IEEE Std 802c: What's New and Useful in the Overview and Architecture

Date: 2017-09-07 (r1)

Authors:

Name	Affiliations	Address	Phone	email
Roger Marks	EthAirNet Associates	Denver, CO, USA	1-802-capable	roger@ethair.net

Abstract

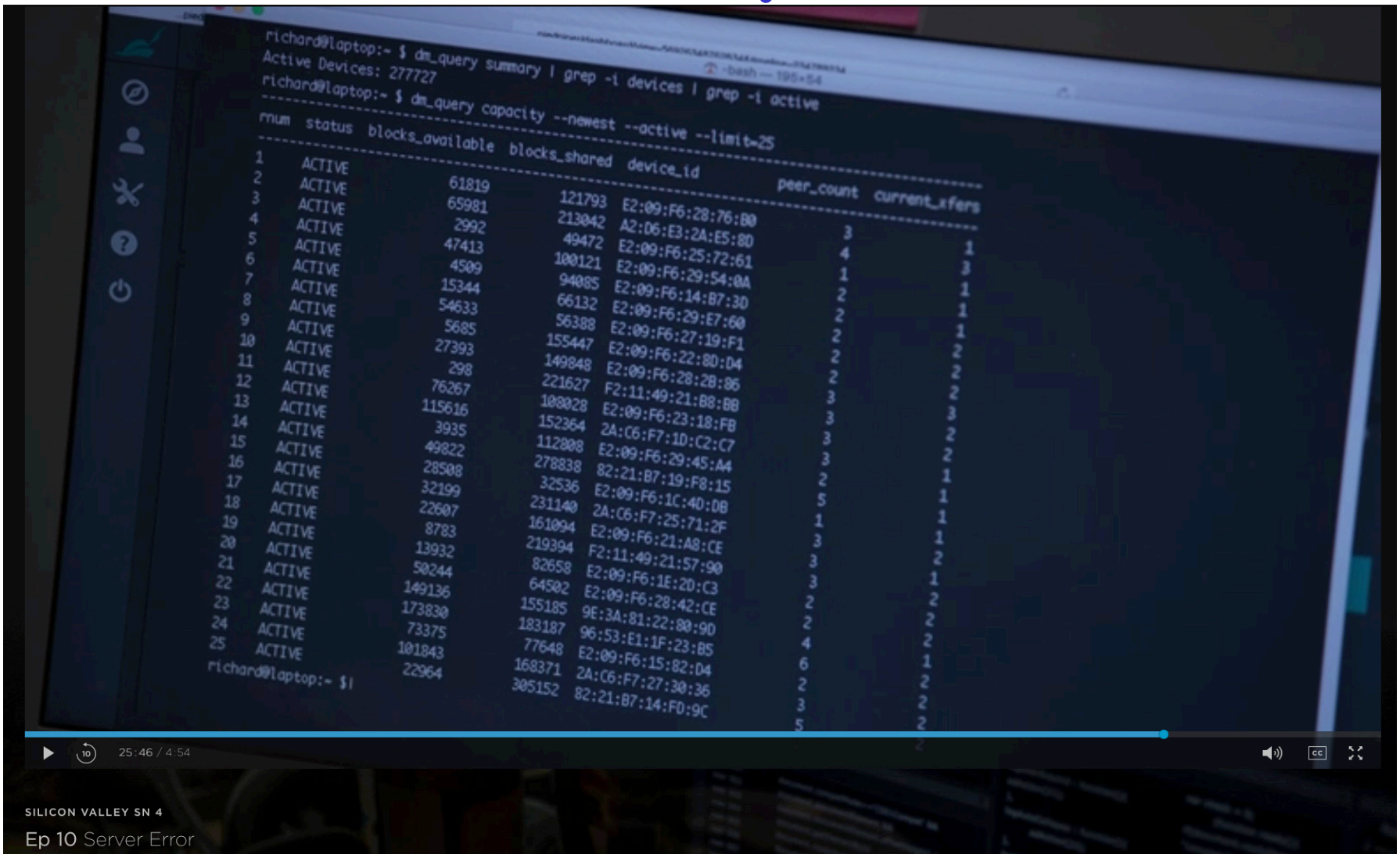
IEEE Std 802c was approved by the IEEE-SA Standards Board on 15 June 2017, amending the IEEE 802 Overview and Architecture to specify Local Medium Access Control (MAC) Address Usage. This slide set summarizes the changes and implications. It also summarizes a new revision, prepared in coordination with 802c, of the relevant tutorial of the IEEE Registration Authority (IEEE RA).

The View from *Silicon Valley*

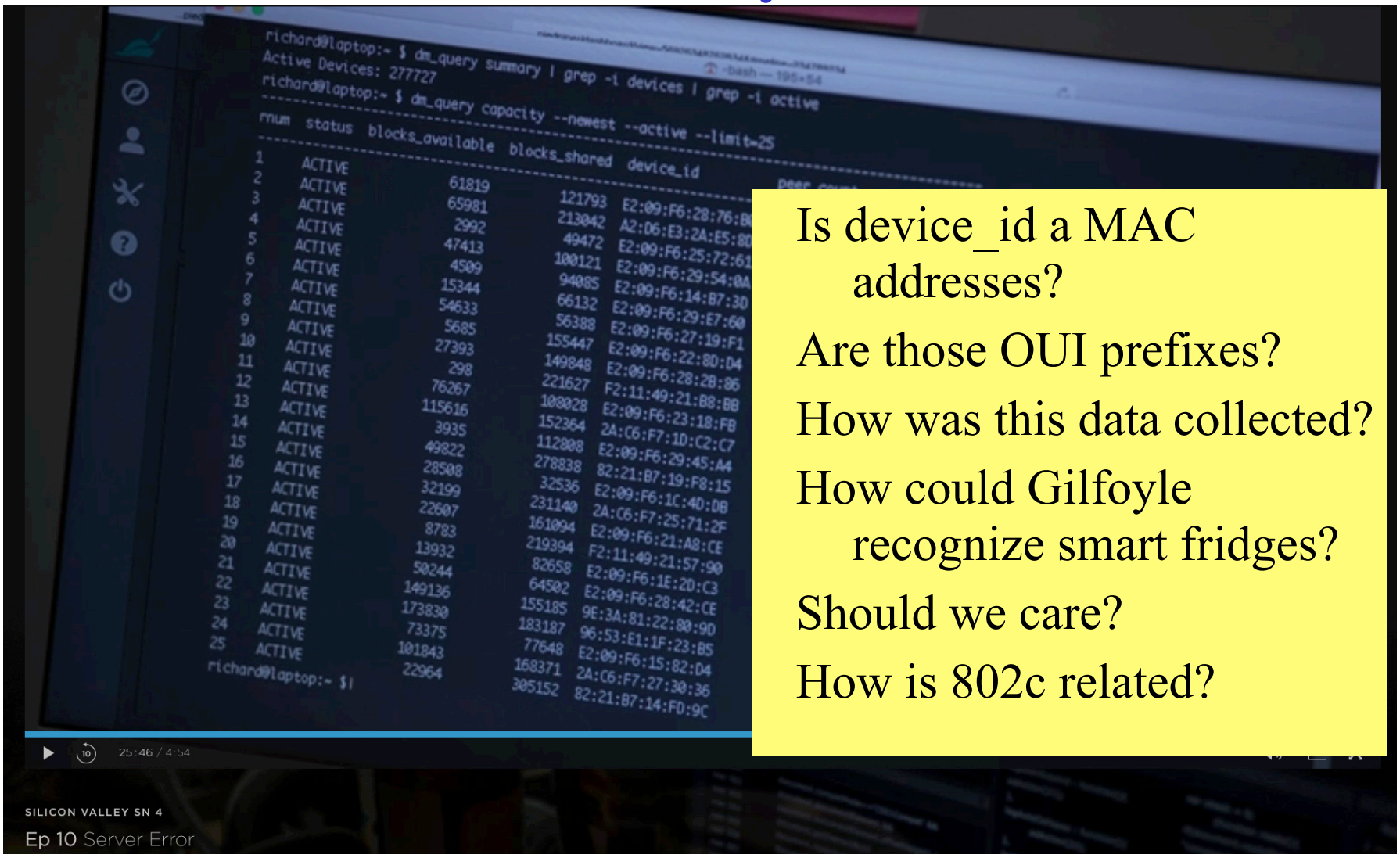
Dinesh: *What are those devices? Those aren't phones.*
Gilfoyle: *Look at that OUI prefix in these MAC addresses.*
Richard: *OK, so what are those?*
Gilfoyle: *Smart fridges. About 30,000 of them.*

