Spark

IP CENTRIX

Increase collaboration with a cloud-based, flexible and cost efficient alternative to maintaining an on-site PBX.

TABLE OF CONTENTS

1 INTRODUCTION

1.1 PURPOSE OF THIS DOCUMENT

This document provides an overview and in-depth technical recommendations on customer IT environment to support IP Centrex deployed Over The Top (OTT) or Integrated Customer Lan (ICL).

1.2 GLOSSARY OF TERMS

Term	Description
DMS	Device Management Service (Broadsoft's automated Device Configuration service, hosted on Broadworks)
ICL	Integrated Customer LAN. (Refers to local connectivity for IPC devices, which previously were on a dedicated LAN).
IPC	IP Centrex (Product name for IP Centrex service hosted on BroadWorks)
OTT	"Over the top" (Refers to the network access type which was previously limited to managed (dedicated and guaranteed) access).
LAN	Local Area Network, a computer network that interconnect IT devices in a limited area, e.g., office building
MSSA	Multiple Service Single Access. An example of MSSA is WAN and IP Centrex services connected to the customer site via a single fibre access using a separate VLAN (virtual LAN) for each service.
PC	Personal Computer

2 OVERVIEW

There are three deployment options for IP Centrex fixed service: managed access with dedicated LAN, managed access with Integrated Customer LAN (ICL), and Over The Top (OTT).

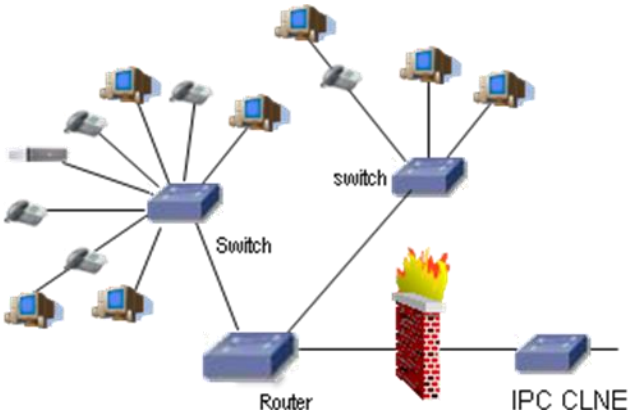
With ICL, the service demarcation point is IP Centrex CLNE. Customers are responsible for their environment configuration and maintenance between the IP Centrex devices and the CLNE.

OTT deployment does not require a Spark CLNE, therefore the IP Centrex phones can be connected directly to the broadband interface or via the customer switching gear.

IP Centrex devices for OTT and ICL options will be delivered to the nominated by the customer site pre-configured and can be connected to the customer LAN together with other network devices. Customer will have an option to self-install the Spark provided IP Phones. If for some reason, Spark assistance on site is required, the customers may request Spark install through a change request (additional fees apply).

This document provides instructions and recommendations for the customer LAN set up, when customer chose ICL or OTT deployment methods for IP Centrex fixed service.

The diagram below illustrates an example of possible network topologies for IPC with ICL in the customer's mixed environment with multiple subnets, IP Phones that provide Ethernet connectivity to desktop PC's and other network devises.



2.1 CUSTOMER LAN CONNECTION

2.1.1 MANAGED ACCESS CONNECTIVITY

The demarcation point of the IP Centrex service delivered over the managed access with ICL is the customer facing LAN port of the IP Centrex CLNE.

The CLNE by default is configured to meet a simple topology where all IPC VoIP devices are configured on a single subnet to which the CLNE IP Centrex customer LAN port is connected.

When the CLNE is configured to operate in an MSSA environment (with WAN or Managed Internet services) , a static default route may be configured pointing to a next-hop in the customer network.

The base configuration of the IP Centrex CLNE has the following two routes available:

- 10.0.0.0/8
- 192.168.0.0/16

If the customer must have support for subnets that belong to the 172.16.0.0/12 range or use public IP subnets then these will need to be provided to Spark in addition to the next-hop address above, so the CLNE can be configured accordingly.

2.1.2 OTT CONNECTIVITY

When IP Centrex is delivered OTT, an IP Centrex CLNE is not provided, therefore the IP Phones should be connected to the Broadband modem directly or via customer LAN.

