



TELECOM REGULATORY AUTHORITY OF INDIA

Recommendations

On

Improvement in the Effectiveness of
National Internet Exchange of India (NIXI)

APRIL 20, 2007

Mahanagar Doorsanchar Bhavan
Jawahar Lal Nehru Marg
New Delhi-110002.

CONTENTS

	Page No.
Preface	3
1. Background	4
2. Interconnection issues at NIXI	6
3. Domestic Traffic routing	13
4. Segregation of traffic	16
5. Installation and interconnection of NIXI nodes	21
6. Up gradation NIXI nodes and QoS	25
7. Other Misc. Issues	28
8. Summary of Recommendations	30
Annexes	
A. Comments of Stakeholders	33
B. International Experience	38
C. TEC report on segregation of National and International Traffic	43
D. QoS recommendations on NIXI	58
E. Abbreviations	60

Preface

1. National Internet Exchange of India (NIXI) was set up on the recommendation of Telecom Regulatory Authority of India (TRAI) by Department of Information Technology (DIT), Government of India in 2003 to ensure that Internet traffic, originating and destined for India, should be routed within India.
2. NIXI's infrastructure has not been utilized optimally due to limited number of ISPs joining NIXI. Therefore a need is felt to revisit the framework of NIXI to provide impetus to effectively exchange domestic Internet traffic. Various options for improving the effectiveness of NIXI have been explored which includes direct domestic peering of Internet service providers (ISP) with International Internet bandwidth providers.
3. The Authority is aware that effective functioning of NIXI can reduce the carriage cost for domestic Internet traffic to great extent which will facilitate cheaper content download and encourage web hosting services. Accordingly, The Authority is sending these recommendations suo-motu in accordance with section 11(a)(iv) of TRAI Act 1997.
4. A light regulatory approach has been adopted at present and different options to improve effectiveness of NIXI have been recommended. It is hoped that implementation of these recommendations will improve effectiveness of NIXI platform for exchange of domestic traffic resulting in reduction of content download prices which may encourage use of broadband due to net reduction in its usage cost.

(Nripendra Misra)
Chairman

CHAPTER 1

BACKGROUND

1.1 A National Internet Exchange of India (NIXI) is a framework for Internet Service Providers (ISPs) to Peer and Exchange IP traffic with each other. The main purpose of NIXI is to facilitate exchange of Internet traffic originated and destined within the country among peering Internet Service Provider (ISP) members. The key objective of NIXI is to,

- i) Enable domestic bandwidth utilization for routing of the domestic traffic resulting in reduction in cost for bandwidth utilization.
- ii) Improvement in Quality of Services in terms of lower latency and number of hops. This will also help to effectively utilize International Internet bandwidth for routing International Internet traffic.

1.2 TRAI had set up a Task Force in 2002 having experts from various Agencies/Departments to examine the slow growth of internet services in the country. The recommendations of the Task Force were forwarded by TRAI to DoT in August 2002. Government broadly accepted the recommendations of TRAI and National Internet exchange of India (NIXI) was set up as a Non-profit company under Section 25 of Company's Act with initial grant from Department of Information Technology (DIT). Presently 4 nodes of NIXI are operational at Delhi (Noida), Mumbai, Kolkata and Chennai.

1.3 NIXI's infrastructure has not been utilized optimally as only 27 ISPs out of 135 operational ISPs have joined NIXI nodes at four locations. The total number of connections to NIXI from these ISPs are only 53. A lot of domestic traffic is still not routed through NIXI

defying the very purpose of setting up NIXI. There is a strong case to address the functional weak links with a view to improving the effectiveness of NIXI. Some of the burning issues like interconnection of NIXI nodes, non-announcements of routes by some major ISPs, possible misuse of NIXI's infrastructure by member ISPs for routing International traffic and opening of NIXI nodes at state capitals have been raised time and again by the majority of ISPs.

- 1.4 In order to address the above issues, a consultation process was initiated through a consultation paper on "Improvement in the Effectiveness of National Internet Exchange of India (NIXI). The open house discussions on this subject were held at New Delhi during December 2006. The comments of the stakeholders received in writing, and submissions made during open house discussions have been analyzed in detail. These are summarized in annexure 'A'. The International best practices were also examined to determine their relevance to India.
- 1.5 The Authority is aware of divergent requirements of the ISPs having International Internet gateway and ISPs not having International Internet gateway. Therefore due consideration has been given while finalizing recommendations on "Improvement in the Effectiveness of National Internet Exchange of India".
- 1.6 The recommendation on "Improvement in the effectiveness of National Internet Exchange of India (NIXI)" is being forwarded to Department of telecommunications (DoT) suo motu by the Authority in accordance with section 11(a)(iv) of TRAI Act 1997.

CHAPTER-2

INTERCONNECTION ISSUES AT NIXI

2. Interconnection of ISPs at NIXI

2.1 In spite of NIXI being setup in 2003, the number of the ISPs connected to NIXI remains limited and its infrastructure is under utilized.

2.2 The issue of effectiveness of NIXI was deliberated during 2004 also during consultation process on “Growth of Internet and Broadband Penetration”. One of the main reason for low utilization of NIXI as perceived in 2004 was that since NIXI nodes are available only at four locations and ISPs are spread across the country, the cost of taking leased line to reach to NIXI nodes and interconnect it would be prohibitively high. The overwhelming view at that time was that either NIXI nodes be setup at all state capitals or cost of leased line from ISP to nearest NIXI node be subsidized.

2.3 The Authority in its recommendation on “Growth of Internet and Broadband Penetration” during April 2004, recommended (recommendation no. 4.2.19 & 4.2.20) that

“4.2.19 Providers of backbone services, including National Long distance operators (NLDOs), Access providers and IP-II operators, should be mandated for the next two years to provide links to NIXI for ISP’s, if it is technically feasible.

4.2.20 The Government should consider for the first two years subsidizing the cost of leased lines from a Class B or C ISPs point of presence to a NIXI node for purposes of promoting inter-connection. The order of magnitude of this support could be 30 – 50%.”

2.4 The poor utilization of NIXI has compelled ISPs to carry even domestic traffic on links meant for International traffic. ISPs pay much higher charges for such links. Since there is no mechanism available to measure volumes of domestic and International traffic transacted separately on such links, even domestic traffic is charged at International bandwidth rates.

2.5 At present, there are approximately 135 operational ISPs, out of which 40 are 'A' category, 54 'B' category and 41 'C' category. Presently only 27 ISPs are connected to 4 nodes of NIXI as detailed below:

Sl no.	NIXI NODE	ISP Connected				Traffic Exchanged (In Mb)
		A	B	C	Total	
1	NOIDA	16	1	-	18*	245
2	MUMBAI	13	8	-	21	734
3	CHENNAI	11	-	-	11	134
4	KOLKATA	4	-	-	4	0.9
	Total	Connections			54	1113.9
*- Including NIC which is not an ISP						

2.6 This clearly indicates that many ISPs have not joined NIXI. This is resulting in suboptimal use of NIXI's infrastructure. Though many ISPs have stated that non availability of leased lines and non availability of the NIXI nodes at State capital level as the two key factors, there are other reasons as well for not joining NIXI.

2.7 NIXI has prescribed pre-requisites for joining. Some of the conditions are;

- i) An ISP licensed by the Department of Telecommunications, Ministry of Communications and Information Technology, Government of India can only become member.
- ii) The member ISP must have his own Autonomous System Number (AS) and use Border Gateway Protocol Version 4 and above (BGP4+) for peering.

- iii) The peering ISP must be identified at the local Internet registry of Asia Pacific Network Information Center (APNIC).
- iv) Connectivity to the NIXI will be through dedicated leased lines of sufficient capacity based on which NIXI charges will be billed.
- v) Peering ISPs will not be allowed to have NIXI facilities as a default route.
- vi) Members will ensure that use of NIXI facilities is not detrimental to other members in any way and all equipments used are compliant with Internet Engineering Task Force (IETF) standards.

2.8 The key factors for ISPs not joining at NIXI are;

- i) Most of the ISPs do not have Autonomous System (AS) number while it is mandatory for connectivity at NIXI.
- ii) Cost of dedicated link to connect individual ISPs to NIXI is prohibitively high.
- iii) Some of the ISPs, which are connected at NIXI, do not announce and accept all routes. This defeats the very purpose of new ISPs to join at NIXI.

The above reasons have been dealt in the following paragraphs.

2.9 AS Number

2.9.1 As per the present NIXI policy, AS number has been mandated to connect at NIXI to facilitate BGP4 + Sessions between connecting ISPs but AS number is not a mandatory requirement to obtain ISP license as per present licensing conditions. Therefore only those ISPs who are having their AS number can get connected at NIXI.

2.9.2 There are two options to obtain AS number from APNIC:

- (i) As non-member of APNIC
- (ii) AS member of APNIC

Only those ISPs are eligible to obtain AS number who fulfills following criteria:

- ISP is Multi-homed

- ISP has a single, clearly defined routing policy that is different from its providers routing policy.

An ISP, who is non member of APNIC, has to pay US\$ 500 as one time fee and US\$ 50 per year to obtain AS Number. This does not include allocation of any IP address. An ISP who is a member of APNIC has to pay member fee charges (Presently minimum Membership charge is US\$ 1250) however allocation of AS number is free.

2.9.3 Most of the ISPs do not fulfill the AS number allocation criteria. The high fee required to obtain AS number is the main barrier.

2.9.4 The allocation of IP address by APNIC is also done in two categories:

- (i) As non-member of APNIC
- (ii) AS member of APNIC

2.9.5 The non members have to pay US \$ 1.0 per IP address subject to minimum of US\$ 8192 for allocation of IP address. In addition to above US\$ 0.10 per IP address per year has to be paid as yearly maintenance charge.

2.9.6 The Minimum IP block which is allocated by APNIC to a member is /21 i.e. 2048 IP addresses. ISPs have to submit complete detail of IP addresses being utilized by them before getting IP block allocation from APNIC. In case the IP address utilization is less, the APNIC will not allocate IP addresses in member category and IP addresses have to be taken as non member.