- *Silicon Valley* (a fictional television comedy)
  Season 4, Episode 10 ("Server Error")
  First aired on HBO, 2017-06-25

What Gilfoyle saw



What Gilfoyle saw

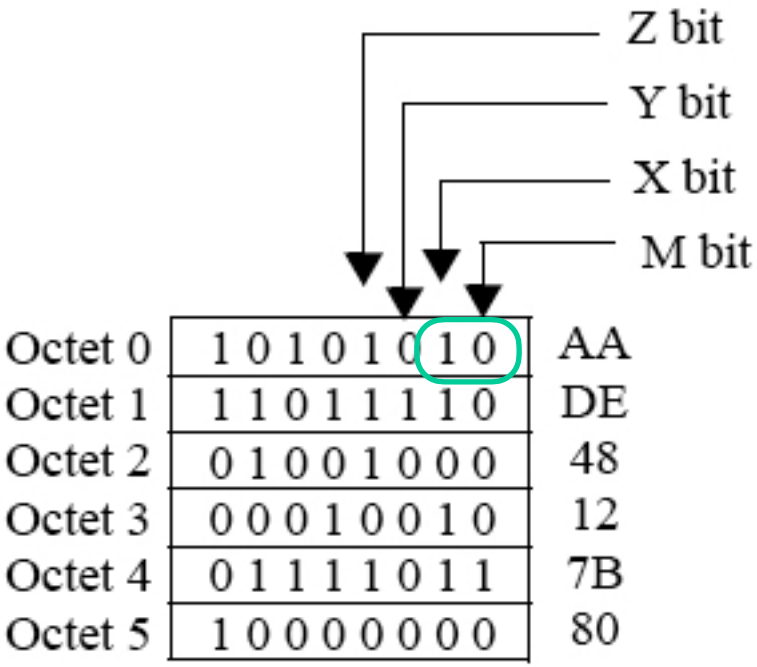


- Is device_id a MAC addresses?
- Are those OUI prefixes?
- How was this data collected?
- How could Gilfoyle recognize smart fridges?
- Should we care?
- How is 802c related?

IEEE Std 802c: Key Facts

- IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture – Amendment 2: Local Medium Access Control (MAC) Address Usage
- Standard approved: 2017-06-15; published 2017-08-25
  - 802 pseudo-tutorial, 2014-11-03
  - 802.1 Local Address Study Group, Nov 2014 - July 2015
  - PAR Authorized: 2015-01-11
  - PAR Revised: 2016-12-07 (to add maintenance issues)
- Scope in brief:
  - *provide an optional local MAC address space structure to allow multiple administrations to coexist*
  - *designate a range of local MAC addresses for protocols using a Company ID (CID) assigned by the IEEE Registration Authority*
  - *range of local MAC addresses will be designated for assignment by local administrators*
  - *a range of local MAC addresses for use by IEEE 802 protocols*

Local Address: Example



- M bit (I/G bit): as before, 1 for multicast
- X bit (U/L) bit: as before, 1 for local
  - Y and Z bits: new designations

SLAP

- *Structured Local Address Plan (SLAP): An optional standardized specification for the use of local medium access control (MAC) address space entailing the use of*
  - *Extended Local Identifier (ELI),*
  - *Standard Assigned Identifier (SAI), and*
  - *Administratively Assigned Identifier (AAI)*

  addresses in specific disjoint ranges.

Assignment Protocols

- *An address assignment protocol assigning local MAC addresses to devices on a LAN should ensure uniqueness of those addresses.*
- *When multiple address assignment protocols operate on a LAN without centralized administration, address duplication is possible, even if each protocol alone is designed to avoid duplication, unless such protocols assign addresses from disjoint address pools.*
- *Administrators who deploy multiple protocols on a LAN in accordance with the SLAP will enable the unique assignment of local MAC addresses within the LAN as long as each protocol maintains unique assignments within its own address subspace.*

