

DANCERT and securing the GÉANT network

**Robert Walton, Security
DANTE
11th TF-CSIRT**

Who Are DANTE?

- Established in 1993 and based in Cambridge, UK
- A not-for-profit organisation
- Created and owned by a number of Europe's National Research and Education Networks (NRENs)
- DANTE organise, manage and build pan-European research and education networks
- 2002 Annual Turnover – approximately 50M Euros
- 24 staff members (10 nationalities)

DANTE's Role

- GÉANT is operated by DANTE to provide a pan-European Multi-gigabit research and education network
- Actively involved in developing new network services to support the European research and education community
- DANTE also participates in:
 - EUMEDCONNECT (Mediterranean)
 - ALICE (Latin America)
 - SEEREN (South Eastern Europe)
 - SERENATE (next generation studies)
 - 6NET (IPv6)

DANCERT

- Is the Incident Response team within DANTE
- Is responsible for the security policy within DANTE
- Involved within GÉANT as regards security policy and Authentication and Authorisation issues.
- Designs and implement security features on the GÉANT network.

What is GÉANT?

- 6th generation of pan-European research network infrastructure
- Connecting national research and education networks (NRENs) in 32 countries around Europe
- Serving over 3500 research and education establishments across Europe
- Providing international connectivity to other world regions
 - Abilene, CANARIE and ESnet in North America
 - SINET in Japan
- Funded jointly by NRENs and European Commission
- Project timescale November 2000 - October 2004



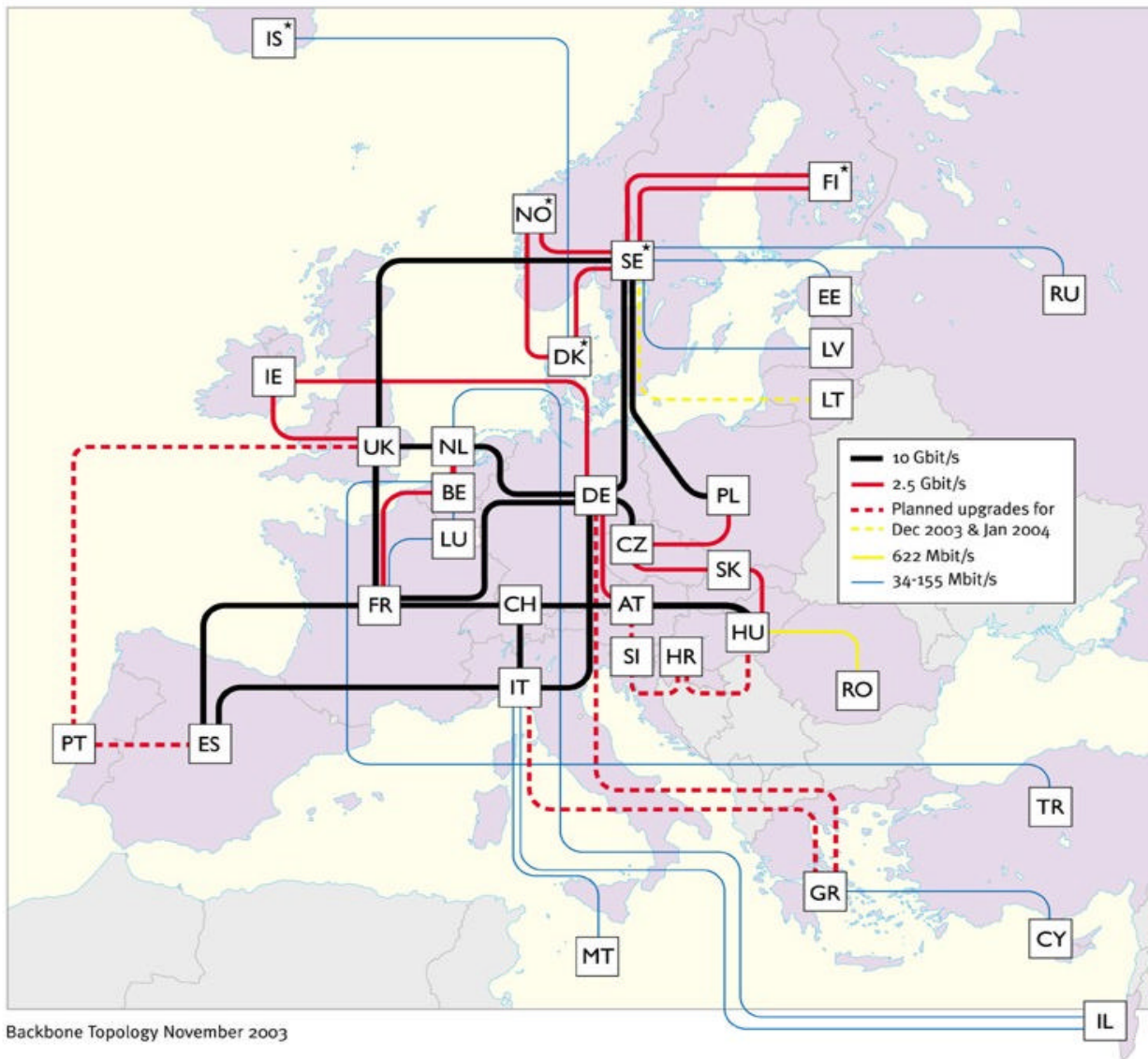
NRENs (National Research and Education Networks) served by GÉANT

