

# INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME



## Large Scale Monitoring Broadband Internet Infrastructure Contract No. 004336

### D0.1 “Requirement collection and analysis”

**Abstract:** In this deliverable we present our findings about the current state of monitoring, expectations and requirements of organisations that were identified as those that can benefit from the monitoring infrastructure to be implemented by Lobster.

Contractual Date of Delivery	31 March 2005
Actual Date of Delivery	10 April 2005
Delivarable Security Class	Public
Editor	Sven Ubik
Contributors	CESNET, FORTHnet, Terena

The LOBSTER Consortium consists of:

FORTH-ICS	Coordinator	Greece
VU	Principal Contractor	The Netherlands
CESNET	Principal Contractor	Czech Republic
UNINETT	Principal Contractor	Norway
ENDACE	Principal Contractor	United Kingdom
Alcatel	Principal Contractor	France
FORTHnet	Principal Contractor	Greece
TNO	Principal Contractor	The Netherlands
TERENA	Principal Contractor	The Netherlands

# Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>General information about organisations</b>	<b>4</b>
<b>3</b>	<b>Network infrastructure of organisations</b>	<b>5</b>
<b>4</b>	<b>Passive monitoring issues</b>	<b>8</b>
<b>5</b>	<b>Lobster operation policy</b>	<b>12</b>
<b>6</b>	<b>Anonymization</b>	<b>15</b>
<b>7</b>	<b>Conclusion</b>	<b>19</b>
<b>A</b>	<b>Questionnaire</b>	<b>21</b>

# 1 Introduction

In order to find out what is the current state of monitoring in European NRENs (National Research and Educational Networks) and selected ISPs, IXPs and other Lobster candidate users, we prepared and distributed a comprehensive questionnaire to representatives of these organisations.

We divided the questionnaire into five sections:

- Part A - General information about organisations
- Part B - Network infrastructure of organisations
- Part C - Passive monitoring issues
- Part D - Lobster operation and policy
- Part E - Anonymization

The goal of sections A and B was to find out information about the current state of networking in organisations. We wanted to know what network technologies organisations currently use to find what technology is needed to monitor the operation of these networks. The goal of section C was to get an overview of the current as well as the planned state of network monitoring within organisations, particularly looking at passive monitoring. We wanted to gather people preferences regarding metrics, monitoring goals and target users of monitoring. Finally, the goal of sections D and E was to investigate people expectations of the Lobster infrastructure, their preferences and constraints regarding local policies. The complete set of questions in the questionnaire can be found in Appendix A.

In the following sections we summarize and comment obtained responses to individual questions. We present overall conclusions and directions obtained from the questionnaires in Section 7.

## 2 General information about organisations

We sent questionnaires to 60 organisations and we received a total of 24 responses. The number of different types of organisations that responded to our questionnaire is shown in Fig. 1. We obtained quite a lot of responses from NRENs and a few responses from other types of organisations. Unfortunately, we obtained only two responses from ISPs. We expected to get a response from about 50% of organisations to whom we sent our questionnaire. We received responses from 40% of organisations. We comment more on the number of obtained responses in section 7.

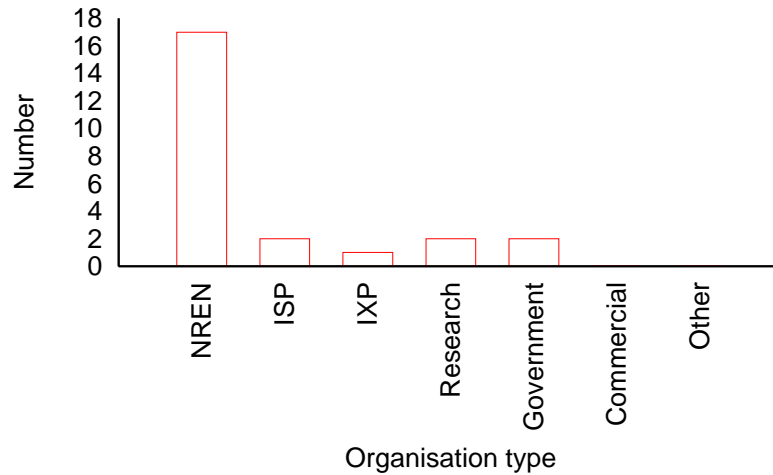


Figure 1: Type of organisations that responded to the questionnaire

### 3 Network infrastructure of organisations

In Fig. 2 we can see that almost all organisations operate their own network and in Fig.3 we can see that most organisations also operate their own NOC (Network Operation Centre) and only a few organisations have their NOC outsourced. The number of customer organisations connected to the networks operated by the queried organisations is quite high, see Fig. 4. The number of PoPs (Points of Presence) of the queried organisations is also quite high, see Fig. 5, but significantly lower than the number of customer organisations, that is there are many customer organisations connected through one PoP. These numbers imply that monitoring nodes will need to be connected to the lines connecting participating organisations to the Internet, rather than to the lines leading from the participating organisations to their customer organisations.

We can see in Fig. 6 that approximately half of the organisations use dark fibre (either their own or rented) and the other half use fibre lit by a telco operator. The organisations use various types of physical and link layer technologies and speeds, as we can see in Fig. 7 for internal lines (within the network operated by the organisation) and in Fig. 8 for external lines (connecting the network operated by the organisation to the public Internet). Most links are based on PoS (Packet over SONET), Ethernet or ATM and a few links use wireless technologies. Speeds range from 34 Mb/s to 10 Gb/s. The SCAMPI architecture that we plan to use in the LOBSTER project can use regular NICs (Network Interface Cards), SCAMPI adapters developed within the project and DAG cards produced by Endace. With the latest versions of these adapters we should be able to cover all technologies and speeds except wireless connections and except certain ATM links. However, ATM is generally considered a legacy technology and we expect that it will be gradually replaced by Ethernet or PoS.

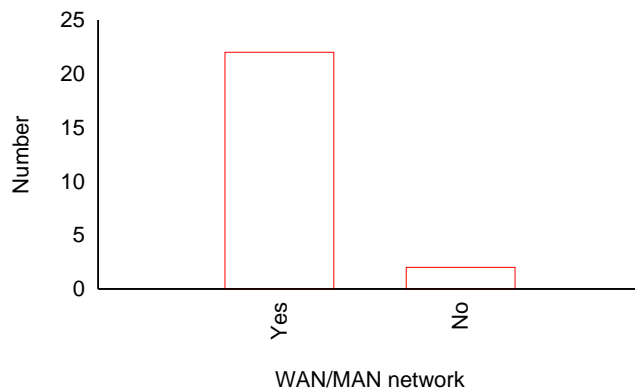


Figure 2: Do you have you own WAN or MAN network?

