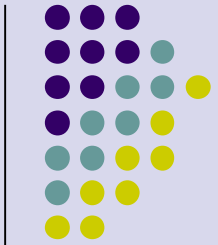


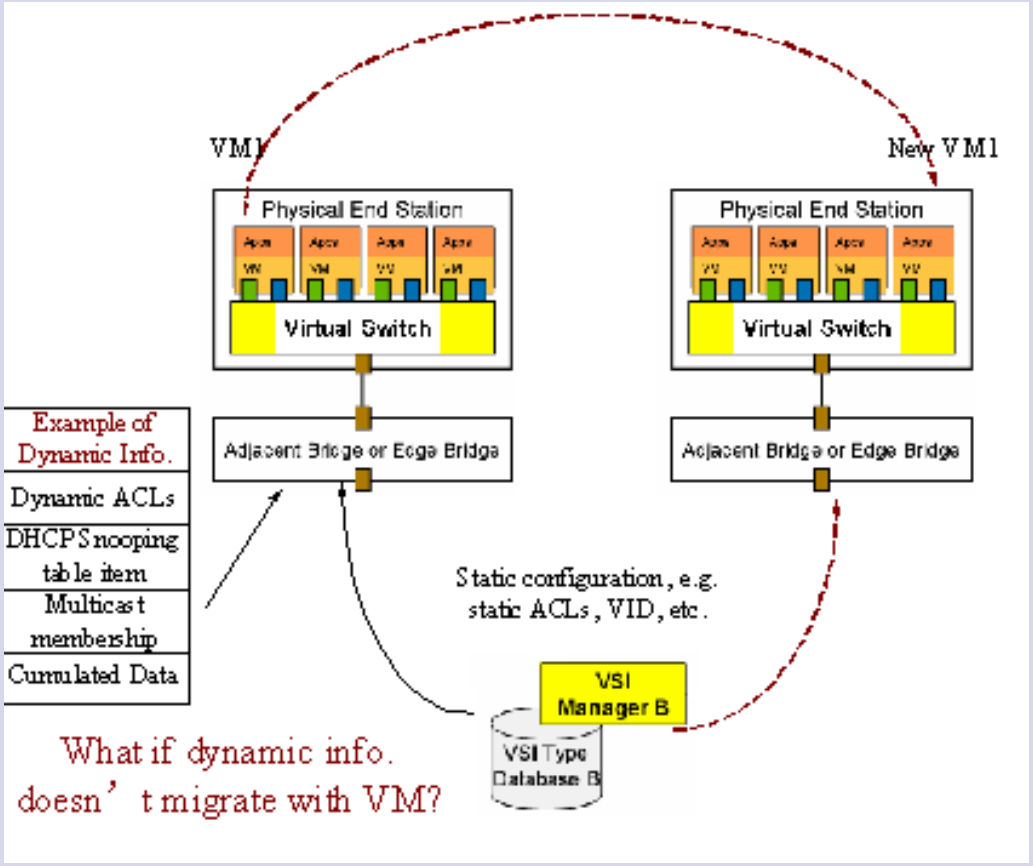
Dynamic information Migration

Gu Yingjie (guyingjie@huawei.com)

