Click to prove you're human

This page describes the configuration of the Semtech Basic Station on the MultiTech mPower class of Gateway. Prefer a video walkthrough? On boarding a MultiTech Conduit AP using the Netmoregroup Developer Portal and configuring the Gateway as a Semtech Basic Station is outlined from a Developer perspective on YouTube: System Requirements MultiTech provides a wide variety of models for the Conduit platform. Most of these models are variations based on network connectivity and operating system (OS); as such if you do not see your model listed, it is highly likely these instructions are still applicable. Warning To use Basic Station a supported Gateway with a MTAC-LORA-H mCard is required. The (deprecated) USB variety of MCAT-LORA-1.0 accessory cards are no longer supported. Model OS Type OS Version MultiConnect Conduit mPower (AEP) 5.3.0+ MultiConnect Conduit AP mPower (AEP) 5.3.0+ MultiConnect Conduit IP67 mPower (AEP) 5.3.0+ Prerequisites Verify Version Compatibility Ensure your Gateway is running mPower Software version 5.3.0 or greater to take advantage of the Configuration Web interface and included Basic Station software. It is recommended to upgrade to the latest mPower Software version before continuing. MultiTech mPower Software upgrade instructions are available at: Determine the MultiTech Conduit Serial Number The Serial Number is 8-Digits and found on the bottom of the Conduit Gateway labeled Serial #. Note The Serial Number can also be found in the Configuration Web interface under Home > Device > Serial Number. Determine the MultiTech Conduit Manufacturer EUI The Manufacturer EUI is 16-Digits and found on the bottom of the Conduit Gateway labeled LoRa Node. Note The Manufacturer EUI can also be found in the Configuration Web interface under Home > Lora > EUI. Security Check As a basic security precaution, we ask that you change the default password of the Gateway to ensure basic security protection. For more information, please refer to the documentation that came with your Gateway Registration on the Netmoregroup network If you have not done so already you will need to register your gateway through your Developer or RAN Provider account. 1. Enter the 8-Digit Serial Number. 2. Enter the 16-Digit Manufacturer (Lora Node) EUI. 3. Complete the registration process by filling in the remaining fields. Note The Gateway supports a maximum of 8 channels at any given time. During registration you will have a chance to select which sub-band of 8 RX Channels the Gateway should operate on to start. Tip: After registration is complete, you can use the Netmoregroup Portal to reconfigure the RX Channel sub-band without the need to login to the Configuration web interface. Semtech Basic Station Configuration Navigate to the Conduit mPower Web Interface. By default the address will be 192.168.2.1. Select LoRaWAN > Network Settings. Select BASIC STATION from the LoRa Mode dropdown menu. A section Basic Station Configuration will appear. In the Credentials dropdown menu select LNS. The Station Config can be left at the default values. Netmoregroup LNS URI The Netmoregroup LNS URI value can be configured in two different ways: 1. Secured (recommended) 2. Unsecured Secured LNS URI (Secured) 1. Enter wss://ns-gw.netmoregroup.com:6042 as the URI value. 2. A copy of the Netmoregroup Server Certificate (tc.trust) can be downloaded directly from: Netmoregroup TLS Server Certificate 3. Extract the contents from the Certificate, or copy the value below, into the Server Cert menu entry box. Netmoregroup LNS URI (Unsecured) 1. Enter ws://ns-gw.netmoregroup.com:6040 as the URI value. 2. A copy of the Netmoregroup Server Certificate (tc.trust) is not required. 3. Leave the Server Cert menu entry box empty. Finishing Up 1. The Gateway Cert menu entry box can be left empty. 2. The Gateway Key menu entry box can be left empty. 3. Click Submit 4. Click Save and Apply Verifying Connection to the Netmoregroup Network Upon successful completion, the Gateway status will update to Registered - Active. (this may require a refresh of the browser) To start configuring your conduit connect a computer to its LAN interface and open a browser to . This opens the login dialog for the configuration interface of the conduit. If it is your first time configuring the conduit, you will be prompted to create a username and password. First-Time Setup Wizard # After login (be patient, it takes a while) the First-Time Setup Wizard opens: Click Next to begin. Choose Password # The first step it to change the current default password (admin): Keep your new password in a safe place, you will have to reset to factory defaults if you lose it! Time