Patton Electronics Company, Inc.
7622 Rickenbacker Drive
Gaithersburg, MD 20879 USA
Tel. +1 (301) 975-1000
Fax +1 (301) 869-9293
support@patton.com
http://www.patton.com

SmartWare Migration Notes

R3.20 to R3.21

Introduction

SmartWare R3.21 is a Maintenance Release of SmartWare, the software for all Patton SmartNode products. R3.21 is the Maintenance Release following on R3.20.

The SmartWare Software Release Concept dictates the life cycle of SmartWare R3.21, this document is available on upgrades.patton.com.

New hardware product support introduced with R3.21

The following products are first supported with SmartWare R3.21:

- SmartNode 4650 Series with ADSL or G.SHDSL WAN interface
- SmartNode 4830 Series with ADSL or G.SHDSL WAN interface
- SmartNode 4900 Series with FXO interfaces
- SmartNode 4900 Series with G.SHDSL WAN interface
- SmartNode 4554

Hardware products not supported by R3.21

The following products that run SmartWare R3.20 are not supported anymore by R3.21:

- SmartNode 1200
- SmartNode 1400
- All SmartNode 2300 models

New software features introduced with R3.21

The following software features are new in R3.21 and only available in R3.21:

- Reverse ARP
- SIP multicast registration
- SIP diversion header support
- Possibility to revert calls to audio after T.38 fails
- SIP multiple user registration with different credentials (for ISDN MSN lines in certain carrier environments)
- AOC (advice of charge) transmission between SIP and ISDN (also H.323 and ISDN)
- Permanent IKE tunnels

- Enhanced policy routing – allows to route IP packets based on traffic classes
- Caller name support on T1 ISDN

Software features not supported by R3.21

All software features present in SmartWare R3.20 are available in R3.21. No features have been lost or disabled.

Compatibility of Configuration Files

Configuration files used with SmartWare R3.20 are fully backwards compatible and can be used on R3.21. As new features have been added compared to R3.20, behavioral changes can't be excluded with an unchanged configuration file.

Changed/New Configuration Commands

Please see the Software Configuration Guide R3.21 for a comprehensive overview of all configuration commands of SmartWare R3.21. It is available on upgrades.patton.com. The following is a list of all commands that have been added between R3.20 and R3.21:

SIP Multicast Registration

SmartWare supports now SIP multicast registration, by sending a REGISTER message to a multicast IP address or domain. When a registrar answer to a multicast or unicast REGISTER message with a "302 moved temporarily" message, SmartWare can now send a REGISTER to a given contact in the "302 moved temporarily" message. This behavior must be enabled.

Registration

To accept "302 moved temporarily" messages and send REGISTER messages to a contact in the received message, registration must be set to auto. When a REGISTER to a redirected contact fails, a new multicast REGISTER is sent to the configured registration. When registration is set to manual, redirect messages are ignored and REGISTER is always send to the configured address. Sending REGISTER messages via default server with option "use-default-server" is only allowed with manual configuration.

Mode

gateway sip <gateway>/service <service>

	Command	Purpose
Step 1	[*name*] **(svc-sip)**[*service*]**#[no] registration (manual** <host> **[**<port>**] [use-default-server]) | (auto** <host> **[**<port>**])**	Set ip-address or domain with optional port on which REGISTER messages should be sent. Auto enables acceptation of redirection messages, while manual fixes the address.

Default Server

Additionally the default server can be set to auto that always the actual registrar is taken as default server. When both are set to auto, the registration mechanism discovers the registrar and the address of

the discovered registrar is also taken as default server. When set to manual the default server can be set to a fixed address.

Mode

gateway sip <gateway>/service <service>

	Command	Purpose
Step 1	[*name*] (**svc-sip**)[*service*]**#no] defaultserver ((manual <**host**> [<**port**>]) | auto) [loose-router | strict-router]**	Set IP address with optional port, which is used as default server. Auto sets the default server always to the actual registration contact, and updates when a new contact is treated as registrar.

SIP Diversion Header

SmartWare supports now the SIP Diversion Header for transmitting redirecting information over SIP according to draft-levy-sip-diversion-08. Sending and receiving of the header can be configured independent of each other. Even the Diversion Header standard would allow appending a header for each diversion occurred in the network, SmartWare only records the last and the first diversion. If only one Diversion Header is attached to the INVITE request, then it represents the last diversion.

Transmit Direction

For enabling sending of the Diversion Header, an outgoing address translation expression must be configured on the sip interface. This expression specifies how to create the Diversion URI of the header. As User Part of the URI the Calling Redirecting number will always be taken. The user must configure the Host Part that is set per default to 'none'. Setting the Host Part to 'none' disables transmission of the Diversion Header.

