6LoBAC: A new IPv6 Data Link

Kerry Lynn
<kerlyn@ieee.org>
15 December 2015

IoT Background

By Neil Gershenfeld, Raffi Krikorian and Danny Cohen

In Barcelona about a century ago, Antoni Gaudí pioneered a fluid building style that seamlessly integrated visual and structural design. The expressive curves of his buildings were not just ornamental facades but also integral parts of the load-bearing structure. Unfortunately, a similar unification has yet to happen for the electronic infrastructure in a building. Switches, sockets and thermostats are grafted on as afterthoughts to the architecture, with functions fixed by buried wiring. Appliances and computers arrive as after-the-fact intrusions. Almost nothing talks to anything else, as evidenced by the number of devices in a typical house or office with differing opinions as to the time of day.

These inconveniences have surprisingly broad implications for construction economics, energy efficiency, architectural expression and, ultimately, quality of life. In the U.S., building buildings is a $1-trillion industry. Of that, billions are spent annually on drawing wiring diagrams, then following, fixing and revising them. Over the years, countless "smart home" projects have sought to find new applications for intelligent building infrastructure—neglecting the enormous existing demand for facilities that can be programmed by their occupants rather than requiring contractors to fix their functionality in advance.

Any effort to meet that demand, though, will be doomed if a lightbulb requires a skilled network engineer to install it and the services of a corporate IT department to manage it. The challenge of improving connectivity requires neither gigabit speeds nor gigabyte storage but rather the opposite: dramatic reductions in the cost and complexity of network installation and configuration.

Over the years, a bewildering variety of standards have been developed to interconnect household devices, including X10, LonWorks, CEBus, BACnet, ZigBee, Bluetooth, IrDA and HomePlug. The situation is analogous to that in the 1960s when the Arpanet, the Internet's predecessor, was developed. There were multiple types of computers and networks then, requiring special-purpose hardware to bridge these islands of incompatibility.

The solution to building a global network out of heterogeneous local networks, called internetworking, was found in two big ideas. The first was packet switching: data are chopped up into packets that can be routed independently as needed and then recombined. This technique marked a break from the traditional approach, used in telephone networks, of dedicating a static circuit to each connection. The second idea was the "end-to-end" principle: the behavior of the network should be determined by what is connected to it rather than by its internal construction, a concept embodied in the Internet Protocol (IP). Gradually the Internet expanded to handle applications ranging from remote computer access to e-commerce to interactive video. Each of these services introduced new types of data for packets to carry, but engineers did not need to change the network's hardware or software to implement them.

These principles have carried the Internet through three decades of growth spanning seven orders of magnitude in both performance and size—from the Arpanet's 64 sites to today's 200 million registered hosts. They represent timeless insights into good system design, and, crucially, they contain no specific performance requirements. With great effort and discipline, technology-dependent parameters were kept out of the specifications so that hardware could evolve without requiring a revision of the Internet's basic architecture.

