

In this newsletter
read about

- CCR2004-16G-2S+ • cAP XL ac • KNOT LR8/LR9 kit • TG-BT5-IN • TG-BT5-OUT • HGO-LTE-W
- UNII-2 support for more products • ZeroTier added to RouterOS v7 • Info on the MÉRIS botnet
- Diving deep into RouterOS: Switching • Bridging two centuries with MikroTik

CCR2004-16G-2S+

\$ 465



16x Gigabit Ethernet ports



2x 10G SFP+ cages



RJ-45 console port

Like the other models in CCR2004 series, this CCR also features the Amazon Annapurna Labs Alpine v2 CPU with 4x 64-bit ARMv8-A Cortex-A57 cores running at 1,7GHz. But here's the difference. This powerful router crushes all previous CCR models in single-core performance, and that is the most important aspect when it comes to heavy operations based on per-connection processing. Like queues, for example.

But that's not all! It also has the best single-core performance per watt and best overall performance per watt among all the CCR devices. **Better for the planet, better for the bills, it's a win-win!**



Best single-core performance in the CCR family
Built-in dual redundant power supplies


The new router has 18 wired ports, including 16x Gigabit Ethernet ports and two 10G SFP+ cages. It also has a RJ-45 console port on the front panel.

Like all CCR devices, it comes in a classic white 1U rackmount case. Built-in dual redundant power supplies are included, so you have one less thing to worry about. And, of course, there is active cooling to keep things nice and cool.

Each group of 8 Gigabit Ethernet ports is connected to a separate Marvell Amethyst family switch-chip. Each switch chip has a 10 Gbps full-duplex line connected to the CPU. The same goes for each SFP+ cage - a separate 10 Gbps full-duplex line. Boards come with 4GB of DDR4 RAM and 128MB of NAND storage.

So as you can see - no bottlenecks. As long as the CPU can handle the processing, all ports can reach wire speed. And this CPU is a beast that can handle a lot. If we look at the performance, you can see that it is trading blows with our CCR1009. Even surpassing it in CPU-heavy configurations! And if that wasn't enough – it can even reach the performance of CCR1016.

CCR1009-7G-1C-S+




Bridging

Configuration	64 byte		512 byte		1518 byte	
	kpps	Mbps	kpps	Mbps	kpps	Mbps
none (fast path)	9816.7	5340.3	3759.4	15398.5	1300.4	15791.9
25 bridge filter rules	1868.4	1016.4	1817.6	7445.1	1300.4	15791.9

Routing

Configuration	64 byte		512 byte		1518 byte	
	kpps	Mbps	kpps	Mbps	kpps	Mbps
none (fast path)	11627.7	6325.5	3759.4	15398.5	1300.4	15791.9
25 simple queues	960.2	522.4	964.1	3948.8	917.5	11142.1
25 ip filter rules	638	347	639.2	2618	615.8	7477.9

CCR2004-16G-2S+



Bridging

Configuration	64 byte		512 byte		1518 byte	
	kpps	Mbps	kpps	Mbps	kpps	Mbps
none (fast path)	9697.9	5275.7	5648.4	23136	2591.6	31472
25 bridge filter rules	2424.2	1318.8	2451.7	10042.1	2249.5	27318.5


Routing

Configuration	64 byte		512 byte		1518 byte	
	kpps	Mbps	kpps	Mbps	kpps	Mbps
none (fast path)	8664.2	4713.3	5239.6	21461.2	2532.4	30753.8
25 simple queues	1316.8	716.3	1217.6	4987.2	1174.6	14264.6
25 ip filter rules	842.1	458.1	860.7	3525.5	866	10517.1

The best part? This brand new CCR is among the most affordable options out there - not only within the CCR series, but on the market in general.

One of the most common ways to use this device would be: Gigabit Ethernet ports for the internal network; SFP+ ports for downlink and uplink. The perfect all-in-one solution for small and medium-sized businesses. Easy and efficient.

With the new CCR2004, you can take your office network to the next level. Without breaking the bank.



