Welcome to the World of Standards

ETSI

World Class Standards

Software Upgrade Process:
Minimizing Service Disruptions and Maintaining Service Availability and Continuity

Stefan Arntzen, ETSI NFV REL Acting Chair, Huawei

SDN OpenFlow WORLD CONGRESS

Software upgrade in ETSI NFV

- ETSI GS NFV-REL003:
  Models and Features for E2E Reliability
  - Study and develop a reliability estimation model for NFV environment
  - Aspects to be considered are as follows:
    - Software reliability
    - Protection schemes and involvement of NFV-MANO (including fault management, failure detection, etc)
    - Dynamic aspects of operation: impact of load, life-cycle operations, such as **software upgrade**, scaling etc. (Clause 8)
  - Recommendations or guidelines will be provided to realize services of different resiliency levels.
  - Published Spring 2016

Upgrade vs. Update

- Definition of update/upgrade
  - Found in NFV Software Architecture document (ETSI GS NFV-SWA 001)
  - A VNF update does not introduce new functionality and/or new interfaces.
 - A VNF upgrade might introduce new functionality and/or new interfaces

- Upgrade/Update VNFs
  - VNF internal IF changes are not visible to MANO
  - If an VNF upgrade is initiated, MANO has to assume that IFs are changed

➔ ETSI GS NFV-REL003 deals with general software upgrade case

Software Upgrade in the Traditional Way

- **Split System into halves**
  - All traffic will be migrated to and handled by the left half

- **Upgrade right half**
  - Install new software version
  - Convert user related state data from old version to new version

- **Switchover traffic from old to new version**

- **Upgrade left half**
  - Install new software version

- **Join the two halves**

Software Upgrade in the Traditional Way

Software Upgrade in the Traditional Way
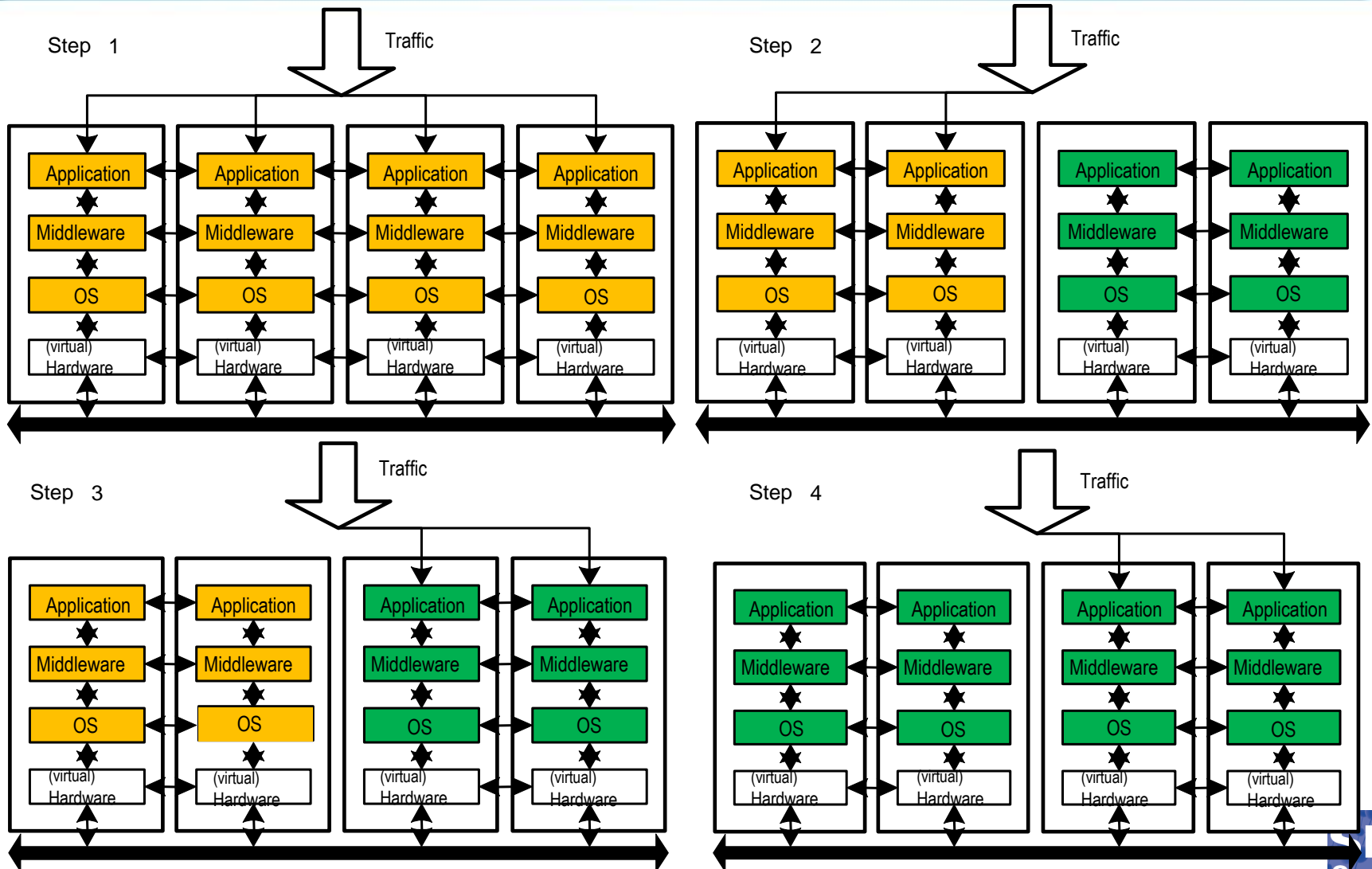
- Disadvantages

