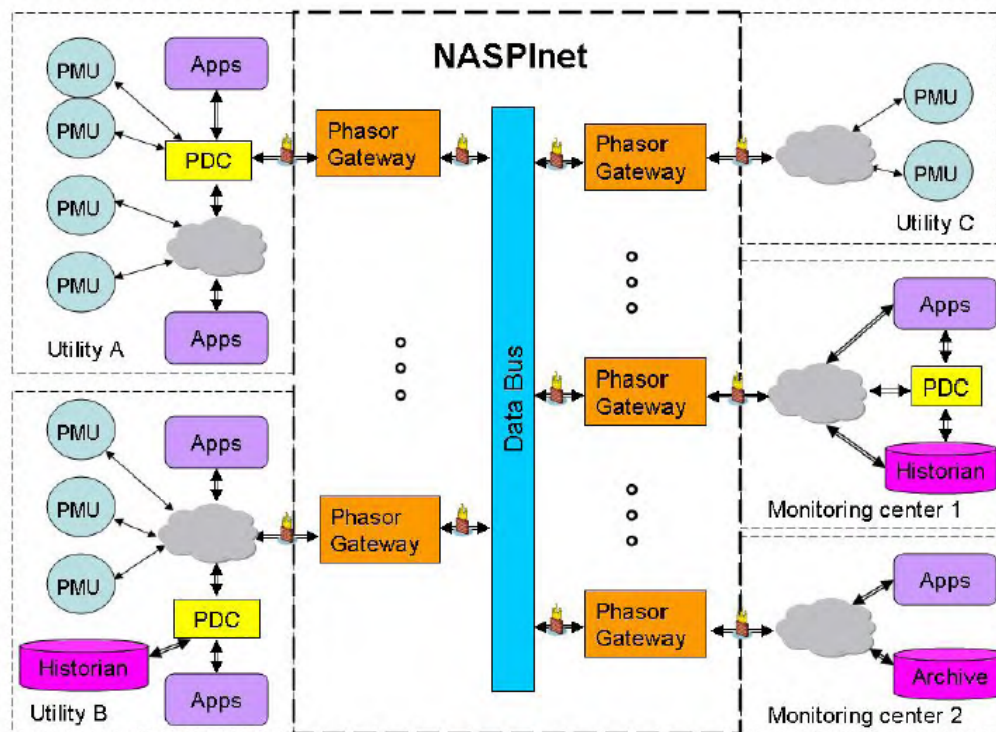


An Overview of the New IEC 61850 Synchrophasor Publish-Subscribe Profile

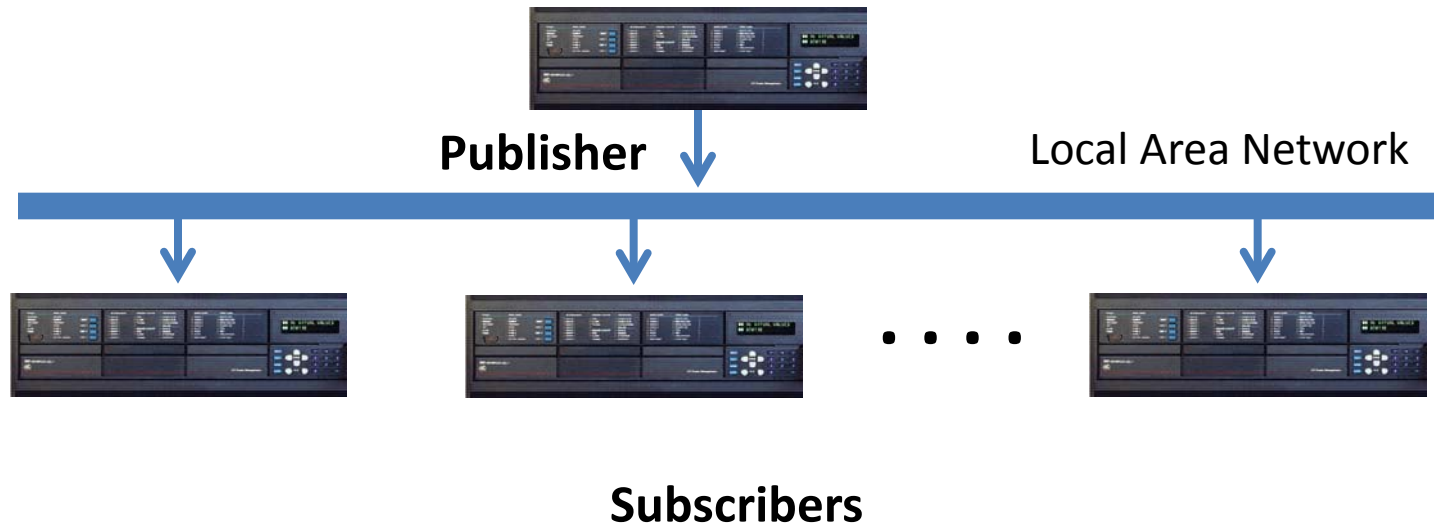
Mark Adamiak
Drew Baigent
GE Grid Automation

