SÉCURITÉ.ORG

Hack.LU 2006

In SPace Nobody Can Hear You Scream

Nicolas FISCHBACH
Senior Manager, Network Engineering Security, COLT Telecom
nico@securite.org - http://www.securite.org/nico/

v1

COLT

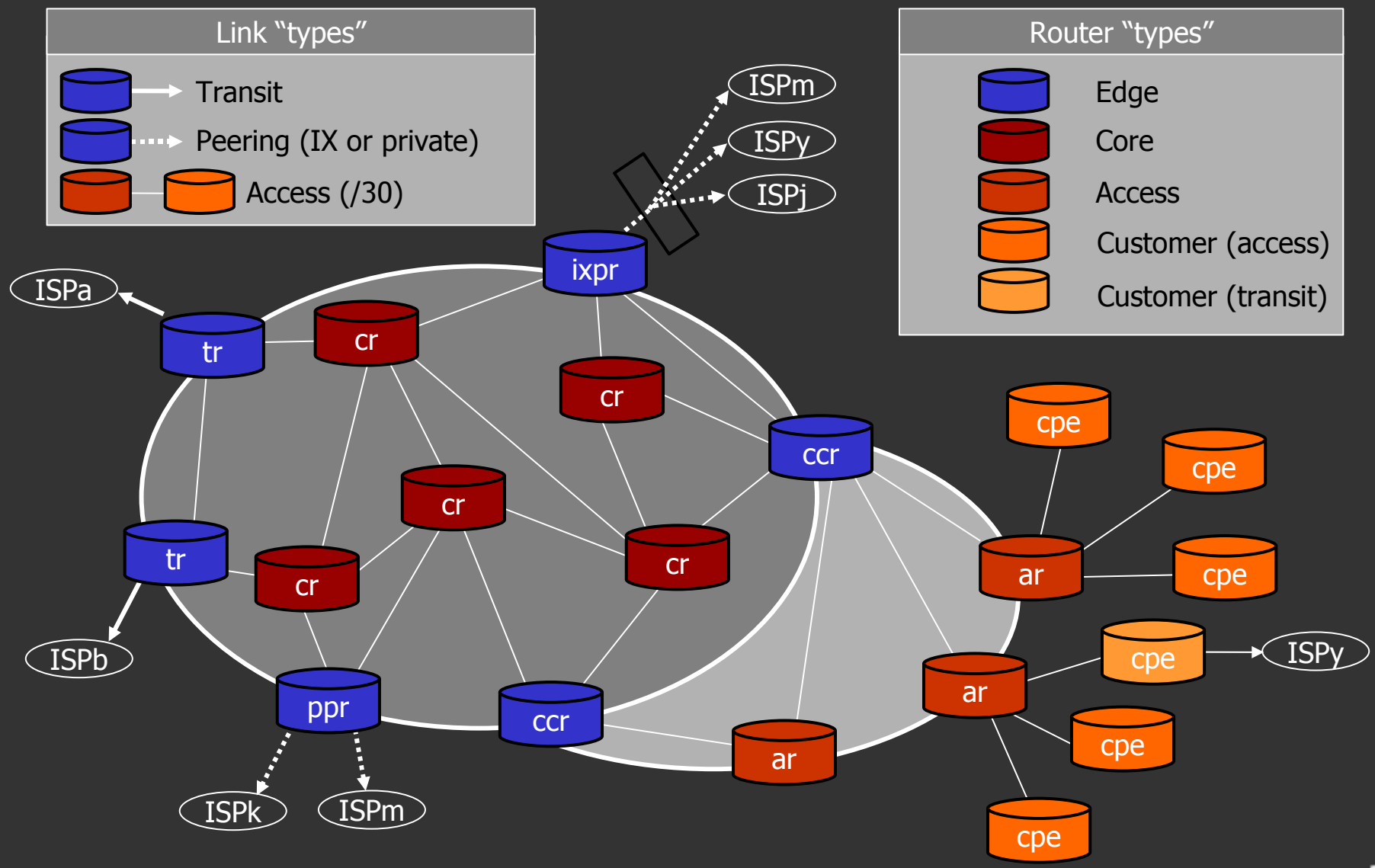
Internet-wide Security Issues

- **What kept us up at night :)**
- SNMP
- SQL Slammer (and friends)
- Cisco wedge bug
- BGP TCP window [not really actually]
- Botnets and DDoS

