DISH WIRELESS Enhanced Policy Management and Control

White Paper – August 12 2022

This white paper describes how enterprise customers can leverage the capabilities of a standalone 5G wireless network to support their evolving needs for policy management and control.

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This white paper describes the characteristics of effective, innovative policy management and control using the advantages of a standalone 5G wireless network. Network policy management and control refers to the rules that determine how network services are provided to customers in real-time. It includes access control policies, quality of service (QoS) requirements, service level agreement (SLA) considerations, traffic steering and routing configurations, charging policies and usage monitoring.

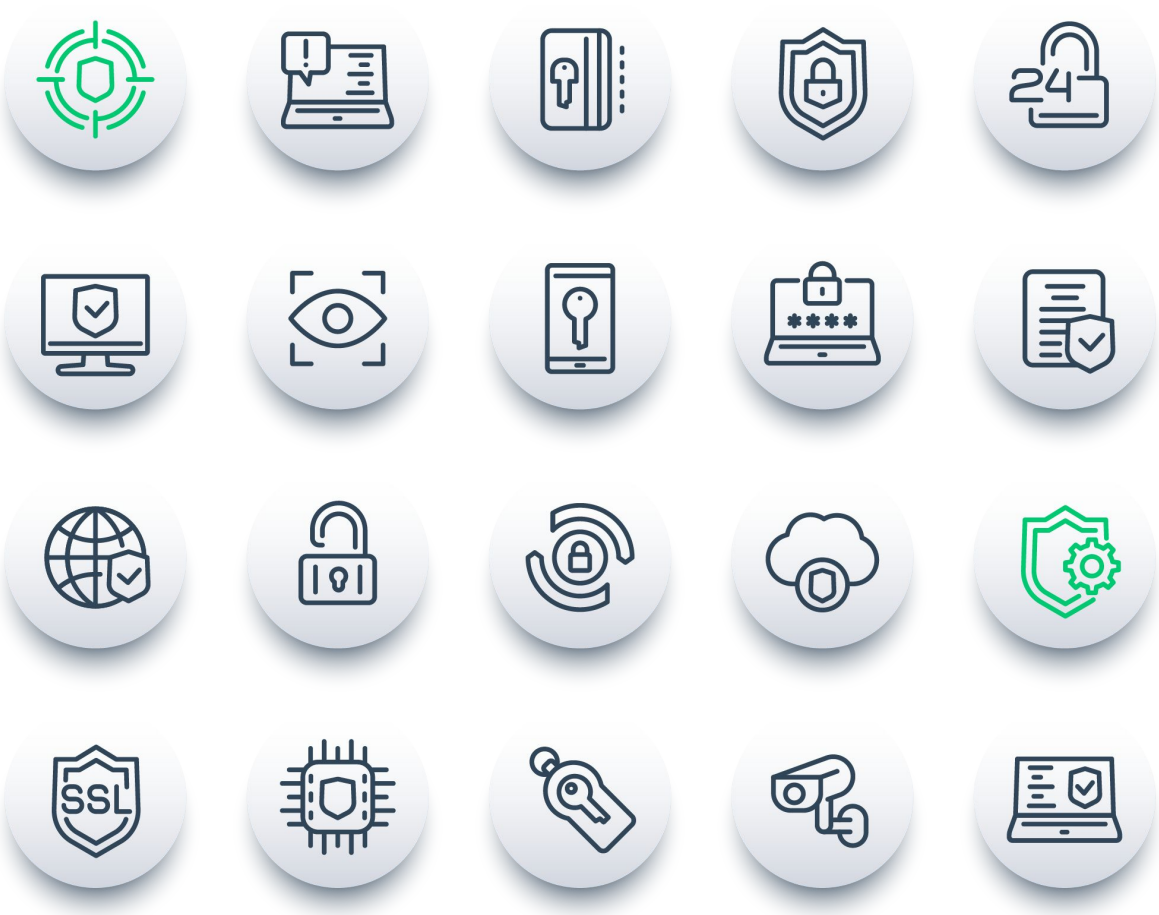
Different applications across various customer types and industry verticals can have divergent network requirements, but enterprises and mobile virtual network operators (MVNOs) have historically been restricted by a traditional “one-size-fits-all” network policy model deployed by existing wireless communications service providers (CSPs). Traditional wireless networks such as 4G LTE were designed to support predefined parameters such as throughput and policy management, based on estimated peak customer usage and customer classifications. While upgrades of the 4G LTE infrastructure are possible to create hybrid systems (non-standalone 5G), the result is an inconsistent network that is still more 4G than 5G, as the legacy core still limits the operations. It is not able to yield comprehensive 5G benefits across a wide footprint.

The traditional, one-size-fits-all approach essentially offers a best-effort attempt to provide a requested QoS level for a customer based on their service plan. The number of available service plans has traditionally been limited to 3 distinct classes of services with no ability to make customizations or modifications. To overcome these constraints, customers have traditionally utilized third-party policy management platforms to manage their policy needs and to implement rules for specific applications and use cases. While these platforms may provide additional capabilities to manage diverse technology rule sets, they are still subject to the limitations and constraints imposed by the CSP’s network. It can be difficult or impossible to maintain consistency or provide dynamic policy enforcement and solutions may be challenging to scale.

DISH’s standalone 5G network, designed from the ground up, will offer greater freedom and customization for supporting the management and control needs of customers with:

1. **Consistent policy management and control**
2. **Service-level Agreement (SLA) assurance and guarantees**
3. **Flexibility and scalability for business growth**

Thanks to our cloud-native, greenfield network architecture, the standalone 5G wireless network can be tailored to meet specific customer policy needs. Customers will no longer be limited to accepting a one-size-fits-all experience or have to rely on over-the-top policy management solutions, but can leverage the network to have consistent end-to-end control across all device categories, user groups and hierarchies.