Configuration # Select your time zone and update both date and time if required. Click Next to proceed. Internet Configuration # Set the Mode to DHCP Client if you use DHCP on your network (most likely) or manually configure your internet connection. Click Finish once you are done. If you changed the IP Address or selected DHCP a popup will appear warning you that the DHCP Server of the Conduit itself will be disabled. This is fine, so click OK to continue. Before you continue, verify that the Conduit AEP runs Firmware 5.3 or later. This is displayed in the header of the web interface. If it is out-dated, follow the instructions to upgrade to the latest version. Access & Network Configuration # As the LAN interfaces do not allow specifying a DNS server and we need DNS to work later on we will now change to network to WAN. However as this would lock us out we need to allow remote access for the management first. Skip this step if you are using a cellular modem to connect the gateway to the internet. Just configure the cellular modem per instructions on the MultiTech website. Access Configuration # In the left hand menu choose Administration followed by Access Configuration: On the next screen tick the boxes marked yellow in the next screenshot: When you select Via WAN under HTTPS a warning will appear. Just click Continue. Once you have selected the 3 checkboxes, click Submit to save the changes. Network Interfaces # Select Setup > Network Interfaces from the left menu: In the next screen select the pencil in the eth0 row: In the configuration popup change the Type from LAN to WAN. If you use a static IP, fill out the gateway and DNS entries. Use 8.8.8.8 for Google’s public DNS if you do not have (or know) the local DNS server information. Click Finish to save. Now select Save and Restart from the menu: You will be prompted to confirm the restart. Choose OK to proceed. Disconnect the temporary network cable and connect the Conduit to the target network while it is restarting. TTN Configuration # Once the Conduit has finished restarting and is connected to the target network, connect a computer to the same network and login to the Conduit by entering its IP in a browser. If you have not configured your Conduit with a static IP, you will have to find out which IP the DHCP assigned to it. Click the LoRaWAN tab on the left. In the Mode dropdown, choose Basic Station. Select LNS in the Credentials dropdown. See the Basics Station guide for the Server Certificate and Server Address. After entering the LNS configuration, click the Submit button, and then click Save and Apply. The gateway will apply the changes. Note: TC_TIMEOUT was included in early versions of station.conf examples. The value was set to “2s” which is too low for some cellular networks causing the MUXS connection to timeout after receiving the LNS URI configuration. This setting has been removed from the examples as it should not be needed, the default values will work for all networks. There is no benefit of a low timeout value other than for testing the timeout code is functioning. Hardware Requirements To use basic station an MTCAP or MTCDT with MTAC-LORA-H mCard is required. The Basic Station does not support the MTAC-LORA-1.0 USB cards. mPower 5.3 includes UI configuration and basic station packages Configuration Requirements Internet Access through Ethernet, Cellular or WiFi DNS access to resolve host names Updated system time using GPS or SNTP Connecting to Actility TLS certs and keys will be downloaded from Actility when Basic Station connects. These files need to be stored in persistent FLASH to be restored after reboot. The firmware mPower 6.3.2 or greater is needed to persist these files. There is a known issue with mPower 6.3.1 where some of these files were being overwritten on reboot. Connecting to TTN TTN Basic Station Instructions for Conduit Logging The JSON station configuration file has options to enable logging files, level and rotation The following settings can be used for maximum debugging and rely on the system logrotate process to correctly rotate and gzip files. The Basic Station built-in rotate mechanism does not keep a chronological record over multiple rotate files or compress rotated logs. "log_file": "/var/log/lora-station.log", "log_level": "XDEBUG", "log_size": 1000000, "log_rotate": 0, GPS PPS Settings On MTCDT, MTCAP and MTCAP3 units without GPS hardware can disable PPS sync to reduce log messages for failed timesync with PPS. { "SX1301_conf": { "lorawan_public": true, "clksrc": 0, "pps": false, Antenna Gain Antenna gain can be configured for radio_0 if a different antenna is used. A default value of +3 dBi is used in mPower. For US915 the current