Oracle® Communications Performance Intelligence Center

Customer Integration

Release 9.0

909-2241-01, Revision E

February 2014

ORACLE®

Oracle Communications Performance Intelligence Center Customer Integration, Release 9.0

CHANGE HISTORY

Date	Version	Author	Comments	Approved (Yes/No)
17/09/2012	0.1	F. Cêtre	New Document	No
03/10/2012	0.2	J. Grimont	Insert DataBroker configuration	No
08/11/2012	0.3	JF Muller	Update charts Add DWS customer integration steps	No
29/11/2012	0.4	JF Muller	Update DWS section	No
30/11/2012	0.5	JF Muller	CSV streaming feed configuration	No
03/12/2012	0.6	JF Muller	Update DataBroker and CSV export configuration	No
06/12/2012	0.7	D. Becq	Update XMF part How to configure IPRaw transport with ns timestamp resolution instead of ms	No
11/12/2012	0.8	S.Haegelin	RAMP feedback & update Network ports for PIC 9	No
16/01/2013	0.9	JM. Duraffourg	PR222575 : procedure to exchange Key between Neptune and NSP	No
17/01/2013	1.0	JM. Duraffourg	Fix a mistake for deleting the import in the Key exchange procedure	No
23/01/2013	1.1	JM. Duraffourg	Update	No
12/02/2013	1.2	S.Haegelin	PR 222358	No
14/02/2013	1.3	P.Tribollet	PR 223910	No
14/02/2013	1.4	S.Haegelin	Update Neptune Key exchange	No
22/05/2013	1.6	S.Haegelin	Added Switch config template	No
23/05/2013	1.7	S.Haegelin	Update Switch config template	No
24/05/2013	1.8	S.Haegelin	Update Switch config template	No
27/05/2013	1.9	S.Haegelin	Update Switch config template	No
28/05/2013	1.10	F. Cêtre	PR 228201 path to listLicencedHosts script	No
29/05/2013	1.11	S.Haegelin	Update Switch config	No

			template	
31/05/2013	1.12	S.Haegelin	Update Switch config template	No
3/06/2013	1.13	S.Haegelin	Update Switch config template	No
17/06/2013	1.14	S.Haegelin	Update Switch config template	No
19/06/2013	1.15	S.Haegelin	Update Switch config template	No
20/06/2013	1.16	G.Agnihotri	Added Switch config template for T1100 for Cisco 2950 & 4948 (PR 228825 & 228226)	No
20/06/2013	1.17	S.Haegelin	Update Switch config template	No
24/06/2013	1.18	S.Haegelin	Update Switch config template	No
25/06/2013	1.19	S.Haegelin	Update Switch config template	No
27/06/2013	1.20	S.Haegelin	Update Switch config template	No
01/07/2013	1.22	S.Haegelin	Typo correction	No
01/07/2013	1.23	S.Haegelin	Correct Switch config template	No
04/07/2013	1.24	S.Haegelin	Add SSH configuration on Switch	No
05/07/2013	1.26	S.Haegelin	Add RM mediation Switch	No
18/07/2013	1.27	S.Haegelin	PR 230127	No
23/07/2013	1.28	S.Haegelin	PV feedback	No
24/07/2013	1.29	S.Haegelin	Fixed VLAN in the IMF port allocation	No
26/07/2013	1.30	S.Haegelin	PV feedback	No
29/07/2013	1.31	S.Haegelin	Update for PIC 9.0.2 new switch config	No
30/07/2013	1.32	S.Haegelin	Rename section 14.1.5 to add the 2950	No
1/08/2013	1.33	S.Haegelin	PV feedback on section 14.1.7	No
13/08/2013	1.34	S.Haegelin	PR 231039	No
13/08/2013	1.35	S.Haegelin	PR 231040 & 231041	No
13/08/2013	1.36	S.Haegelin	Added comment for NTP in the blade enclosure switch config	No
14/08/2013	1.37	S.Haegelin	Update 4948 reset to factory	No

			defaults and add the IOS software upgrade	
14/08/2013	1.38	S.Haegelin	Update balde enclosure switch	No
20/08/2013	1.39	S.Haegelin	PR 231182	No
22/08/2013	1.41	S.Haegelin	PR 231322	No
23/08/2013	2.0	S.Haegelin	PV desk review	Yes
26/08/2013	4.1	JF. Muller	DWS customer integration	No
06/09/2013	4.2	S.Haegelin	IMF Layer switch config	No
25/09/2013	4.3	S.Haegelin	blade enclosure switch config	No
27/09/2013	4.4	S.Haegelin	PR 231964	No
8/11/2013	4.5	S.Haegelin	Move the switch configuration instructions from the manufacturing guide	No
8/11/2013	4.6	S.Haegelin	PR 232495	No
18/11/2013	4.7	S.Haegelin	PR 231963	No
20/01/2014	4.10	S.Haegelin	PR 236252	No
30/01/2014	4.11	B. Chappell	Replaced title page and added page 2 with Oracle re-branding information	No
10/02/2014	4.14	JF. Muller	PR 236975 – DataExport activation	No
21/02/2014	4.15	S.Haegelin	PR 237069	No
21/02/2014	5.0	B. Chappell	Accepted all changes and published as Rev E	No

Table of Contents

1 Introduction

Topics:

1.1 Access the Customer Support Site (ESWD Download Center)

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a software. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Tekelec Customer Support site (http://support.tekelec.com/ or https://secure.tekelec.com/OA_HTML/ibuhpage.jsp within Tekelec network).

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.
2. Click the **Download Center** tab to access the software iso file.
3. Firmawares are available faor all customers under the name A-Tekelec Firmware Releases
4. The PIC product is availbale under the customer name.
5. To download a file to your location, right-click the file name and select **Save Target As**.

1.2 Documentation Admonishments

Admonishments are icons and text throughout this manual that alert the reader to assure personal safety, to minimize possible service interruptions, and to warn of the potential for equipment damage.

Table 1: Admonishments

	DANGER: (This icon and text indicate the possibility of personal injury.)
	WARNING: (This icon and text indicate the possibility of equipment damage.)
	CAUTION: (This icon and text indicate the possibility of service interruption.)

1.3 Reference Documents

EAGLE SW Compatibility Matrix SS005887 V18
HP Solutions Firmware Upgrade Pack Upgrade Procedures 2.2 909-2234-001 Revision B, April 2013
Platform 6.x Configuration Procedure Reference 909-2209-001 Revision E, January 2013
IXP License Key request form WI005536.xlsx

1.4 Related Publications

For information about additional publications that are related to this document, refer to the *Release Notice* document. The *Release Notice* document is published as a part of the *Release Documentation*.

1.5 Access the Customer Support Site (ESWD Download Center)

Access to Tekelec's Customer Support site is restricted to current Tekelec customers only. This section describes how to log into the Tekelec Customer Support site and locate a software. Viewing the document requires Adobe Acrobat Reader, which can be downloaded at www.adobe.com.

1. Log into the Tekelec Customer Support site (http://support.tekelec.com/ or https://secure.tekelec.com/OA_HTML/ibuhpage.jsp within Tekelec network).

   Note: If you have not registered for this new site, click the **Register Here** link. Have your customer number available. The response time for registration requests is 24 to 48 hours.
2. Click the **Download Center** tab to access the software iso file.
3. Firmawares are available faor all customers under the name A-Tekelec Firmware Releases
4. The PIC product is availbale under the customer name.

5. To download a file to your location, right-click the file name and select **Save Target As**.

1.6 Scope and Audience

This document describes the procedures to integrate the operating system and applications software for a PIC system at Release 9.0 within a customer network environment.

This document is intended for use by internal Tekelec personnel trained in software installation on rackmount and c-class blades system, trained Distribution Partners and trained Customer representatives. A working-level understanding of Linux and command line interface is expected to successfully use this document.

It is strongly recommended that prior to performing an integration of the operating system and applications software, on a rackmount or c-class blades system, the user read through this document.

Note: The procedures in this document are **not** necessarily in a sequential order. There are flow diagrams in the *Integration Overview Flowcharts* chapter that provide the sequence of the procedures for each component of this PIC system. Each procedure describes a discrete action. It is expected that the individuals responsible for installing the PIC system should reference these flow diagrams during this installation process.

Note: For hardware purchased from a source toher that Tekelec, hardware issues should be escalated with the provider of the hardware, not Tekelec.

1.7 Requirements

Software

Prerequisite: PIC software has already been installed in Tekelec manufacturing and has been shipped to customer.
No other additional software DVD or ISO file is required during the customer network integration procedure.

Licenses

Licenses required for software installation of PIC 9.0 are embedded licenses and do not require an explicit license key be applied. The exception to this is the xDR Builder license.

The following license is required for this installation:

- xDR Builder License (use the form WI005536.xlsx to request it)

Hardware

For non-Tekelec purchased hardware, the software must be installed first using the Manufacturing Installation Procedure prior to starting the Customer Integration Procedure.

PIC release 9.0 supports the following hardware for the Manufacturing Installation:
http://signal.tekelec.com/Depts/salesmktg/ProductInformationLibrary/Forms/FeaturePlanningGuides.aspx
http://signal.tekelec.com/sites/Engg/FeatureReqtsSpec/Shared%20Documents/FE007228.doc
http://signal.tekelec.com/sites/Engg/FeatureReqtsSpec/Shared%20Documents/FE007119.docx

POWER	PRODUCT	CABINET P/N	TECHNICAL REFERENCE (T.R)	SYSTEM INTERCONNECT (S.I)
G8&D2700 PRODUCT				
AC	CTRL CABINET (NSP IXP) RM	870-3115-03&04	821-0042-02	892-0098-03
AC	Extension CABINET (IXP) RM	870-3115-01&02	821-0043-02	892-0099-02
AC	PMF CABINET RM	870-3115-06&07	821-0045-02	892-0101-02
AC	BASE STORAGE C-Class	870-3115-10	821-0049-02	892-0103-11
AC	EXTENSION STORAGE C-Class	870-3115-09		892-0103-12
AC	COMPUTE C-Class	870-3115-11		892-0103-13
AC	NETWORK C-Class	870-3115-12		892-0103-14
DC	IMF DC ENTREPRISE 36U RM NEBS	870-3115-08	821-0054-02	892-0105-02
DC	IMF DC ENTREPRISE 42U RM	870-3115-05	821-0048-02	
G6&D2700 PRODUCT				
AC	CTRL CABINET (NSP IXP) RM on HP G6	870-3021-XX	821-0042-01	892-0098-XX
AC	Extension CABINET (IXP) RM on HP G6	870-3022-XX	821-0043-01	892-0099-01
AC	PMF CABINET RM on HP G6	870-3023-XX	821-0045-01	892-0101-01
AC	BASE STORAGE C-Class on HP G6 (P2000 & D2700)	870-3042-01	821-0049-01	892-0103-01
AC	EXTENSION STORAGE C-Class on HP G6 (P2000 & D2700)	870-3042-02		892-0103-02
AC	COMPUTE C-Class on HP G6 (P2000 & D2700)	870-3042-03		892-0103-03
AC	NETWORK C-Class on HP G6 (P2000 & D2700)	870-3042-04		892-0103-04
AC	LAB TRIAL C-Class on HP G6 (P2000 & D2700)	870-3042-05		892-0103-05
DC	IMF DC ENTREPRISE 36U RM on HP G6	870-3039-01	821-0046-01	892-0102-01
DC	IMF DC ENTREPRISE 42U RM on HP G6	870-3031-01	821-0048-01	892-0105-01
AC	IMF AC ENTREPRISE 42U RM on HP G6	870-3063-XX	821-0050-01	892-0107-01
G5&MSA PRODUCT				
AC	*BASE STORAGE on C-Class on HP G6 (MSA2000 & MSA2012)*	*870-3020-01*	*821-0044-01*	*892-0100-01*
AC	*EXTENSION STORAGE on C-Class on HP G6 (MSA2000 & MSA2012)*	*870-3020-02*		*892-0100-02*
AC	*COMPUTE on C-Class on HP G6 (MSA2000 & MSA2012)*	*870-3020-03*		*892-0100-03*
AC	*NETWORK on C-Class on HP G6 (MSA2000 & MSA2012)*	*870-3020-04*		*892-0100-04*
AC	*LAB TRIAL on C-Class on HP G6 (MSA2000 & MSA2012)*	*870-3020-05*		*892-0100-05*
AC	*BASE STORAGE on C-Class on HP G5*	*870-3010-01*	*821-0037-01*	*892-0093-01*
AC	*EXTENSION STORAGE on C-Class on HP G5*	*870-3010-02*		*892-0094-01*
AC	*COMPUTE on C-Class on HP G5*	*870-3010-03*		*892-0095-01*
AC	*NETWORK on C-Class on HP G5*	*870-3010-04*		*892-0094-02*
AC	*LAB TRIAL on C-Class on HP G5*	*870-3010-05*		*892-0096-01*
TEKII & TEKIII PRODUCT				
DC	IMF DC ENTREPRISE RM on TEK II (T1100) with CISCO2950 redundant WAN	870-0211-01	TR005727	892-0072-02
DC	IMF DC ENTREPRISE RM on TEK II (T1100) with CISCO4948			892-0078-01
DC	IMF DC ENTREPRISE RM on TEK III (T1200)	870-3009-01	821-0034-10	892-0091-08

Cha Chapter

2 Integration Overview Flowcharts

Topics:

-

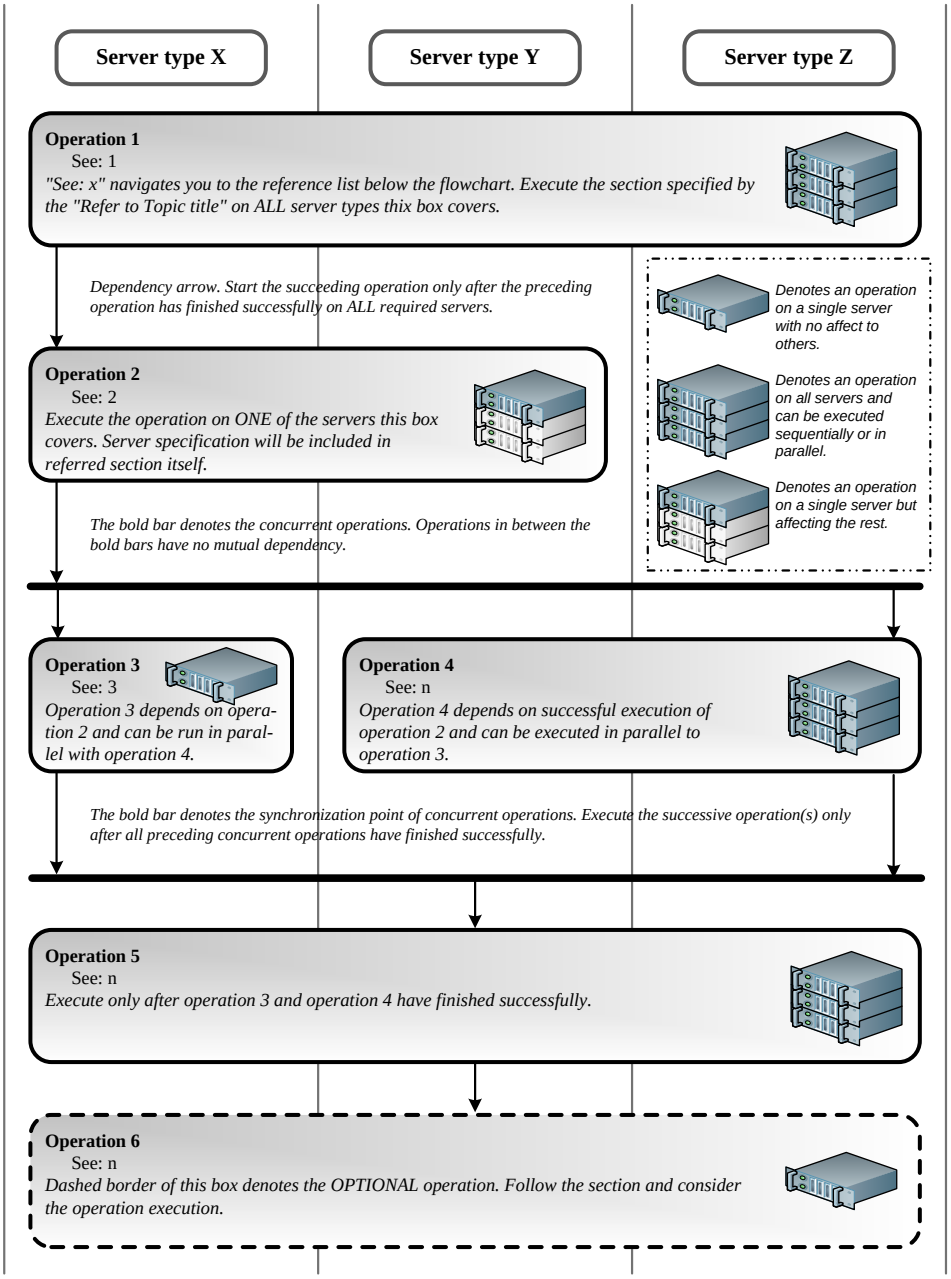
- *EFS Customer Network Integration* **Overview**
-
- *RSP Customer Network Integration*

  Overview
- *DWS Customer Network Integration Overview*

2.1 Flowchart Description

The flowcharts within each section depict the sequence of procedures that need to be executed to install the specified subsystem.

Each flowchart contains the equipment associated with each subsystem, and the required tasks that need to be executed on each piece of equipment. Within each task, there is a reference to a specific procedure within this manual that contains the detailed information for that procedure.

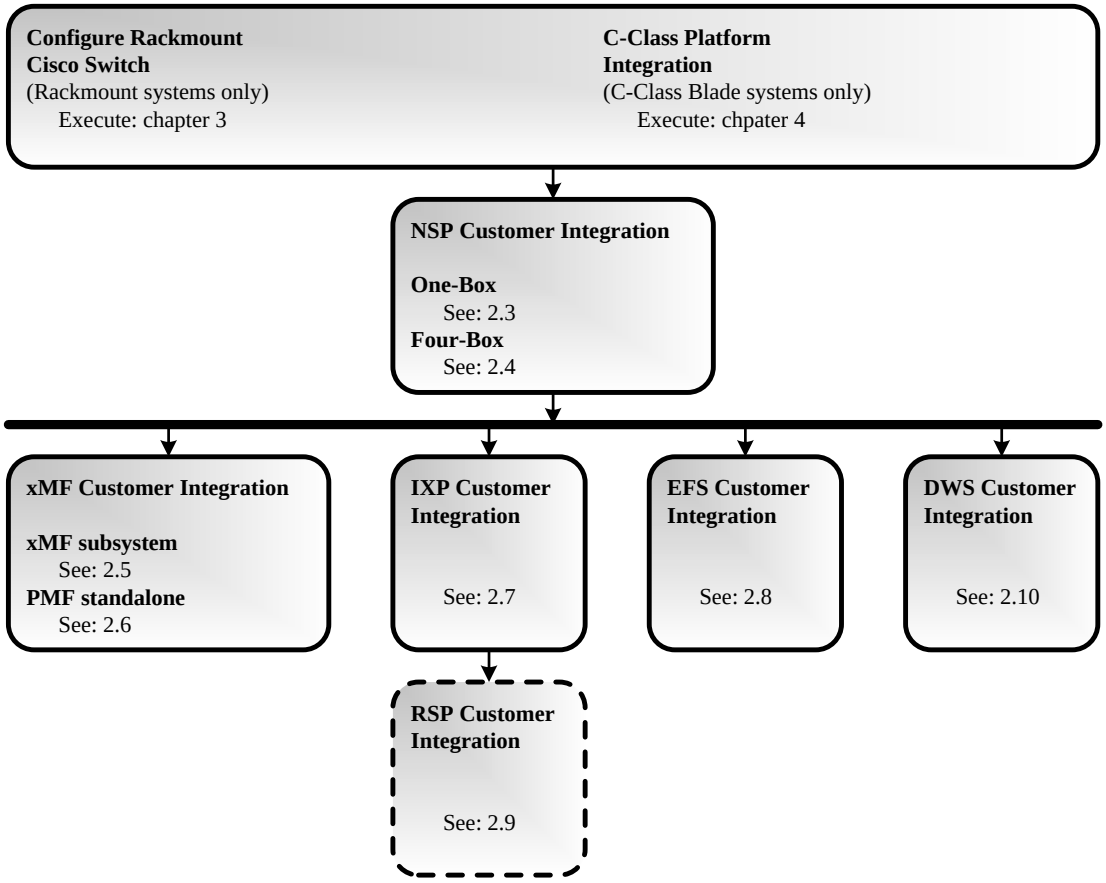


2.2 PIC Customer Integration Overview

This flowchart describes PIC high-level customer network integration overview. Follow the dependencies depicted in the flowcharts.

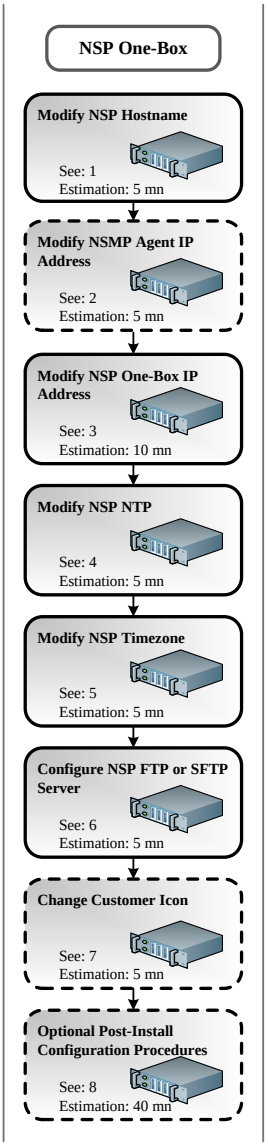
Based on the system type execute first rackmount switch customer integration or C-Class blade system customer integration.

Accordingly to dependency depicted in the flowchart run the NSP customer network integration as next. The following xMF/IXP/EFS customer network integration can be run in parallel. RSP customer network integration can be run after IXP customer network integration. Referring to graphic below, the system type applicable to each component is identified and the applicable flowchart is identified by section of this document where it is located.



2.3 NSP: One-Box Customer Integration Sequence

This flowchart depicts the sequence of procedures that must be executed to integrate

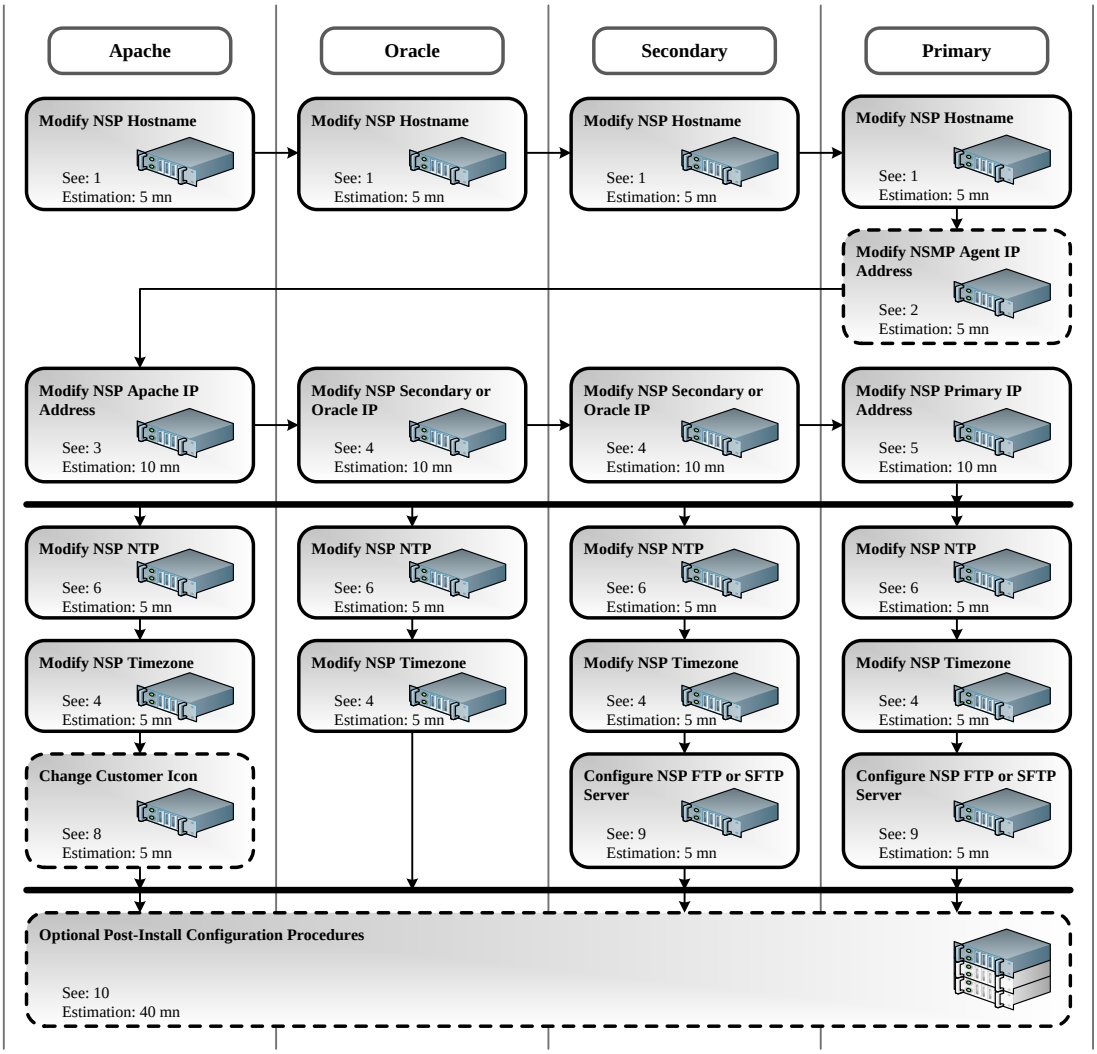


1. Refer to *Modify NSP Hostname*.
2. Refer to *Modify SNMP Agent IP Address (Optional)*.
3. Refer to *Modify NSP One-Box IP Address*.
4. Refer to *Modify NSP NTP*.
5. Refer to *Modify NSP Timezone*.
6. Refer to *Configure NSP FTP or SFTP Server*.
7. Refer to *Change Customer Icon (Optional)*.
8. Refer to
9.

10. *Optional Post-Install Configuration* **Procedures**.

2.4 NSP: Four-Box Customer Integration Sequence

This flowchart depicts the sequence of procedures that must be executed to integrate the NSP Four-Box setup.

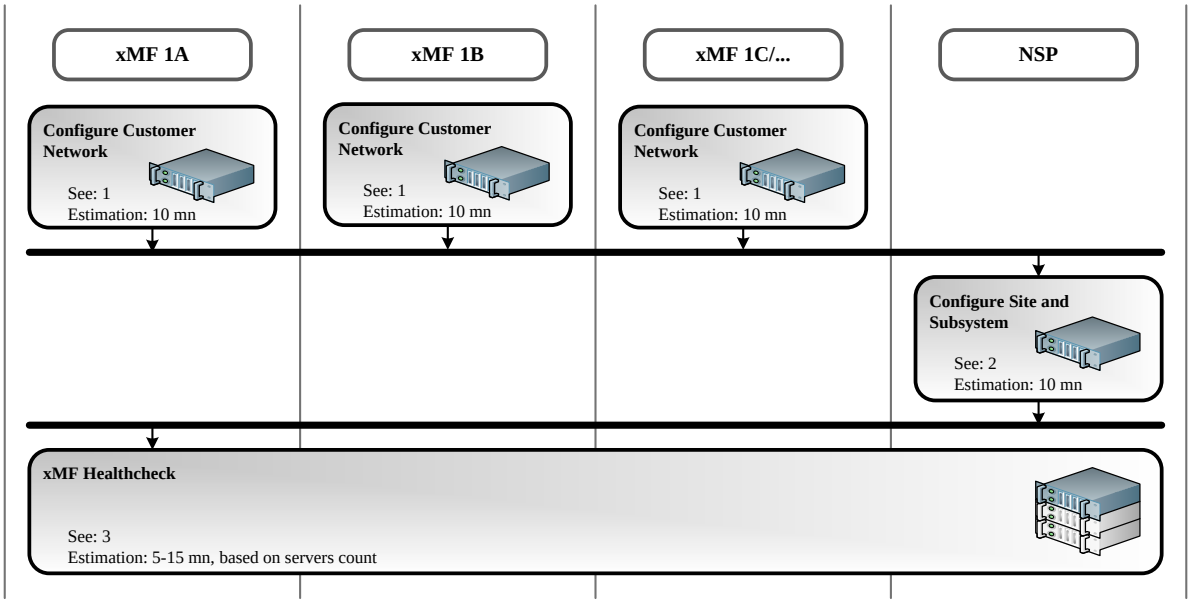


1. Refer to *Modify NSP Hostname*.
2. Refer to *Modify SNMP Agent IP Address (Optional)*.
3. Refer to *Modify NSP Apache IP Address (Four-Box Configuration)*.
4. Refer to *Modify NSP Secondary or Oracle IP Address (Four-Box Configuration)*.
5. Refer to *Modify NSP Primary IP Address (Four-Box Configuration)*.
6. Refer to *Modify NSP NTP*.
7. Refer to *Modify NSP Timezone*.
8. Refer to *Change Customer Icon (Optional)*.
9. Refer to *Configure NSP FTP or SFTP Server*.
10. Refer to
11.
12. *Optional Post-Install Configuration* **Procedures**.

2.5 XMF T1200/DL380 G6 Subsystem Customer Integration

The flowchart navigates through the customer integration of the following xMF subsystems:

- IMF Subsystem



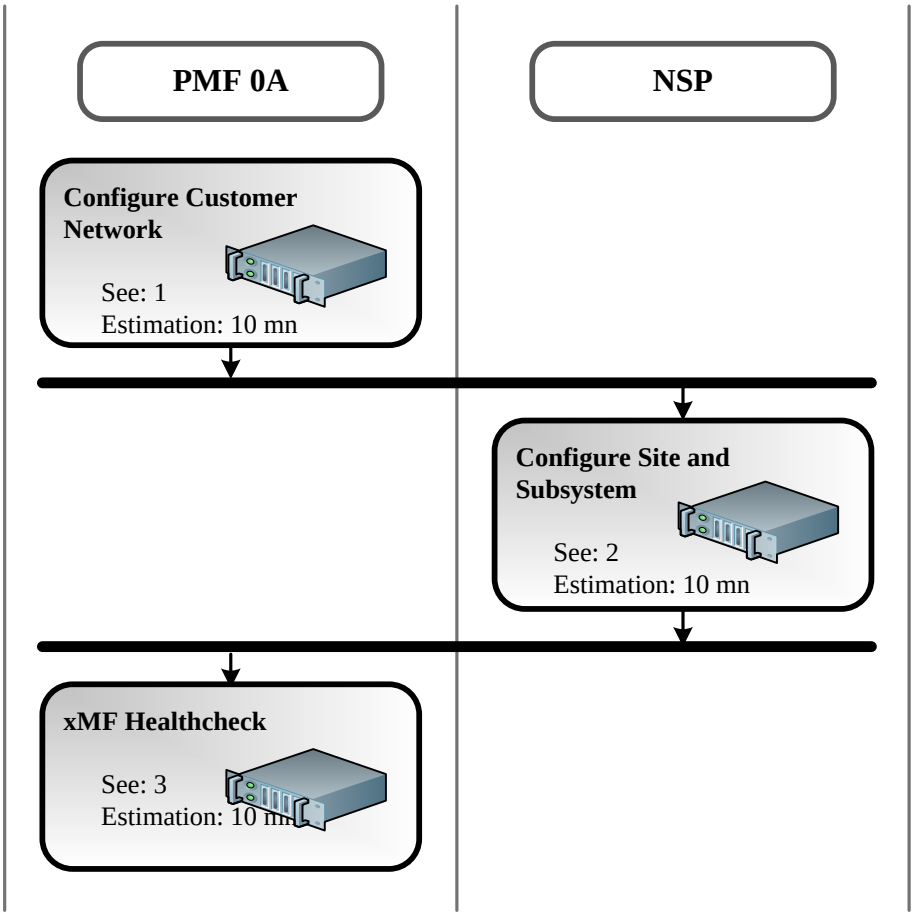
1. PMF Subsystem Refer to

2. *Customer Network Configuration T1100, T1200, G5,* **G6 and Gen8**.
3. Refer to *Configure Site and Subsystem for xMF*.
4. Refer to *xMF Healthcheck*.

2.6 PMF DL380 G6 Standalone Customer Integration Overview

The flowchart navigates through the customer integration of the following xMF server function:

• PMF Standalone Server

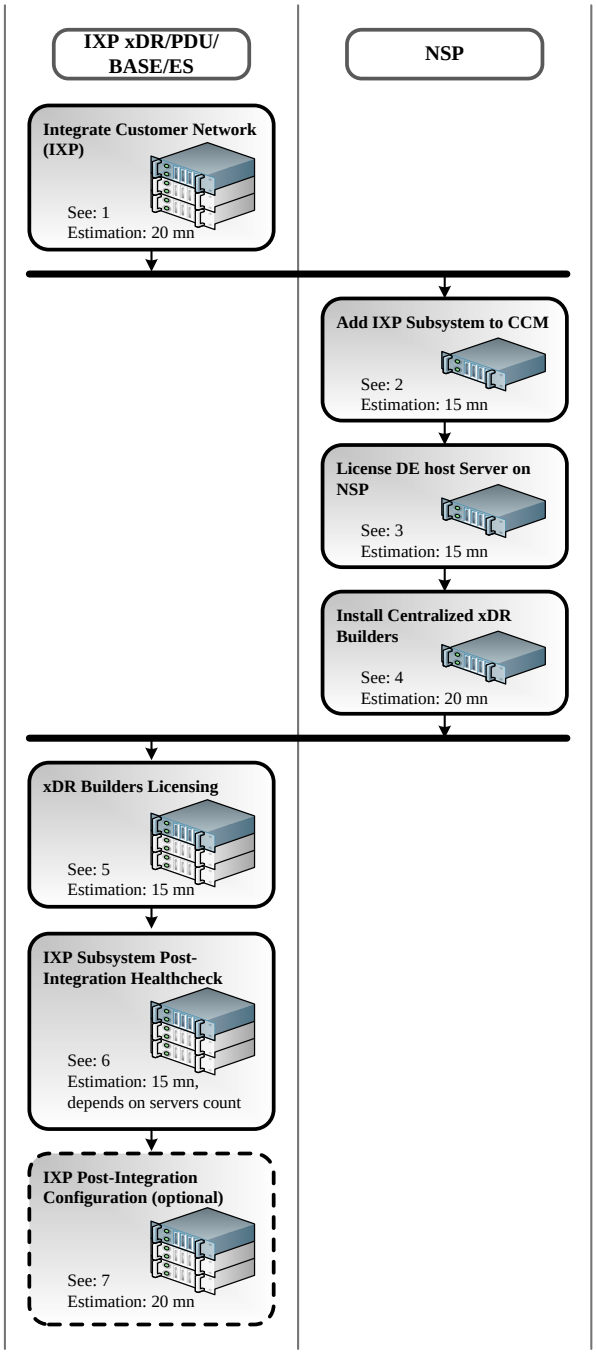


1. Refer to

2. *Customer Network Configuration T1100, T1200, G5,* **G6 and Gen8**.
3. Refer to *Configure Site and Subsystem for xMF*.
4. Refer to *xMF Healthcheck*.

2.7 IXP Customer Network Integration Overview

This flowchart depicts the sequence of procedures that must be executed to integrate the IXP subsystem setup.