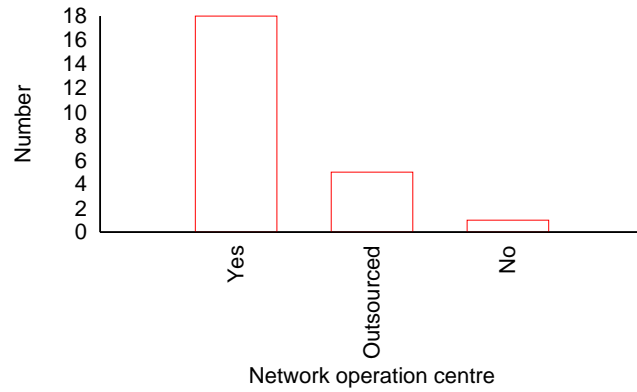


Figure 3: Do you have a NOC (Network Operation Centre)?

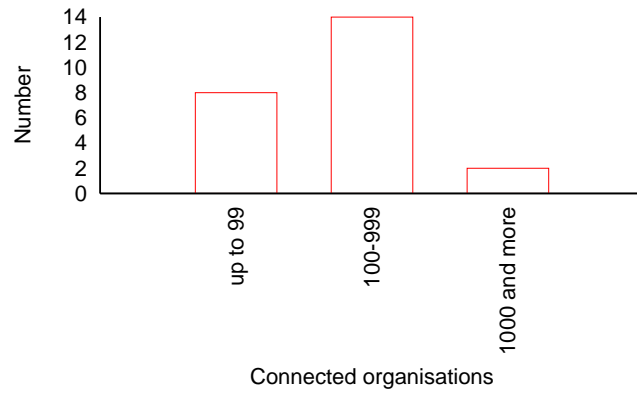


Figure 4: Number of customer organisations connected to your network

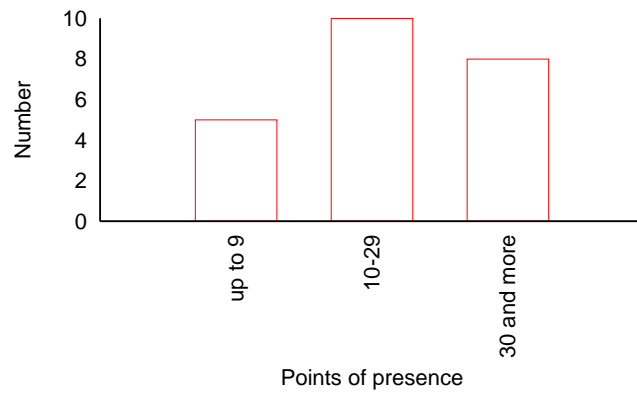


Figure 5: Number of PoPs (Points of Presence) in your network

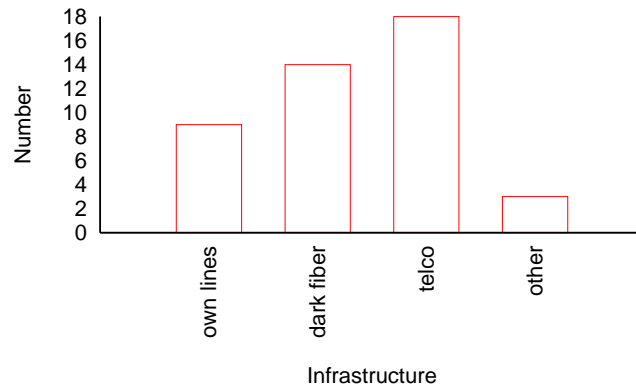


Figure 6: What physical layer infrastructure do you use?

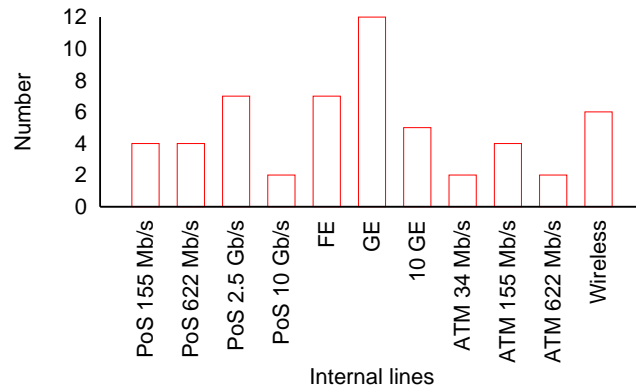


Figure 7: Technology and speed of internal lines in your network

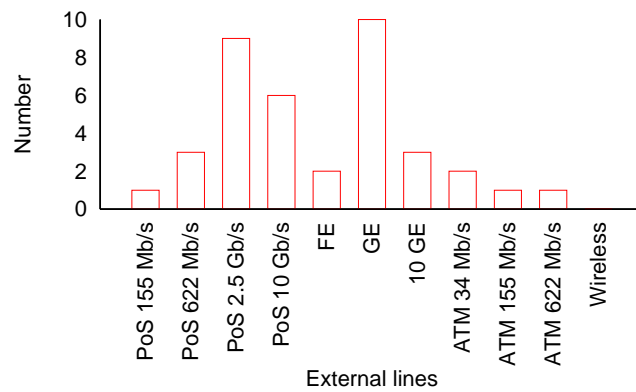


Figure 8: Technology and speed of external lines from your network

## 4 Passive monitoring issues

The frequency of current use of different monitoring tools in the queried organisations is summarized in Fig. 9. We can see that various Netflow-based tools and MRTG are the most popular options. Other than these two common tools, the rest of monitoring was spread in a lot of different tools, most of which were used just in one organisation, counted in "other" column. Organisations also frequently use their own home-made scripts for monitoring.

The objectives why people want to monitor their networks are classified in Fig. 10. We can see that various goals are frequently represented, that is we cannot say there is one reason why people want to monitor their network. In other words, a monitoring system must be general and flexible enough to satisfy different monitoring goals.

A similar observation can be drawn about metrics to be monitored, see Fig. 11. People are interested in different metrics. There was a slightly lower interest in one-way delay and throughput (although each metric was also requested by several organisations) than in other metrics. These metrics are more often measured by active monitoring and some of the queried organisations probably already monitor them in their networks and are thus less interested in them.

As we can see in Fig. 12 people consider both active and passive monitoring approximately equally important. A good point is that many organisations already do passive monitoring on a regular basis, as we can see in Fig. 13. Considering the tools reported to be used by organisations, it is clear that people include in the passive monitoring also the approach when data is retrieved from networking devices (e.g., netflow records or SNMP MIB items) and processed into metrics. That is our approach to passive monitoring by observing and analysing network traffic by capturing packets is not yet widespread.

