FCoE: Unified ACL Theory

T11/08-058v0

Joe Pelissier, Cisco

Claudio DeSanti, Cisco

John Hufferd, Brocade

Anoop Ghanwani, Brocade

Introduction

- **T11/08-038v0, *FCoE Common Addressing Structure,* provides a framework in which both SPMA and FPMA may be supported in FC-BB-5**
  - **The scheme and protocol proposed endeavors to allow both addressing methods to operate in a substantially similar manner**
- **This presentation proposes a common ACL framework**
  - **As is the case with the addressing proposals, this framework endeavors to make the ACLs as agnostic as possible between the two methods**
- **This presentation is intended to be an informative discussion of best practices related to ACLs and FCoE**
  - **This may result in an informative annex in FC-BB-5, but there is no intention for this to be normative**

Observations and Goals

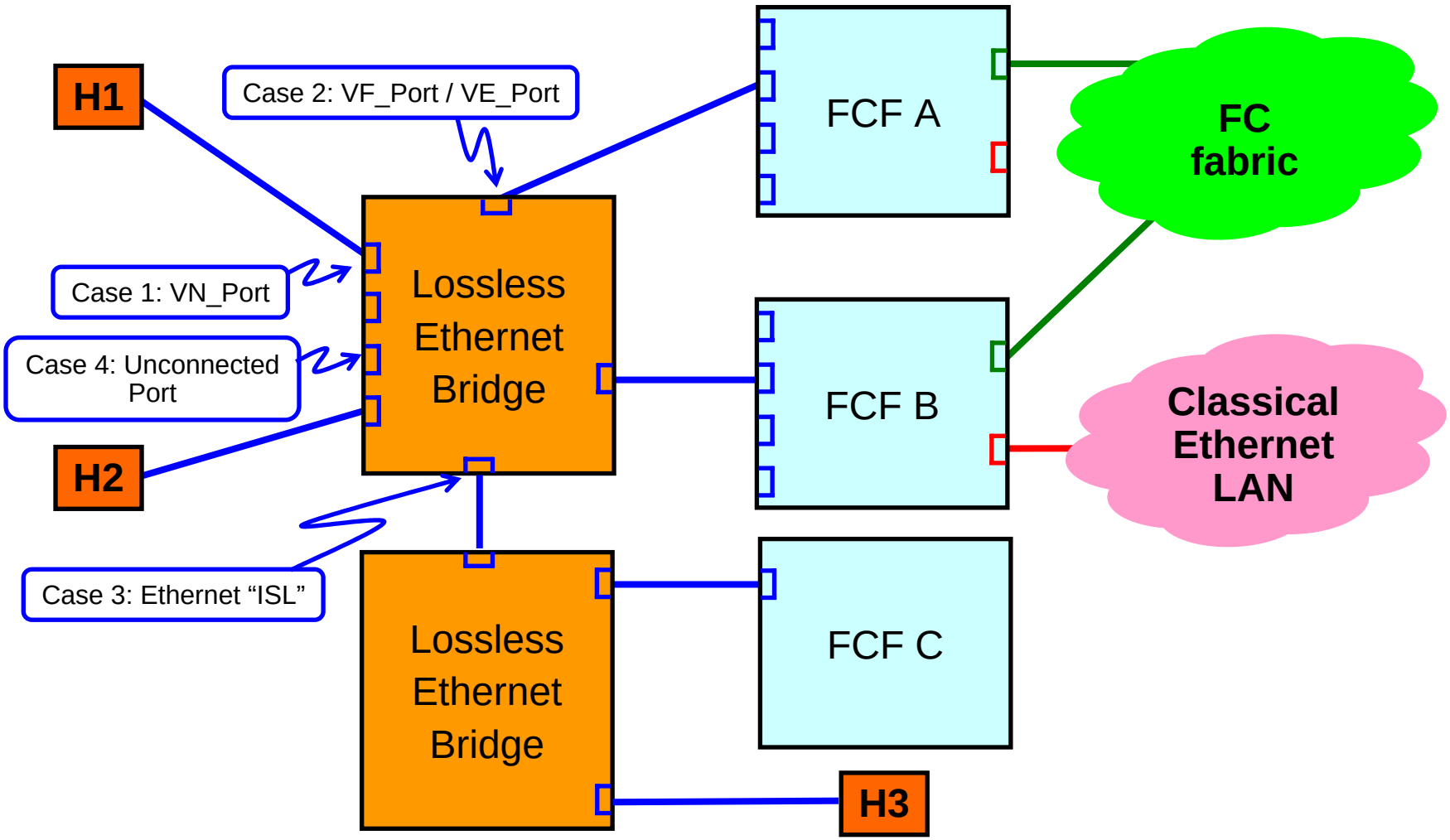
- **The use of ACLs in data centers varies widely today**
  - **Use ranges from not used at all to completely locking down every port**
- **It has been shown and generally agreed upon that ACLs may be used in FCoE to effectively address the various "Whack-a-Mole™" scenarios**
  - **See 07-683v1 for examples**
- **It is highly desirable that it be possible to deploy FCoE with a level of security and robustness comparable to Fibre Channel**
  - **Given that Storage and LAN fabrics are generally administered by different groups within the IT organization, it may well be that the desired level of security and robustness may differ between the two applications**
    - Furthermore, different techniques may be used to achieve the desired level of security and robustness between the two applications

Observations and Goals

- **In a converged fabric, it is highly desirable to eliminate any interdependencies between the FCoE related ACE's and whatever ACE's may be utilized for the remaining LAN traffic**
- **Note that this presentation assumes that VN_Port MAC addresses are used exclusively for FCoE traffic**

  However, if it is desired to use the same MAC address for FCoE and LAN traffic, the ACLs are easily modified to accommodate this
- **The Source MAC address used by ENodes for FIP frames may or may not be used exclusively for that purpose**

