International Telecommunication Union

ITU-T G.7714.1/Y.1705.1

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Amendment 1
(02/2006)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

Data over Transport – Generic aspects – Transport network control aspects

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

Internet protocol aspects – Operation, administration and maintenance

---

Protocol for automatic discovery in SDH and OTN networks

Amendment 1: New Appendix VI – Usage of the different discovery mechanisms

ITU-T Recommendation G.7714.1/Y.1705.1 (2003) – Amendment 1

ITU-T

International Telecommunication Union

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
General	G.7000–G.7099
Transport network control aspects	**G.7700–G.7799**
ETHERNET OVER TRANSPORT ASPECTS	G.8000–G.8999
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

ITU-T Recommendation G.7714.1/Y.1705.1

Protocol for automatic discovery in SDH and OTN networks

Amendment 1

New Appendix VI – Usage of the different discovery mechanisms

Summary

This new Appendix VI provides clarification of the network scenarios under which the various discovery mechanisms described in the main body of this Recommendation may be utilized, including guidelines for usage of mechanisms and procedures as well as potential associated implications.

Source

Amendment 1 to ITU-T Recommendation G.7714.1/Y.1705.1 (2003) was agreed on 17 February 2006 by ITU-T Study Group 15 (2005-2008).

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

CONTENTS

ITU-T Recommendation G.7714.1/Y.1705.1

Protocol for automatic discovery in SDH and OTN networks

Amendment 1

New Appendix VI – Usage of the different discovery mechanisms

VI.1 Introduction

This appendix provides clarification of the network scenarios under which the various discovery mechanisms described in the main body of this Recommendation may be utilized, including guidelines for usage of mechanisms and procedures as well as potential associated implications.

VI.2 Categories of Type 1 layer adjacency discovery use cases

The auto-discovery use cases can be subdivided into the categories depicted in Figure VI.1, i.e., Pre-Service, In-Service and Out-of-Service. Within the context of this Recommendation the terms: Pre-Service, In-Service and Out-of-Service are defined as follows:

Pre-Service: The entity that is in a pre-service state is the trail whose associated client link connections have not been allocated. As a consequence, operations will not impact any traffic. Pre-service includes scenarios where discovery is done immediately after a fault has been cleared and before service is considered restored (e.g., during soaking interval).

In-Service: The entity that is in an in-service state is the trail whose associated client link connections have been allocated (one or more).

Out-of-Service: The entity that is in an out-of-service state is the trail where all allocated client link connections are in a failed or non-usable state.

This appendix only addresses auto-discovery use cases where the applied auto-discovery mechanism may cause some behavioural problems in the network, i.e., 'in-service' case. The 'pre-service' and 'out-of-service' use cases, drawn with dotted lines in Figure VI.1, are not further discussed. Moreover, Type 2 LAD is also not considered because the link connections (LCs) cannot be in service (i.e., carry traffic) at the same time when Type 2 LAD is applied (see ITU-T Rec. G.7714/Y.1705 for the definition of Type 1 and Type 2 LAD).

