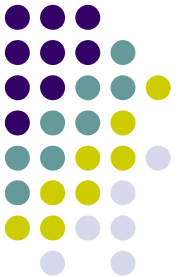
Migrate Dynamic information on Bridge While VMs migrate

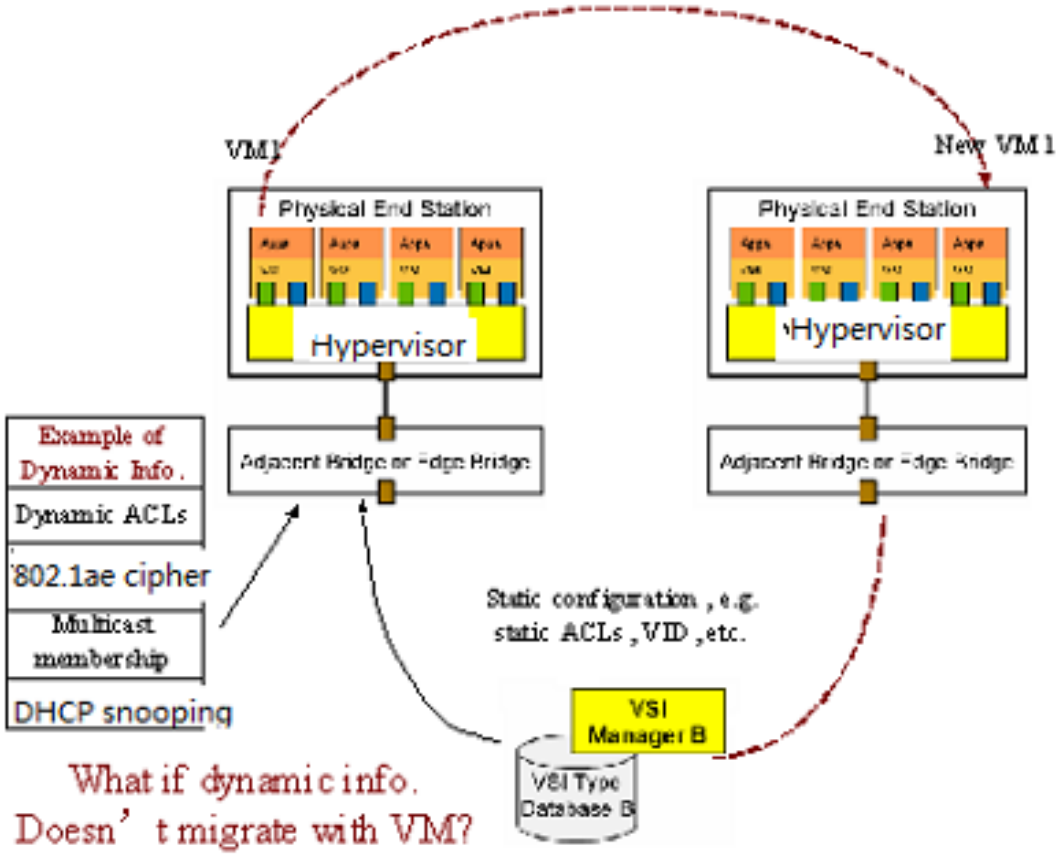
Gu Yingjie (guyingjie@huawei.com)

Generation of Dynamic Info.(DI) on edge bridge



- In addition to static configuration configured by network manager, some info. may also be dynamically generated on edge bridge during forwarding service:
  - Dynamic ACLs:802.1x Authentication;
  - 802.1AE Cipher suite: VM and bridge negotiate Cipher Suite; VM encrypts frames with Cipher, calculate ICV with Cipher; Bridge decrypts packets with Cipher.
  - Multicast Membership: a port Join or Leave a multicast group by listening IGMP membership report.
  - DHCP snooping table item: establish IP/MAC mapping by listening DHCP Response
  - may find more examples of DI

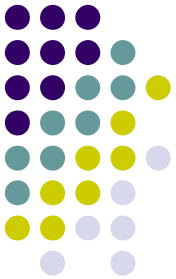
What if DI doesn't migrate?