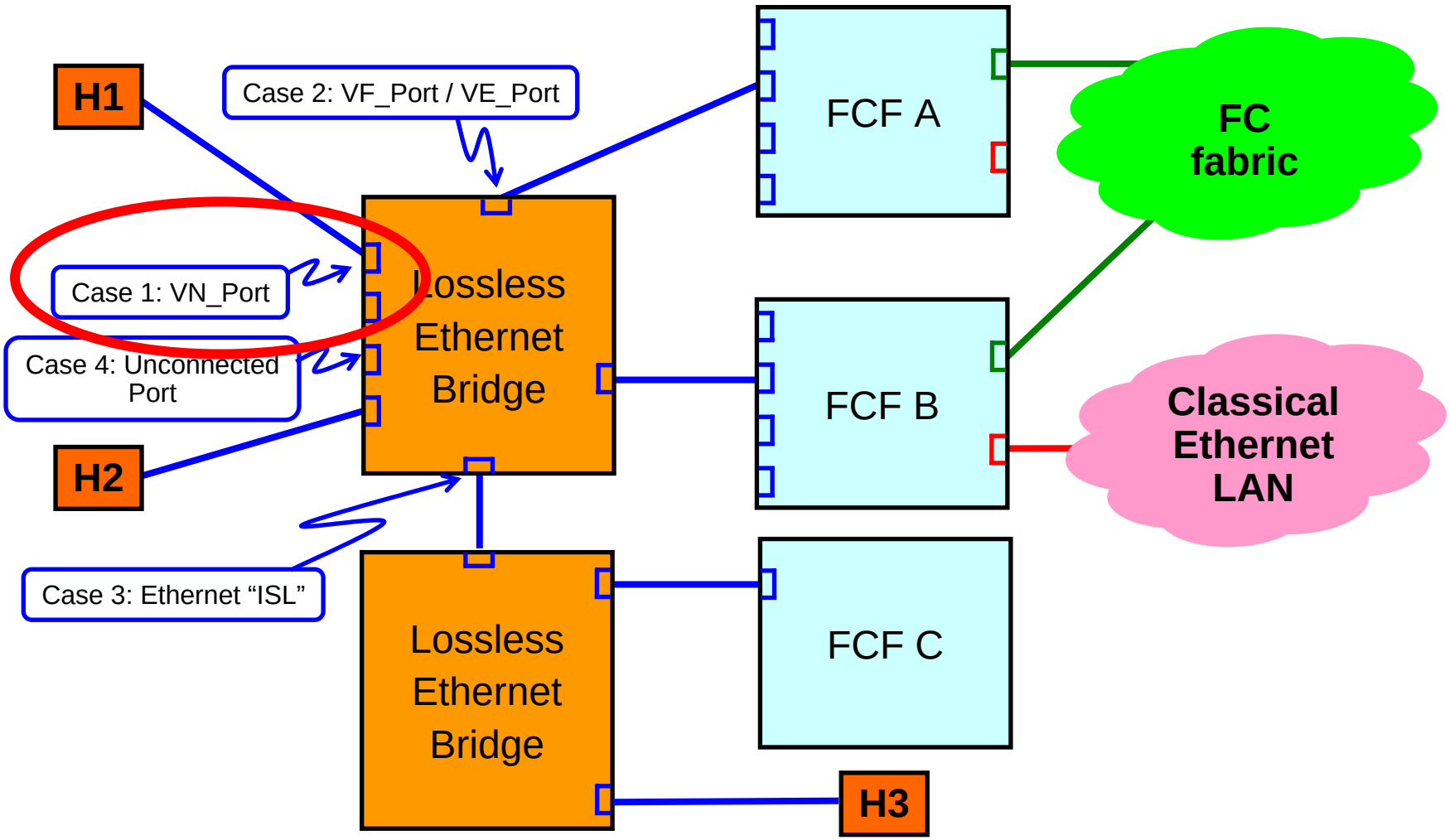
Four Possible ACLs Examined



The Variables:

- **MAC{FCoE}: the set of valid FCoE MAC addresses of VN_Ports that may be received on a given switch port. (Note that for SPMA, this set is identical to MAC{FIP} below)**
- **MAC{FIP}: the set of valid FIP MAC addresses that may be received on a given switch port**
- **MAC{FCF}: the set of valid FCF MAC addresses that may be received on a given switch port**
- **MAC{non-FCoE MACs}: the set of all valid MAC addresses that may be received on a given switch port except those used exclusively for FCoE (if a MAC is shared between FCoE and other uses, then it is included in this set)**
- **All-FCFs: the multicast address that targets all FCFs**
- **FC_MAP: the prefix that identifies FPMA MAC addresses. For simplicity, this presentation assumes FC_MAPs are 24 bits. Other smaller sizes may also be used**
- **FIP: FIP Ethertype**
- **FCoE: FCoE Ethertype**

Four Possible ACLs Examined



Requirements of the VN_Port FCoE ACL (1)

- **Enable transmission of FCoE frames with a valid FCoE source address**

  SA = MAC{FCoE}, DA=MAC{FCF}, Eth=FCoE, permit

  One entry like the above is required for each VF_Port reachable from the switch port

  These may be added statically or dynamically via snooping when the "link" is formed

  Static configuration may require gaining knowledge of the MAC addresses to be assigned via means not necessarily covered by standards.

- **Ensure that ENode unicast FIP frames travel only between VN_Ports and VF_Ports**

  SA=MAC{FIP}, DA=MAC{FCF}, Eth=FIP, permit

  Note that this requires a priori knowledge of the source MAC the device will use for FIP frames

  If this is not known, the "SA=MAC{FIP}" term may be omitted. Doing so opens a slight risk of a DOS attack on initialization.

- **Enable transmission of multicast FIP frames**

  SA=MAC{FIP}, DA=All-FCFs, Eth=FIP, permit

  Same note as above with respect to the source MAC address

Requirements of the VN_Port FCoE ACL (2)

Disable transmission of any other FIP or FCoE frame

- **Eth=FIP, deny**
- **Eth=FCoE, deny**

Requirements of the VN_Port FCoE ACL (3)

- **Remaining Pre-existing ACEs**

  Note that the above ACEs are all specifically related to FCoE and FIP, and are therefore guaranteed to not conflict with any pre-existing, non-FCoE related ACEs

  Assuming they are placed prior to the pre-existing ACEs

- **Protection against Rogue Host Learning Address**

  Note that the pre-existing ACL may provide some of the ACEs required to achieve this

  Must ensure that pre-existing ACL does not contain a permit that would enable any source MAC address (e.g. Eth=IP, permit)

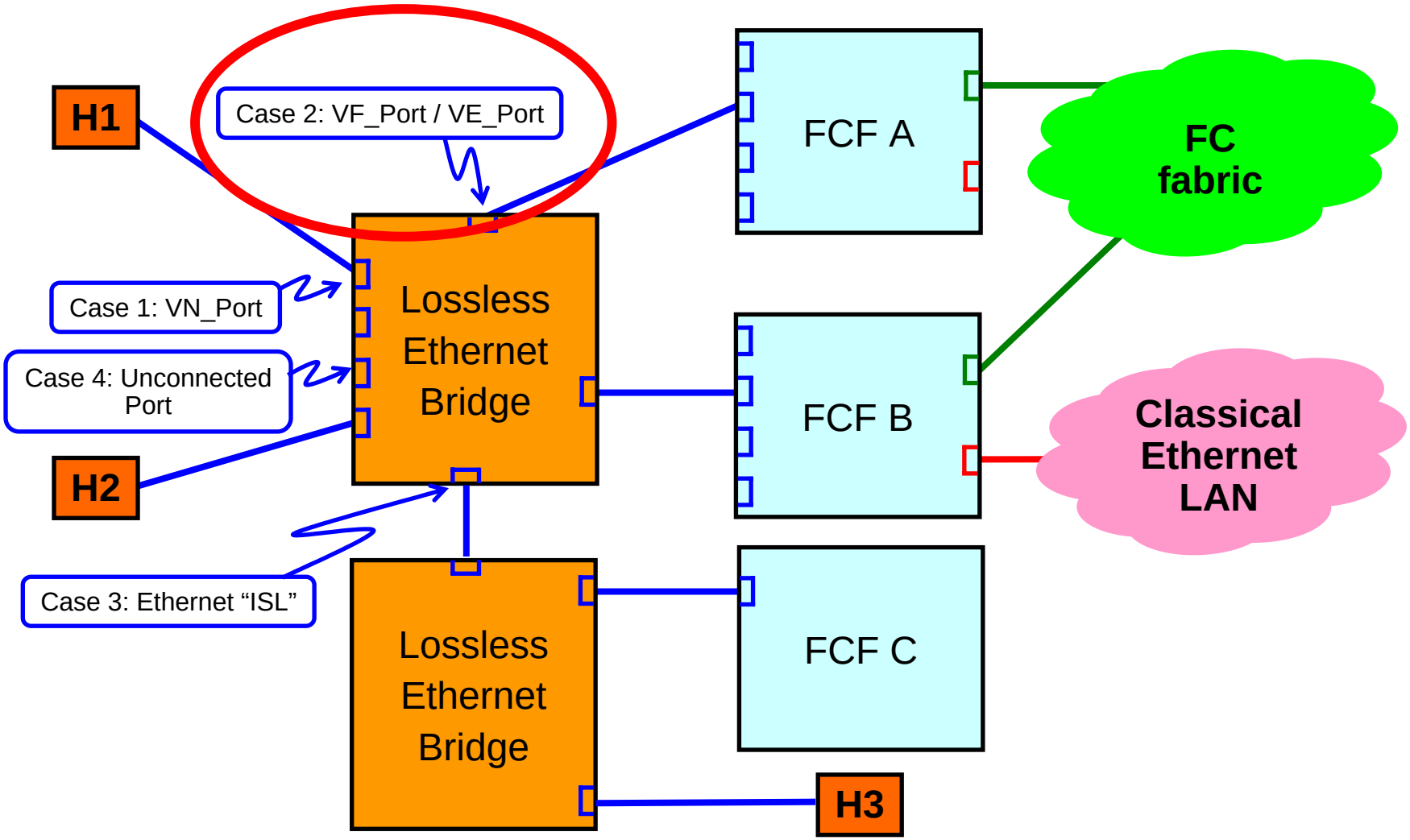
  Explicitly enable all valid MAC addresses and deny all others

  SA=MAC{non-FCoE MACs}, permit

  Deny

  Note: There are frequently simpler ways to achieve this that depend on specific deployment scenarios (e.g. virtualization middleware, addressing mode selected, etc.)

