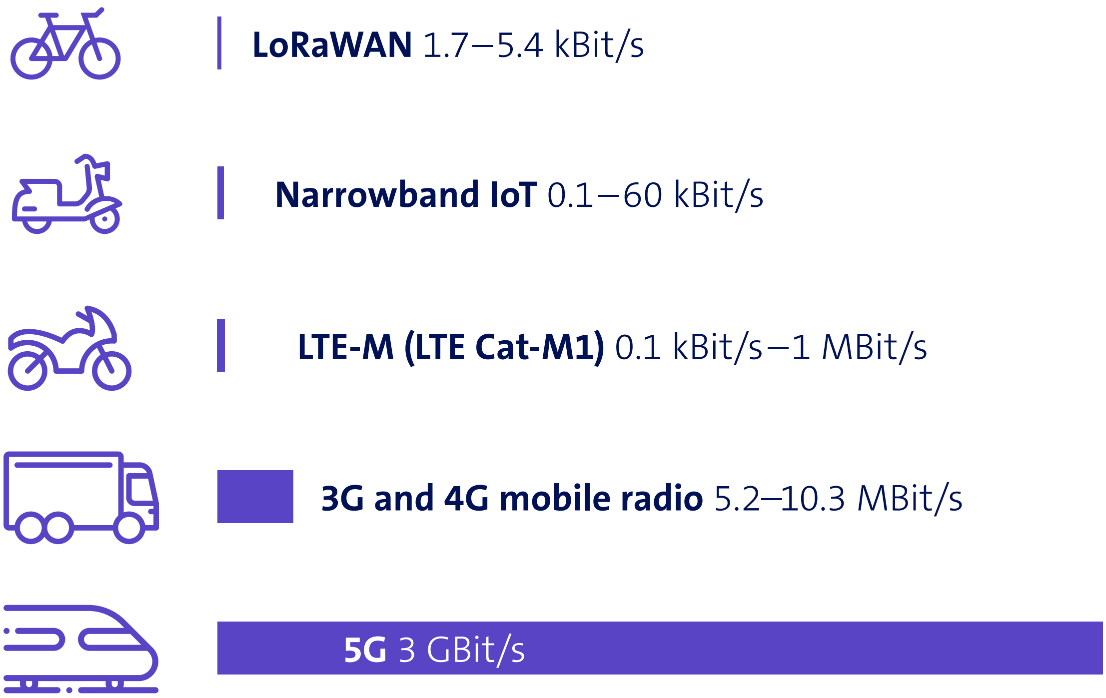
IoT access technologies
How things get on the Internet

Since 2020, the Internet of Things includes 30 billion devices. All of these devices must be connected to the Internet and the associated applications. This can be done using various access technologies: While M2M communication was initially transmitted via the 2G network, which will soon be obsolete, IoT users can now choose the most suitable access technology from a wide range of options. This white paper highlights the characteristics of key technologies and indicates which technology is right for which application.



