

Recommendation

ITU-T Y.3657 (12/2023)

SERIES Y: Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

Big Data

Big data driven networking – Requirements and capabilities of network visibility

Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities

GLOBAL INFORMATION INFRASTRUCTURE	Y.100-Y.999
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	Y.1000-Y.1999
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
IPTV over NGN	Y.1900-Y.1999
NEXT GENERATION NETWORKS	Y.2000-Y.2999
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
Enhancements to NGN	Y.2300-Y.2399
Network management	Y.2400-Y.2499
Computing power networks	Y.2500-Y.2599
Packet-based Networks	Y.2600-Y.2699
Security	Y.2700-Y.2799
Generalized mobility	Y.2800-Y.2899
Carrier grade open environment	Y.2900-Y.2999
FUTURE NETWORKS	Y.3000-Y.3499
CLOUD COMPUTING	Y.3500-Y.3599
BIG DATA	Y.3600-Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800-Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	Y.4000-Y.4999
General	Y.4000-Y.4049
Definitions and terminologies	Y.4050-Y.4099
Requirements and use cases	Y.4100-Y.4249
Infrastructure, connectivity and networks	Y.4250-Y.4399
Frameworks, architectures and protocols	Y.4400-Y.4549
Services, applications, computation and data processing	Y.4550-Y.4699
Management, control and performance	Y.4700-Y.4799
Identification and security	Y.4800-Y.4899
Evaluation and assessment	Y.4900-Y.4999

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

Recommendation ITU-T Y.3657

Big data driven networking – Requirements and capabilities of network visibility

Summary

Recommendation ITU-T Y.3657 specifies requirements and capabilities of network visibility for big-data-driven networking (bDDN). It focuses on the scenario where network infrastructure layer of bDDN corresponds to Internet protocol (IP) bearer network.

The scope of this Recommendation includes the following aspects of network visibility of bDDN: overview for network visibility of big-data-driven networking, requirements and capabilities for network visibility of the control aspect, requirements and capabilities for network visibility of the forwarding aspect, requirements and capabilities for network visibility of the management aspect, interface requirements for network visibility and security considerations.

History *

Edition	Recommendation	Approval	Study Group	Unique ID
1.0	ITU-T Y.3657	2023-12-14	13	11.1002/1000/15748

Keywords

Big-data-driven networking (bDDN), capabilities, IP bearer network, network visibility, requirements.

* To access the Recommendation, type the URL <https://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID.

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 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/software copyrights, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the appropriate ITU-T databases available via the ITU-T website at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2024

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 Recommendation.....	2
4	Abbreviations and acronyms	2
5	Conventions	4
6	Introduction.....	4
7	Overview for network visibility of bDDN.....	4
	7.1 Network telemetry	4
	7.2 Overview of network visibility based on bDDN	5
8	Requirements and capabilities for network visibility of control aspect of bDDN	7
	8.1 Requirements for network visibility of the control aspect of bDDN	7
	8.2 Capabilities for network visibility of the control aspect of bDDN	15
9	Requirements and capabilities for network visibility of the forwarding aspect of bDDN.....	15
	9.1 Requirements for network visibility of the forwarding aspect of bDDN.....	15
	9.2 Capabilities for network visibility of the forwarding aspect of bDDN	20
10	Requirements and capabilities for network visibility of the management aspect of bDDN.....	20
	10.1 Requirements for network visibility of the management aspect of bDDN	21
	10.2 Capabilities for network visibility of the management aspect of bDDN	23
11	Interface requirements for network visibility of bDDN	23
	11.1 NETCONF.....	24
	11.2 gRPC network management interface (gNMI).....	25
	11.3 UDP based publication channel (UPC)	27
	11.4 BGP-LS	27
	11.5 BMP.....	28
	11.6 Other interfaces	28
12	Requirements for network visibility of other aspects	29
	12.1 Requirements for the visibility of real-time congestion	29
	12.2 Requirements for the visibility of real-time link quality	31
13	Security considerations	33
	Bibliography.....	34

Recommendation ITU-T Y.3657

Big data driven networking – Requirements and capabilities of network visibility

1 Scope

This Recommendation studies requirements and capabilities for network visibility of big-data-driven networking, which focuses on network visibility for bDDN in the scenario where the network infrastructure layer of big data driven networking (bDDN) corresponds to the Internet protocol (IP) bearer network.

