FUJITSU

Technical Report

Carrier Software Defined Networking (SDN)

March 2014

0.1. Preface

This Fujitsu technical report was commissioned by Ofcom in January 2014. The report has been compiled by Fujitsu technical experts, specifically to inform Ofcom about Software Defined Networking (SDN) and Network Functions Virtualisation (NFV).

The reader should be aware that this report does not necessarily reflect Fujitsu's corporate view on SDN and NFV. Rather, it provides the results of a reasoned and objective analysis of the state of the industry. Where the report presents any views on regulatory or business impacts, these are the views of the authors and not those of Ofcom.

In coming to its conclusions the report has analysed in detail the work of the key standards bodies and researched a large amount of technical data, marketing information, and product literature. The report provides a full list of references, although due to the transient nature of the web these hyperlinks may cease to work over time.

To inform the work, the authors also conducted detailed confidential interviews with some carriers and vendors, in order to understand how they saw the technology impacting their business. As these interviews are confidential, it is not possible to acknowledge the contribution of the individuals concerned. However, the authors would like to extend their thanks to all who responded to our questions and their management who sanctioned the time of some of their most valuable staff.

The authors would also like to thank Tim Chown, Dan King, Meral Shirazipour and Chris Sidwell-Smith for their assistance.

Any questions about this report should be addressed to Chris Gallon at Fujitsu (chris.gallon@uk.fujitsu.com).

Questions about Ofcom's work in the area of SDN and NFV should be addressed to Robindhra Mangtani at Ofcom (Robindhra.Mangtani@ofcom.org.uk).

0.2. Glossary of Terms and Abbreviations

The glossary lists the terms and abbreviations that apply specifically to this document.

Note: The terms and abbreviations used in this document may have different meanings in other contexts.

ALA	Active Line Access
ANCP	Access Node Control Protocol
ANDSF	Access Network Discovery and Selection Function
API	Application Program Interface
ARPU	Average Revenue Per User
ASIC	Application-Specific Integrated Circuit
BBU	Base Band Unit
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BNG	Broadband Network Gateway
BOF	Birds of a Feather
BRAS	Broadband Remote Access Server
BSS	Business Support System
CAPEX	CAPital Expenditure
CLI	Command Line Interface
CDN	Content Delivery Network
CDPI	Control Data Plane Interface
COTS	Commercial Off The Shelf
CPE	Customer Premises Equipment
CPRI	Common Public Radio Interface
CPU	Central Processing Unit
C-RAN	Cloud Radio Access Networks
DDIO	Data Direct Input Output
DDoS	Distributed Denial of Service
DG	Discussion Groups
DLNA	Digital Living Network Alliance
DNS	Domain Name System
DPDK	Data Plane Developer Kit
DPI	Deep Packet Inspection
D-SBG	Data Path - Session Border Gateway
DSLAM	Digital Subscriber Line Access Multiplexer
DWDM	Dense Wavelength Division Multiplexing

ECMP	Equal Cost Multiple Path
EMS	Element Management System
eNodeB	Evolved Node B
EPC	Evolved Packet Core
ERO	Explicit Route Object
eTOM	Enhanced Telecom Operations Map
ETSI	European Telecommunications Standards Institute
EU	European Union
E-VPN	Ethernet Virtual Private Network
FAWG	Forwarding Abstraction Working Group (ONF)
FCAP	Fault, Configuration, Accounting, Performance, Security
FCoE	Fibre Channel over Ethernet
FEC	Forward Error Correction
FTTdp	Fibre to the Distribution Point
FTTH	Fibre to the Home
GEA	Generic Ethernet Access
GMPLS	Generalised Multiprotocol Label Switching
GPON	Gigabit Passive Optical Network
GPRS	General Packet Radio Service
GRE	General Routing Encapsulation
GTP	GPRS Tunnelling Protocol
HetNet	Heterogeneous Network
HGI	Home Gateway Initiative
I/O	Input / Output
I2RS	Interface to the Routing System
IAAS	Infrastructure As A Service
ICT	Information and Communications Technology
IDPS	Intrusion Detection and Prevention Systems
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IMS	IP Multimedia Subsystem
IOTLB	Input Output Translation Look aside Buffer
IP	Internet Protocol
JSON	JavaScript Object Notation
L2VPN	Layer 2 Virtual Private Networks
L3VPN	Layer 3 Virtual Private Networks
LDP	Label Distribution Protocol
LER	Label Edge Router

LLU	Local Loop Unbundling
LSDB	Link State Data Base
LSP	Label-Switched Path
LTE	Long Term Evolution
M2M	Machine to Machine
MAC	Media Access Control
MANO	Management and Orchestration
MPLS	Multiprotocol Label Switching
MPLS-TE	Multiprotocol Label Switching - Traffic Engineering
MPLS-TP	Multiprotocol Label Switching - Transport Profile
NBI	NorthBound Interface
NDM	Negotiable Datapath Models
NE	Network Element
NETCONF	Network Configuration Protocol
NFV	Network Functions Virtualisation
NIC	Network Interface Controller
NICC	Network Interoperability Consultative Committee
NID	Network Interface Device
NNI	Network-to-Network Interface
NPU	Network Processing Unit
NSC	Network Service Chaining
NTU	Network Termination Unit
NVGRE	Network Virtualisation using Generic Routing Encapsulation
OAM	Operations Administration and Maintenance
ONF	Open Networking Foundation
OPEX	OPerational EXpenditure
OSS	Operational Support System
OTN	Optical Transport Networks
OTT	Over The Top
OVSDB	Open vSwitch DataBase management protocol
PBB-TE	Provider Backbone Bridging - Traffic Engineering
PCC	Path Computation Client
PCE	Path Computation Element
PCEP	Path Computation Element - Communication Protocol
PE	Provider Edge
P-GW	Packet Data Network Gateway
PIA	Physical Infrastructure Access
PKS	Path Key Sub-object

PMIP	Proxy Mobile IP
PSTN	Public Switched Telephone Network
PVR	Personal Video Recorder
QoE	Quality of Experience
QoS	Quality of Service
RACS	Resource and Admission Control Subsystem
REST	REpresentational State Transfer
RFC	Request for Comments
RG	Residential Gateway
RIB	Routing Information Base
ROADM	Reconfigurable Optical Add/Drop Multiplexer
RSVP-TE	Resource Reservation Protocol - Traffic Engineering
RTOS	Real Time Operating System
SBG	Session Border Gateway
SDH	Synchronous Digital Hierarchy
SDK	Software Development Kits
SDN	Software Defined Networking
SGi-LAN	Serving Gateway interface – Local Access Network
SIP	Session Initiation Protocol
SLU	Sub Loop Unbundling
SME	Small, Medium Enterprises
SONET	Synchronous Optical Network Technology
SR-IOV	Single Root-I/O Virtualisation
S-SBG	Signalling - Session Border Gateway
TCAM	Ternary Content Addressable Memory
TDF	Traffic Detection Function
TDM	Time-Division Multiplexing
TED	Traffic Engineering Database
TMF	TeleManagement Forum
TRILL	Transparent Interconnection of Lots of Links
TTP	Table Type Patterns
UDP	User Datagram Protocol
UNI	User Network Interface
vCPE	virtual Customer Premises Equipment
VDSL2	Very-high-bit-rate Digital Subscriber Line 2
vEPC	virtualised Evolved Packet Core
VLAN	Virtual Local Area Network
VNF	Virtual Network Functions

VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
vRG	Virtual Residential Gateway
VULA	Virtual Unbundled Local Access
VXLAN	Virtual Extensible LAN
WAN	Wide Area Network
WDM	Wavelength Division Multiplexing
WG	Working Groups
XMPP	Extensible Messaging and Presence Protocol
XNC	Extensible Network Controller

0.3. References

[Ref 1] "AT&T Looks To Mitigate Impact Of Saturated Wireless Market With SDN Adoption" Trefis (trefis.com) - 25th February 2014

[Ref 2] "AT&T Launches Supplier Domain Program 2.0" – Press Release - 23rd September 2013

[Ref 3] "Carriers Say SDN Won't Save Capex" - Carol Wilson Light Reading – 30th September 2013

[Ref 4] ONS2014 Keynote: John Donovan, AT&T - March 2014

[Ref 5] "Infonetics: SDN is leading carrier router/switch market into a period of hesitation" - March 4th 2014

[Ref 6] "Software Defined Networking (SDN) - Bridging the Mobile Backhaul Funding Gap" Sue Rudd Strategy Analytics - August 31st 2013

[Ref 7] "Telefonica forges ahead on end-to-end virtualisation of its network" Press Release - 24th February 2014

[Ref 8] OpenDaylight Defense4All tutorial - webpage was last modified on 30th January 2014

[Ref 9] "SDN, NFV, and open source: the operator's view" Mark Leary, Gigacom Research - March 2014 (sponsored by the OpenDaylight project)

[Ref 10] Future electronic communication markets subject to ex-ante regulation – Ecorsys 18th September 2013

[Ref 11] NICC ND1644 – Architecture for Ethernet ALA V1.1.1 (2010-12)

[Ref 12] "Watchdogs have grave concerns over Netflix deal with cable giant Comcast" Dominic Rushe, The Guardian - 24th February 2014

[Ref 13] "Net neutrality: Industry MEPs want stricter rules against blocking rival services" European Parliament Press Release Ref: 20140318IPR39210 - 18th March 2014

[Ref 14] "The Guardian – Edward Snowden – Investigative Journalist"

[Ref 15] "Demand Attentive Networks" – The IET - November 2013

[Ref 16] The Openstack Project

[Ref 17] IETF RFC 4447 (Proposed Standard) Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) - Last updated: 2nd Feb 2013

[Ref 18] Google - B4: Experience with a Globally-Deployed Software Defined WAN - August 2013

[Ref 19] ITU-T Rec G.694.1 - Spectral Grids for WDM Applications: DWDM Frequency Grid - 02/2012

[Ref 20] Broadband Forum TR-101 - Migration to Ethernet-Based DSL Aggregation - April 2006

[Ref 21] "SoftRAN: Software Defined Radio Access Network" Aditya Gudipati, Daniel Perry, Li Erran Li, Sachin Katti - August 2013

[Ref 22] C-RAN The Road Towards Green RAN White Paper version 2.6 – China Mobile Research Institute Ver 2.6 - September 2013

[Ref 23] Transform Your Mobile Network Environment with the World's First Commercial Cloud Based LTE Enhancement Solution KT LTE WARP Product Literature - March 2013

[Ref 24] ETSI Network Functions Virtualisation Industry Specification Group (NFV ISG) - October 2013

[Ref 25] Broadband Forum SD-326 – Flexible Service Chaining - Work-in-Progress

[Ref 26] Broadband Forum WT-317 – Network Enhanced Residential Gateway - Work-in-Progress

[Ref 27] Home Gateway Initiative - HGI-RD008-R3 - HG Requirements for Software Execution Environment Andrea Sayegh - June 2011

[Ref 28] Juniper Networks Cloud CPE Services - webpage published October 2013

[Ref 29] MEF 33 - Ethernet Access Services Definition - January 2012

[Ref 30] OpenDaylight Service Providers Edition - February 2014

[Ref 31] OpenContrail Architecture Documentation - Bruno Rijsman and Ankur Singla November 20th 2013

[Ref 32] Open Networking Forum - Software-Defined Networking: The New Norm for Networks - White Paper April 13th 2013

[Ref 33] Open Networking Forum - SDN Architecture Overview - V1.0 December 12th 2013

[Ref 34] Open Networking Forum - OpenFlow Switch Specification - Version 1.4.0 (Wire Protocol 0x05) October 14th 2013

[Ref 35] Open Networking Forum - Outcomes of the Hybrid Working Group - March 2013

[Ref 36] Open Networking Forum - OpenFlow Management and Configuration Protocol - OF-CONFIG 1.2 January 2014

[Ref 37] I2RS Interface to the Routing System (i2rs) - Charter for Working Group - charter-ietf-i2rs-01 - Approved January 29th 2013

[Ref 38] I2RS An Architecture for the Interface to the Routing System - draft-ietf-i2rs-architecture-02 - Work-in-Progress - February 12th 2014

[Ref 39] I2RS Interface to the Routing System Problem Statement - draft-ietf-i2rs-problem-statement00 – Work-in-Progress – August 16th 2013

[Ref 40] I2RS Routing Information Base Info Model - draft-ietf-i2rs-rib-info-model02 - Work-in-Progress – February 14th 2014

[Ref 41] I2RS An Information Model for Network Topologies - draft-medved-i2rs-topology-im-01 - Work-in-Progress – October 21st 2013

[Ref 42] I2RS Topology API Use Cases draft-amante-i2rs-topology-use-cases-01 - Work-in-Progress - October 20th 2013

[Ref 43] IETF RFC 6241 Network Configuration Protocol (NETCONF) - June 2011

[Ref 44] Netconf white paper “NETCONF Ready for Primetime or Work in Progress?” - David French V1.0 January 2009

[Ref 45] IETF RFC 6020 YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF) - October 2010

[Ref 46] A YANG Data Model for Routing Management draft-ietf-netmod-routing-cfg-13 - Work-In-Progress – January 10th 2014

[Ref 47] RFC 5623 Framework for PCE-Based Inter-Layer MPLS and GMPLS Traffic Engineering - September 2009

[Ref 48] I2RS PCEP Extensions for Stateful PCE draft-ietf-pce-stateful-pce-08 - Work-In-Progress - February 12th 2014

[Ref 49] “In Operation Network Planning” Luis Velasco and Alberto Castro, Daniel King, Ori Gerstel, Ramon Casellas, Victor López - IEEE Communications Magazine - January 2014

[Ref 50] I2RS PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model draft-ietf-pce-pce-initiated-lsp-00 - Work-In-Progress - December 2nd 2013

[Ref 51] RFC 5440 Path Computation Element (PCE) Communication Protocol (PCEP) - March 2009

[Ref 52] I2RS A PCE-based Architecture for Application-based Network Operations draft-farrkingel-pce-abno-architecture-07 - Work-In-Progress - February 13th 2014

[Ref 53] "Segment Routing" Clarence Filsfils and Christian Martin – Presentation to RIPE 66 - May 2013

[Ref 54] Segment Routing Architecture draft-filsfils-rtgwg-segment-routing-01 - Work In Progress - October 21st 2013

[Ref 55] I2RS PCEP Extensions for Segment Routing draft-sivabalan-pce-segment-routing-02 - Work In Progress - October 16th 2013

[Ref 56] ETSI Network Functions Virtualisation - Introductory White Paper - October 2012

[Ref 57] ETSI GS NFV 001 v1.1.1 Network Functions Virtualisation (NFV) Use Cases - October 2013

[Ref 58] ETSI Network Functions Virtualisation - Updated White Paper - October 2013

[Ref 59] ETSI GS NFV 002 v1.1.1 Network Functions Virtualisation (NFV) Architectural Framework - October 2013

[Ref 60] ETSI GS NFV INF 001 V0.3.6 Network Functions Virtualisation Infrastructure Architecture; Overview - January 2014

[Ref 61] ETSI GS NFV-MAN 001 Management and Orchestration - An Overview Presentation by Mehmet Ersue to IETF #88 - November 2013

[Ref 62] ETSI GS NFV-SEC 001 V0.0.9 Network Functions Virtualisation (NFV); NFV Security; Problem Statement - Work-In-Progress - January 2014

[Ref 63] "Making NFV Work PoCs and Trials" Francisco-Javier Ramon Salguero - Telefonica webcast March 2014

[Ref 64] "TeraStream – A Simplified IP Network Service Delivery Model" Peter Lothberg, Deutsche Telekom - October 2013

[Ref 65] "A Realtime OSS-based SDN Approach" – Pipeline KnowledgeCast Webinar - October 2013

[Ref 66] "Network & Platforms what's next ?" Nicholas Fischbach Colt – November 2012

[Ref 67] "Heavy Reading Implementing the Innovative Edge for Cloud-Based Services" - Stan Hubbard (Juniper sponsored paper) November 2012

[Ref 68] Keynote SDN and OpenFlow World Congress – Carrier vision of SDN – Stu Elby, Verizon – webcast October 23rd 2012

[Ref 69] Alcatel-Lucent, Huawei tout their respective NFV roadmaps - Tammy Parker Fierce Wireless - 19th February 2014

[Ref 70] "Ericsson Unveils Virtual EPC" LightReading - 12th February 2014

[Ref 71] The Open Compute Project - website

[Ref 72] The Open Grid Forum - website

[Ref 73] RFC 5441 A Backward-Recursive PCE-Based Computation (BRPC) Procedure to Compute Shortest Constrained Inter-Domain Traffic Engineering Label Switched Paths – April 2009

[Ref 74] RFC 6805 The Application of the Path Computation Element Architecture to the Determination of a Sequence of Domains in MPLS and GMPLS - November 2012

FUJITSU

0.4. Table of Contents

1. Executive Summary

SDN and NFV will have a significant impact on carrier networks in the next few years. Carriers are already starting to deploy aspects of these technologies and this trend will continue; although the extent to which the claims for SDN and NFV will match the reality of deployment is uncertain. The nature of carrier networks and the current maturity of the technology means that SDN and NFV will be deployed in an evolutionary and not a revolutionary way, and some of the more complex SDN and NFV scenarios will not be deployed for many years, if ever.

The original work on SDN, which had its roots in academia, had a vision of SDN that supported the low level programming of the network behaviour by the application, this allowed the applications to replace the network protocols, or to define their own network protocols. Today a number of academic networks implement SDN in this way and it provides an invaluable tool for technology development and innovation. However, carrier networks have a very different set of customers and design requirements. They will implement SDN and NFV but they will not use it to enable low level network programming by third parties.

Carrier networks will remain fundamentally based on IP, Ethernet and Multiprotocol Label Switching (MPLS) technologies. Carrier interconnects and particularly the Internet peering infrastructure built around the Border Gateway Protocol (BGP) will remain in place. However, SDN and NFV technology will become embedded in carrier networks and this will lead to the increased use of service orchestration, which can be driven by high level programmatic interfaces. These interfaces will offer network abstractions from the carrier to the application and will provide a network API that is broadly similar in scope to some of today's OSS interfaces; but that is more capable and easier for applications to consume.

The introduction of SDN and NFV into carrier networks, and the flexibility that they bring in terms of service configuration and service delivery, may well lead to additional service offerings for residential consumers, business consumers and Over The Top (OTT) service providers. Indeed, a primary motivator for many carriers in looking at the technology is a desire to replicate the OTT providers flexible "fail fast" approach to service development and deployment. In this model services are trialled, deployed on commodity hardware and either discarded if they fail to gain traction, or rapidly scaled out if they take off. This is a very different model to the traditional telco service delivery approach which often requires long lead times dominated by the OSS development, and where scaling decisions have to be made very early on in the development process.

In the case of residential consumers, they are likely to see an increase in tailored offerings from the network that they can order via self-care portals. These services could provide items like Intrusion Detection and Prevention; or possibly even managed home networks using network based virtual Customer Premises Equipment (CPE). From a business perspective, SDN and

NFV offer a range of options for more flexible, virtual private network offerings; and from an OTT provider perspective, the technology is most likely to offer them more efficient ways of using the network to reach their end consumers.

SDN and NFV will also impact the network in ways that the customer cannot directly see, but which may give them significant benefit. Carriers can use SDN and NFV capabilities to maximise the Quality of Experience for their customers, either by the wider application of traffic management, or the ability to easily drop in content optimisation capabilities as the end user's access quality changes.

From a regulatory perspective SDN and NFV create benefits in competition, service innovation should increase, but they also generate risks. If it becomes necessary, for example, to integrate with a network to maximise the Quality of Experience (QoE) of an OTT service, then arguably larger networks and larger OTT providers may benefit. Within the context of EU and national regulation SDN and NFV will provide additional challenges to regulators, for example, in the area of monitoring compliance with the emerging net neutrality legislation. However, in general both of these technologies fit reasonably well with the existing regulatory framework, although the potential for carriers to control how they distribute NFV capability around their networks, and how they permit their customers to access that capability, could potentially cause regulatory issues in certain markets.

One area where the regulation may need further clarification is around the mobile fronthaul services that Cloud-Radio Access Networks (C-RAN) will require to be economic. There is significant evidence that countries with a fibre rich environment suitable for C-RAN, will gain significant benefits over those that are fibre poor; specifically because of the improved spectrum utilisation (and hence bandwidths) C-RAN offers. Because mobile fronthaul services have very special restrictions on the type of access they can use, and because of the economics of deployment, dark fibre availability is a requirement for C-RAN. To date, many countries have viewed the access transport speed rather than the access type as the critical factor for the user experience. In the case of mobile data in city environments, this may no longer be true.

The question of how and when carriers will implement SDN and NFV, and what applications they will target, has been considered by this study. There is a consensus amongst the carrier community that SDN and NFV are of interest, although both are relatively immature technologies. Nevertheless, there is a significant divergence in how individual carriers are considering the technology. Some carriers are adopting an enthusiastic visionary approach, looking to push the boundaries of the technology to gain specific business advantages, typically in cost savings and / or in service agility. Other carriers are taking a more sceptical approach; these carriers are typically looking at specific projects where they can gain quick wins from deploying the technology and trying to limit business disruption, particularly in the area of the Operational Support System/ Business Support System (OSS/BSS). Part of this divergence may be because

of different carrier focus, in terms of their key services, part of it may be due to a lack of consensus on the business benefits of the technology. Arguments are currently being made for big CAPEX and OPEX savings from deploying SDN and NFV, but there are dissenting voices arguing that both savings are likely to be difficult to achieve.

Where SDN and NFV have demonstrated real benefits to carriers, the technology is either being rolled out or is being trialled. Google already deploy SDN for an application in a live network. Colt, Deutsche Telekom and Telefonica have all made announcements about deployments of SDN and or NFV in production networks or live trials. KT have an in-service C-RAN based LTE network deployed in Korea.

In general, carriers will deploy point solutions where SDN can solve key problems for them, without disrupting their existing OSS/BSS systems and processes. SDN implementations that enable incremental and non-disruptive deployments will have a big advantage in carrier networks. Even these deployments may be delayed because of organisational issues within carriers and possible OSS implications. NFV is, to a degree, already happening today within carrier networks for compute intensive applications such as DNS, call control and for small scale network elements such as low functionality enterprise CPE. For mobile networks virtualised Evolved Packet Core (vEPC) capability and flexible service chaining within the SGi-LAN are driving an early deployment of NFV.

The roadmap from pragmatic and tactical SDN and NFV deployment towards more comprehensive architectures will be long and will vary between carriers. It is easier to make the case for changes that can drive additional service revenue or service velocity, than changes related to reducing CAPEX and OPEX. Solutions that trade CAPEX costs for additional integration and incur additional OPEX, such as support and product development costs, are harder still to make for most operators. However, over time it is to be expected that SDN and NFV solutions will increase their footprint in carrier networks and start to impact the OSS, BSS and operations of the carrier. This will result in changes to the way carriers are organised and to the mix of skills that they require from their staff. For example, service development will be very much more agile than it is in today’s networks and will cut across multiple disciplines within the carrier.

While the impact of SDN and NFV on carrier networks is likely to be evolutionary, there is still a potentially significant disruption to the network equipment vendor environment. It is unclear how far carriers envisage taking the commoditisation of hardware that some NFV use cases imply, and there are visions that suggest carriers may wish to bring some vendor capabilities in-house. This environment creates uncertainty and there is some risk that this may in turn delay investment in certain types of network equipment. In order to mitigate this risk, it seems likely that vendors will concentrate on moving value from hardware to software and in improving their portfolios to make their products SDN and NFV friendly. This will allow their products to be easily

integrated into SDN and NFV deployments. This trend can be seen with traditional routing vendors now offering Software Development Kits (SDKs) and specialised SDN controllers that can form part of an integrated solution.

SDN and NFV standardisation is far from complete and missing in some important areas. The work of the Internet Engineering Task Force (IETF) and of the Open Networking Foundation (ONF) on SDN are both important, and both have their place in the solution set. The recent emergence of Segment Routing may also prove to be an important technology within the SDN landscape. In the case of NFV, the work being done by European Telecommunications Standards Institute (ETSI) is acting as a catalyst for the accelerated deployment of the technology. One area of concern that may slow NFV adoption, is that in order to make the technology genuinely open and multi-vendor, a significant amount of work will be required in the area of operations and management. This work that is nascent in the TeleManagement Forum (TMF).

The early stage of standardisation means that individual carriers implementing SDN will pick the most appropriate SDN technology for their chosen use case. This technology may differ according to the network domain and the scope that the carrier is seeking to address. For example, in core networks technologies such as Segment Routing have a big advantage, while service chaining in the carrier data centres may be based on overlay solutions or on OpenFlow versions 1.3 and later. Some SDN use cases have chosen network management protocols like Network Configuration Protocol (NETCONF) to implement the solution. It should be noted that a number of vendors have developed integrated turnkey solutions for specific SDN use cases and in the absence of standards maturity these may provide an easy way for carriers to deploy the solution.

While it is not possible to predict the timescales of SDN and NFV with any certainty, as a general principle, deployments of well-defined point solutions with compelling business cases are either happening, or will happen in the next year to two years. These are typically single domain, single vendor (or known vendor ecosystem). Single domain multi-vendor use cases may take longer because of a lack of standards and the more OSS/BSS integration any use case requires, the longer it will take. The more complex multi-domain, multi-operator use cases are probably five years away, or more, from implementation.

Because different carriers have different visions for SDN and NFV, it is possible that this technology will disrupt the relatively uniform view of network architecture that exists in carrier networks today. This may mean that the medium term future will be one of competing network visions and technologies operating within the existing IP networking space. Of course different carrier networks also have different priorities, and it may be that there is no one size fits all solution for SDN and NFV.

2. Introduction

The world has seen rapid and historically unparalleled changes in technology over the past ten to twenty years, particularly in the area of data centre infrastructure, network communications, and service provider networks. At the heart of these changes is the bandwidth demand explosion driven by end user applications and ubiquitous access through mobile technology. At the same time carriers are facing the challenges posed by steadily falling Average Revenue Per User (ARPU) and the emergence of OTT providers who are consuming an ever larger percentage of end user communications spending.

SDN and NFV are two technologies that carriers are looking towards, to solve some of these issues. Carriers are examining how these technologies can reduce their costs, help them scale their network, and help them offer innovative new services that can provide them with new revenue. Nevertheless, it is also true that SDN and NFV are currently very hot topics in the telecommunications industry, with a huge quantity of publicity and press promoting their capabilities; in the current environment most major new or enhanced products claim SDN or NFV capability. This marketing environment, plus the wide range of ambitions quoted for these technologies, mean that it can be hard to get a feel for how these technologies will be deployed. This report investigates the current state of SDN and NFV within the industry and to provide a reasoned analysis of how these technologies will be utilised in future carrier networks.

The first few sections of the report provide a high level view of the SDN and NFV landscape and its likely impact on the carrier landscape. Specifically:

- Section 3 provides an overview of SDN and NFV, and sets out how they relate to each other, providing an overview of the SDN ecosystem.
- Section 4 looks at the business and regulatory impacts of SDN. This includes the carrier view of SDN and NFV and the likely impact of these technologies on carrier organisations and network infrastructure. This section also considers what new services may be supported, discusses the barriers to SDN deployments, and highlights potential regulatory concerns triggered by these new technologies.

The remainder of the report drills down progressively into SDN and NFV, providing an overview of the use cases and network architectures of SDN and NFV; examining the technology behind SDN and NFV and considering what has been, and may be deployed. These sections form a technical analysis, suited to engineers seeking a broad overview of the technology; specifically:

- Section 5 looks at the individual use cases and the business needs they are trying to meet.
- Section 6 looks at the end-to-end architecture of carrier networks and how the various SDN and NFV solutions may impact it.
- Section 7 provides an overview of the key SDN technologies, their current state and open issues that still require resolution.
- Section 8 investigates the work of ETSI NFV in detail, its ambition, solution and looks at some of the issues and limitations of NFV.
- Section 9 provides an overview of how SDN and NFV solutions will impact the OSS.
- Section 10 highlights existing and likely future deployments and considers the implications for equipment vendors.
- Section 11 provides a list of related projects and initiatives.
- Section 12 provides a rough estimate of timescales for SDN and NFV deployments in carrier networks.

In compiling this report, Fujitsu has drawn on a wide range of referenced material and carried out a detailed review of the work of the key industry forums working on SDN and NFV technologies. A number of confidential interviews were also carried out with fixed and mobile carriers, a major IP routing vendor and a supplier of optical transport solutions. This information was also used to inform the report.

3. Software Defined Networking Landscape

3.1. What is SDN

There are a large number of definitions that are used in the industry to describe what SDN actually is. Some of these views are closely bound to a particular protocol, equating SDN with OpenFlow, others define it simply as the separation of the network control plane from the forwarding plane, and others talk of programmable networks. At a high level it is more useful to consider what SDN is used for rather than how it is defined.

SDN is an enabler to allow an Orchestration function to configure end-to-end services within the network. The Orchestration function interacts with SDN controllers which provide the network component of this orchestration. The SDN controller configures the forwarding of flows within a network and steers those flows to different locations depending on the requirements of the orchestrator. This configuration of flows may replace, over-ride, or complement control plane mechanisms that exist within the network. The orchestration function may expose aspects of the networks to its clients in order to enable them to configure their services via Application Program Interface APIs (application centric networking).

There are different SDN approaches to allowing an orchestration function to control the network forwarding. Typically, these all offer some degree of control plane centralisation and the separation of it from the data plane. This may use protocols such MPLS Segment Routing, Path Computation Element - Communication Protocol (PCEP), or OpenFlow to control the underlying network switches and routers, and may be deployed on a network wide basis or just within specific network domains. SDN can also be deployed in networks by building a tunnel overlay and using SDN protocols to control just the end points of these tunnels. This is known as an overlay solution and is often used to provide SDN in a constrained network domain (such as a data centre).

Within carrier networks SDN use cases can be summarised into three key groupings:

- Service Orchestration and automation use cases.
- Application Centric Networking
- Network Functions Virtualisation support.

Each of these uses cases requires different aspects of SDN technology to implement it, and each has a different set of business drivers behind it.

This report takes a broad view of SDN and, therefore, views NFV as part of the SDN landscape, partly because the two technologies are complementary, but mainly because many of the

economic and business cases made for each technology also require the support of the other technology.

It is important to note, that while this report considers SDN and NFV to be part of the SDN landscape, and hence both are in scope; they are different technologies. At a technical level, SDN implementations do not require NFV, and NFV implementations do not require SDN.

3.2. What is NFV?

Network Functions Virtualisation is the running of traditional network functions, for example, a Session Border Gateway, a firewall, a Broadband Network Gateway (BNG), typically in a virtual machine running on commodity Commercial Off The Shelf (COTS) hardware. This allows operators to use their x86 server infrastructure to run network services that traditionally used to run on service cards within routers or switches, or on specialised hardware.

It is possible to virtualise routers and switches and CPE, the limitations of what is possible relate to packet throughput and latency requirements. Low latency Input/Output (I/O) centric applications typically run best on network hardware. Less delay critical, compute intensive applications can be more cost effective to run on x86 hardware, rather than dedicated service cards on routers. However, this is a constantly evolving picture as NFV solutions are refined and is discussed in Section 8.

3.3. SDN and NFV as Complementary Technologies

SDN and NFV are as discussed separate technologies. However, they are also highly complementary and are both enablers of service orchestration and portability. For example, consider the case of a customer ordering a network provided service such as a firewall from a web portal.

The customer logs onto the portal and orders the firewall service. The service orchestrator can determine where the service is to be provided, where the customer is located and can select a data centre (or other location) to provide the service. The orchestrator can then configure the servers in the data centre and initiate the virtual network function required (in this case firewall). This may simply require configuration of an already running firewall system to support another customer, or it may invoke another instance of a firewall on a separate virtual machine depending on the service requirements. This part of the service provisioning is the NFV component (with some BSS/OSS orchestration).

The orchestrator can then set up the traffic steering in the data centre network to ensure that the customer flows are routed to the correct virtual machine, and potentially within the carrier

network to steer the customer flows to the correct data centre. This is the SDN component and it removes the requirement for the data centre operator to configure the network manually every time a new virtual machine is added, or its location changed (which may happen for operational reasons or because of server failure).

Where multiple services need to be invoked, (for example, load balancing, firewall and video transcoding) then the flow will be steered through each of these services, this is known as Service Chaining and has aspects of both SDN and NFV technologies. In the event of a service failure, it is possible to move the network function (without interruption) to a new location and to dynamically re-configure the forwarding in the network to steer traffic to the new location. The introduction of SDN increases the rate of configuration changes supportable by orders of magnitude over alternative solutions.

3.4. The SDN Technology Ecosystem

The components of an SDN ecosystem are shown, at a high level, in Figure 1.

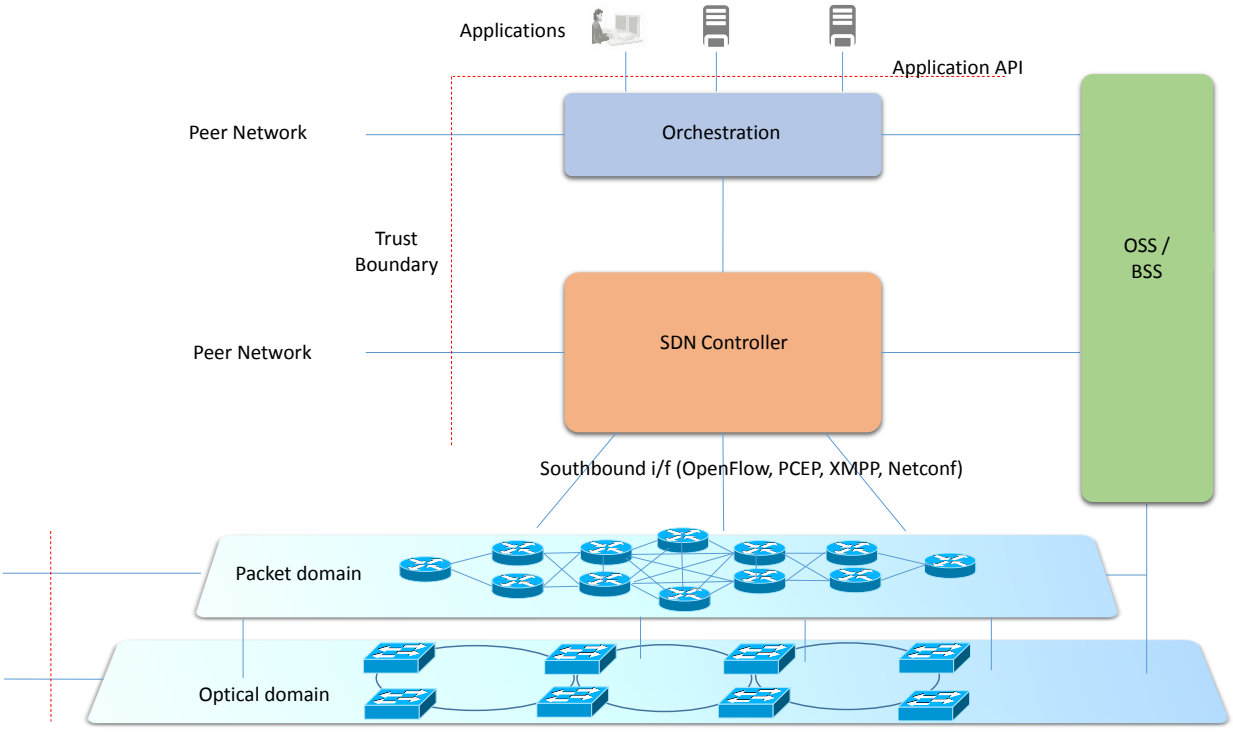

Figure 1 The SDN Ecosystem

The orchestration function is not part of the SDN solution, but forms a key part of the end-to-end service delivery.

The orchestrator is responsible for providing the entire end-to-end service configuration function. Specifically, it provides the following:

- Application interfaces to third party organisations, such as the carriers customers, these may be Representational State Transfer - Application Program Interface (REST API) based or may be via a web portal.
- Interfaces to the OSS and BSS
- Interfaces to the SDN controller that will configure the network to support the service.
- Interfaces to any NFV management and orchestration functions to provide virtual machines and start applications as required.

The SDN controller has a logical view of either the entire network, or the component of the network it is responsible for, including an understanding of the location and functions of subordinate or peer controllers. The SDN controller must translate the instructions from the orchestrator (which it sees as an application) into a set of configurations to be applied to the network elements. It may configure multiple network elements using multiple protocols, depending on the network element and it may be also be responsible for providing control plane functions for some network elements (depending on the protocol and solution). The SDN controller also requires interfaces to the OSS/BSS.

An important function of an SDN controller is topology management and topology abstraction, it must provide the applications (including the orchestrator) with sufficient information about the network to enable service configuration and management, whilst hiding the complexities of the underlying infrastructure. Further information about the SDN controller component is provided in Section 7.

The OSS is not considered part of the SDN solution, however, it still provides a key component of the network. It must provide a set of functions such as fault management, inventory management and configuration that fall outside the domain of SDN but often interact and sometimes conflict with the SDN domain. Further information about the OSS is provided in Section 9.

The BSS is a critical component of the carriers systems as it provides all of the functions required to manage customer information, ordering and critically, billing for services. Like the OSS, it is not considered part of SDN but must be integrated with it. Further information about the BSS is provided in Section 9.

The network sits below the SDN controller and comprises of a number of different layers and domains. At a high level the packet domain (IP routing and Ethernet switching) is one level of networking, below which may sit the Optical transport domain. These two network views are very different and have traditionally been mostly separate; however, SDN solutions are now being

proposed that offer a unified view of the two domains, which permits a more efficient use of the underlying infrastructure.