cAP XL ac

\$ 99



DUAL-BAND,
DUAL CHAIN



GIGABIT ETHERNET



IMPROVED HIGH-
GAIN ANTENNA



POE-IN, POE-OUT



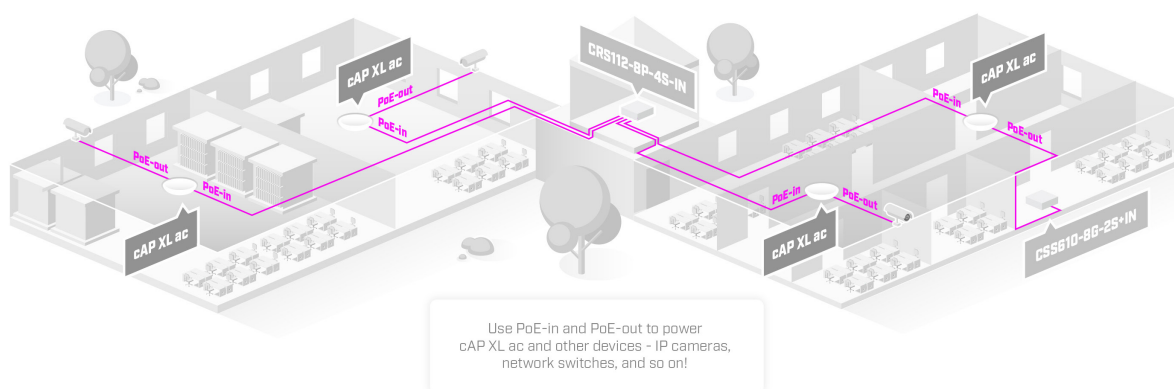
INCONSPICUOUS
AND COMPACT

Need a nice-looking access point that won't get in your way? Or perhaps you're managing the network in a crowded place and don't want everyone to have physical access to the device? Either way – ceiling is the answer! The “XL” in the name is only referring to the antenna within – the new cAP is a pretty compact device that attracts less attention than a smoke sensor. Your clients, guests, or colleagues won't even notice it. But they will definitely notice the blazing fast wireless connection all across the premises.



The new design features a larger high-gain antenna, higher sensitivity, and a built-in reflector.

These improvements allow increasing the covered area by twice, compared to the previous cAP models!



The dual-band, dual-chain 2.4 and 5 GHz wireless radio provides a strong coverage in 360 degrees around it, so you don't have to worry about the placement of the device so much. Putting it on the ceiling eliminates many signal absorption problems, such as the signal being blocked by large TV sets, metal cubicle walls in open space offices, etc.

Even though the radio supports repeater mode, the two Gigabit Ethernet ports give you the ability to extend your network with cables, even if PoE power is required: the cAP XL ac supports 802.3af/at PoE input on the first port and passive PoE output (up to 57V) on the second port.

Quick cAP tip: the customizable mode button in the center will turn off all lights, but can be reconfigured to launch any RouterOS script.



KNOT LR8/LR9 kit

\$ 199



LORA ® 868MHZ OR 915MHZ	CAT-M/NB TECHNOLOGY	2.4 GHZ WIRELESS	BLUETOOTH	2X 100 MBPS ETHERNET PORTS
POE-IN & POE-OUT	MICROUSB	GNSS	GPIO	RS485/MODBUS

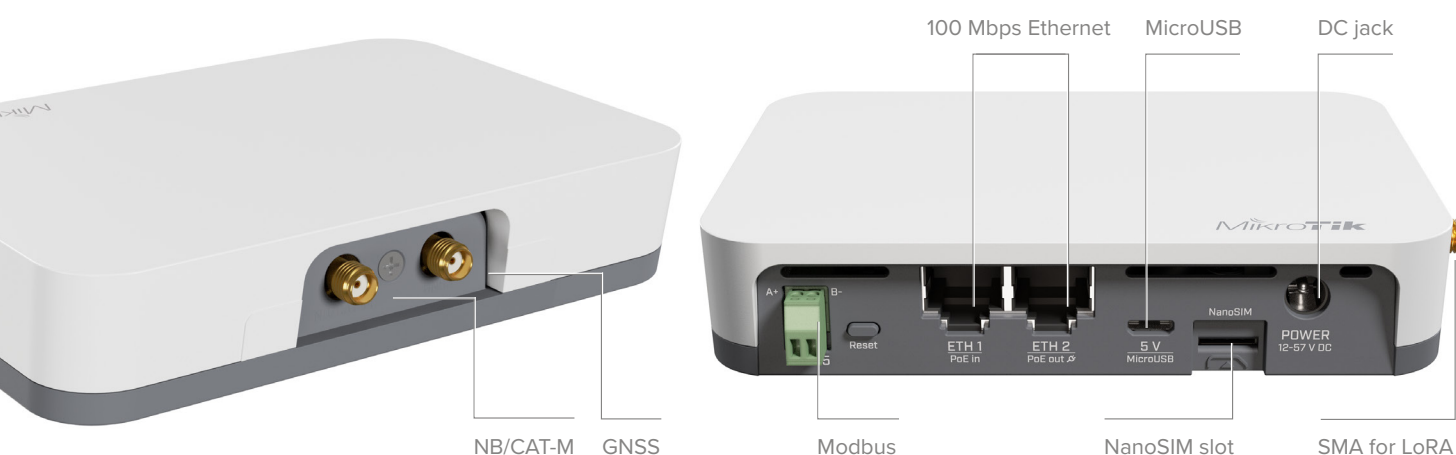
We all know the struggle of managing so many devices with different interfaces and communication protocols. You keep adding new solutions to your setup to keep up, but the older devices are still too good to let them go. How do you integrate all of them in a single system that will serve you right? Easy – you “tie” them together by using the KNOT!