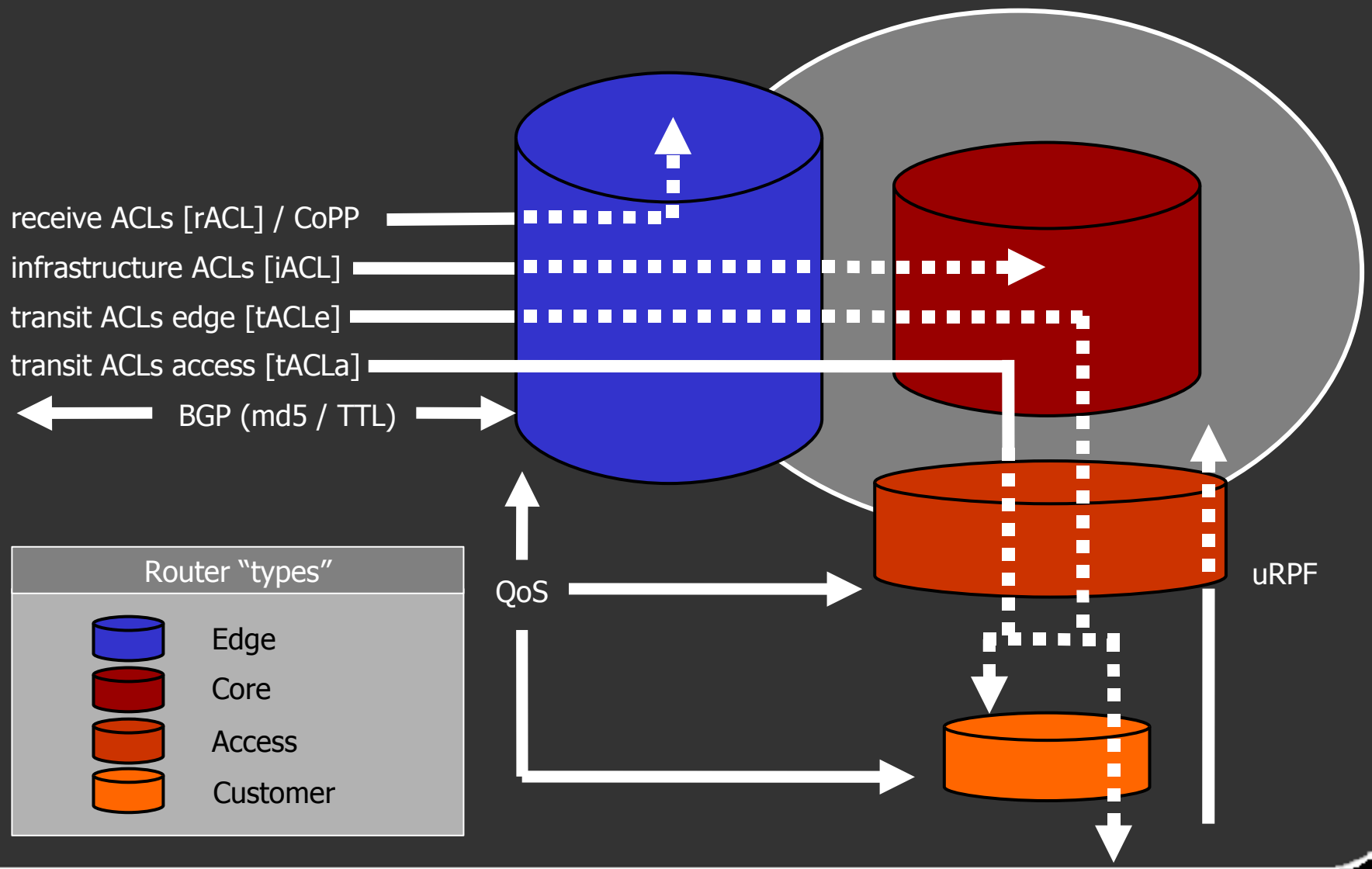
Internet-wide Security Issues

- **What have we done about it ? A lot. Too much maybe ?**
- Route/prefix filtering
- DDoS detection: Netflow
- DDoS mitigation: BGP (+ MPLS (+ Cleaning))
- xACLs and MPLS Core hiding
- QoS and Control Plane Policing (CoPP)
- BGP TTL trick (GTSM) and BGP TCP md5
- Unicast RPF (uRPF)
- Router security 101

