

# FCoE End-to-End Connection

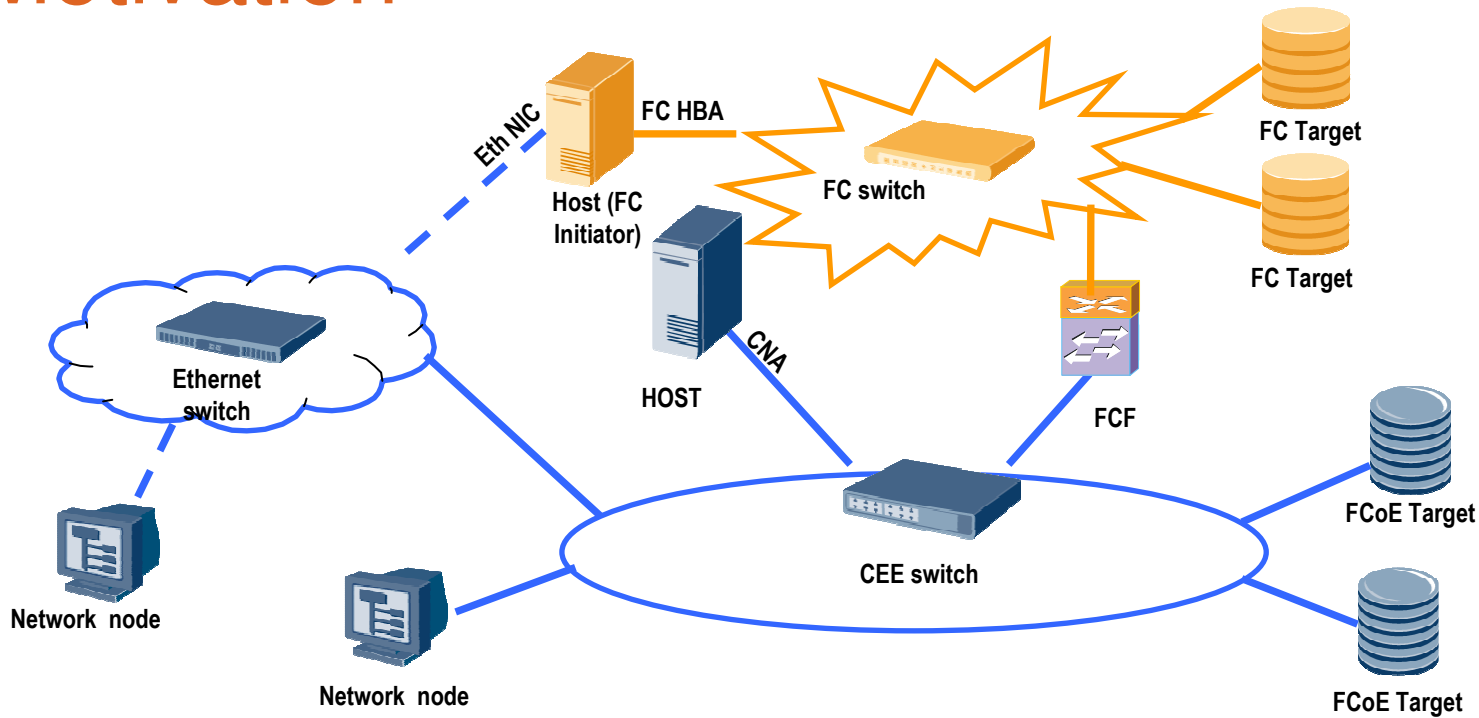
Michael Ko

T11/10-132v0



**Huawei Symantec**

# Motivation



- We want to provide an end-to-end connectivity solution for native FCoE storage targets that is more suitable for a small datacenter
- We want to avoid the bottleneck problems associated with FCFs

