Course Objectives

At the end of this presentation the student should be able to:

- Understand the function of service processor
- Understand the procedure to rebuild the SP
- Explain the 3PAR remote support functionality
- Access STaTs and SPOCC

The SP(Service Processor)

Currently an SP is a 1U PC, pre loaded with software, mounted in the storage server rack

It is designed to provide remote error detection and reporting, and to support diagnostic and maintenance activities involving the HP 3PAR storage server

The data collected by the SP is used to maintain, troubleshoot, and upgrade the SP and storage server at the operating site

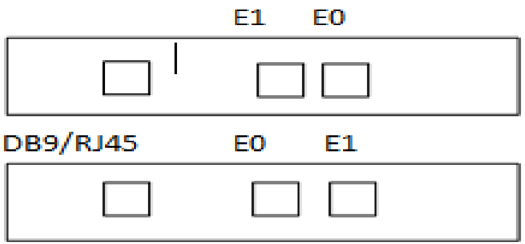
Service processor

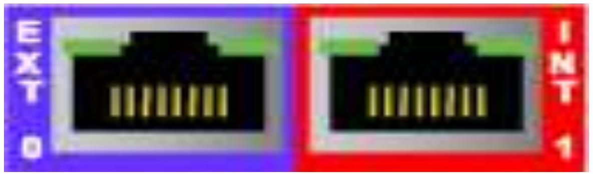
Models—Array dependant, STaTS model lookup

3PAR Part #	HP Part #	Description	SP ID Range
F970-0017-01	N/A	Service Processor 2U (Cal Digital)	SP00001 - SP00199
F970-0085-*	N/A	Service Processor 1U (Dell-650)	SP00300 - SP00399
F970-0088-*	649875-001	Service Processor 1U (Dell-750)	SP00400 - SP00899
F975-0009-50-R5	642000-001	Service Processor 1U (WINTEC)	SP00900 - SP01999
F979-200051	641753-001	Service Processor 1U (SuperMicro)	SP20000 - SP20999
F975-200010	641719-001	Service Processor 1U (SuperMicro II)	SP03000 - SPxxxxx

SP Types
Dell

Wintec
Supermicro





Service processor
Port details

Serial Port: DB9

- 38400/8 /N/XON – XOFF Please note for SS7000 physical should use 57600
- Connector DB9 to RJ45 PN: 180-0059

NOTE: Laptop side DB9 to RJ45 PN: 180-0055

Network Ports

- E0 – (E0/EXT 0)
  - Normally connected to Customer Network
  - IP Address—Customer defined
- E1 – (E1/INT 1)
  - Maintenance Connection
  - IP Address: 10.255.155.54

NOTE: Set laptop pc to: IP-10.255.155.49/Gateway – 255.255.255.248

The SP cont:

The current SP model is a super micro II

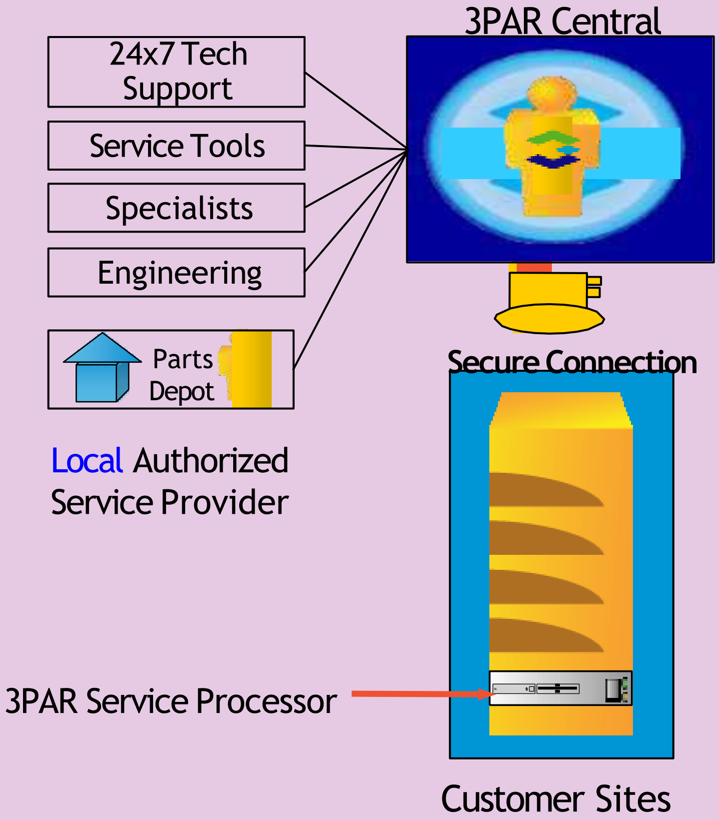
Normally one SP per storage system

SP is not in the data stream

SP can operate in two modes

- SP mode
- Secure Network mode

3PAR REMOTE SUPPORT OVERVIEW



Centralized support strategy

- Secure network connectivity
- System Health Check
- Full remote diagnostics
- Remote online software updates

24x7 coverage

- 4 hour onsite response times
- Strict escalation procedures

Point & Click maintenance

- Automated and pre-tested
- GUI Guided maintenance
- Minimized manual service errors

Authorized Service Partners

- Hardware break-fix
- Spare parts logistics and depots

3PAR REMOTE SUPPORT ARCHITECTURE

Currently, there are 2 secure remote support approaches to access the 3PAR InServ Storage Server at customer site

1. Connection to 3PAR Connection Portal through Secure Shell – (SP Mode - Legacy)

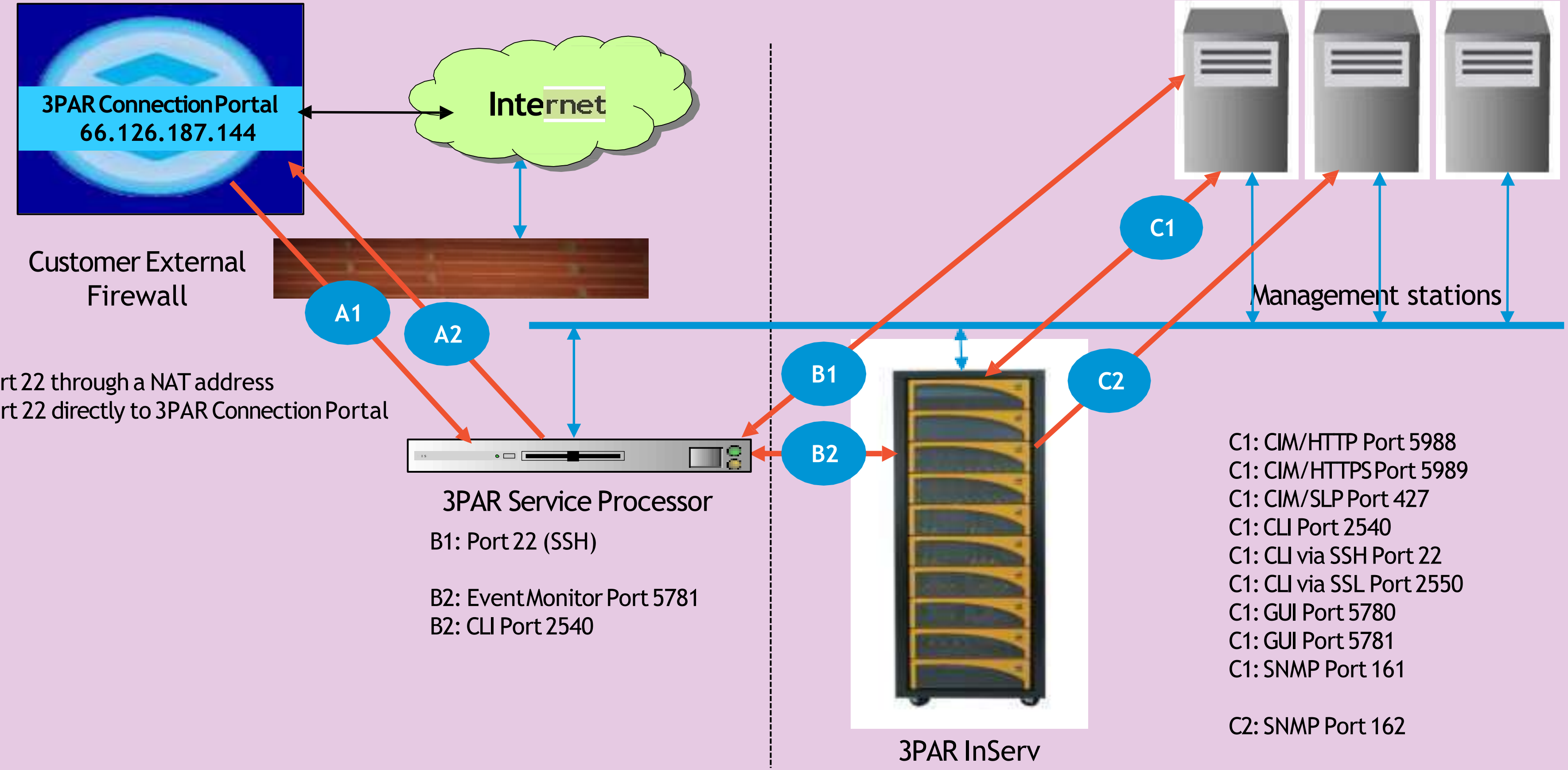
2. Connection to 3PAR Collector Server via HTTP over Secure Socket Layer (HTTPS) – (SP Secure Network Mode)

