STRATEGY ANALYTICS
Research, Experts, and Analytics

Wireless Networks and Platforms

Next Gen. Networks Must Meet Seven Key Challenges To Deliver *IoT Services, Security, FMC, Cloud, Network Slices, 5G and Bursty Video*

Wireless Networks and Platforms (WNP)

Snapshot

Strategy Analytics lays out seven challenges that could be 'show stoppers' for the major markets that Service Providers are looking to address over the next decade.

Both generic capabilities like Security and Bursty Traffic Optimization as well as the specific requirements for IoT Services, Fixed Mobile Convergence, Cloud, Network Slicing, 5G and 4K Mobile Video create significant challenges that cannot be addressed at scale today. Even massive additional bandwidth will not be enough to solve these problems - new approaches are needed and work is just beginning.

This report reviews these challenges and the specific requirements needed for Next Generation Broadband networks to deliver what is needed for the multi-billion dollar markets of the next decade.

November 2016

Sue Rudd
Tel: 1 617 614 0709
email: srudd@strategyanalytics.com

Executive Summary

Moore's Law is running out of steam and faster processing will no longer conceal the problems inherent in today's networks. Router tables are getting too large and the Scope, Scale and Speed of Networks must increase dramatically.

Internet Protocols and Architecture were designed in the era of narrowband networks. In 1978 when TCP was first modified to accommodate "all kinds of network interconnections" data rates on modems were generally 9.6 Kbps and widespread use of Ethernet was several years away. Many problems that have emerged over the last 30 years must now be addressed to deliver the promise of broadband networks for 2017, 5G and beyond.

Many of the benefits of Next Generation Networking cannot be achieved unless the network allows new approaches to Security, End to End (E2E) Service Layers that are independent of lower layer resource allocation and guaranteed Quality of Service (QoS).

In this report we analyze seven critical challenges and the requirements to meet the demands of both fixed and mobile Next Generation Broadband networking. These are:

- ***Unique Identifiers*** - Unique 'Names' for billions of IoT devices
- ***Security*** that is inherent in the system or services design and that prevents applications from attacking either the network or other applications
- ***Services that operate seamlessly both over any layer 1 physical Transport and any layer 2 Protocol*** to enable true Fixed Mobile Convergence
- ***Global layer 2 support of vLAN Connectivity*** for Global Cloud and Software Defined Data Centers
- ***End to End Services*** - for seamless end user to Service/Applications Assurance
- ***Guaranteed Quality of Service (QoS and Security for 'Network Slicing'*** Latency, Bandwidth SLAs.
- ***Bursty Traffic Management*** that can mix hugely bursty video traffic efficiently with voice calling, mobile money transactions and occasional messaging

ETSI has initiated work to address these challenges.

In January 2016 ETSI formed a Next Generation Protocol (NGP) Industry Specification Group (SG) and in May 2016 the group presented a Webinar that described why many aspects of 5G, IoT and Scalable Broadband Networking demand new approaches. In October 2016 ETSI's Next Generation Protocol (NGP) group published its revised NGP *Scenario Definitions* and ran an NGP Forum at 2016 SDN World Congress. The PRISTINE group an EU Initiative also ran a workshop on new approaches to a Next Generation Architecture.

Strategy Analytics has prepared this White Paper to contribute a perspective on the importance of the seven challenges and the Scenarios being developed by NGP.

Failure to address these challenges will dramatically reduce the ability of service providers to address multi-billion dollar market opportunities in ***IoT Services, Security, FMC, Cloud, Network Slices, 5G*** and ***Bursty Video***.

An Introductory overview video for this report was recorded at Broadband World Forum 2016 and is available online.

Table of Contents

1. The Seven Critical Challenges

In this report we review seven critical challenges and the requirements that must be met if Next Generation Broadband networks are to deliver what is needed for major markets of the next decade. The table below describes the specific needs associated with each specific challenge and the markets critically impacted.

