INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2001-2004

STUDY GROUP 13

TD 23 Rev.1 (PLEN)

English only

Question(s): 3/13 Geneva, 21 July - 1 August 2003

TEMPORARY DOCUMENT

Source: Rapporteur, Q.3/13

Title: Draft Recommendation Y.17ethreq (Y.1730) (Requirements for OAM functions in Ethernet based network)

This TD provides the text for Draft Recommendation Y.17ethreq (Requirements for OAM functions in Ethernet based network) in its Annex. It is proposed for consent.

Contact: Hiroshi Ohta
NTT
Japan

Tel: +81 422 59 3617
Fax: +81 422 59 3782
Email: ohta.hiroshi@lab.ntt.co.jp

ANNEX

ITU-T Draft Recommendation Y.17ethreq

Requirements for OAM functions in Ethernet based networks

Summary

This Recommendation provides the motivations and requirements for user-plane OAM (Operation, Administration and Maintenance) functionality for Ethernet based networks. The scope of this recommendation includes the requirements for OAM functions for the point-to-point and multipoint-to-multipoint Ethernet connections including both dedicated and shared access. It is noted that this Recommendation does not address the administration aspects of OAM.

Key Words

Ethernet, OAM, ETH, ETY, EPL, EVPL, EPLAN, EVPLAN

Draft Recommendation Y.17ethreq

Requirements for OAM functions in Ethernet based networks

1. Scope

This Recommendation provides the motivations and requirements for user-plane OAM (Operation, Administration and Maintenance) functionality for Ethernet based networks. The scope of this recommendation includes the requirements for OAM functions for the point-to-point and multipoint-to-multipoint Ethernet connections including both dedicated and shared access. It is noted that this Recommendation does not address the administration aspects of OAM.

2. References

The following ITU-T Recommendations and other references contain provisions, which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published.

Note - The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[1] ITU-T Recommendation I.610 (1999), *B-ISDN operation and maintenance principles and functions*.

[2] ITU-T Recommendation G.805 (2000), *Generic functional architecture of transport networks*.

[3] ITU-T Recommendation G.806 (2000), Characteristics of transport equipment – description methodology and generic functionality

[4] ITU-T Recommendation G.809 (2003), *Functional architecture of connectionless layer networks*

3. Definitions

This Recommendation introduces some functional architecture terminology that is required to discuss the network components associated with OAM. Relevant terms are defined below.

3.1 **anomaly:** The smallest discrepancy which can be observed between the actual and desired characteristics of an item. The occurrence of a single anomaly does not constitute an interruption in the ability to perform a required function. Anomalies are used as the input for the Performance Monitoring (PM) process and for the detection of defects [3].

3.2 **defect**: The density of anomalies has reached a level where the ability to perform a required function has been interrupted. Defects are used as input for PM, the control of consequent actions, and the determination of fault case [3].

3.3 **ETH trail:** a connectionless trail in the ETH layer network[4].

3.4 **ETH link:** a flow point pool link in the ETH layer network[4].

3.5 **failure**: The fault cause persisted long enough to consider the ability of an item to perform a required function to be terminated. The item may be considered as failed; a fault has now been detected.

3.6 **fault cause:** A single disturbance or fault may lead to the detection of multiple defects. A fault cause is the result of a correlation process which is intended to identify the defect that is representative of the disturbance or fault that is causing the problem [3].

3.7 **flow domain:** A topological component used to effect forwarding of a specific characteristic information

3.8 **flow point:** A “reference point” that represents a point of transfer for traffic units between topological components

3.9 **flow point pool link:** A “topological component” which describes a fixed relationship between a “flow domain” or “access group” and another “flow domain” or “access group” [4].

3.10 **link:** A "topological component" which describes a fixed relationship between a "subnetwork" or "access group" and another "subnetwork" or "access group" in a connection-oriented layer network[2].

3.11 **termination flow point:** A reference point that represents the binding of a flow termination to a flow.

3.12 **trail:** A "transport entity" in a connection-oriented layer network which consists of an associated pair of unidirectional trails capable of simultaneously transferring information in opposite directions between their respective inputs and outputs[2].

4. Symbols and abbreviations

This Recommendation uses the following abbreviations.

AP	Access Point
CO-CS	Connection-Oriented Circuit Switching
CO-PS	Connection-Oriented Packet Switching
CLPS	Connectionless Packet Switching
DoS	Denial of Service
ETH	Ethernet
ETY	Ethernet physical layer
EPL	Ethernet Private Line
EVPL	Ethernet Virtual Private Line
EPLAN	Ethernet Private LAN
EVPLAN	Ethernet Virtual Private LAN
FD	Flow Domain
FP	Flow Point
LF	Link Flow
MAC	Media Access Control
ME	Maintenance Entity
NMS	Network Management System
NNI	Network Node Interface

OAM	Operation, Administration and Maintenance
SLA	Service Level Agreement
TFP	Termination Flow Point
UNI	User-Network Interface

5. Reference networks

This Recommendation specifies the requirements for OAM functions which are applied to point-to-point and multipoint-to-multipoint Ethernet flows. Figure 1 provides a layered network perspective of a point-to-point flow according to the methodology of Recommendation G.809. In this particular example, network elements A and D, which are placed in customer premises, are associated with ETH TFPs and the ingress and egress of a network flow.

Note that between the network elements B and C, which are placed at the edges of the provider's network, the ETH link flow is supported by a single server layer, (S), trail. S may be a connection oriented circuit switched or connection oriented packet switched. S may itself be supported by lower layer networks.