3 CUSTOMER NETWORK SET UP FOR IP CENTREX DEVICES.

3.1 CABLING

Cabling standards require that all eight conductors in Cat5/5e/6 cable are connected, resisting the temptation to 'double-up' or use one cable for both voice and data. IP phone systems, however, can run the telephone and the computer on the same wires as each phone is a small switch.
New Zealand has the TCF 'Premises Wiring code of Practise' which although aimed at the residential and SOHO segments has a number of good points that are applicable to larger commercial premises:
http://www.tcf.org.nz/content/dc07abcd-21f8-4288-b55b-6f861bdd4d02.html

Also, customers can refer to the Telecommunications Industry Association (TIA) standards

- ANSI/TIA-568-C.0, Generic Telecommunications Cabling for Customer Premises, 2009
- ANSI/TIA-568-C.1, Commercial Building Telecommunications Cabling Standard, 2009

3.2 ADDRESSING

In general, DHCP clients should verify that the address in a DHCP offer is not already in use (e.g. using IPv4 Address Conflict Detection as described in RFC 5227). However, testing with Cisco IP phones (SPA504G and SPA525G2) has indicated that while the phones perform address conflict detection, they do not decline the address in the DHCP offer when a conflict is detected. This creates the potential for duplicate IP addresses on the LAN segment. It is recommended that a policy of not mixing DHCP clients with Static clients is applied in the customer environment which will reduce the risk significantly.

3.3 NAMING

The IPC solution relies on DNS queries for the applications to function.
All IPC phones rely on SRV queries with a subsequent or fall-back to 'A' record queries thus making DNS critical to the success of a call.

DHCP is used to provide the DNS server IP addresses to the IPC phones. Customers can use non-Spark Internet Root derived DNS servers for DNS queries.

Customers that wish to use the Spark DNS services over their Spark access can configure the following IP addresses for DNS in the DHCP scope.

- 122.56.237.1
- 210.55.111.1

To confirm that DNS servers are reachable, use *nslookup*, as the DNS servers do not respond to ICMP ping requests.
An nslookup can be performed from a command or shell prompt of a PC, example below shows an nslookup from a DOS prompt

```
C:\>nslookup spark.co.nz 122.56.237.1
```

```
Server:  ns1.xtra.co.nz
Address:  122.56.237.1

Non-authoritative answer:
Name:    spark.co.nz
Address:  146.171.248.36
```

The 'Server' line says which server was used to provide the results. Receiving an 'Address' for spark.co.nz shows that DNS resolution is working for spark domain from that server, another one can be done for the alternative DNS server to be certain.

It is recommended when configuring any DNS caching servers to be mindful that increasing the TTL time will slow down propagation time and potentially cause outage when a master root server change occurs. It is good practise to honour the TTL as set by the DNS record owner which may be different across record types.

3.4 TIME

NTP services are offered by Spark and are reachable to all Spark accesses that support IPC including the Spark internet accesses.

Alternative connectivity options exist for NTP and it is recommended that the advice offered by the pool.ntp.org project at http://www.pool.ntp.org/en/use.html is followed. E.g. NTP sources in preference order:

1. Utilise Customers own NTP Servers
2. Utilise Service Providers NTP Servers
3. Utilise the local (nz.pool.ntp.org) NTP pool Servers

If the customer chooses to provide the DHCP server then the Spark NTP servers can be connected to over a Spark access on the following IP addresses.

- 122.56.252.129
- 122.56.252.137

The IP Phones provided with IP Centrex will be provisioned with New Zealand Local Time offset and this is the time that will be shown on any display to the user, additional time zones will not be supported.

3.5 DHCP

The following DHCP options are required for the IP Centrex phone to connect Spark Device Management Server and download required device prolife:

- TFTP server name (DHCP option 66)
- HTTP/HTTPS server name (DHCP option 160)

option 66 ASCII "dms.telecom.co.nz"
option 160 ASCII "https://dms-cisco.telecom.co.nz:444/dms/def/$PSN.xml"

DHCP options 66 and 160 have been quoted to ensure that any trailing spaces are ignored by the DHCP server. If not quoted, any trailing spaces will be included in the DHCP reply message which may result in the option being rejected by the IP phone.

