Cryptome

Downloaded 16 June 2010

http://www.unispeed.com/Docs/BlueShield_docu.pdf

unispeed

Unispeed Blue Shield system

ETSI and CALEA Compliant Data retention and Lawful interception system

System documentation v2.0

The Unispeed Blue Shield system is designed for Network operators complying with Anti-terror logging and lawful interception requirements, and integrates the Unispeed Remote probe monitoring, authentication and gateway support systems.

unispeed

Table of Contents

1 System overview

The Unispeed Blue Shield system is an integrated solution consisting of Blue Shield Data Loggers (BSP), Blue Shield management system (BMS), Blue Shield data logging services (BSDS, Remote Authentication Server (RAS) and Network storage facilities (NAS).

The system is designed for Network operators and telecommunication service providers that must provide interception capabilities in their network for persons under surveillance.

The main functions of any LI solution are to access Interception-Related Information (IRI) and Content of Communication sessions (CC) from the telecommunications network and to deliver the information in a standardised format via the handover interface to one or more monitoring centres of law enforcement agencies.

Lawful Interception (LI) is the legally approved surveillance of telecommunication services - it has become an important tool for law enforcement agencies (LEAs) around the world for investigating and prosecuting criminal activities and terrorism.
Most countries have passed laws that require telecommunication service providers to support LEAs with duly authorised requests to identify, monitor, and deliver all of the electronic communication of specified individuals and groups.

The Unispeed RTM system offer the costumer the opportunity to combine anti-terror solutions with add value solutions for their networks.

2 System components

2.1 Blue Shield Probe - BSP

The Blue Shield probes combine the Unispeed anti-terror logger with advanced logging functions derived from the Unispeed Netlogger series packet sniffers.
The Probes are a series of hardware devices capable of collecting and analysing Ethernet traffic. The product portfolio ranges from dual 100 MBit interface loggers to 2 x 10 GBASE interface equipped servers. The BSP can operate as a passive sniffer, in bridge mode or in mixed mode depending on costumer preference.

The Unispeed BSP can collect both interception related information (IRI) and content of communication sessions (CC) for all types of Internet traffic.

The advanced filter, aggregation and classification tools employed in the BSP ensure that future legislation is easily complied with and offers the costumer a variety of possible add-on including:

- Traffic and content billing
- Ad-serving and web analysis
- Network security
- Policy enforcement

- GEO-Location
- Network monitoring and management

In bridge mode the Blue Shield integrates provisions for routing, firewall / traffic shaping, access control and DHCP functions, and is designed as a stand alone device for small and medium size network. (Blue Shield gateway Probe)

In passive mode the Blue Shield Probe is added to the existing network components and will collect traffic information from span/mirrored or network tabs making the solution virtually invisible and immune to intrusion.

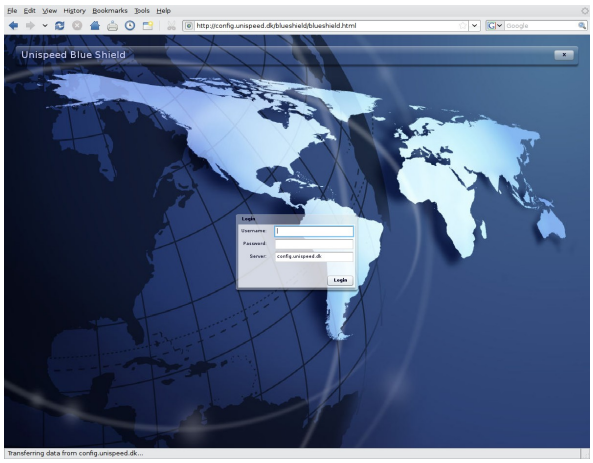
In mixed mode the Blue Shield Probe is capable of performing Routing/NAT and DHCP services for one part of the network while passively collecting traffic information from other parts of the network.

When attached to the network the Blue Shield Probe will automatically establish a secure connection to the BMS. At regular intervals the Blue Shield Probe will submit status reports and log files and query the BMS for system and configuration updates and security patches.

2.2 Blue Shield management system (BMS)

The management system is the component from where the Probes are managed.

The BMS has provisions for:



- Continuously updated monitoring of probe status
- Full configurable alarms with text message push
- Remote probe maintenance
- Full configurable command cue system with comprehensive documentation
- Centralised software updates
- User administration – integrates with LDAP, MS AD, etc.

From The BMS an unlimited number of Blue Shield probes can be remotely monitored and managed.

2.3 Blue Shield Data Logging services

The Blue Shield data logging services is the component responsible for data retention, lawful interception and handover interfaces and has provisions for:

- Create job command cue for Blue Shield probes

- Schedule logging tasks to the probes for IRI and CC logging
- Receive Call data (CDR) from The Probes. (HI 2)
- Receive Content of communication (CC) from the probes (HI 3)
- Receive User ID related data from extracted DHCP leases - including Option 82 fields
- Receive User Identification from gateway units and authentication servers
- Backup data to the NAS or SAN
- Extract and Mediate CDR log data from storage and directly from probes
- Provide Handover HI 1 interfaces to LEA's in ETSI and CALEA standards
- Comprehensive reporting-, status- and alert system

2.4 Remote Authentication Server (RAS)

The remote authentication server is the component responsible for access control to a network controlled by a Blue Shield gateway probe.

The RAS integrates with costumer support systems and billing solutions and employs different methods for identifying the end costumer or target for Lawful interception.

Different login and access methods for Blue Shield Gateway controlled networks are supported and adjusted to costumer preference including:

- Secure web login
- SMS / text message login via SMS / text message gateway
- Credit card verification and billing

2.5 Network Attached Storage (NAS)

The network attached storage is a highly secured storage system for backing up data received from the Blue Shield data logging services and RAS or directly from the probes.

Intercept related information is stored in an optimized binary log format reducing the required storage needs to a minimum.

Aged data is automatically erased when the required period expires.

Data streamed directly from probes is automatically backed up to the storage system.

