



Technical Paper

6Core Project Document

Fahad Ali Khan

Project Lead 6Core
IP Engineering Group

CYBERNET





Contents

ABSTRACT	3
INTRODUCTION	3
IPV6 AND PAKISTAN	4
IPV6 DEPLOYMENT IN PAKISTAN	4
PAKISTAN IPV6 NATIONAL BACKBONE PROJECT – 6CORE.....	5
<i>The 6Core Network.....</i>	<i>6</i>
<i>Phases of 6Core.....</i>	<i>8</i>
Phase I:	8
Phase II:	8
Phase III:	8
Phase IV:	9
Phase V:	9
<i>IPv6 National Backbone Ring.....</i>	<i>9</i>
CYBERNET – DANCOM Connectivity:.....	11
CYBERNET – SUPERNET Connectivity:	12
SUPERNET – DANCOM Connectivity:	13
BGP4+ Neighborhood	13
Routing Policies	15
<i>Becoming a TLA on the 6Core.....</i>	<i>16</i>
<i>Current Status.....</i>	<i>17</i>
IPV6 IN CYBERNET	18
<i>Addressing Scheme</i>	<i>22</i>
<i>Subnet Size</i>	<i>22</i>
<i>CYBERNET Testbed Connectivity.....</i>	<i>23</i>
<i>IGP Routing</i>	<i>24</i>
<i>EGP Routing.....</i>	<i>24</i>
<i>Monitoring</i>	<i>25</i>
<i>Other Services</i>	<i>25</i>
<i>Current Status.....</i>	<i>25</i>



Abstract

The 6Core project was started in October, 2006 by the Pakistan IPv6 Task Force as Pakistan IPv6 National core network to enable various IPv6 testing as well as to assist in the transitioning of Pakistan ISP/NSP and other Enterprises' IPv4 networks into IPv6 Internet.

The Concept of 6Core project evolved during SANOG 8 Meetings where the initial draft was present by Haris Shamsi. Fahad Ali Khan from CYBERNET, Tariq Mustafa and Hasan Asghar from SUPERNET and Zaeem Arshad from DANCOM showed their commitment towards the establishment of an IPv6 testbed and connect them over IPv6 tunnels. Extensive moral support has been provided by Khalid Raza & Yousuf Bhaiji (Cisco Systems), Gaurab Upadhaya (SANOG Chair) in Project 6Core.

This document describes the design details and best practices adapted in the initiation phase of Project 6Core.

Introduction

Currently the most widely accepted and deployed version of Internet Protocol in Internet is version 4 (IPv4). It was deployed in early 70's to facilitate communication and information sharing between US government researchers and academics. It was consider to be a most flexible and scalable technology but as every well designed and stable systems age and new featured systems takes their place, this is the certain case with IPv4 and gradually it shows some weakness and today it is no longer to support the requirement of modern and dynamic suture of internet.

Today the Internet does not mean only accessing Web Sites and checking emails. Explosive growth in network devices diversity and mobile communication, forces the global adoption of IP services and Technologies built over it. IP is considered by the market as the common denominator to converge different application layers such as data, voice, and audio. However, these new devices require many more IP addresses to interconnect all kinds of IP appliances besides just the computers currently interconnected on the Internet. This is the main reason for overwhelming the IPv4 address space. This exhaustion prompted the Internet Engineering Task Force to come to general consensus that to develop the next-generation Internet Protocol.



IPv6 and Pakistan

The origin of internet in Pakistan was back in 1991, when two Pakistani computer enthusiasts established a UUCP (Unix-to-Unix CoPy) email connection to the global Internet from the IMRAN.AR.PK host. In 1996 ISP licenses were provided to launch Internet services to end consumer. Since than number of ISPs have been established and services more than Million end consumers.

Today it is recognized worldwide that the new version of the Internet Protocol (IPv6) can play a fundamental role in shaping the future communication landscape, in tools of providing tools for ubiquitous access to internet, in liberating innovation potential of internet user and in strengthening Pakistan industry, notably in the domain of new generation mobile communication.

“IPv6 is the future Corner stone technology to rule the World”

The availability of so many possible addresses makes IPv6 the only realistic technology to serve the future needs and make the real goal of end to end IP model possible. The inherit features of QoS and security in IPv6 will boost the deployment of new innovative applications. These two features are necessary for Pakistan’s future eCommerce, eLearning, eHealth and eGovernment facilities.

The expanded address space together with more efficient and robust mobility (Mobile IPv6) model is especially important in the context of the proliferation of more and more sophisticated mobile communication devices.

The main feature of IPv6 described above as well as other like Stateless AutoConfiguration will enable creation of new application and services only limited by our imagination. IPv6 is essential to ensuring the growth and development of tomorrow’s internet.

IPv6 Deployment in Pakistan

With the goal of spreading IPv6 to every end user, major Pakistani ISPs (CYBERNET, SUPERNET & DANCOM) stands together with Pakistan IPv6 Task Force to work for the deployment of IPv6 in Pakistan. All of these ISPs previously working individually for IPv6 Testing at their ends, now working under the umbrella of Pakistan IPv6 Task Force and all of them extend their test bed to International and National boundaries.



Pakistan IPv6 National Core Project – 6Core

6Core stands for "IPv6 National Core." which is the First IPv6 based project initiated by ISPs of Pakistan under the common platform of Pakistan IPv6 Task Force. The 6Core is a test-bed network that was started in 2006 by the CYBERNET, SUPERNET, DANCOM and IPv6 Forum Pakistan to take one step towards transition from IPv4 to IPv6.

In this regard the base of IPv6 Task Force has been presented which work for the promotion of IPv6 deployment in ISP/NSP, Education and research institutes, Corporate and Government sectors. This project is limited to Pakistan based network only.

Another goal of the 6Core was to test the IPv6 implementations and network services to provide feedback to developers and protocol designers of IETF, then the 6Core deploy and test to validate operational procedures and test transition and coexistence mechanisms.

The whole work will be built around the adaptation of Best practices of IPv6 and slowly test and migrate all the possible services currently running in Pakistan over IPv4 to IPv6 Network. Finally we will provide Standard Operation Procedures (SOP) to the enterprises and other organizations to easily and seamlessly migrate their existing IPv4 network to new required IPv6 network.

The 6Core is informally operated by the Pakistan IPv6 Task Force along with the IPv6 Forum Pakistan and it is managed on a collaborative, best-effort basis by its Nationwide ISP/NSPs, Educational institutes etc.

