ECE 444/544 Supervisory Control & Critical Infrastructures

Session 12

POWER ENGINEERS

Presented by: Chris Dyer

20 February 2024

Protocol Definition

- These are the rules or a standard that define the syntax, semantics and synchronization of **communication** and possible error recovery methods. **Protocols** may be implemented by hardware, software, or a combination of both. Communicating systems use well-defined formats (**protocol**) for exchanging messages.

Topic Overview

- Terms/Acronyms Used
  - » RTU, Communications Processor, Data Concentrator
  - » IED, relay, meter, field device, PLC
  - » EMS, DMS, Management System
  - » DNP, MODBUS, IEC-61850
- What is a SCADA Protocol
  - » EMS vs Substation
  - » Operations vs Engineering vs …..

Topic Overview

- SCADA/Protocol History
  - » 1930s – Used Telco Tech
    - – Wire for wire (think telegraph systems)
  - » 1960s – intro of a 'true' protocol
    - – 10 bit, slow speeds
  - » 1960s/1970s – intro of modems, using voice lines to carry data streams at higher speeds
    - – No more wire for wire
  - » 1970s – intro of 'affordable' microprocessor

Topic Overview

- SCADA/Protocol History
  - 1970s/1980s more advancement of RTUs/IEDs due to lowering cost of microprocessors and advancement of functions
    - More advanced protocols and more data
  - 1980s – move away from proprietary protocols
    - There were 10s, or 100s of different protocols and variants
      Some back and forth on this move still ongoing
    - Integrated systems using off the shelf components

Topic Overview

- SCADA/Protocol History
  - » 1980s-current
    - – Advancement was slow but in most recent years large moves to high speed networks, newer protocols, etc
    - – Many proprietary RTUs with open protocols, programming languages, etc.
    - – Self describing, object oriented

Other Protocols

- » SEL
- » Conitel - CONtrol Indication TELemetry (Leeds & Northrup)
- » CDC (Control Data Corporation)
- » L&G 8979 (Landis & Gyr / Telgyr)
- » Westinghouse REDAC
- » Cooper 2179 (PG&E 2179)
- » Harris
- » GETAC

Selecting Protocols

- Primary Usage
  - SCADA
    - DNP, Modbus, MMS
  - System Protection
    - GOOSE
  - Special Functions
    - Sampled Values
- Data Requirements
- Equipment
- Common Practice

What do we want in a SCADA protocol

- Device Addressing
- Device Health
- Data Integrity Checks
- Security
- Reasonable Update Times (within device limits)
- Discovery
- Data Value
- Timestamp
- Validity / Quality
- Others?

Numbering Systems

- Decimal
  - » Decimal definition – a numeral system with a base of ten (0-9)
  - » More human readable
  - » Less matched with bits
    - – 16 bit number 65535 does not match easily with a decimal number when broken down into its base components
    - – $198 = 1x10^2 + 9x10^1 + 8x10^0 = 198$

Numbering Systems

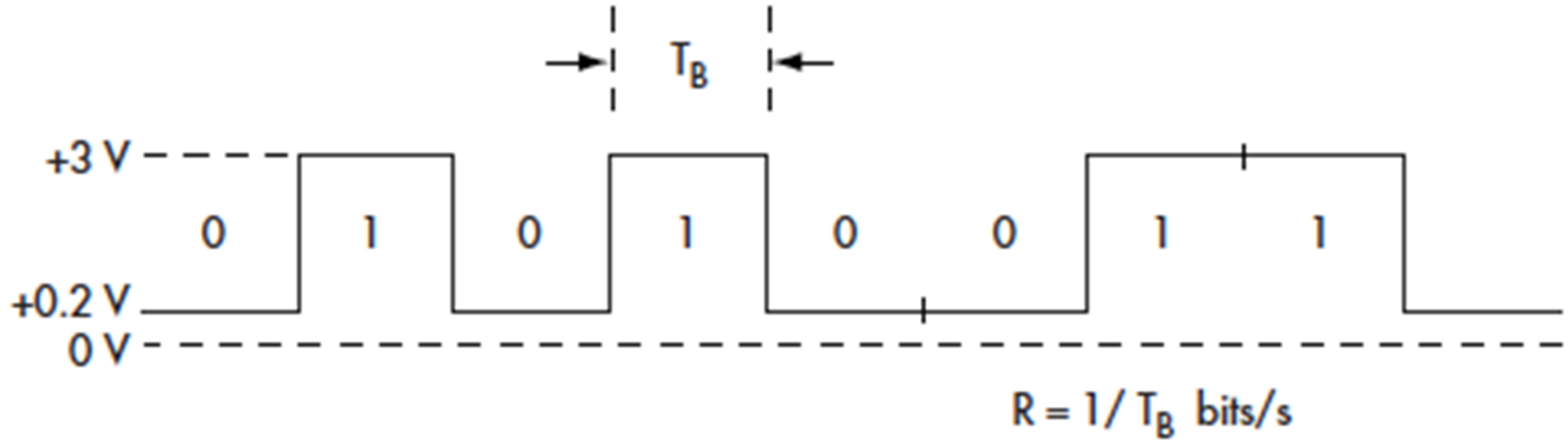
- Binary
  - » Binary definition – a numeral system with a base of two (0, 1)
  - » Binary digit is one bit
  - » Binary nibble is four bits
  - » Binary byte is eight bits or two nibbles
  - » Example:
    - – $11000110 = 1x2^7 + 1x2^6 + 0x2^5 + 0x2^4 + 0x2^3 + 1x2^2 + 1x2^1 + 0x2^0$ (198 Decimal)