The trust boundaries in the diagram show interfaces where the network operator may connect to their customers or to other network operators. Proposals exist for SDN and orchestration solutions to interface with peer operators at the orchestration level and at the SDN controller level. Today's networks typically interconnect via Network-to-Network Interface (NNI) which may be IP NNIs, MPLS NNIs or Ethernet NNIs. Further information about the underlying network architectures and how SDN and NFV functions impact them is set out in Section 6.

4. Business and Regulatory Impacts

This section looks at the impact of SDN and NFV on carrier networks from a business and also a regulatory viewpoint. It considers how carriers are intending to apply the technology and what this might mean for the wider industry.

Later sections of this report progressively drill down into some of the detail and technology behind these conclusions.

4.1. Carrier Perspectives on SDN and NFV

Carriers are looking for SDN and NFV to provide them with a number of advantages; service velocity, OPEX reduction and CAPEX reduction. However, different carriers have different views as to which of these benefits is of most interest. Therefore, it is true to say that SDN and NFV may trigger a divergence in the current carrier consensus of networking.

This is certainly true when comparing the different views of carriers on SDN ranging from the enthusiastic advocates to the more sceptical. Of these groupings the former are promoting broad visions and seeking radical organisational change, the latter are looking for tactical wins and a more evolutionary approach where each implementation is supported by its own individual business case. It is not clear at this stage which approach will prove to be correct and to a degree the choice comes down to carrier focus and appetite for risk.

Carriers do not embrace the original academic view of SDN as driving a customer programmable network which allows the customer to run their own protocols on top of network hardware using OpenFlow as their API to the network. In the carrier world, customer access to network functions and services will continue to be defined at a higher layer of abstraction using orchestration functions to configure the network to provide the service ordered. From a carrier perspective OpenFlow is one of a number of protocols that may be used within their network by their SDN controllers to control their network infrastructure.

Carriers are seeking to exploit the data centre service orchestration paradigm in their future networks. This approach to the data centre is based around automation, service chaining and network functions virtualisation; supported by SDN to provide service steering. A key concept for carriers is to replicate the fail fast philosophy of the data centre services rolled out by the internet technology giants. This approach seeks rapid prototyping and soft launches of services, leading either to rapid scale roll-out (using virtualisation), or discarding of failed concepts and then rapidly moving on to the next project. Virtualisation and flexible orchestration solutions are enablers for this approach, as it avoids heavy up-front investment in OSS/BSS and network hardware.

4.2. A View on SDN and NFV Cost Claims for Carriers

One of the problems in assessing the impact of SDN and NFV in future networks is that there are some very large claims made for the cost benefits of the technologies, which is not unusual for any new networking technology. SDN is still relatively immature technology from a carrier perspective, as shown in Section 7. Many of the benefits that carriers hope to see from SDN, for example, application centric networking and service automation, are difficult to quantify at this stage because the concepts are still in development.

Many claims are made around NFV with respect to large CAPEX savings. These claims are based on a view from some operators that traditional routing vendors equipment is over-priced (this may be a particular factor in markets where vendors known for more aggressive pricing face political barriers to entry). As an example of this, looking at recent AT&T announcements Forbes considered the impact of SDN/NFV on the capital network cost per mobile subscriber, postulating that SDN/NFV might reduce AT&T's costs from their estimate of $95 per subscriber to $85 per subscriber [Ref 1]. This followed AT&T statements about their SDN/NFV Domain 2.0 programme that "AT&T expects this program to reflect a downward bias toward capital spending" [Ref 2].

However, this view is not universally shared and other operators have different views, questioning both CAPEX and OPEX savings (at least in the short term). This alternative view considers the wider costs of turning telco central offices into data centres (CAPEX) and the operational issues that NFV/SDN will face on introduction (OPEX) [Ref 3].

There are clear benefits in an NFV approach that reduces the count of physical servers required to support key services. The flexibility provided in being able to deploy customised solutions on commodity hardware also seems significant (for example, being able to deploy small virtual routers or a dedicated Evolved Packet Core (EPC) for a given customer); however, as the use cases expand towards more radical SDN/NFV approaches, more questions arise as to the real savings.

One particular issue with evaluating the potential for NFV to save CAPEX in various network functions, is that the performance of x86 based applications needs to be assessed against the performance of Application-Specific Integrated Circuit (ASIC) based equivalents. This is a complex task, for the reasons set out in Section 8. Furthermore, it is also a constantly moving target as the x86 architecture is tuned for network I/O functions, and the bottlenecks are understood and mitigated. At the same time, the costs of dedicated network hardware are unlikely to remain static as the industry works to take cost out of their solutions. Additionally, network equipment vendors always have the option to change their pricing models, and there may be a future price to be paid for the limited competition in the NFV focussed x86 silicon market.

A significant concern must also apply to some of the OPEX savings claimed for SDN/NFV. The challenge of operating a network made up of white-box switches from one vendor, configured by a control plane running on a virtual machine from two other vendors, should not be neglected and may in fact be higher than the OPEX required by current technology (at least initially). There must also be a question as to how far carriers are prepared to go down the road of developing their own applications to support white-box solutions. Routing and networking products require significant development, support and maintenance, which at the moment is outsourced to very large vendors supplying multiple multinational operators. Can a carrier afford to develop and support their own networking products, and will doing so be cheaper than purchasing solutions from the industry leading networking vendors?

While service automation can reduce OPEX most large carriers already have highly automated OSS/BSS chains for their high volume services. Where SDN/NFV undoubtedly will help is in bringing new and innovative services to market quickly (service velocity) and offering an automation framework for these services. However, the revenues, and indeed numbers of these services are as yet unclear, which is a concern as they are to a degree being used to justify large scale SDN/NFV investments.

Given the fact that SDN and NFV are relatively new technologies in carrier networks and the fact that there are many different views of the business benefits, which in turn, may actually depend on the particular carrier implementing the technology; this paper deliberately avoids trying to quantify CAPEX and OPEX savings. Carriers will build their business cases based on the experiences of their proof of concepts and trials and these outcomes will be shaped by the particular constraints, or strengths of their business. Also, it may be the case that what works for one carrier from a business case perspective, may not work for another.

Carriers are, therefore, likely to pick and choose initial SDN/NFV applications that are relatively non-disruptive to implement and that provide the most business benefit quickly. These early projects will determine how quickly and how far each carrier proceeds down the SDN/NFV road.

4.3. Changes in Carrier Networks

Potentially, SDN and NFV are both disruptive technologies for carriers;, while they offer significant benefits, they are also likely to result in widespread changes to carrier networks, organisations and possibly business models.

4.3.1. Organisational Impacts

Today, many traditional carriers still operate their organisation in silos. The operational teams are separate from the network designers, the data centre teams are separate from the network teams and the OSS/BSS teams are different again.

SDN and NFV cuts right through these silos requiring the data centre and the networking functions of an organisation to work more closely together, since the network will increasingly take on aspects of a data centre, even in the metro node. The OSS/BSS functions must integrate with the SDN/NFV capabilities, but must also work with the orchestration function, which itself may require web based APIs and portals. The operations teams must be closely engaged at each step in the process, otherwise the whole solution will “hit a brick wall” when service is turned up. If history is a guide, it could be noted that the replacement of SDH with carrier Ethernet and MPLS required many of the legacy SDH management concepts to be retro-fitted to the new technology so it could be operated in a telco environment.

For carriers seeking a radical approach, board sponsorship and a willingness to re-organise and re-configure the company will overcome these barriers. For more cautious carriers seeking tactical and evolutionary change, strong leadership and executive sponsorship will be needed to create smaller project teams able to achieve set objectives without hitting the organisational barriers.

If carriers are to achieve their goal of increased service velocity and a move to a fail fast development philosophy, then they will have to transition their service development teams to a more development and operations based approach, with rapid design, prototyping and deployment following Agile methodology (at least for small scale innovation). Care will need to be taken to avoid compromising quality and to prevent hitting a chasm when trying to transition from concept to robust deployment, and this will require a mature and supported service development environment ensuring easy integration with the orchestration systems, the SDN controllers, and the OSS/BSS.

It is important to note that the operations teams tasked with running the network are not going to become network programmers, instead they will be performing very similar fault finding and diagnostics tasks as for today’s networks. In order to achieve this task, they will need to be

provided with a robust tool chain to support them in what may be a far more dynamic environment of virtual network functions and service chaining.

Carriers looking to reduce the network vendor to the role of commodity and to customise their own control planes will need to invest, not just in integration capabilities, but also development, testing and ongoing roadmap and maintenance support. To various degrees carriers have moved to outsource this capability to vendors, so this may require a significant growth in capability (and hence cost base). Carriers looking to rely on their chosen network vendors to take the lead can avoid these costs, but will need to work hard to avoid lock in and to ensure that their service innovation teams can develop value added services on the platform.

Within complex SDN/NFV deployments there will be a large task to integrate with the OSS/BSS systems. It is not clear if carriers will attempt this themselves, outsource it to a lead vendor, or deploy specialist systems integrators to manage their vendor ecosystem. Since carriers will take different approaches, it is possible to see these skills being provided by all three. This is likely to be a significant investment cycle, and with the business case as yet unproven, adoption is likely to start relatively slowly. There is a risk that the uncertainly created may have a chilling effect on short term network investment.

One of the key benefits of SDN/NFV is it offers the possibility to automate some of the network operations tasks that are carried out manually today. In particular, path computation and optimisation of packet and optical networks, as well as automated provisioning of complex low volume but high touch services. This is likely to reduce the demand for some of the skilled network configuration and optimisation engineering functions currently employed by carriers. Network configuration tasks are likely to move from repetitive resource heavy Command Line Interface (CLI) tasks to scripting activities and network programming (as part of the SDN component of a new service build, or as part of an optimisation function).

4.3.2. Network Infrastructure

The impact of SDN and NFV on network infrastructure will be significant, with platforms moving from dedicated hardware (custom or COTS) onto virtual hardware running on x86 servers. Network applications suited to virtualisation (which are not latency critical and are Central Processing Unit (CPU) rather than I/O intensive) will rapidly move to this new deployment model. Applications that are easy to scale out and which may form part of complex service chains (such as video transcoding and firewalling) are also a focus for an early transition.

It is not clear how much of this virtualisation will hit traditional router vendors, core routers will be least effected, but smaller IP edge nodes may move onto virtual platforms in the medium term. There is also a possibility that white-box switches will replace more expensive custom hardware from IP router vendors to provide a hardware acceleration function to permit larger IP edge

nodes to be virtualised and commoditised. For some network operators their vision is likely to require modification of their existing estate to support data centre infrastructure in their central office locations [Ref 4]. The architectural impacts of this are discussed in Section 6, and the limits of network functions virtualisation explored in Section 8.

Currently, there is some anecdotal evidence that the advent of SDN and NFV is already creating market uncertainty and driving a slowdown in the service provider router market.

Infonetics Research claim that “Service provider router and switch revenue rose just 2% in 2013” and that the 4Q13 figure was “down 4% from the same period a year ago”. Infonetics Research attributes this to “weakness coming mostly from Verizon and AT&T, among the global leaders of SDN activities.” On the basis of this analysis they predict “worldwide service provider router and switch revenue to grow at a low single-digit CAGR from 2013 to 2018.” [Ref 5].

There is some evidence that carriers are under pressure to improve link utilisation within their networks in order to reduce network spend, this may lead to adoption of traffic engineering more widely within networks, possibly utilising SDN techniques to reduce the costs and improve the efficiency of traffic engineering. In one of the earliest SDN deployments, Google were able to achieve link utilisations close to 100% as opposed to the telecom standard of 30-40 percent (see Section 10). However, while this will permit greater link utilisation the growth of traffic being experienced by networks means that the amount of infrastructure will continue to grow. It should be noted that much of the cost of networks is in the access networks rather than the core and these access links have many less options for routing than core nodes. This suggests that the savings available in network links from SDN may not be hugely significant against the whole network cost.

Within the mobile environment, solutions that can cost optimise the RAN will provide the most benefit. Of these C-RAN has some very large OPEX and CAPEX reductions claimed for it but requires a fibre rich environment for cost effective deployment; solutions such as Wavelength Division Multiplexing (WDM) to optimise fibre for fronthaul are still seen by carriers as prohibitively expensive. In reality, this is likely to mean that countries with fibre rich city infrastructure will benefit far more from these savings than those with low fibre availability.

SDN could also assist mobile operators in optimising their backhaul and possibly optimising microwave and small cell network power budgets, these savings are referenced in a Tellabs sponsored Strategy Analytics paper [Ref 6]. (Caution is required because of a conflation between SDN and non-SDN solutions in the paper). These applications could lead to a reduction in mobile operator infrastructure, however, given the data growth from mobile devices, they are more likely to be used by the mobile carriers to improve QoE and reduce their transport costs.

Overall, therefore, SDN and NFV are likely to permit network operators to increase network utilisation, which will assist in handling some of the projected bandwidth growths in networks. There is likely to be a shift towards virtual platforms running on x86 servers rather than dedicated network hardware, for non I/O intensive applications and for smaller IP edge nodes. This may lead to carrier central offices becoming small data centres. There is some evidence that the uncertainty created by the transition to SDN/NFV by early advocates is suppressing the router market. However, it is too early to say if this reduction in investment in the IP Edge will continue, in part because the boundaries of cost effective network virtualisation are unclear, and in part because traditional IP edge router vendors may well be able to exploit their solutions within an SDN/NFV world.

4.4. Future Network Services

One of the attractions of SDN from a carrier perspective is that, in theory, it permits rapid service innovation and development, and it can provide interfaces for application centric networking to permit third party applications to leverage the networks capability. It should be noted that not all operators necessarily see this as a major benefit of SDN. There is certainly a degree of caution with respect to application centric networking and whether such facilities will be of interest to OTT providers. It is very early in the SDN cycle to get clarity as to what these services are, however, this section looks at likely candidates from a residential, business and OTT service provider perspective.

4.4.1. Residential Customer Services

The high volume, low margin nature of residential services means that carriers existing OSS and BSS provide a very high degree of automation. However, SDN and NFV may still have an impact on residential services because it will increase the rate of service innovation, and there is an element of self-care and self-ordering of these services that has been inherited from the cloud computing environment. Therefore, a carrier may be able to offer residential customers the options to add specific value added services to their portfolio, some on a short term basis and some on a longer term basis.

There are some SDN/NFV use cases around security that may be of interest to residential customers. Intrusion Detection and Prevention Systems (IDPS) can be configured by SDN on an as needed basis to analyse and profile a customer’s traffic to identify known threats or unusual traffic patterns. SDN would permit short duration service to be provided, as well as longer term premium subscriptions.

Potentially, SDN and service steering could also be used to provide on demand content filtering returning full control of the service to the end user (versus the current government push), and

permitting the service to be dropped in or out of the service chain depending on the customers particular circumstances. The benefits of SDN mean that this could be provided on a per device basis and, depending on commercial considerations, could follow the device as it moved between domains, (for example, a child's tablet moving from a home network to a mobile network). An example of such a service is shown in Figure 2.

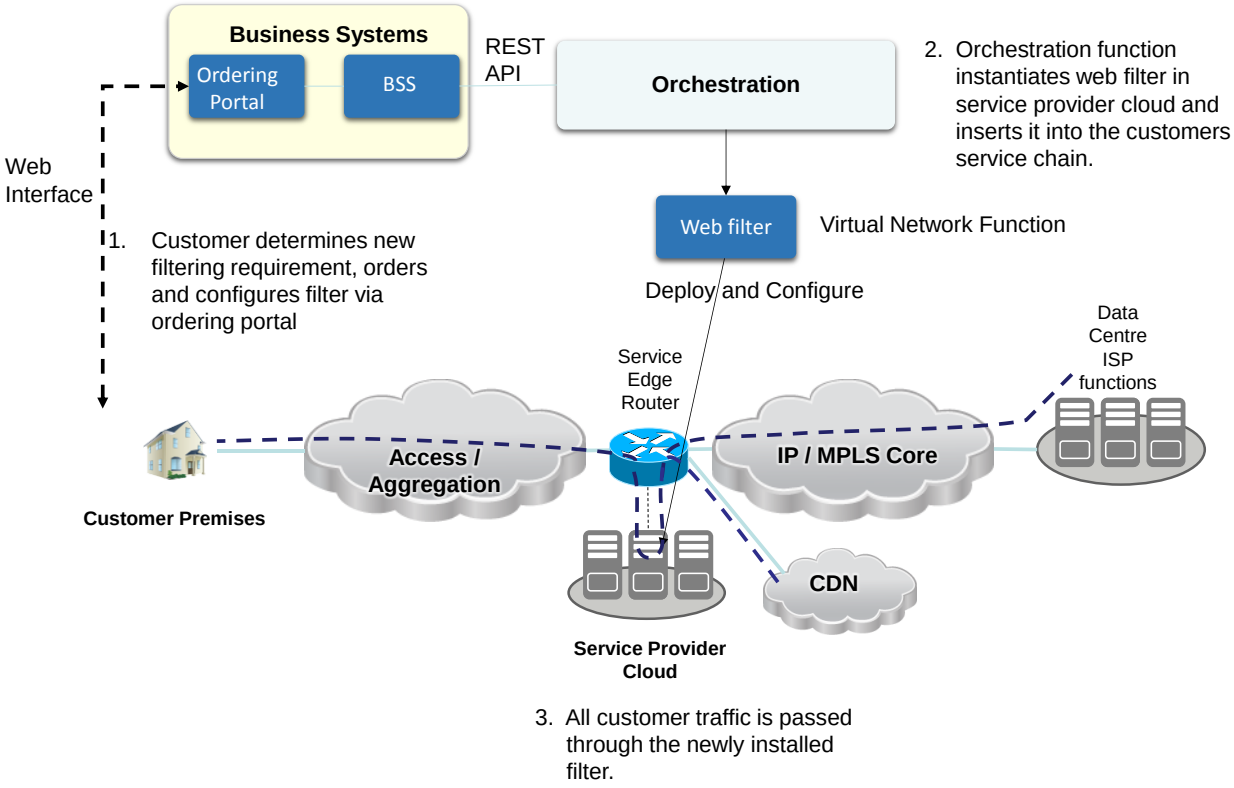

Figure 2 An SDN and NFV approach to customer configurable web filtering

One of the benefits of using SDN and NFV capabilities to deploy filtering services is that the technology makes it relatively easy to scale filtering up or down as required. If the filtering is implemented on x86 hardware with appropriate orchestration functions, spare processing capacity can be rapidly applied to scale out the network filters in the event that unusual circumstances (for example civil unrest, or a wide scale DDoS attack) create a sudden demand.

Services such as the network based Personal Video Recorder (PVR) could make a return, as these could be supported by compute and storage in the metro node in close proximity to Content Delivery Network (CDN) connectivity. This migration of video centric services from the data centre to the metro node will save on core bandwidth and SDN may also enable carriers to look again at providing their own CDN solutions.

In theory, residential customers could also gain access to bandwidth on demand services so as to enable them to enjoy improved QoE for premium OTT content. In reality, however, the history of these services suggests that customers are relatively resistant to such concepts and simply expect their broadband services to work.

Virtual CPE for residential customers provide the carrier with the opportunity to manage the home network for the end customer. This can include managing the transition to IPv6, and providing capabilities such as home network nomadicity which permits a subscriber to take their home network (and all its facilities) with them wherever they go. These sorts of applications may benefit from access to compute and storage functions within the telco metro node (e.g. the network PVR). This service vision is very much part of the Telefonica Unica concept [Ref 7] . In addition to the customer features provided by virtual CPE offerings, there are significant service provider benefits from this approach. In particular, there may be OPEX savings because in broadband networks a large number of customer faults are caused by unsupported home networking problems. This view of virtual CPE is however not shared by all broadband service providers, some of whom see their customised CPE as a service differentiator.

Mobile networks can take advantage of the flexibility offered by service chaining to optimise their content delivery networks and content optimisation so as to maximise a customer's QoE for their current access. NFV and service chaining within the SGi-LAN should provide significant benefits in terms of the cost and flexibility of these solutions. While these services are not necessarily seen by the end user, the optimisation of content types and flows through the network, especially if combined with Heterogeneous Networks (HetNets) and the EPC Access Network Discovery and Selection Function (ANDSF), may provide a very real improvement in the end user QoE.

4.4.2. Services for Existing Carrier Business Customers

Many of the services that SDN enables will be targeted at the large business customers of carriers, either end user corporations or corporate Information and Communications Technology (ICT) providers depending on the carriers business and regulatory environment.

These customers are already served today by providing simple leased lines, backhaul services and potentially layer 2 and layer 3 Virtual Private Networks (L2VPNs and L3VPNS). SDN provides a way to automate and streamline VPN configuration, delegating control to the customer and removing the need to perform resource intensive configuration each time a customer network changes its routing requirements. These services have traditionally not been well served by the OSS/BSS stack as they are complex, high margin services and are, therefore, less critical (and harder) to automate than high volume simple services such as residential broadband. Using SDN it would be possible to offer an ordering and configuration portal that let

the customer configure their own layer 3 VPN and maintain it themselves. The portal would interface to the orchestration platform which would provide the end-to-end service build and modification (using SDN controllers within the network). Such a solution could also provide performance monitoring and alarms to the end user, obtained from Operations Administration and Maintenance (OAM) functions in the network. To an extent some of this is happening already using router vendor SDK capabilities and SDN can be expected to accelerate this trend.

Where the carrier has moved to add data centre capabilities to their metro node more radical service models become possible. For example, the carrier can offer an NFV capable Infrastructure As A Service (IAAS) solution. This would permit an ICT provider (or enterprise) to purchase compute and storage capability from the carrier at select nodes, purchase a series of layer 2 pipes to connect this compute and storage facility together, and then install virtual IP routers on the compute platforms. This would allow them to install their own IP network running over the top of a carrier's infrastructure and removing their reliance on the carrier to support them each time their customer wished to change the service. This effectively overlays a completely separate corporate IP network on top of a carrier network, providing a separation well beyond traditional layer 3 IP VPNs. It should be noted that this sort of NFV capable IAAS service may be a viable alternative to, and possibly replacement for, exchange hosting facilities currently offered by some carriers to support their leased line products. This is discussed further in Section 4.6.1.

A (slightly) less radical way of achieving a similar solution would be for the carrier to offer either a Virtual Network Function as a service, in effect a complete virtual router, or a Virtual Network Platform as a service (a group of network functions). The ICT provider in this model purchases a standard service provider defined virtual router (and connectivity) plus any other facilities such as firewalling and networking that they require.

Carriers will also be able to exploit SDN and NFV to offer businesses local on demand storage and compute services (a distributed cloud platform) as well as firewall services. This coupled with a suitable orchestration and ordering system allows new and innovative network applications to be created, advertised on a portal and dropped into a customer's service chain if they choose to add the new facility to their service.

The carrier can also offer IDPS solutions as per the residential case and SDN/NFV provides an excellent platform for tackling Distributed Denial of Service (DDoS) attacks directed at a given user. This technology allow classifiers to be installed that will identify suspect flows at the edge of the network and re-direct them to Deep Packet Inspection platforms where the traffic can be scrubbed. Meanwhile, clean flows can be passed through to the enterprise over the usual network path. These attacks can be highly dynamic in both the quantity of the traffic they generate and the attack vector, however, SDN provides a similarly dynamic tool for combatting them. The OpenDaylight SDN controller has integrated elements of this capability in their Defense4All application [Ref 8].

The principles of using SDN and NFV for IDPS and DDoS systems are shown in Figure 3.

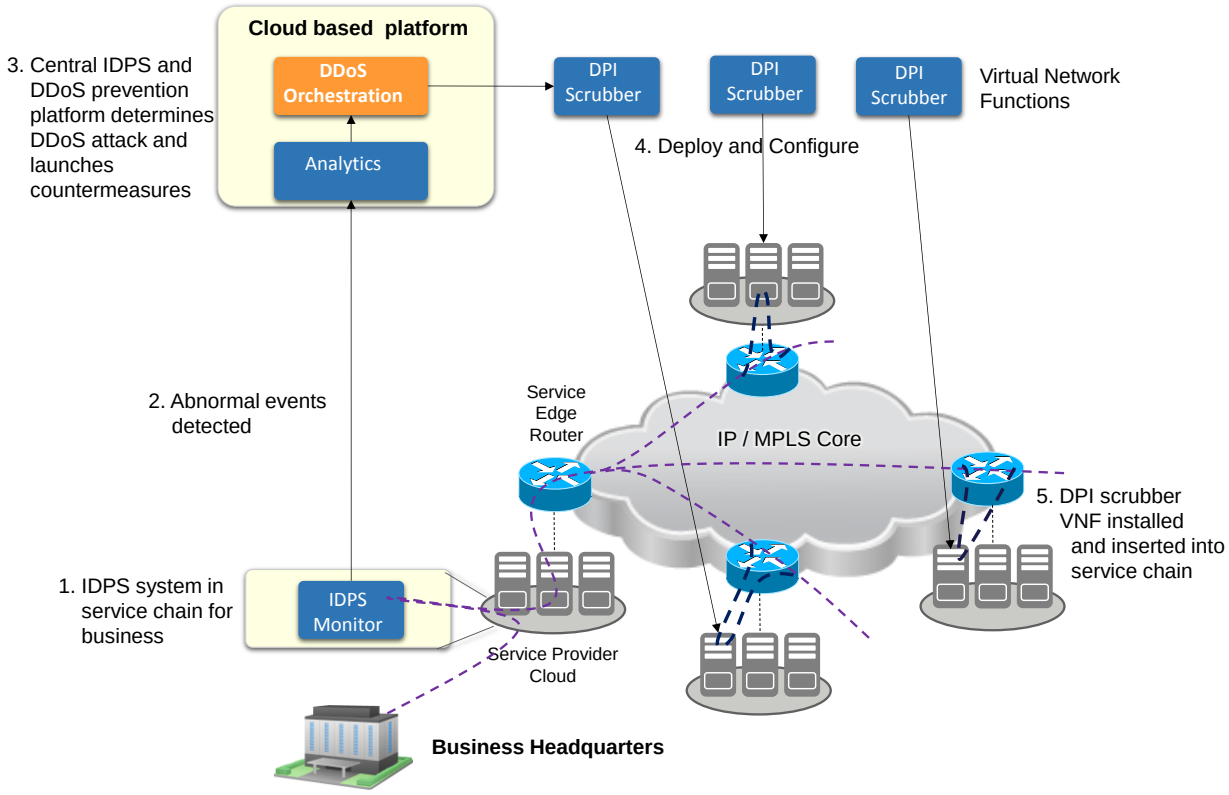

Figure 3 An SDN and NFV approach to IDPS and DDoS mitigation

Carriers may also offer virtual CPE solutions to business customers (this solution is currently deployed today, see Section 10). This may not add significantly to the capabilities offered by carrier solutions, however, it will provide cost benefits for smaller business premises compared with a traditional layer 3 CPE and if it can be integrated with the access network Network Interface Device (NID) it may provide additional operational benefits.

The carrier may also be able to deploy application centric service interfaces, offering their customers additional information about network capabilities and state to enable them to tailor their network usage as required by an individual application. These services might include enhanced traffic management options and potentially offering bandwidth brokering and flexible bandwidth services. For example, a flexible bandwidth service could enable an enterprise to take advantage of time variable bandwidth pricing (or spot bandwidth pricing) to schedule data transfers in low network usage periods. It should be noted that there is some scepticism around these types of short duration bandwidth on demand services, as they have been proposed a number of times without achieving market traction.

4.4.3. Services for OTT Providers

OTT content providers tend to have a slightly different relationship with mobile network operators compared to fixed network operators. A fixed network operator has access to high speed links to the customer, therefore, this combined with partnership with one or more CDN providers means that the OTT content provider can be assured that their content (be it real time video, or software updates) will reach their customers with an acceptable quality.

For a mobile provider, the RAN is of more variable quality and is resource constrained, therefore, OTT providers must optimise their content and both the mobile provider and the OTT provider has an incentive to collaborate to ensure the maximum possible QoE for their customer. Network operators are already considering the benefits of using NFV and service chaining as a way to enhance SGi-LAN capabilities for content optimisation.

One possible application that could be enabled by SDN application based networking is multicast delivery enablement. While multicast protocols exist today in the IP network, and are implemented in both fixed and mobile networks; it is hard for applications to understand either the availability of multicast service delivery, or the desirability of multicast service delivery, for a given piece of content. By allowing either the network or the OTT provider to offer, or ask for, multicast delivery, it is possible that media streams where both parties can benefit from multicast could be identified. This benefits the mobile operator because it uses their spectrum efficiently, and it benefits the OTT provider because they send less traffic into the mobile network and get an improved QoE for their customer.

One example of such a scenario is shown in Figure 4 for a sports stadium, where a large number of customers are watching the same unicast live broadcast (for example, the game's half time highlights, or another game in a tight end of season relegation or promotion battle).

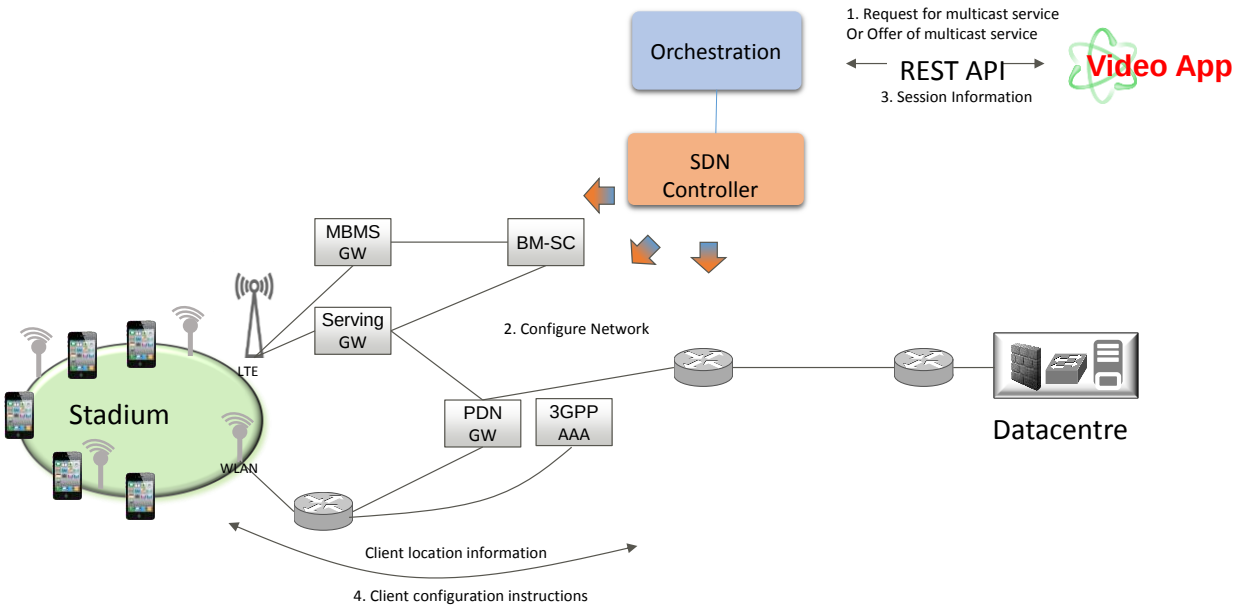

Figure 4 The Use of SDN as an Enabler for Efficient Video Delivery by Multicast

In this example, the mobile carrier and the OTT provider collaborate to discover that a multicast service is the best option, to enable its real time provisioning within the network and to move the clients from a congested stadium Wi-Fi onto the Long Term Evolution (LTE) operator's multicast service. The SDN controller must inform the OTT provider of the multicast group and configure the multicast service, the OTT provider application must inform the client applications of the multicast session and instruct them to move over to it. It should be noted that this is a complex scenario, and provides an example of the sorts of networking and commercial issues that need to be addressed to make this type of application a reality. The SDN north bound interfaces being discussed in standards organisations are a long way from this capability today.

Other possible applications around SDN and OTT providers may arise in the area of CDN providers, and optimising their interactions with the carrier network. However, there is also a risk that OTT providers may resist taking advantage of network integration facilities if faced with a fragmented landscape of network specific solutions. In this case the OTT provider will limit their integration to mobile networks where QoE is critical and ignore other opportunities, as this will avoid creating expensive individual network customisations. This is a significant concern because of the current lack of consensus on an application (or northbound) API.

4.5. Challenges and Barriers in Implementing SDN and NFV

SDN and NFV are relatively immature technologies in the carrier space, however, both will clearly have a role in future networks. The issue for carriers is how they implement SDN (as there are many technology options), how far do they push the boundaries of NFV capability, and how fast do they move. It is practical today to roll out SDN and NFV implementations in specific focussed use cases, and indeed organisations have done so. However, there are some challenges and issues that may delay or limit the technology adoption.

Organisationally, SDN and NFV have a significant impact on carriers, as described above. This is likely to lead to organisational conflict which must be managed, and a reluctance for departments to release key staff may slowdown SDN and NFV projects. This organisational friction may combine with business concerns as SDN and NFV projects inevitably run into implementation problems (as predicted by the Gartner hype-cycle model of technology introduction).

SDN and NFV have significant impacts on the OSS/BSS and on a carriers operational systems, furthermore, large scale SDN and NFV projects (for example, transition of a routing infrastructure to a white-box deployment model) will carry a heavy integration cost. Carriers will either h to outsource this, or to bring it in house and recruit resource to execute it.

A major justification for some SDN/NFV deployments is reduced CAPEX because the carrier is free to replace expensive routing equipment with cheaper white boxes, or entirely virtual solutions. There is a risk that such projects may find the CAPEX required to deploy them outweighs the savings in routing equipment (especially if router vendors change their pricing models). This may mean that a carrier can leverage the threat of radical SDN/NFV deployments to reduce their costs without deploying the technology.

Another risk for SDN/NFV deployments is that the cost of operating distributed control planes and multiple software platforms, plus a significant move away from tested operational procedures, processes and tool chains may sharply increase the OPEX incurred by the network operator. It is entirely possible that a badly implemented SDN/NFV solution will increase both CAPEX and OPEX incurred by the operator, and may well be broadly cost neutral even in well implemented solutions (see Section 4.2). This risk is amplified if a carrier brings the development in-house, as they are now their own Systems Integrator and Vendor and may have to support their own equipment and its feature roadmap. This burden in traditional networks is carried by large multi-national equipment vendors serving multiple markets and customers.

There are also security risks in moving to SDN as the controller needs to be secured along with the interfaces to the equipment it is controlling. In reality, however, this is actually only an extension of the security already deployed between, for example, an Element Management System (EMS) and a Network Element. It is possible that SDN may improve security with its support for DDoS capabilities and automation of security tasks, (for example, BGP filtering). NFV

has more impact on security because of its dynamic nature and will require specific management tools to be developed to provide end-to-end security. For high value secure customers it may be a long time (possibly never) before NFV solutions will be acceptable.

The motivation for much of the investment in SDN is a desire from carriers to offer new and innovative services quickly and easily in their networks. This has been the holy grail of telecommunications since the days of Intelligent Networking and is still a big draw for carriers seeking to stem or reverse the ever declining ARPU. However, the northbound interface to the applications that would enable this is not well defined at this time, and is really only starting to be considered. Furthermore, carriers may be reluctant to open this interface fully which will limit its attraction to OTT providers. It is also unclear what services carriers will be able to sell over and above their existing portfolio when placed in competition with the large OTT providers. The risk to SDN and NFV is that if these services do not materialise, it may not be possible to justify (or recover) the costs of SDN/NFV deployment.

From a technology perspective there remain some challenges for SDN outside of the constrained data centre environment. Many of the standards specifically targeting the WAN are in the early stages of development (e.g. Interface to the Routing System (I2RS)) or have not yet been widely implemented, (for example, PCEP). While OpenFlow is a more established standard it faces a significant number of technical barriers that must be overcome before it can be seen as a good fit for general WAN applications.

The lack of standardised hybrid support in OpenFlow is an issue for Wide Area Network (WAN) deployments and the relative lack of support for the later versions of the standard in silicon remains a concern (outside of virtual network function deployments). A major issue faced by switch vendors is that the cost of developing new silicon that supports the later versions of OpenFlow is likely to be significant. However, this must be balanced against the risks that encroaching NFV capabilities pose to future silicon sales. This calculation is made even less favourable by the fact OpenFlow is still a standard very much in flux and is difficult to implement. It should be noted that a critical attribute of OpenFlow solutions for the WAN will be the number of flows that they are able to support.

The ONF is looking to adopt more silicon friendly approaches to OpenFlow by adapting its flat model and taking care to consider silicon in implementation decisions. However, this may prove difficult to achieve without additional changes to their governance and may limit the number of flows that can be supported in networking equipment. Further information about the challenges that the ONF is addressing can be found in Section 7.3.1.

In addition to the challenges for carrier SDN/NFV deployments that this report identifies, it is also interesting to consider the wider industry perception on the barriers to adoption. The

OpenDaylight project recently sponsored market research from Gigaom looking at a whole range of SDN and NFV issues and also the implications of Open Source in SDN and NFV [Ref 9].

They asked a large number of operators, only some of whom were service providers, their views on SDN/NFV adoption barriers. The two issues raised by the most respondents were uncertainty around the risks and rewards associated with SDN and concerns about migrating existing networks.

Note:	Caution is required in interpreting the survey as it asked a prompted question and concepts like security and organisational impacts were not prompted for.

To an extent these views reflect the current state of solutions and standards which over time will evolve. However, the concerns about risks and deployment complexity are one reason some carriers are taking an evolutionary approach to SDN deployment, and requiring each project adopted to pass a business case.

4.6. Regulatory Concerns

This research report is not primarily concerned with regulation, since that falls entirely within the remit of the relevant national and EU regulators. However, SDN and NFV will have significant impacts on networks and this section highlights areas of regulation where the technology may have a future impact.

4.6.1. SDN and NFV and Existing Regulatory Markets

At a very high level SDN and NFV technologies are unlikely to change the nature of interconnect between carriers, so existing interconnect interfaces and processes will remain relevant. Service providers, OTT providers and other customers will order the same sorts of services they do today, although the service set will be enhanced and a more flexible range of offerings will be available.

