SIP to SS7 Configuration Guide

- Perform the First Boot/Initial Setup
  - Power Connection
    - PSU Connection
    - DC PSU Connection
  - Establishing Initial WebGUI Connection
  - Change Password
  - Console SSH Configuration
  - NSG License
- Network Configuration
  - Network Setup
    - CAUTION:
    - Physical Network Interface Configuration
    - Appliance Network Interfaces
    - Selecting Default Route
    - Network Section
    - Interface Section
      - Network Role
      - Types
      - Ethernet Options
  - Virtual IP’s
  - IP Troubleshooting
  - Static Routes
    - Routing Table Status
  - VLAN
    - VLAN Configuration
    - VLAN Routes
  - Additional VLAN
    - VLAN Status
  - Date & Time Service Config
- Initial Gateway Configuration
  - Global Gateway Configuration
- SS7 ISUP Configuration
  - TDM SS7 Configuration Page
  - Port Identification
  - Edit T1/E1 Config
    - Standard T1/E1 Parameters
    - Advanced T1/E1 Parameters
  - Span Link Type
  - SS7 Network Overview
    - Links
    - Linksets
    - Routes
  - MTP2 Link Configuration
  - MTP3 Linkset Configuration
  - MTP3 SS7 Route
  - ISUP Interface Configuration
  - ISUP CIC Channel Mapping
- Media Transcoding Configuration
  - Media Hardware
- Applying Configuration
- Dialplan
  - Dialplan Reload/Apply
  - PSTN to SIP Dialplan
  - Dialplan Syntax
    - Context
    - Extensions
    - Conditions
    - Multiple Conditions (Logical AND)
    - Multiple Conditions (Logical OR, XOR)
    - Complex Condition/Action Rules
    - Variables
    - Built-In Variables
    - Caller Profile Fields vs. Channel Variables
- Starting the Gateway

Perform the First Boot/Initial Setup
Power Connection

Sangoma NSG comes with three types of power supplies

- **AC PSU**
  - AC Single PSU (Default)
  - AC Dual-Redundant PSU
- **DC PSU**
  - DC Dual-Redundant PSU

### PSU Connection

- Standard 110V or 220V, 50-60Hz connection.
- Optional Dual-Redundant AC 110V or 220V, 50-60Hz connection.
- Optional Dual-Redundant DC -48V

### DC PSU Connection

Connecting cables to a power supply depends on the remote power source.

<table>
<thead>
<tr>
<th>Power Source Type</th>
<th>Black Wire</th>
<th>Red Wire</th>
</tr>
</thead>
<tbody>
<tr>
<td>If power source -48V</td>
<td>-48V</td>
<td>0V (Ground)</td>
</tr>
<tr>
<td>If power source +48V</td>
<td>0V (Ground)</td>
<td>+48V</td>
</tr>
</tbody>
</table>

- The PSU has voltage reverse protection.

If the red and black wires are connected the wrong way, the system will not power up. But there will be no damage to the PSU or the system.

<table>
<thead>
<tr>
<th>VOLTAGE</th>
<th>DC -36V ~ -72V</th>
</tr>
</thead>
<tbody>
<tr>
<td>INPUT CURRENT:</td>
<td>12.0A (RMS), FOR -48 VDC</td>
</tr>
<tr>
<td>INRUSH CURRENT</td>
<td>20A (Max)</td>
</tr>
<tr>
<td>DC OUTPUT</td>
<td>400W (Max)</td>
</tr>
</tbody>
</table>

### Establishing Initial WebGUI Connection

NSG factory settings are not very useful, as the Primary Ethernet port: eth0 is set to a static IP address. Proceed to connect to the NSG Appliance via Laptop’s web browser.

- Connect the Primary Signaling Port: eth0 to a LAN Switch
- Connect Laptop to LAN Switch
- Configure Laptop to IP address: 192.168.168.1/24
- Login via
• Username: root, Password: sangoma

Change Password

After successful Login, please proceed to change the default password. Sangoma NSG appliance comes with default password. For security reasons please change the password.

• Select Password page from side/top System menu
• Enter your new password
• Press update to save
Console SSH Configuration

By default NSG systems come with SSH enabled. To configure ssh service

- Select Services from side/top System Menu
- Enable or disable Secure Shell service

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Samba/Windows NetBIOS</td>
<td>Windows NetBIOS server</td>
<td>Not used / Not required</td>
</tr>
<tr>
<td>Service</td>
<td>Description</td>
<td>Status</td>
</tr>
<tr>
<td>----------------------</td>
<td>------------------------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>MySQL</td>
<td>MySQL database</td>
<td>Not used / Not required</td>
</tr>
<tr>
<td>Samba/Windows Server</td>
<td>Windows File server</td>
<td>Not used / Not required</td>
</tr>
<tr>
<td>Time Server</td>
<td>Network Time Protocol</td>
<td>Should be configured and enabled. Note: There must be internet access to reach the NTP service.</td>
</tr>
<tr>
<td>Web Server</td>
<td>web/httpd server</td>
<td>Not used / Not required</td>
</tr>
<tr>
<td>Gateway Service</td>
<td>NSG VoIP to SS7 gateway</td>
<td>Do not configure it here Use Control Panel</td>
</tr>
<tr>
<td>Logging Services</td>
<td>Syslog, logging service</td>
<td>Should be configured and enabled.</td>
</tr>
<tr>
<td>Samba/Windows Winband</td>
<td>Not used/ Not required</td>
<td></td>
</tr>
<tr>
<td>Secure Shell</td>
<td>SSH server</td>
<td>Should be configured and enabled.</td>
</tr>
<tr>
<td>System Scheduler/Cron</td>
<td>System scheduler</td>
<td>Should be configured and enabled</td>
</tr>
<tr>
<td>System Watch</td>
<td>System watch</td>
<td>Should be configured and enabled</td>
</tr>
</tbody>
</table>

**NSG License**

Each NSG appliance comes with pre-installed license.

In case of upgrades, of expansions please contact Sangoma Sales.

To update NSG license

- Select **License** from side/top **Configuration** Menu
- NSG License from Sangoma Support
- Upload the License into the NSG Gateway via the **Upload** Button The License page offers the detailed license overview.
### License Variables

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Customer Name</td>
</tr>
<tr>
<td>Email</td>
<td>Customer Email</td>
</tr>
<tr>
<td>Reseller</td>
<td>Reseller Name</td>
</tr>
<tr>
<td>License</td>
<td>NA</td>
</tr>
<tr>
<td>SPC</td>
<td>SPC stands for: self point code. It's used to bind a specific set of point codes to the license. ANY: is a special value which allows use of an SPC value.</td>
</tr>
<tr>
<td>MAC</td>
<td>System's MAC address. License code checks the MAC address and confirms if MAC is correct. One can check vs License Information section.</td>
</tr>
<tr>
<td>CICS</td>
<td>Number of TDM channels allowed by the license. From example above CICs = 600. For RTP to TDM calls: License allows 600 calls For TDM to TDM calls: License allows 300 calls</td>
</tr>
</tbody>
</table>

### Network Configuration

Network configuration section only applies to Physical Network Interfaces: eth0 and eth1. It does not apply to VLAN IP and route configuration.

### Network Setup

- Physical network interfaces: eth0, eth1 are configured in the section

Configuration-> Settings-> IP Settings.
This section can only be used to modify/configure IP, Host, DNS information for Physical Network interfaces eth0 and eth1.

Default Route/Gateway

- To configure a system default route through the IP Settings section, the appropriate interface role type to use is “External”. The External interfaces get associated to the default system route.

CAUTION:

- There can only be ONE External network interface.
- There can only be ONE system default route.

Static Routes

- Static routes that apply to physical network interfaces eth0, eth1 should be configured in Configuration-> Network -> IP Route section.

CAUTION:

- Do not try to configure VLAN routes in this section.
- route configuration files are only meant to be used for eth0,eth1 interfaces.

Media Ethernet Interface: Transcoding

- NSG comes with optional, media/codec transcoding hardware. The media transcoding hardware network interface is: eth2. The media transcoding network interface comes preconfigured with a 10.x.x.x ip address.

Configuration of the eth2 device should be performed in Configuration->Settings->Media.

CAUTION:

One should take this into account when assigning IP addresses to eth0,eth1 or VLAN interfaces. Confirm that ip address range set does not conflict with eth2 media transcoding network interface.

