SBCC21

SBC Core Support and Certification

Student Lab Guide

Document Revision: 4.5

RIBBON products and services are produced using a TL 9000 certified Quality Management System.

CERT-0056636

RIBBON Education Services

SBC Core Support and Certification

Software Release number: 9.2

Document release date: January, 2021

NOTICES

Copyright © 2021 Sonus Networks, Inc. (d.b.a. Ribbon Communications Operating Company)("Ribbon"). All rights reserved. Proprietary and Confidential.
This item and the information contained herein are the property of Ribbon. This document, and any software of Ribbon mentioned in this document, whether delivered electronically or via other media, are the sole property of Ribbon and are available only under and pursuant to this agreement.
All copy, reproduction, derivatives (including, without limitation, translation), modification, distribution, republication, transmission, re-transmission and public display or showing of this document, whether in whole or part is strictly prohibited without the prior written permission of an authorized Ribbon representative.

Third-party Copyrights
Open BSD Copyright (c) 1982, 1986, 1990, 1991, 1993. The Regents of the University of California. All rights reserved.
THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the above disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

Warranties
RIBBON, PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS, IMPLIED OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.
Ribbon MAKES NO WARRANTY OF ANY KIND WITH RESPECT TO THE SUBJECT MATTER INCLUDED HEREIN, THE PRODUCTS LISTED HEREIN, OR THE COMPLETENESS OR ACCURACY OF THE INFORMATION. This publication could include technical inaccuracies or typographical errors. Changes may be periodically made to the information herein; these changes will be incorporated in new editions of this publication. Ribbon may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

NOTICES

Ribbon assumes no liability for damages of any kind, or any damages whatsoever resulting from technical errors, editorial errors, omissions, loss of use, data or profits, whether or not advised of the possibility of damage, and on any theory of liability, arising out of or in connection with the furnishing, use or performance of this information.
References to corporations, their services and products, are provided “as is” without warranty of any kind, either expressed or implied.
Descriptions of, or references to, products, services or publications within Ribbon’ documentation do not imply endorsement of that product, service or publication.

Disclaimer
Material contained in this document is subject to change without notice. The material herein is solely for training purposes and does not represent a commitment by Ribbon or its representatives. Ribbon has prepared the information contained in this document solely for use by its employees, agents and customers for the use and understanding of Ribbon’s products and solutions.

Warning
This publication is intended for training purposes only. Always refer to the procedures described in the Ribbon standard documentation that are appropriate for the system and software release that you support. Failure to use the appropriate documentation can result in serious technical difficulties and damage to your system. For additional information about referenced documentation, visit www.ribboncommunications.com or contact your local Ribbon sales office or account representative.

Trademark acknowledgements
Ribbon and the Ribbon corporate logo are registered trademarks of Ribbon and its affiliates.
Ribbon trademarks may not be used in connection with any product or service that is not Ribbon ´s in any manner that is likely to cause confusion among customers or in any manner that disparages or discredits Ribbon.
All other company, product, logos or service names mentioned herein are trademarks, service marks, registered trademarks, registered service marks or copyright material of their respective owners.

Embedded Software
Oracle Enterprise Edition is an embedded part of the Ribbon product line. The programs included herein are subject to a restricted use license and can only be used in conjunction with this application. You are not allowed to navigate or modify the underlying database schema unless explicitly authorized in writing by Ribbon.

Revision History

Version	Date	Changes incorporated
1.0		Initial Release
4.0	July, 2019	Update for R8.0
4.1	December, 2019	Update for R8.1
4.2	January, 2020	Updated for R8.2
4.3	June, 2020	Updated for R9.0
4.4	August, 2020	Call procedure updated
4.5	January, 2021	Update for R9.2

References

Document Number	Document Name

Contents

Lab 01	Navigation Exercise	1
Lab 02	Provisioning	5
Lab 03	Route Provisioning	11
Lab 04	PSP Provisioning	17
Lab 05	Call Details Records	23
Lab 06	Call Trace	27
Lab 07	Packet Capture	31
Lab 08	Alarms/Live Monitor	33
Lab 09	SBC CLI — Part 1	35
Lab 10	SBC CLI — Part 2	37
Lab 11	Security	39
Lab 12	Additional CONFIG	43
Lab 13	Troubleshooting	45
Lab 14	System Backup	47
Lab 15	Exploring the Configuration	49
Lab 16	Debugging and Gathering Info	51

Contents

Lab 17 SIP Peering CONFIG Script 56

Before you Begin

During these exercises, you will provision objects on the SBC. To distinguish your work from other students and avoid naming conflicts, you will often be asked to add your student number to the object's name. Your instructor will assign your student number to you. Write this number on your name card for the instructor's reference. Substitute this number during these exercises when you see the letter *n* in the instructions.

Your Student number is: _____ (Assigned by the instructor)
The exercises for this course require access to a Ribbon SBC. The following information describes how to log into the SBC. Record below the details of the server you will be using for the lab exercises. Your instructor will assign you to an SBC detailed in the student lab handout.

Record the SBC name here: _____

Record the EMA IP address here: _____

(Optional) Record the BMC IP address here: _____

(Optional) Record the EMS IP address here: _____

Open the Mozilla Firefox web browser on your computer and type the IP address for the SBC provided by your instructor, and press Enter.

**If you have difficulty accessing the system, please inform your instructor now.*

Lab

1

Navigation Exercise

Description

This exercise will allow you to get familiar with the SBC EMA and CLI. Optionally, if you have an Insight EMS in your system then you can also look at the SBC Manager.

Procedure

Step 1: Using putty (ssh terminal), login to the management port of your assigned SBC.

Username	admin
Password	Ribbon_SBC1

Step 2: Type the following:

a) config <enter>

b) set oam localAuth user **Student#** group Administrator passwordAgingState disabled <enter> (Substitute your student number for the #)

c) commit <enter>

d) When you enter commit, you will see a **password**. Copy the password by highlighting it and put it into notepad, because you will need it to login to EMA.

e) After making sure you have your password safely copied, type the following to exit the cli session: exit <enter> exit <enter>

Part A: Navigating in EMA

Step 1: Using the Firefox browser, enter the management IP address of your assigned SBC to access EMA. You will change your password after login using the username and password that you just created from your SBC CLI session. Enter the new password as follows: **Ribbon_SBC1**

Step 2: How many Functional Categories are there (Hint - Top Line of GUI)?

_____

Step 3: Using the "Search Function" at upper right-hand side of the screen, search for **event log**. How many results are returned?

_____

Step 4: Under the **Troubleshooting > Call Trace/Logs/Monitor Functional** Category, click on the **Log Management** perspective. In the display window, how many log types are shown?

NOTE: Everything shown is a log type even if it doesn't contain the word "logs"

_____

Step 5: What is the purpose of the "Custom" functional category?

_____

Step 6: Which Functional Category allows you to view any object in the system?

_____

Step 7: Take a few minutes, and click on each Functional Category, each perspective and sub-category where appropriate and familiarize yourself with the EMA interface, and where objects are located.

Part B: Using the CLI

Step 1: Logout of EMA then use putty or another ssh program to open a CLI session on your assigned SBC management port (Use the username and password that you just created)

a) Once logged in, type a ? to see a list of commands available on the top level of the CLI

b) Type in “show config” to see the configuration of the SBC. Enter “Q” to exit out of the config.

c) Type “exit” to exit the SBC CLI. The SBC CLI will be covered in more detail later in the course.