If customer already uses DHCP Options (66 & 160) internally, then this would cause complication and perhaps even a show stopper for some customers as the solution is to set-up DHCP Classes. Here is an example for a Cisco 525G2 DHCP specific configuration:

```
option boot-server code 66 = string;
option option-66 code 66 = text;
option option-160 code 160 = string;

        class "cisco525G" {
        match if substring (option vendor-class-identifier,0,14) = "Cisco SPA525G2";
                option option-66 "dms.telecom.co.nz";
                option domain-name-servers 210.55.111.1,122.56.237.1;
                option ntp-servers 122.56.252.129,122.56.252.137;
                option option-160 "https://dms-cisco.telecom.co.nz:444/dms/def/$PSN.xml";
                default-lease-time 43200;
                max-lease-time 86400;
        }


        pool {
                range 192.168.0.30 192.168.0.35;
                allow members of "cisco525G";
                }
```

3.6 ROUTING

The customers will need to ensure that any routers that exist on the path from an IP Centrex device to the IPC CLNE or Spark Proxy are configured to route traffic destined for the following subnets go via the IP Centrex CLNE gateway or via the internet:

Description	Subnet/Mask
Spark SIP Proxy in Auckland (SBC MDR)	122.56.253.0/25
Spark SIP Proxy in Hamilton (SBC HN)	122.56.254.192/27
Spark SIP Proxy in Wellington (SBC WN)	122.56.254.0/25
Spark SIP Proxy in Christchurch (SBC CH)	122.56.255.0/25
Spark SIP Proxy in Auckland (SBC PAK)	122.56.253.224/27
Spark SIP Proxy in Tauranga (SBC TG)	122.56.254.224/27
Spark SIP Proxy in Porirua (SBC PRO)	122.56.254.160/27
Spark SIP Proxy in Riccarton (SBC RIC)	122.56.255.160/27
Spark Device Management System (DMS1)	122.56.65.9/32
Spark Device Management Server System (DMS2)	122.56.65.10/32
Spark Device Management System (DMS3)	125.236.69.249/32

The mandatory routes above will also be provided by a dynamic routing protocol (RIPv2) enabled on the Spark CLNE if managed access is used to announce the ‘mandatory routes’ on the local customer LAN subnet.

The advantage of using a dynamic routing protocol is reduced information passed to the customer and any changes in the network in the future for "Mandatory Routes" can be deployed automatically into production using current CLNE configuration update processes.

The table below has the routes that customers may use for the IP Centrex devices or can choose to use alternative services as described elsewhere in this document.

Description	Subnet/Mask
DNS1	122.56.237.0/24
DNS2	210.55.111.0/24
NTP1	122.56.252.128/29
NTP2	122.56.252.136/29

3.7 COS & QOS

The IPC phones will not be provided with the tools needed to configure them to be on a specific VLAN (802.1Q) or to mark frames with layer 2 CoS (802.1p). The customer can use their own switches to set up VLAN and CoS on the switch ports to which the IP Centrex devices connect.

The pass-through port configuration cannot be changed to meet customers' needs if however it suits the customer to use the port they are free to do so.

The IEEE 802.1p marking for frames that egress the Spark CLNE LAN interface for IP Centrex delivered over a managed access has been set as follows.

- Audio stream – 5
- SIP signalling – 3

As a rule when a choice must be made it is generally better to trust the DSCP marking than the CoS for the Spark VoIP service.

- Audio Stream: EF
- SIP Signalling: CS3 (or AF31 *)

It is recommended that a professional RF audit, site-survey and installation are performed for all wireless LAN installations. When voice traffic is to be passed over the wireless LAN a voice readiness test regime with periodic reassessments should be put in place.

Each IP Centrex profile/user requires 64Kbps to maintain voice quality. Customers need to make sure that their LAN bandwidth is sufficient to support the number or simultaneous calls as required.

3.8 NAT

The IP Centrex service when delivered over a managed access uses a CLNE where NAT is provided by the CLNE so that each IP Centrex phone is represented in the public network as a unique IP & Port signalling combination. All media must also traverse the NAT function on the CLNE.

The IP Centrex service utilises NAT with a 20 minute UDP timeout to optimise the session refresh rate. It is typically for the Ethernet IP Centrex phones to re-register every 15 Minutes.