Carrier Backone

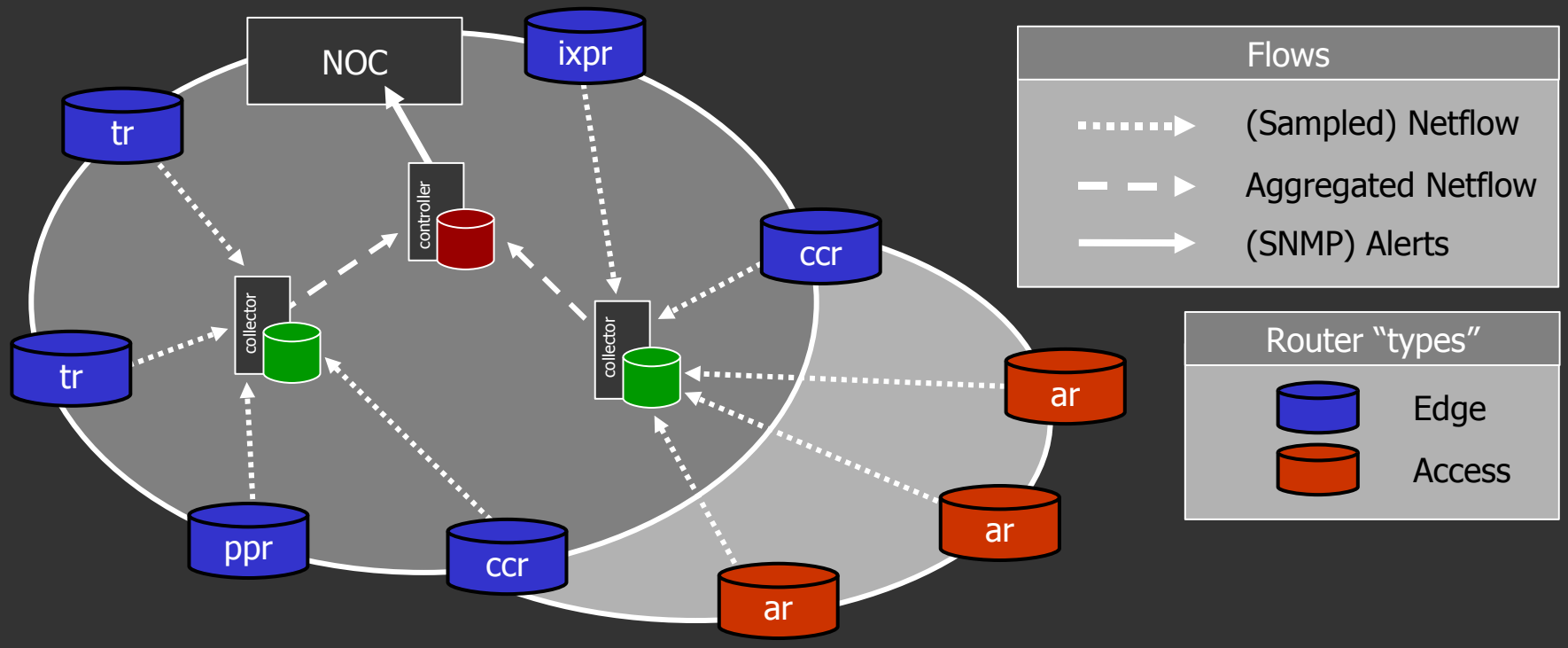


Carrier Backbone Security

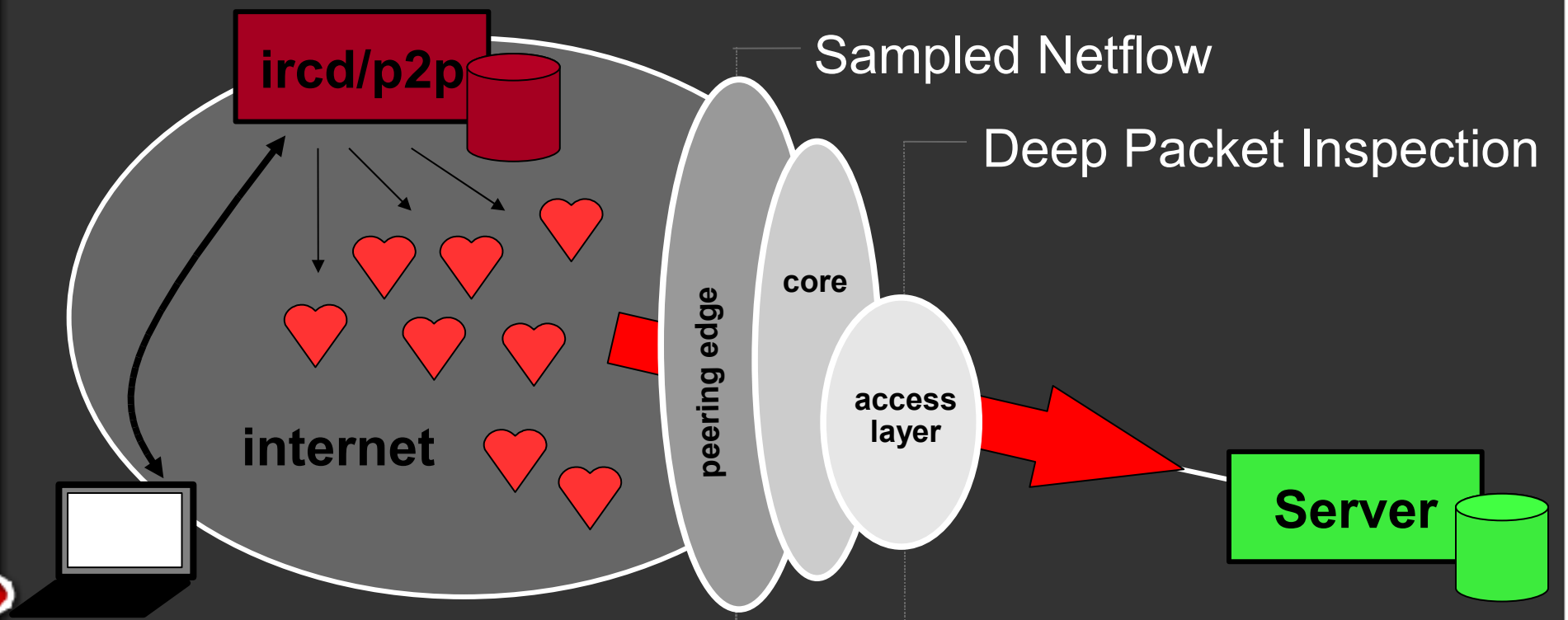


Carrier Backbone DDoS Detection

- Netflow (src/dst IP/port, protocol, ToS, interface - no payload, BPS/PPS/Time)