Part C: Navigating in the BMC

Note: The next step has you login to the BMC where system impacting operations can occur. Only the SBC hardware platforms (SBC 5x00 and SBC 7000) provide this feature, SWe does not include a BMC.

Do not to make any system impacting changes such as power cycling the host.

Step 1: The Baseboard Management Controller (BMC) is used primarily for initial configuration of the server. **Use your student handout to perform the instructions below.**

a) Login to the BMC and Navigate through the different tabs

b) After initial configuration, when would do you think the BMC would be needed?

_____

c) In the BMC, how would you get to a Linux console session? (Do not attempt to login once the console is visible).

_____

d) Logout of the BMC

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

2

Provisioning

Description

In this exercise, you will use the information from exercise 2 to create the objects required to connect to a SIP peer.

Procedure

Part A:

Step 1: From EMA, go to:

Configuration → System Provisioning → Sip Carrier Peering

Part B: Create your External Address Context

Step 1: Create your Address Context with the name **AC_EXTERNAL#**, (**The "#" is your assigned student number**)

Part C: Create your Interface Group and objects inside

Step 1: Create your Interface Group with the name **IG_EXTERNAL#**. (**Leave IPsec disabled!**). Make sure you are creating your interface groups and other objects in YOUR address context.

Step 2: In the next step, you will build an IP Interface. **Make sure to assign your IP interface a VLAN**. Otherwise, other students on your assigned SBC will not be able to create their IP interfaces!

Open your interface group and create your Interface with the name **IF_EXTERNAL#** (where # is your assigned student number). Refer to the information in your **student handout** in the green table of the SBC assigned to you and complete the parameters requested.

NOTE: The **CE Name** is the name of your system as specified in the Student Handout. The system name is the name of the slide of your assigned SBC.

Step 3: Save your interface and make sure it is **enabled and in service**

Step 4: Add a static route in your Address Context that will point to your external IP PEER address.

a) In EMA go to:

Configuration → System Provisioning → Base Provisioning

b) Select **Static Route**

c) Make sure that you have selected your external **Address Context** and create a new static route as follows:

I. Destination IP Address = 0.0.0.0

II. Prefix = 0

III. Next Hop (check your student handout)

IV. IP Interface Group and IP Interface = your Interface group and Interface

V. Preference = 100.

d) Select "Save"

Part D: Create your Zone and the objects inside

Step 1: Select your address context and **create your Zone** with the name **ZONE_EXTERNAL#**. And use your assigned **VLAN tag** for the **Zone ID**

Step 2: Go to **Sip Signaling Port**, select your address context and zone, and select "New SIP Sig Port". Enter your information as follows:

a) **Index** = your assigned VLAN ID

b) **Mode** = **In Service** and **State = Enabled**

c) **IP Interface Group** = Your External Interface Group

d) **Signaling Port IP Address (V4)** = (check your student handout)

e) **Port Number** = 5060

Step 3: Select **SIP Trunk Group** and select your External Address Context and Zone

Step 4: Select "New SIP Trunk Group" and Create your SIP Trunk Group with the name **TG_EXTERNAL#**. Make sure that you make it State Enabled and Mode In Service.

Step 5: To the left of the screen, expand the **Sip Trunk Group** object, and select the **Media** subcategory, make sure that you have the "Media IP Interface group name" setting set to your External Interface Group that you built earlier in this lab exercise.

Step 6: To the left of the screen, also under the **Sip Trunk Group**, find **Ingress IP Prefix** subcategory, select your Address Context, Zone, and SIP Trunk Group and your External peer in this table as follows:

a) **IP Address** = Enter the IP PEER address on your student handout

b) **Prefix** = 32

Step 7: After creating your trunk group verify that it is **In Service** and **Enabled**.

Step 8: Select **IP Peer**, and select your Address Context and Zone, and select "New IP Peer"

Step 9: Create your IP Peer with the name **PEER_EXTERNAL#** and enter the **IP PEER** Address from your student handout and use IP **Port 5060**.

Part E: Review your provisioning

Step 1: Go back and review your configuration and make sure all relevant objects are "enabled" and "in service". (IP Interface, Trunk Group, and SIP Sig Port)

Part F: OPTIONS Ping

Step 1: Once all the required parameters are configured, you should be able to test your peer reachability by using the OPTIONS Ping command.

Step 2: To access OPTIONS Ping, select as follows in the EMA Interface:

All → Address Context → cmds

Step 3: Select your **Address Context**, then choose the **OPTIONS ping command** and click the **Select** button. In the pop-up window provide the following information:

a) **Sig Port** = INDEX NUMBER of your SIP signaling port

b) **PEER** = IP address of your External Peer

c) **Peer port** = 5060

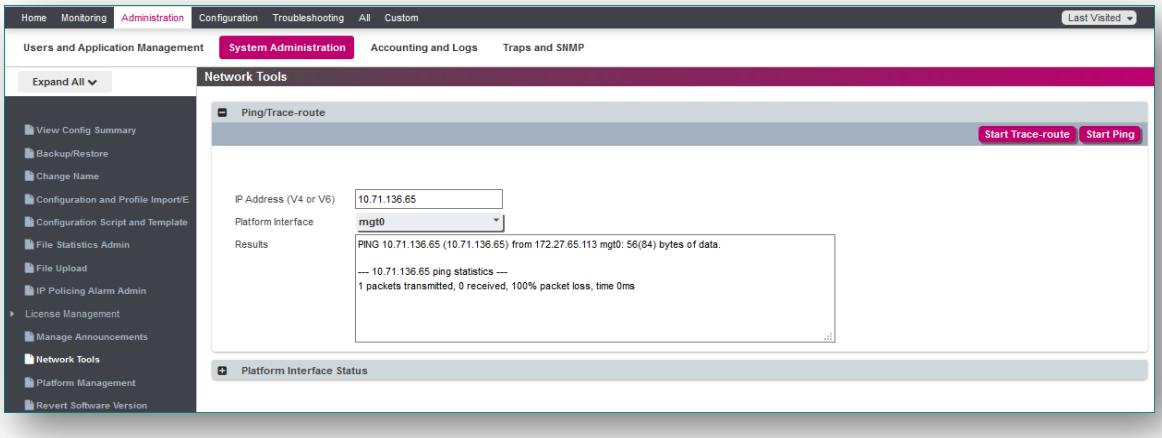
d) **Transport** = UDP

Step 4: Select the **OptionsPing button** to send the ping to your external PEER. You should receive a message indicating "**SUCCESS**". If the OPTIONS Ping fails, verify that the configuration you just made is correct.

