HACKING THE USB WORLD WITH FACEDANCER

STANDARDIZATION AND DEVICE CLASSES

these two devices have a lot in common,
even if only one of them looks like a weird alien egg

- send motion updates at regular intervals
- report the status of a few buttons

left: image credit HP
right: image credit UHURU, Inc.

these two devices have a lot in common,
even if only one of them looks like a weird alien egg

- send motion updates at regular intervals
- report the status of a few buttons

Q: Should these devices really need custom drivers?
A: No! *But wait… how do we do that?*

left: image credit HP
right: image credit UHURU, Inc.

STANDARD DEVICE CLASSES

these two devices have a lot in common,
even if only one of them looks like a weird alien egg

- send motion updates at regular intervals
- report the status of a few buttons

Q: Should these devices really need custom drivers?
A: No! *But wait… how do we do that?*

left: image credit HP
right: image credit UHURU, Inc.

STANDARD DEVICE CLASSES

Not an exhaustive list.

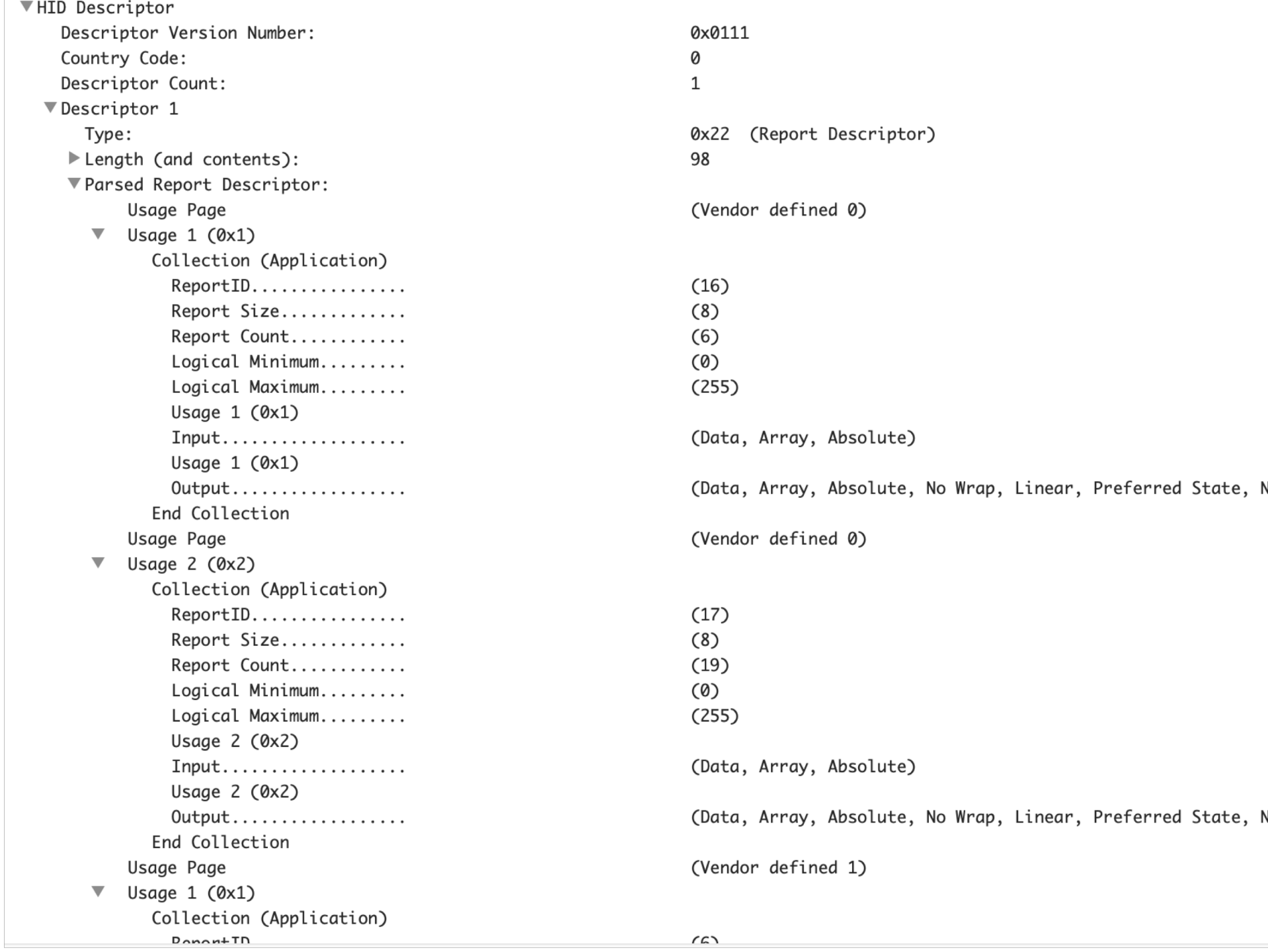
Class Number	Name	Standardized in…
0x1	Audio	Device Class Specification
0x2	Communications Device (CDC)	Device Class Specification
0x3	Human Interface Device (HID)	Device Class Specification
0x6	Still Image Capture	Device Class Specification
0x7	Printer	Device Class Specification
0x8	Mass Storage (UMS)	Device Class Specification
0x9	USB Hub	USB core specifications
0xE	Video Capture	Device Class Specification

```
▼Full Speed device @ 13 (0x14200000): ..................................  Composite device: "USB Receiver"
  ▶Port Information:                                                    0x001a
  ▶Number Of Endpoints (includes EP0):
  ▶Device Descriptor
  ▼Configuration Descriptor (current config): ......................    "RQR36.00_B0005"
    ▶Length (and contents):                                             59
     Number of Interfaces:                                              2
     Configuration Value:                                               1
     Attributes:                                                        0xA0 (bus-powered, remote wakeup)
     MaxPower:                                                          98 mA
    ▶Interface #0 - HID/Boot Interface
    ▼Interface #1 - HID
       Alternate Setting                                                0
       Number of Endpoints                                              1
       Interface Class:                                                 3   (HID)
       Interface Subclass;                                              0
       Interface Protocol:                                              0
      ▼HID Descriptor
         Descriptor Version Number:                                     0x0111
         Country Code:                                                  0
         Descriptor Count:                                              1
        ▼Descriptor 1
           Type:                                                        0x22  (Report Descriptor)
          ▶Length (and contents):                                       98
          ▶Parsed Report Descriptor:
    ▶Endpoint 0x82 - Interrupt Input
```

