Requirements for 802.1Qay protection switching

March 2008

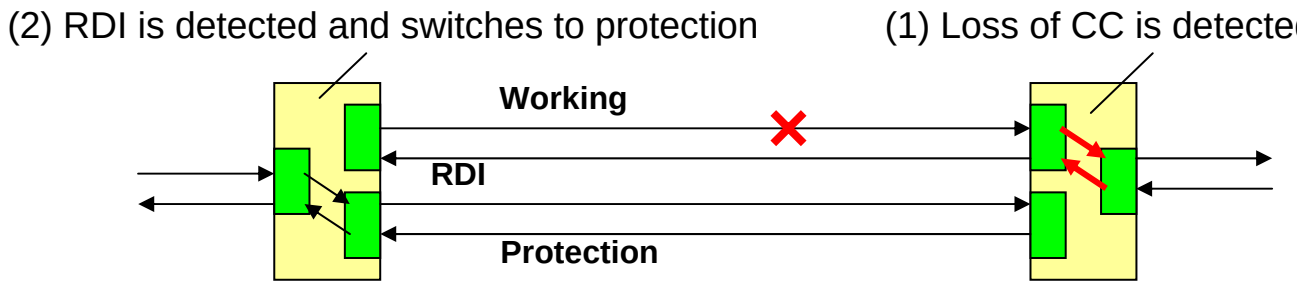
Hiroshi Ohta, NTT

Requirements to PBB-TE protection switching

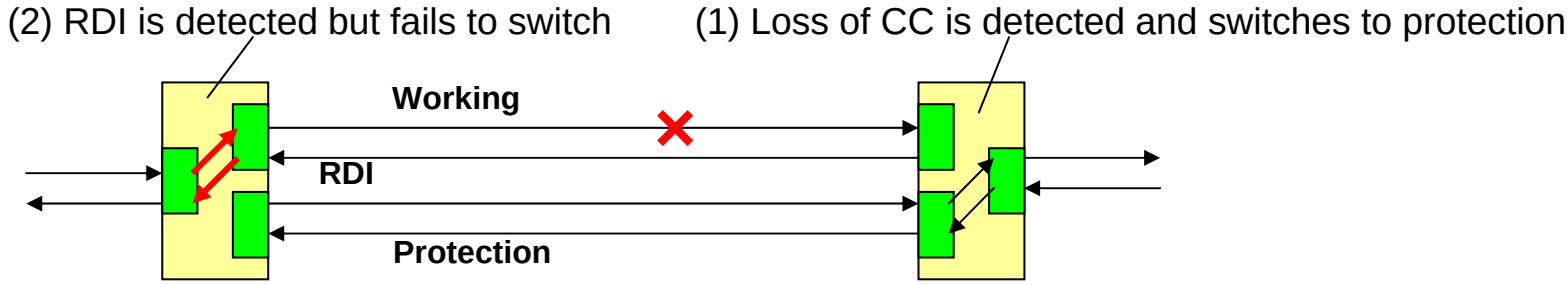
- Requirements identified by ITU-T Rec. G.8031 include the followings:
  - *A mismatch between the bridge/selector positions of the near end and the far end should be detected.*
    - *The bridge/selector mismatch for the local network element should be detected and reported.*
    - *The bridge/selector mismatch should be cleared by a network operator.*
  - *Operator requests such as lockout of protection, forced switch and manual switch commands should be supported.*
  - *Prioritized protection between Signal Fail (SF) and operator requests should be supported.*
- In addition, applicability to NNI/multi-domain case (lines between carriers/providers) can also be a basic requirement.

Mismatch of bridge/selector positions of near end and far end (1)

- Mismatch can happen when:
  - The near end fails to switch over but it sends RDI to the far end due to a hardware malfunction
  - The near end detects a defect and switch but the far end fails to switch even it receives RDI