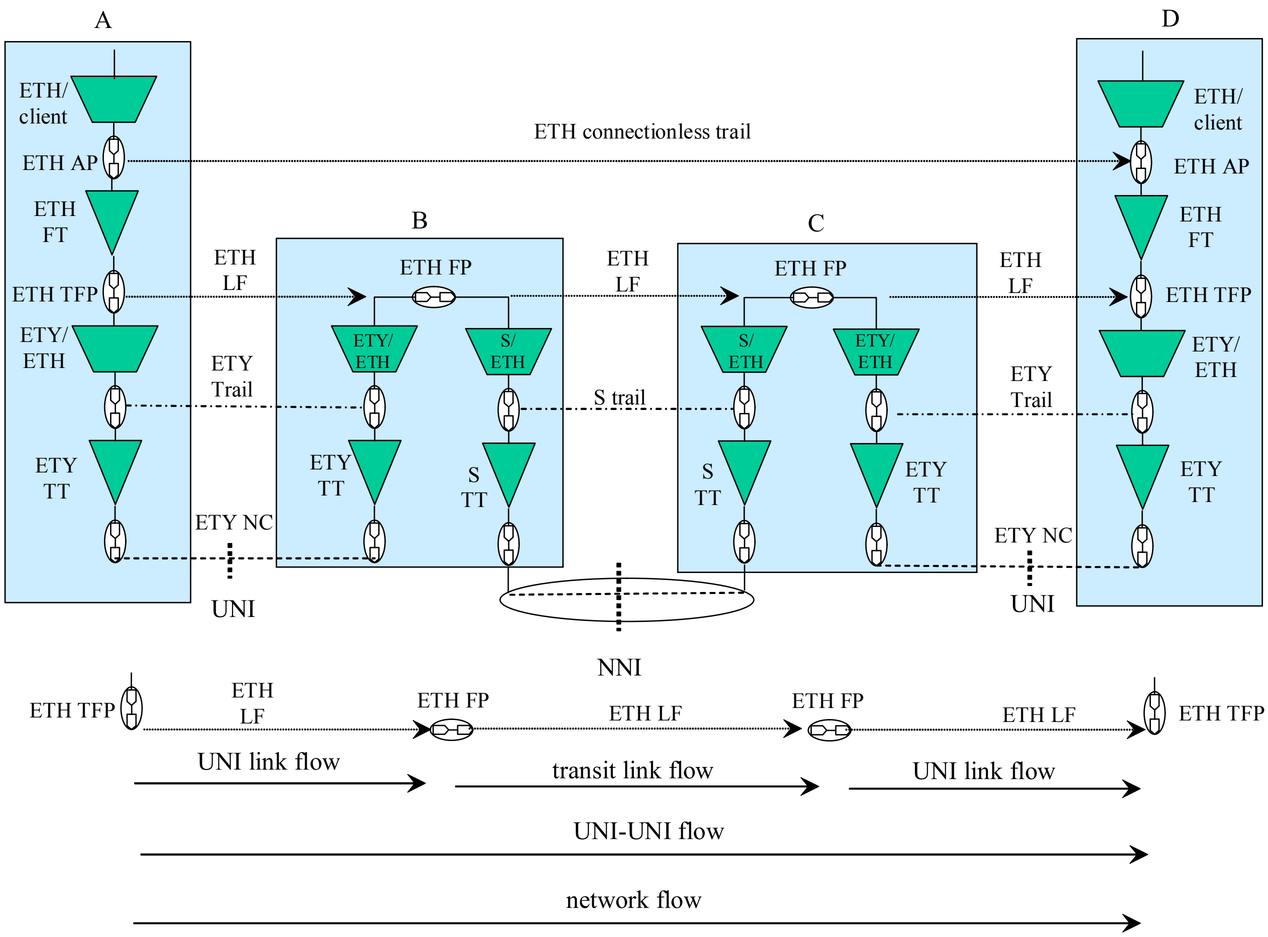

Figure 1/Y.17ethreq Example of point-to-point Ethernet flow reference model (1)

A second case of a flow is illustrated in figure 2. Here the network elements A and D, which are placed in user premises, are associated with ETH FPs, indicating that they are associated with bridging. In this case the "UNI-UNI" flow is between flow points rather than termination flow points. As such the UNI-UNI flow is not the same as the network flow.

