ITUPublications
Recommendations

International Telecommunication Union
Standardization Sector

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

ITU-T Y-SERIES RECOMMENDATIONS

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/.

Table of Contents

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.

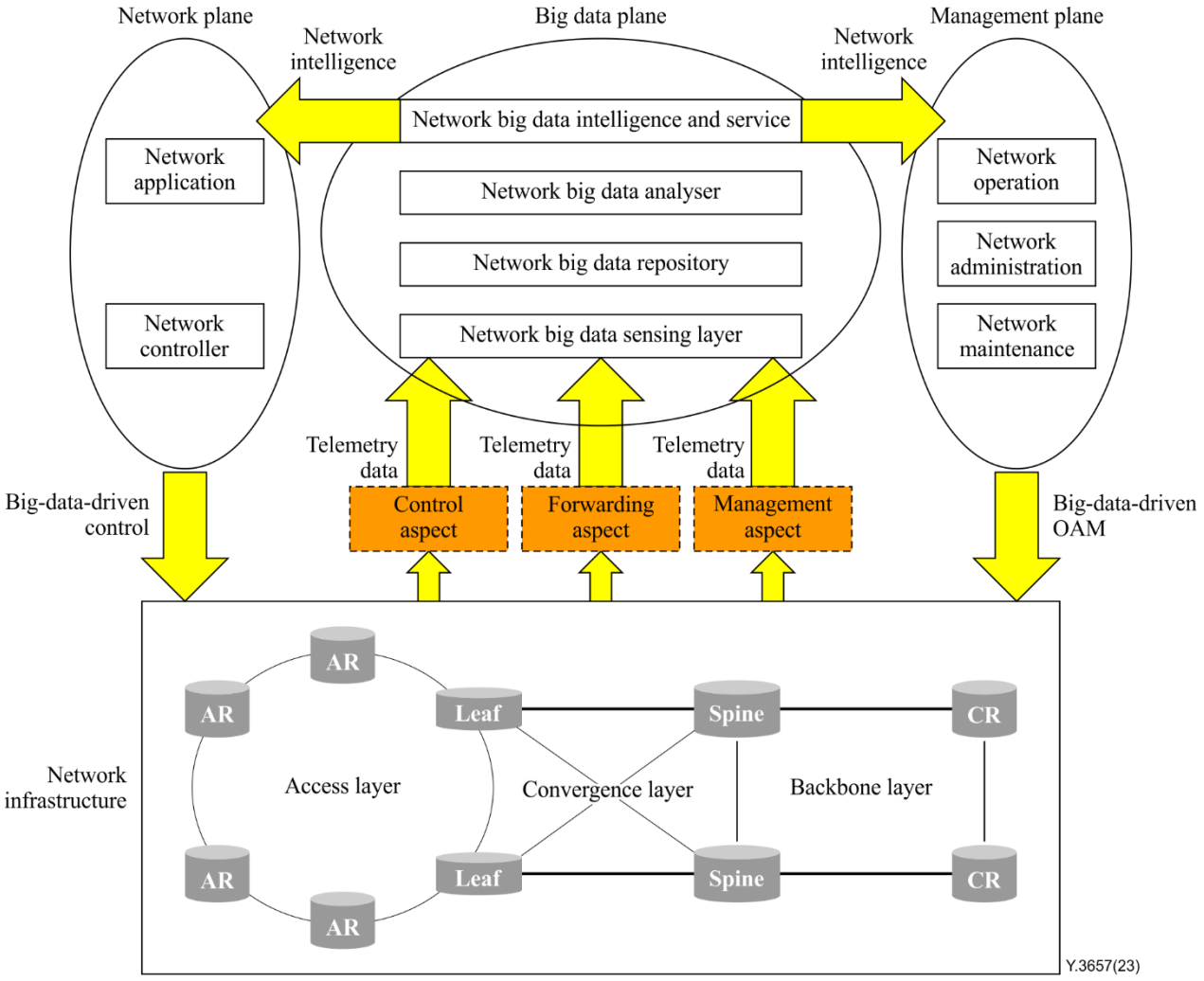

Figure 7-1 – Architecture of network visibility based on bDDN

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.

– It is recommended to support the visibility of multi-protocol label switching-traffic engineering (MPLS-TE) running status, including resource reservation protocol (RSVP) status, MPLS-TE master and standby tunnel switching status.
– It is required to support the visibility of SR/SRv6 policy running status.
– It is required to support the visibility of Ethernet virtual private network (EVPN) running status, including EVPN routes, media access control (MAC) address routes suppressed, loop detected, routes discarded, EVPN instance status changed, etc.
– It is required to support the visibility of multi-protocol label switching (MPLS) Layer 2 virtual private network (L2VPN) running status, including pseudo wire (PW) status changed, PW protection switching, etc.
– It is required to support the visibility of MPLS Layer 3 virtual private network (L3VPN running status, including virtual private network (VPN) tunnel status, virtual routing and forwarding (VRF) binding interface status, the number of routes exceeded, etc.
– It is recommended to support the visibility of address resolution protocol (ARP) table.
– It is recommended to support the visibility of neighbour discovery protocol (NDP) table.
– It is recommended to support the visibility of bidirectional forwarding detection (BFD) session status.

In order to achieve network visibility of the control aspect of bDDN, telemetry data collection of key control protocols is necessary. Table 8-1 presents relevant telemetry data collection of the control aspect.

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
BGP	BGP routing table	BGP RIB, including the following parameters: − BGP table version − Origin − Destination prefix/subnet mask − Next hop − Metric − Local preference − AS PATH		On-change
	BGP route statistics	1. Total number of public IPv4 routes 2. Total number of public IPv6 routes 3. Number of VPN IPv4 instance routes 4. Number of VPN IPv6 instance routes 5. Number of prefixes rejected by inbound policy 6. Total number of BGP updates invalidated 7. Number of updates invalidated due to AS_PATH loop	≤ 60	Periodic
	Threshold alarm	1. An alarm is generated when the total number of global routes reaches the overload threshold 2. An alarm is generated when the total number of VPN routes reaches the overload threshold 3. An alarm is generated when the number of routes received from BGP neighbour reaches the preset threshold 4. An alarm is generated when the number of BGP peering sessions reaches the preset threshold.		Event-triggered
	BGP neighbour status	1. IDLE 2. CONNECT		On-change

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
		3. ACTIVE 4. OPENSENT 5. OPENCONFIRM 6. ESTABLISHED		
	The causes of BGP peering disconnected	1. Configuration error 2. Notification message received 3. Received BGP message including one or more error fields 4. Hold timer timeout. 5. Neighbour unreachable 6. Connected interface down		Event-triggered
	BGP neighbour security	1. BGP session authentication failed		Event-triggered
RIB	IP routing table	1. Global routing table 2. VRF routing table IP routing table includes the following parameters: – Destination prefix/subnet mask – Next hop – Protocol type – Preference – Metric – Outbound interface	≤ 300	Periodic
IS-IS	IS-IS memory overload	1. Number of label switching paths (LSPs) reaches the overload threshold 2. Link-state data base (LSDB) size is overloaded 3. LSDB size exits overload state 4. New adjacency is rejected due to memory overload		Event-triggered
	IS-IS adjacency establishment failed	Fails to establish adjacency with the neighbour when receiving Hello message, possible reasons include: – Configured local system ID is the same as the neighbour system ID – Interface authentication fails due to the configured authentication mode or password problem – The IS-IS level-1 neighbours connected to the same link have different area addresses configured – The IS-IS neighbours connected to the same link have different Level class configured – In a broadcast network, the local interface receives a hello message with network field values different from the local interface – In a P2P network, the local interface receives a hello message with network field values different from the local interface – The neighbour interfaces connected directly have different maximum transmission units (MTUs) configured		On-change
	IS-IS adjacency status changed	IS-IS adjacency state changes to: – DOWN		On-change