These same ideas can now solve the problem of connecting

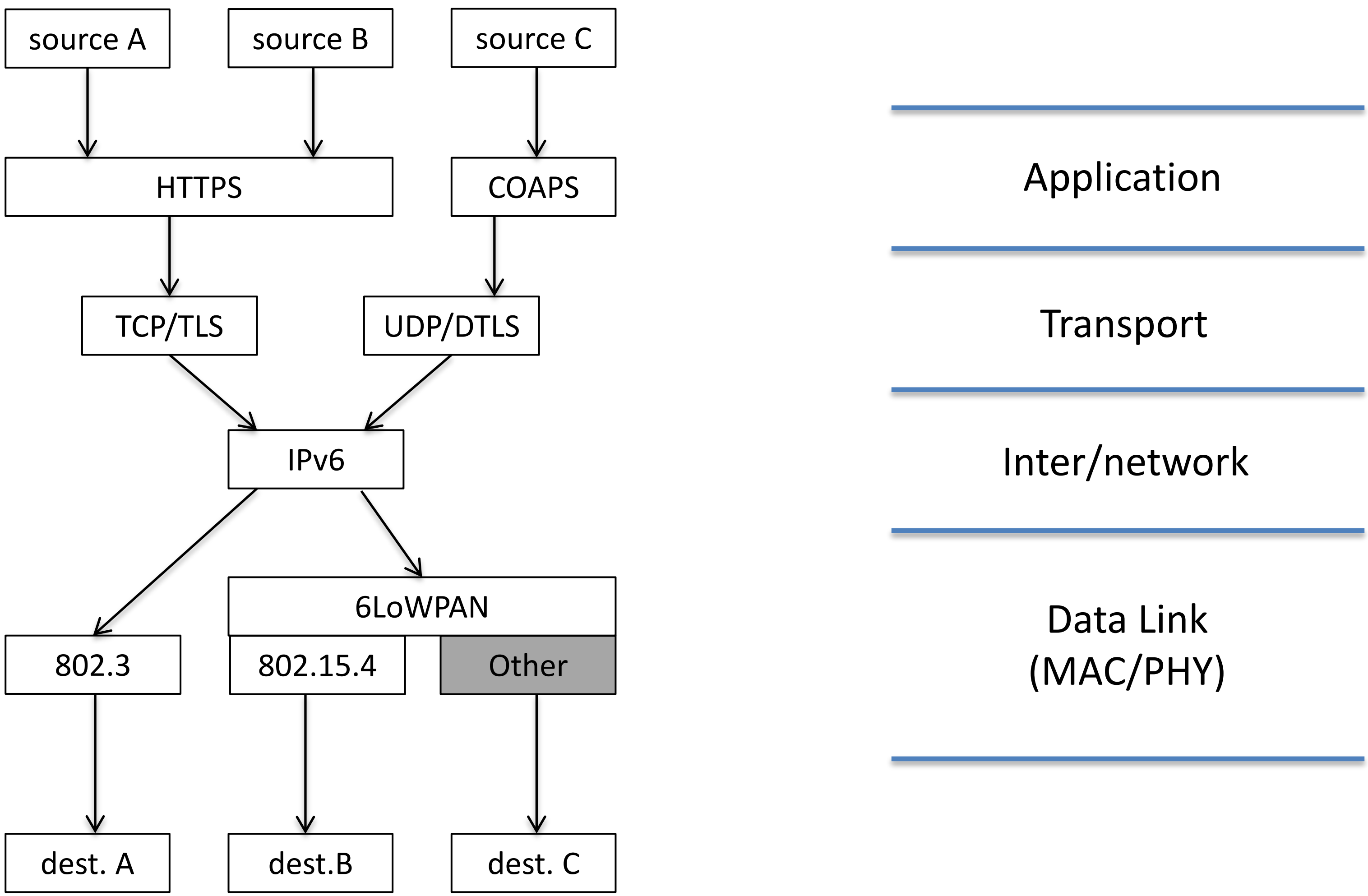
The Internet of Things

The principles that gave rise to the Internet are now leading to a new kind of network of everyday devices, an "Internet-0"

EVEN SOMETHING AS SIMPLE as a lightbulb could be connected directly to the Internet, if suitably equipped with cheap circuitry that sends signals along the electrical wiring.

76 SCIENTIFIC AMERICAN OCTOBER 2004

Review (Layered Model)