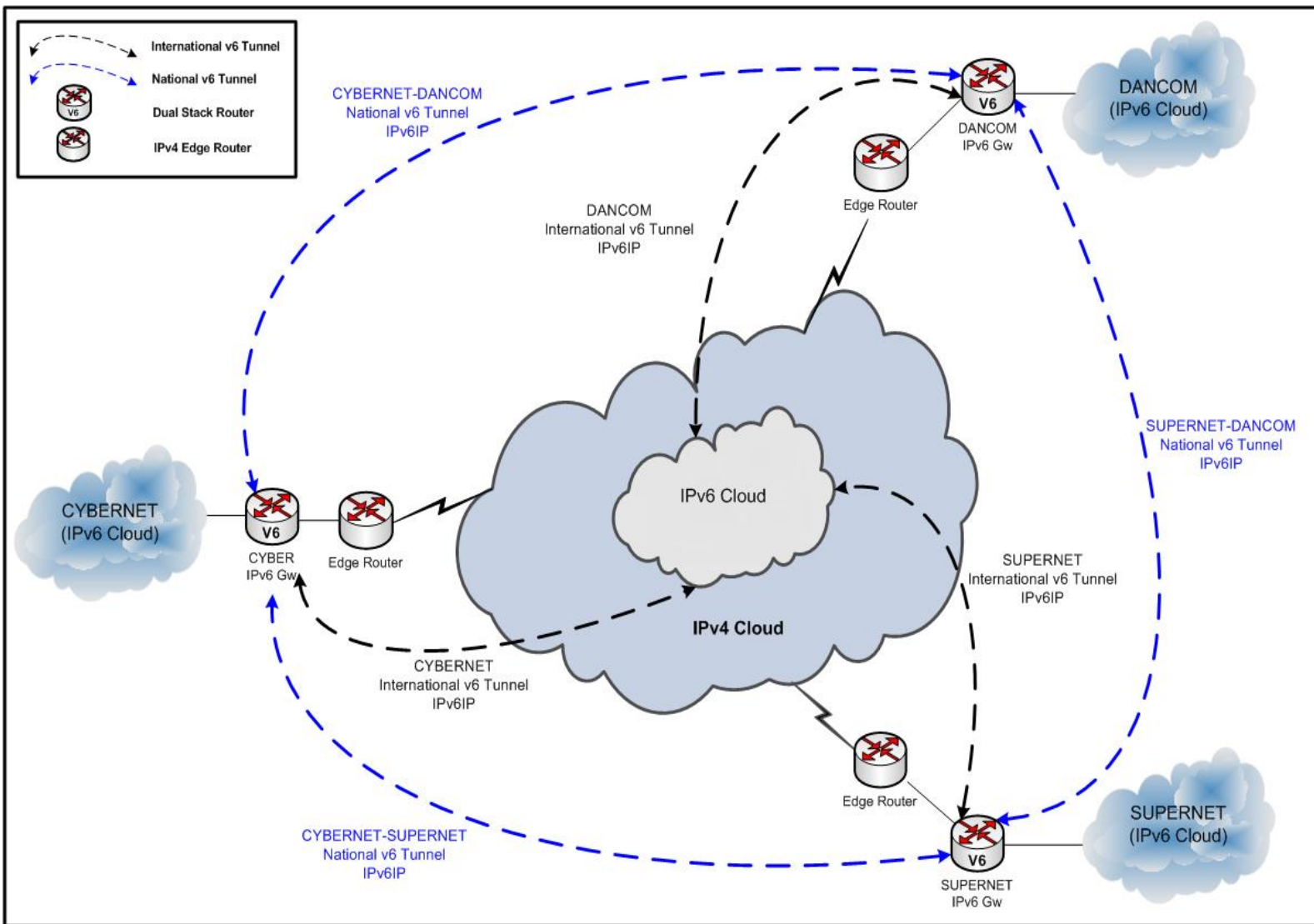
The project also has the support of market leaders that helps Pakistan's Engineers to work in parallel with the International organizations promoting IPv6. Haris Shamsi and Fahad Ali Khan (CYBERNET), Tariq Mustafa and Hasan Asghar (SUPERNET), Shiraz Malik and Zaeem Arshad (DANCOM), are the current members of 6Core Project.

This project is open for all the ISP/NSP, Enterprise and Educational and Research Institutes of Pakistan to take active participation. The participation procedure has been mentioned at www.ipv6tf.org.pk or participation request can be submitted on fahadak@cyber.net.pk or h.shamsi@cyber.net.pk.



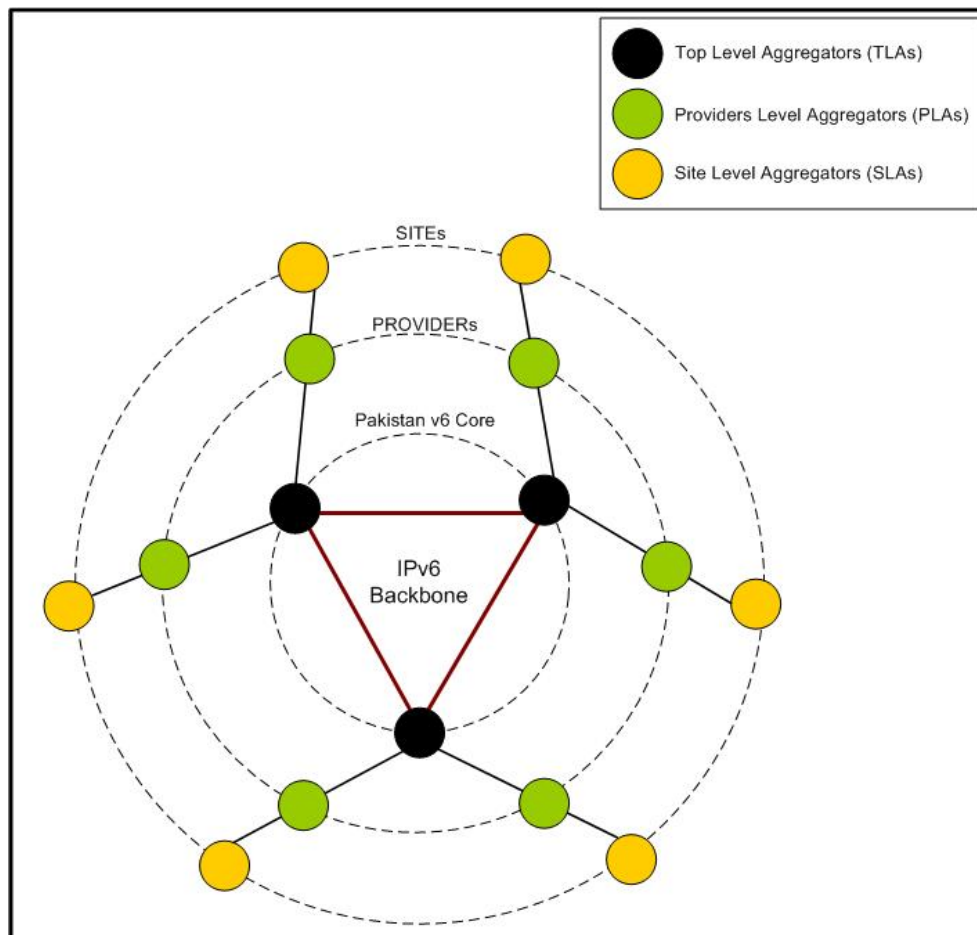
The 6Core Network

The 6Core is a network of IPv6 clouds present in Pakistan to share Information without going to International IPv6 Cloud. The links between these IPv6 clouds on the 6Core are made using IPv6. The IPv6 protocol currently is carried over IPv6 over IPv4 Tunnels because of unavailability of IPv6 WAN (Native) connectivity in Pakistan NAPs (FLAG Telecom, ITI PIE).



On 13 September 2006, the 6Core started as a virtual network over the IPv4 Internet using IPv6-over-IPv4 tunnels to enable easy IPv6 connectivity and peering between IPv6 networks of CYBERNET, DANCOM and SUPERNET. Later, this links will be shifted to native IPv6 links which is our ultimate goal. Also Past experience on the IPv4 Internet such as with the Mbone (multicast datagrams over the IPv4 Internet) suggested the deployment of IPv6-over-IPv4 tunnels until all links are converted to native IPv6 links.

