ngmn

the engine of broadband wireless innovation

A White Paper by the NGMN Alliance

LTE Backhauling Deployment Scenarios

next generation mobile networks

ngmn

LTE backhauling deployment scenarios

by NGMN Alliance

Version:	**1.4.2 FINAL**
Date:	**3rd July 2011**
Document Type:	**Final Deliverable (approved)**
Confidentiality Class:	**P**
Authorised Recipients:	**N/A**

Project:	**P-OSB: Optimized Backhaul**
Editor / Submitter:	Miguel Angel Alvarez, Frederic Jounay, Tamas Major, Paolo Volpato
Contributors:	**NGMN Optimised Backhaul Project Group**
Approved by / Date:	**BOARD July 3, 2011**

Abstract

With the introduction of LTE operators need to look at how the backhauling network, the network domain that connects evolved NodeBs (eNBs) to MME and S/P-GW, is capable of adapting to the new requirements, namely the adoption of a packet infrastructure, without disrupting the existing services.

This paper introduces some reference architectures, moving from a pure layer 2 topology to a full layer 3 one, discussing some elements to be considered in the design process of a network. The purpose of this is to support operators in their migration from current architectures to new, packet-based backhaul networks.

Since the migration phase might pose concerns to operators still engaged in 2G/3G deployment or in maximizing the profitability of their existing networks, the scenarios described hereafter have been designed considering, among the other aspects, possible paths to migrate from circuit based network, and represent a kind of target architecture to aim at. Clearly, the path to an all packet-based backhaul will depend on the specific market, technical environment and services an operator is operating or dealing with.

Although this paper primarily focuses on LTE backhauling, some advanced topics are also referenced and constitute the basis for further studies on LTE-A.

Table of Contents

1. Introduction

The goal of this paper is to describe how the mobile backhauling network will evolve to support the deployment of LTE.

1.1. NGMN TWG P11 - P-OSB Scope

The Optimized Solutions for Backhaul and Meshed Networks (P-OSB) project aims to define requirements and to assess innovative all-IP transport solutions for facilitating optimum backhauling (including self-backhauling).

1.2. What this paper is and why it is in line with P-OBS

This paper addresses the logical topologies that can be deployed on top of the connectivity scenarios described in [2].

2. Definitions and abbreviations

Abis	Logical interface between 2G BTS and BSC	**PDH**	Plesiochronous Digital Hierarchy
ATM	Asynchronous Transfer Mode	**POS**	Packet Over Sonet
BGP	Border Gateway Protocol	**PPP**	Point to Point Protocol
CAC	Call Admission Control	**QoS**	Quality of Service
CE	Customer Edge	**S1**	Logical interface between LTE BTS and packet core
CPE	Customer Premises Equipment	**SDH**	Synchronous Digital Hierarchy
CSG	Cell Site Gateway	**SGSN**	Serving GPRS Support Nodes
DSCP	Differentiated Service Code Point	**TDM**	Time division Multiplex
EPC	Evolved Packet Core	**TE**	Traffic Engineering
GGSN	Gateway GPRS Support Node	**UMTS**	Universal Mobile Telecommunication Service
GPRS	General Packet Radio Service	**VC**	Virtual Circuit
GW	Gateway	**VLAN**	Virtual LAN
HSPA	High Speed Packet Access	**VPLS**	Virtual Private LAN Service
Iub	Logical interface between 3G BTS and RNC	**VPN**	Virtual Private Network
LSP	Label Switched Path	**VRF**	Virtual Routing and Forwarding
LTE	Long Term Evolution	**VSI**	Virtual Switching Instance
MPLS	Multi Protocol Label Switching	**X2**	Logical interface between LTE BTS
MASG	Mobile Aggregation Site Gateway		
OSPF	Open Shortest Path First		
P	Provider (Router)		
PE	Provider Edge (Router)		
PHB	Per Hop Behaviour		

3. Framework and terminology

A backhaul network serves as the transport medium for a mobile Radio Access Network (RAN) and connects the base stations to their relevant controllers. The term “controller” is used in the context of this document as a representation of the complete EPC (Evolved Packet Core) including MME and S/P-GW in case of LTE, and the controllers of other radio technologies like RNC in case of 3G and BSC in case of 2G.

In essence, a typical network built for mobile backhaul consists of three domains: Core, Aggregation and Access. The domain borders are mostly defined by the technology and topology used within the domain and the deployed radio nodes.

The access network provides the connectivity to the BTS at the cell sites and is predominantly based on tree and chain topologies built with microwave radios, but also with a good share of fiber and copper usage.

Starting from the aggregation network we see very often ring and mesh topologies, mostly on top of an optical network flavor. The aggregation network is normally terminated at the controller site, where RNCs and BSCs are mostly located.

The controller sites are connected to other controller sites and the packet core as well as the EPC (Evolved Packet Core) via the core network, which is nearly in all cases an IP/MPLS routed network.

This structure is represented in the following picture.

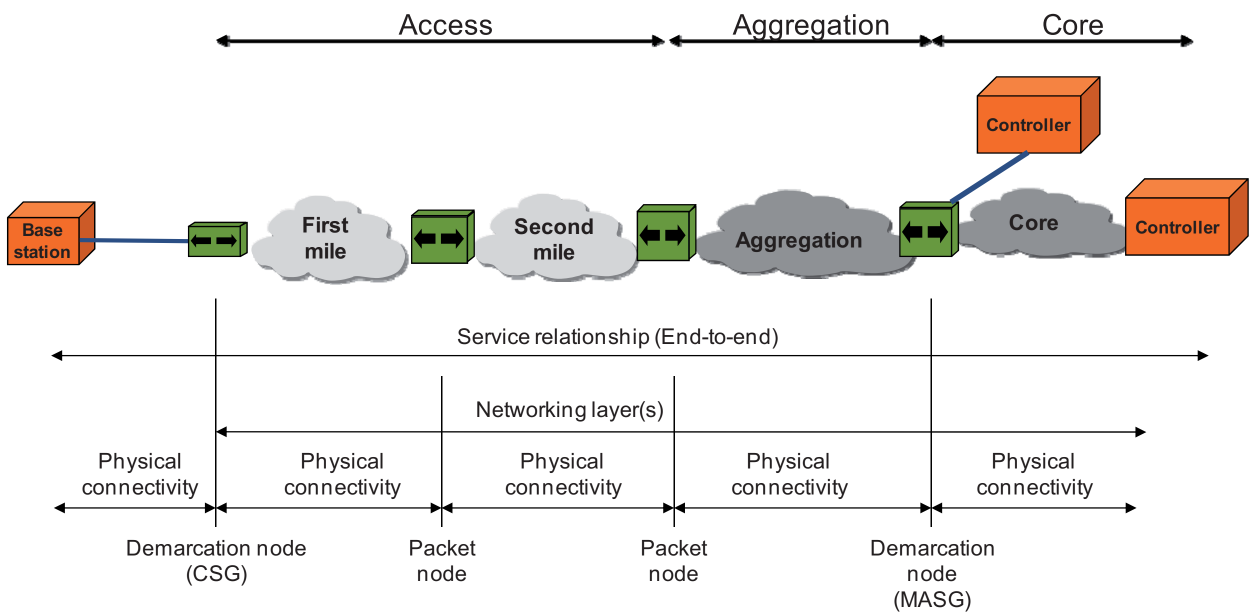


Figure 1: Basic Structure of a Mobile Backhaul Network

For the scope of this paper, the backhaul network will be limited to only two network domains: access and aggregation.

The reason why access may be composed of several sub-domains (first mile, second mile, etc.) is to consider different physical technologies and topologies. Moving left to right, the first mile (first hop) connects a demarcation device, usually deployed at the cell site, to a first stage of traffic grooming and concentration. The second mile, in turn, further aggregates traffic, adapts any technology change and provides the hand-over point to a metro/aggregation network.

Another demarcation device exists at the right border of the aggregation domain, connecting the backhaul network directly to a RAN controller or to the network core.

The list of nodes that are part of a backhaul network then includes:

- a Cell Site Gateway (CSG, also referred to as Cell Site Aggregator, or Demarcation device), usually deployed at a cell site, which is the first network node where the logical architectures described hereafter apply
- some packet nodes belonging either to access or aggregation
- a Mobile Aggregation Site Gateway (MASG) which acts as a counterpart of the CSG.

The term “physical connectivity” is used to represent whatever technology can be used to connect nodes, as explained later on.
On top of the physical layer a networking layer can be found. This is the focus of the present analysis; again the term is wide enough to embrace all of the possible logical architectures needed to steer LTE traffic and applications.
The highest layer is represented by the service, where this applies to the S1 and X2 interfaces. Even if not explicitly mentioned, the transport of S1 and X2 relies on an IP stratum which is not part of networking.

3.1. HSPA+/LTE/4G requirements for backhauling

The technical requirements of a backhaul network have been derived either from 3GPP specifications, the primary reference for HSPA+ and LTE, and other industry/normative bodies’ specifications (IETF, Metro Ethernet Forum, DSL Forum, ITU, etc.).

At a very high level, the basic requirement on a backhaul network is to support LTE, HSPA+, and in general 4G transport, but for the scope of this analysis it can be summarized into the following points, which are not necessarily always supported by current networks:

- The backhaul network is packet based
- Provides high bandwidth
- Network nodes are characterized by high capacity interfaces and perform QoS aware traffic aggregation
- Enables end-to-end Operation, Administration & Maintenance (OAM)
- Possibly has a lower TCO (total cost of ownership) than traditional TDM or hybrid (TDM and Ethernet) networks
- Supports the networking models and transport services as defined by MEF, BBF, IETF and any other relevant industry organizations.

The majority of the LTE backhaul traffic follows still the traditional hub-and-spoke architecture, i.e. eNBs send their S1 traffic towards the core network via a common peering point.

LTE introduces a new logical interface for BTS to BTS communication called X2, which was not existing (and also not needed) with earlier 2G and 3G systems. Its main usage is in supporting the handover process when a terminal is changing from one BTS to another.

The logical connectivity for the X2 traffic can be provided at various points in the backhaul network

At a first glance, it seems obvious that it would be beneficial if the X2 “turning point” would be located close to the base stations, allowing to benefit from low X2 latency and avoiding that X2 traffic will load higher parts of the Mobile Backhaul Network.

However keeping the X2 latency significantly lower than the radio link interruption time of 30 .. 50 ms during handover does not add any value. As in a well designed network the S1 transport path is anyhow optimized for low latency, it mostly does not cause any harm to provide the X2 connectivity at a higher point in the network. Furthermore, the amount of X2 traffic is marginal compared to S1 traffic, so the additional load is negligible.

3.2. Evolving from current backhauling: main issues

The introduction of LTE might pose some concerns to operators still engaged in 2G/3G deployment or in maximizing the profitability of their existing networks. For this reason, the scenarios described hereafter have been designed considering, among the other aspects, the shift from a more “traditional” network (e.g. circuit based) and represent a kind of target architecture to aim at. Clearly, the path to an all-packet based backhauling will depend on the specific market, technical environment and services an operator is operating or dealing with.

Without the aim of being exhaustive, current backhaul networks supporting 2G/3G services are mostly based on legacy technologies (TDM/ATM). In general, 2G Abis is carried on TDM, while 3G Iub transport relies on ATM over TDM. Physical technologies may include PDH and/or SDH.

One first approach to tackle the move to a packet backhaul is the realization of a dedicated network for HSPA+/LTE, whilst maintaining the existing network for current services. The parallel networks’ approach leaves an operator the flexibility of gradually introducing packet-based technologies in certain segments of the networks and selecting, when needed, the preferred method to handle legacy services. For example, 2G/3G data services can be carried in their native form or can be offloaded to the new Ethernet network (e.g. for HSDPA).
In selecting such an approach, scenarios based on Ethernet (please see 5.1) are likely to simplify the interconnection of existing network domains and support the typical hub & spoke logical topology between RAN controllers or EPC components and base stations. A high level schematic is represented into the next picture.

