casa systems

Course 1010 ICCAP Practical Labs

Lab Guide

Version 7.2.4
September, 2017

Table of Contents

LAB GUIDE I

VERSION 7.2.4 I

TABLE OF CONTENTS III

1 CASA ICCAP NETWORK SIDE INTERFACE (NSI) CONFIGURATION **1**

1.1 OVERVIEW 1

1.2 HOW TO LOGIN TO CASA LABS 1

1.3 CONNECT TO THE LABS 1

1.4 CONFIRM CLASS NETWORK CONNECTIVITY 2

1.5 DEBUGGING 3

2 UPGRADING YOUR ICCAP **5**

3 LAYER 2 AND LAYER 3 CONFIGURATIONS **7**

3.1 C100G INSTRUCTIONS (ENGINEER 1 THROUGH ENGINEER 5) 8

3.2 C40G INSTRUCTIONS (ENGINEER 6) 9

3.3 COMBINED INSTRUCTIONS (ALL ENGINEERS) 10

3.4 OSPF V2 V3 CONFIGURATIONS 11

3.5 VERIFYING OSPF CONFIGURATIONS 12

3.5.1 Verify BFD *12*

3.5.2 Verify OSPFv4 ..... *12*

3.6 VERIFY OSPFV3 14

3.7 OSPF ASBR CONFIGURATION 15

3.7.1 Create a RIP Instance *15*

3.7.2 Create an IP Prefix List *16*

3.7.3 Create a Route Map *16*

3.7.4 Redistribute Your RIP Route *16*

3.7.5 Check Your Work *16*

3.8 ISIS CONFIGURATIONS 17

3.9 ISIS REDISTRIBUTION CONFIGURATIONS 18

3.9.1 Create a RIP Instance *18*

3.9.2 Redistribute Your RIP Route *18*

3.9.3 Check Your Work *19*

3.10 VERIFYING ISIS CONFIGURATIONS 19

3.10.1 Verify IS-IS V4 ..... *19*

4 SYSADMIN CONFIGURATIONS 20

4.1 ENABLE THE "SAVE CONFIGURATION" MESSAGE 20

4.2 TELNET SETTINGS 20

DISPLAY YOUR CONFIGURATION BY TYPING, SHOW RUNNING-CONFIG | INC LINE. 21

4.3 SSH CONFIGURATION 21

4.4 SET THE SYSTEM TIME 21

4.5 CONFIGURE NETWORK TIME PROTOCOL 22

4.6 CONFIGURE DNS 22

4.7 PRIVILEGED MODE PASSWORD 22

4.8 ENCRYPTING NETWORK SERVICE PASSWORDS 23

4.9 ADDING LOCAL USERS 23

4.10 CREATING ALIASES 24

4.11 CONFIGURING LOCAL LOGGING 24

4.12 CONFIGURING SYSLOG 25

4.13 CONFIGURING SNMP 26

4.13.1 Configure SNMP Communities *26*

4.13.2 SNMPv2 ..... *27*

4.13.1 Protocol Independent Multicast SNMP Support *27*

4.13.2 Enabling SNMP on Your Cable Modems *28*

5 ACCESS CONTROLS (ACLS) 29

INTRODUCTION 29

5.1 CREATING AN ACCESS GROUP ON AN INTERFACE 29

5.2 CREATING A GLOBAL ACCESS CLASS 30

6 NSI DIAGNOSTICS 31

6.1 DIAGNOSING INTERFACE ISSUES 31

6.2 DIAGNOSING MEMORY AND PROCESS ISSUES 32

6.3 DIAGNOSING DHCP ISSUES 32

6.4 DIAGNOSING HIGH AVAILABILITY ISSUES 32

6.5 DIAGNOSING TRUNKING ISSUES 32

6.6 OBTAINING SYSTEM INFORMATION 33

6.7 DIAGNOSING INITIALIZATION PROCESSES 33

6.8 THE SHOW TECH COMMAND 33

6.9 TCP DUMP 34

6.9.1 Exploring TCP Dump *34*

6.9.2 Run TCP Dump on a Specific Protocol *35*

6.9.3 Run TCP Dump for a Specific Number of Captures *35*

6.9.4 Using TCP Dump to Gather Information *35*

6.9.5 Using TCP Dump to Track Flows *35*

6.9.6 Writing the Dump to a File for Viewing *36*

7 RFI CONFIGURATIONS 37

7.1 ENABLE DOCSIS 3.1 37

7.2 Create OFDM Modulation Profiles 37
7.3 Configure an OFDM Channel for Your Annex B Modems 37
7.4 Configure a Second OFDM Channel for Your Annex B Modems 37
7.5 Configuring Downstream Transmitters for DOCSIS MAC 1 (Annex B) 38
7.6 Configuring Upstream Receivers 38
7.6.1 C100G Instructions (Engineer 1 through Engineer 5) 38
7.6.2 C40G Instructions (Engineer 6) 40
7.6.3 Combined Instructions (All Engineers) 41
7.6.4 C100G Instructions (Engineer 1 through Engineer 5) 41
7.6.5 C40G Instructions (Engineer 6) 41
7.7 Configuring Downstream Transmitters for an Annex A MAC Domain (All Engineers) 41
7.8 Configuring Upstream Receivers for an Annex A MAC Domain 42
7.8.1 C100G Instructions (Engineer 1 through Engineer 5) 42
7.8.2 C40G Instructions (Engineer 6) 43
7.8.3 C100G Instructions (Engineer 1 through Engineer 5) 43
7.8.4 C40G Instructions (Engineer 6) 43
7.9 Configuring DOCSIS MAC Interfaces 44
7.9.1 Create a DOCSIS MAC Interface for your Annex B Modems (All Engineers) 44
7.9.2 C100G Instructions (Engineer 1 through Engineer 5) 45
7.9.3 C40G Instructions (Engineer 6) 45
7.9.4 Create a DOCSIS MAC Interface for your Annex A Modems (All Engineers) 46
7.9.5 C100G Instructions (Engineer 1 through Engineer 5) 47
7.9.6 C40G Instructions (Engineer 6) 47
7.10 DOCSIS Security Configurations 48
7.10.1 Early Authentication and Encryption 48

7.10.2 TFTP Proxy/TFTP Enforce *48*

7.10.3 BPI Enforce *48*

7.11 PHY AND DOCSIS MAC BEST PRACTICES 49

7.11.1 Static MAP Advance *49*

7.11.2 Interleave Level *49*

7.11.3 Pre-equalization *50*

7.11.4 Modulation Profiles *50*

7.11.5 Dynamic interleaving *51*

7.11.6 Small Signal Compensation *51*

7.12 LOAD BALANCING AND CHANNEL BONDING CONFIGURATIONS 52

7.12.1 Configuring Service Groups *52*

7.12.2 Create a Second Service group for your Annex A modems *53*

7.12.3 Load Balancing *53*

7.12.4 Channel Bonding *54*

7.13 CASA SYSTEMS RFI FEATURES 56

7.13.1 Ingress noise cancellation *56*

7.13.2 Spectrum Management *56*

8 RFI DIAGNOSTICS 58

8.1 DOCSIS MODULES 58

8.2 DIAGNOSTIC MODE INTERFACE COMMANDS 58

8.3 CABLE MODEM DEBUG 58

TYPE DEBUG CABLE MAC-ADDRESS <MAC ADDRESS>. 59

8.4 CABLE MODEM SHOW COMMANDS 59

8.5 DIAGNOSING RF-RELATED PROBLEMS 60

8.6 REMOTE QUERY 60

8.7 DOCSIS PING COMMAND 61
8.8 CM STATUS MESSAGES 61
8.9 CABLE FLAP LIST 61
8.10 OBSERVING THE CABLE MODEM BOOT PROCESS 62
8.11 CABLE MIRRORING 63
8.12 CABLE MODEM DEBUG WITH SNMP 64
9 APPENDIX A 65
9.1 IBGP/LDP/MPLS CONFIGURATIONS 65
9.2 VERIFYING IBGP/LDP/MPLS 66
9.3 L2 VPN CONFIGURATIONS 67
9.3.1 Configuring EoMPLS 67
9.3.1 Configuring VPLS 69

1 Casa ICCAP Network Side Interface (NSI) Configuration

1.1 Overview

Casa Systems Hands-On Labs give you access to your own Casa ICCAP platform to configure. This step-by-step lab guide will guide you through the most common configurations that are typical of most network implementations of the Casa ICCAP. We cannot, of course, cover every possible configuration in this guide.

As you go through the formal written labs, and you have any questions, problems or would like to try your hand at configuring something that is not the formal lab guides, please contact us at training@www.casa-systems.net. We will provide a response within 24 hours.

1.2 How to Login to Casa Labs

You will need a username and password to login into Casa labs. You will find this information in the Messages section of your Learning Portal Home Page. Use the table below to correlate your username to your assigned ICCAP.

Username (assigned by Casa Training	ICCAP number
engineer1	1
engineer2	2
engineer3	3
engineer4	4
engineer5	5
engineer6	6

1.3 Connect to the Labs

From your computer, **ssh to port 22** on the lab server i.e., ssh yourusername@casalabs.training -p 22. Your ssh client will prompt you:

```
The authenticity of host '111.222.333.444 (111.222.333.444)' can't be
established.

RSA key fingerprint is f3:cf:58:ae:71:0b:c8:04:6f:34:a3:b2:e4:1e:0c:8b.

Are you sure you want to continue connecting (yes/no)?
```

Type or click **yes** to continue.

You should now be at the class server host prompt, for example:

```
engineer1@lab-jump-srv:~$
```

Use the table below to connect to your ICCAP primary SMM console port from lab-jump-srv through the classroom terminal server (PS2 or PS4).

ICCAP	SMM 6
trainlab-iccap1	telnet ps3 2001
trainlab-iccap2	telnet ps3 2002
trainlab-iccap3	telnet ps3 2003
trainlab-iccap4	telnet ps2 2004
trainlab-iccap5	telnet ps2 2005
trainlab-iccap6	telnet ps2 2006

For example:

```
engineer1@lab-jump-srv:~$ telnet ps3 2001
```

This will connect you to your ICCAP console port. Log in with the default username root and the default password casa, for example:

```
Trying 10.5.5.115...
Connected to ps2.sdclasslab.local.
Escape character is '^]'.
console login: root
console password:********<-----This is casa
trainlab-iccap1#
```

Notice the line that says Escape character is '^]'. This is the CTRL key and the right bracket characters on your keyboard. You will use these keystrokes to gracefully disconnect from your telnet session with your ICCAP console. If you do not gracefully disconnect, or if you lose network connectivity and then try to reconnect, you may receive the following message.

```
engineer1@lab-jump-srv:~$ telnet ps2 2004
Trying 10.5.5.115...
telnet: Unable to connect to remote host: Connection refused
```

If you receive this message then contact your lab proctor. They will have to clear the connection so you can proceed.

1.4 Confirm Class Network Connectivity

The lab begins with IP routing already configured. (Later in the lab, you will default your ICCAP and configure routing.) Check that the network is up and functioning. From privileged mode ping the classroom-srv1 IPv4 address. Type **ping 10.4.1.254**. It should be successful; if not inform your proctor.

Type **traceroute 10.4.1.254**. You should see three hops: your VLAN interface, gige 0/0 on R2 (your next hop) and gige 0/1 on R4 which is the gateway for the 10.4.1.0/24 network.

From privileged mode type **show cable modem.**

You should observe your lab station modems in an online state. The modems may have both IPv4 and IPv6 addresses. Example:

```
trainlab-iccap1#show cable modem

MAC Address  IP Address   US     DS    MAC     Prim RxPwr Timing Num BPI

                Intf    Intf   Status   Sid (dB) Offset CPEs Enb

0025.f2ee.9024 192.168.6.58  13/0.0/0  0/0/0  online(pt) 242 0.0  2313  0  yes

386b.bbd7.ea35 192.168.6.65  13/0.0/0  0/0/1  online   241 0.2  2487  0  yes

Output Cut.......
```

Next confirm your OSPFv2 and v3 routes. Type, **show ip route** and **show ipv6 route.** You should have routes to the:

- Backbone Network
- R2 subinterfaces subnets
- Backbone routers and other ICCAP loopbacks
- Other ICCAP IP bundle interfaces

1.5 Debugging

As you move through the rest of this lab, you may find that your networking configurations fail. When that occurs, ALWAYS use debugging to attempt to diagnose the issue.

The ICCAP has two different methods for turning on debugging, depending on how you are connected to it. You are on a console connection, so ensure you are in config mode. Type, **logging system debugging**. Exit config mode.

Type **debug ?** to view your debugging options. You have just verified that OSPF is working, so view your OSPF debugging options by typing, **debug ip ospf ?**

Start debugging OSPF by typing, **debug ip ospf packet all**. Observe your console until you see a few OSPF messages. You should see something similar to:

```
trainlab-iccap1#[Thu Sep 29 14:36:09 2016]-EM-ROUTER-1330860102: smm6: : Instance 1
SEND[Hello]: To 224.0.0.5 via vlan100:10.3.11.6, length 64

[Thu Sep 29 14:36:13 2016]-EM-ROUTER-1330860102: smm6: : Instance 1 RECV[Hello]: From
10.254.5.12 via vlan100:10.3.11.6 (10.3.11.5 -> 224.0.0.5)

[Thu Sep 29 14:36:19 2016]-EM-ROUTER-1330860102: smm6: : Instance 1 SEND[Hello]: To
224.0.0.5 via vlan100:10.3.11.6, length 64

[Thu Sep 29 14:36:22 2016]-EM-ROUTER-1330860102: smm6: : Instance 1 RECV[Hello]: From
10.254.5.12 via vlan100:10.3.11.6 (10.3.11.5 -> 224.0.0.5)
```

Turn off OSPF debugging by typing, no debug ip ospf packet all.

Use this method for your initial troubleshooting of any problems you have in this lab.

2 Upgrading your ICCAP

Now that we have confirmed everything is working normally, in this section we will save the startup configuration and default your ICCAP. In addition, we will upgrade the software and perform a service patch.

Save the current startup-configuration file to a custom file stored in NVRAM by typing, **copy nvram startup-config nvram prep-upgradeX,** where X is your ICCAP#.

You can view the contents of files that are on the local nvram by using the **show nvram <filename>** command.

