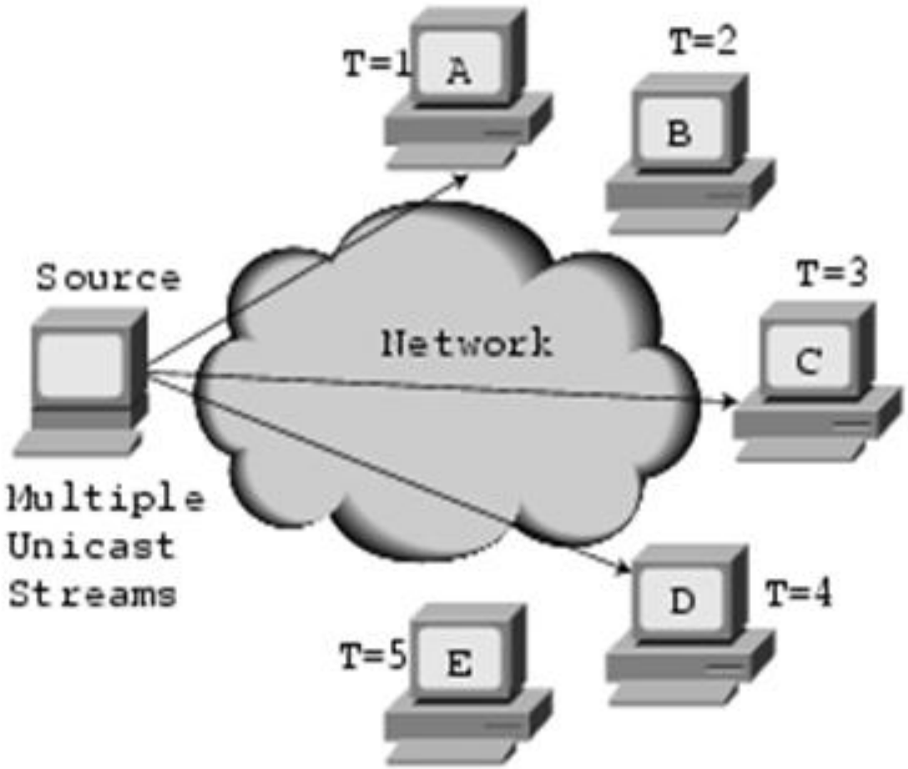
The New GOOSE & SV

Mark Adamiak
GE Digital Energy

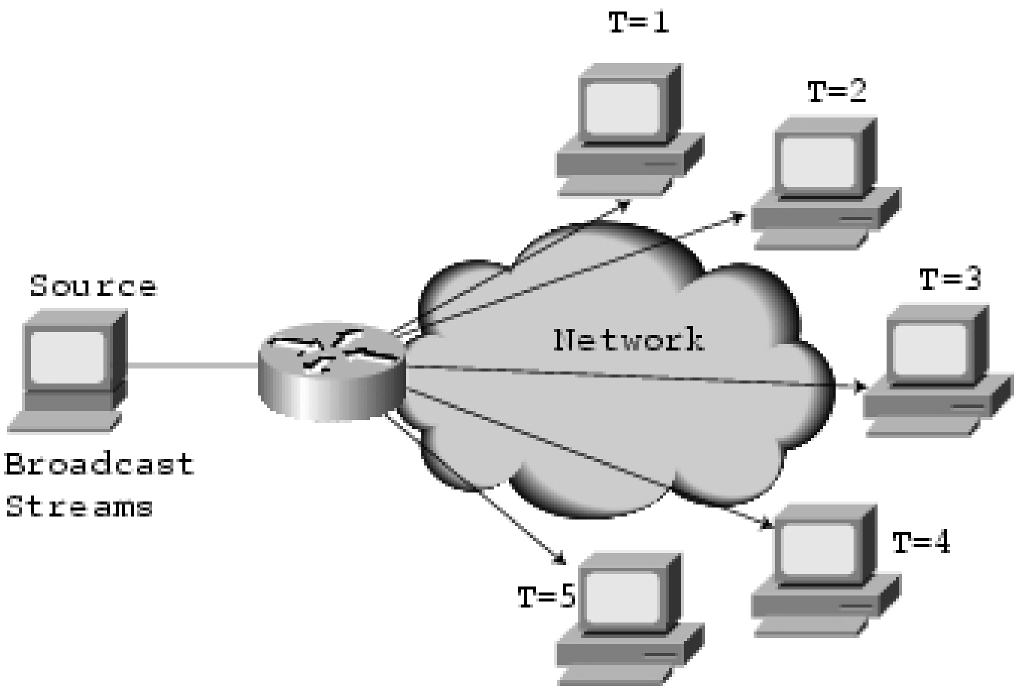
imagination at work

Functional Requirement: One message to multiple subscribers



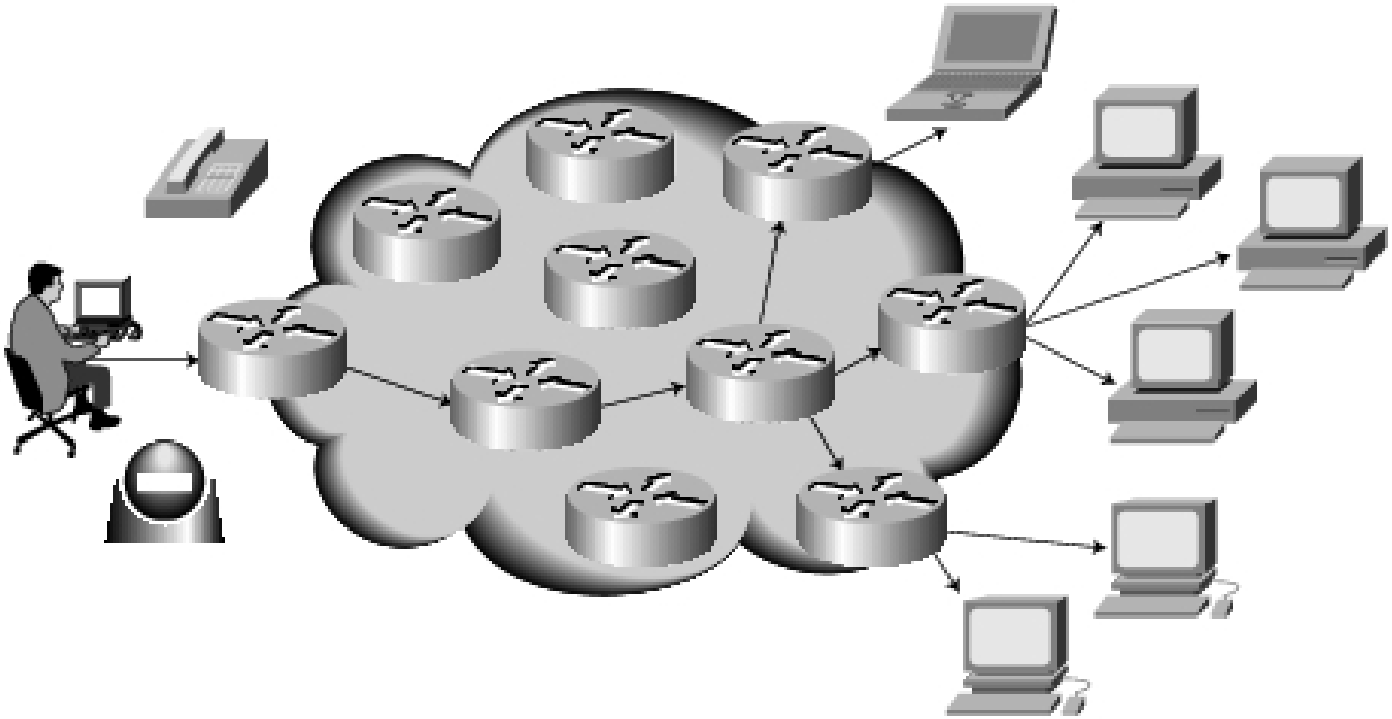
Unicast solution – limited on connection

Definition of Terms: Broadcast



Router Duplicates Packet to ALL Locations

Multicast Solution:



One Message Only Sent to Intended Recipients

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])