Note:

All remote connection are made through the 3PAR Service Processor to 3PAR Central and vice-versa.

The Service Processor (SP) is housed within the base cabinet of each InServ Storage Server, serves as the communication interface within the customer's IP network for all service-related communication from/to an InServ Storage Server.

3PAR REMOTE SUPPORT – SP MODE (LEGACY)



3PAR Connection Portal
66.126.187.144

Internet

Customer External
Firewall

A1

A2

B1

B2

C1

C2

Management stations

A1: Port 22 through a NAT address
A2: Port 22 directly to 3PAR Connection Portal

3PAR Service Processor

B1: Port 22 (SSH)

B2: EventMonitor Port 5781
B2: CLI Port 2540

3PAR InServ

C1: CIM/HTTP Port 5988
C1: CIM/HTTPS Port 5989
C1: CIM/SLP Port 427
C1: CLI Port 2540
C1: CLI via SSH Port 22
C1: CLI via SSL Port 2550
C1: GUI Port 5780
C1: GUI Port 5781
C1: SNMP Port 161

C2: SNMP Port 162

3PAR REMOTE SUPPORT – SP MODE (LEGACY)

Outbound - Call home

Outbound access from Service Processor (SP) to (66.126.187.144) ORIGINATES from ports 1024-65535 TO port 22 on , and requires all related session traffic be allowed.

Only connection from Connex will be allowed access the SP. Users have two layers of security to be able to initiate the connection.

Outbound connection enables:

Error, configuration, and performance data from the 3PAR InServ system or Service Processor is transferred to 3PAR Central, 3PAR’s global IT center.

Analysis and automated notification to technical support representatives enables proactive maintenance.

3PAR REMOTE SUPPORT – SP MODE (LEGACY)

Inbound – Remote Support Connection

To enable inbound Ethernet connectivity from the 3PAR Connection Portal to the Service Processor the customer will need to change their firewall rules to allow ports 1024 through 65535 of the Connection Portal IP address to communicate with port 22of the Service Processor IP address.

Customer to set up NAT (network address translation) IP address that the firewall translates to the actual SP IP address:
66.126.187.144 -> SP NAT IP Address (using port 22)

Only connection from Connex will be allowed access the SP. Users have two layers of security to be able to initiate the connection.

