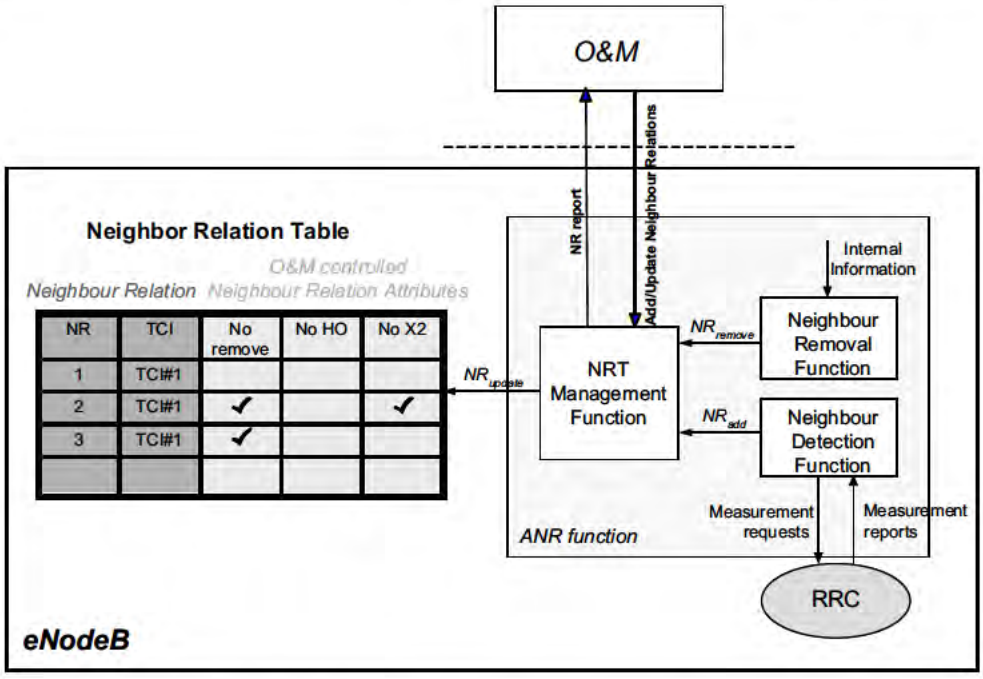

Figure 25.2: The ANR function and the ANR table. Reproduced by permission of © 3GPP.

1. In connected state, the eNodeB instructs a UE to search for neighbour cells in the target RATs/frequencies (it may need to schedule appropriate idle periods for this).
2. The UE reports the PCIs of the detected cells in the target RATs/frequencies (note that each RAT has its own specific format of PCI).
3. The eNodeB instructs the UE, using the newly discovered PCI as a parameter, to read the key RAT-specific cell identification parameters from the broadcast channel of the cell (e.g. the CGI and Routing Area Code (RAC) for GERAN; CGI, Local Area Code (LAC) and RAC for UTRAN; CGI for CDMA2000).
4. The UE reports these key RAT-specific cell identification parameters to the eNodeB of the serving cell.
5. the eNodeB updates its inter-RAT/inter-frequency NRT. The eNodeB can then make use of the NR, for example when triggering subsequent handovers.

25.3 Self-Configuration of eNodeB and MME

Self-configuration of the eNodeB/MME is a SON function which is implemented in the basic S1 and X2 interface procedures [1, 2].

25.3.1 Self-Configuration of eNodeB/MME over S1

With the native support of the S1-flex function in LTE (see Section 2.5), an eNodeB must set up an S1 interface towards each MME of the pool area to which it belongs. The list of MME nodes of the pool area together with an initial corresponding remote Internet Protocol (IP) address can be directly configured in the eNodeB at deployment (although other means may also be used). Once the eNodeB has initiated a Stream Control Transmission Protocol (SCTP, see Section 2.5.1.1) association with each MME of the pool area using that IP address, they can exchange, via the 'S1 Setup procedure' (see Section 2.5), some application-level configuration data which is essential for the system operation. This automatic configuration process thus saves some manual configuration effort for the network operator, together with the associated risk of human error.

Examples of such application-level configuration data exchanged between the eNodeB and the MMEs include Tracking Area (TA) identities,[5] lists of PLMNs of different operators who may be sharing the network so that all the PLMN IDs can be broadcast over the air for their respective UEs, and Closed Subscriber Group (CSG) IDs to allow auto-configuration of the Home eNodeB (HeNB) gateway when it connects to thousands of HeNBs.[6] Once all the data to be broadcast over the radio interface have been configured within each and every eNodeB, they are sent automatically to all the relevant MME nodes of the pool area via the S1 Setup procedure.[7]

The eNodeB can later update the configuration data it had previously sent to the MME by sending an 'eNB CONFIGURATION UPDATE' message. In this case it only sends the updated configuration data, and the data that is not included is interpreted by the MME as being unchanged. Conversely, the MME can also send updates of its data to the eNodeBs by means of an 'MME CONFIGURATION UPDATE'. The updated configuration data is assumed to be stored in both the eNodeB and the MME for the duration of the SCTP association or until any further update occurs.