View the contents of the file prep-upgradeX; type, **show nvram prep-upgradeX.**

As a second backup, copy prep-upgradeX to the class tftp server. Type, **copy nvram prep-upgradeX tftp 10.4.1.254.** You should see a similar message to the one below:

```
putting /fdsk/pepupgrade3 to 10.4.1.254:prepupgrade3 [octet]

Sent 35086 bytes in 0.2 seconds [1818243 bit/s]
```

Display the current software version. Type, **show bootdev;** it should be **ccsi.gz.rel7.2.6.1_build7b6a**.

Now, let's upgrade the software. To upgrade the software successfully, you MUST remove any patches that have been installed to the current code version. Revert and disable the patch file with the **system patch revert** command. This may take up to 10 minutes to complete.

FTP the new software to the ICCAP with the **copy ftp guest 10.4.1.254 /home/guest/ccsi.gz.rel8.6.4.3_build98b2 nvram** command. You will be prompted for your password, which is **lab_files**.

If successful you should see similar messages to those in the figure below.

```
...ccsi.gz.rel8.6.4.3_build98b2:  ETA:  5:19  0.00/ 65.19 MB 208.
...ccsi.gz.rel8.6.4.3_build98b2:  ETA:  0:09  1.08/ 65.19 MB  7.
...ccsi.gz.rel8.6.4.3_build98b2:  ETA:  0:08  7.79/ 65.19 MB  6.
...ccsi.gz.rel8.6.4.3_build98b2:  ETA:  0:07  38.17/ 65.19 MB  3.69 MB/s
Output Cut.....................................................................
.....................................................................
.....................................................................
.....................................................................
Sent 68352000 bytes in 36.8 seconds [14868147 bit/s]
move file to fdsk of peer smm
```

From privileged mode type **ls.** You see the new software on the file system.

Upgrade the ICCAP to the new software with the **system bootdev nvram ccsi.gz.rel8.6.4.3_build98b2** command.

If successful you should see messages similar to the figure below:

```
...H/W information was updated successfully
[Tue Jul 22 17:54:06 2014]-AL-CLI-1: smm6: User root Updated system boot device to
NVRAM, bootfile=ccsi.gz.rel8.6.4.3_build98b2
update system bootdev of peer smm
Output Cut.......
update smm system bootdev successful
```

Next, configure your ICCAP to reboot in one minute and assign a reason that will be logged to the syslog by typing, **system reboot reason "training lab upgrade" in 1.**

In one minute you should see your ICCAP reboot messages being displayed on your screen. Give the ICCAP about five minutes to completely reboot. **Note: you may have to hit enter after messages have stopped to get the default log in prompt.**

Log in to your ICCAP.

3 Layer 2 and Layer 3 Configurations

Prepare for the rest of the lab by booting your ICCAP to a clean configuration. Start by removing your startup configuration file. Type **rem startup-config** or **del startup-config**, and confirm you want to remove the startup configuration file by typing **Yes**. Reboot your ICCAP with the **system reboot** command. Wait for your system to reboot.

In this section we will assign IP addresses, configure a VLAN and enable a routing protocol. For the latter, you have your choice of OSPF v2 and v3 or ISIS. Please choose only one and proceed to the appropriate section.

Use the information in the table below for the required configuration information.

Device	Interface	IPv4 Address	IPv6 Address	Loopback Address	OSPFv3 RID	ISIS NET-ID
ICCAP 1	VLAN 100	10.3.11.6/30	fd25:5899:2cba:b390::2/64	10.254.1.1/32	10.10.10.10	49.0001.1720.1600.0011.00
ICCAP 2	VLAN 200	10.3.12.10/30	fd0a:e4fb:a312:bb1b::2/64	10.254.2.1/32	20.20.20.20	49.0001.1720.1600.0013.00
ICCAP 3	VLAN 300	10.3.13.14/30	fd44:70a4:fda1:c3ca::2/64	10.254.3.1/32	30.30.30.30	49.0001.1720.1600.0015.00
ICCAP 4	VLAN 400	10.3.14.18/30	fd8a:8264:c20d:4f4f::2/64	10.254.4.1/32	40.40.40.40	49.0001.1720.1600.0017.00
ICCAP 5	VLAN 500	10.3.15.22/30	fd95:814e:9487:bde9::2/64	10.254.5.1/32	50.50.50.50	49.0001.1720.1600.0019.00
ICCAP 6	VLAN 600	10.3.16.26/30	fd22:b541:ee3b:4801::2/64	10.254.6.1/32	60.60.60.60	49.0001.1720.1600.0021.00
ICCAP 1	eth 6/0	192.168.200.100				
	eth 7/0	192.168.200.101				
ICCAP 2	eth 6/0	192.168.200.102				
	eth 7/0	192.168.200.103				
ICCAP 3	eth 6/0	192.168.200.104				
	eth 7/0	192.168.200.105				
ICCAP 4	eth 6/0	192.168.200.106				
	eth 7/0	192.168.200.107				
ICCAP 5	eth 6/0	192.168.200.108				
	eth 7/0	192.168.200.109				
ICCAP 6	eth 6/0	192.168.200.110				
	eth 7/0	192.168.200.111				
ICCAP 1	IP Bundle 1 - CM	192.168.1.1/24	fd8c:ad35:46e5:461d::1/64			
	IP Bundle 1 - CPE	172.16.1.1/24	N/A			
	IP Bundle 1.2 - CPE	172.16.11.1/24	N/A			
ICCAP 2	IP Bundle 1 - CM	192.168.2.1/24	fd4d:77b8:26fa:73c6::1/64			
	IP Bundle 1 - CPE	172.16.2.1/24	N/A			
	IP Bundle 1.2 - CPE	172.16.12.1/24	N/A			

Device	Interface	IPv4 Address	IPv6 Address	Loopback Address	OSPFv3 RID	ISIS NET-ID
ICCAP 3	IP Bundle 1 – CM	192.168.3.1/24	fd56:a21e:6d08:ed24::1/64			
	IP Bundle 1 – CPE	172.16.3.1/24	N/A			
	IP Bundle 1.2 – CPE	172.16.13.1/24	N/A			
ICCAP 4	IP Bundle 1 – CM	192.168.4.1/24	fd8e:993b:0b92:1988::1/64			
	IP Bundle 1 – CPE	172.16.4.1/24	N/A			
	IP Bundle 1.2 – CPE	172.16.14.1/24	N/A			
ICCAP 5	IP Bundle 1 – CM	192.168.5.1/24	fd0b:41d3:3a8c:3565::1/64			
	IP Bundle 1 – CPE	172.16.5.1/24	N/A			
	IP Bundle 1.2 – CPE	172.16.15.1/24	N/A			
ICCAP 6	IP Bundle 1 – CM	192.168.6.1/24	fdac:97b4:7e30:03c6::1/64			
	IP Bundle 1 – CPE	172.16.6.1/24	N/A			
	IP Bundle 1.2 – CPE	172.16.16.1/24	N/A			

Enter configuration mode. Type,

config

Configure the hostname on your system with the **hostname trainlab-iccapX** command, where "X" is your ICCAP number.

3.1 C100G Instructions (Engineer 1 through Engineer 5)

Configure gige 6/0 and 7/0 into a trunk. Type,

interface trunk 1
gige 6/0 mode active
gige 7/0 mode active
no shutdown
end

Confirm you are exchanging LACP information with SW2. Type:

show lacp summary

Confirm your gige 6/0 state is "bind". (Port gige 7/0 is not connected, and will remain operationally down.)

```
Trunk Port    Mode   State   Priority Flag  Receive  Send
1   gige6/0  active  bind   32768   ACDEF  19575   18105
1   gige7/0  active  down   32768   ACDEF  19561   18106
```

Create a VLAN and assign IP addressing and bi-directional forwarding and routing information to the VLAN interface. Refer to the Table of Addresses for the information for your ICCAP number. Type,

interface vlan <your VLAN ID>
trunk 1
ip address <your iv4 address> 255.255.255.252
ipv6 address <your ipv6 address>/64
bfd interval 100 min_rx 100 multiplier 4
no shutdown
end

Configure IP addresses on your eth0 interfaces, to avoid an IP address conflict in the lab. From config mode, use the commands below.

interface eth 6/0
ip address <your eth 6/0 IP Address> 255.255.255.0
end
interface eth 7/0
ip address <your eth 7/0 IP address> 255.255.255.0
exit

3.2 C40G Instructions (Engineer 6)

Enter configuration mode type,

config

Configure gige 2/0 and 3/0 into a trunk. Type,

interface trunk 1
gige 2/0 mode active
gige 3/0 mode active
no shutdown
end

Confirm you are exchanging LACP information with SW2. Type:

show lacp summary

Confirm your gige 2/0 and 3/0 state is "bind".

```
Trunk Port    Mode   State   Priority Flag  Receive  Send
1   gige2/0  active  bind    32768    ACDEF  19575    18105
1   gige3/0  active  bind    32768    ACDEF  19561    18106
```

Create a VLAN and assign IP addressing and bi-directional forwarding and routing information to the VLAN interface. Refer to the Table of Addresses for the information for your ICCAP number. Type,

interface vlan <your VLAN ID>
trunk 1
ip address <your iv4 address> 255.255.255.252
ipv6 address <your ipv6 address>/64
bfd interval 100 min_rx 100 multiplier 4
no shutdown
end

Configure IP addresses on your eth0 interfaces, to avoid an IP address conflict in the lab. From config mode, use the commands below.

interface eth 2/0
ip address <your eth 6/0 IP Address> 255.255.255.0
exit
interface eth 3/0
ip address <your eth 7/0 IP address> 255.255.255.0
exit

3.3 Combined Instructions (All Engineers)

Configure your loopback interface. Type **interface loopback 0** and use the **ip address <your loopback address> 255.255.255.255** command to do so. Exit back to config mode.

Create your first IP bundle interface. Move to interface config mode with the **interface ip-bundle 1** command. Refer to the Table of Addresses, and configure the primary IPv4 interface on your bundle with the **ip address 192.168.X.1 255.255.255.0** command, where "X" is your ICCAP number. Configure a secondary IP address (for your CPEs) with the **ip address 172.16.X.1 255.255.255.0 secondary**

command, where "X" is your ICCAP number. Configure the cable helper address with the **cable helper-address 10.4.1.254** command.

Configure the primary IPv6 address with the **ipv6 address <your ipv6 ip bundle address>** command. Add a primary cable helper address with the **cable helper-ipv6-address fdf6:556d:f7e3:7adf::3** command. Type **show this** to confirm your configuration, and **exit**.

3.4 OSPF v2 v3 Configurations

In this section you will configure your ICCAP to advertise v4 and v6 prefixes using OSPF. Please use the information from **Table 2: Classroom Network ICCAP Addressing** in the Course 1 Table of Addresses document for your configuration information.

Create an OSPf routing instance. From config mode type:

router ospf 1
passive-interface ip-bundle 1
network <your vlan ip subnet>/30 area 0 (Note this is the subnet address of the /30 network)
network <your loopback address>/32 area 0
network <your CM network>/24 area 0
network <your CPE subnet>/24 area 0
area 0 authentication message-digest
log-adjacency-changes
bfd all-interfaces
exit

Assign routing information to your VLAN interface and enable bidirectional forwarding on the vlan interface. Refer to the Table of Addresses for your information for your ICCAP number. Type,

interface vlan <your vlan ID>
ip ospf network point-to-point
ipv6 ospf network point-to-point
ipv6 router ospf 1 area 0.0.0.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 are2@casa
no shutdown
end

Configure Global OSPFv3 parameters. Type:

router ospf6 1
router-id <your router id>
redistribute connected
end
end
clear ipv6 ospf process
yes

3.5 Verifying OSPF Configurations

Now that you have your IPs, VLANs and trunks configured for the NSI, let's verify the routing protocol and BFD configured.

3.5.1 Verify BFD

Confirm BDF. Type, **show bfd session.** You should see an up state, similar to the following:

```
Sess-Idx  Remote-Disc Interface  Lower-Layer Sess-Type  Sess-State UP-Time  Remote-
Addr

 1     1       vlan100  IPv4     Singl-hop  Up     01:13:25 10.3.11.5/32
```

To get more detail on the session type; **show bfd session detail.**

3.5.2 Verify OSPFv4

In this section we will verify OSPF routing. The steps to verify basic OPSF are:

- Verify OSPF routing protocol
- Verify OSPF interface information
- Verify OSPF neighbors
- Verify OSPF routes that are learned by the ICCAP
- Verify configured IP routing protocol processes
- Verify OSPF LSDB

Use the show ip ospf command to display general information about OSPF routing processes. Type **show ip ospf**.

Examine the output of this command and look for the:

- Router ID
- OSPF timers

- Number of times the SPF algorithm has executed
- LSA information
- Authentication

Use the show ip ospf interface command to display OSPF related interface information. Type **show ip ospf interface vlan< your VLAN number>.**

Examine the output of this command and verify:

- OSPF is running on the interface and which OSPF area that interface is in
- Process ID
- Router ID
- OSPF Network Type

Use the **show ip ospf neighbor** command to verify you have an adjacency(s) with upstream routers. This command can also display more verbose information by adding the **detail** argument. Type, **show ip ospf neighbor detail.**

Examine the output of this command and verify:

- The adjacency state
- The neighbor's Router ID
- The neighbor's IP interface address

Use the s**how ip OSPF database** command to display the OSPF v4 Link State Database (LSDB). Type, **show ip ospf database.**

Examine the output of this command and verify:

- LSA types per area
- Advertising router
- Link ID

Because the OSPF topology can be very large, the ip ospf database command can specify detail on the different links in the database. Type **show ip ospf database ?** to see a list of the arguments you can use to display a specific link type or advertising router.

3.6 Verify OSPFv3

Many of the same OSPFv2 verification commands are available for OSPFv3. Use the show ip ospf command to display general information about OSPF routing processes. Type **show ipv6 ospf**

Examine the output of this command and look for the

- Router ID - Notice here we specified a router ID in the configuration. OSPFv3 maintains the 32 bit dotted decimal notation from OPSFv2. If you do not configure a RID then it will use the v4 loopback address or ip interface address.
- Process uptime
- Number of times the SPF algorithm has executed
- LSA information
- Authentication

Use the show ip ospf6 interface command to display OPPF related interface information. Type, **show ipv6 ospf interface vlan< your VLAN number>.**

Examine the output of this command and verify:

- IPv6 Prefixes
- Process ID
- Router ID
- OSPF Network Type
- Neighbor Counts

Use the **show ip ospf neighbor** command to verify you have an adjacency(s) with upstream routers. This command can also display more verbose information by adding the detail argument. Type, **show ipv6 ospf neighbor detail**.

