


**IM 2011 Application Session**

**LTE Relay Node Self-Configuration**

**Péter Szilágyi, Henning Sanneck**

**Nokia Siemens Networks Research**

1 © Nokia Siemens Networks LTE Relay Node Self-Configuration, IM 2011 Application Session



## **Abstract**

Relays are mobile network base stations, which connect to the network via an in-band wireless backhaul link instead of using a dedicated wired or microwave backhaul link as regular base stations do. Connecting through a wireless backhaul raises difficulties when it comes to accessing the operator's Operation, Administration and Maintenance (OAM) System, since prior to the appearance of relay nodes, wireless access was reserved solely for user equipments and not used by network elements at all. However, after deploying a relay node, establishing an initial OAM access is essential in any kind of configuration, particularly when considering an automated configuration process known as self-configuration in principle. Self-configuration is gaining more importance for regular base stations as well as relays as automation of OAM processes is seen as a major contributor to reduce complexity and cost in network operation. In this paper, we introduce a conceptual separation of the initial configuration phase and the operational phase and present a detailed concept for automatic connectivity establishment to the OAM system. The transition from configuration to operational phase is also covered. The results have been verified by an event-driven packet based simulator and the proposed method has been accepted by the 3<sup>rd</sup> Generation Partnership Project (3GPP) as the baseline solution for configuring relays in the next generation radio access technology, Long Term Evolution (LTE).

## Introduction to LTE Relay Nodes (RNs)

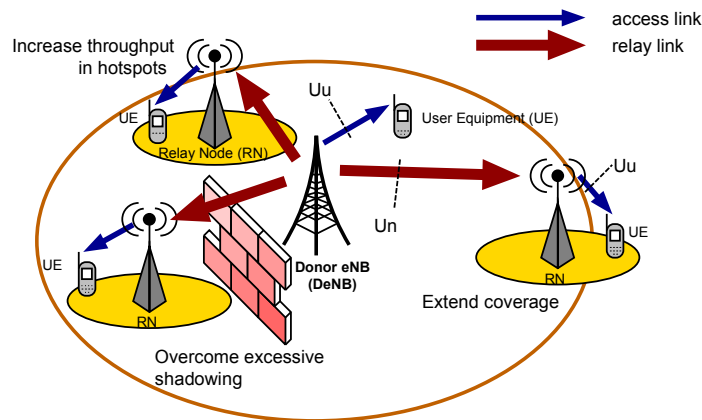


Figure 1: Relay nodes in operation, depicting the most important use cases: coverage extension, increasing throughput and overcoming shadowing.

2

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session



Self-Organizing Networks (SON) is the technical solution to achieve management of complexity in networks and thus provide OPEX reduction and revenue protection [1]. SON refers to the combination of several functions in different areas (configuration, optimization, healing) [2]. Self-configuration, in particular, deals with the auto-configuration of newly inserted network elements, configuring initial parameters and establishing connections [3].

Relay nodes are mobile network base stations, which connect to a radio network via an in-band wireless backhaul link instead of using a dedicated wired or wireless backhaul link, such as Ethernet or microwave link. In-band relaying means that the same radio resources are used both by relays and by customer user equipments (UE) such as mobile terminals. The purpose of using relays is to provide coverage extension to regions of high shadowing (including indoor areas) or locations where dedicated backhaul links are not (or cannot be) deployed. In 3GPP Long Term Evolution (LTE) networks, relaying functionality is to be provided by Relay Nodes (RNs) [4]. An RN connects to an enhanced NodeB (eNodeB or eNB), which is referred to as the Donor eNodeB (DeNB) for that particular RN. Communication between the RN and the network is performed via the DeNB. A radio link between the RN and the DeNB is called a relay link and uses the so-called Un interface, which is a new interface in LTE especially for RN–DeNB backhaul communication. Mobile terminals can connect either directly to an eNodeB or to a RN, and both connection types are called access links and they use the same Uu interface. Fig. 1 shows an overview about the possible scenarios. The relaying architecture is being standardized by 3GPP [5].

Due to the demand for deployment costs to be minimized [6], procedures related to deploying network elements should be automated to avoid costly human intervention. It is anticipated that a large total number of relay nodes will be deployed relative to the number of deployed regular LTE eNBs, hence, automation is also a requirement with regard to scale. Furthermore, it is expected that physical relocations may take place much more often for RNs than for regular eNBs in order to deal with changing operator requirements. Therefore, automation of initial configuration, also referred to as self-configuration, is even more important for RNs than for regular eNBs. However, no LTE relay self-configuration concepts have been developed so far, either in the academic domain or in 3GPP standardization. This paper addresses that gap and provides a suitable self-configuration solution for LTE RNs.

