TECHNICAL REPORT

ISO/IEC TR 29181-3

First edition
2013-04-15

Information technology — Future Network — Problem statement and requirements —

Part 3: Switching and routing

Technologies de l'information — Réseaux du futur — Énoncé du problème et exigences —

Partie 3: Commutation et routage

Reference number
ISO/IEC TR 29181-3:2013(E)

Contents

Page

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

In exceptional circumstances, when the joint technical committee has collected data of a different kind from that which is normally published as an International Standard ("state of the art", for example), it may decide to publish a Technical Report. A Technical Report is entirely informative in nature and shall be subject to review every five years in the same manner as an International Standard.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC TR 29181-3 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

ISO/IEC TR 29181 consists of the following parts, under the general title *Information technology — Future Network — Problem statement and requirements*:

- *Part 1: Overall aspects*
- *Part 3: Switching and routing*
- *Part 4: Mobility*
- *Part 6: Media transport*
- *Part 7: Service composition*

The following parts are under preparation:

- *Part 2: Naming and addressing*
- *Part 5: Security*

Introduction

ISO/IEC TR 29181-1 describes the definition, general concept, problems and requirements for the Future Network (FN). The other parts of ISO/IEC TR 29181 provide details of various components of the technology.

This part of ISO/IEC TR 29181 examines the requirements for carrying data over digital networks, and identifies those that are not satisfied by the current Internet.

It also notes some expected characteristics of new systems that are better able to satisfy the requirements, and specifies a model which supports both the existing system and the new systems. This will enable a migration to the new systems; it is also intended to make networks of all sizes easier to manage.

Information technology — Future Network — Problem statement and requirements —

Part 3: Switching and routing

1 Scope

This part of ISO/IEC TR 29181 contains the problem statement and requirements for switching and routing in the Future Network, in particular:

a) description of the requirements for carrying data over digital networks;

b) description of the ways in which these requirements are not satisfied by current networks;

c) functional architecture for switching and routing in the Future Network; and

d) requirements for control plane information flows for finding, setting up, and tearing down routes.

The requirements in (d) include support for both current ("legacy") and future ("new") switching technologies, to aid the transition between them.

NOTE A distinction is made between "data", which is simply a string of bytes, and "content", for which an interpretation, for instance as text, sounds, or still or moving images, is defined. Content is addressed in ISO/IEC TR 29181-6.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC TR 29181-1, *Information technology — Future Network — Problem statement and requirements — Part 1: Overall aspects*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC TR 29181-1 and the following apply.

3.1
data unit
sequence of octets which is conveyed across the network as a single unit

3.2
flow
sequence of data units

3.3
asynchronous flow
flow consisting of data units for which the time of arrival at the destination is unimportant

3.4
synchronous flow
flow for which the network delay experienced by data units is required to be within specified limits, the size of the units, and also the number of units to be transmitted per unit time, being either fixed, or variable with a defined upper limit

3.5
connectionless data unit
data unit which is not part of a flow

3.6
network delay
time from submission of a data unit to the network by the sender to its delivery to the recipient

NOTE The exact events which constitute submission and delivery are not specified in this document, as they depend on internal details of the equipment.

3.7
network element
piece of equipment which takes part in the process of conveying data, such as a switch, gateway, or interface

3.8
FN-aware network element
network element which implements a protocol which will be standardised, based on the requirements in clauses 9 and 10

3.9
legacy network
network composed of network elements which are not FN-aware

3.10
end equipment
equipment that is connected to the network and produces or consumes data units

3.11
identifier
value that identifies a subnetwork, network element, service, or piece of content

3.12
locator
value that identifies a subset of the network which is the scope of an identifier or in which the object identified by an identifier is to be found

3.13
address
identifier, or locator together with an address whose scope is defined by the locator

3.14
label
information in the encapsulation of a data unit which defines, to the network element which receives the data unit, how it is to be routed

EXAMPLE 1 IP address and port number

EXAMPLE 2 MPLS label

EXAMPLE 3 ISDN channel number

3.15
encapsulation
additional octets or other symbols associated with a data unit which serve to delimit it or to identify aspects of the service it should receive

3.16
packet
data unit together with its associated encapsulation

4 Abbreviations

Numbers in square brackets identify references in the Bibliography. Numbers prefixed by RFC identify IETF "Request For Comments" documents.

ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol (RFC 826)
AoIP	Audio over Internet Protocol
ATM	Asynchronous Transfer Mode
AVB	Audio Video Bridging [1]
CO	Connection Oriented
CL	ConnectionLess
DAB	Digital Audio Broadcasting
DHCP	Dynamic Host Configuration Protocol (RFC 2131)
DNS	Domain Name System (RFC 1034, 1035)
DSL	Digital Subscriber Line
DWDM	Dense Wavelength Division Multiplexing
EUI	Extended Unique Identifier
FEC	Forward Error Correction
FM	Frequency Modulation
GPS	Global Positioning System
HTTP	HyperText Transfer Protocol (RFC 2616)
IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPv4	Internet Protocol version 4 (RFC 791)
IPv6	Internet Protocol version 6 (RFC 2460)
ISDN	Integrated Services Digital Network [2]
ISP	Internet Service Provider
MAC	Media Access Control
MPLS	MultiProtocol Label Switching (RFC 3031)
MTU	Maximum Transmission Unit size
NAT	Network Address Translation
OSI	Open Systems Interconnection
PC	Personal Computer
PCM	Pulse Code Modulation
QoS	Quality of Service
RSVP	resource ReSerVation Protocol (RFC 2205)

SDH	Synchronous Digital Hierarchy [3]
SDP	Session Description Protocol (RFC 4566)
SIP	Session Initiation Protocol (RFC 3261)
SNAP	SubNetwork Access Protocol
SNMP	Simple Network Management Protocol (RFC 1157)
STL	Studio-Transmitter Link
STUN	Session Traversal Utilities for NAT (RFC 5389)
TCP	Transmission Control Protocol (RFC 792)
UDP	User Datagram Protocol (RFC 768)
UHF	Ultra High Frequency
URL	Universal Resource Locator
VCI	Virtual Channel Identifier
VPI	Virtual Path Identifier

5 Background

5.1 Main features

New switching technologies are expected to support virtual circuits, in contrast to the connectionless paradigm of the current Internet Protocol: see 5.2.

The control protocols outlined in this document allow an application to negotiate with the network, and with the remote application, to achieve the communication of its data in the most appropriate way. They do not constrain the system to use any particular method of delivering the data to its destination, and thus support both existing and new switching technologies. They do, however, require the network to report explicitly (to the application) parameters defining the service it will receive; this allows the application to take advantage of the facilities offered by the new networks if available, and to make provision for the deficiencies of existing technologies otherwise.

The Internet Protocol world is often depicted as an hour-glass, with many applications at the top, many network technologies at the bottom, and IP as the narrow waist through which everything must pass. FN has a similar structure, but there are some important differences in the nature of the narrow waist:

- there are two kinds of interaction between the application and the network, which we describe as control plane and data plane;
- control plane messages usually refer to a “flow” (a sequence of data units) rather than to a single data unit, so are able to include the QoS parameters needed for live media, also other session-related information such as security checks and per-call billing; and
- the data plane carries data units whose encapsulation depends only on the local switching technology.

Thus different kinds of switching technology can be supported, even those (such as DWDM) that do not route according to information in packet headers. Where packet switching is used, the routing information in the packet does not need to include the kind of globally unique addresses that are required for IP.

5.2 Rationale for a new paradigm

5.2.1 Appropriateness for today's traffic

Today's Internet mainly carries two kinds of traffic: static objects such as files and web pages, and continuous media such as audio and video. The connectionless service provided by Internet Protocol is transmission of individual packets from one interface to another; it is a “best effort” service, aiming to deliver each packet as soon as possible but not giving any guarantees as to when (or even whether) each packet will be delivered.

A user downloading a file simply requires a copy of the file to be received by a particular piece of equipment (such as a PC) as soon as possible after it is requested, so a “best effort” service such as that provided by IP is appropriate. However, the equipment may have several different interfaces to the network, and the user should not need to consider through which interface the data should be received, nor the location of the server on which it is hosted.

In the case of continuous media, the source produces data at regular intervals and the destination consumes it at regular intervals. The time between the source sending some data and the destination consuming it must be long enough for the slowest packet to arrive. (The destination must hold data packets that arrive more quickly in a buffer.) In connectionless packet networks, this time interval includes an unpredictable amount of queuing time and is thus not well-defined. For some applications, such as streaming recorded material, this is of minor importance, but for others, such as videoconferencing, it degrades the user experience and in some cases, for instance some telemedicine and industrial control applications, delays will compromise safety.

To deliver a service appropriate for continuous media, the network needs to configure resources to be ready to pass on the data with a minimum of delay; a negotiation is therefore required between the application and the network before transmission begins. Various measures have been introduced to improve the service experienced by continuous media on the current Internet, but this traffic still experiences dropped packets and unnecessarily long delays. Moreover, the addition of new protocols and procedures increases the complexity of the system, decreasing its reliability and making it more difficult to manage: see reference [4] in the Bibliography.

