

# **ModFLEX™**

## **FLEXCONNECT™ USER'S GUIDE**



**LS RESEARCH, LLC**  
WIRELESS PRODUCT DEVELOPMENT

Last updated  
March 15<sup>th</sup>, 2012

---

The information in this document is subject to change without notice.

---

## Table of Contents

---

<b>1</b>	<b>Overview .....</b>	<b>3</b>
1.1	<i>Device Types .....</i>	3
1.2	<i>Typical Network Architectures .....</i>	3
<b>2</b>	<b>Using FLEXConnect™ .....</b>	<b>6</b>
2.1	<i>Device Configuration .....</i>	6
2.2	<i>Simple Repeating vs. Source Routing.....</i>	6
2.3	<i>Simple Repeating Overview .....</i>	7
2.4	<i>Source Routing.....</i>	10
<b>3</b>	<b>Configuration.....</b>	<b>15</b>
3.1	<i>Network Variables .....</i>	15
3.2	<i>Device Types .....</i>	15
3.3	<i>Timing Implications.....</i>	15
<b>4</b>	<b>Broadcasting Overview.....</b>	<b>16</b>
4.1	<i>Implications with Timing .....</i>	17
4.2	<i>Broadcasting Repeated Messages to Establish Source Routes.....</i>	17
<b>5</b>	<b>Messaging options .....</b>	<b>20</b>
5.1	<i>Clear Channel Assessment (CCA).....</i>	20
5.2	<i>RF Retries.....</i>	20
5.3	<i>Security/Encryption.....</i>	20
<b>6</b>	<b>Time to Live Overview.....</b>	<b>21</b>
6.1	<i>Calculating Simple Repeating TTL.....</i>	21
6.2	<i>Calculating Source Routed TTL .....</i>	22
<b>7</b>	<b>Encryption .....</b>	<b>23</b>
7.1	<i>Implications with Timing .....</i>	23
7.2	<i>Frame Counter.....</i>	23
7.3	<i>Configuration .....</i>	23
<b>8</b>	<b>Troubleshooting .....</b>	<b>24</b>
8.1	<i>Issues with Basic RF Settings .....</i>	24
8.2	<i>Issues with Repeater Settings.....</i>	24
8.3	<i>Issues with Encryption.....</i>	24
8.4	<i>Firmware Version .....</i>	24
<b>9</b>	<b>Contacting LS Research .....</b>	<b>25</b>

## 1 Overview

Selected ModFLEX™ series modules ship with LSR's FLEXConnect™ firmware. The idea behind FLEXConnect™ is to support applications that require range extension, but don't need the complexities of a full blown mesh network. FLEXConnect™ is comprised of two main features, "Simple Repeating" and "Source Routing". These terms will be explained in further sections.

### 1.1 Device Types

#### 1.1.1 Node

##### Concentrator

A typical system consists of a single concentrator which is the focal point of the network. A Concentrator is the source or sink for all communications within the wireless network. It also is typically the node used to bridge between the wireless and wired infrastructures.

##### End Device

End devices are typically sensors or control devices in the network that do not act as repeaters.

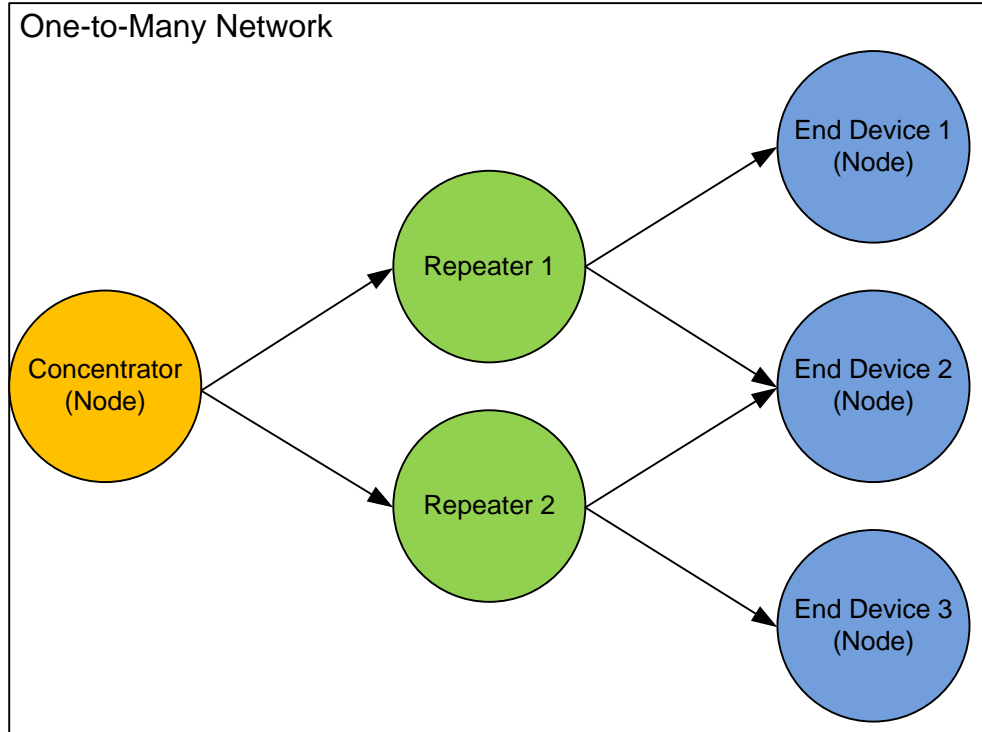
#### 1.1.2 Repeater

Each system can have between 1 and 15 repeaters. Repeaters are enhanced devices in that not only do they support the functions that a node does, but they can also repeat and route messages from other devices within the network.

### 1.2 Typical Network Architectures

The typical applications are suited for **one-to-many** and **many-to-one** architectures. Either architecture allows for data flow in both directions. Both network architectures allow any device to talk to any other device.

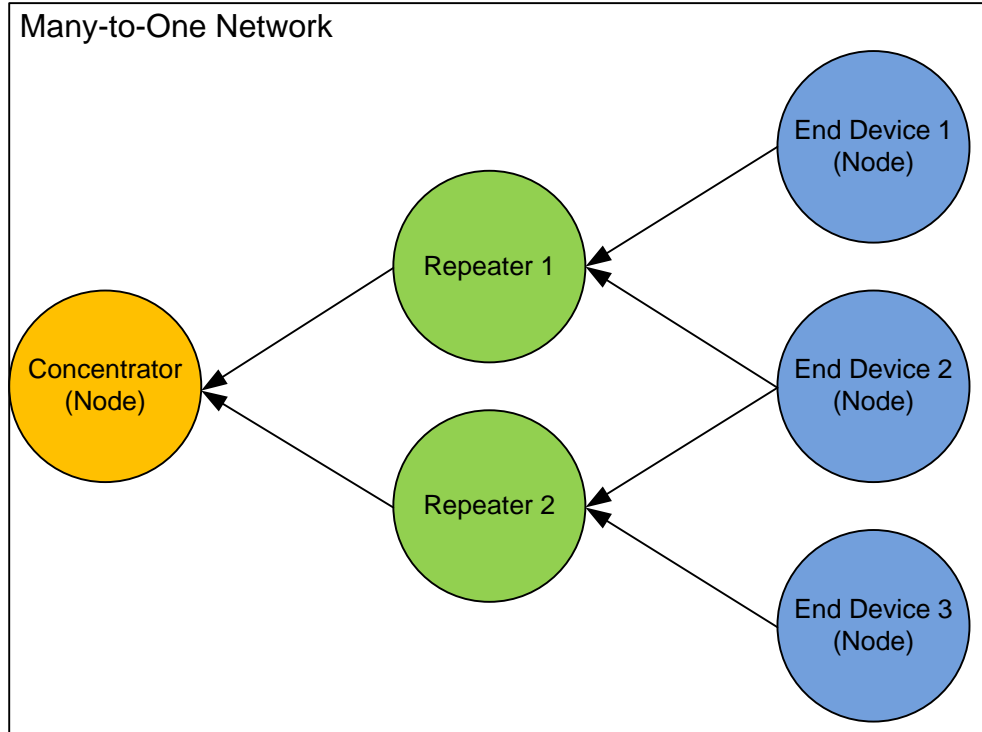
### 1.2.1 One-to-Many Network



**Figure 1 – One-to-Many Network**

Figure 1 depicts a one-to-many network. In a one-to-many network the concentrator commands and/or polls the other nodes in an ordered and coordinated fashion. A destination device can receive a message directly from a concentrator, or through repeaters. Destination devices (repeaters or end devices) respond with an acknowledgement or other data in response to receiving a message from the concentrator.