Table A. Seven Challenges Must be Met to Reach Major New Markets

	Challenge	User Concerns	Major Markets Critically Impacted
1	**Network Independent Personal or Unique Digital Identifiers**	*"Don't make me change my name when I move addresses."* *"I don't want to 'port my phone number' I want to port myself. "*	• **Mobility as 'just' a Dynamic Addressing Problem** • **Logical eSIM and other Personal Identity Mgt. independent of Phone Numbers and Device IDs** • **IoT and M2M. Services with huge numbers of user equipment (UE) terminations e.g. Assets Tags, RFIDs or Smart Car Parts**
2	**Inherent Security**	*"When do I actually feel secure? Only when I am fully separated from harm."*	• **Security for Critical Transactions like eCommerce** • **Security for Network resources** • **Security for Everyday Users**
3	**Seamless Layer 1 *and* Layer 2 Service Access**	*"I just want to get my own stuff and other stuff wherever I am and however (or wherever) I want to access the network with any or all of my devices."*	• **Fixed Mobile Convergence (FMC)** • **Multi-Access and Multi-Device Voice and Video 'Delivery Anywhere Anytime'**
4	**Unlimited Global Layer 2 support for vLANs**	*Users and CIOs Say "Why am I now trapped in Cloud Provider's 'Walled Garden'? Why can't we just get access to anything on any server in any Data center just as we do on our LAN?*	• **Global Cloud Providers - Google, AWS, Azure etc.** • **Multinational Enterprise Networks** • **Software Defined Data Centers (SDDCs)**
5	**Services Optimized End to End without Tunnels or VPNs**	*User and CIOs say "Service providers want to charge me extra when we just want to get the guaranteed quality we need for each app as we need it."*	• **End to End (E2E) Service Layers with guaranteed Quality or Class of Service (CoS) is essential for SLAs and Consumer Experience Management (CEM)** • **5G and Pre- 5G 'Network Slicing' needs E2E guarantees so every app or service gets exactly the 'Class of Service' it requires**
6	**Quality of Service (QoS) guarantees better than Internet 'Best Efforts'**	*"What do you mean the 'network threw away my packets'? And resent them minutes later?"*	• **Low latency apps Autonomous Vehicles and eCommerce / Financial Transactions**
7	**Bursty Traffic Optimization**	*"Why can't I do live streaming broadcasts or HD Video downloads cheaply any time I want to?"*	• **Two Way Video** • **Live User Originated Streaming** • **4K Video Download for Mobile Devices** • **Remote Drone or Robot Control**

If Service Providers cannot address the critical user needs shown in the middle column above they will be ***unable to address the major markets summarized in the right column***. These markets represent the largest multi-billion dollar opportunities over the next decade for Mobile Operators and Fixed Broadband Service Providers.

Each of the seven challenges can separately undermine a Service Provider's ability to address specific key markets. But if several challenges are looked at together the problem will appear less intractable.

For example if we look at the need for *Security* in conjunction with the need for *Network Independent Digital Identifiers* and for *Services Optimized End to End* as layers = an integrated approach may address all three challenges. A new way to approach ***how names are mapped to network addresses*** and resources in real time can be combined with ***applications grouped appropriately as services layers*** *(Network Slices)* to ensure the isolation of applications from both the network and one another as ***inherent security*** demands.

The best solutions will address multiple challenges at the same time or enable otherwise vastly complex challenges to be dramatically simplified. One key example is security.

Security, Network Independent Identifiers and Services Optimized End to End can be resolved better together

Security must become inherent in the network design not 'plastered on' after the fact. A key component of a best-in-class approach to security is ***isolation***. In the world of Network Functions Virtualization (NFV) this isolation must be both logical and physical. By mapping identifiers dynamically to network addresses and containing applications in separate layers we can keep services and applications from ever seeing network addresses and, if done right, when an application request for authentication is rejected it should ***not even see the mechanism that rejected it or know why it was refused***. That way the application cannot turn around and hack the access mechanism.

