IPv6 over MS/TP Networks

draft-ietf-6lo-6lobac-04

Kerry Lynn, Editor <kerlyn@ieee.org>
Jerry Martocci <jerald.p.martocci@jci.com>
Carl Neilson <cneilson@deltacontrols.com>
Stuart Donaldson <stuart.donaldson@honeywell.com>
6lo WG, IETF 95, Buenos Aires, 07 Apr 2016

Motivation

Develop a low-cost **wired** IPv6 solution for commercial building control applications
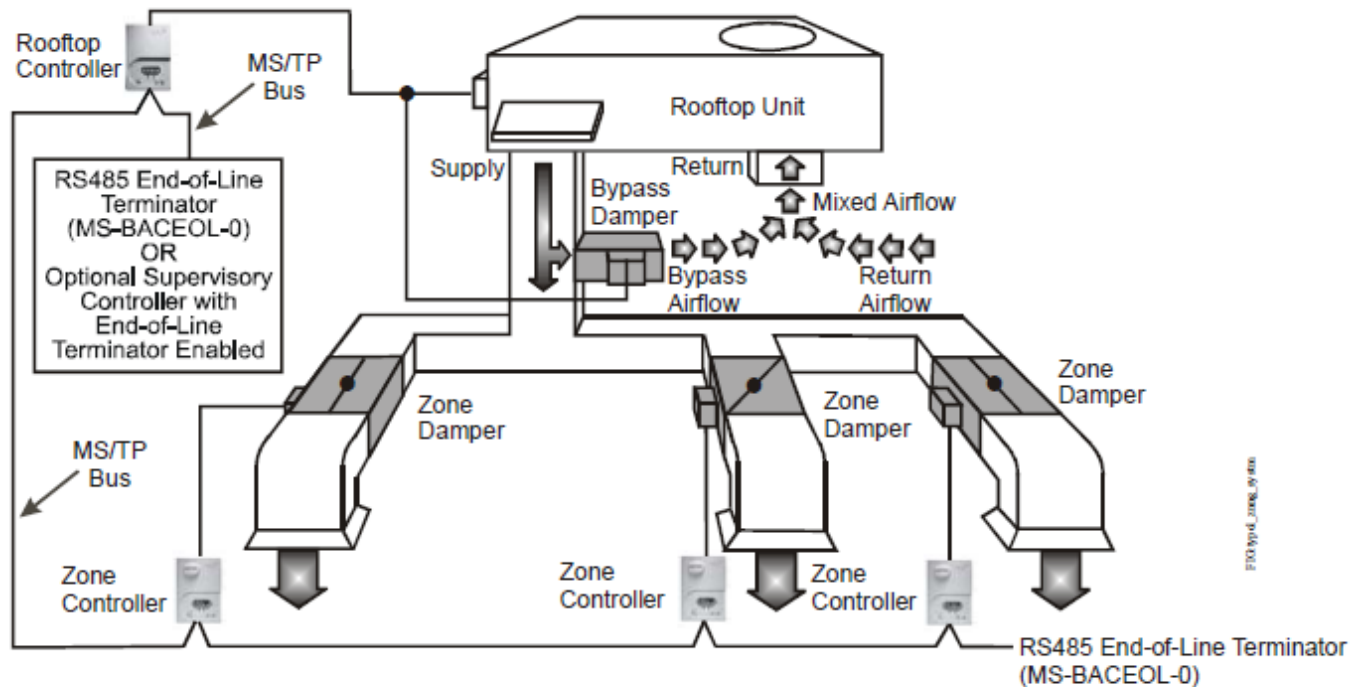

Figure 1: Typical Zoning Control System Installed on a Single MS/TP Bus

Background

- **BACnet** is the ISO/ANSI/ASHRAE [Standard 135-2012] data communication protocol for Building Automation and Control networks

- **MS/TP** (Master-Slave/Token-Passing) is a widely used data link defined in BACnet
  - Based on RS-485 single twisted pair PHY; supports data rates up to 115.2 kbps over 1 km distance
  - Contention-less MAC (token passing bus)
  - Consider it a wired alternative to IEEE 802.15.4

Technical Approach

- Leverage 6Lo specs [RFCs 4944, 6282, 6775]
- Minimize changes to existing MS/TP specification [BACnet Clause 9]
- Goal: co-existence with legacy MS/TP nodes
  - No changes to frame header format, control frames, or MS/TP Master Node state machine
- MS/TP Extended Frames proposal includes:
  - New frame type for IPv6 (LoBAC) Encapsulation
  - Larger MSDU (1500+ octets)
  - 32-bit FCS (CRC-32K)
 - COBS (Consistent Overhead Byte Stuffing) encoding