Step 5: If your options ping still fails perform a regular IP ping to ping your network PEER_EXTERNAL. Go to

Administration → System Administration → Network Tools

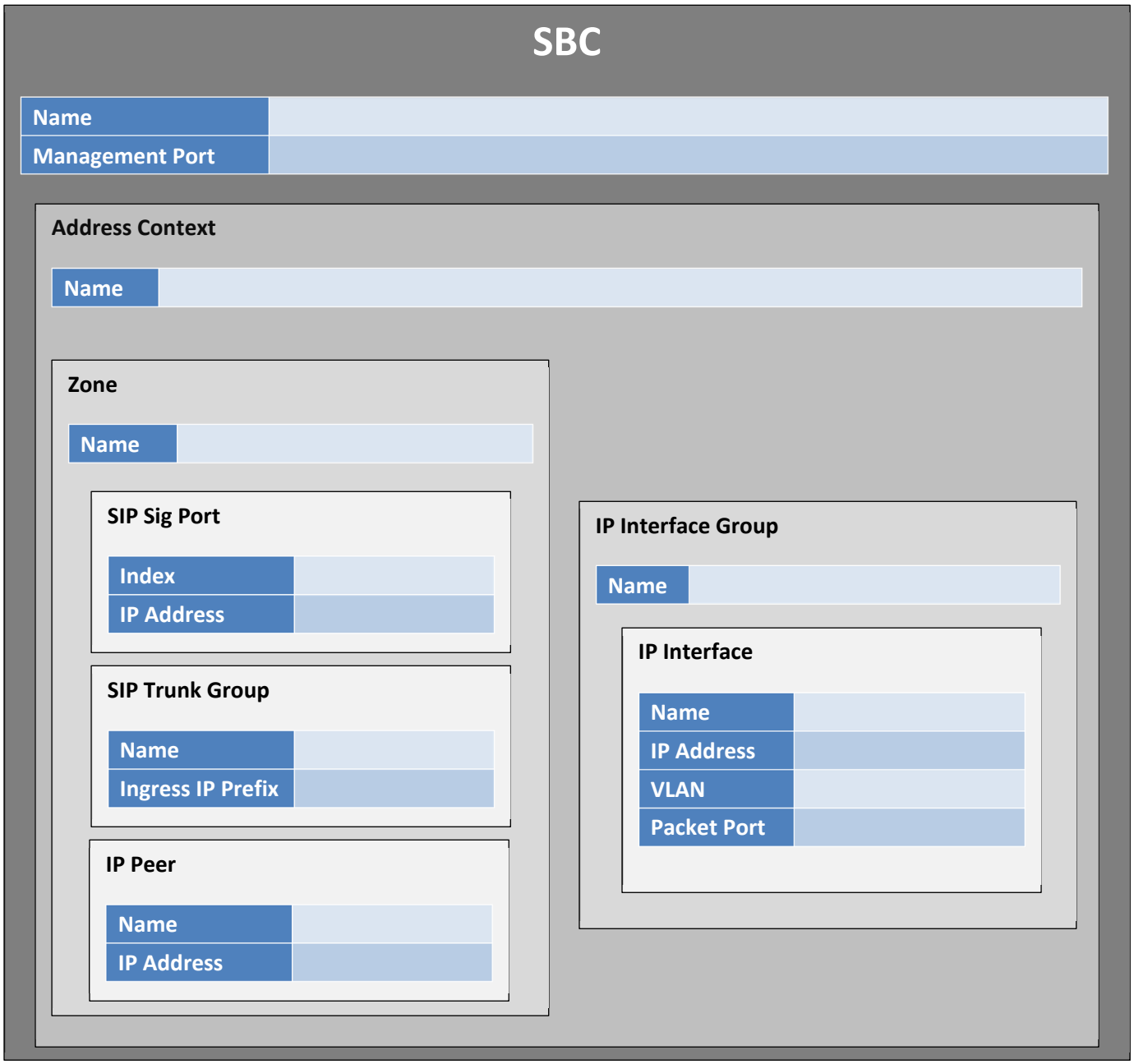
In this perspective, do a regular ping towards your peer. An example is below. Keep in mind your Interface will be either pkt1.xxx or pkt3.xxx (where xxx is your vlan ID) depending on your system type and lab assignment. Your address and port will be different from the example below.



Some other points that you could verify are listed as follows:

- Check your Interface Group and make sure IPSec is disabled on your interface group.
- Make sure that your IP Interface is Enabled and In-Service
- Also check to make sure your SIP port is enabled and in service.
- Check to make sure your trunk group is enabled and in service.
- Check that your static route is provisioned correctly.
- Make sure your ZONE has the “Zone Level Loop Detection” parameter set to disabled.
- Make sure that your PEERS “Default for IP” setting is set to False.
- Double check that all of your IP Addresses that you entered in the provisioning are correct for your assigned student ID

Step 6: Finally, the following table with the names and IP addresses of the objects that you configured in this exercise.



Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

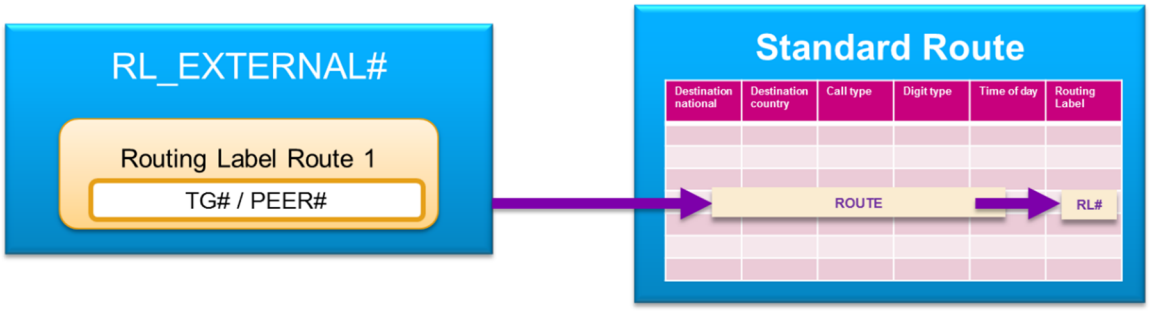
Lab

3

Route Provisioning

Description

In this exercise, you will create the configuration necessary to route a call towards the PEER_EXTERNAL that you configured before. At the end of this exercise, calls should successfully complete to your assigned telephone number. The phone numbers you should use are in your student handout in slide 3 and are dependent on your student number and the SBC you are assigned. Your instructor will refer to this number as the External number. Again, in this set of instructions, the # is your student number.



Procedure

Part A: Create the External Routing Label

Step 1: To access Routing, In EMA select as follows:

Configuration → System Provisioning → SIP Carrier Peering → Routing

Step 2: Select **Routing Labels + Routing Labels Routes** and select the **Create Routing Label + Routing Labels Routes** button.

Step 3: Create a routing label with the ID Name = **RL_EXTERNAL#**

Step 4: The new Routing Label will show in the table. Select your Routing Label using the radio button located to the left of its name.

Step 5: The *Edit Routing Label* window will show again. Select the **Add Routing Label Route** button.

Step 6: The Add Routing Label Route will open at the bottom of the screen. On the right-hand side select the following:

- ***Route type:*** Trunk Group
- ***Zone for TG and IP PEER:*** ZONE_EXTERNAL#
- ***Trunk Group:*** TG_EXTERNAL#
- ***IP PEER:*** PEER_EXTERNAL#

Step 7: Make sure that the routing label is set to **IN SERVICE** and Save.

NOTE: the save operation will give very little confirmation.

Step 8: To verify that your routing label was saved properly, select again your Routing Label in the table located at the top of the screen. Once selected, look for the ***Routing Label Route Sequence*** table inside the ***Edit Routing Label*** window.

Part B: Create the External Route

Step 1: Select **Routes** and select the **Create Route** button.