It was a little bit surprising that people expressed interested in various types of result presentation, see Fig. 14. Our previous experience was that people preferred graphical presentation. Here we can see that people also require raw data for further processing. However, it is likely that the response was affected by allowing people to simply click on any option, and as it did not cost anything, people could select options just in case.

As we can see in Fig. 15, the expected audience of the monitoring system are qualified network personnel, rather than management people and end users.

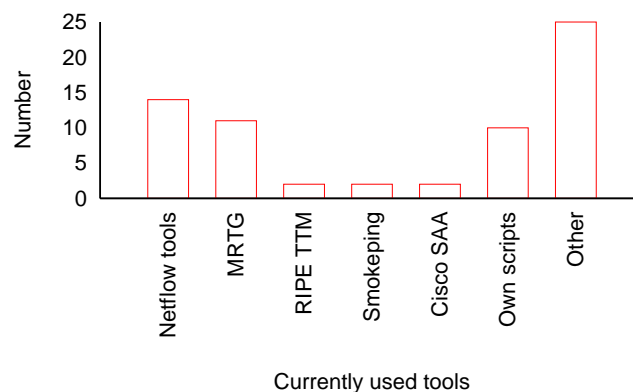


Figure 9: Monitoring tools currently used in your network

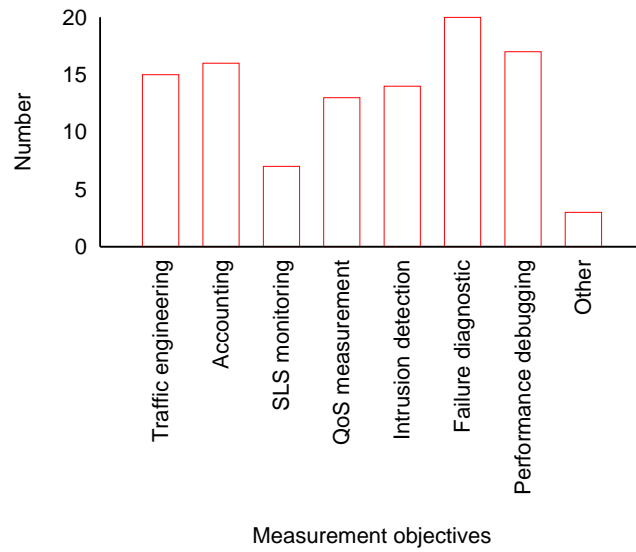


Figure 10: What are objectives of network monitoring for you?

