SubCERTs: The JANET Approach

Garaidh Cochrane
Senior Member
JANET-CERT

XIV Reunión del Grupo de coordinación IRIS-CERT
GT2004 - Madrid

JANET

The Academic and Research network in the UK

- All universities, colleges, research institutes
- Scottish schools
- English and Welsh schools by the end of 2004
- Many government departments and agencies
- Libraries, Councils, much more besides
- 20,000+ connected sites
- 16,000,000+ end users

JANET

UK Wide IP Network

- Cornwall to Shetland Islands
- 10 Gb backbone
- 7.5 Gb transatlantic
- 2.5Gb to GEANT
- Multiple peering links
- Upgrade to 40Gb soon.
- Most customers connected at 100Mb or better

JANET-CERT

Responsible for overall security of JANET

- Incident Response and Coordination
- Advisories
- Education
- Liaison
- Analysis
- Monitoring

7 people and one manager

Problem

JANET is quite big

- Too many incidents, too many customers

Sites not responsive

- afraid to talk to JANET-CERT
- person we talk to on holiday
- Single security contact leaves/retires

SubCERTs

SubCERTs on JANET provide CERT capability at customer sites.

- May be 'real' CERT teams, virtual CERTs, one man CERTs or completely off-site response capability.

SubCERTs are transparent to people outside JANET

- All incidents routed through JANET-CERT
- JANET subCERTs do not advertise their existence
- From an external perspective they are part of JANET-CERT
- We trust them – they trust us. Mostly.

SubCERTs - Duties

SubCERTs are used

- To coordinate response at customer sites
- To escalate security management issues to senior management at JANET sites.
- To relay information back to JANET-CERT
- To act as the single trusted point of contact for JANET-CERT, 24 hours a day, 365 days of the year
- As the contact point for Law Enforcement/Security Services matters
- To implement network controls for incidents - blocks.

SubCERTs' obligations

The JANET Security Policy states:

SubCERT Contacts:

"For many JANET primary sites, this will mean 24 hrs. per day, 365 days per year, and these sites need to have an accessible central contact throughout the whole of the same period"

SubCERT Investigations:

"In respect of organisations, this duty includes.......assisting in the investigation of a breach of security"

SubCERT Actions:

"Require a primary site, through its nominated contact, to rectify any omission in its duty of responsibility"

http://www.ja.net/documents/JANET_security_policy.html

SubCERTs

JANET-CERT is **solely** responsible for AS786 (JANET) and AS1213 (HeaNET)

- We have an IRT object
- We are in TF-CSIRT
- Our SubCERTs have no easy way of advertising their existence, this is deliberate
- If they are responsible for an address space, and advertise themselves, they are CERTs

SubCERT types

There are several type of organisation on JANET that can act as SubCERTs

- Security Contacts
- Virtual CERTs
- Real CERTs
- Regional Network Operators Security Contacts
- Regional Support Centre

It depends on the capability of the institution

Security Contacts

Each JANET site must have a CERT contact

- Someone to be contact for JC
- To deal with incidents
- To assist JC in investigations
- All JANET IP ranges **must** have contact name, email and telephone number
- So all JANET sites must have some CERT functionality

Security Contacts

```
[garaidhc@snotra garaidhc]$  whois -h whois.cert 193.60.160.250
[Querying whois.cert]
[whois.cert]
route:       193.60.160.0/20
descr:       University of Abertay
site-name:   University of Abertay Dundee
cert-name:   Mr Norman Phipps | Tel: 01382 308xxx
tech-name:   Norman Phipps | Tel: 01382 308xxx
manage-name: Frazer Greig | Tel: 01382 308xxx
cert-mail:   cert@abertay.ac.uk
tech-mail:   n.phipps@abertay.ac.uk
manage-mail: f.greig@abertay.ac.uk
```

CERT Contact is only for JANET-CERT

Security Contacts

- For many sites this is just one person
  - A system administrator
  - The Network Manager
  - A network technician
  - A member of teaching staff
- But they must know their responsibilities

SubCERT types

There are several type of organisation on JANET that can act as SubCERTs

- Security Contacts
- **Virtual CERTs**
  - Where the institution has no fixed IR capability

Virtual CERTs

Most JANET sites have a cert@university.ac.uk address for their incident response capability