2.9.7 APNIC charges very high fee for its membership on the basis of size of operation of ISP. The lowest slab of annual membership fee is US \$ 1250 per year as per present rates. In addition to above, ISP has to pay one time IP resource allocation fee of US \$ 2500.

2.9.8 The high cost to obtain AS number, APNIC membership and leased line to connect to NIXI outweigh the likely advantages. As a result many ISPs do not join NIXI. Only such ISPs who have their own AS

number and have substantially high domestic traffic find connectivity to NIXI economical.

- 2.9.9 One of the option to overcome the AS number allocation problem can be to use private AS numbers from upstream provider. Private AS number is a series which can be used to run Border gateway Protocol version 4 (BGP4+) routes with upstream provider. However the upstream provider has to allocate unique private AS number to its downstream ISPs. Please see note below.
- 2.9.10 Small ISPs usually depend on larger ISPs for their upstream connectivity to International internet gateways. Therefore these ISPs can take unique private AS number from their upstream providers.
- 2.9.11 In case upstream providers are connected to NIXI, and announce and accept all the routes on behalf of their down stream service providers (ISPs), then there will be no need for direct connectivity of the individual ISPs at NIXI and domestic traffic can be exchanged between ISPs. This will help small ISPs to escape from high cost of AS number allocation by APNIC and leased line cost.

2.10 Dedicated Link of Individual ISPs

- 2.10.1 The solution discussed above will not require separate links to NIXI by each ISP. Hence, riding on the upstream provider may be

Note: -

- Upstream provider is an ISP who is carrying the traffic to International internet gateway or NIXI.
- Downstream provider is an ISP who is connected to smaller ISPs or directly provides service to Internet subscribers at one hand and upstream provider at the other hand.
- Domestic traffic means internet traffic which originates in India and is destined within India.

economical for small ISPs. The purpose will be served if either an ISP or its upstream provider is connected at NIXI. Similar alternatives can be used for multi-homed ISPs also. There is more than one upstream provider for an ISP in multi-homing scenario. Hence such multi-home ISP can designate one of the upstream providers to carry and announce its traffic at NIXI.

2.11 Views were also expressed by International Internet bandwidth providers that they may also be considered to provide domestic peering services to ISPs. While exploring the possibility to improve effectiveness of NIXI, the Authority is open to consider various options to ensure domestic traffic is exchanged within country at domestic bandwidth cost. Since measurement of volumes of domestic and international traffic on one single link is technically not possible at present, such effective domestic traffic exchange is only possible when separate domestic peering is done between ISPs and International Internet Bandwidth providers for exchange of domestic and International traffic. In view of above International internet bandwidth provider can also provide domestic peering services if following conditions are met:

- (i) Separate dedicated peering is done for domestic traffic.
- (ii) All International Internet bandwidth providers are mandated to connect to NIXI nodes to facilitate exchange of traffic between them.

2.12 It was also stated that mutual arrangement to exchange domestic traffic between International Internet bandwidth providers would be sufficient to ensure that domestic traffic between International Internet bandwidth providers is routed within country and not forced to get routed through International links. This holds good only when we assume that all ISPs are connected to International Internet Bandwidth providers and not to NIXI. Segregation of Domestic and International traffic will also be required in this

scenario. Hence connection of all International Internet bandwidth providers at NIXI is necessary.

2.13 The options to connect International Internet bandwidth providers using dedicated domestic peering link will be beneficial as it will provide alternate domestic peering point other than NIXI. Such initiatives will reduce cost of content download, encourage web hosting in India and will bring in more competition.

2.14 Recommendations

The Authority recommends,

- (i) All ISPs or their upstream providers should either be connected at all NIXI nodes or to International internet bandwidth provider through separate domestic peering link.**
- (ii) All the ISPs providing International Internet bandwidth should be connected at all the 4 nodes of NIXI.**
- (iii) In case of multi-homing ISP, such ISP will decide one of the up stream provider to carry domestic traffic to NIXI or to ISP providing International Internet bandwidth through domestic peering link.**
- (iv) Domestic traffic shall either be routed through NIXI or through dedicated domestic peering of ISP with International Internet Bandwidth providers.**

CHAPTER-3

DOMESTIC TRAFFIC ROUTING

3. Announcement and acceptance of all routes on NIXI

- 3.1 One of the main reasons of limited flow of domestic traffic through NIXI is non-announcement/ non-acceptance of routes at NIXI by the ISPs connected at NIXI. The problem becomes acute with those ISPs who are peering as well as transiting the Internet traffic i.e. an ISP is providing Internet protocol (IP) port in India for International Internet bandwidth as well as have domestic ISP operations. Such ISPs feel that NIXI platform can be misused by other ISPs connected at NIXI to route their International traffic by manipulating Border Gateway Protocol (BGP) routes.
- 3.2 IP packet flow is destination based routing. All the connected networks announce the accessible routes through them. Based on the various routing protocols, most suitable route based on routing algorithm is selected and traffic is routed. Efficient routing requires announcement and acceptance (learning) of all the routes.
- 3.3 The data traffic flow is one way, hop by hop, routed by analyzing destination address based on the routes learnt. The selection of the route path in Internet environment depends on announcement and acceptance of the routes by connected nodes. Therefore announcement and acceptance of the routes plays very important role on flow of the traffic. In order to ensure smooth flow of traffic between connecting ISPs at NIXI, it is necessary to announce and accept all routes (including that of down stream providers) at NIXI.
- 3.4 Possibility of misuse of NIXI connectivity by connecting ISPs to route their International Internet traffic can not be ruled out. However, there are several technical solutions like controlled

announcement of route, use of route filters for unexpected routes, which can effectively block such possibilities.

3.5 All connecting ISPs can also be asked to publish their routing policy at NIXI on its website under protected password so that all NIXI members can see it and take advance actions to rule out any misuse possibilities.

3.6 Juniper, the Original Equipment manufacturer (OEM) in its response to Telecom Engineering Centre (TEC) on issue of segregation of domestic and International internet bandwidth has advocated announcement and acceptance of all routes at NIXI platform to effectively handle exchange of domestic traffic at NIXI.

3.7 The effectiveness of NIXI will improve by encouraging ISPs connected to NIXI to announce and accept all their routes at the NIXI nodes. Provision of stringent penalties can be made to deter the practices of any misuse of NIXI platform. The details of the routes declared and accepted by various ISPs must be intimated in advance to NIXI and put on its web side under protected folders so that same can be viewed only by NIXI members. This will help in curbing the possibilities of misuse of NIXI connectivity. The announcement of the prefix while announcing the routes should also be regulated. It will be desirable that NIXI works out model route announcement code and makes it mandatory for all its members to follow the same.

3.8 These steps will ensure effective exchange of domestic traffic at NIXI and take care both technically and administratively any possible misuse of NIXI platform.

3.9 Recommendations

The Authority recommends,

- (i) All ISPs announce and accept all their routes (including that of their down stream providers) at NIXI nodes or at direct peering point as the case may be.**

- (ii) Provision of stringent penalties may be made in the licensing conditions to curb the tendencies of misuse at any interconnection points by ISPs.**

- (iii) It is desirable that details of the routes declared and accepted by various ISPs be intimated in advance to NIXI and put on its website under protected folders so that same can be viewed by NIXI members only. This will help to curb the possibilities of misuse of NIXI connectivity.**

- (iv) It will be desirable that NIXI works out model route announcement code and makes it mandatory for all its members to follow the same.**

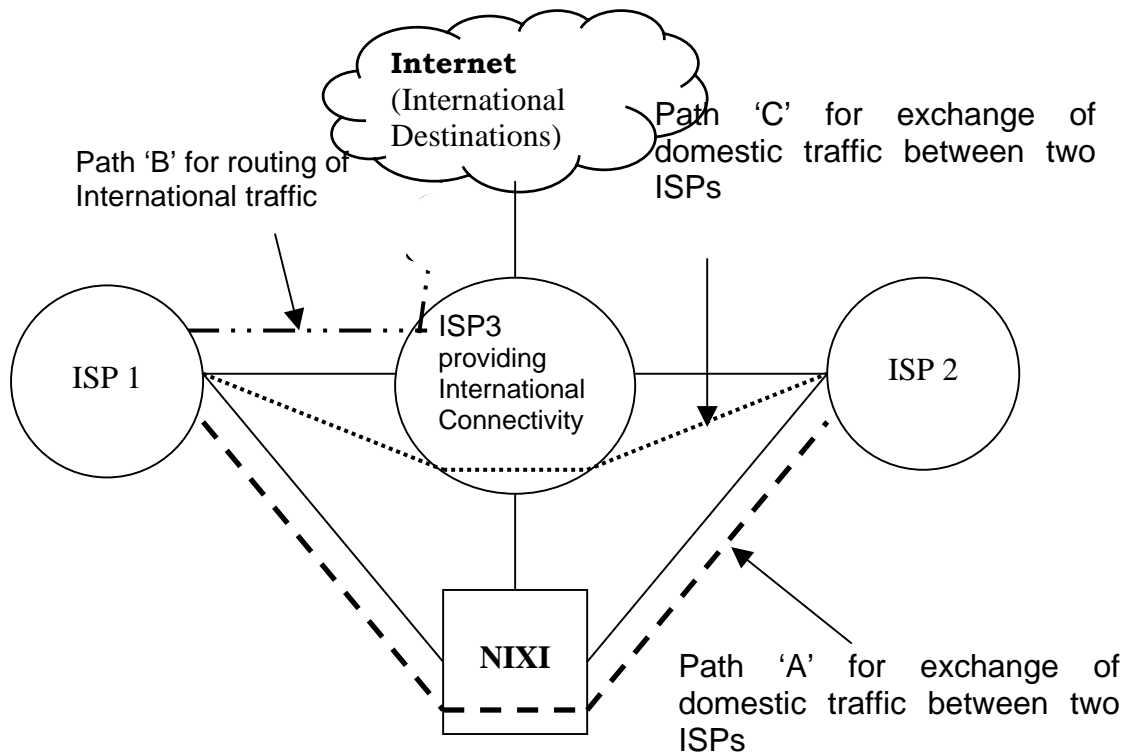
CHAPTER-4

SEGREGATION OF TRAFFIC

4. Segregation of domestic and International traffic

4.1 All ISP will require connectivity to International Internet bandwidth even if connected at NIXI. Such bandwidth can be provided either using International Private Lease Circuit (IPLC) or through an IP port (International Internet bandwidth) in India by International Internet bandwidth providers. The use of IPLC is advantageous when traffic is destined from India to one specific country. In practice most of the IP traffic is destined to different countries. In such a scenario, use of IP port in India becomes beneficial to most of the ISPs.