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
		– Initialization – UP		
	IS-IS interface status changed	Possible causes for interface status change include: – The physical state of the interface changes – The Protocol state of the interface changes – Enable or disable IS-IS – Reset IS-IS all command		On-change
	IS-IS neighbour flapping suppression changed	IS-IS neighbour flapping suppression changes: – IS-IS interface is in the flapping suppression phase – IS-IS interface exits the flapping suppression phase		On-change
	System ID conflicted	IS-IS detects a system ID conflict. In the same topology, the system ID's configurations of two IS-IS devices are duplicate.		On-change
	Routing loop detected	The device detects a loop in the route		Event-triggered
	Prefix SID problems	1. Prefix SID conflicts 2. The received prefix SID exceeds the range of the local SRGB		Event-triggered
OSPFv2/v3	The introduced external routes overrun	1. The number of AS external link-state advertisements (LSAs) introduced by OSPF is greater than the upper threshold 2. The number of not-so-stubby area (NSSA) LSAs introduced by OSPF is greater than the upper threshold		Event-triggered
	LSA aged	1. One or more LSAs in LSDB have reached the aging time		Event-triggered
	Adjacency status changed	OSPF adjacency state changes to: – Down – Attempt – Init – 2-Way – ExStart – Exchange – Loading – Full		On-change
	Interface status changed	Possible causes for interface state change include: – The physical state of the interface changes – The Protocol state of the interface changes – Enable or disable OSPF – Reset OSPF all command		On-change
	Configuration error for the neighbour interface detected	The interface configuration to establish OSPF adjacency is inconsistent. the types of configuration errors include: – Inconsistent version number – Area mismatch – Unknown non-broadcast multiple access (NBMA) neighbour – Unknown virtual neighbour.		On-change

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
		– Inconsistent type of authentication configured – Authentication fails – Inconsistent mask configured – Inconsistent Hello time configured – Inconsistent Dead time configured – Inconsistent Option field configured – Inconsistent MTU configured – RouterID configuration conflicts – Unknown error		
	OSPF neighbour flapping suppression changed	OSPF neighbour flapping suppression changes: – OSPF interface is in the flapping suppression phase – OSPF interface exits the flapping suppression phase		On-change
	Routing loop detected	The device detects a loop in the route		On-change
	Prefix SID problems	1. Prefix SID conflicts 2. The received prefix SID exceeds the range of the local SRGB		Event-triggered
IP multicast	IGMP/MLD	1. The IGMP/MLD group memberships of the specified interface exceed the threshold, and discard the Report messages 2. The number of IGMP/MLD table entries of the specified interface reaches the upper threshold 3. Prompt on receiving IGMP/MLD group member Report message 4. Prompt on receiving IGMP/MLD group member Leave message 5. The IGMP version configured on the interface is inconsistent with the version of the Query message received		Event-triggered
	PIM	1. The number of PIM neighbours reaches the upper limit of system capacity. 2. PIM neighbour lost 3. The number of the global PIM table entries reaches the limit 4. The number of PIM multicast table entries in the VPN instance reaches the limit 5. Reverse path forwarding (RPF) routes flap, causing an alarm		Event-triggered
LDP	LDP session state changed	1. The LDP session state changes from UP to DOWN due to the receipt of wrong message or notification message: – Receives the message with wrong LDP ID – Receives the message with wrong version number – Receives the message with wrong PDU length – Receives the message with wrong packet length – Receives the message with wrong TLV value. – Receives Notification message about hello timeout – Receives Notification message about keepalive timeout		On-change

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
		– Receives Notification message about shutdown 2. The LDP session state changes from UP to DOWN due to TCP disconnection 3. The Hello hold timer for LDP session timed out 4. The Keepalive hold timer for LDP session timed out 5. Restarts LDP command 6. Configures graceful restart (GR) attribute of LDP session		
	The number of LDP labels exceeded	When the number of LDP labels exceeds the limit, an alarm will be generated.		Event-triggered
	LDP session deleted	An LDP session is deleted		Event-triggered
	LDP session security	The LDP session authentication fails		Event-triggered
MPLS-TE	RSVP status	1. RSVP is UP 2. RSVP is DOWN Telemetry data SHOULD carry the following tunnel attributes: – Tunnel ID – Tunnel ingress label switching router (LSR) ID – Tunnel Egress LSR ID		On-change
	MPLS-TE master and standby tunnel switching	1. The traffic is switched from the master tunnel to the hot-standby LSP 2. The traffic is switched from the hot-standby LSP to the master tunnel Telemetry data SHOULD carry the following tunnel attributes: – Master tunnel ID – Master tunnel ingress LSR ID – Master tunnel egress LSR ID – Master LSP protocol status – Standby LSP ID – Standby LSP protocol status – Switch reason		Event-triggered
SR/SRv6 POLICY	SR POLICY status changed	1. SR POLICY is UP 2. SR POLICY is DOWN Telemetry data SHOULD carry the following SR POLICY attributes: – SR POLICY name – SR POLICY endpoint address – SR POLICY colour – SR POLICY binding segment identification (BSID)		On-change
	BSID allocation failed	An allocation failure for the binding SID of SR policy is detected.		Event-triggered
EVPN	Types of EVPN routes	1. RT-1, Ethernet auto-discovery route 2. RT-2, MAC/IP advertisement route 3. RT-3, multicast Ethernet tag route 4. RT-4, Ethernet segment route 5. RT-5, IP prefix route	≤ 300	Periodic
	MAC address	Due to frequent MAC addresses migration in the		Event-triggered

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
	routes suppressed	specified EVPN instance, the routes corresponding to these MAC addresses are suppressed.		
	Loop detected	In the dual-homing scenario of EVPN E-Tree instance, the traffic loop occurs, due to the inconsistent leaf attribute configurations on the two dual-homing PEs.		Event-triggered
	Routes discarded	The newly learned MAC and MAC/IP routes are discarded in an EVPN instance		Event-triggered
	EVPN instance status changed	1. An EVPN instance state is DOWN 2. An EVPN instance state is UP		On-change
	Number of MAC addresses exceeded	The number of MAC addresses in the EVPN instance reaches the maximum		Event-triggered
L2VPN	PW status changed	PW state changes to DOWN/UP. Telemetry data SHOULD carry the following PW attributes: – Virtual circuit (VC) ID – Remote peer address – Type of PW encapsulation – Local VC label – Remote VC label The causes of PW DOWN include: – Local VC deleted – LDP session disconnected – LDP mapping interface parameters not matched – LDP Withdrawn message received – LDP Release message received – Interface down – Type of interface encapsulation changed – MTU not matched – Unknown cause		On-change
	Insufficient label blocks	1. An alarm is generated when the VPLS label blocks are insufficient 2. An alarm is generated when the VPWS label blocks are insufficient		Event-triggered
	PW protecting group fault	An alarm is generated when the working PW or protecting PW fails in the PW protecting group, carrying the parameters including: – VSI name – PW ID – Remote peer IP address – Possible cause		Event-triggered
	PW protection switching	1. The master PW switches to the standby PW 2. The standby PW switches to the master PW		Event-triggered
L3VPN	Number of routes exceeded	The number of IPv4/v6 routes in the VPN instance exceeds the configured maximum number of VPN routes		Event-triggered
	VRF binding interface status	The interface binding a VPN instance is DOWN		Event-triggered
	VPN tunnel status	An alarm is generated when the VPN tunnel is DOWN, carrying the following parameters:		On-change