Unless names and identifiers can be isolated from network addresses there is no inherent security. The internet today assumes that everyone can access everything and then adds restrictions. We need an approach that does the opposite.

Quality of Service and the Ability to Guarantee it are at the heart of multiple critical service markets

Network Slicing is all about matching the right Class and Quality of Service or QoS to every application – for example, ***real time two-way video*** and ***file downloads*** would operate over different *'Slices'*. If Network Slices and End to End (E2E) Quality of Service Guarantees can only be delivered over VPNs or tunnels with dedicated physical resources they just become silos of 'nailed up' assets that cannot be allocated dynamically - undermining the value of dynamically shared NFV capabilities.

QoS and End-to-End service level guarantees are the pre-requisite not only for low latency apps like ***remote robotics control*** and ***autonomous vehicles*** but also for financial transactions such as ***mobile money*** and ***ecommerce*** and even for the most basic of SDN enabled services ***'bandwidth on demand.'***

Not only do very low latency apps become impossible without improved congestion control that delivers something better than TCP's 'Best Efforts', but financial transactions that demand almost instantaneous processing cannot be handled.

Similarly, while we have grouped markets for each of the seven challenges, in some cases *one key market will be the driver for a specific challenge or a couple of them*. A good example is IoT.

IoT Needs both Unique Identifiers and Security

IoT will go nowhere without mechanisms to identify vast number of devices that are not tied to network addresses. The conventional internet approach to IoT addressing is not only **inherently insecure** and hackable but also simply infeasible as we will run out of network addresses even with IPv6.

Alternatively a *couple of markets may need the same challenges* to be resolved.

Fixed Mobile Convergence (FMC) and Cloud Data Centers both need Seamless Layer 1 and Layer 2 Access and Global Cloud support for Seamless vLANs

True ***Fixed Mobile Convergence (FMC)*** must by definition be independent of ***both*** physical access and the vast array of layer 2 access protocols. Even if we standardize on Ethernet for fixed services, there is ***no limit to the number of layer 2 wireless protocols mobile standards will invent.*** And the 5G vision demands interworking services across a wide array of those mobile access networks.

In addition, if public Service Provider Data Centers and Cloud vLAN services are to become seamlessly available - both regionally and globally - today's layer 2 vLAN approach presents a problem, since vLAN connectivity e.g. with Virtual Extensible LAN (VXLAN) - is inherently limited to about 1 million addresses. ***FMC Video Content Delivery Networks, Cloud Data Centers*** and ***Software Defined Data Centers*** (SDDCs) probably need at least an order of magnitude more than that for Cloud Services. We need new mechanisms that enable Data Centers and the Cloud to connect as seamlessly as if they were on the same LAN.

A common approach that would allow seamless global layer 2 networking would not only remove these significant obstacles but would also open up major new opportunities for ***Telco Global Cloud and Interworking*** services.

Bursty Traffic Optimization

And finally we must find *new ways to manage bursty traffic that today disrupts traditional voice and data flows* so as to ensure any Class of Service at all. The voice traffic models of the 1950s that drive both voice and data networking today are inadequate to handle ***huge bursts of video*** or ***peer to peer live Broadcast Streaming*** *in the same mix* with such things as ***sensor alerts***, ***voice calls*** and ***low priority messaging***.

Even Gigabit pipes cannot always deliver services without experiencing massive congestion unless we adopt new approaches to bursty traffic optimization with E2E guaranteed QoS on an application by application or service layer basis. Resolving this network focused challenge will become a critical enabler for two of the other challenges - *Quality of Service Guarantees* and the *E2E Services without Tunnels for 'Network Slicing'*

Where multiple network challenges are resolved together, Service Providers can evolve to a Next Generation Architecture that simplifies the escalating complexity of today's congested network.

2. Requirements to Meet the Seven Challenges

For each of the seven challenges specific user functionality is required as summarized below.

