White Paper

Transformation to a Next Generation IoT Service Provider

Executive Summary

Over the past 5 years, the IoT sector demonstrated high growth for communications service providers (SPs) yielding 20-50% annual increases in device connections and increased new revenue clarity[1]. As the IoT grows, SPs find requirements extend well beyond connectivity to security, privacy, applications, analytics, cloud and managed services, as well as big data management.

To meet the opportunity, SPs are realigning service strategy and operations. The most progressive SPs have executed multiple IoT planning cycles which illustrate the priority and broad scope of future IoT services profitability. In these cycles they have prioritized opportunities, ran multiple customer trials, and built capabilities and capacity to scale. In our companion white paper, *How Service Providers Can Help Businesses to Realize the Promise of the IoT Revolution*, we articulate why SPs are getting into IoT. The SP 'right to play' is derived from scale and scope economies their platforms are able to provide in a secure and highly reliable manner. Additionally some SPs will create differentiated products on those platforms. Success herein has delivered a position of high trust in such a role with customers. The gap, opportunity and challenge is in extending integration capabilities to software and data management.

[1] MachNation, Inc., 2015.

In this whitepaper we will explore the strategy, technology and GTM decisions which SPs need to take as they transform to a next-generation IoT Service Provider.

- SPs should:
  - develop scalable platform driven value-added service competencies (either internally or externally) to become a provider of services at a business level capable of delivering high velocity, high value insights from data
  - select/build an IoT enabled cloud platform for managed service offerings
  - define a partnership eco-system and embrace developer communities
  - decide when to partner, purchase or produce services for ongoing technology evolution
  - challenge legacy organizational structures and culture when deciding on accountability for products, security, privacy, apps, analytics and underlying big data capabilities
  - rapidly iterate on 'data as a service' interoperability and business models
  - leverage their supplier relationships to deliver on a joint go to market, especially in cases where the supplier and the SP have common customers
  - leverage their customers' development teams to develop key applications for use cases that can be consumed by other similar businesses

Introduction

SPs are concerned about decreasing ARPU in connectivity businesses but are taking different approaches to addressing the IoT market. Generally one of two strategic approaches to the enterprise IoT sector appeals to most SPs. Many extend legacy service portfolio capabilities in search of low hanging fruit in favorite verticals. Common verticals include: manufacturing, transportation (biggest) and retail. Others include automotive (connected car), energy, and financial services. Some SPs develop new platform eco-systems that promise exponential growth by capturing SaaS revenues.

Some leading analysts contend that SPs will struggle to earn meaningful new IoT revenues, given the competitive challenges from more nimble OTT software players. Selection of strategy requires consensus on 'what you have

to believe' about demand, velocity and capabilities, which often leads to a chicken vs. egg debate. Winners execute on high CAGR, low complexity applications and services that compete with SaaS model start-ups.

Build vs buy decisions throttle EBITDA growth. As usual, risk tolerant operators gain advantage, but there will be winner and losers.

The global scale of IoT contrasts with SP 'local' native networks and drives transformation toward competing on global software industry terms. While there is no silver bullet, SP focus should be on building a horizontal managed service platform capability upon which ecosystem partners depend on interoperability standards, operating models and functionality that facilitates "roaming" of IoT services.

Current State of Play

Developing and launching an interoperable IoT service portfolio on a horizontal platform enables wholesale, enterprise and B2B2C models, but is a daunting corporate development and software integration journey. 2015 - 2020 is a period of strategy definition and selectively grasping emerging opportunities. Many enterprise IoT solutions quickly evolved as a SaaS model serving endpoint device management, data security, ingestion, stream processing, application enablement, storage, and API based partner ecosystems. Interoperability is under development via the Industrial Internet Consortium, Industrie 4.0 and others, but will only be a reality in 2017.

What Should Service Providers Do?