The 6Core topology is a hierarchy of providers and their corresponding Sites. This hierarchy is shown in Figure 2; the first level of the hierarchy consists of 6Core's backbone nodes which are the ISP taking part in direct connectivity between each other over IPv6, representing the Top-Level Aggregators (TLAs). These first-level nodes (TLAs) are called aggregators because they must aggregate the IPv6 traffic of all their downstream customers and announce only a few IPv6 prefixes (/32) on the 6Core. Aggregation is necessary as aggregation of routes in IPv6 promotes efficient and scalable routing to the IPv6 Internet.



The TLAs peer with other TLAs using BGP4+ to exchange their IPv6 routes. The peering between the TLAs on the 6core currently done over IPv6-over-IPv4 tunnels but they will be shifted to native in future.

To form this hierarchy we first need to deploy IPv6 Core network between TLAs. CYBERNET, SUPERNET and DANCOM are the initial TLAs who connect themselves over IPv6.

Second level of hierarchy defines IPv6 providers of Pakistan who cannot reach to IPv6 World directly. They will connect to TLAs and get connected to IPv6 zone.



They need to acquire IPv6 CIDR from APNIC and get connected to TLAs either using BGP4+ which is preferred and if not then static. These providers are the IPv6 service providers to the end consumers; TLAs can also provide IPv6 services directly to their customers. Providers also follow the aggregation rule.

Finally the last level of hierarchy is Site Level Aggregator (SLAs) which are the IPv6 customers. They will preferably be over native IPv6 connection but due to unavailability of native IPv6 services in Pakistan IPv6 traffic can be tunneled.

Phases of 6Core

This whole project is broken into phases and in each phase number of tasks and tests will be proposed, which will be implemented in each domain separately and then integrated to each other over National v6 Backbone. Most of these tests are already been done at very high scale in other IPv6 projects like 6bone, moonv6 etc. The goal of this project is to educate people of Pakistan about the future needs and get ready them to face the new challenges.

The phases proposed are,

Phase I:

- Every TLA ISP will initiate single IPv6 Tunnel with all other TLA ISPs in Pakistan to establish IPv6 tunnel ring.
- Every TLA will advertise its /32 CIDR only (No v6 Transit services will be offered between TLAs).
- IPv6 Tunnel will be used only for IPv6 traffic (unicast/multicast) only.
- BGP4 neighborship will be created over National IPv6 tunnels.
- For international IPv6 traffic every TLA will forward it to their International IPv6 Tunnel provider.

Phase II:

- Every ISP will launch www6, DNS and FTP services over IPv6 in their Testbeds.
- Services like TFTP, Telnet and SSH, and DHCPv6 will be tested.
- ICMPv6 functions verification i.e. ICMPv6 Echo Request, Reply and Redirect, ICMP "hop limit exceeded," Neighbor Unreachability Detection, Path MTU Detection and Fragmentation/Reassembly, Address Autoconfiguration, Duplicate Address Detection, Multiple Prefixes, and Network Renumbering.

Phase III:

- Multiple v6 Tunnel between the ISP (based on major regions KHI/LHR/ISB only).



- Every ISP will relax the prefix filter policy to /32 upto /48 to implement BGP4 Multi-homed Traffic Engineering.
- Routing Protocol performance “OSPFv3, ISIS and BGP4+” will be tested.
- Different Tunnel scenarios i.e. static tunnels, 6to4, ISATAP, Teredo and Tunnel Broker will be tested.

Phase IV:

- IPv6 over DSL (IPoA/PPPoE) will be test.
- IPv6 over WiFi will be test.
- IPv6 over dialup/DXX/Ethernet and other lastmiles with different Layer2 Encapsulations will be test.
- Different client scenarios will be implemented over Native IPv6 links between providers and Sites.

Phase V:

- QoS implementation will be test.
- 6PE and 6VPE will be test.
- Voice over IPv6 will be test.
- Firewall and other security features will be test.

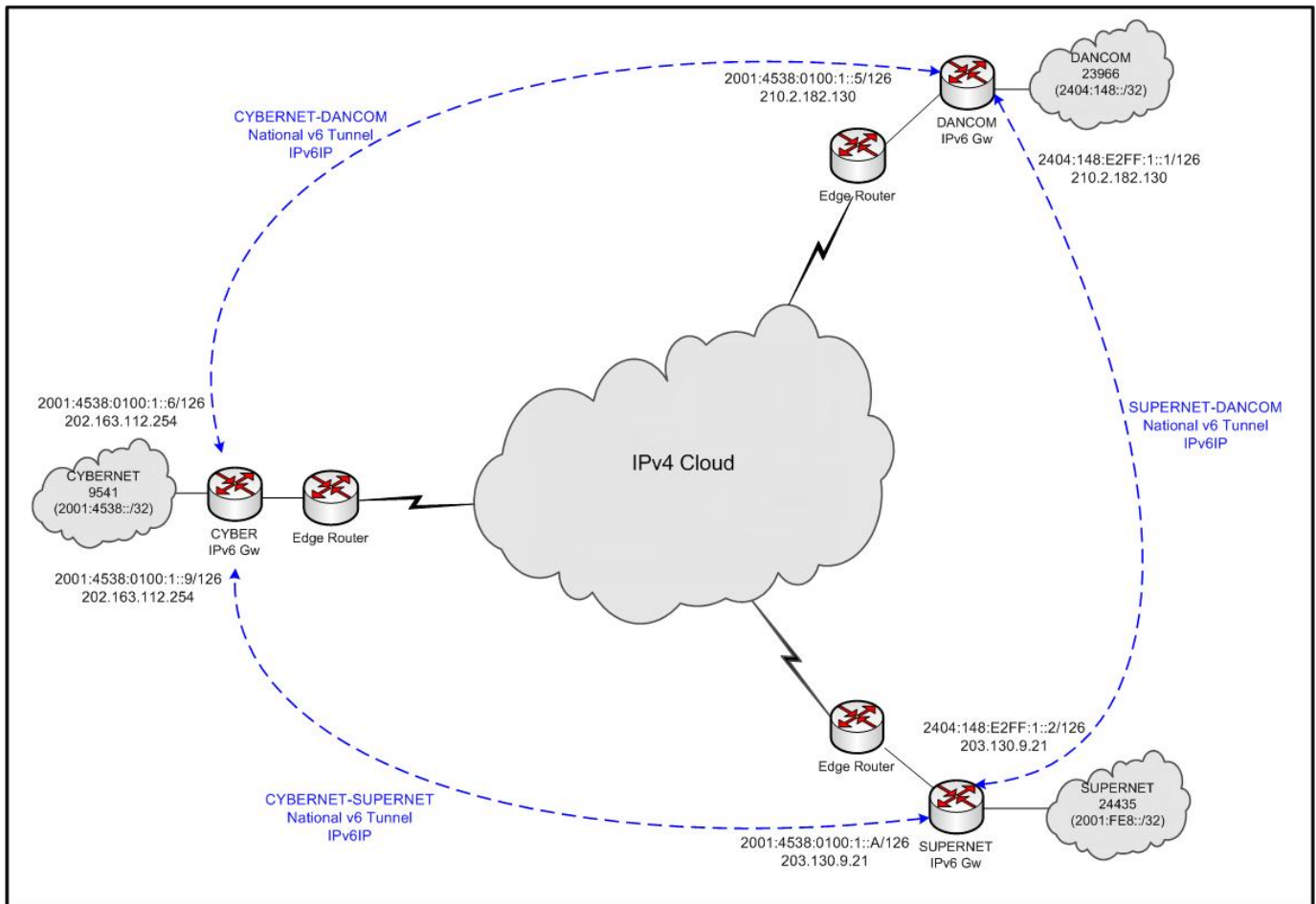
Further phases will be decided later and modifications in these phases are also possible.