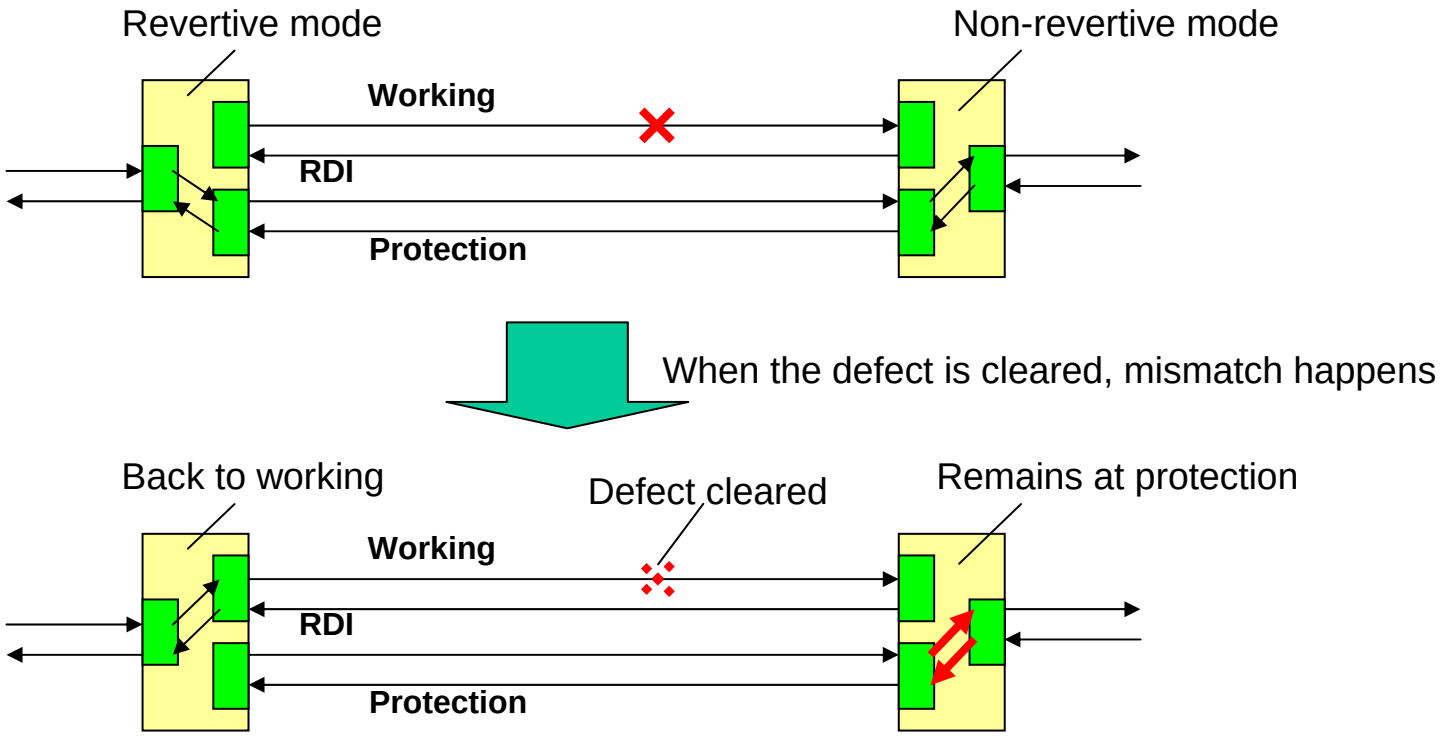
Case A: Switching failure at the near end



Case B: Switching failure at the far end

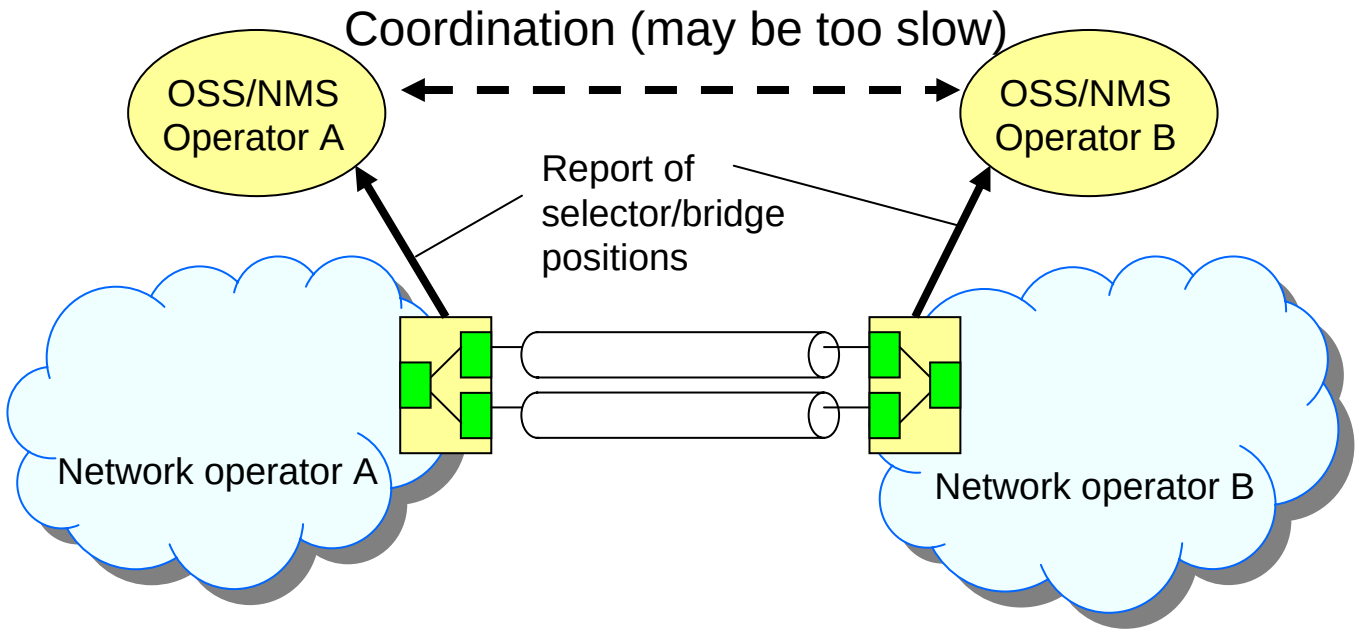
Mismatch of bridge/selector positions of near end and far end (2)

