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

Customer Deliverable Documentation
Revision 1.00, June 6, 2014

SmartWare R6.T Release Notes

Build Series 2014-05-28

SmartWare is the embedded application software of the SmartNode™ series of VoIP Gateways and Gateway Routers. SmartWare provides a full set of IP routing features, advanced Quality of Service and traffic management features plus industry leading Voice over IP functionality including SIP and H.323

Released Build Numbers

SmartNode 4110 Series R6.T Build 2014-05-28
SmartNode 4120 Series R6.T Build 2014-05-28
SmartNode 4300 Series R6.T Build 2014-05-28
SmartNode 4400 Series R6.T Build 2014-05-28
SmartNode 4520 Series R6.T Build 2014-05-28
SmartNode 4600 Series R6.T Build 2014-05-28
SmartNode 4600 Series R6.T DSL Build 2014-05-28
SmartNode 4660 Series R6.T Build 2014-05-28
SmartNode 4670 Series R6.T Build 2014-05-28
SmartNode 4830 Series R6.T Build 2014-05-28
SmartNode 4830 Series R6.T DSL Build 2014-05-28
SmartNode 4900 Series R6.T Build 2014-05-28
SmartNode 4940 Series R6.T Build 2014-05-28
SmartNode 4950 Series R6.T Build 2014-05-28
SmartNode 4960 Series R6.T Build 2014-05-28
SmartNode 4970 Series R6.T Build 2014-05-28
SmartNode 4980 Series R6.T Build 2014-05-28
SmartNode 4990 Series R6.T Build 2014-05-28
SmartNode 5200 Series R6.T Build 2014-05-28
SmartNode 5400 Series R6.T Build 2014-05-28
SmartNode 5480 Series R6.T Build 2014-05-28
SmartNode 5490 Series R6.T Build 2014-05-28
SmartNode DTA Series R6.T Build 2014-05-28

About this Release

R6.T is a SmartWare Technology Release. Please see the White Paper about SmartWare software releases http://www.patton.com/solutions/SmartWare%20Release%20Strategy%20White%20Paper.pdf for more information about this terminology.

Supported Products

SmartNode 4110 Series (HW Version: 1.x, 2.x, 4.x)
SmartNode 4120 Series (HW Version: 1.x, 2.x)
SmartNode 4300 JS Series (HW Version: 2.x)
SmartNode 4300 JO Series (HW Version: 1.x)
SmartNode 4400 JS Series (HW Version: 2.x)
SmartNode 4400 JO Series (HW Version: 1.x)
SmartNode 4520 Series (HW Version: 1.x, 2.x, 4.x)
SmartNode 4600 Series (HW Version: 1.x)
SmartNode 4600 Large Series (HW Version: 1.x, 2.x)
SmartNode 4660, 4670 Series (HW Version: 2.x, 3.x, 4.x)
SmartNode 4830 Series (HW Version: 1.x, 2.x, 4.x)
SmartNode 4830 Large Series (HW Version: 1.x, 2.x)
SmartNode 4900 JS Series (HW Version: 1.x, 2.x)
SmartNode 4900 JO Series (HW Version: 1.x)
SmartNode 4940 Series (HW Version: 5.x)
SmartNode 4950 Series (HW Version: 5.x)
SmartNode 4960 Series (HW Version: 1.x, 2.x, 3.x, 4.x, 5.x)
SmartNode 4970, 4980, 4990 Series (HW Version: 1.x)
SmartNode 5200 Series (HW Version: 6.x)
SmartNode 5221 Series (HW Version: 4.x)
SmartNode 5400 Series (HW Version: 5.x)
SmartNode 5480, 5490 Series (HW Version: 1.x)
SmartNode DTA Series (HW Version: 1.x, 2.x)

History of Solved CTS Cases

The following list refers to open cases in the Change Tracking System 'CTS'.

This Build Series 2014-05-28

12351 Corrected reception and transmission of SIP AOC headers

Processing of SIP AOC Headers has been reworked, both for reception and transmission.

The AOC type (-S, -D or -E) is now determined based on the received packet type (e.g. 200OK, INFO, BYE). This is compatible with Asterisk and Snom implementations.

The conversion of charging information to and from SIP Headers has also been adapted to be inter-operable with Snom and Asterisk.

12271 Rejected INVITE with ambiguous SDP content header

When receiving a SIP packet with the following SDP characteristics

```
Content-Type: application/sdp

Content-Length: 0
```

the SmartNode would always respond with "488 Not Acceptable Here".

To correct this behavior such a packet is considered to contain no SDP at all right from the start. Such a packet is then processed like a SIP packet that does not contain any SDP.

12272 Failed to send SIP BYE message

Under some specific conditions the device was not able to send the SIP BYE message. These conditions were met when a 200OK had been sent in response to a Re-INVITE, but before the ACK was received. If a BYE was attempted to be sent at exactly that moment, this would fail.

This problem is now solved by waiting for the ACK message from the peer before trying to send the BYE.

Build Series 2014-03-12

12188 SIP Trusted Host enhancement

In some cases it is desirable not to send an answer back to an untrusted SIP host. The SmartNode responds with a “SIP/2.0 503 Service Unavailable” to SIP requests received from hosts which are not trusted. Therefore an additional command for the "trusted host" feature has been implemented in context sip-gateway: *answer-untrusted-hosts*. It specifies if an error message (SIP/2.0 503 Service Unavailable) or nothing at all should be replied. See full details in the *New configuration commands* section.

12268 Configurable time zone for CDR messages (accounting data)

A new CLI command has been added to the AAA profile: *local-time-cdr*. If this is set, the time in the CDR messages will be in local time instead of UTC. To avoid confusion, there is a label in the CDR for every call specifying the time (Local/UTC). See full details in the *New configuration commands* section.

12276 Removed *no* form of address-translation incoming-call commands

The "no" form of all *address-translation incoming-call* commands in the sip interface has been removed. They were inconsistent with the address-translation outgoing-call commands and their only purpose was to set the parameters to default, which can be done by issuing those commands with no parameters. See full details in the *New configuration commands* section.

12297 Calling-Name support for DMS-100

The Calling-Name feature for DMS-100 has been implemented according to the *NIS-A211-1* standard which describes how to encode calling-name into the *Display* information element.

12301 SIP AOC-E (advice of charge) not sent

During more extensive AOC-header tests, it turned out that on SIP side no AOC-E was being sent when the charging value had not changed between the last AOC-D and AOC-E state. This issue has been fixed and now AOC-E is always sent when configured.

12309 DTMF tones propagation on the SIP receive side

Up to now the *dtmf-relay* command in the *profile voip* only defined the translation of DTMF tones received on the TDM side to the defined method on the IP side. The effect of this command has now been extended to the reverse direction, with the limitation that inband tones will always be relayed to the TDM side, no matter what the configuration is. This means that if DTMF relay signaling is configured, then only inband and SIP INFO DTMF tones are propagated and if DMTF relay default or rtp is configured then only inband and RFC2833 events are propagated.

12326 Changed verbiage in GUI for reloads

Improved message in GUI when reloading the Smartnode. It was somehow confusing when importing a config.

12333 More tolerance for SDP parsing of received messages

Even if the standard exactly describes how the SDP must be formatted (see RFC4566, SDP grammar in ABNF format), we have made SmartWare more tolerant for SDP parsing. For example, having multiple "c=" lines in a wrong order in the SDP resulted in dropping the call. This scenario is now working.

12344 calling-redir-e164 cannot be configured in web GUI

It was not possible to configure the calling-redir-e164 in web GUI as the value fields were not present. Value fields for calling-redir-e164 and calling-second-e164 are now text inputs in both mapping and routing tables configuration pages.

12345 Web GUI display issue: AOC SIP-header

Clicking on a SIP interface status page, the AOC format was displayed as (invalid) when AOC method "SIP-header" was set. This issue has been fixed.

12353 Support for upgrade to Trinity with multiple shipping-configs

SmartWare now supports upgrading to Trinity with an image containing multiple shipping-configs.

12358 E1T1 channel-group encapsulation voiceband not available

With the channel-group model on E1T1 it is possible to share the same link for different protocols. For a partial ISDN usage the *encapsulation voiceband* command was missing. With that type of encapsulation the user defines which b-channels are available for ISDN voice transmission. See full details in the *New configuration commands* section.

Build Series 2014-01-10

12285 EFM card firmware version in show command

It was not possible to determine which firmware version was installed on the EFM daughterboard. This is now possible via the existing “*show dsl all*” command.

12290 Show command formatting for EFM card

Until now, the output of the “*show port dsl*” command was not correctly formatted for the EFM daughter card. This is now fixed.

12312 Crash in Advice of Charge scenarios when using SIP headers

A crash was occurring when SmartWare was receiving Advice of Charge indications in SIP header format. The advice of charge is now correctly working when receiving and sending SIP requests.

12320 Random crash during calls

Random crash during calls using the DSP has been fixed.

12330 Identical SIP-Header X-Org-ConnID for two simultaneous calls

If two SIP packets arrived at the same time, then the same X-Org-ConnID was sent back in the response to both packets. Now, the X-Org-ConnID is unique for every incoming INVITE packet.

12341 X-Org-ConnID with call diversion

Previously a new X-Org-ConnID was generated if a call diversion happened for the second time. Now X-Org-ConnID always stays the same in case of call diversion.

Build Series 2013-11-13

12243 SIP B2BUA dynamic registration support

This new feature allows dynamic back-to-back registration. An inbound registration can trigger an outbound registration to an external registrar. In addition to a hunt-group and/or the penalty-box, this feature offers new fallback possibilities. See full details in the *New configuration commands* section.

12287 Crash on terminating SIP call with DNS

In a certain scenario of terminating a SIP call a serious software failure could cause the device to crash with a SW Watchdog exception. For this to happen the call was originated from the remote SIP device. Then the Patton device wants to communicate changes to the call or wants to terminate the call. Therefore we want to send a request to the remote device, which needs to be resolved through DNS first. The crash could occur when the DNS resolving is still ongoing and an additional event causes the Patton device to release the call. In that certain sequence of events the SIP session is now terminated without crashing.

12302 Parameters not applied to EFM daughter card during startup

A configuration parameter was not applied on the EFM daughter card after startup. This issue has been fixed.

12307 Local tax pulse generation on FXS

The ability to let the FXS port periodically generate a tax pulse towards the connected phone has been introduced. For more details on the new command see the *New configuration commands* section.

12313 Inbound call to FXO, ringing not always dispatched to the call-control

When a ringing did occur on the FXO port, the call was not always dispatched to the call-control. This bug is now fixed.

12318 SIP NOTIFY check-sync

Now it is possible to trigger auto-provisioning with a SIP NOTIFY request. Refer to the section *New Configuration Commands* for a detailed description.

12319 Screening and presentation indicators treated incorrectly for diverted calls

Until now, when a call diversion has occured, the screening and presentation indicators were treated incorrectly. Those parameters were applied to the calling party number information element instead of the diversion information element. This is now treated correctly in SIP and ISDN signaling.

12322 Wrong help text for the annex-type parameter of EFM daughter card

Help text described the default value of the annex-type parameter as “a-b”. The real default value is “a-f”. The help text has been modified accordingly.