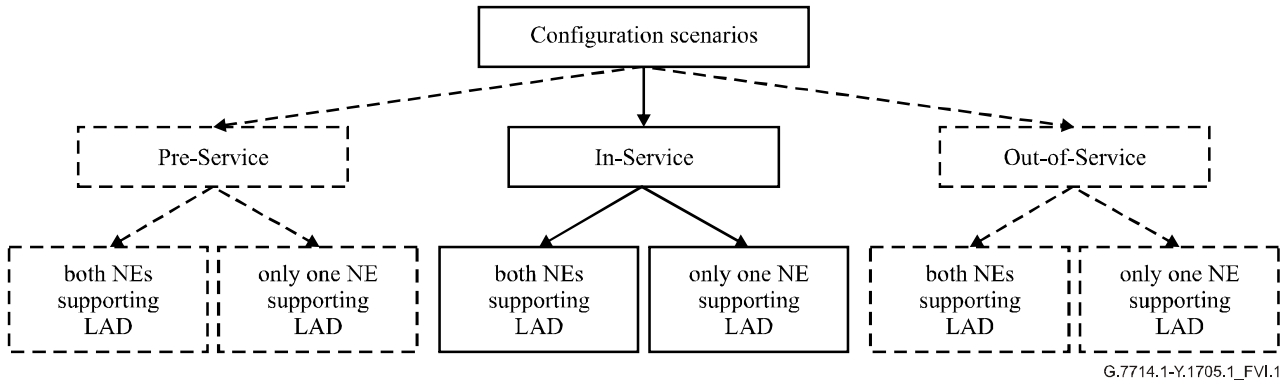

Figure VI.1/G.7714.1/Y.1705.1 – Categorization of discovery scenarios

VI.3 Use cases and scenarios

The various use cases where Type 1 layer adjacency auto-discovery (LAD) can be applied are described in this clause and guidelines are provided in VI.4 that explain how discovery can be accomplished based on the constraints imposed by the different scenarios. As specified in the main body of this Recommendation, it is assumed that there is always congruency between the signal being used for layer adjacency discovery and the entity being discovered. In describing the various scenarios we broadly distinguish between two cases:

a) the case where all the Network Elements (NEs) are auto-discovery capable; and

b) the case where some of the NEs within the network are not auto-discovery capable.

VI.3.1 All NEs are auto-discovery capable (ubiquitous deployment)

Ubiquitous deployment means that all NEs are auto-discovery capable and it is assumed that all involved NEs support LAD as defined in ITU-T Rec. G.7714/Y.1705 and in the main body of this Recommendation respectively. For this subset of cases one can use either trail-trace-based or ECC-based discovery messages, provided all the NEs agree on a specific common mechanism.

VI.3.2 All NEs are not auto-discovery capable

In this case some of the NEs within the network are assumed to be unable to understand the auto-discovery messages (e.g., legacy equipment). We consider two scenario classes for the case where auto-discovery is being performed at a particular layer between the two NEs that represent the endpoints of that layer:

- scenarios where both NEs are LAD-capable;
- scenarios where one of the two NEs does not support LAD.

VI.3.2.1 Auto-discovery between LAD-capable NEs

As described in ITU-T Rec. G.7714/Y.1705, the LAD process requires that two NEs that are performing layer adjacency discovery must be immediate neighbors with respect to the layer where discovery is taking place (e.g., for SDH at RS, MS, HO or LO path layer). It is not possible, for example, to perform LAD based on using the section trail trace (J0), RS DCCs, or MS DCCs when there is a NE between the two LAD-capable NEs that does not support LAD and terminates the regenerator and multiplex sections (RS and MS). Therefore, it is only possible to perform LAD at the path layer for such a configuration and the HOVC path-trace (J1)-based discovery method may have to be used. This is illustrated in Figure VI.2. It is also possible for the network management system to run the HO path layer LAD process by proxy for the NEs, as depicted in Figure VI.3.