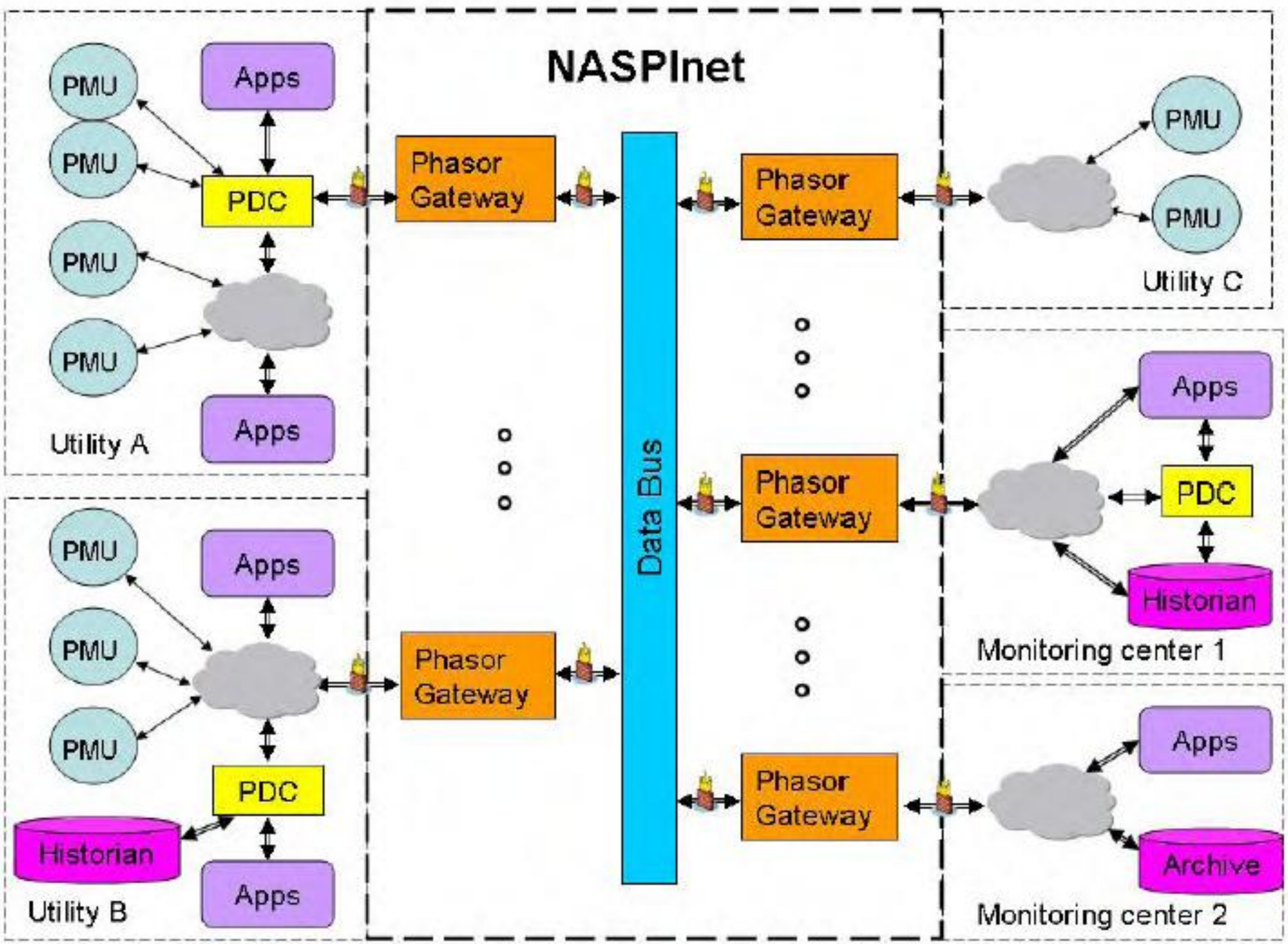
imagination at work

1 – CISCO Recommended

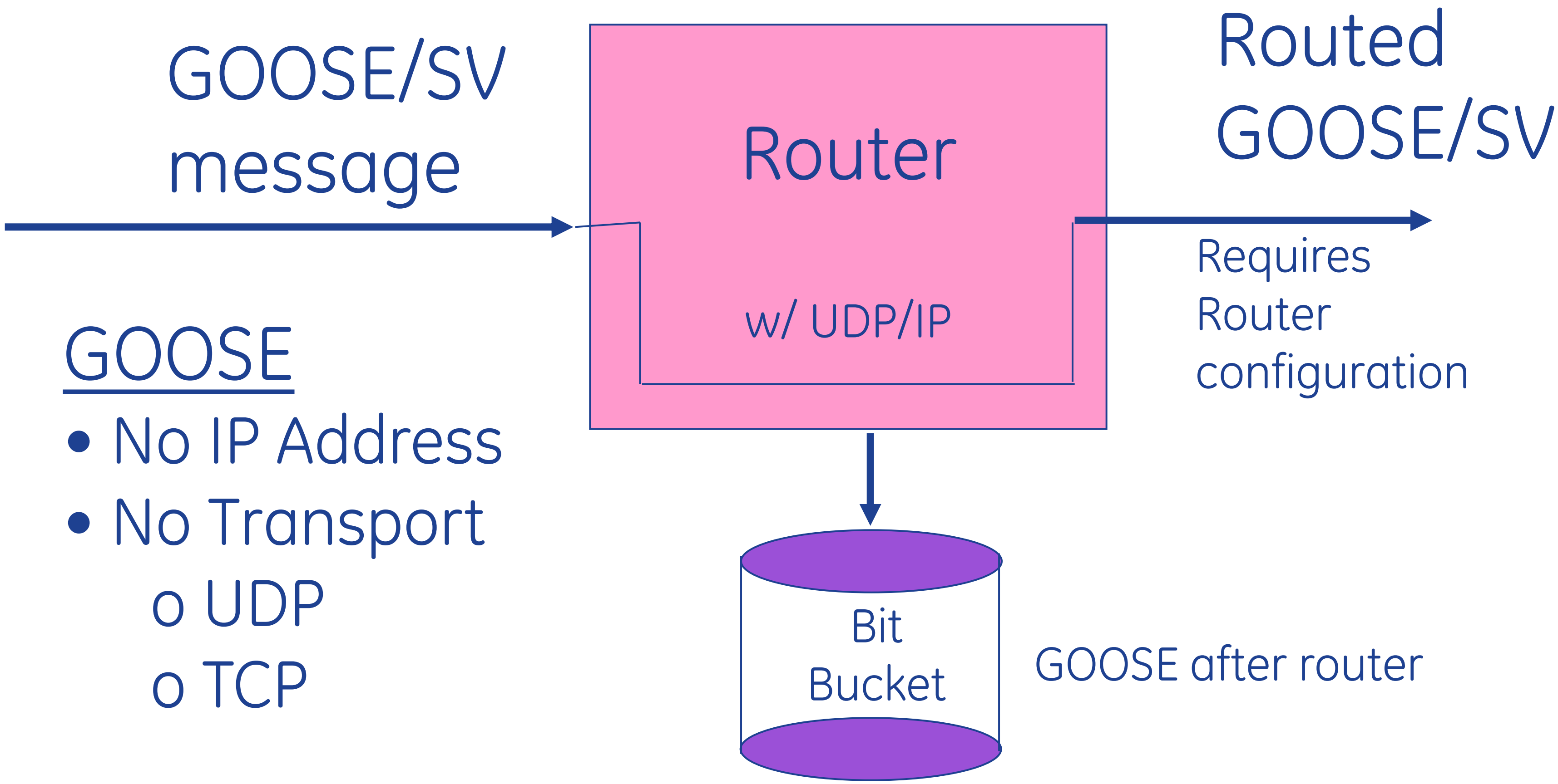
Gaps in C37.118

- No defined security
  - Requires an external solution
  - Multicast and associated security not defined
- Dataset Configuration tools are vendor specific
- No standard data names
- Limitations on dataset name length
- Lack of Negative response from the server
  - Some consider this a feature…..

North American SynchroPhasor Initiative Network - NASPInet Vision



Mapping Synchrophasors into GOOSE



GOOSE

- No IP Address
- No Transport
  - o UDP
  - o TCP

imagination at work

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

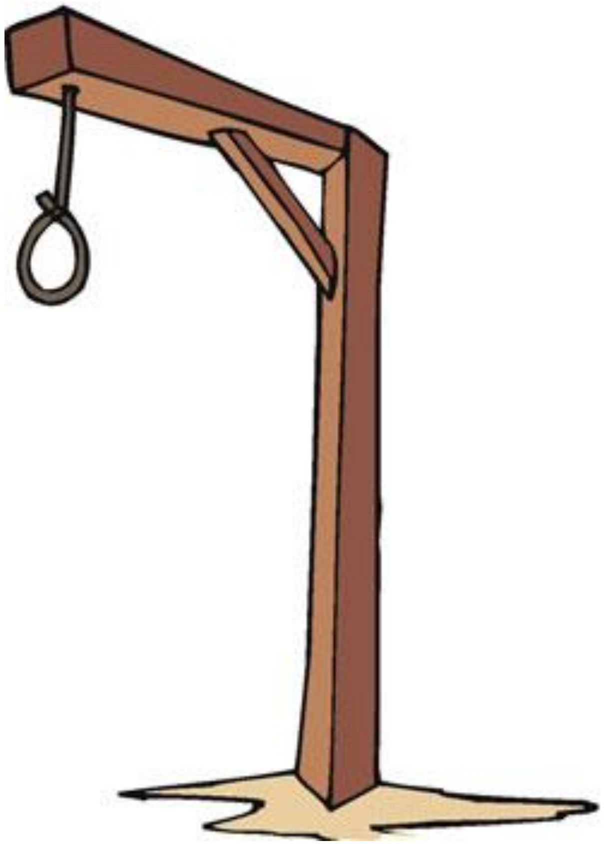
Committee Approved Technical Report:

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 **O**bject **O**riented **S**ubstation **E**vent

The NOOSE !



imagination at work

But people got hung up on the idea… So we have:

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

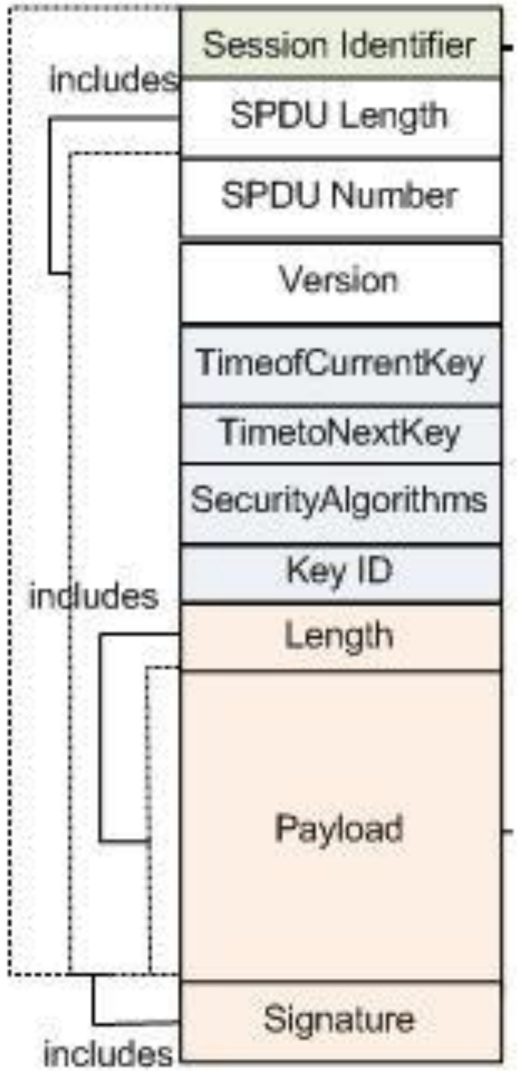
And

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

imagination at work

IEC 90-5 Data Model

SPDU:
Session
Protocol
Data
Unit

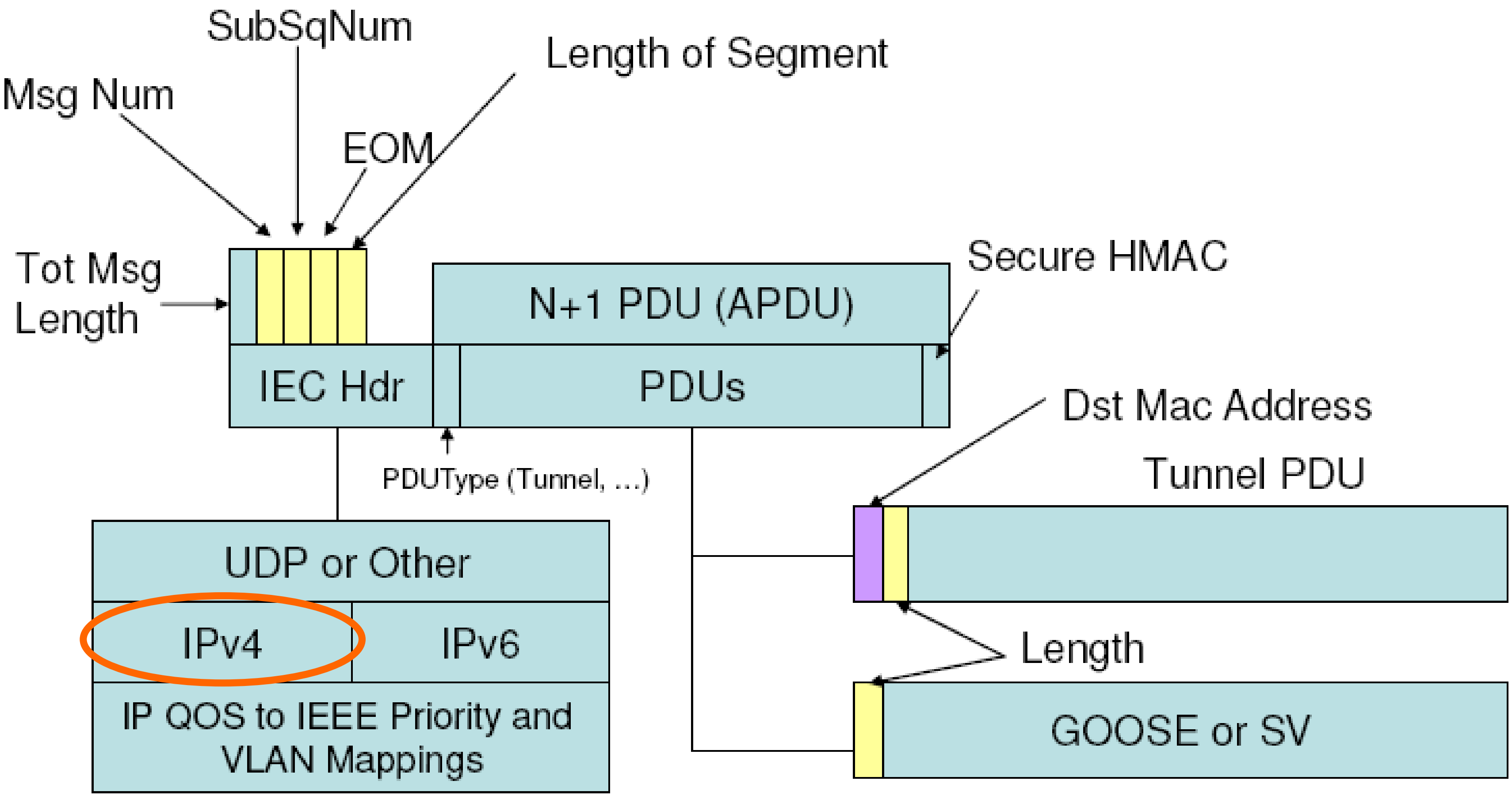


Detail Format

Total Max Size: 65535 bytes

Supports Multiple non-time-aligned PMU datasets

IEC 61850 90-5 Networked GOOSE/SV



Potential Solution for NASPINet

imagination at work

Payload

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

An Implementation Agreement is proposed to “agree” to the items in the Header and Dataset

imagination at work

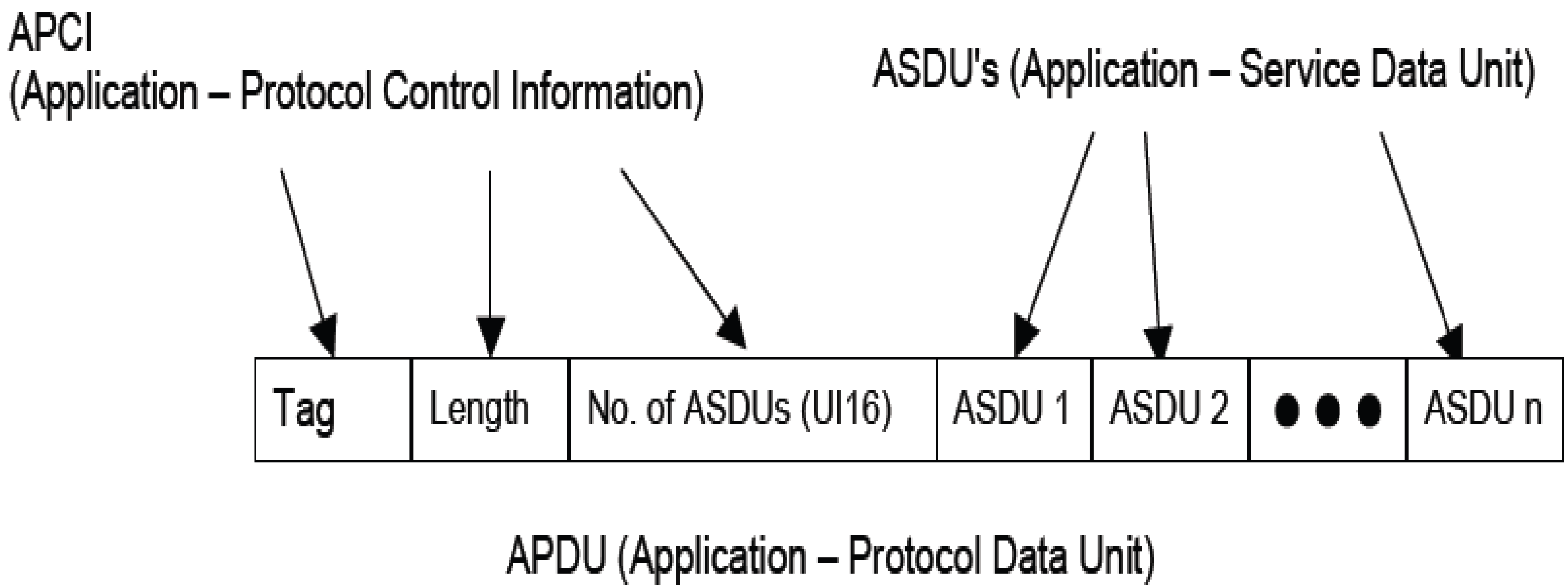
Implementation Agreement: Header

- 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

Implementation Agreement Dataset inclusions

- STAT word
  - 16 bit Unsigned Integer
  - Semantics from C37.118
- Synchrophasors Frequency and ROCOF to be included
- Synchrophasors
- Analog Values

Reliable Transport through Repeat



ASDU1 – Oldest data

ASDUn – Newest data

n is a user-settable parameter

Internet Protocol Priority via 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

Mapping of C37.118 FoS to 61850

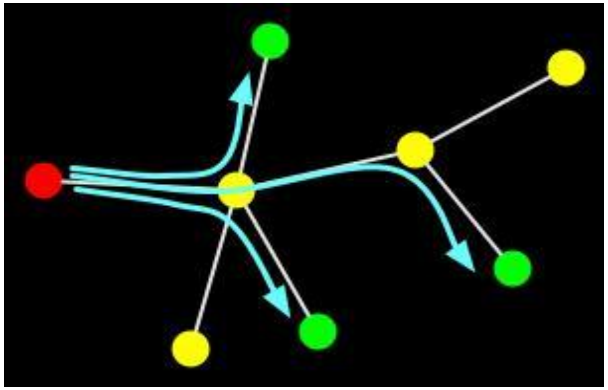
FractionOfSecond_61850 =

$$\frac{FractionOfSecond\_C37.118}{C37.118\_Time\_BASE} * 16{,}777{,}216 (2^{24})$$