25.3.2 Self-Configuration of IP address and X2 interface

Similarly to the S1 interface, self-configuration of IP addresses and of the X2 interface is implemented in the basic X2 and S1 interface procedures. The X2 interface may be established between one eNodeB and one of its neighbour eNodeBs when they need to exchange load, interference or handover related information (see Section 2.6). The automatic initialization of the X2 interface consists of three steps:

1. The eNodeB identifies a suitable neighbour;
2. The eNodeB retrieves a suitable IP address for this neighbour if not already available and sets up an SCTP association with it;
3. The two eNodeBs exchange configuration data.

[5] TAs correspond to the zones in which UEs are paged, and their mapping to eNodeBs must remain consistent between the E-UTRAN and the Evolved Packet Core (EPC).

[6] This enables the paging optimization feature in the HeNB gateway. Further details can be found in Chapter 24.

[7] Note that in case of CSG, the S1 Setup messages are exchanged via the Home eNodeB gateway to the MME (see Section 24.2).

The first step can be achieved either by configuration or by using the ANRF described in Section 25.2. If the ANRF is used, this step basically consists of the eNodeB being made aware of the ECGI and Tracking Area Identity (TAI) of the detected neighbour.

For the second step, the eNodeB needs to know the IP address of the neighbour in order to set up an SCTP association. This IP address may again be either configured or retrieved via the network (the latter being used if the ANRF is used during the first step). Auto-configuration of the IP address is achieved by the requesting eNodeB sending over the S1 interface a dedicated 'eNB CONFIGURATION TRANSFER' message that includes both routing information (such as the ECGI of the detected target cell) and the nature of the information that is requested – in this case an IP address for the purpose of X2 initiation. The requesting eNodeB also includes its own ECGI to be used for routing back the answer.

If the receiving eNodeB agrees, it returns one or more IP addresses which can be used for the establishment of an X2 interface. When this procedure is complete, the requesting eNodeB can set up the SCTP association with its neighbour by sending an SCTP INIT message. In Release 10, in order to protect the eNodeBs from malicious SCTP INIT requests from unauthorized parties, this auto-configuration process has been enhanced to enable the use of an Access Control List (ACL)[8] of authorized source IP addresses in the receiving eNodeB. For this purpose, the 'eNB CONFIGURATION TRANSFER' message has been enhanced with the possibility for the requesting eNodeB to include one or several IP addresses that the receiving eNodeB can store in its ACL. Thus, whenever a further SCTP INIT message is received to set up an X2 interface, the receiving eNodeB can first check that the source IP address corresponds to one notified earlier. The protocol also allows the requesting eNodeB to provide IP addresses for an IPSec[9] transport endpoint for scenarios where IPSec is expected to be used (e.g. routing via a security gateway). Finally, the requesting eNodeB can also include the IP addresses that it intends to use for the data-forwarding GPRS Tunnelling Protocol (GTP) tunnels that it will later establish. This would also allow for checking of the user plane traffic at the receiving eNodeB. The reciprocal behaviour is also supported: the receiving eNodeB may similarly provide in the 'eNB CONFIGURATION TRANSFER' message to the requesting eNodeB all the IP addresses it intends to use for its control plane SCTP endpoint, user plane GTP endpoints and/or IPSec endpoint.

Once an SCTP association exists between these two neighbour eNodeBs, the third step can be started, i.e. exchanging configuration data. This consists of application-level data similar to the data exchanged during the self-configuration of the S1 interface (see Section 25.3.1). In this case, the 'X2 Setup' procedure is used for the exchange. For example, an eNodeB can report, via the 'X2 SETUP REQUEST' message to a neighbour eNodeB, information about each cell it manages, such as the cell's PCI, frequency band, TAI and/or associated PLMNs. More detailed radio parameters can also be included, such as the cyclic prefix length (see Section 5.4.1), the transmission bandwidth or the uplink-downlink subframe configuration (see Section 6.2) for Time Division Duplex (TDD) cells.

An eNodeB can also exchange the list of pool areas to which it belongs with a neighbour eNodeB. The neighbour eNodeB can thus automatically learn if it shares a pool area in common and therefore whether it will need to use the S1 or the X2 handover procedure

[8] A receiving network node where ACL functionality is applied may only accept connections from other peer network nodes once the source addresses of the sending network node are known in the receiving node.

[9] IP Security – a collection of protocols and algorithms for IP security, including key management.

to transfer UEs. Indeed, if the eNodeBs do not share a pool area in common, the MME associated with the UE must be relocated on handover and the S1 handover has to be used (see Sections 2.5.6 and 2.6.3 respectively).

25.4 Automatic Configuration of Physical Cell Identity

The application-level configuration data exchanged during the X2 setup procedure is also the core of another SON feature: automatic self-configuration and self-optimization of the Physical Cell Identities (PCIs). This helps the eNodeBs to select PCIs that avoid collisions and hence cell confusion. Cell confusion arises when two neighbouring cells broadcast the same PCI so that a UE cannot discriminate between the two cells when it reports measurements. As a consequence the serving eNodeB of that UE cannot determine which one of these two cells should be the handover target for the UE. Increased inter-cell interference may also arise. The possibility for cell confusion stems from the fact that only about five hundred PCI values are available. PCI collision can be avoided by careful configuration on the part of the network operator, i.e. by selecting the PCIs allocated to each cell so that they are unique within clusters of adjacent neighbouring cells; however, this is a laborious operation, and moreover there remains an ongoing risk of further PCI collisions due to the start up of new eNodeBs as the network is densified.