Build Series 2013-09-13

12220 SIP stack upgrade to V4.2.8

The SmartWare SIP stack has been upgraded to the latest version V4.2.8.

12239 Fixed crash when receiving 302 moved temporarily SIP message

Fixed a crash that occurred when a SIP interface was configured with *no call-reroute accept* and *new-session-after-redirect* and when the SmartNode received a 302 moved temporarily response after creating a new SIP session.

12240 SIP registration expiry time is wrong

The SmartNode was re-registering to late with the registrar. With this fix, the negotiated SIP registration lifetime is respected. Now Re-REGISTER requests are sent before the lifetime elapses. We defined a minimal lifetime value of four seconds to avoid heavy network load.

12255 Radius authentication profile for SSH is not saved in the configuration

The authentication profile to be used by the SSH terminal did not appear in the running-config. As a consequence, the SSH authentication configuration could not be saved persistently. This issue has been fixed.

12261 Traffic-class not set on stack-generated SIP messages

In previous builds, the traffic-class for SIP calls was specified for each call outbound identity in the location service. This did not work well: the traffic-class was not set properly on stack-generated SIP responses such as 100 Trying. We fixed this problem by moving the traffic-class configuration command into the context sip-gateway. The deprecated command in the location service is still available but should not be used anymore; a warning will be printed if you enter it. For more details on the new command see the *New configuration commands* section.

12270 FXS port stops ringing the phone

For electrical reasons, SmartWare limits the number of FXS ports that are ringing simultaneously. SmartWare has to allocate a ringing resource for ringing and release it when ringing stops. In certain call-flow scenarios these ringing resources were never released and consequently, later calls could not ring the phone anymore until the device was reset. One example that triggered this problem was a phone that was picked up before the first ring started. This problem has been fixed and the device does not run out of ringing resources anymore.

12272 SIP AoC not sent when overlap dialing is enabled

If overlap dialing was configured on a SIP interface, the Advice of Charge updates arriving at the peer interface (e.g. ISDN) were not forwarded over SIP. This issue has been fixed: AoC information is correctly tunneled over overlap-dialed SIP calls.

12277 SN4660/SN4670 - HW QUEUE FULL error while receiving DTMF tone

When *dtmf-relay* was enabled on a SN4660/SN4670, after receiving a few DTMF tones, the media gateway reported *NETWORK TX: HW QUEUE FULL* and no call was working anymore until the device was reset. This problem only occurred if the DTMF-end message was received within less than 20ms after the previous DTMF-update message. This problem has been fixed in the DSP software.

12282 Auto-provisioning fails when DHCP option 66 is missing

Since build series 2012-09-17 the auto-provisioning does not work if DHCP is not used or the DHCP server does not return an option 66. This dependency has been removed again and DHCP option is no longer mandatory for auto-provisioning.

12298 EFM, communication broken with the card

When an EFM card was not responding to the card's supervisor, the connection between the main-board and the card was considered down after a timeout of only 20 seconds. If the connection to the card was re-established, the configuration parameters entered in the mean time were not applied to the card. This issue has been fixed. Additionally, the supervisor tries for three times to re-establish the communication with the card before the connection is reported down.

Build Series 2013-07-17

10977 Support for call deflection on ISDN

In addition to the call reroute facility SmartWare supports now the call deflection facility as well. When issuing a call reroute through an ISDN connection, the type of facility is selected depending on the layer 2 protocol. For point-to-point links a call reroute facility is sent and for point-multi-point links a call deflection facility is sent. In the incoming direction both types of facility are accepted, independent from the layer 2 protocol.

11990 Incorrectly encoded Calling-Name for NI-2 and DMS-100

If a SmartNode was configured to send the Calling-Name through the connected T1 link some peers returned a parsing error. This happened due to an encoding failure in the sent Facility message. The problem has been fixed and Calling-Name delivery is now working for the NI-2 protocol as well as for DMS-100.

12028 SIP AOC Header support

In addition to ASN1 and XML format for AOC-S, AOC-D and AOC-E, it is now possible to use a SIP Header for advice of charge purposes. This format is currently used by Snom phones and Swyx IP-PBX. See full details in the *New configuration commands* section.

12205 New SIP Header "X-USE302: YES"

It is now possible to add a new SIP Header in SIP requests. The X-USE302 header is used by some IP-PBXs to enforce the use of the *SIP 302 Moved Temporarily* Redirection response. See full details in the *New configuration commands* section.

12206 Unique SIP connection ID for calls

A new command is available to enable an ID as a SIP header (X-Org-ConnID) which is unique in a call forwarding scenario. See full details in the *New configuration commands* section.

12209 Invalid BGP identifier

The process of determining the BGP identifier for a certain device did not work in case of IP interfaces which obtain their ip-address through DHCP. If at least one static IP address is configured a valid BGP identifier will now be generated.

12214 Configurable calling party or facility IE on ISDN

In ISDN calls, Called party numbers starting with '#' or '*' characters were always sent in a facility information-element. It is now possible to configure to send this called party number in a calling-party information-element. See full details in the *New configuration commands* section.

12215 Broken policy-routing for SIP calls over UDP

By default all sent SIP UDP messages are marked with the 'local-default' traffic-class. SmartWare provides the possibility to change that traffic-class on a per-identity basis using the Location-Service framework. If the traffic-class has been changed for an identity or identity-group, policy-routing rules that included the new traffic-class did not have any effect. The same broken behavior could also be discovered in service-policy profiles using that traffic-class for DSCP/TOS marking.

12216 Determine reachability with SIP OPTION requests

Normally a SIP call is started by sending an INVITE request to the destination. If that destination is unavailable for any kind of reason it could take some time to detect that this destination is failing. During that time the party who initiated the call is waiting for the ring-back tone as feedback. To try an alternative path to reach the called destination it is practically too late because the caller gave up during that time. It is now possible to determine reachability of destinations ahead of actual calls. For a failing destination an alternative routing path to the called end user could be issued immediately without having a timeout. See details in the *New configuration commands* section.

12221 SIP penalty box behavior improved

Until now the SIP penalty box was not working as expected. The blacklist service of the SIP stack always kept a last valid destination to use even if this destination was not responding. This is now fixed and the SIP requests are no longer sent to destinations which have been placed in the blacklist.

12222 Missing identity header for empty calling party number

For empty calling party numbers there was no P-Asserted-Identity or P-Preferred-Identity header added to the SIP messages even if configured to do so. This is fixed now and in such a case an identity header with a default URI is added to the SIP messages. In addition the privacy header was never added for P-Preferred-Identity. This is fixed as well. A Privacy header is now added for any identity header when the presentation indicator from call-control is set to “restricted”.

12224 Identity headers not parsed for SIP overlap dialing calls

When receiving a call on a SIP interface which is configured to accept SIP overlap dialing calls, no identity headers were parsed. Now the P-Asserted-Identity or P-Preferred-Identity headers are parsed and the content is passed to call-control according to address-translation.

12230 SIP-Gateway wrong address lookup

When the Smartnode had several SIP gateways bound to different IP addresses or the same IP address with different ports, then the local address of the SIP header were wrong is some cases. A new route lookup has been implemented to assure that the correct local address is used in the SIP header.

12234 G.SHDSL link UP with cell delineation error or with training error

With some DSLAM no traffic is going through the DSL line although the G.SHDSL interface notified an up link. This problem can occur randomly or after an event on the DSLAM. This is caused by two different errors during the line training.

The first error is a Cell delineation Hunt state. When reaching this state the interface should retrain the line automatically, but in some particular scenarios the retrain needs to be done manually.

The second error occurs during the training phase and the interface will notify a LastStatusFailed. This error can be recovered by a line retrain.

The Smartware DSL port supervisor has been enhanced to detect and automatically retrain the line when one of these errors is present. To enable the supervisor enter this command on the *port dsl 0 0*:

[node](port-dsl)[0/0]# supervisor { boot | *always* | *observe }*

Note that the *observe* mode will not retrain the line, but only detect the errors. *boot* mode will only detect and retrain the line during boot phase! (See configuration guide for more details on the supervisor).

Errors can be displayed by entering the *show log event* command and the actual state of the line can be shown with the command *show port dsl 0 0*.

12241 Missing shipping-config after upgrade to Trinity

When upgrading from SmartWare to Trinity, the shipping-config was missing in the system because it was copied to the wrong location. The location has been corrected and the shipping-config is available on Trinity when upgrading from this version of SmartWare.

12244 SDP ptime attribute

The SDP *ptime* attribute announces the maximum receive duration for the offered coders. Because *ptime* can only be offered on media level and not on a per coder basis, SmartWare selects the *rx-length* of the first configured coder as value for the *ptime* attribute. By default the new attribute is not included in SIP's SDP content. It can be configured to be included with the voip profile's *sdp-ptime-announcement* command. For exact configuration syntax please consult *New Configuration Commands*.

12245 Rejected INVITE when Call-ID contains a '<' character

If a received INVITE contained a '<' character in the Call-ID, this INVITE was rejected with 'SIP/2.0 400 Bad Request' due to a parsing error. This has been corrected and such INVITEs are accepted.

12247 SIP request URI length limitation

This new feature allows denying incoming SIP request whose URI length exceeds a user specified value. Limiting the request URI length has device wide validity. The configured number of characters is applied for all incoming SIP requests on the whole device. Therefore the new *max-request-uri-length* is located in the global *sip* configuration mode. By default the request URI length is unlimited. For exact configuration syntax please consult *New Configuration Commands*.

12252 Local RAS port is configurable for H.323

Up until now RAS messages were sent from the same local port number as it was configured for the local call-signaling port. This caused problems for H.323 gatekeepers which required different port numbers. Therefore the local port for RAS messages can now be configured. See details in the *New configuration commands* section.

12253 H.323 Gatekeeper fallback not working

It is possible to configure multiple H.323 gatekeepers. The SmartNode should register to the first one with the others a fallback if the first is not available. There were two issues with this. The first one is that the SmartNode tried to register with the second gatekeeper first. This is fixed and now the first configured gatekeeper is the first to register with. The second issue was that when receiving a "RegisterReject" answer from a gatekeeper, the fallback to the other configured gatekeeper did not work. This is fixed and the fallback to the second gatekeeper is working now.

12256 License installation fails on Trinity after upgrade from SmartWare

When upgrading to Trinity from a previous SmartWare version it was impossible to install any new license while running Trinity. At the same time any license that was present on SmartWare has not been transferred to the Trinity system. Both issues will not be observed any longer if upgrading to Trinity from this version of SmartWare.

12263 Wrong MOS value for G.723

The MOS value for G.723 codec was computed with wrong factor values, which results in a slightly incorrect value. This has been fixed and now the MOS value is correct for the G.723 codec.

12284 Compatibility with EFM DB V3.3.1

This version introduces compatibility with the EFM daughter board software V3.3.1. Note that this version of SmartWare will not work any previous version of EFM DB software. Likewise any previous version of SmartWare will not work with V3.3.1 of the EFM DB software.

The major enhancement which is introduced with this new version is that the SmartNode with EFM interface can now also be operated in a 192.168.20.0/24 network without issues.