Table 8-1 – Relevant telemetry data collection of the control aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
		– VPN ID – Outer tunnel ID – Next hop		
LLDP	Neighbour status	The neighbour status SHOULD include the following TLVs: – System name – System description – Chassis-id – Port-id – Time to live – Management address	≤ 60	Periodic
ARP	ARP table	Number of ARP entries cached by the specified interface Each ARP entry SHOULD contain the following parameters: – Interface name – MAC address – IPv4 address – Aging time of dynamic learning	≤ 300	Periodic
NDP	ND table	Number of ND entries stored by the specified interface Each ND entry SHOULD contain the following parameters: – Interface name – MAC address – IPv6 address – Aging time of dynamic learning	≤ 300	Periodic
BFD	BFD session status changed	An alarm is generated when the BFD session state changes, carrying the following parameters: 1) My discriminator 2) Your discriminator 3) Session state: – AdminDown – Down – Initiation – Up 4) The possible causes for session state change (Diagnostic word) include: – No diagnostic – Control Detection time expired – Echo function failed – Neighbour signalled session down – Forwarding plane reset – Path down – Concatenated path down – Administratively down – Reverse concatenated path down – Application remove		On-change

8.2 Capabilities for network visibility of the control aspect of bDDN

Network visibility of the control aspect includes mainly the following functions:

- Status data collecting: Collecting the running status data related to the main control protocols.
- Status data transforming: Transforming the collected status data to the format that big data plane of bDDN can easily understand.
- Running status visualizing: Visualizing the running status in the form of curves, tables, charts, etc.
- Running status tracking: Continually tracking the running status of the main control protocols.
- Running status predicting: Predicting the health trend of the running protocols based on the collected status data.

9 Requirements and capabilities for network visibility of the forwarding aspect of bDDN

Network visibility of the forwarding aspect of bDDN is also significant for operating and controlling the network (e.g., network planning, network optimization, traffic prediction, congestion avoidance and packet loss localizing). As an effective network data collection technique, 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. In addition, bDDN needs to support relevant capabilities for network visibility of the forwarding aspect.

9.1 Requirements for network visibility of the forwarding aspect of bDDN

– It is required to support the visibility of interface traffic statistics and status, including physical interface traffic statistics, sub-interface traffic statistics, interface status, sub-interface status, interface buffer/queue, interface packets discarded, etc.

– It is required to support the visibility of optical module performance.

– It is required to support the visibility of L2VPN traffic statistics.

– It is required to support the visibility of L3VPN traffic statistics.

– It is required to support the visibility of MPLS/SR-TE traffic statistics.

– It is required to support the visibility of SR/SRv6-policy TE traffic statistics.

– It is required to support the visibility of QoS queue information statistics.

– It is recommended to support the visibility of access control list (ACL) rules statistics.

– It is required to support the visibility of tow-way active measurement protocol (TWAMP) measured data.

– It is recommended to support the visibility of in-situ flow information telemetry (iFIT) measured data.

– It is recommended to support the visibility of in-situ operations, administration, and maintenance (IOAM) monitored data.

In order to achieve network visibility of forwarding aspect of bDDN, telemetry data collection of key forwarding performance is necessary. Table 9-1 presents relevant telemetry data collection of the forwarding aspect.

Table 9-1 – Relevant telemetry data collection of the forwarding aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
Interface	Physical interface traffic statistics	1. Number of inbound/outbound bytes 2. Number of in/out unicast packets 3. Number of in/out broadcast packets 4. Number of in/out multicast packets 5. Number of in/out discarded packets 6. Number of in/out error packets 7. Number of in/out packets 8. In/out utilization 9. In/out bit rate (Mbit/s) 10. In/out packet rate (kbit/s) 11. In/out IPv4 bytes 12. In/out IPv4 packets 13. In/out IPv4 bit rate (Mbit/s) 14. In/out IPv4 packet rate (kbit/s) 15. In/out IPv4 utilization 16. In/out IPv6 bytes 17. In/out IPv6 packets 18. In/out IPv6 bit rate (Mbit/s) 19. In/out IPv6 packets (kbit/s) 20. In/out IPv6 utilization	≤ 60	Periodic
	Sub-interface traffic statistics	1. Number of in/out bytes 2. Number of in/out unicast packets 3. Number of in/out broadcast packets 4. Number of in/out multicast packets 5. Number of in/out discarded packets 6. Number of in/out error packets 7. Number of in/out packets 8. In/out utilization 9. In/out bit rate (Mbit/s) 10. In/out packet rate (kbit/s) 11. In/out IPv4 bytes 12. In/out IPv4 packets 13. In/out IPv4 bit rate (Mbit/s) 14. In/out IPv4 packet rate (kbit/s) 15. In/out IPv4 utilization 16. In/out IPv6 bytes 17. In/out IPv6 packets 18. In/out IPv6 bit rate (Mbit/s) 19. In/out IPv6 packets rate (kbit/s) 20. In/out IPv6 utilization	≤ 60	Periodic
	Interface status	1. Type of interface encapsulation 2. Interface management state 3. Interface physical state 4. Interface layer 2 protocol state 5. Interface IPv4/v6 protocol state 6. Interface index		On-change

Table 9-1 – Relevant telemetry data collection of the forwarding aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
	Sub-interface status	1. Type of interface encapsulation 2. Interface management state 3. Interface physical state 4. Interface layer 2 protocol state 5. Interface IPv4/v6 protocol state 6. Interface index		On-change
	Interface buffer/queue	1. Current used buffers/depth 2. Queue threshold exceeded	≤ 60	Periodic Event-triggered
	Interface packets discarded	1. The time when packets are discarded 2. The causes of packets discarded: – due to queue overflow – due to cyclic redundancy check (CRC) error – due to forwarding failure (e.g., FIB match failed, ACL match failed, etc.).		Event-triggered
Optical module	Performance	1. Transmitting optical power 2. Receiving optical power 3. Optical module current (mA) 4. Optical module voltage (mV) 5. Optical module temperature (C°)	≤ 60	Periodic
	Performance abnormal	1. Transmitting optical power exceeds the limit 2. Receiving optical power exceeds the limit 3. Optical module current exceeds the limit 4. Optical module voltage exceeds the limit 5. Optical module temperature exceeds the limit		Event-triggered
PW	PW traffic statistics	1. PW name 2. VC ID 3. Number of in/out bytes 4. Number of in/out unknown unicast bytes 5. Number of in/out unicast bytes 6. Number of in/out broadcast bytes 7. Number of in/out multicast bytes 8. Number of in/out discarded bytes 9. Number of in/out packets 10. Number of in/out unknown unicast packets 11. Number of in/out unicast packets 12. Number of in/out broadcast packets 13. Number of in/out multicast packets 14. Number of in/out discarded packets 15. In/out utilization 16. In/out bit rate (Mbit/s) 17. In/out packets rate (kbit/s)	≤ 60	Periodic

Table 9-1 – Relevant telemetry data collection of the forwarding aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
L3VPN	VPN instance traffic statistics	1. VRF name 2. Number of in/out bytes 3. Number of in/out packets 4. Number of in/out discarded bytes 5. Number of in/out discarded packets 6. In/out bit rate (Mbit/s) 7. In/out packets rate (kbit/s)	≤ 60	Periodic
MPLS/SR-TE	TE traffic statistics	1. Tunnel ID 2. Number of Outbound bytes 3. Outbound packets 4. Outbound discarded bytes 5. Outbound discarded packets 6. Outbound bit rate (Mbit/s) 7. Outbound packets rate (kbit/s)	≤60	Periodic
SR/SRv6-Policy [b-IETF RFC 9256]	TE traffic statistics	1. Policy name 2. Number of Outbound bytes 3. Outbound packets 4. Outbound discarded bytes 5. Outbound discarded packets 6. Outbound bit rate (Mbit/s) 7. Outbound packets rate (kbit/s)	≤ 60	Periodic
QoS	Queue information statistics	1. Interface name 2. Queue ID 3. Committed information rate (CIR) 4. Peak information rate (PIR) 5. Maximum buffers 6. Current used buffers 7. Buffer utilization 8. Total packets passed 9. Total bytes passed 10. Discarded packets 11. Discarded bytes 12. Current bit rate passed (Mbit/s) 13. Current packets rate passed (kbit/s)	≤ 60	Periodic
ACL	ACL rules statistics	1. Interface ID 2. Maximum number of configurable ACL rules supported 3. Current number of the used ACL rules configured 4. ACL rules table	≤ 300	Periodic
STAMP/TWAMP [b-IETF RFC 5357]	Measured data	1. Connection ID 2. Measurement ID 3. Number of testing packets sent by client 4. Number of testing packets received by client 5. Discarded testing packets 6. Testing packet loss 7. Minimum bidirectional delay (ns) 8. Maximum bidirectional delay (ns)	According to testing duration	Periodic