- Virtual CERT set up as and when required
- Uses people from other areas of IT services/departments
- After incident resolved, everyone goes back to their normal jobs
- Becoming less common on JANET

Virtual CERTs Problems

Virtual CERTs have a lot of problems

- Unable to take a strategic view
- Take a long time to form (compared to lifecycle of incident)
- May not have good reporting structures to senior management
- Are becoming less common as a full time incident response and security need is identified
- Virtual CERTs tend to be NOC staff, who do not normally have the skills for host intrusions

SubCERT types

There are several type of organisation on JANET that can act as SubCERTs

- Security Contacts
- Virtual CERTs
- Real CERTs
  - Real in the sense that they are full-time Incident Response and Security teams.

Real CERTs on JANET

JANET has a lot of real CERT teams, some as old as JANET-CERT

- OxCERT
  - Neil Long held chair of FIRST in 2003
  - 8 people, 2 full time
- CamCERT
  - 3 full time CERT staff
- Edinburgh IRT
  - 8 people, 1 full time

Real CERTs on JANET

UCL-CERT

- 3 full time CERT staff
- (1 ex JANET-CERT)

Newcastle

Birmingham

Dundee (2 full time), York (1 full time)

Many more...all at bigger universities (>20000 students)

Real CERTs on JANET

Good:

- Provide 24/7 incident response cover
- Are capable of doing most of JC's work.
- Are very effective in resolving incidents without JC help.
- Some are **very** highly skilled.

Bad:

- Cost a **lot** of money, especially for the full time dedicated CERT staff (e90,000/person)
- Argue with JANET-CERT all the time

SubCERT types

There are several type of organisation on JANET that can act as SubCERTs

- Security Contacts
- Virtual CERTs
- Real CERTs

And

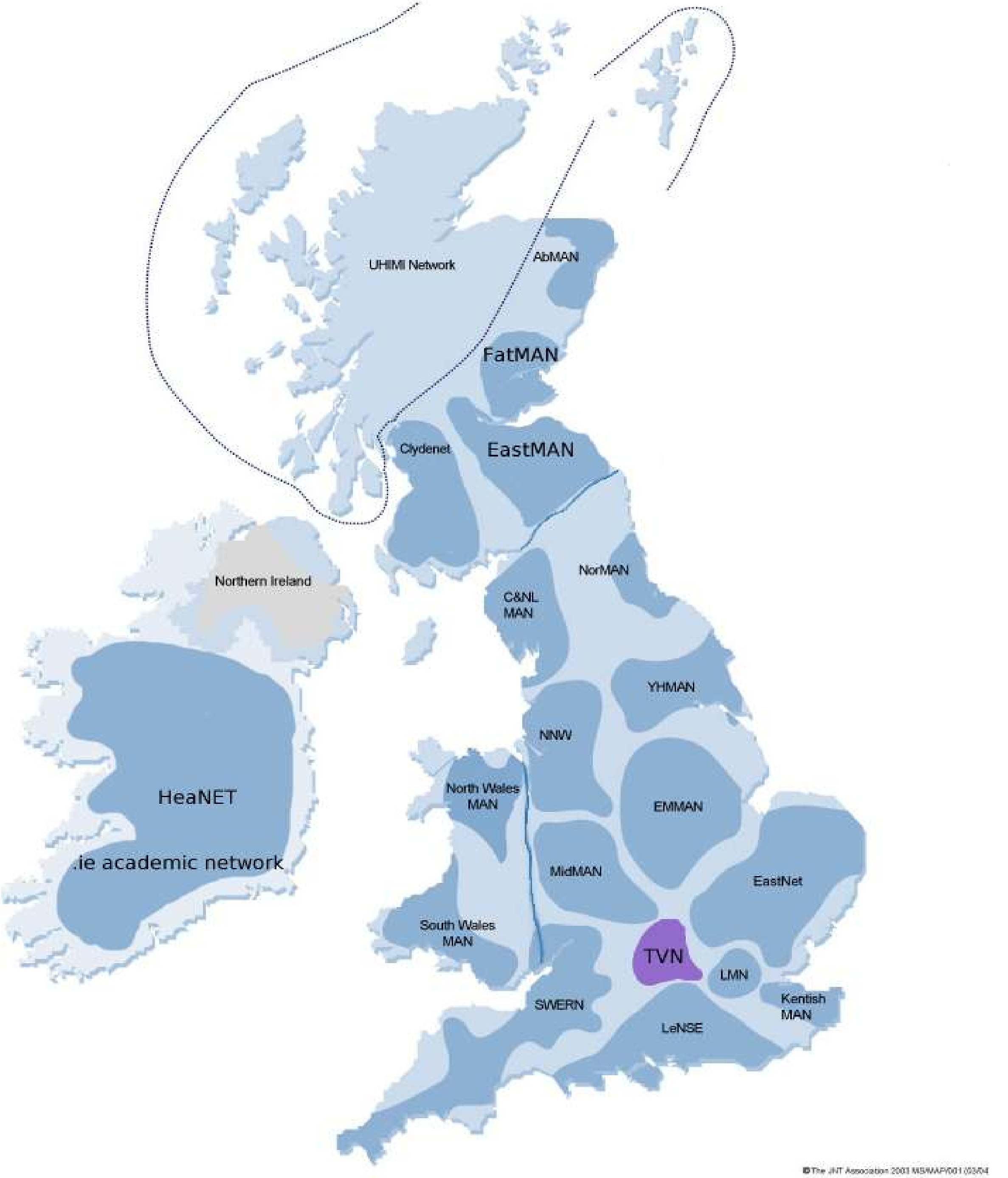
- Regional Network Operators Security Contacts
- Regional Support Centres
    - External JANET organisations