3 Advanced Application areas

Ref. Unispeed White papers

4 Appendixes

4.1 Hardware specification (Appendix)

BSP 2000/4000/8000/X20

Hardware / Software Features	Yes	No	Comment
Server			Dell Power Edge 1950/2950
Operating system	Hardware accelerated K-sniffer/Linux		
Processor capacity max	Intel core duo/1/2 x Quad Core Xeon X5355 2,66MHz 1333 FSB		
Number of cooling units	4		
Number of power supplies	2		
Amount of Memory	2GB FB 667MHZ DIMMs extendible to 32GB		
Local storage capacity (GB)	2 X SAS 73Gb (Raid 1) max 1.8TB SATA		
Fast Ethernet ports (number / type)		X	N/A
Gigabit Ethernet ports management/uplink	X		Broadcom Dual port GB
Gigabit Ethernet ports Sniffer max	X	X	2 X Intel Pro 1000 quad ports or 2 x 10GBASE
Other interfaces and hardware	X		USB, RGB, 8 X IDEDVD- ROM DRIVE, RAID ctlr.
Manufacturer name	Dell/Unispeed		
Manufacturer origin country	US/Denmark		
Expected lead time	30 days		
Warranty in months	24		
Input capacity			
Packets per second(400 byte packets)	400.000/800.000/1.600.000 /20M		
Wire rate performance	X		
Output			
uplink interface	1 Gbit/s		
Available output formats	ODBC, CSV/W3C, PCAP / TCP, BINARY		
Environment variables			
Width (mm)	426		
Depth (mm)	772		
Height (mm)	42,6		
Weight (kg)	16,3		
Operating temperature	10°C-35°C		
Operating humidity (%)	20%-80%		
Max power consumption (watt)	670W		
Electromagnetic Compatibility compliance with CENELEC norms/standards			CE

BSP 100/200/500

Hardware / Software Features	Yes	No	Comment
Server			Dell Power Edge 860
Operating system	Hardware accelerated K-sniffer/Linux		
Processor capacity	Intel Dual Core Xeon 3040/3050/3070		
Number of cooling units	4		
Number of power supplies	2		
Amount of Memory	1GB DDR2 SDRAM 667MHZ extendible to 8GB		
Local storage capacity (GB)	2 X SATA 160Gb (Raid 1) max 2.0TB SATA		
Fast Ethernet ports (number / type)	(X)		2 x100 MB (ATL 100)
Gigabit Ethernet ports management/uplink	X		Broadcom Dual port GB
Gigabit Ethernet ports Sniffer max	(X)		Intel Pro 1000 quad port
Other interfaces and hardware	X		USB, RGB, 8 X IDEDVD- ROM DRIVE, RAID ctlr.
Manufacturer name	Dell/Unispeed		
Manufacturer origin country	US/Denmark		
Expected lead time	30 days		
Warranty in months	24		
Input capacity			
Packets per second (600byte)	20.000/40.000/100.000		
Packets per second (200byte)			60.000/120.000/300.000
Wire rate performance	(X)	X	Wire rate performance on 100MB only
Output			
uplink interface	1 Gbit/s		
Available output formats	ODBC, CSV/W3C, PCAP / TCP, BINARY		
Environment variables			
Width (mm)	447		
Depth (mm)	546		
Height (mm)	42,7		
Weight (kg)	11,8		
Operating temperature	10°C-35°C		
Operating humidity (%)	20%-80%		
Max power consumption (watt)	345W		

BSP Light / BSP gateway unit

Hardware / Software Features	Yes	No	Comment
Server			TK64 Thick system
Operating system	Linux		
Processor capacity	VIA EDEN N Nano 800MHz Fanless		
Number of cooling units	0		
Number of power supplies	1		
Amount of Memory	256/512MBDDR266 standard		
Local storage capacity (GB)	4GB Flash memory max 16GB		
Fast Ethernet ports (number / type)	X		2 x VT6103 10/100 MB
Gigabit Ethernet ports management/uplink		X	
Gigabit Ethernet ports Sniffer max		X	
Other interfaces and hardware	X		2 X USB, RGB,
Manufacturer name	TK/Unispeed		
Manufacturer origin country	Taiwan/Denmark		
Expected lead time	On stock / 6 weeks		
Warranty in months	12		
Input capacity			
Packets per second (600byte)	20.000		
Packets per second (200byte)			50.000
Wire rate performance		X	approximately 80 Mbps
Output			
uplink interface			
Available output formats	ODBC, CSV/W3C, PCAP / TCP, BINARY		
Environment variables			
Width (mm)	38		
Depth (mm)	120		
Height (mm)	170		
Weight (kg)	0.94		
Operating temperature	0°C-60°C		
Operating humidity (%)	0%-90%		
Max power consumption (watt)	22.5W		

4.2 Probe installation General(Appendix)

The Blue Shield probes are attached to the network by means of network tabs or a router / switch span port.

The mirrored / span port is connected to the sniffer network card typically installed in one of the PCI slots of the server.

The sniffer interfaces are typically designated eth2 and up. And should be set to “promisc” mode

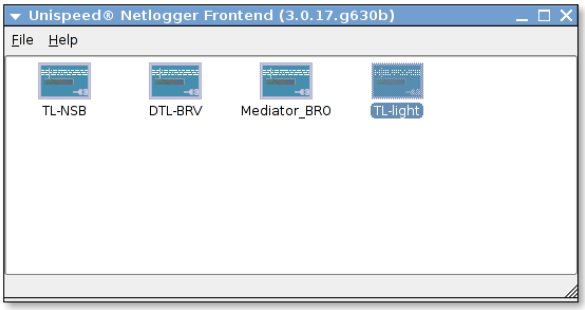
The management/ data uplink interface eth0 and the uplink interface eth1 will typically be assigned to the the interfaces residing on the server motherboard.

4.2.1 Connecting via Netlogger Frontend

The Netlogger Frontend is installed on a Linux or Windows platform.

The windows version is downloaded from the Unispeed server and automatically installed by the windows installer.

A new configuration for each Probe or Gateway probe shall be created from the file menu.



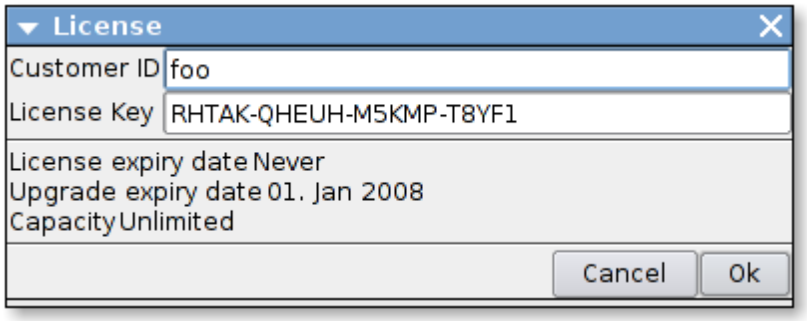
If connecting to the Probe from other than a local area network (LAN) connection a secure shell tunnel to the probe must be created.