Examine the output of this command and verify:

- The adjacency state
- The neighbor's Router ID
- The neighbor's IPv6 interface address. Note this will be the link local address of the the upstream router(R2). OPSV3 and IPV6 use the link local address to establish and maintain adjacencies.

Type **show ipv6 ospf neighbor** and compare the output with that of the show ipv6 ospf neighbor detail command. Examine the output of this command and determine whether you can verify:

- The adjacency state
- The neighbors Router ID
- The neighbors IP interface address

Use the **show ipv6 route ospf** command and the classroom network diagram to verify OPSF routes in the IP routing table. Type, **show ipv6 route ospf.**

Examine the output of this command and verify:

- You have connectivity to all other ICCAP VLAN interfaces
- You have connectivity to the Provisioning subnet
- You have connectivity to Backbone network

Use the **show ipv6 ospf database** command to display the OSPF v6 Link State Database (LSDB) type, **show ipv6 ospf database.**

Examine the output of this command and verify:

- LSA types per area,
- Advertising router
- Link ID

Use the show ipv6 neighbor command to show your link local addresses type **show ipv6 neighbor**.

Examine the output of this command and verify:

- Link Local addresses for your ip bundle interface
- Link Local addresses for your VLAN interface

3.7 OSPF ASBR Configuration

Small businesses that need internal routing commonly use RIP for that purpose, and MSOs that support those businesses commonly redistribute those RIP routes across their network. In this section of the lab you will explore redistributing a RIP route using a route map.

3.7.1 Create a RIP Instance

Configure an interface on your ICCAP that will run RIP. To do so, move to config level and create an IP bundle sub-interface with the **interface ip-bundle 1.2** command. Assign the bundle an IP address according to the table of addresses earlier in this document, with the ip address <your IP Bundle 1.2 – CPE address> 255.255.255.0 command. Type **exit**.

Configure a RIP instance with the **router rip** command. Add your IP bundle 1.2 interface to the RIP instance with the **network <your IP Bundle 1.2 – CPE address>/24** command, and exit.

3.7.2 Create an IP Prefix List

Create an IP prefix list to identify your RIP route. From config mode, enter the **ip prefix-list redistribute_rip permit 172.16.1X.1/24** command, where "X" is your ICCAP number, and then exit. Check your work with the show ip prefix-list detail command.

3.7.3 Create a Route Map

Next, create a route map. From config mode, enter the **route-map connect_rip_to_ospf permit 10** command. Configure the route map to reference your prefix list with the **match ip address prefix-list redistribute_rip** command, and then exit.

3.7.4 Redistribute Your RIP Route

Now, configure OSPF to redistribute the RIP routes that match the routes in your prefix list. From config mode, move to **router ospf 1** configuration mode. Type **redistribute connected route-map connect_rip_to_ospf.** Check your configuration with the **show this** command. Type **exit**.

3.7.5 Check Your Work

Check your work with the **show ip ospf database** command. At the end of the output you should see your IP bundle 1.2 interface advertised as an AS External Link.

If other engineers in your class are configuring OSPF ASBRs, you may be able to see those routes with the show ip route command.

Type **show ip ospf** and examine the output. Look for the line that says, "This router is an ASBR (injecting external routing information)".

Confirm that you are receiving intra-area routes with the **show ip ospf border-routers** command.

Do NOT perform IS-IS configurations. Move to topic 3.11, IBGP/LDP/MPLS Configurations.

3.8 ISIS Configurations

Create a VLAN and assign IP addressing and routing information to the VLAN interface. Refer to Table 2: Classroom Network ICCAP Addressing in the Course 1 Table of Addresses document for your information for your ICCAP number. Type:

interface vlan <your VLAN ID>
trunk 1
ip address <your ip v4 address>
ipv6 address <your ipv6 address>
ip router isis ICCAPX (where X is your ICCAP number)
ipv6 router isis ICCAPX (where X is your ICCAP number)
isis network point-to-point
no shutdown
exit

Configure an IPv4 loopback address. Type:

interface loopback 0
ip address <your loopback ip address> 255.255.255.255
end

Configure Global IS-IS parameters. Type,

router isis ICCAPX (where X is your ICCAP number)
metric-style wide
net <your NET-ID>
redistribute connected level-1-2
address-family ipv6
redistribute connected level-1-2
exit-address-family

Use the **show ip route isis** command and the classroom network diagram to to verify ISIS routes in the IP routing table. Type, **show ip route isis.**

Examine the output of this command and verify:

- You have connectivity to all other ICCAP VLAN interfaces
- You have connectivity to the Provisioning subnet
- You have connectivity to Backbone network

Use the show ipv6 route ospf command and the classroom network diagram to to verify IS-IS routes in the IP routing table type, **show ipv6 route isis.**

Examine the output of this command and verify:

- You have connectivity to all other ICCAP VLAN interfaces
- You have connectivity to the Provisioning subnet
- You have connectivity to Backbone network

Use the show ipv6 neighbor command to show your link local addresses type show **ipv6 neighbor**.

Examine the output of this command and verify:

- Link Local addresses for your ip bundle interface
- Link Local addresses for your VLAN interface

Note the CATV MAC link locals are used for the CMs and CPEs on the HFC network.

3.9 ISIS Redistribution Configurations

Small businesses that need internal routing commonly use RIP for that purpose, and MSOs that support those businesses commonly redistribute those RIP routes across their network. In this section of the lab you will explore redistributing a RIP route using a route map.

3.9.1 Create a RIP Instance

Configure an interface on your ICCAP that will run RIP. To do so, move to config level and create an IP bundle sub-interface with the interface ip-bundle 1.2 command. Assign the bundle an IP address according to **Table 2: Classroom Network ICCAP Addressing** in the Course 1 Table of Addresses document, with the ip address <your IP Bundle 1.2 – CPE address> 255.255.255.0 command. Type exit.

Configure a RIP instance with the **router rip** command. Add your IP bundle 1.2 interface to the RIP instance with the **network <your IP Bundle 1.2 – CPE address>/24** command, and exit.

3.9.2 Redistribute Your RIP Route

Now, configure ISIS to redistribute the RIP routes that match the routes in your prefix list. From config mode, where X is your ICCAP number, move to router isis ICCAPX configuration mode. Type the command below.

redistribute connected level-1-2

Check your configuration with the s**how this** command.

3.9.3 Check Your Work

Check your work with the **show isis database** command.

If other engineers in your class are configuring their ICCAPs to redistribute RIP, you may be able to see those routes with the show ip route command.

3.10 Verifying ISIS Configurations

Consult the Training Lab Diagram in your Course 1 Table of Addresses document for a graphic presentation of the connections in the lab.

3.10.1 Verify IS-IS V4

In this section we will verify IS-IS routing. The steps to verify basic IS-IS are:

- Verify IS-IS interface information
- Verify IS-IS neighbors
- Verify IS-IS routes that are learned by the ICCAP
- Verify IS-IS LSDB

Begin with basic interface verification. Type **show isis interface vlan <your vlan ID>** and examine the output. Look for the:

- Routing protocol
- Network Type
- Circuit type
- IPv6 Interface address
- Number of active level-2 adjacencies

Verify your ISIS neighbors. Type **show isis neighbors** and determine from the output who your neighbor is.

Verify that you are learning routes through ISIS with the **show ip[v6] isis** route command. Issue both the "ip" and the "ipv6" versions of the command, and locate your L2 routes and your External routes.

Examine your ISIS database. Type **show isis database** and identify how many Level-1 LSAs and how many Level-2 LSAs your ICCAP is receiving. View the same information in more detail with the show isis database verbose command.

Verify your next hop information with the **show isis topology** command. What is the next hop to all of the Level-2 routers?

4 SysAdmin Configurations

In this lab you will implement common "out of the box" SysAdmin configurations.

Typically, you'll want to create a login banner on your ICCAP that stipulates that the admin user agrees to the terms and conditions of accessing the CLI. Be careful when you do so: it is possible that, if you make a mistake in configuring your login banner, you could lose the ability to connect to your ICCAP via telnet.

You will not create a login banner in this lab.

Should you wish to create a login banner on your network, you would follow the procedure below. Again, do not perform this procedure in this lab.

You would move to config mode, type "banner login" and hit return. The ICCAP will capture the text you enter and use it as a banner. You would type something like:

```
**************************************************

WARNING: By using this system, you agree to comply with Casa Systems' Corporate
policies governing the access and use of Casa's systems and data. Activites on this
system are monitored and recorded and are subject to audit. Unauthorized access or
use of this system is prohibited and subject to disciplinary actions as well as
potential criminal and/or civil penalties.

**************************************************
```

Note that your banner login configuration must end with a period (".") all by itself on a line. Note also that you must put quotation marks around an apostrophe.

4.1 Enable the "Save Configuration" Message

The system reboot confirm command configures the ICCAP software to display a "save configuration" message to remind you to either save the configuration before a system reboot (in privileged mode), or to proceed with the reboot without saving the latest configuration.

Connect to your ICCAP via the console port and move to config mode. Use the **system reboot confirm** to enable the save configuration message.

4.2 Telnet settings

By default a maximum number of concurrent sessions are 31. This can be changed with the line vty <number> command. Telnet can be disabled in version 6.4 or above.

Explore your current telnet configuration with the command **show telnet port**. The default is the well-known port 23. If you need to change it use the telnet port <port number> command. DO NOT CHANGE THE PORT. THIS IS INFORMATIONAL ONLY. Continue your exploration by viewing the the number of default connections with the **line vty ?** commmand.

Change the maximum number of connections with the line vty <1-31> command to 12.

Display your configuration by typing, **show running-config | inc line.**

4.3 SSH configuration

Note: these ssh commands are informational only. Do NOT generate ssh keys in this lab.

From config mode, explore your ssh config mode options with the **ssh ?** command. Examine the output and look for:

The ability to enable ssh

The ability to set the ssh server port number

Return to root privileged mode. Type **exit**.

Explore your ssh key options. Type, **ssh-server gen-hostkey ?** Examine the output and look for:

The ability to generate a DSA key

The ability to generate an RSA key

Backspace out of your command and type **show ssh server** to verify that SSH is enabled. The ICCAP allows 64 SSH sessions by default.

4.4 Set the System Time

Configure your ICCAP to the correct system time. From **config** mode, start by using the **show timezone list** command to explore your timezone options. Locate the timezone string for New York. Type **Q** to halt the output, and issue the **system timezone <string>** command to put the ICCAP in that timezone. Complete your configuration by setting the date and time with the **system clock <MMDDhhmmYYYY>** command. Use a 24-hour click for setting the hour value.

Confirm your configuration with the **show clock** command.

4.5 Configure Network Time Protocol

You can also configure the ICCAP to get its time from a Network Time Protocol server. Use the **ntp server 10.4.1.254** command to do so. Then tell the ICCAP to synchronize with the NTP server with the **ntp sync 10.4.1.254** command.

Examine the output of this command and look for:

The offset value – how far off from NTP the ICCAP was

The NTP server restart nameserver 10.4.1.254 process

4.6 Configure DNS

Configure the ICCAP for the classroom Domain Server from configuration mode. Type, **nameserver 10.4.1.254.**

Add the domain name to your ICCAP. Type, **ip domain-name sdclasslab.local**.

4.7 Privileged Mode Password

Typically the passwords to the ICCAP will be protected with an external AAA system, TACACS+, RADIUS etc. Basic password administration can also be entered manually on each ICCAP in the local AAA database.

Change the vty privileged mode password to "userX" where X is your ICCAP number with the **password userX** command.

This command changes only the vty password. There is a separate command to change the console privileged mode password.

Exit gracefully out of your telnet connection to your ICCAP by typing **exit exit** to return to non-enable prompt ICCAPX>. Then type **<CTRL>]** to exit to telnet>, and **quit** to exit to lab-jump-srv.

Reconnect to your console session, and try to login to privileged mode with casa password. You should be unsuccessful, since you just changed the password.

Reset your password to the default casa at the non-privileged mode prompt by typing the **reset password** command. You may receive the error message Cannot open Password file: No such file or directory.

Now login to privileged mode with the casa default password.

Note that you can reset the enable password from the privileged mode or in the case where the privileged mode password is not known you can reset it from non-privileged mode console connection with the reset console-password command.

4.8 Encrypting Network Service Passwords

The service password-encryption command enables encryption of DES 56 for passwords, such as BGP neighbor passwords, RIP, OSPF, and IS-IS protocol authentication passwords on GigE interfaces. By default, passwords are not encrypted in the ICCAP running configuration.

From configuration mode, enable the hashing of all passwords created in the ICCAP such as RIP, OSPF, etc., with the **service password-encryption** command.

4.9 Adding Local Users

In this section of the lab you add two local users to the ICCAP: a local superuser with all privileges, and an operator user who can execute show commands.

From configuration mode, create a superuser with a privilege level of 15, a username of ckent and password of Superman15 with the **adduser ckent privilege 15** command. When the ICCAP prompts you to enter a password, type: **Superman15**.

Reenter the password when you are prompted.

Now, create an Operator level user with a privilege level of 1, with a username of jimmy and a password of Olson1. Use the command **adduser jimmy privilege 1**. When the ICCAP prompts you for the password, use **Olson1**.

Exit to lab-jump-srv.

From lab-jump-srv, ssh to your ICCAP as jimmy with the command **ssh jimmy@<your ICCAP ip address>**. Enter **Olson1** as your password.

Type **?** to see your available CLI commands. What are your options?

Type **show ?** to see your available show commands. What are your options?

Attempt to move to privileged mode. Type: **enable** and note the error message you receive.

Log out of your ICCAP. From Class Server 1, ssh to your ICCAP as ckent with the **ssh ckent@<your ICCAP ip address>** command. Enter **Superman15** as your password.

Move to config mode and type **show user**. Examine the output of your command and look for:

Users with superuser privileges

Users with operator privileges

Verify that user ckent has full admin privileges by deleting the user "jimmy". Type **deluser jimmy** and then reissue the **show user** command. How has the output changed?

Log out of your ICCAP and reconnect through the console port. Move to config mode and issue the **deluser ckent** command. Use **show user** to view your resulting user list.