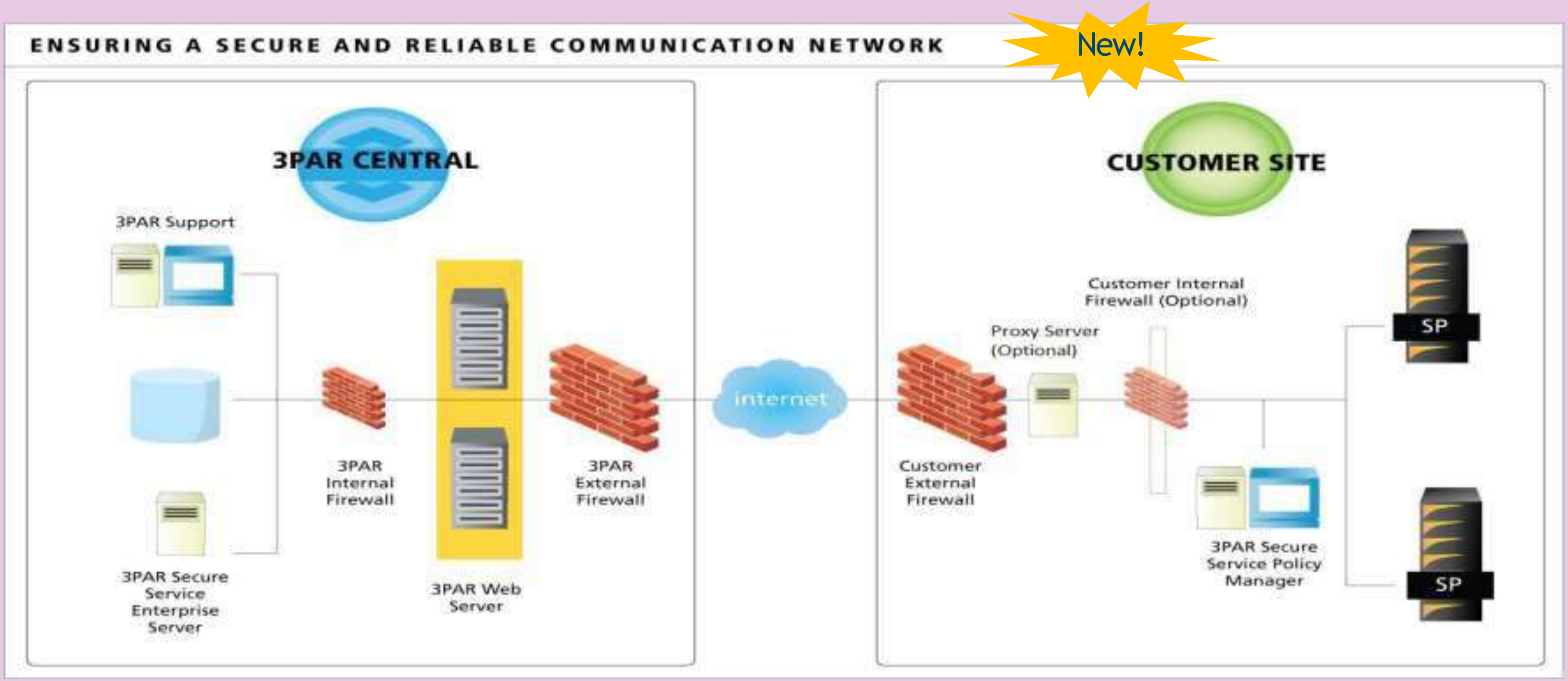
For Inbound connectivity:

– The SP will receive transferred fixes and firmware and software updates from 3PAR Central.

–At a time that is convenient for the customer, the updates will be installed on the 3PAR product. This function eliminates the need for human intervention for software downloads thereby reducing the possibility of human error.

– Remote connectivity will allow 3PAR to put the appropriate technical resources on a problem from any given location throughout the world.