Numbering Systems

- Hexadecimal
  - » Hexadecimal definition – a numeral system with a base of sixteen (0-9, A, B, C, D, E, F)
  - » Easier way to represent binary
    - – One hex digit represents four binary digits (nibble)
    - – Easily translatable to other numbering systems
    - – $C6_H$ = CH(12D)x16(D)^1 + 6(H/D)x16(D)^0 (198 Decimal)
    - – C6 = Cx16^1 + 6x16^0 (198 Decimal)
    - – C6 = 12x16^1 + 6x16^0

Numbering Systems

- It all looks the same on the wire. Previous numerical systems are only a way to describe the binary system. On vs Off



Numbering Systems

- Least significant bit / Most significant bit
- 1101 vs 1011 (13 or 11 decimal?)
- Least significant byte / Most significant byte
- C6 vs 6C (198 or 108 decimal)
- Least significant word / Most significant word
- 00 C6 vs C6 00 (198 vs 50,688)

Numbering Formats

- 12 bit integer = 4095 Unsigned
- 16 bit integer = 65535 Unsigned
- 32 bit integer = 4294967295 Unsigned
- 32 bit floating point ~ 10^{38}
- Signed / Unsigned
  - » MSB carries the sign
    - – 12 bit integer = -2048 to 2047
    - – 16 bit integer = -32768 to 32767
    - – 32 bit integer = -2147483648 to 2147483647

Numbering Interpretation / Scaling

» Why so much time spent on scaling for protocol discussion.
  - This is the single most common place mistakes are made.
  - Many people have an outlook that we can just figure it out on site, etc.
    - This takes more time
    - We don't have easy access to manufacture's docs
  - "Scaling isn't that big of a deal, what's the worst that can happen"
    - Wind park curtailed and thousands lost due to a 100 MW curtailment becoming a 10 MW curtailment
    - Generator tripped offline due to an overscale causing the generator logic to think it was seeing a negative number which 'purposely' called for the trip

Numbering Interpretation / Scaling

- Why so much time spent on scaling for protocol discussion.
  - This becomes very important:
    - As we move to more true SCADA automation; curtailment, load shedding, distribution automation
      - Real time $ decisions being made based using scaling
    - As we move to IEC61850 or others like it
      - Real time protection decisions being made using scaling

Distributed Network Protocol v3

- Early 1990s – Westronics -> GE-Harris
- Open standard
- DNP, DNP3, IEEE 1815-2012
- Client/Server (EMS/Outstation)
  - » Legacy terminology
- Serial or Ethernet options

DNP Pros and Cons

» Pros

- Object oriented which allows for more than just data value
  - Has timestamp capability
  - Has data quality built in
  - Has outstation (device) health built in (IIN bits)
- Has data integrity checks built in
  - CRC every 16 bytes
- Has server and client device addressing
- Included on many devices
- Capable of supporting 65520 addresses on one system (full 16 bits for address info)
- When configured correctly, message structure allows for very efficient communication, timing, etc.
- Secure Authentication
- Unsolicited responses