Table 9-1 – Relevant telemetry data collection of the forwarding aspect

Data class	Data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, on-change or event-triggered)
		9. Average bidirectional delay (ns) 10. Minimum bidirectional delay jitter (ns) 11. Maximum bidirectional delay jitter (ns) 12. Average bidirectional delay jitter (ns) 13. Minimum forward delay (ns) 14. Maximum forward delay (ns) 15. Average forward delay (ns) 16. Minimum forward delay jitter (ns) 17. Maximum forward delay jitter (ns) 18. Average forward delay jitter (ns) 19. Minimum reverse delay (ns) 20. Maximum reverse delay (ns) 21. Average reverse delay (ns) 22. Minimum reverse delay jitter (ns) 23. Maximum reverse delay jitter (ns) 24. Average reverse delay jitter (ns)		
Alternate-Marking [b-IETF RFC 9341]	Measured data	1. Flow ID 2. Testing duration ID 3. Node ID 4. Number of packets 5. Number of bytes 6. Timestamp	According to testing duration	Periodic
IOAM	Measured data for passport mode [b-IETF RFC 9197]	1. IOAM namespace ID 2. Node ID 3. TTL or Hop Limit 4. Ingress interface ID 5. Egress interface ID 6. Timestamp 7. Forwarding delay 8. Queue depth 9. Buffer occupation	According to testing duration	Periodic
	Measured data for postcard mode [b-IETF RFC 9326]	1. IOAM namespace ID 2. Flow ID 3. Sequence Number 4. TTL or Hop Limit 5. Node ID 6. Ingress interface ID 7. Egress interface ID 8. Timestamp 9. Forwarding delay 10. Queue depth 11. Buffer occupation	According to testing duration	Periodic

9.2 Capabilities for network visibility of the forwarding aspect of bDDN

Network visibility of the forwarding aspect includes mainly the following functions:

- Data collection configuring: Selecting, on-demand, which class of telemetry data should be collected.

- Data collecting: Collecting the telemetry data related to the forwarding aspect.
- Data transforming: Transforming the collected data to the format that the big data plane of bDDN can easily understand.
- Data statistics and visualization: Making the statistics of traffic and performance data, and visualizing the statistical data in the form of curves, tables, charts, etc.
- Traffic predicting: Predicting network traffic trend based on traffic statistics.
- Congestion and link quality management: managing network congestion level and link quality level based on performance data statistics.

10 Requirements and capabilities for network visibility of the management aspect of bDDN

Network visibility of the management aspect of bDDN is beneficial to network OAM such as troubleshooting, root cause analysis and event tracking. The management plane should provide network performance data, network logging data, device status data, fault, security, etc. Therefore, the management entity needs to support relevant requirements and capabilities for network visibility.

10.1 Requirements for network visibility of the management aspect of bDDN

– It is required to support the visibility of device performance, including central processing unit (CPU), memory, power supply, fan, temperature, etc.

– It is required to support the visibility of device fault alarms.

– It is required to support the visibility of device security, including security management of user login, CPU safety protection.

– It is recommended to support the visibility of telemetry dynamic subscription management.

To achieve network visibility of management aspect of bDDN, telemetry data collection of key management indicators is necessary. Table 10-1 presents relevant telemetry data collection of the management aspect.

Table 10-1 – Relevant telemetry data collection of the management aspect

Data class	data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, On-change or event-triggered)
Performance	CPU	1. CPU utilization 2. CPU utilization reaches overload threshold 3. CPU working status	≤ 30 ≤ 30	Periodic Event-triggered Event-triggered
	Memory	1. Memory utilization 2. Memory utilization reaches overload threshold 3. Memory working status	≤ 30 ≤ 30	Periodic Event-triggered Event-triggered
	Power supply	1. Power 2. Voltage 3. Current 4. Power working status	≤ 30 ≤ 30 ≤ 30 ≤ 30	Periodic Periodic Periodic Event-triggered
	Fan	1. Fan speed 2. Fan working status	≤ 30 ≤ 30	Periodic Event-triggered
	Temperature	1. CPU temperature 2. Fan temperature 3. Temperature reaches the threshold	≤ 30 ≤ 30	Periodic Periodic Event-triggered
Fault	Fault alarm	1. System restart 2. Device fault (CPU, memory, power supply, fan, etc.)		Event-triggered

Table 10-1 – Relevant telemetry data collection of the management aspect

Data class	data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, On-change or event-triggered)
		3. Board hardware fault 4. Operating system fault 5. Interface fault 6. Link fault 7. Licence expired 8. Protection switching		
Security	Security management of user login	1. The number of login failures reaches the threshold within a period of time 2. Add a user, including parameters: − Operator name − Operator's IP address − New username 3. Delete a user, including parameters: − Operator name − Operator's IP address − User name deleted 4. The user password has expired, including parameters: − Username 5. The user has been locked, including parameters: − Number of consecutive login failures − Statistical time of consecutive login failures − Locked time − Type of user access. 6. Locked user is released, including parameters: − Username − Unlocking mode (automatic or manual)		Event-triggered
	CPU safety protection	1. An attack on the CPU is detected. The attack type includes: − TCP − UDP − ICMP − ARP − NDP − DHCP − DNS 2. Number of the discarded packets generated by tackling CPU attack packets.		Event-triggered
Telemetry	Dynamic subscription management	1. User login fails, including parameters: − Username − User's IP address − Port number − VPN instance name − Cause of login failure 2. User login succeeds, including parameters: − Username − User's IP address − Port number		Event-triggered

Table 10-1 – Relevant telemetry data collection of the management aspect

Data class	data item	Contents of data collection	Sampling interval (second)	types of subscription (periodic, On-change or event-triggered)
		– VPN instance name 3. Dynamic subscription fails. the possible causes include: – Sampling nodes/group (filters) not supported – Subscription parameters not supported – Insufficient resources – Transport encoding not supported – QoS not supported 4. Dynamic subscription disconnects. The possible causes include: – Remote process call (RPC) execution error – Google remote procedure calls (GRPC) internal execution error – The submitted contents not recognized – GRPC fails to parse the submitted contents		

10.2 Capabilities for network visibility of the management aspect of bDDN

Network visibility of management aspect mainly includes the following functions:

- Management data collecting: Collecting the configuration, performance, fault alarms and security data related to management aspect.
- Management data transforming: Transforming the collected management data to the format that the big data plane of bDDN can easily understand.
- Management data visualizing: Visualizing the collected management data in the form of curves, tables, charts, etc.
- Network device management: Managing the device running status based on the collected management data.
- Network device security management: Managing device operating security based on the collected management data.

11 Interface requirements for network visibilityof bDDN

According to the framework of bDDN [ITU-T Y.3650], there are several interfaces between different planes or between different layers. However, this Recommendation mainly specifies the requirements of interfaces between the data sensing layer of the big data plane and the network infrastructure layer of the network plane named as iBN, as shown in Figure 11-1. The iBN can be implemented network configuration protocol (NETCONF), gNMI, UDP-based publication channel (UPC), BGP monitoring protocol (BMP), BGP-LS, SNMP, Syslog, IP flow information export (IPFIX), etc. The requirements for these interfaces are described in clauses 11.1 to 11.6.

