

## Krav på kundens LAN och beskrivning av gränssnitt mot Telia DataNet-anlutning

1	Byggsätt för kund-LAN.....	2
1.1	Telefoni i separat nät.....	2
1.2	Telefoni och data i gemensamt LAN.....	3
2	Krav på kundens lan.....	4
2.1	Passiv infrastruktur (kabelsystem) .....	4
2.2	Hastighet och Duplex .....	4
2.3	DHCP.....	6
2.4	DNS och adressering .....	6
2.5	Routing .....	6
2.6	Brandvägg, proxy och NAT .....	7
2.7	Spårbarhet.....	9
2.8	QoS .....	9
2.9	Adresscanning.....	11
2.10	Krav vid Internetanslutet LAN .....	11
2.11	WAN-tjänst från annan leverantör än Telia.....	11

## 1 Byggsätt för kund-LAN

För att kunna implementera IP-access till Centrex i ett företags lokala nätverk (LAN) måste vissa grundkrav uppfyllas av kundens passiva och aktiva infrastruktur. Som grundregel gäller att den aktiva LAN-utrustningen ska vara baserad på switch-teknologi med full duplex. I annat fall kan inte talkvaliteten garanteras.

Det finns olika sätt för kunden att hantera IP-telefoni i nätet; separata nät, separata VLAN på samma fysiska nät eller ett gemensamt LAN för all trafik. Centrex IP stöder samtliga alternativ, men de olika byggsätten, liksom vilken typ av Internetaccess som kunden använder, påverkar hur man ansluter mot DataNets CPE, liksom de krav som ställs på nätverksutrustningen.

### 1.1 Telefoni i separat nät

#### 1.1.1 Nätarkitektur

Separat nät används om kunden har IP-telefoner på ett lite större nät, vill ha fysisk och/eller logisk separering av adressrymder, eller av säkerhetsskäl mm. Kund ansluter switch, switchnät, eller VLAN mot Telias utrustning. Ingen logisk (eller i vissa fall fysisk) koppling finns mellan IP-telefoni och övrig trafik. Denna trafik, bland annat Internettrafik, har eget LAN/VLAN och påverkar inte telefonin.

Fördelar med fysisk separering är att:

- Inga särskilda krav behöver ställas på switch-utrustningen, t.ex. QoS.
- Ingen hänsyn behöver tas till det redan existerande lokala nätverkets logiska uppbyggnad och eventuella "trånga sektorer" som kan påverka kvaliteten för telefonin.
- Inga särskilda åtgärder behövs för isolering mot annan trafik.

Fördelar med logisk separering (oavsett om fysisk separering används eller inte)

- Adressmässig isolering
- Separat routing för telefonin
- Högre nivå av säkerhet för telefonin som inte exponeras mot exempelvis Internet (dock behöver DNS vara åtkomligt).

Nackdelar

- Användning av mjukvaruklient (softphone) i PC blir mer komplex eftersom PC-trafiken kommer att tillhöra både telefonin och den övriga trafiken. Det krävs skilda VLAN i PC:n, eller behov av en router för att särskilja IP-telefonitrafiken samt för att telefonin ska få tillgång till DNS.
- Parallella fysiska nät medför högre kostnad

#### 1.1.2 Krav

För att särskilja olika IP-strukturer används någon lämplig metod beroende på vilken teknik LAN:et baseras. Exempelvis kan VLAN-teknik och/eller routing användas för att särskilja IP-telefonitrafiken.

Vid delad fysisk infrastruktur (VLAN-nät) krävs switchar med stöd för VLAN (802.1Q) och rekommenderas starkt switchar med QoS-stöd (802.1p). För att uppfylla telefonins krav är det tillräckligt med två trafikklasser ("data" och "voice") men behovet varierar naturligtvis beroende på vilka trafiktyper i övrigt som finns i nätet. Se vidare avsnitt "QoS".

# TELIA CENTREX

Vid fysisk separerade nät kan krav på switchen eller switchnätet sättas lägre. Det är tillräckligt med switchat Ethernet 10 Mb/s (endast mot klient) eller 100 Mb/s utan stöd för 802.1Q (VLAN-tagging) eller 802.1p (VLAN-prioritering).