4.10 Creating Aliases

In this section of the lab you will create CLI aliases for common commands. Use the alias command to create the aliases listed below.

alias ccm "clear cable modem"
alias cpu "show cpu-process | exc 00:00:00"
alias du "show docsis downstream channel utilization"
alias scgv "show service group verbose"
alias scm "show cable modem"
alias scmv "show cable modem verbose"
alias uptime "show cpuinfo all | i up"
alias crs "copy running-config startup-config"

Check your work by typing, **show alias**.

4.11 Configuring Local Logging

By default, the Casa ICCAP saves logging messages to local flash as a log file. Logging levels determine the level of information collected in the log file. This section of the lab demonstrates how changing the logging level will change the information the ICCAP reports.

Make sure you have two connections to your ICCAP: one through the console port (telnet through the terminal server) and one via ssh. In your console session, move to privileged mode. In your ssh connection, move to configure mode.

In either session, use the **show logging all** command to view your default logging settings. Examine the results of this command and look for:

- Which logging targets are receiving errors

- Which logging targets are receiving warnings
- Which logging targets are not receiving log messages

From your ssh session set your logging level for the console to “informational” with the **logging system informational** command. From your console connection, examine the results of this command and look for:

- The active SMM module
- The time and date the command was executed

Switch back to your ssh connection to the ICCAP. Exit config mode and save your configuration as logging_test with the **copy run nvram logging_test** command. From your console connection, examine the results of this command and look for:

- Which user executed the copy command
- The name of the saved file

Switch back to your ssh connection to the ICCAP. Delete the file logging_test with the **del logging_test** command. Note that you do not receive a message.

From your ssh connection to the ICCAP, enter config mode. View your logging levels with the **show logging all** command Note how the output differs from the default logging levels.

Reconfigure your logging levels to their defaults with the **logging system errors** command. Note that you see no message in your telnet connection.

Exit config mode and execute the commands below.

copy run nvram logging_test
del logging_test

Note that you see no messages in your console connection.

4.12 Configuring Syslog

Configure your ICCAP to log to a remote Syslog server. Move to config mode and use the command **logging host 10.4.1.254**. Set the logging level to warning with the **logging syslog warning** command. Then check your work by typing, **show syslog**.

Set your ICCAP to use its loopback interface as the source address for all Syslog logging messages with the **logging source-interface loopback 0** command.

4.13 Configuring SNMP

In this section of the lab we will use the class server to issue SNMP queries to the ICCAP and cable modems. Many customers do not use command line SNMP for Diagnostics, so this lab is optional.

4.13.1 Configure SNMP Communities

From root privileged mode, type: **snmp default**. You may receive a warning message; if so, type **yes**. Move to config mode, and configure an SNMP read only community name with the **snmp community readmibs ro** command. Then, configure a read/write community string with the **snmp community letmewrite rw** command.

Restart the SNMP processes. Move to diag mode by typing **diag**. Enter the diag mode password, **casadiag**. Shut down the SNMP process by typing, **snmp shutdown**. Restart the SNMP process by typing, **snmp start**. Type **exit** to return to config mode.

Configure the SNMP syscontact with the **device contact admin@casa-sytems.net** command. Then, configure the SNMP location with the **device location training_lab** command.

Save your configuration.

4.13.2 SNMPv2

This section of the lab gives you practice in configuring SNMPv2 settings on your ICCAP. You will establish three SNMP communities:

- An SNMP community with full read/write access
- An SNMP community with full read only access
- An SNMP community with limited read only access

4.13.2.1 Initial Configuration

Reconnect to your ICCAP. Enter config mode. Begin by establishing lab-jump-srv as your SNMP trap receiver for SNMP version 2, by typing the command below.

snmp tgt-addr lab-jump-srv snmpUDPDomain 10.4.1.254 500 1 TrapV2cSNMPv2cTrapsTagList TrapV2cSNMPv2cTraps non-volatile 0.0.0.0 500

Note that in this command, "500" refers to the retry time should a trap not go through, and "1" refers to the number of retries.

Configure the ICCAP to use SNMPv2 for its inform messages with the **snmp inform version 2** command.

Configure the notify properties with the **snmp notify tapUserTrapTagList tapUserTrapTagList trap non-volatile** command.

Configure your loopback interface as the SNMP trap source with the **snmp trap-source loopback 0** command.

Configure the SNMP syscontact with the **device contact admin@www.casa-systems.net** command. Then, configure the SNMP location with the **device location training_lab** command.

4.13.1 Protocol Independent Multicast SNMP Support

The Casa ICCAP provides SNMP support for sending traps on Protocol Independent Multicast (PIM) events. View the PIM events on which you can establish traps. From config mode, type: **ip pim trap ?**

Set traps on all three of your trapping options. Type:

ip pim trap invalid-pim-message enable
ip pim trap neighbor-change enable
ip pim trap rp-mapping-change enable

Check your work with the **show running-config | include "ip pim"** command. Your results should be similar to those below.

```
ICCAP2(config)#show running-config | include "ip pim"

ip pim trap neighbor-change enable

ip pim trap rp-mapping-change enable

ip pim trap invalid-pim-message enable
```

4.13.2 Enabling SNMP on Your Cable Modems

For the purposes of our lab, establish SNMP querying of your cable modems every 30 minutes with the **cable modem remote-query 30** command. The query generates a great deal of SNMP traffic, so in large deployments it is common to configure the query at more extended intervals. The largest configurable query interval is 1800 minutes, or one day.

5 Access Controls (ACLs)

Introduction

This section of the lab gives you practice in configuring simple access controls on your ICCAP. Access controls manage IP access to the ICCAP via certain interfaces, access groups, and access classes. The interfaces are the Ethernet management interface, gigabit Ethernet data traffic interfaces, and DOCSIS mac-domain interfaces. The access classes are incoming and outgoing classes. The access controls deny or permit the flow of data traffic to or from user-defined IP addresses and upper layer protocols specified in the IP protocol (TCP, UDP) field, such as tcp, udp, tftp, telnet, etc.

The Casa ICCAP supports two forms of IP access control for interfaces: Access Groups and Access Classes.

To implement IP access control, start by creating an Access Control List (ACL). You can then apply the ACL globally, as an access class, or on specific interfaces, as an access group.

5.1 Creating an Access Group on an Interface

An Access Group is simply an Access Control List applied to a specific interface.

Open a second connection from your computer to lab-jump-srv. From lab-jump-srv, connect to your ICCAP either by ssh or by your console connection through the terminal server.

Create an ACL that will deny Telnet access from lab-jump-srv. Move to **config** mode, and begin to create your ACL with the **ip access-list restrict-telnet** command. Enter the commands below to create your ACL.

remark "deny TELNET access from lab-jump-srv"
deny telnet 10.4.1.254 255.255.255.255 any
exit

Note that on the ICCAP there is neither an implicit "permit all" nor an implicit "deny all" at the end of an ACL.

View your IP interfaces with the **show ip interface brief** command and locate your VLAN interface. Move to the interface configuration level for that VLAN – for example, for VLAN 200 type, interface vlan 200. Use the **show this** command to view your current VLAN interface configuration.

Apply your ACL to inbound traffic on your VLAN with the command, **ip access-group restrict-telnet**. Note that the default is to apply the ACL to inbound traffic.

From lab-jump-srv, attempt to telnet to your VLAN ip address. Telnet should time out. Check your work by connecting to your ICCAP from lab-jump-srv using ssh. Your connection should succeed.

On your ICCAP, from interface configuration mode for your VLAN, remove the ACL with the **no ip access-group** command. Attempt again to telnet from Class Server 1; you should succeed.

5.2 Creating a Global Access Class

An Access Class is simply an Access Control List applied globally across all the interfaces of the ICCAP.

Start by creating an ACL that allows ssh only to the loopback address of your ICCAP. From Class Server 1, connect to your ICCAP by your console connection through the terminal server. (Note: do NOT use ssh for this exercise, or you will find yourself cut off from your ICCAP.)

Move to config mode, and begin to create your ACL with the **ip access-list restrict-ssh** command. Enter the commands below to create your ACL.

remark "allow ssh only to the loopback address"
permit ssh any <your loopback IP address> 255.255.255.255
deny ssh any any
exit

You should now be in config mode. From config mode, apply your ACL as an Access Class with the **access-class in restrict-ssh** command.

Test your work. From Class Server 1, ssh to the loopback address on your ICCAP; you should succeed. Exit, and ssh to the IP address on your VLAN interface. You should fail.

From your console connection to the ICCAP, remove your Access Class with the **no access-class in** command. Ensure that you can ssh to your VLAN IP address.

Note that a typical enterprise deployment will used multiple access lists. For example, you might use access lists to define:

- Which Label Switch Routers can be Lable Distribution Protocol (LDP) Neighbors for MPLS
- Which LDP prefixes are allowed
- Which IP addresses are allowed SNMP read-write access
- Which IP addresses are allowed SNMP read-only access
- Which devices are allowed ssh and/or VTY access

- Which TFTP servers are allowed
- Which IPv6 provisioning servers are allowed

You can use the ICCAP's ACL ability to help secure your network.

6 NSI Diagnostics

The ICCAP offers many different “show” commands you can use to investigate what is occurring on your Network Side Interface.

You can use “show” commands from all four CLI modes. Each mode gives you access to all the global commands; both diag mode and privileged mode provide a set of show commands unique to that mode.

6.1 Diagnosing Interface Issues

Move to diag mode. View all your configured IP interfaces:

show ip interface brief

Type **show ip interface ?** and explore the various IP interfaces you can see.

View statistics on a specific controller interface:

show controller <interface type>

Type **show controller ?** to view the types of interfaces you can view. Look at each of the controller interfaces.

show controller upstream: compare the number of broadcasts, errors, and unerroreds on each upstream interface.

show controller gige: compare the number of in unicast packets on your gige ports.

Check the admin and operational status on your Ethernet ports.

show iftable eth

6.2 Diagnosing Memory and Process Issues

View your RAM statistics:

show meminfo

If RAM is low, show the running processes and the percent of memory each is using:

show cpu-memory process-list

Display the receive rate from the gigabit interface to the cpu interface:

show gigabit-rx-cpu-rate

To check which debugging processes are running:

show debugging

6.3 Diagnosing DHCP Issues

View the DHCP messages that have crossed the ICCAP:

show dhcp-trace

6.4 Diagnosing High Availability Issues

Check your HA configuration.

show ha configuration

Check the current recovery configuration of the hardware.

show ha hardware qam8x192 recovery

Check the communication status between your switch fabrics. Repeat the command below several times to ensure the sequence number is increasing.

show ha switch fault monitor status

6.5 Diagnosing Trunking Issues

Check the LACP status on your trunk.

show lacp summary

6.6 Obtaining System Information

Check the image you are booting to.

show bootdev

To get detailed information regarding environmental conditions of the chassis such as power inputs, fuse conditions, fan RPM, temperature and module temperature, type:

show envm

6.7 Diagnosing Initialization Processes

Exit from diag mode to privileged mode. In privileged mode, type **show alarm** to view any Read or Amber LED statuses.

From root privileged mode type **show dmesg**. This log captures messages from the boot process in a controlled manner after the system has started without having to observe the console output. Even after the system has fully booted, the kernel may occasionally produce further diagnostic messages that will also be captured in this log. Look for any key words like oops, panic or failure.

Type **show log**. System logs deal primarily with the normal functioning of the system. Examples include authorization mechanisms, system daemons, system messages, etc. The logs can tell you almost anything you need to know, as long as you have an idea where to look first. This log is very verbose, so it is recommended this log be searched using a filter or regular expression.

6.8 The show tech command

The “show tech” command combines the output of all the 48 show commands, plus the output of 6 linux shell diagnostic commands that retrieve all logs of recent software processes. These include:

- Show version
- Show system
- Show running config
- The logs in each module (not the system log)

It’s best to create a file with the output of the show tech command, so that you can effectively evaluate it. From lab-jump-srv, ssh to your ICCAP and redirect the screen output to a file in your home directory on lab-jump-srv. Type, **ssh –l root <your ICCAP IP address> | tee showtech.log**.

On the ICCAP, ensure you are in privileged mode. Turn pagination off with the **page off** command.

Type **show tech**. You should see the output of the command on your screen. Wait until it has finished, and then **exit** your ssh session with your ICCAP.

From lab-jump-srv type **ls**. You should see a file called "showtech.log". Review the file with the **less showtech.log** command. Hit enter to advance one line, spacebar to advance one page, and q to exit the file. Use the information to answer the questions below:

- What's the total modem count at this ICCAP?
- Are there any ICCAP Video sessions?
- What are the total multicast clients?
- What are the maximum routes supported in this ICCAP? How many of them are utilized? (see cat /proc/bcm/route-entry-usage)
- What is the current DOCSIS channel utilization?
- How many OSPF neighbors are up currently?

6.9 TCP Dump

The ICCAP supports the tcpdump utility, which allows you to capture all the packets that go whizzing through your interfaces. If you are familiar with tcpdump, everything you know will transfer to the ICCAP with two caveats:

You must be in diag mode to run tcpdump

The tcpdump utility requires you to treat your arguments as a text string, and put that string in quotation marks

6.9.1 Exploring TCP Dump

To explore the TCP Dump utility, open an ssh connection to your ICCAP and move to diagnostic mode. Use the **diag** command and the password **casadiag**. Type **tcpdump -D** to view the interfaces on your ICCAP upon which you can run TCP Dump. In the output, locate your trunk interface and your VLAN interface.

Determine which interface is carrying what kinds of traffic by typing the commands below. (The "-i" flag specifies the interface to capture on.) Observe the output of each command.

tcpdump "-i trunk1"
tcpdump " -i <your vlan interface (e.g., vlan100)>"

What traffic is the trunk carrying? What traffic is the VLAN carrying?

6.9.2 Run TCP Dump on a Specific Protocol

The ICCAP allows you to run TCP Dump to capture the specific protocol of your choice as it crosses the interface. Run TCP Dump to capture DNS on your VLAN with the **tcpdump "-i <vlan interface> tcp port 53 or udp port 53"** command.

Open a second connection to lab-jump-srv, and telnet to your ICCAP through the terminal server. From privileged mode, create a ping that requires DNS resolution, for example, **ping lab-jump-srv.sdclasslab.local**. Observe the TCP Dump capture. Experiment by pinging both IP addresses and domain names.

