

**ITU-T**

TELECOMMUNICATION  
STANDARDIZATION SECTOR  
OF ITU

**Y.3180**

(02/2022)

SERIES Y: GLOBAL INFORMATION  
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,  
NEXT-GENERATION NETWORKS, INTERNET OF  
THINGS AND SMART CITIES

Future networks

---

**Mechanism of traffic awareness for application-  
descriptor-agnostic traffic based on machine  
learning**

Recommendation ITU-T Y.3180

# ITU-T Y-SERIES RECOMMENDATIONS

## GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

### GLOBAL INFORMATION INFRASTRUCTURE

|                                           |             |
|-------------------------------------------|-------------|
| General                                   | Y.100–Y.199 |
| Services, applications and middleware     | Y.200–Y.299 |
| Network aspects                           | Y.300–Y.399 |
| Interfaces and protocols                  | Y.400–Y.499 |
| Numbering, addressing and naming          | Y.500–Y.599 |
| Operation, administration and maintenance | Y.600–Y.699 |
| Security                                  | Y.700–Y.799 |
| Performances                              | Y.800–Y.899 |

### INTERNET PROTOCOL ASPECTS

|                                                                    |               |
|--------------------------------------------------------------------|---------------|
| General                                                            | Y.1000–Y.1099 |
| Services and applications                                          | Y.1100–Y.1199 |
| Architecture, access, network capabilities and resource management | Y.1200–Y.1299 |
| Transport                                                          | Y.1300–Y.1399 |
| Interworking                                                       | Y.1400–Y.1499 |
| Quality of service and network performance                         | Y.1500–Y.1599 |
| Signalling                                                         | Y.1600–Y.1699 |
| Operation, administration and maintenance                          | Y.1700–Y.1799 |
| Charging                                                           | Y.1800–Y.1899 |
| IPTV over NGN                                                      | Y.1900–Y.1999 |

### NEXT GENERATION NETWORKS

|                                                                   |               |
|-------------------------------------------------------------------|---------------|
| Frameworks and functional architecture models                     | Y.2000–Y.2099 |
| Quality of Service and performance                                | Y.2100–Y.2199 |
| Service aspects: Service capabilities and service architecture    | Y.2200–Y.2249 |
| Service aspects: Interoperability of services and networks in NGN | Y.2250–Y.2299 |
| 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

|                                                         |               |
|---------------------------------------------------------|---------------|
| 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.3180

## Mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning

### Summary

Recommendation ITU-T Y.3180 specifies the mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning. This Recommendation specifies the following aspects related to traffic awareness for application-descriptor-agnostic traffic including an overview, general mechanism, used machine learning methods, implementation consideration based on machine learning, report and auxiliary control mechanism for the malicious application-descriptor-agnostic traffic and security considerations.

### History

| Edition | Recommendation | Approval   | Study Group | Unique ID*                                                                |
|---------|----------------|------------|-------------|---------------------------------------------------------------------------|
| 1.0     | ITU-T Y.3180   | 2022-02-13 | 13          | <a href="http://handle.itu.int/11.1002/1000/14856">11.1002/1000/14856</a> |

### Keywords

Application descriptor agnostic, machine learning, traffic awareness.

---

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

## FOREWORD

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

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

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

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

## NOTE

In this 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 2022

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 .....                                                                                                             | 3    |
| 6 Overview of traffic awareness for application-descriptor-agnostic traffic.....                                                | 3    |
| 7 General mechanism of traffic awareness for application-descriptor-agnostic traffic...                                         | 4    |
| 7.1 Basic architecture of traffic awareness for application-descriptor-agnostic traffic .....                                   | 4    |
| 7.2 Architecture for independent machine learning system .....                                                                  | 7    |
| 7.3 Protocol layer mechanism of traffic awareness for application-descriptor-agnostic traffic .....                             | 12   |
| 7.4 Application layer mechanism of traffic awareness for application-descriptor-agnostic traffic.....                           | 13   |
| 7.5 Reliability and availability mechanism for independent machine learning system .....                                        | 14   |
| 8 Machine learning methods used for application-descriptor-agnostic traffic awareness.....                                      | 16   |
| 8.1 Overview of machine learning methods used for traffic awareness.....                                                        | 16   |
| 8.2 Supervised learning methods.....                                                                                            | 16   |
| 8.3 Unsupervised learning methods .....                                                                                         | 19   |
| 9 Implementation consideration of traffic awareness for application-descriptor-agnostic traffic based on machine learning ..... | 20   |
| 9.1 Implementation for flow feature based methods .....                                                                         | 20   |
| 9.2 Implementation methods based on analysis for payload features .....                                                         | 22   |
| 9.3 Implementation of methods based on analysis of traffic behaviour feature...                                                 | 23   |
| 9.4 Hybrid methods based on analysis for multiple features.....                                                                 | 23   |
| 10 Report and auxiliary control mechanism for the malicious application-descriptor-agnostic traffic .....                       | 23   |
| 10.1 Report mechanism for malicious application-descriptor-agnostic traffic .....                                               | 23   |
| 10.2 Auxiliary control mechanism for malicious application-descriptor-agnostic traffic .....                                    | 25   |
| 11 Security considerations.....                                                                                                 | 25   |
| Bibliography.....                                                                                                               | 26   |