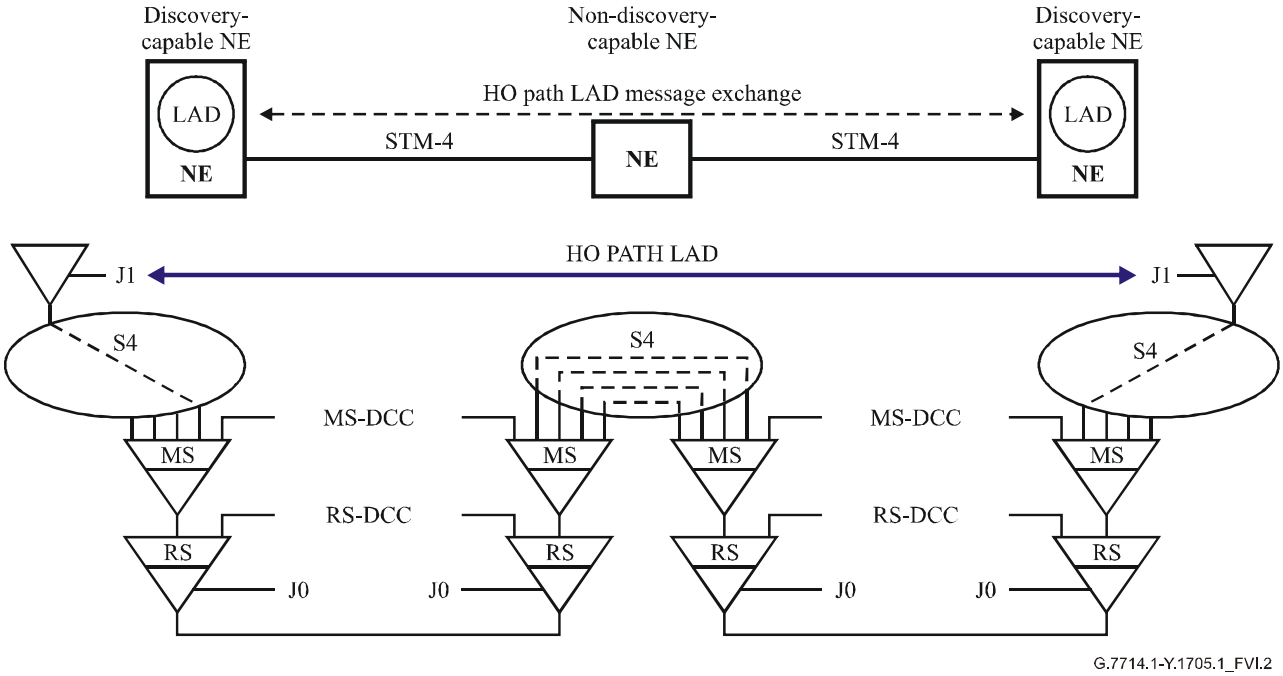

Figure VI.2/G.7714.1/Y.1705.1 – Immediate discovery-capable neighbours at HO path layer – LAD done by NEs

