General specification of Internet service

version 1.0

Observatory Report 38/2001

The Swedish ICT Commission – the Swedish Agency for Administrative Development

Address*:The* Observatory for IT infrastructure, ITC Commission, SE-103 33 Stockholm
Street address: Regeringsgatan 30-32, IV floor
Telephone: +46-(0)8-405 18 51 ***Fax:*** +46-(0)8-650 65 16
E-mail: info@itkommissionen.se
Website**:** http://www.itkommissionen.se

ISSN*:* 1404-8744

List of contents

Preface

Internet communication efficiency is important to many organizations and private individuals. Internet services are being offered by a large number of operators in Sweden, but very often without specifying what the service includes, e.g. as regards performance, availability, operating functions and user support.

An initial version of this General Specification of Internet Service – *Generell specifikation av Internettjänst (version 0.93)* – was published in 1997 as part of the "Specification of requirements – Internet services for national authorities, municipalities and county councils" – *Kravspecifikation - Internettjänster för statliga myndigheter, kommuner och landsting* (K:142) – compiled by the Swedish Agency for Administrative Development.

Work began in 1999 on a version 1.0 of the specification. The working group responsible comprised Jan Berner, the ICT Commission (until 1st October 1999 employed at the Swedish Agency for Administrative Development), Anne-Marie Eklund Löwinder, the ICT Commission, Peter Löthberg, STUPI, Börje Josefsson, Luleå Technical University and about ten members of SOF (Swedish Operators Forum). The ICT Commission's Observatory for Information Security contributed viewpoints on security functions. SOF has had an open invitation to state viewpoints on draft versions of the specification, which, accordingly, can be deemed to have the firm support of the majority of Internet service providers. Version 1.0 supersedes version 0.93.

The purpose of this *General Specification of Internet Service* is to give organizations and similar bodies about to procure Internet services from providers a survey of the demands which can be made when formulating a specification of requirements, so as to obtain an Internet service of high quality. The specification, then, is to be regarded as a guide to this process and not in itself a specification of requirements. It can also be used by providers wishing to measure the quality of their own service.

The intention is for this specification to be continuously updated by a suitable organization in response to technical progress and user feedback. The search for an organization of this kind is in progress, and in the meantime the specification will be managed by the ICT Commission.

Questions concerning the specification will therefore until further notice be published on http://www.itkommissionen.se/obs/obs_infra.html.

Comments on this specification should be sent to info@itkommissionen.se

Stockholm, November 2001

Christer Marking *Administrative Director,* *the ICT Commission*	*Connie van der Capellen* *Head of the IT Division of the Swedish* *Agency for Administrative Development*

Introduction

Purpose of the specification

On the basis of this specification, a requirer can frame an independent specification of requirements, indicating what demands are to be made on an Internet service. This specification describes the various components which should be included in, respectively, a dialup and "always on" connection to an Internet provider's service. The specification describes in very great detail a service delivered from operator (provider) to subscriber (customer). "Service" in this specification denotes the transmission and reception of IP packet at the subscriber's access point for the service. The service also includes technical and administrative routines.

Many of the components included in an Internet service are more or less tacitly understood. This specification documents these services in such a way that the parties in a subscriber-provider relation have a common foundation on which to base a procurement or a comparison of the services offered by different operators.

In order to obtain a specification of requirements for a desired case, the requirer selects the components for which it is important to define parameters. Examples of requirement specification design are appended.

The specification presupposes that the subscriber has access to sufficient competence within his organization or suchlike to make relevant demands and to evaluate the operator's replies, and also, where applicable, to carry out necessary measurements.

As regards use of Internet service, it is assumed that the subscriber's own equipment conforms to current standards of communication in accordance with the IP architecture. The subscriber is also assumed to have personnel who are competent enough to both operate the network and to keep abreast of IP standards development.

Various forms of applications and services not included in the basic function of the Internet are for the most part disregarded in this document.

Use of this specification is decided on by each individual organization or the equivalent, on its own responsibility. The ICT Commission and the Agency for Administrative development wish to make clear that anyone intending to use the specification must first clarify any points of law which its use may entail.

Structure of the specification

This document is divided into the following parts

Part 1 Forms of connection.
Describes what is meant by dialup and "always on" connection to an Internet service.
Part 2 Internet service components.
Description of the components for each service.
Part 3 List of components for each service.
Glossary List of abbreviations used.

Using the designations described in part 2 of the specification, the service delivered from operator to subscriber can be described by referring to designations in part 3.

Note that in this version, version 1.0, certain parts have been renumbered compared with version 0.93, published previously. This is due to new protocols and requirements having been added and to certain older protocols and requirements no longer being relevant.

Part 1 Forms of connection

The communications architecture used for the Internet is commonly known as TCP/IP or just IP and comprises the collection of protocols described in the RFCs indicated by the IAB/IESG as a description of a protocol standard. (There are also RFCs which do not have the status of a standard but are proposals, reports or other matter of interest to the IETF.)

There are now two distinct main models of access to the Internet, namely dialup connection and “always on” connection.

Dialup connection

A dialup connection means the subscriber establishing a connection, e.g. by phoning the operator’s equipment, before traffic can be exchanged through the operator’s Internet service.

This is the type of service nearly always used by private individuals for accessing the Internet. By definition, it is unsuitable for applications with more than one single user, and it also depends on no traffic being initiated *towards* the subscriber from elsewhere on the Internet.

An organization can, for example, use a dialup connection for employees who are travelling or telecommuting, so as to give them remote access to computer resources within their own organization. The connection is then arranged using one of the security protocols in the IP architecture, which permit secure identification and encryption of information in transit between the remote-connected employee and the organization’s computer system.

Dialup connection to an operator’s Internet service is dealt with in **point 03** of parts 2 and 3 of this specification.

“Always on” connection

With an “always on” connection the subscriber (the subscriber’s equipment) can deliver IP packets to a transit element (at the point of access) without having to make a connection with the operator’s Internet service every time. Similarly, IP packets sent from another point on the Internet can, without any special action being necessary, be delivered from a transit element to the subscriber via the access point.

An operator can use any equipment for the access point of the service and any mode of transmission in relation to the operator’s network, so long as the agreed performance is achieved and the Internet architecture complied with. The technology used is the operator’s responsibility and must be transparent to the user.

A **“always on” connection** to an operator’s Internet service includes the following parts:

04	The access point
05	Level 2 protocol
06	Level 3 protocol
07	Routing protocol
08	Performance on the operator’s network and at the access point
09	Dynamic parameters
10	Availability/unavailability
11	Traffic filtering
12	Monitoring functions
13	Reachability
15	Network Address Translator (NAT)
16	Domain Name System (DNS)
17	E-mail
18	Network Time Protocol (NTP)
19	News
20	Subscriber support
21	Operational monitoring
22	Other services
23	Security
24	Scheduled maintenance and service times
40	Internet development
41	Development of the service

Part 2 Internet service components

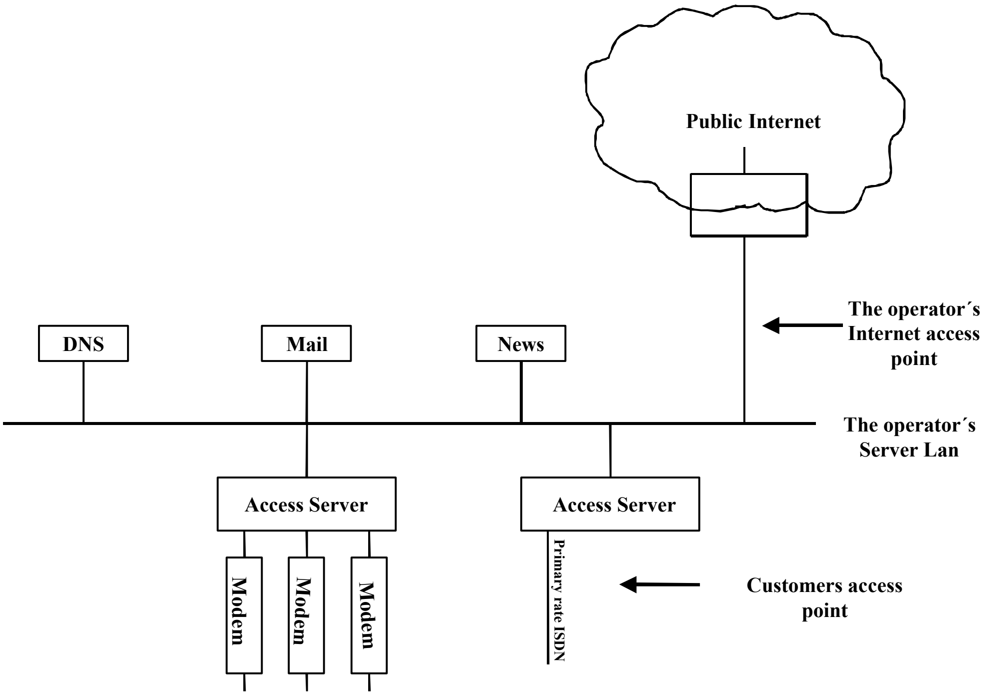
This part describes the components included in an Internet service. Some of them are *national* in character and have been numbered xx.9x to show that they are local and valid in Sweden only. To avoid detaching them from their context in the descriptions, they have in certain cases been given their logical place there, in which case the sequence number is followed by an asterisk, e.g. 08.91*. Part 3, on the other hand, employs a strictly numerical order, to facilitate adjustment of the specification to other countries.

H in the document denotes a *historical* function, e.g. 05.13H.

Dialup connection

03 Dialup connection

The Internet service is delivered to the subscriber (customer) through some form of connected network intended mainly for other types of traffic than the Internet, e.g. telephony.



03.01 IPv4 Unicast traffic

Does the operator offer a service based on IPv4 Unicast?

Alternatives: YES or NO.

03.02 IPv4 Multicast traffic with IGMP

Does the operator offer a service based on IPv4 Multicast traffic with IGMPv2 or IGMPv3 as "group member protocol"?

Alternatives: YES or NO.

03.03 IPv6 Unicast traffic

Does the operator offer a service based on IPv6 Unicast?

Alternatives: YES or NO.

03.04 IPv6 Multicast traffic

Does the operator offer a service based on IPv6 Multicast?

Alternatives: YES or NO.

03.06 Access by analog modem
Alternatives: YES or NO. If YES, then
The operator shall indicate:
(a) Which modem interface (V,34 etc.) each modem pool supports.

(b) Whether the PPP datalink protocol is supported.

(c) Whether group numbers can be used for reaching the modem pools.

(d) Which operator (i.e. an operator with an independent core network) is used for connection to the Internet.

03.08 Access by digital connection, e.g. ISDN
YES or NO. If YES then

The operator shall indicate:
(a) Whether one or two B channels are supported.

(b) Whether the PPP datalink protocol is supported.

(c) Whether group numbers can be used for reaching the modem pools.

(d) Which operator (i.e. an operator with an independent core network) is used for connection to the Internet.

03.10 Address allocation and verification methods

The operator shall indicate:

(a) How the IP address is assigned (dynamically or permanently, based on user identity).

(b) Whether the modem pool concerned supports PAP or CHAP for user verification.

03.20 E-mail services

Explanation: Computer systems used for managing electronic mailboxes should have a good-performance Internet connection. In the event of the system going down, it must be possible for e-mail to be put into intermediate storage elsewhere (with a secondary mailhost). It is assumed here that the system components will conform to current Internet standards (STD) and that updated and current versions of SMTP software will be used for communication to and from the Internet.

03.21 30 minutes' uninterruptable power supply

Are computer systems and communications equipment for e-mail management and dialup connection have a uninterruptable power supply with at least 30 minutes reserve capacity?

Alternatives: YES or NO

03.22 Internet connection with at least two redundant links

Are computer systems used for e-mail handling connected by at least two redundant links to the Internet?

Alternatives: YES or NO

03.23 Support for the POP-2 protocol

Is subscriber access with the POP-2 protocol supported?

Alternatives: YES or NO

03.24 Support for the POP-3 protocol

Is subscriber access with the POP-3 protocol supported?

Alternatives: YES or NO

03.25 Support for the IMAP protocol

Is subscriber access with the IMAP protocol supported?

Alternatives: YES or NO

03.26 E-mail disk storage space available per receiver

Is disk storage space available for storage of e-mail received per user identity?

Alternatives: YES or NO

If YES: State number of megabytes available per user identity.

03.27 Customer's domain address indicated for incoming and outgoing e-mail

Can an electronic mailbox be given the customer's domain address, e.g. nisse.nilsson@myndighet.se, for both incoming and outgoing e-mail?

Alternatives: YES or NO.

03.30 News services

Explanation: News is a structure of discussion groups containing articles in various subject fields. It must be possible to read articles written by other people in other systems, and articles created must be distributed to other News systems.

03.31 Reading of News with the NNTP protocol

Is reading of News from subscriber with the NNTP supported?

Alternatives: YES or NO.

03.32 Sending of News with the NNTP protocol

Is sending of News from subscriber with the NNTP supported?

Alternatives: YES or NO

03.33 Total newsfeed

Is it possible for the operator to distribute all public news groups occurring?

Alternatives: YES or NO.

03.34 Selected groups from total newsfeed

(a) Does the operator have a policy whereby the subscriber cannot gain access to other known groups/types of group?

Alternatives: YES or NO.
If the answer is YES, indicate the policy which applies.

(b) Can the subscriber specify groups to be received?

Alternatives: YES or NO.

(c) Can the subscriber specify groups not to be received?
Alternatives: YES or NO.

03.35 Pre-distribution spam selection

Does the operator filter for spam before distributing news articles to subscriber?

Alternatives: YES or NO.

03.90* Number of days swnet* and se.* are saved

For how many days are articles for the Swedish news structures (swnet* and se.*) saved?

