M. Lind (ed.)
J. Mulahusic
TeliaSonera
D. Park
Samsung Electronics
A. Baudot
France Telecom
P. Savola
CSC/Funet
October 2003

Scenarios for Introducing IPv6 into ISP Networks

Status of this Memo

Abstract

This document describes different scenarios for the introduction of IPv6 into an existing IPv4 ISP network without disrupting the IPv4 service. During the IPv6 introduction can the network go through different stages. The first one is the initial stage of an IPv4-only infrastructure, and the final one corresponds to a whole dual-stack infrastructure enabling full coexistence of IPv4 and IPv6 traffic and services. In between, typical intermediate stages involving

coexistence mechanism are identified. The scenarios depicted in this document are describing the way to move along these different possible stages.

Table of Contents

1. Introduction

An ISP offering an IPv4 service will find that there are different ways to add IPv6 to this service. During the introduction of IPv6 the network will go through different stages of IPv6 maturity. In addition to this there has to be a transition between these stages to make them feasible to implement. The main goal of this document is to provide possible scenarios to the ISP when introducing IPv6 connectivity in the existing ISP IPv4 legacy network.

In this document different transition scenarios and situations during the introduction of IPv6 are covered in a broader perspective and deals only with a generic view of how an ISP network is built. This should be seen as the starting point for further documentation

in a companion document of how the introduction of IPv6 can be done in an ISP network.

2. Scope of the document

The scope of the document is to describe different cases for the introduction of an IPv6 service in a generic IPv4 ISP network. This means that the document will be limited to services that include both IPv6 and IPv4 and will not cover issues surrounding an IPv6 only service. Therefore, the ISP network should be able to carry IPv4 and IPv6 traffic without any distinction related to the version of the protocol.

The different building blocks that will be considered are the customer network, the access networks, the core network and exchange points.

The network can be at a different stage relating to, either how far it has adopted IPv6, or to how likely it may be upgraded to IPv6. We will consider these stages, as well as the transition scenarios between the different stages.

It is outside the scope of this document to describe different types of access or network technologies. It is also outside of the scope to propose different solutions. Solutions will be covered in a separate document.

3. Terminology used

This section defines and clarifies the terminology used in this document:

"CPE" : Customer Premise Equipment

"PE" : Provider Edge equipment

"Access" : This is the part of the network which is used by a customer when connecting to an ISP network. It includes the CPEs, the last hop links and the parts of the PE interfacing to the last hop links.

"Core" : This is the rest of the ISP network infrastructure.

It includes the parts of the PE interfacing to the core backbone, the core routers of the ISP and the border routers used in order to exchange routing information with other ISPs (or other administrative entities).

"IT infrastructure" :
This is the part of the ISP network which hosts the services required for the correct operation of the ISP network. It usually includes DNS servers,Radius servers, monitoring and configuration applications...

"Dual network": A network which supports natively both IPv4 and IPv6.

4. Brief description of a generic ISP network

A generic ISP network topology can be divided into two main parts; the core network and the access networks connecting the customers.

The core network or the backbone is the part of the network that interconnects the different access networks and provides transport to the rest of the Internet via exchange points or other means. The core network can be built on different technologies but in this document the only interest is whether it is capable of carrying IPv6 traffic natively or not. Since there is no clear definition of core, it is defined in this document as being all routers that are a part of the same routed domain in the transport network. This means that all routers up to the PE router are a part of the core. The PE router can also be partially part of the core if it exchanges routing information and transports traffic to and from the core.

The access networks provide connectivity to enterprise and private customers. Other ISPs might as well be customers and connected to the ISP's access network. As with the core the absence or presence of native IPv6 capability is the only thing of real interest in the access network technology.

It is noticeable that, in some cases (e.g. European legacy operators), a given access network may have to be shared between different ISPs. According to the type of the access network used (e.g. involving only layer 2 devices, or involving non-IP

technology), this constraint result into architectural considerations that may be relevant in the analysis document.

