International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

D.50

Supplement 1

(04/2011)

SERIES D: GENERAL TARIFF PRINCIPLES

General tariff principles – Principles applicable to GII-Internet

International Internet connection

Supplement 1: General considerations for traffic measurement and options for international internet connectivity

Recommendation ITU-T D.50 – Supplement 1

ITU-T D-SERIES RECOMMENDATIONS

GENERAL TARIFF PRINCIPLES

TERMS AND DEFINITIONS	D.0
GENERAL TARIFF PRINCIPLES	
Private leased telecommunication facilities	D.1–D.9
Tariff principles applying to data communication services over dedicated public data networks	D.10–D.39
Charging and accounting in the international public telegram service	D.40–D.44
Charging and accounting in the international telemessage service	D.45–D.49
Principles applicable to GII-Internet	**D.50–D.59**
Charging and accounting in the international telex service	D.60–D.69
Charging and accounting in the international facsimile service	D.70–D.75
Charging and accounting in the international videotex service	D.76–D.79
Charging and accounting in the international phototelegraph service	D.80–D.89
Charging and accounting in the mobile services	D.90–D.99
Charging and accounting in the international telephone service	D.100–D.159
Drawing up and exchange of international telephone and telex accounts	D.160–D.179
International sound- and television-programme transmissions	D.180–D.184
Charging and accounting for international satellite services	D.185–D.189
Transmission of monthly international accounting information	D.190–D.191
Service and privilege telecommunications	D.192–D.195
Settlement of international telecommunication balances of accounts	D.196–D.209
Charging and accounting principles for international telecommunication services provided over the ISDN	D.210–D.269
Charging and accounting principles for next generation networks (NGN)	D.270–D.279
Charging and accounting principles for universal personal telecommunication	D.280–D.284
Charging and accounting principles for intelligent network supported services	D.285–D.299
RECOMMENDATIONS FOR REGIONAL APPLICATION	
Recommendations applicable in Europe and the Mediterranean Basin	D.300–D.399
Recommendations applicable in Latin America	D.400–D.499
Recommendations applicable in Asia and Oceania	D.500–D.599
Recommendations applicable to the African Region	D.600–D.699

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

Recommendation ITU-T D.50

International Internet connection

Supplement 1

General considerations for traffic measurement and options for international internet connectivity

Summary

Supplement 1 to Recommendation ITU-T D.50 provides considerations and options for traffic measurement in support of the provisions of Recommendation ITU-T D.50. It identifies different approaches for measuring IP traffic flow at the interconnect (at the Border Gateway Protocol interconnect or other interconnect point) between networks operated by administrations and operating agencies authorized by Member States. IP traffic flows can be measured at different points, including at the Border Gateway Protocol (BGP) interconnect point (for example by hardware or software within or external to BGP routers or related equipment). This Supplement is not intended to imply the need for any changes in the IETF Border Gateway Protocol (BGP). Options for traffic measurement that are not addressed in this Supplement are for further study.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T D.50	2000-10-06	3
1.1	ITU-T D.50 (2000) Amd. 1	2004-06-04	3
2.0	ITU-T D.50	2008-10-30	3
3.0	ITU-T D.50	2011-04-01	3
3.1	ITU-T D.50 Suppl. 1	2011-04-01	3

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/.

Table of Contents

Page

Recommendation ITU-T D.50

International Internet connection

Supplement 1

General considerations for traffic measurement and options for international internet connectivity

1 Scope

This Supplement provides considerations and options for traffic measurement in support of the provisions of Recommendation ITU-T D.50. It identifies different approaches for measuring IP traffic flow at the interconnect (at the Border Gateway Protocol interconnect or other interconnect point) between networks operated by administrations and operating agencies authorized by Member States. IP traffic flows can be measured at different points, including at the Border Gateway Protocol (BGP) interconnect point (for example by hardware or software within or external to BGP routers or related equipment). This Supplement is not intended to imply the need for any changes in the IETF Border Gateway Protocol (BGP). Options for traffic measurement that are not addressed in this Supplement are for further study.[1]

2 Purposes/rationale

Recommendation ITU-T D.50 recommends that the value of traffic flow be one of the elements, amongst others, to be taken into account by parties involved in the provision of international Internet connections in their bilateral commercial arrangements, or other arrangements. Furthermore, Appendix I of [ITU-T D.50] indicates that the agreed level of traffic exchanged may also be taken into consideration.