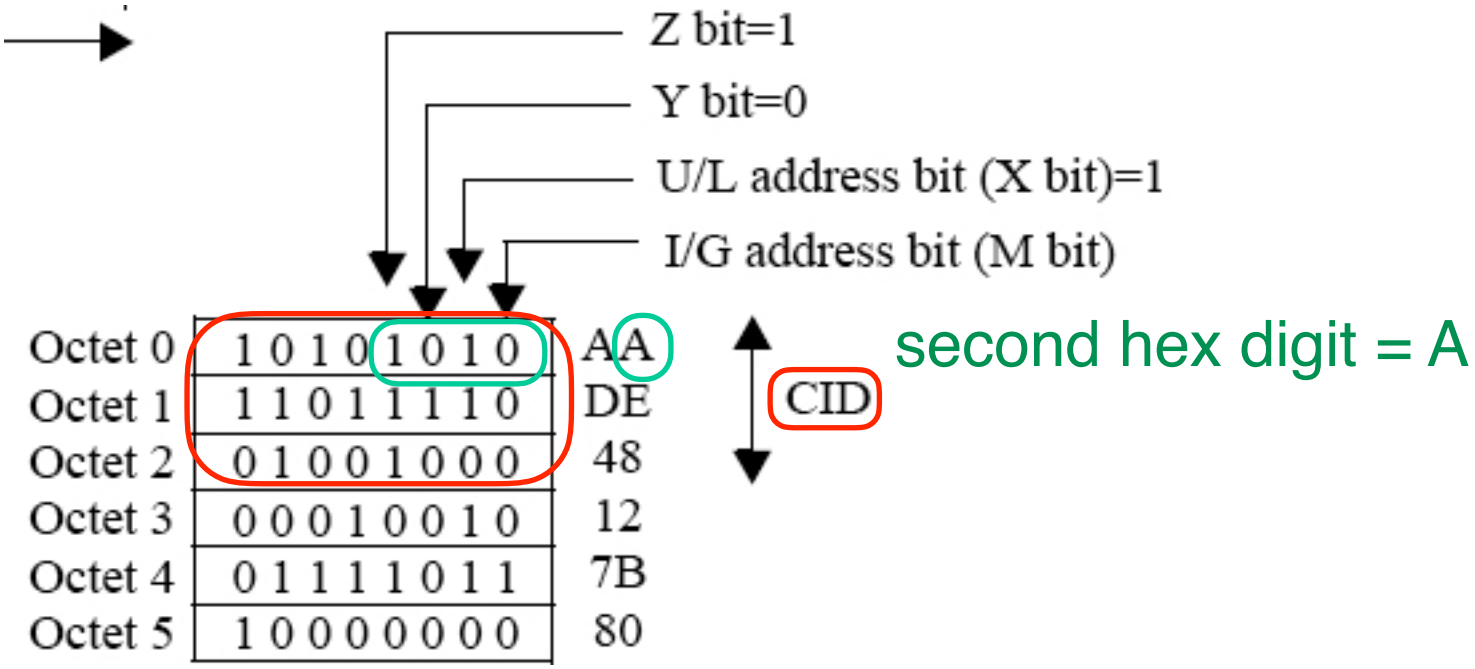
SLAP Quadrants

SLAP quadrant	Y bit	Z bit	ZYXM	second hex digit	SLAP local identifier type	SLAP local identifier
01	0	1	1010	A	Extended Local	ELI
11	1	1	1110	E	Standard Assigned	SAI
00	0	0	0010	2	Administratively Assigned	AAI
10	1	0	0110	6	*Reserved*	*Reserved*

"A" for AAI and "E" for ELI would have been nice, but prior IEEE RA assignments put ELI in the "A" quadrant.

	Y = 0	Y = 1
Z = 0	AAI	*Reserved*
Z = 1	ELI	SAI

ELI: Extended Local Identifier



- like an EUI, but with a Company ID (CID) instead of an OUI
  - CID has X = 1 (local space).
- IEEE Registration Authority (RA) assigns CIDs, all in SLAP 01
  - CID predates 802c
- 802c reserves 4 CIDs for the local administrator

AAI: Administratively Assigned Identifier

- AAI: Administratively Assigned Identifier
  - second hex digit = 2
  - *Administrators who wish to assign local MAC addresses in an arbitrary fashion (for example, randomly) and yet maintain compatibility with other assignment protocols operating under the SLAP on the same LAN may assign a local MAC address as AAI.*
- Reserved quadrant can be used like AAI, with reservations:
  - second hex digit = 6
  - *may be administratively used and assigned in accordance with the considerations specified for AAI usage, without effect on SLAP assignments. However, administrators should be cognizant of possible future specifications… that would render administrative assignment incompatible with the SLAP.*

SAI: Standard Assigned Identifier

- second hex digit = E
- *Specification of the use of the SAI quadrant for SLAP address assignments is reserved for the standard forthcoming from IEEE P802.1CQ.*
- *An SAI is assigned by a protocol specified in an IEEE 802 standard.*
- *Multiple protocols for assigning SAI may be specified within various IEEE 802 standards. Coexistence of such protocols may be supported by restricting each to assignments within a subspace of SAI space.*
- *In some cases, an SAI assignment protocol may assign the SAI to convey specific information. Such information may be interpreted by receivers and bridges that recognize the specific SAI assignment protocol, as identified by the subspace of the SAI. The functionality of receivers and bridges that do not recognize the protocol is not affected.*

P802.1CQ

- IEEE Standard for Local and Metropolitan Area Networks: Multicast and Local Address Assignment
- PAR authorized: 2016-02-05
- Scope: *This standard specifies protocols, procedures, and management objects for locally-unique assignment of 48-bit and 64-bit addresses in IEEE 802 networks. Peer-to-peer address claiming and address server capabilities are specified.*
- Need: *Currently, global addresses are assigned to most IEEE 802 end station and bridge ports. Increasing use of virtual machines and Internet of Things (IoT) devices could exhaust the global address space. To provide a usable alternative to global addresses for such devices, this project will define a set of protocols that will allow ports to automatically obtain a locally-unique address in a range from a portion of the local address space. Multicast flows also need addresses to identify the flows. They will benefit from a set of protocols to distribute multicast addresses. Peer-to-peer address claiming and address server capabilities will be included to serve the needs of smaller (e.g. home) and larger (e.g. industrial plants and building control) networks.*
- Progress so far: little

Address Block Sizes (48-bit addresses)

second hex digit	address type	Admin	Block Size	Subdivision	Subdivision Block Size
..00 (0,4,8,C)	EUI-48	IEEE RA	$2^{46} \approx 7.0*10^{13}$	MA-L (OUI)	$2^{24} \approx 1.7*10^{7}$
				MA-M	$2^{20} \approx 1.0*10^{6}$
				MA-S	$2^{12} \approx 4.1*10^{3}$
..01 (2,6,A,E)	all local unicast		$2^{46} \approx 7.0*10^{13}$		
1010 (A)	ELI	IEEE RA	$2^{44} \approx 1.8*10^{13}$	CID	$2^{24} \approx 1.7*10^{7}$
1110 (E)	SAI	IEEE 802	$2^{44} \approx 1.8*10^{13}$		
0010 (2)	AAI		$2^{44} \approx 1.8*10^{13}$		
0110 (6)	*Reserved*		$2^{44} \approx 1.8*10^{13}$		

- How many is is 2^{46}?
  - IEEE manages EUI-48 space to support unique identification of hardware anywhere in the world for 100 years.
  - The SLAP gives IEEE 802 a space one quarter of that size to exploit for a LAN!

Did Gilfoyle see OUIs?

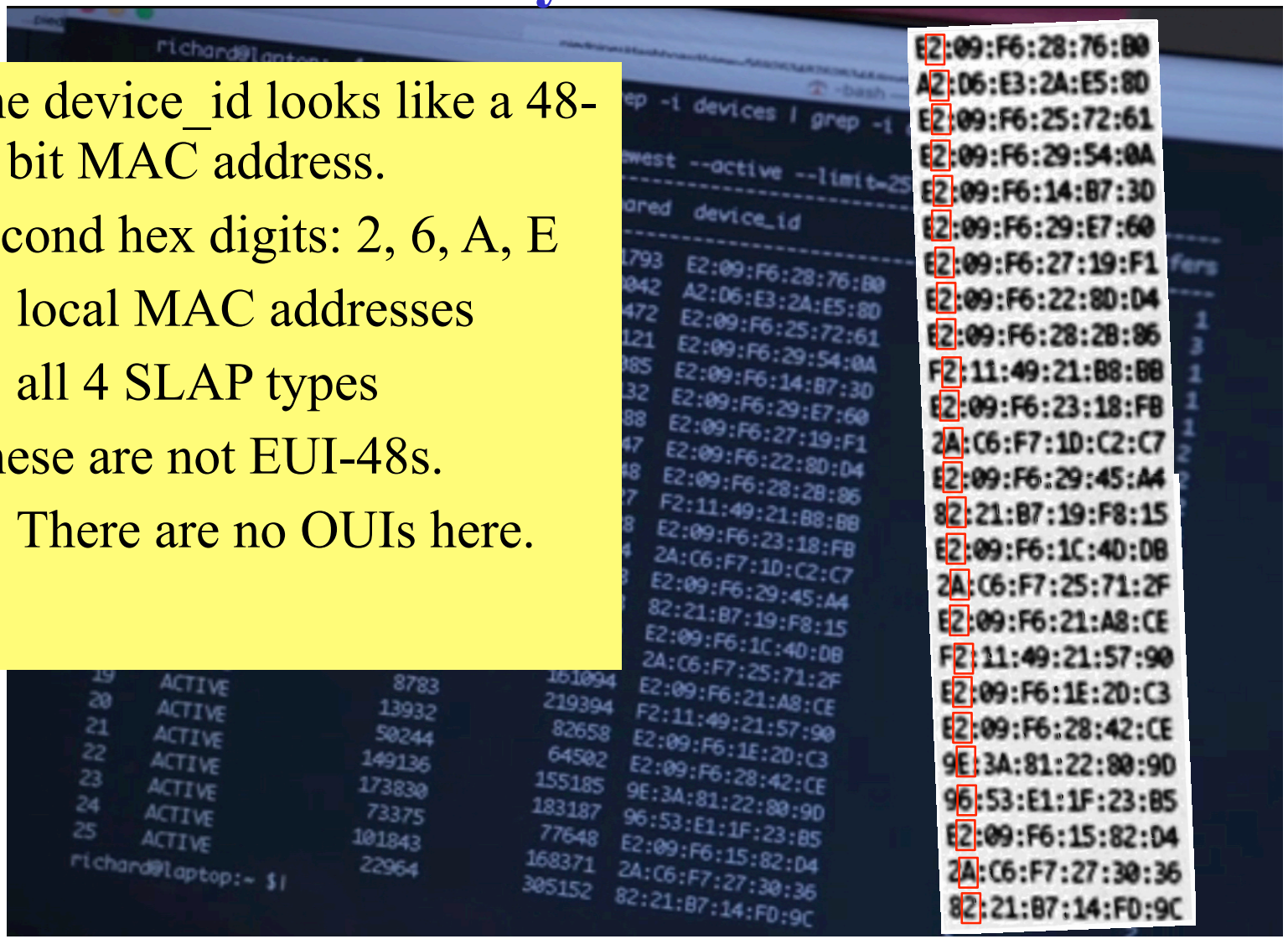
The device_id looks like a 48-bit MAC address.