03.36 Number of days for which articles in other News groups are saved.

For how many days are articles saved in all other News groups?

03.37 Number of incoming complete newsfeeds etc.

The operator shall:
(a) Indicate the number of complete incoming newsfeeds.
(b) Name a domain address for transmitting systems.

03.38 Number of outgoing newsfeeds for locally posted articles etc.

The operator shall:
(a) Indicate the number of outgoing feeds for locally posted articles.
(b) Name the domain address for receiving systems.

03.91* Average delay in minutes from posted to readable article

The operator shall indicate the mean delay in minutes from the posting of an article to SUNET’s central news server in the swnet.test group until it can be read by the subscriber against the operator’s service.

Time in minutes.

03.40 DNS support

03.41 A caching DNS resolver exists which can be used by the subscriber

Is there a caching DNS resolver which can be used by the subscriber?

Alternatives: YES or NO.

03.42 Secondary DNS servers exist at no less than two different places in the network.

Are there secondary DNS servers at no less than two different places in the network for the domains handled by the mail system?

Alternatives: YES or NO.

03.43 Support for secure DNS

Explanation: In cases where the user's client uses the operator's DNS resolver for recursive look up and at the same time uses secure DNS, the operator's DNS is required to support secure DNS and there have to be suitable security routines for verifying that the operator's computer system handles secure DNS correctly, that it has current keys updated and that these keys have not been manipulated without authorisation. The reason for these requirements is that the subscriber's client application is forced to rely on the information which the operator's system delivers in reply to a recursive DNS question.

Does the operator have support for secure DNS, with suitable security routines?

Alternatives: YES or NO.

03.50 Throughput and performance

03.51 Measurement of throughput between subscriber system and the operator's server

Method of measurement: Measurement is performed by the subscriber having a V.34 modem with compression connected to his computer system with 115.2 kbit/s.

A specific test file of 800 kbyte is transferred by FTP from the subscriber system to the operator's server, and then by FTP back to the subscriber system. A binary test file for this purpose is available from the ICT Commission.

Effective transmission capacity (transmission speed) is calculated from the transmission time.

The operator shall indicate effective transmission capacity in both directions, in kbit/s.

03.52 Minimum throughput

Method of measurement: Traffic is sent as TCP streams in both directions, e.g. by running TCP-spray from a dialup client against the TCP loopback interface of a computer system provided by the operator in conjunction with a national exchange point (see illustration accompanying 08.30). The sample shall contain a data quantity of at least 1 Mbyte.

The test is performed three times, for an hour each time, 09.00-10.00 hours, 14.00-15.00 hours and 21.00-22.00 hours, on weekdays.

For throughput in each direction, the operator shall indicate the lowest transmission time value in seconds which is never undershot in any of the tests.

03.53 Measurement of throughput between subscriber connection and a national main exchange point.

Method of measurement: Traffic is sent as TCP streams in both directions, e.g. by using the TCP loopback interface on a computer system in one connection and TCP spray from the other. For measurement against exchange points, the operator shall indicate a relevant computer system/IP address against which to perform the measurement.

The test is performed three times, for an hour each time, 09.00-10.00 hours, 14.00-15.00 hours and 21.00-22.00 hours, on weekdays.

The operator shall indicate the lowest throughput value (kbit/s) which is never fallen short of in any of the tests.

03.54 Throughput between a subscriber connection and NY-NAP in Pennsauken USA

Method of measurement as per 03.53.

The operator shall indicate the lowest value (kbit/s) for throughput never fallen short of in any of the tests.

03.55 Roundtrip delay between subscriber connection and national main exchange point.

Method of measurement: ICMP Echo Reply messages (pings) with a data content of 64 bytes are sent to a computer system connected at the subscriber connection. The time given is that elapsing from the whole packet being sent to the whole packet being received back again.

To compensate for any system delays in the measuring equipment, 5 ms is deducted from the value recorded by the computer system.

The test is performed three times, for an hour each time, 09.00-10.00 hours, 14.00-15.00 hours and 21.00-22.00 hours, on weekdays. The measurement is conducted by sending an ICMP echo packet (ping) every other second during the 60-minute test period, making a total of 1,800 packets of 64 bytes each.

The measured value is the average delay time for packets received within 2 seconds of being sent.

The operator shall indicate the roundtrip delay between a subscriber connection and a main national exchange point, measured as described above. The time is given in milliseconds.

03.56 Roundtrip delay between subscriber connection and NY-NAP in Pennsauken, USA

Indicate roundtrip delay between a subscriber connection and NY-NAP in Pennsauken, USA, measured as per 03.55.

State time in milliseconds.

03.60 Security

Remarks: Security here means the security of the operator's network and support system.

03.61 Software updates at access point and in core network

Is the software in the equipment forming the backbone network and located at the access point continuously updated?

Alternatives: YES or NO.

03.62 Information from equipment manufacturers, CERT, CIAC etc.

Does the operator receive continuous information from equipment manufacturers, CERT, CIAC etc.?

Alternatives: YES or NO.

If YES, state from which sources.

03.63 Routines for dealing with security incidents

Are there documented routines for dealing with security incidents?

Alternatives: YES or NO.

03.64 Routines for informing the subscribers affected of an incident

Do routines exist for informing the subscribers affected of any incident?

Alternatives: YES or NO.

03.65 Filters on outgoing router to prevent spoofing of IP addresses

Are there filters on outgoing router (or the equivalent) which make spoofing of IP addresses as hard as possible from the operator's network against another operator?

Alternatives: YES or NO.

03.66 Filters in access servers to prevent spoofing of the subscriber's addresses for blocking incoming packets

Are there filters in access servers or the equivalent which prevent spoofing of the subscriber's addresses, i.e. block incoming packets with sender addresses equal to, smaller than or greater than the subscriber's addresses?

Alternatives: YES or NO.

03.67 Filters in access server to prevent spoofing of IP addresses from a subscriber's network by blocking outgoing packets

Are there filters in access servers or the equivalent which prevent spoofing IP addresses from a subscriber's network, i.e. block outgoing packets with sender addresses, smaller than or greater than the subscriber's addresses?

Alternatives: YES or NO.

03.68 Filter in e-mail systems etc. so that the operator's e-mail system cannot be used for relaying e-mail

Remarks: A sender wishing to conceal the sender address can use other systems to relay outgoing mail. This can be done, for example, when dispatching unsolicited commercial email or unsolicited bulk email, otherwise known as spam. An e-mail system shall only carry e-mail with known sender and recipient addresses.

Are there filters in e-mail systems etc. which make it impossible for the operator's e-mail system to be used for relaying e-mail?

Alternatives: YES or NO.

If YES: Indicate how filters are implemented.

03.69 Filter lists for filtering unsolicited e-mail advertising

Are filter lists used for filtering unsolicited e-mail advertising?

Alternatives: YES or NO.

If YES: Indicate which filters lists are used (e.g. RBL, DUL, ORBS).

03.70 The subscriber can add addresses of his own to e-mail filter lists

Can the subscriber add addresses of his own to e-mail filter lists?

Alternatives: YES or NO.

03.71 Filters in DNS systems which minimize spoofing of DNS information

Are there filters in DNS systems which minimize spoofing of DNS information, i.e. the introduction of incorrect DNS items into the operators' DNS?

Alternatives: YES or NO.

03.72 Filters in router (or the equivalent) so that incorrect routing information will not be spread between the operators' networks

Are there filters in routers (or the equivalent) so that incorrect routing information from another operator will not spread into the operator's network?

Alternatives: YES or NO.

03.73 Protection of BGP sessions (or the equivalent) at peering points

Are BGP sessions (or the equivalent) protected at peering points, using methods corresponding to that described in RFC 2385?

Alternatives: YES or NO.

03.74 Filters between all subscribers

Are there filters (logical) between all subscribers, so that no two subscribers can interfere with each other, for example by replying to DHCP inquiries, ARP/RARP and other "level 2 broadcasting?"

Alternatives: YES or NO.

If YES: Indicate how subscribers are separated.

03.75 Access control between the Network Operations Center and equipment in the network with personal access control

Is access control between the Network Operations Center (or its equivalent) and active equipment in the network managed with personal access control (password, certificate or suchlike)?

Alternatives: YES or NO.

03.76 Routines for access control adjustment when personnel leave the company.

Are there routines for adjusting the access control (e.g. as per 03.75) when personnel leave?

Alternatives: YES or NO.

If YES: Indicate which department or the equivalent handles personnel who are leaving and how the information is spread within the enterprise (the operator) to the part handling access information.

03.77 Security policy for computer systems

There should be a security policy defined for computer systems providing services to the subscriber. Is this security policy communicated to the subscriber?

Alternatives: YES or NO.

If YES: Indicate how the security policy is communicated to the subscriber.

03.80 Other additional services

03.81 Shell account for permanently connected Unix computer

Is a shell account provided for a permanently connected Unix computer?

Alternatives: YES or NO.

03.82 Possibility for a subscriber to create his own web pages.

Is it possible for a subscriber to create his own web pages?

Alternatives: YES or NO.

03.83 Disk space available for subscriber's own web pages, standard

If the subscriber can create web ages of his own, indicate disk storage space available to the subscriber as part of the standard service.

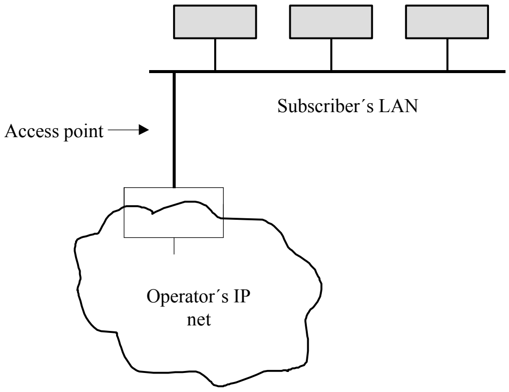
Give space in Mbytes.

“Always on” connection

04 The access point

The service is delivered to the subscriber at the access point. This consists of several different levels, such as the electrical/optic link, the IP packet encapsulation, routing and monitoring. The service also includes technical and administrative routines.

The access point can, for example, take the form of a router or modem. The equipment constituting the access point has a connection as per section 05, level 2 protocol, e.g. an Ethernet interface. Unless otherwise indicated, communication is here presumed to be symmetrical, i.e. with the same capacity (speed) in both directions.



04.11 Connection capacity for service access point

The operator shall state the connection capacity (speed) in kbit/s or in Mbit/s, referring to the IP traffic received through the access point between the user’s network and the operator’s service.

04.12 Access point address

Give the physical address for delivery of the IP service.

05 Level 2 protocol

05.11 10 Mbit/s Ethernet

Is 10 Mbit/s Ethernet offered over an electrical, 10Base2, AUI interface, 10Base T interface or optic Foil interface?

Alternatives: YES or NO.
State what is offered.

Remarks: At the time of ordering, the subscriber and the operator should indicate the interface to be used, e.g. an AUI interface.

05.12 100 Mbit/s Ethernet

Is 100 Mbit/s Ethernet offered over an electrical, 100BaseTX half duplex, 100BaseTX full duplex, MII contact for transceiver or 100BaseFX optic interface?

Alternatives: YES or NO.
State what is offered.

Remarks: At the time of ordering, the subscriber and the operator should indicate the interface to be used, e.g. 100BaseTX half duplex.

05.13H Token Ring, 4 or 16 Mbit/s

05.14H FDDI/ISO 9314 single attachment with multimode fiber

05.15H FDDI/ISO 9314 dual attachment with single mode fiber

05.16 1 Gbit/s Ethernet

a) Is 1 Gbit/s Ethernet offered on a category 5 twisted pair cable?

Alternatives: YES or NO.

b) Is 1 Gbit/s Ethernet offered by optic cable?

Alternatives: YES or NO.

Note: At the time of ordering the subscriber and operator agree on the interface to be used, e.g. an optic interface and multimode fiber connection with SC duplex contacts.

Commentary:
Items 05.21-05.28 of **part 3** are an enumeration of conceivable level 2 protocols which are more or less relevant to an IP service. These are included in part 3 to make the list more complete. If any of these interfaces (05.21-05.28) is used as a delivery point, the LAN interface or equivalent of the equipment terminating the connection from the operator constitutes the point at which the service is delivered.

06 Level 3 protocol (IPv4, IPv6)

06.11 IPv4 Unicast forwarding

Explanation: IPv4 Unicast forwarding means that the operator provides transport of IPv4 packets with an address to the sender and an address to the receiver. The IP packets are switched by the operator's network based on the routine information the operator obtains from his subscribers and from others with whom routing information is exchanged.

A Unicast packet has receiver addresses in the space between 1.0.0.0 and 223.255.255.255.

Does the operator offer IPv4 Unicast forwarding?

Alternatives: YES or NO.

06.12 IPv4 Multicast forwarding

Explanation: IP Multicast forwarding means that the operator provides transport of IPv4 packets where the receiver address is an IP group address. The forwarding service keeps track of all receivers in a certain group and delivers a copy of all packets to all receivers who are members of a certain group.

Between the subscriber's computer and the first router, IGMP (version 2 or 3) is used to indicate which groups an end system wishes to take part in. Between routers, PIM-SM and perhaps a Unicast routing protocol are used to deal with cases where the Unicast and Multicast topologies are not the same.

In case where the subscribers has routers of his own on his side of the delivery point, the customer can either use an RP (a rendezvous point, where sender and receiver meet to be able to built source-based distribution trees) within the operator's network for global group addresses. Otherwise MSDP or BGMP can be used between the operator and the subscriber.

In cases where the subscriber is multiple-connected to the same or a number of different operators, BGP4+ with Multicast NLRI has to be used.

The operator's network shall be designed so that when no receiver is registered with the subscriber the distribution tree will be cut off as far up as possible. No traffic shall be sent through the access point to the subscriber's network (after a certain delay after leaving a certain group).