# Recommendation ITU-T Y.3180

## Mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning

### 1 Scope

This Recommendation specifies a mechanism of traffic awareness for application-descriptor-agnostic traffic based on machine learning. The scope of this Recommendation includes:

- a) Overview of traffic awareness for application-descriptor-agnostic traffic;
- b) General mechanism of traffic awareness for application-descriptor-agnostic traffic;
- c) Machine learning methods adopted to traffic awareness for application-descriptor-agnostic traffic;
- d) Implementation considerations of traffic awareness for application-descriptor-agnostic traffic based on machine learning;
- e) Report and auxiliary control mechanisms for the malicious application-descriptor-agnostic traffic;
- f) 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 X.200] Recommendation ITU-T X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic reference model: The basic model*.
- [ITU-T Y.2701] Recommendation ITU-T Y.2701 (2007), *Security requirements for NGN release 1*.
- [ITU-T Y.2704] Recommendation ITU-T Y.2704 (2007), *Security mechanisms and procedures for NGN*.
- [ITU-T Y.2770] Recommendation ITU-T Y.2770 (2012), *Requirements for deep packet inspection in next generation networks*.

### 3 Definitions

#### 3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

**3.1.1 application-descriptor (also known as application-level conditions)** [ITU-T Y.2770]: A set of rule conditions that identifies the application (according to clause 3.2.1 of [ITU-T Y.2770]). This Recommendation addresses the application descriptor as an object in general, which is synonym to application-level conditions. It does not deal with its detailed structure such as syntax, encoding, and data type.

**3.1.2 application tag** [ITU-T Y.2770]: A unique name for an application which is used to indicate the application semantics and is typically used for reporting scenarios.

**3.1.3 machine learning (ML)** [b-ITU-T Y.3172]: Processes that enable computational systems to understand data and gain knowledge from it without necessarily being explicitly programmed.

**3.1.4 network element** [b-ITU-T M.60]: It consists of telecommunication equipment (or groups/parts of telecommunication equipment) and support equipment.

## 3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

**3.2.1 application-descriptor-agnostic traffic:** Traffic that cannot be identified by a set of rule conditions or the set of rule conditions corresponding to the traffic are much difficult to be set up.

## 4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

|       |                                    |
|-------|------------------------------------|
| AI    | Artificial Intelligence            |
| DL    | Deep Learning                      |
| DPI   | Deep Packet Inspection             |
| FI    | Flow Identifier                    |
| FF    | Flow Feature                       |
| GMM   | Gaussian Mixture Model             |
| HCA   | Hierarchical Cluster Analysis      |
| HSTS  | HTTP Strict Transport Security     |
| HTTP  | Hyper Text Transfer Protocol       |
| HTTPS | HTTP over SSL                      |
| IP    | Internet Protocol                  |
| kNN   | k-Nearest Neighbour                |
| ML    | Machine Learning                   |
| NFV   | Network Function Virtualization    |
| NMS   | Network Management System          |
| P2P   | Peer-to-Peer                       |
| SSL   | Secure Sockets Layer               |
| SVM   | Support Vector Machine             |
| TA    | Traffic Awareness                  |
| TCP   | Transport Control Protocol         |
| TLS   | Transport Layer Security           |
| VLAN  | Virtual Local-Area Network         |
| VM    | Virtual Machine                    |
| VoIMS | Voice over Integrated Media System |
| VoIP  | Voice over Internet Protocol       |

|       |                                    |
|-------|------------------------------------|
| VoLTE | Voice over Long-Term Evolution     |
| VoNGN | Voice over Next Generation Network |
| VoP2P | Voice over Peer to Peer            |
| XML   | extensible Markup Language         |

## 5 Conventions

In the body of this Recommendation, the words should, and can sometimes appear, in which case they are to be interpreted, respectively, as is recommended, and is/are able to. The appearance of such phrases or keywords in an appendix or in material explicitly marked as informative are to be interpreted as having no normative intent.