Recap of DI (Dynamic Information) migration

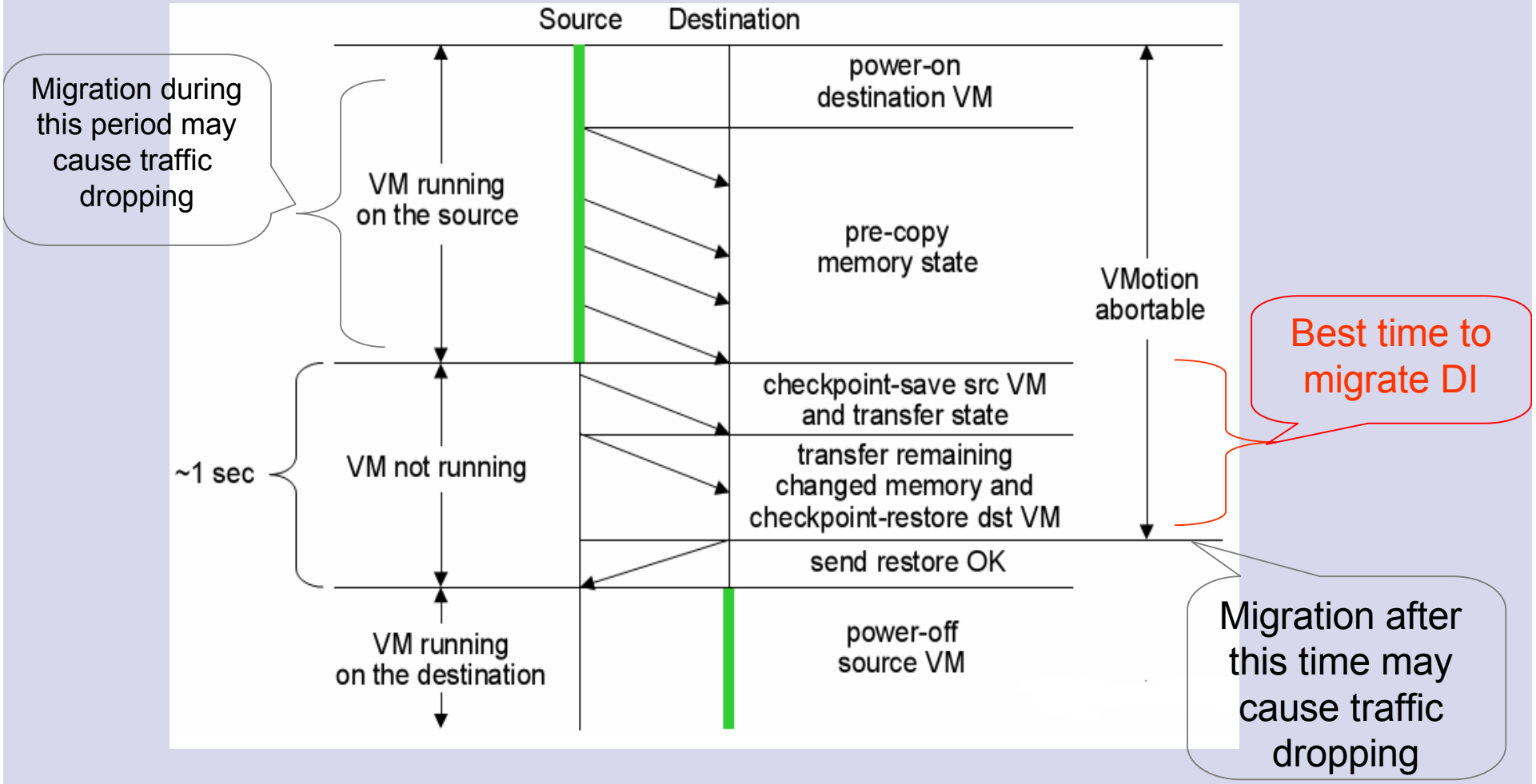
Static policies can be reconfigured on destination bridge any time before the new VM starts.

But DI can be migrated accurately only if old VM stops running and new VM hasn't be started yet. 'Migration is time sensitive'

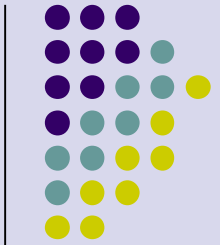


Recap of DI (Dynamic Information) migration

- Good Timing:

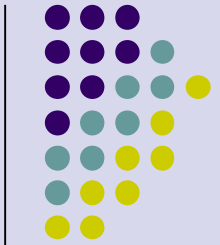


Feedback from Singapore meeting

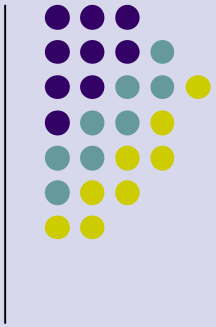


- More use cases
  - List more and detail use cases
- Concrete Proposals

All-around Overview of DI

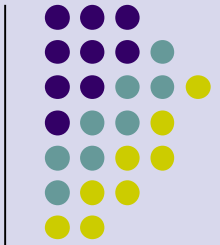


- Enumerate Layer 2 to Layer 7 DI in Data Center
  - On adjacent bridge
  - On middle-box
  - On gateway
- We don't mean to ask IEEE802.1 to resovle Layer 3 and upper DI migration, however:
  - An all-around overview of DI can help to understand the whole problem, and
  - We can figure out the part of the problem that can be resolved by IEEE802.1



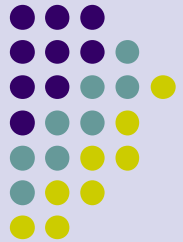
Use Cases

Use cases presented at previous meeting:



- Use Case 1: 802.1X authentication
- Use Case 2: Dynamic ACL
- Use Case 3: DHCP Snooping table
- Use Case 4: IGMP Snooping table

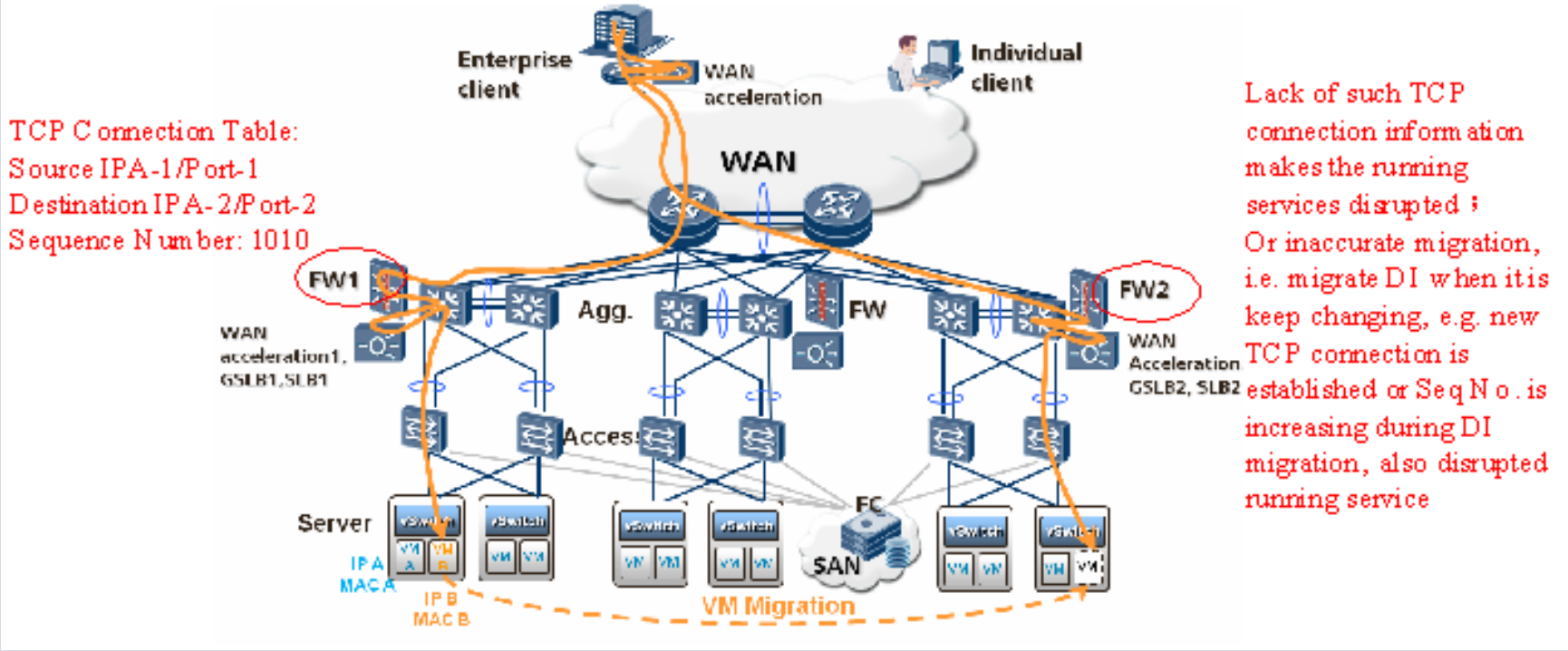
Use Case 5: Packet rate



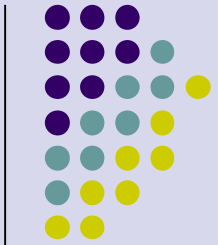
- To ensure VMs consume no more than assigned bandwidth and to enable QoS control, bridges accumulate packet counts and calculate packet rate. Failure to properly migrate cumulative statistics will impact the accuracy of these statistics..
- Some dynamic ACL is generated upon VM's statistic data, lack of which increase security risk. E.g. Firewall creates dynamic ACL to block a certain client who has set up unfinished TCP connections more than threshold.

Use Case 6: Dynamic Information on Firewall

- Take Proxy Firewall as example, it proxies TCP connections between internal servers and external clients, caching TCP connection table.

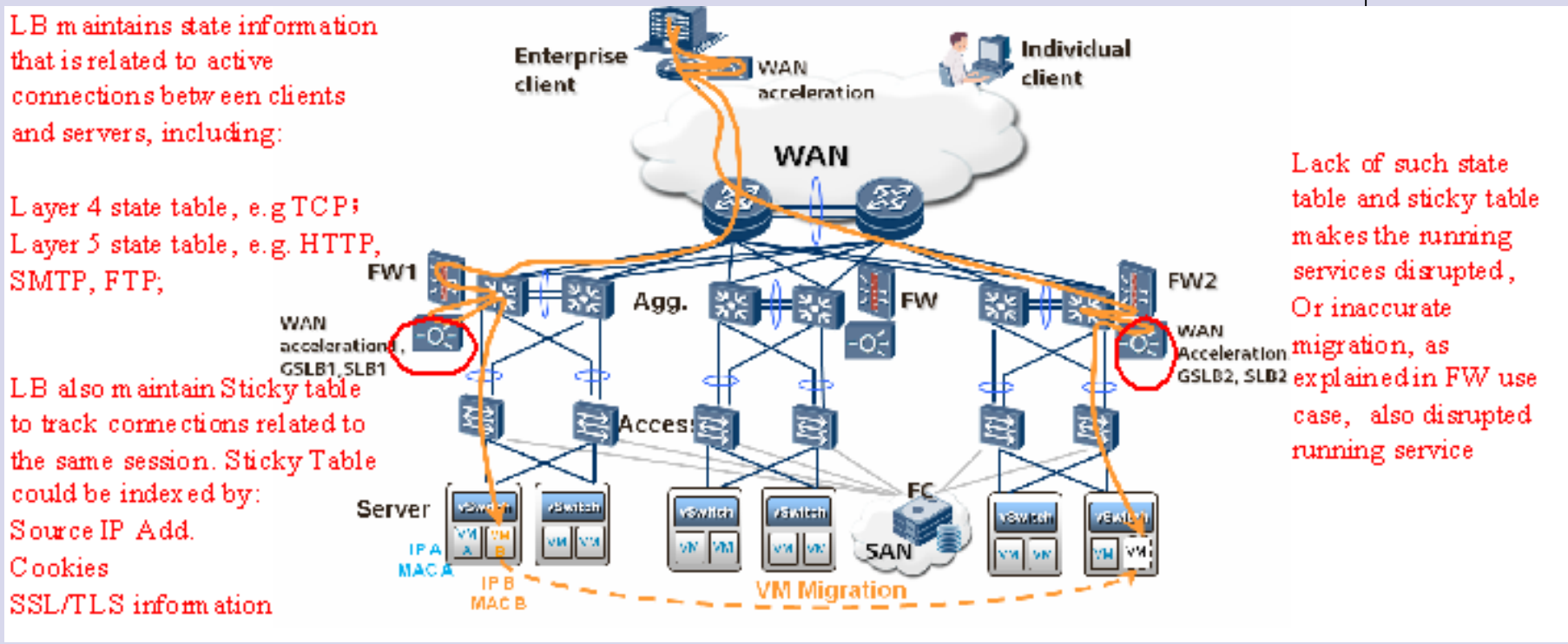


Use Case 6: Dynamic Information on Firewall

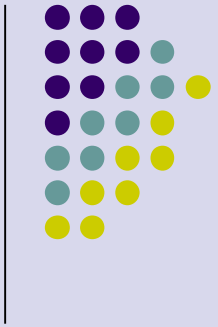


- Proxy Firewall may also support client authentication, audit and logging, which are dynamic information too.
- As for Packet Filter Firewall, dynamic ACL could be generated to protect internal network/servers from attacks, similar to use case 2.
- If NAT function is enabled on Firewall, the address mapping table is another example of dynamic information, lack of which disable NAT on destination FW and disrupt running service.

Use Case 7: Dynamic Information on Load Balancer

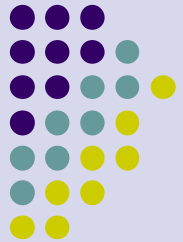


- If NAT function is enabled on LB, the address mapping table is another example of dynamic information, lack of which disable NAT on destination LB and disrupt running service.



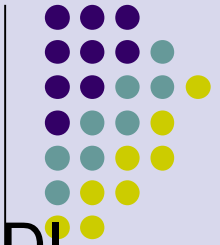
Overview of Remedy

The crucial part of remedy — notification



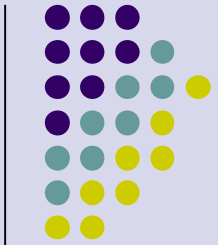
- When and Where to migrate DI?
  - Rely on the notification from Hypervisor, which can be
- IEEE802.1 can define a basic (Layer 2) notification protocol to notify VM status;
  - Layer 2 device can be triggered by the basic notification protocol
  - Extension to the basic trigger can be made by other IEEE WGs or SDOs to distribute the notification to upper layer.

A Feedback Mechanism



- DI migration might fail for many reasons. If essential DI Migration fails, it's necessary to feedback result.
  - E.g. fail to migrate ACL will cause security risk, and fail to migrate TCP conn. table will disrupt running service. If VM is forced to migrate without regard to DI migration failure, managers must be aware of the risk. Otherwise, just rollback and find a better location.
- So we may need feedback mechanism to notify whether DI has been migrated successfully. Manager can make final decision whether to go on with the process.
- IEEE802.1 can define a basic feedback mechanism which can be used by Layer 2 devices and be easily reused by upper layer devices.

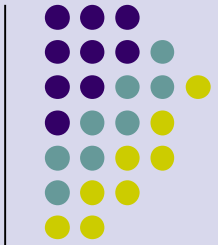
A Transfer Protocol



- Transfer DI from original device to destination device.
  - Should be transferred on control or manage plane
  - Should be a common protocol for both Layer 2 device and upper layer device.

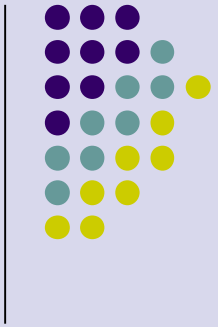
Considerations

- This is an important problem to VM migration;
- This is a problem that can not be exclusively resolved by IEEE802.1, but IEEE802.1 is very crucial to the whole remedy, to know when and where to migrate DI, and to feedback migration result.