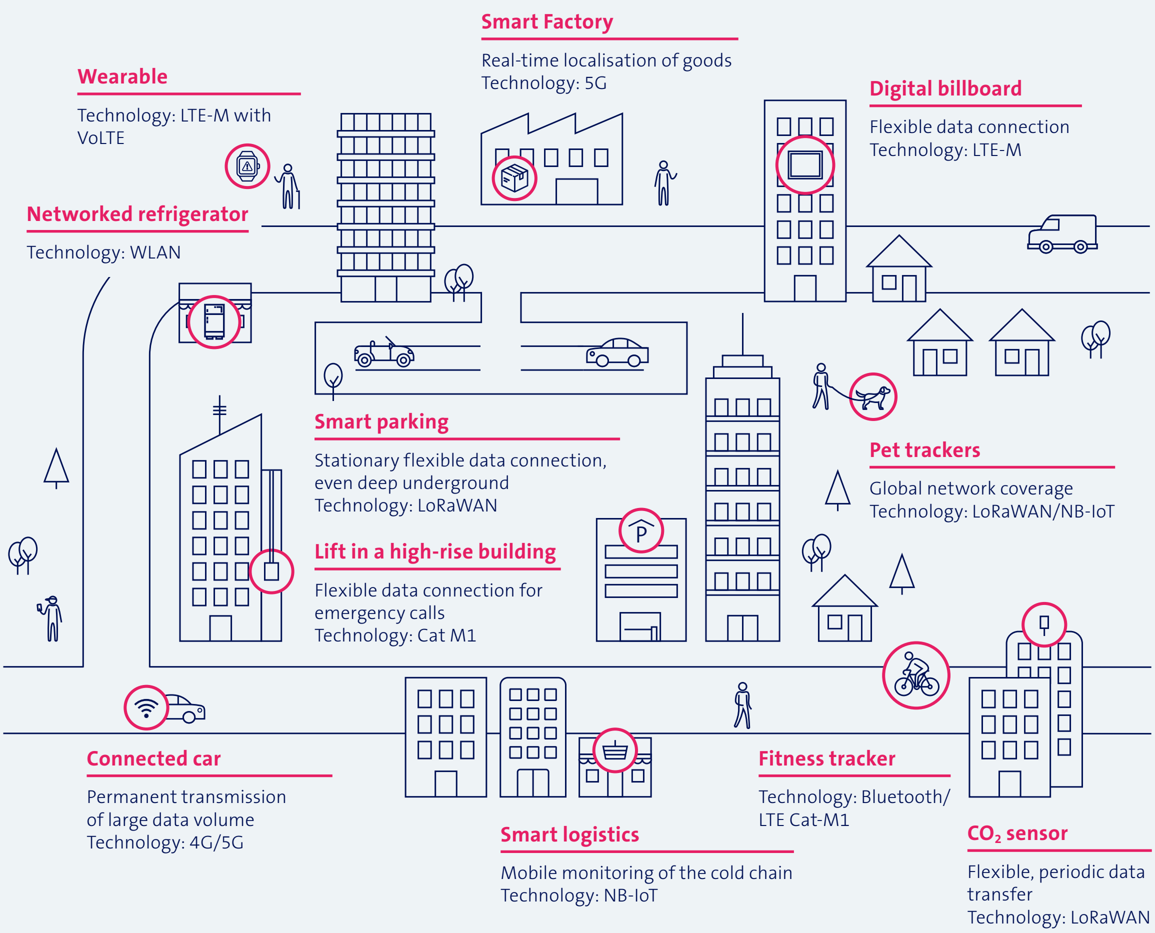
swisscom

Billions of devices are already connected in the Internet of Things (IoT). According to market researchers, this number will continue to rise massively; depending on the forecast, there could be up to 30 billion (according to MIT) or even 50 billion (according to Cisco) connected devices.

These include conventional devices connected to the Internet, from PCs to smartphones, as well as the actual IoT "things" such as sensors, trackers, building automation devices and public infrastructure elements. According to the IoT Analytics forecast, equal numbers of IoT and non-IoT devices (smartphones, tablets, laptops) will be in operation for the first time in 2021.

All these devices require a connection to the applications they serve, either over the public Internet, a private network or virtual-private network (VPN). Various access technologies are available for this purpose, from good old WiFi to the upcoming 5G mobile radio standard.

The variety of IoT applications: A technological mix for success



Requirements for IoT access technologies

When it comes to the Internet of Things, there are those who speak of a "profusion of access technologies". We're spoilt for choice. This brings a whole series of questions into play:

- What kind of devices should be networked?
- How many devices should be networked?
- Are the devices mobile or fixed – and how are they geographically distributed?
- Which distance needs to be bridged?
- Which data volume will be transported?
- Which bandwidth is required?
- How time-critical is the transmission?
- Should voice be transmitted in addition to data?
- In the case of battery-powered devices, how long should the power source last?
- What are the costs?
- Is it a personal or a non-personal device?
- Does the device have to work worldwide or regionally?
- Where is the device used – in the basement, outdoors, etc.?

Although some of these aspects sound technical, they are actually questions related to business. Ultimately, the point is to find out which IoT connection promises the best results at the lowest possible cost for the respective application.

Autonomous cars, for example, permanently transmit telemetry data, receive large data volumes for entertainment systems and are dependent on feedback. In contrast, when the temperature of production machines is monitored, it may be sufficient for a sensor to transmit the temperature measurement every fifteen minutes.

