

ICON-PEP-2.0

Icon-PEP Administration Guide

Isode

Table of Contents

Chapter 1	Icon-PEP Overview.....	1
	This chapter contains a general overview of Icon-PEP.	
Chapter 2	Initial Setup of Icon-PEP.....	5
	This chapter describes how to perform initial setup of Icon-PEP.	
Chapter 3	Configuring Icon-PEP.....	10
	This chapter describes how to configure Icon-PEP.	
Chapter 4	Operating and Monitoring Icon-PEP.....	16
	This chapter describes how to operate and monitor Icon-PEP.	
Chapter 5	General management API.....	23
	This chapter describes the web-API that allows external tools to manage Icon-PEP.	

Isode and Isode are trade and service marks of Isode Limited.

All products and services mentioned in this document are identified by the trademarks or service marks of their respective companies or organizations, and Isode Limited disclaims any responsibility for specifying which marks are owned by which companies or organizations.

Isode software is © copyright Isode Limited 2002-2023, all rights reserved.

Isode software is a compilation of software of which Isode Limited is either the copyright holder or licensee.

Acquisition and use of this software and related materials for any purpose requires a written licence agreement from Isode Limited, or a written licence from an organization licensed by Isode Limited to grant such a licence.

This manual is © copyright Isode Limited 2023.

1 Software Version

This guide is published in support of Isode Icon-PEP 2.0. It may also be pertinent to later releases. Please consult the release notes for further details.

2 Readership

This guide is intended for an administrator to set up and operate Icon-PEP.

3 How to use this guide

It is recommended that all administrators read the entire manual.

4 Typographical conventions

The text of this manual uses different typefaces to identify different types of objects, such as file names and input to the system. The typeface conventions are shown in the table below.

Object	Example
File and directory names	<i>isoentities</i>
Program and macro names	mkpasswd
Input to the system	<code>cd newdir</code>

Arrows are used to indicate options from the menu system that should be selected in sequence.

For example, **File** → **New** means to select the **File** menu and then select the **New** option from it.

5 File System placeholders

A number of directory names are given in the text, and the actual locations (below) vary depending on the target platform.

Name	Place holder for the directory used to store...	UNIX
(<i>ETCDIR</i>)	System-specific configuration files.	<i>/etc/isode/icon-pep</i>
(<i>SBINDIR</i>)	Programs run by the system administrators.	<i>/opt/isode/icon-pep/sbin</i>
(<i>LOGDIR</i>)	Log files.	<i>/var/log/isode/icon-pep</i>

6 Support queries and bug reporting

A number of email addresses are available for contacting Isode. Please use the address relevant to the content of your message.

1. For all account-related inquiries and issues: customer-service@isode.com [mailto:customer-service@isode.com]. If customers are unsure of which list to use then they should send to this list. The list is monitored daily, and all messages will be responded to.
2. To provide keys necessary to activate products, send the generated string to support@isode.com [mailto:support@isode.com] along with information on what is being evaluated or what has been purchased.
3. For all technical inquiries and problem reports, including documentation issues from customers and evaluators: support@isode.com [mailto:support@isode.com]. Customers should include relevant contact details in initial calls to speed processing. Messages which are continuations of an existing call should include the call ID in the subject line.
4. Customers may also submit support queries through the customer section of the Isode web site using the URL provided. Customers with silver or gold support may also submit support queries by telephone.
5. For all sales inquiries and similar communication: sales@isode.com [mailto:sales@isode.com].

Bug reports on software releases are welcomed. These may be sent by any means, but electronic mail to the support address listed above is preferred.

Isode sends release announcements and other information to the Isode News email list, which can be subscribed to from the address: <http://www.isode.com/company/contact.html>

7 Export controls

Icon-PEP may use TLS (Transport Layer Security) to encrypt HTTP traffic between the service and the web-browser, and also when querying an OAuth server. When TLS is enabled, Icon-PEP is subject to UK Export Controls. For some countries (at the time of shipping this release, these comprise all EU countries, United States of America, Canada, Australia, New Zealand, Switzerland, Norway, Japan), these Export Controls can be handled by administrative process as part of evaluation or purchase.

For other countries, a special Export License is required. This can be applied for only in context of a purchase order for Icon-PEP.

The TLS feature of 2.0 is enabled by a TLS Product Activation feature. This feature may be turned off, and 2.0 without this TLS feature is not export controlled. This can be helpful to support evaluation of 2.0 in countries that need a special export license. Note that when TLS is disabled, Icon-PEP is still able to forward TLS-encrypted connections such as HTTPS over S'5066 because no encryption or decryption occurs within Icon-PEP.

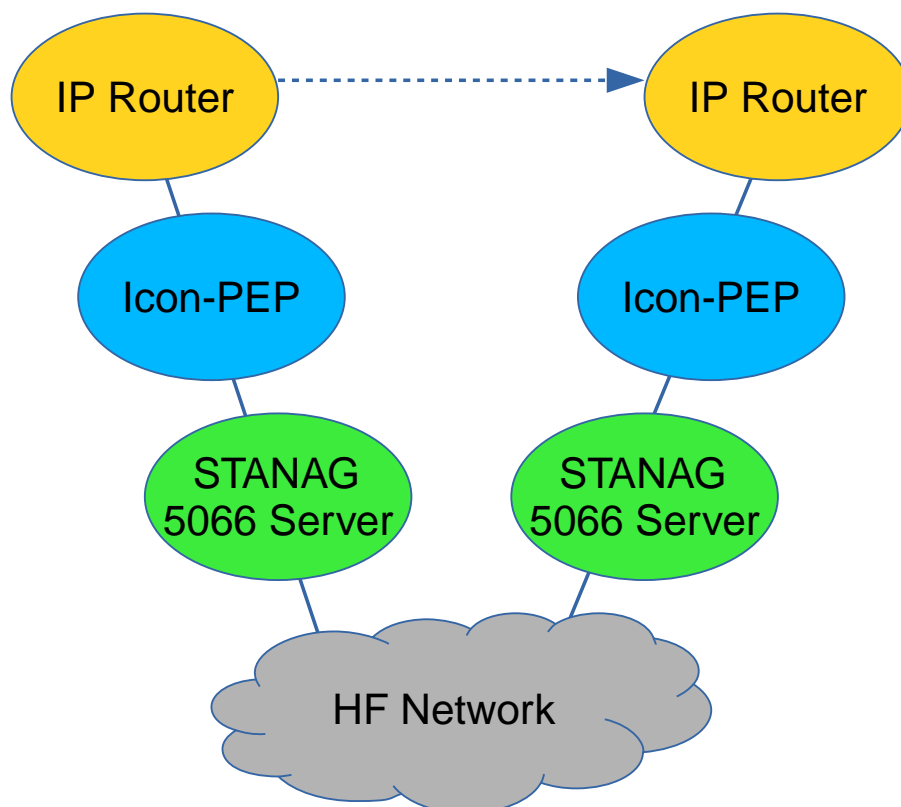
Isode strongly recommends that all operational deployments of Icon-PEP use the export-controlled TLS feature.

You must ensure that you comply with these Export Controls where applicable, i.e. if you are licensing or re-selling Isode; products. All Isode Software is subject to a license agreement and your attention is also called to the export terms of your Isode license.

Chapter 1 Icon-PEP Overview

This chapter contains a general overview of Icon-PEP.

