

LIPA: Local IP Access via Home Node B

By: Siddhartha Kundalkar and Madhur Raj N.

Overview

Local IP Access (LIPA) is the ability for an IP-enabled device to access a consumer's home-based local area network as well as the broader Internet directly using the air interface of a femtocell, or Home NodeB (HNB). Using LIPA allows for greater performance, innovative services that mesh mobile and home networks, and the off-loading of traffic from the operator's packet core network which is ultimately destined for the Internet.

Enabling LIPA benefits mobile operators, subscribers and Internet Service Providers (ISPs). For mobile operators, the ability to offer LIPA via the HNB would mean higher revenues by way of value added services without having to invest significantly in upgrading network infrastructure to cope with the higher speeds that such applications would demand. For subscribers, LIPA would mean faster and more secure on-the-move data transfer since traffic within the home network would not travel outside the subnet. Users could add customized high-speed applications like file transfer, video streaming and device sharing without involving the operator's core network, thus avoiding associated bottlenecks and possibly yielding lower data costs since the operator is not burdened. For ISPs, who might or might not be part of the same company as the mobile operator, LIPA would mean the ability to offer specialized high-value services with higher quality of service. Thus, the offering of LIPA for mobile devices via the HNB would present a win-win-win situation for all parties involved.

CONTENTS

Why LIPA? *pg. 2*

Requirements Related to LIPA *pg. 2*

Architectural Issues and Solutions *pg. 2*

Conclusion *pg. 9*

Glossary *pg. 9*

References *pg. 11*

Why LIPA?

As connected device (i.e., mobiles, laptop data cards, USB dongles, etc.) penetration increases globally, more and more users are using their mobile devices not just for voice but also for data services. Today's high-speed mobile broadband access technologies—including Wideband CDMA (WCDMA) and Long Term Evolution (LTE)—are ensuring that users have the dual benefits of high mobility and high speed data access. The ever-increasing content available online via email, social networking sites, blogs, RSS feeds, multimedia calls, streaming video and online music coupled with faster and higher capacity equipment driven by personal digital assistants (PDAs), smartphones and netbooks have led to a boom in the demand for Internet data access using high-speed mobile network infrastructure.

As a result, many operators are faced with bandwidth and network capacity limitations, thus putting a tremendous strain on the existing network infrastructure—hence operators are investing significantly in ramping up existing network capacity on the access network as well as in the core of the network. On the access network side, the introduction of HNBs ensures efficient usage of radio spectrum by allowing home users to access the network through the HNB using a local IP backhaul link to the core network. However, this puts an increasing amount of stress on core network nodes such as SGSN and GGSN since more HNBs connected to the core network means that these nodes have to handle exponentially higher traffic.

Since HNBs typically use the ISP's broadband link to provide backhaul connectivity to the core network, it would lessen the stress on core network nodes if IP traffic generated via the HNB were routed through the ISP's Internet access gateway. This would also reduce the number of hops taken by the IP data to reach the destination. Another benefit would be the ability to communicate with other devices within the local subnet without having to go via the mobile operator's core network—hence keeping local traffic truly local. Providing access to the home network connected devices (i.e., desktop/laptop computers, Internet-enabled gaming systems, media centers and so on) provides a rich canvas for the development of services that leverage both these devices and the mobility/broad connectivity of the wireless network.

Requirements Related to LIPA

The requirements for Local IP Access can be broadly classified into two main categories: LIPA to the home network and IP access to the Internet.

For LIPA to the home network, the User Equipment (UE) should be able to exchange data via the operator's core network and LIPA to the home-based network simultaneously, depending upon the destination. The HNB should decide, based upon policies, whether to route the data via the core network or to use LIPA. Furthermore, the UE should be able to access other devices on the home network via the HNB using the HNB only as an access medium.