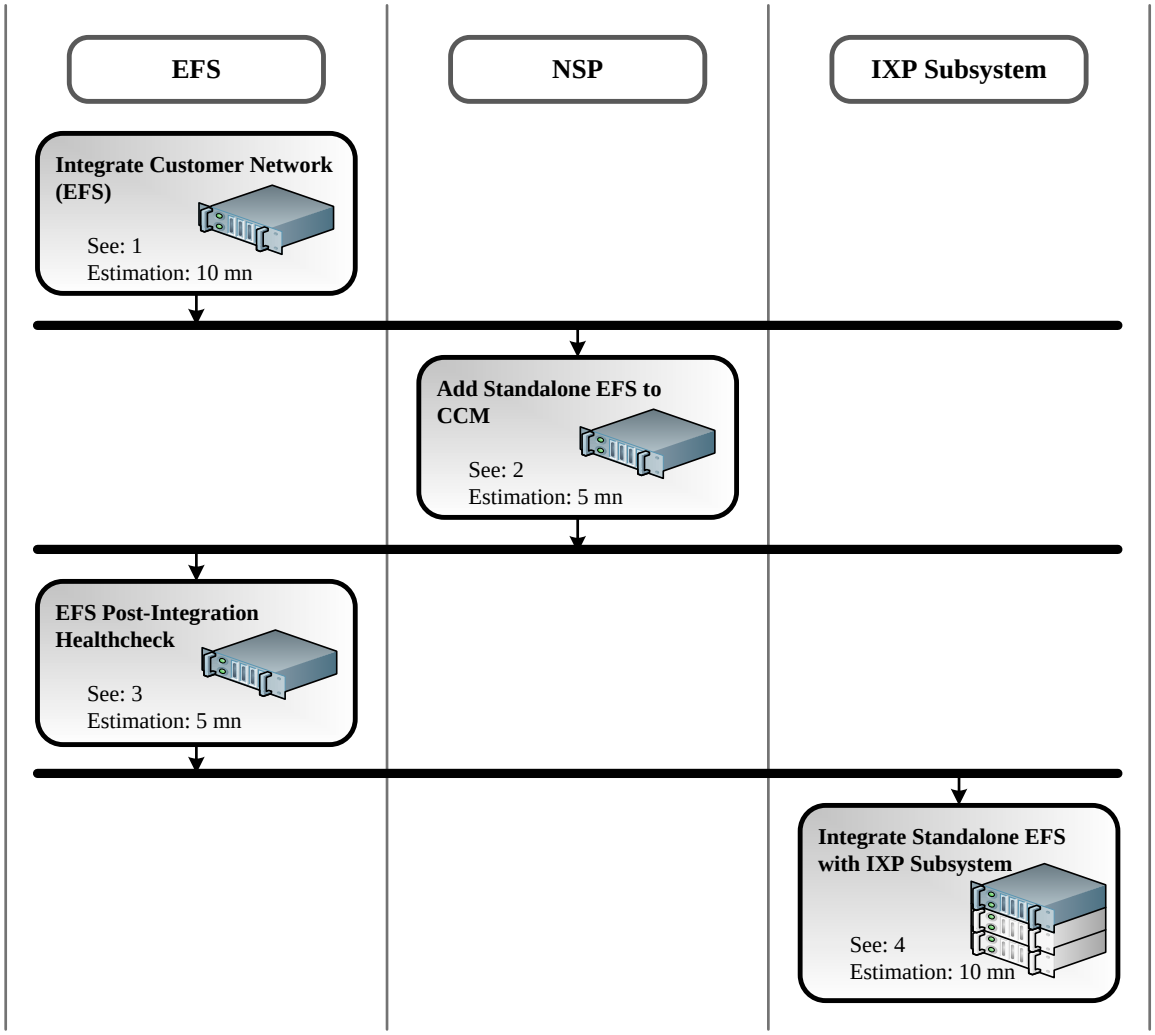


1. Refer to *Integrate Customer Network (IXP)*.
2. Refer to *Add IXP Subsystem to CCM*.

3. Refer to *License DataFeed Host Server* .
4. Refer to *Install xDR Builders*.
5. Refer to *xDR Builders Licensing*.
6. Refer to *IXP Subsystem Healthcheck*.
7. Refer to *IXP Post-Integration Configuration (Optional)*.

2.8 EFS Customer Network Integration Overview

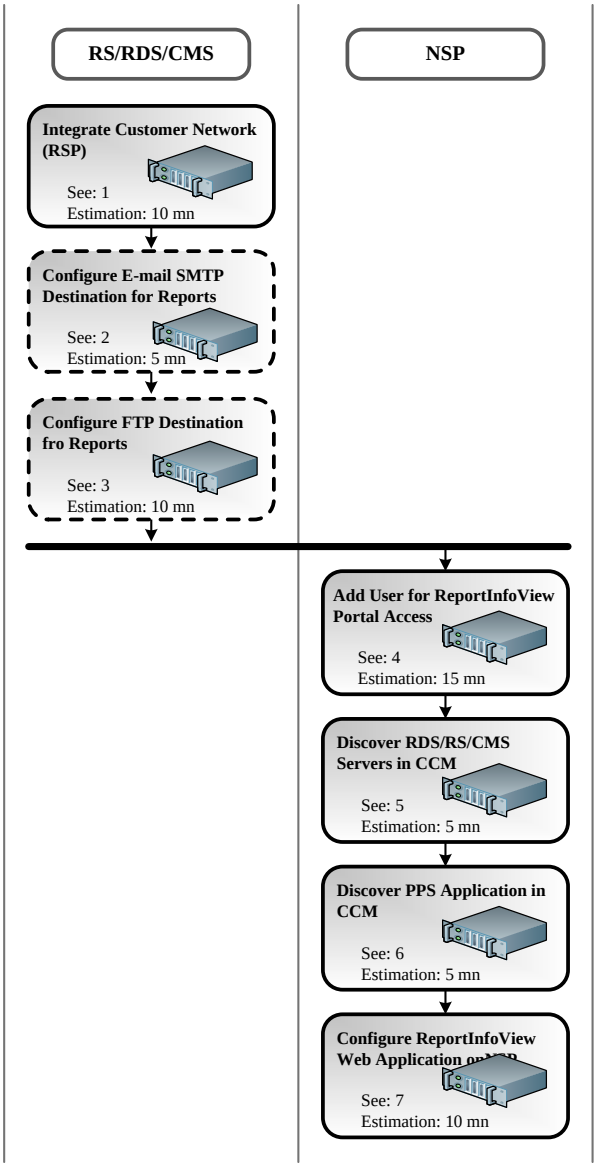
This flowchart depicts the sequence of procedures that must be executed to integrate the EFS setup.



1. Refer to *Integrate Customer Network (EFS)*.
2. Refer to *Add Standalone EFS to CCM*.
3. Refer to *EFS Healthcheck*.
4. Refer to *Integrate Standalone EFS with IXP Subsystem*.

2.9 RSP Customer Network Integration Overview

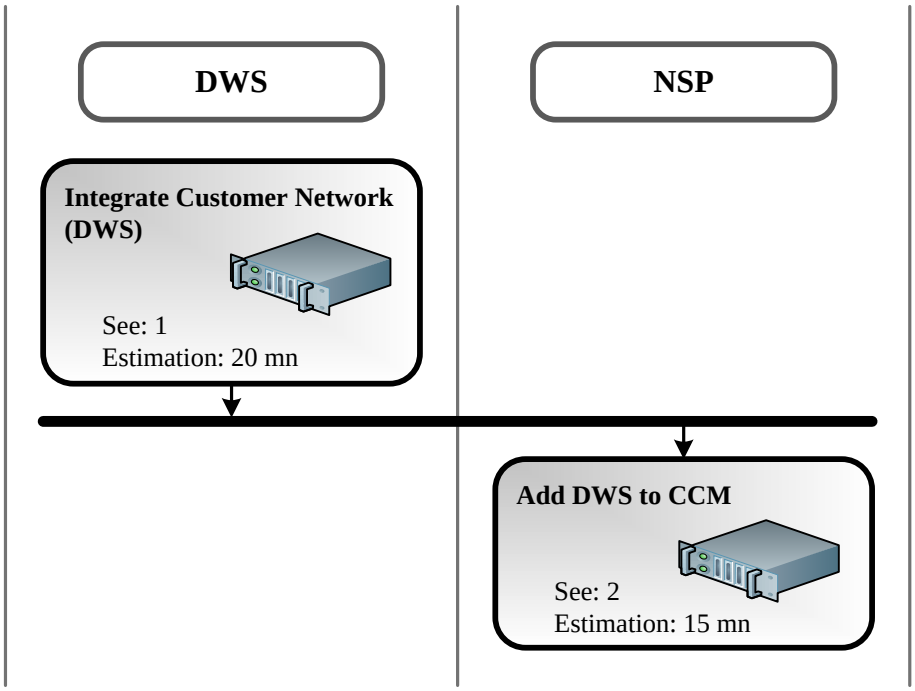
This flowchart depicts the sequence of procedures that must be executed to integrate the RSP setup.



1. Refer to *Integrate Customer Network (RSP)*.
2. Refer to *Configure E-mail SMTP Destination for Reports* (Optional).
3. Refer to *Configure FTP Destination for Reports* (Optional).
4. Refer to *Add User for ReportInfoView Portal Access (Optional)*.
5. Refer to *Discover RDS/RS/CMS Servers in CCM*.
6. Refer to *Discover PPS application in CCM*.
7. Refer to *Configure ReportInfoView Web Application on NSP*.

2.10 DWS Customer Network Integration Overview

This flowchart depicts the sequence of procedures that must be executed to integrate the DWS setup.



1 Refer to *Integrate Customer Network (DWS)*.
2 Refer to *Add DWS to CCM*.

Chapter
3

3 Rackmount Switches Configuration

Topics:

3.1 Configure Rackmount Cisco Switch

3.1.1 For PIC 9.0.1 and lower

This procedure describes how to configure the Cisco Catalyst 3560/4948 distribution and backbone switch.

Note: Make sure that the cables have been properly installed prior to this configuration procedure. Verify that the iLOs are connected to the odd ports and the servers are connected to the even ports.

Note: Repeat this procedure once for each Cisco Catalyst 3560/4948 distribution/backbone switch that is part of the PIC system.

1. **Verify the switch is connected to the IXP xDR Storage server serial interface**

   a) Verify that the blue serial cable from the switch you want to configure is connected to the serial port of any IXP xDR Storage server.

   Note: If the cable is not connected, then connect the serial cable before proceeding with this procedure.

2. **Power on the switch and wait until POST is complete**

   Power on the switch.

   The Power-On-Self-Test (POST) begins. Wait until the test is complete (may take up to several minutes to complete).

   - If the POST is successful, the **SYST** LED rapidly blinks green. Continue with this procedure.
   - If the POST fails, the **SYST** LED is amber. Discontinue this procedure and contact the Tekelec Customer Care Center.

3. **Set the switch configuration type and IP address**

   a) Log in as root on the IXP server where the serial cable from the requested switch is connected.

   b) Enter the **platcfg** menu. As root,
   run: # su - platfg

   c) Select **IXP Configuration ► Switch Configuration**
   The **Switch Configuration Menu** window appears and lists associated switches.

   d) Select the appropriate switch and press **<ENTER>.**

   Example:

   c3560-bb - Cisco c3560 backbone c3560-db - Cisco c3560 distribution c4948-bb - Cisco c4948 backbone c4948-db - Cisco c4948 distribution

   Note: Cisco c3560 is the legacy no longer supported hardware but still showing in the platcfg menu.

   e) On the next screen, click **Edit.**
   The **Edit Switch Details** window appears.

   f) Type information in all of the fields and click **OK.**

   g) Return to main **platcfg** menu.

4. **Configure the switch**

   a) From the main **platcfg** menu, select **Network Configuration ► Configure switch.**

   b) Select the switch type that was set in the preceding step and press **<ENTER>.**
   You will be asked to verify this operation. Click **Yes.** The switch configuration process begins. When complete, a status message of the configuration process appears.

   Example output of a successful configuration:

   Successfully enabled on switch ixp-switch.

Reloading switch ixp-switch with defaults, please standby... Switch ixp-switch successfully set to default configuration. Successfully started management VLAN on ixp-switch. Removing config file ixp-switch.startup-config from /tfpboot. Reloading switch ixp-switch, please standby... Reload of switch ixp-switch complete. Switch ixp-switch successfully complete. Press any key to continue...

If an error occurs in the log during the switch configuration, repeat this step. If this step will fail again contact the Tekelec Customer Care Center.

c) Exit the **platcfg** menu

3.1.2 For PIC 9.0.2 and higher

Note: In case in the procedure would failed, refer to 909-2247-01 PIC 9.0 Maintenance guide in order to recover the switch from rommon prompt.

A. Configure and access the serial console from the server on the switch
   a. Refer to section 14.1.1
B. Reset the switch to factory default
   a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

   b. Refer to section 14.1.3 to reset the switch
C. Configure the switch using the appropriate template
   a. Refer to section 14.2 to select and the appropriate configuration template and adapt it to the customer IP network.
   b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
   c. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.

   d. Paste all the commands from the template config you have adated to you network. The lines you need to customize are higlited with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
   e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

   f. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

   g. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

```
Switch# reload
```

   h. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

   i. Finally to configure the SSH access to the switch refer to section 14.1.7
   j. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

   k. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

   l. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

Chapter
4

4 C-Class Platform Integration

Topics:

The HP C-Class PIC system is extremely complex and has several components which can be challenging and time-consuming during the installation phase. For this reason, many of the installation steps have been completed in Manufacturing before shipment.

The purpose of this procedure is to provide the onsite PSE with the instructions to follow when deploying a HP C-Class PIC system. In order to take full advantage of the time savings provided by in-house manufacturing, these procedures should be followed closely to avoid complete rebuild of any system components.

This section requires the IP addressing scheme to be changed to match the customer's network requirements.

For an estimated time for this procedure, refer to the *Integration Overview Flowcharts*

4.1 Update PM&C Configuration

Do not use platcfg to update PM&C server IP addresses. The PM&C network parameters can be changed through the GUI only after resetting the network information using the 'pmacadm resetProfileConfig' command in the PM&C shell. This will delete the existing configuration and allow you to run through the initialization wizard again. Keep in mind that the reset will not run until all provisioned enclosures and cabinets are deleted.

This procedure outlines the steps to update the PMAC configuration to reflect the customer network addresses.

Note: If you are using a PM&C on a virtual server you may update the TVOE host IP before to proceed with the virtual guest hosted.

An estimated time for this procedure is 10 minutes.

1. **Connect to PM&C GUI**
   a) Open Internet Explorer and enter the following URL: **http://<pmac bond0.2 ip>/gui**
   b) Login as pmacadmin.

2. **Delete existing enclosures**
   a) In the PM&C GUI navigate to **System Configuration ► Configure HPC Enclosures**
   b) Note down the enclosure IDs.
   c) Select **Delete Enclosure**
   d) Enter enclosure number, ie. 01 and click on **Delete.**
   e) Repeat steps b-d for remaining enclosures.

3. **Delete existing cabinet(s)**
   a) In the PM&C GUI navigate to **System Configuration ► Configure HPC Cabinets**
   b) Note down the cabinet IDs.
   c) Select **Delete Cabinet**
   d) Enter cabinet number, ie. 101 and click on **Delete.**
   e) Repeat steps b-d for remaining cabinets.

4. **Reinitialize PM&C configuration**
   a) Login to the PM&C via ssh as root and run the following command:
      - **pmacadm resetProfileConfig**
   b) This will reinitialize the PM&C and clear all network settings.

5. **PM&C GUI: Load GUI initialization wizard**
   a) In the PM&C GUI navigate to **PM&C Administration ► PM&C Initialization**
   b) Select the existing profile. Press **Next**
   c) Enter the **Network Address** and the **VLAN ID** for each VLAN in order (0,2, and 3) to match the network configuration at your site and click **Next.**
   d) The **Network** and the **Roles Description** is not midifiable. Click **Next.**
   e) Enter the IP addresses for each PMAC interface to the correct values for your site.
      - The line with the description of **Application interface** should contain the IP address of your back-end network interface (bond0.3).
      - The line with the description of **Control network for blades** should contain the IP address of your control network interface (bond0).
      - The line with the description of **PM&C Management** should contain the IP address of your management network interface. (bond0.2)

f) After entering the correct information click **Next.**
g) Configure the default route for the management network.

- Leave **Destination IP** and **Netmask** as 0.0.0.0.
  - Set the **Gateway IP Address** to the gateway IP address on your management network.

h) Click **Next.**
i) Enter the DHCP range:

- START: 169.254.100.10
- END: 169.254.100.254

j) Click **Next.**
k) The next window displays a summary of all the settings. Verify the settings are correct and click **Finish**

Note: Connection to the PM&C GUI will be lost at this point.

4.2 Update 4948 Switch 1A IP Address

The first step in the process is to gain connection to the system on the 1B 4948 switch using the Manufacturing IP addresses. The top (1A) switch will be reconfigured in this section to enable connection using the updated customer IP addresses.

This procedure outlines the steps to paste a new switch configuration into a Cisco 4948 switch through the PM&C ssh terminal.

An estimated time for this procedure is 30 minutes.

1. **Connect to the system**

a) Assign IP address to your laptop and connect to the 4948 switch1B using Port 46 for access to system components.

- IP address: 192.168.100.7
- Netmask: 255.255.255.0
  - Default Gateway: 192.168.100.1

Note: Some systems were manufactured with different subnets. If connection to the PM&C iLO in the next step is not successful, change the subnet to 192.168.101.xxx on your laptop, and use 192.168.101.5 for connecting to PM&C iLO.

2. **Connect to PM&C server via iLO**

a) Login to the PM&C iLO address in Internet Explorer:

- URL: http://192.168.100.5 (should be the address set in manufacturing)
- User: Administrator or root
- Password: <see password dragon>

b) Open the remote console and login as root.

3. **Determine current PMAC bond0.2 IP address**

a) From the PM&C iLO remote consol run as root:

ifconfig bond02

b) Note the IP address assigned to bond0.2 to be used in the next step.

4. Connect to the PM&C via ssh

a) Open a ssh session to the PM&C bond0.2 IP address and login as root.

5. Edit switch host IP addresses

a) Enter the platcfg menu. As root run:

```
# su - platcfg
```

b) Navigate to **Network Configuration ► Modify Hosts File**
c) Select **Modify Host**
d) Select **switch1A** and change the IP to the switch Management Network IP address for the customer network.
e) Click the **OK** button.
f) On the next screen confirm host addition. Navigate back to the main platcfg menu.
g) Repeat steps b-f for **switch1B**
h) Exit the platcfg menu.

6. Reconfigure switch1A

Note: In case in the procedure would failed, refer to 909-2247-01 PIC 9.0 Maintenance guide in order to recover the switch from rommon prompt.

A. Configure and access the serial console from the server on the switch it it is not already done
   a. Refer to section 14.1.2
B. Reset the switch to factory default
   a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

   b. Refer to section 14.1.3 to reset the switch
C. Configure the switch using the appropriate template
   a. Refer to section 14.3 to select and the appropriate configuration template and adapt it to the customer IP network.
   b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
   c. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.

   d. Paste all the commands from the template config you have adated to you network. The lines you need to customize are higlited with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
   e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

   f. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

   g. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

```
Switch# reload
```

   h. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

   i. Finally to configure the SSH access to the switch refer to section 14.1.7
   j. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

k. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

l. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

4.3 Update PM&C iLO IP Address

This procedure outlines the steps to update the PM&C iLO IP address to the customer IP address. An estimated time for this procedure is 15 minutes.

1. Enter the HP setup utility

a) In the PM&C integrated remote console run as root:

reboot

As the server boots watch for the prompt to press any key to enter setup. Press the <spacebar> at this point.
The boot sequence will enter setup mode and there will be a prompt:

Press F8 to enter iLO setup utility

Press <F8> at this point.

2. Change the iLO TCP/IP settings

b) In the iLO configuration window select **TCP/IP Settings**
c) Enter the customer IP address for the PM&C iLO interface.
d) Press <F10> to save the changes.

3. Exit iLO Configuration

a) In the iLO configuration window navigate to **File ► Exit**
b) The system will continue to boot. Connection to the iLO window will be lost at this point.

4.4 Update 4948 Switch 1B IP Address

After the PMAC configuration and ILO address has been updated, we can now connect to these elements though switch1A, which has already been configured with the customer networks settings. This section updates the second (1B) switch.

This procedure outlines the steps to paste a new switch configuration into a Cisco 4948 switch through the PMAC ssh terminal.

An estimated time for this procedure is 30 minutes.

1. Connect to the system

a) Move the laptop connection from switch1B to switch1A.
b) Verify connection to the PM&C GUI and iLO on the customer network addresses.
c) Open a ssh session to the PM&C bond0.2 IP address and login as root

2. Reconfigure switch1B

Note: In case in the procedure would failed, refer to 909-2247-01 PIC 9.0 Maintenance guide in order to recover the switch from rommon prompt.

A. Configure and access the serial console from the server on the switch it it is not already done
    a. Refer to section 14.1.2
B. Reset the switch to factory default
    a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

    b. Refer to section 14.1.3 to reset the switch
C. Configure the switch using the appropriate template
    a. Refer to section 14.3 to select and the appropriate configuration template and adapt it to the customer IP network.
    b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
    c. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.

    d. Paste all the commands from the template config you have adated to you network. The lines you need to customize are higlited with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
    e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

    f. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

    g. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

```
Switch# reload
```

    h. Move from the user mode to priviledge mode and than to config mode

```
Switch# enable
Switch# configure terminal
```

    i. Finally to configure the SSH access to the switch refer to section 14.1.7
    j. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

    k. If the configuration is fine than you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

    l. If there is an issue in your config you can can reboot the switch without saving and than restart the config from the step a

4.5 Update OA IP Address

The OA IP address settings are updated through the insight display on the front of each enclosure. This procedure details the steps to update the OA IP address using the insight interface. An estimated time for this procedure is 5 minutes.

Configure OA IP address using insight display on the front side of the enclosure

a) Navigate to **Enclosure Settings ► OA1 Info**
b) Select the **OA1 IP** and press **OK.**
c) On the **OA1 Network Mode** screen choose **static** and press **OK.**
d) On the **OA1 IP address** fill in **IP, mask** and **gateway.**
e) Press **OK** and then press **Accept All.**

4.6 Update OA Configuration

The OA settings (blade ILO addresses, NTP server, enclosure interconnect bays, SNMP settings) need to be updated to reflect actual customer network IP addresses. DO NOT MAKE ANY MODIFICATIONS TO USER ACCOUNTS.

This procedure outlines the steps to update blade ILO addresses, OA NTP server, 3020 and Brocade switch IP addresses, and OA SNMP settings

An estimated time for this procedure is 15 minutes.

1. **Connect to OA GUI**
   a) Open web browser and enter the URL: `http://<OA1 IP address>`
   b) Login as root

2. **Enter First Time Setup Wizard**
   a) In the OA GUI navigate to **Wizards ► First Time Setup**
   b) Click **Next** in the Welcome page.
   c) In the Enclosure Selection window select the enclosure and click **Next.**
   d) In the Configuration Management window click **Next.**

3. **Rack and enclosure settings**
   a) Check **Set time using an NTP server.** and enter Primary NTP server (which should be set to the IP address of the PM&C server on the Management Network), Poll interval (720 seconds) and select Time Zone.
   b) Enter **Primary NTP server.** Value should be set to the IP address of the PM&C server on the management network.
   c) Set **Poll interval** to 720 seconds
   d) Select the appropriate **Time Zone.**
   e) Click **Next.**

   Note: OA will be reset and you will need to log back into OA and configuration Wizard (Step 1 and 2) and continue with Step 4.

4. **Skip Administrator Account Setup and Local User Accounts setup**

   Note: Do not change any user account information.

   a) In the Administrator Account Setup window press **Skip.**
   b) In the Local User Accounts window press **Skip.**

5. **EBIPA settings**
   a) On the Enclosure Bay IP Addressing screen click **Next** to continue.
   b) In the Shared Device Settings window fill in the following values:

      - Fill in the **Subnet Mask** field.
      - Fill in the **Gateway** field.
      - Fill in iLO's IPs in the **Device List.** You can use autofill button which will sequentially fill in IP addresses below the current entry. Click to **Enabled** to enable all servers.

        Note: DO NOT fill in bays 1A-16A and 1B-16B. These are used for double-density blades (f.e. BL2x220c) which are not supported in this release.

- Scroll to the **Interconnect Settings** section at the bottom of the page.
- Fill in the **Subnet Mask** field.
- Fill in the **Gateway** field
- Fill in the IP addresses that will be assigned to the interconnect bays (Cisco 3020 switches and Brocade switches) in the rear of the enclosure and enable them.

c) Click **Next** to apply those settings. System will restart devices such as interconnect devices or iLOs to apply new addresses. After finishing check the IP addresses to ensure that apply was successful.

6. Skip Directory Groups, Directory Settings and Onboard Administrator Network Settings setup

a) In the Directory Groups window press **Next.**
b) In the Directory Settings window press **Next.**
c) In the Onboard Administrator Network Settings window press **Next.** There were set up earlier using the OA interface.

7. SNMP Settings

a) Check **Enable SNMP.**
b) Fill in **System Location** that is equal to **Enclosure Name** .
c) Do not set **Read Community** and **Write Community.**
d) Set SNMP Alert Destination to IP of the IXP VIP.
e) Set **Community string** to TEKELEC.
f) Click on **Next.**

8. Power management

a) Use default settings displayed on Power Management screen. Do not change anything.
b) Click on **Next.**

9. Exit the wizard

a) Click on **Finish** on the final screen to exit.

4.7 Configure Fibre Channel Controller

This section defines the process of updating the SAN controllers. **This is only possible using the proprietary serial cable originally provided with the units at shipping.** The addresses for both the 'a' and 'b' controllers are set through the 'a' controller.

This procedure outlines the steps to reset modify the network parameters, timezone, and NTP setting of the fiber channel controllers

An estimated time for this procedure is 15 minutes.

1. Configure IP address on Fibre Channel Disk Controller

a) Connect to the disk array serial console with following settings:

- 115200 bps, 8 data bits, no parity, 1 stop bit, no flow control

b) Proprietary cable that ships with the controller is required for console access.
c) You may have to log in using hte manage username and the corresponding password.
d) Once at the prompt (#), execute the following commands:

- **set network-parameters ip <controller_A_IP_address> netmask <netmask> gateway <gateway_IP_address> controller a**

- **set network-parameters ip <controller_B_IP_address> netmask <netmask> gateway <gateway_IP_address> controller b**

e) To verify the values were entered correctly, run the following command and check the output:

- **show network-parameters**

f) Since you are currently logged in at the cli, execute the following command at this time to make sure the expansion disk arrays will be identified correctly:

- **Rescan**

2. **Configure NTP and timezone on Fibre Channel Disk Controller**

a) Run the following command:

- **set controller-date <month> <day> <hh> :<mm> :<ss> <year> <time-zone> ntp enabled ntpaddress <PM&C_management_network_IP>**

where:

- month: jan|feb|mar|apr|may|jun|jul|aug|sep|oct|nov|dec
- day: 1-31
- hh: 0-23
- mm: 0-59
- ss: 0-59
- year: four-digit number
- timezone: offset from Universal Time (UT) in hours (e.g.: -7) for example:
- set controller-date sep 22 13:45:0 2007 -7 ntp enabled ntpaddress 69.10.36.3

b) Check the time settings:

show controller-date
show ntp-status

3. Configure SNMP trap host

a) Run the following command:

set snmp-parameters enable crit add-trap-host <target_IP>

This will enable delivery of critical events to the target destination.

If the target destination is IXP server set the IP address to IP of the IXP VIP.
If the target destination is NSP server set the IP address to IP of the NSP WebLogic primary server.

4. Repeat settings on remaining controllers

a) Repeat steps 1-3 on all Fibre Channel Disk Controllers at the site.

Chapter 5

5 NSP Customer Integration

Topics:

5.1 Modify NSP Hostname

This procedure describes how to update the hostname for an NSP Server.

For an estimated time for this procedure, refer to the NSP flowcharts in *Integration Overview Flowcharts*.

Note: This procedure is applicable to any NSP server.

1. Open a terminal window and log in as root on the NSP server.
2. Enter the **platcfg** menu. As root, run: # su -
   platcfg
3. Select **NSP Configuration ► Hostname Configuration.**
4. Click **Edit.**
5. Type the new NSP hostname and click **OK.**
   When the process is complete, the new hostname appears on the screen.
6. Verify the new hostname; then, click **Exit** to return to the **platcfg** menu
7. Exit the **platcfg** menu.

5.2 Modify SNMP Agent IP Address *(Optional)*

This procedure describes how to change the SNMP Agent IP address and version. This procedure is optional. If a customer has an alarm forwarding application installed which is optional application, then execution of this procedure is mandatory.

For an estimated time for this procedure, refer to the NSP flowcharts in *Integration Overview Flowcharts*.

1. Open a terminal window and log in as root on the NSP server (One-box) or the Primary server (Four-box).
2. Enter the **platcfg** menu. As root, run: # su -
   platcfg
3. Select **NSP Configuration ► SNMP Agent Configuration.**
4. Click **Edit.**
5. Type the SNMP Agent IP address in the **SNMP Management platform IP address** field. Then, select the desired SNMP version in the **SNMP version for access rights** field and click **OK.**
6. Exit the **platcfg** menu.

5.3 Modify NSP One-Box IP Address

This procedure describes how to update the IP address on the NSP One-box server.

1. Open a terminal window and log in as root on the NSP One-Box server.
2. Enter the **platcfg** menu. As `root,` run:
   - **`su - platcfg`**
3. Select **Network Configuration ► Network Interfaces ► IPv4 ► Edit an Interface** .

4. Select the appropriate interface option and click **OK:**

   - **eth01** for rackmount
   - **bond0.3** for blade

5. Select **OK** and press **Enter.**
6. Select Boot Protocol as **none** and press **ENTER**
7. Choose Address Action as **edit** and press **ENTER**
8. Type the new IP address for this interface and the netmask, if needed.

   Note: Update the netmask only if different from the original setting.

9. Select **OK** and press **Enter.** Then navigate back to the **platcfg** main menu.
10. Repeat steps 3-7 for the second interface. Use the appropriate option:

    - **eth02** for rackmount
    - **bond0.4** for blade

11. Select Boot Protocol as **none** and press **ENTER**
12. Choose Address Action as **edit** and press **ENTER**
13. From main **platcfg** menu, select **Network Configuration ► Routing ► IPv4 ► Static Routes ► Display Table ► main ► Edit ► Edit Route ► default.**
14. Select the route to edit. Then select **Type** as default and click **OK.**
15. Type the new gateway IP address and click **OK.**
16. Click **Exit** until the main **platcfg** menu appears.
17. If the second interface gateway IP address needs to be modified, repeat steps 9-12 for the second interface (either **eth02** or **bond0.4).**
18. From the main **platcfg** menu, select **NSP Configuration ► IP Configuration.**
19. Click **Edit.**
20. Click **Yes.**

    The IP address is changed.

21. Exit the **platcfg** menu.
22. After the IP address is changed , run the below command as a root user

    - **su - cfguser -c "setCCMnode *new_onebox_ip"***

    where *new_onebox_ip* will be the new IP address of NSP server.

5.4 Modify NSP Apache IP Address (Four-Box Configuration)

This procedure describes how to update the IP address on the NSP Apache server.

1. Open a terminal window and log in as root on the NSP Apache server.
2. Enter the **platcfg** menu. As `root`, run:

   # su –platcfg

3. Select **Network Configuration ► Network Interfaces ► IPv4 ► Edit an Interface** .

4. Select the appropriate interface option and click **OK:**
   - **eth01** for rackmount
   - **bond0.3** for blade
5. Select **OK** and press **Enter.**
6. Select Boot Protocol as **none** and press **ENTER**
7. Choose Address Action as **edit** and press **ENTER**
8. Type the new IP address for this interface and the netmask, if needed.

   Note: Update the netmask only if different from the original setting.
9. Select **OK** and press **Enter.** Then navigate back to the **platcfg** main menu.
10. Repeat steps 3-7 for the second interface. Use the appropriate option:
    - **eth02** for rackmount
    - **bond0.4** for blade
11. Select Boot Protocol as **none** and press **ENTER**
12. Choose Address Action as **edit** and press **ENTER**
13. From main **platcfg** menu, select **Network Configuration ► Routing ► IPv4 ► Static Routes ► Display Table ► main ► Edit ► Edit Route ► default.**
14. Select the route to edit. Then select **Type** as default and click **OK.**
15. Type the new gateway IP address and click **OK.**
16. Click **Exit** until the main **platcfg** menu appears.
17. If the second interface gateway IP address needs to be modified, repeat steps 9-12 for the second interface (either **eth02** or **bond0.4).**
18. From the main **platcfg** menu, select **NSP Configuration ► IP Configuration.**
19. Click **Edit.**
20. Type the new IP addresses for the NSP Primary and NSP Secondary in the appropriate fields and click **OK.**
21. Press **Enter.**
    A confirmation prompt appears.
22. Click **Yes.** This step will finalize NSP Apache IP change procedure. Leave the **platcfg** menu.

5.5 Modify NSP Secondary or Oracle IP Address (Four-Box Configuration)

This procedure describes how to update the IP address on the NSP Secondary or the Oracle server.

1. Open a terminal window and log in as root on the NSP Secondary server or NSP Oracle server.]
2. Select **Network Configuration ► Network Interfaces ► IPv4 ► Edit an Interface** .
3. Select the appropriate interface option and click **OK:**
   - **eth01** for rackmount
   - **bond0.3** for blade
4. Select OK and press Enter**.**
5. Select Boot Protocol as **none** and press **ENTER**

6. Choose Address Action as **edit** and press **ENTER**
7. Type the new IP address for this interface and the netmask, if needed.

   Note: Update the netmask only if different from the original setting.

8. Select **OK** and press **Enter.** Then navigate back to the **platcfg** main menu.
9. From main **platcfg** menu, select **Network Configuration ► Routing ► IPv4 ► Static Routes ► Display Table ► main ► Edit ► Edit Route ► default.**
10. Select the route to edit. Then select **Type** as default and click **OK.**
11. Type the new gateway IP address and click **OK.**
12. Click **Exit** until the main **platcfg** menu appears.
13. From the main **platcfg** menu, select **NSP Configuration ► IP Configuration.**
14. Click **Edit.**
15. Click **Yes.**

    The IP address is changed.
16. Exit the **platcfg** menu.

5.6 Modify NSP Primary IP Address (Four-Box Configuration)

This procedure describes how to update the IP address on the NSP Primary server.

1. Open a terminal window and log in as root on the NSP Primary server.
2. Enter the **platcfg** menu. As root, run:
   - **su - platcfg**
3. Select **Network Configuration ► Network Interfaces ► IPv4 ► Edit an Interface** .
4. Select the appropriate interface option and click **OK:**
   - **eth01** for rackmount
   - **bond0.3** for blade
5. Select **OK** and press **Enter.**
6. Select Boot Protocol as **none** and press **ENTER**
7. Choose Address Action as **edit** and press **ENTER**
8. Type the new IP address for this interface and the netmask, if needed.
   Note: Update the netmask only if different from the original setting.
9. Select **OK** and press **Enter.** Then navigate back to the **platcfg** main menu.
10. From main **platcfg** menu, select **Network Configuration ► Routing ► IPv4 ► Static Routes ► Display Table ► main ► Edit ► Edit Route ► default.**
11. Select the route to edit. Then select **Type** as default and click **OK.**
12. Type the new gateway IP address and click **OK.**
13. Click **Exit** until the main **platcfg** menu appears.
14. From the main **platcfg** menu, select **NSP Configuration ► IP Configuration.**
15. Click **Edit.**
16. Type the new IP addresses for the NSP Apache, NSP Oracle, and NSP Secondary servers in the appropriate fields and click **OK.**

17. Press **Enter.** A confirmation prompt appears.
18. Click **Yes.** This step will finalize NSP Apache IP change procedure. Leave the **platcfg** menu.
19. After the IP address is changed , run the below command as a root user **# su -**

    cfguser -c "setCCMnode *new_oracle_ip"*

    where *new_oracle_ip* will be the IP address of new oracle server.

5.7 Modify NSP NTP

This procedure describes how to update the NTP information.

For an estimated time for this procedure, refer to the NSP flowcharts in *Integration Overview Flowcharts*.

1. Open a terminal window and log in as root on the NSP server.
2. Enter the **platcfg** menu. As root, run: **# su -**

   platcfg

3. Select **Network Configuration ► NTP.**
4. Click **Edit.**
5. Type the new NTP Server IP address and click **OK.**
6. Exit the **platcfg** menu.

5.8 Modify NSP Timezone

This procedure describes how to update the Timezone information.

For an estimated time for this procedure, refer to the NSP flowcharts in *Integration Overview Flowcharts*.

1. Open a terminal window and log in as root on the NSP server.
2. Enter the **platcfg** menu. As root, run:
   # su - platcfg
3. Select **Server Configuration ► Timezone.**
4. Click **Edit.**
5. Select appropriate time zone and click **OK.**
6. Exit the **platcfg** menu.

5.9 Configure NSP FTP or SFTP Server

This procedure describes how to configure NSP to allow xDR export from ProTrace application to customer's external FTP or SFTP server.

Note: For an NSP Four-box, this procedure needs to be run on both the Primary server and the Secondary server.

1. **Copy the FTP security file from the NSP server**
   a) Open a terminal window and log in as root on the NSP server (One-box), Primary/Secondary server

(Four-box).

b) As root, run:

```
# cd /opt/nsp/bea/user_projects/domains/tekelec/nsp
```

c) Copy the contents of file sftp_security.pub.

2. Update the FTP or SFTP server

a) Log in on the FTP or SFTP server.

b) In the file $HOME/.ssh/authorized_keys, add the contents of file sftp_security.pub that you copied in the previous step.

c) Make sure that the FTP or SFTP server is properly configured to allow file transfer.

5.10 Change Customer Icon *(Optional)*

This procedure describes how to change the customer icon (for example, replace the standard Tekelec logo with a customer logo). This procedure is optional.

1. Open a terminal window and log in as tekelec on the NSP server (One-box) or NSP Apache server (Four-box).
2. Copy the customer icon file (customer_icon.jpg) to the /opt/www/resources directory.
3. Verify the customer icon properties:
   - The file name must be customer_icon.jpg.
   - The file must belong to user tekelec in group tekelec.
   - The compression format must be **Jpeg.**
   - Optimum width/height ratio is **1.25.**
   - Any image can be used; the suggested minimum width/height is **150** pixels.

5.11 Optional Post-Install Configuration Procedures

After NSP has been installed, there are optional configuration procedures that can be performed.

5.11.1 Install Optional Applications *(Optional)*

This procedure describes how to install optional applications. This procedure is optional.

