

VOICE&DATA ROUTER ITX 495 01

PRODUCT DOCUMENTATION



CONTENTS

PRODUCT OVERVIEW	3
PRODUCT FEATURES	3
VARIANTS	5
APPLICATIONS	6
TECHNICAL SPECIFICATION	10
OPERATING INSTRUCTIONS	13
MANAGEMENT	17
WEB MANAGER	18
<i>Users Menu</i>	21
<i>Trunks Menu</i>	28
<i>Traffic Menu</i>	44
<i>Globals Menu</i>	58
<i>System Menu</i>	87
<i>Diagnostics Menu</i>	103
<i>Specials Menu</i>	112
UNIMAN	113
<i>Connection to the device</i>	113
<i>Setting of password</i>	115
<i>Configuration files editor</i>	116
<i>Diagnostics</i>	118
<i>Listing Messages</i>	119
<i>Identification</i>	121
TERMS OF SALE	122

PRODUCT OVERVIEW

The device is a multifunction VoIP gateway with application in SIP Trunking, PBX IP Trunking and PSTN access for local IP telephony solutions. There are many usage applications available. It is a perfect solution to decrease costs of all your calls.



PRODUCT FEATURES

- OS LINUX, SD card, Asterisk SW
- **2 x ETHERNET 10/100 BT** or 1 x 10/100 BT and 1 x 10/100 FX*
 - * WAN ETHERNET fiber optic interface (SC DUPLEX) can be single mode or multi mode; for single mode device can use only 1 optical fiber; Auto MDIX option – for both Ethernet interfaces*
- **4 x E1/T1** 120/75 Ohm PRI DSS1/QSIG or R2 MFC ports software configurable
- Optional interfaces:
 - **BRI (8/16 x BRI U0 or 4 x BRI S0)**
 - **GSM (12 x GSM 2G)**
 - **Analogue (32 x FXS, 16 x FXO, 6 x E&M)**
- Console port RS232 (RJ45)
- USB 1.1 host port
- VoIP support: SIP, RTP, UDPTL, T.38
- Codecs: G.711, G.726, G.729a/b, G.723.1
- G.165 / G.168 - 2004 Echo Cancellation up to 128 ms
- Silence detection / suppression and comfort noise generation (VAD/CNG)
- Simultaneous calls
 - VoIP – G.711: 48/64
 - VoIP – G.726, G.729 a/b: 16/32
 - VoIP – G.723.1, GSM: 16/24
 - TDM – not limited
- G.165 / G.168 - 2004 Echo Cancellation up to 128 ms
- Multiple codec support
- Fax over IP support, including T.38
- Remote management capabilities
- SIP signaling
- SNMP
- LCR
- AOC generation
- Diagnostics of all interfaces
- Alarm indication
- Routing to another E1/T1 if there is no more free capacity for simultaneous calls
- Call Forwarding
- Call Hold/Transfer
- Music On Hold
- Speed Dial
- CLIP/CLIR
- Automatic Attendant
- DTMF generation and detection
- Two step dial (ISDN / MFC R2 and than DTMF) - for alternative carrier
- Call progress tone generation
- Carrier tone generation and detection
- Caller ID generation and detection (FSK)
- Silence detection / suppression and comfort noise generation (VAD/CNG)

- Call permissions
- Calling Groups
- Ring Groups
- Call Pickup
- Announcement playback
- Remote management capabilities
- HTTP, SNMP, SSH, SCP, SFTP, TFTP
- Diagnostics functions

VARIANTS

1U version

- **ITX 495 01** Voice&Data Router – desktop with rack mount option (4 x E1/T1, optional 12 x GSM interface, optional 32 x analogue interface, optional 4 x BRI S0, optional 16 x BRI Uk0)

ITX 495 01 . a b c d e f g h i j – Voice&Data Router

Optic Communication	X = 2 optic fibers A = Type A, 1 optic fiber B = Type B, 1 optic fiber
Distance	1 = 2km 2 = 15km 3 = 40km 4 = 80km
Wave Length	1 = 1300nm 2 = 1500nm
Optic Mode	0 = none 1 = SM (Single Mode) 2 = MM (Multi Mode)
E1 Interface	0 = none 1 = RJ45 2 = BNC
Power Supply	1 = 230V, 48V 2 = 230V 3 = 48V
GSM Interface	0 = none 1, 2, 3, 4, 5, 6, 7, 8, 9 a = 10, b = 11, c = 12
Analogue Interface	0 = no 1 = yes
BRI Interface	0 = no 4 = 4 BRI S0 7 = 8 BRI S0 5 = 8 BRI Uk0 8 = 16 BRI S0 6 = 16 BRI Uk0 9 = 8 BRI Uk0, 8 BRI S0
Compression	0 = no SIP 1 = 16 channels G.729 2 = 32 channels G.729 48 channels G.711 64 channels G.711

19" Rack 6U version

- **ITX 402 41** Voice&Data Router – 6U rack card (4 x E1/T1)
- **ITX 222 05** 19" rack 6U
- **ITX 802 05** Converter DC/DC + 5V/20A

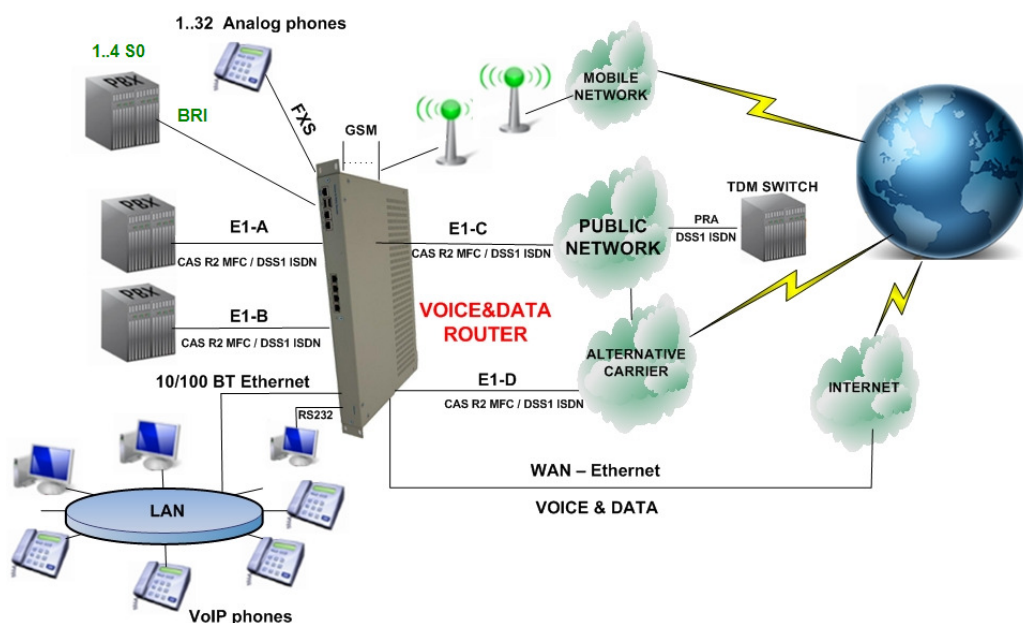
ITX 402 41 . a b c d e – Voice&Data Router (rack card)

Optic Communication	X = 2 optic fibers A = Type A, 1 optic fiber B = Type B, 1 optic fiber
Distance	1 = 2km 2 = 15km 3 = 40km 4 = 80km
Wave Length	1 = 1300nm 2 = 1500nm
Optic Mode	0 = none 1 = SM (Single Mode) 2 = MM (Multi Mode)
Compression	1 = 16 channels G.729 48 channels G.711 2 = 32 channels G.729 64 channels G.711

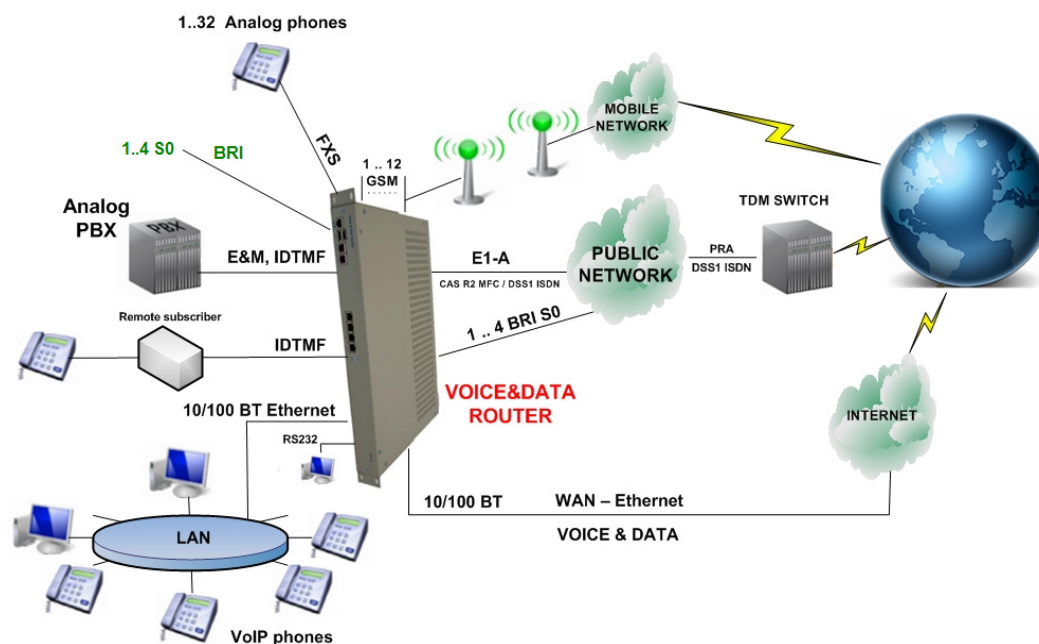
APPLICATIONS

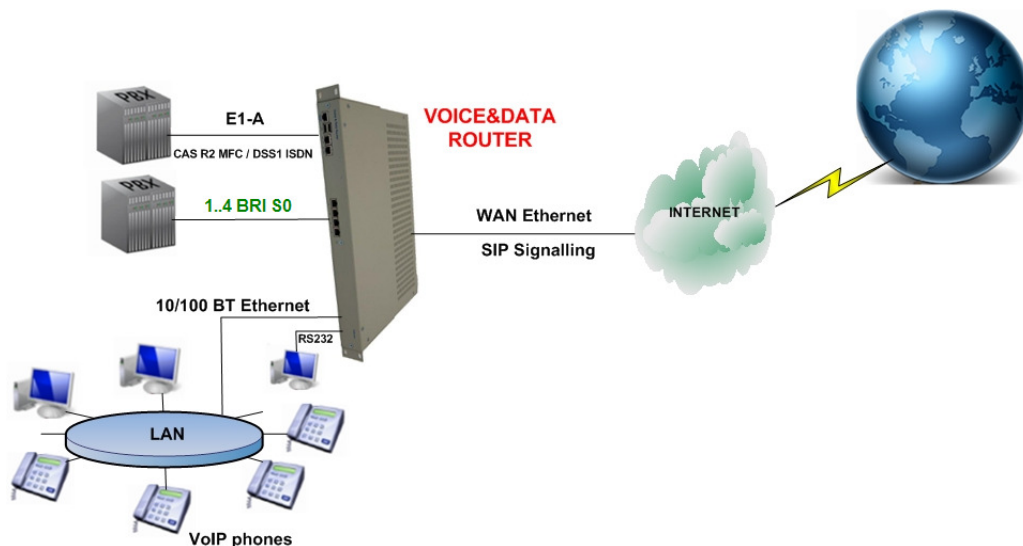
- Voice & Data Router
- VoIP, TDM PBX (SW Asterisk)
- TDM - VoIP Gateway
- Signaling converter R2 MFC / ISDN DSS1 – SIP, Routing to another E1 if there is no more free capacity for simultaneous calls
- Concentration of max. 4xE1 (considering the limitation of max. number of simultaneous calls depending on the codec used)
- Multiple Gateway (possibility to connect several customers and divide them)
- SIP PROXY Server

Voice&Data Router / VoIP, TDM PBX

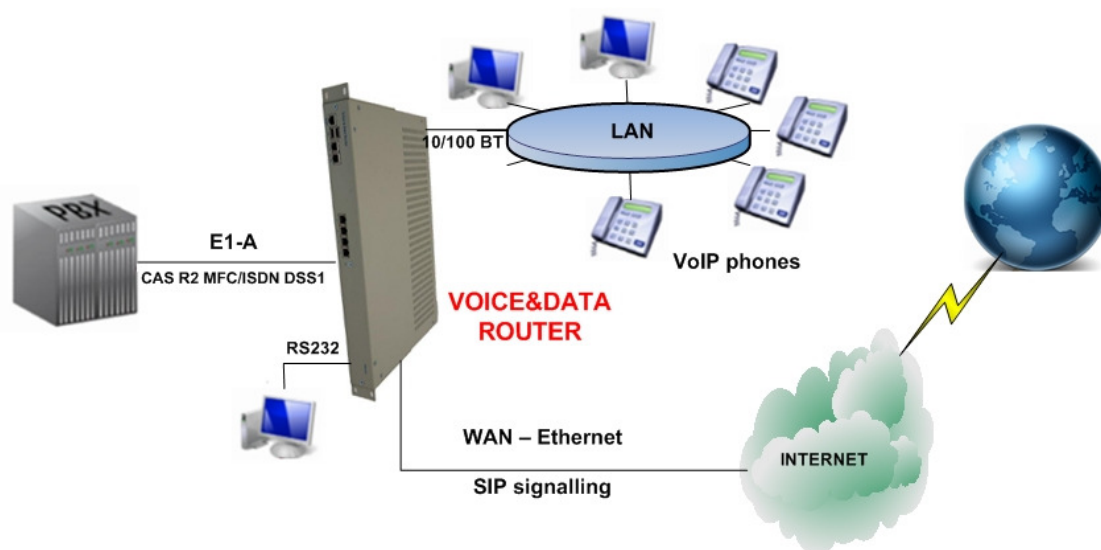


TDM – VoIP Gateway

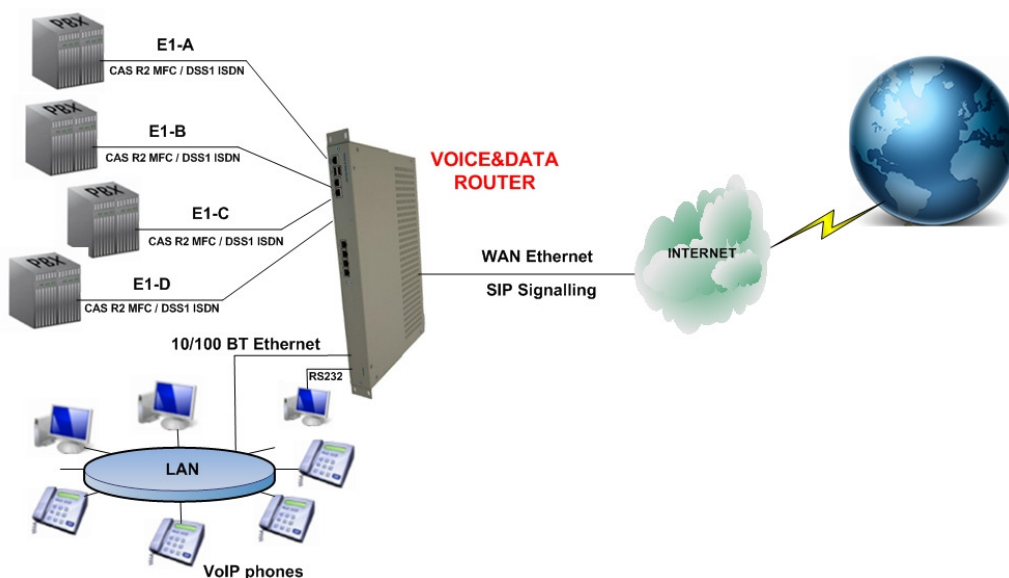




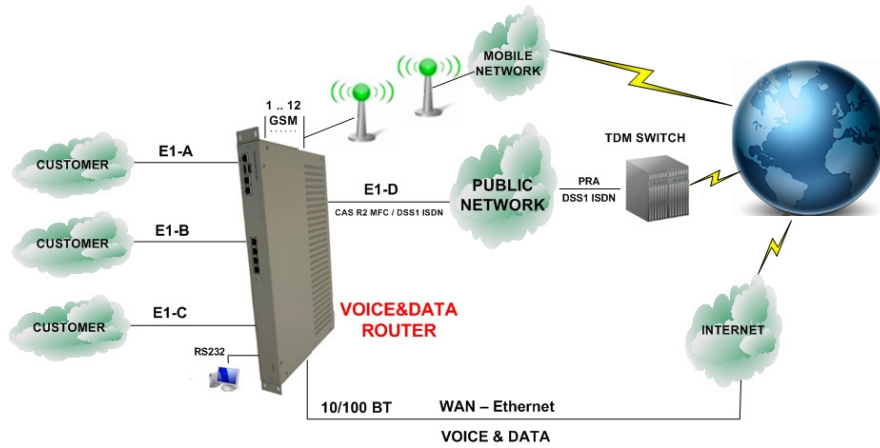
Signaling converter R2 MFC / ISDN DSS1 – SIP



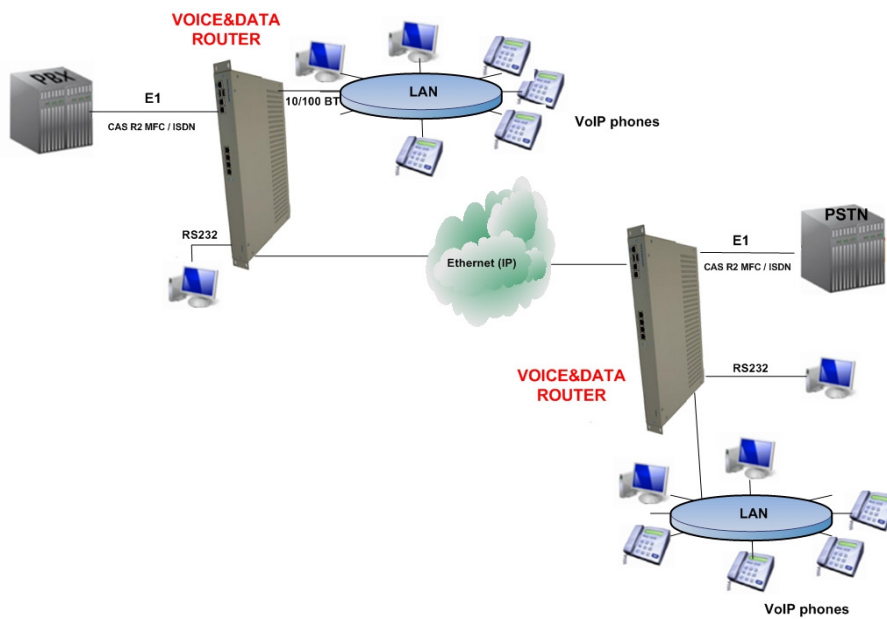
Concentration of max. 4xE1/T1 (considering the limitation of max. number of simultaneous calls depending on the codec used)



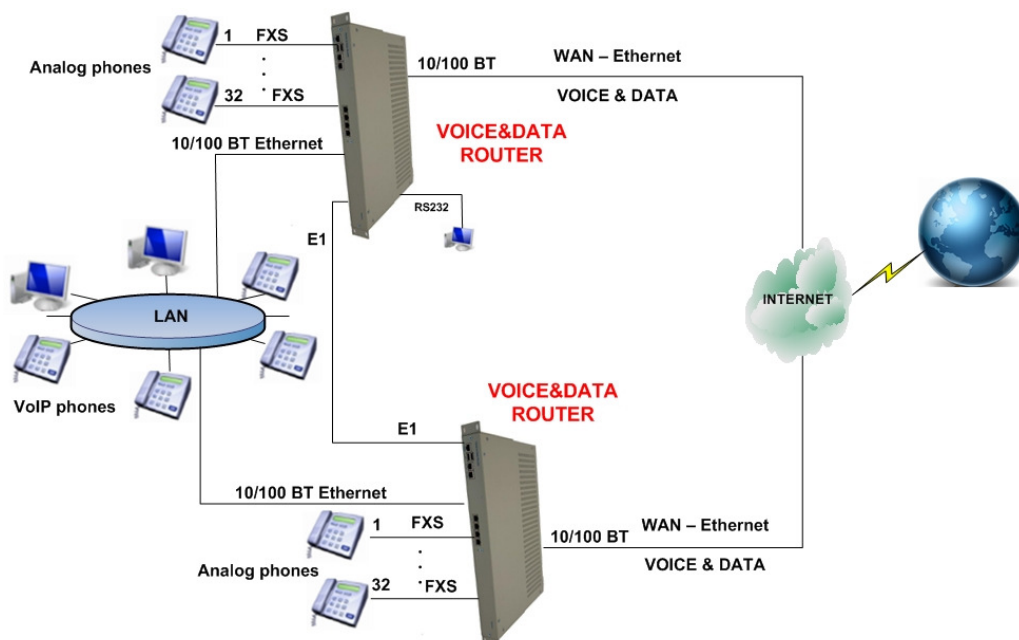
Multi Gateway (possibility to connect several customers and divide them)



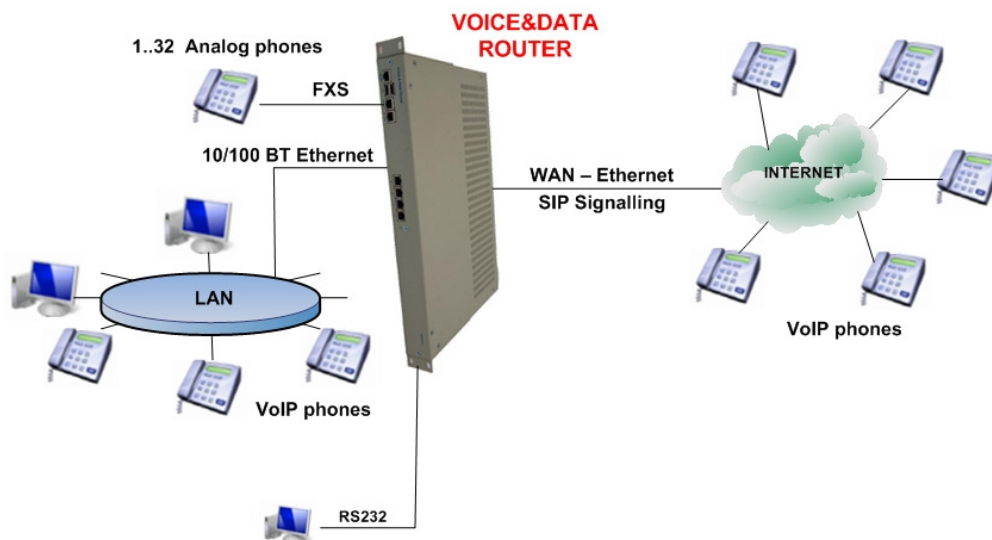
E1/T1 over Ethernet (IP)



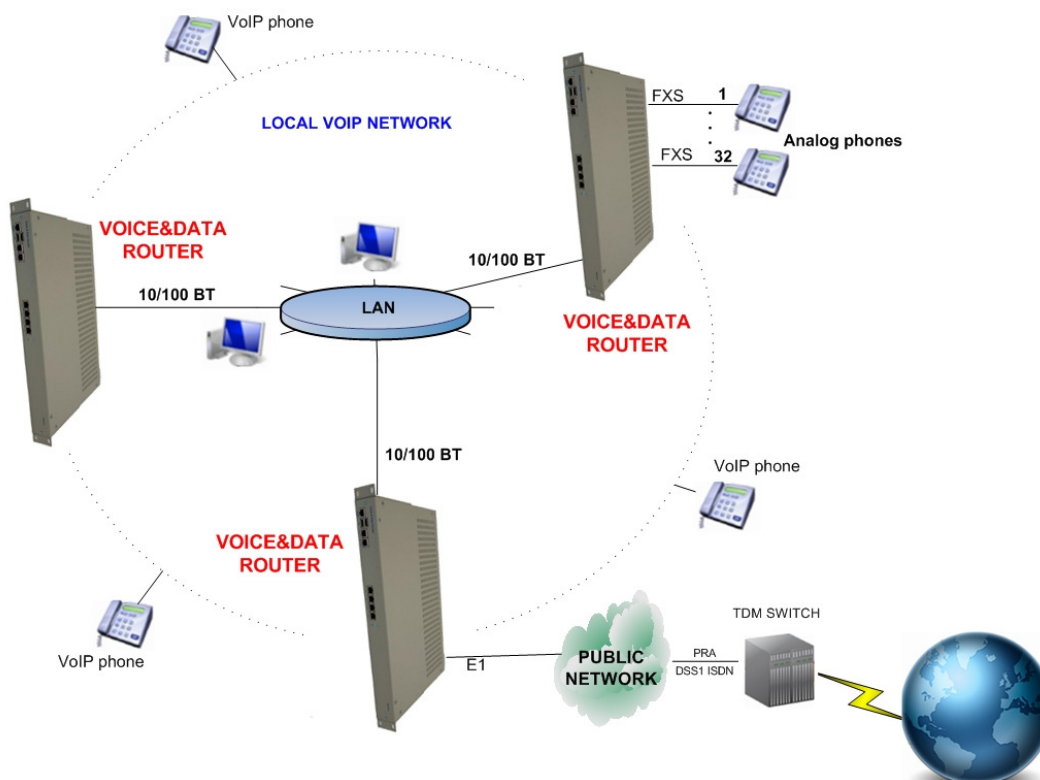
Extending



SIP PROXY Server



Local VoIP network



TECHNICAL SPECIFICATION

IP Telephony Protocols

- SIP – RFC 3261
- SDP – RFC 2327
- RTP – RFC 1889, RFC 2833, RFC 3389

ISDN Signaling

- Euro ISDN EDSS – 1/ETSI PRI/ NET5
- ETS 300 011 (ISDN PRI UNI)
- ETS 300 012-1 (ITU – T I.430)
- ETS 300 402-2 (ITU-T Q I.921)
- ETS 300 403-1/2 (ITU-T Q.931)
- ETS 300 102-2 (ITU-T Q.931)
- ISDN speech, audio and data (Fax Gr4, UDI 64)

CAS MFC R2 Signaling

- ITU – T from Q.440 to Q.480, Q.490
- ITU – T from Q.421 to Q.424
- Basic Technical Requirements for Digital Switching System and PCM Transmission System
- National variants, DTMF dial

GSM parameters

- Quad-Band 850/900/1800/1900 MHz
- GPRS multi-slot class 10/8
- GPRS mobile station class B
- Compliant to GSM phase 2/2+
 - Class 4 (2W @850/900 MHz)
 - Class 1 (1W @1800/1900 MHz)
- Voice specification
 - Tricodec
 - Half rate (HR)
 - Full rate (FR)
 - Enhanced Full rate (EFR)
 - AMR
 - Half rate (HR)
 - Full rate (FR)
- Echo suppression

FAX and Modem Support

- FAX Relay T.38
 - Supported modulations:
 - V.21 Ch2
 - V.27 2400 / 4800
 - V.29 7200 / 9600
 - V.17 7200 / 9600 / 12000 / 14400)
- FAX Pass-Through – transport of fax modulations over G.711 connections
- Modem Pass-Through – transport of modem modulations over G.711 connections.