Build Series 2013-05-16

12016 PSTN configuration on a R2 interface was cleared after a few calls

PSTN configuration on a R2 interface was correctly set to the DSP channels, however after a call this configuration was cleared on the DSP channel, resulting in the next call on this DSP channel using the default PSTN configuration instead of what is configured. This has been fixed and the DSP is reconfigured with the correct PSTN configuration after each call.

12145 ISDN interface is capable of triggering actions

The action framework is enhanced with the capability of executing actions upon state changes of ISDN interfaces in the call-control. See details in the *New configuration commands* section.

12167 Alcatel signaling method for flash-hook SIP info message

A new signaling method is available for flash-hook SIP info message. See full details in the *New configuration commands* section.

12169 SIP request not being sent

An issue in the SIP transport layer has been fixed which caused a SIP request (INVITE, REGISTER) not to be sent out. If the monitor "*debug context sip-gateway stack all detail 5*" is switched-on, the error "*No local address found for destination:*" is displayed. The problem occurred if a request for a given destination had to be sent from a different local ip-address than the sip-gateway was actually bound to. It always occurred if a sip-gateway was bound to an IP *loopback* interface.

12183 Downloadable CDR records

The new *upload profile* as been defined in order to upload information from the SmartNode. It is now possible to upload the locally stored CDR records to a TFTP or HTTP server. This new profile is similar to the provisioning profile and it allows the use of a timer in order to have this task automated. See full details in the *New configuration commands* section.

12186 SNMP allowed network

Until now, it was only possible to allow SNMP requests from hosts. It is now possible to add the permissions to an entire network range. See full details in the *New configuration commands* section.

12190 Display error of ISDN binding

When executing the command *show call-control provider ISDN* the Binding would be displayed with garbage characters. This was due to an incorrect memory access which has been corrected now.

12195 Adaptions to maximal possible SIP sessions on ESBR

For the new Enterprise Session Border Router products the way of determining the maximum available SIP sessions is changed with respect to existing products. Previously this number was calculated in relation to the available DSP channels. Now this is independent and read from the hardware description on the device. Devices manufactured before this change but using this new software build will have zero available SIP sessions and customers are asked to contact their support representative for obtaining the SIP sessions. The following existing products are concerned:

- SN5200 with HW version <= 6.1
- SN5480 with HW version <= 1.2
- SN5490 with HW version <= 1.2.

New SN5221 model with X.21 interface

The software supports the new Enterprise Session Border Router SN5221. It has two Ethernet ports and an X.21 serial interface and the capability of doing VoIP calls.

12196 Availability of H.323 in ESBR products

All the Enterprise Session Border Router products have now the possibility to activate H.323 by importing the H.323 license. This concerns SN5200, SN5221, SN5400, SN5480 and SN5490. Previously H.323 was disabled and not available for these products.

12199 Support for EFM daughter card (Rev A)

SmartWare now supports the newly introduced EFM daughter card. It is possible to configure the card via new CLI commands. See full details in the *New configuration commands* section.

12204 Duplicate T.38 attributes in SDP

Smartware now accepts duplicate T.38 attribute fields for the T38FaxRateManagement and the T38FaxUdpEC fields in received SDP offers. However SmartWare itself does only support these values:

- T38FaxRateManagement:transferredTCF
- T38FaxUdpEC:t38UDPRedundancy

The following rules apply:

1. If a duplicate entry for either of the attribute-fields is received, the response will only contain the value supported by SmartWare.
2. If a single entry for either of these attribute-fields is received and the value is not supported by SmartWare, then the response will not contain this attribute-field at all.

Note that this feature has originally been introduced into R5.6 of SmartWare. It was broken in R6.T_2012-07-18 and R6.3 and is now reintroduced with this build.

12211 Logging error when a WAN card is detected but unknown

The SN4970, SN4980, SN4990, SN5480 and SN5490 did not log anything if a WAN card was detected but could not be recognized and initialized. This has been fixed and now an error message will be logged if a WAN card is present but cannot be recognized for any reason.

12212 Crash in SIP transfer scenarios

A problem has been fixed that let the SmartNode crash in various SIP transfer scenarios. Generally, a received *REFER* request containing the *Refer-To* header with the *Replaces* parameter forced the SmartNode into a spurious behavior.

Build Series 2013-03-14

11683 Network and user provided secondary calling party number

Now it is possible to receive and send secondary calling party numbers through ISDN and SIP interfaces. Refer to the section *New Configuration Commands* for a detailed description.

11925 Encryption key provisioning

It is now possible to perform provisioning for local encryption key. See full details in the *New configuration commands* section.

11961 PRACK not working for forked INVITE

In forking scenarios only the provisional answers from the first dialog were acknowledged with a PRACK request. The provisional answers from all additional dialogs were not acknowledged with a PRACK request. This lead to retransmission of such unacknowledged answers, but the call continued and could be connected successfully. Now this is fixed and all provisional answers are acknowledged with a PRACK request.

11973 Incoming calls refused with 481 after PPP cycle

It is now possible to receive incoming calls correctly even if a PPP cycle happened before the INVITE packet.

12114 Unknown SAPI message on E1 port

After a series of link down/up events on the E1 port, the HDLC controller loses alignment, which is reflected by unknown SAPI messages. To avoid this problem the HDLC controller is reset each time the port is going up.

12136 Crash during startup with large configurations (also fixes 12113, 12085, 12132)

Two issues have been fixed that could cause a crash during startup of the SmartNode. Both cases are configuration related and are depending on the number of entries which have been configured in the specified configuration section.

- authentication-service / location-service
  The problem occurred if these two modes together contained the critical amount of configuration entries.

- dialplan-file
  The problem occurred if such a pre-configured and downloaded call routing file contained the critical amount of lookup entries.

12153 SIP overlap dialing causing unexpected reboot

The overlap dialing feature contained a bug causing unexpected reboot when receiving duplicated SIP offers. This bug has been fixed and overlap dialing is working properly now.

12163 Reset log shows ‘HW watchdog’ as ‘Power off/Man reset’

On SN4970-90 and SN4580-90 devices resets caused by the ‘HW watchdog’ are shown as ‘Power off/Man reset’. This issue is fixed for devices produced with a hardware version higher or equal to 1.2. For devices with hardware version 1.1 the issue remains present.

12170 Changing SSRC causes one-way voice connection

In some scenarios the remote party changes the SSRC of the RTP stream. Since the SmartNode did not correctly detect this change, this could lead to a one-way voice connection. The RTP stream detection algorithm has been modified to properly detect such cases, thus avoiding any one-way voice.

Affected devices: SN4660/70, SN4940/50/60, SN4970/80/90, SN5400, SN5480/90.

12178 SIP register not working in combination with loopback interface

It is now possible to register with loopback interface. Software changes reverted for 11872 and another solution applied in 11973. See full details above.

12182 ASN1 AOC not working

Previously the AOC data processor answered with the following error message: “FACILITY IE HAS LENGTH ZERO”. The problem is fixed and now it’s possible to receive and parse SIP INFO packets with ASN1 AOC information.

12184 Crash when receiving a SIP answer without Via header

When SmartWare sends an INVITE request to a remote device it would crash with a 'SW Watchdog' exception if it received a reply completely lacking any Via header. This is fixed now and SmartWare does not crash anymore when the Via header is missing.

12191 AAA framework problem

Now it is possible to send authentication requests even if the accounting profile is not set.

Build Series 2013-01-15

11214 Ethernet speed capability for manual settings

11944 Action script trigger for SIP registration

11984 G.SHDSL interface software upgrade failed

12079 RTP payload type conflict

12115 G.SHDSL mode auto detection fixed

12120 Support for short delay re-INVITE in SBC scenario

12125 SN4991 Models with ADSL interface supported

12128 RTP through VPN broken

12130 Wrong drop cause reported by SIP endpoints, resulting in failed call hunting

12131 Spelling error corrected on BGP configuration web page

12135 SN4660/70 cooling fan speed adjusted

Build Series 2012-12-03

11863 SIP supports TCP flows according to RFC5626

11906 SNMP OID for DSL card firmware version

11916 Support for SN4832/LLA and SN4834/LLA models

11943 New NTP server in factory-config

11958 SIP AOC XML support

11959 Sending tax-pulses on FXS for AOC

12039 Incorrect answer to SIP INFO message

12062 G.SHDSL software upgrade progress indication updated

12074 Increased timeout for redirection service

12082 183 Session Progress not being forwarded in SBC scenarios

12083 Minimal SIP registration time

12086 Added support for SFP interface (Fiber interface)

12093 SIP calls over TCP failed

12097 DSL supervisor log notifies wrong DSL line state

12111 Missing user part from SIP contact header

Build Series 2012-09-17

11717 Invalid REGISTER request when spoofed contact is set

11846 SIP multipart message support

11854 Support for 4300/JO and 4400/JO products

11859 Media detection timeout

11912 Enhanced AAA debug logs

11999 New Patton corporate style applied to web interface

12014 Wrong help text for blink command

12036 Limit packets to prevent SIP overload condition

12040 SIP *register back-to-back* command removed

12043 Added option DHCP.66 error message when not available

12045 Concurrent *Dynamic IP Configuration (DIC)* removes default gateway

12055 Flash hook on FXO interface broken

Build Series 2012-07-18

11497 Configuration option for caller-ID checksum verification on FXO interface

11728 G.SHDSL interface: service-mode auto-detection

11811 ISDN status errors on Web UI

11835 MWI on FXS not working

11860 SIP re-register not working

11879 ADSL annex A/B/M

11888 Improved dial ‘on-caller-id’ on FXO

11908 Layer 2 COS for PPP and PPPoE control packets

11935 Administrator login to administrator exec mode

11937 MWI Subscription failing

11940 H.323 Call Resuming

11955 Dial tone played a second time

11981 G.S line rate negotiation fails at high distance

11989 FXO dial-tone detection

12019 Invalid SDP offer in SIP provisional response

Build Series 2012-05-23

10983 DTMF caller ID transmission on FXS

11716 Crash when a ‘#’ character is present in SIP contact header

11785 Support for p-called-party-id header

11872 Incoming SIP calls refused with 481 after an IP address change over PPP

11882 Cooling fan always running at full speed on SN4670

11889 No final answer when receiving BYE

11891 SN4660/SN4670 Rev C and Rev D support

11895 Ethernet switch problem on SN4660/SN4670

11898 Enhancement of software upgrade procedure

11899 SIP Hold/Unhold behavior

11902 SIP q-value of 1.0

11929 SN-DTA clock synchronization

11932 SIP 503 error handling

11936 Broken T.38 transmission

11942 Redirection service for provisioning supported in factory configuration

11950 Modified memory layout for SDTA, SN4552, SN4554 and SN5200

11954 FXS hanging calls

11957 Basic PRACK scenario broken

11965 **Spurious error messages from G.S interface**

11968 **Missing command ‘payload-rate’ on SN4660/SN4670**

11983 **Verbose software upgrade of G.S interface card**

11987 **Removed support for hardware version 4.x for SN4552, SN4562, SN4554, S-DTA**