From a Linux terminal enter the following command:

ssh root@xxx.xxx.xxx.xxx -L8000:ipaddress:8000

If you are using the windows Frontend you will have to configure the tunnel in Cygwin or Putty. Refer to the Putty / Cygwin manuals for more information.

Each device is given a costumer ID and a license key, typically for one year at a time. If the license expires the device will cease to work.

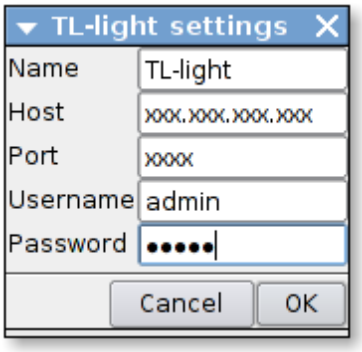


The device is given a meaning full name in the option dialogue,

Host should read the IP-address of the Probe (Netlogger) you wish to connect to, If you are using port forwarding enter ”localhost”

Port number is 8000 for XML-RPC connections

Default User name and Password is ”admin”, this should be changed



Dobbelt click the Netlogger icon to enter the main configuration window

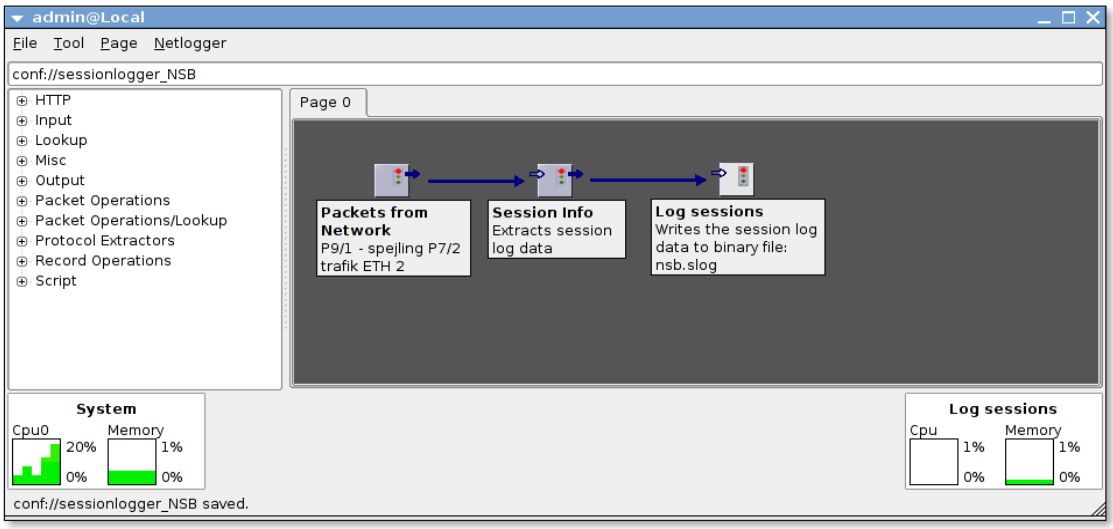
For detailed configuration description please refer to the Netlogger manual HTML.

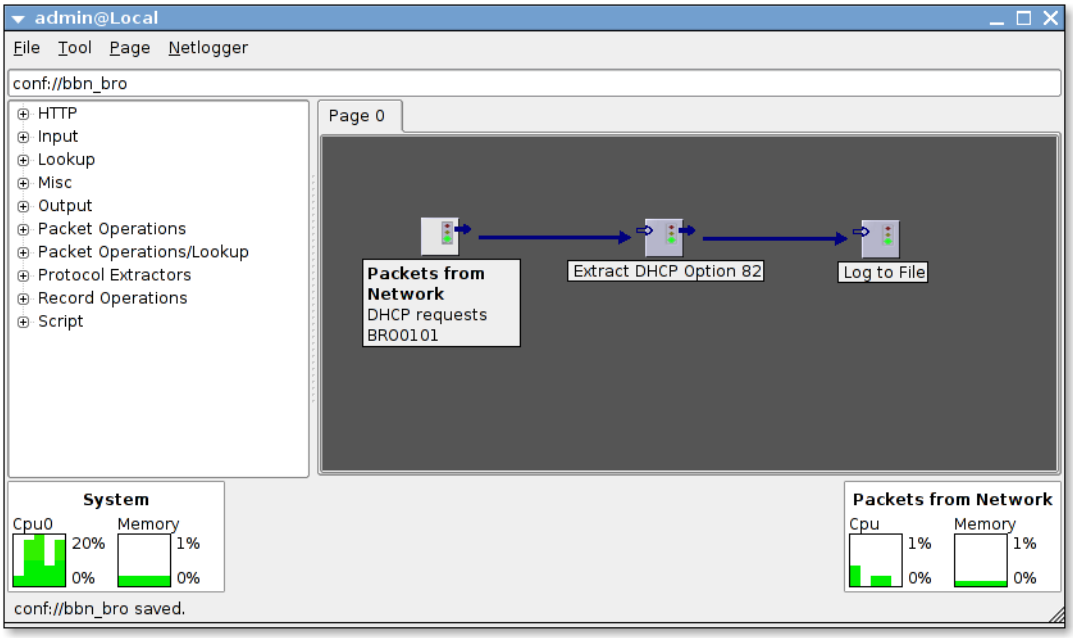
http://www.unispeed.com/manual/index.html

Drag and drop the relevant tools onto the canvas – configure and connect the tools according to desired configuration.

Configuration changes must be saved in the file menu as the Probe will reload last configuration in case of a manual or automatic restart

Annotating each tool eases the mental overview as you build your configuration.


admin@Local
File Tool Page Netlogger
conf://sessionlogger_NSB
HTTP
Input
Lookup
Misc
Output
Packet Operations
Packet Operations/Lookup
Protocol Extractors
Record Operations
Script
Page 0
Packets from Network
P9/1 - spejling P7/2 trafik ETH 2
Session Info
Extracts session log data
Log sessions
Writes the session log data to binary file: nsb.slog
System
Cpu0
20%
0%
Memory
1%
0%
Log sessions
Cpu
1%
0%
Memory
1%
0%
conf://sessionlogger_NSB saved.


admin@Local
File Tool Page Netlogger
conf://bbn_bro
HTTP
Input
Lookup
Misc
Output
Packet Operations
Packet Operations/Lookup
Protocol Extractors
Record Operations
Script
Page 0
Packets from Network
DHCP requests
BRO0101
Extract DHCP Option 82
Log to File
System
Cpu0
20%
0%
Memory
1%
0%
Packets from Network
Cpu
1%
0%
Memory
1%
0%
conf://bbn_bro saved.