"IT infrastructure" building blocks refer to the basic main functions needed for a regular backbone operation. This building block is dealing with: network management, customers' authentication and accounting, address assignment and naming. It represents the minimum functions needed to provide a customer service, referring to both network infrastructure operation, and administrative management of customers.

It doesn't matter if these customer networks have a single node or a large routed network. What is of interest is if routing information is exchanged or not since it will affect the ISP's network. The existence of customer placed equipment will also affect how a service can be delivered. In addition to the ISP's actual network components there are a lot of support and backend systems that have to be considered.

```
        ------------    ---------
       |    IT      |  |         |
       |infrastruct.|--|  CORE   |
       |            |  |         |\
        ------------    ---------  \
           .             / | \      \
           .            /  |  \      \_Peering( Direct & IX )
           .           /   |   \
           .          /    |    \
           .         /     |     \
        -------     /   -------   \     -------
       |       |   /   |       |   \   |       |
       |Access1|--/    |Access2|    \--|Access3|
       |       |       |       |       |       |
        -------         -------         -------
           |               |               | ISP Network
       -------------------------------------------------------
           |               |               | Customer Networks
       +--------+      +--------+      +--------+
       |        |      |        |      |        |
       |Customer|      |Customer|      |Customer|
       |        |      |        |      |        |
       +--------+      +--------+      +--------+
```

Figure 1: ISP network topology

5. Scenarios

The scenarios section describes different stages an ISP might consider when introducing IPv6 connectivity in the existing IPv4 network and the different scenarios that might occur in the respective stages.

The stages here are snapshots of an ISP's network with respect to IPv6 maturity. Since an ISP's network is constantly evolving, a stage is a measure of how far an ISP has come in turn of implementing necessary functionality to offer IPv6 to the customers.

It is possible to freely transition between different stages. However, a network segment can only be in one stage at a time but an ISP network as a whole can be in different stages. There are different transition paths between the first and final stage. The transition between two stages does not have to be immediate but can occur gradually.

Each stage has different IPv6 properties. An ISP can therefore, based on the requirements it has, decide into which stage it will transform its network.

5.1 Assumptions

The stages are derived from the generic description of an ISP network in section 3. A combination of different building blocks that constitute an ISP environment will lead to a number of scenarios, which an ISP can choose from. The scenarios of most relevance to this document are considered to be the ones that in the most efficient and feasible way maximize the ability for an ISP to offer IPv6 to its customers.

The most predominant case today is considered to be an operator with a core and access IPv4 network delivering IPv4 service to a customer that is running IPv4 as well. At some point in the future, it is expected that the customer will want to have an IPv6 service, in addition to the already existing IPv4 service. This IPv6 service may be offered by the same ISP, or by a different one. Anyway the challenge for the ISP is to deliver the requested IPv6 service over the existing infrastructure and at the same time keep the IPv4 service intact.

5.2 Customer requirements and ISP offerings

Looking at the scenarios from the end customer's perspective there might be a demand for three different services; the customer might demand IPv4 service, IPv6 service or both services. This can lead to two scenarios depending on the stage the ISP's network is in.

If an ISP only offers IPv4 or IPv6 service and a customer wants to connect a device or network that only supports one service and if that service is not offered, it will lead to a dead-end. If the customer or ISP instead connects a dual stack device it is possible to circumvent the lack of the missing service in the access network by using some kind of coexistence mechanism. This scenario will only be considered in the perspective of the ISP offering a mechanism to bridge the access and reach the IPv6 core.

In the case where the customer connects a single stack device to a corresponding single stack access network or when the customer connects a single stack device to a dual stack access network is covered by the all over dual stack case. Therefore, neither of these cases need further be explored separately in this document but can be seen as a part of a full dual stack case.