Four Possible ACLs Examined



Requirements of the VF_Port / VE_Port ACL

- **It is debatable whether any ACL is required for a port dedicated to an FCF**

  FCFs are generally trusted devices

  However, if you are truly paranoid…

- **Enable FIP and FCoE traffic from the FCF**

  SA=MAC{FCF}, Eth=FIP, permit

  SA=MAC{FCF}, Eth=FCoE, permit

- **Disable any other traffic with the FCF MAC address (unless it is being used for other traffic types)**

  SA=MAC{FCF}, Deny

- **Disable any FCoE or FIP traffic that does not contain the FCF's MAC address**

  Eth=FIP Deny

  Eth=FCoE Deny

Requirements of the VF_Port / VE_Port ACL

- **Remaining Pre-existing ACEs**

  Note 1: In many cases, with a direct connection to an FCF, there would be no pre-existing ACEs

  However, if the FCF is co-located with other functions (e.g. IP routing), then pre-existing ACEs may exist

  Note 2: the above ACEs are all specifically related to FCoE and FIP, and are therefore guaranteed to not conflict with any pre-existing, non-FCoE related ACEs

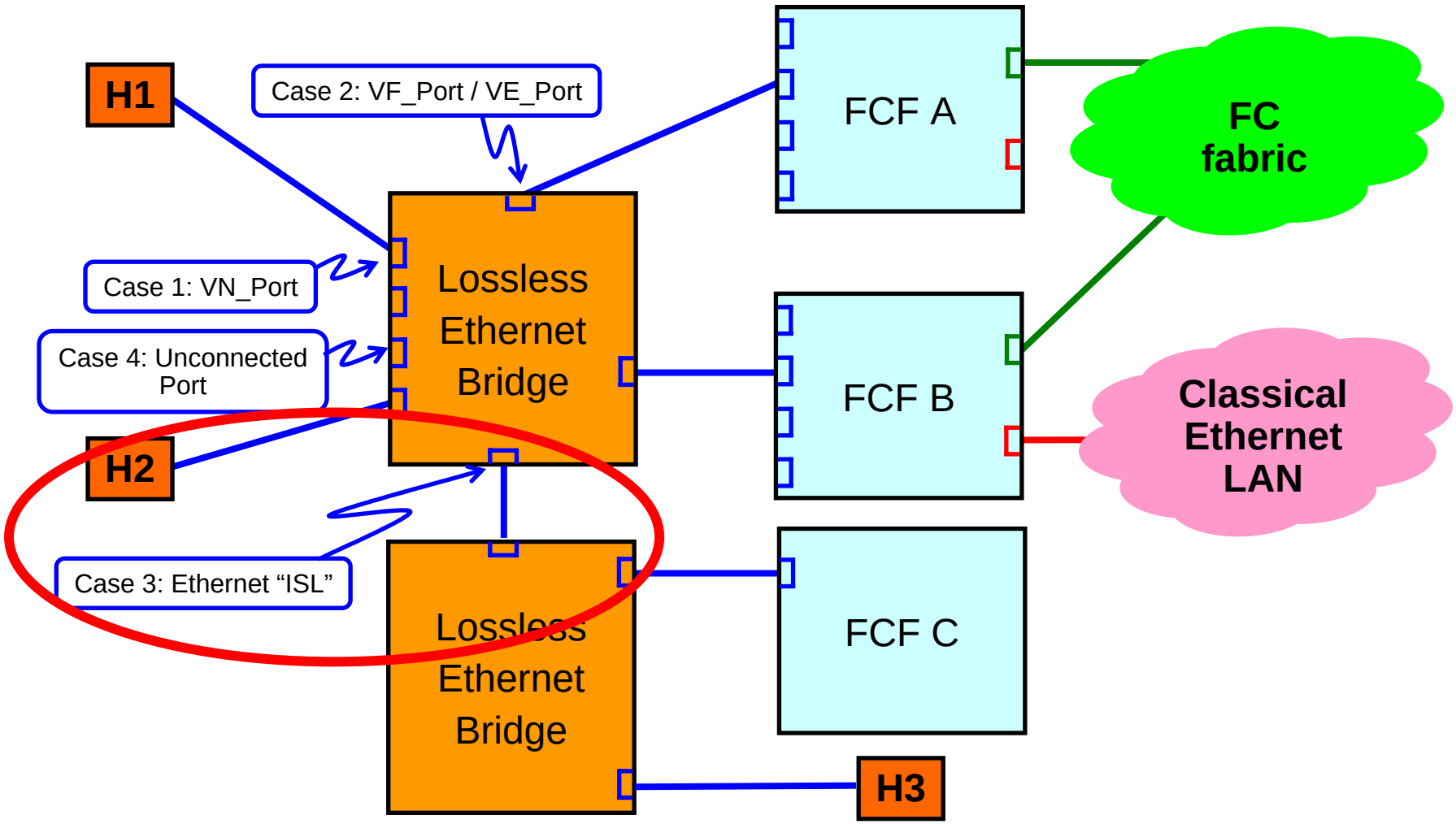
  This assumes that the MAC address for the FCF is not used for any other purpose (e.g. shared with a co-located IP router). If the address is shared, a more complex form of the ACEs may be developed to accommodate this. Doing so is left as an exercise to any vendor that wishes to deploy such a device.

- **Note: this ACL does not provide for Rogue Host Protection; it is assumed that the FCF provides this protection**

  It may not be possible in the general case to assure direct connection to an FCF, or to be assured that the FCF is providing the protection

  In this case, use the Ethernet "ISL" ACL instead

Four Possible ACLs Examined



Requirements of the Ethernet “ISL” ACL (1)

- **In many cases, deploying an ACL on ISLs is not practical**
  - **The number of ACEs exceeds the scalability limits of most switches**
- **Therefore, best practice would dictate that the fabric should be secured at the edges using the previously described VN_Port ACL**
- **For completeness, and to illustrate the challenge of deploying it, the ISL ACL is described**

Requirements of the Ethernet “ISL” ACL (2)

- **Enable transmission of FCoE frames with a valid FCoE source address**
  - **SA = MAC{FCoE}, DA=MAC{FCF}, Eth=FCoE permit**
  - **One entry like the above is required for each VF_Port on the link**
  - **These may be added statically or dynamically via snooping**
- **Ensure that unicast FIP frames travel only between VN_Ports and V_FPorts**
  - **SA=MAC{FIP}, DA=MAC{FCF}, Eth=FIP, permit**
  - **SA=MAC{FCF}, DA=MAC{FIP}, Eth=FIP, permit**
  - **Note that this requires a priori knowledge of the source MAC the device will use for FIP frames**
    - If this is not known, the “SA=MAC{FIP}” and “DA=MAC{FIP}” terms may be omitted. Doing so opens a slight risk of a DOS attack on initialization.
- **Enable transmission of multicast FIP frames**
  - **SA=MAC{FIP}, DA=All-FCFs, Eth=FIP, permit**
  - **Same note as above with respect to the source MAC address**
- **Enable FIP and FCoE traffic from the FCF**
  - **SA=MAC{FCF}, Eth=FIP, permit**
  - **SA=MAC{FCF}, Eth=FCoE, permit**

Requirements of the Ethernet “ISL” ACL (2)

- **Disable any other traffic with the FCF MAC address (assuming the FCF MAC address is not shared with any other purpose)**

  SA=MAC{FCF}, deny

- **Disable transmission of any other FIP or FCoE frame**

  Eth=FIP, deny

  Eth=FCoE, deny

Requirements of the Ethernet “ISL” ACL (3)

- **Remaining Pre-existing ACEs**

  Note that the above ACEs are all specifically related to FCoE and FIP, and are therefore guaranteed to not conflict with any pre-existing, non-FCoE related ACEs

  Assuming they are placed prior to the pre-existing ACEs

- **Protection against Rogue Host Learning Address**

  Note that the pre-existing ACL may provide some of the ACEs required to achieve this