Status

- Proposal is mature and stable
  - First presented to 6man in July '11
  - Two interoperable implementations, Contiki and RIOT (tested at ETSI 6lo PlugTest in Yokohama)
  - No external dependencies; BACnet has assigned a FrameType and draft of new Clause 9 is available
  - Two detailed reviews
  - ➔ Only Security Section remains unreviewed

Changes since -03

- § 12, Security Considerations
  - 6LoBAC is wired; reduced threat of eavesdropping
  - 6LoBAC nodes are stationary; unlikely that traffic analysis could be used for correlation of activities or location tracking of *individuals*
  - 6LoBAC traffic is mostly on-link, e.g. from zone to supervisory controller

  ➔A MAC-derived IID is recommended for on-link and 64-bit privacy IID for off-link traffic

Backup Slides

MS/TP Control Frame Format

0   31

0x55	0xFF	FrameType	DestAddr
SrcAddr	Length = 0		HeaderCRC
Optional 0xFF			
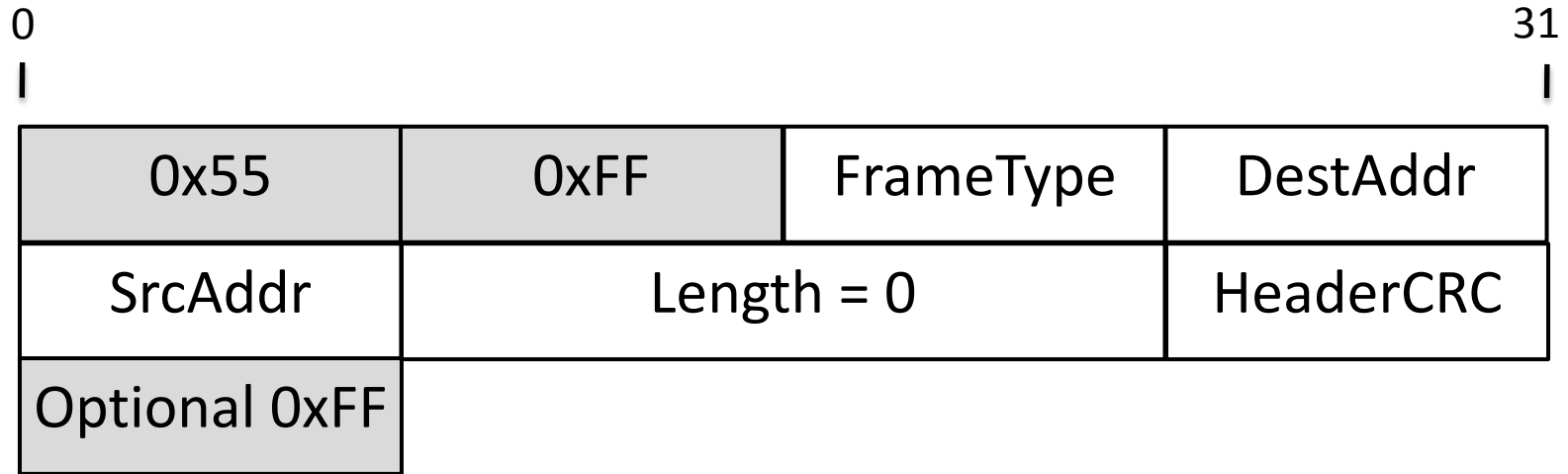
Frame Type: 0 = Token
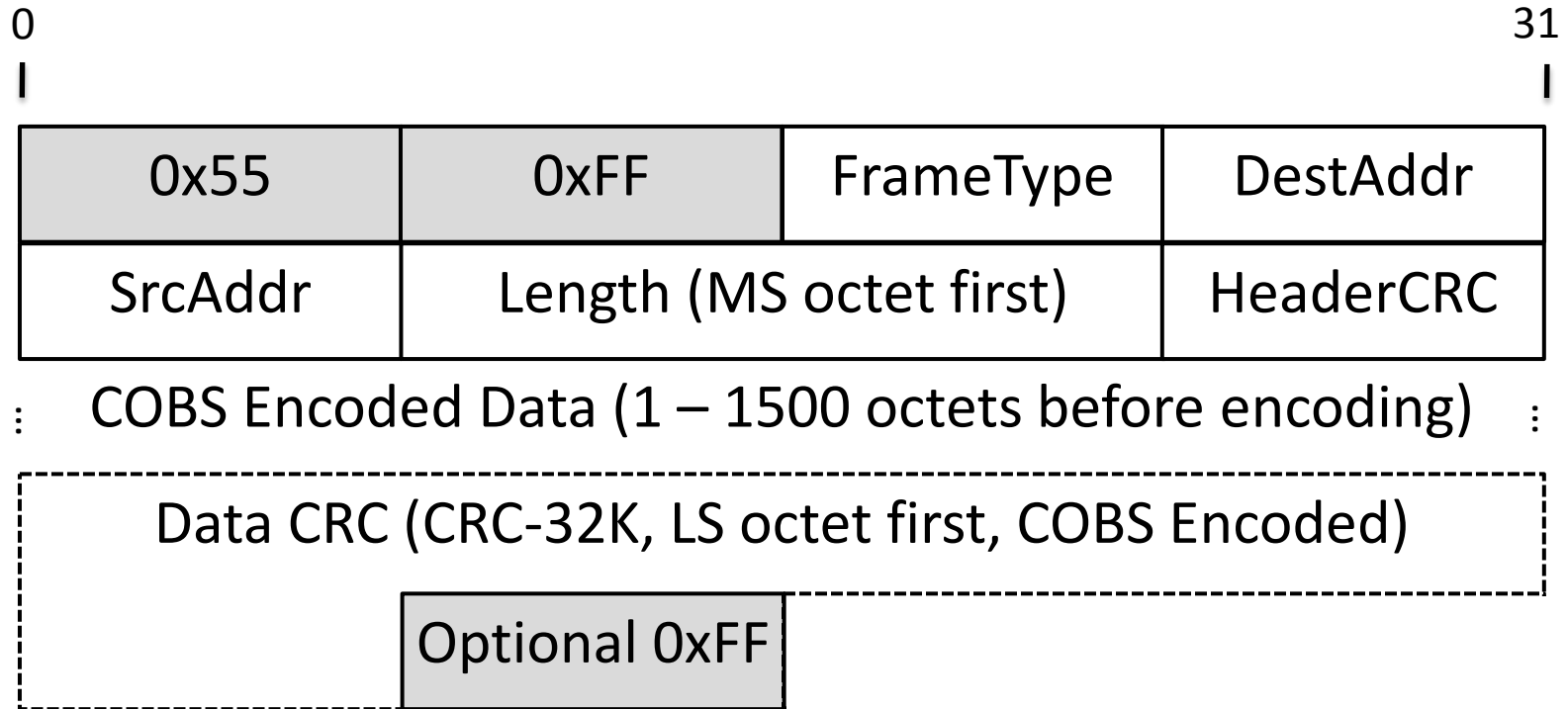   1 = Poll for Master
                           2 = Reply to Poll for Master
Destination Address: 0 – 127
Source Address: 0 – 127