SIP destination port is the IANA registered one of 5060 for UDP/TCP use. Current TLS is not implemented. The RTP and UDPTL media may use UDP ports 1024-65535 the precise port number is stipulated in the SDP (Session Description Protocols) of the signalling.

Although NAT is used on the IP Centrex CLNE when delivered over a managed access Spark strongly recommends that customers do not use NAT 'fix-up' techniques, such as firewalls with SIP ALG (Application Layer Gateway) prior to SIP leaving their site.

Spark does not support a "Double-NAT' scenario, i.e. using NAT between the CLNE customer LAN port and the IP Centrex phone when delivered over a managed access.

3.9 LAN

Although high speed LAN infrastructure have led to VoIP quality issues being uncommon they are still present and a mistake or error in design or configuration of the customer LAN can cause voice quality deterioration.

Listed below are some general statements on LAN infrastructure design that all help towards maintaining quality voice calls when the customer provides the infrastructure components.

- Use 'Auto' for both speed and duplex negotiation for Spark supplied VoIP devices.
- Check that the IP Centrex device can and does negotiate the maximum speed capable to the switch.
- Check that the IP Centrex device can and does negotiate full duplex.
- Ensure the broadcast layer 2 & 3 traffic as well as multicast traffic levels are kept low as significant levels will cause unnecessary loading of the IP Centrex device.
- If a PC is connected on a IP phone pass-through make sure it is not a bandwidth hungry power user and also that its connection speed is not in excess of the IP Centrex device to switch uplink speed.
- Whenever possible the Spark will mark traffic using the CoS and DSCP markings to indicate the importance of the traffic, customers are advised to prioritise the traffic appropriately.

4 TROUBLESHOOTING

4.1 IP CENTREX WITH ICL AND CUSTOMER PROVIDED DHCP

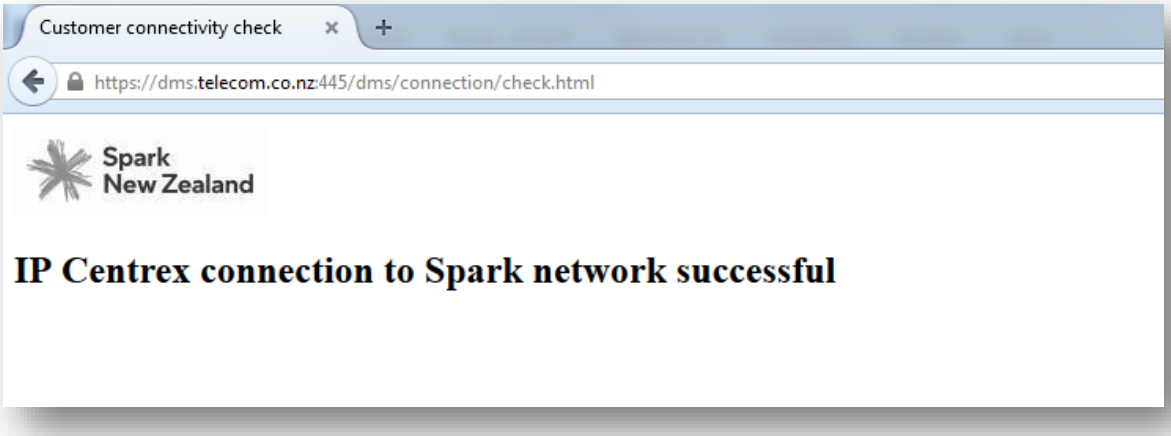
It is critical to configure correctly the name of Spark Device Management System (DMS) address on the customer DHCP server to connect the phone to Spark network. To confirm that DMS servers are reachable use nslookup:

- Check IP@ returned when User performs nslookup dms-cisco.telecom.co.nz in shell
- Check IP@ returned when User performs nslookup dms.telecom.co.nz in shell
- Check IP@ returned when User performs nslookup dms.spark.co.nz in shell

The expected DNS resolution:
dms-cisco.telecom.co.nz 122.56.65.10
dms.telecom.co.nz 122.56.65.9
dms.spark.co.nz 125.236.69.249

The following link provides a connectivity test to Spark IP Voice network:
https://dms.telecom.co.nz:445/dms/connection/check.html