Another aspect in addition to the transfer technology itself is the level of security and privacy offered by the transmission network:

- If devices are networked via public Internet, they themselves must be designed for security right from the start – for example, with encryption integrated into the hardware.
- By encapsulating the data stream, for example via IPsec (Internet Protocol Security) tunnels or MPLS (Multiprotocol Label Switching), virtual private networks enable a secure connection in a shared infrastructure with logical domains – in most cases, this is sufficient.
- Dedicated point-to-point connections are suitable for particularly sensitive, time-critical and high-performance applications. This results in a completely self-contained network that requires no shared infrastructure. One example might be a nuclear power plant which, by its very nature, must operate in isolation from all public grids. And in industrial applications, high transmission performance and minimum latency times in the microsecond range are often important; a private network also makes sense in this case.

The most important wireless access technologies at a glance

Common IoT access technologies can be categorised in various ways. One aspect is their range. Short-range technologies such as Bluetooth, WiFi and Zigbee are designed for distances ranging from a few metres to 30 metres. Wide-range technologies can be further divided into two subcategories: NarrowBand IoT and LoRaWAN offer a small bandwidth but bridge distances of up to 35 kilometres and more. High bandwidths and distances of several hundred metres to several kilometres are available with 4G mobile radio in the form of LTE and LTE-M.

Further categorisation can be made according to frequency use. Bluetooth, WiFi, LoRaWAN, Zigbee and SigFox work in license-free, unregulated spectra. All technologies from 2G to LTE-M to 5G based on mobile radio use licensed, strictly regulated frequency bands and protocols standardised by the 3GPP mobile broadband standardisation organisation.

Comparison of IoT access technologies

Technology	Bluetooth	WiFi	LoRaWAN	NB-IOT (NB-IoT Cat 1)	LTE-M (LTE Cat M1)	4G (LTE Cat 1)
Spectrum	unlicensed	unlicensed	unlicensed	licensed	licensed	licensed
Bitrate	20 MBit/s	up to 1.73 GBit/s	DL 1.7–5.4 kBit/s UL 0.3–5.4 kBit/s	DL 0.4–30kBit/s UL 0.1–60kBit/s	DL & UL 0.1 kBit/s to 1 MBit/s	DL 10.3 MBit/s UL 5.2 MBit/s
Latency	not specified	2 to 4 ms	1 to 10 s	1.4 to 10 s	10 to 200 ms	10 to 100 ms
Pop. coverage outdoors	–	–	97.2 %	99.9 %[1]	99.9 %[1]	99.5%
Module costs	•	•	•	••	••	•••
Voice support	–	–	no	no	yes	yes
Battery life	–	–	≤ 10 years	< 10 years	< 5 to 10 years	several days

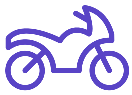
[1] In urban areas and outdoors, the technologies are comparable. NB-IoT has comparatively better coverage in buildings and locations which are far away from transmission masts.

Which technology for which purpose?

The **short-range wireless technologies** WiFi, Bluetooth and Zigbee are established in IoT, particularly for connecting smart home devices, fitness trackers, smart TVs and other devices in private households. The devices communicate with a home network's WLAN router using WiFi. The connections to the Internet and the manufacturer's applications are made via the domicile's Internet connection: Usually DSL, cable or optical fibre.

LoRaWAN offers only low bandwidth and low data throughput. However, the coverage is first class: Swisscom operates a Switzerland-wide LoRaWAN network that can be used at low cost. The LoRaWAN standard is defined and promoted by the open LoRa Alliance. Its penetration in buildings is also excellent; it is ideal for permanently installed sensor and measurement devices such as water meters, smart meters or heating thermostats, which transmit little data at comparatively long intervals and rarely receive feedback from the application. LoRa radio modules are also very cost-efficient. If LoRaWAN were a means of transport, it could be described as a cost-efficient, nimble bicycle for sporty cyclists.