  Must ensure that pre-existing ACL does not contain a permit that would enable any source MAC address (e.g. Eth=IP, permit)

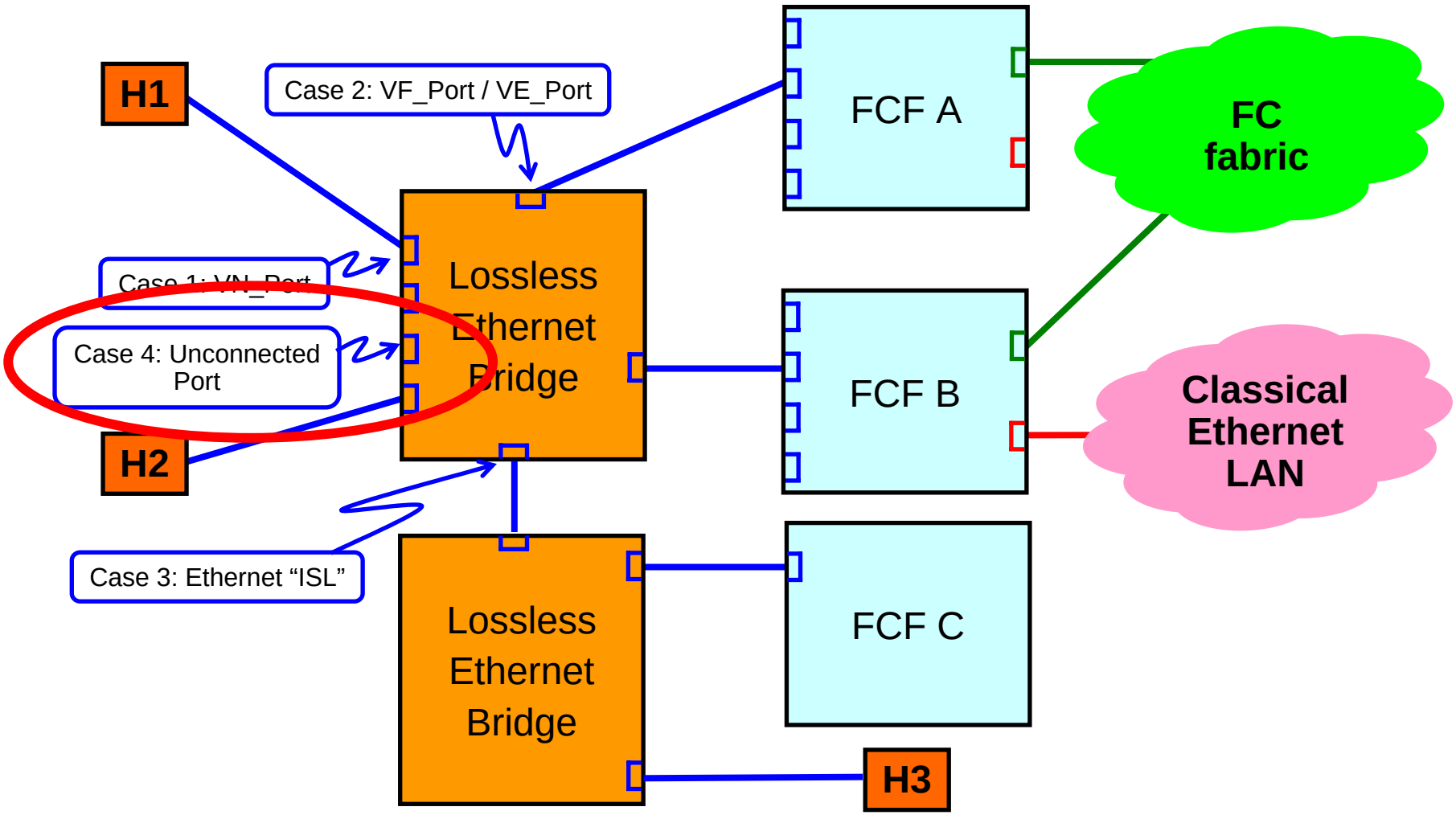
  Explicitly enable all valid MAC addresses and deny all others

  SA=MAC{non-FCoE MACs}, permit

  Deny

  Note: There are frequently simpler ways to achieve this that depend on specific deployment scenarios (e.g. virtualization middleware, addressing mode selected, etc.)

Four Possible ACLs Examined



Requirements of the Unconnected Port ACL (1)

- **The ACL for unconnected ports depends on site policy**

  Option 1: Nothing is allowed to connect without management approval

  Port is simply disabled (port shut down, ACL set to deny, etc.)

  Appropriate ACL is loaded before port is enabled

  Option 2: LAN devices may connect but no FCoE related traffic is allowed:

  Eth=FIP, deny

  Eth=FCoE, deny

  Utilizing this as a "best practice" helps to prevent some of the looping scenarios presented by David Black

  Option 3: Devices may connect and use FIP. All other FCoE traffic is prohibited until completion of FIP

  Eth=FCoE, deny

  Note: Opens potential that rogue host could disrupt FIP traffic. If a device uses the same address for FIP and FCoE traffic (SPMA), then the attack could disrupt or intercept the storage traffic

The Unified FCoE ACL

VN	VF	ISL	UN	Access Control Entry	Notes
x		x		SA=MAC{FCoE}, DA=MAC{FCF}, Eth=FCoE, permit	;Enable FCoE frames from VN_Ports
x		x		SA=MAC{FIP}, DA=MAC{FCF}, Eth=FIP, permit	;Enable unicast FIP frames
		x		SA=MAC{FCF}, DA=MAC{FIP}, Eth=FIP, permit	
x		x		SA=MAC{FIP}, DA=All-FCFs, Eth=FIP, permit	;Enable multicast FIP frames
	x	x		SA=MAC{FCF}, Eth=FIP, permit	;Enable FIP frames from FCF
	x	x		SA=MAC{FCF}, Eth=FCoE, permit	;Enable FCoE frames from FCF
	x	x		SA=MAC{FCF}, deny	;Deny non FCoE and FIP traffic from FCF
x	x	x	x	Eth=FIP, deny	;Deny FIP with invalid SA
x	x	x	x	Eth=FCoE, deny	;Deny FCoE with invalid SA
x	x	x	x	Pre-existing ACL	;Possibly modified if RHLA protection ;desired
x		x		SA=MAC{non-FCoE MACs}, permit	;Req. only for RHLA protection, Enable all ;other valid MAC addresses
x		x		deny	;Req. only for RHLA protection, deny ;everything else

Notes:
VN: ACE used in VN_Port ACL
VF: ACE used in VF_Port / VE_Port ACL
ISL: ACE used in the switch "ISL" ACL
UN: ACE used in the unconnected port ACL

Also, note that the switch ISL ACL is a superset of the other ACLs and may be used in all cases.

Static Forwarding Table Entries

- **Note that learning in some Ethernet switches is not filtered by the ACLs**
  - **This is compensated for by creating a static forwarding entry for the source address in each “permit” ACE**
- **These static forwarding entries do not eliminate the need for the ACEs**
  - **Static forwarding entries do not perform ingress filtering**
  - **Therefore, the static forwarding entry prevents a learning attack, but not an imposter attack**

Static and Dynamic ACL Creation

- **The resultant ACL is identical regardless of whether created statically or dynamically**
- **Dynamic ACL creation is identical for both SPMA, FPMA, or a mix**
- **The common ACL requires an ACE specific to each assigned MAC address, namely:**

  SA=MAC{FCoE}, DA=MAC{FCF}, Eth=FCoE, permit
- **These entries may be statically configured**
- **Alternatively, these entries may be dynamically populated using snooping**

