Agenda: 12.2

Source: Motorola

Title: **RNSAP Adaption Layer**

Title: **RNSAP Adaptation Layer**

Date: **March 15 -19th, 1999**

Source: **MOTOROLA**

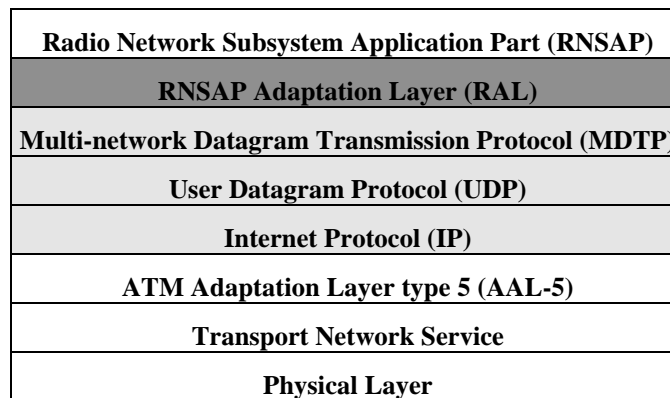**Key Issue:** I_U **Control Plane for the IP Domain**

1.   Introduction

Tdoc numbers R3-99-136 refers to the RNSAP Adaptation Layer (RAL). This contribution provides details of the RAL protocol.

The RNSAP Adaptation Layer (RAL) provides a mapping of the RNSAP primitives and addressing to/from the lower layer protocols. RAL is responsible for the abstraction of the various underlying transport technologies, load management, fault management, as well as presenting a unified communication interface to RNSAP.

2.   Overview

As an adaptation layer, RAL does not prefix a protocol header to datagrams passed to/from RNSAP and MDTP. Figure 1 provides an overview of where RAL is positioned within the I_{ur} protocol stack.

Figure 1: RAL Protocol Stack

Radio Network Subsystem Application Part (RNSAP)
RNSAP Adaptation Layer (RAL)
Multi-network Datagram Transmission Protocol (MDTP)
User Datagram Protocol (UDP)
Internet Protocol (IP)
ATM Adaptation Layer type 5 (AAL-5)
Transport Network Service
Physical Layer

The RAL layer is responsible for translating RNSAP Connection Identifiers to protocol specific IP Addresses, which consist of IP and Port numbers. IP addresses can be statically defined, or they can be dynamically acquired using Dynamic Host Configuration Protocol (DHCP). To take advantage of the multiple linkset services in MDTP, it may be possible for a single physical node to be assigned multiple IP addresses, whereby the group of IP addresses could be considered a single endpoint. Knowledge of connected endpoints may also be statically defined, or endpoints could be discovered (Endpoint Discovery) using techniques similar to Mobile IP Agent Discovery or ICMP Router Discovery. Across the interface between RNSAP and RAL, an *Endpoint Name* will be used to abstract the details of the underlying Signaling Bearer protocols from the RNSAP layer.

March, 15-19, 1999
Stockholm, Sweden

3.   RAL Procedures

3.1   RNSAP Procedures

Although the RNSAP is not fully defined, some functionality can be assumed with regard to the RAL
procedures required to support the RNSAP interface.

3.1.1   Connection Establishment

RNSAP should send an *N-CONNECT Request* primitive, for a specified endpoint name, to request
association of a *Connection Identifier* with the establishment of an endpoint session. Since the lower layer
MDTP is a connectionless protocol, a connection request should be interpreted by the RAL layer as a
request to associate the connection identifier with the assignment of UDP Port Numbers.

The local and remote RAL layers will be responsible for determining which UDP Port Numbers are to be
associated with the *Connection Identifier*. The local and remote RAL layers will associate the local and
remote IP Addresses and UDP Port numbers with the *Connection Identifier* received in the *N-CONNECT
Request*. All subsequent RNSAP messaging for that *Connection Identifier* will use the associated IP
Addresses and UDP Port Numbers. If the RAL layer is unable to translate the *Endpoint Name* received in
the N-CONNECT Request, then an error should be returned in a RNSAP *N-STATUS Indication* primitive
generated by the local RAL layer, to the upper RNSAP layer.

