



Digi Cellular Application Guide

Using Digi Surelink

Introduction

Digi's SureLink is a mechanism to help maintain persistent wireless connections. It contains four main components:

1. Mobile Link Rx Inactivity Timer
2. SureLink Settings - Hardware Reset Thresholds
3. SureLink Settings - Link Integrity Monitoring
4. iDigi Connection Keep-alive Settings (used with an iDigi server connection, see <http://www.idigi.com> for more information)

Once the Digi cellular device is provisioned and configured for its wireless plane, it will immediately attempt connection to the cellular network upon initial boot. And, if for any reason the connection is dropped, the Digi firmware will immediately attempt to reconnect and will continue to do so as long as it is powered up and in a sane state.

The following items add a level of robustness above and beyond this basic functionality. More information is available in Digi manuals and embedded WebUI help screens.

1. Inactivity Timer

Wireless networks will normally terminate a mobile PPP session after a set time period of inactivity. This period ranges anywhere from 30 minutes to 4 hours. This is a problem if the session is dropped and an application needs to contact the mobile IP address. The Inactivity Timer will proactively bring down and then re-establish the mobile PPP connection before the carrier network does; thus refreshing the carrier's inactivity timer. This ensures the Digi device is available to the application immediately.

By default this session time is one hour (3600 secs) and can be adjusted via the **Configuration > Mobile > Mobile Connection Setting**:

▼ Mobile Settings

Select the service provider, service plan, and connection settings used in connecting to the mobile network.
These settings are provided by and can be retrieved from the service provider.

Mobile Service Provider Settings

Service Provider:

Mobile Connection Settings

Re-establish connection when no data is received for a period of time.
Inactivity timeout: seconds



Digi Cellular Application Guide

Using Digi Surelink

2. SureLink Settings - Hardware Reset Thresholds

Hardware reset thresholds will proactively reset the embedded cellular modem (mobile interface) or the entire Digi device if the device fails to connect for any reason. This adds an extra level of robustness to the connection attempts.

These settings are available via **Configuration > Mobile > SureLink**

▼ **SureLink Settings**

SureLink™ provides an "always-on" mobile network connection to ensure rapid on-demand communication. The configuration settings below allow you to customize how SureLink detects when a connection has been lost, in order to re-establish the link.

Hardware Reset Thresholds

The SureLink Hardware Reset Thresholds are observed if a problem occurs while initializing and establishing the mobile data connection. Please refer to the SureLink help section for additional information.

Hard reset the mobile interface after the following number of consecutive failed connections.
 (1-255)

Reboot the device after the following number of consecutive failed connections.
 (1-255)

By default, the mobile interface reset is set to 3 failed attempts. i.e. the internal modem is “power cycled” if the mobile connection is not established after 3 attempts.

The “Reboot device” option, where the whole Digi device is reset, is off by default. This should be enabled if devices fail to reconnect without being rebooted. A rule-of-thumb setting is 8 attempts.

3. Link Integrity Monitoring

Link Integrity Monitoring will send a small amount of data to a host(s) to test the integrity of the wireless connection. If this setting is enabled, the other Link Integrity Monitoring settings may be configured and are used to verify the functional integrity of the mobile connection. The default is OFF.

Three different tests are available for selection:

1. Ping Test
2. TCP Connection Test
3. DNS Lookup Test

Each of these tests can be used to demonstrate two-way communication is working over the mobile connection. This variety of tests is provided because different mobile networks or firewalls may allow or block Internet packets for various services. The appropriate test may be selected according to mobile network constraints and user preference.

The link integrity tests are performed only while the mobile connection is established. If the mobile connection is disconnected, the link integrity tests are suspended until the connection is established again.



Digi Cellular Application Guide

Using Digi Surelink

For the link integrity tests to provide meaningful results, the remote or target hosts must be accessible over the mobile connection and not through the LAN interface of the device (if it has one). That is, the settings should be configured to guarantee that the mobile connection is actually being tested.

The link integrity test settings may be modified at any time. The changes are used at the start of the next test interval.

Link Integrity Monitoring

The SureLink Link Integrity Monitoring tests are performed only while the mobile network connection is established, and when the tests are enabled in these settings.

Enable Link Integrity Monitoring using the test method selected below.

Ping Test
Verifies that a valid reply is received for a ping request sent to the following:
Primary Address:
Secondary Address:

TCP Connection Test
Verifies that a TCP connection can be established with the following:
TCP Port:
Primary Address:
Secondary Address:

DNS Lookup Test
Verifies that a DNS reply is received when requesting a DNS lookup of the following:
Primary DNS Name:
Secondary DNS Name:

Repeat the selected link integrity test every: seconds (10-65535)

Test only when idle: if no data is received for the above period of time.

Reset the link after the following number of consecutive link integrity test failures.
 (1-255)

Ping Test

The test is successful if a valid ping reply is received in response to the ping request sent. The ping test actually sends up to three ping requests, at five second intervals, to test the link. When a valid reply is received, the test completes successfully and immediately. If a reply is received for the first request sent, there is no need to send the other two requests.

Two destination hosts may be configured for this test. If the first host fails to reply to all three ping requests, the same test is attempted to the second host. If neither host replies to any of the ping requests sent, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.

- Primary Address: First host to test
- Secondary Address: Second host to test (if the first host fails)



TCP Connection Test

Enables or disables the creation of a TCP connection as a test to verify the integrity of the mobile connection. The test is successful if a TCP connection is established to a specified remote host and port number. If the remote host actively refuses the connection request, the test is also considered to be successful, since that demonstrates successful two-way communication over the mobile connection. The TCP connection test waits up to 30 seconds for the connection to be established or refused. When the TCP connection is established, the test completes successfully, and the TCP connection is closed immediately.