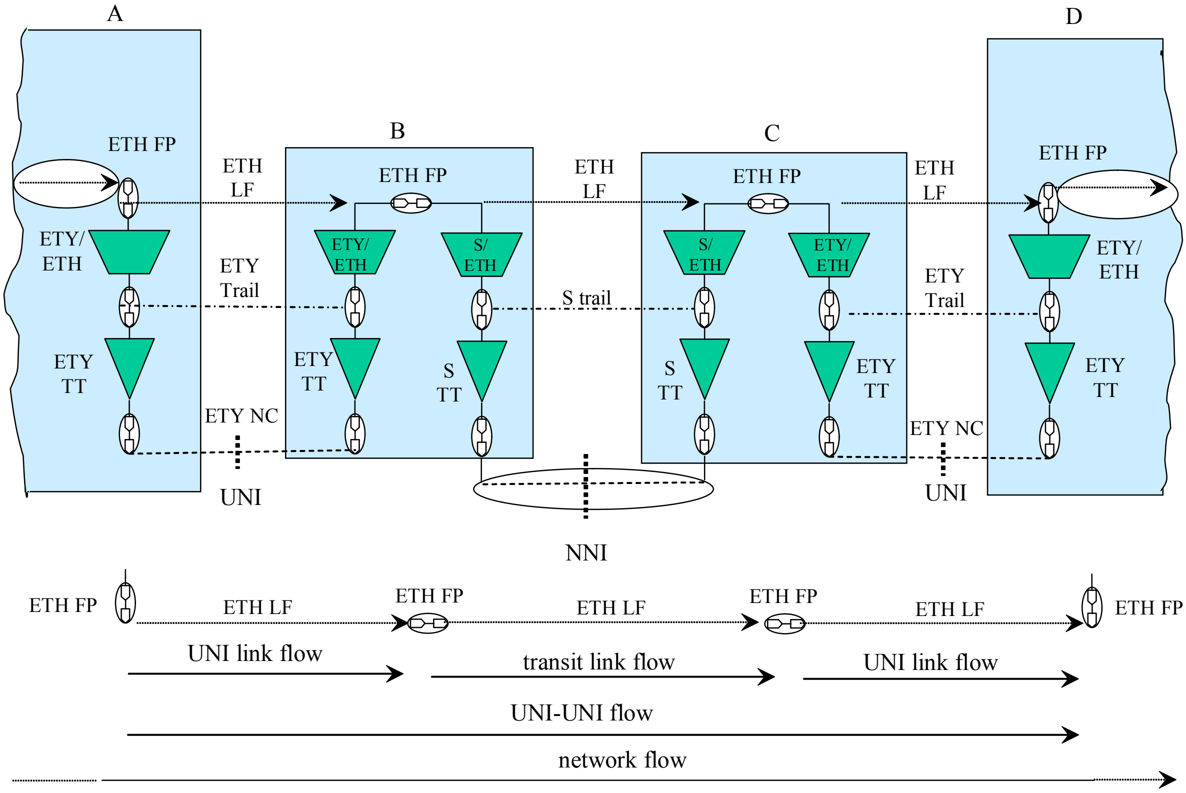

Figure 2/Y.17ethreq Example of point-to-point flow reference model (2)

In both the cases above there is a single server technology between the network elements B and C. Reference models where ETH link flows are supported by different server layer technologies, S and Z, are as illustrated in figures 3 and 4. The difference between Figures 3 and 4 is whether the network elements A and E are associated with flow points or termination flow points.

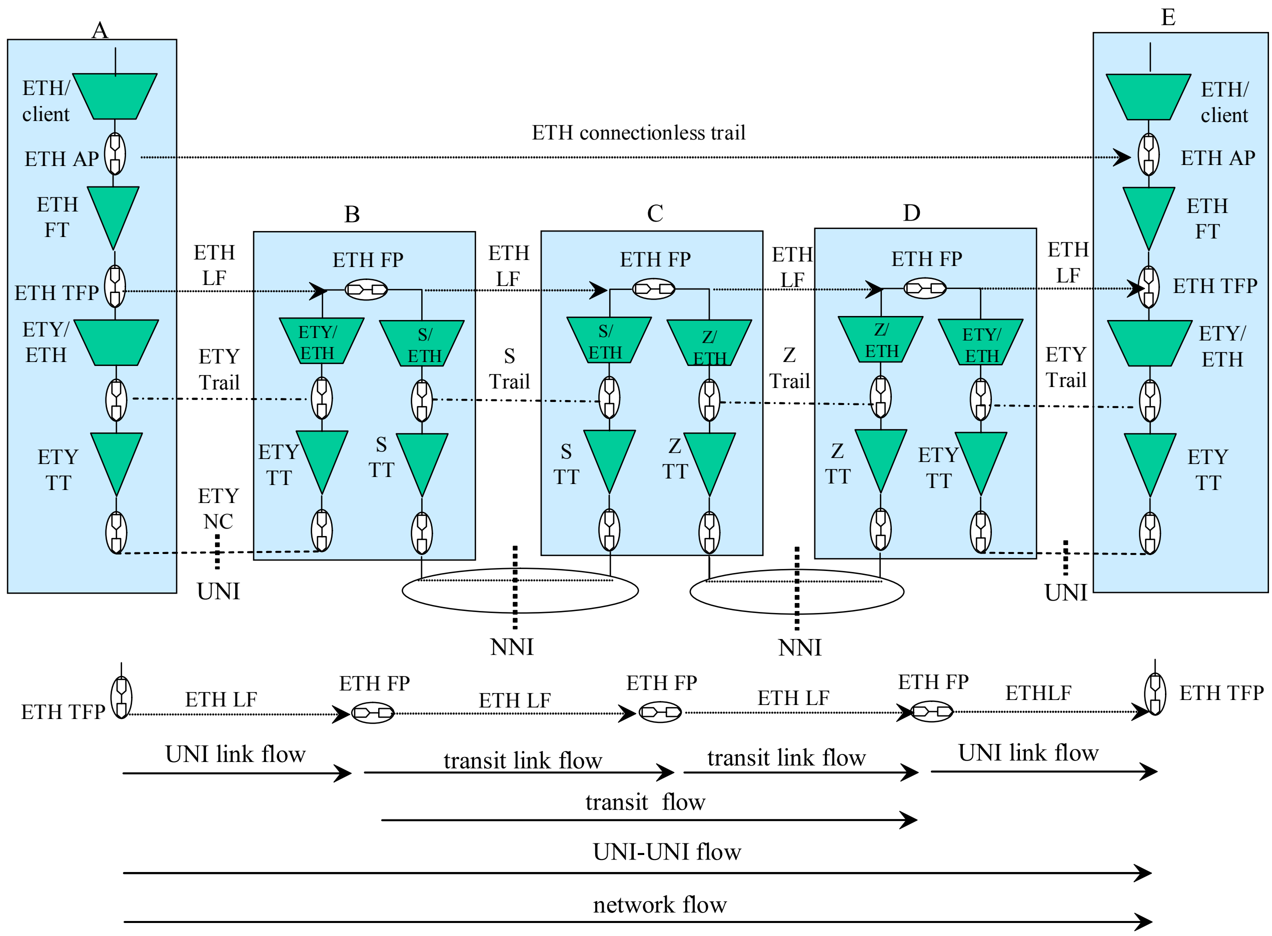

Figure 3/Y.17ethreq Example of point-to-point flow reference model (3)