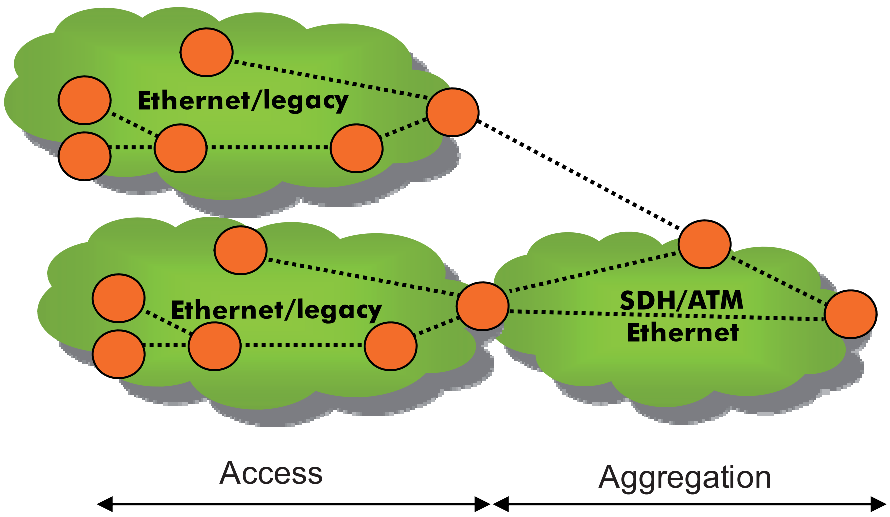


Figure 2: High-level representation of a circuit-based network

A different approach might consider the adoption of Ethernet as the common backhaul technology, from the cell site to the aggregation, used across only one network. The main impact is the upgrade to Ethernet on every base station site and network element, even if Ethernet and legacy transport can coexist in the access domain (hybrid approach). Legacy services are mapped onto the Ethernet layer using pseudowires or circuit emulation techniques and encapsulated into e.g. VLANs. The aggregation domain could still employ SDH, bringing an Ethernet over SDH transport. The typical topology is still hub & spoke, as seen into the next picture, and reference scenarios could be 5.1 or 5.3.

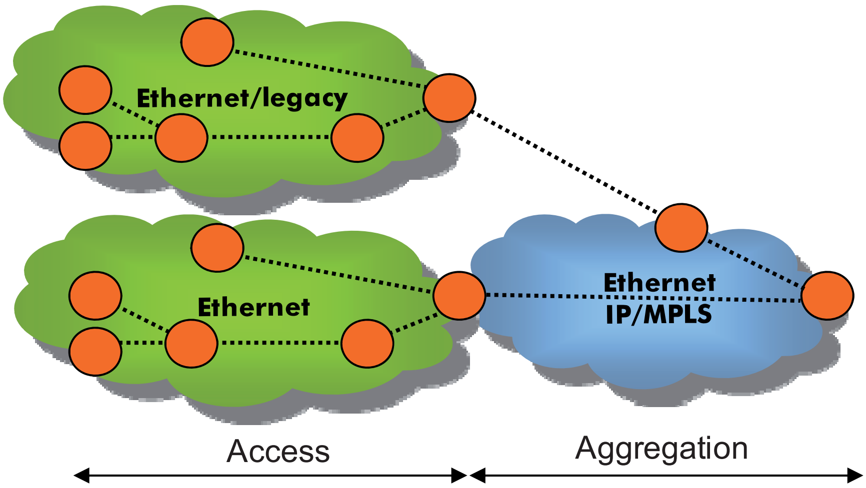


Figure 3: High-level representation of a mixed circuit-based and packet-based network

One last approach foresees the deployment of an MPLS-based VPN spanning from cell sites to RAN controllers or EPC components, either at layer 2 or 3. Ethernet may remain the underlying transport technology but other solutions are possible (e.g. SDH, WDM for the aggregation, GPON, dark fiber, microwave for the access).
Cell site gateway equipment is distributed at the cell sites and services are encapsulated as pseudowire or circuit emulation. The supported topologies include hub & spoke, mesh and ring.
The overall architecture is represented in the next picture and can be considered by scenarios from 5.4 onwards.

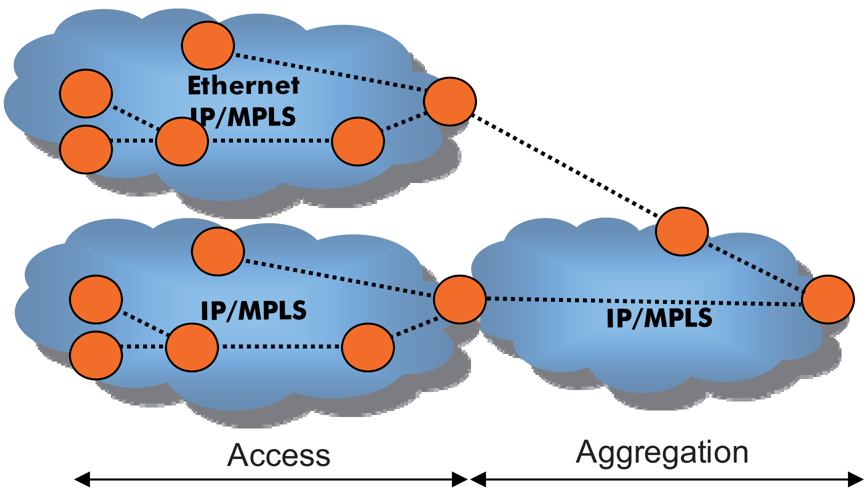


Figure 4: High-level representation of a packet-based network

As said, the approaches can be seen as different alternatives or different steps in the move to packet-based backhauling. Specifically the last one is often seen as the last to arrive on the market and to be adopted by carriers.

3.3. Gluing the organic view and the logical view

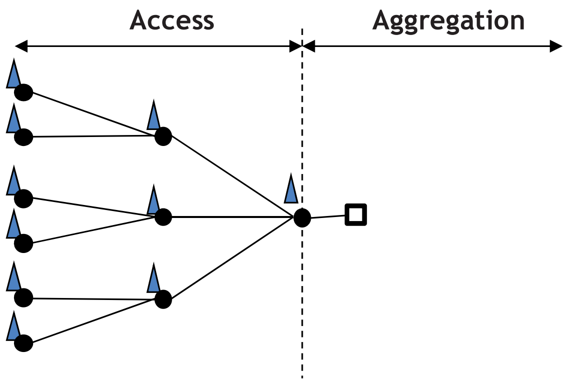
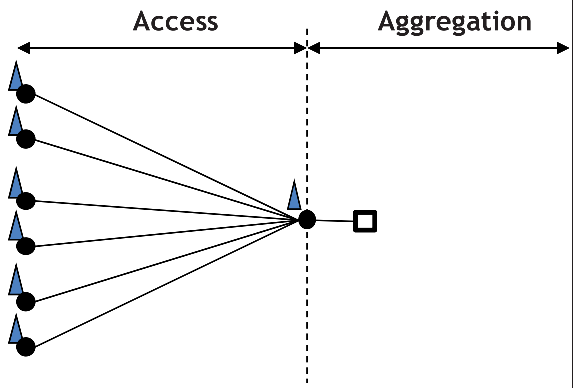
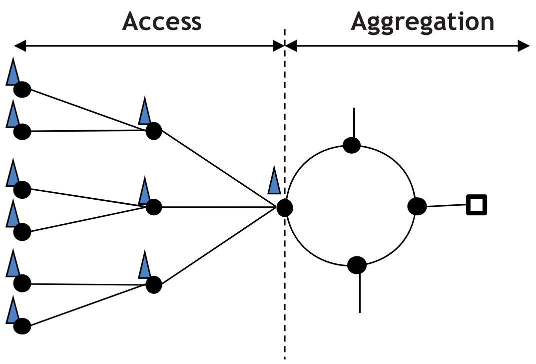
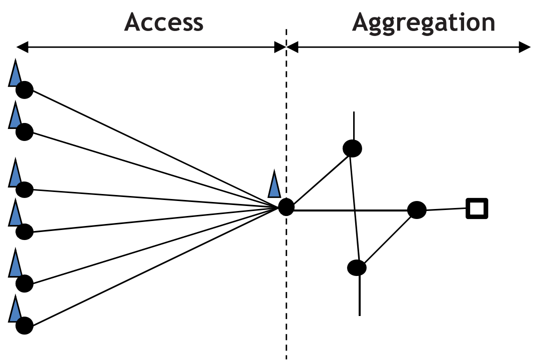
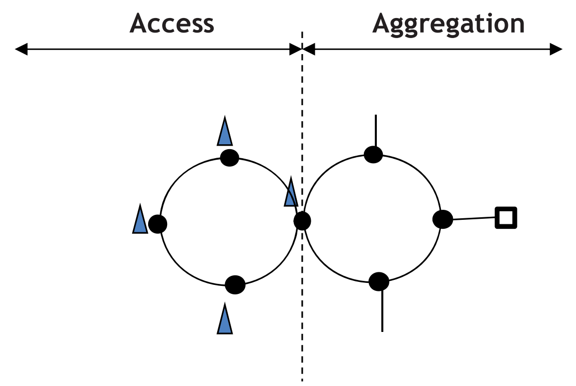
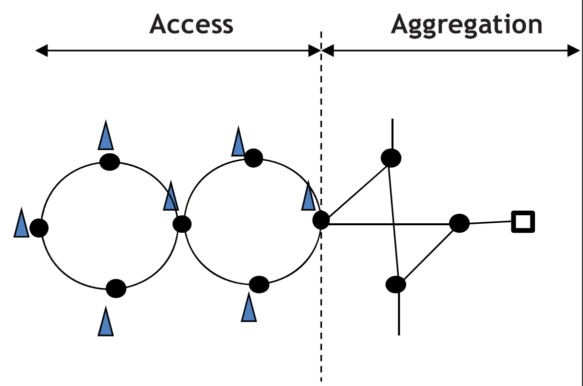
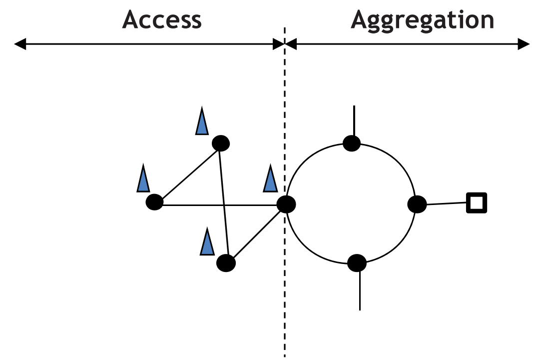
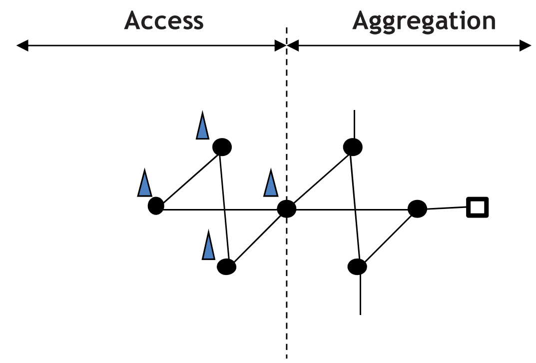
Backhauling has been studied from a physical standpoint in [1]. The main technologies included in that analysis are listed here for reference:

- Microwave point-to-point
- Microwave point-to-multipoint
- DSL
- GPON
- Ethernet Leased Line
- Fiber point-to-point
- Ring or mesh - Ethernet, NG-SDH, (D)WDM.

Depending on the physical transmission technologies Service Providers have deployed in the field and how they are combined, a few topologies are possible for a backhaul network. This analysis has focused on the following cases, considered as general combinations of access and aggregation topologies:

Case	Access	Aggregation	Examples
1	Tree	No aggregation	Point-to-point or point-to-multipoint fiber or microwave connections groomed by a packet node in front of RAN controllers
2	Tree	Mesh/Ring	Point-to-point or point-to-multipoint fiber or microwave connections with aggregation by a metro Ethernet or SDH network
3	Ring	Mesh/Ring	Fiber or microwave based access rings, with metro Ethernet or SDH aggregation
4	Mesh	Mesh/Ring	Fiber or microwave based mesh in access, with metro Ethernet or SDH aggregation

To better visualize how a backhaul network is shaped the next table provides a few examples of topologies.

Case	Example 1	Example 2
1		
2		
3		
4		
Legenda:	● **Packet node** — **Backhaul link**	▲ **eNB site** ☐ **Controller**

Although high level, the table gives a first hint on the characteristics of topologies. These characteristics will also be considered later on to determine what logical architectures can be applied to every case:

- Case 1 is characterized by direct connectivity with no or little path diversity for redundancy. Protection tends to be at the transmission layer, posing less stringent requirements on the logical architecture to be adopted;
- Case 2 limits the topology described by case 1 to the access, while a ring or mesh infrastructure is considered in the aggregation, for a denser grooming of traffic. The same consideration made for case 1 applies to the access, while the presence of a ring or even a mesh in the aggregation suggests considering architectures supporting fast detection and reaction time;
- Case 3 and case 4 further increase the complexity of backhaul networks: the difference between the two is how the access domain is shaped (ring for case 3 and mesh for case 4, where a ring is seen as collapsed mesh). Depending of Service Providers' preference, several architectures are possible, all of them generally based on MPLS.

