DDoS Detection & Mitigation Experience @ ACOnet

RIPE 50, Stockholm

May 3, 2005

Christian.Panigl@UniVie.ac.at

Zentraler Informatikdienst
Universität Wien

aconet

Agenda

- Who is ACOnet
- Why DDoS Protection
- Selected Products
- Experience & Lessons Learned
- Future

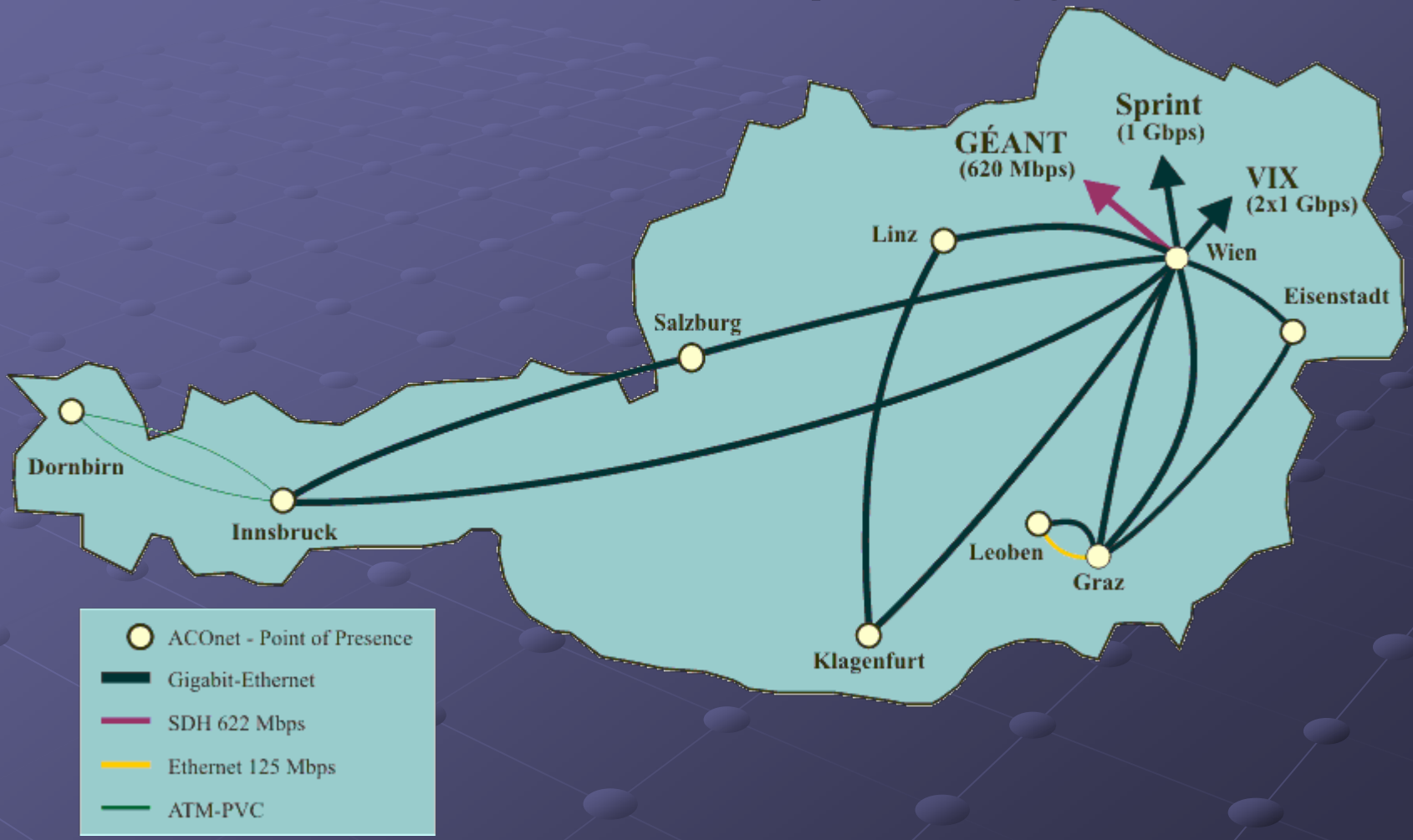
Who is ACOnet

- Austria's NREN http://www.ACO.net/
  - Connecting Universities,
    regional School Networks,
    Research Institutes,
    governmental Departments
  - Switched/Layer2 GbEthernet Core (AT-wide)
  - Routed/Layer3 Global Connectivity Service
  - Operated by UniVie and operations partners at universities hosting a POP

Zentraler Informatikdienst
Universität Wien

aconet

ACOnet Topology



Zentraler Informatikdienst
Universität Wien

aconet

Why DDoS Protection ?

- Regular attacks experienced since 2001 specifically towards IRC servers (at universities in Linz, Graz, Vienna)
- Attacks have been affecting POP infrastructure and customers
- UniVie technically responsible for .AT-ccTLD nameservers

Why “Riverhead“ Guard ?

- Scaling well for our network size and topology
- Diversion model instead of in-line
- „Self removing“ in case of failure
- Excellent & helpful staff cooperation during test installation and early production phase
- Good understanding of customer needs
- Fast and flexible with implementation of improvements

Why Arbor Peakflow ?

- Complementary tool needed for Anomaly Detection in the core
- Neither Cisco Detector nor IDS generally suited for anomaly detection in the core
- Looking for Netflow based analyzer
- Talking to other “Riverhead” users
- Testing Arbor: Peakflow/DoS & Traffic
- Promise to integrate & consolidate and to directly interface with Cisco Guard

Experience and Lessons Learned

- Generally good experience with both products, however
  - Peakflow quality highly depends on Netflow quality, which hasn‘t been as good as expected on our Cat65k
  - Cisco Support (?)
  - Learning curve longer than expected on Arbor products

Future

- Still working on migration to consolidated platform (Peakflow SP)
- Integration with Cisco Guard
- Cooperation with upstreams and peers
- “Fingerprint Sharing” !?
- Keeping our minds open for other / complementary solutions