3.1.2   Disconnect and Release Resources

Once RNSAP has associated a *Connection Identifier* with a set of resources (using Connection
Establishment procedure), all RNSAP messaging will use Connection Identifier, as opposed to Endpoint
Name. This means that N-DISCONNECT Request can be treated as a request to disassociate resources
with the given Connection Identifier. Therefore, the remote endpoint's RAL layer will disassociate
resources with the Connection Identifier (e.g. UDP Port Number) upon receipt of the N-DISCONNECT
Request. The local RAL layer will disassociate resources with the Connection Identifier upon receipt of the
N-DISCONNECT Indication.

3.1.3   RNSAP Message Exchange

With the exception of N-CONNECT Request, if the RAL layer ever receives a RNSAP primitive to send a
message for a *Connection Identifier* that does not have resources associated with it, then an error should be
returned in a RNSAP *N-STATUS Indication* primitive, generated by the local RAL layer, to the upper
RNSAP layer.

If the local RAL layer ever receives a RNSAP message from MDTP, for a *Connection Identifier* that does
not have resources associated with it, then an error should be returned in a RNSAP *N-STATUS Indication*
message, generated by the local RAL layer, to the remote RAL layer, and sent via MDTP.

3.2   Endpoint Procedures

When an endpoint is initialized, it will send an *Endpoint Advertisement* as either a multicast or broadcast
message. Optionally, the endpoint may choose to also send an *Endpoint Solicitation* as either a multicast or
broadcast message. At this point, the endpoint will begin listening for *Endpoint Advertisement* messages
from other connected endpoints.

The lifetime field in each *Endpoint Advertisement* message indicates the maximum amount of time an
endpoint should wait before it receives another *Endpoint Advertisement* message from that endpoint. If the
lifetime period is exceeded, then the endpoint should be considered out of service. The endpoint originating
an *Endpoint Advertisement* message shall retransmit the *Endpoint Advertisement* messages at a frequency of
1/3 the lifetime value. This means that the other connected endpoints would need to miss three (3)
Endpoint Advertisement messages from an endpoint before marking that endpoint out of service.

As RAL detects new endpoints, or determines that existing endpoints have transitioned in or out of service, it shall notify the upper layer protocol, RNSAP, via the *N-STATUS Indication* primitive. The format of the *N-STATUS Indication* primitive is f.f.s., but minimally, the *N-STATUS Indication* primitive should contain data from the *Endpoint Name* and *Endpoint Capabilities* information elements, as well as the state of the endpoint.

4. RNSAP Primitive Handling

RAL will use the MDTP primitives for exchanging RNSAP messages and events over a Signaling Bearer. Table 1 provides a mapping of the RNSAP Application Programming Interface (API) to MDTP primitives.

Table 1: RAL Primitive Mapping

RNSAP API	MDTP Primitive
N-CONNECT Request	Data.Request
N-CONNECT Indication	Data.Indication
N-CONNECT Response	Data.Request
N-CONNECT Confirm	Data.Indication
N-DISCONNECT Request	Data.Request
N-DISCONNECT Indication	Data.Indication
N-DATA Request	Data.Request
N-DATA Indication	Data.Indication
N-UNITDATA Request	Data.Request
N-UNITDATA Indication	Data.Indication
N-STATUS Indication	Error.Indication Restore.Indication Endpoint Discovery Translation Errors

The actual definition of the RNSAP primitives is for f.f.s. Where applicable, assumptions and suggestions regarding RNSAP primitives are presented in subsequent sections of this document.

4.1 Data.Request

One of the most basic services requested of the lower layer is the Data.Request. After mapping an endpoint name to an IP Address, RAL would format a Data.Request as follows:

Data.Request(*Datagram, DatagramSize, AddressInformation, Options*)

The *Datagram* field holds the application data being transmitted. The *DatagramSize* holds the number of octets being transmitted. The *AddressInformation* contains an IP address. The *Options* field holds only options being passed to the lower layer.

4.2 Data.Indication

Another basic service that must be supported by RAL is the Data.Indication. The RAL will periodically call this primitive as follows:

Data.Indication(*Datagram, DatagramSize, AddressInformation, AddressType*)

The datagram should carry the information sent by the remote endpoint. The *DatagramSize* should be the number of octets sent by the remote endpoint. The *AddressInformation* should be the address of the sender. RAL is responsible for mapping this *AddressInformation* into an *Endpoint Name* for communication to the upper layer protocol, RNSAP. *AddressType* should be an indication of the type of address information (e.g. IPv4 vs. IPv6) contained in the *AddressInformation* field.