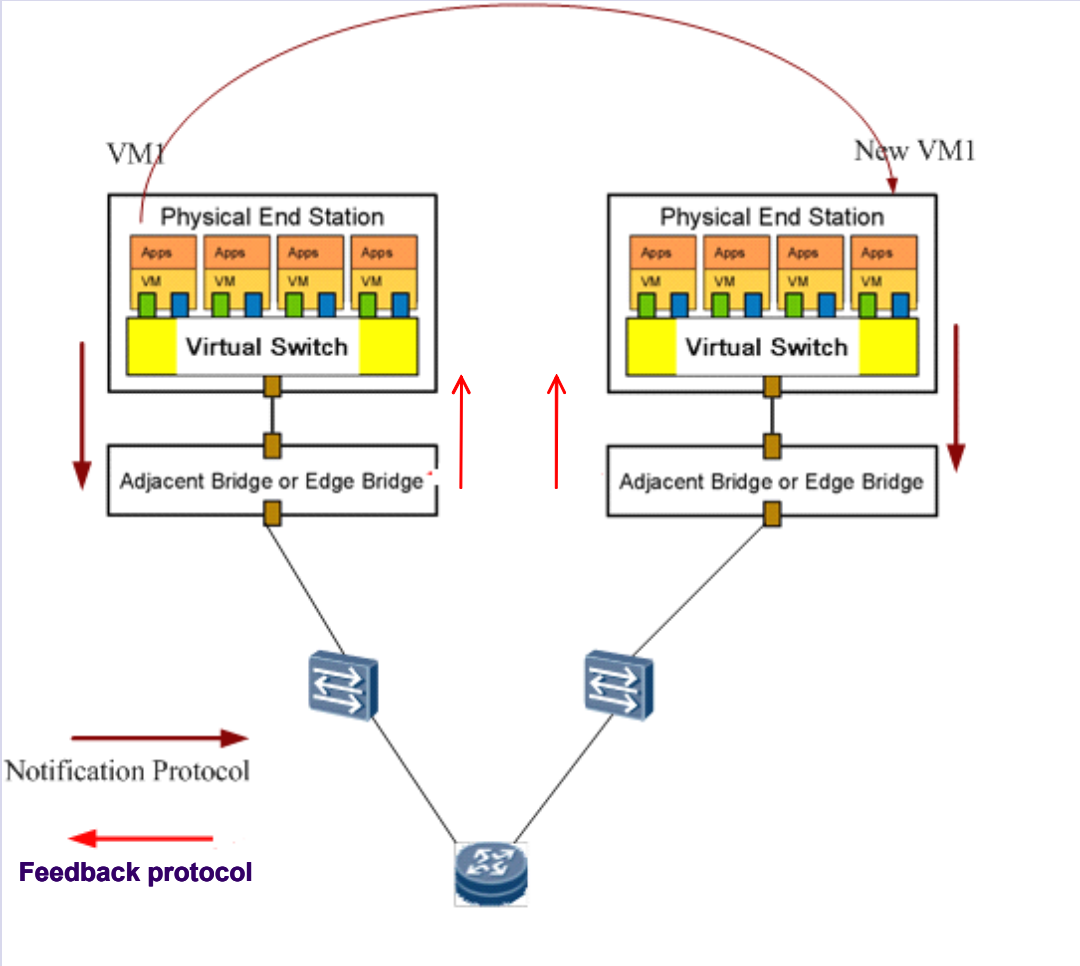
Proposals to IEEE802.1 DCB

Proposals



- Notification Protocol
  - From Hypervisor to Bridge, carry ‘Original bridge’ or ‘Destination bridge’, and VM status, e.g. the key time point for DI migration;
- Feedback mechanism
  - From Bridge to Hypervisor, notifying whether DI migration is successful or not.

Proposal


VM1
New VM1
Physical End Station
Apps
VM
Virtual Switch
Adjacent Bridge or Edge Bridge
Physical End Station
Apps
VM
Virtual Switch
Adjacent Bridge or Edge Bridge
Notification Protocol
Feedback protocol