6.9.3 Run TCP Dump for a Specific Number of Captures

You can use TCP Dump to capture a specific number of packets. To see this behavior, from diag mode type **tcpdump "-i <vlan interface> ip proto 89 -c 10"**. TCP Dump will capture 10 OSPF packets and exit. Observe your output to determine how many packets were received, and how many packets were dropped.

6.9.4 Using TCP Dump to Gather Information

Use TCP Dump to drill down into your OSPF configuration. Use the up arrow to retrieve your last command, and add the –v argument. Your command should look something like **tcpdump "-i <vlan interface> ip proto 89 -c 10 -v"**. Once the capture completes, observe the output of your command. Can you determine:

- The neighbor router IP?
- The OSPF authentication type?
- Your router ID?
- The mask on the network connecting you to your neighbor?
- How often (approximately) the ICCAP is sending updates?

6.9.5 Using TCP Dump to Track Flows

You can use TCP Dump to track traffic between two hosts. In your ssh connection to your ICCAP, from diag mode, configure TCP Dump to report on traffic between your ICCAP's VLAN interface and lab-jump-srv with the **tcpdump "-i vlan300 -n dst host <your ipbundle 1 ip address>"** command.

Exit gracefully (with **ctrl-]** and **quit**) from your telnet connection to your ICCAP. You should be at lab-jump-srv. Ping your ICCAP's ipbundle 1 address. Observe the output of the TCP Dump. Experiment by pinging your ICCAP's loopback address. Telnet to your console connection, and ping 10.4.1.254 from your ipbundle interface. When you have finished experimenting, return to your ssh connection to the ICCAP and press ctrl-C to end the capture.

6.9.6 Writing the Dump to a File for Viewing

You can write your TCP Dump capture to a file for later review. In our labs we use a file called “dumptest” for this purpose. To be sure you get a clean capture, type **ls** and look for the “dumptest” file. If you find it, type **del dumptest** to remove it.

Now, start your capture. Type **tcpdump “-i <vlan interface> -w /fdsk/dumptest –U”** to begin the dump. Note that the “-w” argument tells the ICCAP to “write” to the file name, and the “-U” argument clears the cache so that the file will actually capture the packets. Allow the dump to run for about a minute, then type **ctrl-C**.

If you wish, type **ls** to make sure the file was created. Now, view the file using the **tcpdump “-r /fdsk/dumptest”** command. (The “-r” argument means “read”.) What traffic do you see?

Exit diag mode.

7 RFI Configurations

In this section of the lab we will configure the DOCSIS modules to enable RFI connectivity to enable modems to initialize and register on the ICCAP.

7.1 Enable DOCSIS 3.1

Start by enabling DOCSIS 3.1 capabilities on your ICCAP. Move to config mode and type **cable docsis version 31**.

7.2 Create OFDM Modulation Profiles

Next, create two modulation profiles for OFDM. For your first profile, type **ofdm profile 1** to enter profile configuration context. Type **profile-modulation 256qam** to create the profile, and **end.**

Create your second profile and give it a modulation rate of **128qam**.

7.3 Configure an OFDM Channel for Your Annex B Modems

To configure your OFDM channel, type **interface qam 0/0** to move to interface config mode. Set the start frequency of the OFDM channel with the **ofdm-channel 0 lower-freq 605000000** command. For this lab, hit **Enter** to allow the ICCAP/CCAP to automatically generate your upper frequency and PLC frequency. (Note that you can also set these frequencies manually.)

Specify your preferred and fall-back modulation profiles for the channel. Type **ofdm-channel 0 profile 1 2**.

Enable the channel with the **no ofdm-channel 0 shutdown** command, and type **show this** to check your work.

7.4 Configure a Second OFDM Channel for Your Annex B Modems

Create your second OFDM channel with the **ofdm-channel 1 lower-freq 800000000** command. Specify your modulation profiles by typing **ofdm-channel 1 profile 2 1**. Enable the channel with the **no ofdm-channel 1 shutdown** command, and type **show this** to check your work.

7.5 Configuring Downstream Transmitters for DOCSIS MAC 1 (Annex B)

Type **end** to return to the interface context for QAM 0. Enable your interface with the **no shutdown** command, and configure the specifics of your interface with the commands below.

- Adjust the power to 55 dBmV with the **power 550** command.
- Add a description to channel 0 with the **channel 0 description FNB** command.
- Change the downstream frequencies on channels 0 -2 by typing, **channel 0 frequency 555000000 8**. Note this command will start at the frequency 555 MHZ and then change the next 8 channels by 6 or 8MHz.

Enable each channel. Type **no channel 0 shutdown 8.**

Confirm your configuration. Type **show this** and compare your configuration to the table below. If it matches, save your configuration. Return to config mode.

Downstream Channels			
Module	Port	Channel	Frequency
0	0	0	555 MHz
0	0	1	561 MHz
0	0	2	567 MHz
0	0	3	573 MHz
0	0	4	579 MHz
0	0	5	585 MHz
0	0	6	591 MHz
0	0	7	597 MHz

7.6 Configuring Upstream Receivers

Next, configure your upstream receivers. Type **show interface upstream brief**. Observe the output, and note that all of the upstream frequencies are set to 20 MHz by default. You must configure your upstream interfaces to use the appropriate frequency and to be enabled.

7.6.1 C100G Instructions (Engineer 1 through Engineer 5)

Start by enabling OFDMA on your upstream interface. Type, **module 13 ofdma enable. Exit** to privileged mode, and issue the **reboot module 13** command. Use the **show system** command to verify that module 13 has rebooted.

Move back to config mode. Establish your OFDMA probe interval by typing, **ofdma probe interval 1024**.

Next, create an Interval Usage Code profile for your OFDMA channel. Type, **ofdma iuc-profile 1** to move to the iuc-profile context. Enter the **fine-ranging-iuc 32 800000** command, the **initial-ranging-iuc 32 800000** command, and the **data-iuc 13 modulation 1024qam pilot-pattern 2** command. Type exit to return to config mode.

Create an OFDMA exclusion zone. Type, **ofdma exclusion-band 1**. From that context, type, **exclusion-sc-group 1 17000000 30000000.** Note that this exclusion zone only includes the frequencies of your three lower SC-QAM channels. Exit back to config mode.

Move to interface configuration mode on your 13/0.0 interface by typing, **interface upstream 13/0.0** (where 13 is the slot number, the first 0 is the port and second 0 is the channel. Configure your SC-QAM channels. Set the frequency and enable the interface on logical channel 0 type with the commands below.

frequency 20000000
no shut
no logical-channel 0 shut

Note: At least one logical channel must be enabled for every physical upstream channel enabled.

Repeat the interface configuration process for your other three upstream interfaces, using the commands below.

```
interface upstream 13/0.1
 frequency 24000000
  no logical-channel 0 shutdown
  no shutdown
end
interface upstream 13/0.2
 frequency 28000000
  no logical-channel 0 shutdown
  no shutdown
end
 interface upstream 13/0.3
  frequency 32000000
  no logical-channel 0 shutdown
  no shutdown
end
```

7.6.2 C40G Instructions (Engineer 6)

Start by enabling OFDMA on your upstream interface. Type, **module 5 ofdma enable**. Establish your OFDMA probe interval by typing, **ofdma probe interval 1024**.

Next, create an Interval Usage Code profile for your OFDMA channel. Type, **ofdma iuc-profile 1** to move to the iuc-profile context. Enter the **fine-ranging-iuc 32 800000** command, the **initial-ranging-iuc 32 800000** command, and the **data-iuc 13 modulation 1024qam pilot-pattern 2** command. Type exit to return to config mode.

Create an OFDMA exclusion zone. Type, **ofdma exclusion-band 1**. From that context, type, **exclusion-sc-group 1 17000000 30000000.** Note that this exclusion zone conly includes the frequencies of your three lower SC-QAM channels. Exit back to config mode.

Move to interface configuration mode on your 5/0.0 interface by typing, **interface upstream 5/0.0** (where 5 is the slot number, the first 0 is the port and second 0 is the channel. Configure your SC-QAM channels. Set the frequency and enable the interface on logical channel 0 with the commands below.

- **frequency 20000000**
- **no shut**
- **no logical-channel 0 shut**

Note: At least one logical channel must be enabled for every physical upstream channel enabled.

Repeat the interface configuration process for your other three upstream interfaces, using the commands below.

```
interface upstream 5/0.1
 frequency 24000000
  no logical-channel 0 shutdown
  no shutdown
end
interface upstream 5/0.2
 frequency 28000000
  no logical-channel 0 shutdown
  no shutdown
end
 interface upstream 5/0.3
  frequency 32000000
  no logical-channel 0 shutdown
  no shutdown
end
```

7.6.3 Combined Instructions (All Engineers)

Confirm your configuration with the **show interface upstream brief** command. If your configuration is correct, save it.

7.6.4 C100G Instructions (Engineer 1 through Engineer 5)

Add your OFDMA channel to interface 13/0.0 From config mode type, **interface ofdma 13/0.0** to enter OFDMA configuration context. Establish the width of your channel by typing, **lower-freq 10000000 upper-freq 85000000**. Specify the IUC profile by typing, **iuc-profile 1.** Add your exclusion zone by typing, **exclusion-band 1** and turn on the channel with the **no shutdown** command. Return to config mode by typing **exit**.

7.6.5 C40G Instructions (Engineer 6)

Add your OFDMA channel to interface 5/0.0. Type, **interface ofdma 5/0.0** to enter OFDMA configuration context. Establish the width of your channel by typing, **lower-freq 10000000 upper-freq 85000000**. Specify the IUC profile by typing, **iuc-profile 1**. Add your exclusion zone by typing, **exclusion-band 1** and turn on the channel with the **no shutdown** command. Return to config mode by typing **exit**.

7.7 Configuring Downstream Transmitters for an Annex A MAC Domain (All Engineers)

Next, create an Annex A DOCSIS MAC domain on your ICCAP.

Enter interface context for the QAM module 0 with the **interface qam 0/1** command. View the interface configuration with the show this command. Type q to exit the output.

- Set the interface to Annex A with the **annex A** command. (Note that the "A" must be a capital A.)
- Adjust the power to 55 dBmV with the **power 550** command.
- Add a description to channel 0 with the **channel 0 description FNA** command.
- Change the downstream frequencies on channel 0 by typing, **channel 0 frequency 650000000 8**
- Enable channel 0. Type, **no channel 0 shutdown 8**
- Type **show this** and confirm your configuration matches the table below.

Downstream Channels			
Module	Port	Channel	Frequency
0	1	0	650 MHz
0	1	1	658 MHz

0	1	2	666 MHz
0	1	3	674 MHz
0	1	4	682 MHz
0	1	5	690 MHz
0	1	6	698 MHz
0	1	7	706 MHz

- Enable your interface with the **no shutdown** command.
- Type **end** to exit back to config mode.

7.8 Configuring Upstream Receivers for an Annex A MAC Domain

Your Annex A MAC domain requires upstream receivers.

7.8.1 C100G Instructions (Engineer 1 through Engineer 5)

Move to interface configuration mode on your 13/1.0 interface by typing, **interface upstream 13/1.0** (where 13 is the slot number, the first 1 is the port and second 0 is the channel. Set the frequency and enable the interface on logical channel 0 with the commands below.

frequency 20000000
no shut
no logical-channel 0 shut

Note: At least one logical channel must be enabled for every physical upstream channel enabled.

Repeat the interface configuration process for your other three upstream interfaces.

Use the frequency argument to change the upstream frequencies from the default of 20 MHz for each of the channels other than the first. Consult the table below for the appropriate frequencies.

Upstream Channels			
Module	Port	Channel	Frequency
13	0	0	20 MHz
13	0	1	24 MHz
13	0	2	28 MHz
13	0	3	32 MHz

7.8.2 C40G Instructions (Engineer 6)

Move to interface configuration mode on your 5/1.0 interface by typing, **interface upstream 5/1.0** (where 5 is the slot number, the first 1 is the

port and second 0 is the channel. Set the frequency and enable the interface on logical channel 0 with the commands below.

frequency 20000000
no shut
no logical-channel 0 shut

Note: At least one logical channel must be enabled for every physical upstream channel enabled.

Repeat the interface configuration process for your other three upstream interfaces.

Use the frequency argument to change the upstream frequencies from the default of 20 MHz for each of the channels other than the first. Consult the table below for the appropriate frequencies.

Upstream Channels			
Module	Port	Channel	Frequency
5	0	0	20 MHz
5	0	1	24 MHz
5	0	2	28 MHz
5	0	3	32 MHz

Confirm your configuration with the **show interface upstream brief** command. If your configuration is correct, save it.

7.8.3 C100G Instructions (Engineer 1 through Engineer 5)

Add your OFDMA channel to interface 13/1.0. Type, **interface ofdma 13/1.0** to enter OFDMA configuration context. Establish the width of your channel by typing, **lower-freq 35000000 upper-freq 85000000**. Specify the IUC profile by typing, **iuc-profile 1** and turn on the channel with the **no shutdown** command. Return to config mode by typing **end**.

7.8.4 C40G Instructions (Engineer 6)

Add your OFDMA channel to interface 5/1.0 Type, **interface ofdma 5/1.0** to enter OFDMA configuration context. Establish the width of your channel by typing, **lower-**

freq 35000000 upper-freq 85000000. Specify the IUC profile by typing, **iuc-profile 1** and turn on the channel with the **no shutdown** command. Return to config mode by typing **end**.

7.9 Configuring DOCSIS MAC Interfaces

In this section we will add the downstream and upstream channels into two DOCSIS MAC interfaces.

7.9.1 Create a DOCSIS MAC Interface for your Annex B Modems (All Engineers)

In config mode, create a DOCSIS MAC interface with the **interface docsis-mac 1** command. Note: the DOCSIS mac interface is enabled by default, so there is no need to use the **no shut** command.

Configure the first downstream into the mac domain. Type, **downstream 1 interface qam 0/0/0** where the first 0 is the slot, the second 0 is the port and the third 0 is the actual qam channel number.

Configure the second downstream channel in the DOCSIS MAC 1 domain. Type, **downstream 2 interface qam 0/0/1**. **Repeat** these steps for all remaining downstreams (6) configured earlier.