  Similar to IGMP snooping

  FLOGI Accepts contain all the information necessary to populate the ACE

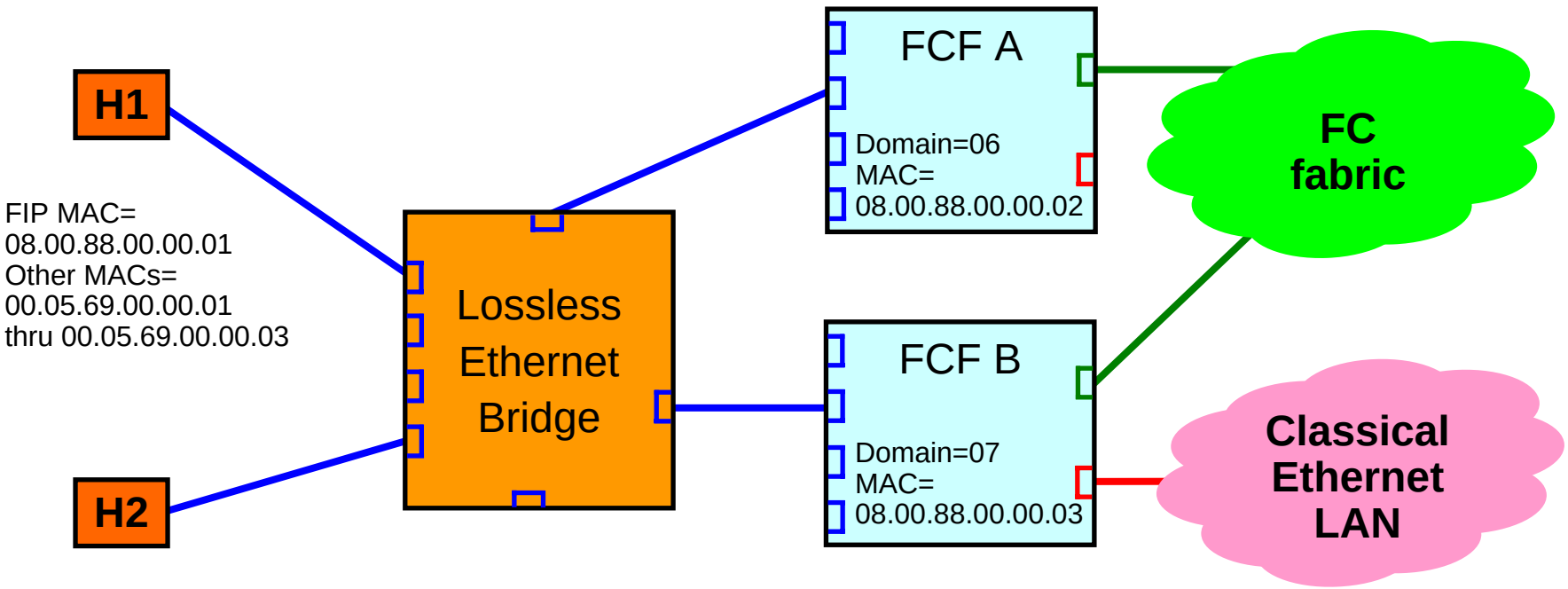
  Easily snooped: just look for Eth=FIP

  Hardware capable of (not very) deep packet inspection may further filter to find just the FLOGI accepts

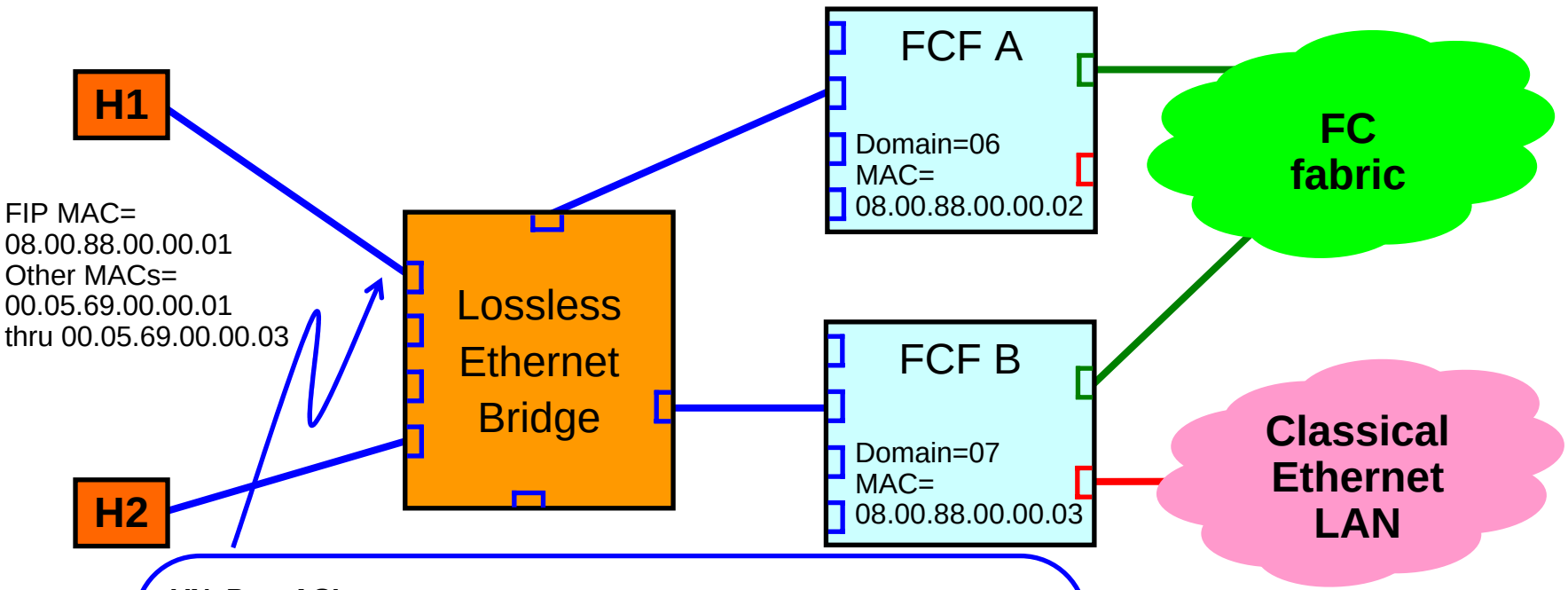
  Note: may not operate on ISLs with TRILL due to asymmetric paths

