



## **Configuration Guide**

**for**

**Sipera IPCS 210/310/410/510**

**Version: 3.6**

**with**

**Nortel Communication Server 1000**

**Release 5.5**

**Issue 1.0**

**November 2008**

**Sipera Systems  
1900 Firman Drive  
Suite 600  
Richardson, TX 75081**

## Table of Contents

Table of Contents .....	2
Objective .....	3
IPCS SIP Trunking Overview .....	3
Configuration Steps .....	4
Step 1: IP Addresses .....	4
Step 2: Signaling Interfaces .....	5
Step 3: Media Interfaces .....	6
Step 4: Topology Hiding Profile for Line-side CS 1000 .....	7
Step 5: Topology Hiding Profile for Trunk-side CS 1000.....	8
Step 6: Routing Profile for Line-side CS 1000 .....	9
Step 7: Routing Profile for Trunk-side CS 1000 .....	10
Step 8: CS 1000 Interworking Profile – General Tab.....	11
Step 9: CS 1000 Interworking Profile – Advanced Tab .....	12
Step 10: Server Configuration for Line-side CS 1000 – General .....	13
Step 11: Server Configuration for Line-side CS 1000 – Advanced.....	14
Step 12: Server Configuration for Trunk-side CS 1000 - General .....	15
Step 13: Server Configuration for Trunk-side CS 1000 - Advanced.....	16
Step 14: Server Flows for Line-side CS 1000 .....	17
Step 15: Server Flows for Trunk-side CS 1000 .....	18

## Objective

The aim of this document is to provide guidelines to configure IPCS 210/310/410/510 in a SIP trunking deployment interoperating with Nortel CS 1000 platforms on the line side as well as the trunk side.

## IPCS SIP Trunking Overview

The Sipera IPCS SIP Trunking solution provides connectivity to IP private branch exchanges (IP PBXs). The SIP trunk provides direct access to the customer premise-based IP PBX via SIP signaling, and complements the existing features of the IP PBX. The SIP trunk architecture has the following components-

- Line-side IP-PBX (CS 1000) provides the call control, call capacity, voice mail, etc.
- Sipera IPCS is the SBC which hides the network topology, providing network security and the demarcation point between the remote call server and the peer/enterprise call server.
- Trunk-side IP-PBX (CS 1000) provides call routing and phone service at the remote site.

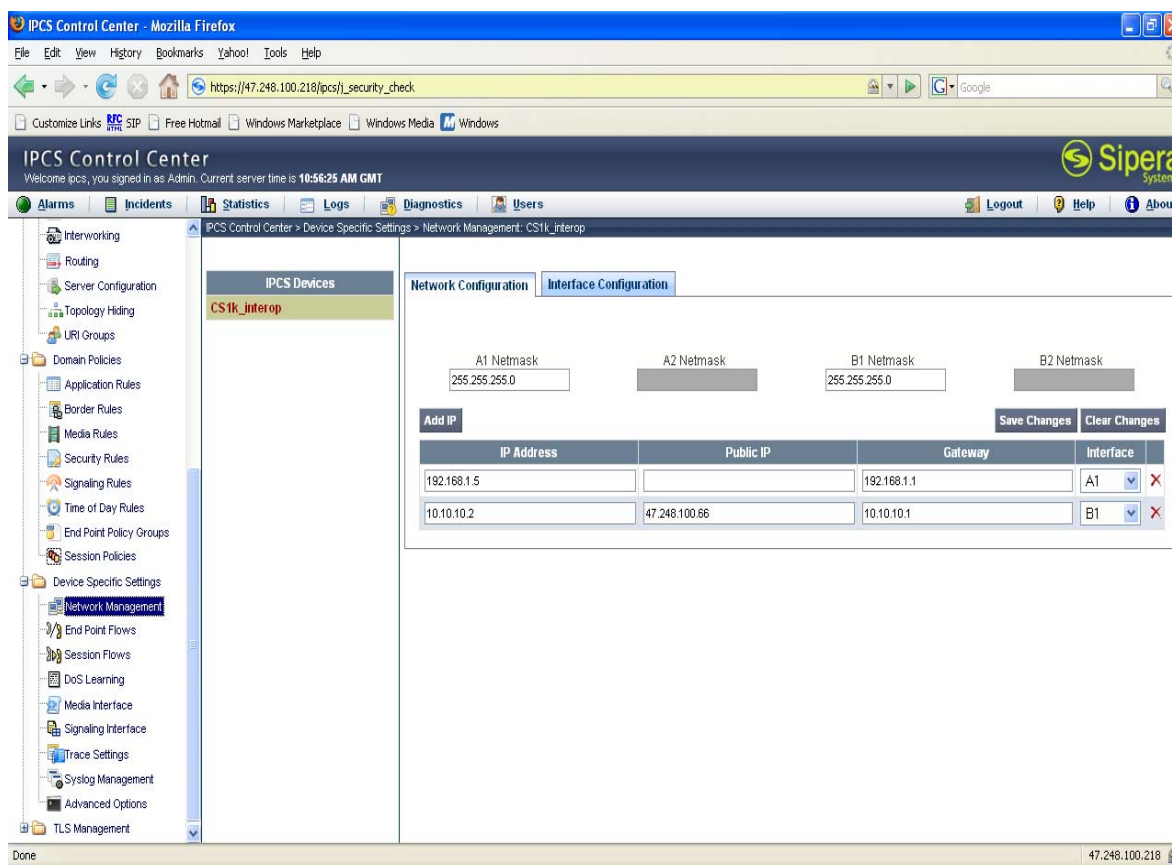
## Configuration Steps

### Step 1: IP Addresses

**Goto “Device Specific Settings” → “Network Management” → “Network Configuration”**

Configure the IP addresses, subnet mask and the default gateways for the network interfaces on IPCS. This step requires the configuration of a minimum of two IP addresses, one for communication between IPCS and the line side CS 1000, and the other for communication between IPCS and the trunk side CS 1000. The two IP addresses, if on the same subnet, can be configured on the same network interface (single-wire mode). If the IP addresses are on different subnets, they must be configured on two separate network interfaces (two-wire mode).