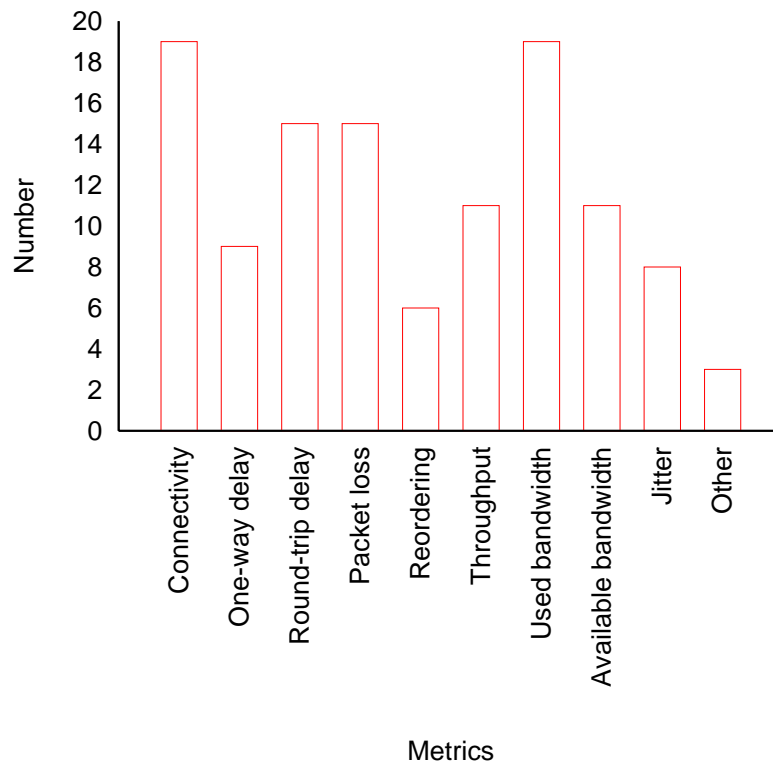


Figure 11: Importance of metrics

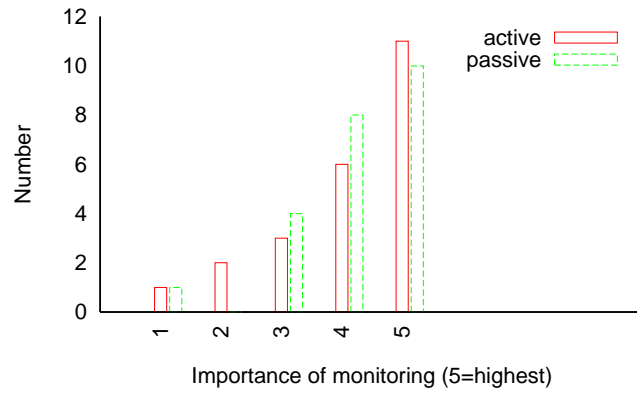


Figure 12: Importance of active and passive monitoring

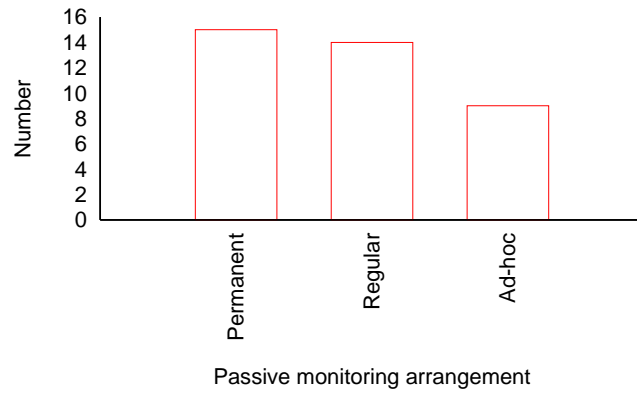


Figure 13: Arrangement of running passive monitoring

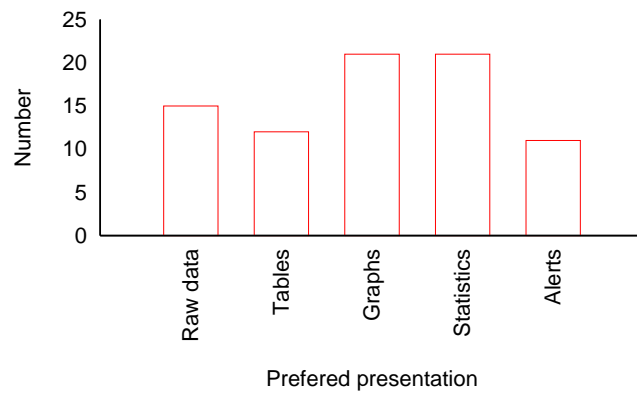


Figure 14: Preferable way of result presentation

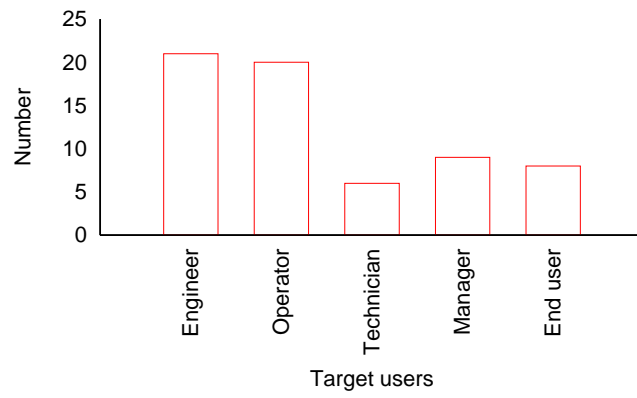


Figure 15: Target users of monitoring results

## 5 Lobster operation policy

The interest of people in cooperating with the Lobster project in different areas is summarized in Fig. 16. Highest level of interest was most frequently indicated for detecting denial of service attacks and for packet loss monitoring. It was followed by detecting high-level anomalies in network traffic and various statistics. However, this question would probably provide statistically representative indicators only when a high number of responses was processed. We should therefore take into account all areas where several partners expressed their interest.

The types of data that people are generally willing to provide to other Lobster participants is shown in Fig. 17. Unfortunately, many people said that they are not willing to share any data and those who are willing to share data prefer to give out only filtered data, packet headers, anonymized data and statistics. Only three partners are willing to provide raw data. It was surprising that some people want to get various types of data from others (see Fig. 14), but they are reluctant to give out their own data at the same time. We assume that people responded so because they are not fully aware of possibilities of data anonymization, which the Lobster project will provide and which will allow people to safely share their data. However, as we can see in Fig. 18, even though most organisations preferred to process data into statistics before giving them out, some organisations would be happy when packet traces are properly hashed or anonymized. As we can see in Fig. 19, most organisations accept using their packet traces for research purposes, but only half of organisations accepts using their traces also for educational purposes.

We also asked people about their preferences on installation, operation and failure management of the Lobster infrastructure, see Fig. 20. Most partners prefer to make installation themselves, but some partners also want to have it done remotely. Almost all organisations want to operate their monitoring node themselves. However, in case of a failure, most organisations prefer to have a failure helpdesk available, even though people are also willing to cooperate in case of failure.