VLAN Config IP & Routes

- VLAN’s can be configured in section Configuration-> VLAN
- VLAN can be configured on top of eth0 and eth1 network interface only.
- All VLAN related configuration such as IP address, VLAN ID and VLAN routes must be configured in VLAN configuration section only.

CAUTION:

- Do not use Static IP Route section to create a VLAN routes.
- Static IP Route section is only for physical interfaces eth0 and eth1.

VLAN Default Route

- If a system default route needs to be configured via VLAN interface.
- Configure the system default route in Configuration-> VLAN section.
- Refer to the VLAN section below.

CAUTION:

- Make sure that all physical network interfaces in IP Settings section are configured for role “LAN”. No physical network interface eth0, eth1 should be configured for role “External”. This would result in multiple system default routes.
Physical Network Interface Configuration

By default the NSG appliance pre-configured with 192.168.168.2/24 address on Primary Port (eth0). The IP address can be changed based as follows

- Select IP Settings from side/top Configuration menu
- Specify Firewall Mode and Hostname
- Select Edit under eth0 and eth1 device and configure

NOTE

- eth2 device is a Sangoma Transcoding device and should be modified.
- eth2 device is configured in Configuration -> Media section of the GUI will configure this device

Appliance Network Interfaces

- eth0
  - Primary Signaling Port
  - By default provisioned as static 192.168.168.2
  - By default allows access to ssh and management http
- eth1
  - Secondary Signaling or Management Port
  - By default provisioned as static no IP address
  - By default allows access to ssh and management http
- eth2
  - Sangoma transcoding DSP board
  - Provisioned using Media page. Do not modify in this section.
Selecting Default Route

NSG appliance should have a single default route. The default route is used to access Internet.

To configure a default route on eth0

- Set the eth0 interface mode to **External**.
- Refer to section below.

### Network Section

<table>
<thead>
<tr>
<th>Variable</th>
<th>Input Options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>Standalone – No Firewall</td>
<td>Firewall Disabled</td>
</tr>
</tbody>
</table>
|               | Standalone                     | Firewall Enabled Warning:
|               |                                | All active service ports must be explicitly enabled                         |
| Hostname      | String                         | A hostname is the full name of your system. If you have your own domain, you | |
|               |                                | can use a hostname like **nsg.example.com**. Alternatively, you can also make | |
|               |                                | one up: gateway.lan, mail.lan. The hostname does require at least one period | |
| Name/DNS Servers | Domain Name or IP address eg. 8.8.8.8 | On DHCP and DSL/PPPoE connections, the DNS servers will be configured        |
|               |                                | automatically for your IP Settings. In these two types of connections there | |
|               |                                | is no reason to set your DNS servers. Users with static IP addresses should | |
|               |                                | use the DNS servers provided by your Internet Service Provider (ISP). If you | |
|               |                                | are using Multi-WAN, please review the documentation on the topic of DNS   |
|               |                                | servers.                                                                   |

### Interface Section
Network Role

When configuring a network interface, the first thing you need to consider is the network role in IP Settings. Will this network card be used to connect to the Internet, for a local network, for a network with just server systems? The following network roles in IP Settings are supported in NSG and are described in further detail in the next sections:

- External - network interface with direct or indirect access to the Internet
- LAN - local area network
- Hot LAN - local area network for untrusted systems
- DMZ - de-militarized zone for a public network

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **External** | Network interface with direct or indirect access to the Internet
|          | External interface is used as the system default route. |
|          | **WARNING:** You should have only ONE external network interface. Usually eth0 is the external interface |
| **LAN**  | Connection to your local network Usually eth1 is the LAN interface |
| **Hot LAN** | Hot LAN (or “Hotspot Mode”) allows you to create a separate LAN network for untrusted systems. Typically, a Hot LAN is used for: |
|          | - Servers open to the Internet (web server, mail server) |
|          | - Guest networks |
|          | - Wireless networks |
|          | A Hot LAN is able to access the Internet, but is not able to access any systems on a LAN. As an example, a Hot LAN can be configured in an office meeting room used by non-employees. Users in the meeting room could access the Internet and each other, but not the LAN used by company employees. |
In NSG, a DMZ interface is for managing a block of public Internet IP addresses. If you do not have a block of public IP addresses, then use the Hot LAN role of your IP Settings. A typical DMZ setup looks like:

- **WAN**: An IP addresses for connecting to the Internet
- **LAN**: A private network on 192.168.x.x
- **DMZ**: A block of Internet IPs (e.g. from 216.138.245.17 to 216.138.245.31)

NSG GUI has a DMZ firewall configuration page to manage firewall policies on the DMZ network.

### Types

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DHCP</strong></td>
<td>For most cable and Ethernet networks, DHCP is used to connect to the Internet. In addition, your system will have the DNS servers automatically configured by your ISP when the Automatic DNS Servers checkbox is set.</td>
</tr>
<tr>
<td><strong>Static</strong></td>
<td>If you have a static IP, you will need to set the following parameters:</td>
</tr>
<tr>
<td></td>
<td>- IP</td>
</tr>
<tr>
<td></td>
<td>- Netmask (e.g. 255.255.255.0)</td>
</tr>
<tr>
<td></td>
<td>- Gateway (typically ends in 1 or 254)</td>
</tr>
<tr>
<td></td>
<td>- Ethernet Options (able to force 100MB or 1000mb)</td>
</tr>
<tr>
<td><strong>PPPoE DSL</strong></td>
<td>For PPPoE DSL connections, you will need the username and password provided by your ISP. In addition, your system will have the DNS servers automatically configured by your ISP when the Automatic DNS Servers checkbox is set.</td>
</tr>
</tbody>
</table>

### Ethernet Options

Setting custom Ethernet options such as disabling auto negotiation is done as part of the IP Settings.

- Select **IP Settings** from side/top **Configuration** Menu
Specify **Options** field in order to add special configuration to this interface.

**Options** are any device-specific options supported by ethtool.

In above example the Ethernet device is set for 100Mb with negotiation disabled.

| Options | [ speed 10|100|1000|2500|10000 ] | [ duplex half|full ] |
|---------|----------------|-------------------|
|         | [ port tp|au|bnc|mii|fibre ] | [ autoneg on|off ] |
|         | [ advertise %%x ] | [ phyad %%d ] |
|         | [ xcvr internal|external ] | [ wol p|u|m|b|a|g|s|d... ] |
|         | [ sopass %%x:%%x:%%x:%%x:%%x:%%x:%%x ] | [ msglvl %%d ] |

**Virtual IP’s**

NSG supports virtual IPs. To add a virtual IP address, click on the link to configure a virtual IP address and add specify the IP Address and Netmask. You will also need to create advanced firewall rules if the virtual IP is on the Internet.

**IP Troubleshooting**

In most installs, the network cards and IP settings will work straight out of the box. However, getting the network up the first time can be an exercise in frustration in some circumstances. Issues include:

- Network card compatibility
- Invalid networks settings (username, password, default gateway)

Cable/DSL modems that cache network card hardware information

**Static Routes**

In some cases a static route must be defined for a specific network interface: eth0 or eth1. The static route support is done via File Editor.

- Select IP Route from side/top Configuration Menu
- Add a custom route command

Save and Apply
The IP Route section only allows route add command syntax

<table>
<thead>
<tr>
<th>Route File Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Usage**       | Use to create static routes for Primary Signaling Ethernet Port:eth0 Usage:  
- (-host|-net) Target[/prefix] [gw Gw] [metric M]  
- [netmask N] [mss Mss] [window W] [irtt I] [dev If]  
Example:  
  #Route a class C network 10.133.20.0 via gw IP  
  -net 10.133.20.0 netmask 255.255.255.0 gw 10.132.30.1  
  #Route a class B network 10.133.0.0 via gw IP  
  -net 10.133.0.0 netmask 255.255.0.0 gw 10.132.30.1  
  #Route a class B network 10.133.0.0 via device eth0  
  -net 10.133.0.0 netmask 255.255.0.0 dev eth0 |
Virtual local area network, virtual LAN or VLAN is a concept of partitioning a physical network, so that distinct broadcast domains are created. NSG marks packets through tagging, so that a single interconnect (trunk) may be used to transport data for various VLANs.

A VLAN has the same attributes as a physical local area network (LAN), but it allows for end stations to be grouped together more easily even if not on the same network switch. VLAN membership can be configured through software instead of physically relocating devices or connections. Most enterprise-level networks today use the concept of virtual LANs (VLAN). Without VLANs, a switch considers all interfaces on the switch to be in the same broadcast domain.

**VLAN Configuration**

Currently NSG only supports VLAN configuration via GUI

- Select **VLAN** from side/top **Configuration** Menu
- Copy in the VLAN configuration script below into the file editor
- Save
  - On save the VLAN configuration will be applied
• Proceed to VLAN Status confirm VLAN configuration

The VLAN network interfaces are created over physical network interface. Make sure that the physical network interface eth0 or eth1 are configured in IP Settings, before attempting to configure VLAN on top of them eth0 or eth1.

The Save/Apply post processing will display VLAN configuration status

Example of sample script that could be copied into the VLAN config startup script:

```plaintext
#Create a VLAN device on eth0 interface with VLAN ID of 5 vconfig
add eth0 5

#configure VLAN device with IP/Net mask
ifconfig eth0.5 192.168.1.100 netmask 255.255.255.0 broadcast 192.168.1.255 up

#configure a default route within a vlan
route add -net 192.168.1.0/24 gw 192.168.1.1

#if system default route needs to go through VLAN
>Note that there can only be ONE system default route.
```

In the example above, a single VLAN was created

• on top of the Primary Signaling Ethernet Port:eth0 with
• VLAN ID=5 and
• IP =192.168.1.100/24.

**VLAN Routes**
An optional route can be created to point to a gateway within a VLAN network

Only routes related to VLAN interfaces are allowed in the VLAN configuration section

If a system default route needs to go through a VLAN

- Confirm that IP Settings interfaces are all set to **LAN** role.
- As there can be only ONE system default route.

**Additional VLAN**

If more VLAN's are needed, proceed to repeat the above steps for all VLANs.

When **Save** button is pressed

- The VLAN configuration will be applied
- The script above will be executed line by line.
- Status window will pop up with VLAN config status. If one of the lines fails, the pop up will report it.
- Proceed to **Overview -> VLAN status** below to confirm VLAN and Route configuration

```bash
# vconfig
Expecting argc to be 3-5, inclusive. Was: 1

Usage: add [interface-name] [vlan_id]
    rem [vlan-name]
    set_flag [interface-name] [flag-num] [0 | 1]
    set_egress_map [vlan-name] [skb_priority] [vlan_qos]
    set_ingress_map [vlan-name] [skb_priority] [vlan_qos]
    set_name_type [name-type]

* The [interface-name] is the name of the ethernet card that hosts the VLAN you are talking about.
* The vlan_id is the identifier (0-4095) of the VLAN you are operating on.
* skb_priority is the priority in the socket buffer (sk_buff).
* vlan_qos is the 3 bit priority in the VLAN header
* name-type: VLAN_PLUS_VID (vlan0005), VLAN_PLUS_VID_NO_PAD (vlan5), DEV_PLUS_VID {eth0.0005}, DEV_PLUS_VID_NO_PAD {eth0.5}
* bind-type: PER_DEVICE # Allows vlan 5 on eth0 and eth1 to be unique. PER_KERNEL # Forces vlan 5 to be unique across all devices.
* FLAGS: 1 REORDER_HDR When this is set, the VLAN device will move the ethernet header around to make it look exactly like a real ethernet device. This may help programs such as DHCPd which read the raw ethernet packet and make assumptions about the location of bytes. If you don't need it, don't turn it on, because there will be at least a small performance degradation.
Default is OFF
```

**VLAN Status**

- Select VLAN Status from side/top Overview Menu
This page shows
- All configured VLANs
- System Routing table
- Individual VLAN configuration
- Individual VLAN IP information

Date & Time Service Config

The Date/Time configuration tool allows you to:
- Select your time zone
- Synchronize your clock with network time servers
- Enable/disable a local time server for your network

Note that you need to configure your IP address and default route in order to be able to use a default time server that is located on the internet.

Confirm that VLAN Interface contains the correct IP address.

If the IP address is not set, the VLAN configuration has not been set properly.
To configure

- Select **Date** from side/top **System** menu
- Refer below to all available options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Date/Time</strong></td>
<td>The system date, time and time zone information is displayed for informational purposes. Please make sure it is accurate since it is not unusual to have computer clocks improperly set on a new installation.</td>
</tr>
<tr>
<td><strong>Time Zone</strong></td>
<td>It is important to have the correct time zone configured on your system. Some software (notably, mail server software) depends on this information for proper time handling.</td>
</tr>
<tr>
<td><strong>NTP Time Server</strong></td>
<td>An NTP Time Server is built into NSG.</td>
</tr>
<tr>
<td><strong>Time Synchronization</strong></td>
<td>Hitting the Synchronize Now button will synchronize the system's clock with network time servers.</td>
</tr>
</tbody>
</table>

**Initial Gateway Configuration**

NSG by default contains following VoIP/TDM Sections

- **Global Gateway Config**
  - Configured in Global gateway section.
  - Used to configure SIP, RTP, RADIUS options.

- **SIP/RTP**
  - Configured in Global Gateway section
  - SIP profile is always started

- **MG**
  - Configured in MG gateway section
  - MG Termination ID’s are mapped to TDM channels in TDM gateway section.
  - For full MG configuration one must configure MG and TDM sections.

- **SS7**
- Configured in TDM gateway section
- ISUP Termination
- M2UA Signaling Gateway

- Media/Transcoding
  - Configured in Media gateway section
  - Enable and select hw codec support
  - Note: HW transcoding is an optional feature.

- Dialplan
  - Used for SIP to TDM
  - Note: Dialplan is not used in MG/Megaco/H.248 mode.

- Apply
  - All configuration files are saved to disk at this step.
  - Above configuration sections only save information in local database.
  - NSG Gateway can be started in Control Panel after this step
  - TDM Status can be used to monitor Gateway Status.

Global Gateway Configuration

- Select Global from side/top Configuration Menu
- Change a SIP global variable and Click on Save (Disk Icon)
- Proceed to Control Panel and Restart the VoIP Gateway.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gwuser</td>
<td>Any string</td>
<td>Sangoma</td>
<td>NSG SIP incoming registration authentication user name. For security reasons, make sure to change these default settings.</td>
</tr>
<tr>
<td>gwpassword</td>
<td>Any string</td>
<td>Sangoma</td>
<td>NSG SIP incoming registration authentication password For security reasons, make sure to change these default settings</td>
</tr>
<tr>
<td>outbound_caller_name</td>
<td>Any string</td>
<td>Netborder SS7 to VoIP Media Gateway</td>
<td>Global caller id name defaults (used if no caller id name is present on the call) for both PSTN and SIP</td>
</tr>
<tr>
<td>outbound_caller_id</td>
<td>Any digits</td>
<td>9054741990</td>
<td>Global caller id defaults (used if no caller id is present on the call) for both PSTN and SIP</td>
</tr>
<tr>
<td>sip_port</td>
<td>Any port number</td>
<td>5062</td>
<td>SIP service local port number.</td>
</tr>
<tr>
<td>sip_ip</td>
<td>Any ip address</td>
<td>System IP</td>
<td>SIP service, local IP address. By default a local system eth0 address is taken as default ip address.</td>
</tr>
</tbody>
</table>
| sip_dtmf_type    | rfc2833 info none | rfc2833      | rfc2833 - DTMF passed via RTP oob message info  
                        - DTMF passed via SIP INFO message none  
                        - DTMF passed via inband media |
| rfc2833_pt       | Any number     | 101           | rfc2833 rtp payload type override. Ability to set the RTP payload type for rfc2833. Use d edge cases where remote equipment is not per spec. |
| sip_user_agent   | Any string     | Netborder SS7 to VoIP Media Gateway 4.0 | SIP INVITE user agent name string. |
| rtp_start_port   | Any port       | 21000         | RTP port starting range value. NSG will pick RTP ports for each call within this range. |
| rtp_end_port     | Any port       | 31000         | RTP port stop range value. NSG will pick RTP ports for each call within this range |
| pstn_default_group | g1,g2,g3,g4 .... | g1          | Default pstn dial group number, in case the group is not specified in the dial string. |
| radius_auth_host | Any ip address:port | 10.199.0.3:1812 | Location of the Radius server, that will be used to authenticate incoming calls. |
| radius_auth_secret | Any string    | testing123   | Password of the remote Radius server. |

**SS7 ISUP Configuration**

SS7 is a signaling protocol, it is used to carry call control information such as call start, call progress, call hang-up etc. The SS7 call control information is used to control arbitrary number of voice channels that are carried using T1/E1 spans.

In a typical SS7 setup the telco will provide you with SS7 information that will be used to map T1/E1 physical spans and channels into SS7 call control information.

The NSG TDM SS7 configuration page has been designed as bottom up SS7 configuration approach.
1. Identify T1/E1 spans on your system
2. For each T1/E1 span on your system:
   1. Determine which T1/E1 spans will carry SS7 Link channels
   2. T1/E1 Span can either carry an
      1. SS7 Link in one of its channels or
      2. All T1/E1 channels can be used to carry voice.
   3. Configure T1/E1 physical configuration parameters
   4. Identify if T1/E1 span carries SS7 link or is Voice Only

1. If T1/E1 span has an SS7 link associate with it:
   1. Create a new SS7 Link
   2. Next step is to bind the new SS7 Link to an SS7 Linkset.
   3. If an SS7 Link set does not exist, Create a new SS7 Link Set
   4. Then bind the SS7 Link to an existing or new SS7 Link Set
   5. Next step is to bind the SS7 Linkset into an SS7 Route.
   6. If an SS7 Route does not exist, Create a new SS7 Route
   7. Then bind the SS7 Linkset to an existing or new SS7 Route
   8. Next step is to bind the SS7 Route into an SS7 ISUP Interface
   9. If an SS7 ISUP Interface does not exist, Create a new SS7 ISUP Interface
   10. Then bind the SS7 Route to an existing or new SS7 ISUP Interface

1. The Last step is to assign CIC values to each physical T1/E1 timeslot in the span.

Whether the Span carries only voice or it contains the SS7 Link, each timeslot must be associated with a SS7 CIC value.

This way when an incoming SS7 Call Start message arrives with an arbitrary CIC value. The NSG system can open the appropriate physical voice channel associated with the CIC value.

Once all T1/E1 spans are configured you need to Apply the configuration files.

Note that this step does not start the NSG gateway. It just writes the appropriate configuration files.

Proceed to the Control Panel to start the NSG SS7 to VoIP Gateway.

**TDM SS7 Configuration Page**

- Select TDM from side/top Configuration menu
- The TDM section will display all installed TDM Spans/Ports.

The TDM Configuration page will display to the user every T1/E1 card detected by NSG.

Each card is logically separated into ports, which initially displays the firmware version and the Echo Cancellation security chip ID. If the echo cancellation security chip ID is 0, then the card installed does not have echo cancellation. If there is a alert image next to the firmware version, that means the firmware on the system is out of date, and must be updated in order to have the most up to date and efficient firmware running.
Port Identification

- In order to determine which physical T1/E1 port is: Port 1 Card 1
- Select Identify button for Port 1 Card 1
- The LED light will start flashing on a rear RJ45 T1/E1 port: rear panel.
- Look at the rear panel of the appliance and plug in RJ45 cable to the blinking RJ45 T1/E1 port.
- Once the Port 1 Card 1 is identified, the subsequent ports for that board are labeled.
- Or alternatively keep using the Identify feature for each port.
Once the port has been identified and plugged into the T1/E1 network.
Select button for Port 1 Card 1 to configure the physical T1/E1 parameters.

- Edit
  - Select the port configuration type: T1 or E1
    - T1: North American Market and Japan
    - E1: Europe and the world
  - Fill in Physical Configuration T1 or E1 parameters
  - Fill in the T1/E1 parameters based on the provider provision document.

- Identify picture of the device is always set to A108D – 8 T1/E1 card. The LED will always bling port 1. The image is not meant to reflect the real hardware image, nor real port location. User should always view the rear panel for the flashing LED.
- All Sangoma TDM T1/E1 cards Port 1 is closest to the PCI slot.

---

**Edit T1/E1 Config**

- Once the port has been identified and plugged into the T1/E1 network.
- Select **Edit** button for Port 1 Card 1 to configure the physical T1/E1 parameters.
- Select the port configuration type: T1 or E1
  - T1: North American Market and Japan
  - E1: Europe and the world
- Fill in Physical Configuration T1 or E1 parameters
- Fill in the T1/E1 parameters based on the provider provision document.

---

**Standard T1/E1 Parameters**
In case advanced parameters are not necessary proceed

- Apply to Port
  - Applies the configuration for a single T1/E1 port
  - (The one that is currently being edited)
- Apply to all Ports
  - Apply to all T1/E1 ports on a board.
  - Bulk config feature
  - (This feature saves time as T1/E1 ports are usually provisioned the same)

**Advanced T1/E1 Parameters**
Span Link Type

When configuring TDM Terminations for SIP to ISUP Media Gateway there are two possibilities

- **Voice Mode**
  - All TDM channels are used for Voice 64kbs G.711
  - Example: All channels 1-31 on an E1 line are used for voice
  - Link Type = Voice Only

- **Mix Mode**
  - Voice 64kbs G.711 channels and SS7 signaling channels.
  - Example: Channel 16 is used for SS7 signaling, 1-15,17-31 are used for voice.
  - Link Type = ISUP Termination

- If configuring for **Voice Mode** select No Signaling Link
- If configuring for **Mixed Mode** select ISUP Termination

After T1/E1 configuration, the NSG wizard will request **Link Type** Configuration.
• The rest of this section will continue to document the ISUP Termination option.
• In case of Voice Mode – the GUI will skip the ISUP configuration and proceed directly to Channel Map Section below.

SS7 Network Overview

SS7 Network Diagram
Links

- physical signaling links between the TX board and the adjacent signaling points. One link configuration must be performed for each physical signaling link. The attributes of a link include the point code of the adjacent signaling point, protocol variant employed on the link (ITU-T or ANSI), point code length, maximum packet length, various timer values, membership in a linkset, and others.

Linksets

- are groups of from one to 16 links that directly connect two signaling points. Although a linkset usually contains all parallel signaling links between 2 SPs, it is possible to define parallel link sets. Each signaling link defined is assigned membership in exactly one link set.

Routes

- specify the destination signaling points (or sub-networks (clusters) when route masks are employed) that are accessible from the target node. Each route is assigned a direction - up or down. One up route is required for the actual point code assigned to the signaling point being configured and for each point code that is to be emulated. Up routes are used to identify incoming messages that are to be routed up to the applications/user parts. One down route is required for each remote signaling point/network/cluster that is to be accessible from the SP being configured.

MTP2 Link Configuration

Proceed to configure the SS7 ISUP link that exists on a DS0 timeslot of a T1/E1 port. The information required for the SS7 Link configuration must be provided by the Telco.

Next screen will confirm if the T1/E1 port contains a signaling link.

- Please select YES if the SS7 signaling link exists on current T1/E1 port.
- By selecting NO this T1/E1 port would not contain a signaling link, but the voice channels would still be controlled by the ISUP signaling. Thus channel mapping would still apply.

The following screen will configure the MTP1 and MTP2 protocol configuration of the SS7 Link.
- The SLC configuration value MUST be unique for each SS7 Link, in case all SS7 Links belong to same Link Set.

Click on Apply to Port button to proceed to next configuration section

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Link Name</td>
<td>Any String</td>
<td>Link1</td>
<td>Name to identify the SS7 Link. By default the GUI will select a unique name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>However it is sometimes useful to specify a SS7 Link name that relates to the remote destination.</td>
</tr>
<tr>
<td>Span</td>
<td></td>
<td></td>
<td>This is readonly information field. Provides the user with span number information.</td>
</tr>
<tr>
<td>Line Media Type</td>
<td></td>
<td></td>
<td>This is readonly information field. Provide the user with T1/E1 link type that has previously been configured.</td>
</tr>
<tr>
<td>Signaling Channel</td>
<td>Single Digit 1-31</td>
<td></td>
<td>User must specify the DS0 location of the SS7 signaling channel. The timeslot number relates to physical DS0 channel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Valid options are E1: 1 to 31</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>T1: 1 to 24</td>
</tr>
</tbody>
</table>
A usual location of a SS7 signaling channel is 1 or 16.