Step 2: Create a route using the destination number for your **external phone**. Use the parameter values below, (for any parameters not specified, leave them at their default values)

a) Route Type = None

b) Routing type = standard

c) Destination Country = 1 – USA, Canada…

d) Destination National = Enter your External Phone Number (see Student Handout sheet)

e) Routing Label = Select your Routing label that you built in the steps above

f) Call Parameter Filter Profile = none

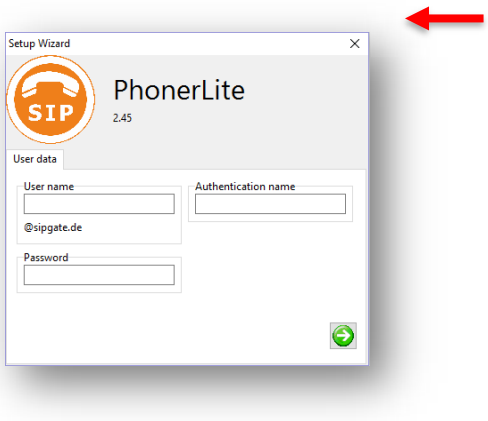
g) Time Range = all

h) Call Type = all, Digit Type = all

i) Select SAVE

Part C: Configure your Softphone

Step 1: Open the “Phonerlite ” application on your desktop, the following window will show:



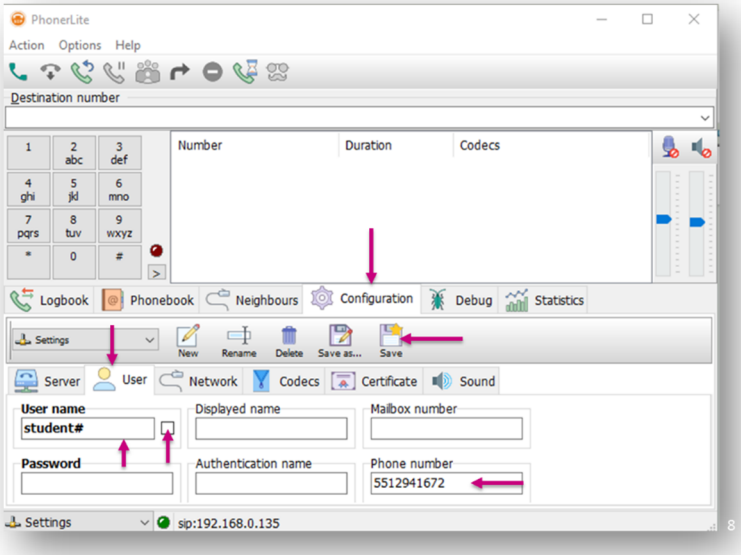
Close this window without making changes

Step 2: Select the **configuration** Tab, and select the **USER** Tab, enter as follows:

a) User Name = student# (your assigned student name, example student7)

IMPORTANT: make sure the check box next to your student name is UNCHECKED

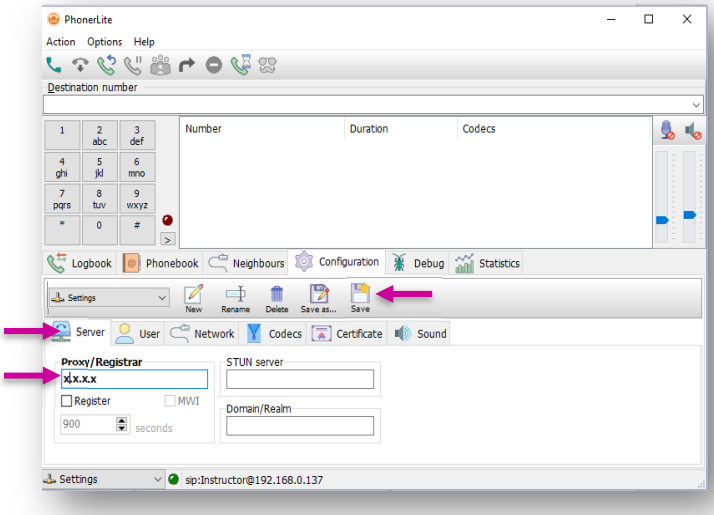
b) Phone Number = Enter your **Internal Phone Number** for your assigned student ID, (see Student Handout sheet)



Step 3: Select the **configuration** Tab, and select the **SERVER** Tab, enter as follows:

a) **Proxy/Registrar** = Enter your assigned SBC's PKT0 Interface IP Address (check your student handout)

b) Select the "SAVE" icon



Part D: Call your external number.

Step 1: After saving your configuration in Phonerlite , Call your external phone number. Your external endpoint should answer the call (it is set to auto answer).

a) Your call should stay up at least 4 seconds (don't hang up)

Step 2: Before you hang-up your call, take a look at call detail status and call media status, perform as follows:

Step 3: From EMA Select as follows:

All → Global

Step 4: View the **Call Detail Status** and **Call Media Status**

Step 5: Find your call, and note the codecs used and number dialed.

Step 6: Hang-up the call

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

4

PSP Provisioning

Description

In the previous exercise, you successfully made calls to your external peer using the “default” Packet Service Profile. In this exercise, you will provision two new Packet Service Profiles and apply them so that calls between your internal peer (Phonerlite) to your external peer will transcode from G711 to G729AB. You will verify that transcoding has occurred by looking at call media and call detail status once the call completes. **This is a two-part exercise**:

Prior to commencing this exercise, ensure that you can call your external peer as you did in the previous exercise.

Part 1

So far, we have created the objects necessary to communicate with the External side of our network. In our environment, this external side is represented by the external numbers that we dialed before. When a call is placed for these external numbers, your call is associated to TGINTERNAL as your ingress Trunk Group, which was created for you before class started. This TG is an object inside of the Zone ZONE_INTERNAL and is currently configured to accept any incoming call. This is something that you can verify by looking into the Ingress IP Prefix table associated to it where you will see an entry for IP address 0.0.0.0, which means any IP address.

In this part, you will create additional configuration to the internal side of our scenario. First you will create a new Trunk Group, which you will use now as ingress TG. Then, a new IP Peer, which will represent your Phonerlite . Finally, you will require a Route and Routing Label to point to your Phonerlite .

Then, by the end of this part, you should be able to call yourself and call other people assigned to your same SBC.

Procedure

Part A: Find the IP address of your desktop

When you call using the Phonerlite application, the IP address that is used as originating IP for your SIP traffic is the one that is assigned to your desktop. This is the IP address that the SBC will recognize as IP Peer in the internal side of our network.

Step 1: Find out the IP address of your desktop. This will be a 10.128.175.x address. If necessary, use the "ipconfig" command to find it.

Step 2: You will use this address for your **internal IP PEER** and as the **ingress IP prefix in your internal trunk group** that you will build in the steps that follow.

Part B: Create your Internal Peer

Step 1: From EMA, go to the section where you would create a new IP Peer.

Step 2: Create your IP Peer with the name **PEER_INTERNAL#**

a) This will be created in the **default** Address Context and in zone **ZONE_INTERNAL**

b) **IP Address** = Use your desktop IP address for the new peer.

c) **IP Port** = 5060

Part C: Create your internal Trunk Group

Step 1: From EMA, go to the section where you would create a new SIP Trunk Group

Create a new Trunk Group in zone ZONE_INTERNAL, enter as follows, (make sure to save it)

a) This will be created in the **default** Address Context and in zone **ZONE_INTERNAL**

b) NAME = **TG_INTERNAL#**

c) **State = Enabled** and **Mode = In Service**

Step 2: On the menu to the left, expand **SIP Trunk Group** and select the **Media** subcategory, make sure that you have the Media IP Interface group name setting set to the **IGINTERNAL** Group.