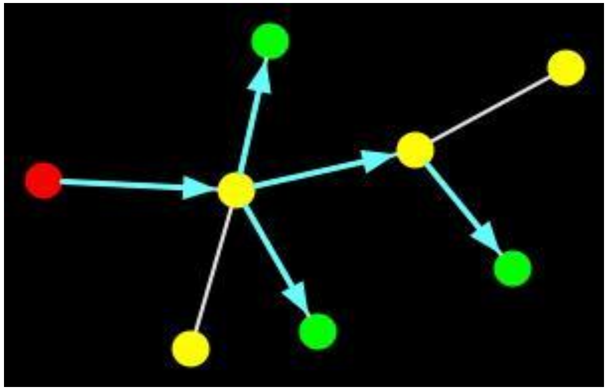
imagination at work

Unicast vs. Multicast

Point-to-Point
Multiple Streams

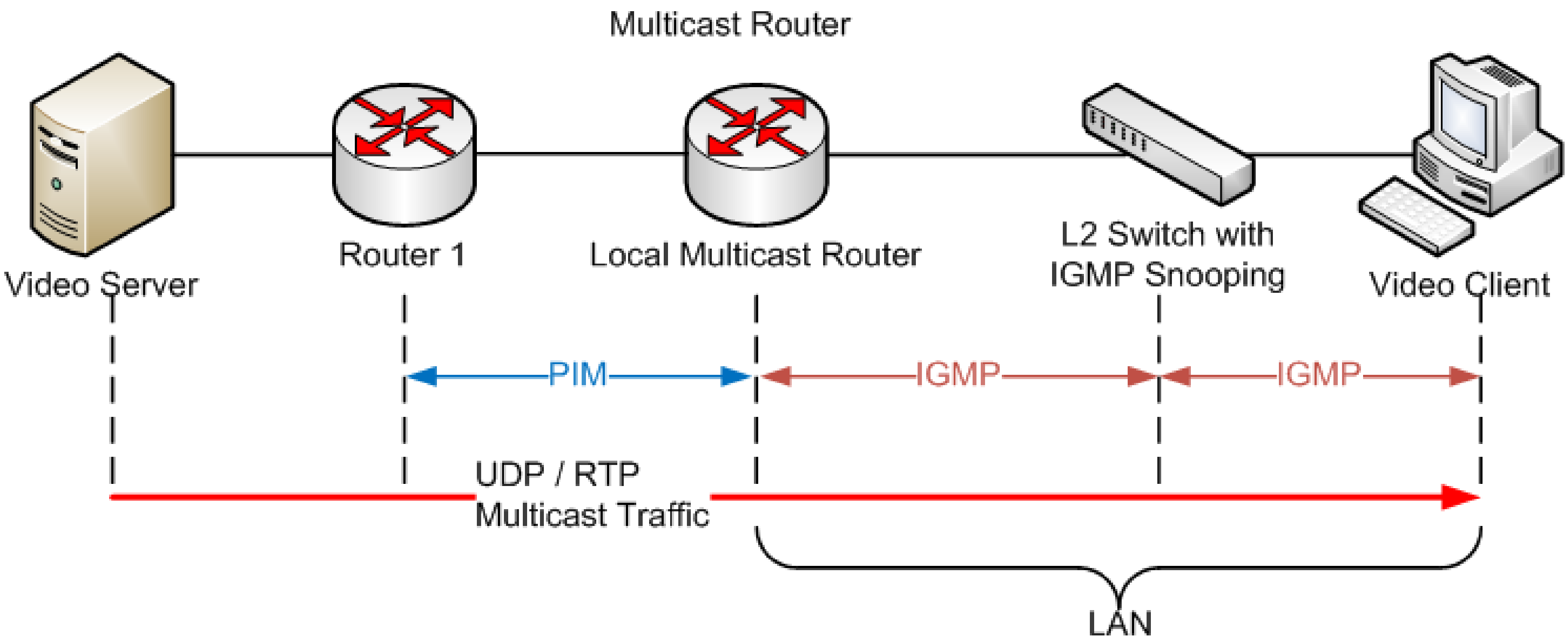


Multicast
One Output Stream



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

Multicast Path Establishment via Internet Gateway Management Protocol – IGMP



imagination at work

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

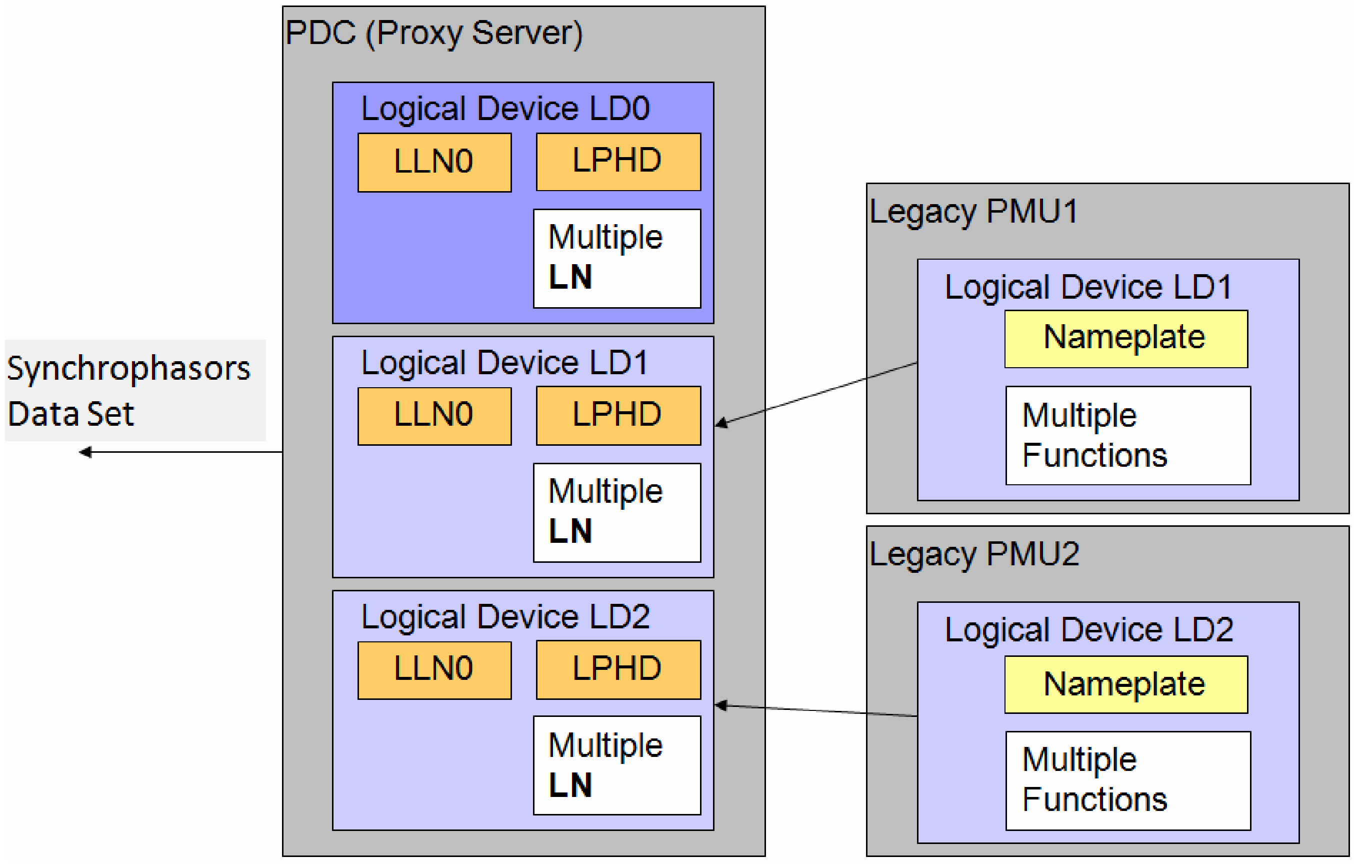
- LNs Identified as a C37.118 Calculation Type "P" or "M"
- Report rate included in the LN
- Nominal Frequency added to LPHD

Mapping of C37.118 STN and IDCode

- STN and IDCode mapped into “d”escription field of the Label CDC (LPL) of LLN0
- Mapped as:
  - <STN>-<IDCode>
- SmpRate added as a DO in LLN0

imagination at work

PMU to PDC Mapping



imagination at work

Implementation Agreement

C37.118.2 to 90-5 Data Mapping Proposal:

PMU1 STAT Word (C37.118 Type Bitstring)

PMU1 Data

PMU2 STAT Word

PMU2 Data

………

PMUn STAT Word

PMUn Data

imagination at work

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)

Standardized Dataset Configuration

- Uses the IEC 61850 XML Configuration language
  - SCL Extensions added for the 16 bit – bit strings used in C37.118
    - There is now a C37.118 “Data Type”
- Dataset members can be published via standard registration services

imagination at work

Security Definition in 90-5

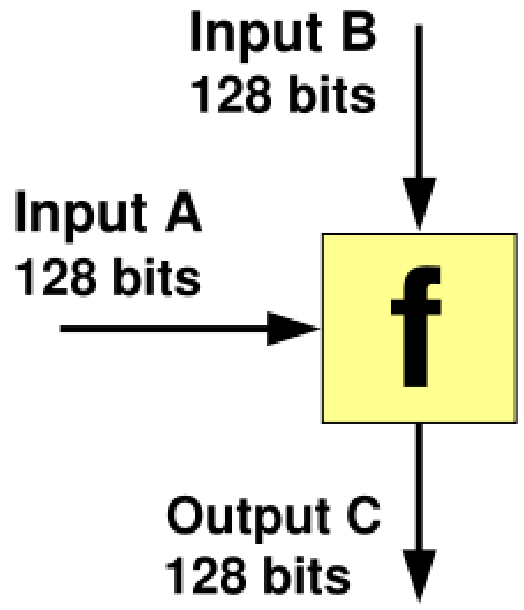
- Defines a Secure Hash Algorithm - SHA2 Hash code for message authentication / integrity
- Defines AES as the encryption algorithm
- Identifies / Extends a Key management system
  - RFC 3547 The Group Domain of Interpretation
  - The publisher manages the keys to all subscribers
  - Same key for Hash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

Security Options as defined in 90-5:

Table 9 – Allowed values for MAC signature value calculations

Enumerate value	HMAC algorithm	Number of bits	Designation	Mandatory (m), Optional (o)
0	None	None	MAC-None	c1
1	SHA-256	80	HMAC-SHA256-80	m
2	SHA-256	128	HMAC-SHA256-128	m
3	SHA-256	256	HMAC-SHA256-256	m
4	AES-GMAC	64	AES-GMAC-64	m
5	AES-GMAC	128	AES-GMAC-128	m
c1 – Shall only be used when encryption is also in use.				