Table B. Seven Challenges demand Specific Functionality

	Challenge	Required User Functionality	Description
1	Network Independent Personal or Unique Digital Identifiers	**Vast Numbers of IDs or 'Names' that are not Network Addresses**	**Scalable Naming AND Dynamic Address Assignment.** There is an obvious difference between a person's name and his address. Any address change must not force users or things to change their names if they move to a new address.
2	Inherent Security	**Security through isolation of Applications from one another and from Network Resources**	**Security not only for Financial Transactions, Signaling Network and Encrypted Communications, but Inherent in every application.** *Apps that are not validated for access should be isolated from what they are not supposed to see.* ***Refused apps should not even see the Access Request Mechanism or any related Network Address***
3	Seamless Layer 1 *and* Layer 2 Service Access	**Services that operate not only over any Physical Transport but also over any layer 2 protocol fixed or mobile**	**Converged Services Access** Seamless End to End (E2E) Service from any local access network to any other with seamless converged access at both Physical Transport Layer and Layer 2. Winners will be service providers who can originate and terminate services seamlessly from any access network to any other.
4	Unlimited Global Layer 2 support for vLANs	**Seamless Global Connectivity for vLANs**	**Global Connectivity for Telco & Enterprise Hybrid Clouds.** Users need the same simple access to any Cloud or Remote Corporate Data Center that they get on a Local Area Network (LAN)
5	Services Optimized End to End without Tunnels or VPNs	**End to End Service Layers without VPNs and Tunnels**	**Requests for QoS and Service Level Agreements (SLAs) that support multiple Classes of Service above 'best efforts'.** The Promise of Class of Service (CoS) guarantees for 5G and pre-5G 'Network Slicing' demands a new approach that does not require MPLS tunnels or VPNs
6	Quality of Service (QoS) guarantees better than Internet 'Best Efforts'	**Congestion Avoidance instead of Queuing**	**Pro-Active Congestion Avoidance. The** Internet was designed for unreliable transport that has time to retransmit everything in case of congestion or network resource failure. TCP latency becomes too great in Next Gen. Broadband networks over 20 nodes. So throwing away packets when queues get too long and then restarting all transmissions is likely to make congestion far worse.
7	Bursty Traffic Optimization.	**New Traffic Model for Huge Bursts of Broadband Traffic**	**New Traffic Management Approaches for 'Extremely Bursty' Broadband Traffic.** Ability to optimize the mix of all types of network traffic from High Bandwidth Bursts to low latency alerts

Although each of these requirements may appear relatively obvious they cannot be met on a massive scale on today's public Internet or Service Provider networks.

3. Solution Approaches to Address the Requirements

To respond to the needs identified above we summarize in the followings table some possible approaches for each of the market groups identified in the seven categories and list some of the technical requirements as well as possible solutions.

Table C. Generic Requirements and Solution Approaches by Market - Challenge 1

	Major Markets Impacted	Requirements for 1. Network Independent Personal or Unique Digital Identifiers	Possible Solution Approach	Suggested Approach
1.	• **Mobility as a 'just' a Dynamic Addressing Problem** • **Logical eSIM and other Personal Identity Mgt. independent of Phone Numbers and Device IDs** • **IoT and M2M** • **Services with huge number of user equipment (UE) terminations e.g. Assets Tags, RFIDs or Smart Car Parts**	• **Names of any type and number should be mapped in real time to available addresses that are assigned independently**. • Names should be 'inherently mobile' like SIM cards not associated with 'Ports on Switches' or nailed to appliances/devices. • Even the fixed network should allow that computers - especially robots - may eventually move even if they cannot all walk…yet. • In addition full **Context Awareness** depends critically on associating unique information about users and their 'toys' with *personal or device identifiers that are totally independent of any network, data center, geographic location* etc.	**Application Specific Name Spaces for billions of IDs that allow Service Providers to offer truly Personal or Application Specific Device Identifiers and IoT 'Name Spaces' on any Network independent of the network resource addressing scheme.**	Personal/Device. IoT or OTT App IDs map dynamically to network addresses including new network and legacy IP addresses

Each of the remaining six market groups follow below.