IMPORTANCE OF NETWORK CAPABILITIES FOR POLICY MANAGEMENT

Wireless devices are essential tools for the enterprise workforce. As new wireless use cases and applications emerge, so does the need for the enterprise to manage the policy rules that apply to them. It bears responsibility for how devices are used and the risks associated with them. The enterprise not only needs the ability to own and manage the corporate data and applications being used, but must consider the cybersecurity risks.

Enterprises must define, build and manage the user experience across all wireless devices and services. They have a need to guarantee service performance, restrict data usage, safeguard corporate data and systems, ensure devices are not misused and meet regulatory compliance. Finally, policies must be managed across IT and OT (operational technology) systems, and tools often include a mix of proprietary as well as third-party solutions.

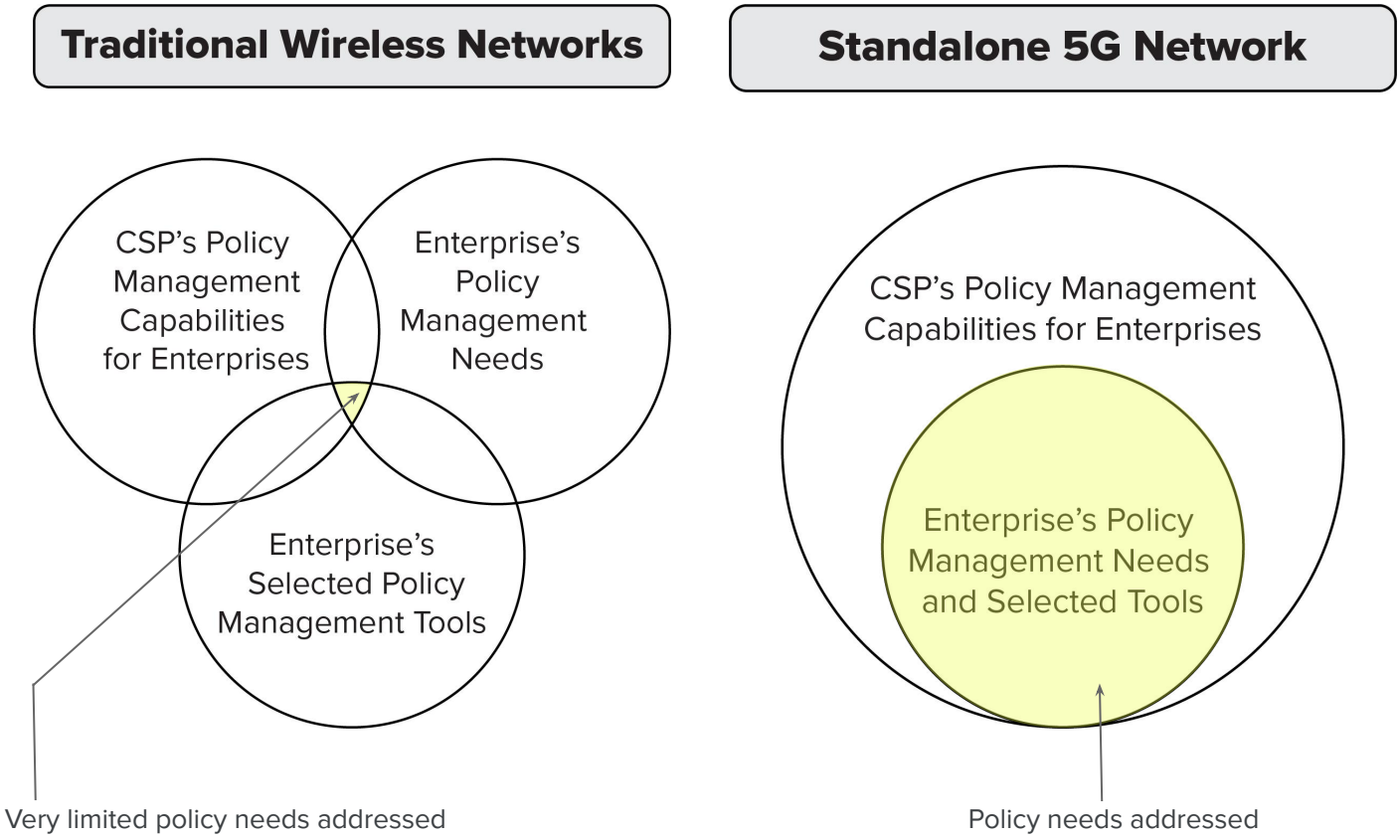
There are two specific challenges when policy management solutions involve traditional networks:

1. The management of the physical devices is subject to the capabilities and compatibility of the wireless device management platform (DMP) or mobile device management (MDM) platform supported by the CSP. The DMP or MDM tool may not support all of the enterprise policy rules, or it may be encumbered by operational complexity.

2. The CSP may not be able to guarantee that specific policy rules can be met. Reasons for this may include: lack of policy-based operating capabilities or enforcement; variability in architecture across the country; or lack of dynamic capabilities to deliver a QoS when a component fails.

These challenges have imposed a ceiling on policy management and control, limiting an enterprise's ability to effectively utilize wireless technology. As the enterprise data plane expands and requires access from anywhere, it is critical that CSPs begin to support the growing policy needs of the enterprise by providing policy-based network management.

Figure 1 - Policy Management Capabilities



THE NEW DISH 5G WIRELESS NETWORK

DISH is taking a customer and developer-centric approach to its standalone 5G network implementation. The demand for connectivity is growing exponentially with diverse and diverging requirements. Instead of building a one-size-fits-all network and making assumptions about customer needs, DISH is embracing an open business model where customers and developers can utilize network services, resources and functions in a deliberate and customizable manner.