JANET Layers

JANET has layers

- Backbone
  - Connects Regional Networks
- Regional Networks
  - Connect customer sites
- Customer Sites
  - Connect sponsored connections (small sites)
- Regional Support Centres
  - Provide support for small sites

JANET Networks



Regional Network Organisations

RNOs run the Metropolitan Area Networks (MANs)

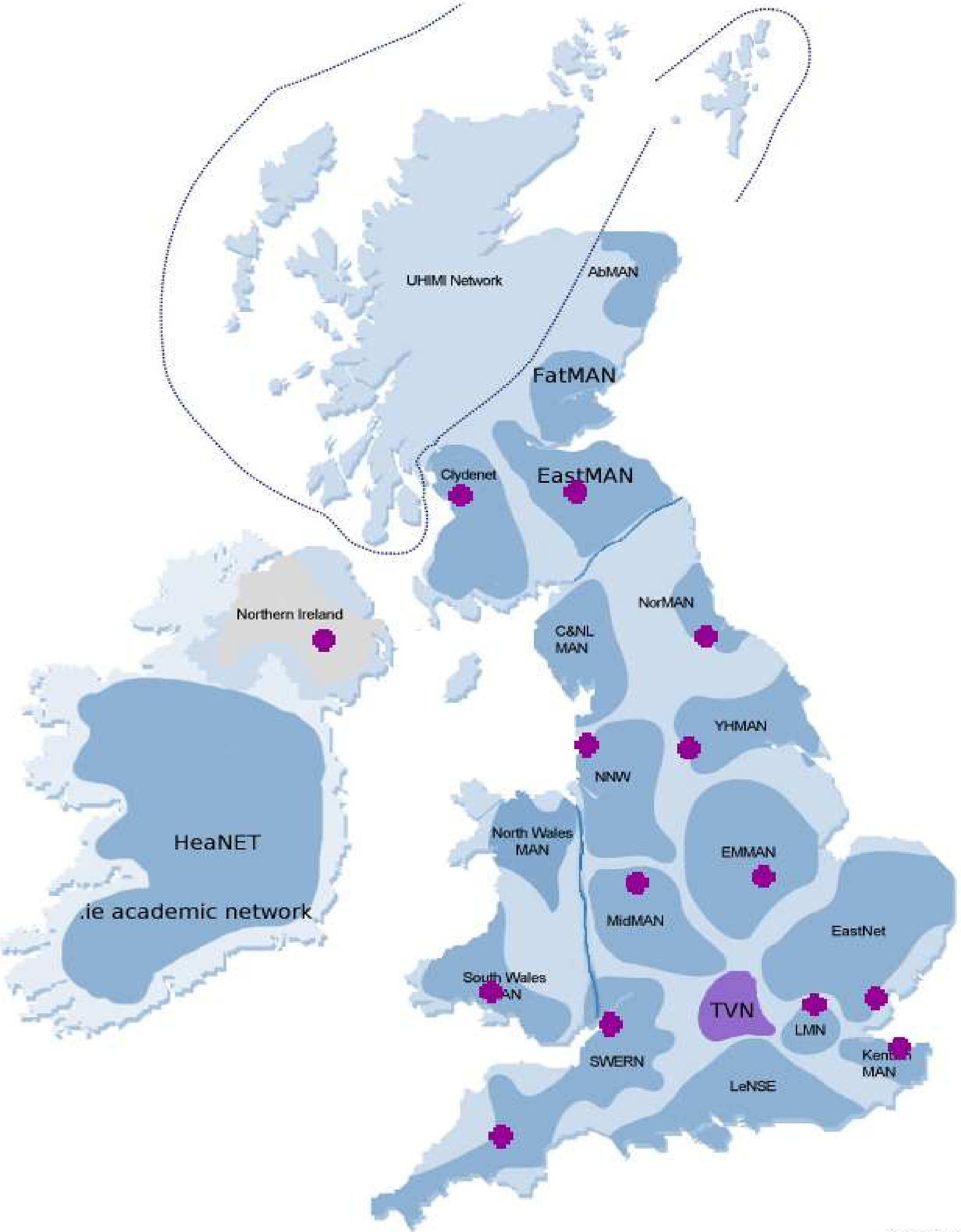
- Nearly all JANET sites connect to a MAN
- One MAN router sees all traffic for connected sites
- Under contract to JANET
- Contractually obliged to assist JANET-CERT
- Each has security contact
- Can apply network blocks under instruction from JC
- RNOs are separate legal entities from JANET