It doesn't matter whether you have devices that are no longer in production, devices that came out this year, or even some custom solutions by your technician – the KNOT can handle them all!

KNOT LR8/LR9 kit is an out-of-the-box IoT Gateway solution for LoRa® technology. It uses Narrow Band and CAT-M technology. Because of the low cost, low bandwidth cellular connection, it is supported by countless mobile operators around the globe. This kit contains a pre-installed UDP packet forwarder to any public or private LoRa® servers. With the support of 8 different channels, Listen Before Talk (LBT) and spectral scan features this product will astound you with its enticing price point.

It could be used as a backup connection for the Ethernet or as a management channel for your network. NB/CAT-M monthly plan is much cheaper than LTE. Why spend extra money on bandwidth you don't need? For example, you can manage a KNOT-powered vending machine with temperature and moisture sensors using only a few megabytes per day!

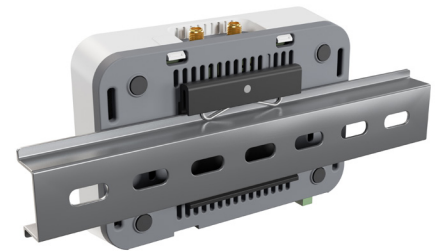
KNOT features so many protocol support and connectivity options: 2.4 GHz wireless, Bluetooth, LoRa®, 2x 100 Mbps Ethernet ports with PoE-in and PoE-out, Micro-USB. Maximum convenience at the lowest cost!



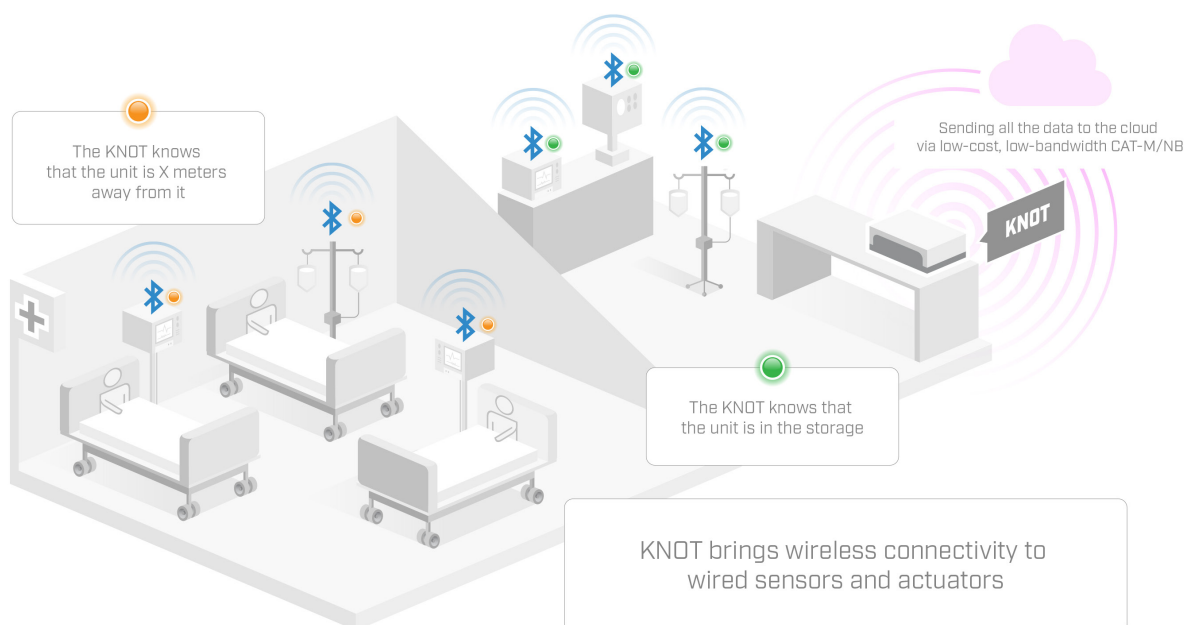
With the Bluetooth interface, you can use the KNOT for asset tracking and telemetry based on Bluetooth advertisement packets. KNOT supports any BLE tag that sends advertisement data. iBeacon, Eddystone or any other format. It has powerful filters for forwarding only relevant packets and ignoring others.