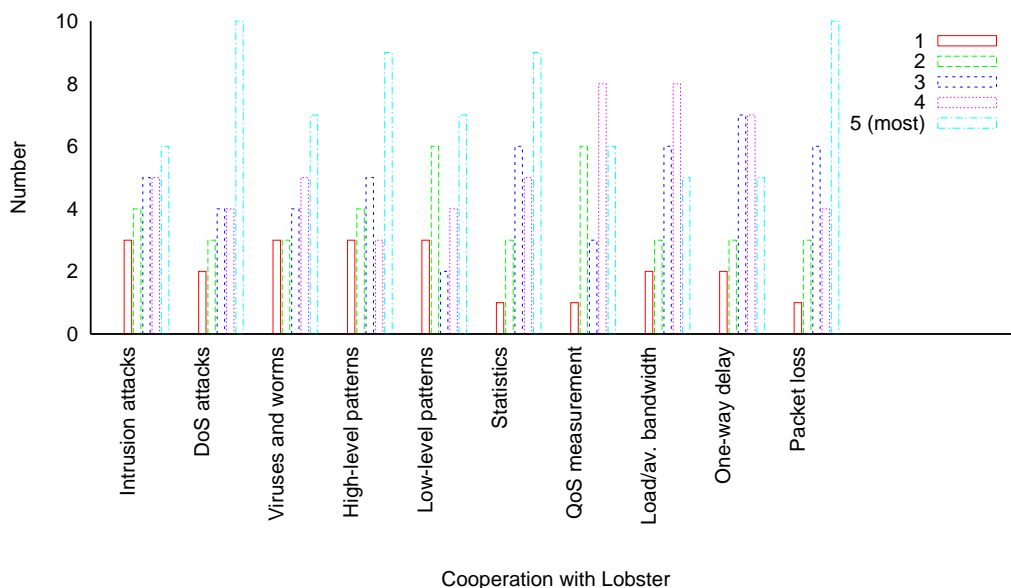


Figure 16: Cooperation with Lobster activities

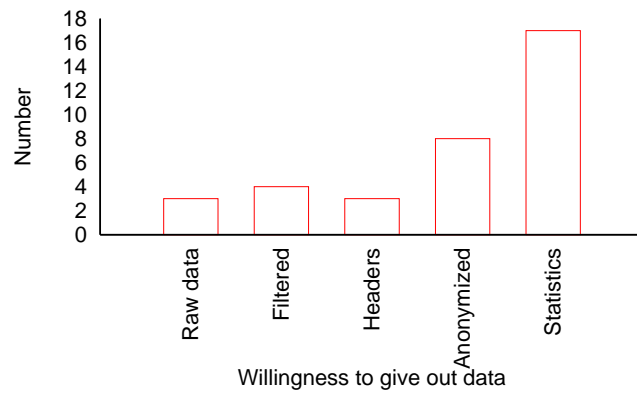


Figure 17: Data you could give to Lobster

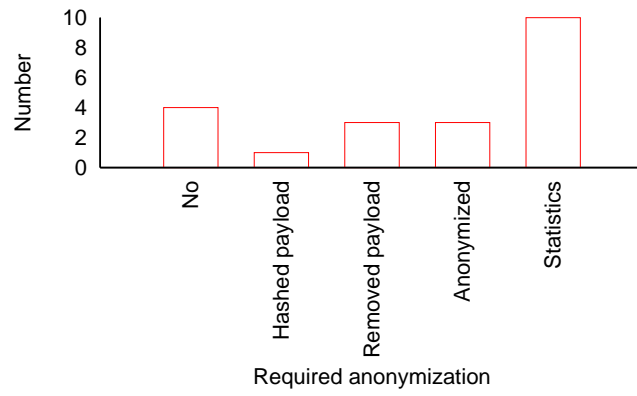


Figure 18: Required level of data anonymization

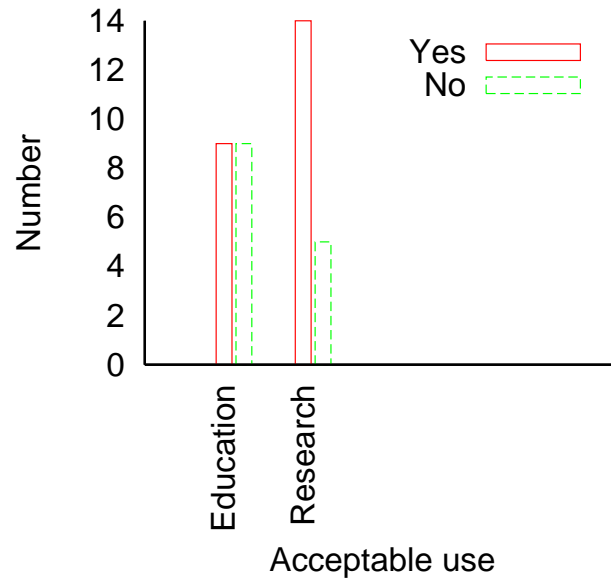


Figure 19: Acceptable usage of provided data

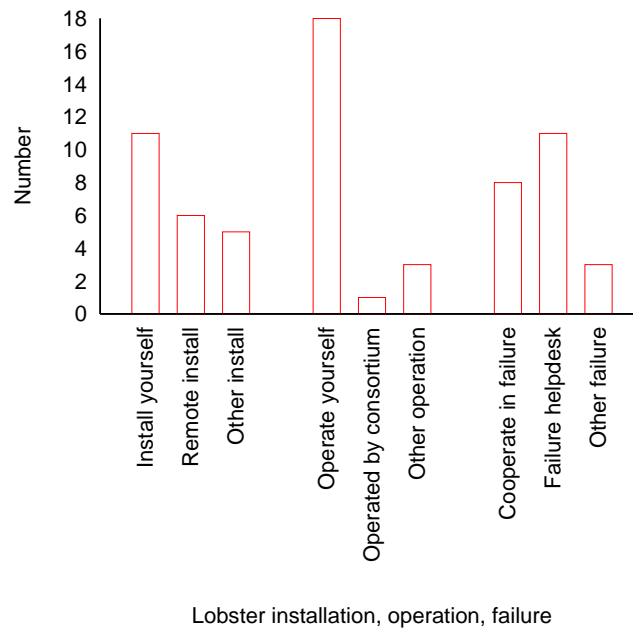


Figure 20: Lobster installation, operation and failure management

## 6 Anonymization

While most organisations already provide packet traces for their own use, see Fig. 21, only three organisations provide traces to other parties, but several other organisations share their flow records, aggregated data and statistics, see Fig. 22. General conditions under which organisations are willing to share their data with others are shown in Fig. 23. We can see that organisations consider as the most important factor the ability to choose to whom they provide data, followed by requiring that other parties are members of the Lobster community and that data must be anonymized.

We first asked people about their general preferences regarding anonymization, which are summarized in Fig. 24. People mostly prefer to remove packet packet and to hash IP addresses in packet headers. Some people would be happy with hashed payloads. Then we asked people about their detailed requirements on anonymization of different parts of packets when sharing traces with different types of other parties. The result is illustrated in Fig. 25. For each kind of anonymization there are five columns corresponding to different kinds of packet trace uses - own organisation, sharing with selected partners, sharing within the Lobster consortium, sharing with known third parties outside consortium and sharing with random other parties. The first thing that we can see is that almost all possibilities are represented, that is our solution must be configurable so that users can choose the kind of anonymization based on their preferences and the target packet trace user. Some kinds of anonymization are mutually exclusive (e.g., drop or hash payload), whereas other are complementary (e.g., hash IP address and hash ports). It is sometimes not clear, if a user selected several options because they want them all at the same time in order to share data or if they would be happy with any of them. Anyhow, it is clear that all envisioned anonymization types must be provided. Finally, we asked people about their view on the way that anonymization should be performed, see Fig. 26. Again, people find choosing the type of anonymization and the party with whom the packet trace is shared as the most important factor. An interesting point is that significant percentage of organisations prefer anonymization to be done directly on the monitoring card, so that clear text data do not get to the host computer.

