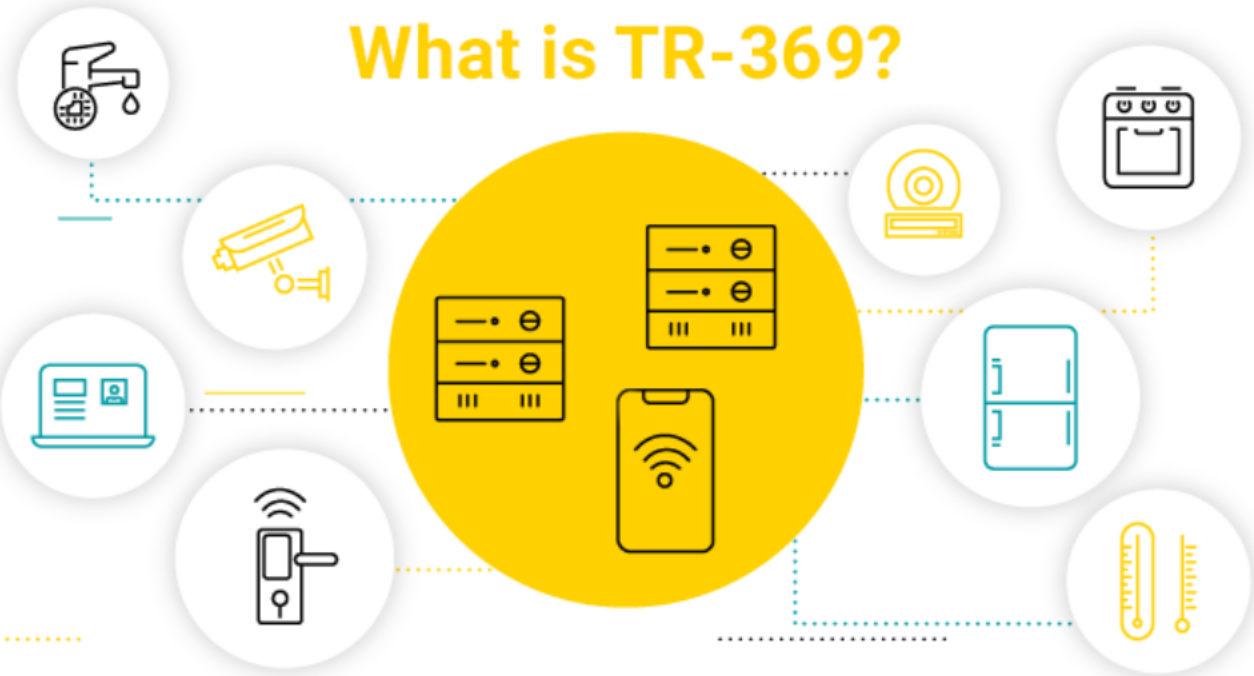
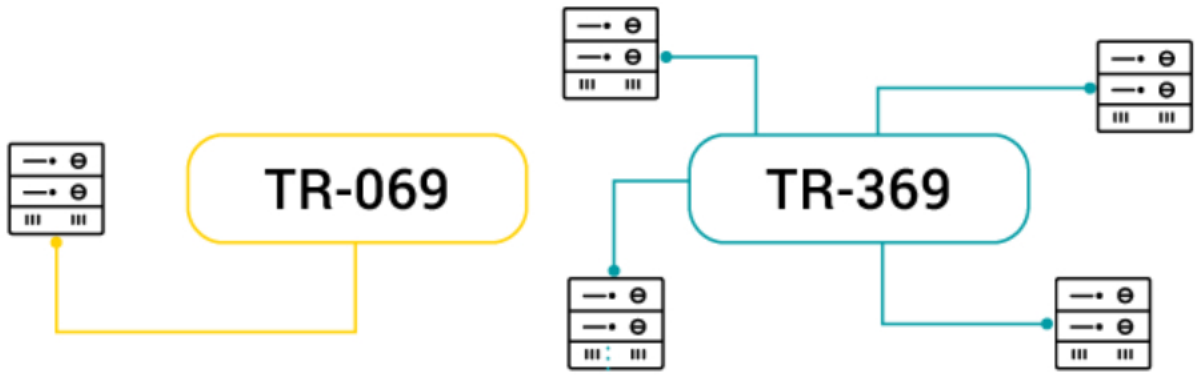
What is TR-369? An overview of the TR-369 protocol



TR-369, otherwise known as User Services Platform (USP), is a technical standard that describes the application layer protocol and data model for remote management of connected consumer and enterprise devices by both providers and end users alike. Easy, right? Well, easier said than done – coming up with a solution that not only responds to the current needs of the industry, but also fits well in a brownfield environment is one hefty task.