Multicast group addresses have IP addresses in the space between 224.0.0.0 and 239.255.255.255.

Does the operator offer IPv4 Multicast forwarding?

Alternatives: YES or NO.

06.13 Multicast addresses

If the subscriber needs to send information to Multicast groups where the Multicast address is more or less static, does the operator provide a class D address for this purpose?

Alternatives: YES or NO.

06.14 Multicast addresses between 239.0.0.0 and 239.255.255.255

Explanation: Multicast addresses between 239.0.0.0 and 239.255.255.255 are intended for local use.

Has the operator organised these Multicast addresses in such a way as can locally mean traffic between subscribers to the same operator?

Alternatives: YES or NO.

06.21 IPv6 Unicast forwarding

Explanation: IPv6 Unicast forwarding means that the operator provides transport of IPv6 packets with a sender address and a receiver address as per IPv6. Some form of routing protocol is used for routing.

Does the operator offer IPv6 Unicast forwarding?

Alternatives: YES or NO.

06.22 IPv6 Multicast forwarding

Explanation: IPv6 Multicast forwarding means that the operator provides this within the part of the IPv6 address space intended for Multicast traffic.

Does the operator offer IPv6 Multicast forwarding?

Alternatives: YES or NO.

07 Routing protocols

Routing protocols are used to inform the Internet routers where different destinations (prefix/mask) are connected in the network. In order for traffic to reach a subscriber, the path to the addresses used by the subscriber has to be known within the rest of the Internet.

External routing protocols

07.11 Routing information with BGP4

a) Does the operator offer the possibility of exchanging routing information with the subscriber with the BGP4+ protocol?

Alternatives: YES or NO.

b) **Explanation:** BGP4+ includes the possibility of multi-protocol management in BGP. The following functions are relevant, depending on the service provided:

1. IPv4 Multicast NLRI
2. IPv6 Unicast NLRI
3. IPv6 Multicast NLRI

IPv4 Unicast is not included in the above list because it is necessary in order for BGP to function.

Does the operator support other NLRI besides IPv4 Unicast?

Alternatives: YES or NO.

If YES: Indicate 1, 2 or 3, depending on which additional NLRI is supported in the interface with subscriber.

07.12 Routing information with BGP4, including communities

Does the operator offer the possibility of exchanging routing information with the subscriber with the BGP4 protocol including BGP communities?

Alternatives: YES or NO.

If YES: The operator shall append a list of the communities used and their functions.

07.13H Routing information with IDRP

07.14 Manually preconfigured routing (static)

Do the operator and the subscriber have manually preconfigured routing on their respective sides of the access point (instead of exchanging dynamic routing information)?

Alternatives: YES or NO.

Internal routing protocols

07.21 Routing information with RIPv2

Does the operator offer the possibility of exchanging routing information with the subscriber's equipment using RIv2?

Alternatives: YES or NO.

07.22 Routing information with OSPF

Does the operator offer the possibility of exchanging routing information with the subscriber's equipment using OSPF?

Alternatives: YES or NO.

07.23 Routing information with Integrated IS-IS

Does the operator offer the possibility of exchanging routing information with the subscriber's equipment using Integrated IS-IS?

Alternatives: YES or NO.

07.24 Routing information with EIGRP

Does the operator offer the possibility of exchanging routing information with the subscriber's equipment using EIGRP?

Alternatives: YES or NO.

07.25 Routing information with OSPF-16

Does the operator offer the possibility of exchanging routing information with the subscriber's equipment using OSPF-16?

Alternatives: YES or NO.

07.26 Routing information with RIPv1

Does the operator offer the possibility of exchanging routing information with the subscriber's equipment using RIPv1?

Alternatives: YES or NO.

Remarks: The RIPv1 protocol does not support classless routing, but can in certain cases be used for simpler applications.

07.27 Static configuration

Is static (manual) configuration of routing used at the access point between the operator and the subscriber?

Alternatives: YES or NO.

Routing protocols for Multicast

Explanation: Multicast is used in cases where information is to be distributed to one or more receivers from one more senders. If several receivers in the same part of the infrastructure wish to receive the same amount of information, bandwidth savings will be achieved compared with sending a copy to each of them from the source (Unicast). Depending on the subscriber's requirements – in practice, on whether or not the subscriber has an infrastructure of his own with routers – several protocols are used at the interface.

In the simplest instance, the subscriber uses IGMP for registering membership of a group for receiving, and if the subscriber sends to a group the traffic is sent out as Multicast to the access point. In this case the entire management of Multicast comes within the operator's sphere of responsibility.

In the event of the subscriber having his own infrastructure (in addition to the access router) or other special requirements, it may be necessary to use one or more of the following protocols.

07.31 IGMP

Does the operator support IGMP with version 2 or above from the subscriber's end system to the operator's router?

Alternatives: YES or NO.

07.32 MSDP

Explanation: MSDP (Multicast Source Discovery Protocol) is used for joining together rendezvous points (RP) so that the sources available within one's own network will come to the knowledge of other logical networks.

Does the operator support MSDP at the access point?

Alternatives: YES or NO.

07.33 PIM-SM

Explanation: PIM-SM (Protocol Independent Multicast – Sparse Mode) is used for building Multicast distribution trees.

In PIM-SM there must be one of the following alternatives:
- using an RP in the operator's network for global groups
- exchanging information on active senders with MSDP, or
- using a BGMP/mask.

Does the operator support PIM-SM at the access point?

Alternatives: YES or NO.

07.34 Use of PIM-SM but not MSDP

Explanation: In cases where the interface at the access point between subscriber and operator uses PIM-SM but not MSDP, the subscriber has to indicate an RP within the operator's network.

Indicate an IP address for RP within the operator's network.

07.35 Use of NLRI Multicast when BGP4 is not used

If the interface at the access point between subscriber and operator does not use BGP4 with NLRI Multicast but there are Multicast sources within the subscriber's network, can the operator advertise prefixes belonging to the subscriber to the rest of the Internet with NLRI Multicast?

Alternatives: YES or NO.

07.38 BGMP

Is information exchange with the BGMP protocol supported?

Alternatives: YES or NO.

Routing information transferred from operator to subscriber

07.41 Full Internet routing (without default)

Does the operator transmit a prefix/mask for all destinations currently reaachable on the Internet?

Alternatives: YES or NO.

07.42 Selected routing information
Explanation: The selection criterion can be based on BGP AS-path filtering, a list of prefix filters (with mask and length), BGP communities or a combination of these.

Does the operator only transmit a selected portion of the prefix/mask combinations known?

Alternatives: YES or NO.

07.43 Default route to the subscriber

Does the operator transmit exclusively by a default route (prefix/mask = 0/0) to the subscriber?

Alternatives: YES or NO.

Routing information transmitted from subscriber to operator

07.51 Only address blocks from the operator's address space

Doe the operator only accept addresses included in the address block allotted to the operator?

Alternatives: YES or NO.

07.52 Prefixes up to a certain length

Explanation: In order for all parts of the Internet to be reachable, a special agreement may be needed with another operator, who may possibly have different max. length requirements for routing acceptance. The operator should inform the subscriber of any such known conditions on every occasion.

Does the operator accept prefixes up to a certain length, e.g. an old-fashioned "class C" network of 24 bites length or a "class B" network of 16 bites length?

Alternatives: YES or NO.
If YES: Indicate in no. bites the longest prefix which the operator will accept.

07.53 Arbitrary prefix registered in the subscriber's name

Does the operator accept an arbitrary prefix registered in the subscriber's name?

Alternatives: YES or NO.

07.54 Address from another operator's address block

Will the operator accept an address (sub-block) from another operator's address block?

Alternatives: YES or NO.

07.55 Multihoming

Explanation: Multihoming means a subscriber being connected to more than one operator.

Does the operator's routing system support a configuration in which a subscriber is connected to one or more *other* operators?

Alternatives: YES or NO.

07.56 Filtering of routing information from subscriber

Does the operator implement filter lists for filtering of the routing information accepted from a subscriber?

Alternatives: YES or NO.

07.57 Transmission of information concerning Unicast addresses containing Multicast sources

Explanation: Information from subscriber to operator as to which Unicast addresses may contain Multicast sources can be transmitted in a variety of ways.

(a) Are all Unicast addresses presumed also to be Multicast sources?

Alternatives: YES or NO.

(b) Does the subscriber transmit information about Unicast addresses for Multicast sources in the form of an accessions list, while the operator attends to their inputting in the Multicast-capable part of the Internet?

Alternatives: YES or NO.

(c) Does the subscriber transmit information containing Unicast addresses of Multicast sources, using BGP4+ as Multicast NLRI?

Alternatives: YES or NO.

Descriptive formats of access lists

07.61 Ripe-81

Does the operator support Ripe-81 format?

Alternatives: YES or NO.

07.62 Ripe-181

Does the operator support Ripe-181 format?

Alternatives: YES or NO.

07.63 RPSL

Does the operator support RPSL?

Alternatives: YES or NO.

07.64 List of prefixes/masks as e-mail

Does the operator handle a list of prefixes/masks as e-mail?

Alternatives: YES or NO.

07.65 List of prefixes/masks as fax

Does the operator handle a list of prefixes/masks as fax?

Alternatives: YES or NO.

07.66 Authentication with PGP or S/MIME

Does the operator authenticate information received with PGP or S/MIME?

Alternatives: YES or NO.
If YES, indicate which ones are supported.

07.71 BGP dampening of external routes

a) Are incoming external routes BGP dampening?

Alternatives: YES or NO.

b) If BGP dampening is used other than the standard settings of the routers or RIPE's recommendation, describe the configuration used.

07.72 BGP dampening of subscriber routes received

Are incoming subscriber routes BGP dampening?

Alternatives: YES or NO.

b) If BGP dampening is used other than the standard settings of the routers or RIPE's recommendation, describe the configuration used.

DHCP server function at the access point

07.81 DHCP server at the access point

Explanation: DHCP is a protocol for automatically configuring end systems connected to a network. DHCP is used when an end system requests to be assigned an IP address and for obtaining other information necessary for the automatic configuration of the end system when connecting to a new network.

Is a DHCP server provided at the access point?

Alternatives: YES or NO.

07.82 Address space in static addresses and dynamic address pool

Explanation: In some cases a certain portion of the address space which the operator has allotted the subscriber has to be set aside for "always on" static addresses, e.g. for mail server, DNS server, web server, while the rest of the available address space is placed in a pool for dynamic allocation to new end systems connected.

Is division of address space into static addresses and a dynamic address pool provided?

Alternatives: YES or NO.

07.83 Log function on DHCP server

Explanation: For fault diagnosis and handling of cases of abuse of network resources occurring from the subscriber's network against another party on the Internet, a log function may be needed concerning the DHCP server allocations of time/date/IP address/MAC address.

Does the operator have a log function on the DHCP server?

Alternatives: YES or NO.

If YES, how long are the logs saved?
State no. days.

08 Performance on the operator's network and at the access point

08.11 Minimum throughput capacity at the access connection

Explanation: The intention is to measure the minimum performance between the access point and the IP function on the operator's network.

Indicate the minimum throughput offered to the subscriber, ***measured as IP datagram*** containing UDP packets sent from the subscriber's equipment to the operator's backbone network router.
(Commentary: A loopback function can be used at one end. This can be turned off, with the operator turning as required.) Verify the performance of equipments involved.

Give minimum throughput in bit/s.
Describe the method of measurement.

Commentary: The purpose of 08.11 and 08.12 is to identify the basic performance of the service/method chosen for arranging data transport between the subscriber's connecting equipment and the logical IP network, the reason being that some operators have opted for using a level 2 service, e.g. in the form of ATM to define the performance of the IP service provided.

08.12 Maximum throughput capacity at the access connection

Explanation: The intention is to measure the maximum performance between the access point and the IP function in the operator's network.

State the maximum throughput offered to the subscriber ***measured as IP datagram*** containing UDP packets sent from the subscriber's equipment to the operator's backbone network router and vice versa, i.e. from equipment connected to a backbone network router to the subscriber. (Commentary: A loopback function can be used at one end.)

Give maximum throughput in bit/s.
Describe the method of measurement.

08.21 Maximum MTU prior to fragmentation of packets

Explanation: Maximum MTU (Maximum Transfer Unit) between two subscribers is the size in bytes of the biggest IP packet which can be sent before the network routers fragment the IP packets.

Is the operator capable of sending ICMP messages indicating that fragmentation has occurred, without these packets being filtered off in a security function?

Alternatives: YES or NO.

If YES, indicate the largest possible packet (measured in bytes) which can pass between two subscriber connections before being fragmented by the operator's network.

08.30 Method for measuring throughput

Explanation: The intention is to measure the total network's service performance between two subscriber connections to the same operator. Since the earlier measurements have been concerned with the performance of the access lines (08.11 and 08.12), it remains, among other things, to measure the performance of the operator's service between the two connecting points (see 08.31). The distance requirement below is related to the fact of our wishing to measure through the operator's network, not just on two access lines which could be connected to the same exchange point/router.

Method of measurement: Two subscribers are connected to the operator's network with throughput performance corresponding to the connection capacity (bit/s as per 04.11).

The connections are to be made to two different exchange points for the backbone network within the operator's network. The exchange points for the backbone network shall be at least 150 km apart.

Traffic is sent as TCP streams in both directions, e.g. by using the TCP loopback port of a computer system in one connection and TCP spray from the other connection.

In the test, a data quantity of 14.4 Mbyte is to be sent, corresponding to 60 seconds' traffic at 1,920 kbit/s. A reference file is obtainable from the ICT Commission.

The test is performed three times, for an hour each time, 09.00-10.00 hours, 14.00-15.00 hours and 21.00-22.00 hours, on weekdays.