4.2.2 Manual Call data retention and retrieval

The Netlogger drop down window contain a menu called ATL Logs.

Data is extracted based on IP address – Time frame – and Mac address

The Mac- Address being retrieved from log files previously generated by the DHCP extractor function of the Probe.

The purpose of the Netlogger ATL extension is to process and combine

information generated by the tools "Extract DHCP Option 82" and "Session

Info" and return the result to the Netlogger Frontend.

4.2.2.1 Setup

The following describes the requirements for the extension to work properly.

The extension works by reading output of the tools from disk files.

The output of "Extract DHCP Option 82" must be written to disk by "Log to

File". Name of log file must be 'pub://_dhcp/dhcp.log',

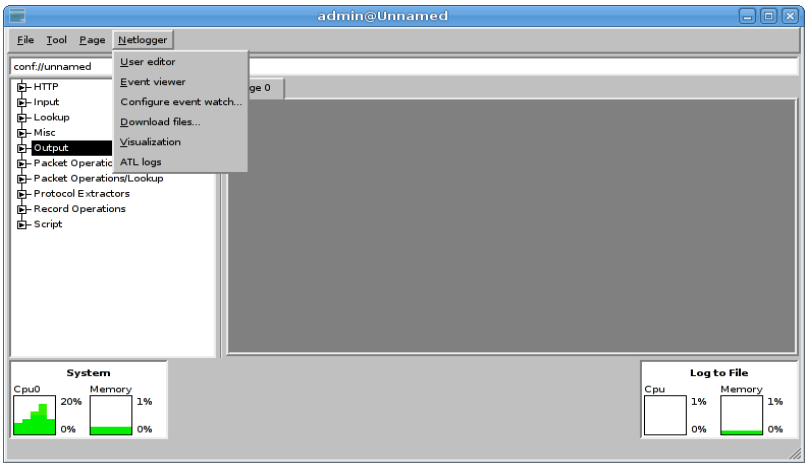
The switch interval should be something like 10 minutes, and all other options

should be left at the default values.

The output of "Extract Session Info" must be written to disk by "Log Sessions". If session info is extracted from more than one packet source, e.g there is more than one "Extract Session Info" tool in the configuration, a distinct prefix must be selected in the options for every "Log Sessions" tool.

4.2.2.2 Usage

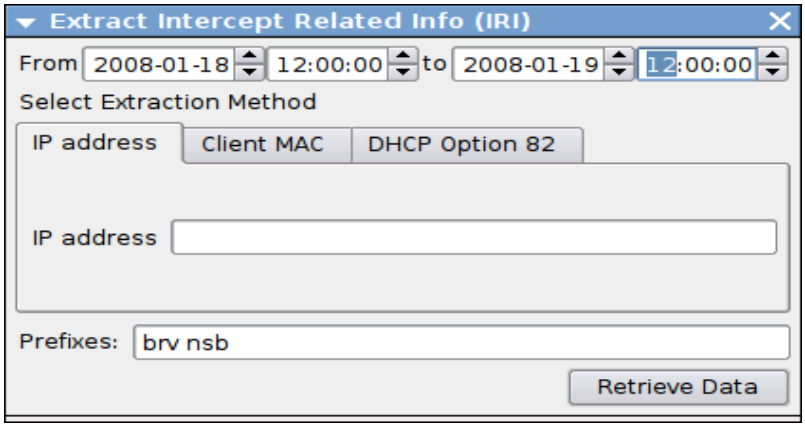
To get started, select the "ATL logs" item in the Netlogger menu of the Frontend. This opens the "Extract Intercept related Info" dialogue.



The first line of the dialogue lets the user specify time interval of interest. The extraction procedure has three main modes. Information can be extracted by Client hardware address (MAC), IP address and Remote/Circuit ID with option 82 enabled on the network. The combo box of the second line switches between these modes, and the text entry box lets the user type the target MAC, IP or remote/circuit ID to be searched for.

The prefix field automatically lists the log files stored in /pup/_slog://

Simply erase the prefixes you do not want to extract data from.

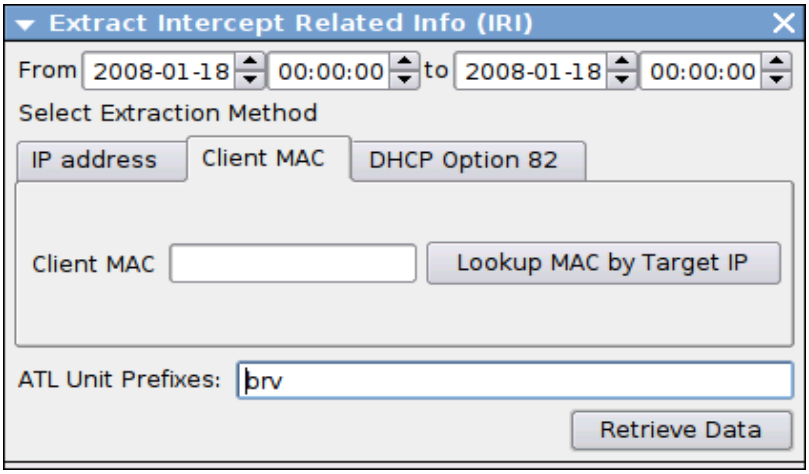


Extraction by IP address allows for two way data search:

If a client IP address is entered the output will reflect the transactions created by the client or clients to whom the address was leased in the time interval of interest.

If a remote host address is entered the output will reflect the transactions of all clients that visited the address in the specified time interval.

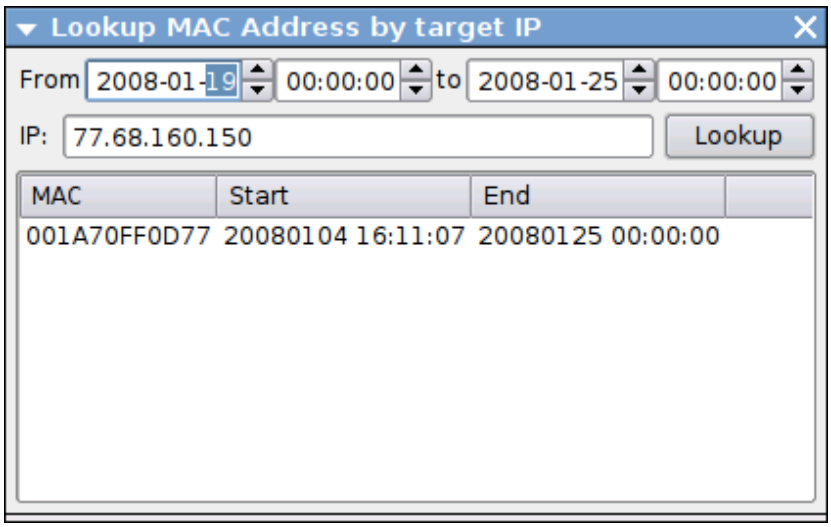
The IP address should be entered in the format xxx.xxx.xxx.xxx



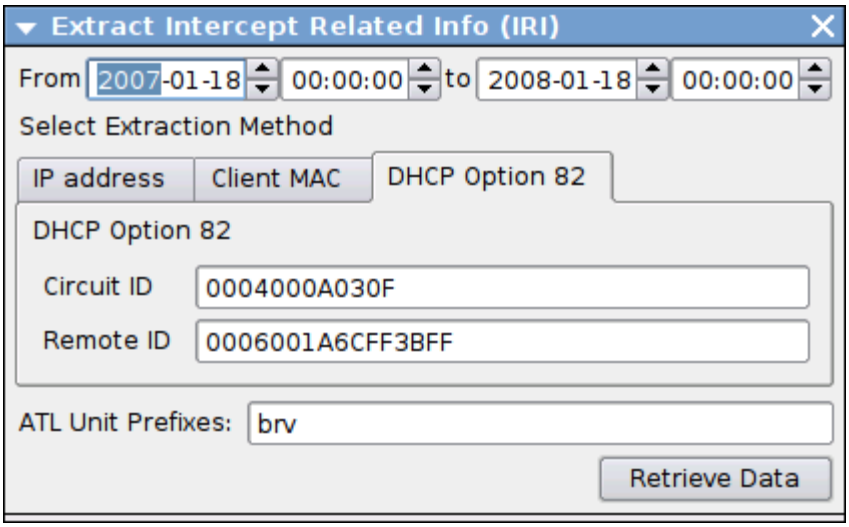
If extract by Client MAC method is selected enter the client hardware address in the Client MAC input field.

The input format is xx:xx:xx:xx:xx

In this mode the "The lookup MAC by Target IP..." button is activated. A click on this button opens a new dialogue, that helps the user find the MAC address or addresses that leased a specific IP address in the specified time interval.



The user should adjust the time interval enter an IP address in the IP field and press the "Lookup" button. This will populate a list of MAC addresses and the start and end time for their respective leases of the IP address. Simply double click the desired MAC to transfer it to the main dialogue.



The last extraction method allows the user to extract by circuit ID and remote ID derived from option 82

The two strings is to be entered in the same format as previously captured by the DHCP extractor.

In this way the system is not sensitive to future changes in the option 82 format and will accept different length of the two strings.

When all options are in place, click the "Retrieve Data" button, and a file dialog will open (this can take some time, don't attempt to close the dialog while waiting).

Select your desired destination and the file will be downloaded to your local machine.

The written text file is formatted as follows:

The first line contains information about the content of the file.

#Unispeed ATL 1.0; BY MAC; TARGET B; TIME 19700101 00:00:00 to 19710101 00:00:00

The file contains session info for the MAC B in the time interval from midnight January 1. 1970 to midnight January 1. 1971.

#Unispeed ATL 1.0; BY IP; TARGET 192.168.1.22; TIME 19700101 00:00:00 to 19710101 00:00:00

The file contains session info for the IP 192.168.1.22 in the same time interval as above.

#Unispeed ATL 1.0; BY IP; TARGET 209.85.175.99; TIME 20080121 10:00:00 to 20080121 23:00:00

This example contains all traffic generated against 209.85.175.99 which is a ”Google” address

#Unispeed ATL 1.0; BY Option82; TARGET 0004000A0319|0006001A6CFF3C00; TIME 20080121 10:00:00 to 20080121 15:00:0

The final example contains sessions extracted by option 82 values

The rest of the file is comma separated values, each line describing a session. The fields are in the order:

MAC/circuit ID and remote ID, start time, end time, initiating IP, initiating port, receiving IP, receiving Port, IP protocol

The file can be opened by a text editor or spreadsheet.

4.3 Blue Shield Management system configuration (temporary)

4.3.1 Overview

The Blue shield management system (BMS) is designed to manage a large number of probes from a remote location.

The BMS has provisions for:

- Configuration of Gateway properties
- Receiving data from The Probes.
- Configuration of access control
- Schedule logging tasks to the probes for IRI and CC logging
- Issue upgrades and configuration changes to the probes
- Backup data to the NAS
- Extract and Mediate log data from probes and RAS
- Provide Handover interfaces to LEA's

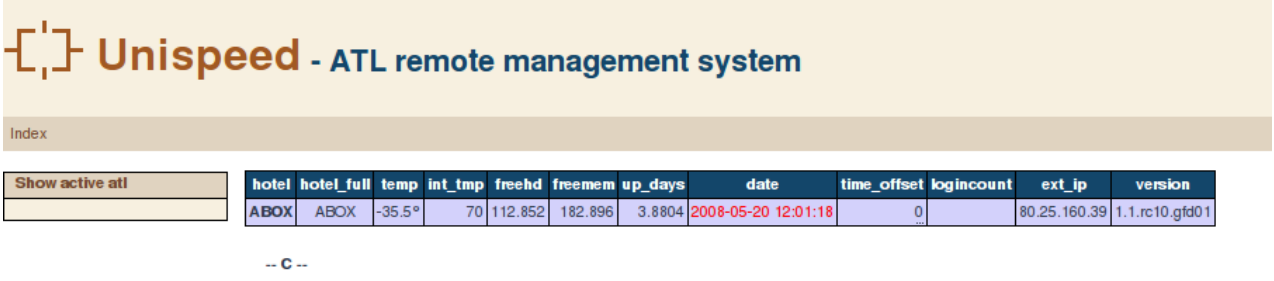
Upon delivered Unispeed will preconfigure the Blue Shield management server.