## 1.1.3 Gränssnitt mot DataNet

Telefoni-wlan:ets trafik överlämnas till eget interface på DataNet CPE. Detta interface kan vara antingen ett separat fysiskt interface i CPE kopplat mot en separat routerport, brandväggsport eller switchport i kundens LAN (typiskt scenario om man valt fysiskt separerat telefoninät), eller ett separat VLAN på ett interface gemensamt med annat/andra VLAN för datatrafik mot DataNet.

## 1.1.4 Kund med både Softphones och hårdvaruklienter

Softphones på PC kan inte dirigera trafik till visst VLAN vilket innebär att man antingen måste avstå separering mellan data och tal på LAN:et, eller lösa separeringen på annat sätt.

I första alternativet, att avstå separering, blir nätlösningen lika som i avsnitt 1.2, dvs. att alla klienter (både softphones och hårdvarutelefoner) kopplas på samma LAN/VLAN, och att någon router i kundens nät skiljer taltrafik mot Centrex IP från annan trafik.

I andra alternativet sätter man upp ett separat LAN för hårdvarutelefonerna, och ett separat nät (LAN eller VLAN) för PC-klienterna. Detta nät betjänar endast PC med softphones (till exempel i ett Call Center) och skiljs alltså från annan datatrafik hos företaget. Nätet kopplas till ett separat interface på en router i kundens nätmiljö, som skiljer taltrafik från vanlig datatrafik. Data routas mot kundens övriga datanät, medan taltrafiken routas till samma nät som hårdvarutelefonerna, för vidare överlämning enligt punkt 1.1.3.

Hos denna typ av kund förekommer dessutom ofta trafik mot CallGuide, som måste skiljas ut på likartat sätt.

## 1.1.5 Om kunden har separat Internetaccess

I de fall kunden har en separat Internetaccess (via Telia eller annan operatör) är grundprincipen för anslutning att kunden separerar trafik mot Internet från trafik som ska nyttja DataNet (dvs. trafik både mot Centrex IP och VPN-trafik mot kundens övriga adresser). Det är en fördel att likaledes separera Centrextrafiken från övrig VPN-trafik (liksom CallGuide-anslutning och liknande) i kundens överlämningspunkt (brandvägg eller router). I så fall sätts separata VLAN/subinterface upp i gränssnittet.

Kunden har en separat brandvägg för Internettrafiken vilket förenklar regelverket i gränssnittet mot DataNet.

## 1.1.6 Om kunden har Internetaccess med FW som VAS-tjänst i DataNet

Internettrafiken ansluter till kundens data-VPN och berör inte Centrextrafiken. Telia hanterar brandvägg mot Internet.

## 1.2 Telefoni och data i gemensamt LAN

### 1.2.1 Nätarkitektur

Detta är ofta den enklaste lösningen för kunden, men man får ingen logisk eller adressmässig separering. Situationen uppstår typiskt vid användning av softphones, men kan förekomma även med hårdvarutelefoner i exempelvis mindre nät. Lösningen ställer större krav på utrustningen i LAN:et inklusive gränssnittets utrustning med avseende på kapacitet, QoS etc. eftersom telefoni är känsligt mot störningar.

Trafiken mot Internet måste särskiljas i kundens utrustning (router krävs). Vidare måste telefoni och VPN-trafik överlämnas till DataNet CPE.

**DataNet** i sin tur skiljer ut trafik mot Centrex IP från kundintern VPN-trafik. Det rekommenderas att Centrextrafiken separeras från övrig VPN-trafik (liksom CallGuide-anslutning och liknande) i kundens överlämningspunkt (brandvägg eller router). I så fall sätts separata VLAN/subinterface upp i gränssnittet mot CPE.

## 1.2.2 Krav

Switchar och routrar i kundens LAN måste vara av s.k. Non Blocking-arkitektur, samt bör stödja standarder som IEEE802.1Q (VLAN-tagging) och IEEE802.1p (VLAN-prioritering), alternativt IP ToS/Precedence eller DSCP (DiffServ). Risk finns annars för störningar såsom att ljudet/talet hackas upp eller till och med i vissa lägen försvinner helt.