DNP Pros and Cons

» Cons

- Higher complexity than “simple” protocols
  - More “free-flowing”
  - Larger messages
  - Challenging to interpret
- DNP has provisions for security although many devices don’t utilize
- Difficult to troubleshoot
- CAN be very inefficient if incorrectly configured

DNP Details - Objects

» Data Types

– Object Based

- 01 → Binary Input
- 02 → Binary Input Change
- 10 → Binary Output
- 12 → Control Block
- 20 → Binary Counter
- 21 → Frozen Binary Counter
- 22 → Binary Counter Change
- 30 → Analog Input
- 32 → Analog Input Change

DNP Details - Variations

» Data Types

– Variations

- Object 32
- Var 0 → Analog Change (no specific variation)
- Var 1 → 32 Bit Analog Change Event Without Time
- Var 2 → 16 Bit Analog Change Event Without Time
- Var 3 → 32 Bit Analog Change Event With Time
- Var 4 → 16 Bit Analog Change Event With Time
- Var 5 → Short Float Bit Analog Change Event Without Time
- Var 6 → Long Float Bit Analog Change Event Without Time
- Var 7 → Short Float Bit Analog Change Event With Time
- Var 8 → Long Float Bit Analog Change Event With Time

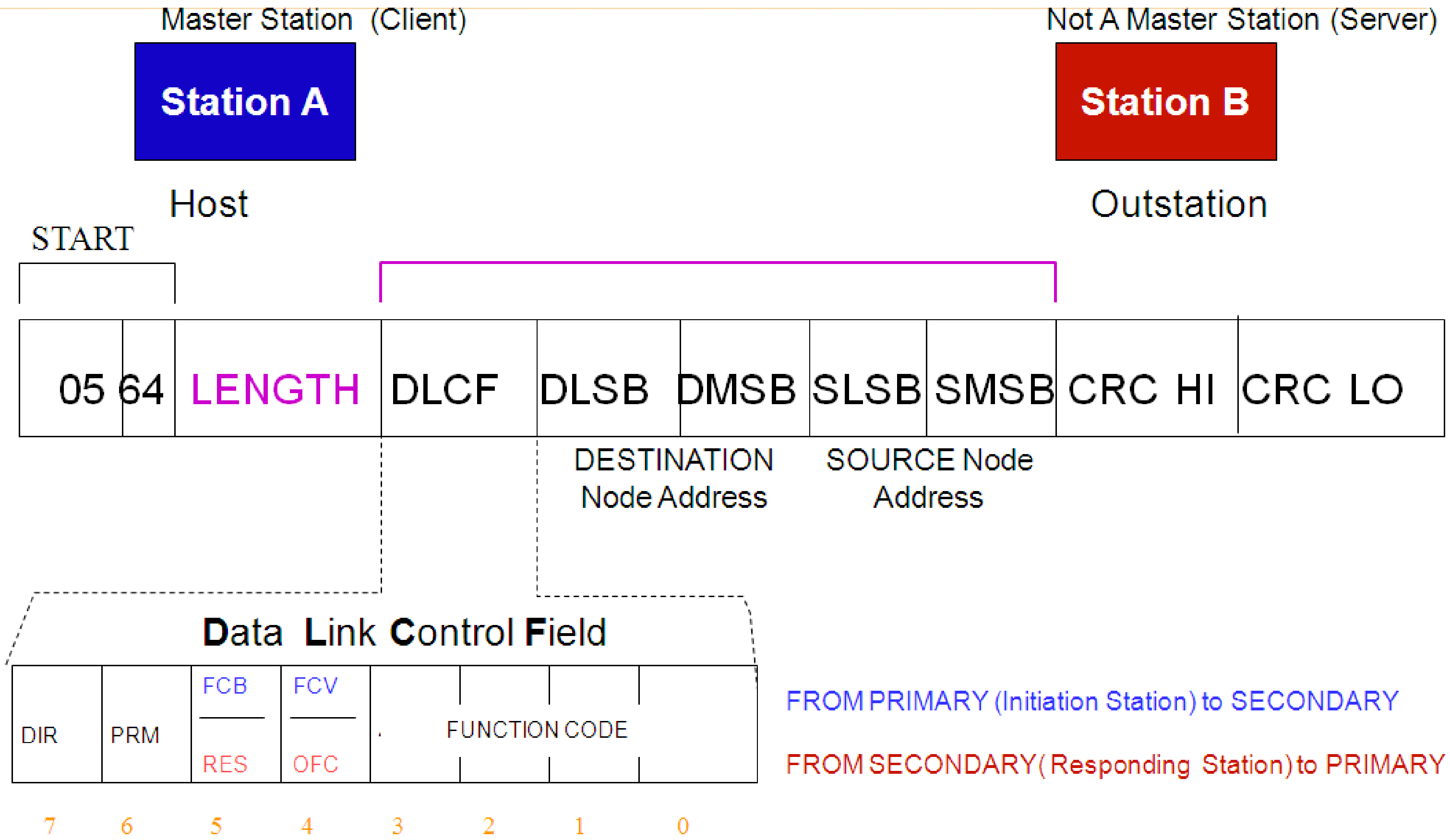