Consequence if DI doesn't migrate

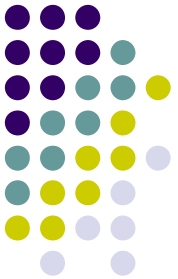
- No Dynamic ACLs: Bridge regards VM as non-authorized client and drop VM's packets; VM could login again, but the service is distrupted.
- No 802.1AE cipher: packet will be dropped, becasue bridge can not decrypt packet.
- No Multicast Membership: Bridge doesn't multicast packets to the port VM is attached until it receives IGMP membership report on that port.
- No DHCP snooping table item: Bridge cannot find IP/MAC pair then drop VM's packets;

A general mechanism for all possible dynamic info. instead of specific solution for each



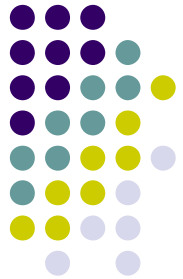
- Except for the four items mentioned in previous slide, we may also need to migrate other information:
  - On behalf of security
  - On behalf of service continuity.
  - On behalf of monitoring
  - Etc.

Benefits of a general solution to bulk DI migration by bridge instead of by Hypervisor



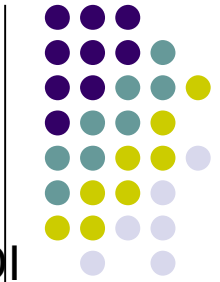
- Save Hypervisor from deploying every single solution for each type of DI;
- Reduce the work to keep updating Hypervisor to adapt to evolving DI, e.g.:
  - DI introduced by new mechanism in the future
  - update Hypervisor in consistence with updating protocol
- Doesn't conflict with 'Powerful Hypervisor' who would like to deploy all possible DI-relevant protocols. Beneficial to vendors who wouldn't carry so many duties on their Hypervisor.

Some considerations to DI migration

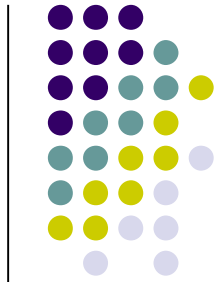


- Key points:
  - To define a mechanism to migrate DI as a bulk, e.g. to learn when to migrate DI, and a mechanism to transfer DI
  - To define a mechanism to notify the result of migration from bridge to Server

Some considerations to DI migration

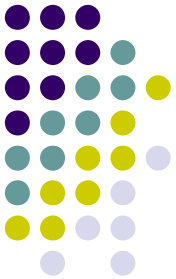


- Why not rely on 'Association response'?
  - Association can happen at any time, Bridge needs not to migrate DI every time.
  - When a VM is ready on destination server, there is no guarantee an Association message must be sent from server to bridge. Hence one can not rely on Association response to know the status of DI migration.
- DI migration response, from Bridge to Server:
  - A 'SUCCESS' response means the Bridge has successfully transfered DI, the new VM can begin running service and the old VM can be shut down.
  - A 'FAIL' response may be caused by several reasons:
    - Limited Bridge resource to deal with DI, 'stop trying to move VM here'
    - Unsuccessful transferring, 'maybe you can try again,or continue moving but be aware of the risk'
    - Invalid DI, 'Bridge doesn't support some DI, stop moving or continue with risky'
    - DI conflict with current policy on the Bridge, 'stop moving'
- We need new mechanism for DI transfer and response;



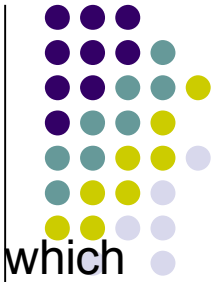
- Proposals
  - Start a new PAR
    - to design a general mechanism to migrate DI while VM migrates.
    - to define a mechanism to notify server the Result of DI migration

