Y-Net Protocol Stack Overview

Important Notice

All products are sold subject to the terms and conditions of sale supplied at the time of order acknowledgment, including those pertaining to warranty, patent infringement, and limitation of liability. Yitran Communications Ltd. (“Yitran”) reserves the right to make changes to its products or to discontinue any product or service without notice, and advise customers to obtain the latest version of relevant information to verify, before placing orders, that information being relied on is current and complete.

Yitran warrants performance of its semiconductor products to the specifications applicable at the time of sale in accordance with Yitran’s standard warranty. Testing and other quality control techniques are utilized to the extent Yitran deems necessary to support this warranty. Specific testing of all parameters of each device is not necessarily performed, except those mandated by government requirements.

Certain applications using semiconductor products may involve potential risks of death, personal injury, or severe property or environmental damage (“Critical Applications”). Yitran’s PRODUCTS ARE NOT DESIGNED, AUTHORIZED, OR WARRANTED TO BE SUITABLE FOR USE IN LIFE–SUPPORT DEVICES OR SYSTEMS OR OTHER CRITICAL APPLICATIONS. INCLUSION OF Yitran’s PRODUCTS IN SUCH APPLICATIONS IS UNDERSTOOD TO BE FULLY AT THE CUSTOMER’S RISK.

In order to minimize risks associated with the customer’s applications, the customer, to minimize inherent or procedural hazards, must provide adequate design and operating safeguards.

Yitran assumes no liability for applications assistance or customer product design. Yitran does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right of Yitran covering or relating to any combination, machine, or process in which such semiconductor products or services might be or are used. Yitran’s publication of information regarding any third party’s products or services does not constitute Yitran’s approval, warranty or endorsement thereof.

All company and brand products and service names are trademarks or registered trademarks of their respective holders.

About This Guide

This document describes Yitran's Y-Net protocol stack.

This guide contains the following chapters:

- **Chapter 1, Introduction,** page 7, introduces the Y-Net protocol stack.
- **Chapter 2, Y-Net Protocol Stack Layering Mode,** page 8, describes the Y-Net protocol stack-layering mode.
- **Chapter 3, Media Access Control (MAC),** page 9, describes the Y-Net protocol stack's Media Access Control (MAC) layer.
- **Chapter 4, Network Layer (NL),** page 12, describes the Y-Net protocol stack's network layer (NL).
- **Chapter 5, Host Application,** page 28, describes the Y-Net protocol stack's application-level functionality.

Table of Contents

Table of Tables

Table of Figures

Chapter 1

Introduction

The Y-Net protocol stack provides a set of advanced communication services enabling a standard, rapid and simple method of development for narrow bandwidth, low-cost command and control networking applications over the power line media using IT900. Both the Protocol Controller Architecture and the Open Solution Architecture version of the IT900 are accompanied by Yitran's Y-Net protocol firmware.

The Y-Net stack provides high flexibility and an extensive range of modes and configurations for developing applications based on the most suitable network installation scenario requirements for that application. The Y- Net stack supports network installation scenarios varying from simple plug-and-play networks (Y-Net defaults) to highly secured (for example, application controlled) networks.

The services provided by the Y-Net protocol stack enable developers to focus their efforts on the implementation of their applications, rather than on the communication and networking function.

Chapter 2

Y-Net Protocol Stack Layering Mode

The Y-Net protocol stack is based on the OSI 7-Layer Network Reference model, with some modifications to match the specific requirements of command and control applications. The layering model of the Y-Net protocol stack is compared with the OSI 7-Layer Network Reference model in the following figure.

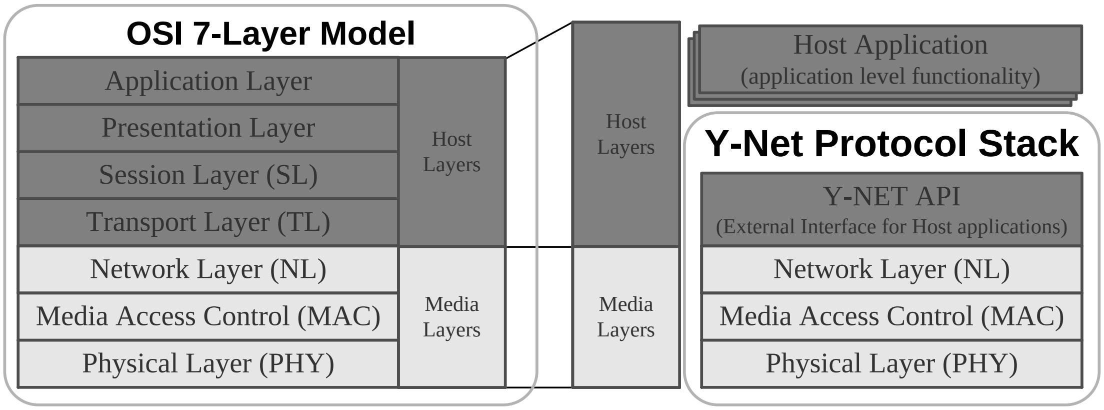

Figure 1: Layering Model of the Y-Net Protocol Stack versus the OSI 7-Layer Model

The Y-Net protocol stack defines only those layers and sub-layers relevant to typical Y-Net host applications.

The Y-Net protocol stack consists of the following:

- Physical (PHY) layer consisting of the physical interface to the power line media.
- Media Access Control (MAC) layer providing a Y-Net stack interface for lower-layer communication services (you may refer to *Chapter 3, Media Access Control (MAC)*, on page 9 for more information).
- Network layer (NL) providing a Y-Net stack interface for advanced networking services, such as admission, routing and addressing (you may refer to *Chapter 4, Network Layer (NL)*, on page 12 for more information).
- The host application in which specific application logic and management resides (you may refer to *Chapter 5, Host Application*, on page 28 for more information).

Chapter 3

Media Access Control (MAC)

3.1 Introduction

The MAC layer implements a highly efficient channel access management function, which enables the channel to be occupied by only a single node at any given time while providing adequate Quality of Service (QoS) among nodes and maintaining high overall network throughput (you may refer to the *Section 3.2*, *Channel Access Method*).