This year several leading analysts agreed that in the long run, a managed services model will dominate the IoT sector. SPs are naturally positioned to drive these managed services given their trusted position with visibility and links to multiple connectivity options, devices, data and SaaS. But there is also a potential that a Newco will emerge, just as Android did, to challenge incumbents.

The only certain 'Impact of IoT' is that everyone agrees that billions of connected devices requires embracing new ways of thinking of incremental software, cloud, and network service competencies to manage the exponential benefits of connected intelligence.

One SP alternative is to execute as a separate startup externally to the core business to develop IoT competencies adjacent to core telco products and operations. This approach offers the benefits of speed and agility borne from a minimum viable product development culture. Connected intelligence, in terms of velocity of endpoint device proliferation, data generation, and market demand for analytics far exceeds the capabilities of most legacy SP software capabilities.

This whitepaper explores the different aspects of what SPs need to do to make the journey to this new way of thinking.

Target Markets & Segmentation

Identify and quantify vertical markets in native geographies or global scope

To effectively execute on IoT product and services investments, SPs benefit from practical reviews of use cases mapped across essential functional capabilities and assets (both existing and potential). At the intersection of these decision criteria lies an initial answer to the strategic question of 'where to begin?' Insights from strategic assessments will vary for SPs given their geographical footprint, distinctive market positions, inherent strengths

and ability to invest in platform development. But they all share in common a rich customer base to provide services. Selecting the right use cases and demonstrating both customer value as well as SP business value establishes the 'right to play' above the connectivity layer and is the essential first step to a solid IoT SaaS strategy.

Determine value to be generated for given verticals

Developing an IoT platform business case will challenge traditional SP decision- making culture by forcing acceptance of 'straw-man' profitability assumptions. Determining the value generated by new services in a green-field context requires a range-of-value assumption set for pricing and margins, which ensures a higher degree of uncertainty. SPs must identify what is challenging to do in the context of value creation and then define what is important to own in terms of asset capabilities. Answers may vary across verticals.

Substantive use case and vertical market data is available to support development of credible total addressable market (TAM) estimates. SPs often gravitate toward the largest TAM opportunities where capabilities are strongest and execution risk is lowest. The global maturity of cloud services and transparency of compute costs enables business case estimation confidence.

The investment decision challenge for SPs becomes more complex when considering vertical market opportunities and horizontal platform capabilities. In this context, IoT data services investment requires a similar decision posture to that of building a network. The total value of vertical market opportunities cannot be known ahead of a decision to own the services platform. Build it and they will come?

Where organic synergies are easily found, SPs will partner with early adopters such as the auto insurance industry for user-based insurance, CCTV video for smart object recognition or the energy sector where smart buildings offer data sets for cross domain analytics with occupant mobile based location and anonymous application activity data. Outcomes from combined analytic insights will be powerful and command a premium service value.

Determine synergistic set of services to go to market with

In addition to connectivity and the base platform SPs need to decide how much of the value they want to address with their offerings. Given 70% of the revenue and profitability of the IoT offering will come from application level services SPs need to determine what capabilities they will drive themselves and bundle and what they are going to rely on partners to provide offerings. The models for providing this service can vary from SP being the responsible counterparty where they bundle all services underneath them to being an IoT IaaS/PaaS platform for others to offer service. A critical risk/reward decision SPs need to make. Some areas where SPs have started to develop capabilities are around transportation and smart cities.

Services Portfolio and Integration Capabilities

Identify core set of horizontal capabilities to build

In order for SPs to become effective IoT providers they have to bring strong horizontal capabilities to address the cross-section of capabilities required for IoT applications. These include:

Fog Platform: IoT applications will require a combination of different types of connectivity (Mobile, Wi-Fi, Low Powered etc.) along with the capability to carry out computing both at the edge and in the cloud. IT is critical for SPs to determine how to plan out their fog foot-print in a scalable manner based on the range of use cases they look to support. Fog utilization is especially required in areas where large data volumes, remote location or high latency makes local processing more optimal than shipping data to a cloud. Examples of these include remote site management and Oil and Gas exploration.