- Mismatch can also happen when the near end is set up in revertive mode and the far end is set up in non-revertive mode by mistake.



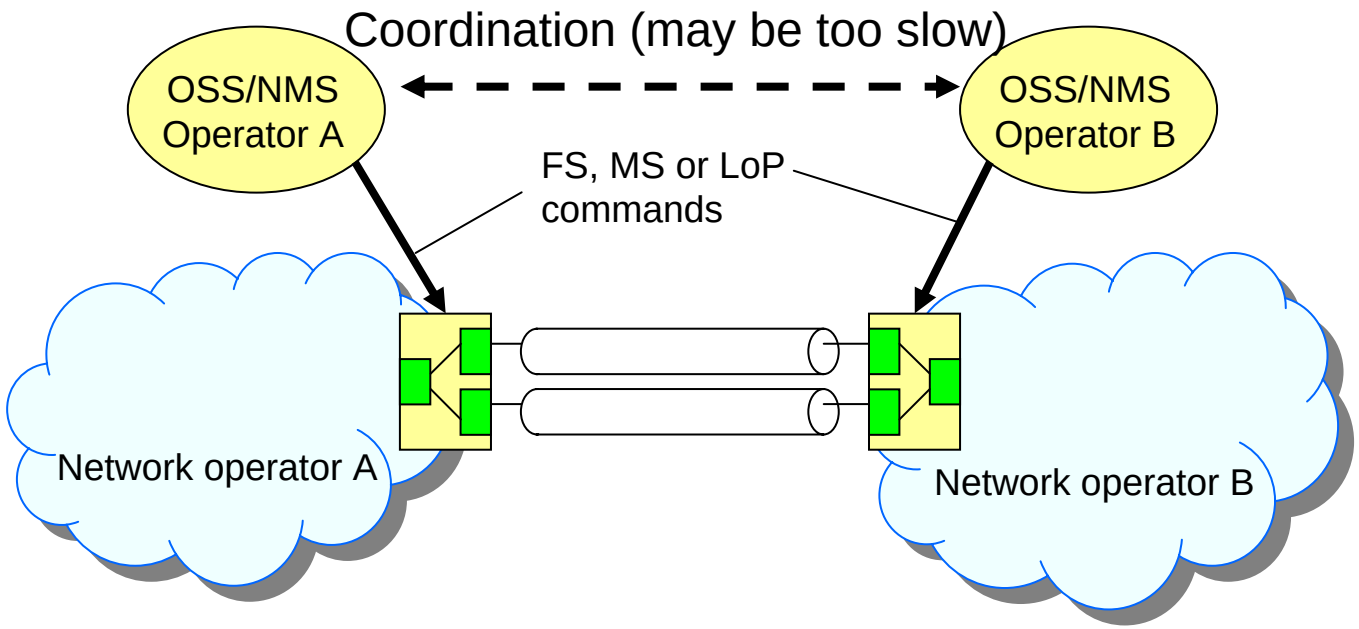
Detection of mismatch

- APS can detect a selector/bridge position mismatch because it exchanges the selector/bridge positions between the near end and the far end.
- Without APS, OSS/NMS needs to compare the selector/bridge positions.
- In the single domain case, either method can be used. However, it should be noted that OSS/NMS may be too slow to detect this mismatch and thus it may not be acceptable.
- In the multi-domain case, OSS/NMSs at the near end and at the far end need to be coordinated to detect the mismatch. In this case, the process may be even slower.