Access to local IP through the HNB UTRAN-interface should only be granted to UEs with a valid subscription, and pre-Release 9 UEs should be able to use LIPA. What this means is that, as far as possible, no special modifications need to be done to the UE to support LIPA. In addition, it should be possible for a device in the home-based network to contact a UE via LIPA. There should not be any impact felt by the user in accessing packet data services via the existing setup, i.e., through the traditional core network. This means minimal changes needed to the protocol stacks on the core network, few or no additional network nodes being introduced and no impact on the speed of processing signaling or data in the core network.

For IP access to the Internet, it should be possible without needing to traverse the operator's network. What's more, simultaneous access from a UE to both the operator's core network and LIPA to the Internet should be supported. The operator or the HNB owner, within the limits set by the operator, should be able to enable/disable LIPA to the Internet per the HNB.

It should also go without saying that LIPA to the Internet should not compromise the security of the operator's network. Furthermore, LIPA to the Internet should support the scenario when the HNB and backhaul are provided by the same operator as well as the scenario when the HNB and backhaul are provided by different operators.

Lastly, it should also be possible to distinguish between packets sent using LIPA and packets sent via the operator's core network so as to apply Quality of Service (QoS) policies, differential charging, etc.

Architectural Issues and Solutions

As we saw in the previous section, LIPA enables value added services that benefit users and can help increase the Average Revenue Per User (ARPU) for service providers while reducing the burden on the wireless core network. However, all benefits typically come with costs / issues and LIPA is no exception. To understand these issues, let us look at two alternative solutions for achieving LIPA, the issues these alternatives pose and how to get around those issues. Note that the appendix to this article contains a glossary which helps clarify and explain the definitions of the various acronyms.

The typical setup of a femtocell/HNB appears as given in Figure 1.

Issues

Two scenarios are envisaged, and each has its own set of issues:

1. UE making a data call via a PDP context and such data is routed via HNB/HNB-GW/SGSN/GGSN while simultaneously another application on the UE is accessing the internet via the HNB.
2. UE has a PDP context setup, and the data for this call is routed from HNB directly via router to the Internet instead of going to HNB-GW/SGSN/GGSN/Internet.

For scenario 1, the issues include:

- The IP address for the UE is allocated by the GGSN for the PDP session and the HNB is not aware of this IP address.
- If another data path (not involving a PDP context) is to be setup via the HNB to the Internet, who allocates the IP address to the UE?
- The second IP address would be part of the home network, so is there a DHCP client on the UE that requests for this second IP address?

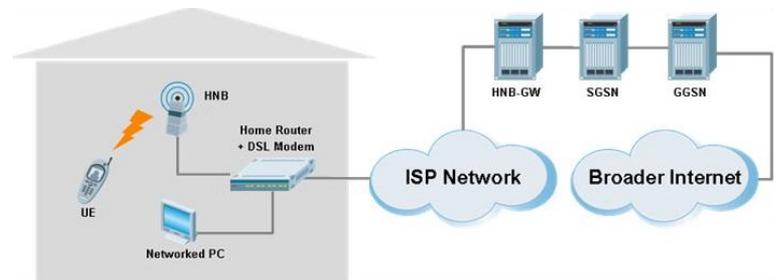


Figure 1. Network Femtocell/HNB Network Architecture

- Would the UE support multiple IP addresses?
- For the second (direct) data session, what triggers the HNB to set up radio bearers?
- How does the HNB distinguish between the PDCP packets that are related to the PDP session and those that are related to the local IP session?
- How does another device in the local network send data to the UE?

For scenario 2, the issues are:

- How does the HNB know the IP address allocated to the UE?
- How does the HNB forward data to the Internet gateway? Is this done transparently (i.e., over the Ethernet to the router/gateway) or does the HNB use its own IP address to tunnel the data?
- How does the router know the IP address allocated to the UE?
- The IP address allocated to the UE by the GGSN would be of a different subnet than the subnet of the home network—so how is the gateway/router able to route packets, especially downlink ones?
- In case another device wants to contact the UE, how does it know the UE's IP address? Also, in the case when this IP address is allocated only for the duration of the PDP session, is it only possible to route data to the UE when a PDP session is created?
- What about QoS differences between the PDP Context and the ISP's broadband network?