Therefore, SDN and NFV are unlikely to have a fundamental impact on regulatory markets, however, the nature of the technology is such that they will have some impact on the services covered by at least some of those markets.

4.6.1.1. Market Definitions

This picture is somewhat complicated by the fact that the current market definitions are up for review within Europe and are to a degree in flux. A report prepared for the EU on "Future Electronic Markets" [Ref 10] proposes to map the 2007 markets to a new set of markets, shown in Figure 5.

Retail fixed access	1		
Fixed voice call origination	2		
Fixed voice call termination	3	1a	Call termination on fixed networks
Mobile voice call termination	7	1b	Call termination on mobile networks
Local loop unbundling	4	2	Wholesale Local Access
Wholesale broadband access	5	3	Mass market Wholesale Central Access in sub-national markets
		4a	Business grade Wholesale Central Access
Leased lines terminating segments			
	6	4b	High-quality business data connectivity

Figure 5 Proposed Future Markets – source [Ref 10]

This paper considers SDN and NFV in the context of this proposed new mapping.

4.6.1.2. Voice and Telephony Markets

SDN and NFV are unlikely to have any regulatory impact on voice services, since voice is an application running over the top of an SDN and NFV infrastructure and many voice services are deployed in data centres today. SDN and NFV offer benefits to a voice deployment, in that they enable it to be deployed flexibly and they permit easy scaling out of the service, which is a very useful tool for handling signalling overload events (called by mass calling events). The benefits of SDN and NFV can be realised regardless as to whether the voice operator is a carrier or an OTT provider and as such it is not a regulatory concern.

4.6.1.3. Wholesale Local Access

The new regulatory proposals suggest that Local Loop Unbundling (LLU) will become Wholesale Local Access and apply equally to genuine Local Loop Unbundling, Sub Loop Unbundling (SLU) and also Virtual Unbundled Local Access (VULA) solutions. Within the UK, for a number of reasons, the primary concern is VULA. For Next Generation Access (superfast broadband) services VULA is implemented using the Active Line Access architecture defined by the UK Network Interoperability Consultative Committee (NICC) in ND1644 [Ref 11] and reproduced in Figure 6.

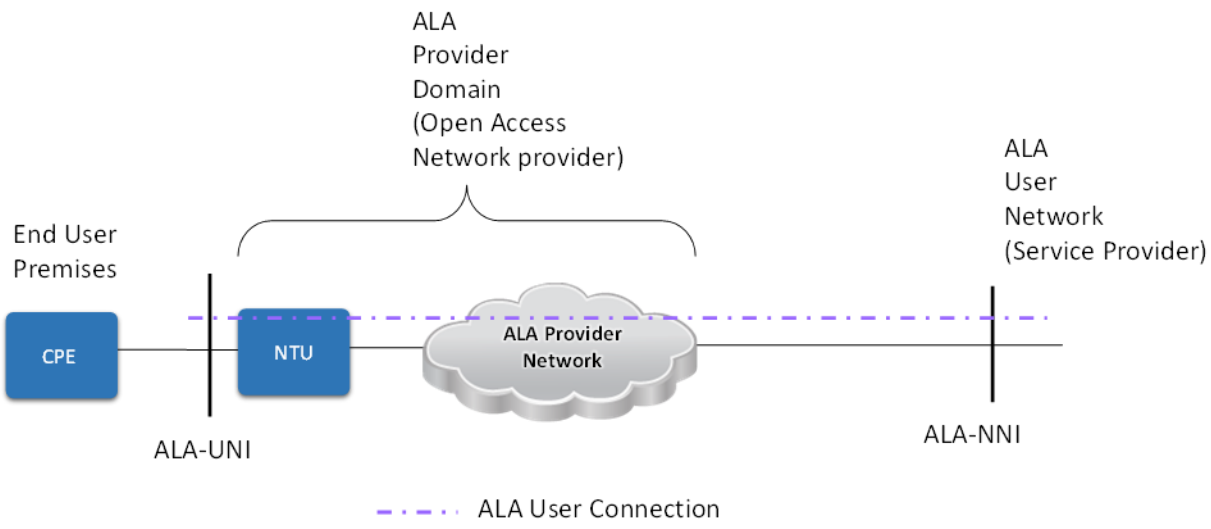

Figure 6 ALA Architecture

The nature of Active Line Access (ALA) is that it provides an Ethernet Virtual Circuit between the customer premises and their service provider (the ALA User) over the access network operator's (the ALA Provider) infrastructure.

Because the service is a layer 2 pipe, SDN and NFV innovations such as virtual CPE (vCPE) can be fully supported, with the vCPE located either at the ALA provider Broadband Remote Access Server (BRAS) or their data centre depending on their preference. In this architecture, the choice as to how data centre functions are distributed through the network is for the ALA User to determine, although this architecture allows the ALA provider to dictate handover points (and hence limit this potential distribution).

In the UK, the advent of LLU required the use of hostels and co-location products within the incumbent operator's exchanges. This led to a number of products being defined that the LLU operator could purchase depending on their requirements. The possibilities of NFV mean that some LLU operators may seek to provide additional networking capability using virtual functions running on x86 servers and it may be necessary to consider the impact of this on existing hosting product sets.

4.6.1.4. Mass Market and Business Grade Wholesale Central Access

These markets are aimed at service providers looking to support residential and business grade broadband access without deploying infrastructure within the network. Business grade access typically requires lower contention ratios, and facilities such as Quality of Service (QoS) and guaranteed bandwidth; but from an SDN and NFV perspective these two markets can be considered the same.

Typically, the wholesale network provider backhauls the broadband service to a metro node, and either provides BRAS functionality or tunnels the service to a central handover point.

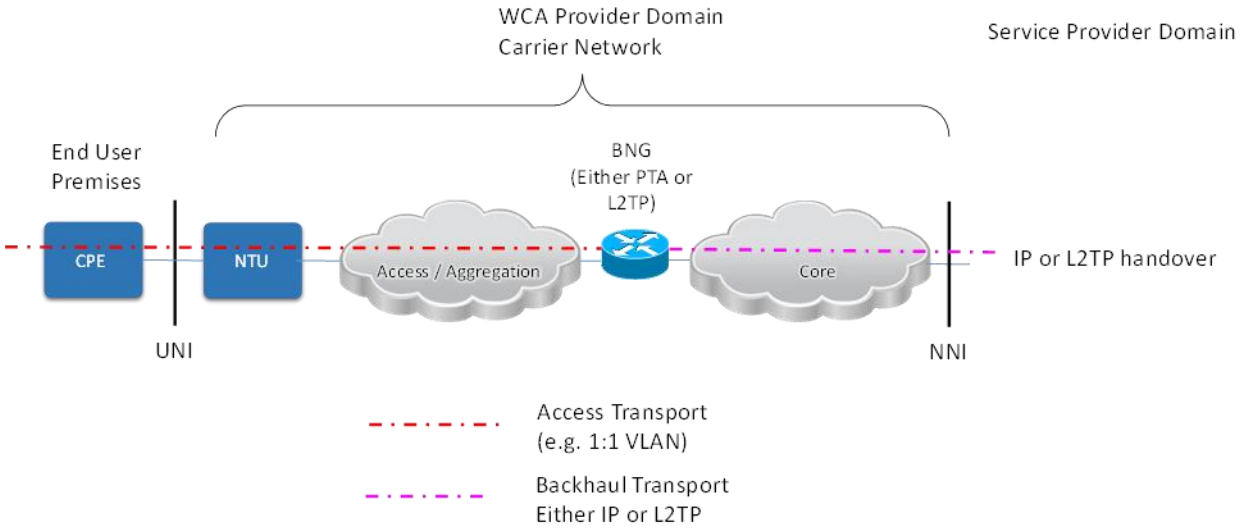

Figure 7 A Wholesale Central Access Architecture

The fact that this service may provide a BRAS, which is a potential platform to support virtual CPE, and that this service has fewer options for service providers to deploy their own infrastructure, means some care is required from a regulatory viewpoint. If a wholesale network provider chooses to adapt their data centre to an NFV/SDN capable infrastructure, then they may offer a range of services to their wholesale customers. These services include at the lowest level an NFV capable IAAS offering, or it may be specific virtual network functions. Services offered at this point must be offered on a non-discriminatory basis, and care should be taken to ensure that when offering internal and external SDN/NFV services the wholesale network operator uses the same orchestration capabilities; this latter point prevents automation barriers being placed in front of third parties seeking to access their products, as seen in some SLU deployments.

If SDN and NFV capabilities in the metro node start to become requirements for effective broadband service deployment (which would be the case if a killer application is discovered that requires SDN/NFV close to the customer), then there is a risk that by refusing to support such a capability for Wholesale Central Access a network operator could use this to make such offerings unattractive (relative to a Wholesale Local Access offering). It is not possible to see such an

application at this stage, or indeed a motivation for a wholesale operator to behave in this way; therefore, this seems unlikely, but it should be monitored.

From a business grade perspective, virtual CPE may be a requirement for cost effective deployment of services in the future. However, provided the implementation of the service supports an Ethernet Virtual Circuit between the customer premises and the service provider's central handover point, this capability can be supported.

4.6.1.5. High Quality Business Data Connectivity

This market effectively covers leased lines which may be Ethernet services or alternative technologies. These services do not themselves place restrictions on SDN and NFV capabilities and are not impacted by the technology. Where leased lines can be complimented by exchange based equipment hosting then there may be some regulatory considerations as to what may be supported in the exchange to avoid penalising SDN and NFV centric network deployments.

It is currently possible to purchase hosting in the incumbent operator's exchange to support network elements that are using leased lines (based on an evolution of the original LLU concept). The advent of NFV means that these hostels may become potential locations for virtualised network elements running on x86 servers and as noted previously this may have an impact on the hosting products.

A more radical solution that may emerge, if the technology and market demand requires it, is that the incumbent operator could offer virtual hosting using an NFV optimised IAAS solution. In this solution they would offer network connectivity, possibly as part of the leased line, compute and storage and the hosted operator would deploy their network equipment as an application on top of a virtual machine.

4.6.2. Mobile Network Fronthaul

This is a new market, and one that does not seem to have been considered in the EU's "Future Electronic Markets" report [Ref 10]. The requirements of mobile fronthaul are imposed by the nature of Common Public Radio Interface (CPRI), see Section 6.4.2 and is required by an operator seeking to deploy Cloud-RAN solutions. This is distinct from backhaul because it encodes the radio directly onto the transport solution and, therefore, only dark fibre, WDM or microwave products are suitable (and microwave lacks bandwidth).

There is a consensus in industry that for cost effective deployments dark fibre is the only viable option. In the UK an alternative exists where dark fibre is not available, duct sharing; known as Physical Infrastructure Access (PIA). In order to support mobile fronthaul the regulation around PIA would need updating because mobile fronthaul is excluded from the current product.

There are major benefits claimed for C-RAN and countries able to deploy it may gain from a lower cost RAN, a green dividend owing to power efficiencies, and improved data speeds. In some deployed networks C-RAN improves data speed by 1.6 to 1.8 times for the equivalent spectrum. In urban areas where a competitive dark fibre market does not exist, it may be beneficial to consider what action may be required to remove this block on fibre availability so as to make the UK C-RAN friendly.

4.6.3. Risks to Net Neutrality

Clearly, within any network that is using traffic engineering to maximise link utilisation, packet marking and QoS are essential components of the architecture. This means strict definitions of net neutrality where all packets are treated equally simply cannot apply, since with no way to prioritise delay sensitive services pretty much every low latency application running over the network will break. While SDN is seen as a tool to enable efficient traffic management it is not a requirement for it, and this fundamental issue will apply to both SDN and non SDN enabled networks.

Therefore, it follows that any net neutrality regulation must both permit the use of traffic management and prevent its abuse for competitive advantage. This is a complex issue as recent events in the USA [Ref 12], and the reception of recent legislation in the EU [Ref 13] show. SDN does not fundamentally change the problem of forming a regulatory solution for net neutrality, however, it is possible to identify areas where SDN and NFV may pose additional risks that regulators may need to mitigate.

The use of SDN and NFV to support service chaining and to drop services and facilities into and out of a traffic path in a dynamic way may complicate net neutrality enforcement. These sorts of service re-configurations could include scrubbing traffic that is part of DDoS attack, or enforcing

a bandwidth cap by moving customer traffic to be low priority. It could also be used to transcode video to ensure acceptable delivery over a degraded network or to apply content filtering. While all of these applications have legitimate uses and will provide a valuable service if deployed correctly they may also be used to selectively degrade specific services (possibly on an occasional basis) by an unscrupulous operator. This means that regulators who are checking conformance will have to develop measurement tools and methodologies that are capable of detecting this kind of abuse.

The use of SDN to provide service APIs may mean that in the future on demand premium bandwidth can be sold on a short duration basis to applications requiring assured delivery. These sorts of services will have to fit within any net neutrality framework and must (if they are permitted) be offered on a non-discriminatory basis by the operator. It is possible that the availability of a wider range of service APIs, supported by SDN technology, may have implications for competition beyond net neutrality, see Section 4.6.5.

4.6.4. Security and Privacy

The separation of the control and data planes that SDN implies introduces an additional network element, the SDN controller, and this must be secured. For example, the controller must be authenticated and the control interfaces to the network elements must be secured. Similarly, the network elements themselves must also be authenticated and protected from unauthorised access. Depending on the deployment scenario, a controller may be required to re-apply a known configuration to a network element that has become isolated from it (in the same way an EMS will over-write a local configuration on a network element). Third party applications that are using the Service APIs will also need appropriate security, in a similar way that the current network secures OSS/BSS interfaces that cross trust boundaries.

While these security requirements complicate any solution, it is a well understood problem in networks and the mechanisms used will be similar to those used for securing network management applications today. The industry has a long track record in securing these types of interfaces and supporting functions such as secure software upgrades.

From an NFV perspective security is much more of an issue. This is because it is now possible to instantiate and destroy virtual network functions and to build flexible service chains connecting these ephemeral functions; this represents a big change to the networking operational environment. Previously, network equipment had credentials; a physical presence and connectivity that could be audited by inspection. Indeed, some high security deployments locked down interfaces, banned fibre patching and would monitor fibre interfaces to prevent tap insertion. While encrypting traffic provides a degree of protection it is also an expensive cost burden for network based services and a potential barrier to QoE. Carriers will, therefore, have to adopt operational methods and tool chains for securing virtual network functions and their

connectivity. This will require the use of certificates for authentication (which must be issued to new virtual functions and revoked when the function is removed) and mechanisms for identifying each virtual network function in a service chain (to prevent rogue functions being inserted). The potentially transient nature of NFV applications and their number may mean that the generation of certificates and their revocation may be more complex than in a traditional telecommunications network (see Section 8). Given this complexity it may be necessary to consider whether there may be a case for some sort of enhanced security oversight of networks (in the same way has been required for critical infrastructure such as smart metering).

Privacy concerns are a topical subject within networks today [Ref 14], and in this environment SDN capabilities are of relatively low concern because the technologies they use that give rise to privacy concerns are already in use today (for example Deep Packet Inspection).

Virtual CPE for residential services may have some potential privacy implications, depending on their deployment model. The service can be deployed either by using the CPE as a layer 2 bridge (and sending all packets into the network) or by deploying an OpenFlow capable device at the customer premises and using OpenFlow to configure the CPE. The potential privacy issues arises from the fact that the service provider is effectively managing the home network and has much greater visibility of what is being done within it, rather than any implication from traffic snooping.

The nature of self-learning bridges is such that, while broadcast and flooded packets within the home will be sent into the network, this will not result in the hair-pinning of traffic flows through the network (as the CPE will learn the correct local interface for the traffic). In the case of the use of an OpenFlow switch as CPE the control plane will prevent hair-pinning by ensuring only WAN traffic is sent to the network. In both cases there is potential for the network operator to install mirror ports within the CPE (effectively snooping home traffic), however, as many service providers currently bundle their own CPE to customers today this possibility already exists in current networks.

The increased use of Deep packet inspection for service chaining and content optimisation may also have some privacy implications, but this is not related to SDN or NFV because this functionality has been deployed in carrier networks for some time, for example, parental controls, and the mobile networks policy, Traffic Detection Function (TDF) and content optimisation solutions. These applications are already handling sensitive information (for example, URLs) and a properly secured SDN/NFV solution will not add to the risk. From a regulatory perspective the same rules that apply to other network services with respect to privacy will continue to apply, for example, those rules preventing operators selling, or using confidential customer information for inappropriate purposes and for limiting the encroachment of big data applications.

4.6.5. Competition Issues

SDN and NFV introduce competition opportunities and threats. From an end user residential and business market perspective, the major benefit of SDN and NFV is that they will allow service providers to rapidly introduce new services to their portfolio, or to streamline existing ones.

The following high level examples show the sorts of competitive offerings SDN and NFV might enable if the promise of the technology is fully met.

- Self-care and self-provisioning for virtual private networking, either sold directly to the end user or to an ICT provider managing the end user's network.
- Managed home networks through virtual CPE and managed firewalls.
- Targeted security applications, such as DDoS protection for business and Intrusion Detection and Prevention Systems for residential and business customers.
- More flexible and customisable solutions for content filtering.
- Reduced cost of business CPE through virtualisation.
- Improved QoE through application aware networking, and distribution of functions (such as DNS or network PVR) closer to the end user.
- More scalable performance monitoring solutions, enabling more rapid isolation of customer issues.
- Improved mobile data performance as C-RAN results in more efficient use of the available spectrum.

However, there are potential competition issues that are raised by SDN and NFV. One major area of risk is around the APIs to the network (the northbound API) and another is related to the degree of service and network integration permitted and the ability of infrastructure providers to constrain the supported services.

Northbound APIs that are non-standard may be offered by large service providers to existing OTT content providers. If the APIs are compelling the content provider may choose to exploit them to improve the performance (or capabilities) of the application over the service providers network. However, smaller carriers may be unable to provide the APIs, or will provide different APIs that while functionally equivalent, require OTT provider integration. If the OTT provider determines not to bother carrying the costs of integrating with the smaller operators, then they will be at a disadvantage compared to their larger competitor. Even if the northbound APIs become standardised nationally or internationally, the smaller operator may be unable to get the OTT provider to offer the enhanced service over their network because the OTT provider may

not wish to bear the cost of the necessary legal agreements. Over time this may favour larger carriers over smaller ones (and vice-versa established OTT providers versus new upstarts).

Carriers that are able to offer an end-to-end integrated solution, including the access network, the metro network, mobile networks and cloud computing networks may be in a much stronger position to leverage the capabilities of SDN and NFV than carriers with only part of the solution. For example, in the case of virtual CPE, performance monitoring within the access network can be integrated into a carrier's end-to-end service assurance platform. For an operator supporting fixed and mobile network infrastructure, applications such as content filtering can be offered consistently as a device's network access changes, and content delivery solutions, such as network based PVR, may benefit from being able to be simultaneously located in the optimal location for both fixed and mobile infrastructure.

Within any given market, regulation may limit the extent of integration that is permitted (for example, in the UK the concept of open access networks), and with the appropriate mix of services within each network domain it should be possible to permit the same capabilities to be deployed as for a single integrated operator. However, it is true that the complexities of such a multi-domain implementation are likely to slow down the speed of deployment for these network architectures.

In these multi-domain networks, which typically have an infrastructure provider supporting wholesale customers, there is also the risk that the infrastructure provider can control the distribution of capabilities within the network. For example, they can choose not to permit NFV friendly IAAS beyond their data centres, or they can place restrictions on the virtual functions supported and how they can be configured. One example would be an infrastructure provider who constrained the vCPE capabilities supported by the network.

5. The SDN Use Cases and their Business Drivers

As noted previously SDN breaks down into three use cases, each with different objectives, economics and challenges. It is important to understand at a high level what each of these use cases entail and what the carrier hopes to get out of it.

5.1. Service Orchestration and Automation Use Cases

Tier one carriers have large OSS/BSS systems that sit at the core of their business and provide an automated provisioning interface to their customers for high volume services; unfortunately these systems are complex, have built up over many years, and are often fragmented. It is, therefore, usually the case that in any carrier environment the OSS/BSS is a bottleneck to service development and deployment. Typical carriers have a finite resource in the space and long development queues, this is particularly true if they are in the middle of a network upgrade; in these environments delays of up to two years are not unheard of to get a feature supported in the OSS.

While the OSS/BSS approach works well for simple high volume services (such as residential broadband or mobile services), it is very cumbersome for supporting value added services, or for low volume, high touch services such as Layer 3 VPNs. For these services a customer might wish to be able to pick from a menu of options, and the carrier may wish to be able to offer innovative product enhancements (such as advanced intrusion detection solutions). In this case the long OSS/BSS development times and costs are a block to deployment.

Operators are looking to Service Orchestration to provide an automated end-to-end service configuration solution that utilises SDN and NFV to fulfil the service whilst minimising configuration within the OSS. SDN supports the concepts of Service Chaining (being able to bolt together sets of atomic well understood services to create an end-to-end offering) and traffic steering by modifying the control plane as part of the service configuration. It is possible for the orchestrator to support many variations of a service or a service set without needing each variant to be specifically provisioned within the OSS stack. This can allow a customer to bolt together their own service variation from a service creation environment provided by the carrier, (for example, a web portal) and have the whole end-to-end connectivity built by the orchestrator and SDN controller. The automation of the process both ensuring rapid hands off delivery and repeatability/reliability of the service build. For a discussion of Service Chaining in the data centre see Section 6.2.1, and for an example of how MPLS Segment Routing can enable it in core networks see Section 7.6.

The automation use case for SDN does not just work for providing new services, it can also be used inside the carriers own network provisioning and operations processes. Currently, carriers spend a significant time optimising the traffic paths taken through the network to allow for likely

network load and to ensure that links are efficiently loaded. This often requires optimisation over multiple layers (the packet transport layer and the optical transport layer) and it may require configuration and maintenance of QoS functions such as MPLS-Traffic Engineering.

An SDN controller running a path computation application should be able to analyse the traffic in the network, determine the optimum traffic paths at the packet and optical layer to support the traffic and configure the routers, switches and Optical Nodes accordingly. This is a complex problem, but if correctly implemented can save OPEX by reducing the amount of resource required to perform manual path computations and network optimisation and potentially permit more efficient loading of the links. For further information on how the packet and optical layers can be optimised using SDN see Section 6.3.

Operators targeting this SDN use case are, therefore, seeking to achieve three goals:

- Reduced OPEX costs by removing repeated manual provisioning either to support service configuration or to support network resource optimisation and planning.
- Increased service velocity, by allowing services to be chained together in innovative ways and deployed without imposing OSS enhancements or incurring large manual provisioning overheads.
- Improving network utilisation, either by providing a more efficient way of chaining virtual services and/or by increasing the frequency of network resource optimisation.

The case for automation is, therefore, attractive at a high level, however, there is speculation as to how easy this will prove to be to implement in reality and carriers are likely to attack this use case as a series of tactical wins over a long period of time as set out in Section 10.2.

5.2. Application Centric Networking

Application centric networking takes the core concepts of automation and service chaining and extends them further via one or more open interfaces to the application layer (REST APIs being the most commonly proposed). The applications may be the carriers own or they may be customer / partner applications.

The principle of this approach to SDN is that if the network is able to expose information about its topology and state to the application, and the application is able to similarly share information about its specific requirements; then it is possible to either create dynamic new services, or to optimise the use of the network resources.

Examples of these types of applications are:

- On demand bandwidth services, which permit applications to request network resources with a guaranteed QoS when they need it and to release it when they do not. This can potentially be expanded to support bandwidth brokering applications. These applications are able to offer the cheapest possible options for connectivity which may vary on a time of day basis, depending on network loading.

- Multicast enablement services, which permit the network to signal the availability of multicast for a service, or for the application to request multicast for a service. This would make it much easier to invoke multicast capabilities for video delivery in broadband and mobile networks. For example, a mobile network could determine that a given video stream was being watched by a large number of users in a given location and offer a multicast service. The application could accept the service and then configure its clients to receive it (as described in Section 4.4).

- On demand service chaining and steering, for example, an enterprise determines that it is a target of a DDoS attack and requests additional DDoS protection from the network.

- CDN optimisation, the network could pass information about network conditions to a CDN partner application which might impact how the CDN application passed traffic into the network.

These types of applications require a suitable set of application or northbound interfaces to be defined to interface the network with application providers. This capability would also allow a carrier to upsell network capability beyond simple transport to OTT providers.

Carriers targeting this application of SDN are, therefore, seeking a number of business benefits:

- Additional revenue, by offering their customers value added services that have benefit and can be charged for.

- OPEX and CAPEX savings by potentially increasing the efficiency of the network, by encouraging their customers to maximise the use of network resources and smoothing demand peaks.

- Network differentiation by ensuring that the applications using the networks can maximise their chance of delivering a good service to the end user. This, combined with the options for smoothing demand peaks may be an enabler for the IET's "Demand Attentive Networks" concept [Ref 15]. Similarly by exposing a flexible application interface the carrier may encourage high value customers onto their network because it is an attractive and flexible platform for them to build their own services on top of. In effect the carrier is offering their customer enhanced service velocity. This may be attractive to organisations selling, for example, flexible layer 3 VPNs supported on carrier infrastructure.

Application Centric Networking could potentially provide carriers with the additional revenue streams that they are seeking as they struggle to avoid becoming simple commodity. Furthermore it offers the potential to improve the customer experience and also improve network utilisation. However, of all the SDN use cases this is also the least defined in the standards and the one that is hardest to implement in carrier networks because of the commercial considerations. The issues of application APIs are explored in Section 7.7.

5.3. Network Functions Virtualisation Support

Network Functions Virtualisation, as discussed in Section 3.2, is separate from SDN, but part of the SDN landscape and, therefore, considered in scope for this report. It is certainly the case that NFV may have a significant impact on telecommunications networks and services in the future.

Carriers looking to deploy NFV may have a number of different motivations:

- They may wish to migrate their existing applications such as DNS to an NFV platform to provide them with more flexibility in respect to scaling the application. For example, a carrier could seek to improve the performance of DNS by migrating from a few large platforms on dedicated hardware to a large number of smaller platforms deployed on COTS hardware and distributed throughout the network.
- They may wish to have more flexibility to scale out their platforms in order to react quickly to changing network circumstances, (for example, a DDoS attack), or as part of a gradual introduction of a service for which demand is uncertain.
- They may wish to decouple the hardware platform in the data centre or metro node from the applications it is supporting. This will permit them to cope with changing customer demand patterns over time, without hardware swap out; and to support more flexible solutions for service chaining.
- They may be looking to reduce the costs of CPE for business services by replacing high cost and inflexible layer 3 CPE for some customer sites with a lower functionality (cheaper) layer 2 CPE and a network based virtual CPE function. This virtual CPE can provide the layer 3 routing functions and possibly value added services such as firewalling and intrusion detection. It can do so more cheaply than dedicated hardware in the customer premises and it can be upgraded far more easily.
- They may be seeking to reduce the operational costs associated with broadband residential CPE. This typically results in home networking faults being raised as faults with the operator's service, or it may result in customers leaving an operator because their own home network is preventing the service from working. By deploying a virtual CPE solution for residential customers the operator hopes to manage the customer home network and have visibility of its operation, making problem resolution significantly easier. This

approach also has the advantage that the virtual network function can be enhanced to support additional requirements (such as IPv6) without swapping out the CPE.

- The carrier could be looking to decouple the service functions supported by a network platform such as a BNG, from the hardware that performs packet forwarding. This may also allow them to deploy their own customised applications rather than being beholden to the vendor's product roadmap. For example, a network operator may wish to create their own policy engines and authentication platforms instead of purchasing a router vendors service card for a BNG.

- There is also a more ambitious approach, that seeks to replace network routing and switching functions that run on dedicated hardware with virtual network functions operating on x86 hardware where traffic volumes make this possible. A variation on this approach is that the operator may look to replace router vendor hardware with a lower cost hardware acceleration platform for packet forwarding (a white box) and a router control plane running as a virtual network function.

There is a degree of consensus within the carrier community that NFV is an important technology, however, there are a large number of different use cases being defined and promoted by carriers as described in Section 8. It is certainly true that not every carrier is interested in every use case.

Depending on the use case being targeted, the carrier may be seeking the following business benefits:

- CAPEX reduction by replacing expensive dedicated network hardware with cheaper virtual network functions running on COTS x86 platforms, and possibly white box commodity hardware acceleration.

- Additional flexibility in deployment by being able to quickly spin up virtual network functions in response to a sudden demand for a service and to chain them together to produce composite services. The use of COTS x86 platforms avoids the need to deploy dedicated hardware, and the ability to source virtual network functions from different vendors can remove the risk of vendor roadmap delivery.

- OPEX reduction, for example, by using virtualisation to standardise CPE (both business and residential offerings) and deploying a management wrap around previously unmanaged networks; or by deploying simpler virtual solutions, for example, a virtual EPC for a dedicated customer, instead of a more complex partitioning of a single large platform.

The architectural impacts of NFV are described in Section 6, an overview of the current state of the art and its potential limitations are described in Section 8. It should be noted that while many claims are made for NFV from a business benefits perspective the industry is divided as to the cost benefits of the technology for carriers, and this is especially true for the more challenging

NFV scenarios, such as the virtual IP edge described in Section 6.6.3. The reasons for the divergent views of cost benefits are discussed in Section 4.2.

6. Network Architecture

The networks that carriers deploy today have an architecture that has been refined over a number of years. Some aspects of this architecture are to a degree fixed by geography and topology, others are more variable and subject to changing design views.

This section describes the architecture of a Software Defined Carrier Network. It describes the differences between the network domains and shows how these drive different SDN requirements and implementations. The SDN controller functions, interfaces and protocols that may be deployed within each of these domains are covered in more detail in Section 7.

6.1. The Software Defined Carrier Network

The Software Defined Carrier Network leverages SDN and the performance of NFV infrastructure to minimise the number of service-specific nodes within the carrier network and to enable application-aware networking.

Carrier networks are structured by the requirements of different network domains and this will not change with the advent of SDN. This report categorises these network domains as data centre, core and access. There are also some key locations within the network of interest for Network Functions Virtualisation. The Service Node, Evolved Packet Core, Provider Edge Routers and Customer Premises Equipment are potential targets addressable by NFV infrastructure. This means that in a software defined carrier network, an operator can try to replace physical infrastructure with distributed NFV infrastructure whilst retaining network transmission technology specific nodes, for example, Digital Subscriber Line Access Multiplexer (DSLAMs), eNodeBs and transport nodes (aggregation and core).

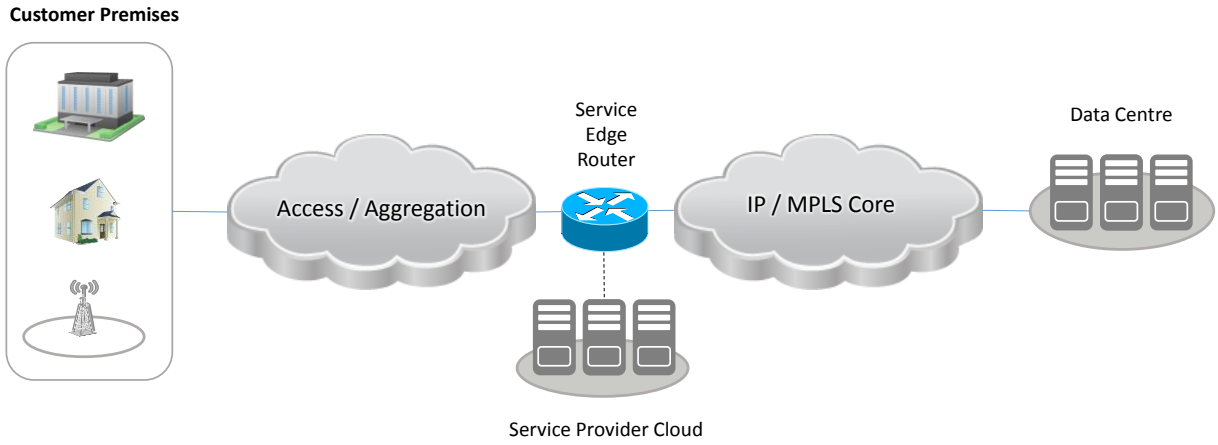

Figure 8 Reference Network Architecture

Figure 8 shows the reference architecture used within this report highlighting the different network domains. The typical migration approach towards carrier SDN is through discrete implementation in each network domain. This is driven by:

- The different networking topologies and technologies present in each domain.
- Business drivers differing between optimisation and monetisation.
- Service provider organisational constraints.

The SDN control plane is separate from the existing element management / network management systems. Therefore, an SDN controller and network application framework will need to integrate with network management systems for the domain concerned. An opportunity for SDN is that it might provide a path for a network operator to configure services with a lower burden of OSS change than in the absence of SDN.

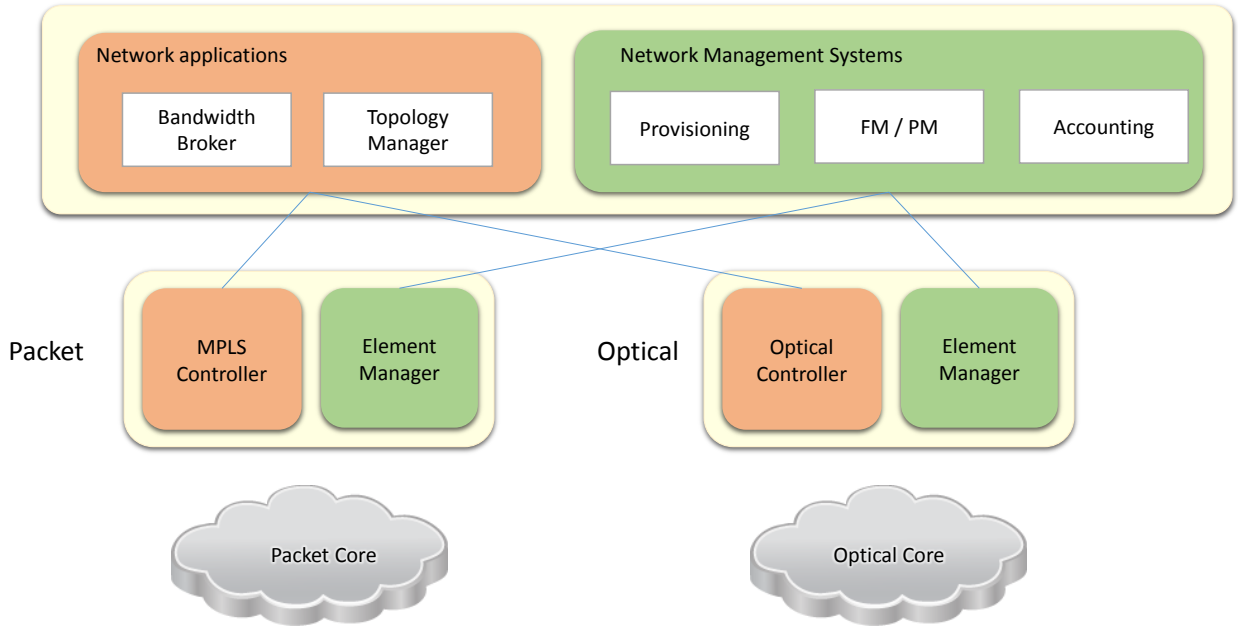

Figure 9 Hierarchical SDN in a Converged Core Network

Within a domain there may still be multiple technologies that need to be orchestrated to achieve the business objectives. Figure 9 shows an example of this for a core network. The core network consists of packet and optical networks. There are a number of ways to manage these, from one extreme where they might be regarded as independent network domains, to another where there is convergence at the management and control layers. In practice most networks are somewhere in-between. In such an approach with a loose coupling of the management systems between packet and optical it might be possible to deploy SDN for one layer while leaving the other with a traditional implementation of embedded control plane and network management systems. In any case there must be at least some co-ordination between the OSS and the SDN controller in order to delegate control of interfaces to the SDN controller and configure the control channels.

Software Defined Networking does not necessarily mean that existing network protocols are replaced. Any migration plan requires a mechanism to emulate control protocols between an SDN and non-SDN domain. At inter-operator Network-Network Interfaces, this situation may be permanent, especially where the protocols have been optimised over time to solve the specific problem of inter-domain interfaces.

Implementing existing network protocols with separation of control plane and data plane may require distribution of functions for performance reasons. Figure 10 shows an example distribution of SDN functionality for an MPLS implementation. In this example path computation is centralised to make use of a network wide topology view. The control protocols are regionally distributed to make use of available NFV infrastructure, while some functions are co-located with the network element to minimise latency and leverage hardware acceleration on the network elements.

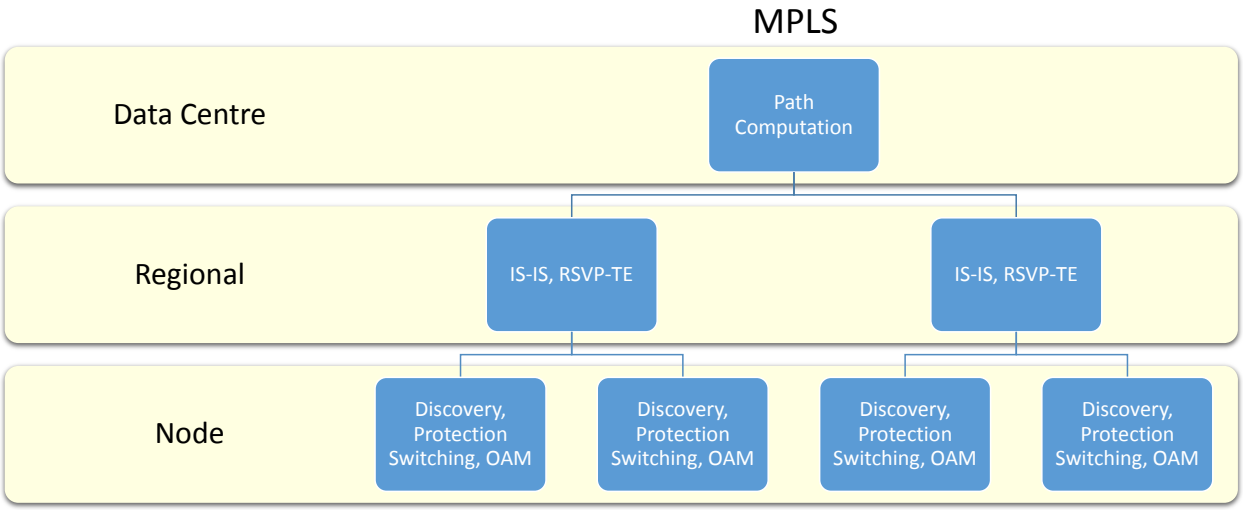

Figure 10 SDN Function Distribution – MPLS

6.2. Data Centre

Data centre orchestration is the origin of SDN. Virtualisation of the compute infrastructure and applications such as virtual machine migration created a requirement to automate the provisioning of the supporting data centre network. This section gives a summary of SDN in the data centre and then relates this to service provider applications.