IPv6 National Backbone Ring

The project started with the joining hands of three biggest ISP of Pakistan CYBERNET, DANCOM and SUPERNET. All of them take their efforts and use the platform of IPv6 Task Force to build the Pakistan’s virtual IPv6 backbone. This initial setup is to build the IPv6 National Backbone Ring between these three ISPs. This Ring is established on the IPv6 over IPv4 Tunnels (protocol 41).

The 6Core topology is the conceptual view of this backbone, but the architecture of the 6Core will be established and grow over the time with a diversity of links. The Top Level Aggregators (TLAs) on the 6Core (currently CYBERNET, DANCOM and SUPERNET) are connected using tunnels over the IPv4 Internet.

These TLA list is not fixed, it is open for all other ISP/NSP to join this Project and actively participate in promotion of IPv6 in Pakistan. These TLAs will provide IPv6 Native or Tunnel IPv6 connectivity to other ISP/NSPs, educational and research institutes, organizations and government sectors.



Following are the sample configuration for IPv6IP tunnels,

CISCO

```
interface Loopback1
description *** Loopback Interface ***
ip address A.B.C.D 255.255.255.255

interface Tunnel100
description *** IPv6 Tunnel ***
ipv6 address XXXX:XXXX::X/126
ipv6 enable
tunnel source Loopback1
tunnel destination A.B.C.D
```

JUNIPER

```
interfaces lo0
description " *** Loopback Interface *** ";
unit 0 {
```



```
family inet {
    address A.B.C.D /32;
}
}
interfaces ip-0/2/0
unit 0 {
    description "*** IPv6 Tunnel ***";
    point-to-point;
    tunnel {
        source lo0;
        destination A.B.C.D;
    }
    family inet6 {
        address XXXX:XXXX::X/126;
    }
}
```

CYBERNET – DANCOM Connectivity:

Following are the details for establishing v6 Tunnel between CYBERNET and SUPERNET.

- Connection Type: ipv6ip Tunnel (ipip Protocol 41) Circuit.
- Tunnel ID: CYB-DCom_v6-Tunnel
- CYBERNET IPv6 End Point: 2001:4538:0100:1::6/126
- DANCOM IPv6 End Point: 2001:4538:0100:1::5/126
- CYBERNET IPv4 End Point: 202.163.112.254
- DANCOM IPv4 End Point: 210.2.182.130

CYBERNET end

```
interface Loopback1
description *** Loopback Interface ***
ip address 202.163.112.254 255.255.255.255

interface Tunnel100
description *** IPv6 Tunnel to DANCOM ***
ipv6 address 2001:4538:100:1::6/126
ipv6 enable
tunnel source Loopback1
tunnel destination 210.2.182.130
tunnel mode ipv6ip
```

DANCOM end

```
interface Loopback1
description *** Loopback Interface ***
ip address 210.2.182.130 255.255.255.255
```



```
interface Tunnel100
  description *** IPv6 Tunnel to CyberNet ***
  ipv6 address 2001:4538:100:1::5/126
  ipv6 enable
  tunnel source Loopback1
  tunnel destination 202.163.112.254
  tunnel mode ipv6ip
```

CYBERNET – SUPERNET Connectivity:

Following are the details for establishing v6 Tunnel between CYBERNET and SUPERNET.

- Connection Type: ipv6ip Tunnel (ipip Protocol 41) Circuit.
- Tunnel ID: CYB-SN_v6-Tunnel
- CYBERNET IPv6 End Point: 2001:4538:0100:1::9/126
- SUPERNET IPv6 End Point: 2001:4538:0100:1::A/126
- CYBERNET IPv4 End Point: 202.163.112.254
- SUPERNET IPv4 End Point: 203.130.9.21

CYBERNET end

```
interface Loopback1
  ip address 202.163.112.254 255.255.255.255

interface Tunnel150
  description *** IPv6 Tunnel to SuperNet ***
  ipv6 address 2001:4538:100:1::9/126
  ipv6 enable
  tunnel source Loopback1
  tunnel destination 203.130.9.21
  tunnel mode ipv6ip
```

SUPERNET end

```
interface Loopback1
  ip address 203.130.9.21 255.255.255.255

interface Tunnel150
  description *** IPv6 Tunnel to CyberNet ***
  ipv6 address 2001:4538:100:1::A/126
  ipv6 enable
  tunnel source Loopback1
  tunnel destination 202.163.112.254
  tunnel mode ipv6ip
```



SUPERNET – DANCOM Connectivity:

Following are the details for establishing v6 Tunnel between DANCOM and SUPERNET.

- Connection Type: ipv6ip Tunnel (ipip Protocol 41) Circuit.
- Tunnel ID: CYB-DCom_v6-Tunnel
- DANCOM IPv6 End Point: 2404:148:E2FF:1::1/126
- SUPERNET IPv6 End Point: 2404:148:E2FF:1::2/126
- DANCOM IPv4 End Point: 210.2.182.130
- SUPERNET IPv4 End Point: 203.130.9.21

DANCOM end

```
interface Loopback1
 ip address 210.2.182.130 255.255.255.255

interface Tunnel200
 description *** IPv6 Tunnel to SuperNet ***
 ipv6 address 2001:4538:100:1::9/126
 ipv6 enable
 tunnel source Loopback1
 tunnel destination 203.130.9.21
 tunnel mode ipv6ip
```

SUPERNET end

```
interface Loopback1
 ip address 203.130.9.21 255.255.255.255

interface Tunnel200
 description *** IPv6 Tunnel to DANCOM ***
 ipv6 address 2001:4538:100:1::A/126
 ipv6 enable
 tunnel source Loopback1
 tunnel destination 210.2.182.130
 tunnel mode ipv6ip
```

BGP4+ Neighborhood

All these TLAs have created BGP4+ neighborhood over configured IPv6 in IPv4 tunnels. Over this BGP session their IPv6 prefixes will be exchange. Parameters configured for BGP4+ neighborhood are,



CYBERNET

ASN: 9541

IPv6 CIDR: 2001:4538::/32

Authentication Type: MD5

```
router bgp 9541
  no bgp default ipv4-unicast
  neighbor 2001:4538:100:1::5 remote-as 23966
  neighbor 2001:4538:100:1::5 password 7 *****
  neighbor 2001:4538:100:1::A remote-as 24435
  neighbor 2001:4538:100:1::A password 7 *****
address-family ipv6
  neighbor 2001:4538:100:1::5 activate
  neighbor 2001:4538:100:1::A activate
network 2001:4538::/32
```