In the beginning, there was TR-069

It is impossible to discuss the TR-369 protocol without first mentioning its predecessor: TR-069. When Broadband Forum came up with **CPE WAN Management Protocol (CWMP), also called TR-069 after the name of its technical specification, it was the perfect solution for remote management of modems, routers, or gateways**. The thing is, the year was 2004, so it's very likely you only had one PC at home, you couldn't stream movies on Netflix, and your fridge surely didn't give you an advanced notice that you're about to run out of kale. All this is to say, a bidirectional connection between the CPE and the autoconfiguration server (ACS) that characterizes TR-069 seemed like a reasonable solution at the time. Fast forward 15 years to a whole world of connected devices and it may turn out that CWMP is no longer enough when you're deploying services that allow multiple end users to manage the eternally spawning devices on their own.

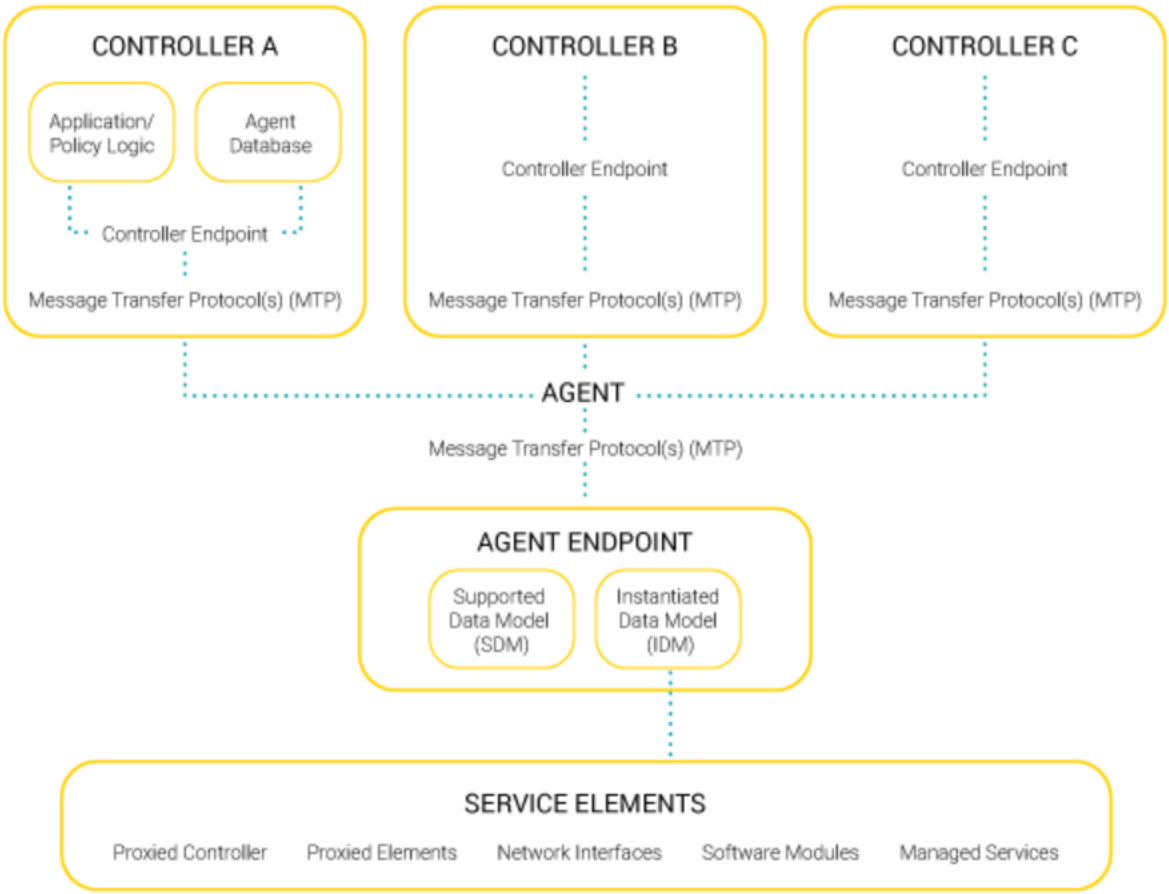


So what has changed with TR-369?

In 2018 it was clearly time for a re-do. Considering the success of CWMP, it wasn't much surprising that Broadband Forum would use it as a framework when building TR-369, which is why it's sometimes referred to as "next-gen TR-069" or "TR-069 for IoT devices". Indeed, the idea was to create **a protocol that would enable lifecycle management of smart and IoT devices while also ensuring interoperability between providers**. But the creators of TR-369 protocol didn't stop at that. Clearly, the strength of smart appliances lies in them being accessible to and manageable by end users, which factored heavily in the development process. But the protocol offers incredible value for service providers as well. Many consider the ability to implement managed WiFi services, i.e. outsourced WiFi network management, in their business offer as one of the main benefits of switching to TR-369.

