# Host Image OTA CDLD requirements and recommendations

* The OTA CDLD process is done by broadcasting one image to all nodes on one gateway.
* At some point during the OTA CDLD of a host image, the node will notify the host that a new host image is being downloaded to the node. It will do this by using a Broadcast Start Indication message. The Broadcast Start Indication message contains the following information:
  + Broadcast ID
  + First 256 bytes of OTA CDLD broadcast data
  + Length, in bytes, of the broadcast
* Upon reception of the Broadcast Start Indication by the host, it is the responsibility of the host to make a determination, based on the data provided by the Broadcast Start Indication message, of whether the node should continue the host image download or reject it and stop the download. This is important for power savings since downloading a full host image can potentially consume a lot of power and drain the node and host batteries relatively quickly. If the image is inappropriate for the host, then the download should be rejected such that maximum power savings and battery life can be realized.
* The first 256 bytes of the image must contain the following information:
  + The first several bytes must be a magic number that is unique to this host type. A magic number of at least four bytes is to be used. This value does not change between different images for the same host type. This information is used by the host to determine if this image is for this type of node. If the image type is incorrect, then the image should be rejected.
  + Some information about the version of this host image. This value will change between different images for the same host type. This information is used by the host to determine if this image is newer than the image already on the host and should therefore be accepted, or if this image is the same as or older than the image already on the host and should therefore be rejected.
* The remainder of the 256 bytes can be used as desired by the host designers. It is recommended that the following fields are included in the remainder of the first 256 bytes of the image:
  + Some form of indication of the layout of the first 256 bytes. If the first 256 bytes are called a “file”, then this value can be a file format version number. This may be useful when a field is to be added or removed or changes in size.
  + The actual size of the host image. The first 256 bytes can be considered as overhead information and there is some padding and CRC appended. The actual number of bytes in the host image may be useful in determining the amount of data to write or erase in NVM.
* In order to accept or reject the download indicated by the Broadcast Start Indication, the host must send a Broadcast Start Confirmation message to the node. The same Broadcast ID as was contained within the Broadcast Start Indication must be used in the Broadcast Start Confirmation. The Broadcast Start Confirmation message will contain accept/reject notification to the node, based on the information in the first 256 bytes of the image data.
* The Broadcast Start Indication and Broadcast Start Confirmation are used by the node to determine whether the download should continue or not. There no 1:1 association of Broadcast Start Indication messages to Broadcast End Indication Messages. The host must be capable of processing one or multiple Broadcast Start Indication messages without any matching Broadcast End Indications and vice versa.
* The current system design allows for a maximum of one OTA CDLD being in progress at a time. This means that if a Broadcast Start Indication is received, then information from previous Broadcast Start Indications is old.
* When the OTA CDLD of a host image to the node is complete, the node will notify the host that a host image is available at the node and that the host can obtain that data from the node. The node will indicate that a host image is available at the node by sending a Broadcast End Indication message. The Broadcast End Indication message contains the following information:
  + Broadcast ID
  + Length, in bytes, of the broadcast
* The Broadcast End Indication may be received by the host without the host previously receiving a Broadcast Start Indication. The host must treat each Broadcast End Indication as an indication that there may be a new host image available at the node. Since the Broadcast End Indication message does not contain information about the first 256 bytes of data, the host needs to request the first 256 bytes of data from the node before the host can make a determination of whether the image is for this host or not. In some circumstances, it may be possible that the length of the broadcast can be used to determine that the image is not for this host, but these recommendations are written with the assumption that this is not done.
* A new Broadcast End Indication may be received by the host without receiving a Broadcast Start Indication or while the host is currently working on a previous Broadcast End Indication. In this event, the new Broadcast End Indication should be treated normally. Any processing of a previously received Broadcast End Indication needs to end and the new processing of the new Broadcast End Indication must start from the beginning, as described below.
* When the host receives the Broadcast End Indication message, it must request the first 256 bytes from the node by sending to the node a Broadcast Data Request message. The Broadcast Data Request message contains the following information:
  + Broadcast ID
  + Offset, in bytes, of the data being requested
  + Length, in bytes, of the data being requested
* The first Broadcast Data Request message should request from the node the first 256 bytes of image data. It should use the same Broadcast ID as was in the Broadcast End Indication message.
* When the first 256 bytes of image data is received by the host from the node, the host should make a determination of whether to download the rest of this image from the node (in the same fashion as was done with the Broadcast Start Indication message).
* It is recommended that when the host image is being retrieved from the node by the host that the host store this information in some temporary staging area until the entire image has been read from the node and exists on the host. Once the entire image is in the staging area, the host can then enter a special section of firmware that copies the image from the staging area to its final destination in NVM. Once in NVM, the host can then reset and start running its new version of firmware.