SUPERNET

ASN: 24435

IPv6 CIDR: 2001:fe8::/32

Authentication Type: MD5

```
router bgp 24435
  no bgp default ipv4-unicast
  neighbor 2404:148:E2FF:1::1 remote-as 23966
  neighbor 2404:148:E2FF:1::1 password 7 *****
  neighbor 2001:4538:100:1::9 remote-as 9541
  neighbor 2001:4538:100:1::9 password 7 *****
address-family ipv6
  neighbor 2404:148:E2FF:1::1 activate
  neighbor 2001:4538:100:1::9 activate
network 2001:fe8::/32
```

DANCOM

ASN: 23966

IPv6 CIDR: 2404:148::/32

Authentication Type: MD5

```
router bgp 23966
  no bgp default ipv4-unicast
  neighbor 2404:148:E2FF:1::2 remote-as 24435
  neighbor 2404:148:E2FF:1::2 password 7 *****
  neighbor 2001:4538:100:1::6 remote-as 9541
  neighbor 2001:4538:100:1::6 password 7 *****
address-family ipv6
  neighbor 2404:148:E2FF:1::2 activate
  neighbor 2001:4538:100:1::6 activate
network 2001:fe8::/32
```



Routing Policies

The routing policy for the 6Core is according to the policy of 6bone i.e. described in RFC 2772. This policy was defined and designed to maintain the stability of routing on the 6Core by having a common set of rules and guidelines.

The routing policy has to be applied by 6Core providers and by all TLAs. The routing policy contains the following rules:

- **Prohibited address ranges**— Specific ranges of addresses such as link-local, site-local, multicast, and loopback, of the whole IPv6 space must not be advertised by TLAs on the 6Core. Following are the prohibited address ranges on the 6NBone.
 - **Link-local prefix (FE80::— Because the link-local prefix is for a local scope purpose only, it must not be advertised on the 6Core by TLAs.**
 - **Site-local prefix (FEC0::— Because the site-local prefix is for a site local scope purpose only, it must not be advertised on the 6Core by TLAs.**
 - **Multicast prefix (FF00::— Because the multicast prefix is used only in a multicast context, multicast addresses must not be advertised by TLAs in a unicast IPv6 routing domain (6Core).**
 - **Loopback and unspecified**— The 1/128 (:::1) and ::0/128 (::) prefixes must not be advertised on the 6Core.
 - **IPv4-compatible prefix (:::/96)**— The IPv4-compatible prefix is for automatic tunneling. It has no need to change the IPv6 routing domain (6Core), so it must not be advertised on the 6Core.
 - **IPv4-mapped prefix (::FFFF:d.d.d.d/96)**— Because the IPv4-mapped prefix is used internally in the applications, there is no need to change the IPv6 routing. Thus, the IPv4-mapped prefix must not be advertised on the 6Core.
 - **Default route**— Because a TLA must be default-free, the default route must not be advertised on the 6Core by any TLA.
 - **Other unicast prefixes**— Any other unicast prefixes from undefined or unallocated prefixes by any RIRs that are not defined in the permitted announcement must not be advertised on the 6Core.
- **Legal prefix lengths**— Allocation of prefixes to TLAs on the 6Core changed over time. The policy defines the maximum length of prefixes announced on the 6Core. The prefix lengths vary from /32 through /48.
- **Guidelines for enforcement**— These are the guidelines for the enforcement of the routing policy. Organizations connected on the 6Core commit to implement the 6Core's rules and policies, they should report any issues and problems detected to the 6Core Operations Group



(Pakistan IPv6 Task Force) over v6ops-pk@nsp.org.pk, and they are responsible for working toward the problem's resolution.

Recommended BGP Filter

CISCO

```
ipv6 prefix-list ipv6-ebgp deny 3ffe::/16 le 128
ipv6 prefix-list ipv6-ebgp deny 2001:db8::/32 le 128
ipv6 prefix-list ipv6-ebgp permit 2001::/32
ipv6 prefix-list ipv6-ebgp deny 2001::/32 le 128
ipv6 prefix-list ipv6-ebgp permit 2002::/16
ipv6 prefix-list ipv6-ebgp deny 2002::/16 le 128
ipv6 prefix-list ipv6-ebgp deny 0000::/8 le 128
ipv6 prefix-list ipv6-ebgp deny fe00::/9 le 128
ipv6 prefix-list ipv6-ebgp deny ff00::/8 le 128
ipv6 prefix-list ipv6-ebgp permit 0::/0 le 48
ipv6 prefix-list ipv6-ebgp deny 0::/0 le 128
```

Juniper

```
policy-statement ipv6-ebgp-relaxed {
  from {
    family inet6;
    route-filter 3ffe::/16 orlonger;
    route-filter ::/8 orlonger;
    route-filter 2001:db8::/32 orlonger;
    route-filter 2001::/32 exact next policy;
    route-filter 2001::/31 longer;
    route-filter 2002::/16 exact next policy;
    route-filter 2002::/16 longer;
    route-filter fe00::/9 orlonger;
    route-filter ff00::/8 orlonger;
    route-filter ::/0 upto /48 next policy;
  }
  then reject;
}
```

Becoming a TLA on the 6Core

It is possible for providers and ISPs to qualify as TLAs on the 6Core. 6Core Backbone Routing Guidelines defines the rules, criteria, and policy for becoming a TLA on the 6Core:

- To become a TLA, the applicant must be ISP with reachability in major areas of Pakistan. The applicant ISP must have its IPv6 CIDR registered with APNIC.

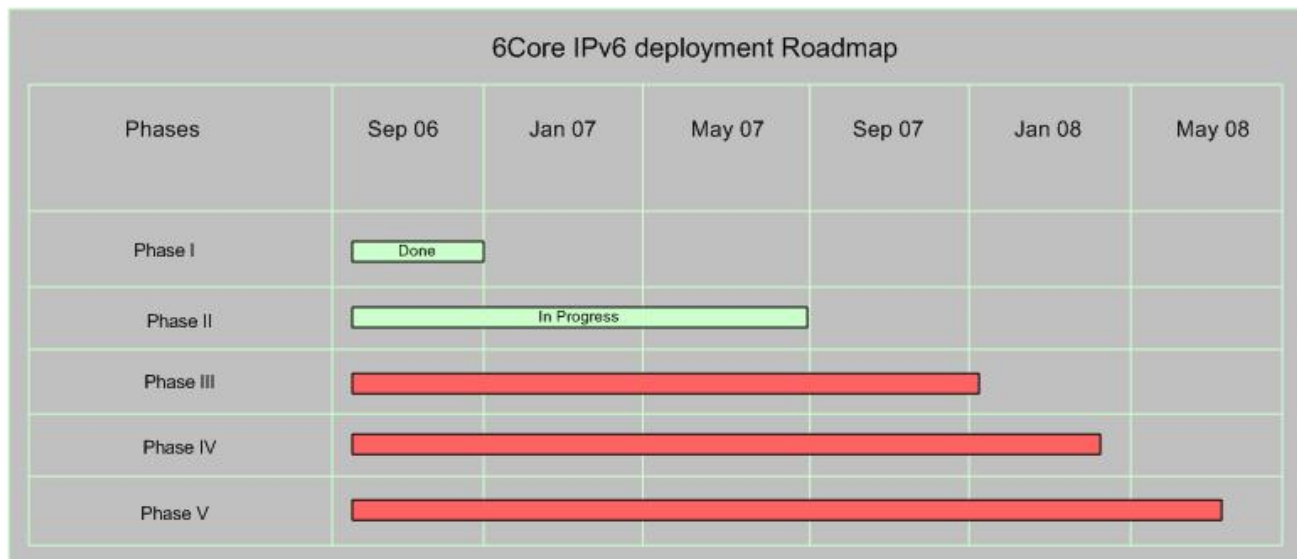


Pakistan IPv6 National Core Project

- BGP4+ peering need to be created with all TLAs
- Maintained AAAA and PTR records for its border router in a local DNS server
- Maintained an IPv6-accessible system providing at least one web page or more of information
- The applicant must have the ability and the intent to provide "production-quality" 6Core backbone service. More specifically, the applicant must claim to have the support staff and tools to operate as a TLA.
- The applicant must have potential end users who would be served by it as a TLA.