1.1 Icon-PEP Functionality

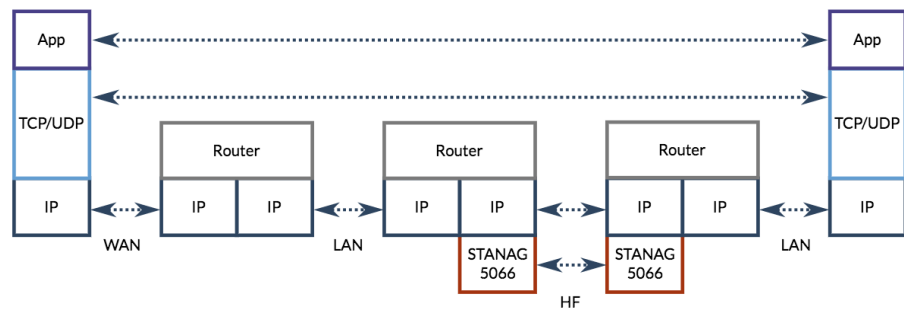


Icon-PEP enables provision of IP services over an HF network, with performance optimization for TCP and HTTP (Web) connections.

Icon-PEP operates over the STANAG 5066 HF Link layer, and connects to a STANAG 5066 server such as Isode's Icon-5066 product. Icon-PEP connects directly to an IP router, as illustrated above. Icon-PEP communicates with a peer server using standard protocols, to enable transfer of IP packets between a pair of routers.

In addition, using the NAT configuration options, remotely-initiated traffic may be proxied directly by Icon-PEP out to the local network without needing to go via an IP router. So if there is no locally-initiated traffic, the IP router might not be required.

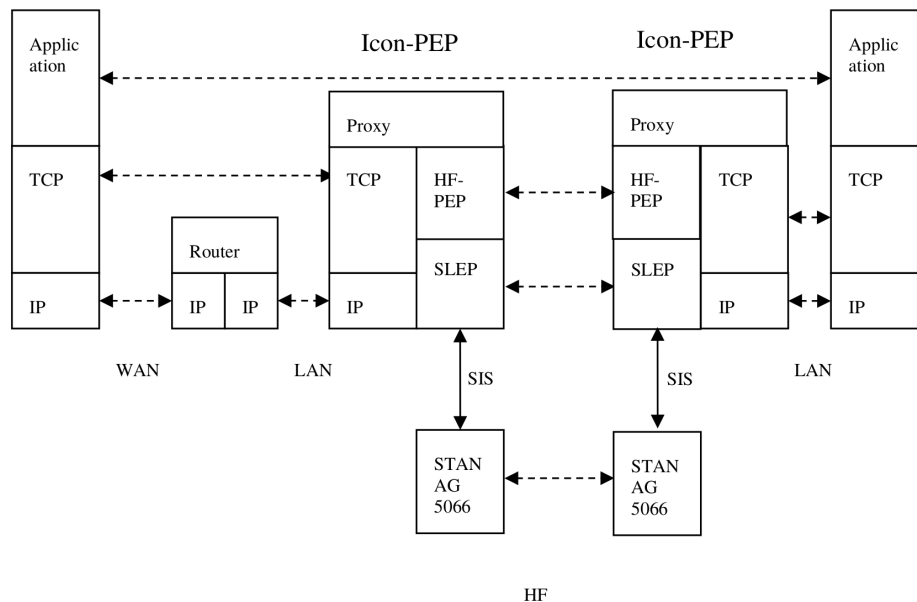
1.1.1 STANAG 5066 IP Client Service



STANAG 5066 Annex F.12 defines “IP Client” services for operating an IP subnet over HF, as shown in the diagram above. The approach is discussed in detail in the Isode white paper [Measuring and Analysing STANAG 5066 F.12 IP Client](https://www.isode.com/whitepapers/measuring-stanag5066-f12-ip-client.html) [https://www.isode.com/whitepapers/measuring-stanag5066-f12-ip-client.html].

Icon-PEP supports this protocol, which is suitable for some low volume services such as ICMP Ping, and it works acceptably for some specialized military applications and services such as DNS Lookup.

1.1.2 HF-PEP Service



Use of IP Client leads to poor performance for bulk applications and in particular for TCP and HTTP. To address this, Icon-PEP includes a PEP (Performance Enhancing Proxy) architecture to efficiently provide support.

In this TCP Proxy architecture, an application is communicating over TCP, running over IP in the normal manner. The TCP connection from each application is peered with Icon-PEP, rather than the other application. Icon-PEP then communicates using the HF-PEP protocol specified in [HF-PEP: STANAG 5066 TCP Performance Enhancing Proxy Protocol \(S5066-APP9\)](https://www.isode.com/whitepapers/S5066-APP9.html) [https://www.isode.com/whitepapers/S5066-APP9.html].

HF-PEP operates over SLEP (SIS Layer Extension Protocol), specified in [S5066-APP3](https://www.isode.com/whitepapers/S5066-APP3.html) [https://www.isode.com/whitepapers/S5066-APP3.html]. SLEP provides the Stream Services used by HF-PEP. SLEP communicates over STANAG 5066, using the local STANAG

5066 SIS (Subnet Interface Service) to connect. STANAG 5066 peers communicate over an HF network, as shown.

Icon-PEP can multiplex TCP connections over a single HF link, so that a single STANAG 5066 SAP can be shared by multiple TCP connections and multiple applications running over TCP.

Further details on HF-PEP and performance measurements are provided in the Isode white paper “Measuring and Analysing HF-PEP for TCP communication and Web Browsing over HF”.

1.1.3 Connections to STANAG 5066 Server

Icon-PEP connects to one or more STANAG 5066 servers using one or more connections using the STANAG 5066 SIS protocol. Two types of SIS connection are supported:

1. IP Client (default SAP: 9)
2. HF-PEP (default SAP: 13)

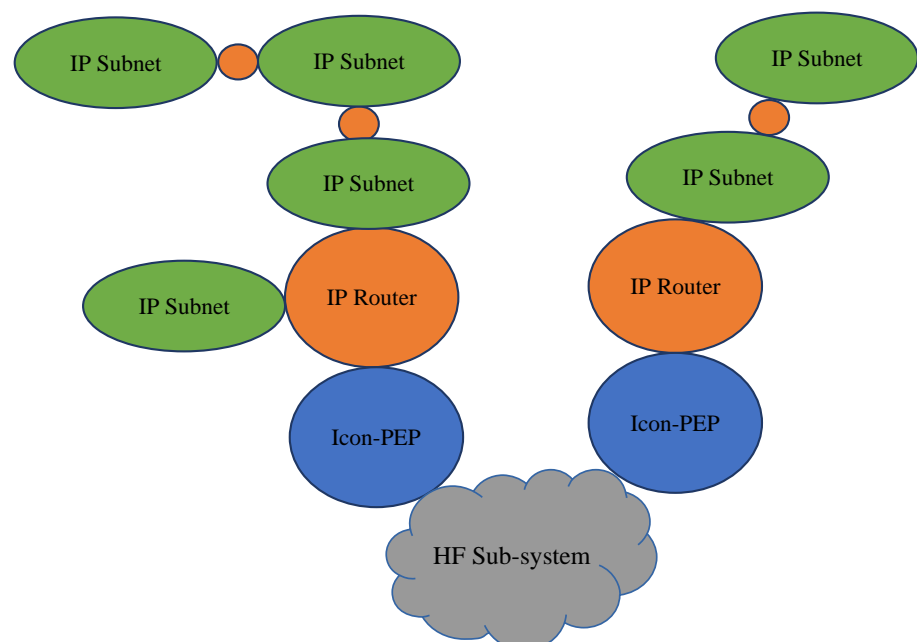
1.1.4 Connections to Router (GRE)

Icon-PEP communicates with one or more IP Routers using Generic Routing Encapsulation (GRE), specified in RFC 2784. GRE provides a simple mechanism to exchange packets between routers over IP, often described as a “GRE Tunnel”.

Icon-PEP terminates the GRE tunnel from a connected IP router. This means that there is no requirement for a peer system to use GRE. Routers commonly monitor GRE tunnel availability using ICMP Ping; Icon-PEP responds to these pings.