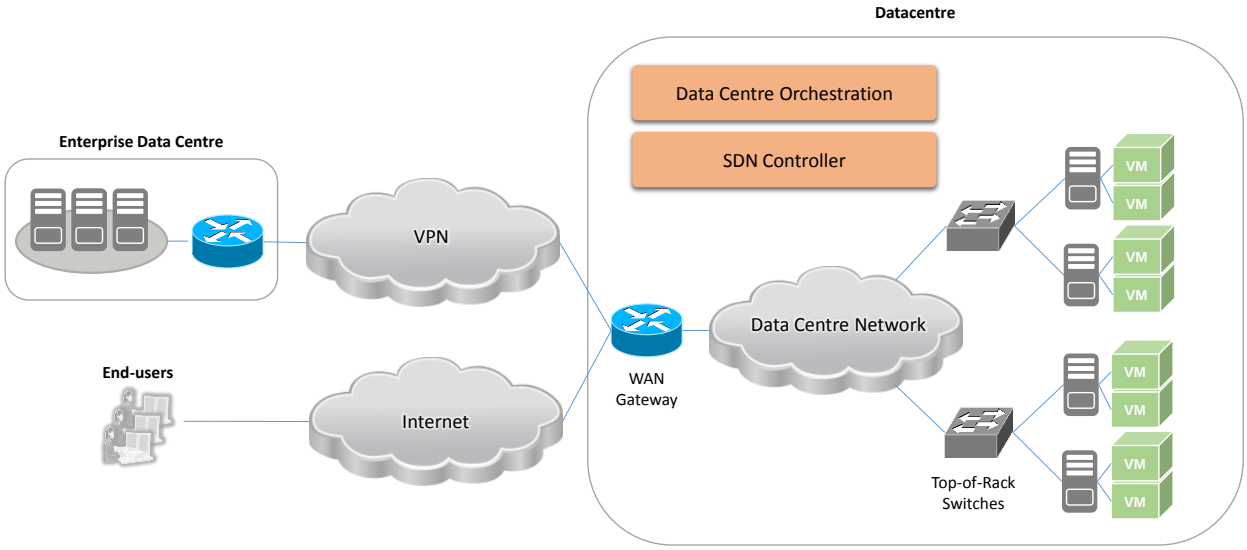

Figure 11 Data Centre Networking

The data centre network, as shown in Figure 11, connects the WAN gateway and top-of-rack switches providing connectivity to servers together. This infrastructure is unified so that non-IP based network protocols, for example, Fibre Channel over Ethernet (FCoE) can be supported by data centre orchestration systems in the same way as any other protocol that can be mapped over Ethernet. FCoE is one example of storage virtualisation that means SDN orchestration provides a mechanism that unites the three key infrastructure components of Compute, Storage and Network.

The nature of the data centre network depends on the scale of the infrastructure. For small private cloud deployments it may be sufficient to mesh together top-of-rack switches. Larger deployments make use of fabric architectures that exploit a core layer of switches and require multipath support at the Ethernet layer to scale bandwidth. This multipath requirement is beyond the capability of traditional Ethernet forwarding based on Media Access Control (MAC) learning / spanning-tree. Ethernet fabrics, therefore, deploy a control plane, often based on IETF Transparent Interconnection of Lots of Links (TRILL), to provide routing capability for MAC addresses.

The data centre network now extends beyond the physical switched infrastructure terminating at top-of-rack switches and into the hypervisors of virtual machines. This has spawned a class of virtual switches implemented within the hypervisors that forward traffic between physical network

interfaces and the virtual machines virtual network interfaces. This layer of virtual switches is an area of competition between different SDN solutions.

In an overlay approach, it is possible to create overlay networks which separate the orchestration of connectivity between virtual machines and the forwarding of the underlying data centre network. The overlay technologies used in the data centre depend on the overlay vendor and hypervisor chosen and include Virtual Extensible LAN (VXLAN) and Network Virtualisation using Generic Routing Encapsulation (NVGRE). The separation of overlay / underlay networks is familiar to service providers where technologies such as MPLS provide a key mechanism to isolate the operation of core networks from the services they provide. Alternative approaches extend the data centre fabric into the virtual switching layer. This provides more control of the network paths but provides less flexibility to manage the services separately from the network.

A data plane control protocol such as OpenFlow provides an alternative approach to controlling the data centre network infrastructure. The deployment of OpenFlow switches gives the data centre operator flexibility to innovate at the network layer by directly controlling the routing of traffic. This approach has been termed data plane SDN. It can be deployed as a replacement for an Ethernet fabric control protocol like TRILL. This is more disruptive to the data centre infrastructure than deploying a pure overlay, but gives the SDN controller more visibility of the data centre resources than an overlay approach. The OpenFlow protocol can be implemented either as an add-on to more fully featured platforms or on a white-box switches that are entirely managed by OpenFlow. Extending OpenFlow into the hypervisor virtual switches can allow a flat data centre network to be created although this does not have the scaling and isolation benefits of using an overlay.

6.2.1. Data Centre Service Chaining

In a virtualised data centre environment, the SDN infrastructure is used to connect together virtual machines, network services and WAN access. The connectivity typically appears to a virtual machine as a Virtual Local Area Network (VLAN) regardless of how this is implemented by the SDN infrastructure. A typical application architecture uses components such as load balancers and firewalls as hops in a network path. In a virtualised data centre these network services may also be implemented as virtual appliances. The SDN controller stitches together these network services providing connectivity between the various Virtual Machines that the applications are running on.

The services themselves must be provisioned by a data centre orchestration function such as OpenStack. The OpenStack project [Ref 16] is producing an open source orchestration framework that includes among other things Compute (Nova), Block Storage (Cinder) and Networking (Neutron) orchestration components. The Neutron component is responsible for requesting the network connectivity between the service elements, and this request can be fulfilled by an SDN

controller. The initial Neutron interface supports the VLAN overlay abstraction for datacentre connectivity, while Neutron v3 will add awareness of more complicated L3 domains, for example, Internet VPNs and policy rules.

The data centre operator builds business logic above the orchestration function to provide ordering, billing, customer portals. In a telecoms environment this is equivalent to the interfaces to the OSS/BSS.

6.2.2. Service Provider Applications in the Data Centre

Network service providers have a number interests in data centres. Firstly, a service provider is likely to operate a number of data centres as part of their enterprise infrastructure. These will support some network functions and application services. Cloud services are increasingly being bundled with network services so, for example, a service provider might choose to deploy a hosted VoIP or collaboration service together with network connectivity. In this sense a service provider will likely be deploying SDN in the datacentre as part of the trend towards data centre virtualisation that is already well established in the IT industry.

The earliest examples of NFV in a service provider network are often like for like replacements of hardware appliance solutions with directly equivalent virtualised appliances in the datacentre. DNS is a commonly cited example of a service that can utilise the scaling benefits of virtualised infrastructure. The service chaining application for service nodes described in Section 6.6.1 has the same solution space as service chaining in the data centre and so can make use of SDN orchestration techniques.

Synchronisation and backup between data centres can require a large amount of bandwidth for short periods. This provides an opportunity for service providers to offer a bandwidth calendaring application for data centre interconnect services that allows WAN bandwidth between data centres to be flexed at different times of day. Depending on the bandwidth required this could leverage the optical layer in addition to the packet layer using multi-layer optimisation discussed further in Section 6.3.3.

Data centre interconnect is a service provider product that spans a number of use cases. Connectivity can be data centre to data centre or data centre to enterprise. Making this seamless creates a requirement to merge the virtual bridge domains in the different data centres. In the enterprise to cloud case, this is often performed using internet VPNs to tunnel between the two domains. However, quality of service can be improved by integrating between the data centre network and managed L2VPNs operated by the network carrier. A L2VPN technology can be extended from the WAN into the data centre, or the data centre WAN gateway can interwork between the data centre overlay technology and the L2VPN. Integration must be performed at all three of the data, control and management planes. A complete solution could enable applications

such as cloud burst where an enterprise leverages the scale of the public cloud to smooth uneven loads within a private cloud implementation.

6.3. Core Network

Network operators have converged on IP/MPLS at the packet layer for their core networks. This is typically supported by a Dense Wavelength Division Multiplexing (DWDM) transmission network for all but the smallest operators. These networks are frequently operated by different functions within a network operator with loose co-ordination to allow optical paths to be provisioned to support the needs of the links between Core IP/MPLS routers.

6.3.1. IP/MPLS

Standards for IP/MPLS networks have evolved from their beginnings as solution for fast-packet switching to make MPLS the technology of choice for a multiservice core network. MPLS provides the ability to use an IP based control plane to control label switched paths built across the core network. The MPLS encapsulation removes the requirement to implement full service awareness at each core router. Service intelligence is constrained to the Provider Edge (PE) routers at the edge of the network. The original example of this is MPLS based L3VPNs where the address space for the customer VPN is shared between MPLS Provider Edge routers using BGP while MPLS core routers can forward traffic by classifying on the MPLS label stack. Similar constructs have been deployed using MPLS pseudo-wires to provide emulation of layer-2 Ethernet and Time-Division Multiplexing (TDM) circuits.

SDN marketing refers to underlay and overlay networks. In the case of MPLS applications, a pseudo-wire connection typically uses a pseudo-wire (inner) label within a tunnel (outer) label [Ref 17]. Multiple pseudo-wires each with a unique pseudo-wire label can share the same tunnel. The tunnel Label-Switched Paths form an underlay network that can be managed independently from the pseudo-wires that are mapped or overlaid on them. This means that SDN technologies can be applied to the tunnel layer, the pseudo-wire layer or both depending on whether it is the overlay or underlay network that is being optimised. Data centre applications of MPLS have so far focussed on overlay networks.

Network operators deploy differing approaches to traffic engineering in an MPLS environment. One approach relies on provisioning sufficient bandwidth such that capacity admission control across the core network can be performed offline. The parameters of the IP interior gateway protocol are tuned to ensure that there is a level of determinism in the path selection. An alternative approach requires signalling of bandwidth reservations across the core network using an MPLS optimisation of the IETF resource reservation protocol (RSVP-TE). This reserves bandwidth between pairs of PEs and provides mechanisms for local repair of faults for fast

protection switching using MPLS fast re-route and path pre-emption if sufficient bandwidth is not available at any congestion point in the network. The RSVP-TE paths can either follow the Interior Gateway Protocol (IGP) or be pre-computed via a Path Computation Element. Services mapped over the traffic engineered network can utilise load-balancing to improve utilisation of spare WAN capacity.

SDN approaches to re-engineering the core network centralise the path computation function, removing it from the network nodes. Both PCEP and OpenFlow are possible protocols to provision the computed paths in the network. The Google B4 network [Ref 18] has been the poster child for OpenFlow implementations in the WAN. Google achieved a 2-3 times improved efficiency in its usage of WAN capacity between data centres by deploying OpenFlow controlled edge routers, and integrating this SDN environment with a centralised bandwidth management and traffic engineering function. OpenFlow is discussed in Section 7.3. The PCEP approach uses a Path Computation Element together with an interface to the IGP to synchronise the Traffic Engineering Database (TED) so as to allow an SDN controller to influence the selection of routes within an MPLS network. This is discussed in more detail in Section 7.5. In addition, technologies such as Segment Routing are also being proposed. This changes the semantics of the MPLS label stack to improve the scalability of traffic engineering and to permit traffic steering. This is discussed further in Section 7.6.

Two similar alternatives to running a full IP/MPLS control-plane have been standardised that provide a more connection oriented approach to service provisioning and OAM. This has been attractive to implementers of transport equipment where the complexity of implementing a full MPLS control-plane has been a barrier to getting products to market. MPLS Transport Profile (MPLS-TP) reuses the MPLS data-plane while Provider Backbone Bridging - Traffic Engineering (PBB-TE) provides a similar construct using provider Ethernet. In both cases, the forwarding path is configured using an OSS rather than a control protocol. Fault restoration is provided by end-to-end protection switching. Of these two, MPLS-TP perhaps has the greater traction in the industry due to the greater deployment of MPLS pseudo-wires as a client-layer transport. The configuration interface for both MPLS-TP and PBB-TE has relied on flow-through provisioning via the equipment EMS and NMS, similar to the model for legacy circuit switched networks. There is an opportunity for implementation of an SDN interface such as OpenFlow on these Network Elements to provide an alternative route to service provisioning that bypasses the traditional OSS stack. This is discussed further in Section 7.3 on OpenFlow.

The original MPLS implementations were constrained to operate within a single network operators' domain. Interconnect required falling back to the client layer protocol, for example, Ethernet / IP. More recent extensions have permitted an MPLS inter-carrier interconnect, which allows the MPLS encapsulation to be presented at the NNI between different service providers. In addition to the MPLS encapsulation, the interconnect definition includes the client-layer signalling, routing and OAM protocols required to operate the end-to-end services. The

extension of an SDN network domain across an inter-carrier interconnect would require similar standardisation of interfaces at the data and control-plane. One of the components of this would be an interface between SDN controllers, which has not yet been attempted, although PCEP allows for multi-domain bandwidth reservation. For this reason any SDN extension across interconnects is likely to lag any deployment of SDN within the carrier. Initially, NNIs will require an SDN domain to emulate the operation the existing data-plane protocols, (for example, IP, MPLS, Ethernet) and control-plane protocols, (for example, BGP).

6.3.2. Transmission Networks

Transmission networks are migrating from Synchronous Optical Network Technology/ Synchronous Digital Hierarchy (SONET/SDH) transport to Optical Transport Networks (OTN) utilising DWDM. In the Core, optical networks include the flexibility to build a logical path without physically configuring the network nodes. This can be achieved either by using optical wavelength selective switches to build Reconfigurable Optical Add/Drop Multiplexer (ROADM) networks, or by using OTN switching at the electrical layer. OTN framing is common to both approaches, as it provides the means to add an overhead to the end-to-end path for trail supervision and Forward Error Correction (FEC).

The configuration of end-to-end paths in a transmission network using OTN switching or ROADMs is either performed using configuration at each switching node, or signalled end-to-end on the path. In the latter case, this is achieved using Generalised Multiprotocol Label Switching (GMPLS) extensions to the RSVP-TE protocol that is used for IP/MPLS signalling in a packet network. Similarly to packet networks, path computation can either be performed by the network nodes, or can be computed offline using the operators Network Management System. An ONF working group has been established to investigate use cases for SDN in an Optical Transport Network and potential OpenFlow extensions for configuration of OTN paths. This is discussed in more detail in Section 7.3.

ROADM technology has evolved over time. Original designs had constraints on the wavelengths that could be dropped at each node, the number of fibre directions (degrees) that could be switched, the combinations of wavelengths that could be switched, and the upgradability of nodes once they have been deployed. Current generation ROADM designs are available that are colourless, directionless and contentionless; which removes these constraints simplifying the task of path computation. However, the task of optical network design and path computation often relies on vendor specific tools that run either offline, or are centralised in an NMS to offload this requirement from the network nodes. As the upfront design constraints are removed, the possibility of performing more of the path computation and optimisation at runtime becomes more realistic. This function is being integrated into SDN controllers for transport networks.

Next generation ROADMs are being developed that introduce a 'Gridless' characteristic. DWDM relies on a frequency grid defined by ITU-T G.694.1 [Ref 19] which specifies the channels (wavelengths) that may be used by optical signals. Grids are defined with 12.5 GHz, 25 GHz, 50 GHz and 100 GHz spacing between the bearer channels, with the spacing chosen depending on the fibre characteristics and modulation schemes required for the client signals. Traditionally, DWDM networks have operated with a fixed grid. However, recently core transmission systems have begun to make use of super-channels to improve spectral efficiency for clients supporting greater than 100 Gbps per channel. DWDM channels are grouped according to a flexible grid that allows the channels to be bundled together into a super-channel while still providing inter-operability with conventional fixed-grid channels. Flex-Grid aware ROADMs will be able to switch these super-channels in addition to channels on a fixed DWDM grid. The grooming of services using this flexible grid to defragment the available optical network capacity is currently a labour intensive process and provides a key opportunity for intelligent network provisioning systems in future optical transport networks.

6.3.3. Bandwidth Optimisation and Packet/Optical Convergence

Many use cases for SDN in the core network focus on bandwidth optimisation. Service providers may be able to offer elastic bandwidth applications that make use of application layer knowledge of bandwidth requirements. The most often cited example of this is for data centre interconnect where there are some workloads such as backup and database synchronisation that place short duration demands on WAN bandwidth. If a network operator offers an interface to request these short term bandwidth reservations, then the application could potentially realise a saving on the cost of WAN bandwidth. Depending on the WAN capacity required the additional bandwidth could be delivered using either packet or optical infrastructure. The more predictable the traffic patterns are, the higher the potential savings as the application can be tighter in its bandwidth scheduling.

The alternative use case is internal to network operators. The challenge is to deliver today's network services more efficiently over the core network infrastructure that has already been deployed. In today's networks the packet and optical layers are loosely coupled. The optical transmission network provides the circuits that carry the links between core routers. The selection and dimensioning of which circuits to provision is largely an offline, manual process that is computationally intensive. It does not react quickly to the changing bandwidth requirements of the packet layer. If an SDN controller can build a multi-layer view of physical and logical network topology together with utilisation that is updated in real-time, then SDN applications that simultaneously and reactively optimise both layers of the network may become possible.

Some of the network enablers for this are already in place. Physical integration between the packet layer and optical layers allows optical transceiver costs to be optimised. DWDM optical interfaces are being deployed on MPLS routers removing the requirement for back-to-back

transponders at the optical layer. Tuneable optics mean that it is possible to logically groom circuits at the optical layer in this collapsed model without site visits to replace the router optics. Packet-optical platforms are available that combine optical transport and packet switching. Dark resources – router interfaces that are connected to the optical layer on-demand – can be used to flex the capacity between any pair of routers. The optical layer signalling for these interfaces can be performed by extending the optical layer GMPLS control-plane to the IP/MPLS router or by using a multilayer OSS/controller to orchestrate the configuration of the two network layers.

The major challenge to this vision of multi-layer optimisation come from operator organisational constraints and the technological complexity of integrating a multilayer SDN, orchestration and BSS solution.

6.4. Access Network

6.4.1. Fixed Access Network

The fixed access network differs from the core network in terms of topology and node complexity. Figure 12 shows an overview of typical fixed Access Network Architecture, as defined by Broadband Forum TR-101 [Ref 20].

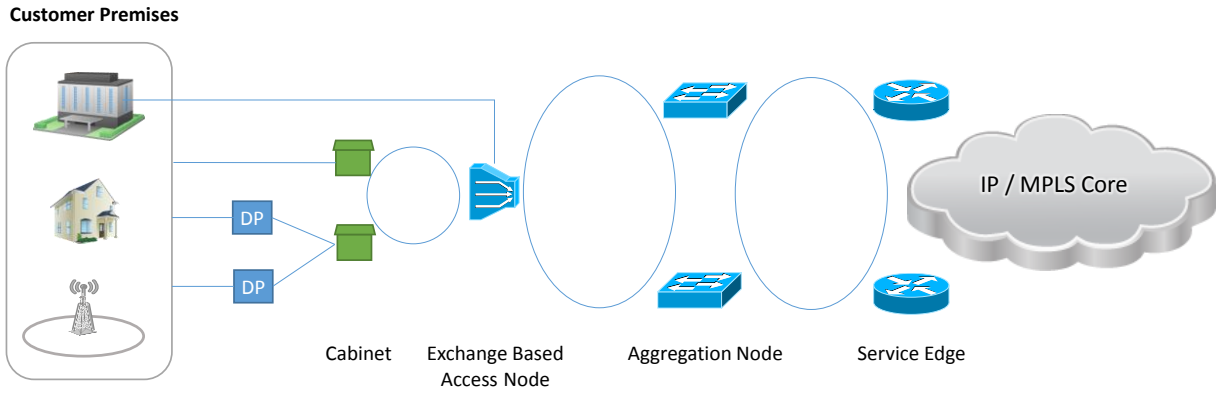

Figure 12 Fixed Access Network

Implementations of the metro aggregation network for TR-101 use either Carrier Ethernet or Ethernet over MPLS backhaul techniques to connect the exchange-based access node to the Broadband Network Gateway. In many operators there is convergence between the BNG and the MPLS PE functionality used for business services. It is marked here simply as Service Edge. This recognises that many implementations use the BNG to centralise service logic, (for example, authentication, authorisation, accounting, traffic management) and have tried to limit the complexity of all downstream nodes. This lowers the operational costs for access nodes as it is common that the access network is a multi-vendor environment.

Broadband Forum TR-101 defines the Ethernet capabilities required on an Access Node and this has been extended to support Fibre to the Home (FTTH) networks using Gigabit Passive Optical Network (GPON) and Very-high-bit-rate Digital Subscriber Line 2 (VDSL2). Remote broadband access nodes are typically designed around an Ethernet switching function while MPLS functionality is more common at central-office based nodes. The physical backhaul topology of the access network means that while there is potential gain to be had from load balancing across a pair of backhaul links, greater efficiency gains similar to the fabric approaches deployed in a core network environment are not possible.

To a certain extent, functionality within the broadband access network has already been centralised before the introduction of SDN. Multi Service Access Nodes may provide application layer functionality e.g. Session Initiation Protocol (SIP)/H.248 gateway functionality for Public Switched Telephone Network (PSTN) services. H.248 already provides separation of the voice signalling control from the media adaptation and transport functions. Subscriber management and IP functionality is performed at the BNG rather than at the Access Node. In addition, the Access Node Control Protocol (ANCP) allows the multicast control plane to be centralised at the BNG. Both H.248 and ANCP can support a node partition concept, similar to OpenFlow slicing techniques. Together, with limited potential backhaul efficiencies, this means that SDN in the access network has to date been of less interest to network operators than other domains.

However, one of the promises for SDN in the metro / access network is that while the network elements are specialised, the control plane can be further centralised. This would provide the ability to run more complex topologies than can be supported by the current Ethernet focussed model without pushing a fully featured IP/MPLS control and routing plane onto nodes that are often mixed vendor and subject to long technology refresh cycles. This means that in return for the effort of implementing SDN there is the potential to reduce interoperability issues between network nodes. SDN in Access Networks is a current study topic in the Broadband Forum through SD-313. While this is a work in progress, it puts forward the following SDN use cases:

- Plug and play for remote nodes
- Access network open interface for wholesale
- SDN driven network located residential gateway
- SDN driven business CPE
- Bandwidth on demand for hybrid clouds
- Centralised subscriber state management

As broadband access nodes are distributed deeper into the access network with VDSL2 and potentially Fibre to the Distribution Point (FTTdp) deployments in the future, there is a driver to try to minimise the complexity of the remote access nodes and centralise control plane functionality on an exchange-based access node. In this case the access node could run an OpenFlow controller to control the forwarding behaviour of subtended access nodes. This means that the subtended access nodes do not need to operate a full management plane. This may be

particularly relevant in the case of FTTdp where the power constraints on the node may mean that there is very limited processing resource available.

Fixed access / metro networks have converged on carrier Ethernet as the service layer technology of choice, so any transport technology that can support an Ethernet services layer can be used. Network slicing is OpenFlow terminology for partitioning the network bandwidth and forwarding space. For an Ethernet based access environment this is effectively partition of bandwidth by VLAN or MAC address. Implementing centralised MAC address learning in an SDN controller could improve security for some deployment models where end-users share VLANs. However, the 1 VLAN per user model used by Ethernet ALA [Ref 11] that is currently deployed for logical access network unbundling in the UK, would not benefit from this. Therefore, SDN in the access network may not provide any additional capability for an operator who has already implemented ALA.

Use cases around CPE and bandwidth on demand are covered in other sections.

6.4.2. Wireless Access Networks

In the modern network there are a large number of wireless access networks of differing types. The mobile network RAN is the most important for carrier networks, but even this is typically a highly complex mix of technologies with greatly differing capabilities. These networks currently consist of the following:

- LTE mobile access offering high speed data suitable for a wide range of applications.
- 3G mobile access offering data speeds adequate for most web browsing.
- General Packet Radio Service (GPRS)/Edge mobile access offering very limited web browsing but adequate for Machine to Machine (M2M) communications.
- Public Wi-Fi access, offering variable quality data rates either as part of a dedicated public Wi-Fi network or as part of the FON network.
- Whitespace access, suitable for some non-critical M2M applications.

While the mobile networks are brought together under the Evolved Packet Core concept to provide the user with seamless mobility between the network types, Wi-Fi networks are typically separate and were historically hard to integrate with the mobile data experience.

This has led to initiatives to optimise the use of these differing access networks (referred to as a Heterogeneous Network, or HetNet). A key focus of his effort it to try and integrate mobile and Wi-Fi infrastructure (from a user perspective at least) two approaches being HotSpot 2.0 and the 3GPP EPC ANDSF. These two approaches to exploiting the heterogeneous nature of the RAN

are very different technically and commercially. HotSpot 2.0 takes a user driven approach while ANDSF takes a network driven view, (for example, to enable Wi-Fi off-load). It is important to note that neither of these solutions use SDN to achieve their objectives.

While SDN is not a major component of wireless access network solutions it is being considered for optimising authentication in some Wi-Fi applications, and for optimising the traffic path in Wi-Fi and mobile applications (see Section 6.6.2). The use of SDN for the optimisation of the RAN backhaul may become more compelling with the increased use of femto and pico cell infrastructures. This is particularly the case where the small cells use Self Optimising Network (SON) techniques to configure the radio path, but are not part of a Cloud RAN. This may, in some deployments, lead to rapidly changing radio connectivity with fluid backhaul requirements. These types of deployments would benefit from a central management capability enabled by SDN.

Whitespace networks are specialist applications which seek to share low frequency M2M friendly spectrum with other infrequent (but high priority services) such as outside broadcast support. While SDN could play a role in distributing the frequency database to whitespace nodes (which informs them which frequencies they may use), it is not a natural application of the technology and other solutions will work equally well.

Some papers have proposed the use of SDN technology within the RAN, as an alternative to the 3GPP LTE architecture, one example of this being the SoftRAN concept from Stanford and Bell Labs [Ref 21]. While these concepts are interesting it seems unlikely that they will gain traction (given the maturity of LTE), and they fail to address many of the benefits offered by the emerging Cloud RAN concept.

Cloud RAN is a key concept with the LTE architecture that exploits the benefits of centralising the RAN processing within an area. The eNodeB is in effect distributed between the C-RAN hostel and the radio head end at the cell site. In this architecture the cell site simply acts as the transmitter and receiver of the radio, all of the encoding and decoding decisions are made in the cloud. The interface between the radio head end and the C-RAN hostel is effectively radio over glass (or radio over microwave) and is known as CPRI. The connection between the radio head end and the Base Band Unit (BBU) is described as a fronthaul interface.

This architecture has been adopted as a key ETSI-NFV use case and is shown in Figure 13.

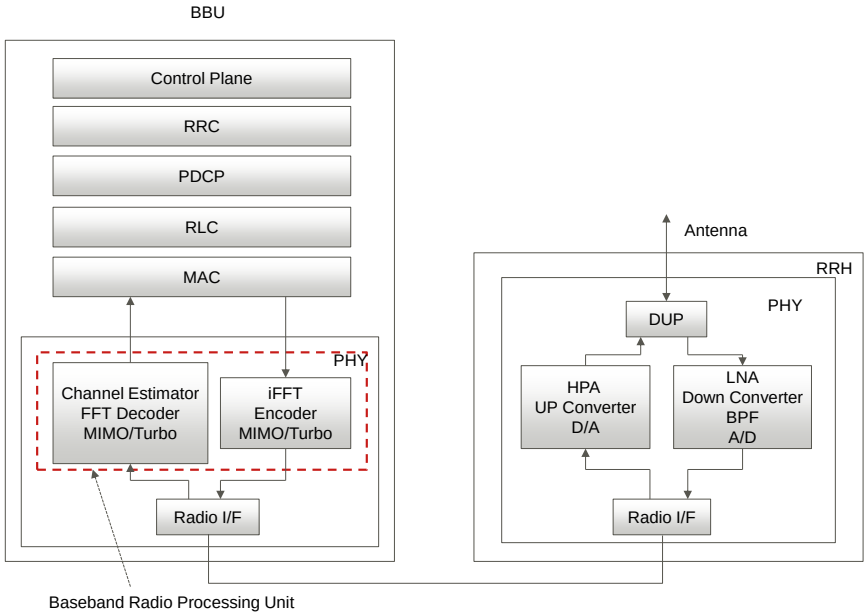

Figure 13 C-RAN ETSI Defined NFV Use Case

The CPRI interface has a number of limitations: it is very bandwidth hungry, requiring multiple gigabits per second per cell site; it is extremely delay sensitive, limiting the effective fronthaul distance for fibre connected sites to between 20 and 40 km; it cannot be transported over Ethernet, requiring dark fibre, microwave or WDM transport.

However, despite these limitations the potential for radio network optimisation, the pooling of BBU resources and other benefits make this a key target for NFV. China Mobile claim C-RAN offers CAPEX savings of 30% and OPEX savings of 53% for some deployments [Ref 22]. Many of these benefits are related to space and power savings at the remote cell sites, although some gains come from simplification of handover and resource pooling. There are also benefits in terms of Cell Edge performance by permitting the use of Coordinated Multi-Point (CoMP) joint processing. KT have deployed a commercial cloud based LTE solution (which is branded as LTE WARP) and claim a capacity increase of between 60% and 80% because of cell edge improvements [Ref 23].

It should be noted that this application is pushing the very limits of virtualisation, see Section 8, and may also be impractical in fibre poor countries, such as the UK. Therefore, this application of NFV may be restricted in some markets to niche deployments such as large campus environments.

6.5. Mobile Aggregation and Backhaul Networks

The SDN environment is slightly different between mobile and fixed network operators, because of the EPC deployed by mobile operators. In a mobile network the access component is provided by the RAN and the traffic is backhauled over microwave and fibre links to a comparatively centralised EPC. The EPC provides mobility management, policy, security and charging functions for the mobile operator. In addition it supports integration with Wi-Fi networks and facilities such as multicast services. The functions of the EPC are defined by 3GPP and are out of scope of this document.

Mobile traffic is carried from the eNodeB to the Serving Gateway over an aggregation and backhaul network, typically Ethernet based and then onwards to the home network Packet Gateway. There are a large number of variations and options in the EPC with regards to protocols, from an external viewpoint the mobile terminal's IP address is allocated by the Packet Gateway (P-GW) and carried over the necessary infrastructure using tunnelling solutions such as GPRS Tunnelling Protocol (GTP) and Proxy Mobile IP (PMIP).

Mobile networks tend to have more traffic processing and conditioning functions than fixed networks, this is because of the constrained nature of the RAN (the capabilities of which vary with location). This leads to requirements for video and image transcoding that do not exist in the fixed network. These services are configured within the mobile carrier network in a location described as the SGi-LAN.

This architecture is shown in Figure 14.

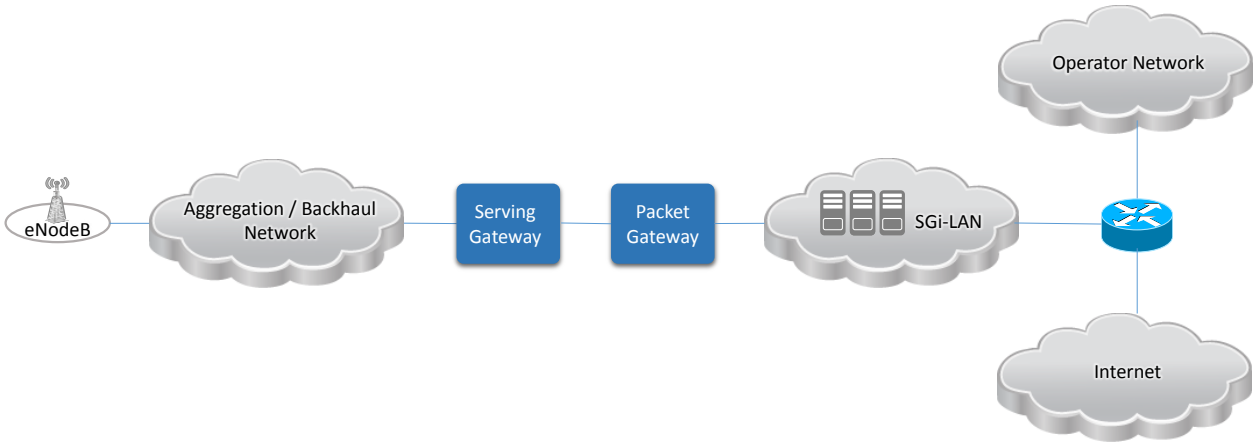

Figure 14 Mobile Aggregation, Backhaul and the SGi-LAN

SDN and NFV provide the network operator with a number of opportunities within the aggregation and backhaul networks:

- SDN can be used to control the establishment of connectivity on demand between eNodeBs to support Automatic Neighbour Relations. The advantage of this is that the controller provides a secure control point for authorising the connections but does not require to be in the traffic path.
- SDN can be used to optimise the traffic flows within the access and backhaul network by decoupling the packet transport domain from the EPC control and data plane. This could potentially allow for a more distributed EPC and more efficient use of capacity in the backhaul network.
- SDN has also been proposed to optimise the microwave transport network, to improve link selection and to improve power efficiency.

These use cases are shown in Figure 15.

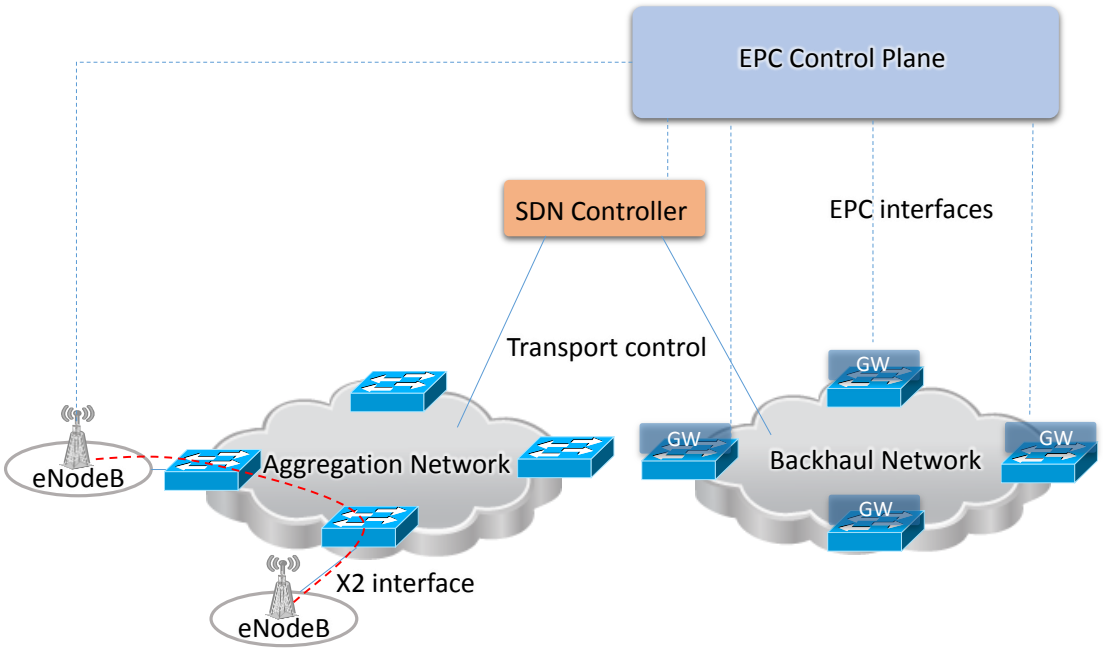

Figure 15 SDN Applications in the Aggregation and Backhaul Networks

The ONF is currently refining these use cases, however, if changes are required within the EPC then this will require a 3GPP initiative.

In addition to the aggregation and backhaul network, SDN and NFV are proposed within the SGi-LAN, this application is discussed in Section 6.6.2.

6.6. Architectural impacts of Network Functions Virtualisation

Network Functions Virtualisation is covered in detail in Section 8. This section describes the key applications being studied by network operators and how they relate to the network architecture.

6.6.1. Service Node

The service node is a point within the service provider network where value-added network services are provided for network flows. Example services are:

- Virtual CPE (see Section 6.6.4)
- Carrier Grade NAT
- Firewalling and Intrusion Detection
- DDoS protection
- Deep packet inspection
- Captive Portal
- Web Filtering / Parental Controls
- Voice / Video quality monitoring

The architecture of a Service Node requires a traffic classification function to identify service flows. Within a broadband network this is the BNG while the 3GPP TDF performs this function for mobile networks. One might envisage a converged deployment, with both 1st level BNG and Mobile P-GW complemented by a shared TDF, although this convergence is often not accomplished in today's networks. Once traffic has been classified into service flows, policy routing can be applied to forward each flow so that it traverses all the service functions in the order required for the service before it leaves the node to be routed further across the service provider core or access networks.