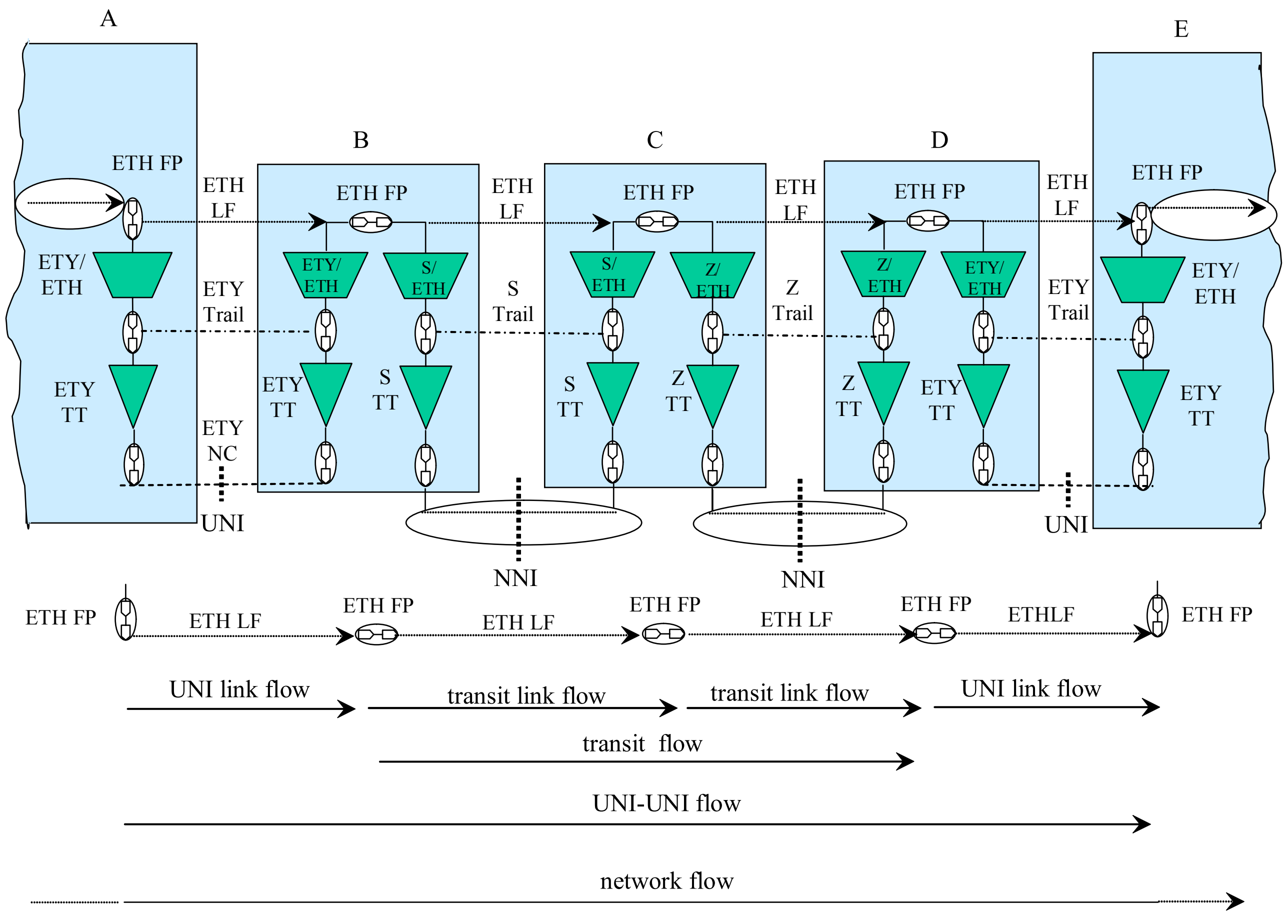

Figure 4/Y.17ethreq Example of point-to-point flow reference model (4)

Figure 5 shows the functional model of hand-off portion between two providers. A and B denote the network elements placed at the boundary. It is noted that server layer between hand-off points can be any physical layer although ETY layer is used in this example.

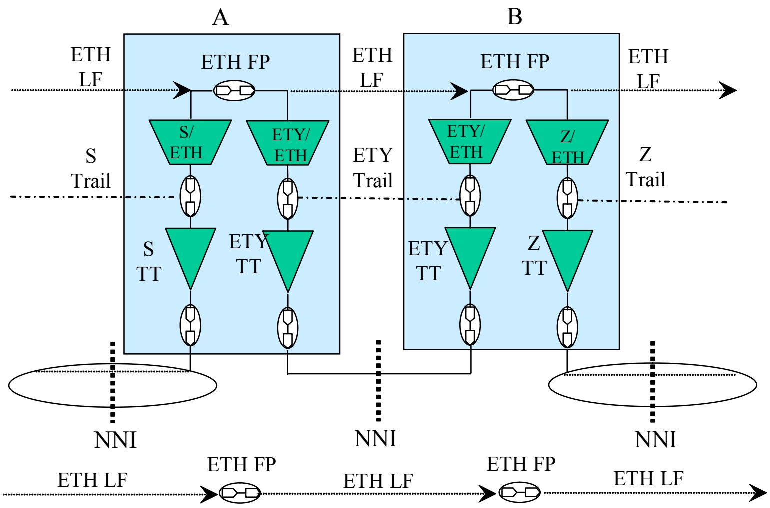

Figure 5/Y.17ethreq Example of hand-off point reference model

The view of the reference models in terms of layer networks and the relationships can be simplified by considering only the flows present in the ETH layer network. This is illustrated in figures 5 and 6.