Cloud Platform: Cloud is an integral component of any IoT play to extend beyond connectivity. The SP needs to be able to assemble and integrate a critical set of services which can enable them to provide a scalable managed services platform for vertical applications. These include:

- Connectivity, Compute and storage management
- Security services across network, cloud, and applications
- Analytical services to drive across applications

Figure 1: IoTWF SP WG: SP IoT Reference Architecture

Ecosystem partnership strategy for vertical markets

While SPs are best positioned to build out horizontal platforms for IoT, that is not enough for an end-to-end offering in a specific vertical. IoT will require specialized vertical services based on the market being addressed. Some examples are; Smart cities (Parking, lighting etc.), Industries (machine automations & Tracking) and Healthcare. For these services the SP needs to assemble the right set of ecosystem partners to work with. These partners can operate and scale on top of the platform created by the SP, or use another platform and embed the SP's offering in that. New and innovative ecosystem partners will also require the SP to evolve their procurement strategy to

accommodate pay as you grow and consumption based transactions. In the new world of IoT the SPs should leverage innovative business models to diversify their risks and enable themselves to try as many viable offers in the market allowing them to choose and further invest in the ones that are successful. Typical business models based on a CAPEX investment up-front ties down the SP and makes it very difficult for the SP to fail fast and exit a particular market regardless of its performance. The value created when you have an established a good ecosystem of partners are many, both for the customers and the SP. This includes faster time to market, higher quality of service and a more cost efficient solution.

Service integration capabilities to implement large scale offerings

Enterprise/public sector IoT offerings will involve close integration into the standing legacy and future data sets and resources to real true ROI from the offerings. Additionally given the security issues surrounding IoT integration in to enterprise “Defense in Depth” plans are critical. These indicate that service integration capabilities will be key to the implementations. In order for SPs to be the master contractors of these implementation they have to develop the SI capabilities to offer these services

Technology Evolution

SPs continue to evolve their technology to match market demands. These technology evolutions have required SPs to re-invest in their networks while also incorporating ancillary technologies and systems including fog platforms, application platforms and security services to meet the future needs of enterprise, government and residential customers.

This whitepaper does not provide recommendations on the most appropriate IoT technology adoption approach (i.e., partnerships, acquisitions or technology development) for SPs. Each SP must make that decision independently. There are numerous examples of SPs that have pursued one or more approach and been successful in their markets.

This whitepaper discusses 3 of the most pressing technology and technology-related issues for SPs as they evolve from providers of M2M/IoT connectivity to offering a more complete managed services model to customers. This whitepaper focuses on evolving the overall IoT technology stack (see Figure1), the power of monetizing big data and creating secure IoT solutions.