Second hex digits: 2, 6, A, E

- local MAC addresses
- all 4 SLAP types

These are not EUI-48s.

- There are no OUIs here.



Did Gilfoyle see CIDs?

Six-digit prefixes are apparent.

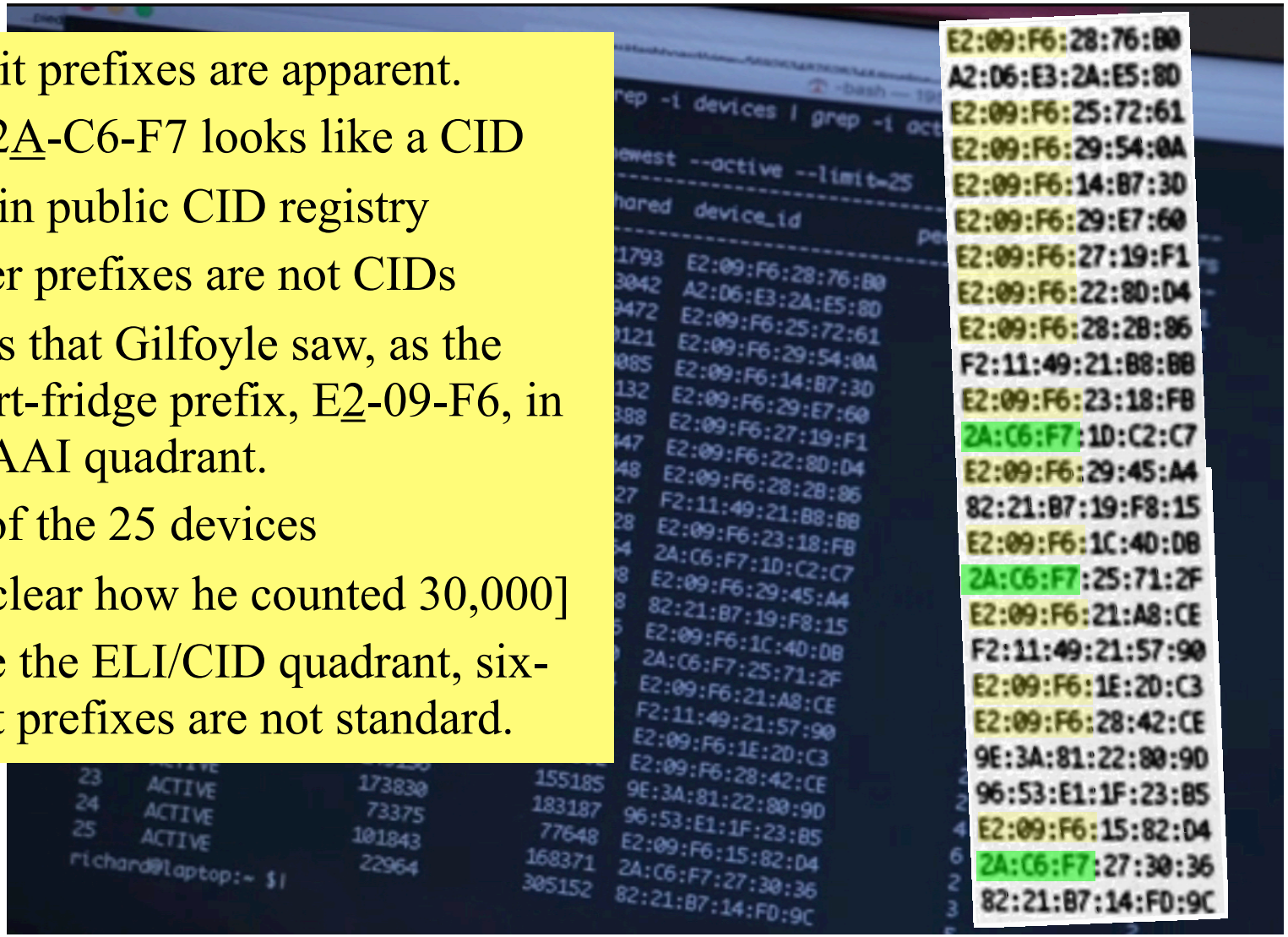
Prefix 2A-C6-F7 looks like a CID

- not in public CID registry
- other prefixes are not CIDs

It seems that Gilfoyle saw, as the smart-fridge prefix, E2-09-F6, in the AAI quadrant.

- 15 of the 25 devices
- [unclear how he counted 30,000]

Outside the ELI/CID quadrant, six-digit prefixes are not standard.



Could Gilfoyle detect smart fridges?

- In general, the MAC address is not forwarded past an IP router.
  - However, it could be tracked and passed by a device on the LAN, and then be entered into a database.
  - Devices could be programmed to send their addresses.
- Smart-fridge OUIs could potentially be identified by OUI, if the EUI was assigned under a specific smart-fridge OUI.
- Local addresses are not global and not normally permanent.
- Smart-fridge addresses would typically not be identified by CID.
  - CID is not definitively tied to the host hardware.
  - For example, CID may identify an assignment protocol.
  - It's feasible for the manufacturer to assign an address to a device as an ELI using a manufacturer's registered CID
    - extension bits could be static or dynamic

Would a fridge maker use an ELI?

- Fridge manufacturer could register a CID and assign MAC address as an ELI
  - could specify informative subfields
  - e.g. could encode model number or serial number
- This might be useful.
  - for example, a smart home hub might be able to discover the fridge solely from its address
- But it may also be dangerous
  - fridge may be susceptible to attack based on characteristics inferred from its address

Is fridge detection a good idea?

- MAC addresses are visible on the LAN, and could be tracked outside the LAN.
  - This could lead to a privacy violation.
  - But it could offer opportunities
    - Gilfoyle took advantage of a property of an address
    - Other addresses can have other special properties
    - Network management takes advantage of known addresses
- If we keep informative addresses separate from flat (e.g. random) addresses, then we can support both types on the LAN.
- If we don't keep them separate, then we may see collisions.