HID DEVICES

All diagrams from the USB 2.0 specification.

HID DEVICES



```
▼HID Descriptor
    Descriptor Version Number:                  0x0111
    Country Code:                               0
    Descriptor Count:                           1
  ▼Descriptor 1
      Type:                                     0x22  (Report Descriptor)
    ▶Length (and contents):                     98
    ▼Parsed Report Descriptor:
        Usage Page                              (Vendor defined 0)
      ▼ Usage 1 (0x1)
          Collection (Application)
            ReportID.................           (16)
            Report Size..............           (8)
            Report Count.............           (6)
            Logical Minimum.........            (0)
            Logical Maximum.........            (255)
            Usage 1 (0x1)
            Input....................           (Data, Array, Absolute)
            Usage 1 (0x1)
            Output...................           (Data, Array, Absolute, No Wrap, Linear, Preferred State, N
          End Collection
        Usage Page                              (Vendor defined 0)
      ▼ Usage 2 (0x2)
          Collection (Application)
            ReportID.................           (17)
            Report Size..............           (8)
            Report Count.............           (19)
            Logical Minimum.........            (0)
            Logical Maximum.........            (255)
            Usage 2 (0x2)
            Input....................           (Data, Array, Absolute)
            Usage 2 (0x2)
            Output...................           (Data, Array, Absolute, No Wrap, Linear, Preferred State, N
          End Collection
        Usage Page                              (Vendor defined 1)
      ▼ Usage 1 (0x1)
          Collection (Application)
            ReportID                            (6)
```