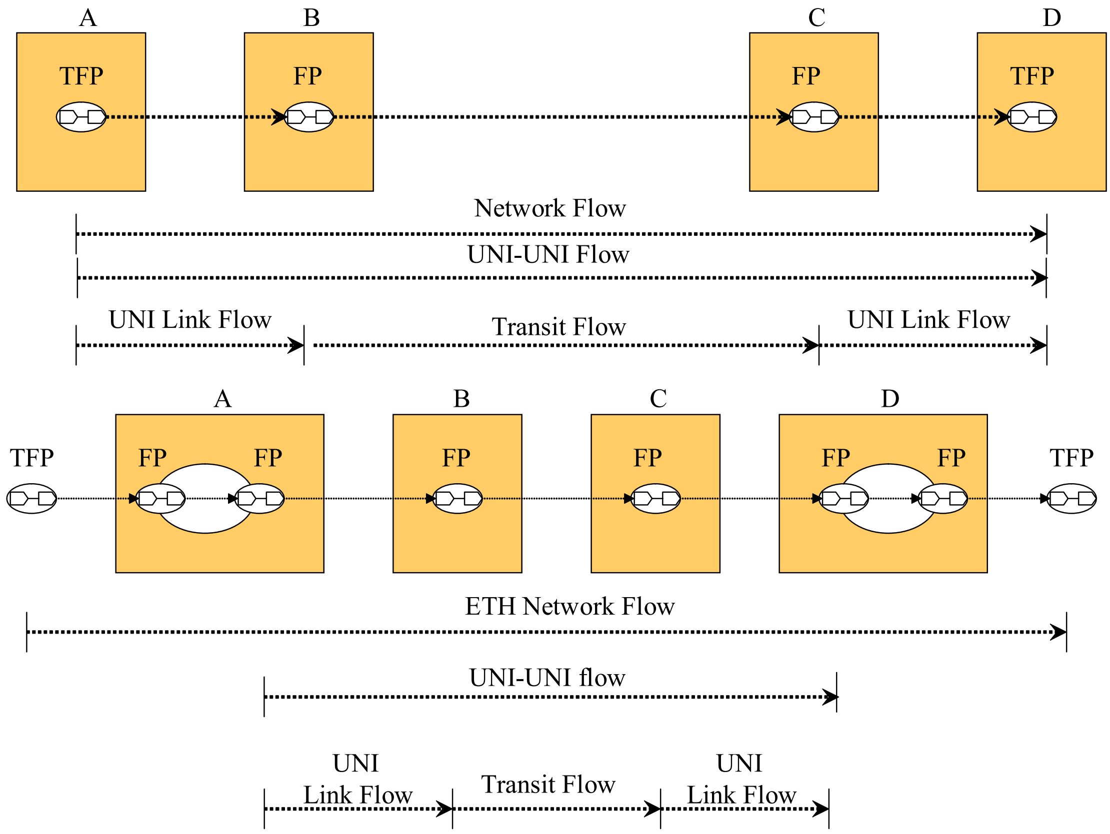

Figure 6/Y.17ethreq Example of point-to-point flow reference model in the ETH layer network (1)

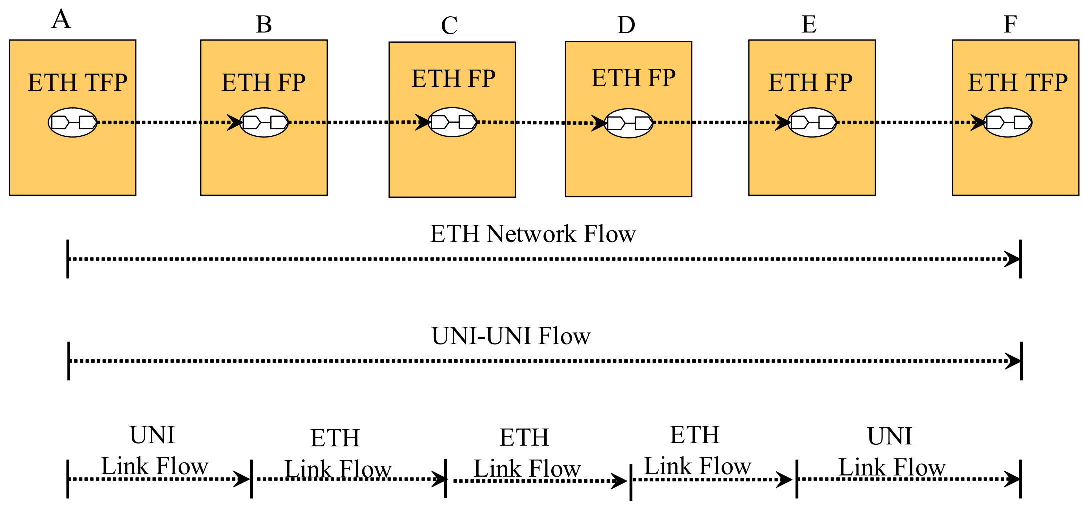

Figure 7/Y.17ethreq Example of point-to-point flow reference model in the ETH layer network (2)

This single layer network view is used to describe the multipoint-to-multipoint case. This is illustrated in figure 7. The ETH flow domains (FDs) is present as a provider network. In this figure, network element A, B, C, D, E and F are network elements owned by each user. A to E are bridges while F is a host. G, H and I are provider network elements placed at their edge. J is a network element placed in the core of the provider's network. G to I can be bridges.