AUSTRIA	ACOnet	LATVIA	LATNET
SLOVENIA	ARNES	LITHUANIA	LITNET
BELGIUM	BELNET	NORDIC countries	NORDUnet
CROATIA	CARNet	POLAND	PSNC
CZECH REPUBLIC	CESNET	SPAIN	RedIRIS
CYPRUS	CYNET	FRANCE	RENATER
GERMANY	DFN	LUXEMBOURG	RESTENA
ESTONIA	EENet	ROMANIA	RoEduNet
PORTUGAL	FCCN	SLOVAKIA	SANET
ITALY	GARR	THE NETHERLANDS	SURFnet
GREECE	GRNET	SWITZERLAND	SWITCH
IRELAND	HEAnet	TURKEY	TUBITAK-ULAKBIM
HUNGARY	HUNGARNET	UK	UKERNA
ISRAEL	IUCC	MALTA	University of Malta



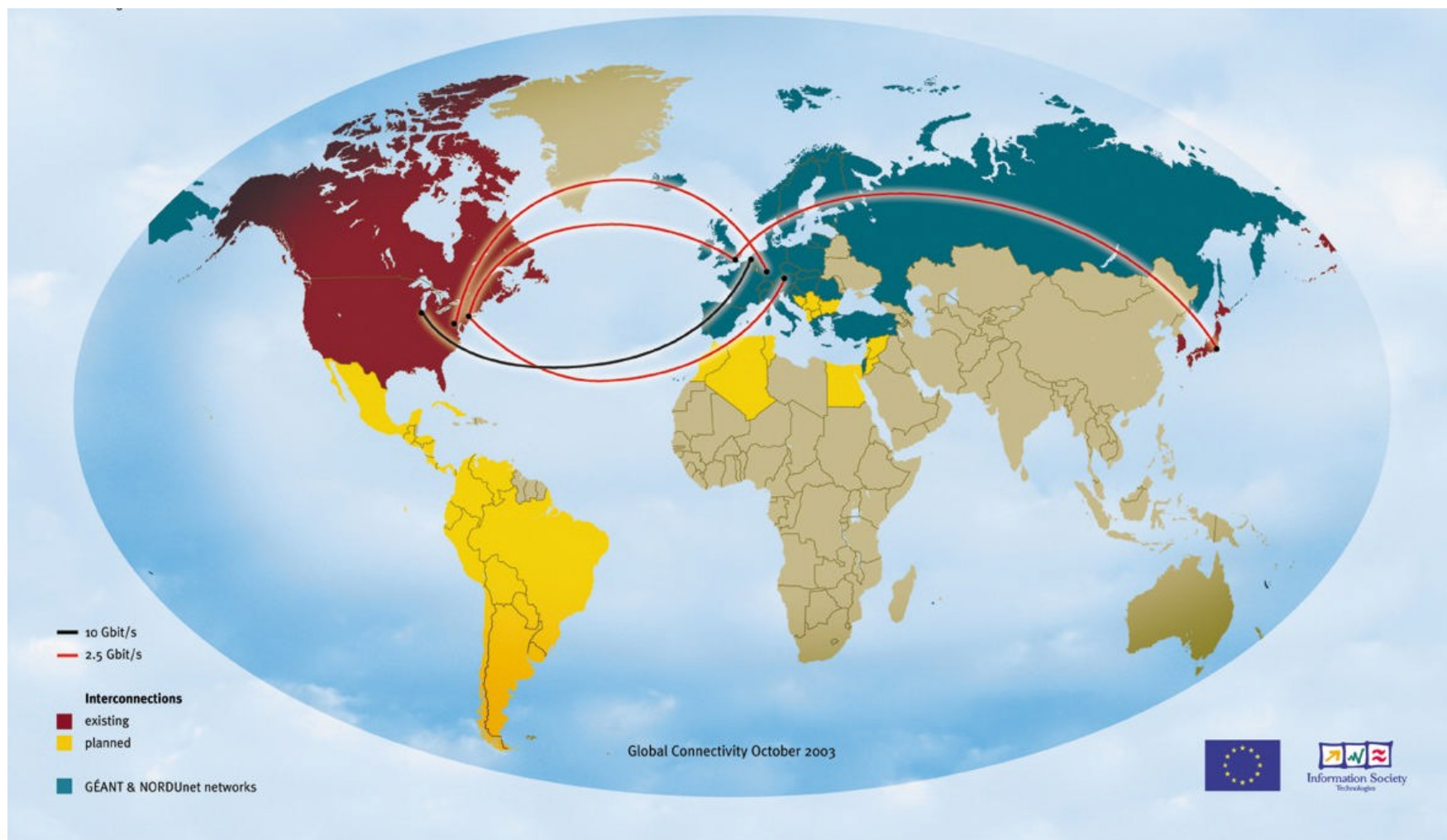
Multi-Gigabit pan-European Research Network

Backbone Topology November 2003



- Connecting 32 European Countries and 28 NRENs
- Backbone capacity in the range of: 34Mb/s-10Gb/s

Global Connectivity-October 2003



DANCERT and GÉANT

1. The day to day security
2. Help ensure the high level of integrity and stability on the network.
3. Consider security implementations of newer network services
 - Quality of Service
 - Multicast
 - MPLS
 - IPv6
4. Provide a platform of report and response for the network.