IEEE 802 is SLAP Happy

- The SLAP offers:
  - organizations a block of ~17M addresses for innovative ELI uses
  - IEEE 802 a block of ~ $1.8*10^{13}$ addresses for innovative SAI uses
  - administrators a block of ~ $1.8*10^{13}$ addresses to do what they want while avoiding collision with ELI and SAI users
- The SAI block is a huge opportunity for IEEE 802!
- Let's use it!

Annex 1: IEEE RA Tutorial – Guidelines for Use of EUI, OUI, CID

IEEE RA Tutorial – Guidelines for Use of EUI, OUI, CID

- IEEE Registration Authority assigns OUIs, CIDs, etc.
- Provides tutorials on identifiers and policies:
  - http://standards.ieee.org/develop/regauth/tut
- Tutorial on EUI (referenced in IEEE Std 802):
- *Guidelines for Use of Extended Unique Identifier (EUI), Organizationally Unique Identifier (OUI), and Company ID (CID)*
  - Published August 2017, in coordination with 802c
  - Supersedes:

    Guidelines for Use Organizationally Unique Identifier (OUI) and Company ID (CID)

    Guidelines for 48-Bit Global Identifier (EUI-48)

    Guidelines for 64-bit Global Identifier (EUI-64)

Guidelines for Use of EUI, OUI, CID – more details

- Published August 2017
  - http://standards.ieee.org/develop/regauth/tut/eui.pdf
- Covers local addresses, SLAP, CID, and ELI
- Clarifies other policies; notably (unrelated to local addressing) regarding the multicast bit:
  - *The assignee of an OUI or OUI-36 is exclusively authorized to assign group MAC addresses, with I/G=1, by extending a modified version of the assigned OUI or OUI-36 in which the M bit is set to 1. Such addresses are not EUIs and do not globally identify hardware instances, even though U/L=0.*
  - *The assignee of a CID may assign local group MAC addresses by extending a modified version of the assigned CID by setting the M bit to 1 (so that I/G=1). The resulting extended identifier is an ELI.*

Annex 2: Non-permanent Addresses

Non-permanent Addresses

- IEEE 802 is most familiar with permanent addresses
- Local addresses are typically not permanent
  - they may be assigned during use
- Need to consider the ramifications

Some Address Features

- Uniqueness
  - most fundamental property
  - local (on the LAN), or universal
  - relevant to identity
- Permanence/Longevity
  - relevant to trackability
  - relevant to management
- Structure and Information content
  - Does the address convey information beyond identity?
  - Can address convey location (e.g., IP)
  - other possibilities

Example: IPv4

- IPv4 address can be globally routable
- IPv4 address can be local
- IPv4 address is hierarchical, with two components:
  - prefix: identifies network or subnet
  - host identifier: identifies interface
  - must separately specify the prefix length to distinguish the two

View from IETF: IPv6

For ideas on possible protocols, consider IETF.

- IPv6 unicast address (128 bits) includes:
  - subnet prefix (*n* bits, typically 64)
  - interface ID (IID) (128-*n* bits, typically 64)
    - used to identify interfaces on a link
    - formerly encouraged creation from IEEE EUI (e.g. RFC 4291)
    - RFC 7136: *various new forms of IIDs have been defined: including temporary addresses [RFC4941], Cryptographically Generated Addresses (CGAs) [RFC3972] [RFC4982], Hash-Based Addresses (HBAs) [RFC5535] …*

Some IPv6 IID Forms

- temporary addresses [RFC4941]
  - use with SLAAC; IID changes for privacy
- Semantically Opaque Interface Identifiers [RFC7217]
  - use with SLAAC; IID changes when subnet changes
  - *benefits of stable addresses can be achieved without sacrificing the security and privacy of users*
- Cryptographically Generated Addresses (CGAs) [RFC3972]
  - verification of source address
- Hash-Based Addresses (HBAs) [RFC5535]
  - bind multiple addresses assigned to a single host
- ISATAP addresses [RFC5214]
  - IPv4 address embedded in IPv6 address

Some Assignment Protocols

- Stateful (per IETF)
  - typically server-based
  - example: DHCP
- Stateless (per IETF)
  - IPv6 “Stateless Address Autoconfiguration” (SLAAC)
    - could be based on IEEE EUI
    - requires Duplicate Address Detection (DAD)
- claiming
  - device claims an address by announcement, but:
    - may probe first for addresses in use
    - may check afterwards for collisions

✶P802.1CQ PAR mentions “peer-to-peer address claiming and address server capabilities”

IETF: Temporary Addresses

- SLAAC = "Stateless Address Autoconfiguration"
- RFC 4941: Privacy Extensions for SLAAC in IPv6
  - Sept. 2007
  - *…for interfaces whose interface identifier is derived from an IEEE identifier. Use of the extension causes nodes to generate global scope addresses from interface identifiers that change over time, even in cases where the interface contains an embedded IEEE identifier. Changing the interface identifier (and the global scope addresses generated from it) over time makes it more difficult for eavesdroppers and other information collectors to identify when different addresses used in different transactions actually correspond to the same node.*

Semantically Opaque Interface Identifiers

- RFC 7217
  - Apr. 2014
  - *temporary addresses can be challenging.... from a network-management point of view, they tend to increase the complexity of event logging, troubleshooting, enforcement of access controls, and quality of service.... some organizations disable the use of temporary addresses even at the expense of reduced privacy… may also result in increased implementation complexity*
  - *...Interface Identifier changes when the host moves from one network to another. This method is meant to be an alternative to generating Interface Identifiers based on hardware addresses (e.g., IEEE LAN Media Access Control (MAC) addresses), such that the benefits of stable addresses can be achieved without sacrificing the security and privacy of users.*