Please note that the nodes at the border between two domains (and providing the connection between them), e.g.: between access and aggregation, are typically configured in a redundant manner for high availability.

3.4. Guidelines followed to define a logical scenario

The physical and topological aspects of access and aggregation described earlier can pose some requirements on the definition of logical architectures.

At the same time, other factors may determine an impact on that. Some of them have been already mentioned in the previous paragraph, some depend on local preferences or guidelines. In general we have:

- LTE traffic flows steering (from eNBs to MME and S/P-GW vs. from eNBs to eNBs)
- Underlying technology
- Need for physical or logical protection
- Constraints from the environment (e.g. radio based transport vs. fiber).

Then the following criteria have been identified for mapping topologies to functional architectures:

- Forwarding technology
- Control plane usage for protection
- Support of end-to-end OAM
- Preference of availability of end-to-end services (MEF based, L2VPN, L3VPN, etc.).

4. RAN Configuration

Most base stations support a flexible way to bind eNB applications (S1/X2 U-plane, S1/X2 C-plane, M-plane, S-plane) arbitrarily to either

- eNB interface address(es) or
- eNB virtual (loopback) address(es).

This flexibility allows base stations to be configured according to the transport services offered by the backhaul network, but also applying traffic separation (e.g. M-plane from U/C-plane traffic) as needed.

eNB interface IP address(es) can be assigned either to

- one or more physical interface(s) or
- one or more logical interface(s).

A physical interface is typically provided by an Ethernet port, whereas a logical interface is provided by a VLAN termination. Different interfaces as well as VLANs belong to different IP subnets.

There are many configurations possible, but for the sake of simplicity only two exemplary configurations will be shown:

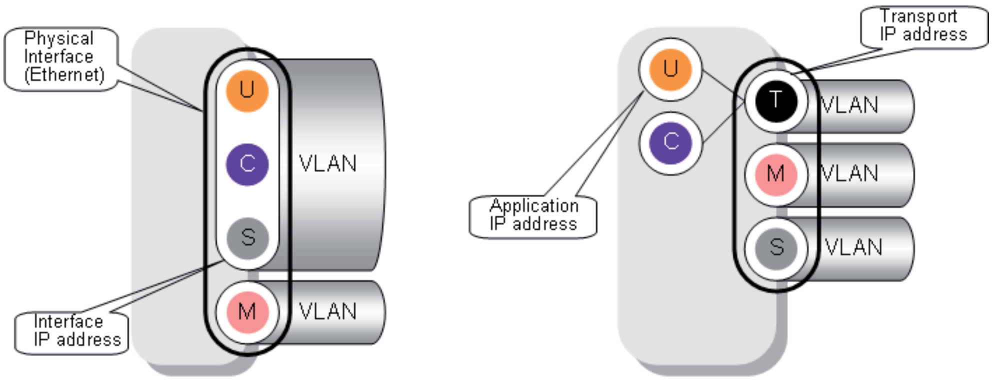


Figure 5: Example IP configurations of eNB

In the left example one IP address is used for terminating control, user and synchronization plane traffic and a second one solely for management plane traffic. As both IP addresses are running over different logical interfaces created by two VLANs, the addresses have to belong to different IP subnets.
In the right example separate logical interfaces (VLAN) and IP addresses are used for the management and synchronization plane. User and control plane traffic are terminated on individual virtual (also called loopback) addresses, which can be reached via a dedicated transport IP address. In most cases such configurations in the eNB are created by using BTS-internal routing functionality.
For both examples it has been assumed that IEEE1588 is used for synchronization purposes, but if this is not the case the S-plane termination point becomes obsolete. Also only a single Ethernet interface on the eNB has been considered, but also configurations with multiple Ethernet interfaces are possible.

In case IPSec is used then the configurations are typically done by using IPSec Tunnel mode. The IP address for IPsec tunnel termination (interface IP address) may be different from the IP addresses which eNB U/C/M/S-plane applications are bound to (virtual IP addresses). Configuration and usage in the network would be similar to the case depicted in the right side of Figure 5.

Also other configurations can be foreseen: If for example the backhaul network is offering different transport services for meshed X2 and hub-and-spoke S1 traffic, then a configuration with S1 U/C plane on one logical interface and X2 U/C plane on another logical interface would be very reasonable.

4.1. MPLS in the eNB

Some scenarios described in chapter 5 of this document are based on MPLS and/or MPLS-TP in the backhaul network, and in some scenarios even down to the cell site. The question coming immediately to mind is whether it would make sense to extend in those cases the MPLS layer into the eNB itself.

From a concept perspective, this would be the equivalent of moving the demarcation device at the cell site, also called Cell Site Gateway (CSG), into the eNB itself. The logical interfaces, as described in the previous chapter, would be e.g. IP carried over an MPLS LSP.

3GPP has specified the S1 and X2 protocols to run over IP, but without being specific on the data link layer technology to be used. They have indicated that suitable options are Ethernet and PPP.

Having this in mind, the usage of another networking layer below IP in the eNB – like MPLS – would not be in contradiction to 3GPP standards.

The benefit of such an integration of MPLS into the eNB would be mainly a simplification of the network architecture and a reduction of the required footprint at the cell site by making the CSG obsolete. It would also help to improve the operation of the network as it would allow direct access to the MPLS OAM functionality as well as the performance measurements within the BTS.

On the other hand there are certain disadvantages, which should be also considered: By basically moving the CSG into the eNB, the interface between radio and transport equipment would turn into an NNI, hence there would be no clear demarcation anymore between the radio and transport domain. Also the operational complexity will be increased in case there is a separation between transport and radio department within the operator's organization. The main concern with such integration would be on the interoperability between the eNB and the transport equipment, which would become more complex than with a plain, simple and well defined IP/Ethernet interface.

We can conclude that there are several reasons which speak against and in favor of an integration of MPLS into the eNB, and the operator has to decide whether the benefit of the footprint reduction at the cell site is worth the extra effort.

5. LTE-ready backhauling scenarios

This chapter introduces a few scenarios that have been recognized as the most probable or interesting ones during the analysis activity. They comprise a L2-oriented architecture up to a full L3 one, with several steps in between.

5.1. Technology

For the sake of simplicity all scenarios have been defined only on top of Ethernet (IEEE 802.3), as it is expected to be the dominant transport technology in future. Other technologies can be considered as well, and at the end of section 5.2.2 an example with DWDM is given. The use of Ethernet interfaces has been also assumed for all base station and controller types. With LTE this is anyhow the only defined transport interfaces and more and more 3G as well as 2G systems are moving towards Ethernet connectivity.

Another point worth mentioning is the way MPLS-TP and IP/MPLS are considered. Both have their own applicability in the scenarios presented hereafter, each with its own specificity.

Whilst, in theory, a lot of protocol combinations are possible, from a practical point of view IP/MPLS can be used for implementing both L2 and L3 VPNs. Often they can be found in the aggregation domain but nothing prevents their adoption even in the access.

MPLS-TP has its applicability for point-to-point transport services, suitable in access and for those cases where a point-to-point L2 VPN (VPWS) can be extended also into the aggregation.

5.2. Scenario 1 – Carrier Ethernet

The first scenario is characterized by Ethernet as the service layer that carries S1 and X2 traffic on top of any transport network used either in access and aggregation. Scenario 1 is represented in the next picture.

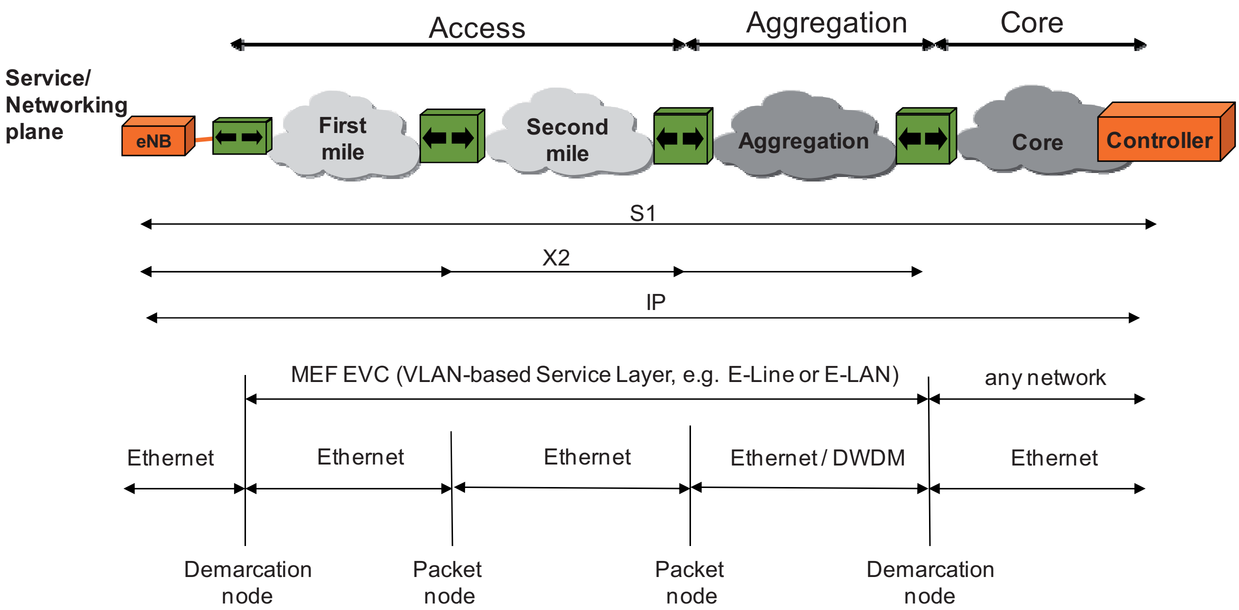


Figure 6: Backhaul Scenario based on Carrier Ethernet

The traffic steering is based upon VLAN, defining Ethernet Virtual Connections between eNBs and MME or S/P-GW. The service layer might rely on any of MEF's models (E-Line, E-LAN, E-Tree), as appropriate.[1]

While there is no doubt the S1 interface spans from an eNB to EPC components, the X2 interface can be switched at any of the packet nodes in access or aggregation. A Service Provider can choose whether to favor a lower latency (retaining the switching point close to the eNBs) or a tighter control of the traffic (thus moving the X2 switching point close to the EPC).

5.2.1. Applicability

This scenario does not rely on IP/MPLS for redundancy and protection. Reliability is provided by protection mechanisms at the transmission (physical) layer (e.g. microwave 1+1 hot-standby, leased lines in LAG, etc.). Even if not exclusive to that, this scenario is considered to fit into case 1.
End-to-end OAM is at Ethernet level (802.1ag, 802.3ah, Y.1731 are examples of available tools).

[1] For harmonization with the protocol stacks figures as well as with for those using different transport technologies, the service termination point has been placed in the middle of the demarcation node and by that in contradiction to MEF specifications. According to MEF terminology the UNI is actually between e.g. the demarcation node (CSG) and the eNB

5.2.2. Considered implementations (protocol stacks)

In this section some protocol stacks that support this logical architecture are shown. As mentioned earlier, the focus is on Ethernet as a common transport layer on top of any transmission technology, but other solutions can also be considered. For that one example relying on SDH is also shown.

The first example is a pure IEEE 802.1ad based scenario. Service VLANs (S-VLAN) are used to carry Customer VLANs (C-VLAN) across the Ethernet domain. One or more C-VLANs can be used (e.g. 1 per eNB, different VLANs per different flows, etc.).
The Ethernet control plane is represented, for example, by protocols such as G.8031 (Ethernet Line Protection), G.8032 (Ethernet Ring Protection) or standard Spanning Tree algorithms.