## Requirements, basic concepts and considerations for RN self-configuration

- Ability to access the OAM system
  - Challenging due to the wireless backhaul link
- Possible Donor eNB selection strategies
  1. Off-line selection by the operator during network planning
    - provisioned with planning data into the OAM system
    - when RN is deployed, selected DeNB association is downloaded
    - (self-)configuration takes place through the initial OAM link
  2. Dynamic selection by the OAM system during deployment, based on
    - data acquired from the RN, e.g., the strengths of received radio signals from different eNBs
    - additional knowledge about the network that is present at the OAM level but not at the network element level (e.g., planned locations of eNBs)
    - selected DeNB association is downloaded to the RN
  3. Dynamic selection by the RN
    - upload of selected DeNB association to the OAM system

3

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session



The self-configuration of a network element (NE) first requires the NE to connect to the operator's network. Then it has to gain access to the OAM system, identify itself and download configuration data. All NEs in a mobile network (e.g., eNBs) have dedicated wired (e.g., Ethernet) or wireless (e.g., microwave) backhaul connections that can be used to just plug the NE into the operator's network and provide it with Layer-2 access. Then the NE can use standard DHCP to get an IP address and learn the IP addresses of the other nodes that participate in the self-configuration (most importantly, the OAM system, which can be seen as one logical entity, although it may be distributed among several physical nodes).

The method outlined above can be used by all kinds of eNBs, but it is not suitable for RNs without modification. The reason is that the RN, being a wireless node, has no Layer-2 network to just being plugged in. Moreover, the Un interface seen in Fig. 1 can only be used between the RN and its DeNB when the RN is in operational state, that is, when the RN has finished negotiating the resource partitioning with the DeNB concerning its relay link and access link and the RN is ready to accept incoming UE connections. When the RN is initially powered up, it is not yet recognized and authenticated as a network element, so the RN has to use the only access method over the radio interface that is standardized, namely the Radio Resource Connection (RRC) establishment followed by the UE Attach procedure [7] (its purpose and what is exactly established will be described later). Using a standardized access method is important to avoid any standardization impacts that would be an obstacle to relay self-configuration. For the UE Attach procedure, however, the RN needs to be able to act as a UE and have a UE identity.

Another concern is which eNB can or should be used by the RN to make its initial access through the UE Attach procedure to the network. One obvious choice would be the DeNB, since it is the eNB through which the RN will connect to the network after it has been configured. This choice, however, may not be fortunate or even feasible. To understand the obstacles, let us consider the possible DeNB selection strategies that determine when and where the decision about the DeNB is made. The details can be read on the slide.

## Core contribution: “Configurator eNB” concept

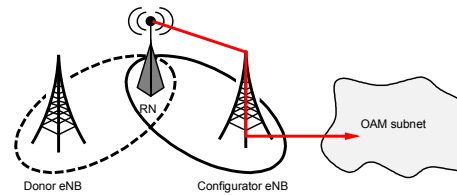


Figure 2 (a): Initial OAM access through the configurator eNB

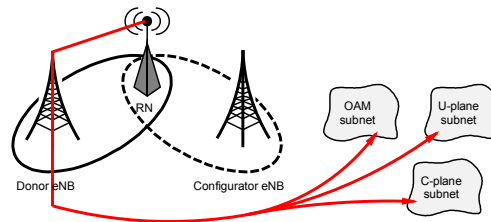


Figure 2 (b): OAM and User/Control-plane access through the DeNB

4

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session

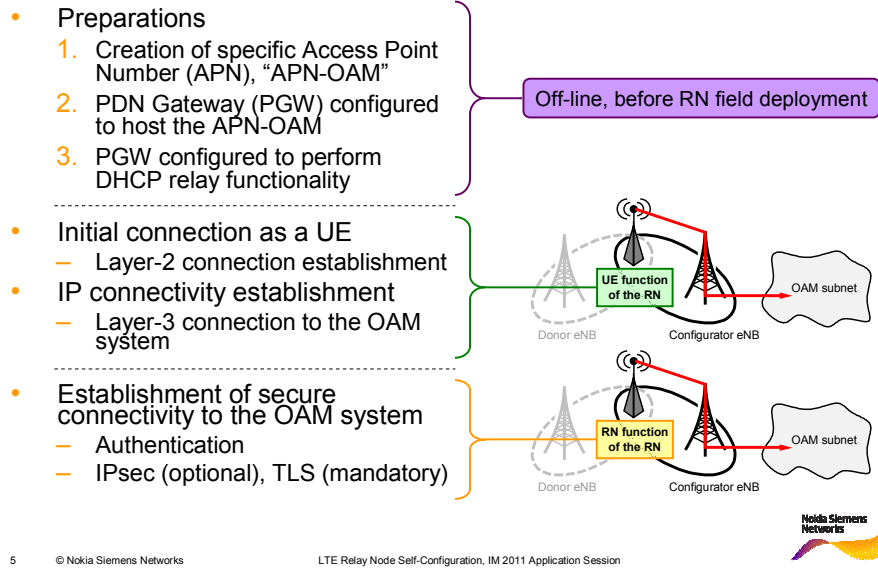


It is clear that in the first two cases of DeNB selection strategies, the RN does not have prior knowledge about its DeNB association before it has already connected to the OAM system. On the other hand, since the RN is a radio node, it has to connect to an eNB in order to access the core network and the OAM system even for its initial configuration. Therefore, we propose that an intermediate eNB is needed that can provide the RN with a connection to the OAM system for the time of its initial connectivity. This eNB will be referred to as the “configurator eNB” or “CeNB” for short (see Fig. 2 (a)). After the self-configuration is completed through the configurator eNB, the RN can switch over to the DeNB and enter operational state (see Fig. 2 (b)). Our detailed solution for the whole RN self-configuration process that is unfolded in the rest of the paper is built around this core concept.