4.2 Majority of International Internet bandwidth providers are ISPs themselves and expected to have their presence at NIXI also. In this way, an ISP who is connected at NIXI and have also taken IP port from one of the International Internet bandwidth providers will have two connectivities to such International Internet bandwidth provider (one through IP port and other through NIXI). The diagram given below depicts the scenario.



- 4.3 While International Internet bandwidth providers prefer to route all the traffic (Domestic and International) through IP port to avoid any possibility of misuse through NIXI, the ISPs end up paying International Internet Bandwidth charges for exchange of domestic traffic also. ISPs have demanded that domestic traffic must be routed through NIXI so that they do not pay International Internet bandwidth charges for routing of the domestic traffic. High cost of routing domestic Internet traffic increases content down load cost. It is desirable to reduce content down load charges. Such charges can be reduced only when domestic traffic is effectively exchanged at NIXI. However, it has been noted that full routes are neither being announced nor accepted by such International Internet bandwidth providers resulting in sub-optimal exchange of domestic traffic at NIXI even when they are connected. As a result, stand alone ISP have no other option but to route their traffic using link provided for international traffic by ISP providing International Internet bandwidth and end up paying International bandwidth charges for such domestic traffic.
- 4.4 This issue has been deliberated in chapter 3 in detail and M/s Juniper (OEM) has opined that domestic traffic can be effectively exchanged at NIXI. Accordingly all ISPs or their upstream providers are being mandated to announce and accept all routes. Exchange of such traffic at NIXI will not require any segregation of domestic and international traffic.
- 4.5 Here the issue of concern is the provision of domestic peering by international internet bandwidth providers. ISPs providing International Internet bandwidth have expressed the concern that option to provide domestic peering may also be provided to them and not only limited to NIXI. The Authority feels that such options will be useful to provide alternate domestic peering points and may increase competition which shall be beneficial to ultimate subscribers. Measurement of volumes of traffic of domestic and

international destination at one single link is technically not feasible and therefore in order to ensure that domestic traffic is exchanged at domestic bandwidth cost between the ISPs and international internet bandwidth providers without going through NIXI will require direct domestic peering. Direct domestic peering is only possible when domestic and international traffic is segregated by international internet bandwidth provider. This will serve the purpose as ultimate aim is to provide flexibility to exchange domestic traffic at domestic bandwidth cost.

4.6 Separation of domestic and International traffic is possible by utilization of the advance tools and techniques like route filtering, MPLS etc. However considering the importance of the issue and complex technical nature, the Authority decided to refer the matter to Telecom Engineering center (TEC).

4.7 TEC has deliberated upon the issue and called the meeting of stake holders including OEMs. Two options were analyzed,

- **Option I:** Segregation of Domestic and International Traffic without use of NIXI
- **Option II:** Segregation Of Domestic and International traffic with use of NIXI

4.8 After threadbare deliberation TEC has Informed the Authority that **“It is opined that although both options for segregating domestic and international internet traffic are technically feasible** yet following observations have also to be taken into account before going ahead with any of them:

Option 1 (without NIXI):

- a. It requires the redesigning of existing service provider network with MPLS.

- b. Virtual Private Network (VPN) for domestic traffic is required to be formed and domestic connectivity is required to be shifted into this VPN.
- c. In case the smaller ISP takes only one link (international), that ISP needs to be connected as tier-1 ISP's own customer through tier-1 ISP's access network.
- d. Core and access network of ISP is required to be separated.
- e. This option is relatively complex and involves reconfiguration of the existing network but it does not require NIXI to act as transit point for domestic internet traffic.

Option 2 (transiting all domestic traffic through NIXI)

- a. It requires MPLS enabled router at only NIXI Point of presence (PoP) locations.
- b. In this case all smaller ISPs are required to be connected to both NIXI for domestic internet traffic and a tier-I ISP for international internet traffic.
- c. All intra country internet traffic shall have to transit through NIXI.

4.9 The Authority notes that segregation of the Domestic and International bandwidth is technically possible but may require certain actions by ISPs providing International Internet bandwidth before such schemes are implemented.

4.10 Since it has been recommended that domestic traffic is exchanged either through NIXI or direct domestic peering points, no domestic traffic is envisaged through international internet link in case of stand alone ISPs. The international internet bandwidth providers are being permitted to have direct domestic peering with ISPs to exchange domestic traffic on their own request.

4.11 Therefore it is expected that any technical up gradations if required will also be implemented by them. In any case, NIXI will provide at least one effective platform for exchanging domestic traffic.

4.12 The technological advancements and convergence is likely to change the network topology in years to come. Effective exchange of the domestic traffic will become crucial. The sheer volumes and business models and increase of web hosting business in India will encourage facilitation of effective domestic exchange points.

4.13 Recommendations

The Authority recommends,

- (i) All the ISPs who are providing International Internet IP port in India shall be permitted to have peering for exchange of domestic traffic with other ISPs provided such integrated ISPs segregate domestic and International traffic using any technique/ technology suitable to them. This will enable alternate domestic peering points and will bring competition ultimately benefiting the subscribers.**

CHAPTER-5

INSTALLATION AND INTERCONNECTION OF NIXI NODES

5. Interconnection of 4 nodes of NIXI

- 5.1 A Task force was setup to prepare an action plan to achieve the faster growth of Internet and work out methodology to facilitate establishment of Internet exchange point (IXP) for peering within country. Task force suggested in its recommendation in 2002 that NIXI should have a distributed and redundant architecture with deployment at four metro locations i.e. New Delhi, Mumbai, Chennai and Kolkata and these locations to be interconnected for enabling the routing of inter-ISP traffic only and **without carrying any intra-ISP traffic**. President Internet service providers association of India (ISPAI) also expressed the views in 2005 that NIXI is being sub-optimally utilized due to non-connection of four NIXI nodes.
- 5.2 Based on above observations, TRAI recommended on 29th May 2006 that urgent steps are required by Govt. (DIT) in respect of the following:
- All the four nodes of NIXI should be interconnected with each other.
 - Consideration of establishment of NIXI nodes in all state capitals of the country.
- 5.3 Considering the importance, the consultation paper flagged these issues to get feedback of the stake holders. The stakeholder's comments have been compiled and are available at Annexure 'A'.

- 5.4 The consensus view was against any interconnection of the NIXI nodes. It was felt that such interconnections will require huge Capital expenditure and Operational expenditure. As NIXI is a non profit organization, all its expenditure is being met from the contributions of the members. This interconnection shall require increased contributions from members.
- 5.5 The effective utilization and management of such link utilizations will be another problem. Non-equal utilization of backbone may further raise disputes in financial settlement and contribution by NIXI members.
- 5.6 The ISPs or their upstream providers have been permitted to connect to all NIXI nodes. Therefore exchange of domestic traffic between NIXI nodes can be facilitated by ISPs themselves and such interconnections may not be required.
- 5.7 It is expected that present scheme envisaged will help to improve effectiveness of NIXI to exchange domestic traffic. The interconnection of NIXI nodes if not found financially attractive by NIXI members, it may be deferred for the time being.

5.8 Recommendation

The Authority recommends,

- (i) The interconnection of NIXI nodes if not found financially attractive by NIXI members, it may be deferred for the time being.**

5.9 NIXI nodes at all state capitals

- 5.9.1 In order to facilitate connectivity of smaller ISPs (Category B & C) to connect at the local NIXI hubs, it was advocated that NIXI hubs be set up in the State Capitals. It was envisaged that setting up of

such NIXI nodes at state capital will reduce cost of the leased lines required by shall ISPs for connection to NIXI. Based on above observations TRAI recommended on 29th May 2006 that urgent steps are required by Govt. (DIT) to establish NIXI nodes in all state capitals of the country.

- 5.9.2 Move to setup NIXI nodes at each state capital will require huge expenditure both in the form of Capex and Opex. The likely returns are not commensurate with the investments. In addition, serious operational problems were anticipated if such nodes were setup.
- 5.9.3 As deliberated in earlier chapters, the basic reason for non connection of small ISPs at NIXI is not due to high cost of the link to connect to NIXI but due to non availability of AS number and non announcement and acceptance of routes. If upstream providers are permitted to announce and accept all the routes of down stream providers, the small ISPs will not require direct connectivity with NIXI.
- 5.9.4 In view of above scenario, cost benefit analysis for setting up NIXI nodes at all State capital needs to be done before implementing this option. The management issue of such NIXI nodes if established and likely traffic growth etc will require in-depth study. The present traffic handled through NIXI is low and does not justify any additional NIXI node till domestic traffic increases. Also, most of the states at present do not have sufficient domestic internet traffic now; therefore setting of such nodes will only complicate the issue of maintenance of NIXI nodes, its manning and may result in huge expenditure without commensurate returns.
- 5.9.5 At present, total domestic Internet traffic of four NIXI nodes is just 1600 Mb while its capacity to handle such exchange of traffic is very high. Immediate action is required to encourage effective utilization of NIXI. The regional traffic needs to be monitored

regularly and decision to setup any additional NIXI node be taken based on volumes of domestic Internet traffic in a particular region.