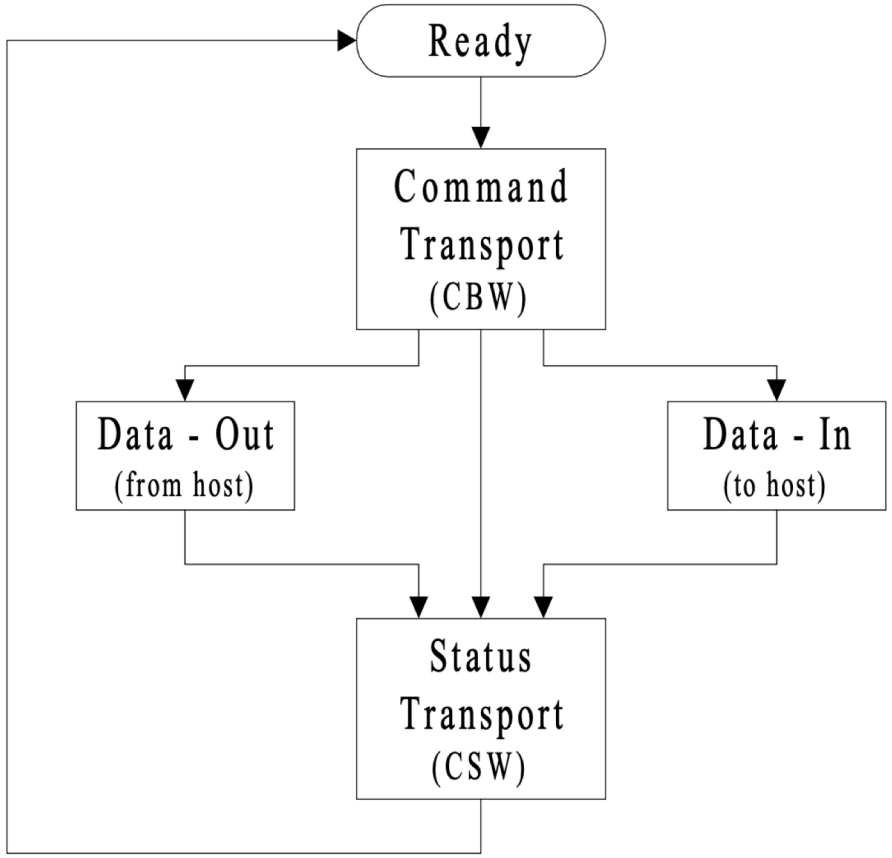


Figure 1 - Command/Data/Status Flow

Table 5.1 - Command Block Wrapper

Byte \ bit	7	6	5	4	3	2	1	0
0-3	*dCBWSignature*							
4-7	*dCBWTag*							
8-11 (08h-0Bh)	*dCBWDataTransferLength*							
12 (0Ch)	*bmCBWFlags*							
13 (0Dh)	Reserved (0)				*bCBWLUN*			
14 (0Eh)	Reserved (0)			*bCBWCBLength*				
15-30 (0Fh-1Eh)	*CBWCB*							

Table 5.2 - Command Status Wrapper

Byte \ bit	7	6	5	4	3	2	1	0
0-3	*dCSWSignature*							
4-7	*dCSWTag*							
8-11 (8-Bh)	*dCSWDataResidue*							
12 (Ch)	*bCSWStatus*							

MASS STORAGE

All diagrams from the Bulk Only Device Class Definition (DCD)..