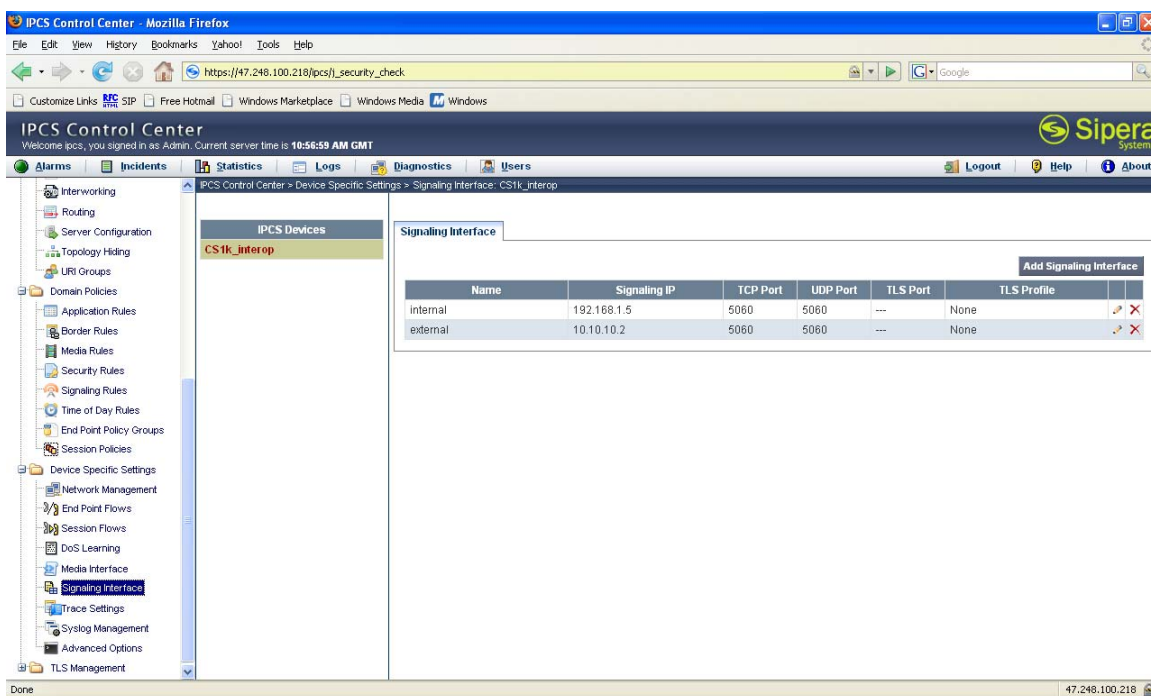
For the trunking configuration in ‘Enterprise NAT’ mode, the Public IP on the B1 interface (interfacing to the trunk-side CS 1000) must be configured as the enterprise NAT’s public IP. In a ‘No NAT’ deployment scenario the Public IP configuration is not needed.







## Step 2: Signaling Interfaces

Goto “Device Specific Settings” → “Signalling Interface” → “Add Signaling Interface”

The signaling interfaces for the IP addresses already configured on the IPCS must be configured with the transport protocol supported on each interface. This will be used for signaling to a logical name, which will be later tied to Server flows.



The screenshot shows the SIPera IPCS Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL [https://47.248.100.218/ipcs/\\_security\\_check](https://47.248.100.218/ipcs/_security_check). The interface includes a navigation menu on the left with categories like Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The main content area is titled "IPCS Control Center > Device Specific Settings > Signaling Interface: CS1k\_interop". It features a table of signaling interfaces and an "Add Signaling Interface" button.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
internal	192.168.1.5	5060	5060	---	None	 
external	10.10.10.2	5060	5060	---	None	 

### Step 3: Media Interfaces

Goto “Device Specific Settings” → “Media Interface” → “Add Media Interface”

The media interfaces for the IP addresses already configured on the IPCS must be configured to assign a logical name to the port ranges used for RTP. This will be tied to Server flows.

The screenshot shows the IPCS Control Center web interface in a Mozilla Firefox browser. The address bar shows the URL [https://47.248.100.218/ipcs/\\_security\\_check](https://47.248.100.218/ipcs/_security_check). The interface has a navigation menu on the left with categories like Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. Under 'Device Specific Settings', the 'Media Interface' option is selected. The main content area shows the configuration for the device 'CS1k\_interop'. A table lists the configured media interfaces:

Name	Media IP	Port Range		
internal	192.168.1.5	35000 - 40000		
external	10.10.10.2	35000 - 40000		