If hosted by Unispeed the system is reached by pointing a browser to the following address: https://config.unispeed/**costumer**/admin/

When receiving and IP address the probe will automatically poll the system for configuration properties, using the eth0 MAC number as identification.

4.3.1.1 Management Setup

To enter the probe configuration menu click the Gateway admin. Icon.



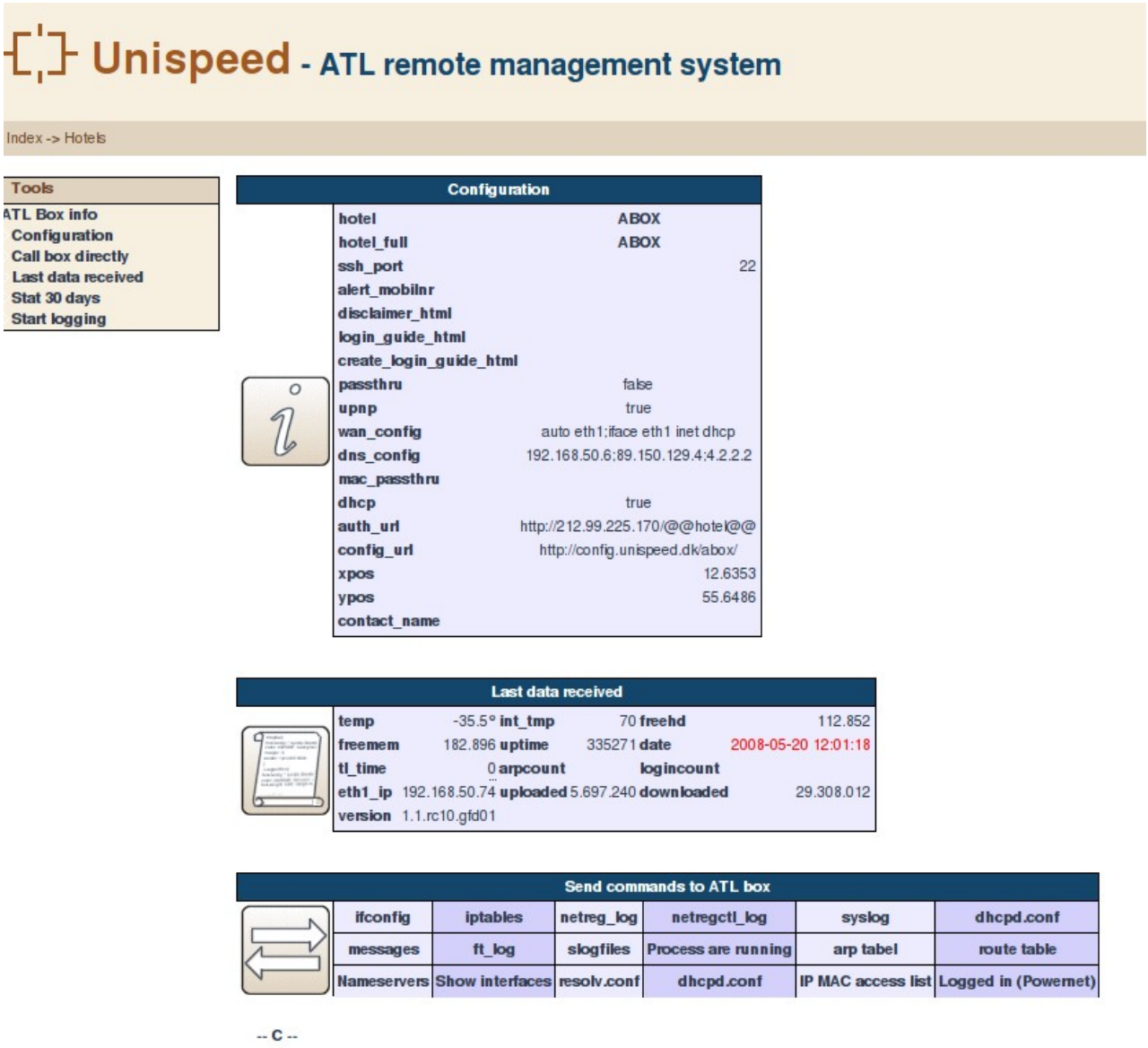
The installed probes should already be listed on the probe status page.

The status page is automatically updated every 5 minutes by the probes.

By default the probes will “check in” as “NEW”.

New probes will show as inactive until configured

Click on the relevant probe in the “hotel” column to enter the probe overview page