Two destination hosts may be configured for this test. If the first host fails to establish (or refuse) the TCP connection, the same test is attempted to the second host. If neither host successfully establishes (or refuses) the TCP connection, the test fails. The primary and secondary addresses may be either IP addresses or fully qualified domain names.

- TCP Port: The TCP port number to connect to on the remote host (default 80)
- Primary Address: First host to test
- Secondary Address: Second host to test (if the first host fails)

DNS Lookup Test

Enables or disables the use of a Domain Name Server (DNS) lookup as a test to verify the integrity of the mobile connection. The test is successful if a valid reply is received from a DNS server. Typically, this means the hostname is successfully "resolved" to an IP address by a DNS server. But even a reply such as "not found" or "name does not exist" is acceptable as a successful test result, since that demonstrates successful two-way communication over the mobile connection. When a valid reply is received, the test completes successfully and immediately.

The DNS servers used in this test for the hostname lookup are the primary and secondary DNS servers obtained from the mobile network when the mobile PPP connection is first established. These addresses may be viewed in your web browser on the **Administration | System Information | Mobile page**.

Note that this DNS test is independent of the normal DNS client configuration and lookup cache, which is used for other hostname lookups. This test has been specifically designed to require communication over the mobile connection for each lookup, and to avoid being "short-circuited" by previously cached information. Also, this test does not interfere in any way with the normal DNS client configuration of this device.



Digi Cellular Application Guide

Using Digi Surelink

Two hostnames may be configured for this test. If the first hostname fails to get a reply, the same test is attempted for the second hostname. If no reply is received for either hostname, the test fails. The primary and secondary DNS names should be fully qualified domain names. Note that the reverse lookup of an IP address is possible, but that is usually unlikely to succeed in returning a name. Still, such a reverse lookup can be used to demonstrate the integrity of the mobile connection.

- Primary DNS Name: First hostname to look up
- Secondary DNS Name: Second hostname to look up (if the first hostname fails)

Repeat the selected link integrity test every N seconds

A new test will be started every N seconds while the mobile connection is established. This value must be between 10 and 65535. The default is 240.

If the configured interval is less time than it takes a test to complete, the next test will not be initiated until the previous (current) test has completed.

Test only when idle: if no data is received for the above period of time

Initiate the selected link integrity test only after no data has been received for the specified interval of time. This changes the behavior of the test in that the test interval varies according to the presence of other data received from the mobile connection.

Although using this idle option may result in less data being exchanged over the mobile connection, it also prevents the link integrity tests from running as often to verify the true bi-directional state of that connection.

Reset the link after the following number of consecutive link integrity test failures

This specifies that after the configured number of consecutive link integrity test failures, the mobile connection should be disconnected and reestablished. This value must be between 1 and 255. The default is 3. When the mobile connection is reestablished, the "consecutive failures" counter is reset to zero.

Note: if the mobile connection is disconnected for any reason (including not as a result of a link integrity test failure), the consecutive failures count is reset to zero when the mobile connection is reestablished.



Digi Cellular Application Guide

Using Digi Surelink

4. iDigi Connection Keep-Alive Settings

The iDigi Device Cloud is the intelligent platform choice for today's and tomorrow's device application solutions within any industry.

If the Digi device is configured for Device-initiated iDigi Connection, it will initiate a TCP connection to the iDigi cloud server. A periodic “keep-alive” or heart-beat message is sent from the device to the server to update the iDigi server on its current status.

This small amount of traffic (typically about 160-170 bytes) will refresh the carrier’s inactivity timer, thus helping maintain the persistent wireless connection. The keep-alive period is by default 15 minutes, but can be changed according to need.

Accessing the iDigi Connection Settings is done via **Configuration>iDigi**.
By default, new devices will automatically point to developer.idigi.com.

▼ Connection Settings

Device-Initiated iDigi Connection

Enable Device-Initiated iDigi Connection
iDigi Server Address:

Automatically reconnect to iDigi after being disconnected
Reconnect after: hrs mins secs

Server-Initiated iDigi Connection

Enable Server-Initiated iDigi Connection

Enable Device IP Address updates to the following server
iDigi Server Address:

Retry if the IP Address update fails
Retry after: hrs mins secs



Digi Cellular Application Guide

Using Digi Surelink

Keep-alive intervals are changed via Advance Settings:

Connection Settings:

Disconnect when the iDigi Connection is idle
Idle Timeout: hrs mins secs

Authenticate to iDigi with a password
Password:

Mobile (Cellular) Settings:

iDigi Connection Keep-Alive Settings:
Device Send Interval: secs Server Send Interval: secs
Assume connection is lost after: timeouts

Connection Method: For iDigi service, must be TCP or SSL.

HTTP over Proxy Settings (optional):
Hostname: Username:
TCP Port: Password:
 Enable persistent proxy connections

Ethernet Settings:

iDigi Connection Keep-Alive Settings:
Device Send Interval: secs Server Send Interval: secs
Assume connection is lost after: timeouts

Connection Method: For iDigi service, must be TCP or SSL.

HTTP over Proxy Settings (optional):
Hostname: Username:
TCP Port: Password:
 Enable persistent proxy connections

For more information about iDigi and how to remotely configure and manage devices, please visit www.idigi.com.

5. More Information

See the Digi's WebUI built-in help. Look for the “ Help” in the upper-right corner of the WebUI screen. More documentation and support are available at www.digi.com/support