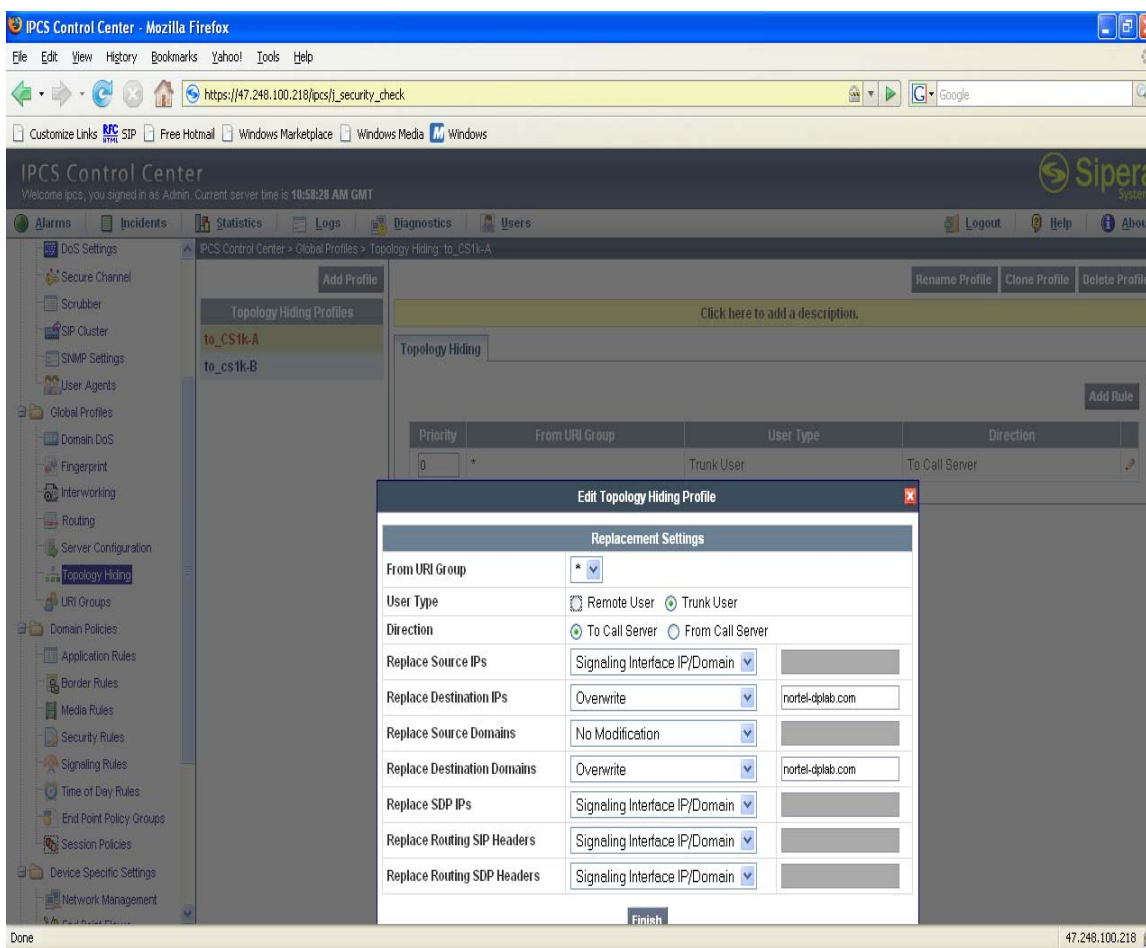
An 'Add Media Interface' button is located at the top right of the table. The status bar at the bottom indicates 'Done' and the IP address '47.248.100.218'.

## Step 4: Topology Hiding Profile for Line-side CS 1000

Goto “Global Profiles” → “Topology Hiding” → “Add Topology Hiding Profile”

Topology Hiding profiles must be configured with the following options:  
 user type defined as ‘Trunk user’,  
 direction defined as ‘To Call Server’

As a result of this configuration, action taken by the topology hiding feature occurs when IPCS is ready to send the SIP message to the call server. The action to be taken by the ‘topology hiding’ feature in both SIP and SDP headers is selected from the drop down menu, as shown in the screen below. The topology hiding profile must be configured for both the line-side and trunk-side CS 1000 servers. The screen below shows the profile configuration for the line-side server.

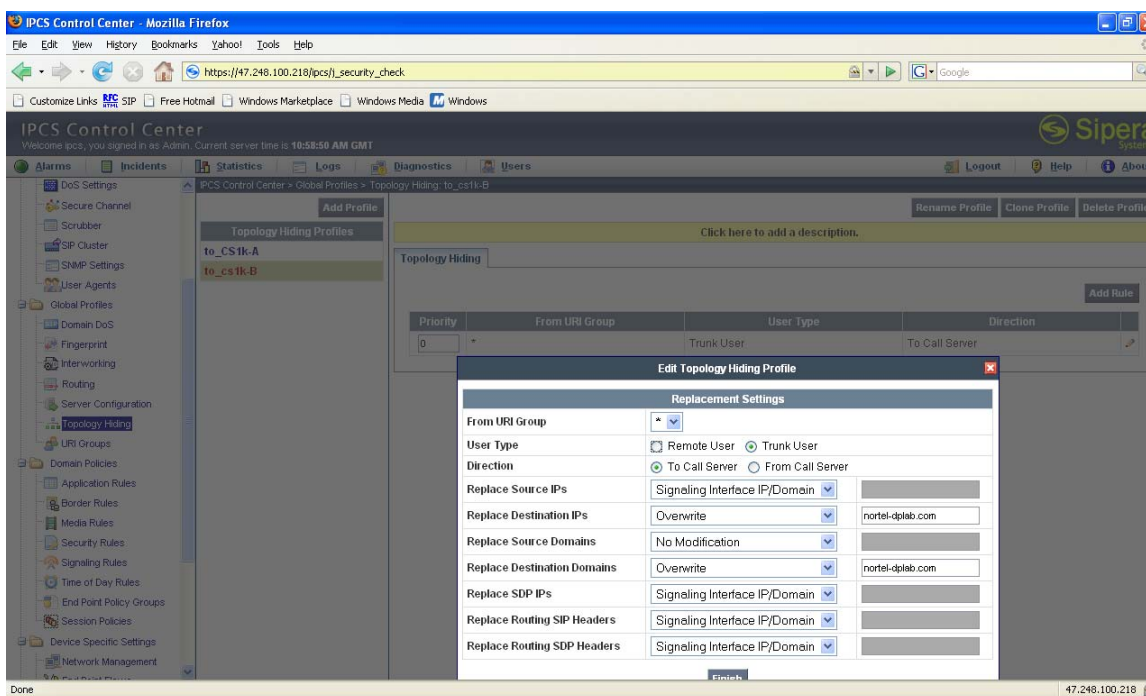


## Step 5: Topology Hiding Profile for Trunk-side CS 1000

Goto “Global Profiles” → “Topology Hiding” → “Add Topology Hiding Profile”

Topology Hiding profiles must be configured with the following options:  
 user type defined as ‘Trunk user’,  
 direction defined as ‘To Call Server’.