### 1.2.2 Many-to-One Network



**Figure 2 – Many-to-One Network**

Figure 2 depicts a many-to-one network. In a many-to-one network end devices and repeaters periodically send data to the concentrator. The concentrator can receive a message directly from an end device or repeater, or through repeaters. The destination device (concentrator) responds with an acknowledgement or other data in response to receiving a message from a repeater or end device.

## 2 Using FLEXConnect™

FLEXConnect consists of two types of messages: Simple Repeating and Source Routing. Both Simple Repeating and Source Routing permit any device to transmit a message to any other device. When the destination address of a RF packet matches the address of a device, it will send the packet to its host.

**Configuration of the ModFLEX™ module can be done using the commands in the Host Protocol Document.**

### 2.1 Device Configuration

#### 2.1.1 Addressing

The 802.15.4 standard supports two addressing modes: two-byte short addressing and eight-byte long addressing. When using FLEXConnect™ devices must be configured to use short addressing.

The receive filters must be configured to “Allow Broadcast Addresses” for all devices in the network.

#### 2.1.2 RF Settings

All devices in a FLEXConnect™ network must be configured to be on the same RF channel and same PAN ID. If security is used, the security keys need to be the same.

#### 2.1.3 FLEXConnect™ Configuration

All devices (repeaters and nodes) need to have several parameters configured. These parameters are described in further sections.

### 2.2 Simple Repeating vs. Source Routing

There are advantages and disadvantages to using Simple Repeating or Source Routing. The advantage of using Simple Repeating is that the device that originates the message does not need to know anything about the network except for the short address of the destination device. However this comes at the expense of latency and bandwidth. These tradeoffs are described in subsequent sections. Generally it is advantageous to use Simple Repeating to obtain a list of route(s) between the sender and receiver. Once this route information is obtained, it can be used to send RF messages using Source Routing.

## 2.3 Simple Repeating Overview

With Simple Repeating a device that originates a message can have that message propagated over the network by repeaters. The destination device may receive the message from multiple repeaters.

Simple repeating is deterministic and uses a time-slotted approach to ensure a reliable repeating mechanism. This time-slotted approach comes with the expense of more bandwidth and latency (takes longer to propagate a message).

### 2.3.1 Repeater Rules

There are several rules that the Repeater uses to determine if and when it will repeat the message.

- Repeaters will only send the RF message in the repeat cycle following that which it received it in.
- Repeaters will only repeat a RF message once.
- Repeaters will repeat a RF message within its designated repeater slot.
- Repeaters will only repeat a RF message assuming the maximum number of repeats has not been exceeded.
- Repeaters will only send a message to their host if the destination of the RF message matches the Repeater's address or it's a broadcast. If the message is a broadcast it will repeat the message assuming the maximum number of repeats has not been exceeded.

### 2.3.2 Repeat Slots and Repeat Cycles

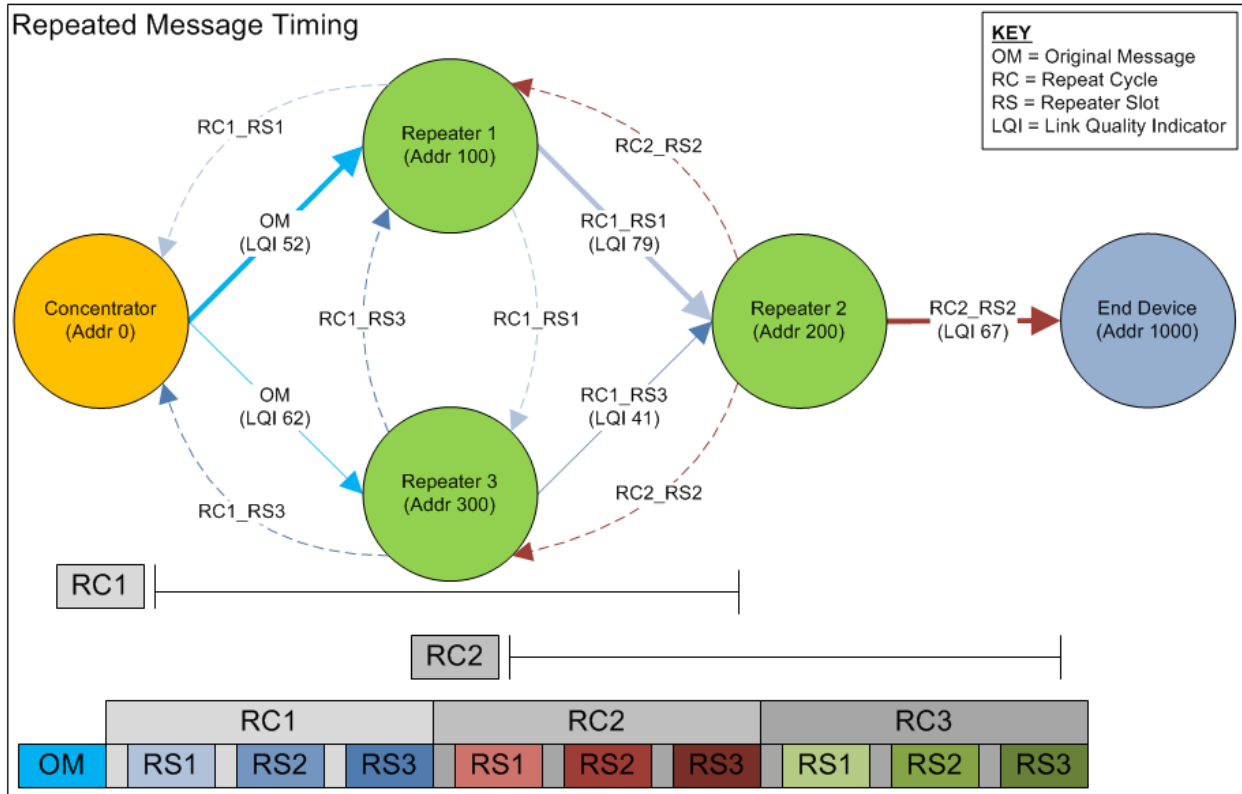
The primary mechanisms behind Simple Repeating are "Repeat Slots" and "Repeat Cycles". The communication is synchronized on a message by message basis. Hence there is no clock or time base being used to keep the network synchronized. The originator of the message establishes the synchronization for that specific message.

**Repeat Slots:** Determined by the Number of Repeaters in the network. The purpose of Repeat Slots is to reserve a unique slot for each repeater. This ensures that repeaters do not talk over one another. It is critical that each repeater be assigned a unique repeater slot. Configuring repeater slots is the responsibility of the end user.

**Repeat Cycles:** Determined by the Maximum Number of Repeats in the network. Each Repeat Cycle consists of the total amount of Repeat Slots, giving each repeater an opportunity to repeat the message.

The module sending the Original Message will not be permitted to send another message until the Time to Live (TTL) has elapsed.