DNP Details - Deadbands

- So what's with all of this change 'stuff'
  - Event reporting
  - User configurable Δ before reporting an event change
  - Bandwidth management
  - Can lead to commissioning or operation issues if not set correctly.

DNP Details – Polling

- Integrity
- Event
- Classes
- Unsolicited

DNP Details – Message Structure



- This is the minimum DNP message Length (Block 0) and is a Length of 5 Octets (10 octets including START and CRC).

DNP Details – Message Structure

DATA LINK Control Field

DIR	PRM	FCB / RES	FCV / OFC	FUNCTION CODE			
7	6	5	4	3	2	1	0

FROM PRIMARY (Initiation Station) to SECONDARY

FROM SECONDARY (Responding Station) to PRIMARY

DIR = DIRECTION - 1 = From A to B 0 = From B to A
Frame direction with respect to the client.

PRM= Data Flow Control 1 = Frame from Initiating Station 0 = Frame from Responding Station
Initiation Frame or Responding Frame Designation.

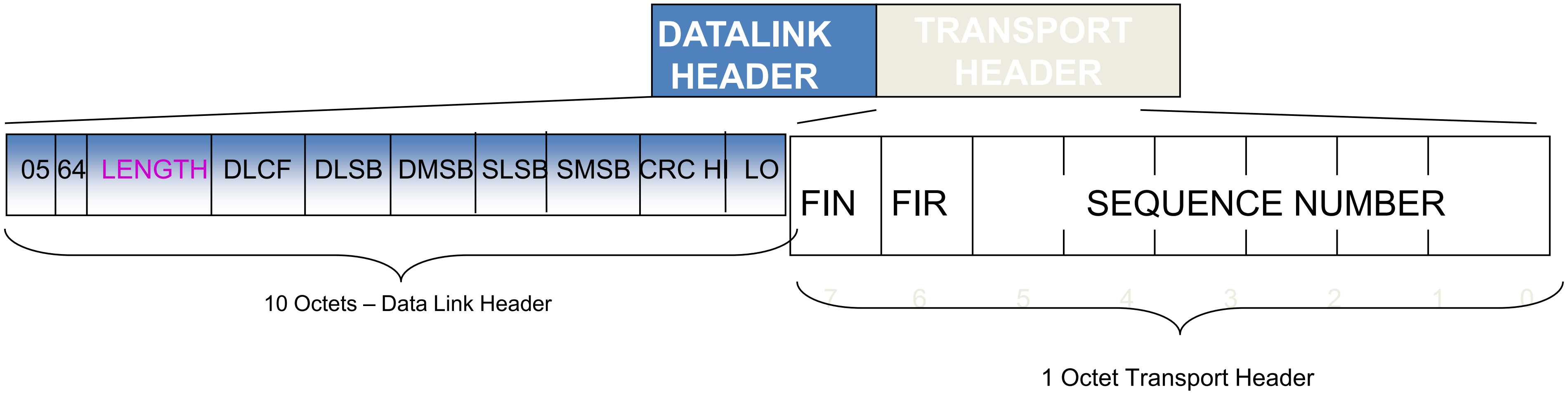
FCB = Frame Count Bit Toggles with each SEND/CONFIRM COMBINATION
(With Each Completed Host / Outstation transaction).
Indicates duplication or frame loss .