Herb Falk
SISCO

Vahid Madani
PG&E



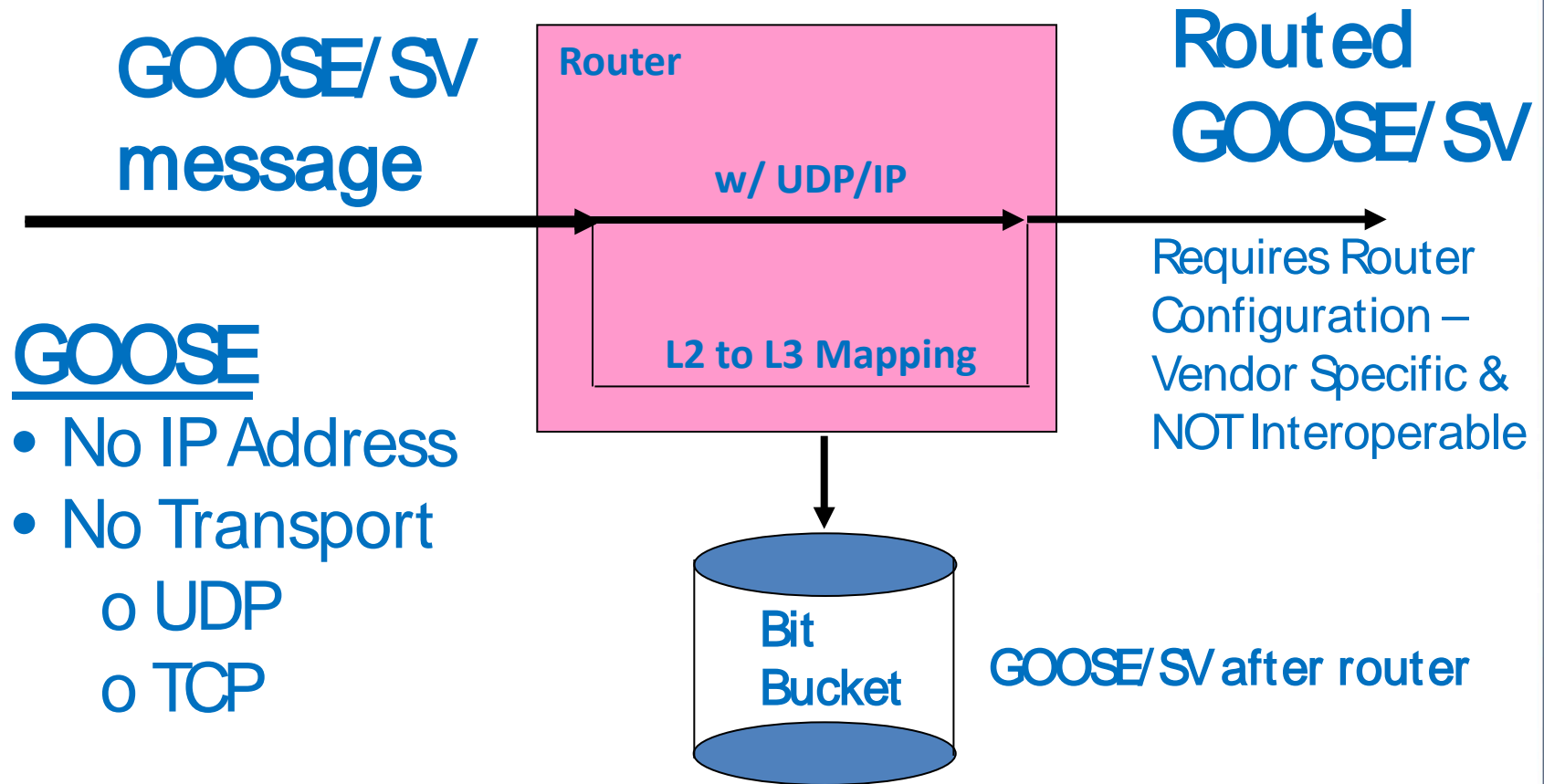
Original Multicast GOOSE



Only Devices on the same LAN and VLAN Received the Message



GOOSE at a Router:

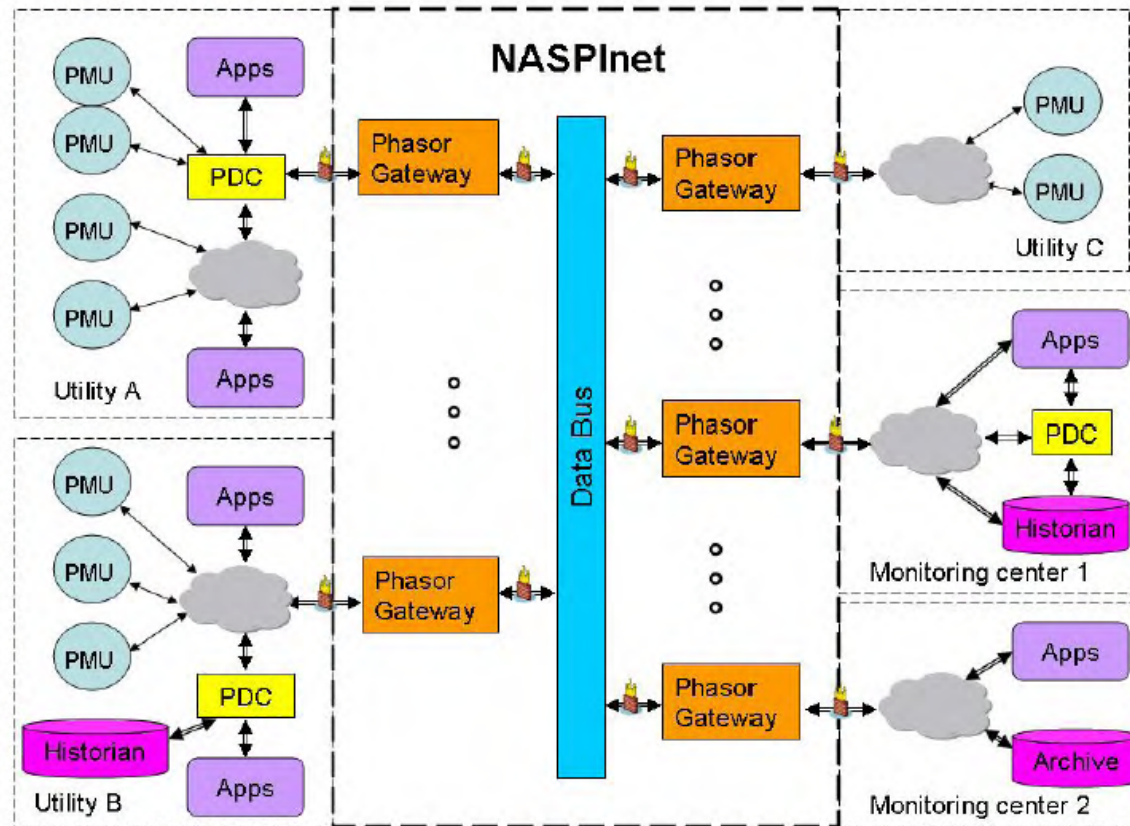


Changing Communication Needs

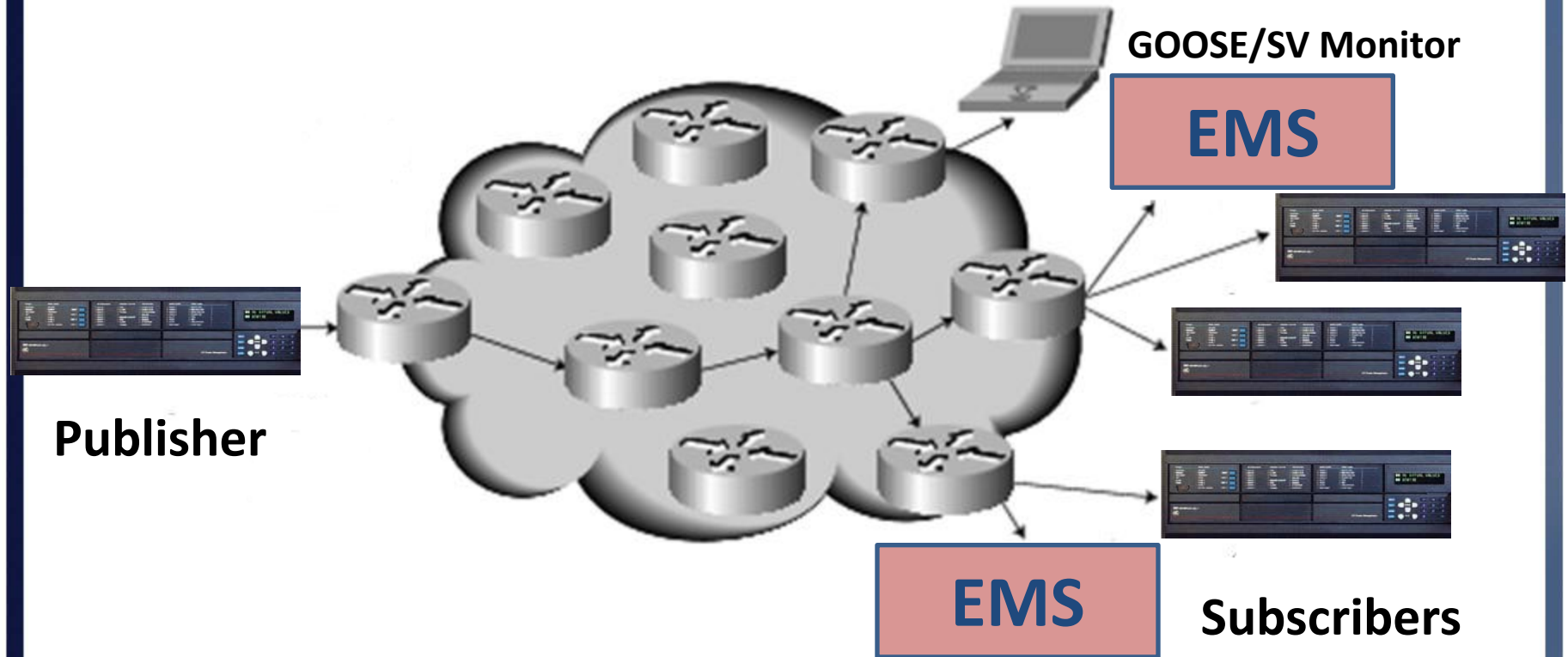
- Substation-to-Substation Communication
- Real-Time streaming of System State
 - Synchrophasors
- Utility-Utility Data Sharing
- Need for End-to-End Security