Design overhaul

The principal difference between the two protocols is that **instead of clients that communicate with auto configuration servers, you now have agents and controllers**. It may seem like a gimmicky change in nomenclature, but in fact agents and controllers operate on a different principle. **Whereas with CWMP there is only one ACS per client, with TR-369 protocol multiple controllers with different permission settings can be subscribed to an agent.** This opens a new door for multiple providers, vendors and even end users to interact with the devices. With such flexibility, both application and network service providers can manage their respective services for the same devices at the same time, which fosters provider partnerships.



Protocol polyglot

Unlike its predecessor, **TR-369 supports multiple message transport protocols (MTPs)**, not just HTTP. These include Websockets, Constrained Application Protocol (CoAP), Simple Text-Oriented Messaging Protocol (STOMP) and Message Queuing Telemetry Transport (MQTT).

Always listening in open sessions

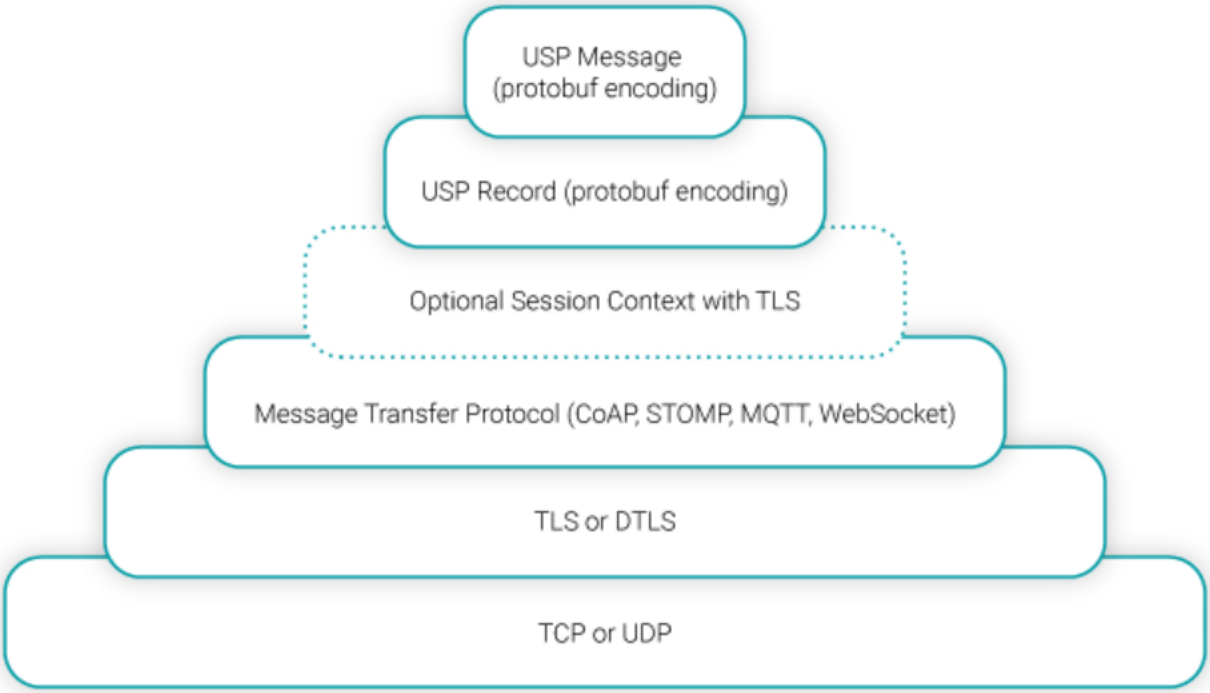
Whereas with CWMP the connection between the client and the ACS is always initiated by the client for a specific purpose and optimized to be as short as possible, **TR-369 is designed for an always-on, direct communication**. Once the connection is established at the start-up, Websockets or STOMP sessions are open indefinitely and the controllers can freely send messages to agents.