3PAR REMOTE SUPPORT – SECURE NETWORK MODE



ENSURING A SECURE AND RELIABLE COMMUNICATION NETWORK
New!
3PAR CENTRAL
3PAR Support
3PAR Internal Firewall
3PAR Web Server
3PAR External Firewall
3PAR Secure Service Enterprise Server
Internet
CUSTOMER SITE
Customer External Firewall
Proxy Server (Optional)
Customer Internal Firewall (Optional)
SP
SP
3PAR Secure Service Policy Manager

3PAR REMOTE SUPPORT – SECURE NETWORK MODE

The preferred method of transfer as it is secure and easy for customers to implement in their firewall.

Call home

Secure Network Mode utilizes the HP-3PAR Secure Service Architecture which leverages the industry-standard HTTP over Secure Socket Layer (HTTPS) protocol for all external communication, ensuring that the communication is secure and any data transmission is encrypted.

The setup only requires secure port (https port 443) be enabled on the customer's external firewall. All communication with HP-3PAR support is initiated in an outbound manner.

To enable communication between the Service Processor with the 3PAR Secure Service Collector Server (66.126.187.154 /) located at 3PAR Central, HTTPS (HTTP with SSL) port 443 should be allowed on customer external firewall rule.

The SP must be able to ping the IP address through the firewall and the 3PAR Trilogy portal URL and IP should be authenticated by the firewall.

3PAR REMOTE SUPPORT – SECURE NETWORK MODE

Remote Support Connection

Remote connections are protected by a secure protocol. All communication between the 3PAR Secure Service Collector Server (at 3PAR Central) and the Service Processor (at the customer site) is conducted using HTTPS.

Remote connections require no special firewall rules to be implemented to allow connectivity. The 3PAR Secure Service Collector Server does not initiate the remote connection; instead, the Collector Server embeds a remote connection request in its response to the normal periodic communication with the Service Processor. The HTTPS session is initiated and driven by the Service Processor.

Once a remote connection is established with a 3PAR Service Processor, the GSS is restricted to executing control operations only on the connected InServ Storage Server. GSS has no access to the customer data since the volume, logical disk, and physical disk level access is blocked.

3PAR REMOTE SUPPORT – SECURE NETWORK MODE

Required Ports (within customer's network)

Service Processor-to-InServ

– Port 22 (SSH)
Used for depositing and executing programmatically driven service scripts and for collecting an archive of diagnostic data (known as an InSplore).

– Port 2540 (CLI)
Used for gathering system health information, configuration data, and performance data.

– Port 5781 (Event Monitor)
Used for monitoring system events on the InServ.

Service Processor-to-Secure Service Policy Manager (**optional**)

– Port 80 (HTTP)
Used for all communication (including policy enforcement) between the Service Processor and Policy Manager.

3PAR REMOTE SUPPORT ARCHITECTURE

3PAR Remote	SP Mode (Legacy)	Secure Network Mode
Support Portal	66.126.187.144 /	66.126.187.154 /
Requirement @ client network	Firewall to allow communication to 66.126.187.144	DNS server to resolve to 66.126.187.154. SNM can also be manually set to use a static IP address.
Port (outbound)	Ports 1024-65535 on the SP to Port 22 on	Port 443 (https)
Port (inbound)	Ports 1024-65535 on to Port22 on the SP	Port 443 (https)
External IP (NAT) for inbound	Firewall must allow ssh connection between 66.126.187.144 and external or NAT IP address assigned to the SP.	Not required

SECURE CUSTOMER SITES

A Secure Customer Site (a.k.a. ‘Dark Site’) is a site where the customer will NEVER allow a Service Processor to transfer files (call home) to 3PAR and will NOT allow ing remote maintenance connections as well.

The SP is prohibited to access public internet and will be used only to access and monitor the 3PAR InServ internally.