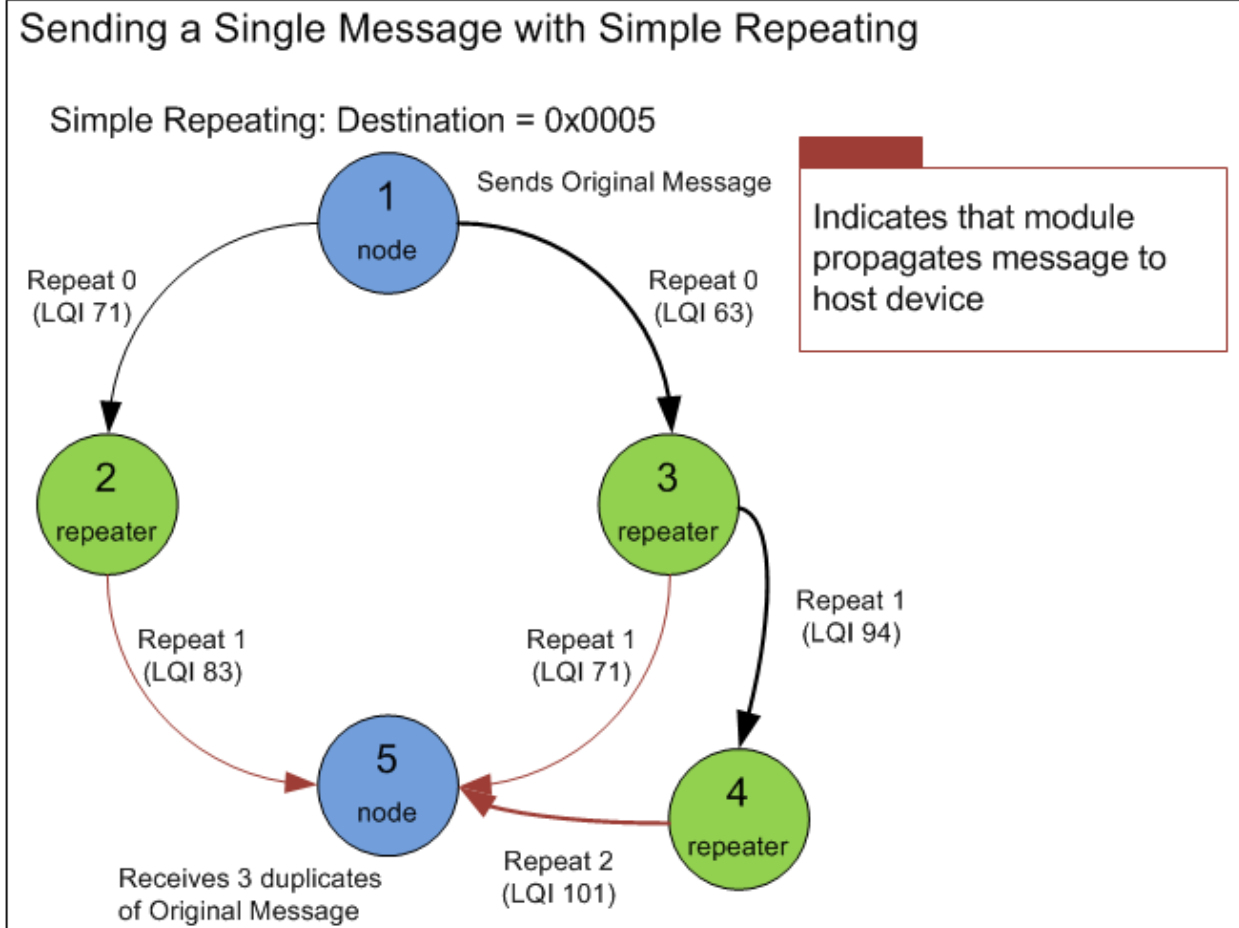
If a repeater receives a data packet with the same **Repeat Count** as its **Repeat Cycle Number** it will not forward the message. Furthermore, if a repeater receives multiple duplicate messages from other repeaters it will repeat the message with the best Link Quality Indicator (LQI). The **Repeat Slot** assigned to each repeater will also determine the order in which a module receives multiple messages.



**Figure 3 – Repeated Message Timing**

Figure 3 depicts a FLEXConnect network in which a Simple Repeated message is transmitted from the Concentrator to an End Device. The Concentrator sends the Original Message which is repeated by Repeaters 1 and 3. Repeater 1 dismisses the repeated message from Repeater 3 because the message's Repeat Count is the same as its Repeat Cycle Number. Repeater 3 dismisses the repeated message from Repeater 1 for the same reason. Repeater 2 receives repeated messages from both Repeater 1 and Repeater 3, but repeats the message from Repeater 1 due to its higher Link Quality Indicator (LQI). Repeaters 1 and 3 receive the repeated message from Repeater 2 but dismiss it because their Repeat Cycle Numbers have been incremented and are now the same as the message's Repeat Count.

When sending Simple Repeated data packets the destination device may receive multiple duplicates of the message. This takes place when the destination transceiver is in a close enough proximity to hear multiple nodes/repeaters, such as in Figure 4:



**Figure 4 – Sending a Single Message with Simple Repeating**

Figure 4 shows a FLEXConnect network where Node 1 sends a message to Node 5, who receives 3 duplicates of the original message due to it being able to “hear” repeaters 2, 3, and 4.

Although Node 5 would receive 3 duplicates of the original message, each data packet would contain a Source Route Address List and Source Route Link Quality Indicator (LQI) List specific to their route of travel:

\*Addresses are 2 bytes and LSB to MSB

1<sup>st</sup> Received Data Packet:

Source Route Address List: [0x0100, 0x0200]

Source Route LQI List: [0x52]

2<sup>nd</sup> Received Data Packet:

Source Route Address List: [0x0100, 0x0300]

Source Route LQI List: [0x47]

3<sup>rd</sup> Data Packet:

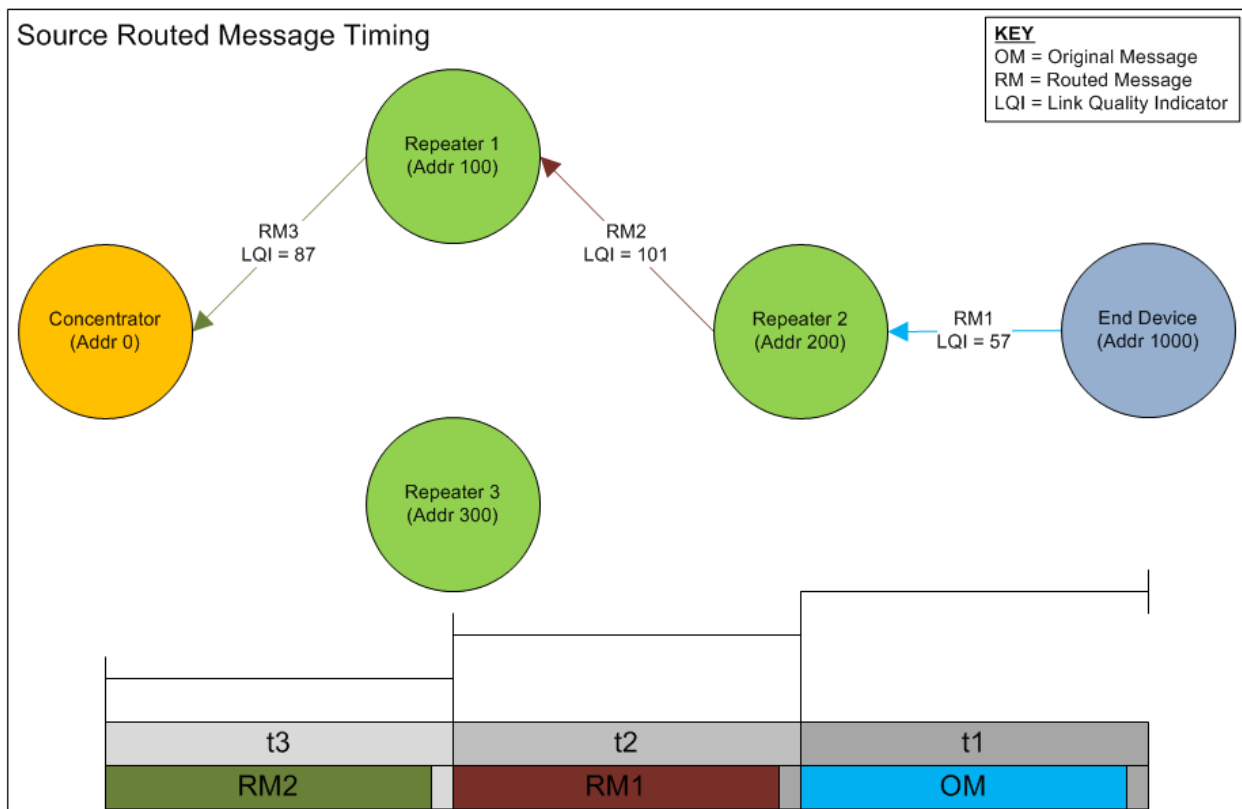
Source Route Address List: [0x0100, 0x0300, 0x0400]