GRE is widely supported by Edge routers, and it is anticipated that Icon-PEP will generally connect to the deployed router. For subnets or single hosts that do not deploy a router, or where the deployed router does not support GRE, it is possible to use a software router, such as the one provided on many Linux systems or a product such as pfSense running in a virtual machine. Alternatively, for shore stations that relay incoming connections from HF to the LAN but do not allow initiation of outgoing connections to HF, NAT mode may be used which does not require a router.

1.1.5 IP Routing and Deployment Model



The IP world comprises multiple IP Subnets, interconnected by IP routers. The routing configuration of an IP Router enables any IP packet to be correctly routed to its destination host via the IP Subnet to which the host is attached.

Icon-PEP core model enables connection of a pair of routers over HF. Icon-PEP simply takes a packet from the local router and sends it over HF to the peer IP router. This is an entirely mechanical function of switching data between STANAG 5066 and the local IP Router.

1.1.6 Icon-PEP Routing

The architecturally simple model described above requires that an IP Router connecting over HF to multiple peer routers requires an instance of Icon-PEP for every peer. This would add significantly to deployment complexity and in practice this approach is rarely needed.

Icon-PEP includes a static IP routing capability. This can be used for systems where all but one node has a known fixed list of IP subnets. One node can be treated as a default route. This reflects a typical HF configuration, with multiple Mobile Units with a known set of IP Subnets, using a default route to a single shore system, which can have complex IP connectivity.

For performance reasons, it is desirable to avoid use of dynamic routing protocols over HF, so this approach is efficient.

Chapter 2 Initial Setup of Icon-PEP

This chapter describes how to perform initial setup of Icon-PEP.

2.1 Installation

Installation of Icon-PEP is covered in the release notes.

2.2 Operation as a Service

Icon-PEP can be operated as a Linux systemd service using the **systemctl** service management capability. This is the recommended way to run Icon-PEP for both initial configuration and deployment. To start Icon-PEP as a service, use the following command:

```
systemctl start iconpepd
```

2.3 Operation from Command Line

Icon-PEP can be run from a Linux command prompt. This may be helpful in some cases for remote debugging. See [Section 4.9, “Command Line Monitoring”](#) for details of the text user interface (TUI).

First stop the Icon-PEP systemd service if it is running:

```
systemctl stop iconpepd
```

Then run Icon-PEP manually using the following command:

```
(SBINDIR)/isode.iconpepd -T
```

Use **Ctrl-C** to stop Icon-PEP when running on the terminal.

Alternatively Icon-PEP may be run with just terminal logging output using the following command:

```
(SBINDIR)/isode.iconpepd -C
```

A usage message showing other command-line options can be obtained by running Icon-PEP with **-?**:

```
(SBINDIR)/isode.iconpepd -?
```

2.4 Connecting with a browser

By default Icon-PEP listens on all interfaces on port 17636 for HTTPS connections from a web browser. However if TLS has been disabled by the activation, then Icon-PEP will expect HTTP connections instead of HTTPS. In addition, the listening interface and port may be changed in the configuration.

Note that if activation or a config modification change the protocol, IP address or port that Icon-PEP uses for web access, then it will be necessary to reload the page, or correct the URL to match the new settings, before continuing to interact with the web-UI.



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **localhost**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

Go Back (Recommended)

Advanced...

localhost:17636 uses an invalid security certificate.

The certificate is not trusted because it is self-signed.

Error code: [MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT](#)

[View Certificate](#)

Go Back (Recommended)

Accept the Risk and Continue

If no private key or public certificate chain have yet been configured, then Icon-PEP will create a temporary self-signed certificate in order to support HTTPS. Your browser will warn you that this is not signed by a known authority. This is expected. To proceed you should select the "advanced" option in the browser and choose to trust the temporary certificate.

So in its initial default state, you may connect to Icon-PEP by entering `https://localhost:17636/` into your browser, replacing `localhost` with the name or IP-address of the machine hosting Icon-PEP if it is not `localhost`.

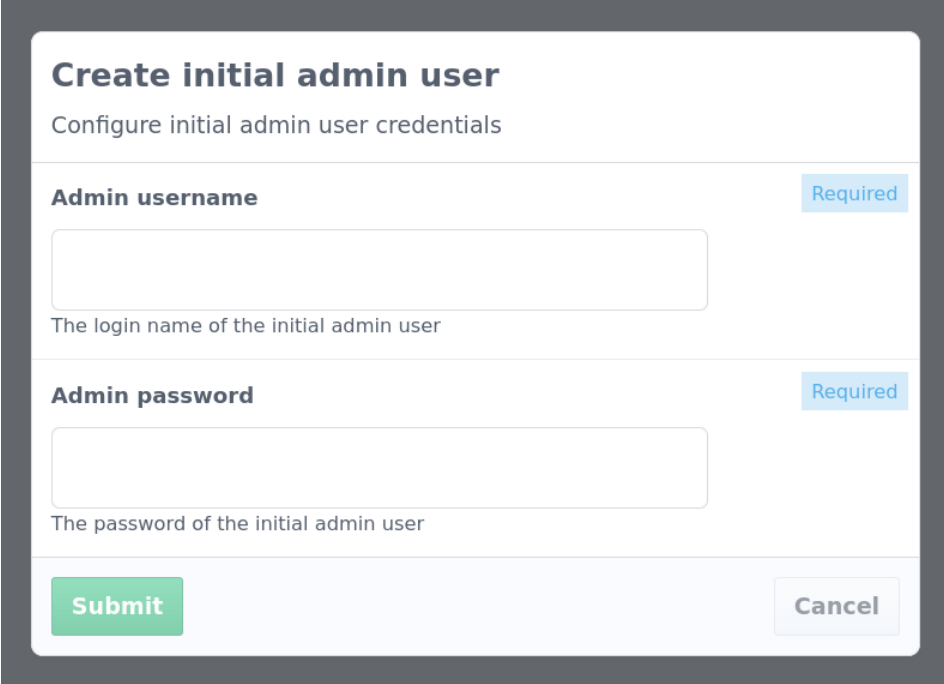
2.5 Recovering from a broken configuration

During the initial setup it is possible to lock yourself out of the web-UI by entering incorrect values. The files set up by initial configuration are found in (*ETCDIR*). If you make a mistake and wish to revert to the unconfigured state, stop Icon-PEP, delete the relevant files under (*ETCDIR*) and then start up Icon-PEP once more.

In the specific case of being locked out due to misconfiguring OAuth, you may recover from this situation without deleting the entire config as follows: First stop Icon-PEP, then edit the (*ETCDIR*)/*pep.json* file and change the "enable_oauth" setting from `true` to

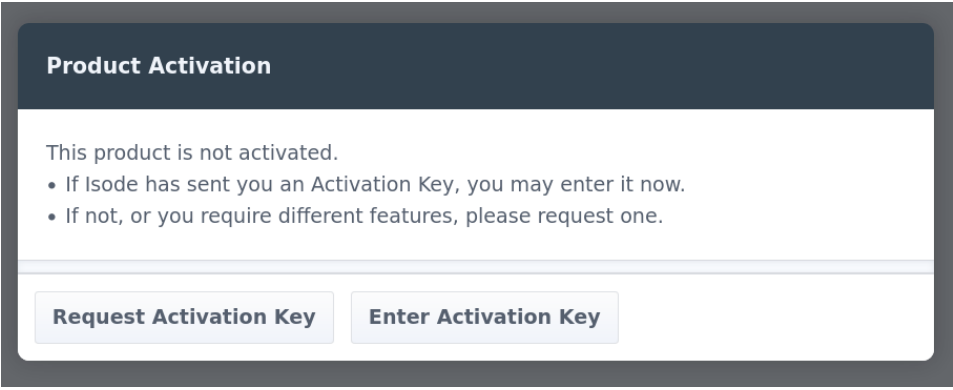
false, save it, and start up Icon-PEP again. Then reload the web-page and you should be able to connect as before and fix the settings.