The operator shall indicate the lowest transmission time value in seconds which is never fallen short of in any of the tests.

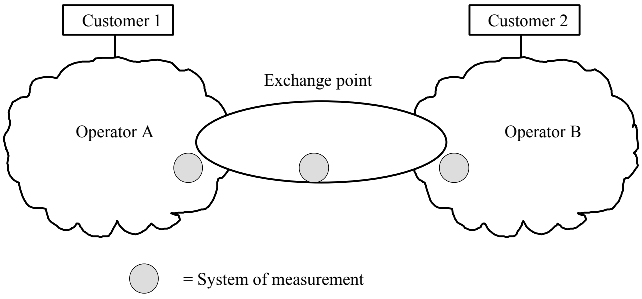


Figure to illustrate system of measurement. Throughput measurements within Operator A take place to A's system of measurement. Operator B's subscribers, similarly, measure in relation to B's system of measurement. Between the operators, measurements are made to the "opposing" system of measurement "behind" the exchange point. The common system of measurement is used for measuring the operator's throughput performance in relation to the exchange point. The system of measurement at the exchange point is one of the resources which Netnod[1] AB provides as a common resource for operators.

08.31 Throughput between two subscriber connections to the same operator.

Explanation: Throughput is measured according to the method indicated in 08.30 and with the connection capacity defined as per 04.11.

What is the throughput between to subscriber connections to the same operator?

Give throughput in bit/s.

08.90* Measuring points in North America

Commentary: Here each operator involved in a procurement or the equivalent indicates his favourite points. For evaluation, measurement shall take place from each operator's network to all these points, and the average throughput (see 08.92) and RTT are to be calculated (see 08.96). The system of measurement shall be connected via 100 Mbit/s Fast Ethernet Full Duplex.

Indicate two exchange points in the USA to be used for measuring throughput and roundtrip time respectively. These exchange points must be generally accessible from the entire Internet.

08.91* Throughput between a subscriber connection and the national main exchange point in Stockholm

[1] Netnod AB = Administers a number of Swedish exchange points.

Explanation: The throughput between a subscriber connection with a connection capacity defined as per 04.11 and the main exchange point in Stockholm, measured in accordance with the principle stated in 08.30.

What is the throughput between a subscriber connection and the main exchange point in Stockholm?

Give throughput in bit/s.

08.92* Throughput between a subscriber connection and points of measurement in North America

Explanation: The throughput between a subscriber connection with a connection capacity defined as per 04.11 and points of measurement in North America as per 08.90, measured in accordance with the principle stated in 08.30. Calculated as the average of these measurements.

Give throughput in bit/s.

08.93* Throughput to a subscriber connected to another operator within the Swedish IT infrastructure

Explanation: Throughput is measured, in accordance with the principle stated in 08.30, between a subscriber connection with connection capacity defined as per 04.11 and a subscriber connected to another operator within the Swedish IT infrastructure.

What is the throughput to a subscriber connected to another operator within the Swedish IT infrastructure?

Give throughput in bit/s.

08.94* Minimum throughput to a subscriber outside the Swedish IT infrastructure

Explanation: Throughput is measured, in accordance with the principle stated in 08.30, between a subscriber connection with connection capacity defined as per 04.11 and a subscriber connected to an operator outside the Swedish IT infrastructure.

What is the minimum throughput to a subscriber connected to an operator outside the Swedish IT infrastructure?

08.40 Roundtrip delay method of measurement

Method of measurement: A computer system is connected to the connection point with an Ethernet interface.

ICMP Echo Reply messages (pings) with a data content of 64 bytes are sent to another computer system connected to the opposing subscriber connection.

The time given is that elapsing from the whole packet being sent to the whole packet being received back again.

To compensate for any system delays in the measuring equipment, 5 ms is deducted from the value recorded by the computer system.

The test is performed three times, for an hour each time, 09.00-10.00 hours, 14.00-15.00 hours and 21.00-22.00 hours, on weekdays. The measurement is conducted by sending an ICMP echo packet (ping) every other second during the 15-minute test period, making a total of 450 packets of 64 bytes each.

The measured value is the average delay time for packets received within 2 seconds of being sent, but at least 98% of all packets shall be returned within 2 seconds in order for the measurement to be approved.

08.41 Roundtrip delay between two subscribers' connections

Explanation: State the roundtrip delay between two subscriber connections with the connection capacity defined as per 04.11 and measured in accordance with the method indicated in 08.40.

To be stated in milliseconds.

08.95* Roundtrip delay between a subscriber connection and the national main exchange point in Stockholm

Explanation: Roundtrip delay between a subscriber connection with a connection capacity defined as per 04.11 and a main exchange point in Stockholm, measured in accordance with the method indicated in 08.40.

To be stated in milliseconds.

08.96* Roundtrip delay between a subscriber connection and measuring points in North America

Explanation: Roundtrip delay between a subscriber connection with a connection capacity defined as per 04.11 and measuring points in North America as per 08.90, measured in accordance with the method indicated in 08.40. Calculated as the average of these measurements.

To be stated in milliseconds.

08.51 Performance guarantees offered by the operator

Indicate the performance guarantees applied by the operator.

08.61 One-way performance measurements

Method of measurement: If the subscriber's access router have a built-in measurement function, that function is to be used. Failing such a function, NTP time-stamped packets can be sent from the using system to the receiver. The transmitting system sends packets with the actual time, compensated in such a way that the time stamp on the packet shows the time when the packet as a whole left the transmitting system. The receiver time-stamps the packet when the whole packet has been received. This calls for very close synchronization of the sender's and receiver's time pieces. Performance is stated in bit/s.

08.71 Performance measurements of services with asymmetric performance

Method of measurement: The direction with the **lower** bandwidth is measured in the same way as other points in this section. Measurement of the direction with the **higher** bandwidth is conducted in accordance with one of the following alternatives:

a) The subscriber's access router has access to an in-built function for measurement, in which case that function is used. This can be regarded as a special instance of. 08.61. Performance is given in bit/s.

b) The subscriber's access router does not have access to in-built function measuring tools (e.g. ADSL delivered as Ethernet TP interface), in which case no measurement is possible.

08.81 Multicast performance measurements

Explanation: Multicast performance resembles Unicast performance in relation to network capacity, but in addition to Unicast functionality it has steering mechanisms etc. for managing the construction of Multicast distribution trees. In addition to lost packets, Multicast may cause duplicated packets.

Method of measurement: A sender and three receivers within the operator's network, together with a sender and a receiver at a national exchange point according to the same model as Unicast. Measurement is done using MRM (Multicast Routing Monitor Protocol, see Internet-draft "Justification for and use of Multicast Routing Monitor (MRM) Protocol" 26th February 1999), in which the receivers are test receivers and the senders test senders. The operator provides a monitoring station which can configure senders and receivers.

The following are to be measured:

?? Packet loss per receiver.
?? Duplicated packets per receiver.
?? Packet delivery delay.
?? Sender-receiver throughput.
?? Availability.

Throughput is stated in Mbit/s of traffic sent from the test sender and received by all test receivers with less than X% packet loss and Y% packet duplication. All receivers must attain these minimum requirements.

(a) State the value of X and Y. (These are stated in %, referring to packet loss and duplication respectively.)

(b) State, in kbit/s or Mbit/s, the minimum throughput without packet loss or duplication with the X and Y limit values.

Method of measurement: A packet is sent from a test sender to a known Multicast group every 60 seconds for 24 hours, making 86,400 seconds altogether.

Test sender: A test sender can be configured to send packets of a certain size and at a certain interval. The size is defined in bytes and the interval in ms. To achieve test traffic corresponding to the throughput to be tested, the test sender is configured to send 64-byte packets at an interval giving an average throughput for 60 seconds corresponding to the throughput capacity it is intended to measure.

Test receiver: A test receiver is configured to listen to a certain Multicast group corresponding to the group which the test sender transmits to and to report the performance received to the Test Manager.

(c) State number of packets lost and duplicated during the period for which measurement continues, i.e. 24 hours.

09 Dynamic parameters

09.30 Method of measurement

Method of measurement: The IP addresses of the different root-name servers are pinged from a subscriber connection (with a connection capacity as per 04.11). One hundred 64-byte pings are transmitted at intervals of 2 seconds. The test is performed at 10.30, 13.30 and 21.30 on weekdays. At least 90% of the packets shall be returned within 2 seconds in order for the test to be passed.

The average for each of the servers is calculated from the averages of the pings to each server, and the average is then calculated for each observation.

09.31 Average distance to root-name servers

Give the average distance to root-name servers in milliseconds as per the method of measurement stated in 09.30.

To be stated in milliseconds (ms).

09.32 Average distances to enumerated exchange points

State average distances in milliseconds to enumerated exchange point. Calculate in accordance with the principles stated in 09.30, though the operator has a free choice of equipment at the exchange point. The following exchange points are referred to unless otherwise indicated:

Stockholm, D-GIX
Göteborg, the exchange point

London, Linx
Pennsauken, NAP
Virginia, MAE-East
California, MAE-West
Amsterdam, Ripe NCC

To be stated in milliseconds (ms).

09.33 Max percentage packet loss in own network

Explanation: When measuring roundtrip delay as per 08.41 and 08.95, state maximum number of packets lost expressed as a percentage. “Packets lost” refers here to packets which vanished completely or were delivered with a delay exceeding 2 sec.

Give the maximum number of packets lost in %.

09.41 Expansion of the backbone network

At what average load on the backbone network during peak traffic (measured as a percentage of available transmission capacity) does enlargement take place?

09.42 Enlargement of capacity to national exchange points

At what average load (measured as a percentage of available transmission capacity) does enlargement of capacity to national exchange points take place?

09.43 Enlargement of capacity to international exchange points

At what average load (measured as a percentage of available transmission capacity) does enlargement of capacity to international exchange points take place?

09.51 Bandwidth delay quota for which the network is designed

Explanation: The bandwidth delay quota is stated as bandwidth in Mbit/s between the communicating systems at a delay RTT of 350 ms.

“Communicating systems” refers to TCP traffic between a subscriber of the operator’s and an arbitrary opposite number. It is presumed that the access connections to the subscriber are limited for bandwidth, not backbone network, which we also take to include connections to other operators.

The bandwidth delay quota is a yardstick of the size of the buffers which the network elements have for outfeed in the following cases:

(1) The network element is installed at a point in the network where incoming burst traffic from several sources has more traffic per unit of time than the capacity of the outgoing interface. The buffer memory is used for temporary storage of data until the burst has faded and the end systems which

communicated through this segment of the network have had the possibility of downscaling the quantity of data they transmit.

(2) The network element is located at the transition between a high-capacity connection and one with lower capacity, and the buffer memory is used for evening out traffic bursts to match the average throughput.

Note that this applies to all intermediary steps in the network between the communicating systems, and that the strategy should be to be able to store enough traffic for the buffer to store a burst of duration RTT with the quantity of data corresponding to the biggest flow that can be exchanged.
350 ms is deemed the biggest RTT on the Internet today. How large a flow between two arbitrary points in the network is the smallest buffer capable of storing?

What bandwidth delay quota is the operator's network dimensioned for?

State for traffic:
(a) between subscribers to the same operator,
(b) between a subscriber and a national exchange point (see Unicast).
(c) to an international exchange point on each continent.

State values for (a) – (c), above, in Mbit/s.

09.52 Queue management strategy in the event of limited resources

Commentary: If, for example, a subscriber wants to build a VPN network for telephony and data between different geographic units, then probably the desire is for the operator to give telephony more priority than web traffic on the connection to the subscriber.

State queue management strategy within the backbone connections of the backbone network (e.g. FIFO, RED, WRED, WFQ).

09.53 Queue management strategy to subscriber line

State queue management strategy on link to connection point (e.g. FIFO, RED, WRED, WFQ).

09.54 Queue management in the event of traffic from flows with a different traffic volume or other criteria

When a queue situation develops in the network, will consideration be paid to traffic from flows with a different traffic volume or other criteria?

Alternatives: YES or NO.
If YES, describe the function and implementation intended.

09.55 Routing statistics

Explanation: In cases where dynamic routing is exchanged between operator and subscriber, it is sometimes of interest to know the stability of the routing in relation to a certain AS.

Can the operator give 24-hour statistics showing the number of routing flaps (i.e. reachability information going from reachable to unreachable and back to reachable, or vice versa) for a certain prefix obtained from AS which are neighbours of the operator's, including the subscriber himself?

Alternatives: YES or NO.

09.56 Routing stability

What is the largest number of routing flaps which the operator permits for a prefix received from a subscriber before the operator contacts the subscriber?

Stated as number of routing faops per prefix per 24 hours.

Commentary: In cases where the number of routing flaps exceeds the agreed limit value, the operator is absolved from his commitment regarding availability and performance.

10 Accessibility/inaccessibility

10.11 Inaccessibility on access line

Method of measurement: Inaccessibility on the access line refers to the time, measured in minutes per month, when traffic *cannot* be conducted between the access point and the opposite connection point in the operator's network. Monitoring is to take place from the operator's Network Operations Center.

An access line is deemed inaccessible when:

?? Traffic cannot be conveyed to the operator's access router for periods of more than 30 seconds.

?? When more than 0.2% of packets transmitted have an incorrect checksum or alternatively more than 2% of packets transmitted disappear at a traffic load equalling 80% of connection capacity.

?? If the line statistically changes from up or down more than 24 times per 24 hours.

State inaccessibility in minutes per month for the access line.

Commentary: The second consecutive measurement can be made by the subscriber, but only if the subscriber has SNMP reading access to the router on the operator's side. The operator must then have replied to the router on the operator's side. The operator must then have replied YES to the SNMP question in 12.22.

10.12 Inaccessibility between two subscribers within the operator’s network.

Method of measurement: Inaccessibility is measured in minutes per month for which traffic *cannot* be conducted between two subscriber exchange points as stated below.