Source Route LQI List: [0x65, 0x5E]

## 2.4 Source Routing

With Source Routing, as with Simple Repeating, any device can transmit a message to any other device. The difference is that the source device specifies the “best” route (as determined by the host controller by using LQI information) the message shall traverse across the Simple Repeating network. Any device receiving a Source Route message forwards the message to the next device in the route list. When a device receives a message wherein the destination address matches its own address, the payload data, route, and LQI information is sent to the host controller.

It is possible and likely that a message may get to a final destination via multiple paths. The application layer software is responsible for choosing which path a message will take when using Source Routing. The benefit of using Source Routing is it increases the available RF bandwidth and throughput.

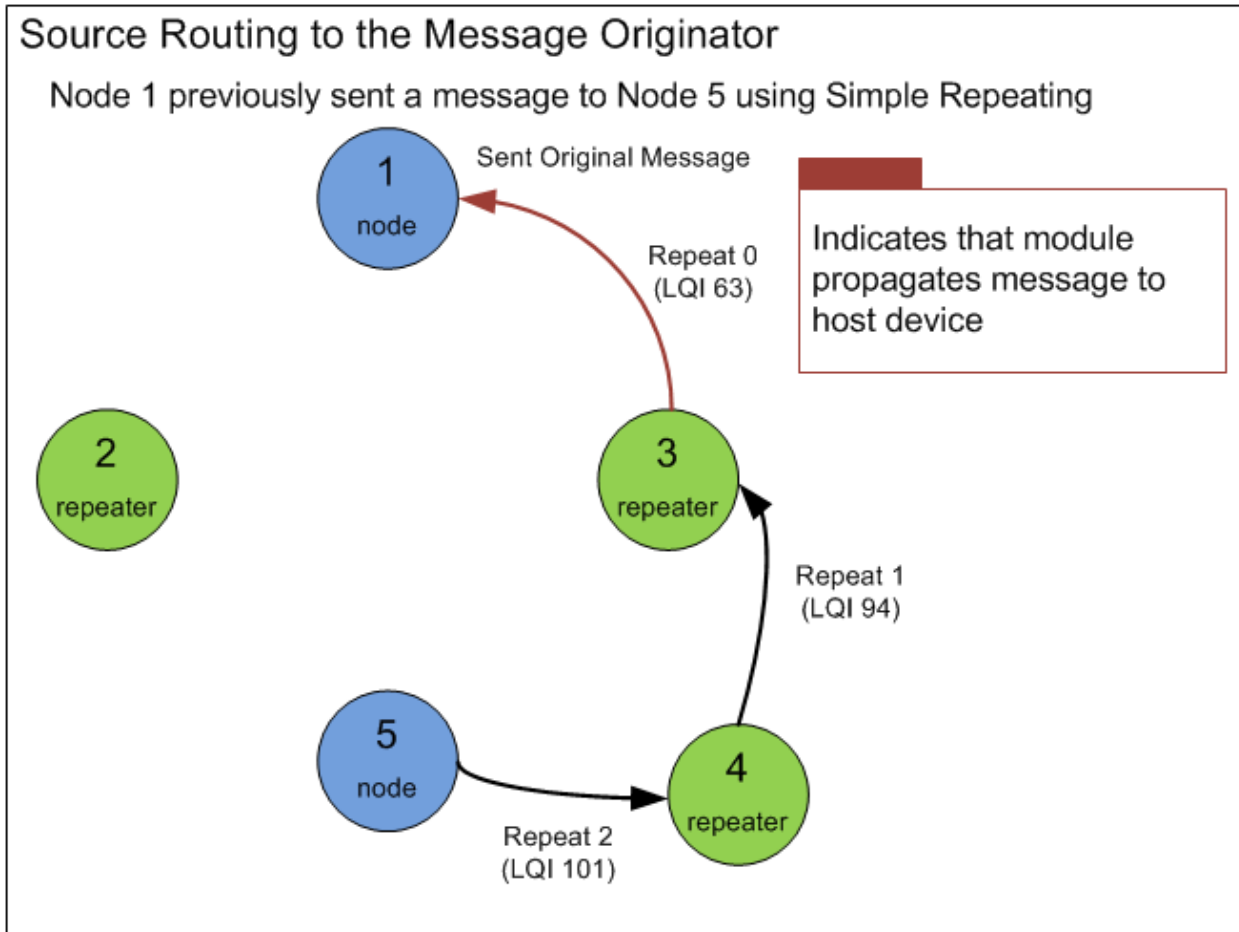


**Figure 5 – Source Routed Message Timing**

Figure 5 depicts a FLEXConnect network in which a Source Routed message is transmitted from an End Device to the Concentrator. The End Device determined the “best” route back to the Concentrator by assessing the LQI information from the various routes in which it received the Simple Repeated message (Figure 3).