DANCERT: Incident Response

Being a transit network we don't have any directly connected users.

- Spam rpts - intermediary response
- Scanning rpts - intermediary response
- Hacking rpts - intermediary response
- DoS attacks - DANCERT DoS tool
- Continue investigation: Severity

DANCERT DoS Tool

Denial Of Service Filtering

[help](#)

Filtered Address

Destination
 Source

PoPs

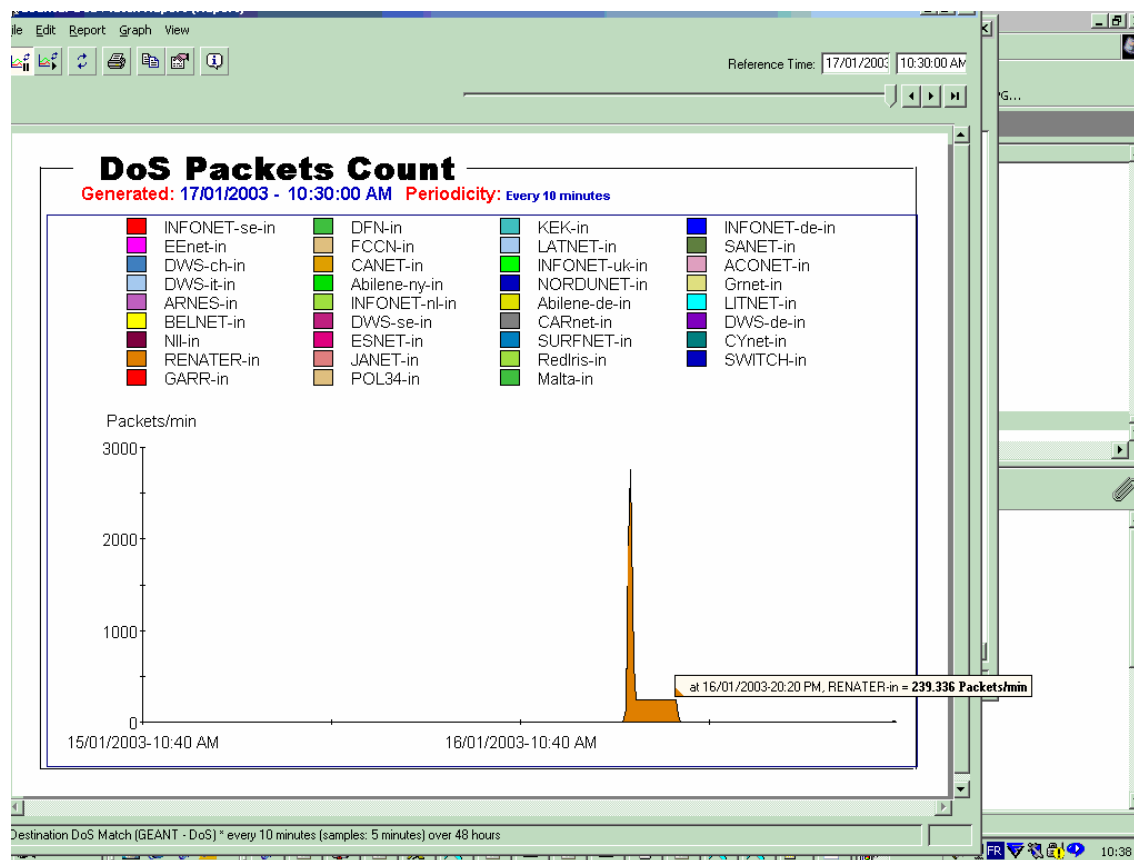
at1.at be1.be ch1.ch de1.de de2.de
 si1.si sk1.sk nl1.nl se1.se ny5.ny
 pl1.pl es1.es uk1.uk hu1.hu fr1.fr
 it1.it ie2.ie All

Action To Perform

Filter new address
 Remove filter for specified address
 Show filtered addresses

[Link to VistaPortal Server \(InfoVista statistics\)](#)

DANCERT DoS Tool



GÉANT security implementation is DANTE additional to the ‘usual’



- Strong password policy
- SSH access only to network equipment
 - SSH access is additionally filtered using prefix lists
 - Access is treated on a ‘required’ basis only.
- Filter and log traffic to lo0 interface
- Filter packets with bogon source addresses at network edge.
- MD5 authentication
 - All eBGP peerings for both IPv4 and IPv6
 - All iBGP peerings for both IPv4 and IPv6