implementation of Basic Station will fix the transmit power to +26 dBm, however this is interpreted as an EIRP value by Basic Station leading to a TX power lower than the maximum allowed for the hardware. To work-around the antenna_gain can be set to 0 or -1 to reach the maximum TX power of the gateway hardware of 26 or 27 dBm conducted. Setting to -4 will then attempt to transmit at the US902-928 regional limit +30, the hardware TX power tables only go up to a certified maximum which will be selected by the software. The -4 antenna gain setting will work on a variety of gateways that may support max transmit of 26, 27 or 28 dBm conducted power depending on the model. A lower transmit power can lead to missed ACK to end-devices at the edge distance of the range of the current datarate. i.e. Any spreading factor used at a low margin threshold may not be able to receive an ACK in certain circumstances. US915 uplink(125KHz)/downlink(500KHz) have a 5 dBm link budget difference so a power at least 5 dBm higher than the end-device transmit is theoretically needed to reach the same distance. End-device transmit around +21/22 dBm EIRP then needing gateway power of +26/27 dBm EIRP for the same distance. So with the default settings the transmit power is just at the theoretical boundary. With a lower RX sensitivity at the end-device a higher gateway power may have some benefit. The LNS basic station connects to can set a maximum gateway power, it will only affect the gateway configuration if lower than the default tx power setting. Therefore this cannot be adjusted higher by the LNS for gateways in the field. Antenna gain can only be set in the station.conf at the gateway. { "radio_0": { /* freq/enable provided by LNS - only HW specific settings listed here */ "type": "SX1257", "rssi_offset": -166.0, "tx_enable": true, "antenna_gain": -4 }, Beaconing Settings Beaconing parameters should come from the LNS. Since the gateway is configured at the LNS for a specific channel plan, the LNS should be setting the gateway beacon. TTN supports basic station beaconing since 2022. Beacon settings can be provided by the LNS in the router_config message. The bcning field is either None or a BCNCONF object with the following layout: { "DR" : INT "layout": [INT,INT,INT] "freqs": [INT, ..] } The layout field specifies the octet offsets for insertion of the message fields Time and GwSpecific, followed by the length of the beacon PDU. // Pack parameters into a BEACON pdu with the following layout: // | 0-n | 4 | 2 | 1 | 3 | 3 | 0-n | 2 | bytes – all fields little endian // | RFU | epoch_secs | CRC | infoDesc | lat | lon | RFU | CRC | // void s2e_make_beacon (uint8_t* layout, sL_t epoch_secs, int infodesc, double lat, double lon, uint8_t* pdu) { int time_off = layout[0]; int infodesc_off = layout[1]; int bcn_len = layout[2]; Beacon Frame Format is found in the LoRaWAN 1.0.4 Specification LoRaWAN® 1.0.4 Specification Package Layout settings for each spreading factor: SF8 – [1, 7, 19] SF9 – [2, 8, 17] SF10 – [3, 9, 19] SF11 – [4, 10, 21] SF12 – [5, 11, 23] Credentials Select LNS or CUPS depending on server requirements. The LNS protocol will downlink the channel plan from a server. The CUPS protocol and redirect the station process to a network server end-point. Connecting to TTN Community v3 TTN Instructions Certificate Information CUPS Use the following command to view the certificate used by the server. openssl s_client -showcerts -servername eu1.cloud.thethings.industries -connect eu1.cloud.thethings.industries:443 TTN Server Cert Info Using CUPS requires creating two API keys for your gateway. The LNS lbs-lns-secret key will be sent to the gateway over the CUPS protocol. The CUPS key will authenticate the gateway when negotiating the CUPS connection. Creating API keys for CUPS URI Set the URI field to point to a network, in this example a TTI private instance is used. Connecting to TTN Community Replace “nam1” with “au1”, “eu1” for the desired region. wss://nam1.cloud.thethings.network:8887 Station Conf The default station configuration can be used as the network will configure the channels based on the selected channel plan in the TTI configuration. Server Certificate TTN Community certificates Replace “nam1” with “au1” or “eu1” for the desired region. openssl s_client -showcerts -servername nam1.cloud.thethings.network -connect nam1.cloud.thethings.network:8887 Use the second certificate output by the open ssl command Gateway Certificate If a TLS client cert is required to connect to the server provide a certificate. Otherwise leave this field blank for connecting to TTN v3. Gateway Key The Gateway Key can be used to populate the authorization header field or be a TLS client key depending on connection method. The Gateway Key needs to be formatted correctly to be used. In The Things Industries v3 GUI, create an API Key with Link as Gateway permissions and copy the key to the text box preceded by “Authorization: ” Creating the Gateway key for LNS Authorization: NNSXS.XXXXXXXXXXXXXXXXXXXXXX.