The scope of this Recommendation includes:

- Overview for network visibility of bDDN;
- Requirements and capabilities for network visibility of the control aspect of bDDN;
- Requirements and capabilities for network visibility of the forwarding aspect of bDDN;
- Requirements and capabilities for network visibility of the management aspect of bDDN;
- Interface requirements for network visibility of bDDN;
- Security considerations.

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

- [ITU-T Y.2704] Recommendation ITU-T Y.2704 (2007), *Security mechanisms and procedures for NGN*.
- [ITU-T Y.3600] Recommendation ITU-T Y.3600 (2015), *Big data – Cloud computing based requirements and capabilities*.
- [ITU-T Y.3650] Recommendation ITU-T Y.3650 (2018), *Framework of big-data-driven networking*.
- [ITU-T Y.3652] Recommendation ITU-T Y.3652 (2020), *Big data driven networking – requirements*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term defined elsewhere:

3.1.1 big data driven networking (bDDN) [ITU-T Y.3650]: A type of future network framework that collects big data from networks and applications, and generates big data intelligence based on the big data; it then provides big data intelligence to facilitate smarter and autonomous network management, operation, control, optimization and security, etc.

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 network visibility: The ability for the network management and control entity to sense the state and behaviour of a network by collecting comprehensive network data.

NOTE – Network visibility is essential and beneficial to network operation, maintenance and management.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

ACL	Access Control List
AI	Artificial Intelligence
ARP	Address Resolution Protocol
bDDN	big Data Driven Networking
BFD	Bidirectional Forwarding Detection
BGP	Border Gateway Protocol
BMP	BGP Monitoring Protocol
BSID	Binding Segment Identification
CLI	Command-Line Interface
CRC	Cyclic Redundancy Check
CPU	Central Processing Unit
EVPN	Ethernet Virtual Private Network
GR	Graceful Restart
gRPC	Google Remote Procedure Calls
IFIT	In-situ Flow Information Telemetry
IGP	Interior Gateway Protocol
IGMP	Internet Group Management Protocol
IOAM	In-situ Operations, Administration, and Maintenance
IP	Internet Protocol
IPFIX	IP Flow Information Export
IS-IS	Intermediate System-to-Intermediate System
ISP	Internet Service Provider
LDP	Label Distribution Protocol
LLDP	Link Layer Discovery Protocol
L2VPN	Layer 2 Virtual Private Network
L3VPN	Layer 3 Virtual Private Network
LSA	Link-State Advertisement
LSDB	Link-State Data Base
LSP	Label Switching Path

LSR	Label Switching Router
MAC	Media Access Control
MIB	Management Information Base
ML	Machine learning
MLD	Multicast Listener Discover
MPLS	Multi-Protocol Label Switching
MPLS-TE	Multi-Protocol Label Switching-Traffic Engineering
MTU	Maximum Transmission Unit
NBMA	Non-Broadcast Multiple Access
NDP	Neighbour Discovery Protocol
NETCONF	Network Configuration protocol
NMS	Network Management System
NSSA	Not-So-Stubby Area
OAM	Operation, Administration and Maintenance
OSPF	Open Shortest Path First
PIM	Protocol Independent Multicast
PW	Pseudo Wire
QoE	Quality of Experience
QoS	Quality of Service
RIB	Routing Information Base
RPC	Remote Process Call
RPF	Reverse Path Forwarding
RSVP	Resource Reservation Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SR	Segment Routing
SRv6	Segment Routing over IPv6
STAMP	Simple Two-way Active Measurement Protocol
TCP	Transfer Control Protocol
TWAMP	Tow-Way Active Measurement Protocol
VC	Virtual Circuit
UPC	UDP based Publication Channel
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
XML	Extensible Markup Language
YANG	Yet Another Next Generation

5 Conventions

In this Recommendation:

The keywords "is required to" indicate a requirement which must be strictly followed and from which no deviation is permitted, if conformance to this Recommendation is to be claimed.

The keywords "is recommended" indicate a requirement which is recommended but which is not absolutely required.

