → 2.14m (14.06.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.242 → 5.4.246

Funktionelle Änderungen:

1. wpa_supplicant aktualisiert auf 2.11-dev (Git Rev. 95C3f0d1)
2. Verbesserung bei der Relais-Steuerung über die REST-API:
Fehlerhafte Sequenzen und falsche Relais-Befehle werden jetzt mit HTTP Error 400 abgelehnt.
3. Ausgabe einer Warnung im Debuglog, wenn bei der Score-Berechnung alle passenden SSID's mit 0 bewertet werden. Das deutet darauf hin, dass eine der Crypto-Einstellungen nicht passt.
4. Warnung im Debuglog nach dem Start wenn Zertifikate (Client und CA-Zertifikate) geladen sind, die bald ablaufen oder schon abgelaufen sind.

Firmware 2.14m → 2.14n (25.07.2023)

Sicherheits-Updates:

Update der Linux Kernel Version von 5.4.246 → 5.4.249

Funktionelle Änderungen:

- 1) Webserver-Security:
 - Es können jetzt Vorgaben für die TLS session's handshake Algorithmen gemacht werden.
 - Neue Option Send HSTS Header
- 2) EAP: EAP-TTLS kann jetzt auch ohne Zertifikate durchgeführt werden. (ähnlich wie bei EAP-PEAP)
- 3) wpa_supplicant: jetzt mit 802.11v Support.
- 4) Wireless: Anzeige in der AP-Liste ob ein Accesspoint 802.11v unterstützt.
- 5) Seriell: Die serielle Schnittstelle kann jetzt auch per TLS kommunizieren.
Dazu können auch Zertifikate zur Authentifizierung installiert werden
- 6) Bridge/NAT: Warnung vor Konflikten von lokalen Services des Geräts mit per Config definierter NAT-Regeln.
- 7) MQTT-Bridge: Jetzt auch mit lokalem Websocket-Port (Default 8080)

Bugfix:

1. Seriell: Bei jedem TCP-Reconnect wurden ca. 1500 Bytes Arbeitsspeicher nicht wieder freigegeben.
2. WLAN-Dump: Wenn im LAN-Client-Cloning ein Filter gesetzt wurde, der nur den eigenen Traffic aufzeichnen soll, dann wurde nicht die richtige MAC zur Definition des Filters genommen.

Firmware 2.14n → 2.14o (25.08.2023)**Sicherheits-Updates:**

Update der Linux Kernel Version von 5.4.249 → 5.4.252

Funktionelle Änderungen:

1. SYN-Flood Erkennung auf 40 SYN Burst heraufgesetzt. Durchschnittlich sind 5 SYN / Sekunde noch Ok.
2. SNMP: Ergänzung der Statuswerte aus den Infos von /proc/net/dev
3. Verbesserung für IPv6 Bridging
4. SCEP: Wenn der CA Identity Parameter für die URL unerlaubte Zeichen enthält wird der Wert URL-Encoded
5. Anzeige zusätzlicher Warnungen im MConfig (ab Vers.: 2_0_3_9) in der Spalte „Status“:
 - Für Zertifikate die zeitnah ablaufen oder schon abgelaufen sind
 - Für fehlerhaft konfigurierten Ping-Test.