Driving the GÉANT security implementation

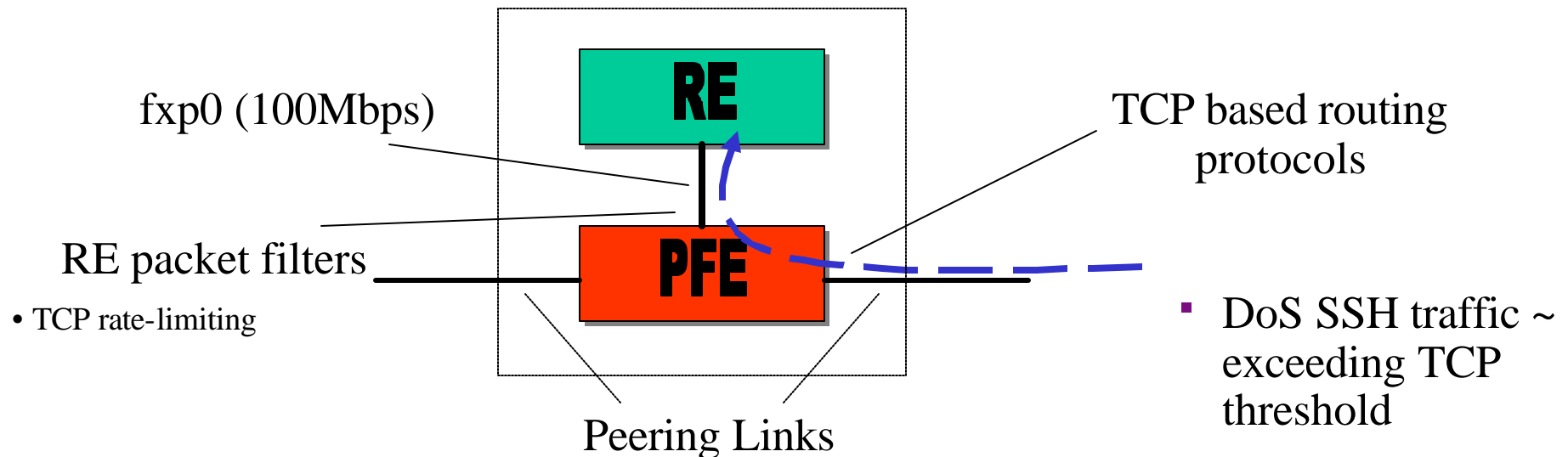
- High Bandwidth Capacity - DoS attacks on backbone links not a realistic concern.
- RIPE AS macro per NREN
- Ability to ‘manage’ illicit traffic effectively
- New Services
- Vulnerabilities of network equipment to DoS.

Protecting the Core Equipment

WHY?

- Designs of router hardware and service application makes core routers vulnerable to DoS attack.

Example:

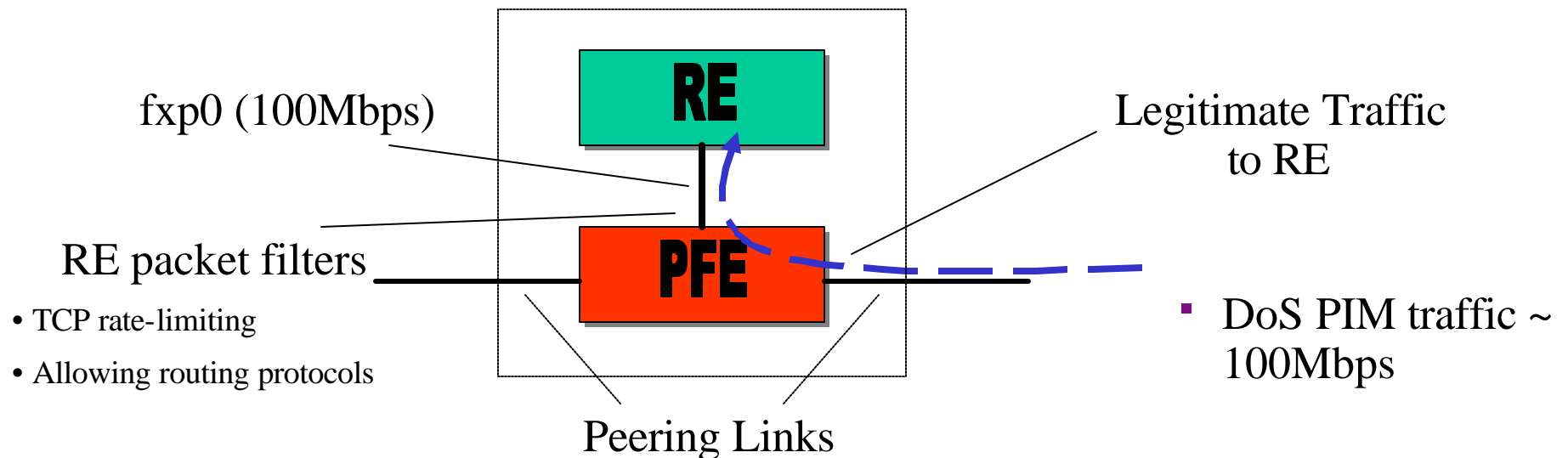


Protecting the Core Equipment

WHY?