This kit can even help you in the most unusual situations. Remember the part about onboard GPIOs? Those pins can be used to read all kinds of analog sensors, interact with a single-board computer or other custom electronics – hobbyist kits, D.I.Y. robotics... It's like getting the whole Swiss Army instead of a Swiss Army knife!

KNOT is a great tool for most outdoor cabinet IoT applications as well. It comes with a DIN rail mount that allows easy integration with all kinds of setups: from agriculture and asset tracking to cold chain monitoring, industrial manufacturing, and so on.



Bring flexible low-cost connectivity to the most remote or tricky areas with the Mikrotik KNOT!



How would all this work in real life? Well, let's imagine a hospital. Lots of expensive assets moving across huge buildings. Tools, equipment, meds, you name it. Everything gets moved around all the time. Usually, hospitals have to spend a lot of resources on inventory checking.

Let's fix that. Place low-cost Bluetooth tags on all the important items. Add a KNOT device in every storage room. Now the hospital management always knows if the equipment is returned to its place. Why stop there? You can add temperature sensors to medical supplies and use the KNOT to keep track. The possibilities are endless.

Take a look at what The Things Industries and Deutsche Telekom IoT had to say about the bright future of LoRaWAN® and LTE-M!

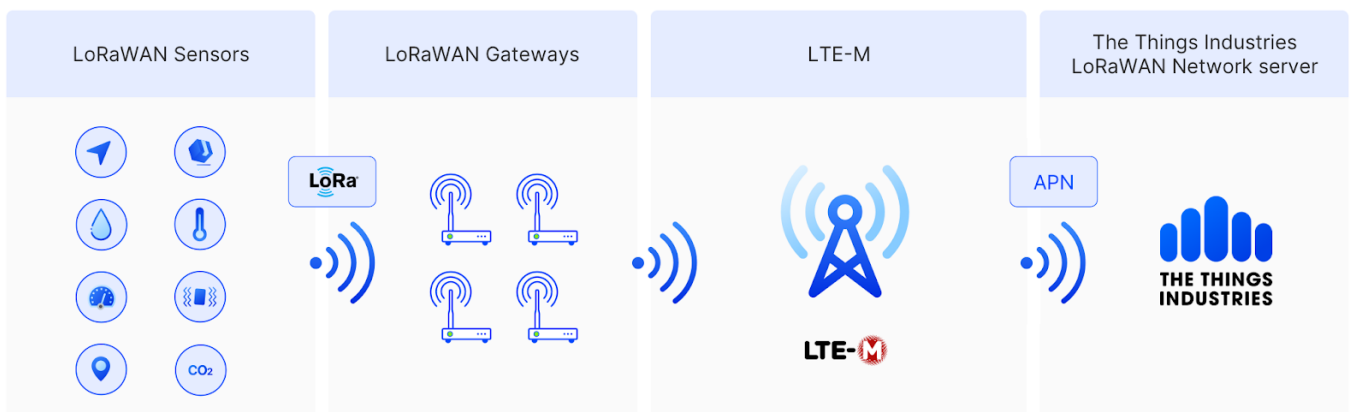
“LTE-M features very good signal penetration, well-suited for standalone, managed gateways inside, for example, smart buildings. The solution will therefore start with a smart building starter kit, comprising a pre-configured LoRaWAN gateway from MikroTik, connected over a LTE-M backhaul to TTI’s device and data platform. “



*“This collaboration is a further step on our way to an open IoT network.
New interfaces allow us to unlock the full potential of IoT”*

Mangal Afzal, Deutsche Telekom IoT.

Read more [here](#) and [here](#).