The configurator eNB can be any of the accessible eNBs that provide coverage at the location of the RN. There is no special requirement on an eNB that is chosen by the RN as configurator, so the choice can be based on any suitable measure, e.g., the eNB with the best SINR. Note that it is not true for DeNBs: a regular LTE eNB needs at least software upgrade in order to become donor-capable, hence, not all available eNBs are automatically potential donor eNBs too (it is unlikely and practically impossible that a network operator upgrades all eNBs to support relay nodes in one step).

Later, when the RN has downloaded configuration data from the OAM system and it is aware of its DeNB association, it may turn out that the DeNB selected by the operator or computed dynamically by the SON functions in the OAM is in fact the same as the configurator eNB selected by the RN. In that case, the OAM connection that the RN already has can be preserved and only the additional connections that are needed in operational phase have to be established. Otherwise, the OAM connection has to be re-established through the DeNB and torn down from the configurator eNB.

## Relay Node Auto-Connectivity: Overview of the proposed solution



Now that our core configurator eNB concept has been presented, let us turn to discuss the details of an RN self-configuration process that is wrapped around this concept.

Since the RN can initially connect to an eNB via the Uu interface, which is only used for UE access and not for network elements, the only way for the RN to connect without introducing new access methods is to first act as a UE. This method implies that relay nodes have two functions: a UE function and a RN function. The following slides detail step by step what are the prerequisites of starting RN self-configuration, how can the RN initially access the network as a UE, gain first Layer-2 then Layer-3 (IP) connectivity to the OAM system, authenticate itself properly as a RN and setup security by using Transport Layer Security (TLS) and optionally also IPsec. The whole process consists of three building blocks: the first is completed before the deployment of the RN; the second is completed by the RN acting as a UE; the third, which closely follows the second, is conducted by the RN acting as a RN.

The following preparations are required to enable the actual auto-connectivity:

1. A specific Access Point Number (APN), which will be referred to as "APN-OAM", defining the OAM subnet as a Packet Data Network (PDN) is configured either in the RN's UE function or included in the HSS subscription data as the default APN for the subscription.
2. There is a PDN Gateway (PGW) hosting the APN-OAM, so that the PGW is configured to be able to route traffic to the OAM subnet. The configuration of an APN at a PGW is a standard procedure, only a new APN number has to be selected, which can be operator-specific.
3. The PGW must have DHCP relay functionality.

Subscription data for the UE identity is provisioned into the Home Subscriber Server (HSS). The HSS data may also contain an *RN indication*, which signals that the UE is capable and permitted to function as a RN. This allows the Mobility Management Entity (MME) to reject the attach request of those UEs that are not authorized to function as a network element. Since later in the process there is a separate security setup for the RN functioning as a network element, the RN indication is considered to be optional. If the RN indication is not used, however, regular UEs which are aware of APN-OAM can perform steps described in the followings, e.g., potentially leading to Denial-of-Service attacks on real RNs wanting to perform the auto-connectivity procedure at the same time.

In the OAM subnet, there must be a DHCP server available configured to provide IP address suitable for use in the OAM subnet. Note that this is also required for the auto-connectivity of regular eNBs, hence it is not a specific requirement for RNs.

## Relay Node Auto-Connectivity: Connectivity Establishment as UE

- Standard LTE UE Attach procedure
  - RRC connection setup to the configurator eNB
  - NAS Attach, authentication with the MME
  - GTP tunnel to the OAM network
- Accessing the OAM system
  - APN-OAM identifies a connection to the OAM subnet
    - this is either sent by the RN during the initial Attach message or stored as part of the HSS subscription data of the RN
  - the RN sends a message destined to the OAM system
    - forwarded in the GTP tunnel from the configurator eNB to the PGW
    - the PGW decapsulates the message from the tunnel and routes it to the OAM system
    - the reply travels on the opposite direction, with the PGW tunneling and the configurator eNB decapsulating from the tunnel

6

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session



As it is difficult to change existing call processing standards, a crucial requirement for a solution is to stay within the boundaries given by current standards. Our solution fully satisfies this requirement. Therefore, the RN employs the regular LTE UE Attach procedure [7] to start the auto-connectivity process. The Attach procedure is used to authenticate the UE function and establish a default bearer. The authentication is done by the MME by signaling towards the HSS. The default bearer, like any data bearer, consists of the concatenation of a Data Radio Bearer (DRB) between the RN and the configurator eNB and an Evolved Packet System (EPS) bearer between the eNB and the core network.

In LTE, an EPS bearer is realized by user plane GTP tunneling and its purpose is to provide access to a specific PDN. For UEs, such PDNs are the Internet or IMS services. Each PDN is accessed through a PGW, which provides specific APNs to differentiate between the PDNs. The user traffic is carried in a GTP tunnel from the eNB serving the UE (which is the CeNB in case of the RN) to the corresponding PGW.