Solutions

Some alternative solutions are available to address some of these issues:

1. LIPA solution using a local PDN connection
2. Single UE IP address with LIPA at the HNB
3. Using mobile IP and having the HNB act as a foreign agent

Alternative 1: LIPA Solution Using a Local PDN Connection

In this approach, the UE would be configured with two different access point names (APNs): one for access via the GGSN and another for access via the local router. If the APN sent in the *Activate PDP Context Request* indicated the GGSN, the HNB would route the signaling (and further on the data) to the core network and the IP address would be allocated by the GGSN.

If the APN indicated the local IP network, the HNB would have limited SGSN/GGSN functionality to allocate an IP address from the local DHCP server (possibly from the router component) and send the *Activate PDP Context Accept* to the UE. Data packets sent by the UE using this IP address would be sent to the local router.

Here are additional comments:

- Two PDN connections are assumed for simultaneous LIPA traffic and non-LIPA traffic
- Pre-Release 9 UEs that support multiple Packet Data Network (PDN) connections can simultaneously access LIPA and non-LIPA PDN connections
- For LIPA traffic, a Local P-GW function or Local GGSN function for EPS and UMTS, respectively, is located within the HNB
- For non-LIPA traffic, GGSN is located within the core network
- The LIPA PDN can be identified by a well-defined APN
- Mobility management signaling between the UE and the network is handled in the core network
- Session management signaling (e.g., bearer setup, etc.) for non-LIPA traffic terminates in the core network

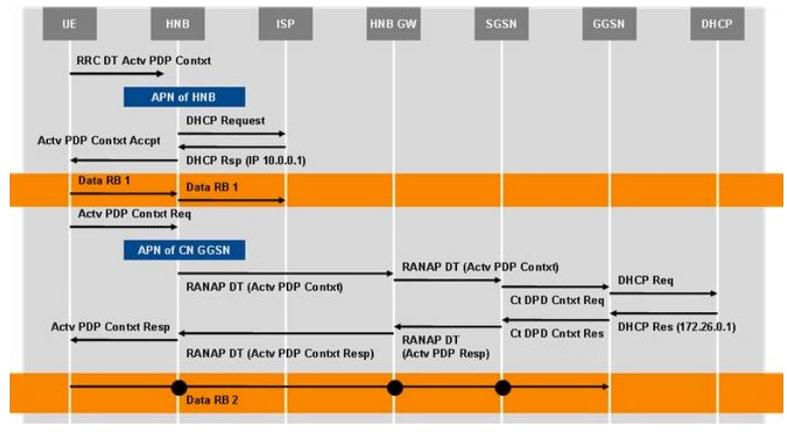


Figure 2. LIPA Solution Based on Traffic Breakout Performed Within the HNB Using a Local PDN Connection

- Before the LIPA PDN connection is established, the UE is authenticated, authorized and registered by the core network

Advantages

1. HNB does not need to inspect the IP data packets to determine routing since both the PDP Contexts would be using distinct radio bearers.
2. Even if one PDP Context is deleted, the data path for the other is not affected.
3. No Network Address Translation (NAT) functionality or mapping is required to be maintained at the HNB in order to route packets correctly.
4. Since the HNB does not need to modify the contents of the packets in order to route them, a lighter processing load and higher speed is achieved.
5. Handover of the GGSN-associated PDP Context to another HNB/macro RNC is easier and is not affected by the other PDP Context.
6. Differential charging for data based upon the destination is easier since distinct radio bearers are used.
7. Differential QoS based upon the destination address (packets destined for a node within the subnet versus packets to be routed via the GGSN) is easier to achieve.