BUILT-IN BATTERY THAT WILL LAST FOR YEARS



BLE (BLUETOOTH LOW ENERGY) 5.2 WITH SILABS BG22



BUILT-IN ACCELEROMETER



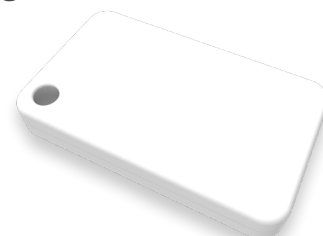
MAGNET ACTIVATION



IBEACON, EDDYSTONE, MIKROTIK TELEMTRY

TG-BT5-IN: slim and sleek, perfect for indoor inventory tracking

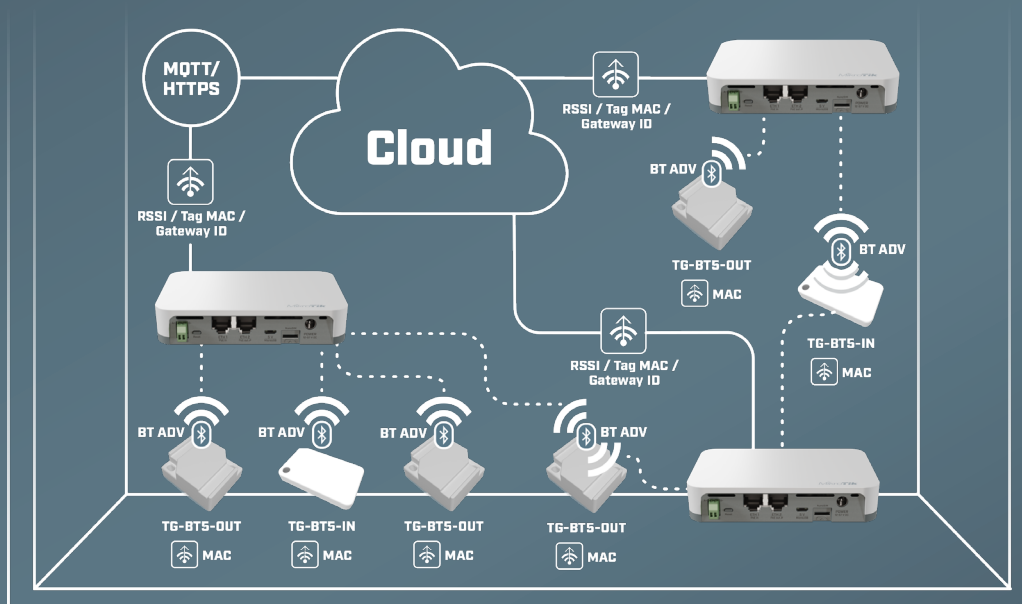
Bluetooth tags play a huge role in IoT setups, where Bluetooth is used to broadcast the data over short distances. You can use these small devices for proximity-based tracking of various objects. For example, if you have a KNOT gateway in different parts of a construction site, you can use these tags to locate construction tools, electrical equipment, and other assets.



37x22x6mm

Just attach the tags to the necessary items - and the nearest gateway will sense the tags in its proximity. Exceptionally useful in warehouse logistics – let your cargo inform you as soon as it enters the warehouse! They use so little power that a single built-in 220 mAh battery will last for years.

Once activated, the tag will broadcast iBeacon, Eddystone or MikroTik telemetry advertising packets to the gateway (such as the KNOT or any other BLE gateway). These packets contain MAC address used for ID, as well as telemetry data – such as acceleration, tilt and battery charge level. The gateway then pushes the data to the remote server utilizing MQTT, HTTP or HTTPs protocols. By default, advertisement packets are sent once every 5 seconds, but you can change this value to your liking. For example, if you set the interval to 1 second, the battery will typically last two years. The built-in accelerometers can not only detect acceleration (movement), but can also register if the device was dropped or tilted (free-fall detection). The indoor version of our BLE tags works best in a temperature range from 0°C to 70°C. It is splash-proof, and comes with a built-in accelerometer.