In addition, the MAC layer supports low-level communication services, as listed below:

- **Packet Transmission Services,** as described in *Section 3.3*
- **Addressing and Logical Networks,** as described in *Section 3.4*
- **Statistics and Diagnostics,** as described in *Section 3.6*

3.2 Channel Access Method

The MAC uses a Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) protocol with an adaptive back-off scheme and channel access prioritization to manage channel access in such a way that only a single sending node occupies the communication channel at any given time. This channel access method is optimized for the power line media and provides optimal performance for network sizes ranging from a few nodes to thousands of nodes.

The media access control is based on the following:

- **Super-frame Time Intervals,** as described in *Section 3.2.1*
- **Carrier Sense Mechanism,** as described in *Section 3.2.2*
- **Packet Prioritization and QoS,** as described in *Section 3.2.3*
- **Adaptive Back-off Algorithm,** as described in *Section 3.2.4*

3.2.1 Super-frame Time Intervals

A super-frame is the time between the end of packet transmission (EOP) and the start of the next packet transmission. The super-frame is sub-divided into time intervals for signaling MAC events, for the back-off period and for the message transmission period.

3.2.2 Carrier Sense Mechanism

The PHY layer provides Carrier Detection (CD) indication to the MAC. The output of the PHY CD signal to the MAC indicates an ongoing transmission on the line.

3.2.3 Packet Prioritization and QoS

Host applications can assign priorities to sent packets, as follows:

- Emergency
- High
- Normal
- Normal Fragmented (dedicated for the transmission of fragmented packets)

The MAC signals the priority of packets transmitted as part of the super-frame (no signal for normal priority packets). The MAC ensures that only transmitters that have packets with the highest priority contend for channel access in each super-frame.

3.2.4 Adaptive Back-off Algorithm

The adaptive back-off algorithm manages the contention for the channel by multiple transmitters. The MAC continuously updates the size of the back-off randomization range (per priority). The back-off range is optimally set for maximizing the throughput as a function of the number of nodes simultaneously contending for channel access.

If the MAC is unable to transmit the packet within the timeout set by the upper layer, it discards the packet as blocked and informs the upper layer.

3.3 Packet Transmission Services

The MAC layer encapsulates the payload received from the upper layer and provides various types of packet transmission services to and from the upper layer.

The MAC protocol supports the packet delivery services detailed in Table 1.

Table 1: Packet Transmission Services

Service	Description
Unicast with Acknowledgement	Unicast transmission in which the receiving node sends an acknowledgment to the transmitting node to indicate the successful reception or a lack of resources to receive the packet.
Unicast Repetitive – without Acknowledgement	Unicast transmission service in which the packet is retransmitted a specified number of times, regardless of its successful or unsuccessful delivery. The receiving node does not send a packet reception acknowledgment.
Broadcast	The MAC provides two types of broadcast services: (1) **Intranetworking Broadcast:** The packet is transmitted to all nodes in the same logical network. (2) **Internetworking Broadcast:** The packet is transmitted to all nodes regardless of their logical network. Broadcast packets may also be retransmitted repetitively, using the Repetitive –without Acknowledgement service.

3.4 IT900 Transmission Rate Modes

The IT900 supports multiple transmission rate modes which are dynamically selected by the IT900 MAC layer according to channel quality and statistics. In addition, the IT900 supports Yitran's IT700/IT800 modulation (DCSK) and rates which will be activated automatically when target device is IT800/IT700 or when channel conditions require.

The table below details the range of transmission rates supported by the IT900 for each operation band:

Table 2: IT900 Transmission Rates

TX Mode	Data Rate [kbps]		
	FCC	CENELEC-A	CENELEC-B
DCSKT Turbo (DCSKT)	Up to 500	Up to 150	Up to 50
DCSK	7.5 (SM), 5(RM), 1.25(ERM)	2.5(RM), 0.625(ERM)	2.5(RM), 0.625(ERM)

3.5 Addressing and Logical Networks

Similar to the unique MAC address in IP networks, IT900's MAC layer uses a 16-byte Serial Number (S/N), which is unique for each IT900 IC. The S/N is used by Internetworking broadcast transmissions to identify the transmitter.

IT900's MAC layer also defines an 11-bit logical node address (Node ID) and a 10-bit logical network address (Network ID). The logical node and network addresses are local to the specific logical network. The network address must be unique for each logical network on the same physical network and the node address must be unique within the same logical network. A node can only use a single logical address. The network and node addresses can be configured by the upper layer. Communication services within the same logical network use logical addressing.

3.6 Statistics and Diagnostics

The PHY and MAC layers collect and provide channel-quality information and statistics to the upper layer.

Chapter 4

Network Layer (NL)

4.1 Introduction

The NL transparently creates and maintains a tree-type topology network and releases the upper layer from the responsibility of handling the constantly changing conditions of the power line media.

The logical network consists of a Network Coordinator (NC) node responsible for network formation activities. The NC is expected to remain online most of the time. All other nodes in the logical network are remote stations (RS). An RS may serve as a router to route packets to or from the NC and may also implement remote application functionality.

The NL provides the following networking services:

- **Data Services:** Providing advanced intranetworking and internetworking services (you may refer to *Section 4.2, Data Services*).
- **Management Services:**
  - **Network Formation Services:** Enabling users without any prior networking or protocol knowledge to easily install, create and maintain logical networks (you may refer to *Section 4.3.1, Network Formation* for more information).
  - **Dynamic Routing Service:** The NL creates a tree topology, enabling the NC to communicate with all nodes in the same logical network and vice versa (via intermediate nodes if required). This service provides complete transparency of the communication between all the ICs and the NC, and makes them behave like standard peer-peer communication. Peer-peer communication between every two ICs is also supported, as long as they have direct physical connectivity (you may refer to *Section 4.3.2, Dynamic Routing* for more information).

The Y-Net protocol permits NL functionalities to be disabled. In such cases, the protocol provides DLL-level functionalities.

4.2 Data Services

4.2.1 Introduction

Data services are responsible for the transmission and reception of upper layer payloads, meaning the transmission (Tx) and Reception (Rx) processes (you may refer to *Section 4.2.2, Tx/Rx Processes* for more information).