Traditional network technology architecture combines the resources used for control with those used for delivering customer products. This introduces disadvantages because any time a modification is required – whether a network upgrade or a new product launch – the implementation impacts both network control and customer product infrastructure. Time-consuming and cost-inefficient processes are required to upgrade equipment, impacting customers and their own product or service-delivery infrastructure.

Thanks to the service-based architecture (SBA) and microservices nature of DISH's standalone 5G network, all functions in the network core have been disaggregated. The network functions responsible for operations and control are decoupled from those that deliver the customer experience. Software functions replace hardware infrastructure, and components can be decentralized ("virtualized" or "containerized"), allowing them to operate from anywhere within the cloud-native network. This allows the user plane network function to be located closer to the customer's connected user equipment (UE) and devices, such as on the customer's premises.

The user plane function (UPF) can also be located at the network "edge," which refers to the edge of the cellular network's physical infrastructure. The edge represents any possible configuration where network functions that provide service provisioning, computing power and intelligence can be located in a way that enhances the overall network services provided to the customer, in real-time and on demand. Redundant functions can live in the cloud as a backup in case there is a service disruption, like a power outage. The infrastructure can be continuously updated with little to no disruption for customers.

The service-based and cloud-native design of our DISH 5G architecture can provide adaptability, scalability and customization to serve customers with powerful capabilities. Different network functions to serve customers can reside on virtual machines or within containers anywhere within our 5G network, providing greater flexibility and scalability across all deployment options. Fine-tuning network operations, optimizing current products and supporting new, customized policies can all be done concurrently. Performance and policy needs that traditional wireless networks were unable or unwilling to meet are now possible. A key network function such as the UPF can be created exclusively for an enterprise customer to provide customized needs such as data segregation and security, reduced latency, minimum throughput and network control.

Table 1 - Group 1 5G Network Functions

Function	Description
User Plane Function (UPF)	**A network function that routes and forwards user plane data packets between the base station (cell site) and the external data network (i.e. Internet).** It is similar to the service and packet gateway functions in a 4G network, but it is cloud-native and can be deployed anywhere to meet service requirements. It can also manage, prioritize, and duplicate data packets as they traverse the network, thus offering redundancy and QoS assurance.
Unified Data Management (UDM)	**A control plane function that manages and stores subscriber and device information, default QoS and prioritization, authorized data channels, maximum bit rates and service continuity provisions.** It is similar to the Home Subscriber Server (HSS) function in a 4G network, but it is cloud-native and designed for 5G services.
Access & Mobility Management Function (AMF)	**A control plane function that manages registration, authorization, connection, reachability, and mobility.** It is similar to the Mobility Management Entity (MME) function in a 4G network, but it is cloud-native and supports many additional capabilities unique to 5G. For example, it also supports dynamic updating of network interfaces and cellular sites, greater privacy via the use of a 5G temporary device identity, enhanced security across the user and control planes, and stores network slice information. It can also select an appropriate Policy Control Function (PCF) for a device or use case.
Session Management Function (SMF)	**A control plane function that oversees packet data session management, IP address allocation, data tunneling from a cell site base station to the user plane function, and downlink notification management.** It performs the tasks of the serving and packet gateways (S-GW & P-GW) in a 4G network, but also allows for control plane and user plane separation in 5G.
Policy and Control Function (PCF)	**A control plane function that provides policies for mobility and session management.** It is similar to the Policy and Charging Rules Function (PCRF) in a 4G network, but it is cloud-native and offers additional capabilities in the 5G network, including event-based policy triggers, resource reservation requests, and access network discovery and selection. The PCF directly influences QoS and subscriber spending limits, and as a result plays a critical role in the enhanced policy management and control capabilities of the 5G network.
Charging Function (CHF)	**A control plane function that provides online and offline charging for multiple services, including 5G and 4G core integration.** It supports real-time control of subscriber's usage of 5G network resources and generates all charging data records. It is similar to the charging capabilities of the PCRF in 4G. However, the intent to break it out separately from Policy and Control Function (PCF) is to offer greater flexibility. For example, connectivity for mission-critical use cases should not be turned off the moment that a monthly data plan is exceeded. In addition, services can be recharged as necessary by the authorized customer.

Network Slicing

“Slicing” takes advantage of the microservices nature of the network to create separate virtual or logical networks that can be made up of shared or dedicated functions, creating a network-of-networks. These sliced networks can be built to support different use cases and customer types with requirements such as availability, reliability, throughput, latency and privacy. They can also support different access policies, traffic steering and routing configurations and different data network endpoints.

A single network slice can support multiple customers or use cases, and multiple slices can be used to provide services to a single customer. Network slicing enables our network to provide a customizable policy management and control experience to any customer, enabling security policy and configuration options never before available.

Figure 2 - Network Slicing Attributes for Enhanced Policy Management and Control

Slicing Attribute	Policy Management Examples
Area of Service	A U.S. government entity requires additional data security and may utilize a network slice that restricts which geographic service area a service is available in.
Isolation Level	An enterprise may wish to segregate and isolate its network traffic from other public traffic for security reasons by requiring dedicated SMF and UPF network functions.
Mission-Critical Support	A first responder agency may utilize a network slice that offers higher prioritized traffic.
Guaranteed Uplink Throughout	An energy production company may use a network slice with guaranteed minimum uplink throughout for IIoT devices, such as surveillance and leak detection cameras.
Customer Network Functions	An enterprise may wish to use its own UPF located on-premises or within a private cloud instance in order to ensure data integrity and security.
Network Slice-Specific Authentification and Authorization Required	An enterprise wants to control access to its network slice by utilizing its own authentification, authorization, and accounting (AAA) server.
Latency from (last) UPF to Application Server	A drone company may utilize a network slice with minimum latency betwen the UPF and an edge-hosted flight application.