IEEE802.1p och IP ToS/Precedence/DSCP används för att prioritera olika typer av trafik i LAN:et. IP-telefoni kräver att telefonitrafiken kan prioriteras. Om inte denna funktion stöds kan inte tjänstens kvalitet garanteras.

## 1.2.3 Om kunden har separat Internetaccess

I de fall kunden har en separat Internetaccess (via Telia eller annan operatör) krävs att kunden separerar trafik mot Internet från trafik som ska nyttja DataNet (dvs. trafik både mot Centrex IP och VPN-trafik mot kundens övriga adresser).

Vidare gäller att kunden ansvarar för brandvägg mot Internet för att skydda telefonin mot störningar och intrång.

## 1.2.4 Om kunden har Internetaccess som VAS-tjänst i DataNet

Internettrafiken ansluter till kundens data-VPN och berör inte Centrextrafiken. Telia hanterar brandvägg mot Internet. Det rekommenderas att trafik till olika VLAN i kundens router eller brandvägg.

## 2 Krav på kundens lan

### 2.1 *Passiv infrastruktur (kabelsystem)*

Kabelsystemet ska minst uppfylla kraven enligt Kategori 5 för 100 Mbit/s och Kategori 5e för 1 Gb/s avseende kabelkapacitet och egenskaper.

Kabelsystemet ska minst uppfylla kraven enligt SSEN50173 klass D.

### 2.2 *Hastighet och Duplex*

#### 2.2.1 Accessport

I anslutning mellan klient (IP-telefon eller PC med softphoneklient) och switch gäller följande:

- Hastighet bör vara minst 100 Mb/s.
- Hastighet ska vara minst 10 Mb/s.
- Full Duplex ska vara säkerställt.
- Flow Control ska inte vara aktiverat på interface som hanterar IP-telefoni. För hantering av överlastsituationer i kundnätet ska prioritering användas.

I normalfallet rekommenderas att använda autonegotiation (AN) för att uppnå (minst) 100 Mb/s samt full duplex. Resultatet kan variera beroende på typ av utrustning och **måste alltid verifieras**.

Om fast konfigurering av något skäl måste användas så sätts AN ur spel, och därför måste även den andra utrustningen konfigureras likadant för att undvika exempelvis duplexfel som leder till kommunikationsstörningar.

Reservation: 10 Mbit/s access till PC med softphone kan anses tillräckligt endast vid normal kontorsanvändning av PC:n (under pågående samtal). Youtube, webb-tv, kvällstidningswebb med mycket reklam etc. kan påverka samtalet negativt.

## 2.2.2 Inom LAN:et

Det är vanskligt att ge rekommendationer för vilken LAN-kapacitet som behövs, detta beror på vilken övrig trafik som körs, på trafikmönster, och naturligtvis på nätets storlek. Det finns ett antal principer och "Best Practice" för hur nät dimensioneras, och de ska givetvis följas.

Några tumregler kan dock nämnas:

Andelen realtidstrafik (IP-telefoni plus eventuella andra realtidsapplikationer) bör inte överstiga 25-30% i nätet, samtidigt som länkarna inte bör lastas till totalt mer än 50% i medellast och 70% intermittent.

Ett modernt switchat nät med 10/100 Mbit/s eller 1 Gbit/s access till PC eller telefon samt 1 Gbit/s mellan switcharna kan betecknas som "tillräckligt kraftfullt" och bör klara voicetrafiken även utan prioritering i nätet. Men eftersom switchar i den klassen oftast stöder prioritering enligt 802.1p bör funktionen aktiveras.

100 Mbit/s mellan switcharna bör också fungera väl i de fall man i övrigt kör normal kontorstrafik understigande c:a 50% last, annars är prioritering mer eller mindre ett ska-krav.

Om man kör mycket "batch"-körningar (backuptagningar, databasuppdateringar etc) eller mycket videotrafik på länkar som bär telefoni är det risk för större variationer i fördröjningen. I dessa fall är det rekommenderat att använda prioritering, eller att sektionera nätet så att man inte blandar trafiken.