This policy routing forms a service chain construct as shown in Figure 16.

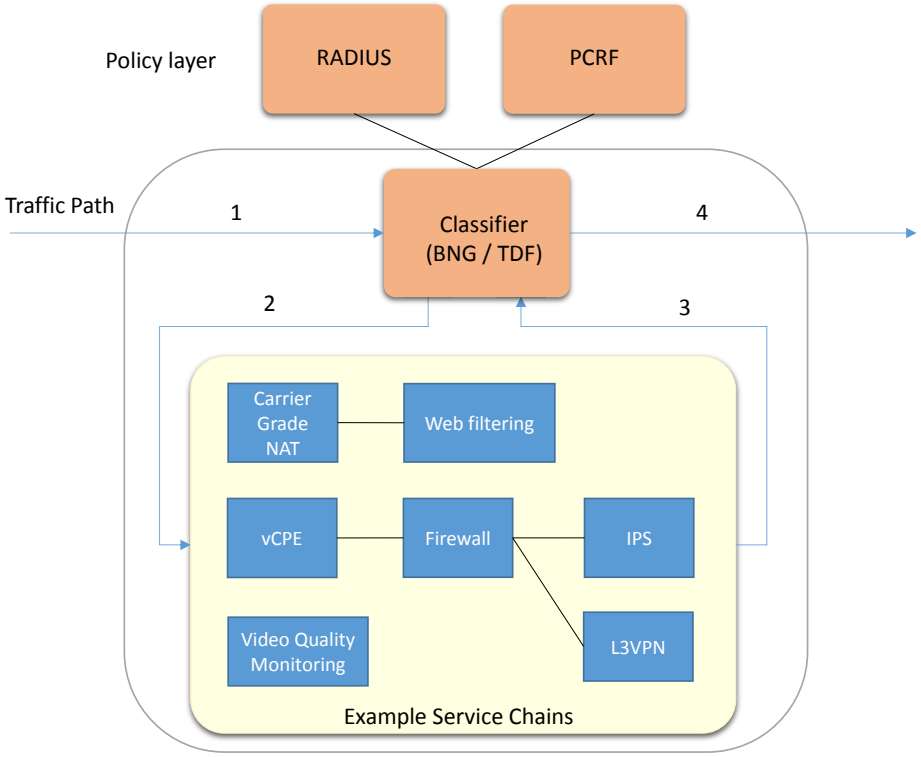

Figure 16 Service Node Architecture

In today's networks, service chains are typically implemented at a single service node. The service paths between service functions are built statically by network management using VLANs, MPLS, GRE or L2TP tunnels. Because the paths are static they are often shared by all users of a product. In addition, there is limited capability to customise the service path for different flows unless the service functions are implemented within the router performing the classification. The degree of service function centralisation can vary by service. Per-subscriber policies are typically enforced near to the boundary between the access and core networks, while shared functions such as web filtering may be performed more centrally.

Service Chaining is being considered by the ETSI NFV ISG [Ref 24] under the related term 'Virtualised Network Function Forwarding Graphs'. Network operators are considering re-engineering these service nodes using NFV to improve agility and replace dedicated hardware with NFV and COTS server infrastructure. In the case of the NFV, service functions can be dynamically created so that the infrastructure scales with the service demand. One of the opportunities for NFV is to remove the penalty for distributing service functions deeper into the carrier network by removing the need for dedicated platforms.

The NFV Infrastructure (or local service provider cloud) built at these service nodes contains compute, storage and networking infrastructure to instantiate and link together the service functions. The combination of dynamic service function creation and dynamic service chains

creates an orchestration problem that may be solved by applying the SDN techniques currently deployed in enterprise data centre environments. An SDN controller could orchestrate the networking element of the service provider cloud in conjunction with the service provider policy framework and the management functions that configure the virtual network functions themselves. This allows the mapping of end-users and flows to the service chains between these functions to become more dynamic.

Flexible Service Chaining is under study by Broadband Forum as part of the SD-326 project [Ref 25]. This is gathering use cases for service chaining within Broadband Networks – focusing on service chains at the BNG. Following a Birds of a Feather (BOF) session at IETF 87 (July 2013), the IETF has a proposal to charter a Network Service Chaining (NSC) working group to look at a standardised data and control-plane protocol stack for service chaining.

6.6.2. NFV in Mobile Networks

In mobile core networks two applications have been proposed for NFV and SDN. These are:

- Evolved Packet Core Virtualisation
- Service Chaining and steering in the SGi-LAN

The Evolved Packet Core is fundamentally a software function that currently resides on specialised hardware. However, it is a good candidate for NFV and mobile operators are looking to deploy virtual EPCs to improve network scaling. The use of NFV will allow a mobile operator to avoid paying for capacity they do not need and provides them with a relatively easy way of scaling out as the network expands. The virtual EPC is one of the use cases specifically identified by ETSI NFV, as described in Section 8.

In mobile architectures the SGi-LAN is where the network operator provides content optimisation solutions (such as transcoding), as well as other support functions, (for example, adult content filtering, DNS and firewalls). Depending on the service offered the mobile operator may wish to classify individual microflows using a TDF and forward them to a given service (or service chain). SDN solutions such as OpenFlow can be used within the SGi-LAN to steer the flows to the appropriate servers. The operator can use NFV to support these functions, allowing them to scale out as necessary and allowing them to re-use their server assets if customer preferences change. This allows the introduction of innovative new services without the expense of new hardware and will allow the rapid scaling of successful new services. This looks very much like the fixed network operators' service node described in Section 6.6.1.

6.6.3. Virtualised IP Edge

There is interest from service providers to explore the potential capabilities of white-box switch platforms and software routers in carrier networks as a replacement for proprietary IP Edge platforms (as currently sold by major router vendors). IP edge routers perform a number of functions including service mapping to the network, authentication, authorisation, accounting and policy enforcement. These functions are central to service definition. Virtualising these functions opens the possibility of the network operator gaining more control over the development of these services and accelerating service deployment. The challenge of virtualising these edge nodes is the high scalability required in terms of flows and hierarchical QoS. These problems also bound the scalability of the current hardware-based implementations, even though these are optimised for packet processing.

A white-box switch implements the switch data-plane while a network operating system (i.e. a routing control plane and its supporting functions) is supplied by a third party. The network operating system is then integrated with the switch using a protocol such as OpenFlow. There is a trade-off between the capital cost of these platforms and the operational cost of integrating and maintain a distributed control-plane solution so the extent to which the migration to white box switches will occur in practice is uncertain.

Software routers run all the functions of the network element within a virtual machine, obviating the need for integration of a control plane with a white-box switch. Software router vendors are now claiming performance of up to 10Gbps per CPU core. However, these performance figures currently require a virtualisation infrastructure that is specifically engineered for high-performance network applications; and each application must be carefully validated against the infrastructure to understand and maximise performance. Therefore, an integration penalty may still exist where a network operator needs to deploy dedicated virtualisation infrastructure for network functions.

Given that white-box switches and software routers are still at an early stage of development it remains to be seen whether service providers will continue to deploy conventional, integrated edge router platforms or if white box switches / software router implementations can gain a foothold in this market.

6.6.4. Virtualised Customer Premises Equipment

The customer premise network is not considered in this report. However, there are SDN / NFV use cases of interest surrounding the CPE that terminates the service provider network. The common principle is to reduce the functionality required to be supported on the CPE hardware – possibly reducing this to layer-2 forwarding functionality only – and to implement this functionality instead at a service node within the service provider network. The aim is to facilitate the

deployment, maintenance and evolution of value-added CPE functions without adding complexity to the CPE.

6.6.4.1. Network Enhanced Residential Gateway

The Network Enhanced Residential Gateway is a service provider response to challenges presented by a fixed-function CPE in an environment where broadband subscriber value is being captured by over-the-top service providers. The current distributed functionality provided by residential gateways is presenting a barrier to service innovation.

The Broadband Forum is specifying the architecture and requirements for the network enhanced residential gateway in the WT-317 project [Ref 26]. The WT-317 project envisions a residential gateway in the home that bridges some or all traffic to IP services functions centralised on a virtual Residential Gateway (vRG) function hosted in the service provider network. The services functions could include basic routing functions, for example, IPv4, IPv6, NAT and also higher layer functions like Digital Living Network Alliance (DLNA), file sharing and M2M gateways. There are a number of possible locations proposed for the vRG function, including the Access Node, Broadband Network Gateway and the Data Centre / Cloud. Hybrid implementations are also possible where protocol implementations are separated from the forwarding plane. This model is similar to the generalised service node architecture described in Section 6.6.1.

The Home Gateway Initiative has identified requirements for an alternative approach for deploying enhanced functionality on residential gateways. HGI-RD008-R3 – “HG Requirements for Software Execution Environment” [Ref 27] identifies requirements for a modular software framework that creates an execution environment on the residential gateway. Service applications can be deployed to the residential gateway that augment the core HGI functionality similar to the way that they might be deployed as part of a vRG in the Broadband Forum’s Network Enhanced Residential Gateway Model. This extends the possible set of locations for service deployment.

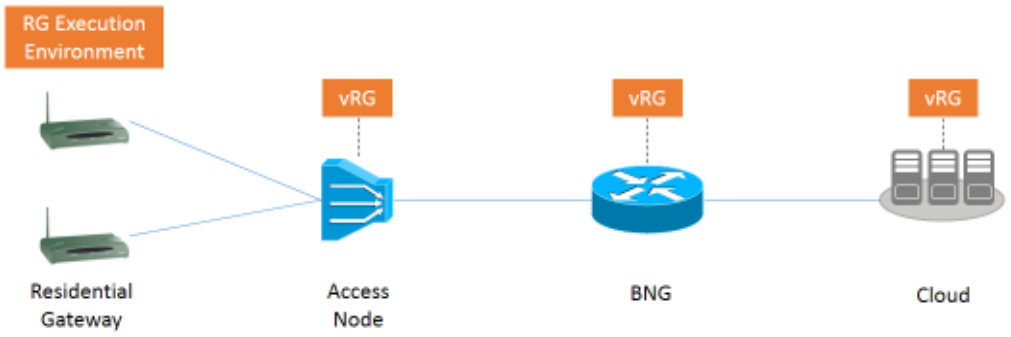

Figure 17 Residential Gateway Virtualisation Options

Figure 17 shows how, if the Home Gateway Initiative and Broadband Forum approaches to Residential Gateway function virtualisation are combined, then all locations in the network are potentially covered. Different distributions of functionality might be required for different applications. For example, integration of an M2M gateway application could be performed with the M2M gateway in a Residential Gateway Execution Environment, or this could be centralised within the network provided that an interworking function is deployed in the RG to extend the M2M HAN across the WAN.

A potential business objective of deploying a Network Enhanced Residential Gateway in a residential ALA wholesale environment [Ref 11] is that an ALA provider might be able to deploy a suitably enhanced RG instead of the existing Network Termination Unit (NTU). This enhanced RG would support the ALA provider network functions, but could also be used by any ALA user instead of them supplying their own CPE. This would simplify the migration process between ISPs as new residential gateway devices would not need to be dispatched and installed as part of the migration.

Virtualising the Home Gateway is a clear SDN/NFV application that has the potential to enable the provision of additional services to end customers but it may also disrupt the existing models of broadband networking and risks allowing the access network operator the power to dictate and constrain the offerings of the Service Providers.

6.6.4.2. Virtual Enterprise CPE

The Virtual Enterprise CPE application redistributes features of the enterprise customer premises router to the cloud. The features supported on enterprise CPE differ from those used for the residential market. Typically these devices support integrated firewalls, unified threat management functionality, VPN functionality and enterprise routing. However, the principle of virtualising the functions that are not directly required to forward traffic is common to the residential case. The virtual CPE use case has been promoted by Juniper Networks [Ref 28] who provide Cloud CPE functionality through service cards in their provider edge routers or a co-located x86 server farm. In the case of implementation within the provider edge router virtual CPE is an example of NFV while offloading the vCPE function to an x86 farm leverages SDN techniques to perform the service chaining for the traffic. An important component of the solution is a management application to hide the implementation complexity of the virtual CPE solution and allow the user to manage it as if the customer router is physically implemented at the customer premises.

Virtual CPE applications may be of particular interest to network service providers delivering IP network services over an access network provided by a third party service provider as shown in Figure 18. If the access network provider offers an access product that can provide IP layer QoS awareness on the Ethernet NID, and can provide network management APIs for service

provisioning and fault / performance management; it becomes possible for the IP service provider to offer services without deploying equipment to the customer premises. This is desirable because the lower box count reduces operational cost and improves service flexibility and availability. The virtual CPE model can still be used with a lower functionality access products, but in this case there may be multiple Ethernet NIDs in the customer premises.

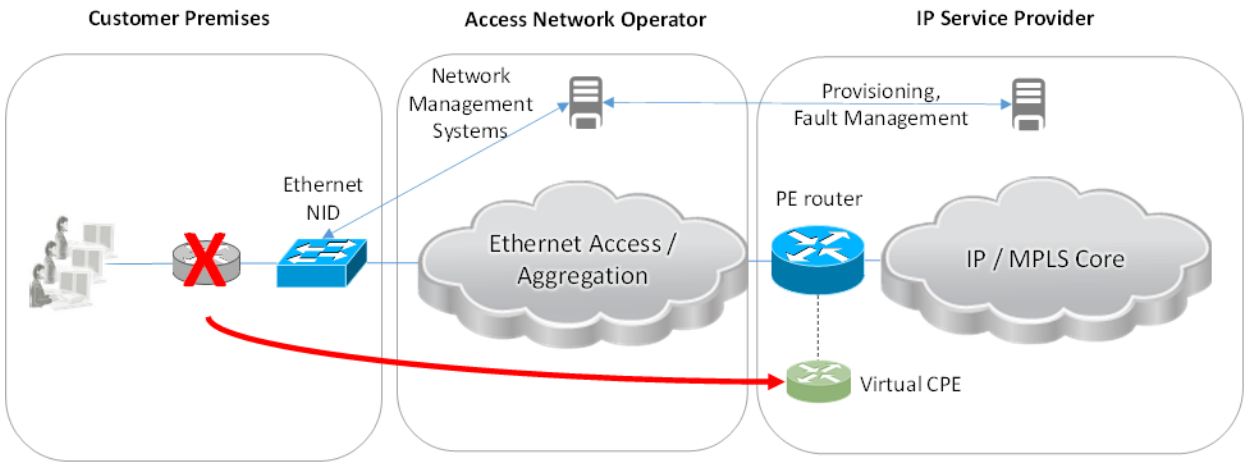

Figure 18 Virtual CPE with Wholesale Carrier Ethernet Access

The virtual CPE model is equally applicable for Ethernet-only services. The Metro Ethernet Forum has standardised an E-Access Service [Ref 29] together with a Virtual User Network Interface (UNI) construct. This allows a Service Provider to centralise Ethernet UNI functionality when delivering Ethernet services to an out-of-franchise customer site, this is similar to the IP services scenario shown in Figure 18.

7. SDN Technologies

This section provides an overview of the key SDN technologies and looks at the work of the relevant standards organisations working on SDN.

7.1. SDN Controllers

The SDN controller forms a key part of any SDN (or SDN/NFV) solution as it is responsible for configuring and maintaining the network so as to support a given service or set of services. The SDN controller sits below the orchestrator within any solution and is driven by instructions from the orchestrator. Because the SDN controller is pushing configuration onto physical and virtual network elements, it may interact with the functions of an OSS. In this case conflicts must be managed either on the basis of rules and policy, or by detecting the conflict and flagging it to a human operator to resolve.

There are a large number of SDN controllers on the market and they vary in the use cases that they are specifically targeted at (although solutions are generally extensible enough to cover a wider set of use cases if required by the operator). There are a selection of Open Source SDN controllers, of which OpenDaylight is probably the most relevant to carriers, but other notable controllers being OpenFloodlight and OpenContrail. There are also vendor developed and supported SDN controllers, which may also leverage the capabilities of the Open Source controllers. For example, Cisco have their extensible network controller XNC, which leverages the capabilities of OpenDaylight, and Juniper offer Contrail which is a Juniper supported version of OpenContrail.

SDN controllers typically provide control within a network domain, this may be as small as an individual data centre or may cover an entire network. The key function of an SDN controller is to integrate with the orchestration layer, providing it with a sufficient abstraction of the network to permit it to build the services it requires without needing a detailed understanding of the underlying network. The SDN controller itself requires a complete knowledge of the network it is controlling, however, some architectures allow the SDN controller to delegate control of portions of the network to peer, or subordinate network controllers. For example, the optical layer of a network may require its own controller and the IETF Path Computation Element (PCE) architecture supports the concepts of subordinate and peer PCEs, see Section 7.5.

The concept of topology abstraction is an important one in SDN, although standardisation is currently nascent in this area. One view suggests that services should be modelled at the orchestration layer and the SDN controller must take the service request, defined in an abstract or service model and convert it into the network model it holds (to understand which elements need configuring). The controller must then further decompose the model of the service build into a set of detailed actions (or configurations) within the individual network element models.

This view of an SDN controller is very much the approach taken by the TeraStream concept, see Section 10.

SDN controllers that support network functions virtualisation and data centre capabilities also look to integrate with cloud orchestration systems like OpenStack, supported via the OpenStack Neutron plug-in. This ensures that when OpenStack provides the compute and storage capabilities for a given application that it can inform the SDN controller of the network connectivity requirements.

Some SDN controllers, such as OpenDaylight set out to support a large number of southbound interfaces to network elements, however, the degree of autonomy of those network elements may vary. Control of entities, via a PCEP interface, typically install a forwarding behaviour in the entity which will still run autonomously, possibly running network routing protocols. Control of network elements running OpenFlow by default provides a much lower level interface requiring the controller to perform learning functions and ARP functions for the network element and then installing forwarding entries into the element. This low level approach is more flexible and provides more control but has scaling and DDoS implications, as well as timing issues. Even within the OpenFlow model of SDN certain low level network element functions must remain within the autonomous control of the network element. These include: sub 50ms optical protection switching, large scale Bidirectional Forwarding Detection (BFD) applications, and Ethernet OAM CC functions. These types of applications have such tight latency and processing requirements that it is impossible to delegate them to a remote controller.

Different SDN controllers typically implement SDN in different ways because each controller tends to be based on its own implementation view of SDN. Some SDN controllers, for example, OpenContrail are based around an overlay model of SDN. This builds an overlay of tunnels over a routed or switched infrastructure that is not SDN aware. SDN configuration in these models is provided at WAN gateways, and in virtual switches or routers on the servers. The alternative approach is to remove the overlay network and directly control the underlay network, which requires SDN interfaces to the network switches. Within a data centre the overlay network approach has widespread support and would equally fit within a telco cloud environment. For a WAN deployment, however, an underlay approach is more appropriate because of tunnel scaling constraints.

7.2. Example SDN controllers

In order to understand how the SDN controller dictates the solution it is instructive to consider some specific examples. The following sections provide an overview of two very different controllers, OpenDaylight (Service Provider edition) and OpenContrail.

7.2.1. OpenDaylight

The OpenDaylight controller is a Linux Open Source project that is backed by a number of major vendors built around a controller core that was contributed by Cisco. The first release of OpenDaylight, “Hydrogen”, was released in early 2014 and has three versions:

- Base Edition, which provides a core controller capability.
- Virtualisation Edition, which supports the functions required to support a data centre deployment, (for example, integration with OpenStack, Virtual Tenant Networks and DOVE VXLAN capability).
- Service Provider Edition which provides a solution focussed on SDN in the WAN, removing the data centre virtualisation capabilities but adding multiple southbound interfaces and a LISP service.

The components of the Service Provider edition of OpenDaylight [Ref 30] are shown in Figure 19.

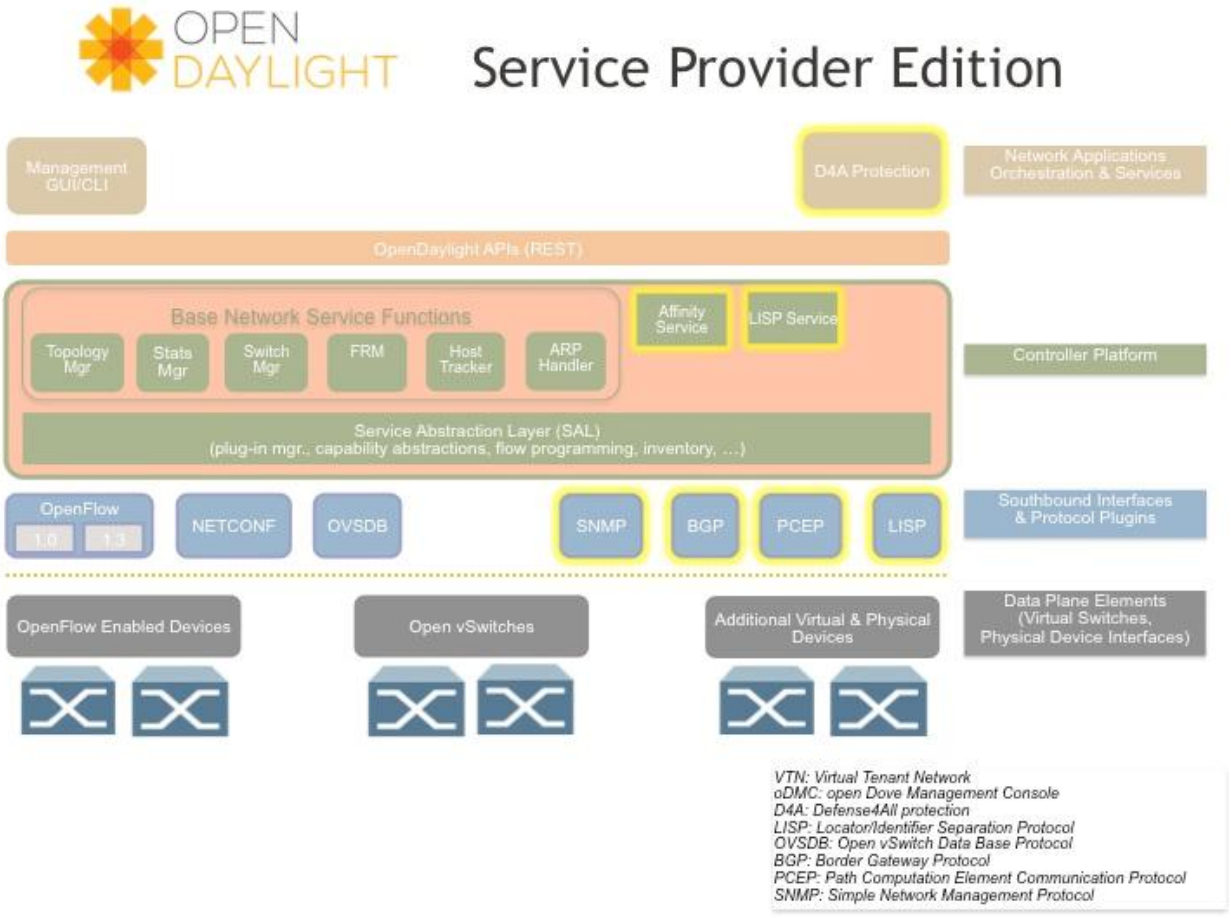

Figure 19 The OpenDaylight Hydrogen Release Service Provider Edition

OpenDaylight has adopted a model driven approach using YANG, where applications are defined as a data model and the APIs required to access them can be auto-generated as part of the integration process. The Model-Driven Service Abstraction Layer (MD-SAL) provides notifications, RPC routing and a data store acting as the glue between the southbound interfaces, the controller applications and the northbound interfaces.

OpenDaylight provides REST APIs to the applications and supports key capabilities such as topology and inventory management (including topology discovery and learning), host tracking and topology export (to applications). As part of the Service Provider release OpenDaylight supports a northbound LISP application interface and also bundles a DDoS protection application, Defence4All.

Hydrogen is the first release for OpenDaylight and it is early in its development cycle. OpenDaylight capability is likely to be imported into commercial controllers (either vendor offerings or Service Provider customisations) and will, therefore, reduce the development times for SDN controller implementations. It should be noted that the Cisco Extensible Network Controller (XNC) controller has already done this, having imported the OpenDaylight Base Edition and added specific applications around it.

Given its alignment with YANG models and with its support for IETF protocols (such as BGP and PCEP) as well as OpenFlow capabilities the Service Provider edition of OpenDaylight looks like a good fit for WAN based Carrier SDN applications.

7.2.2. OpenContrail

The Open Contrail controller architecture [Ref 31] provides the overview of the OpenContrail system, as shown in Figure 20.

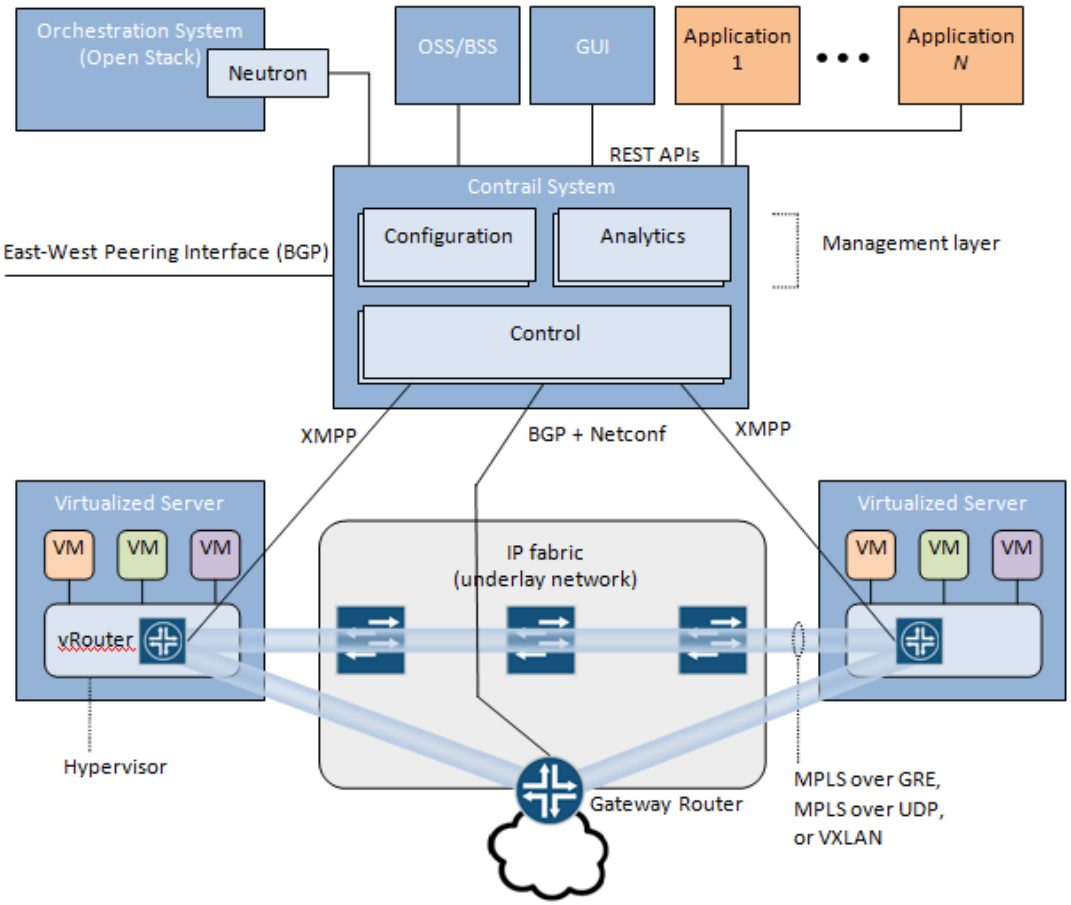

Figure 20 The OpenContrail System

OpenContrail assumes an IP underlay network and uses vRouters in the compute nodes within the data centre to provide the network slicing, connectivity and traffic steering required. These vRouters are themselves split into a forwarding plane and a control plane within the compute node. OpenContrail uses MPLS over IP (GRE or UDP transport) for the overlay network for a layer 3 solution or VXLAN for a layer 2 solution.

OpenContrail has a defined data model around which services are defined in a high level model, this high level model is manipulated by the applications using REST APIs. The Contrail system then maps this model to the network, creating a low level model which is then pushed to the required virtual routers as configuration. The model is defined using an IF-MAP XML schema, however, OpenContrail indicate possible future support for YANG.

The OpenContrail system has three components (plus the vRouters). The configuration component is responsible for processing the data model from the high level service view to the low level data model. The Control nodes provide the control plane and monitor the low level data model to determine the required state of the network; which they configure using the OpenContrail southbound protocols. The analytics nodes collect and collate data about the systems performance.

OpenContrail offers integration with OpenStack and can support service chaining via a policy and route leaking mechanism. It provides resilience to failure by distributing its elements and running an active-active configuration. The system can scale out by creating additional instances of nodes as and when load requires.

OpenContrail is primarily targeted at data centres, i.e. Cloud Networking; and also at Network Functions Virtualisation where it is architected to provide network connectivity for a Service Node type deployment. In this latter deployment the gateway router might be an IP Edge node and OpenContrail provides the SDN connectivity to all of the virtual network functions sitting behind the edge router, (for example, Virtual CPE, Radius, DNS, firewalls).

7.3. OpenFlow

The OpenFlow standard is maintained and developed by the Open Networking Foundation (ONF). The ONF is a user-driven organisation dedicated to the promotion and adoption of Software-Defined Networking (SDN) through open standards development. The OpenFlow standard is central to the ONF's definition of SDN as described by the ONF White Paper [Ref 32]. The ONF is structured into working groups (WGs) and discussion groups (DGs) that are responsible for contributing to extensions to the OpenFlow Technical Specification and other Technical Recommendations that may be published by the ONF. The remainder of this section describes the status of the SDN standards produced by the ONF.

7.3.1. ONF Architecture

The work in progress in the ONF Architecture group is more generalised than described in the ONF White Paper. It leaves open the possibility that protocols other than OpenFlow may have a role at the SDN controller southbound interface. This is a broadening in scope for the ONF from its previous strict focus on the OpenFlow protocol to a wider remit as the lead organisation for SDN standardisation initiatives.

The ONF SDN architecture [Ref 33] does not specify the internal design or implementation of an SDN controller. It is characterised by the use of a control-plane that is logically centralised and de-coupled from the data-plane. Logical centralisation envisages that the functions of the SDN

controller may be distributed within the network. The de-coupling means that there is an open interface between the control and data-plane.

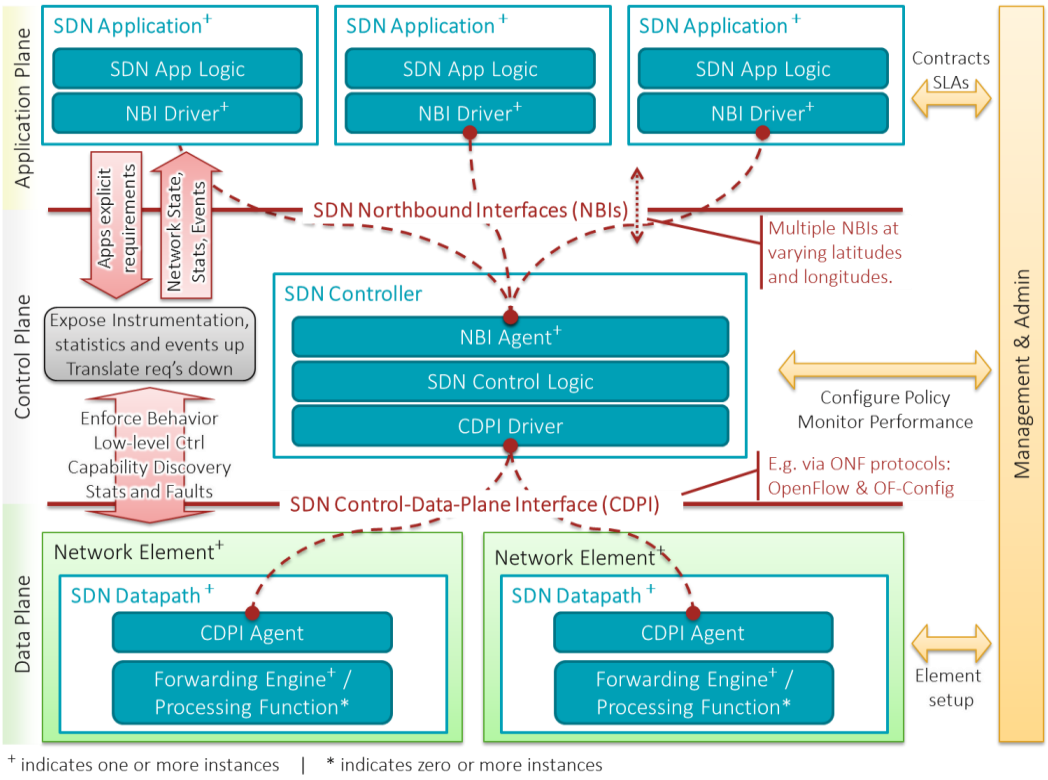

Figure 21 ONF SDN Architecture (source ONF)

Figure 21 shows the high-level ONF SDN architecture. This is reproduced from the ONF SDN Architecture Overview document [Ref 33]. At the interface highlighted "Control Data Plane Interface (CDPI)", the figure shows the use of the OF-Switch (OpenFlow) and OF-Config protocols between the SDN Controller and the Network Elements. The OF-Switch protocol is responsible for configuration of forwarding entries on the network element and the transfer of network packets between the SDN controller and the Network Element. The OF-Config protocol is the management interface responsible for the configuration of the OpenFlow client itself.

Above the SDN controller sits a range of SDN applications that utilise Northbound Interfaces (NBIs) provided by the SDN controller and which may in-turn expose APIs to other applications. The ONF has initiated a working group to study these Northbound Interfaces but has yet to publish (or propose) any standards. In addition to this, the ONF recognises the continuing need for a network management layer to manage the non-OpenFlow specific attributes of each layer.

The internal function of an SDN controller is not tightly defined. However, the externally visible behaviour will include:

- Visibility of the Information Model
- Topology knowledge and Path Computation
- Resource model abstraction

The terms Network Slicing or Network Virtualisation refer to mechanisms for division of physical network resources between applications. One way of doing this is by the use of a proxy between an OpenFlow controller and a switch (at the CDPI interface). An example of this is the FlowVisor tool. The proxy creates a separate flow space for each controller so that the flows they control are isolated from each other. An alternative is a resource co-ordinator function embedded on the network element that controls which resources are delegated to which controller to create a Virtual NE. Resources in this context could be ports, VLANs and bandwidth. OF-Config provides one way of configuring these Virtual NEs. The FlowVisor approach provides a solution for flat Ethernet / IP networks while virtual NEs are easier to map to multi-layer topologies and hierarchical controllers. Virtual NEs may, therefore, see greater use in Carrier Networks.

The adoption of SDN in carrier networks creates a number of architectural challenges that are not apparent in flat data centre networks. The ONF architecture working group is studying these and providing a framework for future work in the ONF and external standards bodies. At a high-level these study items are:

- Hierarchical SDN controllers mirroring the organisation boundaries within network operators or the layered nature of the physical network.
- Distribution of controller functions within the service provider cloud (from co-located with NEs to centrally in data centres).
- Support for multiple administrative domains.
- Interoperation with existing (non-SDN) networks.
- Mixed connection-oriented and packet switched networks.
- Delegation of control to embedded sources / sinks for network control / OAM traffic.
- Support for protection and fast restoration in the network.

The presence of the list of study items does not mean that OpenFlow cannot be deployed today in constrained network domains. However, it is an indication of the level of maturity of the standards and the length of the standardisation journey ahead if it is to become the dominant technology within carrier networks.

7.3.2. OpenFlow Switch Specification

The OpenFlow Switch Specification (OF-Switch) [Ref 34] describes the components and basic functions of an OpenFlow switch in addition to the OpenFlow protocol to manage an OpenFlow switch from a remote controller.

The main constructs in OpenFlow are the flow tables which contain flow entries. Each flow entry contains classification rules to match network traffic and references counters and instructions to apply to matching packets. The instructions define how a packet should be modified and forwarded. The OpenFlow protocol provides a way of transporting packets between the SDN controller and the Network Element. This enables control protocol packets to be processed by the SDN Controller and injected into the network.

There have been a number of versions of the OpenFlow protocol that have added base protocol functionality and packet classification fields. The ONF is currently maintaining the OpenFlow v1.0 and OpenFlow v1.3 specification in addition to the latest release: OpenFlow v1.4.

The OpenFlow Switch protocol itself is extensible allowing proprietary extensions to fill some of the gaps in the OpenFlow specification. In addition, the ONF publishes a set of standard extensions to previous versions of the protocol that have been prototyped and approved by the ONF.

7.3.2.1. OpenFlow Implementation

Implementation targets for OpenFlow include software defined switches implemented on x86 servers and hardware switches implemented using network processing units (NPUs) and fixed-function ASICs. Later versions of the protocol have added advanced capabilities such as flow-table pipelines, VLAN stacking, Provider Backbone Bridging, MPLS and per-flow metering.

The introduction of pipelines in OpenFlow v1.1 has proved to be a double-edged sword. On the one hand it was required to solve the table scaling issues that result from trying to implement packet classification in a single flat lookup. However, hardware implementations are typically constrained in the way that their packet classification and processing pipelines can be built. This means that the OpenFlow controller now requires knowledge of the forwarding architecture of the OpenFlow switch. These constraints are more significant with ASIC based implementations where the forwarding pipeline is fixed, but are still present to some extent with a switch based on an NPU (especially if optimising throughput is a concern). Software implementations of OpenFlow switches are in comparison more flexible. However, the network acceleration features that are present in network interface cards still provide a constraint.