A second group of new 5G network functions includes the NEF, NWDAF, NSSF, NRF, and NSSAAF, and are responsible for providing unique network service capabilities enabled by the introduction of network slicing and not available through traditional wireless networks.

Table 2 - Group 2 5G Network Functions Used for Network Slicing

Function	Description
Network Exposure Function (NEF)	**A control plane function that provides information regarding the network functions that are available to use (by the enterprise customer).** It is similar to the 4G Service Capabilities Exposure Function (SCEF), but it is cloud-native and exposes event information, network monitoring, network control, provisioning capabilities, and policy/charging capabilities externally. This allows the enterprise customer to monitor and affect QoS and charging for devices.
Network Data Analytics Function (NWDAF)	**A control plane function that collects data from all pertinent network infrastructure relevant to a customer's services, including user equipment (device), network functions, network operations and administration, cloud, and edge that can be used for data analytics and insights.** It is a unique standalone 5G network function that exposes full visibility to network performance and operations as they relate to a customer's KPIs.
Network Slice Selection Function (NSSF)	**A control plane function that provides network slices to the AMF.** A network slice is an independent, end-to-end logical network that runs on shared physical network infrastructure. It involves the allocation of network resources across all network infrastructure to meet specific service requirements, from the network core to the radio access network (RAN). Specific requirements may include QoS assurance, security policies, data isolation, dynamic policy management, etc.
Network Function Repository Function (NRF)	**A control plane function that allows 5G network functions to be registered, discovered, and subsequently made available to customers.** This is a unique capability in the standalone 5G network that allows customers to subscribe to the necessary microservices or to have dedicated network functions for their services.
Network Slice Specific Authentication and Authorization Function (NSSAAF)	**A control plane function that supports authentication and authorization of slicing with an AAA server (Authentication, Authorization, and Accounting).** It is a unique capability of the standalone 5G network that allows customers to access a predefined network slice or a newly requested network slice in real-time and using their own existing authentication infrastructure.

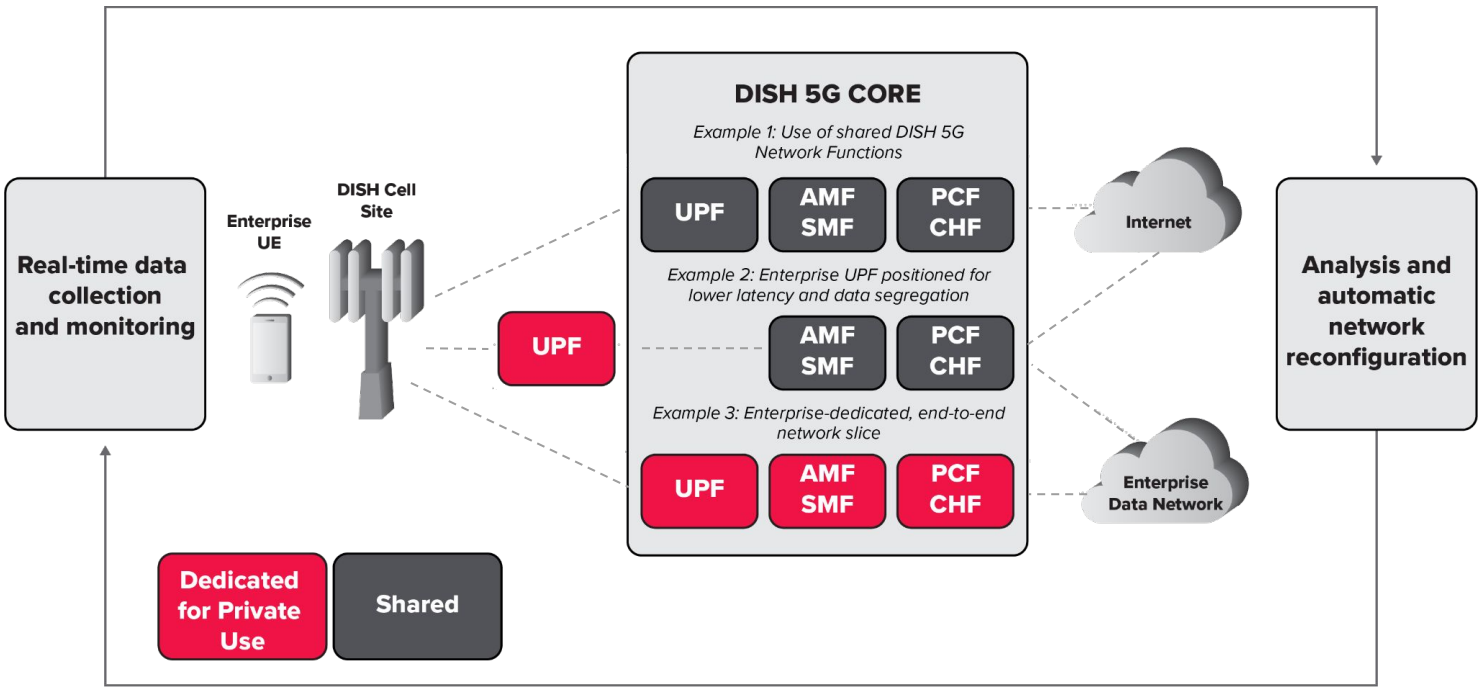
Advanced Orchestration and Closed-Loop Assurance

To manage this complex network-of-networks architecture, the DISH 5G network includes advanced orchestration and closed-loop assurance capabilities.

- Advanced orchestration: the intelligence of the network to coordinate operations and assess real-time resource availability, network conditions, and subscriber demand.
- Closed-loop assurance: the continuous orchestration of the network and predictive capabilities to assure that customer requirements are met at scale.

These tools enable dynamic policy management and guarantee SLA.