5.10 Recommendations

The Authority recommends,

- (i) It will be desirable to make detailed analysis of present domestic traffic, CAPEX and OPEX required to setup NIXI node and optimum capacity utilization of existing nodes before taking any decision to setup any additional node .**

CHAPTER-6

UP GRADATION OF NIXI NODES AND QOS

6. Up gradation of NIXI nodes to facilitate implementation of IPv6

6.1 IPv6 is next generation Internet protocol and it has capacity to expand the available address space on the Internet enormously. It uses 128 bits as compared to 32 bits of IPv4. It inherently possesses capability to provide better QoS as compared to IPv4. In addition, IPv6 is designed to promote higher flexibility, better functionality and enhanced security & mobility support. Because of these advantages, the service providers are generally inclined to migrate to this newer version of Internet technology.

6.2 TRAI in its recommendation dated 9th January 2006 on “Issues Relating to Transition from IPv4 to IPv6” in India has already recommended the Up gradation of NIXI as a national test bed for IPv6.

6.3 Looking at the benefits of IPv6, some ISPs have started implementing IPv6 and some may implement it in near future. This will result in coexistence of both IPv4 and IPv6 traffic. NIXI should be able to handle both types of traffic simultaneously by deploying suitable mechanism like overlay tunneling etc.

6.4 ISPs also need to experiment with IPv6 and conduct trials to get hands on experience before deploying this technology in their networks. For this purpose an IPv6 test bed/ platform is required to which such ISPs can connect to conduct the trials for their traffic flow.

6.5 NIXI during the open house discussion confirmed their readiness to provide such facilities. It will be desirable if detailed plan is worked

out by NIXI and made known to ISPs so that such facilities are effectively utilized by them.

6.6 Recommendations

The Authority recommends,

- (i) It is desirable that NIXI may setup test bed to exchange IPv6 routes between IPv6 enabled networks as well as IPv4 networks based on overlay tunnel. This may be completed in time bound manner, say six months so that NIXI is able to commercially support IPv6 exchange of routes.**

6.7 QoS for NIXI nodes

- 6.7.1 A major advantage of an Internet Exchange Point (IXP) is the reduction in network latency by eliminating the need for multiple hops in the routing of domestic traffic. However, in some cases ISPs may use their transmission links connected to NIXI at 100% of capacity resulting in dropped data packets, retransmission of dropped data packets thereby resulting in increased latency of the traffic flowing through NIXI. This may degrade the quality of traffic exchanged at NIXI nodes and may adversely impact QoS.
- 6.7.2 There is a need to ensure the availability of carrier class facilities at NIXI nodes including non-blocking architecture.
- 6.7.3 It may be possible that ISPs may announce all their routes, but do not have adequate bandwidth connectivity to NIXI resulting in congestion. This may result in degradation in the quality of traffic flowing through NIXI. ISPs should take suitable connectivity to NIXI based on the traffic and should be required to upgrade the connecting links to higher level as soon as the average traffic on the link exceeds certain percentage of the capacity. Hence, there is a need to define important parameters of NIXI.

6.7.4 A core group having representatives from ISPAI, Bharti, BSNL, VSNL, Reliance, and NIXI to deliberate on QoS parameters related to NIXI was setup during open house discussion and it has submitted its recommendations to Authority on 31.12.2006. **These recommendations have been forwarded to DIT on 3rd January 2007 for further necessary action (refer annexure D).**

CHAPTER-7

OTHER MISCELLANEOUS ISSUES

7. Need to encourage Data center and WEB hosting in India

7.1 Presently web-hosting charges in India are substantially higher than in other European countries and USA. As a result lot of Indian websites and contents are hosted outside country. This increases International bandwidth requirement for accessing India specific websites and contents hosted outside India. This can be avoided if website and content hosting is encouraged in the country.

7.2 The present traffic settlement charging formula adopted by NIXI does not encourage data centers to directly connect to NIXI and hence hosting of the local content by Data centers. What is required is to encourage data centers to directly connect to NIXI to encourage development of local contents and web hosting. It will be desirable to request to NIXI to consider these issues while deciding NIXI interconnection policies. This will not only reduce the web hosting charges in India but will also attract the International content providers to locate their servers in India.

7.3 NIXI Structural issues

7.3.1 NIXI should establish good governance, appropriate infrastructure & processes to attract the ISPs to connect to NIXI. NIXI requires skilled manpower for proper management of traffic. Without these NIXI will not be able to fulfill its obligation of providing improved quality for exchange of domestic traffic.

7.3.2 In its recommendations on “Accelerating growth of Internet and Broadband Penetration” during April 2004, the Authority recommended that:

“The structure of the Board of Directors of NIXI should be altered to account for appropriate weight and participation from the applicable constituencies. This should include a total of 12 members, with the greatest weightage given to the largest ISP operators in the country. These large operators should be assigned five seats among them, while smaller ISP’s should have representation via two seats. Two seats should also be reserved for independent individuals who do not have managerial stake in ISP operators, while the remaining three seats should be reserved for Government representatives, one each from DIT, DOT and TRAI. “

- 7.3.3 There is a need to ensure carrier class infrastructure, facilities, processes and governance for NIXI to make it more effective for ISPs to have incentive to join NIXI and thereby allow the country to realize its benefits. The appropriate infrastructure and processes must be established immediately. Better infrastructure will attract more ISPs to join NIXI resulting in additional resource generation for NIXI for further developments and upgradations.

CHAPTER-8

SUMMARY OF RECOMMENDATIONS

I. Interconnection of ISPs at NIXI

The Authority recommends,

- (i) All ISPs or their upstream providers should either be connected at all NIXI nodes or to International internet bandwidth provider through separate domestic peering link.**
- (ii) All the ISPs providing International Internet bandwidth should be connected at all the 4 nodes of NIXI.**
- (iii) In case of multi-homing ISP, such ISP will decide one of the up stream provider to carry domestic traffic to NIXI or to ISP providing International Internet bandwidth through domestic peering link.**
- (iv) Domestic traffic shall either be routed through NIXI or through dedicated domestic peering of ISP with International Internet Bandwidth providers.**

2. Announcement and acceptance of all routes on NIXI

The Authority recommends,

- (i) All ISPs announce and accept all their routes (including that of their down stream providers) at NIXI nodes or at direct peering point as the case may be.**
- (ii) Provision of stringent penalties may be made in the licensing conditions to curb the tendencies of misuse at any interconnection points by ISPs.**

(iii) It is desirable that details of the routes declared and accepted by various ISPs be intimated in advance to NIXI and put on its website under protected folders so that same can be viewed by NIXI members only. This will help to curb the possibilities of misuse of NIXI connectivity.

(iv) It will be desirable that NIXI works out model route announcement code and makes it mandatory for all its members to follow the same.

3. Segregation of domestic and International traffic

The Authority recommends,

(i) All the ISPs who are providing International Internet IP port in India shall be permitted to have peering for exchange of domestic traffic with other ISPs provided such integrated ISPs segregate domestic and International traffic using any technique/ technology suitable to them. This will enable alternate domestic peering points and will bring competition ultimately benefiting the subscribers.

4. Interconnection of 4 nodes of NIXI

The Authority recommends,

(i) The interconnection of NIXI nodes if not found financially attractive by NIXI members, it may be deferred for the time being.

5. NIXI nodes at all state capitals

The Authority recommends,

(i) It will be desirable to make detailed analysis of present domestic traffic, CAPEX and OPEX required to setup NIXI

node and optimum capacity utilization of existing nodes before taking any decision to setup any additional node.

6. Upgradation of NIXI nodes to facilitate implementation of IPv6

The Authority recommends,

- (i) It is desirable that NIXI may setup test bed to exchange IPv6 routes between IPv6 enabled networks as well as IPv4 networks based on overlay tunnel. This may be completed in time bound manner, say six months so that NIXI is able to commercially support IPv6 exchange of routes.**

COMMENTS OF STAKEHOLDERS

1. INTERCONNECTION ISSUES AT NIXI

1.1 Interconnection of ISPs at NIXI

- 1.1.1 Majority of the stakeholders are of the view that ISPs or their upstream providers should be mandated to connect at least at one NIXI node. They also suggested that there is a need to define Up-stream provider.
- 1.1.2 Some ISPs were of the view that the ISPs should not be mandated to connect at NIXI. ISPs should have the choice to connect to NIXI or to the upstream ISPs providing them International bandwidth, based on individual ISPs business needs. Such ISPs can also do transit for domestic traffic.
- 1.1.3 Most of the stakeholders also stated minimum bandwidth pipe size for connectivity to NIXI should be worked out to achieve Quality of Service (QOS).

2 DOMESTIC TRAFFIC ROUTING

2.1 Announcement and acceptance of all routes on NIXI

- 2.1.1 Most of the stakeholders are of the view that only way to improve the effectiveness of NIXI is to mandate all ISPs to announce and accept at least all regional routes at NIXI. While issue of misuse of NIXI node was flagged, it was generally agreed that technical solutions are available to take care of such eventualities.
- 2.1.2 While majority of the stakeholders are in favour of announcing all the routes at NIXI nodes, some felt that only regional routes should be announced as announcement of all routes can be misused to carry transit traffic between different NIXI nodes.

2.1.3 There were views that Regional route boundaries have blurred, hence all routes should be announced and accepted at NIXI. It was also confirmed that announcement of all the routes can not be misused to carry inter NIXI node traffic.

2.1.4 Some stakeholders also felt that there is no need to mandate ISPs to announce and accept all the routes at NIXI. It should be left to the individuals' choice.

3. SEGREGATION OF TRAFFIC

3.1 Segregation of domestic and International traffic

3.1.1 In response to possibility of segregation of domestic and International traffic by ISPs who are transiting as well as peering, most of the stakeholders felt that separation of the domestic and International traffic is possible with the availability of the advanced technologies like MPLS.

3.1.2 Some felt that separation is possible but it may have serious operational difficulties.

3.1.3 Authority also received a request to setup a committee to deliberate upon the possibility of separation of domestic and International traffic so that this issue can be amicably solved.