Build Series 2012-03-15

11560 **Web interface generates a new identity**

11638 **PPPoA on G.S interface**

11722 **SN-Web page refresh causing reboot**

11766 **Enhance DSL status display**

11773 **DTMF Caller-ID reception on FXO**

11778 **Call transfer issue fixed**

11780 **CED-Tone Net Side Detection enhancement**

11802 **Trusted SIP hosts to improve security**

11803 **HTTP download failure blocks the SmartNode**

11804 **T.38 Fax transmission killed by CNG tone**

11810 **Auto-provisioning: redirection target reordering**

11814 **Missing strict-tei-procedure command**

11817 **Provisioning: prevent downloading incompatible configuration**

11819 **New provisioning placeholders**

11818 **Auto-provisioning factory-config (Redirection service support)**

11832 **Wrong G.S port state displayed**

11842 **SN5200 hardware-version 6.X support**

11844 **CED-Tone Net Side Detection not working**

11848 **Crash when downloading G.S firmware with web interface**

11850 **Abnormal call termination due to misinterpreted SDP data**

11852 **Auto-provisioning: Target configuration without leading http or tftp**

11855 **Ethernet lockout on SN4660/70**

Build Series 2012-01-26

11256 Echo Cancellation with RBS

11409 ETSI Caller-ID not detected on FXO

11534 Q-value support for SIP REGISTER

11636 Music on Hold not played to SIP side

11650 Removed DSL options ‘b-anfp’ and ‘a-b-anfp’

11664 Support for SN4660/SN4670 hardware Revision B

11696 Broken modem transmission using H.323

11708 Removed SIP Contact header verification in 200 OK messages

11709 First received IPCP frame dropped in during PPP connection establishment

11755 Added SDP attributes ‘X-fax’ and ‘X-modem’ support

11776 Forced Fax/Modem bypass

11787 Remote Early-H.245 initialization

11791 Wrong mapping table in R2

11806 SN-DTA and SN4120 allow usage of g729 codec

Build Series 2011-11-18

11434 Fixed T.38 packets traffic-class

11632 BRI Daughter-Board

11637 HTTP User Agent enhancement

11641 G.SHDSL power and reset spikes

11655 Syslog-client “no remote …” command crash

11674 Fixed display of mtu and mru max values in *running-config*

11675 Improved clocking precision for SN-DTA and SN4120

11684 Timestamp enhancement for milliseconds

11685 Enhanced spoofed contact to accept hostname

11697 Fax T.38 not working with H.323

11698 Wrong facility callrerouting packet in case of CFU

11726 Missing facility from running-config

11727 New DSL supervisor mode “observe”

Build Series 2011-09-15

11133 Locking DNS records for SIP requests

11487 Improved configuration and display of bit rate for 4-wire G.S interface

11592 HTTP 302 Redirection now supported for provisioning

11594 Additional parameters in G.SHDSL status: SNR, Loop Attenuation, Port States

11604 Clock synchronization improvements

11615 Fixed “police” traffic class configuration option

11622 RTP payload type configuration

11639 Received maddr parameter is reflected in contact header

11649 Proper differentiation between SN4660 and SN4670 product types

11653 Spurious errors reported by SIP and SDP protocols

11654 BRI CRC Failures

11656 Potential memory leak in SIP state machine

11676 Support for SN-DTA and SN4120 series

11676 Global power-feed for BRI

11687 Performance improvements

11700 Wrong factory-config for SN products with DSL

Caveat - Known Limitations

The following list refers to open cases in the Change Tracking System 'CTS'

CTS2236

Only G.723 high rate (6.3kbps) supported by H.323 (receive and transmit).

CTS2702

TFTP may not work with certain TFTP servers, namely the ones that change the port number in the reply. When using the SolarWinds TFTP server on the CD-ROM this problem will not occur.

CTS2980

With 10bT Ethernet ports, only the half duplex mode works. (With 10/100bT Ethernet ports, all combinations work.)

CTS3233

The SolarWinds TFTP server version 2.2.0 (1999) does not correctly handle file sizes of n * 512 Bytes. Use version 3.0.9 (2000) or higher.

CTS3760

The SIP penalty-box feature does not work with TCP. When the penalty box feature is enabled, the TCP transport protocol must be disabled using the ‘no transport tcp’ command in the SIP gateway configuration mode.

CTS3924

Changing a call-progress tone has no effect. Adding a new call-progress tone and using it from the tone set profile works however.

CTS4031

The Caller-ID message length on FXS hardware with Chip Revision numbers below V1.5 is restricted to 32 bytes. If the message is longer the message will be truncated. The FXS Chip Revision can be displayed using the ‘show port fxs detail 5’ CLI command.

CTS4038

When doing 'shutdown' and then 'no shutdown' on an ethernet port that is bound to an IP interface that receives its IP address over DHCP, the IP interface does not renew the lease.

CTS4077

Using the command ‘terminal monitor-filter’ with regular expressions on systems under heavy load can cause a reboot.

CTS4335

The duration of an on-hook pulse declared as flash-hook has been raised from 20ms to 1000ms, to cover the most country specific flash hook durations. Existing installations should not be affected, as all on-hook pulses *lower than 1000ms* are declared as flash-hook, including the previous default of 20ms.

However, care should be taken in analog line extension applications, to make sure that the flash-hook event is allowed to be relayed over SIP or H.323. This can be achieved by disabling all local call features in the fxs interface on context cs: no call-waiting, no additional-call-offering, no call-hold.

CTS10392

The internal timer configuration command is only able to execute commands that produce an immediate result. Some commands that execute asynchronously cannot be executed by the timer. The following commands (among others) cannot be executed by the timer:

- **ping**
- **traceroute**
- **dns-lookup**
- **copy** any kind of files from or to a TFTP server
- **reload** without the **forced** option

CTS10553

The command “no debug all” does not fully disable the ISDN debug logs. As soon as any other ISDN debug monitor is enabled, all the ISDN monitors that were disabled by “no debug all” are re-enabled.

CTS10586

The codecs G.723 and G.729 cannot be used at the same time on all platforms, except on the SmartNode 4960.

CTS10610

SmartNode 4960 Gigabit Ethernet does not properly work with Dell 2708 Gigabit Ethernet Switch. A work-around is to configure 100Mbit.

CTS10730

Due to memory limitations it is not possible to download a software image to the SN4552 when two SIP gateways are active.

CTS11114

On SN46xx units it can happen that there are more open phone calls requiring a DSP channel than DSP channels are available. This leads to the situation where a phone connected on a bri port rings and has no voice after the user picks it up. To limit the number of calls using DSP channels it is suggested to create a limiter service where each call from and to a bri port has to pass. When the total number of calls on the bri ports is limited to the number of DSP channels each call is going to have audio on picking up.

CTS11786

On older SmartNodes the two debug monitors *debug media-gateway rtp* and *debug call-control* print out incorrect RTCP jitter values.

CTS11816

The command ‘call-control call drop <call>’ is not behaving as expected. It drops all calls but does not completely teardown all internal structures. Consequently the call numbers of the dropped call cannot be used anymore for further calls after executing this command. The same is true for the “Drop all” button on the web interface on the “Active Calls” tab of the Call-Router section.

CTS12027

The following configuration may create duplicate packets: If one physical ethernet port is bound to two IP interfaces with different IP addresses and on both IP interfaces a SIP gateway is bound and some static routes are configured, then the SIP gateways may receive duplicate UDP packets.

General Notes

Factory Configuration and Default Startup Configuration

The SmartNodes as delivered from the factory contain both a **factory configuration** and a default **startup configuration**. While the factory configuration contains only basic IP connectivity settings, the default startup configuration includes settings for most SmartWare functions. Note that if you press and hold the system button (Reset) for 5 seconds the factory configuration is copied onto the startup configuration (overwrite). The default startup config is then lost.

IP Addresses in the Factory Configuration

The factory configuration contains the following IP interfaces and address configurations bound by the Ethernet ports 0/0 and 0/1.

```
interface eth0
  ipaddress dhcp
  mtu 1500
interface eth1
  ipaddress 192.168.1.1 255.255.255.0
  mtu 1500
```

New Configuration Commands

The commands documented in the Release Notes only cover new additions which are not yet included in the Software Configuration Guide for R6.5, available from www.patton.com .

http://www.patton.com/manuals/07MSWR65_SCG-UM.pdf

Current Revision:

Part Number: *07MSWR65_SCG, Rev. A*
Revised: January 23, 2014

SIP Trusted Host enhancement: answer-untrusted-hosts

First appeared in build series: 2014-03-12

New CLI command in context sip-gateway: *answer-untrusted-hosts*. It specifies if an error message (SIP/2.0 503 Service Unavailable) or nothing at all should be replied to non-trusted hosts.

Mode: context sip-gateway

	Command	**Purpose**
Step 1	**[node](sip–gw)[SIP]# [no] answer-untrusted-hosts**	Configures whether '503 Service Unavailable' message should be answered or untrusted hosts should be ignored

Configurable time zone for CDR messages (accounting data)

First appeared in build series: 2014-03-12

New CLI command in AAA profile: *local-time-cdr*. If this is set, the time in the CDR messages will be in local time instead of UTC. To avoid confusion, there is a label in the CDR for every call specifying the time (Local/UTC).

Mode: profile aaa

	Command	**Purpose**
Step 1	**[node](pf–auth)[AAA]# [no] local-time-cdr**	Configures whether the time in CDR messages will be local or UTC

Removed "no" form of address-translation incoming commands

First appeared in build series: 2014-03-12

The “no” form of all address-translation incoming-call commands in the sip interface are now removed. They were inconsistent with the address-translation outgoing-call commands. Default parameter for address-translation incoming-call calling-redir is now diversion-header.

Mode: interface sip

	Command	Purpose
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call called-e164**	Removed
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call called-name**	Removed
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call called-uri**	Removed
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call calling-e164**	Removed
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call calling-name**	Removed
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call calling-redir**	Removed
Step 1	**[node](if –sip)[IF_SIP]#no address-translation incoming-call calling-uri**	Removed

With the channel-group model on E1T1 it is possible to share the same link for different protocols. For a partial ISDN usage the *encapsulation voiceband* command was missing. With that type of encapsulation the user defines which b-channels are available for ISDN voice transmission. See full details in the *New configuration commands* section.

E1T1 channel-group encapsulation voiceband

First appeared in build series: 2014-03-12

With the channel-group model on E1T1 it is possible to share the same link for different protocols. For a partial ISDN usage the *encapsulation voiceband* command was missing. With that type of encapsulation the user defines which b-channels are available for ISDN voice transmission. See full details in the New configuration commands section.

Mode: channel-group

	Command	Purpose
Step 1	**[node](ch-grp)[name]#encapsulation voiceband**	Assignes voiceband encapsulation for the selected timeslots.

SIP B2BUA dynamic registration setup

First appeared in build series: 2013-11-13

This new feature gives the possibility to trigger an outbound registration when a matching inbound registration has been detected. As prerequisite you will need to define an inbound registration for the desired identity in the location service. You will need to define a registrar in the outbound registration configuration as well.