3PAR GSS will not have the “real-time” system status and access to the storage system will depend on customer availability, means & approval thus the word DARK SITE. Government agencies, banks & other financial institutions are among the list of customers usually setup as secure sites. i.e. FBI, US Army, ABS

For this type of sites that do not permit the SP to transfer error information when it occurs, 3PAR Customer Services requests the customer to gather and send this weekly file each week (e.g., on Monday) so that the system may be monitored, albeit at a less than optimal rate.

The SP gathers InServ configuration and error information and stores this information as files on the local drive. Once a week (usually on a Sunday 4am), the SP compresses and zips these files into a single weekly file.

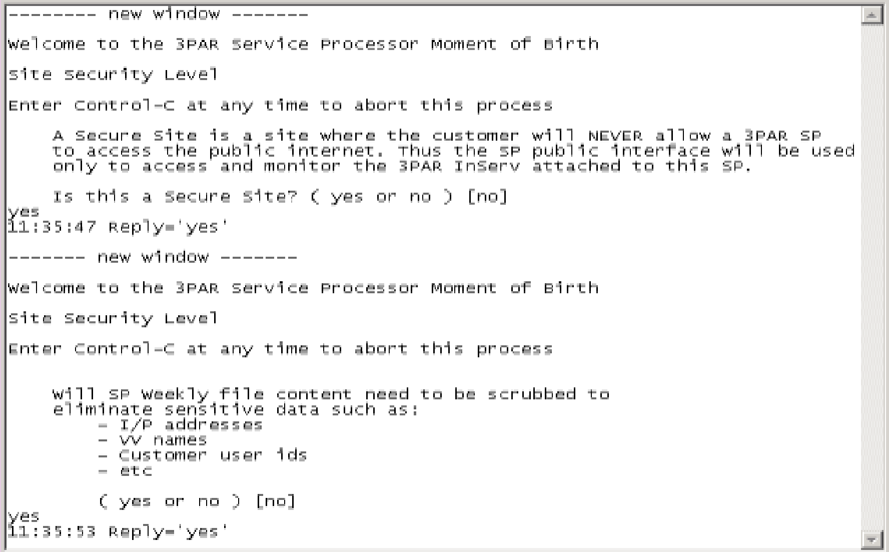
The file may then be retrieved from the SP and transmitted via email or FTP.

SECURE CUSTOMER SITES

At initial installation during the Service Processor - Moment of Birth (MOB), the first question it will ask is how to setup the ‘Site Security Level’.

Is this a Secure Site? (yes or no) _

If the site is secured, we will need answer “yes” to this question.



```
-------- new window -------

Welcome to the 3PAR Service Processor Moment of Birth

Site Security Level

Enter Control-C at any time to abort this process

    A Secure Site is a site where the customer will NEVER allow a 3PAR SP
    to access the public internet. Thus the SP public interface will be used
    only to access and monitor the 3PAR InServ attached to this SP.

    Is this a Secure Site? ( yes or no ) [no]
yes
11:35:47 Reply='yes'

------- new window -------

Welcome to the 3PAR Service Processor Moment of Birth

Site Security Level

Enter Control-C at any time to abort this process


    Will SP Weekly file content need to be scrubbed to
    eliminate sensitive data such as:
        - I/P addresses
        - VV names
        - Customer user ids
        - etc

        ( yes or no ) [no]
yes
11:35:53 Reply='yes'
```

When a weekly file is collected, customer sensitive data are removed (i.e. IP addresses, VV names, Client User IDs).

Customer may carry out additional scrubbing on the information contained in the weekly files to achieved their specific security level.

The compressed files should follow the 3PAR weekly file naming convention so it will be processed timely & correctly.

“3PAR_weekly_1XXXXXX_yymmdd.tbz2”
Where:
1XXXXXX is the InServ serial number
yymmdd is the most recent date

INSPLORE LOG COLLECTION

InSplore

An InSplore collects large amount of InServ Storage Server configuration information, machine state data, and log data to assist in troubleshooting and identifying the root cause of a technical issue. An InSplore is generated automatically in the rare event that an application or InServ Storage Server panic occurs.