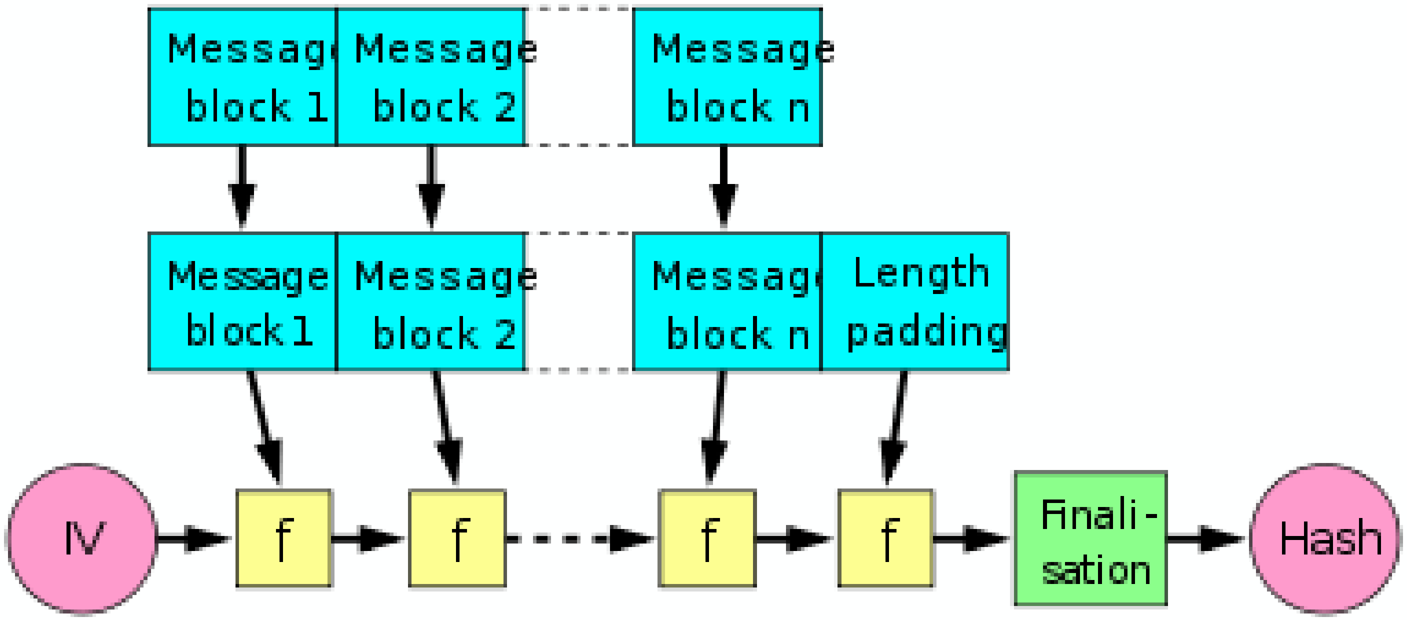
One-way Compression



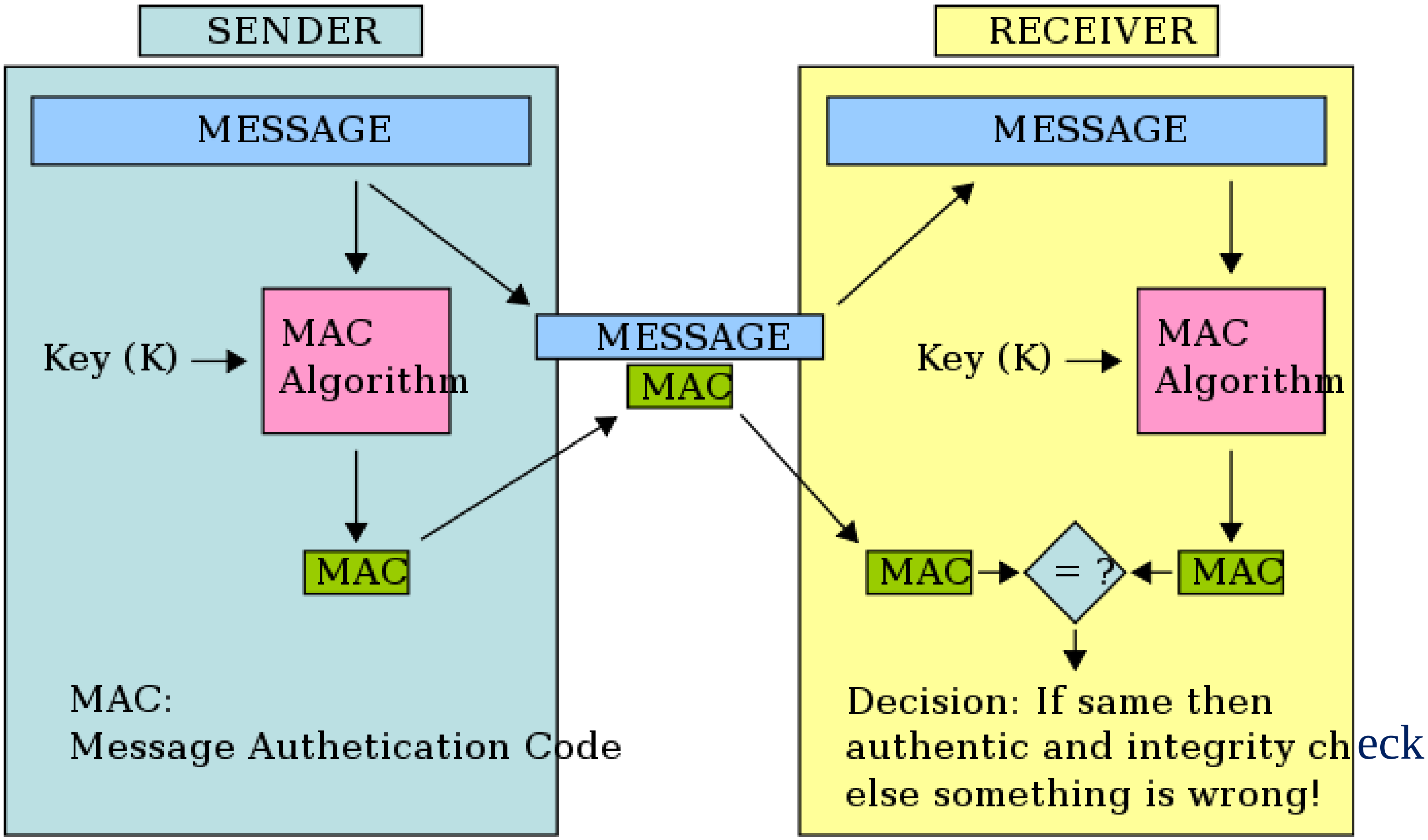
- Input values typically cannot be re-produced

Hash Function Concept

- Processes an arbitrary-length message into a fixed-length output
- Typical implementation breaks the message into N blocks and operates on each block in sequence