1. Open a terminal window and log in as root on the NSP server (One-box) or the Primary server (Four-box).
2. Enter the **platcfg** menu. As root, run:

   ```
   # su - platcfg
   ```

3. Select **NSP Configuration ► Configure optional applications.**
   A window appears with a list of optional applications and their current status **(Installed** if the application is installed or **No** if the application is not installed).
4. Select **Edit.**
   A window appears with a list of all the optional applications that are currently not installed with their value set to **No.**
5. Select the application(s) that you want to install (use the arrowkeys to navigate and **spacebar** to select **Yes** or **No)** and click **OK.**
   The selected applications are installed. The install logs are available at

/var/log/nsp/install/nsp_install.log.

6. Exit the **platcfg** menu.

5.11.2 Configure Apache HTTPS Certificate *(Optional)*

This procedure describes how to configure the Apache HTTPS certificate.

This procedure is optional; however, it is required when operating in a secured network environment and is available only on the NPS One-box or the Apache server (Four-box).

1. Open a terminal window and log in as root on the NSP One-box or the Apache server (Four-box).
2. Enter the **platcfg** menu. As root, run:

   # **su - platcfg**

3. Copy the files server.crt and server.key that are provided by the customer to /root.
4. Select **NSP Configuration ► Configure Apache HTTPS Certificate.**
5. Press **Enter.**
6. Select **Yes** to confirm the action.
7. Exit the **platcfg** menu.

5.11.3 Configure Mail Server *(Optional)*

This procedure describes how to configure the SMTP mail server.
This procedure is optional; however, this option is required for Security (password initialization set to AUTOMATIC) and Forwarding (forwarding by mail filter defined) and is available only on the
NPS server (One-box) or the Primary and Secondary server (Four-box).

1. Open a terminal window and log in as root on the NSP server (One-box) or Primary server (Four-box).
2. Enter the **platcfg** menu. As root, run: # su -

   platcfg

3. Select **NSP Configuration ► SMTP Configuration.**
4. Select **Edit.**
5. Type the IP address of the SMTP server and click **OK.**
   The host file for the alias used in the WebLogic Mail service is updated.
6. Exit the **platcfg** menu.
7. Open a terminal window and log in as root on the Secondary server (Four-box only)
8. Repeat procedure step 2 to 6 (Four-box only).

5.11.4 Configure Authenticated Mail Server *(Optional)*

This procedure describes how to authenticate the mail server. This procedure is optional.

Note: This procedure is performed ***after*** the SMTP has been configured (refer to the *Configure Mail Server (Optional)* procedure).

When a mail server requires authentication, additional parameters must be defined in the WebLogic console.

1. Connect to the NSP application interface.
2. Log in as weblogic on the WebLogic Console.
3. Select **Services ► Mail Sessions ► NspMailSession.**
4. Click **Lock&Edit** and modify the JavaMail properties as needed. For

example:

mail.transport.protocol=smtp,
mail.smtp.host=mail.server, mail.smtp.from=
noreply@tekelec.com, mail.smtp.timeout=5 00,
mail.smtp.connectiontimeout=500

5. Add the following parameters:

   mail.smtp.auth=true
   mail.smtp.port=465
   mail.smtp.quitwait=false
   user=*my_account*
   password=*my_password*

   where *my_account* and *my_password* change according to the customer SMTP server.

6. If the SMTP over SSL is used, then add the following parameters:

   mail.smtp.socketFactory.port=4 6 5
   mail.smtp.socketFactory.class=javax.net.ssl.SSLSocketFactory
   mail.smtp.socketFactory.fallback=false

7. Click **Save.**
8. Click **Activate Configuration.**
9. Log in as root on the NSP server and run: #

   service nspservice restart

5.11.5 Configure SNMP Management Server *(Optional)*

This procedure describes how to configure the SNMP management server.

This procedure is optional; however, this option is required for Forwarding (forwarding by SNMP filter defined) and is available only on the NPS One-box or the NSP Primary WebLogic server (Four-box).

1. Open a terminal window and log in as root on the NSP One-box or NSP Primary WebLogic server (Four-box).
2. Copy the files server.crt and server.key that are provided by the customer to /root.
3. Enter the **platcfg** menu. As root, run:

   # **su - platcfg**

4. Select **NSP Configuration ► SNMP Agent Configuration.**
   A window appears which allows you to enter the IP address of the SNMP management platform and version of SNMP agent and traps.
5. Select **Edit.**
6. Type the appropriate values and click **OK.**
   The SNMP agent configuration is updated and the SNMP Management server is automatically restarted.
7. Exit the **platcfg** menu.

5.11.6 Modify WebLogic Administration Password *(Optional)*

This procedure describes how to modify the WebLogic administration password.

This procedure is optional; however, this option is required for security and is available only on the NPS One-box or the Primary server (Four-box).

1. Open a terminal window and log in as root on the NSP One-box or Primary server (Four-box).
2. Enter the **platcfg** menu. As root, run:

```
# su - platcfg
```

3. Select **NSP Configuration ► NSP Password C onfiguration ► Weblogic Password Configuration (for startup and deploy).**
   A window appears which allows you to enter the password. The password must contain at least 1 non-alphabetical character.
4. Select **Edit.**
5. Type a valid password and click **OK.**

   Note: Make sure the new password contains at least one numeric or special character.

   The configuration files are updated and NSP is restarted automatically.
6. Exit the **platcfg** menu.

5.11.7 Configure Session Timeout *(Optional)*

This procedure describes how to configure the session timeout, the amount of time (in minutes) that a session can remain inactive before it is invalidated and token released.

1. Log in as TklcSrv on the NSP application interface.
2. Select the **Security** application.
3. Select **Action ► Manage Tokens.** The **Tokens** window appears.
4. Type the appropriate value (in minutes; must be from 15 to 480, e.g., 3 0) in the **Session timeout** field and click **Apply.**

5.11.8 Control Access of NSP to HTTPS *(Optional)*

This procedure describes how to control the access (enable or disable) of the NSP front-end to HTTPS. This procedure is optional.

1. Open a terminal window and log in as root on the NSP server (One-box) or the NSP Primary WebLogic server (Four-box).
2. Enter the **platcfg** menu. As root, run:
   ```
   # su platcfg
   ```
3. Select **NSP Configuration ► Enable HTTP Port ► Edit.**
4. Select the appropriate option to either enable or disable the access and click **OK.**
   - Select **Yes** to enable access to HTTP.
   - Select **No** to disable access to HTTP.
5. Exit the **platcfg** menu.

5.11.9 Configure External LDAP *(Optional)*

This procedure describes how to use a customer-provided authentication based on the Lightweight Directory Access Protocol (LDAP). This procedure is optional.

1. Open a terminal window and log in as root on the NSP server (One-box) or the Primary server (Four-box).

   Note: You need to run this procedure on only the Primary server for a Four-box NSP configuration.

2. Configure the NSP database. As root, run:
   ```
   # cd /opt/nsp/scripts/procs
   # sh nsp_update_procs.sh externalLDAP true
   ```

3. From a web brower, connect to the NSP application interface. Use the following URL:

   ```
   http://192.168.1.1/console
   ```

   where 192.168.1.1 is the IP address of the NSP server.

4. Log in to the WebLogic Console as weblogic.
5. Select **Security Realm ► myrealm ► Providers ► Authentication**.
6. Click **Lock&Edit** and add a new LDAP Authenticator.
   Provide the necessary parameters that correspond to the customer LDAP tree configuration (refer to the *WebLogic* documentation for more information about this process).
7. Set the control flag for all of the Authentication Providers to **SUFFICIENT.**
8. Click **Save.**
9. Click **Activate Configuration.**

5.11.10 Control Cisco PMP *(Optional)*

This procedure describes how to enable or disable the Cisco PMP. This procedure is optional.

1. Open a terminal window and log in as tekelec on the NSP server or the NSP Oracle server.
2. Run the appropriate commands:
   - To enable the Cisco PMP, run:
     ```
     # cd /opt/nsp/nsp-package/framework/db/dist/utils/cmd
     # sh PmpOption.sh -e
     ```
   - To disable the Cisco PMP, run:
     ```
     # cd /opt/nsp/nsp-package/framework/db/dist/utils/cmd
     # sh PmpOption.sh -d
     ```

5.11.11 Configure the default settings for the new users *(Optional)*

This procedure describes how configure the default settings for the new users. This procedure is optional.

1. Login on the NSP as user Tekelec
2. Modify the user preferences according the customer requirement and especially the Time Zone.
3. Validate the settings using the button “Save as default” for each panel you modified.

5.11.12 Configure CSV streaming feed feature *(Optional)*

This procedure describes how to enable or disable the CSV streaming feed feature: this feature is subject to subscription and it is disabled after installation.

1. Open a terminal window and log in as tekelec on the NSP server (1 box) or the NSP Primary server (4 box).
2. Run the appropriate commands:
   - To enable CSV streaming feed, run:
     ```
     # cd /opt/nsp/nsp-package/framework/core
     # ant enable.csv.license
     ```
   - To disable CSV streaming feed, run:
     ```
     # cd /opt/nsp/nsp-package/framework/core
     # ant disable.csv.license
     ```

5.11.13 Configure FSE automated update *(Optional)*

This procedure describes how to enable or disable the automatic update of enrichment configuration file defined or to be defined in NSP system.

NSP scan regurlarly defined folder and its subfolder (every 30 mn) to find files with same name as the those declared. In this case it loads file to replace exsiting FSE and reapply it automatically to selected session.

1. Log in as tekelec on the NSP application interface.
2. Select the **Centralized Configuration** application.
3. Select **Mediation ► Enrichment Files**.
   The Enrichment Files List screen opens
4. Click on automated update button in list toolbar  .
   The FSE Auto Update Configuration screen opens.
5. Enter SFTP location where system can find Enrichment FSE file.
   URL should be like *sftp://<USER>:<PASSWORD>@<HOSTNAME_OR_IP>/<PATH>* where
   - <*USER*> is username of SFTP server
   - <*PASSWORD*> is password of SFTP user
   - <*HOSTNAME_OR_IP*> is address of SFTP server
   - <*PATH*> is relative path under user home folder in SFTP server

   Note: Empty string turns off automated update

6. Click OK to validate changes.

Chapter
6

6 xMF Customer Integration

Topics:

- *Customer Network Configuration T1100, T1200, G5, G6* **and Gen8**
- *Configure Site and Subsystem for xMF*
- *xMF Healthcheck*
- **Error! Reference source not found.**

6.1 Customer Network Configuration T1100, T1200, G5, G6 and Gen8

Note: This procedure apply on T1100 only starting PIC 9.0.2 and above once the server is using TPD5 at least.

This procedure describes how to configure the customer network.

Before you perform this procedure, make sure you have read and are familiar with the *xMF Bulkconfig File Description*.

1. **Create the bulkconfig file**
   a) Open a terminal window and log in as root on the xMF server.
   b) Create the bulkconfig file.
   c) Verify the file is in the proper directory. As root, run:

      # **ls /var/TKLC/upgrade/platform.csv**

2. **Run the bulkconfig script**
   a) Run bulkconfig script **since the iLO** as root, run:

      # **bulkConf.pl**

      Example of correct output:

```
Name: imf-1a
        Func: IMF Desig: 1A Cust:
        bond0.2 00 HostIp: 192.168.253.5
        Mask: 255.255.255.224
        Route: 192.168.253.1
Updating hostname to imf-1a. LiveIP: 192.168.253.5...
NTP: ntpserver1
        Ip: 10.250.32.10
        Updating ntpserver1... NTP:
ntpserver2
        Ip: 10.250.32.11
        Updating ntpserver2... NTP:
ntpserver3
        Ip: 10.250.32.12
        Updating ntpserver3... NTP:
ntppeerA
        Ip: 10.250.32.13
        Updating ntppeerA... NTP:
ntppeerB
        Ip: 10.250.32.14
        Updating ntppeerB... APP:
appserver
        Ip: 10.10.10.10
        Adding new appserver... APP:
appserver2
        Ip: 10.10.10.11
        Adding new appserver... TZ:
Europe/Prague
        Updating Timezone America/New_York to Europe/Prague...
```

   b) Verify there are no errors in the script output. If an error occurs in the output contact the Tekelec Customer Care Center.

   c) Reboot the server.

6.2 Configure Site and Subsystem for xMF

This procedure describes how to create a site on NSP and set a subsystem in this new site.

The subsystem is treated by PIC as a cluster, accessible by NSP through this IP address.

A dedicated IP address, called Virtual IP (VIP), is needed for the subsystem. This address must be a real address in the subsystem subnet that is not physically used by any other server or equipment. The current Active Master server in the subsystem is the server representing the VIP.

For a standalone PMF, the VIP is the IP address of the PMF server. For a single-server IMF, it is possible to assign the server IP address as VIP; however, when additional servers are added, the VIP address must be changed to a dedicated IP address to work properly. It is recommended that a dedicated IP address be used from the beginning, to avoid changing the VIP when more servers are added.

Note: There is only one xMF subsystem supported per site. If a standalone PMF is in a site/subsystem, no other IMF or PMF subsystem or standalone PMF can be added. They need to be added to different logical site in **Centralized Configuration.** All of the configuration is performed through the NSP application interface.

1. Log in to the NSP application

a) Log in to the NSP application interface using the NSP Primary server IP address. a) Click **Centralized configuration.** The NSP application launches.

2. Create a site on NSP

a) Select **Equipment Registry ► Sites ► Add.**

b) Type the desired site name and click **Add.**

3. Add the server(s) on NSP

Note: Skip this step if the Site already exists.

a) Select **Equipment Registry ► Sites ►** ***New site name created*** **► XMF ► Add**
b) Type the server IP address(es) for the xMF subsystem and click **Add.**
c) Click **Create.**

4. Apply the changes on NSP

a) Select **Acquisition ► Sites ►** ***New site name created***
b) Expand the subsystem; then, right-click on embedded subsystem name and select **Apply changes.**
c) Click **Next** to see Configuration Changes.
d) Click **Next** to see Warnings.
e) Click **Apply Changes.**
f) Click **Yes** to confirm the change.

6.3 xMF Healthcheck

This procedure describes how to run the healthcheck script on xMF servers.

The script gathers the healthcheck information from each server in the xMF subsystem or from standalone server. The script should be run from only on one server of the XMF subsystem (the 1A server is preferred) or on stand-alone. The output consists of a list of checks and results, and, if applicable, suggested solutions.

1. Open a terminal window and log in as cfguser on any server in the xMF subsystem or standalone server.
2. Run the automatic healthcheck script.

$ **analyze_subsystem.sh**

3. Analyze the output of the script for errors. Issues reported by this script must be resolved before any further usage of this server. Verify no errors are present.

   If the error occurs, contact the Tekelec Customer Care Center.

   Note: For a standalone, there will be only one server in the output.

   Example output for a healthy subsystem:

```
ANALYSIS OF SERVER IMF0502-1A STARTED


11:28:59:     STARTING HEALTHCHECK PROCEDURE - SYSCHECK=0
11:28:59:     date:   02-07-11, hostname: IMF0502-1A TPD VERSION: 3.3.8-
11:28:59:     63.25.0 XMF VERSION:    [  60.6.7-2.1.0 ]
11:28:59:     Checking disk free space
11:28:59:     No disk space issues found
11:28:59:     Checking whether ssh keys are exchanged among machines in frame this
11:28:59:     can take a while
11:29:08:
11:29:08:     3 mates found: yellow-1B yellow-1C yellow-1D
11:29:26:     Connection to all mates without password was successful
11:29:26:     Checking A-Node server
11:29:29:     Connection to A-Node 10.240.9.4 was successful
11:29:29:     A-Node version is: 60.6.7-2.1.0
11:29:29:     Checking version of the nsp
11:29:32:     Connection to nsp 10.240.9.3 was successful
11:29:32:     nsp version is: 6.6.4-7.1.0
11:29:32:     nsp was installed on:   2011-01-13  05:09:26   (25 days 6 hours ago)
11:29:32:     All tests passed. Good job!
11:29:32:     ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1A

ANALYSIS OF SERVER IMF0502-1B STARTED


11:30:04: ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1B

ANALYSIS OF SERVER IMF0502-1C STARTED


11:30:36:     ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER IMF0502-1C

IMF0502-1A TPD: 3.3.8-63.25.0 XMF:   60.6.7-2.1.0 0 test(s) failed
IMF0502-1B TPD: 3.3.8-63.25.0 XMF:   60.6.7-2.1.0 0 test(s) failed
IMF0502-1C TPD: 3.3.8-63.25.0 XMF:   60.6.7-2.1.0 0 test(s) failed
```

   Example output for a subsystem with errors:

```
END OF ANALYSIS OF SERVER IMF0502-1D
IMF0502-1A TPD: 3.3.8-63.25.0 XMF: 60.6.7-2.1.0 1 test(s) failed
IMF0502-1B TPD: 3.3.8-63.24.0 XMF: 60.6.7-1.0.0 3 test(s) failed
server on interface yellow-1c is not accessible (ping)
IMF0502-1D TPD: 3.3.8-63.25.0 XMF: 60.6.7-2.1.0 0 test(s) failed
Differences between tpd platform versions found!
Differences between message feeder application versions found!
```

6.4 Optional: procedure to enable timestamp resolution to ns

This procedure describes how to enable/disable the timestamp resolution to ns on transport for IPRaw packet between PMF and IXP.

By default, this feature is disabled and the default timestamp resolution is the millisecond.

This feature can be activated separately for MFP or DTS transport protocol by the parameter 'TlvDsMask' inside the 'LongParam' table:

```
Yes|TlvDsMask|0|Set the XMF output interface mode (1-TLV_MFP_IP, 2-TLV_DTS_IP, 3-Both)
```

After modification of this parameter, the PMF must be restarted.

Remarks:

- A clobber on the XMF disable automatically this feature.

Chapter
7

7 IXP Customer Integration

Topics:

7.1 Integrate Customer Network (IXP)

This procedure describes how to integrate the IXP subsystem post-manufacturing customer network.

This procedure uses the /root/bulkconfig file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the *IXP Bulkconfig File Description*.

This procedure is run from the iLO.

For an estimated time for this procedure, refer to the IXP flowchart in *Integration Overview Flowcharts*.

1. **Update the bulkconfig file**
   a) Log in on the iLO of **any IXP xDR server** in the IXP subsystem that you want to reconfigure.
   Note: Be sure to log in on an xDR server and that all the IXP servers are up and running.
   b) Update the /root/bulkconfig file with the customer IP addresses and timezone.

2. **Run the customer network integration**
   a) Run the IXP subsystem customer network integration script. As root, run:

      ```
      # bc_customer_integration.sh
      ```

   b) Confirm this operation.

      Enter yes.

      A prompt for the root password appears.
   c) Provide the root password.
   The servers reboot.

3. **Run the post-integration settings**

   Note: The IXP server has new IP address. The previous addresses are no longer accessible.

   a) Run post-integration settings. As root, run:

      ```
      # bc_customer_integration.sh --post
      ```

      Note: The key exchange operation is part of this script.

      A prompt for the root and cfguser passwords appears.
   b) Provide the appropriate passwords.
   c) When the script is complete, check the terminal output for any errors. If the error occurs, contact the Tekelec Customer Care Center.

7.2 Add IXP Subsystem to CCM

This procedure describes how to add the IXP subsystem to the CCM on NSP. This

procedure is performed through the NSP application interface.
For an estimated time for this procedure, refer to the IXP flowchart in *Integration Overview Flowcharts*.

1. **Log in to the NSP and open Centralized Configuration (CCM)**
   a) Log in to the NSP application interface using the NSP Primary server IP address.
   b) Open the **Centralized Configuration** application.
   c) Select **Equipment Registry.**

2. **Configure the new site**
   a) Right-click the **Sites** list and select **Add** to enter new site configuration.
   b) Type the **Site name** and **Description** and click **Add.**

3. **Add the IXP subsystem to the site**
   a) Navigate to **Sites.**
   b) Right-click **IXP** and select **Add** to enter the IXP subsystem configuration.
   c) Type values for the following fields:
      - IXP subsystem name in **Subsystem Name**
      - Dedicated IP address for the IXP subsystem in **VIP Address.**

        Note: The Virtual IP (VIP) Address is an actual IP address in the same subsystem subnet that is not physically used by any other server or equipment. The subsystem is treated by NSP as a cluster accessible from NSP through this IP address.
      - IP address of the IXP server

        Note: The xDR storage server must be the first server added.

   d) Click **Add.**
   e) Repeat steps 3.b.-3.d for each server in the IXP subsystem.
   f) Verify that all of the added servers are listed in the **Locations** list.
   g) If the IXP subsystem is using an external DWS select the check box under the location list and than select the DWH to use. (This is assuming you use Oracle 11, so have 25 disk for the Storage)
   h) Click **Create.**
   Information is synchronized from the IXP servers to the NSP.

4. **Apply the configuration to the IXP subsystem**
   a) Navigate to **Mediation ► Sites.**
   b) Open **IXP.**
   c) Right-click the subsystem and select **Apply changes...**.
   d) Click **Next.**
   e) Click **Apply Changes.**

7.3 License DataFeed Host Server and activate feature

This procedure describes how to license the DataFeed host server on the NSP and how to activate the feature on the IXP server.

For an estimated time for this procedure, refer to the IXP flowchart in *Integration Overview Flowcharts*.

1. **Log in on the NSP Primary server and list the available hosts**
   a) Open a terminal window and log in as tekelec on the NSP Primary WebLogic server.
   b) List the available hosts and already licensed hosts. As tekelec, run:

```
$ cd /opt/nsp/scripts/datafeed
$ ./listLicencedHosts
```

   Example output:

```
*** Available hosts ***
Host id=528 ip address=10.0.0.10
Host id=13881 ip address=10.0.0.11
Host id=363 ip address=localhost
Host id=357 ip address=192.168.1.10
Host id=21255 ip address=192.168.1.11
*** Licenced hosts ***
Host id=528 ip address=10.0.0.10
Host id=13881 ip address=10.0.0.11
```

c) Make a list of the IXP IDs of all hosts that you want to license and those that have not been licensed yet.

2. License DataFeed host

As tekelec, run:

```
$  ./licenceHost hostID
```

where *hostID* is the host ID of the DataFeed host that was provided as a result of the previous step ./listLicencedHosts command.

Example output:

```
[tekelec@nsp scripts]# ./licenceHost 357
* Host with HOST_ID=357 was successfully licenced
```

3. Log in on the DataFeed host (IXP server) and activate the DataExport process

a) Open a terminal window and log in as cfguser on the IXP server.

b) As cfguser, run:

```
$ setDataExport.sh on
```

Example output:

```
Former state:
Testing DataExport IDB .................. ok
Testing DataExport under PM ............. not exists
Testing DataExport service .............. off
Current state:
(please be patient, it can take some time)
Testing DataExport under PM ............. exists
Testing DataExport service .............. on

DONE.
```

The final result should be successful (**DONE**); the current state (or former state, if DataExport was already active) should show the DataExport service as **existing** and **on**.

7.4 Install xDR Builders

This procedure describes how to trigger the xDR Builders installation on the IXP subsystem from the CCM.

1. Log in on the NSP Primary server and insert the xDR DVD/CD or copy the ISO file

a) Open a terminal window and log in on the NSP Primary Weblogic server.

b) Insert the xDR Builders DVD/CD or copy the xDR Builder ISO file to the NSP Primary Weblogic server.

2. Run the install script

a) As root, run:

```
# cd /opt/nsp/scripts/oracle/cmd
# ./install_builders.sh
```

The following prompt appears:

```
Please enter path to Builder CDROM or ISO [/media/cdrom]
```

b) Enter the appropriate response based on the media used:

- For a DVD/CD, press **Enter.**
- For an ISO file, enter the exact path including the ISO file name.

c) Wait until the installation is complete.

3. Verify the ISO installation on NSP

a) Open a web browser and log in as TklcSrv on the NSP application interface.
b) Open the **Upgrade Utility.**
c) Click **Manage Builder Rpm** in the left tree.
A list of xDR Builder RPMs appears. The ISO file installed in the previous step is on this list, with a state **Not Uploaded.**

4. Upload Builders RPM

a) Select the desired xDR Builder RPM with the **Not Uploaded** state and click **Upload.** A confirmation window appears.
b) Click **Continue** to continue the RPM upload.
If the upload is successful, then the RPM state changes to **Uploaded.** If the upload fail contact the Tekelec Customer Care Center.

5. Associate the xDR Builders RPM with the IXP subsystem

a) Click **View Builder RPM Status** in the left tree. A list of the IXP subsystems appears.
b) Select one or more IXP subsystems and click **Associate RPM Package.** A list of Builder RPMs that are uploaded in NSP appears.
c) Select the appropriate xDR Builder RPM and click **Associate.**
If the association is successful, then the list of the subsystems is updated. The **RPM Name** column contains the new RPM package name and **Association Status** is marked as **OK.** If the association fails contact the Tekelec Customer Care Center.

6. Apply the configuration to the IXP subsystem

a) Return to the main page of the NSP application interface.
b) Open the **Centralized Configuration** application.
c) Navigate to **Mediation.**
d) Open **Sites** and open the site; then, open **IXP.**
e) Right-click the subsystem and select **Apply changes...**.
f) Click **Next.**
g) Click **Apply Changes.**
h) When change is complete, verify there are no errors on the result page.

7. Install the xDR Builders RPM on IXP

a) Return to the main page of the NSP application interface.
b) Open the **Upgrade Utility.**

c) Click **View Builder RPM Status** in the left tree.
The available IXP subsystem with their respective RPM Associate Status and Install Status appears.

d) Before initiating the builder installation, make sure the **Builder RPM** that you want to install on the IXP subsystem is associated with the IXP subsystem as indicated by **RPM Name** column and **Association Status** marked as **OK.** Also, **Install Status** should contain either **-** or **No Started.**

e) Select one or more IXP subsystems and click **Install RPM Package.** If the installation is successful, the **Install status** changes to **OK.** If the installation fails contact the Tekelec Customer Care Center.

7.5 xDR Builders Licensing

This section describes how to generate and apply the xDR builders license key.

7.5.1 Use IXP Site Code to generate xDR Builder License Key

This procedure describes how to use the valid IxpSubsystemKey.data file from the IXP subsystem to generate the xDR Builder license key.

Note: The IxpSubsystemKey.data file is generated on the IXP Active Master server after the IXP subsystem is configured or the server is added to the IXP subsystem.

1. **Locate the latest site code file**

a) Open a terminal window and log in cfguser on the IXP Active Master server.

b) Locate the IxpSubsystemKey.data file in the /home/cfguser/ directory.

As cfguser, run:

$ ls -l

A list of files appears. The IxpSubsystemKey.data must be included on this list.

c) Check the timestamp of the file. If the file is older than the time when the last server has been added to the subsystem or if the file is missing, regenerate the file.

As root, run:

 # service TKLCixp restart

d) Locate the IxpSubsystemKey.data file in the /home/cfguser/ directory again.

As cfguser, run: **$ ls**

-l

The list of files must contain the correct IxpSubsystemKey.data file.

2. **Send an email with a request to receive the license key file**

Copy the IxpSubsystemKey.data file to a machine with an email access; then, send the file, along with a copy of the purchase order where the license part numbers are mentioned, to the following address: cssg.product.license.request@tekelec.com

7.5.2 Install xDR Builder License Key

This procedure describes how to install the xDR license key file on the IXP Active Master server.

Note: The xDR license key file (IxpLicenseKey.data) is attached to the response to the license request email.

1. **Transfer the license file to the IXP Active Master server**
   a) Open a terminal window and log in as cfguser on the IXP Active Master server.
   b) Copy the IxpLicenseKey.data file to the IXP Active Master server to /home/cfguser/ directory.
2. **Activate license**

   As soon as the file has been detected and verified, the existing temporary license alarm(s), if any, is automatically cleared.
3. **Verify license installation**
   a) Log in as cfguser on the IXP Active Master server.
   b) Run:

      $ IxpCheckLicense

   c) Verify the output.

      The information about the license should state that license is valid and that license type is not STARTUP. If the license type is STARTUP contact the Tekelec Customer Care Center.

7.6 IXP Subsystem Healthcheck

This procedure describes how to run the automatic healthcheck of the IXP subsystem.

1. Open a terminal window and log in on any IXP server in the IXP subsystem you want to analyze.
2. As cfguser, run: $

   analyze_subsystem.sh

   The script gathers the healthcheck information from all the configured servers in the subsystem. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

   The following examples show the structure of the output, with various checks, values, suggestions, and errors.
   Example of overall output:

```
[cfguser@ixp2222-1a ~]$ analyze_subsystem.sh ANALYSIS OF

SERVER ixp2222-1a STARTED

10:16:05:   STARTING HEALTHCHECK PROCEDURE  - SYSCHECK=0
10:16:05: date: 05-20-11, hostname: ixp2222-1a
10:16:05:   TPD VERSION: 4.2.3-70.86.0 10:16:05:   IXP
VERSION:    [7.1.0-54.1.0]
10:16:05: XDR BUILDERS VERSION:  [7.1.0-36.1.0]
10:16:05:       --
10:16:05:       Analyzing server record in /etc/hosts
10:16:05:                   Server ixp2222-1b properly reflected in /etc/hosts file
10:16:05:       Analyzing IDB state
10:16:05:       IDB in START state

12:21:48: Analyzing disk usage

10:24:09:   ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp2222-1b

ixp2222-1a TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ] 0
test(s) failed
ixp2222-1b TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ] 0
```

test(s) failed

Example of a successful test:

10:24:08: Analyzing DaqServer table in IDB

10:24:08: Server ixp2222-1b reflected in DaqServer table

Example of a failed test:

12:21:48: Analyzing IDB state
12:21:48: >>> Error: IDB is not in started state (current state X) 12:21:48: >>> Suggestion: Verify system stability and use 'prod.start' to start the product

7.7 IXP Post-Integration Configuration (Optional)

This section contains various optional post-integration configuration procedures.

7.7.1 DataBroker and CSV streaming feeds

This procedure describes how to integrate a DataBroker server into an IXP subsystem. Data Broker streaming feeds write files on customer servers providing NFS shared directories.

That same procedure is to be followed to integrate a CSV server into an IXP subsystem; such a server is used by the CSV streaming feed feature to store CSV files on a server that is not part of an IXP subsystem.

Note: For the CSV streaming feed feature, instead of using a dedicated server provided by the customer, it is possible to use a PDU server which is part of the current IXP subsystem or which is part of another IXP subsystem (as long as all the servers are in the same LAN).

Note: The following procedures describe how to setup shared directories using the NFS v3 protocol; it may be possible to use NFS v4, but the commands to execute are not described here (you should refer to linux and NFS documentation to learn how to use NFS v4 protocol).

1. **Configure the shared directory on the sharing server**

   a) Select an existing directory or already mounted local file system in which the exported files will be stored.

   b) Update the exports file. As root, execute:

      If the server uses a versioning system like rcstool, first check out the file:

      ```
      # rcstool co /etc/exports
      ```

      Edit /etc/exports and add this line (<path_to_share> is the directory or path to file system to share, <ip_ixp_export> is the IP address of an IXP server); add as many lines as IXP servers that will remotely access this shared directory

      ```
      <path_to_share>  <ip_ixp_export>(rw,sync,anonuid=-1)
      ```

      If needed, check in the file:

      ```
      # rcstool ci /etc/exports
      ```

   c) Restart the NFS services. As root execute:

      ```
      # chkconfig --levels 345 nfs on
      # service portmap restart
      # service nfs restart
      ```

2. **Mount the shared directory on IXP side**

Note: These steps are to be executed on each IXP server that will remotely access the shared directory of the sharing server.

a) Create the mount point. As root, execute:

```
# mkdir /var/TKLC/ixp/StoreExport
# chown cfguser:cfg /var/TKLC/ixp/StoreExport
```

b) Update the fstab file. As root, execute:

```
# rcstool co /etc/fstab
```

Edit /etc/fstab and add this line (<ip_server_nfs> is the IP address of the sharing server)

```
<ip_server_nfs>:<path_to_share>  /var/TKLC/ixp/StoreExport nfs
rw,rsize=32768,wsize=32768,soft 0 0
# rcstool ci /etc/fstab
# mount -all
```

c) Restart the NFS services. As root execute:

```
# chkconfig --levels 345 nfs on
# service portmap restart
# service nfs restart
```

7.7.2 Delivery Network Failure and Recovery (DataBroker)

This application shall be available 24 hours a day, seven days per week, except for minimal downtime due to planned production maintenance.

Note: Even if this procedure is applicable to all the IXP servers, it is not recommended to apply it for other purposes than DataBroker streaming feed, for which only it has been tested.

1. Configure IDB to extend 24 hours of xDRs can be kept in the DTS buffers

As cfguser on IXP primary , run:

```
# IxpExtendDataBroker24hrs.sh
```

Result with 3 IXP servers:

```
Testing host is primary ..................
Host is primary
Testing user is cfguser ..................
User is cfguser
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1b    === changed 1 records ===
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1c    === changed 1 records ===
Update DtsBlockPart - KeepTime to 24 hours from ixp7601-1a    === changed 1 records ===
```

7.7.3 Activate Session Compression

This procedure describes how to activate/deactivate compression for a particular Oracle session.

Before performing this procedure be aware of the following facts:

- Activated compression will have negative influence on storage speed rate.
- Activated compression will have negative influence on ProTrace queries speed rate.
- Activated compression will have positive influence on storage size.

- All current benchmark tests have been tested with deactivated compression.

Note: Execute this procedure on all IXP xDR Storage servers in IXP xDR Storage Pool where the session is located.

1. **Login to the IXP xDR Storage server**
   a) Open a terminal window and log in to the IXP xDR Storage server as cfguser.
   b) Navigate to /opt/TKLCixp/prod/db/tuning/cmd directory. As cfguser run:
   $ cd /opt/TKLCixp/prod/db/tuning/cmd

2. **How to activate the compression**
   a) To activate compression for particular session as cfguser run: $
   ./TuningPackage.sh ixp/ixp@localhost/ixp -c *session*
   where *session* is the name of particular session.

3. **How to deactivate the compression**
   a) To deactivate compression for particular session as cfguser run: $
   ./TuningPackage.sh ixp/ixp@localhost/ixp -x *session*
   where *session* is the name of particular session.

4. **Verify the settings**
   a) Verify the session list where the session compression is activated. As cfguser run: $
   ./TuningPackage.sh ixp/ixp@localhost/ixp -l
   All session with activated compression will be listed in the command output.

7.7.4 Change Default Passwords of Oracle Accounts

This procedure describes how to modify the default passwords of the Oracle account. This procedure is applicable to any xDR storage server in the subsystem.

1. **Connect as database administrator**
   a) Log in on the xDR storage server.
   b) Connect to Oracle as the database administrator. As the oracle user, run: $
   sqlplus / as sysdba

2. **Set passwords**
   a) Set the password for DBSNMP. Run:
   SQL> **alter user DBSNMP identified by *password;***
   where *password* is actual password.
   b) Set the password for OUTLN. Run:
   SQL> **alter user OUTLN identified by *password;***
   where *password* is the actual password.
   c) Set the password for SYSMAN. Run:
   SQL> **alter user SYSMAN identified by *password;***
   where *password* is the actual password.

3. **Close the Oracle session**

   Exit the Oracle session. Run:

   SQL> **exit;**

Chapter
8

8 EFS Customer Integration

Topics:

8.1 Integrate Customer Network (EFS)

This procedure describes how to integrate the EFS post-manufacturing customer network.

This procedure uses the /root/bulkconfig file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the *EFS Bulkconfig File Description*.

This procedure is run from the iLO.

For an estimated time for this procedure, refer to the EFS flowchart in *Integration Overview Flowcharts*.

1. **Update the bulkconfig file**

   a) Log in on the iLO of the EFS server that you want to reconfigure.
   b) Update the /root/bulkconfig file with the customer IP addresses and timezone.

2. **Run the customer network integration**

   a) Run the EFS customer network integration script. As root, run:

      # bc_customer_integration.sh

   b) Confirm this operation.

      Enter yes.

      A prompt for the root password appears.

   c) Provide the root password.
      The servers reboot.

3. **Run the post-integration settings**

   Note: The EFS server has new IP address. The previous address is no longer able to be accessed.

   a) Log in to EFS server that was integrated into the customer network.
   b) Run post-integration settings. As root, run:

      # bc_customer_integration.sh --post **Note:** The key exchange

      operation is part of this script.

      A prompt for the root and cfguser passwords appears.

   c) Provide the appropriate passwords.
   d) When the script is complete, check the terminal output for any errors. If the error occurs, contact the Tekelec Customer Care Center.

8.2 Add Standalone EFS to CCM

This procedure describes how to add the standalone Export File Server (EFS) to the CCM on NSP. This procedure is performed through the NSP application interface. For an estimated time for this procedure, refer to the EFS flowchart in *Integration Overview Flowcharts*.

1. **Log in to the NSP and open Centralized Configuration (CCM)**
   a) Log in to the NSP application interface using the NSP Primary server IP address.
   b) Open the **Centralized Configuration** application.
   c) Select **Equipment Registry.**
2. **Configure the new site**
   a) Right-click the **Sites** list and select **Add** to enter new site configuration.
   b) Type the **Site name** and **Description** and click **Add.**
3. **Add the EFS subsystem to the site**
   a) Navigate to **Sites.**
   b) Right-click **EFS** and select **Add** to enter the EFS subsystem configuration.
   c) Type the EFS subsystem name into the **Subsystem Name** field.
   d) Type in the IP address of the standalone EFS.
   e) Click **Add.**
   f) Click **Create.**
   Information is synchronized from the standalone EFS to the NSP.
   g) Verify that there are no errors on the result page that will display. If there are any errors contact the Tekelec Customer Care Center.

8.3 EFS Healthcheck

This procedure describes how to run the automatic healthcheck of the EFS.

1. Open a terminal window and log in as cfguser on the EFS server you want to analyze.
2. As cfguser, run:

   $ **analyze_subsystem.sh**

   The script gathers the healthcheck information from all the configured servers in the subsystem. A list of checks and associated results is generated. There might be steps that contain a suggested solution. Analyze the output of the script for any errors. Issues reported by this script must be resolved before any further use of this server.

   The following examples show the structure of the output, with various checks, values, suggestions, and errors.

   Example of overall output:

```
 [cfguser@ixp2222-1a ~]$ analyze_subsystem.sh
10:16:05:   ANALYSIS OF SERVER ixp2222-1a STARTED
10:16:05:   STARTING HEALTHCHECK PROCEDURE-SYSCHECK=0 date:05-20-11, hostname: ixp2222-1a
10:16:05:   TPD VERSION: 4.2.3-70.86.0
10:16:05:   IXP VERSION:    [  7.1.0-54.1.0 ]
10:16:05:   XDR BUILDERS VERSION:  [ 7.1.0-36.1.0 ]
10:16:05:
10:16:05:   Analyzing server record in /etc/hosts
10:16:05:   Server ixp2222-1b properly reflected in /etc/hosts file
10:16:05:   Analyzing IDB state
10:16:05:   IDB in START state
12:21:48:   Analyzing disk usage
10:24:09:   ENDING HEALTHCHECK PROCEDURE WITH CODE 0
END OF ANALYSIS OF SERVER ixp2222-1b
ixp2222-1a TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ]
0 test(s) failed
ixp2222-1b TPD:[ 4.2.3-70.86.0 ] IXP:[ 7.1.0-54.1.0 ] XB:[ 7.1.0-36.1.0 ]
0 test(s) failed
```

Example of a successful test:

```
10:24:08: Analyzing DaqServer table in IDB
10:24:08:         Server ixp2222-1b reflected in DaqServer table
```

Example of a failed test:

```
12:21:48: Analyzing IDB state
12:21:48: >>> Error:   IDB is not in started state (current state X) 12:21:48: >>>
Suggestion: Verify system stability and use 'prod.start' to start the product
```

8.4 Integrate Standalone EFS with IXP Subsystem

This procedure describes how to integrate the standalone EFS with the IXP subsystem.

The standalone EFS is not part of the IXP subsystem. This procedure is applicable to an IXP subsystem with Data Export hosts. Run this procedure on a single server per IXP subsystem.

1. **Log in on the IXP server and add standalone EFS to the bulkconfig file**
   a) Log in as root on any IXP server in the IXP subsystem with Data Export hosts that are supposed to export data to requested EFS.
   b) Update the IXP subsytem /root/bulkconfig file. Add the following line:

   efs,*hostname_of_EFS*,*IP_address_of_EFS* where:

   - *hostname_of_EFS* is the hostname of the standalone EFS
   - *IP_address_of_EFS* is the IP address of the standalone EFS

   For example:

   efs,ixp77 77-1e,10.236.0.33

2. **Adjust the IXP subsystem**

   As root, run:

   # **bc_adjust_subsystem.sh**

   Verify command line output for eny errors. If an error occurs contact the Tekelec Customer Care Center.

   Note: The standalone EFS is added to /etc/hosts for all of the IXP servers in the subsystem and all of the IXP servers in the subsystem are added to the /etc/hosts on the standalone EFS.

Chapter

9 RSP Customer Integration

Topics:

9.1 Integrate Customer Network (RSP)

This procedure describes how to integrate the RSP post-manufacturing customer network.

This procedure uses the /root/bulkconfig file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the *IXP Bulkconfig File Description*.

This procedure is run from the iLO.

For an estimated time for this procedure, refer to the RSP flowchart in *Integration Overview Flowcharts*.

1. **Update the bulkconfig file**

   a) Log in on the iLO of the RSP server that you want to reconfigure.
   b) Update the /root/bulkconfig file with the customer IP addresses and timezone.

2. **Run the customer network integration**

   a) Run the RSP customer network integration script. As root, run:

      # bc_customer_integration.sh

   b) Confirm this operation.

      Enter yes.

      A prompt for the root password appears.

   c) Provide the root password.
      The servers reboot.

3. **Run the post-integration settings**

   Note: The IXP server has new IP address. The previous addresses are no longer accessible.

   a) Log in to RSP server that was integrated into the customer network.
   b) Run post-integration settings. As root, run:

      # bc_customer_integration.sh --post

      # **Note:** The key exchange operation is part of this script.

      A prompt for the root and cfguser passwords appears.

   c) Provide the appropriate passwords.
   d) When the script is complete, check the terminal output for any errors. If the error occurs, contact the Tekelec Customer Care Center.

9.2 Configure E-mail SMTP Destination for Reports *(Optional)*

1. **Log in on the Central Management Console (CMC)**

   Log in as Administrator on the CMC, if not already logged in.

2. **Check Help for details**

   a) Click **Help.**

b) Select **Managing and Configuring Servers ► Configuring server settings ► Configuring destinations for job servers** for details.
c) Click **Help.**
d) Select **Scheduling Objects ► Setting the scheduling objects ► Selecting a destination ► Email (SMTP) support** for details.

9.3 Configure FTP Destination for Reports *(Optional)*

This procedure describes steps to configure an FTP destination for reports.

1. **Log in on the Central Management Console (CMC)**

   Log in as Administrator on the CMC, if not already logged in.

2. **Check Help for details**
   a) Click **Help.**
   b) Select **Scheduling Objects ► Setting the scheduling objects ► Selecting a destination ► FTP support** for details.

9.4 Add User for ReportInfoView Portal Access (Optional)

Default Tekelec user will be able to access the ReportInfoView portal, however if you want to create more user to be able to access ReportInfoView, please follow this procedure.

1. NSP: create a new user and assign a profile
   a) Open a web browser and log in to NSP application interface as tekelec.
   b) Go to Security Portal and create a new user.
   c) Assign a profile listed in the first column of the NSP Profile table.
   d) Confirm changes.
2. CMC: load a new user
   a)
   a) Log in on th eCentral Management Console (CMC) as iasadmin
   b) Click on **Users and Groups.**
   c) Click on **Create New User.**
   d) Select the **LDAP** authentication type and check Connection Type **Named User**
   e) Into **Account Name** enter the user you have created in the first step.
   f) Click on **Create & Close**
   g) Remove unused users such as NSPInternal and TklcSrv to free up some named license.

9.5 Discover RDS/RS/CMS Servers in CCM

This procedure describes how to discover the RDS, RS, and CMS servers on NSP.

In the 9.0 Report Server Platform architecture, there can be a Primary, Cluster, and multiple RDS machines that comprise the Report Server Platform. After the Report Server 9.0 has been installed, all of these servers contained in the Report Server Platform need to be discovered on the NSP.

The discovery of Report Server components needs to be accomplished in a specific order; consequently, the procedure must be run in this order:

- Any RDS (Report Data Server, database only) component—application type is RDS.
- Cluster Report Server—application type is RS.
- Primary Report Server—application type is RS.
- CMS (SAP Change Management System), if different from the Primary—application type is CMS.

Each of these components must to be installed as standalone IXP servers with the designation if **1A** and such each of the servers must be discovered as separated subsystem. When the CMS is discovered, all of the Report Packages that are installed on the Report Server Platform will also be discovered. There need to be one report package installed at least.

Once all of the Report Server components and Report Packages have been discovered, the ReportAdmin application can be used to configure and work with the Report Packages. The configuration of the ReportAdmin with each ReportPackage will be documented with the *Install Manual* that is released with each Report Package.

For an estimated time for this procedure, refer to the Report Server Platform flowchart in *Integration Overview Flowcharts*.

1. Log in to the **NSP** application interface.
2. Open the **Centralized Configuration** application.
3. Select **Equipment Registry ► Sites ► NOC.**
4. Right-click **Report Server** and click **Add.**
5. Type the **Subsystem Name** and **IP Address** and click **Add.**
6. Click **Create.**
7. Repeat the steps 5 and 6 for each RS that need to be discovered in the order described at the beginning of the procedure
8. For any other additional report package installed on the Report Server after this discovery user need to perform a separated Discover Application operation in Centralized Configuration (CCM). In such case navigate to **Equipment Registry ► Sites ► NOC ► Report Server ► *subsystem_name*** and click on **Discover Applications** icon in a toolbar.

9.6 Discover PPS application in CCM

This procedure describes how to discover the PPS application on NSP. PPS is used when TDM Voice Analytics are implemented in the system.
The PPS application is installed as a part of the IXP subsystem and, consequently, the PPS application discovery is part of the IXP subsystem discovery. The method used to discover the PPS application depends on when it was installed:

- If PPS is installed ***before*** the IXP subsystem is discovered in CCM, then PPS is discovered along with the IXP subsystem, *Add IXP Subsystem to CCM*. No additional operation is required here.

  —OR—

- If PPS is installed ***after*** the IXP is discovered in CCM, then the IXP server that contains the PPS application needs to be rediscovered.

If PPS is installed ***after*** the IXP is discovered in CCM, then perform this procedure.

1. Log in to the **NSP** application interface.

2. Open the **Centralized Configuration** application.
3. Select **Equipment Registry ► Sites ► *Site* ► IXP ► *IXP subsystem.***
4. Select the host on which PPS is installed and click **Discover Applications** to synchronize the host.

9.7 Configure ReportInfoView Web Application on NSP

This procedure describes how to verify the ReportInfoView Web Application is running on NSP and how to configure the starting page.

For an estimated time for this procedure, refer to the RSP flowchart in *Integration Overview Flowcharts*.

1. Log in to ReportInfo View application

a) Log in as tekelec on the NSP application interface.
b) Click **ReportInfoView.**

2. Configure the starting page

a) Select **Preferences.**
b) Configure the starting page according to requirements.

Chapter 10

10DWS Customer Integration

Topics:

10.1 Integrate Customer Network (DWS)

This procedure describes how to integrate the DWS post-manufacturing customer network.

This procedure uses the /root/bulkconfig file as an input for the customer network integration. Before you perform this procedure, make sure you have read and are familiar with the *IXP Bulkconfig File Description* (be sure to check steps dedicated to DWS).

This procedure is run from the iLO.

For an estimated time for this procedure, refer to the DWS.flowchart in *Integration Overview Flowcharts*.

1. **Update the bulkconfig file**
   a) Log in on the iLO of **DWS** that you want to reconfigure.
   b) Update the /root/bulkconfig file with the customer IP addresses and timezone.

2. **Run the customer network integration**
   a) Run the IXP subsystem customer network integration script. As root, run:

```
# bc_customer_integration.sh
```

   Note: in case the following error message is displayed, check and fix /root/bulkconfig file (refer to *IXP Bulkconfig File Description*, steps dedicated to DWS). Verify the syntax of the *host* line (some fields might have been inverted).

```
# bc_customer_integration.sh
Incorrect syntax of record [ host,ixp...
Check and correct the /root/bulkconfig, ending procedure
```

   b) Confirm this operation.
   Enter yes.
   A prompt for the root password appears.
   c) Provide the root password.
   The servers reboot.

3. **Run the post-integration settings**

   Note: The DWS has new IP address. The previous addresses are no longer accessible.

   a) Run post-integration settings. As root, run:

```
# bc_customer_integration.sh --post
```

   Note: The key exchange operation is part of this script.

   A prompt for the root and cfguser passwords appears.
   b) Provide the appropriate passwords.
   c) When the script is complete, check the terminal output for any errors. If the error occurs, contact the Tekelec Customer Care Center.

4. **Finalize the DWS conversion**

   Note: At this step, the formerly existing IXP xDR server is turned into a DWS (avoiding it to be recognized from the NSP as an IXP xDR server).

   a) Run conversion command. As cfguser, run:

```
$ makeDWH.sh
```

A prompt for the root password will appear: type in the root password (input is not visible).

A prompt for the NSP Primary IP address may appear: enter the correct IP address (not a host name) of the NSP Primary (in case of a 4 box NSP) or of the NSP server (in case of a 1 box NSP).

10.2 Add DWS to CCM

This procedure describes how to add the DWS to the CCM on NSP. This procedure is performed through the NSP application interface.

For an estimated time for this procedure, refer to the DWS flowchart in *Integration Overview Flowcharts*.

1. **Log in to the NSP and open Centralized Configuration (CCM)**
   a) Log in to the NSP application interface using the NSP Primary server IP address.
   b) Open the **Centralized Configuration** application.
   c) Select **Equipment Registry.**
2. **Configure the new site**
   a) Right-click the **Sites** list and select **Add** to enter new site configuration.
   b) Type the **Site name** and **Description** and click **Add.**
3. **Add the DWS to the site**
   a) Navigate to **Sites.**
   b) Right-click **DWH** and select **Add** to enter the DWS configuration.
      - Fill the DWS server hostname into the **Storage Name** field.
      - Fill the **Login user Id** (IXP by default)
      - Fill the **Password** (refer to TR006061 for the default value of the “Oracle IXP” password)
      - Fill the **Service Name** (IXP by default)
      - Fill in the **IP address** of the DWS.
   c) Click **Add.**

11Key exchange procedure with Neptune probe

This procedure must be applied after a fresh install or upgrade of the Neptune probe.
It must applied on NSP servers for NSP 1 box and on both Primary WebLogic and Secondary WebLogic servers in case of NSP 4 boxes

These are the steps to follow (**step 2 and 3 must be run for each Neptune probe**)

1. Loggin as root on the NSP server
2. Create the file containing the key
    a. Run the command : ***/usr/TKLC/nsp/nsp-package/proadmin/scripts/retreive-cert.sh x.x.x.x > /tmp/neptune.crt***
    b. x.x.x.x is the administration IP address of the Neptune probe
3. Import of the key
    a. Run the command : ***WL_HOME=/usr/TKLC/nsp/bea/wlserver_10.3***
    b. Run the command *:* ***keytool -import -trustcacerts -alias x.x.x.x -file /tmp/neptune.crt -keystore $WL_HOME/server/lib/DemoTrust.jks***
        i. x.x.x.x is the administration IP address of the Neptune probe
        ii. *For* Password : enter the value defined in TR006061 for “Neptune SSH Key”
        iii. Answer ***Yes*** when it is asking if the certificate is reliable
4. Restart the server
    a. In case of NSP 4 boxes, the following command must be run only when the steps below were applied on all WL servers
    b. Run the command (for NSP 4 boxes, run this command only on the Primary WebLogic server): ***service nspservice restart***

Remark *:* If the certificate is already present, the import must be deleted.
For deleting the import

1. Run the command *:* ***keytool -delete –keystore /usr/TKLC/nsp/bea/wlserver_10.3/server/lib/DemoTrust.jks -storepass DemoTrustKeyStorePassPhrase -alias*** **x.x.x.x** **(x.x.x.x** is the administration IP address of the Neptune probe)
2. Remove the file Neptune.crt under /tmp
3. Rerun import (step 2 above)

12PIC Bulkconfig File Description

Topics:

This section provides the bulkconfig file descriptions for PIC application components.

12.1 NSP Bulkconfig File Description

The NSP subsystem bulkconfig file contains the overall NSP pre-installation configuration information, most importantly the hostname and SNMP configuration. During the installation process, various scripts use this file to configure NSP.

The bulkconfig file is a text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The bulkconfig file templates can be found on the NSP iso in the / directory. For NSP One-Box you can use the /bulkconfig.nsp-onebox template together with the /bulkconfig.example.nsp-onebox example showing an updated bulkconfig template. Do not use this reference example to configure the NSP system. For NSP Four-Box you can use the /bulkconfig.nsp-fourbox template together with the /bulkconfig.example.nsp-fourbox example.

Note: When you install PIC, you are asked to create this bulkconfig file and update this file. **DO NOT** remove the NSP bulkconfig file from the server.

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Note: If the bulkconfig file is copied form ISO and moved to the /root , the permission will be Read-only. In this case change the rights to match the example below.

```
[root@nsponebox~]# pwd /root
[root@nsponebox ~]# ls -l  |  grep bulkconfig
-rw-r--r--  1 root root      358 Dec    4  19:20 bulkconfig
```

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

host,*hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway*
ntpserver1,*IP_address*
ntpserver2,*IP_address*
timezone,*time_zone*

Refer to the following descriptions of each keyword and its associated values.

host Description

host,*hostname_of_server,IP_address,function, interface_name,network_mask,network_gateway*

Example (Four-Box Configuration):

host,nsp-apache,10.236.2.141,NSP_APACHE,eth01,255.255.255.224,10.236.2.129

host,nsp-apache,10.236.1.141,NSP_APACHE,eth02,255.255.255.224,10.236.1.129
host,nsp-oracle,10.236.2.142,NSP_ORACLE,eth01,255.255.255.224,10.236.2.129
host,nsp-secondary,10.236.2.143,NSP_SECONDARY,eth01,255.255.255.224,10.236.2.129
host,nsp-primary,10.236.2.144,NSP_PRIMARY,eth01,255.255.255.224,10.236.2.129...

There is single host line for each server except for the NSP Apache.

The host keyword has the following associated values:

hostname_of_server A valid hostname , it should match the hostname set on server.

IP_address The IP address of the server. For blade systems, the internal IP address of the server.

function The function of the server. Use one of the following entries:

- NSP_ONEBOX for the NSP One-box Server
- NSP_APACHE for the NSP Apache Server
- NSP_ORACLE for the NSP Oracle Server
- NSP_SECONDARY for the NSP Secondary Server
- NSP_PRIMARY for the NSP Primary Server

interface name Name of the interface where the network settings are applied.

- Use eth01 for a rackmount system and eth02 for the second interface on Apache and One-box servers.
- Use bond0.3 for the blade systems and bond0.4 for the second interface on Apache and One-box servers.

network_mask The network mask.

network_gateway The default gateway.

ntpserver Description

ntpserver1,*IP_address*
ntpserver2,*IP_address*

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server

Example:

ntpserver1,10.236.129.11
ntpserver2,

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

timezone Description

timezone,*time_zone*

Example:

timezone,Europe/Prague

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab --CUT--
#code      coordinates                 TZ comments
```

```
AD      +4230+00131     Europe/Andorra
AE      +2518+05518     Asia/Dubai
AF      +3431+06912     Asia/Kabul
AG      +1703-06148     America/Antigua
CZ      +5005+01426     Europe/Prague
-----CUT—
```

NSP One-box bulkconfig

Template

host,*hostname_of_server,IP_address,function, interface_name,network_mask,network_gateway*
host,*hostname_of_server,IP_address,function,interface_name,network_mask,network_gateway*
ntpserver1,*IP_address*
ntpserver2,*IP_address*
timezone,*time_zone*

Example:

A bulkconfig file needs to be created for the NSP One-box:

- Server hostname: nsp-onebox
- Because it is a one-box server, two interfaces are needed
- Because it is a rackmount system, use eth01 and eth02 for these interfaces

  Note: If you are configuring C-class blades, replace eth01 with bond0.3 and eth02 with bond0.4 when you create this file.

- IP addresses:
  - First interface (eth01): 10.236.2.141
  - Second interface (eth02): 10.236.1.141
- Subnet mask: 255.255.255.254
- Gateway addresses:
  - First interface (eth01): 10.236.2.12 9
  - Second interface (eth02): 10.236.1.129
- NTP server IP address: 10.236.129.11
- Server timezone: Europe/Prague

The corresponding bulkconfig file you create should appear as follows: **Note:** There is no new line character in the middle of the host configuration.

```
 [root@nsp-onebox ~]# cat /root/bulkconfig
host,nsp-onebox,10.236.2.141,NSP_ONEBOX,eth01,255.255.255.224,10.236.2.129
host,nsp-onebox,10.236.1.142,NSP_ONEBOX,eth02,255.255.255.224,10.236.1.129
ntpserver1,10.236.129.11
ntpserver2,
timezone,Europe/Prague
```

NSP Four-box bulkconfig

Template

host,*hostname_apache,IP_address,function,interface_name,network_mask,network_gateway*
host,*hostname_apache,IP_address,function,interface_name,network_mask,network_gateway*

host,*hostname_oracle,IP_address,function,interface_name,network_mask,network_gateway*
host,*hostname_secondary,IP_address,function,interface_name,network_mask,network_gateway*
host,*hostname_primary,IP_address,function,interface_name,network_mask,network_gateway*
ntpserver1,*IP_address*
ntpserver2,*IP_address*
timezone,*time_zone*

Example:

A bulkconfig file needs to be created for the NSP cluster setup with four physical servers:

- Server hostname: nsp-apache
- Server hostname: nsp-oracle
- Server hostname: nsp-secondary
- Server hostname: nsp-primary
- Because it is a rackmount system, use eth01 and eth02 for interface names

  Note: If you are configuring C-class blades, replace eth01 with bond0.3 and eth02 with bond0.4 when you create this file.

- Apache IP addresses:
  - First interface (eth01): 10.236.2.141
  - Second interface (eth02): 10.236.1.141
- Oracle IP address (eth01): 10.236.2.142
- Secondary IP address (eth01): 10.236.2.143
- Primary IP address (eth01): 10.236.2.144
- Subnet mask: 255.255.255.254
- Gateway addresses:
  - Apache eth01: 10.236.2.129
  - Apache eth02: 10.236.1.129
  - Default for all other servers: 10.236.2.129
- NTP server IP address: 10.236.129.11
- Server timezone: Europe/Prague

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of host configuration, and there should not be any typos in bulkconfig file.

```
 [root@nsp ~]# cat /root/bulkconfig
host,nsp-apache,10.236.2.141,NSP_APACHE,eth01,255.255.255.224,10.236.2.129
host,nsp-apache,10.236.1.141,NSP_APACHE,eth02,255.255.255.224,10.236.1.129
host,nsp-oracle,10.236.2.142,NSP_ORACLE,eth01,255.255.255.224,10.236.2.129
host,nsp-secondary,10.236.2.143,NSP_SECONDARY,eth01,255.255.255.224,10.236.2.129
host,nsp-primary,10.236.2.144,NSP_PRIMARY,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
timezone,Europe/Prague
```

12.2 IXP Bulkconfig File Description

The IXP subsystem bulkconfig file contains the overall IXP pre-installation configuration information. During the installation process, various scripts use this file to configure IXP.

The bulkconfig file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The IXP bulkconfig file is also used when installing a Data Warehouse Server (DWS), in which case the file is structured as if the IXP subsystem was made of one single xDR server.

The IXP bulkconfig file template is located on the IXP iso on the /upgrade/IXP_bulkconfig_template path.

The file is unique for the IXP subsystem and is present on each server in this subsystem.

Note: When you install PIC, you are asked to create this bulkconfig file and update this file. **DO NOT** remove the IXP bulkconfig file from the server.

The IXP subsystem bulkconfig file is used during these processes:

- Manufacturing installation
- Customer network integration
- Change IP
- Disaster recovery procedure
- RSP install/upgrade procedure

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Note: If the bulkconfig file is copied form ISO and moved to the /root , the permission will be Readonly. In this case change the rights to match the example below.

```
[root@ixp1981-1a ~]# pwd
/root

 [root@ixpl981-la ~]# ls -l   |  grep bulkconfig
-rw-r--r--  1 root root      358 Dec    4  19:20 bulkconfig
```

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

host, *hostname_of_1st_server, IP_address, function, interface_name,network_mask,network_gateway*
host, *hostname_of_2nd_server, IP_address, function, interface_name,network_mask,network_gateway*
host, *hostname_of_nth_server, IP_address, function, interface_name,network_mask,network_gateway*

ntpserver1, *IP_address*
ntpserver2, *IP_address*
ntpserver3, *IP_address*
ntppeerA,
ntppeerB,
nspprimary, *IP_address_of_primary_weblogic_or_onebox_nsp*
nspsecondary, *IP_address_of_secondary_weblogic*
nsporacle, *IP_address_of_oracle_server*
timezone, *time_zone*

Refer to the following descriptions of each keyword and its associated values.

host Description

host, *hostname_of_1st_server, IP_address, function, interface_name,network_mask,network_gateway*
host, *hostname_of_2nd_server, IP_address, function, interface_name,network_mask,network_gateway*
host, *hostname_of_nth_server, IP_address, function, interface_name,network_mask,network_gateway*

Example (installation):

host,ixp1981-1a,10.236.2.141,IXP-XDR,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-PDU,eth01,255.255.255.224,10.236.2.129

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

Example (disaster recovery of ixp1981-1b server):

host,ixp1981-1a,10.236.2.141,IXP-XDR,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142**,DR-BASE**,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-PDU,eth01,255.255.255.224,10.236.2.129

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname of nth server The server hostname in the standard IXP format: ***ixp****NNNN-MA* where:

- *N* is numeric 0-9
- *M* is numeric 1-9
- *A* is alphabetical a-z

Note: This bulkconfig is either used for the Report Server installation. All Report Servers must be installed with 1a designation.

IP_address The IP address of the server. For blade systems, the internal IP address of the server.

function The function of the server. Use one of the following entries for installation:

- IXP-XDR for the xDR Storage Server, Primary Report Server and Data Warehouse Server (DWS)
- IXP-PDU for the PDU Storage Server

- IXP-BASE for the IXP Base Server, Cluster Report Server and PPS server
- IXP-ES for the Export Server

Function for the disaster recovery procedure for the particular server is different. Use one of the following entries for disaster recovery:

- DR-XDR for the xDR Storage Server
- DR-PDU for the PDU Storage Server
- DR-BASE for the IXP Base Server
- DR-ES for the Export Server

interface_name Name of the interface where the network settings are applied.

- eth01 for the rackmount systems
- bond0.3 for the blade systems

network_mask The network mask.

network_gateway The default gateway.

ntpserver Description

ntpserver1,*IP_address*
ntpserver2,*IP_address*
ntpserver3,*IP_address*
ntppeerA,
ntppeerB,

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server
- ntpserver3 is the third NTP server
- ntppeerA not applicable; leave empty
- ntppeerB not applicable; leave empty

Example:

ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

NSP Description

nspprimary,*IP_address_of_primary_weblogic_or_onebox_nsp*
nspsecondary,*IP_address_of_secondary_weblogic*
nsporacle,*IP_address_of_oracle_server*

- nspprimary is the NSP Primary WebLogic server or the One-box NSP server

- nspsecondary is the NSP Secondary WebLogic server
- nsporacle is the NSP Oracle server

Example (for a One-box NSP):

```
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
```

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp The IP address of the NSP server:

- One-box: IP address of the One-box NSP server
- Four-box: IP address of the NSP Primary WebLogic server

IP_address_of_secondary_weblogic The IP address of the NSP server:

- One-box: not applicable; leave empty
- Four-box: IP address of the NSP Secondary WebLogic server

IP_address_of_oracle_server The IP address of the NSP Oracle server:

- One-box: not applicable; leave empty
- Four-box: IP address of the NSP Oracle server

timezone Description

timezone,*time_zone*

Example:

```
timezone,Europe/Prague
```

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file **TZ** column. For example:

```
 [root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT—
#code      coordinates      TZ                  comments
AD         +4230+00131      Europe/Andorra
AE         +2518+05518      Asia/Dubai
AF         +3431+06912      Asia/Kabul
AG         +1703-06148      America/Antigua
CZ         +5005+01426      Europe/Prague

--CUT--
```

bulkconfig file: installation example

A bulkconfig file needs to be created for the following IXP subsystem:

- Subsystem hostname: ixp1981
- 1a server is the xDR Storage Server with the IP address: 10.236.2.141
- 1b server is the Base Server with the IP address: 10.236.2.142
- 1c server is the PDU Storage Server with the IP address: 10.236.2.143
- Network interface: eth01
- Network mask: 255.255.255.254
- Default gateway: 10.236.2.129
- NTP server IP address: 10.236.129.11
- NSP One-box IP address: 10.10.10.10
- Server timezone: Europe/Prague

The corresponding bulkconfig file you create should appear as follows: **Note:** There is

no new line character in the middle of the host configuration.

```
[root@ixp1981-1a ~]# cat /root/bulkconfig
host,ixp1981-1a,10.236.2.141,IXP-XDR,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1b,10.236.2.142,IXP-BASE,eth01,255.255.255.224,10.236.2.129
host,ixp1981-1c,10.236.2.143,IXP-PDU,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
timezone,Europe/Prague
```

Automated records in /etc/bulkconfig file

During the automated integration of IXP subsystem with EFS server(s) the following line is added to the /etc/bulkconfig file (one per integrated EFS server):

efs,*hostname_of_EFS,IP_address_of_EFS*

where

- *hostname_of_EFS* is the hostname of EFS that local DataFeeds hosts uses as an export target
- *IP_address_of_EFS* is the IP address of such EFS

Example:

efs,ixp77 77-1e,10.236.0.33

12.3 EFS Bulkconfig File Description

The standalone Export File Server (EFS) bulkconfig file contains the overall EFS pre-installation configuration information. During the installation process, various scripts use this file to configure the EFS server.

The bulkconfig file is a case sensitive text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The EFS bulkconfig file template is located on the EFS iso on the /upgrade/EFS_bulkconfig_template path.

For the EFS server, you must create a new and unique bulkconfig file. Do **not** reuse the bulkconfig file that was created for the servers in the IXP subsystem.

Note: When you install PIC, you are asked to create this bulkconfig file and update this file. **DO NOT** remove the EFS bulkconfig file from the server.

The EFS bulkconfig file is used during these processes:

- EFS Manufacturing installation
- Customer network integration
- Change IP

This topic provides a description of each keyword and parameter used in the bulkconfig file. It is important to read and understand the contents of this file.

bulkconfig file location and rights

File name: bulkconfig

File absolute path: /root/bulkconfig

Note: If the bulkconfig file is copied form ISO and moved to the /root , the permission will be Readonly. In this case change the rights to match the example below.

```
 [root@ixp1981-1a ~]# pwd
/root
[root@ixp1981-1a ~]# ls -l | grep bulkconfig
-rw-r--r--  1 root root      358 Dec    4  19:20 bulkconfig
```

bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword, and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

host, *hostname_of_efs_server, IP_address, function, interface_name,network_mask,network_gateway*
ntpserver1,*IP_address*
ntpserver2,*IP_address*
ntpserver3,*IP_address*
ntppeerA,
ntppeerB,
nspprimary,*IP_address_of_primary_weblogic_or_onebox_nsp*
nspsecondary,*IP_address_of_secondary_weblogic*
nsporacle,*IP_address_of_oracle_server*
timezone,*time_zone*

Refer to the following descriptions of each keyword and its associated values. **host**

Description

host,*hostname_of_efs_server,IP_address,function,interface_name,network_mask,network_gateway*

Example (installation):

host,ixp1981-1a,10.236.2.141,**EFS**,eth01,255.255.255.224,10.236.2.129

Example (disaster recovery):

host,ixp1981-1a,10.23 6.2.141**,DR-EFS**,eth01,2 55.2 55.2 55.2 24,10.23 6.2.12 9

The host keyword has the following associated values:

hostname_of_efs_server	The server hostname in the standard IXP format: ***ixp****NNNN-MA* where: • *N* is numeric 0-9 • *M* is numeric 1-9 • *A* is alphabetical a-z **Note:** This bulkconfig is either used for the Report Server installation. All Report Servers must be installed with 1a designation.
IP_address function	The IP address of the server. The function of the server. Use EFS.
interface name	Name of the interface where the network settings are applied. Use eth01 for the rackmount system.
network_mask	The network mask.
network_gateway	The default gateway.

ntpserver Description

ntpserver1,*IP_address*
ntpserver2,*IP_address*
ntpserver3,*IP_address*
ntppeerA,
ntppeerB,

- ntpserver1 is the first NTP server
- ntpserver2 is the second NTP server
- ntpserver3 is the third NTP server
- ntppeerA not applicable; leave empty
- ntppeerB not applicable; leave empty

Example:

ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,

The ntpserver keyword has the following associated value:

IP_address The IP address of the NTP server.

NSP Description

nspprimary,*IP_address_of_primary_weblogic_or_onebox_nsp*

nspsecondary,*IP_address_of_secondary_weblogic*

nsporacle,*IP_address_of_oracle_server*

- nspprimary is the NSP Primary WebLogic server or the One-box NSP server
- nspsecondary is the NSP Secondary WebLogic server
- nsporacle is the NSP Oracle server

Example (for a One-box NSP):

nspprimary,10.10.10.10
nspsecondary,
nsporacle,

The NSP keyword has the following associated values:

IP_address_of_primary_weblogic_or_onebox_nsp The IP address of the NSP server:

- One-box: IP address of the One-box NSP server
- Four-box: IP address of the NSP Primary WebLogic server

IP_address_of_secondary_weblogic The IP address of the NSP server:

- One-box: not applicable; leave empty
- Four-box: IP address of the NSP Secondary WebLogic server

IP_address_of_oracle_server The IP address of the NSP Oracle server:

- One-box: not applicable; leave empty
- Four-box: IP address of the NSP Oracle server

timezone Description

timezone,*time_zone*

Example:

timezone,Europe/Prague

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the /usr/share/zoneinfo/zone.tab file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab --CUT--
#code      coordinates          TZ comments
AD         +4230+00131          Europe/Andorra
AE         +2518+05518          Asia/Dubai
AF         +3431+06912          Asia/Kabul
AG         +1703-06148          America/Antigua
CZ         +5005+01426          Europe/Prague
   ----CUT—
```

bulkconfig file: example

A bulkconfig file needs to be created for the following EFS:

- EFS server hostname: ixp1981-1a
- EFS server IP address: 10.236.2.141
- Network interface: eth01
- Network mask: 255.255.255.254
- Default gateway: 10.236.2.129
- NTP server IP address: 10.236.129.11
- NSP One-box IP address: 10.10.10.10
- Server timezone: Europe/Prague

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@ixp1981-1a ~]# cat /root/bulkconfig
host,ixp1981-1a,10.236.2.141,EFS,eth01,255.255.255.224,10.236.2.129
ntpserver1,10.236.129.11
ntpserver2,
ntpserver3,
ntppeerA,
ntppeerB,
nspprimary,10.10.10.10
nspsecondary,
nsporacle,
timezone,Europe/Prague
```

Automated records in /etc/bulkconfig file

During the automated integration of EFS server with IXP subsystem the following line is added to the /etc/bulkconfig file (one per IXP DataFeed hosts server):

ixp,*hostname_of_IXP,IP_address_of_IXP*

where

- *hostname_of_IXP* is the hostname of IXP server that hosts DataFeed application.
- *IP_address_of_IXP* is the IP address of such IXP server

Example:

ixp,ixp77 77-1a,10.236.0.33

12.4 xMF Bulkconfig File Description

This topic describes the syntax and use of the xMF bulkconfig file.

The xMF subsystem bulk configuration file contains the overall xMF subsystem configuration information. The bulkConf.pl script uses this single file to configure the xMF subsystem accordingly.

The bulkconfig file is a text file and as such can be created or updated with any available text editor, e.g. vi or vim.

The xMF bulkconfig file template is located on the XMF server on the `/usr/TKLC/plat/etc/platform.csv` path. Example of bulkconfig file is located on the `/usr/TKLC/plat/etc/platform.example.csv` path. Do not use this reference example to configure the xMF server!

The file is unique per subsystem and is present on each server in the subsystem.

DO NOT remove the xMF bulkconfig file from the server or subsystem.

This topic provides a description of each keyword and parameter used in the bulkconfig file (platform.csv). It is important to read and understand the contents of this file.

Bulkconfig file location and rights

File name: `platform.csv`
File path:`/var/TKLC/upgrade/platform.csv`

Bulkconfig file: template

The bulkconfig file is written in the CSV format.

Each line begins with a keyword that describes the type of information that the line contains. The keyword is mandatory. Each line must begin with the keyword and then contains various values for this keyword. The keyword and its associated values are separated by a comma. There are no empty spaces in the lines.