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX TTN Community gateway key Currently the TTN Community servers to not authenticate the gateway key. Any value can be set, the file needs have proper contents to allow parsing by the basic station daemon. Authorization: NNSXS.XXXXXXXXXXXXXXXXXXXXXX.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX Click Save and Apply and the station will be started. Duty-cycle, listen-before-talk (LBT/CCA), and dwell-time Basic Station enables LBT for AS923-1 by default, see ccaEnabled is set in the region configuration. See region name “AS923-1 (CCA)” in the logs and LBT is enabled for 8 channels. If the gateway does not have FPGA v33 or v35 installed the concentrator fails to start with the LBT settings. 2024-06-18 03:44:29.475 [AIO:XDEB] [4|WS] < {"msgtype":"router_config","NetID":null,"JoinEui":null,"region":"AS923","hwspec":"sx1301/1","freq_range":[920000000,923400000],"DRs":[[12,125,0],[11,125,0],[10,125,0], [9,125,0],[8,125,0],[7,125,0],[7,250,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0],[0,0,0]],"sx1301_conf":[{"radio_0":{"enable":true,"freq":923000000},"radio_1": {"enable":true,"freq":9221000 00},"chan_multiSF_0":{"enable":true,"radio":0,"if":200000},"chan_multiSF_1":{"enable 2024-06-18 03:44:29.475 [AIO:XDEB] [4|WS] . ":true,"radio":0,"if":400000},"chan_multiSF_2":{"enable":true,"radio":1,"if":100000},"chan_multiSF_3":{"enable":true,"radio":1,"if":300000},"chan_multiSF_4":{"enable": true,"radio":0,"if":-400000},"chan_multiSF_5":{"enable":true,"radio":0,"if":-200000},"chan_multiSF_6":{"enable":true,"radio":0,"if":0},"chan_multiSF_7":{"enable":true,"radio":1,"if":0,"bandwidth":250000,"spread_factor":7},"chan_FSK":{"enabl 2024-06-18 03:44:29.475 [AIO:XDEB] [4|WS] . e":true,"radio":1,"if":-300000,"datarate":50000}}],"MuxTime":1718682269.2040114,"bcning":{"DR":3,"layout":[2,8,17],"freqs":[923400000]}} ... 2024-06-18 03:44:29.215 [S2E:INFO] Configuring for region: AS923-1 (CCA) -- 920.0MHz..923.4MHz ... 2024-06-18 03:44:29.216 [S2E:INFO] Dev/test settings: nocca=0 nodc=0 nodwell=0 ... 2024-06-18 03:44:29.694 [S00:INFO] SX130x LBT enabled: rssi_target=-80 rssi_offset=0 2024-06-18 03:44:29.694 [S00:INFO] 0: freq=923.2MHz scan=5000us 2024-06-18 03:44:29.696 [S00:INFO] 1: freq=923.4MHz scan=5000us 2024-06-18 03:44:29.697 [S00:INFO] 2: freq=922.2MHz scan=5000us 2024-06-18 03:44:29.699 [S00:INFO] 3: freq=922.4MHz scan=5000us 2024-06-18 03:44:29.700 [S00:INFO] 4: freq=922.6MHz scan=5000us 2024-06-18 03:44:29.700 [S00:INFO] 5: freq=922.8MHz scan=5000us 2024-06-18 03:44:29.701 [S00:INFO] 6: freq=923.0MHz scan=5000us 2024-06-18 03:44:29.701 [S00:INFO] 7: freq=922.0MHz scan=5000us INFO: FPGA supported features: [TX filter] [Spectral Scan] 2024-06-18 03:44:30.291 [S00:ERRO] Concentrator start failed: lgw_start The network can send nocca, nodc, and nodwell settings in the router config, The basic station source repo does not enable them for production builds. We have changed the in mPower 6.3.4 to allow these settings from the LNS or in the configuration file. In mPower 6.3.4 we added the option to set nocca=0 nodc=0 nodwell=0 in the station.conf. This will override the default cca settings in the region and settings sent from the LNS router_config message. Add nocca to the station_conf section of the Station Config. The options for nodc and nodwell can be set as well. "station_conf": { "TC_TIMEOUT": "20s", "euiprefix": "::0", "log_file": "/var/log/lora-station.log", "log_level": "XDEBUG", "log_rotate": 0, "log_size": 1000000, "routerid": "", "nocca": true } Now the station will start with nocca enabled and LBT settings will not be used. 2024-06-27 12:40:42.697 [S2E:INFO] Dev/test settings: nocca=1 nodc=0 nodwell=0 Troubleshooting If there are issues and the station needs to be run manually, you can ssh into the gateway and issue these commands to see output. The station.conf logging feature can also be used to get messages to find any issue details. $ /etc/init.d/lora-networks-server stop $ cd /var/run/lora/1 $ sudo ./station With persistent config enabled, additional files are downloaded when the station connects to the server. The station process is run within the /var/config directory so files maintained by the station will be saved. $ /etc/init.d/lora-networks-server stop $ cd /var/config/lora/1 $ sudo ./station Installation on MTCDT/MTCAP Install the Basic Station from downloads. $ sudo -s # wget # opkg install lora-basic-station_2.0.3-r1.0_arm926ejste.ipk The /opt/lora/station binary will be installed. Basic Station to Packet Forwarder This example python script shows how to send a channel configuration to the connection basic station gateway. It is useful for getting started and ensuring the gateway is functioning. Basic Station Examples TTI Configuration The Things Industries provide private server instances that Basic Station can connect to. Visit TTI for details. tc.uri wss://..cloud.thethings.industries:8887 wss://multitech.eu1.cloud.thethings.industries:8887 tc.key – Gateway Token The tc.key file needs to be formatted correctly to be used and can be created with this command. In The Things Industries v3 GUI, create an API Key with Link as Gateway permissions and copy the key to the tc.key file. echo -en "Authorization: NNSXS.XXXXXXXXXXXXXXXXXXXXXX.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX\r" > tc.key tc.trust Use the following command to view the certificate used by the server. openssl s_client -showcerts -servername multitech.eu1.cloud.thethings.industries -connect multitech.eu1.cloud.thethings.industries:8887 Configuration files Adjust the station.conf file for the desired frequencies, see examples.Download station.confUse the routerid and euiprefix fields to assign the Gateway EUI. See Basic Station Doc for EUI. Configure tc.uri to point to the network server web socket port ws://192.168.52.72:6090 For secure web sockets use wss and provide tc.key or tc.trust and tc.crt files wss://192.168.52.72:6090 Running the Basic Station root@mtcdt:/opt/lora$ sudo ./station 2020-02-26 16:56:02.698 [SYS:WARN] Ignoring field: region 2020-02-26 16:56:02.700 [SYS:INFO] Logging : stderr (maxsize=10000000, rotate=3) 2020-02-26 16:56:02.700 [SYS:INFO] Station Ver : 2.0.3(mlinux/std) 2020-01-24 16:54:44 2020-02-26 16:56:02.700 [SYS:INFO] Package Ver : (null) 2020-02-26 16:56:02.701 [SYS:INFO] proto EUI : ::1 (station.conf) 2020-02-26 16:56:02.701 [SYS:INFO] prefix EUI : ::0 (station.conf) 2020-02-26 16:56:02.701 [SYS:INFO] Station EUI : ::1 2020-02-26 16:56:02.701 [SYS:INFO] Station home: ./ (builtin) 2020-02-26 16:56:02.701 [SYS:INFO] Station temp: /var/tmp/ (builtin) 2020-02-26 16:56:02.701 [SYS:WARN] Station in NO-CUPS mode 2020-02-26 16:56:02.903 [TCE:INFO] Starting TC engine 2020-02-26 16:56:02.908 [TCE:INFO] Connecting to INFOS: ws://192.168.52.72:6090 2020-02-26 16:56:02.912 [TCE:INFO] Infos: ::1 muxs-::0 ws://192.168.52.72:6092/router-::1 2020-02-26 16:56:02.912 [AIO:DEBU] [3] ws_close reason=1000 2020-02-26 16:56:02.913 [AIO:DEBU] [3] Server sent close: reason=1000 2020-02-26 16:56:02.913 [AIO:DEBU] [3] WS connection shutdown... 2020-02-26 16:56:02.916 [TCE:VERB] Connecting to MUXS... 2020-02-26 16:56:02.917 [TCE:VERB] Connected to MUXS. INFO: FPGA supported features: [TX filter] [Spectral Scan] [LBT] 2020-02-26 16:56:03.219 [S2E:WARN] Unknown field in router_config - ignored: bcning (0x1EE5E245) 2020-02-26 16:56:03.219 [S2E:WARN] Unknown field in router_config - ignored: config (0xF7A3E35F) 2020-02-26 16:56:03.219 [S2E:WARN] Unknown field in router_config - ignored: protocol (0xFD309030) 2020-02-26 16:56:03.220 [S2E:WARN] Unknown field in router_config - ignored: regionid (0xE6FFB211) 2020-02-26 16:56:03.220 [S2E:WARN] Unknown field in router_config - ignored: upchannels (0x7FCAA9EB) 2020-02-26 23:08:46.995 [RAL:WARN] Ignoring unsupported/unknown field: lbt_conf 2020-02-26 23:08:47.049 [RAL:INFO] Lora gateway library version: Version: 5.0.1-mts-1; 2020-02-26 23:08:47.049 [RAL:DEBU] SX1301 txlut table (2 entries) 2020-02-26 23:08:47.049 [RAL:VERB] SX1301 txlut 0: dig_gain=0 pa_gain=0 dac_gain=3 mix_gain=11 rf_power=-6 2020-02-26 23:08:47.049 [RAL:VERB] SX1301 txlut 1: dig_gain=0 pa_gain=0 dac_gain=3 mix_gain=13 rf_power=-3 2020-02-26 23:08:47.049 [RAL:VERB] SX1301 rxrfchain 0: enable=1 freq=868475000 rssi_offset=-162.000000 type=2 tx_enable=1 tx_notch_freq=0 2020-02-26 23:08:47.049 [RAL:VERB] SX1301 rxrfchain 1: enable=1 freq=869287500 rssi_offset=-162.000000 type=2 tx_enable=0 tx_notch_freq=0 2020-02-26 23:08:47.049 [RAL:VERB] SX1301 ifchain 0: enable=1 rf_chain=0 freq=-375000 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 1: enable=1 rf_chain=0 freq=-175000 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 2: enable=1 rf_chain=0 freq=25000 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 3: enable=1 rf_chain=0 freq=375000 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 4: enable=1 rf_chain=1 freq=-237500 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 5: enable=1 rf_chain=1 freq=237500 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 