7.3.2.2. Negotiable Datapath Models

Recognising the need to model hardware constraints with OpenFlow implementations, the ONF has a Forwarding Abstraction Working Group (FAWG) that is defining an architectural model for OpenFlow switches. The idea is that this will simplify the mapping of multiple flow tables onto hardware implementations, which in turn will simplify SDN controller implementation.

The architectural model is described in the form of Negotiable Datapath Models (NDMs). The first example of an NDM are Table Type Patterns (TTPs). A TTP describes a set of flow tables and the valid operations to be supported by an OpenFlow logical switch. Although the syntax and definition of TTPs is still a work-in-progress at the ONF there is a mechanism in OF-Config v1.2 that allows some negotiation of the supported TTP at switch initialisation. The promise of NDMs is that they will provide a path to standardisation of OpenFlow switch hardware and improve interoperability between switches and controllers.

7.3.2.3. Hybrid Operation

Some network use cases envisage a hybrid of SDN controlled functionality on switches integrated together with existing feature sets. An example of this might be to mix OpenFlow control of the Ethernet bridging domain, to be forwarded over MPLS tunnels configured with an integrated MPLS control-plane; to produce an alternative to Virtual Private LAN Service/Ethernet Virtual Private Network (VPLS/E-VPN) solutions.

The OF-Switch specification specifies the use of logical ports to represent constructs such as tunnels and lower layer interfaces. The naming conventions for these interfaces are, however, not well defined. This will possibly be addressed by work in the Transport WG.

The ONF spawned a Hybrid working-group to investigate the definition of hybrid switches and hybrid networks [Ref 35]. However, this work concluded without publishing any specifications so implementation of integrated hybrid switches is currently described by the OF-Switch protocol draft but otherwise proprietary. In a layered transport network, it is not clear how an implementation can avoid being some kind of hybrid.

7.3.3. OpenFlow Config

The OF-Config protocol configures and manages the OpenFlow function on an OpenFlow capable switch. The OF-Config protocol initiates the control channel between the switch and the OpenFlow controller and also performs configuration actions that are not implemented as entries in flow tables. These configuration actions include mapping physical ports and queues to an OpenFlow Logical Switch and building flow tables.

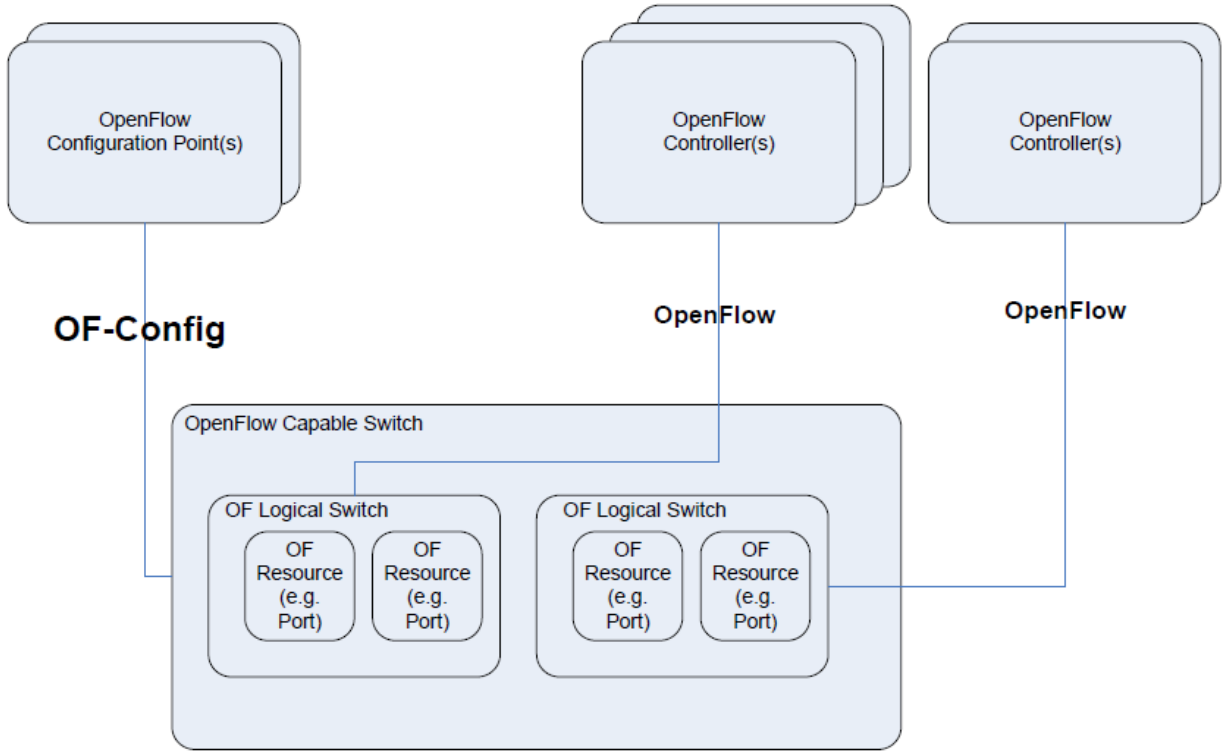

Figure 22 Relationship between OpenFlow and OF-Config (source ONF)

The OF-Config protocol is implemented using NETCONF. Figure 22, which is reproduced from the ONF OpenFlow Management and Configuration Protocol document [Ref 36], shows the relationship between OpenFlow and OF-Config. The OpenFlow configuration point that manages the OpenFlow capable switch may be implemented as part of the OpenFlow controller or may be part of a separate management system, for example, an EMS in a Telco environment.

The OF-Config protocol allows the negotiation of the switch capability using Network Device Models. This allows the OpenFlow Configuration Point to discover the profile of OpenFlow supported by the logical switch and control elements such as flow table sizes.

OF-Config has limited support for tunnel configuration – currently including IP-in-GRE, NVGRE and VXLAN. These implementations assume a hybrid switch with an underlying IP data plane outside the scope of the OpenFlow Logical Switch. Future work may extend this to carrier

tunnelling encapsulations. Allied to this will be the support for configuration of BFD and OAM functions implemented using helper functions on the network element.

It should be noted that there is limited support for OF-Config in industry, with many solutions preferring to implement Open vSwitch DataBase management protocol (OVSDB).

7.3.4. Current ONF Work

7.3.4.1. Optical Transport

The Optical Transport working group is investigating how to control optical transport networks using OpenFlow. A number of use cases have been proposed, including ROADM configuration in photonic enterprise networks, network virtualisation for multi-layer networks and packet-optical integration. OpenFlow v1.4 includes the concept of using optical port attributes to control the physical layer parameters, for example, power and wavelength. However, there are open issues around the mechanisms used to model the multiplexing hierarchy on an OTN switch and configure optical layer connections. In addition there are challenges with how optical layer topology is discovered and reported to the controller.

For these reasons while there have been proprietary demonstrations and trials of use-cases such as packet-optical integration and optimisation, further extensions to the ONF protocols are required for any standardised implementation. This may take a further 6-12 months of work in the ONF and potentially further activity in other organisations such as the TM Forum.

7.3.4.2. Wireless and Mobile

The Wireless and Mobile working group is collecting use cases for OpenFlow in relation to IEEE wireless and 3GPP mobile standards. The work is currently at an early stage, but the group is currently splitting the use-cases into three strands:

- Wireless Transport – SDN control of microwave and mobile backhaul systems.
- Mobile Packet Core – SDN enhanced mobility management, EPC infrastructure and service chaining
- Enterprise Wireless – Focussing on unified access control using 802.1X

If these use cases are progressed, extensions will be required to the OpenFlow protocol to capture the requirements for physical layer and mobile packet tunnelling protocols, (for example, GTP).

The use cases related to the EPC have so far looked at the concept of optimising the traffic flows in the backhaul and aggregation networks to efficiently meet the requirements set by the EPC. If the industry determines that SDN capabilities should be embedded within the EPC itself then this aspect of SDN is likely to be defined by the 3GPP standards organisation which defines the EPC.

7.3.4.3. Northbound Interface

ONF work on Northbound Interfaces from an SDN controller is embryonic. The architecture work is defining some scenarios where there is an interface between hierarchical SDN controllers. Other than this, the black box perspective on an SDN controller limits the extent to which data models for controller components and interfaces between these components can be defined.

The OpenStack project provides a concrete example of a Northbound API through the Neutron project. There is also an initiative within the ONF to liaise with open source controller framework projects, for example Open Daylight, to co-ordinate progress in this space.

7.3.5. OpenFlow Conclusions

OpenFlow was originally conceived in the context of flat Ethernet / IP networks and is evolving to add features that make it applicable for carrier networks. Use cases coming from the optical transport market are driving work on SDN architecture that will extend the scope of the OpenFlow protocol to meet Carrier SDN requirements.

Carrier SDN is likely to encompass hybrid network elements that include OpenFlow logical switches alongside functions with an embedded control plane. It is yet to be seen whether OpenFlow will continue to develop as a set of incremental backwards compatible extensions or whether an OpenFlow 2.0 proposal will emerge to provide a richer set of constructs for modelling the hybrid data path and control plane of carrier class network elements.

The ONF is the logical organisation to develop a framework for SDN technologies in addition to OpenFlow. However, work in this area is nascent and will require considerable effort from industry to align the various initiatives that lay claim to the SDN banner and get to a consensus on the functionality exposed by an SDN controller. Some of the standardisation gaps may be filled by the open source SDN controller initiatives.

SDN proponents preach a vision of an open interface between the SDN controller and ‘white box’ network switches. The OpenFlow protocol provides a concrete example of control plane – data plane separation that provides an important target specification for both equipment vendors looking to develop these white box switches and suppliers of the associated network silicon. Achieving an open market for these products is critical for some of the plans proposed by network operators for a virtualised replacement for existing network infrastructure. This in turn

depends on the success of the ONF Network Datapath Model initiative to leverage the power of the multi-stage OpenFlow pipeline that is required for all but the most trivial OpenFlow implementations.

In the meantime, it is likely that SDN controllers will implement proprietary interfaces and be tightly coupled to the implementation of carrier class network switches in order to fully leverage the accelerated forwarding paths made available by the hardware. The availability of white-box switches implementing a carrier class feature set and interoperating with multiple controllers and applications will provide a metric of the maturity of the ONFs vision for SDN. There is still some way to go before this becomes a reality outside the data centre.

7.4. Interface to the Routing System (I2RS)

7.4.1. Overview

Interface to the Routing System (I2RS) is an IETF project tasked with allowing applications access to the routing and topology information in the network, and to provide these applications with a way of modifying the routing within the network. The working group [Ref 37] is tightly chartered.

The key objectives are briefly summarised below:

- The ability to read from and write to the Routing Information Base (RIB).
- Monitoring and Control of the Border Gateway Protocol (BGP) including policy enforcement.
- The ability to control the routing in the network for given flows (allowing application layer routing decisions to be made), whilst leaving standard routing rules in place for other flows.
- The ability to extract information about topology from the network.

The I2RS approach to network control differs from OpenFlow in that it operates at a much higher level, seeking to optimise and adjust the behaviour of the control plane that is running in the network rather than seeking to replace it. Given the very large amount of investment in IP routing protocols such as BGP, IS-IS and OSPF as well as the widespread use of MPLS, it may be that this approach to application based network control will be more suited to carrier core network applications than OpenFlow.

The I2RS work is at an early stage within the IETF, the capabilities and architecture are being defined and consideration is just being given to the selection of an I2RS control protocol. While

the standardisation of I2RS is still in its early stages, it is possible to see it within the wider context of the SDKs and open interfaces that router vendors are promoting on their routing platforms. It may be that I2RS acts as a vehicle to standardise these capabilities.

7.4.2. I2RS Architecture

The I2RS architecture is defined in “An Architecture for the Interface to the Routing System” [Ref 38]. It is at a relatively early stage of definition, however, the fundamentals of how the I2RS solution is intended to interact with the underlying network elements are clear. Figure 23 shows a high level view of the I2RS architecture based on IETF diagrams presented in “An Architecture for the Interface to the Routing System” [Ref 38] and the “Interface to the Routing System Problem Statement” [Ref 39].

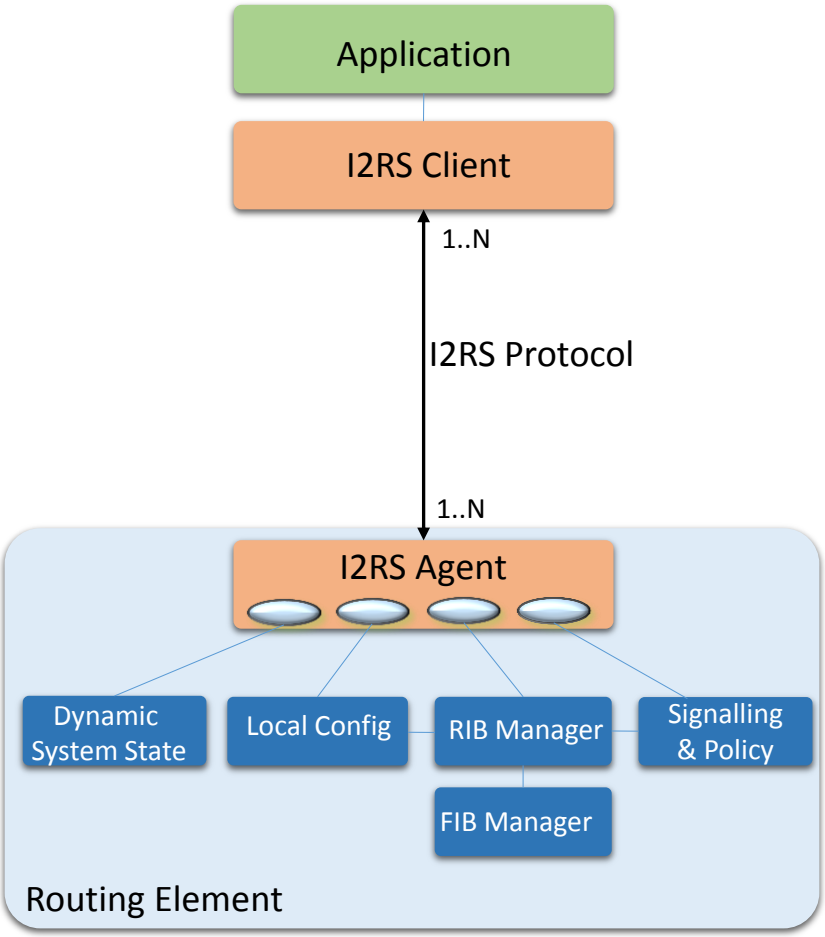

Figure 23 I2RS High Level Architecture

Fundamental to the I2RS solution are assumptions as to how it will interact with functions that currently exist within today’s routing platforms. I2RS defines the ability to read and write to the RIB that is held by the network element. This enables the application to over-ride the routing decisions that would have been taken by the network element if it were left to run autonomously

but it does not permit the overwriting of the lower layer entities the Forwarding Information Base (FIB) and the Link State Data Base (LSDB). The application can, therefore, insert its own routes, for example, to direct certain traffic to a service node, or to drop traffic that is currently subject to a DDoS attack without requiring it to understand the detailed routing and forwarding within the network. In order to standardise the process of reading and writing information into a RIB the I2RS working group has started work on a Routing Information Base Info Model [Ref 40].

Another application of I2RS is to be able to control what is advertised by the routing protocols. This includes the ability for an application to apply policy to prevent routes being advertised, or to provide policy to advertise a given prefix. Using I2RS it would be possible to build an application that took security and policy information about the range of valid AS numbers for peers to advertise and then automatically install this policy in the routers using the I2RS interface to the BGP protocol on the router. This would conceivably allow real time updates to policy on the routers simplifying the process of configuring BGP peering. In a similar way an I2RS controller could install static routes for adjacent nodes to the router that don't run a routing protocol and request that the router advertises the routes.

Because I2RS closely mirrors typical router implementations supporting I2RS should be relatively straightforward for an existing router architecture, unlike OpenFlow which may require significant re-engineering. An I2RS agent implemented on a router must provide a standard model of the RIB, routing policy engines and router state information, (for example, interface counters and statistics) to allow the I2RS controller to manipulate them using the I2RS protocol. These I2RS abstractions of the router can then be mapped to the actual RIB, state and policy engines implemented on the router using vendor proprietary interfaces (as shown in Figure 23).

In addition to being able to read/write to the RIB, and control routing policy, any I2RS client must be able to understand the underlying network topology, which may involve a number of IGPs and BGP, as well as information from the Traffic Engineering Database (TED). At this stage in I2RS development it is not clear whether I2RS will offer any support for this capability or whether it will be obtained using mechanisms such as peering with the IGP/BGP running in the network. Contributions have been received for the I2RS working group that defines the topology model [Ref 41] and one contribution has suggested that the topology information will be augmented with information from the network operators' inventory management systems [Ref 42]. It remains to be seen whether these proposals will be adopted by the working group.

7.4.3. I2RS Protocol

The I2RS working group has currently, not yet formally identified a protocol for the interface. It is possible that IETF will choose to use the NETCONF protocol for I2RS [Ref 43], or the closely related REST alternative RESTCONF. The NETCONF protocol is already used in the management of routers. However, in common with many management protocols NETCONF is really a framework rather than a fully formed protocol, and as such it will require the I2RS working group to define the information models that are being manipulated on the router. For background on NETCONF and its strengths and weaknesses refer to “NETCONF Ready for Primetime or Work in Progress?” David French 2009” [Ref 44].

The data models for NETCONF based control of devices are described using the YANG modelling language which is defined in IETF RFC 6020 [Ref 45]. The IETF Netmod working group have gone on to produce a number of RFCs and drafts, the most relevant to any I2RS use of the protocol being the YANG data model for routing management [Ref 46].

In addition to the challenges related to information models, an I2RS protocol will also need to be able to support the capability for multiple I2RS clients to control the same I2RS agent. This will require some sort of resource contention management solution which is currently under consideration by the working group.

7.4.4. I2RS Conclusions

Conceptually, I2RS is a good fit for implementing the SDN concepts of application layer control of networks within a conventional IP/MPLS carrier network. In fact, because it is aligned closely to router implementations, it looks a more promising candidate than OpenFlow in this space. The key strengths of the I2RS solution are:

- It provides an evolutionary approach to SDN that re-uses much of the existing proven capabilities within carrier IP networks.
- It works alongside proven and scalable routing protocols such as IS-IS and BGP. The significance of this should not be understated as BGP in particular is a critical component of the Internet and has very many years of experience and engineering refinement.
- It aligns with some of the SDK capabilities currently being provided by major router vendors, these may provide an early path to I2RS like applications in networks.

Despite these strengths I2RS faces significant challenges that must be overcome if the work is to reach maturity. Progress within the IETF has been relatively slow to date, the standard is in a very early stage of development and it is not assured that standardisation will be successful. The choice of I2RS protocol will be a significant factor in this but it is not the overriding one. The

major challenge that I2RS must overcome is that much of the work that must be completed is architectural and related to standardised information modelling. These are traditionally areas that the IETF has struggled with because it primarily standardises protocol.

7.5. PCE and PCEP

7.5.1. PECP Overview

Path Computation Element and the Path Computation Element Protocol provide a mechanism for the calculation, control and re-optimisation of MPLS Traffic Engineering tunnels (MPLS-TE). PCE is defined in a series of IETF RFCs and internet drafts produced by the IETF PCE working group. PCE is applicable to networks of MPLS routers and GMPLS capable optical elements.

Path Computation is the process of calculating the route through a network that should be taken by an MPLS or GMPLS traffic engineered tunnel of a defined size, delay and jitter in order to meet the requirements of the bandwidth reservation that it is supporting. The path computation element is a computing function within the network that the MPLS Label Edge Router has elected to delegate this calculation to. The Path Computation Element Protocol is the protocol run between the MPLS Label Edge Router (LER), known as the Path Computation Client (PCC) and the PCE. This protocol supports the signalling of the path characteristics from the PCC to the PCE.

To calculate the path, the PCE utilises its knowledge of the availability in the network based on its view of the Traffic Engineering Database (TED). The TED contains the set of all of the links within the MPLS domain, their characteristics and their available bandwidth. This information is distributed by traffic engineering enhancements to the IGP running in a given domain. One solution for a PCE to gain access to the TED is simply to peer with the IGP; in this way a PCE gains access to a TED that is effectively shared between all of the nodes (PCC and PCE) within a given domain. It is possible to use other out of band mechanisms to obtain access to the TED, or potentially to supplement the information in the TED, for example, information about non active links that are not part of the IGP topology. These mechanisms must, however, support continual updates and must be capable of scaling to support all of the nodes within the domain. It is possible that some of the work of I2RS could improve the topology information available to a PCE.

The PCE calculates a path within the domain that it is responsible for and returns the results of the path to the PCC within the PCEP protocol. This path computation is returned as an MPLS explicit route object which provides a set of IP addresses that the MPLS Label Switched Path for the reservation must pass through. It is possible for a PCE to return a less prescriptive path computation by returning one or more loose hops as part of a path calculation. A loose hop would

be, for example, an abstract IP address (which refers to a set of nodes) or an AS number. In this case further action will be required by another PCC to complete the end-to-end path calculation. This architecture is shown in Figure 24.

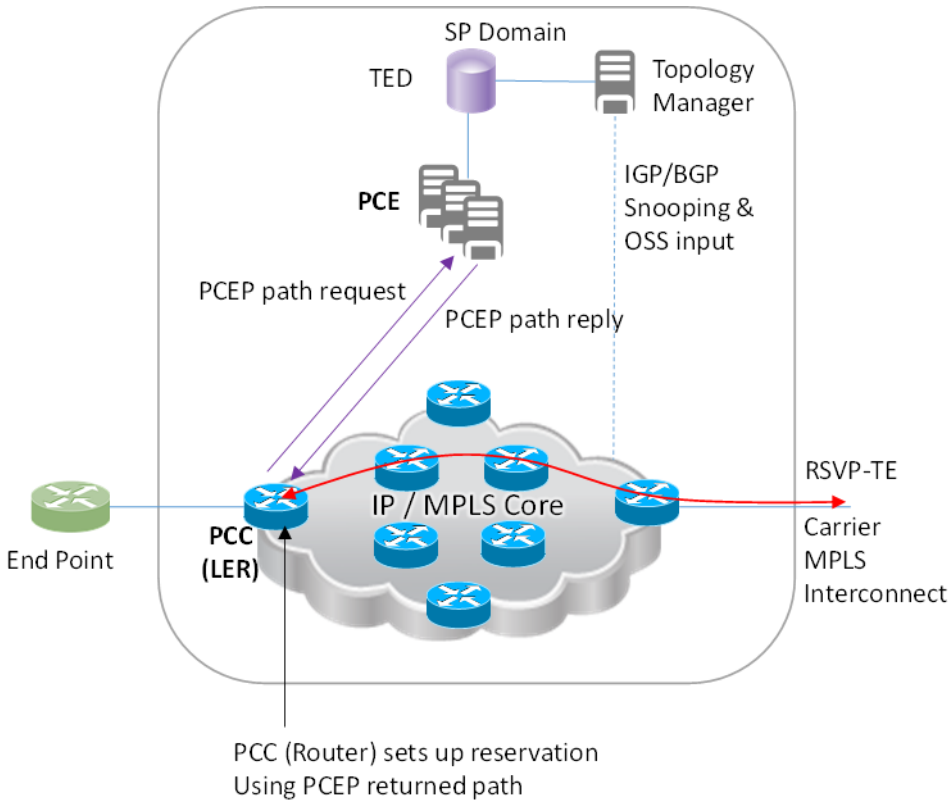

Figure 24 Stateless PCE Architecture

7.5.2. PCEP in Multi Domain Environments

A distinguishing feature of the PCE and PCEP solution, when compared to other SDN technologies is that is functions within multi-domain environments, potentially even being able to cross trust boundaries where required.

The PCE architecture is flexible with respect to the number of PCEs deployed, how they interact and how they scale. It supports a centralised computational model, where a single PCE (most likely resilient) is responsible for calculating the paths for a given domain. It supports a distributed computational model, where multiple PCEs exist for a domain and share path calculation responsibilities. Architectures have also been proposed to cater for so called multi-layer traffic engineered networks, which is most likely where a path must share a mix of MPLS controlled router and GMPLS controlled optical elements. In this scenario a PCE may have access to all the layers of the virtual network topology or it may communicate with multiple PCEs each responsible for a given layer of the topology. The implications of multi-layer networks on PCE and how the PCE architecture can accommodate it is described in “RFC 5623

Framework for PCE-Based Inter-Layer MPLS and GMPLS Traffic Engineering [Ref 47]. Where two PCEs communicate with each other for the purposes of path computation the PCE making the request acts as the PCC for the request and the PCE acting on the request acts as the PCE.

The multi-domain capabilities of PCEP are described in Appendix 1.

7.5.3. Using PCE and PCEP for SDN Applications

In order to utilise the IETF PCE architecture for SDN, it must be deployed as an active stateful PCE [Ref 48]. The fundamental difference between a passive and active stateful PCE is that the active stateful PCE can control the setup and tear down of the LSP resources that it is responsible for. This is achieved by having the PCC delegate the set of LSPs to the PCE that it wishes the PCE to control. Once a PCE has been delegated to control the LSP then it can instruct the PCC to update the LSP to reflect changing conditions in the network, including assigning it a new path. In the PCE architecture the PCC still remains in control of the LSP, and update requests that violate the local policy held at the PCC may result in the PCE request being rejected.

The ability for the PCE to modify the LSPs that it is responsible for allows it to pro-actively modify reservations in response either to changing network conditions or as a result of additional reservations being requested in the network. Because PCE has been specified to support both MPLS and GMPLS functions this capability can be used by applications wishing to optimise the mapping of MPLS bearers to the optical layer; an example of this is shown in “In Operation Network Planning” - IEEE Communications Magazine January 2014 [Ref 49] .The paper shows that a PCE based optimisation tool can be used to prevent spectrum fragmentation in optical networks that support variable sized frequency slots. This can be achieved by allowing a controller to adjust the allocation of lightpaths within the optical spectrum to group smaller light paths and free up larger contiguous blocks of spectrum.

The stateful PCE architecture has also been extended, as described in “PCEP Extensions for PCE-initiated LSP Setup in a Stateful PCE Model” [Ref 50] to permit a PCE to request that a PCC initiate an LSP. This allows application driven reservation of resources in the network and turns the PCE into a component of a fully-fledged bandwidth management implementation.

This type of stateful PCE can support the following use cases:

- Maintenance of bandwidth reservations in the network.
- Optimisation of network resources across packet and optical transport layers.
- Re-optimisation, re-establishment and prioritisation of reservations in the event of network disruption.
- Handling of on demand bandwidth requests from a bandwidth management function (either triggered from the OSS or from a web services interface, or from a future SDN application API).

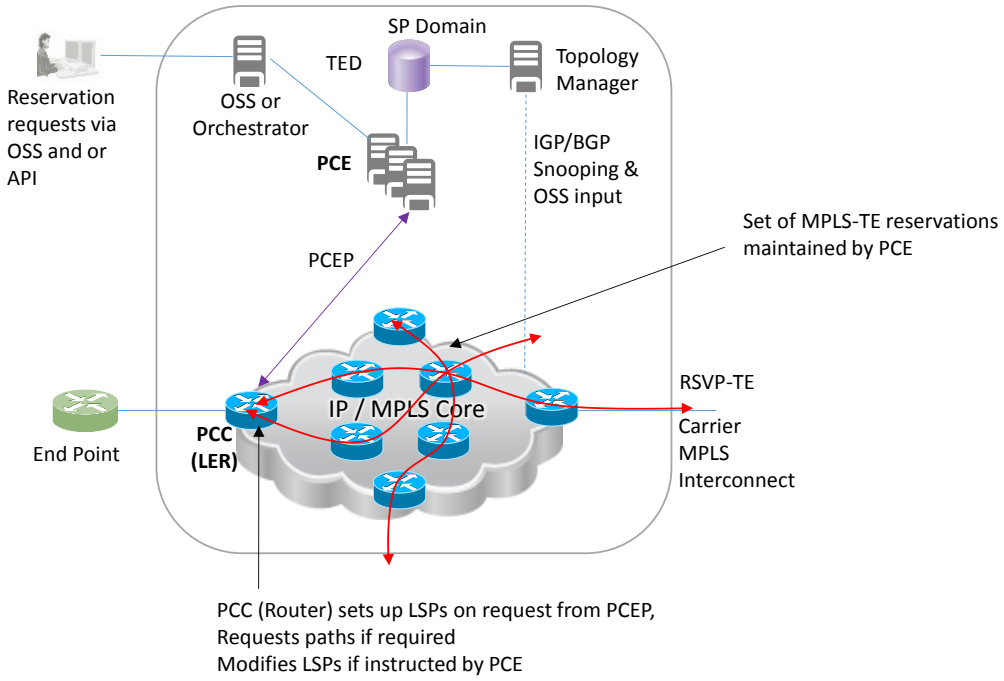

Figure 25 Stateful Active PCE in a Bandwidth Manager Application

It should be noted that there is a significant commonality between integrating the packet transport layer and the optical transport layer using OpenFlow (as being defined by the ONF) and offering the same functions using PCE. The fundamental difference between the two solutions is simply that PCE is optimised for MPLS transport and IP routers and OpenFlow is optimised for Ethernet switches and Ethernet transport. An individual vendor or carrier's preference for PCEP or OpenFlow for this application will depend on the approach they are taking to SDN. Carriers looking to re-use existing routing and transport architectures may consider PCEP, those looking for a white-box and NFV implementation of SDN will naturally view OpenFlow to be a better fit.

7.5.4. PCEP Protocol

The PCEP protocol is defined in “RFC 5440 Path Computation Element (PCE) Communication Protocol (PCEP)” [Ref 51]. The PCC first establishes a session with the PCE and having done so can request path computations and obtain the results of the path computation request. Keep Alive messages are supported in the protocol and notifications between the PCE and PCC (or vice versa) are also supported.

PCEP is a feature rich protocol that allows the requestor to indicate performance targets for resources and constraints, for example, to request a diverse route. It is also an extensible protocol and has been proposed to support new capabilities such as segment routing.

As noted previously an interesting aspect of PCEP is its support for multi-domain reservations and its potential ability to cross trust boundaries. A key aspect of trust boundaries is topology confidentiality which is a significant issue for a carrier network, especially where PCE is crossing not just domain boundaries but organisational boundaries (carrier interconnect points). Since the PCE architecture effectively requires an explicit path (in most cases) to be calculated end-to-end the question arises as to how a carrier’s internal topology confidentiality can be preserved.

In the PCE architecture each network segment that requires confidentiality can achieve it by having the PCE identify the segment that it requires to keep confidential (the Path Key Segment) and the generating a Path Key Value which is an opaque value understood by the PCE to map to a computed path. The Path Key Value plus the PCE-Id is sent as the Path Key Sub-object and included in the Explicit Route Object (ERO) signalled by the PCE in the Path Computation Report to the peer network. This defines part of the end-to-end route, and explicitly identifies the Border Router that is to act as ingress to the domain.

When the LSP setup is required by the Border Router (as requested by RSVP-TE from the peer network) it is able to retrieve the PCE-Id from the Path Key Sub-object it received from the peer network. It can then pass the Path Key Value contained in the Path Key Sub-object to the PCE (in its own network) that generated it. The PCE can then map this value to the explicit path it calculated earlier and return this ERO to the Border Router which can establish the LSP.

This sort of topology hiding is likely to become a consideration for other SDN technologies if they seek to interface with a peer network below the orchestration layer.

7.5.5. The ABNO Architecture

The PCEP architecture itself provides a framework for path computation and maintenance within an MPLS and GMPLS network. By adding active Stateful PCE capabilities the IETF have enabled the creation of bandwidth management functions within this environment. This is to a

degree an updated version of previous Bandwidth Management solutions such as ETSI Resource and Admission Control Subsystems (RACS) which was targeted at access networks and the MultiService Forum bandwidth manager which was an early proposal for core networks.

As noted in the discussions on I2RS, the IETF does not in general standardise network architectures but protocol solutions and architectures. However, some work has been done at the IETF in pulling this together as the Architecture for Application-based Network Operations, which is documented in an individual IETF draft [Ref 52]. This architecture is shown in Figure 26 (redrawn with permission from the original IETF version).

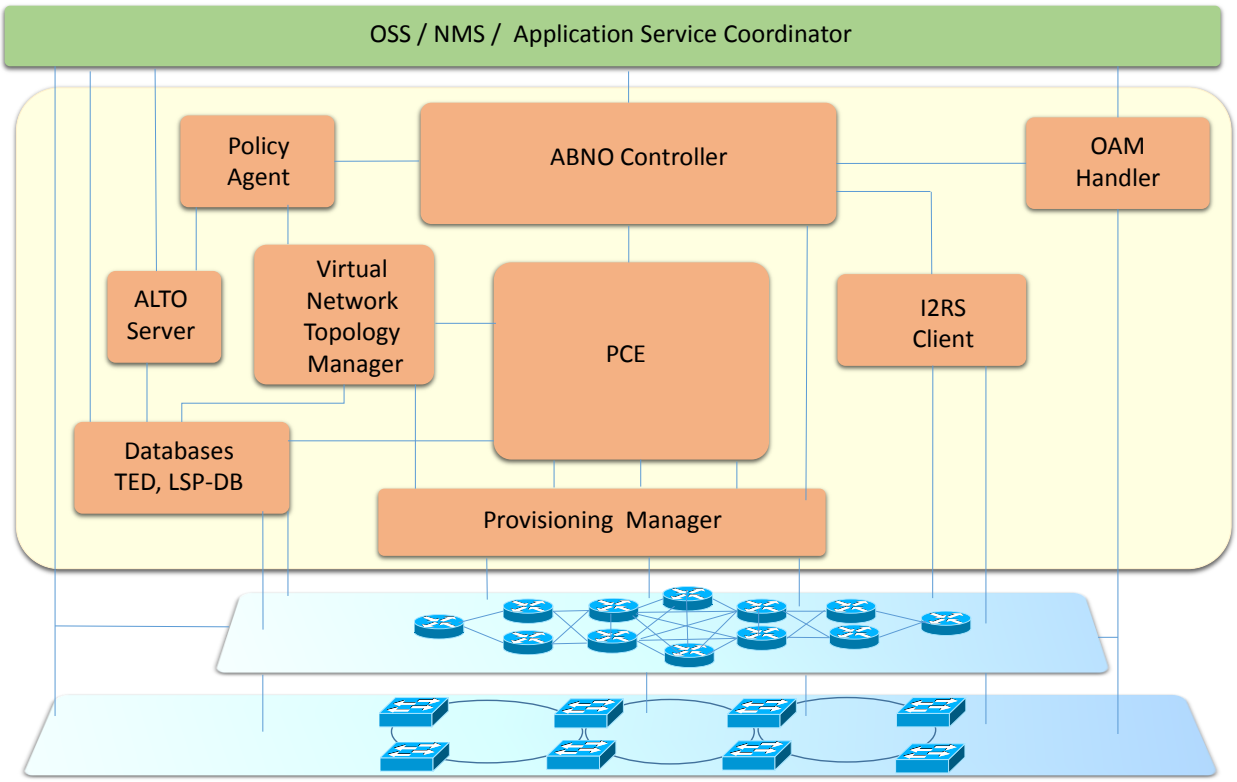

Figure 26 The ABNO Architecture

The ABNO architecture can be seen as a Path Computation centric version of the more generic SDN controller architectures. The ABNO controller provides an orchestration function, with northbound interfaces to the OSS and an application services interface (to permit real time requests from applications). It allows the applications using the network to request specific paths through the network, with specific performance criteria. The same orchestration function can also be used for OSS initiated connections and can integrate into the network operators processes around areas such as network planning.

Within the ABNO architecture the interfaces to the network are I2RS for routing control and policy, plus (if supported) supplemental topology information, IGPs and BGP-LS for TED synchronisation, and primarily PCEP for MPLS path provisioning. The architecture suggests the

use of ALTO as one possible solution for presenting the applications with an abstracted network topology.

There is some interest in the ABNO architecture from elements within the carrier community, however, it is too early to determine if this will become widely adopted. The most likely deployment scenario would seem to be in the area of rapid path calculation and maintenance over an MPLS/GMPLS network. In particular in any deployments where a network operator must handle significant numbers of high bandwidth flows that change destination or bandwidth/latency characteristics on a regular basis. Some examples of the functions and capabilities of the ABNO architecture for these sorts of applications are described in the article “In Operation Network Planning” IEEE Communications Magazine - January 2014 [Ref 49]. In addition the recent segment routing proposal (Section 7.6) can be seen as aligning closely with the principles of the ABNO architecture, although the implementation is different.

7.5.6. PCEP Conclusions

PCE is a relatively mature standard, although the components of it that permit the use of stateful PCE are slightly less mature and the capability for the PCE to trigger LSP creation is a recent (although straight forward) addition.

Although PCE has been available for a number of years as a standard it does not have a significant existing implementation base, this is most likely because the high volume complex multi-domain path computations that would justify it do not yet exist in today’s networks. However, path computation is a significant overhead for network operators and an efficient external PCE platform might become attractive as a solution to optimising networks in support of Optical/Packet integration and video content delivery. PCE is currently implemented by both Cisco and Juniper equipment and third party protocol stacks are available. The integration of PCE with GMPLS and its application in preventing spectral fragmentation in optical networks may also act as a driver for future deployment. The ABNO architecture provides a coherent vision of how PCEP may be used to support SDN functions within a network.

In addition to the applications that have existed for PCE since its creation, Segment Routing has recently emerged which provides yet another approach to optimising core networks. This is described in Section 7.6 and makes use of PCEP to provide path computation information.

7.6. Segment Routing (IETF SPRING Working Group)

This section describes segment routing with a particular emphasis on its impact on MPLS networks and how it can be used to enable SDN within the carrier network. It is important to note the segment routing is not limited to MPLS networks and that it does not mandate the use of PCEP, however, other applications of segment routing are not considered in this paper.