Cryptographic Hash Concept

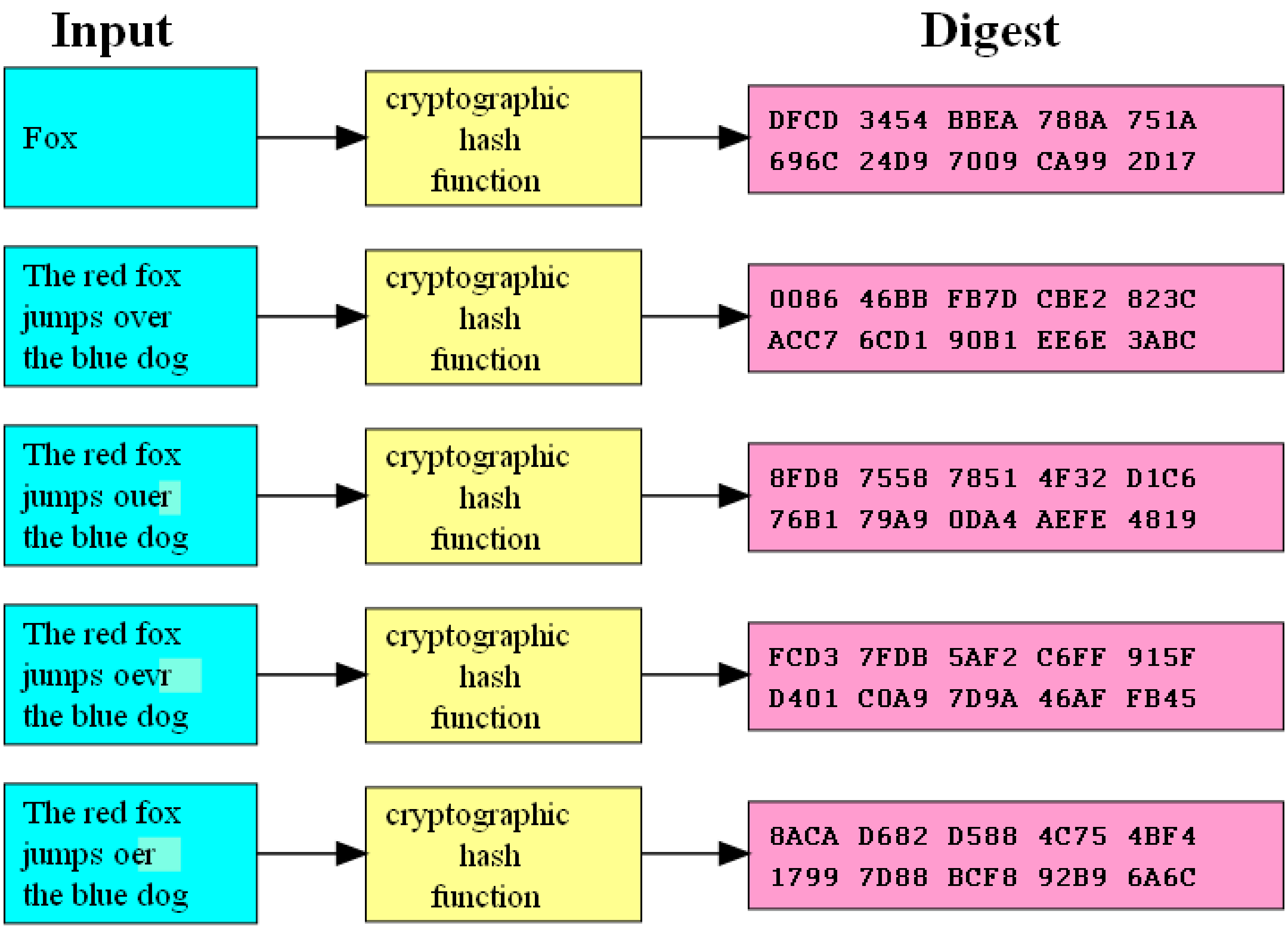


Also known as a Hash based Message Authentication Code – **HMAC**

Also called a Message Integrity Code **- MIC**

imagination at work

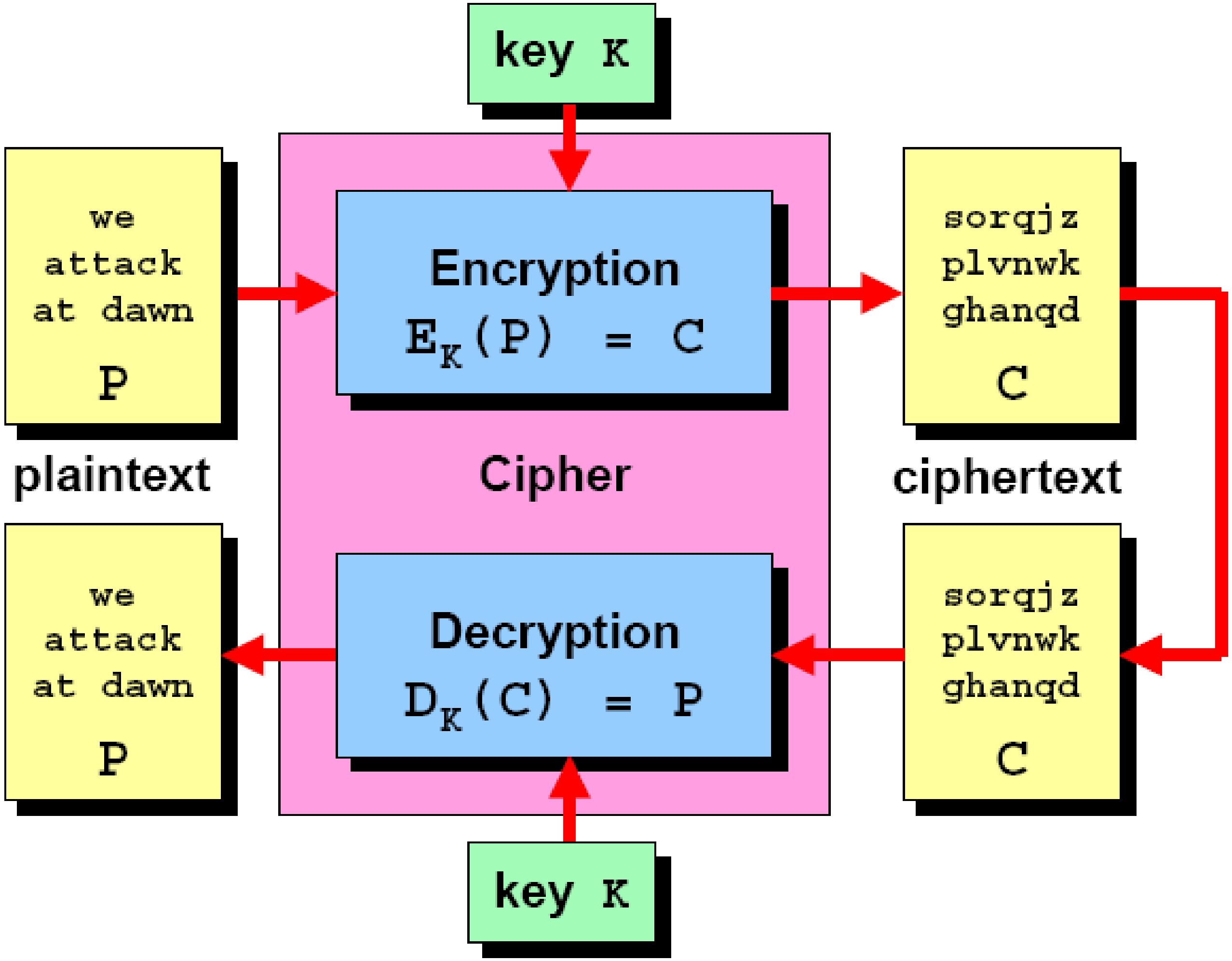
Example of Hash Outputs from SHA-1*



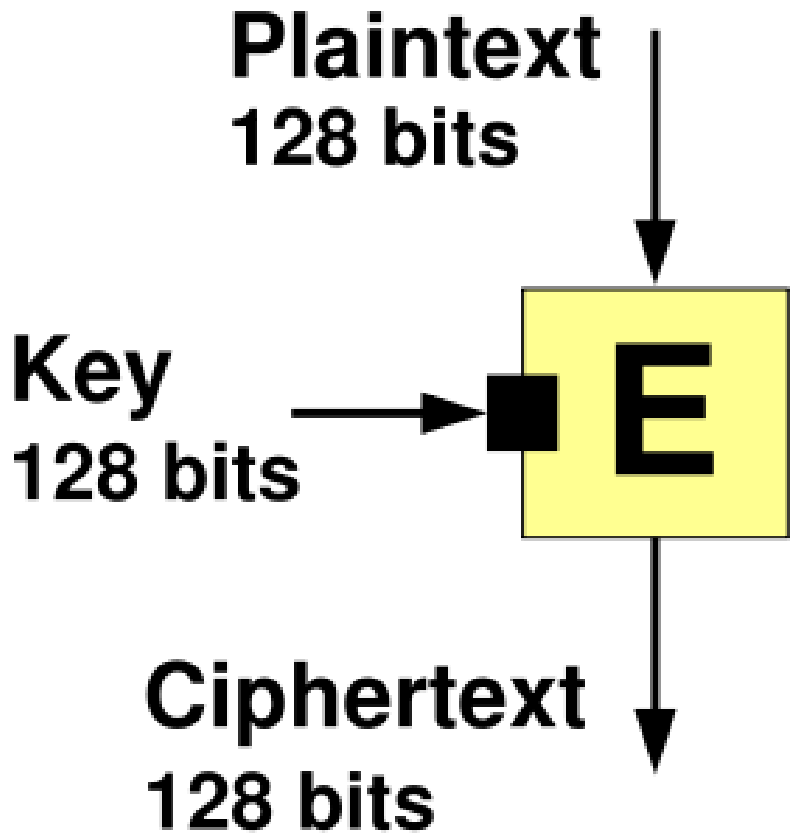
* SHA-1 now deprecated due to vulnerabilities

imagination at work

Cryptography Basics



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.

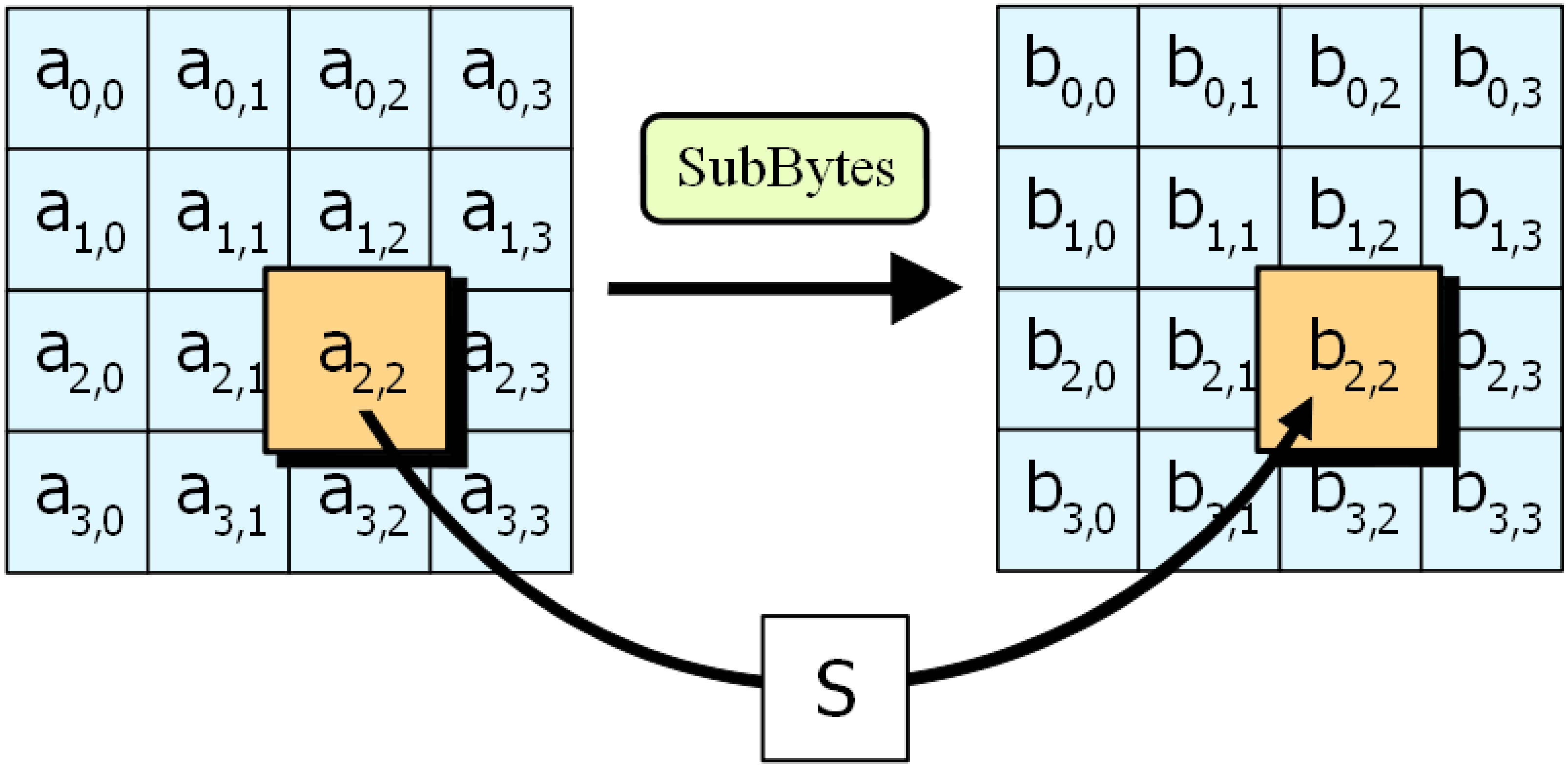
The AES **encryption package** is a cryptographic algorithm that can be used to protect electronic data. Specifically, AES is an iterative, symmetric-key block cipher that can use keys of 128, 192, and 256 bits, and encrypts and decrypts data in blocks of 128 bits (16 bytes).