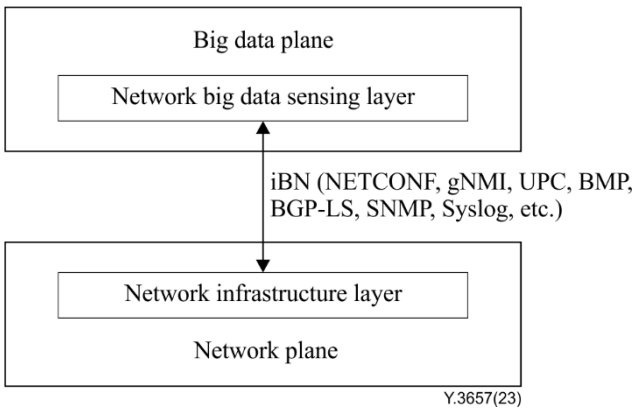

Figure 11-1 – Interface between network sensing layer and network infrastructure layer

11.1 NETCONF

The NETCONF [b-IETF RFC 6241] protocol defines a simple mechanism through which a network device can be managed, configuration data information can be retrieved, and notification data information can be subscribed. NETCONF uses a simple RPC-based mechanism to facilitate communication between a client and a server.

– NETCONF is required to support dynamic subscriptions, where a subscriber initiates a subscription negotiation with a publisher via an RPC. If the publisher is able to serve this request, it accepts it and then starts pushing notification messages back to the subscriber. If the publisher is not able to serve it as requested, then an error response is returned. This response may include hints for subscription parameters that, had they been present, may have enabled the dynamic subscription request to be accepted. The lifetime of a dynamic subscription is bound by the transport session used to establish it, and the loss of the transport session will result in the immediate termination of any associated dynamic subscriptions.

– NETCONF is required to support configured subscriptions, which allow the management of subscriptions via a configuration so that a publisher can send notification messages to a receiver. Configured subscriptions can be configured to persist across reboots and even when its publisher is fully disconnected from any network.

– NETCONF is required to support the ability to create, renew, time out, and terminate a subscription.

– NETCONF is required to support and independently track multiple subscription requests by the same Subscriber.

– NETCONF is required to support subscriptions against operational datastores, configuration datastores, or both.

– NETCONF may include Filters as defined within a subscription request, therefore the Subscription Service MUST publish only data nodes that meet the Filter criteria within a subscription.

– NETCONF is required to support the ability to subscribe to periodic updates. The subscription period shall be configurable as part of the subscription request.

– NETCONF is required to support the ability to subscribe to updates on-change, i.e., whenever values of subscribed data objects change.

– For on-change updates, NETCONF is required to support a dampening period that needs to be passed before the subsequent on-change updates are sent. The dampening period should be configurable as part of the subscription request.

– NETCONF is required to support the ability to subscribe to the adaptive updates for interface traffic collection. In order to capture the congestion state of interfaces, such as microburst, a（i.e., subscription period）sub-second level sampling interval, or even a millisecond level sampling interval is necessary. However, under normal network conditions, a minute-level sampling interval can satisfy the requirements for traffic visibility, thus reducing enormously resources occupancy.

  1) The network device is required to support determining the interface traffic sampling interval based on the current output queue length, which is detected by a dedicated hardware chip in real time. The longer the output queue, the shorter the sampling interval is. When the output queue is less than the preset safety threshold, a minute-level sampling interval is adopted; otherwise, a sub-second level sampling interval or even a millisecond-level sampling interval is adopted, whose parameter is negatively correlated with the difference between the current output queue length and the safety threshold.

  2) The network device is required to support determining the interface traffic sampling interval based on the current output packet drop, which is detected by the dedicated hardware chip in real time. As soon as packet drop occurs, the sampling interval must be adjusted to a sub-second or even millisecond level.

  3) The network device is required to support determining the interface traffic sampling interval based on the current port utilization, which is detected (i.e., millisecond interval) by the dedicated hardware in real time. The higher the port utilization, the shorter the sampling interval is. When the port utilization is less than the preset safety threshold, a minute-level sampling interval adopted; otherwise, a sub-second level sampling interval or even a millisecond level sampling interval is adopted, whose parameter depends on the corresponding port utilization threshold.

– NETCONF is required to support the termination of a subscription when requested by the subscriber.

– NETCONF is required to support the ability to suspend and to resume a subscription on request of a client.

– NETCONF may on self-determination to suspend an existing subscription. Reasons may include transitory resource limitation, credential expiry, failure to reconfirm a subscription, loss of connectivity with the receiver, etc. When this occurs, the subscription service must notify the subscriber and update the subscription status.

– NETCONF is required to support subscription to yet another next generation (YANG) notifications defined in [b-IETF RFC 8639].

– NETCONF is required to support subscription to YANG-push defined in [b-IETF RFC 8641].

11.2 gRPC network management interface (gNMI)

The gRPC network management interface (gNMI) [b-GNMI-SPEC] supports modification and retrieval of configuration, as well as telemetry streams from a network element to a data collection system. gNMI derives a number of benefits from being built on gRPC and HTTP/2, including modern security mechanisms, bidirectional streaming, binary framing and a wide variety of language bindings to simplify integration with management applications. With protobuf encoding, it also provides significant efficiency advantages over extensible markup language (XML) serialization with a 3 to 10 times reduction in data volume.

The conceptual layers and requirements for gNMI serving as the collection and encapsulation of telemetry data are depicted as Table 11-1.

Table 11-1 – Conceptual layers and requirements for gNMI serving as the collection and encapsulation of telemetry data

Layer		Requirements
Data model	Service data	Must include the service data from the specified paths.
	Telemetry header	Must include timestamp, the time when the device collects the service data, and the paths from which the service data originates.
gRPC		gRPC is required to provide the following RPCs: • Capabilities, used by the client and target as an initial handshake to exchange capability information. • Get, used to retrieve snapshots of the data on the target by the client. • Set, used by the client to modify the state of the target. • Subscribe, used to control subscriptions to data on the target by the client.
HTTP/2		HTTP/2 is required to support header field compression and binary framing, allowing multiple concurrent exchanges on the same connection.
Secure transport based on TCP		gNMI connection is required to provide authentication, data integrity, confidentiality, and replay protection (e.g., Transport layer security (TLS) [b-IETF RFC 5246].

– gNMI is required to support the ability to create, renew, time out, and terminate a subscription.

– gNMI is required to support an add/change/deletion of subscriptions.

– gNMI may include filters as defined within a subscription request, therefore the Subscription Service must publish only data nodes that meet the filter criteria within a subscription.

– gNMI is required to support STREAM subscription, a long-lived subscription which continues to transmit updates relating to the set of paths that are covered within the subscription indefinitely. STREAM subscription includes one of the following modes:

  • On change-data updates are only sent when the value of the data item changes. For all On-change subscription, the target must first generate updates for all paths that match the subscription path(s), and transmit them. Following this initial set of updates, updated values should only be transmitted when their value changes. A heartbeat interval may be specified along with an "on change" subscription. In this case, the value of the data item(s) must be re-sent once per heartbeat interval regardless of whether the value has changed or not.

  • Sampled-the value of the data item(s) must be sent once per sample interval to the client. Optionally, the suppress_redundant field of the Subscription message may be set for a sampled subscription. In the case, the target Should Not generate a telemetry update message unless the value of the specified path has changed.

– gNMI is required to support POLL subscription, used for on-demand retrieval of data items via long-lived RPCs. On reception of such a "SubscribeRequest" message containing a poll field, the target MUST generate updates for all the corresponding paths.