Uppgradering till 1 Gbit/s bör klara också de flesta fall, även utan prioritering. Återigen brukar dock Gigabit-switchar stödja prioritering, varför det rekommenderas att slå på denna funktion.

- Flow Control ska inte vara aktiverat på interface som hanterar IP-telefoni. För hantering av överlastsituationer i kundnätet ska prioritering användas.

## 2.2.3 Interface mot DataNet

Dimensionering av länk mot DataNet ska ta hänsyn till den totala trafikmängden, till mängden telefonitrafik, och till totala mängden prioriterad realtidstrafik över interfacet. Realtidsklassen i DataNet har en gräns på 25% realtidstrafik, som alltså måste rymma både telefoni och eventuell annan realtidstrafik (t.ex. video-konferenser).

Interface för anslutning till DataNet-CPE är i normalfallet Fast Ethernet (100 Mbit/s), men 1 Gbit/s finns som tillval.

- Interface mot DataNet ska i normalfallet vara konfigurerat för Autonegotiation. Det måste verifieras att utrustningen verkligen kör full duplex.

# TELIA CENTREX

- Flow Control ska inte vara aktiverat på interface som hanterar IP-telefoni. För hantering av överlastsituationer i kundnätet ska prioritering användas.

## 2.3 DHCP

Generellt stöder Centrex IP både DHCP och manuell konfiguration av IP-adress, DNS etc. i klienterna.

Om IP-telefoner från Aastra används är DHCP ett krav. Orsaken är att automatisk konfiguration har införts för dessa telefoner. Det innebär att telefonen kontaktar en extern server "rcs.aastra.com" på port 443 (HTTPS) efter att ha fått IP-adress via DHCP. Det finns planer på att införa detta även för telefoner från SNOM.

## 2.4 DNS och adressering

Adresseringen i Centrex IP är DNS-baserad, på så sätt att adresser till telefoniserver och gateway anges i telefoniklienterna med en URL (ipac.telia.com). Detta förfarande kräver tillgång till en DNS-server, för att korrekta IP-adresser ska kunna förmedlas till telefoniklienterna. Alternativet att manuellt ange serverns IP-adress i klienten är möjligt, men då förloras möjligheten att nå en alternativ server vid fel på den primära.

Likaså måste kundnät med Aastratelefoner kunna slå upp " rcs.aastra.com".

Eftersom tjänsten DataNet i grunden är en VPN-tjänst mellan olika kundadresser ingår inte DNS som standard. Kunden måste därför se till att det/de nätsegment som ansluter telefoniklienter har tillgång till en DNS-server, och att DNS-trafiken inte är spärrad till och från det/de nätsegment som ansluter telefoniklienterna.

Om kunden valt Internetaccess som tillvalstjänst till DataNet ingår normalt DNS.

Om kunden väljer att isolera telefoninätet från Internetaccess kan i stället någon form av spegling till lokal DNS-server användas.

## 2.5 Routing

Internt i lan:et måste kunden ange route till Centrex IP-plattformens adresser via CPE:ns interface. Route kan vara statisk (vanligast) eller via routingprotokoll mellan kundutrustning och CPE (särskild option i DataNet).

Route till följande publika host-adresser ska konfigureras i kundens utrustning:

212.181.217.2	212.181.197.129	212.181.196.129
	212.181.197.130	212.181.196.130
	212.181.197.131	212.181.196.131
	212.181.197.132	212.181.196.132
	212.181.197.133	212.181.196.133
	212.181.197.134	212.181.196.134
	212.181.197.135	212.181.196.135
	212.181.197.136	212.181.196.136

Kunden kan valfritt aggregera adresserna eller ange dem host för host.

Den mjukvaruklient (softphone) som erbjuds i Centrex IP kan inte märka paketen med VLAN-tag och således inte separera tal- och datatrafik till olika VLAN. I stället måste separering göras av någon router i kundens nät.

Kund får inte annonsera ut route till Centrex IP-plattformens anropsadresser på Internet.

För kundnät med Aastratelefoner måste "rcs.aastra.com" på Internet vara nåbart.