Disadvantages:

1. The HNB needs modification for SGSN/GGSN functionality.
2. The UE should be able to support multiple APN configurations.

Alternative 2: Single UE IP Address with LIPA at HNB

In this approach, the UE would be configured with only one APN. It is not aware of the distinction between LIPA and GGSN; thus, it would be aware of only one IP address. This address would be allocated by the GGSN in the *Activate PDP Context Accept* message and this SM message would be read by the HNB to derive the IP address allocated to the UE. The HNB would then request for a local subnet IP address from the DHCP server and map this IP address to the GGSN allocated IP address. The HNB would be able to route packets either via GPRS Tunneling Protocol (GTP) through the Core Network or via the local router. The HNB would take this decision based upon the source and destination IP addresses of the uplink and downlink data.

In this approach, the HNB would need the ability to decode GMM/SM signaling but not originate or terminate such signaling. Thus, no SGSN- or GGSN-like functionality is required. However, the HNB would need significant Deep Packet Inspection (DPI) capabilities to inspect the IP headers of each packet for taking a routing decision.

Comments

- UEs are only required to activate one PDN connection for LIPA and non-LIPA traffic.
- HNB has the ability to drag/insert the LIPA traffic from/into PDP context/bearers based on destination address
- There is a NAT inside HNB to ensure that returning LIPA traffic reaches the HNB despite a topologically incorrect source address
- Pre-Release 9 UEs that support single PDN connections can simultaneously access LIPA and non-LIPA traffic

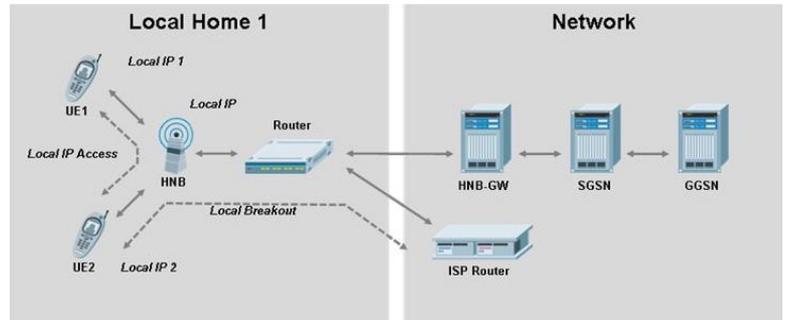


Figure 3. Network Architecture for Single UE IP Address with LIPA at HNB

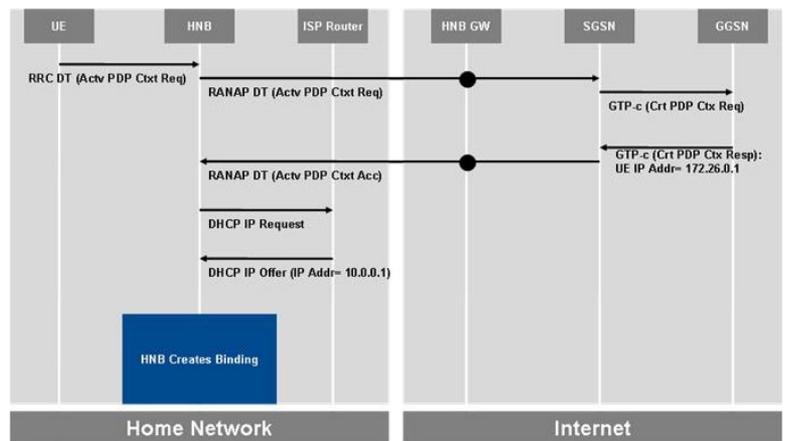


Figure 4. Single UE IP Address with LIPA at HNB

See Figures 3 and 4 for an approach note for LIPA using the local IP router provisioning method described.