# N\_Port ID Assignment

- The basic idea is to support VN\_Port to VN\_Port Virtual Links but use the FCF for N\_Port ID assignment and its name server function
- An ENode (initiator or target) first discovers the FCF and proceeds to FLOGI as per FC-BB-5
- After FLOGI, an ENode (initiator or target) then proceeds to PLOGI to the name server to register its information with the name server
  - An initiator ENode may also query the name server to find out the N\_Port IDs of the target ENodes that it can access
- So far there are no changes required to the existing FC-BB-5 standard

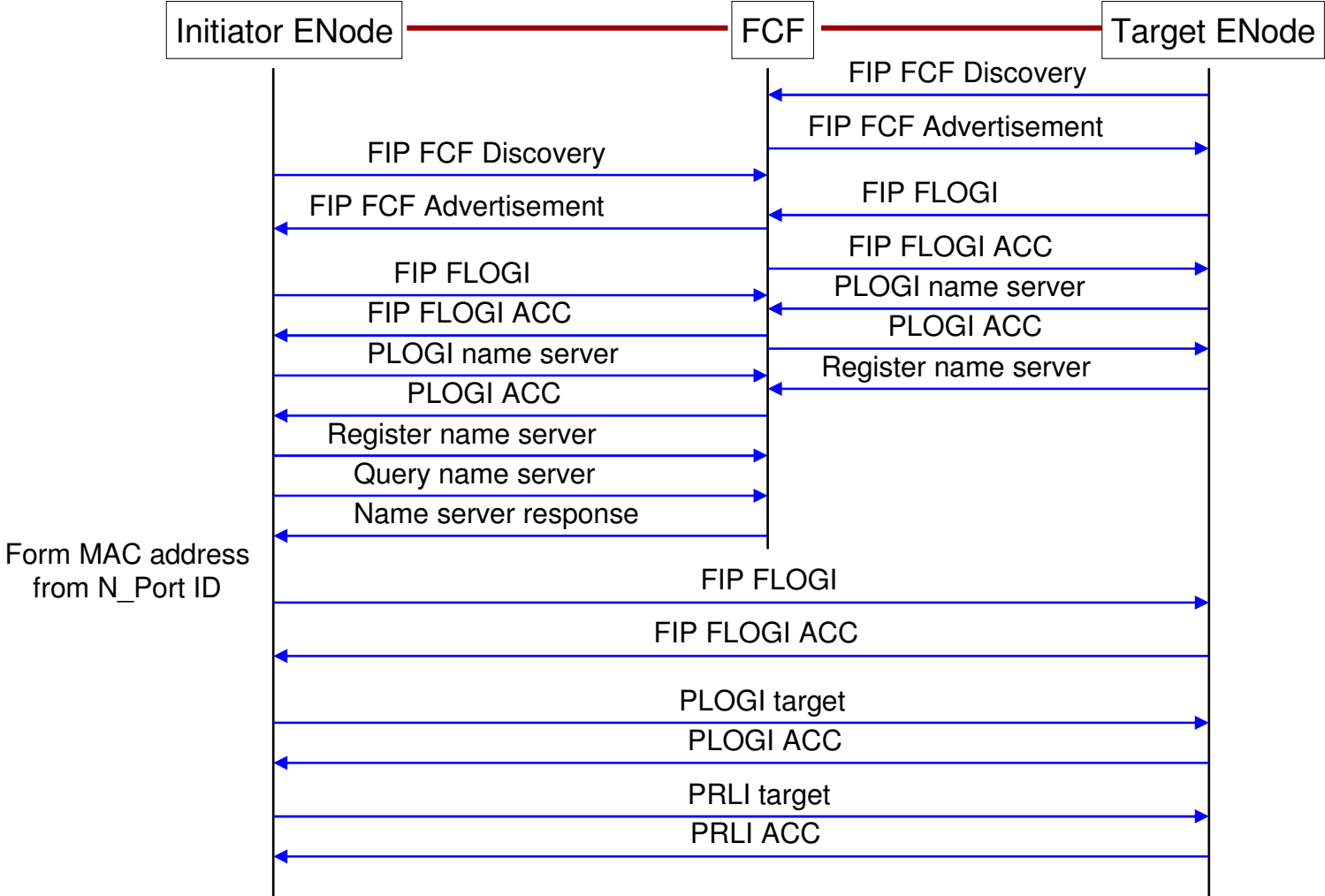


# End-to-End Connection with Target ENode

- If the initiator knows something about the target, such as WWN, it can use the name server to quickly determine the N\_Port ID
- The initiator computes the MAC address of a native FCoE target conforming to this proposal and not connected to an FCF by concatenating the N\_Port ID of the target ENode with the FC-MAP
  - The value of the FC-MAP is determined from its own MAC address assigned by the FCF
- An initiator ENode then issues FLOGI to the target ENode following the model for point-to-point connection using the MAC address computed earlier
- The initiator ENode then follows with PLOGI with the target and other FCoE functions



# Connection Process



# Location of FC/FCoE Target

- But what if the target is an FC target or a native FCoE target connected to an FCF?
- 3 alternatives to determine the MAC address to reach the target
  1. Use the name server
  2. Use Discovery Advertisement
  3. Use timeout



# 1. Use the Name Server

- A native FCoE target is required to store the word “FCoE” in the first 4 bytes of the Symbolic Node Name field in its name server entry
- If the initiator finds this string in the Symbolic Node Name for the target
  - Then the MAC address of the target is equal to FC-MAP concatenated with the N\_Port ID
  - The initiator can then issue FLOGI to the target using the computed MAC address
- Otherwise the initiator issues PLOGI to the target using the MAC address of the FCF



## 2. Use Discovery Advertisement

- All native FCoE target ENodes are required to respond to the ALL\_FCF\_MAC Discovery Solicitation
- Included in the Discovery Advertisement is the VN\_Port MAC address
- The initiator ENode can distinguish the response of a native FCoE target from a real FCF by recognizing FC-MAP in the MAC address