ACLs in Action:
SPMA and Dynamic ACL Population

Initial Set-up Prior to FLOGI



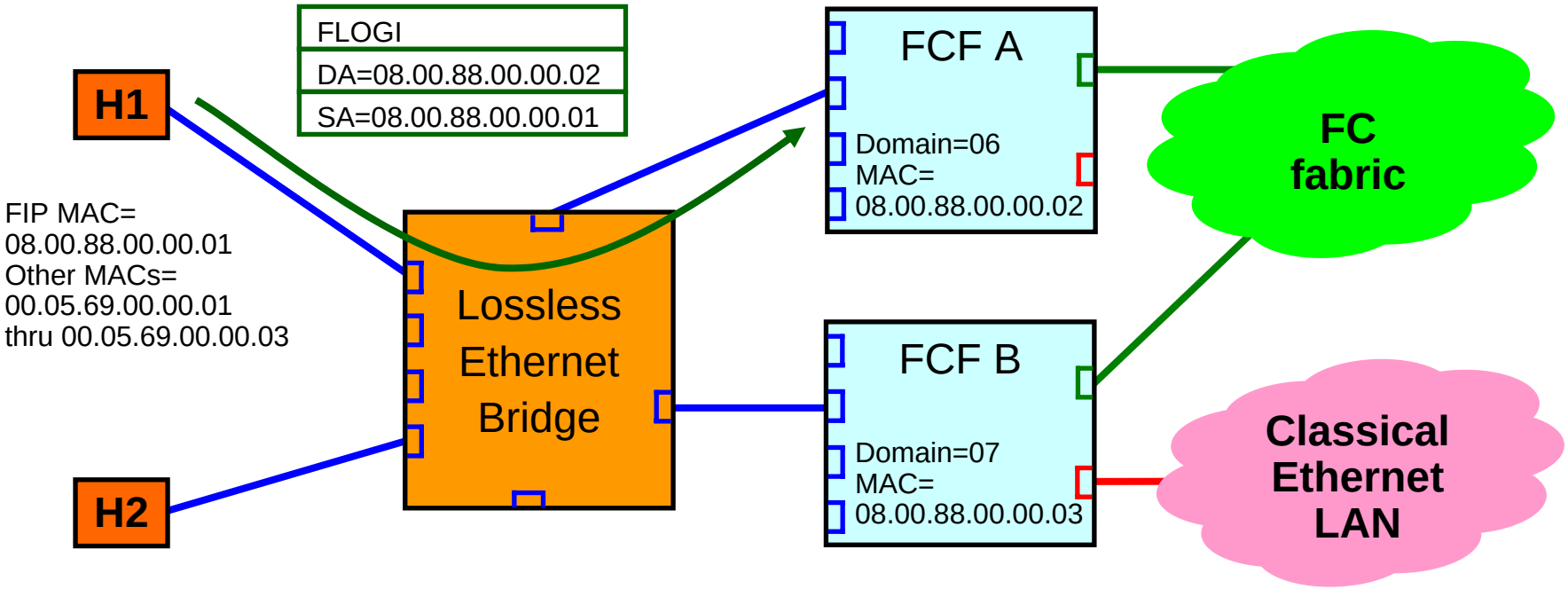
Initial Port ACL Prior to FLOGI



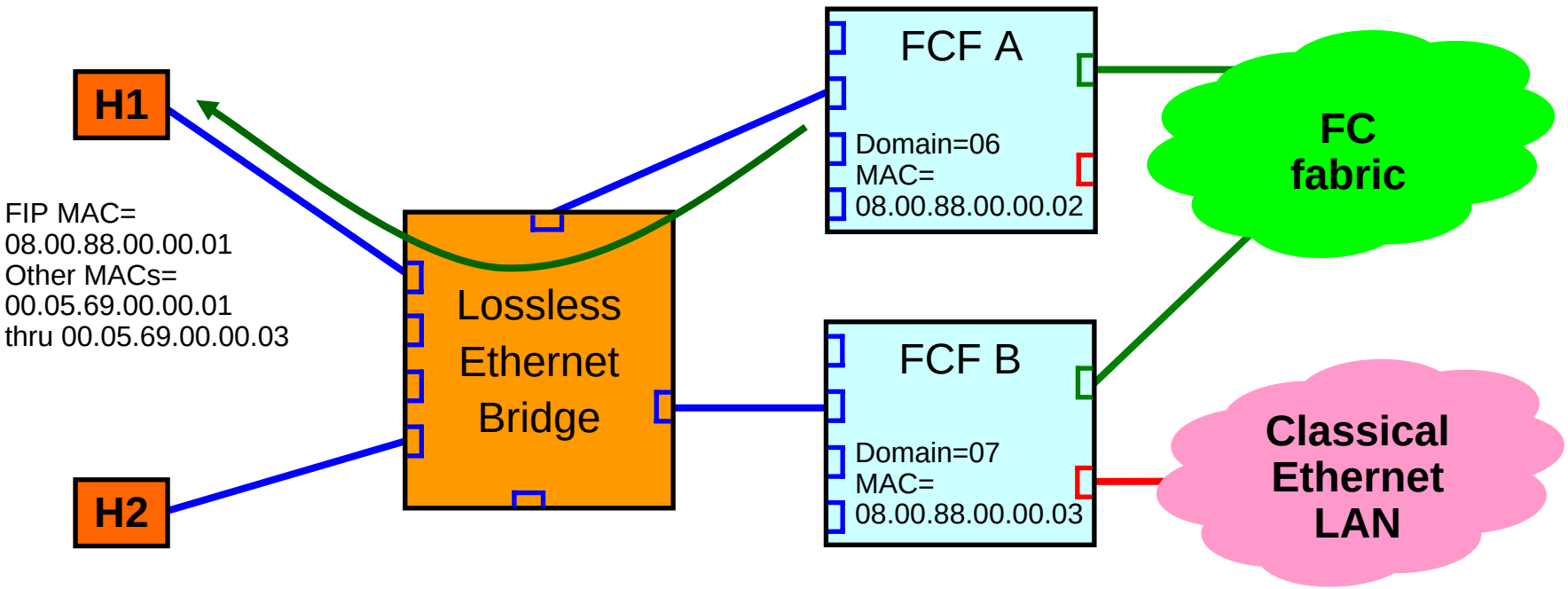
VN_Port ACL:

SA=08.00.88.00.00.01, DA=08.00.88.00.00.02, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=08.00.88.00.00.03, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=All-FCFs, Eth=FIP, permit
Eth=FIP, deny
Eth=FCoE, deny
Pre-existing ACEs
SA=00.05.69.00.00.01, permit
SA=00.05.69.00.00.02, permit
SA=00.05.69.00.00.03, permit
deny

FLOGI Sent

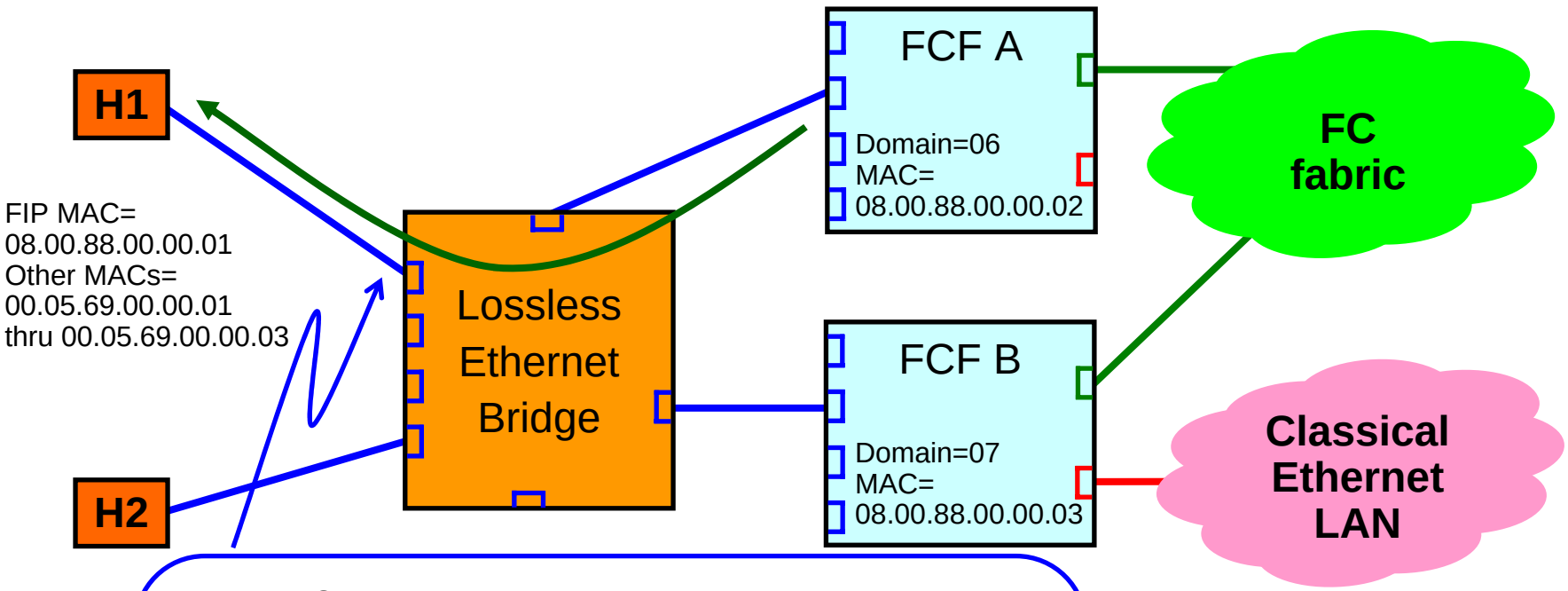

FLOGI
DA=08.00.88.00.00.02
SA=08.00.88.00.00.01
H1
H2
FIP MAC=
08.00.88.00.00.01
Other MACs=
00.05.69.00.00.01
thru 00.05.69.00.00.03
Lossless
Ethernet
Bridge
FCF A
Domain=06
MAC=
08.00.88.00.00.02
FCF B
Domain=07
MAC=
08.00.88.00.00.03
FC
fabric
Classical
Ethernet
LAN