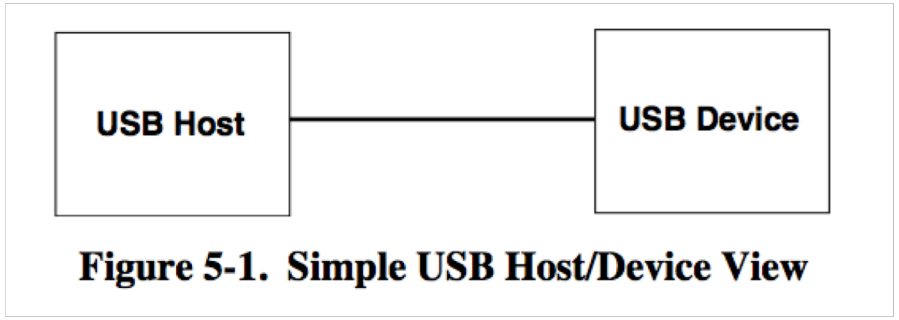
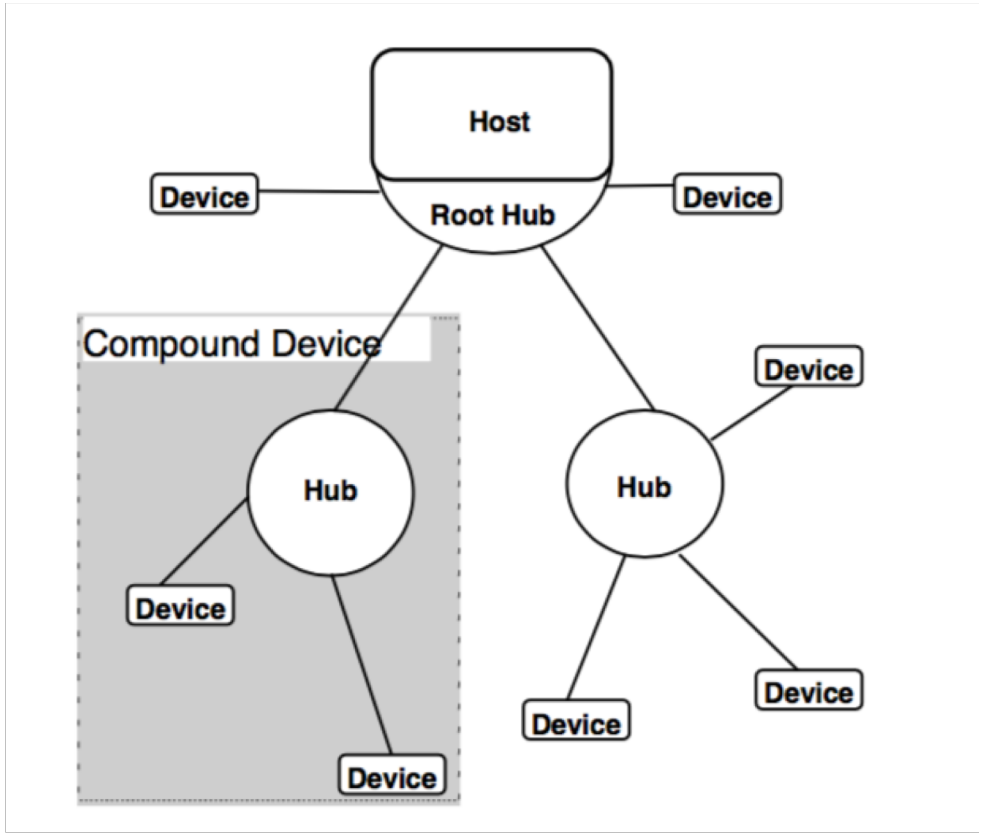