6: enable=0 rf_chain=1 freq=200000 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 7: enable=0 rf_chain=1 freq=400000 bandwidth=0 datarate=0 sync_word=0/0 2020-02-26 23:08:47.050 [RAL:VERB] SX1301 ifchain 8: enable=0 rf_chain=0 freq=-200000 bandwidth=2 datarate=2 sync_word=0/0 2020-02-26 23:08:47.051 [RAL:VERB] SX1301 ifchain 9: enable=0 rf_chain=0 freq=300000 bandwidth=3 datarate=50000 sync_word=0/0 2020-02-26 23:08:47.051 [RAL:VERB] SX1301 LBT not enabled 2020-02-26 23:08:47.051 [RAL:INFO] Station device: /dev/spidev0.0 (PPS capture enabled) 2020-02-26 23:08:50.049 [S2E:INFO] Configuring for region: EU863 -- 863.0MHz..870.0MHz 2020-02-26 23:08:50.049 [S2E:VERB] DR0 SF12/BW125 2020-02-26 23:08:50.049 [S2E:VERB] DR1 SF11/BW125 2020-02-26 23:08:50.049 [S2E:VERB] DR2 SF10/BW125 2020-02-26 23:08:50.049 [S2E:VERB] DR3 SF9/BW125 2020-02-26 23:08:50.049 [S2E:VERB] DR4 SF8/BW125 2020-02-26 23:08:50.049 [S2E:VERB] DR5 SF7/BW125 2020-02-26 23:08:50.049 [S2E:VERB] DR6 SF7/BW250 2020-02-26 23:08:50.049 [S2E:VERB] DR7 FSK 2020-02-26 23:08:50.049 [S2E:VERB] DR8 undefined 2020-02-26 23:08:50.049 [S2E:VERB] DR9 undefined 2020-02-26 23:08:50.049 [S2E:VERB] DR10 undefined 2020-02-26 23:08:50.049 [S2E:VERB] DR11 undefined 2020-02-26 23:08:50.050 [S2E:VERB] DR12 undefined 2020-02-26 23:08:50.050 [S2E:VERB] DR13 undefined 2020-02-26 23:08:50.050 [S2E:VERB] DR14 undefined 2020-02-26 23:08:50.050 [S2E:VERB] DR15 undefined 2020-02-26 23:08:50.050 [S2E:VERB] TX power: 16.0 dBm EIRP 2020-02-26 23:08:50.050 [S2E:VERB] 27.0 dBm EIRP for 869.4MHz..869.65MHz 2020-02-26 23:08:50.050 [S2E:VERB] JoinEui list: 0 entries 2020-02-26 23:08:50.050 [S2E:VERB] NetID filter: FFFFFFFF-FFFFFFFF-FFFFFFFF-FFFFFFFF 2020-02-26 23:08:50.050 [S2E:VERB] Dev/test settings: nocca=0 nodc=0 nodwell=0 Use the LoRa Network Server Configuration settings for the LoRa networking configured on the Conduit. When LoRa is enabled, the Conduit acts as a network server allowing end-points to join with the correct credentials on the correct frequency and sub-band. Configured LoRa for either the 915 frequency band (NAM), or the 868 frequency band (EU). For NAM, the 915 band allows 8 sub-bands. For the EU, the 868 band has three default channels and five configurable channels. Use the TX Power setting to control the gateway’s transmission power. The Rx 1 DR Offset and RX 2 Datarate are sent with a join response to configure the data rates used for receive windows. The offset is applied to the upstream data rate for reception on the first window. For more information about setting up a LoRa network on a Conduit AEP, go to Getting Started with LoRa Conduit AEP (LoRa Configuration) LoRa Configuration The LoRa Configuration pane contains the configuration values for the LoRa network server that acts as a gateway for the LoRa endpoint devices. Item Default Value Description Enabled Checked (enabled) Enable the LoRa network server. Public Unchecked (disabled) Enable public compatibility mode: changes the join response time from 1 to 5 seconds and the sync word from 0×12 to 0×34 Frequency Band 915 (US) Frequency band to use. Values are 915 (US) or 868 (EU). Lease Time (dd-hh-mm) 60-00-00 (60 days) Amount of time until a successful join expires. Frequency Sub-Band 1 For US only, 8 sub-bands are available. Additional ChannelsFrequency (MHz) 869.5 MHz For EU only, center the frequency to configure five additional 125 kHz channels at 200 kHz spacing. Network ID Name Name of the network that the network server supports or the EUI of the network. Tx Power (dBm) 26 Transmit power of the Conduit. Value range is from 1 to 26. Name Model-SerialNumber Editable name of network used to generate EUI. EUI Blank Editable EUI of network. Rx 1 DR Offset 0 Offset applied to upstream data rate for downstream data rate on first receive window. Network Key Passphrase Passphrase used to join the network or network key. Rx 2 Datarate 12 Data rate to use for second receive window. Passphrase Blank Arbitrary textual passphrase used to generate network key. Key Blank 128-bit AES key used to generate session keys. Address Range Start 00:00:00:01 Start address to assign to OTA joining motes. Address Range End FF:FF:FF:FE End address to assign to OTA joining motes. Server Ports The server ports communicate via UDP with other processes running on the Conduit. Item Default Value Description Upstream Port 1780 Upstream communication port from radio. Downstream Port 1782 Downstream communication port to radio. App Port Up 1784 Application can open a socket on this port to receive upstream messages from motes. App Port Down 1786 Application can send to this port to send downstream messages to motes. Payload Broker The payload broker