RNOs

RNOs used by JC

- To perform Netflow analysis
- Report probes
- To track unusual traffic **not** on the backbone
- IntraMAN traffic
- Useful for blocking as close to the offending machine as possible.
- Usually also the some of the same people as big uni CERTs

JANET Networks and RSCs



Regional Support Centres

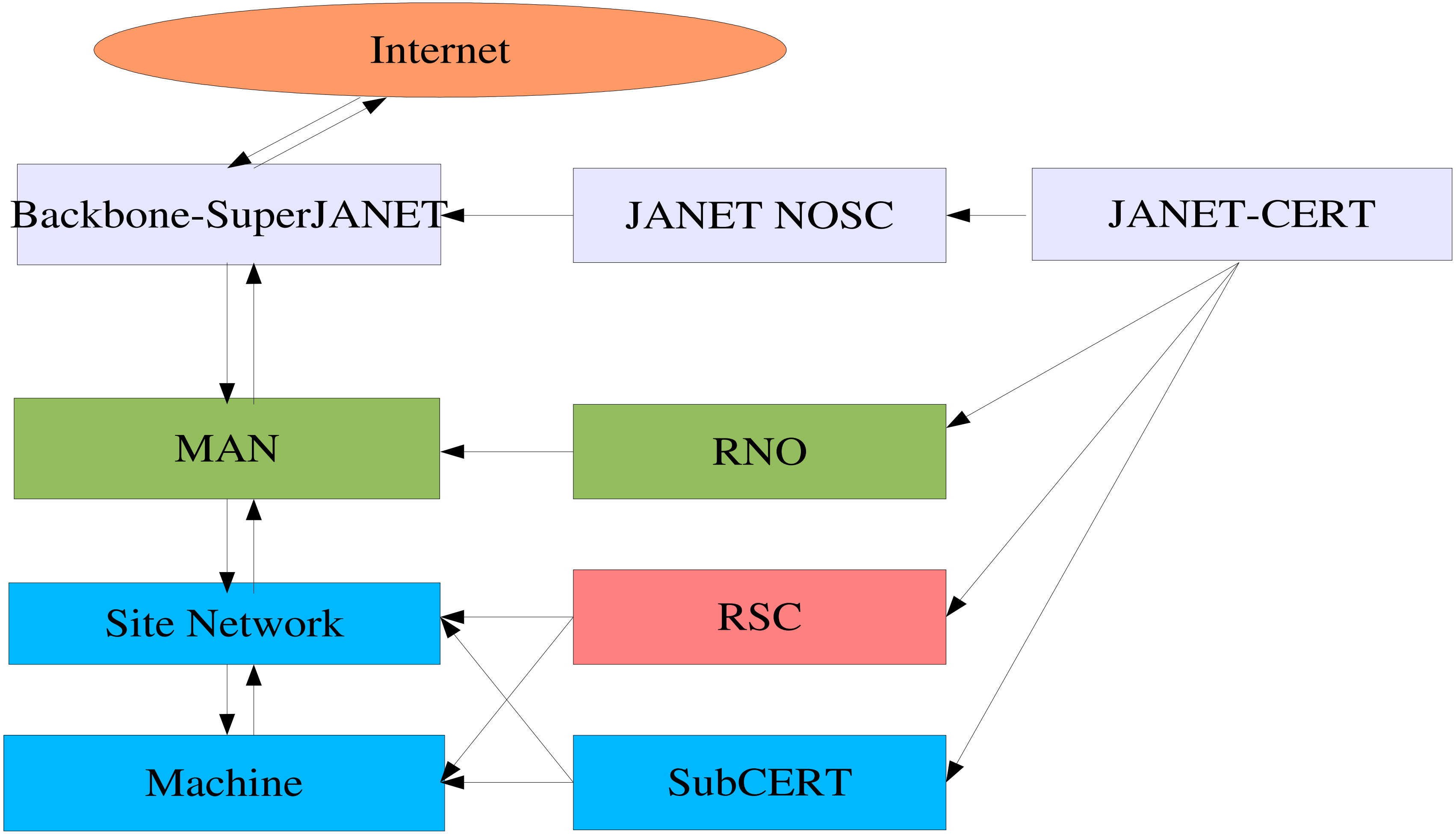
For customer organisations that do not have technical staff, they support:

- Further Education colleges (<6000 students),
- Specialist colleges (<100 students),
- Other small sites
- Funded by same people who fund JANET
- Usually based at a big University
- Not part of JANET (big mistake)

RSCs

- Used by JC for incidents where small site cannot do their own incident response.
  - May also be the same people as run the MAN
  - Usually set up the small site's router and know their network.
  - Can access router at problem site, know the people, have been there before
  - Often is the same people as University CERT
- In a **very** useful position for JANET-CERT
- BUT, don't have to help us. At all.

JANET-CERT has multiple paths



SubCERT involvement

SubCERTs play an active role in JC services

- Netflow Analysis
- Probe reporting
- Forensics

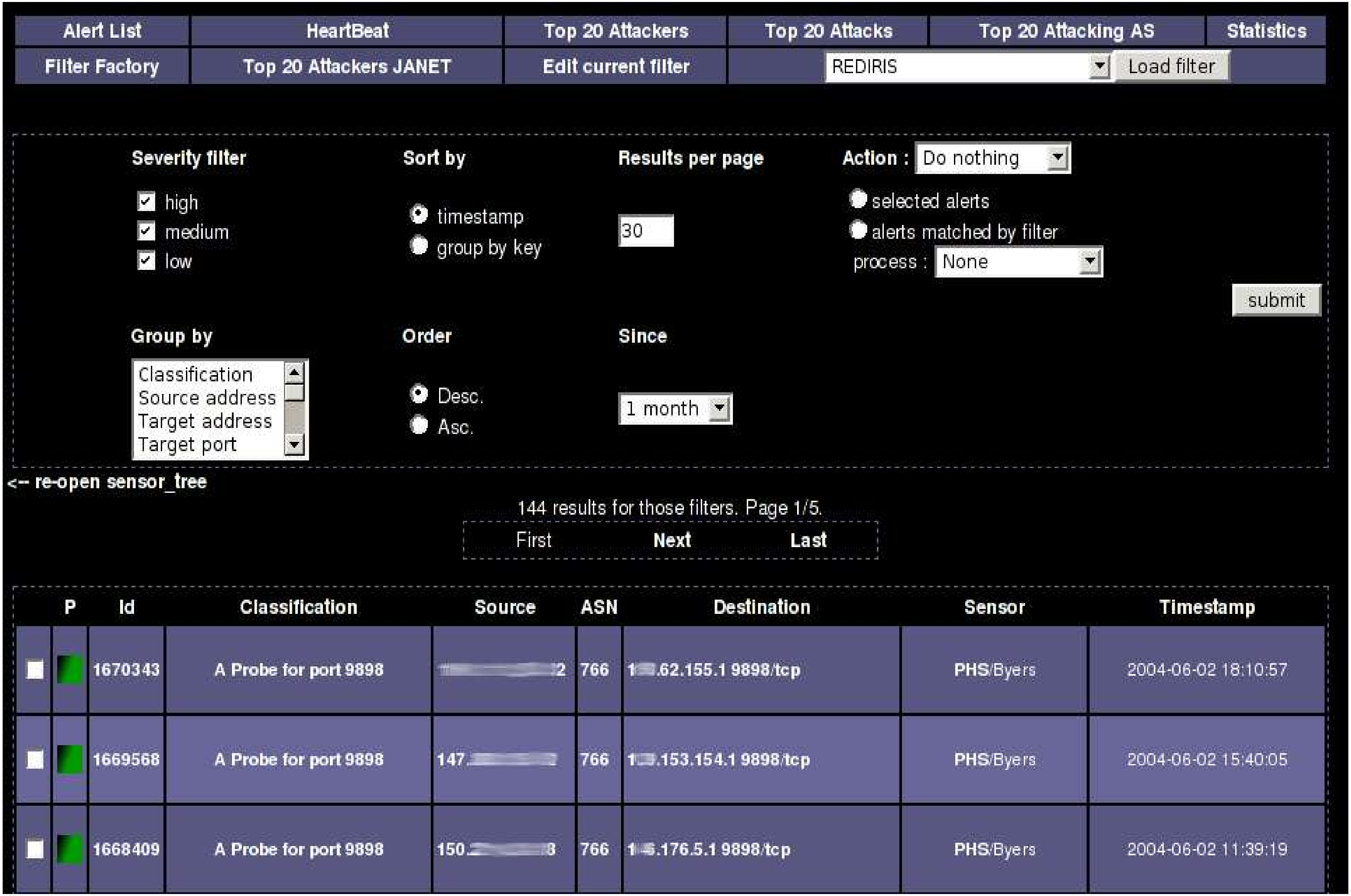
JC acts as co-ordination centre for SubCERTs, and as escalation point.

- All subCERT -> subCERT activity routed through JC
- SubCERT -> outside routed through or cc'd to JC

Netflow

- SubCERTs report probe activity
  - Trusted subCERTs have direct access to JC probes system
  - Can report scans of their netranges directly into the JC database
  - Saves JC a lot of work analysing 600GB of Netflow / day
  - JC act as central coordination centre for scanning complaints
  - JC alerted of scans reported directly to our PHS

Probe Reporting/Flow Analysis



REDIRIS

Severity filter
☑ high
☑ medium
☑ low

Sort by
● timestamp
○ group by key

Results per page: 30

Action : Do nothing
