PBB-TE Infrastructure Protection Proposed PAR

IEEE 802.1 May 2009 Interim Meeting
Pittsburgh, PA., USA

Bob Sultan; Ben Mack-Crane (Huawei Technologies)
Vinod Kumar (Tejas Networks)
Corona Wei; Irene Ao (ZTE)
Steve Haddock
Ken Young (Gridpoint Systems)
Dave Martin (Nortel Networks)
Abhay Karandikar (Indian Institute of Technology, Bombay)
John Lemon (Adtran)
Haim Porat (Ethos Networks)

Title

- PAR for an amendment to an existing Standard 802.1Q
- P802.1Qbc (or Qbd, etc., as appropriate)
- lEEE Standard for Local and Metropolitan Area Networks---Virtual Bridged Local Area Networks - Amendment: PBB-TE Infrastructure Segment Protection

Scope (1)

- **Protect a specified group of Traffic Engineered Shared Forwarding Paths that traverse an Infrastructure Segment, where an Infrastructure Segment is a sequence of LANs and intervening bridges;**
- **Support for explicit association of a Shared Forwarding Path with a Protected Segment or explicit exclusion of a Shared Forwarding Path from participation in Infrastructure Segment Protection;**
- **Support Infrastructure Segment Protection by diverting traffic from the failed segment to a backup segment having the same segment endpoint bridges but an otherwise diverse path;**
- **Support Infrastructure Segment Protection by methods that do not require modification of data or control frames;**

Scope (2)

- **May support the protection of a single segment by multiple backup segments (M:1 Infrastructure Segment Protection) where backup segments become active in a specified priority order;**
- **Support for topologies having adjacent Infrastructure Segments (ie., segments sharing a common endpoint bridge);**
- **Specification of a method to monitor Infrastructure Segment continuity using existing OAM mechanisms;**
- **Operator requests (e.g., FS, MS, LoP) and operational modes (e.g., revertive, non-revertive) consistent with those supported by PBB-TE TESI Protection.**
- **MIBs and Managed Objects associated with Infrastructure Segment Protection.**

Purpose

- **Address the relatively high failure rate of particular links or bridges within a network.**
- **Address the likelihood of concurrent failures occurring in different segments of a network.**
- **Allow maintenance activities to be performed independently in different segments of the network.**
- **Allow maintenance activities to be performed in one segment of a network without disabling protection in another segment.**
- **Localize changes in traffic distribution due to failure or maintenance actions.**

Need

- It is anticipated that Traffic Engineered bridged networks will be widely deployed when the PBB-TE (IEEE 802.1Qay) standard becomes available. Currently, only end-to-end 1:1 TESI protection is specified. Localized infrastructure protection is supported by TDM-based and MPLS-based networks. The absence of such localized protection capability in PBB-TE networks puts Bridging technology at a competitive disadvantage.

Stakeholders

- Vendors, users, administrators, designers, customers, and owners of traffic-engineered bridged networks.

Other standards with similar scope

- There are no standards providing localized protection for IEEE 802.1Q PBB-TE networks.

Five Criteria

Broad Market Potential

A standards project authorized by IEEE 802 shall have a broad market potential. Specifically, it shall have the potential for:

- Broad sets of applicability.
  - The commercial provision of Traffic Engineered services is a large and growing business.
- Multiple vendors and numerous users.
  - The same large body of vendors and users having a requirement for IEEE 802.1Qay.
- Balanced costs (LAN versus attached stations).
  - This project does not materially alter the existing cost structure of bridged networks.

Compatibility

- IEEE 802 defines a family of standards. All standards shall be in conformance with the IEEE 802.1 Architecture, Management, and Interworking documents as follows: 802. Overview and Architecture, 802.1D, 802.1Q, and parts of 802.1f. If any variances in conformance emerge, they shall be thoroughly disclosed and reviewed with 802.
  - This PAR is for an amendment to 802.1Q, thus ensuring compatibility.
- Each standard in the IEEE 802 family of standards shall include a definition of managed objects that are compatible with systems management standards.
  - Such a definition will be included.

Distinct Identity

Each IEEE 802 standard shall have a distinct identity. To achieve this, each authorized project shall be:

- Substantially different from other IEEE 802 standards.
  - This project will amend the only IEEE 802 standard defining Traffic Engineered bridged networks.
- One unique solution per problem (not two solutions to a problem).
  - There are no other standard solutions to localized recovery in a Traffic Engineered bridged network.
- Easy for the document reader to select the relevant specification.
  - This project will amend the only IEEE 802 standard defining Traffic Engineered bridged networks.

Technical Feasibility

For a project to be authorized, it shall be able to show its technical feasibility. At a minimum, the proposed project shall show:

- Demonstrated system feasibility.
  - The function technically is similar to PBB-TE TESI protection which is currently specified by amendment 802.1Qay to 802.1Q, which has been successfully implemented.
- Proven technology, reasonable testing.
  - The function can be implemented using existing bridge behaviors. Compliance with the project can be tested using straightforward extensions of existing test tools for bridged networks.
- Confidence in reliability.
  - The reliability of the modified protocols will be not be measurably worse than that of the existing Traffic Engineered Bridged networks.

Economic Feasibility

For a project to be authorized, it shall be able to show economic feasibility (so far as can reasonably be estimated) for its intended applications. At a minimum, the proposed project shall show:

- Known cost factors, reliable data.
  - This project introduces no hardware costs beyond the minimal and well-known resources consumed by extending an existing software protocol.
- Reasonable cost for performance.
  - The cost of upgrading software and configuring a priori knowledge of the overall system topology is reasonable for the significant reduction in the time required to recover from a network failure.
- Consideration of installation costs.
  - The cost of installing enhanced software, in exchange for improved network performance, is familiar to vendors and users of bridged networks.