As a result of this configuration, action taken by the topology hiding feature occurs when IPCS is ready to send the SIP message to the call server. The action to be taken by the topology hiding feature in both SIP and SDP headers is selected from the drop down menu as shown in the screen below. The topology hiding profile must be configured for both the line-side and trunk-side CS 1000 servers. The screen below shows the profile configuration for the trunk-side server.

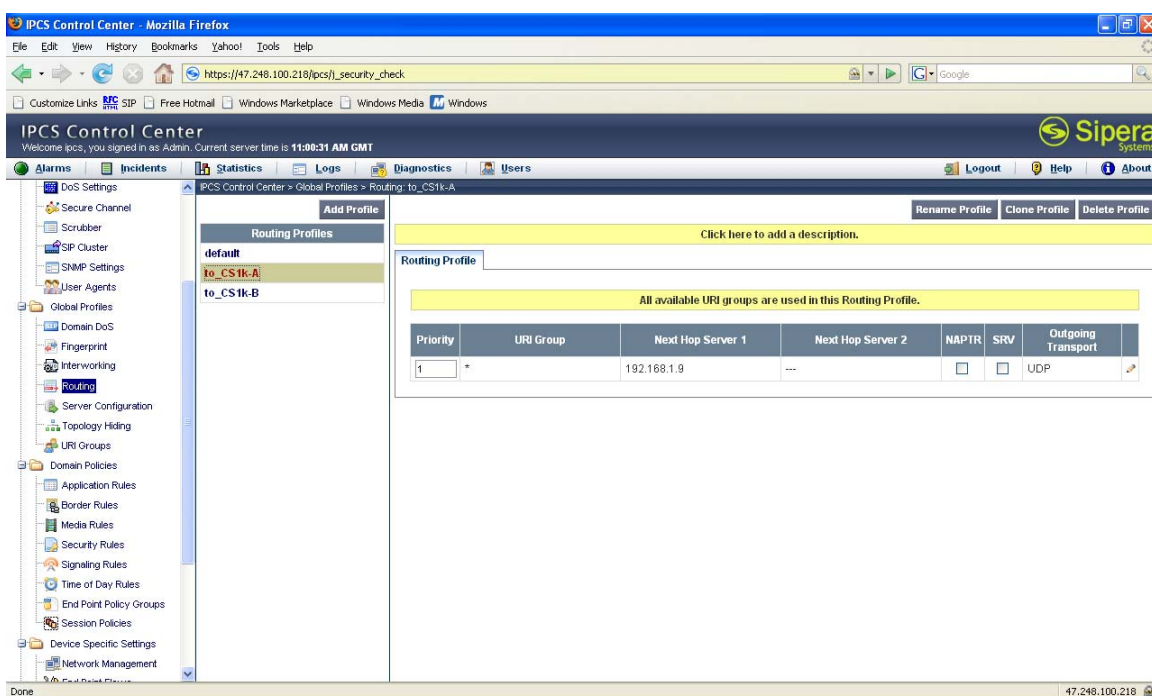




## Step 6: Routing Profile for Line-side CS 1000

Goto 'Global Profiles' → 'Routing' → 'Add Profile'

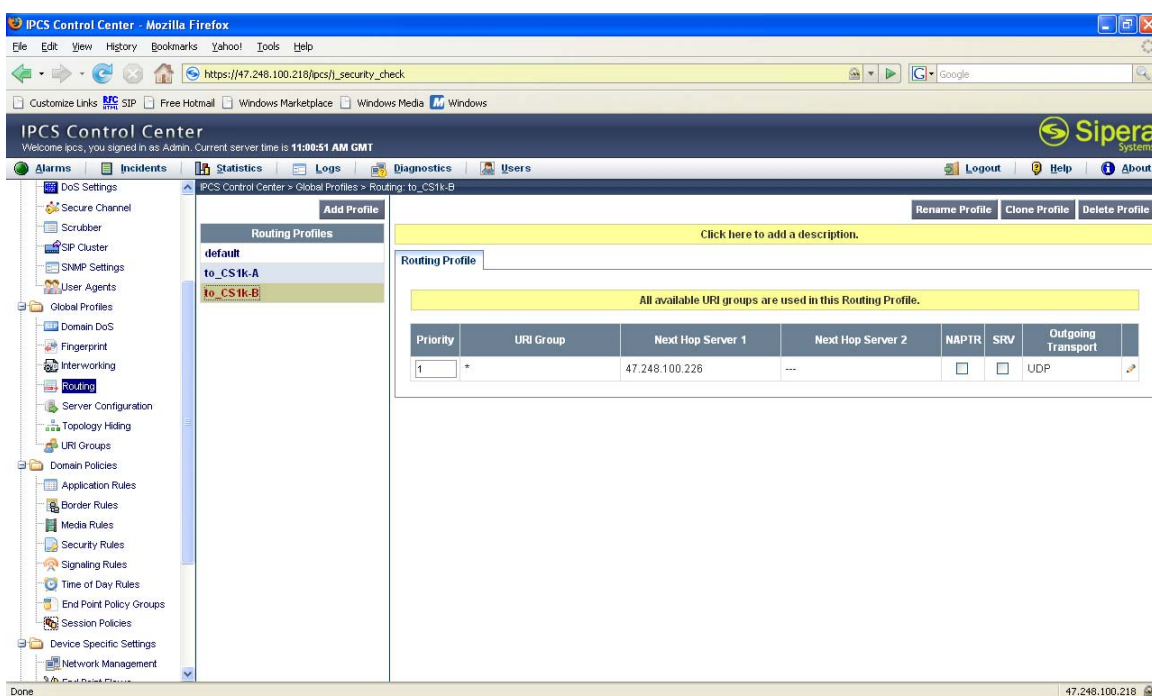
Routing profiles define where SIP packets will be routed when the profile is used in a 'Server Configuration'. The routing can either be 'Next Hop Server'-based or based on DNS (NAPTR, SRV) lookups. The configuration provide below is 'Next Hop server'-based. This profile is used in the server configuration for 'CS 1000-B', which means that any SIP packets originating from the trunk-side server will be routed to the identified IP address, which is the line-side server.