After eliminating a number of cases explained above, there are four stages that are most probable and where an ISP will find its network in. Which stage a network is in; depends on whether or not some part of the network previously has been upgraded to support IPv6 or if it is easier to enable IPv6 in one part or another. For instance, routers in the core might have IPv6 support or might be easily upgradeable, while the hardware in the access might have to be completely replaced in order to handle IPv6 traffic.

Note that in every stage except Stage 1, the ISP can offer both IPv4 and IPv6 services to the customer.

The four most probable stages are:

o Stage 1	Launch
o Stage 2a	Core
o Stage 2b	Access
o Stage 3	Complete

Generally the ISP is able to upgrade current IPv4 network to IPv4/IPv6 dual network via Stage 2b but the IPv6 service can also be implemented at a small cost with simple tunnel mechanisms on the existing system. When designing a new network Stage 3 might be the first and last step since there is no legacy concerns. Absence of IPv6 capability in the network equipment can still be a limiting factor nevertheless.

5.3 Stage 1 Scenarios: Launch

The first stage is an IPv4 only ISP with an IPv4 customer. This is the most common case today and has to be the starting point for the introduction of IPv6. From this stage, an ISP can move (transition) to any other stage with the goal to offer IPv6 to its customer.

The scenario and the immediate first step is to get a prefix allocation (typically a /32) from the appropriate RIR according to allocation process. For the IPv6 migration scenarios described in this document, an ISP has to be able to exchange IPv6 traffic, e.g. by connecting to an exchange, through a direct peering/transit or a tunnel, prior to introducing customers in Stage2 and Stage 3.

```
   Customer    Access      Core     Exchange
   +------+   +------+   +------+   +------+
   |      |   |      |   |      |   | IPv4 |
   | IPv4 |---| IPv4 |---| IPv4 |---|   +  |
   |      |   |      |   |      |   | IPv6 |
   +------+   +------+   +------+   +------+
<--------------IPv4-------------->
```

Figure 2. IPv4 network

5.4 Stage 2a Scenarios: Core

Stage 2a is an ISP with access networks that are IPv4 only and a core that is IPv4 and IPv6. In particular, the ISP considers it possible to make the core IPv6 capable either through software or hardware upgrades. In this stage the customer should have support for both IPv4 and IPv6 and use a tunneling mechanism to be able to run the IPv6 service. To offer the IPv6 service, the ISP also has to exchange IPv6 traffic with other ISPs e.g. by connecting to an IPv6 exchange point. In particular, An ISP has to provide IPv6 connectivity through its IPv4 access networks.

An ISP can consider two kinds of scenarios such as automatic tunnels (e.g. provided by the 6to4 mechanism) and configured tunnels to bring IPv6 connectivity on top of an IPv4 only service. Both methods have advantages and limitations which are out of scope in this document and will be covered in the analysis document. The existence of NATs and firewalls in the path is also to be considered.

```
Customer    Access      Core     Exchange
+------+   +------+   +------+   +------+
|      |   |      |   |      |   | IPv4 |
| Dual |---| IPv4 |---| Dual |---|   +  |
|      |   |      |   |      |   | IPv6 |
+------+   +------+   +------+   +------+
   <---------IPv4-------->

   +=====================+
             IPv6         <---IPv6--->
   +=====================+
  Tunnel via access network
```

Figure 3. Upgraded core

5.5 Stage 2b Scenarios: Access

Stage 2b is an ISP with a core network that is IPv4 and an access network that is IPv4 and IPv6. Since the service to the customer is native IPv6 there is no requirement for the customer to support both IPv4 and IPv6. This is the biggest difference in comparison to the previous stage. The need to exchange IPv6 traffic or similar still exists but might be more complicated than in the previous case since the core isn't IPv6 enabled. After completing stage 2b the original

IPv4 core still is unchanged. This doesn't imply that there is no IPv6 core just that the IPv6 core is an overlay to or partially separated from the IPv4 core.

Like in section 5.4 tunnels is a possible scenario and can be used for IPv6 connectivity over the IPv4 network parts. Other forms of transport over for example an MPLS enabled core are also possible scenarios.