The keywords "can optionally" indicate an optional requirement which is permissible, without implying any sense of being recommended. This term is not intended to imply that the vendor's implementation must provide the option, and the feature can be optionally enabled by the network operator/service provider. Rather, it means the vendor may optionally provide the feature and still claim conformance with this Recommendation.

6 Introduction

The future network should no longer be a vehicle only for best effort connectivity, but a programmable infrastructure of connectivity and applications supporting vital and high precision services that require low latency and extremely high reliability communications. How to guarantee the quality of service (QoS) and improve user quality of experience (QoE) will be a major challenge for IP bearer networks, widely adopted by telecom operators to carry telecommunication services. The conventional network management system (NMS) cannot provide real-time network visibility and traffic visibility. Network visibility is the ability of management tools to see the state and behaviour of a network. It is essential for successful network operation, management and maintenance. The future autonomous networks will require a holistic view on network visibility. A holistic view on network visibility needs comprehensive data. Network telemetry, as one of network data collection techniques, can gain network insight and facilitate efficient and automated network management.

Conventional operation, administration and maintenance (OAM) only covers a narrow range of data, and those data are insufficient to gain network visibility. Compared with the conventional OAM, network telemetry is an ideal tool to gain sufficient network visibility with better flexibility, scalability, accuracy, coverage and performance.

[ITU-T Y.3650] specifies a framework for big-data-driven networking (bDDN) – A type of future network framework that collects big data from networks and applications, and generates big data intelligence based on the big data. It then provides big data intelligence to facilitate smarter and autonomous network management, operation, control, optimization, security, etc. [ITU-T Y.3652] specifies requirements of big data driven networking. All these Recommendations provide the specification for high-level aspects of bDDN.

Network visibility is a fundamental requirement and capability for big data-driven networks, which exploit the bDDN architecture to achieve massive network data collection, storage, analysis and visual presentation. Moreover, when bDDN is applied in an IP bearer network, those requirements and capabilities are more important and urgent.

7 Overview for network visibility of bDDN

It can be learned from clause 6 that network visibility is essential and that beneficial functional features for bDDN and network telemetry is a proper method for network visibility.

7.1 Network telemetry

For a long time, network operators have relied upon simple network management protocol (SNMP), command-line interface (CLI), or Syslog to monitor the network. These conventional techniques are

not sufficient to support operations and maintenance of the future networks, such as security anomaly detection, policy and intent compliance, service level agreement (SLA) compliance, root cause analysis (RCA), event tracking and prediction, network optimization, etc. The reason is as follows:

- Most use cases need to continuously monitor the network and dynamically refine the data collection in real-time. The conventional poll-based low-frequency data collection is not appropriate for these applications. Comprehensive data is needed from all aspects of a network device. Conventional OAM only covers a narrow range of data (e.g., SNMP only handles data from the management information base (MIB)).
- Many application scenarios need to correlate network-wide data from multiple sources (i.e., from distributed network devices, different components of a network device, or different network planes).
- Some of the conventional OAM techniques (e.g., CLI and Syslog) lack a formal data model. The unstructured data hinder the tool automation and application extensibility. Standardized data models are essential to support the programmable networks.
- The conventional measurement techniques can interfere with the user traffic and their results are indirect. Techniques that can collect direct and on-demand data from user traffic are more favourable (e.g., in-situ OAM).

Network telemetry [b-IETF RFC 9232] has emerged as a mainstream network data collection and consumption technique, and it covers the conventional network OAM. Hence, network telemetry can directly trigger automated network operation, while in contrast some conventional OAM tools are designed and used to help human operators to monitor and diagnose the networks and guide manual network operations. It is expected that network telemetry can provide the necessary network insight for autonomous networks and address the shortcomings of conventional OAM techniques.

Network telemetry is expected to hold the following characteristics:

- Push and streaming: Instead of polling data from network devices, telemetry collectors subscribe to streaming data pushed from data sources.
- Volume and velocity: The data volume can be huge, and the processing is optimized for the needs of automation in real-time.
- Normalization and unification: Telemetry aims to address the overall network automation needs. Efforts are made to normalize data representation and unify the protocols, so as to simplify data analysis and provide integrated analysis across heterogeneous devices and data sources across a network.
- Model-based: Telemetry data are modelled in advance, which allows applications to configure and consume data with ease.
- Dynamic and interactive: Since network telemetry is meant to be used in a closed control loop for network automation, it needs to run continuously and adapt to the dynamic and interactive queries from the network management system or the controller.