Mode

interface sip <interface>

	Command	Purpose
Step 1	[*name*] (**if-sip**)[*interface*]**#address-translation outgoing-call diversion-header host-part {call | default-server | domain | fix | interface | none}**	Enables or disables sending of the Diversion Header and specifies the Host Part of the URI. **call:** If available, the Host Part of the calling from-header will be taken else the local ip address. **default-server:** The ip address of the configured default-server will be taken. **domain:** The configured domain name will be taken. **fix:** Allows to specify a user configured Host Part. **interface:** The local ip address will be taken. **none:** Disables sending of the Diversion Header.

Receive Direction

For receiving of the Diversion Header, an incoming address translation expression must be configured on the sip interface. Because several methods for transmitting redirecting information are available, this expression specifies that they must be taken from the Diversion Header for providing them to the call control.

Mode

interface sip <interface>

	Command	Purpose
Step 1	**[** *name***] (if-sip)[***interface***]#[no] address-translation incoming-call calling-redir diversion-header**	Enables or disables extracting of the redirection information from the Diversion Header.

ISDN DivertingLegInformation2 Facility

SmartWare is now able to extract the redirecting information from the DiverstingLegInformation2 Facility and to provide them to the call control. In the other direction, the redirecting information can be sent as DiverstingLegInformation2 Facility in addition to the Redirecting Number Information Element.

Transmit Direction

Mode

interface isdn <interface>

	Command	Purpose
Step 1	**[** *name***] (if-isdn)[***interface***]#[no] diversion emit**	Enables or disables transmitting of the DivertingLegInformation2 Facility.

Receive Direction

Mode

interface isdn <interface>

	Command	Purpose
Step 1	**[** *name***] (if-isdn)[***interface***]#[no] diversion accept**	Enables or disables receiving of the DivertingLegInformation2 Facility.

SIP User Registration And Authentication

The previously used commands *user* and *authentication* were merged to a unified *user* command to decouple the user names for SIP registration from the user names for authentication. With the new

command all users can be authenticated with a different login name than the username for registration. In addition a given authentication credential can be set as default for all users with no credentials defined.

Mode

gateway sip <gateway> / service <service>

	Command	Purpose
Step 1	**[** *name***] (svc-sip)[***service***]# user <user> [authenticate [name <login>] password <password> [default]] [register [display-name <display-name>][phone-context <phone-context>]]**	Adds a user for SIP registration and the credentials for authentication.

When the **authenticate** branch of the command is specified, the user is considered when a proxy requires client authentication. The credentials used for client authentication are formed by {<login>, <password>} or {<user>, <password>} if the login-name is not explicitly specified. One user of a service can be tagged with the **default** keyword. The credentials of this default user are used for client authentication if no other user matches.

When the **register** branch of the command is specified, the user is registered with a SIP registrar. The registered URI is formed by <user>@<domain>, using the domain specified with the SIP gateway service or the local IP address if not explicitly specified.

Using both the **authenticate** and **register** branch, allows you to register a user and use (different) credentials for client authentication.

Examples

Create three users each registering to a SIP registrar without client authentication:

user 101 register display-name "User1"
user 102 register display-name "User2"
user 103 register display-name "User3"

Don't use a registrar but use the following authentication credentials when the proxy requires client authentication.

user MY-DEFAULT-USER authenticate name my-name password my-password default

Since the user is not registered, the user-name can directly be used as login-name. Thus the following command configures the same:

user my-name authenticate my-password default

Register three users to a SIP registrar all using the same authentication credentials:

user 101 register display-name "User1" authenticate name my-name password my-password
user 102 register display-name "User2" authenticate name my-name password my-password
user 103 register display-name "User3" authenticate name my-name password my-password

This can also be expressed as three users without authentication credentials, but with a default authentication credentials specified separately.

user 101 register display-name "User1"
user 102 register display-name "User2"
user 103 register display-name "User3"
user my-name authenticate password my-password default

Time Offset Change

Previously you had to configure the local clock offset using the "sntp-client gmt-offset" command. This command is now deprecated. You should use the new command "clock local offset" to configure the local clock offset. The deprecated "sntp-client gmt-offset" command is still accepted when appearing in the startup-config. However it is automatically converted to the new command in the running-config.

show clock local

Mode

enable

	Command	**Purpose**
Step 1	[*name*]**# show clock local**	Displays the local time, UTC and the offset of the local time from UTC.

clock local offset

Mode

configure

	Command	**Purpose**
Step 1	**[** *name***] (cfg)# clock local offset (+|-)hh:mm**	Enables the reception of SIP Info messages containing AOC-D elements and propagate Charging information to adjacent peer.