Step 3: On the left menu, select the **Ingress IP Prefix** subcategory, and select the **default** Address Context, **ZONE_INTERNAL** Zone, and your **TG_INTERNAL#**

Step 4: Select "**New ingress IP Prefix**", and enter as follows, and save it.

a) **IP Address** = Enter your desktop IP Address

b) **Prefix** = 32

Part D: Create the routing configuration to the internal side

Step 1: In EMA, go to **Routing** as you did in the previous exercise.

Step 2: Create a routing label with the ID Name = **RL_INTERNAL#**.

Step 3: Add a routing label route, selecting **ZONE_INTERNAL**, your **TG_INTERNAL#**, and your **PEER_INTERNAL#**

Step 4: Make sure that the routing label is **IN SERVICE**

NOTE: the save operation will give very little confirmation.

Step 5: To verify that your routing label was saved properly, hover over it in the route label list, this should display your Internal Trunk Group and your Internal Peer that you assigned to it. If it does not correct your provisioning before continuing.

Step 6: When creating the route, your internal phone route number will be 50**9**56789XX, 67**4**567895XX, or 97**9**56789XX (XX is your 2 digit student

number) depending on the SBC you are assigned. Please refer to slide 8 in your Student handout. The right number is marked as Student#.

Step 7: Create a route using the destination number for Internal phone in your student handout sheet. Use the parameter values below (for any parameters not specified, leave them at their default values)

a) **Route Type** = None

b) **Routing type** = standard

c) Destination Country = 1 – USA, Canada…

d) **Destination National** = Enter your **Internal Phone Number** for your assigned student ID, (see Student Handout sheet)

e) **Routing Label** = Select your **Internal Routing label** that you built in the steps above

f) **Call Parameter Filter Profile** = none

g) **Time Range** = all

h) **Call Type** = all, **Digit Type** = all

i) Select "Save" to save your route

Step 8: If all went well, bring up Phonerlite and call the number you just created. Your Phonerlite should ring, and you should be able to answer it.

NOTE: After other students on your assigned SBC have completed the steps above, you should be able to call their internal numbers (Phonerlites) as well.

Part B

In this part, you will be creating two packet service profiles. One called PSPINTERNAL# and one called PSPEXTERNAL#. Your PSPINTERNAL# (# is your student number) will contain 1 codec G711-default and allow transcoding to G711 A or U. Your PSPEXTERNAL# (# is your student number) will contain 1 codec…G729AB- default and allow transcoding to G729AB.

Part A: Create the External Packet Service Profile

Step 1: Using EMA select as follows:

All → Profiles → Media → Packet Service Profile.

Step 2: Create a new PSP called **PSPEXTERNAL#** (the # is your student number) by clicking on + New Packet Service Profile in the upper right-hand corner of the working window. Then save it (bottom right corner of working screen – you may have to scroll down).

Step 3: Now, expand the Packet Service Profile object on the left of your screen and click on **Codec**.

Step 4: On the perspective screen (to the right of the objects), select your Packet Service Profile from the drop down in the gray area. You will see that 12 drop lists will appear in this window; this is where you select the codecs to be added to your Packet Service Profile.

a) Select the codec **G729AB-DEFAULT** from the pull down for **Codec Entry 1**. Then click **save**.

Step 5: Now click on the **Packet-to-Packet Control** object below the Packet Service Profile Object. Select Transcode **CONDITIONAL** from the pull down, then click save at the bottom of the screen.

Step 6: Now, expand the **Packet-to-Packet control** object and click on **Codecs allowed for transcoding**

a) Check the box (This leg only) that says **g729**, then click save. This action will allow calls to transcode using the G729AB codec.

Part D: Create the Internal Packet Service Profile

Step 1: Now repeat step 1 above to create your second packet service profile named **PSPINTERNAL#**. Here, you want only the **G711-DEFAULT** for codec entry 1 and allow transcoding to **both G711A and G711U** on "**this Leg**" only.

Step 2: Before assigning your PSP's in the steps that follow, verify that you can successfully call your **external phone**. Then proceed with this exercise.

Step 3: To Assign your **PSPEXTERNAL** packet service profile to your **EXTERNAL SIP Trunk group**, Perform the following Steps

a) Expand the SIP Trunk Group object in

Configuration → System Provisioning → SIP Carrier Peering

b) Open policy (inside the SIP Trunk Group object).

c) Click on **Media**

d) On the gray area in the working screen, select your External Address Context, External Zone, and External SIP Trunk Group.

e) Select your **external PSP** from the drop-down menu and save it.

Step 4: Now attempt to place a call from your Phonerlite to your external peer. The call should fail with 488 "Not Acceptable Here".

a) Why did the call fail?

_____

b) What do you think you must do to correct the problem so that the call will transcode between G711A/U and G729AB?

_____

Step 5: Using what you have learned to this point, take the appropriate action so that calls will transcode from G711A/U to G729.

Step 6: Once you make your call, **select from EMA** as follows:

All → Global

and check **Call Media Status** and **Call Detail Status** which should indicate the call was transcoded, and the codecs involved in the call.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

5

Call Details Records

Description

In this exercise, you will take a look at the CDR's and logs for the calls being made. You will also set up call trace filters and look at the packet captures (signaling and media) for the calls.

Procedure

Step 1: Make a call, then use EMA Troubleshooting functional category/ Troubleshooting Tools perspective/ CDR Viewer object. Enable the CDR Viewer function and select your STOP record from the list, then answer the following questions.

a) On what SBC did the call arrive? (Gateway Name):

_____

b) In what time zone is the SBC is located? (Node Time Zone):

_____

c) When was the call answered, in GMT? (Start Time):

_____

d) What is the disconnect reason code? (Call Disconnect Reason)

_____

e) On what type of interface did the call come into this SBC and how did the call egress (Call Direction):

_____

f) What was the calling party phone number (Calling Number), if any?

_____

g) What was the destination phone number (Called Number):

_____

h) What route label was selected (Route Label):

_____

i) If the call was routed out, what route did the SBC use for this call? (Route Selected):

_____

j) Which trunk group did the call arrive on (Ingress Trunk Group Name):

_____

k) What are the local and remote IP addresses and port numbers for this call (Ingress IP Circuit End Point):

Local: _____ Remote: _____

l) (Egress IP Circuit End Point):

Local: _____ Remote: _____

m) Who hung up first, the caller or the called party? (Disconnect Initiator):

n) Calling Party is 1, Called Party is 2 or Neither (circle one)

o) What is the egress trunk group name (Egress Trunk Group name)

_____

p) What was the ingress codec type? (Ingress Codec Info):

_____

q) What was the egress codec type? (Egress Codec Info):

_____

r) What script was returned? (Script):

_____

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

6

Call Trace

Description

In this exercise, each one of the students will create a Call Trace Filter. Then, each student will make a test call and get the Trace file from the SBC to analyze it. All students will perform the test call simultaneously. Then it will be the responsibility of the student with the lowest number assigned to start and stop the trace.

Procedure

Step 1: Using EMA, go to:

Troubleshooting → Call Trace/Logs/Monitors → Call Trace and Packet Capture

Step 2: Select **Call Trace**.

Step 3: Scroll to the bottom of the screen to the Call Trace Filters section and click on **+ New Call Filter**.