Light as a feather

This need to be responsive requires TR-369 to be lightweight in return. **The amount of overhead was indeed significantly reduced compared to its precursor.** For instance, the open sessions mentioned above removed the need for repeated connection requests that generated a lot of unnecessary handshaking. Improvements like this are particularly important for IoT deployments that rely on low data consumption, however they cannot be underestimated by telecoms either. Operators previously had to balance the gains of frequent device monitoring with the impact it had on the network. **Because TR-369 protocol is so efficient, it allows for more frequent and precise monitoring of the device, effectively ensuring better quality of service for the customer.**

Buff(ered) up with protobufs

The application layer in TR-369 is wrapped in a protocol buffer before it’s encapsulated in any MTP. **Protobufs, as they are called for short, are somewhat like XML, however they are not human-readable after encoding and need a schema (a .proto file) to be decoded.** The existence of schemas makes it easier to apply data structure.



Security features solid as a rock

TR-369 also offers state of the art security.**USP message is wrapped in a USP record which can be encrypted with TLS. The message can also be secured in the MTP layer:** for Websockets with HTTPS, for CoAP – DTLS, and for STOMP – with TLS. Additionally, **the end-to-end (E2E) message exchange feature makes it possible to establish a session context which ensures integrity, protection and segmentation of data** if the message is too large for transfer.

Structured with data model

TR-369 protocol relies heavily on data modelling, in particular on slightly modified **Device:2 Root (TR-181) data model**, version 1 of which was applied to TR-069. Broadband Forum's TR-181 specification defines it as **a set of data objects**, such as "basic device information, time-of-day configuration, network interface and protocol stack configuration, routing and bridging management, throughput statistics, and diagnostic tests." Since network interfaces and protocols are considered objects, they can be freely stacked to match the device configuration.

Do you really need TR-369?

TR-369 was designed to fill a niche that emerged as the landscape of smart devices began to shift rapidly. However, the protocol was not meant to always replace its ancestor, as there are still use cases where it is more than enough for a deployment, especially if there is already an existing compatible architecture in place. Despite everything, **TR-069 still remains a go-to standard with a proven track record of many success stories.** If you are ready to take the next step, though, you should be mindful that your auto configuration server – whether it's in the cloud or on-prem – can support both these protocols simultaneously.**After all, you will probably not be upgrading your whole fleet all in one go and it's entirely possible that there are some devices you will not want upgraded at all.**This is why it's important for your device management platform to be able to handle both TR-069 and TR-369, so that they can coexist in your deployment.

There certainly is a case to be made for **an up-and-coming standard developed in tandem with industry experts by a well-established standards body, such as the Broadband Forum**. Be mindful, though, that there are plenty of solutions on the market to consider. And many come with similar credentials, such as for example LwM2M – a standard also developed in response to the needs of the growing IoT world. As always, there is no clear answer to the question which standard is the best. You can only ask: which is the best for your deployment?