<table>
<thead>
<tr>
<th>Error Type</th>
<th>Basic PCR</th>
<th>Basic</th>
<th>MTP2 error correction type forms of error correction are defined for an SS7 signaling link at MTP2: the basic method and the PCR method.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>: Basic</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The basic method is generally applied to configurations in which the one-way propagation delay is less than 40 ms, : PCR</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PCR is applied on intercontinental signaling links in which the one-way propagation delay is greater than 40 ms and on all signaling links established via satellite.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>maximum supported signaling link loop (round trip) delay is 670 ms (the time between the sending of a message signal unit [MSU] and the reception of the acknowledgment for this MSU in undisturbed operation).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LSSU Length</th>
<th>1 or 2</th>
<th>1</th>
<th>1- or 2-byte link status signal unit (LSSU) format</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Link Type</th>
<th>ITU92 ITU88 ANSI96 ANSI92 ANSI88</th>
<th>ITU92</th>
<th>MTP2 protocol supports different variants Outside North America • ITU and ETSI standards are used In North America • ANSI standards are used.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>MTP3 Priority</th>
<th>ETSI</th>
<th>Digit</th>
<th>0</th>
<th>Default traffic priority for this link.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Switch Type</th>
<th>ITU00 ITU97 ITU92 ITU88 ETSI V2 ETSI V3 UK RUSSIA INDIA ANSI92 ANSI95</th>
<th>ITU00</th>
<th>MTP3 protocol supports different variants Outside North America • ITU and ETSI standards are used In North America • ANSI standards are used.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Sub Service Filed (SSF)</th>
<th>National International Spare Reserved</th>
<th>National</th>
<th>Please confirm with your provider which value to use.</th>
</tr>
</thead>
</table>

| Signaling Link Selection Code (SLC) | Digit 0-X | 0 | SLC can normally be set to 0 by default. Except when there are multiple SS7 Links in a Link Set. In such case SLC must be unique for each SS7 Link. In such case |
MTP3 Linkset Configuration

A number of links can be grouped into a linkset that connects to an adjacent point. Each signaling link is provided with a unique code called a signaling link code (SLC). Traffic is load-shared across this linkset. The signaling links within a linkset also provide a redundant transport mechanism. Therefore the more links there are to a linkset the higher the transport bandwidth is and the higher the redundancy.

Linkset configuration on NSG GUI is based on Linkset profiles. It is designed so that multiple SS7 signaling links can use the same SS7 Linkset Profile. The term used when attaching links to linksets in NSG is BIND. You have to bind a link to a linkset in order to proceed.

NOTE

- If no Linkset profile exists, user will be directed to the Linkset profile creation page.
- If Linkset profile already exists, user will be directed to Link profile list page. Where user will be able create a Linkset profile or edit existing Linkset profile.

Click on Create Profile once the configuration is completed.

NOTE

- On very list Linkset profile, the Link will automatically be BINDED to the Linkset.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Any String</td>
<td>LS1</td>
<td>Name to identify the SS7 Linkset. By default the GUI will select a unique name. However it is sometimes useful to specify a SS7 Linkset name that relates to the remote destination.</td>
</tr>
<tr>
<td>Adjacent Point Code</td>
<td>If ITU integer: 1 to X If ANSI</td>
<td></td>
<td>Point-code is an SS7 address for an element in the SS7 network.</td>
</tr>
<tr>
<td>three integers separated by dash</td>
<td>The Adjacent point is the SS7 equipment which the signaling links terminate on. This equipment will also have a unique point code. This equipment may be either STP equipment or SSP equipment depending on type of interconnect</td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| If ITU
  - Single integer number: eg 500 If ANSI
  - Three integers separated by dash: eg 100-200-400 Please refer to your Telco provider for this information. |

| Minimum Active Signaling Links | Integer 1-X | A Linkset can contain number of SS7 Links.
This field defines how data should be distributed across links in a linkset.
For Round Robin – make the value equal number of links in a linkset
  - This mode will use all links equally. **Recommended**
For Active Standby – make the value 1 or less than total number of links.
  - This mode will use the first link until it gets saturated.
  - And only use another link if necessary |

---

**MTP3 SS7 Route**

Route is a collection of linksets to reach a particular destination. A linkset can belong to more than one route. Service Provider personnel statically maintain signaling endpoint routing tables. The routing table identifies the links, linksets, primary routes, and alternate routes for each DPC. All links in the linkset share the traffic load equally.

After a successful Linkset configuration, NSG GUI will present a user with Route Configuration screen.

- If no Route profiles exist, user will be presented with Route create page.
- If a Route profile already exists, user will be presented with Route profile list. Where user will be able to either create new Route or edit existing Route profile.
If a new linkset needs to be attached to a route, the user must edit the route, then add the new linkset to that route.

The user will only need to edit a route if a new linkset is created on the system. If no new linksets are created, the user will proceed directly to the channel map and CIC map configuration.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Any String</td>
<td>ROUTE1</td>
<td>Name to identify the SS7 Route. By default the GUI will select a unique name. However it is sometimes useful to specify a SS7 Route name that relates to the remote destination.</td>
</tr>
</tbody>
</table>
| Destination Point Code     | If ITU integer: 1 to X If ANSI three integers separated by dash |               | Point-code is an SS7 address for an element in the SS7 network. The Destination Point of the SS7 network defines the switching equipment within the PSTN network which terminates the TDM interfaces of this interconnect. This point is also allocated a unique point-code within the SS7 network. If the adjacent point is a SSP or MSC interconnect the destination point will be the same as the adjacent point.  

Eg:

A-Link = APC differs from DPC F-Link = APC is equal to DPC

If ITU (outside North America)

- Single integer number: eg 500
- Default link type – F link

If ANSI (North America)
ISUP Interface Configuration

ISUP connects, manages, and disconnects all voice and data calls in the PSTN. ISUP sets up and tears down the circuits used to connect PSTN voice and data subscribers. ISUP is used in cellular or mobile networks for trunking connections.

ISUP information is transferred in MTP3 messages similar to the other L4 protocols. The ISUP section covers the following topics:

- ISUP Services
- Basic and Supplementary
- End-to-end Signaling
- Pass-along and SCCP
- Call Setup and Teardown
- ISUP Message Format
- ISUP Call Control Messages

Like the linkset configuration and route configuration profiles, the ISUP Interface configuration is also configured as profiles. It is setup so that 1 SS7 route can be attached to 1 ISUP Interface.

After a successful Route configuration, NSG GUI will present a user with Route Configuration screen.

- If no ISUP profiles exist, user will be presented with ISUP create page.

If an ISUP profile already exists, user will be presented with ISUP profile list. Where user will be able to either create new ISUP Interface Profile.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Any String</td>
<td>ISUP1</td>
<td>Name to identify the SS7 ISUP Interface profile. By default the GUI will select a unique name.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>However it is sometimes useful to specify a SS7 ISUP Interface name that relates to the remote destination.</td>
</tr>
<tr>
<td>Self Point Code</td>
<td>If ITU: 1 to X If ANSI integers separated by dash</td>
<td></td>
<td>Point-code is an SS7 address for an element in the SS7 network. The Self Point Code /Originating Point describes the equipment that is</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>interconnecting into the SS7 network. The originating point will be provided with a unique point-code by the network provider allowing for</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>identification of this point with in the SS7 network.</td>
</tr>
<tr>
<td>Sub Service Field SSF</td>
<td>National International Spare Reserved</td>
<td>National</td>
<td>Self Point Code is the address of the NSG SS7 Gateway in the SS7 network. If ITU (outside North America)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Single integer number: eg 500</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• Three integers separated by dash: eg 100-200-400</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Please refer to your Telco provider for this information.</td>
</tr>
<tr>
<td>Route</td>
<td></td>
<td></td>
<td>List of existing Route profiles that can be bound to a Route profile. There has to be a single Route bound to an ISUP Interface profile.</td>
</tr>
<tr>
<td>ISUP Timer</td>
<td>Spec Value (s)</td>
<td>Default Value (s)</td>
<td>Timer Name</td>
</tr>
<tr>
<td>------------</td>
<td>----------------</td>
<td>-------------------</td>
<td>------------</td>
</tr>
<tr>
<td>T1</td>
<td>15-60</td>
<td>15</td>
<td>isup.t1</td>
</tr>
<tr>
<td>T2</td>
<td>180</td>
<td>180</td>
<td>isup.t2</td>
</tr>
<tr>
<td>T3</td>
<td>120</td>
<td>120</td>
<td>isup.t3</td>
</tr>
<tr>
<td>T4</td>
<td>300-900</td>
<td>300</td>
<td>isup.t4</td>
</tr>
<tr>
<td>T5</td>
<td>300-900</td>
<td>300</td>
<td>isup.t5</td>
</tr>
<tr>
<td>T6</td>
<td>60-120</td>
<td>60</td>
<td>isup.t6</td>
</tr>
<tr>
<td>T7</td>
<td>20-30</td>
<td>20</td>
<td>isup.t7</td>
</tr>
<tr>
<td>T8</td>
<td>10-15</td>
<td>10</td>
<td>isup.t8</td>
</tr>
<tr>
<td>T9</td>
<td>90-180</td>
<td>180</td>
<td>isup.t9</td>
</tr>
<tr>
<td>T10</td>
<td>4-6</td>
<td>4</td>
<td>isup.t10</td>
</tr>
<tr>
<td>T12</td>
<td>15-60 (ITU)</td>
<td>150</td>
<td>isup.t12</td>
</tr>
<tr>
<td></td>
<td>4-15(ANSI)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>T13</td>
<td>300-900</td>
<td>300</td>
<td>isup.t13</td>
</tr>
<tr>
<td>T14</td>
<td>15-60</td>
<td>15</td>
<td>isup.t14</td>
</tr>
<tr>
<td>T15</td>
<td>300-900</td>
<td>300</td>
<td>isup.t15</td>
</tr>
<tr>
<td>T16</td>
<td>15-60</td>
<td>15</td>
<td>isup.t16</td>
</tr>
<tr>
<td>T17</td>
<td>300-900</td>
<td>300</td>
<td>isup.t17</td>
</tr>
<tr>
<td>T27</td>
<td>240</td>
<td>240</td>
<td>isup.t27</td>
</tr>
<tr>
<td>T31</td>
<td>360</td>
<td>360</td>
<td>isup.t31</td>
</tr>
<tr>
<td>T33</td>
<td>12-15</td>
<td>12</td>
<td>isup.t33</td>
</tr>
<tr>
<td>T34</td>
<td>2-4</td>
<td>4</td>
<td>isup.t34</td>
</tr>
<tr>
<td>T35</td>
<td>15-20</td>
<td>15</td>
<td>isup.t35</td>
</tr>
<tr>
<td>T36</td>
<td>10-15</td>
<td>12</td>
<td>isup.t36</td>
</tr>
</tbody>
</table>