The data services used by the NL are as follows:

- **Internetworking:** Transmission of data between networks (you may refer to *Section 4.2.3, Internetworking Services* for more information).
- **Intranetworking:** Transmission of data (may be over multiple hops) between nodes in the same network (you may refer to *Section 4.2.4, Intranetworking Services* for more information).

The maximum payload size per data service is summarized in *Section 4.2.5,* *Maximum Payload Size per NL* Data Service.

4.2.2 Tx/Rx Processes

The data transmission process (Tx) begins with a request from the upper layer to the NL consisting of payload and transmission parameters. The NL prepares the transmission header and executes the transmission of the payload based on these parameters.

The data reception process (Rx) is triggered by the arrival of a packet to the NL from the MAC. The packet header is processed, as follows:

- Forward the payload to the upper layer if the receiver is the authorized destination of the received packet.
- Route the packet if the packet header processing indicates that routing is required. Otherwise, discard the packet.

4.2.3 Internetworking Services

4.2.3.1 Internetworking Unicast Service

The Internetworking Unicast service enables a source node from one logical network to transmit packets to an individual destination node in another logical network, as shown in Figure 2.

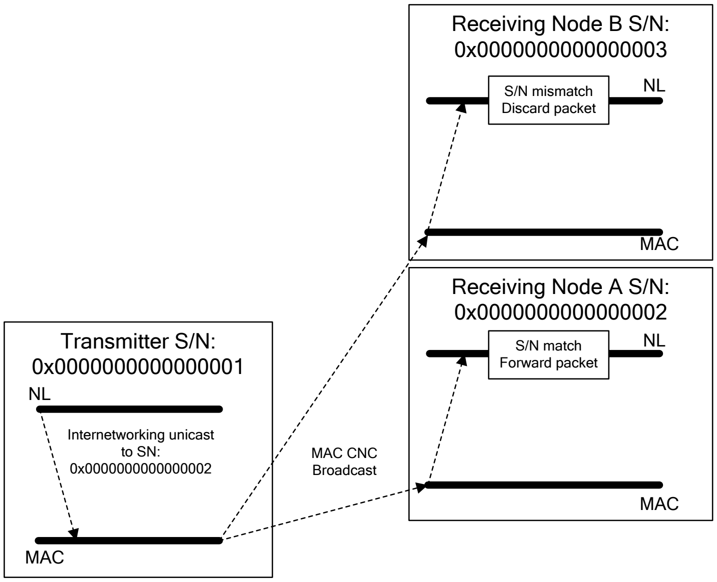

Figure 2: Internetworking Unicast Service

4.2.3.2 Internetworking Broadcast Service

The Internetworking Broadcast service enables a source node to transmit packets to all surrounding nodes in the physical network, as shown in Figure 3.

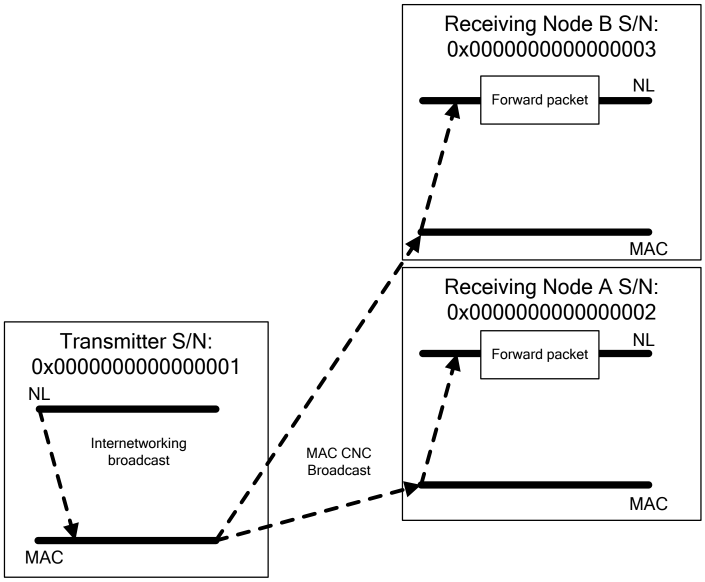

Figure 3: Internetworking Broadcast Service

4.2.4 Intranetworking Services

4.2.4.1 Direct Intranetworking Unicast

The Direct Intranetworking Unicast service enables a source node to transmit packets to an individual destination node from the same logical network, when they can communicate directly, as shown in Figure 4.

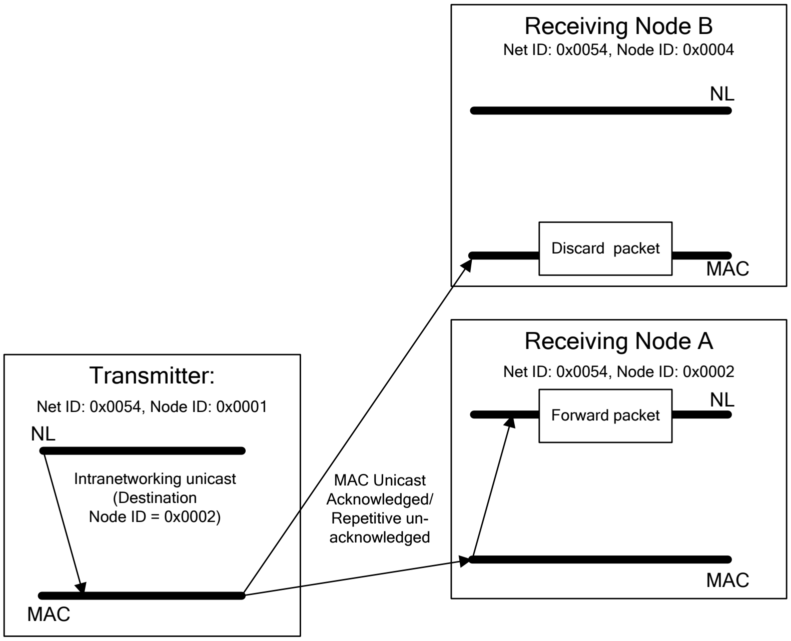
Receiving Node B
Net ID: 0x0054, Node ID: 0x0004
NL
Discard packet
MAC
Receiving Node A
Net ID: 0x0054, Node ID: 0x0002
NL
Forward packet
MAC
Transmitter:
Net ID: 0x0054, Node ID: 0x0001
NL
Intranetworking unicast (Destination Node ID = 0x0002)
MAC
MAC Unicast Acknowledged/ Repetitive un-acknowledged

Figure 4: Direct Intranetworking Unicast

4.2.4.2 Routed Intranetworking Unicast

The MAC provides unicast transmission services to transmit a packet from a single source node to an individual destination node in the same logical network if there is a direct connection between the two. The NL routing capabilities extend the MAC transmission service to enable nodes from the same logical network, which have no direct connection, to communicate via intermediate nodes.

