

Krav på kundens LAN och gränssnitt ProLane

Bilaga till offert/avtal

Det här dokumentet innehåller konfidentiell information som berör kunden och Telia och får inte föras vidare till tredje part.

1. Byggsätt för kund-LAN.....	2
1.1 Nätarkitektur.....	2
1.1.1 Telefoni i separat nät	2
1.1.2 Telefoni och data i gemensamt LAN.....	2
1.2 QoS.....	3
2. Gränssnitt mot ProLane	3
2.1 Anslutning och gränssnitt vid olika byggsätt i kundens LAN	3
2.1.1 All trafik på ett gemensamt LAN	3
2.1.2 Separat VLAN för telefoni	4
2.1.3 Separat VLAN för telefoner, men dessutom softphones på PC utan VLAN-stöd	4
3. Krav på kundens LAN.....	4
3.1 Passiv infrastruktur (kabelsystem)	4
3.2 Hastighet och Duplex.....	4
3.2.1 Inom LAN:et.....	5
3.2.2 Interface mot ProLane	5
3.3 DHCP.....	5
3.4 DNS och adressering.....	6
3.5 Routing.....	6
3.6 Brandvägg, proxy och NAT	6
3.7 Spårbarhet	7
3.8 QoS.....	7
3.9 ICMP.....	7
3.10 Krav vid Internetanslutet LAN	8
4. WAN-tjänst från annan leverantör än Telia	8

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 skall vara baserad på switch-teknologi med full duplex. I annat fall kan inte talkvaliteten garanteras.

Beroende på om kund använder befintlig nätverksutrustning (gemensam med datatrafiken) eller separat switch/separat nät för att sprida telefoni ställs olika krav på nätverksutrustningen.

1.1 Nätarkitektur

1.1.1 Telefoni i separat nät

1.1.1.1 Beskrivning

Kund ansluter fristående switch eller switchnät mot Telias utrustning. Ingen fysisk koppling finns mellan IP-telefoni och övrig LAN-trafik.

Fördelar med denna variant är att:

- Inga särskilda krav behöver ställas på switch-utrustningen,
- 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.

Nackdelar

- Användning av mjukvaruklient (softphone) i PC blir mer komplex (skilda VLAN i PC:n, eller behov av en router för att särskilja IP-telefonitrafiken).
- Parallella nät medför högre kostnad

1.1.1.2 Krav

Krav på switchen eller switchnätet kan i detta scenario sättas lägre. Det är tillräckligt med switchat Ethernet 10 Mb/s (mot klient) eller 100 Mb/s utan stöd för 802.1Q (VLAN-tagging) eller 802.1p (VLAN-prioritering).

1.1.2 Telefoni och data i gemensamt LAN

1.1.2.1 Beskrivning

Kund ansluter Telias utrustning mot befintligt LAN.

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.

1.1.2.2 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 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 annan metod är att märka trafik i de switchportar som ansluter IP-telefoner. Enklare spridnings-switchar klarar dock inte detta, dessutom kommer all trafik, inte bara IP-telefonin, från PC med softphone 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 ProLane-anslutning. Oavsett detta regelverk krävs alltid full duplex i anslutningen eftersom den hanterar realtidstrafik.

2. Gränssnitt mot ProLane

Accessen utgörs av en Internetaccess av typ ProLane, med CPE-router. CPE tunnlar VPN:et mot Centrex IP-plattform med GRE-teknik över Internetanslutningen. Observera att Internetanslutningen används som bärare av VPN-tunneln, inte som trafikväg för telefonin.

Kundens router eller nätlösning måste ha skilda interface mot ProLane-CPE för VPN och Internet. Ett interface kan i detta fall vara antingen egen fysisk port alternativt skilda VLAN eller subinterface. Denna åtskillnad krävs eftersom VPN-interfacet logiskt ligger inne på LAN:et (innanför brandväggen eller i DMZ) medan Internetinterfacet är "osäker zon".

2.1 Anslutning och gränssnitt vid olika byggsätt i kundens LAN

Det finns olika sätt för kunden att hantera IP-telefoni på ett LAN, 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 ProLanes CPE.

I samtliga nedanstående alternativ förutsätts att kundens Internetanslutning sker separat via brandvägg.

Anslutning vid olika LAN-alternativ:

2.1.1 All trafik på ett gemensamt LAN

Detta är oftast den enklaste lösningen för kunden, men man får ingen logisk eller adressmässig separering.

Anslutningssätt

Trafiken mot Internet måste särskiljas i kundens utrustning (router krävs). Telefonitrafiken överlämnas till VPN-interface på ProLane-CPE. Detta interface kan vara en separat fysisk port (standard Ethernet-interface) eller ett separat VLAN på gemensam fysisk port (VLAN-trunk används i anslutningen).

2.1.2 Separat VLAN för telefoni

Kan vara fallet om kunden har IP-telefoner på ett lite större nät och vill ha logisk separering av adressrymder, eller av säkerhetsskäl mm.