Step 4: Name your filter: **student#** and enter the information from the table below. Save the filter. (where # = your student number)

Filter Name	Student#
State	Enabled
Capture Type	Capture trace information (.trc logs only)
Detail Level to Log	Level 2
Capture Calls that match these filters:	Called Number (your external phone number)
Stop Match	"Continue to Try…"

After you save your filter let the instructor and the classmates in charge of starting the call trace know.

Part A: Test Call

Step 1: After saving your filter, return to the top of the Call Trace window and check the following settings:

a) Call Trace Duration: **Stop trace after 180 minutes**.

Step 2: The student with the lowest number will select **Save and Start Trace**.

Step 3: Make a call to your external number.

Step 4: After making your call, hang up and check your .TRC file to see if it has grown (captured something) by looking at type status. Also, go to the CDR Viewer and identify the GCID of your call.

Step 5: If your call was captured, you should be able to find it by looking for the GCID in the trace file. Now:

a) Disable your call trace filter (remember to "save" after disabling)

b) Go to "Log Management" and Download your trace log file

c) Open the file using the LX tool – you should see the SIP messages for your call displayed in the primary LX window.

d) Click Editor at the top of the LX screen – you now see the raw text of the log file

Step 6: The student with the lowest number will now stop the Call Trace.

Step 7: Open your .TRC file in Notepad++. Use the find function to find the mentioned entries in the file:

a) rtpmap This is Peer-PSP

b) Ingress PSP-Ri & Egress PSP-Re

c) 100 Trying, 180 Ringing, Call Answered & Bye

d) What is the name of the call trace filter?

_____

e) What is the IP address of the Ingress Peer?

_____

f) Who is the contact on the ingress side?

_____

g) Is 100rel supported?

_____

h) What was the CSEQ# for the ingress invite?

_____

i) What was the CSEQ# for the Egress invite?

_____

j) What was the GCID assigned to the call?

_____

k) Locate the call accounting record (Process CAM) in the trace file. Can you tell from that information which codecs were selected for the call? You can look in the SBC Operations Guide for Field definitions of a STOP record and see if you can find the answer. Hint – the codec identifiers start with a "P":

_____

I. Was the call transcoded or passthru?

_____

II. What codec were used in this call?

- Ingress_____
- Egress_____

l) Which process reports SIP messages, like 100 Trying, 180 Ringing, 200OK?

_____

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

7

Packet Capture

Description

In this exercise, you will modify your Call Filter in order to collect a Packet Capture. In this exercise it will be necessary to take turns while collecting your files. Remember that the calls must be shorter that 15 seconds.

Procedure

Part A:

Step 1: Make sure you have **disabled** your "**student#**" call trace filter from the prior exercise to make the changes outlined below.

Step 2: Modify the trace filter that you created in the previous lab as follows:

Set the **Capture Type** to **Capture trace information** (**.trc logs**) and **media information** (**.pkt logs**).

Part B:

Now, tell your instructor that you are ready to start the test. The instructor will tell you when it is your turn. When the instructor gives you the go:

Step 1: Go to

Troubleshooting → Call Trace/Logs/Monitors → Log Rollover

and rollover the PKT file.

Step 2: Now, go to

Troubleshooting → Call Trace/Logs/Monitors → Event Logs → Type Status

and verify that the PKT file is now empty. Also, make a note of the name of the file, so you can download the correct file.

Step 3: Enable your Filter and Start the trace.

Step 4: **Call your external number** to capture the associated media and packets. While the call is up, **press a few keys on the phone keypad** to generate DTMF in the media stream. When complete, hang up the call.

Step 5: **Check your packet file**, ("type status"), If information is captured in your file **Disable your trace filter**, and tell the instructor, so the next student can run the test.

Step 6: **Download your .PKT file**, and open it **using Wireshark**. Wireshark should be the default program to open .PKT files.

Step 7: To see your signaling capture and hear media in Wireshark, **select Telephony** then:

a) Select **VoIP Calls**

b) Select the streams, and select **Play Streams** and also make sure to look at the **Flow Sequence**

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

8

Alarms/Live Monitor

Procedure

Part A:

Step 1: Using the EMA view both the current and cleared alarms, and select one from either list

Step 2: Make a comment and save it. You should be able to view your comment in the list of alarms.

Step 3: Acknowledge one of the alarms and view the results under the “Status” field of the alarm.

Step 4: See if you can find the alarm in the documentation, (for example, perform a documentation lookup on the “type” field)

Step 5: In EMA: Go to the **Monitor** functional category and choose the **Dashboard perspective**, then select the **Live Monitor** object.

Step 6: **Enable Live Monitor**, and if necessary, **configure it to show call related detail**.

Step 7: Take a look at some of the information available in Live Monitor.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

9

SBC CLI — Part 1

Procedure

Part A:

In this exercise, you log into the CLI and issue various commands.

Step 1: Using Putty, log into the CLI of your assigned SBC.

Step 2: What are the two different levels of the CLI and how can you tell which level you are in?

_____

Step 3: From the General Level, show the configuration of your Address Context. Remember to use tab completion to help you through the command.

Step 4: From the General Level, **show the state (enabled/disabled) of your External Trunk Group.**

Step 5: Issue the **set-path** command to position the system to display only **your Address Context**.

Step 6: Issue a **show configuration displaylevel 2**. Use the up arrow to retrieve your previous command and change the **displaylevel to 7**. Which command displays more information?

Step 7: Issue the **request** command to send a message to all students in the class.

Step 8: Issue the **reset** command to reset the screen and then issue the **Top** command to take you back to the top level.

Step 9: To see your routing information, issue the command **show configuration global** followed by tabs to try and complete this command

Step 10: Enter the Configuration Level by typing **config**.

a) Type "**edit addressContext (your address context name)**. What other command does the same thing in the General Level?

_____

b) Type "**top**" to return to the default level of the CLI

c) Use the "**set**" command to create another Address Context using your name as the name of the object. Use the commit command to commit the change. Is your new address context visible in EMA?

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

10

SBC CLI — Part 2

Procedure

Part A:

In this exercise, you will learn how to delete objects from EMA, then replace them with using SBC Cli commands.

Step 1: First, delete your **External** side route. Then delete your routinglabel route and routing label.

Step 2: Next, delete your remaining **External** side objects starting in the zone and working your way up to your address context.

a) Which objects needed to be disabled and out of service prior to deleting them?

_____

Step 3: Open the AC_Student.dox file with Notepad++ and change the values to reflect your configuration. Once you think you are finished, let the instructor see it before pasting it into the SBC Cli command line

Step 4: Once you have pasted the "Cli script" into the command line, check your configuration in EMA, and make sure your call works as before.

Step 5: If your script fails, see if you can figure out what went wrong, and fix it.

