stacuity

How can you select and control edge locations for mobile IoT data?

The launch of stacuity's new Software-Defined Distributed Edge Network revolutionises connectivity for IoT and enterprise customers and provides granular control over how their data is routed globally.

Today's breakout solutions don't offer the granular control over how and where remote IoT application traffic is routed. Routing this valuable data to the home network introduces delays, exposes traffic to security threats – and cannot be directly controlled by IoT service providers.

The challenge for optimising remote IoT application routing and performance

What's needed is a way to control traffic at a granular level before it reaches the public internet and IPX network. Applying policies at the edge protects traffic, enables optimised routing and control – and lets IoT service providers deliver better performance to their customers. How?

Find out how can you take control, optimise traffic and – and bring new connectivity tools like SD-WAN to the mobile edge? Find out how to take full control over breakout and routing, with policy-based conditions to enhance security for valuable data traffic – and benefit from distributed private edge routing for your IoT services.

What is the Distributed Edge Network, and what does it do?

Data from mobile devices – such as IoT sensors and enterprise assets – often takes a long and convoluted path to get to its destination. This affects speed, reliability, and security - and brings increasingly regulatory challenges in terms of data sovereignty and local regulations.

With our Distributed Edge Network, we have deployed PGWs (Packet Gateways) and our Smart Packet Steering platforms around the world to allow our customers to control the path that this data takes – improving performance, reliability, and security – in many cases avoiding the Internet entirely.

How does it work?

> "Using our Edge Network, data can be routed from the device, directly from the closest hub on the IPX network and on to the cloud application - without touching the public Internet."

IPX transport adds latency and reduces efficiency

The world's mobile operators are connected to a vast global network called IPX – which is a 'private internet' separate from the Internet we all use day-to-day. When mobile devices are in different regions, and particularly when they are roaming, this IPX network is used to transport the data back to the home network from where it is forwarded to its destination.

This home network can be geographically distanced from the device itself – and from the data's destination. This introduces unnecessary 'data miles' making the whole end-to-end process complex and inefficient.

In building our Distributed Edge Network, we have created edge hubs at strategic points on the IPX worldwide – removing the need to bring the data back to a single, central point.

This removes the inefficiency and brings significantly improved performance and a host of other benefits.

How does it improve security?

When it comes to security, the weakest link is almost always the public Internet. The Internet was designed to allow anything to communicate with anything – which is perfect for applications such as the web.

For most IoT-style devices and applications, this is far from ideal – communication is only required between the device and a limited number of systems which might be in public cloud.

Using our Edge Network, data can be routed from the device, directly from the closest hub on the IPX network and on to the cloud application - without touching the public Internet. The devices can only access services intended – and the devices are out of reach of malicious actors on the Internet. This hugely improves both security, performance, and operational resilience from within the network itself – particularly important when the devices themselves might be reasonably unsophisticated, inaccessible and difficult to manage.

How can mobile providers take advantage of it?

Through the existing stacuity distributed core network, our customers already have powerful control over their fleet of devices and connected systems. With the launch of the Distributed Edge Network, they can now also define policies appropriate to each use case to control which IPX hubs are used for which devices in which country.

This is step beyond typical 'local breakout' services where the customer is not in control. Customers have full control and visibility – either via our portal or API.

> "In building our Distributed Edge Network, we have created edge hubs at strategic points on the IPX worldwide – removing the need to bring the data back to a single, central point."

What use cases can benefit?

Any use cases where security, performance or reliability are important can benefit from the optimisation of the traffic path – so that covers most IoT and enterprise applications. However, for certain types of application it is particularly advantageous:

> 1. Where performance is important – for example, streaming applications such as security cameras benefit from low and predictable latency.

> 2. Where regulatory requirements dictate that the data must remain with a particular region or country – such as payment terminals or connected health.

> 3. Where secure, controlled connectivity is required into a small number of central systems – either hosted, or in public cloud.

> 4. Where devices do not have sophisticated security capabilities of their own - or are difficult to configure or control due to their location.

Where is it available?

The Distributed Edge Network is now available – and expands the global reach of our unique software-defined mobile platform.

Our initial Edge Network hubs are at the main global IPX peering locations – Ashburn Virginia (for the Americas), Amsterdam (for Europe) and Singapore (for Asia). These sites are where mobile operators already come together to exchange their traffic – so are ideal points for us to connect.

The next stage of our expansion is in progress. It will cover South and Central America, and Africa. We can move fast, because launching new sites is a straightforward process for our network team, so we can expand our service wherever there is a need. While we have a defined roadmap for stacuity's global locations, we also offer a cost-effective solution to meet bespoke location requirements and dedicated instance, where required.

Transforming IoT connectivity

stacuity has been designed and built to enhance digital transformation in the IoT connectivity space. Features such as self-provision of defined data routing policies; recognised as minimum requirements to enhance security and control in traditional SD-WAN networking, can now be leveraged in the mobile connectivity domain utilising stacuity.

stacuity offers a step-change in how IoT and enterprise customers can control how their data is routed globally. This allows customers to meet the varied and growing demands placed on connectivity – such as reduced latency, increased security, reliability, and self-service control.

To speak to a member of the stacuity Sales Team and learn more about our solutions please contact sales@stacuity.com

"Our initial Edge Network hubs are at the main global IPX peering locations – Ashburn Virginia (for the Americas), Amsterdam (for Europe) and Singapore (for Asia). These sites are where mobile operators already come together to exchange their traffic – so are ideal points for us to connect."

Silverdale,
Silverdale Road,
Ballasalla
Isle of Man,
IM9 3DS

Stacuity.com