North American SynchroPhasor Initiative Network: NASPInet



Networked Function-to-Function Communication Use Case



Synchrophasor Communication as defined in IEEE C37.118

- No defined security
 - Requires an external solution
 - Multicast Implementation and associated security not defined
- Dataset Configuration tools are vendor specific
- No standard data names
- Limitations on dataset name length
- Rejected by IEC TC57 61850 WG as Dual Logo Standard



Communication NEEDS:

Networked Publish/Subscribe Message

- Should be routable
 - Multicast to reach multiple subscribers
- Message should be authenticated
- Message should be able to be encrypted
- Should accommodate large message size
- Should manage the Authentication and Encryption key



Committee Approved Technical Report:

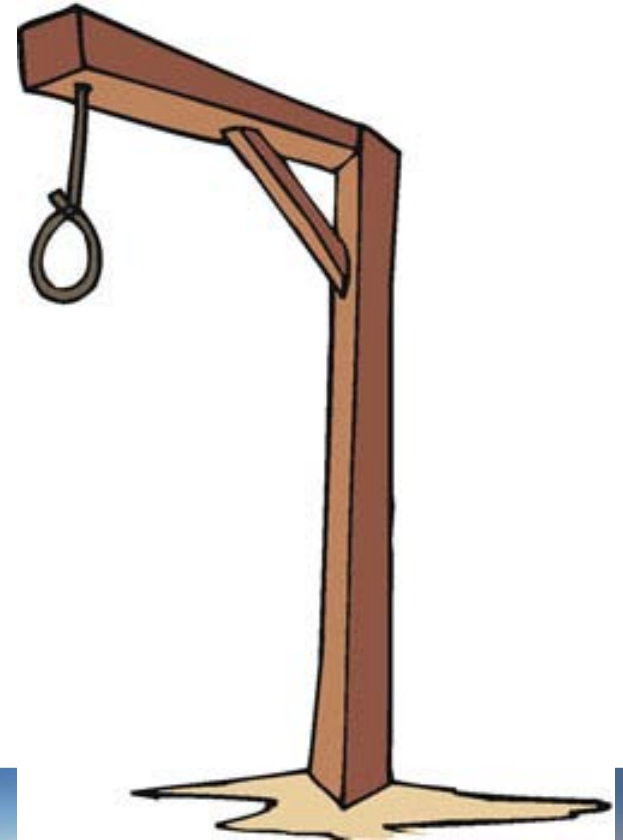
**IEC 61850:
COMMUNICATION NETWORKS AND
SYSTEMS FOR POWER UTILITY
AUTOMATION –**

**Part 90-5: Use of IEC 61850 to transmit
synchrophasor information according to
IEEE C37.118**



Mark's Proposed name for IEC 90-5: **Networked Object Oriented Substation Event**

The NOOSE !



But people got hung up on the
idea...

So we have:

- R-GOOSE (for Routed GOOSE)
 - ✓ For routing of Event Data

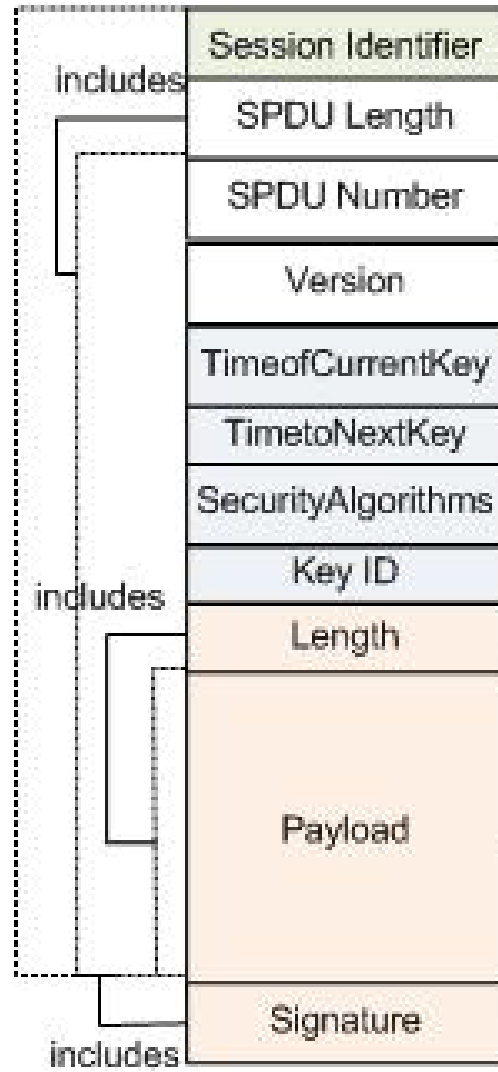
And

- R-SV (for Routed Sample Values)
 - ✓ For routing periodic data



IEC 90-5 Data Model

SPDU:
Session
Protocol
Data
Unit



Detail Format

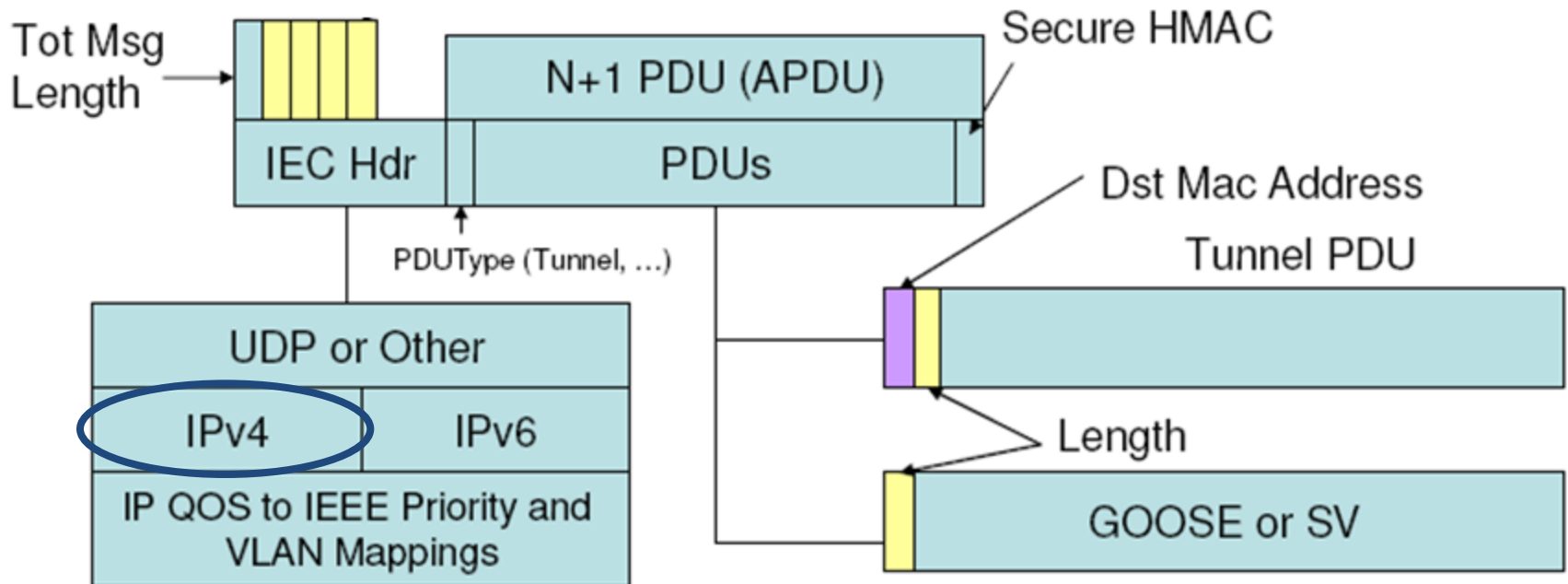
Total Max Size:

- 65535 bytes
- Segmented by IP

Supports Multiple
non-time-aligned PMU
datasets – per 61850-9-2



61850 90-5 Networked GOOSE/SV



An Implementation Agreement has been Created to Define the mapping of Synchrophasors into 90-5