## Step 7: Routing Profile for Trunk-side CS 1000

Goto 'Global Profiles' → 'Routing' → 'Add Profile'

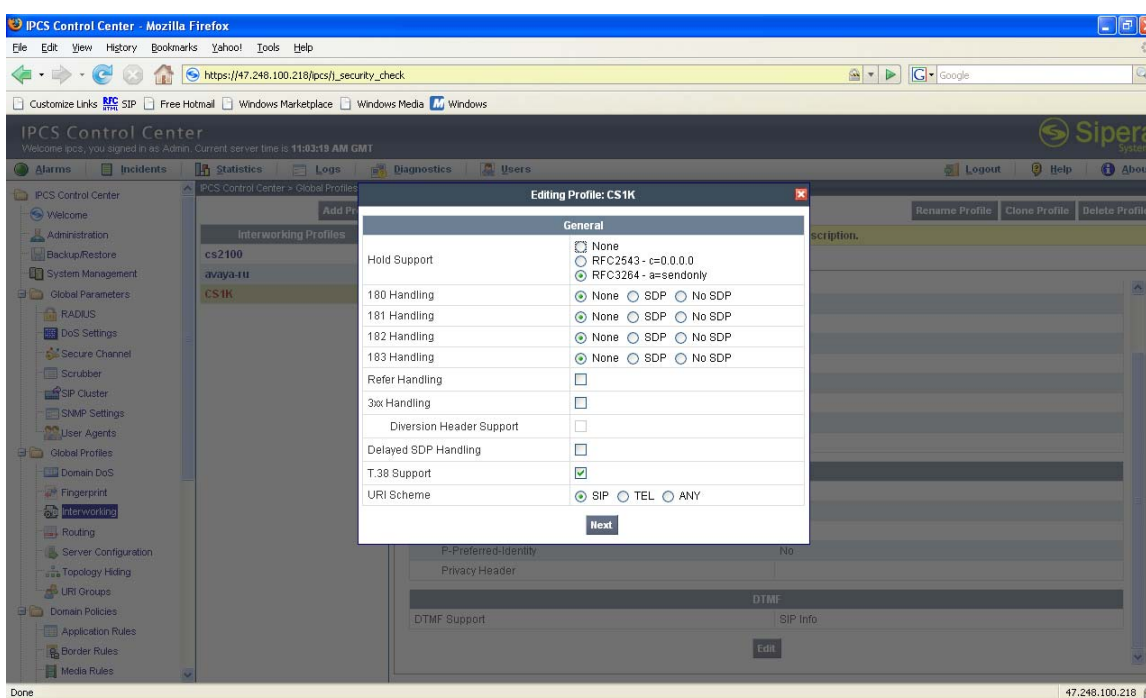
Routing profiles define where SIP packets will be routed when the profile is called in a 'Server Configuration'. The routing can either be 'Next Hop Server'-based, or based on DNS (NAPTR, SRV) lookups. The configuration provided below is 'Next Hop server'-based. This profile is used in the server configuration 'CS 1000-A', which means that any SIP packets originating from the line-side server will be routed to the identified IP address, which is the trunk-side server.



## Step 8: CS 1000 Interworking Profile – General Tab

Goto ‘Global Profiles’ → ‘Interworking’ → ‘Add Profile’

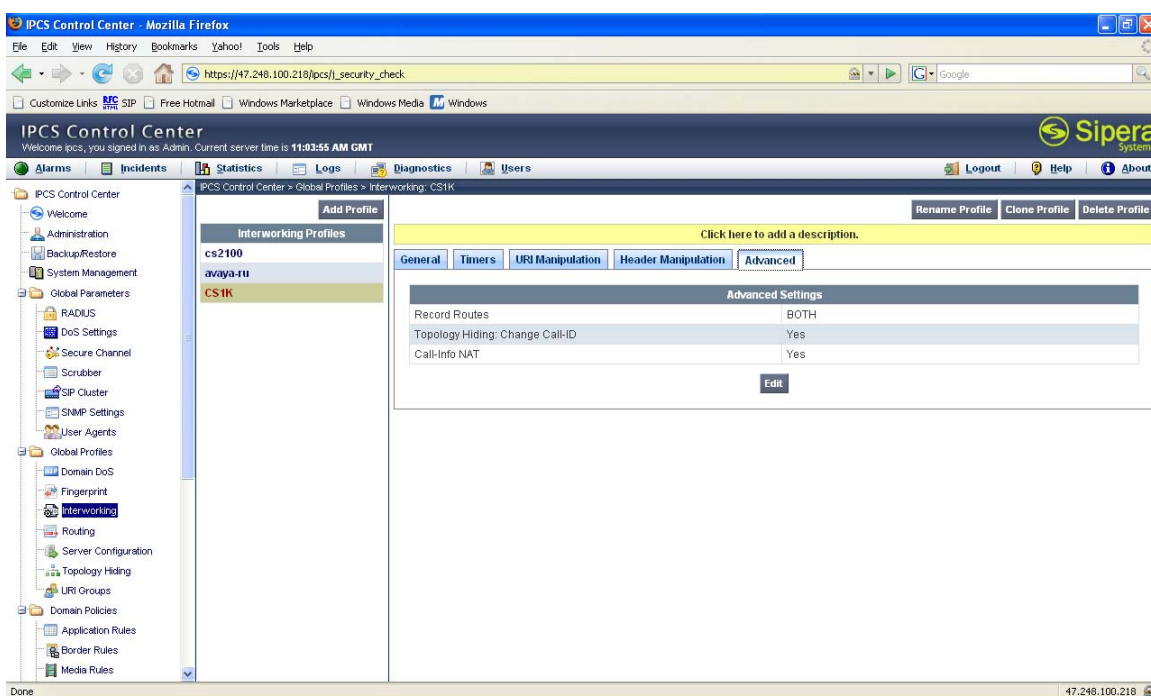
Interworking profiles improve interoperability by enabling communication between servers from different vendors. An interworking profile for CS 1000 is provided below. This profile defines the message handling by IPCS for various messages when communicating to a CS 1000. The profile will be linked to the ‘Server Configuration’. The following screen shows the configuration under the ‘General’ tab in the ‘Interworking Profile’ for CS 1000.