○ selected alerts
○ alerts matched by filter
process : None

Group by
Classification
Source address
Target address
Target port

Order
● Desc.
○ Asc.

Since: 1 month

144 results for those filters. Page 1/5.

	P	Id	Classification	Source	ASN	Destination	Sensor	Timestamp
□	🟩	1670343	A Probe for port 9898	[redacted]2	766	1[redacted].62.155.1 9898/tcp	PHS/Byers	2004-06-02 18:10:57
□	🟩	1669568	A Probe for port 9898	147.[redacted]	766	1[redacted].153.154.1 9898/tcp	PHS/Byers	2004-06-02 15:40:05
□	🟩	1668409	A Probe for port 9898	150.[redacted]8	766	1[redacted].176.5.1 9898/tcp	PHS/Byers	2004-06-02 11:39:19

Support for SubCERTs

Training

- JANET-CERT security course
- TRANSITS - rewritten by JC for delivery to JANET
- JC Security Conference – CERT contacts only
- All **really** cheap

Ongoing support

- Mailing lists
- Emails written for them to show to their managers

Advantages

For JANET-CERT

- We can always get someone out of bed to deal with an incident
- We have experienced incident handlers at many sites
- Or available outside the site to attend the problem
- We can delegate responsibility to someone else to ensure a **complete** resolution at no cost to us
- SubCERTs feel part of JANET security team.
- SubCERTs do some of our work

Advantages for SubCERTs

A 'real' SubCERT tends to be taken more seriously by managers

Separate reporting path to senior management

Better funding

- CERTs usually earn more money ;-)

Better working relationship with central CERT (JANET-CERT)