Figure 3 - Orchestration and Closed-Loop Assurance



Open APIs = Unlimited Functionality

DISH is implementing an open application programming interface (API) policy where any functionality that can be exposed through an API is available to customers. Unlike traditional CSPs that provide a limited and predefined set of APIs, DISH will make its full suite of APIs available to customers to allow network characteristics to be programmable, granular, scalable and customizable. Customers can select a QoS without having to know anything about the technical mechanisms or underlying capabilities. This shortens the development time for customized service delivery, letting customers focus on what they do best without having to become 5G experts. Users do not have to learn new standards to benefit from the 5G network.

API exposure benefits the developer community, providing developers and innovators all the tools they need to design, experiment and create solutions that leverage the 5G network's capabilities. A developer-customer can design and test their products and services in a production-level environment and deploy customized solutions and monitor performance metrics to ensure expectations are being met. They can model network adjustments to service policies in real-time to simulate evolving customer requirements.

The Power of the Cloud

The cloud provides computing resources and services accessible to UE. Instead of depending on physical resources for network upgrades, the cloud can provide network horsepower or customized data management as needed. Resources are accessible from the cloud and can be allocated more efficiently to customers in specific locations.

Containerization makes cloud-based applications easier to manage and deploy, giving customers flexibility to move the same containers between different clouds and use open source tools to manage across any cloud environment. Containers offer security benefits for applications running in the cloud as they provide isolation between the application and host environments. As an example, an enterprise may manage tens of thousands of wireless IoT devices on behalf of its customers and use database and real-time analytics services in the cloud. The enterprise requires full observability of both the devices and the generated data packet traffic flows and is responsible for the overall data security and privacy of its customers. The cloud-native and friendly nature of the DISH 5G network supports integration and interoperability with the database and analytics services in the cloud. The enterprise customer does not require any wireless network expertise. Instead, any pre-existing cloud services can continue uninterrupted as the enterprise wishes to adopt 5G. Plus, the enterprise can manage varying levels of policies on data security and privacy based on their end customers.

The developer-customer introduced above can also leverage the power of the cloud. New products and services can be easily deployed from any vendor lab and use the convenience of the cloud for development and testing. These capabilities empower a customer to participate as a co-developer with DISH. Instead of proposing products to CSPs that go into a long queue and may never be certified for deployment, the customer can develop and test their products independently and simulate their behavior on the DISH 5G network. This provides a quicker path to deployment and a greater likelihood of achieving desired business outcomes.

Bridging Established Wireless and Wireline Networks

Enterprises with established policies on existing networks can benefit from the flexibility of the DISH 5G network. Instead of having to manage enterprise policies across different wireless and wireline networks, or learning how to manage policies in a 5G environment, the standalone 5G network supports access integration for multiple networks and protocols. This makes life easier for IT policy managers; the last thing on their mind is having to worry about administering policies on yet another network. 3GPP partnered with the Broadband Forum to define a set of standards and capabilities called wireless-wireline convergence, in which new 5G network core interfaces allow the integration of different networks while using a common 5G core to manage everything. This new converged network removes the need to have duplicate authentication and service management across multiple networks.

DISH POLICY CONTROL AND MANAGEMENT PROPOSED BENEFITS

Consistent Policy Management and Control

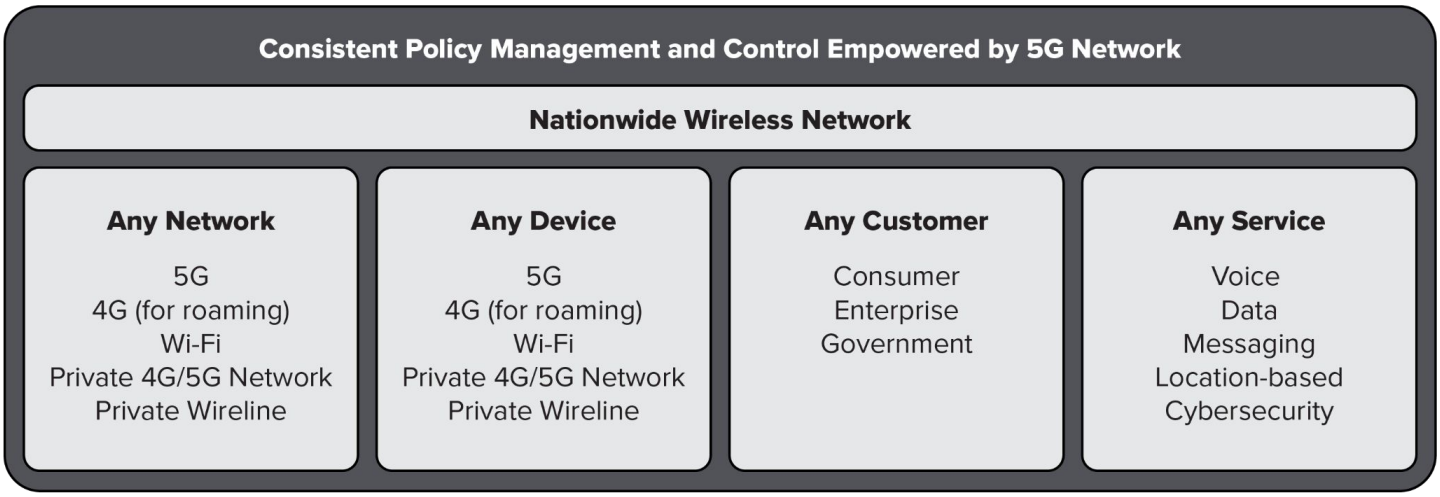
A standalone 5G network architecture is designed to be a service- and policy-based network. That means it is designed so that any combination of network components, functions and resources can be tailored to support optimal service delivery and predictable performance.

Consistency across geography – An enterprise customer can expect to deliver on a uniform set of rules and requirements because the network is designed to guarantee that the same experience in Orlando can be delivered in Houston and Los Angeles. The cloud-native and distributed network architecture allows for the ability to copy, paste and deploy policies for associated services. An enterprise customer that has 200 branch locations can deploy policies to subscribed network services through this method quickly and easily. Traditional networks can't do this because the architecture used in one region may be entirely different from another.

Consistency across networks – Service providers and enterprises have a need to ensure policies are consistently applied even if the device communicates over other networks, whether they are trusted such as enterprise private local area networks (W/LAN) or untrusted (third-party Wi-Fi). Devices and UE can span multiple networks. The PCF function and multiple network bridging capabilities allow for access discovery and selection of multiple and secondary networks while applying consistent policies.

Consistency across customers, services and devices – Required policies need to be mapped across the requested services and corresponding devices that span the enterprise customer operations with the CSP's wireless network. Several capabilities provided by the 5G network can do this. The first is the Open APIs described previously that provides enhanced service delivery control. Second, the enterprise customer can reserve its own dedicated service made up of separate and/or isolated 5G network functions and slices. Third, customers can also choose to bring their own infrastructures and BSS elements and integrate those with the 5G network.

Figure 4 - Policy Management and Control



Service-level Agreement (SLA) Assurance and Guarantees

SLA assurance refers to the ability to confidently predict a level of service to the point that it can be guaranteed for a customer. Traditional wireless networks offer a best-effort QoS delivery, with partial control over the prioritization of data packets. This means that SLA assurance isn't possible because the wireless network service cannot fairly predict that a specific data packet will always be delivered according to a specific customer requirement. In a standalone 5G network full, end-to-end control is possible, which allows for SLA assurance to be outlined in contractual obligations and service expectations between parties.

SLA assurance and empowered QoS – 3GPP recognized this significant SLA capability in a 5G network and defined a list of 5QI values. 5QI stands for 5G QoS Identifier. It is similar to the QoS Class Identifier (QCI) used previously in a 4G network. This set of values describes the priority level and performance requirements for specific use cases.

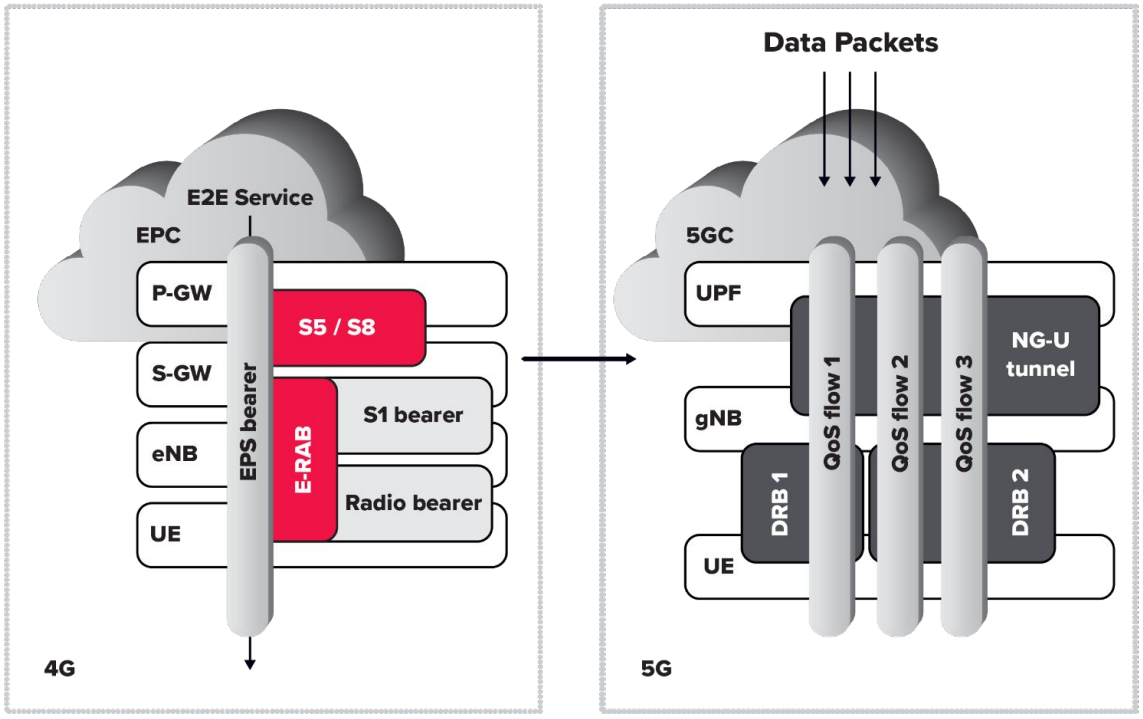
Table 3 - Partial Sample of 5QI Value

5Q1 Value	Resource Type	Default Priority Level	Packet Delay Budget	Default Max Data Burst Volume	Example Services
2	Guaranteed Bit Rate (GBR)	40	150ms	NA	Conversational Video
8	Guaranteed Bit Rate (GBR)	80	300ms	NA	Video (Buffered Streaming)
67	Guaranteed Bit Rate (GBR)	15	100ms	NA	Mission Critical Video User Plane
84	Delay-critical GBR	24	30ms	1354 bytes	Intelligent Transport Systems
88	Delay-critical GBR	25	10ms	1125 bytes	Interactive Services Using Motion Tracking Data

While both QCI and 5QI values are intended to ensure that data traffic in the wireless network is properly handled, there are noticeable differences. First, the 5QI values apply to all of the transport layers that a given data packet will travel through. Essentially, it is a QoS flow that runs from the application on the device or UE through the radio access network, the core and to the cloud. In 4G, the QCI values are based on the assumption that a specific transport layer will be available to satisfy the request, and there is no dynamic network adjustment mechanism available to guarantee that.

Secondly, the addition of network function virtualization and network slicing empowers QoS to be guaranteed through an SLA by provisioning every 5G network function and every component, including the RAN, to prioritize data traffic for the user as needed. The radio access and core network components are decoupled, so multiple pipes can be stood up as needed. Figure 5 illustrates this comparison.

Figure 5 - Comparison of QoS Models of 4G/LTE and 5G



While 4G utilized a single pipe for all data, 5G can establish multiple pipes as needed to provide differentiated service levels.

In downlink:

The UPF maps data packets to QoS flows (based on SDF classification rules provided by the SMF)

The gNB maps QoS flows to data radio bearers

The UE maps packets based on QoS rules from the AMF or via reflective QoS

QoS Extended to third-party applications and services – The PCF network function manages the standard protocol for data packet travel on a wireless network, known as diameter protocol, and also supports service requests using an IP-based interface, expanding 5QI capabilities to third-party or value-added services consumed using the wireless network. Therefore, the 5G network architecture delivers QoS to third-party, over-the-top applications. It can also leverage resources and computing power in the cloud, whether from within its own network or from an enterprise customer's cloud, to deliver the necessary user experience. An example is the Visual Content Rendering 5QI value (89), which supports AR/VR applications in which on-device intelligence and processing is augmented by computing resources in the cloud.

Key Example #1: Video Streaming Services

Services such as Sling TV require a minimum QoS in order to deliver a minimum acceptable user experience. In a 5G network, enhanced policy management and control capabilities would support a minimum downlink throughput for the user.

Key Example #2: Visual Rendering Split Across Device and Cloud

Services such as AR/VR for training and remote analysis can be designed to only require a minimum service-level for throughput, but also they need resource access policies across multiple sources, including the primary network, the enterprise WAN or LAN, and the cloud.

Flexibility and Scalability for Business Growth

Flexibility managing multiple policies and rules – New business applications are made possible, empowering customers with new options and flexible policy management to operate their businesses.

Key Example #3: IoT Devices in Resort Hotel

A hotel resort may have a range of IoT sensors and equipment that have fairly different requirements from a wireless network. The lighter-weight IoT sensors that transport very small data packets on an infrequent basis may not require significant data prioritization, but cybersecurity policies may be required to safeguard the system. On the other hand, wireless, UHD video surveillance cameras used to provide building security would require a guaranteed uplink throughput. The wireless connectivity of these cameras allows them to be installed without the complexity and cost of running network cabling. A network slice could be customized for the building to manage the varying policy needs of these devices, giving the hotel the ability to improve security for guests and employees.

Key Example #4: Personal Device Used at Work

Enterprises that allow employees to use their own personal mobile devices may have policies that require device tracking and usage restrictions to a specific geographic area during business hours. Let's assume that an employee is a field technician and travels regularly. In this example, the PCF has the intelligence to modify subscribed device policy information and inform the AMF if certain rules are triggered, namely when the business day ends and the employee is off the clock. In this case, the device should no longer be tracked accordingly. Thus, the enterprise can save money by avoiding the cost of providing a separate mobile device while assuring that its policies are followed by the employee's personal device.

Scalable business growth including multi-tenancy and multi-branded services – The 5G network architecture enables customers to better manage their own portfolios. One of the biggest challenges with traditional networks is the limitations of supporting multi-tenancy and multi-branded services. Multi-tenancy refers to the ability of managing services delivery across multiple customer groups while using a common denominator of operating tools. For example, a construction company needs to manage cellular services for different categories of employees and types of devices. A CIO for a school district needs to manage different flavors of cellular services across students, faculty, and facilities staff. They may also have an authorized IT contractor that provides advanced services and requires the highest level of access to the district's IT and OT systems.

This requires the ability to create and manage a hierarchy within the subscription to the wireless network. Without this capability, customers are relegated to managing multiple accounts – usually through separate subscriptions – each with its own rate plan and authorized account owner. It's a logistical mess if the designated account owner leaves the company or moves to a different division. Plus, a single account may be limited to a number of lines or devices, or has a default restricted policy.

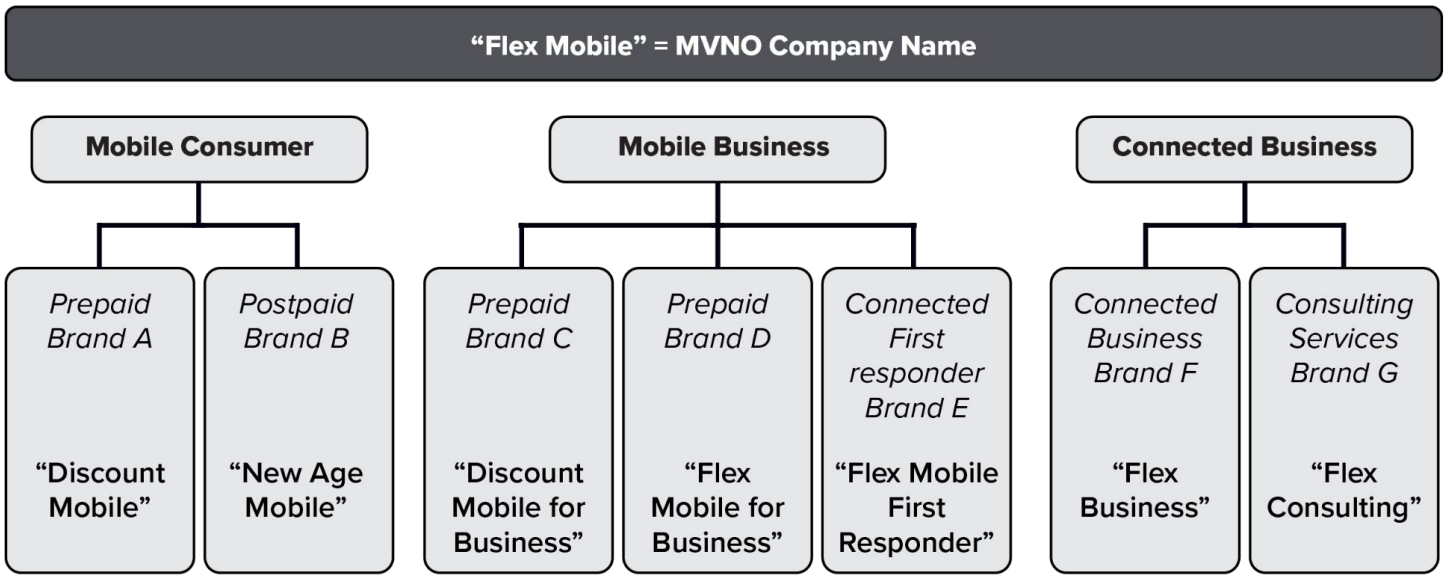
Finally, the same IT contractor may provide services to other school districts, manage subcontractors and have contract employees for dedicated work functions. The contractor needs hierarchy control to manage their own company's policies in addition to the clients they serve.

The same challenge applies to multi-branded services. In the consumer retail wireless space, basic cellular services can be simplified and presented in a good/better/best fashion to customers. However, as additional rate plans, value-added services and accessories enter the picture, managing the entire product catalog becomes more complex. The level of required customization makes it difficult to scale. Enterprises serving business customers need efficient and effective methods of servicing diverse customer segments and their needs. Let's consider another example.

Key Example #5: Product Lifecycle and Growth of an MVNO

A Mobile Virtual Network Operator (MVNO) is empowered by the standalone 5G network architecture and its enhanced policy management and control capabilities. Let's say that a hypothetical company called Flex Mobile launched in the past and started as a value-centric provider of consumer mobile services. It started with a prepaid, consumer mobile brand called "Discount Mobile." However, it then decides to launch 5G services and expands its service portfolio to include postpaid consumer mobile services, which it calls "New Age Mobile." Before long, Flex Mobile believes that it has the resources and competencies to expand into the business (enterprise) segment and offer B2B services. The diagram below summarizes its brand family. In order to scale, it is critical the Flex Mobile manage policies across its various brands.

Figure 6 - Multi-brand Service and Policy Management Capabilities



New monetization opportunities – The standalone 5G network enriches policy management and control to support new monetization opportunities. As an example, consider a cybersecurity solutions provider that sells products and services for businesses. It offers identity and access management, endpoint protection, denial of service protection and firewalls.

Using network slicing, this company can expand its portfolio by offering customized security levels and policies for different slices. Security controls that can be embedded within slices include endpoint (device) protection, denial of service protection, identity and access management, firewalls and gateways, behavioral anomaly detection and many more. Some of the cybersecurity provider's products can be purchased via a licensing fee, but it also sells a fully managed cybersecurity service, complete with turnkey design, installation, real-time monitoring and action-taking on behalf of the customer.

Finally, the cybersecurity solutions provider has a product development team that is continuously exploring service enhancement features. Internal developers can leverage the open characteristics and APIs of the 5G service-based network architecture to develop and test new products and simulate cybersecurity attacks.

Key Example #6: Enhanced Policy Management for Cybersecurity Solutions Provider

Security controls can be embedded into 5G network slices. The network slices can also support a new, additional security safeguard. For example, in the event of a compromise to the solutions provider's own set of customers, a new traffic-isolated network slice can be instantiated to maintain business continuity without service disruption. The end customer's data can be managed accordingly in the new protected network slice. Thus, the standalone 5G network helps the solutions provider deliver its cybersecurity service better, but also it enhances its overall customer value proposition by providing it with additional cybersecurity capabilities.

CONCLUSION

Wireless services are evolving rapidly to support the changing needs of the enterprise customer. By adopting open, cloud-native technologies, the standalone 5G network is primed to support this evolution. With a flexible and enhanced set of policy control and management capabilities, DISH's standalone 5G network will empower all customers with additional policy management and control capabilities. Policies can be managed by DISH, by trusted agencies or by the customer themselves. These policy capabilities not only provide consistency and SLA but also enable disruptive business models to maximize value for the market and create the greatest value for customers.

ACRONYMS

5QI ..... **5G Quality of Service Identifier**

AAA ..... **Authentication, Authorization, and Accounting**

AMF ..... **Access & Mobility Management Function**

API ..... **Application Programming Interface**

CHF ..... **Charging Function**

CSP ..... **Communications Service Provider**

DMP ..... **Device Management Platform**

GBR ..... **Guaranteed Bit Rate**

GSMA ..... **Global System for Mobile Communications**

IT ..... **Informational Technology**

LAN ..... **Local Area Network**

MDM ..... **Mobile Device Management**

MME ..... **Mobility and Management Entity**

MVNO ..... **Mobile Virtual Network Operator**

NWDAF .....**Network Data Analytics Function**

NEF ..... **Network Exposure Function**

NRF ..... **Network Repository Function**

ACRONYMS

NSSAAF ..... Network Slice Specific Authentication and Authorization Function

NSSF ..... Network Slice Selection Function

OT ..... Operational Technology

P-GW ..... Packet Gateway

PCF ..... Policy and Control Function

PCI ..... Payment Card Industry

PCRF ..... Policy and Charging Rules Function

QCI ..... QoS Class Identifier

QoS ..... Quality of Service

RAN ..... Radio Access Network

S-GW ..... Serving Gateway

SLA ..... Service Level Agreement

SMF ..... Session Management Function

UDM ..... Unified Data Management

UE ..... User Equipment

UPF ..... User Plane Function