MS/TP Encoded Data Frame Format

0   31

0x55	0xFF	FrameType	DestAddr
SrcAddr	Length (MS octet first)		HeaderCRC

COBS Encoded Data (1 – 1500 octets before encoding)

Data CRC (CRC-32K, LS octet first, COBS Encoded)

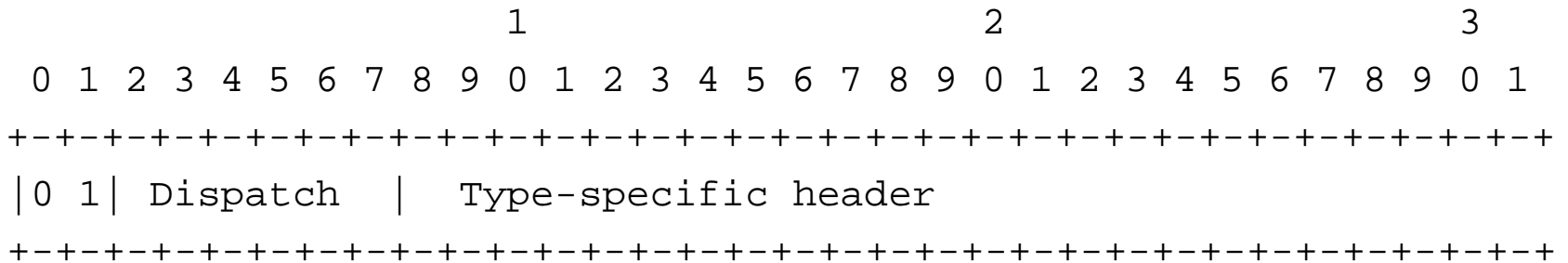Optional 0xFF

Frame Type: 34 = IPv6 (LoBAC) Encapsulation
Destination Address: 0 – 127 or 255 (all nodes)
Source Address: 0 – 127