is an MQTT broker that facilitates communication between an application and the network server. Item Default Value Description Enabled Checked (enabled) Enable the Payload Broker Hostname 127.0.0.1 Local host (no encryption) Port 1883 Default MQTT port Before setting up LoRa, your device should be connected and powered up. If not refer to installation information for your device. Getting Started with LoRa Login to the web management interface. Refer to the software guide if needed. Access the LoRaWAN Network Settings by going to LoRaWAN > Network Settings on the left sidebar. See LoRaWAN Network Settings in the software guide for details. To modify advanced settings, click Show Advanced Settings. For more details, see LoRaWAN Network Settings in the software guide. For configuring as a Packet Forwarder, select Packet Forwarder from Mode under LoRa Mode. For more details, see LoRaWAN Network Settings in the software guide. Setting Up an mDot Establish a serial connection to the mDot™ Connect your PC to the DB9 serial connector on the UDK Open a terminal session using an application such as TeraTerm with baud rate 115,200 Issue these commands with the same values you set for the gateway: AT+FSB=value (915 NA only | value = frequencySubBand from your LoRa gateway) AT+NI=1,value (value = Network Name for your LoRa gateway) AT+NK=1,value (value = Network Passphrase for your LoRa gateway) AT&W (save settings) ATZ (restart) Join the network: AT+JOIN Send data with ACK requested: AT+ACK=1 AT+SEND=hello world Next Steps The MultiTech MultiConnect® Conduit™ is a configurable, scalable cellular communications gateway for industrial IoT applications. This guide will help you set up the Multitech Conduit gateway to communicate over The Things Stack. The technical specifications of the Conduit can be found in the software guide in the official documentation page. Prerequisites Registration Create a gateway by following the instructions for Adding Gateways. The gateway EUI can be found at the bottom of the gateway under the field "LORA NODE". Setting Up the Gateway For the first-time hardware and software setup, you can refer to the appropriate configuration guide on the Multitech documentation page. We have included a few short steps to help you get started. If your gateway is already configured on your local network, skip ahead to Connecting The Gateway to The Things Stack. Connecting to the Gateway as a DHCP Server If you have already connected your gateway to your local network and you can access its configuration page via the gateway’s IP address, skip ahead to Connecting The Gateway to The Things Stack. Since the gateway initializes as a DHCP server, you can not simply connect it to your local network, and you may have to configure TCP/IP manually. After hard resetting the device, connect it directly to a computer via ethernet and use the following TCP/IP settings: IP Address: 192.168.2.2 Subnet Mask: 255.255.255.0 Router Address: 192.168.2.1 Browse to the IP address of the gateway, 192.168.2.1. You may be met with the following screen. In newer versions of Chrome, you can type “thisisunsafe” to continue past the certificate error screen. Other browsers have different ways of advancing past certificate error screens. Once past the certificate screen, create a username and password. You will then be met with the first time setup screen. Click Next. Set a time and date, and skip the rest of the configuration options. Once you have finished the first time setup, click the Setup button in the left hand menu, and choose Network Interfaces. Click on the pen icon for the eth0 interface to modify it. Set the Direction dropdown to WAN, and the Mode dropdown to DHCP Client. Click Submit to save the settings. Next, click the Administration button in the left hand menu, and choose the Access Configuration submenu. Here, enable the Web Server for HTTP via LAN and WAN, and enable HTTPS access via WAN. Optionally, you can also enable SSH via WAN. Warning: If you do not enable Web Server or SSH access via WAN, when you connect the gateway to your local network, you will not be able to access it anymore, and you will have to hard reset and start over. Click Submit to save the Access Configuration Settings. After you have submitted both the Ethernet Configuration and Access Configuration settings, double check them so you don’t lock yourself out! Finally, click Save and Apply to apply your configuration. At this point, the gateway will reboot. It will come back online as a DHCP client, so you can disconnect it from your computer, and connect the gateway directly to your router or local network. Connecting the Gateway to The Things Stack The Multitech Conduit