Voice Processing

- Supported voice codec standards
 - G.711 (A-law, μ -law)
 - G.723.1 and G.723.1 A
 - G.726
 - G.729 Annex A & B
 - GSM

- G.165 / G.168 – 2004 Echo Canceller up to 128 ms
- Robust jitter buffer
- DTMF generation and detection
- Call progress tone generation
- Carrier tone generation
- Caller ID generation and detection
- Voice activity detection and comfort noise
- Announcement playback
- Timeslot interchange for TDM to TDM traffic processing (no compression, no delay)

Voice Channel Density

Supported Voice Codecs	Channel Density	
	16/48 calls	32/64 calls
G.711	48	64
G.726	16	32
G.729 a/b	16	32
G.723.1	16	24
GSM	16	24
T.38	16	16

Voice Routing

- Local switching
- Low Cost Routing
- Analyze called party number
- Analyze calling party number
- Called / calling party number modification
- Call permissions
- Multiple fail-over routes
- Two step dialing (DTMF)
- Calling groups
- Ringing groups

Data Routing

- Basic Routing

QoS Marking

- QoS pre-router
- TOS /DiffServ
- Supported QoS marking

Networking

- DHCP support and capabilities
- Static Routing

Management

- Web management – GUI
- Terminal access
 - Local – control interface RS232
 - Remote – LAN/WAN interface (SSH protocol)
- Inoteska UniMan software
- SNMP v1/2c

Power Supply

19", 1U rack mount

- 85V – 260 V AC or -40V to -65V DC
- Frequency: 48Hz to 52 Hz

19", 6U rack

- 48V DC

Max.power consumption

Max. 50W

Dimensions

19", 1U rack mountable 44 x 282 x 485 mm (h x d x w)

Weight

Approx. 3,5kg (real weight depends on device HW configuration)

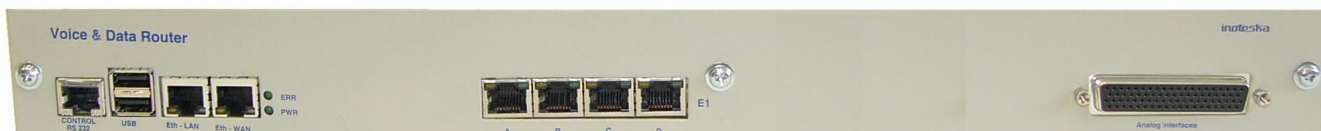
OPERATING INSTRUCTIONS

Operating Environment

Install the device in a place where:

- Operating temperature: 0° C to 55° C
- Storage temperature: -10° C to 65° C
- Humidity: up to 80%, non-condensing

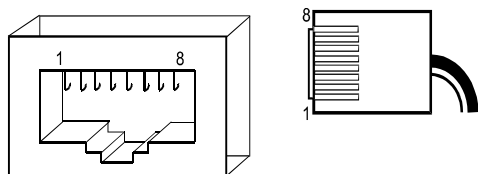
Interfaces



E1/T1 interface

RJ 45 connector

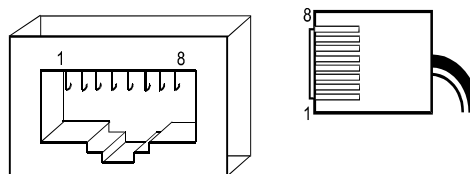
- | | |
|-----------------------------|------|
| 1 – input wire to device | Rx – |
| 2 – input wire to device | Rx + |
| 3 – | |
| 4 – output wire from device | Tx – |
| 5 – output wire from device | Tx + |
| 6 – | |
| 7 – | |
| 8 – | |



Ethernet 10/100Base-T interface

RJ 45 connector

- | | |
|--------------------------|------|
| 1 – transmit from device | Tx + |
| 2 – transmit from device | Tx – |
| 3 – receive to device | Rx + |
| 4 – | |
| 5 – | |
| 6 – receive to device | Rx – |
| 7 – | |
| 8 – | |



Analog interfaces

Analog extension card can contain 1 up to 8 modules.

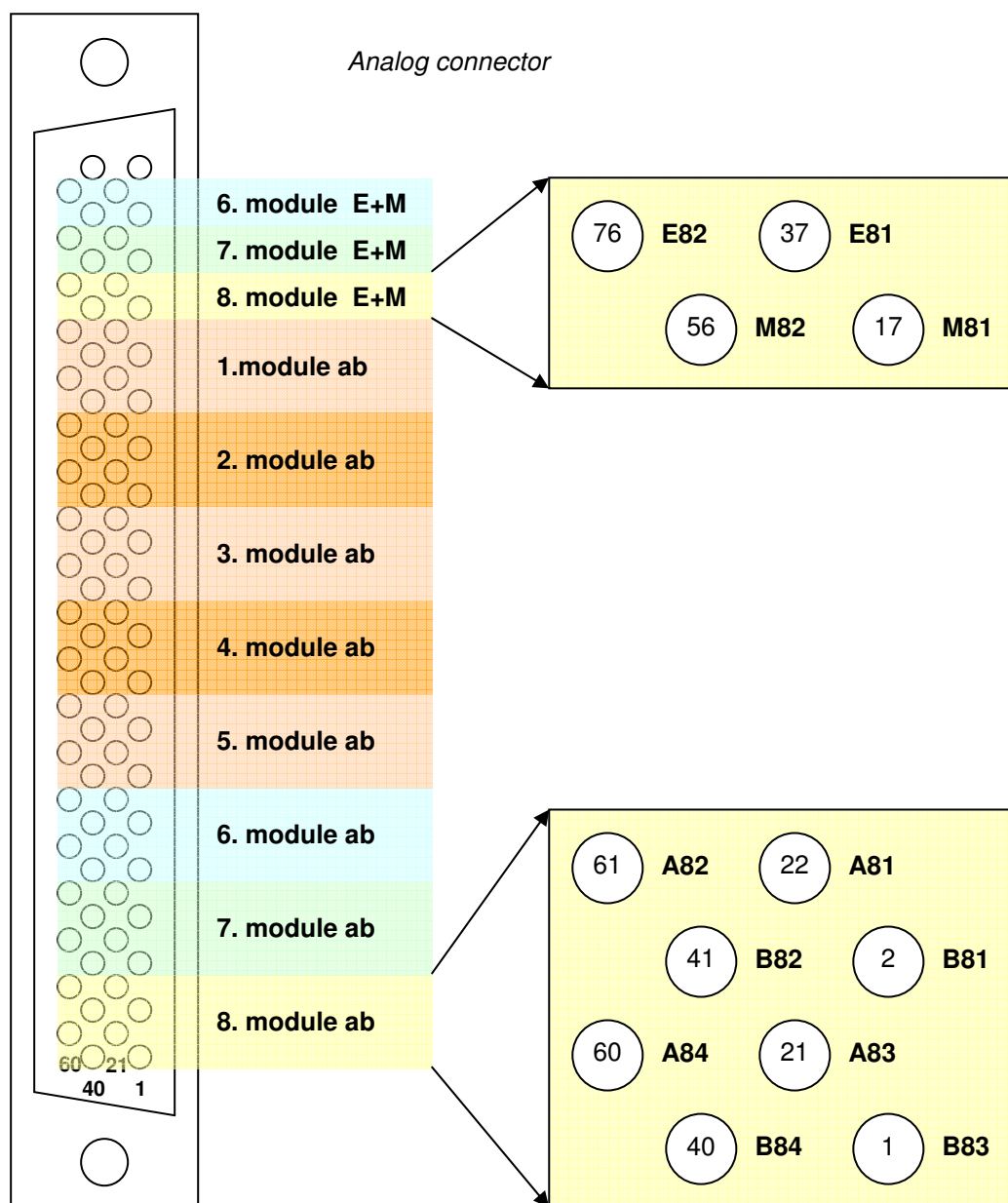
Available modules

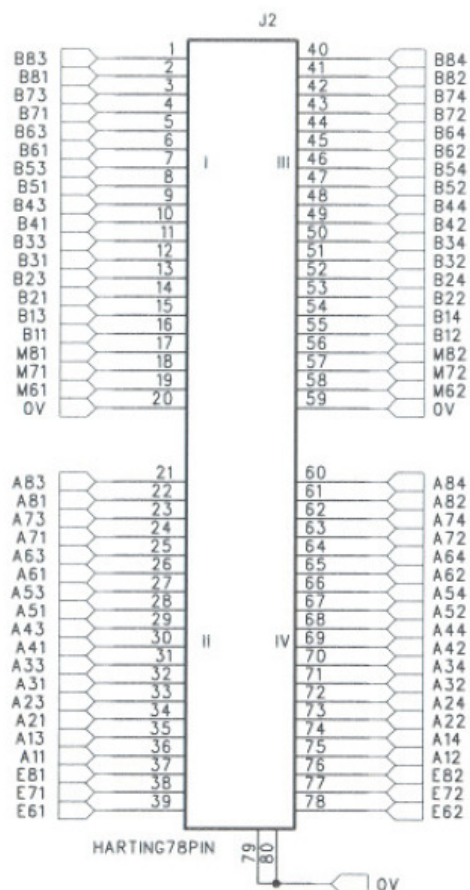
- FXS module – quad
- FXO module – dual
- E&M module – dual

1	2	3	4	5	6	7	8
A11 B11	A21 B21	A31 B31	A41 B41	A51 B51	A61 B61	A71 B71	A81 B81
A12 B12	A22 B22	A32 B32	A42 B42	A52 B52	A62 B62	A72 B72	A82 B82
A13 B13	A23 B23	A33 B33	A43 B43	A53 B53	A63 B63	A73 B73	A83 B83
A14 B14	A24 B24	A34 B34	A44 B44	A54 B54	A64 B64	A74 B74	A84 B84
					E61 M61	E71 M71	E81 M81
					E62 M62	E72 M72	E82 M82

Location of analog modules on analog extension card

Position No. 1 to 5: for FXS/FXO modules
 Position No. 6 to 8: for FXS/FXO/ E&M modules



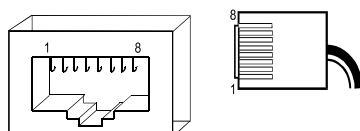


Description of J2 connector

Note: In description of connector, e.g. signal A23 means that it is a-wire from second module (first index) of third interface on module (second index).

BRI interface

Pins are connected as TE in default configuration.



	NT	TE
1 –		
2 –		
3 – Rx+		Tx+
4 – Tx+		Rx+
5 – Tx-		Rx-
6 – Rx-		Tx-
7 –		
8 –		

GSM interface

Antenna connector: GSC connector coaxial SMT male 50R 6GHz

CONTROL RS-232 connector



CANNON - Female for D09F cable	RJ - 45
-	1
-	2
-	3
2	4
3	5
-	6
-	7
5	8
-	-

LED diodes

Interface	Led diode green	Led diode yellow	Status
E1/T1	Off	Off	Not enabled
	Off	On	Not connected
	Fast		CRC error or SLIP
	Slow		ISDN – No DLL
		Slow	AIS detected
		Fast	LFA or RRA detected
	On	Off	OK
Ethernet	Off	Off	Line not connected
	On	(flashes during Reception/ Transmission)	Line active
BRI S0/Uk0	Off		L1 down
	On		L1 up

Off – no light, On – light, Slow – flashes slow (period 1.6sec), Fast – flashes fast (period 0.2sec, 5x/sec)

CRC Cyclic Redundancy Check error
No DLL no Data Link Layer active
AIS Alarm Indication Signal – Transmitted signal is constant with data value Log1
LFA Loss of Frame Alignment – Indicates synchronization error in 0th channel
RRA Receive Remote Alarm – Indicates remote device alarm

MANAGEMENT

Voice&Data Router is supplied with default configuration. Device can be configured using:

- Terminal access
- Inoteska Web Manager (GUI)
- Inoteska UniMan

Terminal access allows direct access to the Linux console and Asterisk command line interface. User has full low level control of the whole system. Knowledge of OS Linux, Asterisk SW and configuration files structure is necessary.

Terminal access is available:

- Locally via RS 232 control interface (baud rate 115200 bps, 8 bits, 1 stop bit, no parity)
- Remotely over the Ethernet interface using SSH protocol

Login parameters for terminal access:

- Login name: **root**
- Default password: **inoteska**

NOTE:

Low level configuration using terminal access is not the scope of this document. Unqualified change of system configuration can make the device non-functional. Please contact the producer in case of difficulties!

Inoteska Web Manager (GUI) provides simple and user-friendly interface for device configuration and supervision using web browser.

Inoteska UniMan is universal software used for communication with Inoteska equipment which supports TCP / UDP protocol. UniMan operates under OS Windows (Win7/Vista/XP/2000). UniMan provides text or graphical mode for device configuration.

WEB MANAGER

Web Manager is Graphic User Interface for device configuration and supervision. It was tested with following web browsers: **Opera, Google Chrome, Mozilla Firefox**. **MS Internet Explorer** is not fully supported and it is not recommended to use with Voice&Data Router.

Default IP address setting:

- LAN: 192.168.1.100
- WAN: 10.1.1.100

Initial screen serves for user (system administrator) login.



Default login parameters:

- Username: **admin**
- Password*: **inoteska**

**Change of password can be done in [Options](#) menu.*

After successful logging in **Home** page with device hardware configuration and identification will be displayed.

Device configuration shows available TDM interfaces (E1/T1 trunks, BRI trunks, GSM trunks, analogue trunks and users) and configured VoIP interfaces (SIP trunks and users). Voice&Data Router is always supplied with 4 E1/T1 interfaces. BRI, analogue and GSM interfaces are optional and their number depends on the hardware configuration. SIP users and SIP trunks shows the number of interfaces configured by device administrator.

Identification provides basic information: device type (product code number), serial number, main board identification and software version.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Home >

System Home Uptime : 08:12:56 up 2 min, 0 users, load average: 0.23, 0.14, 0.05

Device Configuration

Available Interfaces	Count
E1/T1 Trunks	4
BRI Trunks	4
GSM Trunks	4
Analog Trunks	6
Analog Users	8
SIP Trunks	2
SIP Users	5

Identification

Hardware	
Device Type	ITX4024102
Serial Number	402410270008
Main Board	ITB 166 05 + M82810-12 RevB

Software	
Operating System	Linux 2.6.11.7-1.08.5.3malindi (#2 Thu Feb 16 12:21:06 CET 2012)
MSP Firmware	Test_v2_04_82027_01
FPGA Design	2.4
Application	2.5g

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

How to configure Voice&Data Router

Step 1

Make basic system configuration

- IP setting – assign IP addresses to connect to LAN and WAN network. Configure DNS servers. In some cases it can be necessary to configure routing table for static IP routing.
- Firewall setting – configure firewall eventually NAT to keep Voice&Data Router secure from the Internet attacks.
- Date/Time setting – select time zone and actualize time in Voice&Data Router

Step 2

Configure users / trunks. This depends on usage application

- Gateway – only trunk's configuration is required usually. In some cases also users can be needed.
- PBX – both user's and trunk's configuration is required

Depending on the application create the users (SIP or analogue). Configure trunks to connect to PSTN or VoIP provider (usually E1/T1 or SIP), to connect to PBX or other gateway (E1/T1, SIP or analogue trunk), to connect to GSM network (GSM interface), etc. as per device function.

Step 3

Configure call traffic – call routing between users and trunks. Call traffic consists of

- calling rules
- dial plans

Calling rules define set of rules for analysis of dialed number eventually together with caller identification number and for selection of destination of the call. Voice&Data Router in function of gateway without users needs to specify only trunk-to-trunk calling rules. PBX device or gateway with users requires also calling rules for user-to-user calls, user-to-trunk calls and trunk-to-user calls.

Dial plan is set of calling rules. Create dial plans from existing calling rules for users and for trunks as needed. When all dial plans are ready go back to the user's or trunk's configuration to assign dial plan for users / trunks.

Step 4


Configure all other options offered by Web Manager.

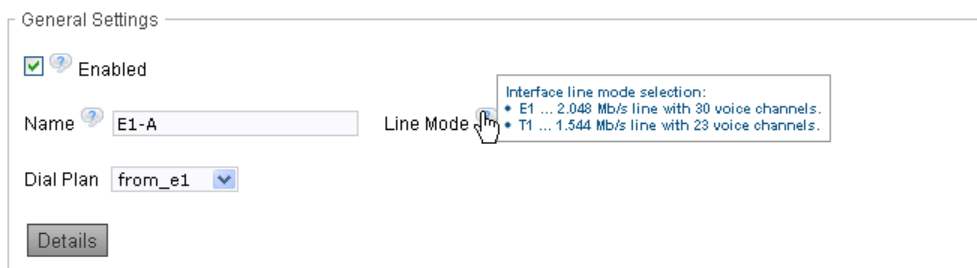
Most of the changes you made are being applied to your Voice&Data Router after click on **Apply Changes** filed in upper right corner. Some settings (e.g. change of IP settings, routing tables, date/time setting, etc.) are done automatically, without need to **Apply Changes**.

GUI-version : 1.0 / Board Type : 1

[Apply Changes](#) [Logout](#)

If you want to end the work with Web Manager click on **Logout** in the upper right corner.

Web Manager has implemented simple context help system. Question mark icon  is displayed everywhere it is available. Moving a mouse pointer over this icon will display tooltip frame with description of selected parameter/setting.



Complete structure of Web Manager menu

[Home](#)

[Users Menu](#)

- [SIP Users](#)
- [Analog Users](#)

[Trunks Menu](#)

- [SIP Trunks](#)
- [E1/T1 Trunks](#)
- [BRI Trunks](#)
- [Analog Trunks](#)
- [GSM Trunks](#)

[Traffic Menu](#)

- [Calling Rules](#)
- [Dial Plans](#)
- [AOC Tables Settings](#)

[Globals Menu](#)

- [SIP Settings](#)
- [RTP/UDPTL Settings](#)
- [Call Groups](#)
- [Ring Groups](#)
- [Carriers](#)
- [Permissions](#)
- [Services Codes](#)
- [CDR Settings](#)
- [Announcement Settings](#)
- [CAS National Variants](#)

[System Menu](#)

- [IP settings](#)
- [Routing Tables](#)
- [SNMP](#)
- [Firewall](#)
- [Options](#)
- [Backup and Restore Upload](#)
- [Firmware Update](#)
- [Date and Time](#)

[Diagnostics Menu](#)

- [Port Status](#)
- [Active Services](#)
- [Identification](#)
- [System Logs](#)
- [CLI Emulator](#)
- [Debug messages](#)
- [System Status](#)
- [File Editor](#)

[Specials Menu](#)

- [AOC Web Update](#)

USERS MENU

Users menu offers configuration of user extension lines. Voice&Data Router supports SIP users and analogue FXS users. Analogue users are optional and they depend on hardware configuration.

SIP users

SIP users configuration allows creating and managing user accounts for SIP phones. SIP users main screen displays table of configured SIP user extensions. Use button **Create New User** to add new account for SIP user and use button **Edit** to modify existing user account. To remove SIP user click on **Delete** button. User can be removed only if does not exist any reference to this user in calling rules and ringing groups.

The screenshot shows the 'voice&data router' web interface. At the top, it says 'GUI-version : 1.0 / Board Type : 1' and 'Logout'. The main navigation bar includes 'Home', 'Users', 'Trunks', 'Traffic', 'Globals', 'System', 'Diagnostics', and 'Specials'. Below this, the breadcrumb 'Users > SIP Users' is visible. The 'SIP Users Settings' section has three buttons: 'Create New User', 'Modify Selected Users', and 'Delete Selected Users'. Below these is a 'List of User Extensions' table.

<input type="checkbox"/>	Extension	Full Name	Host Address	DialPlan	Permit/Deny	Edit	Delete
<input type="checkbox"/>	10	Jack Daniel's	dynamic	from_users	Permit/Deny	Edit	Delete
<input type="checkbox"/>	11	Johnnie Walker	dynamic	from_users	Permit/Deny	Edit	Delete
<input type="checkbox"/>	12	Jim Beam	dynamic	from_users	Permit/Deny	Edit	Delete

At the bottom of the interface, it says 'Copyright © 2010-2012, All Rights Reserved www.inoteska.sk'.

In addition there also exists possibility to change or remove multiple users in one action. In this case use the checkboxes in the first column to select users you want to modify and click either **Modify Selected Users** or **Delete Selected Users** button.

When you are creating new SIP user or when you are changing parameters of the existing one you are switched to user's details form, with all available SIP user account settings. Here you can configure available parameters and click **Update** button to store new setting.

General Parameters

Extension

Extension number associated with this SIP user line. This number is also used as user name for authentication.

Password

Password for the user authentication. If password is not set, authentication will be disabled and Voice&Data Router will never ask for user authentication in this case.

Name

A character-based display name used for caller identification (i.e. Bob Jones). Note that it will overwrite display name configured in the user phone.

Caller ID

Caller identification number. Extension number is used for the caller identification by default. Use this field only if you need to overwrite default identification.

Dial Plan

Select dial plan to handle calls coming from user phone to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules.

GUI-version : 1.0 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Users > SIP Users

Edit User Extension - 10

General

Extension Name DialPlan

Password Caller ID

Host Options

Host Type Host Address Host Port

☐ Enable Voicemail for this User

Access PIN code Mailbox Email Address

Codecs

First Second Third Fourth Fifth

VoIP Settings

Quality ☒ NAT ☒ Can Reinvite ☒ DTMF Mode insecure

Other Options

Pickup Group

User's Services

Call Forward ☒ Do Not Disturb ☒

Permissions

User Permission Group Call Limit

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Host Options

Host Type

Voice&Data Router supports two methods how to connect to user SIP phone. Please select host type **dynamic** to use dynamic SIP registration procedure. Extension number and password from general section will be used for registration authentication. **Static** host type is intended for use as permanent static connection to the dedicated IP address. Note that you can restrict user's access for limited IP addresses or networks by **Permit/Deny** setting in main SIP users' screen.

Host IP address

Address of the user SIP phone in case of static host type (you can use numeric IP address or the host name).

Host Port

SIP protocol port number for this user.

Voice Mail Setting

Enable Voicemail for this User

Enable/Disable user voice mail account.

Access PIN Code

User's Personal Identification Code to access voice mail mailbox (PIN string can contain only digits).

Mailbox

Voice mail mailbox name. It can be different from the extensions number.

Email Address

The e-mail address to notify about new messages in the mailbox (i.e.bobjones@bobjones.com).

Codecs

Here you can define allowed voice compression codecs in order of preference. Voice&Data Router supports following voice codecs:

- **G.711 A-Law**
- **G.711 μ -Law**
- **G.729 Annex A/B**
- **G.726-32**
- **G.723.1**
- **GSM**
- **iLBC**

Up to five different codecs with defined preference can be configured for every SIP user.

VoIP Settings

Qualify

Enable this feature to check if the phone device is reachable. Qualify will send a SIP OPTIONS command regularly to check that the device is still online. If the device does not answer within the configured period Voice&Data Router considers the device off-line for future calls. Expiration time is configured in seconds (default is 2 seconds). This feature may also be used to keep a UDP session open to the device that is located behind the NAT. This can be used in conjunction with the NAT setting.

NAT

This setting allows communication with phone devices behind the NAT. It works properly in conjunction with Qualify setting in order to keep open the connection from Voice&Data Router to the peer behind the NAT.

Can Reinvite

Enabling this option causes Voice&Data Router to attempt to route the RTP media stream directly between SIP endpoints, bypassing Voice&Data Router.

DTMF Mode

Default mode for sending DTMF digits.

