Features of the Simple DRNI

János Farkas

Balázs Péter Gerő

Panagiotis Saltsidis

A simple control for the DRNI

› A simple approach was proposed for the control of the DRNI, details were presented in:
  – new-farkas-DRNI-control-0311.pdf
  – new-farkas-network-interconnect-functionalities-0910-v01.pdf

› The simple DRNI meets the PAR requirements
  – Isolation of the attached networks
    › Failure (independent Gateway selection)
    › Control (minimal external control messages)
    › Management (minimal coordination)
  – Provides redundant, protected connectivity
  – Provides control of forwarding path, thus also providing congruency
  – Backwards compatibility to 802.1AX

› Simplicity is preferred for the open items of DRNI operation

Scope of DRNI
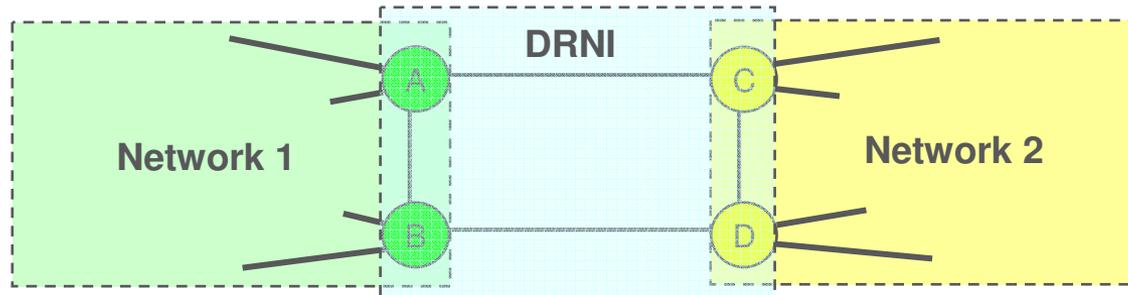
› DRNI covers
- All external links
- All portal nodes and portal internal links

› DRNI may use any of these links for forwarding of user traffic

Status sharing in the simple DRNI
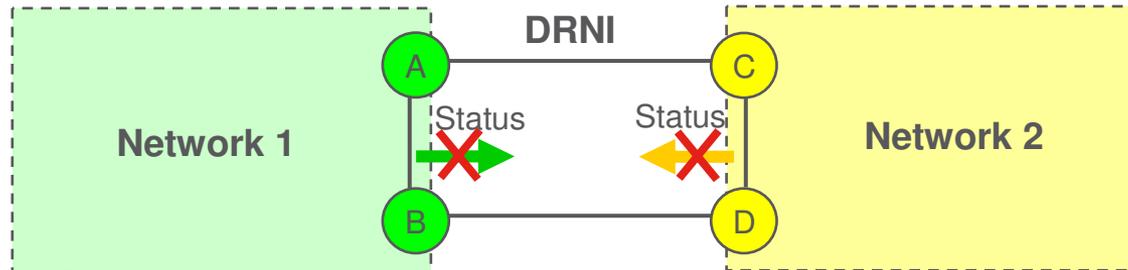
› Status of external links is known by each DRNI node
› Status of provider internal links is not advertised to the peering party
› Nodes of the same Portal (e.g. A and B) claim to be a single node towards the peering party (A and B use the same System ID and Key in LACP)
  – The status of the single node with the common System ID is known to the peering party

Authority of control
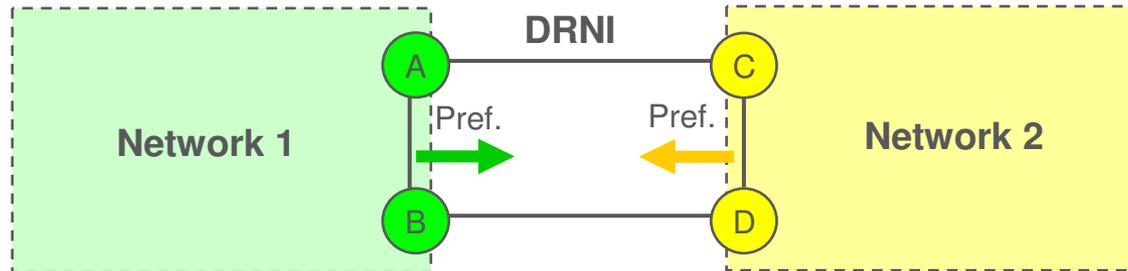
› DRNI adapts to the preferences of the networks
› If failure isolation is required, then DRNI does not re-select Gateways
   – If avoiding Portal internal traffic is preferred to failure isolation, then simple DRNI is able to bind Gateway selection to external link selection