supports LoRa Basics™ Station and the legacy UDP packet forwarder. LoRa Basics™ Station is more secure and supports configuration of custom channel plans, amongst other improvements. Please follow instructions to Connect Multitech Conduit with LoRa Basics™ Station. If for some reason LoRa Basics™ Station is not available to you, instructions for connecting with the legacy packet forwarder are here. Troubleshooting Packet Forwarder Logs Packet forwarder logs contain the messages received from the devices and the network server. You can use the information to debug the issues. You can find the packet forwarder logs using the gateway's web console. Do the following to download the logs onto your device: Login to your gateway's web console and navigate to Administration -> Debug Options. Click on the Download Logs button in the Logging section to download the logs. Now, in the downloaded logs, open the lora-pkt-fwd-1.log file to see the packet forwarder logs. Upgrading the Firmware If you have an issue with the current firmware version, you can use following steps to upgrade the firmware. Refer to the top of your configuration software window to check your firmware version. You have to upgrade the device's firmware to the latest version. You can download the firmware upgrades from the downloads section of the MultiTech website. Do the following to upgrade the firmware on your device: Before you upgrade your firmware, save your present configuration as a backup. Go to the MultiTech website, locate the firmware upgrade file you want for your device(MTCDT AEP x.x.x in the current case, where x.x.x is the latest version available on the website), and download this file to a known location. Navigate to Administration -> Firmware Upgrade. Click on Choose Firmware Upgrade File button, and Click on Browse to find where the firmware file resides that you want to apply. Select the file and click on Open. The file name appears next to the Choose Firmware Upgrade File button. Make sure you select the correct BIN file; otherwise, your device can become inoperable. Click on Start Upgrade. A message about the time needed to upgrade appears. Click on OK. A progress bar appears indicating the status of the upgrade. When the upgrade is completed, your device reboots. After the firmware upgrade is completed, verify your configuration to ensure that it is same as what you expected. The new firmware is written into flash memory. It may take up to 10 minutes to upgrade the firmware. Do not interrupt the devices' power or press the reset button during this time. Before setting up LoRa, your device should be connected and powered up. If not refer to installation information for your device. Getting Started with LoRa Login to the web management interface. Refer to the software guide if needed. Access the LoRaWAN Network Settings by going to LoRaWAN > Network Settings on the left sidebar. See LoRaWAN Network Settings in the software guide for details. To modify advanced settings, click Show Advanced Settings. For more details, see LoRaWAN Network Settings in the software guide. For configuring as a Packet Forwarder, select Packet Forwarder from Mode under LoRa Mode. For more details, see LoRaWAN Network Settings in the software guide. Setting Up an mDot Establish a serial connection to the mDot™ Connect your PC to the DB9 serial connector on the UDK Open a terminal session using an application such as TeraTerm with baud rate 115,200 Issue these commands with the same values you set for the gateway: AT+FSB=value (915 NA only | value = frequencySubBand from your LoRa gateway) AT+NI=1,value (value = Network Name for your LoRa gateway) AT+NK=1,value (value = Network Passphrase for your LoRa gateway) AT&W (save settings) ATZ (restart) Join the network: AT+JOIN Send data with ACK requested: AT+ACK=1 AT+SEND=hello world Next Steps The MultiTech MultiConnect® Conduit™ is a configurable, scalable cellular communications gateway for industrial IoT applications. Conduit allows users to plug in two MultiConnect mCard™ accessory cards supporting wired or wireless interfaces. This guide will help you set up the gateway to communicate over The Things Network. Prerequisites # MultiTech Conduit AEP or mLinux model. Update the Conduit to 5.30 firmware or later to use LoRa Basics Station, which supports channel plan configuration from the Network Server. MultiTech MTAC-LoRa LoRa accessory card, installed as instructed. Do not forget to mount the antenna to the mCard after fitting it in the conduit. Computer with USB port and terminal software. Mac OS and Linux come with terminal software. For Windows you can use something like Putty. For the mLinux version you’ll need a USB stick.