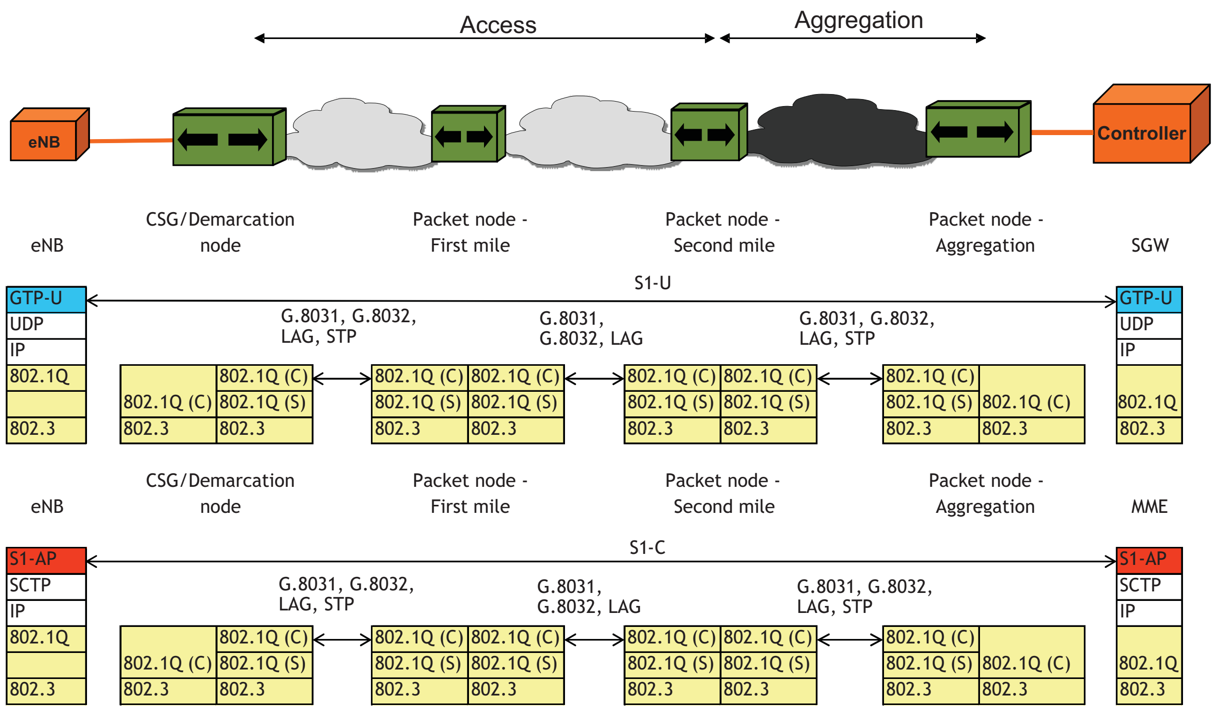


Figure 7: Example protocol stacks for Carrier Ethernet backhaul

A second example is shown in the following figure. It is supposed that SDH is used in access and aggregation (Ethernet over SDH model).

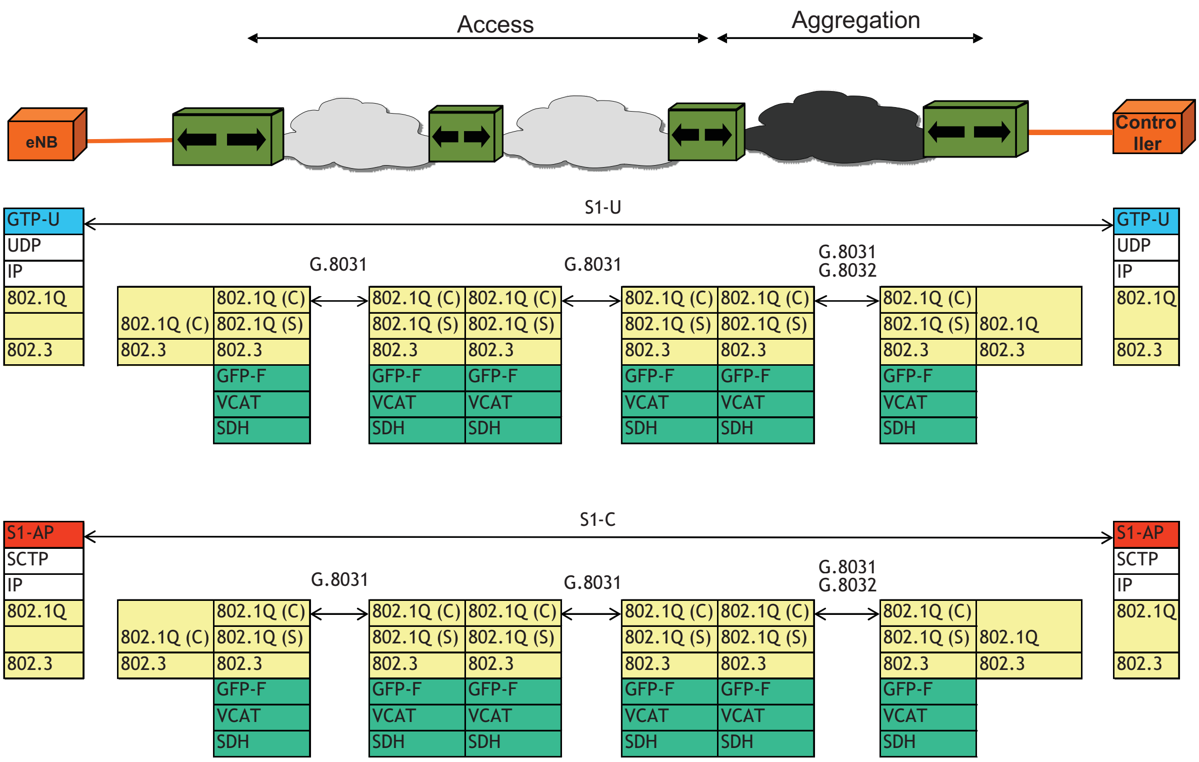


Figure 8: Example protocol stacks for Ethernet over SDH

5.3. Scenario 2 – Carrier Ethernet + L2/L3 VPN

This second scenario considers two different approaches for access and aggregation. The assumption is that access is still based on a tree-like topology, while ring or mesh is introduced in aggregation.
While for access the same reasons for having Ethernet backhaul, as in scenario 1, are still valid, in aggregation it is quite common to have MPLS and leverage its protection capability.
The next picture shows the high level architecture.

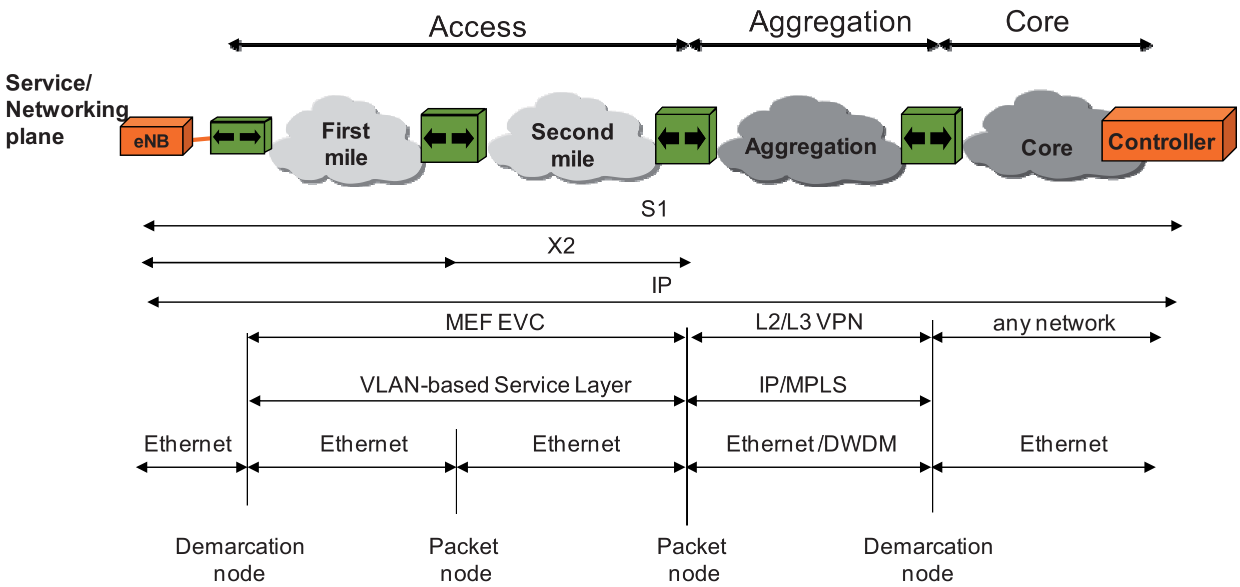


Figure 9: Backhaul Scenario based on Carrier Ethernet with L2/L3VPNs

Specifically in aggregation, technologies such as DWDM can often be found together or as an alternative to Ethernet. On top, an IP/MPLS based transport is used to carry LSPs and pseudowires, realizing a L2 or L3 VPN.
Since access is still based on an Ethernet, as per scenario 1, there is one node at the border between access and aggregation that has the task of adapting the networking technologies and the functional architectures.
As an alternative, MPLS-TP could also be employed in access instead of a VLAN transport. MPLS-TP could also be used in aggregation for implementing a point-to-point L2 VPN (e.g. VPWS).

5.3.1. Applicability

Case 2 is one typical example for having a logical architectural split between access and aggregation. The access can adopt any physical technology and rely on their protection methods (e.g. physical redundancy). For the aggregation, the MPLS control plane handles all the necessary protection mechanisms.
End-to-end OAM can be obtained at the pseudowire level with interworking with Ethernet OAM.

5.3.2. Considered implementations (protocol stacks)

Two examples are shown in this section.
In the first one a L2 VPN is considered.

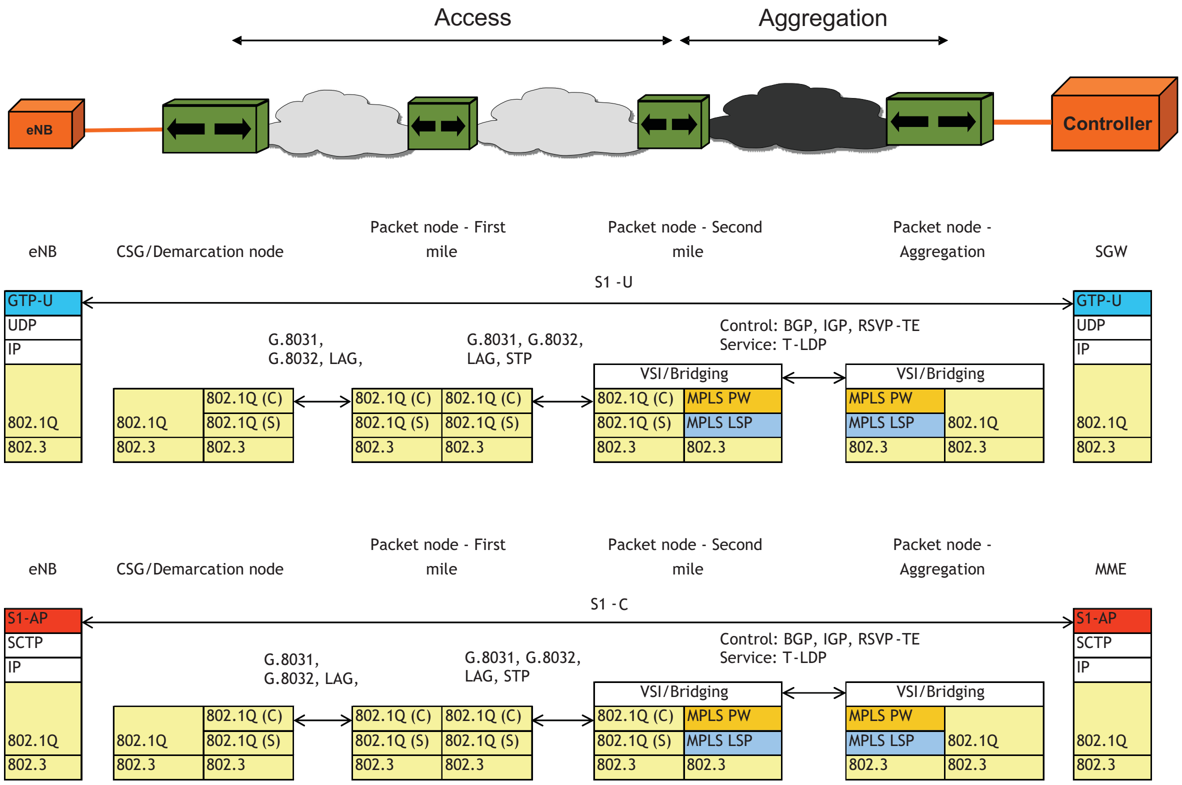


Figure 10: Example protocol stacks for Carrier Ethernet with L2VPN backhaul

The second picture shows the same scenario where L3 VPN is used in aggregation.