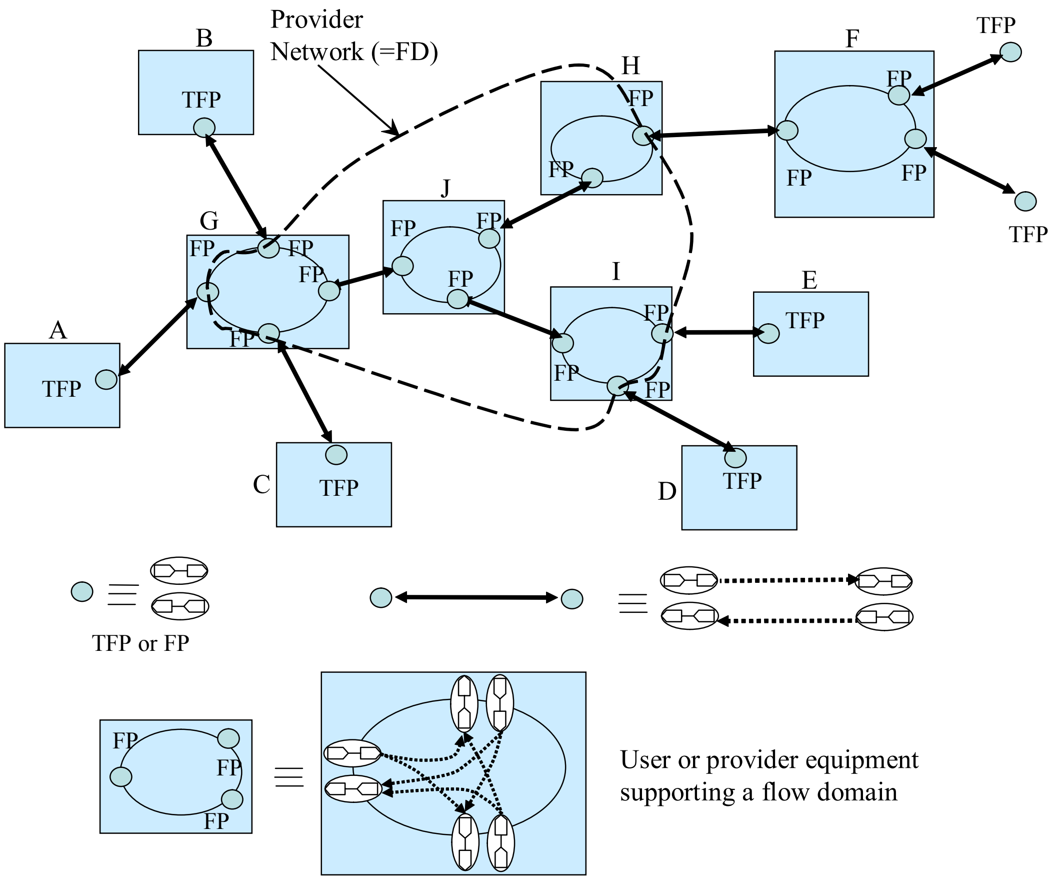

Figure 8/Y.17ethreq Multipoint-to-multipoint reference model in the ETH layer network.

6. Point-to-point and LAN service types

There are two point-to-point service classes, Ethernet Private Line (EPL), and Ethernet Virtual Private Line (EVPL). These may be further classified as providing a full rate or fractional rate service. The reference model for these services is that of figure 6 and 7.

There are two LAN services provided by multi-point to multi-point flows, Ethernet Private LAN (EPLAN), Ethernet Virtual Private LAN (EVPLAN). The reference model for these services is that of figure 8.

These services are described in Appendix III.

7. Motivation for OAM functionalities for Ethernet based networks

It is recognized that OAM functionality is important in public networks for ease of network operation, for verifying network performance, and to reduce operational costs. OAM functionality is especially important for networks that are required to deliver (and hence be measurable against) network performance and availability objectives. In order to offer a reliable Ethernet service that can support the requirements of a service level agreement (SLA), it is necessary that the Ethernet service has its own OAM capabilities.

The major motivations for Ethernet OAM are discussed further below.

1. Ethernet provides a unique connection oriented layer network, ETY, and a connectionless layer network, ETH, and hence there will be failure modes that are only relevant to Ethernet. In

general, lower-layer (server-layer) or higher-layer (client-layer) OAM mechanisms cannot act as a substitute for Ethernet OAM functionality. This observation is also critical to ensure that network technologies can evolve independently.

2. Operators need an ability to determine Ethernet availability and network performance, noting that network performance metrics are only meaningful when the service is in the available state. This information may also be used for accounting and billing purposes to ensure that customers are not inappropriately charged for degraded service or service outages.
3. Reduce operating costs, by allowing efficient detection, handling, and diagnosis of defects. Lack of automatic defect detection and handling forces operators to increase their engineering and support workforce, and hence increases overall operating costs.
4. Reduce the duration of defects and thus improve the availability performance.
5. Demonstrate a commitment to provide customer traffic security/confidentiality by ensuring that any defects that result in mis-directed customer traffic are desired to be detectable/diagnosible and lead to appropriate actions, e.g. squelching of traffic where relevant.
6. Minimise the number of defects that are not automatically detected and still require a customer to report a problem. Pro-active maintenance actions like this also help drive down operating costs by minimising the opportunity for incorrect defect diagnosis, and (like the previous item) they also promote customer trust of an operator.
7. Allow differentiation of defects arising from lower layers to those from within the Ethernet layered network structure to be considered, so that more intelligent protection-switching actions can be used.

