RPR Protection Proposal

Angela Faber, Telcordia

Jason Fan, Luminous

Henry Hsiaw, NEC

John Lemon, Lantern

Vittorio Mascolo, Alcatel
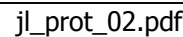
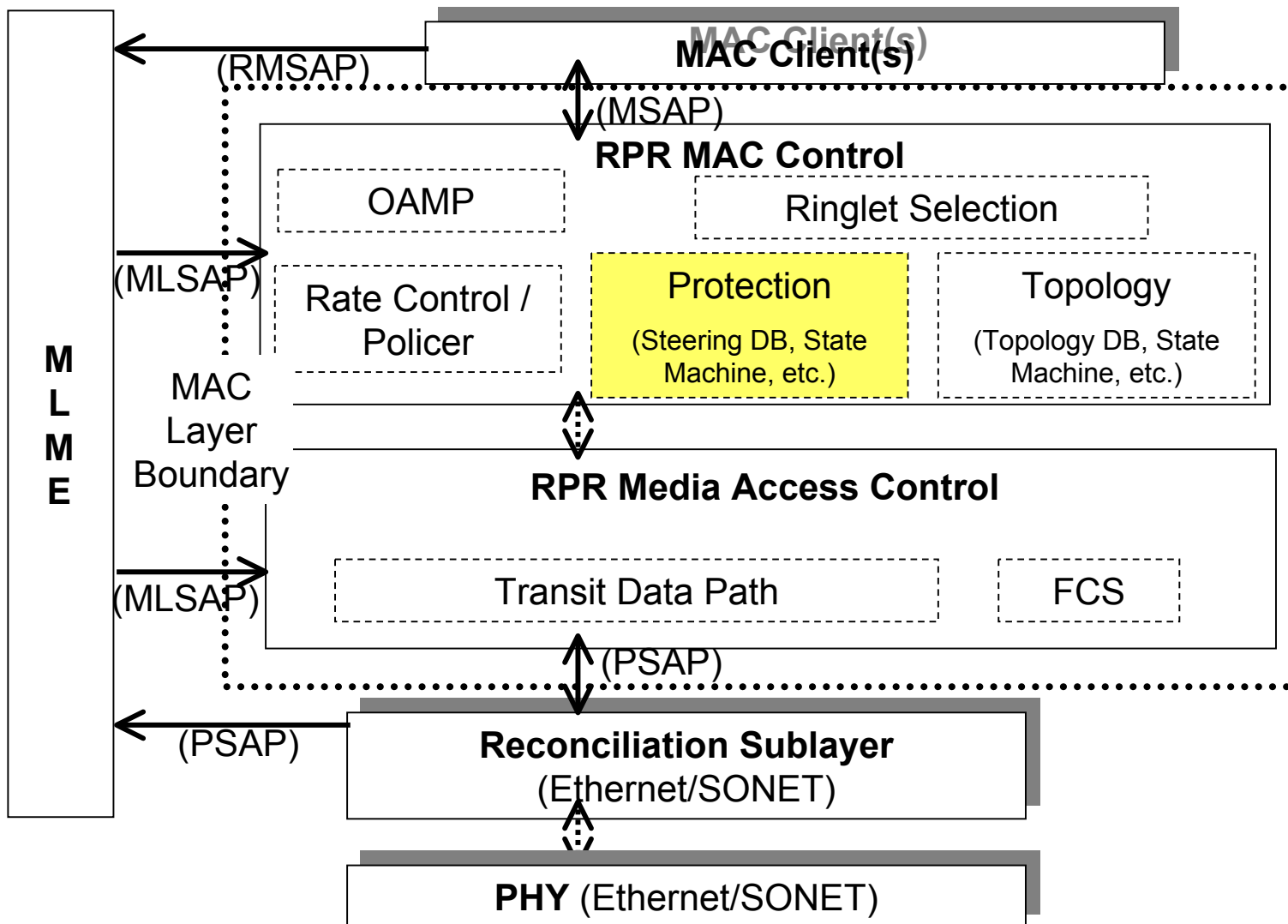Robin Olsson, Vitesse