A connection is deemed to exist between two subscribers if ICMP echo packets can be transmitted between two computer systems with each subscriber and 99% of IP packets of 64 bytes are returned to the dispatching computer system within 150 ms measured for 1 minute. Measurement proceeds continuously.

State inaccessibility in minutes per month.

Commentary: If the operator can show that one of the subscribers has overloaded access lines or overloaded access equipment, this requirement cannot be met.

10.13 Inaccessibility of packet forwarding to national main exchange point.

Method of measurement: Inaccessibility is measured in minutes per month for which traffic *cannot* be conducted between a subscriber exchange point and the operator’s equipment at a national exchange point; method of measurement as stated below.

A connection is deemed to exist between subscriber and exchange point if ICMP echo packets can be transmitted between two computer systems with subscriber and national exchange point and 99% of IP packets of 64 bytes are returned to the dispatching computer system within 75 ms measured for 1 minute. Measurement proceeds continuously.

Disruption of the operator’s logical support system as per 10.90 is here deemed equivalent to packet loss.

The time requirement is based on the existence here of an access line. Connection to a national exchange point is deemed to be part of the operator’s backbone network.

State inaccessibility in minutes per month.

10.14 Inaccessibility of packet forwarding to international exchange point

Method of measurement: Inaccessibility is measured in minutes per month for which traffic *cannot* be conducted between a subscriber exchange point and equipment designated by the operator at a national exchange point (as per 09.32); method of measurement as stated below.

A connection is deemed to exist between subscriber and international exchange point if ICMP echo packets can be transmitted between two computer systems with subscriber and national exchange point and 99% of IP packets of 64 bytes are returned to the dispatching computer system within 175 ms measured for 1 minute. Measurement proceeds continuously.

State inaccessibility in minutes per month.

10.21 Accessibility guarantees

State here the guarantees offered by the operator.

10.22 Redundant connections between backbone network exchange points with at least 50% of normal capacity

Are the connections between backbone network exchange points (exchange points to which subscribers are connected) redundant with at least 50% of normal capacity?

Alternatives: YES or NO.

10.23 Redundant subscriber connections are provided

Can redundant subscriber connections be provided?

Alternatives: YES or NO.

10.24 Connecting time for transition to reserve path

Explanation: The reference here is to the longest downtime (time when packets do not reach their recipient) caused by faults in network elements or transmission within the operator's network for which redundancy exists.

In the event of a subscriber being redundantly connected, how long does it take for full traffic to be resumed by way of an alternative connection if the main path is knocked out?

State in seconds the time for which ICMP echo replies are *not* obtained from opposing systems; method of measurement as per 10.12. Commentary: Applies at IP level only.

State connecting time in seconds.

10.25 Disconnection time for reversion to main path

In the event of disconnection to an alternative path as per 10.24, indicate by the same method of measurement the downtime for re-establishing a main traffic path. Commentary: Applies at IP level only.

State downtime in seconds.

10.26 Connection of subscriber to more than one operator

Is the possibility provided of connecting a subscriber to more than one operator in order to obtain redundancy?

Alternatives: YES or NO.

10.27 Connecting time for transition to reserve path through another operator

To be stated in seconds; method of measurement as per 10.24.

State connecting time in seconds.

10.28 Disconnecting time for reversion to main path through another operator

Explanation: This presupposes that the customer has his own AS and uses BGP with both operators. Use the method of measurement stated in 10.25.

State downtime in seconds.

10.90* The operator's logical support system

Is the operator's logical support system (DNS etc.) designed so that a connection can be established in according with the IP architecture within Sweden, irrespective of resources outside the Swedish IT structure?
Alternatives: YES or NO.

11 Traffic filtering

11.31 Packet filtering at the access point

Does the operator offer to install, on the subscriber's behalf, a filter function at the access point, so that certain traffic between the subscriber's side and the operator's will be blocked?

Alternatives: YES or NO.

11.32 Filtering based on IP addresses

Can filtering conditions be stated based on the sender or receiver address of the IP packet?

Alternatives: YES or NO.

11.33 Filtering based on protocol

Can filtering conditions be stated based on IP protocol? (e.g. UDP, TCP, GRE etc).

Alternatives: YES or NO.

11.34 Traffic filtering based on port number

Can filtering conditions be stated based on TCP/UDP port number?

Alternatives: YES or NO.

11.35 Traffic filtering based on direction

Can filtering conditions be based on the direction of traffic through the access point?

Alternatives: YES or NO.

11.36 Filtering of source routed packets

(a) Can the access point be configured in such a way that packets with the IP source route option activated are not admitted to the subscriber's network?

Alternatives: YES or NO.

b) Filtering of "short fragments". Can the access point be configured in such a way as to block packets with fragments that are so short that complete headers cannot be accommodated (and thus cannot be assessed by the filter)?

Alternatives: YES or NO.

11.37 Verification of the filter function

a) Is the filter function verified regularly?

Alternatives: YES or NO.

b) Is the filter function always verified after a change has been made?

Alternatives: YES or NO.

11.41 The subscriber can insert a filter himself

Does the subscriber have access to and the possibility of arbitrarily configuring the filter function at the access point?

Alternatives: YES or NO.

11.42 The operator filters prefixes intended for local sue and test use

Does the operator filters prefixes intended for local sue and test use (RFC 1918) when receiving routing both from subscribers and from other networks?

Alternatives: YES or NO.

12 Monitoring functions

This section deals with monitoring functions available to the subscriber.

12.11 SNMP with read only access to router

Does the subscriber have access to the connection point equipment for reading parameters including his own access point and remote connection or the equivalent with the operator's network?

Alternatives: YES or NO.

12.12 SNMP with write access to router

Does the subscriber have access to the connection point equipment for reading and writing parameters including his own access point and remote connection or the equivalent with the operator's network?

Alternatives: YES or NO.

12.13 Telnet access to access router, read only

Is it possible for the subscriber to connect up with the connection point equipment with Telnet and after connecting to read operational statistics and issue simple commands such as ping and traceroute?

Alternatives: YES or NO.

12.14 Telnet access to access routerswrite

Is it possible for the subscriber to connect to the connection point equipment with Telnet and after connecting to read operational statistics and arbitrarily reconfigure the access point?

Alternatives: YES or NO.

12.21 SNMP access to backbone network router against access router

Does the subscriber have access for SNMP reading to the equipment in the operator's network which connects with the subscriber's connection point?

Alternatives: YES or NO.

12.22 SNMP access to all backbone network routers in the operator's network

Does the subscriber have read access to the equipment which makes up the operator's backbone network and is shared between several subscribers?

Alternatives: YES or NO.

Services

13 Reachability

The following is a specification of differentiated services with limited reachability. The subscriber can opt for different degrees of reachability for different parts of the world, possibly with differing capacities.

13.11 All destinations within the operator's own network

Does the subscription include access to all destinations within the operator's network?

Alternatives: YES or NO.

13.12 All destinations advertised to any of the named exchange points

Does the subscription include access to all destinations advertised to any of the named exchange points as per point 09.32?

Alternatives: YES or NO.

13.21 Inaccessible destinations

State known reachability limitations of other networks with which traffic cannot be exchanged. State as full AS numbers or individual prefix/mask lengths.

13.22 Multicast forwarding

Explanation: With Multicast, traffic is only to be forwarded from source to receiver in cases where BGMP routing information has been obtained from the source under a direct or indirect peering agreement.

State full AS numbers or individual prefix/mask lengths for destinations to which the operator cannot forward Multicast packets.

13.23 Multicast default routing

Does the operator use default routing for Multicast?

Alternatives: YES or NO.

13.41 Performance guarantees to other operator

State, by quoting their AS numbers, the other operators to whom performance guarantees are offered.

13.50 Connected to national exchange points

Is the operator connected to all active national exchange points co-ordinated within SOF?

Alternatives: YES or NO.

If NO, describe how traffic to common resources placed at exchange points has been arranged.

13.51 Passage of packets to national Internet exchange point

Can packets of all kinds, irrespective of options (e.g. source route), pass through the operator's backbone network and connections to national Internet exchange points?

Alternatives: YES or NO.

15 Address translation functions (NAT)

15.11 NAT at the access point

Can the access point be NAT configured so that IP addresses intended for local use (RFC 1918) can be used on the LAN side and then translated into a globally unique IP address for Internet traffic?

Alternatives: YES or NO.

15.15 NAT with translation 1-1

Can the access point be configured so that each unique address on the LAN side will, if necessary, obtain a globally unique IP address for Internet communication?

Alternatives: YES or NO

15.16 NAT with overload translation

Can the access point be configured so that all addresses on the LAN side share a globally unique IP address for Internet communication?

Alternatives: YES or NO

15.17 Protocol for NAT function

Explanation: The design of certain protocols prevents them from working in an NAT, added to which, support for different protocols changes with the passing of time.

Which protocols are supported by the NAT function?

Indicate the protocols supported by the NAT function.

15.21 NAT for managing multiple connection to various operators

Can the access point be configured for multiple connection to various operators?

Alternatives: YES or NO.

If YES, describe how this is done.

15.22 The access point and use of globally unique addresses

Is it possible for the access point to use globally unique addresses allocated to equipment connected to the access point?

Alternatives: YES or NO.

16 DNS

16.11 Name-to-number for network elements in the operator's network

Does the operator provide name-to-number lookup in a DNS database for all network elements in the operator's network with an IP address?

Alternatives: YES or NO.

16.12 Number-to-name for network elements in the operator's network

Does the operator provide number-to-name lookup in a DNS database for all network elements in the operator's network which might be transited by subscriber traffic or emit IP packets?

Alternatives: YES or NO.

16.13 Support for secure DNS

Does the operator's DNS server support Internet standard for secure DNS as indicated below?

Commentary: It is expected that encryption algorithms which are supported, together with general handling of DNSSEC in the "se" zone, will be specified by ISOC-SE in a BOK.

(a) Does the operator sign zones in in-addr.arpa from which a zone has been delegated for number-to-name lookup to a subscriber's DNS server?

Alternatives: YES or NO.

(b) Does the operator sign a KEY record for a delegated zone for number-to-name (PTR) from which a zone has been delegated to a subscriber's DNS server?

Alternatives: YES or NO.

(c) Does the operator manage, on a subscriber's behalf, KEY management for a customer's zone which has been delegated from another registry on the Internet in case where the DNS for the zone is handled by the operator?

Alternatives: YES or NO.

(d) Does the operator's DNS server verify signatures for incoming DNS records?

Alternatives: YES or NO.

16.14 Duplicated DNS servers

Does the operator have duplicated operating systems for DNS servers positioned in the same place and behind the same non-duplicated network connection?

Alternatives: YES or NO.

16.15 Duplicated DNS servers with dual connection

Explanation: The connections shall offer redundant connection to two exchange points. (Make sure that routing proceeds in such a way that BGP information for the address block used is created in a router close to the DNS system, so that there will be no advertising of "black holes".)

Does the operator have duplicated operating systems for DNS servers positioned in the same place with duplicate connections to the backbone network separately channelled and separate transport systems in other respects as well?

Alternatives: YES or NO.

16.16 Duplicated DNS servers in two geographically separate places

Explanation: The connections shall offer redundant connection to two exchange points and shall also have two paths out towards an international exchange point (NY-NAP). (Make sure that routing proceeds in such a way that BGP information for the address block used is created in a router close to the DNS system, so that there will be no advertising of "black holes".)

Does the operator have double DNS servers in separate geographic locations, connected to the backbone network via different redundant connections?

Alternatives: YES or NO.

16.21 Secondary DNS server for the subscriber's name and number

Does the operator offer secondary DNS server operation for a domain belonging to the subscriber?

Alternatives: YES or NO.

16.22 Primary DNS server for the subscriber's name and number

Does the operator offer primary DNS server operation for a domain belonging to the subscriber?

Alternatives: YES or NO.

16.23 Number-to-name delegation from the operator's address block to the subscriber's primary DNS server

In cases where the operator has delegated IP addresses from his own address block to the subscriber, are they delegated to the subscriber wishing to operate his own DNS server, regardless of the size of the address space?

Alternatives: YES or NO.

16.24 Functions where the operator runs a secondary DNS

Explanation: When the operator runs a secondary DNS for the subscriber's domains and the subscriber adds new second-level domains to his top-level domain, these second-level domains also need a secondary DNS.

State the following:
(a) How are secondary DNS managed by the operator?
(b) Is this a separate service?
(c) How does the subscriber communicate information about a new domain to the operator?
(d) How does the operator monitor the functioning of DNS for second-level domains?

16.25 Functions where the operator runs a primary DNS

In cases where the operator runs the subscriber's primary DNS, are dynamic DNS updates supported, e.g. from the operator's DHCP server?

Alternatives: YES or NO.

16.90* DNS server as per technical specifications from ISOC-SE

Are the DNS servers operated in accordance with the technical specifications (in the form of BOK) issued by ISOC-SE?

Alternatives: YES or NO.

17 E-mail

17.11 The operator can be reached via e-mail as per Internet standard

Is it possible to communicate with all functions within the operator's organization by e-mail as per Internet standard (RFC 822/RFC 821/RFC 1521/RFC 1522)?

Alternatives: YES or NO.

17.12 The operator's MTA DNS server is used for address lookup

Does the operator's Internet mail manager use DNS and, where relevant, MX or A records to find an opposite number of exchanging SMTP dialogue when transmitting e-mail?

Alternatives: YES or NO.

17.13 The operator provides a secondary mailhost

Explanation: A secondary mailhost is used, for example, in the event of the subscriber's e-mail system for some reason being inaccessible from the sender's computer. A secondary mailhost shall be capable of storing 150 % of the subscriber's normal mail flow for 7 days.

Can the subscriber indicate in his DNS server an alternative computer system as recipient of SMTP traffic to a certain domain?

Alternatives: YES or NO.

17.14 Intermediate storage space for a subscriber's e-mail

Explanation: By storage space is meant the space available for storing e-mail on behalf of a subscriber.

Is the e-mail stored with the operator in the event of the subscriber's SMTP mail system being inaccessible?

Give size in MB storage space per subscriber.

Commentary: 17.13 and 17.14 indicate essentially the same function, but 17.14 allows more scope for specifying the function.

17.15 Return of e-mail

Is an attempt made to reach the subscriber's MTA before return takes place?

Alternatives: YES or NO.
If YES, state the number of days for which attempts are made.

17.16 Storage of e-mail

Is the subscriber's e-mail manager contacted in the event of e-mail having been stored for more than a certain number of days?

Alternatives: YES or NO.
If YES, state number of storage days.

17.17 Operator's e-mail system configured with "No relay"

Explanation: A No relay function is necessary to prevent the mail system being used for forwarding spam. This also means that there have to be routines for an exchange of information between operator and subscriber, in order to define which addresses the operator is to act as intermediate storage system for.

Is the operator's e-mail system configured with "No relay", meaning that only e-mail with known sender and receiver addresses will be forwarded?

Alternatives: YES or NO.

Extra e-mail services

17.21H Gateway to UUCP

17.22H Gateway to X.400

17.23H Gateway to X.400 with MIME support for attachments

17.24 The operator provides a complete e-mail function

Does the operator provide a complete e-mail function which manages the whole of the subscriber's domain and provides individual mailboxes which can be reached from the outside world or from a connection within the subscriber's network?

Are POP2, POP3, IMAP and ESMTP supported as protocols?

Alternatives: YES or NO.

Commentary: The rest of this service can be designed in many different ways, e.g. with regard to storage space, number of mailboxes and performance.

17.25 The operator provides parts of an e-mail function

In cases where parts of an e-mail function are provided, which protocols are supported?
(a) Is POP2 supported?

(b) Is POP3 supported?
(c) Is IMAP supported?
(d) Is SMTP supported?
(e) Is ESMTP supported?
(f) Is SMTP Service Extension for Authentication supported?
(g) Is TLS supported as en encryption mechanism for any of the above services?

The answer to (g) shall consist of a description of which systems and in which cases only SSL is used and not TLS.

(h) Are any other access mechanisms than passwords in clear supported for POP2, POP3, IMAP and SMTP AUTH?

The answer to (h) shall comprise a list of the mechanisms supported per service, e.g. stating that SASL is supported for IMAP, together with a list of the SASL mechanisms supported.

18 NTP

18.11 NTP server within the operator's network

Explanation: the NTP service shall be designed so that deviation from UTC time is at no time less than 25 micro seconds at the access point.

When the equipment is uncertain of the correct time, no answer to the time question shall be given to the subscriber's equipment.

Is there a Stratum-1 NTP server within the operator's network?

Alternatives: YES or NO.

18.12 Duplicated NTP server within the operator's network

Is there a duplicated Stratum-1 NTP server within the operator's network?

Alternatives: YES or NO.

18.13 Cryptosigned time indication

Is a cryptosigned time indication supported?

Alternatives: YES or NO.

18.21 NTP/SNTP at the access point

Is NTP/SNTP available at the access point, i.e. can the equipment used for activating the access point provide NTP and SNTP against the subscriber's network?

Alternatives: YES or NO.

18.22 NTP function within the operator's network with IP multicast

Is there an NTP function within the operator's network which communicates with the aid of IP multicast?

Alternatives: YES or NO.

19 News

19.11 Newsfeed to the subscriber's server with NNTP

Does the operator provide newsfeed including all the groups which are circulated in the Nordic area?

Alternatives: YES or NO.

19.12 Operator's throughput delay

The news distribution should have such capacity that an insertion to a group specified at the time of procurement shall reach the subscriber not more than X minutes after being sent to the operator's server, provided the subscriber has only subscribed to this group.

State value of X in minutes.

19.21 Total newsfeed

Is it possible for the operator to distribute all public news groups occurring?

Alternatives: YES or NO.

19.22 Selected groups from total newsfeed

(a) Does the operator have a policy which excludes the subscriber from access to any known groups/types of group?

Alternatives: YES or NO
If YES, state the policy in question.

(b) Can the subscriber specify preferred groups for reception?
Alternatives: YES or NO.

(c) can the subscriber specify groups not to be received?
Alternatives: YES or NO.

19.23 Pre-distribution spam selection

Does the operator carry out filtering for spam before news articles are distributed to the subscriber?

Alternatives: YES or NO.

19.31 NNTP server for news-reading from subscriber's clients
Does the operator provide an NNTP server from which users in the subscriber's network can read news with some form of client software?

Alternatives: YES or NO.

19.32 How long news groups are saved in the operator's system

(a) State how long a news group is saved in the operator's system.

(b) State number of days per hierarchy.

19.41 Number of incoming newsfeeds to the operator's news server

From how many international distribution sources is newsfeed received by the operator's news system?

State number.

Operating functions

"Office hours" refers to the hours between 08.00 – 17.00, Monday – Friday, other than on public holidays.

20 Subscriber support

Subscriber support

"Subscriber support" here means the operator being able to take the customer through the whole of the fault management process, from report to rectification.

20.11 Subscriber support during office hours

Is a helpdesk function available to subscribers during office hours?

Alternatives: YES or NO.

20.12 Subscriber support outside office hours

Is a helpdesk function available outside office hours?

Alternatives: YES or NO.

If YES: State the times (e.g. "24 hours a day,
7 days per week").

20.13 Qualified technical assistance during office hours

Commentary: "Qualified technical assistance" means someone on the operator's premises being able to answer questions about BGP and external networks and to take part in fault diagnosis of DNS, networks, routing and external contacts with other operators.

Does the operator have qualified technical assistance available during office hours?

Alternatives: YES or NO.

20.14 Qualified technical assistance outside office hours

Commentary: "Qualified technical assistance" means someone on the operator's premises being able to answer questions about BGP and external networks and to take part in fault diagnosis of DNS, networks, routing and external contacts with other operators.

Does the operator have qualified technical assistance available outside office hours?

Alternatives: YES or NO.

If YES: State at what times (e.g. “24 hours a day and 7 days per week”).

20.15 Subscriber support via telephone

Can the subscriber support function be reached on a toll-free number?

Alternatives: YES or NO.

20.16 Subscriber support via e-mail

Can the subscriber support function be reached by e-mail and a personal acknowledgement received within 10 minutes of the e-mail reaching the operator’s SMTP system?

Alternatives: YES or NO.

Commentary: The reference here is to the time of day as specified in 20.11 or 20.12.

20.17 Subscriber support via fax

Can the subscriber support function be reached by telefax and a personal acknowledgement received within 30 minutes?

Alternatives: YES or NO.

Commentary: The reference here is to the time of day as specified in 20.11 or 20.12.

20.18 Subscriber support via web

Are subscriber support functions reachable on the web?

Alternatives: YES or NO.

20.90* Subscriber support in Swedish

Can the operator’s personnel provide subscriber support in Swedish?

Alternatives: YES or NO.

20.19 Subscriber support language

State the languages in which the operator’s personnel can provide subscriber support.

20.21 Faults are only handled if occurring within the operator’s own networks

Does the operator only deal with faults and problems occurring within the operator's own networks?

Alternatives: YES or NO.

20.22 Faults are handled for problems everywhere on the Internet

Explanation: Faults are handled for problems everywhere on the Internet by contacting the "next-hop" operator and the destination operator.

Does the operator pass on and monitor fault reports even if a fault can be deemed to lie in another operator's network?

Alternatives: YES or NO.

Trouble management

20.31 Trouble ticket updates are e-mailed

Is the subscriber continuously updated by e-mail while a problem is being dealt with for which a trouble ticket has been opened?

Alternatives: YES or NO.

20.32 Trouble ticket status accessible via the web

Given problem identification in the form of a trouble ticket id, can the subscriber himself track current status on the web?

Alternatives: YES or NO.

20.33 The subscriber is contacted when a trouble ticket is closed

When a fault reported by a subscriber has been rectified, is it regular practice for the subscriber to be contacted so as to verify that the fault has been put right?

Alternatives: YES or NO.

Traffic statistics accessible via the web

20.41 Traffic statistics at own access point

Does the operator supply the subscriber, via the web, with information concerning traffic and availability statistics for the subscriber's access point?

Alternatives: YES or NO.

20.42 Traffic statistics for backbone network connections

Does the operator supply his subscribers, via the web, with information on traffic and availability statistics on his own backbone network?

Alternatives: YES or NO.

20.43 Traffic statistics for connection to other operators

In cases where private connections exist to other operators, does the operator supply his subscribers, via the web, with information on traffic and availability statistics for the other operators' networks?

Alternatives: YES or NO.

20.44 Traffic statistics for connection to exchange points

Does the operator supply, via the web, information on traffic and availability statistics for his own connections to national exchange points?

Alternatives: YES or NO.

Availability statistics

20.51 Availability on own line

Does the operator give a monthly account of backbone network accessibility from the access point?

Alternatives: YES or NO.

20.52 Access to exchange points

Does the operator give a monthly account of the accessibility of the national main exchange points for his backbone network?

Alternatives: YES or NO.

Routing stability

20.61 Statistics of routing stability

Does the operator issue monthly statistics of his routing stability regarding backbone networks and connections to other operators?

Alternatives: YES or NO.

Domain registrations

20.71H Registration of domain names

20.91* The operator is agent for registration of domain names under .SE

Is the operator agent for registration of domain names under the top-level domain .SE?

Alternatives: YES or NO.

20.92* Support systems for guaranteeing subscriber function for traffic within Sweden when registered under a top-level domain other than .SE

In the case of a subscriber electing to register under a top-level domain other than .SE, does the operator provide the support systems necessary for guaranteeing the subscriber's traffic function within Sweden in the event of connection with the outside world being broken or some other action occurring over which the operator has no control?

Alternatives: YES or NO.

20.74 Verification of information in the subscriber's DNS server together with forward and backward lookup and use of permitted characters only

Commentary: This means that name-to-number and number-to-name lookups are verified, and that verification takes place of only permitted characters as per RFC 952 being used in domain names.

Does the operator verify at regular intervals that information contained in the subscriber's DNS server is correct and agrees between forward and backward lookup?

Alternatives: YES or NO.
If YES: describe how this is realised within the operator's infrastructure.

21 Operational monitoring

In cases where the operator monitors a dynamic parameter, e.g. the load on a network element, it is presumed that the material collected will be saved for at least 31 days, so that it can be used for following up the operator's service to the subscriber.

21.11 Monitoring of incoming line load

Is traffic monitored on the connection to the access point from the operator's network?

Alternatives: YES or NO.

21.12 Monitoring of outgoing line load

Is traffic monitored on the connection to the access point from the operator's network?

Alternatives: YES or NO.

21.13 Monitoring of defective packets received

Is the interface monitored at the connection to the backbone network, connection from the backbone network at connection to the point of access and the point of access against the subscriber's equipment with regard to packets received with checksum errors?

Alternatives: YES or NO.

21.14 Monitoring of number of packets ignored

Is the interface monitored at the connection to the backbone network, connection from the backbone network at connection to the point of access and the point of access against the subscriber's equipment with regard to packets which could not be accommodated in a buffer memory in a queue situation?

Alternatives: YES or NO.

21.15 Monitoring of line status (up/down)

Is the interface monitored at the connection between backbone network and point of access with regard to line status, e.g. carrier wave loss or lost keep-alive packets?

Alternatives: YES or NO.

21.16 Monitoring of reachability by ping

Does the operator supervise from a central position in the network the possibility of reaching access point equipment with a periodically transmitted ICMP echo reply packet?

Alternatives: YES or NO.

21.31 Monitoring of accessibility of support systems

Explanation: The term "support system" refers to the computer resources and suchlike which are needed to support all functions in the Internet architecture which are required for the adequate provision of a service to the subscriber.

In cases where the subscriber operates his own primary DNS and the operator provides a secondary DNS, the monitoring is also included in the operator's secondary servers being able to reach the subscriber's primary server.

Is monitoring undertaken to ensure that support systems, such as computers with DNS, News, SMTP-mail etc., have the requisite accessibility to and from the rest of the Internet to be able to perform their task?

Alternatives: YES or NO.

21.32 Monitoring of support system function

Are support systems monitored to ensure that they function as intended, e.g. that DNS servers give the correct reply and that mail servers receive with SMTP and store messages received?

Alternatives: YES or NO.

21.33 Rectification time when a malfunction is detected during office hours

State rectification time when a malfunction is detected during office hours.

State time in minutes.

21.34 Rectification time when a malfunction is detected outside office hours

State rectification time when a malfunction is detected outside office hours.

State time in minutes.

21.41 Indication of alternative traffic path

If the subscriber’s main connection or a redundant path in the backbone network is for some reason not being used, is this indicated at the operator’s Network Operations Center?

Alternatives: YES or NO.

21.42 Rectification of faults

Are there documented routines concerning what is to be rectified and what reports are to be made for different types of fault to the subscribers concerned?

Alternatives: YES or NO.

21.43 Monitoring and rectification based on network data

Is monitoring conducted and some form of rectification undertaken on the basis of network data collected?

Alternatives: YES or NO.

21.44 Rectification threshold values for data collected

If monitoring is conducted and some form of rectification undertaken on the basis of network data collected, state the threshold values for which rectification measures are taken.

If the answer to 21.43 is YES, give benchmark values as per 21.45, 21.46 and 21.47.

Commentary: If traffic is metered, the reference is to mean values under 5 minutes..

21.45 Line load: % of nominal capacity

21.46 Checksum error: Number of defective packets per 5 min

21.47 Ignored packets: Number of packets ignored per 5 min

21.50 Suspension of scheduled maintenance on reserve connections in the event of a failure of the main connection to a subscriber.