– gNMI is required to support the ability to subscribe to the adaptive updates for interface traffic collection. In order to capture the congestion state of interface such as microburst, a sampling interval（i.e., subscription period）of sub-second level, or even millisecond level is necessary. However, under normal network condition, the sampling interval of minute level can satisfy the requirements for the traffic visibility, thus reducing resources occupancy enormously.

  1) The network device is required to support determining the interface traffic sampling interval based on the current output queue length, which is detected by the dedicated

hardware chip in real time. The longer the output queue, the shorter the sampling interval is. When the output queue is less than the preset safety threshold, minute level sampling interval is adopted; otherwise, a sub-second level sampling interval or even a millisecond level sampling interval is adopted, whose parameter is negatively correlated with the difference between the current output queue length and the safety threshold.

2) The network device is required to support determining the interface traffic sampling interval based on the current output packet drop, which is detected by the dedicated hardware in real time. As soon as packet drop occurs, the sampling interval must be adjusted to the sub-second or even the millisecond level according to the subscription period.

3) The network device is required to leverage the dedicated hardware chip to detect interface traffic at millisecond interval periodically. Among the multiple traffic thresholds in ascending order and corresponding sampling intervals acquired from subscription configuration message by the dedicated hardware chip, the higher the traffic threshold, the shorter the sampling interval is. The minimal threshold (i.e., safety threshold) corresponds to a minute-level sampling interval, and other thresholds correspond to the second, sub-second and millisecond level sampling intervals. The dedicated hardware chip compares the interface traffic with the preset multiple traffic thresholds to determine the traffic sampling interval. When the interface traffic (bandwidth utilization) is less than the preset safety threshold, a minute-level sampling interval is adopted; otherwise, a second, sub-second or even millisecond level sampling interval is adopted, whose parameter depends on the corresponding preset traffic threshold when interface traffic reaches it for a specified time (i.e., time threshold acquired from subscription configuration message).

– gNMI is required to support structured data sent by the client or the target in an Update message, which MUST be serialized according to one of the supported encodings.

– gNMI is required to support Protobuf and JSON encoded, and ASCII encoded is optional.

11.3 UDP based publication channel (UPC)

NETCONF and gNMI are ultimately based on the transfer control protocol (TCP) and lack the efficiency needed to stream data continuously at high velocity. On the other hand, in the case of data originating from multiple line cards of a single device, the centralized data collection mechanism such as NETCONF or gNMI requires data to be internally forwarded from those line cards to the main controller board, which then combines the individual data items into a single consolidated stream, resulting in a performance bottleneck, especially when large amounts of data is needed. What is needed instead is the support for a distributed mechanism that allows to directly push multiple individual substreams, e.g., one from each line card, but still allowing those substreams to be managed and controlled via a single subscription. UPC [b-IETF UPC] natively supports the distributed data collection mechanism.

For dynamic subscription, in the case that a receiver (subscriber) is associated with multiple data originators, and notification messages are pushed on separate channels, all publication channels must share the same subscription session.

For a configured subscription, the subscription configuration for every publication channel must contain the receiver's IP address and port number as destination IP address and port number.

11.4 BGP-LS

BGP-LS [b-IETF RFC 7752] specifies a mechanism by which link-state and TE information can be collected from networks and shared with external components using the BGP routing protocol. This is achieved using a new BGP network layer reachability information (NLRI) encoding format. A

router maintains one or more databases for storing link-state information about nodes and links in any given area. Link attributes stored in these databases include local/remote IP addresses, local/remote interface identifiers, link metric, and TE metric, link bandwidth, reservable bandwidth, per class-of-service (CoS) class reservation state, preemption, and shared risk link groups (SRLGs). A BGP speaker may distribute the real physical topology from the link state database (LSDB) or the traffic engineering database (TED). Also, it may create an abstracted topology such as network slice, where virtual nodes are connected by virtual paths.

With the aid of BGP-LS, the big data plane can retrieve the complete topological visibility within a "domain" (such as an interior gateway protocol (IGP) area) or across multiple domains such as a multi-area autonomous system (AS) or multiple ASs. When the whole network topological visibility is transmitted to the network plane, the network controller can determine the end-to-end MPLS-TE path across IGP areas or ASs and can even select the right exit router such as area border router (ABR) or autonomous system border router (ASBR) for an optimal path. However, without the network controller, the source router could only compute the path for the first area because the router only has full topological visibility for the first area along the path.

– bDDN is required to support BGP-LS for network topological visibility. Network devices (e.g., routers) from the network infrastructure layer act as BGP-LS producer, originating link-state information from their underlying link-state IGP protocols into BGP-LS. And the big data plane acts as BGP-LS consumer, handing off the BGP-LS information that they have collected to a consumer application; also, as BGP-LS propagator, propagating the BGP-LS information to the network controller layer of the network plane for path computation and so on.

11.5 BMP

The BGP monitoring protocol (BMP) [b-IETF RFC 7854] can be used to monitor BGP sessions and obtain BGP route views. BMP provides access to the Adj-RIB-In of a peer on an ongoing basis and a periodic dump of certain statistics the monitoring station can use for further analysis.

– bDDN is required to support BMP for the visibility of BGP routes and BGP sessions state, including:

  • Route monitoring: Used to provide an initial dump of all routes received from a peer, as well as an ongoing mechanism that sends the incremental routes advertised and withdrawn by a peer to the monitoring station.

  • Route mirroring: A means of providing a full-fidelity view of all messages received from its peers, for the purpose of error reporting and diagnosis.

  • Statistics reports: An ongoing dump of statistics that can be used by the monitoring station as a high-level indication, including the number of routes in Adj-RIBs-In, the number of routes in Loc-RIB, the number of prefixes rejected by inbound policy, the number of prefixes subjected to treat-as-withdraw treatment, the number of prefixes invalidated due to AS_PATH loop, etc.

  • Peer down notification: A message sent to indicate that a peering session has gone down, with information indicating the reason for the session disconnect.

  • Peer up notification: A message sent to indicate that a peering session has come up.

11.6 Other interfaces

Several conventional techniques and protocols supporting network data collection (e.g., SNMP, Syslog, and IPFIX) have been widely deployed. Based on a large amount of OAM data obtained from these interfaces, network operators can monitor network health status, make troubleshooting, analyse network traffic flows, manage routine operation and maintenance, etc.

The simple network management protocol (SNMP) [b-IETF RFC 3416] uses a polling-based method to periodically retrieve network data, such as interface traffic statistics. Also, SNMP employs event management information base (MIB) and alarm management information base (MIB) (i.e., SNMP trap) to push management plane warnings.

– bDDN is required to support SNMP until it has been completely replaced by network telemetry techniques.

The Syslog protocol [b-IETF RFC 5424] specifies the standard format for syslog messages and is used to convey event notification messages, including interface UP and DOWN, the running status of signalling and control protocol, abnormal login, hardware or software failure, etc. During the runtime of network devices, the log module in the host software will record various conditions, so as to form log information transmitted to a syslog server for analysis. It mainly provides convenience for operators to retrieve the running status of network devices, diagnose network fault and analyse the root causes of failures.

– bDDN is required to support Syslog for log analysis.

IP flow information export (IPFIX) [b-IETF RFC 7011] provides a means of transmitting traffic flow information for administrative or other purposes. IPFIX data enables numerous critical applications, such as usage-based accounting, traffic profiling, traffic engineering, network security, QoS monitoring, and so on. Hence its value is highly weighed by internet service providers (ISPs).

– bDDN is required to support IPFIX for traffic flow visibility.

12 Requirements for network visibility of other aspects

12.1 Requirements for the visibility of real-time congestion

Congestion is a common phenomenon in IP networks. Network congestion leads to the deterioration of network performance and increases the uncertainty of service delivery. In order to reduce the uncertain services caused by network congestion, it is necessary to monitor the status and trend of network congestion in real-time manner, evaluate network congestion level. And the visibility of real-time congestion will provide the accurate basis for network planning, capacity expansion and optimization.