Harry Peng, Nortel

Frederic Thepot, Dynarc

Components of a complete RPR proposal

Topology Discovery
jf_topo_01.pdf

Protection Switching
jl_prot_01.pdf

RPR MAC
jh_over_01.pdf

MAC Service Definition
jl_ref_01.pdf

Media Access Control

Transit Path
sa_transit_01.pdf

Bandwidth Mgmt.
am_fair_01.pdf

Frame Format
rs_frm_01.pdf

OAM and Layer Mgmt
cb_lmgt_01.pdf
ib_oamp_01.pdf

Bridging mh_brdg_01.pdf
mh_ebrdg_01.pdf

PHY interface

Ethernet
rb_phys_01.pdf

SONET/SDH
rb_phy_01.pdf

802.17 MAC Components

MAC Client(s)

(RMSAP)

(MSAP)

RPR MAC Control

OAMP

Ringlet Selection

(MLSAP)

**M
L
M
E**

MAC
Layer
Boundary

Rate Control /
Policer

Protection

(Steering DB, State
Machine, etc.)

Topology

(Topology DB, State
Machine, etc.)

RPR Media Access Control

(MLSAP)

Transit Data Path

FCS

(PSAP)

(PSAP)

Reconciliation Sublayer
(Ethernet/SONET)

PHY (Ethernet/SONET)

Common Goals

- Protection switching within 50ms
- Scalable from 1 to 100's of stations
- Quick dissemination of loss of connectivity information on the ring

- Tolerance of message loss
- Operation without any master station on the ring
- Operation independent of and in the absence of any management systems
- Operation with dynamic addition and removal of stations to/from the ring

Differing Goals

- Maximal utilization and stable/efficient bandwidth management vs minimal packet loss

- Tolerance of multiple failures vs tolerance of only single failures

- Scalable to multiple ringlets vs designed for dual ringlets only

Overview

- Each station knows of a ring segment failure and steers ring traffic away from the failure within 50ms of the failure

- Ring protection is initiated by all stations that become directly aware of a failure via local detection or through broadcast announcement

Use Of Topology Image

- Each station uses its knowledge of the topology of the ring to know how and when to steer ring traffic away from a failure

Use By Ringlet Selection or MAC Client

- The topology information is combined with the state of each link segment to allow a decision of when and where to steer ring traffic

Triggers

- Protection is triggered by reception of a Link_Status message indicating a new link status

- Link_Status messages are generated as a result of a local link failure or restoration as detected by
  - Physical Layer Triggers
    - SONET/SDH Triggers
    - Ethernet Triggers
  - Manual Triggers
  - Keep_Alive Triggers

Protection Hierarchy

- Protection hierarchy is used to handle multiple, concurrent events

  - FS, Forced Switch - operator originated   (highest priority)

  - SF, Signal Fail (e.g LOS, LOF, EXBER, LOK (Loss Of Keep_Alive)) - automatically originated

  - SD, Signal Degrade - automatically originated

  - MS, Manual Switch - operator originated

  - WTR, Wait Time To Restore - automatically originated

 - NR, No Request present   (lowest priority)