Optionally, an authorized Global Services and Support representative can request a manual InSplore once a remote service connection is established with the Service Processor. To make efficient use of data transfer bandwidth, the InSplore is tar'd and compressed.

For more info, see: Procedure_for_Customer_to_create_and_upload_an_HP-3PAR_InSplore.pdf

LOCAL NOTIFICATION

The Service Processor's Local Notification features enables sending important Storage Server events and alerts on a subscription basis. Notifications are sent through email to all subscribers, with each subscriber specifying up to three email addresses.

If Real-time Alert Processing (RAP) forwarding is enabled, copies of all notification messages sent to subscribers are automatically forwarded to 3PAR Central as well.
Note: RAP forwarding will no longer be supported in future releases of SP OS and therefore discourage for further usage.

Local Notification Types

There are two types of local notification messages that you might receive.

Standard Notification Messages

Alerts you to an important event or alert generated by a storage server.

When an event or alert is received, a corrective action may need to be taken to correct the issue.

Low Urgency Notification Messages

Informs you of noncritical events generated by a storage server.

Low urgency notification messages are informational and do not typically require a corrective action be taken. When a situation or event reported in a low urgency notification message es urgent, a standard notification message is issued to alert subscribers.

LOCAL NOTIFICATION

Setting up Local Notification

1. Enable Local Notification Access in SPOCC
2. Configure mail host
3. Enter site information
4. Create user profiles
5. Add records

For more info, see: Local Notification and RAP Forwarding Setup.docx

We will collect an InSplore later at the Demo.

3PAR Diagnostic Information (1 of 2)

The diagnostic information that is collected and transferred to 3PAR Central includes the following:

CONFIG – The Service Processor executes every two hours a number of *show commands on the InServ Storage* Server to collect configuration and status information. This information represents the output of multiple *show* commands including *showsys, showvlun, showcage, showpd, showport, etc*.

STATUS – The output of a health check that is run on an hourly basis on the InServ Storage Server

PERFORM – Collects performance information about the InServ Storage Server three times a day for the duration of a 3-minute period each time. This represents the output of multiple *stat commands including statvlun, statcpu, statport, etc*.

EVTLOG – Contains the event log, which provides an audit trail of all change commands that are executed on the InServ Storage Server, plus any events that have occurred. The event log represents the output of the *showeventlog* command and is collected every 4 hours.

ALERT – Contains any alerts that have not been acknowledged or removed by the storage administrator. This represents the output of the command *showalert and is run every 4 hours*.

3PAR Diagnostic Information (2 of 2)

EVENT – Any events or errors that may occur are transmitted immediately to 3PAR Central.