4. INSTALLATION AND INTERCONNECTION OF NIXI NODES

4.1 Interconnection of 4 Nodes of NIXI

4.1.1 All stakeholders including NIXI were not in favour of interconnection of NIXI nodes.

4.1.2 Stake holders also felt that Interconnection of NIXI nodes might result in NIXI functioning as domestic transit provider and compete with other ISPs and may change the basic philosophy of NIXI to be a neutral body.

- 4.1.3 Some stake holders also felt that NIXI may be required to obtain NLD licence from DoT for carrying ISPs traffic over such backbone.
- 4.1.4 It was widely shared view that if NIXI nodes are interconnected than the bigger ISPs might connect only at one or two locations just for peering and would ride on NIXI' s backbone for the transit of their traffic between various NIXI nodes.
- 4.1.5 It was also stated by some stakeholders that to carry the traffic between interconnected nodes a robust network is required. Such interconnection might be misused by some ISPs in the absence of proper network discipline by participating ISPs.
- 4.1.6 Since NIXI is an organization not for profit, stake holders raised the issue of funding of the link cost also as utilization of such links can be manipulated by connecting ISPs.

4.2 NIXI Nodes at all State Capitals

- 4.2.1 Most of the stakeholders felt that there is no justification of formation of NIXI nodes at all the state capitals, as most of the states do not have sufficient traffic.
- 4.2.2 Representative of ISPAI suggested that instead of all the state capitals, cities like Bangalore, Hyderabad, Pune, Ahmedabad, etc may be considered for putting up of the NIXI nodes as these places are developing as IT Hubs.
- 4.2.3 There was general consensus that decision to set up NIXI nodes should be based on the traffic analysis and likely domestic traffic to be exchanged vis-a-vis the expenditure on the project. The NIXI nodes should be setup only if commercial analysis justifies the need.

5. UP-GRADATION OF NIXI NODES AND QOS

5.1 Up-gradation of NIXI nodes to facilitate implementation of IPv6

5.1.1 Most of the stakeholders were of the opinion that NIXI should be ready to handle IPv6 traffic and a roadmap should be prepared for timely implementation.

5.1.2 Representative of NIXI informed that its equipments are IPv6 compatible and can support IPv6 traffic.

5.2 QoS for NIXI Nodes

5.2.1 Almost all the stakeholders felt the need for well define QoS of NIXI for reliable functioning of NIXI

6. OTHER MISCELLANEOUS ISSUES

6.1 Need to encourage Data center and WEB hosting in India

6.1.1 Most of the stakeholders felt that there is no need to make any changes in the present settlement formula of NIXI.

6.1.2 Representatives of ISPAI mentioned that Datacenters should be insisted to have a mandatory interconnect with NIXI, as it will benefit both content providers and customers in terms of huge saving of International bandwidth and increase access speed.

6.2 NIXI Structural Issues

6.2.1 It is suggested that there is a need to modify NIXI's structure from a limited liability company to a mutual not-for-profit organization.

6.2.2 It was also stated that ISPs should have member status and rights, obligations to seek the best strategic direction and promote best practices operations.

6.2.3 Some of the stakeholders were of the view that major ISPs should be part of governing body of NIXI for proper administration. A

periodical review of physical infrastructure of NIXI is necessary. Suitable investment to cope up with the increasing traffic and number of connections is also required.

- 6.2.4 Almost all the stakeholders emphasized the need for well trained technical manpower to manage NIXI.

INTERNATIONAL EXPERIENCE

In most of the countries there are multiple Internet exchanges, which are independent and are not interconnected. Here are some of the examples:

1. UK

1.1 London Internet Exchange (LINX)

LINX is a mutual not-for-profit organisation, owned by the ISPs and content service delivery providers, which have connections there. The LINX Network consists of two separate high-performance Ethernet switching platforms installed across seven interconnected locations in London. It has more than 200 members – both ISPs and content delivery service providers – from the UK, mainland Europe, the USA, Africa and the Far East. It handles up to 95 per cent of all UK Internet traffic.

1.2 London Internet Providers Exchange (LIPEX)

Started in October of 2001, Lipex is one of the fastest growing Internet Exchange Points (IXP) or Peering Points in Europe. It has 56 members and has 6 PoPs in London.

1.3 London Network Access point (LoNAP)

A neutral not-for-profit, independent peering point, LoNAP has been providing the infrastructure for its members to establish peering and exchange traffic since 1997. It has 43 members and 3 PoPs in London.

1.4 Manchester Network Access point (MaNAP)

MaNAP is a neutral, not-for-profit Internet Exchange committed to the provision of continuous and resilient layer two ethernet connectivity to operators of Autonomous Systems. It has 29 members and 4 PoPs.

It has created the first National peering LAN in the UK by extending its network to London and allow providers in London to peer at MaNAP without the need to buy expensive circuits to the North of England. Continuing to support the MaNAP membership, it will provide special pricing on Point to Point circuits to London from Manchester for MaNAP members only, with an almost 50% reduction on 1Gbps connections. This will benefit members wanting to source their transit in London, which is typically cheaper, and also for members who wish to co-locate a router in Manchester to expand their own network.

1.5 Redbus Interhouse Internet Exchange (RBIEX)

RBIEX is a neutral Internet Exchange with 15 members and 3 PoPs in London.

1.6 Scottish Internet Exchange (SCOTIX)

ScotiX" - Scotland's first Internet Exchange opened for business on 14th September 1999. ScotIX is a not for profit company, limited by guarantee, and registered in Scotland. The Stakeholders are ISPs or Telcos who have their own permanent connection to the Internet and their own paths from an IP address within the Autonomous System.

2. Australia

2.1 PIPE Internet Exchange

PIPE Networks is Australia's largest peering provider with 16 IX locations across 6 metro-IX networks. PIPE Networks is a Metro Area Internet Exchange that has distributed its switching capacity in areas of high customer density in Brisbane, Sydney, Melbourne, Adelaide, Hobart and Canberra. As such the PIPE network can connect to customers in buildings other than its main point of presence. It has 59 members at present. PIPE Networks operates a vendor and carrier neutral environment for its peers and provides

fully redundant, state of the art layer 2/3 Ethernet switches and routers operating up to gigabit speed.

2.2 West Australia Internet Exchange (WAIX)

WAIX commenced in early 1997 to allow members of the WA Internet Association (WAIA) the ability to inter-connect using an independent facility. The facility allows members to multi-laterally peer their networks at a considerably reduced rate. WAIA charges each of the four ISPs a quarterly fixed fee (plus setup charge) for connection and this allows them access to all shared information.

2.3 Equinix Sydney

Equinix Exchange is a solution for Internet Service Providers (ISP), Content Service Providers (CSP), and large enterprises seeking to expand geographically without incurring the cost of building new data centers. Equinix Exchange provides new peering flexibility and intra-data center LAN connectivity to ISPs, CSPs and large enterprise customers at multiple Asian and U.S. locations.

2.4 Globalcenter Internet Exchange (AUSIX)

As the first successful neutral commercial Internet Exchange in Australia, AUSIX's Melbourne facility is recognized as one of the top ISP interconnection points in the world.

2.5 Victorian Internet Exchange (VIX)

The **Victorian Internet Exchange** is an Internet Exchange Point in Australia. Formed from the Australian Internet Exchange (AUIX) project, VIX is located in the Australian Associated Press Telecommunication (AAPT) Exchange at Melbourne and offers multi-lateral peering.

3. Hongkong

3.1. Hong Kong Internet eXchange (HKIX)

HKIX is initiated and coordinated by Information Technology Services Centre (ITSC) of the Chinese University of Hong Kong (CUHK). **HKIX is not a transit service provider**; instead, it is a layer-2 settlement-free multi-lateral exchange point mainly for routing of intra-HongKong Internet traffic. However, HKIX can also be used for routing of Internet traffic between the networks in Hong Kong and the peer or downstream networks of HKIX participants in other countries. The peering model of HKIX is a SKA (Sender Keep All) peering model.

3.2. The Equinix Internet Business Exchange

Equinix Exchange is a solution for Internet Service Providers (ISP), Content Service Providers (CSP), and large enterprises seeking to expand geographically without incurring the cost of building new data centers.

4. Singapore

4.1. Singapore Open Exchange

Singapore Open Exchange (SOX) is a public/neutral Internet exchange Point (IXP) hosted by National University of Singapore. SOX differs from existing IXPs in Singapore as it operates at OSI layer 2 and does not provide any transit traffic. It has 13 members.

4.2. StarHub IP Exchange (SiX)

StarHub IP Exchange or SiX is a comprehensive IP Transit Service designed to help Service Based Operators (SBOs) such as Domestic and Regional ISPs and content providers.

4.3. Equinix Internet Business Exchange

Equinix Exchange is a solution for Internet Service Providers (ISP), Content Service Providers (CSP), and large enterprises seeking to

expand geographically without incurring the cost of building new data centers.

5. Indonesia Internet Exchange (IIX)

All active ISPs in Indonesia including Govt. owned TelkomNet and IndosatNet are connected to IIX, which is administered by the Association of Internet Service Providers of Indonesia (APJII). IIX has two nodes; one Telkom building and other is at Internet Data Center Indonesia.

**Telecommunication Engineering Centre
Department of Telecommunication
K. L. Bhavan, Janpath, New Delhi-110 001**

No.TBI/Internet Traffic/TRAI/2007-TEC

Dated: 30.03.2007

**To,
Advisor (CN)
TRAI
New Delhi**

REF: Your letter no. 1-6/2006-CN dated 09/01/2007

Sub: Technical solution for segregating domestic and international internet traffic

1. This is in reference to your above mentioned letter requesting technical solution for segregating domestic and international internet traffic. Two meetings to discuss the issue with service providers and equipment manufacturers were held on 24.01.2007 and 05-03-2007. Minutes of meeting are attached for reference. Two options for segregating domestic and international internet traffic was discussed and comments received by M/s Bharti, M/S VSNL and M/s Juniper are also attached along with the technical detail of the options. These comments are analysed and remarks against each comment are available at annexure-I:
2. **It is opined that although both options for segregating domestic and international internet traffic is technically feasible** yet following observations have also to be taken into account before going ahead with any of them:

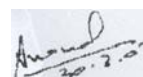
Option 1 (without NIXI):

- a. It requires the redesigning of existing service provider network with MPLS.
- b. VPN for domestic traffic is required to be formed and domestic connectivity is required to be shifted into this VPN.
- c. In case the smaller ISP takes only one link (international), that ISP needs to be connected as tier-1 ISP's own customer through tier-1 ISP's access network.
- d. Core and access network of ISP is required to be separated.
- e. This option is relatively complex and involves reconfiguration of the existing network but it does not require NIXI to act as transit point for domestic internet traffic.

Option 2 (transiting all domestic traffic through NIXI)

- b. It requires MPLS enabled router at only NIXI PoP locations.
- c. In this case all smaller ISPs are required to be connected to both NIXI for domestic internet traffic and a tier-I ISP for international internet traffic.
- d. All intra country internet traffic shall have to transit through NIXI.

This is for your information and perusal please.



(Anand Verma)
ADG (IC)

Enclosure:

1. Two options for segregating domestic and international internet traffic.
2. Minutes of meetings held on 24.01.2007 and 05-03-2007.
3. Comments received by M/s Bharti, M/s VSNL and M/s Juniper

Annexure-I

Bharti Comments	Remarks
<p><u>Unreachability of domestic traffic.</u></p> <ol style="list-style-type: none"> 1. Tier1 ISP, X, is connected to other Tier1 ISP, Y, on domestic peering. ISP Y may not be announcing all domestic routes to Tier1 ISP `X`. Moreover the international path is also not available to D VPN. Thus the traffic originated in D VPN of ISP `X` for destination on D VPN of ISP `Y` may get dropped in such cases. 2. The Tier1 ISP may have peering with one or two other Tier1 ISPs but may not be with all. In that case domestic traffic destined for other non-peering Tier1 ISP may get dropped. 3. In case Tier1 ISP `X` connected to other Tier1 ISP `Y` in a location (say Delhi). Now Tier1 ISP 1Y' may be connected to Tier1 ISP say `Z` in Chennai. T1 ISP `X` is not directly peering with T1 ISP `Z`. Now D-VPN customer of Tier1 ISP `X` wants to connect to D VPN customer of Tier1 ISP `Z`. The only way it can access ISP Z is via ISP Y and thus ISP Y is working as transit in this case and without getting any net revenue. 4. Example : Customer A is connected to tier-1 ISP using only I link and Customer B is connected to Tier-1 ISP using D link only. The D VPN has its own RR (route reflector) which is not connected to international gateway and is not learning routes from RR used for I links. Thus customer B will not having any routes of customer A which is sending the routes/traffic on link I and thus connected using RR of `I` links. This may result in domestic traffic from customer `B`, destined for customer `A` may getting dropped. 	<p>This is based upon the assumption that ISP Y may not be announcing all domestic routes to Tier1 ISP X. this is however mandated by regulator.</p> <p>In that case domestic traffic destined for other non-peering Tier1 ISP will go through international gateway as the D VPN of ISP will not have the routes of other ISP customer.</p> <p>Domestic peering charges will be applicable.</p> <p>It is envisaged that customers will not be directly connected to core network. They will be connected through access network which in turn connected to core network with two links.</p>

<p>5. How to ensure that a content customer (like portal) will surely take D link. As the content customer (portal) will be accessed by India based as well as international users, there is high possibility that content customer will take only 'I' link. The portal customer who has taken only 'I' link will required to be accessed by many of the customers who have taken only 'D' links. But as the routes are not available of 'I' link into 'D' VPN, the traffic destined for the portal customer connected with only 'I' link will be reachable by customers taking only 'D' link.</p> <p>For customers who have taken 'D' as well as 'I' link will be able to access the portal but traffic will flow on 'I' link instead of 'D' link and thus defeating the purpose of taking 'D' link.</p>	<p>Same as above</p>
<p>B) International traffic delivered on domestic link</p> <p>Example :</p> <p>Customer A has taken 'D' link as well as 'I' link. Customer advertises larger prefixes (say /24) on 'I' link and more specific prefixes (say /28) on 'D' link. This 'I' link RR (route reflector) has /24 route whereas 'D' link RR has /28 route available.</p> <p>As the 'I' network also has to have 'D' routes, means that 'I' RR will learn the more specific prefix from 'D' RR. Thus 'I' RR has more specific route to reach customer A via 'D' link. Traffic coming from international location will also be routed via 'D' link. Thus customer will get the downstream traffic from international location on 'D' link rather than 'I' link.</p> <p>Traffic not taking optimum Path</p> <p>1. Example : Customers 'A' has taken both 'D' as well 'I' links. Customer B has taken only 'I' link. Traffic from Customer B will flow through 'I' link towards Customer A even though the traffic is domestic and thus defeating the purpose of taking separate 'D' link.</p>	<p>Not possible as any traffic received form international gateway can not enter into D VPN. this is the basic philosophy of VPN.</p>

<p>2. Example : Customers `A` has taken both D as well `I` links. Customer B has also taken D as well as `I` link. As the domestic routes are available both in D as well `I` links, the customer traffic may flow from `D` or `I` link.</p>	
<p>D) Other technical & operational challenges</p>	
<p>1. The solution further complicates the configuration requirements beyond the Tier 1 ISP or Category A ISPs and extends to Category-B (Tier 2) or Category-C ISPs (Tier 3) as well.</p>	<p>No comments</p>
<p>2. Segregation of domestic & international network will require connecting customers to also run BGP. It means that even smaller ISP & enterprise customer would need to invest in high-end routers to be able to accept more than default route. They would also need BGP/OSPF protocols with the upstream service provider which means more resources required in terms of skilled manpower and thus higher cost.</p>	<p>This is in case customers have links with different ISPs. Otherwise customer can always create static route on different links.</p>
<p>3. Tier 1 or Category-A ISPs must ensure smaller ISPs & enterprise customers must have the right configurations to work, this is just not under the control of ISP-A.</p>	<p>No comment</p>
<p>4. Bharti Airtel core internet backbone network is not MPLS enabled. Internet in a VRF solution requires complete re-design of the routing architecture currently followed. A large number of routes to be placed under a single VRF and expected to grow substantially needs to be tested thoroughly as no Service Provider in the world is placing such a large number of routes under a single VRF. Two years to five years down the line, there is expected to be a significant Increase in the domestic prefixes and it may turn out to be operational nightmare to manage. This is a deviation from best practices.</p>	<p>Internet in VRF is successfully working in service provider's networks.</p>

<p>5. At a site a customer prefix needs to be inserted into the Global Internet VRF and Domestic Internet VRF. This will require high-end Routers which have higher scalability of FIB entries and BGP Peering Sessions cost substantially more. If smaller ISPs request full Internet Routing table the scalability will push the PE Routers to the limits of scalability.</p>	<p>No comment</p>
<p><u>Conclusion</u></p> <p>Considering the above facts, we would like to submit that Redesigning of internet network will not able to meet the objective of TRAI/TEC. With the proposed design, domestic traffic may come via International internet link if the peering ISPs are not announcing the IP prefixes in domestic peering. Moreover with customer subscribing to two links, the internet link may still be used for domestic traffic. In addition to this it will be operationally huge overhead to maintain such network due to complexities involved. In the view of above reasons & the constraints, it does not appear feasible to implement 'internet using separate VRF' model.</p> <p>Bharti Airtel has following suggestion to make to ensure that domestic traffic remains in India and the end customers should be benefited with such arrangement.</p> <p>NIXI was created to provide platform for exchange of domestic traffic between ISPs in India. Parallel platform for domestic traffic exchange may not as stable, as effective as NIXI and may even weaken the NIXI structure as well.</p> <p>The key expectation of NIXI stakeholders is that the domestic routes should be available on NIXI for exchanging domestic traffic through it. Bharti Airtel has been strong supporter of NIXI & announcing its domestic routes on NIXI. ISP should be mandated to announce all their domestic routes on all its NIXI nodes, where the ISP is peering.</p>	<p>NIXI option is also possible to implement.</p>

Reliance Comments	Remarks
<p>VSNL Response on first proposal:</p> <p>The above solution changes from the first proposed solution w.r.t to running only one MPLS tunnel for domestic traffic and keeping Internet traffic (Domestic +International) as it is working in current way. The solution need to be targeted to only small ISP market in India, which may not provide enough market & business case to support the investment required in the network to change the architecture. Apart from the challenges mentioned above, following are the additional challenges, which would arise due to this model :-</p> <ol style="list-style-type: none"> 1. Normally MPLS PE & IP PE routers are separate on access layer. ISP needs to take two separate miles for connecting to two separate edge routers, as D-VPN would be configured in MPLS-PE router and "I" would be working on normal IP-PE router. 2. Route duplication would take place in the network which would impact the resources (CPU, memory) in the routers reducing the over all performance of the equipment. This in turn would call for either more powerful models or simply more number of routers in the place of few to address this issue. Increasing the number of routers to address the same traffic requirement would pose a serious threat to scalability and makes it difficult network architecture to manage. 3. Since the domestic routes are available thru both D and I links to the Tier 2 ISP, they could use any of the links for domestic traffic .Smaller ISPs must have the right configurations to send the traffic thru correct link and this is just not under the control of Tier-1 ISP. 4. Retail & Enterprise customers of Tier-1 ISPs are connected to multiple exit points in a big carrier network and have only one last mile for access. Since this last mile would be in I traffic mode, routes received via NIXI of domestic VPN would not be available to them hence they would not be able to 	<p>No comment</p> <p>It is envisaged that customers will not be directly connected to core network. They will be connected through access network which in turn connected to core</p>

<p>reach NIXI routes domestically.</p> <p>5. MPLS customers always ask for a separate network from the internet for security reasons. This calls for building a new MPLS VPN network to cater to the Domestic traffic alone</p> <p>6. Internet in a VRF solution requires complete re-design of the routing architecture currently followed. This is a clear deviation from global best practices which is nowhere adopted in the world.</p> <p>7. The re-design and implementation come at the cost which Tier 1 or Category-A ISPs must absorb. Migrations require meticulous planning and execution which requires experts to be involved and is very time consuming.</p> <p>8. Tier 1 or Category-A ISP's will need to deal with completely new BGP configurations and those who use provisioning systems will need to re-look the changes need for their provisioning systems also.</p> <p>9. Lets take a case where ISP B and ISP C connect to ISP A at different cities and not connected to each other. Domestic traffic between ISP B and ISP C would flow thru ISP A which is now acting as transit with no revenue may be attached for this transit service. This is a clear disadvantage for ISP A.</p> <p>10. There may be case that few ISPs (ISP A & B) take I connectivity from Tier-1 ISPs and one ISP (ISP C) only takes D-VPN service. Since both the routes would be not be available to each other, ISPs taking I connectivity would not be able to reach ISP-C network domestically and traffic would go to International path.</p>	<p>network with two links.</p> <p>No comment</p> <p>Internet in VRF is proven solution.</p> <p>No comment</p> <p>No comment</p> <p>Domestic peering charges will be applicable.</p> <p>All ISPs have to take I link, option of D link is to be available.</p>
<p>VSNL Response on second proposal:</p> <p>The above solution talks about exchange of all domestic traffic via NIXI only. The issues with MPLS tunnel for Domestic traffic remains same as explained in VSNL responses above to other proposed models. ISPs/Enterprise customers taking I connectivity from Tier-1 ISPs would not be able to access NIXI routes.</p>	<p>It is envisaged that customers will not be directly connected to core network connecting NIXI. They will be connected through access network</p>

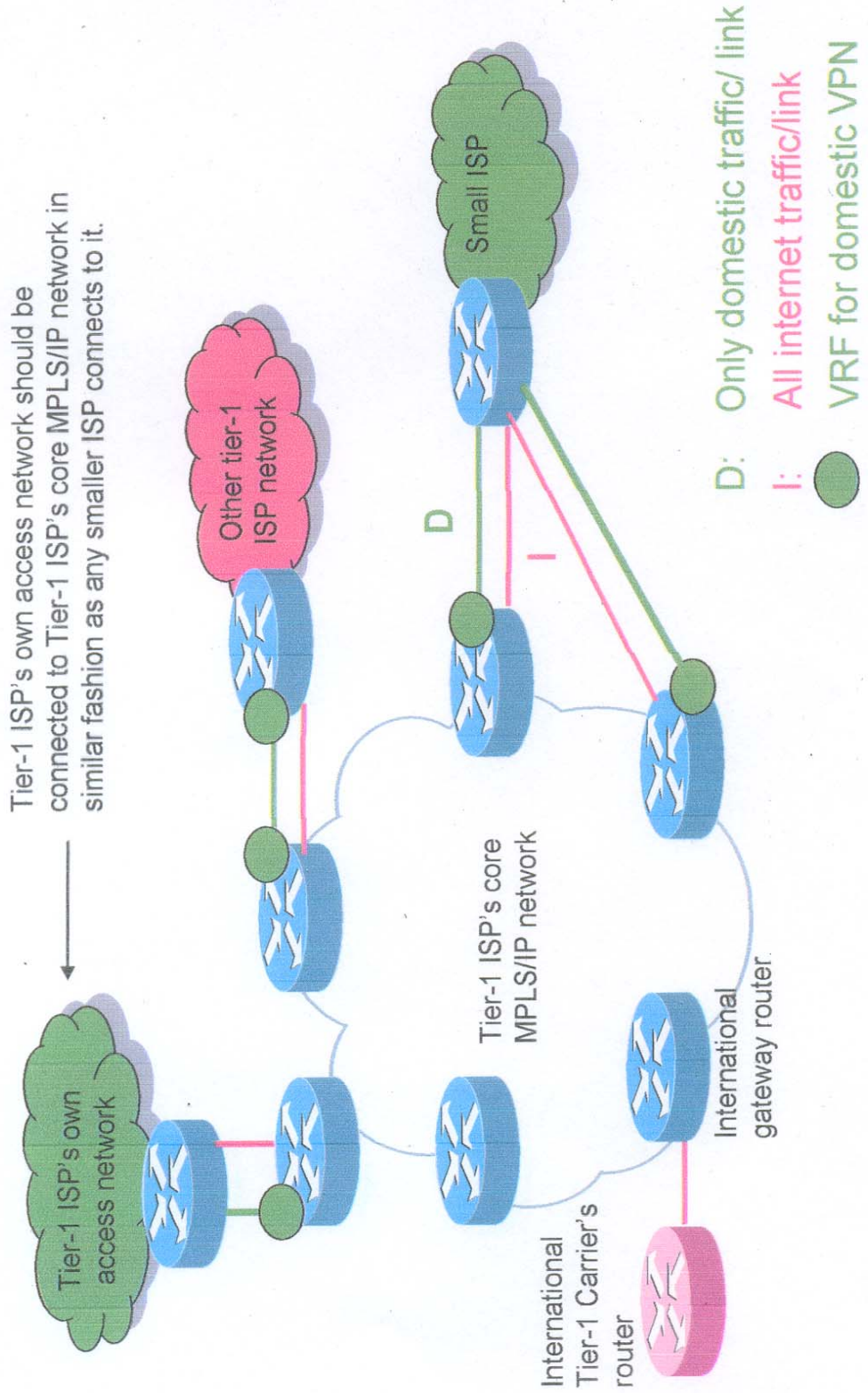
Tier-1 ISPs would not be able to access NIXI routes.	which in turn connected to core network with two links.
<p>Summary & Conclusion:-</p> <p>Splitting the existing network into two separate networks causes huge operational, technical & architectural overhead in maintaining the network due to the reasons listed above.</p> <p>This certainly is not in line with the international best practices and may lead to substantial increase in the cost of operation & servicing end customer.</p> <p>Global ISPs are questioning the relevance of deploying MPLS in the core owing to the trend in increased traffic which is predominantly Video.</p> <p>VSNL is also in the process of selection & finalization of NGN IP Platform on a global basis to replace/migrate existing IP infrastructure. In view of the growing traffic requirement on our global backbone, we are considering IP Core instead of MPLS Core. This RFP is in the final stage of commercial negotiation and once we are through with the commercials, we may implement this in future.</p> <p>As per global best practices the Internet Service Providers have flexibility of choosing technology neutral platforms which provide them operational and commercial efficiency which helps in growth of the entire industry and providing better services to the end customers.</p> <p>Taking away this flexibility from ISPs in India (specially Tier-1) will not create a level playing field for ISPs with in India and will put Indian ISPs in a weaker position with in India as well as globally vis a vis Global Tier-1 ISPs who have plan to serve in India or already competing with Indian ISPs globally.</p> <p>Further, this solution still does not guarantee that the entire domestic traffic will be exchanged with in India and there are potential chances that the traffic may go outside India due to the complex routing dependencies on various stake holders in the entire traffic chain. On the contrary it will increase the cost of operations and the service and is not good for the growth of entire Internet Industry in India.</p> <p>In view of the reasons and the constraints mentioned as above, it would not be technically &</p>	No comments

<p>operationally feasible to segregate International & domestic traffic in the current architecture of the network using MPLS technology. Also, as we are in the process of deploying NGN IP Global Backbone, we may not consider to deploy MPLS in the core.</p>	
<p align="center">Juniper comments</p>	<p align="center">Remarks</p>
<ol style="list-style-type: none"> 1. As of now the number of domestic routes would roughly be 20,000 to 30,000 IPv4 prefixes. Two years to five years down the line, there is expected to be a significant Increase in the domestic prefixes. 2. For the solution to work, one primary pre-requisite is that the SP core has to be modified to enable the CORE to cater to the MPLS VPN functionality. For those SP's which do not have MPLS enabled in their ISP network, this will involve enabling of MPLS on all the routers or carry MPLS traffic over GRE tunnels. Increasing large number of GRE tunnels will remove optimal routing for customers and increase operational challenges. 3. In case, the CORE is to be MPLS enabled, the routers should also be MPLS capable routers from the platform point-of-view as well as from physical RAM, FLASH etc. point of view. Primarily will include extra OPEX and CAPEX. Same is required at customer end. 4. All the internet applications (many of them non-standard applications) running properly under a VRF are not tested and no clue on behavior. 5. Tier 1 or Category-A ISP's will need to deal with completely new BGP configurations and those who use provisioning systems will need to re-look the changes need for their provisioning tools and systems also. 6. At a site a customer prefix needs to be inserted into the Global Internet VRF and Domestic Internet VRF. This will require high-end Routers which have higher scalability of FIB entries and BGP Peering Sessions cost substantially more. If smaller ISPs request full Internet Routing table they need to go in for routers which would cater to the full internet routes. 7. Segregation of domestic & international network will require connecting customers to also run 	<p>Internet in VPN is working in big service provider's network.</p>

BGP. It means that even smaller ISP & enterprise customer would need to invest in high-end routers to be able to accept more than default route. They would also need BGP/OSPF protocols with the upstream service provider which means more resources required in terms of skilled manpower and thus higher cost.

8. Tier 1 ISP's must ensure smaller ISPs & enterprise customers must have the right configurations to work, this is just not under the control of Tier1 ISP's
9. Internet in a VRF solution requires complete re-design of the routing architecture currently followed. A large number of routes to be placed under a single VRF and expected to grow substantially needs to be tested thoroughly as no Service Provider in the world is placing such a large number of routes under a single VRF. Two years to five years down the line, there is expected to be a significant Increase in the domestic prefixes and it may turn out to be operational nightmare to manage.
10. The field-proven ness of the solution needs to be thoroughly tested and simulated as no precedence exists for it anywhere in the Global SP environment.
11. Since the solution provided by TEC would involve major restructuring of Internet infrastructure of all TIER-1 Service Providers, it would be prudent to consider the same which might affect the present and growing Internet Customer base. Since final cost of internet bandwidth also depends on the cost of infrastructure borne by SP's, it might have to be passed on to the end customer.
12. One of the options for achieving the required segregation of domestic and international internet traffic would be to make NIXI(National Internet Exchange) , the Internet exchange point for all domestic routes with all Service Providers announcing and exchanging all domestic routes through NIXI.

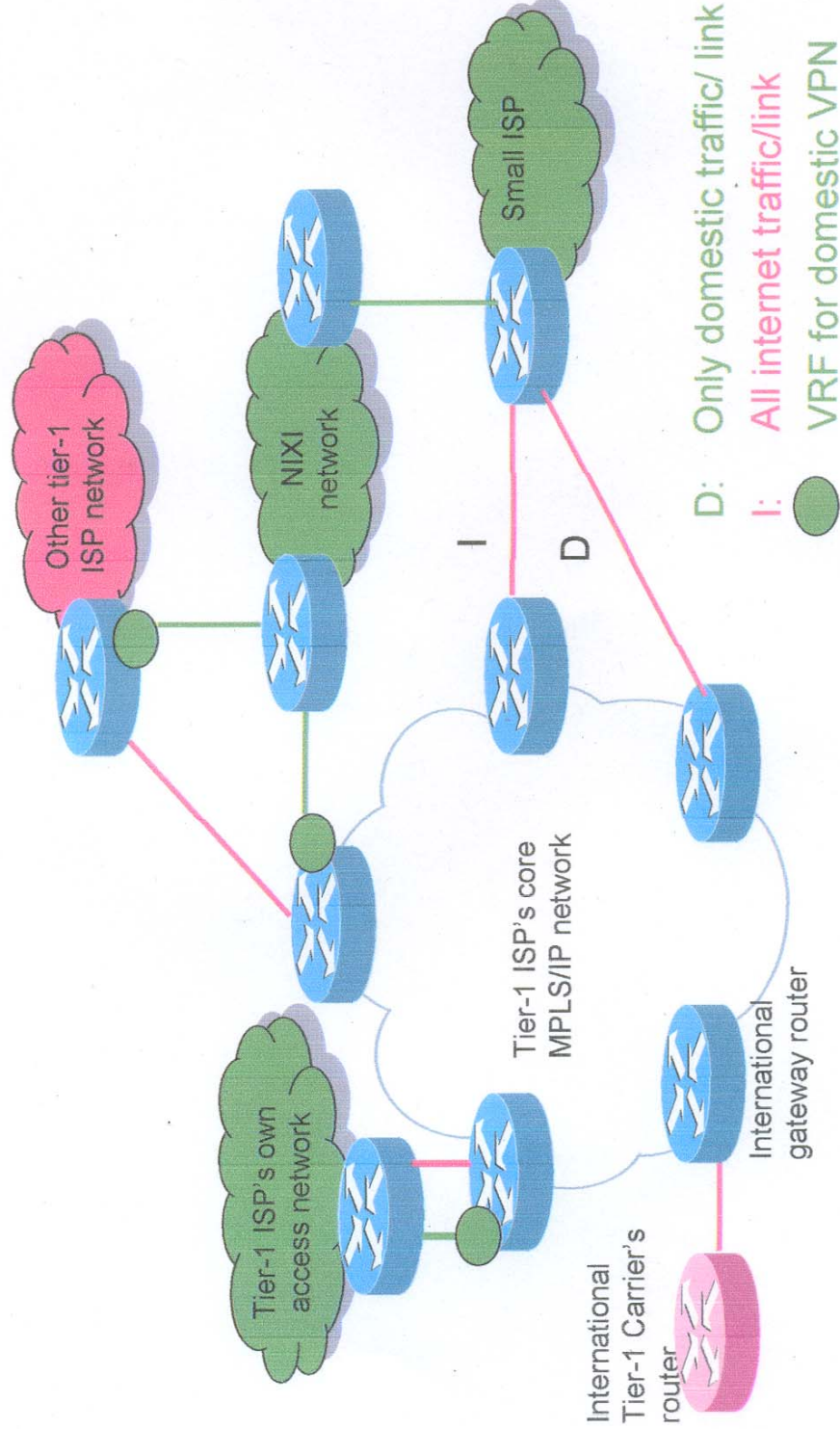
Segregation of international and domestic traffic option 1 (without NIXI)



Segregation of international and domestic traffic option 1 (without NIXI) cont...

- Tier-1 ISP need to run MPLS in their network for domestic peering. All and only domestic routes should be available in the D VPN. D VPN shall not be connected to international gateway.
- Tier-1 ISP has choice to carry internet traffic belong to international destinations in VPN/ over native routing in same network or he may have a different network based on his choice for carrying the same.
- Small ISP shall announce his routes to both links (I and D). However small ISP sends domestic traffic on D link and international traffic on I link. In case small ISP send international traffic on D link, the traffic will never reach to its destination as D VPN do not have international routes. I link can take all internet traffic and can be used even for domestic traffic in case of domestic link failure. Small ISP network itself need not to be MPLS enabled.
- Tier-1 ISP's own access network should be connected to Tier-1 ISP's core MPLS/IP network in similar fashion as any smaller ISP connects to it (with two links). Tier-1 ISP shall also announce his routes to both links (I and D) but the domestic traffic should only be send on D link. This arrangement will ensure that the domestic traffic of customers of Tier-1 ISP connected with single link (I link) will also flow through D VPN. Access network of Tier-1 ISP, itself need not to be MPLS enabled.
- In case the routers of tier-1 IPS and small ISP are connected with Ethernet link, these two interfaces can be logically separated over same physical interface.
- Connectivity to other Tier -1 ISP shall be again through two links. Domestic peering shall be done on D link only. This arrangement will ensure that the domestic traffic of customers of other Tier-1 ISP connected with single link (I link) will also flow through D VPN.
- Small ISPs has a choice to take the D link or not, otherwise they can always connect only on I link.

Segregation of international and domestic traffic option 2 (with NIXI)



Segregation of international and domestic traffic option 2 (with NIXI) cont...

- This option is similar to option 1 except that domestic peering will only be done through NIXI.
- NIXI shall be connected to D VPN of Tier-1. NIXI shall only learn the domestic routes announced by the peering partners. It shall not have any international route. No default gateway should be configured in NIXI.
- However this option is technically inferior to option 1 as it mandates the involvement of the NIXI as transit point for all inter ISP domestic traffic which can be avoided by direct peering.

QoS Recommendations on NIXI

1. All critical components of NIXI node should be up for 99.9% of time in a year. These critical components are NIXI routers/Switches, interface module on which the links of the ISPs are terminated and any other equipment which affects the NIXI traffic. Non critical faults which do not affect NIXI traffic like failure of one power supply module should be rectified by NIXI within 48 hours.
2. Switching Architecture of NIXI should be non-blocking, so that it does not introduce any delay.
3. Uninterrupted power should be ensured to the equipment of the ISP and NIXI router itself in the NIXI node. Power availability can be 99.95% in a year.
4. NIXI should ensure proper carrier class environment (Proper Air-conditioning with Humidity control) for housing equipments of NIXI and its member ISPs
5. **Augmentation of ISPs Bandwidth to NIXI:-**

ISP should augment its bandwidth to NIXI, if the utilization of the existing link exceeds 70% of the capacity for 4 hrs in a day and for 5 days. Such capacity management shall be through increase of capacity and not through reduction routes announced. The augmentation should normally be completed within a period of one month after NIXI intimates to the concerned ISP. This time should be extendable by one more month in valid cases like ISP not having last

mile and in case some additional equipment is required to be procured.

6. Carrier class facility for ensuring security of NIXI equipments like access control, monitoring and keeping records of entry in equipment room etc should be ensured.

Abbreviations

APJII	Association of Internet Service Providers of Indonesia
APNIC	Asia Pacific Network Information Centre
AAPT	Australian Associated Press Telecommunication
AS	Autonomous System
AUIX	Globalcenter Internet Exchange
BGP	Border Gateway Protocol
BSNL	Bharat Sanchar Nigam Limited
CAPEX	Capital Expenditure
CPU	Central Processing Unit
CSP	Content Service Providers
CUHK	Chinese University of Hong Kong
DIT	Department of Information Technology
DoT	Department of Telecommunications
FIB	Forwarding Information Box
Gbps	Gigabit Per Second
GRE	Genetic Routing Encapsulation
HKIX	Hong Kong Internet Exchange
IIX	Indonesia Internet Exchange
IP	Internet Protocol
IPLC	International Private Lease Circuit
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
ISP	Internet Service Provider
ISPAI	Internet Service Providers Association of India
IT	Information Technology
ITSC	Information Technology Services Centre
IX	Internet Exchange
IXP	Internet Exchange Point
LAN	Local Area Network
LINX	London Internet Exchange
LIPEX	London Internet Providers Exchange
LoNAP	London Network Access Point
MaNAP	Manchester Network Access Point
Mb	Mega bits
MPLS	Multi Protocol Label Switching
NGN	Next Generation Network
NIXI	National Internet Exchange of India
NLDO	National Long Distance Operator

OEM	Original Equipment Manufacturer
OPEX	Operational Expenditure
OSPF	Open Shortest Path First
PE Router	Provider Edge Router
PoP	Point of Presence
QoS	Quality of Service
RAM	Random Access Memory
RBIEX	Redbus Interhouse Internet Exchange
RFP	Request for Proposal
SBO	Service Based Operators
SCOTIX	Scottish Internet Exchange
SiX	StarHub IP Exchange
SKA	Sender Keep All
SOX	Singapore Open Exchange
SP	Service Provider
TEC	Telecom Engineering Centre
TRAI	Telecom Regulatory Authority of India
USA	United States of America
VIX	Victorian Internet Exchange
VPN	Virtual Private Network
VRF	Virtual Routing & Forwarding
VSNL	Videsh Sanchar Nigam Limited
WAIA	West Australia Internet Association
WAIX	West Australia Internet Exchange