Mode: location-service

	Command	Purpose
Step 1	**[node](ls)[name]#[no] identity <name>**	Adds a new identity to the location service.
Step 2	**[node](identity)# [no] authentication inbound**	Define if inbound authentication is used or not.
Step 3	**[node](identity)# [no] authentication outbound**	Define if outbound authentication is used or not.
Step 4	**[node](identity)[name]# [no] registration inbound**	Add inbound registration
Step 5	**[node](identity)[name]# [no] registration outbound**	Add outbound registration
Step 6	**[node](regout)# [no] register [auto|none|back-to-back]**	Set the back-to-back parameter in the outbound registration configuration

Local tax pulse generation on FXS

First appeared in build series: 2013-11-13

It is possible to generate and send tax pulses locally on the FXS port. This only happens for calls originating from the connected Phone. As soon as the called party picks up the call, the SmartNode sends the first tax pulse towards the connected phone. For the ongoing call a new tax pulse is generated and sent when the configured pause time has expired. At termination of the call no pulse is generated.

Mode: interface fxs

	Command	Purpose
Step 1	**[node](if-fxs)# [no] aoc generate-tax-pulses <**pause between pulses**>**	Configures local generation and sending of tax-pulses. As parameter the pause time between the pulses in seconds is provided. Default: disabled.

SIP notify check-sync event

First appeared in build series: 2013-11-13

Now it is possible to trigger auto-provisioning with a SIP NOTIFY request. Basically the SIP gateway has to be configured to accept the related packet which will trigger an action script event when the proper information arrived. Finally the action will execute the configured provisioning. The notify packet has to contain the following information:

- A required “Event” header which must be “check-sync”

- An optional “reboot” parameter can be set inside the “Event” header. The possible values are: “true” or “false”. If this parameter is missing then true will be assumed.

Mode: context sip-gateway

	Command	Purpose
Step 1	**[node](sip–gw)[GW_SIP]#[no] notify check-sync accept**	Configures whether the notify check-sync packet will be accepted or not. Default: disabled

Mode: actions

	Command	Purpose
Step 1	**[node](act)# rule RULE**	Defines the rule under which the condition has to be checked.
Step 2	**[node](act)[RULE]# condition sip <gateway: gatewayname> { NOTIFY_CHECK_SYNC_NORELOAD | NOTIFY_CHECK_SYNC_RELOAD }**	Defines the condition under which the action has to be executed.
Step 3	**[node](act)[RULE]# action "provisioning execute <pf-name>"**	Defines the action which has to be executed.

Mode: profile provisioning

	Command	Purpose
Step 1	**[node](pf-prov)[<pf-name>]# [no] activation reload { deferred | graceful | immediate }**	Sets what should happen at the end of provisioning.

Set traffic-class on the sip gateway

First appeared in build series: 2013-09-13

The traffic-class command in the call outbound identity of the location service is now deprecated and is replaced by the following new command in context sip-gateway.

Mode: context sip-gateway

	Command	Purpose
Step 1	**[node](sip-gw)[gw-name]#traffic-class <traffic-class>**	Sets a traffic class on the sip gateway. SIP signaling packets sent from this gateway will be tagged with this traffic class.

AOC in SIP Header format

First appeared in build series: 2013-07-17

In addition to the existing XML and ASN1 format, SmartWare also allows sending and receiving Advice Of Charge in SIP Header format.

Mode: interface sip

	Command	Purpose
Step 1	**[node](if-sip)[if-name]#[no] aoc-format { asn1 | xml | sip-header }**	Sets the SIP interface AOC format Default: asn1

X-USE302 SIP Header

First appeared in build series: 2013-07-17

In order to indicate to some IP-PBX to use the SIP 302 Moved Temporarily response, it is necessary to set the parameter as follow:

Mode: interface sip

	Command	Purpose
Step 1	**[node](if-sip)[if-name]#[no] x-use302**	Add the x-use302 SIP header (default: disabled)

Unique SIP connection ID for calls

First appeared in build series: 2013-07-17

In case of CFU (call forwarding unconditional) it is impossible to relate the two invite packets. Let's take a simple scenario. If one has sent an invite packet to the target device and received "302 moved temporarily" back then a new peer address is received in this packet. Then another invite packet has to be sent to this new peer. In both invite packets a Call-ID header is added but they must be different according to the standard. This makes it impossible to realize that they are technically the same call The following command can be used can be used to enable an ID as a SIP header which is unique in such a scenario.

Mode: interface sip

	Command	Purpose
Step 1	**[node](if-sip)[name]#[no] x-org-connid accept**	With this command the user can enable or disable whether the x-org-connid header will be parsed. (Default: disabled)
Step 2	**[node](if-sip)[name]#[no] x-org-connid emit**	With this command the user can enable or disable whether the x-org-connid header will be sent. (Default: disabled)

Configurable calling party or facility IE on ISDN

First appeared in build series: 2013-07-17

Defines if called-party numbers starting with '#' or '*' characters are sent in a keypad-facility info-element or in a calling-party info-element. When this *Keypad-facility* command is inverted, the called-party number is placed in a calling-party info-element.

Mode: context cs switch

	Command	Purpose
Step 1	**(if-isdn)[if-name]# [no] keypad-facility**	Default: enabled

Determine reachability with SIP OPTION requests

First appeared in build series: 2013-07-17

Normally a SIP call is started by sending an INVITE request to the destination. If that destination is unavailable for any kind of reason it could take some time to detect that this destination is failing. During that time the party who initiated the call is waiting for the ring-back tone as feedback. To try an alternative path to reach the called destination it is practically too late because the caller gave up during that time. It is now possible to determine the reachability of destinations ahead of actual calls. For a failing destination an alternative routing path to the called end user could be issued immediately without having a timeout.

This is done by periodically sending SIP OPTION requests to the configured remote address. If we receive an answer for that OPTIONS request the destination is still alive and calls are forwarded toward it. For the reachability the content of the answer does not matter, neither if the answer is a failing or successful one. If there is no answer during the configured timeout, the remote destination is added to the penalty-box. For a certain time such destinations are considered not reachable, no requests are sent to them and calls can be redirected immediately without timeout. This could happen for example with a hunt-group service in the call-control.

Mode: interface sip <name>

	Command	Purpose
Step 1	**[node](if –sip)[<name>]#[no] penalty-box [sip-option-trigger interval <seconds> timeout <seconds>]**	Enables penalty-box with optional sending of OPTIONS requests ahead of calls.

SDP ptime attribute

First appeared in build series: 2013-07-17

The SDP *ptime* attribute announces the maximum receive duration for the offered coders. Because *ptime* can only be offered on media level and not on a per coder basis, SmartWare selects the *rx-length* of the first configured coder as value for the *ptime* attribute. By default the new attribute is not included in SIP's SDP content. It can be configured to be included with the voip profile's *sdp-ptime-announcement* command.

Mode: profile voip

	Command	Purpose
Step 1	***node*(pf-voip)[name]#[no] sdp-ptime-announcement**	Enables/Disables announcement of the *ptime* attribute in SIP's SDP content. Default: disabled

SIP request URI length limitation

First appeared in build series: 2013-07-17

This new feature allows denying incoming SIP request whose URI length exceeds a user specified value. Limiting the request URI length has device wide validity. The configured number of characters is applied for all incoming SIP requests on the whole device. Therefore the *max-request-uri-length* is located in the global *sip* configuration mode. By default the request URI length is unlimited.

Mode: sip

	Command	Purpose
Step 1	***node*(sip)#[no] max-request-uri-length <length>**	Enables/Disables request URI length limitation. The given *length* specifies the maximum number of characters including all URI parameters. Default: disabled

Local RAS port is configurable for H.323

First appeared in build series: 2013-07-17

Up until now RAS messages were sent from the same local port number as it was configured for the local call-signaling port. This caused problems for H.323 gatekeepers which required different port numbers. Therefore the local port for RAS messages can now be configured. If it is not configured, the same port number as for call signaling is taken as local RAS port.

Mode: gateway h323 <name>

	Command	Purpose
Step 1	***node*(gw-h323)[<name>]# [no] ras [<port>]**	Enable registration authentication service with optionally specifying the local signaling port

Alcatel signaling method for flash-hook SIP info message

First appeared in build series: 2013-05-16

The following command can be used for the configuration:

Mode: profile voip

	Command	Purpose
Step 1	**[node](pf-voip)[name]#flash-hook-relay [dtmf | rtp | signaling [default|broadsoft|alcatel]]**	With the “flash-hook-relay” command the user can chose a different relay method for flashhook than for the other DTMF keys. The default setting is dtmf.

Upload profile for CDR records

First appeared in build series: 2013-05-16

Local CDR records can be uploaded to a TFTP or HTTP server. In order to have CDR records stored locally on the SmartNode, you first have to define it through the AAA call service (see configuraton notes). The format of the CDR records can either be plain (*cdr* as source) or in CSV (*cdr-csv* as source).

Profile setup

Mode: configure

	Command	Purpose
Step 1	**(cfg)# profile upload <name>**	Create an upload profile
Step 2	**(pf-upload)[name]# location { tftp://<hostname>/<file> | http://<hostname>/<file> }**	Define the location list (file destinations to be tried sequentially)
Step 3	**(pf-upload)[name]# source { cdr | cdr-csv }**	Specify the type of upload

Execute an upload profile

This command executes the upload profile. This command is useful to use the upload functionality along with a timer.

Mode: enabled

	Command	Purpose
Step 1	**# upload execute <profile>**	Execute the upload profile

SNMP allowed network

First appeared in build series: 2013-05-16

Allow a full network range to send SNMP request to the SmartNode.

Mode: configure

	Command	Purpose
Step 1	**(cfg)# snmp network <network-ip> <netmask> security-name <community>**	Define a network range with a specific community

EFM interface configuration

First appeared in build series: 2013-05-16

With these commands the configuration of the EFM interface can be done transparently. The parameters are applied directly to the interface.

Mode: port dsl <slot> <port>

	Command	Purpose
Step 1	**[node](prt-eth)[slot/port]# annex-type { a-f | b-g }**	Set the annex-type Default: a-f
Step 2	**[node](prt-eth)[slot/port]# mode { co | cpe }**	Set the mode Default: cpe
Step 3	**[node](prt-eth)[slot/port]# payload-rate { 0192 | … | 5696 }**	Set the payload rate Default: 1088
Step 4	**[node](prt-eth)[slot/port]# service-mode { 2-wire | 4-wire | 6-wire | 8-wire }**	Set the amount of pairs Default: 2-wire
Step 5	**[node](prt-eth)[slot/port]# [no] shutdown**	Enable/disable the DSL port on the card Default: no shutdown

Network and user provided secondary calling party number

First appeared in build series: 2012-03-14

ISDN

Basically ISDN can send two calling party numbers but previously only the first one was parsed. Now the second number is also read if it is available. The incoming part of this feature is not configurable because all available information is going to be parsed without any condition. Right after that the outgoing side can decide what and how the information should be forwarded.

Mode: interface isdn

	Command	Purpose
Step 1	**[node](if –isdn)[IF_ISDN]#calling-party-number emit { single-primary | single-secondary | single-user | single-network | double-primary-first | double-secondary-first | double-user-first | double-network-first }**	Configures which calling party number in which order has to be sent (default: single-primary)

- **single-primary**: Sends only the first number if exists.