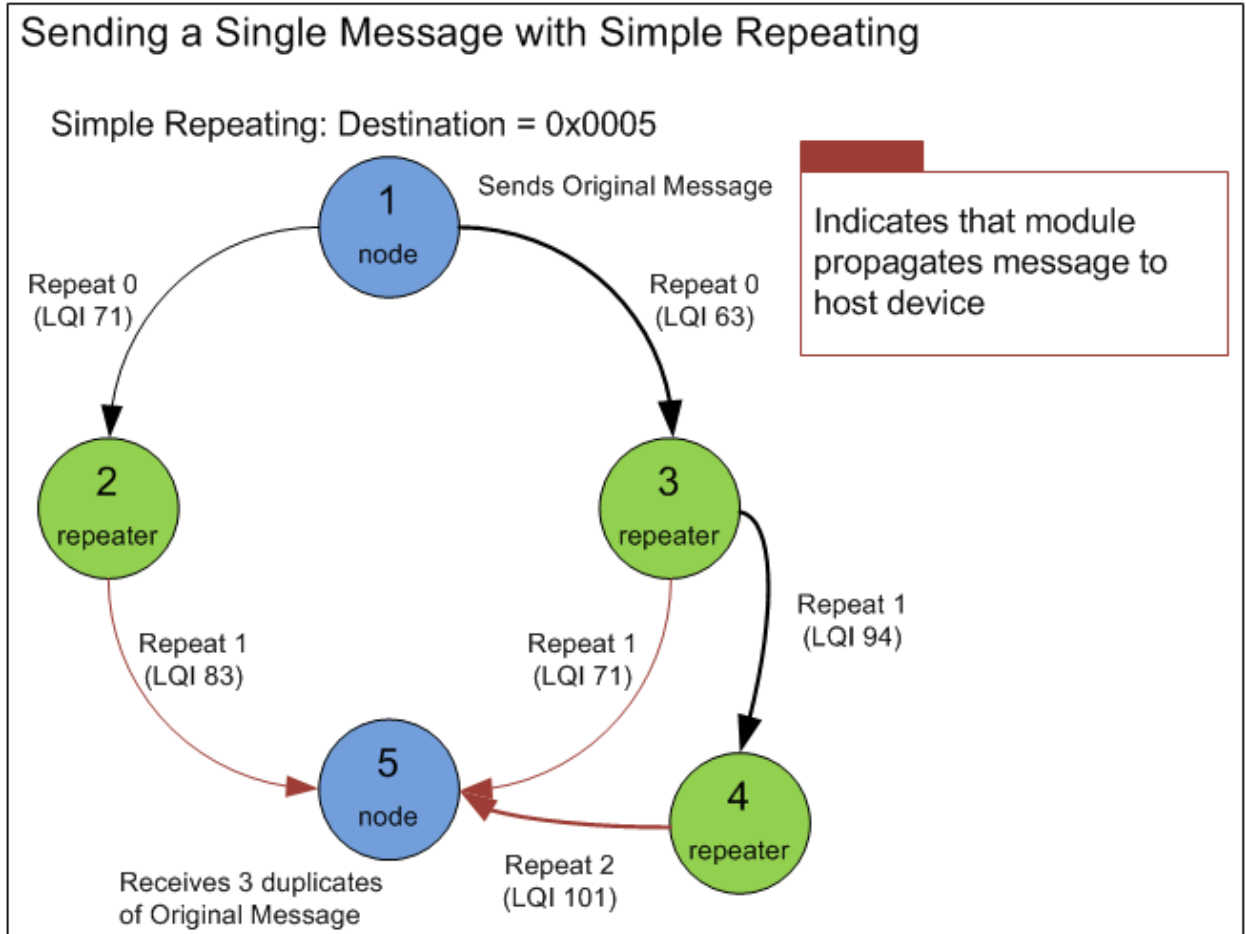
Source Routing makes use of the LQI information to determine the “best” route for the message to traverse the Simple Repeating network. The LQI information is assessed to determine the quality of links between transceivers.

For example, the LQI information portrayed in Figure 6 provides indicators for Node 5's host controller to determine the "best" route to send a message via Source Routing back to the originator, Node 1:



**Figure 6 – Source Routing to the Message Originator**

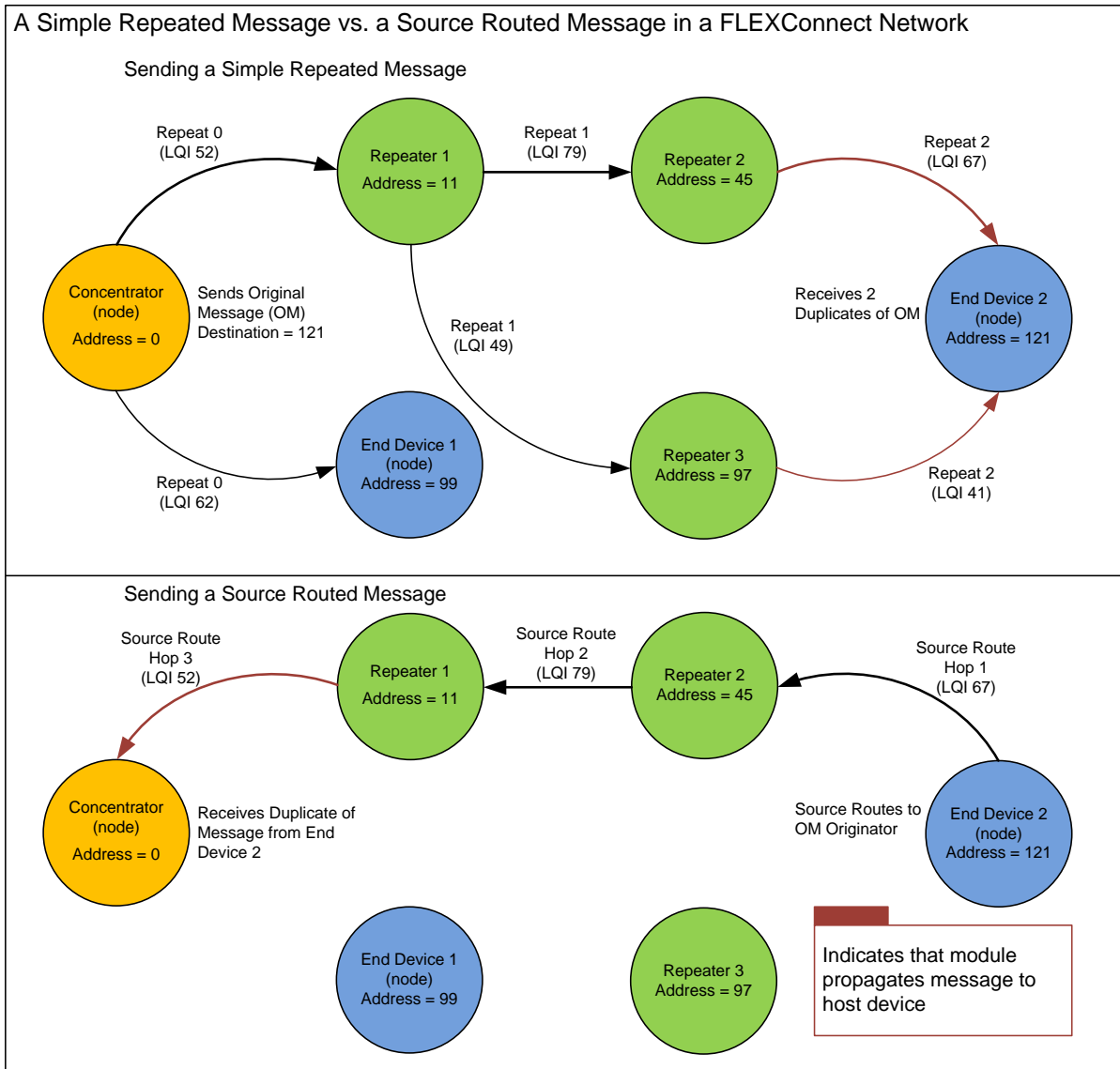
Figure 6 depicts Node 5's host controller assessing the LQI information from



and determining the “best” route back to the originator, Node 1. A Source Route Address List was compiled, and each device that received a Source Route message forwarded that message to the next device in the route list.

When using source routing the host processor duties, in addition to transmitting the original message and receiving it at the destination, include the following:

- Maintaining source route information
- Determining the best route for data packet transmissions
- Filtering duplicate received messages (e.g. from various route paths)
- Other application specific duties



**Figure 7 – Simple Repeated vs. a Source Routed Messaging**

Figure 7 shows the transmission of both a Simple Repeated message and a Source Routed message. For the sending of a Simple Repeated message the concentrator sends the Original Message with a destination address 121. End Device 1 dismisses this, while Repeater 1 propagates the message to Repeaters 2 and 3, which both propagate the message to End Device 2.

For the sending of a Source Routed message, End Device 2's host device assesses the LQI information and determines the route (45, 11, 0) which is the "best".

## 3 Configuration

### 3.1 Network Variables

Prior to using a FLEXConnect™ network, four variables must be configured: **Device Type**, **Max Repeaters**, **Max Repeats**, and **Repeater Slot** (valid only when a module is defined as a Repeater).

- **Device Type:** Repeater or Node
- **Max Repeaters:** 1-15
- **Max Repeats:** 1-7
- **Repeater Slot:** 1-15

All modules in a FLEXConnect network must have the same values for Max Repeaters and Max Repeats. Each repeater must be assigned a unique slot, which needs to be managed by the user.

Address assignments are arbitrary, but each module must have a unique address.

These variables are configured via a serial host command, and it is the responsibility of the Network Manager to properly configure all of the devices.

### 3.2 Device Types

In a FLEXConnect network a module is defined as either a **Node** or **Repeater**.

- **Repeater:** Repeats Simple Repeating packets and routes Source Routed packets.
- **Node:** Does not repeat.

Any module can transmit a message to any other module regardless of it being a Repeater or a Node.

### 3.3 Timing Implications

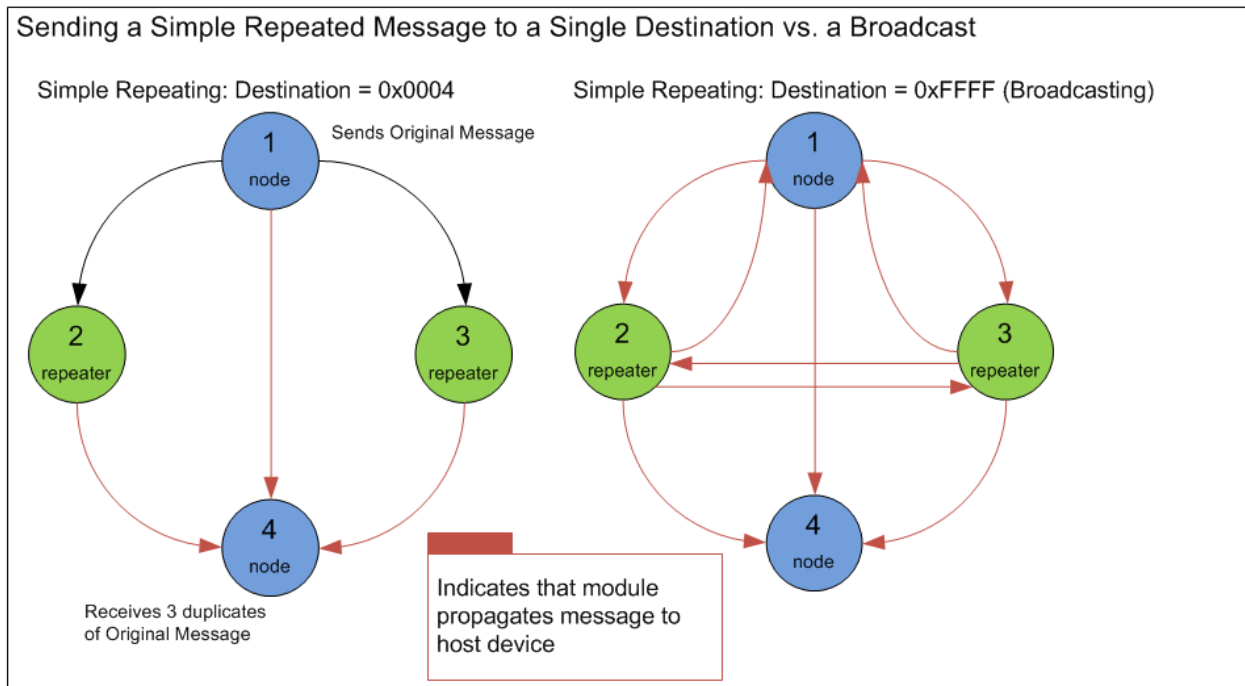
Although increasing the number of Repeaters and Repeats extends the range of the network, it also affects the Time to Live (TTL). The TTL is the amount of time a module must wait after sending a message before it can send another. Increasing the TTL creates latency, ultimately resulting in a lower bandwidth:

- Simple Repeating:  $TTL = ((\text{Max\# of Repeaters} \times \text{Max\# of Repeats}) + 1) \times \text{Slot Time}$
- Source Routing:  $TTL = \text{Slot Time} \times \text{Number of Hops}$

## 4 Broadcasting Overview

A node is capable of broadcasting a message to all host devices by setting its destination address to 0xFFFF. Typically a module only returns the message it received to the host device when the destination address matches its own. The exception is when the destination address is 0xFFFF.

In a repeating system this can result in the host device[s] receiving many copies of the same message. Take into account a FLEXConnect network where all the modules are in close proximity such as Figure 8 below:



**Figure 8 – Sending a Simple Repeated to a Single Destination vs. a Broadcast**

Figure 8 depicts a FLEXConnect network where all the nodes and repeaters are within close proximity. When Node 1 sends a message to a single destination, Node 4, it receives the original message as well as 2 duplicates. When Node 1 broadcasts, all Nodes except Node 1 will receive the original message and all nodes will receive duplicates of the original message.

When broadcasting there will be no acknowledgments (acks) or retries.

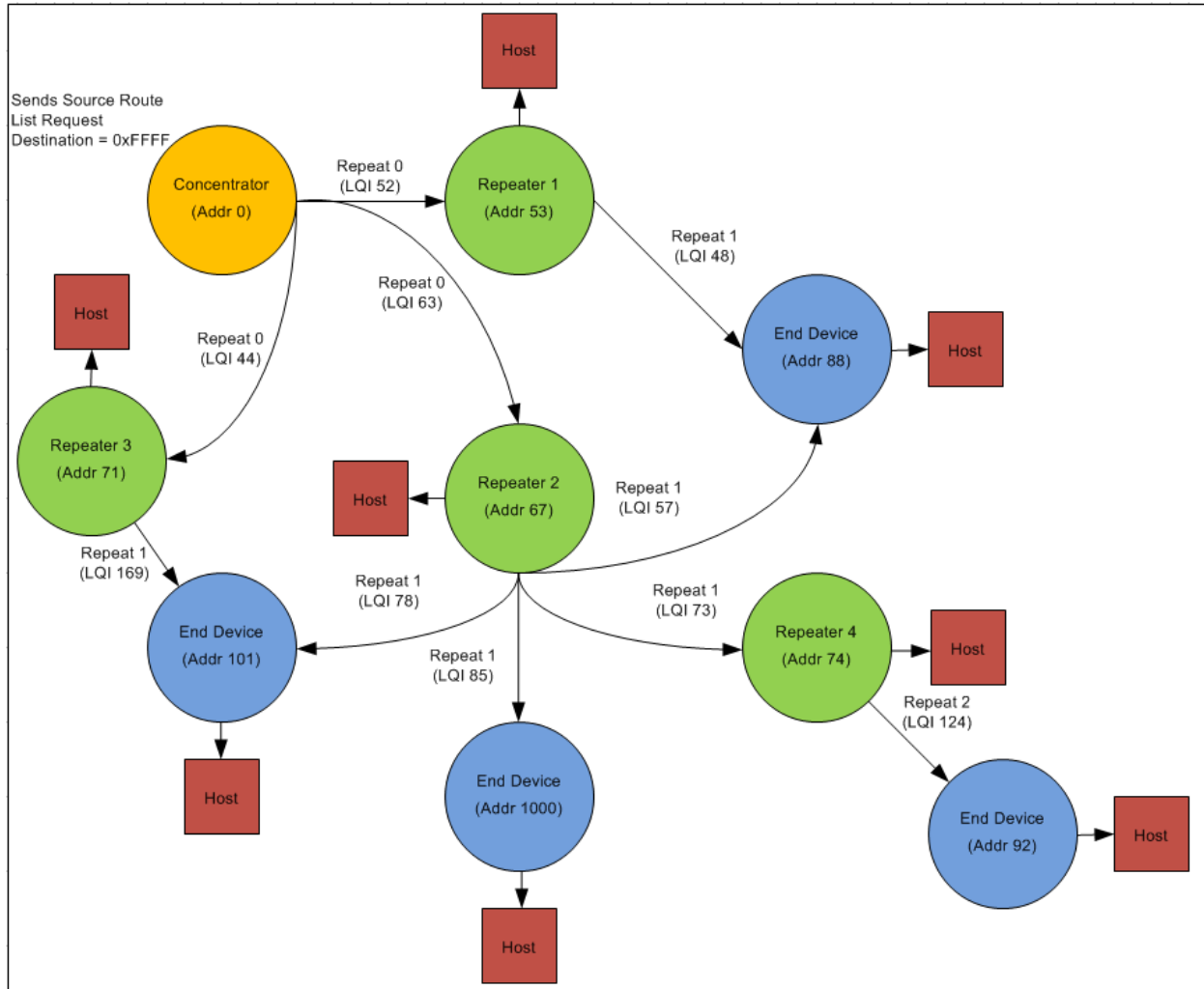
## 4.1 Implications with Timing

Broadcasting a Simple Repeated message will increase the Time to Live (TTL), causing it to take longer for a broadcast message to be sent. When broadcasting, an additional overhead is added onto the Slot Time, which is a variable within the TTL.