LoBAC Encapsulation

- Uses 6LoWPAN Dispatch Header [RFC 4944]:

```
                      1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|0 1| Dispatch  |  Type-specific header
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Pattern	Header Type
01 1XXXXX	LOWPAN_IPHC – Compressed IPv6 header

LoBAC Encapsulation (cont.)

- No mesh, broadcast, or fragmentation headers
  - One option remains:

IPHC Dispatch	IPHC Header	Payload

A LoBAC encapsulated LOWPAN_IPHC
[RFC 6282] compressed datagram

IPHC Compression [RFC 6282]

- Assumes some 6LBR-like behavior, e.g. 6LoWPAN Context Option (6CO, [RFC 6775])

- Uses 6LoWPAN short address format, formed by appending 8-bit MS/TP address to the octet 0x00
  - For example, an MS/TP node with a MAC address of 0x4F results in the following IPHC short address:

```
|0               1|
|0               5|
+-----------------+
|0000000001001111|
+-----------------+
```
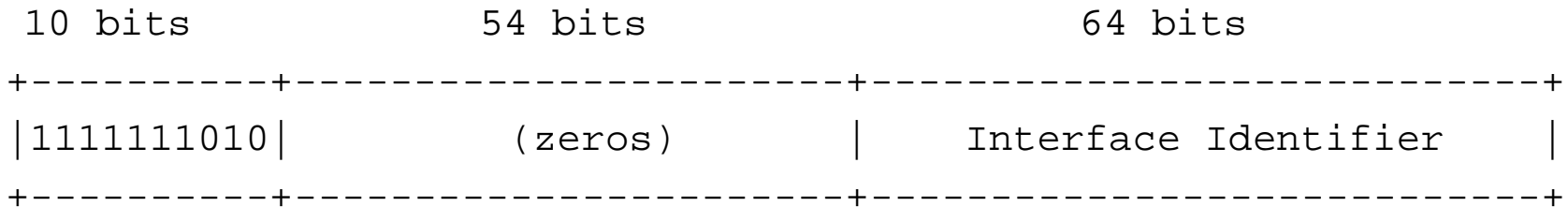
Stateless Address Auto-Configuration

- Typically, 8-bit MAC address is appended to the seven octets 0x00, 0x00, 0x00, 0xFF, 0xFE, 0x00
  - For example, an MS/TP node with a MAC address of 0x4F results in the following Interface ID:

```
|0              1|1              3|3              4|4              6|
|0              5|6              1|2              7|8              3|
+---------------+---------------+---------------+---------------+
|0000000000000000|0000000011111111|1111111000000000|0000000001001111|
+---------------+---------------+---------------+---------------+
```

- A privacy address **may** be used for the Interface Identifier (SHOULD be for ULA/Global addresses)
  - In this case there **must** be a way to map the address to an 8-bit MAC address (e.g. ARO in NS [RFC 6775])
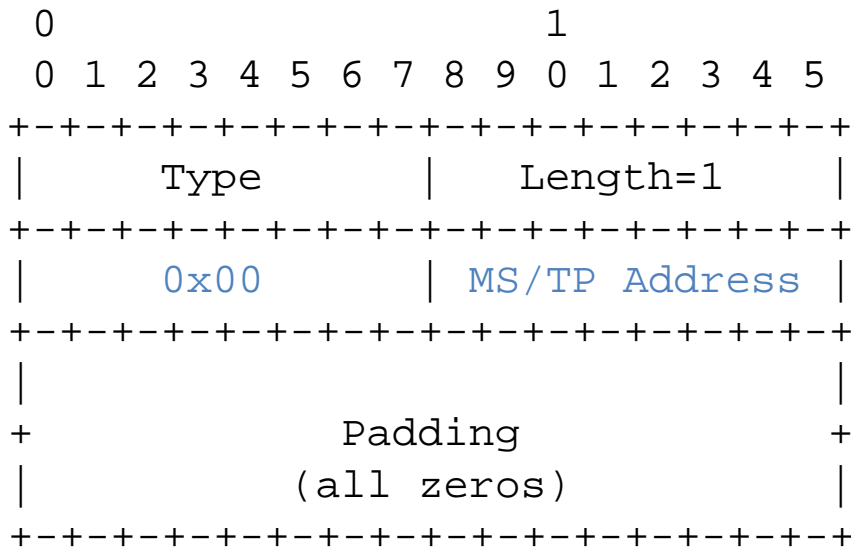
IPv6 Link Local Address

- The IPv6 link-local address [RFC 4291] for an MS/TP interface is formed by appending the Interface Identifier (defined in previous slide) to the prefix FE80::/64:

```
 10 bits                54 bits                       64 bits

+----------+-----------------------------+---------------------------+
|1111111010|          (zeros)            |    Interface Identifier   |
+----------+-----------------------------+---------------------------+
```

Unicast Address Mapping

- The Source/Target Link-Layer Address option has the following form when the link layer is MS/TP and the addresses are 8-bit MS/TP MAC addresses:

```
 0                   1
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type      |    Length=1   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      0x00      | MS/TP Address |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |
+             Padding           +
|            (all zeros)        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
Option fields:

Type:
  1 = Source Link-layer address
  2 = Target Link-layer address

Length:
  The value of this field is
  1 for 8-bit MS/TP addresses

MS/TP Address:
  The 8-bit MAC address in
  canonical bit order
```

Multicast Address Mapping

- MS/TP only supports link-local broadcast
- Uses 6LoWPAN short address format, formed by appending 0xFF to the octet 0x00
  - All IPv6 multicasts on the MS/TP link map to the following IPHC short destination address:

```
|0              1|
|0              5|
+----------------+
|0000000011111111|
+----------------+
```

COBS Encoding Basics

Code	Followed By	Meaning
0x00	(not applicable)	(not allowed)
0x01	nothing	A single zero byte
0x02	one data byte	The single data byte, followed by a zero byte
n	$(n-1)$ data bytes	The $(n-1)$ data bytes, followed by a zero byte
0xFE	253 data bytes	The 253 data bytes, followed by a zero byte
0xFF	254 data bytes	The 254 data bytes, **not** followed by a zero byte

| 00 | ➜ | 01 |

| x | 00 | ➜ | 02 | x |

| x | y | 00 | ➜ | 03 | x | y |

| x | y | z | ... | z | y | ➜ | FF | x | y | z | ... | y |
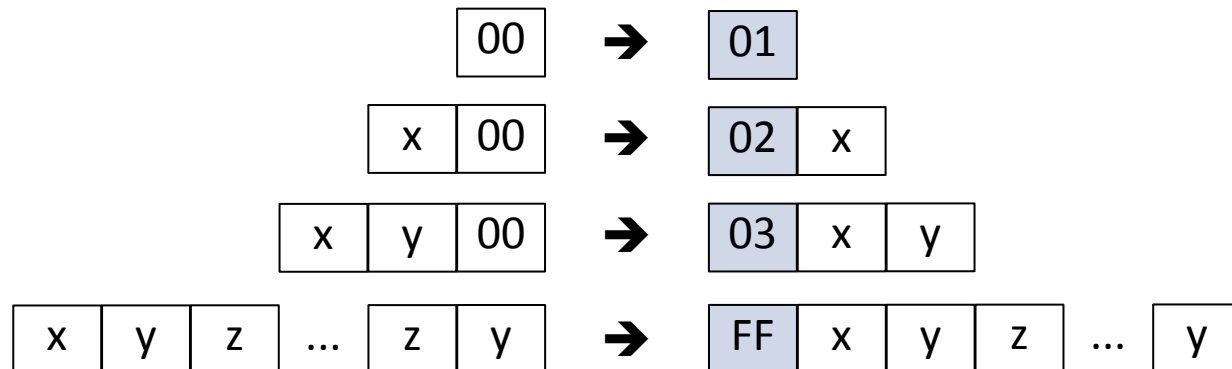
COBS Encoding in Detail

- "Phantom zero" is appended to input to resolve ambiguity in final code block:

H	e	l	l	o		➜	06	H	e	l	l	o

H	e	l	l	o	00	➜	06	H	e	l	l	o	01
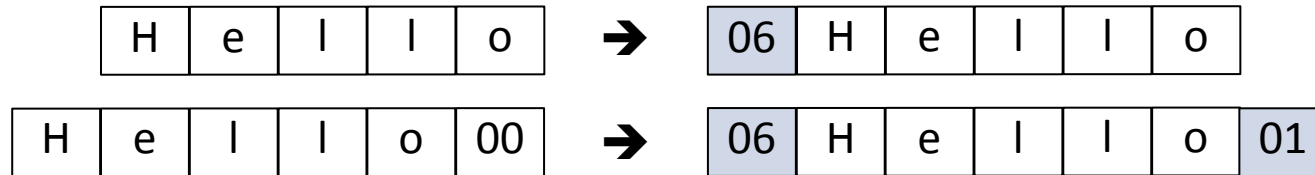
- An arbitrary octet (e.g. 0x55) may be removed by XOR-ing it over the COBS encoder **output** stream

- COBS overhead:
  - At least one octet per encoded field
  - At most one octet in 255 (6 octets in 1501; ≈ 0.4%)