FCV = Frame Count Valid 1 = Frame Count Bit Valid 0 = Ignore Frame Count Bit.
Enables Function of Frame Count Bit. (Sent From Host)

RES = Reserved Bit - No Function Defined

DFC = Data Flow Control 1 = D L Buffer Overflow Condition in Receiving Station 0 = Primary Can Send Data.
Prevents Overflow of Data buffers in IED (Buffer Health Indication of Responding Station)

Transport Layer



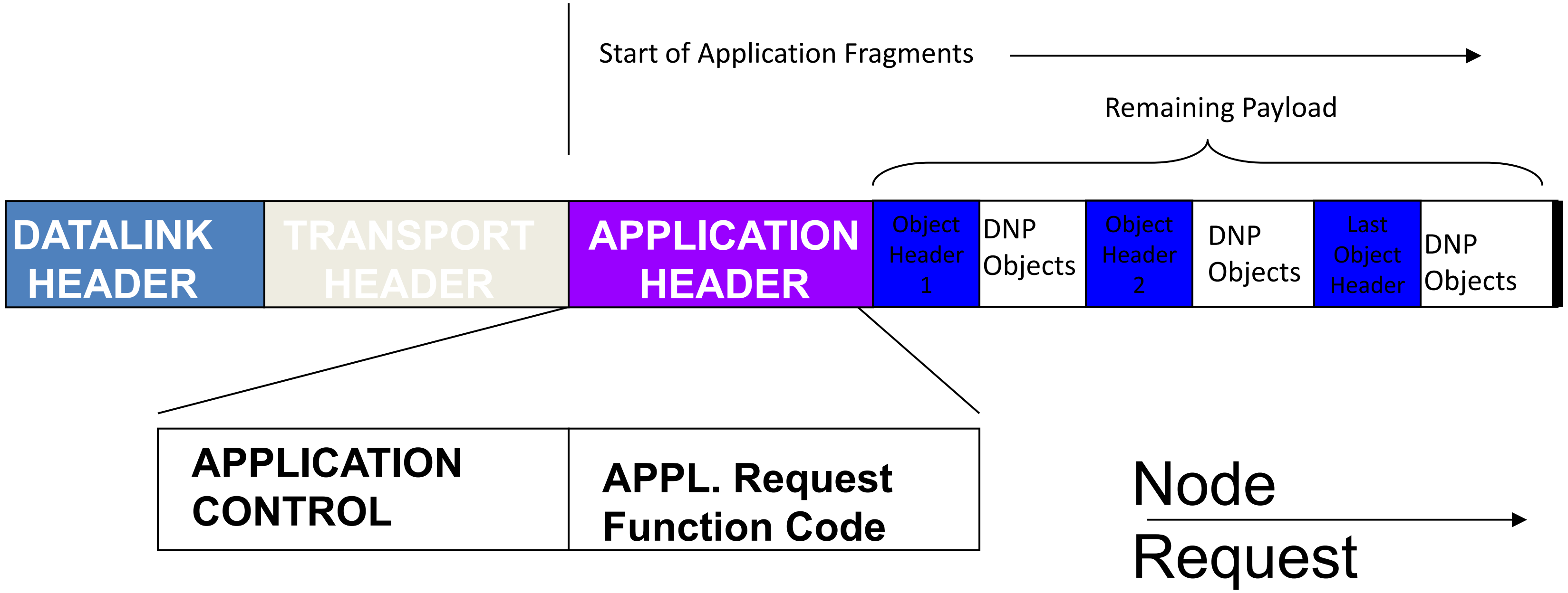
FIN = Final Indication 1 = FINal Frame in sequence 0 = More Frames Follow

FIR = FIRst Frame 1 = FIRst Frame In a Sequence 0 = Not The First Frame

0 <= Sequence Number <= 63 (Number rolls over if more frames than 63)