FLOGI Accept



FLOGI Accept
DA=08.00.88.00.00.01
SA=08.00.88.00.00.02
Your MAC= 08.00.88.00.00.02
Your FCID= 06.01.00

ACL Populated



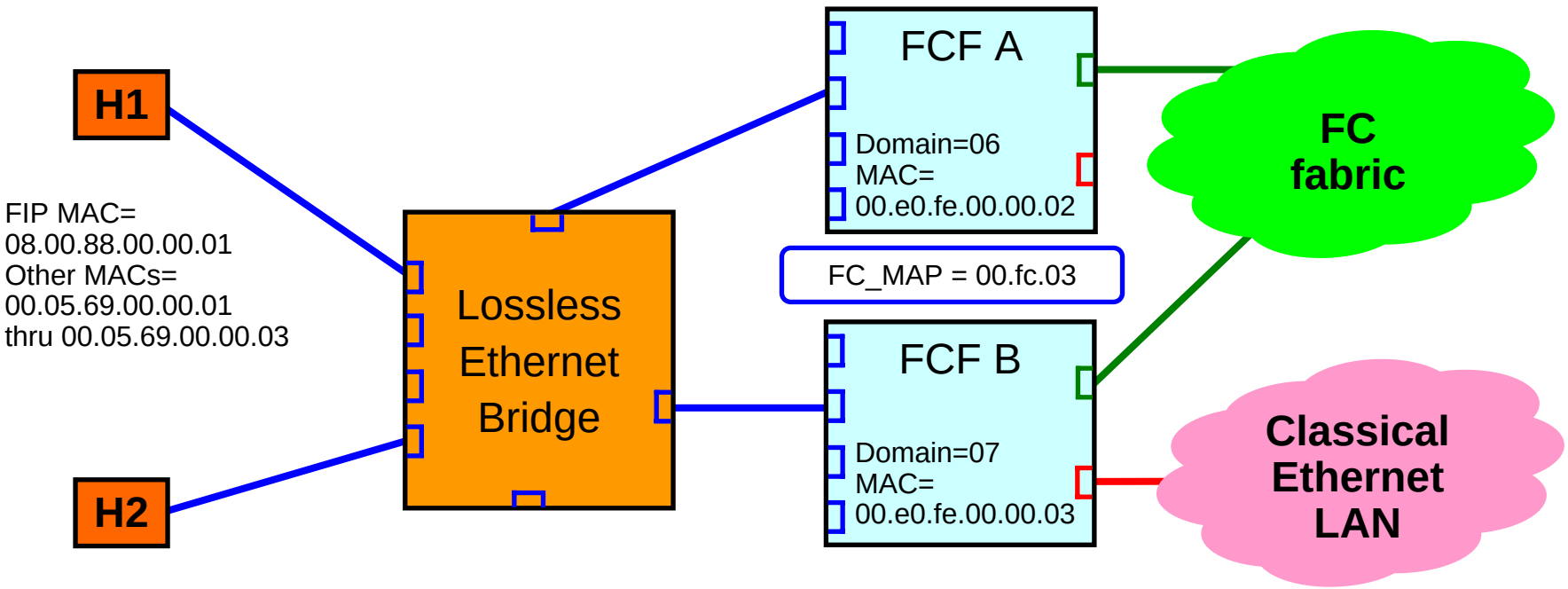
VN_Port ACL:

SA=08.00.88.00.00.01, DA=08.00.88.00.00.02, Eth=FCoE, permit
SA=08.00.88.00.00.01, DA=08.00.88.00.00.02, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=08.00.88.00.00.03, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=All-FCFs, Eth=FIP, permit
Eth=FIP, deny
Eth=FCoE, deny
Pre-existing ACEs
SA=00.05.69.00.00.01, permit
SA=00.05.69.00.00.02, permit
SA=00.05.69.00.00.03, permit
deny

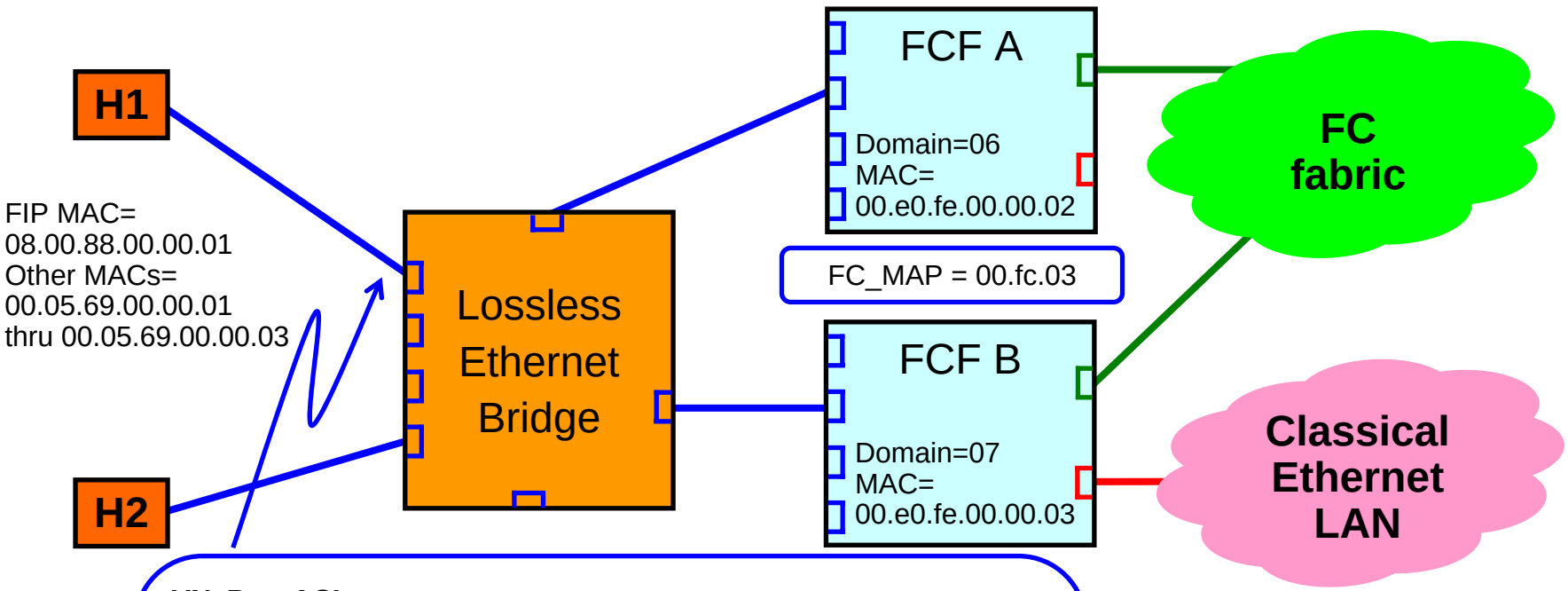
FLOGI Accept
DA=08.00.88.00.00.01
SA=08.00.88.00.00.02
Your MAC= 08.00.88.00.00.02
Your FCID= 06.01.00