8. General requirements for Ethernet OAM functions

The following requirements should be satisfied by Ethernet OAM:

1. Support of client/server OAM relationships between Ethernet and its server layers (e.g., signal fail/signal degrade). Applicability of this item to LAN service is for further study. Applicability of this item in the case where the server layer is connection oriented and client layer is connectionless LAN service is for further study.
2. Both on-demand and continuous connectivity verification of communication between edges of OAM maintenance entities to confirm that defects do not exist across the monitored Ethernet maintenance entity.
3. If a defect occurs, it is necessary to detect it, diagnose it, localise it, notify network management systems and take corrective actions appropriate to the type of defect. The primary objective is to reduce operating costs by minimising service interruptions, operational repair times and operational resource.
4. In the case of the provider UNI-UNI OAM maintenance entity, OAM mechanisms provided should ensure (as far as reasonably practicable) that customers should not have to detect failures. It is therefore necessary that defects associated with this entity are detected and notified automatically by the service provider.
5. The following anomalies should be automatically detected and corresponding defect states, with well defined entry/exit criteria and appropriate consequent actions should be defined:
   - simple loss of connectivity
   - unintended self-replication (e.g., looping, denial of service (DoS) attack).
   - lost frames
   - errored frames
   - misinserted frames (e.g., misinsertion of a frame into unintended VLANs)

6. OAM functions should detect anomalies which impacts the transport of user ETH flows in the network. Ethernet OAM frames should be forwarded on the same route as the user ETH flow is forwarded.
7. A defect event in a given layer network should not cause multiple alarm events to be raised, nor cause unnecessary corrective actions to be taken, in any higher layer level client layer networks. The Ethernet layer network should support alarm suppression for server layer sourced defects whose presence have been communicated by forward defect indication means. Ethernet layer network should support forward defect indication capability.
8. OAM functions should be simple and easily configured (ideally automatically) to allow efficient scaling to large network sizes.
9. The use of Ethernet OAM functions should be optional for the operator. Network operators should be able to choose which OAM functions to use and which flows they apply them to.
10. Ethernet OAM functions should be backward compatible. Ethernet OAM frames should be defined such that Ethernet switches that do not support such functions will be able to either silently discard the OAM frames addressed to an ETH flow termination point in this switch, or let OAM frames pass through transparently if not addressed to an ETH flow termination point in this switch without disturbing the user traffic or causing unnecessary actions.
11. There should be a capability to measure availability and network performance of a maintenance entity. Since network performance metrics are only meaningful when the Ethernet flow is in the available state, then the entry/exit of the available state and all appropriate consequent action (like the starting/stopping of network performance metric aggregation) should be specified.
12. The functionality of an Ethernet OAM flow should not be dependent on any specific server or client-layer network. This is architecturally critical to ensure that layer networks can evolve (or new/old layer networks can be added/removed) without impacting other layer networks.
13. The functionality of an Ethernet OAM flow should be sufficiently independent of any specific control-plane such that any changes in the control plane do not impose changes in user-plane OAM (including the case of no control-plane). Like the previous requirement, this is also architecturally critical to ensure that user-plane and control-plane protocols can evolve (or new/old control-plane protocols added/removed) without impacting each other.
14. Connectivity status assessment should not be dependent on the dynamic behaviour of customer traffic.
15. The OAM function should perform reliably even under degraded link conditions, e.g., error events.
16. If the UNI-to-UNI Ethernet flow is being transported over networks belonging to different operators, the one that offers the service to the customer should be aware of a service fault even if the fault and detection point are located in the network of another operator.
17. The “down” time of the service should be able to be recorded for performance and availability measurements.

9. Requirements for maintenance entities (MEs)

The reference models indicate traffic flows. OAM flows can be inserted and extracted at the reference points, namely the flow points and termination flow points of the reference models. The OAM flows represent the maintenance entities. The following maintenance entities are defined:

- Customer UNI-UNI maintenance entity in the ETH layer network between reference points on the customer side of the UNI.

- Provider UNI-UNI maintenance entity in the ETH layer network between reference points on the provider side of the UNI
- Segment OAM maintenance entity between flow points. A segment may be:
    - Between flow points on the boundary of a providers network
    - Between flow points on the boundaries of two adjacent provider networks
    - Between any flow points as required
- ETY link connection OAM based on IEEE 802.3ah (see Appendix II)

10. Required OAM functions

10.1 Point-to-point services

Necessary OAM functions for point-to-point Ethernet services include:

- Continuous connectivity check (CC)
- Alarm suppression function
- Intrusive Loopback and non-intrusive Loopback
- Path trace
- Discovery
- Performance monitoring
- Survivability function (e.g., protection switching, restoration, etc.)

10.2 Multipoint-to-multipoint services

- Continuous connectivity check (CC)
- Alarm suppression function
- Non-intrusive Loopback
- Path trace
- Discovery
- Performance monitoring
- Survivability function (e.g., protection switching, restoration, etc.)

11 Security aspects

The following items are related to security aspects:

- item 5 of clause 8 and
- item 5 of clause 9.

In addition, the following items should be considered

1) OAM should have mechanisms that make sure customers are not able to trigger any service provider/network operator OAM function.
2) OAM should have mechanisms that make sure service provider/network operator's OAM flows, which are meant for their internal use, are confined within their networks and do not leak out to customers or other service providers/ network operators.
3) OAM should have mechanisms to detect mis-delivered flows.

Appendix I

Examples of the protocol stack reference model

The following figure depicts examples of the protocol stack reference model for Ethernet services. This reference model can be used to show the traffic flow through different protocol stack layers for the following types of traffic:

- User data traffic
- User control traffic (such as user BPDUs, user-to-user OAM, UNI OAM etc.)
- Provider control traffic (e.g., Provider OAM, Provider BPDUs, Provider GARP etc.)

As it can be seen from the figure, Ethernet MAC sub-layer can reside on top of a variety transport layers (e.g., referred to in the figure as Foo). Foo transport layer can itself consist of one or more network layers.