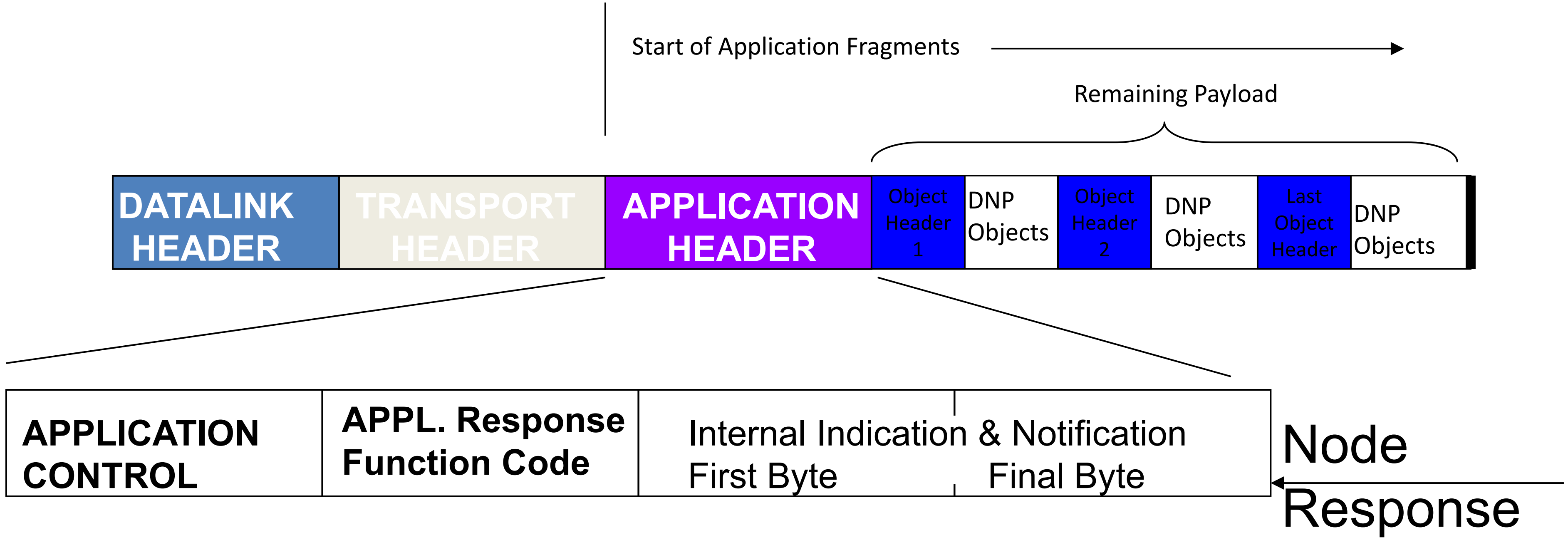
- Allows Primary and Secondary Devices to Assemble Multi-Fragment Messages.

Application Layer



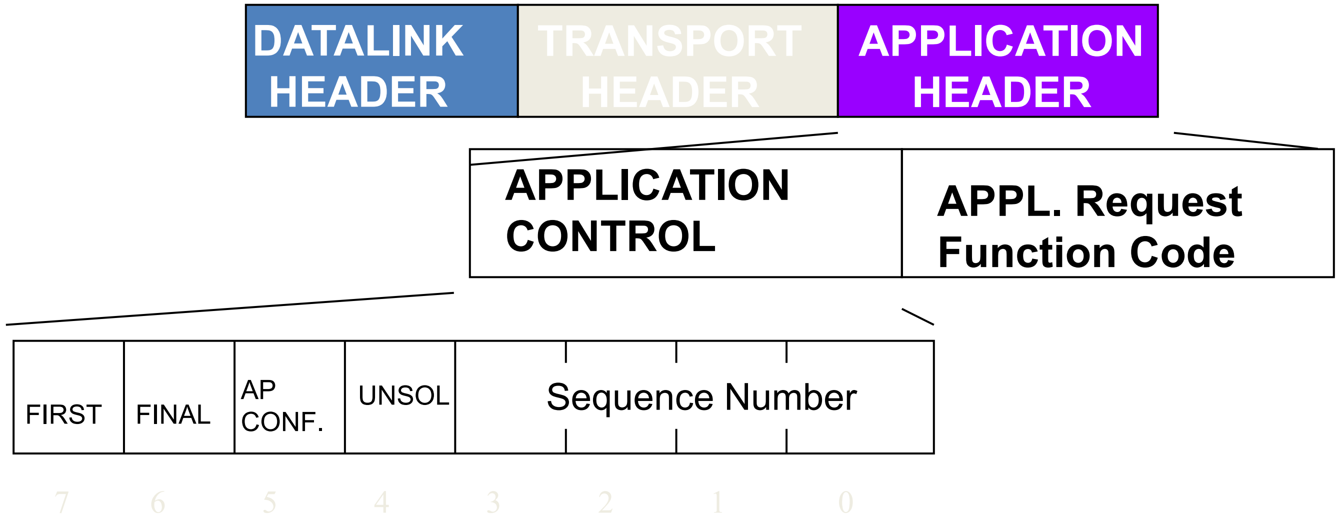
- Application Header is 2 Octets As Illustrated
- Application Fragment contains Individual Object Headers and Object Data

Application Layer



- Application Header is 2 Octets As Illustrated
- Application Fragment contains Individual Object Headers and Object Data

Application Header (Request)



FIN = Final Indication 1 = FINal Fragment in sequence 0 = More Fragments Follow

FIR = FIRst Frame 1 = First Fragment In a Sequence 0 = Not The First Fragment

AP CONF. = Application Confirm 1 = Ap Layer Confirm Expected 0 = No Ap Layer Confirm Expected.