2.6 Setting an admin password

A dialog box titled "Create initial admin user" with the subtitle "Configure initial admin user credentials". It contains two input fields: "Admin username" and "Admin password". Both fields have a "Required" label to their right. Below the "Admin username" field is the text "The login name of the initial admin user". Below the "Admin password" field is the text "The password of the initial admin user". At the bottom of the dialog are two buttons: "Submit" (green) and "Cancel" (grey).

Choose a username and password. These will be required for all future logins into this web-UI.

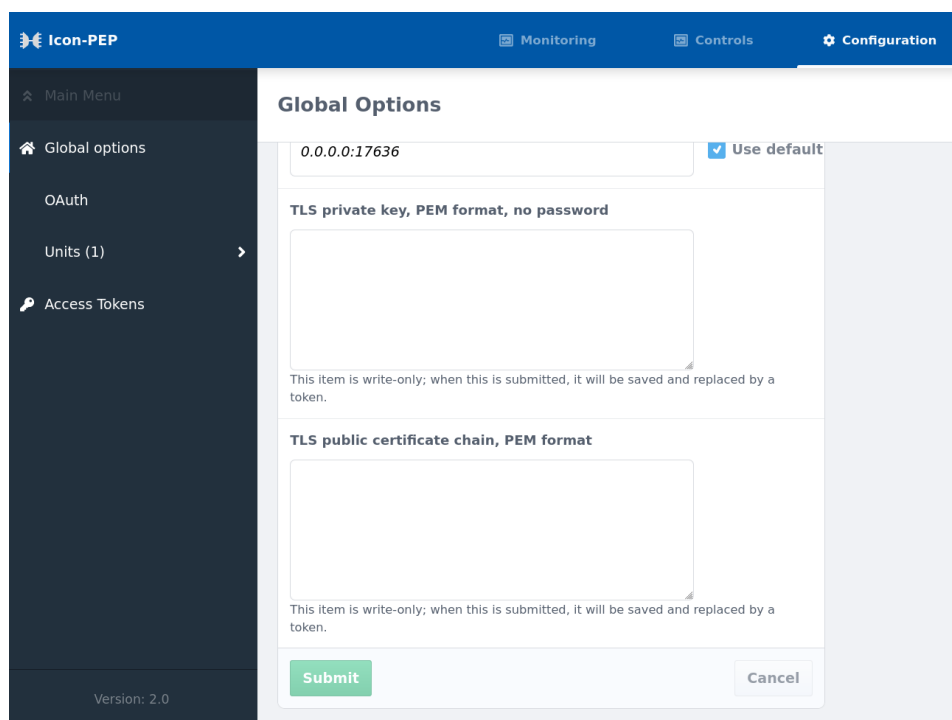
2.7 Product Activation

A dialog box titled "Product Activation". It contains the text "This product is not activated." followed by a bulleted list: "• If Isode has sent you an Activation Key, you may enter it now." and "• If not, or you require different features, please request one." At the bottom of the dialog are two buttons: "Request Activation Key" and "Enter Activation Key".

In this dialog, first choose **Request Activation Key**, and send the activation request to Isode. When the activation key has been provided, choose **Enter Activation Key** and paste in the key. This will activate Icon-PEP. If the activation does not include TLS, then you will have to change the browser's URL from https: to http: in order to continue using the web-UI.

To check the activation status or to reactivate or deactivate Icon-PEP, go to the top-right menu and select **About Icon-PEP**. **Update Key** and **Deactivate** buttons provide the necessary functions.

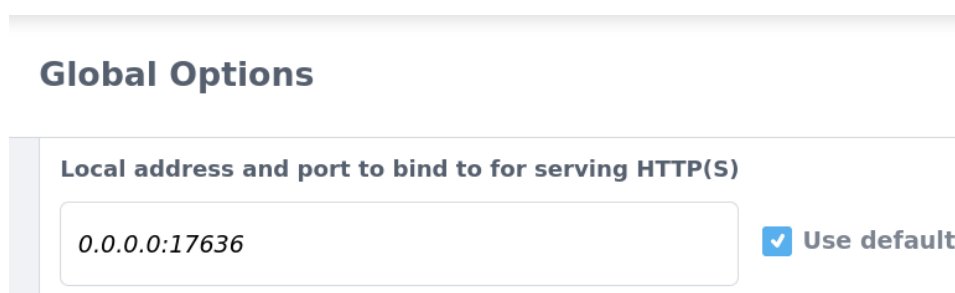
2.8 Configuring a TLS key and certificate



The screenshot shows the Icon-PEP web interface. The top navigation bar includes 'Monitoring', 'Controls', and 'Configuration'. The left sidebar has 'Main Menu', 'Global options', 'OAuth', 'Units (1)', and 'Access Tokens'. The 'Global Options' section is active, displaying a form for TLS configuration. The form includes a text input for '0.0.0.0:17636' with a 'Use default' checkbox. Below this are two large text areas for 'TLS private key, PEM format, no password' and 'TLS public certificate chain, PEM format'. Each text area has a note: 'This item is write-only; when this is submitted, it will be saved and replaced by a token.' At the bottom of the form are 'Submit' and 'Cancel' buttons. The version '2.0' is shown in the bottom left corner.

By default, Icon-PEP will operate using a temporary self-signed certificate which changes each time Icon-PEP restarts its web service. If you wish to provide a proper private key and public certificate chain so that HTTPS can operate without a warning in the browser, then go to the top level of the **Configuration** under **Global Options** and paste in both the private key and the public certificate chain in PEM format, submit and then reload the page. Note that the private key must not be protected with a passphrase. The certificates are replaced by tokens in the UI, and the sensitive content is saved to disk in an encrypted and machine-locked format. If there are any problems with the PEM files then errors or warnings will be visible in the log file, found under (*LOGDIR*).

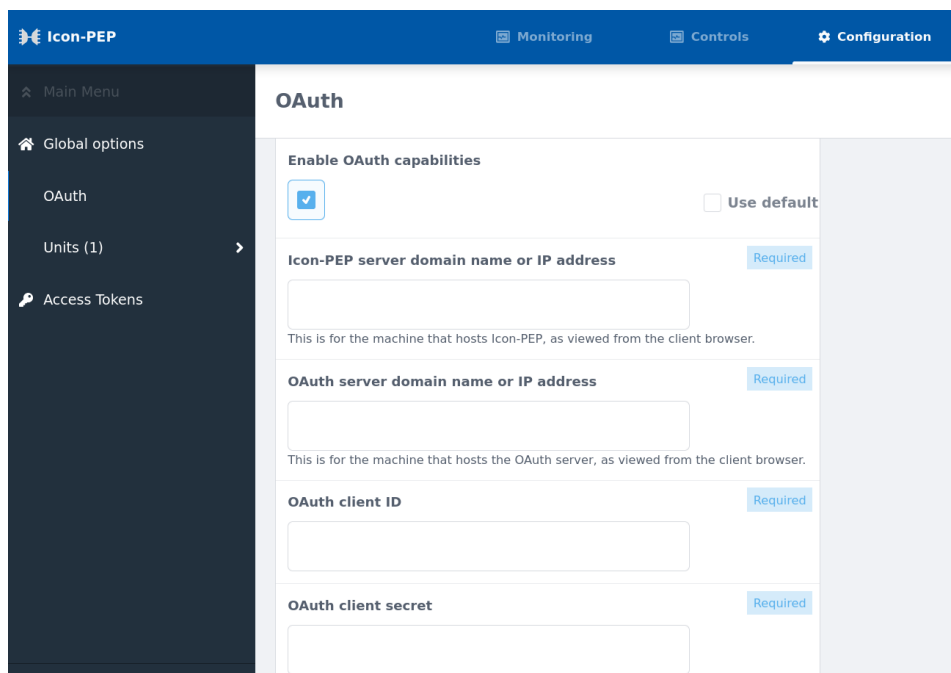
2.9 Changing HTTP(S) listening port



The screenshot shows the 'Global Options' section of the Icon-PEP web interface. It features a form titled 'Local address and port to bind to for serving HTTP(S)'. The form contains a text input field with the value '0.0.0.0:17636' and a 'Use default' checkbox. The 'Submit' button is visible at the bottom right of the form.