- Data conversion in step 2 may be difficult and can take long

- In case of 2N redundancy the standby half is upgraded first
  - Reduced redundancy during upgrade process
  - No failover possibility while switching over

- In case of all nodes active
  - Reducing the capacity of the system by 50%
  - Upgrade can only take place during off-peak periods
    - To reduce load
    - To limit data conversion time

VNF software upgrade in a NFV environment

- Principles to be followed by VNF upgrade in an NFV environment
  - Software upgrade can be done at any time during the day.
    - The full capacity should be served and the system high availability should not be compromised during the upgrade.

  - The verification of the new software version and the new configuration should be carried out with real traffic

  - Software upgrade should be done in a scalable way, e.g. upgrade a fraction of the whole capacity, a certain service type or a certain user group, with the constraint of preserving the service availability and service continuity.
    - The rollback process can allow for a fast recovery without causing outage in the event of failure in the new software version and/or new configuration.
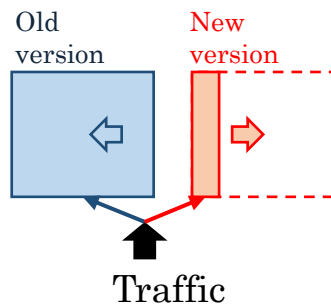
One or more instances of the old software version implementing the network function are providing services, while one or more instances of the new software version (VNF) with limited capacity are instantiated for preparing to support the new version of the service.

1

Old version

New version
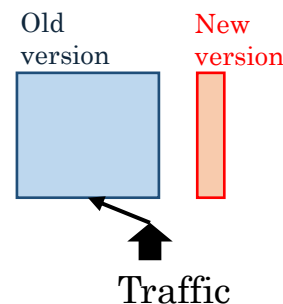
Traffic

Some new service requests are routed to the new software version, while the existing service is still being supported by the old software version. Thus, the new version of software or new configuration could be verified with real traffic. User and traffic affinity should be taken into account when transferring the new service requests to the new software version.

Service Upgrade (Step 3)

The serving capacity of the new software version is increased, e.g. by routing more service requests to the new software. Adding additional capacity or more instances in that part of the new software version with scaling up/out procedure might be needed. As the serving capacity of the old software version is decreased because of less new service requests and some users getting into idle, scaling in/down is executed to remove instances or decreasing capacity in the old software part. The serving capacity of the old software version could be successively decreased, while the serving capacity of the new software could be successively increased.


Old version   New version
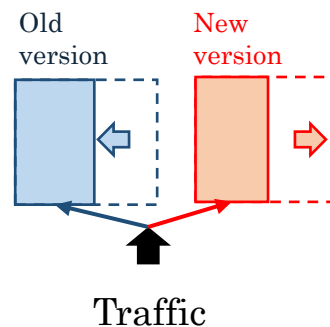
Traffic

When there is no, or very little, traffic left in the old software version instance(s), the service is fully switched into the new version of software system.

4

Old
version

New
version

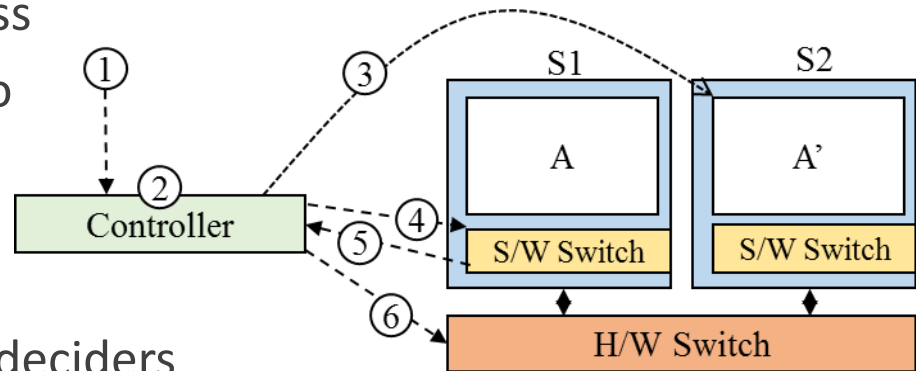Traffic

Traffic Migration during Software Upgrade
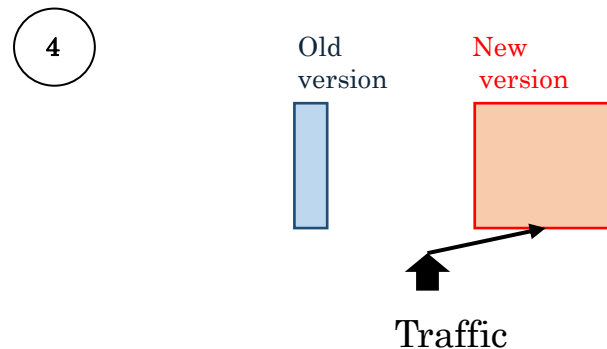
- Depending on the type of service, transactions may be long-lived. Migration can be done by
  - Termination of flows (if flows can be restarted)
  - Migration of flow (if flows cannot be restarted)
    - Expensive
  - State data may have to be shared by old and new version
    - Store in external database
    - Migrate data
- Gradual migration
  - The gradual migration of new service may be done by a selection criteria (service type, user group, ..)
 - A traffic decider can execute rules
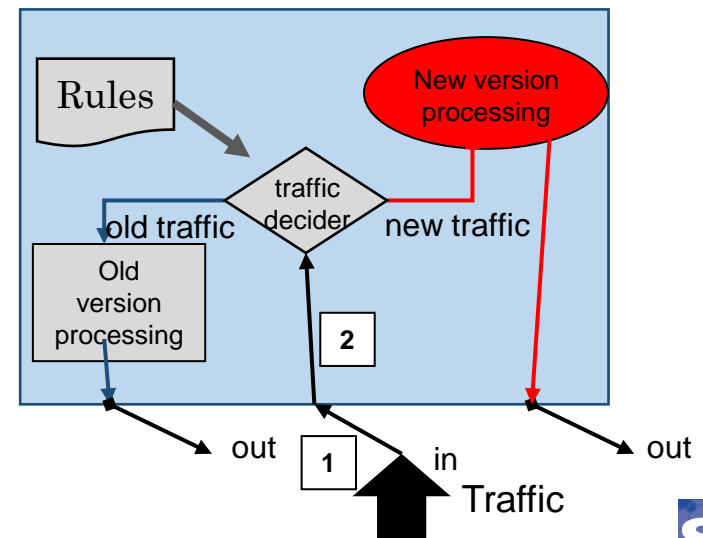
Example: Migration avoidance