Insecure

Insecure feature specifies how to handle incoming SIP session and user matching. If it is disabled normal IP-based matching applies and the authentication is required (when password is set for SIP user extension). Set insecure to **port** to allow matching of SIP user by IP address without matching port number. Set insecure to **invite** to remove the requirement for authentication of incoming INVITE messages. And use **very** value to allow both, the matching of user by IP address without matching port number and to remove the requirement for authentication of incoming INVITE messages.

Other Options

Pickup Group

Pickup group allows to pickup fellow workers' calls. Users from the same group can pickup incoming calls each other using code defined in [Services Codes](#) menu.

User's Services

Here you can permit/deny special services for extension user. Any permitted service can be activated and deactivated by service codes defined in [Services Codes](#) menu. Voice&Data Router supports following services:

- **Call Forward** (unrestricted / when busy / when no answer)
- **Do Not Disturb**

User's Permission

User's Permission Group

Select permission group to restrict outgoing calls for this user. User permission group defines a collection of call permission flags. User permission groups are assigned to the users and call permission flags are assigned to the calling rules. User is allowed to make a call only if his permission group includes call permission flag assigned to calling rule for the call. Please see [Permissions](#) menu for more details.

User's Call Limit

Enter maximal number of simultaneous calls permitted for this user.

Voice&Data Router allows controlling SIP user's access according to the IP addresses. There are no restrictions by default. Click **Permit/Deny** button in the SIP users' list to configure range of IP addresses from which the user extension device can connect to Voice&Data Router. There are two types of access rules you can use

- permit
- deny

Each of them can define range of IP addresses (IP address and network mask) to enable or disable access from/to. To create rule for single IP address use network mask 255.255.255.255. You can enter several rules which are applied in the order they were created – order is important.

The screenshot shows the Voice&Data Router web interface. At the top, it says 'GUI-version : 1.0 / Board Type : 1' and 'Logout'. The main header features the 'voice&data router' logo and the 'inoteska' brand name. A navigation bar includes links for Home, Users, Trunks, Traffic, Globals, System, Diagnostics, and Specials. Below this, the breadcrumb 'Users > SIP Users' is visible. The main content area is titled 'Permit/Deny list' and includes buttons for 'Add new rule', 'Delete Selected', and 'Back to Extensions'. A warning box states 'Warning! Order is important'. Below the warning is a table with columns for 'Permit/Deny', 'IP', and 'Network Mask'. The table contains two rules: a 'Deny' rule for IP '0.0.0.0' with network mask '0.0.0.0', and a 'Permit' rule for IP '192.168.1.0' with network mask '255.255.255.0'. Each rule has 'Edit' and 'Delete' buttons. The footer of the interface shows 'Copyright © 2010-2012, All Rights Reserved www.inoteska.sk'.

<input type="checkbox"/>	Permit/Deny	IP	Network Mask		
<input type="checkbox"/>	Deny	0.0.0.0	0.0.0.0	Edit	Delete
<input type="checkbox"/>	Permit	192.168.1.0	255.255.255.0	Edit	Delete

Example:

If you want to restrict the user to access Voice&Data Router account only from your local network with address 192.168.1.0/24 then you should create following rules

1. Deny All
2. Allow 192.168.1.0/255.255.255.0

Analog users

Main screen for analogue users displays table of all available analogue FXS user extensions. Analogue users are optional interfaces depending on hardware configuration of Voice&Data Router. Because FXS module has 4 ports we can have from 4 up to 32 analog users in the system (FXS module can occupy all 8 slots available on the analogue extension card).

GUI-version : 1.0 / Board Type : 1 Voice&Data Router Reloaded !! Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Users > Analog Users

Analog Users Settings

List of Analog Users



Position	Extension	Full Name	Channel	DialPlan		
1	20	Doug Coombs	144	from_fxs	Unused	Edit
2	21	Hugo Harrison	145	from_fxs	Unused	Edit
3	22	Seth Morrison	146	from_fxs	Unused	Edit
4	23	Shane McConkey	147	from_fxs	Unused	Edit
5	24	Glen Plake	148	from_fxs	Unused	Edit
6	25	Kaj Zacrisson	149	from_fxs	Unused	Edit
7	26	Mike Hattrup	150	from_fxs	Unused	Edit
8	27	Chris Davenport	151	from_fxs	Unused	Edit

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

All available FXS ports are always displayed. Unused ports (not configured) are marked as **unset position**. Use **Edit** button to create analogue user extension (configure unused port) or to modify existing one. To remove user extension (set FXO port to unused state) click on **Unused** button. User extension can be removed only if there does not exist any reference to this user in calling rules and ringing groups.

To configure analogue user extension new form with all available settings appears. Here you can configure available parameters and click **Save** button to store new user configuration.

GUI-version : 1.0 / Board Type : 1 Voce&Data Router Reloaded !! Logout

[Home](#) | [Users](#) | [Trunks](#) | [Traffic](#) | [Globals](#) | [System](#) | [Diagnostics](#) | [Specials](#)

Users > Analog Users

Edit Details

General

Position
Extension
DialPlan

Channel
Full Name

Parameters

Echo Cancellation

Supervisory Tones

Polarity Reversal ☒

Rx Gain Tx Gain

Impedance Loop Current

Flash length

User's Services

User Permission Group

Pickup Group

☒ Call Transfer
☒ Call Forwarding
☐ Do Not Disturb

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

General Parameters

Position

This is analogue port position (number from 1 up to 32).

Channel

Internal channel number.

Extension

Extension number associated with this analogue user.

Full Name

A character-based display name used for caller identification (i.e. Bob Jones).

Dial Plan

Select dial plan to handle calls coming from user phone to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules.

Other Parameters

Echo Cancellation

Enable/Disable echo cancellation for VoIP calls and select echo canceller tail length. Voice&Data Router supports echo canceller length from 8 ms up to 128 ms in step of 4 ms. Default echo canceller tail length is 64 milliseconds.

Supervisory Tones

Select one of predefined set of supervisory (indication) progress tones for this user extension.

Polarity Reversal

Enable/disable FXS line polarity reversal. When enabled every answer and hang-up of the remote party is signaled to the line by changing/switching its polarity.

Rx Gain, Tx Gain

Use these parameters for FXS line volume adjustment – transmit and receive gain or attenuation. Rx gain defines the level of voice received by Voice&Data Router from the FXS line and tx gain parameter defines the level of voice transmitted from Voice&Data Router to the FXS Line. You can modify volume level in range from -18 dB up to 6 dB.

Impedance

FXS line impedance setting. Two line impedance modes are available

- 600 Ω
- Complex global impedance

Loop Current

This setting allows to define FXS line loop current limit. It is available to set the constant loop current in range between 18 mA and 28 mA (default value is 18 mA).

Flash Length

Maximal length of hook flash in milliseconds. Only hook flash shorter than defined time can be evaluated to hold/unhold active calls.

Services**User's Permission Group**

Select permission group to restrict outgoing calls for this user. User permission group defines a collection of call permission flags. User permission groups are assigned to the users and call permission flags are assigned to the calling rules. User is allowed to make a call only if his permission group includes call permission flag assigned to calling rule for the call. Please see [Permissions](#) menu for more details.

Pickup Group

Pickup group allows to pickup fellow workers' calls. Users from the same group can pickup incoming calls each other using code defined in [Services Codes](#) menu.

Call Transfer

Permit/deny call transfer service. If enabled the user is allowed to transfer active call to previously held one by hang-up the handset.

Call Forwarding

Permit/deny Call Forwarding services for extension user. If enabled the user can activate/deactivate call forwarding service (unrestricted / when busy /when no answer) by service codes defined in [Services Codes](#) menu.

Do Not Disturb

Permit/deny Do Not Disturb service for extension user. If enabled the user is allowed to activate or deactivate this service by service codes defined in [Services Codes](#) menu.

TRUNKS MENU

Trunks menu offers trunks configuration. Voice&Data Router supports SIP trunks, E1/T1 trunks, BRI trunks (S0 or U0), analogue trunks (FXO and E&M) and GSM trunks. BRI, analogue and GSM trunks are optional and they depend on hardware configuration.

SIP Trunks

SIP trunks main screen displays table of all configured trunks. You can use the **New SIP Trunk** button to create and configure new VoIP SIP trunk. Button **Edit** serves to modify appropriate SIP trunk setting and the **Delete** button is dedicated to remove existing trunk. Trunk can be removed only if there does not exist any reference to this trunk in calling rules.

GUI-version : 1.0 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > SIP Trunks

SIP Trunks Settings New SIP Trunk

Provider/Client Name	DialPlan	Hostname/IP	Username	Edit	Delete
sipp_client	from_sip	192.168.1.14	sipp_client	Edit	Delete
sipp_server	from_sip	192.168.1.48	sipp_server	Edit	Delete
TEST	from_sip	192.168.1.166	test_trunk	Edit	Delete

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

When you are creating new SIP trunk or when you are changing parameters of the existing one you are switched SIP trunk's details form, with all available trunk settings. Here you can configure available parameters and click **Save** button to store new configuration.

SIP trunk parameters

Provider/Client Name

A unique label to help you identify this VoIP trunk. This identifier is used over all of Voice&Data Router configuration where we need reference to this trunk.

Dial Plan

Select dial plan to handle calls coming from SIP trunk to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules.

Hostname

There are two possibilities how to connect to the remote peer (SIP server). **Static** connection defines permanent static connection to the dedicated IP address. It should be used in case when the trunk connects Voice&Data Router to superior system (SIP provider) and the registration with this system is required. Remote peer address should be configured for static connection (you can use numeric IP address or the host name). On the other hand, **dynamic** connection type is selected when remote peer is registering with Voice&Data Router. It is also possible to change standard port number of SIP protocol to listen for SIP signaling.

Username

SIP channel user name. This field specifies the user name for the authentication.

Authuser

User name used for authentication when Voice&Data Router is registering with the SIP provider or another superior system (see Register option below). Use this field only if you need different name than the username option above.

GUI-version : 1.0 / Board Type : 1 Edit Trunk Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > SIP Trunks

Edit SIP trunk - TEST

Provider/Client Name

DialPlan

Hostname :

Username

Authuser

Fromuser

Fromdomain

Password

Contact

Qualify ☒

Insecure Type

Codecs First Second Third

Fourth Fifth

Caller ID

VoIP Settings Register ☒ NAT ☒ Can Reinvite ☐ DTMF Mode

Call Limit

Fax & Modem Support Enable T.38 ☒

Fax Passthrough ☒ Codec

Modem Passthrough ☒ Codec

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Fromuser

This allows you to overwrite the user name in the From and Contact SIP header fields of the INVITE request. It may be required by some providers for authentication.

Fromdomain

This allows you to set the domain in the From SIP header field of the INVITE request. It may be required by some providers for authentication

Password

Password to use for authentication.

Contact

SIP URI contact name (user name in Contact SIP header field) used when Voice&Data Router is registering with the SIP provider or another superior system (see Register option below).

Qualify

Enable this feature to check if remote device is reachable. Qualify will send a SIP OPTIONS command regularly to check that the remote device is still online. If the device does not answer within the configured period Voice&Data Router considers the remote device off-line for future calls. Expiration time is configured in seconds (default is 2 seconds). This feature may also be used to keep a UDP session open to a device that is located behind a NAT. This can be used in conjunction with the NAT setting.

Insecure Type

Insecure option specifies how to handle incoming SIP session and trunk matching. If it is disabled normal IP-based matching applies and the authentication is required (when password is set for user extension). Set insecure to **port** to allow matching of SIP trunk by IP address without matching port number (useful when we have multiple endpoints behind NAT). Set insecure to **invite** to remove the requirement for authentication of incoming INVITE messages. And use **very** value to allow both, the matching of trunk by IP address without matching port number and to remove the requirement for authentication of incoming INVITE messages.

Codecs

Here you can define allowed voice compression codecs in order of preference. Voice&Data Router supports following voice codecs:

- **G.711 A-Law**
- **G.711 μ -Law**
- **G.729 Annex A/B**
- **G.726-32**
- **G.723.1**
- **GSM**
- **iLBC**

Up to five codecs with defined preference can be configured for every SIP trunk.

Caller ID

This is the caller identification number that the trunk will try to use when making outbound calls. Set this field if you want to overwrite original calling user identification. It is useful when unique identification for all calls is required.

VoIP Settings**Register**

Check this to enable registering at remote server. When enabled Voice&Data Router will register this trunk with the SIP provider or another superior system.

NAT

This setting allows communication with remote device behind the NAT. It works properly in conjunction with Qualify setting in order to keep open the connection from Voice&Data Router to the peer behind the NAT.

Can Reinvite

Enabling this option causes Voice&Data Router to attempt to route the RTP media stream directly between SIP endpoints, bypassing Voice&Data Router.

DTMF Mode

Default mode for sending DTMF digits.

Call Limit

Enter maximal number of simultaneous calls permitted for this trunk.

Fax & Modem Support**Enable T.38**

Enable/disable T.38 protocol (real-time Fax over IP) support. When enabled, Voice&Data Router can work as T.38 Fax Relay between SIP and TDM.

Fax Passthrough

Enable Fax Pass-Through for automatic switch to the codec G.711 to transfer Fax stream over the SIP trunk. If enabled together with T.38 protocol, T.38 Fax Relay will be used as preferred method for FAX transmission and if not acceptable by the peer then G.711 codec will be used instead. Please select G.711 codec version (A-Law/ μ -law) to use for Fax Pass-Through.

Modem Passthrough

Enable Modem Pass-Through for automatic switch to the codec G.711 to transfer modem data over the SIP trunk. Please select G.711 codec version (A-Law/ μ -law) to use for Modem Pass-Through.

E1/T1 trunks

Main screen for E1/T1 trunks displays table of available E1/T1 interfaces. There are always four E1/T1 ports in Voice&Data Router and unnecessary ports can be disabled. Use **Edit** button to modify configuration of selected E1/T1 interface.

E1/T1 trunk is configured in two steps. First of all some essential settings are done (including selection of line mode and signaling type). After that the configuration of all other details can be completed.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > E1/T1 Trunks

E1/T1 Trunks Settings

E1/T1 Interfaces

Interface	Name	Line Mode	Signaling	DialPlan	Status	
A	E1-A	E1	isdn	from_e1	ON	Edit
B	E1-B	E1	isdn	from_e1	ON	Edit
C	E1-C	E1	cas	from_e1	ON	Edit
D	E1-D	E1	cas	from_e1	OFF	Edit

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

When you click the **Edit** button in the trunks table new form with general settings appears. Here you can select basic parameters of E1/T1 interface and click on **Details** to process detailed configuration. Or use **Save** button to store new settings.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > E1/T1 Trunks

Interface B

General Settings

☒ Enabled

Name Line Mode Signaling

DialPlan

[Details](#)

[Save](#) [Cancel](#)

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

General Settings

Enabled

Enable/Disable E1/T1 interface.

Name

A unique label to help you identify E1/T1 trunk. This identifier is used over all of Voice&Data Router configuration where we need reference to this trunk.

Line Mode

Choose line mode

- **E1** 2,048 Mb/s line divided to 32 timeslots
- **T1** 1,544 Mb/s line divided to 24 timeslots.

Note that CAS signaling is only available in E1 mode. It is also important to know that line mode changing resets the entire trunk configuration to default status. You should use **Details** button to modify this default setting where it is necessary.

Signaling

Signaling type selection. Voice&Data Router supports **ISDN** and **CAS** (MFC/R2) signaling. Note that CAS signaling is only available in E1 mode. Changing of signaling type resets signaling dependent parameters to their default values. Use **Details** button to check and modify these parameters.

Dial Plan

Select dial plan to handle calls coming from E1/T1 line to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules.

Click **Details** button to continue with detailed configuration. E1/T1 trunk details form can differ in dependence on selected signaling type.

GUI-version : 1.1 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > E1/T1 Trunks

Details: Interface B

Line Parameters

☒ CRC
Clock Mode Slave 1
☐ Longhaul RX
☐ Longhaul TX

ISDN Details

Switch Type EuroISDN
Mode TE
☐ Restart L3

Channels

Channels 1-15,17-31
Signaling Channel 16

Channel Selection Descending
☐ Cyclic

Parameters

☒ Overlap Dial
First Digit Timeout 15
Other Digits Timeout 10

☒ Echo Cancellation default

Supervisory Tones Slovak Republic

☐ Play Progress Tone
☒ Play Ringback Tone
☐ Play Dial Tone

AOC

☐ Generate AOC Charging default
☐ Add Incoming Charging

Save Go Back Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Line Parameters

CRC

Enable CRC4 multiframe format of framing mode.

Clock Mode

Choose clock synchronization source

- **Master** device provides synchronization clock to the line

- **Slave 1** device is synchronized by the clock from the line
- **Slave 2** device is synchronized by the clock from the line

Slave 1 has higher priority than Slave 2.

Longhaul RX, Longhaul TX

These options enable to increase the device radius by setting the receiving/transmitting more sensitive. Long haul parameter is within G.703 specification and it is also possible to connect a standard device to the device with long haul.

ISDN Details

This is signaling dependent part is available only for E1/T1 trunk with ISDN signaling.

Switch Type

Select ISDN signaling variant.

Mode

Select ISDN signaling mode

- **NT** network side
- **TE** terminal/user (CPE) side

Restart L3

Enable automatic restart procedure on 3rd layer for all voice channels. Restart procedure starts after D-channel coming up and repeats every hour.

CAS Details

This is signaling dependent part is available only for E1 trunk with CAS signaling type.

Register Signaling

Select register signaling

- **MFC/R2** Use MFC/R2 tones to transfer DNIS number, ANI number and call progress status.
- **DTMF** Use DTMF tones to transfer DNIS number. No caller identification is available for this register signaling.
- **MFC/R2+DTMF** Allows combination of MFC/R2 and DTMF signaling when you can select different register signaling in outgoing direction and incoming direction.
- **Pulse** Use line signaling pulses to transfer DNIS number. No caller identification is available for this register signaling.

CAS Variant

Select CAS national variant. Voice&Data Router offers predefined national variants you can use. There is also possibility to customize predefined variants for your needs or to create your own national variant. See section [CAS National Variants](#) for more details.

Max Length of ANI Number

Maximal number of ANI (Automatic Number Identification) digits = caller identification number. This option is valid only for MFC/R2 register signaling.

Max Length of DNIS Number

Maximal number of DNIS (Dialed Number Identification Service) digits = called party address.

Send ANI after DNIS

Enable this option if you want transfer whole DNIS number before ANI number. This option is valid only for MFC/R2 register signaling.

Ask for ANI

Enable caller identification request. Disable this option if remote exchange does not support or you do not require caller identification (ANI number). This option is valid only for MFC/R2 register signaling.

Use FORCED RELEASE

Enable Forced Release line signal.

Send CLEAR BACK

Enable sending of Clear-Back line signal to remote side.

Accept CLEAR BACK

Enable receiving of Clear-Back line signal from remote side.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > E1/T1 Trunks

Details: Interface B

Line Parameters

☒ CRC Clock Mode Slave 1 ☐ Longhaul RX ☐ Longhaul TX

CAS Details

Register Signaling MFC/R2 Send MFC/R2 receive DTMF

CAS Variant Czech-Slovak

Max.length of DNIS Number 24 Max.length of ANI Number 24

☐ Send ANI after DNIS ☒ Ask for ANI

☒ Use FORCED RELEASE ☒ Send CLEAR BACK ☒ Accept CLEAR BACK

Channels

Channels 1-15,17-31

Channel Selection Descending ☐ Cyclic

Parameters

☒ Overlap Dial First Digit Timeout 15 Other Digits Timeout 10

☒ Echo Cancellation default

Supervisory Tones Slovak Republic

☐ Play Progress Tone ☒ Play Ringback Tone ☐ Play Dial Tone

AOC

☐ Generate AOC Charging default ☐ Add Incoming Charging

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Channels**Channels**

Choose available voice channels.

- E1 mode use channel range from 1 to 31.
- T1 mode use channel range from 1 to 24.

Avoid of collision with signaling channel. E1 line with CAS signaling has reserved channel 16 for line signaling transfer.

Signaling Channel

Signaling channel (ISDN D-channel) selection. It is possible to move ISDN signaling channel to any position when it is necessary. E1 line uses channel 16 and T1 line uses channel 24 for signaling by default. This option is available only for ISDN signaling type. CAS signaling has always reserved 16th channel for line signaling transmission and it cannot be changed.

Channel Selection

Choose method how to select voice channel for outgoing call.

- **Ascending** search for the lowest available channel number.
- **Descending** search for the highest available channel number

Cyclic

Enable cyclic search of available channel for outgoing call instead of sequential.

Parameters**Overlap Dial**

Enable/disable overlap dialing in ISDN signaling. If not enabled, complete called number in SETUP is required. E1 line with CAS signaling always uses overlap dialing.

First Digit Timeout

Enter timeout for the first digit to detect dialing hesitation during overlap dialing. When it expires end of dial is indicated.

Others Digits Timeout

Enter timeout of others to detect dialing hesitation during overlap dialing. End of dial is indicated after the timeout.

Echo Cancellation

Enable/Disable echo cancelation for VoIP calls and select echo canceller tail length. Voice&Data Router supports echo canceller length from 8 ms up to 128 ms in step of 4 ms. Default echo canceller tail length is 64 milliseconds.

Supervisory Tones

Select one of predefined set of supervisory/indication tones generated by this E1/T1 line.

Play Progress Tone

Enable generation of progress supervisory/indication tones.

Play Ringback Tone

Enable generation of ring-back tone.

Play Dial tone

Enable generation of dial tone.

AOC**Generate AOC Charging**

Enable/disable generation of charging information according selected AOC table. See section [AOC Tables Settings](#) for details about configuration of AOC charging generation.

Add Incoming Charging

If enabled charging units received from destination will be added to the charging units generated by Voice&Data Router according AOC table.

Use **Go Back** button to return to general settings or click on **Save** button to confirm changes and store new setting.

BRI Trunks

Voice&Data Router supports up to 16 BRI Uk0 interfaces or 4 BRI S0 interfaces. Initial screen for BRI trunks displays table of available interfaces according hardware configuration. BRI trunks are configured in two steps. First of all some essential settings are done. After that the configuration of all other details can be completed.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Trunks > BRI Trunks

BRI Trunks Settings

BRI Interfaces

Interface	Name	Line Mode	Dial Plan	Channel	Status	
A	UK0-A	Uk0	t	177,178	ON	Edit
B	UK0-B	Uk0	t	180,181	ON	Edit
C	UK0-C	Uk0	t	183,184	ON	Edit
D	UK0-D	Uk0	t	186,187	ON	Edit
E	UK0-E	Uk0	t	189,190	ON	Edit
F	UK0-F	Uk0	t	192,193	ON	Edit
G	UK0-G	Uk0	t	195,196	ON	Edit
H	UK0-H	Uk0	t	198,199	ON	Edit

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

When you click the **Edit** button in the trunks table new form with general settings appears. Here you can select basic parameters of BRI interface and click on **Details** to process detailed configuration. Or use **Save** button to store new settings.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Trunks > BRI Trunks

Interface B

General Settings

☒ Enabled

Name Dial Plan

[Details](#)

[Save](#) [Cancel](#)

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

General Settings**Enabled**

Enable/Disable BRI interface.

Name

A unique label to help you identify BRI trunk. This identifier is used over all of Voice&Data Router configuration where we need reference to this trunk.

Dial Plan

Select dial plan to handle calls coming from this BRI line to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules configuration.

Click **Details** button to continue with detailed configuration.

Line Parameters**Clock Mode**

Choose clock synchronization source

- **Master** device provides synchronization clock to the line. This is the only option when line is configured in NT mode (S0 interface) or LT mode (Uk0 interface).
- **Slave 1** device is synchronized by the clock from the line
- **Slave 2** device is synchronized by the clock from the line

Slave 1 has higher priority than Slave 2.

Line Power Supply

Enable line power supply. Line can be powered only in NT mode (S0 interface) or LT mode (Uk0 interface). This function depends on type of device power supply.

GUI-version : 1.8 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics

Trunks > BRI Trunks

Interface B

Line Parameters

Clock Mode ? Master ▼ ☒ ? Line Power Supply

ISDN Details

Switch Type ? EuroISDN ▼ Mode ? LT ▼ ☒ ? Point-to-Multipoint
☐ ? L2 Deactivation

Channels

Channels 180,181
Channel Selection ? Ascending ▼ ☐ ? Cyclic

Parameters

☒ ? Overlap Dial First Digit Timeout 15 Other Digits Timeout 7
☒ ? Echo Cancellation default ▼
Supervisory Tones ? Slovak Republic - PBX ▼
☒ ? Play Progress Tone ☒ ? Play Ringback Tone ☒ ? Play Dial Tone

AOC

☐ ? Generate AOC Charging default ▼ ☐ ? Add Incoming Charging

Save Go Back Cancel

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk
ISDN Details**Switch Type**

Select ISDN signaling variant.

Mode

Select ISDN signaling mode.

Modes for S0 interface:

- **NT** network/provider side
- **TE** terminal/user (CPE) side

Modes for Uk0 interface:

- **LT** network/provider side
- **NT** terminal/user (CPE) side

Point-to-Multipoint

Enable point-to-multipoint mode when Voice&Data Router is attached to an ISDN bus (more than one devices can be used at the CPE side).

L2 Deactivation

Enable automatic deactivation of L2 data-link connection for line configured in point-to-multipoint mode.

Channels

Channels

List of B channels timeslots.