Generally, the ISP will continue providing IPv4 connectivity; in many cases private addresses and NATs will continue to be used. Access networks should make use of a mechanism to delegate a global IPv6 address prefix from the ISP to the customer.

```
   Customer    Access      Core     Exchange
   +------+   +------+   +------+   +------+
   |      |   |      |   |      |   | IPv4 |
   | Dual |---| Dual |---| IPv4 |---|   +  |
   |      |   |      |   |      |   | IPv6 |
   +------+   +------+   +------+   +------+
             <---------IPv4-------->

                 +=====================+
    <---IPv6--->          IPv6
                 +=====================+
                Tunnel via core network
```

Figure 4. Upgraded access

5.6 Stage 2a and 2b combination scenarios

Some ISPs may use different access technologies of varying IPv6 maturity. This may results in a combination of the former stages.

The case depicted in the figure 5 below, has no impact on stage 2a since it results in interconnection a dual access network to a dual core network.

```
Customer A  Access 1
+------+   +------+
|      |   |      |
| Dual |---| Dual |---+
|      |   |      |   |
+------+   +------+   |
                      |
Customer B  Access 2   \ Core    Exchange
+------+   +------+   +-+----+   +------+
|      |   |      |   |      |   | IPv4 |
| Dual |---| IPv4 |---| Dual |---|   +  |
|      |   |      |   |      |   | IPv6 |
+------+   +------+   +------+   +------+
   <---------IPv4-------->

   +=====================+
             IPv6         <---IPv6--->
   +=====================+
  Tunnel via access network
```

Figure 5. Upgraded core with multiple access

The case depicted in the figure 6 below, results in tunnel chaining, in order to keep independent access and core upgrade that may happened according to totally different timeframe.

```
      <--IPv4--> | <------IPv4------->

      +=========+ +==================+
         IPv6             IPv6
      +=========+ +==================+
     Tunnel via       Tunnel via
   access network     Core network

   Customer    Access
   +------+   +------+
   |      |   |      |
   | Dual |---| IPv4 |---+
   |      |   |      |   |
   +------+   +------+   |
                          \
   Customer    Access      | Core   Exchange
   +------+   +------+   +-+----+   +------+
   |      |   |      |   |      |   | IPv4 |
   | Dual |---| Dual |---| IPv4 |---|   +  |
   |      |   |      |   |      |   | IPv6 |
   +------+   +------+   +------+   +------+
<---------IPv4-------->

                 +=====================+
<---IPv6--->          IPv6
                 +=====================+
                Tunnel via access network
```

Figure 6. Upgraded access with upgrade core

5.7 Stage 3 scenarios: Complete

Stage 3 can be said to be the final step in introducing IPv6, at least in the scope of this document. This is an all over IPv6 service with native support for IPv6 and IPv4 in both core and access networks. This stage is identical to the previous stage in the customer's perspective since the access network hasn't changed. The requirement for exchanging IPv6 traffic is identical to stage 2.

```
   Customer    Access      Core     Exchange
   +------+   +------+   +------+   +------+
   |      |   |      |   |      |   | IPv4 |
   | Dual |---| Dual |---| Dual |---|   +  |
   |      |   |      |   |      |   | IPv6 |
   +------+   +------+   +------+   +------+
<--------------IPv4-------------->
<--------------IPv6-------------->
```

Figure 7. Completely upgraded network

5.8 Impact on the "IT infrastructure"

The different stages above are dealing with fundamental issues such as IPv6 connectivity and IPv6 traffic forwarding.

Some other background tasks must be realized in parallel to complete the new IPv6 service. The main tasks identified are:

- Customer authentication and accounting
- Address assignment
- Network management
- Naming service

Customer authentication and accounting and address assignment are relevant to the access network, and address assignment may have an impact on the core network.

Network management is relevant to both access and core networks.