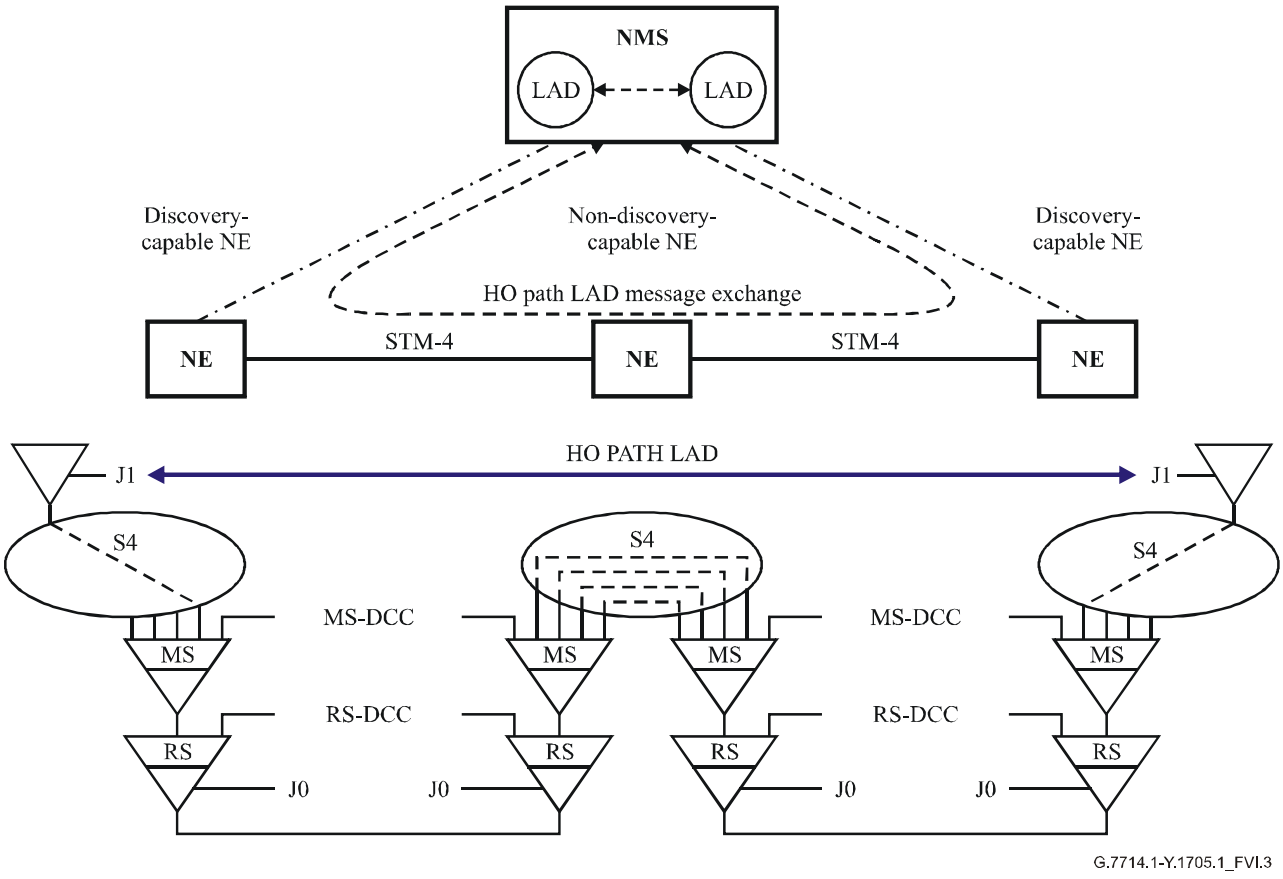

Figure VI.3/G.7714.1/Y.1705.1 – Immediate discovery-capable neighbours at HO path layer – LAD done by NMS

VI.3.2.2 Auto-discovery between a LAD-capable NE and a non-LAD-capable NE

In this case we make the assumption that the non-LAD-capable NE terminates the layer being discovered (see Figure VI.4). In such a case, layer adjacency discovery cannot be performed at that specific layer since the discovery messages sent by the LAD-capable NE are not understood by the non-LAD-capable NE. In such a scenario it is important that the non-LAD-capable NE does not generate alarms and, more important, not perform consequent actions that could unnecessarily disrupt service. One possible means for the network operator to avoid such alarms and consequent actions is to disable the transmission of discovery messages at the LAD-capable NE or to obey the guidelines as described in VI.4.