```
host,hostname_of_1st_server,function,designation,interface_name,IP_address,network_mask,network_gateway
host,hostname_of_2nd_server,function,designation,interface_name,IP_address,network_mask,network_gateway
host,hostname_of_nth_server,function,designation,interface_name,IP_address,network_mask,network_gateway
ntp,ntpserver1,IP_address
ntp,ntpserver2,IP_address
ntp,ntpserver3,IP_address
ntp,ntppeerA,IP_address
ntp,ntppeerB,IP_address
app,appserver,IP_address_of_primary_nsp
app,appserver2,IP_address_of_secondary_nsp
tz,time_zone
```

Refer to the following descriptions of each keyword and its associated values. **host Description**

```
host,hostname_of_1st_server, finction,designaticn, interface_name, IP_address,network_rrask,network_gateway
host,hostname_of_2nd_server, finction,designaticn, interfacejname, IP_address,netiork_nask,network_gateway
host,hostname_of_nth_server, function, designation,interface_name, IP_address,netiork_nask,network_gateway
…
```

Example:

```
host,imf-1a,IMF,1A,bcnd0.200,192.168.253.5,255.255.255.224,192.168.253.1
host,imf-1b,IMF,1B,bcnd0.200,192.168.253.6,255.255.255.224,192.168.253.1
host,imf-1c,IMF,1C,bcnd0.200,192.168.253.7,255.255.255.224,192.168.253.1
```

The count of the host lines equals to the count of the servers in the subsystem. There is a single host line per server in the subsystem.

The host keyword has the following associated values:

hostname of nth server The server hostname.

Note: It is recommended that the hostname ends with the designation of the server (for example, malibu-1a).

function The function of the server. Use one of the following entries:

- IMF
- PMF

designation The designation of the server is a combination of frame number and position of the server in the frame. Use the following rule:

- xMF subsystem: 1A for the first server, 1B for the second server, etc.
- PMF standalone: 0A

interface name Name of the interface where the network settings are applied.

- `bond0.200` for the IMF servers
- `eth01` for the PMF servers

IP_address The IP address of the server. For blade systems, the internal IP address of the server.

network_mask The network mask.

network_gateway The default gateway.

ntpserver Description

```
ntp,ntpserver1,IP_address
ntp,ntpserver2,IP_address
ntp,ntpserver3,IP_addres
ntp,ntppeerA,IP_address
ntp,ntppeerB,IP_address
```

- `ntpserver1` is the first NTP server
- `ntpserver2` is the second NTP server
- `ntpserver3` is the third NTP server
- `ntppeerA` not applicable; leave empty
- `ntppeerB` not applicable; leave empty

Example:

```
ntp,ntpserver1,10.236.129.11
```

The ntpserver keyword has the following associated value:

IP_address	The IP address of the NTP server.

nsp Description

```
app,appserver,IP_address_of_primary_nsp
app,appserver2,IP_address_of_secondary_nsp_appserver
```

- `appserver` is the NSP Primary server
- `appserver2` is the NSP Secondary WebLogic server

Example (for a One-box NSP):

```
app,appserver,10.10.10.10
```

The nsp keyword has the following associated values:

IP_address_of_primary_nsp	The IP address of the NSP Primary server: • One-box: IP address of the One-box NSP server • Four-box: IP address of the NSP Primary server
IP_address_of_secondary_nsp	The IP address of the NSP Secondary server: • One-box: not applicable; leave empty • Four-box: IP address of the NSP Secondary server

timezone Description

```
tz,time_zone
```

Example:

```
tz,Europe/Prague
```

The timezone keyword has the following associated value:

time_zone The timezone string. For a list of available timezones that you can use, refer to the `/usr/share/zoneinfo/zone.tab` file **TZ** column. For example:

```
[root@nsp ~]# cat /usr/share/zoneinfo/zone.tab
--CUT--
#code       coordinates      TZ                comments
AD          +4230+00131      Europe/Andorra
AE          +2518+05518      Asia/Dubai
AF          +3431+06912      Asia/Kabul
AG          +1703-06148      America/Antigua
CZ          +5005+01426      Europe/Prague
----CUT—
```

Bulkconfig file: example

A bulkconfig file needs to be created for the following xMF subsystem:

- Subsystem hostname: imf-1a
- 1a server with the IP address: `192.168.253.5`
- 1b server with the IP address: `192.168.253.6`
- 1c server with the IP address: `191.168.253.7`
- IMF subsystem, interface: `bond0.200`
- Network mask: `255.255.255.224`
- Default gateway: `192.168.253.1`
- NTP server IP address: `10.250.32.10`
- Subsystem is added to the appserver with IP address: `10.10.10.10`
- Subsystem timezone: `Europe/Prague`

The corresponding bulkconfig file you create should appear as follows:

Note: There is no new line character in the middle of the host configuration.

```
[root@T3-1A upgrade]# cat platform.csv
host,imf-1a,IMF,1A,bond0.200,192.168.253.5,255.255.255.224,192.168.253.1
host,imf-1b,IMF,1B,bond0.200,192.168.253.6,255.255.255.224,192.168.253.1
host,imf-1c,IMF,1C,bond0.200,192.168.253.7,255.255.255.224,192.168.253.1
ntp,ntpserver1,10.250.32.10
ntp,ntpserver2,10.250.32.11
ntp,ntpserver3,10.250.32.12
ntp,ntppeerA,10.250.32.13
ntp,ntppeerB,10.250.32.14
app,appserver,10.10.10.10
app,appserver2,10.10.10.11
tz,Europe/Prague
```

13 FSE Enrichment file syntax

The first step in configuring an xDR Static Enrichment file is the naming process. Static enrichment files must begin with a dollar sign character ($) and have an extension of fse. The name of the enrichment file determines the processing order in the case of multiple files, as the data server processes the files in alphabetical order.

For example, a file with the name *$0addfile.fse* will process before a file with the name *$testfile.fse*.

A static enrichment file must contain three sections:

- Main
- Filter
- Mapping

All of your MAIN sections should look like the following:

```
SECTION:MAIN
VERSION:200
DLL:FSEMAP
MODE:BEFORE
```

It should be noted that each of your filter sections will be a little different, depending on the type and field that the enrichment is changing. The following sample should appear similar to your Filter section:

```
SECTION:FILTER
NAME:Not_International
EXPR:A
COND:A:BNumberNature:<>:International number
```

The mapping section will be different for each enrichment being done. Each file should reflect a different field that the enrichment is chafollowing is an example of a MAPPING section with sample data:

```
SECTION:MAPPING
INPUT:BNumber
OUTPUT:OCNB

MAP:201007:7229
MAP:201032:0138
MAP:201040:9206
MAP:201200:9206
MAP:201202:6630
```

The above statement specifies that for this particular enrichment, we will take the value from the column “BNumber”, and if it matches a predefined value, populate a column called “OCNB” with the specified “new” value. In the example above, if the column “BNumber” is populated with a value of “201007”, place a value of “7229” in the column called “OCNB”.

14Switch Configuration

14.1 Cisco basic knowledge

enable to move from user mode to priviledge mode

disable to move from priviledge mode to user mode

show running-config to display the current configuration in RAM

show startup-config to display the saved configuration in NVRAM

configure terminal to move from priviledge mode to config mode

interface gi1/1 to move from config mode to an interface config

copy running-config startup-config save the current configuration

show interfaces display the interfaces status

reload to reboot the switch

show version to display the ROM and IOS information

show tech-support to display a full switch status report. It should be caoptured in a file because it is long and takes a few minutes

14.1.1 Configure and access the serial console on TPD

Setup minicom access for 4948/4948E switches
Determine whether needed minicom files are already available by issuing the following command:

```
# ls /etc/minirc.*
```

If the file "minirc.switch" is not listed, proceed with the rest of this step, otherwise skip to the next step:
Setup the serial connections for a switch by issuing the following command:

```
# remoteConsole --add --name=switch --bps=9600 --parity=N --databits=8
--handshake=none --port=<switch_serial_port>
```

Note: The default switch_serial_port should be /dev/ttyS1
Connect serially to switch by issuing the following command as root on the management server:

```
# minicom switch
Press RETURN to get started.
Press Enter
```

If the "autoinstall" line below does not appear, the switch may not be in factory default condition, continue with the step, disregarding this line:

```
Would you like to terminate autoinstall? [yes]:Enter
Switch> enable
Switch#
```

If "enable" command above prompts for a password, the switch is not in factory default configuration. This may be due to a previous configuration attempt. This procedure is for initial install.
To exit from the console, enter **<ctrl-a><q>** and you will be returned to the server prompt.

14.1.2 Configure and access the serial console on TVOE

From TVOE server: Setup conserver serial access a switch and open the firewall to allow for future tftp use in this procedure.
From management server, configure the conserver service to enable serial access to the switches:

```
# conserverAdm --addConsole --name=switch_console --device=/dev/ttyS4
```

Open the conserver port on the firewall of the TVOE management server:

```
# iptables -I INPUT -s <pmac_mgmtVLAN_ip_address>/255.255.255.255 -p all -j ACCEPT
# service iptables save
```

Note: The default devices should be /dev/ttyS4 and /dev/ttyS5 for PM&C

Connect serially to switch by issuing the following command from the PM&C server or any other servers you open the port on the firewall.

```
# console -M <TVOE_server_mgmtVLAN_ip_address> -l platcfg switch_console
Enter platcfg@pmac5000101's password: <platcfg_password>
[Enter `^Ec?' for help]
Press Enter
Switch>
```

Depending on the switch config you might have to provide also the appropriate password to access the switch console after having provided the platcfg password.
To exit from the console, enter **<ctrl-E><c><.>** and you will be returned to the server prompt.

14.1.3 4948&4948EF Reset to factory defaults

Using this procedure you might loose the network connectirty.

It is advice to not do it with a remote connection

In priviledge mode type

```
Switch#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
*May 23 07:28:47.754: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#erase cat4000_flash:
Erasing the cat4000_flash filesystem will remove all files! Continue? [confirm]
[OK]
Erase of cat4000_flash: complete
Switch#reload
System configuration has been modified. Save? [yes/no]:   <- if the question is asked the answer to this question is no
Proceed with reload? [confirm]
```

Once the switch rebooted you might receive the following question before to get the prompt

```
Press RETURN to get started!
  00:00:01: %C4K_IOSSYS-3-BLANKSTARTUPCONFIG: Blank or invalid startup-config, bo
s00:00:17: %SPANTREE-5-EXTENDED_SYSID: Extended SysId enabled for type vlan
 00:00:18: %C4K_IOSMODPORTMAN-6-MODULEONLINE: Module 1 (WS-C4948 S/N: FOX11450NC
e00:00:37: %SYS-5-RESTART: System restarted --
 Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-IPBASEK9-M), Vers
)Technical Support: http://www.cisco.com/techsupport
 Copyright (c) 1986-2008 by Cisco Systems, Inc.
 Compiled Tue 29-Jul-08 12:15 by tinhuang

 Would you like to terminate autoinstall? [yes]:    <- if the question is asked the answer to this question is yes
```

Configure the switch to boot properly by verifying that the bootvar is showing the correct configuration, from 0-IPBASEK9-M), V`# dir bootflash:`
determine from the output the latest image (check the version at cisco website if necessary)
if the width of the screen does not permit to see the complete output, use the following (the question mark Number", and if it `# show file info bootflash:?`

```
# show bootvar
```

if how b variablebootflash:?oes not permit to /or config register is not 0x2102:
basically follow:

```
# config terminal
(config)# boot system flash bootflash:<name of image with latest version>
(config)# config-register 0x2102
(config)# end
# write memory
# show bootvar
```

14.1.4 Assign an IP address on a 3020

Refer to 909-2209-001 section 3.6.2 Configure initial OA settings via configuration wizard step 8 OA GUI: EBIPA settings

14.1.5 2950 & 3020 Reset to factory defaults

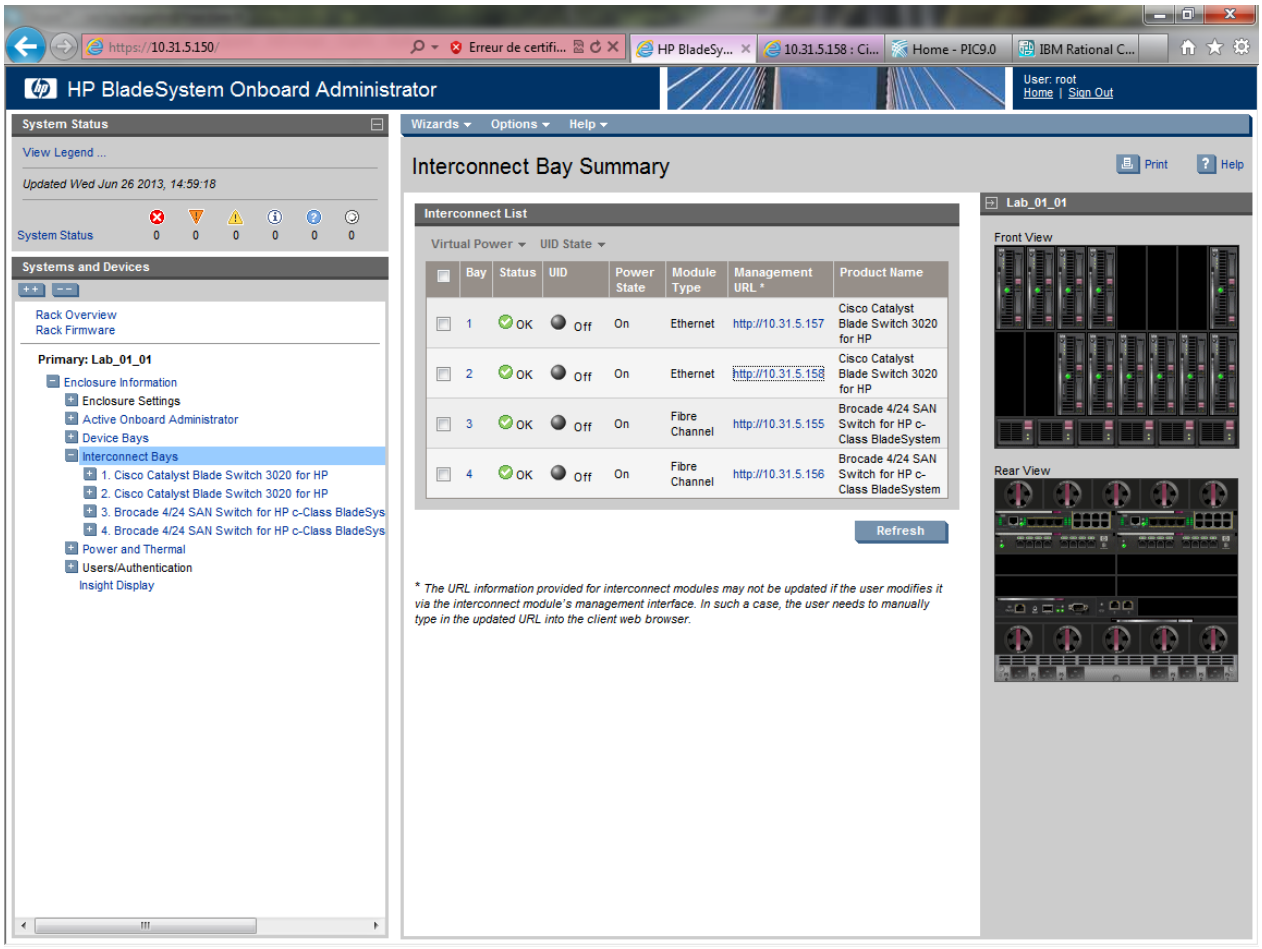
Using this procedure you might loose the network connectivity.

It is advice to not do it with a remote connection

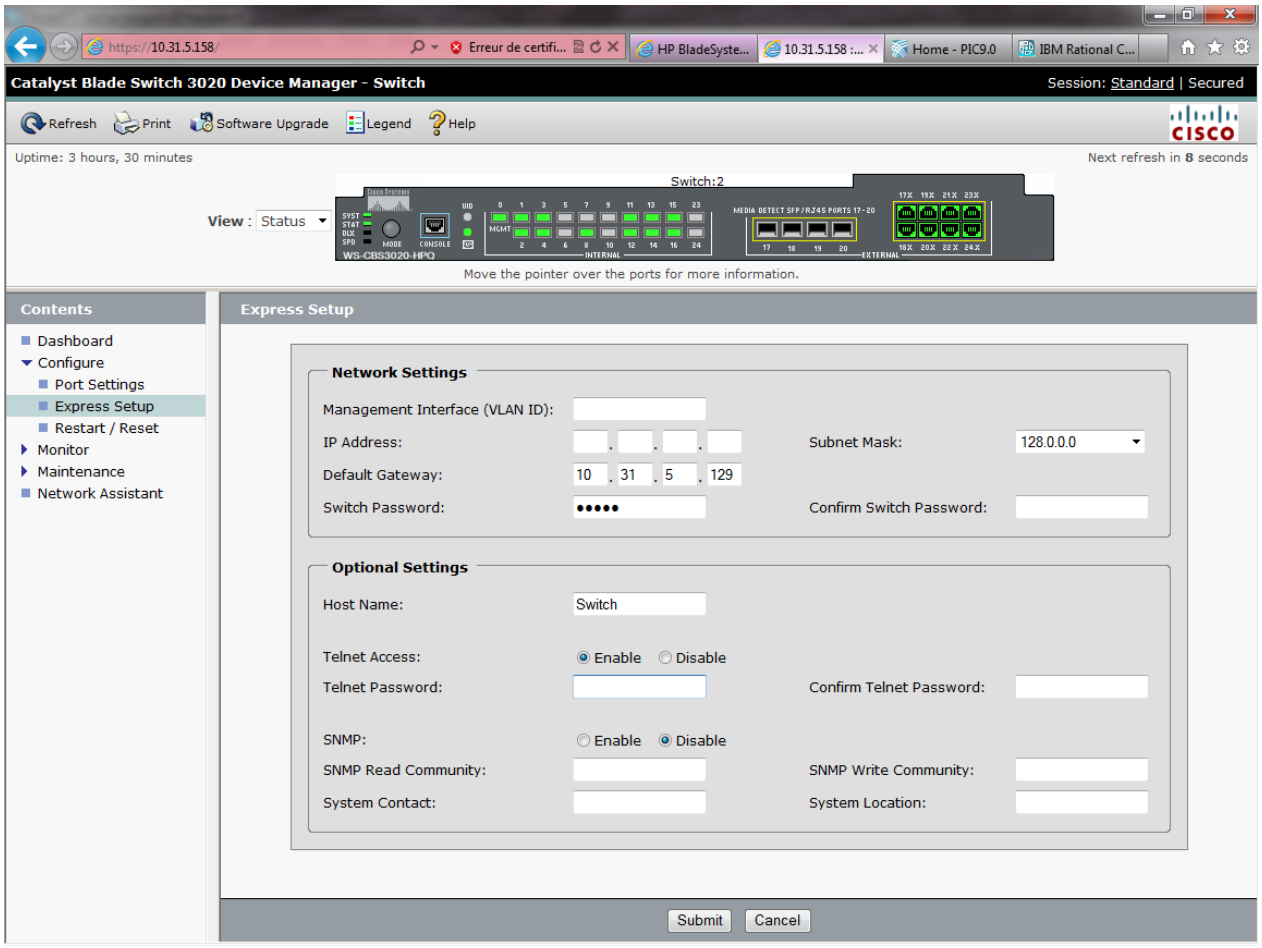
In priviledge mode type

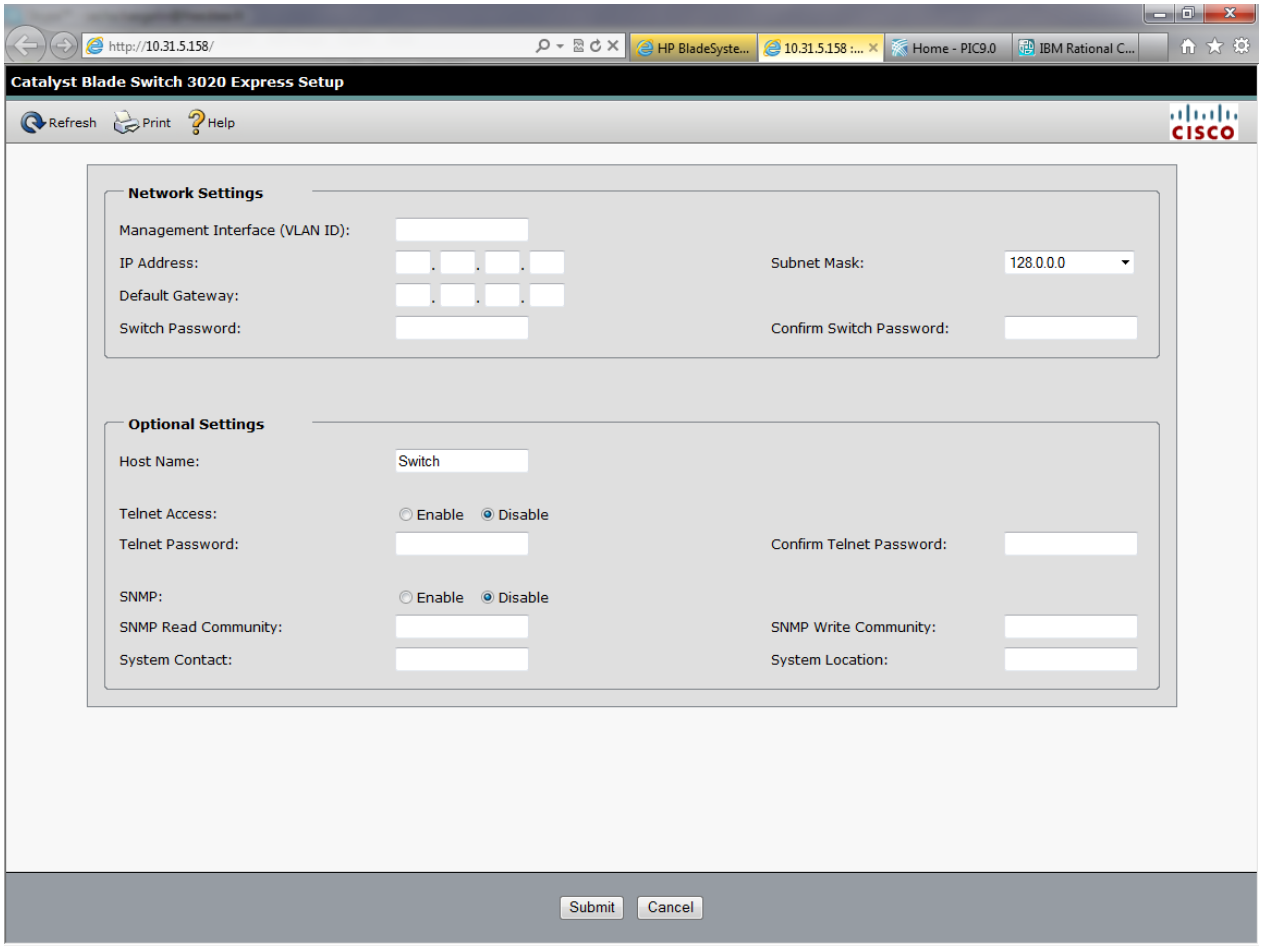
```
Switch#write erase
Erasing the nvram filesystem will remove all configuration files! Continue? [confirm]
[OK]
Erase of nvram: complete
*May 23 07:28:47.754: %SYS-7-NV_BLOCK_INIT: Initialized the geometry of nvram
Switch#delete flash:vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#reload
System configuration has been modified. Save? [yes/no]:    <- if the question is asked
the answer to this question is no
Proceed with reload? [confirm]
```

14.1.6 Configure telnet access on a 3020



If it is the first access the web interface will open directly on the express setup, otherway you can access it from the configure menu.


https://10.31.5.158/
Erreur de certifi...
HP BladeSyste...
10.31.5.158 :...
Home - PIC9.0
IBM Rational C...
Catalyst Blade Switch 3020 Device Manager - Switch
Session: Standard | Secured
Refresh
Print
Software Upgrade
Legend
Help
Uptime: 3 hours, 30 minutes
Next refresh in 8 seconds
Switch:2
View : Status
WS-CBS3020-HPQ
Move the pointer over the ports for more information.
Contents
Dashboard
Configure
Port Settings
Express Setup
Restart / Reset
Monitor
Maintenance
Network Assistant
Express Setup
Network Settings
Management Interface (VLAN ID):
IP Address:
Subnet Mask:
128.0.0.0
Default Gateway:
10 . 31 . 5 . 129
Switch Password:
Confirm Switch Password:
Optional Settings
Host Name:
Switch
Telnet Access:
Enable
Disable
Telnet Password:
Confirm Telnet Password:
SNMP:
Enable
Disable
SNMP Read Community:
SNMP Write Community:
System Contact:
System Location:
Submit
Cancel


http://10.31.5.158/
HP BladeSyste...
10.31.5.158 :...
Home - PIC9.0
IBM Rational C...
Catalyst Blade Switch 3020 Express Setup
Refresh
Print
Help
Network Settings
Management Interface (VLAN ID):
IP Address:
Subnet Mask:
128.0.0.0
Default Gateway:
Switch Password:
Confirm Switch Password:
Optional Settings
Host Name:
Switch
Telnet Access:
Enable
Disable
Telnet Password:
Confirm Telnet Password:
SNMP:
Enable
Disable
SNMP Read Community:
SNMP Write Community:
System Contact:
System Location:
Submit
Cancel

From there you can enable the telnet access and define the password.
You will have also to specify the VLAN ID to 1 and an IP in this VLAN, but don't configure the gateway. The IP will be removed while the switch config, and all configuration will be done using telnet on the EBIPA address.

14.1.7 Configure SSH access

In order to configure the SSH access you must have an IOS supporting the encryption. To check you must ensure the IOS file name contain "K9"
Move from the user mode to priviledge mode.

```
Switch#enable
Switch#show version | include IPBASE
Cisco IOS Software, Catalyst 4500 L3 Switch Software (cat4500-IPBASEK9-M),
Version 12.2(53)SG2, RELEASE SOFTWARE (fc1)
```

If it is the case than you can proceed with the following commands once you moved to the config mode:

```
Switch# configure terminal
username root password 0 *****      ! <--------- replace ***** with password
specified in password dragon as Cisco SSH
ip domain-name tekelec.com
crypto key generate rsa
% You already have RSA keys defined named switch1B.tekelec.com.
% Do you really want to replace them? [yes/no]: yes
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.
How many bits in the modulus [512]: 1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
ip ssh version 2
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
 transport input telnet
line vty 5 15
 login local
 transport input ssh
Switch(config)# end
Switch# copy running-config startup-config
```

14.1.8 Recover a switch from rommon prompt

In case the switch configuration failed and the switch would be in rommon follow this procedure to boot the switch

```
rommon 6 >dir bootflash:
   File size                 Checksum      File name
   -----------------------------------------------
  12632100 bytes (0xc0c024)   0x8136853a    cat4500-ipbasek9-mz.122-31.SGA8.bin
    456060 bytes (0x6f57c)    0x66d8b2a7    cat4500-ios-promupgrade-122_31r_SGA1
   Total space = 60817408 bytes, Available = 47728992 bytes

rommon 8 >confreg
 Configuration Summary :
 => console baud: 9600
 => autoboot from: commands specified in 'BOOT' environment variable
```

```
 do you wish to change the configuration? y/n  [n]:  y
 enable  "diagnostic mode"? y/n  [n]:  n
 enable  "use net in IP bcast address"? y/n  [n]:
 enable  "load rom after netboot fails"? y/n  [n]:
 enable  "use all zero broadcast"? y/n  [n]:
 enable  "break/abort has effect"? y/n  [n]:  y
 enable  "ignore system config info"? y/n  [n]:
 change console baud rate? y/n  [n]:
 change the boot characteristics? y/n  [n]:  y
 enter to boot:
 0 = disable autoboot
 1 = the first file from internal flash device
 2 = commands specified in 'BOOT' environment variable
 [2]:
 Configuration Summary :
 => break/abort has effect
 => console baud: 9600
 => autoboot from: commands specified in 'BOOT' environment variable

 do you wish to save this configuration? y/n  [n]:  y
 You must reset or power cycle for new configuration to take effect
rommon 10 >boot bootflash:cat4500-ipbasek9-mz.122-31.SGA8.bin
Rommon reg: 0xE2004180
############
k2diags version 5.2_c
Switch> enable
Switch# config t
Switch(config)# config-reg 0x2102
Switch(config)# boot system flash bootflash:cat4500-ipbasek9-mz.122-31.SGA8.bin
Switch(config)# end
Switch# copy running-config startup-config
Switch# reload
Configuration has been modified, save?  No
<reboots>
```

The following links provide additional info if needed.

http://www.cisco.com/en/US/products/hw/switches/ps663/products_configuration_example09186a0080094ecf.shtml

14.1.9 Upgrade IOS software

Copy the new IOS file on the server you will use as tftp server in the directory /tftpboot.
In the following example 10.10.10.10 is the IXP used as tftp server and 10.10.10.11 is the switch to load the new software. The tftp server must have an IP connectivity to the switch.

```
[root@ixp0000-1a tftpboot]# ping 10.10.10.11
PING 10.10.10.11 (10.10.10.11) 56(84) bytes of data.
64 bytes from 10.10.10.11: icmp_seq=1 ttl=255 time=0.659 ms
64 bytes from 10.10.10.11: icmp_seq=2 ttl=255 time=1.47 ms
64 bytes from 10.10.10.11: icmp_seq=3 ttl=255 time=1.38 ms
```

If the switch have no IP configured, from the priviledge mode

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip address 10.10.10.11 255.255.255.0
```

Start the tftp service on the server

```
[root@ixp0000-1a tftpboot]# service xinetd start
Starting xinetd:
[root@ixp0000-1a tftpboot]# /usr/TKLC/plat/sbin/tftpctl --start
RCS_VERSION=1.3
Stopping xinetd:                                           [  OK  ]
```

```
Starting xinetd:                                          [  OK  ]
```

Copy the new software to the switch

```
Switch#copy tftp: bootflash:
Address or name of remote host []? 10.10.10.10
Source filename []? cat4500-ipbasek9-mz.122-53.SG2.bin
Destination filename [cat4500-ipbasek9-mz.122-53.SG2.bin]?
Accessing tftp://10.10.10.10/cat4500-ipbasek9-mz.122-53.SG2.bin...
Loading cat4500-ipbasek9-mz.122-53.SG2.bin from 10.10.10.10 (via Vlan1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 16332568 bytes]
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
16332568 bytes copied in 73.440 secs (222393 bytes/sec)
Switch#dir bootflash:
Directory of bootflash:/
  1  -rwx    14569696  May 23 2009 11:53:09 +00:00  cat4500-ipbase-mz.122-46.SG.bin
  2  -rwx    16332568  Aug 14 2013 05:29:21 +00:00  cat4500-ipbasek9-mz.122-53.SG2.bin
60817408 bytes total (775240 bytes free)
```

Modify the configuration to boot using the new software and no more the previous one.

```
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#boot system flash bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin
Switch(config)#no boot system flash bootflash:cat4500-ipbase-mz.122-46.SG.bin
Switch(config)#exit
Switch #copy running-config startup-config
Switch #reload
```

14.1.10 Backup the switch config on a server

Use the following command to backup a switch configuration on a server.

```
blue-sw1-1#copy running-config scp:
Address or name of remote host []? 172.22.49.10
Destination username [root]?
Destination filename [blue-sw1-1-confg]?
Writing blue-sw1-1-confg
Password:
!!
9314 bytes copied in 14.292 secs (652 bytes/sec)
blue-sw1-1#
```

14.2 RM mediation

The VLAN values must be customized according customer requirement

14.2.1 Switch port allocation

The first IXP Server iLO are directly connected to customer network. Server E in th control frame and server A in teh extension frames

All or no vlan	vlan 100 iLO	vlan 200 CUST	vlan 300 Frontend

Ctrl Frame RM

Port 1 ServerA iLO	Port 3 ServerB iLO	Port 5 ServerC iLO	Port 7 ServerD iLO	Port 9	Port 11 ServerF iLO	Port 13 ServerG iLO	Port 15 ServerH iLO	Port 17 ServerI iLO	Port 19 ServerJ iLO	Port 21 ServerK iLO	Port 23 ServerL iLO	Port 25 Next Frame	Port 27 Next Frame	Port 29 Next Frame	Port 31 Next Frame	Port 33 Next Frame	Port 35 Next Frame	Port 37 Next Frame	Port 39 Next Frame	Port 41 Cust Net iLO	Port 43	Port 45	Port 47 Cust Net SW A
Port 2 ServerA eth1	Port 4 ServerB eth1	Port 6 ServerC eth1	Port 8 ServerD eth1	Port 10 ServerE eth1	Port 12 ServerF eth1	Port 14 ServerG eth1	Port 16 ServerH eth1	Port 18 ServerI eth1	Port 20 ServerJ eth1	Port 22 ServerK eth1	Port 24 ServerL eth1	Port 26 Next Frame	Port 28 Next Frame	Port 30 Next Frame	Port 32 Next Frame	Port 34 Next Frame	Port 36 Next Frame	Port 38 Next Frame	Port 40 Next Frame	Port 42 NSP Frontend	Port 44 Free	Port 46 Free	Port 48 Cust Net SW B

Ext Frame RM 7.1 and higher

Port 1 Free	Port 3 ServerB iLO	Port 5 ServerC iLO	Port 7 ServerD iLO	Port 9 ServerE iLO	Port 11 ServerF iLO	Port 13 ServerG iLO	Port 15 ServerH iLO	Port 17 ServerI iLO	Port 19 ServerJ iLO	Port 21 ServerK iLO	Port 23 ServerL iLO	Port 25 Free	Port 27 Free	Port 29 Free	Port 31 Free	Port 33 Free	Port 35 Free	Port 37 Free	Port 39 Free	Port 41 Free	Port 43 Free	Port 45 Free	Port 47 iLO Ctrl Frame
Port 2 ServerA eth1	Port 4 ServerB eth1	Port 6 ServerC eth1	Port 8 ServerD eth1	Port 10 ServerE eth1	Port 12 ServerF eth1	Port 14 ServerG eth1	Port 16 ServerH eth1	Port 18 ServerI eth1	Port 20 ServerJ eth1	Port 22 ServerK eth1	Port 24 ServerL eth1	Port 26 Free	Port 28 Free	Port 30 Free	Port 32 Free	Port 34 Free	Port 36 Free	Port 38 Free	Port 40 Free	Port 42 Free	Port 44 Free	Port 46 Free	Port 48 Eth Ctrl Frame

Ext Frame RM 7.0 and lower

Port 1 Free	Port 3 ServerB iLO	Port 5 ServerC iLO	Port 7 ServerD iLO	Port 9 ServerE iLO	Port 11 Free	Port 13 Free	Port 15 Free	Port 17 Free	Port 19 Free	Port 21 ServerF iLO	Port 23 ServerG iLO	Port 25 ServerH iLO	Port 27 ServerI iLO	Port 29 ServerJ iLO	Port 31 ServerK iLO	Port 33 ServerL iLO	Port 35 Free	Port 37 Free	Port 39 Free	Port 41 Free	Port 43 Free	Port 45 Free	Port 47 iLO Ctrl Frame
Port 2 ServerA eth1	Port 4 ServerB eth1	Port 6 ServerC eth1	Port 8 ServerD eth1	Port 10 ServerE eth1	Port 12 Free	Port 14 Free	Port 16 Free	Port 18 Free	Port 20 Free	Port 22 ServerF eth1	Port 24 ServerG eth1	Port 26 ServerH eth1	Port 28 ServerI eth1	Port 30 ServerJ eth1	Port 32 ServerK eth1	Port 34 ServerL eth1	Port 36 Free	Port 38 Free	Port 40 Free	Port 42 Free	Port 44 Free	Port 46 Free	Port 48 Eth Ctrl Frame

14.2.2 Configure the switch

This procedure is only for RMS server and only the first IXP server from the cabinet.

Note: In case in the procedure would failed, refer to 909-2247-01 PIC 9.0 Maintenance guide in order to recover the switch from rommon prompt.