During the routing process, each node along the route, from the originating node to the final destination node, retransmits the packet using one of the MAC unicast transmission services (acknowledged or repetitive un-acknowledged). The originating node defines which MAC transmission service to use and all intermediate nodes use the same MAC service to retransmit the packet to the next node along that route.

The NL routing function selects the next node along the route to the final destination and retransmits the packet to that node, as shown in Figure 5.

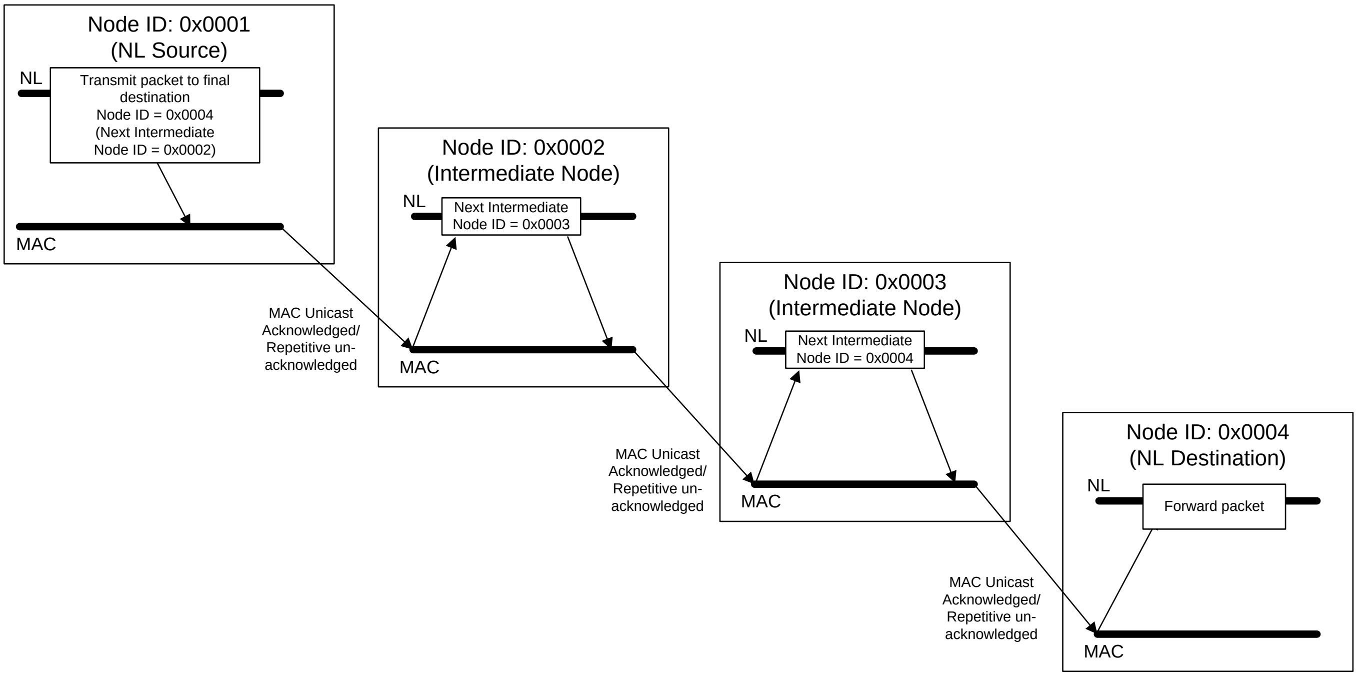
Node ID: 0x0001
(NL Source)
NL
Transmit packet to final destination
Node ID = 0x0004
(Next Intermediate Node ID = 0x0002)
MAC
MAC Unicast Acknowledged/ Repetitive un-acknowledged
Node ID: 0x0002
(Intermediate Node)
NL
Next Intermediate Node ID = 0x0003
MAC
MAC Unicast Acknowledged/ Repetitive un-acknowledged
Node ID: 0x0003
(Intermediate Node)
NL
Next Intermediate Node ID = 0x0004
MAC
MAC Unicast Acknowledged/ Repetitive un-acknowledged
Node ID: 0x0004
(NL Destination)
NL
Forward packet
MAC

Figure 5: General Routing Message Flow

The NL of each station consists of two unicast routing types: **Table Routing** and **Source Routing**. When any packet transmitted is received by the NL, the routing method is automatically selected. The NL performs packet routing according to the route information in its routing tables. The maximum number of hops in routed unicast packets is eight.

The routing service enables packets to be sent from the RS to the NC in the same logical network (and vice versa), even when they lack a direct communication link, as follows:

- **Table routing:** Is used by the NL when routing packets from the RS to the NC. This routing table, maintained by each node, indicates the node ID of the next node on the route to the destination node (in the case of the RS and NC, it is the parent of the RS). Table routing requires very small routing tables in the RS. An illustration of the Table Routing service is shown below in Figure 6.