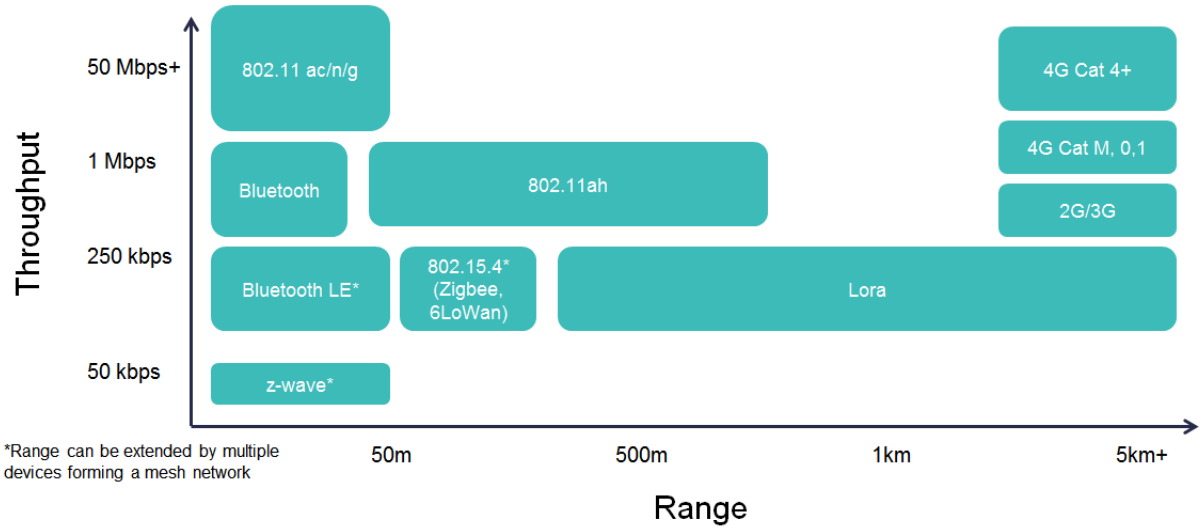
SPs realize that IoT requires an evolution of their technology stack. Today SPs are offering M2M/IoT communications, but many public and private sector customers want to engage in a more holistic way with their SPs. So SPs need to have technology that supports a managed services model to meet customers’ needs.

Next, we’ll cover critical elements of SP IoT technology evolution.

Edge Devices and Networks

Some of the most important SP technology decisions are occurring around edge devices and networks. In particular, SPs are determining the costs and benefits associated with using existing mobile and fixed networks for IoT services versus deploying new IoT-specific, low-powered networks. While SPs are testing various types of IoT-specific networks, there is no de facto standard for the industry.

Currently, the most common types of SP-powered M2M/IoT solutions use mobile networks for their connectivity – 2G, 3G and 4G. These networks provide secure, reliable, efficient bandwidth for many IoT solutions. The connectivity field is expected to evolve rapidly over the next few years. The considerations would be based on combinations of cost, power, bandwidth and capacity.



Edge devices running on these networks generally have access to power and a range of processing capabilities. Having processing capabilities at the edge provide SPs' customers with added value from the insights that SPs can gather from the edge devices. The value of an IoT solution is only as good as the value of the data insights, therefore, having high-quality and secure edge devices is critically important for SPs and their customers.

If these new types of networks were in place, demand for IoT solutions might increase significantly. These IoT-specific networks, often called low-powered device networks or narrowband networks, might open up a new type of IoT market for SPs.

SPs are exploring low-powered device networks currently. While the list of network options is long there is no consensus amongst SPs on the best network to implement. Some SPs have made financial and technology investments in the vendors that own these technologies, while other SPs are partnering with network vendors to trial these solutions.

Fog Platforms and Cloud Platforms

While the IoT ecosystem abounds with things that vendors call "platforms", for purpose of this whitepaper we will describe two common platforms features – connectivity management and analytics -- and the ways in which SPs are using or considering both.

Connectivity management gives the SP the ability to manage the connectivity element of the IoT solution. For example, in the case of a GSM network, the SP would be able to manage the mobile SIM. The management features vary by vendor, but generally allow the SP to turn on/off the connectivity element, set-up alerts and determine if there are problems with the connectivity element. This platform also allows the SP to collect usage data from the connectivity element for tariffing and billing purposes.

Almost all SPs that have launched M2M/IoT services in the last 5 years have implemented IoT connectivity management. Some SPs have partnered with connectivity platform vendors while others have built their own platform.

Analytics and big data features are the technology domains that allow SPs or their partners to make sense of huge quantities of IoT data. Much of the value of an IoT solution comes from analytics, visualization and big data capabilities. These features allow users of IoT solutions to understand the myriad data streaming from edge devices.

It is important that SPs have a way to conduct analytics in the fog platform – fairly close to the edge devices -- and in the datacenter or cloud. Having the ability to do analytics at both places gives an SP the most flexibility in offering a managed services model to its customers. This becomes important to address the range of use cases which SP's will need to support ranging from high-bandwidth remote applications which require local high-speed processing (e.g: Oil& Gas, Transportation, Remote sites) to high speed cloud driven applications(e.g: Smart cities, Retail Operations).