## Step 9: CS 1000 Interworking Profile – Advanced Tab

Goto ‘Global Profiles’ → ‘Interworking’ → ‘Add Profile’

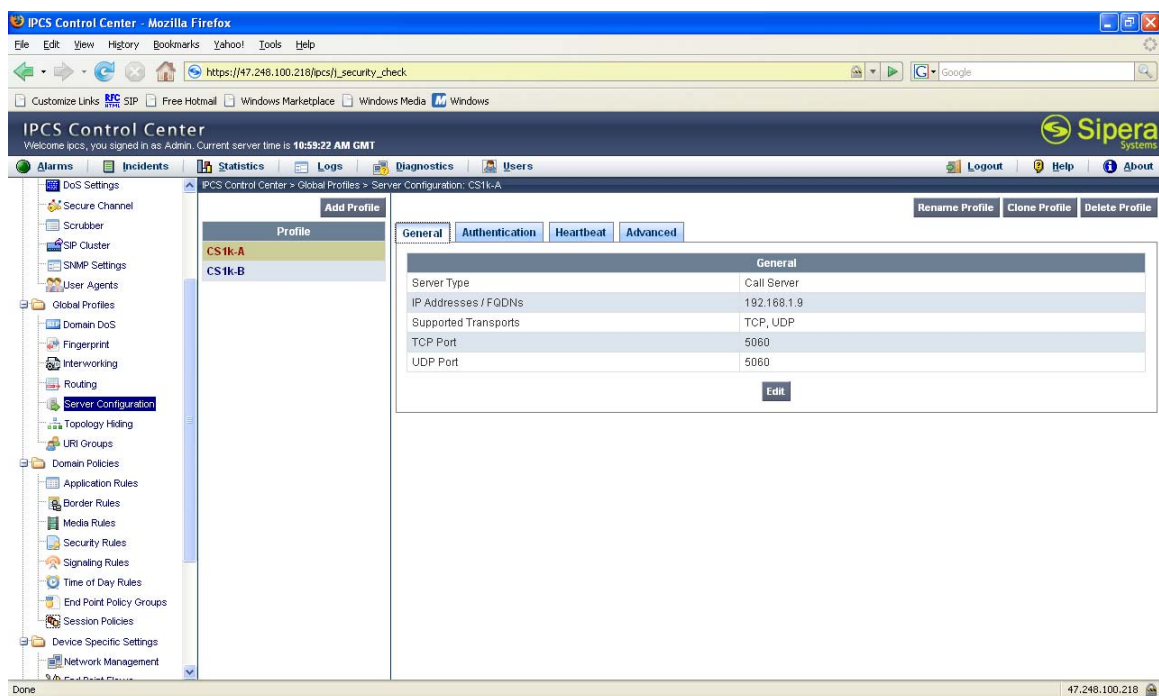
Interworking profiles improve interoperability by enabling communication between servers from different vendors. An interworking profile for CS 1000 is provided below. This profile defines the message handling by IPCS for various messages when communicating to a CS 1000. This profile will be linked to the ‘Server Configuration’. The following screen shows the configuration under the ‘Advanced’ tab in the ‘Interworking Profile’ for CS 1000.



## Step 10: Server Configuration for Line-side CS 1000 – General

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

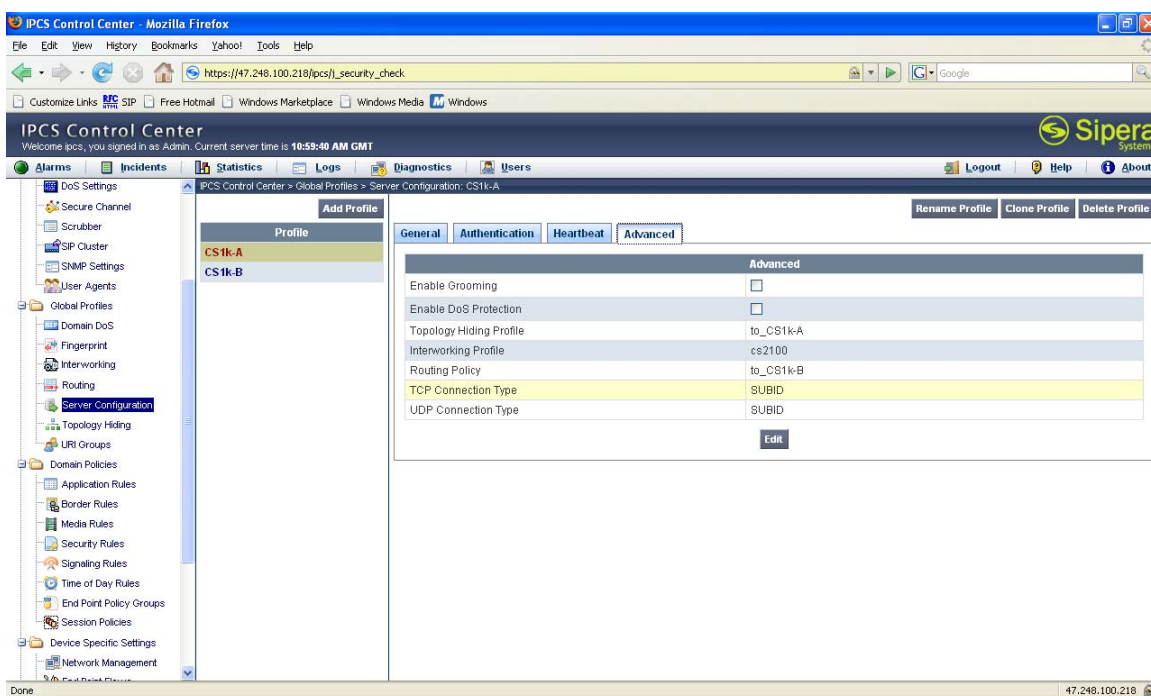
A server configuration must be established for both the line-side and trunk-side CS 1000 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that IPCS will perform when SIP packets are received from the CS 1000 server defined in this ‘Server Configuration’. The following diagram shows the ‘General’ configuration tab including the defined supported transports and port numbers which will be used when communicating with the line-side CS 1000 server.