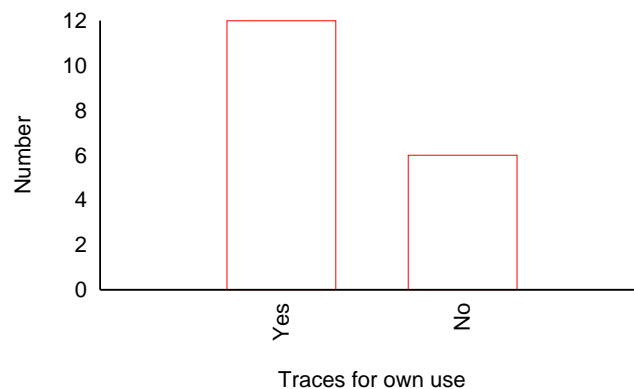


Figure 21: Providing traces for own use

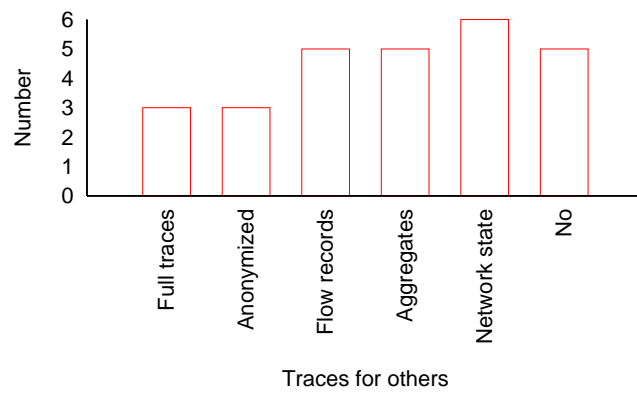


Figure 22: Providing traces to others

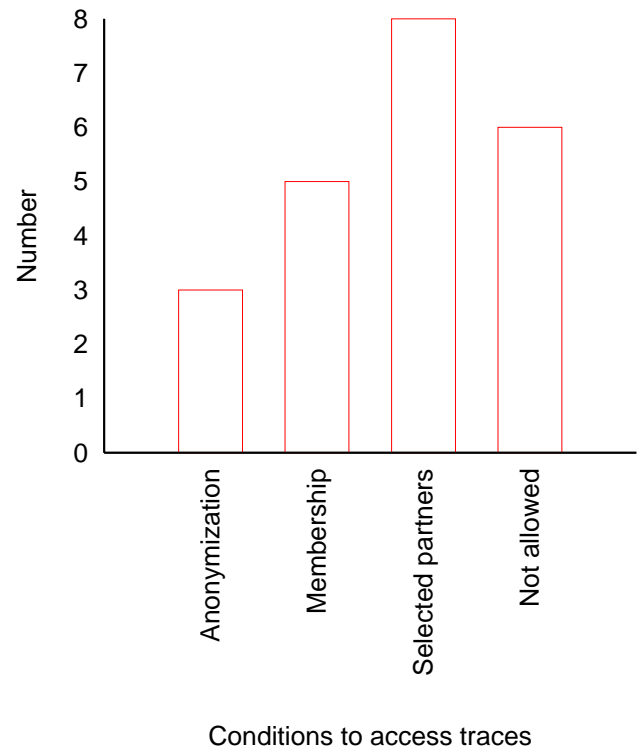


Figure 23: Conditions to provide traces to others

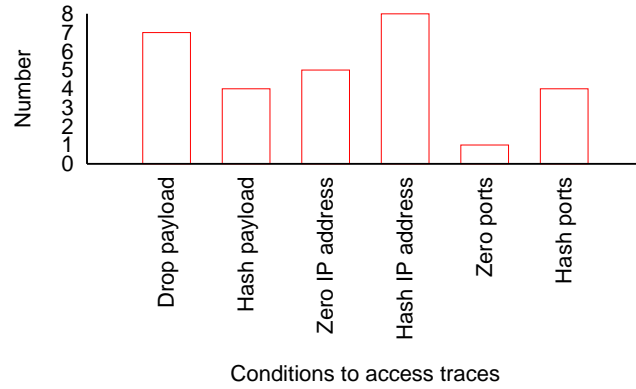


Figure 24: Required level of anonymization

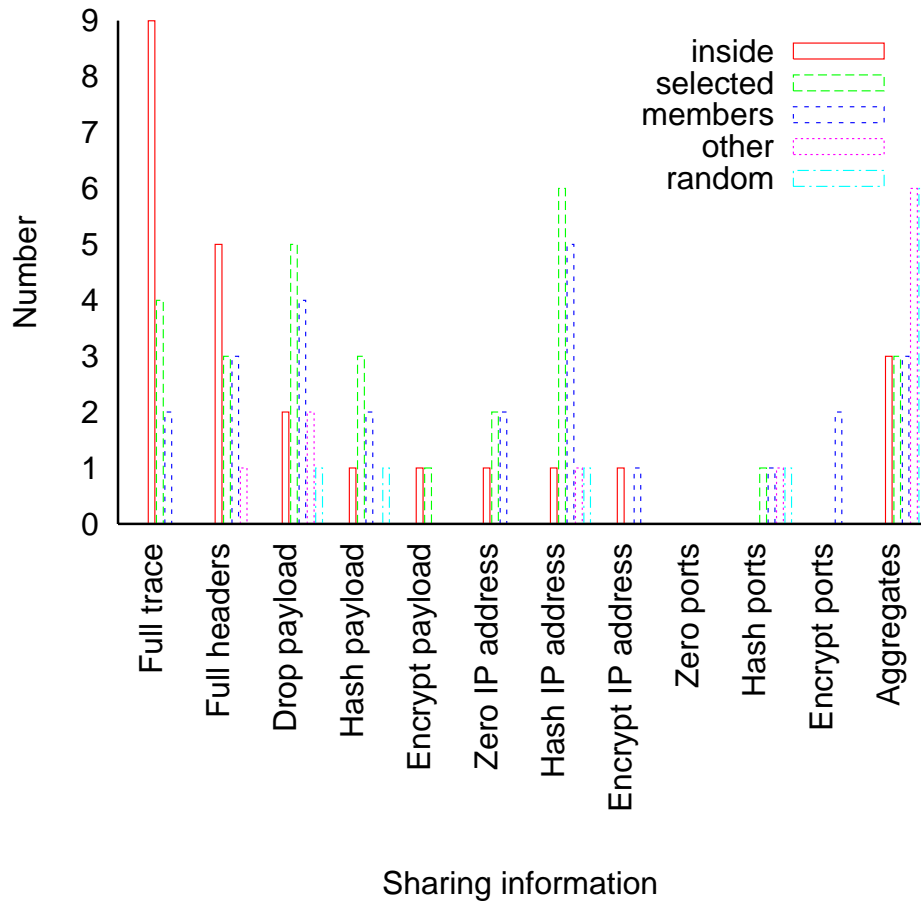


Figure 25: Anonymizing conditions on sharing information to different parties

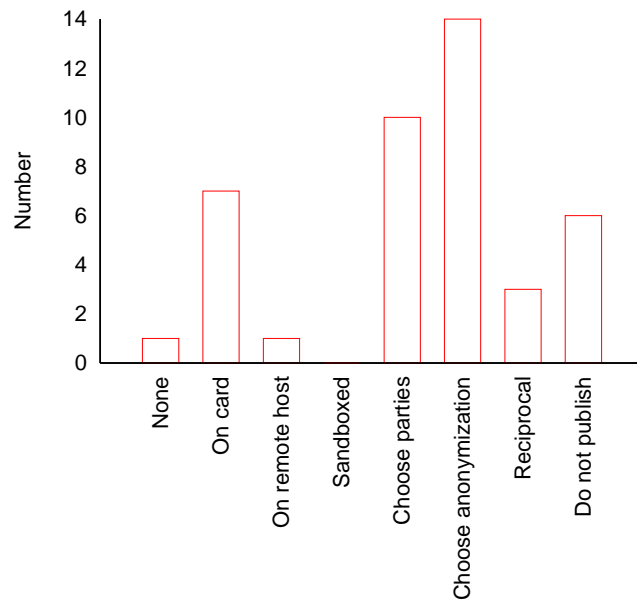


Figure 26: General conditions on sharing information to different parties

## 7 Conclusion

We sent out 60 questionnaires and received 24 responses, that is from 40% of queried organisations. We expected that some organisations would find it difficult to dedicate their time to fill out our questionnaire. We also assume that particularly commercial ISPs were reluctant to give out information about their networks. However, our project is primarily targeted towards NRENs in the first phase with the possibility to extend the scope of our infrastructure to ISPs in the second phase. We believe that when ISPs see the benefits of the existing infrastructure and possibilities of configurable anonymization, they may be attracted to join later.

Consequently, the number of received responses is too low to be really statistically representative. However, we can see how user preferences are varying and we should design our infrastructure to comply with the varying options - if there is a non-zero requirement for some option, we should provide it, otherwise we will lose our users. And the responses gave us the clues what we should provide.