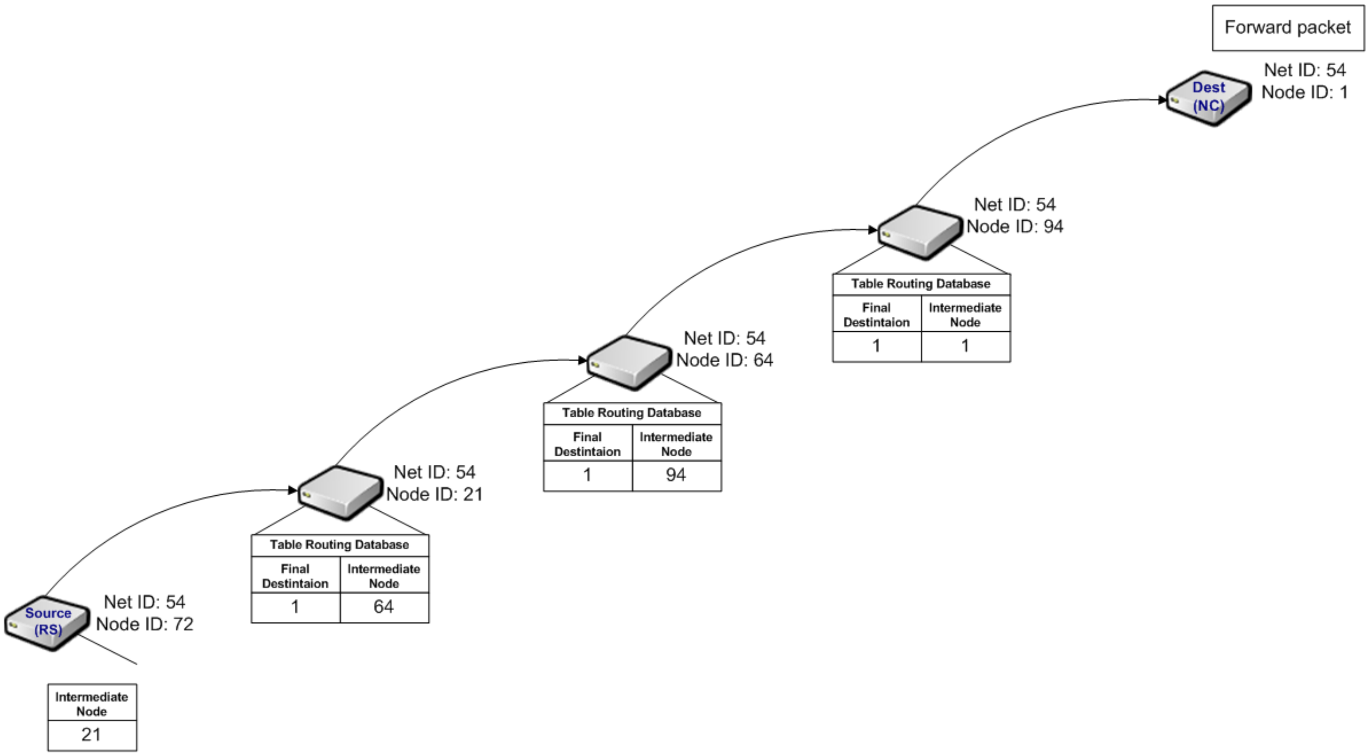

Table Routing Database	
Final Destintaion	Intermediate Node
1	1

Table Routing Database	
Final Destintaion	Intermediate Node
1	94

Table Routing Database	
Final Destintaion	Intermediate Node
1	64

Intermediate Node
21

Figure 6: Illustration of the Table Routing Service

- **Source Routing:** Is used by the NL when routing packets from the NC to any RS. The entire route from the transmitter to the final destination is set in the packet header. Nodes along the route extract the next node to which it should retransmit from the packet (in the case of the NC and the RS, the NC sets the route to the destination RS on the packet header, and the RS along the route to the final destination extracts the next hop from the packet header). Source routing requires a larger routing table only in the NC. An illustration of the Source Routing service is shown below in Figure 7.

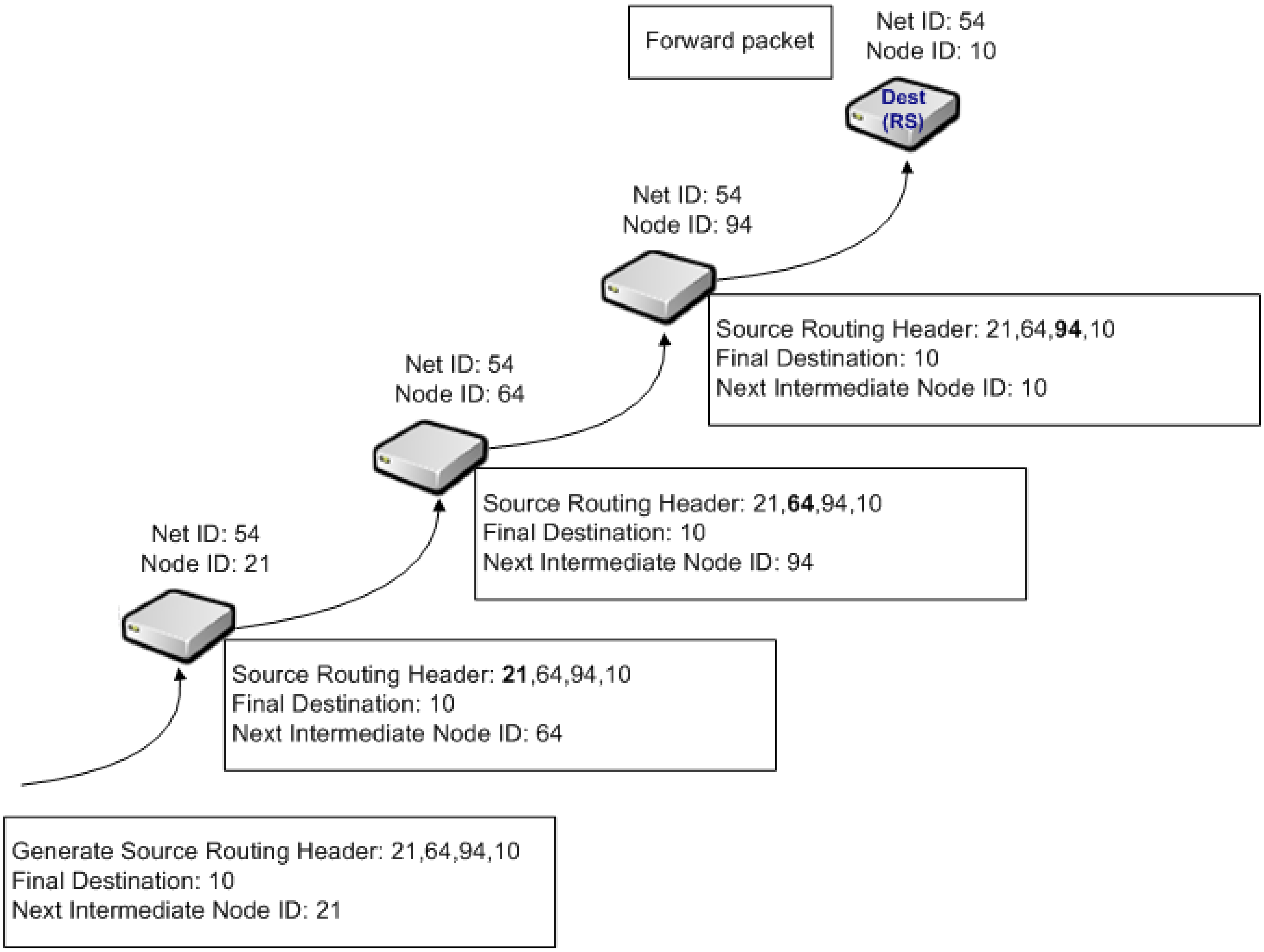
Forward packet
Net ID: 54
Node ID: 10
Dest (RS)
Net ID: 54
Node ID: 94
Source Routing Header: 21,64,**94**,10
Final Destination: 10
Next Intermediate Node ID: 10
Net ID: 54
Node ID: 64
Source Routing Header: 21,**64**,94,10
Final Destination: 10
Next Intermediate Node ID: 94
Net ID: 54
Node ID: 21
Source Routing Header: **21**,64,94,10
Final Destination: 10
Next Intermediate Node ID: 64
Generate Source Routing Header: 21,64,94,10
Final Destination: 10
Next Intermediate Node ID: 21