During the Attach procedure, the UE function of the RN indicates within the standard Protocol Configuration Options (PCO) element that it prefers to obtain the IP address later with DHCP. Thus, the PGW does no automatic address allocation as part of the bearer establishment, as it would do without such an indication. If the APN-OAM is configured in the RN, it has to send it within the UE Attach message. If the APN-OAM is provisioned in the HSS subscription data, the RN should not send any APN (in fact, the RN does not have to know the APN at all). Instead, the MME will use the APN retrieved from the HSS to connect to the right PGW. At this point, the RN has physical (Layer 2) connectivity to the OAM subnet, but does not have IP (Layer 3) connectivity yet, so the next step is IP connectivity establishment.

## Relay Node Auto-Connectivity: IP Connectivity Establishment

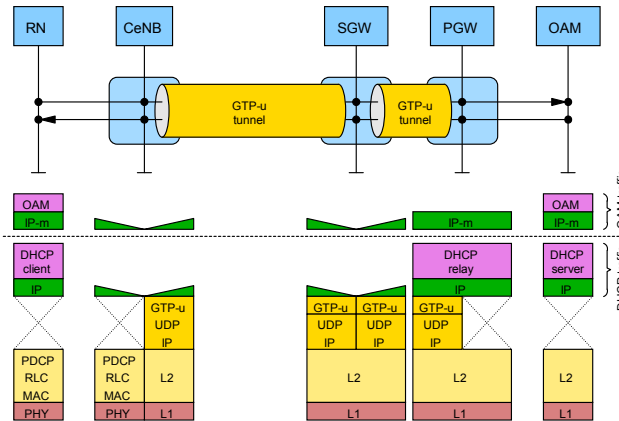


Figure 3: DHCP and OAM protocol stack

7

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session



In order to establish connectivity with the OAM system, the RN now follows the conventional DHCP protocol procedures [8], see Fig. 3.

The DHCP client on the RN sends a broadcast DHCP DISCOVER over the radio link to the eNB. At the eNB, the DHCP DISCOVER message is sent over the established GTP tunnel to the SGW, which forwards it further to the PGW. At the PGW, the DHCP DISCOVER message is received by the DHCP relay process which sends the message to its configured DHCP server in the OAM subnet. At the DHCP server in the OAM subnet, the message is processed. In the successful case that an IP address can be offered to the RN (e.g., there is enough free addresses in the address pool), a DHCP OFFER is sent back from the DHCP server to the DHCP relay which in turn sends it back to the RN (note that additional information like the IP addresses of operator specific network elements, e.g. node(s) hosting the OAM system may also be returned by the DHCP server).

At the RN, the received IP address is configured and used further for OAM-related traffic (as of Fig. 3). The layer "IP-m" is referring to connectivity (IP addresses, routing entries, etc.) with the OAM subnet. Note that the depicted "OAM" layer is the OAM protocol stack above IP for the southbound management interface, but any IP traffic could be exchanged over the established connection of course. Additional information received in the DHCP OFFER message is processed and stored in the RN for further usage.

## Relay Node Auto-Connectivity: IP subnet separation in mobile backhaul

LTE backhaul configuration for relay auto-connectivity showing the most important radio access and transport network nodes. The different alternatives for RN→OAM access path are also indicated.

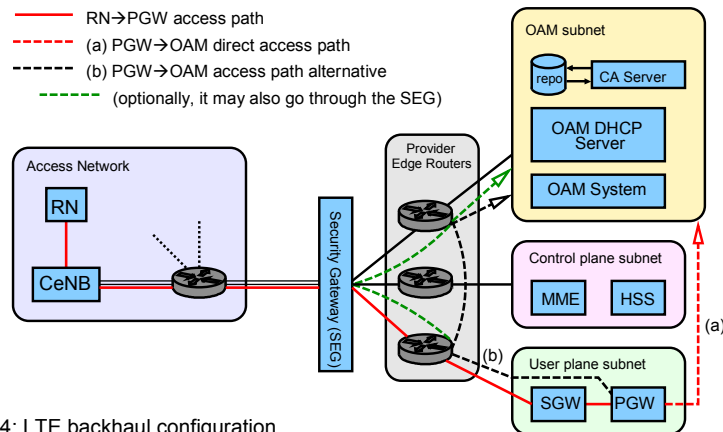


Figure 4: LTE backhaul configuration

8

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session



Fig. 4 shows an overview of the LTE backhaul configuration depicting the relevant nodes and connections from RN auto-connectivity point of view. The figure portrays the common subnet separation scheme that puts the OAM system, the control plane nodes and the user plane nodes into separate IP subnets. The solid red line indicates the first part of the OAM access path, from the RN to the PGW. This path, apart from the initial RN–CeNB hop (which is the in-band wireless relay backhaul), goes inside the user-plane GTP tunnel that was established between the CeNB and the PGW as part of the UE Attach procedure (see Section III-B and Fig. 3). From the PGW to the OAM system, two alternatives are shown, (a) and (b). Alternative (a) is accessing the OAM subnet as an external PDN (just like e.g. an IP Multimedia Subsystem (IMS) would be accessed). Alternative (b) is accessing the OAM subnet through the same provider edge routers that are used to maintain the subnet separation. This alternative path can even go through the SEG in case the communication between the RN and the OAM system is secured in the IP layer using IPsec (see next slide).

The choice between the alternatives can be a matter of taste from the network operator's side, but in fact the first (dashed red) one should work regardless of the network configuration: since all nodes, including PGWs, need to access the OAM subnet for their own OAM purposes, a PGW can also provide access to the OAM subnet for UEs (provided that the proper APN-OAM has been configured at the PGW).