Keep_Alive Control Message

- Provides a means of detecting link failure or station failure

- No data field

- Broadcast on each ringlet with TTL = 1
  - Removed by neighbor

Keep_Alive

Keep_Alive

Keep_Alive
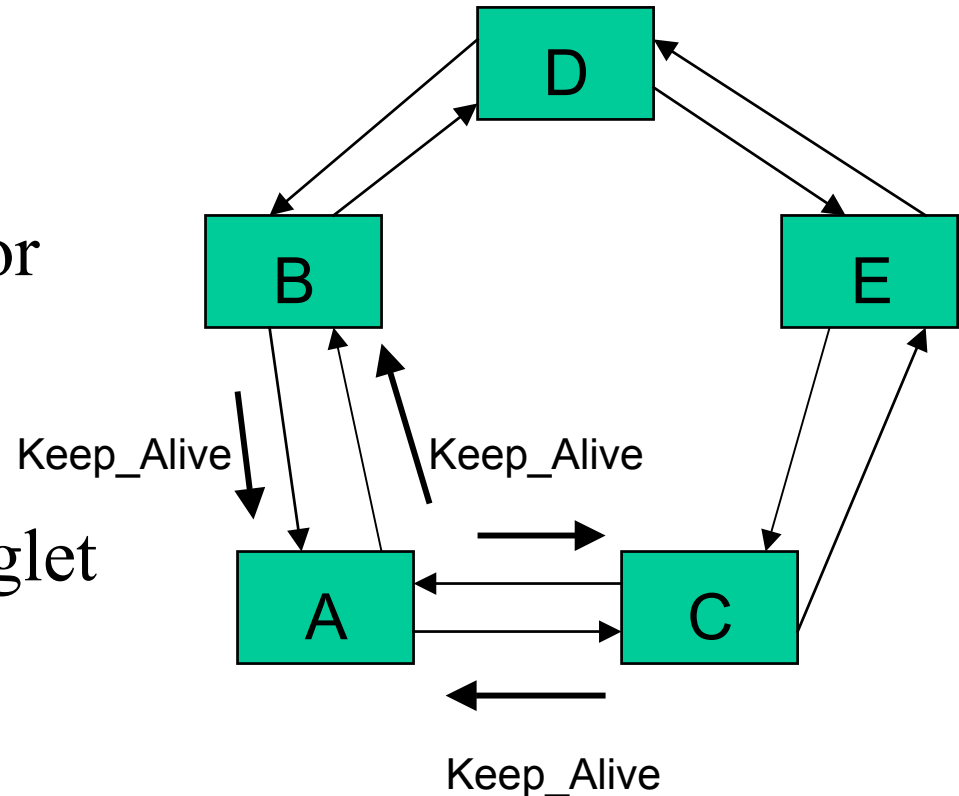
Link_Status Control Message

- Reports changes in neighbor link status

- Key fields
  - Ringlet ID
  - Neighbor link status

- Broadcast on each ringlet with TTL = Max_Ring_Size
  - Removed by source

- Evaluating sending continuously

- Evaluating possibly combining with RCM

Link_Status
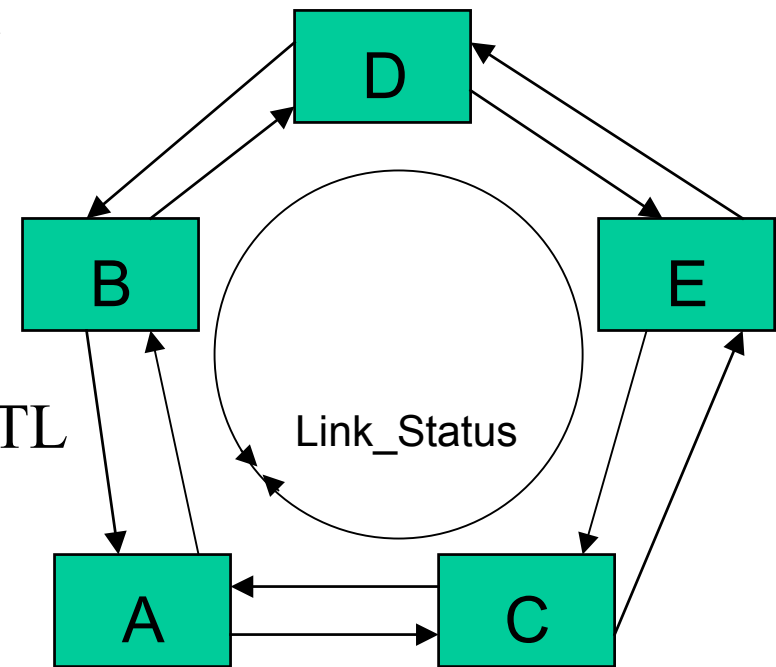
Configurable Parameters

- Hold-Off Time

- Wait To Restore time

- Keep Alive loss threshold for down link declaration

- Uni-directional/Bi-directional protection switching mode

- Revertive/Non-revertive protection switching mode

Unicast Protection

- If sourcing station can reach intended destination through normal route, then use normal route

- Otherwise, if packet is protected and it can reach intended destination through protection route, then use protection route

Multicast Protection

- If sourcing station can reach intended destination through normal route, then use normal route

- Else, if packet is protected and it can reach intended destination through protection route, then use protection route

- Otherwise, use both routes (2 counter-rotating ringlets)

- TTL is set to the distance to the failed link on each ringlet

Steering Performance Analysis

- Set up
  - 64 stations, 640 km circumference
  - Dual ringlet ring, 1 Gbps ring rate
  - Processing times for messages set to exponentially distributed times around mean of 200 usec for Keep_Alive messages and 500 usec for Link_Status messages
  - Keep_Alive interval: 1ms

- Failure Scenario
  - Link 0->1 goes down
  - Failure is detected by not receiving a Keep_Alive in 3 intervals

Steering Performance Analysis, contd

- Response time = time when all the stations can start protection switching – time when the failure occurs

- Response time = 5.2 ms

Protection Summary

- Broadcast based algorithm best for steering
- Stability and robustness in case of multiple failures
- Support for multiple ringlets
- Support for Layer 1+2 failure detection
- Also works well for wrapping