Check your work with the **show interface docsis-mac 1** command. Your output should be similar to that below:

```
trainlab-iccap1#show interface docsis-mac 1

Output Cut......


downstream 1 interface qam 0/0/0

downstream 2 interface qam 0/0/1

downstream 3 interface qam 0/0/2

downstream 4 interface qam 0/0/3

downstream 5 interface qam 0/0/4

downstream 6 interface qam 0/0/5

downstream 7 interface qam 0/0/6

downstream 8 interface qam 0/0/7
```

Add your OFDM interfaces to the domain by typing, **downstream 33 interface ofdm 0/0/0** and **downstream 34 interface ofdm 0/0/1**. Type **show this** to check your work.

7.9.2 C100G Instructions (Engineer 1 through Engineer 5)

Now add the first upstream receiver on module 13 to the DOCSIS MAC domain. Type **upstream 1 interface upstream 13/0.0/0** where 13 is the slot, the first 0 is the port, the second 0 is the physical upstream channel and the last 0 is the logical channel.

Add all of the remaining up streams configured earlier(3) into the DOCSIS MAC. Check your work with the **show interface docsis-mac 1** command. Your output should show similar results to that below:

```
trainlab-iccap1#show interface docsis-mac 1

Output Cut.....

upstream 1 interface upstream 13/0.0/0

upstream 2 interface upstream 13/0.1/0

upstream 3 interface upstream 13/0.2/0

upstream 4 interface upstream 13/0.3/0
```

Add your upstream OFDMA interface by typing, **upstream 5 interface ofdma 13/0.0**. Type **show this** to check your work.

Apply the IP bundle you created earlier to DOCSIS MAC 1. Type**, ip bundle 1.**

Confirm your DOCSIS MAC configuration. Type, **show interface docsis-mac 1 topology**.

7.9.3 C40G Instructions (Engineer 6)

Now add the first upstream receiver on module 5 to the DOCSIS MAC domain. Type **upstream 1 interface upstream 5/0.0/0** where 5 is the slot, the first 0 is the port, the second 0 is the physical upstream channel and the last 0 is the logical channel.

Add all of the remaining up streams configured earlier(3) into the DOCSIS MAC. Check your work with the **show interface docsis-mac 1** command. Your output should show similar results to that below:

```
trainlab-iccap6#show interface docsis-mac 1

Output Cut.....

upstream 1 interface upstream 5/0.0/0

upstream 2 interface upstream 5/0.1/0

upstream 3 interface upstream 5/0.2/0

upstream 4 interface upstream 5/0.3/0
```

Add your upstream OFDMA interface by typing, **upstream 5 interface ofdma 5/0.0**. Type **show this** to check your work.

Apply the IP bundle you created earlier to DOCSIS MAC 1. Type**, ip bundle 1.**

Confirm your DOCSIS MAC configuration. Type, **show interface docsis-mac 1 topology.**

7.9.4 Create a DOCSIS MAC Interface for your Annex A Modems (All Engineers)

Create a second DOCSIS MAC interface with the **interface docsis-mac 2** command.

Configure the first downstream into the mac domain. Type, **downstream 1 interface qam 0/1/0** where the first 0 is the slot, the second 1 is the port and the third 0 is the actual qam channel number.

Configure the second downstream channel in the DOCSIS MAC 1 domain. Type **downstream 2 interface qam 0/1/1**. **Repeat** these steps for all remaining down streams (6) configured earlier.

Add your OFDM interface to the domain by typing, **downstream 33 interface shared-ofdm 0/0 secondary**. Type **show this** to check your work. Your output should be similar to that below:

```
trainlab-iccap1#show interface docsis-mac 2
Output Cut......
downstream 1 interface qam 0/1/0
downstream 2 interface qam 0/1/1
downstream 3 interface qam 0/1/2
downstream 4 interface qam 0/1/3
downstream 5 interface qam 0/1/4
downstream 6 interface qam 0/1/5
```

```
downstream 7 interface qam 0/1/6
downstream 8 interface qam 0/1/7
downstream 33 interface shared-ofdm 0/0 secondary
```

Apply the IP bundle you created earlier to DOCSIS MAC 2. Type**, ip bundle 1.**

View the details of your interface with the **show interface docsis-mac 2** command. Note the information the output provides you.

7.9.5 C100G Instructions (Engineer 1 through Engineer 5)

Now add the first upstream receiver on module 13 to the DOCSIS MAC domain. Type **upstream 1 interface upstream 13/1.0/0** where 13 is the slot, the first 1 is the port, the second 0 is the physical upstream channel and the last 0 is the logical channel.

Add all of the remaining up streams configured earlier(3) into the DOCSIS MAC.

Add your upstream OFDMA interface by typing, **upstream 5 interface ofdma 13/1.0**.

Check your work with the **show interface docsis-mac 2** command. Your output should show similar results to that below:

```
trainlab-iccap1#show interface docsis-mac 2
Output Cut.....
upstream 1 interface upstream 13/1.0/0
upstream 2 interface upstream 13/1.1/0
upstream 3 interface upstream 13/1.2/0
upstream 4 interface upstream 13/1.3/0
upstream 5 interface ofdma 13/1.0
```

7.9.6 C40G Instructions (Engineer 6)

Now add the first upstream receiver on module 5 to the DOCSIS MAC domain. Type **upstream 1 interface upstream 5/1.0/0** where 5 is the slot, the first 1 is the port, the second 0 is the physical upstream channel and the last 0 is the logical channel.

Add all of the remaining up streams configured earlier(3) into the DOCSIS MAC.

Add your upstream OFDMA interface by typing, **upstream 5 interface ofdma 5/1.0**.

Check your work with the **show interface docsis-mac 2** command. Your output should show similar results to that below:

```
trainlab-iccap6#show interface docsis-mac 2
Output Cut.....
upstream 1 interface upstream 5/1.0/0
upstream 2 interface upstream 5/1.1/0
upstream 3 interface upstream 5/1.2/0
upstream 4 interface upstream 5/1.3/0
upstream 5 interface ofdma 13/1.0
```

7.10 DOCSIS Security Configurations

In this section we will explore your DOCSIS security options.

7.10.1 Early Authentication and Encryption

To prevent unauthorized access to the provisioning messages in the CM/ICCAP initialization process, DOCSIS 3.0 introduced a new encryption technique that leverages BPI+ key management early in the initialization process to strongly encrypt the DHCP and TFTP exchanges directly after initial ranging.

Enable Early Authentication and Encryption on both of your DOCSIS MAC interfaces with the command, **early-authentication-encryption ranging.**

7.10.2 TFTP Proxy/TFTP Enforce

Another new feature in DOCSIS 3.0 Security specification is the tftp proxy. The tftp-enforce command enables the ICCAP to reject registration requests from cable modems on the specific MAC domain. If set, cable modems must download their DOCSIS configuration files from a TFTP server located on the NSI before the modems are allowed to register with the ICCAP. The default setting is disabled. If disabled, the CMs are allowed to register with the ICCAP and come online without first downloading their DOCSIS configuration file.

Configure the ICCAP for TFTP proxy for DOCSIS MAC Interface 1. Type, **tftp-enforce. Exit** out of interface configuration mode.

7.10.3 BPI Enforce

A new security mechanism in DOCSIS 3.0 Security specification is BPI enforce. This requires that only CMs with BPI+ should go online. The command “cable privacy bpi-enforce mandatory” will prevent all non-BPI modems from registering with the ICCAP. If the mandatory option is not specified, then non-BPI modems will register and come online with ICCAP. It is recommended that both commands below are used and configured. Note: BPI enforce is only required if legacy 1.0 modems are included in the Service Group.

Configure BPI enforce and BPI plus enforce on the ICCAP globally. From configuration mode type,

cable privacy bpi-enforce mandatory
cable privacy bpi-plus-enforce mandatory

Our cable modems do not have certificates configured, so turn off certificate checking. Type:

no cable sec modem-cert check

Note that if you neglect this command, your modems will get stuck in BPI+(init) when they reboot.

Reset your cable modems by typing **clear cable modem reset**. Type **yes**.

At this point all of your cable modems connected to your lab station should be initializing and coming on line with IPV4 and IPV6 addresses.

Confirm your modems are up and in an online state. Type **show cable modem.** Repeat the command until all your cable modems are online. If your cable modems do not come online, review your configuration for completeness.

We will explore detailed cable modem show commands later in this lab.

7.11 PHY and DOCSIS MAC Best Practices

In this section we will configure miscellaneous RFI and DOCSIS MAC Configurations.

7.11.1 Static MAP Advance

By default dynamic Map advance is enabled on the Casa ICCAP. In a case where you may have legacy CMs or misbehaving CMs with regard to badly reporting their timing offset, this can lead to increased latency for the whole MAC Domain. To help this situation you may configure MAP advance as static until the CMs are removed.

Configure Map Advance to static + 200 ms on your active upstream interfaces. From each upstream interface config mode, type **map-advance static 200**. Confirm your configuration with the **show run | inc map** command.

7.11.2 Interleave Level

Interleaving can help mitigate errors in the downstream data transmissions caused by electrical burst noise from amplifier power supplies and utility powering. The trade off however is latency; the higher the interleaving the more latency is introduced into

the transmission of data. Interleaving doesn't add overhead bits like FEC, but it does add latency, which could affect voice, gaming, and real-time video. It also increases the Request/Grant round trip time (RTT).Configure the interleave level to 16 for your Downstream(s). From interface mode for the active downstream interface type, **interleave 16**.

7.11.3 Pre-equalization

The upstream path can be susceptible to more noise & burst noise within the cable plant, so Casa recommends turning on the pre-equalization on all upstream channels to compensate for micro-reflections in the network.

A traditional problem with pre-equalization is a corruption of the coefficients sent in the downstream direction to the modem. For D2.0 and D3.0 modems, SNR is monitored in ranging packets. If the SNR is lower than the correctable FEC error threshold (25dB for 64QAM for example) for multiple RNG-REQ's, the pre-equalization coefficient is reset to the unit response in the RNG-RSP.

Casa recommends this configuration. To enable pre-equalization auto-reset use the command under each upstream interface configuration: **logical-channel 0 pre-equalization auto-reset**.

Confirm your configuration and save it.

7.11.4 Modulation Profiles

Modulation Profiles define the upstream phy layer attributes of the CM transmissions. There are several template configurations for you to use "out of the box", however some operators may want to create their own. Careful consideration and testing is recommended before applying custom modulation profiles in a production network.

Display the template modulation profiles from global configuration mode with the **show modulation-profile** command. The Casa ICCAP platform has 5 predefined modulation profiles (1 - 5). You can configure an additional 59 modulation profiles (6 – 64) based on requirements.

Scroll down to view modulation profile two. This is the default modulation profile and will be applied to all upstream traffic unless you edit the current profiles or create your own.

Display the configured modulation profile with the **show interface upstream 13/0.0 | inc profile** command. (C40G command: **show interface upstream 5/0.0 | inc profile**). Notice both logical profiles are associated with profile 2.

While pre-equalization can address group delay introduced by the amplifiers, it will not fix the non-linear distortions such as laser clipping. The only way of addressing

this in the ICCAP is to use a stronger FEC and enable interleaving. Casa recommends both. Modulation profiles is where you can add more FEC.

7.11.5 Dynamic interleaving

CASA recommends turning on the dynamic inter-leaver for data burst types “a-short, a-long and a-ugs” IUC’s only for a robust burst noise immunity and where burst noise could be greater than 10 microseconds. To reach the maximum burst noise immunity, we recommend changing the inter-leaver settings for these IUCs. The “0” enables the inter-leaver in dynamic mode, which means it dynamically adjusts to the burst length. The “2048” ensures maximum burst-duration immunity; in the case there is no burst noise to contend with, then the inter-leaver has no benefit, however it is harmless if configured this way.

Let’s configure a modulation profile 6 with the recommended values and apply them to your modems.

From configuration mode type,

modulation-profile 6
request atdma qpsk off 64 0 16 338 0 16 fixed on 1 1536 qpsk0
initial atdma qpsk off 640 5 34 338 0 48 fixed on 1 1536 qpsk0
station atdma qpsk off 384 5 34 338 0 48 fixed on 1 1536 qpsk0
a-short atdma qpsk off 104 12 75 338 13 8 shortened on 0 2048 qpsk1
a-long atdma qpsk off 104 16 223 338 0 8 shortened on 0 2048 qpsk1
ugs atdma qpsk off 104 16 223 338 0 8 shortened on 0 2048 qpsk1

View the newly created profile type,

exit
show modulation-profile 6

7.11.6 Small Signal Compensation

The small-signal-compensation command has been introduced on the interface upstream configuration to handle sudden power swings (up to 12 dB) over upstream channels that could result in modem de-registration. The default setting is OFF. Note that enabling this feature will result in a slight decrease in SNR, so it is recommended to only enable this feature in conditions where known power swings occur. The most common cause of sudden power swings is loose connections. To enable small signal compensation on the upstream interface from config mode move to your upstream interface and type,

small-signal-compensation

To check the current modulation profile on upstream channel type

show interface upstream 13/0.0 current

(C40G command: **show interface upstream 5/0.0 current).**

7.12 Load Balancing and Channel Bonding Configurations

In this section of the lab we configure DOCSIS 3.0 features on the DOCSIS Mac to include:

- Service groups
- Load Balancing
- Channel Bonding

7.12.1 Configuring Service Groups

Service groups are required to implement certain DOCSIS features, namely Load Balancing and Channel Bonding. In this configuration we will create a single service group with 8 downstream channels and 4 upstream channels.

From configuration mode, create your service group with the **service group FNB** command.

Add the first active upstream with the **upstream 13/0.0** command. (C40G command: **upstream 5/0.0**). **Add the remaining active upstreams.**

Add your ofdma upstream with the **ofdma 13/0.0** command. (C40G: **ofdma 5/0.0**).

Add your first active downstream channel with the **qam 0/0/0** command. **Add the remaining active downstreams**.

Add your first OFDM channel with the command **ofdm 0/0/0**. Add your second OFDM channel by typing, **ofdm 0/0/1**.

Confirm your configuration with the **show this** command. Compare your output to the output below. If it matches, save your configuration.

```
trainlab-iccap1(conf-svc-grp FNB)#show this
service group  FNB
  qam 0/0/0
  qam 0/0/1
  qam 0/0/2
  qam 0/0/3
  qam 0/0/4
  qam 0/0/5
  qam 0/0/6
  qam 0/0/7
  upstream 13/0.0
  upstream 13/0.1
  upstream 13/0.2
  upstream 13/0.3
  ofdm 0/0/0
  ofdm 0/0/1
  ofdma 13/0.0
```

7.12.2 Create a Second Service group for your Annex A modems

From configuration mode, create your service group with the **service group FNA** command.