UNSOL = Unsolicited 1 = Unsolicited Message 0 = Polled Message

SEQUENCE NUMBER 0 <= X<= 15 – Sequence Fragment Number (Rollover at 15)

DNP Details – Device Health/Internal Indications

» Internal Indications (IIN)

IIN1.0 ALL_STATIONSAn all-stations message was received.
IIN1.1 CLASS_1_EVENTS The RTU has unreported class 1 events.
IIN1.2 CLASS_2_EVENTS The RTU has unreported class 2 events.
IIN1.3 CLASS_3_EVENTS The RTU has unreported class 3 events.
IIN1.4 NEED_TIME Time synchronization is required.
IIN1.5 LOCAL_CONTROL One or more of the points are in local control
IIN1.6 DEVICE_TROUBLE An abnormal, device-specific condition exists
IIN1.7 DEVICE_RESTART The RTU restarted.
IIN2.0 NO_FUNC_CODE_SUPPORT-The RTU does not support this function code.
IIN2.1 OBJECT_UNKNOWN RTU does not support requested operation for objects in the request.
IIN2.2 PARAMETER_ERROR A parameter error was detected.
IIN2.3 EVENT_BUFFER_OVERFLOW -An event buffer overflow condition exists in the RTU and at least one unconfirmed event was lost.
IIN2.4 ALREADY_EXECUTING The operation requested is already executing. Support is optional.
IIN2.5 CONFIG_CORRUPT The outstation detected corrupt configuration. Support is optional.
IIN2.6, 7 RESERVED_2 , _1 Reserved for future use. Always set to 0.

DNP Details – Message Example

- Query
  - 05 64 14 C4 01 00 65 00 **29 7D**
  - DE CE 01 3C 04 06 3C 03 06 3C 02 06 3C 01 06 **EE 5D**
    - 05 64 // start
    - 14 // length (not including CRC)
    - C4 // data link control field
    - 01 00 // destination device address
    - 65 00 // source device address
    - **29 7D // CRC**

DNP Details – Message Example

- Query
  - 05 64 14 C4 01 00 05 00 2B 25
  - DE CE 01 3C 04 06 3C 03 06 3C 02 06 3C 01 06 **EE 5D**
    - DE CE // Transport Header / Application Control
    - 01 // Application Function (Read)
    - 3C 04 06//Obj60 (class),Var4(class 3), Qual6(all points)
    - 3C 03 06//Obj60 (class),Var4(class 2), Qual6(all points)
    - 3C 02 06//Obj60 (class),Var4(class 1), Qual6(all points)
    - 3C 01 06//Obj60 (class),Var4(class 0), Qual6(all points)
    - **EE 5D // CRC**

DNP Details – Message Example

- Response
  - 05 64 FF 44 65 00 01 00 **17 ED**
  - 64 EE 81 00 00 20 02 17 14 10 01 3A 0E 11 01 2C EA BF
  - 06 17 01 A7 00 1C 01 A3 00 2F 01 F6 F1 30 01 E7 4D 90
  - F8 31 01 7C 03 06 01 D2 0D 25 01 EB F1 26 01 F6 31 C5
  - F8 10 01 4B 0E 11 01 3F 06 1C 01 A7 00 2F 01 ED 09 1B
  - F1 30 01 EE F8 06 01 B6 0D 07 01 72 06 22 01 A3 66 0D
  - 00 25 01 FA F1 26 01 04 F9 01 02 00 00 EF 01 81 21 12
  - 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 74 13
  - 01 01 01 01 01 01 01 01 01 01 01 01 81 01 01 01 67 CF
  - 01 01 01 01 01 01 01 01 01 01 81 01 01 01 01 01 38 D2
  - 81 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 B7 F4
  - 81 81 81 81 01 01 01 01 01 01 01 01 01 81 01 01 86 E7
  - 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 BB C3
  - 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 74 13
  - 01 01 01 01 01 01 01 01 01 81 01 01 01 01 01 01 F4 3F
  - 01 01 01 01 01 01 01 81 01 01 01 01 01 81 01 01 15 9D
  - 01 01 01 01 01 01 01 01 01 01 8D 7B
    - 05 64 // start
    - FF // length (not including CRC)
    - 44 // data link control field
    - 65 00 // destination device address
    - 01 00 // source device address
    - **17 ED // CRC**