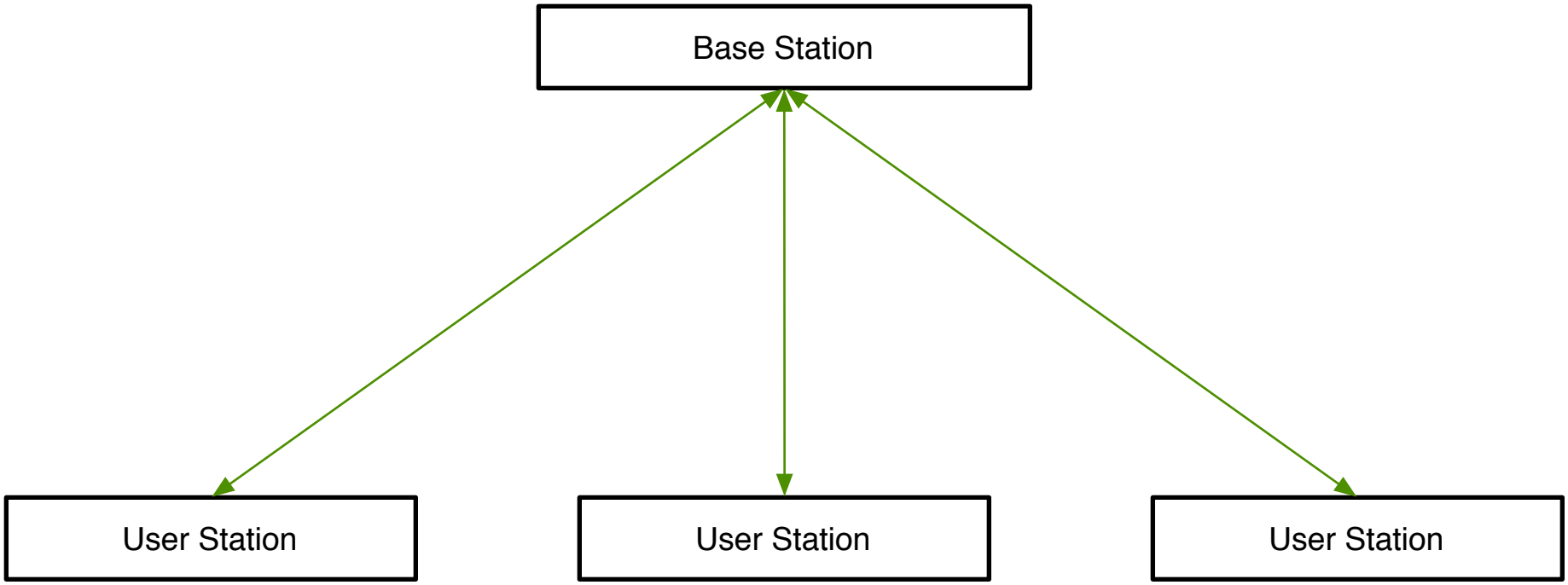
IETF CGA

- CGA = "Cryptographically Generated Address"
- RFC 3972
  - March 2005
  - *interface identifier is generated by computing a cryptographic one-way hash function from a public key and auxiliary parameters. The binding between the public key and the address can be verified by re-computing the hash value and by comparing the hash with the interface identifier. Messages sent from an IPv6 address can be protected by attaching the public key and auxiliary parameters and by signing the message with the corresponding private key. The protection works without a certification authority or any security infrastructure.*
  - includes collision count field based on duplicate address detection

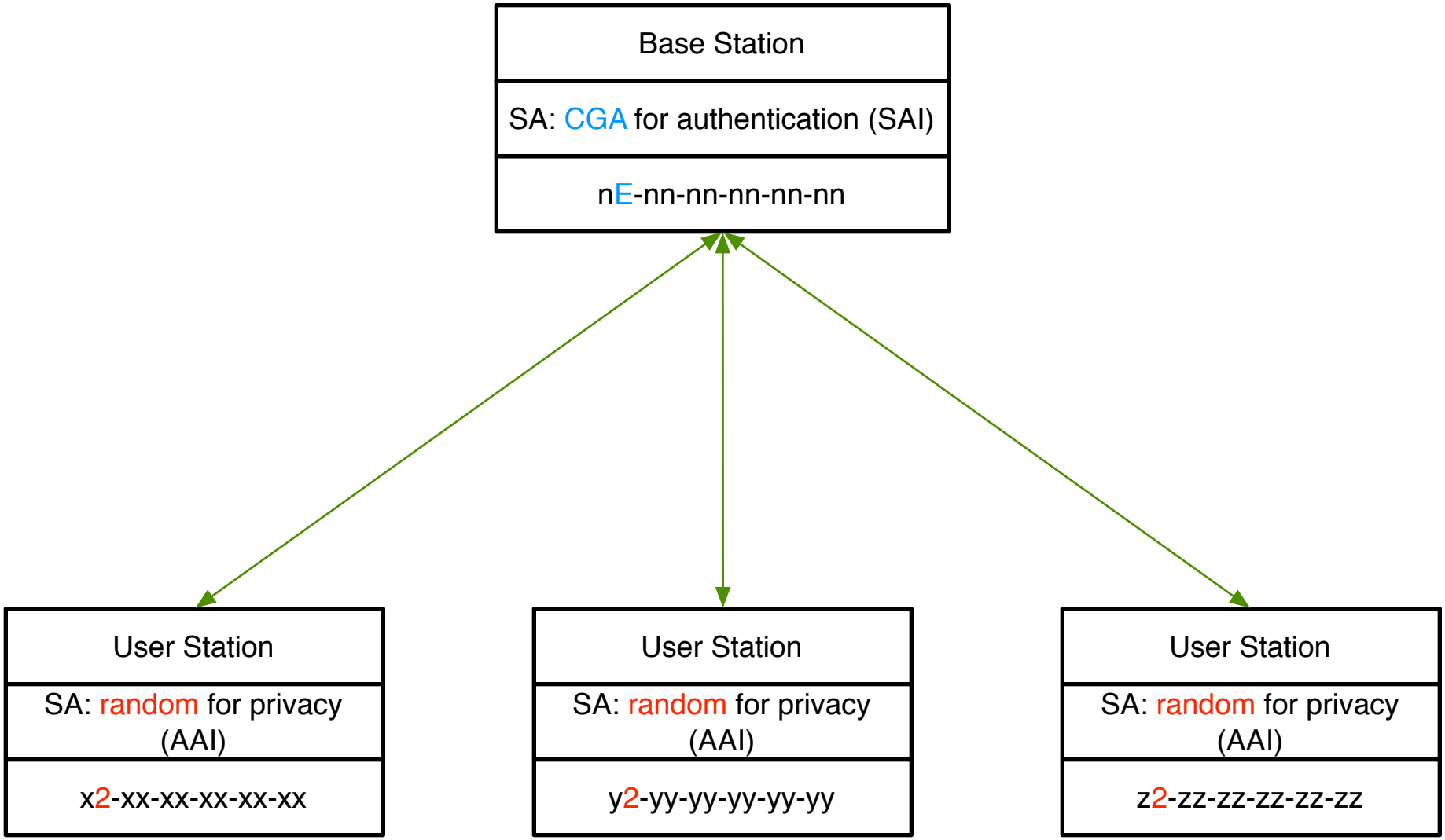
Example: CGA and Privacy can coexist

- On a LAN, some devices strive for privacy
  - may use a randomized address
- On a LAN, some devices may not value privacy but put value on other features, such as verification
  - example: servers should be easily found
  - address may be structured for meaning
- Both types of devices should be able to coexist
  - random addresses should stay out of assigned space
  - receiver can then determine the type of address and respond accordingly