## 2.6 Brandvägg, proxy och NAT

Telia Centrex ger inte specifika rekommendationer gällande val av brandvägg. Om brandvägg används i anslutningen mot Telia måste några villkor uppfyllas för att funktionen ska garanteras. Ett alternativ till brandvägg är att använda filtrerande router, dvs. att konfigurera accesslistor i kundens router i stället för i separat brandvägg.

Kund kan använda brandvägg och/eller NAT i anslutningen mot Centrex IP-plattformens tjänst under följande förutsättningar:

- Om brandväggen är baserad på servermjukvara ska den köras på en server som har goda realtidsprestanda.
- Brandvägg eller router i kundanslutning mot Centrex IP SKALL INTE utföra PAT.
- Brandvägg eller router i kundanslutning SKALL INTE utföra NAT om inte FULL funktionalitet kan garanteras. I detta begrepp ingår att samtliga SIP-meddelanden SKALL var fullständigt NAT:ade även i payload.
- Brandvägg i kundanslutning SKALL vara kompatibel med SIP version 2.0. Beakta särskilt stödet för option "rel100" som är kritiskt för flera Centrex-funktioner.

Om brandvägg inte är fullt kompatibel SKALL manuell konfigurering kunna göras. Detta rekommenderas också om osäkerhet råder om SIP-stödet, eller som teståtgärd vid felsökning. Följande gäller:

- Brandvägg SKALL INTE göra dynamisk portöppning för talströmmar med hjälp av funktioner som "SIP aware", "SIP ALG" eller liknande, såvida inte FULLT stöd kan garanteras. I stället skall manuell öppning göras. Observera att olika fabrikat av telefonklienter använder olika portspann.
- Brandväggsöppning SKALL göras för följande adresser och portar.

### **Inkommande trafik mot kundnät**

- SIP-signalering

Source address 212.181.197.128/28 source port TCP 5060 (SIP)  
Source address 212.181.197.128/28 source port UDP 5060 (SIP)

Source address 212.181.196.128/28 source port TCP 5060 (SIP)  
Source address 212.181.196.128/28 source port UDP 5060 (SIP)

- Talströmmar

Source address 212.181.197.128/28 dest port range UDP 3000 till 3005 (Aastra)

# TELIA CENTREX

Source address 212.181.197.128/28 dest port range UDP 4000 till 4011 (Telia Centrex Softphone, SNOM)

Source address 212.181.197.128/28 dest port range UDP 16384 till 32767 (Ascom IP-DECT)

Source address 212.181.196.128/28 dest port range UDP 3000 till 3005 (Aastra)

Source address 212.181.196.128/28 dest port range UDP 4000 till 4011 (Telia Centrex Softphone, SNOM)

Source address 212.181.196.128/28 dest port range UDP 16384 till 32767 (Ascom IP-DECT)

- Svar på HTTP- och HTTPS-sessioner från kundens administratör.

Source address 212.181.217.2/32

## Utgående från kundnät (om kundens brandvägg filtrerar denna)

- SIP-signalering

Dest address 212.181.197.128/28 dest port TCP 5060 (SIP)

Dest address 212.181.197.128/28 dest port UDP 5060 (SIP)

Dest address 212.181.196.128/28 dest port TCP 5060 (SIP)

Dest address 212.181.196.128/28 dest port UDP 5060 (SIP)

- Talströmmar

Dest address 212.181.197.128/28 source port range UDP 3000 till 3005 (Aastra)

Dest address 212.181.197.128/28 source port range UDP 4000 till 4011 (Telia Centrex Softphone, SNOM)

Dest address 212.181.197.128/28 source port range UDP 16384 till 32767 (Ascom IP-DECT)

Dest address 212.181.196.128/28 source port range UDP 3000 till 3005 (Aastra)

Dest address 212.181.196.128/28 source port range UDP 4000 till 4011 (Telia Centrex Softphone, SNOM)

Dest address 212.181.196.128/28 source port range UDP 16384 till 32767 (Ascom IP-DECT)

- HTTP och HTTPS från kundens administratör

Dest address 212.181.217.2 HTTP och HTTPS

NAT och Proxyservrar medför i regel olika typer av problem i kommunikationen.