A. Configure and access the serial console from the server on the switch
   a. Refer to section 14.1.1
B. Reset the switch to factory default
   a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

   b. Refer to section 14.1.3 to reset the switch
C. Configure the switch using the appropriate template
   a. Refer to the following section 14.2 to select the appropriate configuration template and adapt it to the customer IP network.
   b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
   c. Move from the user mode to priviledge mode and then to config mode

```
Switch# enable
Switch# configure terminal
```

   Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.
   d. Paste all the commands from the template config you have adapted to your network. The lines you need to customize are higlighted with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
   e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

f. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

g. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

```
Switch# reload
```

h. Finally to configure the SSH access to the switch refer to section 14.1.7

i. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

j. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboots

```
Switch# copy running-config startup-config
```

k. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

14.2.3 Control Frame Switch

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service compress-config
!
hostname Switch
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
no aaa new-model
ip subnet-zero
no ip source-route
no ip domain-lookup
!
vtp mode transparent
!
!
!
power redundancy-mode redundant
no file verify auto
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
vlan 100          ! <--------- replace VLAN with customer value
 name iLO
```

```
!
vlan 200          ! <--------- replace VLAN with customer value
 name CUST
!
vlan 300          ! <--------- replace VLAN with customer value
 name NSP_Front
!
Interface range Gi1/1 ,Gi1/3 ,Gi1/5 ,Gi1/7 ,Gi1/9
 description Server iLO Access
 switchport access vlan 100   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/11 ,Gi1/13 ,Gi1/15 ,Gi1/17 ,Gi1/19
 description Server iLO Access
 switchport access vlan 100   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/21 ,Gi1/23 ,Gi1/25 ,Gi1/27 ,Gi1/29
 description Server iLO Access
 switchport access vlan 100   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/31 ,Gi1/33 ,Gi1/35 ,Gi1/37 ,Gi1/39
 description Server iLO Access
 switchport access vlan 100   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/41
 description Server iLO Access
 switchport access vlan 100   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/2 ,Gi1/4 ,Gi1/6 ,Gi1/8 ,Gi1/10
 description Server CUST Access
 switchport access vlan 200   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/12 ,Gi1/14 ,Gi1/16 ,Gi1/18 ,Gi1/20
 description Server CUST Access
 switchport access vlan 200   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/22 ,Gi1/24 ,Gi1/26 ,Gi1/28 ,Gi1/30
 description Server CUST Access
 switchport access vlan 200   ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
```

```
!
interface range Gi1/32 ,Gi1/34 ,Gi1/36 ,Gi1/38 ,Gi1/40
 description Server CUST Access
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/42
 description NSP NIC2 CUST Ethernet Access
 switchport access vlan 300    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range GigabitEthernet1/43 - 46
 description UNUSED
 shutdown
!
interface GigabitEthernet1/47
 description 802.1Q trunk link to backbone SWA
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
!
interface GigabitEthernet1/48
 description 802.1Q trunk link to backbone SWB
 switchport trunk encapsulation dot1q
 switchport mode trunk
 media-type rj45
 spanning-tree cost 20
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100              ! <--------- replace VLAN with customer value
 description Optional Switch Virtual Interface (SVI) for iLO Subnet - switch
management
 no ip address
 shutdown
!
interface Vlan200              ! <--------- replace VLAN with customer value
 description Optional Switch Virtual Interface (SVI) for CUST Subnet - switch
management
 no ip address
 shutdown
!
no ip http server
!
!
!
no cdp run
!
control-plane
!
```

```
!
line con 0
 exec-timeout 30 0
 logging synchronous
 stopbits 1
line vty 0 15
 exec-timeout 30 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 logging synchronous
 login
!
end
```

14.2.4 Extension Frame Switch

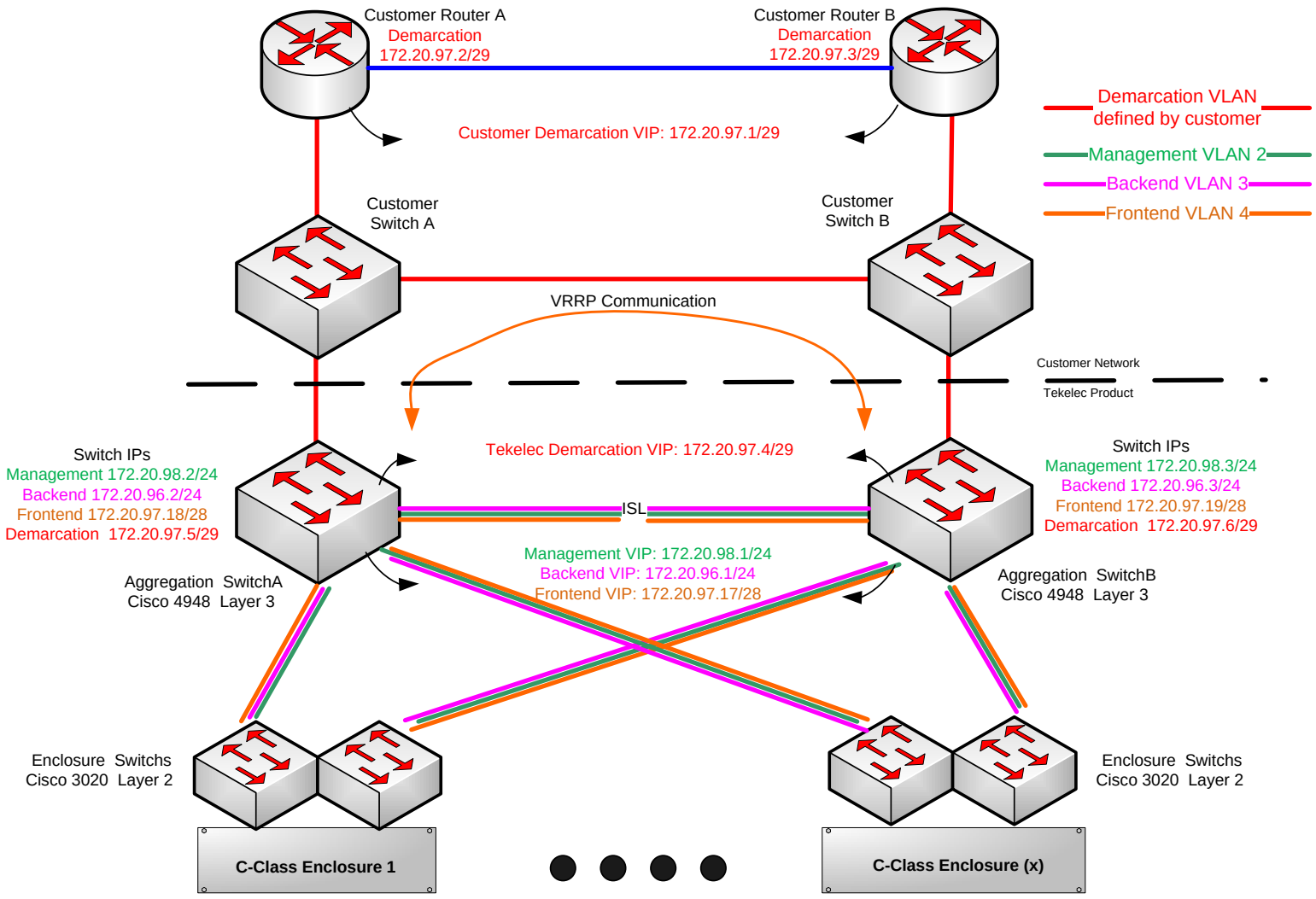
```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service compress-config
!
hostname Switch
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
no aaa new-model
ip subnet-zero
no ip source-route
no ip domain-lookup
!
vtp mode transparent
!
!
!
power redundancy-mode redundant
no file verify auto
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
!
vlan 100                ! <--------- replace VLAN with customer value
 name iLO
!
vlan 200                ! <--------- replace VLAN with customer value
 name CUST
!
```

```
Interface range Gi1/1 ,Gi1/3 ,Gi1/5 ,Gi1/7 ,Gi1/9
 description Server iLO Access
 switchport access vlan 100    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/11 ,Gi1/13 ,Gi1/15 ,Gi1/17 ,Gi1/19
 description Server iLO Access
 switchport access vlan 100    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/21 ,Gi1/23 ,Gi1/25 ,Gi1/27 ,Gi1/29
 description Server iLO Access
 switchport access vlan 100    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/31 ,Gi1/33 ,Gi1/35 ,Gi1/37 ,Gi1/39
 description Server iLO Access
 switchport access vlan 100    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
Interface range Gi1/41 ,Gi1/43 ,Gi1/45
 description Server iLO Access
 switchport access vlan 100    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/2 ,Gi1/4 ,Gi1/6 ,Gi1/8 ,Gi1/10
 description Server CUST Access
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/12 ,Gi1/14 ,Gi1/16 ,Gi1/18 ,Gi1/20
 description Server CUST Access
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/22 ,Gi1/24 ,Gi1/26 ,Gi1/28 ,Gi1/30
 description Server CUST Access
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface range Gi1/32 ,Gi1/34 ,Gi1/36 ,Gi1/38 ,Gi1/40
 description Server CUST Access
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
```

```
interface range Gi1/42 ,Gi1/44 ,Gi1/46
 description Server CUST Access
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/47
description Connection to Control Frame Switch on iLO VLAN
 switchport access vlan 100    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/48
description Connection to Control Frame Switch on CUST VLAN
 switchport access vlan 200    ! <--------- replace VLAN with customer value
 switchport mode access
 spanning-tree portfast
!
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan100              ! <--------- replace VLAN with customer value
 description Optional Switch Virtual Interface (SVI) for iLO Subnet - switch
management
 no ip address
 shutdown
!
interface Vlan200              ! <--------- replace VLAN with customer value
 description Optional Switch Virtual Interface (SVI) for CUST Subnet - switch
management
 no ip address
 shutdown
!
no ip http server
!
!
!
no cdp run
!
control-plane
!
!
line con 0
 exec-timeout 30 0
 logging synchronous
 stopbits 1
line vty 0 15
 exec-timeout 30 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 logging synchronous
 login
```

```
!
end
```

14.3 Blade mediation



14.3.1 Switch port allocation

All the following information assume the cabling has been done according the System Interconnect diagrams 893-0103-XX to be used for G6 &G8 servers with P2000 storage arrays

PM&C iLO is directly connected to customer network

no vlan	vlan 1-4	vlan 2 management	Vlan 1-2	Vlan 2-3	vlan X customer

Encosure 7 Switch1

Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23
Server1 eth2	Server3 eth2	Server5 eth2	Server7 eth2	Server9 eth2	Server11 eth2	Server13 eth2	Server15 eth2	Agg SW A P5	Agg SW A P7	SAN contr1	SAN contr3
Port 2	Port 4	Port 6	Port 8	Port 10	Port 12	Port 14	Port 16	Port 18	Port 20	Port 22	Port 24
Server2 eth2	Server4 eth2	Server6 eth2	Server8 eth2	Server10 eth2	Server12 eth2	Server14 eth2	Server16 eth2	Agg SW A P6	Agg SW A P8	SAN contr2	SAN contr4

Encosure 1 Switch1

Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23
Server1 eth2	Server3 eth2	Server5 eth2	Server7 eth2	Server9 eth2	Server11 eth2	Server13 eth2	Server15 eth2	Agg SW A P29	Agg SW A P31	SAN contr1	SAN contr3
Port 2	Port 4	Port 6	Port 8	Port 10	Port 12	Port 14	Port 16	Port 18	Port 20	Port 22	Port 24
Server2 eth2	Server4 eth2	Server6 eth2	Server8 eth2	Server10 eth2	Server12 eth2	Server14 eth2	Server16 eth2	Agg SW A P30	Agg SW A P32	SAN contr2	SAN contr4

Aggregation SwitchA

Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23	Port 25	Port 27	Port 29	Port 31	Port 33	Port 35	Port 37	Port 39	Port 41	Port 43	Port 45	Port 47
Agg SW B P1	Agg SW B P3	Enc1 SW1 P17	Enc1 SW1 P19	Enc2 SW1 P17	Enc2 SW1 P19	Enc3 SW1 P17	Enc3 SW1 P19	Enc4 SW1 P17	Enc4 SW1 P19	Enc5 SW1 P17	Enc5 SW1 P19	Enc6 SW1 P17	Enc6 SW1 P19	Enc7 SW1 P17	Enc7 SW1 P19	Enc1 OA1	Enc3 OA1	Enc5 OA1	Enc7 OA1	Free	Free	For Laptop	Free
Port 2	Port 4	Port 6	Port 8	Port 10	Port 12	Port 14	Port 16	Port 18	Port 20	Port 22	Port 24	Port 26	Port 28	Port 30	Port 32	Port 34	Port 36	Port 38	Port 40	Port 42	Port 44	Port 46	Port 48
Agg SW B P2	Agg SW B P4	Enc1 SW1 P18	Enc1 SW1 P20	Enc2 SW1 P18	Enc2 SW1 P20	Enc3 SW1 P18	Enc3 SW1 P20	Enc4 SW1 P18	Enc4 SW1 P20	Enc5 SW1 P18	Enc5 SW1 P20	Enc6 SW1 P18	Enc6 SW1 P20	Enc7 SW1 P18	Enc7 SW1 P20	Enc2 OA1	Enc4 OA1	Enc6 OA1	PM&C Eth1	Free	Free	For Laptop	Cust Net eth

Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23	Port 25	Port 27	Port 29	Port 31	Port 33	Port 35	Port 37	Port 39	Port 41	Port 43	Port 45	Port 47
Agg SW A P1	Agg SW A P3	Enc1 SW2 P17	Enc1 SW2 P19	Enc2 SW2 P17	Enc2 SW2 P19	Enc3 SW2 P17	Enc3 SW2 P19	Enc4 SW2 P17	Enc4 SW2 P19	Enc5 SW2 P17	Enc5 SW2 P19	Enc6 SW2 P17	Enc6 SW2 P19	Enc7 SW2 P17	Enc7 SW2 P19	Enc1 OA2	Enc3 OA2	Enc5 OA2	Enc7 OA2	Free	Free	For Laptop	Free
Port 2	Port 4	Port 6	Port 8	Port 10	Port 12	Port 14	Port 16	Port 18	Port 20	Port 22	Port 24	Port 26	Port 28	Port 30	Port 32	Port 34	Port 36	Port 38	Port 40	Port 42	Port 44	Port 46	Port 48
Agg SW A P2	Agg SW A P4	Enc1 SW2 P18	Enc1 SW2 P20	Enc2 SW2 P18	Enc2 SW2 P20	Enc3 SW2 P18	Enc3 SW2 P20	Enc4 SW2 P18	Enc4 SW2 P20	Enc5 SW2 P18	Enc5 SW2 P20	Enc6 SW2 P18	Enc6 SW2 P20	Enc7 SW2 P18	Enc7 SW2 P20	Enc2 OA2	Enc4 OA2	Enc6 OA2	PM&C Eth2	Free	Free	For Laptop	Cust Net eth

Aggregation SwitchB

Encosure 1 Switch2

Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23
Server1 eth2	Server3 eth2	Server5 eth2	Server7 eth2	Server9 eth2	Server11 eth2	Server13 eth2	Server15 eth2	Agg SW B P5	Agg SW B P7	SAN contr1	SAN contr3
Port 2	Port 4	Port 6	Port 8	Port 10	Port 12	Port 14	Port 16	Port 18	Port 20	Port 22	Port 24
Server2 eth2	Server4 eth2	Server6 eth2	Server8 eth2	Server10 eth2	Server12 eth2	Server14 eth2	Server16 eth2	Agg SW B P6	Agg SW B P8	SAN contr2	SAN contr4

Encosure 7 Switch2

Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23
Server1 eth2	Server3 eth2	Server5 eth2	Server7 eth2	Server9 eth2	Server11 eth2	Server13 eth2	Server15 eth2	Agg SW B P29	Agg SW B P31	SAN contr1	SAN contr3
Port 2	Port 4	Port 6	Port 8	Port 10	Port 12	Port 14	Port 16	Port 18	Port 20	Port 22	Port 24
Server2 eth2	Server4 eth2	Server6 eth2	Server8 eth2	Server10 eth2	Server12 eth2	Server14 eth2	Server16 eth2	Agg SW B P30	Agg SW B P32	SAN contr2	SAN contr4

14.3.2 Configure Cisco 4948/4948E/4948E-F aggregation switches (PM&C installed)

A. Configure and access the serial console from the PM&C server on the switches
    a. Refer to section 14.1.2
B. Reset the switch to factory default
    a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

    b. Refer to section 14.1.3 to reset the switch
C. Configure the switch using the appropriate template
    a. Refer to following section 14.3 to select the appropriate configuration template and adapt it to the customer IP network.
    b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
    c. Move from the user mode to priviledge mode and then to config mode

```
Switch# enable
Switch# configure terminal
```

    Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.
    d. Adapt the template configuration to your network. The lines you need to customize are higlited with Yellow comments. Paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
    e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

    f. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

    g. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

```
Switch# reload
```

    h. Finally to configure the SSH access to the switch refer to section 14.1.7
    i. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

    j. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

    k. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

14.3.3 Aggregation Switch

Note : The command "`spanning-tree portfast trunk`" will return the following warning, you can ignore:

```
%Warning: portfast should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this
interface  when portfast is enabled, can cause temporary bridging loops.
 Use with CAUTION
```

```
!
!
! Aggregation Switch configuration
! MASTER VRRP switch
!
!
hostname switchA        ! <------ replace the hostname to identify the switch
!
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/48 line-protocol
ip subnet-zero
vtp mode transparent
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan internal allocation policy ascending
!
vlan 2
 name management
!
vlan 3
 name back-end
!
vlan 4
 name front-end
!
vlan 110    ! <------ Enter customer value for demarcation VLAN

 name customer
!
!
!  INTER switch1A to other switch ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_switch1A_and_Enc1SW1
 switchport
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel2
 description Trunk_between_switch1A_and_Enc2SW1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel3
 description Trunk_between_switch1A_and_Enc3SW1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel4
 description Trunk_between_switch1A_and_Enc4SW1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel5
 description Trunk_between_switch1A_and_Enc5SW1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel6
 description Trunk_between_switch1A_and_Enc6SW1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel7
 description Trunk_between_switch1A_and_Enc7SW1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
!
interface Port-channel8
 description Trunk_between_switch1A_and_switch1B
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
!
!
```

```
!  INTER switch1A to other switch PORTS (internal)
!
!
interface range GigabitEthernet1/1-4
 description Trunk_between_switch1A_and_switch1B
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 switchport nonegotiate
 channel-group 8 mode active
!
interface range GigabitEthernet1/5-8
 description Trunk_between_cxeny(en1)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/9-12
 description ISL_to_cxeny(en2)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 2 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/13-16
 description ISL_to_cxeny(en3)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 3 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/17-20
 description ISL_to_cxeny(en4)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 4 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/21-24
 description ISL_to_cxeny(en5)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 5 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/25-28
 description ISL_to_cxeny(en6)-sw1
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 6 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/29-32
 description ISL_to_cxeny(en7)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 7 mode active
 spanning-tree portfast trunk
!
!
! OA PORTS
!
!
interface range GigabitEthernet1/33-39
 description cxeny(enX)-OA
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
!
! PM&C PORTS
!
!
interface GigabitEthernet1/40
 description c1ms1-nic
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-3
 switchport mode trunk
 media-type rj45
 spanning-tree portfast trunk
!
interface GigabitEthernet1/41
 description c1ms1-iLO for compatibilty with G6 & G5, it is recommanded to
connect directly on customer network
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
!
! UNSUSED PORTS
!
!
interface range GigabitEthernet1/42-44
 description Unused
 shutdown
!
interface GigabitEthernet1/47
 description Unused
 shutdown
!
```

```
!
! Laptop PORTS
!
!
interface range GigabitEthernet1/45-46
 description for Laptop connection
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
 no shutdown
!
!
! Customer uplink PORTS
!
!
interface GigabitEthernet1/48
 description Customer_Uplink
 switchport access vlan 110
 switchport mode access
 media-type rj45
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 ip address dhcp
 no shutdown
!
interface Vlan2
description IP address, netmask, and gateway for this switch in the
management VLAN
 ip address 172.20.98.2 255.255.255.0      ! <------ Enter IP and netmask FOR
management VLAN
 vrrp 2 ip 172.20.98.1         ! <------ replace IP with gateway for
management VLAN
 vrrp 2 track 1
 no shutdown
!
interface Vlan3
description IP address, netmask, and gateway for this switch in the backend
VLAN
 ip address 172.20.96.2 255.255.255.128    ! <------ Enter IP and netmask FOR
backend VLAN
 vrrp 3 ip 172.20.96.1               ! <------ replace IP with gateway for
backend VLAN
 vrrp 3 track 1
 no shutdown
!
interface Vlan4
description IP address, netmask, and gateway for this switch in the frontend
VLAN
```

```
 ip address 172.20.97.18 255.255.255.240  ! <------ Enter IP and netmask for
frontend VLAN
 vrrp 4 ip 172.20.97.17             ! <------ replace IP with gateway for
frontend VLAN
 vrrp 4 track 1
 no shutdown
!
description VLAN ID, IP address, netmask, and gateway for this switch in the
demarcation VLAN
interface Vlan110       ! <------ Enter customer value for demarcation VLAN
 ip address 172.20.97.5 255.255.255.248    ! <------ Enter IP and netmask for
demarcation VLAN
 vrrp 5 ip 172.20.97.4        ! <------ replace IP with gateway for
demarcation VLAN
 vrrp 5 track 1
 no shutdown
!
ip route 0.0.0.0 0.0.0.0 172.20.97.1      ! <--------- replace IP with
customer default gateway
ip route 0.0.0.0 0.0.0.0 172.20.96.3 200  ! <--------- replace IP with other
aggregation switch IP address in back-end vlan
no ip http server
!
!
logging 172.20.96.4           ! <--------- replace IP with PM&C address
no cdp run
!
snmp-server user cfguser cfguser v1
snmp-server user cfguser cfguser v2c
snmp-server community cfguser RO
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps tty
snmp-server enable traps fru-ctrl
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config
snmp-server enable traps ipmulticast
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 172.20.96.132 version 2c tekelec    ! <--------- replace IP
with WL1 address
!
control-plane
!
!
line con 0
password ***** ! <--------- replace ***** with password specified in password
dragon as Cisco telnet
 login
```

```
 stopbits 1
line vty 0 4
password ***** ! <--------- replace ***** with password specified in password
dragon as Cisco telnet
 login
line vty 5 15
password ***** ! <--------- replace ***** with password specified in password
dragon as Cisco telnet
 login
!
ntp clock-period 17179480
ntp server 10.27.8.4     ! <--------- replace IP with NTP server address
end
```

14.3.4 Configure Cisco 3020 switch

A. Assign IP addesses to the switches
   a. Refer to 909-2209-001 section 3.6.2 Configure initial OA settings via configuration wizard step 8 OA GUI: EBIPA settings if this was not done earlier
B. Reset the switch to factory default
   a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

   b. Refer to section 14.1.5 to reset the switch. Take care to only erase the vlan.dat and not the whole content of the flash.
C. Reconfigure the telnet access
   a. Refer to section 14.1.6.
D. Configure the switch using the appropriate template
   a. Refer to the following section 14.3.5.
   b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
   c. Open a telnet session on the switch and then move from the user mode to priviledge mode and then to config mode

```
Switch# enable
Switch# configure terminal
```

   Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.
   d. Paste all the commands from the template config you have adated to you network. The lines you need to customize are higlited with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
   e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

   f. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

   g. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

```
Switch# reload
```

   h. Finally to configure the SSH access to the switch refer to section 14.1.7
   i. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

j. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

k. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

14.3.5 Enclosure Switch

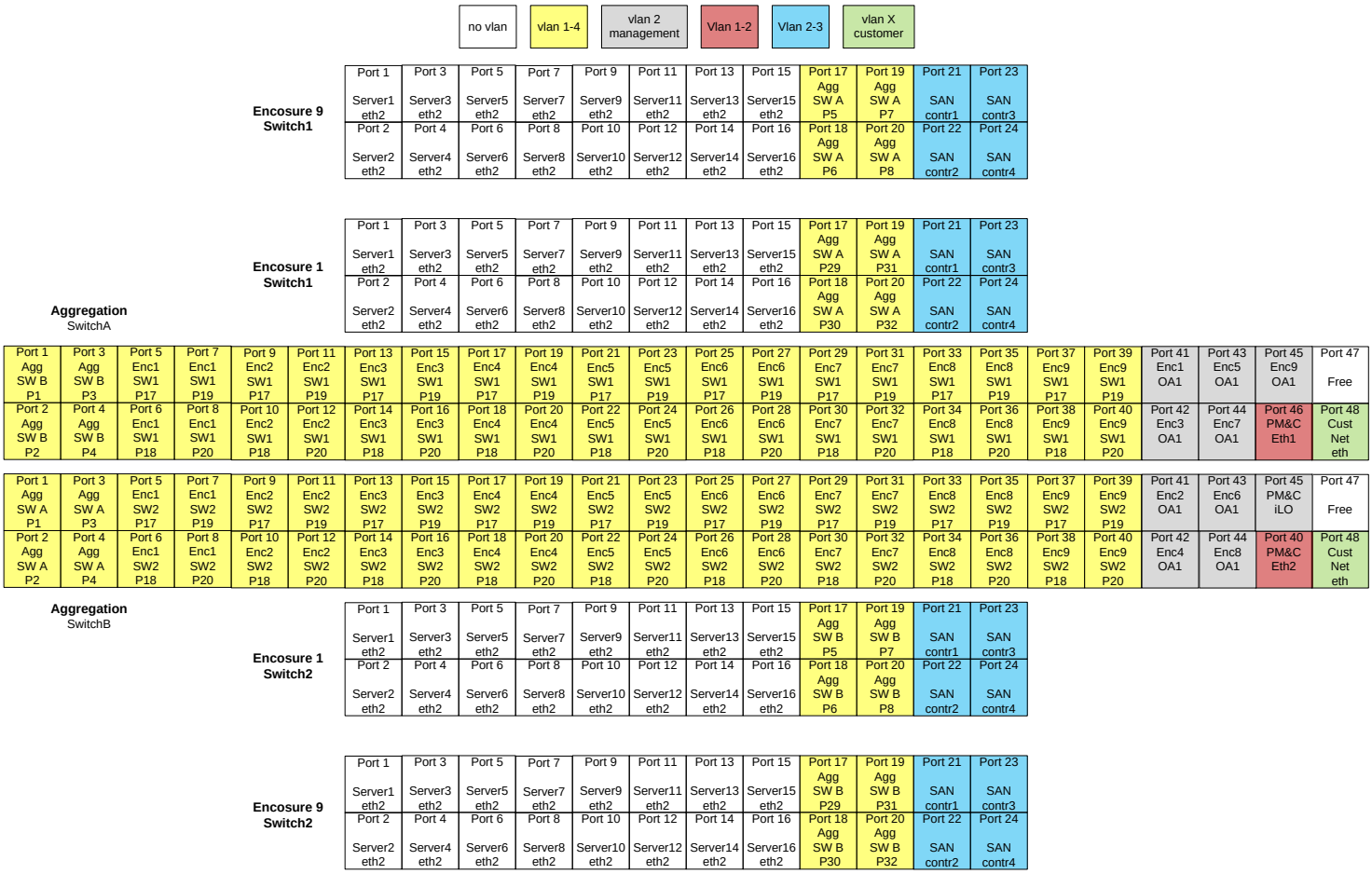
```
!
!
! Enclosure Switch configuration
!
!
hostname C3020A_IOBAY
!
no service config
no service pad
service timestamps debug datetime
service timestamps log datetime
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
!
link state track 1
ip subnet-zero
no ip domain-lookup
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 53248
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan internal allocation policy ascending
!
vlan 2
 name management
!
vlan 3
 name back-end
!
vlan 4
 name front-end
!
interface Port-channel1
 description ISL_between_4948_and_3020
 switchport trunk allowed vlan 1-4
 switchport mode trunk
```

```
 link state group 1 upstream
!
interface range GigabitEthernet0/17-20
 description ISL_between_4948_and_3020
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface FastEthernet0
 description IP address configured in the OA interface
! ip address dhcp        ! <--------- remove the comment only in case the
interface would not be already configured in dhcp
!
interface range GigabitEthernet0/1-16
 description bay.ethx
 switchport mode trunk
 link state group 1 downstream
 spanning-tree portfast trunk
!
interface range GigabitEthernet0/21-24
 description P2000 SAN controller
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip http server
ip http secure-server
!
logging 172.20.96.4      ! <--------- replace IP with PM&C management address
no cdp run
snmp-server community tekelec RO
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps tty
snmp-server enable traps entity
snmp-server enable traps cpu threshold
snmp-server enable traps vlancreate
snmp-server enable traps vlandelete
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps config
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps syslog
snmp-server enable traps vlan-membership
snmp-server host 172.20.96.132 version 2c tekelec     ! <--------- replace IP
with WL1 backend address
!
control-plane
!
```

```
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
ntp clock-period 36028892
ntp server 10.31.3.132  ! <--------- replace IP with NTP server address
end
```

14.3.6 G5 and G6 MSA cabling diagram

All the following information assume the cabling has been done according the System Interconnect diagrams 892-0093-01, 892-0094-01, 892-0095-01, and 892-0094-02 to be used for G5 &G6 servers with MSA storage arrays



14.3.6.1 Aggregation Switch 4948

```
!
! No configuration change since last restart
! NVRAM config last updated at 15:38:22 gmt-5 Thu Apr 16 2009
!
version 12.2
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
service compress-config
!
```

```
hostname switch1A
!
no logging console
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
no aaa new-model
!
track 1 interface GigabitEthernet1/48 line-protocol
ip subnet-zero
!
vtp mode transparent
!
!
!
!
!
power redundancy-mode redundant
no file verify auto
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 45056
!
vlan internal allocation policy ascending
!
vlan 2
 name management
!
vlan 3
 name back-end
!
vlan 4
 name front-end
!
vlan 10           ! <--------- replace VLAN with customer value
 name cust
!
interface Port-channel1
 description ISL_between_c1as1_and_c1en1-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel2
 description ISL_between_c1as1_and_cxeny(en2)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
```

```
!
interface Port-channel3
 description ISL_between_c1as1_and_cxeny(en3)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel4
 description ISL_between_c1as1_and_cxeny(en4)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel5
 description ISL_between_c1as1_and_cxeny(en5)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel6
 description ISL_between_c1as1_and_cxeny(en6)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel7
 description ISL_between_c1as1_and_cxeny(en7)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel8
 description ISL_between_c1as1_and_cxeny(en8)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel9
 description ISL_between_c1as1_and_cxeny(en9)-sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
```

```
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Port-channel10
 description ISL_between_c1as1_and_c1as2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/1-4
 description switch1B.gi1/1-4
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 10 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/5-8
 description ISL_to_c1en1(en1)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/9-12
 description ISL_to_cxeny(en2)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 2 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/13-16
 description ISL_to_cxeny(en3)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 3 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/17-20
 description ISL_to_cxeny(en4)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 4 mode active
 spanning-tree portfast trunk
!
interface GigabitEthernet1/21-24
 description ISL_to_cxeny(en5)-sw1
 switchport trunk encapsulation dot1q
```

```
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 5 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/25-28
 description ISL_to_cxeny(en6)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 6 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/29-32
 description ISL_to_cxeny(en7)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 7 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/33-36
 description ISL_to_cxeny(en8)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 8 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/37-40
 description ISL_to_cxeny(en9)-sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 9 mode active
 spanning-tree portfast trunk
!
interface range GigabitEthernet1/41-45
 description oa1&iLO
 switchport access vlan 2
 switchport mode access
 spanning-tree portfast
!
interface GigabitEthernet1/46
 description c1ms1-nic1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1-3
 switchport mode trunk
 media-type rj45
 spanning-tree portfast trunk
!
interface GigabitEthernet1/47
 description unused
 switchport trunk encapsulation dot1q
```

```
 switchport mode trunk
 shutdown
 media-type rj45
 spanning-tree portfast trunk
!
interface GigabitEthernet1/48
description Customer_Uplink
switchport access vlan 10      ! <--------- replace VLAN with customer value
 switchport mode access
 media-type rj45
 spanning-tree portfast
!
interface Vlan1
 no ip address
!
interface Vlan2
description IP address, netmask, and gateway for this switch in the
management VLAN
ip address 10.240.8.2 255.255.255.0        ! <------ replace IP and netmask
for management VLAN
 vrrp 2 ip 10.240.8.1                 ! <------ replace IP with gateway for
management VLAN
 vrrp 2 track 1
 no shutdown
!
interface Vlan3
description IP address, netmask, and gateway for this switch in the backend
VLAN
 ip address 10.240.9.2 255.255.255.0       ! <------ Enter IP and netmask for
backend VLAN
 vrrp 3 ip 10.240.9.1                 ! <------ replace IP with gateway for
backend VLAN
 vrrp 3 track 1
 no shutdown
!
interface Vlan4
description IP address, netmask, and gateway for this switch in the frontend
VLAN
 ip address 10.240.10.2 255.255.255.0      ! <------ Enter IP and netmask for
frontend VLAN
 vrrp 4 ip 10.240.10.1              ! <------ replace IP with gateway for
frontend VLAN
 vrrp 4 track 1
 no shutdown
!
interface Vlan10           ! <--------- replace VLAN with customer value
description VLAN ID, IP address, netmask, and gateway for this switch in the
demarcation VLAN
ip address 10.250.54.24 255.255.255.0      ! <------ Enter IP and netmask for
demarcation VLAN
 vrrp 10 ip 10.250.54.26                 ! <------ replace IP with Tekelec
gateway for demarcation VLAN
 no shutdown
!
```

```
ip route 0.0.0.0 0.0.0.0 10.250.54.1      ! <--------- replace IP with
customer default gateway
no ip http server
no ip http secure-server
!
!
logging 10.27.8.0       ! <--------- replace IP with PM&C address
no cdp run
!
snmp-server community cfguser RO
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps flash insertion removal
snmp-server enable traps cpu threshold
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps port-security
snmp-server enable traps storm-control trap-rate 5
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps vlan-membership
snmp-server host 10.31.5.211 version 2c cfguser     ! <--------- replace IP
with WL1 address
!
control-plane
!
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
 stopbits 1
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
ntp clock-period 17179453
ntp server 10.240.8.4   ! <--------- replace IP with NTP server address
end
```

14.3.6.2 Encosure Switch 3020

```
version 12.2
no service pad
service timestamps debug uptime
service timestamps log uptime
```

```
service password-encryption
!
hostname c1en1p1
!
no logging console
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
no aaa new-model
clock timezone gmt+1 1
system mtu routing 1500
vtp mode transparent
ip subnet-zero
!
!
spanning-tree mode rapid-pvst
no spanning-tree optimize bpdu transmission
spanning-tree etherchannel guard misconfig
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 53248
!
vlan internal allocation policy ascending
!
vlan 2
 name management
!
vlan 3
 name back-end
!
vlan 4
 name front-end
!
!
!
interface Port-channel1
 description ISL_between_4948_and_3020
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 spanning-tree portfast trunk
!
interface FastEthernet0
 ip address dhcp
!
interface range GigabitEthernet0/1-16
 description bay.ethx
 switchport mode trunk
 spanning-tree portfast trunk
!
interface range GigabitEthernet0/17-20
 description ISL_between_4948_and_3020
 switchport trunk allowed vlan 1-4
 switchport mode trunk
 channel-group 1 mode active
 spanning-tree portfast trunk
```

```
!
interface range GigabitEthernet0/21-24
 description cxsan-fc-port-mngt
 switchport trunk native vlan 2
 switchport trunk allowed vlan 2,3
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 0.0.0.0 0.0.0.0 10.31.5.129 254       ! <--------- replace IP with
customer default gateway
ip http server
ip http secure-server
!
logging 10.27.8.0                    ! <--------- replace IP with PM&C address
no cdp run
snmp-server community cfguser RO
snmp-server enable traps snmp authentication linkdown linkup coldstart
warmstart
snmp-server enable traps cpu threshold
snmp-server enable traps flash insertion removal
snmp-server enable traps port-security
snmp-server enable traps envmon fan shutdown supply temperature status
snmp-server enable traps storm-control trap-rate 5
snmp-server enable traps config
snmp-server enable traps hsrp
snmp-server enable traps bridge newroot topologychange
snmp-server enable traps mac-notification change move threshold
snmp-server enable traps vlan-membership
snmp-server host 10.31.5.211 version 2c cfguser    ! <--------- replace IP
with WL1 address
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
ntp clock-period 36029033
```

```
ntp server 10.31.5.132  ! <--------- replace IP with NTP server address
end
```

14.4 IMF

For new sytems installed using HPGen8 it is recomanded to use the following configuration described in section 14.4.1 and assuming the system is installed in accordance with the hardware requirements defined in section 1.6 and summarized in section 14.4.3 describing the switch port allocation.

If requirested by customer an alternate config can be used and is described in section 14.4.2 and in this case you have to configure the switch as for the default and than add the few lines described in this section.

The Layer 3 configuration described in section 14.4.4 to 14.4.9 are deigned for the CISCO 49448EF switch but is keeping also some commands in order to remain compatible with the previous CISCO 4948.

In case of switch installed to extend existing systems it is is recommended the same Layer 2 config used in the previous PIC releases and remembered in section:

- 14.4.11 for HP and TEKIII cabinets
- 14.4.12 for TEKII cabinets using Cisco 4948 switches
- 14.4.13 for TEKII cabinets using Cisco 2950 switches

If customers don't want to use Layer 3 configuration for a new system installation, those Layer 2 configuration can still be used even if you have 4948EF instead of 4948 switches.

14.4.1 default config

The interface to customer switch are configured in natif mode.If customer use vlans they must be configured on his switch (transparent for Tekelec) :

- Vlan 100 172.21.49.0 255.255.255.0

vlan can't be changed and is transaparent to the customer
IP can't be changed and shall not be used for servers communicating with IMF (NSP&IXP&VPN)

- Vlan 101 172.22.49.0 255.255.255.0

vlan can't be changed and is transaparent to the customer
IP can't be changed and shall not be used for servers communicating with IMF (NSP&IXP&VPN)

- Vlan 200 192.168.0.0 255.255.255.224 internal network minimum size for largets config

IP must be changed according values customer provided
vlan can't be changed and is transaparent to the customer
in the following config 192.168.0.1 is reserved and shall be used as default route for the IMF servers. 192.168.0.2 & 192.168.0.3 are reserved for switch IP

- Vlan 300 192.168.10.0 255.255.255.224 iLO network

IP must be changed according values customer provided

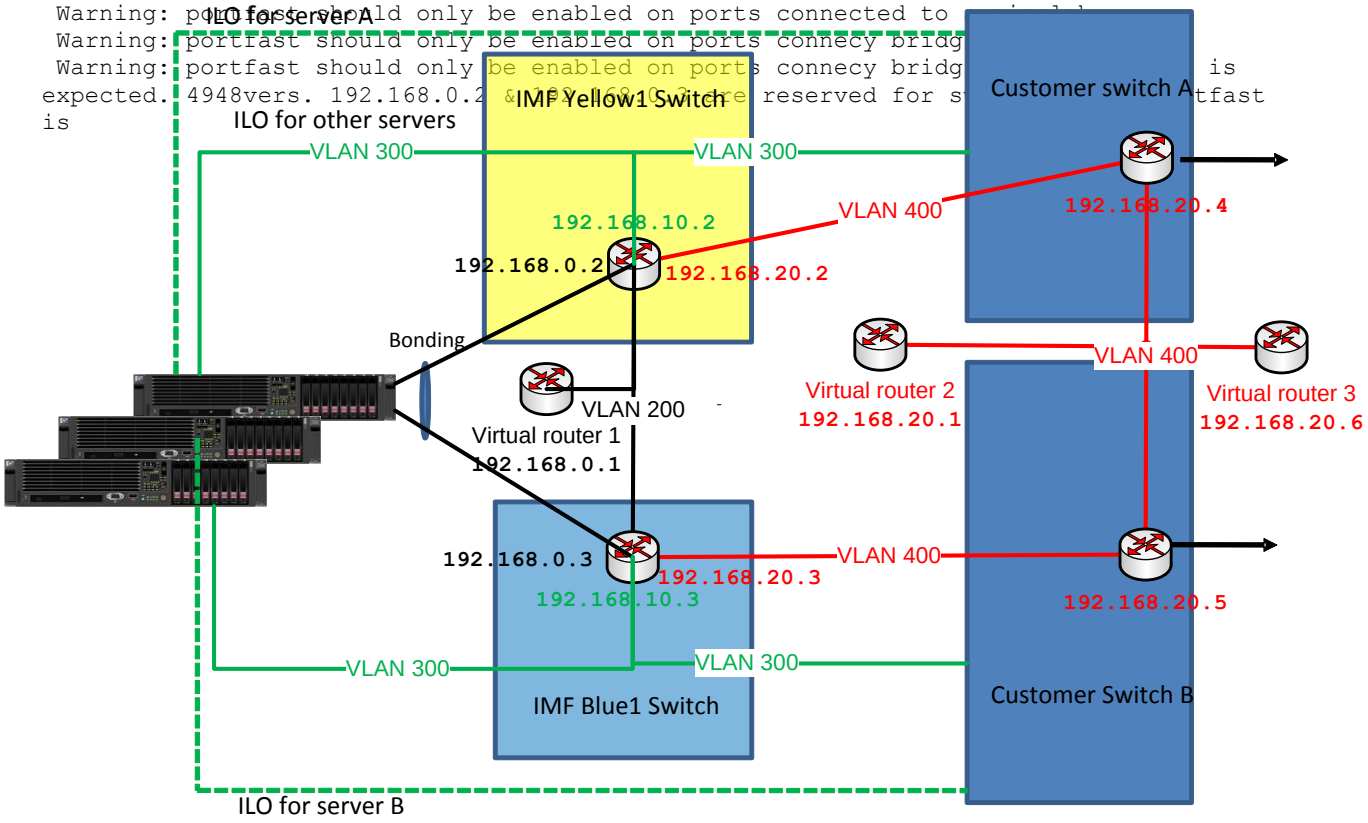
- Vlan 400 192.168.20.0 255.255.255.240 external network (demarcation)

IP must be changed according values customer provided

Note : the command "`switchport trunk encapsulation dot1q`" will fail on the 4948EF switch but it is kept this config for compatibility with the previous 4948

Note: While the configuration you may receive warnings like the one bellow, but this is expected.