Figure 7: Illustration of the Source Routing Service

4.2.4.3 Intranetworking Broadcast Service

The Intranetworking Broadcast service enables a source node to transmit packets to all nodes with the same Network ID, meaning nodes that are from the **same** logical network, as shown below in Figure 8.

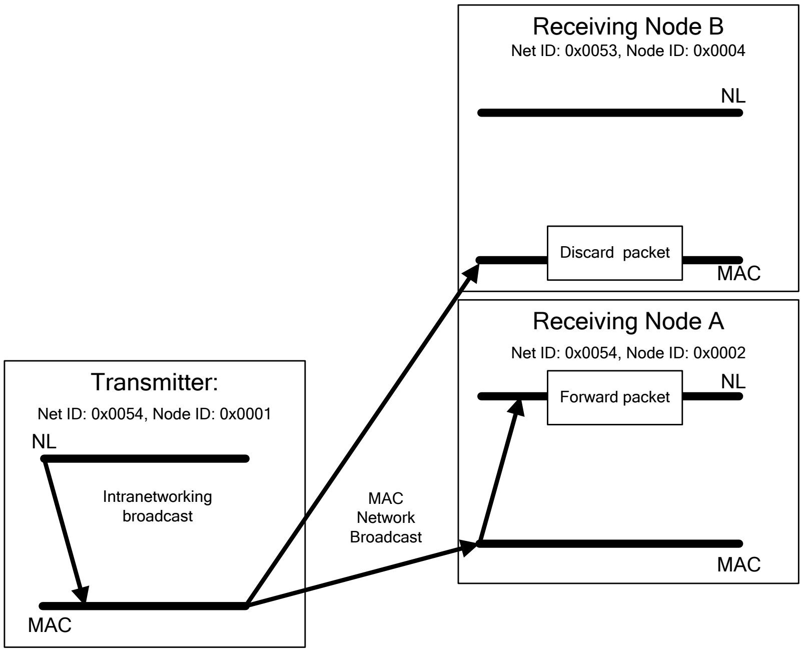
Receiving Node B
Net ID: 0x0053, Node ID: 0x0004
NL
Discard packet
MAC
Receiving Node A
Net ID: 0x0054, Node ID: 0x0002
Forward packet
NL
MAC
Transmitter:
Net ID: 0x0054, Node ID: 0x0001
NL
Intranetworking broadcast
MAC
MAC Network Broadcast

Figure 8: Intranetworking Broadcast Service

The Intranetworking Broadcast packets may be repeated over multiple hops (Multi-Hop Broadcast). When a Broadcast packet is transmitted, the transmitting node will define the number of hops that the packet may be repeated. A receiving node will decrease the packet’s HOPS counter by 1 and retransmit it to the line if the counter is greater than 0 (the same packet will not be re-transmitted twice by the same node).

However, in large networks, the broadcast repetition may cause high congestion in the network as many unnecessary transmissions may take place by this flooding mechanism.

In order to reduce the congestion level during Multi-Hop Broadcast transmissions, the Y-Net protocol may be configured to prevent from network leafs (Remote stations without children) to repeat the Multi-Hop Broadcast packets.

4.2.5 Maximum Payload Size per NL Data Service

The maximum payload size supported per NL data service is shown in Table 3 below.

Table 3: Maximum Payload Size per NL Data Service

#	Service	Max Payload Size – DCSK Turbo rates	Max Payload Size – DCSK rates	
		Encrypted/Non Encrypted	Encrypted	Non Encrypted
1	Internetworking Unicast	Up to 1522 bytes	77 bytes	87 bytes
2	Internetworking Broadcast	Up to 1522 bytes	93 bytes	103 bytes
3	Intranetworking source routing service	Up to 1522 bytes	67 bytes	76 bytes
4	Intranetworking table routing service	Up to 1522 bytes	97 bytes	106 bytes
5	Intranetworking direct Unicast service	Up to 1522 bytes	100 bytes	109 bytes
6	Intranetworking Broadcast service	Up to 1522 bytes	100 bytes	109 bytes
7	Fragmented Intranetworking services	1522 bytes		

The actual size of single fragment varies according to the transmission rate mode and regulation.