In addition to concrete numbers of organisations requesting particular options, we can draw the following overall conclusions from the received responses:

- The number of links to monitor to give a complex view on the network is large. A monitoring station should be ideally connected to an optical splitter on the external link leading from the organisations to the public Internet or to a port on a router or switch configured to mirror traffic from this external link. This may require to deal with MPLS headers, but mirroring of internal links (without MPLS) may not be possible due to limitations on the number and directions of ports to be mirrored on a router.
- We will have to provide solution for both Ethernet and PoS. The current versions of SCAMPI adapters are designed for Ethernet only, but the new versions already in design process will support PoS as well. DAG cards already support PoS.
- There is little coordination in network monitoring among organisation. Each organisation deploys tools by their own, often with home-made scripts and tools not used by anyone else.
- People envision the system to provide information for qualified networking personnel rather than for managers or end users.
- People want to get results not only in a graphical form (a traditional preference), but also as raw data. On the other hand, few people are willing to provide raw data to others.
- As people are generally afraid to give out their data, we should explain that with anonymization it is safe and that they can select themselves what parts of packet traces to share and with whom they are willing to share.
- The monitoring applications suggested by us are highly demanded, such as virus and worm detection, detecting traffic anomalies and passively obtained statistics about network traffic.
- People generally prefer to install and operate the monitoring stations themselves, but some people request remote installation and almost all people request assistance in operation failure. Therefore, we will have provide for this assistance.

- Regarding anonymization, people prefer to configure the kind of performed anonymization and to choose parties to whom the anonymized traces can be provided and they prefer anonymization to be done directly on the monitoring adapter. The kind of preferred anonymization was the most varying factor in obtained responses and should therefore be highly configurable.

# A Questionnaire

\*Part A - general\*

\*1.1: Organization/company \*

Name or acronym of your organization and URL of main web page

Name:

URL:

-----  
\*1.2: Category\*

What category describes your organization?

\_Please choose \*only one\* of the following:\_

NREN

ISP

IXP (Internet Exchange Point)

Research/Education

Government

Commercial

Other

-----  
\*1.3: Interviewed person contact details\*

Name:

Address:

E-mail:

-----  
\*1.4: Manager contact details\*

Name:

Address:

E-mail:

-----  
\*1.5: Measurement responsible person contact details\*

Name:

Address:

E-mail:

-----  
\*1.6: Other information\*

Any other relevant information describing your organization

-----  
\*Part B - network\*

\*2.1: WAN/MAN network\*

Do you operate your own WAN or MAN network?

Yes

No

-----  
\*2.2: Network operation centre\*

Does your network have NOC (Network operation centre)

Yes

Outsourced

No

-----  
\*2.3: Connected organizations/customers\*

Number of organizations (customers) connected to your network

-----  
\*2.4: Points of presence\*

Number of points of presence of your network

-----  
\*2.5: Infrastructure\*

Common method of building your infrastructure (main lines provision)

Own lines

Rented dark fibre

Provided by TELCO operator

Other:

-----  
\*2.6: Technology and speed of main network lines\*

Type and speed your main lines, e.g. backbone

\_Please choose all that apply and provide a comment\_

PoS (Packet over Sonet/SDH)

Ethernet

ATM

Wireless

---

\*2.7: Technology and speed of external lines\*

Type and speed of lines that connect your network to global Internet or superior network

\_Please choose all that apply and provide a comment\_

PoS (Packet over Sonet/SDH)

Ethernet

ATM

Wireless

---

\*2.8: Current active/passive monitoring tools \*

Tools for network monitoring you currently use (in order of importance)

Tool 1:

Tool 2:

Tool 3:

Tool 4:

Tool 5:

---

\*2.9: Measurement objectives\*

Choose all network measurement objectives in your network

\_Please choose \*all\* that apply\_

Traffic engineering

Accounting

SLS monitoring

QoS measurement

Intrusion detection

Failure diagnostic

Debugging performance problems

Other:

---

\*2.10: Metrics \*

Main metrics that are applied in monitoring of your network

\_Please choose \*all\* that apply\_

Connectivity

One-way delay

Round-trip delay

Packet loss  
Packet reordering  
Throughput  
Used bandwidth  
Available bandwidth  
Jitter  
Other:

---

\*2.11: Other information\*

Any other information to specify you network

---

\*Part C - passive monitoring issues\*

\*3.1: Importance of monitoring \*

How important is passive and active monitoring for operation of your network ( 1 - not important,.... 5 - very important)

Passive monitoring 1 2 3 4 5

Active monitoring 1 2 3 4 5

---

\*3.2: Passive monitoring tools description \*

The most important passive monitoring tools that are used in your organization

---

\*3.3: Tools you plan to deploy \*

Passive monitoring tools your organization plans to use in next 12 months

---

\*3.4: Method of data collection\*

Methods of data collection of passive monitoring that are used in your organization

Isolated point(s) of measurement

Centralized processing/aggregation

Other:

---

\*3.5: Passive monitoring arrangement\*

Characteristic of passive monitoring arrangement in your network

Permanent measurement

Regular periodical measurement

Ad-hoc measurement

-----  
[Only answer this question if you answered 'Regular periodical measurement' to question '3.5 ']

\*3.5.1: Period of regular periodical measurement\*

-----  
\*3.6: Monitoring results presentation.\*

Preferred method of presentation of passive monitoring results

Raw data

Tables

Graphs

Statistics

Real-time alerts

Other:

-----  
\*3.7: Target users of monitoring results\*

Regular target users of passive monitoring results in your organization

Network engineer

Network operator

Technician

Corporate manager

End user

Other:

-----  
\*Part D - LOBSTER operation and policy\*

\*4.0: Questions in this part concern your potential cooperation with the Lobster project as a pilot user. Brief description of the project is in attached document and also at <http://www.ist-lobster.org/> .....\*

-----  
\*4.1: Cooperation with Lobster activities\*

Indicate your interest to cooperate with the Lobster project in given monitoring goals (1=Not Interested, 5=Very Interested)

\_Please choose the appropriate response for each item\_

Intrusion attacks                    1 2 3 4 5

Denial of service attacks           1 2 3 4 5

Viruses and worms                   1 2 3 4 5

High-level traffic patterns (e.g. network overloads identifications)

   1 2 3 4 5

Low-level traffic patterns (e.g. TCP stack behavior in end host)

	1	2	3	4	5
Traffic statistics	1	2	3	4	5
QoS measurement	1	2	3	4	5
Load/available bandwidth	1	2	3	4	5
One-way delay	1	2	3	4	5
Loss ratio	1	2	3	4	5

---

**\*4.2: Lobster service operation\***

Who should operate the Lobster service in your network?

Your organization

Independent consortium

Other

---

**\*4.3: Expected output from Lobster system\***

What kind of output from Lobster system do you prefer? Put also optional comments.

Raw data for own processing

Processed data (e.g. warnings, alerts, graphs, tables)

Aggregated data

---

**\*4.4: Data you could give to Lobster\***

What kinds of traffic data and information could you provide for (selected) Lobster participants? Put also optional comments.

