Frequently Asked Questions

General

What is The Things Network and how is it different from LoRaWAN and LoRa?

The Things Network (TTN) is a free data network for the Internet of Things. LoRa is an innovative way of using unlicensed radio spectrum to transmit small amounts of data, at long range with minimal power. The Things Network uses a standardized protocol called LoRaWAN which uses LoRa technology to connect many devices to the Internet.

What is the difference between a node and a gateway?

Nodes are usually small, battery-powered sensors that upload their data to the Internet via The Things Network. Gateways are strategically-placed access points that provide coverage for The Things Network.

What is the difference between network operators, application providers, and application users?

Network operators are the many community members (both corporate and individual) who own and operate the infrastructure behind The Things Network. Application providers provide services based on data and analytics from nodes they control. The application users benefit from the data from applications.

Does The Things Network New York provide a Service Level Agreement (SLA)?

No, but application providers may.

Let's take an example. Suppose a company called "TrashAware" provides a garbage can monitoring service to U.S. cities. The city of "Smallville" is interested in TrashAware's product but requires an SLA stipulating 99.9% uptime. TrashAware assesses the current network coverage in Smallville, and then partners with the city to deploy additional gateways to ensure complete coverage and reliable service. TrashAware then issues an SLA to Smallville covering their entire application, which includes availability of data via their website and a mobile application.

Security and Privacy

As a gateway operator, does installing the gateway make my own network vulnerable?

Technically yes, but the security risk is less than a smartphone connecting to your network's WiFi.

A gateway *does* technically represent an additional access point into a LAN and should not be placed inside of a trusted zone, however it is an order of magnitude less risk than a smartphone or employee PC. The gateways use industry-standard access control and are secured with administrative credentials setup during installation. While vulnerabilities via the packet forwarding protocol or the LoRa interface are conceivable, they are highly unlikely in practice. A LAN operator can mitigate the risk of compromised gateways on their network by placing them in a separate segment (VLAN), as is routinely done in corporate networks.

As an application provider or user, is my data private?

Data is encrypted from the node to the application: The Things Network does not have access to the decrypted data.

It is the application provider's responsibility to ensure that their nodes are designed to adequately protect data prior to transmission. LoRaWAN has AES128 encryption by default, which should be sufficient for most uses, and additional encryption and security measures can be applied for applications which require them.

The greatest threat to privacy is not in The Things Network itself, but rather in the third-party applications where the data is stored. TTN has no control over the security of data after it has been sent to and decrypted by applications. A bad actor could theoretically break into the application server and steal/delete/manipulate data or send control commands to IoT devices. Thus, application providers must take security precautions to ensure users can trust them with their data. This is a challenge for IoT in general and not specific to TTN.

At the end of the day, if you are using any wireless tech whatsoever, you are transmitting in spectrum that is easily monitored by the public, so you must secure the data at the transmitter and not trust the network like we could(?) with landline telephone. That said, of course we should encourage good security/privacy practices throughout the network.

As an operator of a gateway, am I responsible for user's privacy?

No. The gateways simply listen for radio signals from nodes and pass encrypted data to the network. Gateways do not contain decryption keys or any privileged information about users.