From what you learned in the previous section, add all the Annex A upstreams you enabled on port 13/1. (C40G: 5/1). Add your Annex A downstreams on port 0/1.

Confirm your configuration with the **show this** or **show service group** command.

7.12.3 Load Balancing

Move to configuration mode and enable global load balancing with the **load-balance enable** command.

Create an execution rule with the **load-balance execution-rule 1** command.

Define your load balancing method with the **method modem** command, and specify the dynamic method based on utilization with the **method utilization dynamic** command.

Set a threshold to load balance. Type, **threshold load 10 enforce 20 minimum 20 dynamic minimum 60**.

Return to config mode.

Create a load-balance policy with the **load-balance policy 1** command, and assign an execution rule to the policy with the **rule execution 1** command.

Return to config mode.

Enter the general load balance group default settings. Type, **load-balance general-group default-settings**

Enable the default settings. Type, **enable**

Configure the load balance as static. Type, **initial-tech broadcast-ranging**

Associate the default settings with policy 1. Type, **policy-id 1**

Return to configuration mode and reboot your cable modems. Type **clear cable modem reset** and type **YES** when prompted. Wait for them to register.

View the load-balance static log. Type **show load-balance static.**

Because of the small number of 2.0 modems in each lab station you may only see 1 modem move or none at all because they may have balanced within the thresholds on registration and there is no need to move them. The 3.0 cable modems will not move because they you have created a service group and by default the modems will bond to 8 downstream channels and 4 upstream channels, therefore they have nowhere to move.

7.12.4 Channel Bonding

Remember that Channel Bonding is enabled by default as long as you create an intersection of the DOCSIS mac domain and a service group. All of your 3.0 modems should be bonded across the downstream frequencies and upstream frequencies available to them.

7.12.4.1 **Confirm bonding**

There are several ways to view cable modem bonding. First, use the **show cable modem** command. Any modem with an asterisk next to the DS and US Intf column indicates a bonding modem. Anything with a pound sign will indicate partial service bonding.

Type **show cable modem bonding.** This will display the upstream and downstream channel sets configured at registration time.

Type **show downstream channel set.** The individual DSIDs will listed for each channel and the bonding channel set will list, showing each downstream channel that is bonding within the set. The same is true for **show upstream channel set**.

7.12.4.2 Partial Service

Partial Service occurs in channel bonding when the CM detects that one or more channels in the Transmit Channel Set (TCS) and/or the Receive Channel Set (RCS) are unusable due to low SNR. This detection can happen during registration or after registration. The CM will signal this partial service to the ICCAP with CM status messages if the partial service is detected after registration or in the registration ACK if at the time of registration. Once the ICCAP is alerted to the partial service the modem will no longer receive data transmission grants on that channel but will continue to receive unicast station maintenance grants on the channel(s). This way the CM can recover the channel if it becomes usable once again.

7.12.4.3 Partial Service Best practices

To cover all CM-STATUS messages regarding partial service, Casa recommends enabling the following messages:

- 1: Secondary Channel MDD timeout - The MDD (Mac Domain Descriptor) is transmitted every two seconds on the downstream channels and part of the process involves fragmenting the MDD if it's large. The MDDs often get dropped, and if too many of them are dropped, the modem's MDD timer expires and it begins looking for them again.
- 4: Secondary Channel MDD Recovery
- 7: T3 re-tries exceeded
- 8: Successful ranging after T3 retries exceeded

Enable these messages. From config mode type:

int docsis-mac 1
cable cm-status report event-list 1,4,7,8

Repeat for DOCIS MAC 2

You can check this log with the command:

show cable modem cm-status log

Also you should enable "**cable partial-service continue-ranging**." With this enabled the ICCAP will never expire sending the unicast ranging opportunities for a Cable Modem that is in partial service mode, unless it's completely offline.

cable partial-service continue-ranging

7.13 Casa Systems RFI Features

In this section we configure RFI features exclusive to Casa software to include:

- Ingress Cancellation
- Casa Spectrum Management

7.13.1 Ingress noise cancellation

Casa's ingress cancelation is a proprietary feature and has documented positive results for many customers. By default the Ingress Noise Cancellation is not turned on, the ingress cancellation feature can be very beneficial in canceling narrow band ingress noise in the upstream. Casa recommends a sampling interval in milliseconds for "ingress noise cancellation" the reason for this is that the ingress noise won't change much in this interval, thus giving the best results.

Move to configuration mode. To enable ingress cancellation on your upstream interfaces, move to the configure interface upstream 13/0.0 interface context. Enable ingress cancellation with the default sampling interval time of 200 milliseconds by typing, **ingress-cancellation. Repeat** for all your upstream interfaces.

7.13.2 Spectrum Management

Spectrum Management allows an operator to configure rules such as minimum SNR and FEC errors and, based on the thresholds set within these rules, take certain actions to maintain the channel(s). Casa Spectrum Management monitors the quality of all upstream channels by periodically polling measured parameters of SNR, correctable and uncorrectable FECs. This polling interval is configurable, the default is 30 seconds but the range is 5 to 3600 seconds. Use the cable spectrum monitor-period <5 3600> command to change the default value.

The first step in configuration is to create rules which will be responsible for defining the action taken when SNR and uncorrectable FEC reach configured thresholds. In the rules we create we will:

- Configure a change in modulation as the primary action
- Configure the correctable-fec threshold to 100 which essentially ignores correctable-fec.
- set 1% as threshold for UNCOR-FEC
- set 22db – 2db hysteresis as a threshold for
- Configure SNR with a hysteresis of 2db from the default SNR threshold.

First display the default SNR thresholds. From root privileged mode type, **show spectrum snr-threshold-default.**

Now create spectrum rule 1. Move to config mode and type, **spectrum rule 1**

From spectrum rule 1 mode, create the actions and thresholds as described earlier.

action modulation
correctable-fec threshold 100
uncorrectable-fec threshold 1
profile 10 snr-threshold 200 220
exit

The next step is to bind the created spectrum rules to particular upstream channel. Move to your 13/0.0 upstream interface and type,

spectrum-rule 1

Repeat for each of your upstream interfaces.

The last step is to bind secondary modulation profiles for every upstream channel in specific order, changing from the highest modulation to the lowest. In our case we will move from modulation profile 6 (we created earlier) to default modulation profile 1. Move to each of your upstream channels in sequence, and in each case type,

logical-channel 0 profile 1

8 RFI Diagnostics

In this section we will use CLI and SNMP diagnostic commands to gather information as it relates to the cable plant, cable modems and and the RF interfaces.

8.1 DOCSIS Modules

Display packet statistics for the RFI interfaces. From root privileged mode use the following commands to view status, errors, and statistics on the upstream and downstream interfaces:

show interface qam brief
show interface qam stat
show interface upstream brief
show interface upstream stat

8.2 Diagnostic Mode Interface Commands

Enter diagnostic mode by typing, **diag**. Enter the password, **casadiag**.

Check your gige interfaces for errors with the **show module 0 stat gige** command. If the errors on the interface exceed 0.1% (divide the number of errors by total rx packets), the SMM is likely the cause of the errors.

Show the memory on the downstream module. Where X is a downstream module number, type, **show module X stat himem**. View the output and do a little math in your head to estimate your current percentage of free buffers. Then, subtract the low water mark value from the total_buf_cnt value to determine the maximum number of buffers used since the last reboot.

Show your downstream card statistics by typing, **show module X stat qam**. Scroll down until you get the line pkt drop due to ENQ limit. This is important to diagnose whether packet drops on the downstream module are due to overload.

View your upstream card statistics with the **show interface upstream 13/0.0 stat** command. Examine the output, and determine the proportion of errored frames to unerrored frames.

8.3 Cable Modem Debug

There are CLI show commands, traffic capture tools and debugging available for cable modem diagnostics. The most commonly used will be cable debug. For this section ensure you are connected to the vty interface not the console interface.

Move to root privileged mode and display the boot up process for one of your cable

modems with the debug trace process. Start by choosing a cable modem mac address of one of your registered modems. Type **show cable modem** to see your mac addresses.

Type **logging debugging**.

Type **debug cable mac-address <mac address>**.

Reset your cable modem. Type clear cable modem <mac address> reset.

Type **debug cable**. Observe the messages; you should see the entire registration process for this cable modem.

Once registration completes, turn off logging to standard output. Type **no logging**.

Turn off debugging. Type **no debug cable**

8.4 Cable Modem Show Commands

By default, the show cable modem commands are accessible at all user levels. This means that CLI users, including users at the most restricted administrative access, can display cable modem information. Using the show cable modem commands has no effect on the system configuration and will not impact system performance.

The most commonly used command will be the show cable modem command. This command has several arguments.

Type **show cable modem ?** to display a list of the commands specific to cable modems. Take a few moments to review the list.

Type **show cable modem verbose** to display a detailed output about each cable modem. Take a few moments to review the output.

Type **show cable modem mac** to display the version and MAC layer capabilities for each modem.

Type **show cable modem verbose | inc Stn** to display a list of T3 timeouts for all modems. This could help determine the health of the cable plant.

Type **show cable modem verbose | inc US** to display a list of Upstream service flows and throughput.

Type **show cable modem verbose | inc DS** to display a list of Downstream service flows, throughput, and data.

Type **show cable modem verbose | inc Online** to display the total time online for each cable modem.

Type s**how cable modem counters** to display upstream and downstream packet counts and bytes for each modem

Type **show cable modem errors** to display the errors on DOCSIS frames' HCS (Header Check Sequence) and CRC (Cyclical Redundancy Check) for each modem.

Type **show cable modem dropped-packets** to display dropped packets for all modems.

8.5 Diagnosing RF-Related Problems

In this section of the lab we will explore some CLI diagnostics tools to help you gather information to assist in the diagnosing RF related problems.

Show your downstream channel utilization. Type, **show docsis downstream channel utilization.** Which channel is supporting the largest number of online modems?

Substitute upstream for downstream in the above command to display the upstream utilization. Which channel is supporting the largest number of online modems?

To show cable modem throughput per DOCSIS mac and service group, type:

show cable modem docsis-mac 1 service-group FNA downstream throughput

Display the upstream signal quality. Type, **show upstream signal-quality**. What is the SNR on your active channels?

Display the signal quality for each frequency. Type, **show spectrum upstream 13/0.0**. What are the noise levels?

Display the upstream burst noise for each channel. Type, **show upstream burst-noise**.

Display modems that are in partial service, type **show cable modem partial service.**

8.6 Remote Query

The remote query command can be useful for obtaining real time information from an individual cable modem. First it must be enabled to so from config mode type,

cable modem remote-query 30

Now, query your modems. Type,

show cable modem remote-query immediate

To get verbose information from a single cable modem combine this command with a mac address or ip address.

show cable modem <mac address| ip address> remote-query verbose immediate

8.7 DOCSIS ping Command

To determine whether a specific cable modem (CM) is reachable from the CCAP: at the DOCSIS MAC layer, use the docsis ping command. Type **ping docsis <mac address>** This can be useful to verify the modem is responding a layer 2 but IP connectivity to the modem is lost.

8.8 CM Status messages

As mentioned in the partial service lab there are CM status messages that can be enabled to help diagnose cable modem problems. Additional CM status messages that should be enabled are:

- 2:QAM/FEC lock failure
- 5:QAM/FEC Lock Recovery
- 6:T4 timeout – Downstream MAP is not available.

8.9 Cable Flap List

The flap list can be helpful when troubleshooting cable modems. You can configure the flap list to include or exclude certain modem scenarios.

Move to configuration mode and type **show cable flap-list config** to view your current configuration.

Use the **cable flap-list ?** command to help you configure the flap list according to the following parameters.

power-adjust threshold 1
miss threshold 7 90
insertion-time 90

Check your work with the **show cable flap-list config** command.

8.10 Observing the Cable Modem Boot Process

In this section you will view a TFTP request from the ICCAP IP bundle interface. Note: you will not see the read request at the ICCAP unless TFTP proxy is enabled.

Move to interface configuration mode on your docsis-mac 1 interface, and type **tftp-proxy.**

Enter diag mode.

Set tcpdump on the VLAN interface to listen for tftp messages. Where "X" is your engineer number, type, **tcpdump "-i vlanX00 -vvv udp port 69 or udp port 69"**.

Open another connection to your ICCAP with SSH. Reset a cable modem with the **clear cable modem <mac address> reset** command. Observe your tcpdump. You should see something like the following:

```
tcpdump: listening on vlan100, link-type EN10MB (Ethernet), capture size 96 bytes

14:15:38.001871 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17),
length 86) 192.168.6.1.41636 > class-

srv1.sdclasslab.local.tftp: 58 RRQ "classgateways.bin" octetnetaddr 1,192.168.6
```

Type **<CTRL C>** to escape from your capture.

Start another capture except this time use port 67 and 68. Type **tcpdump "-i vlanX00 -vvv udp port 67 or udp port 68"**. Reset your cable modem and observe your capture output. Note that, because the ICCAP is always a DHCP proxy/relay agent you can observe bootp messages with TCP dump from the NSI side.

Another command that can be used for gleaning DHCP messages is the dhcp trace command. This command checks the last 128 DHCP transactions for all modems. From diag mode type **show dhcp-trace**.

8.11 Cable Mirroring

The cable mirror command allows you to capture the traffic to and from a cable modem on the SMM and lets you read the file with a packet capture program such as Wireshark. ***Note that you must have Wireshark installed on your computer to complete this lab.***

You will need to have two connections to the ICCAP for this lab: one SSH and one console. Open them now if you do not have them open from the previous section.

From diag mode on one connection, pick an online modem and copy its MAC.

Begin a mirror. Type, **mirror cm traffic 127.1.1.7 <macaddress>**. You should receive the message, " Mirroring traffic for MAC <macaddress> ff.ff.ff.ff.ff.ff to 7f010107 fr idx=-1 00000000 f=3 us_id=0 ds_id=0".