Can the subscriber or the operator's Network Operations Center suspend scheduled maintenance on reserve connections in the event of a failure of the main access connection to a subscriber?

Alternatives: YES or NO.

22 Other services

22.11 Web cache for the operator's subscribers

Can the operator provide a computer system for intermediate storage of commonly used web documents (a web-cache)?

Alternatives: YES or NO.

22.12 Web cache storage capacity

State storage capacity in MB for available disk space.

22.13 Bandwidth from web cache against backbone network

State bandwidth against backbone network in kbit/s.

23 Security

The term "security" here refers to the security of the operator's network and support system.

23.11 Updating of software at point of access and in backbone network

Is software in the equipment forming the software at point of access and in backbone network continuously updated?

Alternatives: YES or NO.

23.12 Information from equipment manufacturers, CERT, CIAC etc.

Does the operator continuously receive information from equipment manufacturers, CERT, CIAC etc?

Alternatives: YES or NO.

If YES: State sources.

23.13 Procedures for dealing with security incidents

Are there documented routines for dealing with security incidents?

Alternatives: YES or NO.

23.14 Procedures for informing the subscribers concerned of any incident

Are there procedures for informing the subscribers concerned in the event of an incident?

Alternatives: YES or NO.

Technical safeguards for the prevention of incidents

23.15 Filters in outgoing routers to prevent spoofing of IP addresses

Are there filters in outgoing routers (or the equivalent) which make spoofing of IP addresses impossible from the operator’s network to another operator?

Alternatives: YES or NO.

23.16 Filters in the access server to prevent spoofing of the subscriber’s addresses for blocking incoming packets

Are there filters in the access server which prevent spoofing of the subscriber’s addresses, i.e. block incoming packets with addresses equal to, less than or greater than the subscriber’s addresses?

Alternatives: YES or NO.

23.17 Filter in access server to prevent spoofing of IP addresses from a subscriber’s network by blocking outgoing packets

Is there a filter in the access server which prevents spoofing of IP addresses from a subscriber's network, i.e. blocks outgoing packets with sender addresses smaller or greater than the subscriber's addresses?

Alternatives: YES or NO.

23.18 Filter in e-mail system so that the operator's e-mail system cannot be used for e-mail relay

Commentary: When a sender wishes to conceal the sender address, other systems can be used for relaying mail. This can be used, for example, when transmitting Unsolicited Commercial Email or Unsolicited Bulk Email, otherwise termed spam. An e-mail system shall only carry e-mail with known sender and receiver addresses.

Are there filters in e-mail systems etc. so that the operator's e-mail system cannot be used for relaying e-mail?

Alternatives: YES or NO.

If YES: State how filters are implemented.

23.19 Filter lists for filtering unsolicited e-mail

Are filter lists used for filtering unsolicited e-mail?

Alternatives: YES or NO.

If YES: Indicate the filter lists used (e.g. RBL, DUL, ORBS).

23.20 The subscriber adds addresses to mail filter lists

Can the subscriber add addresses to mail filter lists?

Alternatives: YES or NO.

23.21 Filter in DNS system to minimize spoofing of DNS information

Are there filters in DNS systems which minimize spoofing of DNS information, i.e. introduction of incorrect DNS items in the operators' DNS?

Alternatives: YES or NO.

23.22 Filter in router (or equivalent) so that incorrect routing information is not spread between the operators' networks

Are there filters in routers (or the equivalent) so that incorrect routing information cannot spread to the operator's network from another operator?

Alternatives: YES or NO.

23.23 Protection of BGP sessions (or the equivalent) at peering points

Is protection of BGP sessions (or the equivalent) used at peering points by methods corresponding to those described in RFC 2385 or suchlike?

Alternatives: YES or NO.

23.24 Filter (physical or logical) between all subscribers

Is there a filter (physical or logical) between all subscribers, so that no two subscribers can interfere with each other, e.g. by replying to DHCP inquiries, ARP/RARP and other “level-2 broadcasts”?

Alternatives: YES or NO.

If YES: Indicate how subscribers are segregated.

23.25 Access control between Network Operations Center and equipment in the network with personal access control

Is access control between Network Operations Center (or the equivalent) and active equipment in the network managed by personal access control (password, certificate or the equivalent)?

Alternatives: YES or NO.

23.26 Routines for adjusting access control when personnel leave

Are there routines for adjusting access control (i.e. as per 23.25) when personnel leave?

Alternatives: YES or NO.

If YES: State the department etc. dealing with personnel who leave and how information is distributed within the enterprise (the operator) to the part dealing with access information.

Other matters

23.30 Security policy for computer systems

A security policy should be defined and documented for the computer systems providing services to the subscriber. Is this security policy communicated to the subscriber?

Alternatives: YES or NO.

If YES. State how the security policy is communicated to the subscriber.

23.91*H Membership of national CERT

24 Scheduled stops and service times

From time to time the operator has to suspend the availability of the service in order to carry out maintenance and upgrading of the network.

To simplify matters for both operator and subscriber, they shall agree in advance on appropriate times for network service and maintenance which are liable to entail stoppages or reduced efficiency.

Stoppages for agreed service periods do not count as breaks in the availability of the service.

24.01 Scheduled service times

State scheduled service times.

Commentary: Most operators have a fixed time for this purpose, e.g. Sundays 18.00 - 21.00 UTC.

24.02 Incident training

Does training in the form of simulated incidents and incident management as described in point 23.14 proceed in collaboration with the subscriber?

Alternatives: YES or NO.

If YES: State how the exercise is conducted.

Development

40 Internet development

“Internet development” IP architecture and membership of joint organizations of Internet operators. All the organizations referred to here are international except for SOF, which is a Swedish joint organization.

40.11 Membership of RIPE

Does the operator participate in RIPE?

Alternatives: YES or NO.

40.12 Membership of EOF

Does the operator participate in EOF?

Alternatives: YES or NO.

40.13 Membership of IETF

Does the operator participate in IETF?

Alternatives: YES or NO.

40.14 Membership of NANOG

Does the operator participate in NANOG?

Alternatives: YES or NO.

40.15 Membership of APRICOT

Does the operator participate in APRICOT?

Alternatives: YES or NO.

40.90* Membership of SOF

Does the operator participate in SOF?

Alternatives: YES or NO.

41 Development of the service

41.11 Fault prevention routines

Do preventive routines exist for spotting faults and bottlenecks before they happen?

Alternatives: YES or NO.

41.12 Test laboratory with dedicated personal

Does the operator have a test laboratory with dedicated personnel ?

Alternatives: YES or NO.

41.13 Pilot activity with new protocols

Does the operator carry out pilot activities with new protocols which are being developed within the IETF?

Alternatives: YES or NO.

41.90* IP version 6 testing

Does the operator have an IP version 6 test scheme in which the subscribers can take part?

Alternatives: YES or NO.

Part 3 List of components

03 Dialup connection

03.01 IPv4 Unicast traffic
03.02 IPv4 Multicast traffic with IGMP
03.03 IPv6 Unicast traffic
03.04 IPv6 Multicast traffic
03.06 Access by analog modem
03.08 Access by digital connection, e g ISDN

03.10 Address allocation and verification methods

03.20 E-mail services
03.21 30-minute uninterruptable power supply
03.22 Internet connection with at least two redundant links
03.23 Support for POP-2 protocol
03.24 Support for POP-3 protocol
03.25 Support for IMAP protocol
03.26 E-mail disk storage space available per receiver
03.27 Customer's domain address indicated for incoming and outgoing e-mail

03.30 News services
03.31 Reading of News with the NNTP protocol
03.32 Transmission of News with the NNTP protocol
03.33 Total newsfeed
03.34 Selected groups from total newsfeed
03.35 Selection of UBE before distribution
03.36 Number of days for which articles in other News groups are saved
03.37 Number of incoming complete newsfeeds etc.
03.38 Number of outgoing newsfeeds locally posted articles etc.

03.40 DNS support
03.41 A caching DNS resolver exists which can be used by the subscriber
03.42 Secondary DNS servers at not less than two different places in the network
03.43 Support for secure DNS

03.50 Throughput and performance
03.51 Measurement of throughput between subscriber systems and the operator's server
03.52 Minimum throughput
03.53 Measurement of throughput between subscriber connection and national main exchange point
03.54 Throughput between a subscriber connection and NY-NAP in Pennsauken, USA
03.55 Roundtrip delay between subscriber connection and national main exchange point
03.56 Roundtrip delay between subscriber connection and NY-NAP in Pennsauken, USA

03.60 Security

03.61 Software updates at access point and in care network

03.62 Information from equipment manufacturers, CERT, CIAC etc.

03.63 Routines for dealing with security incidents

03.64 Routines for informing the subscribers affected of an incident

03.65 Filters in outgoing router to prevent spoofing of IP addresses

03.66 Filters in access server to prevent spoofing of subscriber's addresses, for blocking of incoming packets

03.67 Filters in access server to prevent spoofing of IP addresses from a subscriber's network by blocking outgoing packets

03.68 Filters in e-mail systems etc. so that the operator's e-mail system cannot be used for relaying e-mail

03.69 Filters lists for filtering unsolicited e-mail advertising

03.70 The subscriber can add addresses of his own e-mail filter lists

03.71 Filters in DNS systems which minimize spoofing of DNS information

03.72 Filter in router (or the equivalent) so that incorrect routing information will not bespread between the operators' networks

03.73 Protection of BGP sessions (or the equivalent) at peering points

03.74 Filters between all subscribers

03.75 Access control between Network Operations Center and equipment in the network with personal access control (password, certificate or suchlike)

03.76 Routines for access control adjustment when personnel leave the company

03.77 Security policy for computer systems

03.80 Other additional services

03.81 Shell account for permanently connected Unix computer

03.82 Possibility for a subscriber to create his own web pages

03.83 Disk space available for subscriber´s own web pages, standard

03.90 No. days for which swnet.* and se.* are saved

03.91 Average delay in minutes from posted to readable article

“Always on” connection

04 The access point

04.11	Connection capacity for service access point
04.12	Access point address

05 Level 2 protocol

05.11	10 Mbit/s Ethernet
05.12	100 Mbit/s Ethernet
05.13H	Token-Ring, 4 or 16 Mbit/s
05.16	1 Gbit/s Ethernet
05.21	ATM/AAL5
05.22	Frame Relay
05.23H	X.25
05.24H	SMDS
05.25	ISDN
05.26	GSM
05.27	SNA
05.28	ADSL

06 Level 3-protocol (IPv4, IPv6)

06.11	IPv4 Unicast forwarding
06.12	IPv4 Multicast forwarding
06.13	Multicast addresses
06.14	Multicast addresses between 239.0.0.0 to 239.255.255.255
06.21	IPv6 Unicast forwarding
06.22	IPv6 Multicast forwarding

07 Routing protocol

External routing protocols

07.11	Routing information with BGP4
07.12	Routing information with BGP4 incl. BGP communities
07.13H	Routing information with IDRP
07.14	Manually preconfiguerad routing (static)

Internal routing protocols

07.21	Routing information with RIP 2
07.22	Routing information with OSPF
07.23	Routing information with Integrated IS-IS
07.24	Routing information with EIGRP

07.25 Routing information with OSPF-16
07.26 Routing information with RIP 1
07.27 Static configuration

Routing protocols for Multicast
07.31 IGMP
07.32 MSDP
07.33 PIM-SM
07.34 Use of PIM-SM but not MSDP
07.35 Use of NLRI Multicast when BGP4 not used
07.38 BGMP

Routing information transmitted from operator to subscriber
07.41 Full Internet routing (without default)
07.42 Selected routing information
07.43 Default routing to the subscriber
07.44 BGP4+ as multicast NLRI

Routing information transmitted from subscriber to operator
07.51 Only address block from operator’s address space
07.52 Prefix up to a certain length
07.53 Arbitrary prefix registered in subscriber’s name
07.54 Addresses from another operator’s address block
07.55 Multihoming
07.56 Filtering of routing information from subscriber
07.57 Transmission of information concerning Unicast addresses containing Multicast sources

Descriptive format access lists
07.61 Ripe-81
07.62 Ripe-181
07.63 RPSL
07.64 List with prefix/mask as e-mail
07.65 List with prefix/mask as fax
07.66 Authentication with PGP or S/MIME

07.71 BGP dampening of external routes received
07.72 BGP dampening of subscriber routes received

DHCP server function at access point
07.81 DHCP server at access point
07.82 Address space in static addresses and dynamic address pool
07.83 Log function on DHCP server

08 Performance in operator’s network and access point

08.11 Minimum throughput capacity in access connection (bit/s)
08.12 Maximum throughput capacity in access connection (bit/s)

08.21 Maximum MTU prior to fragmentation of packets

08.30 Method for measuring throughput
08.31 Throughput between two subscriber connections to same operator

08.40 Roundtrip delay measuring method
08.41 Roundtrip delay between two subscribers' connections

08.51 Performance guarantees offered by operator

08.61 One-way performance measurements

08.71 Performance measurements of service with asymmetric performance

08.81 Multicast performance measurements

08.90 Measuring points in North America
08.91 Throughput between a subscriber connection and the national main exchange point in Stockholm
08.92 Throughput between a subscriber connection and measuring points in North America
08.93 Throughput to subscriber connected to another operator within the Swedish IT infrastructure
08.94 Minimum throughput to subscriber outside the Swedish IT infrastructure
08.95 Roundtrip delay between a subscriber connection and the national main exchange point in Stockholm
08.96 Roundtrip delay between a subscriber connection and measuring points in North America

09 Dynamic parameters

Performance
09.30 Method of measurement
09.31 Average distance to root-name servers (ms)
09.32 Average distances to enumerated exchange points
09.33 Max percentage packet loss in own network

09.41 Expansion of the backbone network
09.42 Enlargement of capacity of national exchange points
09.43 Enlargement of capacity to exchange points

09.51 The bandwidth-delay-quota for which the network is designed for
09.52 Queue management strategy in the event of limited resources
09.53 Queue management strategy to subscriber line
09.54 Queue management in the event of traffic from flows with a different traffic volume or other criteria
09.55 Routing statistics
09.56 Routing stability

10 Accessibility/Inaccessibility

10.11 Inaccessibility on access line
10.12 Inaccessibility between two subscribers within the operator’s network
10.13 Inaccessibility of packet forwarding to national main exchange point
10.14 Inaccessibility of packet forwarding to international exchange point

10.21 Accessibility guarantees
10.22 Redundant connections between backbone network exchange points with at least 50 % of normal capacity
10.23 Redundant subscriber connections provided
10.24 Connecting time for transition to reserve path
10.25 Disconnection time for reversion to main path
10.26 Connection of subscriber to more than one operator
10.27 Connecting time for transition to reserve path via other operator
10.28 De-activation time for reversion to main path through another operator

10.90 The operator’s logical support system

11 Traffic filtering

11.31 Packet filtering at the access point
11.32 Filtering at IP addresses
11.33 Filtering based on protocol
11.34 Traffic filtering based on port number
11.35 Traffic filtering based on direction
11.36 Filtering of source routed packets
11.37 Verification of the filter function

11.41 The subscriber can a filter himself
11.42 The operator filters prefixes intended for local use and test use

12 Monitoring functions

12.11 SNMP with read only access to router
12.12 SNMP with write access to router
12.13 Telnet access to access router, read only
12.14 Telnet access to access router write
12.21 SNMP access to backbone network router against access router
12.22 SNMP access to all backbone network routers in the operator’s network

Services

13 Accessibility

13.11 All destinations within the operator’s own network
13.12 All destinations advertised to any of the named exchange points
13.21 Inaccessible destinations
13.22 Multicast forwarding
13.23 Multicast default routing
13.41 Performance guarantees to other operator
13.50 Connected to national exchange points
13.51 Passage of packets to national exchange points

15 Address translation functions (NAT)

15.11 NAT at the access point
15.15 NAT with translation 1-1
15.16 NAT with overload translation
15.17 Protocol for NAT function
15.21 NAT for managing multiple connection to various operators
15.22 The access point and use of globally unique addresses

16 DNS

16.11 Name-to-number for network elements in the operator’s network
16.12 Number-to-name for network elements in the operator’s network
16.13 Support for secure DNS
16.14 Duplicated DNS servers
16.15 Duplicated DNS servers with dual connection
16.16 Duplicated DNS servers in two geographically separate places
16.21 Secondary DNS for the subscriber’s name and number
16.22 Primary DNS server for the subscriber’s name and number
16.23 Number-to-name delegation from the operator’s address block to the subscriber’s primary DNS server
16.24 Functions where the operator runs a secondary DNS
16.25 Functions where the operator runs primary DNS

16.90 DNS server as per technical specifications from ISOC-SE

17 E-mail

17.11 The operator can be reached via e-mail as per Internet standard
17.12 The operator’s MTA uses DNS server is used for address
17.13 The operator provides a secondary mailhost
17.14 Intermediate storage space for at subscriber´s e-mail
17.15 Return of e-mail
17.16 Storage of e-mail

17.17 Operator’s e-mail system configured with “No relay”

Extra e-mail services

17.21H Gateway to UUCP
17.22H Gateway to X.400
17.23H Gateway to X.400 with MIME support for attachments
17.24 The operator provides a complete e-mail function
17.25 The operator provide parts of an e-mail function

18 NTP

18.11 NTP server within the operator’s network
18.12 Duplicated NTP server within the operator’s network
18.13 Cryptosigned time indication

18.21 NTP/SNTP at the access point
18.22 NTP function within the operator’s network with IP multicast

19 News

19.11 Newsfeed to subscriber’s server with NNTP
19.12 Operator´s throughput delay
19.21 Total newsfeed
19.22 Selected groups from total newsfeed
19.23 Pre-distribution spam selection

19.31 NNTP server for news-reading from subscriber’s clients
19.32 How long news groups are saved in the operator’s system

19.41 Number of incoming newsfeeds to the operator’s news server

Operating functions

20 Subscriber support

Subscriber support

20.11 Subscriber support during office hours
20.12 Subscriber support outside office hours
20.13 Qualified technical assistance during office hours
20.14 Qualified technical assistance outside office hours
20.15 Subscriber support via telephone
20.16 Subscriber support via e-mail
20.17 Subscriber support via fax
20.18 Subscriber support via web
20.19 Subscriber support language

20.21 Faults are only handled if occurring within the operator's own networks
20.22 Faults are handled for problems everywhere on the Internet

Trouble management

20.31 Trouble ticket updates are e-mailed
20.32 Trouble ticket status accessible via the web
20.33 The subscriber is contacted when a trouble ticket closed

Traffic statistics accessible on the web

20.41 Traffic statistics at own access point
20.42 Traffic statistics at backbone network connections
20.43 Traffic statistics at connection to other operators
20.44 Traffic statistics at connection to exchange points

Accessibility statistics

20.51 Availibility on own line
20.52 Access to exchange points

Routing stability

20.61 Statistics of routing stability

Domain registrations

20.71H Registration of domain names
20.74 Verification of information in the subscriber's DNS server, together with forward and backward lookup and use of permitted characters only

20.90 Subscriber support in Swedish
20.91 Operator agent for registration of domain names under .SE
20.92 Support system to guarantee subscriber function for traffic within Sweden when registered under a top-level domain other than .SE.

21 Operational monitoring

21.11 Monitoring of incoming line load
21.12 Monitoring of outgoing line load
21.13 Monitoring of defective packets received
21.14 Monitoring of number of packets ignored
21.15 Monitoring of line status (up/down)
21.16 Monitoring of accessibility by Ping

21.31 Monitoring of support system function
21.32 Monitoring of functioning of support systems
21.33 Rectification time when a malfunction is detected during office hours
21.34 Rectification time when a malfunction is detected outside office hours

21.41 Indication of alternative traffic path
21.42 Response of faults
21.43 Monitoring and rectification based on network data
21.44 Rectification threshold values of data collected
21.45 Line load: % of nominal capacity
21.46 Checksum error: Number of incorrect packets per 5 min
21.47 Packets ignored: Number of packets ignored per 5 min

21.50 Suspension of scheduled maintenance on reserve connections in the event of a failure of the main connection to a subscriber

22 Other services

22.11 Web cache for the operator's subscribers
22.12 Web cache storage capacity
22.13 Bandwidth from web cache against backbone network

23 Security

23.11 Updating of software at point of access and in backbone network
23.12 Information from equipment manufacturers, CERT, CIAC etc.
23.13 Procedures for dealing with security incidents
23.14 Procedures for informing the subscribers concerned of the event of an incident

Technical protection for prevention of incidents

23.15 Filters in outgoing routers to prevent spoofing of IP addresses
23.16 Filters in the access server to prevent spoofing of the subscriber's addresses for blocking incoming packets
23.17 Filter in access server to prevent spoofing of IP addresses from a subscriber´s network by blocking outgoing packets
23.18 Filter in e-mail system so that the operator's e-mail system cannot be used for e-mail relay
23.19 Filter lists for filtering unsolicited e-mail

23.20 The subscriber adds addresses to mail filter lists
23.21 Filter in DNS system to minimize spoofing of DNS information
23.22 Filter in router (or equivalent) so that incorrect routing information is not spread between the operators' networks
23.23 Protection of BGP sessions (or the equivalent) at peering points
23.24 Filter (physical or logical) between all subscribers
23.25 Access control between Network Operations Center and equipment in the network with personal access control
23.26 Routines for adjusting access control when personnel leave

Other matters
23.30 Security policy for computer systems
23.91H Membership of national CERT

24 Scheduled stops and service times

24.01 Scheduled service times
24.02 Incident training

Development

40 Internet development

40.11	Membership of RIPE
40.12	Membership of EOF
40.13	Membership of IETF
40.14	Membership of NANOG
40.15	Membership of APRICOT
40.90	Membership of SOF

41 Development of the service

41.11	Fault prevention routines
41.12	Test laboratory with dedicated personal
41.13	Pilot activity with new protocols
41.90*	IP version 6 testing

Glossary of terms

ADSL	Asymmetric Digital Subscriber Line
ARP	Address Resolution Protocol
APRICOT	Asia Pacific Regional Internet Conference on Operational Technology
AS	Autonomous System
Asymmetric	Asymmetric communication means that transfer capacity is greater in the direction communication *towards* the user than *away from* the user
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
BGP	Border Gateway Protocol
BGMP	Border Gateway Multicast Protocol
BNC	Type of connector for Ethernet
BOK	A Swedish request of documents, published by ISOC-SE
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Protocol
CIAC	Computer Incident Advisory Committee
D-GIX	Distributed Global Internet Exchange, exchange point for traffic between operators
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DNSSEC	Secure DNS
DVMRP	Distance Vector Multicast Routing Protocol
DUL	Dial-up User List (Mail Abuse Prevention System's Dial-up User List, MAPS DUL)
EIGRP	Enhanced IGRP
EOF	European Operators Forum
ESMTP	Extended Simple Mail Transfer Protocol
Ethernet	Standard for local networks
FDDI	Fiber Distributed Data Interface
FIFO	First In First Out
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
IAB	Internet Architecture Board, appointed by the ISOC for architectural oversight of Internet architecture and protocols. Acts as adviser to the IETF and ISOC in matters of technology, architecture, procedures and policy for the Internet
ICMP	Internet Control Message Protocol
ISOC-SE	The Swedish branch of the ISOC
IDRP	Inter-Domain Routing Protocol
IEPG	Internet Engineering and Planning Group
IESG	Internet Engineering Steering Group, part of the IETF responsible for directing the IETF's technical activities. Leads the Internet standardization process and approves specifications as Internet standards
IETF	Internet Engineering Task Force, consisting of network builders, operators, suppliers and researchers engaged in developing Internet operations and architecture. It is primarily this task force which specifies new Internet standards.
IGMP	Internet Group Management Protocol
IGRP	Interior Gateway Routing Protocol
IMAP	Internet Message Access Protocol
INET	Internet Society Networking Conference
IPv4	Internet Protocol, version 4
IPv6	Internet Protocol, version 6
IS-IS	Intermediate System to Intermediate System
ISO	International Organization for Standardization
ISOC	Internet Society
LAN	Local Area Network

Linx	London Internet Exchange
LLC	Logical Link Control
MAU	Media Attachment Unit
MIME	Multipurpose Internet Mail Extensions
MRM	Multicast Routing Monitor Protocol
Mrouted	Multicast routing daemon
MSDP	Multicast Source Discovery Protocol. Protocol linking together PIM-SM
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit
Multihoming	Means that a subscriber is connected to more than one operator
MX	DNS records
NANOG	North American Network Operators' Group
NAT	Network Address Translator
Netnod	Netnod Internet Exchange i Sverige AB
NIC-SE	Network Information Centre Sweden AB, provides, co-ordinates and operates the national register for domain names under .SE on the Internet
NLRI	Network Layer Reachability Information
NNTP	Network News Transfer Protocol
NOC	Network Operation Center
NTP	Network Time Protocol
Optic foil	Ethernet via fibre
ORBS	Open Relay Behaviour-modification System
OSPF	Open Shortest Path First
PAP	Password Authentification Protocol
PGP	Pretty Good Privacy
PIM	Protocol Independent Multicast
PIM-SM	PIM Sparse Mode, Multicast where traffic has to be requested for a particular group
PING	Packet Internet Groper, popular expression for sending data to the ICMP echo-port of a computer system and timing the operation
POP	Post Office Protocol
PPP	Point-to-Point Protocol
PTR	DNS-records
RBL	Realtime Blackhole List (Mail Abuse Prevention System's Realtime Blackhole List, MAPS RBL)
RARP	Reverse Address Resolution Protocol
RED	Random Early Drop
RFC	Request For Comments, a series of documents containing Internet standards and other documents relating to the Internet
RIP	Routing Information Protocol
RIPE	Resaux IP Européens
RPSL	Routing Policy Specification Language
RJ45	Registered Jack, modular contact
RP	Rendezvous Point for senders and receivers in Multicasting
RTT	Round Trip Time, the time it takes a packet to get from A to B and back again from B to A
S/MIME	Secure/Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SNAP	Sub-Network Access Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SOF	Swedish Operators Forum
Spam	Otherwise known as UCE (Unsolicited Commercial E-mail) or UBE (Unsolicited Bulk E-mail), alias junk mail
Spoofing	When someone generates and sends data packets with bogus sender addresses in order to conceal their identity and in these way impede traceability

SSL	Secure Socket Layer
STD	Standard documents, subserie of RFC:s
STUPI	Svensk Teleutveckling & Produktinnovation AB
	Symmetrical communication means that transmission capacity is the same in both directions, i.e. both *to* and *from* the user
SUNET	Swedish University Computer Network
TCP	Transmission Control Protocol
TLS	Transport Layer Secure
UDP	User Datagram Protocol
UTC	Universal Time Coordinated
UUCP	Unix to Unix Copy
VPN	Virtual private network
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection, a more advanced version of Random Early Detection
xDSL	x Digital Subscriber Line, where x is interchangeable with A (Asymmetric), H (High data rate), S (Single line) or V (Very high data rate)
10Base2	Ethernet standard, 10 Mbit/s, thin wire
10BaseT	Ethernet standard, 10 Mbit/s, twisted pair
100BaseFX	Ethernet standard, 100 Mbit/s, fast fiber link
100BaseTX	Ethernet standard, 100 Mbit/s, fast twisted pair