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>-48V</td>
<td>-48V</td>
<td>0V (Ground)</td>
</tr>
<tr>
<td>+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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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></td>
<td>Not used / Not required</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.
<table>
<thead>
<tr>
<th>License Variables</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>
</tbody>
</table>
| SPC               | 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. |
| MAC               | System’s MAC address.  
License code checks the MAC address and confirms if MAC is correct. One can check vs License Information section. |
| CICS              | 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 |

**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/Gateways**

- 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 Name</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>
<tr>
<td></td>
<td>Standalone</td>
<td>Firewall Enabled Warning:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>All active service ports must be explicitly enabled</td>
</tr>
<tr>
<td>Hostname</td>
<td>String</td>
<td>A hostname is the full name of your system.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>If you have your own domain, you can use a hostname like nsg.example.com</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Alternatively, you can also make one up: gateway.lan, mail.lan. The hostname does require at least one period (.)</td>
</tr>
<tr>
<td>Name/DNS Servers</td>
<td>Domain Name or IP address eg. 8.8.8.8</td>
<td>On DHCP and DSL/PPPoE connections, the DNS servers will be configured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>

**Interface Section**

![Network Interface](image_url)

**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>
<tbody>
<tr>
<td>External</td>
<td>Network interface with direct or indirect access to the Internet External interface is used as the system default route. <strong>WARNING:</strong> You should have only ONE external network interface. Usually eth0 is the external interface</td>
</tr>
<tr>
<td>LAN</td>
<td>Connection to your local network Usually eth1 is the LAN interface</td>
</tr>
</tbody>
</table>
| 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. |
| DMZ      | 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>DHCP</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>
</tbody>
</table>
| Static     | If you have a static IP, you will need to set the following parameters:  
  - IP  
  - Netmask (e.g. 255.255.255.0)  
  - Gateway (typically ends in 1 or 254)  
  - Ethernet Options (able to force 100MB or 1000mb) |
| PPPoE DSL  | 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. |
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.

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

<table>
<thead>
<tr>
<th>Route File Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Usage</td>
<td>Use to create static routes for Primary Signaling Ethernet Port:eth0</td>
</tr>
</tbody>
</table>

Usage:

```
(-host|-net) Target[/prefix] [gw Gw] [metric M]
[netmask N] [mss Ms] [window W] [irtt I] [mod] [dyn] [reinstate] [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
```

The IP Route section only allows route add command syntax
Routing Table Status

- Select **VLAN Status** from side/top **Overview** Menu
- Second table shows full system routing table.

