Network Working Group
Internet Draft
Expiration Date: September 2001

Hirokazu Ishimatsu
Shinya Tanaka
Japan Telecom

Zhi-Wei Lin
Yangguang Xu
Lucent Technologies

Juergen Heiles
Siemens AG

Yang Cao
Sycamore Networks

March 2001

Security Requirements for Lightpath Services

draft-ishimatsu-ipo-lightpath-scrty-00.txt

Status of this Memo

Abstract

Many efforts have been introduced to achieve lightpath services using optical cross-connects (OXCs). This document surveys security prerequisites to be considered when lightpath services are offered to users.

Section 5 discussed prerequisites for lightpath services. Section 6 discussed required actions for the prerequisites that are described

in section 5. Section 7 discussed security requirements for possible business models of lightpath services.

Table of Contents

1. Specification

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

2. Acronyms

ASTN	Automatic switched Transport Network
BIP	Bit Interleaved Parity
CPE	Customer Premises Equipment
CRC	Cyclic Redundancy Check
DoS	Denial of Service
FEC	Forward Error Correction
ISP	Internet Service Provider
NMS	Network Management System
OTN	Optical Transport Network
OXC	Optical Cross-connect
SLA	Service Level Agreement

3. Introduction

In these days, traffic demand has been increasing rapidly because of the explosive spread of the internet and telecommunication has been getting more and more essential to our daily life. Under such a circumstance, it is obvious that the layer 1 optical network, on which data is carried, is important as the backbone of telecommunication. Therefore layer 1 optical network should be reliable and secured in order to function as the necessary infrastructure.

In addition to that, it is often said that generation shift in layer

1 optical network is necessary to deal with the explosion of traffic demand. One of such next generation layer 1 network is ASTN (Automatic Switched Transport Network)[ITU-ASTN]. ASTN is able to supply on-demand lightpath provisioning by users and offer users

lightpath services. This means the layer 1 connection setup is controlled by users. Therefore it needs very severe accounting, call acceptance, billing, etc.

The remainder of this draft claims security requirements for lightpath services.

4.Lightpath services

Lightpath services are to offer users end-to-end connectivity. These connectivity may be in the form of SONET/SDH rate services, emerging OTN-based services, and transparent wavelength services.

5. Security prerequisites for lightpath services

The following items are related to the security aspect of lightpath services

5.1 Confidentiality

A lightpath should be disclosed only to authorized persons, entities and processes at authorized time and in the authorized manner.

5.2 Integrity

The characteristics of data and information that a lightpath carries should be accurate and complete. While a lightpath is offered, the presentation of accuracy and completeness should be kept. This characteristic is inherent to the network design of each service provider.

5.3 Serviceability

A lightpath should be available on demand by an authorized entity. An authorized entity should be able to request service for a light path on demand.

5.4 Accountability

It should be ensured that the billable actions of an entity can be allocatable to the correct account.

5.5 Authenticity

It should be ensured that the identity of a subject or resource is the one claimed authenticity. Authenticity applies to entities such as users, processes, systems and information.

5.6 Reliability/Availability

Intended behavior and results should be consistent with that agreed between the authorized entity and the service provider.

5.7 Ethics

Lightpath services should be provided and used in such a manner that the rights and legitimate interests of others are respected.

6. Required actions for prerequisites

6.1 Confidentiality

lightpaths on each link are isolated by wavelengths. Therefore confidentiality of each lightpath is naturally kept. Encryption of data at application level can add additional confidentiality to a lightpath. As the connection-oriented world does not have issues with merging of packets, user traffic isolation and thus confidentiality mechanisms are not as critical. However, misconnection may still occur due to defected cross-connects by equipment fault or miss-destination by human error; thus a mechanism to ensure no misconnection is needed. One example of this mechanism may be making lightpath requestors send their IDs to lightpath receivers and allowing lightpath receivers to decide if they accept the lightpath by the ID sent.

6.2 Integrity

Perfect integrity is a trade-off against infinite-cost. Integrity requirements should be quantified, and those quantified requirements should be kept less than the thresholds set by a lightpath service provider in practice.

Some performance monitoring scheme should be done in order to quantify integrity requirements. At wavelength level, performance can be monitored by analog measurements such as S/N, toned modulation monitor[TMM], and etc. In the case of transparent end-to-end lightpath service where optical signal is not terminated digitally within a service provider's domain, analog type of measurements should be performed. At upper layers, where optical signal is terminated digitally, Digital performance monitoring, such as FEC, BIP, CRC and etc., can be done. For the emerging OTN-based network, the tandem connection monitoring may be used to provide flexible monitoring points across multiple sub-networks. Multiple performance monitoring schemes at multiple layers may be needed to keep integrity of data. Choice of performance monitoring scheme depends on service provider's policy and technical constraints.

6.3 Serviceability

Any lightpath service provider cannot guarantee 100% serviceability since denial of service (DoS) can be occurred by network failures, customer premises equipment (CPE) failures, shortage of network resource, and etc.. Practical actions that service providers can do is to set an objective percentage of serviceability and try to keep that percentage as possible as they can. An objective percentage of serviceability may be contracted between a lightparh service provider and its customer as a single item, or may be included in the concept of availability. The way to show customers serviceability depends on service provider's policy.

In order to maintain serviceability, DoS should be considered. DoS is categorized into two. One is the DoS caused by the network side, for example, network equipment failures, shortage of network resource, and etc.. The other is the DoS caused by the user side, for example, CPE failures, destined end points being in use. From an SLA perspective, the network side DoS and the user side DoS should be distinguishable.