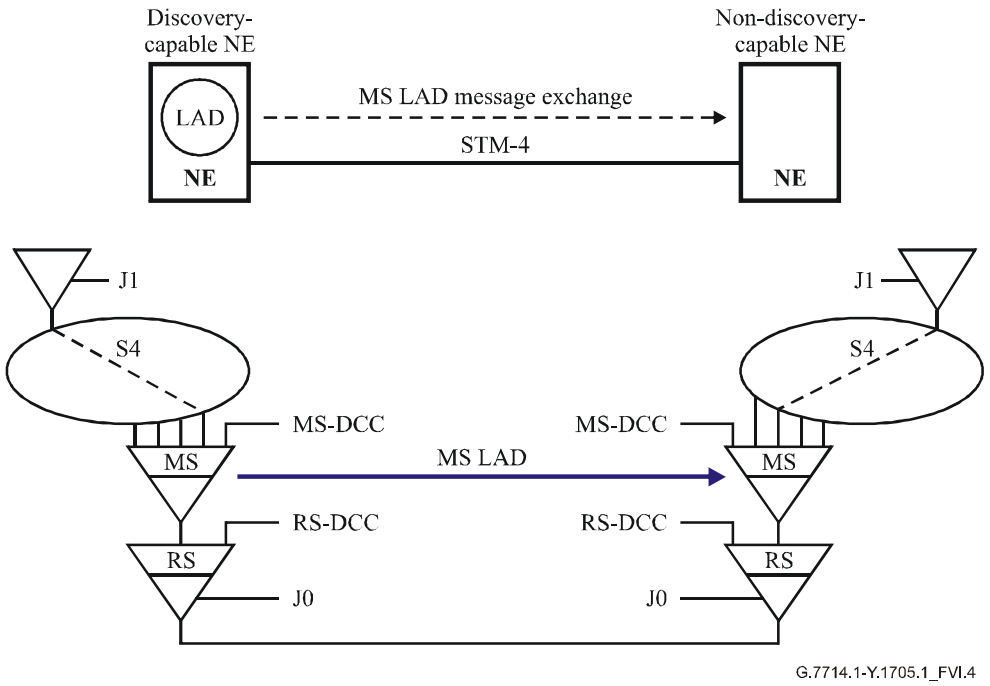

Figure VI.4/G.7714.1/Y.1705.1 – Discovery-capable NE trying to discover a non-discovery-capable NE

VI.4 Guidelines for mechanisms and procedures

This clause provides guidelines on the usage of the trail trace (J0, J1 and J2) and ECC (MS DCC or RS DCC) mechanisms for LAD for the various use cases and scenarios described in VI.3.

VI.4.1 ECC-based LAD

Auto-discovery using the DCC is a viable option when the DCC is available on the STM-n interface that needs to be discovered. The DCC provides a packet-based interface; its use for LAD is not affected by the service state (in-service, out-of-service, pre-service) of the given STM-n interface it is associated with. The LAD process making use of the DCC does not have any impact on the traffic on the STM-n interface. However, there are a number of use cases where the DCC may not be sufficient for LAD, based on DCC availability given the DCN deployment scenarios described below.

VI.4.1.1 DCN deployment scenarios impacting the availability of DCCs

There are two scenarios which affect the deployment of DCC-based LAD messages:

a) No DCC connectivity (e.g., Central Office LAN supporting the DCN).

In this scenario, there is no DCC connectivity between the ADMs and the DXC in the Central Office (CO). Instead, as shown in Figure VI.5, the CO LAN is used to carry the

management communication between the Network Elements in the CO. Although there is connectivity (e.g., STM-n) between the ADMs and the DXC, the management communication does not follow the same topology as these optical connections that contain the DCCs. The DXC could be used to inter-connect low-speed optical interfaces between ADMs within a CO – and therefore the DCC on these low-speed optical interfaces are not available for auto-discovery.

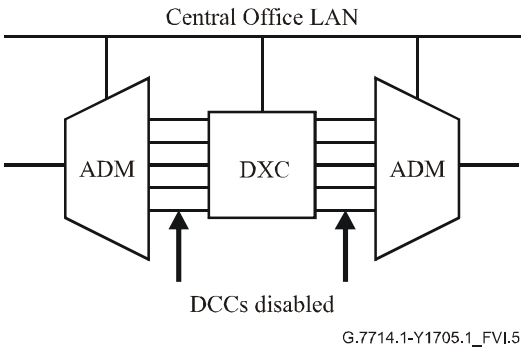

Figure VI.5/G.7714.1/Y.1705.1 – Central Office with disabled DCC connectivity

b) Limited DCC availability or DCCs not enabled on all parallel interfaces between two NEs.

In this scenario, as depicted in Figure VI.6, there may be limited or no DCC availability for management communication between Network Elements – e.g., due to disabling of DCCs, or limited DCC resources. This could occur between multiple carriers, at a customer-to-carrier interface, or where only out-of-band connectivity is available between the NEs – and therefore the DCC is not available for auto-discovery. It is also possible that there are multiple parallel optical interfaces connecting the two NEs. However, the DCCs on only one link or a small subset of links may be enabled. This may be the case for several administrative reasons, e.g.:

- DCC processing not supported for all interfaces;
- configuration decision (e.g., in case of multiple parallel links, the DCCs are only enabled on some of them since the capacity of a single DCC may be sufficient for management communication between the two NEs);
- policy decisions in the case of connectivity of NEs between different administrative domains.