Implementation Agreement Dataset

- Synchrophasor STATUS word
 - 16 bit Unsigned Integer
 - Semantics from C37.118
- Frequency and ROCOF
- Synchrophasors – Polar format ONLY
- Analog Values
- Digital Status – 16 bit Unsigned Integer

***All Measurements* in Float32 Format**
Now part of an IEEE PSRC Working Group

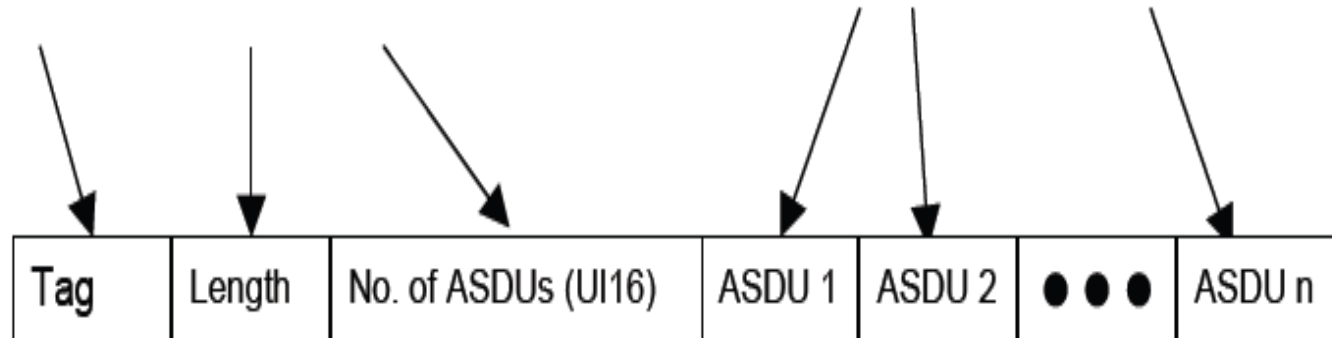


Reliable Transport through Repeat

APCI

(Application – Protocol Control Information)

ASDU's (Application – Service Data Unit)



APDU (Application – Protocol Data Unit)

ASDU1 – Oldest data

ASDUn – Newest data

n is a user-settable parameter



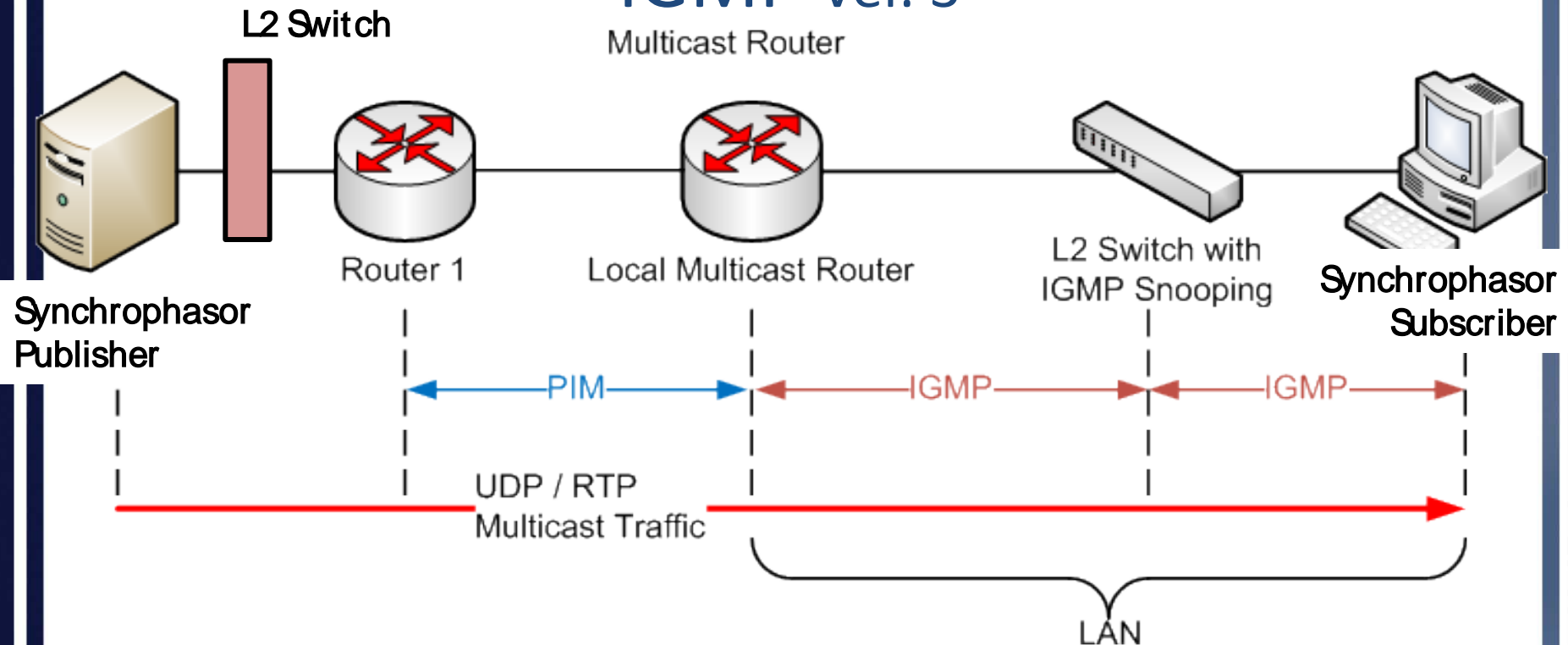
Routing Priority via the IP Differentiated Services byte

Bit #:	0	1	2	3	4	5	6	7
Value:	1	0	1	1	1	0	0	0
DSCP						ECN		

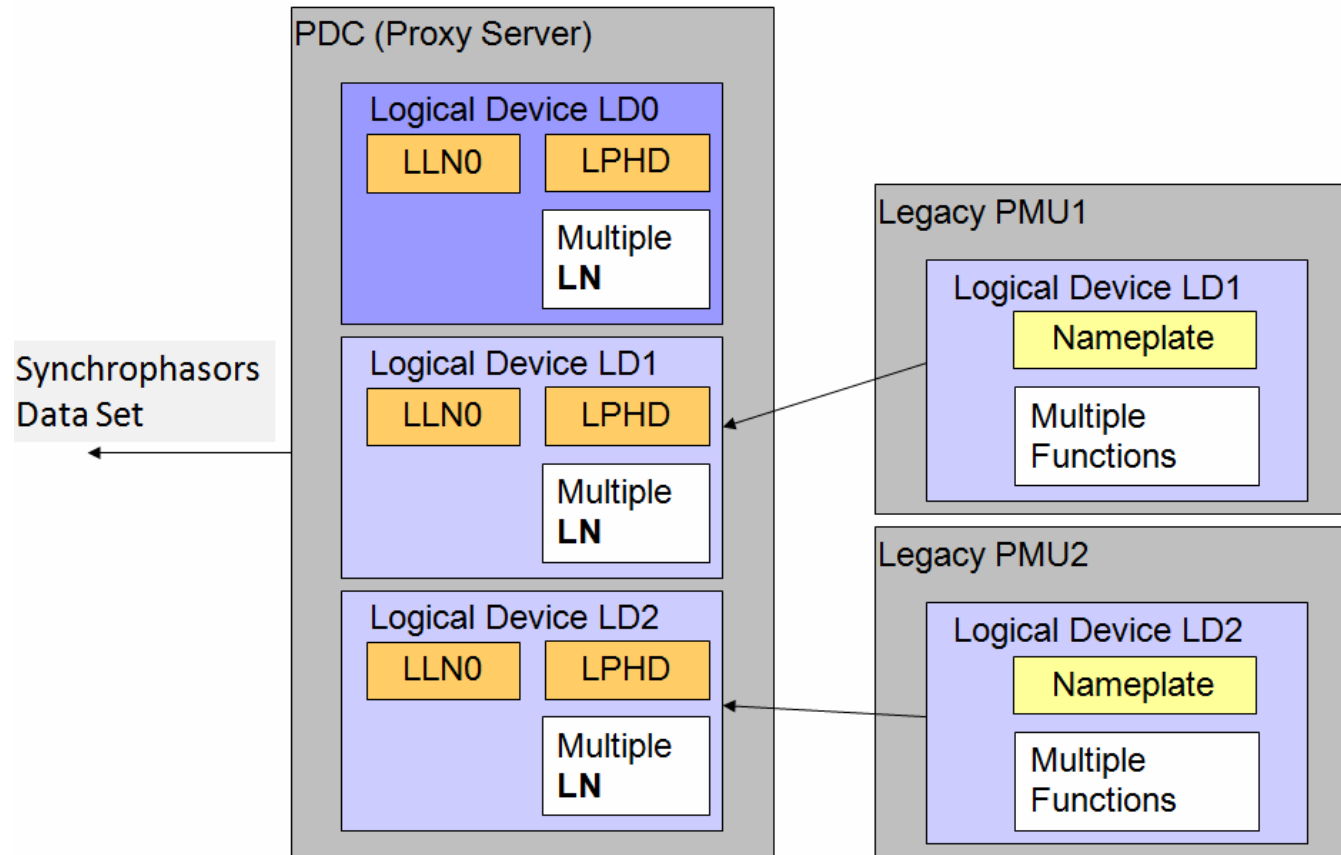
- DSCP - Differentiated Service Code Point
 - set for Expedited Forwarding (0x2E)
- ECN – Explicit Congestion Notification
 - Set by the routers if enabled
- Overall byte value: 0xB8



Multicast Path Establishment via Internet Gateway Management Protocol – IGMP Ver. 3



PMU to PDC Mapping Via Self-Description / XML File

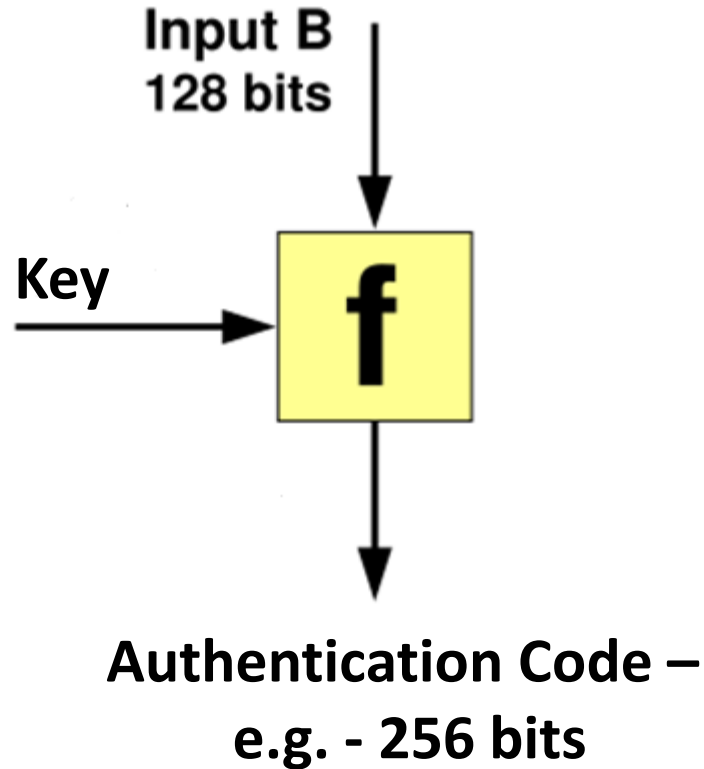


Security Definition in 90-5

- Defines a Secure Hash Algorithm - SHA2 Hash code for message authentication / integrity
- Defines AES as the encryption algorithm
- Identifies / Extends a Key management system
 - RFC 3547 The Group Domain of Interpretation
 - The publisher manages the keys to all subscribers
 - Same key for Hash and Encryption