Step 6: You have successfully completed this exercise when you can successfully make a call to yourself and your external peer. Also, you should be able to call someone else on your system.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

11

Security

Description

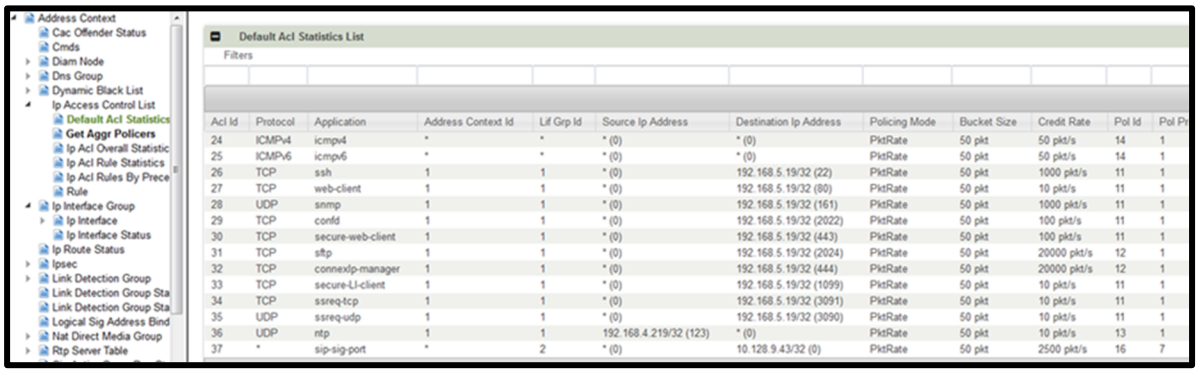
In this exercise you will first look at the System Default ACLs, where you will try to find your Unknown Peer ACL.

Then, you will create Access Control Lists that will deny, accept, and police traffic.

Procedure

Part A: Unknown Peer ACL

Step 1: Under the default Address Context; find your Unknown Peer ACL. It will look something like this, (Default ACL Statistics).



Acl Id	Protocol	Application	Address Context Id	Lif Grp Id	Source Ip Address	Destination Ip Address	Policing Mode	Bucket Size	Credit Rate	Pol Id	Pol Pr
24	ICMPv4	icmpv4	*	*	* (0)	* (0)	PktRate	50 pkt	50 pkt/s	14	1
25	ICMPv6	icmpv6	*	*	* (0)	* (0)	PktRate	50 pkt	50 pkt/s	14	1
26	TCP	ssh	1	1	* (0)	192.168.5.19/32 (22)	PktRate	50 pkt	1000 pkt/s	11	1
27	TCP	web-client	1	1	* (0)	192.168.5.19/32 (80)	PktRate	50 pkt	10 pkt/s	11	1
28	UDP	snmp	1	1	* (0)	192.168.5.19/32 (161)	PktRate	50 pkt	1000 pkt/s	11	1
29	TCP	confd	1	1	* (0)	192.168.5.19/32 (2022)	PktRate	50 pkt	100 pkt/s	11	1
30	TCP	secure-web-client	1	1	* (0)	192.168.5.19/32 (443)	PktRate	50 pkt	100 pkt/s	11	1
31	TCP	sftp	1	1	* (0)	192.168.5.19/32 (2024)	PktRate	50 pkt	20000 pkt/s	12	1
32	TCP	connexip-manager	1	1	* (0)	192.168.5.19/32 (444)	PktRate	50 pkt	20000 pkt/s	12	1
33	TCP	secure-LI-client	1	1	* (0)	192.168.5.19/32 (1099)	PktRate	50 pkt	10 pkt/s	11	1
34	TCP	ssreq-tcp	1	1	* (0)	192.168.5.19/32 (3091)	PktRate	50 pkt	10 pkt/s	11	1
35	UDP	ssreq-udp	1	1	* (0)	192.168.5.19/32 (3090)	PktRate	50 pkt	10 pkt/s	11	1
36	UDP	ntp	1	1	192.168.4.219/32 (123)	* (0)	PktRate	50 pkt	10 pkt/s	13	1
37	*	sip-sig-port	*	2	* (0)	10.128.9.43/32 (0)	PktRate	50 pkt	2500 pkt/s	16	7

Part B: Create your ACL

Step 1: In EMA, go to:

All → Address Context → IP Access Control List → Rule

Step 2: Next, you will create **3 new ACLs Rules** in the **default Address Context** as listed below (one at a time).

Step 3: You will be creating these in the Interface Group **IGINTERNAL**, IP Interface **IFINTERNAL**, and using your **PEER_INTERNAL** address as the IP Source address.

Step 4: Add the following 3 new rules:

Policer rule POLICER_nn

a) **Name** = POLICER_NN (where nn is your student number, hence 09, 12 etc..)

b) **Precedence** = Use nn (your student number) as the precedence number,

c) Action **ACCEPT**

d) **Fill Rate** = 2

e) **Bucket size** = 2

f) State **Disabled**

Part B: Accept Rule ACCEPT _1nn

a) **NAME** = ACCEPT_1nn

b) **Precedence** = Use 1nn as the precedence number (100 + your student number)

c) Action **ACCEPT**

d) **Fill Rate** = unlimited

e) **Bucket size** = unlimited

f) State **Disabled**

Part C: Deny Rule DENY_2nn

a) **NAME** = DENY_2nn

b) **Precedence** =Use 2nn the precedence number (200 + your student number)

c) Action **DISCARD**

d) State **Disabled**

Part D:

Before performing the steps below, verify that your soft phone is operational by making a call to your external phone. This should work before you proceed with the steps below.

Step 1: First, enable your **DENY_2nn** ACL

a) Make a call to your external number using the configuration sheet if you do not remember the phone number.

b) The call should fail, why?

_____

Step 2: Now enable your ACCEPT_1nn ACL.

a) Make a call to your external number

b) The call should go through, why? _____

Step 3: Now enable your **POLICER_nn** ACL.

a) Make a call to your external number, and hit the redial key several times in Phonerlite

b) Some call attempts may fail, why? _____

NOTE: the redial action can leave calls open, if there are calls open they will be visible in the "call details" view and subsequent calls may fail. Calls can be cleared using the CLI command: "request global terminateCall GCID (Gcid of actual call)

Step 4: Now check your rules statistics using the object IP ACl Rule Statistics. From EMA, select as follows:

All → Address Context → IP Access List → IP ACL Rule Statistics

a) How many Matches?

_____

b) How many policer discards?

_____

c) If there are enough packet discards, you may be able to find your peer IP address in an offenders list. Select the

All → System → IP Policing → ACL offenders list

object and take a look. **Disable all your ACLs when you are finished.**

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

12

Additional CONFIG

Description

This is a Team exercise. At the completion of this lab, you should be able to:

- Make calls from ANY phone on ANY SBC to any other phone on any SBC.

Procedure

Part A:

Step 1: The team using each SBC must create a SIP Trunk Group and Peer for each other SBC being used by the class.

Step 2: Each SBC will also require Call Routing to send the correct calls to the correct SBC, based on the area code used for the phone numbers on that SBC.

Step 3: Once all SBCs have been configured, test calls between SBCs to make sure that all calls work. If any calls are not working, troubleshoot the problem.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

13

Troubleshooting

Description

In this exercise, you will find that the calls going to your external peer are not getting established. Troubleshoot the configuration in order to find out what is causing the problem. By the end of this exercise, you should be able to call your external peer again.

NOTE: you will not be able to call other students or other SBCs at this point.

Procedure

Part A:

Step 1: Go to your browser and type the Management IP address of the SBC assigned to you. Login using the following users and password:

SBC				User	Password
Westford	Prague	MOP	RTP		
WES1	PRA1	MOP1	RTP1	Student1	Ribbon_SBC1
				Student2	Ribbon_SBC1
				Student3	Ribbon_SBC1
				Student4	Ribbon_SBC1
WES2	PRA2	MOP2	RTP2	Student5	Ribbon_SBC1
				Student6	Ribbon_SBC1
				Student7	Ribbon_SBC1
				Student8	Ribbon_SBC1
WES3	PRA3	MOP3	RTP3	Student9	Ribbon_SBC1
				Student10	Ribbon_SBC1
				Student11	Ribbon_SBC1
				Student12	Ribbon_SBC1

Step 2: You will test the calls going to your external number. At this point the calls will fail. Use the knowledge now you have of the SBC and the troubleshooting tools discussed in this course to finds out what is wrong. Then document all your progress in the following table.