VLAN

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

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

```
#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: PERDEVICE # 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.

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>Date/Time</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>Time Zone</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>NTP Time Server</td>
<td>An NTP Time Server is built into NSG.</td>
</tr>
<tr>
<td>Time Synchronization</td>
<td>Hitting the Synchronize Now button will synchronize the system's clock with network time servers.</td>
</tr>
</tbody>
</table>

Megaco/H.248 Media Gateway Configuration

Overview
H.248 or Megaco or Gateway Control Protocol is a recommendation from ITU which defines protocols that are used between elements of a physically decomposed multimedia gateway. It is an implementation of the Media Gateway Control Protocol Architecture (RFC 2805). H.248 is also called Megaco or in IETF domain. It is now known as Gateway Control Protocol.

H.248/Megaco is standard protocol for controlling the elements of a physically decomposed multimedia gateway, which enables separation of call control from media conversion. H.248/Megaco is a master/slave protocol used to separate the call control logic from the media processing logic in a gateway.

The H.248/Megaco model describes a connection model that contains the logical entities, or objects, within the Media Gateways (MGs) that can be controlled by the Media Gateway Controller. The main entities are Contexts and Terminations.

The H.248/Megaco model describes a connection model that contains the logical entities, or objects, within the Media Gateways (MGs) that can be controlled by the Media Gateway Controller. The main entities are Contexts and Terminations.

**Terminations**

These source or sink one or more media streams or control streams. Terminations may be physical or ephemeral.

Physical Terminations represent physical entities that have a semi-permanent existence. For example, a Termination representing ports on the gateway, such as TDM channel or DS0 might exist for as long as it is provisioned in the gateway. Ephemeral Terminations represent Connections or data flows, such as RTP streams, or MP3 streams, and usually exist only for the duration of their use in a particular Context.

Terminations have properties, such as the maximum size of a jitter buffer, which can be inspected and modified by the MGC. A termination is given a name, or Termination ID, by the MG.

**Context**

These are star connections created by associating multiple terminations. A Context is a logical entity on an MG that is an association between a collection of Terminations. A NULL context contains all non-associated terminations. A Context is a logical entity on an MG that is an association between a collection of Terminations. A ContextID identifies a Context.

The normal, "active" context might have a physical termination (say, one DS0 in a DS3) and one ephemeral one (the RTP stream connecting the gateway to the network). Contexts are created and released by the MG under command of the MGC. A context is created by adding the first termination, and it is released by removing (subtracting) the last termination.

A termination may have more than one stream, and therefore a context may be a multistream context. Audio, video, and data streams may exist in a context among several terminations.

**Commands**

The commands defined by megaco are very simple, since they can be heavily extended using packages.

### Sent from controller to gateway

**Add**

- Used to add a termination to a context
- Modify
- Used to modify an existing termination
- Subtract:
  - Used to remove a termination from a context
  - Move:
    - used to move a termination to another context (call-waiting is achieved by moving it to the NULL context, which keeps it opened).

**AuditValue**

- Returns the current values of properties, signals and statistics
- AuditCapabilities:
  - Returns metadata on the current termination (the possible values for all elements)

### 8.2.2 Sent from gateway to controller

**Notify**

- Carries an event defined in one of the packages [P1] ServiceChange:
  - Notifies the controller that the gateway is going out of service / back in service. [P1]

A MEGACO-configured NSG starts by sending a Service Change command to its MGC. When an MGC accepts the NSG registration, the session can start. Subsequently, the NSG responds to MGC commands. Event notifications are sent only if the MGC requests them specifically.
Packages

Additional features are provided in packages, which define additional properties, events and signals that are included in the descriptors used in the protocol’s commands. Packages follow an inheritance model similar to object oriented programming, with some of those defined as “to be extended only” providing only an indicative structure for proprietary implementation.

Some properties are read-only and others are read-write, for more information refer to H.248.1 Appendix E.

Create MG Profile

Media gateway profile will contains all the required configuration parameters to bring up the Media gateway stack.

- Select MG from the side/top Configuration menu