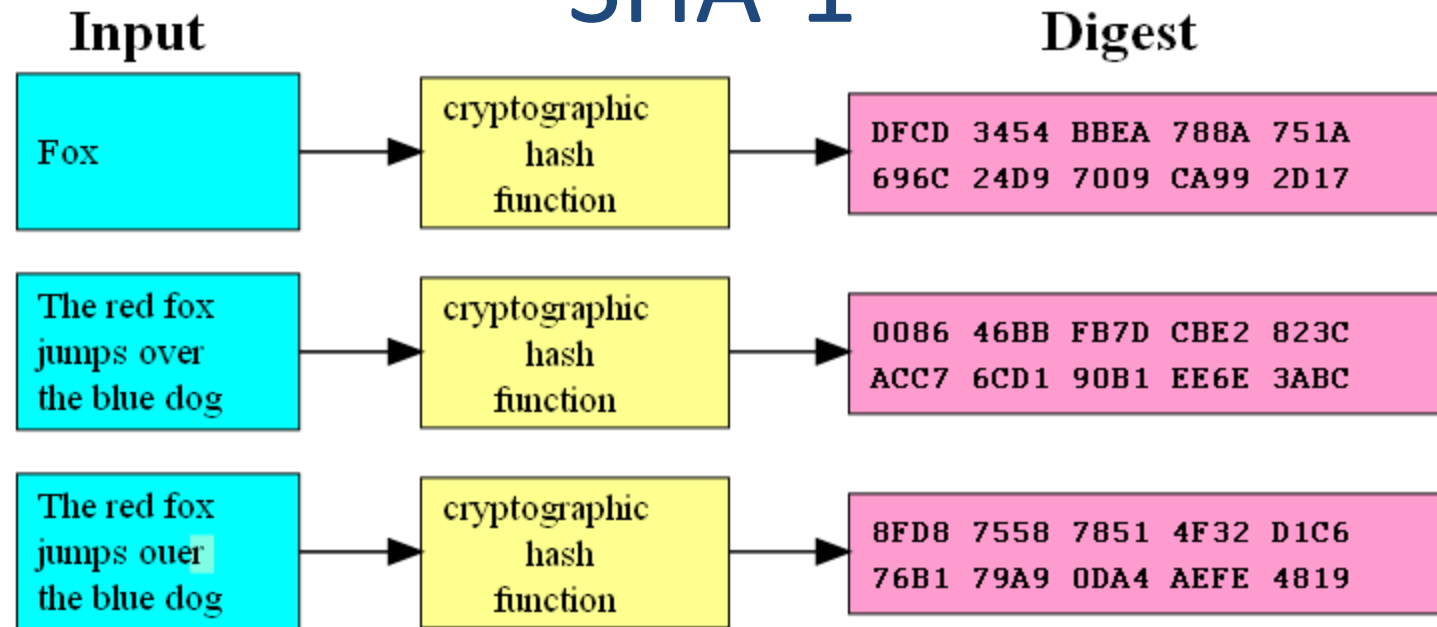
Hash/Digest: One-way Compression



Similar to a CRC – only longer and computed with a Key



Example of Hash Outputs from SHA-1*

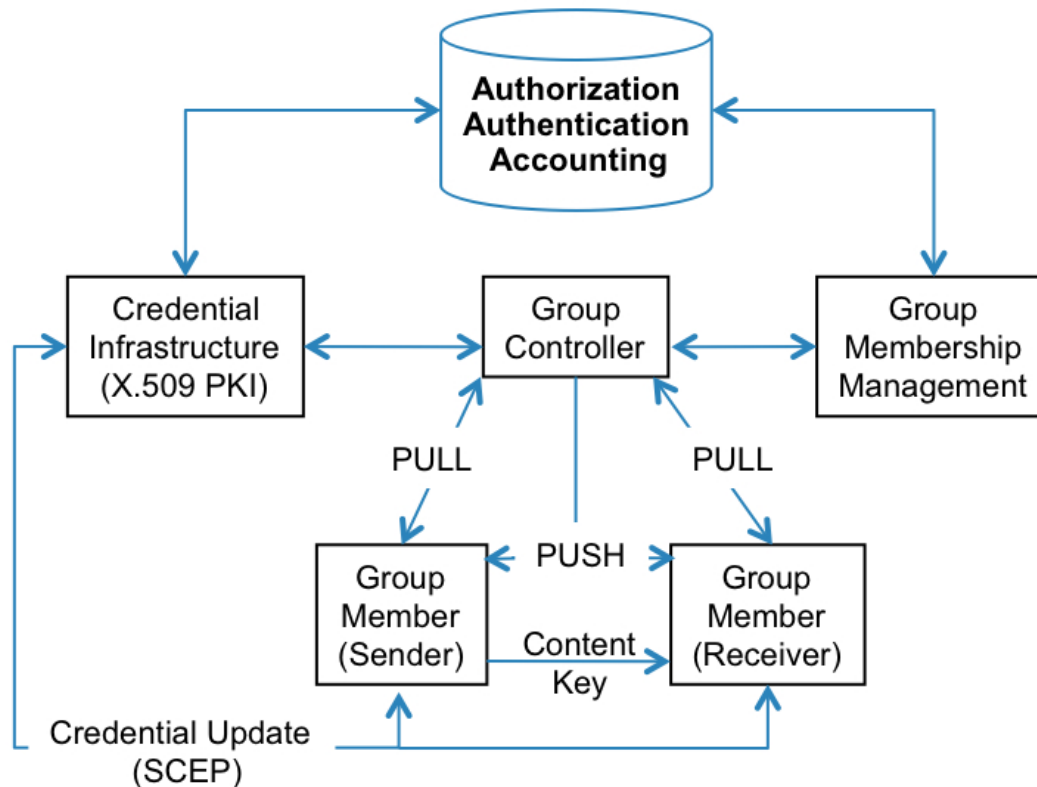


- Digest Output Size is Independent of Input data Size
- Change in ONE character results in RADICAL change in Hash

* SHA-1 now deprecated due to vulnerabilities



Key Distribution: Group Domain of Interpretation - GDOI



Group Members “Pull” new keys from the Controller



Conclusions

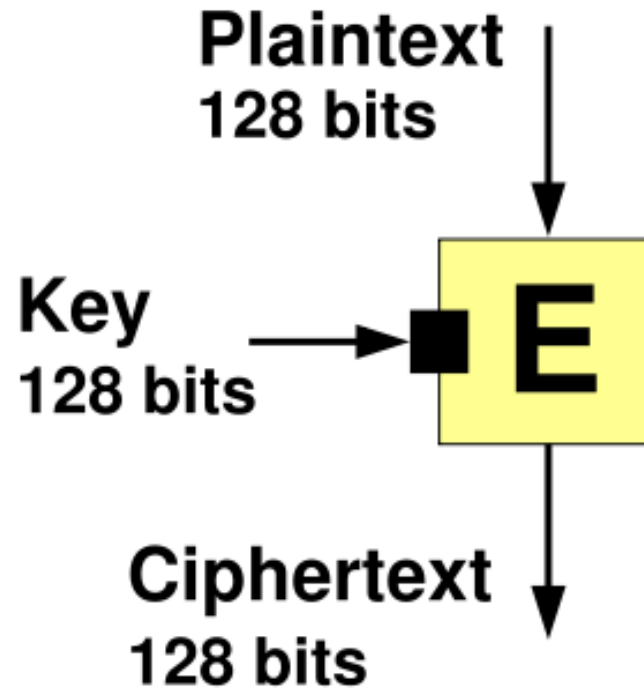
- IEC61850 has demonstrated its capability to meet the needs of next generation communication functionality
- End-to-End security can now be implemented as part of GOOSE and Sample Value Messages



Backup Material



Block Cypher Concept



AES Works on 128 Bit blocks of data

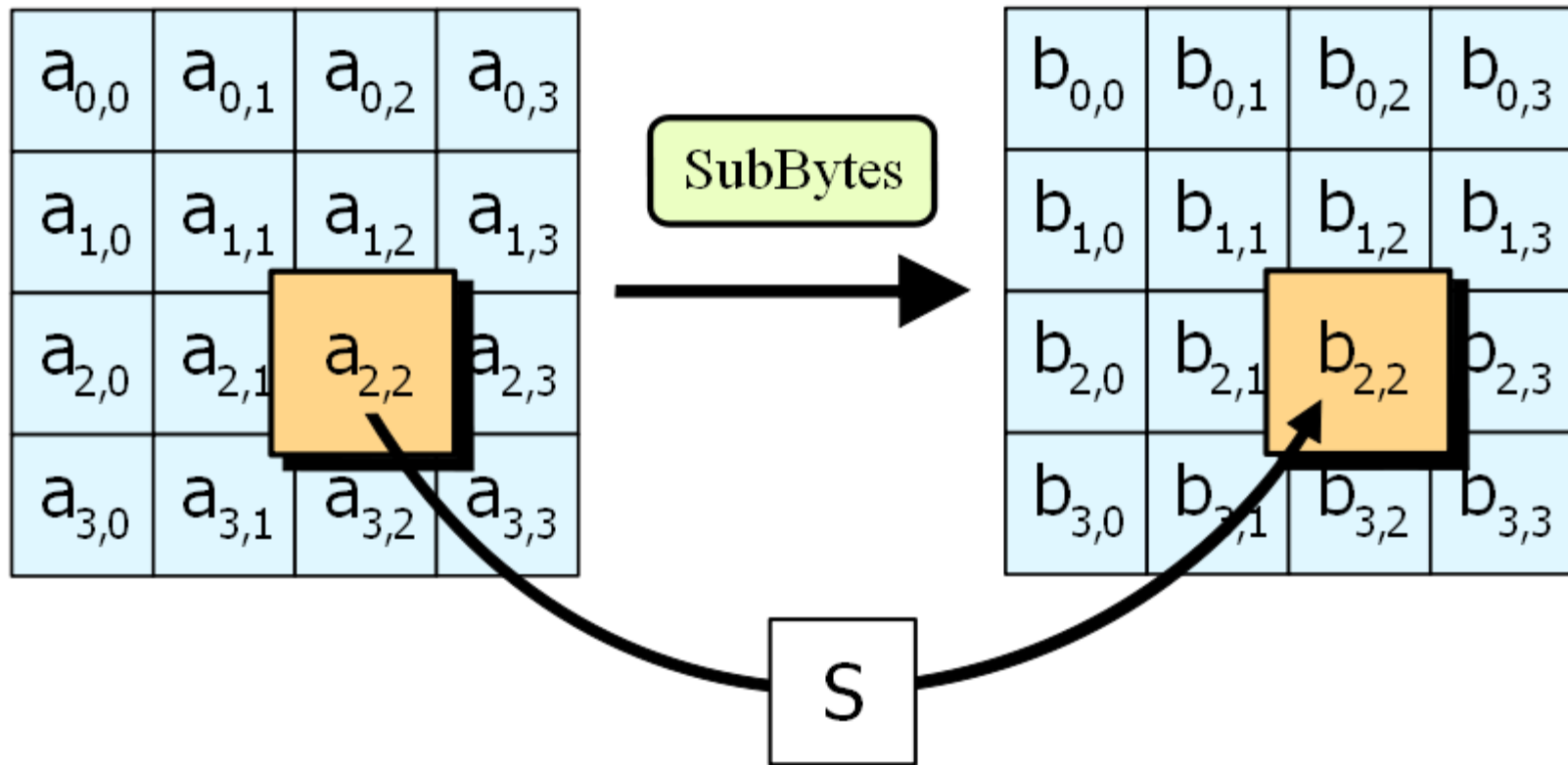


Packet Encryption via: Advanced Encryption Standard (AES)