Goal

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

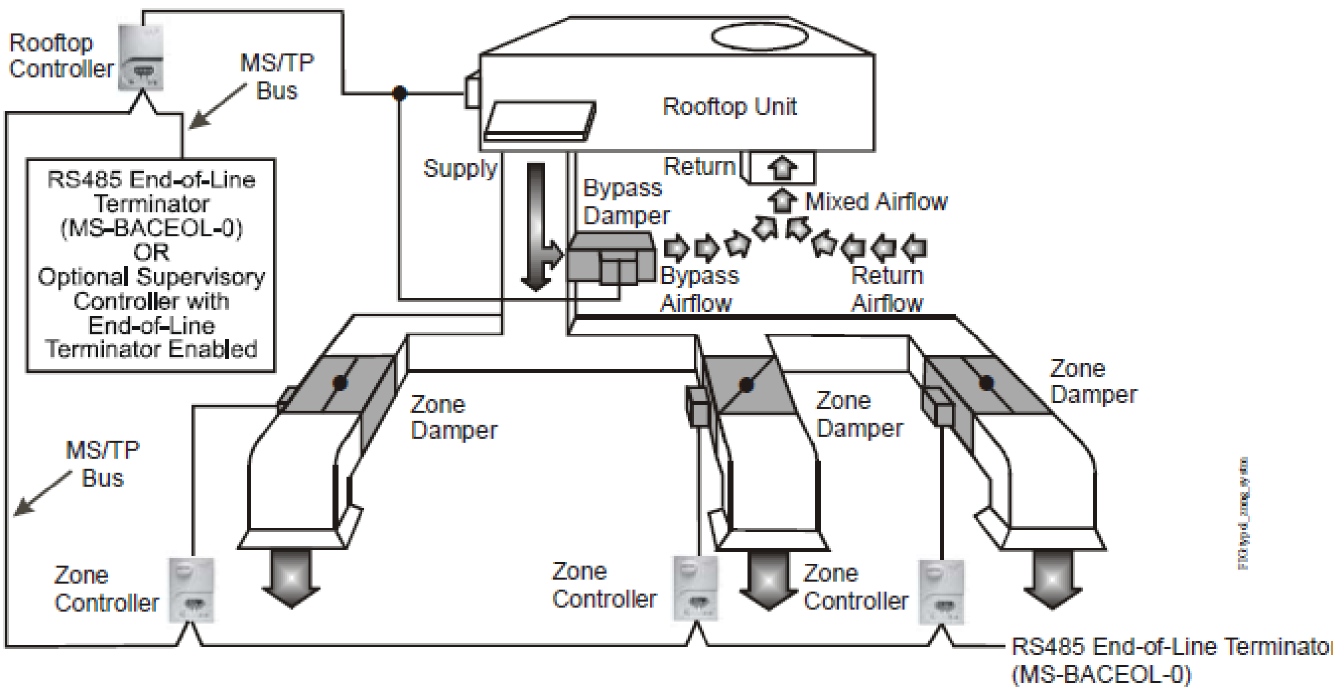


Figure 1: Typical Zoning Control System Installed on a Single MS/TP Bus

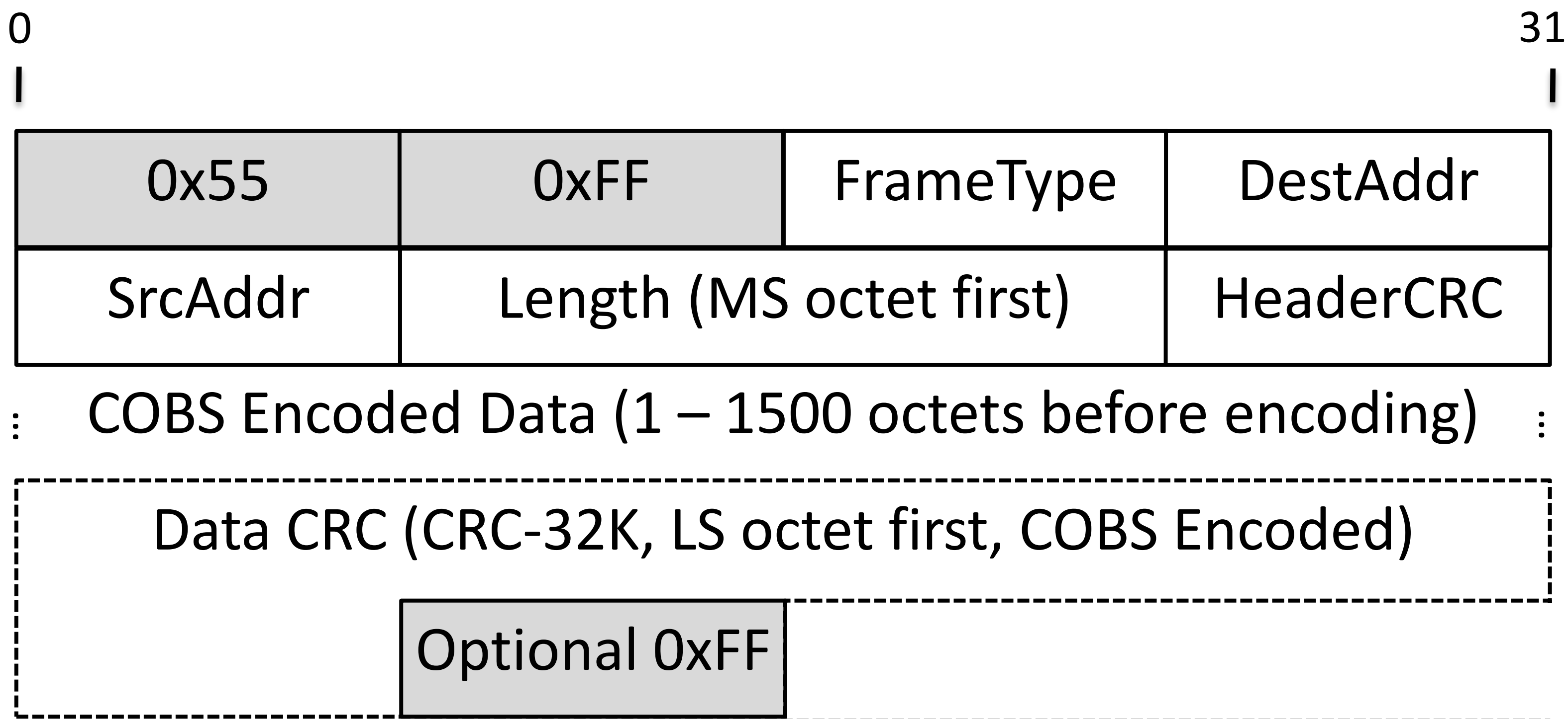
Technical Approach

- Leverage elements of 6LoWPAN solution [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