In all these cases it may not be possible to perform LAD on every link using DCC because some of the links may not have the DCC enabled.

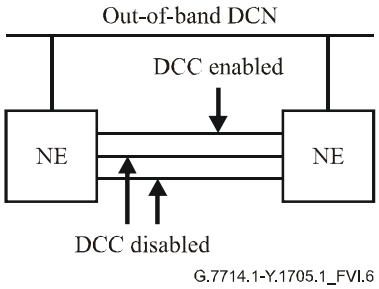

Figure VI.6/G.7714.1/Y.1705.1 – Central Office with DCC enabled on only one link or using an out-of-band DCN

VI.4.2 Trail-trace-based LAD (e.g., using J0, J1 and J2 bytes)

The trail-trace bytes can be utilized for Type 1 LAD, which allows one to infer the client layer LCs from the discovered server layer trail as depicted in Figure 1/G.7714.1/Y.1705.1. Depending on the configuration of the trail termination functions involved in the LAD process, some behavioural issues could arise. In particular, traffic impact has to be avoided while the interfaces are in the 'in-service' state and are carrying traffic. These scenarios where such behavioural issues might occur are addressed in this clause and are discussed in detail below. Moreover, application and configuration guidelines are provided in order to avoid traffic impacts.

VI.4.2.1 Pre-service and out-of-service cases

The use of the trail-trace bytes for LAD does not cause any behavioural issues as long as the interface is in a pre-service or out-of-service state because no traffic is being carried over it.

VI.4.2.2 In-service cases

It should be noted that Discovery Enabling/Disabling capability is provided at each link end at a specific layer independent of the remote end. Note that the discovery process is only permitted to change (provision) the TTI when the discovery process is enabled.

Usage of the trail-trace bytes as defined in ITU-T Rec. G.707/Y.1322 allow transmission and reception of Access Point Identifiers (APIs) so that the receiving terminal can verify its continued connection to the intended transmitter. The formats used for LAD are different to formats commonly used for pre-existing applications. It is expected that new equipment should be able to recognize this usage. In order to avoid undesired trace identifier mismatch (TIM) alarms for some legacy equipment, the discovery-capable NE should not change the TTI (i.e., should disable auto-discovery) at its trail end when there is a non-discovery capable NE at the other end. Discovery should also be disabled when the trail includes monitors that are monitoring the TTI and are unable to distinguish discovery messages.

Note that the discovery process could be performed in a management system, thereby making an NE discovery capable.

For some existing equipment, use of the trail-trace bytes for discovery may raise alarms, and if the consequent action (AIS insertion) is not disabled, may cause traffic loss. Therefore, trail termination points that allow trail-trace-based discovery should set TIMAISdis=true to prevent the insertion of AIS when the Trail-Trace Identifier does not match. In national networks where TIMAISdis is required to be always false (see ITU-T Rec. G.806), trail-trace-based discovery should not be performed.

If dTIM detection is enabled, the LAD process can use the MI_cTIM as a notification that the trail trace has changed (MI_AcTI).

Non-intrusive monitoring

Non-intrusive monitor functions (see ITU-T Rec. G.783) may observe the trail trace. If the non-intrusive monitor function is not aware of the use of trail-trace for discovery, unexpected changes in trail trace information (TTI) will be observed.

VI.4.3 Inter-carrier, user-provider implications

The LAD process can be enabled or disabled on each interface. This allows the network operators to configure the interfaces according to their policy.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	**Y.1700–Y.1799**
Charging	Y.1800–Y.1899
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Numbering, naming and addressing	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	**Transmission systems and media, digital systems and networks**
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects and next-generation networks**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2006