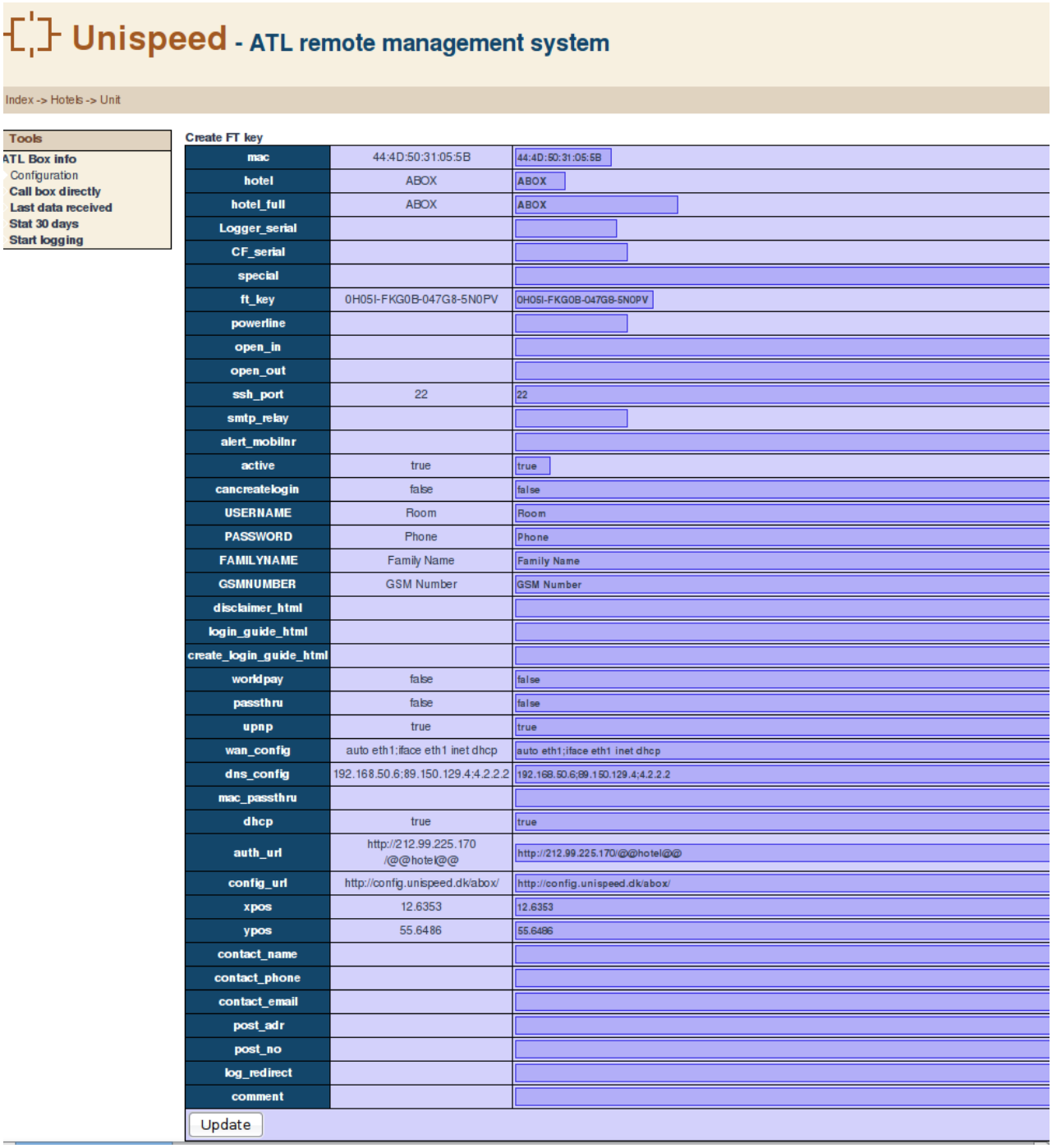
The probe overview page show the

- Current configuration of the selected probe.
- Last data set received from the probe.
- And the “Send commands to ATL box” dialogue

Short cut links are presented in the left side of the page.

The probe name (hotel) in the configuration summary, links to the Remote Authentication Server (RAS) if provided.

To configure the probe click the “i” icon to the left of the Configuration window.



Unispeed - ATL remote management system

Index -> Hotels -> Unit

Tools

ATL Box info
Configuration
Call box directly
Last data received
Stat 30 days
Start logging

Create FT key

mac	44:4D:50:31:05:5B	44:4D:50:31:05:5B
hotel	ABOX	ABOX
hotel_full	ABOX	ABOX
Logger_serial		
CF_serial		
special		
ft_key	0H05I-FKG0B-047G8-5N0PV	0H05I-FKG0B-047G8-5N0PV
powerline		
open_in		
open_out		
ssh_port	22	22
smtp_relay		
alert_mobilnr		
active	true	true
cancreatelogin	false	false
USERNAME	Room	Room
PASSWORD	Phone	Phone
FAMILYNAME	Family Name	Family Name
GSMNUMBER	GSM Number	GSM Number
disclaimer_html		
login_guide_html		
create_login_guide_html		
worldpay	false	false
passthru	false	false
upnp	true	true
wan_config	auto eth1;iface eth1 inet dhcp	auto eth1;iface eth1 inet dhcp
dns_config	192.168.50.6;89.150.129.4;4.2.2.2	192.168.50.6;89.150.129.4;4.2.2.2
mac_passthru		
dhcp	true	true
auth_url	http://212.99.225.170/@@hotel@@	http://212.99.225.170/@@hotel@@
config_url	http://config.unispeed.dk/abox/	http://config.unispeed.dk/abox/
xpos	12.6353	12.6353
ypos	55.6486	55.6486
contact_name		
contact_phone		
contact_email		
post_adr		
post_no		
log_redirect		
comment		

Update

To configure the probe enter the desired value in the right column and press the update bottom. The new values are now updated on the management server and will be polled by the probe automatically.

4.3.1.1.1 Probe configuration menu

Mac – The mac number (eth0) is the unique identifier for the probe and can not be changed

Hotel – The abbreviation for the probe location used by the RAS

Hotel Full – Full name of the probe location

Logger serial – Serial number on the probe, the entry is not used by the system

CF-serial – Serial of the flash storage card

Special – Reserved for future purpose

ft-key – the ft-key is licence key for the FT data logging system – a new key can be created by pressing the Create FT key bottom in the top left corner. The system will auto generate a key in case the probe abbreviation is changed (Hotel field)

Powerline – This entry is used to control “internet via powerline” system if installed

open-in – Enables the operator to open specific inbound ports in the firewall. Enter one or more port numbers separated by “ **;** ”

Format: 8080 192.1.1.50 8080; 1500 192.1.1.51 1500

open-out - Enables the operator to open specific outbound ports in the firewall. Enter one or more port numbers separated by “;”

ssh-port – This is the only port that needs to be open to operate the probe remotely.

smtp_relay -

alert-mobilnr – Enter one or more phone numbers that should be alerted in case of system alerts

active – Enter the desired status of the probe. Valid inputs **false** / **true**

cancreatelogin – If set to **false** the authentication system is disabled allowing open access to the internet from the LAN side. If set to **true** the probe will present a login screen in accordance with the below values. The probe must be designated on the RAS for this function to be operational.

USERNAME – Enter the text you wish to appear in front of the login method combo box **GSM NR – ROOM NR – Credit card -** reflected on the login screen

Password – Enter the text in the languish you wish to appear in front of password combo box – **Pass code** / **Access code** or similar (if GSM Number is used for authorisation the costumer will receive the code via text message.

FAMILYNAME – Use this option together with GSM Number

GSMNUMBER – If set to **GSM Number** the system will generate a pass code and sen it to the costumers Mobile phone via text message gateway – otherwise leave blank.