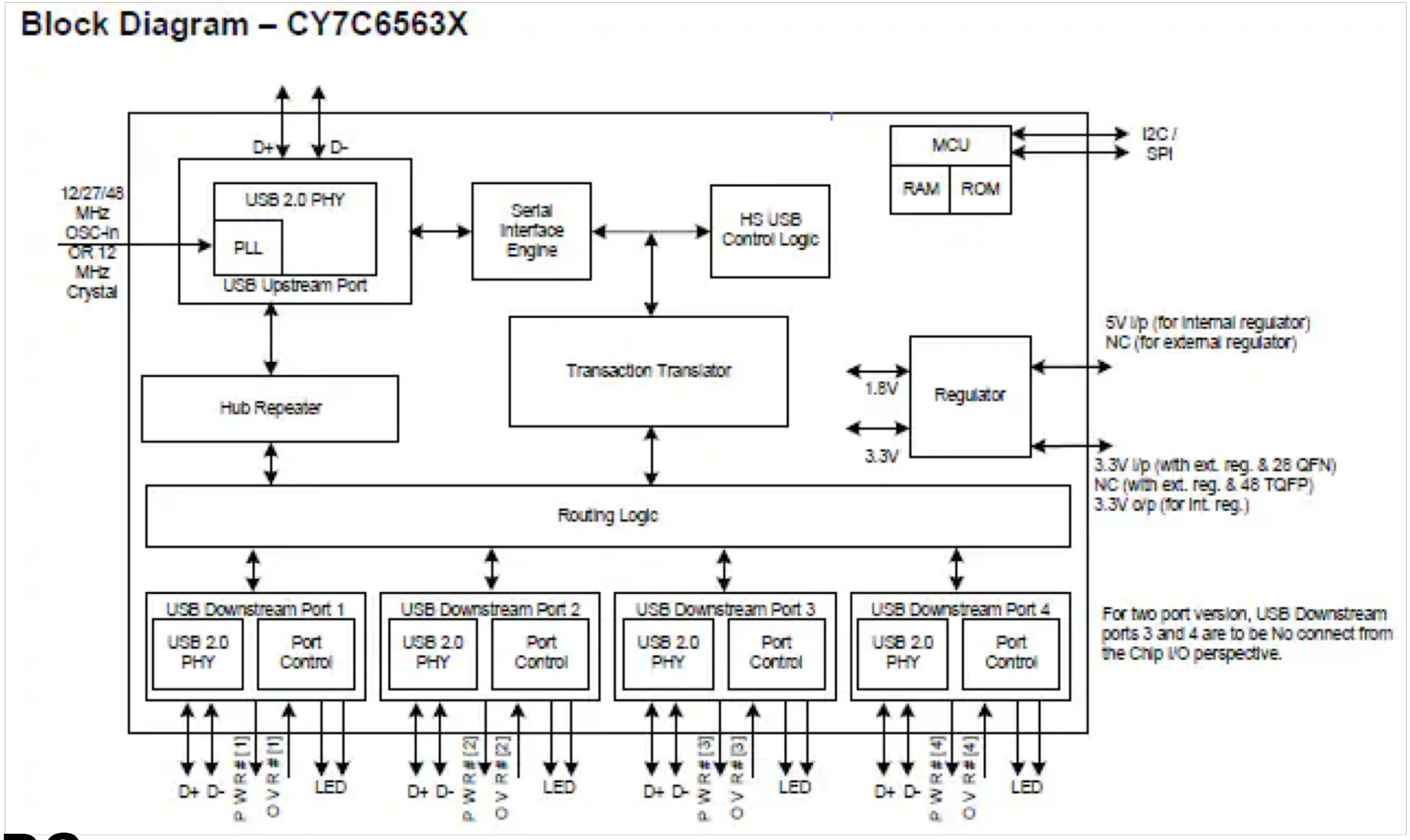
Figure 5-1. Simple USB Host/Device View



USB HUBS