## 6 Overview of traffic awareness for application-descriptor-agnostic traffic

An application-descriptor is a set of rule conditions that can identify an application, see [ITU-T Y.2770]. In network scenarios, application-descriptor is a set of rule conditions that can identify a certain packet flow or a certain class of network traffic.

Application-descriptor-agnostic traffic is the class of network traffic which cannot be identified or classified based on an application descriptor, e.g., compressed traffic, various peer-to-peer (P2P) traffic, encrypted traffic, etc.

Because an application descriptor cannot be used to classify it, application-descriptor-agnostic traffic is difficult to be identified through traditional application-descriptor-based technologies or methods such as deep packet inspection (DPI) related technologies.

So, new mechanisms are needed to identify application-descriptor-agnostic traffic, In addition, the aforementioned mechanism should not only rely on traffic features that come from payload of the packet directly. Traffic features from payload are necessary information processed by traditional application identification technologies.

Machine-learning based mechanisms are appropriate for identifying application-descriptor-agnostic traffic because they can work without depending on payload of the packet. Through analysis for multi-dimension features other than packet payload, machine-learning based mechanisms can build up connections between multi-dimension features and a certain kind of network traffic, then machine-learning based mechanisms can identify the network traffic according to the multi-dimension features.

In order to provide identification capability for application-descriptor-agnostic traffic, the following functional elements should be supported by a machine-learning based mechanism:

- Designing and deploying machine learning function.
- Flow feature picking up, designing and representing.

In addition, the following functional elements are also important to the machine-learning based mechanism:

- Machine learning methods that can be used by the machine-learning based mechanism.
- Implementation methods of the machine-learning based mechanism.
- Report and control mechanisms.

## 7 General mechanism of traffic awareness for application-descriptor-agnostic traffic

### 7.1 Basic architecture of traffic awareness for application-descriptor-agnostic traffic

#### 7.1.1 Overview of traffic awareness combined with machine learning technologies

It can be seen from clause 6 that it is very difficult to identify application-descriptor-agnostic traffic through traditional traffic awareness methods. In addition, machine learning technologies are quite appropriate for the aforementioned awareness of application-descriptor-agnostic traffic. An important aspect of the machine-learning based traffic awareness mechanism is the designing and deploying machine learning function.

In other words, the critical problem for machine learning technologies to be used in traffic awareness is how to deploy a machine learning function in the traffic awareness context. Generally, there are three kinds of deployment modes:

- traffic awareness with independent machine learning system;
- traffic awareness with embedded machine learning system;
- traffic awareness with hybrid machine learning system.