If you wish to have Icon-PEP listen for HTTP(S) connections on a different port, or to listen only on one interface, then go to **Configuration, Global Options** and visit the **Local address ...** field. The default IP of 0 . 0 . 0 . 0 listens on all interfaces. To listen on just one interface, use the IP address that the host machine has on that interface. After submitting the new IP and port number, change the URL in the browser to match the same settings and reload the page.

2.10 OAuth configuration



The screenshot shows the Icon-PEP web interface with the 'Configuration' tab selected. The left sidebar contains a 'Main Menu' with options: 'Global options', 'OAuth', 'Units (1)', and 'Access Tokens'. The 'OAuth' option is currently selected. The main content area is titled 'OAuth' and contains the following configuration fields:

- Enable OAuth capabilities:** A checkbox that is checked. To its right is a link 'Use default'.
- Icon-PEP server domain name or IP address:** A text input field. To its right is a 'Required' label. Below the field is a note: 'This is for the machine that hosts Icon-PEP, as viewed from the client browser.'
- OAuth server domain name or IP address:** A text input field. To its right is a 'Required' label. Below the field is a note: 'This is for the machine that hosts the OAuth server, as viewed from the client browser.'
- OAuth client ID:** A text input field. To its right is a 'Required' label.
- OAuth client secret:** A text input field. To its right is a 'Required' label.

OAuth centralizes login credential handling, meaning that no login-related secrets have to be kept by Icon-PEP. If you wish to use OAuth, fill in the configuration in the OAuth tab with details provided by the OAuth server. After clicking **Submit** to apply an OAuth configuration, Icon-PEP will restart its web service, so it is necessary to reload the page in order to continue using the UI.

Chapter 3 Configuring Icon-PEP

This chapter describes how to configure Icon-PEP.

Icon-PEP should be configured through the **Configuration** tab of the web-UI. The configuration is saved to a single JSON file stored in *(ETCDIR)/pep.json*

3.1 Units

Each "Unit" is like a separate independent running instance of Icon-PEP. Most sites will only require a single Unit. However a more complicated shore station using several S'5066 server nodes to access HF will need to set up a different Unit for each S'5066 server.

To add a Unit, go to the **Units** entry in the left-hand pane of the **Configuration** tab, and select **Add...** The top-level configuration for a Unit can be made at Unit creation, or changed later if required. It is as follows:

The screenshot shows the Icon-PEP web-UI with the 'Configuration' tab selected. The left-hand pane shows a menu with 'Main Menu', 'Units (1)', and 'Unit 0'. The 'Units (1)' entry is expanded, showing 'Unit 0'. The main content area is titled 'Add new item' and contains a form for adding a new Icon-PEP unit. The form has the following fields:

- Label to identify unit** (Required): A text input field.
- S'5066 server IP address** (Required): A text input field.
- S'5066 server SIS port number** (Required): A text input field.
- Simplified NAT shore proxy**: A checkbox with the label 'Use default' checked. Below it, a note states: 'Routing and node addresses do not need to be configured in this mode.'
- Node address** (Required): A text input field. Below it, a note states: 'S'5066 node address of this node'.

3.1.1 S'5066 server details

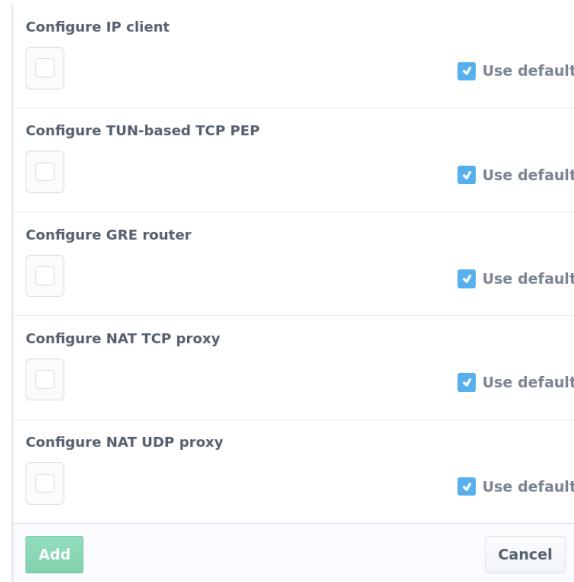
S'5066 server IP address and **S'5066 server SIS port number** give the socket address for connecting to the S'5066 server. **Node address** gives the S'5066 node address represented by the S'5066 server.

Node addresses are expressed as a dotted-quad, like an IPv4 address. Where the first number of the dotted-quad is below 16, leading zero half-bytes are stripped off and the remaining half-bytes are taken to be the S'5066 node address. So the shortest S'5066 node address would be in the range 0.0.0.0 to 0.0.0.15, which corresponds to a single half-byte in S'5066 addressing. If the first number is 16 or over, that represents either a group address or an unnormalized node address, but these are unlikely to be required in this application.

3.1.2 Simplified NAT shore proxy

This enables a simplified configuration for a shore station that does not permit outgoing connections from the shore to the mobile units. It only accepts incoming TCP, UDP and ICMP ping requests from mobile units, which it proxies out to the local network in the style of NAT. This configuration does not require HF routing tables to be set up, and will accept traffic from any valid S'5066 node or IP address.

3.1.3 Subsection selection



The screenshot shows a dialog box titled "Configure IP client" with five subsections, each with a checkbox and a "Use default" button:

- Configure IP client**: ☐ Use default
- Configure TUN-based TCP PEP**: ☐ Use default
- Configure GRE router**: ☐ Use default
- Configure NAT TCP proxy**: ☐ Use default
- Configure NAT UDP proxy**: ☐ Use default

At the bottom, there are "Add" and "Cancel" buttons.

3.1.3.1 Configure IP Client

This enables S'5066 Annex U "IP Client" functionality, both for incoming and outgoing IP traffic. This relays IP packets directly over HF without any performance enhancement.

3.1.3.2 Configure TUN-based TCP PEP

This enables performance enhancement for any protocol carried over TCP (including HTTP and HTTPS), both for incoming and outgoing connections. TCP connections are terminated by Icon-PEP and the raw stream data is passed over HF using an HF-optimised protocol. When enabled alongside "IP Client", this takes only the TCP traffic, leaving all other traffic for IP Client to handle.

This has one required field to fill in: **TUN device IPv4 subnet**. The suggested value of 172.30.0.0/16 is fine unless that will clash with one of the subnets used on the local network. If IPv6 is required, this can be configured later.

3.1.3.3 Configure GRE router

This enables the connection to the local network via a GRE tunnel to a router. This is required for traffic to flow, unless only NAT options are configured.

This has one required field to fill in: **Local IP address to bind GRE listener to**. This should be the host machine's IP address on the network interface that will be used to communicate with the GRE router. This is the IP address that the router will be configured to send GRE traffic to.

3.1.3.4 Configure NAT TCP proxy

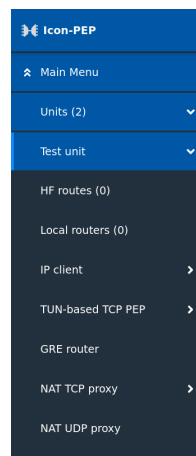
This may be used to forward incoming TCP PEP connections directly to the local network. The TCP connection is made directly from Icon-PEP, giving the appearance of NAT, and so this doesn't require a GRE router. Note that this does not permit TCP connections to be

initiated from the local network. This cannot be used at the same time as TCP PEP, since it performs the same function but in a different way.