- NAT:ande router i kundanslutning SKALL vara fullt kompatibel med SIP version 2.0. Detta innebär att samtliga SIP-meddelanden skall stödjas av routern.
- Kunden SKALL INTE använda sig av PAT (Port Address Translation) mot Centrex IP-plattformen.
- Proxy SKALL INTE användas för telefonitrafik till och från Centrex IP.

Med "SIP" avses i texten även eventuella övriga protokoll som kan användas av SIP (exempelvis SDP).

TSS har rätt att med tre månaders varsel byta IP-telefoniprotokoll eller uppgradera sådant protokoll till högre version.



Aastratelefoner hämtar en baskonfiguration från leverantören vid installation. Detta medför att:

- Brandvägg mot Internet i kundnät med Aastratelefoner måste tillåta utgående HTTPS (port 443) mot "rcs.aastra.com" i anslutningen mot Internet.

## 2.7 Spårbarhet

- Om kunden använder egen DHCP ska klientens IP-adress vara låst till klientens MAC-adress så länge en användare är inloggad. Efter utloggning tillåts byte av IP-adress på den fysiska terminalen.
- Observera att när Softphone används måste klienten loggas ur och stängas innan PC:n tillåts byta IP-adress. I annat fall kommer softphonen att använda den gamla adressen i kommunikation med Centrex IP:s serverplattform. Ett vanligt feltillfälle är när en bärbar maskin tas ur dockan och får en ny IP-adress via WiFi/WLAN.
- Tidigare krav på tidssynkronisering som bas för autenticeringshash utgår, pga. att annan metod används. Det är dock fortfarande en **rekommendation** att kunden tidssynkroniserar nätelement och klienter mot UTC, bl.a. för att det underlättar felsökning. En lämplig NTP-server är tick.telia.net.

## 2.8 QoS

I normalfallet bör kundens utrustning CoS-märka trafik baserat antingen på applikation, på fysisk port, på VLAN eller på destinationsadress. Centrex IP-plattformens trafik har en entydig destination från klienterna, vilket talar för destinationsbaserad märkning.

En metod är att märka trafik i de switchportar som ansluter IP-telefoner. Enklare spridningsswitchar klarar dock inte detta, eller kan inte klassa trafik baserat på applikation. I dessa fall kan all trafik, inte bara IP-telefonin, från en PC med softphone komma att klassas som realtidstrafik.

Applikationsbaserad eller VLAN-baserad märkning kan ofta utföras av kundens router (beroende på fabrikat och modell).

Många hårdvarutelefoner kan märka trafiken korrekt. För information hänvisas till respektive tillverkare. Av de telefoner Telia erbjuder stöds märkning av bl.a. Aastra och SNOM.

För detaljkrav på interface mellan CPE och kundutrustning gäller de generella reglerna för DataNet-anslutning. Oavsett detta regelverk krävs alltid full duplex i anslutningen eftersom den hanterar realtidstrafik.

### 2.8.1 Krav

- Terminalen ska vara ansluten till ett switchat lan.
- Fördröjning mellan terminal och anslutningspunkt till IP-access ska understiga 20 ms.
- Jitter ska understiga 10 ms.
- Paketförluster i nätet ska vara låga.

Kommentar: Det finns inget exakt tröskelvärde för paketförluster. Successivt ökande förluster ger successivt sämre ljudkvalitet. Om så stora förluster uppstår att talkvaliteten blir besvärande dålig, finns det troligen problem i nätet som skapar ännu större problem för andra applikationer, och som kräver omedelbar åtgärd.

## 2.8.2 Problemscenarion och åtgärder

### Prioritering

- Om terminaler delar lan med annan trafik ska prioritering för IP-telefonitrafik tillämpas. Telefoner i Centrex IP använder p-värde 5 enligt 802.1, och trafik från Centrex IP mot klient är märkt med p-värde 5 samt IP ToS 5 (motsvarande DSCP 40).

### Ip-telefoner

Ip-telefoner på marknaden erbjuder olika metoder för QoS-märkning av signalering och talströmmar, både på nivå 2 och nivå 3. Datapaketen med denna märkning måste passera oförändrade (transparent) genom ert nätverk eller åtminstone överlämnas till Telias nät oförändrade.