During *Activate PDP Context Accept* the GGSN assigns an IP address. The HNB should intercept the contents of SM signaling messages to decipher the IP address allocated to the UE. The HNB then queries for a DHCP request from the local router for the UE. Using the allocated local IP address from the router, the HNB creates a mapping between the local IP address and the GGSN-allocated IP address for the UE. The HNB then inspects all data packets originating from/destined to the UE for the source and destination IP addresses. Depending upon these, the HNB shall modify the source/destination IP address in the packet so as to enable proper routing of the data either via the GTP tunnel to the core network or to the local router.

For example, let's say that the GGSN-allocated IP address for the UE is 172.26.0.1 and the local DHCP allocated IP address is 10.0.0.1. In case the UE initiates a data packet for a node within the local subnet (e.g., a local PC with IP address 10.0.0.2) with source IP = 172.26.0.1 and destination IP = 10.0.0.2, then the HNB would change the source IP address of the packet to 10.0.0.1 before forwarding the packet to the router so as to enable the router to correctly route it over the local subnet. Similarly, for an IP packet originating from 10.0.0.2 and destined for 10.0.0.1, the router would forward this to the HNB which would then change the destination IP address to 172.26.0.1 before giving it to the UE. For packets destined to be sent over the GTP tunnel (say destination IP = 215.34.6.10) or received downlink from the GGSN, the HNB would not modify the IP packets.

Advantages

1. Multiple APNs are not necessary to be configured on the UE.
2. The HNB does not need functionality of the SGSN/GGSN; however, it does need to be able to decipher SM signaling.
3. The normal path to the GGSN is not changed, hence handover to another HNB or to a macro RNC is easier.

Disadvantages

1. DPI capabilities are required at the HNB to inspect each data packet; this would lead to greater processing and hardware capability requirements.
2. Assigning priority to data destined for one stream over another (e.g., higher priority to GGSN-destined data over local subnet data) takes higher processing since there are no separate radio bearers which the HNB can use to distinguish the packets easily; the HNB has to instead rely on DPI to take such a decision.
3. Differential charging of data based upon destination becomes more difficult.

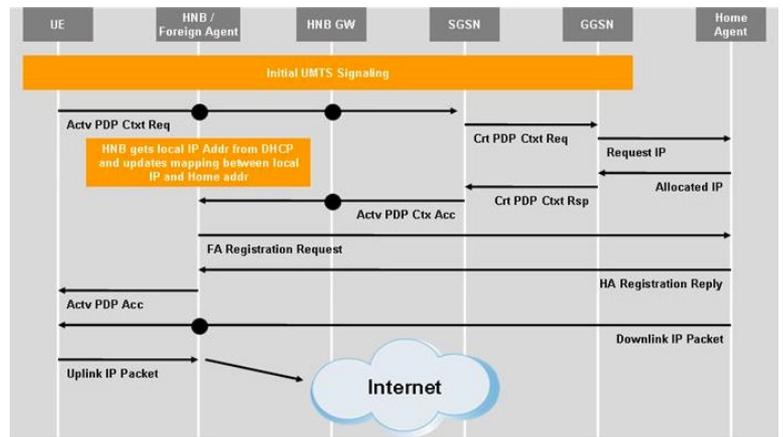


Figure 5. Using mobile IP and having the HNB act as a foreign agent

Alternative 3: Using Mobile IP and Having the HNB Act as a Foreign Agent

In this approach the UE initiates a PDP session establishment by sending an Activate PDP Context Request for a dynamic IP address to the SGSN via the HNB. The HNB deciphers but does not modify the SM messages. The GGSN contacts a mobile IP Home Agent (HA) located topologically close to the user's home network and requests the HA to allocate an IP address to the UE which is stored as the UE's home address in the HA.