DDoS Attack Mitigation



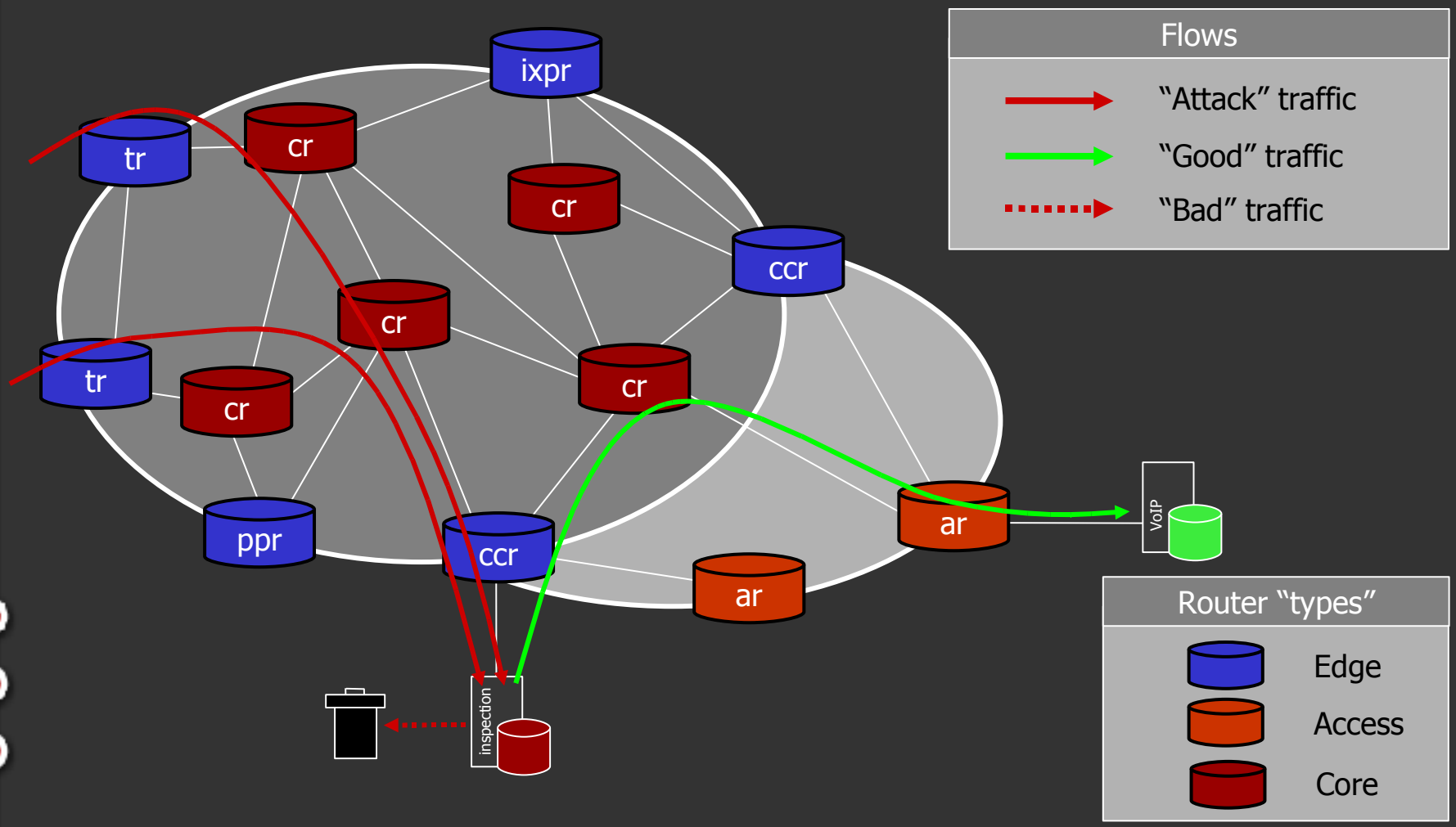
Sampled Netflow

Deep Packet Inspection

Network Level Mitigation

Data Center Level Mitigation

Carrier Backbone DDoS Mitigation



Internet-wide Security Issues

- **What has really changed ?**
- Route filtering : quite relax still
- DDoS detection, but weak mitigation : DDoS == background noise
- QoS : not for security, but for NGN
- CoPP : not widely deployed
- uRPF : not widely deployed
- BGP : md5 common (but useful ?), TTL-trick (the exception)

Internet-wide Security Issues

- **Have we learned the lesson ?**
- IPv6
- Lots of security features in software (not in hardware)
- Will we ever see SoBGP / Secure BGP ? Do we need it ?
- Going up the stack, no mitigation at network level anymore (everything on top of 80/tcp, DNS attacks, etc)

Security Features

- **What's the driver ?**
- How to get those features across product ranges and vendors
- Shift of features towards edge, access, last/first mile
- But these features are not (often) security features
- Devices that never “saw” the “bad” Internet
- Features vs power vs cooling
- Hardware limitations (FPGA, ASIC, NP)

Security – which future ?

- No “big” “nation-wide” “critical infrastructure” issue recently
- IP/Data network infrastructure has become a commodity (until it's down)
- No focus on infrastructure security anymore (but the wake up call will be “funny”)
- So where do people put security research and resources into ?