Note: The solutions and approaches proposed here are designed to stimulate thought and discussion rather than provide final definitive answers.

Table C. Generic Requirements and Solution Approaches by Market - Challenges 2 and 3 (Continued)

	Major Markets Impacted	Requirements for 2. Inherent Security and 3. Seamless Layer1 *and* Layer 2 Service Access	Possible Solution Approach	Suggested Approach
2.	• **Security for Critical Transactions like eCommerce** • **Security for Network resources** • **Security for Everyday Users**	• **Isolate layers from one another and only allow a layer to request resources and receive responses from layers immediately above and below. If an application is not allowed access it will *never even see the connection* information. 'You cannot hack what you cannot see'. Apps should never see Network Addresses and especially not Global Addresses** • Critical to separate User Apps and Services from even seeing each other. Many security attacks occur because an app can see (or penetrate) another app or get at network addresses of another app that it was never supposed to know. • In Next Gen. Networks it is also critical to isolate Signaling, NFVI/Hypervisor Control and DNS network services from **end user apps.** • Internal Operator Application Requests should have their own Secure Layer(s)	**Inherently Secure Layers for every Application Service to isolate User Services from Network Attacks and Network Services from Application Attacks**	Secure Layers where members of the layer authenticate with each other to gain admission to the layer. Must avoid Physical VPNs or Tunnels that create 'nailed up' Silos and so lose all the efficiencies of Network Function Virtualization (NFV) dynamic resource sharing
3.	• **Fixed Mobile Convergence (FMC)** • **Multi-Access and Multi-Device Voice and Video 'Delivery Anywhere Anytime'**	• **Applications/ Services should be Layer 1 AND Layer 2 Access Agnostic so that any service can connect across any mobile or fixed access network especially 3G, 4G, 5G, WLAN and Carrier Ethernet.** • Users should be able to originate and/or terminate 'any service anywhere over any physical transport and protocol'.	**Seamless Interworking** of any combination of Layer 2 protocols over any physical transport. Access over any Layer 2 can originate and/or terminate a service for fixed Cable, fixed Telco, Wi-Fi and Mobile Operators to deliver seamless service for: • IoT • Video/Content • Automotive	Truly multi-protocol Bridge/Router for any Layer 2 Or potentially future Unified Layer 2 Protocol Chipset.

Table C. Generic Requirements and Solution Approaches by Market -- Challenges 4 and 5 (Continued)

	Major Markets Impacted	Requirements for 4. Unlimited Global Layer 2 Support for vLANs and 5.Services Optimized E2E without Tunnels or VPNs	Possible Solution Approach	Suggested Approach
4.	• **Global Cloud Providers - Google, AWS, Azure etc.** • **Multinational Enterprise Networks** • **Software Defined Data Centers (SDDCs)**	• **Layer 2 vLANs and Cloud Services should be able to connect seamlessly** between any LAN and/or multiple Software Defined Data Centers (SDDCs) to multiple services across competing Cloud Providers (AWS, Azure, Google etc.). • Google and other Cloud Providers would potentially love to **design their Global Data Center Networks as if everything was connected on a single vLAN.** • E2E connectivity at Layer 2 could dramatically simplify networking and reduce the number of bridge/routers required. This would simplify the network and thereby reduce the energy consumption by Service Providers	Allow seamless regional or global connectivity without tunnels that makes multiple vLANs look like a single network and avoid estimated one million address vLAN limit	New simple bridge/router that links across multiple vLANs etc.
5.	• **End to End (E2E) Service Layers with guaranteed Quality or Class of Service (CoS) is essential for SLAs and Consumer Experience Management (CEM)** • **5G and Pre- 5G 'Network Slicing' needs E2E guarantees so every app or Service gets exactly the 'Class of Service' it requires**	• **Upper Layer End to End (E2E) Services and soon 'Network Slices' must be able to request and actually get the requested QoS/CoS** which must not be overridden by 'best efforts' of TCP/IP at lower layers. And must not require 'nailing up' costly IPSec/ MPLS tunnels or VPNs. • *Net Neutrality* can only work in SDN controlled Next Gen. Networks once ***every user can select and get exactly what each selected narrowband or broadband app requires.*** • The Operator's **NFV Business Case for multiple 'nichey' IoT Verticals** depends on E2E Service Layers with diverse QoS and Service Chains being able to share all lower layer network Physical Network Function (PNF) resources dynamically among diverse Virtual Network Functions (VNFs)**.**	Every layer can negotiate with the layer below it for the resources it requires Important to avoid 'silos' that are 'nailed up' via VPNs to dedicated physical network resources. TCP mechanisms today pre-empt upper layer QoS and SLA requests with 'best efforts'	Architecture must allow for layers *(slices)* that operate not only E2E from user application to server, but also across segments of the network e.g. 'RAN slice' or 'Core Service Cloud Slice' etc.