ACLs in Action:
FPMA and Static ACL Population

Initial Set-up



Initial Port ACL Prior to FLOGI

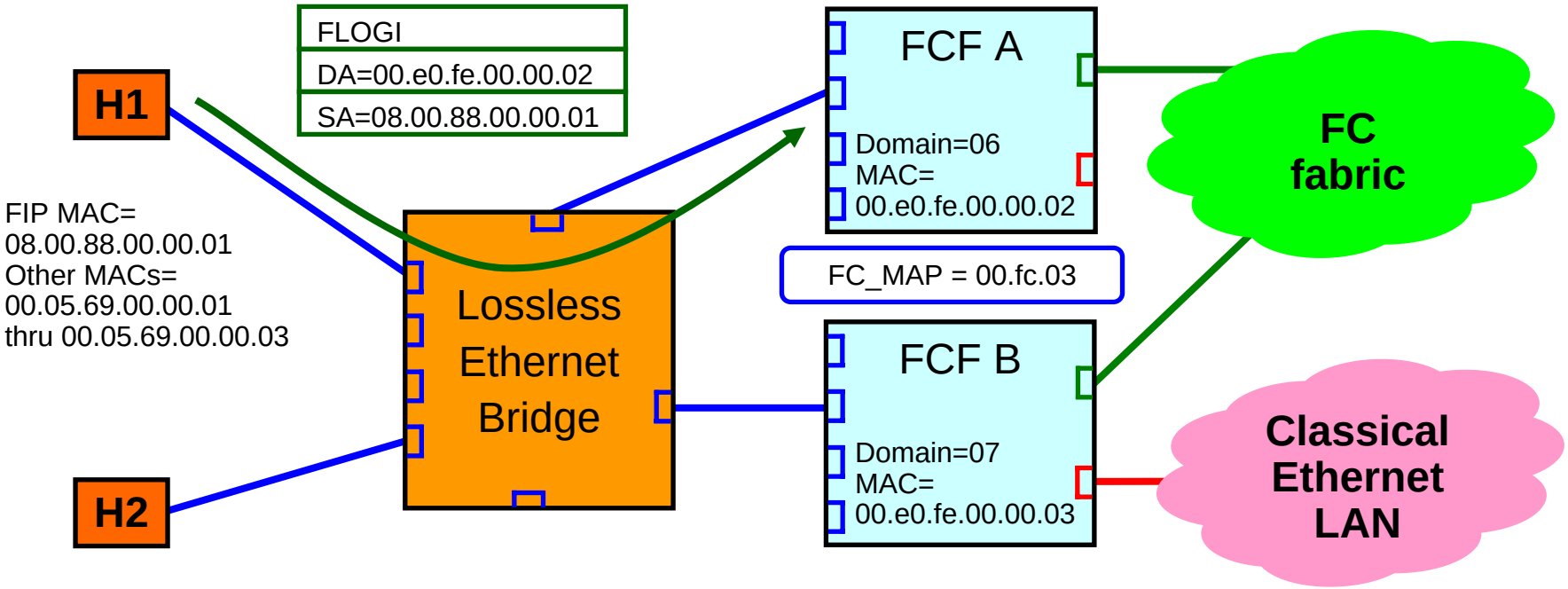


VN_Port ACL:

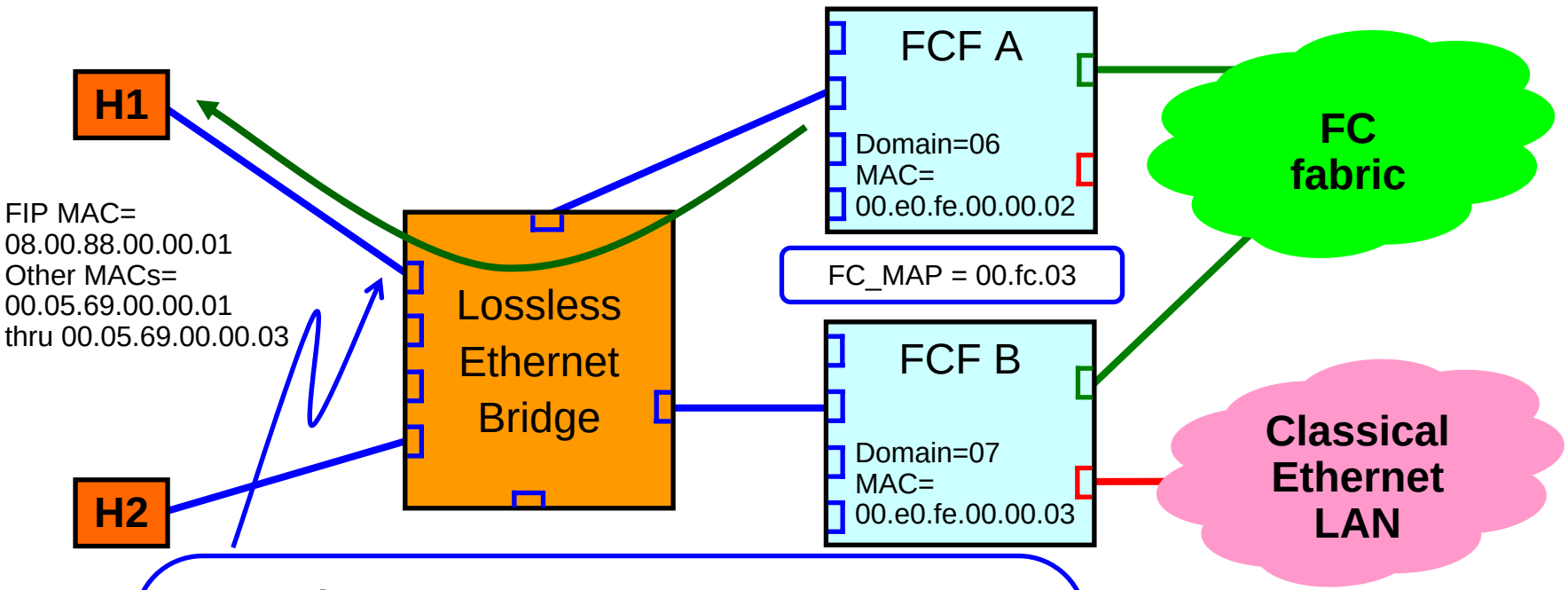
SA=00.fc.0e.06.01.00, DA=00.e0.fe.00.00.02, Eth=FCoE, permit
SA=08.00.88.00.00.01, DA=00.e0.fe.00.00.02, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=00.e0.fe.00.00.03, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=All-FCFs, Eth=FIP permit
Eth=FIP, deny
Eth=FCoE, deny
Pre-existing ACEs
SA=00.05.69.00.00.01, permit
SA=00.05.69.00.00.02, permit
SA=00.05.69.00.00.03, permit
deny

Note: With static ACLs, regardless of the addressing mode being used (SPMA or FPMA), the MAC address to be used for FCoE traffic must be pre-determined. This may be set by the ENode hardware, ENode OS, virtualization middleware, or FCF. In any case, the MAC address may be determined from the appropriate agent assigning it.

FLOGI Sent


FLOGI
DA=00.e0.fe.00.00.02
SA=08.00.88.00.00.01
H1
H2
FIP MAC=
08.00.88.00.00.01
Other MACs=
00.05.69.00.00.01
thru 00.05.69.00.00.03
Lossless
Ethernet
Bridge
FCF A
Domain=06
MAC=
00.e0.fe.00.00.02
FC_MAP = 00.fc.03
FCF B
Domain=07
MAC=
00.e0.fe.00.00.03
FC
fabric
Classical
Ethernet
LAN

FLOGI Accept



VN_Port ACL:

SA=00.fc.0e.06.01.00, DA=00.e0.fe.00.00.02, Eth=FCoE, permit
SA=08.00.88.00.00.01, DA=00.e0.fe.00.00.02, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=00.e0.fe.00.00.03, Eth=FIP, permit
SA=08.00.88.00.00.01, DA=All-FCFs, Eth=FIP permit
Eth=FIP, deny
Eth=FCoE, deny
Pre-existing ACEs
SA=00.05.69.00.00.01, permit
SA=00.05.69.00.00.02, permit
SA=00.05.69.00.00.03, permit
deny

FLOGI Accept
DA=08.00.88.00.00.01
SA=00.e0.fe.00.00.02
Your MAC= 00.fc.oe.06.01.00
Your FCID= 06.01.00

Recommendations

- **FC-BB-5 Include an Informative Annex describing best practices for ACLs including**
  - **A discussion of the need for ACLs and the protection they provide**
  - **A discussion of static and dynamic ACL population**
  - **A discussion of the need for static forwarding table entries**
  - **A recommendation that the VN_Port ACL be deployed at all edges**
  - **A recommendation that this ACL be deployed in addition to checking rules based on T11/08-055v0**
    - Whether these rules are informative, normative, or some combination is beyond the scope of this presentation
    - It is recognized that T11/08-055v0 is a “work in progress” and that the final rules are likely to be a refinement of this document

Thank you