7.6.1. Segment Routing Overview

Segment Routing is a technology that was announced by Cisco in 2013 and has the interest of a significant number of service providers. There is now a significant quantity of material published on Segment Routing, a good overview from the perspective of routing is provided in a presentation given to RIPE 66 [Ref 53].

Work is currently underway in the IETF within the Spring Working Group to standardise Segment Routing, however, this work is at an early stage. The Segment Routing architecture is currently described in “Segment Routing Architecture” document [Ref 54].

The fundamentals of Segment Routing are as follows:

- Nodes advertise a label to identify themselves via an IGP such as IS-IS. This requires a single label and is known as a Node Segment.
- For each link a node generates a local label to represent the link and advertises it as an adjacency label in the IGP.
- Segment Routing works with the existing MPLS data plane without requiring changes to it.
- A network that uses Segment Routing for an MPLS data plane does not need to implement Label Distribution Protocol (LDP) or RSVP-TE.
- The solution uses a separate Segment Routing Label space and can interoperate in a ships in the night approach with existing MPLS services.
- All of the routing behaviour and flow state is imposed at the ingress node in the domain, core routers do need to hold flow state but instead forward only on the label.
- The solution allows the ingress node to impose a stack of labels to a flow that can determine not only its destination in terms of loose routing, but also a strict routing path through the network that can mandate the individual links traversed. By an appropriate choice of labels it is possible for an ingress node to combine the two approaches and specify an explicit path for only part of the route. This allows the use of Equal Cost Multiple Path (ECMP) mechanisms with segment routing.

- A node's adjacency label can be used as a service identifier which supports the chaining of services within the network. Since adjacently labels only have meaning at the node they were issued at this is highly scalable.
- Segment Routing when combined with an SDN controller effectively provides a degree of network programmability equivalent to that provided by OpenFlow within a data centre, but implemented incrementally on an operators existing MPLS routing infrastructure.

While a full discussion of segment routing is beyond the scope of this paper, it has clear applications within the SDN space and with relatively minor changes to PCEP as described in the "PCEP Extensions for Segment Routing" document [Ref 55], it can re-use the Path Computation Element architectures and solutions. In addition to support of the PCE architecture segment routing also provides an easy route to service chaining which adds considerably to the PCE capabilities. It should be noted that the enablement of SDN is not necessarily the only reason for implementing segment routing within MPLS networks, as it improves RSVP-TE scalability issues and removes the need for LDP.

7.6.2. Segment Routing and SDN

Figure 27 shows how segment routing can be used with an SDN controller to support Service Orchestration and service chaining in a network environment. The diagram shows how a flow can be classified, assigned a path through the network and have a service applied to it (in this case firewall) at a defined point in the network. It should be noted that this is a high level example to illustrate the concept, the actual implementations are likely to vary significantly in the details.

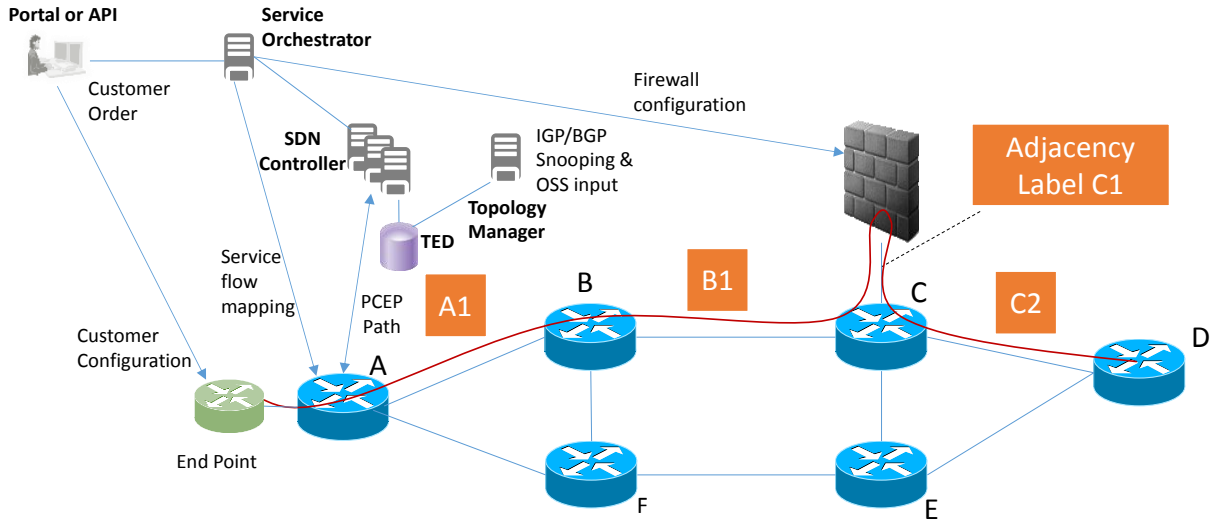

Figure 27 An SDN Application of Segment Routing

In this example, it is assumed that the network is an MPLS network, and that the SDN controller is configuring the segment routing within the network by acting as a PCE to the edge nodes. Depending on how service flows are classified the end customer may be required to configure their router as part of the service set up.

The key points of this high level example are as follows.

- The SDN controller can act as a bandwidth manager for the network to control the reservation of resources within it (effectively it is acting as an active stateful PCE even though it is not controlling LSPs).
- The SDN controller must have access to topology information about the network and is responsible for path calculation. It configures the paths in the network by using PCEP to signal the label stacks to the ingress nodes of the network.

- This solution can support a number of fast re-route protection mechanisms, however, they are not described here.
- The SDN controller must provide a mechanism to map the customer flows arriving at the ingress node to the flow configured for the service in the network. There are a number of ways that this can be done, including passing the entire label stack to the customer, or more likely signalling a token and mapping this token to the label stack at the ingress node. An OpenFlow solution that defined the mapping would also be an option.
- The entire path through the network, the node, and the services selected (which can be at any point in the network journey and can be chained), are determined by the SDN controller and fixed by the ingress node when the label stack is imposed.
- Options exist for the path to be strictly or loosely defined or a combination of the two.
- MPLS-TE and LDP are not required, however, the SDN controller will be responsible for enforcing any bandwidth reservations it has applied.
- The operator can run their existing MPLS control plane for all of their other services independently of this SDN service, however, the operator must have a solution for solving bandwidth and resource contention.

7.6.3. Segment Routing Conclusions

Although segment routing is very early in the standardisation process it is backed by Cisco and has a number of significant advantages for any operator looking to move towards a more SDN centric approach to their WAN. This technology is being looked at by operators not only because of SDN but because it permits them to remove LDP and RSVP-TE from an MPLS network. This has a significant advantage in terms of scalability within such a network.

The single biggest advantage segment routing has in the SDN space is that it can support a ships in the night approach with regards to existing services. This means the network operator has the option to use it for only a few services, whilst leaving the rest of their service portfolio untouched. Furthermore, it does not need changes to the IP routing infrastructure and it has no significant impact on the IGP, BGP and MPLS control plane run by the network operator. This means a network operator looking at an evolutionary approach to SDN can deploy a solution using segment routing in a relatively risk-free way. For example, a network operator could leave their high volume but low touch services unchanged, (residential broadband and Small, Medium Enterprises - SMEs) whilst introducing an SDN component for their large enterprise (lower volume but high touch) services.

Another key advantage is the hooks it provides for service chaining which makes it relatively easy for a suitable controller to set up and move services around the network. This is a capability that PCE architectures did not support and may prove a reason for an operator to consider implementing segment routing and an SDN controller.

While it is early days with respect to segment routing and SDN, the approach looks a very good fit for a carrier network where evolution rather than revolution is required. The fact that the technology is backed by Cisco (who also provide a set of APIs and an SDN controller) makes early deployment of this technology likely at least as a proof of concept. The IETF standardisation process that is underway should also ensure that other router vendors will support segment routing, provided they get sufficient customer pull.

7.7. SDN Application API

One of the promises of SDN is the ability to expose the power of the network to Service Provider customers and application providers. In reality what this means is that the network should be able to expose information about its topology, state, resources and available services in a way that the application can understand and utilise. Similarly the application should be able to provide the network with key information about its requirements so that the network can select an appropriate service. The information required to be exchanged varies on a per application basis.

Such an interface should permit rapid innovation from OTT providers, potentially leading to an SDN ecosystem of innovative applications that combine the network and other domains to provide compelling functionality. This interface is referred to by industry as the SDN Northbound API.

However, in reality there is little standards work in this area and while there are a plethora of SDN controller APIs there is no consensus as to what the application API should look like, beyond the simple statement that it should be REST. There is some indication that part of this may be a carrier reluctance to expose the northbound interfaces to OTT providers, perhaps fearing that such an interface would confine them to the status of bit transport. However, another issue is that the current immaturity of the SDN solution space means that the northbound API is difficult to address, as there are many architectural options and it is not clear which API should be standardised.

This is shown in Figure 28.

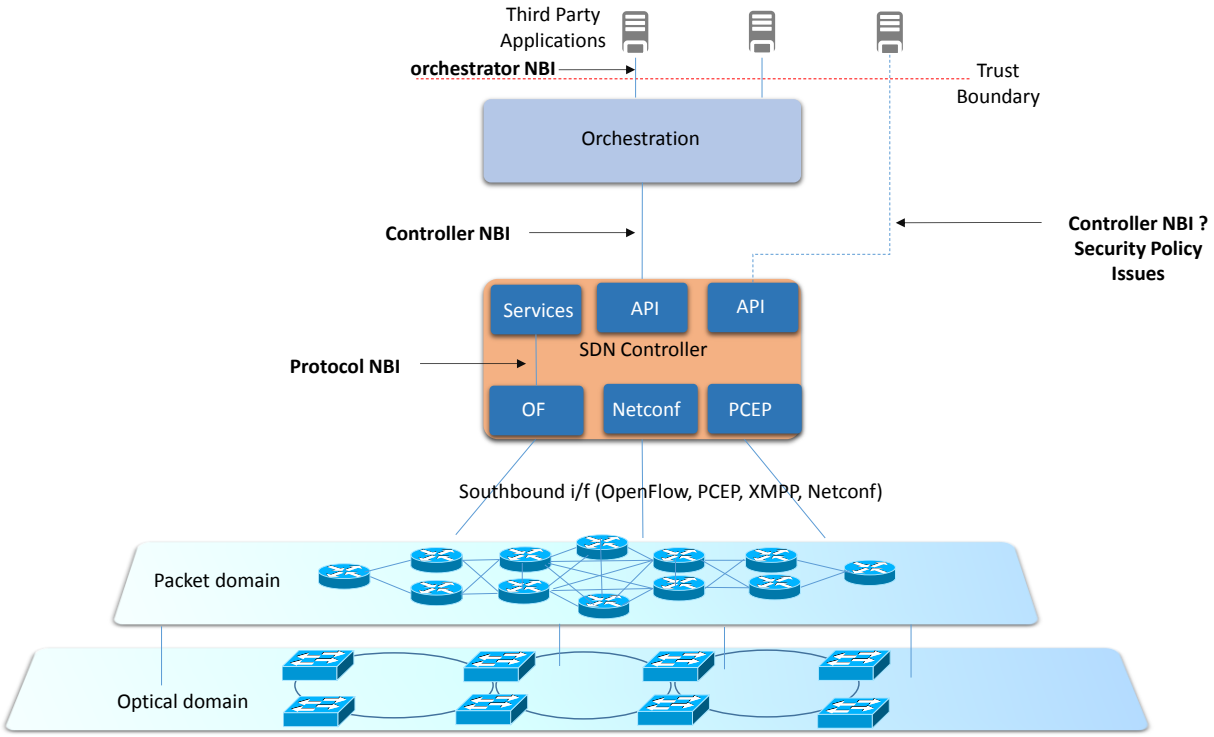

Figure 28 Multiple Northbound APIs

From an OpenFlow viewpoint the API is buried deep within an SDN controller function. From the SDN controller viewpoint the northbound API may connect to third party organisations but in reality is more likely to interface to an orchestration function for a number of reasons including:

- Security aspects of permitting third party organisations direct access to an SDN controller.
- Business rules many need to be applied over the northbound interface which may require BSS capabilities.
- Any service offered over the northbound interface may require the functions of an orchestrator as well as an SDN controller, for example, cloud services may require the configuration of physical or virtual servers and the instantiation of network services as well as the network connectivity.

It seems likely, therefore, that from a carrier perspective the critical northbound interface to application providers will resemble their existing automated OSS/BSS interfaces to customers and be north of the orchestrator. To exploit SDN, this interface must be more real time than existing OSS/BSS interfaces and must expose additional network capabilities, as considered in Section 4.4. There may also be benefit in aligning the service model at this interface with the YANG models in SDN controllers such as OpenDaylight.

If the northbound interface is above the orchestrator then it is likely to be carrier specific, which may prevent the adoption of standard APIs to applications. This in turn may prevent OTT providers from developing applications because of the overhead of customising a global “consume anywhere over any network” product to individual carrier networks. It is possible that a set of common capabilities and interfaces may emerge from standardisation to resolve this issue.

One important initiative in the industry comes from the ONF and OpenDaylight. These organisations are looking to collaborate on the northbound interface to define use cases and develop reference applications in order to stimulate the SDN ecosystem. The progress achieved in this area may be critical to determining if SDN can succeed in fostering rapid service innovation.

8. Network Functions Virtualisation

Network Functions Virtualisation is a term used to describe replacing an existing network element that is running on dedicated hardware, such as a firewall, with a software version of the network element running on a COTS computing platform. This process has been ongoing for a considerable amount of time within data centres and within networks.

The initial phase of development was simply replacing the dedicated hardware used by network equipment vendors with commercial servers, with or without a Real Time Operating System (RTOS) depending on the platform requirements. For some network platforms this coincided with the split of the control and data planes and the introduction of a control protocol between the two planes that permitted the controller to configure the data plane. As an example the Session Border Gateway was decomposed into a Signalling Border function (which handled the control plane signalling) and a Media Border function which handled the media flows and any transcoding requirements. The advantage of this solution was that it permitted the media border function to run on dedicated hardware, designed to handle media flows and equipped with specialist transcoding hardware, whilst the signalling border function could run on a COTS server. The ITU-T H.248 protocol was used to allow the signalling border function to control, and receive notifications from, the media border function. This control was achieved by adding specific packages to the ITU-T H.248 protocol that permitted the admission and rejection of specific media flows and the control of NAT.

Network Functions Virtualisation has become more important with the arrival of virtual machines, hypervisors and the modern data centre. Today data centres run software firewalls and load balancers in virtual machines on x86 servers, and virtual Switches (vSwitches) within the hypervisors. It is true today that the majority of Ethernet ports in data centre infrastructures are virtual ports, and this provides a significant flexibility in moving services round (and between) data centres.

The next stage of Network Functions Virtualisation is to start to provide software versions of traditional carrier network functions running in virtual machines, either in data centres or in metro nodes. However, it is less straight forward to virtualise carrier network functions than it is to virtualise enterprise network functions for a whole host of reasons including:

- Data plane performance requirements.
- Security requirements.
- Operations and management complexity.

A number of network operators have, therefore, collaborated under the umbrella of ETSI ISG to try and accelerate progress in this area. This organisation is known as ETSI NFV.

8.1. ETSI NFV Overview

ETSI set up an Industry Specification Group to look at network functions virtualisation to meet the needs of a number of operators who outlined their vision for Network Functions Virtualisation in an introductory white paper published in 2012 [Ref 56]. The vision of ETSI NFV is that any network function can potentially be virtualised, replacing dedicated network hardware with a virtual instance on commercial x86 based computing platforms.

This broad vision was set out in the white paper [Ref 56] and is reproduced in Figure 29.

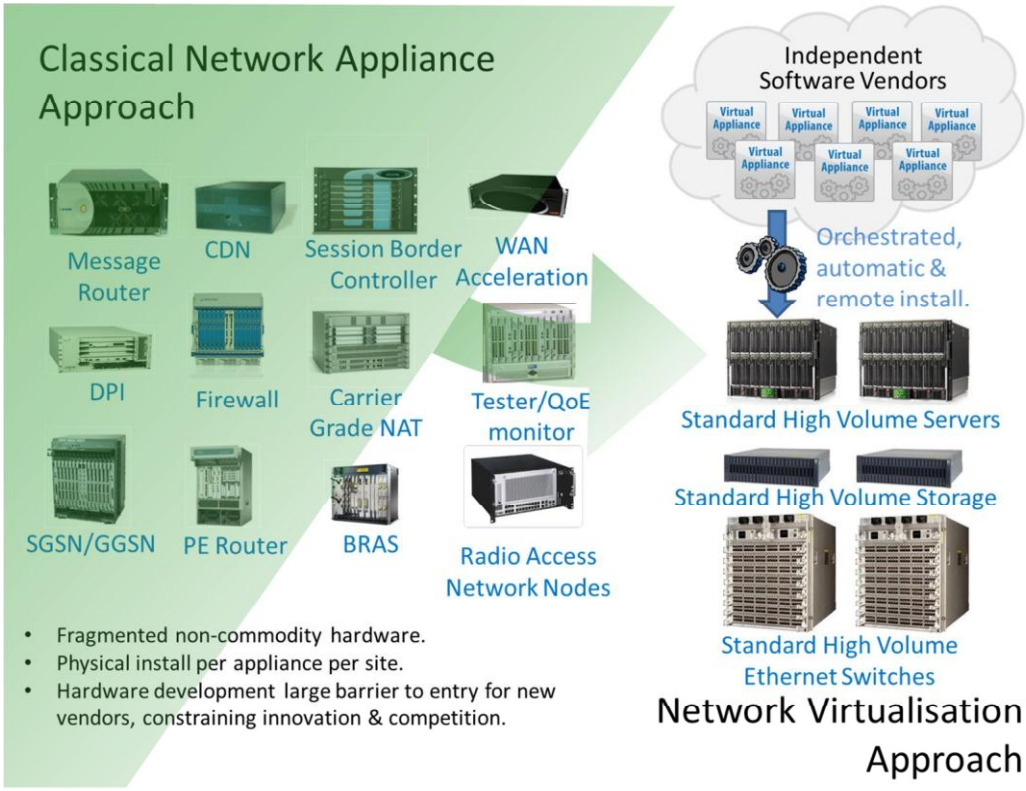

Figure 29 The ETSI NFV Vision

It is important to note that this vision is independent of SDN. While SDN technologies assist in aspects of an NFV deployment it is not strictly necessary to use SDN to support NFV. For example, an operator can simply virtualise an existing platform such as a BNG but leave the functions and protocols untouched from the version running on dedicated hardware.

ETSI NFV is looking at all aspects of NFV, including the architecture, the management problems, performance and security. As part of this work activity ETSI has also defined a set of virtualisation use cases that are of significant interest to its members working in NFV.

The ETSI NFV Use Cases [Ref 57] provide an insight into where the industry is targeting virtualisation. They are summarised as follows:

- Network Functions Virtualisation as a Service.
  This use case exposes the NFV Infrastructure as a service permitting a third party organisation to run a virtual network function on top of it. This is effectively an NFV optimised version of the traditional data centre IAAS offering.

- Virtual Network Function as a Service
  This use case exposes a single network virtual function as a service permitting a third party to purchase that function. ETSI give two examples a virtual CPE and a virtual PE.

- Virtual Network Platform as a Service
  ETSI define this as an extension of a virtual network function to include a package of network functions offered as a service, with higher layer configurations and possibly control interfaces and APIs.

- Virtual Network Functions (VNF) Forwarding Graphs
  VNF forwarding graphs can be considered as a way of describing service chaining. This use case exists to demonstrate how this can be achieved within an NFV infrastructure.

- Virtualisation of Mobile Core Network and IP Multimedia Subsystem (IMS).
  A use case to establish an EPC and an IMS within an NFV framework.

- Virtualisation of Mobile base station
  Support for a virtualising the Baseband Band Unit as part of a C-RAN scenario, which is described in Section 6.4.2.

- Virtualisation of the Home Environment
  The use case is an extension of the virtual CPE case to cover the entire home environment including not just the broadband router / modem but also the Set Top Box.

- Virtualisation of Content Delivery Networks (CDNs)
  This looks at how an operator can deploy NFV to virtualise devices such as CDN controllers and CDN cache's to reduce the physical hardware they require in the network.

- Fixed Access Network Functions Virtualisation
  Considers how the elements of a fixed access network can be virtualised, with specific reference to future deployment models such as FTTdp and G.Fast where power and cost will be even more critical than they are today. This looks very much like an SDN use case where the virtualisation is of the control plane.

Following the work of ETSI NFV a number of operators issued Network Functions Virtualisation update white paper published in 2013 [Ref 58], summarising the progress to date.

8.2. Architectural Aspects of NFV

ETSI NFV have defined an architectural framework for NFV [Ref 59]. The high level architecture that they have documented was summarised in [Ref 58] and is reproduced in Figure 30.

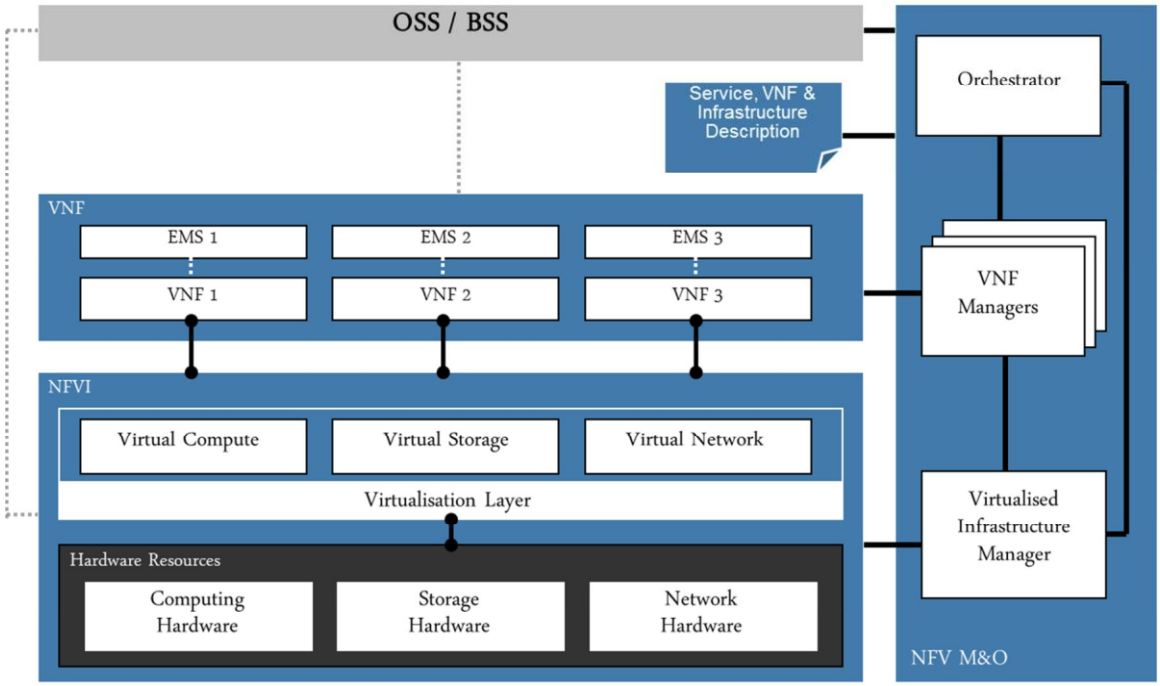

Figure 30 NFV Architectural Framework (source ETSI)

Work within ETSI NFV has further decomposed this architecture to consider key areas. This includes the Infrastructure Architecture [Ref 60] which is further broken down into the Compute, Hypervisor and Infrastructure Network Domain, and the Management and Orchestration function which is described in [Ref 61].

A key difference between the ETSI NFV requirements and the typical data centre virtualisation solutions is the Hypervisor and its relationship to network functions. In a traditional data centre the virtual machine running on top of the hypervisor runs an application which terminates the traffic and utilises the compute and storage facilities available to it to execute a service. With Network Functions Virtualisation, the virtual machine running on top of the hypervisor is a network function which may have many logical interfaces and may onward route the traffic to other virtual network functions, or indeed physical network entities. This connectivity may also change over time and different flows may utilise different virtual network functions in different orders, depending on the service that has been invoked. This is an example of service chaining and the ETSI model using Virtual Network Functions Forwarding Graphs to describe the path through the network.

Because network functions can be transient in this architecture, and because of the flexible nature of service chaining network functions running on virtual machines, the NFV environment is operationally complex. All of these virtual network functions will require provisioning, service assurance and performance management. This will require a capable management and orchestration solution. For example, to start up a network virtual function a number of carefully sequenced steps are required. The physical server must be started, then its management applications, and then virtualisation solutions such as OpenStack must be used to create the virtual machines that have been allocated to the server. One this has been done the network functions themselves can be started on the correct virtual machine and the network connectivity provided. Only once these steps have been taken can the network supported by the network functions start to instantiate itself.

One of the issues that the flexibility of NFV raises is that of security and service assurance. Because the network connectivity is more flexible than traditional hardware, it is important that tools are provided to enable the actual path being taken through the network to be determined and its actual performance in terms of delay, jitter and packet loss measured. This is particularly important from a security viewpoint as the possibility now exists for traffic to be accidentally or maliciously routed to incorrect or undesirable network functions. ETSI are addressing these concerns in an ongoing security [Ref 62].

Another challenge of NFV is to support the sort of intensive Input/Output (I/O) operations that network functions require in order to avoid the virtualisation tax, where network throughput is compromised by the use of virtualisation and emulation software such as the vSwitch. This can lead to a performance penalty of up to an order of magnitude compared with a bare metal server. In order to address this ETSI NFV has proposed a specific Hypervisor solution that differs from a typical Cloud computing Hypervisor in its ability to permit the applications to access the Network Interface Controller (NIC) without utilising the vSwitch.

The ETSI NFV Hypervisor architecture is described in ETSI GS NFV INF 001 Network Functions Virtualisation Infrastructure Architecture; Overview - Sub-section 7.2 Hypervisor Domain [Ref 60]. The differences between a traditional cloud computing architecture and ETSI NFV compatible architectures are summarised in Figure 31.

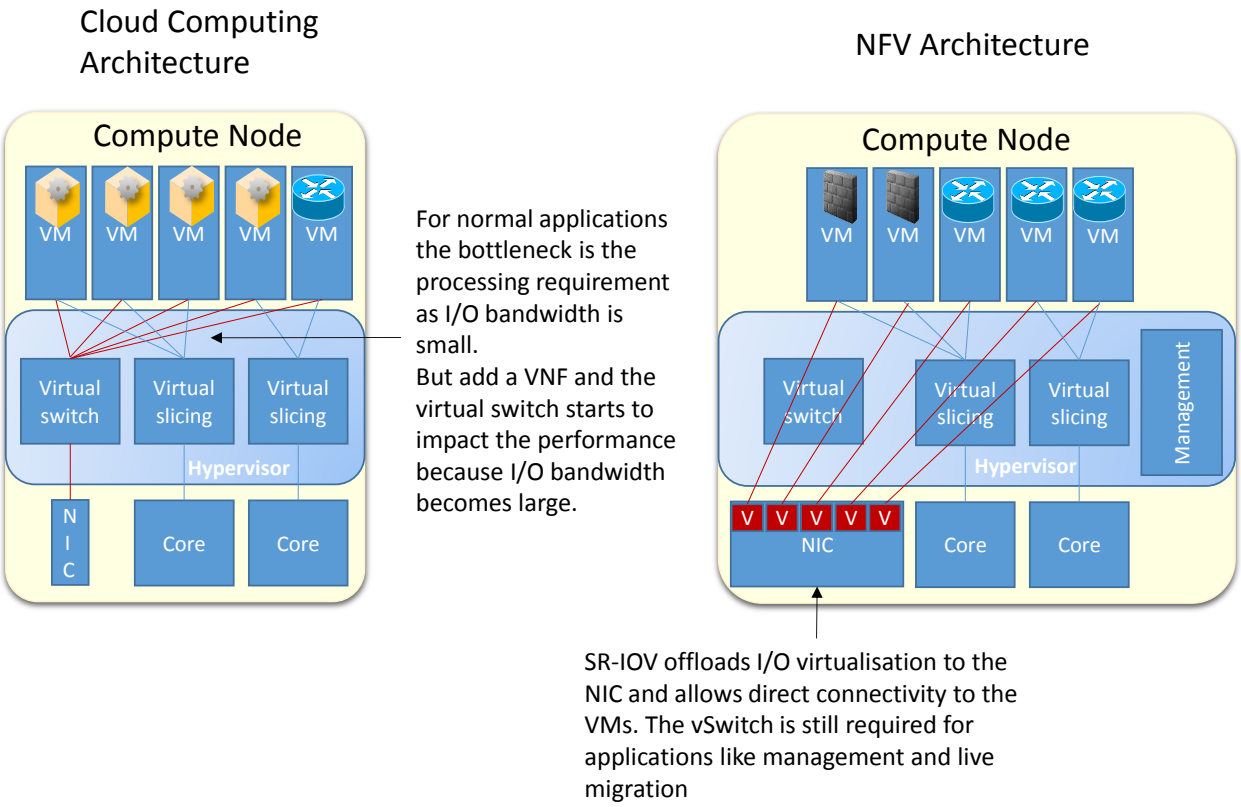

Figure 31 Cloud Computing and NFV Hypervisor Architectures

The objective of the NFV hypervisor architecture is to permit NFV applications to maximise the performance they can achieve within a virtualised environment and to minimise the performance penalties caused by virtualisation. However, these architectural refinements have impacts in other areas of virtualisation, as they complicate traditional cloud computing facilities such as live migration capabilities. These capabilities are used to support the movement of virtual machines, either because of a service requirement, (for example, follow the moon energy saving solutions) or because of a hardware maintenance need.

X86 vendors can support these NFV requirements, and have gone further by providing additional capabilities in their products that are specifically aimed at supporting virtualisation. The key technologies that achieve this are:

- Direct Assignment, This allows an I/O device to be assigned to a specific virtual machine, which is one way that the ETSI NFV Hypervisor can achieve its target architecture as

shown in Figure 31. This, however, has obvious scaling limits for deployments requiring a large number of virtual machines.

- Single Root-I/O Virtualisation (SR-IOV). This permits the efficient sharing of a PCI device among virtual machines. It can be layered on top of direct assignment to permit a single physical device to be virtualised and shared between multiple virtual machines with minimal overhead. This requires support in the chipset, the NIC, BIOS, Hypervisor and guest OS drivers.
- Optimisation of interrupt handling to minimise latency.
- Careful memory handling aimed at removing the penalties of virtualisation. This includes optimisations to support Non Uniform Memory Access such that the memory space and scheduling are optimised for performance; and address translation support to allow the CPU to directly access memory without using the Hypervisor (Intel Extended Page Tables®, AMD Rapid Virtualisation Indexing®). Note that with current generation of chipsets certain NFV applications hit a problem known as Input Output Translation Look aside Buffer (IOTLB) eviction, this can halve the achievable throughput versus a bare metal solution. This is a limitation as to the size of I/O pages that can be supported in virtualised hardware, however, it is expected to be mitigated significantly in future x86 processors.

In addition, Intel have added a feature called Data Direct I/O Technology (DDIO) which permits I/O data to use the processor cache rather than the slower main memory.

To assist developers in optimising performance, Intel provide a Data Plane Development Kit (DPDK) to allow developers to easily integrate with I/O optimisations on the Intel platform.

8.3. The Limitations of Network Functions Virtualisation

The ETSI NFV hypervisor architecture, and the optimisations of the x86 architecture to support NFV have significantly narrowed the gap between what can be achieved on dedicated network hardware and what can be achieved on virtualised hardware.

However, it is also true that ASIC and network processors still have some advantages because they are optimised for I/O and packet classification in a way that x86 architectures are not. For example, network equipment makes extensive use of Ternary Content Addressable Memory (TCAM) for packet classification. This is not available within an x86 architecture, which must perform multiple memory lookups to implement the same operations. While some of these limitations may be removed in later x86 implementations it is also true that dedicated hardware will be required to match the packet forwarding performance of large routing and switching platforms.

One approach to solving this is to adopt hardware acceleration in the NFV environment. This allows the NFV application to split the control and forwarding application and to pass high I/O, low compute flows to a hardware accelerated device. This approach would make an NFV application look much like a traditional router vendor service node (where they offload compute intensive processes to x86 servers). This is the white-box architecture, previously discussed in this paper. By its nature such a solution is less flexible than a purely virtual NFV solution, and as noted whether there are economic benefits from this approach versus using dedicated router vendor hardware for these applications is still an open issue.

Currently, there seems relatively little hard information about the performance of x86 based virtual solutions versus ASIC / Network processor based hardware. It seems likely, however, that compute intensive applications such as the EPC, IMS and DNS will be virtualised, while packet forwarding intensive applications such as core routers will not. Similarly, it seems likely that extremely delay critical applications will also remain on custom hardware.

There is, however, a debate about at what point PE routers and BNG nodes can be virtualised and it seems likely that some smaller nodes will be candidates for virtualisation whereas larger ones probably will not. However, there is some evidence that this will also depend on the actual application being supported by the PE router rather than just its raw capacity. Initial reports from industry leaders in the field suggest that for some network applications a throughput of 10 Gbps per x86 core can be achieved with virtualisation [Ref 63].

The extent to which NFV approaches win out versus a router vendor service node approach at the metro node may depend on the individual network operator’s appetite for becoming a systems integrator versus accepting a turnkey fully supported solution.

9. SDN and OSS/BSS

9.1. The Nature of OSS/BSS in Carrier Networks

Today's tier one carriers typically have large and complex OSS and BSS systems that sit right at the core of their business. These systems are essential to the day-to-day running of the business and allow orders to be taken and billed, equipment to be provisioned and dispatched as part of order fulfilment, and once the service is running, the assurance and maintenance of the service. In many cases carriers offer APIs to their customers to permit the automation of the service, allowing large numbers of orders to be placed and tracked without requiring manual intervention. These interfaces typically use xml, although there is a move towards Representational State Transfer/JavaScript Object Notation (REST/JSON) type interfaces. Within a tier one carrier all high volume, low touch services (such as residential broadband and phone services) would typically have this type of OSS/BSS support.

However, as OSS development is expensive, not all features that can be automated, are automated. Certain services, such as high value but relatively low volume services may never be automated; either because the complexities and overheads of implementing the OSS mean the investment cannot be justified in terms of the cost of remaining with a manual process, or because OSS technology (which is typically non real time) is just not suited to automating the task. For example, layer 3 VPN services are complex and time consuming to provision but the volume of changes may not justify automation.

Smaller tier two and tier three carriers often have lower volumes of services and so tend to deploy smaller more lightweight OSS/BSS capabilities, typically automating far less. However, they are also more likely to operate in a single vendor environment which allows them to purchase turn-key solutions with integrated management and some OSS/BSS support.

The impact of the OSS/BSS on a carrier should not be underestimated. The lack of a large scale OSS/BSS can cause smaller carriers significant costs and operational issues and limit their ability to roll services out at large scale. However, the single vendor environments and simplified OSS/BSS they run can also allow them to be much more agile than the larger carriers in deploying services. In contrast a tier one carrier has an OSS/BSS geared to reliable high volume, low cost operation of their key services. However, the OSS/BSS can choke innovation because any new service may have to sit in a development stack for up to two years before it can be rolled out. In this environment the large carrier looks to SDN as an adjunct to the OSS/BSS to give them service agility and free them from the OSS bottleneck, and the smaller carrier looks to SDN to give them repeatable, automated error free configuration in-lieu of the equivalent capability from their OSS.

9.2. The Impact of SDN on the OSS/BSS

SDN will exist within the established hierarchy of management systems. These support the business processes defined by the TMF Enhanced Telecom Operations Map (eTOM) framework including: order handling, service fulfilment, service assurance and billing. All of these business processes are still a requirement in an SDN world. This means that services that are orchestrated through an SDN framework will need to have touch points into the OSS and BSS systems already deployed by service providers. Where SDN differs is in how those services are defined.

A traditional deployment uses flow through provisioning of services from an ordering portal through to a network management system, and then on to an element management system; which will finally result in modifications to a configuration file stored on a network element. The management plane on the network element is then responsible for instantiating the required forwarding entries and control functions for the service. Service assurance requires integration with network management systems to collect details of network faults and performance monitoring information. Any change to a network service potentially requires co-ordinated changes to many of these systems which is both costly and slow. This has been termed ‘ossification’ of networks. Systems cannot be bypassed because the interfaces between them are often proprietary. This is even the case where standardised management interfaces are used, due to the diverse approaches taken to data modelling.

In an SDN environment, this management stack is disrupted. From the perspective of a network element, service configuration is ephemeral. Configuration is centralised with the SDN controller and does not need to be maintained within element management systems and network devices themselves. Therefore, in principle service changes can be implemented solely by an SDN controller.

Different flavours of SDN simplify management in different ways. OpenFlow provides a single model for network equipment. Network overlay solutions reduce points of configuration by pushing the configuration to the edge of the network. Solutions such as PCEP centralise the high touch elements of the control-plane, allowing service changes to be implemented on the central functions independently of the underlying network equipment.

However, many functions of the EMS/NMS (inventory management, alarm monitoring, node configuration) will either have to be migrated into the SDN controller, or handled by existing management platforms and the conflicts resolved. One case highlighted by the IETF work in I2RS is the example of non-active topology (i.e. links that are present in equipment but not activated, and, therefore, not detected by peering with link discovery and routing protocols). Given the overlap of SDN and OSS in certain areas the key to smooth transition is probably

going to be about identifying data that needs to be shared between SDN centric and OSS centric applications and ensuring this sharing is managed well.

It should also be noted that NFV complicates this picture still further. ETSI have defined a Management and Orchestration (MANO) component of the architecture that will manage the Virtual Functions Network Infrastructure (i.e. the compute, storage and network resources). However, the virtual network functions themselves must also have the full Fault, Configuration, Accounting, Performance and Security (FCAPS) management capability which may integrate with an existing OSS and/or an Orchestration function. This is an area that the TMF are looking at because managing it well will require new capabilities from the future OSS (see Section 11).