- **AES Encryption Package**
- the Advanced Encryption Standard (AES) **encryption package**, also known as Rijndael, is a block cipher adopted as an encryption standard by the US government. The National Institute of Standards and Technology (NIST) established the new Advanced Encryption Standard (AES) specification on May 26, 2002.
- The AES **encryption package** is a cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes).
- AES is the successor to the older Data Encryption Standard (DES). DES was approved as a Federal standard in 1977 and remained viable until 1998 when a combination of advances in hardware, software, and cryptanalysis theory allowed a DES-encrypted message to be decrypted in 56 hours. Since that time numerous other successful attacks on DES-encrypted data have been made and DES is now considered past its useful lifetime.
- The AES algorithm is based on permutations and substitutions. Permutations are rearrangements of data, and substitutions replace one unit of data with another. AES performs permutations and substitutions using several different techniques.
- The AES **encryption package** will certainly become a de facto standard for encrypting all forms of electronic information, replacing DES. AES-encrypted data is unbreakable in the sense that no known cryptanalysis attack can decrypt the AES cipher text without using a brute-force search through all possible 256-bit keys.



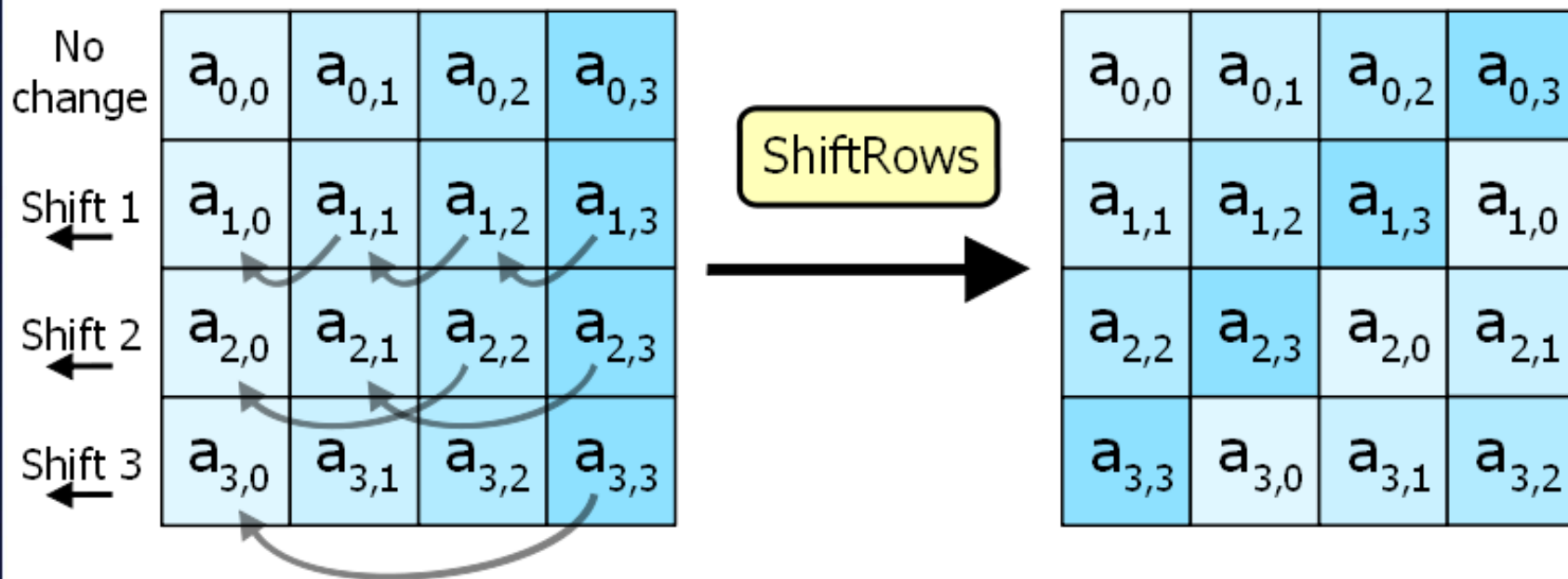
AES Step 1 – Substitute Bytes



In the SubBytes step, each byte in the state is replaced with its entry in a fixed 8-bit lookup table, S ; $b_{ij} = S(a_{ij})$.



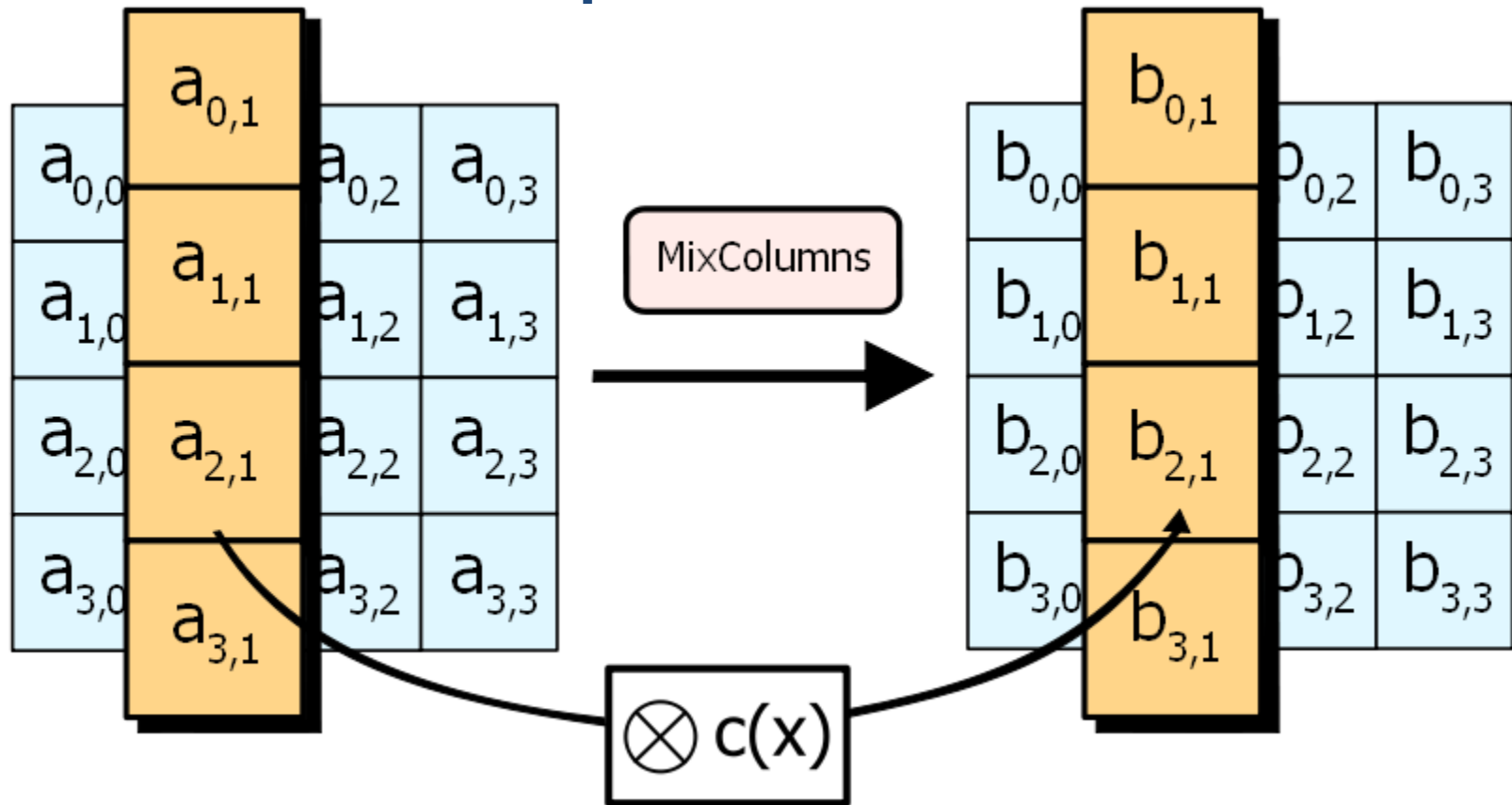
AES – Step 2 – Shift Rows



In the ShiftRows step, bytes in each row of the state are shifted cyclically to the left. The number of places each byte is shifted differs for each row.