Anslutningssätt

VLAN:et överlämnas från exempelvis switchport till CPE:ns VPN-interface. Vanlig otaggad anslutning om VPN-interface är fysisk port, taggat interface (VLAN-trunk) om VLAN-gränssnitt används.

2.1.3 Separat VLAN för telefoner, men dessutom softphones på PC utan VLAN-stöd

Detta fall är mer komplext eftersom PC ofta inte konfigureras med VLAN-stöd, alternativt saknar stöd för detta. Trafiken från softphones är alltså blandad med datatrafik medan telefoner i övrigt använder separat VLAN.

Anslutningssätt

Separering mellan softphone- och datatrafik från en PC till olika interface eller VLAN mot CPE görs i kundnätet. Kunden kan routa softphonetrafik till ett särskilt VLAN eller VLAN gemensamt med IP-telefoner, och överlämna trafiken till VPN-interfacet.

3. Krav på kundens LAN

3.1 Passiv infrastruktur (kabelsystem)

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

Kabelsystemet skall minst uppfylla kraven enligt SSEN50173 klass D.

3.2 Hastighet och Duplex

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

- Hastighet BÖR vara minst 100 Mb/s.
- Hastighet SKALL vara minst 10 Mb/s.
- Full Duplex SKALL vara säkerställt.
- Flow Control SKALL ICKE vara aktiverat på interface som hanterar IP-telefoni. För hantering av överlastsituationer i kundnätet SKALL 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.

3.2.1 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 SKALL-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 SKALL ICKE vara aktiverat på interface som hanterar IP-telefoni. För hantering av överlastsituationer i kundnätet SKALL prioritering användas.

3.2.2 Interface mot ProLane

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

Interface för anslutning till ProLane-CPE är i normalfallet Fast Ethernet (100 Mbit/s).

- Interface mot ProLane SKALL I NORMALFALLET vara konfigurerat för Auto-negotiation. Det måste verifieras att utrustningen verkligen kör full duplex.
- Flow Control SKALL ICKE vara aktiverat på interface som hanterar IP-telefoni. För hantering av överlastsituationer i kundnätet SKALL prioritering användas.

3.3 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.

3.4 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 ProLane i grunden är en Internetaccess ingår tillgång till DNS, men kunden måste se till att DNS-trafiken inte är spärrad till och från det/de nätsegment som ansluter telefoniklienterna.

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

3.5 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 ProLane).

Route till följande publika host-adresser skall 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.

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.

3.6 Brandvägg, proxy och NAT

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

- Brandvägg i kundanslutning SKALL vara kompatibel med SIP version 2.0
- Proxy i kundanslutning SKALL vara kompatibel med SIP version 2.0
- NAT i kundanslutning SKALL vara kompatibel med SIP version 2.0
- Kunden BÖR ICKE använda sig av PAT (Port Address Translation) mot Centrex IP-plattformen. Telia garanterar inte full funktionalitet om PAT används.

Med "SIP" avses i texten även eventuella övriga berörda protokoll.

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

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

3.7 Spårbarhet

- Om kunden använder egen DHCP SKALL 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.
- 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.

3.8 QoS

- Terminalen SKALL vara ansluten till ett switchat LAN.
- Fördröjning mellan terminal och anslutningspunkt till IP-access SKALL understiga 20 ms.
- Jitter SKALL understiga 10 ms.
- Paketförluster i nätet skall 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.

- Om terminaler delar LAN med annan trafik SKALL 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).
- Softphoneklienten kan för närvarande inte sätta prioritet. Därför rekommenderas att portar i kundens nätswitchar, som ansluter PC med installerad softphone, klassar och märker trafiken.

3.9 ICMP

- Om kund använder någon typ av pingserver för adressscanning på LAN:et SKALL anropsadresser till Centrex IP plattformen undantas.

Kommentar: Centrex IP plattformen använder publika adresser för anrop, och normalt finns ingen anledning att "pingscanna" publika adresser, men om kunden exempelvis använder interna adresser för destinationer på utsidan, och NAT:ar utgående trafik, skulle pingscanning kunna nå Centrex IP-plattformen.

3.10 Krav vid Internetanslutet LAN

Följande krav tillkommer för Internetanslutna LAN:

- Kunden måste tillse att fungerande brandvägg finns. Angrepp mot telefoner och mjukvaruklienter, belastningsattacker etc. kan i hög grad påverka prestanda för telefontrafiken, eller orsaka totalt avbrott i tjänsten.
- 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.

4. WAN-tjänst från annan leverantör än Telia

Om kunden använder annan leverantör av WAN-tjänst än Telia, och Telia ansluter med ProLane 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 telefontrafiken i en sådan lösning får göra ett extra hopp, jämfört med att använda exempelvis ett fullmaskat DataNet-VPN, 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.