  - For native FCoE targets, the initiator can create a list of N\_Port IDs from the MAC addresses returned in the Discovery Advertisement
  - The initiator can then issue FLOGI to the target using the computed MAC address
- If the N\_Port ID of the target does not appear in this list
  - The initiator then issues PLOGI to the target using the MAC address of the FCF
- Unlike a real FCF, a native FCoE target ENode does not send out periodic Advertisement
- Alternatively, we can create a new FIP operation to broadcast the discovery solicitation to native FCoE targets only



## 3. Use Timeout

- An initiator ENode issues FLOGI to the target ENode using the computed MAC address
- If the target is an FC target or a native FCoE target connected to the FCF, the FLOGI will time out
- The initiator then issues PLOGI to the target using the MAC address of the FCF



# FCF Considerations

- For legacy customers with FC SAN, FCFs will be used in the FCoE network
- For new customers with no FC SAN, the needed control and management plane functions of the FCF can be provided in redundant servers in the network
  - Functions needed include
    - Respond to FCF Discovery
    - Respond to FLOGI/PLOGI
    - Assign N\_Port ID
    - Provide the name server function
  - Conceptually similar to the FC-CMP proposal in T11/09-425



# Security Considerations

- This proposal is similar to T11/10-019 with similar risk factors
  - T11/10-019 advocates using distributed means to guarantee uniqueness of N\_Port IDs
  - This proposal uses a central repository to control and manage the assignment of N\_Port IDs
- The Access Control List described in T11/10-019 is equally applicable to this proposal



# Summary

- No FCF changes are required
  - But only the control and management plane functions of the FCF are needed
- No FIP frame format changes required
  - Unless we decide to defined a new FIP operation to multicast to all native FCoE targets
- No name server changes required
  - Unless we decide to store the word “FCoE” in the first 4 bytes of the Symbolic Node Name
- No multicast storm associated with the determination of the uniqueness of N\_Port ID
  - Less changes required at the CNA to support end-to-end connectivity



**Thanks!**  
[www.huaweisyntec.com](http://www.huaweisyntec.com)



**Huawei Symantec**