This command replaces the following deprecated command:

Mode

configure

	Command	Purpose
Step 1	**[** *name***] (cfg)# sntp-client gmt-offset (+|-) hh:mm:ss**	This command is no longer used and deprecated.

AOC Over SIP

This enhancement allows sending AOC information transparently from ISDN (or H.323) to SIP and vice-versa. AOC-D elements are hex-encoded and sent as application/QSIG content in SIP INFO messages during a session

aoc-d accept

Mode

context cs / interface sip

	Command	Purpose
Step 1	**[***name***] (if-sip)[**interface**]# [no]** ***aoc-d accept***	Enables or disables the reception of SIP Info messages containing AOC-D elements and propagate charging information to adjacent peer.

aoc-d emit

Mode

context cs / interface sip

	Command	Purpose
Step 1	**[***name***] (if-sip)[**interface**]# [no]** ***aoc-d emit***	Enables or disables the sending of SIP Info messages with AOC-D elements containing charging information from adjacent peer. If no charging information is available, no message is sent.

Permanent IKE Tunnels

By default IKE tunnels are established as late as possible (when the first packet is flowing through) and IKE tunnels with expired lifetimes are reestablished only in case there is traffic flowing through. With the permanent option set, IKE tunnels are established shortly after boot and are reestablished after the expiration of their lifetime even if there was no traffic flowing through.

Mode

configure

	Command	Purpose
Step 8	***node*(pf- ipsik)[<*name*>]# protected-network {host <local-host-ip>}|{subnet <local-subnet-address> <local-subnet-mask>}|{range <local-range-start> <local-range-end>} {host <remote-host-ip>}|{subnet <remote-subnet-address> <remote-subnet-mask>}|{range <remote-range-start> <remote-range-end>} [permanent-tunnel]**	Optionally if the remote system requires protected networks to be specified in the identity payload of the quick mode, you can define one or more protected networks using this command. If the tunnel shall be established permanently the permanent-tunnel flag must be set.

Policy Routing Phase 2

The traffic class for SIP signaling, H323 signaling, voice data and fax data is configurable. The configured traffic class is used as additional routing criterion in the IP routing table (see Policy Routing)

SIP Signaling

Mode

gateway sip <gateway>

	Command	Purpose
Step 1	**[** *name***] (gw-sip)[***gateway***]# call-signaling-trafficclass <traffic-class>**	Sets traffic class for SIP signaling packets. The traffic class may be new or may already exist.

H323 Signaling

Mode

gateway h323 <gateway>

	Command	Purpose
Step 1	**[** *name***] (gw-h323)[***gateway***]# call-signaling-trafficclass <traffic-class>**	Sets traffic class for H323 signaling packets. The traffic class may be new or may already exist.

Voice and Fax data

Mode

profile voip <profile>

	Command	Purpose
Step 1	**[** *name***] (pf-voip)[***profile***]# rtp traffic-class <traffic-class>**	Sets traffic class for voice data and fax data packets. The traffic class may be new or may already exist.

CLI ZIP File Software Download

It is possible to upgrade the software directly by passing the name of the delivered zip-file to the CLI command “copy”.

The SmartWare downloads the whole ZIP file. During this time the download progress is displayed in bytes. After downloading, the ZIP file containing batch file “bw” or “b” will be extracted and executed. This leads to writing the SmartWare image, which is also part of the ZIP file, to the flash. The web pages are updated too.

After writing the image to the flash, the Smartware needs to be reloaded with the command **reload.**

Mode

enable

	Command	Purpose
Step 1	***node*(cfg)#copy tftp://<server-ip-address>/<path>/<smartwaredeliveryfile>.zip :flash**	Downloads the specified delivery file from the TFTP server and starts the driver software image upgrade process.

An example of such a Smartware upgrade session, where the new software is in the file *SN1000_SIP_R3.T_2006-08-10.zip* which is stored on a tftp-server with the ip address *192.186.22.44:*

```
SN1200#copy tftp://192.186.22.44/SN1000_SIP_R3.T_2006-08-10.zip flash:
Download...   3124510 Bytes
Downloading image...completed (2715796 bytes)
Erasing flash...completed.
Writing to flash...completed
Processing files...completed
SN1200#reload
```

T1 Caller-Name Support

The ISDN implementation now supports reception and transmission of the caller-name on T1 links as it is used in NI2 networks according to Bellcore GR-1367-CORE. Transmission of the caller-name is part of the Calling Name Delivery (CNAM) service.