$$\text{TTL} = ((\text{Max \# of Repeaters} \times \text{Max \# of Repeats}) + 1) \times \text{Slot Time}$$

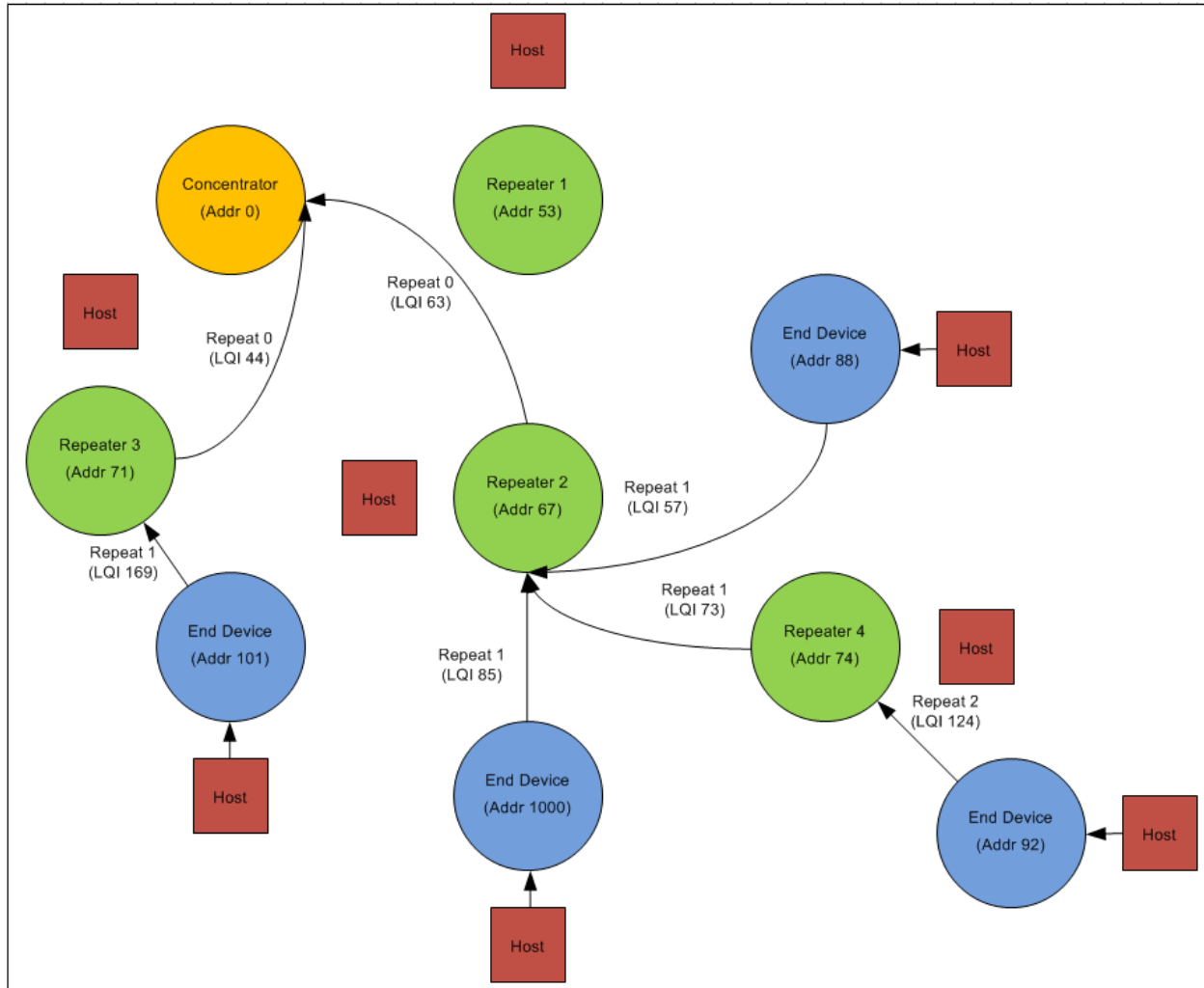
## 4.2 Broadcasting Repeated Messages to Establish Source Routes

It is possible to use broadcasting in a FLEXConnect network in order to get each end device a source route back to the concentrator. This can be accomplished by having the concentrator periodically broadcast a Simple Repeated message. Each device in the network (repeater or node) could then record one or multiple source routes back to the concentrator. Then whenever a device needed to communicate with the concentrator, it would use one of its source routes to send a Source Routed message to the concentrator. In addition the concentrator would receive the Source Routed message from each device, which it could then use to know the route to get back to the device. The concentrator could then keep a table of sources routes for each device in the network. From that point forward the concentrator could use Source Routing to communicate with any device in the FLEXConnect network.



**Figure 9 – Concentrator Broadcasting to Establish Source Routes**

Figure 9 depicts a FLEXConnect network where the concentrator broadcasts a command in order to get each end device to Source Route its Source Route List back to itself.



**Figure 10 – End Devices Source Routing back to the Concentrator**

Figure 10 depicts end devices in a FLEXConnect network Source Routing back to the concentrator. The concentrator would then build a table that has a source route back to each end device in the network.

## 5 Messaging options

### 5.1 Clear Channel Assessment (CCA)

Clear Channel Assessment or CCA is a messaging option used to minimize RF crosstalk. When CCA is enabled the module listens for RF energy on the channel prior to transmitting a message. The device will not send a data packet until the background energy is below a certain threshold.

Enabling CCA will increase the Guard Band Time on each slot, which increases the TTL, ultimately increasing the amount of time it takes to send a message.

CCA is not applicable when sending Simple Repeated Messages.

### 5.2 RF Retries

RF retries is a mechanism that helps to ensure that a data packet reaches its destination. When RF retries are enabled, if a module sends a data packet and does not receive an RF ack, it will retry sending the data packet up to 3 more times. The use of RF retries also increases the Slot Time, which results in it taking longer to send a data packet.

Retries are not applicable for Simple Repeated messaging, but come in to play with Source Routed messaging.

Due to a hardware limitation, the disabling of CCA prevents the use of RF acks and retries in the SiFLEX02 module.

### 5.3 Security/Encryption

Security can be added to RF packets by enabling AES encryption. When encryption is enabled an additional 14 bytes of overhead gets added to each packet. This reduces the maximum amount of payload data by 14 bytes as well.

The use of security/encryption on RF packets adds additional overhead and reduces the maximum amount of payload bytes by 14.

For a more in depth description see the Encryption section.