3.1.3.5 Configure NAT UDP proxy

This may be used to forward IP Client UDP exchanges and ICMP pings incoming from HF to the local network. All other IP Client traffic is dropped. The requests are made directly from Icon-PEP in the style of NAT, so a GRE router is not required. Note that this does not permit UDP or ping requests to be initiated from the local network and sent to remote networks, but local responses to incoming UDP packets or ping requests are captured and returned to the originator over HF.

3.2 Configuration subsections



Most of the configuration can be left with the default values, and is not described here. Certain subsections such as SLEP have a lot of tunable parameters. In general it is safest to leave these parameters as they are unless a problem has arisen and been thoroughly analysed and Isode support agrees that modifying those parameters will help resolve it.

The following subsections however are required for correct operation, or may be necessary in certain deployments.

3.2.1

HF route configuration

The screenshot shows the Icon-PEP Configuration interface. On the left is a sidebar menu with options: Main Menu, Units (2), Unit 0, HF routes (2), default, and 10.8.2.0/24. The main content area is titled '10.8.2.0/24' and contains a configuration form. At the top of the form is a note: 'Any outgoing IP packet which matches the given subnet is sent to ...'. Below this are three fields: 'IP subnet, or "default"' with the value '10.8.2.0/24', 'HF node-address' with the value '4.0.0.2', and 'Notes' which is empty. There is a 'Use default' checkbox which is checked. At the bottom of the form are 'Submit' and 'Cancel' buttons.

Routing over HF is determined by a fixed mapping table between IP subnets and S'5066 node addresses. When an IP address is looked up, if it matches ones of the subnets, then the corresponding node address is used to send out the traffic. If it matches none of the subnets but a "default" entry is present then the corresponding default node address is used. This "default" route would typically be for a shore station that connects to the wider shore network. However if no route matches then the packet is regarded as unroutable and will be dropped, and a warning will appear in the logs.

Subnets are specified in standard IPv4 or IPv6 network address/netmask format, such as 10.0.2.0/24. Each subnet is associated with a node identified by its S'5066 address. Multiple subnets may be associated with a node.

The routing table must include one or more entries for the local node as well as for all remote nodes. One model of deployment of routing tables is to copy the same routing table to all nodes, which avoids the possibility of packets being delivered somewhere where the return packets will be unroutable. The routing table is also used to check incoming and outgoing traffic. If the IP address on traffic doesn't correspond to the expected node address for that IP address, the traffic is rejected with a warning in the logs, since any return traffic along the same path would be unrouteable.

3.2.2 Local routers configuration

The screenshot shows the 'default' configuration page for local routers. The left sidebar contains a menu with 'Main Menu', 'Units (2)', 'Unit 0', 'Local routers (1)', and 'default'. The main content area is titled 'default' and contains a form with the following fields:

- IP subnet, or "default"**: A text box containing 'default'. A 'Required' label is to the right.
- Router used to access that subnet**: A text box containing '10.0.0.3'. A 'Required' label is to the right.
- Notes**: A text box with a 'Use default' checkbox.
- Submit** and **Cancel** buttons at the bottom.

Routing to the local network over GRE tunnels is done via this table. Typically there will be just one entry, with `default` for the IP subnet, and the IP address of the GRE router for the **Router**. However if the local network configuration is more complicated, it is possible set up several entries so that traffic for different IPv4 or IPv6 subnets is sent to different GRE routers accordingly.

3.2.3 IP Client Traffic Rules configuration

The screenshot shows the 'Reject Spotify P2P' configuration page for IP client traffic rules. The left sidebar contains a menu with 'Main Menu', 'Units (2)', 'Unit 0', 'IP client', 'Traffic rules (1)', and 'Reject Spotify P2P'. The main content area is titled 'Reject Spotify P2P' and contains a form with the following fields:

- Label to identify traffic rule**: A text box containing 'Reject Spotify P2P'. A 'Required' label is to the right.
- DSCP match**: A section with a '+ Add item' button and a note: 'If non-empty, rule matches only if the DSCP value matches one of the given values. [More...](#)'
- Protocol and destination port match**: A text box containing 'udp:57621' and a close button (X).

Traffic rules allow blocking and selection of priority and other settings for outgoing IP Client packets. The first rule that matches is used. If no rule matches then the packet is allowed to pass with default settings. Each rule may match on any of DSCP, protocol and destination port, source IP subnet and/or destination IP subnet. On matching, the packet is dropped if **Drop packet** is enabled. Otherwise the provided SIS priority, ARQ and in-order settings are applied.

3.2.4 TUN-based TCP PEP

Icon-PEP Configuration page for TUN-based TCP PEP. The left sidebar shows the navigation menu with 'TUN-based TCP PEP' selected. The main content area has a title 'TUN-based TCP PEP' and a form with three sections:

- TUN device IPv4 subnet** (Required): 172.30.0.0/16. Subnet to use for the TUN device for IPv4 traffic. [More...](#)
- TUN device IPv6 subnet**: Subnet to use for TUN device for IPv6 traffic. [More...](#)
- Connection limit**: If specified, then Icon-PEP aborts any new incoming TCP connection from the LAN once the given number of simultaneous connections is reached, until it drops back again. [More...](#)

To support IPv6 TCP connections, provide a value for **TUN device IPv6 subnet**. Also you may wish to specify a **Connection limit** to limit the number of simultaneous outgoing TCP connections.

The **Traffic Rules** section allows blocking of outgoing TCP connections and selection of priority and compression. The first rule that matches is used. If no rule matches then the connection is allowed using default settings. Rules may match on destination port, source IP subnet and/or destination IP subnet.

3.2.5 GRE router configuration

Icon-PEP Configuration page for GRE router. The left sidebar shows the navigation menu with 'GRE router' selected. The main content area has a title 'GRE router' and a form with two sections:

- Local IP address to bind GRE listener to** (Required): 10.0.0.9
- Ping-intercept subnets**: 10.8.2.1/32. [+ Add item](#)
Intercept and immediately reply to pings addressed to these subnets, without passing them over HF

Some routers send pings over the GRE tunnel to check that the other end is alive, using “internal” addresses. It is inefficient to pass these over HF, so these should be intercepted and replied to locally. Set this up using the **Ping-intercept subnets** field. These subnets will typically cover a single IP address, so the subnet mask will be /32.

Chapter 4 Operating and Monitoring Icon-PEP

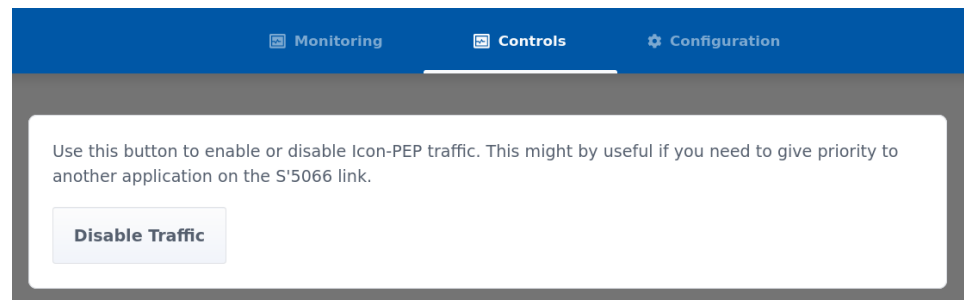
This chapter describes how to operate and monitor Icon-PEP.

4.1 Echo server

For testing, when TCP PEP or NAT TCP is enabled on all the Icon-PEP servers, each server provides a built-in TCP echo server on port 7 of its remote IP address. When a TCP client such as **telnet** connects to port 7 of an IP address which is handled by another node, the traffic goes out over HF to that node, and then Icon-PEP on that node echoes the data back again over TCP. This provides a test that transmission over HF to that node is operating correctly, without having to set up any services on that remote network to test against. For example:

```
telnet 10.0.2.1 7
```

4.2 Enable/disable control



Under **Controls** there is a single control that may be used for enabling or disabling traffic. This may be useful when the S'5066 connection needs to be kept free for higher-priority traffic from another application. This stops Icon-PEP from sending new data. Any outstanding SLEP connections are shut down nicely, however, so there may still be a little bit of traffic as these connections terminate.