Naming service intends to address minimum DNS facilities an ISP may have to provide.

From a general point of view these functions may be realized based on an IPv4 transport layer, an IPv6 transport layer, or both.

A service, such as a web server, advertised by an IPv6 address must be reachable from any IPv6 node.

6. Transition Scenarios

Given the different stages it is clear that the ISP has to be able to transition from one stage to another. The initial stage, in this document, is the IPv4 only service and network. The end stage is the dual IPv4/IPv6 service and network. As mentioned in the scope, this document does not cover the IPv6 only service and network and its implications on IPv4 customers. This has nothing to do with the usability of an IPv6 only service.

The transition starts out with the IPv4 ISP and then moves to one of three choices. These choices are the different transition scenarios. One way would be to upgrade the core first which leads to stage 2a. Another way to go could be to upgrade the access network which leads to stage 2b. The final possibility is to introduce IPv6 in the whole network at once which would lead to stage 3.

The choice is dependent on many different issues. For example it might not be possible to upgrade the core or the access network without large investments in new equipment which could lead to any of the two first choices. In another case it might be easier to take the direct step to a complete IPv6/IPv4 network due to routing protocol issues or similar.

If a partially upgraded network (stage 2a or 2b) was chosen as the first step, a second step remains before the network is all over native IPv6/IPv4. This is the transition to an all over dual stack network. This step is perhaps not necessary for stage 2b with an already native IPv6 service to the customer but might still occur when the timing is right. For stage 2a it is more obvious that a transition to a dual stack network is necessary since it has to be done to offer a native IPv6 service.

As most of the ISPs keep evolving continuously their core IPv4 networks (new firmware versions in the routers, new routers), they will be able to get them IPv6 ready, without additional investment, except the staff training. It may be a slower transition path, but useful since it allows an IPv6 introduction without any actual customer demand. This will probably be better than making everything at the last minute with a higher investment.

7. Future Stages

After a while the ISP might want to transition to a service that is IPv6 only, at least in certain parts of the network. This transition creates a lot of new cases in which to factor in how to maintain the IPv4 service. Providing an IPv6 only service is not much different than the dual IPv4/IPv6 service described in stage 3 except from the need to phase out the IPv4 service. The delivery of IPv4 services over an IPv6 network and the phase out is left for a future document.

8. Example networks

In this section, a number of different network examples are presented. They are only example networks and will not necessary match to any existing networks. Nevertheless, the examples will hopefully be useful even in the cases when they do not match the target networks. The purpose of the example networks is to exemplify the applicability of the transition mechanisms described in this document on a number of different example networks with different prerequisites.

The example network layout will be the same in all network examples. The networks examples are to be seen as a specific representation of the generic network with a limited number of network devices. An arbitrary number (in this case 7) of routers have been selected to represent the network examples. However, since the network examples follow the implementation strategies recommended for the generic network scenario, it should be possible to scale the example to fit a network with an arbitrary number, e.g. several hundreds or thousands, of routers.

The routers in the example are interconnected with each other as well as with another ISP. The connection to another ISP can either be a direct connection or through an exchange point. In addition to these connections, there are also a number of access networks connected to the routers. Access networks are normally connected to the core via access routers, but can in some cases be directly connected to the core routers. As described earlier in the generic network scenarios, the access networks are used to connect the customers. Access networks can, for example, be xDSL or cable network equipment.

```
                       |
                  ISP1 | ISP2
             +------+  |  +------+
             |      |  |  |      |
             |Router|--|--|Router|
             |      |  |  |      |
             +------+  |  +------+
             /      \  +-----------------------
            /        \
           /          \
       +------+    +------+
       |      |    |      |
       |Router|----|Router|
       |      |    |      |
       +------+    +------+\
           |           |    \             | Exchange point
       +------+    +------+  \  +------+  |  +------+
       |      |    |      |   \_|      |  |  |      |--
       |Router|----|Router|----\|Router|--|--|Switch|--
       |      |    |      |     |      |  |  |      |--
       +------+   /+------+     +------+  |  +------+
           |     /     |                  |
       +-------+/  +-------+              |
       |       |   |       |
       |Access1|   |Access2|
       |       |   |       |
       +-------+   +-------+
         |||||       |||||  ISP Network
       ----|-----------|----------------------
           |           |    Customer Networks
       +--------+  +--------+
       |        |  |        |
       |Customer|  |Customer|
       |        |  |        |
       +--------+  +--------+
```