DRNI control messages between peers
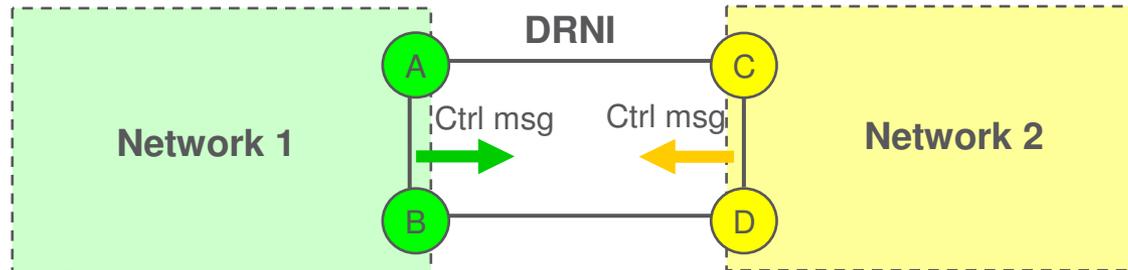
› Split-brain is handled as discussed before
  – new-haddock-RNNI-split-brain-avoidance-1210-v1.pdf
  – Graceful name change: new-nfinn-light-nni-0710-v04.pdf
› Simple DRNI minimizes messaging between peers
  – Digest exchange for misconfiguration detection
  – A message in order to express external link preference is possible
› Bundling becomes simpler with minimal messaging
 – DRNI bundles (if any) are Portal internal for an S-tagged Interface

Traffic distribution by DRNI
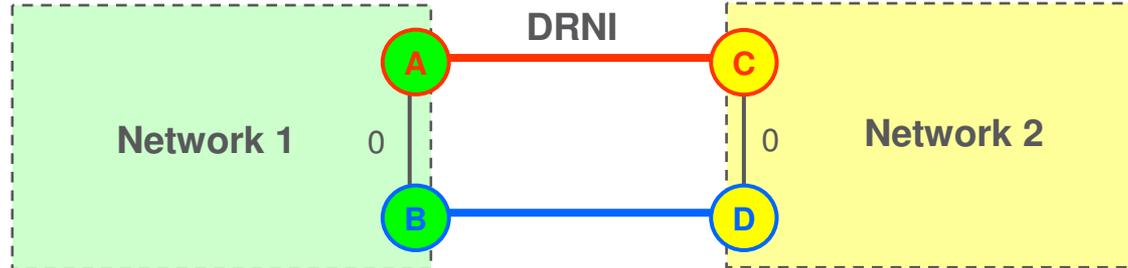
› Simple DRNI does not use Portal internal links for congruent data traffic during normal conditions, unless manual configuration overrides
  – Auto-provisioning (Portal internal) selects Gateways directly attached to the external link selected
  – Auto-provisioning may take Bandwidth Profile into account for better load distribution

Discussion on load distribution

› How much capacity do we need?

› We need spare capacity to carry all the protected traffic in case of a single failure

  – Red set of services need T1 capacity in total
  – Blue set of services need T2 capacity in total

Normal operation   Failure event
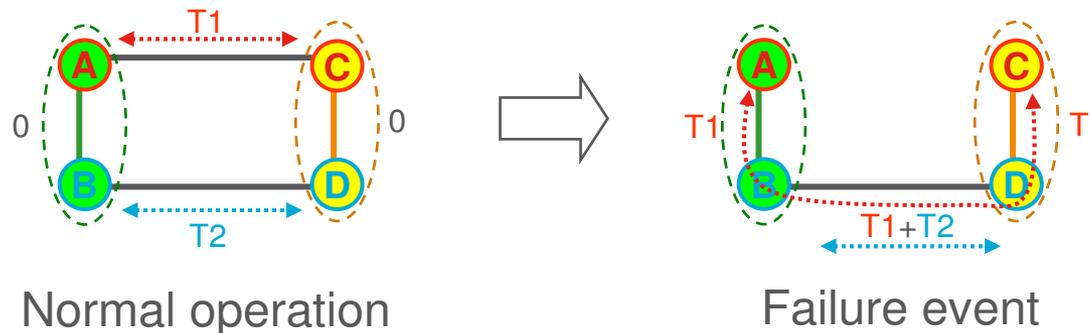
Summary

› Simple DRNI is quite capable

› Besides meeting the PAR requirements, simple DRNI
  – hides provider internal data
  – adapts to provider preferences
  – minimizes messaging between peers thus simplifies bundling
  – able to distribute traffic on the external links
  – able to provide zero Portal internal traffic