Note that for security reasons regular UEs cannot gain access to the OAM system this way, since they would fail the strict authentication process discussed in slide 9. Normally this access is never required for a regular UE, since device management is done in a separate entity; the OAM system is used for network element management, for nodes such as the RN or eNBs.

## Relay Node Auto-Connectivity: Secure Connectivity to the OAM subnet

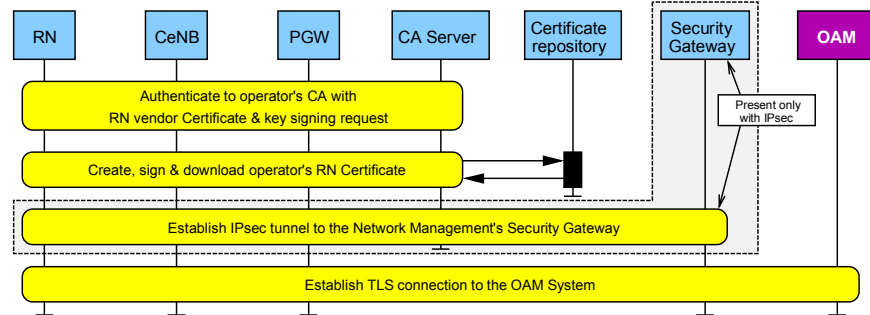


Figure 5: Two options for secure connectivity establishment

- Option 1: using IPsec and TLS
- Option 2: using TLS only



9

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session

After the initial connection has been set up, the RN has IP connectivity to the OAM subnet and it is ready to establish a secure connection to the OAM nodes involved in the further self-configuration process. It is usually done by verifying the identity of the RN and provisioning operator certificates for secure communication with other network elements within the operator's network. This is most commonly realized with a Public Key Infrastructure (PKI). The RN then establishes a mutually authenticated TLS session with the OAM system.

There are two options in how to do this step: using IPsec and TLS or using TLS only. In the first option, the connection is secured in the IP layer as well by using IPsec tunnel between the RN and the security gateway. It means that in Fig. 4, the PGW→OAM path should take the second alternative and even go through the SEG. Beware that the overall RN→OAM path goes through the SEG twice: first in the RN→PGW part, second in the PGW→OAM part. In the first part, the RN-SEG IPsec tunnel goes through the SEG transparently and it terminates in the SEG only the second time when it turns back and reaches the SEG from within the user plane subnet. This is because the first time all packets (including IPsec and upper layer data) originating from the RN are passed through the transport network as a payload, and the SEG at this part only acts as a normal IP router. In other words, the IPsec tunnel goes inside the user plane GTP tunnel that spans from the CeNB to the PGW. However, from the IPsec point of view, the secured connection is between the RN and the SEG, regardless of the transport path of the IPsec packets.

The secure connection is used by the RN to register itself to the OAM system, which then can continue with the self-configuration of the RN. Fig. 5 shows the corresponding message flow for the authentication and secure link establishment.

Alternatively, the IPsec connection to the Security Gateway (SEG) can be omitted as the RN has in fact already access to the trusted domain by connecting to the user plane subnet. Fig. 5 shows this alternative procedure as well. The only difference is that this time the SEG is not actively involved since no IP layer security is used. Based on established secure OAM link, the RN can continue with the further steps in the auto-commissioning procedure.

## Auto-Commissioning

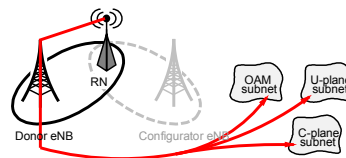
- Secure connectivity is established between RN and OAM
  - the RN is connected to the OAM through the configurator eNB
  - any kind of data exchange is possible
  - RN identity has to be matched with the planning data in order to provide the RN with the proper parameter set
    - by means of HW-to-site mapping
- OAM provides the RN with initial parameters
  - DeNB list
    - according to the DeNB selection strategies, the OAM provides the RN with the identities of eNBs that may be used as the DeNB of the RN
    - the RN may select any of the provided nodes based on, e.g., the received signal strength
    - this is the current proposal in 3GPP RAN3

Using the secured connection to the OAM system, any kind of data exchange can take place between the RN and the OAM system. It includes downloading of software and configuration data to the RN, and also uploading data from the RN to the OAM system, such as status reporting of the self-configuration process. Some configuration parameters are prepared off-line by the operator, some of them are computed dynamically and automatically at the OAM system (such as the physical cell identity for the RN's cell). The self-configuration process is currently being standardized by 3GPP [9].

The actual data exchange depends on what planning data has been pre-computed during off-line planning and which parameters are computed on-the-fly during the self-configuration process. The planning data is previously associated with a site (regular base station site, lamppost or public facility) where a RN can possibly be deployed. When a specific RN is deployed at the site, the RN instance is mapped to the planned site (e.g., the RN sends a registration message including its measured geo-location, which is matched against the stored geo-locations of pre-planned sites in the OAM system). This *HW-to-site mapping* allows for selecting the correct planning data for the specific RN instance. After a successful mapping, the configuration data can be downloaded to the RN instance.