```
%Warning: portfast should only be enabled on ports connected to a single
 Warning: portfast should only be enabled on ports connected to
 Warning: portfast should only be enabled on ports connecy bridg
 Warning: portfast should only be enabled on ports connecy bridg                is
expected. 4948vers. 192.168.0.2 &192.168.0.3 are reserved for s                tfast
is
```

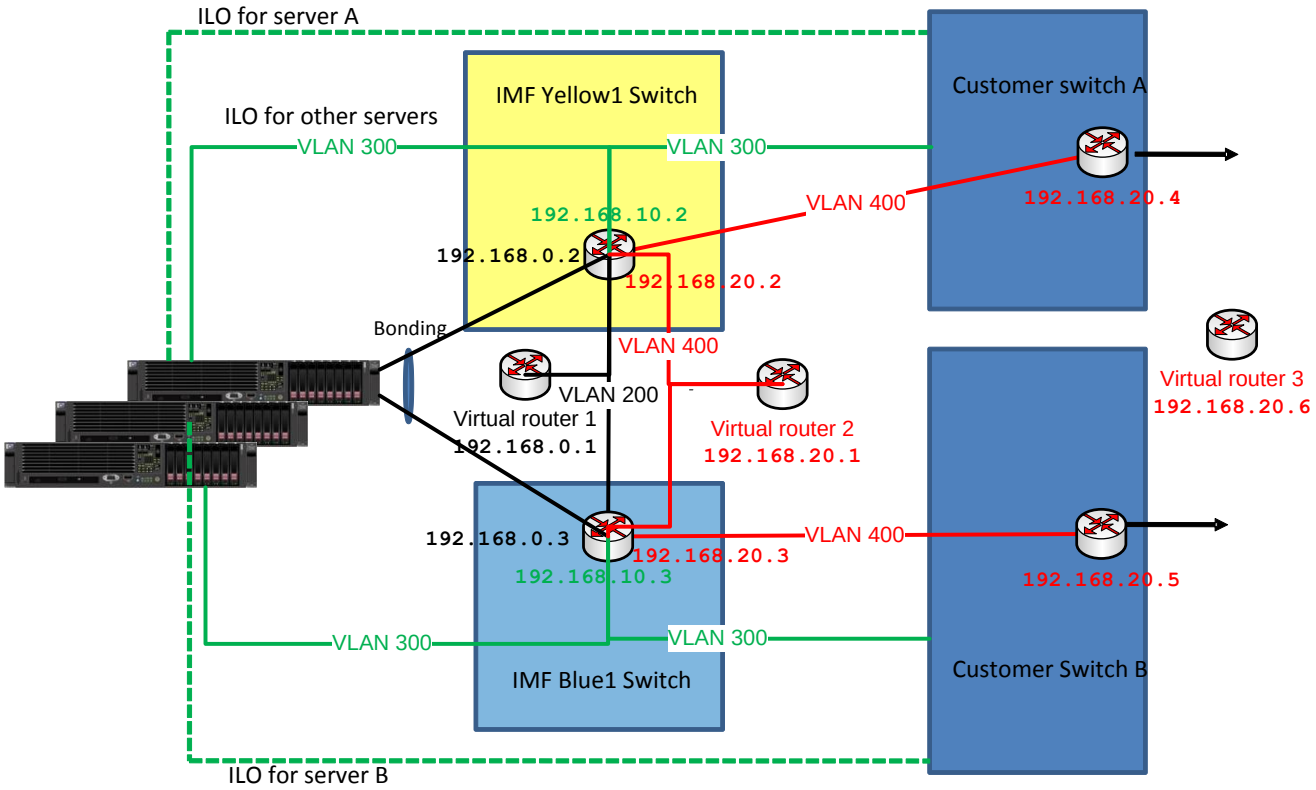


14.4.2 alternate config

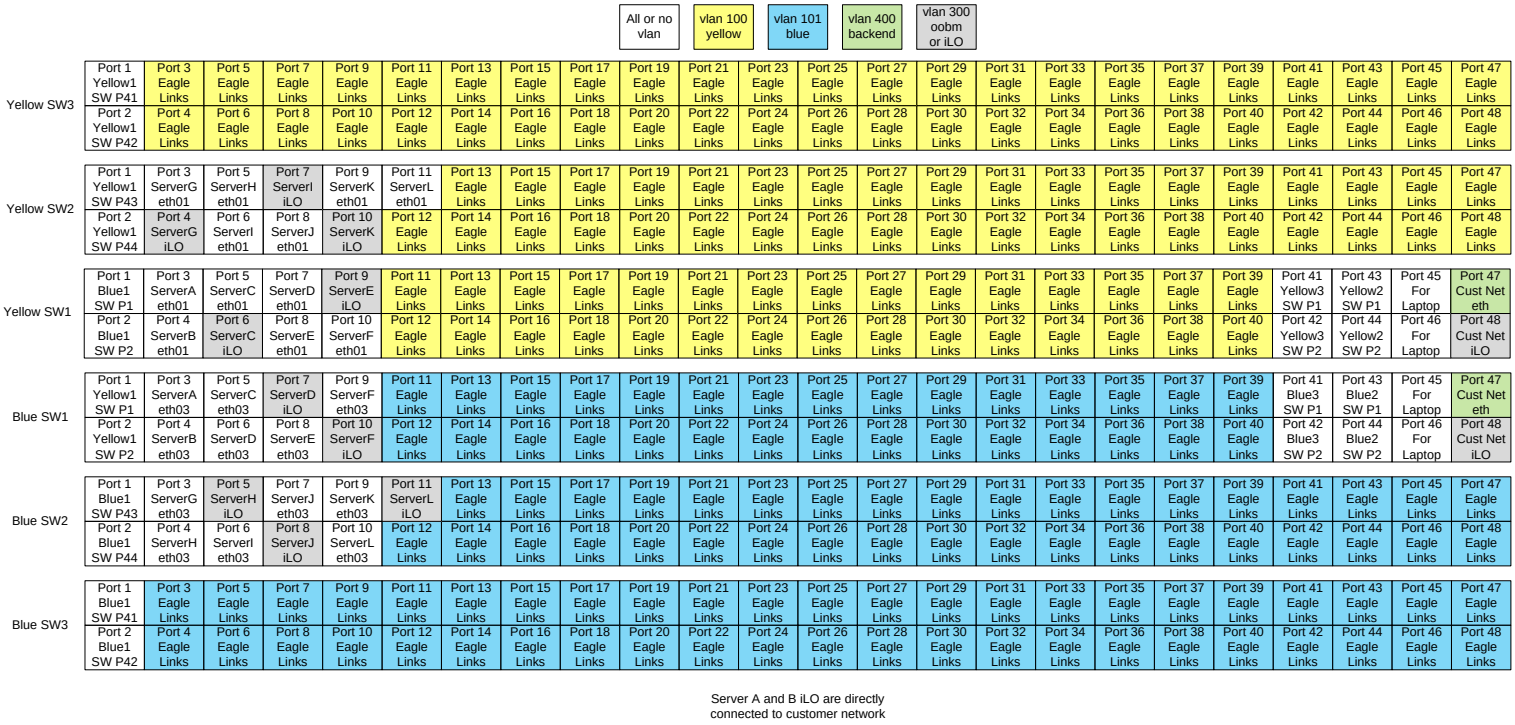
If the customer want to configure on Tekelec switches, we can use the alternate config bellow just by adding the few lines bellow to the default config.

This configuration can be dangerous, because customer must guarantee the is no link between the two switch access, other way it would make a loop and his network may crash.

```
interface Port-channel1
 switchport trunk allowed vlan 100,101,200,300,400
interface GigabitEthernet 1/1
 switchport trunk allowed vlan 100,101,200,300,400
interface GigabitEthernet 1/2
 switchport trunk allowed vlan 100,101,200,300,400
no track 1 int gigabitEthernet 1/47 line-protocol
track 1 interface port-channel 1 line-protocol
```



14.4.3 Switch port allocation



14.4.4 Configure switches

Note: In case in the procedure would failed, refer to 909-2247-01 PIC 9.0 Maintenance guide in order to recover the switch from rommon prompt.

A. Configure and access the serial console from the server on the switch
   a. Refer to section 14.1.1
B. Reset the switch to factory default
   a. If you are reconfiguring a switch backup the current config in a file using the command

```
Switch# show running-config
```

   b. Refer to section 14.1.3 to reset the switch
C. Configure the switch using the appropriate template
   a. Refer to following sections in 14.4 to select the appropriate configuration template and adapt it to the customer IP network.
   b. As there is no log file for the following steps it is recomanded to enable the log feature from your terminal in case something would not work as expected and assistance is required.
   c. Move from the user mode to priviledge mode and then to config mode

```
Switch# enable
Switch# configure terminal
```

Note : if you reset the switch to factory default no password should be requested to connect on it and move to enable mode.

d. Paste all the commands from the template config you have adapted to your network. The lines you need to customize are higlighted with Yellow comments. You can paste the command in block and not necessary one by one but don't do it with too much commands at a time in order to take care if an error message would appear.
e. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

f. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboot

```
Switch# copy running-config startup-config
```

g. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

```
Switch# reload
```

h. Finally to configure the SSH access to the switch refer to section 14.1.7
i. Once the config is in place you can check it is matching your expectation using the command

```
Switch# show running-config
```

j. If the configuration is fine then you can save it in the flash in order to have it automatically reloaded if the switch reboots

```
Switch# copy running-config startup-config
```

k. If there is an issue in your config you can can reboot the switch without saving and then restart the config from the step a

14.4.5 Yellow-sw1-1 Switch (Layer 3)

```
! IMF YELLOW1 SWITCH configuration
!
!
hostname yellow-sw1-1
!
no spanning-tree vlan 1-4094
no spanning-tree optimize bpdu transmission
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/47 line-protocol
ip subnet-zero
!
ip multicast-routing
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
!  INTER YELLOW SW1 TO BLUE SW1  ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_yellow_sw1_and_blue_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 mtu 9198
```

```
 no shutdown
!
!
! INTER YELLOW SW 1 TO YELLOW SW2 ETHERCHANNEL (internal)
!
!
interface Port-channel2
 description Trunk_between_yellow_sw1_and_yellow_sw2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER YELLOW SW 1 TO YELLOW SW3 ETHERCHANNEL (internal)
!
!
interface Port-channel3
 description Trunk_between_yellow_sw1_and_yellow_sw3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER YELLOW SW1 TO BLUE SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description ISL_between_yellow_sw1_and_blue_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 switchport nonegotiate
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! INTER yellow SW1 TO yellow SW2 PORTS (internal)
!
!
Interface range GigabitEthernet 1/43 - 44
 description Trunk_between_yellow_sw1_and_yellow_sw2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
```

```
!
!
! INTER yellow SW1 TO yellow SW3 PORTS (internal)
!
!
Interface range GigabitEthernet 1/41 - 42
 description Trunk_between_yellow_sw1_and_yellow_sw3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface range GigabitEthernet 1/3 - 5
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/7 - 8
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/10
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! iLO PORTS
!
!
interface GigabitEthernet 1/6
description IMF iLO ports
switchport access vlan 300
 switchport mode access
 no shutdown
!
interface GigabitEthernet 1/9
 description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
```

```
!
!
! EAGLE PORTS
!
!
interface range GigabitEthernet 1/11 - 40
description Eagle FC or STC ports
 switchport access vlan 100
 switchport mode access
 mtu 9198
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH A
!
!
interface GigabitEthernet 1/47
 description to customer switch A
 switchport access vlan 400
 switchport mode access
 media-type rj45
 no shutdown
!
interface GigabitEthernet 1/48
 description reserved for optional direct access to ILO in case of disaster
 switchport access vlan 300
 switchport mode access
 media-type rj45
 no shutdown
!
!
! Laptop PORTS
!
!
interface range GigabitEthernet 1/45 - 46
 description for Laptop
 switchport access vlan 200
 switchport mode access
 media-type rj45
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 no ip address
!
!
interface VLAN 100
 ip address 172.21.49.1 255.255.254.0
 ip pim dense-mode
 no shutdown
!
```

```
!
track 1 int gigabitEthernet 1/47 line-protocol
interface Vlan200
 description internal VRRP for IMF to IXP traffic. Both IP addresses and
netmask must be configured according customer network.
 ip address 192.168.0.2 255.255.255.224    ! <--------- replace IP with the
value provided by the customer
 vrrp 1 ip 192.168.0.1         ! <--------- replace IP with default gateway
 vrrp 1 priority 100
 vrrp 1 track 1
 vrrp 1 preempt
 no shutdown
!
!
interface Vlan300
 description oobm or iLO optional IP. IP address and netmask must be
configured according customer network.
 ip address 192.168.10.2 255.255.255.240  ! <--------- replace IP with the
value provided by the customer
 no shutdown
!
!
interface Vlan 400
 description external VRRP for IMF to IXP traffic to Customer switches. Both
IP addresses and netmask must be configured according customer network.
 ip address 192.168.20.2 255.255.255.248  ! <--------- replace IP with the
value provided by the customer
 vrrp 2 ip 192.168.20.1        ! <--------- replace IP with default gateway
 vrrp 2 priority 100
 vrrp 2 preempt
 no shutdown
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.6 1    ! <--------- replace IP with
customer default gateway
!
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
no cdp run
!
end
```

14.4.6 Blue-sw1-1 Switch (Layer 3)

```
! IMF BLUE1 SWITCH configuration
!
!
hostname blue-sw1-1
!
no spanning-tree vlan 1-4094
no spanning-tree optimize bpdu transmission
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/47 line-protocol
ip subnet-zero
!
ip multicast-routing
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
!  INTER YELLOW SW1 TO BLUE SW1  ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_yellow_sw1_and_blue_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 mtu 9198
```

```
 no shutdown
!
!
! INTER BLUE SW 1 TO BLUE SW2 ETHERCHANNEL (internal)
!
!
interface Port-channel2
 description Trunk_between_ blue_sw1_and_ blue_sw2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER BLUE SW 1 TO BLUE SW3 ETHERCHANNEL (internal)
!
!
interface Port-channel3
 description Trunk_between_ blue_sw1_and_blue_sw3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER BLUE SW1 TO yellow SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description ISL_between_blue_sw1_and_yellow_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 switchport nonegotiate
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! INTER BLUE SW1 TO BLUE SW2 PORTS (internal)
!
!
Interface range GigabitEthernet 1/43 - 44
 description Trunk_between_blue_sw1_and_blue_sw2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
```

```
!
!
! INTER BLUE SW1 TO BLUE SW3 PORTS (internal)
!
!
Interface range GigabitEthernet 1/41 - 42
 description Trunk_between_blue_sw1_and_blue_sw3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface range GigabitEthernet 1/3 - 6
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/8 - 9
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! iLO PORTS
!
!
interface GigabitEthernet 1/7
description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
!
interface GigabitEthernet 1/10
 description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range GigabitEthernet 1/11 - 40
description Eagle FC or STC ports
```

```
 switchport access vlan 101
 switchport mode access
 mtu 9198
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH B
!
!
interface GigabitEthernet 1/47
 description to customer switch B
 switchport access vlan 400
 switchport mode access
 media-type rj45
 no shutdown
!
!
interface GigabitEthernet 1/48
 description not used to avoid loop risk on iLO VLAN.
 switchport access vlan 300
 switchport mode access
 media-type rj45
 shutdown
!
!
! Laptop PORTS
!
!
interface range GigabitEthernet 1/45 - 46
 description for Laptop
 switchport access vlan 200
 switchport mode access
 media-type rj45
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 no ip address
!
!
interface VLAN 101
 ip address 172.22.49.1 255.255.254.0
 ip pim dense-mode
 no shutdown
!
!
track 1 int gigabitEthernet 1/47 line-protocol
interface Vlan200
 description internal VRRP for IMF to IXP traffic. Both IP addresses and
netmask must be configured according customer network.
```

```
 ip address 192.168.0.3 255.255.255.224    ! <--------- replace IP with the
value provided by the customer
 vrrp 1 ip 192.168.0.1         ! <--------- replace IP with default gateway
 vrrp 1 priority 99
 vrrp 1 track 1
 vrrp 1 preempt
 no shutdown
!
!
interface Vlan 400
 description external VRRP for IMF to IXP traffic to Customer switches. Both
IP addresses and netmask must be configured according customer network.
 ip address 192.168.20.3 255.255.255.248  ! <--------- replace IP with the
value provided by the customer
 vrrp 2 ip 192.168.20.1        ! <--------- replace IP with default gateway
 vrrp 2 priority 99
 vrrp 2 preempt
 no shutdown
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.20.6 1    ! <--------- replace IP with
customer default gateway
!
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
no cdp run
!
end
```

14.4.7 Yellow-sw2-1 Switch (Layer 3)

```
! IMF YELLOW2 SWITCH configuration
!
!
hostname yellow-sw2-1
!
no spanning-tree vlan 1-4094
no spanning-tree optimize bpdu transmission
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
```

```
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/47 line-protocol
ip subnet-zero
!
ip multicast-routing
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
! INTER YELLOW SW 2 TO YELLOW SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel2
 description Trunk_between_yellow_sw2_and_yellow_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER yellow SW2 TO yellow SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description Trunk_between_yellow_sw2_and_yellow_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
```

```
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface GigabitEthernet 1/3
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/5 - 6
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/8 - 9
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/11
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! iLO PORTS
!
!
interface GigabitEthernet 1/4
description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
!
interface GigabitEthernet 1/7
 description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
!
interface GigabitEthernet 1/10
 description IMF iLO ports
```

```
 switchport access vlan 300
 switchport mode access
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range GigabitEthernet 1/12 - 48
description Eagle FC or STC ports
 switchport access vlan 100
 switchport mode access
 mtu 9198
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 no ip address
!
!
interface VLAN 100
 ip address 172.21.49.2 255.255.254.0
 ip pim dense-mode
 no shutdown!
!
interface Vlan200
 description for remote access though telnet
 ip address 192.168.0.4 255.255.255.224          ! <--------- replace IP with
the value provided by the customer
 no shutdown
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.0.1 1     ! <--------- replace IP with VLAN
200 vrrp IP
!
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
no cdp run
```

```
!
end
```

14.4.8 Blue-sw2-1 Switch (Layer 3)

```
! IMF BLUE2 SWITCH configuration
!
!
hostname blue-sw2-1
!
no spanning-tree vlan 1-4094
no spanning-tree optimize bpdu transmission
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/47 line-protocol
ip subnet-zero
!
ip multicast-routing
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
! INTER BLUE SW 2 TO BLUE SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel2
```

```
 description Trunk_between_ blue_sw2_and_ blue_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER BLUE SW2 TO BLUE SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description Trunk_between_blue_sw2_and_blue_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface range GigabitEthernet 1/3 - 4
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/6 - 7
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
interface range GigabitEthernet 1/9 - 10
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! iLO PORTS
!
!
interface GigabitEthernet 1/5
description IMF iLO ports
 switchport access vlan 300
 switchport mode access
```

```
 no shutdown
!
interface GigabitEthernet 1/8
 description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
!
interface GigabitEthernet 1/11
 description IMF iLO ports
 switchport access vlan 300
 switchport mode access
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range GigabitEthernet 1/12 - 48
description Eagle FC or STC ports
 switchport access vlan 101
 switchport mode access
 mtu 9198
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 no ip address
!
!
interface VLAN 101
 ip address 172.22.49.2 255.255.254.0
 ip pim dense-mode
 no shutdown
!
!
interface Vlan200
 description for remote access though telnet
 ip address 192.168.0.5 255.255.255.224         ! <--------- replace IP with
the value provided by the customer
 no shutdown
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.0.1 1     ! <--------- replace IP with VLAN
200 vrrp IP
!
!
line con 0
```

```
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
no cdp run
!
end
```

14.4.9 Yellow-sw3-1 Switch (Layer 3)

```
! IMF YELLOW3 SWITCH configuration
!
!
hostname yellow-sw3-1
!
no spanning-tree vlan 1-4094
no spanning-tree optimize bpdu transmission
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/47 line-protocol
ip subnet-zero
!
ip multicast-routing
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
```

```
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
! INTER YELLOW SW 3 TO YELLOW SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel3
 description Trunk_between_yellow_sw3_and_yellow_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER yellow SW3 TO yellow SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description Trunk_between_yellow_sw3_and_yellow_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range GigabitEthernet 1/3 - 48
description Eagle FC or STC ports
 switchport access vlan 100
 switchport mode access
 mtu 9198
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 no ip address
!
!
interface VLAN 100
 ip address 172.21.49.3 255.255.254.0
 ip pim dense-mode
```

```
 no shutdown
!
!
interface Vlan200
 description for remote access though telnet
 ip address 192.168.0.6 255.255.255.224          ! <--------- replace IP with
the value provided by the customer
 no shutdown
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.0.1 1     ! <--------- replace IP with yellow
VLAN 200 vrrp IP
!
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
no cdp run
!
end
```

14.4.10 Blue-sw3-1 Switch (Layer 3)

```
! IMF BLUE3 SWITCH configuration
!
!
hostname blue-sw3-1
!
no spanning-tree vlan 1-4094
no spanning-tree optimize bpdu transmission
!
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
service password-encryption
no service pad
service timestamps debug datetime
service timestamps log datetime
no logging console
no aaa new-model
track 1 interface GigabitEthernet1/47 line-protocol
ip subnet-zero
```

```
!
ip multicast-routing
!
power redundancy-mode redundant
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
! INTER BLUE SW 3 TO BLUE SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel3
 description Trunk_between_ blue_sw3_and_ blue_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 no shutdown
!
!
! INTER BLUE SW3 TO BLUE SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description Trunk_between_blue_sw3_and_blue_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 no shutdown
!
!
! EAGLE PORTS
!
!
```

```
interface range GigabitEthernet 1/3 - 48
description Eagle FC or STC ports
 switchport access vlan 101
 switchport mode access
 mtu 9198
 no shutdown
!
!
! VLAN INTERFACE CONFIGURATION
!
!
interface Vlan1
 no ip address
!
!
interface VLAN 101
 ip address 172.22.49.3 255.255.254.0
 ip pim dense-mode
 no shutdown!
!
interface Vlan200
 description for remote access though telnet
 ip address 192.168.0.7 255.255.255.224          ! <--------- replace IP with
the value provided by the customer
 no shutdown
!
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.0.1 1     ! <--------- replace IP with yellow
VLAN 200 vrrp IP
!
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
no cdp run
!
end
```

14.4.11 Single Switch yellow-blue-sw1-1

```
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
service compress-config
!
hostname yellow-blue-sw1-1
!
no logging console
!
no aaa new-model
ip subnet-zero
!
ip multicast-routing
vtp mode transparent
!
!
!
power redundancy-mode redundant
no file verify auto
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan internal allocation policy ascending
!
vlan 100
 name internal_yellow
!
vlan 101
 name internal_blue
!
vlan 200
 name IMF2IXP_internal_(backend)
!
vlan 300
 name oobm_or_iLO
!
vlan 400
 name IMF2IXP_external_(frontend)
!
!
!  INTER YELLOW SW1 TO BLUE SW1  ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Red_Wan_Trunk_between_Yellow_and_Blue (unused here but reserved)
 switchport
 switchport trunk encapsulation dot1q
 switchport mode trunk
```

```
 mtu 9198
!
!
! INTER YELLOW SW1 TO BLUE SW1 PORTS (internal)
!
!
Interface range GigabitEthernet 1/1 - 2
 description Red_Wan_Trunk_between_Yellow_and_Blue (unused here but reserved)
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
!
!
! IMF Servers PORTS
!
!
interface range GigabitEthernet1/3 - 4
 description for IMF 1A external + internal networks port
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300,400
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! EAGLE PORTS
!
!
interface range GigabitEthernet1/5 - 24
description yellow network port for Eagle connectivity
 switchport access vlan 100
 switchport mode access
 mtu 9198
 spanning-tree portfast
!
!
interface GigabitEthernet1/25-44
description blue network port for Eagle connectivity
switchport access vlan 101
switchport mode access
 mtu 9198
 spanning-tree portfast
!
interface range GigabitEthernet1/45-46
description unused
shutdown
!
!
! PORT TO CUSTOMER SWITCH A
!
!
interface GigabitEthernet1/47
 description port where customer is connected to IMF
```

```
 switchport access vlan 400
 switchport mode access
 media-type rj45
!
interface GigabitEthernet1/48
description port where customer is connected to ILO
 switchport access vlan 300
 switchport mode access
 media-type rj45
!
interface Vlan1
 no ip address
!
interface Vlan100
 ip address 172.21.49.1 255.255.254.0
 no ip route-cache cef
 no ip route-cache
 no shutdown
!
!
interface Vlan400
 ip address 10.27.56.166 255.255.255.240  ! <--------- replace IP with an
address from customer network
 no shutdown
!
no ip http server
no ip http secure-server
!
!
logging 172.21.49.10
no cdp run
!
End
```

14.4.12 T1200 & HP Layer 2 switch configurations (PIC 9.x and earlier)

14.4.12.1 Yellow-sw1-1

```
!
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
no logging console
!
hostname yellow-sw1-1
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
```

```
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 40960
!
ip multicast-routing
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
!  INTER YELLOW SW1 TO BLUE SW1  ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Red_Wan_Trunk_between_Yellow_and_Blue
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER YELLOW SW 1 TO YELLOW SW2 ETHERCHANNEL (internal)
!
!
interface Port-channel2
 description Trunk_between_Yellow_sw1_and_Yellow_sw2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER YELLOW SW 1 TO YELLOW SW3 ETHERCHANNEL (internal)
!
!
interface Port-channel3
 description Trunk_between_Yellow_sw1_and_Yellow_sw3
```

```
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER YELLOW SW1 TO BLUE SW1 PORTS (internal)
!
!
interface range gigabitEthernet 1/1 - 2
description ISL_between_yellow_sw1_and_blue_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! INTER yellow SW1 TO yellow SW3 PORTS (internal)
!
!
interface range gigabitEthernet 1/41 - 42
description Trunk_between_yellow_sw1_and_yellow_sw3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 3 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! INTER yellow SW1 TO yellow SW2 PORTS (internal)
!
!
interface range gigabitEthernet 1/43 - 44
description Trunk_between_yellow_sw1_and_yellow_sw2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 2 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/3 - 5
```

```
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface range gigabitEthernet 1/7 - 8
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface gigabitEthernet 1/10
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! iLO PORTS
!
!
interface gigabitEthernet 1/6
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
interface gigabitEthernet 1/9
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/11 - 40
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
```

```
! Laptop PORTS
!
!
interface range GigabitEthernet 1/45 - 46
 description for Laptop
 switchport access vlan 200
 switchport mode access
 media-type rj45
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH A
!
!
interface gigabitEthernet 1/47
description to customer switch A
 switchport mode access
 switchport access vlan 200
 media-type rj45
 no shutdown
!
interface gigabitEthernet 1/48
description to customer switch A (iLO)
 switchport mode access
 switchport access vlan 300
 media-type rj45
 no shutdown
!
interface VLAN 100
 ip address 172.21.49.1 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
```

```
end
```

14.4.12.2 *Blue-sw1-1*

```
!
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
no logging console
!
hostname blue-sw1-1
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 40960
!
ip multicast-routing
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
!  INTER YELLOW SW1 TO BLUE SW1  ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Red_Wan_Trunk_between_Yellow_and_Blue
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
```

```
 spanning-tree portfast trunk
!
!
! INTER BLUE SW 1 TO BLUE SW2 ETHERCHANNEL (internal)
!
!
interface Port-channel2
 description Trunk_between_Blue_sw1_and_Blue_sw2
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER BLUE SW 1 TO BLUE SW3 ETHERCHANNEL (internal)
!
!
interface Port-channel3
 description Trunk_between_Blue_sw1_and_Blue_sw3
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 spanning-tree portfast trunk
!
!
! INTER BLUE SW1 TO yellow SW1 PORTS (internal)
!
!
interface range gigabitEthernet 1/1 - 2
description ISL_between_blue_sw1_and_yellow_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! INTER BLUE SW1 TO BLUE SW3 PORTS (internal)
!
!
interface range gigabitEthernet 1/41 - 42
description Trunk_between_blue_sw1_and_blue_sw3
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 channel-group 3 mode active
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
```

```
!
!
! INTER BLUE SW1 TO BLUE SW2 PORTS (internal)
!
!
interface range gigabitEthernet 1/43 - 44
description Trunk_between_blue_sw1_and_blue_sw2
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 channel-group 2 mode active
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/3 - 6
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface range gigabitEthernet 1/8 - 9
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! iLO PORTS
!
!
interface gigabitEthernet 1/7
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
interface gigabitEthernet 1/10
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
!
```

```
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/11 - 40
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
! Laptop PORTS
!
!
interface range GigabitEthernet 1/45 - 46
 description for Laptop
 switchport access vlan 200
 switchport mode access
 media-type rj45
 no shutdown

!
!
! PORT TO CUSTOMER SWITCH B
!
!
interface gigabitEthernet 1/47
description to customer switch B
 switchport mode access
 switchport access vlan 200
 media-type rj45
 no shutdown
!
interface gigabitEthernet 1/48
description to customer switch B (iLO)
 switchport mode access
 switchport access vlan 300
 media-type rj45
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.1 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
```

```
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.12.3 Yellow-sw2-1

```
!
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
no logging console
!
hostname yellow-sw2-1
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
boot-start-marker
boot system flash bootflash:cat4500-ipbasek9-mz.122-53.SG2.bin
boot-end-marker
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 53248
!
ip multicast-routing
!
!
! VLAN CONFIGURATION (internal)
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
```

```
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! INTER YELLOW SW 2 TO YELLOW SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_Yellow_sw2_and_Yellow_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER yellow SW2 TO yellow SW1 PORTS (internal)
!
!
interface range gigabitEthernet 1/1 - 2
description Trunk_between_yellow_sw2_and_yellow_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface gigabitEthernet 1/3
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface range gigabitEthernet 1/5 - 6
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
```

```
interface range gigabitEthernet 1/8 - 9
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface gigabitEthernet 1/11
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! iLO PORTS
!
!
interface gigabitEthernet 1/4
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
interface gigabitEthernet 1/7
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
interface gigabitEthernet 1/10
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/12 - 48
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
!
interface VLAN 100
```

```
 ip address 172.21.49.2 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
end
```

14.4.12.4 Blue-sw2-1

```
!
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
no logging console
!
hostname blue-sw2-1
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 53248
!
ip multicast-routing
!
!
! VLAN CONFIGURATION (internal)
```

```
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! INTER BLUE SW 2 TO BLUE SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_Blue_sw2_and_Blue_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER BLUE SW2 TO BLUE SW1 PORTS (internal)
!
!
interface range gigabitEthernet 1/1 - 2
description Trunk_between_blue_sw2_and_blue_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/3 - 4
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface range gigabitEthernet 1/6 - 7
```

```
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
interface range gigabitEthernet 1/9 - 10
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! iLO PORTS
!
!
interface gigabitEthernet 1/5
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
interface gigabitEthernet 1/8
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
interface gigabitEthernet 1/11
description IMF iLO ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/12 - 48
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.2 255.255.254.0
```

```
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.12.5 Yellow-sw3-1

```
!
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
no logging console
!
hostname yellow-sw3-1
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 53248
!
ip multicast-routing
!
!
! VLAN CONFIGURATION (internal)
!
```

```
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! INTER YELLOW SW 3 TO YELLOW SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_Yellow_sw3_and_Yellow_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER yellow SW3 TO yellow SW1 PORTS (internal)
!
!
interface range gigabitEthernet 1/1 - 2
description Trunk_between_yellow_sw3_and_yellow_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/3 - 48
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
!
interface VLAN 100
 ip address 172.21.49.3 255.255.254.0
```

```
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
end
```

14.4.12.6 Blue-sw3-1

```
!
no service pad
service timestamps debug datetime
service timestamps log datetime
service password-encryption
no logging console
!
hostname blue-sw3-1
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
spanning-tree vlan 1-1024 priority 53248
!
ip multicast-routing
!
!
! VLAN CONFIGURATION (internal)
!
```

```
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! INTER BLUE SW 3 TO BLUE SW 1 ETHERCHANNEL (internal)
!
!
interface Port-channel1
 description Trunk_between_Blue_sw3_and_Blue_sw1
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
!
!
! INTER BLUE SW3 TO BLUE SW1 PORTS (internal)
!
!
interface range gigabitEthernet 1/1 - 2
description Trunk_between_blue_sw3_and_blue_sw1
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 1,100,101,200,300
 switchport mode trunk
 mtu 9198
 channel-group 1 mode active
 spanning-tree portfast trunk
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/3 - 48
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.3 255.255.254.0
```

```
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.13 T1100 Switch 4948 Configurations

All or no vlan	vlan 100 yellow	vlan 101 blue	vlan 200 backend	vlan 300 oobm or iLO

Yellow SW2-2

Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45	Port 47 SW1-2 Port 48
Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46	Port 48

Yellow SW1-2

Port 1 ServerG eth91	Port 3 ServerI eth91	Port 5 ServerK eth91	Port 7	Port 9	Port 11	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45	Port 47 SW1-1 SW2-1
Port 2 ServerH eth91	Port 4 ServerJ eth91	Port 6 ServerL eth91	Port 8	Port 10	Port 12	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46	Port 48 SW2-2 Port 47

Yellow SW2-1

Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45	Port 47 SW1-1 Port 48
Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46	Port 48 SW1-2 Port 47

Yellow SW1-1

Port 1 ServerA eth91	Port 3 ServerC eth91	Port 5 ServerE eth91	Port 7 For laptop	Port 9 For laptop	Port 11 For laptop	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45 Blue1 SW P45	Port 47 Cust Net eth
Port 2 ServerB eth91	Port 4 ServerD eth91	Port 6 ServerF eth91	Port 8 For laptop	Port 10 For laptop	Port 12 For laptop	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46 Cust Net OOBM	Port 48 SW2-1 SW1-2

Blue SW1-1

Port 1 ServerA OOBM	Port 3 ServerC OOBM	Port 5 ServerE OOBM	Port 7 ServerA eth93	Port 9 ServerC eth93	Port 11 ServerE eth93	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45 Yellow1 SW P45	Port 47 Cust Net eth
Port 2 ServerB OOBM	Port 4 ServerD OOBM	Port 6 ServerF OOBM	Port 8 ServerB eth93	Port 10 ServerD eth93	Port 12 ServerF eth93	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46 Cust Net OOBM	Port 48 SW2-1 SW1-2

Blue SW2-1

Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45	Port 47 SW1-1 Port 48
Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46	Port 48 SW1-2 Port 47

Blue SW1-2

Port 1 ServerG OOBM	Port 3 ServerI OOBM	Port 5 ServerK OOBM	Port 7 ServerG eth93	Port 9 ServerI eth93	Port 11 ServerK eth93	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45	Port 47 SW1-1 SW2-1
Port 2 ServerH OOBM	Port 4 ServerJ OOBM	Port 6 ServerL OOBM	Port 8 ServerH eth93	Port 10 ServerJ eth93	Port 12 ServerL eth93	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46	Port 48 SW2-2 Port 47