Channel Selection

Choose method how to select B channel for outgoing call.

- **Ascending** search for the lowest available channel number.
- **Descending** search for the highest available channel number

Cyclic

Enable cyclic search of available B channel for outgoing call instead of sequential.

Parameters

Overlap Dial

Enable/disable overlap dialing. If not enabled, complete called number in SETUP is required.

First Digit Timeout

Enter timeout for the first digit to detect dialing hesitation during overlap dialing. When it expires the end of dial is indicated.

Others Digits Timeout

Enter timeout of others digits to detect dialing hesitation during overlap dialing. The end of dial is indicated after the timeout.

Echo Cancellation

Enable/Disable echo cancelation for VoIP calls and select echo canceller tail length. Voice&Data Router supports echo canceller length from 8 ms up to 128 ms in step of 4 ms. Default echo canceller tail length is 64 milliseconds.

Supervisory Tones

Select one of predefined set of supervisory/indication tones generated by this BRI line.

Play Progress Tone

Enable generation of progress supervisory/indication tones.

Play Ringback Tone

Enable generation of ring-back tone.

Play Dial tone

Enable generation of dial tone.

AOC

Generate AOC Charging

Enable/disable generation of charging information according selected AOC table. See section [AOC Tables Settings](#) for details about configuration of AOC charging generation.

Add Incoming Charging

If enabled charging units received from destination will be added to the charging units generated by Voice&Data Router according AOC table.

Use **Go Back** button to return to general settings or click on **Save** button to confirm changes and store new setting.

Analog Trunks

Main screen for analogue trunks displays table of all available FXO interfaces. Analogue trunks are optional interfaces depending on hardware configuration of Voice&Data Router. Because FXO module/card has 2 ports we can have from 2 up to 16 analogue FXO trunks in the system (FXO module can occupy all 8 slots available on the analogue extension card).

All available analogue trunks are always displayed. Unused ports (not configured) are marked as **unset position**. Use **Edit** button to configure selected interface – modify existing setting or configure unused port. To remove some trunk from the configuration click on **Unused** button. Analogue FXO trunk can be removed only if there does not exist any reference to this port in any calling rules or calls groups.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router

inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > Analog Trunks

Analog Trunks Settings

Analog Interfaces

Position	Name	Trunk Type	DialPlan	CID Number	Channel		
9	FX01	FXO	from_fx0		152	Unused	Edit
11	FX02	FXO	from_fx0		153	Unused	Edit
13	FX03	FXO	from_fx0		156	Unused	Edit
15	FX04	FXO	from_fx0	0445567888	157	Unused	Edit
17	FX05	FXO	from_fx0		160	Unused	Edit
19	FX06	FXO	from_fx0		161	Unused	Edit
21	unset position	FXO			164		Edit
23	unset position	FXO			165		Edit

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

When you click on **Edit** button to configure selected analogue trunk you will continue with new screen with detailed configuration. Here you can configure all parameters and click **Save** button to store new setting.

General Settings

Trunk Type

Analogue trunk type

- FXO FXO interface

Position

This is analogue port position (number from 1 up to 32).

Channel

Internal channel number.

Name

A unique label to help you identify analogue trunk. This identifier is used over all of Voice&Data Router configuration where we need reference to this trunk.

Dial Plan

Select dial plan to handle calls coming from this analogue trunk line to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules.

CID Number

This is the caller identification number you can use to overwrite original calling user identification.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > Analog Trunks

Edit Trunk Settings

General Settings

Trunk Type

Position

Channel

Name

DialPlan

CID Number

Parameters

Echo Cancellation

Polarity reversal ☒ Pulse dial ☐

Rx Gain Tx Gain

Impedance

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Parameters

Echo Cancellation

Enable/Disable echo cancellation for VoIP calls and select echo canceller tail length. Voice&Data Router supports echo canceller length from 8 ms up to 128 ms in step of 4 ms. Default echo canceller tail length is 64 milliseconds.

Polarity Reversal

Enable/disable polarity reversal detection on FXO trunk. When enabled then answer or hang-up of the remote party can be signaled to the Voice&Data by change of polarity on FXO line.

Pulse Dial

Enable pulse dialing instead of using DTMF tones.

Rx Gain, Tx Gain

Use these parameters for line volume adjustment – transmit and receive gain or attenuation. Rx gain defines the level of voice received by Voice&Data Router from the FXO trunk and tx gain parameter defines the level of voice transmitted from Voice&Data Router to the FXO trunk. You can modify volume level in range from -15 dB up to 12 dB.

Impedance

FXO line AC termination impedance setting. Two modes are available

- 600 Ω
- Global Complex impedance

GSM Trunks

GSM trunks main screen displays table of available GSM interfaces. GSM trunks are optional interfaces depending on hardware configuration of Voice&Data Router. It is possible to have up to 12 GSM ports in the system.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > GSM Trunks

GSM Trunks Settings

GSM Trunks

Interface	Name	DialPlan	Channel	
1	GSM1	from_gsm	128	Edit
2	GSM2	from_gsm	129	Edit
3	GSM3	from_gsm	130	Edit
4	GSM4	from_gsm	131	Edit

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

To modify GSM trunk configuration use appropriate **Edit** button in GSM trunks table.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Trunks > GSM Trunks

Edit Trunk Settings

General Settings

Name [?](#)

DialPlan [?](#)

PIN Number [?](#)

Echo Cancellation [?](#) ☐

Audio Level

From GSM [?](#)

To GSM [?](#)

[Save](#) [Cancel](#)

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

General Settings

Name

A unique label to help you identify GSM trunk. This identifier is used over all of Voice&Data Router configuration where we need reference to this trunk.

Dial Plan

Select dial plan to handle calls coming from this GSM interface to Voice&Data Router. Dial plan consists of calling rules and it defines call routing scenario. Please see chapter [Traffic Menu](#) for more details about dial plans and calling rules.

PIN Number

Enter valid PIN code to access GSM SIM card.

Echo Cancellation

Enable/disable echo cancellation on GSM module to suppress acoustic echo from GSM network.

Audio Level

From GSM

Configure speaker volume level in range from 0 to 99. This is voice level received by Voice&Data Router from GSM trunk. Default value is 91.

To GSM

Configure microphone volume level in range from 0 to 15. This is level of the voice transmitted from Voice&Data Router to GSM trunk. Default value is 3.

TRAFFIC MENU

Traffic menu defines call routing between users and trunks. Call routing system of Voice&Data Router can be very easy but it can be also really complex depending on system functionality. It seems to be the most important part of the whole system which designates if Voice&Data Router works correctly or not.

Call routing consists of

- Calling rules
- Dial planes

Calling rules define new call destination on the basis of analysis of dialed number eventually dialed number together with caller identification number. Calling rules are divided according type of source and destination to rules for User to User, User to Trunk, Trunk to User and Trunk to Trunk. Calling rules also allow defining modification of dialed number or caller identification number.

Dial plans group existing calling rules. Dial plans are assigned to users and trunks. Calling rules included in dial plan then will apply for all inbound calls from the user or trunk.

Configuration of call routing is two-level

1. Define calling rules.
2. Group existing calling rules to dial plans.

Finally, it is necessary to assign dial plans to users and trunks. Interfaces without dial plan can not serve inbound calls and the calls will be refused.

Calling Rules

Main screen for calling rules configuration shows list of existing calling rules.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > Calling Rules

Calling Rules Settings

Calling Rules Groups

Calling rules are divided into four groups according to the method of call routing (User-User, User-Trunk, Trunk-User, Trunk-Trunk). This allows different patterns to be dialed to the local and remote destination. You can optionally set three failover trunks to use when the primary trunk fails. Note that this panel manages only individual call rules. See the Dial Plans section to associate multiple calling rules to be used for User and Trunk dialing.

User to User

Calling Rules: User to User	New Calling Rules Group Name	Create
internal		Edit Delete

User to Trunk

Calling Rules: User to Trunk	New Calling Rules Group Name	Create
e1		Edit Delete
sip		Edit Delete

Trunk to User

Calling Rules: Trunk to User	New Calling Rules Group Name	Create
users		Edit Delete

Trunk to Trunk

Calling Rules: Trunk to Trunk	New Calling Rules Group Name	Create
out		Edit Delete

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Calling rules are divided into four tables

- User to User
- User to Trunk
- Trunk to User
- Trunk to Trunk

You can create new empty calling rules group when you enter new unique label into the field **New Calling Rules Group Name** of appropriate table and click on the **Create** button. This name is used to identify calling rules group in dial plan configuration. Use the **Edit** button to modify configuration of selected group of calling rules. And use the **Delete** button to remove selected group of calling rules. Calling rules can be removed only if there does not exist any reference to this group of calling rules in any dial plan.

When you click on the **Edit** button for selected group of calling rules new form with list of calling rules appears. Table shows analysis pattern and call destination (the details depend on calling rule type). You can create new calling rule by clicking on the **New Calling Rule** button, you can modify calling rule by clicking on the **Edit** button or you can delete calling rule using the **Delete** button.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > Calling Rules

Calling Rules Settings "USER TO TRUNK"

Calling Rules: e1

New Calling Rule Back to Calling Rules List

Pattern	Trunk	Failover Trunks	Clone to Rules Group Name	Clone
_01.	E1 :E1-A			Edit Delete
_02.	E1 :E1-B			Edit Delete
_03.	E1 :E1-C			Edit Delete
_04.	E1 :E1-D			Edit Delete
_8.	FXO:FXO2			Edit Delete
_9.	CallGroup: FXO			Edit Delete

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

If you need to make copy of calling rules group you can use the **Clone** button. Before you click on the **Clone** button you have to enter unique identifier of new group of calling rules in the field **Clone to Rules Group Name**.

Calling Rules Patterns

Every calling rule has pattern for analysis of incoming dialed number eventually caller identification number. Pattern for caller identification number is added to the dialed number pattern by forward slash character (example: _NXXXXXX/_04455XXXXX). Calling rules patterns may be numbers, letters, or combinations thereof. One pattern can match single specific number or whole group of multiple numbers. If the pattern is used for multiple matching it must be prefixed by underscore symbol (_). After the underscore, you can use one or more of the following special characters.

- **X** Matches any single digit from 0 to 9.
- **Z** Matches any single digit from 1 to 9.
- **N** Matches any single digit from 2 to 9.
- **[15-7]** Matches a single digit from the range of digits specified. In this case, the pattern matches a single 1, 5, 6, or 7.
- **.** (period) Wildcard match – matches one or more characters, no matter what they are.
- **!** (bang) Wildcard match – matches zero or more characters, no matter what they are.

There is also special pattern **s** that will match to empty dialed number. This is intended for non-DID lines, where call comes in without any dialed number information (like FXO or GSM trunk).

Examples:

111 matches single extension 111.

_NXXXXXX	matches normal 7 digit number.
_1NXXNXXXXXX	would represent an area code plus phone number preceded by a one.
_9011.	matches any string of at least five characters that starts with 9011, but it does not match the four-character string 9011 itself.
_9011!	same as above but matches 9011 too.
_#	matches a single # key press.
s	matches when dialed number is not available

If you are not careful, wildcard matches can make your call routing do things you are not expecting. You should use the wildcard match in a pattern only after you have matched as many other digits as possible. For example, the pattern match “_.” should probably never be used. Use pattern “_X.” instead, if at all possible.

User to User Details

User to User calling rules defines call routing between local user extensions of Voice&Data Router.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > Calling Rules

Edit Calling Rule: internal

Pattern

Call Permission Flag

Send to Destination

Local Destination

Save Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Pattern

Pattern for analysis of the incoming dialed number from the user. If you need to analyze also caller identification number, you can append caller identification pattern to dialed number pattern using forward slash character (_XXX/_111). Only calls that match this pattern will apply this calling rule. See explanation above for details about calling rules pattern syntax.

Call Permission Flag

Select call permission flag to allow outgoing calls for only selected users. Each user can be assigned to a user permission group. User permission group defines a collection of call permission flags. The call is allowed only in case when user permission group of calling user incorporates permission flag of the calling rule. Please see [Permissions](#) menu for more details.

Send to Destination

Local Destination



Select call local destination. It is possible to select:

- **Existing user extension** – call will be routed directly to the selected user extension.
- **Existing ring group** – call will be routed to the selected ring group (group of user extensions which can ring simultaneously or sequentially, see [Ring Groups](#) for details).
- **User DID** – call will be routed to the user extension specified by dialed number. This option is useful with multiple matching patterns like _XX or _[234]XX. It can simplify calling rules to only a few lines when we do not need to create separate rules for every user.
- **Hangup** – call will be refused (with busy tone)
- **Congestion** – call will be refused (with congestion tone)

User to Trunk Details

User to Trunk calling rules defines call routing from local user extensions outside of Voice&Data Router over the trunk interfaces. It can be call to PSTN, call to VoIP provider or call to cooperative gateway/PBX.

GUI-version : 1.8 / Board Type : 1 Logout

Home
Users
Trunks
Traffic
Globals
System
Diagnostics

Traffic > Calling Rules

Edit Calling Rule: out

Pattern

Call Permission Flag -- none --

Send to Destination

Use Trunk E1: E1-A

Strip 2 digits

and Prepend these digits before dialling

☒ Change TON / NPI

National / ISDN/Telephony

☐ Two Step Dial

Strip 0 digits from Caller ID

and Prepend these digits to Caller ID

Presentation Original

☒ Change TON / NPI of Caller ID

National / ISDN/Telephony

☐ Use Fail-Over Trunk 1

Fail-Over Trunk

Strip digits

and Prepend these digits before dialling

☐ Change TON / NPI

Unknown / Unknown

☐ Two Step Dial

Strip digits from Caller ID

and Prepend these digits to Caller ID

Presentation Original

☐ Change TON / NPI of Caller ID

Unknown / Unknown

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Pattern

Pattern for analysis of incoming dialed number from the user. If you need to analyze also caller identification number, you can append caller identification pattern to dialed number pattern using forward slash character (`_044[5-8]XXXXXX/_111`). Only calls that match this pattern will apply this calling rule. See explanation above for details about calling rules pattern syntax.

Call Permission Flag

Select call permission flag to allow outgoing calls for only selected users. Each user can be assigned to a user permission group. User permission group defines a collection of call permission flags. The call is allowed only in case when user permission group of calling user incorporates permission flag of the calling rule. Please see [Permissions](#) menu for more details.

Send to Destination

This section defines primary routing destination of the call.

Use Trunk

Select destination trunk to place call through. It is possible to choose directly one of existing trunk or existing call group configured in Voice&Data Router. Call groups can group multiple trunks to one "trunk-group" with defined method of channel selection. Please see [Call Groups](#) menu for more details. It is also possible to select Hangup or Congestion options to refuse the call.

Two Step Dial

Enable two-stage dialing using selected alternative carrier. Two-stage dialing replaces dialed number with carrier access number and on carrier's answer the security code (if set) and the destination number are transmitted in DTMF. See [Carriers](#) menu for alternative carrier configuration details.

Strip digits, and Prepend these digits before dialing

These parameters allow modifying dialed number before the call is placed on the outbound trunk. You are allowed to strip specified number of digits from the front of dialed number and you can enter prefix string which will be prepended to the dialed number.

Change TON/NPI

Enable to overwrite Type of Number and Numbering Plan Identification of dialed destination number before the call is placed on the selected outbound trunk. This option is applied only on trunk with ISDN signaling.

Strip digits from Caller ID, and Prepend these digits to Caller ID

These parameters allow modifying caller identification number before the call is placed on the outbound trunk. You are allowed to strip specified number of digits from the front of the caller identification number and you can enter prefix string which will be prepended to this number.

Presentation

This option allows modifying of caller identification presentation before the call is placed on the outbound trunk.

Change TON/NPI of Caller ID

Enable to overwrite Type of Number and Numbering Plan Identification of caller identification number before the call is placed on the selected outbound trunk. This option is applied only on trunk with ISDN signaling.

Use Fail-Over trunk 1, 2, 3

This section allows you to define alternative routing of the call if primary destination is busy or down. It is possible to define maximally 3 fail-over alternatives. Each fail-over destination has same options as we define for primary call destination.

Trunk to User Details

Trunk to User calling rules defines call routing from external interface to the local Voice&Data Router user extensions. It can be call from PSTN or VoIP provider or call from another gateway/PBX.

GUI-version : 1.8 / Board Type : 1 Edit Calling Rule ! Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Traffic > Calling Rules

Edit Calling Rule: in

Pattern

Send to Destination

Local Destination

Strip digits and Prepend these digits before dialling

Strip digits from Caller ID and Prepend these digits to Caller ID

Presentation

☐ Connect announcement before the call

Save Cancel

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Pattern

Pattern to match incoming dialed number from the trunk. If you need to analyze also caller identification number, you can append caller identification pattern to dialed number pattern using forward slash character `_NXXXXXX/_04455XXXXX`). Only calls that match this pattern will apply this calling rule. See explanation above for details about calling rules pattern syntax.

Send to Destination:**Local Destination**

Select call local destination. It is possible to select:

- **Existing user extension** – call will be routed directly to the selected user extension.
- **Existing ring group** – call will be routed to the selected ring group (group of user extensions which can ring simultaneously or sequentially, see [Ring Groups](#) for details).
- **User DID** – call will be routed to DID (Direct Inward Dialing) user extension. Destination user extension number is extracted from incoming dialed number after applying modifications (strip/prepend). This option is useful with multiple matching patterns like _55679XX. It can simplify calling rules to only a few lines when we do not need to create separate rules for every user.
- **Hangup** – call will be refused (with busy tone)
- **Congestion** – call will be refused (with congestion tone)

Strip digits, and Prepend these digits before dialing

These parameters allow modifying dialed number for “User DID” routing. You are allowed to strip specified number of digits from the front of dialed number and you can enter prefix string which will be prepended to the dialed number.

Strip digits from Caller ID, and Prepend these digits to Caller ID

These parameters allow modifying caller identification number before the call is routed to the selected local destination. You are allowed to strip specified number of digits from the front of the caller identification number and you can enter prefix string which will be prepended to this number.

Presentation

This option allows modifying of caller identification presentation before the call is routed to the selected local destination.

Connect announcement before the call

This option allows to play predefined announcement to the caller before the call will be routed to the selected local destination.

Trunk to Trunk Details

Trunk to Trunk calling rules defines transit call routing between external interfaces (trunks).

Pattern

Pattern to match incoming dialed number from the trunk. If you need to analyze also caller identification number, you can append caller identification pattern to dialed number pattern using forward slash character _NXXXXXX/_04455XXXXX). Only calls that match this pattern will apply this calling rule. See explanation above for details about calling rules pattern syntax.

Send to Destination:

This section defines primary destination of the call.

Use Trunk

Select destination trunk to place call through. It is possible to choose directly one of existing trunk or existing call group configured in Voice&Data Router. Call groups can group multiple trunks to one “trunk-group” with defined method of channel selection. Please see [Call Groups](#) menu for more details. It is also possible to select Hangup or Congestion options to refuse the call.

Two Step Dial

Enable two-stage dialing over selected alternative carrier. Two-stage dialing replaces dialed number with carrier access number and on carrier's answer the security code (if set) and the destination number are transmitted in DTMF. See [Carriers](#) menu for alternative carrier configuration details.

Strip digits, and Prepend these digits before dialing

These parameters allow modifying dialed number before the call is placed on the outbound trunk. You are allowed to strip specified number of digits from the front of dialed number and you can enter prefix string which will be prepended to the dialed number.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic **Globals** System Diagnostics

Traffic > Calling Rules

Edit Calling Rule: tt

Pattern

Send to Destination

☐ Use Trunk
☐ Two Step Dial

Strip digits
 and Prepend these digits before dialling
 and Prepend these digits to Caller ID

☐ Change TON / NPI /
☐ Change TON / NPI of Caller ID /

☐ Use Fail-Over Trunk 1
☐ Two Step Dial

Strip digits
 and Prepend these digits before dialling
 and Prepend these digits to Caller ID

☐ Change TON / NPI /
☐ Change TON / NPI of Caller ID /

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Change TON/NPI

Enable to overwrite Type of Number and Numbering Plan Identification of dialed destination number before the call is routed to the selected outbound trunk. This option is applied only on trunk with ISDN signaling.

Strip digits from Caller ID, and Prepend these digits to Caller ID

These parameters allow modifying caller identification number before the call is placed on the outbound trunk. You are allowed to strip specified number of digits from the front of the caller identification number and you can enter prefix string which will be prepended to this number.

Presentation

This option allows modifying of caller identification presentation before the call is sent to the outbound trunk.

Change TON/NPI of Caller ID

Enable to overwrite Type of Number and Numbering Plan Identification of caller identification number before the call is placed on the selected outbound trunk. This option is applied only on trunk with ISDN signaling.

Use Fail-Over trunk 1, 2, 3

This section allows to define alternative routing of the call if primary destination is busy or down. It is possible to define maximally 3 fail-over alternatives. Each fail-over destination has same options as we define for primary call destination.

Dial Plans

Main screen for dial plans configuration shows list of existing dial plans. It is divided into two tables

- Users
- Trunks

Users' dial plan can be assigned to the user extensions and trunks' dial plan can be assigned to the trunk interfaces.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > Dial Plans

Dial Plans Settings

Dialplan is a collection of Calling rules, which defines dialing string analyze and call routing rules.
Dialplan are assigned to users and trunk to handle incoming calls from these interfaces.

Users

DialPlan: Users	Calling Rules	New DialPlan Name	Create
from_users	internal, e1, sip, services		Edit Delete

Trunks

DialPlan: Trunks	Calling Rules	New DialPlan Name	Create
from_e1	users, out		Edit Delete
from_gsm	users		Edit Delete
from_sip	out, users		Edit Delete
from_fxo	out, users		Edit Delete

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

You can create new empty dial plan when you enter new unique label into the field **New Dial Plan Name** of appropriate table and click on the button **Create**. This name is used to identify the dial plan over all of Voice&Data Router configuration. Use the **Edit** button to modify setting of selected dial plan. And use the **Delete** button to remove dial plan from the configuration. Dial plan can be removed only if it is not assigned to any user or trunk.

Users' Dial Plan

Users' dial plan consists of User to User and User to Trunk calling rules and it defines call routing from the user extensions. You can select existing calling rules group in the field **Add Calling Rule** and click on the **Add** button to add calling rules to the dial plan. Only calling rules applicable for users' dial plan are offered for adding. Use the **Delete** button if you want to remove calling rules from the dial plan.

Please note, that the order of calling rules is important for correct functionality of call routing. Same order is used to match dialed number to the calling rule pattern. It is important to have general calling rules (patterns like _X.) at the end of the calling rules. You can control the order of the calling rules using arrows in the first column of the table.

Options

Use Services Codes

Enable this option if you want to include users' service codes into this dial plan. Service codes define dial codes that can be used for controlling services (e.g. activation and deactivation) from user's phone. See [Services Codes](#) menu for details.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > Dial Plans

Edit DialPlan from_users

Calling Rules		Add Calling Rule	internal	Add
↓	internal			Delete
↑ ↓	e1			Delete
↑	sip			Delete

Options

☒ Use Services Codes

☐ Ignore Pattern

Back

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Ignore Pattern

This option tells Voice&Data Router to continue to provide a dial tone on an analogue line, even after the caller has dialed the indicated pattern. This will not work with SIP phones, as they usually do not send digits to the system as they are input but they are sent to Voice&Data Router all at once.

Trunks' Dial Plan

Trunks' dial plan consists of Trunk to User and Trunk to Trunk calling rules and it defines call routing from the trunk interfaces. You can select existing calling rules group in the field **Add Calling Rule** and click on the **Add** button to add these calling rules to the dial plan. Only calling rules applicable for trunks' dial plan are offered for adding. Click on the **Delete** button if you want to remove calling rules from the dial plan.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > Dial Plans

Edit DialPlan from_e1

Calling Rules		Add Calling Rule	users	Add
↓	users			Delete
↑	out			Delete

Back

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

As for calling rules order the same regulations are valid as for users' dial plan. Searching for the valid calling rule which match to the incoming dialed number is executed in the same order as the calling rules are configured in the dial plan. It is important to have general calling rules (patterns like _X.) at the end of the calling rules. You are allowed to control the order of the calling rules using arrows in the first column of the table.

AOC Tables Settings

One of useful feature of Voice&Data Router is generation of charging information on E1/T1 lines. E1/T1 trunks with ISDN signaling use AOC supplementary service (AOC-D and AOC-E) and the trunks with CAS signaling uses billing pulses to generate charging information. Different parameters of call charging can be used for working days, weekend eventually for public holidays.

AOC tables setting consist of

- AOC tables
- Time tables
- Holidays definition

AOC tables assign charging rules to call prefixes. AOC table is assigned to E1/T1 trunk with enabled charging generation (see [E1/T1 Trunks](#)). Each trunk can use different AOC table than means different charging rules.

Charging rules are defined in time tables and existing time table can be assigned to the call prefix in AOC table. AOC table should define all prefix numbers you want to generate charging information for.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > AOC Tables Settings

AOC Tables Settings AOC Tables Time Tables Holidays

AOC Tables

Name
default

Create New Table Create

Edit Details Delete Table

[Download AOC File](#)
Right Click on the above link and download using the 'Save Link As..' option

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

To create new AOC table enter new table name in the **Create New Table** field and click on the **Create** button. To edit existing AOC table use **Edit Details** button and to remove AOC table use **Delete Table** button.