Figure 2: ISP network example

8.1 Example 1

In example 1 a network built according to the example topology is present with a native IPv4 core, the routers. The core is running IS-IS and IBGP as routing protocol for internal and external routes

respectively. In the connection to ISP2 and the exchange point MBGP is used to exchange routes. Multicast is present and is using PIM-SM routing. QoS is present and is using DiffServ.

Access 1 is xDSL, connected to the core through an access router. The xDSL equipment, except for the access router, is considered to be layer 2 only, e.g. Ethernet or ATM. IPv4 addresses are dynamically assigned to the customer using DHCP. No routing information is exchanged with the customer. Access control and traceability is done in the access router. Customers are separated in VLANs or separate ATM PVCs up to the access router.

Access 2 is Fiber to the building/home connected directly to the core router. The FTTB/H is considered to be layer 3 aware and performs access control and traceability through its layer 3 awareness. IPv4 addresses are dynamically assigned to the customers using DHCP. No routing information is exchanged with the customer.

8.2 Example 2

In example 2 the core is running IPv4 with MPLS. Routing protocols used are OSPF and IBGP for internal and external routes. In the connection to ISP2 and the exchange point BGP is used to exchange routes. Multicast and QoS are not present.

Access 1 is a fixed line access, e.g. fiber, connected directly to the core. CPE is present at the customer and routing information is in some cases exchanged otherwise static routing is used. Access 1 can also be connected to BGP/MPLS-VPN running in the core.

Access 2 is xDSL connected directly to the core router. The xDSL is layer 3 aware. Addresses are dynamically assigned using DHCP. Access control is achieved on the physical layer and traceability is achieved using DHCP snooping. No routing information is exchanged with the customer.

8.3 Example 3

A transit provider offers IP connectivity to other providers, but not to end users or enterprises. IS-IS and IBGP is used internally and BGP externally. Its accesses connect Tier-2 provider cores. No multicast or QoS is used.

8.4 Example 4

Yet another example, if needed. To be done.

9. Security Considerations

This document describes different scenarios for the introduction of IPv6 in an IPv4 ISP network. Solutions are described in other documents hence this document has no security considerations.

Intellectual Property Statement

Full Copyright Statement

Acknowledgements

This draft is a joint effort of the ISP design team. The team consists of Jordi Palet, Suresh Satapati, Myung-Ki Shin, Vladimir Ksinant, Cleve Mickles, Marc Blanchet, Soohong Daniel Park, Alain Baudot and Mikael Lind

This draft has also greatly benefited from input by Margaret Wasserman.

Authors' Addresses

Mikael Lind
TeliaSonera
Vitsandsgatan 9B
SE-12386 Farsta, Sweden
Email: mikael.lind@teliasonera.com

Jasminko Mulahusic
TeliaSonera
Vitsandsgatan 9B
SE-12386 Farsta, Sweden

Email: jasminko.mulahusic@teliasonera.com

Soohong Daniel Park
Mobile Platform Laboratory, SAMSUNG Electronics.
416, Maetan-3dong, Paldal-Gu,
Suwon, Gyeonggi-do, Korea
Email: soohong.park@samsung.com

Alain Baudot
France Telecom R&D
42, rue des coutures
14066 Caen - FRANCE
Email: alain.baudot@rd.francetelecom.com

Pekka Savola
CSC/FUNET
Espoo, Finland
EMail: psavola@funet.fi