5.2.2 Addressing and scalability

Use of Internet Protocol also requires every packet to carry the IP addresses of sender and destination. These addresses have global scope, and must therefore be large enough to uniquely identify every endpoint; as the number of endpoints increases (a process that will accelerate as the Internet of Things develops), addresses need to become larger, for instance changing from 32-bit IPv4 addresses to 128-bit IPv6 addresses. A system with a fixed address format in which addresses have global scope cannot scale beyond a certain size; for instance a system using IPv4 cannot have more than 4 billion endpoints.

However, a switch or router simply needs to forward the packet to the correct neighbour with the correct level of service, and locally-significant forms of identification have the potential to allow this task to be performed more efficiently and more reliably. Moreover, they do not impose any limitations on the total size of the network because addresses in one area can be re-used in other areas. Network address translation has retro-fitted this feature to IPv4, but caused other problems which required the introduction of further protocols such as STUN.

FN makes possible a migration from IP to improved switching technologies in which the information used for local routing is separate from global addressing.

5.2.3 Security

Another area of concern is security. In a connectionless packet-switched network, all the information needed to route a packet has to be included in the packet header. This limits the amount of checking that can be done without unreasonably increasing the packet size, or the amount of processing required per packet at each switching point, or both. A system in which the routing information in a packet refers, indirectly, to a route that was set up as a result of a negotiation which can include much more thorough checking of identity etc, has the potential to be much more secure. It can also enhance privacy by allowing a client to set up a session with a server without disclosing the client's address to the server.

5.2.4 Complexity of routing hardware

Connectionless packet switching requires each switch or router to read and interpret addressing information in each packet, in order to discover on which output to forward it and what service (e.g. higher- or lower-priority queue) it should experience. This information is usually too long to be used as a memory address for direct lookup, for instance an IPv6 address is 128 bits and the information necessary to identify a flow in an IPv4 packet is over 100 bits, so the more complex and power-hungry associative or content-addressable memory must be used. Other techniques, where much of the work is done once (when the call is set up) rather than for every packet, allow switching equipment (and particularly large switches) to be simpler and less power-hungry; see, for instance, 4.1 of reference [6]. With increasing traffic on the Internet, and increasing concern over energy use and its contribution to climate change, efficiency of switching equipment will become more important over the coming decade.

5.3 Migration

The FN model allows a network to be seen as a “black box”, so it is only the edge devices that need to be FN-aware. If the network supports QoS, its native QoS mechanisms can be used and the resulting QoS parameters reported to the application. Otherwise, the application will be informed that only a “best effort” service is possible, with an indication of the performance expected (for instance, whether the network is the public Internet or a small Ethernet network). This allows piecemeal migration in both private and public networks.

For instance, on an AVB network [1] the resource reservation mechanisms of IEEE 802.1Qat and Qav can be used to deliver defined QoS. The edge devices need to support the FN protocols, but within the network only the AVB protocols need to be supported.

An application on an FN-aware terminal on the AVB network can ask to receive video from a server identified by a URL; if the server is on the AVB network, IEEE 1722 can be used for transport and there is no need to use IP at all. If the server is on the Internet, there are two possibilities: either the application is told it has to use IP over the Ethernet network, or the gateway between the AVB network and the Internet implements the IP protocols.

A public network which supports non-IP routing may tunnel IP packets through its asynchronous service, and it may convert between IP and FN protocols in gateway devices. It may intercept protocols such as SIP and set up synchronous flows for them.

On the link between two networks, for instance an ADSL link between a private network and an ISP, if the devices at both ends of the link are FN-aware the FN protocols can be used. Otherwise, legacy protocols must continue to be used.

5.4 Structure of this document

Clause 6 lists requirements for applications that transmit information across digital networks, and clause 7 lists ways in which the current technology fails to meet those requirements.

Clause 8 examines the functionality of switching and routing equipment. Clauses 9 and 10 list requirements for the communication between network elements, and clause 11 outlines the requirements for the process of exchanging information between network elements that allows the route to any given destination to be established.

6 Requirements

6.1 Introduction

The basic service provided by the network is to convey data units between end equipment.

This clause reviews the requirements which applications that transmit various kinds of data across digital networks have for this service.

Many different kinds of application will use this service to convey information encoded as octet strings, and the network should not attempt to interpret the data units it conveys. It should not deliberately alter them in any way, although transmission errors may occasionally occur (see 6.4.2). Many different kinds of network element will participate in the conveying of an application's data unit, and the application should not make assumptions about their characteristics.