1) Requirements for the network infrastructure layer

The network infrastructure layer includes all kinds of IP network devices implementing packet forwarding.

– The network infrastructure layer is required to support dynamic subscription or configured subscription, serving as a publisher that can send notification messages to a receiver. It accepts subscription services from the big data plane and sends telemetry data according to the subscription requests.

– The network infrastructure layer device is required to support sending interface congestion state data to the big data plane in real-time manner, including packet loss data caused by queue overflow or/and queue depth data, in the case of the congestion conditions satisfied.

– The network infrastructure layer device is required to leverage built-in dedicated hardware chip to detect interface congestion state at millisecond interval periodically, including packet loss by queue overflow or/and queue depth., in the case of the congestion conditions satisfied, that is, when the number of dropped packets caused by queue overflow is greater than the preset threshold (e.g., 0), or queue depth is greater than the preset threshold, it must send the corresponding congestion state data to CPU of main control card or line card in real time, which encapsulates them as telemetry packets with the timestamp of congestion occurrence and then sends them to the big data plane. Also, the interface congestion state

data must carry congestion location information including device ID, interface ID and queue ID.

– The network infrastructure layer device is required to support sending the congestion state data via the dedicated hardware chip to management or control entity (CPU) in on-change mode, which encapsulates it as telemetry data to the big data plane. For on-change updates, it is required to support a dampening period that needs to be passed before the subsequent on-change updates are sent. The dampening period should be configurable as part of the subscription request. Compared with periodic updates, on-change updates can cut down data volume sent greatly.

– The network infrastructure layer device is also required to configure management or control entity (CPU) to collect interface traffic statistics at minute-level interval periodically.

2) Requirements for the big data plane

– The big data plane is required to support dynamic subscriptions or configured subscriptions, serving as a subscriber that can accept notification messages from a publisher.

– The network big data sensing layer is required to collect congestion state data from the network infrastructure layer in real-time manner. Also, it is required to collect interface traffic statistics at minute-level interval periodically.

– The network big data repository layer is recommended to store the aforementioned congestion state data and interface traffic statistics for at least a month.

– The network big data analyser layer is required to perform real-time computation and analysis of the collected data. Some data analysis methods such as statistical analytical method, visualization analytical method, correlation analytical method are necessary.

– The data intelligence and service layer is required to support the real-time visualization of interface congestion state data and traffic data. Visualization should exhibit interface congestion state and traffic data in the form of curves, tables, charts and topology maps, etc., so that network operators can see and understand it intuitively. Figure 12-1 is an example of interface packet loss chart, Figure 12-2 is an example of interface queue depth chart, and Figure 12-3 is an example of interface traffic curve. Figure 12-4 is an example of network topology map with the congested interface on real-time display in bright red colour.

– Data intelligence and service layer is required to provide the network plane with real-time congestion status and trend, so that those key traffic flows can be optimized promptly.

– Data intelligence and service layer is also required to provide the management plane with interface traffic statistics, so that the capacity expansion and optimization can be evaluated appropriately.

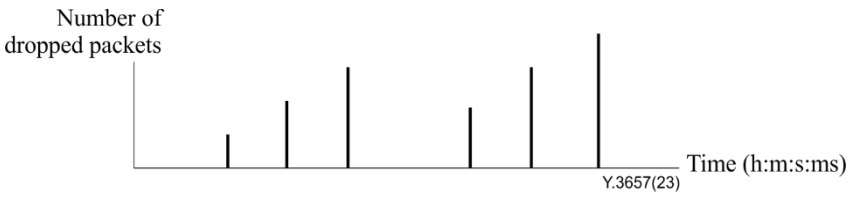

Figure 12-1 – An example of interface packet loss chart

Figure 12-2 – An example of interface queue depth chart

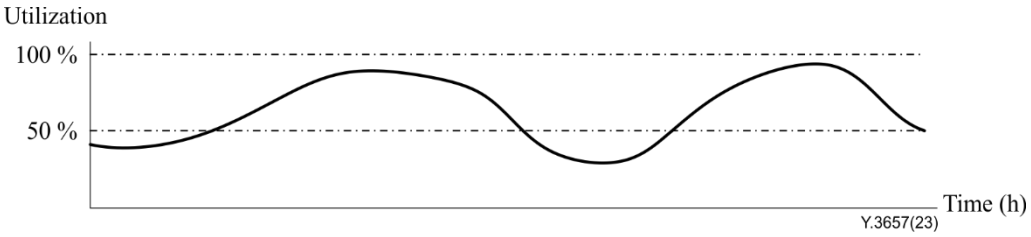

Figure 12-3 – An example of interface traffic curve

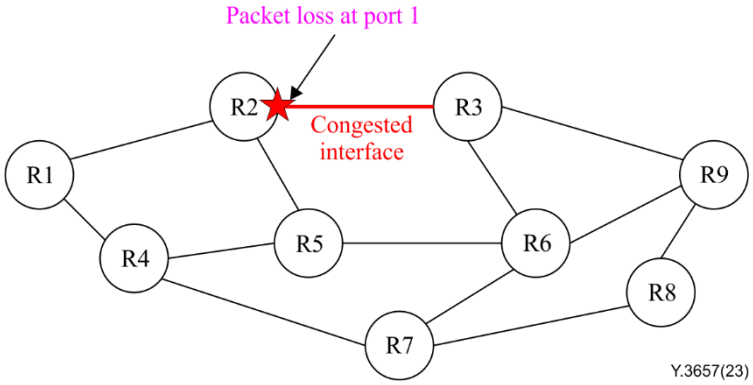

Figure 12-4 – An example of network topology with the congested interface on real-time displayed in bright red colour

12.2 Requirements for the visibility of real-time link quality

The link quality of IP bearer network plays a key role in network transmission performance. The degradation of link quality will lead to the increase of transmission bit error rate (BER), which will convert to cyclic redundancy check (CRC) error packets discarded by the network forwarding device. The increase of network packet loss rate will affect the quality of service, especially to applications with sensitivity of packet loss. It is necessary to monitor the status and degradation trend of link quality in real-time manner and evaluate the level of link quality. Furthermore, the visibility of real-time link quality will help network operators improve the efficiency of fault diagnosis and root cause analysis.

1) Requirements for the network infrastructure layer

The network infrastructure layer includes all kinds of network devices performing packet forwarding.

– The network infrastructure layer device is required to support dynamic subscriptions or configured subscriptions, serving as a publisher that can send notification messages to a receiver. It accepts subscriptions services from the big data plane and sends telemetry data according to the subscription requests.

– The network infrastructure layer device is required to support sending port link quality data to the big data plane periodically, including the number of CRC error packets of interface, transmitting optical power of optical module, receiving optical power of optical module.

Also, the suppress_redundant function is needed, so that it should not generate a telemetry update message unless the value of the subscribed data object has changed.

– The network infrastructure layer device is required to support sending the corresponding telemetry data to the big data plane in on-change mode, i.e., whenever values of subscribed data objects change. For on-change updates, it is required to support a dampening period that needs to be passed before the subsequent on-change updates are sent. The dampening period should be configurable as part of the subscription request. Compared with periodic updates, on-change updates can cut down data volume sent greatly.

– The network infrastructure layer device is required to support sending the corresponding telemetry data to the big data plane based on the threshold triggered. That is, when the number of CRC error packets, or the transmitting optical power, or the receiving optical power exceeds its preset threshold, respectively, a warning telemetry update must be generated. The update frequency should be configurable as part of the subscription request.

– The network infrastructure layer device is required to encapsulate the aforementioned data as telemetry packets, which carry information including timestamp, device ID and interface ID.