MS/TP 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 kpbs and 1 km diameter
  - Contention-free MAC (token passing bus)
  - Consider it a wired alternative to IEEE 802.15.4

MS/TP *Extended Frame* Format



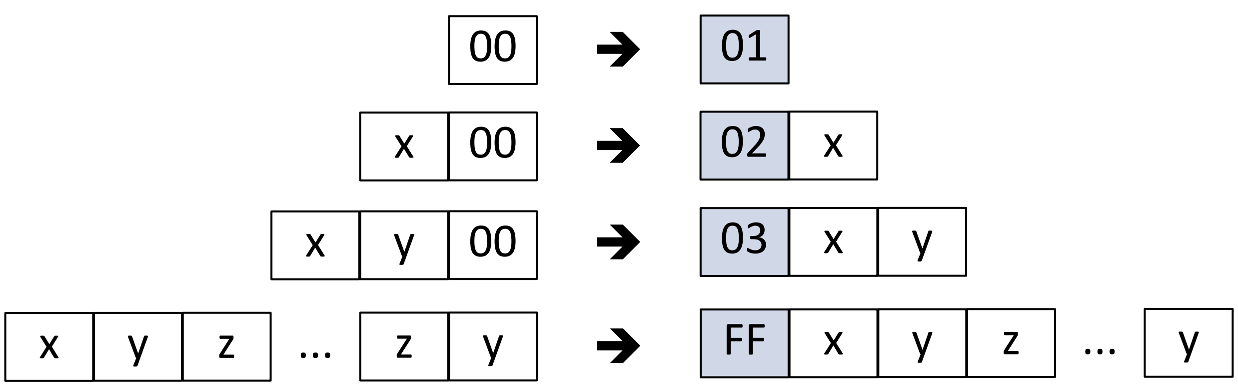
Frame Type:	34 = IPv6 (LoBAC) Encapsulation
Destination Address:	0 – 127, 255 (all nodes)
Source Address:	0 – 127

CRC Background

- Noisy channel acts like a random bit mask XOR'd with the data word
- We use cyclic redundancy code (CRC) to *detect* these errors
- Data word (frame) is divided by a polynomial G(x); remainder is CRC
- Detection capability is related to size and co-efficients of G(x)

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
$1 \le n \le 253$	($n - 1$) data bytes	The ($n - 1$) data bytes, followed by a zero byte
0xFF	254 data bytes	The 254 data bytes, **not** followed by a zero byte



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 field
  - At most, one octet per 254 (6 octets per 1500; ≈ 0.4%)

6Lo Background

- Need to define encapsulation
- Need to define mapping of MAC address for:
  - Interface Identifier (IID)
  - Stateless Address Auto-Configuration (SLAAC)
  - Unicast and multicast transmission
- Header compression
- Security Considerations
- Other (e.g. abstract MAC interface)

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
00 XXXXXX	NALP – Not a LoWPAN (LoBAC) frame
01 000000	ESC – Additional Dispatch octet follows
01 000001	IPv6 – Uncompressed IPv6 header
...	Reserved by RFC 4944
01 1XXXXX	LOWPAN_IPHC – Compressed IPv6 header

LoBAC Encapsulation (cont.)

- No mesh, broadcast, or fragmentation headers
  - Two options remain:

IPv6 Dispatch	IPv6 Header	Payload

A LoBAC encapsulated IPv6 datagram

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|
+----------------+
```

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    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                               |
+            Padding            +
|          (all zeros)          |
+               +-+-+-+-+-+-+-+-+
|               | MS/TP Address |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
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|
+----------------+
```

Summary

- 6LoBAC was the first to propose re-use of 6LoWPAN solutions (RFCs 4944, 6282, 6775)
- Served as a pattern for subsequent proposals (Z-Wave, BTLE, NFC, etc.) resulting in formation of the IETF 6lo working group
- Remains the only wired 6lo PHY
- Has passed ETSI Interoperability Plugtest
- About to enter WG “last call”

Thank You

- Questions?