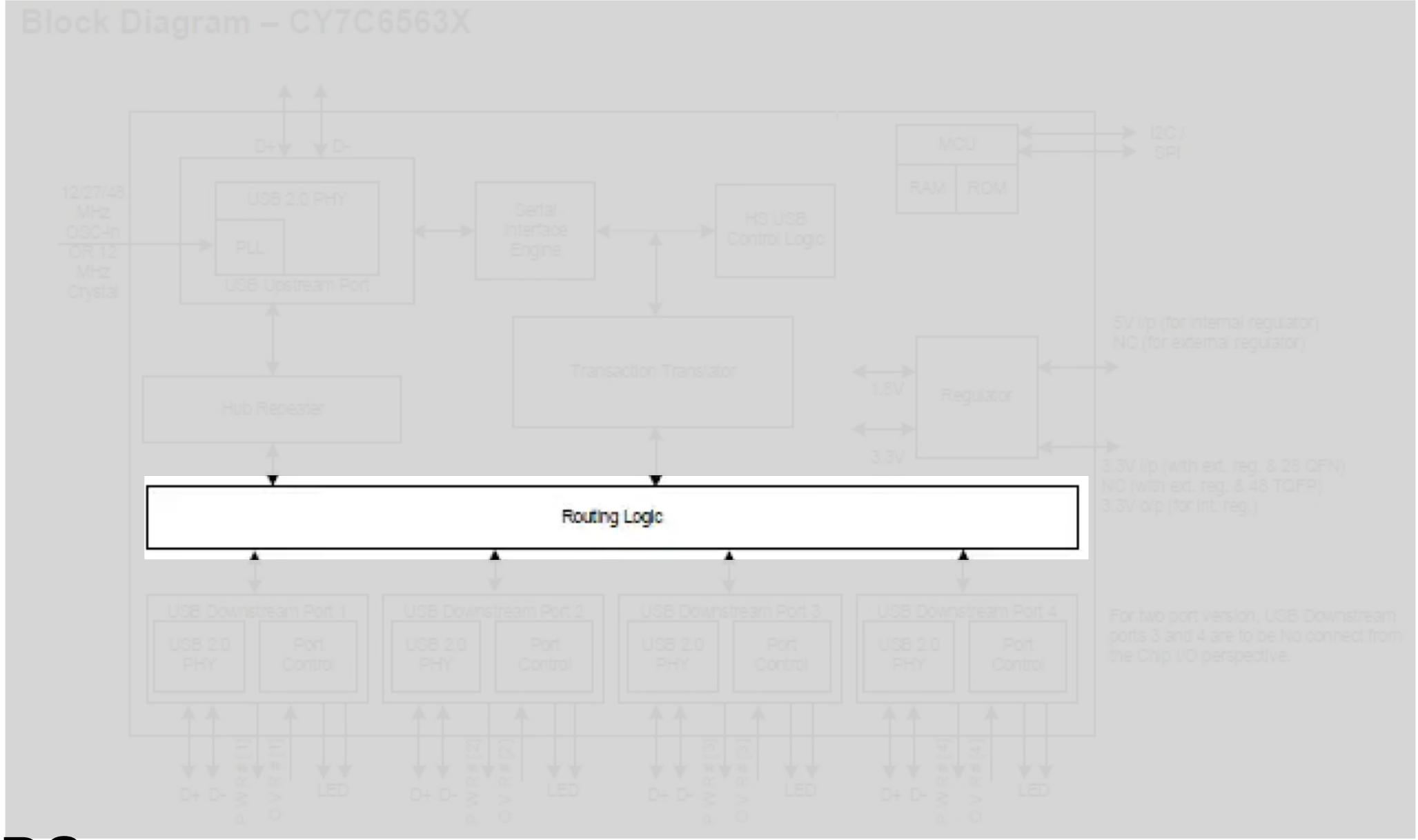
All diagrams from the USB 2.0 specification.