While SPs have implemented big data solutions for their own internal IT needs, an SP's decision to implement analytics and visualization tools as a product to sell to customers is a more complex decision. Below we discuss some of the issues associated with these technologies from SPs' perspectives.

Opportunities of leveraging analytics and big data solutions

SPs recognize that there is tremendous value in being able to capture, aggregate, federate, analyze and visualize the data obtained from IoT devices. SPs would like to deliver as much value from IoT data as possible, therefore, implementing analytics and visualization tools is something SPs take very seriously.

There are a few SPs that have implemented analytics and visualization tools – either through a partnership with a vendor or by building their own solutions – to help customers get maximum business value from IoT data. Often SPs choose to implement these tools because they have strong expertise in a given industry sector. They use their existing customer relationships to help define the parameters of the analytics and visualization tools.

Challenges of leveraging analytics and big data solutions

There are two general challenges for SPs implementing big data solutions. First, the IoT sales offerings associated with analytics, visualization and big data are not often sold to customers by most SPs. While SPs have great expertise in technology deployment, marketing/sales of solutions and customer support, higher level operations such as analytics have been obtained from SPs in limited capacity.

Second, there are often cultural, societal and governmental sensitivities associated with SPs accessing and selling services related to customers' data. Even when an existing relationship between a customer and an SP is very strong, there can be a series of customer and SP concerns that make it very difficult to create a contractual relationship for big data services. In particular, it can be difficult to balance the trade-offs between privacy and the business value of customer data. However, in cases where customers have engaged SPs for big data services, the relationships are strengthened and both parties benefit.

Application Enablement

In an IoT deployment, application enablement provides a way to store and transfer device data to applications in an efficient manner. Application enablement has a series of components including data storage, data management, data virtualization, analytics, platform rules engine and APIs.

SPs are currently deciding how to implement application enablement to support their IoT businesses. Those that have are selling a series of platform, application and integration services in some of their key target segments.

While few SPs have implemented a truly horizontal application enablement capability, there are some that have built or bought industry-specific capabilities covering sectors like automotive/transport, healthcare and connected home. These SPs have made strategic decisions – sometimes based on expertise in given industry sectors – to sell a more end-to-end solution in these industry sectors. Whether an SP has implemented an industry-specific or a horizontal application enablement capability, almost all SPs have partnerships and integrations to ensure the efficient storage and secure transfer of device data from the SPs' networks and edge devices to the end customers' applications.

OSS/BSS

SPs need to adapt to newer billing and tariff schemes and need to be able bill and account for new features and services. IoT will require a completely new way of billing that the SPs are not used to. In a number f cases, consumers are willing to pay a significant cost for connectivity when needed but not necessarily willing to get tied to a monthly connectivity fee. SPs should enable billing models for consumers and B2B2C where the consumer can choose to pay a heavy cost only when connectivity is used. An example is a fire extinguisher, defibrillator or other devices that are not in high use but when connectivity is required the manufacturer and/or the consumer is willing to pay upwards of $15-20 dollars for one time connectivity.

They should also setup a variety of different tariff plans based on the type of asset that they are providing connectivity and API Calls to. Industrial machines paying a much higher price per call vs Elevators etc. SPs billing systems should also be able to accommodate MVNOs who they can partner to provide new IoT solutions in the market.

Security

Security is one of the most hotly discussed topics in IoT[2]. Fortunately SPs have a strong history of providing extensive security across all of their edge devices, networks, fog platforms, cloud platforms and application enablement layers. It is common for public and private sector organizations to have discussions about technology security with their trusted SPs. And SPs can provide the necessary information to help organizations implement, test and manage secure solutions.

Below we summarize important IoT security issues that SPs can address with public and private sector organizations. We present this material using recent research on top IoT security practices as published by IoT research firm MachNation. See Figure 2.