## 6 Time to Live Overview

Time to Live (TTL) is a calculated value used to prevent another message from being transmitted until the current message has finished propagating. Table 1 depicts the variables that TTL is based upon:

TTL Variables	Simple Repeating	Source Routed
Security Enabled	X	X
Data Rate	X	X
Maximum Number Repeaters In System	X	
Maximum Number Repeats Allowed	X	
Number Bytes To Be Sent	X	X
CCA		X
Retries		X
Number Hops		X

Table 1 – Variables which affect Time To Live

### 6.1 Calculating Simple Repeating TTL

$$\text{TTL} = ((\text{Max\# of Repeaters} \times \text{Max\# of Repeats}) + 1) \times \text{Slot Time}$$

$$\text{Slot Time} = ((\text{Mac OH} + \text{LSR OH} + \text{Security OH} + \text{Payload Length}) \times (8 \text{ bits per byte} / \text{Data Rate})) + (\text{Guard Band Time})$$

- OH = Overhead
- Mac OH (bytes) = 17
- SiFLEX02 LSR OH (bytes) = 7 + ((Max# of Repeats + 1) x 3)
- ProFLEX01 LSR OH (bytes) = 6 + ((Max# of Repeats + 1) x 3)
- Security OH (bytes) = 14 (if security is used)
- Payload Length in units of bytes
- Data Rate is the RF data rate in bits per second
  - SiFLEX02: 40kbps, 250kbps, or 1Mbps
  - ProFLEX01: 250kbps
- SiFLEX02 Guard Band Time = 2550usec
- ProFLEX01 Guard Band Time = 2224usec
- Guard Time is a fixed value within the hardware
- When broadcasting an additional 4 msec is added onto the Slot Time

## 6.2 Calculating Source Routed TTL

TTL = Slot Time x Number of Hops

\*Note that if Retries are enabled the TTL is doubled.

Slot Time = Guard Band Time + Transmit Time

Transmit Time = ((Mac OH + LSR OH + Security OH + Payload) x (8 bits per byte / Data Rate))

- OH = Overhead
- Mac OH (bytes) = 17
- SiFLEX02 LSR OH (bytes) = 6 + (Number of Hops x 3)
- ProFLEX01 LSR OH (bytes) = 5 + (Number of Hops x 3)
- Security OH (bytes) = 14 (if security is used)
- Payload Length in units of bytes
- Data Rate is the RF data rate in bits per second  
     SiFLEX02: 40kbps, 250kbps, or 1Mbps  
     ProFLEX01: 250kbps

### 6.2.1 Source Routed Guard Band Time

CCA Disabled	Retries Enabled	Guard Band Time (msec)	Guard Band Time (msec)	Guard Band Time (msec)
		40kbps Data Rate	250kbps Data Rate	1Mbps Data Rate
		5.20	3.64	3.78
X		1.40	1.40	1.54
	X	6.44	4.21	4.50

**Table 2 – SiFLEX02 Guard Band Time**

\*If the CCA is disabled on the SiFLEX02 Retries cannot be enabled.

CCA Disabled	Retries Enabled	Guard Band Time (msec)
		3.43
	X	3.74
X		1.51
X	X	1.82

**Table 3 – ProFLEX01 Guard Band Time**

## 7 Encryption

Using encryption results in adding 14 bytes of additional packet overhead. This reduces the maximum payload length by 14 bytes, and increases the amount of time it takes to send a message.

### 7.1 Implications with Timing

Encryption increases the amount of time it takes to send a data packet due to the addition of 14 overhead bytes. Adding 14 bytes to the data packet length increases the Slot Time by  $14/\text{Data-Rate}$  (ms). This also increases the Time to Live (TTL), which increases the overall time before being able to send another data packet.

- Simple Repeating:  $\text{TTL} = ((\text{Max\# of Repeaters} \times \text{Max\# of Repeats}) + 1) \times \text{Slot Time}$
- Source Routing:  $\text{TTL} = \text{Slot Time} \times \text{Number of Hops}$

### 7.2 Frame Counter

In order to use encryption the Frame Counter must be utilized in order to prevent replay attacks. The concept behind the Frame Counter is to insure sequential freshness of each new message that is received. The module receiving a new incoming message needs to check that the received Frame Counter is larger than that of the last received message. Frame Counter management is the user's responsibility, but here are a couple recommendations.

- Each device should have a frame counter that gets incremented each time a new RF message is transmitted.
- The host processor should keep a table which consists of a device ID and the last received frame count. The table needs to be as large as the number of devices it communicates with.
- Upon receiving an encrypted message, the host processor should compare the newly received frame count to that which is stored in the table for that particular device. If the "new" frame count is larger than the "last received" frame count, then the message can be processed. The "new" frame count value should be updated into the frame counter table.
- While the frame counter is a 4 byte value, it will eventually roll over and a mechanism needs to be in place to handle such an event. The reason for this is that when a rollover occurs, the "new" frame count will be less than the "last received" frame count.

### 7.3 Configuration

Serial host commands must be issued to do the following:

- *Receiver Configuration Receive Filters* must allow the use of security.
- The *Options* byte in any of the *Send Data Packet Commands* must be set to use security.
- All modules within the secure network must have the same *Security Key*.

## 8 Troubleshooting

If your FLEXConnect network is not operating correctly, following is a list of subjects that may be causing your device[s] to not work properly.

### 8.1 Issues with Basic RF Settings

- Address: Make sure that all modules are assigned a unique address, and that those addresses are short (two byte) address.
- Personal Area Network ID: Every module must have the same Personal Area Network (PAN) ID in order to communicate.
- RF Channel: All modules must be on the same RF Channel.
- RF Data Rate: All modules must have the same RF Data Rate. This only applies to the SiFLEX02 module.
- Host Serial Baud Rate: Higher host data rates should be used to prevent running out of buffers and missing data packets.

### 8.2 Issues with Repeater Settings

- Max Number of Repeaters: The maximum number of repeaters must be set to the same value for all modules within the FLEXConnect network.
- Max Number of Repeats Allowed: The maximum number of repeats must be set to the same value for all modules within the FLEXConnect network.
- Repeater Slot: Each repeater within the Simple Repeating network must have a unique slot number assigned to it. This only applies to devices which are configured as repeaters.
- Time to Live (TTL): If a device is prompted to send a data packet via a serial host command, and nothing happens (other devices don't receive the message and a host ack is not sent back from the module), there may be a TTL issue. The TTL begins counting down after a data packet is sent. Until this time elapses the module will not send another data packet. This is to ensure a data packet is propagated across the network before trying to send another. Use either the LSR ModFLEX Test Tool Suite or the TTL Calculator to determine what your TTL is. Then you can determine whether or not you are trying to send another message too quickly.

### 8.3 Issues with Encryption

- Security Key: All modules must have the same Security Key.
- Allow Secured Packets: All modules must be enabled to accept secured Data Packets.
- Secured Data Packet: Data Packets must be set to be secured.

### 8.4 Firmware Version

Modules may not be able to communicate correctly because their firmware versions differ. Query the firmware version of the modules and make sure that they are all the same.

## 9 Contacting LS Research

<b>Headquarters</b>	LS Research, LLC W66 N220 Commerce Court Cedarburg, WI 53012-2636 USA Tel: 1(262) 375-4400 Fax: 1(262) 375-4248
<b>Website</b>	<a href="http://www.lsr.com">www.lsr.com</a>
<b>Wiki</b>	<a href="http://wiki.lsr.com">wiki.lsr.com</a>
<b>Technical Support</b>	<a href="http://forum.lsr.com">forum.lsr.com</a>
<b>Sales Contact</b>	<a href="mailto:sales@lsr.com">sales@lsr.com</a>

The information in this document is provided in connection with LS Research (hereafter referred to as "LSR") products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of LSR products. EXCEPT AS SET FORTH IN LSR'S TERMS AND CONDITIONS OF SALE LOCATED ON LSR'S WEB SITE, LSR ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL LSR BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF LSR HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. LSR makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. LSR does not make any commitment to update the information contained herein. Unless specifically provided otherwise, LSR products are not suitable for, and shall not be used in, automotive applications. LSR's products are not intended, authorized, or warranted for use as components in applications intended to support or sustain life.

---

The information in this document is subject to change without notice.