DNP Details – Message Example

- 05 64 FF 44 65 00 01 00 17 ED
- 64 EE 81 00 00 20 02 17 14 10 01 3A 0E 11 01 2C **EA BF**
- 06 17 01 A7 00 1C 01 A3 00 2F 01 F6 F1 30 01 E7 **4D 90**
- F8 31 01 7C 03 06 01 D2 0D 25 01 EB F1 26 01 F6 **31 C5**
- F8 10 01 4B 0E 11 01 3F 06 1C 01 A7 00 2F 01 ED **09 1B**
- F1 30 01 EE F8 06 01 B6 0D 07 01 72 06 22 01 A3 **66 0D**
- 00 25 01 FA F1 26 01 04 F9 01 02 00 00 EF 01 81 **21 12**
- 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 **74 13**
- 01 01 01 01 01 01 01 01 01 01 01 01 81 01 01 01 **67 CF**
- 01 01 01 01 01 01 01 01 01 01 81 01 01 01 01 01 **38 D2**
- 81 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 **B7 F4**
- 81 81 81 81 01 01 01 01 01 01 01 01 01 81 01 01 **86 E7**
- 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 **BB C3**
- 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 **74 13**
- 01 01 01 01 01 01 01 01 01 81 01 01 01 01 01 01 **F4 3F**
- 01 01 01 01 01 01 01 81 01 01 01 01 01 81 01 01 **15 9D**
- 01 01 01 01 01 01 01 01 01 01 8D 7B
  - 64 EE // Transport Header / Application Control
  - 81 // Application Function (Read)
  - 00 00//Internal Indications
  - 20 02 17 // Object/Variation/Qualifier
  - 14// Number of objects returned
  - 10 (index) 01 (quality) 3A 0E (value) // Index Flag, Value
  - **EA BF // CRC**

DNP Details – Message Example

- 05 64 FF 44 65 00 01 00 17 ED
- 64 EE 81 00 00 20 02 17 14 10 01 3A 0E 11 01 2C **EA BF**
- 06 17 01 A7 00 1C 01 A3 00 2F 01 F6 F1 30 01 E7 **4D 90**
- F8 31 01 7C 03 06 01 D2 0D 25 01 EB F1 26 01 F6 **31 C5**
- F8 10 01 4B 0E 11 01 3F 06 1C 01 A7 00 2F 01 ED **09 1B**
- F1 30 01 EE F8 06 01 B6 0D 07 01 72 06 22 01 A3 **66 0D**
- 00 25 01 FA F1 26 01 04 F9 01 02 00 00 EF 01 81 **21 12**
- 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 **74 13**
- 01 01 01 01 01 01 01 01 01 01 01 01 81 01 01 01 **67 CF**
- 01 01 01 01 01 01 01 01 01 01 81 01 01 01 01 01 **38 D2**
- 81 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 **B7 F4**
- 81 81 81 81 01 01 01 01 01 01 01 01 01 81 01 01 **86 E7**
- 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 01 **BB C3**
- 01 01 01 81 01 01 01 01 01 01 01 01 01 01 01 01 **74 13**
- 01 01 01 01 01 01 01 01 01 81 01 01 01 01 01 01 **F4 3F**
- 01 01 01 01 01 01 01 81 01 01 01 01 01 81 01 01 **15 9D**
- 01 01 01 01 01 01 01 01 01 01 8D 7B
  - 11 (index) 01 (flag) 2C 06 (value) // Index Flag, Value
  - 17 (index) 01 (flag) A7 00 (value) // Index Flag, Value
  - 1C (index) 01 (flag) A3 00 (value) // Index Flag, Value
  - 2F (index) 01 (flag) F6 F1 (value) // Index Flag, Value
  - **4D 90 // CRC**

What Questions Do You Have?

- Thank you for your attention.