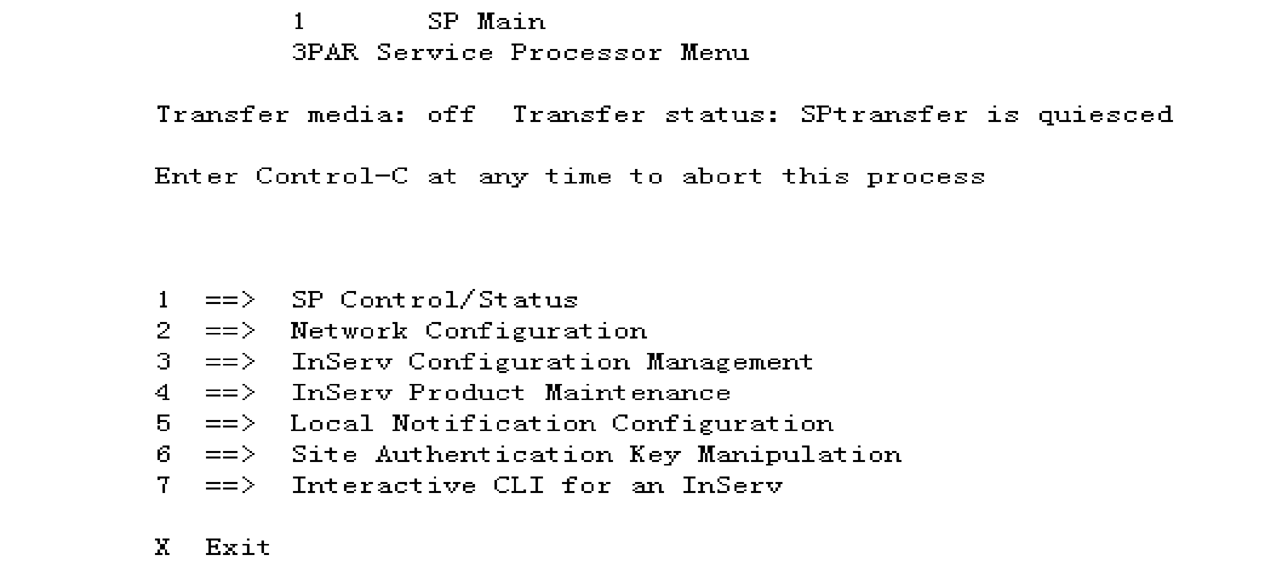
InSplore – An InSplore collects large amount of InServ Storage Server configuration information, machine state and log data to assist in troubleshooting and identifying the root cause of a technical issue. InSplore is generated automatically in the rare event that an application or InServ Storage Server panic occurs. Optionally, an authorized customer service representative can request an InSplore manually once a remote service connection is established with the Service Processor. To make efficient use of data transfer bandwidth, the InSplore is tar'd and compressed.

SPLOR – A SPLOR is generated after each reboot of the Service Processor or once each day. SPLOR collects Service Processor configuration, machine state, and log data to assist in troubleshooting and analyzing any technical issues with the Service Processor.

DUMPS – DUMPS represent application core dumps (excluding buffer contents) from a controller node on the InServ Storage Server DUMPS are collected on an as needed basis.

SPmaint

Launched automatically when log as spvar or 3parcust



```
                1        SP Main
                3PAR Service Processor Menu

Transfer media: off   Transfer status: SPtransfer is quiesced

Enter Control-C at any time to abort this process



1   ==>  SP Control/Status
2   ==>  Network Configuration
3   ==>  InServ Configuration Management
4   ==>  InServ Product Maintenance
5   ==>  Local Notification Configuration
6   ==>  Site Authentication Key Manipulation
7   ==>  Interactive CLI for an InServ

X   Exit
```

SP Users

HP Internal

spdood

root

field (during re-image. Right after re-image, until MOB is run root has no password)

Partner/ASP

spvar

- has no Linux shell , cannot enable/disable customer firewall setting
- has no spmaint menu #8 for running Unix command from the SP
- need to help them when data gather requires access to shell (ie: getting Linux log files, narrowing down IP connectivity issues ie: at initial install between SP and CP)

Customer

3parcust

- has no Linux shell,
- has no spmaint menu #8 for running Unix command from the SP

SPmaint Menu Differences Among the SP Users

Some menus will not be authorized. It will depend on who you login as.

- Menus that 3parcust user can do that spvar cannot:
  - Change customer controlled access (2.1)
  - Change permissive mode (2.3.6)
  - Turn off firewall (2.3.4)
  - Turn on firewall (2.3.5)
- Menus that spvar user can do that 3parcust cannot:
  - Site authentication key manipulation

Both spvar and 3parcust has no menu#8, which allows user to run Linux command in the InServ

SP (ItSelf) Maintenance

SP itself is a FRU (HW problem with the SP will require the whole SP replacement)

- replace the whole server, re-image (re-install the Linux image and re-install the SP software)

We do check SP health particularly during OS upgrade analysis and before actually running OS upgrade analysis

- df -k, free -lt
- presence of IP errors at netstat –s, InServ health status (contains IP statistics)

Quick Look at Some Extra InFormation about SP:

Refer to “SP documents” directory.

Quick scan thru “SP Troubleshooting Guide (Sept 2010).pdf”