AOC table details screen shows list of defined prefixes and associated timetables. To add new item to the AOC table enter call prefix into the **Prefix** field, choose time table to use and click on the **Add** button. The **Edit** button allows you to change time table assignment for existing prefix number. The **Remove** button can be used to delete selected item from the AOC table.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router

inoteska

Home Users Trunks Traffic **Globals** System Diagnostics Specials

Traffic > AOC Tables Settings

AOC Table: default

Prefix Time Table table1 Add Edit Remove

00301	table4
00302	table4
00305	table4
003060	table4
003061	table4
003062	table4
003063	table4
003064	table4
003065	table4
003066	table4
003067	table4
003068	table4
0030691	table4
0030692	table4
0030696	table4
00307	table4
00308	table4
00309	table4
0031	table4
0032	table4
0033	table4
00330	table4
00331	table4
00332	table4
00333	table4

Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Time tables define charging rules – frequency and number of charging units. Time table can divide the day into zones with different charging rules. Each time table defines charging rules separately for working day, weekend and public holiday. Charging rules allow setting of three time intervals for each call with different parameters.

GUI-version : 1.2 / Board Type : 1 **Voce&Data Router Reloaded !!** Logout

voice&data router

inoteska

Home Users Trunks Traffic **Globals** System Diagnostics Specials

Traffic > AOC Tables Settings

AOC Tables Settings AOC Tables Time Tables Holidays

Time Tables

Name	Create New Table	Create
table1	Edit Details	Delete Table
table2	Edit Details	Delete Table

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

To create new time table enter new name in the **Create New Table** field and click on the **Create** button. To edit existing time table use the **Edit Details** button and to remove time table use the **Delete Table** button. Time table can be removed only if it is not assigned to any prefix in the AOC tables.

Time table details show charging rules for

- Working day
- Weekend
- Holiday

You can use the **Create** button to define new day time zone and the **Edit Details** button to change charging parameters of existing time zone. The **Remove** button can be used to delete selected time zone.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > AOC Tables Settings

Time Tables: table9

Working Day									Create New Item	Create
START	LT11	CHI1	CHU1	LT12	CHI2	CHU2	CHI3	CHU3		
00:00	60		50				6	5	Edit Details	Remove
07:00	60		100				3	5	Edit Details	Remove
18:00	60		50				6	5	Edit Details	Remove

Weekend									Create New Item	Create
START	LT11	CHI1	CHU1	LT12	CHI2	CHU2	CHI3	CHU3		
00:00	60		50				6	5	Edit Details	Remove

Holiday									Create New Item	Create
START	LT11	CHI1	CHU1	LT12	CHI2	CHU2	CHI3	CHU3		
00:00									Edit Details	Remove

Holiday Table --- v Set

Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Charging parameters:

- **START** Beginning of day charging zone
- **LT11** Length of the first time interval of the call
- **CHI1** Charging interval during the first time interval
- **CHU1** Number of charging units for the first time interval
- **LT12** Length of the second time interval of the call
- **CHI2** Charging interval during the second time interval
- **CHU2** Number of charging units for the second time interval
- **CHI3** Charging interval during the third time interval
- **CHU3** Number of charging units for the third time interval

START defines beginning of day charging zone. It can be set in one hour step. The first zone must start at 0:00 and the last zone automatically ends at 23:59.

LT11, **CHI1** and **CHU1** define charging generation for the first time interval of the call. LT11 is length of the interval in seconds. CHI1 designates charging rate during this period. It is configured in seconds with precision on tenths of the second (you can use decimal numbers like 1.5). CHU1 specifies number of charging units to generate.

LT12, **CHI2** and **CHU2** define charging generation for the second time interval of the call.

CHI3 and **CHU3** define charging generation for the rest of the call up to the call end.

It is not necessary to set all parameters and they can be unset (zero).

- If all parameters are not set then no charging is generated (call is free of charge)
- If time interval length is not set then charging interval is ignored.
- If time interval length is not set and no charging units are defined then time interval is skipped and it continues with next one.
- If time interval length is not set and charging units exist then specified charging units are generated once and it continues with next time interval.
- If charging units are not set then no charging is generated for this time interval.

- If charging interval is not set then charging units are generated only once for this time interval.

Example 1

START	LT11	CHI1	CHU1	LT12	CHI2	CHU2	CHI3	CHU3
0:00	0	0	0	0	0	0	10	1

This setting will generate regularly 1 charging unit every 10 seconds during the whole call. It does not matter what time you call.

Example 2

START	LT11	CHI1	CHU1	LT12	CHI2	CHU2	CHI3	CHU3
0:00	0	0	1	60	1	1	10	1
7:00	0	0	5	60	1	2	2	1
19:00	0	0	1	60	1	1	10	1

This setting is more complex. Within hours 7:00 – 19:00 you will get 5 charging units immediately after call answer then 2 charging units per second during the first minute of the call and 1 charging unit every 2 seconds during the rest of the call. At the time 19:00 – 7:00 you will get 1 charging unit after the call answer and 1 charging unit every second during the first minute of the call. And then it will continue with 1 charging unit every 10 seconds up to the end of the call.

Charging rules for holidays are needed only if some holiday table is assigned to the current time table.

Holidays section defines public holidays. Each holiday is defined as a date (day and month). Holiday table can be assigned to the time table to apply special charging rules for these days.

To create new holiday table enter new name in the **Create New Table** field and click on the **Create** button. To edit existing holiday table use the **Edit Details** button and to remove holiday table use the **Delete Table** button.

Holidays table details show list of public holidays. Use the **Add** and **Remove** buttons to edit the holiday table.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Traffic > AOC Tables Settings

Holidays: holidays

Date (Day/Month)

1

1

Add

Holidays

1.1.

6.1.

6.4.

9.4.

1.5.

8.5.

5.7.

29.8.

1.9.

15.9.

Remove

Save

Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Note that correct functionality of generation of charging information depends on setting of Voice&Data Router system time. See [Date and Time](#) setting for more details about system time adjustment.

GLOBALS MENU

SIP settings

SIP settings define common options of SIP protocol valid for all SIP users and SIP trunks. SIP protocol options are divided into the following groups:

- General Preferences
- TOS
- NAT
- Miscellaneous
- Registrations
- Authentications
- Jitter Buffer
- Codecs

General Preferences

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic **Globals** System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

General Preferences TOS NAT Miscellaneous Registrations Authentications Jitter Buffer

Realm for Digest Authentication

UDP Port to Bind to

IP Address to Bind to

Domain

Overlap Dialling Support ☒

Allow Transfers ☒

Enable DNS SRV Lookups (on Outbound Calls) ☒

Pedantic ☐

Always Auth Reject ☒

SIP Domain Support

Auto Domain ☐

Allow External Domains ☒

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Realm for Digest Authentication

Realm for digest authentication. Realms must be globally unique according to RFC 3261. You can set realm to your host name or domain name.

UDP Port to Bind to

UDP port that Voice&Data Router will listen on (SIP standard port is 5060).

IP Address to Bind to

IP address that Voice&Data Router will listen on. The address 0.0.0.0 tells device to listen on all interfaces. Use LAN or WAN IP address to limit SIP connections only for selected interface.

Domain

Default domain setting. If configured, Voice&Data Router will allow INVITE and REFER messages only to defined domains. REGISTER to non-local domains will be automatically denied if a domain list is configured.

Overlap Dialing Support

Enable/disable overlap dialing support.

Allow Transfers

Enable/disable call transfers.

Enable DNS SRV Lookups (on Outbound Calls)

Enable DNS SRV lookups on outbound calls. Voice&Data Router only uses the first host in SRV records. Disabling DNS SRV lookups disables the ability to place SIP calls based on domain names to some other SIP users on the Internet.

Pedantic

Enable slow, pedantic checking of Call-IDs, multiline SIP headers and URI-encoded headers. This option enables more strict SIP RFC compliancy.

Always Auth Reject

When an incoming INVITE or REGISTER is to be rejected, for any reason, always reject with an identical response (401 Unauthorized) instead of letting the requester know whether there was a matching SIP account username for their request. This reduces the ability of an attacker to scan for valid SIP usernames.

Auto Domain

Enable automatic adding of local host name and local IP to domain list.

Allow External Domains

Enable/disable INVITE and REFER to non-local domains.

TOS

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

General Preferences **TOS** NAT Miscellaneous Registrations Authentications Jitter Buffer

TOS for Signalling Packets	CS3	TOS for RTP Audio Packets	ef
Trust Remote Party ID	<input checked="" type="checkbox"/>	Send Remote Party ID	<input checked="" type="checkbox"/>
Generate In-Band Ringing	never	Server User Agent	Inoteska Voice&Data R
Allow Nonlocal Redirect	<input type="checkbox"/>	Add 'user=phone' to URI	<input type="checkbox"/>
DTMF Mode	rfc2833	Send Compact SIP Headers	<input type="checkbox"/>
Max Registration/Subscription Time	3600		
Min Registration/Subscription Time	60		
Default Incoming/Outgoing Registration Time	1800		
Min Roundtrip Time (T1 Time)	100		

Save Cancel

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

TOS for Signaling Packets

TOS (Type of Service) for outgoing SIP signaling packets.

TOS for RTP Audio Packets

TOS (Type of Service) for outgoing RTP packets.

Trust Remote Party ID

This option specifies whether or not Voice&Data Router should trust the value in the Remote-Party-ID header.

Send Remote Party ID

This parameter specifies whether or not Voice&Data Router should send a Remote-Party-ID header.

Generate In-Band Ringing

Configuration of in-band ringing generation.

- **yes** – always send 180 Ringing (if it hasn't been sent yet) followed by 183 Session Progress and in-band audio tones.
- **no** – send 180 Ringing if 183 has not yet been sent establishing audio path. If audio path is established already (with 183) then send in-band ringing.
- **never** - Whenever ringing occurs, send 180 Ringing as long as 200 OK has not yet been sent.

Server User Agent

Customizing User-Agent field in the SIP messages.

Allow Nonlocal Redirect

Enable support for 302 Redirects.

Add 'user=phone' to URI

This option tells Voice&Data Router to add “;user=phone” to SIP URIs that contain a valid phone number.

DTMF Mode

Set default mode for sending DTMF digits.

Send Compact SIP Headers

Enable compact format of the SIP headers, which may be required if the size of the SIP header is larger than the maximum transmission unit (MTU), causing the IP packet to be fragmented. Do not use this option unless you know what you are doing

Max Registration/Subscription Time

Maximum allowed time of incoming registrations and subscriptions (in seconds).

Min Registration/Subscription Time

Minimum allowed time of incoming registrations and subscriptions (in seconds).

Default Incoming/Outgoing Registration Time

Default expiration time of SIP registration for incoming and outgoing registrations (in seconds). For incoming registration default value you set here is used only if the client does not specify a timeout when it registers. If you are registering to another user agent server (UAS), this is the registration timeout that it will send to the far end.

Min Roundtrip Time (T1 Time)

Minimum round-trip time for messages to monitored hosts (in milliseconds).

NAT**Extern IP**

IP address that will replace the private IP address in outbound SIP messages if Voice&Data Router is behind a NAT.

Extern Host

Fully qualified domain name to determine extern IP address. Voice&Data Router performs periodic DNS lookups on this name and replaces the private IP address with the IP address returned from the DNS lookup in case it is behind the NAT.

Extern Refresh

Time period of regular DNS lookups on the extern host (in seconds).

Local Network Address

This is used to tell Voice&Data Router which IP addresses are considered local, so that the address in the SIP header can be translated to that specified by extern IP or extern host. The IP addresses should be specified in CIDR notation (e.g. 192.168.1.0/24).

NAT Mode

Select default behavior when Voice&Data is on a public IP and communicating with devices hidden behind a NAT.

- **yes** – always ignore info and assume NAT
- **Server User Agent** – use NAT mode only according to RFC3581 (:rport)
- **never** – never attempt NAT mode or RFC3581 support
- **route** – assume NAT, don't send rport

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router

inoteska

Home Users Trunks Traffic Globals System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

General Preferences TOS **NAT** Miscellaneous Registrations Authentications Jitter Buffer

Extern IP

Extern Host

Extern Refresh

Local Network Address

NAT Mode

Allow RTP Reinvite

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Allow RTP Reinvite

Configure default media path redirection.

- **yes** – allow direct RTP media stream
- **nonat** – allow direct RTP media stream but only when the peer where the media is being sent is known to not be behind a NAT
- **update** – use UPDATE instead of INVITE

Miscellaneous

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router

inoteska

Home Users Trunks Traffic Globals System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

General Preferences TOS NAT **Miscellaneous** Registrations Authentications Jitter Buffer

Generate Manager Events ☐

Outbound SIP Registrations

Register Timeout

Register Attempts

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Generate Manager Events

Enable/disable generation of Asterisk Manager events.

Register Timeout

Time interval to retry unsuccessful outbound registration calls (in seconds).

Register Attempts

Number of outbound registration attempts before giving up. Setting to 0 means that Voice&Data Router will retry indefinitely.



Enable Jitter Buffer

Enable/disable the use of an RTP jitter buffer on the receiving side of a SIP channel.

Registrations

These global outbound SIP registrations can be useful for instances when Voice&Data Router needs to register multiple users/extensions to a single SIP proxy (provider).

GUI-version : 1.8 / Board Type : 1 Logout

[Home](#) | [Users](#) | [Trunks](#) | [Traffic](#) | [Globals](#) | [System](#) | [Diagnostics](#)

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

[General Preferences](#) | [TOS](#) | [Debug Notify](#) | [NAT](#) | [Miscellaneous](#) | **[Registrations](#)** | [Authentications](#) | [Jitter Buffer](#) | [Codecs](#)

Outbound SIP registrations can be useful for instances when Voice&Data Router needs to register multiple users/extensions to a single SIP proxy (provider).



Username	Host	
0445567755	sip.vvn.telekom.sk:5060	Add Edit Delete
0445567758	sip.vvn.telekom.sk:5060	Edit Delete

[Save](#) [Cancel](#)

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Click on **Add** button to create new outbound SIP registration. Use the **Edit** button to modify selected SIP registration. And use the **Delete** button to remove outbound SIP registration from the configuration.

GUI-version : 1.8 / Board Type : 1 Logout

[Home](#) | [Users](#) | [Trunks](#) | [Traffic](#) | [Globals](#) | [System](#) | [Diagnostics](#)

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

Outbound SIP Registration

Username

?

Host

:

?

AuthUser

?

Password

?

[Save](#) [Cancel](#)

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Username

Registration user name.

Host

SIP registrar server address (IP address or host name)

AuthUser

User name used for the authentication. Use this setting only if it differs from the registration user name above.

Password

Password used for the authentication.

Authentications

Global credentials for outbound calls can be used when a proxy challenges Voice&Data Router for authentication. These credentials override any credentials in user/trunk definition if realm is matched. This way, Voice&Data Router can authenticate for outbound calls to other realms.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

General Preferences TOS Debug Notify NAT Miscellaneous Registrations **Authentications** Jitter Buffer Codecs

Global credentials for outbound calls, i.e. when a proxy challenges Voice&Data Router for authentication. These credentials override any credentials in user/trunk definition if realm is matched. This way, Voice&Data Router can authenticate for outbound calls to other realms.

Realm	Username		
KUCAPACA	5567755	Edit	Delete
KUCAPACA	5567758	Edit	Delete
KUCAPACA	5567759	Edit	Delete

Add

Save Cancel

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Click on **Add** button to create new global authentication. Use the **Edit** button to modify selected global authentication. And use the **Delete** button to remove global authentication from the configuration.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

Global Authentication

Realm

Username

Password

Save Cancel

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Realm

Authentication realm. If it is matched to realm in proxy challenge, these authentication credentials override any credentials in user/trunk definition.

Username

Authentication user name for specified realm.

Password

Authentication password for specified realm.

Jitter Buffer
Force Jitter Buffer

Force the use of the RTP jitter buffer on the receiving side of a SIP channel.

Max Jitter Buffer

Maximum length of the jitter buffer (in milliseconds).

Resync Threshold

Jump in the frame timestamps over which the jitter buffer is resynchronized. It is useful to improve the quality of the voice, with big jumps in/broken timestamps (in milliseconds).

Implementation

Jitter buffer implementation, used on the receiving side of a SIP channel. Two implementations are currently available

- **fixed** – jitter buffer has fixed size that equals to maximum defined length
- **adaptive** – jitter buffer size varies up to the maximum defined length

Codecs

Global codecs setting.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router **inoteska**

Home Users Trunks Traffic Globals System Diagnostics

Globals > SIP Settings

SIP (Session Initiation Protocol) Configuration Settings

General Preferences TOS Debug Notify NAT Miscellaneous Registrations Authentications Jitter Buffer **Codecs**

Allowed Codecs

☒ u-law ☒ a-law ☒ GSM ☒ G.729 ☒ G.723 ☒ G.726 ☐ ILBC

Save Cancel

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

RTP/UDPTL Settings

RTP and UDPTL protocol configuration. Here you can define port range allocated for voice (RTP) and T.38 fax (UDPTL) transmission.

The screenshot shows the web interface of a voice&data router. At the top, there is a header bar with 'GUI-version : 1.1 / Board Type : 1' on the left and a 'Logout' link on the right. Below this is a large banner with the 'voice&data router' logo and the 'inoteska' logo on the right. A navigation menu is located below the banner, with tabs for 'Home', 'Users', 'Trunks', 'Traffic', 'Globals', 'System', 'Diagnostics', and 'Specials'. The 'Globals' tab is selected, and the breadcrumb trail shows 'Globals > RTP/UDPTL Settings'. The main content area is titled 'RTP/UDPTL Settings' and contains a section 'RTP/UDPTL Port Range'. This section has two input fields: 'Start port' with a value of '8000' and 'End port' with a value of '8099'. Each field has a small question mark icon to its left. Below these fields is a 'Save' button. At the bottom of the page, a footer bar contains the text 'Copyright © 2010-2012, All Rights Reserved www.inoteska.sk'.

Start Port

First port number reserved for RTP/UDPTL protocol.

End Port

Last port number reserved for RTP/UDPTL protocol.

Note that only odd port numbers (half of the allocated range) can be used for RTP or UDPTL stream. Odd port numbers are reserved for RTCP protocol.

Call Groups

Call groups can group together outgoing trunks. Call group joins multiple TDM trunks (E1/T1, analogue and GSM) to a single group for outgoing calls (grouping of VoIP trunks is not supported). Such group can be used in the calling rules as the call destination (user to trunk or trunk to trunk). Outgoing call is placed on the first idle channel which is found according method defined in call group configuration.

Call groups have predefined channel order that is fixed. Channel order is determined by arrangement of Voice&Data Router internal TDM bus.

Internal numbering of TDM channels

Channel	Interfaces
0 - 127	E1/T1 – 4 x 32 channels
128 - 143	GSM – 16 channels (only 12 can be used)
144 - 175	Analogue – 32 channels
176 - 223	BRI – 16 x 3 channels

The screenshot shows the Voice&Data Router web interface. At the top, it says 'GUI-version : 1.1 / Board Type : 1' and 'Logout'. The main header features the 'voice&data router' logo and the 'inoteska' brand name. A navigation bar includes links for Home, Users, Trunks, Traffic, Globals, System, Diagnostics, and Specials. The breadcrumb trail indicates 'Globals > Call Groups List'. The main content area is titled 'Call Groups Settings' and includes a 'New Call Group' button. Below this is a 'Call Groups List' table with three entries: E1, FXO, and GSM. Each entry shows the interfaces it includes and has 'Edit' and 'Delete' buttons. The footer contains the copyright notice: 'Copyright © 2010-2012, All Rights Reserved www.inoteska.sk'.

Call Group Name	Interfaces	Edit	Delete
E1	E1: E1-A, E1: E1-B		
FXO	FXO: FXO1, FXO: FXO2, FXO: FXO3		
GSM	GSM: GSM1 Orange, GSM: GSM2 T-Mobile, GSM: GSM3 O2		

To create new call group click on the **New Call Group** button. Use the **Edit** button if you want to modify existing call group. And use the **Delete** button to remove call group from the configuration. Call group can be removed only if there does not exist any reference to this group in the calling rules.

Call Group Name

A unique label to help you identify call group. This identifier is used over all of Voice&Data Router configuration where we need reference to this call group.

Call Group Members

List of call group members. Use arrow buttons to add group members from available trunks' list or to remove them from the call group.

Available Trunks

List of available TDM trunks, which can be added to the call group.

Channel Selection

Idle channel selection to place outgoing call.

- Ascending – search for the lowest available channel number
- Descending – search for the highest available channel number

Note that internal fixed channel order is always used for the channel searching, does not matter what is displayed in call group members' list.

Cyclic

Enable cyclic search of the first available channel instead of sequential.

GUI-version : 1.1 / Board Type : <https://ib.sisp.sk> Logout

voice&data router

inoteska

HomeUsersTrunksTrafficGlobalsSystemDiagnosticsSpecials

Globals > Call Groups List

Edit Call Group: GSM

Call Group name

Call Group Members

GSM: GSM1 Orange

GSM: GSM2 T-Mobile

GSM: GSM3 O2

Available Trunks

FXO: FX01

FXO: FX02

FXO: FX03

FXO: FX04

FXO: FX05

FXO: FX06

FXO: FX07

FXO: FX08

E1: E1-A

E1: E1-B

<<

←

→

>>

Call Group options

Channel Selection

Ascending

☒ Cyclic

Save

Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Ring Groups

Ring groups join user extensions to the single group that can ring a group of phones simultaneously, stopping when any one of them is picked up. Such group can be used in the calling rules as the call destination (user to user or trunk to user).

Create new ring group by clicking on the **New Ring Group** button. Use the **Edit** button if you want to modify existing ring group. And use the **Delete** button to remove selected ring group from the configuration. Ring group can be removed only if there does not exist any reference to this group in the calling rules.

GUI-version : 1.1 / Board Type : 1 Voice&Data Router Reloaded !! Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Ring Groups

Ring Groups Settings New Ring Group

Ring Group List

Ring Group List	Members		
GROUP1	10, 11, 12	Edit	Delete
GROUP2	20, 21, 22, 23	Edit	Delete

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Ring Group Name

A unique label to help you identify ring group. This identifier is used over all of Voice&Data Router configuration where we need reference to this ring group.

Ring Group Members

List of ring group members. Use arrow buttons to add group members from available users' list or to remove them from the ring group.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Ring Groups

Edit Ring Group - GROUP1

Ring Group Name:

Ring Group Members

- 10 (SIP) Jack Daniel's
- 11 (SIP) Johnnie Walker
- 12 (SIP) Jim Beam

Available Users

- 20 (Analog) Doug Coombs
- 21 (Analog) Hugo Harrison
- 22 (Analog) Seth Morrison
- 23 (Analog) Shane McConkey
- 24 (Analog) Glen Plake
- 25 (Analog) Kaj Zacrisson
- 26 (Analog) Mike Hattrup
- 27 (Analog) Chris Davenport

Ring Group Options

Strategy:

Seconds to ring each member:

If not answered Goto:

Save Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Available Users

List of available user extensions, which can be added to the ring group.

Strategy

Define what ringing strategy is used

- Ring All Simultaneously – all phones are ringing at once
- Ring in Order – ring group phones are ringing step by step

Seconds to Ring Each Member

Enter time how long to ring phones in the ring group.

If Not Answered Goto

Define what to do when nobody answers.

- Hangup – call will be refused (with busy tone)
- Congestion – call will be refused (with congestion tone)

Carriers

Alternative carriers supporting two-stage dial service can be used to lower communication costs. Two-stage dialing allows you to dial carrier access number first (this is usually low-tariff number). And then after call answer, DTMF tones are used to authenticate and dial destination number. Two step calls over alternative carrier can be enabled in the calling rules (user to trunk or trunk to trunk) and Voice&Data Router makes such calls automatically so it appears like ordinary call.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Carriers

Carriers Settings Create New

List of Carriers

Name	Carrier Prefix	Ringing Tone
MOJ_OPERATOR	012004	Generate

Edit Delete

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

To create new carrier, click on the **Create** New button. Use the **Edit** button to modify existing carrier configuration. And use the **Delete** button to remove selected carrier from the configuration. Carrier can be removed only if does not exist any reference to this carrier in the calling rules.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Carriers

Carrier's Options - MOJ_OPERATOR

Details

Name

Carrier Prefix

Security Code

Ringing Tone ☒

Save Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Name

A unique label to help you identify carrier. This identifier is used over all of Voice&Data Router configuration where we need reference to this carrier.

Carrier Prefix

Carrier access number.

Security Code

Customer PIN code to authenticate.

Ringing Tone

Enable false ringing tone generation immediately when call started. Use this feature to prevent long period of silence during connection set-up.

Permissions

Permissions are used to limit outgoing communication of local users. Every user extension has assigned permission group. Permission group is a collection of permission flags which can be assigned to the calling rules (user to user or user to trunk). User is allowed to make a call only if his permission group includes call permission flag assigned to calling rule for dialed number. If there is no permission flag assigned to the calling rule, permissions are not tested and all users are allowed to proceed.

GUI-version : 1.1 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Permissions

Permission Settings
Save Changes Cancel Changes

User permission group defines a collection of call permission flags (1 to 16). User permission groups are assigned to the users. Call permission flags are assigned to the user calling rules (User to User or User to Trunk).
User is allowed to make a call only if his permission group includes call permission flag assigned to calling rule for this call.

User Permission Groups

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	Permission Group
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Without limitation
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Only internal calls
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sk
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Sk+Cz
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	International
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Only incoming calls
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Call Permission Flags

Permission Flag	Flag Name
1	Internal
2	Local
3	Toll
4	CZ
5	International
6	Mobile
7	flag 7
8	flag 8
9	flag 9
10	flag 10
11	flag 11
12	flag 12
13	flag 13
14	flag 14
15	flag 15
16	flag 16

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

User Permission Group

This table defines permission groups which are assigned to the user extensions. Voice&Data Router supports 12 permission groups. Permission group is a set of 16 call permission flags. You can use

check boxes to select call permission flags for each group. Every group can have symbolic name to easier understanding.

User permission group with all call permission flags checked is the most privileged group. There are no restrictions for the user with such group because all permission flags are allowed.

On the other hand user permission group that does not have selected any call permission flag can be limited only for incoming calls. In that case all outgoing calls matching the calling rules with assigned call permission flag will be refused. Only calling rules which don't use call permission flags are allowed for such user.

Call Permission Flags

This table defines call permission flags. There are 16 permission flags and you can assign each of them symbolic name for better orientation. These identifiers are used in calling rules configuration where call permission flags are associated to dialed number patterns.

Services Codes

Users' service codes configuration. Here you can define dial codes for activation, deactivation or execution of users' services form the phone. Note that the user is allowed to use configured service codes only if his dial plan includes service codes (see [dial plan](#) configuration).

GUI-version : 1.1 / Board Type : 1 Voice&Data Router Reloaded !! Logout

voice&data router

inoteska

Home
Users
Trunks
Traffic
Globals
System
Diagnostics
Specials

Globals > Services Codes

Services Codes Settings

Set Call Forwarding
Set Call Forwarding if user is busy
Set Call Forwarding if no respond No respond time:

Clear Call Forwarding
Clear Call Forwarding if user is busy
Clear Call Forwarding if no respond

Set Do Not Disturb
Clear Do Not Disturb

Call Pickup

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Default service codes setting

Service	Activation	Deactivation	Execution
Call forwarding (unconditional)	*21*	*21#	
Call forwarding if busy	*22*	*22#	
Call forwarding if not answered	*23*	*23#	
Do not disturb	*78	*79	
Call pickup			*8

CDR Settings

CDR – Call Detail Records – save information about Voice&Data Router calls. CDR records are stored in the text file as comma separated values.

CDR Note

Here, you can enter optional string that will be added to every CDR.

CDR User to User

Enable to log CDR for local calls between Voice&Data Router users.

CDR Trunk to User

Enable to log CDR for Voice&Data Router incoming calls.

CDR User to Trunk

Enable to log CDR for Voice&Data Router outgoing calls. This option also enables transit calls CDR – trunk to trunk.

You can click on the **CDR Records** button to view stored CDR records. Use the **Refresh View** button to update displayed list CDRs or click on the **Delete File** to clear stored CDR records.

CDR record fields:

- CDR note – string you configured in CDR Details
- Source number – caller identification number
- Destination number – dialed number
- Source channel – incoming channel internal name
- Destination channel – outgoing channel internal name
- Date/Time – call timestamp
- Duration – total time in system, in seconds
- Billing time – total time call is up, in seconds
- Disposition – what happened to the call (ANSWERED, NO ANSWER, BUSY, FAILED)
- Call type – call type from routing point of view (LOCAL, IN, OUT)

GUI-version : 1.1 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > CDR Settings

CDR Settings

CDR Details CDR Records

CDR Records

Refresh View Delete File

TEST,10,22,SIP/10-00000004,UniCall/146-ANA18589397,2012-05-14 15:37:38,6,4,ANSWERED,LOCAL

TEST,10,0104155,SIP/10-00000005,UniCall/1-E142fb0a00,2012-05-14 15:37:50,6,5,ANSWERED,OUT

TEST,10,0104155,SIP/10-00000006,UniCall/1-E1578829ef,2012-05-15 08:03:00,32,0,NO ANSWER,OUT

TEST,10,0104155,SIP/10-00000007,UniCall/1-E15e53bb3f,2012-05-15 08:03:53,29,0,NO ANSWER,OUT

TEST,,010,UniCall/1-E119143216,UniCall/2-E1412c7a0a,2012-05-15 08:13:34,6,0,NO ANSWER,OUT

TEST,,012,UniCall/1-E139fe8b61,UniCall/2-E1053c77c4,2012-05-15 08:13:47,2,0,NO ANSWER,OUT

TEST,,012004,UniCall/1-E14f6c15eb,UniCall/2-E16b05a1ff,2012-05-15 08:13:57,1,0,FAILED,OUT

TEST,,012000,UniCall/1-E125fc1d01,UniCall/2-E17af07032,2012-05-15 08:14:07,0,0,FAILED,OUT

TEST,,010003,UniCall/1-E162b55c8a,UniCall/2-E10d2149a0,2012-05-15 08:14:13,12,6,ANSWERED,OUT

TEST,,s,UniCall/1-E1617063d1,UniCall/147-ANA7578bebc,2012-05-15 08:20:52,20,0,NO ANSWER,IN

TEST,,s,UniCall/1-E17dfd4416,UniCall/146-ANA6fb96760,2012-05-15 08:21:23,29,26,ANSWERED,IN

[Download CDR File](#)
Right Click on the above link and download using the 'Save Link As..' option

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

You can use link **Download CDR File** to download CDR file from Voice&Data Router for additional processing.

Announcement Settings

Announcement management is used for configuration of announcement files for call routing. New announcement file can be recorded from user phone or existing file can be uploaded. Only files of supported format can be uploaded. Voice&Data Router uses Microsoft WAVE files with following format

Sample rate 8 kHz
 Sample size 16 bit
 Channels 1 (mono)
 Auto format PCM

Sample rate 8 kHz
 Sample size 8 bit
 Channels 1 (mono)
 Audio format CCITT A-Law
 CCITT μ -Law

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Announcement Settings

Announcement Settings Settings Upload File Record File Play Sound

Announcement Files

#	Announcement File Name		
1	tada.wav	Download File	Delete File
2	test.wav	Download File	Delete File

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

To download announcement file from Voice&Data Router click on the **Download File** button for selected announcement. Download link appears to save file on your local PC. To remove announcement file from Voice&Data Router use the **Delete File** button. File removal is allowed only if there does not exist any reference to this announcement in the calling rules.

Use the **Upload File** button to switch to announcement upload form. You can select WAV file to upload and click on **Upload** button. Only files of supported format be used – see description above.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Announcement Settings

Announcement Settings Settings Upload File Record File Play Sound

Upload Announcement File

Upload

tada.wav

- tada.wav (audio/wav) - 31128 bytes

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Use the **Record File** button to switch to announcement recording form. Voice&Data Router allows you to record your voice message file from your phone. You need to select one user extension, enter new announcement name and click on the **Start** button. Voice&Data Router rings selected user extension. Pick up the phone, wait for beep sound and then say your new voice message. When you finish press # key on your phone or hang-up.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Announcement Settings

Settings Upload File Record File Play Sound

Record New Announcement File

Select a user and enter new name of the audio file without an extension (such as.: welcome_message).
After pressing "Start" button selected user is ringing.
Pick up the phone. Wait for the sound tone and then say new voice message.
Confirm the end of message by pressing "#" at the phone.

Record File

Extension SIP: 10 Announcement File Name test

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Use the **Play Sound** button to test announcement files. Voice&Data Router can play back selected announcement to your phone. In this way you can test ability to play uploaded files or recording voice quality. Select one user extension, select announcement file and click on the **Start** button. Voice&Data Router rings selected user extension and after phone pick-up it plays back selected voice file.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > Announcement Settings

Settings Upload File Record File Play Sound

Play Announcement File

Select a user and the name of sound file.
After pressing "Start" button selected user is ringing.
Pick up the phone and the sound file is played.

Play Sound

Extension SIP: 10 Announcement File tada.wav

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

CAS National Variants

There are various country-specific variants of E1 CAS signaling protocol. Voice&Data Router offers set of configurable parameters to adapt CAS signaling to specific requirements of each installation. Device is supplied with several predefined variants of CAS signaling you can use and you are allowed to customize these predefined variants for your needs or to create your own variant. Modified CAS signaling variant can be then assigned to E1 port in [E1/T1 Trunks](#) configuration.

To modify existing CAS signaling variant choose one variant from the selection list and click on **Edit Existing** button. To create new CAS signaling variant enter name of the variant and click on the **Create New** button.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > CAS National Variants

CAS National Variants Settings

default Edit Existing

Create New

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

CAS signaling variant configuration parameters is divided into five basic categories.

- Line Signals
- MFC/R2 Forward Signals
- MFC/R2 Backward Signals
- Options
- Timers

Line Signals define CAS line signaling. Line signaling supports 4 signaling bits (ABCD) in each direction. Only 2 of them (AB) are used and can be configured. Unused bits (CD) have fixed status (01) and they don't change. Signaling bits are transmitted over 16th signaling channel. Here you can configure AB signaling bits for particular line signals/states.

Common Signals

Line signals for both forward and backward direction.

Idle

Line idle/release signal.

Blocking

Line blocking signal, calls are not allowed.

Forward Signals

Line signals for forward direction (signals sent by the originating point).

Seizure

Line seizure signal – start new call.

Clear-Forward

Clear-Forward signal – normal call clearing initiated by calling party.

Dialing Pulse

Line signal to generate dialing pulses for provision of DNIS number.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > CAS National Variants

CAS National Variants Settings - default

Line Signals MFC/R2 Forward Signals MFC/R2 Backward Signals Options Timers

Common Signals

Idle 10

Blocking 11

Forward Signals

Seizure 00

Clear-Forward 10

Dialing Pulse 01

Backward Signals

Seizure ACK 11

Answer 01

Clear-Back 11

Forced Release 00

Billing Pulse 00

Save Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Backward Signals

Line signals for backward direction (signals sent by the terminating/destination point).

Seizure ACK

Line seizure acknowledge signal.

Answer

Line answer signal.

Clear-Back

Clear-Back signal – normal call clearing initiated by called party after call answer.

Forced Release

Forced Release signal – call clearing request before call answer.

Billing Pulse

Line signal to generate billing pulses.

MFC/R2 Forward Signals and **MFC/R2 Backward Signals** categories define MFC/R2 register signaling parameters. MFC/R2 register signaling uses MFC/R2 tones (1 – 15) transmitted in voice channels to provide addressing information and call progress status. The forward as well as backward signals have primary and secondary meanings. The forward primary and secondary signals are usually described as group I and group II. The backward primary and secondary signals are described as group A and group B. Some countries extend MFC/R2 register signaling of backward group C. Here you can configure MFC/R2 tones (1 – 15) for register signals/states.

Group I

Primary forward signals are used to provide DNIS and ANI numbers.

End of DNIS

Indication of the end of DNIS (Dialed Number Identification Service) number.



End of ANI

Indication of the end of ANI (Automatic Number Identification) number.

ANI not Available

ANI number is not available – ANI restriction.

GUI-version : 1.1 / Board Type : 1 Logout



Home
Users
Trunks
Traffic
Globals
System
Diagnostics
Specials



Globals > CAS National Variants



CAS National Variants Settings - default

Line Signals
MFC/R2 Forward Signals
MFC/R2 Backward Signals
Options
Timers



Group I



End of DNIS  I-15 



End of ANI  I-15 



ANI not Available  unused 



Group II



National Subscriber  II-1 



National Priority Subscriber  II-2 



National Maintenance  II-3 



National Operator  II-5 



National Data  II-6 

National PayPhone  unused 

International Subscriber  II-7 

International Priority Subscriber  II-9 

International Operator  II-10 

International Data  II-8 

Save
Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Group II

Secondary forward signals are used to provide calling party category.

National Subscriber

Calling party is subscriber without priority.

National Priority Subscriber

Calling party is subscriber with priority.

National Maintenance

Calling party is maintenance equipment.

National Operator

Calling party is operator.

National Data

Calling party is data transmission equipment.

National PayPhone

Calling party is pay-phone.

International Subscriber

Calling party is international subscriber without priority.

International Priority Subscriber

Calling party is international subscriber with priority.



International Operator

Calling party is international operator.

International Data

Calling party is international data transmission equipment.

GUI-version : 1.1 / Board Type : 1 Logout

Home
Users
Trunks
Traffic
Globals
System
Diagnostics
Specials

Globals > CAS National Variants

CAS National Variants Settings - default

Line Signals
MFC/R2 Forward Signals
MFC/R2 Backward Signals
Options
Timers

Group A

Send Next DNIS Digit	A-1
Send Previous DNIS Digit	A-2
Address Completed, Switch to Group B	A-3
Network Congestion	A-4
Send Calling Party Category	A-5
Immediate Accept	A-6
Send Second-to-last DNIS Digit (N-2)	A-7
Send Third-from-last DNIS Digit (N-3)	A-8
Repeat All DNIS Digits	unused
Send Next ANI Digit	A-5
Send Calling Party Category and Switch to Group C	unused

Group B

Send Special Information Tone	B-2
User Busy	B-3
Network Congestion	B-4
Unassigned Number	B-5
Line Free Charge	B-6
Line Free No Charge	B-7
Line Out Of Order	B-8
Line Free Charge Alternative 1	unused
Line Free Charge Alternative 2	unused

Group C

Send Next ANI Digit	unused
Repeat all DNIS digits and switch to Group A	unused
Send next DNIS digit and switch to Group A	unused
Send previous DNIS digit and switch to Group A	unused
Address Completed, Switch to Group B	unused
Network Congestion	unused

Save
Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Group A

Primary backward signals are used especially to collect DNIS and ANI digits from the calling party.

Send Next DNIS Digit

Request to send next DNIS digit.

Send Previous DNIS Digit

Request to repeat last DNIS digit.

Address Completed, Switch to Group B

Indication of the complete DNIS number and switch over to reception of group B signals.

Network Congestion

Call failure, network congestion indication.

Send Calling Party Category

Request to send calling party category.

Immediate Accept

Indication of the complete DNIS number and immediate call acceptance.

Send Second-to-last DNIS Digit (N-2)

Request to repeat second-to-last DNIS digit.

Send Third-from-last DNIS Digit (N-3)

Request to repeat third-from-last DNIS digit.

Repeat All DNIS Digits

Request to repeat complete DNIS number from the beginning – send the first DNIS digit again.

Send Next ANI Digit

Request to send next ANI digit.

Send Calling Party Category and Switch to Group C

Request to send calling party category and switch over to reception of group C signals.

Group B

Secondary backward signals are used for indication of status of called party.

Send Special Information Tone

Call failure, send special information progress tone.

User Busy

Call failure, destination user/line is busy.

Network Congestion

Call failure, network congestion.

Unassigned Number

Call failure, called number does not exist.

Line Free Charge

Call accepted.

Line Free No Charge

Call accepted.

Line Out Of Order

Call failure, destination line is out of order.

Line Free Charge Alternative 1, 2

Call accepted. Assign this if there are available more signals for call acceptance.

Group C

Group C backward signals are used to collect called identification address (ANI number) from the calling party. Group C signals are not in common use, only some countries support them.

Send Next ANI Digit

Request to send next ANI digit.

Repeat All DNIS Digits and Switch to Group A

Request to repeat complete DNIS number from the beginning and switch over to reception of group A signals.

Send Next DNIS Digit and Switch to Group A

Request to send next DNIS digit and switch over to reception of group A signals.

Send Previous DNIS Digit and Switch to Group A

Request to repeat last DNIS digit and switch over to reception of group A signals.

Address Completed, Switch to Group B

Indication of the complete DNIS number and switch over to reception of group B signals.

Network Congestion

Call failure, network congestion indication.

Options category defines special parameters which can be used to tune the behavior of CAS signaling protocol.

Special Parameters

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > CAS National Variants

CAS National Variants Settings - default

Line Signals MFC/R2 Forward Signals MFC/R2 Backward Signals Options Timers

Special Parameters

- Switch to Group B on DNIS Timeout ☐
- ANI Repeat ☐
- Ignore Invalid Line Forward Signal During MFC/R2 ☒
- Ignore Invalid Line Forward Signal During Ringing ☒
- Ignore Invalid Line Backward Signal During MFC/R2 ☐
- Ignore Invalid Line Backward Signal During Ringing ☐
- Switch to Group A on End of ANI During Group C ☐
- Billing Pulse after Answer ☐

Save Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Switch to Group B on DNIS Timeout

Enable this option to use expiration of compelled MFC/R2 cycle (timer T3) for DNIS digit request as indication of end of DNIS number. Call set-up goes on with reception of group B signals in this case.

ANI Repeat

Enable repetition of complete ANI number from the beginning when it is requested after previous end of ANI indication.

Ignore Invalid Line Forward Signal during MFC/R2**Ignore Invalid Line Backward Signal during MFC/R2**

If enabled then invalid (unexpected) line forward/backward signals during MFC/R2 register signaling phase are ignored.

Ignore Invalid Line Forward Signal during Ringing**Ignore Invalid Line Backward Signal during Ringing**

When enabled then invalid (unexpected) line forward/backward signals during ringing phase (between end of MFC/R2 register signaling phase and the call answer) are ignored.

Switch to Group A on End of ANI during Group C

Enable switch over to reception of group A signals when end of ANI number indication is sent during reception of group C signals.

Billing Pulse after Answer

Enable generation of one billing pulse automatically after call answer. Some older exchanges can require this option for correct operation.

Timers category define various protocol timing settings. All timers are configured in milliseconds.

Timers

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Globals > CAS National Variants

CAS National Variants Settings - default

Line Signals MFC/R2 Forward Signals MFC/R2 Backward Signals Options **Timers**

Timers

Seizure ACK Timeout ?	2000
Clear-Back Persistence Timeout ?	400
Forced Release Persistence Timeout ?	400
Clear-Forward Persistence Timeout ?	100
Billing Pulse On-time ?	95
Billing Pulse Off-time ?	600
Max.Forward MFC/R2 Signal On-time (T1) ?	5000
Max.Forward MFC/R2 Signal Off-time (T2) ?	5000
Inbound Side Compelled Cycle Timer (T3) ?	15000
MFC/R2 Backward Non-compelled Pulse Length ?	150
Delay Before Backward Non-compelled MFC/R2 Pulse ?	300
Wait for Group B Signal Timeout ?	15000

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Seizure ACK Timeout

Maximal time of waiting for seizure acknowledge line signal.

Clear-Back Persistence Timeout

Minimal time to evaluate clear-back line signal as valid signal.

Forced Release Persistence Timeout

Minimal time to evaluate forced release line signal as valid signal.

Clear-Forward Persistence Timeout

Minimal time to evaluate clear-forward line signal as valid signal.

Billing Pulse On-time

Length of billing pulse.

Billing Pulse Off-time

Minimal length of delay between two subsequent billing pulses.

Max.Forward MFC/R2 Signal On-time (T1)

Maximum time a forward MFC/R2 signal can be on, from the outbound perspective.

Max.Forward MFC/R2 Signal Off-time (T2)

Maximum time a forward MFC/R2 signal can be off, from the outbound perspective.

Inbound Side Compelled Cycle Timer (T3)

Maximum time a whole compelled MFC/R2 cycle can take, from the inbound perspective.

MFC/R2 Backward Non-compelled Pulse Length

Duration of non-compelled MFC/R2 signaling pulse in backward direction. Some countries require such pulse, even though they break the compelled signaling scheme, and introduce timeout delays.

Delay Before Backward Non-compelled MFC/R2 Pulse

Minimum delay between end of compelled MFC/R2 signaling cycle and non-compelled pulse from destination side.

Wait for Group B Signal Timeout

Maximal time of waiting for MFC/R2 Group B signal after provision of the complete addressing information – call acceptance/failure indication.

SYSTEM MENU

IP settings

IP settings provide basic configuration of the Ethernet interfaces LAN and WAN (IP address assignment, MAC address modification, DNS setting, etc). Voice&Data Router is supplied with the following default setting:

	LAN	WAN
Mode	static	static
IP Address	192.168.1.100	10.1.1.100
Mask	255.255.255.0	255.0.0.0
Gateway		10.1.1.1
MAC Address	default	default

GUI-version : 1.1 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > IP Settings

IP Settings

LAN
eth0
Mode: static
IP Address: 192.168.1.170
Mask: 255.255.255.0
Gateway: 192.168.1.123
MAC Address: ☒ Default

WAN
eth2
Mode: static
IP Address: 10.1.1.170
Mask: 255.0.0.0
Gateway:
MAC Address: ☒ Default

DNS
Server Address: 192.168.1.210
Server Address: 8.8.8.8

HOSTNAME
TEST

Save & Apply Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Mode

Select **static** option if you want to configure IP address manually by your own. Select **dhcp** option to obtain IP address automatically from the network.

IP Address

IP address configuration (static setting).

Mask

Subnet mask configuration (static setting).

Gateway

Default gateway (static setting). Note that default gateway can be only one – it should be configured only for one Ethernet interface LAN or WAN.

MAC Address

Check **Default** if you want to use Ethernet hardware address assigned by producer. If you need to overwrite hardware Ethernet address for some reason to suit your preference then uncheck **Default** and enter new address as colon separated hexadecimal numbers (e.g. 00:50:C2:38:76:80). Modified MAC address will be applied only after reboot of Voice&Data Router.

DNS

Enter IP address of Domain Name Server (primary and secondary).

HOSTNAME

Enter Voice&Data Router hostname.

Network configuration changes apply immediately after clicking on the **Save & Apply** button. There is no need to activate standard Apply Changes function.

When you change IP address of the interface you use to communicate with Voice&Data Router then Web Manager automatically tries to switch to the new address (it works only for static setting of IP address).

Routing Tables

Routing tables define rules for static IP routing. In most cases it is enough to configure basic IP settings and no additional rules for IP routing are necessary. Here you can configure additional gateways for routing to the target address (host or network).

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Routing Tables

Routing Tables Settings

List of Routes

<input checked="" type="checkbox"/>	192.168.2.0	255.255.255.0	10.1.1.1
<input type="checkbox"/>	192.168.10.0	255.255.255.0	10.1.1.1

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Use the **Create New** button to add new route to the routing table. Check existing route in the table and click on the **Modify Selected** to change route parameters. You can remove selected (checked) routing items when you click on the **Delete Selected** button.

New common form is used for creating and editing item of the routing, where you can enter specific route parameters.

IP Address

Enter IP address of the destination network or host.

Mask

Enter network mask to be used for the network destination. When the destination is host, use value 255.255.255.255 for network mask or leave this field empty.

Gateway

Enter address of the gateway to use for routing. The specified gateway must be reachable first.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Routing Tables

Add or Edit Route

IP address:

Mask:

Gateway:

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Routing tables changes apply immediately after clicking on the **Save & Apply** button. There is no need to activate standard Apply Changes function.

SNMP

SNMP (Simple Network Management Protocol) is an application layer protocol used in network management systems to monitor network-attached devices for conditions that warrant administrative attention. On Voice&Data Router, SNMP agent is running to allow administrators to remotely manage device status and configuration. Voice&Data Router supports SNMP version v1/v2c.

SNMP protocol setting is divided into two parts

- General Settings
- Trap Settings

General Settings are used to enable the SNMP agent and to define system options required for its remote administration.

Enable SNMP Agent

Enable SNMP agent for remote system monitoring.

System Name

System name for identification of Voice&Data Router.

System Description

Detailed information about managed system.

System Location

Information to describe the network where SNMP management is performed.

System Contact

Information about the contact person responsible for the SNMP management in the defined network. Field may indicate the point person's name, email address, phone number or other contact information.

Read-Only Community

SNMP v1/v2c read-only community description (public, private, etc.) for the read-only management. It may contain some kind of password which should be matching both on the device and on the administrating application for successful SNMP management.

Trap Settings are used to define the traphosts that should be informed when certain events occur on the Voice&Data Router.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

System > SNMP

SNMP Settings General Settings Trap Settings

Trap Settings

Traphost	Community	
192.168.1.14	public	<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Use the **Add** button to define new SNMP traphost. Click **Edit** button to modify selected SNMP traphost. To remove existing traphost use the **Delete** button.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

System > SNMP

SNMP Settings

Edit Traphost

Traphost

Community

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

Traphost

IP address or the host name of the traphost. Administrating application's host address should be inserted here.

Community

Trap community description (public, private, etc.) for the administrating application to accept the notifications about the certain events on the device. Field may contain some kind of password which should be the same both on the device and on the administrating application for successful SNMP management.

Firewall

Voice&Data Router firewall function can protect LAN network and Voice&Data Router itself from unauthorized users of other networks. It is recommended to activate firewall if Voice&Data Router is used in function of access data router or if it is connected directly to the Internet on public address.

Firewall implementation in Voice&Data Router allows:

- Control incoming traffic on both LAN and WAN interfaces
- Control packet forwarding between LAN and WAN interfaces
- Network address translation – NAT

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Firewall

Firewall Settings Edit Input Firewall Edit Forward Firewall Edit Destination NAT

General Settings

Enable Input Firewall <input checked="" type="checkbox"/>	Global Policy <input type="text" value="DROP"/>
Enable Forward Firewall <input checked="" type="checkbox"/>	Global Policy <input type="text" value="DROP"/>
Enable Source NAT <input checked="" type="checkbox"/>	

Save & Apply Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Enable Input Firewall

Enable/disable input firewall functionality. Input firewall controls incoming traffic to Voice&Data Router on both Ethernet interfaces (LAN and WAN). You can select global policy which defines default behavior when packet does not match any input firewall rule:

- **ACCEPT** – let the packet through
- **DROP** – drop the packet on the floor

Use the **Edit Input Firewall** button for configuration of firewall rules to filter incoming packets.

Enable Forward Firewall

Enable/disable forward firewall functionality. It allows you to control packet forwarding between LAN and WAN interfaces. You can select global policy which defines default behavior when packet does not match any firewall rule:

- **ACCEPT** – let the packet through
- **DROP** – drop the packet on the floor

Use the **Edit Forward Firewall** button to configure rules for the forward firewall.

Enable Source NAT

Enable/disable NAT (Network Address Translation) functionality. NAT translates source private local network address to WAN interface (public) address. It allows users from LAN network to connect to the external network (such as the Internet) using WAN IP address. Use the **Edit Destination NAT** button to configure rules for destination NAT, which provides translation of the destination address from WAN to the private local network address.

Input firewall configuration consists of set of the rules to filter incoming packets to the Voice&Data Router. Input firewall rules apply only to packets addressed to Voice&Data Router not to forwarded packets. Click on the **Add New** button if you want to create new input rule. Use the **Edit** button to modify existing rule. Use the **Delete** button to remove selected rule and the **Delete All** button to remove all the rules from the list. Note that the rules are evaluated in the order they are configured and that is why the rules order is important for correct functionality of the firewall. You can control the order of the rules by using arrows in the first column of the table.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Firewall

Firewall Settings

Input Firewall Details

Order	Protocol	Policy	Interface	Src Address	Src Port	Dst Port	
↓	tcp	ACCEPT	wan	195.168.205.88		22	<input type="button" value="Add New"/> <input type="button" value="Delete All"/>
							<input type="button" value="Edit"/> <input type="button" value="Delete"/>
↑	tcp	DROP	any			22	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Input firewall rules define condition to match incoming packet and the policy. Input packets which satisfy the rule condition are accepted/dropped according rule policy. If packet does not match condition of any rule then global policy is applied.

Protocol

Select the IP transport protocol of incoming packet to apply the rule. The following protocol options are available: all, TCP, UDP, ICMP.

Policy

Select the policy for input packet matching rule condition. Policy specifies if the packet is allowed or not. You can select following values

- **ACCEPT** – let the packet through
- **DROP** – through the packet away

Interface

Select Ethernet interface of incoming packets. It allows firewall to filter packets coming only from certain interface.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Firewall

Firewall Settings

Input Firewall Rule

Protocol tcp

Policy ACCEPT

Interface wan

Src Address 195.168.205.88 /

Src Port to

Dst Port 22 to

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Src Address

Enter packet source address. Source address condition can restrict/allow packets from certain IP addresses. You can specify single IP address or network IP address with mask. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0.

Src Port

Enter packet source port or port range. Source port condition is allowed only for TCP and UDP protocol and it filters input packets according source port numbers.

Dst Port

Enter packet destination port or port range. Destination port condition is allowed only for TCP and UDP protocol and it can filter input packets by destination port numbers.

Forward firewall configuration is the list of the rules to filter packet forwarding between LAN and WAN interfaces. Click on the **Add New** button if you want to create new forward rule. Use the **Edit** button to modify existing rule. Use the **Delete** button to remove selected rule and the **Delete All** button to remove all the rules from the list. Note that the rules are evaluated in the order they are configured and that is why the rules order is important for correct functionality of the firewall. You can change the rules' order by arrows in the first column of the table.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Firewall

Firewall Settings

Forward Firewall Details

Order	Protocol	Policy	Src Interface	Src Address	Src Port	Dst Interface	Dst Address	Dst Port
	all	ACCEPT	lan	192.168.1.0/24		wan		

Add New Delete All Edit Delete

Back

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Forward firewall rules consist of filtering condition and the policy. Forward rules apply to packets coming from local LAN network to WAN network and on the contrary from WAN to LAN. Packets which satisfy the rule condition are accepted or dropped according policy of the rule. If packet does not match condition of any rule then global policy is applied.

Protocol

Select the IP transport protocol of filtered packets to apply the rule. The following protocol options are available: all, TCP, UDP, ICMP.

Policy

Select the policy for packet matching rule condition. Policy specifies if the packet is allowed or not. Following values are available

- **ACCEPT** – let the packet through
- **DROP** – through the packet away

Src Interface

Select Ethernet interface via which a packet is received. Together with setting of destination interface we can define condition for packet direction (from LAN to WAN or vice-versa).

Dst Interface

Select Ethernet interface via which a packet is going to be sent. Together with source interface setting we can define condition for packet direction (from LAN to WAN or vice-versa).

Src Address

Enter packet source address. Source address condition can restrict/allow packets from certain IP addresses. You can specify single IP address or network IP address with mask. The mask can be

either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0.

Dst Address

Enter packet destination address. Destination address condition can restrict/allow packets addressed to specific IP addresses. You can write single IP address or network IP address with mask. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic **Globals** System Diagnostics Specials

System > Firewall

Firewall Settings

Forward Firewall Rule

Protocol tcp

Policy ACCEPT

Src Interface lan Dst Interface wan

Src Address 192.168.1.0 / 24 Dst Address /

Src Port to Dst Port 22 to

Save Record
Cancel

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Src Port

Enter packet source port or port range. Source port condition is allowed only for TCP and UDP protocol and it filters packets according source port numbers.

Dst Port

Enter packet destination port or port range. Destination port condition is allowed only for TCP and UDP protocol and it can filter packets by destination port numbers.

GUI-version : 1.2 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic **Globals** System Diagnostics Specials

System > Firewall

Firewall Settings

Destination NAT Details

Order	Protocol	Src Address	WAN Port	LAN Address	LAN Port	
↓	tcp	188.133.99.137	2222	192.168.1.14	22	Add New Delete All
↑ ↓	udp		20000:20999	192.168.1.48	20000:20999	Edit Delete
↑ ↓	tcp		88	192.168.1.170	80	Edit Delete
↑	tcp		89	192.168.1.171	80	Edit Delete

Back

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Destination NAT allows remote users from WAN network (for example, computers on the Internet) to connect to a specific computer or service within our LAN network. This technique is often called port

forwarding or port mapping. You can define set the rules for LAN destination address translation. Click on the **Add New** button if you want to create new destination NAT rule. Use the **Edit** button to modify existing rule. Use the **Delete** button to remove selected rule and the **Delete All** button to remove all the rules from the list. Note that the rules are evaluated in the order they are configured and that is why the rules order is important for correct functionality of the firewall. You can change the rules' order by arrows in the first column of the table.

Destination NAT rules consist of filtering condition and definition of LAN destination. Rules apply to packets coming from external WAN network and if the rule condition is matching packet is redirected to specified LAN destination address.

The screenshot shows the 'voice&data router' web interface. At the top, it says 'GUI-version : 1.2 / Board Type : 1' and has a 'Logout' link. Below the header is a navigation bar with tabs: Home, Users, Trunks, Traffic, Globals, System, Diagnostics, and Specials. The 'System' tab is selected, leading to 'System > Firewall'. The main content area is titled 'Firewall Settings' and contains a section for 'Destination NAT Rule'. Inside this section is a form with the following fields: 'Protocol' (a dropdown menu set to 'tcp'), 'Src Address' (two input fields separated by a slash), 'WAN Port' (an input field with '89' and a 'to' field), 'LAN Address' (an input field with '192.168.1.171'), and 'LAN Port' (an input field with '80' and a 'to' field). Below the form are two buttons: 'Save Record' and 'Cancel'. At the bottom of the page, a copyright notice reads 'Copyright © 2010-2012, All Rights Reserved www.inoteska.sk'.

Protocol

Select the IP transport protocol of filtered packets to apply the rule. The following protocol options are available: TCP, UDP, ICMP.

Src Address

Enter packet source address. Source address condition can limit access only for users from certain IP addresses. You can specify single IP address or network IP address with mask. The mask can be either a network mask or a plain number, specifying the number of 1's at the left side of the network mask. Thus, a mask of 24 is equivalent to 255.255.255.0.

WAN Port

Enter destination port or port range of received packet. WAN port condition is allowed only for TCP and UDP protocol and it filters packets according destination port numbers.

LAN Address

Enter new destination IP address. Packets matching rule condition are redirected to this address.

LAN Port

Enter new destination port or port range. Destination port can be specified only for TCP or UDP protocol.

Firewall setting applies immediately after clicking on the **Save & Apply** button on the main screen of firewall setting. There is no need to activate standard Apply Changes function.

Options

Use **Change password** to change password of active user (admin) for access to Voice&Data Router Web Manager. Password should be at least 4 characters long. For password changing type your new password in the **Enter New Password** text field and confirm it in the **Retype New Password** field. New password is activated after click on the **Update** button and you are automatically redirected to the initial login screen to re-login with new authentication.

GUI-version : 1.1 / Board Type : 1 Password should be at least 4 characters ! Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Options

Change Password

Change Password Reset Configuration Reboot

Enter New Password

Retype New Password

Update

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Reset Configuration restores default factory configuration. Default factory setting is created and loaded into the device during production and it is the basic setting the device is supplied with. If the **Keep Network Settings** checkbox is enabled network configuration is not changed and you don't need to change the address in your web browser to re-connect to Voice&Data Router. Use **Reset to Defaults** button to restore factory default configuration.

To avoid losing of actual configuration [Backup and restore](#) function can be used before reset to defaults. Voice&Data Router will restart automatically after applying reset to the default setting.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Options

Reset to Factory Defaults

Change Password Reset Configuration Reboot

Warning: By resetting your Voice&Data Router to factory defaults, you will lose all your configuration !
You can take a backup of your current configuration from the [Backup page](#).

☒ Keep Network Settings

Reset to Defaults

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Reboot allows Voice&Data Router restart. System reboot usually takes about 1 minute but it can vary. Web Manager automatically re-connects to Voice&Data Router after minute and half. You can also use browser reload function to try to re-connect before this timeout.

Reboot Appliance[Change Password](#) [Reset Configuration](#) [Reboot](#)

Warning: Rebooting the appliance will terminate all active calls.

[Reboot Now](#)

Backup and Restore

Voice&Data Router allows you to manage configuration data backups. You can create and store backup of actual Voice&Data Router configuration. It is possible to return back to the stored configurations at any moment in the future. You can also download configuration backups to archive them out of the device.

To backup actual configuration of Voice&Data Router click on the **Create New Backup** button. New backup file is stored in the file system. You can use **Restore** button to restore device configuration from selected backup file. System will restart automatically after applying of configuration restoring. Note that this operation can change Voice&Data Router network setting and it may be necessary to enter new IP address to your web browser to recover the connection after device restart. Existing configuration backup can be removed by using of **Delete** button.

GUI-version : 1.8 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics

System > Backup and Restore

Backup / Restore Configurations Create New Backup Upload Backup File

List of Configuration Backups

#	Name	Date	
1	backup1_TEST_UK0_121631	Jan 26, 2016	Download Restore Delete
2	backup1_TEST_UK0_153918	Jan 25, 2016	Download Restore Delete

Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

If you want to download configuration backup to your PC, click on the **Download** button. Direct link to the backup file appears and can be used to download.

[Download File](#) [close](#)

Right Click on the above link and download using the 'Save Link As..' option

If you want to upload configuration backup from your PC to Voice&Data Router use **Upload Backup File** button. You need to choose file to upload and click on the **Submit** button. Only files previously downloaded from the device can be successfully uploaded and restored.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Backup and Restore

Upload a previous backup File List of Backups Upload Backup File

File Uploading

Upload

Choose File backup1_201...eb23.tar.gz

- backup1_2012feb23_091524__2012feb23.tar.gz (application/gzip) - 314830 bytes

Submit

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Firmware Update

Voice&Data Router supports three possibilities how to update firmware

- TFTP protocol download
- HTTP protocol download
- File upload

Use TFTP Server

Check this option to use TFTP protocol to download firmware update file. Enter TFTP URL address – server address with path to the update file, into the input field and click on **Update Firmware** button. Voice&Data Router downloads specified file and starts update process. Firmware is checked for validity after download and the warning is displayed if it does not suit.

Use HTTP Server

Check this option to use HTTP protocol to download firmware update file. Enter HTTP URL address – server address with path to the update file, into the input field and click on **Update Firmware** button. Voice&Data Router downloads specified file and launches update process. Firmware is checked for validity after download and the warning is displayed if it does not suit.

Use File

Check this option to upload firmware update file from your PC. Use the **Choose File** button to select file for upload and then click on the **Upload file** to transfer selected file to Voice&Data Router. Click on the **Update Firmware** button to start update process. Firmware is checked for validity before update is executed and the warning is displayed if it does not suit.

GUI-version : 1.1 / Board Type : 1 Logout


voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Firmware Update

Firmware Update

Firmware Source

 ☒ Use TFTP Server

☐ Use HTTP Server

☐ Use File

 No file chosen

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

System will automatically restart after firmware update.

Date and Time

Voice&Data Router system time adjustment.

Date and Time Setting

Date, Time

Current date and time.

Get Device Time

Click to read current system time from Voice&Data Router and refresh displayed date and time.

Get Computer Time

Click to get current system time of your PC and refresh displayed date and time (can be used to synchronize Voice&Data Router with your PC).

Set Time

Adjust system time of Voice&Data Router. Values in **Date** and **Time** fields are used. Date and time setting applies immediately; there is no need to activate standard Apply Changes function.

GUI-version : 1.1 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

System > Date and Time

Date and Time Settings

Date and Time Setting

Date (DD MM YYYY)

Time (HH MM SS)

Time Zone Setting

Time zone

☒ Day Light Saving

NTP Server Setting

☒ NTP enabled

Server Address Update Interval

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Time Zone Setting

Time Zone

Select time zone of your country.

Day Light Saving

Enable daylight saving time (summer time).

NTP Server Setting

NTP enabled

Enable automatic clock synchronization with NTP (Network Time Protocol) server.

Server Address

Enter NTP server address (IP address or host name).

Update interval

Select interval of automatic clock synchronization.

- Hourly every hour
- Daily every day at 2:25 am
- Weekly every Sunday at 2:47 am

Configuration changes apply immediately after clicking on the **Save & Apply** button. There is no need to activate standard Apply Changes function.

DIAGNOSTICS MENU

Port Status

Port status displays actual status of selected ports. Actual status is read from Voice&Data Router after pressing **Display Status** button. If **Enable Auto Updating** is checked status is updated automatically circa every 3 seconds.

You can display status of the following ports/channels:

- E1/T1 – actual status of E1/T1 ports
- BRI – actual status of BRI ports
- GSM – actual status of GSM modules (optional)
- Analog – actual status of analog ports (optional)
- SIP – actual status of SIP trunks and users
- Ethernet – actual status of Ethernet ports

GUI-version : 1.2 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Diagnostics > Port Status

Port Status
☐ Enable Auto Updating
E1/T1
Display Status

E1/T1 Status

```

FALC-framer[0x0]
STS = 0x00000000 decoding: --- --- --- --- --- --- ---
FEC = 0x0000004a Framing Error Counter
CVC = 0x000000ee Code Violation Counter
CEC = 0x0000000b CRC Error Counter
SLI = 0x00000004 Slip Error Counter
LOS = 0x0000001d Loss of signal
AIS = 0x00000000 Alarm Indication
LFA = 0x0000001c Loss of frame
RRA = 0x00000006 Receive remote alarm

FALC-framer[0x1]
STS = 0x000000a8 decoding: LOS --- LFA --- DLL --- --- ---
FEC = 0x00000007 Framing Error Counter
CVC = 0x00000045 Code Violation Counter
CEC = 0x00000001 CRC Error Counter
SLI = 0x00000001 Slip Error Counter
LOS = 0x00000007 Loss of signal
AIS = 0x00000000 Alarm Indication
LFA = 0x00000004 Loss of frame
RRA = 0x00000001 Receive remote alarm

FALC-framer[0x2]
STS = 0x000000a8 decoding: LOS --- LFA --- DLL --- --- ---
FEC = 0x00000001 Framing Error Counter
CVC = 0x00000003 Code Violation Counter
CEC = 0x00000000 CRC Error Counter
SLI = 0x00000001 Slip Error Counter
LOS = 0x00000003 Loss of signal
AIS = 0x00000000 Alarm Indication
LFA = 0x00000001 Loss of frame
RRA = 0x00000001 Receive remote alarm

FALC-framer[0x3]
STS = 0x00000001 decoding: --- --- --- --- --- --- --- OFF
FEC = 0x00000000 Framing Error Counter
CVC = 0x00000000 Code Violation Counter
CEC = 0x00000000 CRC Error Counter
SLI = 0x00000000 Slip Error Counter
LOS = 0x00000001 Loss of signal
AIS = 0x00000000 Alarm Indication
LFA = 0x00000000 Loss of frame
RRA = 0x00000000 Receive remote alarm

```

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Active Services

Use active services function to display actual status of users' services. It displays list of all users with active services like Do Not Disturb and Call Forwarding.

You can use **Delete User** and **Delete All** buttons to deactivate services for selected user eventually for all users.

GUI-version : 1.2 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Diagnostics > Active Services

Delete User
Delete All

Do Not Disturb

User	Status
10	on

Call Forwarding (Unrestricted)

User	Forward Number
10	12365
12	0104155

Call Forwarding if Busy

User	Forward Number

Call Forwarding if no Respond

User	Forward Number

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Identification

Identification provides basic hardware information about Voice&Data Router. BASIC section information is read from permanent memory which is programmed during device production. Here you can find information such as device type – product code number, serial number, date of production, hardware interfaces, etc. CONFIG and FUNCTIONS parts are stored in the file and they can be used to enable/disable optional interfaces and functionalities.

GUI-version : 1.2 / Board Type : 1
Logout

voice&data router
inoteska

Home Users Trunks Traffic Globals System Diagnostics Specials

Diagnostics > Identification

Identification

Details

[BASIC]

TYPE=ITX495012000220
SN=495010990102
ID=5490
DATE=21.1.2010
SERVP=F3DE1AF32994DA01EA9299293C6157B0
MAN=103,104
DPS=ITB 166 09
PROD=INOTESKA
ADR=PODTUREN-ROVEN221,LIPTOVSKY HRADOK,03301
TEL=+421445221809,+421903360360
MAIL=MAIL@INOTESKA.SK
WWW=WWW.INOTESKA.SK
HW=1000
RD=D
SDRAM=128M
FLASH=8M
CARD=SD
FPGA=ICDP1C12F324C8
CPU=M82810
CON=1
E1=4
ETH=2
TEST=

[CONFIG]

TYPE=ITX495012000220
SN=495010990102
ID=5490
USERS=108
USERB=108
E1=0,1,2,3
ETH=0,1

[FUNCTIONS]

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

System Logs

Voice&Data Router stores operation logs in the file system. Voice&Data Router logs management is divided into two parts:

- Asterisk Log Files
- System Log Files

Asterisk Log Files cover log messages from the Asterisk voice communication system application. It is possible to enable/disable Asterisk logging, set logging level and display stored logs.

The screenshot shows the Voice&Data Router web interface. At the top, it says 'GUI-version : 1.8 / Board Type : 1' and has a 'Logout' link. The main header features the 'voice&data router' logo and the 'inoteska' brand name. A navigation bar includes links for Home, Users, Trunks, Traffic, Globals, System, and Diagnostics. Below this, a breadcrumb trail reads 'Diagnostics > System Logs'. The main content area is titled 'Voice&Data Router Log messages' and contains two tabs: 'Asterisk Log Files' (selected) and 'System Log Files'. Under the 'Asterisk Log Files' tab, there is a 'Disable Logger' button and a row of checkboxes for logging levels: 'notice' (unchecked), 'warning' (checked), 'error' (checked), 'debug' (unchecked), and 'verbose' (unchecked). Below these controls is a table listing log files:

File	Size	Date	
event_log	1 kB	Jan 26 10:21	Show Reset
messages	11 kB	Jan 26 10:21	Show Reset

At the bottom of the interface, a copyright notice states: 'Copyright © 2010-2016, All Rights Reserved www.inoteska.sk'.

There is **Disable Logger** or **Enable Logger** button to switch on and off Asterisk logging. When logging is enabled you can use check boxes (notice, warning, error, debug and verbose) to set logging level.

Recorded log files are listed in the table. You can use **Show** button to display content of select log file and you can clear selected log file with the **Reset** button.

System Log Files allows

Voice&Data Router Log messages

Asterisk Log Files

System Log Files

System Log Files

File	Size	Date		
btmtp	1 kB	Jan 25 16:24	Show	Reset
syslog.log	81 kB	Jan 26 12:17	Show	Reset
wtmtp	23 kB	Jan 26 07:21	Show	Reset

/var/log/syslog.log

```

Jan 25 15:41:25 VD_ROUTER syslogd 1.4.1#17: restart.
Jan 25 15:41:25 VD_ROUTER kernel: klogd 1.4.1#17, log source = /proc/kmsg started.
Jan 25 15:41:25 VD_ROUTER kernel: Inspecting /boot/System.map
Jan 25 15:41:26 VD_ROUTER nrpe[888]: Starting up daemon
Jan 25 15:41:26 VD_ROUTER kernel: Loaded 22768 symbols from /boot/System.map.
Jan 25 15:41:26 VD_ROUTER kernel: Symbols match kernel version 2.6.11.
Jan 25 15:41:26 VD_ROUTER kernel: No module symbols loaded - kernel modules not enabled.
Jan 25 15:41:26 VD_ROUTER kernel: Linux version 2.6.11.7-1.08.5.3malindi (root@debian-dev2) (gcc version 3.3.2 20030820
Jan 25 15:41:26 VD_ROUTER kernel: CPU: ARM920Tid(wb) [41129200] revision 0 (ARMv4T)
Jan 25 15:41:26 VD_ROUTER kernel: CPU0: D VIPT write-back cache
Jan 25 15:41:26 VD_ROUTER kernel: CPU0: I cache: 16384 bytes, associativity 64, 32 byte lines, 8 sets
Jan 25 15:41:26 VD_ROUTER kernel: CPU0: D cache: 16384 bytes, associativity 64, 32 byte lines, 8 sets
Jan 25 15:41:26 VD_ROUTER kernel: Machine: ARM-M828xx Concerto
Jan 25 15:41:26 VD_ROUTER kernel: Memory policy: ECC disabled, Data cache writeback
Jan 25 15:41:26 VD_ROUTER kernel: On node 0 totalpages: 28672
Jan 25 15:41:26 VD_ROUTER kernel: DMA zone: 28672 pages, LIFO batch:7
Jan 25 15:41:26 VD_ROUTER kernel: Normal zone: 0 pages, LIFO batch:1
Jan 25 15:41:26 VD_ROUTER kernel: HighMem zone: 0 pages, LIFO batch:1
Jan 25 15:41:26 VD_ROUTER kernel: Built: 1 zonelists

```

[Download /var/log/syslog.log](#)

Right Click on the above link and download using the 'Save Link As...' option

CLI Emulator

CLI emulator provides you access to Command Line Interface of internal Asterisk. It allows you to execute CLI commands you enter in the **CLI Command** field.

GUI-version : 1.2 / Board Type : 1

Logout

voice&data router

inoteska

Home

Users

Trunks

Traffic

Globals

System

Diagnostics

Specials

Diagnostics > CLI Emulator

Voice&Data Router CLI

CLI Command:

Command>core show version

Asterisk 1.4.42-1 built by jch @ debian-dev2 on a i686 running Linux on 2012-05-22 09:02:22 UTC

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

Use command “help” to display all available CLI commands. To display brief command description you can use “help” plus complete command (e.g. “help core show channels”).

Debug messages

Debug messages can log GUI manager functionality. Use the **Start DEBUG** and **Stop DEBUG** buttons to control Voice&Data Router GUI manager debugging.

GUI-version : 1.2 / Board Type : 1

Logout

voice&data router

inoteska

Home

Users

Trunks

Traffic

Globals

System

Diagnostics

Specials

Diagnostics > Debug Messages

Debug Messages

Start DEBUG

Stop DEBUG

Status

List of messages is **OFF**

Copyright © 2010-2012, All Rights Reserved www.inoteska.sk

System Status

System status shows actual status of Voice&Data Router. It involves actual system time and device running time, usage of hardware resources (CPU, memory, file system) and information about software version.

GUI-version : 1.8 / Board Type : 1

Logout

voice&data router

inoteska

Home

Users

Trunks

Traffic

Globals

System

Diagnostics

Diagnostics > System Status

System Status

GUI 1.8

System Time: 12:26:04

Uptime: 5:06

CPU Usage:

1%

Total Active Processes: 63

Memory Usage:

97%

of 108 MB


Kernel: 2.6.11.7-1.08.5.3malindi

Root Filesystem Usage:

7%

of 3664 MB

Firmware: 2.6



Copyright © 2010-2016, All Rights Reserved www.inoteska.sk

File Editor

File editor provide direct access to selected configuration files of Voice&Data Router. In this way you are able to configure nonstandard functions or functions not supported by Web Manager.

Files you can access are listed in the **Config Files** list on the right side. Selected file is displayed on the screen. File editor can handle only files divided into the contexts/sections. All the comments are filtered out – not displayed. The comments are all lines starting with semi-colon ‘;’ and also multi-line blocks between comment markers “;--” and “--;”.

Clicking on the selected context it is switched to the edit mode. You can use **Add Context** button to create new file context.

Note that direct changing of configuration files is not recommended for people without detailed knowledge of the system. . Unqualified change of the configuration can make the device non-functional.