When the payload size exceeds the actual single fragment size the Y-Net splits the transmission into multiple fragments that are then reassembled in the receiving node. This mechanism is called **fragmentation** at the transmitting node and **reassembly** at the receiving node.

4.3 Management Services

4.3.1 Network Formation

4.3.1.1 Introduction

The NL network formation services consist of the following:

- **Logical Network Creation,** as describes in *Section 4.3.1.2*
- **Network Admission Control,** as describes in *Section 4.3.1.3*
- **Addressing Management,** as describes in *Section 4.3.1.4*
- **Networking Indications to Host,** as describes in *Section 4.3.1.5*
- **Cold/Warm Start Modes,** as describes in *Section 4.3.1.6*

4.3.1.2 Logical Network Creation

The logical network creation service enables a NC to select a unique Network ID (automatically or manually by configuration), thereby enabling RS nodes to join the logical network of the NC.

When a new node tries to join an existing network, it will first try to quickly join an optimal parent (for details refer to Section 4.3.2). The joining time of a few nodes to an existing network does not depend on the network size, and even for very large networks, it is kept extremely low (few seconds).

In networks where it is impossible to connect a node, the joining node will inflict with minimal disturbance to other networks. The disconnected node will continue to sense traffic and will only attempt to connect when overhearing relevant management traffic from potential parents.

In addition, nodes may accidentally join one NC, when in fact there was a significantly better NC to connect to. The NL periodic management processes can allow these nodes to switch between networks in this case based on configurations by the installer (for details refer to Section 4.3.2).

4.3.1.3 Network Admission Control

In a multiple-overlapping logical networks environment (multiple NCs utilizing the same physical network), it may be required for nodes to be associated to a specific logical network. The Network Admission Control services enable and assist the user to (automatically or in conjunction with the application):

- Associate nodes that should belong to the same logical network.
- Prevent hostile or incorrect nodes from joining a logical network.
- Prevent nodes from joining a hostile or incorrect logical network.

Two services enable the user to perform the above in a simple and quick manner, as follows:

- **Admission Process (in NC):** The NC admits only correct nodes to its network based on configurations of admission mode (meaning only nodes that should belong to the logical network are admitted, and potentially hostile or incorrect nodes are rejected). The admission modes are described in Table 4.

- **Node Key Approval (in RS):** The RS can overrule the NC's decision to admit it to its logical network (meaning prevent nodes from joining a hostile or incorrect logical network). When the NC admits a new node to the network, it attaches an 8-byte Node Key field to the admission approval packet sent to the RS. The Node Key can be set per RS by the NC application in application mode, admission mode or by default using the Node Key configured to the NC. If the Node Key configured in the RS matches the one received from the NC, the RS accepts the admission of the NC to its logical network. If not, the RS rejects the admission of the NC and does not join the network. The Node Key mechanism can be used for auto-segmentation of overlapping logical networks by configuring the same Node Key to an NC and all RSs that should be associated with the logical network of that NC. The RS can optionally disable the use of the Node Key mechanism, thereby accepting admission of any admitting NC by setting all the bytes of its configured Node Key to 0x00.

Table 4: NC Admission Modes

Admission Mode	Description
Auto Mode	No admission restrictions and host application involvement. When an admission request arrives at the NL of the NC from an RS, the NC immediately admits the RS to its network.
S/N Range Mode	S/N range restriction without host application involvement. When an admission request arrives at the NL of the NC from an RS, the NC admits only RSs whose MSBs of their S/N are within the S/N range configured in the NC (the number of MSBs to use is configurable in the NC).
Application Mode	Application restrictions. When an admission request arrives at the NL of the NC from an RS, the NL indicates so to the host application. The host application is responsible for deciding whether to admit the RS based on the S/N of the RS provided by the NL of the NC. The implementation usually consists of an admission table containing the allowed S/N. Note that in this mode, if the application recognizes the RS and admits the RS, the application may also be required to provide the Node Key of the RS to the NL of the NC. Otherwise, the Node Key configured in the NC is used by default.
S/N Range or Application Mode	When an admission request arrives at the NL of the NC from an RS, the NC attempts to admit the RS using the S/N Range mode first. If the RS is rejected using the S/N Range mode, the NC uses the Application Mode admission mode to admit the RS.

4.3.1.4 Addressing Management

Addressing management services are responsible for ensuring that each node is assigned with a unique logical address, meaning a unique Node ID within its Network ID (you may refer to *Section 3.4*).

The addressing management services consist of:

- Allocating logical addresses to nodes that guarantee a unique logical address within a physical network.
- Maintaining logical addressing uniqueness and resolving conflicts (both Network ID and Node ID).

4.3.1.5 Networking Indications to Host

The Y-Net stack interface provides NL indications to NC and RS node applications when networking events that may be relevant to device applications occur. These indications consist of the following:

- **NC Notifications:**
  - Notify when a new Network ID was assigned.
  - Notify when the NC Node ID is assigned.
  - Notify when a conflicting Network ID was replaced.
  - Notify when a new RS node attempts to join the network in applicable admission modes (you may refer to *Section 4.3.1.3, Network Admission Control*).
  - Notify when a new RS successfully joined the network.
- **RS Notifications:**
  - Notify when successfully joining a logical network.
  - Notify when leaving the logical network and failed admission attempts.
  - Notify about routing condition changes with the NC.
  - Notify about addressing allocation.
  - Notify about addressing conflicts.

4.3.1.6 Cold/Warm Start Modes

When the node is powered up, it initializes the NL management based on its starting mode:

- **Warm Start:** Is an NL start-up sequence mode in which a node restores its NL management data from its Non-Volatile Memory (NVM) and operates according to its state before it was shut down (meaning retains address, routing state with its parent, distance from the NC and so on).
- **Cold Start:** Is an NL start-up sequence mode, in which the RS rejoins a logical network on every power-up. In this mode, the RS may join a different logical network on every power-up.

4.3.2 Dynamic Routing

The physical network can be represented as a graph at any given time where links connect nodes that communicate directly. Links can be either unidirectional (if only one of the nodes can communicate with the other) or bidirectional (if the nodes on both ends of the link can communicate with each other).