TG-BT5-OUT

\$ 18



BUILT-IN TEMPERATURE SENSORS



BUILT-IN BATTERY THAT WILL LAST FOR YEARS



BLE (BLUETOOTH LOW ENERGY) 5.2 WITH
SILABS BG22



BUILT-IN ACCELEROMETER



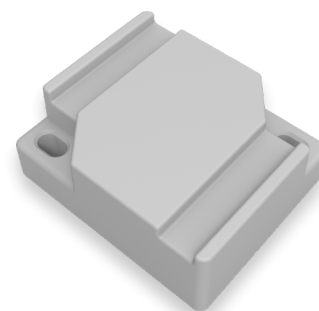
MAGNET ACTIVATION



IBEAON, EDDYSTONE, MIKROTIK TELEMETRY

TG-BT5-OUT: the heavy-duty tag for industrial challenges

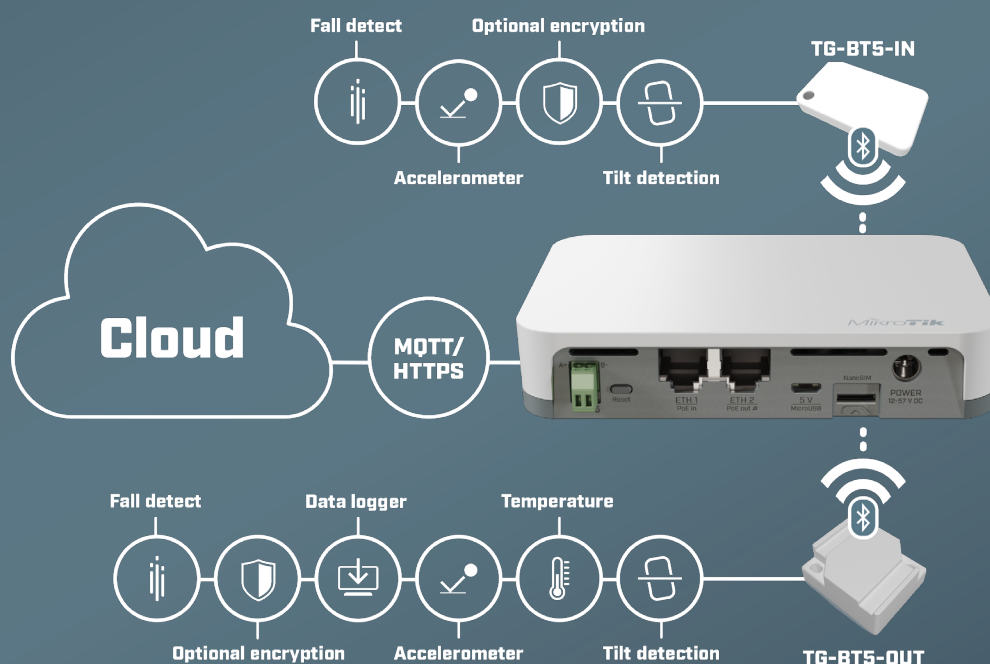
This version of our BLE tags comes completely sealed, cast in industrial-grade molds to give it a solid IP69k ingress protection rating. In other words, this tag is dust-tight – nothing gets in, and it is fully protected against close-range high-pressure, high-temperature spray downs. Perfect for industrial telemetry systems or to track all kinds of heavy equipment and materials at a construction site.



38x32x16 mm

Like the indoor version, this tag also supports iBeacon, Eddystone, and MikroTik telemetry formats. There is an NFC encoded MAC address and optional encryption. Unlike the indoor version, the outdoor tag comes with a built-in temperature sensor that can be used for condition monitoring. The $\pm 0.5^{\circ}\text{C}$ precision can be very useful in cold supply chain logistics.

TG-BT5-OUT features an improved 550 mAH battery that will last around five years (with a sending interval of 1s). It is suitable for strapping to all kinds of surfaces, and it can handle a temperature range of -20°C to 85°C .



Combine these tags with our [KNOT](#) IoT gateway to create the most affordable and flexible asset-tracking or telemetry setup ever!



A handy IoT combo antenna for both LTE and LoRa® frequencies.



Perfect for the MikroTik
KNOT LR series!

No need to buy several antennas for your Internet-of-things setups – just grab the new HGO-LTE-W antenna that can handle an impressive frequency spectrum: 699MHz – 3,8GHz.

That's right – you can use the same antenna for LTE, CAT-M/NB and LoRa® connectivity.

This antenna will transmit whichever signal your modem provides. For example, if you are using our KNOT LR8/LR9 kit, you can use this powerful 1.5 – 4 dBi antenna to communicate with all your 868 MHz devices and then send the data to the cloud via LTE.

Specifications

Product code	HGO-LTE-W
Connector type	SMA male
Operating temperature	-40°C to +70°C

UNII-2 support for more products

The following information will be useful for the United States and Canada customers, who use -US locked wireless products, others can skip this article.

We are happy to report that with the release of RouterOS 6.48.4, more devices are receiving UNII-2 frequency support:

- 1. hAP ac3 LTE6 kit (RBD53GR-5HacD2HnD-US&R11e-LTE6)**
- 2. hAP ac3 (RBD53iG-5HacD2HnD-US)**
- 3. hAP ac (RB962UiGS-5HacT2HnT-US)**
- 4. Audience (RBD25G-5HPacQD2HPnD-US)**
- 5. Audience LTE6 kit (RBD25GR-5HPacQD2HPnD-US&R11e-LTE6)**



This update gives a wider range of 5 GHz channels to choose from - not only UNII-1 (5.170-5.250 GHz) and UNII-3 (5.725-5.835 GHz), but also UNII-2 (5.250-5.350 GHz and 5.470-5.725 GHz). To use UNII-2, you need to update your product to the latest software version (at least 6.48.4).


ZeroTier added to RouterOS v7

We are happy to announce ZeroTier support for ARM and ARM64 architectures with enough space. You can check out ZeroTier documentation [here](#).

ZeroTier combines the capabilities of VPN and SD-WAN. It provides advanced network virtualization and management capabilities. Basically, you can have all the benefits of a personal cloud without complicated configuration, setting up a domain name, or having a public IP.

For example, install the iPhone ZeroTier client and join your home LAN without a hitch. But that's not all. ZeroTier allows your devices to communicate directly, despite the different environments. Since communication is not going through one specific server, as in the case of VPN, you won't be losing too much speed. Any two devices in the world should be able to locate each other and communicate through the most optimal path, almost instantly. With almost zero configuration. Obviously, this communication is end-to-end encrypted – don't you worry!