- Designs in router hardware and service application makes core routers vulnerable to DoS attack.

Example:



Protecting the Core Equipment

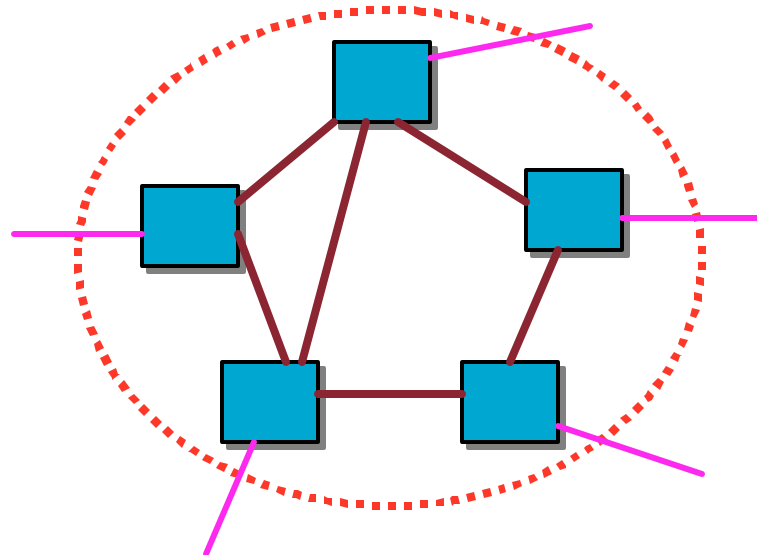
WHY? Cont....

- Prevent scanning of ALL network equipment- e.g.webservers.
- Zero day exploits - reduce the potential for effect (SSH, snmp)
- Protect integrity of none MD5'd routing protocols - MSDP
- Spot attempted attacks - monitoring system (in process)
- Easy to manage due to generic nature
- Services that require to accept traffic that affects CPU from anywhere in the internet - PIM rate limiting (in process)

Protecting the Core Equipment

How?

- Applying packet filters on the edge interfaces of the network, specifically only for traffic destined for GEANT equipment...

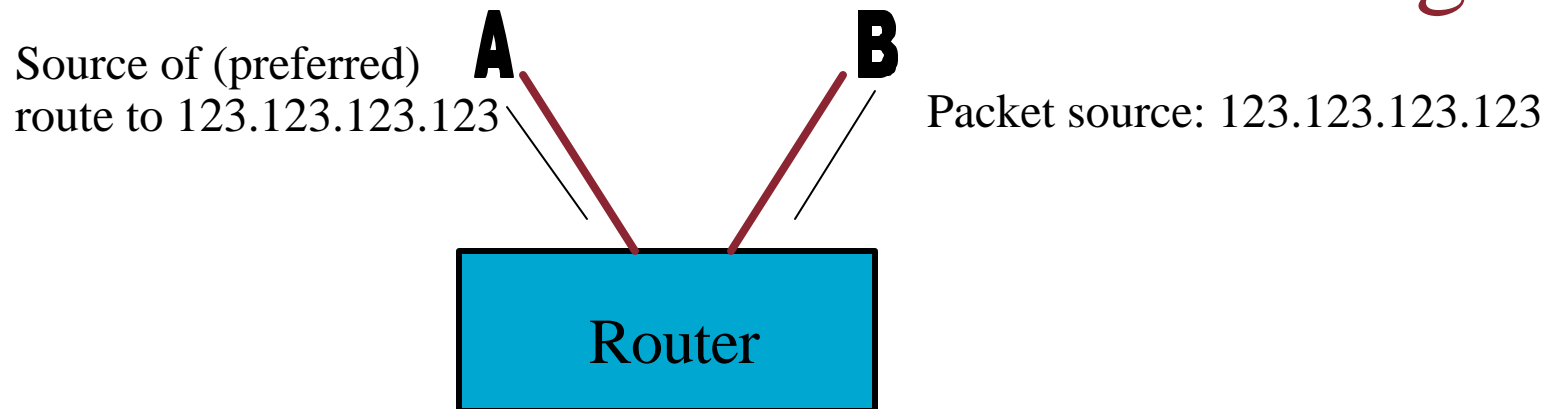


Protecting the Core Equipment

How? Cont...