- A technique called ‚Migration Avoidance', developed in ETSI GS NFV-REL 002, can be used to demonstrate how to do a gradual migration of traffic for software upgrade

  - An external controller is used to manage the entire process
  - A hash function is applied to relevant header fields to identify flows
  - Hardware- and Software-switches are used as traffic deciders

- For detailed explanation see ETSI GS NFV-REL 002 clause 6.2

NFVI software upgrade

- VM Live Migration is used to offload the traffic from hardware that is affected by
  - Software upgrade of firmware and/or device drivers of NFVI hardware (including the whole physical hardware)
  - Upgrade of guest OS
  - Upgrade of virtualisation layer

Outlook: REL006 Software Upgrade
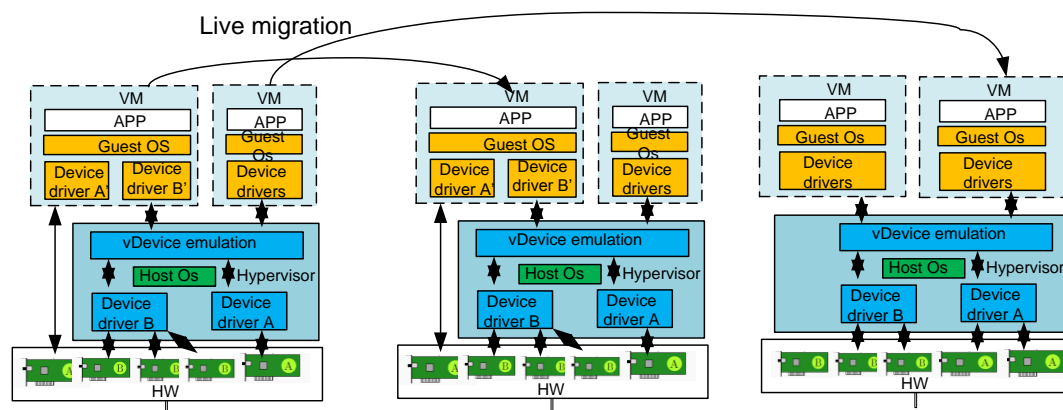
- Objective and Scope
  - Specify requirements for the purpose of Software Update/Upgrade, such that service availability and continuity is maintained.
  - All types of software related to NFV (e.g., VNFs, MANO and NFVI) as well as required controlling and supporting functionality will be addressed.
  - Identification of requirements to enhance the architectural framework.
- Close collaboration with TST006
  - Report on NFV CICD and DevOps
- Adjust with Interfaces and Architecture WG (IFA)
  - VNF package management (IFA007)
  - SW image management (IFA005)
  - Other IFA documents as applicable (IFA011, ..)

More information:

NFV Technology Page (information)
http://www.etsi.org/nfv

NFV Portal (working area)
http://portal.etsi.org/nfv

NFV Proofs of Concept (information)
http://www.etsi.org/nfv-poc

NFV Plugtest (information & registration)
http://www.etsi.org/nfvplugtest

Open Area:

Drafts http://docbox.etsi.org/ISG/NFV/Open/Drafts/

Issue tracker http://nfvwiki.etsi.org/index.php?title=NFV_Issue_Tracker