- **single-secondary**: Sends only the second number if exists. Otherwise sends only the first number if exists.
- **single-user**: Sends only the first user provided number if exists. If neither are user provided then first is going to be sent if exists.
- **single-network**: Sends only the first network provided number if exists. If neither are user provided then first is going to be sent if exists.
- **double-primary-first**: Sends both numbers if they exist. The order remains the same (transparent).
- **double-secondary-first**: Sends both numbers if they exist. The order is going to be reverse.
- **double-user-first**: Sends both numbers if they exist. The first number is going to be the first user provided. If neither are user provided then use natural order.
- **double-network-first**: Sends both numbers if they exist. The first number going to be the first network provided. If neither are network provided then use natural order.

SIP

Basically SIP can send three calling party numbers but previously only the first two were parsed. Now all three numbers are read if it they are available. These three numbers can come from the following places:

- From header
- P-Asserted-Identity header
- P-Preferred-Identity header

Enabling SIP RFC Privacy, Asserted-Identity and Preferred-Identity headers (RFC3323 / RFC3325)

The following command sequence enables support for the SIP Asserted-Identity, Preferred-Identity and Privacy headers, which are described in RFCs 3323 & 3325. This provides the required identity to SIP entities. The privacy header suppresses the forwarding of the identity to the final station. Handling of the Identity headers can be configured in the same way as for any other SIP header using the address-translation command in the SIP interface configuration mode. The privacy header is mapped to the call-control's presentation indicator property field. The type of header sent depends on the screening-indicator property of the call-control. When receiving one of these privacy headers the screening-indicator is also set depending on the received header type.

Mode: interface sip

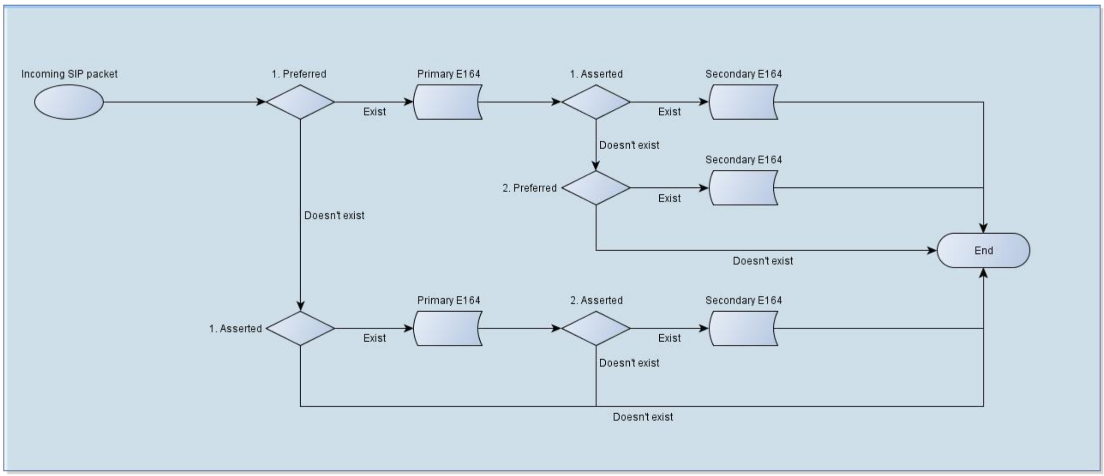
	Command	Purpose
Step 1	**[node](if –sip)[IF_SIP]#[no] privacy**	Enables / Disables privacy (default: disabled)
Step 2	**[node](if –sip)[IF_SIP]#address-translation incoming-call calling-e164 { fix | from-header | identity-header }**	Enables calling party number mapping (default: identity-header)

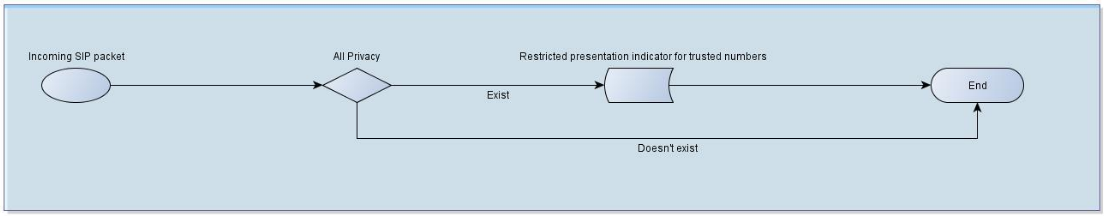
Step 3	**[node](if –sip)[IF_SIP]#address-translation outgoing-call identity-header user-part call e164 { single-primary | single-secondary | single-user | single-network | double-primary-first | double-secondary-first | double-user-first | double-network-first }**	Configures which calling party number in which order has to be sent (default: single-primary)

- **fix**: Sets a preconfigured static number as a first calling party number. Second calling party number is going to be empty.
- **from-header**: Takes the first calling party number from "From" header and the second from Identity header.
- **identity-header**: Takes both calling party numbers from Identity headers. If they do not exist then the fallback algorithm will take the first calling party number from the "From" header.

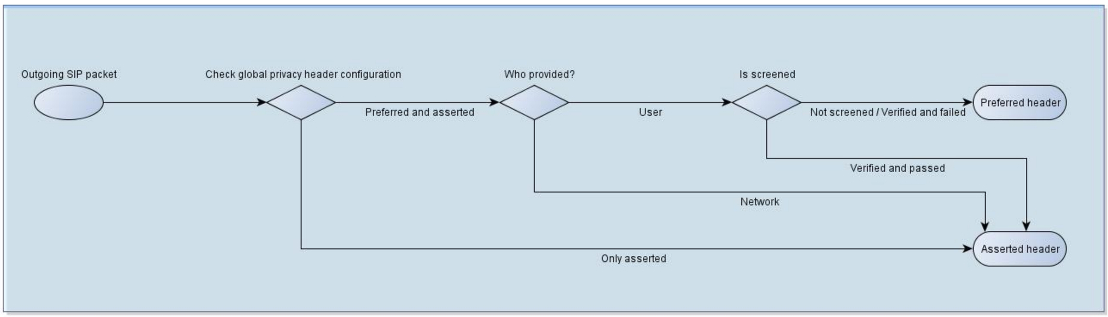
- **single-primary**: Sends only the first number if exists.
- **single-secondary**: Sends only the second number if exists. Otherwise sends only the first number if exists.
- **single-user**: Sends only the first user provided number if exists. If neither are user provided then first is going to be sent if exists.
- **single-network**: Sends only the first network provided number if exists. If neither are user provided then first is going to be sent if exists.
- **double-primary-first**: Sends both numbers if they exist. The order remain the same (transparent).
- **double-secondary-first**: Sends both numbers if they exist. The order is going to be reverse.
- **double-user-first**: Sends both numbers if they exist. The first number going to be the first user provided. If neither are user provided then use natural order.
- **double-network-first**: Sends both numbers if they exist. The first number going to be the first network provided. If neither are network provided then use natural order.

SIP identity-header -> Call-Control parameter mapping





Call-Control -> SIP identity-header parameter mapping



Encryption key provisioning

First appeared in build series: 2013-03-14

Key provisioning is now possible in SmartWare. It uses the same principle as the other existing provisioning options (e.g. configuration or dial plan provisioning).

Mode: profile provisioning

	Command	Purpose
Step 1	**[node](pf-prov)[<pf-name>] # destination key**	Sets the destination for the downloaded file in local key
Step 2	**[node](pf-prov)[<pf-name>] # location tftp://<server>/<file>**	Location of the key file on the remote TFTP server.

Ethernet port manual mode for speed and duplex

First appeared in build series: 2013-01-15

Until now, it was only possible to force capabilities of an ethernet port by using auto negotiation with single capabilities. It is now possible to force the capabilities by using "true" manual mode. This new mode is only available for SN4660/70, SN4940/50/60/70, SN4600 and SN-DTA.
The following command can be used for the configuration:

Mode: port ethernet <slot> <port>

	Command	Purpose
Step 1	**[node](prt-eth)[slot/port]# medium { auto | negotiated { 10 | 100 | (1000) } { half | full } | manual { 10 | 100 } { half | full } }**	Set the medium mode Default: auto

Note : Be aware that using manual mode to define the Ethernet port speed and duplex is not recommended as this might result in problems to detect cable or connectivity issues. It is generally more reliable to use the negotiated parameters.

Action script trigger for SIP registration

First appeared in build series: 2013-01-15

SmartWare supports action scripts which provide the possibility to execute user defined CLI commands when a specific event has occurred. Now two additional events have been added to the framework: REGISTERED and NOT_REGISTERED. The REGISTERED event occurs when the first identity belonging to the specified SIP gateway has registered. The NOT_REGISTERED event occurs when the last registered identity belonging to the specified SIP gateway has unregistered or the registration has become invalid.

Mode: rule

	Command	Purpose
Step 1	**[node](act)[RULE]# condition ip <routername:interfacename> { LINKUP | LINKDOWN }**	Defines the condition under which the action has to be executed.
	[node](act)[RULE]# condition sip <gateway: gatewayname> { REGISTERED | NOT_ REGISTERED }	Defines the condition under which the action has to be executed.

SIP supports TCP flows according to RFC5626

First appeared in build series: 2012-12-03

SmartWare supports the ‘User Agent Procedures’ described in RFC5626 with the exception of ‘Keep-Alive with STUN’. Registrations can now open a TCP flow to the registrar and keep it open through CRLF keep-alive or other messages. Through that flow calls can traverse through NAT and reach the registered user. Together with this addition some of the older nat-traversal and keep-alive capabilities were extended too. A summary is provided here of all nat-traversal commands for registrations and calls.

Registration nat-traversal disabled

When nothing is configured all nat-traversal procedures are disabled. With this command a configured nat-traversal mode can be removed and the normal registration behavior is restored.

Mode: registration outbound

	Command	Purpose
Step 1	**[node](regout)# no nat-traversal**	Disables nat-traversal procedures. Default: disabled.

Registration nat-traversal mode: minimal (new)

In nat-traversal mode minimal the goal is to register the globally accessible NAT address, but without having an additional keep-alive mechanism. This could be the case when the registrar server has such a mechanism, the NAT does not need such or the registration lifetime is short enough that the keep-alive is done with the REGISTER requests.

In this mode a REGISTER request is first sent with the local IP address as contact and the ‘rport’ option. If that request results in a successful answer the ‘received’ and ‘rport’ parameters are examined to detect the globally accessible IP address and port. With these correct parameters a second REGISTER request with the corrected contact header is then sent to the registrar.

Mode: registration outbound

	Command	Purpose
Step 1	**[node](regout)# nat-traversal minimal**	Activate nat-traversal without keep-alive.

Registration nat-traversal mode: nortel (no change)

This is the nat-traversal method to use together with certain Nortel devices. The discovery of the global IP address and port is done by sending a PING request and examining the answer to that. After that a REGISTER request with the global IP address in the contact header is sent for registration. Once registered the keep-alive is achieved with sending PING requests.

Mode: registration outbound

	Command	Purpose
Step 1	**[node](regout)# nat-traversal nortel [keepalive-interval <**seconds**>]**	Activate nat-traversal the Nortel way. Default keepalive-interval: 55 seconds.

Registration nat-traversal mode: keep-alive (enhanced)

Up until now this mode always used OPTIONS requests for achieving the keep-alive. In addition SmartWare supports PING requests for the same purpose. OPTIONS is still the default when not explicitly specified otherwise in the command.