This Supplement provides an overview of possible approaches for measuring IP traffic flow between networks. The choice of which approach would be used and how the traffic measurement data collected would be used in an international Internet connection is typically determined by negotiations between the concerned parties. This Supplement provides general considerations for measuring traffic flow to be referred to in bilateral negotiation. As technologies and networks evolve, new methods could be developed for measuring traffic flow. This Supplement is not meant to be exclusive.

3 References

[ITU-T D.50] Recommendation ITU-T D.50 (2008), *International Internet connection*.

4 Approaches/mechanisms to estimate traffic flows

This Supplement, noting the possibility under [ITU-T D.50], provides considerations on estimating the flow of IP traffic at the interconnect between networks. The traffic flows referred to in [ITU-T D.50] can be measured at the interconnect. Approaches and mechanisms to establish traffic flow measurement may include but not be limited to the following considerations.

[1] This Supplement benefits from the ongoing contributions and work of the Study Group 3 International Internet Connectivity (IIC) and Traffic Flow Multifactors (TFMF) Rapporteur Groups.

4.1 Architecture of traffic measurements

In general, traffic measurements are made at the interconnect between networks. There can be multiple links between networks at multiple, geographically separate locations. In addition, routing within and between networks can direct traffic flows on different paths between networks in each direction. Therefore, the information gathered at the measurement points must be collected, aggregated and processed before it can be used.

4.2 Types of measurements

The fundamental traffic flow measurements include a number of key elements.

Routing information, using a variety of protocols, can be used to aggregate and correlate traffic measurements.

4.3 Location of measurements

4.3.1 Traffic measurement

In general, the device measuring traffic flow is located in the data path of the traffic, preferably at the interconnect itself. IP traffic flow measurements can be performed by a border router at the interconnect while forwarding the traffic or by a traffic measurement probe attached to a line or a monitored port on network equipment at the interconnect.

4.3.2 Routing information collection

Although not required for flow analysis, for enhanced reporting an operator can collect information on the routing paths for traffic exchanged with a peer. Such routing information can be collected from information exchanged using a variety of available protocols, including the Border Gateway Protocol (BGP).

4.4 Effect of connectivity and routing on measurements

Traffic measurement depends on the connectivity between networks and routing paths available for the traffic to follow. In general, a network will only be able to measure traffic that crosses its facilities.

4.5 Correlation and analysis

Traffic measurements collected from various measurement points are aggregated and transmitted back to a collection point for analysis. The derived information can be combined with routing information collected to analyze traffic flows based on the path the traffic takes through the network. This information can be combined with other information, e.g., financial information, business goals, etc., when determining bilateral commercial agreements on interconnections.

4.6 Schematic process

When the measuring point detects traffic passing the interconnect, it checks the packet header to obtain information about the packet, including total length of packet and length of the IP header.

From this information the traffic flow to which this packet belongs can be identified and the size of the packet (total length minus IP header length) can be calculated. Alternatively, a sample of packets transiting the interconnect can be counted. This information is added to the traffic flow.

The traffic measurements collected can be used in negotiating commercial agreements between two parties.

Appendix I

Additional considerations

I.1 Approaches/mechanisms to estimate traffic flows

This Supplement, noting the possibility under [ITU-T D.50], provides considerations on estimating the flow of IP traffic at the interconnect between networks. The Internet Engineering Task Force (IETF), as the organization that defines standards for the Internet infrastructure, have developed methods for measuring IP traffic flow and reporting those measurements, for example IPFIX [RFC 3917]. It should be noted that the capabilities defined for IPFIX are for generalized IP networks including Service Provider, Enterprise, consumer, etc., networks and not all the capabilities described therein are appropriate for application to the international interconnect.

The traffic flows referred to in [ITU-T D.50] should be measured at the interconnect.

I.1.1 Architecture of traffic measurements

This Supplement follows the architecture and reference model for flow measurements defined by IETF in [RFC 5470] as applied to an international Internet interconnection.

In general, traffic measurements are made at the interconnect between networks. There can be multiple links between networks at multiple, geographically separate locations. In addition, routing within and between networks can direct traffic flows on different paths between networks in each direction. Therefore, the information gathered at the measurement points must be collected, aggregated and processed before it can be used.

Due to the large amount of data available for collection, network operators (i.e., administrations or operating agencies authorized by Member States) can choose to use sampling and aggregation techniques to reduce the amount of measurement data collected and to reduce the load on the measurement equipment.

The typical traffic measurement system consists of three basic parts:

– a flow source,

– a flow collector, and

– a flow analyzer.

The flow source typically resides on the IP network routing hardware itself, but also can reside on a separate device that can detect network traffic (e.g., port mirroring, passive optical splitter) or on a middle-box (e.g., firewall, session border controller). The flow source hardware must either provide standards-based access to flow data (e.g., via SNMP) or have the ability to generate standards-based flow records (e.g., IPFIX). For measuring traffic at the interconnect, the flow source should be as close as possible to the interconnect point.

The flow collector must have the ability to poll and/or capture flow data and store it in a format suitable for further processing. The flow collector can also perform preliminary aggregation of data. The number and location of the flow collectors depend on network design and scaling characteristics.

The flow analysis and reporting system takes the stored data from the flow collectors, processes the data and produces reports from it. The flow collector and flow analyzer often are served from a single device. The flow collector and/or flow analyzer can also pull data from other sources (e.g., routing records) to use to aggregate the data and produce reports.

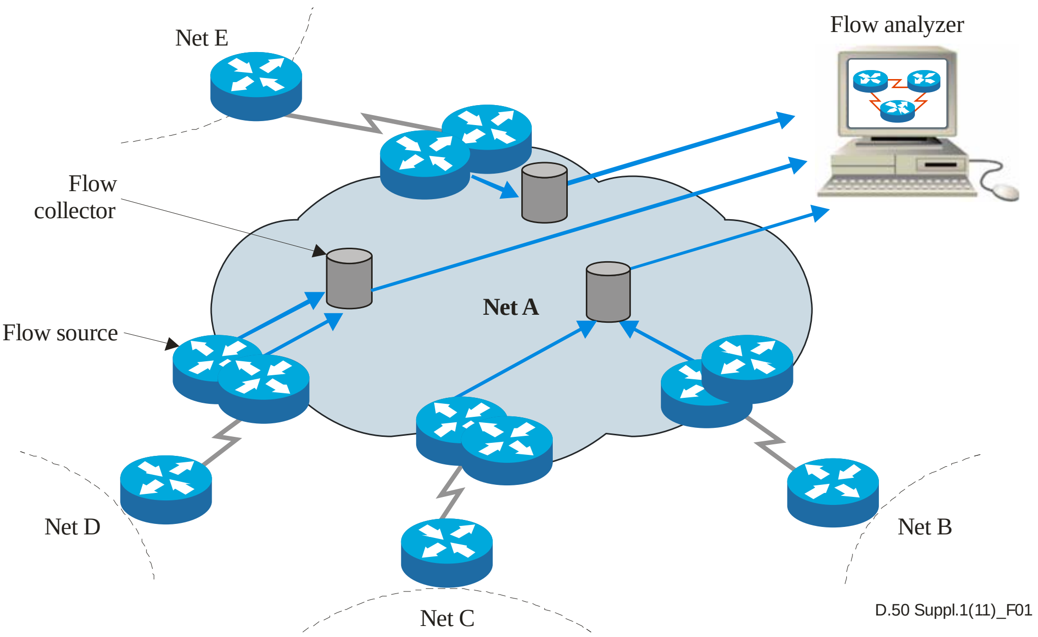

Figure I.1 – General flow measurement architecture

I.1.2 Types of measurements

The fundamental traffic flow measurements gathered at a measurement point includes:

- Source IP address and port
- Destination IP address and port
- Flow size (packets and octets)
- Protocol type

Routing information can be used to aggregate and correlate traffic measurements. This routing information can be gathered from the standard Border Gateway Protocol (BGP) [RFC 4271] and from the network's routing tables and can include:

- Source/Destination ASNs
- Origin peer/Destination peer ASNs
- AS Paths

Note that traffic flow measurements are not carried in the BGP itself.

Use of this information for aggregating and correlating traffic measurements might be better suited for short-term and limited traffic optimization studies rather than ongoing detailed accounting.

I.1.3 Location of measurements

I.1.3.1 Traffic measurement

In general, the device measuring traffic flow must be located in the data path of the traffic, preferably at the interconnect itself. IP traffic flow measurements can be performed by a border router at the interconnect while forwarding the traffic or by a traffic measurement probe attached to a line or a monitored port on network equipment at the interconnect.

If the measurements are made on the border router, then the measurement process can potentially adversely affect the ability of the router to pass traffic. Increasing the measurement load and complexity of measurements increases this probability.

I.1.3.2 Routing information collection

Although not required for flow analysis, for enhanced reporting an operator can collect information on the routing paths for traffic exchanged with a peer. Such routing information can be collected from information exchanged using standard BGP. There are several options for collecting the routing information:

- At the point of traffic flow measurement (e.g., border routers)
- At a point in the network that collects BGP information (e.g., route reflector)
- At a route collector set up specifically for this purpose

Regardless of the location, the routing information, if used for enhanced reporting, must be transmitted to the flow collector or flow analyzer system.

It should be noted that BGP is not required in all cases for interconnects between networks (e.g., a single-homed network). In this case, flow measurements can still be gathered on the packets transiting the interconnect.

I.1.4 Effect of connectivity and routing on measurements

Traffic measurement depends on the connectivity between networks and routing paths available for the traffic to follow. In general, a network will only be able to measure traffic that crosses its facilities. Measurements taken on one network will not provide visibility into traffic that takes a route through another network.

Routing policies in place in a network in the path generally result in asymmetry in routing. In the case of asymmetric routing, the ingress (or egress) point in a network of a traffic flow from the traffic originator will not be the same as the egress (or ingress) point for traffic in the reverse direction. In the worst case scenario, the traffic in one direction can take a completely different path than traffic in the other direction and in fact traverse a completely different autonomous system in the reverse direction, resulting in the flow capture system missing half of the transaction.

Figure I.2 illustrates this case in which a customer attached to Network A makes a FTP request to a server located on Network B. Network B's routing policy causes the return packets to transit Network C instead of directly back to Network A. In this case, Network A's flow measurements would show the egress flow for this traffic exiting to Network B, but the return path would show up as ingress traffic from Network C. In addition to routing asymmetry, there can also be application traffic asymmetry where a small flow in one direction can result in a large flow in the opposite direction (e.g., an end-user requesting a streaming video from a remote server).

The implications of this on traffic measurement is that determining the origin AS-peer of traffic by mapping the source IP address of a traffic flow to a destination AS-peer might lead to inaccurate measurements. Traffic back to that source might follow a path to a different AS. Therefore service providers must take care in aggregating, correlating and utilizing the flow measurements, taking into account asymmetries in routing.

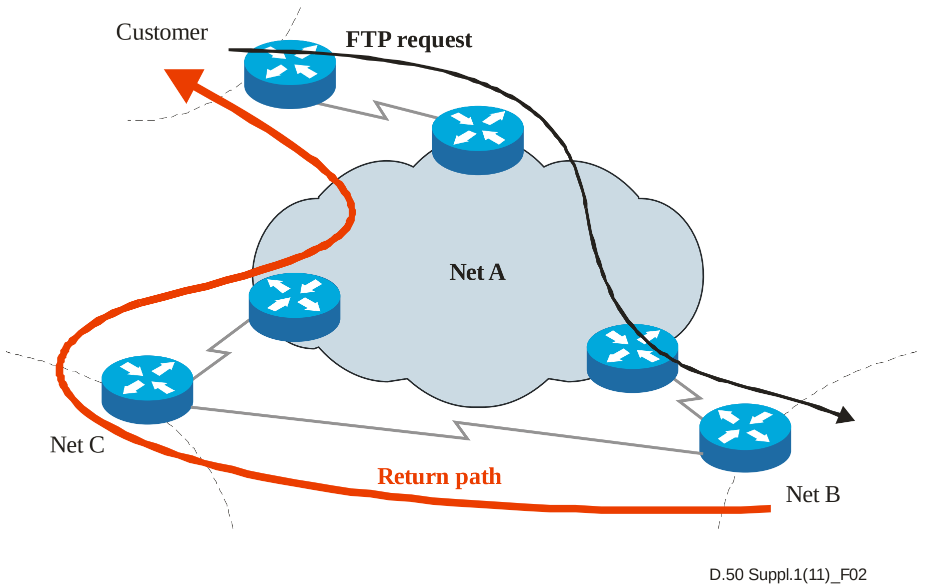

Figure I.2 – Routing path effect on traffic measurement

I.1.5 Correlation and analysis

As mentioned previously, traffic measurements collected from various measurement points are aggregated and transmitted back to a collection point for analysis.

Examples of aggregation schemes include:

- Source/Destination autonomous system
- Source/Destination IP address prefix
- Protocol type distribution
- Packet size distribution
- Port number distribution

The traffic flow measurements can be combined with the routing information collected to analyze traffic flows based on the path the traffic takes through the network. This information can be combined with other information, e.g., financial information, business goals, etc., when determining bilateral commercial agreements on interconnections.

I.1.6 Schematic process

When the measuring point detects traffic passing the interconnect, it checks the packet header to obtain information about the packet (see clause 4.6) including total length of packet and length of the IP header.

From this information the traffic flow to which this packet belongs can be identified and the size of the packet (total length minus IP header length) can be calculated. Alternatively, a sample of packets transiting the interconnect can be counted. This information is added to the traffic flow.

Based on this information collected and based on the routing tables in the network, the traffic flow can be aggregated in one or more of the following ways:

- Source autonomous system
- Destination autonomous system
- Peer source autonomous system
- Peer destination autonomous system

Aggregation can occur at the measuring point by the flow source, at the flow collector or at the flow analysis point.

The traffic measurement system can compute the traffic flows exchanged with a partner over all interconnects with that partner taking into account the aggregation mentioned above over a period of time to develop the total traffic flow with that partner.

The traffic measurements collected as described above can be used as input to commercial agreements between two parties.

The choice of which traffic measurements would be used in IIC is determined based on bilateral negotiation rather than on an international standard.

I.1.7 Definitions and abbreviations

traffic flow [RFC 3917]:

A flow is defined as a set of IP packets passing an observation point in the network during a certain time interval. All packets belonging to a particular flow have a set of common properties. Each property is defined as the result of applying a function to the values of:

1. one or more packet header field (e.g., destination IP address), transport header field (e.g., destination port number), or application header field (e.g., RTP header fields [RFC 3550]);
2. one or more characteristics of the packet itself (e.g., number of MPLS labels, etc.);
3. one or more of fields derived from packet treatment (e.g., next hop IP address, the output interface, etc.).

A packet is defined to belong to a flow if it completely satisfies all the defined properties of the flow.

autonomous system (AS) [RFC 1930]: A connected group of one or more IP prefixes run by one or more network operators which has a **single** and **clearly defined** routing policy.

autonomous system number (ASN): A code that uniquely identifies an AS.

I.1.8 Bibliography

[RFC 1930] IETF RFC 1930 (1996), *Guidelines for creation, selection, and registration of an Autonomous System (AS).*

[RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[RFC 3917] IETF RFC 3917 (2004), *Requirements for IP Flow Information Export (IPFIX).*

[RFC 4271] IETF RFC 4271 (2006), *A Border Gateway Protocol 4 (BGP-4).*

[RFC 5101] IETF RFC 5101 (2008), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*.

[RFC 5102] IETF RFC 5102 (2008), *Information Model for IP Flow Information Export*.

[RFC 5470] IETF RFC 5470 (2009), *Architecture for IP Flow Information Export*.

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	Terminals and subjective and objective assessment methods
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, 2011