The SON solution to this problem relies on the exchange of PCI values between neighbour eNodeBs during the X2 Setup procedure. In both the 'X2 SETUP REQUEST' and the 'X2 SETUP RESPONSE' messages, an eNodeB can include the list of PCI values used not only by its own cells but also by the 'direct neighbours' of its own cells. A direct neighbour of a cell is defined as any cell controlled by an eNodeB that is a neighbour of the eNodeB controlling the first cell (even if that cell has not yet been reported by any UE). This exchange of direct neighbour PCI values over the X2 interface enables an eNodeB to become quickly aware of the set of PCI values that are being used in the cluster to which it belongs. In particular the eNodeB can easily identify any collision in this cluster and can decide to change the PCI of one of its cells if needed; if it does so, it can signal the change to its neighbours in an 'eNB CONFIGURATION UPDATE' message. However, the exact PCI change algorithm supported by eNodeBs is not standardized and remains up to vendor implementations. An example of self configuration of PCIs is illustrated in Figure 25.3.

Via O&M, the network operator can use a variety of degrees of self-configuration at start up of the network: the operator could assign no PCI values and let each eNodeB select PCIs fully autonomously, or alternatively a range of possible PCI values can be assigned in order to assist the convergence of the self-configuration algorithms.

25.5 Mobility Load Balancing Optimization

Release 9 incorporates SON load balancing functionality, the objective of which is to counteract local traffic load imbalance between neighbouring cells with the aim of improving the overall system capacity and reducing congestion. The feature functions by first detecting any traffic imbalance and then applying solutions such as adjusting the cell reselection/handover parameters (such as handover thresholds). These parameters can be autonomously changed

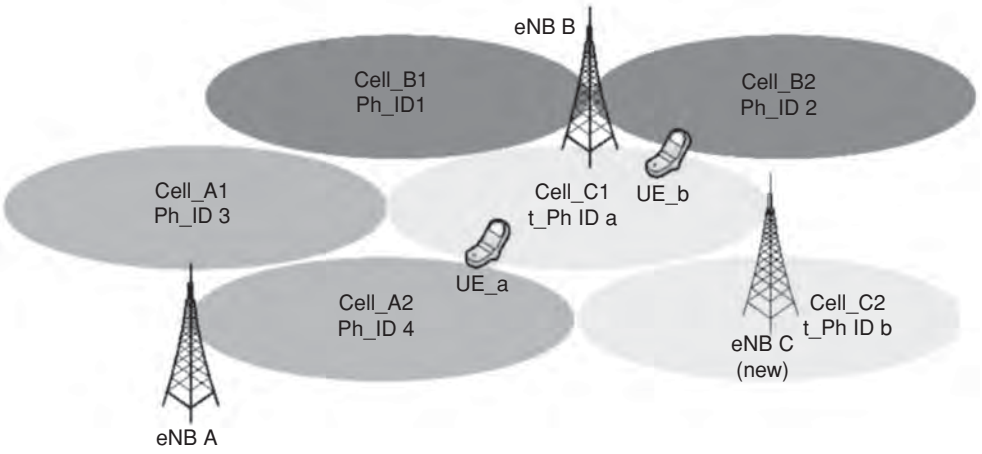

Figure 25.3: Illustration of PCI allocation. Reproduced by permission of © 3GPP.

and directly communicated between neighbouring cells by means of the X2 Parameter Negotiation procedure as explained in Section 25.5.2.

25.5.1 Intra-LTE Load Exchange

In order to detect an imbalance, it is first necessary to exchange load information between neighbouring eNodeBs over X2 for comparison. A client-server mechanism is used for this purpose: a requesting eNodeB (client) sends a 'RESOURCE STATUS REQUEST' message to request a load report from some of its neighbours. The 'RESOURCE STATUS REQUEST' message can simultaneously request multiple types of load report and may also be directed at multiple cells of the receiving eNodeB (server). The neighbours that receive the request report the requested load information over the X2 interface via the 'RESOURCE STATUS RESPONSE/UPDATE' message. The reporting of the load is periodic with period indicated in the 'RESOURCE STATUS REQUEST' message.

The reported information can indicate any of four different types of cell load information:

- Current usage of Physical Resource Blocks (PRBs), possibly partitioned into real-time and non-real-time traffic;
- Current hardware load;
- Current S1 transport load;
- Available composite load.

The first three measurements represent a global view of the current load situation in the node that reports them. The 'available composite load' indicator represents the amount of overall resources that the reporting node is ready to accept. 'Composite' means that the reporting node takes into account multiple internal resource criteria via a proprietary evaluation to build up its report. The 'available' characteristic is interesting as an estimate

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.