- Specifying allowed protocols
- Filtering packets on source where possible - BGP, SSH, snmp
- Filtering packets on TTL where possible - eBGP, eMSDP
- Specific discard terms for the 'more' illicit packets.
- Rate-limiting protocols where possible (in process)
- Discarding everything else towards 62.40.96/19

Unicast Reverse Path Forwarding



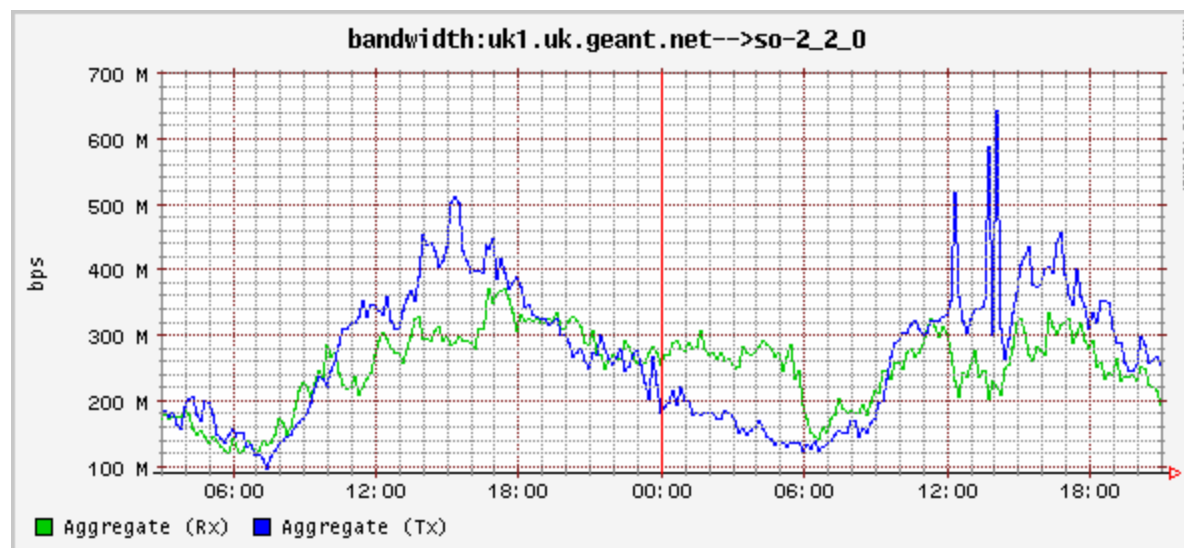
- Anti-spoofing measure based on the routing table
- Different flavours: Strict, Feasible and Loose
- Why this works with GEANT - NREN RIPE AS macro's
- Applied to 90% of GEANT NREN access interfaces.
- Allowance for leakage traffic - 200kbps
- To be included in monitoring infrastructure.

uRPF issues

- Tunnel PIC application on Juniper routers - unexpected behaviour.
- Leakage can suggest poor network performance rather than route filter issue.
- Investigating possible alternative implementation:
 - packet filters, generated by NREN RIPE AS macro, inserted into uRPF application.
 - As above, but the ability to to add prefixes to allow for leakage.

Monitoring Infrastructure (in process)

Web based interface for both NREN's and DANCERT/GEANT NOC; representing how much traffic has been discarded by the major filters e.g. bogon and core attack



Monitoring Infrastructure

Plans to implement a logging and alarm structure for the potentially more serious packets and traffic patterns:

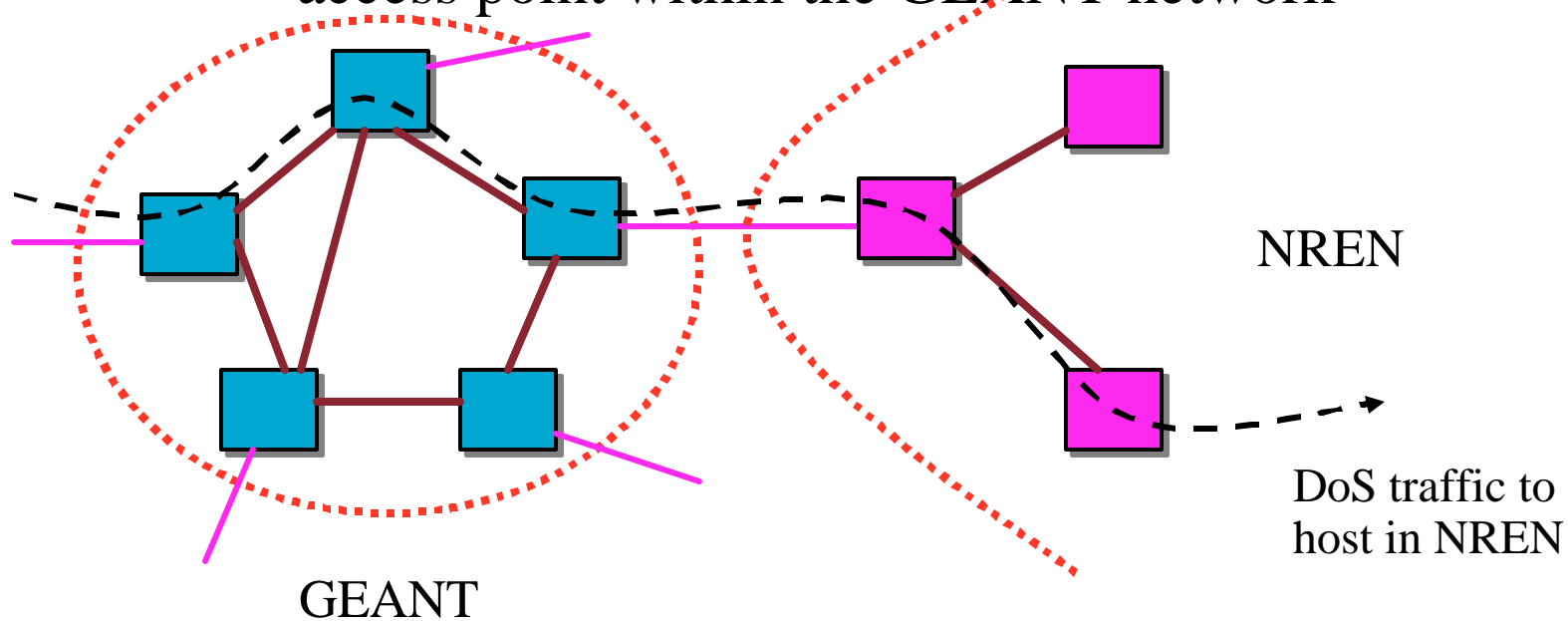
- BGP, MSDP, SSH packets that are deemed as illegitimate
- Packets that exceed rate-limiting thresholds (excluding ICMP and UDP traceroute) - NTP, PIM et al....
- Notification when specific rate-limiting functions are being exceeded.