Table C. Generic Requirements and Solution Approaches by Market - Challenges 6 and 7 (Continued)

	Major Markets Impacted	Requirements for 6. Quality of Service (QoS) guarantees better than Internet 'Best Efforts' and 7. Bursty Traffic Optimization	Possible Solution Approach	Suggested Approach
6.	• **Low Latency apps** • **Remote Robotics** • **Autonomous Vehicles** • **eCommerce/ Financial Transactions**	• **Next Gen. Broadband moves too fast with too much traffic across too many nodes to wait for long queues to develop before handling congestion. To ensure reliable delivery and avoid network collapse, pre-emptive congestion management and new traffic monitoring are needed.** • Need new model for Next Generation High reliability Low Latency Broadband networks that operates more like Banking and Airline Reservation Networks do today i.e. 'state aware' Transactions Processing. • Predicting and Pre-empting congestion will both improve performance and reduce the energy required for constant re-transmission. It has been estimated that today the average internet packet is retransmitted 1.5 times which is very wasteful.	Real Time service and resource layer traffic data should be used to predict and pre-empt massive congestion floods that can occur in nanoseconds and lead to outages.	Predictive Pro-Active Traffic Management based on feedback from every layer
7.	• **Two Way Video** • **Live User Originated Streaming** • **4K Video Download for Mobile Devices** • **Remote Drone or Driverless Car Configuration and Control**	• **To achieve low latency high throughput networking need a true Broadband Traffic Model that allows multiple applications to share all the 'Broadband Capacity on Demand'** • Traffic Models today are still based on Poisson/Weibull arrival rate models of the 1940s voice network. Bursty Video and even Data transfers don't look like voice traffic.	Next Gen. apps e.g. massive live uplink video streaming will create unpredictable 'bursts' of traffic in milliseconds or less that must be redirected instantaneously before content queues overwhelm traditional routers. New diverse routing and traffic models are required. *Example:* Think of bubbles moving down an Elastic 3D 'Pipe' based on priority, policy and embedded intelligence not bumping into each other. Just like Collision Detection and Avoidance in Wi-Fi networks	Dramatically better traffic management will improve capacity utilization by co-ordinating big and small 'bubbles' of Low and High Priority Traffic' in an Elastic 3D space with Collision Avoidance mechanisms.

4. Initiatives for Next Generation Networking

As can be seen from the previous section there is significant work to be done to address these challenges. And there are massive implications if they are not addressed. The good news is that recent standards and EU initiatives are starting to address the requirements and approaches needed.

ETSI Next Generation Protocols (NGP) Industry Specification Group

In January 2016 ETSI opened a new Industry Specification Group (ISG) to commence work on Next Generation Protocols (NGP) to look at "evolving communications and networking protocols to provide the scale, security, mobility and ease of deployment required for the connected society of the 21st century."

This new protocol standards initiative was motivated by the fact that "the industry has reached a point where forward leaps in the technology of the local access networks will not deliver their full potential unless, in parallel, the underlying protocol stacks used in core and access networks evolve. The development of future 5G systems presents a unique opportunity to address this issue, as a sub-optimal protocol architecture can negate the huge performance and capacity improvements planned for the radio access network."