Backup slides



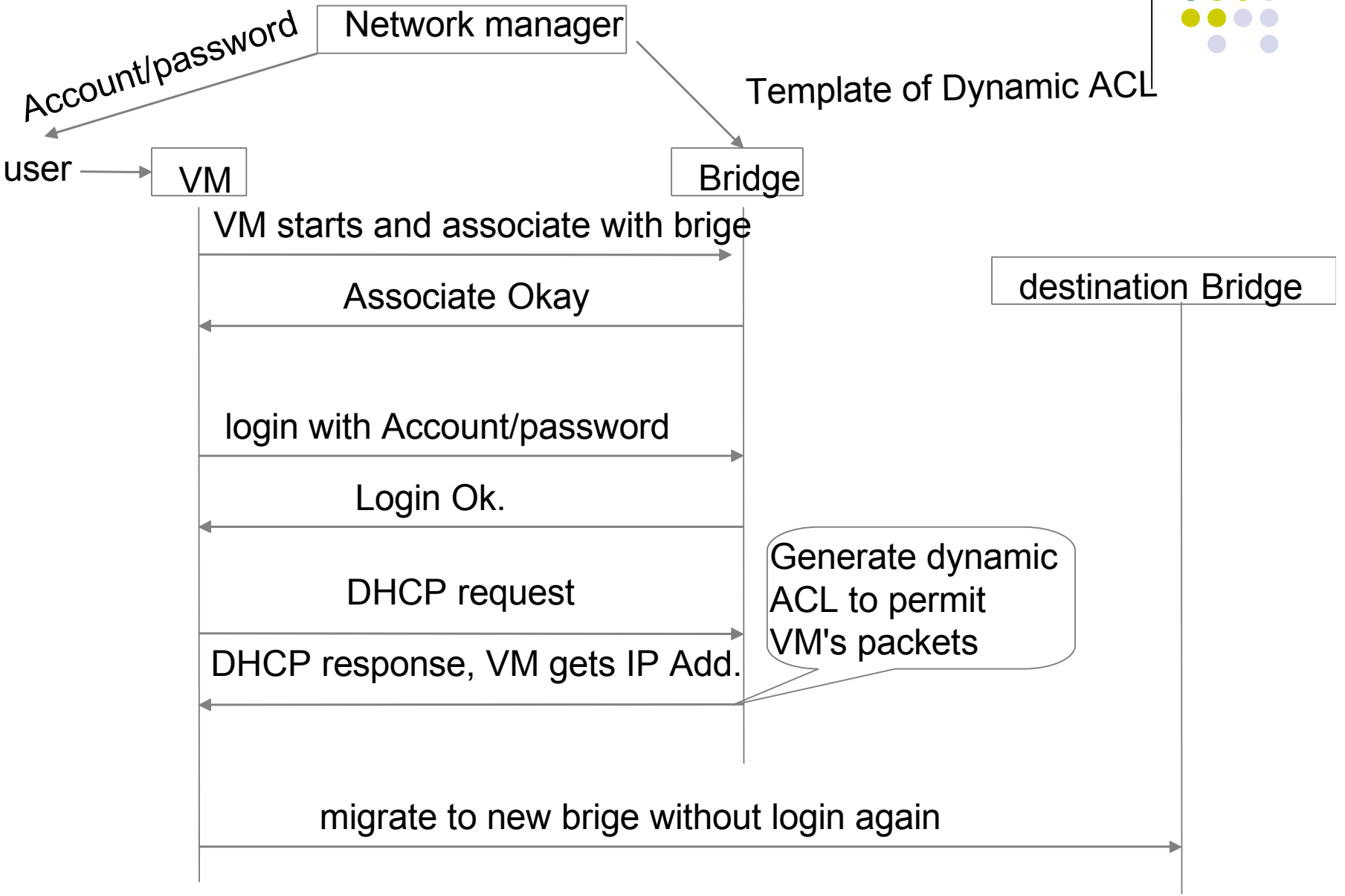
- Table content
  - Dynamic ACL
  - 802.1AE Cipher