Other works in process

- Rate limiting of protocols destined for RE of core routers.
- Counteract specific DoS vulnerabilities from new services.
 - Multicast requires that a router receive PIM packets to the RE from anywhere in the internet.
 - MPLS - RSVP
- In addition, protocols such as ntp, snmp, SSH.
- Study will be completed on GEANT test bed for a deemed level of acceptable use - and then we'll double it!!!!

Dynamic NREN Blackhole Routing

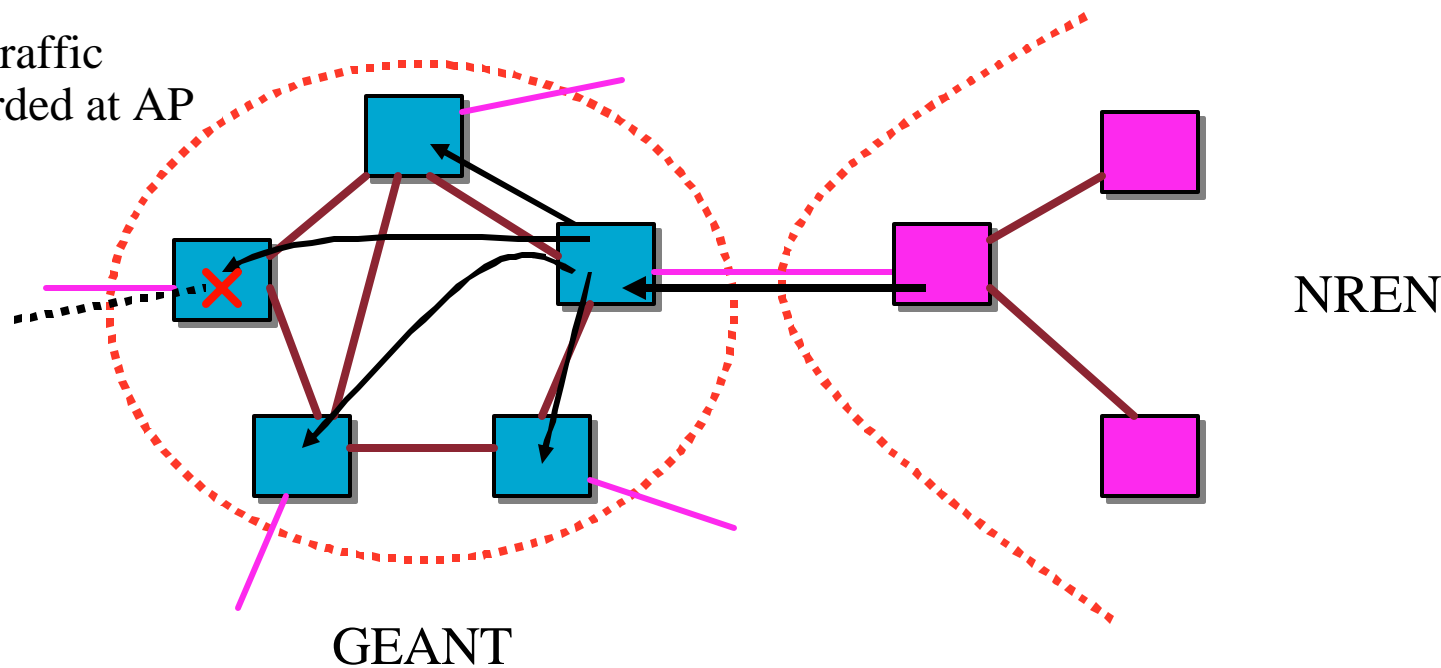
We are undertaking a feasibility study at present regarding the potential ability of NREN's to blackhole DoS traffic at a given access point within the GEANT network



Dynamic NREN Blackhole Routing

NREN advertises blackhole route to GEANT using specific community which is distributed to all routers in GEANT.

DoS traffic
discarded at AP



Dynamic NREN Blackhole Routing

NREN accesses web based blackhole monitoring tool - inputs the destination address of the victim which inturns updates logging and counting packet filters on discard interfaces.

Denial Of Service Filtering

[help](#)

Filtered Address

Destination
 Source

PoPs

at1.at be1.be ch1.ch de1.de de2.de
 si1.si sk1.sk nl1.nl se1.se ny5.ny
 pl1.pl es1.es uk1.uk hu1.hu fr1.fr
 it1.it ie2.ie All

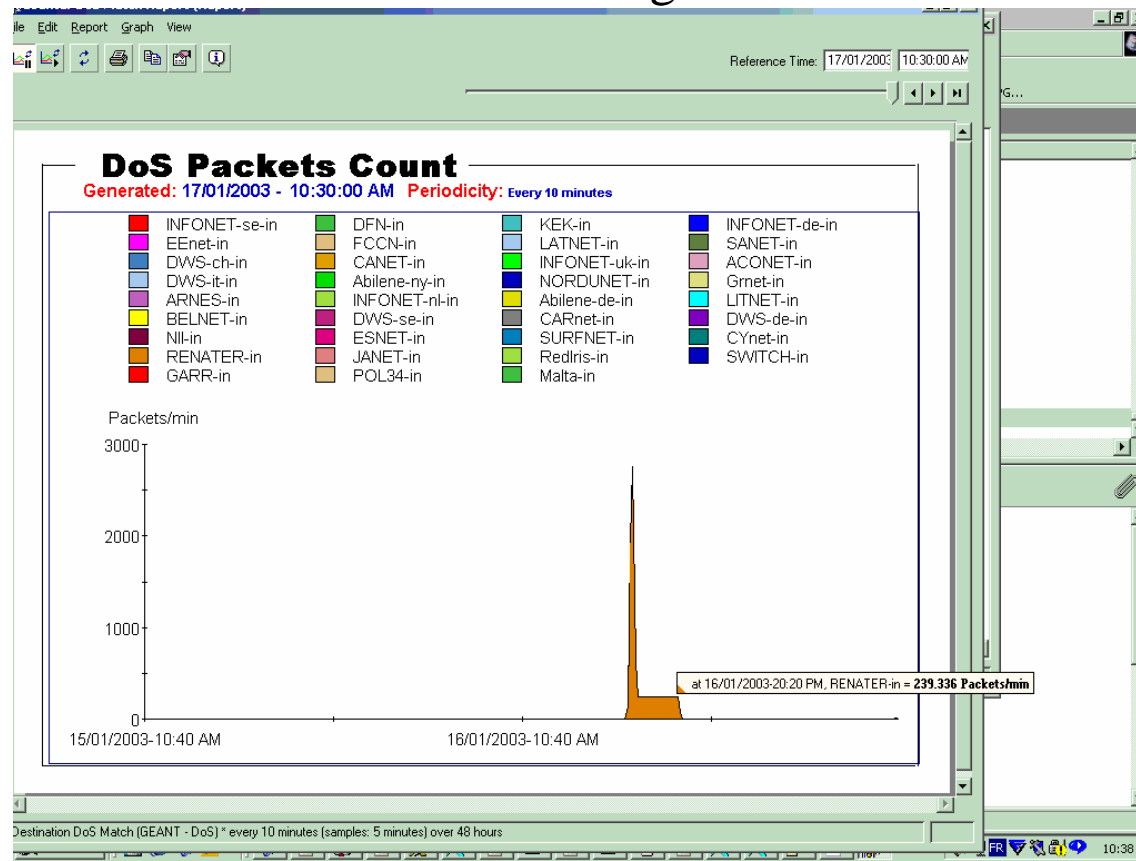
Action To Perform

Filter new address
 Remove filter for specified address
 Show filtered addresses

[Link to VistaPortal Server \(InfoVista statistics\)](#)

Dynamic NREN Blackhole Routing

NREN can the deduce using web based tool at which GEANT router the traffic is being discarded



Dynamic NREN blackhole routing

- NREN's will only be able to advertise routes associated to their RIPE AS macro.
- The technical aspect of GEANT side already concluded
- NREN side of technical still to be concluded
- Monitoring infrastructure already there from DoS tool
- Additional work making this 'web based' - Authentication etc..
- Will be put to APM's before implementation work begins.

QUESTIONS???

Any security issues should be addressed to
dancert@dante.org.uk and security@noc.geant.net

Robert Walton fingerprint:

0644 B936 ECEC 5C70 EC1C BCF1 7DC6 E963 405F 2DA2