4.3 TCP monitoring

This display shows Active and recently closed TCP Connections

Summary

Open Connections: 0
Recently Closed Connections: 1

Page 1 of 1

Tcp Connection #19 [More Info](#)

Opened: 08:09:23 11:44:45
Duration: 00:24

Source (HF) : 10.8.2.1:48718
Dest (LAN) : 54.170.59.182:80

From HF: 0
To HF: 14,550

Type	Method	Hostname/Path	Code	Size
HttpRequest	GET	hf-browse.com/military-...	200	14,225

The TCP monitoring page shows the status of all TCP connections passing through when in the TCP PEP or NAT TCP mode of operation. For HTTP connections, details of the request or response are also available. The **Pause** allows the display to be paused. The layout buttons to the right of **Pause** allow different display styles to be selected. When there are a large number of TCP connections active or recently closed, you may need to use the page arrows to find the connection that you are interested in.

4.4 DNS monitoring

DNS Queries

Time	Type	Client IP	Server IP	Record	Name	Answer
08:09:23 11:44:45	DnsAnswer	10.8.2.1	8.8.8.8:53	A	hf-browse.com	54.170.59.182
08:09:23 11:44:45	DnsQuery	10.8.2.1	8.8.8.8:53	AAAA	hf-browse.com	
08:09:23 11:44:45	DnsQuery	10.8.2.1	8.8.8.8:53	A	hf-browse.com	
08:09:23 11:44:45	DnsQuery	10.8.2.1	172.20.0.22:53	AAAA	hf-browse.com	

The DNS monitoring page shows the contents of all DNS requests and responses passing through the server. DNS usually uses UDP, but for larger requests it may also use TCP. TCP will be monitored only if the server is in the TCP PEP or NAT TCP mode of operation. The **Pause** button allows the display to be paused.

4.5 GRE tunnel monitoring

The screenshot shows the 'Monitoring' tab of the Icon-PEP interface. The 'GRE Tunnel' section is active, displaying a summary of traffic data. A 'Pause' button is visible in the top right corner. The interface includes a 'Batch duration' selector with options: None, 2 mins (selected), 5 mins, and 10 mins. Below this is a table showing traffic data grouped by route.

Time	Source	Dest	Protocol	To HF	From HF
08:09:23 11:58:25	54.170.59.182:80	10.8.2.1:54402	TCP	20	20
08:09:23 11:58:18	8.8.8.8	10.8.2.1	ICMP_3_3	220	0
08:09:23 11:58:09	54.170.59.182:80	10.8.2.1:54402	TCP	100	5,962
08:09:23 11:58:08	8.8.8.8:53	10.8.2.1:50449	UDP	78	164

This shows a summary of all traffic passing over the GRE tunnel. This may include traffic which is subsequently filtered out by traffic rules. The **Pause** button allows the display to be paused.

4.6 IP Client monitoring

MonitoringControlsConfiguration

IP ClientPaused

This view gives an overview of all data passing from Icon-PEP to an associated STANAG 5066 server using IP Client. Note that this excludes TCP traffic, which will be sent using SLEP (SIS Layer Extension Protocol), so it gives an easy way to monitor non-TCP traffic.

This displays a list of rows, one per route summarising traffic grouped in periods with upper bound limited by the "Batch duration" selected below.

Batch duration

Group traffic data with the same route by the selected duration:

None

2 mins

5 mins

10 mins

Time	Source	Dest	Protocol	To HF	From HF
08:09:23 12:06:31	54.170.59.182	10.8.2.1	ICMP_8_0	1,260	0
08:09:23 12:06:23	8.8.8.8	10.8.2.1	ICMP_3_3	260	0
08:09:23 12:06:16	54.170.59.182	10.8.2.1	ICMP_8_0	672	0
08:09:23 12:06:08	8.8.8.8:53	10.8.2.1:47714	UDP	118	204

This shows a summary of all IP Client traffic passing through the server. If TCP PEP is enabled, then this will not include TCP traffic. The **Pause** button allows the display to be paused.

4.7 Logging display

MonitoringControlsConfiguration

LoggingPaused

```
11:43:35 11 : AUDIT :: Init : {"addr":"127.0.0.1","port":5066}
11:43:35 11 : AUDIT :: BindAccept : {"mtu":2048}
11:43:35 07 : AUDIT :: Bound : {"mtu":2048}
11:43:35 09 : AUDIT :: BindAccept : {"mtu":2048}
11:43:35 09 : AUDIT :: Init : {"addr":"127.0.0.1","port":5066}
11:43:35 10 : AUDIT :: Init : {"sapid":2,"ext":0}
11:43:35 11 : OPEN :: SisClient : {"parent":10}
11:43:35 07 : AUDIT :: Init : {"subnet_v4":"172.30.0.0/16"}
11:43:35 10 : OPEN :: Slep : {"parent":7}
11:43:35 09 : OPEN :: SisClient : {"parent":6}
11:43:35 08 : OPEN :: GreDecode : {"parent":5}
11:43:35 05 : AUDIT :: Init : {"bind_addr":"127.99.99.21"}
11:43:35 05 : OPEN :: GreTunnel : {"parent":2}
11:43:35 07 : OPEN :: TcpProxy : {"parent":2}
11:43:35 04 : OPEN :: WsListen : {"parent":1}
11:43:35 06 : OPEN :: AnnexF12 : {"parent":2}
11:43:35 03 : OPEN :: UdpMonitor : {"parent":2}
11:43:35 02 : OPEN :: IconPepUnit : {"parent":1}
11:43:35 01 : AUDIT :: WebStart : {"addr":"0.0.0.0:17636"}
```

This shows logging from Icon-PEP with the most recent logs at the top. This is a filtered logging stream. All the logging metrics that are used to drive the other displays are omitted. The **Pause** button allows the display to be paused.