## Step 11: Server Configuration for Line-side CS 1000 – Advanced

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

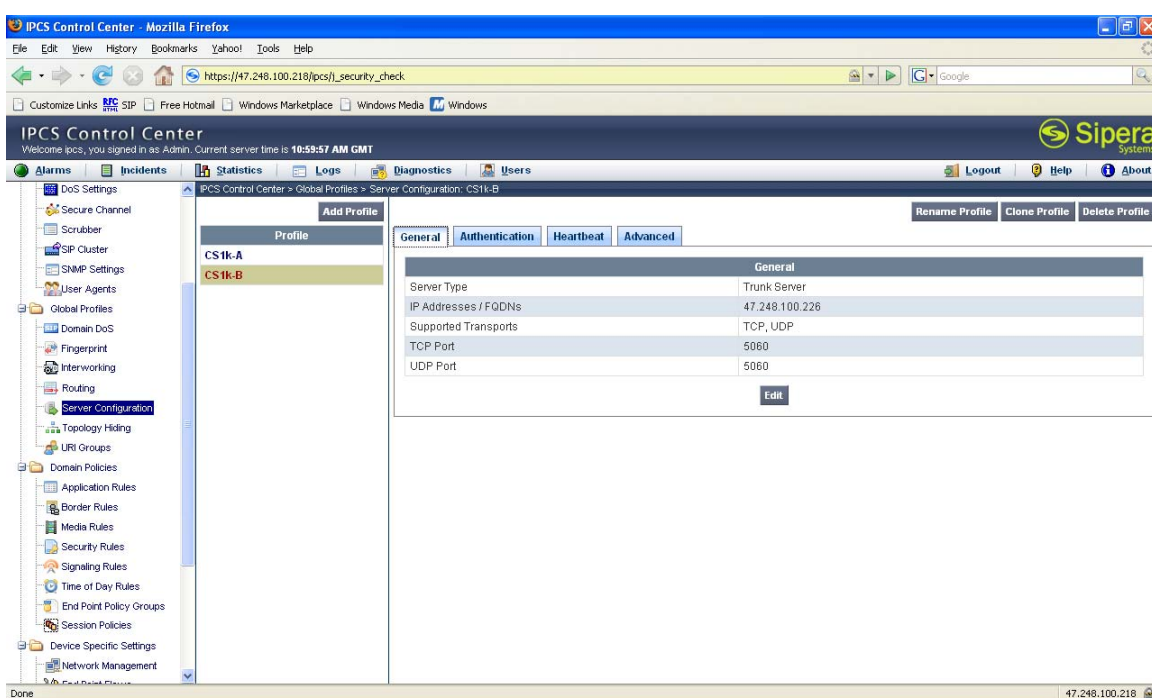
A server configuration must be established for both the line-side and trunk-side CS 1000 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that IPCS will perform when SIP packets are received from the CS 1000 server defined in this ‘Server Configuration’. The following diagram shows the ‘Advanced’ configuration tab including the ‘Topology Hiding’ profile, ‘Routing policy’ and ‘Interworking Profile’, for this ‘Server Configuration’.



## Step 12: Server Configuration for Trunk-side CS 1000 - General

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

A server configuration must be established for both the line-side and trunk-side CS 1000 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that IPCS will perform when SIP packets are received from the CS 1000 server defined in this ‘Server Configuration’. The following diagram shows the ‘General’ configuration tab including the supported transports and the port numbers which will be used when communicating with the trunk-side CS 1000 server.

