



IPv6 Transition strategies

White paper November 2003

Author: Saisree Subramanian

Table of Contents

1	INTRODUCTION	3
2	BACKGROUND.....	3
3	SCENARIOS FOR IPV6 DEPLOYMENT	4
4	TRANSITION METHODOLOGIES.....	5
4.1	TUNNELING MECHANISMS.....	7
4.1.1	<i>Configured tunnels.....</i>	7
4.1.2	<i>Automatic tunnels</i>	7
4.1.3	<i>6to4.....</i>	7
4.1.4	<i>ISATAP</i>	7
4.1.5	<i>Tunnel Broker</i>	7
4.1.6	<i>NAT-PT with SIIT.....</i>	7
4.1.7	<i>Transport relay translators.....</i>	8
4.1.8	<i>Socks64</i>	8
4.1.9	<i>Shipworm.....</i>	8
4.1.10	<i>DSTM.....</i>	8
4.1.11	<i>BIS.....</i>	8
4.1.12	<i>6over4.....</i>	8
4.1.13	<i>Bump in the API.....</i>	8
4.2	SOME IMPORTANT ASPECTS OF TRANSITION	9
4.2.1	<i>Routing protocols.....</i>	9
4.2.2	<i>DNS support</i>	9
4.2.3	<i>Network management.....</i>	9
4.2.4	<i>Which technique should I choose?.....</i>	9
5	CONCLUSION.....	10
6	ACRONYMS AND DEFINITIONS	10
7	REFERENCES	10

1 Introduction

Next Generation IP or IPv6 is a technology which is gaining a lot of momentum. This proposes a major change in the basic network infrastructure of the internet and is poised to have far-reaching effects due to the ubiquity of the internet today. In this paper, basic issues on the transition from the current IPv4 networks towards IPv6 are addressed giving a brief overview of how the transition can happen and an introduction to the relevant technical issues in this area.

2 Background

IP is a basic layer of the networking stack and the IP address is a fundamental identifier for any entity on the network. The primary problem that is being addressed by moving to IPv6 is the lack of IPv4 addresses with the current addressing scheme. IPv6 offers 128 bit addresses which are foreseen to be large enough for future purposes. While upgrading the address structure, various other features are being built into the new IP protocol to easily enable features like security, QoS, mobility etc. (Note: These features can be used with IPv4 also, but IPv6 is better tuned towards these features).

The change in the IP address structure impacts the whole networking stack. Firstly, the IP layer needs to be completely replaced and the new IP layer has to be tuned to run over the various L2 mechanisms that are prevalent today. Then the transport protocols have to be built which use the new IP layer (TCP, UDP and other new transport mechanisms like SCTP). Most of today's applications are built on top of a socket layer and hence they have to be updated to use new socket mechanisms.

Since this task is fairly complex, it is not possible to throw away the existing IPv4 network and adopt IPv6 immediately. It is foreseen that the transition will happen in stages with a few IPv6 nodes introduced into an IPv4 network and the number gradually increasing over time till some time in the distant future when the entire network becomes IPv6.

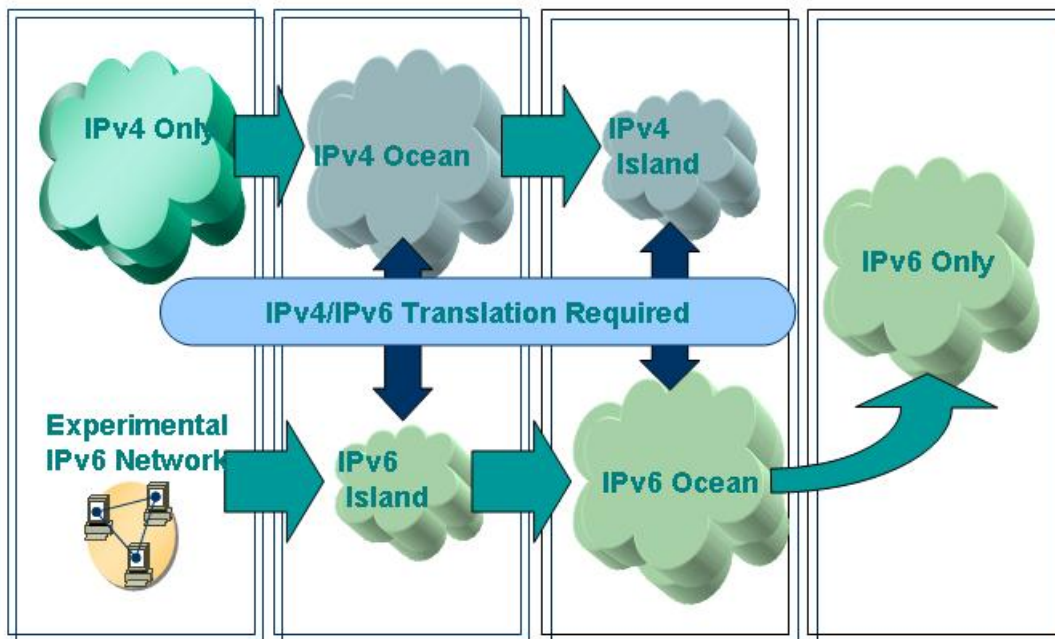


Figure 1: IPv4-IPv6 transition (Acknowledgement: Presentation made by Seungyun Lee from ETRI titled “IPv6 Status in Korea”, Global IPv6 Summit in Japan, Dec 2001)

It is fairly evident that it would be impossible for the entire internet to work only on IPv6 since the existing backbone IPv4 networks would pose a great difficulty towards complete adoption of IPv6. Hence there is a requirement for co-existence of the two networking technologies and internetworking requirements have emerged.

3 Scenarios for IPv6 deployment

Since the existing internet backbone would continue to remain an IPv4 network, the scenario of how IPv6 will be deployed needs to be understood.

Next generation wireless networks are a hot topic in today’s world. Irrespective of whether European or American standards are followed, it is clear that the end-user terminal will have to support both voice and data features. While the requirements of data traffic did not require the device to be a uniquely addressable entity (it is possible to have a scenario of private addresses and usage of an address translation gateway), a voice channel requires the setup of a peer-to-peer connection where the terminal needs to be directly addressable in order to be contacted by external applications. With the arrival of broadband technologies, and the always-on internet, even data applications (for example, multi-party gaming) bring in requirements for unique addresses. With the current rapidly diminishing pool of IPv4 addresses, it would be infeasible to support such requirements. Hence, wireless networks become the most important business case to serve as a driver to migrate towards IPv6.

Even within wired networks, IP has become an essential part of network. There is a move away from circuit switched networks towards packet switched networks or IP networks while attempting to retain some of the features of circuit switching (for example, end-to-end connectivity) through additional features/applications built on top of IP. In countries like Japan, which are acknowledged leaders in technology deployment (considering the fact that I-mode has been available in Japan for the past few years), the scarcity of IPv4 addresses is felt very deeply and hence it is taking the lead to move towards IPv6. Countries like US which have already received huge blocks of IPv4 addresses do not yet feel the requirement to move towards IPv6. This results in a strange scenario where the technical superiority of the new protocol is strongly established, but the business case for deployment makes sense only in pockets.

To briefly cover the deployment status of IPv6, it is widely deployed in test networks especially in Japan and Europe and is being followed by China and Korea. Japanese ISPs have started commercial sales of IPv6 addresses. IPv6 is completely endorsed by the IETF but is not deployed much in the US. Earlier this year, the US Department of Defence has established a goal of transitioning to IPv6 by 2008 and as a first step the DoD has announced that any new equipment purchased after September 2003 should support IPv6.

There has been a huge test network called the 6-bone which consists of independent sets of IPv6 networks across the globe linked together by special tunneling mechanisms over the IPv4 internet. As IPv6 slowly moves into becoming a production technology rather than an experimental technology, the 6-bone will be phased out (date for phase out set at 2006).

Equipment vendors all over the world are today including IPv6 support as a checkbox item in any network equipment that is being manufactured allowing the ISP the freedom to decide whether to use it. The missing link is unavailability of applications supporting IPv6 – the port of existing applications and creation of new applications is yet to happen on a large scale.

4 Transition methodologies

The transition towards IPv6 is a topic which has been in discussion for years. There is no exclusive or correct mechanism but various organizations have defined and tested multiple methodologies. At a very basic level, there are two different categories of transition mechanisms:

- Mechanisms deployed at specific devices, which are designated gateways to a network
- Mechanisms which involve change to every host in the network

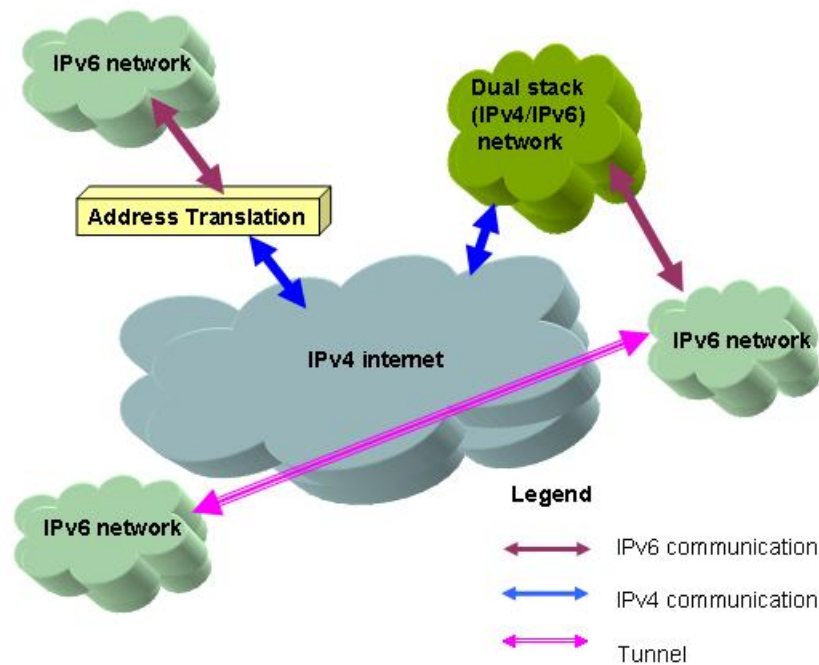


Figure 2: Different transition technologies

The above diagram illustrates the different types of technologies that can be used like tunnels, address translation techniques and dual stack devices.

The most widely deployed mechanism is to make changes to the network gateway since this scheme is a tried and tested method and can be directly applied to the scenario of having a small IPv6 island network connecting to the IPv4 internet. Some of the techniques available are:

- ❖ Tunneling mechanisms
- ❖ NAT-PT with SIIT
- ❖ Transport relay translators
- ❖ Socks64
- ❖ Shipworm

For host to host communication there are some techniques like:

- ❖ DSTM
- ❖ BIS
- ❖ 6over4
- ❖ BIA

Overall sixteen different transition technologies have been currently identified and with the possibilities of interactions between different networks implementing different mechanisms a very complex picture of the mixed IPv4-IPv6 internet emerges.

The V6OPS working group at IETF is focusing on prioritizing and recommending appropriate transition mechanisms for different network scenarios. One major concern that the V6OPS group is trying to address is the inherent problem for transitioning to IPv6 due to too many transition

mechanisms being available. This paper lists many of the available techniques although some of them are not being given a very high priority in the current discussions at the V6OPS working group.

4.1 Tunneling mechanisms

The simplest co-existence mechanism is of tunneling one protocol through the other. In this case, at the egress point of the IPv6 network, the IPv6 packet is converted to IPv4 payload till it reaches the tunnel end-point on the IPv4 network where the IPv4 header is stripped off and the IPv6 packet is routed to its ultimate destination. There are different ways in which tunneling can be achieved.

4.1.1 Configured tunnels

Manually configured tunnels are used to set up permanent pathways for IPv6 across the IPv4 internet. Much of the 6bone operates in this fashion. Routing decisions require the information on all tunnel end points (which IPv6 addresses are available behind which IPv4 address) and the tunneling software needs to be installed on the gateway.

4.1.2 Automatic tunnels

Automatic tunnels are set up when required and torn down at the end of the traffic relay. This mechanism requires "IPv4 compatible" addresses that are available to each IPv6 host which are used to derive the tunnel endpoints, thereby forcing a major limitation on the usage of this technique.

4.1.3 6to4

This mechanism uses unique 6to4 prefixes in the IPv6 address to determine the IPv4 address of the egress gateway and hence is widely used as a tunneling mechanism.

4.1.4 ISATAP

ISATAP is an Intra-Site Automatic Tunneling Addressing Protocol that connects IPv6 hosts and routers within IPv4 networks. ISATAP treats the site's IPv4 infrastructure as non-broadcasting multiple access link layer and tunnels the IPv6 payload in an IPv4 packet.

4.1.5 Tunnel Broker

When an isolated IPv6 host within an IPv4 only network would like to contact an external IPv6 network, it uses the facilities of a tunnel broker which ensures the management of the tunnel – IPv6 address allocation to the host, DNS reachability information propagation to remote IPv6 networks etc.

4.1.6 NAT-PT with SIIT

NAT-PT is a well established translation mechanism. This is merely an extension of the existing NAT mechanism, which allows a private IPv4 network to exist behind a few defined public IPv4 addresses. In the case of NAT-PT the private network can be an IPv6 network. SIIT or Simple IP-ICMP Translation is the technique defined to translate between IPv4 and IPv6 payloads. As in the case with NAT, ALGs or Application Layer Gateways have to be defined for each application which requires passing through the NAT-PT gateway.

Note: Another technique for IPv6 packet transmission across IPv4 networks is under discussion at the V6OPS group involving the use of the existing functionality to forward packets of protocol type 41 which is available with many v4-only NAT implementations.

4.1.7 Transport relay translators

Conceptually these are exactly the same as NAT-PT devices except that the translation is done at the transport layer rather than the IP layer – (ie) at the TCP/UDP layer.

4.1.8 Socks64

This is again an extension of the existing socks-proxy techniques that are used in a pure IPv4 world. The Socks clients would run over IPv6 and the server would be upgraded to service such clients. The limitation of socks that all applications have to be “socksified” would continue to apply in the new scenario also.

4.1.9 Shipworm

Shipworm or Torpedo is a technique for the transport of UDP packets across NATs which works well in the scenario when there is a private IPv6 network behind the NAT machine. Torpedo servers and relays are designated machines which allow the overlay of the Torpedo network over the existing IPv4 network. IPv6 packets are encapsulated as UDP payload and are relayed by the Torpedo relay which is available within the local network to the connected Torpedo server, from there it is routed to the appropriate Torpedo server nearest to the ultimate destination where the decapsulation of IPv6 is handled by the Torpedo relay. Torpedo is defined as a last resort mechanism to be used where 6 to 4 or other tunneling mechanisms are unavailable since there is an overhead due to the encapsulation into UDP.

4.1.10 DSTM

The best mechanism for individual hosts to communicate in the absence of a gateway mechanism is to implement both IPv4 and IPv6 stacks on the device. Since most vendors ship with this feature today, DSTM has evolved as a transition mechanism. All the devices in the network are configured for IPv6 but not for IPv4, a single machine within the network operates as a DSTM server allotting temporary IPv4 addresses to devices on a need basis to enable communications over the IPv4 network.

4.1.11 BIS

Bump-in the-stack is a technique for non-IPv6 compliant applications on an IPv4 only host to communicate with IPv6 hosts. The IPv4 stack on the host has a “bump” added which converts the specific packets designated to the IPv6 destination into IPv6 packets and performs the reverse mapping for the replied packets.

4.1.12 6over4

This technique encapsulates IPv6 in IPv4 without explicit tunnels. Other than the requirements for dual stack support on hosts, a gateway port also requires specific configuration to work as 6over4 interface.

4.1.13 Bump in the API

BIA is a technique similar to BIS. While the IP layer did the translation for BIS, the transport layer translation is done for BIA by having an API translator function between the socket layer and the actual transport layer. BIA requires a complete dual stack host, however, the application can be either IPv4 or IPv6 enabled but can still freely communicate in either network.

4.2 Some important aspects of transition

4.2.1 Routing protocols

Routing is the most important function in the internet which relies completely on IP addresses for the propagation of reachability information. With the transition towards IPv6 and in a mixed network scenario, existing routing protocols for both interior and exterior routing require upgrades.

The IGP protocols like OSPF, RIP and IS-IS have directly newer versions defined which operate on IPv6 addresses as the basic identifiers.

There is only one EGP used in the internet – BGP-4. BGP-4 is merely used to propagate reachability information between autonomous systems and leaves the specifics of routing within the autonomous system to IGPs. Extensions have been defined on BGP-4, which allow the exchange of information on non-IPv4 protocols which includes IPv6. Also, BGP-4 operates over TCP sockets and the protocol can function irrespective of whether the transport medium is IPv4 or IPv6. BGP-4 has been extensively used in the 6bone for propagating the routing information of IPv6 networks.

4.2.2 DNS support

DNS support requires some specific attention. The existing DNS mechanism for IPv4 networks provides the name to address lookup and the reverse mapping from address to name. The name servers now require to store the associated IPv6 address of a name (in addition to the IPv4 address) as well as they should be able to perform the reverse lookup functionality.

The DNS records for IPv6 currently use the A6 format or the AAAA format (A6 has experimental status and AAAA is the preferred IETF supported mechanism). Hence a DNS client requiring the IPv6 address of a host would request the server for the AAAA entry (not many servers support A6) of that host. If the entry is found, it is used directly, otherwise the A entry corresponding to the IPv4 address is retrieved and mapped into an IPv6 address by using standard procedures.

4.2.3 Network management

SNMP is the de-facto management protocol used in the current internet. As new standards are being defined for the IPv6 protocol and all other related technologies, the corresponding SNMP MIB definitions for these are also being made. However, vendor adoption of these MIBs has been slow and recently vendors have started implementing some of the MIBs. The standard transport mechanism for SNMP is over UDP which could run either over IPv4 or IPv6 with appropriate changes to the socket layer. Standard SNMP management platforms like HP-OV have basic support for IPv6 available and are also indicating roadmaps with full feature support for IPv6. Unless sufficient management tools are available, the commercial deployment of IPv6 would be difficult since ISPs and enterprise network managers require the tools to configure and monitor IPv6 networks. The tools become very important especially in a mixed network scenario where the network manager will have to keep track of tunnels, routing issues, DNS configurations etc across both IPv4 and IPv6 networks.

4.2.4 Which technique should I choose?

There is no straightforward answer to this question and difficulty compounds when we consider the vast list of possible techniques suggested in previous sections. Network operators and administrators choose to experiment with a few techniques and the IETF V6OPS workgroup is working towards providing guidance in the choice of these techniques for different usage scenarios. Further, since multiple transition techniques are defined, it is likely that multiple techniques can be used within a local network and hence the network administrator has to consider issues arising out of combinations of techniques. For example, DSTM and ISATAP

have opposite functions and should not be used on the same host. The network administrator would require comprehensive tools to configure and manage a network where multiple transition techniques interact with each other.

5 Conclusion

This paper briefly covers the mechanisms and the issues involved in the transition from pure IPv4 networks into a mixed IPv4-IPv6 networks and the further progress into pure IPv6 networks. Since many aspects are still undergoing standardization, commercial implementation of the transition has got delayed. Several experimental networks working individually and the 6bone on a global level have established the viability of creating IPv6 island networks within the IPv4 network. However, applications and management/network configuration tools are required to be migrated to work in mixed network scenarios before the transition becomes a reality.

6 Acronyms and definitions

ALG	Application Level Gateway
BGP-4	Border Gateway Protocol – version 4
BIS	Bump-in-the-stack
DNS	Domain Name Service
DSTM	Dual Stack Transition Mechanism
EGP	Exterior Gateway Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IP	Internet Protocol
ISATAP	Intra Site Automatic Tunnel Addressing Protocol
IS-IS	Intermediate System to Intermediate System Intra-domain routing exchange protocol
MIB	Management Information Base
NAT-PT	Network Address Translation – Protocol Translation
OSPF	Open Shortest Path First
QoS	Quality of Service
RFC	Request for Comment
RIP	Routing Information Protocol
SCTP	Stream Control Transmission Protocol
SIIT	Simple IP-ICMP translation
SNMP	Simple Network Management Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

7 References

1. S. Thomson and C. Huitema, "DNS Extensions to support IP version 6", RFC 1886, December 1995.
2. Malkin, G. and R. Minnear, "RIPng for IPv6", RFC 2080, January 1997.
3. R. Callon, D. Haskin, "Routing Aspects of IPv6 Transition", RFC 2185, September 1997.
4. Bates, T., Chandra, R., Katz, D. and Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 2283, February 1998.
5. B. Carpenter, C. Jung, "Transmission of IPv6 over IPv4 Domains without Explicit Tunnels", RFC2529, March 1999.

6. P. Marques, F. Dupont, "Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing", RFC 2545, March 1999.
7. R. Gilligan, S. Thomson, J. Bound, W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 2553, March 1999.
8. R. Coltun, D. Ferguson, J. Moy, "OSPF for IPv6", RFC 2740, December 1999.
9. G. Tsirtsis, P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000.
10. K. Tsuchiya, H. Higuchi, Y. Atarashi, "Dual Stack Hosts using the Bump-in-the-Stack technique", RFC 2767, February 2000.
11. R. Rockell, R. Fink, "6Bone Backbone Routing Guidelines", RFC 2772, February 2000.
12. T. Bates, R. Chandra, D.Katz, Y. Rekhter, "Multiprotocol Extensions for BGP-4", RFC 2858, June 2000.
13. M. Crawford, C. Huitema, S. Thomson, "DNS Extensions to Support IP Version 6", RFC 2874, July 2000
14. R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 2893, August 2000.
15. A. Durand, P. Fasano, I. Guardini, D. Lento, "IPv6 Tunnel Broker", RFC3053, February 2001
16. B. Carpenter, K Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC3056, February 2001
17. H. Kitamura, A. Jinzaki, S. Kobayashi, "A SOCKS-based IPv6/IPv4 Gateway Mechanism", RFC3089, April 2001.
18. J. Hagino, K. Yamamoto, "An IPv6-to-IPv4 transport relay translator", RFC3142, June 2001.
19. Seungyun Lee et al, "Dual Stack Hosts using "Bump-in-the-API" (BIA)", RFC 3338, October 2002.
20. C. Hopps, "Routing IPv6 with IS-IS", draft-ietf-isis-ipv6-05, January 2003 (work in progress).
21. C Huitema, "Teredo: Tunneling IPv6 over UDP through NATs", draft-huitema-v6ops-teredo-00, June 2003 (work in progress).
22. R. Fink, R. Hinden, "6bone (IPv6 Testing Address Allocation) Phaseout", draft-fink-6bone-phaseout-04, June 2003, work in progress
23. J. Bound, (editor), "Dual Stack Transition Mechanism (DSTM)", draft-bound-dstm-exp-00, August 2003 (work in progress).
24. F. Templin, T. Gleeson, M. Talwar, D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", draft-ietf-ngtrans-isatap-16, October 2003, (work in progress).
25. Myung-Ki Shin et al, "Application Aspects of IPv6 Transition", draft-shin-v6ops-application-transition-01, October 2003, (work in progress).
26. E. Nordmark, R. E. Gilligan, "Basic transition mechanisms for IPv6 hosts and routers", draft-ietf-v6ops-mech-v2-01, October 2003, (work in progress)
27. J. Palet et al, "Forwarding protocol 41 in NAT boxes", draft-palet-v6ops-proto-41-nat-03, October 2003, (work in progress).
28. <http://ipv6.disa.mil/> - Website of the US Department of Defense on IPv6

About the Author

Saisree is a Technical Manager associated with Wipro for 8 years. The **author's** specific areas of interest are next generation networking protocols and network management techniques.

Contact Us:

If you need to contact us regarding any clarification or feedback, mail us at timktg@wipro.com

About Wipro Technologies

Wipro is the first PCMM Level 5 and SEI CMMi Level 5 certified IT Services Company globally. Wipro provides comprehensive IT solutions and services (including systems integration, IS outsourcing, package implementation, software application development and maintenance) and Research & Development services (hardware and software design, development and implementation) to corporations globally.

Wipro's unique value proposition is further delivered through our pioneering Offshore Outsourcing Model and stringent Quality Processes of SEI and Six Sigma.

Wipro in T&I

Wipro T&I offers comprehensive solutions for telecommunications to confront challenges, and convert every challenge into an opportunity. With over two decades of Telecom experience, Wipro T&I offers a wide range of solutions in the following domains:

- Wireless Networking
- Broadband ((Data, optical and access networking)
- Voice Switching
- Network Management
- Hardware Design

Wipro T&I also provides several IPs, Components and Reference Solutions in these domains which help our customers in reducing Time to Market and Save Costs. We offer complete Consulting, Architecting, Design, Implementation and Maintenance Services to the Telecom Equipment Manufacturers. We do not sell or manufacture any products as we are very focused in the R&D and Engineering Design Services Outsourcing.