Changes are needed if the legacy fixed Internet is not to become the bottleneck for new high performance 5G mobile access and other technologies.

In May 2016 NGP published an initial White Paper on '*Next Generation Protocols – Market Drivers and Key Scenarios'* and delivered an introductory Webinar.

In October the Next Generation Protocol (NGP) Industry Specification Group (SG) published its revised 'NGP Scenario Definitions' and ran an NGP Forum at SDN World Congress. The PRISTINE EU Initiative also ran a workshop on Next Generation Architecture.

European Commission ICT Initiatives: PRISTINE and ARCFIRE

Over the last ten years the European Commission has funded several initiatives for Next Generation Networking. As part of the 7th. Framework Programme (2007-2013)

PRISTINE was one of the initiatives funded as part of EU Future Networks - See PRISTINE Fact Sheet. The program's initial goals are to design, develop and implement innovative internals for 'Recursive InterNetwork Architecture' (RINA) including programmable functions for: *security of content* and *application processes* as well as support for *QoS* and *congestion control, protection* and *resilience*, more efficient *topological routing*, and *multi-layer management* for handling configuration, performance and security. RINA is an emerging 'clean-slate' approach centered on ***Inter-Process Communications (IPC)*** and designed to support ***high scalability***, ***multi-homing***, ***built-in security***, ***seamless access to real-time information*** and ***operation in dynamic environments***. PRISTINE ran a workshop at the 2016 SDN and OpenFlow World Congress on new approaches for handling ***configuration, performance*** and ***security*** in this next generation architecture.

The EU's Horizon 2020 program has also now funded multiple ICT projects including ARCFIRE to address current limitations and the commercial viability of the RINA approach and its applicability for full integration of distributed computing and networking. See tutorial slides presented in Athens in June at EUCNC 2016 by both PRISTINE and ARCFIRE.

5. Legacy Internet was designed in 1970s for narrowband services

These initiatives are designed to address some of the limitations of today's Internet that was originally designed for the narrowband world of the 1970s and 80s and now needs to be rethought for the high bandwidth, massively scalable, low latency broadband network which is needed for the 21st Century.

Internet was born into the world of the 1970s

To put the Internet timeline in perspective, ARPANET performed its first successful Internetworking demonstration at the International Conference on Computer Communications (ICCC) in October 1972 forty four years ago. This was only a year after the first ever commercial microprocessor was announced by Intel in November 1971. In 1976 DARPA forwarded its Specification for **TCP version 2** to MIT. That same year the first modem at 9.6 Kbps launched commercially by Codex (later Motorola) was viewed as a revolutionary technology.

By 1978 TCP Version 2 was modified to accommodate "all kinds of network interconnections" and split into two layers, network and transport as **TCP/IP**.-That was the same year that the first Ethernet LAN patent was issued.

Mobile Networking, Distributed Computing and Client Server Networking in 1980s/90s

It was not until 1983 that the first 1G cellular voice only network became operational in the US. The first standard mobile data networks only emerged in the late 1980s and 1990s - initially on packet radio networks (Mobitex & iDEN) then as an overlay on voice networks with CDPD for 2G/2.5G and EV-DO, and UMTS/HSPA for 3G.

Ethernet LANs became widespread in the 1980s as minicomputers proliferated and after the IBM business personal computer (PC) was introduced in August 1981.

By 1985 the global Internet had spread to Europe and the *Domain Name System* could rapidly map human readable domain names to the IP network addresses they represent. In 1988 the first direct IP connection between Europe and North America was made; and the Internet grew rapidly in the developed world expanding to the developing world in the late 1990s.

By 1988 the success of the personal computer had created a new model of corporate computing, client server computing." And client server computing has pre-empted the distributed minicomputer networking model ever since. This centralized model has worked well for data centers and the traditional TCP/IP based Internet.