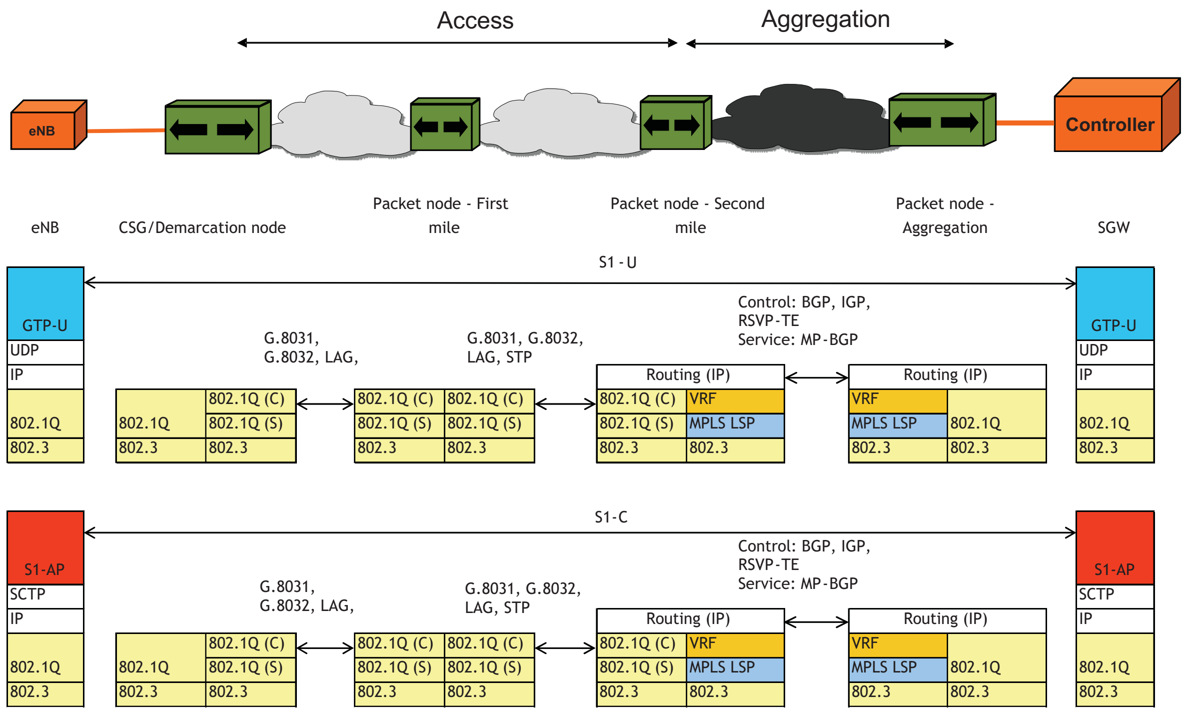


Figure 11: Example protocol stacks for Carrier Ethernet with L3VPN backhaul

5.4. Scenario 3 – MPLS access + L2/L3 VPN

This scenario mainly focuses on the transport capability of MPLS, which is also used in access. Specifically, MPLS or MPLS-TP is considered to build point-to-point connections in the access domain as a way to enter a VPN into the aggregation.

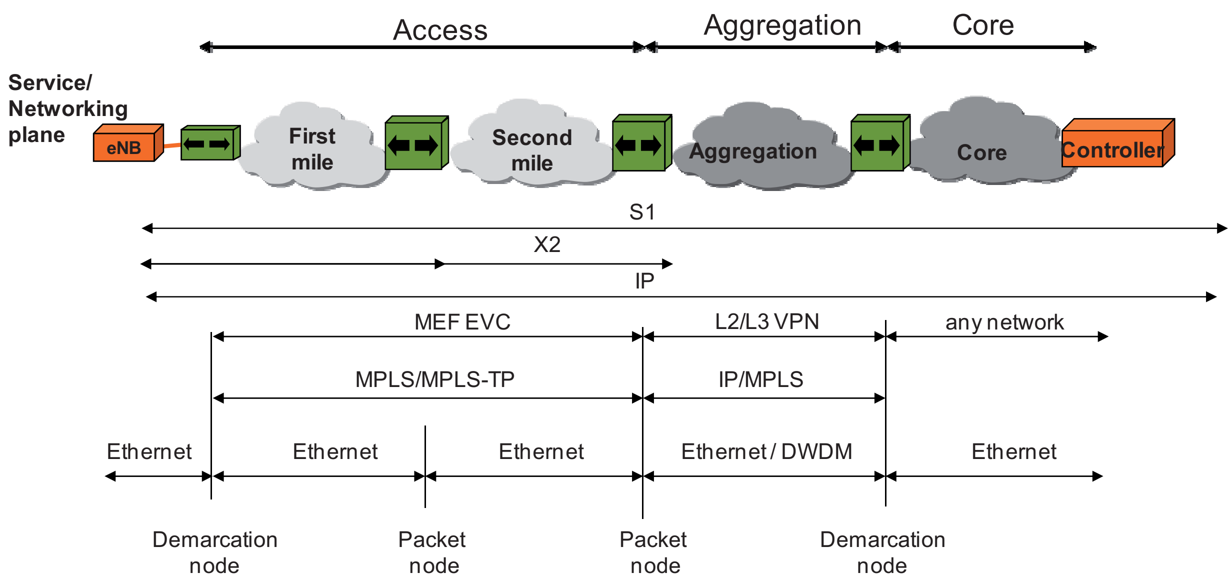


Figure 12: Backhaul Scenario based on MPLS with L2/L3VPN

5.4.1. Applicability

Case 2 is probably the most suitable for adopting this logical architecture, especially if the need is to leverage on the transport facilities of MPLS/MPLS-TP even in the access. In doing that, one or more pseudowires carry the relevant traffic across the access network up to the first aggregation node where traffic enters a L2 or L3 VPN.

End-to-end pseudowire OAM can be enabled through standard mechanisms such as VCCV ping, traceroute or BFD.

5.4.2. Considered implementations (protocol stacks)

Again, two examples are reported here. The first one is based on a L2 VPN in the aggregation domain (H-VPLS).

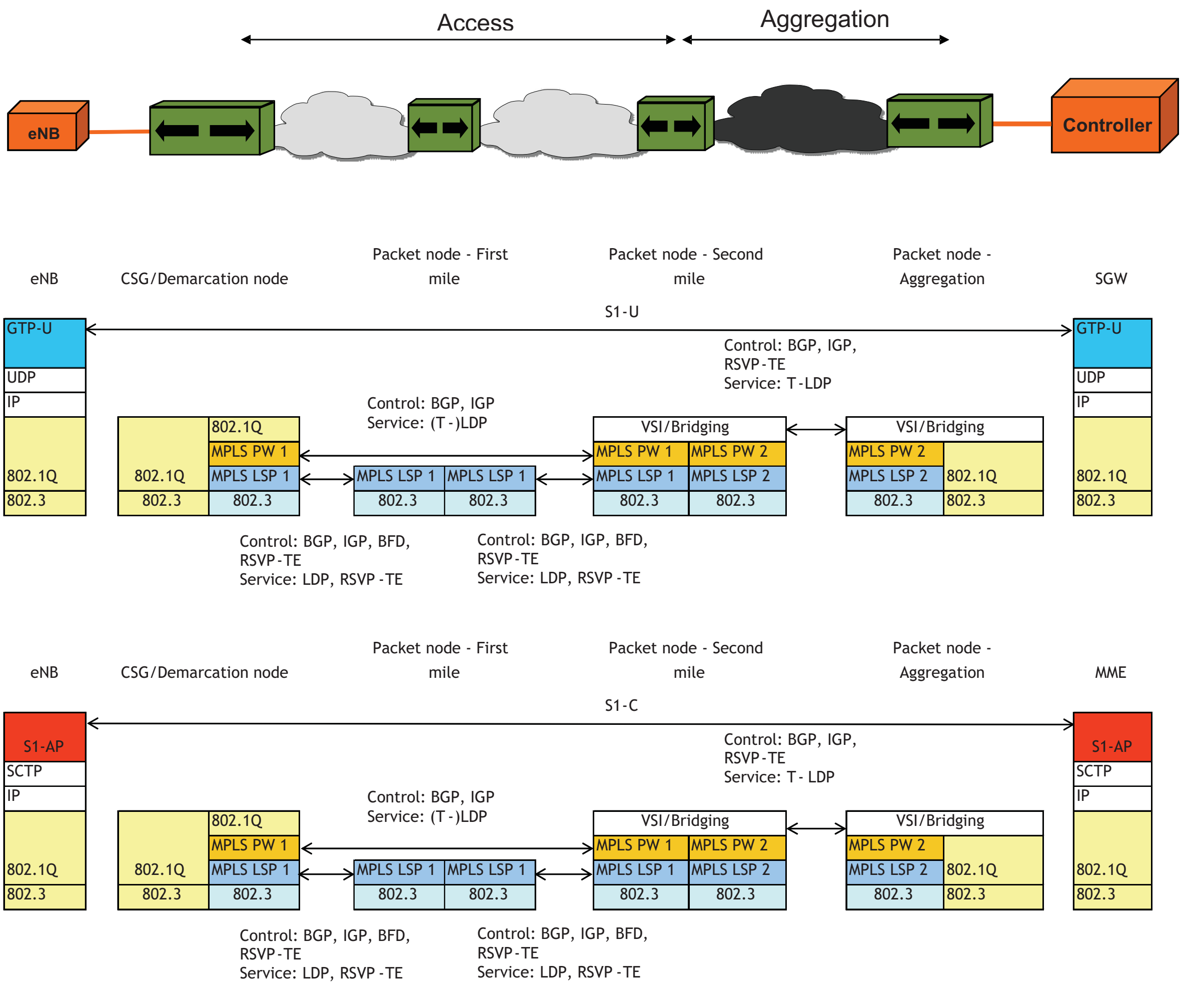


Figure 13: Example protocol stacks for MPLS with L2VPN backhaul

The second examples only differentiate for having a L3 VPN in aggregation.