7.2 Overview of network visibility based on bDDN

As described in [ITU-T Y.3650], bDDN is composed of three planes, and each plane is composed of several layers. Figure 7-1 depicts the architecture of network visibility based on bDDN.

The big data plane is composed of four layers, and the bottom layer is the data sensing layer which collects various data from the network infrastructure layer of the network plane. To gain a holistic view on network visibility, it is necessary to collect comprehensive data from network control components, network forwarding components and network management components in real time. The telemetry of control aspect refers to the health condition monitoring of different network control protocols covering Layer 2 to Layer 7. Keeping track of the running status of these

protocols is beneficial for detecting, localizing, and even predicting various network issues, as well as network optimization in real time and in fine granularity. An effective telemetry of the forwarding aspect relies on the data that the network device can expose. The quality, quantity and timeliness of data must meet some stringent requirements. The data plane programmability of network elements is essential to support network telemetry. The management plane of network elements interacts with the NMS, and provides information such as performance data, network logging data, network warning and defects data, and network statistics and state data. The management plane includes many protocols, including some that are considered "legacy", such as SNMP and Syslog.

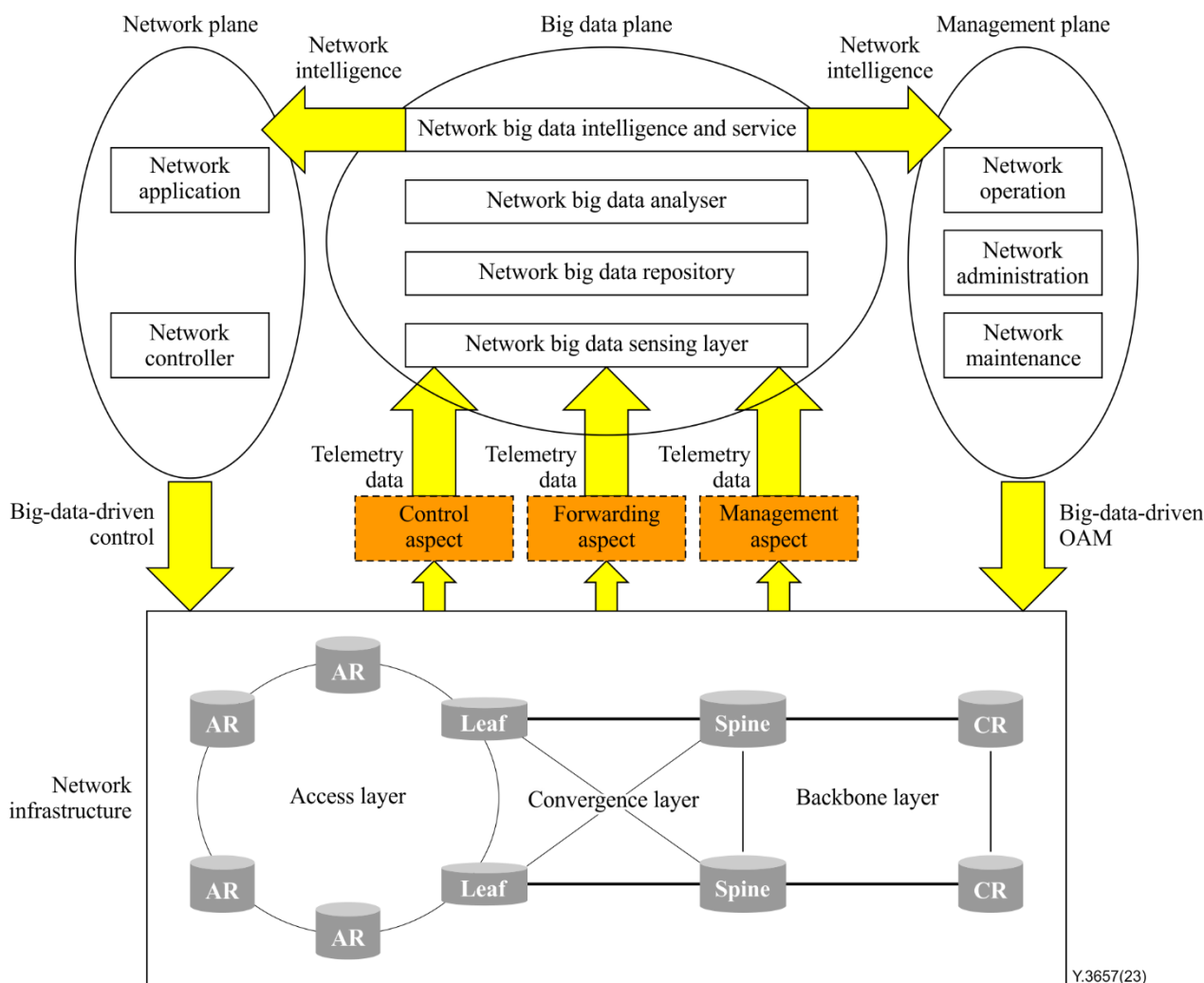


Figure 7-1 – Architecture of network visibility based on bDDN

The collected telemetry data is stored in a data storage repository. Meanwhile, some data pre-processing is required in accordance with several pre-set rules, including data filtering and cleaning, data labelling, data aggregating, data normalizing, etc. All these pre-processed data are saved to the corresponding database.

The network big data analysing layer utilizes traditional data analysis methods (e.g., statistical analytical method, visualization analytical method, correlation analytical method) as well as the advanced big-data and machine learning techniques to process and analyse data.

The network big data intelligence and service layer needs to further transform the processed data into valuable information and instructions and provide data intelligence to the other two planes in the form of services.

The network plane consists of three layers: network infrastructure layer, network controller layer and network application layer. The network infrastructure layer includes all kinds of network devices implementing packet forwarding. The network controller layer includes network controllers, responsible for policy decision and real-time control of traffic flows, such as distribution of flow table, preferential path calculation, dynamic modification of configuration and so on. The application layer includes different kinds of network applications, such as path optimization, load balancing, service function chain (SFC), etc.