- De ip-telefoner som rekommenderas av Telia märker i regel trafiken med s.k. p-tag i Ethernetheadern (defaultvärdet är 5). Detta innebär att även switchar med enklare typ av QoS-stöd (t.ex. att endast två trafikklasser hanteras) kan ge prioritering för telefonitrafiken på ett blandat lan. Ett undantag är Linksys som saknar vlan-stöd och därmed också stöd för p-tag.
- Stöd för Diffserv/ToS kan förekomma. Se nedanstående tabell.

Klient	VLAN-tag	ToS/Precedence	DSCP	L2 prio (p-tag)	PC-uttag
Aastra 6755i	X	x	x	x	x
SNOM 320	X	-	-	x	x
Linksys ATA	-	x	x	-	-
Cisco 122 2 ATA Ersätter Linksys	X	-	-	x	-

- Rekommenderad lösning är dock att så långt möjligt använda separat lan för telefonin.

### Softphone

Den mjukvaruklient som erbjuds i Centrex IP kan inte märka paketen på något av sätten. Detta får konsekvenser för QoS.

- För användning av softphone gäller att PC:n bör anslutas till en switch som kan klassa och märka trafik utifrån UDP/TCP-port eller destinationsadress, eller att hög bandbredd används konsekvent i nätet fram till Telias router (Gigabit Ethernet rekommenderas för lägsta möjliga fördröjningar).
- Nätsegment som bär taltrafik (exempelvis en kundtjänst) bör separeras från nätsegment där tyngre applikationer körs.

## Wifi

Trådlöst lan (wifi, wlan) kan fungera bra om det sätts upp och konfigureras genomtänkt, men det finns ingen garanti för detta. Det finns flera områden där problem kan uppstå:

- Ett wlan utgör en s.k. kollisionsdomän där samtliga klienter delar befintlig bandbredd. Därför kan fördröjningarna bli stora, framför allt när lasten går över c:a 30%.
- Angränsande wlan-nät eller nätsegment kan använda samma eller angränsande radiokanal vilket medför att tillgänglig kapacitet delas eller att trafiken störs ut.
- Stödet för QoS varierar mellan olika WiFi-utrustningar.

## 2.9 Adressscanning

- Kund får inte använda någon typ av adressscanning, pingsserver eller dylikt mot anropsadresserna hos Centrex IP.
- Att tänka på: Om kunden exempelvis NAT:ar externa adresser till interna, och scannar interna LAN, måste adresserna mot Centrex IP undantas.

## 2.10 Krav vid Internetanslutet LAN

- I de fall kunden har egen Internataccess måste kunden tillse att fungerande brandvägg finns. Angrepp mot telefoner och mjukvaruklienter, belastningsattacker etc. kan i hög grad påverka prestanda för telefonitrafiken, eller orsaka totalt avbrott i tjänsten.

Om Telia tillhandahåller Internet med hostad brandvägg via DataNet-tjänsten bortfaller ovanstående krav.

- Kund får inte annonsera ut route till Centrex IP-plattformens anropsadresser på Internet.
- Kund måste spärra inkommande trafik från Internet mot Centrex IP-plattformens anropsadresser.

## 2.11 WAN-tjänst från annan leverantör än Telia

Om kunden använder annan leverantör av wan-tjänst än Telia, och Telia ansluter med DataNet mot en enda kopplingspunkt i kundens nät, gäller i princip samma krav som på kundens lan med avseende på säkerhet, spårbarhet, brandväggar, QoS-parametrar mm, dvs. wan:et betraktas från Telias synvinkel som en del av kundens nätlösning.

Man bör tänka på att telefonitrafiken i en sådan lösning får göra ett extra hopp, jämfört med ett fullmaskat DataNet, vilket leder till ytterligare fördröjning. I princip ska man då räkna in detta extra hopp (över det "främmande" wan:et) i fördröjningsbudgeten för lan:et, men en ytterligare fördröjning på upp till c:a 10 ms per riktning bör kunna accepteras i de flesta fall.