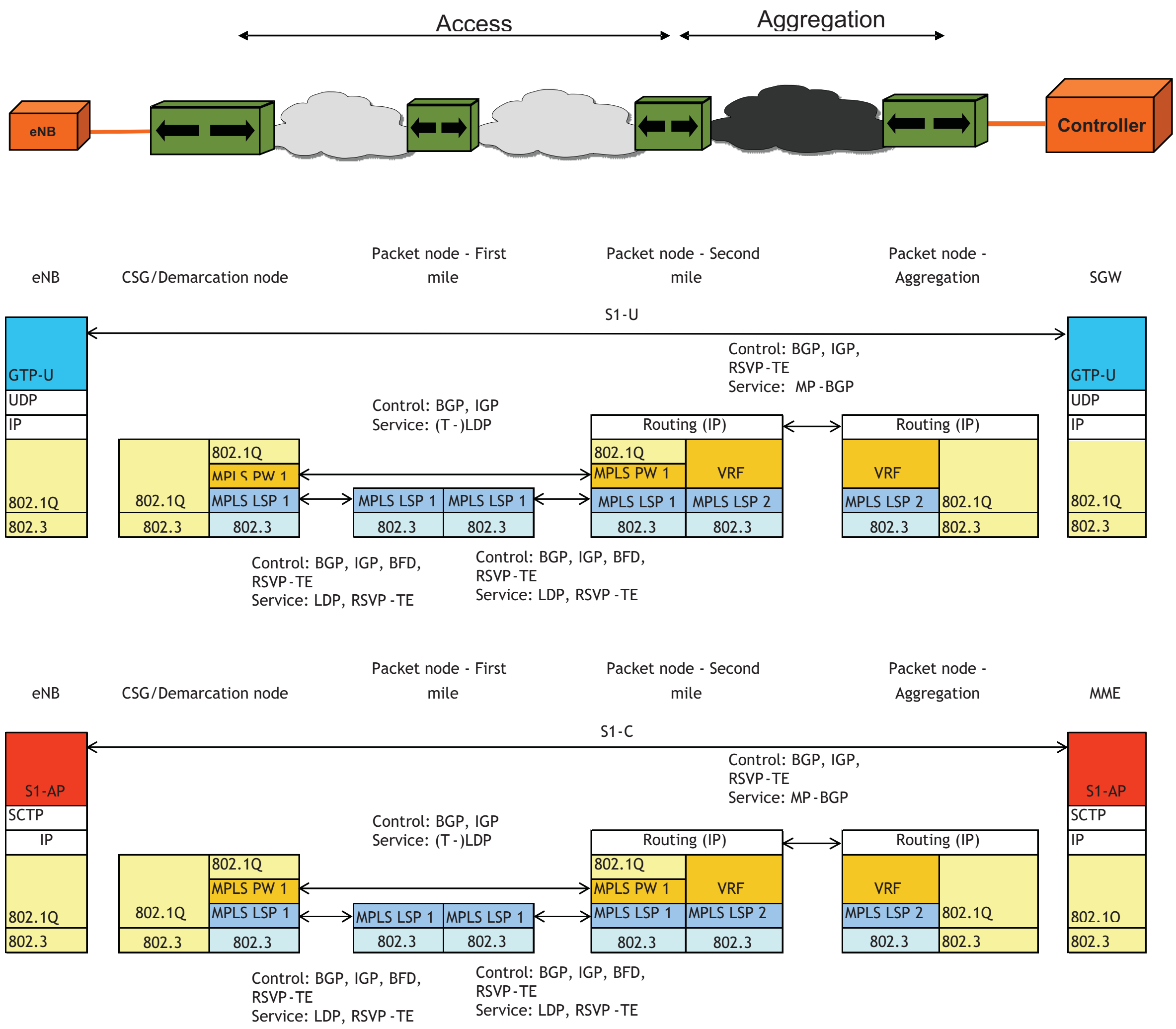


Figure 14: Example protocol stacks for Carrier Ethernet with L3VPN backhaul

5.5. Scenario 4 – L2/L3 VPN in access + L2/L3 VPN in aggregation

Scenario 4 constitutes an interesting variation of scenario 3, where not only is the transport and protection capability of MPLS exploited in access, but also the MPLS traffic segregation through VPN to have the isolation of the two domains. In this case two distinct VPNs are provisioned, one in the access domain and a second one into the aggregation.

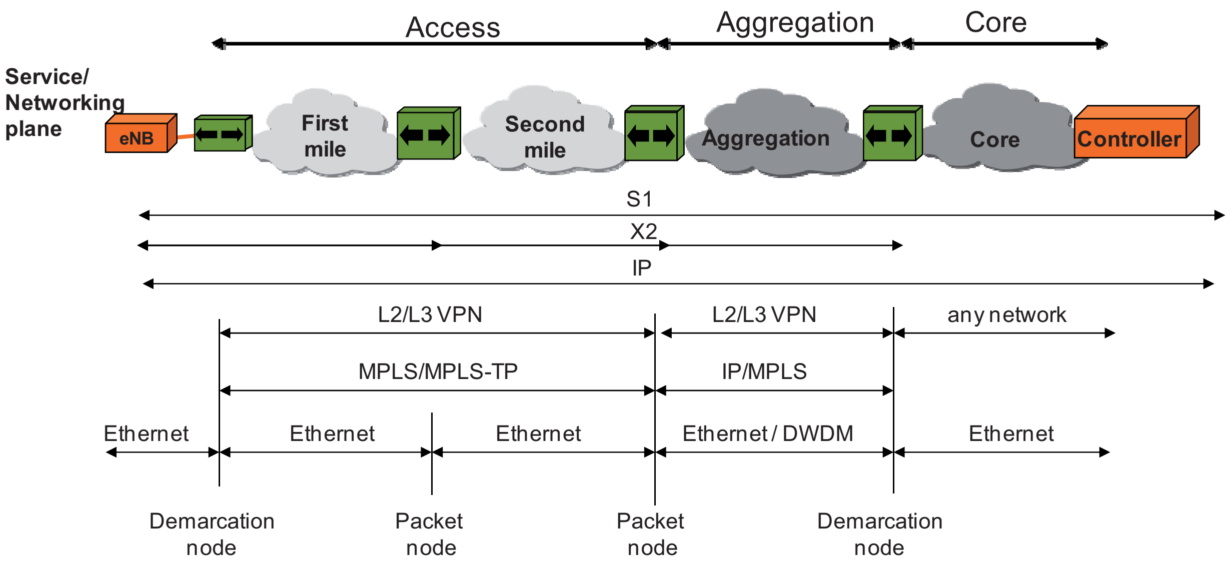


Figure 15: Backhaul Scenario based on L2/L3VPNs in access and aggregation

5.5.1. Applicability

Several combinations are possible, using either IP/MPLS or MPLS-TP to obtain the different flavors of VPN. The most likely see the presence of a L3 VPN in the aggregation, based on IP/MPLS, and a L2 VPN in access (even based on MPLS-TP), but for sake of completeness all the protocols stacks are shown.

Case 3 and case 4 can be considered for implementing this scenario.

End-to-end OAM can combine LSP and pseudowire tools.

5.5.2. Considered implementations (protocol stacks)

A few possibilities are considered.
A first example shows a L2 VPN in the access domain combined with L3 VPN in aggregation.

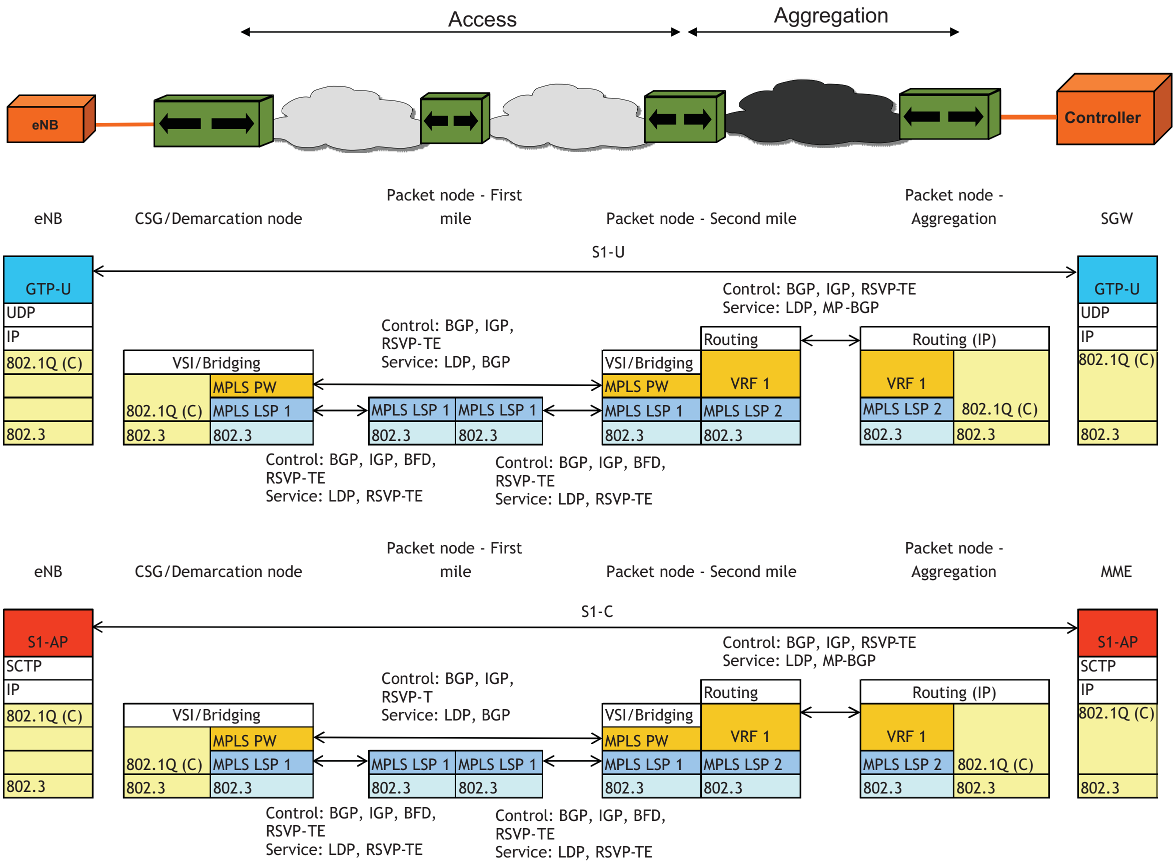


Figure 16: Example protocol stacks for combined L2VPN and L3VPN backhaul

Another possibility is given by a double L2 VPN, as show in the next figure.

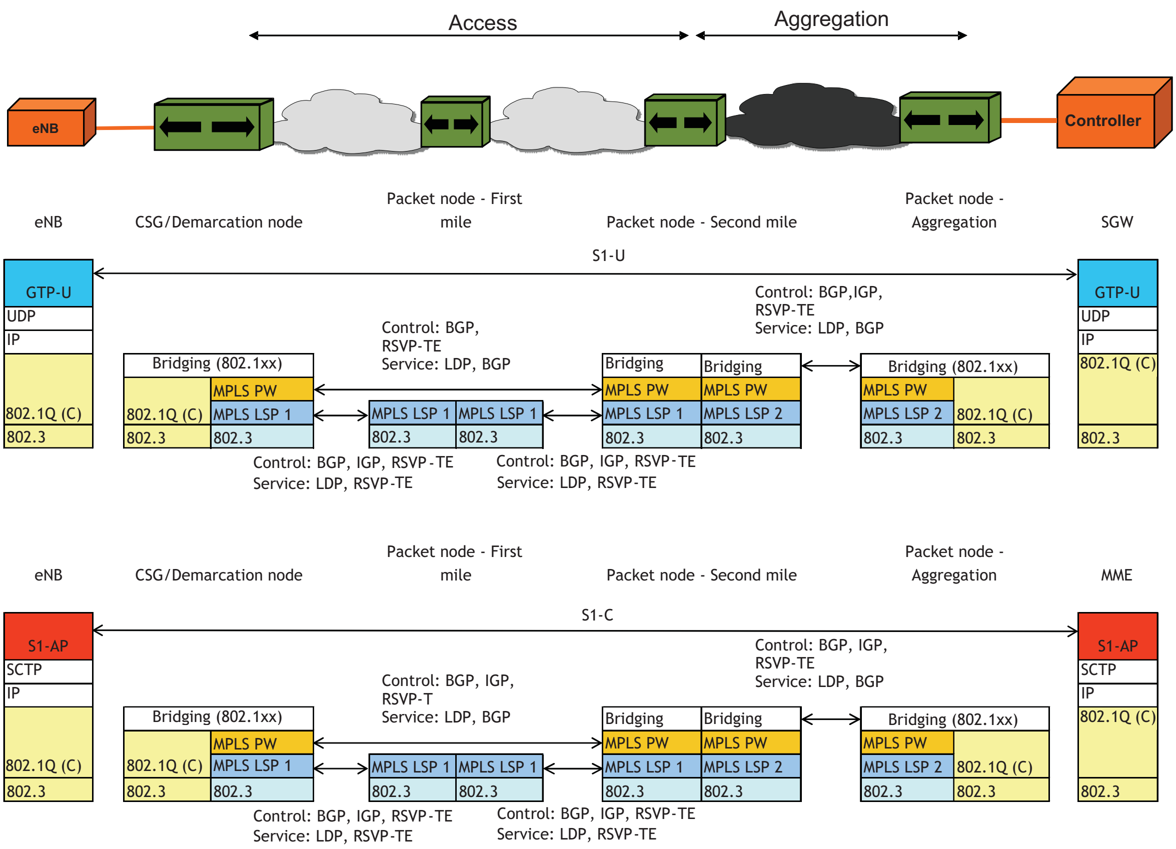


Figure 17: Example protocol stacks for two L2VPNs

At last, the case with two L3 VPNs is shown.