- Select Add New Profile

o Use default profile name, or specify one

- Select Create Media Gateway Profile

  - Configure the MG Profile based on information received from our provider.
  - Select Update Media Gateway Profile to save

Followings are the fields, that need to be configured.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible values</th>
<th>Default Values</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>MEGACO MGCP</td>
<td>MEGACO</td>
<td>Type of protocol Media Gateway is going to use.</td>
</tr>
<tr>
<td><strong>Message Type Identifier</strong></td>
<td><strong>IP-PORT IP DOMAIN</strong></td>
<td><strong>IP-PORT</strong></td>
<td></td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>NOTE: Currently Media Gateway supports only MEGACO</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Media gateway message identifier (MID) type field will be used to build the message identifier field which Media Gateway will use in all the originating messages.

For example:

- If MID type is IP-PORT then Message identifier format will be `[@IP-Address]:Port`
- If MID type is DOMAIN then message identifier format will `<Domain>`. Refer to Domain section below.
- If MID type is IP then message identifier format will `[@IP-Address]`

Note: IP-Address, Port and Domain values will be as defined above.

<table>
<thead>
<tr>
<th><strong>Signaling IP</strong></th>
<th><strong>any ipv4 addr</strong></th>
<th><strong>NA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Gateway, Megaco, source IP address.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Port</strong></th>
<th><strong>1 - 65000</strong></th>
<th><strong>NA</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Gateway source Port.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Domain</strong></th>
<th><strong>(a string value)</strong></th>
<th><strong>NA</strong></th>
</tr>
</thead>
</table>
| Media Gateway domain name.  
Used as MID Type, when MID Type is set to DOMAIN. Ignored if MID Type is not Domain. Default to system domain name. |

<table>
<thead>
<tr>
<th><strong>Megaco Version</strong></th>
<th><strong>1</strong></th>
<th><strong>2</strong></th>
<th><strong>3</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Megaco protocol version which Media Gateway will use while communicating with Media Gateway Controller</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>T.38 Fax</strong></th>
<th><strong>Enable/Disable</strong></th>
<th><strong>Enable</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>If enable MG will configure to detect and send CNG/CED Fax notify events to MGC. This will prompt MGC to modify the RTP stream to T.38. If disable MG will not notify MGC about</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>RTP IP</strong></th>
<th><strong>any ipv4 addr</strong></th>
<th><strong>Same as Signaling IP.</strong></th>
</tr>
</thead>
</table>
| Megaco RTP source IP address.  
By default it should be set to Signaling IP address, this way both signaling and media originate from single IP address.  
In VLAN scenarios it’s possible to use separate IP addresses for Signaling and RTP. |

<table>
<thead>
<tr>
<th><strong>Termination-ID Prefix</strong></th>
<th><strong>any number starting from 1</strong></th>
<th><strong>NA</strong></th>
</tr>
</thead>
</table>
| RTP termination id prefix which Media Gateway will use while allocating RTP terminations.  
This variable is used as a name of RTP termination. Eg: RTP/1, RTP/2 ... |

**Create MG Peer Profile**
Each Media gateway profile will associate with one or multiple peers. NOTE: As of now NSG supports only "one peer per MG profile".

- Select **Add Peer** in MG Section
- Fill in the peer information
- Select **Update** to Save

Followings are the fields which need to be configured.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible values</th>
<th>Default Values</th>
<th>Description</th>
</tr>
</thead>
</table>
| Message Identifier Type        | IP-PORT IP      | IP-PORT        | Media gateway Controller message identifier (MID) type field will be used by Media Gateway to identify the peer.
|                                |                 |                | Message identifier value will be built based on MID type field.
<p>|                                |                 |                | For example:                                                               |
|                                |                 |                | If MID type is IP-PORT then Message identifier format will be               |
|                                |                 |                | &quot;[IP-Address]:Port&quot;                                                        |
|                                |                 |                | If MID type is IP then message identifier format will                       |
|                                |                 |                | &quot;[IP-Address]&quot;                                                             |
|                                |                 |                | Note: IP-Address and Port values will be as defined above.                 |
| IP Address                     | NA              | NA             | Media Gateway Controller IP address.                                       |