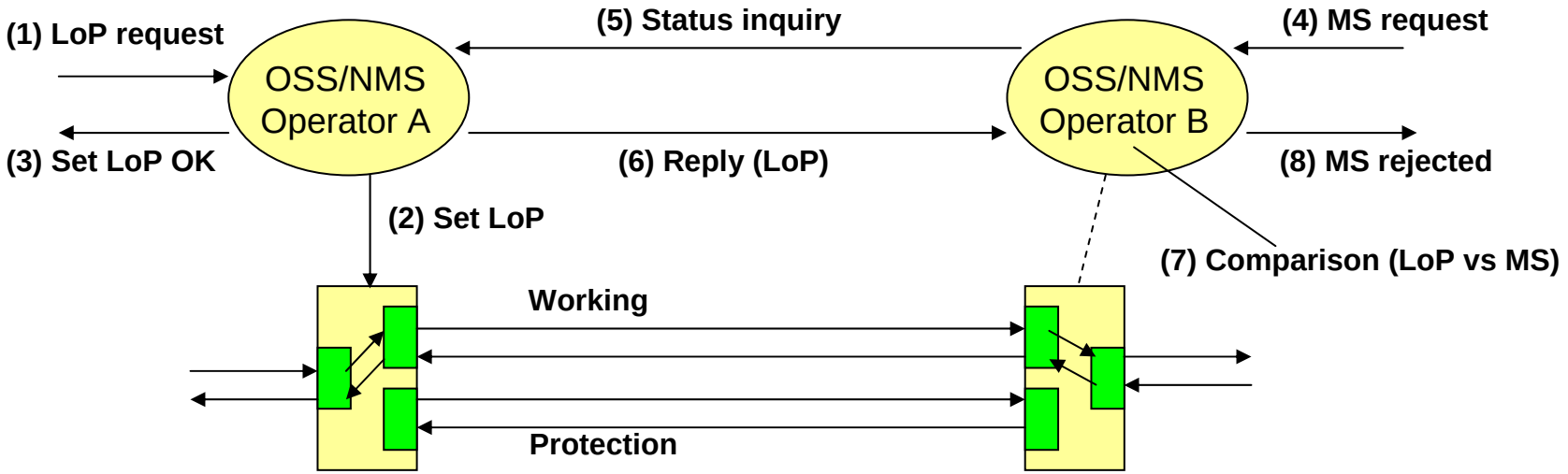
Operator commands without APS

- Without an APS, coordination between two OSS/NMSs is necessary to synchronize both ends for manual switch, forced switch or lockout if both end points belong to different operators.
- It should be noted that the OSS/NMS may be too slow to synchronize the both ends and thus it may not be acceptable (e.g., interruption time may be too long when MS or FS is conducted).



Contention between operator commands and defect status

- If there is a contention between operator commands (MS, FS or LoP) and local/remote request/defect status, the one with the highest priority should be selected.
- Contention can be addressed in the bridges at both ends with the APS protocol or at OSS/NMS.
- If both ends are under the control of different OSS/NMS, coordination between these OSSes/NMSes is necessary for comparison (see below).



Summary and proposals (1)

- For the single domain case (i.e., both ends are under the control of the same OSS/NMS), requirements listed in this presentation can be met with or without APS.
- For the multi-domain case, solution without APS requires coordination between OSS/NMS at both ends. It seems difficult (e.g. from the security viewpoint) because these OSSes/NMSes belong to different carriers.
- It should be noted that coordination between OSSes/NMSes may be too slow for protection switching activities and thus it may not be acceptable.
- It is envisaged that applicability to multi-domain will be required in the near future.
- Even if the current 802.1Qay specifies a solution without APS for the single domain case, it may need to use the APS for multi-domain case.

Summary and proposals (2)

- It should be avoided creating/using two (or more) standards to solve one problem because:
  - It confuses the industry
  - It may cause interoperability problems
  - It may increase the implementation cost to cope with two (or more) standards
- If it is intended to expand 802.1Qay to be applicable to multi-domain case, the current draft should use the protection switching mechanism which is applicable to multi-domain case to be future proof even if the current target is the single domain case only.
- One possible way is to use a mechanism which is compatible with (i.e., subset of) G.8031.