ZeroTier emulates a true Ethernet switch. You can have L2 bridges with other Ethernet networks – wired, wireless, even virtual. The best part? This open-source service offers enterprise-level subscriptions, as well as several free plans for home labs, remote access, tunneling, and so on.



```
[normis@Home] /zerotier/interface> add network=XXXXXX instance=1  
[normis@Home] /zerotier>enable zt1
```

Info on the MĒRIS botnet



In early September 2021, QRATOR labs published an article about a new wave of DDoS attacks, which are originating from a botnet involving MikroTik devices.

As far as we have seen, these attacks use the same routers that were compromised in 2018, when MikroTik RouterOS had a vulnerability, that was quickly patched.

There is no new vulnerability in RouterOS and there is no malware hiding inside the RouterOS filesystem even on the affected devices. The attacker is reconfiguring RouterOS devices for remote access, using commands and features of RouterOS itself.

Unfortunately, closing the old vulnerability does not immediately protect these routers. If somebody got your password in 2018, just an upgrade will not help. You must also change the password, re-check your firewall if it does not allow remote access to unknown parties, and look for scripts that you did not create.

We have tried to reach all users of RouterOS about this, but many of them have never been in contact with MikroTik and are not actively monitoring their devices. We are working on other solutions too.

There are no new vulnerabilities in these devices. RouterOS has been recently independently audited by several third parties.

Best course of action:

- Keep your MikroTik device up to date with regular upgrades.
- Do not open access to your device from the Internet to everyone, if you need remote access, only open a secure VPN service, like IPsec.
- Use a strong password and even if you do, change it now!
- Don't assume your local network can be trusted. Malware can attempt to connect to your router if you have a weak password or no password.
- Inspect your RouterOS configuration for unknown settings (see below).

In collaboration with independent security researchers, we have found malware that attempts to reconfigure your MikroTik device from a Windows computer inside your network. This is why it's important to set a better password now (to avoid passwordless login or a dictionary attack by this malware) and to keep your MikroTik router upgraded (since this malware also attempts to exploit the mentioned CVE-2018-14847 vulnerability which has long been fixed).

Configuration to look out for and remove:

- System -> Scheduler rules that execute a Fetch script. Remove these.
- IP -> SOCKS proxy. If you don't use this feature or don't know what it does, it must be disabled.
- L2TP client named "lvpn" or any L2TP client that you don't recognize.
- Input firewall rule that allows access for port 5678.

You can also work with your ISPs to block the following addresses, which these malicious scripts are connecting to:

Block these tunnel endpoint domains:

- **.eeongous.com* **.leapproach.info* **.mythtime.xyz*

Block these script download domains:

- | | | |
|--------------------------|-------------------------|-------------------------|
| • <i>1abcnews.xyz</i> | <i>hitsmoby.com</i> | <i>specialword.xyz</i> |
| <i>1awesome.net</i> | <i>massgames.space</i> | <i>spgames.site</i> |
| <i>7standby.com</i> | <i>mobstore.xyz</i> | <i>strtbiz.site</i> |
| <i>audiomain.website</i> | <i>motinkon.com</i> | <i>takebad1.com</i> |
| <i>bestony.club</i> | <i>my1story.xyz</i> | <i>tryphptoday.com</i> |
| <i>ciskotik.com</i> | <i>myfrance.xyz</i> | <i>wchampmuse.pw</i> |
| <i>cloudsond.me</i> | <i>phonemus.net</i> | <i>weirdgames.info</i> |
| <i>dartspeak.xyz</i> | <i>portgame.website</i> | <i>widechanges.best</i> |
| <i>fanmusic.xyz</i> | <i>senourth.com</i> | <i>zancetom.com</i> |
| <i>gamedate.xyz</i> | <i>sitestory.xyz</i> | |
| <i>globalmoby.xyz</i> | <i>spacewb.tech</i> | |

As reported by others on the Internet, these domains are also used by the botnet:

- | | | |
|-----------------------|---------------------|---------------------|
| • <i>bestmade.xyz</i> | <i>mobigifs.xyz</i> | <i>onlinegt.xyz</i> |
| <i>gamesone.xyz</i> | <i>myphotos.xyz</i> | <i>picsgifs.xyz</i> |

Diving deep into RouterOS: Switching

Dive deep into the world of hardware offloading with Kaspars and Edgars!