Raw data (packet headers and payload)

Filtered raw data

Packet headers only

Anonymized headers

Statistics

No data

---

**\*4.5: Required level of data anonymization\***

What kind of stored data anonymization would you require?

No anonymization

Hashed payload preserving attacks signatures

Removed payload

Light sanitized IP address (unchanged network part of IP address)

Removed payload + fully anonymized IP address

Other:

-----  
\*4.6: Issues of restricted participation in Lobster\*

Are there any organization, country or EU regulations that may restrict your participation in the Lobster project?

-----  
\*4.7: Sensitive data that limit Lobster operation\*

Are there any kind of provided data/information that the Lobster project has to keep confidential?

-----  
\*4.8: Acceptable usage of provided data \*

Is it acceptable to use your data for education or research? Put also optional comments.

\_Please choose all that apply and provide a comment\_

Educational  
Research

-----  
\*4.9: Bandwidth used by Lobster\*

Estimation of bandwidth (in Mb/s) that you could grant to operation of the Lobster system

-----  
\*4.10: Solving Lobster installation/troubleshooting issues\*

Action you would take in case of installation or troubleshooting issues of the Lobster system

\_Please choose \*only one\* of the following:\_

Deal with it yourself  
Grant remote access to other participant  
Other

-----  
\*4.11: Solving Lobster system failure/malfunction\*

Support you would expect in case of Lobster system failure or malfunction

\_Please choose \*only one\* of the following:\_

Cooperation with other participants  
Centralized Lobster helpdesk  
Other

---

\*4.12: Lobster comments\*

Any other hints, comments or questions

---

\*Part E - anonymization\*

\*5.0: Traffic traces could contain sensitive information in packets payload and also headers of packets discover activities of each individual IP address user. As the Lobster project lays emphasis on reasonable anonymization of traffic traces, this last part of the questionnaire concerns anonymization issues.\*

---

\*5.1: Network monitoring\*

Does your organization monitor the network ?

Yes

No

---

\*5.2: Internet traces\*

Do you provide Internet traces for your own use?

Yes

No

---

\*5.3: Access to traffic traces \*

Do you provide parties outside your own organization access to traces or monitoring information?

\_Please choose \*all\* that apply\_

Full traces

Anonymized traces or headers

Flow records (e.g., netflow)

Only high level aggregate information

Only state of the network

No

Other:

---

\*5.4: Condition to access traffic traces\*

What is or would be a condition to access your traffic traces

\_Please choose \*all\* that apply\_

Trustworthy anonymization  
Membership in a consortium  
Partners selected by us  
Not allowed  
Other:

-----  
\*5.5: Required level of anonymization\*

What level of anonymization do you use (or prefer to use if not yet applied)?

\_Please choose \*all\* that apply\_

Drop payload  
Hash of payload  
Zero IP addresses  
Scramble IP addresses (e.g., hash)  
Zero TCP/UDP ports  
Scramble TCP/UDP ports (e.g., hash)  
Other:

-----  
\*5.6: Form of anonymization\*

What form of anonymization of selected fields do you prefer/accept?

\_Please choose \*all\* that apply\_

Zero the field  
Replace by one-way function (hashing)  
Encrypt with strong encryption  
Other:

-----  
\*5.7.1: Sharing information (inside own organization)\*

Inside your own organization: What level of sharing would you like or be comfortable with?

\_Please choose \*all\* that apply\_

Full trace  
Full headers  
Drop payload  
Hash payload  
Encrypted payload

Zero IP addresses  
Scramble IP addresses (irreversible hash)  
Scramble IP addresses (strong encryption)  
Zero TCP/UDP ports  
Scramble TCP/UDP ports (irreversible hash)  
Scramble TCP/UDP ports (strong encryption)  
Aggregates (e.g., utilization)  
Other:

-----  
\*5.7.2: Sharing information (with selected partners)\*  
Partners selected by you: What level of sharing would you like or be comfortable with?

\_Please choose \*all\* that apply\_

Full trace  
Full headers  
Drop payload  
Hash payload  
Encrypted payload  
Zero IP addresses  
Scramble IP addresses (irreversible hash)  
Scramble IP addresses (strong encryption)  
Zero TCP/UDP ports  
Scramble TCP/UDP ports (irreversible hash)  
Scramble TCP/UDP ports (strong encryption)  
Aggregates (e.g., utilization)  
Other:

-----  
\*5.7.3: Sharing information (inside monitoring consortium)\*  
Partners in a monitoring consortium (such a Lobster): What level of sharing would you like or be comfortable with?

\_Please choose \*all\* that apply\_

Full trace  
Full headers  
Drop payload  
Hash payload  
Encrypted payload  
Zero IP addresses  
Scramble IP addresses (irreversible hash)  
Scramble IP addresses (strong encryption)  
Zero TCP/UDP ports

Scramble TCP/UDP ports (irreversible hash)  
Scramble TCP/UDP ports (strong encryption)  
Aggregates (e.g., utilization)  
Other:

---

\*5.7.4: Sharing information (with third parties)\*

Third parties on reciprocal basis: What level of sharing would you like or be comfortable with?

\_Please choose \*all\* that apply\_

Full trace  
Full headers  
Drop payload  
Hash payload  
Encrypted payload  
Zero IP addresses  
Scramble IP addresses (irreversible hash)  
Scramble IP addresses (strong encryption)  
Zero TCP/UDP ports  
Scramble TCP/UDP ports (irreversible hash)  
Scramble TCP/UDP ports (strong encryption)  
Aggregates (e.g., utilization)  
Other:

---

\*5.7.5: Sharing information (random third parties)\*

Random third parties: What level of sharing would you like or be comfortable with?

\_Please choose \*all\* that apply\_

Full trace  
Full headers  
Drop payload  
Hash payload  
Encrypted payload  
Zero IP addresses  
Scramble IP addresses (irreversible hash)  
Scramble IP addresses (strong encryption)  
Zero TCP/UDP ports  
Scramble TCP/UDP ports (irreversible hash)  
Scramble TCP/UDP ports (strong encryption)  
Aggregates (e.g., utilization)  
Other:

-----  
\*5.8: In order to protect privacy of network users, Lobster develops a flexible anonymization framework (SiSaL), which allows network operator to choose which parties should be given access to what data. Lobster aims to perform a single baseline anonymization on the network card (in hardware), while additional anonymization levels can be specified. Get conditions of your participation. \*  
Indicate under what circumstances you would want to participate.

\_Please choose \*all\* that apply\_

None whatsoever

If anonymization is done on the card

If the common access platform resides on remote host

If the common access platform is in a 'sandboxed' environment (e.g., Java)

If we get to pick parties that see my data

If we get to decide sort of anonymization for any party.

If access is done on reciprocal basis

If nothing is published about traffic in our network

Other: