OBSERVATORIET FÖR
IT-INFRASTRUKTUR

Generell specifikation av Internettjänst

version 1.0

Observatorierapport 2/2000

KOMMISSIONEN

Generell specifikation av Internettjänst

version 1.0

Observatorierapport 2/2000

IT-kommissionen – Statskontoret

***Adress**:* Observatoriet för IT-infrastruktur, IT-kommissionen, 103 33 Stockholm
Besöksadress: Hantverkargatan 25, uppgång B, plan 4
Telefon: 08-405 47 01 ***Fax:*** 08-650 65 16
E-post: jan.berner @itkommissionen.se
***Webbplats*:** http://www.itkommissionen.se

ISSN: 1404-8744

Innehållsförteckning

Förord

En väl fungerande kommunikation via Internet är viktig för många organisationer och privatpersoner. Ett stort antal operatörer i Sverige erbjuder Internettjänster. I många fall är det dock inte specificerat vad Internettjänsten omfattar vad avser exempelvis prestanda, tillgänglighet, driftsfunktioner, användarstöd.

År 1997 publicerades en första version av *Generell specifikation av Internettjänst (version 0.93)* som en del av Statskontorets *Kravspecifikation - Internettjänster för statliga myndigheter, kommuner och landsting* (K:142).

Under 1999 påbörjades arbetet för att ta fram en version 1.0 av specifikationen. Arbetet har utförts av en arbetsgrupp bestående av Jan Berner, IT-kommissionen (fram till den 1 oktober 1999 anställd vid Statskontoret), Anne-Marie Eklund Löwinder, IT-kommissionen, Peter Löthberg, STUPI, Börje Josefsson, Luleå tekniska universitet och ett 10-tal personer från SOF (Swedish Operators Forum). IT-kommissionens Observatorium för informationssäkerhet har bidragit med synpunkter på säkerhetsfunktioner. SOF har löpande haft möjlighet att lämna synpunkter på utkast till specifikationen. Specifikationen kan därför anses vara väl förankrad hos de flesta leverantörer av Internettjänster. Version 1.0 ersätter version 0.93.

Syftet med *Generell specifikation av Internettjänst* är att ge de organisationer och motsvarande som skall upphandla Internettjänster från operatörer en översikt över de krav som kan ställas vid formuleringen av kravspecifikation för att erhålla en Internettjänst av hög kvalitet. Specifikationen skall därför ses som en vägledning i detta arbete och är inte i sig en kravspecifikation. Specifikationen kan också användas av operatörer som vill mäta kvaliteten på den egna tjänsten.

Avsikten är att denna specifikation fortlöpande skall uppdateras av en därtill lämplig organisation med hänsyn till den tekniska utvecklingen och erhållna erfarenheter från specifikationens användning. Arbetet med att finna en sådan organisation pågår och fram till dess kommer IT-kommissionen att handha specifikationen.

Frågor gällande specifikationen kommer därför att tills vidare publiceras på http://www.itkommissionen.se/obs/obs_infra.html.

Kontaktperson för specifikationen är Jan Berner, IT-kommissionen. E-post: jan.berner@itkommissionen.se.

Stockholm maj 2000

Christer Marking
Kanslichef för IT-kommissionen

Connie van der Capellen
Chef för Statskontorets IT-enhet

Inledning

Syftet med specifikationen

Utgående från denna specifikation kan en kravställare utforma en egen kravspecifikation och ange vilka krav som skall ställas på en Internettjänst. I denna specifikation beskrivs de olika komponenter som bör ingå i en uppringd respektive fast anslutning till en Internetoperatörs tjänst. Specifikationen beskriver tjänst levererad från operatör (leverantör) till abonnent (kund) på en mycket detaljerad nivå. Med tjänst avses i specifikationen sändning och mottagning av IP-paket i abonnentens accesspunkt för tjänsten. I tjänsten ingår också tekniska och administrativa rutiner.

Många av de komponenter som ingår i en Internettjänst är mer eller mindre underförstådda. Denna specifikation dokumenterar dessa komponenter på ett sådant sätt att parterna i ett abonnent-/operatörsförhållande har en gemensam grund att utgå från vid en upphandling eller för vid en jämförelse mellan olika operatörers tjänsteutbud.

För att erhålla en kravspecifikation för ett önskat fall väljer kravställaren ut de komponenter som är viktiga att parametersätta. Exempel på hur en kravspecifikation kan utformas framgår av bilagan.

Specifikationen förutsätter att abonnenten har tillgång till en tillräcklig kompetens inom sin organisation eller motsvarande för att ställa relevanta krav och utvärdera svaren från operatören liksom för att i förekommande fall utföra nödvändiga mätningar.

Vid användning av Internettjänsten förutsätts att abonnentens egen utrustning uppfyller gällande standarder för kommunikation enligt IP-arkitekturen. Abonnenten förutsätts även ha personal som är kompetent nog att både driva nätet och att följa utvecklingen när det gäller standarder inom IP-området.

Olika former av tillämpningar och tjänster som inte ingår i Internets grundfunktion behandlas i huvudsak inte i detta dokument.

Användningen av denna specifikation beslutas av varje enskild organisation eller motsvarande och under dennes eget ansvar. IT-kommissionen och Statskontoret vill peka på att den som avser att nyttja specifikationen dessförinnan det görs, klargör de eventuella juridiska frågeställningar som en användning medför.

Specifikationens struktur

Dokumentet är uppdelat i följande delar:

Del 1 Anslutningsformer.
Beskriver vad som avses med uppringd anslutning och fast anslutning till en Internettjänst.

Del 2	Komponenter för Internettjänst. Beskrivning av de ingående komponenterna för respektive tjänst.
Del 3	Förteckning över ingående komponenter för respektive tjänst.
Ordlista	Förteckning över förekommande förkortningar.

Med hjälp av de beteckningar som är beskrivna i specifikationens del 2 skall den tjänst som levereras från operatör till abonnent kunna beskrivas genom att referera till beteckningar i del 3.

Observera att i denna version, version 1.0, har vissa delar omnumrerats i förhållande till version 0.93 som tidigare har publicerats. Detta har gjorts med hänsyn till att nya protokoll och krav har tillkommit, respektive att vissa äldre protokoll och krav inte längre är relevanta.

Del 1 Anslutningsformer

Den kommunikationsarkitektur som används för Internet kallas vanligen för TCP/IP eller bara IP och omfattar den samling av protokoll som är beskrivna i de RFC:er som av IAB/IESG utpekas såsom beskrivning av en protokollstandard. (Det finns även RFC:er som inte har status av en standard utan är förslag, rapporter eller annat av intresse för IETF.)

Nu förekommer två olika huvudmodeller för åtkomst till Internet. Dessa är uppringd anslutning och fast anslutning.

Uppringd anslutning

En uppringd anslutning innebär att abonnenten upprättar en förbindelse innan trafik kan utväxlas till operatörens Internettjänst, t.ex. genom att via telefonnätet ringa upp förmedlingsutrustningen hos operatör.

Denna typ av tjänst används nästan alltid för att ordna åtkomst (access) till Internet för en enstaka privatperson.

Denna typ av tjänst lämpar sig således inte för tillämpningar där man har mer än en enstaka användare. Den förutsätter också att det inte finns någon trafik som initieras i riktning *till* abonnenten från övriga Internet.

En organisation kan exempelvis använda en uppringd anslutning för medarbetare på resa eller för medarbetare som distansarbetar så att dessa kan fjärranslutas till datorresurser inom den egna organisationen. Anslutningen anordnas då med hjälp av något av de säkerhetsprotokoll som finns i IP-arkitekturen, vilka medger s.k. säker identifiering och kryptering av informationen under dess transport mellan den fjärranslutna medarbetaren och organisationens datorsystem.

Anslutningsformen **uppringd anslutning** till en operatörs Internettjänst behandlas under **punkt 03** i del 2 och 3 av denna specifikation.

Fast anslutning

En fast anslutning innebär att abonnenten (abonnentens utrustning) kan överlämna IP-paket till ett förmedlande element (i accesspunkten), utan att vid varje tillfälle på förhand koppla upp sig till operatörens Internettjänst. Likaså kan IP-paket som avsänts från annan plats inom Internet utan särskilda åtgärder levereras från ett förmedlande element till abonnenten via accesspunkten.

En operatör kan använda valfri utrustning för tjänstens accesspunkt och valfritt transmissionssätt mot operatörens nät, förutsatt att de prestanda som avtalats uppfylls och att arkitekturen för Internet följs. Den teknik som används är operatörens ansvar och skall vara transparent för användaren.

Följande delar ingår i en **fast anslutning** till en operatörs Internettjänst:

04	Accesspunkten
05	Nivå 2-protokoll
06	Nivå 3-protokoll
07	Routingprotokoll
08	Prestanda i operatörens nät och accesspunkt
09	Dynamiska parametrar
10	Tillgänglighet/otillgänglighet
11	Trafikfiltrering
12	Övervakningsfunktioner
13	Nåbarhet
15	Adressöversättningsfunktioner (NAT)
16	DNS
17	E-post
18	NTP
19	News
20	Abonnentstöd
21	Driftövervakning
22	Övriga tjänster
23	Säkerhet
24	Planerade avbrott och servicetider
40	Utveckling av Internet
41	Utveckling av tjänsten

Del 2 Komponenter för Internettjänst

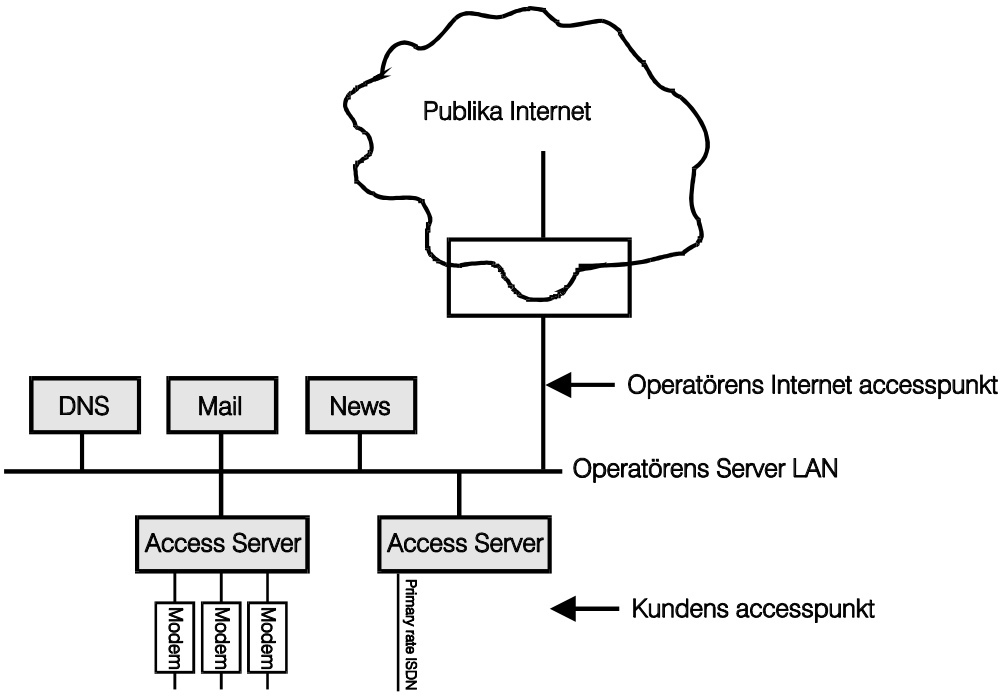
I denna del beskrivs de komponenter som ingår i en Internettjänst. Vissa komponenter är av *nationell* karaktär. Dessa har numrerats med xx.9x för att markera att de är lokala och gäller enbart för Sverige. För att inte dessa skall ryckas ur sitt sammanhang i beskrivningarna har de i vissa fall placerats på sin logiska plats i beskrivningen. I de fallen följs sekvensnumret av en asterisk, t.ex. 08.91*. I del 3 däremot är ordningen strikt numerisk för att möjliggöra anpassning av specifikationen till andra länder.

H i dokumentet anger en *historisk* funktion, t.ex. 05.13H.

Uppringd anslutning

03 Uppringd anslutning

Internettjänsten levereras till abonnenten (kunden) via någon form av kopplat nät vilket huvudsakligen är avsett för andra trafiktyper än Internet, t.ex. telefoni.



03.01 IPv4 Unicast trafik

Erbjuder operatören en tjänst baserad på IPv4 Unicast?

Alternativ är JA eller NEJ.

03.02 IPv4 Multicast trafik med IGMP

Erbjuder operatören en tjänst baserad på IPv4 Multicast trafik med IGMPv2 alternativt IGMPv3 som ”gruppmedlemsprotokoll”?

Alternativ är JA eller NEJ.

03.03 IPv6 Unicasttrafik

Erbjuder operatören en tjänst baserad på IPv6 Unicast?

Alternativ är JA eller NEJ.

03.04 IPv6 Multicasttrafik

Erbjuder operatören en tjänst baserad på IPv6 Multicast?

Alternativ är JA eller NEJ.

03.06 Access med analogt modem

Operatören skall ange:
a) Vilka modemgränssnitt (V.34 osv) som respektive modempool stöder.

b) Om datalänkprotokollet PPP stöds.

c) Om gruppnummer kan användas för att nå modempoolerna.

d) Vilken operatör (dvs. operatör med eget stamnät) som utnyttjas för anslutning till Internet.

03.08 Access med digital förbindelse typ ISDN

Operatören skall ange:
a) Om en eller två B-kanaler stöds.

b) Om datalänkprotokollet PPP stöds.

c) Om gruppnummer kan användas för att nå ISDN-poolerna.

d) Vilken operatör (dvs. operatör med eget stamnät) som utnyttjas för anslutning till Internet.

03.10 Adresstilldelning och verifieringsmetoder

Operatören skall ange:
a) Hur IP-adressen tilldelas (dynamiskt eller fast utgående från användaridentitet).

b) Om respektive modempool stöder PAP eller CHAP för verifiering av användaren.

03.20 E-posttjänster

Förklaring: Datorsystem som används för hantering av e-postlådor bör ha en anslutning till Internet med goda prestanda. I de fall systemet drabbas av avbrott skall e-post kunna mellanlagras på annan plats (secondary mailhost). Här förutsätts att ingående systemkomponenter följer aktuella Internetstandarder (RFC) samt att man för kommunikation till och från Internet använder uppdaterade och aktuella versioner av SMTP programvara.

03.21 Kraftförsörjning med avbrottsfri kraft i 30 minuter

Är datorsystem och kommunikationsutrustning för e-posthantering och uppringd anslutning kraftförsörjd via avbrottsfri kraft med minst 30 minuters reservgång?

Alternativ är JA eller NEJ.

03.22 Internetanslutning med minst två redundanta förbindelser

Är datorsystem som används för e-posthantering anslutet via minst två redundanta förbindelser till Internet?

Alternativ är JA eller NEJ.

03.23 Stöd för protokollet POP-2

Stöds abonnentaccess med protokollet POP-2?

Alternativ är JA eller NEJ.

03.24 Stöd för protokollet POP-3

Stöds abonnentaccess med protokollet POP-3?

Alternativ är JA eller NEJ.

03.25 Stöd för protokollet IMAP

Stöds abonnentaccess med protokollet IMAP?

Alternativ är JA eller NEJ.

03.26 Tillgängligt diskutrymme för lagring av e-post/mottagare

Finns diskutrymme tillgängligt för lagring av mottagen e-post per användaridentitet?

Alternativ är JA eller NEJ.

Om JA: Ange antal megabyte tillgängligt per användaridentitet.

03.27 Kundens domänadress anges för in- och utgående post

Kan e-postlåda förses med kundens domänadress, t.ex. nisse.nilsson@myndighet.se för såväl ingående som utgående e-post?

Alternativ är JA eller NEJ.

03.30 Newstjänster

Förklaring: News är en struktur av diskussionsgrupper vilka innehåller artiklar inom olika ämnesområden. Man skall kunna läsa artiklar skrivna av andra på andra system och artiklar som skapas skall distribueras till andra News-system.

03.31 Läsning av News med protokollet NNTP

Stöds läsning av News från abonnent med protokollet NNTP?

Alternativ är JA eller NEJ.

03.32 Sändning av News med protokollet NNTP

Stöds sändning av News-artikel med protokollet NNTP?

Alternativ är JA eller NEJ.

03.33 Total news-feed

Finns möjlighet för operatören att distribuera alla förekommande publika news-grupper?

Alternativ är JA eller NEJ.

03.34 Selekterade grupper ur total news-feed

a) Har operatören en policy som gör att abonnenten inte kan få access till några kända grupper/typer av grupper?

Alternativ är JA eller NEJ
Om svaret är JA, ange den policy som gäller.

b) Kan abonnenten specificera vilka grupper man önskar ta emot?
Alternativ är JA eller NEJ.

c) Kan abonnenten specificera de grupper man inte vill ta emot?
Alternativ är JA eller NEJ.

03.35 Selektering vid massutskick före distribution

Utför operatören filtrering mot massutskick (spam) innan news-artiklar distribueras till abonnent?

Alternativ är JA eller NEJ.

03.90* Antal dagar som swnet.* och se.* sparas

Hur många dagar sparas artiklar för de svenska News-strukturerna (swnet.* och se.*)?

03.36 Antal dagar som artiklar i andra News-grupper sparas

Hur många dagar sparas News i alla andra grupper?

03.37 Antal inkommande kompletta newsfeeds m.m.

Operatören skall:
a) Ange antal inkommande kompletta newsfeeds (matningar).
b) Namnge domänadress för sändande system.

03.38 Antal utgående newsfeeds för lokalt postade artiklar m.m.

Operatören skall:
a) Ange antalet utgående feeds (matningar) för lokalt postade artiklar
b) Namnge domänadress för mottagande system.

03.91* Medelfördröjningen i minuter från postad till läsbar artikel

Operatören skall ange medelfördröjning i minuter från det att en artikel postats till Sunets centrala newsserver i gruppen swnet.test till dess att den kan läsas av abonnent mot operatörens tjänst.

Anges i minuter.

03.40 DNS-stöd

03.41 Cachande DNS-resolver finns som kan användas av abonnent

Finns cachande DNS-resolver som kan användas av abonnent?

Alternativ är JA eller NEJ.

03.42 Sekundära DNS-servrar finns på minst två olika platser i nätet

Finns sekundära DNS-servrar för de domäner som hanteras av postsystemet på minst två olika platser i nätet?

Alternativ är JA eller NEJ.

03.43 Stöd för Secure-DNS

Förklaring: I de fall användarens klient använder operatörens DNS-resolver för rekursiv uppslagning och samtidigt använder secure-DNS krävs att operatörens DNS stödjer secure-DNS och att lämpliga säkerhetsrutiner finns för att verifiera att operatörens datorsystem korrekt hanterar secure-DNS, har aktuella nycklar uppdaterade samt att dessa inte blivit obehörigt manipulerade. Motivet till detta är att abonnentens klient-applikation tvingas att lita på den information som operatörens system levererar som svar på en rekursiv DNS fråga.

Har operatören stöd för secure-DNS, med lämpliga säkerhetsrutiner?

Alternativ är JA eller NEJ.

03.50 Genomströmning och prestanda

03.51 Mätning av genomströmning mellan abonnentsystem och operatörens server

Mätmetod: Mätning utförs genom att abonnenten har ett V.34-modem med kompression anslutet till sitt datorsystem med 115,2 kbit/s.

Från abonnentsystemet överförs med FTP en specifik testfil om 800 kbyte till operatörens server varefter man överför filen med FTP från operatörens server tillbaka till abonnentsystemet. En binär testfil för ändamålet tillhandahålles av IT-kommissionen.

Effektiv överföringskapacitet (överföringshastighet) beräknas utifrån överföringstiden.

Operatören skall ange effektiv överföringskapacitet i båda riktningarna, i kbit/s.

03.52 Minsta genomströmning

Mätmetod: Trafik skickas som TCP-strömmar i båda riktningarna, t.ex. genom att man från uppringd klient kör TCP-spray mot TCP loopbackporten på ett datorsystem operatören tillhandahåller i anslutning till nationell knutpunkt (se bild i an-

slutning till 08.30). Provet skall innefatta en datamängd av minst 1 Mbyte.

Provet utförs vid tre tillfällen under vardera en timme, kl 09.00-10.00, kl 14.00-15.00 samt kl 21.00-22.00, vardagar.

Operatören skall ange lägsta värdet för överföringstid i sekunder för genomströmning i respektive riktning som aldrig underskrids vid något av proven.

03.53 Mätning av genomströmning mellan abonnentanslutning och nationell huvudknutpunkt

Mätmetod*:* Trafik skickas som TCP-strömmar i båda riktningarna, t.ex. genom att man utnyttjar TCP loopbackporten på ett datorsystem i den ena anslutningen och TCP-spray från den andra anslutningen. Vid mätning mot knutpunkter skall operatören anvisa relevant datorsystem/IP-adress att utföra mätningen mot.

Provet utförs vid tre tillfällen under vardera en timme, kl 09.00-10.00, kl 14.00-15.00 samt kl 21.00-22.00, vardagar.

Operatören skall ange det lägsta värdet (kbit/s) för genomströmning som aldrig underskrids vid något av proven.

03.54 Genomströmning mellan en abonnentanslutning och NY-NAP i Pennsauken USA

Mätmetod enligt 03.53.

Operatören skall ange det lägsta värdet (kbit/s) för genomströmning som aldrig underskrids vid något av proven.

03.55 Roundtrip delay mellan abonnentanslutning och nationell huvudknutpunkt

Mätmetod*:* ICMP Echo Reply-meddelanden (ping) med 64 bytes datainnehåll skickas till ett datorsystem anslutet hos motstående abonnentanslutning. Tiden anges från det att hela paketet avsänts till dess att hela paketet har mottagits i retur.

Från av datorsystemet uppmätt värde avgår 5 ms som kompensation för eventuella systemfördröjningar i mätutrustningen.

Provet utförs vid tre tillfällen under vardera en timme, kl 09.00-10.00, kl 14.00-15.00, samt kl 21.00-22.00, vardagar. Mätningen genomförs genom att man skickar ett ICMP echopaket (ping) varannan sekund under provperioden om 60 minuter, dvs. totalt 1800 paket om vardera 64 bytes.

Som mätvärde används medelvärdet av fördröjningstiden på paket som mottagits inom 2 sekunder efter det att paketet har avsänts.

Operatören skall ange roundtrip delay mellan en abonnentanslutning och nationell huvudknutpunkt mätt enligt ovan. Tiden anges i millisekunder.

03.56 Roundtrip delay mellan abonnentanslutning och NY-NAP i Pennsauken, USA

Ange roundtrip delay mellan en abonnentanslutning och NY-NAP i Pennsauken, USA, mätt enligt 03.55.

Ange tiden i millisekunder.

03.60 Säkerhet

Kommentar: Med säkerhet avses här säkerhet i operatörens nät och stödsystem.

03.61 Uppdatering av programvara i accesspunkt och stamnät

Sker kontinuerlig uppdatering av programvara i den utrustning som bildar stamnätet och som finns i accesspunkten?

Alternativ är JA eller NEJ.

03.62 Information från utrustningstillverkare, CERT, CIAC etc.

Erhåller operatören kontinuerligt information från utrustningstillverkare, CERT, CIAC etc?

Alternativ är JA eller NEJ.

Om JA, ange från vilka källor.

03.63 Rutiner för att hantera säkerhetsincidenter

Finns dokumenterade rutiner för att hantera säkerhetsincidenter?

Alternativ är JA eller NEJ.

03.64 Rutiner för att informera berörda abonnenter vid en incident

Finns rutiner för att informera berörda abonnenter vid en eventuell incident?

Alternativ är JA eller NEJ.

03.65 Filter i utgående router för att förhindra s.k. spoofing av IP-adresser

Finns det filter i utgående routrar (eller motsvarande) så att s.k. spoofing av IP-adresser inte är möjlig från operatörens nät mot annan operatör?

Alternativ är JA eller NEJ.

03.66 Filter i accesserver för att förhindra s.k. spoofing av abonnentens adresser för blockering av inkommande paket

Finns det filter i accesserver eller motsvarande som förhindrar s.k. spoofing av abonnentens adresser, dvs. blockerar inkommande paket med avsändaradresser lika med, mindre än eller större än abonnentens adresser?

Alternativ är JA eller NEJ.

03.67 Filter i accesserver för att förhindra s.k. spoofing av IP-adresser från en abonnents nät genom blockering av utgående paket

Finns det filter i accesserver eller motsvarande som förhindrar s.k. spoofing av IP-adresser från en abonnents nät, dvs. blockerar utgående paket med avsändaradresser mindre än eller större än abonnentens adresser?

Alternativ är JA eller NEJ.

03.68 Filter i e-postsystem etc. så att operatörens e-postsystem inte kan användas för s.k. relay av e-post

Kommentar: När en avsändare vill dölja avsändaradressen kan andra system användas för att ”reläa” utskick. Detta kan exempelvis utnyttjas vid utskick av stora mängder e-post (s.k. Unsolicited Commercial Email eller Unsolicited Bulk Email), även kallat spam. Ett e-postsystem skall bara vidarebefordra e-post med kända avsändar- och mottagaradresser.

Finns det filter i e-postsystem etc. så att operatörens e-postsystem inte kan användas för s.k. relay av e-post?

Alternativ är JA eller NEJ.

Vid JA: Ange hur filter implementeras.

03.69 Filterlistor för filtrering av oönskad e-postreklam

Används filterlistor för filtrering av oönskad e-postreklam?

Alternativ är JA eller NEJ.

Vid JA: Ange vilka filterlistor som används (exempel: RBL, DUL, ORBS).

03.70 Abonnenten lägger till egna adresser till mailfilterlistor

Kan abonnenten lägga till egna adresser till mailfilterlistor?

Alternativ är JA eller NEJ.

03.71 Filter i DNS-system som minimerar s.k. spoofing av DNS-information

Finns det filter i DNS-system som minimerar s.k. spoofing av DNS-information, dvs. att felaktiga DNS-poster införs i operatörernas DNS?

Alternativ är JA eller NEJ.

03.72 Filter i router (eller motsvarande) så att felaktig routinginformation inte sprids mellan operatörernas nät

Finns det filter i routrar (eller motsvarande) så att felaktig routinginformation hos annan operatör inte sprids in i operatörens nät?

Alternativ är JA eller NEJ.

03.73 Skydd av BGP-sessioner (eller motsvarande) vid peeringpunkter

Används skydd av BGP-sessioner (eller motsvarande) vid peeringpunkter med metoder motsvarande den som beskrivs i RFC 2385?

Alternativ är JA eller NEJ.

03.74 Filter mellan samtliga abonnenter

Finns det filter (logiskt) mellan samtliga abonnenter, så att två abonnenter inte kan störa varandra genom t.ex. att svara på DHCP-förfrågningar, ARP/RARP och annan ”nivå-2 broadcast”?

Alternativ är JA eller NEJ.

Vid JA: Ange hur abonnenter är skilda åt.

03.75 Accesskontrollen mellan Network Operations Center och utrustning i nätet med personlig accesskontroll

Sköts accesskontrollen mellan Network Operations Center (eller motsvarande) och aktiv utrustning i nätet med personlig accesskontroll (lösenord, certifikat eller dyl.)?

Alternativ är JA eller NEJ.

03.76 Rutiner för justering av accesskontroll när personal slutar

Finns det rutiner för justering av accesskontrollen (dvs. enligt 03.75) i samband med att personal slutar?

Alternativ är JA eller NEJ.

Vid JA: Ange vilken avdelning eller motsvarande som hanterar personal som slutar och hur informationen sprids inom företaget (operatören) till den del som handhar accessinformationen.

03.77 Säkerhetspolicy för datorsystem

För de datorsystem som tillhandahåller tjänster till abonnent bör det finnas definierad säkerhetspolicy. Delges abonnenten denna säkerhetspolicy?

Alternativ är JA eller NEJ.

Vid JA. Ange hur säkerhetspolicyn delges abonnenten.

03.80 Övriga tilläggstjänster

03.81 ”Shell account” på permanent uppkopplad Unix-dator

Tillhandahålls "Shell account" på permanent uppkopplad Unix-dator?

Alternativ är JA eller NEJ.

03.82 Möjlighet för abonnent att lägga upp egna webbsidor

Finns möjlighet för abonnenten att lägga upp egna webbsidor?

Alternativ är JA eller NEJ.

03.83 Tillgängligt diskutrymme för egna webbsidor, standard

I det fall abonnenten kan lägga upp egna webbsidor, ange för abonnenten tillgängligt diskutrymme ingående i standardtjänsten.

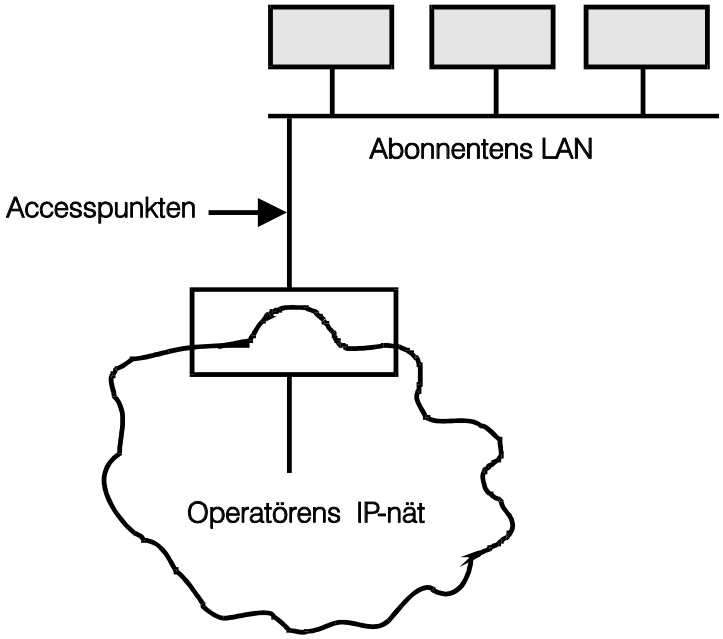
Anges i Mbytes.

Fast anslutning

04 Accesspunkten

Tjänsten levereras till abonnenten i accesspunkten. Accesspunkten består av flera olika nivåer såsom den elektriska/optiska förbindelsen, IP-paketens inkapsling, routing och övervakning. I tjänsten ingår också tekniska och administrativa rutiner.

Accesspunkten kan exempelvis utgöras av en router eller av ett modem. Utrustningen som utgör accesspunkten har en anslutning enligt avsnitt 05, nivå 2-protokoll, exempelvis ett Ethernetgränssnitt. Där inget annat anges förutsätts här symmetrisk kommunikation, dvs. samma kapacitet (hastighet) i båda riktningarna.



04.11 Anslutningskapacitet för accesspunkt mot tjänst

Operatören skall ange anslutningskapaciteten (hastigheten) i kbit/s eller i Mbit/s som avser den IP-trafik som erhålls igenom accesspunkten mellan användarens nät och operatörens tjänst.

04.12 Adress för accesspunkten

Ange fysisk adress för leverans av IP-tjänsten.

05 Nivå 2-protokoll

05.11 10 Mbit/s Ethernet

Erbjuds 10 Mbit/s Ethernet över elektriskt, 10Base2, AUI-gränssnitt, 10BaseT-gränssnitt eller optiskt Foil-gränssnitt?

Alternativ är JA eller NEJ.
Ange vad som erbjuds.

Kommentar: Abonnenten och operatören bör vid beställningstillfället ange vilket gränssnitt som skall användas, exempelvis ett AUI-gränssnitt.

05.12 100 Mbit/s Ethernet

Erbjuds 100 Mbit/s Ethernet över elektriskt 100BaseTX halv duplex, 100BaseTX full duplex, MII-kontakt för transceiver eller 100BaseFX optiskt gränssnitt?

Alternativ är JA eller NEJ.
Ange vad som erbjuds.

Kommentar: Abonnenten och operatören bör vid beställningstillfället ange vilket gränssnitt som skall användas, exempelvis 100BaseTX halv duplex.

05.13H Token Ring, 4 eller 16 Mbit/s

05.14H FDDI/ISO 9314 single-attachment med multimode-fiber

05.15H FDDI/ISO 9314 dual-attachment med singlemode-fiber

05.16 1 Gbit/s Ethernet

a) Erbjuds 1 Gbit/s Ethernet över kategori 5 partvinnad kabel?

Alternativ är JA eller NEJ.

b) Erbjuds 1 Gbit/s Ethernet över optisk kabel?

Alternativ är JA eller NEJ.

Anmärkning: Abonnenten och operatören avtalar vid beställningstillfället vilket gränssnitt som skall användas, exempelvis optiskt gränssnitt och multimode fiberanslutning med SC-duplexkontakter.

Kommentar:
05.21 -05.28 i **del 3** är en uppräkning av tänkbara nivå 2-protokoll som är mer eller mindre relevanta för en IP-tjänst. Dessa inkluderas i del 3 för att göra förteckningen mera komplett. Används något av dessa gränssnitt (05.21-05.28) som avlämningspunkt, utgör LAN-interfacet eller motsvarande på den utrustning som terminerar förbindelsen från operatören den punkt där tjänsten levereras.

06 Nivå 3-protokoll (IPv4, IPv6)

06.11 IPv4 Unicastförmedling

Förklaring: IPv4 Unicastförmedling innebär att operatören tillhandahåller transport av IPv4-paket med en adress till avsändaren och en adress till mottagaren. IP-paketen förmedlas av operatörens nät baserat på den routinginformation operatören erhåller från sina abonnenter och från andra med vilka man utbyter routinginformation.

Ett Unicast-paket har mottagaradresser i utrymmet mellan 1.0.0.0 och 223.255.255.255.

Erbjuder operatören IPv4 Unicastförmedling?

Alternativ är JA eller NEJ.

06.12 IPv4 Multicastförmedling

Förklaring: IP Multicastförmedling innebär att operatören tillhandahåller transport av IPv4-paket där mottagaradressen är en IP-gruppadress. Förmedlingstjänsten håller reda på alla mottagare i en viss grupp och levererar en kopia av alla paket till alla mottagare som är medlemmar i en viss grupp.

Mellan abonnentens dator och den första routern används IGMP (version 2 eller 3) för att indikera vilka grupper ett ändsystem önskar delta i. Mellan routrar används PIM-SM och eventuellt något Unicast routingprotokoll för att hantera de fall då Unicast- och Multicast-topologierna inte är samma.

I de fall abonnenten har egna routrar på sin sida av avlämningspunkten, kan kunden endera använda en RP (RP är mötesplatsen, rendez vous point, där sändare och mottagare möts för att kunna bygga källbaserade distributionsträd) inom operatörens nät för globala gruppadresser. Om inte så kan MSDP eller BGMP användas mellan operatören och abonnenten.

I de fall abonnenten är multipelansluten till samma eller flera olika operatörer måste BGP4+ med Multicast NLRI användas.

Operatörens nät skall vara så utformat att då ingen mottagare finns registrerad hos abonnenten skall distributionsträdet klippas av så långt upp som möjligt. Ingen trafik skall skickas genom accesspunkten till abonnentens nät (efter viss fördröjning från det att man lämnat viss grupp).

Multicast gruppadresser har IP-adresser i utrymmet mellan 224.0.0.0 och 239.255.255.255.

Erbjuder operatören IPv4 Multicastförmedling?

Alternativ är JA eller NEJ.

06.13 Multicastadresser

Om abonnenten har behov av att skicka information till Multicastgrupper där Multicastadressen är mer eller mindre statisk, tillhandahåller operatören en klass D-adress för detta ändamål?

Alternativ är JA eller NEJ.

06.14 Multicastadresser mellan 239.0.0.0 till 239.255.255.255

Förklaring: Multicastadresser mellan 239.0.0.0 och 239.255.255.255 är avsedda för lokalt bruk.

Har operatören organiserat dessa multicastadresser på ett sådant sätt att det lokalt kan innebära trafik mellan abonnenter till samma operatör?

Alternativ är JA eller NEJ.

06.21 IPv6 Unicastförmedling

Förklaring: IPv6 Unicastförmedling innebär att operatören tillhandahåller transport av IPv6-paket med en avsändaradress och en mottagaradress enligt IPv6. För vägval används någon form av routingprotokoll.

Ett Unicastpaket har mottagaradresser inom den del av adressrymden för IPv6 som är avsedd för Unicasttrafik.

Erbjuder operatören IPv6 Unicastförmedling?

Alternativ är JA eller NEJ.

06.22 IPv6 Multicastförmedling

Förklaring: IPv6 Multicastförmedling innebär att operatören tillhandahåller detta inom den del av IPv6-adressrymden som är avsedd för Multicasttrafik.

Erbjuder operatören IPv6 Multicastförmedling?

Alternativ är JA eller NEJ.

07 Routingprotokoll

Routingprotokoll används för att informera Internets routrar om var olika destinationer (prefix/mask) är anslutna i nätet. För att trafiken skall kunna nå en abonnent krävs att vägen till de adresser som används av abonnenten är kända inom resten av Internet.

Externa routingprotokoll

07.11 Routinginformation med BGP4

a) Erbjuder operatören möjlighet att utbyta routinginformation med abonnenten med protokollet BGP4+?

Alternativ är JA eller NEJ

b) **Förklaring:** BGP4+ innehåller möjlighet till multiprotokoll-hantering i BGP. De funktioner som är relevanta, beroende på levererad tjänst, är:

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

IPv4 Unicast är inte upptaget i förteckningen ovan då detta är ett krav för att BGP skall fungera.

Stödjer operatören ytterligare NLRI förutom IPv4 Unicast?

Alternativ är JA eller NEJ.

Vid JA: Ange 1, 2 eller 3 beroende på vilka ytterligare NLRI som stöds i gränsytan mot abonnent.

07.12 Routinginformation med BGP4 inklusive communities

Erbjuder operatören möjlighet att utbyta routinginformation med abonnenten med protokollet BGP4 inkluderande BGP communities?

Alternativ är JA eller NEJ.

Vid JA: Operatören skall bifoga en förteckning över vilka communities som används och deras funktioner.

07.13H Routinginformation med IDRP

07.14 Manuellt förkonfigurerad routing (statisk)

Har operatören och abonnenten manuellt förkonfigurerad routing på respektive sida om accesspunkten (i stället för att utbyta dynamisk routinginformation)?

Alternativ är JA eller NEJ.

Interna routingprotokoll

07.21 Routinginformation med RIP-2

Erbjuder operatören möjlighet att utbyta routinginformation med abonnentens utrustning med hjälp av RIP-2?

Alternativ är JA eller NEJ.

07.22 Routinginformation med OSPF

Erbjuder operatören möjlighet att utbyta routinginformation med abonnentens utrustning med hjälp av OSPF?

Alternativ är JA eller NEJ.

07.23 Routinginformation med Integrerad IS-IS

Erbjuder operatören möjlighet att utbyta routinginformation med abonnentens utrustning med hjälp av Integrerad IS-IS?

Alternativ är JA eller NEJ.

07.24 Routinginformation med EIGRP

Erbjuder operatören möjlighet att utbyta routinginformation med abonnentens utrustning med hjälp av EIGRP?

Alternativ är JA eller NEJ.

07.25 Routinginformation med OSPF-16

Erbjuder operatören möjlighet att utbyta routinginformation med abonnentens utrustning med hjälp av OSPF-16?

Alternativ är JA eller NEJ.

07.26 Routinginformation med RIP-1

Erbjuder operatören möjlighet att utbyta routinginformation med abonnentens utrustning med hjälp av RIP-1?

Alternativ är JA eller NEJ.

Anmärkning: Protokollet RIP-1 understödjer inte klasslös routing, men kan i vissa fall användas för enklare applikationer.

07.27 Statisk konfigurering

Används statisk (manuell) konfigurering av routing i accesspunkten mellan operatören och abonnenten?

Alternativ är JA eller NEJ.

Routingprotokoll för multicast

Förklaring: Multicast används i det fall man vill distribuera information till en eller flera mottagare från en eller flera sändare. Om flera mottagare i samma del av infrastrukturen önskar ta del av samma informationsmängd erhålls bandbreddsbesparingar jämfört med att skicka en kopia till var och en från källan (Unicast). Beroende på abonnentens krav, i praktiken om abonnenten har egen infrastruktur med routrar eller inte, finns ett flertal protokoll vilka används i gränsytan.

I det enklaste fallet använder abonnenten IGMP för att registrera medlemskap i en grupp för mottagning, och i det fall att abonnenten sänder till en grupp skickas trafiken ut som Multicast till accesspunkten. I detta fall är hela hanteringen av Multicast inom operatörens ansvarsområde.

I det fall att abonnenten har egen infrastruktur (förutom accessroutern) eller andra speciella krav kan det vara nödvändigt att använda ett eller flera av nedanstående protokoll.

07.31 IGMP

Stödjer operatören IGMP med version 2 eller högre från abonnentens ändsystem till operatörens router?

Alternativ är JA eller NEJ.

07.32 MSDP

Förklaring: MSDP (Multicast Source Discovery Protocol) används för att knyta samman mötesplatser (RP, Rendez vous point) så att andra logiska nät får kännedom om de källor som finns inom eget nät.

Stödjer operatören MSDP i accesspunkten?

Alternativ är JA eller NEJ.

07.33 PIM-SM

Förklaring: PIM-SM (Protocol Independent Multicast - Sparse Mode) används för att bygga multicast distributionsträd.

I PIM-SM måste finnas något av följande alternativ:
- använda en RP i operatörens nät för globala grupper
- utbyta information om aktiva sändare med MSDP, eller
- använda BGMP/mask.

Stödjer operatören PIM-SM i accesspunkten?

Alternativ är JA eller NEJ.

07.34 Användning av PIM-SM men inte MSDP

Förklaring: I det fall gränsytan i accesspunkten mellan abonnent och operatör använder PIM-SM men inte MSDP krävs att abonnenten utpekar RP inom operatörens nät.

Ange IP-adress för RP inom operatörens nät.

07.35 Användning av NLRI Multicast när inte BGP4 används

Om gränsytan i accesspunkten mellan abonnent och operatör inte använder BGP4 med NLRI Multicast men det finns Multicast-källor inom abonnentens nät, kan operatören då annonsera prefix tillhörande abonnenten med NLRI Multicast till resten av Internet?

Alternativ är JA eller NEJ.

07.38 BGMP

Stöds utbyte av information med protokollet BGMP?

Alternativ är JA och NEJ.

Överförd routinginformation från operatör till abonnent

07.41 Full Internetrouting (utan default)

Skickar operatören över prefix/mask för alla destinationer som för tillfället är nåbara i Internet?

Alternativ är JA eller NEJ.

07.42 Selekterad routinginformation

Förklaring: Urvalskriteriet för selektering kan vara baserat på BGP AS-path filtrering, prefixfilterlista (med mask och längd), BGP communities eller en kombination av dessa.

Skickar operatören över endast en utvald del av de kombinationer av prefix/mask man känner till?

Alternativ är JA eller NEJ.

07.43 Default route till abonnenten

Skickar operatören enbart över en defaultroute (prefix/mask=0/0) till abonnenten?

Alternativ är JA eller NEJ.

07.44 BGP4+ som multicast NLRI

I de fall Unicast- och Multicast-topologierna skiljer sig från varandra, kan operatören då skicka Multicast-informationen separat med BGP4+ som Multicast NLRI?

Alternativ är JA eller NEJ.

Överförd routinginformation från abonnent till operatör

07.51 Endast adressblock ur operatörens adressutrymme

Accepterar operatören enbart adresser som omfattas av adressblock tilldelat operatören?

Alternativ är JA eller NEJ.

07.52 Prefix upp till viss längd

Förklaring: För att erhålla nåbarhet till alla delar av Internet kan det krävas speciell överenskommelse med annan operatör vilken eventuellt har andra krav på maxlängd för att acceptera routing. Operatören bör vid varje tillfälle informera abonnenten om sådana kända förhållanden.

Accepterar operatören prefix upp till viss längd t.ex. ett gammaldags "klass-C"-nät av längd 24 bitar eller ett "klass-B"-nät av längd 16 bitar?

Alternativ är JA eller NEJ.
Om JA: Ange i antal bitar vilket längsta prefix som operatören accepterar.

07.53 Godtyckligt prefix som är registrerat på abonnenten

Accepterar operatören godtyckligt prefix som är registrerat på abonnenten?

Alternativ är JA eller NEJ.

07.54 Adress ur annan operatörs adressblock

Accepterar operatören adress (sub-block) ur annan operatörs adressblock?

Alternativ är JA eller NEJ.

07.55 Multihoming

Förklaring: Multihoming innebär att en abonnent är ansluten till flera operatörer.

Stödjer operatörens routingsystem en konfiguration där en abonnent är ansluten till en eller flera *andra* operatörer?

Alternativ är JA eller NEJ.

07.56 Filtrering av routinginformation från abonnent

Implementerar operatören filterlistor för filtrering av den routinginformation man accepterar från en abonnent?

Alternativ är JA eller NEJ.

07.57 Överföring av information om Unicast-adresser innehållande Multicast-källor

Förklaring: Överföring av information från abonnent till operatör om vilka Unicast-adresser som kan innehålla Multicast-källor kan ske på olika sätt.

a) Alla Unicast-adresser antas också vara Multicast-källor?

Alternativ är JA eller NEJ.

b) Abonnenten skickar information om Unicast-adresser för Multicast-källor i form av en accesslista och operatören ombesörjer att de sänds in i den Multicast-kapabla delen av Internet?

Alternativ är JA eller NEJ.

c) Abonnenten skickar över information om Multicast-källors Unicast-adresser med hjälp av BGP4+ som Multicast NLRI?

Alternativ är JA eller NEJ.

Beskrivningsformat accesslistor

07.61 Ripe-81

Stödjer operatören Ripe-81-format?

Alternativ är JA eller NEJ.

07.62 Ripe-181

Stödjer operatören Ripe-181-format?

Alternativ är JA eller NEJ.

07.63 RPSL

Stödjer operatören RPSL?

Alternativ är JA eller NEJ.

07.64 Lista med prefix/mask som e-post

Hanterar operatören lista med prefix/mask som e-post?

Alternativ är JA eller NEJ.

07.65 Lista med prefix/mask som fax

Hanterar operatören lista med prefix/mask som fax?

Alternativ är JA eller NEJ.

07.66 Autenticering med PGP eller S/MIME

Autenticerar operatören mottagen information med PGP eller S/MIME?

Alternativ är JA eller NEJ.
Vid JA, ange vilka som stöds.

07.71 BGP-dämpning av mottagna externroutes

a) BGP-dämpas mottagna externroutes?

Alternativ är JA eller NEJ.

b) Om annan BGP-dämpning än routrarnas standardinställningar eller Ripes rekommendation används, beskriv använd konfiguration.

07.72 BGP-dämpning av mottagna abonnentroutes

a) BGP-dämpas mottagna abonnentroutes?

Alternativ är JA eller NEJ.

b) Om annan BGP-dämpning än routrarnas standardinställningar eller Ripes rekommendation används, beskriv använd konfiguration.

DHCP-serverfunktion i accesspunkten

07.81 DHCP-server i accesspunkten

Förklaring: DHCP är ett protokoll för att automatiskt konfigurera ändsystem som ansluts till ett nät. DHCP används när ett ändsystem begär att få en IP-adress tilldelad samt för att erhålla annan information som är nödvändig för att automatiskt konfigurera ändsystemet vid anslutning till ett nytt nät.

Tillhandahålls DHCP-server i accesspunkten?

Alternativ är JA eller NEJ.

07.82 Adressutrymme i statiska adresser och dynamisk adresspool

Förklaring: I vissa fall är det nödvändigt att avdela en viss del av det adressutrymme operatören tilldelat abonnenten för fasta statiska adresser, för t.ex. mailserver, DNS-server, webb-server, medan resten av tillgängligt adressutrymme placeras i en pool för dynamisk allokering till nya ändsystem som ansluts.

Tillhandahålls uppdelning av adressutrymme i statiska adresser och en dynamisk adresspool?

Alternativ är JA eller NEJ.

07.83 Loggfunktion på DHCP-server

Förklaring: För felsökning och hantering av fall med missbruk av nätresurser som skett från abonnentens nät mot annan inom Internet kan det finnas behov av loggfunktion av DHCP-servrars tilldelningar vad gäller tid/datum/IP-adress/MAC-Adress.

Har operatören loggfunktion på DHCP-servern?

Alternativ är JA eller NEJ.

Om JA, hur länge sparas loggarna?
Anges i antal dagar.

08 Prestanda i operatörens nät och accesspunkt

08.11 Minsta genomströmningskapacitetet i accessförbindelsen

Förklaring: Avsikten är att mäta minsta prestanda mellan accesspunkten och IP-funktionen i operatörens nät.

Ange minsta genomströmning som erbjuds till abonnent, ***mätt som IP-datagram*** innehållande UDP-paket som skickas från utrustning hos abonnenten till stamnätsrouter hos operatören. (Kommentar: Man kan använda loopback-funktion i den ena änden. Den kan vara avslagen, operatören slår på vid behov). Verifiera prestanda på inblandade utrustningar.

Ange minsta genomströmning i bit/s.
Beskriv mätmetoden.

Kommentar: Avsikten med 08.11 och 08.12 är att identifiera basprestanda på den tjänst/metod som valts för att ordna datatransport mellan abonnentens anslutningsutrustning och det logiska IP-nätet. Detta beroende på att vissa operatörer har valt att använda en nivå-2 tjänst, t.ex. i form av ATM för att definiera prestanda på den levererade IP-tjänsten.

08.12 Största genomströmningskapacitet i accessförbindelsen

Förklaring: Avsikten är att mäta största prestanda mellan accesspunkten och IP-funktionen i operatörens nät.

Ange största genomströmning som erbjuds till abonnent***, mätt som IP-datagram*** innehållande UDP-paket skickade från utrustning hos abonnenten till stamnätsrouter hos operatören och omvänt, dvs. från utrustning ansluten till stamnätsrouter till abonnenten. (Kommentar: Man kan använda loopback-funktion i den ena änden.)

Ange största genomströmning i bit/s.
Beskriv mätmetod.

08.21 Maximal MTU innan fragmentering sker av paket

Förklaring: Maximal MTU (Maximum Transfer Unit) mellan två abonnenter är storleken av det största IP-paketet i bytes som kan skickas innan nätets routrar fragmenterar IP-paketen.

Klarar operatören av att skicka ICMP-meddelanden som talar om att man har fragmenterat, utan att dessa paket filtreras bort i någon säkerhetsfunktion?

Alternativ är JA eller NEJ.

Om JA, ange största möjliga paket (mätt i bytes) som kan passera mellan två abonnentanslutningar innan det fragmenteras av operatörens nät.

08.30 Mätmetod genomströmning

Förklaring: Avsikten är att mäta det totala nätets tjänsteprestanda mellan två abonnentanslutningar till samma operatör. Eftersom de tidigare mätningarna har mätt upp accessledningarnas prestanda (08.11 och 08.12) återstår bl.a. att mäta prestanda på operatörens tjänst mellan de två anslutningspunkterna (se 08.31). Avståndskravet nedan relateras till det faktum att man vill mäta genom operatörens nät, inte bara på två accessledningar vilka skulle kunna vara anslutna till samma nod/router.

Mätmetod: Två abonnenter ansluts till operatörens nät med prestanda på genomströmning som motsvarar anslutningskapaciteten (bit/s enligt 04.11).

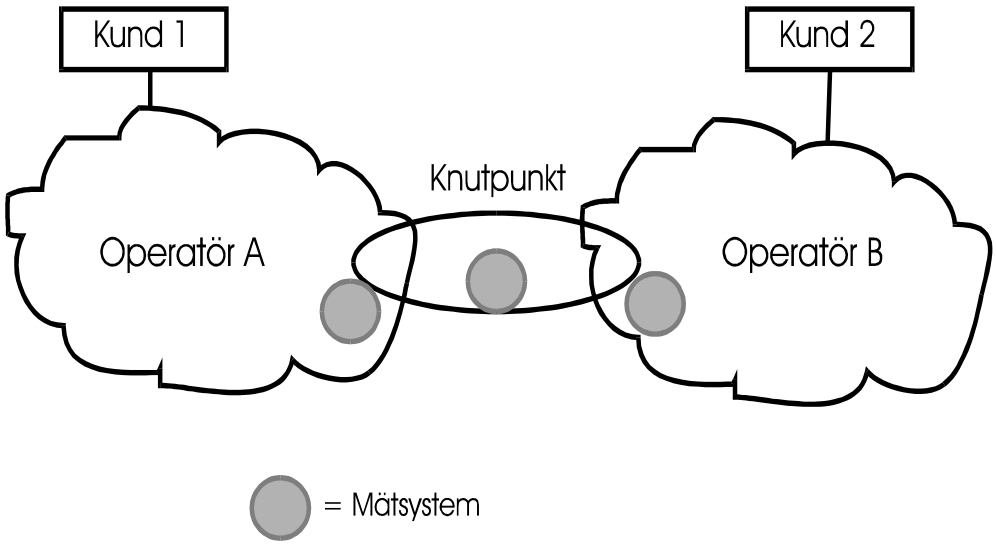
Anslutningarna skall göras till två olika noder för stamnätet inom operatörens nät. Noderna för stamnätet skall vara separerade med minst 150 km.

Trafik skickas som TCP-strömmar i båda riktningarna, t.ex. genom att man utnyttjar TCP-loopbackporten på ett datorsystem i den ena anslutningen och TCP-spray från den andra anslutningen.

Vid provet skall en datamängd av 14,4 Mbyte skickas, vilket motsvarar 60 sekunders trafik vid 1920 kbit/s. Referensfil tillhandahålles av IT-kommissionen.

Provet utförs vid tre tillfällen under vardera en timme, kl 09.00-10.00, kl 14.00-15.00 samt kl 21.00-22.00 vardagar.

Operatören skall ange det lägsta värdet (bit/s) för genomströmning som aldrig underskrids vid något av proven.



Figur mätsystem. Genomströmningsmätningar inom Operatör A sker mot A:s mätsystem. Operatör B:s abonnenter mäter på samma sätt mot B:s mätsystem. Mellan operatörerna sker mätningarna mot "motstående" mätsystem ”bakom” knutpunkten. För mätning av operatörens genomströmningsprestanda mot knutpunkten används det gemensamma mätsystemet. Mätsystemet i knutpunkten är en av de resurser som Netnod AB driver som gemensam resurs för operatörerna.

08.31 Genomströmning mellan två abonnentanslutningar till samma operatör.

Förklaring: Genomströmningen mäts enligt den metod som anges i 08.30 och med anslutningskapaciten definierad enligt 04.11.

Vad är genomströmningen mellan två abonnentanslutningar till samma operatör?

Ange genomströmningen i bit/s.

08.90* Mätpunkter i Nordamerika

Kommentar: Varje operatör som är aktuell i en upphandling eller motsvarande anger här sina favoritpunkter. Vid utvärdering skall mätning ske från varje operatörs nät till alla dessa punkter, och medelvärdet av genomströmning (se 08.92) respektive RTT beräknas (se 08.96). Mätsystemet skall vara anslutet via 100 Mbit/s Fast Ethernet Full Duplex.

Ange två stycken knutpunkter i USA, att användas vid mätningar av genomströmning respektive roundtrip time. Dessa knutpunkter skall vara generellt tillgängliga från hela Internet.

08.91* Genomströmning mellan en abonnentanslutning och nationell huvudknutpunkt i Stockholm

Förklaring: Genomströmningen mellan en abonnentanslutning med anslutningskapaciteten definierad enligt 04.11 och huvudknutpunkten i Stockholm mätt enligt den princip som anges i 08.30.

Vad är genomströmningen mellan en abonnentanslutning och huvudknutpunkten i Stockholm?

Ange genomströmningen i bit/s.

08.92* Genomströmning mellan en abonnentanslutning och mätpunkter i Nordamerika

Förklaring: Genomströmningen mellan en abonnentanslutning med anslutningskapaciteten definierad enligt 04.11 och mätpunkter i Nordamerika enligt 08.90, mätt enligt princip som anges i 08.30. Beräknas som medelvärdet av dessa mätningar.

Ange genomströmningen i bit/s.

08.93* Genomströmning till abonnent som är ansluten till annan operatör inom svensk IT-infrastruktur

Förklaring: Genomströmningen mäts enligt den princip som anges i 08.30 mellan en abonnentanslutning med anslutningskapaciteten definierad enligt 04.11 och en abonnent ansluten till annan operatör inom svensk IT-infrastruktur.

Vad är genomströmningen till abonnent ansluten till annan operatör inom svensk IT-infrastruktur?

Ange genomströmningen i bit/s.

08.94* Minsta genomströmningen till abonnent utanför svensk IT-infrastruktur

Förklaring: Genomströmningen mäts enligt den princip som anges i 08.30 mellan en abonnentanslutning med anslutningskapaciteten definierad enligt 04.11 och en abonnent ansluten till operatör utanför svensk IT-infrastruktur.

Vad är minsta genomströmningen till abonnent ansluten till operatör utanför svensk IT-infrastruktur?

08.40 Mätmetod roundtrip delay

Mätmetod: Ett datorsystem ansluts till anslutningspunkten med Ethernet-gränssnitt.

ICMP Echo Reply-meddelanden (ping) med 64 bytes datainnehåll skickas till ett annat datorsystem som är anslutet hos motstående abonnentanslutning.

Tiden anges från det att hela paketet avsänts till dess att hela paketet har mottagits i retur.

Från det av datorsystemet uppmätta värdet avgår 5 ms som kompensation för eventuella systemfördröjningar i mätutrustningen.

Provet utförs vid tre tillfällen inom perioderna, kl 09.00-10.00, kl 14.00-15.00 samt kl 21.00-22.00 vardagar. Mätningen genomförs genom att man skickar ett ICMP echo-paket (ping) varannan sekund under provperioder om 15 minuter, dvs. totalt 450 paket om vardera 64 bytes.

Medelvärdet av fördröjningstiden på paket som mottagits inom 2 sekunder efter det att paketet har avsänts används. Dock skall minst 98 % av alla paket returneras inom 2 sekunder för att mätningen skall godkännas.

08.41 Roundtrip delay mellan två abonnenters anslutningar

Förklaring: Ange roundtrip delay mellan två abonnentanslutningar med anslutningskapaciteten definierad enligt 04.11 och mätt enligt den metod som anges i 08.40.

Anges i millisekunder.

08.95* Roundtrip delay mellan en abonnentanslutning och nationell huvudknutpunkt i Stockholm

Förklaring: Roundtrip delay mellan en abonnentanslutning med anslutningskapacitet definierad enligt 04.11 och huvudknutpunkt i Stockholm mätt enligt den metod som anges i 08.40.

Anges i millisekunder.

08.96* Roundtrip delay mellan en abonnentanslutning och mätpunkter i Nordamerika

Förklaring: Roundtrip delay mellan en abonnentanslutning med anslutningskapacitet definierad enligt 04.11 och mät-

punkter i Nordamerika enligt 08.90, mätt enligt den metod som anges i 08.40. Beräknas som medelvärdet av dessa mätningar.

Anges i millisekunder.

08.51 Prestandagarantier som operatören erbjuder

Ange de prestandagarantier operatören tillämpar.

08.61 Envägs prestandamätningar

Mätmetod: Om abonnentens accessrouter har inbyggd funktion för mätningar skall denna funktion användas. Om sådan funktion inte är tillgänglig kan man skicka tidsstämplade paket med NTP-tidsstämplar från det användande systemet till mottagaren. Det avsändande systemet skickar paket med aktuell tid, kompenserad så att paketets tidsstämpel anger den tid när paketet i sin helhet lämnat det sändande systemet. Mottagaren tidsstämplar paketet när hela paketet tagits emot. Detta kräver tillgång till mycket väl synkroniserade klockor mellan sändare och mottagare. Prestanda anges i bit/s.

08.71 Prestandamätningar av tjänster med asymmetriska prestanda

Mätmetod: Mätning av riktningen med den **lägre** bandbredden sker på samma sätt som övriga punkter i detta avsnitt. Mätning av riktningen med den **högre** bandbredden hanteras enligt något av följande alternativ:

a) Abonnentens accessrouter har tillgång till inbyggd funktion för mätning. Mätning sker då med denna funktion. Detta kan ses som ett specialfall av 08.61. Prestanda anges i bit/s.

b) Abonnentens accessutrustning har inte tillgång till inbyggda mätverktyg (t.ex. ADSL avlämnat som Ethernet TP-gränssnitt). Ingen mätning är här möjlig.

08.81 Multicast prestandamätningar

Förklaring: Multicastprestanda liknar Unicastprestanda till den del som är relaterad till nätets kapacitet, men förutom Unicastfunktionaliteten tillkommer styrmekanismer etc. för att hantera byggandet av Multicast distributionsträd. Förutom förlorade paket kan Multicast förorsaka duplicerade paket.

Mätmetod: En sändare och tre mottagare inom operatörens nät samt en sändare och en mottagare vid nationell knutpunkt enligt samma modell som vid Unicast. Vid mätning används MRM (Multicast Routing Monitor Protocol, se Internet-draft ”Jusitification for and use of Multicast Routing Monitor (MRM) Protocol” 26 februari 1999), där mottagarna är test-

mottagare och sändarna är testsändare. Operatören tillhandahåller övervakningsstation som kan konfigurera sändare och mottagare.

Följande skall mätas:

- Paketförlust fördelat på respektive mottagare.
- Duplicerade paket fördelade på respektive mottagare.
- Fördröjning för leverans av paket.
- Genomströmning från sändare till mottagare.
- Tillgänglighet.

Genomströmning anges i Mbit/s av trafik sänd från testsändaren mottagen hos samtliga testmottagare med mindre än X % paketförlust och Y % paketduplicering. Alla mottagare måste uppnå dessa minimikrav.

a) Ange värde på X och Y. (Anges i % och avser förlust respektive duplicering av paket).

b) Ange i kbit/s eller Mbit/s den minsta genomströmningen utan paketförlust eller duplicering inom gränsvärdena X resp Y.

Mätmetod: Från testsändare till känd Multicastgrupp skickas ett paket var 60:e sekund under 24 timmar vilket motsvarar 86.400 sekunder.

Testsändare: En testsändare kan konfigureras att skicka paket av en viss storlek och med ett visst intervall mellan paketen. Storleken definieras i Byte och intervall i ms. För att åstadkomma testtrafik motsvarande den genomströmning man avser att prova konfigureras testsändaren att skicka paket om 64 bytes med ett intervall som ger medelgenomströmning under 60 sekunder motsvarande den genomströmningskapacitet man avser att mäta.

Testmottagare: En testmottagare konfigureras att lyssna på viss Multicastgrupp motsvarande den grupp som testsändaren sänder till och att rapportera mottagen prestanda till övervakningsstationen (Test Manager).

c) Ange antal förlorade respektive duplicerade paket under den tid mätningen pågår, dvs. 24 timmar.

09 Dynamiska parametrar

09.30 Mätmetod

Mätmetod: Från en abonnentanslutning (med anslutningskapacitet enligt 04.11) pingar man de olika rootname-servrarnas IP-adresser. 100 st 64 bytes ping avsänds med 2 sek mellanrum. Provet utförs kl 10.30, kl 13.30 samt kl 21.30 vardagar. Minst 90 % av paketen skall returneras inom 2 sek för att provet skall vara godkänt.

Ur medelvärdena från ping mot respektive server beräknas medelvärdet för var och en av servrarna, varefter medelvärdet för varje mättillfälle beräknas.

09.31 Medelavstånd till root-name servrar

Ange medelavstånd till root-name-servrar i millisekunder enligt mätmetod i 09.30.

Anges i millisekunder (ms).

09.32 Medelavstånd till uppräknade knutpunkter

Ange medelavstånd till uppräknade knutpunkter i millisekunder. Beräknas enligt den princip som anges i 09.30, men operatören får ha valfri utrustning på knutpunken. Om inget annat anges avses följande knutpunkter:

Stockholm, D-GIX
Göteborg, knutpunkten
London, Linx
Pennsauken, NAP
Virginia, MAE-East
Kalifornien, MAE-West
Amsterdam, Ripe NCC

Anges i millisekunder (ms).

09.33 Max antal förlorade paket i procent inom eget nät

Förklaring: Vid mätning av Roundtrip delay enligt 08.41 och 08.95, ange maximalt antal förlorade paket uttryckt i procent. Med förlorat paket avses här paket som helt försvann eller som levererades med större fördröjning än 2 sek.

Ange det maximala antalet förlorade paket i %.

09.41 Utbyggnad av stamnätet

Vid vilken medelbelastning på stamnätet under högtrafik (mätt i procent av tillgänglig transmissionskapacitet) sker utbyggnad?

09.42 Utbyggnad av kapacitet till nationella knutpunkter

Vid vilken medelbelastning (mätt i procent av tillgänglig transmissionskapacitet) sker utbyggnad av kapacitet till nationella knutpunkter?

09.43 Utbyggnad av kapacitet till internationella knutpunkter

Vid vilken medelbelastning (mätt i procent av tillgänglig transmissionskapacitet) sker utbyggnad av kapacitet till internationella knutpunkter?

09.51 Bandbredds-delay-quota som nätet är designat för

Förklaring: Bandbredds-delay-quota anges som bandbredd i Mbit/s mellan de kommunicerande system vid en delay-RTT av 350 ms.

Med kommunicerande system avses TCP-trafik mellan en abonnent till operatören och godtycklig motpart. Här förutsätts att accessförbindelserna mot abonnenten är begränsande för bandbredd, inte stamnät dit vi även räknar förbindelser till andra operatörer.

Bandbredd-delay-quota är ett mått på hur stora buffertar som nätelementen har för utmatning för följande fall:

1) Nätelementet sitter på plats i nätet där inkommande skurvis (burstig) trafik från flera källor har mer trafik per tidsenhet än det utgående interfacets kapacitet. Buffertminnet används för att temporärt lagra data tills dess att bursten har klingat av och då de ändsystem som kommunicerade genom detta segment av nätverket har haft möjlighet att reglera ner den mängd data de skickar.

2) Nätelementet sitter i övergång mellan en förbindelse med hög kapacitet och en med lägre kapacitet, och buffertminnet utnyttjas för att utjämna trafikskurar att motsvara medelgenomströmningen.

Observera att detta gäller för alla mellanliggande steg i nätet mellan de kommunicerande systemen, och att strategin bör vara att kunna lagra så mycket trafik att bufferten kan lagra en skur (burst) av tidslängden RTT med datamängden motsvarande det största flöde som kan utväxlas.

Största RTT i dagens Internet anses vara 350 ms. Hur stort flöde mellan två godtyckliga platser i nätet kan den minsta bufferten lagra?

Vilken bandbredd delay-quota är operatörens nät dimensionerat för?

Anges för trafik:
a) mellan abonnenter till samma operatör.
b) mellan abonnent och nationell knutpunkt (se Unicast).
c) till internationell knutpunkt i respektive världsdel.

Ange värden för a) - c) ovan i Mbit/s.

09.52 Strategi för köhantering vid begränsade resurser

Kommentar: Om exempelvis en abonnent vill bygga ett VPN-nät för telefoni och data mellan olika geografiska enheter vill man troligen att operatören på förbindelsen till abonnenten skall prioritera telefoni framför webb-trafik.

Ange köhanteringsstrategi inom stamnätets trunkförbindelser (t.ex. FIFO, RED, WRED, WFQ).

09.53 Strategi för köhantering mot abonnentledning

Ange köhanteringsstrategi på förbindelse till anslutningspunkten (t.ex. FIFO, RED, WRED, WFQ).

09.54 Köhantering vid trafik från flöden med annan trafikvolym eller andra kriteria

Vid uppkommen kösituation i nätet, tas då hänsyn till trafik från flöden vilka har annan trafikvolym eller andra kriteria?

Alternativ är JA eller NEJ.
Vid svar JA, beskriv avsedd funktion och genomförande.

09.55 Routingstatistik

Förklaring: I det fall dynamisk routing utväxlas mellan operatör och abonnent finns det i vissa fall intresse av att veta hur stabil routingen mot ett visst AS är.

Kan operatören ange statistik på 24 timmars basis som visar antalet routingcykler (dvs. nåbarhetsinformation som går från nåbar, till onåbar tillbaka till nåbar eller omvänt) för visst prefix som erhållits från alla AS som är granne med operatören, inklusive abonnenten själv?

Alternativ är JA eller NEJ.

09.56 Routingstabilitet

Vilket är det största antal routingcykler som operatören tillåter för ett prefix mottaget från abonnent innan operatören kontaktar abonnenten?

Anges som antal routingcykler per prefix per 24 timmar.

Kommentar: I det fall antalet routingcykler överskrider avtalat gränsvärde är operatören inte ansvarig för att uppfylla åtagande vad gäller tillgänglighet och prestanda.

10 Tillgänglighet/otillgänglighet

10.11 Otillgänglighet på accesslinje

Mätmetod: Otillgängligheten på accesslinjen avser tiden mätt i minuter per månad då trafik *inte* kan framföras mellan accesspunkten och motstående anslutningspunkt i operatörens nät. Övervakning skall ske från operatörens driftcentral.

En accesslinje anses vara otillgänglig när:

- Trafik inte kan framföras till operatörens accessrouter under perioder längre än 30 sekunder.
- När mer än 0,2 % av överförda paket är behäftade med felaktig kontrollsumma alternativt mer än 2 % av överförda paket försvinner vid en trafiklast om 80 % av anslutningskapaciteten.
- Om ledningen statiskt ändrar sig från uppe eller nere fler än 24 gånger per dygn.

Ange otillgängligheten i minuter per månad för accesslinjen.

Kommentar: Den andra mätningen i ordningen kan göras av abonnenten, men det förutsätter att abonnenten har SNMP läsaccess till routern på operatörens sida. Då måste operatören ha svarat JA på SNMP-frågan i 12.22.

10.12 Otillgänglighet mellan två abonnenter inom operatörens nät

Mätmetod: Otillgängligheten mäts i minuter per månad under vilka trafik *inte* kan framföras mellan två abonnentnoder enligt nedan.

Förbindelse anses finnas mellan två abonnenter i det fall att ICMP echopaket kan framföras mellan två datorsystem hos vardera abonnenten och där 99 % av IP-paket om 64 bytes returneras till avsändande datorsystem inom 150 ms mätt under 1 minut. Mätningen sker kontinuerligt.

Ange otillgängligheten i minuter per månad.

Kommentar: Om operatören kan påvisa att någon av abonnenterna har överbelastade accesslinjer respektive överbelastad accessutrustning kan detta krav inte uppfyllas.

10.13 Otillgänglighet på paketförmedling till nationell huvudknutpunkt

Mätmetod: Otillgängligheten mäts i minuter per månad under vilka trafik *inte* kan framföras mellan en abonnentnod och operatörens utrustning vid nationell knutpunkt, mätmetod enligt nedan.

Förbindelse anses finnas mellan abonnent och knutpunkt i det fall att ICMP echopaket kan framföras mellan datorsystem hos abonnenten och nationell knutpunkt och där 99 % av IP-paket om 64 bytes returneras till avsändande datorsystem inom 75 ms mätt under 1 minut. Mätningen sker kontinuerligt.

Avbrott i operatörens logiska stödsystem enligt 10.90 anses här vara likvärdigt med att paket förloras.

Tidskravet baserar sig på att det här finns en accesslinje. Anslutning till nationell knutpunkt anses vara del av operatörens stamnät.

Ange otillgängligheten i minuter per månad.

10.14 Otillgänglighet på paketförmedling till internationell knutpunkt

Mätmetod: Otillgängligheten mäts i minuter per månad under vilka trafik *inte* kan framföras mellan en abonnentnod och av operatören utpekad utrustning vid internationell knutpunkt (enligt 09.32), mätmetod enligt nedan.

Förbindelse anses finnas mellan abonnent och internationell knutpunkt i det fall att ICMP echopaket kan framföras mellan datorsystem hos abonnenten och operatörens utrustning och där 99 % av IP-paket om 64 bytes returneras till avsändande datorsystem inom 175 ms mätt under 1 min. Mätningen sker kontinuerligt.

Ange otillgängligheten i minuter per månad.

10.21 Tillgänglighetsgarantier

Här anges de tillgänglighetsgarantier som operatören erbjuder.

10.22 Redundanta förbindelser mellan stamnätsnoder med minst 50 % av normal kapacitet

Är förbindelserna mellan stamnätsnoder (noder till vilka abonnenter är anslutna) redundanta med minst 50 % av normal kapacitet?

Alternativ är JA eller NEJ.

10.23 Redundanta abonnentanslutningar tillhandahålls

Kan redundanta abonnentanslutningar tillhandahållas?

Alternativ är JA eller NEJ.

10.24 Inkopplingstid vid övergång till reservväg

Förklaring: Här avses den största avbrottstid (tid då paket inte når sin mottagare) som orsakas av fel på nätelement eller transmission inom operatörens nät för vilket redundans finns.

I det fall att en abonnent är redundant ansluten, vilken tid tar det innan full trafik har återupptagits via alternativ förbindelse i det fall att huvudvägen slås ut?

Ange i sekunder den tid som ICMP-echo-svar *inte* erhålls från motstående system, mätmetod enligt 10.12. Kommentar: Gäller endast på IP-nivå.

Ange inkopplingstiden i sekunder.

10.25 Urkopplingstid vid återgång till huvudväg

I det fall att omkoppling skett till alternativväg enligt 10.24, ange med samma mätmetod avbrottet vid återetablering av huvudtrafikväg. Kommentar: Gäller endast IP-nivån.

Ange avbrottstiden i sekunder.

10.26 Anslutning av abonnent till mer än en operatör

Tillhandahålls möjlighet att ansluta abonnent till mer än en operatör för att erhålla redundans?

Alternativ är JA eller NEJ.

10.27 Inkopplingstid vid övergång till reservväg via annan operatör

Anges i sekunder, mätmetod enligt 10.24.

Ange inkopplingstiden i sekunder.

10.28 Urkopplingstid vid återgång till huvudväg via annan operatör

Förklaring: Förutsättningen är att kunden är ett eget AS och utnyttjar BGP med båda operatörerna. Använd mätmetoden enligt 10.25.

Ange avbrottstiden i sekunder.

10.90* Operatörens logiska stödsystem

Är operatörens logiska stödsystem (DNS m.m.) utformat så att förbindelse kan etableras enligt IP-arkitekturen inom Sverige oberoende av resurser utanför svensk IT-infrastruktur?

Alternativ är JA eller NEJ.

11 Trafikfiltrering

11.31 Paketfiltrering i accesspunkten

Erbjuder operatören att för abonnentens räkning installera filterfunktion i accesspunkten, så att viss trafik mellan abonnentens och operatörens sida spärras?

Alternativ är JA eller NEJ.

11.32 Filtrering på IP-adresser

Finns möjlighet att ange filtreringsvillkor baserade på IP-paketets avsändar- eller mottagaradress?

Alternativ är JA eller NEJ.

11.33 Filtrering på protokoll

Finns möjlighet att ange filtreringsvillkor baserade på IP-protokoll? (t.ex. UDP, TCP, GRE etc).

Alternativ är JA eller NEJ.

11.34 Trafikfiltrering på portnummer

Finns möjlighet att ange filtreringsvillkor baserade på TCP/UDP-portnummer?

Alternativ är JA eller NEJ.

11.35 Trafikfiltrering på riktning

Kan filtrering ske på basis av trafikens riktning genom accesspunkten?

Alternativ är JA eller NEJ.

11.36 Filtrering av sourceroutade paket

a) Kan man konfigurera accesspunkten så att paket som har IP source route option påslagen inte släpps igenom till abonnentens nät?

Alternativ är JA eller NEJ.

b) Filtrering av ”short fragments”. Kan man konfigurera accesspunkten till att blockera paket med fragment som är så korta att fullständiga headers inte ryms (och således inte kan bedömas av filter)?

Alternativ är JA eller NEJ.

11.37 Verifiering av filterfunktionen

a) Verifieras filterfunktionen regelbundet?

Alternativ är JA eller NEJ.

b) Verifieras filterfunktionen alltid efter utförd förändring?

Alternativ är JA eller NEJ.

11.41 Abonnenten kan lägga in filter själv

Har abonnenten access till och möjlighet att själv godtyckligt konfigurera accesspunktens filtreringsfunktion?

Alternativ är JA eller NEJ.

11.42 Operatören filtrerar bort prefix avsatta för lokalt bruk och test-bruk

Filtrerar operatören bort prefix som är avsatta för lokalt bruk och testbruk (RFC 1918) vid mottagning av routing från såväl abonnenter som andra nät?

Alternativ är JA eller NEJ.

12 Övervakningsfunktioner

Detta avsnitt omfattar övervakningsfunktioner som är tillgängliga för abonnenten.

12.11 SNMP endast med läsning av accessrouter

Har abonnenten access till anslutningspunktens utrustning för läsning av parametrar omfattande egen accesspunkt och fjärrförbindelse eller motsvarande mot operatörens nät?

Alternativ är JA eller NEJ.

12.12 SNMP med skrivrättigheter till accessrouter

Har abonnenten access till anslutningspunktens utrustning för läsning och skrivning av parametrar omfattande egen accesspunkt och fjärrförbindelse eller motsvarande mot operatörens nät?

Alternativ är JA eller NEJ.

12.13 Telnet-access till accessrouter, endast läsning

Har abonnenten möjlighet att koppla upp sig mot anslutningspunktens utrustning med Telnet och efter uppkoppling läsa driftsstatistik och ge enklare kommandon som ping och traceroute?

Alternativ är JA eller NEJ.

12.14 Telnet-access till accessrouter med skrivrättigheter

Har abonnenten möjlighet att koppla upp sig mot anslutningspunktens utrustning med Telnet och efter uppkoppling läsa driftsstatistik samt godtyckligt konfigurera om accesspunkten?

Alternativ är JA eller NEJ.

12.21 SNMP-access till stamnätsrouter mot accessrouter

Har abonnenten access för läsning med hjälp av SNMP till den utrustning i operatörens nät som ansluter mot abonnentens anslutningspunkt?

Alternativ är JA eller NEJ.

12.22 SNMP-access till alla stamnätsroutrar i operatörens nät

Har abonnenten access för läsning i den utrustning som utgör operatörens stamnät och som är delad mellan flera abonnenter?

Alternativ är JA eller NEJ.

Tjänster

13 Nåbarhet

Nedan specificeras differentierade tjänster med begränsad nåbarhet. Abonnenten kan vilja ha olika nåbarhet för olika delar av världen, eventuellt med olika kapaciteter.

13.11 Alla destinationer inom operatörens eget nät

Omfattar abonnemanget nåbarhet till alla destinationer inom operatörens nät?

Alternativ är JA eller NEJ.

13.12 Alla destinationer annonserade till någon av de namngivna knutpunkterna

Omfattar abonnemanget nåbarhet till alla destinationer annonserade till någon av de namngivna knutpunkterna enligt punkt 09.32?

Alternativ är JA eller NEJ.

13.21 Icke nåbara destinationer

Ange kända begränsningar i nåbarhet till andra nät, med vilka trafik inte kan utbytas. Anges som hela AS-nummer eller individuella prefix/masklängder.

13.22 Vidarebefordran vid multicast

Förklaring: Vid Multicasttrafik skall trafik bara vidarebefordras från källa till mottagare i det fall man erhållit BGMP routinginformation från källan genom direkt eller indirekt peeringavtal.

Ange hela AS-nummer eller individuella prefix/masklängder för destinationer som operatören inte kan vidarebefordra Multicastpaket.

13.23 Default-routing vid multicast

Använder operatören default-routing i multicastsammanhang?

Alternativ är JA eller NEJ.

13.41 Prestandagarantier till annan operatör

Ange till vilka andra operatörer som prestandagarantier erbjuds genom att ange deras AS-nummer.

13.50 Ansluten till nationella knutpunkter

Är operatören ansluten till alla aktiva nationella knutpunkter som koordineras inom SOF?

Alternativ är JA eller NEJ

Om NEJ beskriv hur trafik till gemensamma resurser placerade vid knutpunkterna ordnats.

13.51 Passage av paket till nationell Internetknutpunkt

Kan alla sorters paket oberoende av options, t.ex. source-route, passera operatörens stamnät och anslutningar till nationella Internetknutpunkter?

Alternativ är JA eller NEJ.

15 Adressöversättningsfunktioner (NAT)

15.11 NAT i accesspunkten

Kan accesspunkten konfigureras med NAT som innebär att IP-adresser avsedda för lokalt bruk (RFC 1918) kan användas på LAN-sidan som sedan översätts till globalt unik IP-adress vid trafik mot Internet?

Alternativ är JA eller NEJ.

15.15 NAT med översättning 1-1

Kan accesspunkten konfigureras så att varje unik adress på LAN-sidan vid behov erhåller en globalt unik adress vid kommunikation mot Internet?

Alternativ är JA eller NEJ

15.16 NAT med s.k. "overload"-översättning

Kan accesspunkten konfigureras så att alla adresser på LAN-sidan delar på en globalt unik adress vid kommunikation mot Internet?

Alternativ är JA eller NEJ

15.17 Protokoll för NAT-funktionen

Förklaring: Vissa protokoll kan på grund av design inte fungera i en NAT. Stödet för olika protokoll förändras dessutom över tiden.

Vilka protokoll stöds av NAT-funktionen?

Ange de protokoll som stöds av NAT-funktionen.

15.21 NAT för att hantera multipelanslutning till olika operatörer

Kan accesspunkten konfigureras för multipelanslutning till flera operatörer?

Alternativ är JA eller NEJ.
Om JA, beskriv hur detta sker.

15.22 Accesspunkten och användning av globalt unika adresser

Har accesspunkten möjlighet att använda globalt unika adresser som är tilldelade utrustning anslutna till accesspunkten?

Alternativ är JA eller NEJ.

16 DNS

16.11 Namn-till-nummer för nätelement i operatörens nät

Tillhandahåller operatören uppslagning namn-till-nummer i DNS-katalog för alla nätelement i operatörens nät som har en IP-adress?

Alternativ är JA eller NEJ.

16.12 Nummer-till-namn för nätelement i operatörens nät

Tillhandahåller operatören uppslagning nummer-till-namn i DNS-katalog för alla nätelement inom operatörens nät som kan komma att transiteras av abonnenttrafik eller sända ut IP-paket?

Alternativ är JA eller NEJ.

16.13 Stöd för secure DNS

Stödjer operatörens DNS-server Internetstandard för secure-DNS enligt nedanstående?

Kommentar: Krypteringsalgoritmer som stödjs, samt hantering generellt av DNSSEC i zonen "se", förväntas att specificeras av ISOC-SE i en BOK.

a) Signerar operatören zoner i in-addr.arpa ur vilka man delegerat zon för uppslagning av nummer-till-namn till en abonnents DNS-server?

Alternativ är JA eller NEJ.

b) Signerar operatören KEY-record för delegerad zon för nummer-till-namn (PTR) ur vilken man delegerat zon till abonnents DNS-server?

Alternativ är JA eller NEJ.

c) Hanterar operatören åt abonnent nyckelhantering för kundens zon som delegerats från annan registry på Internet i de fall DNS för zonen hanteras av operatören?

Alternativ är JA eller NEJ.

d) Verifierar operatörens DNS-server signaturer för inkommande DNS-record?

Alternativ är JA eller NEJ.

16.14 Dubblerade DNS-servrar

Har operatören dubbla system för drift av DNS-server placerade på samma plats och bakom samma icke-dubblerade nätanslutning?

Alternativ är JA eller NEJ.

16.15 Dubblerade DNS-servrar med dubbel anslutning.

Förklaring: Anslutningarna skall erbjuda redundant tillkoppling till två knutpunkter. (Beakta att routing görs på ett sådant sätt att BGP-informationen för använt adressblock skapas i router nära DNS-system så att man inte annonserar "svarta hål".)

Har operatören dubbla DNS-servrar placerade på samma plats med dubblerade anslutningar till stamnät framförda i åtskild kanalisation och även i övrigt skilda transportsystem?

Alternativ är JA eller NEJ.

16.16 Dubblerade DNS-servrar på två geografiskt skilda platser

Förklaring: Anslutningarna skall erbjuda redundant tillkoppling till två knutpunkter och även ha två vägar ut mot internationell knutpunkt (NY-NAP). (Beakta att routing görs på ett sådant sätt att BGP-informationen för använt adressblock skapas i en router nära DNS så att man inte annonserar "svarta hål".)

Har operatören dubbla DNS-servrar placerade på skilda geografiska platser och anslutna till stamnätet via olika redundanta anslutningar?

Alternativ är JA eller NEJ.

16.21 Sekundär DNS-server för abonnentens namn och nummer

Erbjuder operatören drift av sekundär DNS-server för domän som tillhör abonnent?

Alternativ är JA eller NEJ.

16.22 Primär DNS-server för abonnentens namn och nummer

Erbjuder operatören drift av primär DNS-server för domän som tillhör abonnent?

Alternativ är JA eller NEJ.

16.23 Delegering av nummer-till-namn ur operatörens adressblock till abonnentens primära DNS-server

I de fall operatören tilldelat IP-adresser ur eget adressblock till abonnenten, delegeras dessa till den abonnent som önskar driva sin egen DNS-server oberoende av adressrymdens storlek?

Alternativ är JA eller NEJ.

16.24 Funktioner då operatören driver sekundär DNS

Förklaring: När operatören driver sekundär DNS för abonnentens domäner och abonnenten adderar nya underdomäner till sin huvuddomän behöver också dessa underdomäner sekundär DNS.

Ange följande:
a) Hur hanteras sekundära DNS hos operatören?
b) Är det en separat tjänst?
c) Hur kommunicerar abonnenten information om ny domän till operatören?
d) Hur övervakar operatören funktionen av DNS för underdomäner?

16.25 Funktioner då operatören driver primär DNS

I det fall operatören driver abonnentens primära DNS, stöds dynamiska DNS-uppdateringar, t.ex. från abonnentens DHCP-server?

Alternativ är JA eller NEJ.

16.90* DNS-servern enligt tekniska normer från ISOC-SE

Drivs DNS-servrarna enligt de tekniska normer (i form av BOK) som framställts av ISOC-SE?

Alternativ är JA eller NEJ.

17 E-post

17.11 Operatören kan nås via e-post enligt Internetstandard

Är det möjligt att kommunicera med samtliga funktioner inom operatörens organisation via elektronisk post enligt Internet-standard (RFC 822/RFC 821/RFC 1521/RFC 1522)?

Alternativ är JA eller NEJ.

17.12 Operatörens MTA DNS-server används för adressuppslagning

Använder operatörens Internet-posthanterare DNS och i förekommande fall MX- eller A-records för att finna motpart för utväxling av SMTP-dialog vid utsändning av e-post?

Alternativ är JA eller NEJ.

17.13 Operatören tillhandahåller "sekundär mailhost"

Förklaring: Sekundär mailhost används t.ex. i det fall abonnentens e-postsystem av någon anledning inte är nåbart från användarens dator. En sekundär mailhost skall kunna lagra 150 % av abonnentens normala postflöde under 7 dagar.

Kan abonnenten i sin DNS-server ange alternativt datorsystem som mottagare av SMTP-trafik till viss domän?

Alternativ är JA eller NEJ.

17.14 Lagringsutrymme för mellanlagring av e-post för en abonnent

Förklaring: Med lagringsutrymme avses här det utrymme som finns tillgängligt för lagring av e-post för viss abonnent.

Lagras posten hos operatören i det fall att en abonnents primära SMTP-postsystem är onåbart?

Ange storleken i megabyte diskutrymme per abonnent.

Kommentar: 17.13 och 17.14 anger i princip samma funktion, men 17.14 ger större frihet att specificera funktionen.

17.15 Retur av e-post

Sker försök att nå abonnentens MTA innan retur sker?

Alternativ är JA eller NEJ.
Om JA, ange antal dagar som försök görs.

17.16 Lagring av e-post

Kontaktas abonnentens e-postansvarige i det fall att e-post lagrats i mer än ett visst antal dagar?

Alternativ är JA eller NEJ.
Om JA, ange hur många dagar lagring sker.

17.17 Operatörens e-postsystem konfigurerat med s.k. ”Norelay”

Förklaring: En Norelay-funktion är nödvändig för att förhindra att postsystemet används för vidarebefordran av massutskick av e-post. Det innebär vidare att det måste finnas rutiner för att utbyta information mellan operatören och abonnenten för att definiera vilka adresser operatören skall agera mellanlagringssystem för.

Är operatörens e-postsystem konfigurerat med s.k. "Norelay" vilket innebär att man bara vidarebefordrar post med kända avsändar- och mottagaradresser?

Alternativ är JA eller NEJ.

Extratjänster e-post

17.21H Gateway mot UUCP

17.22H Gateway mot X.400

17.23H Gateway mot X.400 med Mime-stöd för attachments

17.24 Operatören tillhandahåller komplett e-postfunktion

Tillhandahåller operatören en komplett postfunktion som hanterar abonnentens hela domän och tillhandahåller individuella postboxar vilka kan nås från omvärlden eller från en anslutning inom abonnentens nät?

Som protokoll stöds POP2, POP3 och IMAP samt ESMTP.

Alternativ är JA eller NEJ.

Kommentar: Denna tjänst kan i övrigt utformas på många olika sätt, t.ex. vad gäller lagringsutrymme, antal postboxar, prestanda.

17.25 Operatören tillhandahåller delar av en e-postfunktion

I de fall delar av en e-postfunktion tillhandahålls, vilka protokoll stöds?
a) Stöds POP2?

b) Stöds POP3?
c) Stöds IMAP?
d) Stöds SMTP?
e) Stöds ESMTP?
f) Stöds SMTP Service Extension for Authentication?
g) Stöds TLS som krypteringsmekanism för några av de ovanstående tjänsterna?

Svaret på g) skall bestå av beskrivning av vilka och i vilka fall enbart SSL och inte TLS används.

h) Stöds några andra accessmekanismer än klartextlösenord för POP2, POP3, IMAP och SMTP AUTH?

Svaret på h) skall bestå av en lista över vilka som stöds per tjänst, t.ex. att SASL stöds för IMAP tillsammans med lista över vilka SASL-mekanismer som stöds.

18 NTP

18.11 NTP-server inom operatörens nät

Förklaring: NTP-tjänst skall vara så utformad att avvikelse från UTC-tid är mindre än 25 mikrosekunder i accesspunkten oberoende av mättillfälle.

När utrustningen är osäker på korrekt tid skall inget svar ges på tidsförfrågan till abonnentens utrustning.

Finns Stratum-1 NTP-server inom operatörens nät?

Alternativ är JA eller NEJ.

18.12 Dubblerad NTP-server inom operatörens nät

Finns dubblerad Stratum-1 NTP-server inom operatörens nät?

Alternativ är JA eller NEJ.

18.13 Kryptosignerad tidsangivelse

Stöds kryptosignerad tidsangivelse?

Alternativ är JA eller NEJ.

18.21 NTP/SNTP i accesspunkten

Är NTP/SNTP tillgänglig i accesspunkten, dvs. kan den utrustning som används för att åstadkomma accesspunkten tillhandahålla NTP och SNTP mot abonnentens nät?

Alternativ är JA eller NEJ.

18.22 NTP-funktion inom operatörens nät med IP-multicast

Finns NTP-funktion inom operatörens nät som kommunicerar med hjälp av IP-multicast?

Alternativ är JA eller NEJ.

19 News

19.11 Newsfeed till abonnentens server med NNTP

Tillhandahåller operatören news-feed omfattande alla de grupper som cirkuleras i Norden?

Alternativ är JA eller NEJ.

19.12 Genomströmningsfördröjning hos operatören

Newsdistributionen bör ha sådan kapacitet att ett inlägg till en vid upphandlingstillfället specificerad grupp skall komma fram till abonnenten högst X minuter efter det att det skickats till operatörens server, under förutsättning att abonnenten bara prenumererat på denna grupp.

Ange värdet för X i minuter.

19.21 Total news-feed

Finns möjlighet för operatören att distribuera alla förekommande publika news-grupper?

Alternativ är JA eller NEJ.

19.22 Selekterade grupper ur total news-feed

a) Har operatören en policy som gör att abonnenten inte kan få access till några kända grupper/typer av grupper?

Alternativ är JA eller NEJ
Om svaret är JA, ange den policy som gäller.

b) Kan abonnenten specificera vilka grupper man önskar ta emot?
Alternativ är JA eller NEJ.

c) Kan abonnenten specificera de grupper man inte vill ta emot?
Alternativ är JA eller NEJ.

19.23 Selektering vid massutskick före distribution

Utför operatören filtrering mot massutskick (spam) innan news-artiklar distribueras till abonnent?

Alternativ är JA eller NEJ.

19.31 NNTP-server för newsläsning från abonnentens klienter

Tillhandahåller operatören NNTP-server från vilken användare inom abonnentens nät kan läsa news med någon form av klientprogramvara?

Alternativ är JA eller NEJ.

19.32 Hur länge newsgrupper sparas i operatörens system

a) Ange hur länge en newsgrupp sparas i operatörens system.

b) Ange antal dagar per hierarki.

19.41 Antal inkommande newsfeeds till operatörens news-server

Från hur många internationella distributionskällor tas newsmatning emot till operatörens news-system?

Ange antalet.

Driftfunktioner

Med kontorstid avses här helgfri måndag – fredag kl 08.00 – 17.00.

20 Abonnentstöd

Abonnentstöd

Med abonnentstöd avses här att operatören kan ta kunden genom hela felhanteringsprocessen från anmälan till avhjälpning.

20.11 Abonnentstöd under kontorstid

Finns helpdesk-funktion tillgänglig för abonnenterna under kontorstid?

Alternativ är JA eller NEJ.

20.12 Abonnentstöd utanför kontorstid

Finns helpdesk-funktion tillgänglig utanför kontorstid?

Alternativ är JA eller NEJ.

Om JA. Ange under vilka tider (t.ex. ”24 timmar om dygnet, 7 dagar i veckan”).

20.13 Kvalificerad teknisk assistans under kontorstid

Kommentar: Med kvalificerad teknisk assistans avses att någon hos operatören kan svara på frågor om BGP, externa nät och medverka i felsökning som omfattar DNS, nät, routing och externa kontakter med andra operatörer.

Har operatören kvalificerad teknisk assistans tillgänglig under kontorstid?

Alternativ är JA eller NEJ.

20.14 Kvalificerad teknisk assistans utanför kontorstid

Kommentar: Med kvalificerad teknisk assistans avses att någon hos operatören kan svara på frågor om BGP, externa nät och medverka i felsökning som omfattar DNS, nät, routing och externa kontakter med andra operatörer.

Har operatören kvalificerad teknisk assistans tillgänglig utanför kontorstid?

Alternativ är JA eller NEJ.

Om JA. Ange under vilka tider (t.ex. ”24 timmar om dygnet och 7 dagar i veckan”).

20.15 Abonnentstöd via telefon

Kan abonnentstödsfunktionen nås med telefon till ett icke ”betalsamtalsnummer”?

Alternativ är JA eller NEJ.

20.16 Abonnentstöd via e-post

Kan abonnentstödsfunktionen nås med e-post och kvittens från en person erhållas inom 10 minuter från det att e-post nått operatörens SMTP-system?

Alternativ är JA eller NEJ.

Kommentar: Här avses den tid av dygnet som specificerats i 20.11 alternativt 20.12.

20.17 Abonnentstöd via fax

Kan abonnentstödsfunktionen nås via telefax och kvittens från en person erhållas inom 30 minuter?

Alternativ är JA eller NEJ.

Kommentar: Här avses den tid av dygnet som specificerats i 20.11 alternativt 20.12.

20.18 Abonnentstöd via webb

Är abonnentstödsfunktioner åtkomliga via webb?

Alternativ är JA eller NEJ.

20.90* Abonnentstöd på svenska

Kan operatörens personal ge abonnentstöd på svenska?

Alternativ är JA eller NEJ.

20.19 Språk vid abonnentstöd

Ange på vilka språk som operatörens personal kan lämna abonnentstöd.

20.21 Fel hanteras endast om de är inom operatörens egna nät

Hanterar operatören endast fel och problem som ligger inom operatörens eget nät?

Alternativ är JA eller NEJ.

20.22 Fel hanteras för problem inom hela Internet

Förklaring: Fel hanteras för problem inom hela Internet genom att "next-hop"-operatören och destinationsoperatören kontaktas.

Förmedlar och bevakar operatören felanmälningar även om ett fel kan anses ligga i annan operatörs nät?

Alternativ är JA eller NEJ.

Trouble management

20.31 Trouble ticket-uppdateringar skickas via e-post

Uppdateras abonnenten kontinuerligt via e-post medan ett problem åtgärdas för vilket en trouble-ticket har öppnats?

Alternativ är JA eller NEJ.

20.32 Trouble ticket-status tillgänglig via webb

Kan abonnenten med identifikation av ett problem i form av ett trouble-ticket-id själv följa upp aktuell status med hjälp av webb?

Alternativ är JA eller NEJ.

20.33 Abonnent kontaktas när trouble-ticket stängs

När ett fel som anmälts av abonnent är åtgärdat, kontaktas abonnenten regelmässigt för att verifiera att felet verkligen är avhjälpt?

Alternativ är JA eller NEJ.

Trafikstatistik tillgänglig via webb

20.41 Trafikstatistik på egen accesspunkt

Tillhandahåller operatören via webb information om trafik- och tillgänglighetsstatistik över abonnentens accesspunkt till abonnenten?

Alternativ är JA eller NEJ.

20.42 Trafikstatistik på stamnätsförbindelser

Tillhandahåller operatören via webb information om trafik- och tillgänglighetsstatistik över eget stamnät till sina abonnenter?

Alternativ är JA eller NEJ.

20.43 Trafikstatistik på anslutning till andra operatörer

I det fall privata hopkopplingar finnes till andra operatörer, tillhandahåller operatören via webb information om trafik- och tillgänglighetsstatistik för de andra operatörernas nät till sina abonnenter?

Alternativ är JA eller NEJ.

20.44 Trafikstatistik på anslutning till knutpunkter

Tillhandahåller operatören via webb information om trafik- och tillgänglighetsstatistik över egna anslutningar till nationella knutpunkter?

Alternativ är JA eller NEJ.

Tillgänglighetsstatistik

20.51 Tillgänglighet på egen linje

Redovisar operatören tillgänglighet för accesspunkten mot stamnät per månad?

Alternativ är JA eller NEJ.

20.52 Tillgänglighet till knutpunkter

Redovisar operatören tillgänglighet från sitt stamnät till de nationella huvudknutpunkterna per månad?

Alternativ är JA eller NEJ.

Routingstabilitet

20.61 Statistik över routingstabilitet

Redovisar operatören statistik över sin routingstabilitet vad det gäller stamnät och anslutningar till andra operatörer på månadsbasis?

Alternativ är JA eller NEJ.

Domänregistreringar

20.71H Registrering av domännamn

20.91* Operatören är ombud för registrering av domännamn under .SE

Är operatören ombud för registrering av domännamn under toppdomänen .SE?

Alternativ är JA eller NEJ.

20.92* Stödsystem för att garantera abonnentfunktion för trafik inom Sverige vid registrering under annan toppdomän än .SE

I de fall abonnenten väljer att registrera sig under annan toppdomän än .SE, tillhandahåller operatören nödvändiga stödsystem för att garantera abonnentens funktion för trafik inom Sverige i det fall att förbindelser mot omvärlden bryts eller om annan åtgärd utanför operatörens kontroll sker?

Alternativ är JA eller NEJ

20.74 Verifiering av information i abonnentens DNS-server samt fram- och baklängesuppslagning och enbart användning av tillåtna tecken

Kommentar: Innebär att uppslagning av namn-till-nummer respektive nummer-till-namn verifieras, samt att verifiering sker av att enbart tillåtna tecken enligt RFC 952 används i domännamn.

Verifierar operatören med regelbundna intervall att information som finns i abonnentens DNS-server är korrekt och överensstämmer mellan fram- och baklängesuppslagning?

Alternativ är JA eller NEJ
Om JA, beskriv hur detta realiseras inom operatörens infrastruktur?

21 Driftsövervakning

I de fall operatören övervakar en dynamisk parameter, t.ex. belastningen på ett nätelement, förutsätts att det insamlade materialet sparas i minst 31 dagar, så att denna information kan användas vid uppföljning av operatörens tjänst till abonnenten.

21.11 Övervakning av ingående linjebelastning

Övervakas trafiken på förbindelse från accesspunkten mot operatörens stamnät?

Alternativ är JA eller NEJ.

21.12 Övervakning av utgående linjebelastning

Övervakas trafiken på förbindelse till accesspunkten från operatörens nät?

Alternativ är JA eller NEJ.

21.13 Övervakning av mottagna felaktiga paket

Övervakas gränssnitt i anslutning till stamnät, anslutning från stamnät i anslutning mot accesspunkt samt accesspunkt mot abonnentens utrustning med avseende på mottagna paket med kontrollsummefel?

Alternativ är JA eller NEJ.

21.14 Övervakning av antal ignorerade paket

Övervakas gränssnitt i anslutning till stamnät, anslutning från stamnät i anslutning mot accesspunkt samt accesspunkt mot abonnentens utrustning med avseende på paket som inte kunde beredas plats i buffertminne i en kösituation?

Alternativ är JA eller NEJ.

21.15 Övervakning av linjestatus (upp/ner)

Övervakas gränssnitt i anslutning mellan stamnät och accesspunkt med avseende på linjestatus, t.ex. bärvågsförlust eller uteblivna keep-alive-paket?

Alternativ är JA eller NEJ.

21.16 Övervakning av nåbarhet genom Ping

Övervakar operatören från central plats i nätet att access-punktsutrustning kan nås med periodiskt utskickade ICMP echo replay-paket?

Alternativ är JA eller NEJ.

21.31 Övervakning av stödsystems nåbarhet

Förklaring: Med stödsystem avses de datorresurser och liknande som erfordras för att kunna stödja alla funktioner i Internetarkitekturen som krävs för en fullgod leverans av tjänst till abonnent.

I det fall abonnenten driver sin egen primära DNS och operatören tillhandahåller sekundär DNS omfattas övervakningen även av att operatörens sekundärservrar kan nå abonnentens primärserver.

Övervakas att stödsystem, såsom datorer med DNS, News, SMTP-mail etc, har erforderlig nåbarhet till och från övriga Internet för att kunna utföra sin uppgift?

Alternativ är JA eller NEJ.

21.32 Övervakning av stödsystems funktion

Övervakas att stödsystem fungerar på avsett sätt, t.ex. att DNS-servrar ger korrekt svar och att mail-servrar tar emot med SMTP och lagrar mottagna meddelanden?

Alternativ är JA eller NEJ.

21.33 Åtgärdstid vid detektering av felfunktion under kontorstid

Ange åtgärdstid vid detektering av felfunktion under kontorstid.

Anges i minuter.

21.34 Åtgärdstid vid detektering av felfunktion utanför kontorstid

Ange åtgärdstid vid detektering av felfunktion utanför kontorstid.

Anges i minuter.

21.41 Indikering av alternativ trafikväg

I det fall att abonnentens huvudförbindelse eller redundant väg i stamnät av någon anledning inte används, indikeras detta hos operatörens driftcentral?

Alternativ är JA eller NEJ.

21.42 Åtgärder vid fel

Finns dokumenterade rutiner om vad som skall åtgärdas och vilken rapportering som skall ske till berörda abonnenter vid olika typer av fel?

Alternativ är JA eller NEJ.

21.43 Övervakning och åtgärder baserade på nätdata

Övervakas och vidtas någon form av åtgärd baserat på insamlade nätdata?

Alternativ är JA eller NEJ.

21.44 Tröskelvärden på insamlade data för åtgärd

I det fall man övervakar och vidtar någon form av åtgärd baserat på insamlade nätdata, ange de tröskelvärden för vilka åtgärd vidtas.

Om svaret på 21.43 är JA, ange riktvärden enligt 21.45, 21.46 och 21.47.

Kommentar: I det fall man mäter trafik avses medelvärden under 5 minuter.

21.45 Linjebelastning: % av nominell kapacitet

21.46 Kontrollsummefel: Antal felaktiga paket per 5 min

21.47 Ignorerade paket: Antal ignorerade paket per 5 min

21.50 Stopp av planerade arbeten på reservförbindelser i händelse av avbrott på huvudförbindelse till abonnent

Kan abonnenten eller operatörens nätövervakningscentral stoppa planerade arbeten på reservförbindelser i händelse av avbrott på huvudaccessförbindelse till abonnent?

Alternativ är JA eller NEJ.

22 Övriga tjänster

22.11 Webb-cache för operatörens abonnenter

Kan operatören tillhandahålla ett datorsystem för mellanlagring av vanligt använda webb-dokument (webb-cache)?

Alternativ är JA eller NEJ.

22.12 Lagringskapacitet i webb-cache

Ange lagringskapacitet i megabyte för tillgängligt diskutrymme.

22.13 Bandbredd från webb-cache mot stamnät

Ange bandbredd mot stamnät i kbit/s.

23 Säkerhet

Med säkerhet avses här säkerhet i operatörens nät och stödsystem.

23.11 Uppdatering av programvara i accesspunkt och stamnät

Sker kontinuerlig uppdatering av programvara i den utrustning som bildar stamnät och accesspunkt?

Alternativ är JA eller NEJ.

23.12 Information från utrustningstillverkare, CERT, CIAC etc.

Erhåller operatören kontinuerligt information från utrustningstillverkare, CERT, CIAC etc?

Alternativ är JA eller NEJ.

Om JA, ange från vilka källor.

23.13 Rutiner för att hantera säkerhetsincidenter

Finns dokumenterade rutiner för att hantera säkerhetsincidenter?

Alternativ är JA eller NEJ.

23.14 Rutiner för att informera berörda abonnenter vid en incident

Finns rutiner för att informera berörda abonnenter vid en eventuell incident?

Alternativ är JA eller NEJ.

Tekniskt skydd för att förhindra incidenter

23.15 Filter i utgående router för att förhindra s.k. spoofing av IP-adresser

Finns det filter i utgående routrar (eller motsvarande) så att s.k. spoofing av IP-adresser inte är möjlig från operatörens nät mot annan operatör?

Alternativ är JA eller NEJ.

23.16 Filter i accesserver för att förhindra s.k. spoofing av abonnentens adresser för blockering av inkommande paket

Finns det filter i accesserver som förhindrar s.k. spoofing av abonnentens adresser, dvs. som blockerar inkommande paket

med avsändaradresser lika med, mindre än eller större än abonnentens adresser?

Alternativ är JA eller NEJ.

23.17 Filter i accesserver för att förhindra s.k. spoofing av IP-adresser från en abonnents nät genom blockering av utgående paket

Finns det filter i accesserver som förhindrar s.k. spoofing av IP-adresser från en abonnents nät, dvs. som blockerar utgående paket med avsändaradresser mindre än eller större än abonnentens adresser?

Alternativ är JA eller NEJ.

23.18 Filter i e-postsystem etc. så att operatörens e-postsystem inte kan användas för s.k. relay av e-post

Kommentar: När en avsändare vill dölja avsändaradressen kan andra system användas för att ”reläa” utskick. Detta kan exempelvis utnyttjas vid utskick av stora mängder e-post (s.k. Unsolicited Commercial Email eller Unsolicited Bulk Email), även kallat spam. Ett e-postsystem skall bara vidarebefordrar e-post med kända avsändar- och mottagaradresser.

Finns det filter i e-postsystem etc. så att operatörens e-postsystem inte kan användas för s.k. relay av e-post?

Alternativ är JA eller NEJ.

Vid JA: Ange hur filter implementeras.

23.19 Filterlistor för filtrering av oönskad e-postreklam

Används filterlistor för filtrering av oönskad e-postreklam?

Alternativ är JA eller NEJ.

Vid JA: Ange vilka filterlistor som används (exempel: RBL, DUL, ORBS).

23.20 Abonnenten lägger till egna adresser till mailfilterlistor

Kan abonnenten lägga till egna adresser till mailfilterlistor?

Alternativ är JA eller NEJ.

23.21 Filter i DNS-system som minimerar s.k. spoofing av DNS-information

Finns det filter i DNS-system som minimerar s.k. spoofing av DNS-information, dvs. att felaktiga DNS-poster införs i operatörernas DNS?

Alternativ är JA eller NEJ.

23.22 Filter i router (eller motsvarande) så att felaktig routinginformation inte sprids mellan operatörernas nät

Finns det filter i routrar (eller motsvarande) så att felaktig routinginformation hos annan operatör inte sprids in i operatörens nät?

Alternativ är JA eller NEJ.

23.23 Skydd av BGP-sessioner (eller motsvarande) vid peeringpunkter

Används skydd av BGP-sessioner (eller motsvarande) vid peeringpunkter med metoder motsvarande den som beskrivs i RFC 2385 eller liknade?

Alternativ är JA eller NEJ.

23.24 Filter (fysiskt eller logiskt) mellan samtliga abonnenter

Finns det filter (fysiskt eller logiskt) mellan samtliga abonnenter, så att två abonnenter inte kan störa varandra genom t.ex. att svara på DHCP-förfrågningar, ARP/RARP och annan ”nivå-2 broadcast”?

Alternativ är JA eller NEJ.

Vid JA: Ange hur abonnenter är skilda åt.

23.25 Accesskontrollen mellan Network Operations Center och utrustning i nätet med personlig accesskontroll

Sköts accesskontrollen mellan Network Operations Center (eller motsvarande) och aktiv utrustning i nätet med personlig accesskontroll (lösenord, certifikat eller dyl.)?

Alternativ är JA eller NEJ.

23.26 Rutiner för justering av accesskontroll när personal slutar

Finns det rutiner för justering av accesskontrollen (dvs. enligt 23.25) i samband med att personal slutar?

Alternativ är JA eller NEJ.

Vid JA: Ange vilken avdelning eller motsvarande som hanterar personal som slutar och hur informationen sprids inom företaget (operatören) till den del som handhar accessinformationen.

Övrigt

23.30 Säkerhetspolicy för datorsystem

För de datorsystem som tillhandahåller tjänster till abonnent bör det finnas en definierad och dokumenterad säkerhetspolicy. Delges denna säkerhetspolicy abonnenten?

Alternativ är JA eller NEJ.

Vid JA. Ange hur säkerhetspolicyn delges abonnenten.

23.91*H Deltagande i nationell CERT

24 Planerade avbrott och servicetider

För underhåll och uppgradering av operatörens nät krävs ibland att operatören måste göra avbrott i tjänstens tillgänglighet.

För att underlätta för såväl operatör som abonnent skall dessa i förväg komma överens om tider då service och underhåll på nätet kan utföras, vilket kan resultera i avbrott eller reducerad funktion.

Avbrott vid avtalade serviceperioder räknas inte som avbrott i tjänstens tillgänglighet.

24.01 Planerade servicetider

Ange planerade servicetider.

Kommentar: Oftast brukar operatören ha en fast tid, t.ex. söndagar kl 18.00 - 21.00 UTC.

24.02 Övning av incidenter

Sker övning vid simulerade incidenter och incidenthantering beskriven i punkt 23.14 i samarbetet med abonnent?

Alternativ är JA eller NEJ.

Vid JA: Ange hur övningen genomförs.

Utveckling

40 Utveckling av Internet

Med utveckling av Internet avses här utveckling av IP-arkitekturen och medverkan i samarbetsorganisationer för Internetoperatörer. De organisationer som anges här är internationella, undantaget är SOF som är en svensk samarbetsorganisation.

40.11 Deltagande i RIPE

Deltar operatören i RIPE?

Alternativ är JA eller NEJ.

40.12 Deltagande i EOF

Deltar operatören i EOF?

Alternativ är JA eller NEJ.

40.13 Deltagande i IETF

Deltar operatören i IETF?

Alternativ är JA eller NEJ.

40.14 Deltagande i NANOG

Deltar operatören i NANOG?

Alternativ är JA eller NEJ.

40.15 Deltagande i APRICOT

Deltar operatören i APRICOT?

Alternativ är JA eller NEJ.

40.90* Deltagande i SOF

Deltar operatören i SOF?

Alternativ är JA eller NEJ.

41 Utveckling av tjänsten

41.11 Förebyggande felrutiner

Finns rutiner för att i förebyggande syfte hitta fel och flaskhalsar innan de uppkommer?

Alternativ är JA eller NEJ.

41.12 Testlaboratorium med dedicerad personal

Har operatören ett testlaboratorium med dedicerad personal?

Alternativ är JA eller NEJ.

41.13 Pilotverksamhet med nya protokoll.

Bedriver operatören pilotverksamhet med nya protokoll som är under utveckling inom IETF?

Alternativ är JA eller NEJ.

41.90* Testveksamhet med IP version 6

Har operatören testverksamhet med IP version 6 där abonnenterna kan delta?

Alternativ är JA eller NEJ.

Del 3 Förteckning över ingående komponenter

Uppringd anslutning

03 Uppringd anslutning

03.01 IPv4 Unicast trafik
03.02 IPv4 Multicast trafik med IGMP
03.03 IPv6 Unicasttrafik
03.04 IPv6 Multicasttrafik
03.06 Access med analogt modem
03.08 Access med digital förbindelse typ ISDN

03.10 Adresstilldelning och verifieringsmetoder

03.20 E-posttjänster
03.21 Kraftförsörjning med avbrottsfri kraft 30 minuter
03.22 Internetanslutning med minst två redundanta förbindelser
03.23 Stöd för protokollet POP-2
03.24 Stöd för protokollet POP-3
03.25 Stöd för protokollet IMAP
03.26 Tillgängligt diskutrymme för lagring av e-post/mottagare
03.27 Kundens domänadress anges för ingående och utgående post

03.30 Newstjänster
03.31 Läsning av News med protokollet NNTP
03.32 Sändning av News med protokollet NNTP
03.33 Total news-feed
03.34 Selekterade grupper ur total news-feed
03.35 Selektering av massutskick före distribution
03.36 Antal dagar som artiklar i andra News-grupper sparas
03.37 Antal inkommande kompletta newsfeeds m.m.
03.38 Antal utgående newsfeeds för lokalt postade artiklar m.m.

03.40 DNS-stöd
03.41 Cachande DNS-resolver finns som kan användas av abonnent
03.42 Sekundära DNS-servrar finns på minst två olika platser i nätet
03.43 Stöder Secure-DNS

03.50 Genomströmning och prestanda
03.51 Mätning av genomströmning mellan abonnentsystem och operatörens server
03.52 Minsta genomströmning
03.53 Mätning av genomströmning mellan abonnentanslutning och nationell huvudknutpunkt
03.54 Genomströmning mellan en abonnentanslutning och NY-NAP i Pennsauken USA

03.55	Roundtrip delay mellan abonnentanslutning och nationell huvudknutpunkt
03.56	Roundtrip delay mellan abonnentanslutning och NY-NAP i Pennsauken, USA

03.60 Säkerhet

03.61	Uppdatering av programvara i accesspunkt och stamnät
03.62	Information från utrustningstillverkarna, CERT, CIAC etc
03.63	Rutiner för att hantera säkerhetsincidenter
03.64	Rutiner för att informera berörda abonnenter vid en incident
03.65	Filter i utgående router för att förhindra s.k. spoofing av IP-adresser
03.66	Filter i accesserver för att förhindra s.k. spoofing av abonnentens adresser för blockering av inkommande paket
03.67	Filter i accesserver för att förhindra s.k. spoofing av IP-adresser från en abonnents nät genom blockering av utgående paket
03.68	Filter i e-postsystem etc. så att operatörens e-postsystem inte kan användas för s.k. relay av e-post
03.69	Filterlistor för filtrering av oönskad e-postreklam
03.70	Abonnenten lägger till egna adresser till mailfilterlistor
03.71	Filter i DNS-system som minimerar s.k. spoofing av DNS-information
03.72	Filter i router (eller motsvarande) så att felaktig routinginformation inte sprids mellan operatörernas nät
03.73	Skydd av BGP-sessioner (eller motsvarande) vid peeringpunkter enligt RFC 2385 eller liknande
03.74	Filter mellan samtliga abonnenter
03.75	Accesskontrollen mellan Network Operations Center (eller motsvarande) och utrustning i nätet med personlig accesskontroll
03.76	Rutiner för justering av accesskontroll när personal slutar
03.77	Säkerhetspolicy för datorsystem

03.80 Övriga tilläggstjänster

03.81	”Shell account” på permanent uppkopplad Unix-dator
03.82	Möjlighet för abonnent att lägga upp egna webbsidor
03.83	Tillgängligt diskutrymme för egna webbsidor, standard
03.90	Antal dagar som swnet.* och se.* sparas
03.91	Medelfördröjning i minuter från postad till läsbar artikel

Fast anslutning

04 Accesspunkten

04.11	Anslutningskapacitet för accesspunkt mot tjänst
04.12	Adress för accesspunkten (fysisk)

05 Nivå 2-protokoll

05.11	10 Mbit/s Ethernet V2/ISO 8802.3, LLC1/SNAP (RFC 1042)	
05.12	100 Mbit/s Ethernet	LLC1/SNAP (RFC 1042)
05.13H	Token-Ring/ISO 8802.5	LLC1/SNAP (RFC 1042)
05.14H	FDDI/ISO 9314, single	LLC1/SNAP (RFC 1042)
05.15H	FDDI/ISO 9314, dual	LLC1/SNAP (RFC 1042)
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 Nivå 3-protokoll (IPv4, IPv6)

06.11	IPv4 Unicastförmedling
06.12	IPv4 Multicastförmedling
06.13	Multicastadresser
06.14	Multicastadresser mellan 239.0.0.0 till 239.255.255.255
06.21	IPv6 Unicastförmedling
06.22	IPv6 Multicastförmedling

07 Routingprotokoll

Externa routingprotokoll

07.11	BGP4
07.12	BGP4 inkl. BGP communities
07.13H	IDRP
07.14	Statisk routing

Interna routingprotokoll

07.21	RIP-2
07.22	OSPF
07.23	Integrerad IS-IS
07.24	EIGRP
07.25	OSPF-16
07.26	RIP-1
07.27	Statisk konfiguring

Routingprotokoll för multicast

07.31	IGMP
07.32	MSDP

07.33 PIM-SM
07.34 Användning av PIM-SM men inte MSDP
07.35 Användning av NLRI Multicast när inte BGP4 används
07.38 BGMP

Överförd routinginformation från operatör till abonnent
07.41 Full Internetrouting (utan default)
07.42 Selekterad routinginformation
07.43 Default routing till abonnenten
07.44 BGP4+ som multicast NLRI

Överförd routinginformation från abonnent till operatör
07.51 Endast adressblock ur operatörens adressutrymme
07.52 Prefix upp till viss längd, maximilängd
07.53 Godtyckligt prefix registrerat på abonnenten
07.54 Adresser ur annan operatörs adressblock
07.55 Multihoming
07.56 Filtrering av routinginformation från abonnent
07.57 Överföring av information om Unicast-adresser innehållande Multicast-källor

Beskrivningsformat accesslistor
07.61 Ripe-81
07.62 Ripe-181
07.63 RPSL
07.64 Lista med prefix/mask som e-post
07.65 Lista med prefix/mask som fax
07.66 Autenticering med PGP eller S/MIME

07.71 BGP-dämpning av mottagna externroutes
07.72 BGP-dämpning av mottagna abonnentroutes

DHCP-serverfunktion i accesspunkten
07.81 DHCP-server i accesspunkten
07.82 Adressutrymme i statiska adresser och dynamisk adresspool
07.83 Loggfunktion på DHCP-server

08 Prestanda i operatörens nät och accesspunkten

08.11 Minsta genomströmningskapacitet i accessförbindelsen (bit/s)
08.12 Största genomströmningskapacitet i accessförbindelsen (bit/s)

08.21 Max MTU som stöds av operatörens nät (bytes) innan fragmentering av paket sker.

08.30 Mätmetod genomströmning
08.31 Genomströmning mellan två abonnentanslutningar till samma operatör

08.40 Mätmetod roundtrip delay
08.41 Roundtrip delay mellan två abonnenters anslutningar

08.51 Prestandagarantier som operatören erbjuder.

08.61 Envägs prestandamätningar

08.71 Prestandamätningar av tjänst med asymmetriska prestanda

08.81 Prestandamätningar vid multicast

08.90 Mätpunkter i Nordamerika
08.91 Genomströmning mellan en abonnentanslutning och nationell huvudknutpunkt i Stockholm
08.92 Genomströmning mellan en abonnentanslutning och mätpunkter i Nordamerika
08.93 Genomströmning till abonnent som är ansluten till annan operatör inom svensk IT-infrastruktur
08.94 Minsta genomströmning till abonnent utanför svensk IT-infrastruktur
08.95 Roundtrip delay mellan en abonnentanslutning och nationell huvudknutpunkt i Stockholm
08.96 Roundtrip delay mellan en abonnentanslutning och mätpunkter i Nordamerika

09 Dynamiska parametrar

Prestanda

09.30 Mätmetod
09.31 Medelavstånd till root-name servrar (ms)
09.32 Medelavstånd till uppräknade knutpunkter (ms)
09.33 Max antal förlorade paket i procent inom eget nät (%)

09.41 Medelbelastning på stamnätet vid vilken utbyggnad sker (%)
09.42 Medelbelastning vid vilken utbyggnad av kapacitet till nationella
knutpunkter sker (%)
09.43 Medelbelastning vid vilken utbyggnad av kapacitet till internationella knutpunkter sker (%)

09.51 Bandbredds-delay-quota som nätet är designat för
09.52 Strategi för köhantering vid begränsade resurser
09.53 Strategi för köhantering mot abonnentledning
09.54 Köhantering vid trafik från flöden med annan trafikvolym eller andra kriteria
09.55 Routingstatistik
09.56 Routingstabilitet

10 Tillgänglighet/Otillgänglighet

10.11 Otillgänglighet på accesslinje
10.12 Otillgänglighet mellan två abonnenter inom operatörens nät
10.13 Otillgänglighet på paketförmedling till nationell huvudknutpunkt
10.14 Otillgänglighet på paketförmedling till internationell knutpunkt

10.21 Tillgänglighetsgarantier
10.22 Redundanta förbindelser mellan stamnätsnoder med minst 50 % av normal kapacitet
10.23 Redundanta abonnentanslutningar tillhandahålls
10.24 Inkopplingstid vid övergång till reservväg
10.25 Urkopplingstid vid återgång till huvudväg
10.26 Anslutning av abonnent till mer än en operatör
10.27 Inkopplingstid vid övergång till reservväg via annan operatör
10.28 Urkopplingstid vid återgång till huvudväg via annan operatör

10.90 Operatörens logiska stödsystem (DNS m.m.)

11 Trafikfiltrering

11.31 Paketfiltrering i accesspunkten
11.32 Filtrering på IP-adresser
11.33 Filtrering på protokoll
11.34 Trafikfiltrering på portnummer
11.35 Trafikfiltrering på riktning
11.36 Filtrering av sourceroutade paket
11.37 Verifiering av filterfunktionen

11.41 Abonnenten kan lägga in filter själv
11.42 Operatören filtrerar bort prefix avsatta för lokalt och testbruk

12 Övervakningsfunktioner

12.11 SNMP endast med läsning av accessrouter
12.12 SNMP med skrivrättigheter till accessrouter
12.13 Telnet-access till accessrouter, endast läsning
12.14 Telnet-access till accessrouter med skrivrättigheter

12.21 SNMP-access till stamnätsrouter mot accessrouter
12.22 SNMP-access till alla stamnätsroutrar i operatörens nät

Tjänster

13 Nåbarhet

13.11 Alla destinationer inom operatörens eget nät

13.12 Alla destinationer annonserade till någon av de namngivna knutpunkterna enligt 09.32

13.21 Icke nåbara destinationer (AS-nummer eller prefix)
13.22 Vidarebefordran vid multicast
13.23 Default-routing vid multicast

13.41 Prestandagarantier till annan operatör

13.50 Ansluten till nationella knutpunkter
13.51 Passage av paket till riksknutpunkter

15 Adressöversättningsfunktioner (NAT)

15.11 NAT i accesspunkten
15.15 NAT med översättning 1-1
15.16 NAT med ”overload”-översättning
15.17 Protokoll för NAT-funktionen

15.21 NAT för multipelanslutning till olika operatörer
15.22 Accesspunkten och användning av globalt unika adresser

16 DNS

16.11 Namn-till-nummer för nätelement i operatörens nät
16.12 Nummer-till-namn för nätelement i operatörens nät
16.13 Stöd för secure DNS
16.14 Dubblerade DNS-system
16.15 Dubblerade DNS-system med dubbel anslutning
16.16 Dubblerade DNS-system på olika geografiska platser

16.21 Sekundär DNS för abonnentens namn och nummer
16.22 Primär DNS för abonnentens namn och nummer
16.23 Delegering av nummer-till-namn ur operatörens adressblock till abonnentens primära DNS
16.24 Funktioner då operatören driver sekundär DNS
16.25 Funktioner då operatören driver primär DNS

16.90 DNS-servern enligt tekniska normer från ISOC-SE

17 E-post

17.11 Operatören kan nås via e-post enligt Internetstandard (RFC 822/RFC 821/RFC 521/RFC 1522)
17.12 Operatörens MTA använder DNS för adressuppslagning
17.13 Operatören tillhandahåller "sekundär mailhost"
17.14 Lagringsutrymme för mellanlagring av e-post för en abonnent
17.15 Retur av e-post
17.16 Lagring av e-post
17.17 Operatörens e-postsystem konfigurerat med s.k. ”Norelay”

Extratjänster e-post

17.21H Gateway mot UUCP
17.22H Gateway mot X.400
17.23H Gateway mot X.400 med Mime stöd för attachments
17.24 Operatören tillhandahåller komplett e-postfunktion
17.25 Operatören tillhandahåller delar av en e-postfunktion

18 NTP

18.11 NTP-server inom operatörens nät
18.12 Dubblerad NTP-server inom operatörens nät
18.13 Kryptosignerad tidsangivelse

18.21 NTP/SNTP tillgänglig i accesspunkten
18.22 NTP-funktion inom operatörens nät med IP-multicast

19 News

19.11 Newsfeed till abonnentens server med NNTP
19.12 Genomströmningsfördröjning hos operatören

19.21 Total news-feed
19.22 Selekterade grupper ur total news-feed
19.23 Selektering vid massutskick före distribution

19.31 NNTP-server för newsläsning från abonnentens klienter
19.32 Hur länge newsgrupper sparas i operatörens system

19.41 Antal inkommande newsfeeds till operatörens news-server

Driftfunktioner

20 Abonnentstöd

Abonnentstöd

20.11 Abonnentstöd under kontorstid
20.12 Abonnentstöd utanför kontorstid
20.13 Kvalificerad teknisk assistans under kontorstid
20.14 Kvalificerad teknisk assistans utanför kontorstid
20.15 Abonnentstöd kan nås via telefon
20.16 Abonnentstöd kan nås via e-post
20.17 Abonnentstöd kan nås via fax
20.18 Abonnentstöd nåbar via webb
20.19 Språk vid abonnentstöd

20.21 Fel hanteras endast om de är inom operatörens egna nät
20.22 Fel hanteras för problem inom hela Internet

Trouble management

20.31 Trouble ticket uppdateringar skickas via e-post
20.32 Trouble ticket status tillgänglig via webb
20.33 Abonnent kontaktas när trouble-ticket stängs

Trafikstatistik tillgänglig via webb
20.41 Trafikstatistik på egen accesspunkt
20.42 Trafikstatistik på stamnätsförbindelser
20.43 Trafikstatistik på anslutning till andra operatörer
20.44 Trafikstatistik på anslutning till knutpunkter

Tillgänglighetsstatitik
20.51 Tillgänglighet på egen linje
20.52 Tillgänglighet till knutpunkter

Routingstabilitet
20.61 Statistik över routingstabilitet

Domänregistreringar
20.71H Registrering av domännamn
20.74 Verifiering av information i abonnentens DNS-server samt fram- och baklängesuppslagning och enbart användning av tillåtna tecken

20.90 Abonnentstöd på svenska
20.91 Operatören ombud för registrering av domännamn under .SE
20.92 Stödsystem för att garantera abonnentfunktion för trafik inom Sverige vid registrering under annan toppdomän än .SE

21 Driftsövervakning

21.11 Övervakning av inkommande linjebelastning
21.12 Övervakning av utgående linjebelastning
21.13 Övervakning av mottagna felaktiga paket
21.14 Övervakning av antal ignorerade paket
21.15 Övervakning av linjestatus (upp/ner)
21.16 Övervakning av nåbarhet genom Ping

21.31 Övervakning av stödsystems nåbarhet
21.32 Övervakning av stödsystemens funktion
21.33 Åtgärdstid vid detektering av felfunktion under kontorstid
21.34 Åtgärdstid vid detektering av felfunktion utanför kontorstid

21.41 Indikering av alternativ trafikväg
21.42 Åtgärder vid fel
21.43 Övervakning och åtgärder baserade på nätdata
21.44 Tröskelvärden på insamlade data för åtgärd
21.45 Linjebelastning: % av nominell kapacitet
21.46 Kontrollsummefel: Antal felaktiga paket per 5 min
21.47 Ignorerade paket: Antal ignorerade paket per 5 min

21.50 Stopp av planerade arbeten på reservförbindelser i händelse av avbrott på huvudförbindelse till abonnent

22 Övriga tjänster

22.11 Webb-cache för operatörens abonnenter
22.12 Lagringskapacitet i megabyte för webb-cache
22.13 Bandbredd från webb-cache mot stamnät

23 Säkerhet

23.11 Uppdatering av programvara i accesspunkt och stamnät
23.12 Information från utrustningstillverkarna, CERT, CIAC etc
23.13 Rutiner för att hantera säkerhetsincidenter
23.14 Rutiner för att informera berörda abonnenter vid en incident

Tekniskt skydd för att förhindra incidenter

23.15 Filter i utgående router för att förhindra s.k. spoofing av IP-adresser
23.16 Filter i accesserver för att förhindra s.k. spoofing av abonnentens adresser för blockering av inkommande paket
23.17 Filter i accesserver för att förhindra s.k. spoofing av IP-adresser från en abonnents nät genom blockering av utgående paket
23.18 Filter i e-postsystem etc. så att operatörens e-postsystem inte kan användas för s.k. relay av e-post
23.19 Filterlistor för filtrering av oönskad e-postreklam

23.20 Abonnenten lägger till egna adresser till mailfilterlistor
23.21 Filter i DNS-system som minimerar s.k. spoofing av DNS-information
23.22 Filter i router (eller motsvarande) så att felaktig routinginformation inte sprids mellan operatörernas nät
23.23 Skydd av BGP-sessioner (eller motsvarande) vid peeringpunkter enligt RFC 2385 eller liknande
23.24 Filter (fysiskt eller logiskt) mellan samtliga abonnenter
23.25 Accesskontrollen mellan Network Operations Center (eller motsvarande) och utrustning i nätet med personlig accesskontroll
23.26 Rutiner för justering av accesskontroll när personal slutar

Övrigt

23.30 Säkerhetspolicy för datorsystem
23.91H Deltar i nationell CERT verksamhet

24 Planerade avbrott och servicetider

24.01 Planerade servicetider
24.02 Övning av incidenter

Utveckling

40 Utveckling av Internet

40.11 Deltar i RIPE
40.12 Deltar i EOF
40.13 Deltar i IETF
40.14 Deltar i NANOG
40.15 Deltar i APRICOT

40.90 Deltar i SOF

41 Utveckling av tjänsten

41.11 Förebyggande felrutiner
41.12 Testlaboratorium med dedicerad personal
41.13 Pilotverksamhet med nya protokoll

41.90 Testveksamhet med IP version 6

Ordlista

ADSL	Asymmetric Digital Subsciber Line
APRICOT	Asia Pacific Regional Internet Conference on Operational Technology
AS	Autonomous System
Asymmetrisk kommunikation	Asymmetrisk kommunikation innebär att överföringskapaciteten är högre i riktning *till* användaren än *från* användaren
ATM	Asynchronous Transfer Mode
AUI	Attachment Unit Interface
BGP	Border Gateway Protocol
BGMP	Border Gateway Multicast Protocol
BNC	Kontakttyp för Ethernet
BOK	Begäran om kommentar; dokumentserie som utges av ISOC-SE
CERT	Computer Emergency Response Team
CHAP	Challenge Handshake Protocol
CIAC	Computer Incident Advisory Committee
D-GIX	Distributed Global Internet Exchange, knutpunkt för trafikutbyte mellan operatörer
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 för lokala nät
FDDI	Fiber Distributed Data Interface
FIFO	First In First Out
GRE	Generic Routing Encapsulation
IAB	Internet Architecture Board, utses av ISOC för att hålla uppsikt över Internets arkitektur och protokoll. Fungerar som rådgivare åt IETF och ISOC i frågor om teknik, arkitektur, procedurer och policy för Internet
ICMP	Internet Control Message Protocol
ISOC-SE	Den svenska avdelningen av ISOC
IDRP	Inter-Domain Routing Protocol
IEPG	Internet Engineering and Planning Group
IESG	Internet Engineering Steering Group, del av ISOC med ansvar för ledningen av IETF:s tekniska aktiviteter. Leder Internets standardiseringsprocess och godkänner specifikationer som Internetstandarder
IETF	Internet Engineering Task Force, består av nätbyggare, operatörer, leverantörer och forskare som arbetar med att utveckla driften av Internet och dess arkitektur. Är de som i huvudsak arbetar med att specificera nya Internetstandarder (RFC:er)
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 Organisation for Standardisation
ISOC	Internet Society
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. Protokoll för hopkoppling av PIM-SM
MTA	Message Transfer Agent
MTU	Maximum Transfer Unit
Multihoming	Innebär att en abonnent är ansluten till flera operatörer
NANOG	North American Network Operators' Group
NAT	Network Address Translator
Netnod	Netnod Internet Exchange i Sverige AB
NIC-SE	Network Information Centre Sweden AB, tillhandahåller, koordinerar och står för drift av det nationella registret för domännamn under .SE på Internet
NLRI	Network Layer Reachability Information
NNTP	Network News Transfer Protocol
NTP	Network Time Protocol
Optisk foil	Ethernet över fiber
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 där man måste begära trafik för viss grupp
PING	Packet Internet Groper, populärt uttryck för att skicka data till ett datorsystems ICMP echo-port och mäta tiden
POP	Post Office Protocol
PPP	Point-to-Point Protocol
RBL	Realtime Blackhole List (Mail Abuse Prevention System's Realtime Blackhole List, MAPS RBL)
RED	Random Early Drop
RFC	Request For Comments, en serie dokument som innehåller Internetstandarder och andra dokument som rör Internet
RIP	Routing Information Protocol
RIPE	Resaux IP Europeens
RPSL	Routing Policy Specification Language
RJ45	Registered Jack, modulär kontakt
RP	Mötesplats (”rendez-vous”) för sändare och mottagare vid multicasting
RTT	Round Trip Time, är den tid det tar för ett paket att gå från A till B och tillbaka från B till 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, undergrupp inom ISOC-SE

Spam	Oönskad massutskick av elektronisk post kallas även för UCE (Unsolicited Commercial E-mail) eller UBE (Unsolicited Bulk E-mail), även kallat skräppost
Spoofing	Någon som genererar och sänder datapaket med förfalskade avsändaradresser för att dölja sin identitet och på detta sätt försvåras spårbarheten
SSL	Secure Socket Layer
STUPI	Svensk Teleutveckling & Produktinnovation AB
Symmetrisk kommunikation	Symmetrisk kommunikation innebär att överföringskapaciteten är lika hög i båda riktningarna, dvs. både *till* och *från* användaren
TCP	Transmission Control Protocol
TLS	Transport Layer Secure
UDP	User Datagram Protocol
UTC	Universal Time Coordinated
UUCP	Unix to Unix Copy
VPN	Virtuellt privat nät
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection, som är en vidareutveckling av Random Early Detection
xDSL	x Digital Subsciber Line, där x kan bytas ut mot A (Asymmetric), H (High data rate), S (Singel line) eller V (Very high data rate)
10Base2	Ethernetstandard, 10 Mbit/s, thinwire
10BaseT	Ethernetstandard, 10 Mbit/s, twisted pair (partrådskabel)
100BaseFX	Ethernetstandard, 100 Mbit/s, fast fiber link
100BaseTX	Ethernetstandard, 100 Mbit/s, fast twisted pair