Current Status

As Engineers continues on its bold mission to promote IPv6 throughout the world, the 6Core project has got strong position in Pakistan. IPv6 is penetrating in Pakistani's ISPs and Organizations far more than any other Asian Country. Progress of Phase 1 has been completed and Phase 2 is in progress.

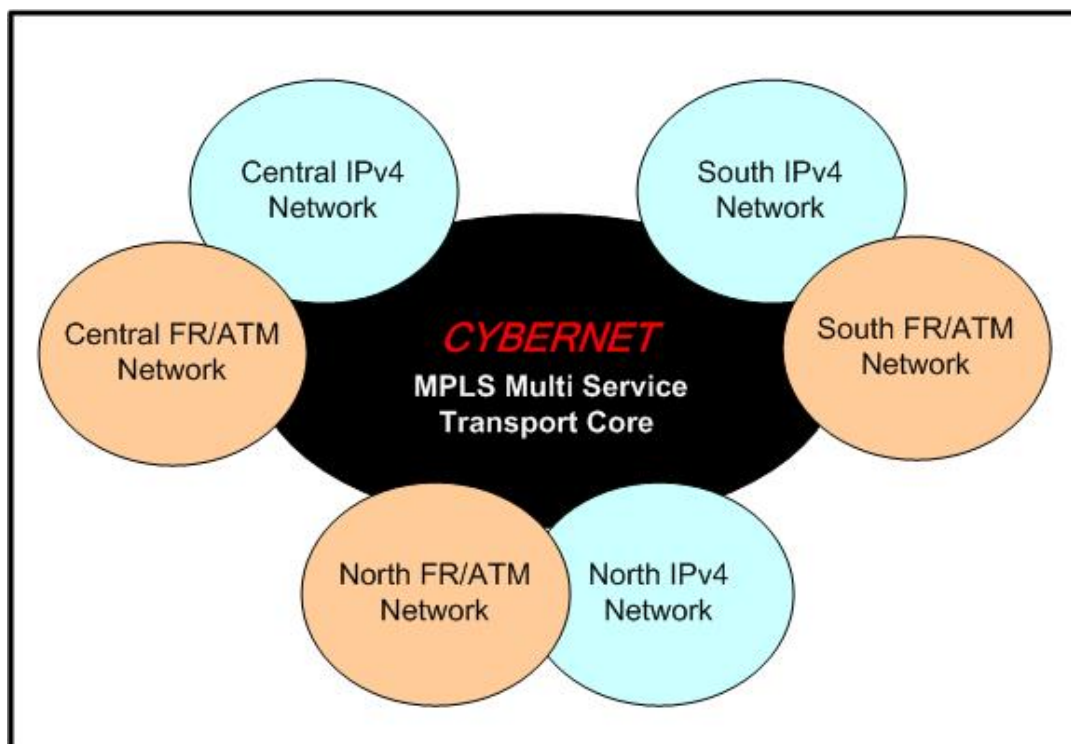


IPv6 in CYBERNET

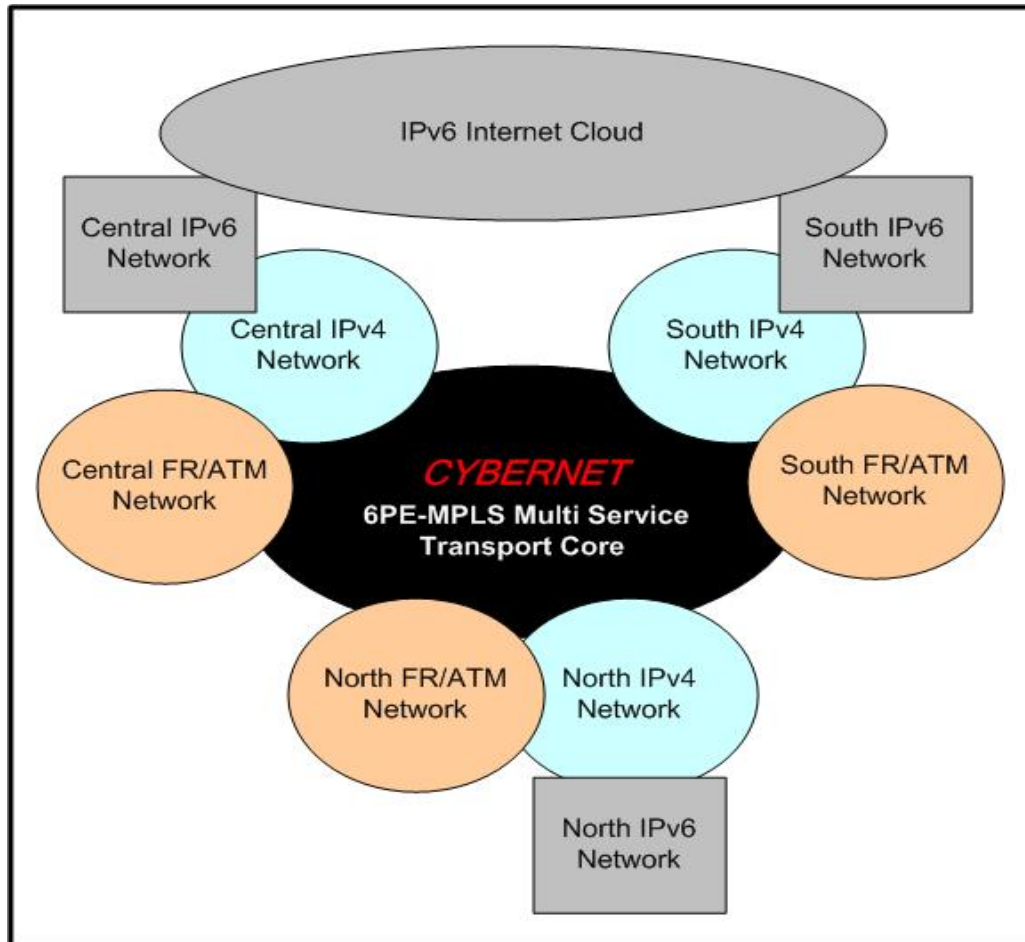
CYBERNET has started offered Internet and Data communication services back in 1997 and since then extends its network all over the Pakistan.