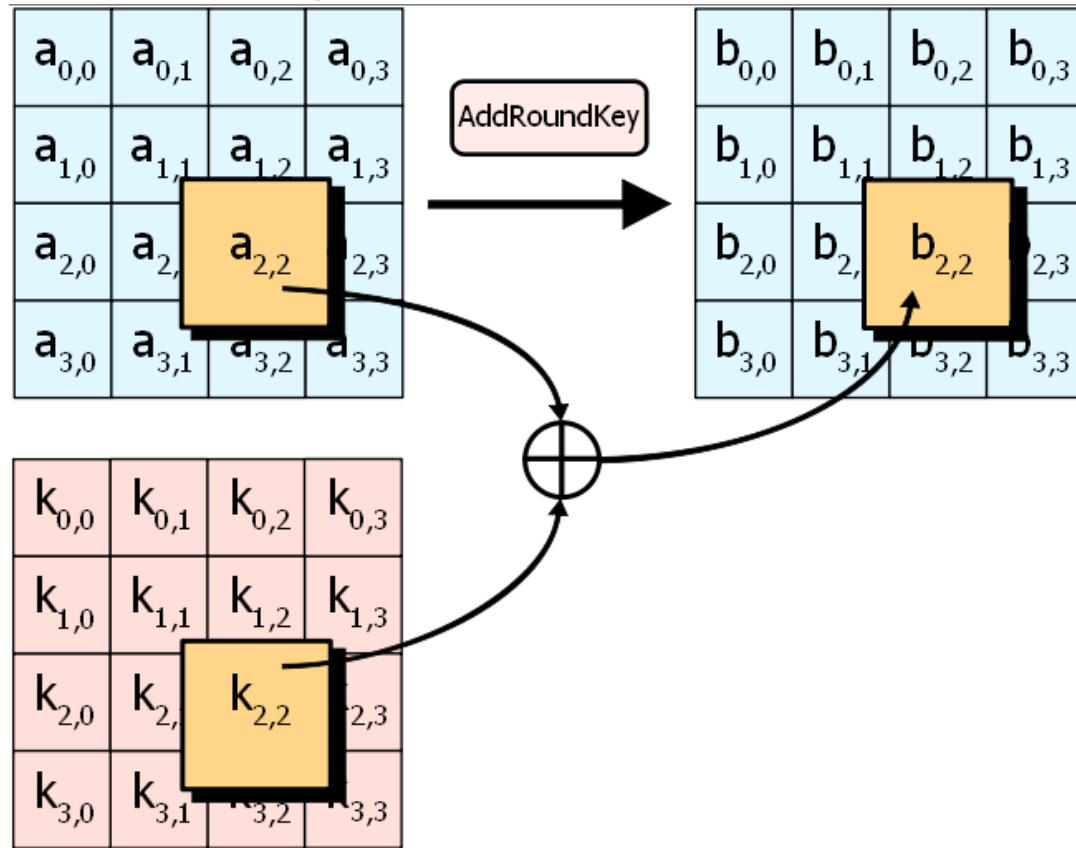
AES – Step 3 – Mix Columns



In the MixColumns step, each column of the state is multiplied with a fixed polynomial $c(x)$.



AES – Step 4 – Add round Key



In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (\oplus).



Multicast Addresses

Class D Address	Purpose
224.0.0.1	All hosts on a subnet
224.0.0.2	All routers on a subnet
224.0.0.4	All DVMRP routers
224.0.0.5	All MOSPF routers
224.0.0.9	Routing Information Protocol (RIP)-Version 2
224.0.1.1	Network Time Protocol (NTP)
224.0.1.2	SGI Dogfight
224.0.1.7	Audio news
224.0.1.11	IETF audio
224.0.1.12	IETF video
224.0.0.13	Protocol Independent Multicasting (PIM ₁)

1 – CISCO Recommended

Payload

- Consists of Multiple IEC 61850-9-2 Protocol Data Units (PDUs)
- PDU consists of:
 - Header
 - Dataset

An Implementation Agreement has been developed to “agree” to the items in the Header and Dataset



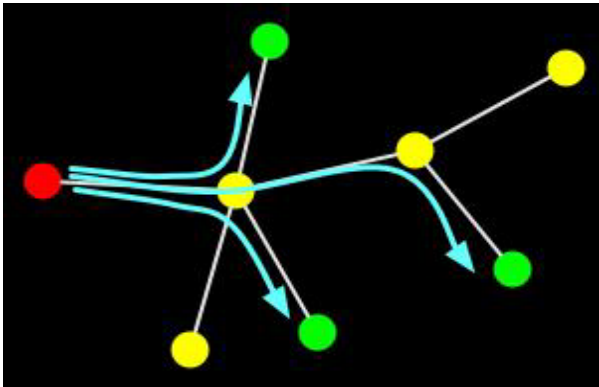
Implementation Agreement:

- Multicast Sample Value ID – MSVID
 - <name>-<IDCode>-<Class>
 - IDCode inherited from C37.118 (PMU or PDC)
 - Class = P, M, or N (for none)
 - All data in a given PDU shall be of the same Class
- RefrTim – Mandatory
 - Synchrophasor TimeStamp per C37.118
 - Same Time Stamp as in C37.118 (SoC+FoS+TQ)
 - TimeBase = $2^{24} = 16,777,216$
 - TQ = C37.118 TQ

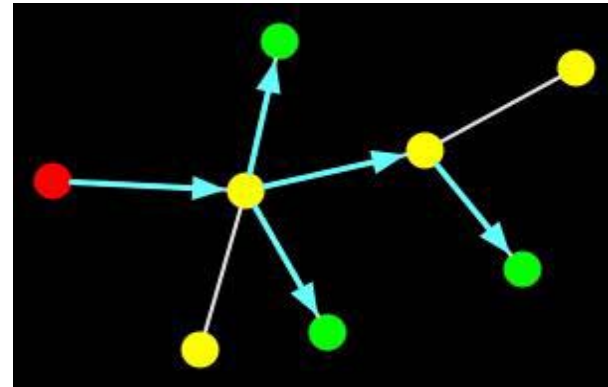


Unicast vs. Multicast

Point-to-Point
Multiple Streams



Multicast
One Output Stream



- Requires 3x Bandwidth in this example
- 3X Infrastructure \$\$\$

IGMP Packet Structure

bit offset	0–3	4	5–7	8–15	16–31
0	Type = 0x11			Max Resp Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address [1]				
128	Source Address [2]				
	...				
	Source Address [N]				

Group Address: This is the multicast address being queried when sending a Group-Specific or Group-and-Source-Specific Query. The field is zeroed when sending a General Query

Input LNs Required

M60MMXUnn

- Calc. Method:
 - “P” or “M” class
- Phase Voltages
- Phase Currents
- Frequency
- Rate of Change of Frequency - (HzRte)
- SmpRate

P120MSQInn

- Calc Method
 - “P” or “M” class
 - Sequence Voltages
 - Sequence Currents
-
- LNs Identified as a C37.118 Calculation Type “P” or “M”
 - Report rate included in the LN
 - Nominal Frequency added to LPHD

PMU Data Organization

- STAT word (16 bit Unsigned Integer) – Semantics from C37.118.2
- Synchrophasors – Float 32 / Polar Format
- Frequency – Float 32
- Rate of Change of Frequency – Float 32
- Analogs – Float 32
- C37.118.2 Binary Status (16 bit Bitstring)