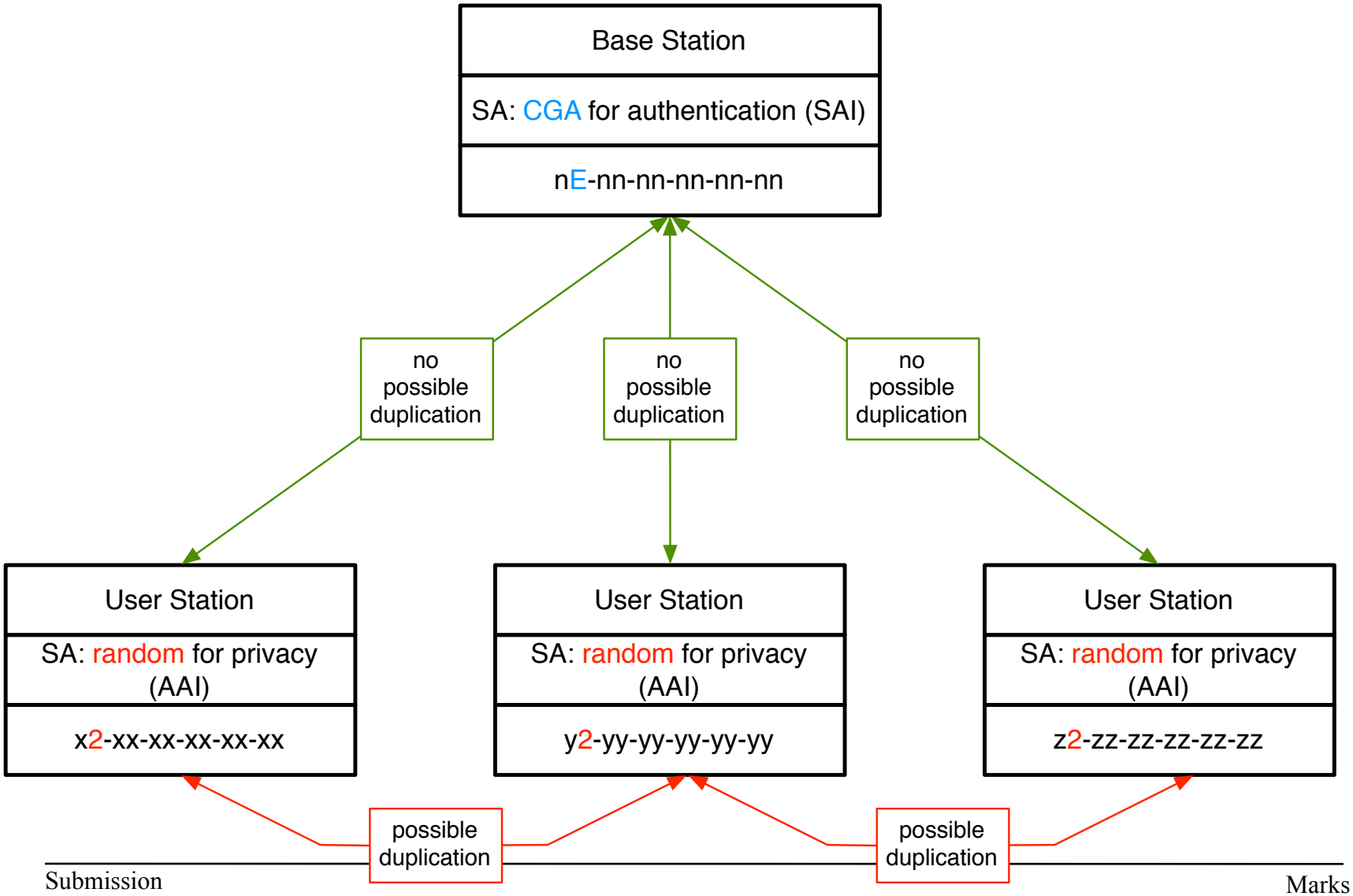
CGA/Privacy Coexistence



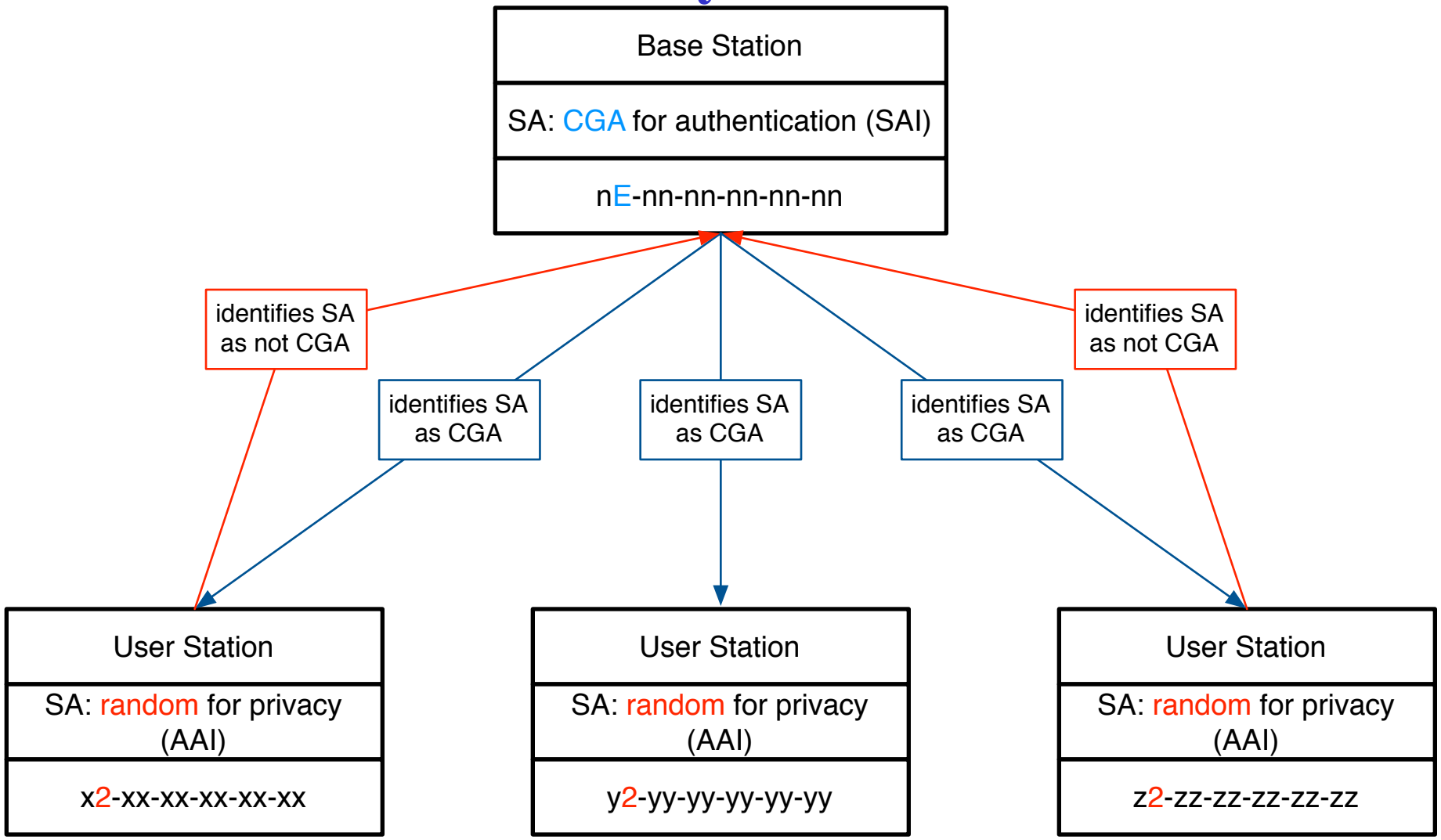
CGA/Privacy Coexistence



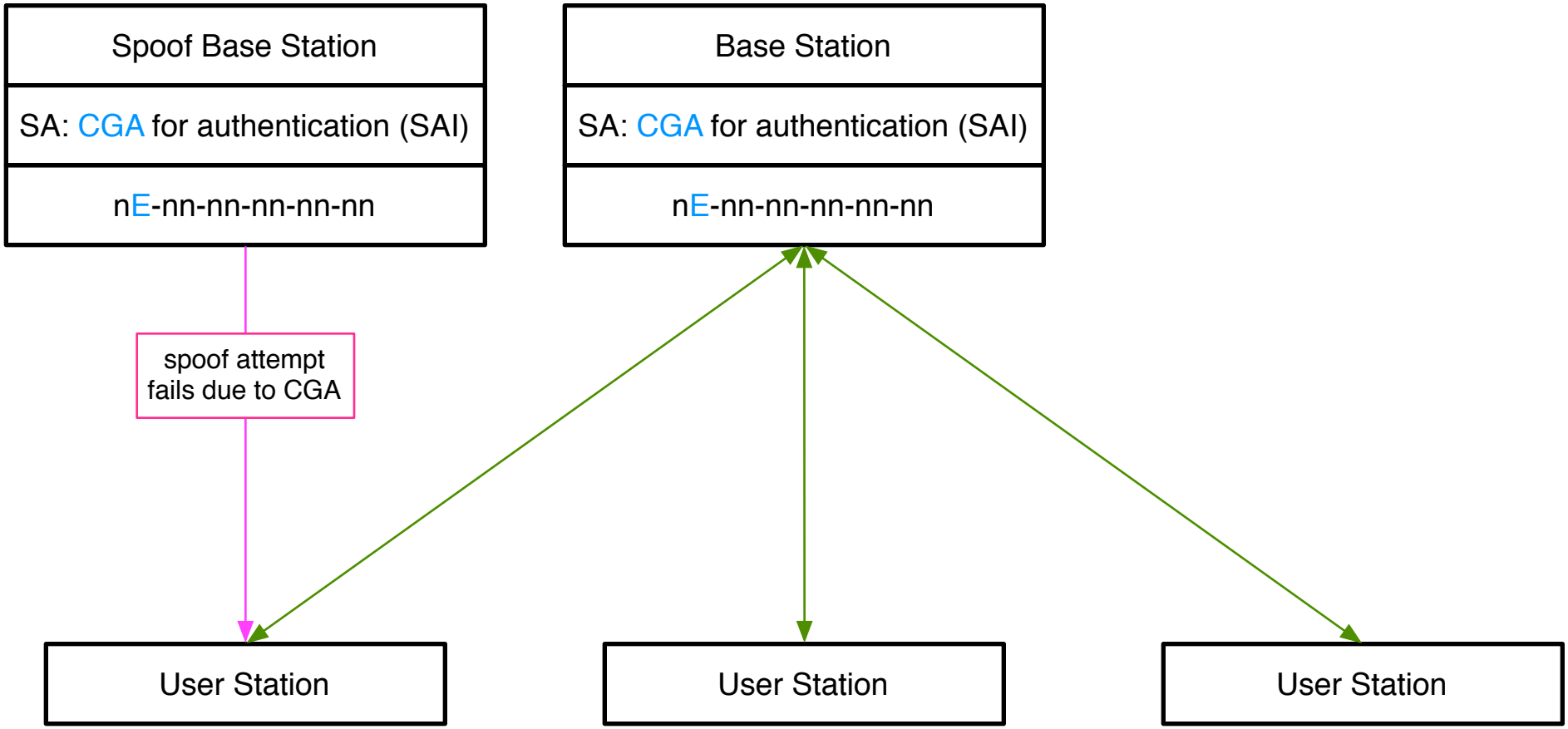
CGA/Privacy Coexistence



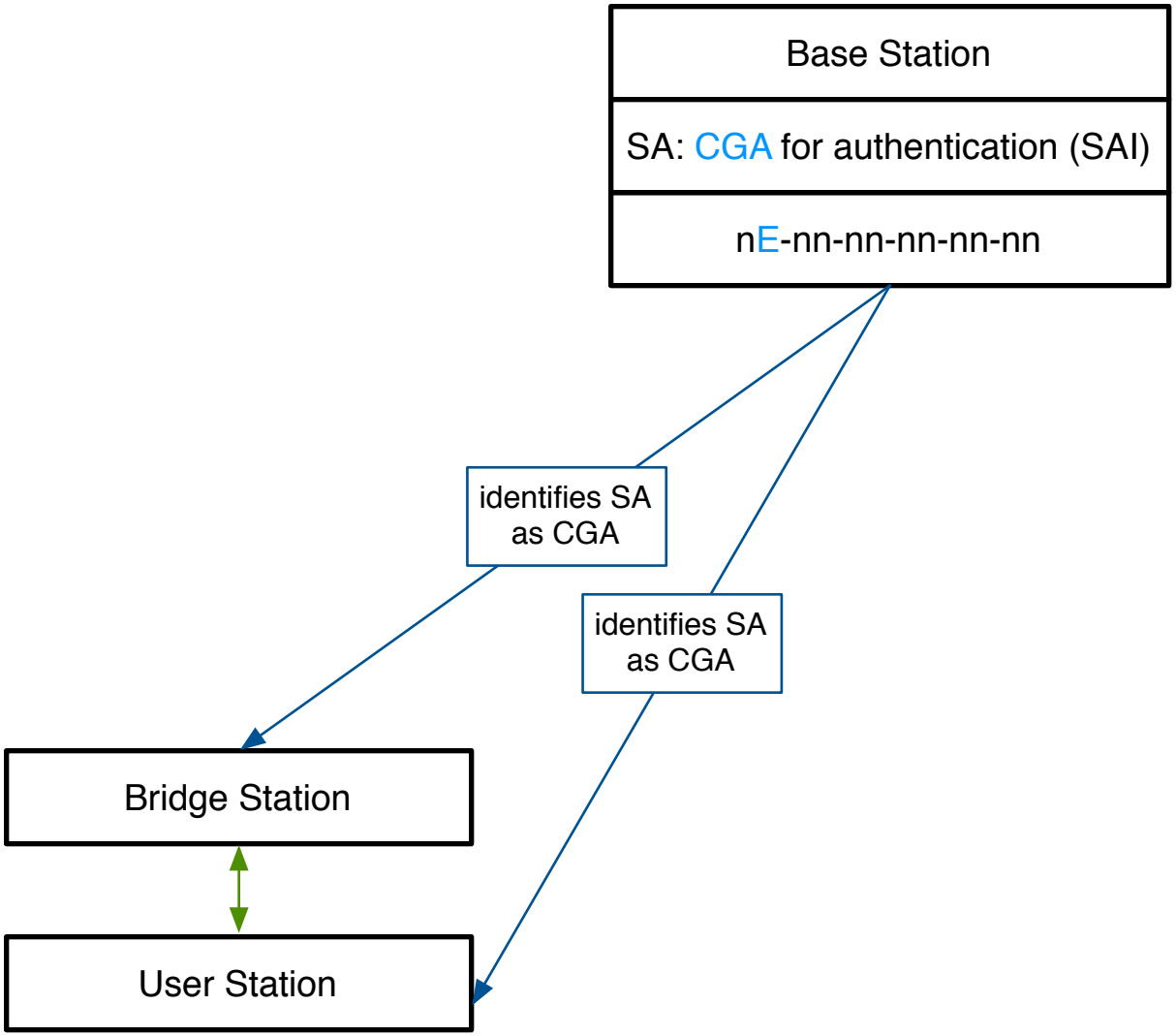
CGA/Privacy Coexistence



CGA/Privacy Coexistence



CGA/Privacy Coexistence



Summary

- The local address space is huge and valuable.
- The IEEE RA's CID give companies a chance to innovate
  - SLAP supports ELIs based on CID
  - 802 standards should not step on any company's ELIs
- SLAP specifies a reserved quadrant
  - 802 standards should not step on it
- SLAP specifies an AAI quadrant
  - 802 standards should use the AAI quadrant in any way
- SLAP offers a 44 bit SAI quadrant to IEEE 802 to exploit.
  - 802 standards should put SAI to use in an orderly fashion.
- Let's ensure protocol coexistence for best success.
- Please participate in development of P802.1CQ.