The WorldWide Web "an information space in which resources are identified by global identifiers called Uniform Resource Locators (URLs)" was invented by Tim Berners-Lee in 1989. The web could have leveraged a flat distributed network effectively. But the web only became readily accessible after the Mosaic browser - precursor of Netscape - arrived in 1993. By that time the PC client server hierarchical model was dominant.

In the metro area Wide Area Network (WAN), although synchronous T1 had been used for point to point TDM connections by businesses since the mid-1980s, they were very expensive.

21st Century Evolution

Affordable consumer IP based broadband access connections of 1Mbps or higher only became widespread in the 21st. Century with the glut of IP capable unused bandwidth following the burst of the dot.com bubble in 2001.

Residential Broadband is now routinely offered to homeowners in North America, Western Europe and Asia Pacific at rates of 3Mbps to 20Mbps or more.

And we have seen dramatic increases in small business and enterprise bandwidth with the advent of widespread Carrier Ethernet that has evolved steadily from 100Mbps in the early part of the century to 1Gbps for business users. Rates up to 100Gigabit Ethernet were standardized in 2010 and 2011.

Similarly mobile rates have accelerated dramatically with 4G/LTE now routinely delivering aggregate rates of 100Mbps and 5G is being tested at 1Gbps.

Despite these massive changes in network communications throughput rates, the internet architecture and its protocols have remained largely unchanged.

And ***critical broadband service issues are now becoming apparent that higher data rates alone cannot resolve.***

6. Time to Rethink High Performance Next Generation networking

As noted during the May the ETSI NGP Webinar many aspects of 5G, IoT and scalable broadband networking demand new approaches to achieve the ***scale and scope demanded by new broadband services***. Specifically Andy Sutton *NGP Editor and Rapporteur and Principal Network Architect at BT* commented that "The industry has reached a point where forward leaps in the technology of the local access networks (such as LTE-A, G.FAST, DOCSIS 3.1 and 5G) will not deliver their full potential unless, in parallel, the entire infoComms protocol stacks evolve more holistically."
Specific areas targeted for new approaches by ETSI NGP are:

- **Embedded Mobility**
- **Ability to Cross-connect diverse IOT networks at scale.**
- **Secure connections across everything**
- **High-throughput transport delivering super media**
- **Self managing, autonomic networks**

The recent 'NGP Scenario Definitions' publication provides specific scenarios for eleven key areas:

- *01 Addressing*
- *02 Security*
- *03 Mobility*
- *04 Multi-Access*
- *05 Context Awareness*
- *06 Performance*
- *07 Network Virtualisation*
- *08 IoT support*
- *09 Energy Efficiency*
- *10 e-Commerce*
- *11 MEC Mobile Edge Computing*

Strategy Analytics has prepared this report to offer an additional perspective on seven specific areas that we have identified as critical for new market opportunities; and to specify some of the requirements for the solutions that Service Providers need to serve several multi-billion dollar market opportunities. We highlight the need for:

- **Network Independent Personal or Unique Digital Identifiers**
- **Inherent Security**
- **Seamless Services over any layer 1 and layer 2**
- **Global layer 2 support for vLANs**
- **Services Optimized End to End (E2E)** without Tunnels or VPNs
- **Quality of Service (QoS) guarantees** better than Internet 'Best Efforts'
- **Bursty Traffic Optimization**

Both generic capabilities like ***Inherent Security*** and ***Bursty Traffic Optimization*** as well as other requirements that are demanded for ***IoT Services***, ***Fixed Mobile Convergence***, ***Cloud***, ***Network Slicing***, ***5G*** and ***4K Mobile Video*** cannot be met in today's networks. Such challenges cannot be addressed solely by adding massive additional bandwidth to traditional networks.

This report has tried to decompose the requirements for next generation broadband services so that it is possible to see what types of solutions are required to achieve high performance cost effective delivery over next generation networks.

New approaches are needed and work is now beginning to address them on a significant scale.