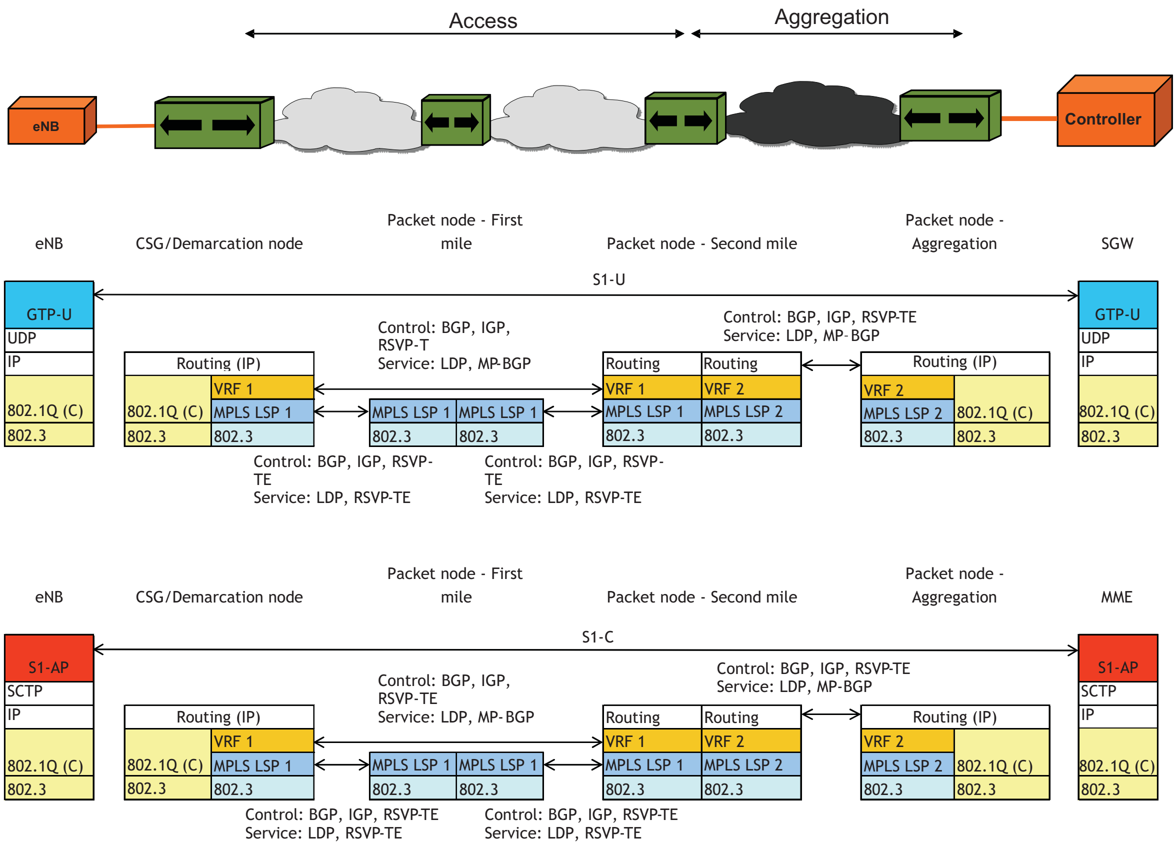


Figure 18: Example protocol stacks for two L3VPNs

5.6. Scenario 5 – End-to-end (Multi-segment) Pseudowire

Scenario 5 constitutes a variation of scenario 3 that combines the approach of having an end-to-end service span (through different segments of the same pseudowire) yet maintaining possible different transport and security domains (e.g. one in the access and another in the aggregation) by having an access/aggregation demarcation node where all pseudowires are terminated or switched. MPLS(-TP) LSPs or Ethernet VLANs can be used to steer and segregate the traffic, depending on Service Providers' attitude.

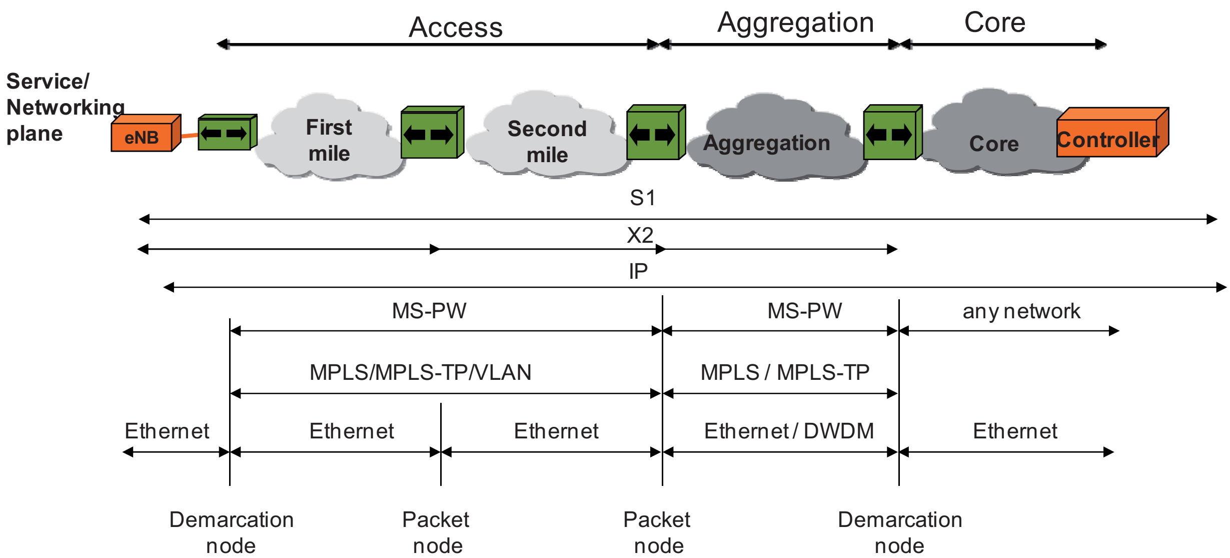


Figure 19: Backhaul Scenario with multi-segment pseudowires

The picture considers only two segments for a pseudowire, for simplicity, but more are also possible.

5.6.1. Applicability

Case 2 and case 3 are well covered by this scenario, since different combinations of L2 and L3 transport options are available, especially in access where Ethernet might be employed as an alternative to MPLS.

5.6.2. Considered implementations (protocol stacks)

The next picture highlights the stack associated with this scenario.

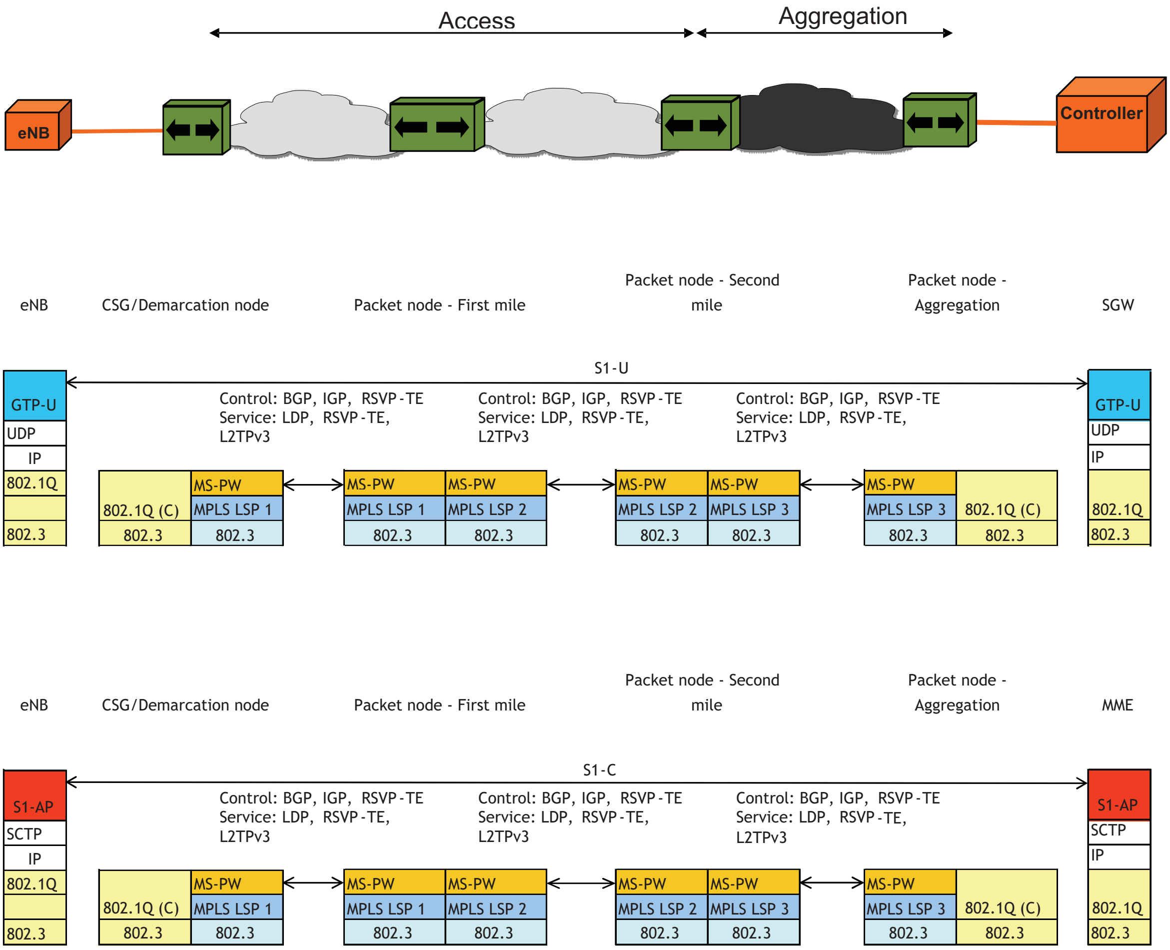


Figure 20: Example protocol stacks for multi-segment pseudowire backhaul

5.7. Scenario 6 – Full L3

The name chosen for this scenario indicates a logical architecture based on MPLS/MPLS-TP as the transport spanning from the eNB to the MME and S/P-GW controllers, on top of which one VPN is provisioned to realize the service, be it a L2 or L3 VPN.
As a result, there is no logical distinction between access and aggregation, both belong to one domain only.

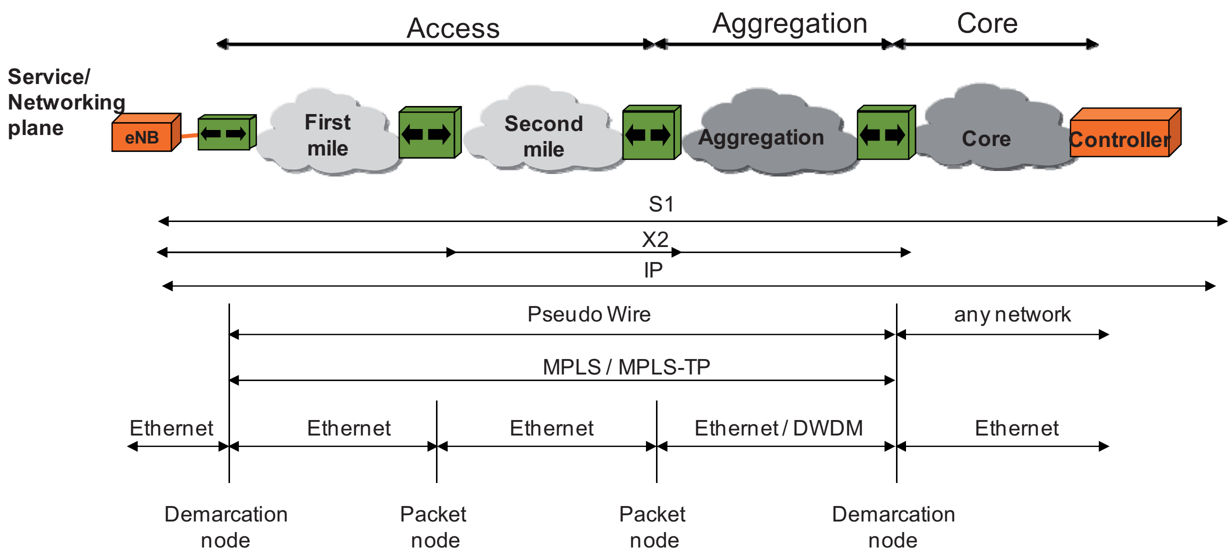


Figure 21: Backhaul Scenario with full L3 network

5.7.1. Applicability

Case 4 is suited for this scenario, fully relying on MPLS or MPLS-TP for steering and protection.
This scenario will be very efficient for multi operator implementation.

5.7.2. Considered implementations (protocol stacks)

The first example shows an end-to-end L2 VPN.