| Port                           | NA              | 2944           | Media Gateway Controller Port number Default: 2944                        |
| H.248 Encoding Scheme          | TEXT BINARY     | TEXT           | Encoding scheme of MEGACO protocol which will be used by Media              |</p>
<table>
<thead>
<tr>
<th>Transport Protocol</th>
<th>UDP TCP SCTP</th>
<th>UDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway while encoding/decoding the H.248 messages.</td>
<td>Media Gateway will use the transport type field to decide which transport to use for transmitting/receiving MEGACO messages.</td>
<td>NOTE: currently we are supporting only UDP/TCP.</td>
</tr>
</tbody>
</table>

- Once the **Media Peer** is configured the Megaco configuration section is complete.
- Proceed to **TDM Termination for Media Gateway**

### TDM Termination for Media Gateway

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

---

**Identify**

- 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.
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**

- 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
• 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
When configuring TDM Terminations for Megaco 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

---

After T1/E1 configuration, the NSG wizard will request **Link Type** Configuration.

**Span Link Type**

When configuring TDM Terminations for Megaco 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 = Signaling Gateway (M2UA)

• If configuring for **Voice Mode** select **No Signaling Link**
• If configuring for **Mixed Mode** select **Signaling Gateway (M2UA)**

Signaling Gateway Overview

NSG supports Signaling Gateway operation mode.

In Signaling gateway mode, NSG will bridge T1/E1 SS7 signaling link to IP and pass it transparently to the MGC/Softswitch, via M2UA protocol. Looking at the diagram below, NSG Signaling Gateway will configure:

• MTP1 & MTP2 protocols over the TDM port
• M2UA/SCTP protocol over IP network
• NIF (Network interworking function) to bridge the two
MTP1/2 Link Configuration

- Specify MTP1/2 information based on provider provision document
- Step 1: Identify which channel on T1/E1 line will carry signaling
- Step 2: Specify MTP2 signaling information based on provision document
- Step 3: Specify M2UA Interface ID based on provision document
- **Apply to Port** to save configuration

<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>NA</td>
<td>NA</td>
<td>M2UA Profile name</td>
</tr>
</tbody>
</table>
Next section in WebUI will relate to M2UA configuration. Before we proceed however, the M2UA interface architecture will be introduced in order to provide a big picture to the user.

### M2UA Interface

This section provides in-depth overview on how the M2UA interface is constructed. It should help the user better understand the WebUI configuration objects for M2UA protocol.

WebUI for M2UA contains 3 sections: Cluster, Peer and SCTP

- SCTP interfaces are standalone objects on which a peer bind to (regardless of its cluster).
  - 1 SCTP binds to 1 or more peers
  - 1 peer binds to 1 SCTP
  - Thus SCTP are shared across all peers
  - SCTP cannot be deleted if used by any peer (even from another cluster).
  - Deleting a peer or a cluster does not delete SCTP.
- Peers are bound to cluster.
  - 1 peer binds to 1 cluster
  - 1 cluster binds to 1 or more peer
  - Deleting a cluster will delete peers.
- Cluster are bound to MTP2 through M2UA binding and nif interface
  - 1 cluster binds to 1 or many MTP2 (through M2UA->NIF relationship)
  - 1 MTP2 binds to 1 cluster through NIF interface binding
M2UA Cluster Creation

M2UA Cluster is a group of peers to which M2UA SG will communicate

- Select Create Cluster
- Leave the Cluster values default unless the provider specifies otherwise.
- Select Save to Continue

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic Mode</td>
<td>Load Share Override Broadcast</td>
<td>Load Share</td>
<td>This parameter defines the mode in which this Cluster is supposed to work.</td>
</tr>
</tbody>
</table>
Load Sharing Method

<table>
<thead>
<tr>
<th>Load Sharing Method</th>
<th>Round Robin Link Specified</th>
<th>Customer Specified</th>
<th>Round Robin</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This parameter defines the load share algorithm which is used to distribute the traffic</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**M2UA Cluster Peers**

M2UA Peers will be configured under the M2UA clusters

- Select **Add** under Cluster Peers Profile
- Select **Create** Cluster Peer Profile
- Specify the Cluster Peer parameters based on provider provision document

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include ASP ID</td>
<td>Disable Enable</td>
<td>Disable</td>
<td>Flag used to indicate whether include the ASP ID in the ASP UP message</td>
</tr>
<tr>
<td>ASP Identifier</td>
<td>NA</td>
<td>NA</td>
<td>ASP identifier for this ASP node. Set to 1 in case ASP is Disabled</td>
</tr>
<tr>
<td>Initialize SCTP</td>
<td>Disable Enable</td>
<td>Disable</td>
<td>Flag used to indicate if M2UA SG has to start SCTP association or not.</td>
</tr>
<tr>
<td>Association</td>
<td></td>
<td></td>
<td>If Disable means M2UA SG will wait for SCTP association request from MGC.</td>