CYBERNET has registered with APNIC for IPv6 on March 2006. CYBERNET has allotted with 2001:4538::/32 CIDR. CYBERNET has started R&D on IPv6 test bed just after the allocation of IPv6 CIDR and appears in IPv6 World map after establishing IPv6 Tunnel with Occaid in September 2006.

CYBERNET has MPLS enabled Core to established multi-service platform. All the services ATM, FR, VLAN, PPP and HDLC are integrated over MPLS Core.



CYBERNET ultimate goal is to achieve end to end IPv6 service enabled in it Access/Distribution/Core. To get this we have two options either built parallel network over IPv6 and migrate every service over IPv6 one by one but this is not suitable in terms of Cost and service disruption.



Second one is recommended and most suitable that to initially go for Dual Stack Core than integrate Dual Stack Distribution and Access Network to IPv6 enabled Core.

Co-existence is the only solution; it will lead to stability and reliable migration from IPv4 network to IPv6 network.

CYBERNET is using OSPFv2 as IGP and it will lead to important design decision that either go for OSPFv3 or ISIS. Migrating whole CYBERNET Nation-wide network over ISIS is not a easy task and cannot be done in hurry. For early deployment OSPFv3 is the best solution and then when CYBERNET going to offer all IPv6 services to end customers and IPv6 routing table increased to the level that impact on services due to dual IGP SPF trees and its calculation, we will go for ISIS. Till then OSPFv3 along with iBGP is the best solution.

Deployment of IPv6 in CYBERNET has been broken down in to number of phases. List of these phases shown below,

Phase I: Registration with APNIC for IPv6 CIDR.



- Phase II:** Building of IPv6 Test bed in KHI, LHR and ISB separately.
- Phase III:** Building First IPv6 Tunnel ring between KHI, LHR and ISB PoPs.
- Phase IV:** Building International IPv6 Tunnel with v6 Tunnel Service Provider.
- Phase V:** Launching of www6 and DNS6 services over Dual Stack Servers.
- Phase VI:** Launching of Dual Stack Media Server.
- Phase VII:** Building National IPv6 Tunnels between Pakistan v6 ISP/NSP.
- Phase VIII:** Establishing 6PE over CYBERNET MPLS Core.
- Phase IX:** Testing of IPv6 over xDSL.
- Phase X:** Testing of 6VPE over CYBERNET MPLS Core.
- Phase XI:**

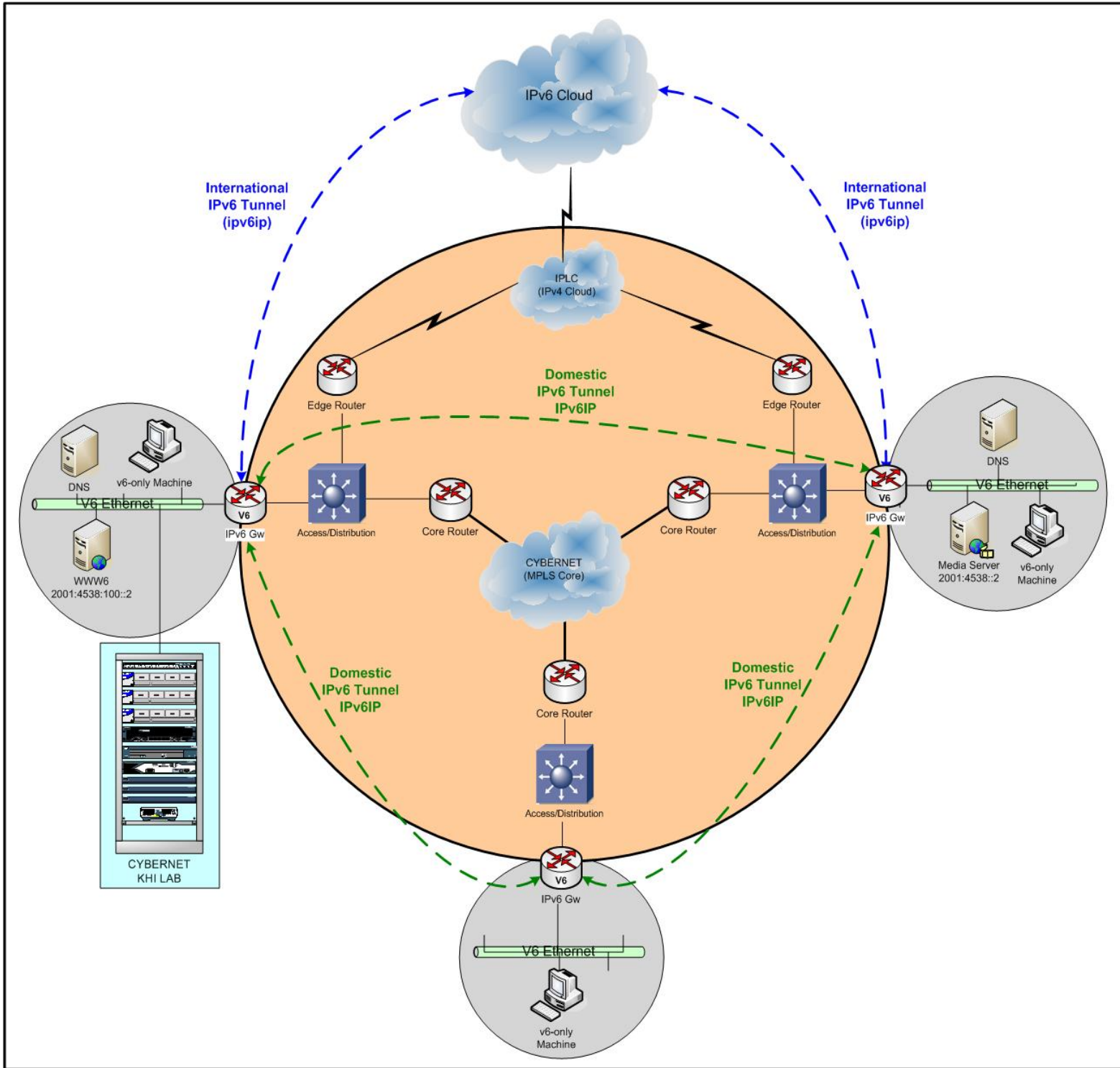
After registering to APNIC on March 2006, CYBERNET backbone interconnect its national testbeds, collectively formed one of the largest IPv6 network in the Pakistan. This provided plenty of scope for trialing the new technology, testing interoperability with existing networks, and demonstrating services and applications.

The CYBERNET IPv6 network consisted of a set of national IPv6 enable PoPs connected over MPLS backbone and a set of access circuits which is currently an ethernet network, is a native connections plus some tunneled connections to test LAB routers and PCs.

In total, there were 3 IPv6 enabled PoPs which are Karachi, Lahore and Islamabad. Each of them is connected via a manual IPv4-to-IPv6 tunnel. In Karachi IPv6 Network we have dual stack www6 & DNS servers and test LAB with number of IPv6 enable routers and machines.

In Lahore we have dual stack Media & DNS servers along with the test v6 LAB of LHR itself. In Islamabad we have IPv6 enable segment which is connected to ISB v6 Test LAB.