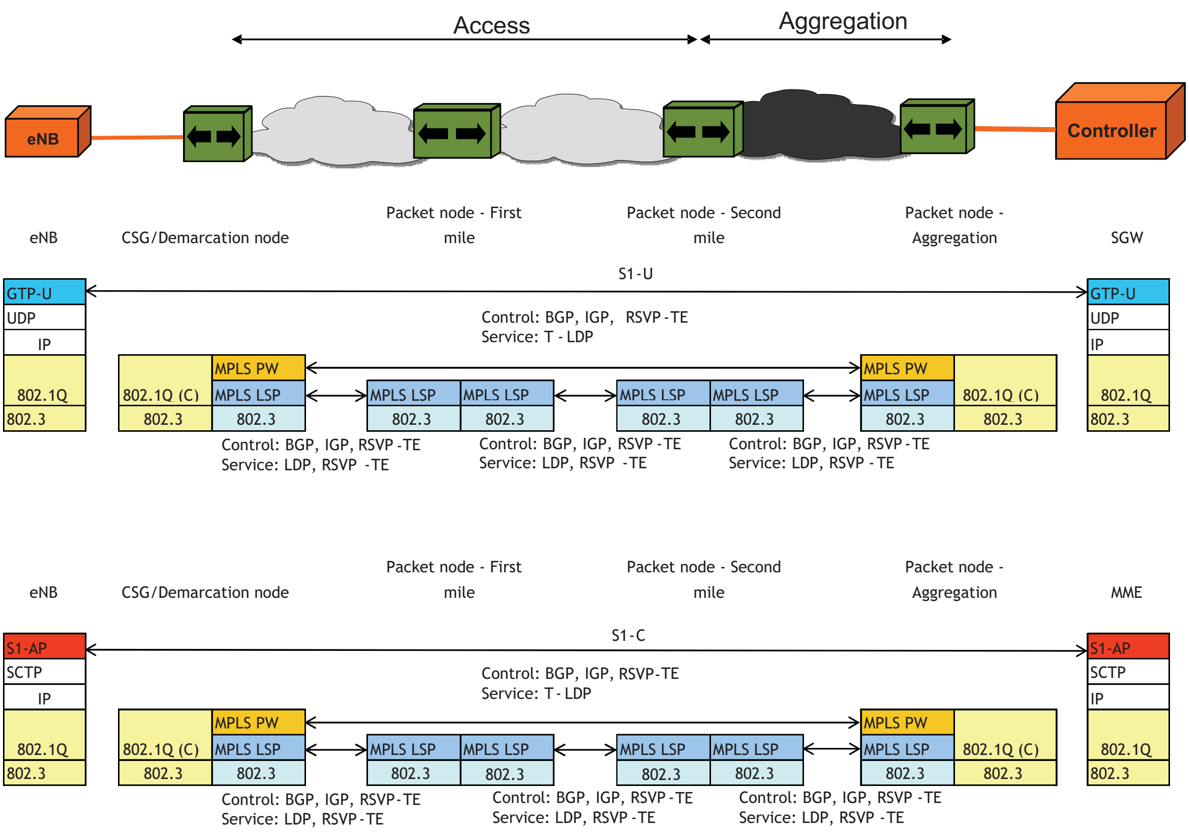


Figure 22: Example protocol stacks for L2VPN based backhaul

This second case shows the routed version (L3) of this scenario.

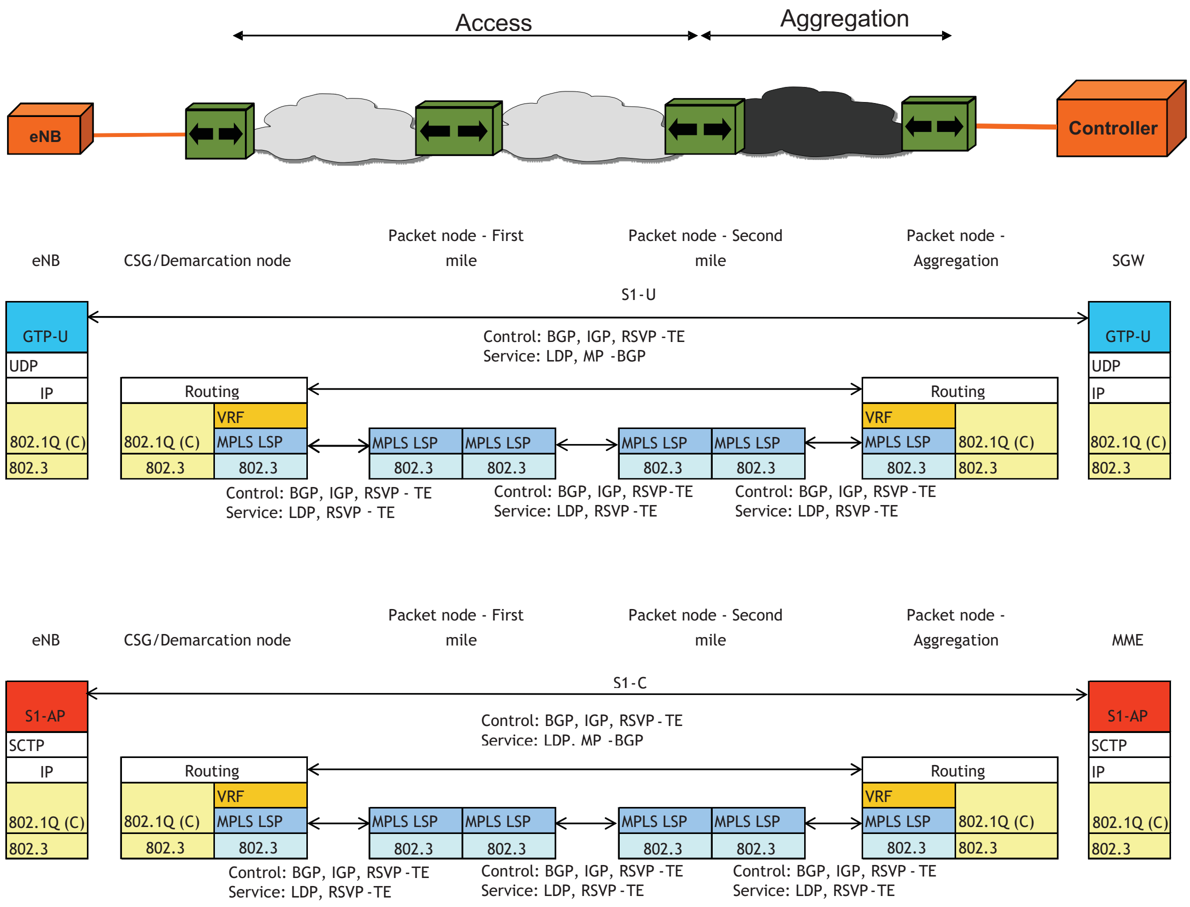


Figure 23: Example protocol stacks for L3VPN based backhaul

6. How to “pick” the right scenario

Even if this could be considered as the key question, the answer is not straightforward and does depend on several factors.
Previous sections of this paper highlighted how the installed base, or even the incumbency of previous technical choices, could be one of the drivers. In that case, operators handling the move from a TDM network might prefer a stepwise approach and progressively introduce layer 2 or 3 solutions in the aggregation before considering the transition in the access.
If this is the case scenarios 2 or 3 might represent the target network, even if a pure layer 2 network as represented by scenario 1 has its own applicability.

Greenfield LTE operators or operators wishing to build a converged network also for enterprise and residential services, might consider layer 3 oriented scenarios, e.g. from 4 to 6. In general, scenario 6 is seen, at the current stage, as a kind of target architecture for the medium-long term.

In any case, each operator will base the choice considering not only technical aspects. Organization, skill and attitude, service opportunity, available budget etc. will also influence the selection of the preferred scenario, technology and products.

7. Future Study Items

The following items have been proposed during the workgroup discussions as trends that might have an impact on the backhaul network. The analysis done so far showed that this is not the case, but in future that might change. For this reason they have been listed as areas where future studies might be directed to.

7.1. LTE-A

LTE Advanced (LTE-A) is a preliminary mobile communication standard, formally submitted as a candidate 4G systems to ITU-T in the fall 2009, and expected to be finalized in 2011. It is standardized by 3GPP as a major enhancement of the LTE standard.
LTE-A provides a toolbox of solutions improving radio performance, like enhanced MIMO, usage of Relay BTS and Coordinated Multipoint Transmission (CoMP). As studies and standardization are still ongoing, it is not possible to identify and quantify the implication of LTE-A on the backhaul network.

7.2. Security

There are two major differences compared to WCDMA with respect to transport security

- Air interface encryption of user plane traffic is terminated at the eNB, thus user plane traffic in the LTE mobile backhaul network is not secured by Radio Network Layer protocols.
- Since the LTE network architecture is flat, adjacent base stations (X2) and core nodes (MME, S-GW) (S1) become directly IP-reachable from base station sites. If physical access to the site cannot be prohibited, a hacker could connect his device to the network port and attack the aforementioned network elements.

Transport security features are seen as mandatory if both the mobile backhaul network and the eNB site cannot be regarded as secure. IPsec provides a comprehensive set of security features (data origin authentication, encryption, integrity protection), solving both problems above. The 3GPP security architecture is based on IPsec and Public Key Infrastructure (PKI).

IPsec is applied between Security Gateways (SEG). Each eNB site instantiates one SEG function. One or more Security Gateways (SEG) should be located at the edge of the operator's "Security Domain" (as per 3GPP Network Domain Security). Typically, the Security Domain includes the backbone network. The SEG is effectively hiding the core nodes (MME, SAE-GW, Network Management System) from the mobile backhaul network. Since the traffic itself is transparent to the SEG, various core network configurations can be supported.

With the introduction of S1-Flex (one eNB connected to multiple EPC) also multiple SEG can be used, which increases the number of security associations needed per eNB and also has some implication on the architecture of the backhaul network itself.

The impact of security onto backhaul architectures will be anyhow addressed into a separate NGMN paper.

7.3. Selective IP Offloading (SIPTO)

SIPTO is a concept being introduced in 3GPP Release 10 for reducing the "cost per bit" in flat networks. It is based on a specific scenario within the operator's network, allowing selective offloading of the traffic away from the Evolved Packet Core network. One of its main goals is cost-optimized handling of the internet traffic that is not intended for the operator's core network (i.e., operator services).
Selective offloading can be based e.g. on the service type or specific QoS needs of the service.

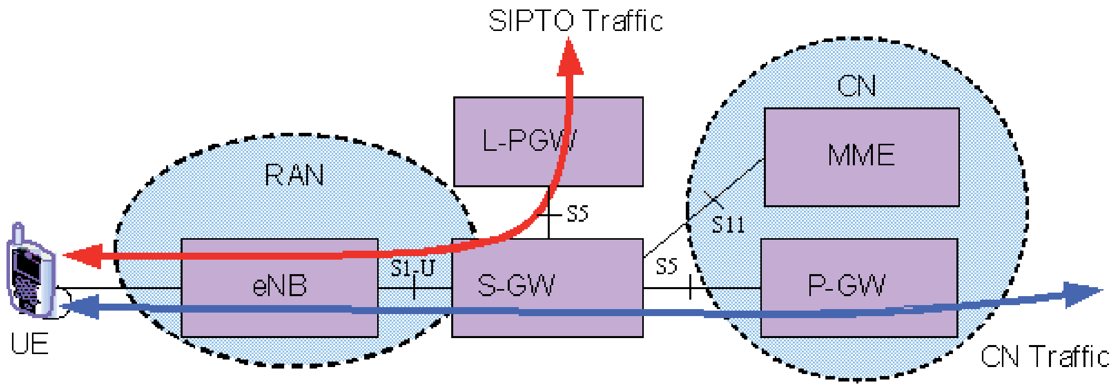


Figure 24: Baseline approach for "SIPTO above RAN" scenario.

As shown in Figure 24 the Local GW is selected for the traffic to be offloaded. Hence for the backhaul network (between eNB and S-GW) there is no implication caused by SIPTO.

7.4. Femto-Cells or none-3GPP Access

Femto-Cell base stations as well as none 3GPP-based radio products can share the same backhaul network with the eNodeBs. In this case the corresponding security elements need to be included.

8. Conclusions and next steps

This paper has analyzed different topologies and architectures for an LTE-ready backhaul network and aimed at supporting operators in their decision process towards a packet-based network capable of supporting current and future requirements, as seen in the paragraph before.
The reason why several scenarios have been presented is that many options are possible, each with its own advantages. In some cases operators will select one of the possible scenarios and will stay with it. In other cases it is also possible to define a roadmap that includes more scenarios.

Before any architecture design, operators shall list their requirements to be considered, among others, the installed base and how simple the migration to packet can be done, economical elements, the desire to include factors not included in this paper such as security and high availability constraints or targeted quality of experience.

9. References

1. NGMN, 'Next Generation Mobile Networks Beyond HSPA & EVDO – A white paper', V3.0, December 2006, available at www.ngmn.org.
2. "Next Generation Mobile Networks Optimised Backhaul Requirements", NGMN Alliance, August 14th, 2008