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.

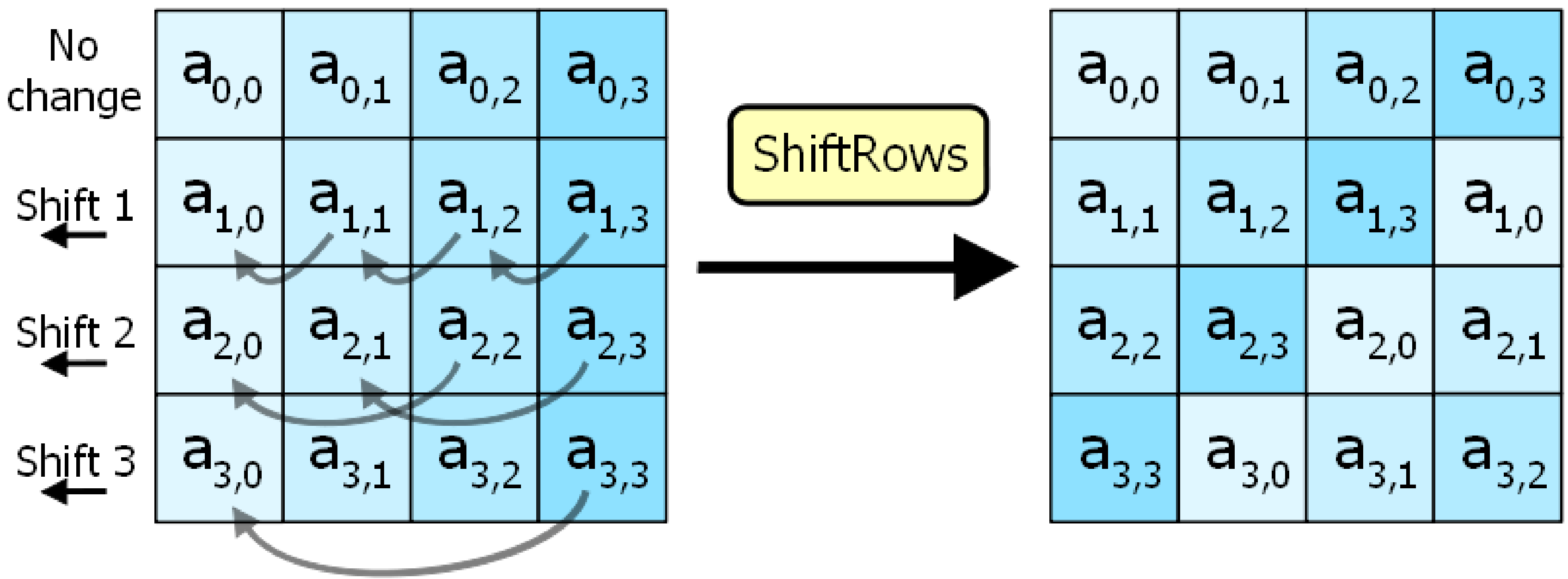
The AES **encryption package** will certainly become a de facto standard for encrypting all forms of electronic information, replacing DES. AES-encrypted data is unbreakable in the sense that no known cryptanalysis attack can decrypt the AES cipher text without using a brute-force search through all 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; $b_{ij} = S(a_{ij})$.

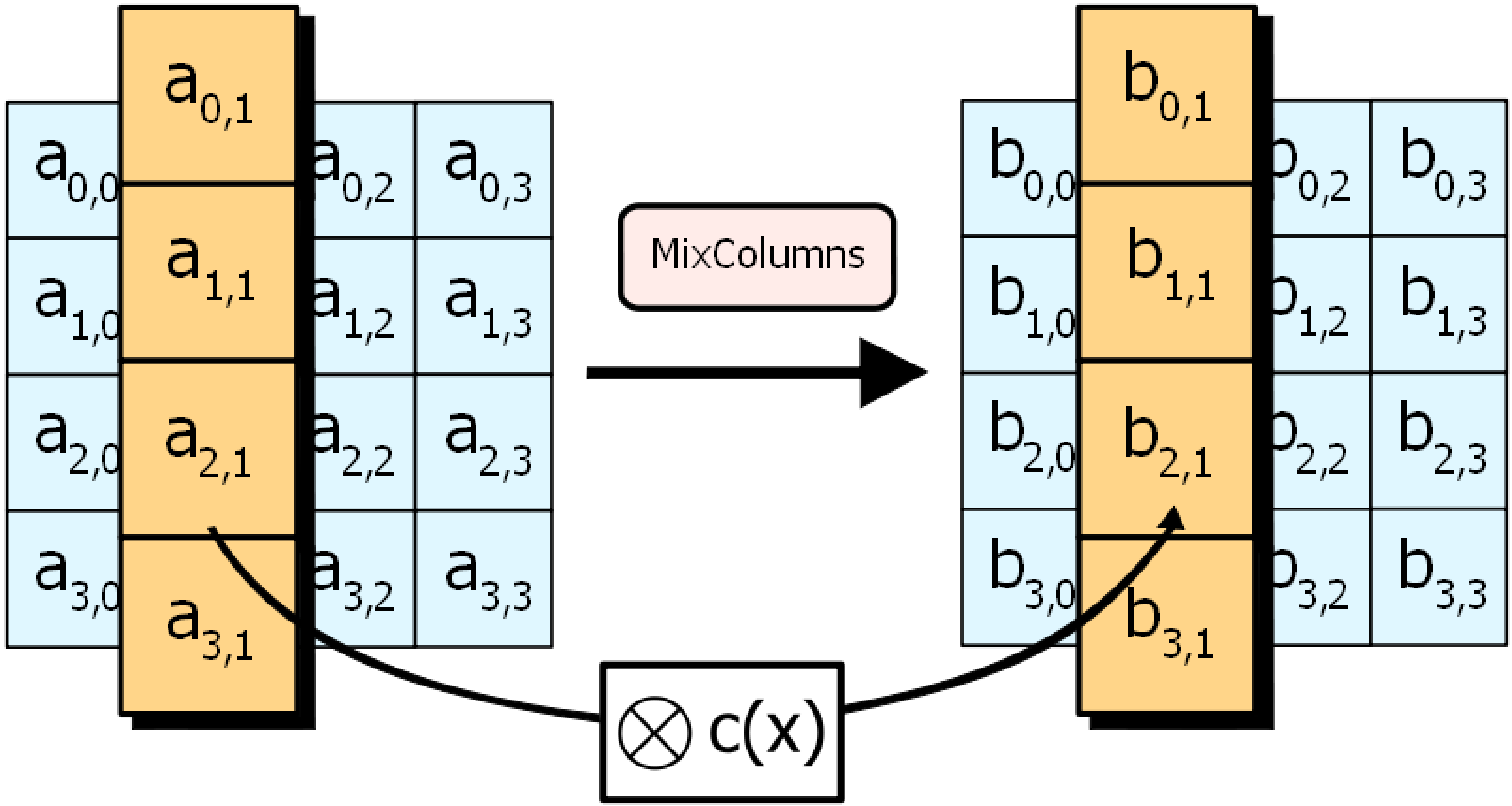
AES – Step 2 – Shift Rows



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.