It is not the purpose of this paper to go into details about the configuration parameters, the only important one with regard to the node being a relay is the DeNB association. Depending on the DeNB selection strategy (see slide 3), the DeNB association is either downloaded to the RN (if it was provisioned statically in the planning data or computed dynamically during the self-configuration process) or uploaded from the RN to the OAM system (if the choice was left up to the RN itself). Uploading in the latter case is important so that the OAM system has a complete view of the network. The current activity in 3GPP RAN3 points towards the OAM sending a list of possible DeNBs from which the RN can select the most appropriate one.

## Switch-over to the Donor eNB



- RN detaches from the configurator eNB
- RN attaches to the selected DeNB
  - establish / resume secure connection to OAM
- OAM provides the RN with additional parameters
  - Cell Global Identity (CGI)
    - it has two parts: eNB identity and local cell identity
    - the eNB identity of the RN has to be the same as the eNB identity of its DeNB
    - the local cell identity has to be different for each cell under the management of the DeNB and the cell under the management of the RN
  - Physical Cell Identity (PCI)
    - has to be assigned collision-free (no adjacent cells shall have the same PCI) and confusion-free (no cell shall have two neighbors with the same PCI); it is the responsibility of the OAM to know the adjacencies and assign PCI values accordingly
- X2 / S1 connection setup

When the auto-commissioning has been completed through the configurator eNB, the RN has to be integrated into the operational network, which means it has to switch-over from the configurator eNB to the DeNB (whose identity was communicated to the RN by downloading the configuration data or was determined by the RN itself and uploaded to the OAM system).

First, let us consider the connections a RN has to set up when it is connected to its DeNB. The most important connection that has to be established after startup (and which is in the focus of this paper) is the OAM connection itself. The RN already has an active OAM connection through the configurator eNB. If the DeNB turns out to be the same as the CeNB, this OAM connection can be used without any further action. Otherwise, the OAM connection should be torn down from the configurator eNB and re-established through the DeNB (via the same auto-connectivity mechanism discussed in Section III). The only difference is that the RN already has an IP address from the OAM subnet, which can be reused (after all, only the Layer-2 connectivity is changing) and thus the DHCP part can be skipped. (Optionally, the original OAM connection through the configurator eNB could be retained until the Layer-2 part of the new OAM connection is successfully established. This way the RN is able to report failure through the original OAM connection.)

Another connection established between the RN and the DeNB is the radio resource control connection used for resource partitioning between the DeNB and the RN. This protocol is similar to the RRC protocol [10] used between an eNB and a UE but it controls the relay link resources. The RN also has to maintain S1 signaling connections towards the SAE-GW and X2 connections to neighbors (either RNs or eNBs whose cells overlap with the RN's own cell). The exact number of signaling connections may vary across the different relay architecture alternatives [5] and they are out of scope of this paper.

Finally, there are connections which are established on a per-need basis. User plane EPS bearers are created for carrying UE traffic when UEs are attached to the RN, and deleted when UEs move away. Automated Neighbor Relations can create X2 connections between RNs and other RNs or between RNs and eNBs. As already mentioned, these are out of scope of the network integration process and belong to the operational phase of the RN.

## Advantages and standardization status

- Advantages of our solution
  - uses only standard procedures and well-known protocols
    - no dedicated standardization is required
  - no pre-configured data is required in the RN
    - supports easy and flexible RN deployment
  - configurator eNB can be any regular eNB
    - RN deployment has no impact on regular LTE eNBs
- Contribution to standardization
  - our work has been accepted in 3GPP as the standard configuration method for RNs, called “two-phase configuration”
    - the first phase is conducted through the configurator eNB
    - the second phase is conducted through the DeNB
  - related issues under discussion in 3GPP
    - MME selection for the initial UE Attach procedure
    - SGW/PGW selection for the RN when it connects to the DeNB
    - DeNB based or OAM based ECGI selection for RN

After presenting the theoretical part of our work, let us briefly discuss and compare some alternatives to the proposed solution.

Our work employs the standard UE Attach procedure and identifies the OAM subnet as a PDN using a specific APN, which consists of well-known and tested protocols. A possible alternative would be to develop a new attach procedure, which inherently contains all RN-specific operations and offers a straight connection to the OAM subnet. This solution could then avoid the usage of APNs and the interaction with the HSS (the RN would not even need a UE identity at all). Although it may be a tempting alternative, it would also require a tremendous amount of standardization and implementation effort, not to mention the security implications. It is not a coincidence that the 3GPP relay architecture comes with built-in UE functionality for the RN; the reason is to reuse as much as possible from the UE-specific connectivity procedures. Using DHCP and IPsec/TLS for IP address management and security is a well-established and studied area, where potential security holes and weaknesses are rare and patched with a high priority. Although using dedicated protocols for these functions could be more tailored to the use case (e.g., changing DHCP so no DHCP relay in PGW would be needed), they would replicate functionality of well-known mature protocols and would not fit well with existing eNB self-configuration solutions [3].