Dynamic ACL

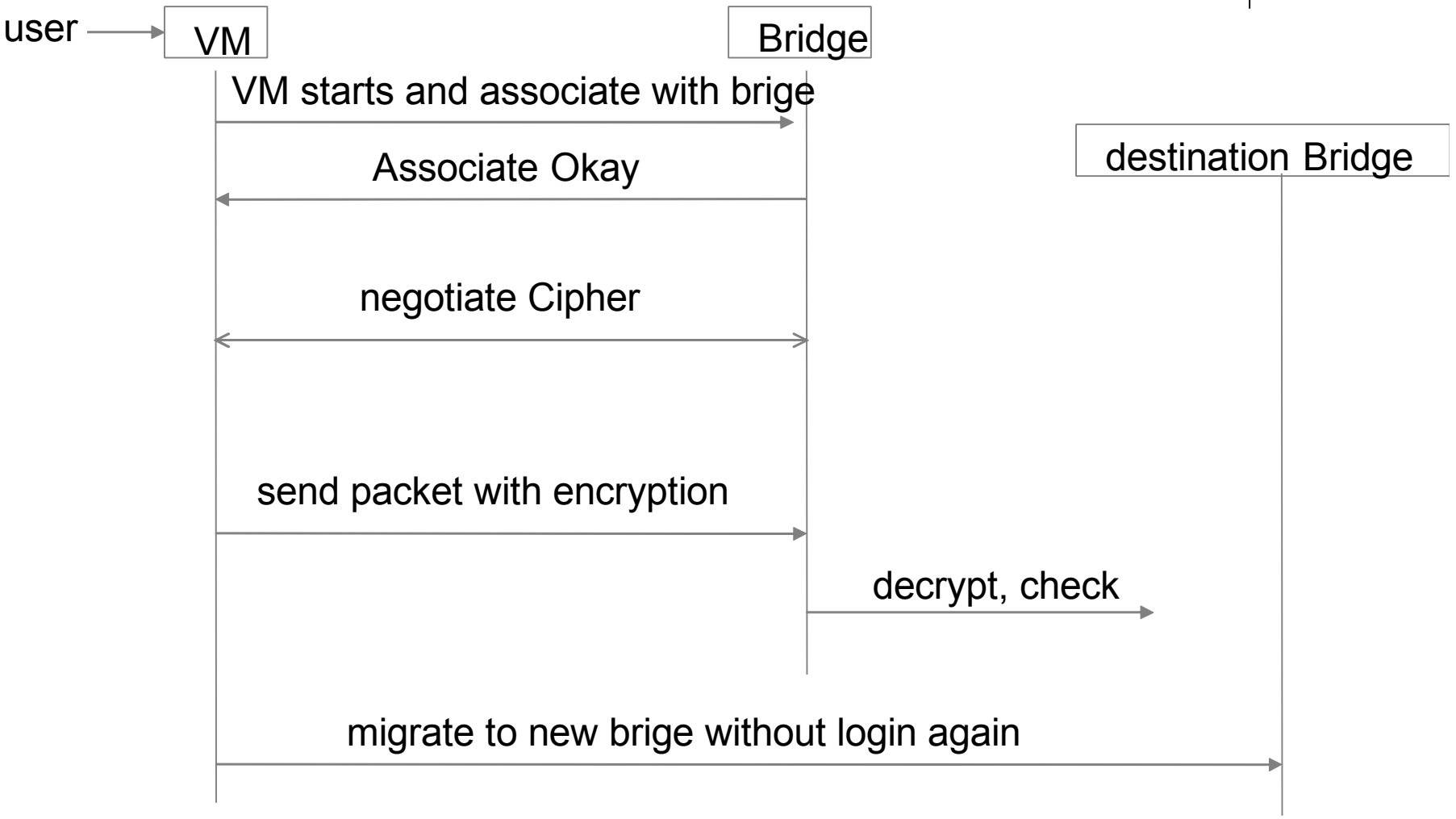


- What is dynamic ACL?
- Static ACL is configured on bridge by network manager, e.g. to define which IP/Port can access to the internet, which can not. An ACL need to specify the IP Address in an ACL. An example is :
  - ACL100 IPAdd-of-VM1 permit;
  - ACL101 All-other-IPAdd deny;
- However, Network Manager can not always know the IP address of a client in advance. For example, the VM use DHCP to apply for an IPAdd. In this case, Network manager just provide a template to bridge and provide a pair of account/password to user of VM. So that VM can start at anywhere with any possible IPAdd. When VM wants to access to internet, Bridge asks VM to provide its account/password, and authenticate the VM by executing 802.1x. If the account/password is correct, which means the vm is authorized, the bridge just fill in the IP Add. in the template, then a dynamic ACL is created to permit the packets from the VM.
- Dynamic ACL is generated after the VM is associated with the Bridge at the very begining, so it's not in the VSI Profile. When we migrate VM, we hope the running service on the VM is least interrupted, so we need to set the dynamic ACL to the destination bridge to guarantee the packets of running service can successfully be forwarded after migration.

Example flow of Dynamic ACL



Example flow of 802.1AE



802.1AE Cipher

- What is 802.1ae cipher? In order to improve network security, 802.1ae enables the end host and the adjacent bridge to negotiate a cipher. The end host send packet encrypted by the cipher and bridge decrypte the packet using the cipher. The negotiation of Cipher could happen after the VM is associated, meaning that the cipher may not going to be included in VSI profile.
- When VM migrate, it still encrypt its packet with cipher, but the destination bridge has no idea of the cipher, so the vm's packets will be dropped.