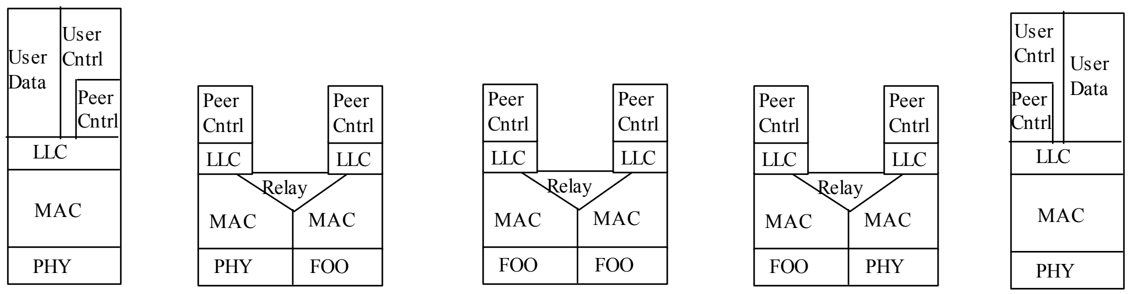

Figure I.1 Protocol Stack Reference Model

User data traffic is injected but the user stations (endpoints) and with respect to the intermediate nodes it stays at the MAC sub-layer and does not go through any sub-layer above it (e.g., doesn't go through LLC or any layer above it).

User control traffic can be broken into two categories: a) user-to-user control traffic and b) user-to-provider control traffic. The first category of user control traffic is seen as user data by intermediate nodes and thus it stays within the MAC sub-layer with respect to the provider nodes. Some examples for this category of traffic are user OAM, user BPDU messages, and user GARP messages. The second category of user control traffic (user-to-provider control traffic), is intercepted by the first provider node and it gets passed to the control plane for processing. Some examples of user-to-provider control traffic are UNI OAM, LACP, 802.1X, and 802.3X.

Provider control traffic is the control traffic between different provider nodes. Depending on the type of the traffic, it can either stay at the MAC sub-layer with respect to the provider intermediate nodes or it can be passed to the upper layers for further processing. Some examples of this kind of traffic are provider's BPDUs, provider's GARP message, and provider's OAM messages.

Appendix II

Bibliography (1)

IEEE Draft P802.3ahTM/D1.414, Draft Amendment to Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method and physical layer specifications – Media Access Control Parameters, Physical Layers and Management Parameters for subscriber access networks

Appendix III

Service description

III.1 Ethernet service

An Ethernet service defines a set of characteristics for an Ethernet flow domain.

III.2 Private service

A private service is characterised by:

- One or more ETH links within the transport network are allocated to transport the ETH_CI of a single customer's service instance.
- These ETH links are supported by COCS or COPS with a defined bandwidth trail (1:1 relationship).

The ETH_CI in a private service either doesn't compete for bandwidth (Ethernet private line/LAN).

III.3 Virtual private service

A virtual private service is characterised by:

- One or more ETH links within the transport network are allocated to transport the ETH_CI of multiple service instances (N:1 relationship), and these ETH links are supported by COCS or COPS CBR trails.
- One or more ETH links within the transport network are allocated to transport the ETH_CI of a single service instance, and these ETH links are supported by COPS (non-CBR) or CLPS trails (1:1 relationship). Multiple of those COPS (non-CBR) or CLPS trails are supported by server layer COCS trails (N:1 relationship).

The ETH_CI in a virtual private service competes for bandwidth with ETH_CI from another service instance of the network (Ethernet virtual private line/LAN).

Note that if the link resources allocated are sufficient then the EVPL service will behave in a way that is similar to EPL.

III.4 Line service

A line service is characterized by:

- One ETH link within the transport network is allocated to transport the ETH_CI of one customer service instance (1:1 relationship), between at most two flow points.
- No additional ETH links can be added to the service

III.5 LAN service

A LAN service is characterized by:

- One (or more) ETH link(s) within the transport network is allocated to transport the ETH_CI of one customer (1:N relationship), between at least two flow points.
- Additional ETH links can be added/deleted to/from this service

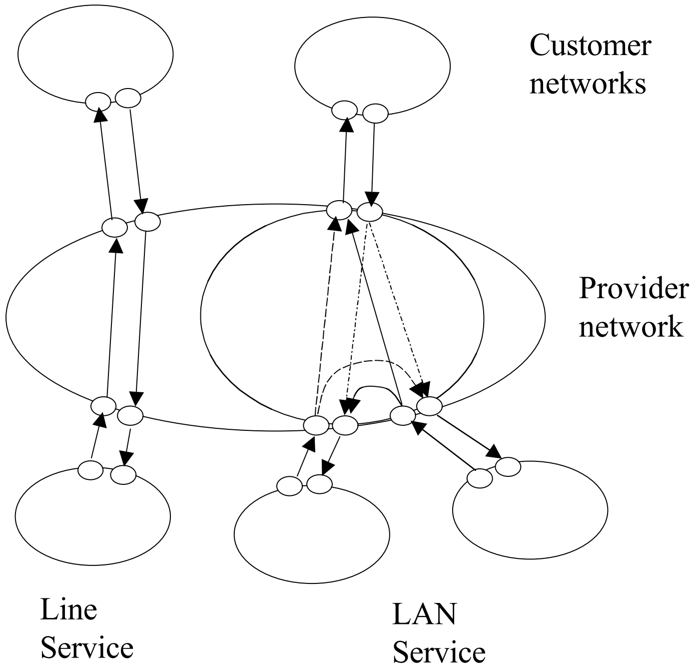

Figure III.1/G.17ethreq – Line vs LAN service

Appendix IV

Bibliography (2)

ITU-T Draft Recommendation G.ethna, Ethernet over Transport Network Architecture

ITU-T Draft Recommendation G.ethsrv, Ethernet over Transport – Ethernet Service Characteristics