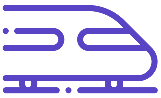
If LoRaWAN were a bicycle, then **NarrowBand-IoT** would be a moped. In contrast to LoRa, NB-IoT operates in a part of the mobile radio spectrum that is subject to licensing; in Swisscom›s case, this is the 800 MHz band. The protocol is globally standardised: If a provider offers NB-IoT somewhere on earth, it must adhere to the standard. This means that NB-IoT-capable devices can theoretically function worldwide. The prerequisites for this are a valid SIM card and technically functioning roaming (will be possible in the near future). NB-IoT is comparable to LoRa in terms of data throughput and latency. NB-IoT is therefore suitable wherever LoRaWAN is an option, as well as for applications that need to function globally. One example would be a suitcases containing a NB-IoT module, which – provided the local mobile phone provider offers NB-IoT – would allow baggage to be located anywhere in the world.



LTE-M is the sound-system-equipped motorbike of access technologies and supports telephony as well as data transmission (LTE Cat-M1). It sets higher standards: The data throughput is up to 1 Mbit/s, and voice transmission is guaranteed to be good quality with features such as Quality of Service (QoS). In contrast to NB-IoT, LTE-M also supports full mobility with mobile radio cell handover. This makes the technology ideally suited to applications in the automotive, transport and logistics sectors such as vehicle location, goods localisa tion, fleet management and telematics. Or where voice is required, for example, in the emergency telephone of a lift. Overall, LTE-M is more complex and not quite as cost-efficient as LoRaWAN and NB-IoT, but offers significantly more possibilities.

The Volte functionality when enabled allows the addition of voice which is beneficial for the wearable segment.

The classic **3G and 4G mobile radio** standards are the 12-tonne and 40-tonne juggernauts in our analogy; they are used when large data volumes have to be transmitted quickly. For example, in autonomous vehicles, for traffic monitoring and control, for health monitoring and for remote-controlled operations in telemedicine, for controlling robots and drones, for train controls and in aviation.



If 3G and 4G are the juggernauts, **5G** is the high-speed train: Both offer extremely high speeds, both are regulated down to the last detail. The 5G network will establish itself as the technology of choice for demanding mobile IoT applications. One example is in industrial applications: Today, production plants are constantly being converted for new products, meaning that machines need to be moved to different positions. The effort of laying new cables each time would be too great. Instead, the machines are networked wirelessly. However, production control relies on fast data throughput and the shortest latencies – and this precisely where 5G comes in. Another area of application is public safety: Police forces are increasingly being equipped with bodycams, heads-up displays in vehicles and tablets. Here, too, enormous data volumes are generated, and the mobility requirements are high.

What about 2G?

Many IoT and M2M applications are still based on **2G mobile radio,** which was introduced over 20 years ago. Especially in Asia and Africa, 2G applications are widespread due to the very low prices for the radio module. To a certain extent, 2G technology was the initial spark for IoT-based solutions. However, with the declining availability of 2G and the emergence of new access technologies, enterprises have new, expanded possibilities and significantly greater flexibility than before, and they can utilise the very technology that best suits their needs. New IoT applications should therefore be implemented from the outset using one of the current technologies. In Switzerland, the 2G network will be deactivated in 2020. It is therefore time to bid farewell to 2G and migrate existing applications to the new NB-IoT or LTE-M alternatives.

“The expanded technology mix provides enough alternatives to 2G for IoT and M2M applications.”

Which technology for which purpose?

Time-critical IoT

Requirements

Low time lag
Extreme reliability
High availability
High security
Flexible data rates
Rather small number of devices

Areas of application

Road safety
Industrial production
Self-driving cars
Public safety
Health
Train control
Aviation
Emergency device wearable
Elderly care

We recommend

LTE-M

4G/LTE

5G

Massive IoT

Requirements

Low costs
Low energy consumption
Small data volumes
Wide ranges
Mobility
High latency tolerance
Large number of devices

Areas of application

Farming
Energy supply
Transport and logistics
Industry 4.0
Smart city
Smart buildings

We recommend

LoRaWAN

NB-IoT

LTE-M

Act now!

Take the first step now and talk to our IoT experts.

Meet the Expert
Our IoT experts will be happy to answer your questions and look forward to hearing from you.

More information about the Internet of Things.

Click here for our fact sheet on low-power wide-area access technologies.