[2] The IoT World Forum Steering Committee has a Working Group that discusses issues associated with security. We encourage readers with interests in IoT security to see additional work produced by the Security Working Group.

Top 10 IoT Security Recommendations

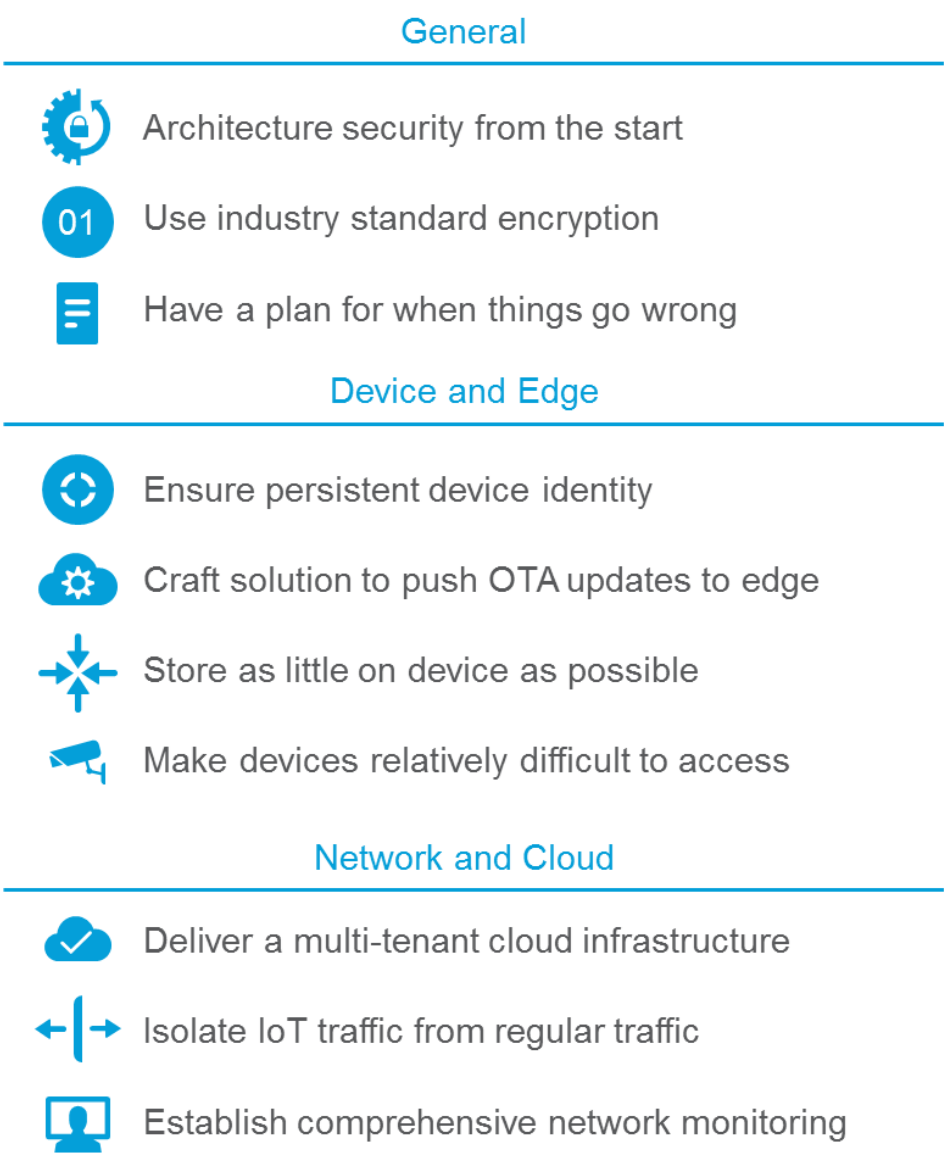


Figure 2: IoT Security recommendations

General security practices

While there are unique attributes of an IoT solution, organizations should not disregard best-practices from IT security as they assemble IoT solutions. In particular, security should be architected from the conception of an IoT project with involvement of IT security personnel. Organizations should ensure that their business continuity and disaster recovery plans are up-to-date and have incorporated the necessary amendments and revisions to take IoT solutions into account. Organizations need to use industry-standards for securing network traffic to reducing the likelihood of sniffing-type attacks from hackers. And finally, firms should evaluate whether data encryption — connecting data from IoT devices to the cloud – is necessary. Encrypting the channel as well as encrypting the data with asymmetric cryptography delivers the strongest security for data in transit, but does have overheads, latency drawbacks and monitoring challenges that make it suitable for some but not all IoT solutions.

Edge security practices

The tremendous number and heterogeneity of IoT devices make securing devices at the edge of an IoT deployment very important. First, each device should have an identity that is persistent and can be relied on as a unique identifier of the device for security and management purposes. Second, a secure IoT solution will provide a mechanism for keeping track of device versions and rolling out over-the-air (OTA) updates to maintain a desired level of security on the device. Knowing that many IoT device are designed to last a decade or more, leading IoT device and gateway vendors must make their devices updatable and upgradeable. Keeping devices secure aid in keeping the SP network secure. Third, a solution should store as little data as possible at the edge, only storing data that is necessary for accomplishing business objectives. And finally, physical security of edge devices augments cybersecurity in creating a barrier to entry to hackers and reducing available attack vectors. IoT devices should be difficult to physically access for non-authorized users while taking into consideration the business needs of the IoT solution.