9.3. SDN and OSS Integration Strategies

The flexibility to define network services comes to the service provider at the cost of having to integrate an SDN controller environment both with the network devices and the OSS. Due to outsourcing of development functions to equipment and OSS vendors, many operators do not have large development teams that are well placed to take up this role. This leaves an operator looking to deploy SDN with the choice of how to integrate an SDN implementation. Because this is a complex problem many carriers are initially looking to SDN solutions that have minimal touchpoints with their existing OSS.

Components will be supplied by the network equipment vendor, SDN controller vendor and OSS vendor. Initially, solutions will be more tractable if they are supplied by a single source and equipment vendors are gearing up by acquiring SDN controller vendors to provide a turn-key solution in this space. This provides a direct challenge to OSS vendors who may see some of their professional services revenues displaced. However, the full promise of SDN will only be realised if the development of the SDN environment can be separated from that of the equipment vendors, leading to an equipment vendor independent ecosystem of network applications.

For this to happen both network operators and their SDN suppliers will need to build an integration capability. A likely path to this is for domain specific orchestration solutions to emerge that solve the integration problem in a smaller space. In due course this may expand to network wide, multi-domain solutions, although this is likely to take longer.

While SDN solutions tend to take a network view of services, effectively programming the network with interfaces like OpenFlow, it is also possible to take a more orchestration centric view of services by creating a new OSS/BSS with SDN like capabilities. This allows orchestration and network configuration using management like interfaces but with much more flexibility than a traditional OSS, this has been styled as a “real time OSS”. It allows the carrier to define and provision services in a flexible way, without needing wholesale network revolution. These

services then flow through to the network, the end result of which can be seen as offering a programmatic approach for service definition, creation, modification and deletion.

An example of such a solution can be seen in the early deployments of the Deutsche Telekom TeraStream concept (see Section 10). This evolves the OSS to become a model based entity, using service and network models based on YANG and then flowing these through to the network using NETCONF. While this is not “full SDN” it can provide service orchestration and can be integrated with SDN protocols if needed, for example, for service steering. In order for this approach to become widely applicable it will require considerable standards effort and vendor collaboration. This is because of the need for vendors to provide YANG models of their equipment, in the same way that they provided SNMP models. This is a large task, more so because YANG provides configuration capabilities and many router vendors did not offer these facilities in SNMP, preferring CLI or proprietary interfaces.

10. SDN Implementations in the Carrier Environment

This section looks at some examples of early SDN implementations and considers future carrier implementation strategies as they impact the various network domains. It considers how network equipment vendors are likely to react to the SDN and NFV challenge.

10.1. SDN Implementations Today

It is very early days for SDN or NFV implementation within carrier environments, although NFV is more advanced than SDN. Virtualisation of network services is in progress by mobile carriers in the SGi-LAN, and fixed carriers around the Broadband Network Gateway. There are some instances of virtual CPE being deployed for business services; there are cases of in-service trials of EPC virtualisation and of residential virtual CPE. It is definitely the case that almost all carriers are actively considering their SDN strategy, although there is a clear divergence in terms of how they see SDN and NFV impacting them.

In addition, some public statements have been made with respect to SDN that go beyond plans and aspirations to actual implementations. A brief overview of three of these deployments is provided here.

10.1.1. Deutsche Telekom TeraStream

Deutsche Telekom have announced their SDN centric architecture called TeraStream and have deployed this solution in a network in Croatia, Hrvatski Telekom, which currently supplies service to hundreds of customers. The TeraStream architecture has a number of innovations and utilises both SDN and NFV concepts. The solution design was described in a presentation at RIPE 67 [Ref 64].

The SDN component of the TeraStream solution is based on a YANG modelling approach, where service and network models are defined in YANG and converted to configuration using what Deutsche Telekom call a Real-time OSS. This configuration is pushed to the network using NETCONF, and OpenFlow is proposed as a possible future enhancement. A description of this solution and its rationale is provided in an audio slide presentation [Ref 65].

10.1.2. COLT

Colt have outlined a long term vision to evolve their network that incorporates both SDN and NFV as part of the solution. This architecture is primarily about optimising the network for cost efficient delivery of services by exploiting the capabilities of SDN and NFV [Ref 66]. As part of this deployment Colt have deployed a virtual CPE solution that replaces traditional layer 3 CPE in the

customer premises with a layer 2 CPE and a virtual layer 3 CPE in a network service platform. Details of the solution have been documented in a Heavy paper [Ref 67].

10.1.3. Google

Google have implemented an SDN solution based on OpenFlow to optimise traffic in their inter-data centre WAN, as described in detail in the report “B4: Experience with a Globally-Deployed Software Defined WAN” [Ref 18]. This is a production network carrying live traffic, and SDN combined with a traffic management application, has improved Google’s link utilisation by 2-3 times versus traditional carrier link utilisation of 30-40 percent.

It should be noted that in order to achieve this Google produced their own switch and made use of a large number of innovations not currently supported by SDN standards, including optimisations of the OpenFlow protocol. It is also true that the Google network and the nature of its traffic are particularly suited to an SDN traffic engineering solution, and that the impressive results achieved may not be universally applicable. However, there is no doubt that the Google reference shows that SDN can, in at least some topologies, offer significant benefits in link utilisation and hence reduce network costs.

10.2. Carrier Implementation Strategies

Section 4 set out at a high level the impacts of SDN and NFV on carrier networks, this section looks at the specifics of this strategy and what it is likely to mean for the low level network implementations.

10.2.1. Core Networks and the Interconnect

Network interconnect will continue as it is today based on IP/BGP with the possibility of MPLS interconnect where services require this. If SDN functionality is required in the core of the network then MPLS Segment Routing, PCE and possibly I2RS will be the easiest to implement. This is because these technologies represent incremental change to established, proven and understood core networking technologies and in some cases can be deployed alongside existing infrastructure.

Technologies that will drive SDN adoption in the core network are likely to be customer VPN automation (which can also be achieved without SDN via an automated OSS), bandwidth on demand, and service chaining where selective steering of flows are required. If all customer flows end up in a data centre then steering for service chaining can be carried out within the data centre infrastructure and the impact on core networks may be minimal. The replacement of large core routers with an NFV solution (with or without white-box hardware acceleration) is unlikely in

the foreseeable future. Similarly the replacement of these routers with low functionality OpenFlow controlled switches seems too disruptive for carriers to contemplate.

10.2.2. The Metro Service Node

Carriers will look to migrate at least some of their metro nodes to become more data centre like. Even in conservative carriers the Provider Edge (PE) router will change to become a service node, possibly as part of a metro hostel. In this environment, packet forwarding intensive processes are handled by the PE router but compute intensive services that today run on router service cards (or in the central processor) will move to commodity x86 hardware. The orchestration functions may be integrated with an end-to-end SDN network play, or may be confined to a metro node specific orchestration supported with an overlay networking solution and OpenStack integration.

Current x86 platforms continue to evolve to support increased I/O capabilities, removing bottlenecks within the bare metal server platform, but also within the virtual machines running on the platform. This means that over time smaller PE routers may move to be entirely virtualised, removing the need for some specialist routing equipment. It is not possible at this point to be definitive about the economics of this at various bandwidth or application requirements. However, it is clear that expensive hardware solutions offering throughput of a few tens of Gigabits per second may well move to entirely virtual solution sooner rather than later.

As Network Functions Virtualisation matures, larger IP Edge Nodes may be replaced with NFV solutions that incorporate white-box hardware acceleration. It is unclear how practical this will be in a complex multi-vendor environment, or whether the cost benefits will stack up. It may be single vendor NFV solutions are deployed that provide this capability (removing the integration risk), however, carriers to date have resisted such an approach seeing it as replacing one vendor proprietary solution with another.

10.2.3. The SGi-LAN and Telco Services in the Datacentre

Mobile operators will rapidly move to exploit NFV and service chaining within the SGi-LAN because of the complexity of their existing solutions and the benefits provided by a virtual solution supported by a flexible SDN based orchestration solution.

These services require micro-flows to be identified and steered within the SGi-LAN to the appropriate service platforms. The later versions of OpenFlow (version 1.4) provide a way to do that and support orders of magnitude more forwarding entry changes per second than traditional data centre solutions.

In addition to the SDN aspects of the SGi-LAN, there is a drive from the mobile operators to move to virtualisation of applications and services, as it assists in scaling. This is being done today by some mobile operators and is imminent for others. As ETSI NFV leads to performance improvements, the range of services that can be cost effectively virtualised will increase.

For both fixed and mobile operators there are a set of services that are provided to support their network that are compute intensive and not I/O intensive and these have either already been virtualised or will be virtualised. Examples include, virtualised DNS (which permits distribution and scaling improvements and may help the customer experience), call control services, Session Border Gateway and Session Router functions.

Mobile operators are deploying virtual EPCs to assist in scaling certain network deployments, including in one case to provide dedicated EPCs for individual corporate customers [Ref 68]. Some fixed operators are looking at a virtual BNG, although the packet processing requirements are challenging.

Some operators may look to distribute their data centre capability to the majority of their metro nodes. This will provide an opportunity to locate services close to customers, trading off the virtualisation penalty for the transport gains from distributing the service. For example there are benefits in distributing DNS services to reduce latency (and hence improve the customer experience).

10.2.4. The EPC and Mobile Backhaul Network

As previously described the EPC is relatively centralised within a mobile operators network and the traffic has to be aggregated and backhauled over the IP/Ethernet infrastructure between the eNodeB and the EPC.

The advent of small cells requires that the X2 interface between eNodeB be dynamically established between cells that determine they need to communicate (Automatic Neighbour Relations). There are some benefits to using a central controller to co-ordinate this, and this is a likely SDN application for the mobile backhaul network. Networks that make use of small cells and SON rather than Cloud RAN may benefit from using SDN to optimise the backhaul transport from a large number of femto and pico cells.

Where the topology justifies it, carriers may also look to deploy an SDN solution to optimise the transport within the backhaul and aggregation domain whilst still providing the end-to-end connectivity demanded by the EPC. This is a complex use case to implement and there may be limited benefits from doing so because of the constrained nature of access and backhaul. An alternative approach may be to replace a single EPC with multiple distributed EPCs running on a NFV infrastructure.

10.2.5. Cloud RAN, Wireless Access CPRI and NFV

Cloud RAN is fundamentally constrained by the nature of the CPRI interface which realistically requires abundant fibre to be cost effective as a solution. There are also significant challenges in virtualising it [Ref 22] which may also limit its applicability. However, where fibre is available, and if the virtualisation performance issues can be resolved, then mobile operators will deploy C-RAN on an NFV infrastructure. KT have already deployed such a service in Korea which they brand as LTE-WARP.

SDN and NFV have limited value to Wi-Fi access as mobile network Wi-Fi offload is best achieved under EPC control using the ANDSF capability. However, SDN may be used to optimise transport and for some Wi-Fi deployments may be used to steer traffic between interfaces to resolve technology limitations.

10.2.6. Fixed Access Networks

The access network is fundamentally Ethernet based for fixed carriers, with limited options for steering traffic flows. Therefore, although access network switching technology is quite suitable for SDN implementations such as OpenFlow, there does not seem to be a significant carrier push for this functionality. It may be that in some cases OpenFlow-like interfaces can assist in network partitioning, however, network slicing is currently not within the domain of the current ONF releases.

Virtual CPE solutions are already happening within the enterprise domain today, and may move to the residential domain, although opinion is divided amongst Service Providers. However, the virtual CPE will be transparent to the access domain and will be hosted in either the PE router or the data centre depending on the network model. Within the UK, ALA and by extension Generic Ethernet Access (GEA) can support his model of deployment should virtual CPE be used.

Future fixed access solutions (such as G.Fast and FTTdp) that seek to push active network components further into the network may benefit from SDN because it will allow the amount of processing required on the access node to be minimised, and can provide a solution for subtending from logical access nodes. It is fair to note that these technologies are some way from volume deployments, and the business case for doing so will need to be proven.

10.2.7. Optical Transport

Carrier networks employ a transport layer operating below the IP/MPLS layer. In the Core, optical networks include the flexibility to build a logical path without physically configuring the network nodes. This can be achieved either by using optical wavelength selective switches to build Reconfigurable Optical Add/Drop Multiplexor (ROADM) networks or by using OTN switching at the electrical layer.

Carriers may look to deploy SDN solutions to improve what is currently a very manual and time consuming multi-layer process of calculating the optimum mapping of IP/MPLS bearers to the optical transport layer. An SDN protocol such as PCEP or OpenFlow could be used to control the packet optical layer.

This is a complex, multi-domain area within the SDN environment and additionally has a significant organisational impact within carriers. This means changes here are likely to be evolutionary, possibly driven by tactical opportunities which can be deployed in a contained manner and with limited OSS/BSS interaction.

10.2.8. OSS and BSS

Where a carrier has either no OSS, or limited OSS, then they will look to use SDN technologies to automate their services. This may involve the use of SDN controllers, PCE, I2RS, OpenFlow and Segment Routing, or it may use more traditional management solutions such as NETCONF (which has the benefit of being easily scriptable). These services will be deployed on a case by case basis and initially for high touch, high value services where they do not impact on the existing OSS/BSS. Integration with the OSS and BSS will be a limiting factor on deployment speed and complexity.

Where a carrier has an established highly automated OSS then adoption of SDN to orchestrate services will be slower and limited initially to those services that have no impact on the existing OSS (they are either new services or they have never been supported by the OSS/BSS).

There is a view of SDN that suggests service orchestration will enable large amounts of the OSS to be replaced with a more automated hands off process. While this promises large OPEX savings, organisational issues and the complexity of the OSS/BSS will also make it hard to implement. This means that such SDN deployments will happen slowly and incrementally over a relatively long time period. In reality the network operators will target orchestration of their high value high touch services first and leave their low value (but high volume) low touch services on the existing OSS.

10.2.9. SDN Protocol Choices

While OpenFlow is often confused with SDN, the reality is it is one of many protocols that carriers may use to satisfy their vision for SDN and NFV. Solutions such as MPLS segment routing, NETCONF, PCEP and Extensible Messaging and Presence Protocol (XMPP) may also be used. The choice of protocol will depend on the application, its existing technology and scalability requirements.

For example, today the easiest solutions to implement are largely overlay solutions, because these avoid direct interaction with the underlying switch infrastructure and allow configuration of virtual switches and routers, either using OpenFlow, or customisable protocols such as XMPP and NETCONF. However, while overlays work well in constrained environments they have limited opportunities to optimise the use of the underlying switch infrastructure and long overlay tunnels do not scale well to WAN deployments.

In the core network, if traffic steering is required some sort of SDN control interface to the routers will be needed. The path of least resistance for operators in this area is likely to be MPLS Segment Routing, augmented with PCEP or possibly OpenFlow or NETCONF to control the classifier at the customer interface.

In the metro node, or SGi-LAN OpenFlow, overlay solutions and MPLS Segment routing are all viable options depending on what the carrier is seeking to achieve and their technology partners. For example, a carrier looking to break apart their routing infrastructure into white-boxes for hardware acceleration and an NFV control plane is likely to look at an OpenFlow solution for control of the white-box, while an operator seeking to sweat their existing routing asset by making it SDN capable may look at segment routing or vendor specific interfaces like XMPP.

In the optical transport and packet transport path computation and optimisation space, a carrier may choose an OpenFlow based solution or a PCEP based solution depending on their given preferences and their optical transport vendor’s capabilities. In Ethernet centric access networks if SDN capabilities are required then today OpenFlow is the logical choice.

10.2.10. Interfaces to Third Party Applications

The lack of progress in standardising these interfaces, suggests that carrier implementations will initially be proprietary and geared to their services and orchestration needs. However, if OpenDaylight is able to offer an easy path to third party service integration then the industry may adopt these interfaces as the defacto standard. There may also be a drive in the medium term by carriers to use application aware networking interfaces to improve their integration with CDN partners.

10.3. Vendor Implementation Strategies

SDN and NFV are both disruptive technologies as far as equipment vendors are concerned. However, within the carrier network changes are likely to be more incremental than in constrained network environments such as the data centre.

10.3.1. IP Router Vendors in Carrier Networks

To an extent the router vendors are reacting to SDN by developing service node solutions at the Provider Edge node, considering applications such as virtual CPE and introducing their own SDN controller architectures to configure the x86 servers and connectivity required in the service node. Router vendors are also looking at evolving their management interfaces to make them easier to integrate with orchestration solutions, providing APIs and SDKs to assist in this.

A key component of this for the vendors is the licencing strategy they adopt and vendors also seek to provide turnkey solutions based on their own SDN controllers (which may simply be supported versions of open source controllers). Juniper offer their own supported Contrail controller, but they provide the same codebase to the OpenContrail community. Cisco contributed their SDN controller codebase to OpenDaylight but also offer their own SDN controller which utilises components of the OpenDaylight Hydrogen release.

The router vendors today offering IP/MPLS solutions in the core network are likely to enhance their offerings to make them more SDN friendly, for example, with PCEP, Segment Routing and possibly in the future I2RS. Cisco are promoting Segment Routing and have also defined their application centric infrastructure concept for data centres complete with a virtual network edge. Alcatel Lucent have attacked the SDN space with their spin-in Nuage to provide a data centre solution.

If the IP Edge starts to become a target for virtualisation, either in whole or in part with attendant white-box hardware accelerators the major router vendors will not be left without options. They have the capability to aggressively discount hardware, thus reducing the CAPEX premium for a turn-key solution or they can look to provide virtual versions of their routers, possibly partnering with their own white-box vendor to offer a turn-key fully supported solution. While this may leave them vulnerable to carriers prepared to sacrifice OPEX for innovation and CAPEX reduction, it should be an attractive proposition for the more OPEX focussed carriers.

The merging of data centre networking concepts with carrier networking and the move towards virtualisation will also provide opportunities for less traditional carrier vendors to break into the carrier space. These are the data centre specialists with scalable support for protocols such as OpenFlow1.3. These vendors may find a niche in the telco cloud and the SGi-LAN.

10.3.2. Optical Transport and Packet Optical Transport vendors

The most significant impact on the optical transport vendors is likely to be around the use of SDN interfaces to allow the automation of path computation and defragmentation of the optical spectrum. In addition to their existing product sets this will require them to integrate with SDN controller functions, some of which they may provide to carriers to assist in the integration of their products with the network.

Vendors who support Packet Optical Transport capabilities will require more significant SDN capabilities than those offering optical transport only.

10.3.3. Mobile Network Vendor Impacts

Mobile vendor roadmaps in the access domain will be driven by the LTE standards roadmap, by small cell requirements and by C-RAN support. While SDN does not impact on their core capabilities there may be benefits in offering some degree of SDN and EPC integration, either to support service interfaces (for third party application integration) or to support transport network optimisation. C-RAN provides an early target for virtualisation, possibly with hardware acceleration and this is currently a key NFV use case.

Virtualisation of components such as the EPC are a key requirement in this market and vendors either support this or are moving to support it [Ref 69] and [Ref 70]. As part of this capability the key mobile vendors are also offering cloud capabilities so as to support SGi-LAN applications.

10.3.4. Fixed Access Network Vendors

Fixed access network vendors have the advantage that their equipment is fundamentally suited to OpenFlow interfaces being in most cases Ethernet based. However, it is hard to see specific applications for SDN in the access other than where they are driven to go by integration with any carrier orchestration functions. These vendors may, however, look to use SDN and NFV to minimise cost and power requirements for the next wave of deep fibre deployments such as FTTdp.

10.3.5. Network Application Vendors

Within any carrier network there are a large number of applications, for example, DNS, Voice and Multimedia call control platforms and CDN applications such as caches to name only a few. In general these vendors will look to support virtualisation efficiently in their products and to make them easy to integrate into an NFV environment.

The move towards more dynamic and flexible service chaining may also see increased opportunities for smaller innovative companies and start-ups to make carrier sales. This will be particularly true if carriers achieve their aims of reducing the long deployment times for new services as this delay is typically toxic to smaller innovative companies.

10.3.6. OSS/BSS Vendors

While SDN provides a solution for service orchestration and automation, it does not replace the OSS/BSS systems that a carrier has deployed because it does not support many of its functions. Element managers and Network managers will continue to be required by carriers. Furthermore innovations like NFV add further complexity to the problem of managing and assuring the network.

OSS/BSS vendors are likely to see significant opportunities within SDN and NFV, both integrating the existing OSS/BSS into solutions and supporting re-modelled OSS/BSS functions targeted at integrating with SDN and NFV orchestration solutions. There is some overlap and a large degree of interaction between SDN control and orchestration functions and the OSS. This has already been seen in the Deutsche Telekom TeraStream deployment (see Section 10.1.1).

10.3.7. Controller Vendors

The SDN controller market is a crowded space with open source and vendor specific solutions on offer. It is unclear at this stage how this will play out partly because the scope of an SDN controller function is very large, encompassing more than one south bound interface and potentially covering multiple network domains. It is unclear who will own the SDN controller and the degree of integration required for large SDN/NFV deployments.

In the short term, for tactical deployments of SDN and NFV it seems likely that the key network equipment vendor, for example, a router or mobile vendor offering a service node solution, will be well placed to provide their SDN control function as a turnkey solution to the carrier. It is too early to be certain how much traction OpenDaylight will gain in this space, however, there is some evidence that its capabilities will be leveraged by a number of controller vendors.

11. Related Projects and Initiatives

This report has focussed on the standards work of the ONF, the IETF and ETSI as these organisations are primarily leading the work on SDN and NFV. It should also be noted that from a mobile network perspective the work of 3GPP remains hugely important and that work has recently started within that organisation looking at some mobile use cases for SDN.

There are also a number of other projects that may impact SDN and NFV, in particular:

- The Open Compute project [Ref 71], which seeks to specify standard bare bones hardware for data centre infrastructure to enable hardware innovation around a low cost platform.
- The Open Grid Forum OGF [Ref 72] is an open community committed to driving the rapid evolution and adoption of applied distributed computing. As part of this activity the OGF has defined a Network Service Instance, currently at version 2.0. This permits OGF platforms to obtain connectivity from the underlying network. This interface is a candidate for a service provider to map it to an SDN NBI to permit the provision of network services for distributed computing.
- The TM Forum have started a program to look at orchestration, operations and management of SDN/NFV solutions which they have called ZOOM (Zero touch Orchestration Operations and Management). This work activity is likely to look at the orchestration management and operations that sit above the ETSI-NFV MANO function.

It is possible that as SDN and NFV are deployed other industry organisations and collaborations will be created to address specific niches and applications.

12. Timescale for SDN Deployments

It is very early in the SDN and NFV deployment cycle. Standards are nascent, and in some areas the work has not yet started. However, there remain a set of SDN and NFV capabilities that exist in the market, and have been deployed, in part because of the track record of SDN and virtualisation in data centres.

A speculative look at how this might play out, based on an understanding of the standards maturity, operator feedback and solution complexity is presented below:

- Current SDN and NFV solutions:
  - Single vendor point solutions, for example, using vendor SDK interfaces to deploy application centric software within the network.
  - Trials, proof of concept and limited deployments of SDN/NFV and C-RAN solutions.
  - Virtualisation of services in the mobile network SGi-LAN
- Short term (up to 2 years) :
  - NFV deployments for compute intensive network services, including DNS and EPC where this makes sense.
  - End-to-end orchestration using SDN for key services in single vendor networks, or for high touch high value services with limited OSS/BSS touch points.
  - Virtual CPE applications – enterprise and some residential (if this makes sense to the ISP).
  - Service Node infrastructure deployments in carrier metro nodes.
  - Service APIs with some automated network configuration and service chaining support for carrier VPN customers.
  - NFV deployments for smaller IP Edge service routers.
  - Service steering in core networks (if required) based on Segment Routing
- Medium term solutions (2-3 years):
  - New network deployments become SDN centric in their approach to management.
  - Service APIs for constrained and understood problems between carriers and their OTT providers and CDN partners.
  - C-RAN deployments where infrastructure allows.
- Long Term (4-5 years and beyond):
  - Service APIs for more complex services, for example, multicast enablement, service chaining APIs.
  - Multi-vendor, multi domain service orchestration solutions, SDN and NFV begin to be well integrated with OSS/BSS systems.
  - Integration of hardware acceleration functions for edge routing and flow classification into NFV solutions, if the business case supports it.

Appendix 1. PCEP and Multi-Domain Bandwidth Reservations

The PCEP solution, unlike many SDN type protocols has defined a rich set of capabilities for multi-domain and multi-carrier operations. An overview of the PCEP solution is provided here, it is of interest because other SDN solutions may need to evolve to provide similar functionality.

Where the end-to-end path crosses multiple domains the PCE making the path calculation will have limited knowledge of the end-to-end path. In this case the PCE will return the path within its domain and select the exit point to the next domain, the path request can then be handled autonomously by the next domain, which may or may not use PCE to reserve paths. However, this approach is limited to the extent that the next domain may be unable to fulfil the request owing to bandwidth or other constraints, which leads to a number of crankback scenarios whereby the egress LER may select another domain to reach the ultimate destination or conceivably drop back to the originating LER which must make another request to the PCE excluding the failed path.

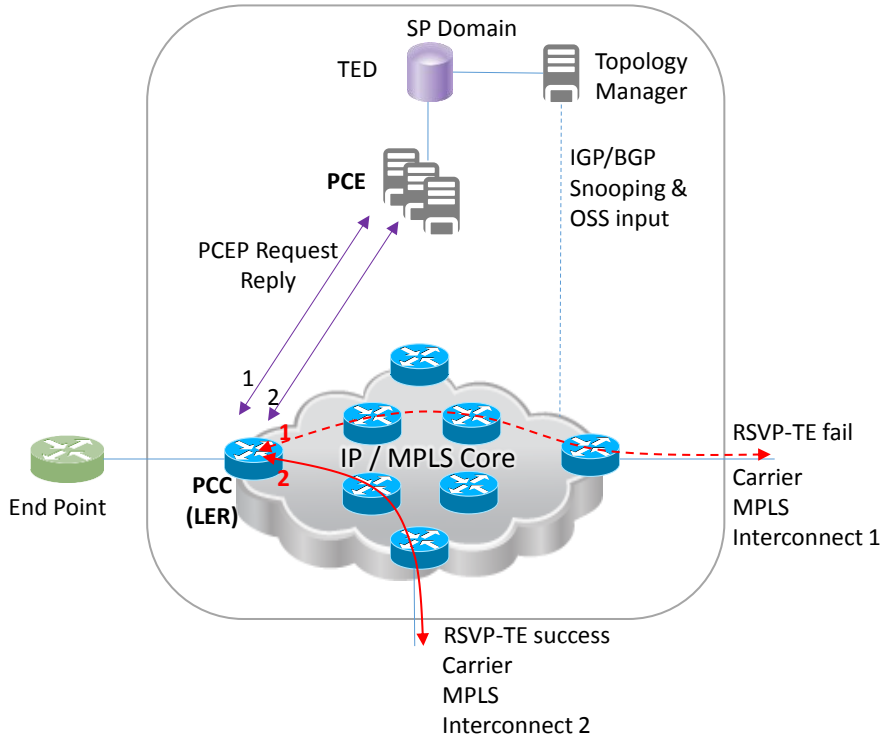

Figure A1 Multi Domain Setup with Crankback

This crankback approach is considered sub optimal and PCE peering can help reduce this overhead by permitting a PCE to request a path computation from a cooperating PCE in the neighbouring domain. This is repeated through the network until the domain which includes the ultimate destination of the path is reached. This may result in a failed path calculation, however,

the originating PCE can then re-attempt the reservation by asking another PCE that is responsible for another domain without requiring the RSVP-TE signalling in the network. This architecture is shown in Figure A2.

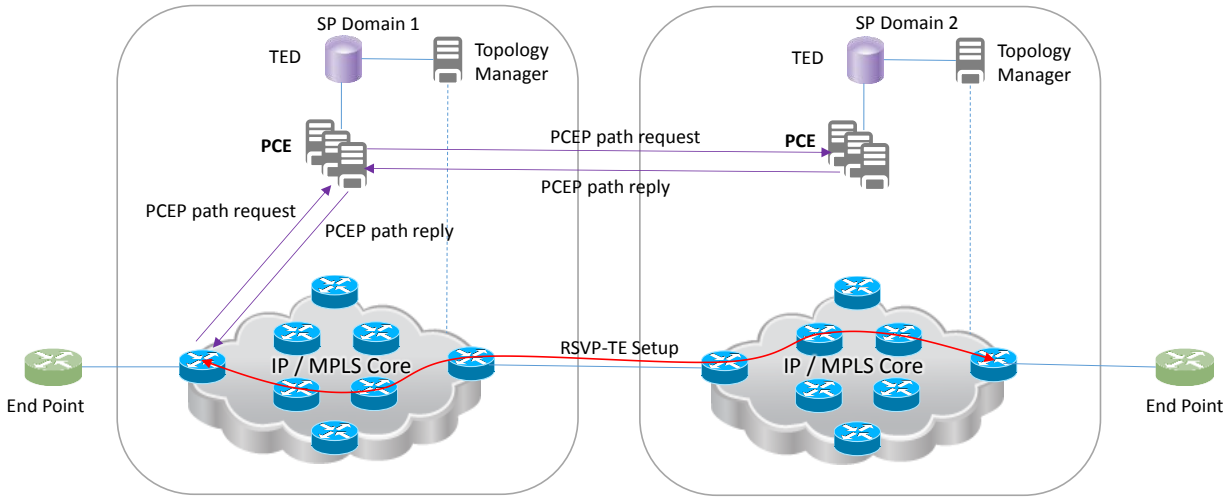

Figure A2 Multi Domain Setup with PCE Peering

This approach has the advantage that there is far less chance of the MPLS LSP setups failing which reduces the signalling load on the underlying network. However, one issue with this approach is that it may chose less optimal paths because each PCE may only have a limited view of the end-to-end route and path calculation failures may lead to non-optimal paths being selected. This occurs when one PCE selects its view of the best egress from its domain (which is the ingress to the next domain, i.e. the interconnect node). However, within the adjacent domain better paths would have been available from one of the alternative interconnect nodes.

This scenario is shown in Figure A3.

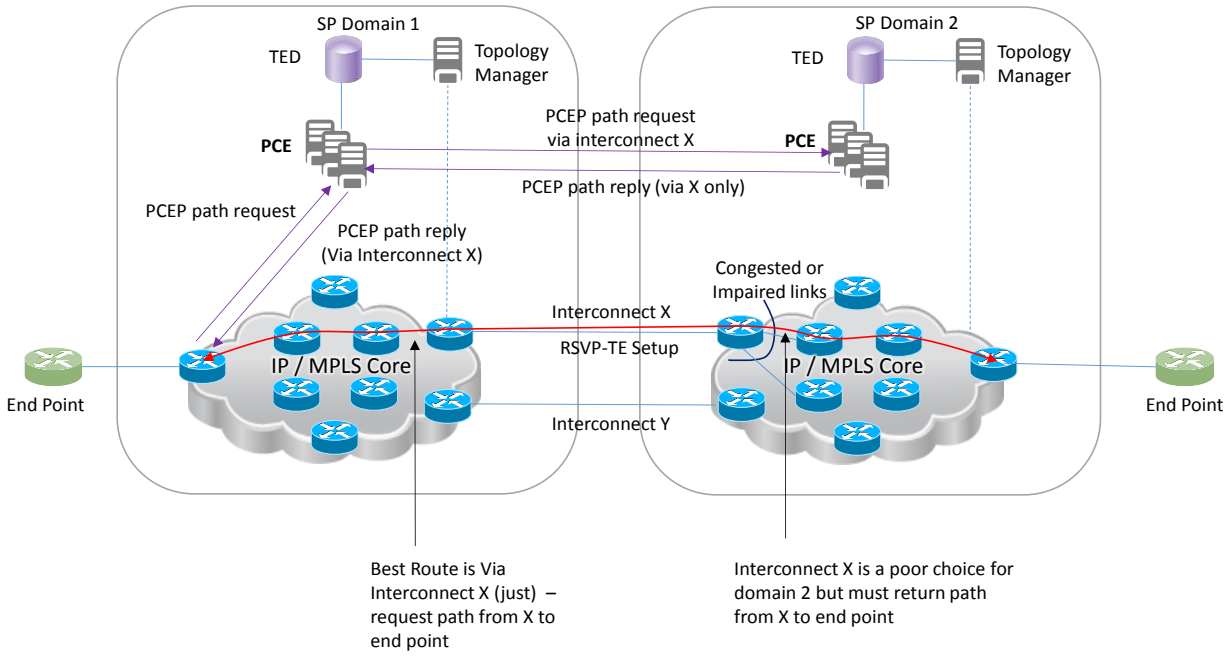

Figure A3 PCE Multi Domain Path Request with Poor Interconnect Decision

To overcome this limitation the PCE working group has created an alternative solution which makes use of a backwards path computation known as a Backwards Recursive PCE Based Computation (BRPC) which is defined in “RFC 5441 A Backward-Recursive PCE-Based Computation (BRPC) Procedure to Compute Shortest Constrained Inter-Domain Traffic Engineering Label Switched Paths” [Ref 73]. In this solution the originating PCE is responsible for selecting the domains to be used to support the reservation (typically based on knowledge of the inter-domain routing and policy). However, no path selection is made within the chosen domains, instead the request is forwarded through a number of PCEs until it reaches the PCE responsible for the destination domain. This then calculates a tree of the shortest paths from the ultimate destination node to the adjacent domain that forwarded to PCE request. This path computation is then passed to the adjacent domain which adds to it, calculating the shortest paths between one or more interconnect points from the ultimate destination domain to each interconnect point with the domain that forwarded it the PCE request. Eventually this calculation will reach the originating PCE which is able to select the optimum path.

This mechanism is shown in Figure A4.

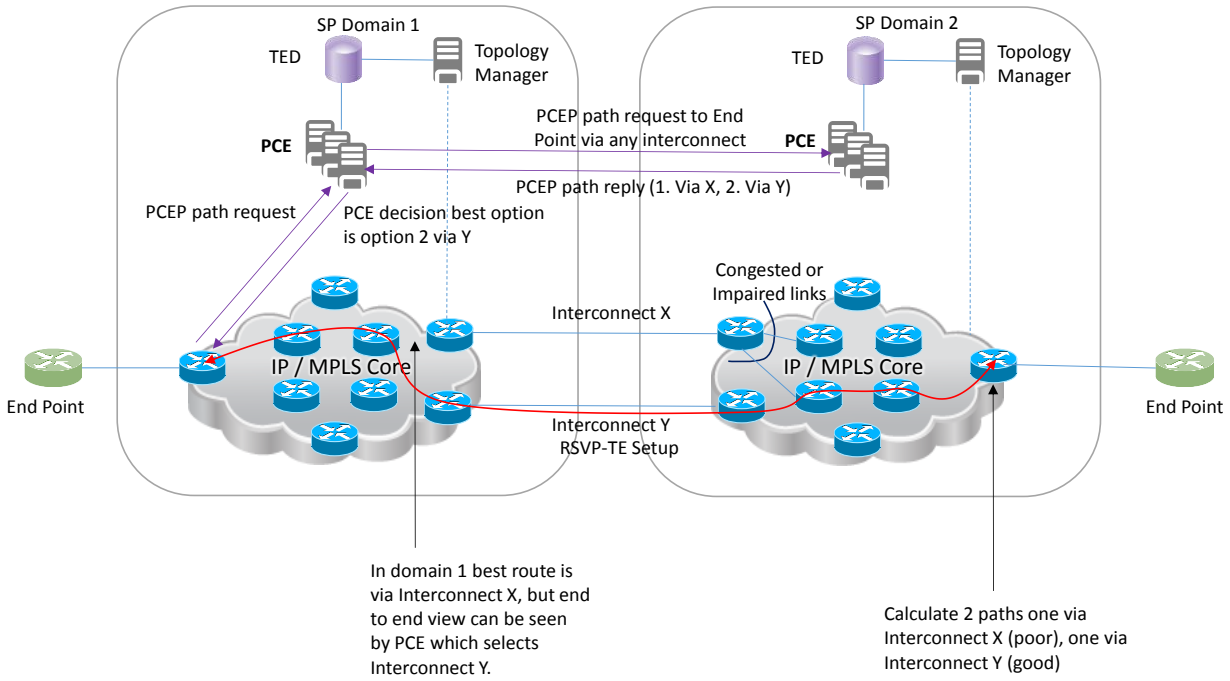

Figure A4 PCE Multi Domain Path Request with Backwards Recursive Computation

This approach to path computation still does not guarantee that the best domains have been chosen to support the reservation, possibly because the originating PCE which made the selection is not in possession of information about the routing, performance and load of the adjacent domains. Therefore, PCE has proposed another solution to overcome this limitation which is the use of PCE hierarchies with parent PCE's responsible for calculating the end-to-end path and child PCEs responsible for path calculations within a domain. This mechanism is described in "RFC 6805 The Application of the Path Computation Element Architecture to the Determination of a Sequence of Domains in MPLS and GMPLS" [Ref 74] and allows the originating PCE to select a path from a set of calculated options that may span entirely different domains in reaching the destination, this approach has limitations on scalability in that if a very large set of domains are traversed the calculation becomes onerous.

It should be noted that PCE is primarily about supporting the calculation of reservation paths in MPLS networks and while these networks are multi-domain the span of MPLS-TE reservations is rather more constrained than the span of domains traversed by internet traffic. This means that path computations may not need the full complexity of hierarchical multi-domain path computations and indeed in many cases a simple domain selection by the originating PCE may suffice.

Contact
Fujitsu Telecommunications Europe Limited
Address: Solihull Parkway, Birmingham Business Park, Birmingham, B37 7YU. UK
Phone: +44 (0) 121 717 6000
E-mail: telecommunications@uk.fujitsu.com
Website: www.uk.fujitsu.com