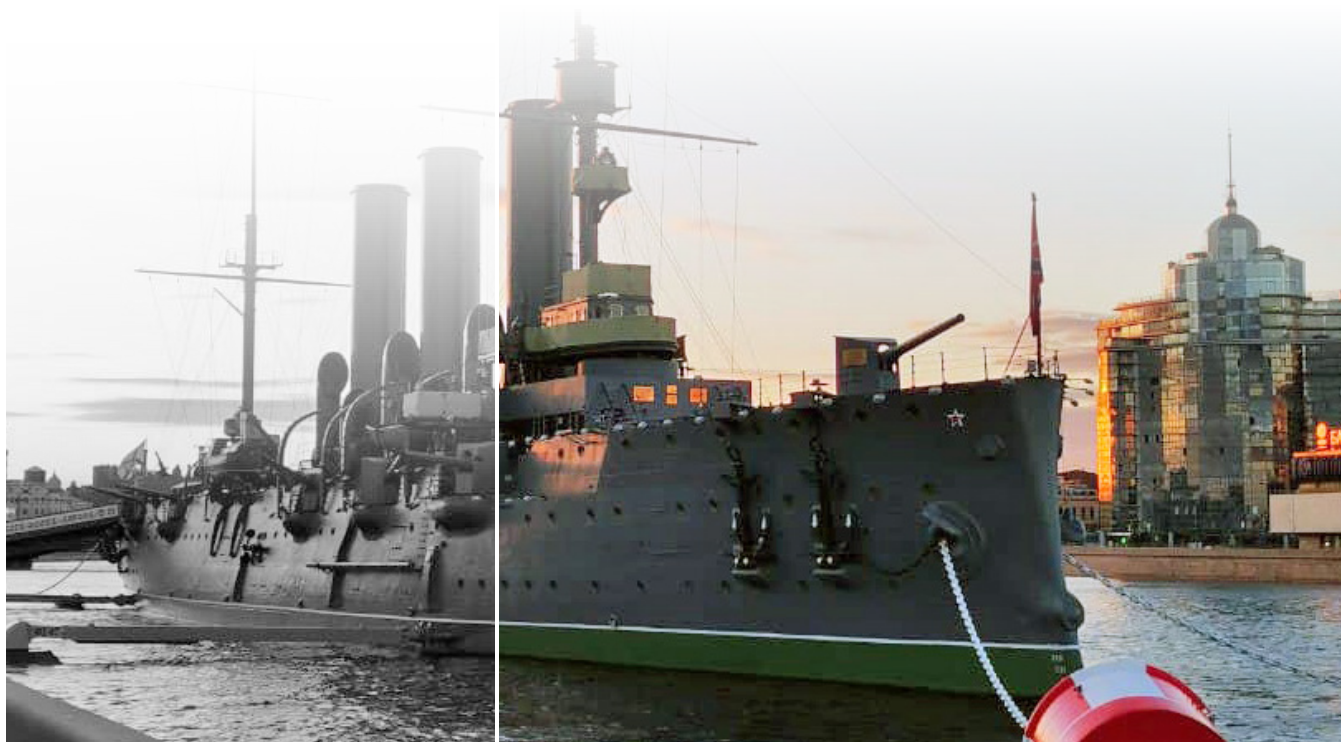
“Does the traffic going between multiple switch chips must go through CPU?”

“Bridge port PVID vs Bridge VLAN untagged port”

"Can I configure the switch using python script?" ...and many more questions answered.



Bridging two centuries with MikroTik

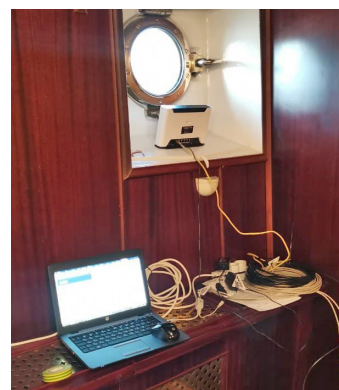


Since its construction in 1900, the famous Russian cruiser “Aurora” has managed to survive the Battle of Tsushima, launch the October Revolution, take part in the Second World War, and finally retire. While this ship is said to still be fully operational, it doesn’t really leave the port. Instead, this famous ship has become a popular tourist attraction in Saint Petersburg.

Being both a museum and a venue for all kinds of events, including the Petersburg International Economic Forum, “Aurora” needed a little update in the communications department. And we’re not talking fathometers and sonars here, arrrrgh!

Our friends at “Интернет Системы” took a powerful RBM33G, a couple of capable R11e-LTE6 modems, put them inside a custom enclosure with some antennas and – voilà! 21st century meets the 20th century!

An elegant Chateau LTE12 with no additional installation costs makes a fine addition to the deck, handling not only the wireless network but also the L2VPN connection.



» Here you can download all the visuals used in this newsletter «