Upon getting an *Activate PDP Context Accept* from the GGSN containing this allocated IP address, the HNB initiates a Registration toward the HA by acting as a foreign agent (FA) on behalf of the UE. The IP address of the HNB is the care-of-address for the UE and the IP address allocated to the UE is the home address. The IP address of the Home Agent could be either configured on the HNB or discovered via dynamic home agent address resolution as given in RFC 3344. Upon successful registration, the downlink packets addressed to this UE are sent to the HA, tunneled to the HNB and then forwarded to the UE. Any uplink packets are directly routed by the HNB to the Internet.

Advantages

1. IP address is allocated dynamically by the HA, thus IP address release on timeout is easier.
2. HNB does not need to modify SM signaling.
3. Since the anchor for the call is the HA, the call continuity is easier even if the UE moves to another HNB or to a macro RNC. In fact, it is possible to ensure call continuity even if the UE moves to a non-3GPP access network like a Wireless LAN.

Disadvantages

1. As per RFC 3344, an FA should not initiate a registration on its own, which is what the HNB is doing.
2. Security context-related issues for mobile IP authentication between HA and mobile node (UE) need to be resolved. (*Note 1*)
3. Since the IP address is of the HA's network, it would be different from the home network subnet and hence the UE would be unreachable from other devices on the home network. (*Note 2*)
4. DPI capability is required at the HNB to decide where to route packets in case the HNB is used to also access the other devices in the local subnet.
5. Differential or QoS-based charging on the destination address of the IP packets (within the subnet or to the GGSN) is difficult since the HNB has to inspect every packet to take such a decision.
6. The GGSN also needs to be modified to interact with the HA.

Note 1: For an HA to accept the RR sent by an FA on behalf of a mobile node, the Registration Request must contain the Mobile-Home Authentication Extension.

This is used by the HA to validate and authenticate the mobile node. The parameters used in the extension are typically pre-configured on the HA. Hence, if the UE did not trigger the registration, the HNB (i.e., foreign agent) would not be able to supply the right Authentication parameters for a particular UE and the registration would fail.

Two possible ways to overcome this issue are:

1. Have a list of pre-configured UEs and their associated MIP authentication parameters that can be used by the HNB when initiating registration on behalf of a particular UE. However, this introduces the limitation that only certain UEs can access the HNB and thus precludes a visiting UE from using the services of the HNB.
2. The HNB itself can have a set of Authentication parameters pre-configured on the HA. It chooses one item from the set per UE while initiating registration for that UE, possibly sending its own address as a co-located care-of-address while registering. Thus a visiting UE could also possibly use the LIPA services via the HNB.

Note 2: This deficiency could be addressed by two possible ways:

1. The HNB also requests a local IP address from the DHCP server of the router for this UE and maps the GGSN-allocated IP address to the local address and then routes packets on the network. The routing in this case would be done by the HNB in a similar manner to approach 2, i.e., by providing a sort of NAT functionality.
2. A separate DHCP client on the UE would request a local IP address from the router and use this to access the other devices via the HNB. How the signaling would take place is via FFS.