Additional text desired to appear on the login screen is entered in the 3 _html fields

Worldpay – Set to true if credit card verification is used otherwise false

passthrue – Set to true if the Router is open otherwise false

upnp – Set to true if upnp support is desired otherwise false

wan-config – Enter the WAN configuration properties - **Format: auto eth1; iface eth1 inet static; address 192.168.28.2; netmask 255.255.255.0; gateway 192.168.28.1**

dns-config – Enter the desired nmeservers – **Format: 212.239.22.181; 193.204.35.27**

Mac-passthru – Enter list of mac numbers with unlimited access to the internet **Format: 00:11:6e:91:2a:80;00:11:6e:91:2a:84**

dhcp – set to true if the probe shall act as dhcp server otherwise false

auth-url – The address of the RAS **Format: http://IP-adr/@@hotel@@**

config_url – The address of the management server **Format:** http://config.unispeed/abox/admin/

xpos and ypos – The LAT/LONG position of the box is entered in order to place the box on a virtual map.

log-redirect – Enter the address of the NAS if other than the management server is used for storing log data from the probes.

4.3.1.2 Probe direct command execution (call box directly)

This page gives a privileged operator the ability to control and issue commands directly to the probes via secure connection. The system bypasses the normal probe command cue. Possible actions are:

- System info calls like network configuration, running processes, route table etc.

  The netreg.log and netregctl.log is generated by the Unispeed netreg system and contains information about the users and authentication status from the RAS.

- Actions on ATL Unit

  The function can be used to force actions on a probe like reboot, reload of configuration, set NTP date, etc.

- Upgrade ATL Unit Commands

  Contains various system upgrade possibilities

- Temporary ATL Unit commands

  These commands are temporary setting and should not be used

4.3.1.3 Last data received

Summery reports from the specified probe

4.3.1.4 Stat. 30 days

30 days summary report from specified probe

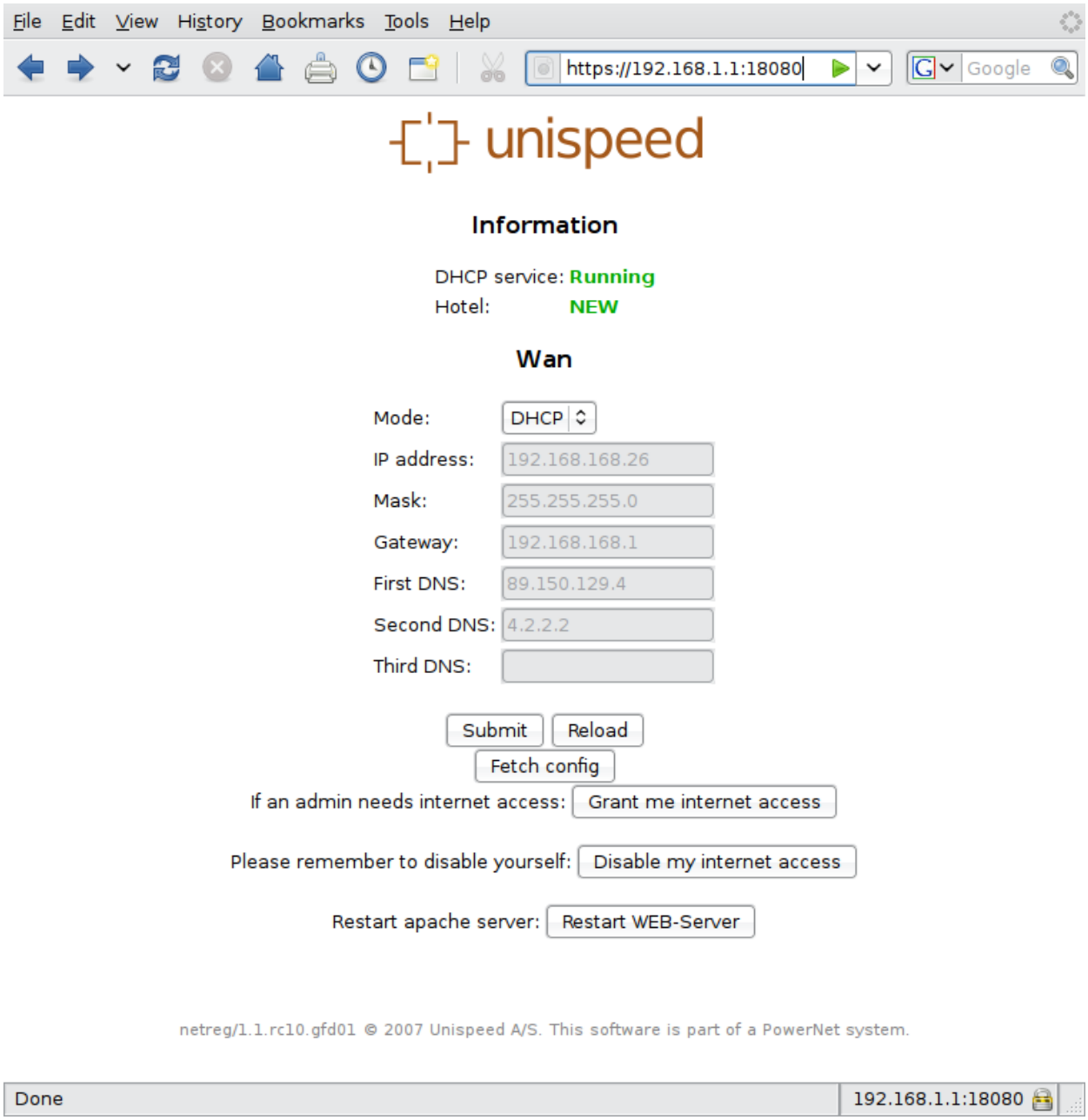
4.3.1.5 Start logging

Law enforcement “Content logging” has been moved to the Blue Shield System.

4.3.2 On-site probe access

To facilitate on-site WAN configuration and trouble-shooting the gateway probe can be accessed via secure http.

To access the probe directly point a browser to https:192.168.1.1:18080


File Edit View History Bookmarks Tools Help
https://192.168.1.1:18080
Google
unispeed
Information
DHCP service: Running
Hotel: NEW
Wan
Mode: DHCP
IP address: 192.168.168.26
Mask: 255.255.255.0
Gateway: 192.168.168.1
First DNS: 89.150.129.4
Second DNS: 4.2.2.2
Third DNS:
Submit
Reload
Fetch config
If an admin needs internet access: Grant me internet access
Please remember to disable yourself: Disable my internet access
Restart apache server: Restart WEB-Server
netreg/1.1.rc10.gfd01 © 2007 Unispeed A/S. This software is part of a PowerNet system.
Done
192.168.1.1:18080