2) Requirements for the big data plane

– The big data plane is required to support dynamic subscriptions or configured subscriptions, serving as a subscriber that can accept notification messages from a publisher.

– Network big data sensing layer is required to support the following three subscription modes for collecting link quality data from the network device:

  • Periodic update.
  • On-change update.
  • Update based on the threshold triggered.

– The network big data repository layer is recommended to store link quality data for at least a month.

– The network big data analyser layer is required to perform real-time computation and analysis of the collected link quality data, including the number of CRC error packets, transmitting optical power and receiving optical power, to determine the port link quality. Some data analysis methods such as statistical analytical method, visualization analytical method, correlation analytical method are necessary.

– The network big data analyser layer is required to make intelligent analysis of the collected link quality data as follows:

  • If the collected data of receiving optical power of optical module deviates from the normal working range, susceptible to transmission BER, also, the number of CRC error packets is increasing, though not beyond the threshold (as shown in Figure 12-5 and Figure 12-6), this port link is determined to be abnormal due to an optical module problem.
  • If both the collected data of receiving optical power of optical module and those of the number of CRC error packets are all warning data triggered by the respective threshold, this port link is determined to be abnormal due to optical power of optical module problem.
  • If the number of CRC error packets is increasing, but the collected data of receiving optical power of optical module are in the normal working range, this port link is determined to be abnormal due to improper configuration or loose contact of interface.
  • If the collected data of transmitting optical power of optical module deviates from the normal working range, or are warning data triggered by the threshold, it will have

influence on packet receiving of the connected device, and this port link is determined to be abnormal due to transmitting optical power of optical module problem.

– Data intelligence and service layer is required to support the visualization of link quality data. Visualization should exhibit link quality state and degradation trend in the form of curves, tables, charts and maps, etc., so that network operators can see and understand it intuitively. Figure 12-5 is an example of curve for the collected data of interface CRC error packets, Figure 12-6 is an example of curve for the collected data of receiving optical power of optical module, and Figure 12-7 is an example of network topology with the link quality on real-time display in bright red colour.

– Data intelligence and service layer is required to provide the network plane with the real-time link quality status and trend, so that network operators can make traffic rerouting or optimization promptly.

– Data intelligence and service layer is also required to provide the management plane with the real-time link quality status and trend, so that network operators can make fault diagnosis and troubleshooting rapidly.

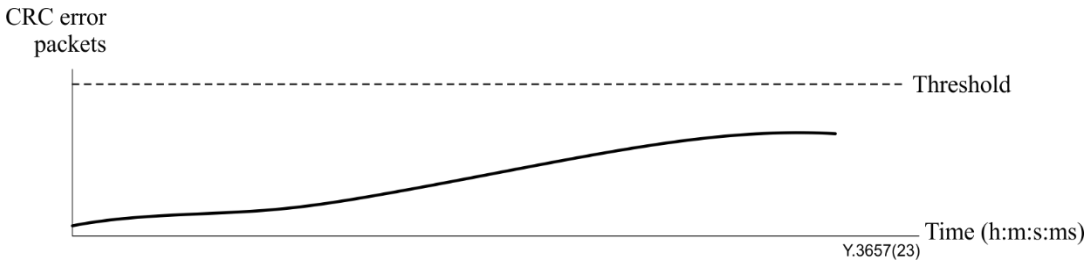

Figure 12-5 – An example of curve for the collected data of interface CRC error packets

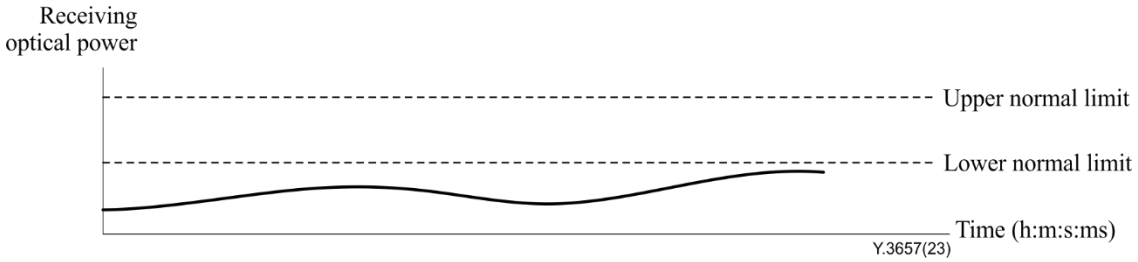

Figure 12-6 – An example of curve for the collected data of receiving optical power of optical module

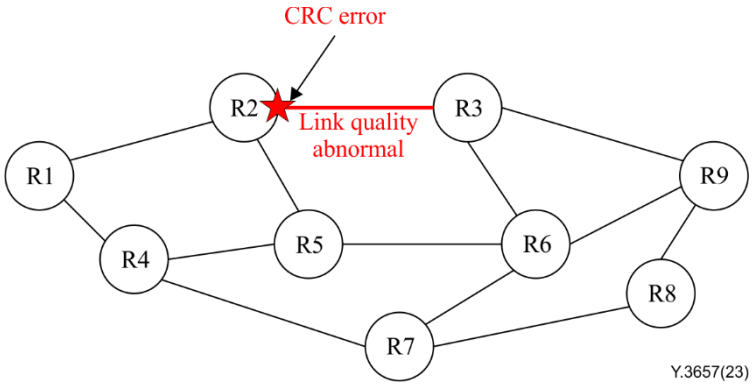

Figure 12-7 – An example of network topology with the link quality on real-time display in bright red colour

13 Security considerations

When implementing network visibility in bDDN, security best practices should be adopted such as authentication, authorization and access control and described in [ITU-T Y.2704].

Bibliography

[b-IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol* Version 1.2.

[b-IETF RFC 5357] IETF RFC 5357 (2008), *A Two-Way Active Measurement Protocol (TWAMP)*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-IETF RFC 6241] IETF RFC 6241 (2011), *Network Configuration Protocol (NETCONF)*.

[b-IETF RFC 7011] IETF RFC 7011 (2013), *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information*.

[b-IETF RFC 7432] IETF RFC 7432 (2015), *BGP MPLS-Based Ethernet VPN*.

[b-IETF RFC 7752] IETF RFC 7752 (2016), *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*.

[b-IETF RFC 7854] IETF RFC 7854 (2016), *BGP Monitoring Protocol (BMP)*.

[b-IETF RFC 8639] IETF RFC 8639 (2019), *Subscription to YANG Notifications*.

[b-IETF RFC 8641] IETF RFC 8641 (2019), *Subscription to YANG Notifications for Datastore Updates*.

[b-IETF RFC 9197] IETF RFC 9197 (2022), *Data Fields for In Situ Operations, Administration, and Maintenance (IOAM)*.

[b-IETF RFC 9232] IETF RFC 9232 (2022), *Network Telemetry Framework*.

[b-IETF RFC 9256] IETF RFC 9256 (2022), *Segment Routing Policy Architecture*.

[b-IETF RFC 9326] IETF RFC 9326 (2022), *In Situ Operations, Administration, and Maintenance (IOAM) Direct Exporting*.

[b-IETF RFC 9341] IETF RFC 9341 (2022), *Alternate-Marking Method*.

[b-IETF RFC 9343] IETF RFC 9343 (2022), *IPv6 Application of the Alternate-Marking Method*.

[b-GNMI-SPEC] GNMI-SPEC (2018), *OpenConfig operator working group, gRPC Network Management Interface (gNMI)* v0.6.0.

[b-IETF UPC] IETF UPC (2020), *UDP based Publication Channel for Streaming Telemetry. Work in progress*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
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	Environment and ICTs, climate change, e-waste, energy efficiency; 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, and associated measurements and tests
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, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Published in Switzerland
Geneva, 2024