March, 15-19, 1999
Stockholm, Sweden
The RAL layer must also recognize RAL layer messages, such as Endpoint Discovery messages. RAL layer messages are not presented to the upper layer, and must be processed within the RAL layer.

4.3   Error.Indication

If a Error.Indication is to be generated to the upper application layer, it will be presented to the RAL layer in the form:

   Error.Indication(*AddressInformation, Datagram, DatagramSize, AddressType*)

A portion of the original *Datagram* should be present in the datagram field (all of the data if possible). The original *DatagramSize* of the sent datagram, and the *AddressInformation* should contain whom the datagram was sent to. This information should be in the form of a handle if possible. The *AddressType* should indicate to the upper layer how to interpret the *AddressInformation* (e.g. IPv4 vs. IPv6).

Upon receipt of an Error.Indication, the RAL layer will translate the *AddressInformation* to *the Endpoint Name*. An *N-STATUS Indication* primitive will be sent to the upper layer protocol, RNSAP.

4.4   Restore.Indication

This indication is sent to the RAL layer when a remote endpoint announces it is shutting down in a graceful manner. Upon receipt of such a event, the RAL layer should remove all routing information associated with this endpoint.

datagram arrives from a endpoint that was previously reported as down in an Error.Indication. The form of this indication is as follows

   Restore.Indication(*AddressInformation*)

Upon receipt of a Restore.Indication, the RAL layer will translate the *AddressInformation* to *the Endpoint Name*. An *N-STATUS Indication* primitive will be sent to the upper layer protocol, RNSAP.

5.

6.   Endpoint Discovery

For implementing procedures, such as Endpoint Discovery, the RAL layer will need to exchange signaling with other endpoints. Therefore, RAL messages will use a common header, depicted in the following figure:

Figure 2: RAL Message Header

8	7	6	5	4	3	2	1	octets
RAL Protocol Discriminator								1
								⋮
								8
Message Type								9
								10
Message Length								11
								12
Information Elements								13
								⋮
								N

Since these RAL messages will be broadcast and/or multicast, a 64-bit Protocol Discriminator was chosen virtually eliminate the possibility of falsing. Following the 16-bit message type and message length fields will be information elements appropriate for each message. The message length equals the length of all information elements plus twelve (12) octets for the *RAL Message Header*. Each Information Element will consist of the following format:

Figure 3: RAL Information Element Structure

8	7	6	5	4	3	2	1	octets
Information Element Type								1
								2
Information Element Length								3
								4
Information Element Data								5
								⋮
								N

Following the 16-bit information element type and information element length fields will be information element data appropriate for the information element type. The information element length equals the length of all data octets plus four (4) octets for the *RAL Information Element* header.

March, 15-19, 1999

Stockholm, Sweden

The Endpoint Discovery message set will be distinguished by a protocol discriminator of hexadecimal E2D90127D15C04E6. The Endpoint Discovery message set will consist of:

Table 2: RAL Endpoint Discovery Messages

Message Type	Message Name	Message Description
0x0001	Endpoint Advertisement	Periodically sent by an Endpoint to Advertise it Address and Capability information.
0x8001	Endpoint Solicitation	Sent by an Endpoint to solicit the broadcast or multicast of the Endpoint Advertisement.

The Information Elements used in the RAL Endpoint Discovery messages will consist of:

Table 3: RAL Endpoint Information Elements

IE Type	Information Element Name	Information Element Description
0x0001	Endpoint Lifetime	Contains data indicating time frame that endpoint information contained in a message shall remain valid.
0x0010	Endpoint Name	Null terminated string identifying Endpoint
0x0011	Endpoint IPv4 Address	Contains IPv4 address information present at an endpoint.
0x0012	Endpoint IPv6 Address	Contains IPv6 address information present at an endpoint.
0x0100	Endpoint Capabilities	Bitmap indicating functionality and capabilities of endpoint.

5.1 Endpoint Advertisement Message

An endpoint will periodically multicast or broadcast an *Endpoint Advertisement* message to those endpoints that it wishes to communicate with. If the *Endpoint Advertisement* message is in response to an *Endpoint Solicitation* message, then it may be sent as a unicast message to the soliciting endpoint. The format of the *Endpoint Advertisement* message will contain all of the information elements currently listed above.

5.2 Endpoint Solicitation Message

An endpoint may multicast or broadcast an *Endpoint Solicitation* message upon transitioning into service, or periodically as an audit to synchronize addressing information. The purpose of this an *Endpoint Solicitation* message is to request *Endpoint Advertisement* messages from the other connected endpoints. The format of the *Endpoint Solicitation* message is only the *RAL Message Header*.

5.3 Endpoint Lifetime Information Element

The Endpoint Lifetime IE is used for

Figure 4: Endpoint Lifetime IE Structure

8	7	6	5	4	3	2	1	octets
Lifetime								1
								2
Sequence Number								3
								4

March, 15-19, 1999

Stockholm, Sweden

The lifetime field indicates the number of seconds that the information sent in the *Endpoint Advertisement* shall be considered valid. The sequence number is the count of advertisement messages sent by the endpoint since the time the endpoint was initialized.

5.4   Endpoint Name Information Element

The Endpoint Name IE is used for identifying the endpoint to the upper layer protocol, RNSAP. The Endpoint Name abstracts the details of the underlying Signaling Bearer protocols from RNSAP.

Figure 5: Endpoint Name IE Structure

8	7	6	5	4	3	2	1	octets
Endpoint Name									1
								⋮
0	0	0	0	0	0	0	0	N

The *Endpoint Name* is a null terminated string. The Information Element Length, less five (5) octets, will equal the length of the *Endpoint Name*.

5.5   Endpoint IPv4 Address Information Element

The Endpoint IPv4 Address IE is used for identifying an endpoint using IPv4 addressing.

Figure 6: Endpoint IPv4 Address IE Structure

8	7	6	5	4	3	2	1	octets
IP Number									1
								2
								3
								4
UDP Port Number									5
								6

The IP Number is the 32-bit IPv4 address format. The UDP Port Number is the well known 16-bit identifier of an endpoint process.

5.6   Endpoint IPv6 Address Information Element

The Endpoint IPv6 Address IE is used for identifying an endpoint using IPv4 addressing.

Figure 7: Endpoint IPv6 Address IE Structure

8	7	6	5	4	3	2	1	octets
IP Number									1
								⋮
								16
UDP Port Number									17
								18

The IP Number is the 128-bit IPv6 address format. The UDP Port Number is the well known 16-bit identifier of an endpoint process.

5.7   Endpoint Capabilities Information Element

The Endpoint Capabilities IE is used for identifying the features and/or services supported by a given endpoint.

Figure 8: Endpoint Capabilities IE Structure

8	7	6	5	4	3	2	1	octets
Capabilities Bitmap								1
								⋮
								N

The definition of the *Capabilities Bitmap* is f.f.s., but conceptually, a coding of 0 for a bit will indicate that the service or feature represented by the bit is not supported by the endpoint, and a coding of 1 for a bit will indicate that the service or feature represented by the bit is supported by the endpoint. The length of the information element is allowed to grow as more capabilities are defined for this information element. The reasoning behind a bitmap is that it enables additional features and services to be added, while maintaining backward compatibility. Furthermore, the bitmap will not dictate a particular endpoint implementation, which allows manufacturers flexibility to combine or distribute capabilities on one or more platforms.

7.   Proposal

It is proposed that:

1. The text in sections 2 to 5 is included in S3.22,within a new subsection 5.3.1 titled RNSAP Adaption Layer.

8.   References

[1] Postel, J. (editor), "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, August 1980.

[2] Postel, J. (editor), "Internet Protocol", RFC 791, USC/Information Sciences Institute, September 1981

[3] Deering, S. (editor), "ICMP Router Discovery Messages", RFC 1256, Xerox Parc, September 1991

[4] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, Bucknell University, March 1997

[5] Stewart R.R., Xie Q. "Multi-network Datagram Transmission Protocol" , draft-sigtran-mdtp-01.txt, February 15, 1999.

[6] S3.22, Iur Signaling Plane, v0.0.2