</tr>
</tbody>
</table>
If Enable that means M2UA SG will initiate the SCTP association request towards MGC.

<table>
<thead>
<tr>
<th>Destination IP Address(es)</th>
<th>NA</th>
<th>NA</th>
<th>Destination IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination port</td>
<td>NA</td>
<td>2904</td>
<td>Destination ASP Port</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Default M2UA ASP port: 2904</td>
</tr>
<tr>
<td>Number of Outgoing Streams</td>
<td>NA</td>
<td>10</td>
<td>Number of outgoing streams supported by this association. Default 10</td>
</tr>
</tbody>
</table>

**SCTP Interface**

- Select Add SCTP Interface
- Select Create SCTP Interface
- Specify SCTP Information based on provider provision document

**Binding all components**

- All components have been created
  - M2UA Cluster
  - M2UA Peer
  - SCTP Interface
- Next step is to Bind / Connect them together
  - SCTP interface into M2UA Peer
  - M2UA peer into M2UA Cluster

![Select Bind](image_url)
Mixed Mode Configuration

- Signaling is bridged by M2UA to the MGC/Soft switch
- Voice is controlled by Megaco/H.248
- Specify that Voice is part of this TDM Span

Rest of this section will document the Mixed Mode Configuration
**Bind Megaco to TDM**

The last step of the configuration is to bind the TDM voice channels to Megaco Profile

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Possible Values</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Gateway Profile</td>
<td>List of Gateways</td>
<td>First in the List</td>
<td>Select Megaco Profile that will be used to control the TDM channels for this span.</td>
</tr>
<tr>
<td>Termination ID Prefix</td>
<td>NA</td>
<td>NA</td>
<td>Usually a letter A-Z. This prefix is defined by MGC. Please refer to MGC configuration.</td>
</tr>
<tr>
<td>Termination ID Base</td>
<td>NA</td>
<td>NA</td>
<td>Usually a number starting from 1. This value is defined by MGC. Please refer to MGC configuration.</td>
</tr>
<tr>
<td>Channel Map</td>
<td>NA</td>
<td>NA</td>
<td>List of channels to be controlled by Megaco Example: 1-15,s16,17-31 Channels 1-15 and 17-31 are used for Voice and should be controlled by Megaco Channel 16 (prefixed by letters) indicates that channel 16 carries signaling channel. Megaco will ignore this channel as it’s not voice. Prefix Letters to signaling channel: s: megaco id not used, id mapped to signaling channel g: megaco id is used, id mapped to next available voice channel. The bind between megaco and TDM would be as follows Channel Map: 1—31 (no signaling channel) A1: channel 1 A2: channel 2</td>
</tr>
</tbody>
</table>
TDM Termination Complete

- A span has been configured and bound to a Megaco Profile.
- Configuration for this span is done
  - Confirmed in WebUI by a green checkmark.

Next step is to repeat the process for the rest of the spans.
- In typical configurations there is one or two spans (T1/E1 ports) that contain signaling channels. The rest of the spans are usually voice only.
- In voice only config, there is no Signaling Gateway configuration.
  - The configuration jumps directly to “Bind TDM to Megaco” section of the WebUI.

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

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.
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 **Configuration 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

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
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.

• The generate config option will not be offered in case NSG gateway is started. Confirm that NSG is fully stopped in Control Panel before Applying configuration.
When the Gateway starts successfully the green status bar will appear.
System is now running.

Configure Additional MG profiles and spans

Profile Panel is used for on the fly configuration without disrupting gateway service. The NSG Gateway has to be started in order to use the Profile Panel.

While the NSG Gateway is running, one can

- Add a new TDM Voice span to existing MG Profile
- Add a new TDM Voice + M2UA SG span to existing MG Profile
- Add a new MG Profile and new TDM Spans and M2UA SG

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.
Each MG Profile is grouped with the TDM Spans associated with it.

- Sync/Stop actions will only affect the selected MG Profile and Spans that are not in Sync.
- Adjacent MG Profiles will not be affected.

**Configuration**

- Select **Profile Panel** from side/top **Overview** Menu
- Select **Sync** Button to apply and start new configuration.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>In Use</td>
<td>Indicates whether the profile is currently running in NSG Gateway</td>
</tr>
<tr>
<td>Config</td>
<td>Indicates whether the profile configuration in database is in sync with what is currently running in the gateway.</td>
</tr>
<tr>
<td>Sync Button</td>
<td>Configure and Start any profile that is In Active or out of Sync.</td>
</tr>
<tr>
<td></td>
<td>Sync operation WILL NOT disrupt service of TDM Spans that are in sync.</td>
</tr>
<tr>
<td></td>
<td>Sync operation WILL Restart the MG (Megaco) profile in order to update termination ids.</td>
</tr>
<tr>
<td>Stop Button</td>
<td>Used to stop the whole MG Profile and associated TDM Spans.</td>
</tr>
</tbody>
</table>