A typical sequence diagram involving the above rules and messages is as follows:

Broadcast Start Cnf

Broadcast Start Ind

Host

Node

Broadcast End Ind

Broadcast Data Req

Broadcast Data Rsp

Broadcast Data Req

Broadcast Data Rsp

Broadcast Data Req

Broadcast Data Rsp

In the above diagram, the node sends the Broadcast Start Indication message to the host such that the host can make a determination of whether or not the rest of the host image should be downloaded. When the host responds in the affirmative in the Broadcast Start Confirmation message, the node continues downloading the image.

Once the OTA CDLD of the host image is complete, the node sends a Broadcast End Indication to the host. The host starts requesting the data, a chunk at a time, using the Broadcast Data Request. The node responds to these requests by sending the appropriate piece of the host image data in Broadcast Data Confirmation message.

Once all of the host image data has been received by the host, the host verifies that the new image is stored in NVM and then resets such that the host will start up with the new image.

# 256 Bytes header data

The first 256 bytes of the OTA CDLD host image data is used for overhead identification purposes. As noted in the requirements above, the first 256 bytes must contain a magic number that is unique to the host type, and it must have version information such that the host can determine whether or not the image being downloaded is newer than the image already running on the host.

An example of the OTA CDLD file is as follows:

256 byte header

Host Image raw data (variable length)

Padding and CRC (variable length)

Bytes 0 - 3: magic number  
Bytes 4 - 7: header format version number  
Bytes 8 - 11: host firmware version number  
Bytes 12 - 15: system release  
Bytes 16 - 19: length of host image raw data  
Bytes 20 - 255: reserved for future header formats

The “256 byte header” is sent to the host in the Broadcast Start Indication message as well in a Broadcast Data Response that in response to a Broadcast Data Request message that requested the first 256 bytes of the Broadcast data.

Note that in order for the host to request the first bytes of the host image raw data, the host must send a Broadcast Data Request message with an offset value of 256 to the node.

The OTA CDLD Broadcast image must be padded and have a CRC. This is appended by a script that is run before the image is uploaded to the NMS for broadcast. Since this block is not meaningful to the host and is used in order to deliver the broadcast over the air to the node, this information does not necessarily need to be obtained by the host. For this reason, it is a recommendation to store the host image raw data length in the first 256 bytes.

# Preparing a host image for OTA CDLD

In order to broadcast a host image, one must assemble the three pieces of the broadcast image before sending it to NMS for OTA CDLD. The three pieces are:

* 256 Byte header
* Host image raw data
* Padding and CRC

It is ultimately up to the host designer on what the format of the host image raw data is. It is recommended, however, that this data be straight forward machine executable binary data such the data can be directly copied to the host’s final NVM destination and run. Other options, such as applying compression to the image, are out of the scope of this document and let entirely to the host designers and implementers.

Once the host image raw data is in a file, the 256 byte header must be prepended to this data. It is recommended that a script be used to facilitate this process.

After the first 256 bytes have been prepended to the host image raw data, the file must be padded and a CRC applied. An existing script, gen\_ota\_image.py, exists for this purpose. In order to use gen\_ota\_script.py, a node type must be specified. All host images have a node type value of 5.

After these three pieces have been put together in the above order, the resulting broadcast image file can be uploaded to NMS for OTA CDLD.

# Pseudo Code for handling OTA CDLD messages from the node

The following chunks of pseudo code demonstrate one possibility of how to handle all of the broadcast messages from the node. This pseudo code requests chunks of 256 bytes of broadcast data at a time from the node and stores it in a temporary staging area until all broadcast data has been received by the host, at which point it copies the image from the staging area to the final NVM destination and resets itself such that the new firmware can start.

ProcessBroadcastStartInd( broadcastId, payload, length ):  
 Verify magic number exists in payload.  
 Verify payload has FW version newer than currently running FW.  
 If either condition above is false, then schedule BroadcastStartCnf with reject to be sent to node.  
 Else schedule BroadcastStartCnf with accept to be sent to node.

ProcessBroadcastEndInd( broadcastId, length ):  
 Note that starting new image download from node.  
 Range check and record the length of the image download.  
 Schedule BroadcastDataReq with offset=0 length=256 to be sent to node.  
  
ProcessBroadcastDataRsp( status, broadcastId, offset, length, payload):  
 Verify that a BroadcastDataRsp is expected.  
 Verify that broadcastId is correct (matches value in sent BroadcastDataReq).  
 Verify that offset is correct (matches value in sent BroadcastDataReq).  
 If any of these check fail, then quit processing this message.  
 If offset==0:  
 Verify magic number exists in payload.  
 Verify payload has FW version newer than currently running FW.  
 If either condition is false, then quite processing this message.  
 Else erase the staging area.  
 Write the payload to the staging area.  
 Increment the offset by the length (always 256 in this example).  
 If length+offset >= BroadcastEndInd length:  
 Copy data (excluding first 256 bytes) from staging area to final NMV destination.  
 Reset host.  
 Else:  
 Schedule BroadcastDataReq with next offset and length=256 to be sent to node.