In previous build series, the caller-name was already supported for DSS-1 networks using User-User information elements and for Q.SIG (PSS-1) networks using FACILITY messages. Now the caller-name is also supported for NI2 networks following the Bellcore standard.

As a prerequisite the *caller-name* feature must be enabled on each ISDN interface in the CS context separately. This command now has additional arguments to configure the SETUP retention as follows:

In NI2 networks an incoming ISDN SETUP message may contain a *NameInfomationFollowing* indication instead of the name. This means that the calling-party name is not available yet, but will be sent later, for example, after the dictionary database lookup in progress succeeded. If such an incoming ISDN call is internally routed to another network (e.g. to a SIP network or to a ISDN DSS-1 network), we must know the name before sending the initial INVITE or SETUP message towards the destination network. Therefore we must retain the SETUP message of the incoming ISDN call until the name is present. The caller-name command now allows you to configure the behaviour of this SETUP retention mechanism. There are three possible options:

- **caller-name ignore-absence <timeout>:** This configuration command specifies the behaviour for incoming ISDN calls. When a *NameInformationFollowing* indication is received with the SETUP message, the call-initiation is retained until the name is received or until this timeout elapses. After that, the call is forwarded to the configured destination interface. When forwarding

a call without a caller-name to a SIP network, please note that there is no chance to send the caller-name later over SIP.

- **caller-name early-alerting <timeout>:** This configuration command specifies the behaviour for incoming ISDN calls. Some networks only deliver the name after an alerting indication. These networks simulate the mid-ring name delivery feature of analog lines. If early alerting is enabled, we send back a faked ALERTING message after a configurable timeout when we receive a *NameInformationFollowing* indication. This command can be used together with the ignore-absence command. For example, you can configure an interface to first generate an ALERTING message and later forward the call anyway. If used that way, the early-alerting timeout should be smaller than the ignore-absence timeout.
- **caller-name send-information-following:** This configuration command specifies the behaviour for outgoing ISDN calls. If there is no name from the originating network, the ISDN interface configured with this command sends a *NameInformationFollowing* indication to the remote side itself.

The following example enables and configures the caller-name feature on a T1 ISDN interface for incoming calls. If no name is present in the SETUP message, but the SETUP message contains the *NameInformationFollowing* indication, an ALERTING message is sent back after 500ms. If there is no name after additional 500ms the call is routed to the destination network anyway.

Mode

context cs / interface isdn

	Command	Purpose
Step 1	***node*(if-isdn)#caller-name**	Enables reception of the caller-name.
Step 2 (optional)	***node*(if-isdn)#caller-name early-alerting 500**	If no name is present in an incoming ISDN call and if the incoming SETUP message contains the *NameInformationFollowing* indication, we send a fake ALERTING message after 500ms towards the caller. The SETUP message is retained for this period, i.e. the call is not forwarded to the configured destination. This step is optional. When not configured, an ALERTING message is faked after **2s by default**. You can disable faking an ALERTING message by using the “no” form of the command. **Note:** If the ignore-absence timeout is also configured, the early-alerting timeout should have a smaller value than the ignore-absence timeout.

Step 3 **(optional)**	***node*(if-isdn)#caller-name ignore-absence 1000**	If no name is present in an incoming ISDN call and if the incoming SETUP message contains the *NameInformationFollowing* indication, we forward the call to the routing destination anyway after 1000ms (500ms after faking the ALERTING message in this example). This step is optional. When not configured, the call is forwarded after **4s by default**. You can disable forwarding a call without a name by using the "no" form of the command. **Note:** The specified timeout is measured starting at the reception of the SETUP message, not when the early-alerting timeout elapses.

The following example enables and configures the caller-name feature on a T1 ISDN interface for outgoing calls. It enables the transmission of the *NameInformationFollowing* indication (encapsulated into sent SETUP message) when no name is present from the originating network:

Mode

context cs / interface isdn

	Command	**Purpose**
Step 1	***node*(if-isdn)#caller-name**	Enables transmission of the caller-name.
Step 2 **(optional)**	***node*(if-isdn)#caller-name send-information-following**	If no name has been received from the originating network a *NameInformationFollowing* indication is send encapsulated into the SETUP message for the outgoing ISDN call. **This feature is disabled by default.**

Additional Help, Questions

For additional help or any questions, please contact Patton or Patton-Inalp Technical Support at:
USA: support@patton.com, **+1-301-975-1007** Monday-Friday, 8:00AM to 5:00PM EST

Switzerland: support@patton-inalp.com **+41-31-985-25-55,** Monday-Friday, 8:00AM to 5:00PM CET