**ISUP CIC Channel Mapping**

The last step of the configuration is to bind the TDM voice channels to ISUP Profile and map ISUP CIC’s to the TDM timeslots.
<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Any String</td>
<td>CC1</td>
<td>Name to identify the SS7 Call Control profile. By default the GUI will select a unique name. However it is sometimes useful to specify a SS7 ISUP Interface name that relates to the remote destination.</td>
</tr>
<tr>
<td>ISUP Interface</td>
<td>List of existing ISUP Interface profiles</td>
<td>Current Profile</td>
<td>ISUP Interface points to the list of currently defined ISUP Interface profiles. Each ISUP profile defines its own Self-Point-Code/Origination Code. With multiple ISUP profiles, one can configure a system with multiple Self-Point-Codes. Selected ISUP Interface Profile will be used to control the physical TDM T1/E1 DS0 channels.</td>
</tr>
<tr>
<td>CIC Base</td>
<td>Integer 1 to Any</td>
<td>1</td>
<td>Start of the ISUP CIC numbers. ISUP CIC numbers are logical representations of the physical DS0 channels. The mapping between CIC and DS0 channels is one to one. This information is provided by the Telco.</td>
</tr>
<tr>
<td>Call Control</td>
<td>Controlled Controlling Bothway Incoming Outgoing</td>
<td>Controlled</td>
<td>Refer to Telco information.</td>
</tr>
<tr>
<td>Channel Map</td>
<td></td>
<td></td>
<td>List of channels to be controlled by ISUP Interface Example: 1-15,s16,</td>
</tr>
</tbody>
</table>
Channels 1-15 and 17-31 are used for Voice and should be controlled by ISUP Interface. Channel 16 (prefixed by letters) indicates that channel 16 carries signaling channel. ISUP Interface will ignore this channel as it’s not voice.

Prefix Letters to signaling channel:
- **S:** ISUP CIC id not used, id mapped to signaling channel
- **G:** ISUP CIC id is used, id mapped to next available voice channel.

The bind between ISUP and TDM would be as follows:

**Channel Map: 1—31 (no signaling channel)**

CIC 1: channel 1
CIC 2: channel 2
...
CIC 16: channel 16
...
CIC 30: channel 30
CIC 31: channel 31

**Channel Map: 1-15,s16,17-31 (signaling on ch 16)**

CIC 1: channel 1
CIC 2: channel 2
...
CIC 15: channel 15
...
CIC 16: not used – A16 points to signaling channel 16 CIC 17: channel 17
CIC 18: channel 18
...
CIC 31: channel 31

**Channel Map: 1-15,g16,17-31 (signaling on ch 16)**

CIC 1: channel 1
CIC 2: channel 2
CIC 15: channel 15
CIC 16: channel 17 - A16 is used and it points to ch 17. CIC 17: channel 18
...
CIC 30: channel 31

**Span Group Number**  
**Integer**  
**1**  
Default group number used to dial out over a trunk group. Usually the group number will correspond to the trunk group.
### Field Name | Possible Values | Default Value | Description
--- | --- | --- | ---
Minimum Incoming Overlap Dialing | Integer |  | Enables overlap dialing in ISUP.
ISUP Interface | List of existing ISUP Interface profiles | Current Profile | ISUP Interface points to the list of currently defined ISUP Interface profiles. Each ISUP profile defines its own Self-Point-Code/Origination Code. With multiple ISUP profiles, one can configure a system with multiple Self-Point-Codes. Selected ISUP Interface Profile will be used to control the physical TDM T1/E1 DS0 channels.
CIC Base | Integer 1 to Any | 1 | Start of the ISUP CIC numbers. ISUP CIC numbers are logical representations of the physical DS0 channels. The mapping between CIC and DS0 channels is one to one. This information is provided by the Telco. **CAUTION**
- Improper mapping between CIC and Physical T1/E1 DS0 can...
result in one way or no audio. Even though the call completes successfully on SS7 signaling.

<table>
<thead>
<tr>
<th>Call Control</th>
<th>Controlled</th>
<th>Controlling Bothway</th>
<th>Incoming</th>
<th>Outgoing</th>
<th>Controlled</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Refer to Telco information.</td>
</tr>
</tbody>
</table>

### Channel Map

List of channels to be controlled by ISUP Interface Example: 1-15, s16, 17-31
Channels 1-15 and 17-31 are used for Voice and should be controlled by ISUP Interface
Channel 16 (prefixed by letters) indicates that channel 16 carries signaling channel. ISUP Interface will ignore this channel as it's not voice.

Prefix Letters to signaling channel:

- **s**: ISUP CIC id not used, id mapped to signaling channel
- **g**: ISUP CIC id is used, id mapped to next available voice channel.

The bind between ISUP and TDM would be as follows

**Channel Map: 1—31 (no signaling channel)**

<table>
<thead>
<tr>
<th>CIC 1</th>
<th>channel 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIC 2</td>
<td>channel 2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 15</td>
<td>channel 16</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 30</td>
<td>channel 30</td>
</tr>
<tr>
<td>CIC 31</td>
<td>channel 31</td>
</tr>
</tbody>
</table>

**Channel Map: 1-15, s16, 17-31 (signaling on ch 16)**

<table>
<thead>
<tr>
<th>CIC 1</th>
<th>channel 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIC 2</td>
<td>channel 2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 15</td>
<td>channel 15</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 16</td>
<td>not used – A16 points to signaling channel 16</td>
</tr>
<tr>
<td>CIC 17</td>
<td>channel 17</td>
</tr>
<tr>
<td>CIC 18</td>
<td>channel 18</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 30</td>
<td>channel 30</td>
</tr>
<tr>
<td>CIC 31</td>
<td>channel 31</td>
</tr>
</tbody>
</table>

**Channel Map: 1-15, g16, 17-31 (signaling on ch 16)**

<table>
<thead>
<tr>
<th>CIC 1</th>
<th>channel 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIC 2</td>
<td>channel 2</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 15</td>
<td>channel 15</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 16</td>
<td>not used – A16 points to signaling channel 16</td>
</tr>
<tr>
<td>CIC 17</td>
<td>channel 17</td>
</tr>
<tr>
<td>CIC 18</td>
<td>channel 18</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>CIC 31</td>
<td>channel 31</td>
</tr>
</tbody>
</table>
Media Transcoding Configuration

NSG will enable ALL Media Codec's by default. There is no extra configuration needed.

Use this configuration page in case you want to limit which codecs should be enabled, or disable media codec support.

To access NSG Media Transcoding Configuration

- Select Media from side/top Configuration Menu
- Select any or all supported/listed codecs
- Once done press Save

At this point the codec selection is over. One can proceed to Media hardware discovery in the Advanced Options of the Media page.

Media Hardware

Once Codec selection has been made, proceed to Advanced Options section of the Media page.
- Select SCAN
  - This step will auto-detect all NSG transcoding resources
    - Confirm that GUI detected exact number of transcoding resources as installed.
    - User has an option of changing the assigned Local IP address of the Media device.

At this point the Media configuration is complete.

- Proceed to the next section, or
- If finished all gateway configuration, proceed to Apply to generate configs

**Applying Configuration**

The changes made in the **Configuration** section of the WebUI are only stored on the scratch disk. User MUST proceed to Apply page in the Management Section to save new configuration.

- Select **Apply** from side/top **Configuration** Menu
- Visually confirm the warnings
  - License warning need to be resolved with Sales
- Select **Generate Config** to apply the configuration to file/disk.
- Generate Config will generate all necessary NSG SS7 VoIP Gateway configuration files needed to successful start the NSG gateway
Dialplan

When a call is received in the NetBorder SS7 Gateway, from SIP, H232 or SS7 the dialplan is fetched to retrieve the route information to find the outgoing call location.

Dialplan is not used in MG/Megaco/H.248 mode: MGC performs the routing.

- PSTN to SIP Dialplan
- SIP to PSTN Dialplan
- References

To access Dialplan configuration section

- Select Dialplan from side/top Configuration Menu
- Change a variable and Click on Save (Disk Icon)
- Proceed to Control Panel and Restart the VoIP Gateway.
Dialplan is pre-configured for

- SIP to TDM and TDM to SIP Bridging.

Section "from-sip" routes calls from SIP to PSTN/SS7 Section "from-pstn" routes calls from PSTN/SS7 to SIP.

Note that default dial plans allow for unchallenged SIP INVITEs. Normally this is OK for equipment that is installed in private networks or behind Session Border Controllers. However, should the SS7 Gateway be installed on a public IP address, the dial plan needs to be modified to block these requests to mitigate security risks. Note however that NSG is not a security device, it is a VoIP Gateway. Sangoma recommendeds to use Session Border Controller to secure VoIP Networks.

**Dialplan Reload/Apply**

Note that Dialplan can be modified in real time without the need to restart the gateway.

When you Save the Dialplan, you will be prompted to Reload the gateway which will apply the changes without any service interrupt. All the currently established calls will not be affected. Only the newly established calls will start using the new dialplan rules.

**PSTN to SIP Dialplan**

By default NSG is setup to send an call to a SIP IP address. The remote SIP address must be configured in Configuration -> Global section.
Dialplan Syntax

There are several elements used to build an XML dialplan. In general, the dialplan groups logically similar functions and calling activities into a 'context'. Within a context are extensions, each with 'condition' rules and associated 'actions' to perform when the condition rules match. Following is a sample dialplan to illustrate these concepts. We have left out the XML "wrapper" to help make the basic concepts more clear:

```xml
<context name="from-pstn-to-sip">
  <extension name="500">
    <condition field="destination_number" expression="^500$">
      <action application="bridge" data="user/500"/>
    </condition>
  </extension>

  <extension name="501">
    <condition field="destination_number" expression="^501$">
      <action application="answer"/>
    </condition>
  </extension>
</context>
```

```xml
<context name="example">
  <extension name="500">
    <condition field="destination_number" expression="^500$">
      <action application="bridge" data="user/500"/>
    </condition>
  </extension>

  <extension name="501">
    <condition field="destination_number" expression="^501$">
      <action application="answer"/>
    </condition>
  </extension>
</context>
```
Each rule is processed in order until you reach the action tag which tells NSG what action to perform. You are not limited to only one condition or action tag for a given extension.

In our above example, a call to extension 501 rings the extensions. If the user does not answer, the second action answers the call, and following actions delay for 1000 milliseconds (which is 1 second) and connect the call to the voicemail system.

**Context**

Contexts are a logical grouping of extensions. You may have multiple extensions contained within a single context. The context tag has a required parameter of 'name'. There is one reserved name, any, which matches any context. The name is used by incoming call handlers (like the [Sofia] SIP driver) to select the dialplan that runs when it needs to route a call. There is often more than one context in a dialplan.

A fully qualified context definition is shown below. Typically you won't need all the trimmings, but they are shown here for completeness.

```xml
<?xml version="1.0"?>
<document
type="freeswitch/xml">

<section name="dialplan"
description="Regex/XML Dialplan">

<!-- the default context is a safe start -->
<context
name="default">
<!-- one or more extension tags -->
</context>
<!-- more optional contexts -->
</section>
</document>
```

**Extensions**

Extensions are destinations for a call. This is the meat of NSG routing dialed numbers. They are given a name and contain a group of conditions, that if met, will execute certain actions.

A 'name' parameter is required: It must be a unique name assigned to an extension for identification and later use.

For example:

```xml
<extension name="Your extension name here">
<condition(s)>
<action(s>
...</action(s>
</condition>
</extension>
```

Typically when an extension is matched in your dialplan, the corresponding actions are performed and dialplan processing stops. An optional continue parameter allows your dialplan to continue running.

```xml
<extension name="500" continue="true">
```
Conditions

Dialplan conditions are typically used to match a destination number to an extension. They have, however, much more power than may appear on the surface.

NSG has a set of built-in variables used for testing. In this example, the built-in variable destination_number is compared against the regular expression '^500$'. This comparison is 'true' if <destination_number> is set to 500

```xml
<extension name="500">
  <condition field="destination_number" expression="^500$">
    <action application="bridge" data="user/500"/>
  </condition>
</extension>
```

Each condition is parsed with the Perl Compatible Regular Expression library. (go here for PCRE syntax information).

If a regular expression contains any terms wrapped in parentheses, and the expression matches, the variables $1,$2..$N will be set to the matching contents within the parenthesis, and may be used in subsequent action tags within this extension's block.

For example, this simple expression matches a four digit extension number, and captures the last two digits into $1.

```xml
<condition field="destination_number" expression="\d\d(\d\d)">
  <action application="bridge" data="sofia/internal/$1@example.com"/>
</condition>
```

A destination number of 3425 would set $1 to 25 and then bridge the call to the phone at 25@example.com

Multiple Conditions (Logical AND)

You can emulate the logical AND operation available in many programming languages using multiple conditions. When you place more than one condition in an extension, all conditions must match before the actions will be executed. For example, this block will only execute the actions if the destination number is 500 AND it is Sunday.

```xml
<condition field="destination_number" expression="^500$"/>
<condition wday="1"> action(s)...
</condition>
```

Keep in mind that you must observe correct XML syntax when using this structure. Be sure to close all conditions except the last one with />. The last condition contains the final actions to be run, and is closed on the line after the last action. By default, if any condition is false, NSG will move on to the anti-actions or the next extension without even evaluating any more conditions

Multiple Conditions (Logical OR, XOR)

It is possible to emulate the logical OR operation available in many programming languages, using multiple conditions. In this situation, if one of the conditions matches, the actions are executed.

For example, this block executes its actions if the destination number is 501 OR the destination number is 502.
This method works well if your OR condition is for the same field. However, if you need to use two or more different fields then use the new `regex` syntax.

Using this method it becomes easier to match the caller's name OR caller ID number and execute actions whether either is true. A slightly more advanced use of this method is demonstrated here:

```xml
<extension name="Regex OR example 1" continue="true">
  <condition regex="any">
    <!-- If either of these is true then the subsequent actions are added to execute list -->
    <regex field="caller_id_name" expression="Some User"/>
    <regex field="caller_id_number" expression="^1001$"/>
    <action application="log" data="INFO At least one of the conditions matched!"/>
    <!-- If *none* of the regexes is true then the anti-actions are added to the execute list -->
    <anti-action application="log" data="WARNING None of the conditions matched!"/>
  </condition>
</extension>

Using this method it becomes easier to match the caller's name OR caller ID number and execute actions whether either is true. A slightly more advanced use of this method is demonstrated here:

```xml
<extension name="Regex OR example 2" continue="true">
  <condition regex="any" break="never">
    <regex field="caller_id_name" expression="^Michael\s*S?\s*Collins"/>
    <regex field="caller_id_number" expression="^1001|3757|2816$"/>
    <action application="set" data="calling_user=mercutioviz" inline="true"/>
    <anti-action application="set" data="calling_user=loser" inline="true"/>
  </condition>
  <condition>
    <action application="answer"/>
  </condition>
  <action application="sleep" data="500"/>
  <action application="playback" data="ivr/ivr-welcome_to_freeswitch.wav"/>
</extension>
```
<action application="sleep" data="500"/>
</condition>
<condition field="${calling_user}" expression="^loser$">
<action application="playback" data="/ivr/ivr-dude_you_suck.wav"/>
<anti-action application="playback" data="/ivr/ivr-dude_you_rock.wav"/>
</condition>
</extension>

<extension name="Regex XOR example 3" continue="true">
<condition regex="xor">
<!-- If only one of these is true then the subsequent actions are added to execute list -->
<regex field="caller_id_name" expression="Some User"/>
<regex field="caller_id_number" expression="^1001$"/>
<action application="log" data="INFO Only one of the conditions matched!"/>
<!-- If *none* of the regexes is true then the anti-actions are added to the execute list -->
<anti-action application="log" data="WARNING None of the conditions matched!">
</condition>
</extension>

Basically, for this new syntax you can have a condition to have a "regex" attr instead of "field" and "expression" etc. When there is a "regex" attr, that means you plan to have one or more <regex> tags that are similar to the condition tag itself that it has field and expression in it.

The value of the "regex" attr is either "all" or "any" or "xor indicating if all expressions must match or just any expression or only one must match (xor). If it's set to "any" it will stop testing the regex tags as soon as it finds one match, if it is set to "all", it will stop as soon as it finds one failure.

From there it will behave like a normal condition tag either executing the actions or anti-actions and breaking based on the "break" attr.

The basic difference here is once there is a "regex" attr, the <regex> tags parsed for "all" or "any" take the place of the single "field" and "condition"

NOTE: Also, if any captures are done in the "expression" attrs of a <regex> tag, only the data from the newest capture encountered will be considered in the $n expansion or FIELD_DATA creation. In addition, you can set DP_REGEX_MATCH_1 .. DP_REGEX_MATCH_N to preserve captures into arrays.

<extension name="Inbound_external">
<condition regex="any">
<regex field="${sip_from_host}" expression="domainA"/>
<regex field="${sip_from_uri}" expression="1234567890@domainB"/>
<regex field="${sip_from_uri}" expression="user@domainC"/>
<regex field="caller_id_name" expression="^(John Smith)$"/>
<regex field="caller_id_number" expression="^(55512341)|(55512342)| (55512343)$"/>
<action application="set" data="domain_name=domainZ"/>
<action application="transfer"
This is another example to show that all regex conditions must be true, then the action will get executed; otherwise, the anti-action will. This is the same logic as follows:

```xml
<condition regex="all">
  <regex field="${sip_gateway}" expression="^${default_provider}$"/>
  <regex field="${emergency_call}" expression="^true$"/>
  <regex field="${db(select/emergency/autoanswer)}" expression="^1$"/>
  <!-- the following actions get executed if all regexes PASS -->
  <action application="set" data="call_timeout=60"/>
  <action application="set" data="effective_caller_id_name=${regex \(${caller_id_name}|^Emerg(_.*)$|Auto%1)}$/"/>
  <action application="set" data="autoanswered=true"/>
  <action application="bridge" data="user/1000@$domain_name,sofia/gateway/1006_7217/${mobile_number}"/>
  <!-- the following anti-actions are executed if any of the regexes FAIL -->
  <anti-action application="set" data="effective_caller_id_name=${regex \(${caller_id_name}|^Emerg(_.*)$|NotAuto%1\)}$/"/>
  <anti-action application="set" data="call_timeout=30"/>
  <anti-action application="set" data="autoanswered=false"/>
  <anti-action application="bridge" data="user/1000@$domain_name,sofia/gateway/1006_7217/${mobile_number}"/>
</condition>
```

### Complex Condition/Action Rules

Here is a more complex example, performing time-based routing for a support organization. The user dials extension 1100. The actual support extension is 1105 and is staffed every day from 8am to 10pm, except Friday, when it is staffed between 8am and 1pm. At all other times, calls to 1100 are sent to the support after-hours mailbox.

```xml
<extension
  name="Time-of-day-tod">
```
<extension name="break-demo">
    <!-- because break=never is set, even when the destination does not begin with 1, we skip the action and keep going -->
    <condition field="destination_number" expression="^1(\d+)$" break="never">
        <action application="set" data="begins_with_one=true"/>
    </condition>
    <condition field="destination_number" expression="^(\d+)$">
        ...other actions that may query begins_with_one...
    </condition>
</extension>

In this example, we use the break=never parameter to cause the first condition to 'fall-through' to the next condition no matter if the first condition is true or false. This is useful to set certain flags as part of extension processing. This example sets the variable begins_with_one if the destination number begins with 1.
**Variables**

Condition statements can match against channel variables, or against an array of built in variables.

**Built-In Variables**

The following variables, called 'caller profile fields', can be accessed from condition statements directly:

- **context** Why can we use the context as a field? Give us examples of usages please.
- **rdnis** Redirected Number, the directory number to which the call was last presented.
- **destination_number** Called Number, the number this call is trying to reach (within a given context)
- **dialplan** Name of the dialplan module that are used, the name is provided by each dialplan module. Example: XML
- **caller_id_name** Name of the caller (provided by the User Agent that has called us).
- **caller_id_number** Directory Number of the party who called (caller) -- can be masked (hidden)
- **ani** Automatic Number Identification, the number of the calling party (caller) -- cannot be masked
- **aniii** The type of device placing the call ANI2
- **uuid** Unique identifier of the current call? (looks like a GUID)
- **source** Name of the FreeSWITCH module that received the call (e.g. PortAudio)
- **chan_name** Name of the current channel (Example: PortAudio/1234). Give us examples when this one can be used.
- **network_addr** IP address of the signaling source for a VoIP call.
- **year** Calendar year, 0-9999
- **yday** Day of year, 1-366
- **mon** Month, 1-12 (Jan = 1, etc.)
- **mday** Day of month, 1-31
- **week** Week of year, 1-53
- **mweek** Week of month, 1-6
- **wday** Day of week, 1-7 (Sun = 1, Mon = 2, etc.) or "sun", "mon", "tue", etc.
- **hour** Hour, 0-23
- **minute** Minute of the hour, 0-59
- **minute-of-day** Minute of the day, 1-1440 (midnight = 1, 1am = 60, noon = 720, etc.)
- **time-of-day** Time range formatted: hh:mm[ss]-hh:mm[ss] (seconds optional) Example: "08:00-17:00"
- **date-time** Date/time range formatted: YYYY-MM-DD hh:mm[ss]-YYYY-MM-DD hh:mm[ss] (seconds optional, note tilde between dates) Example: 2010-10-01 00:00:01~2010-10-15 23:59:59

```
<condition field="network_addr"
expression="^192\.[1-6]\.[1-6]\.[1-6]$"/>
<!-- network address=192.168.1.1 -->

<condition mon="2"> <!-- month=February -->
```

**Caller Profile Fields vs. Channel Variables**

One thing that may seem confusing is the distinction between a caller profile field (the built-in variables) and a channel variable.

Caller profile fields are accessed like this:

```
<condition
field="destination_number" attributes...>
```

While channel variables are accessed like this:

```
<condition
field="${sip_has_crypto}" attributes...>
```
Please take note of the `${variable_name}` syntax. Channel variables may also be used in action statements. In addition, API functions can be called from inside a condition statement to provide dynamic data.

For example, you can use the **cond** API:

```xml
<condition field="${cond($my_var > 12 ? YES : NO)}" expression="^YES$">
  <action application="log"
    data="INFO $my_var is indeed greater than 12"/>
</condition>
```

This example tests `$my_var`. If it is more than 12, "YES" is returned. Otherwise "NO" is returned. The condition tests the results for "YES" and logs the resulting message to the NSG log.

**Starting the Gateway**

After successful initial configuration, the NSG gateway needs to be started. The Control Panel is used to start, stop, restart the complete NSG gateway. One can also control on the fly configuration in the Profile Panel once the gateway has been started.

- Select **Control Panel** from side/top Overview Menu
- Confirm that warnings are clear
- Start the Media Processing First
  - Media Processing will start the Transcoding resources.
  - Note that Media Processing is optional

- Start the Media Gateway Second.
  - Media Gateway will start
  - TDM Hardware Spans (T1/E1 ports)
  - Netborder SS7 to VoIP Gateway Software

- Confirm that the **boot** button is selected.
  - This will confirm that gateway starts on reboot.
- When the Gateway starts successfully the green status bar will appear.
- System is now running.

- Before attempting to pass traffic through the gateway, proceed to **TDM Status** to check the state of the NSG gateway. There is no point of attempting calls while the status of the gateway protocol is down.