With the aid of the big data plane, network visibility and data intelligence make the network plane capture network behaviour and network status quickly and accurately, so that network parameters can be autonomously updated for achieving optimal performance and best SLA guarantee.

The management plane is also composed of three aspects: network operation aspect, network administration aspect and network maintenance aspect. Taking advantage of data analysis results and network intelligence in the big data plane, the management plane realizes a series of network management functions, including troubleshooting, configuration and optimization. Other functions such as expanding network capacity based on timely traffic prediction, and implementing security reinforcement based on the indicated potential risks, can also be supported.

By introducing the big data plane, which concentrates on the collection, processing, analysis and visualization of multi-dimensional network data, the burden of control plane and management plane of the network can be greatly unloaded. This novel architecture of bDDN can fulfil hierarchization and decoupling of traditional network, and is beneficial to accelerate network reconstruction. Furthermore, data intelligence generated from the big data plane helps to implement network automation.

8 Requirements and capabilities for network visibility of control aspect of bDDN

Network visibility of the control aspect of bDDN is of great significance for monitoring the network running state. To gain the visibility of the control aspect, it is necessary collect running status data of main network control protocols and keep tracking the running status of those protocols. Network visibility of control aspect of bDDN is beneficial for detecting, localizing and even predicting various network issues.

8.1 Requirements for network visibility of the control aspect of bDDN

- It is required to support the visibility of border gateway protocol (BGP) running status, including BGP routing table, BGP route statistics, threshold alarm, BGP neighbour status, BGP neighbour flapping, the causes of BGP peering disconnections, etc.
- It is required to support the visibility of routing information base (RIB), i.e., IP routing table.
- It is required to support the visibility of intermediate system-to-intermediate system (IS-IS) running status, including IS-IS memory overload, IS-IS adjacency establishment failed, IS-IS adjacency status changed, IS-IS neighbour flapping, routing loop detected, etc.
- It is required to support the visibility of open shortest path first (OSPF) running status, including the introduced external routes overrun, adjacency status changed, interface status changed, configuration error for the neighbour interface detected, OSPF neighbour flapping, routing loop detected, etc.
- It is recommended to support the visibility of IP multicast protocol running status, including IGMP/MLD and protocol independent multicast (PIM).
- It is recommended to support the visibility of label distribution protocol (LDP) running status, including LDP session state changed, LDP session deleted.