Block Diagram – CY7C6563X



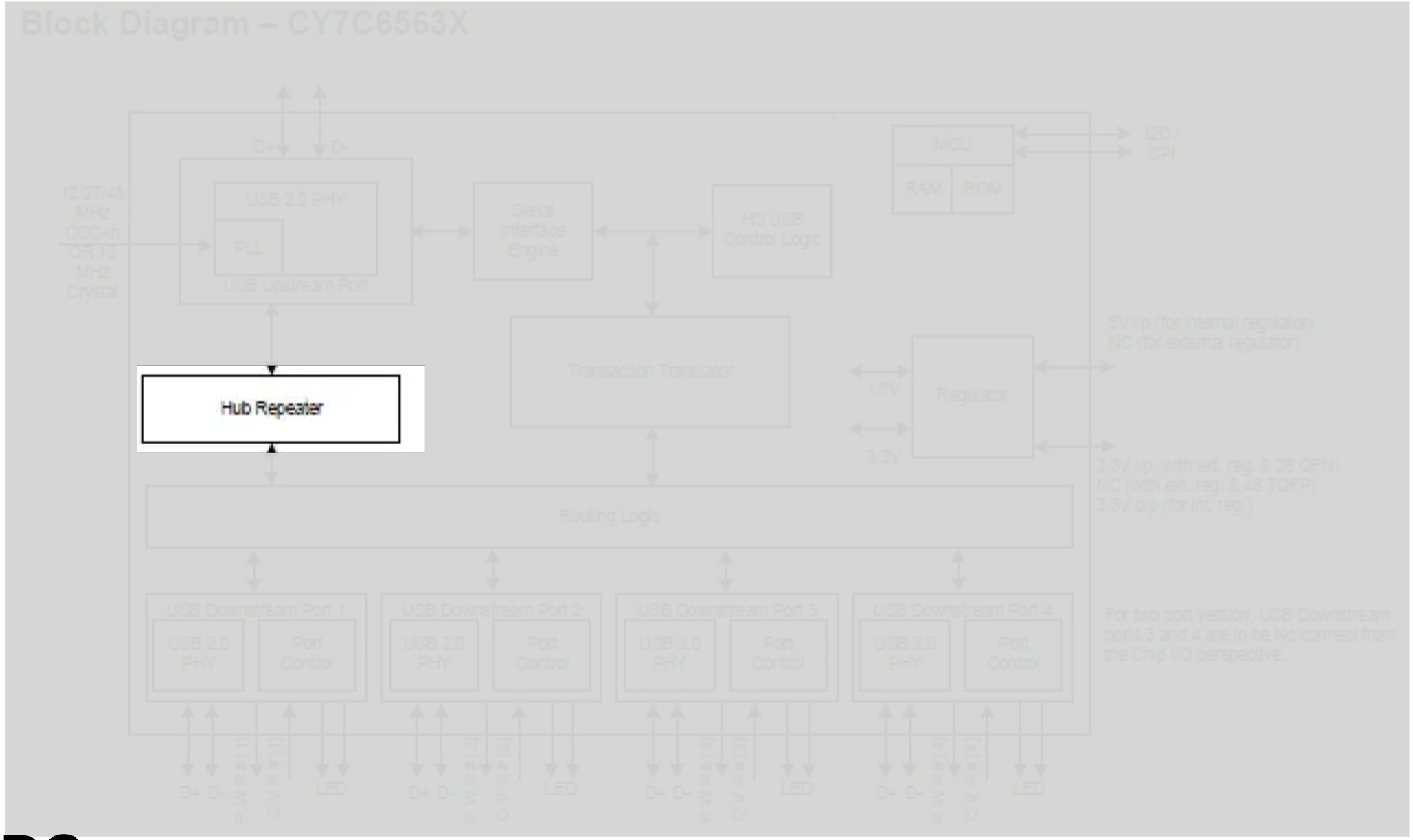
USB HUBS

Diagram courtesy Cypress, Inc.