Error code	Symptom	Fix
i.e. 504 Server timeout	Call drops after 32 seconds	Disable a discard rule that is blocking the service.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

14

System Backup

Description

Students on each system must take turns doing backing up and downloading the backup file. The lowest numbered student will go first. For example, Student1 will back up the system, then student 2, etc.

Procedure

Part A:

Step 1: Students should take turns performing the following steps:

Step 2: Select as follows in EMA:

Administration → ***System Administration*** → ***Backup/Restore***

Step 3: Backup the system you are working on using your student# as the suffix.

Step 4: Save your backup to your desktop.

Step 5: Inform the next student on your SBC that you have finished

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

15

Exploring the Configuration

Description

In this exercise, you will export the current configuration and download it to your desktop. Then you will untar the file you downloaded with 7zip, and examine the contents of the exported files.

Procedure

Part A:

Step 1: **<u>One at a time:</u>** Lowest student number on system goes first (takes 5-6 mins)

Step 2: In EMA, go to:

Administration → System Administration → Configuration and Profile Import/Export

Step 3: Select the **Export Configuration/Profiles** button.

Step 4: Select **Full Configuration** then in the **File Name** field enter student# (for example student7)

Step 5: Select the **Start Export** button.

Step 6: Once the export is finished, download the file and save the file to a folder on your desktop.

Step 7: Using 7zip, extract the files. This will generate a.tar file inside the new folder on your desktop.

Step 8: Use 7zip on the .tar file with the "extract files here" option. Now you should see a new folder called "config_export". Open that folder and answer the following?

a) Which file contains the CLI commands?

_____

b) Which file would be the one you would make changes to if you wanted to change the configuration?

_____

Step 9: Open the server-info.txt file with notepad++.

a) What type of information is in the file, and why is it important?

_____

Step 10: Open the config_dumpxxx.cli file with notepad++.

a) What does the warning say at the top of the file?

_____

Step 11: Open the config_dumpxxx.xml file with notepad++. This is the file you would modify to change values in the configuration if desired. Locate the following information:

a) Information about your Trunk Group(s)

b) Information about your SIP Signaling Port

c) Information about your Zone

d) Information about your PEER(s)

Step 12: This concludes the configuration file exercise.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

Lab

16

Debugging and Gathering Info

Description

At the completion of this lab, you should be able to use EMA or CLI to verify status and overall health of the SBC.

Procedure

Part A:

Step 1: Navigate in EMA to:

Administration → ***System Administration***

Step 2: Answer the following questions.

	Question	Answer
1	Under which Perspective would you check to see what SBC processes were running?	
3	Are all the SBC processes are running?	
4	Which button in the perspective would you click to see if a process changed states?	

Part B:

Step 1: Navigate in EMA to:

Administration → ***System Administration*** → ***Network Tools***

Step 2: Answer the following questions.

	Question	Answer
1	Use the tool in the screen to send a Ping to your IP Peer. Was it successful?	
2	How many packets were sent?	
3	Trace the route to your IP Peer. Was it successful?	
4	Which port was used to source your tests?	
5	Chose an interface and register the following information:	
	Name of your interface:	
	Status:	
	MAC Address:	
	IP Address:	

Part C:

In this section, you will be required to verify the status of your SBC. You can choose between getting the information requested from the GUI or through the CLI. Base your answers on the slides seen in the lecture.

Step 1: Complete the table with the perspective or CLI command that would show the information requested

Information requested	EMA Perspective	CLI command
Current alarms		
CPU usage		
Disk usage		
Memory usage		
Management port status		
HA port status		
Server status		
Power status		
Fan Status		
DSP status		
Policy Server status		

Part D:

The sysdump (System Diagnostics) utility is used to collect all system logfiles, including ones you will not be using in this class. Many of the Tar'd log files are engineering level log files to help Ribbon when additional in-depth info is needed to troubleshoot a L3 problem. This class addresses L1/L2. There are, however, a few logs that are collected you can look at and you will review in the next steps. Sysdump should only be done after you have done a system health check and have eliminated any L1/L2 issues. It should not be done frequently during your troubleshooting exercises, unless directed by Ribbon TAC professionals

Step 2: Your instructor will point you to a Sysdump file that you can use as an example in this section. You will find it in EMA navigating to:

Administration → ***System Administration*** → ***System Diagnostics***

Save the file to your desktop.

Step 3: Extract your sysdump archive to the desktop with an unzip utility (7z). This will be a .tar file.

Step 4: Extract the .tar file to your desktop, and this will yield a folder with more .tar files in it.

Step 5: Answer the following questions. You may have to look at the contents of Sysdump to answer them.

a) What information is contained in swinfo?

_____

_____

b) What information is contained in hwinfo?

_____

c) What information is contained in sbx-status.info?

_____

d) Sbx.conf?

_____

e) Sbc-pkg.info?

_____

f) Where would I find the event logs in the sysdump archive?

_____

Step 6: **Optional Demo**: Tshark can be used to capture signaling traffic. A pcap file gets built on the SSD. It can be retrieved and analyzed with Wireshark.

Step 7: **Optional Lab**: the instructor will introduce problems into the system which you will have to fix. Follow the instructor's directions.

Congratulations, you have completed this lab exercise, please make sure to inform your instructor that you are done

SIP Peering CONFIG Script

```
configure
######### Setup Address Context if needed #########
set addressContext AC99
commit
########## Setup IP Interface Groups ##########
set addressContext AC99 ipInterfaceGroup IG99 ipInterface IF99 portName pkt1 ipAddress 10.0.199.19 prefix 24
ceName T5110 vlanTag 111 state enabled mode inservice
commit
########## Setup Zones & Sip Signaling ##########
set addressContext AC99 zone Z99 id 199 sipSigPort 199 ipInterfaceGroupName IG99 ipAddressV4 10.0.199.19
portNumber 5060 transportProtocolsAllowed sip-udp
commit
set addressContext AC99 zone Z99 id 199 sipSigPort 199 state enabled mode inService
commit
########## Zones & Trunk Groups ##########
set addressContext AC99 zone Z99 sipTrunkGroup TG99 media mediaIpInterfaceGroupName IG99
set addressContext AC99 zone Z99 sipTrunkGroup TG99 signaling timers sessionKeepalive 0
set addressContext AC99 zone Z99 sipTrunkGroup TG99 ingressIpPrefix 10.0.199.100 32
set addressContext AC99 zone Z99 sipTrunkGroup TG99 state enabled mode inService
commit
########## IpPeers ##########
set addressContext AC99 zone Z99 ipPeer PEER99 ipAddress 10.0.199.100 ipPort 5060
commit
########## Routing Label & Routing Label Routes ##########
set global callRouting routingLabel RL99 routingLabelRoute 1 trunkGroup TG99 ipPeer PEER99 inService
commit
########## Route ##########
set global callRouting route none Sonus_NULL standard 9781234599 1 all none Sonus_NULL routingLabel RL99
commit
Exit
```

ribbon™

Education Services

For information about other courses offered by Ribbon, contact your training coordinator or visit:

http://www.ribboncommunications.com