#### 7.1.2 Architecture of traffic awareness with independent machine learning system

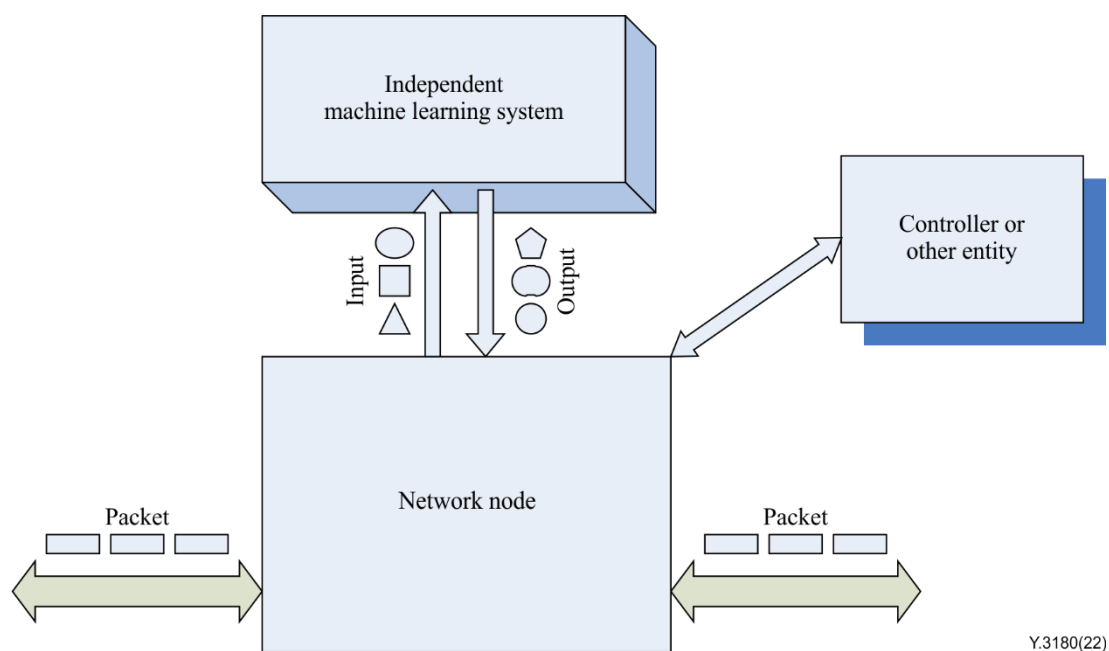


**Figure 7-1 – Architecture of independent machine learning system**

Figure 7-1 describes a typical architecture for deploying machine learning functions as an independent machine learning system. This deployment mode is proper for the majority of the application scenarios, and especially proper for network nodes that have been fully designed and developed. Network nodes mean the physical network elements used in the network. While deploying the machine functions function as an independent system, the basic structure of the network nodes which are going to be deployed with machine learning functions can remain unchanged.

Because the basic structure of the network nodes remain unchanged, only small and minor changes can occur to the network nodes. Under such circumstances, a small agent is needed by the network node to exchange input and output information with the independent machine learning system.

The input between network nodes and an independent machine learning system includes:

- Machine learning rules: some specification for the independent machine learning system, and the machine learning rules is used to tell the independent machine learning system how to use the input information to generate output information. It can be originated from the network controller or the network node.
- Training data: a data set including input data, decision and evaluation score, The evaluation score is the evaluation result for the decision. The training data can be originated from the controller or the network node. It can also be generated by the independent machine learning system itself.
- Input data: some data provided to the independent machine learning system in order to acquire some corresponding decision. It is originated from the network node.

The output refers to the decision information that can make the network node undertake some special actions.

Logically, there are three external interfaces (except for the interfaces between the network node and the independent machine learning system) concerning the network node:

- Packet in interface: a logical interface used for receiving data packets, generally, there is a packet in interface corresponding to each physical interface in the network node.
- Packet out interface: a logical interface used for sending data packets, generally, there is also a packet out interface corresponding to each physical interface in the network node.
- Interface to controller: a logical interface used to exchange information with the controller in order to carry out the control functions for the network node.

### 7.1.3 Architecture of traffic awareness with embedded machine learning functions

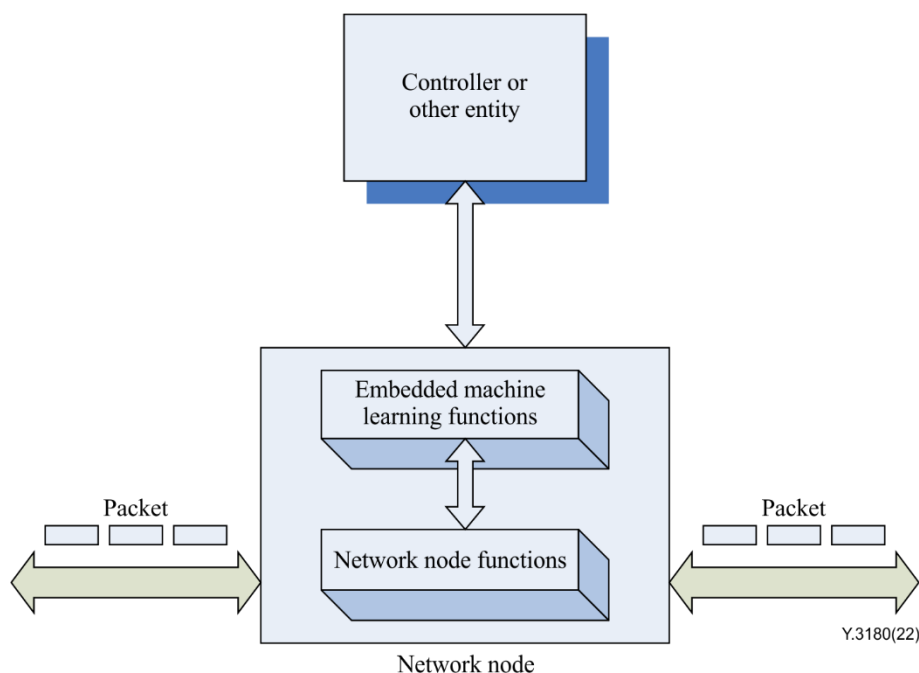


**Figure 7-2 – Architecture of embedded machine learning functions**

Figure 7-2 illustrates a kind of architecture for deploying machine learning functions in embedded mode. This deployment mode is appropriate for the network nodes that are under developing and can be restructured. While deploying machine learning functions in embedded mode, there are substantial changes concerning the basic structure of the network node.