If successful the following screen should appear when you open the link:



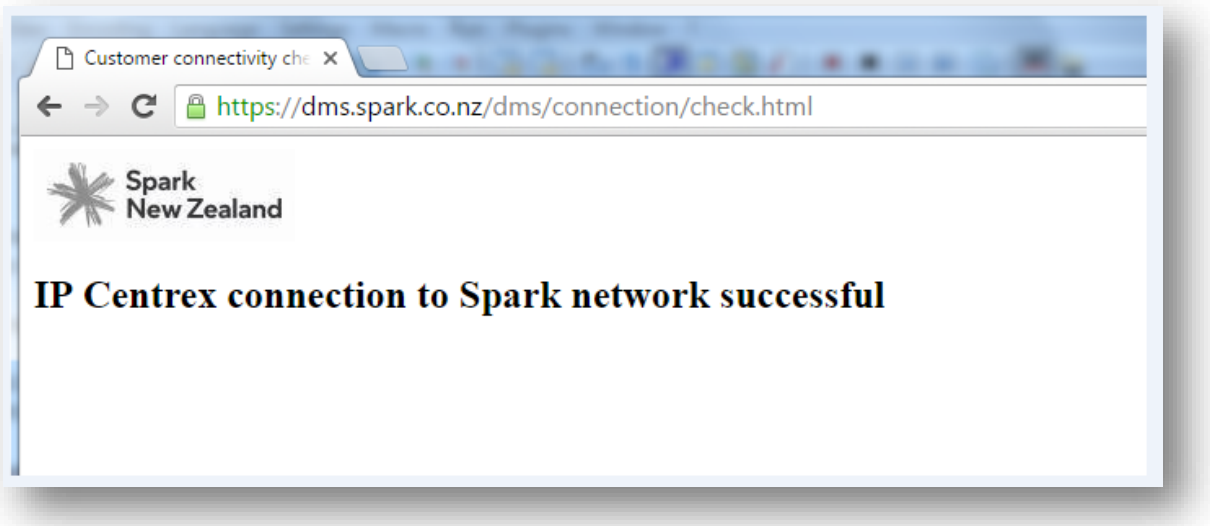
Note: This test is used for a dedicated access connectivity test, the security certificate will not be presented, therefore a security certificate error will pop up. It is safe to continue with to this website, please proceed with the test.

4.2 IP CENTREX OTT. BROADBAND ACCESS TEST.

The following link provides access to the SPARK broadband test tool to measure the performance of a broadband connection: http://www.spark.co.nz/myspark/myinternet/testyourspeed/

The following link provides a connectivity test to Spark IP Voice network:
https://dms/spark.co.nz/dms/connection/check.html

If successful the following screen should appear when you open the link:



4.3 IP CENTREX OTT. LIMITATIONS

4.3.1 SIP ALG

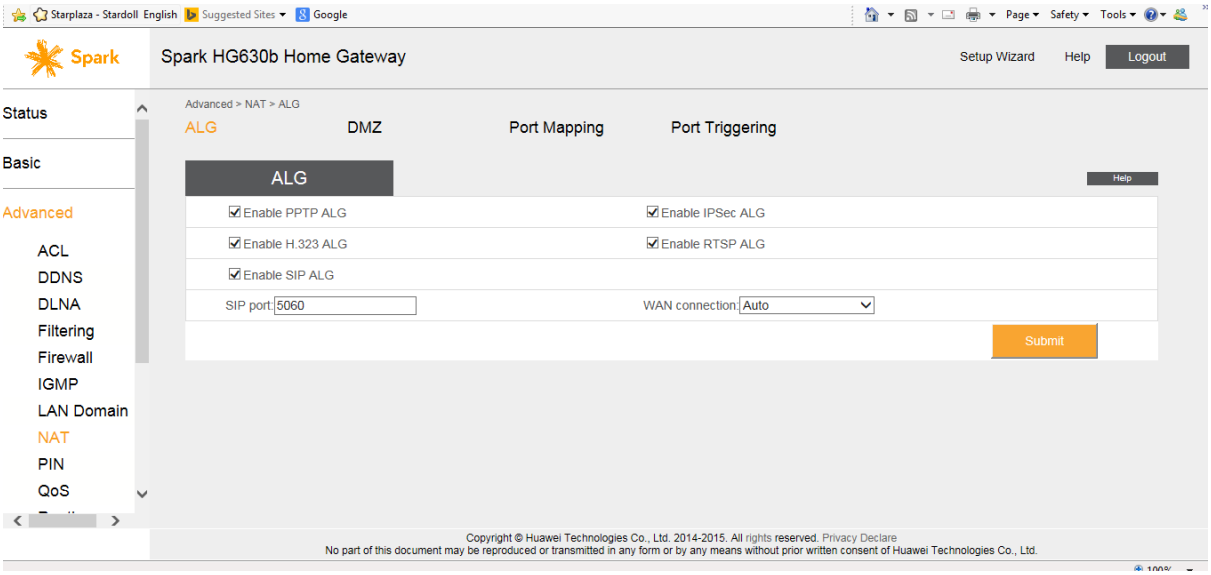
When IP Centrex deployed Over The Top, it is important that SIP ALG is disabled on the Broadband modem. Here is an example how to disable SIP ALG on the Huawei residential gateway:

1. Connect to device via Wi-Fi or USB Data Cable
    - **Note:** If connecting wirelessly you may need to enter the default Service Set Identifier (SSID) and wireless network encryption key. These are printed on the Mobile Wi-Fi label. It is recommended that you log in to the web management page and change your SSID and wireless network encryption key.

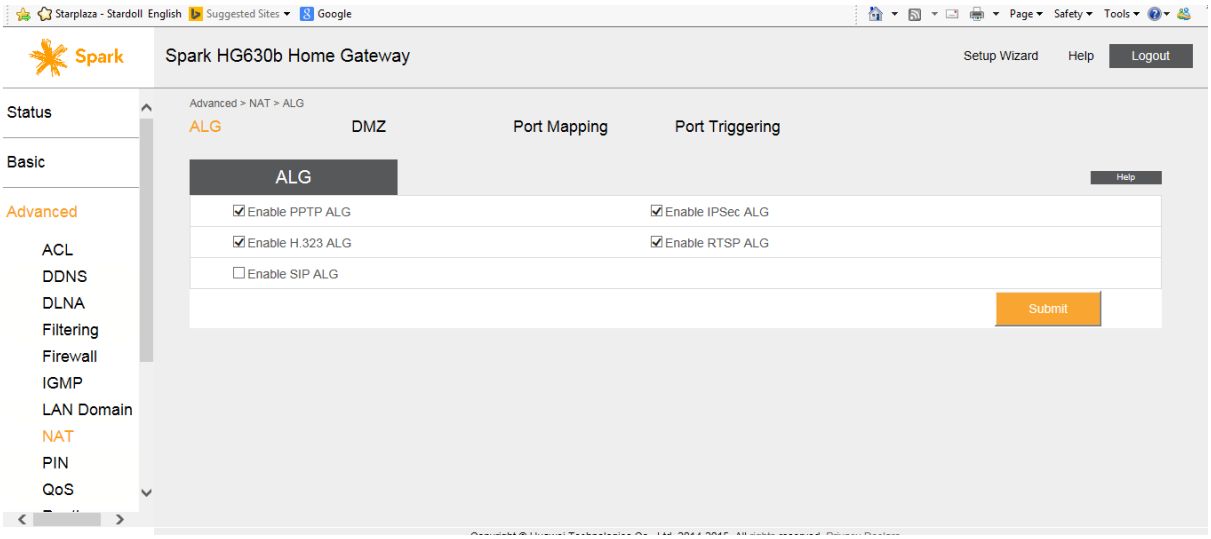
2. Open http://192.168.1.1 in your web browser

3. If you select any of the menu items you will be prompted to login.
    - **Username:** admin
    - **Password:** admin

4. Scroll down in left hand menu to NAT
5. Uncheck “Enable SIP ALG”



6. Click 'Submit'. Will now appear as follows:



4.3.2 THOMSON/TECHNICOLOUR TG585 GATEWAY

One way speech occurs on incoming calls to IPC desk phones when using a Thomson/Technicolour TG585 gateway for OTT access. This issue has not been observed on any of the other gateways tested.