As mentioned above, one possible cause of the network side DoS is shortage of network resource. If network resource is left little and someone tries to create a new lightpath, DoS might occur. To prevent this situation, network resource should be always monitored and some proactive action should be taken (for example, NMS alerts shortage of network resource when remained resource becomes less than 10%).

Another aspect of DoS is DoS attack. DoS attack means that a malicious person continue to create a light path destined to some end point so that other persons cannot create a lightpath to that end point. In order to avoid malicious persons, users of lightpath services should be identified, authorized and managed by a service provider.

6.4 Accountability

In order to keep accountability, entities should be identified whenever they use lightpath services. In addition usage history of each entity's billable actions should be recorded.

6.5 Authenticity

To ensure authenticity, passwords, digital signatures, biometrics and etc. should be used between entities and a service provider.

6.6 Reliability/Availability

To make lightpath services reliable, MTBF and MTTR of the total lightpath system should be calculated, and managed by each service provider.

6.7 Ethics

In order to protect the rights and legitimate interests of others, appropriate rules should be applied to users of lightpath services. Those rules may be on contracts.

7. Security requirements for business models of lightpath services

As mentioned in [ASON-UNI], layer 1 carriers lease a point-to-point service to customers. Layer 1 carriers cannot make any assumption about the business of their customers. A lightpath consists of a set of wavelength links, and links are connected with OXCs.

From customers' view, customers construct user networks on the layer 1 network which is leased from layer 1 carriers. Customers can construct any type of user network and can provide any type of services.

The lightpath service is a layer 1 service, not layer 2 or above. So, customer can do business using any type of networks including not only packet networks but also circuit networks.

The path of light is able to be changed dynamically with some signalling protocols.

Followings are some major business models using lightpath services;

(a) ISP owning all layer 1 infrastructure
ISP provides client service on its own layer 1 network. The ISP is its own layer 1 carrier and uses lightpath services for itself. Therefore there is no security issue between the layer 1 carrier and the ISP because they are the same entity. However internal security issue in the carrier exists. Only authorized persons should be able to change the configuration of layer 1 network.

(b) ISP leasing partial or whole layer 1 infrastructure
ISP provides client service, but leases partial or whole layer 1 network from layer 1 carriers. There are security issues between the layer 1 carrier and the ISP. Prior to offering the ISP a lightpath, the ISP should be identified and authorized by the layer 1 carrier. Any billable deeds of the ISP should be accountable while the ISP uses a lightpath. On the other hand, the layer 1 carrier should keep confidentiality and integrity of the ISP's data. the layer 1 infrastructure should be reliable as well.

(c) Retailer or wholesaler for multi-services
The Customer (retailer/wholesaler) leases layer 1 infrastructure from layer 1 carriers and again sells it to others. Between the layer 1 carrier and its customer, the same security issues as in case (b) exist. Between the customer and the customer's customer, certain security issues apply. However this relation ship is out of the scope.

(d) Carriers carrier, or bandwidth broker
The customer leases layer 1 infrastructure from layer 1 carriers (carriers carrier) and uses it as its layer 1 infrastructure. The

customer network is likely to be a circuit network. The same security issues as in case (b) exist.

8. Acknowledgment

The authors would like to thank Susumu Yoneda, Eve Varma, John Ellson, and Siva Sankaranarayanan for their helpful comments on this work.

9. References

[ITU-ASTN] ITU-T SG13 Draft Recommendation "G.astn; Architecture for the Automatic Switched Transport Network", work in progress, November 2000.

[TMM] Ivan P. Kaminow et al., "OPTICAL FIBER TELECOMMUNICATIONS III A", p.280, 1997.

[ASON-UNI] Curtis Brownmiller et al., "Requirements on the ASON UNI", ANSI T1X1.5/2000-194, October 2000.

10. Security Considerations

This document discussed general security requirements for lightpath services. In each prerequisite, further study in needed in order to implement secured lighpath services practically. It should be noted that the listed security requirements apply to all kinds of automatic switched layer 1 services offered to users, not only to lightpath services (e.g. SDH/SONET TDM services).

11. Authors' Addresses

Hirokazu Ishimatsu
Japan Telecom Co., Ltd.
2-9-1 Hatchobori, Chuo-ku, Tokyo 104-0032 Japan
Phone: +81 3 5540 8493
Fax: +81 3 5540 8485
EMail: hirokazu@japan-telecom.co.jp

Shinya Tanaka
Japan Telecom Co., Ltd.
2-9-1 Hatchobori, Chuo-ku, Tokyo 104-0032 Japan
Phone: +81 3 5540 8493
Fax: +81 3 5540 8485
EMail: tnk@japan-telecom.co.jp

Zhi-Wei Lin
Lucent Technologies
101 Crawfords Corner Red, Room 3C-512, Holmdel, NJ 07733-3030, USA
Phone: +1 731 949 5141

Fax: +1 731 949 3210
EMail: zwlin@lucent.com

Yangguang Xu
Lucent Technologies
21-2A41, 1600 Osgood Street, North Andover, MA 01845, USA
Phone: +1 978 960 6105
Fax: +1 978 960 6329
Email: xuyg@lucent.com

Juergen Heiles
Siemens AG
ICN TR ON BS, Munich, Germany
Phone: +49 89 722 48664
Fax: +49 89 722 31508
EMail: juergen.heiles@icn.siemens.de

Yang Cao
Sycamore Networks
10 Elizabeth Dr., Chelmsford, MA 01824, USA
Phone: +1 978 367 2518
Fax: +1 978 256 4203
EMail: yang.cao@sycamorenet.com