From your other connection start a tcpdump capture. Where "X" is your engineer number, type, ICCAP(diag)# **tcpdump "-i any -n host 10.4.1.254 -xx -s 0 -w /fdsk/MirrorCM_X.pcap"** You should receive this message:

```
*****   Type Ctrl-C to exit   *****
tcpdump: listening on any, link-type LINUX_SLL (Linux cooked), capture size
262144 bytes
```

Return to the other connection and reset the cable modem you are mirroring.

Using **show cable modem**, make sure the modem registers.

Once the modem is registered exit from the tcpdump. Type,**<CTRL C>.** You should receive something similar to the message below:

```
220 packets captured

222 packets received by filter

0 packets dropped by kernel

ICCAP2(diag)#
```

Turn off cable mirroring. Type **mirror cm traffic 0.**

From one of the connections in config mode type **ls**. You should see your capture file in nvram.

FTP the file to lab-jump-srv. Where "X" is your engineer number, type **copy nvram MirrorCM_X.pcap ftp engineerX 10.4.1.253 /home/engineerX**. Enter your assigned password.

Open an SCP session from your computer to casalabs.training. Log in with your assigned engineer account and password. Copy your .pcap file to your computer and open it with Wireshark.

8.12 Cable Modem debug with SNMP

SNMP can be helpful in troubleshooting individual cable modems. The following section walks the MIB that holds the cable modem initialization log. This log will hold the same messages you get in debug but from the modem's perspective.

Open another connection to lab-jump-srv.

On your ICCAP, from a cli session in root privileged mode, type **show cable modem remote-query immediate community string public**. Select a modem that responded with power levels and note its IP address.

Return to lab-jump-srv and issue the command **snmpwalk -c public -v2c <ip address of cable modem> SNMPv2-SMI::mib-2.69.1.5.8.1.7.**

Take a few moments to review the information. A portion of this log should contain the complete initialization process from downstream lock to registration for that modem.

From your ICCAP run a continuous ping down to this CM with the **ping repeat 10000 <ip address>** command.

From lab-jump-srv execute the **snmpwalk -c public -v2c <ip address of cable modem> SNMPv2-SMI::transmission.127.1.1.4.1.4.3** command. Repeat the mibwalk numerous times to see if the counter 32 increments. In our labs it should not, but this is a way for support to see if there is some type of hardware issue with the QAM.

-End of Lab-

9 Appendix A

9.1 IBGP/LDP/MPLS Configurations

In this section of the lab we will configure a Layer 3 VPN on a new IP bundle interface to advertise a network prefix of the WLAN network in the class lab, over an interior BGP (iBGP) peering to R3 from your C100G .

ICCAP#	vrf name	ipbundle 1.1 address	ICCAP loopback
trainlab-iccap1	casalabs	192.168.10.1/24	10.254.1.1
trainlab-iccap2	casalabs	192.168.20.1/24	10.254.2.1
trainlab-iccap3	casalabs	192.168.30.1/24	10.254.3.1
trainlab-iccap4	casalabs	192.168.40.1/24	10.254.4.1
trainlab-iccap5	casalabs	192.168.50.1/24	10.254.5.1
trainlab-iccap6	casalabs	192.168.60.1/24	10.254.6.1

Create a Virtual routing and forwarding table definition. Move to config mode and type,

vrf definition casalabs
rd 1:1
address-family ipv4
route-target export 1:1
route-target import 1:1
exit

Create a new network prefix to advertise and associate that prefix with the casalabs VRF. Note the ip bundle address will be the same on all ICCAPs. This is because a different VRF will be created on each ICCAP and R3.

interface ip-bundle 1.1
vrf forwarding casalabs
ip address <your ip-bundle 1.1 address> 255.255.255.0
end

Enable MPLS and LDP on the VLAN interface. Type,

interface vlan <your vlan id>
mpls ip
enable-ldp ipv4
end

Create the BGP/LDP peering to R3. We will use the loopback 0 address of both devices as the endpoints for the BGP peering. Notice we are creating a BGP session to a router

not directly connected to your ICCAP and transiting R2. Use the information in the table below that matches your ICCAP.

ICCAP#	R3 loopback	ICCAP loopback
trainlab-iccap1	10.254.5.13	10.254.1.1
trainlab-iccap2	10.254.5.13	10.254.2.1
trainlab-iccap3	10.254.5.13	10.254.3.1
trainlab-iccap4	10.254.5.13	10.254.4.1
trainlab-iccap5	10.254.5.13	10.254.5.1
trainlab-iccap6	10.254.5.13	10.254.6.1

router bgp 64512
neighbor 10.254.5.13 remote-as 64512
neighbor 10.254.5.13 update-source loopback 0
address-family ipv4 unicast
neighbor 10.254.5.13 activate
exit-address-family
address-family vpnv4 unicast
neighbor 10.254.5.13 activate
neighbor 10.254.5.13 send-community extended
exit-address-family
address-family ipv4 vrf casalabs
redistribute connected
exit-address-family
exit
router ldp
router-id <your loopback address>
transport-address ipv4 <your loopback address>
exit

9.2 Verifying IBGP/LDP/MPLS

Here are a few commands to verify BGP/MPLS.

Verify BGP neighborship. Type **show ip bgp neighbor** and verify your BGP State is "Established".

You can verify this with the command **traceroute source loopback 0 10.254.5.13**. Notice R3 is one hop away!!!

Verify LDP neighbor-ship with the r2 subinterface for your ICCAP. Type **show mpls ldp neighbor.**

9.3 L2 VPN Configurations

In this section we will explore configuring both EoMPLS and VPLS.

9.3.1 Configuring EoMPLS

Check that you have enabled LDP and MPLS on your VLAN. From config mode, type **interface vlan <your vlan number>**. Type **show this**. Look for the mpls-ip and the enable-ldp ipv4 commands. If you do not see them, enter them now. Type **exit** to leave interface vlan mode.

Configure LDP so that all the ICCAPs have fully meshed targeted LDP sessions. Type **router ldp** to enter router ldp config mode.

Establish your LDP targeted peers. Type **targeted-peer ipv4 <peer device IP>**. Repeat the command for each of your peer devices.

Peer Device	IP Address
trainlab-iccap1	10.254.1.1
trainlab-iccap2	10.254.2.1
trainlab-iccap3	10.254.3.1
trainlab-iccap4	10.254.4.1
trainlab-iccap5	10.254.5.1
trainlab-iccap6	10.254.6.1

Test your work. Type **show ldp targeted-peers**. You need to see at least one targeted peer before you proceed with the lab. Type **exit** to return to config mode.

Create a separate your EoMPLS instance to connect to each of your active targeted peers. Refer to the table below that references your ICCAP.

Table for trainlab-iccap1:

Peer	Peer IP Address	VPWS Name	Virtual Circuit ID
trainlab-iccap2	10.254.2.1	toPeer2	12
trainlab-iccap3	10.254.3.1	toPeer3	13
trainlab-iccap4	10.254.4.1	toPeer4	14
trainlab-iccap5	10.254.5.1	toPeer5	15
trainlab-iccap6	10.254.6.1	toPeer6	16

Table for trainlab-iccap2

Peer	Peer IP Address	VPWS Name	Virtual Circuit ID
trainlab-iccap1	10.254.1.1	toPeer1	21
trainlab-iccap3	10.254.3.1	toPeer3	23
trainlab-iccap4	10.254.4.1	toPeer4	24
trainlab-iccap5	10.254.5.1	toPeer5	25
trainlab-iccap6	10.254.6.1	toPeer6	26

Table for trainlab-iccap3

Peer	Peer IP Address	VPWS Name	Virtual Circuit ID
trainlab-iccap1	10.254.1.1	toPeer1	31
trainlab-iccap2	10.254.2.1	toPeer2	32
trainlab-iccap4	10.254.4.1	toPeer4	34
trainlab-iccap5	10.254.5.1	toPeer5	35
trainlab-iccap6	10.254.6.1	toPeer6	36

Table for trainlab-iccap4

Peer	Peer IP Address	VPWS Name	Virtual Circuit ID
trainlab-iccap1	10.254.1.1	toPeer1	41
trainlab-iccap2	10.254.2.1	toPeer2	42
trainlab-iccap3	10.254.3.1	toPeer3	43
trainlab-iccap5	10.254.5.1	toPeer5	45
trainlab-iccap6	10.254.6.1	toPeer6	46

Table for trainlab-iccap5

Peer	Peer IP Address	VPWS Name	Virtual Circuit ID
trainlab-iccap1	10.254.1.1	toPeer1	51
trainlab-iccap2	10.254.2.1	toPeer2	52
trainlab-iccap3	10.254.3.1	toPeer3	53
trainlab-iccap4	10.254.4.1	toPeer4	54
trainlab-iccap6	10.254.6.1	toPeer6	56

Table for trainlab-iccap6

Peer	Peer IP Address	VPWS Name	Virtual Circuit ID
trainlab-iccap1	10.254.1.1	toPeer1	61
trainlab-iccap2	10.254.2.1	toPeer2	62
trainlab-iccap3	10.254.3.1	toPeer3	63
trainlab-iccap4	10.254.4.1	toPeer4	64
trainlab-iccap5	10.254.5.1	toPeer5	65

From config mode, type **mpls vpws <VPWS Name>**. The ICCAP will assign a unique instance ID and VLAN tag automatically. Identify your peer by typing **peer <peer IP Address> <Virtual Circuit ID>**. If you receive an error message, check that the other ICCAP has been configured.

Type **exit**.

Repeat these commands for each of your active targeted peers.

Check your work. From config mode, type **show mpls vpws xconnect**. Note that you do not have any attached upstream or downstream interfaces, and you have no MAC addresses or PSIDs.

You must assign a cable modem to your VPWS in order to activate your pseudowires. However, at this point, you have not yet configured your DOCSIS parameters, so you have no cable modems active.

Assign one cable modem to each of your VPWS instances to activate your pseudowires. To view the MAC addresses of your CMs, type **show cable modem**. The CM must be using BPI before you can configure it into an L2VPN, so look for cable modems that have BPI enabled. (The Status line will say the modem is "online(pt)".) Use the **cable modem <CM MAC address> mpls vpnid <VPWS Name>** command to assign a CM to your first peer. (An example would be: cable modem 2476.7d98.b798 mpls vpnid toPeer1.) Repeat this command to assign one cable modem to each instance.

Reset your cable modems with the **clear cable modem reset** command. Use the **show cable modem** command to track when your CMs come back on line.

Check your work. From config mode, type **show mpls vpws xconnect**. Note that you now have upstream and downstream interfaces in your VPWS, and you see both MAC addresses and PSIDs.

9.3.1 Configuring VPLS

If you did NOT **do the VPWS portion of this lab, follow the instructions in this section. If you** DID **do the VPWS portion of this lab, continue on to RFI Diagnostics.**

Check that you have enabled LDP and MPLS on your VLAN. From config mode, type **interface vlan <your vlan number>**. Type show this. Look for the mpls-ip and the enable-ldp ipv4 commands. If you do not see them, enter them now. Type **exit** to leave interface vlan mode.

Configure LDP so that all the ICCAPs have fully meshed targeted LDP sessions. Type **router ldp** to enter router ldp config mode.

Establish your LDP targeted peers. Type **targeted-peer ipv4 <peer device IP>**. Repeat the command for each of your peer devices.

Peer Device	IP Address
trainlab-iccap1	10.254.1.1
trainlab-iccap2	10.254.2.1
trainlab-iccap3	10.254.3.1
trainlab-iccap4	10.254.4.1
trainlab-iccap5	10.254.5.1
trainlab-iccap6	10.254.6.1
Router 3	10.254.5.13

Test your work. Type show ldp targeted-peers. You need to see at least one targeted peer before you proceed with the lab. Type exit to return to config mode.

Add the other ICCAPs and Router 3 to your BGP instance as neighbors. From config mode, move to **router bgp 64512**. Refer to the table below for the IP addresses of your neighbors, and issue the commands:

neighbor <neighbor IP Address> remote-as 64512

neighbor <neighbor IP Address> update-source loopback 0

Next, add the other ICCAPs and Router 3 to your l2vpn address family using the commands below.

address-family l2vpn vpls
neighbor <ip address> activate
neighbor <ip address> send-community extended

Refer to the table below for your IP addresses. Repeat the neighbor commands until you have added all of your neighbors.

Neighbor Device	IP Address
trainlab-iccap1	10.254.1.1
trainlab-iccap2	10.254.2.1
trainlab-iccap3	10.254.3.1
trainlab-iccap4	10.254.4.1
trainlab-iccap5	10.254.5.1
trainlab-iccap6	10.254.6.1
Router 3	10.254.5.13

Exit out of the address family with the **exit-address-family** command.

Next, establish your VPLS name and instance identifier. Note that if you have more than one VPLS on a ICCAP, each VPLS must have a unique name and instance identifier. However, it makes life easier if, for a given VPLS, you use the same name and instance identifier for each ICCAP participating in that VPLS. That is what we will do in this lab. To establish your VPLS name and instance identifier, in config mode type, **mpls vpls casalabs_vpls 1000.**

Configure BGP as your signaling protocol. To do so, you must establish a VPLS Edge ID (ve-id), route target, and route distinguisher for each PE router. The Route Distinguishers and Route Targets must be identical for each VPLS. However, each ICCAP must have a unique ve-id in a given VPLS. Refer to the table below for the values to use in your commands.

ICCAP	ve-id	Route Distinguisher	Route Target
1	1	64512:1	64512:1
2	2	64512:1	64512:1
3	3	64512:1	64512:1
4	4	64512:1	64512:1
5	5	64512:1	64512:1
6	6	64512:1	64512:1

The previous command (mpls vpls casalabs_vpls 1000) leaves you in config-vpls mode. From config-vpls mode, type the commands below.

signaling bgp ve-id <your ve-id>
signaling bgp route-distinguisher <your Route Distinguisher>
signaling bgp route-target <your Route Target>

Type **show this** to check your configuration. Type **exit**.

Add a cable modem that is doing BPI (is in online(pt) state) to your VPLS. (Note: if you have no additional BPI enabled modems after the VPWS lab, remove one of those modems from your VPWS configuration with the no cable modem <CM MAC address> mpls command.) From config mode, type **cable modem <CM MAC address> mpls vpls casalabs_vpls**. **Reboot** the CM.

Once the CM comes back online, check your work. Type **show mpls vpls casalabs_vpls detail**. You will see your local CMs, and you should see your neighbors connected via pseudowires.