This nat-traversal method executes the same procedure for registration as the minimal mode. After that either OPTIONS or PING requests are sent periodically for keeping the NAT open and detect changes.

Mode: registration outbound

	Command	Purpose
Step 1	**[node](regout)# nat-traversal keep-alive [options | ping] [keepalive-interval <**seconds**>]**	Activate nat-traversal with OPTIONS or PING as keep-alive. Default keepalive-interval: 55 seconds.

Registration nat-traversal mode: flows (new)

When nat-traversal flows is selected then most of the 'User Agent Procedures' described in RFC5626 are executed for outbound registrations. Each sip gateway maintains its unique instance ID which is used on the registrar to distinguish between flows for different gateways or devices. For each registration the destination IP address is determined by the normal procedure. If a flow already exists for that destination, then the REGISTER request is sent through that flow. Otherwise a new flow to that destination is created before sending the request.

SmartWare currently does not support creating multiple flows for the same registered identity. Therefore the 'reg-id' parameter always is '1'. If a REGISTER request receives a successful answer SmartWare checks the 'received' and 'rport' parameters for correctness of the registered contact. If they do not match, a new REGISTER request with corrected values is sent out. This can happen over the same flow as the previous one or over a newly created flow depending on the destination IP address resolution.

Once a correct contact is successfully registered, the configured keep-alive mechanism is started for the flow of that successful request. When a failure of a flow is detected through the keep-alive mechanism, all registrations associated with that flow are discarded and the registration procedure is started anew. Flows created for requests which were not successful and which are not used by other active calls or registrations are terminated after 120 seconds of idle time.

Flows can be used for other outgoing requests, depending on the configuration. Incoming requests through flows are treated the same was as if they were received through the listening socket of the sip gateway. This ensures that the registrar server can forward calls through NAT to the registered user.

For flows the following keep-alive mechanisms can be configured:

- **no-keep-alive**: Register through flows, but do not start a keep-alive mechanism. This could be the case when the registrar server has such a mechanism, the NAT does not need such or the registration lifetime is short enough that the keep-alive is made with the REGISTER requests.
- **CRLF**: Start the CRLF keep-alive mechanism on **TCP flows** as described in FRC5626. For UDP flows no keep-alive is started with that configuration.
- **options**: Send OPTIONS request in periodic intervals over that flow to keep it active and detect failure or changes.
- **ping**: Send a PING request in periodic intervals over that flow to keep it active and detect failure or changes

Mode: registration outbound

	Command	Purpose
Step 1	**[node](regout)# nat-traversal flows (no-keep-alive | CRLF | options | ping) [keepalive-interval <**seconds**>]**	Activate nat-traversal with flows. Default keepalive-interval: 55 seconds.

Calls using flows (new)

The concept of flows can be used for calls to. When flows are opened by registrations these are re-used for outgoing calls as well, but only if the target resolution procedures for calls are resulting in an IP address which a flow already exists for. Otherwise new flow is created for the duration of the call.

This does not affect incoming calls. Incoming calls are accepted through flows or outside of flows in the same way.

Mode: call outbound

	Command	Purpose
Step 1	**[node](callout)# [no] nat-traversal flows**	Configured if INVITE requests are sent out through flows.

SIP AOC (Advice of Charge)

First appeared in build series: 2012-12-03

With these commands the SmartNode can receive and send Advice Of Charge in ASN1/XML format. Please note that ASN1 format is only supported during a call.

Mode: interface sip

	Command	Purpose
Step 1	**[node](if -sip)[IF_SIP]#[no] aoc-s { accept | emit }**	Enable/disable the SIP interface AOC accept/emit feature at the beginning of a call (default: disabled)
Step 2	**[node](if -sip)[IF_SIP]#[no] aoc-d { accept | emit }**	Enable/disable the SIP interface AOC accept/emit feature during a call (default: disabled)
Step 3	**[node](if -sip)[IF_SIP]#[no] aoc-e { accept | emit }**	Enable/disable the SIP interface AOC accept/emit feature at the end of a call (default: disabled)
Step 4	**[node](if -sip)[IF_SIP]#[no] aoc-format { asn1 | xml }**	Sets the SIP interface AOC format (default: asn1)

Sending tax-pulses on FXS for AOC

First appeared in build series: 2012-12-03

Received AOC information can be forwarded from ISDN or SIP interfaces towards analogue FSX lines. The AOC information is converted from units or currency to a number of tax pulses which are sent out.

AOC-D information received during the call is converted into tax-pulses and these tax pulses are sent out. Subsequent AOC-D information is converted into tax-pulses as well, but only the number of tax-pulses is sent out which is above the total of already sent pulses.

For example: During a call three AOC-D messages are received: the first results in 2 tax pulses, the 2 tax pulses are sent out immediately. The second AOC-D message results in 4 tax pulses, then 2 tax pulses are sent out. Now the third AOC-D message results in 5 tax pulses then only one is sent out. The total of sent out tax pulses is now 5 which corresponds to the amount received with the last message.

Technically the same happens for AOC-E information which is received at the end of a call. But there are two major issues with this. If the user who connected the FXS port did terminate the call with a hang-up, then it is not possible anymore to send tax pulses to that user because the line is on-hook and nobody is listening. The second issue is when the tax pulses from the AOC-E are no higher than the total of already sent pulses form AOC-D messages, in which case no additional pulses have to be sent.

The conversion from AOC to tax pulses is rounded up to provide a higher charge to the user in case of doubts in a way that the amount on the bill never is any bigger than expected from the AOC information. This should prevent the user from bad surprises.

Conversion from units into tax-pulses

If the AOC information received from the SIP or ISDN peer contains units then the number of tax pulses is calculated as this:

Number of tax pulses = round up (Units received / configured units-per-pulse)

For example: Configuration: ‘aoc emit-tax-pulses 12’. Units received: 50. Then the number of tax pulses = round up(50 / 12) = 5

Conversion from currency into tax-pulses

If the AOC information received from the SIP or ISDN peer contains currency then currency has to be converted first into units. This is because the currency information itself consists of an amount and a multiplier.

List of possible currency multipliers:

- one-thousandth
- one-hundredth
- one-tenth
- one
- ten
- hundred
- thousand

Units received = Amount received * currency-multiplier received / currency-multiplier configured

Number of tax pulses = rounded up (Units received / units-per-pulse configured).

In this sense the configured currency multiplier establishes a relation between the received currency and the units used for calculation of the tax pulses. To express for example that one tax pulse is worth 5 euro-cents the command would be: ‘aoc emit-tax-pulses 5 one-hundredth’.

For example: Configuration: ‘aoc emit-tax-pulses 5 one-thousandth’. Currency amount received: 2. Currency multiplier received: one-hundredth. Then units received = 2 * (1/100) / (1/1000) = 20. Then tax pulses sent are = round up(20 / 5) = 4. The configuration specifies to send two tax pulses for each received euro-cent and therefore 4 tax pulses are sent because 2 euro-cents have been received.

Mode: interface fxs

	Command	Purpose
Step 1	**[node](if-fxs)# [no] aoc emit-tax-pulses <**units-per-pulse**> [<**currency-multiplier**>]**	Configures conversion and sending of AOC as tax-pulses. Default: disabled. Default currency-multiplier: one-hundredth.

Enable/disable early-proceeding on SIP interface

First appeared in build series: 2012-12-03

In SBC scenarios, it is possible that multiple provisional responses (1xx) are not correctly forwarded. This can be corrected by *disabling* the early-proceeding parameter on SIP interfaces. In case of PSTN gateway scenarios, it is preferable to leave the early-proceeding parameter set to *enabled* on SIP interfaces.

Mode: interface sip

	Command	Purpose
Step 1	**[node](if-sip)# [no] early-proceeding**	Automatically switches to proceeding state without receiving any provisional response (Default:enabled)

Set SFP mode

First appeared in build series: 2012-12-03

Some SmartNode models provide an SFP port which is compatible with Fiber SFP modules. This interface provides a new Ethernet port to the user. This port is configured in *port ethernet 1 0* mode.

This ethernet port supports the following SFP modules:

- Gigabit Ethernet single/multi-mode Fiber and Copper modules
- Fast Ethernet single/multi-mode fiber modules

SFP modules are automatically detected and configured following the INF-8074i specification for SFP transceivers. The command *show port ethernet 1 0* gives information about the port status and also about the SFP module which is plugged in.

If the SFP module does not follow the INF-8074i specification and can therefore not be properly configured, following command can be used for manual configuration:

Mode: port ethernet <slot> <port>

	Command	Purpose
Step 1	**[node](prt-eth)[slot/port]# [no] sfp-mode { auto | 1000Base-SX | 100Base-FX }**	Set the SFP port mode Default: auto

Mode 'auto' is the default and will automatically configure the SFP port with the correct mode when a SFP module is detected. This is the meaning of all options:

- auto => use auto-detection mode following INF-8074i specification (default)
- 1000Base-SX => configure for Gigabit Ethernet Fiber/Copper module
- 100Base-FX => configure for Fast Ethernet Fiber module

The medium is not configurable and always uses auto-negotiation.

Limit packets to prevent SIP overload condition

First appeared in build series: 2012-09-17

It is possible to limit the maximum amount of incoming SIP packets which are stored to be handled and processed later on. This guarantees a responsive system even in an overload condition. It handles and parses still as much requests as possible but the excess is simply discarded.

When more SIP requests are arriving than SmartWare can handle, the overall system performance decreases. This is because internal resources are occupied for requests which cannot be handled in time. This causes re-transmissions of these requests and adds additional overhead to the system. In order to avoid such a condition where no successful processing of requests is possible anymore, it is better to drop packets early in the processing queue.

Best overall performance in processing the highest number of successful call attempts with a continuously overloaded system was reached by setting this queue limit to a value of 8.

Mode: sip

	Command	Purpose
Step 1	**[node](sip)#[no] max-queued-packets <number of packets>**	Limits the internal SIP queue to discard any packets when the configured number of packets is reached. Suggested: 8

FXO caller-ID checksum verification

First appeared in build series: 2012-07-18

This configuration only has an influence when the caller-ID format is either 'etsi' or 'bell'. These are the two formats which provide a checksum. All of the caller-ID formats with DTMF are not affected because they have no checksum at all.

Enabled (old default behavior)

Until now SmartWare accepted a caller-ID only if it had a valid checksum. A caller-ID without checksum or with an invalid checksum was discarded. The user can establish the old behavior with enabling the caller-ID verification.

Disabled (new default behavior)

The default behavior is changed now that the caller-ID verification is disabled. Here the calling e164 is filled with the received caller-ID data no matter if a checksum is valid or present at all.

Screening-indicator (for advanced use)

Besides the basic setting (enabled/disabled) a third option 'screening-indicator' exists for advanced use. It fills in the received caller-ID to the calling e164 no matter if a checksum is present or valid. But besides that it sets the calling screening-indicator according to the checksum. This allows the user doing manipulation of the call (for example set the caller name) with mapping tables (calling-si) in the call router depending on the validity of the checksum.