Topology is a logical structure consisting of a subset of selected nodes and links from the graph representation of the physical network, such that the selected nodes subset in the topology have routes between them using the selected links subset in the topology to enable them to communicate.

The NL supports tree topology, in which the RS and the NC maintain an optimal symmetric bidirectional route between them (in terms of number of hops from the NC).

Figure 9 illustrates a tree topology for a graph representation of a sample physical network consisting of seven elements. The NC serves as the root of the tree topology and its Node ID is 1. The other nodes are assigned node IDs ranging from 2 to 7 and are arbitrarily organized down the tree, simulating a typical network topology in the NL.

In the tree topology, each RS maintains a link with a single node that is closer to the NC in terms of hops. The node that is closer to the NC is denoted the *parent* of the linked RS (the NC also serves as a parent). From the parent node's perspective, an RS that maintains a link with it is denoted as a *child* node (a parent may have multiple children in the topology). All the nodes on a branch below a parent node (its children, their children and so on) are denoted as the parent node's *siblings*.

For example, in Figure 9, the RS with Node ID 2 is the *child* of the RS with Node ID 5, and consequently, the RS with Node ID 5 is the *parent* of the RS with Node ID 2. The NC is the *parent* of two RSs (Node ID 5 and Node ID 6) and consequently, these RSs are the NC's children. All the RSs are *siblings* of the NC.

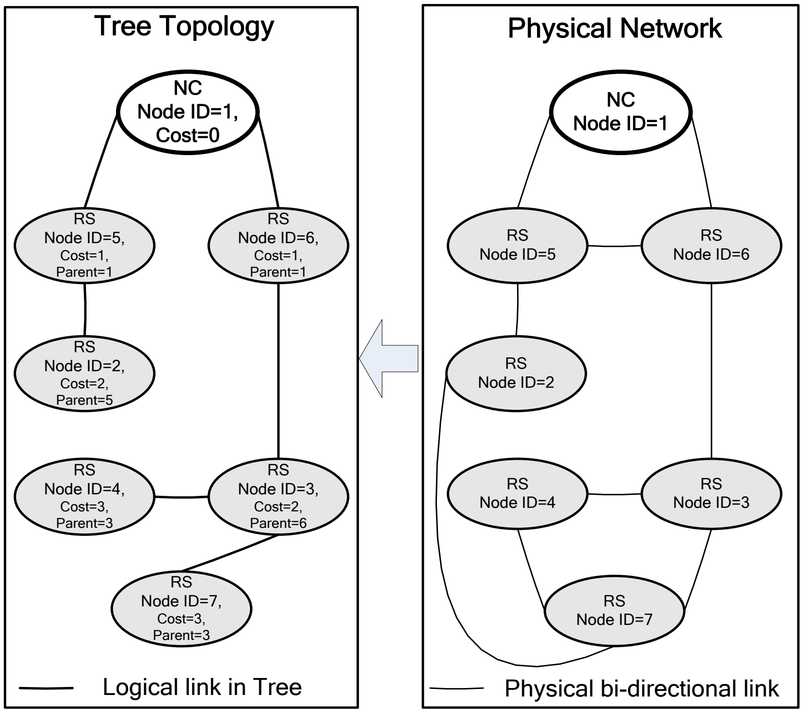
Tree Topology
NC Node ID=1, Cost=0
RS Node ID=5, Cost=1, Parent=1
RS Node ID=6, Cost=1, Parent=1
RS Node ID=2, Cost=2, Parent=5
RS Node ID=4, Cost=3, Parent=3
RS Node ID=3, Cost=2, Parent=6
RS Node ID=7, Cost=3, Parent=3
Logical link in Tree
Physical Network
NC Node ID=1
RS Node ID=5
RS Node ID=6
RS Node ID=2
RS Node ID=4
RS Node ID=3
RS Node ID=7
Physical bi-directional link

Figure 9: Tree Topology Generated from a Graph Representation of a Physical Network

The NL dynamic routing services are as follows:

- **Route Discovery:** Each RS discovers a stable link with a parent that enables to route packets to the NC and vice versa. An optimal link with the parent will be selected based on combined criteria consisting of both minimum number of hops to NC and route robustness.
- **Route Maintenance:**
  - **Parent Link Maintenance:** An RS link with its parent is continuously monitored and maintained. If the link with the parent gets disconnected, the NL attempts to replace the parent with a new one.
  - **RS Route to NC Maintenance:** An RS maintains the route to the NC. If any link on the route to the NC is disconnected, then the RS is notified.
  - **NC Route to RS Maintenance:** The NC maintains active links with the RS. Stale links with the RS and its siblings are marked in the NC source routing database.
  - **Route Optimization:** The route to the NC is continuously optimized by selecting a parent that is closer to the NC than the active parent. The optimized parent will be selected only if the link is found robust for a sufficient period of time.
  - **Internetworking Route Optimization:** In case a potential parent from another network is significantly better than the active parent, the node may switch to the different network (this option can be enabled or disabled based on installer configurations).
  - As the above maintenance processes are performed periodically, the time to resolve disconnections and link optimizations depends on the network size (so that the channel is not overly congested).
- **NC Reset Recovery:** When powered up, the NC retrieves the last known topology from its NVM.

Chapter 5

Host Application

Host applications contain application-level functionality and typically consist of the following (top-down approach):

- Application-specific code (user interface-related functionality, application management and logic).
- Communication protocol between remote applications (used above the Y-Net Stack NL), the application packet structure, payload and parameter preparation for transmission and reception decoding.
- A driver for interfacing with IT900 functions and services that provides the required application functionality in response to IT900 responses to host requests, as well as to significant networking event indications arriving from the IT900 (for example, connections/disconnections to/from the network).
- Host microcontroller's Hardware Abstraction Layer (HAL) modules.

Revision History

Rev	Date	Description
1.0	February 2011	Initial Release

Support and Contact Information

Headquarters: 9 Yehoshua Hatzoref St. Beer Sheva 84106 ISRAEL T +972 8 623 5281 F +972 8 623 5282
yitran@yitran.com