Cloud security practices

For any IoT deployment that has cloud-based components, SPs and IoT customers must ensure holistic security practices. First, multi-tenant cloud platforms must allow deployment of logically separated cloud IoT services in order to ensure that security and reliability for each tenant is never compromised by other instances running in the same cloud. Second, IoT traffic ideally should be isolated from general IT traffic to help ensure that general IT security breaches do not spread rapidly across the network and impact mission critical operations powered by IoT solutions. And finally, organizations should use network traffic monitoring solutions that rely on static rule-based approaches to setup baselines for expected traffic as well as on heuristic-based solutions that can spot unusual activity not easily detectable with predefined rules.

Conclusion

While the market is well positioned to be addressed by SPs a number of critical investments and execution is required to make this a reality. The question is, how can SPs address the needs and drive to profitability and scale in the short run?

Key issues to be addressed include:

- Clear set of verticals and opportunity analysis
- Decisions on services to offer vs those they prefer to work with partners
- Technology stack to built
- GTM to take to market the new services including properly equipped sales force, system integration capabilities and GTM partners

Contributors:

Syed Iftikhar Ali
Senior Product Development Manager, STC Solutions

Alberto Araque
Vice President, IoT
Etisalat UAE

Rami Avidan
Director, M2M,
Tele2 Group

Angel D Barrio
Vice President, M2M
Etisalat Group

Othman al Dahash
Vice President, M2M

Goncalo Fernandes
Vice President, Digital Service

William Gerhardt
Director, Service Provider Strategy, Cisco

Matt Hatton
Founder and CEO,
Machina Research

Steve Hilton
CEO, Machnation

Mohamad Nasser
Sr. Director, M2M/IoT and Business Services, Sprint

Scott Puopolo
Vice President, Service Provider Transformation Group, Cisco

Yasir Qureshi
Senior Manager, Service Provider IoT GTM, Cisco

Vijay Raghavan
Head of Service Provider, IOE Market Development, Cisco

Jeffrey Spagnola
Vice President, Sales/ Global Service Provider Solutions & Architecture, Cisco

Stuart Taylor
Managing Director, Service Provider Transformation Group, Cisco

Brook Wessel
Vice President,
Telstra Software Group

Fred Yentz
CEO, deviceWise Telit

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**