- **user-not-screened**: This is the default value of the screening-indicator and is present when no caller-ID was received or the caller-ID verification is configured to ‘enabled’ or ‘disabled’.
- **user-passed**: This indicates that a caller-ID with a valid checksum has been received.
- **user-failed**: This indicates that a caller-ID with no or invalid checksum has been received.

Please be aware that this use of the screening indicator is slightly different from its original meaning in ISDN. If such calls are routed to ISDN side-effects could arise depending on the value of the screening indicator.

Summary of configuration

	Configuration of caller-ID verification		
	disabled (default)	**enabled**	**screening-indicator**
caller-ID present and checksum valid	insert caller-ID in calling e164	insert caller-ID in calling e164	insert caller-ID in calling e164 and set calling screening-indicator to ‘user-passed’
caller-ID present and checksum invalid or not present	insert caller-ID in calling e164	-	insert caller-ID in calling e164 and set calling screening-indicator to ‘user-failed’
caller-ID not present	-	-	-

For configuration select the desired caller-ID format on the FXS interface.

Mode: interface fxo

	Command	**Purpose**
Step 1	**[node](if-fxo)# caller-id verification { disabled | enabled | screening-indicator }**	Specifies if the checksum of the caller-ID needs to be verified or ignored. (default: disabled)

G.S service-mode auto-detection

First appeared in build series: 2012-07-18

With this command the SmartNode can be configured to automatically detect the G.SHDSL service-mode. It is able to detect whether it is connected to a 2-wire or a 4-wire line. The feature does not detect the interleave nor the enhanced mode. The preferred mode in case a 4-wire line is detected must be configured by the user. Therefore the original service-mode command behaves as a preferred service mode if this feature is enabled. It allows defining the exact 4-wire mode to be selected in case a 4-wire line is detected. Please note that this command is only available if G14 release or later is installed to the G.S interface.

Mode: port dsl

	Command	Purpose
Step 1	**[node](prt-dsl)[0/0]#[no] autodetect-service-mode**	Enable/disable the G.S service-mode auto-detection feature (default: disabled)

Setting annex type

First appeared in build series: 2012-07-18

Mode: port dsl

	Command	Purpose
Step 1	**[node](prt-dsl)[0/0]#annex { a | b | m }**	Sets the annex type for dsl port operation (default: a)

Setting up permanent virtual circuits (PVC) for PPPoE

First appeared in build series: 2012-07-18

Mode: port dsl

	Command	Purpose
Step 1	**[node](prt-dsl)[0/0]#[no] pvc-ethernet <vpi> <vci>**	Creates a PVC and enters configuration mode for this PVC. The "no"-variant deletes the PVC configuration.

Mode: pvc ethernet

Step 2	**[node](pvc)[vpi/vci]# encapsulation { llc | vc }**	Sets the encapsulation to be used. Optionally select either LLC encapsulation or VC multiplexing for this PVC (default: llc)

Using PVC channel with PPPoE

First appeared in build series: 2012-07-18

Mode: pvc ppp

	Command	Purpose
Step 1	**[node](pvc)[vpi/vci]# pppoe**	Enters PPPoE configuration mode for this PVC.
Step 2	**node(pppoe)# session <Session-Name>**	Defines a PPPoE session.
Step 3 **(Optional)**	**node(session)[name]#service <Service-Name>**	Defines the tag ‘Service-Name’ to be supplied with Active Discovery in order to identify the desired remote peer (check whether the remote peer supports this feature)
Step 4 **(Optional)**	**node(session)[name]#access-concentrator <AC-Name>**	The Active Discovery only accepts the PPPoE session if the remote peer provides tag ‘AC-Name’ with its Active Discovery Offer as specified. This allows to identify the desired remote peer
Step 5	**[node](pvc)[vpi/vci]# [no] bind interface <name> [router]** **or** **node](pvc)[vpi/vci]# [no] bind subscriber <name>**	Binds the PPPoE session directly to the IP interface name in case no authentication is required. Binds the PPPoE session to the PPP subscriber name in case authentication is required.
Step 6 **(Optional)**	**[node](pvc)[vpi/vci]# [no] use profile ppp <Profile-Name>**	Assigns a PPP profile other than the default. (default: default)
Step 7	**[node](pvc)[vpi/vci]# [no] shutdown**	Enables or disables PPPoA session. (default: disabled)

Setting up permanent virtual circuits (PVC) for IPoA

First appeared in build series: 2012-07-18

Mode: port dsl

	Command	Purpose
Step 1	**[node](prt-dsl)[0/0]#[no] pvc-ip <vpi> <vci>**	Creates a PVC and enters configuration mode for this PVC. The "no"-variant deletes the PVC configuration.

Mode: pvc ip

Step 2	**[node](pvc)[vpi/vci]# encapsulation { llc | vc }**	Sets the encapsulation to be used. Optionally select either LLC encapsulation or VC multiplexing for this PVC. (default: llc)

Using PVC channel with IPoA

First appeared in build series: 2012-07-18

Mode: pvc ip

	Command	Purpose
Step 1	**[node](pvc)[vpi/vci]# [no] bind interface <name> [router]**	Binds the IPoA PVC directly to the IP interface.

Setting up permanent virtual circuits (PVC) for PPPoA

First appeared in build series: 2012-07-18

Mode: port dsl

	Command	Purpose
Step 1	**[node](prt-dsl)[0/0]#[no] pvc-ppp <vpi> <vci>**	Creates a PVC and enters configuration mode for this PVC. The "no"-variant deletes the PVC configuration.

Mode: pvc ppp

Step 2	**[node](pvc)[vpi/vci]# encapsulation { llc | vc }**	Sets the encapsulation to be used. Optionally select either LLC encapsulation or VC multiplexing for this PVC. Default: llc

Using PVC channel with PPPoA

First appeared in build series: 2012-07-18

Mode: pvc ppp

	Command	Purpose
Step 1	**[node](pvc)[vpi/vci]# [no] bind interface <name> [router]** **or** **node](pvc)[vpi/vci]# [no] bind subscriber <name>**	Binds the PPPoA PVC directly to the IP interface name in case no authentication is required. Binds the PPPoA PVC to the PPP subscriber name in case authentication is required.
Step 2 **(Optional)**	**[node](pvc)[vpi/vci]# [no] use profile ppp <name>**	Assigns a PPP profile other than the default. (default: default)
Step 3	**[node](pvc)[vpi/vci]# [no] shutdown**	Enables or disables PPPoA session. (default: disabled)

Set layer 2 COS for PPP and PPPoE packets

First appeared in build series: 2012-07-18

Layer 2 COS can be configured for PPP and PPPoE control frames. This configuration is only applied when PPP/PPPoE packets are encapsulated in IEEE 802.1Q tagged frames. This new feature allows traffic prioritization of PPP/PPPoE packets and adds a way to provide best effort QoS or CoS at layer 2.

Select the PPPoE session to configure this feature

Mode: session <name>

	Command	Purpose
Step 1	**[node](session)# ctrl-frame-layer2-cos [0 | 1 | .. | 7]**	Set the layer2 COS for PPP/PPPoE control frames (default: 7) Note: use *ctrl-frame-layer2-cos* without parameter to revert to the default.

Administrator exec mode login

First appeared in build series: 2012-07-18

Administrator users do have the privilege to enter the “administrator exec” mode by issuing the command “enable” right after login. With the following configuration command it is possible to allow all administrator user on a SmartNode to skip that step. By enabling the configuration command below, an administrator will directly be in the “administrator exec” mode after he logged in.

Mode: configure

	Command	Purpose
Step 1	**[node](cfg)#[no] cli login administrator-exec-mode**	Enable direct entering of “administrator exec” mode after login (default: disabled)

Set G.S power backoff

First appeared in build series: 2012-07-18

The power backoff on the G.S card can be reduced. By default this power backoff is set to 0dB but it might be needed to reduce it with long distance line.

To configure select the correct dsl port.

Mode: port dsl <slot> <port>

	Command	Purpose
Step 1	**[node](prt-dsl)# [no] power-backoff { 0dB | -1dB | -2dB | .. | -12dB }**	Reduce the power backoff on the G.S interface (default: 0dB) Note: use *no power-backoff* to set default value (0dB)

Documentation

CD-ROM

The CD-ROM that is delivered with SmartNodes includes user documentation and tools for SmartWare R6.T:

- Software Configuration Guide SmartWare Release R6.5
- SmartNode Hardware Installation Guide
- TFTP Server
- Telnet
- Acrobat Reader

WWW

Please refer to the following online resources:

- Software Configuration Guide SmartWare Release R6.5: http://www.patton.com/manuals/07MSWR65_SCG-UM.pdf
- SmartWare Configuration Library: http://www.patton.com/voip/confignotes.asp

How to Upgrade

1. You have the choice to upgrade to R6.T with or without the GUI functionality.

To upgrade to R6.T without the GUI functionality, enter the following command (telnet, console):

```
copy tftp://<tftp_server_address>/<server path>/b flash:
```

To upgrade to R6.T with the GUI functionality, enter the following command (telnet, console):

```
copy tftp://<tftp_server_address>/<server path>/bw flash:
```

2. Load Patton-specific settings (preferences), if available:

Extract the files ‘b_Patton_prefs’ and ‘Patton.prefs’ into the same directory on the TFTP-server.

```
copy tftp://<tftp_server_address>/<server path>/ b_Patton_prefs flash:
```

3. Reboot the SmartNode afterwards:

```
reload
```

Notes about Upgrading from Earlier Releases

Note that SmartWare Release R6.T **introduces some changes in the configuration** compared to Release R5.x, especially in the domain of FXO and ISDN.

Please refer to the SmartWare Migration Notes R5 to R6 available at upgrades.patton.com.

How to submit Trouble Reports

Patton makes every effort to ensure that the products achieve a supreme level of quality. However due to the wealth of functionality and complexity of the products there remains a certain number of problems, either pertaining to the Patton product or the interoperability with other vendor's products. The following set of guidelines will help us in pinpointing the problem and accordingly find a solution to cure it.

Problem Description:
Add a description of the problem. If possible and applicable, include a diagram of the network setup (with Microsoft tools).
Product Description:
When reporting a problem, always submit the product name, release and build number. Example: SmartNode 4960 *V1 R6.T Build 2014-05-28* This will help us in identifying the correct software version. In the unlikely case of a suspected hardware problem also submit the serial number of the SmartNode (s) and/or interface cards.
Running Configuration:
With the Command Line Interface command 'show running-configuration' you can display the currently active configuration of the system (in a telnet and/or console session). When added to the submitted trouble report, this will help us analyze the configuration and preclude possible configuration problems.
Logs and Protocol Monitors:
Protocol traces contain a wealth of additional information, which may be very helpful in finding or at least pinpointing the problem. Various protocol monitors with different levels of detail are an integral part of SmartWare and can be started (in a telnet and/or console session) individually ('debug' command). **N.B.:** In order to correlate the protocol monitors at the different levels in SmartWare (e.g. ISDN layer3 and Session-Router monitors) run the monitors concurrently.
Network Traffic Traces:
In certain cases it may be helpful to have a trace of the traffic on the IP network in order to inspect packet contents. Please use one of the following tools (supporting trace file formats which our tools can read): Ethereal (freeware; www.ethereal.com)
Your Coordinates:
For further enquiries please add your email address and phone number.