Another alternative would require the RN to connect directly to the DeNB, skipping the connection to the initial configurator eNB. This alternative, however, requires that each DeNB broadcasts a type information, separating DeNBs from regular eNBs (i.e., not suitable for operating RNs). Also, for UEs, the different types of eNBs and RNs should be transparent, which is violated if DeNBs broadcast a signal different from that of other eNBs. Additionally, RNs would need to know the identity of its DeNB in advance, which requires either pre-configured data in the RN or allows the RN to choose, taking the DeNB selection completely out of the operator's supervision. In summary, this alternative is not acceptable from either technical or the network operator's point of view.

Based on the comparison of theoretically possible and existing alternatives, we consider our solution superior due to the absence of standardization effort and the flexibility of the CeNB concept. Also, recent advancement in 3GPP standardization has made our proposal the accepted solution for RN configuration [12].

## Proof-of-concept Simulator

- Core network features
  - Ethernet in Layer-2
  - IPv4 in the network layer
  - User Datagram Protocol (UDP)
  - GPRS Tunneling Protocol (GTP)
  - Stream Control Transport Protocol (SCTP) in the transport layer
  - S1 on the S1-MME interface (between an eNB and the MME)
  - Diameter Protocol between the MME and the HSS
  - Radio Resource Control (RRC)
  - Non-Access Stratum (NAS) signaling between the RN and the MME
  - DHCP (including client, server and relay)
- Core network nodes
  - Connectivity: LANs, IP routers
  - User plane: Serving Gateway (SGW), PDN Gateway (PGW), including DHCP relay functionality and hosting a specific Access Point Number (APN) to be used for accessing the OAM subnet
  - Control plane: Mobility Management Entity (MME), Home Subscriber Server (HSS)
  - OAM system: OAM DHCP Server for OAM IP address allocation, OAM System node containing the application logic for OAM functions
- Radio access network features
  - eNodeB (eNB), 60 m antenna height, 46 dBm transmission power
  - Relay Node (RN), 10 m antenna height
  - log-distance radio propagation model



We have implemented an event-driven packet based simulator designed to build up scenarios consisting of network elements and connections and simulate the communication between the nodes. The purpose of the simulator is to provide us with a tangible form of the conceptual work and also to verify the feasibility of the auto-connectivity, especially the UE Attach procedure including the GTP tunnel establishment and the following IP address allocation via DHCP.

The implementation of each radio and transport protocol is completed only to the extent required for connection setup and data transfer. Besides the protocols, the simulator features a network stack capable of managing GTP tunnels, tunnel mappings, performing IP routing, setting up radio bearers, and providing a socket API for the application logic running in network nodes. The scenarios feature a common IP subnet separation between the Radio Access Network, User plane, Control plane and the OAM system. The secure connectivity setup (IPsec tunnels, TLS authentication and encryption) is omitted from this version of the simulator for the sake of simplicity as these are well-established procedures and not in the focus of the simulation.

Basic nodes in the core network, radio access network and the OAM system are implemented.

## Proof-of-concept Simulator

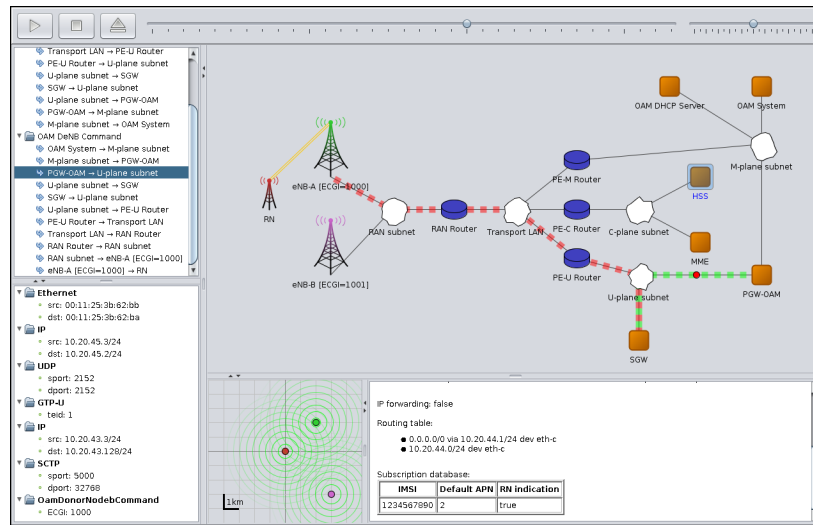


Figure 6: Screenshot of the proof-of-concept simulator implementation



14

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session

The following four scenarios have been defined and simulated:

1. Unsuccessful UE Attach: UE Attach request is rejected.
2. Relay OAM auto-connectivity: successful UE Attach followed by OAM auto-connectivity (establishment of Layer-3 connectivity to the OAM system).
3. OAM-based dynamic DeNB selection: at the beginning of the scenario, the RN already has an established IP connectivity with the OAM system. This scenario is about getting the DeNB association. The DeNB is selected dynamically at the OAM system based on the eNB ECGI and SINR values reported by the RN. The eNB with the lowest SINR is selected as DeNB and its ECGI is sent back to the RN. Since the RN uses the same strategy to select the configurator eNB, no switchover is needed afterwards. Note that in case the RN and the OAM uses different strategy to select the configurator and donor eNB (respectively), they may end up with different choices and a switchover would be necessary.
4. OAM-based static DeNB selection: as with the previous scenario, the RN starts with an established IP connectivity. In this scenario, the DeNB association for the RN is provisioned statically in the OAM system as part of the network planning data. The DeNB selected during network planning is different from the configurator eNB selected by the RN, hence a switch-over to the DeNB is performed but the OAM IP address is reused.