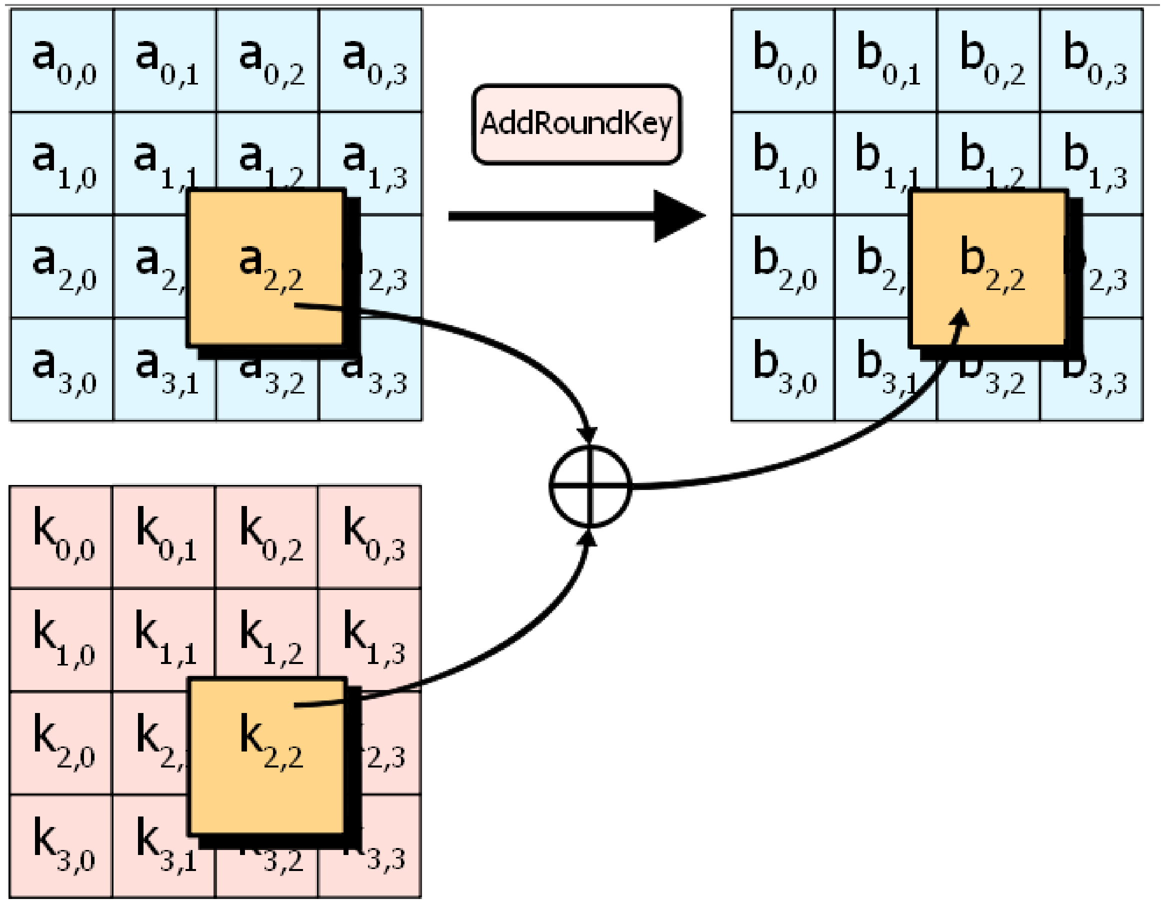
imagination at work

AES – Step 3 – Mix Columns



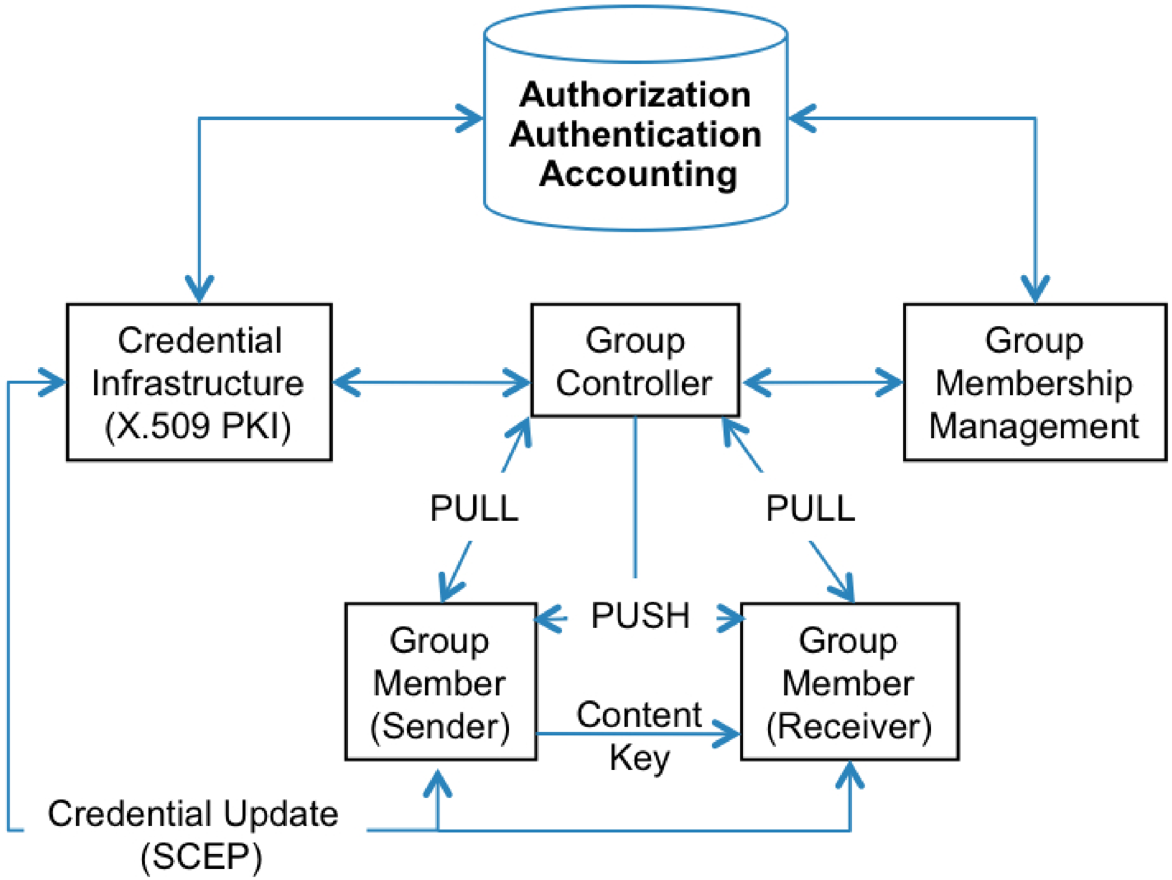
In the MixColumns step, each column of the state is multiplied with a fixed polynomial c(x).

AES – Step 4 – Add round Key



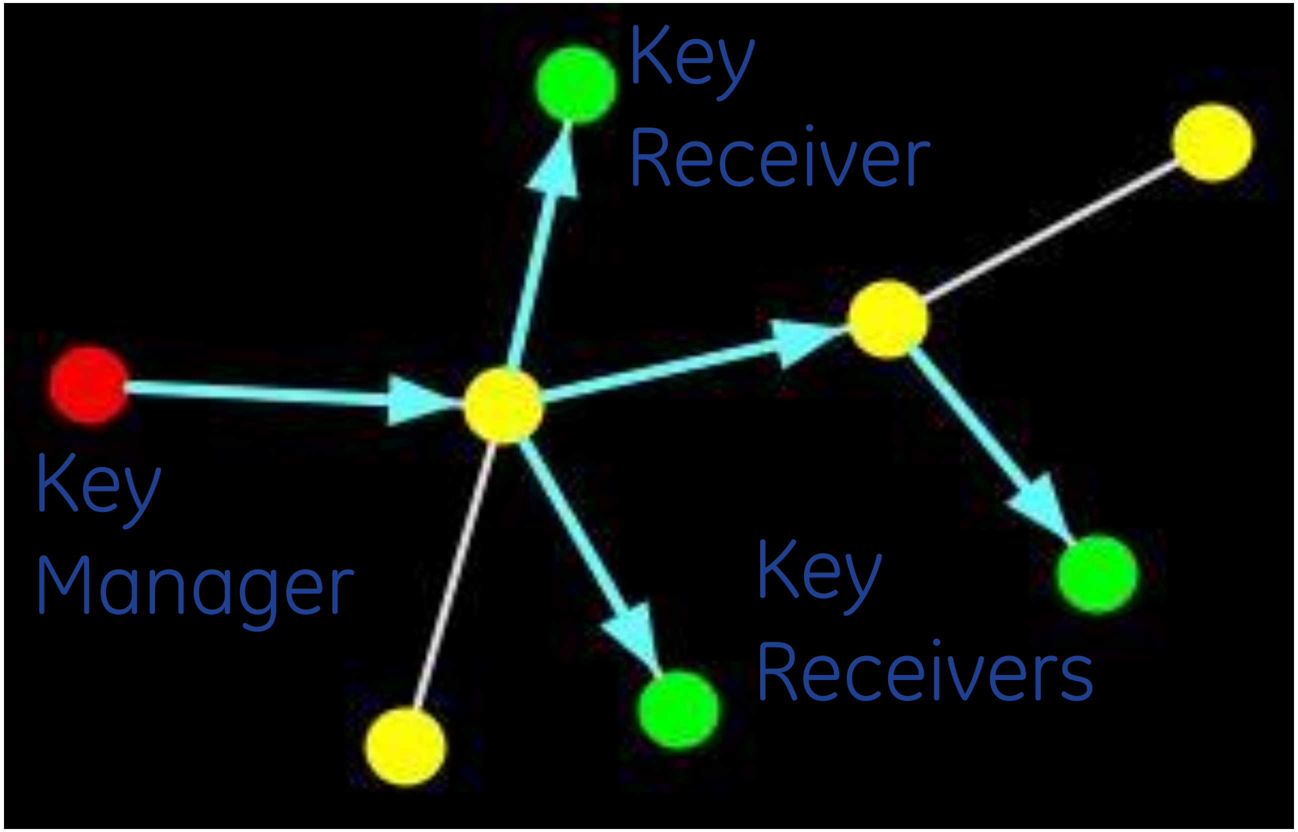
In the AddRoundKey step, each byte of the state is combined with a byte of the round subkey using the XOR operation (⊕).

Group Domain of Interpretation - GDOI



- Publishers act as Controllers
- Receiving Group Members “Pull” new keys
- Centralized Authorization Management

Publisher-based Key Management



Keys are dynamically managed

Changed when a Subscriber is removed