Blue SW2-2

Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	Port 25 Eagle Links	Port 27 Eagle Links	Port 29 Eagle Links	Port 31 Eagle Links	Port 33 Eagle Links	Port 35 Eagle Links	Port 37 Eagle Links	Port 39 Eagle Links	Port 41 Eagle Links	Port 43 Eagle Links	Port 45	Port 47 SW1-2 Port 48
Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Port 26 Eagle Links	Port 28 Eagle Links	Port 30 Eagle Links	Port 32 Eagle Links	Port 34 Eagle Links	Port 36 Eagle Links	Port 38 Eagle Links	Port 40 Eagle Links	Port 42 Eagle Links	Port 44 Eagle Links	Port 46	Port 48

14.4.13.1 Frame 1

14.4.13.1.1 Yellow-sw1-1

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname yellow-sw1-1
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
ip multicast-routing
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/1 - 6
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! Laptop PORTS
!
!
```

```
interface range gigabitEthernet 1/7-12
description for Laptops
 switchport mode access
 switchport acces vlan 200
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/13 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
exit
!
!
!  INTER YELLOW SW1 TO BLUE SW1
!
!
interface gigabitEthernet 1/45
description to Blue1-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH OOBM VLAN
!
!
interface gigabitEthernet 1/46
description to customer switch OOBM VLAN
 switchport mode access
 switchport access vlan 300
 media-type rj45
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH A
!
!
interface gigabitEthernet 1/47
description to customer switch A
 switchport mode access
 switchport access vlan 200
 media-type rj45
 no shutdown
!
```

```
!
!  INTER YELLOW SWITCH
!
!
interface gigabitEthernet 1/48
description to Yellow2-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
interface VLAN 100
 ip address 172.21.49.1 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
end
```

14.4.13.1.2 Blue-sw1-1

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname blue-sw1-1
```

```
enable secret ***** ! <--------- replace ***** with password specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
ip multicast-routing
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/7 - 12
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
!
! OOBM PORTS
!
!
interface range gigabitEthernet 1/1 - 6
description IMF OOBM ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown

!
!
! EAGLE PORTS
!
!
```

```
interface range gigabitEthernet 1/13 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER YELLOW SW1 TO BLUE SW1
!
!
interface gigabitEthernet 1/45
description to Blue1-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH OOBM VLAN
!
!
interface gigabitEthernet 1/46
description to customer switch OOBM VLAN
 switchport mode access
 switchport access vlan 300
 media-type rj45
 no shutdown
!
!
! PORT TO CUSTOMER SWITCH B
!
!
interface gigabitEthernet 1/47
description to customer switch A
 switchport mode access
 switchport access vlan 200
 media-type rj45
 no shutdown
!
!
!  INTER BLUE SWITCH
!
!
interface gigabitEthernet 1/48
description to Blue2-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
```

```
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.1 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.13.1.3 Yellow-sw2-1

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname yellow-sw2-1
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
```

```
ip multicast-routing
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/1 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER YELLOW SWITCH
!
!
interface gigabitEthernet 1/47
description to Yellow1-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
!
!  INTER YELLOW SWITCH
!
!
interface gigabitEthernet 1/48
description to Yellow1-2 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
interface VLAN 100
 ip address 172.21.49.2 255.255.254.0
```

```
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
end
```

14.4.13.1.4 Blue-sw2-1

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname blue-sw2-1
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
ip multicast-routing
!
vlan 100
 name yellow
```

```
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/1 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER BLUE SWITCH
!
!
interface gigabitEthernet 1/47
description to Blue1-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
!
!  INTER BLUE SWITCH
!
!
interface gigabitEthernet 1/48
description to Blue1-2 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.2 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
```

```
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.13.2 **Frame** *2*

14.4.13.2.1 Yellow-sw1-2

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname yellow-sw1-2
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
ip multicast-routing
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
```

```
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/1 - 6
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! EAGLE PORTS
!
!
interface gigabitEthernet 1/13 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER YELLOW SWITCH
!
!
interface gigabitEthernet 1/47
description to Yellow2-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
!
!  INTER YELLOW SWITCH
!
!
interface gigabitEthernet 1/48
description to Yellow2-2 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
```

```
 no shutdown
!
interface VLAN 100
 ip address 172.21.49.3 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
end
```

14.4.13.2.2 Blue-sw1-2

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname blue-sw1-2
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
```

```
ip multicast-routing
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! IMF Servers PORTS
!
!
interface range gigabitEthernet 1/7 - 12
description IMF servers ports
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 no shutdown
!
!
! OOBM PORTS
!
!
interface range gigabitEthernet 1/1 - 6
description IMF OOBM ports
 switchport mode access
 switchport access vlan 300
 spanning-tree portfast
 no shutdown
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/13 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER BLUE SWITCH
!
!
interface gigabitEthernet 1/47
```

```
description to Blue2-1 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
!
!  INTER BLUE SWITCH
!
!
interface gigabitEthernet 1/48
description to Blue2-2 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.3 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.13.2.3 Yellow-sw2-2

```
!
no service pad
service timestamps debug uptime
```

```
service timestamps log uptime
service password-encryption
no logging console
!
hostname yellow-sw2-2
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
ip multicast-routing
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/1 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 100
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER YELLOW SWITCH
!
!
interface gigabitEthernet 1/47
description to Yellow1-2 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 mtu 9198
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
```

```
!
interface VLAN 100
 ip address 172.21.49.4 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.21.49.10
!
end
```

14.4.13.2.4 Blue-sw2-2

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
no logging console
!
hostname blue-sw2-2
enable secret ***** ! <--------- replace ***** with password
specified in password dragon as Cisco enable
!
ip subnet-zero
vtp mode transparent
!
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
ip multicast-routing
```

```
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! EAGLE PORTS
!
!
interface range gigabitEthernet 1/1 - 44
description Eagle FC or STC ports
 switchport mode access
 switchport access vlan 101
 mtu 9198
 spanning-tree portfast
 no shutdown
!
!
!  INTER BLUE SWITCH
!
!
interface gigabitEthernet 1/47
description to Blue1-2 switch
 switchport trunk encapsulation dot1q
 switchport mode trunk
 spanning-tree portfast trunk
 media-type rj45
 no shutdown
!
interface VLAN 101
 ip address 172.22.49.4 255.255.254.0
 ip pim dense-mode
 no shutdown
!
no ip route-cache
!
no ip http server
!
no cdp run
!
line con 0
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 0 4
```

```
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified
in password dragon as Cisco telnet
 login
!
logging 172.22.49.10
!
end
```

14.4.14 T1100 Switch 2950 Configurations

All or no vlan	vlan 100 yellow	vlan 101 blue	vlan 200 backend	vlan 300 oobm or iLO

Yellow SW2-2	Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 YSW1-2 GbPort 2
	Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	Free
Yellow SW1-2	Port 1 ServerG eth91	Port 3 ServerI eth91	Port 5 ServerK eth91	Port 7 Free	Port 9 Free	Port 11 Free	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 YSW2-1 GbPort 2
	Port 2 ServerH eth91	Port 4 ServerJ eth91	Port 6 ServerL eth91	Port 8 Free	Port 10 Free	Port 12 Free	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	GbPort 2 YSW2-2 GbPort 1
Yellow SW2-1	Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 YSW1-1 GbPort 2
	Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	GbPort 2 YSW1-2 GbPort 1
Yellow SW1-1	Port 1 Cust Net eth	Port 3 ServerA eth91	Port 5 ServerC eth91	Port 7 ServerE eth91	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 BSW1-1 GbPort 1
	Port 2 Cust Net eth	Port 4 ServerB eth91	Port 6 ServerD eth91	Port 8 ServerF eth91	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	GbPort 2 YSW2-1 GbPort 1
Blue SW1-1	Port 1 Cust Net eth	Port 3 ServerA eth93	Port 5 ServerC eth93	Port 7 ServerF eth93	Port 9 ServerA OOBM	Port 11 ServerC OOBM	Port 13 ServerE OOBM	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 YSW1-1 GbPort 1
	Port 2 Cust Net eth	Port 4 ServerB eth93	Port 6 ServerD eth93	Port 8 ServerE eth93	Port 10 ServerB OOBM	Port 12 ServerD OOBM	Port 14 ServerF OOBM	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	GbPort 2 BSW2-1 GbPort 1
Blue SW2-1	Port 1 Eagle Links	Port 3 Eagle Links	Port 5 Eagle Links	Port 7 Eagle Links	Port 9 Eagle Links	Port 11 Eagle Links	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 BSW2-1 GbPort 2
	Port 2 Eagle Links	Port 4 Eagle Links	Port 6 Eagle Links	Port 8 Eagle Links	Port 10 Eagle Links	Port 12 Eagle Links	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	GbPort 2 BSW1-2 GbPort 1
Blue SW1-2	Port 1 ServerG eth93	Port 3 ServerI eth93	Port 5 ServerK eth93	Port 7 ServerG OOBM	Port 9 ServerI OOBM	Port 11 ServerK OOBM	Port 13 Eagle Links	Port 15 Eagle Links	Port 17 Eagle Links	Port 19 Eagle Links	Port 21 Eagle Links	Port 23 Eagle Links	GbPort 1 BSW1-1 GbPort 1
	Port 2 ServerH eth93	Port 4 ServerJ eth93	Port 6 ServerL eth93	Port 8 ServerH OOBM	Port 10 ServerJ OOBM	Port 12 ServerL OOBM	Port 14 Eagle Links	Port 16 Eagle Links	Port 18 Eagle Links	Port 20 Eagle Links	Port 22 Eagle Links	Port 24 Eagle Links	GbPort 2 BSW2-2 GbPort 1
	Port 1	Port 3	Port 5	Port 7	Port 9	Port 11	Port 13	Port 15	Port 17	Port 19	Port 21	Port 23	GbPort 1

14.4.14.1 Frame 1

14.4.14.1.1 Yellow-sw1-1

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname yellow-sw1-1
!
no logging console
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
!
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! PORT TO CUSTOMER SWITCH A
!
!
interface range FastEthernet0/1 - 2
description to customer switch A
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
!
! IMF Servers PORTS
!
!
interface range FastEthernet0/3 - 8
description IMF servers ports
```

```
 switchport mode trunk
 spanning-tree portfast trunk
!
!
! EAGLE PORTS
!
!
interface range FastEthernet0/9 - 24
description Eagle FC or STC ports
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
!
!
!  INTER YELLOW SW1 TO BLUE SW1
!
!
interface GigabitEthernet0/1
description to Blue1-1 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
!
!  INTER YELLOW SWITCH
!
!
interface GigabitEthernet0/2
description to Yellow2-1 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan100
 ip address 172.21.49.1 255.255.254.0
 no ip route-cache
!
no ip http server
logging 172.21.49.10
no cdp run
snmp-server community public RO
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps vtp
snmp-server host 172.21.49.10 version 2c public
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
```

```
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
!
end
```

14.4.14.1.2 **Blue-sw1-1**

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname blue-sw1-1
!
no logging console
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
!
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! PORT TO CUSTOMER SWITCH OOBM VLAN
!
!
interface FastEthernet0/1
```

```
description to customer switch OOBM VLAN
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast
!
!
! PORT TO CUSTOMER SWITCH A
!
!
interface FastEthernet0/2
description to customer switch A
 switchport access vlan 200
 switchport mode access
 spanning-tree portfast
!
!
! IMF Servers PORTS
!
!
interface range FastEthernet0/3 - 8
description IMF servers ports
 switchport mode trunk
 spanning-tree portfast trunk
!
!
!
! OOBM PORTS
!
!
interface range FastEthernet0/9 -14
description IMF OOBM ports
 switchport access vlan 300
 switchport mode access
 spanning-tree portfast
!
!
! EAGLE PORTS
!
!
interface range FastEthernet0/15 - 24
description Eagle FC or STC ports
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast
!
!
!  INTER YELLOW SW1 TO BLUE SW1
!
!
interface GigabitEthernet0/1
description to Yellow1-1 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
```

```
!
!  INTER BLUE SWITCH
!
!
interface GigabitEthernet0/2
description to Blue2-1 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan101
 ip address 172.22.49.1 255.255.254.0
 no ip route-cache
!
no ip http server
logging 172.22.49.10
no cdp run
snmp-server community public RO
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps vtp
snmp-server host 172.21.49.10 version 2c public
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
!
end
```

14.4.14.1.3 **Yellow-sw2-1**

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname yellow-sw2-1
!
```

```
no logging console
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
!
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
!
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! EAGLE PORTS
!
!
interface range FastEthernet0/1 - 24
description Eagle FC or STC ports
 switchport access vlan 100
 switchport mode access
 spanning-tree portfast
!
!
!  INTER YELLOW SWITCH
!
!
interface GigabitEthernet0/1
description to Yellow1-1 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet0/2
description to Yellow1-2 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 no ip route-cache
```

```
 shutdown
!
interface Vlan100
 ip address 172.21.49.2 255.255.254.0
 no ip route-cache
!
no ip http server
logging 172.21.49.10
no cdp run
snmp-server community public RO
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
snmp-server enable traps vtp
snmp-server host 172.21.49.10 version 2c public
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
!
end
```

14.4.14.1.4 **Blue-sw2-1**

```
!
no service pad
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname blue-sw2-1
!
no logging console
enable secret ***** ! <--------- replace ***** with password specified in
password dragon as Cisco enable
!
ip subnet-zero
!
vtp mode transparent
!
spanning-tree mode pvst
no spanning-tree optimize bpdu transmission
spanning-tree extend system-id
!
```

```
!
!
!
vlan 100
 name yellow
!
vlan 101
 name blue
!
vlan 200
 name cust
!
vlan 300
 name oobm
!
!
! EAGLE PORTS
!
!
interface range FastEthernet0/1 - 24
description Eagle FC or STC ports
 switchport access vlan 101
 switchport mode access
 spanning-tree portfast
!
!
!  INTER BLUE SWITCH
!
!
interface GigabitEthernet0/1
description to Blue1-1 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
interface GigabitEthernet0/2
description to Blue1-2 switch
 switchport mode trunk
 spanning-tree portfast trunk
!
interface Vlan1
 no ip address
 no ip route-cache
 shutdown
!
interface Vlan101
 ip address 172.22.49.2 255.255.254.0
 no ip route-cache
!
no ip http server
logging 172.22.49.10
no cdp run
snmp-server community public RO
snmp-server enable traps snmp authentication warmstart linkdown linkup
coldstart
```

```
snmp-server enable traps vtp
snmp-server host 172.21.49.10 version 2c public
!
line con 0
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 0 4
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
line vty 5 15
 password ***** ! <--------- replace ***** with password specified in
password dragon as Cisco telnet
 login
!
!
end
```

14.4.15 IMF MTU Configurations

On IMF in order to support Fast Copy, the MTU of the bond0, bond0.100 and bond0.101 interfaces is configured to 2000, however Cisco switch 2950 doesnitch IPopulate a column called , can cause temporary bridging loops.. In the s configured globably for the switch unlike Cisco 4948 switch, where MTU can be configured per interface. Usually the Cisco switches are not used to monitor the Fast Copy traffic and they may be configured with default MTU of 1500, however the MTU can be configured to different value as per the switch configuration. Following table can be taken as reference for MTU.

Cisco Switch	XMF Mode	MTU
2950	STC Copy	1500
2950	Fast Copy	1530
4948	All	2000

14.4.15.1 Procedure to configure the MTU

STEP #	Steps to be completed.	This procedure outlines the steps for configuring MTU on Cisco 2950 Switches and IMFs T1100
1	Take note of existing Switch Connections.	Take note of all existing Yellow and Blue Switch connections.
2	Copy blue-sw1-1 running config to startup config	bue-sw1-1# copy run start
3	Copy yellow-sw1-1 running config to startup config	yellow-sw1-1# copy run start
4	Set blue-sw1-1 switch MTU setting	blue-sw1-1(config)#system mtu 1530
5	Set yellow-sw1-1 switch MTU setting	yellow-sw1-1(config)#system mtu 1530
6	Set Stand-by IMF eth91 MTU to 1530	1. Add MTU="1530" to ifcfg-eth91 file under /etc/sysconfig/network-scripts Initiate service network restart
7	Set Stand-by IMF bond0 MTU to 1530	1. Add MTU="1530" to ifcfg-bond0 file under /etc/sysconfig/network-scripts 2. Initiate service network restart
8	Set Stand-by IMF bond0.100 MTU to 1530	1. Add MTU="1530" to ifcfg-bond0.100 file under /etc/sysconfig/network-scripts 2. Initiate service network restart
9	Set Stand-by IMF bond0.101 MTU to 1530	1. Add MTU="1530" to ifcfg-bond0.101 file under /etc/sysconfig/network-scripts 2. Initiate service network restart
10	Save Cisco 2950 yellow-sw1-1 running config to startup config	2. yellow-sw1-1# copy run start
11	Save Cisco 2950 blue-sw1-1 running config to startup config	3. blue-sw1-1# copy run start

15 Network ports between PIC components

Client	Source IP	Server	Destination IP	Port	Transport	Protocol	Description by port	VLAN by port	Optional
IXP	Rules for IXP RSP ES	IXP_ES	IXP Export Server	7	TCP/UDP	echo	Linux echo test protocol	Admin	N
NSP_PRIMARY	Weblogic server	xMF	IMF and PMF servers	7	TCP/UDP	echo	Linux echo test protocol	Admin	N
NSP_SECONDARY	Weblogic server	xMF	IMF and PMF servers	7	TCP/UDP	echo	Linux echo test protocol	Admin	N
xMF	IMF and PMF servers	NSP_PRIMARY	Weblogic server	7	TCP/UDP	echo	Linux echo test protocol	Admin	N
xMF	IMF and PMF servers	NSP_SECONDARY	Weblogic server	7	TCP/UDP	echo	Linux echo test protocol	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
NSP_PRIMARY	Weblogic server	Customer_source	SFTP source for automatic FSE updates	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	ILO	ILO range	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
NSP_PRIMARY	Weblogic server	IXP	Rules for IXP RSP ES	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
NSP_SECONDARY	Weblogic server	IXP	Rules for IXP RSP ES	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	IXP	Rules for IXP RSP ES	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	IXP	Rules for IXP RSP ES	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Customer_feed	Data export server	IXP_ES	IXP Export Server	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	NSP_APACHE_BACK	NSP back-end side (application)	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_APACHE_BACK	NSP back-end side (application)	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	NSP_ORACLE	Central configuration	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_ORACLE	Central configuration	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	NSP_PRIMARY	Weblogic server	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_PRIMARY	Weblogic server	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	NSP_SECONDARY	Weblogic server	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_SECONDARY	Weblogic server	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N

PM&C	DL360 PMAC	OA	Blade on-board administrator	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	PM&C	DL360 PMAC	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	SAN_Controller	P2000 or MSA2012 controllers	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	SAN_Controller	P2000 or MSA2012 controllers	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	SAN_SWITCH	Brocade switch	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	SAN_SWITCH	Brocade switch	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
NSP_PRIMARY	Weblogic server	xMF	IMF and PMF servers	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
NSP_SECONDARY	Weblogic server	xMF	IMF and PMF servers	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	xMF	IMF and PMF servers	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	xMF	IMF and PMF servers	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
PM&C	DL360 PMAC	SWITCH	Cisco managed switches	23	TCP	telnet	Telnet protocol	Admin	N
NSP_PRIMARY	Weblogic server	Customer_MAIL	Mail server to forward alarms	25	TCP	smtp	Simple Mail Transfer Protocol	Admin	Y
NSP_SECONDARY	Weblogic server	Customer_MAIL	Mail server to forward alarms	25	TCP	smtp	Simple Mail Transfer Protocol	Admin	Y
IXP	Rules for IXP RSP ES	PM&C	DL360 PMAC	69	UDP	tftp	Trivial File Transfer Protocol	Admin	LAN
NSP_APACHE_BACK	NSP back-end side (application)	PM&C	DL360 PMAC	69	UDP	tftp	Trivial File Transfer Protocol	Admin	LAN
NSP_ORACLE	Central configuration	PM&C	DL360 PMAC	69	UDP	tftp	Trivial File Transfer Protocol	Admin	LAN
NSP_PRIMARY	Weblogic server	PM&C	DL360 PMAC	69	UDP	tftp	Trivial File Transfer Protocol	Admin	LAN
NSP_SECONDARY	Weblogic server	PM&C	DL360 PMAC	69	UDP	tftp	Trivial File Transfer Protocol	Admin	LAN
SWITCH	Cisco managed switches	PM&C	DL360 PMAC	69	UDP	tftp	Trivial File Transfer Protocol	Admin	LAN
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS
Tekelec_Admin	Admin remote or jumpoff or VPN	ILO	ILO range	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS
Customer_Workstation	End user LAN	NSP_APACHE_FRONT	NSP front-end side (web clients)	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS

Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_APACHE_FRONT	NSP front-end side (web clients)	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS
OA	Blade on-board administrator	PM&C	DL360 PMAC	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS
IXP	Rules for IXP RSP ES	Customer_feed	Data export server	111	TCP	portmap	NFS dynamic port mapping	Admin	N
IXP	Rules for IXP RSP ES	IXP_ES	IXP Export Server	111	TCP	portmap	NFS dynamic port mapping	Admin	N
IXP	Rules for IXP RSP ES	IXP_PDU	Pool PDU storage	111	TCP	portmap	NFS dynamic port mapping	Admin	N
IXP	Rules for IXP RSP ES	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
MSW	Legacy Message Switch	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
NSP_APACHE_BACK	NSP back-end side (application)	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
NSP_ORACLE	Central configuration	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
NSP_PRIMARY	Weblogic server	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
NSP_SECONDARY	Weblogic server	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
OA	Blade on-board administrator	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
PM&C	DL360 PMAC	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
SAN_Controller	P2000 or MSA2012 controllers	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N

SAN_Switch	Brocade switch	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
SWITCH	Cisco managed switches	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
xMF	IMF and PMF servers	NTP_Server	Customer NTP and/or NSP Apache Back End	123	UDP	ntp	Network Time Protocol (sync)	Admin	N
NSP_SECONDARY	Weblogic server	Customer_SNMP	Alarm forwarding destination	161	UDP	snmp.a	Simple Network Management Protocol (MIB query)	Admin	N
Customer_SNMP	Alarm forwarding destination	NSP_PRIMARY	Weblogic server	161	UDP	snmp.a	Simple Network Management Protocol (MIB query)	Admin	N
NSP_PRIMARY	Weblogic server	Customer_SNMP	Alarm forwarding destination	162	UDP	snmp.b	Simple Network Management Protocol (traps)	Admin	Y
OA	Blade on-board administrator	NSP_PRIMARY	Weblogic server	162	UDP	snmp.b	Simple Network Management Protocol (traps)	Admin	Y
SAN_Controller	P2000 or MSA2012 controllers	NSP_PRIMARY	Weblogic server	162	UDP	snmp.b	Simple Network Management Protocol (traps)	Admin	Y
SAN_SWITCH	Brocade switch	NSP_PRIMARY	Weblogic server	162	UDP	snmp.b	Simple Network Management Protocol (traps)	Admin	Y
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	ILO	ILO range	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Customer_Workstation	End user LAN	NSP_APACHE_FRON	NSP front-end side (web clients)	443	TCP/UDP	https	Hyper Text Transfer Protocol	Data	N

		T					Secure (web)		
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_APACHE_FRONT	NSP front-end side (web clients)	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	OA	Blade on-board administrator	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	PM&C	DL360 PMAC	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	SAN_Controller	P2000 or MSA2012 controllers	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	SAN_SWITCH	Brocade switch	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	SWITCH	Cisco managed switches	443	TCP/UDP	https	Hyper Text Transfer Protocol Secure (web)	Data	N
NSP_PRIMARY	Weblogic server	IXP	Rules for IXP RSP ES	1099	TCP	RMI	RMI Registry Java Remote Procedure Invokation	Admin	N
NSP_SECONDARY	Weblogic server	IXP	Rules for IXP RSP ES	1099	TCP	RMI	RMI Registry Java Remote Procedure Invokation	Admin	N
MSW	Legacy Message Switch	MSW	Legacy Message Switch	1099	TCP	RMI	RMI Registry Java Remote Procedure Invokation	Admin	N
IXP	Rules for IXP RSP ES	NSP_PRIMARY	Weblogic server	1099	TCP	RMI	RMI Registry Java Remote Procedure Invokation	Admin	N
NSP_PRIMARY	Weblogic server	xMF	IMF and PMF servers	1099	TCP	RMI	RMI Registry Java Remote Procedure Invokation	Admin	N
NSP_SECONDARY	Weblogic server	xMF	IMF and PMF servers	1099	TCP	RMI	RMI Registry Java Remote Procedure Invokation	Admin	N

Tekelec_Admin	Admin remote or jumpoff or VPN	IXP_XDR	Pool xDR storage and RSP	1158	TCP	OracleEM.a	Oracle Database remote console	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_ORACLE	Central configuration	1158	TCP	OracleEM.a	Oracle Database remote console	Admin	N
IXP	Rules for IXP RSP ES	Customer_DWH	Non IXP Oracle server	1521	TCP	OracleNet8	Database queries and insertion	Data	N
NSP_PRIMARY	Weblogic server	Customer_DWH	Non IXP Oracle server	1521	TCP	OracleNet8	Database queries and insertion	Data	N
NSP_SECONDARY	Weblogic server	Customer_DWH	Non IXP Oracle server	1521	TCP	OracleNet8	Database queries and insertion	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	1521	TCP	OracleNet8	Database queries and insertion	Data	N
IXP	Rules for IXP RSP ES	IXP_XDR	Pool xDR storage and RSP	1521	TCP	OracleNet8	Database queries and insertion	Data	N
NSP_PRIMARY	Weblogic server	IXP_XDR	Pool xDR storage and RSP	1521	TCP	OracleNet8	Database queries and insertion	Data	N
NSP_SECONDARY	Weblogic server	IXP_XDR	Pool xDR storage and RSP	1521	TCP	OracleNet8	Database queries and insertion	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	IXP_XDR	Pool xDR storage and RSP	1521	TCP	OracleNet8	Database queries and insertion	Data	N
IXP	Rules for IXP RSP ES	NSP_ORACLE	Central configuration	1521	TCP	OracleNet8	Database queries and insertion	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_ORACLE	Central configuration	1521	TCP	OracleNet8	Database queries and insertion	Data	N
xMF	IMF and PMF servers	NSP_ORACLE	Central configuration	1521	TCP	OracleNet8	Database queries and insertion	Data	N
IXP	Rules for IXP RSP ES	Customer_feed	Data export server	2049	UDP	NFS	Linux Network File System	Data	N
IXP	Rules for IXP RSP ES	IXP_ES	IXP Export Server	2049	UDP	NFS	Linux Network File System	Data	N
IXP	Rules for IXP RSP ES	IXP_PDU	Pool PDU storage	2049	UDP	NFS	Linux Network File System	Data	N
IXP	Rules for IXP RSP ES	IXP	Rules for IXP RSP ES	2222	TCP	DTS	PIC Data Transport Service	Data	N
IXP	Rules for IXP RSP ES	xMF	IMF and PMF servers	2222	TCP	DTS	PIC Data Transport Service	Data	N
NSP_PRIMARY	Weblogic server	XMF	IMF and PMF servers	3306	TCP	MySql	My SQL database queries (config DB)	Admin	N
NSP_PRIMARY	Weblogic server	MSW	Legacy Message Switch	3333	TCP	RMI (JMX)	Java Management Extension Remote Invokation	Data	N
NSP_PRIMARY	Weblogic server	IXP	Rules for IXP RSP ES	5031	TCP	DSAPI.a	PDU decoding service, remote invoke	Data	N
NSP_SECONDARY	Weblogic server	IXP	Rules for IXP RSP ES	5031	TCP	DSAPI.a	PDU decoding service, remote	Data	N

							invoke		
NSP_PRIMARY	Weblogic server	IXP	Rules for IXP RSP ES	5055	TCP	DSAPI.b	PDU decoding service, alternate	Data	N
NSP_SECONDARY	Weblogic server	IXP	Rules for IXP RSP ES	5055	TCP	DSAPI.b	PDU decoding service, alternate	Data	N
Tekelec_Admin	Admin remote or jumpoff or VPN	IXP_XDR	Pool xDR storage and RSP	5520	TCP	OracleEM.b	Oracle database remote console	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_ORACLE	Central configuration	5520	TCP	OracleEM.b	Oracle database remote console	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	MSW	Legacy Message Switch	5631	TCP	PCanyw.a	PC Anywhere data	Admin	Y
Tekelec_Admin	Admin remote or jumpoff or VPN	MSW	Legacy Message Switch	5632	UDP	PCanyw.b	PC Anywhere status	Admin	Y
Tekelec_Admin	Admin remote or jumpoff or VPN	MSW	Legacy Message Switch	5900	TCP	VNC	Windows Remote Console	Admin	Y
Tekelec_Admin	Admin remote or jumpoff or VPN	MSW	Legacy Message Switch	6969	TCP	JMX(http)	Java management eXtension, admin console	Admin	OBSOLETE
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_PRIMARY	Weblogic server	8001	TCP	nsp.admin.ldap	NSP Weblogic administration, LDAP, console, sync	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	MSW	Legacy Message Switch	8080	TCP	http(SM)	Hypertext Transfer Protocol for System Mgmt	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	RSP	Report server	8080	TCP	http(SM)	Hypertext Transfer Protocol for System Mgmt	Admin	N
xMF	IMF and PMF servers	Customer_TADAPT	Customer 3rd party application	9090	TCP	MFP.a	Proprietary Message Flow Protocol, PDU	Data	TADAPT
MSW	Legacy Message Switch	IXP	Rules for IXP RSP ES	9090	TCP	MFP.a	Proprietary Message Flow Protocol, PDU	Data	TADAPT
xMF	IMF and PMF servers	IXP	Rules for IXP RSP ES	9090	TCP	MFP.a	Proprietary Message Flow Protocol, PDU	Data	TADAPT
xMF	IMF and PMF servers	IXP	Rules for IXP RSP ES	9094	TCP	MFP.b	Proprietary Message Flow Protocol, xDR	Data	OBSOLETE
Tekelec_Admin	Admin remote or jumpoff or VPN	IXP	Rules for IXP RSP ES	9095	TCP	MFPmaint.b	Proprietary Message Flow Protocol	Admin	OBSOLETE

							maintenance		
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	9300	TCP	iLO.a	HP Integrated Lights Out, shared remote console	Management	N
Tekelec_Admin	Admin remote or jumpoff or VPN	ILO	ILO range	9300	TCP	iLO.a	HP Integrated Lights Out, shared remote console	Management	N
NSP_PRIMARY	Weblogic server	xMF	IMF and PMF servers	15616	TCP	JDBC	Java DataBase Connectivity (config DB)	Admin	N
NSP_SECONDARY	Weblogic server	xMF	IMF and PMF servers	15616	TCP	JDBC	Java DataBase Connectivity (config DB)	Admin	N
IXP	Rules for IXP RSP ES	IXP	Rules for IXP RSP ES	16810	TCP	inetsync	COMCOL internetwork synchronization	Admin	N
xMF	IMF and PMF servers	NSP_PRIMARY	Weblogic server	16810	TCP	inetsync	COMCOL internetwork synchronization	Admin	N
NSP_PRIMARY	Weblogic server	xMF	IMF and PMF servers	16810	TCP	inetsync	COMCOL internetwork synchronization	Admin	N
xMF	IMF and PMF servers	xMF	IMF and PMF servers	16810	TCP	inetsync	COMCOL internetwork synchronization	Admin	N
IXP	Rules for IXP RSP ES	IXP	Rules for IXP RSP ES	16878	TCP	inetmerge	COMCOL internetwork merge	Admin	N
xMF	IMF and PMF servers	NSP_PRIMARY	Weblogic server	16878	TCP	inetmerge	COMCOL internetwork merge	Admin	N
NSP_PRIMARY	Weblogic server	XMF	IMF and PMF servers	16878	TCP	inetmerge	COMCOL internetwork merge	Admin	N
xMF	IMF and PMF servers	XMF	IMF and PMF servers	16878	TCP	inetmerge	COMCOL internetwork merge	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	17988	TCP	iLO.b	HP Integrated Lights Out, virtual media (CD)	Management	N
Tekelec_Admin	Admin remote or jumpoff or VPN	ILO	ILO range	17988	TCP	iLO.b	HP Integrated Lights Out, virtual media (CD)	Management	N
Tekelec_Admin	Admin remote or jumpoff or VPN	Customer_DWH	Non IXP Oracle server	17990	TCP	iLO.c	HP Integrated Lights Out, Console	Managem	N

							relay	ent	
Tekelec_Admin	Admin remote or jumpoff or VPN	ILO	ILO range	17990	TCP	iLO.c	HP Integrated Lights Out, Console relay	Managem ent	N
NSP_PRIMARY	Weblogic server	IXP	Rules for IXP RSP ES	41000	TCP	RMI-JMX-sec	Remote Method Invokation for JMX, secured	Admin	N
NSP_SECONDARY	Weblogic server	IXP	Rules for IXP RSP ES	41000	TCP	RMI-JMX-sec	Remote Method Invokation for JMX, secured	Admin	N
NSP_PRIMARY	Weblogic server	xMF	IMF and PMF servers	41000	TCP	RMI-JMX-sec	Remote Method Invokation for JMX, secured	Admin	N
NSP_SECONDARY	Weblogic server	xMF	IMF and PMF servers	41000	TCP	RMI-JMX-sec	Remote Method Invokation for JMX, secured	Admin	N
NSP_PRIMARY	Weblogic server	IXP	Rules for IXP RSP ES	41090	TCP	NFM.b	NSP File Management	Admin	N
NSP_SECONDARY	Weblogic server	IXP	Rules for IXP RSP ES	41090	TCP	NFM.b	NSP File Management	Admin	N
IXP	Rules for IXP RSP ES	NSP_PRIMARY	Weblogic server	41090	TCP	NFM.b	NSP File Management	Admin	N
IXP	Rules for IXP RSP ES	NSP_SECONDARY	Weblogic server	41090	TCP	NFM.b	NSP File Management	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	IXP	Rules for IXP RSP ES	49696	TCP	JMX(https)	Java management eXtension, admin console secure	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_APACHE_BACK	NSP back-end side (application)	49696	TCP	JMX(https)	Java management eXtension, admin console secure	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_ORACLE	Central configuration	49696	TCP	JMX(https)	Java management eXtension, admin console secure	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_PRIMARY	Weblogic server	49696	TCP	JMX(https)	Java management eXtension, admin console secure	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_SECONDARY	Weblogic server	49696	TCP	JMX(https)	Java management eXtension, admin console secure	Admin	N

Tekelec_Admin	Admin remote or jumpoff or VPN	xMF	IMF and PMF servers	49696	TCP	JMX(https)	Java management eXtension, admin console secure	Admin	N
IXP	Rules for IXP RSP ES	NSP_PRIMARY	Weblogic server	7001;7003	TCP	jms,t3	NSP Weblogic, users, alarms and administration	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_PRIMARY	Weblogic server	7001;7003	TCP	jms,t3	NSP Weblogic, users, alarms and administration	Admin	N
xMF	IMF and PMF servers	NSP_PRIMARY	Weblogic server	7001;7003	TCP	jms,t3	NSP Weblogic, users, alarms and administration	Admin	N
IXP	Rules for IXP RSP ES	NSP_SECONDARY	Weblogic server	7001;7003	TCP	jms,t3	NSP Weblogic, users, alarms and administration	Admin	N
Tekelec_Admin	Admin remote or jumpoff or VPN	NSP_SECONDARY	Weblogic server	7001;7003	TCP	jms,t3	NSP Weblogic, users, alarms and administration	Admin	N
xMF	IMF and PMF servers	NSP_SECONDARY	Weblogic server	7001;7003	TCP	jms,t3	NSP Weblogic, users, alarms and administration	Admin	N
NSP_ORACLE	Central configuration	IXP	Rules for IXP RSP ES	na	ICMP	ICMP	Ping connectivity tests	Admin	TEMPORARY
xMF	IMF and PMF servers	NSP_PRIMARY	Weblogic server	na	ICMP	ICMP	Ping connectivity tests	Admin	TEMPORARY
NSP_ORACLE	Central configuration	xMF	IMF and PMF servers	na	ICMP	ICMP	Ping connectivity tests	Admin	TEMPORARY
IXP	Rules for IXP RSP ES	NEPTUNE	External probe Astellia neptune	56000	TCP	Neptune.up	Astellia probe UP	Data	Y
IXP	Rules for IXP RSP ES	NEPTUNE	External probe Astellia neptune	56001	TCP	Neptune.cp	Astellia probe CP and stats	Data	Y
NSP_PRIMARY	Weblogic server	NEPTUNE	External probe Astellia neptune	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS
Tekelec_Admin	Admin remote or jumpoff or VPN	NEPTUNE	External probe Astellia neptune	22222	TCP	Neptune.htt	Astellia probe configuration	Admin	Y

						ps			
NEPTUNE	External probe Astellia neptune	NSP_PRIMARY	Weblogic server	162	UDP	snmp.b	Simple Network Management Protocol (traps)	Admin	Y
Tekelec_Admin	Admin remote or jumpoff or VPN	TAP	Splitter	80	TCP	http	Hyper Text Transfer Protocol (web)	Admin/Data	OR HTTPS
Tekelec_Admin	Admin remote or jumpoff or VPN	TELENA_FALCO	TDM-SIGTRAN Converter	22	TCP	ssh	Linux Secured Shell including sftp	Admin	N
TELENA_FALCO	TDM-SIGTRAN Converter	NSP_PRIMARY	Weblogic server	162	UDP	snmp.b	Simple Network Management Protocol (traps)	Admin	Y