Fig. 6 shows a screenshot of the simulator while it is executing the end of the third scenario, which is when the identity of the DeNB selected by the OAM System is traveling in the GTP tunnel (indicated by the green dashed line) from the PGW to the SGW. The topology uses the (a) alternative of the PGW→OAM path (see Fig. 4). On the left side of the window, the exchanged packets are listed hop-by-hop, with the detailed content of the current packet displayed at the bottom. The bottom right corner shows the content of the HSS subscription database, which contains the subscription data corresponding to the UE function of the RN. The simulations indicate that with a proper implementation of the required signaling protocols and transport network features (including DHCP relay or IP routing), the RN auto-connectivity procedure and the configurator eNB concept are feasible and well working solutions.

## Summary and Conclusions

- Benefit from network management automation
  - major cost saving for operators
  - the more instances are deployed of a certain network element, the more cost can be saved by automating the configuration of that network element
    - the most densely deployed nodes in an LTE network will probably be the relay nodes emerging in LTE-Advanced, so the self-configuration of RNs is a great opportunity to both save cost and reduce deployment time
- The presented solution (concept & proof-of-concept simulator) covers
  - relay auto-connectivity (including Layer-2 and Layer-3 (IP) connectivity)
  - establishment of a secure link from the RN to the OAM system
  - auto-commissioning process of the RN and network integration
- Key characteristics of the concept
  - conceptual separation of the configurator eNB from the DeNB
  - providing access to the OAM subnet as a PDN via a specific APN-OAM
  - uses only standard procedures, fits in the current 3GPP framework
- Standardization
  - our solution is accepted as the 3GPP standard configuration method for RNs

15

© Nokia Siemens Networks

LTE Relay Node Self-Configuration, IM 2011 Application Session



## References

- [1] SOCRATES, "Self-optimisation and self-configuration in wireless networks," European research project, <http://www.fp7-socrates.eu>, 2008–2010.
- [2] 3GPP, "Telecommunication management; Self-configuration of network elements; Concepts and requirements," 3rd Generation Partnership Project (3GPP), TS 32.501, Apr. 2010. [Online]. Available: <http://www.3gpp.org/ftp/Specs/html-info/32501.htm>
- [3] H. Sanneck, C. Schmelz, E. Troch, and L. D. Bie, "Auto-Connectivity and Security Setup for Access Network Elements," IFIP/IEEE International Symposium on Integrated Management, New York, NY, June 2009.
- [4] D. Soldani and S. Dixit, "Wireless Relay for Broadband Access," IEEE Communications Magazine, Vol. 46, No. 3, March 2008.
- [5] 3GPP, "Relay architectures for E-UTRA (LTE-Advanced)," 3rd Generation Partnership Project (3GPP), TR 36.806, Mar. 2010. [Online]. Available: <http://www.3gpp.org/ftp/Specs/html-info/36806.htm>
- [6] E. Lang, S. Redana, and B. Raaf, "Business Impact of Relay Deployment for Coverage Extension in 3GPP LTE-Advanced," IEEE International Conference on Communications, June 2009.
- [7] 3GPP, "General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access," 3rd Generation Partnership Project (3GPP), TS 23.401, Mar. 2010. [Online]. Available: <http://www.3gpp.org/ftp/Specs/html-info/23401.htm>
- [8] R. Droms, "Dynamic Host Configuration Protocol," Internet Engineering Task Force, RFC 2131, Mar. 1997. [Online]. Available: <http://www.rfc-editor.org/rfc/rfc2131.txt>
- [9] 3GPP, "Telecommunication management; Self-configuration of network elements; Integration Reference Point (IRP); Information Service (IS)," 3rd Generation Partnership Project (3GPP), TS 32.502, Apr. 2010. [Online]. Available: <http://www.3gpp.org/ftp/Specs/html-info/32502.htm>
- [10] 3GPP, "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification," 3rd Generation Partnership Project (3GPP), TS 36.331, Jan. 2010. [Online]. Available: <http://www.3gpp.org/ftp/Specs/html-info/36331.htm>
- [11] 3GPP, "3GPP TSG RAN WG3 #68 meeting; Issues on NAS nodes selection in relay scenario," 3rd Generation Partnership Project (3GPP), TDoc R3-101411, May 2010. [Online]. Available: [http://www.3gpp.org/ftp/tsg\\_ran/WG3\\_lu/TSGR3\\_68/Docs/R3-101411.zip](http://www.3gpp.org/ftp/tsg_ran/WG3_lu/TSGR3_68/Docs/R3-101411.zip)
- [12] 3GPP, "3GPP TSG RAN WG3 #69 meeting; Solution for RN configuration," 3rd Generation Partnership Project (3GPP), TDoc R3-102370, August 2010. [Online.] Available: [http://www.3gpp.org/ftp/tsg\\_ran/WG3\\_lu/TSGR3\\_69/Docs/R3-102370.zip](http://www.3gpp.org/ftp/tsg_ran/WG3_lu/TSGR3_69/Docs/R3-102370.zip)