Figure 6: CYBERNET IPv6 Testbed Network





Addressing Scheme

CYBERNET obtained an IPv6 subTLA of 2001:4538::/32 for its nationwide network. From this IPv6 address space a sub-section was used for IPv6 Testbeds. The allocated Testbeds address space is,

- ✓ LHR IPv6 Testbed address space: '2001:4538::/40'
- ✓ KHI IPv6 Testbed address space: '2001:4538:01::/40'
- ✓ ISB IPv6 Testbed address space: '2001:4538:02::/40'

The CYBERNET testbed address spaces have been divided into logical sub portions to facilitate future expansions and enable simpler summarization rules when required.

The address range can be seen as:

32 Bits	8 Bits	8 Bits	16 Bits
CYBERNET subTLA	Mega PoPs	PoPs	SLA
	/32	/40	/48
			/64

CYBERNET IPv6 CIDR has been broken into three level hierarchies i.e. initial 8 bit is for the assignment of Mega PoPs where all Mini PoPs connected, than we can assign /48 to each Mini PoP from Mega PoP's /40.

To summarize, the assigned IPv6 address consists of the following parts:

Structure = <MPoP>.<PoP>.<SLA>

Where:

<MPoP> = Address assignment to Mega PoPs (KHI/LHR/ISB)

<PoP> = assigned address range per PoP

<SLA> = segmentation of use within the PoP (SLA =Site Level Aggregate)

Subnet Size

Since IPv6 has a default subnet size of 64 bits, to allow Stateless Autoconfiguration to operate, a question arises over the size of network used for point-to-point links.

A /127 size prefix might intuitively be used, but in practice this may not be practical because of the potential use of (additional) subnet-router anycast addresses. This issue is discussed in [RFC3627], which recommends the use of either /112 or /64 or /126 prefixes for point to point links.



CYBERNET IPv6 network initially go for /126 for all type of Point-to-Point links in the Testbeds around Pakistan.

CYBERNET Testbed Connectivity

CYBERNET has built three separate Ipv6 testbeds in Karachi, Lahore and Islamabad. To interconnect them over existing IPv4 based MPLS Core, number of options available which are,

- Using IPv6 over IPv4 Tunnel
- Using MPLS L2VPN (Martini/Kompella)
- Using BGP/MPLS L3VPN

All solutions are feasible but there are some initial hurdles to jump of direct native IPv6 implementation in CYBERNET Core. But this is our ultimate goal to migrate IPv4 core to IPv6 Core through transitions state of Dual Stack implementation.

MPLS L2VPN solution is also very safe solution as it is independent of Layer 3 Protocol of Core, but this decision is also dropped over IPv6 over IPv4 tunnels which are mostly deployed transition procedures applied worldwide.

IPv6 over IPv4 Tunnels can be deployed in number of ways i.e,

- Using IPv6IP – Protocol 41
- Using IPv6 over GRE
- Teredo Tunneling
- ISATAP
- Tunnel Brokers
- 6to4 Tunnels

Also there are some translations procedures are also available, but they highly depreciated,

- NAT-PT
- SIIT
- SOCKS
- ALGs
- Bump-in-the-Stack/API

CYBERNET chooses the IPv6 in IPv4 tunnel technique which use protocol 41 to implement tunnel over IPv4 backbone and transport IPv6 traffic over IPv4 backbone.



IGP Routing

The options available for an IGP routing protocol within CYBERNET are: static routing, RIPv6, OSPFv3 or IS-IS. The option 'static routing' would have been very difficult to manage in practice, and would not have been very scalable. The dynamic routing options available are 'RIPv6', 'OSPFv3' and 'IS-IS'.

RIPv6 is a distance vector routing protocol while 'OSPFv3' and 'IS-IS' is a link-state protocol. Although a distance vector routing protocol is easier to troubleshoot and the operation simpler to understand, it was preferred to utilize a link-state protocol due to its advantages in convergence, tuning and additional features (like opaque information, enhanced TLV (Type/Length, Value) information for Traffic Engineering, etc.).

CYBERNET chooses OSPFv3, to gradually implement IPv6 in the presence of IPv4 network. If CYBERNET choose ISIS than it has to enable IPv6 on all of its nodes and it won't be suitable for gradually deployment of IPv6 network.

EGP Routing

CYBERNET has established its International BGP neighborship with Occaid and become visible to IPv6 Internet World on 19 November 2006. BGP4+ is the only available and most scalable Exterior Routing Protocol. Since Native IPv6 transit is not available in Pakistan therefore to exchange Routing information, BGP4+ neighborship is established over IPv6 over IPv4 Tunnel (ipv6ip-Protocol 41) with MD5 authentication to secure IPv6 Routing updates over BGP4+ session.

As a part of 6Core project, BGP4+ neighborship is also created with DANCOM and SUPERNET over IPv6 over IPv4 (ipv6ip-protocol 41) tunnels.

CYBERNET multihomed its IPv6 network by creating BGP4+ neighborship with three different neighbors from two different locations i.e. in Karachi it is Occaid and in Lahore Lava.Net and UK6x. CYBERNET is advertising its /32 CIDR to both v6 providers and return traffic path is preferred via AS-Path list.

IETF presents IPv6 as the highly simplified and hierarchical way to manage and control routing table entries with in a domain or in the whole global routing world. This is accomplished by forcing the ISP/NSP to aggregate their network at the border with /32 CIDR only (discussed in RF 2772). But this aggressive policy lead to discontinuation of some very important multihomed traffic engineering feature of BGP4+. IETF is currently working very actively to overcome this issues and WG named multi6 was formed. It has come up with number of solutions that are still not mature much.

Most of the RIRs along with the ISP/NSP of their regions are agree to solve this issue by relaxing their prefix filters /32 to "/32 upto /48" this will help to provide



the SITE/PoP level multihoming solution but it is the responsibility of every ISP/NSP not to overwhelm Internet Routing table with all /48. Try to summarize CIRD to /32 as much as possible and advertised larger than /32 CIDR when only required e.g. when you are working on IPv6 Anycast or multihomed Traffic Engineering.

Monitoring

The addresses of all loopback and point-to-point addresses are entered into DNS in a special format. The SNMP and pinger periodically (once in five minutes) checks that the links (including the links to customers and the peers) are up and responding; if not, it sends an alert. MRTG of IPv6 Links is also created. BGP and OSPF adjacencies are also monitored using a tool which collects syslog warnings sent from routers to a central syslog server. If adjacencies or sessions flap, this can be noted in the monitoring page.

All routers and links are collected to a custom network map/monitoring tool, where the traffic levels and similar can be monitored easily. A challenge in the dual-stack infrastructure is getting a feel how much traffic on the links is IPv4 and how much IPv6. As of this writing, there are no good mechanisms to get that. When IPv6 MIBs are complete and are implemented, getting such measurements may be easier.

Other Services

CYBERNET IPv6 Testbed Network is consists of www6 servers which is a dual stack web server hosting IPv6 information resource centre.

2001:4538:100::2
www6.cyber.net.pk

CYBERNET has also launched IPv6 Dual stack Multimedia server, which can be access by following URLs,

2001:4538::2
mms://radio.ipv6.cyber.net.pk/quran
mms://radio.ipv6.cyber.net.pk/urdu
mms://radio.ipv6.cyber.net.pk/english

Current Status

CYBERNET has reached to achieve till Phase VII at 07 November 2006. And workings on other phases are in progress. The roadmap of overall IPv6 deployment in CYBERNET is shown below,



CYBERNET IPv6 deployment Roadmap