4.8 Logging files

Logging appears in dated files under (*LOGDIR*). Files roll over daily. In the following example, some lines have been wrapped to fit the page width.

```
20230831-172208.034    0 INFO   Timezone is +0000
20230831-172208.034    0 INFO   Icon-PEP startup arguments: -T
20230831-172208.035    1 OPEN   Global
20230831-172208.036    2 OPEN   Tui [parent=1]
20230831-172208.043    1 INFO   Successfully activated Icon-PEP
20230831-172208.045    3 OPEN   Terminal [parent=2]
20230831-172208.136    1 AUDIT  WebStart [addr=0.0.0.0:17636]
20230831-172208.138    4 OPEN   IconPepUnit [parent=1]
20230831-172208.138    5 OPEN   UdpMonitor [parent=4]
20230831-172208.138    4 INFO   Config update: Routes GRE F12 PEP
20230831-172208.239    6 OPEN   WsListen [parent=1]
20230831-172208.239    7 OPEN   GreTunnel [parent=4]
20230831-172208.240    8 OPEN   AnnexF12 [parent=4]
20230831-172208.240    9 OPEN   TcpProxy [parent=4]
20230831-172208.240    7 AUDIT  Init [bind_addr=127.99.99.22]
20230831-172208.240    0 INFO   PCAP file created
[fnam=gre-20230831-172208.pcap]
20230831-172208.240    10 OPEN  GreDecode [parent=7]
20230831-172208.241    11 OPEN  SisClient [parent=8]
20230831-172208.241    0 INFO   Dump file created
[fnam=dump-20230831-172208.log]
20230831-172208.241    9 AUDIT  Init [subnet_v4=172.31.0.0/16]
20230831-172208.241    12 OPEN  Slep [parent=9]
20230831-172208.249    11 AUDIT  Init [addr=10.222.0.1 port=6066]
20230831-172208.249    12 AUDIT  Init [sapid=2 ext=0]
20230831-172208.249    13 OPEN  SisClient [parent=12]
20230831-172208.250    13 AUDIT  Init [addr=10.222.0.1 port=6066]
20230831-172208.251    11 AUDIT  BindAccept [mtu=2048]
20230831-172208.251    13 AUDIT  BindAccept [mtu=2048]
20230831-172208.251    9 AUDIT  Bound [mtu=2048]
20230831-172242.859    10 INFO   Incoming GRE packet type:
!key !seq !checksum
20230831-172313.296    5 AUDIT  DnsQuery [client=10.8.2.1
server=172.20.0.66:53 rec=A name=www.isode.com tcp=false]
20230831-172358.827    5 AUDIT  DnsAnswer [client=10.8.2.1
server=8.8.8.8:53 rec=A name=www.isode.com answer=46.32.229.212
tcp=false ttl=600]
20230831-172502.900    16 OPEN  TcpConn [parent=9]
20230831-172503.104    17 OPEN  SlepStream [parent=12]
20230831-172503.105    17 AUDIT  Initiator [node=4.0.0.1 xfid=31364]
20230831-172503.105    16 AUDIT  FromLan [key=1 node=4.0.0.1
xfid=31364]
20230831-172503.105    16 AUDIT  ConnKey [hf_addr=46.32.229.212
hf_port=80 lan_addr=10.8.2.1 lan_port=36826]
20230831-172503.106    16 AUDIT  HttpRequest [method=GET
host=www.isode.com path=/ src=10.8.2.1:36826 dst=46.32.229.212:80]
20230831-172510.375    17 AUDIT  InState [state=Ready]
20230831-172510.377    16 AUDIT  HttpResponse [code=301
host=www.isode.com path=/ src=46.32.229.212:80 dst=10.8.2.1:36826
length=162]
```

```
20230831-172537.384    17 AUDIT OutState [state=Flushing]
20230831-172537.384    17 AUDIT Compression [input=142 output=140
percent=98.59]
```

The logging columns are as follows:

20230831-172208.034

Date as YYYYMMDD, time as HHMMSS and subsecond time in milliseconds.

13

Logging span number. Each instance of a component has a different logging span number. All logging from that component, between OPEN and CLOSE, is logged against the same span.

AUDIT

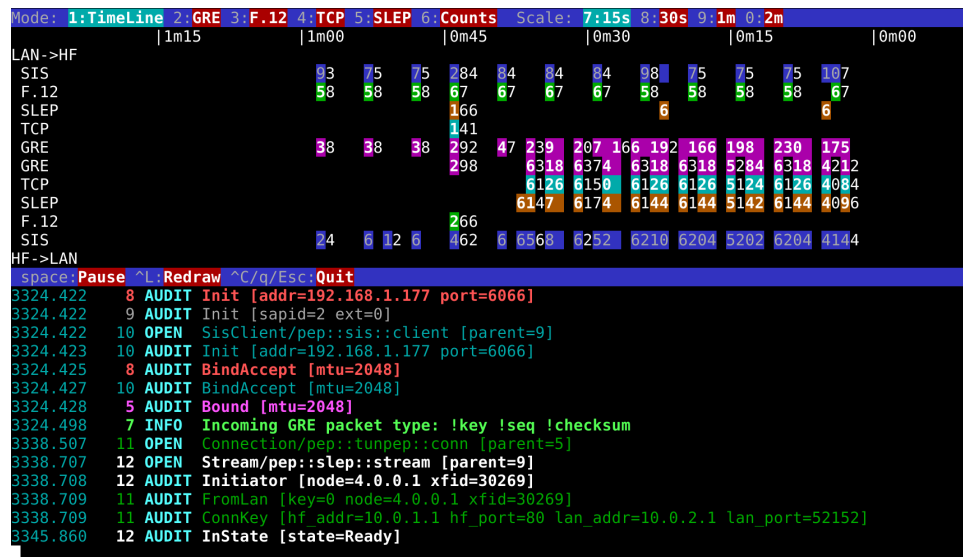
Type of logging record: OPEN and CLOSE record start and end of a span, AUDIT logs machine-readable data, TRACE, DEBUG, INFO, WARN and ERROR log human-readable information at various severity levels.

OutState [state=Flushing]

Data associated with the logging record. The values within square brackets are machine-readable key-value pairs.

4.9 Command Line Monitoring

Figure 4.1. Command Line Monitoring



The command mode of Icon-PEP provides a simple character based GUI to visualize data flowing over GRE, TCP, SLEP, IP Client and STANAG 5066 SIS. This gives a front-panel display to Icon-PEP that may be useful during initial setup or whilst debugging a configuration remotely where it is inconvenient to use the web-based monitoring display. There are the following options, accessed by keyboard control:

1. Timeline (shown above), gives a graphical flow of inbound and outbound traffic at each level. Traffic moving from the LAN towards HF appears in the upper part, and from HF towards the LAN in the lower part.
2. GRE. Data flowing at the Generic Routing Encapsulation layer (GRE).

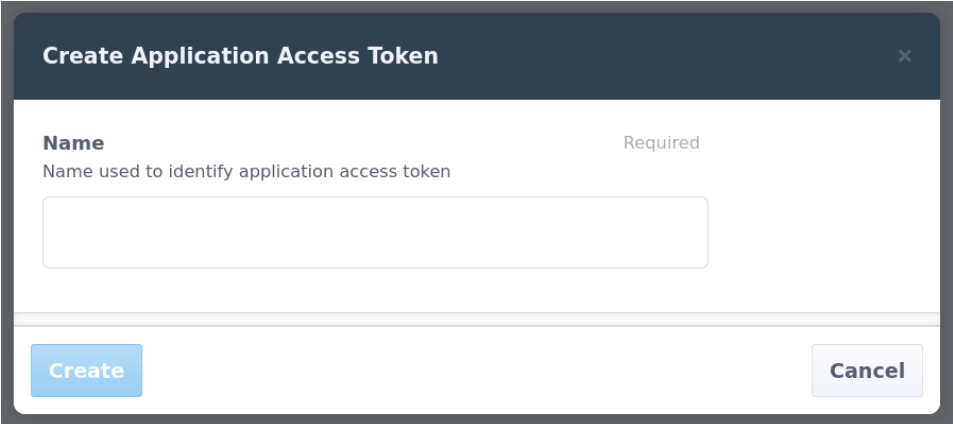
3. IP Client (previously Annex F.12). Data flowing over STANAG 5066 Annex U IP Client.
4. TCP. Data flowing in TCP Tunnel.
5. SLEP. Data from TCP Tunnel flowing over STANAG 5066 SLEP Streaming Service.
6. Counts. Show summary of packet counts at each layer.

Chapter 5 General management API

This chapter describes the web-API that allows external tools to manage Icon-PEP.

This is where interfaces will be exposed for the use of Icon-Topo or Red/Black. Icon-Topo is a product to support Mobile Unit (MU) mobility between HF Networks. [See the Icon-Topo product page](https://www.isode.com/products/icon-topo.html). [https://www.isode.com/products/icon-topo.html]. Red/Black is a management product that monitors and controls devices and servers. [See the Red/Black product page](https://www.isode.com/products/red-black.html). [https://www.isode.com/products/red-black.html].

5.1 Enabling access to the API



Access to the API requires an access token. Go to the **Access Tokens** section under **Configuration** and select **Add token**. The UI will provide a token which must be copied and saved in the configuration of the external tool immediately, and not saved anywhere else. Along with the IP address and port of Icon-PEP, this will enable access by the external tool to Icon-PEP.

5.2 Supported actions

The following actions may currently be performed:

1. Update the entire HF routing table.
2. Change the default HF route to direct traffic to the provided S'5066 node.
3. Abort all traffic to/from the provided S'5066 node.

This interface could be supported for other uses than Icon-Topo or Red/Black if required. Contact Isode support if this is of interest.