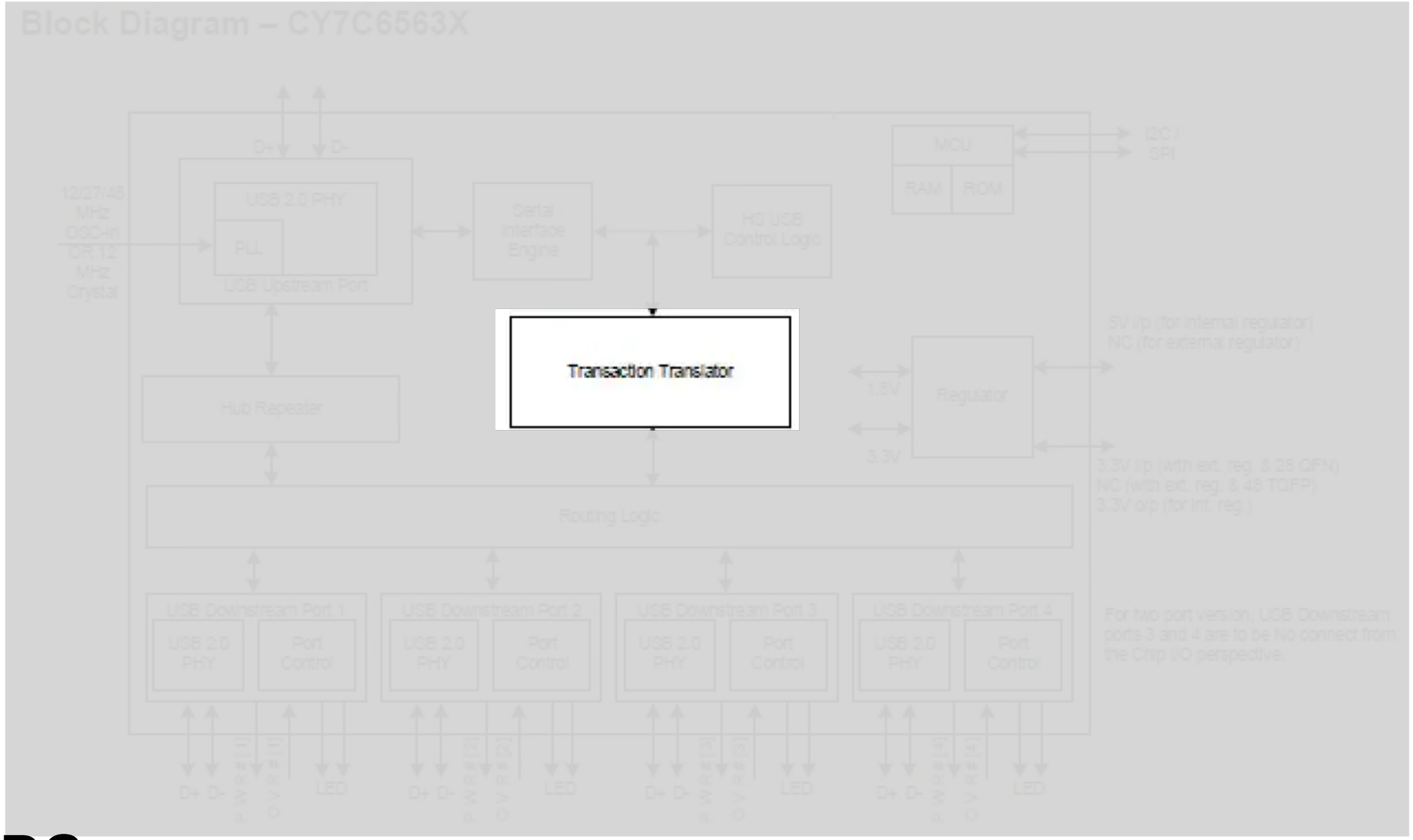
USB HUBS

Diagram courtesy Cypress, Inc.



USB HUBS

Diagram courtesy Cypress, Inc.



USB HUBS

Diagram courtesy Cypress, Inc.