	Alternative 1: (Local IP Access solution using a local PDN connection)	Alternative 2: (Single UE IP address with Local IP Access at the HNB)	Alternative 3: (Using mobile IP and having the HNB act as a foreign agent)
Separate Radio Bearers (RBs) used for different data paths	 Separate RBs used for data routed via CN and data routed via Local IP Access	 Same RB used for data routed via CN and data routed via Local IP Access	 Same RB used for data routed via CN and data routed via Local IP Access
Deep Packet Inspection (DPI) capability needed in HNB to distinguish the data path to be taken	 Not needed since separate RBs are used for different data paths	 DPI capability needed at HNB to decide whether to route data via CN or LIPA	 DPI capability needed at HNB to decide whether to route data via CN or LIPA
Special support needed in UE	 UE should be able to support multiple configuration of APNs and multiple IP addresses	 No special support needed in the UE	 No special support needed in the UE
Modifications needed to existing HNB architecture	 1. Limited GMM state machine. 2. SM state machine and ability to originate and terminate SM and GTP signaling. 3. DHCP client functionality to interact with DHCP server on ISP router	 1. Limited GMM state machine 2. Ability to decipher SM signaling 3. DHCP client functionality to interact with DHCP server on ISP router	 1. Limited GMM state machine 2. Ability to decipher SM signaling 3. DHCP client functionality to interact with DHCP server on ISP router 4. Mobile IP support to act as FA
Modifications needed to other network elements	 No modifications needed	 No modifications needed	 GGSN needs to be modified to interact with HA
Hardware requirements affected	 No special hardware requirements	 DPI capabilities (possibly) needed in hardware	 DPI capabilities (possibly) needed in hardware
Ability for QoS shaping & differential charging based on IP packets destination	 Easily done by HNB without DPI based on different radio bearers	 DPI capability needed to take a decision based on source/destination IP address in the IP packet	 DPI capability needed to take a decision based on source/destination IP address in the IP packet
Ability to handover the PS call to other HNBs or the macro RNC	 Only that PS call that uses GGSN-assigned address can be handed over	 Handover to other HNBs or macro RNC for PS call possible	 Handover to other HNBs or macro RNC for PS call possible
Ability to handover call to non-3GPP network	 Not considered if serving GGSN is not part of the non-3GPP network	 Not considered if serving GGSN is not part of the non-3GPP network	 Possible since the anchor for the call is the Home Agent

Table 1. Comparative Analysis of the Different Alternatives

As seen from Table 1, each of the approaches to providing LIPA has its share of advantages and disadvantages. For operators wishing to provide LIPA services without investing significantly in hardware costs, Alternative 1 is recommended. This is because typically HNBs, being end user devices, would not have high-end hardware or high-speed processors to warrant DPI functionality without very high cost overruns. Adding limited SGSN and GGSN functionality via software upgrades would be much

easier and cheaper than upgrading hardware. Plus, since universal mobility, i.e. the ability for a PS call to continue seamlessly across different radio access technologies like 802.11x, WiMAX and UMTS is still under development, the need to involve mobile IP to maintain the mobility anchor across accesses is not urgent. The architecture could transition from Alternative 1 to Alternative 3 in the future depending upon commercial strategies.

Conclusion

Due to the burgeoning demand to use mobile devices for accessing content-rich, high speed data networks while on the move, it has become increasingly urgent for mobile network operators to apply innovative solutions to minimize the strain that would be imminent on their existing infrastructure. The solutions need to be configured so as to make maximum use of the existing infrastructure without necessitating a large additional capital expenditure. The solutions also need to minimize any changes needed to the UE and provide a seamless experience to the user.

Local IP Access for data transfer is a convenient solution that addresses all these points. The existing home broadband network is efficiently used to provide a high speed Intra/Internet access to UEs via the HNB. The load on the core network infrastructure is reduced without significant additional capital expenditure by bypassing the core network in the data path. The solution does not need Release-9 compliant UEs, so most existing users can seamlessly utilize this service without user intervention, thus enhancing the overall user experience.

Depending upon factors like availability of high-performance hardware, availability of certain nodes (e.g., HA/FA, etc.), availability of protocol support (e.g., Mobile IP), number of nodes that need to be changed and other such decision points, one or more of the above-mentioned approaches can be used for implementing LIPA via the HNB.

Radisys has a range of protocol stacks available in its Trillium product portfolio currently being utilized to implement HNBs for various customers, and the company's Professional Services group is also working on implementations of LIPA. Furthermore, Radisys has proven hardware solutions such as the ATCA-PP50 packet processing blade that are optimized for high performance DPI capability. As such, Radisys offers a one-stop-shop experience in terms of hardware, software and services to HNB vendors for implementing LIPA solutions well in time for the anticipated strong customer demand for such innovative and cost-effective solutions.

