

I n t e r n a t i o n a l T e l e c o m m u n i c a t i o n U n i o n

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 10

(01/2014)

SERIES X: DATA NETWORKS, OPEN SYSTEM
COMMUNICATIONS AND SECURITY

ITU-T X.1205 – Supplement on usability of network traceback

ITU-T X-series Recommendations – Supplement 10

ITU-T

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589
CLOUD COMPUTING SECURITY	
Overview of cloud computing security	X.1600–X.1601
Cloud computing security design	X.1602–X.1639
Cloud computing security best practices and guidelines	X.1640–X.1659
Cloud computing security implementation	X.1660–X.1679
Other cloud computing security	X.1680–X.1699

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

Supplement 10 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on usability of network traceback

Summary

Supplement 10 to the ITU-T X-series of Recommendations provides an overview of traceback for responsive measures to certain network issues within a single or a more complex array of service providers. Traceback may assist in discovering ingress points, paths, partial paths or sources of problematic network events. This information may aid service providers in mitigating such events.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T X Suppl. 10	2011-09-02	17	11.1002/1000/11341
2.0	ITU-T X Suppl. 10	2014-01-24	17	11.1002/1000/12160

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). 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 publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication 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 publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication 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 publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2014

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

		Page
1	Scope.....	1
2	References.....	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this supplement.....	1
4	Abbreviations and acronyms	1
5	Conventions	2
6	Traceback introduction	2
7	Possible traceback capabilities in networks.....	2
	7.1 Source identification.....	2
	7.2 Ingress point identification	2
	7.3 Partial path identification	2
8	Potential applications of traceback	3
	8.1 Application to DDoS attacks	3
	8.2 Application to misconfiguration issues	4
	8.3 Application to routing issues	4
	Appendix I – Overview of traceback mechanisms research	5
	I.1 Abbreviations and acronyms	5
	I.2 Classification of traceback mechanisms.....	5
	I.3 IP layer traceback mechanisms	7
	I.4 Comparison of traceback mechanisms	11
	Appendix II – Comparison of traceback mechanisms based on criteria and taxonomy	13
	Bibliography.....	14

Copyright International Telecommunication Union/ITU Telecommunication Sector
Provided by IHS Markit under license with ITU-T
No reproduction or networking permitted without license from IHS

Supplement 10 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on usability of network traceback

1 Scope

This Supplement provides an overview of traceback capabilities that may be useful in responding to network incidents where some knowledge of the source(s) of those incidents is necessary for effective cybersecurity responsive measures. It includes descriptions and usability considerations of the traceback.

Traceback, as described in this supplement, may be in conflict with laws and regulation (e.g., secrecy of telecommunications or data protection and/or privacy) in some countries or regions, and therefore cannot be applied in those countries or regions. Implementers and users of the described mechanisms shall comply with all applicable national and regional laws, regulations and policies.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

This Supplement uses the following terms defined elsewhere:

3.1.1 domain [b-ITU-T M.3010]: A set of managed resources subject to a common management policy.

3.1.2 event [b-ITU-T M.2140]: An instantaneous occurrence that changes the global status of an object. This status change may be persistent or temporary, allowing for surveillance, monitoring, and performance measurement functionality, etc. Events may or may not generate reports, may be spontaneous or planned, may trigger other events, or may be triggered by one or more other events.

3.2 Terms defined in this supplement

This Supplement defines the following term:

3.2.1 traceback: A technique used to discover technical information concerning the ingress points, paths, partial paths or sources of a packet or packets causing a problematic network event, generally for the purposes of applying mitigation measures.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ADSL	Asymmetric Digital Subscriber Line
DDoS	Distributed Denial of Service
IP	Internet Protocol
IPv4	IP version 4
IPv6	IP version 6
NAT	Network Address Translation

5 Conventions

None.

6 Traceback introduction

IP-based incidents, especially attacks on the network infrastructure, have increased dramatically in number and complexity. End users, service providers and network operators are all adversely affected by such attacks.

In order to deal with these attacks, traceback was developed, and it has now evolved for several years. Traceback attempts to discover information about the attack source(s) for the purpose of pursuing remediation measures. For example, when a distributed denial of service (DDoS) attack occurs, network providers along the attack path may be able to detect and mitigate DDoS traffic at the ingress points with the help of traceback.

Traceback has evolved from network operational tools that have existed for a long time and it has been included as part of the network management systems and products. Indeed, the basic traceroute tool is provided with almost every computer and network element operating system. When combined with directory systems such as WHOIS [b-IETF RFC 3912], some basic traceback capabilities can be created. These, and other techniques, are examples of the type of traceback used by service providers. This Supplement does not describe such techniques but rather the usability considerations of traceback.

Clauses 7 and 8 describe the overview and usability considerations of traceback.

7 Possible traceback capabilities in networks

7.1 Source identification

A service provider seeking to uncover the source of a problematic network event may use traceback immediately after the incident has been identified. In the scenario in which the service provider has made appropriate investment in, and configuration of, core and edge routers based on the applied traceback mechanisms, operators may be able to uncover at the edge router or the incoming physical port the source of the problematic network event. Source identification may help operators stop the problematic network event or mitigate its impact.

7.2 Ingress point identification

A network operator that operates a region/domain (with multiple links to adjacent regions/domains) may use traceback to identify the set of links affected by a particular network incident. The ability to narrow down the number of affected links may help operators expedite the investigation and, when necessary, apply mitigation procedures.

7.3 Partial path identification

If traceback is both deployed and possible across multiple regions/domains, it can be used to uncover a partial path of widespread attacks. While source identification across multiple regions/domains may be difficult under partial traceback deployment, some applications of traceback may be able to identify the partial path or multiple paths of a problematic network event, in support of the mitigation procedures across multiple regions/domains.