AOC Web Update

GUI-version : 1.0 / Board Type : 1 Logout

voice&data router inoteska

Home Users Trunks Traffic Globals System Diagnostics **Specials**

AOC Update Service Settings Check AOC File Now

Details

Domain Name or IP Address

Working Directory Name

Periodicity ☐ regularly every

☒ every day at : o'clock

Repeat Count

Copyright © 2010, All Rights Reserved www.inoteska.sk

Domain Name or IP Address

Name or address of web server where AOC files are saved

Working Directory Name

Directory name on server where AOC files are saved (item can be blank if files are in server main directory)

Periodicity

Periodicity of AOC files correctness control, it is possible to choose either time interval (every 1, 4, 6 or 12 hours) or hour when control will be done

Repeat Count

Number of repeated files control (used when control is executed with error)

Check AOC File Now

Runs immediate control of AOC file. After successful completion, name of currently used AOC file is displayed.

UNIMAN

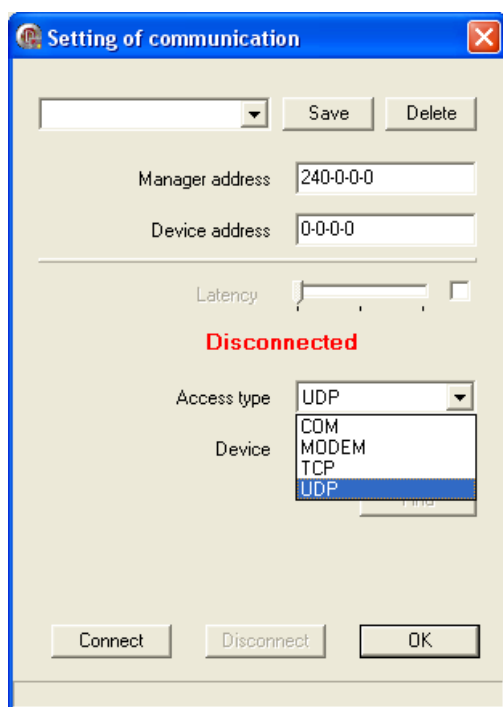
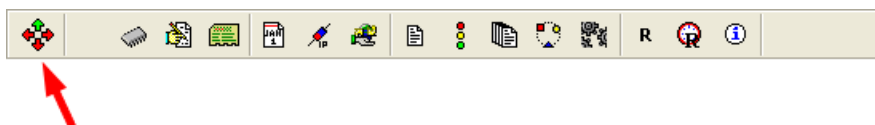
UniMan is proprietary management application running on Windows platform. It can be used for the communication with various Inoteska equipments.

UniMan is not preferred management tool for Voice&Data Router and it does not offer complete device configuration. UniMan support in Voice&Data Router is limited only for network configuration and diagnostics.

CONNECTION TO THE DEVICE

UniMan communicates with Voice&Data Router over Ethernet using TCP or UDP protocol. You can access the device directly connected to the PC or you can access the device co in your local network or you can also connect to the remote device over the Internet.

To open window for communication setting click on the speed button **Setting of communication** or use menu item **Communication/Setting of communication**.



Manager address

Select manager address which is used by UniMan protocol. First number can be from interval 240–254, other three numbers from interval 0–255. Default value (240-0-0-0) can be used for communication with Voice&Data Router.

Device address

Select device address used by UniMan protocol. First number is from interval 0–239, other three numbers from interval 0–255. Use always default setting (0-0-0-0) for Voice&Data Router.

UDP Connection

UDP connection can be used to communicate with local devices. You do not need to know device IP address – UniMan is able to search for available Inoteska equipments.

This access type can be used only if the conditions stated below are met:

Device is connected in network

- Device and PC must be connected in the same local network
- Network must transmit *broadcast*
- PC must have IP address allocated
- Device must have default gateway configured
- Device must be attached by default Ethernet interface

Device is connected to PC locally

- PC must have arbitrary IP address allocated (it is necessary to disable DHCP and set static IP address, e.g. 192.168.1.2)
- Receive/Transmit of *broadcast* packets must be enabled on PC

- UDP port 3864 must be enabled on PC
- Device must have default gateway configured
- Device must be attached by default Ethernet interface

The screenshot shows the 'Setting of communication' dialog box. At the top, there is a dropdown menu and 'Save' and 'Delete' buttons. Below, the 'Manager address' is set to '240-0-0-0' and the 'Device address' is '0-0-0-0'. A 'Latency' slider is visible. The status is 'Disconnected' in red text. The 'Access type' is set to 'UDP' in a dropdown menu. Below it is a 'Device' dropdown menu and a 'Find' button. At the bottom are 'Connect', 'Disconnect', and 'OK' buttons.

1. Set **Access type** to **UDP**.
2. Click on **Connect**. All the devices connected in network will be displayed.
3. Select the device you wish to configure. If it is connected, then **Connected** is displayed.
4. Click **OK**.

TCP Connection

TCP connection can be used if we know IP address of the device we want to connect to. There are no restrictions and you can connect both local device in your LAN and remote device over the Internet.

Default IP address setting:

- LAN: 192.168.1.100
- WAN: 10.1.1.100

The screenshot shows the 'Setting of communication' dialog box configured for TCP. The 'Manager address' is '240-0-0-0' and the 'Device address' is '0-0-0-0'. The status is 'Disconnected' in red text. The 'Access type' is set to 'TCP' in a dropdown menu. Below it are fields for 'IP Address' (195.168.209.42) and 'TCP Port' (7777). At the bottom are 'Connect', 'Disconnect', and 'OK' buttons.

1. Set **Access type** to **TCP**.
2. **Set IP address** and **TCP Port** (by default UniMan communicate on port 7777).
3. Click on **Connect**. If the device is connected, then **Connected** is displayed.
4. Click **OK**.

SETTING OF PASSWORD

To have access to the Voice&Data Router configuration, password authentication is required. Default password is **inoteska**.

You can manage UniMan password using main menu **Options/Password**.

New login

New login with new password.

Change password of device

Change of default password. It is possible to authorize the different levels and passwords for different users.

Change password [default]

User: Password: Level: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6 ☐ 7 ☐ 8 ☐ 9 ☐ 10 ☐ 11 ☐ 12 ☐ 13 ☐ 14 ☐ 15 ☐ 16

default inoteska x x x x x x x x x x x x x x x x

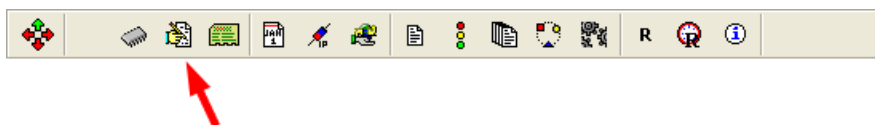
1 - Read configuration 9 - Change of firmware
 2 - Read Access list 10 - Change of Access setting via remote control
 3 - 11 - Change of Remote control and IP/Ethernet setting
 4 - Download of Call log 12 - Change of configuration
 5 - Write configuration 13 - Change of password
 6 - Config files editor 14 -
 7 - 15 -
 8 - 16 - Change of all passwords and levels

BBtnRead Write Cancel

CONFIGURATION FILES EDITOR

Configuration files editor provides access to the device configuration. Just now there is available only network configuration for Voice&Data Router.

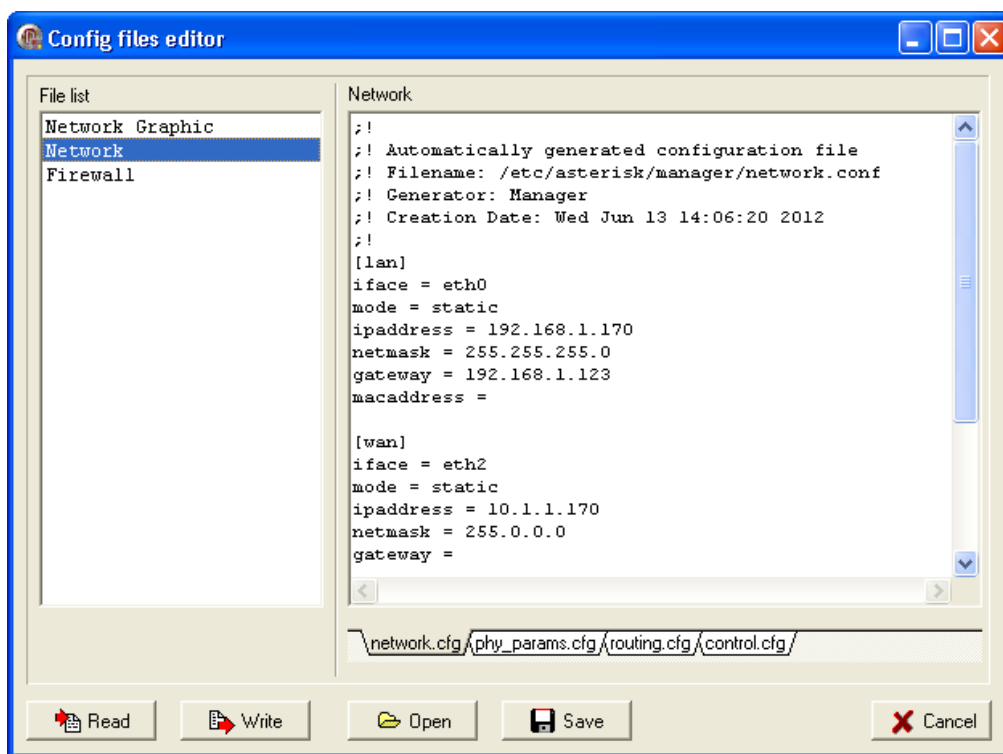
To open configuration editor click on the speed button **Config files editor** or use main menu **Communication/Config files editor**.



File list on the left side of the configuration editor shows list of configurable items. It can work in text mode or in the graphic (GUI) mode. Text mode offers only direct access to the text configuration files. Graphic mode provide comfort GUI interface.

Configurable items in Voice&Data Router

- **Network Graphic** – GUI interface for the network interface configuration.
- **Network** – text mode of the network interface configuration
- **Firewall** – text mode of the firewall configuration



Double click on the selected item in the file list reads configuration files from the device and eventually activates GUI interface. In the text mode you can directly edit configuration files in the right side of the window.

Configuration changes will be applied only after writing configuration files to the device using the **Write** button. You have to write changed configuration also in case of using GUI interface. Buttons **Save** and **Open** can be used to store/load active configuration files to/from disk on your PC.

Network Setting – GUI

GUI interface for network setting is available from the configuration file editor – **Network Graphic** or directly from main window using speed button **Remote control & IP/Ethernet setting** or from main menu **Communication/Remote control IP/Ethernet setting**.

The screenshot shows a 'control' window with two main sections: 'Interface eth0 - LAN' and 'Interface eth2 - WAN'. Each section has a 'MAC Address' field set to 'DEFAULT'. Below each is an 'IP setting' box with a 'DHCP' checkbox (unchecked), an 'IP address' field, a 'Mask' field, and a 'Gateway' field. For the LAN interface, IP is 192.168.1.170, Mask is 255.255.255.0, and Gateway is 192.168.1.123. For the WAN interface, IP is 10.1.1.170, Mask is 255.0.0.0, and Gateway is empty. Below the IP settings are 'Speed' and 'Duplex' sections. For both interfaces, Speed has radio buttons for AUTO, 10M, 100M, 10M Auto, and 100M Auto (100M is selected). Duplex has radio buttons for Half and Full (Full is selected). There is also a checked 'MDIX' checkbox. At the bottom, there is a 'Hostname' field with 'test_170' and a 'DNS server' field with '192.168.1.210'. At the very bottom are 'OK' and 'Cancel' buttons.

MAC Address

Enter 'DEFAULT' if you want to use Ethernet hardware address assigned by producer. If you need to overwrite hardware Ethernet address for some reason to suit your preference enter new address as colon separated hexadecimal numbers (e.g. 00:50:C2:38:76:80). Modified MAC address will be applied only after reboot of Voice&Data Router.

DHCP

Check this option to obtain IP address automatically from the network.

IP address

IP address configuration.

Mask

Subnet mask configuration.

Gateway

Default gateway. Note that default gateway can be only one – it should be configured only for one Ethernet interface LAN or WAN.

Speed, Duplex

Ethernet interface speed and duplex configuration.

MDIX

Enable/disable MDIX (Medium Dependent Interface Crossover) option for Ethernet interface.

Hostname

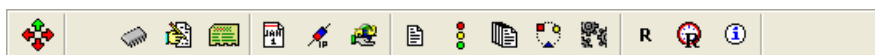
Enter Voice&Data Router hostname.

DNS Server

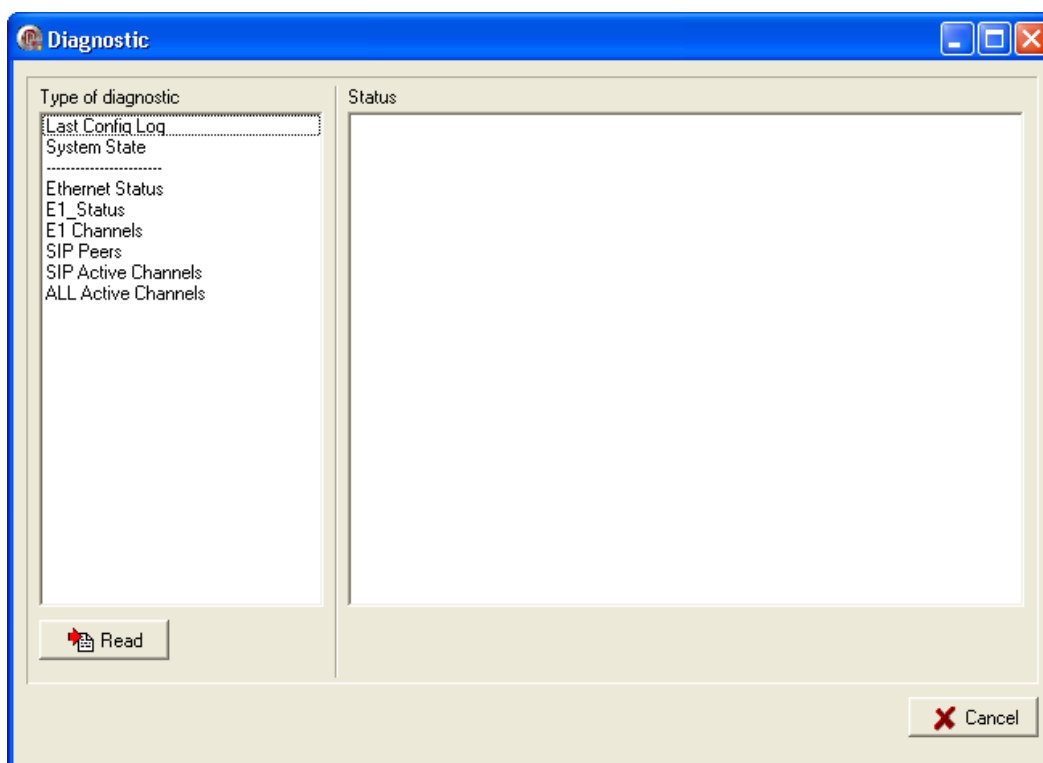
Enter IP address of Domain Name Server (only primary).

DIAGNOSTICS

Use diagnostic window to monitor system status and status of each interfaces. Diagnostic is activated by the speed button **Diagnostic** or from the main menu command – **Communication/Diagnostic**.

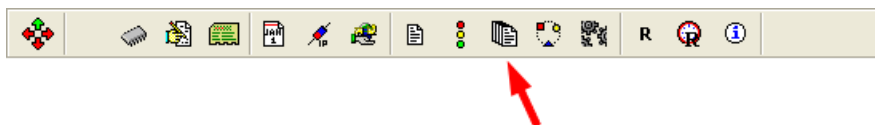


Type of diagnostic list on the left side of the diagnostics shows index of items that can be monitored. Double click on the selected item will display information of actual status. In the most cases is the status automatically updated.

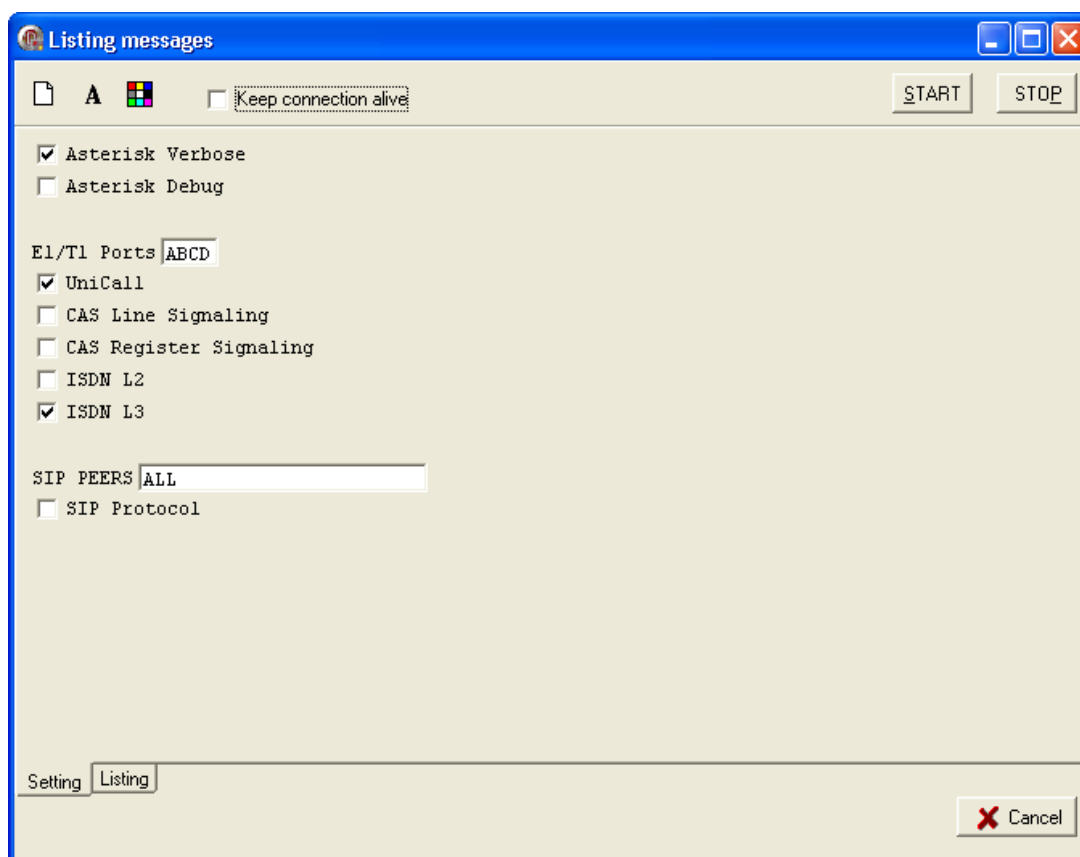


LISTING MESSAGES

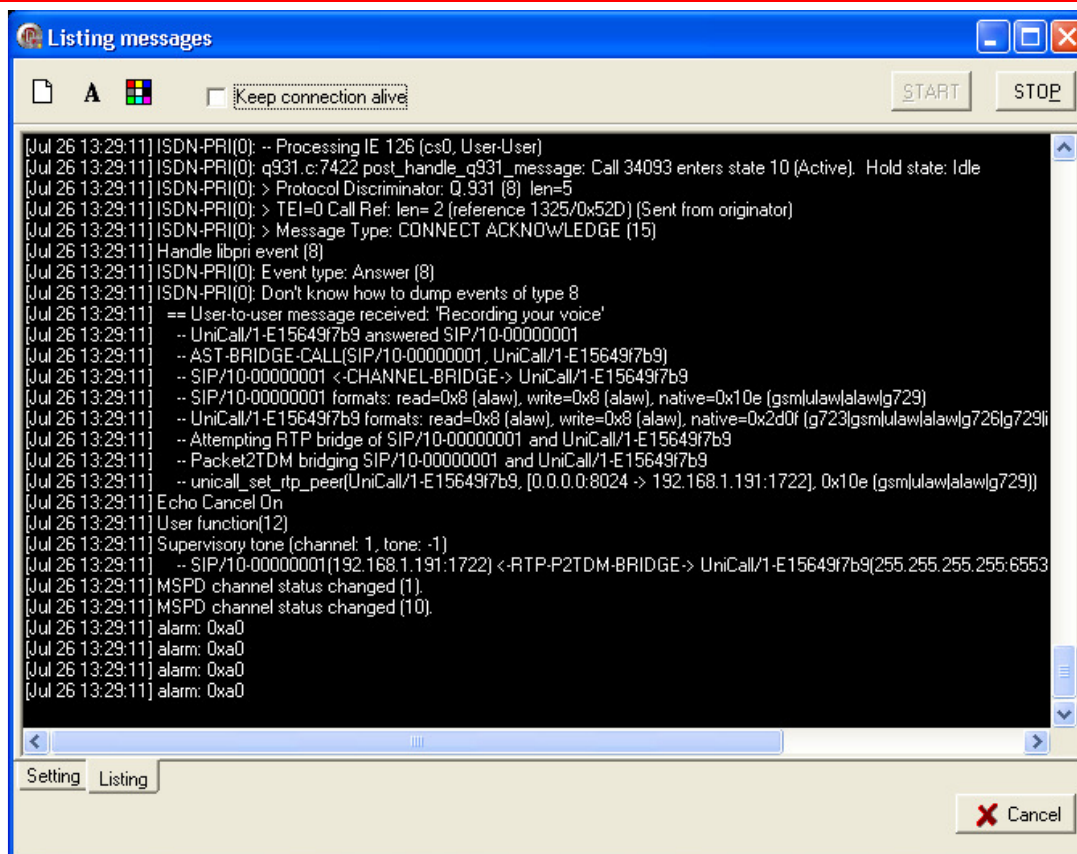
This function allows making online logs of Voice&Data Router call switching. You can access listing window by clicking on the speed button **Listing messages** or by using main menu command – **Communication/ Listing messages**.



On the **Setting** card you can configure logging filter – selection of interfaces and protocols to monitor and also monitoring level.

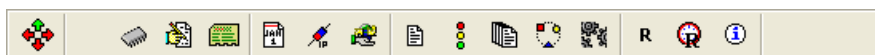


Click **START** button to begin capturing of the logs from the device. Received logs are displayed in real-time on the **Listing** card. Use **STOP** button to finish device monitoring and store captured logs in the text file on the local PC.

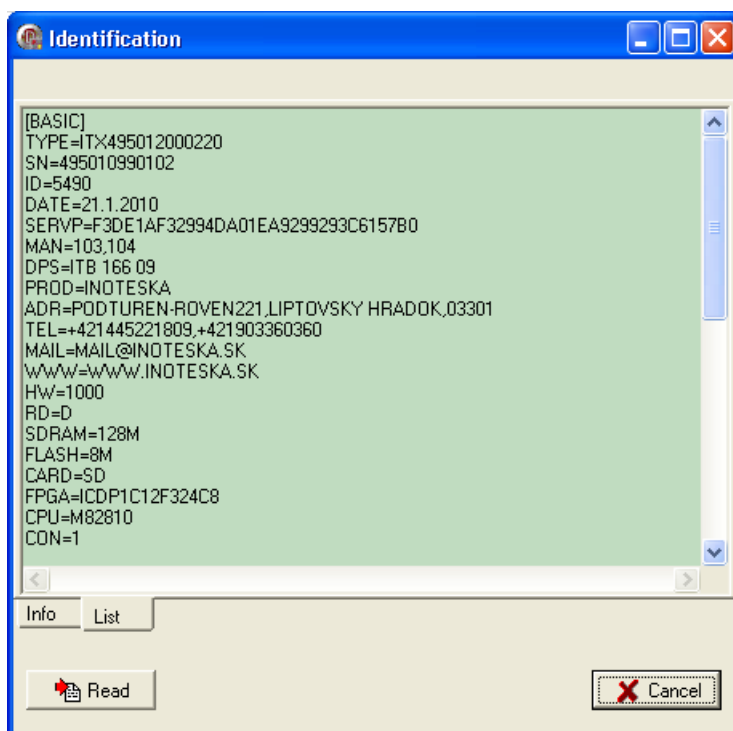


IDENTIFICATION

Identification provides basic hardware information about Voice&Data Router. To open identification window use speed button **Identification** or main menu command – **Communication/Identification**.



BASIC section information is read from permanent memory which is programmed during device production. Here you can find information such as device type – product code number, serial number, date of production, hardware interfaces, etc. CONFIG and FUNCTIONS parts are stored in the file and they can be used to enable/disable optional interfaces and functionalities.



TERMS OF SALE

Warranty:

Product warranty period is 24 months from the date of delivery or installation. Warranty does not apply in case of an accident, handling by a non-professional or improper use or force majeure.

Delivery:

Standard delivery time is max. 6 weeks from the signing of the purchase order or after mutual agreement.

Contact:

Inoteska s.r.o.
Podtureň-Roveň 221
Liptovský Hrádok
033 01
Slovenská Republika

Tel.: + 421 44 5567 911
Fax: + 421 44 5221 519
Hotline: + 421 902 774 538

Web: www.inoteska.sk
E-mail: email@inoteska.sk

VAT no.: SK2020428300

Bank information: Všeobecná úverová banka a.s.

Account no.: 616243342/0200

SWIFT code: SUBASKBX

IBAN: SK3402000000000616243342

Sales department:

Ing. Ľubica Brtáňová +421 903 826 079
Ing. Pavel Wolf +421 903 800 133

Technical department:

Ing. Pavol Perdek +421 903 519 908
Ing. Pavel Wolf +421 903 800 133