Glossary

- APN:** Access point name—the name used to identify a GPRS bearer service in the GSM mobile network. The APN defines the type of service that is provided in the packet data connection.
- Backhaul:** The network link between the HNB and the core network.
- DHCP:** Dynamic Host Configuration Protocol—a network application protocol used by devices (DHCP clients) to obtain configuration information for operation in an Internet Protocol network.
- DPI:** Deep Packet Inspection.
- FA:** Foreign Agent—a router that stores information about mobile nodes visiting its network. Foreign agents also advertise care-of addresses which are used by Mobile IP.
- GGSN:** Gateway GPRS Support Node—the packet gateway in the traditional GPRS core network used to access external PDNs for data services.
- GMM/SM:** GPRS Mobility Management/Session Management—core network protocols (with the peer side as the UE) used for providing mobility and data session related services to the UE.
- GPRS:** General Packet Radio Service—a packet-based air interface designed as a GSM overlay, permitting the use of GPRS as an optional data networking service on GSM-based networks.
- HA:** Home Agent—a router on a mobile node's home network which tunnels datagrams for delivery to the mobile node when it is away from home. It maintains current location (IP address) information for the mobile node and is used with one or more foreign agents.
- HNB:** Home Node B—a user end device that provides radio access to the user for accessing the core network of the mobile operator. Also known as a femtocell.

HNB-GW: HNB Gateway—an aggregator that concentrates HNB traffic and provides a standard Iu interface toward the core network.

Home

Network: A network of IP-enabled devices connected via a router. Within the home network, the devices communicate using protocols such as Ethernet. For accessing the broader Internet, the devices use IP addresses and access is provided via the router.

Home

Router: The home-based IP-enabled device used to route data packets between a device on the home network and the broader Internet, as well as to route data packets between the devices within the home network.

LIPA: Local IP Access—the ability to route packet-switched data traffic via the home-based router over the ISP's network, thereby bypassing the Core Network elements.

LTE: Long Term Evolution—a 4G wireless broadband technology developed by 3GPP.

Mobile IP: An Internet Engineering Task Force (IETF) standard communications protocol that is designed to allow mobile device users to move from one network to another while maintaining a permanent IP address.

NAT: Network Address Translation.

PDN: Packet Data Network—the external network (such as the World Wide Web or WWW) used to transfer data.

PDP

Context: Packet Data Protocol Context—a term used in the mobile wireless network indicating a logical association between a Mobile Station and PDN used to transfer data packets.

PS: Packet Switched.

QoS: Quality of Service—parameters such as transmission rates, error rates, and other characteristics for a data session that can be measured, improved, and, to some extent, guaranteed in advance.

RNC: Radio Network Controller.

SGSN: Serving GPRS Support Node—the core network node that provides mobility and session management functionality to the UE.

UE: User Equipment—a device such as a mobile phone or laptop with data card that is used to access the mobile network.

UMTS: Universal Mobile Telecommunications System—a third generation mobile network system of 3GPP used to provide circuit switched and packet switched mobile services.

UTRAN: UMTS Terrestrial Radio Access Network—a collective term for the NodeB's and Radio Network Controllers which make up the UMTS radio access network.

WCDMA: Wideband Code Division Multiple Access—an ITU standard derived from Code Division Multiple Access (CDMA) which is a third-generation (3G) mobile wireless technology that offers high data speeds to mobile and portable wireless devices.

References

¹3GPP TS 22.220 V9.1.1—Service requirements for Home NodeBs and Home eNodeBs (Release 9)

²3GPP TR 23.830 V0.5.0 (2009-05)—Architecture aspects of Home NodeB and Home eNodeB (Release 9)

The Radisys logo consists of the word "radisys" in a lowercase, sans-serif font, with a registered trademark symbol (®) to the right. The text is white and is set against a dark red rectangular background.

Corporate Headquarters

5435 NE Dawson Creek Drive
Hillsboro, OR 97124 USA
503-615-1100 | Fax 503-615-1121
Toll-Free: 800-950-0044
www.radisys.com | info@radisys.com