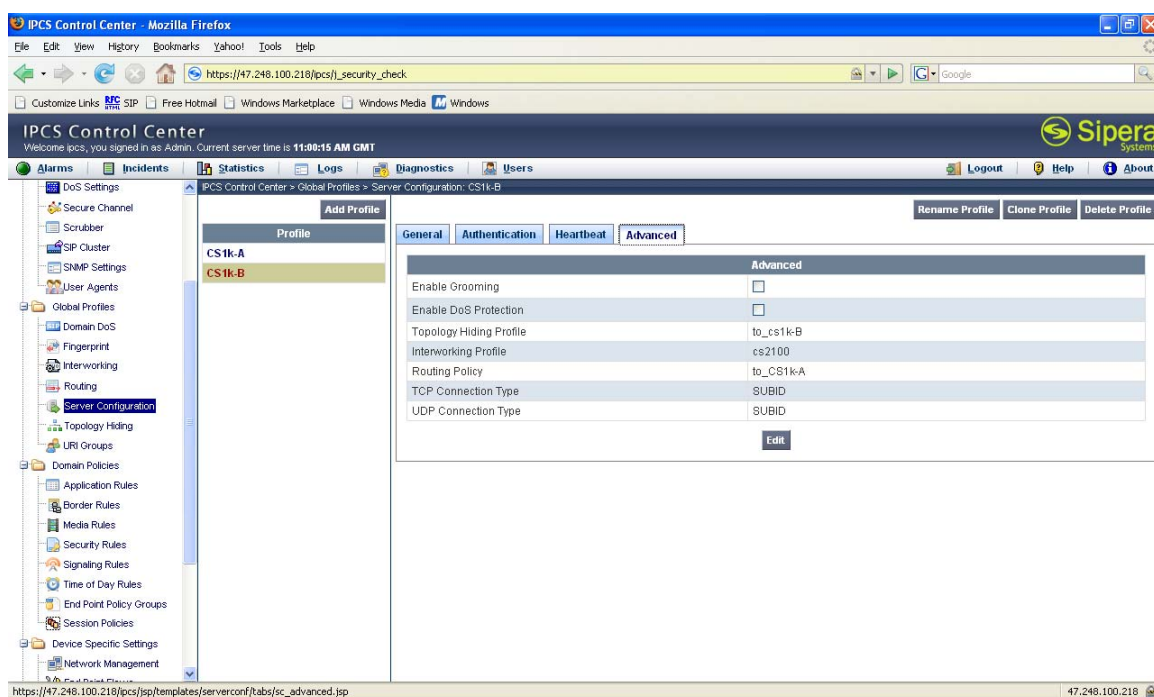




## Step 13: Server Configuration for Trunk-side CS 1000 - Advanced

Goto “Global Profiles” → “Server Configuration” → “Add Profile”

A server configuration must be established for both the line-side and trunk-side CS 1000 servers. The ‘Server Configuration’ is a set of properties along with a list of actions that IPCS will perform when SIP packets are received from the CS 1000 server defined in this ‘Server Configuration’. The following diagram shows the ‘Advanced’ configuration tab, including the ‘Topology Hiding’ profile, ‘Routing policy’ and ‘Interworking Profile’ for this ‘Server Configuration’.

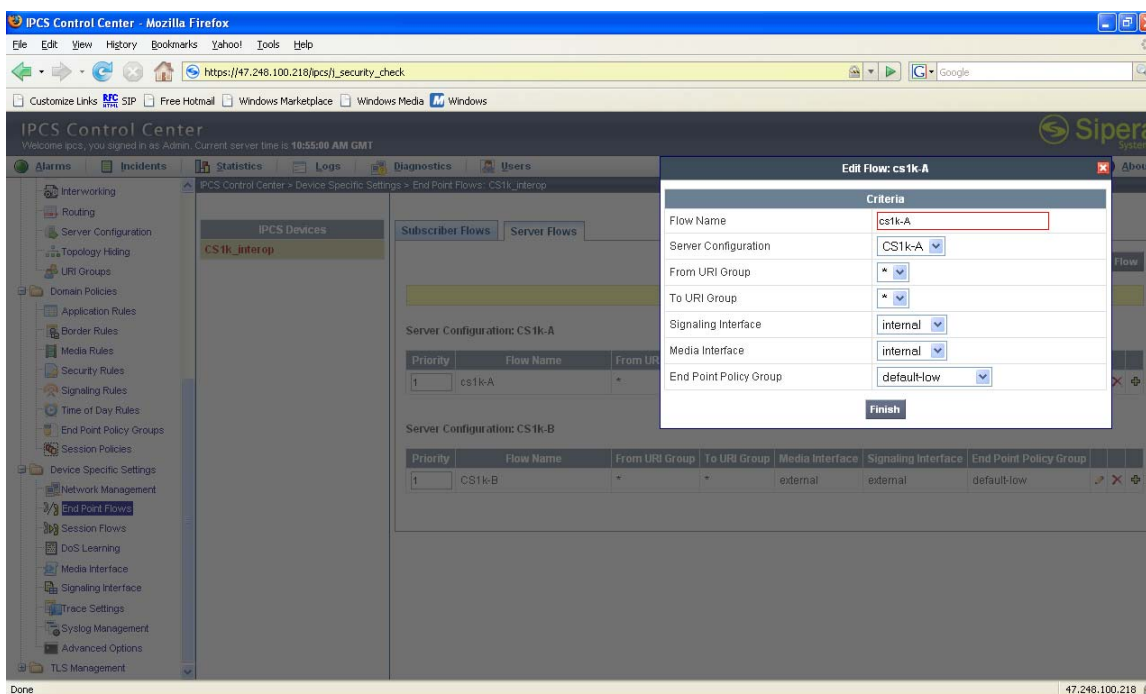




## Step 14: Server Flows for Line-side CS 1000

Goto “Device Specific Settings” → “Server Flows” → “Add Flow”

Server flows must be configured for both the line-side and trunk-side CS 1000 servers. The following configuration shows that any SIP and RTP packets arriving on the internal signaling and media interfaces are tied to the server flow for CS 1000-A, which is the line-side server. The properties defined in the ‘Server Configuration’ named ‘CS 1000-A’ and the ‘End-Point Policy Group’ named ‘default-low’ are applied to this server flow. The ‘End-Point Policy Group’ is a set of security configuration profiles for a particular group. As the security configuration is not within the scope of this document, a detailed configuration and explanation is not provided.



## Step 15: Server Flows for Trunk-side CS 1000

Goto “Device Specific Settings” → “Server Flows” → “Add Flow”

Server flows must be configured for both the line-side and trunk-side CS 1000 servers. The following configuration shows that any SIP and RTP packets arriving on the external signaling and media interfaces are tied to the server flow for CS 1000-B which is the trunk-side server. The properties defined in ‘Server Configuration’ named ‘CS 1000-B’ and the ‘End-Point Policy Group’ named ‘default-low’ are applied to this server flow. The ‘End-Point Policy Group’ is a set of security configuration profiles for a particular group. As the security configuration is not within the scope of this document, a detailed configuration and explanation is not provided.