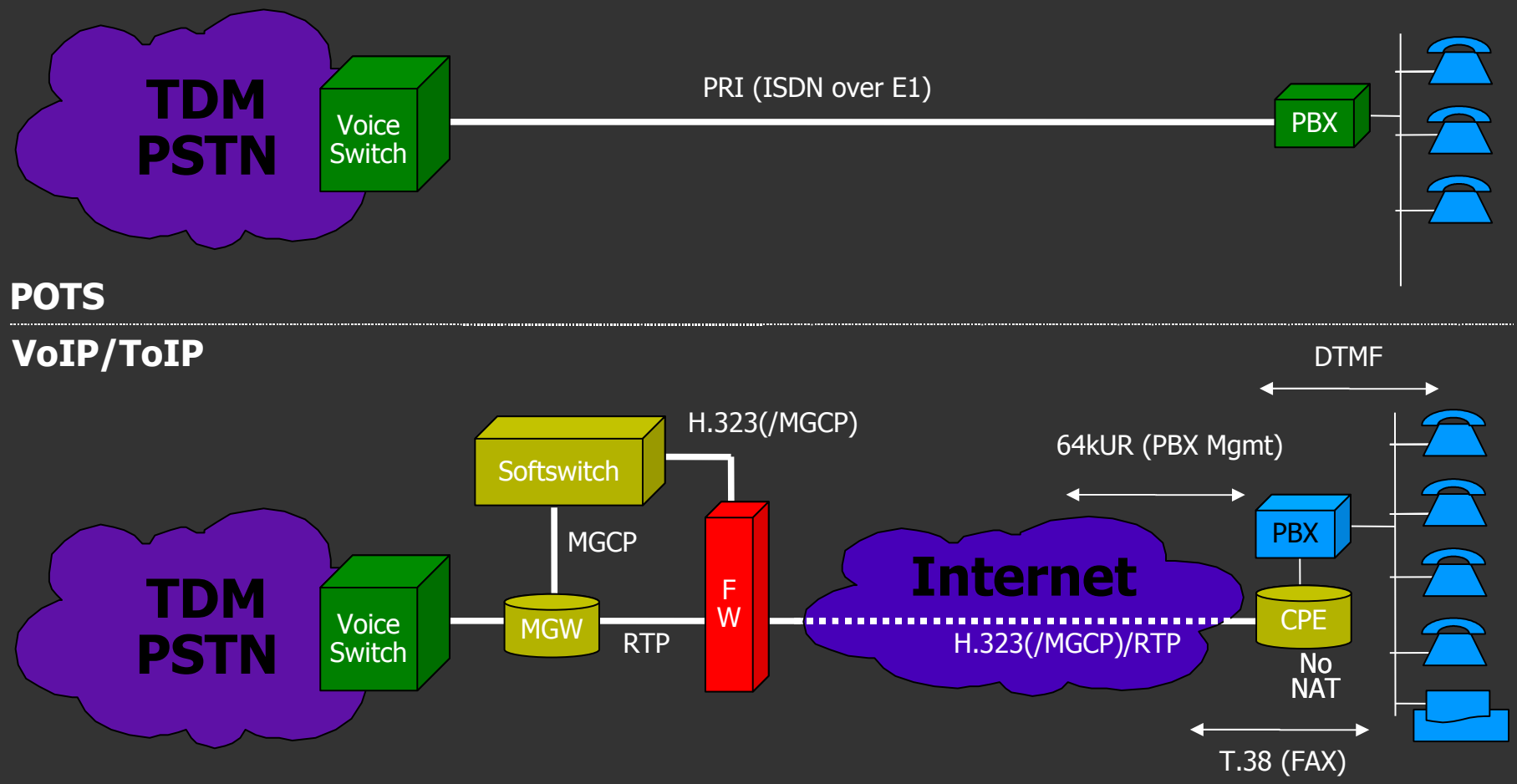
NGN

(Next Generation Networks)

NGNs

- **Next Generation Networks**
- VoIP and IMS
- Ethernet/DSL services
- Converged Networks
- Moving up and down the stack at the same time

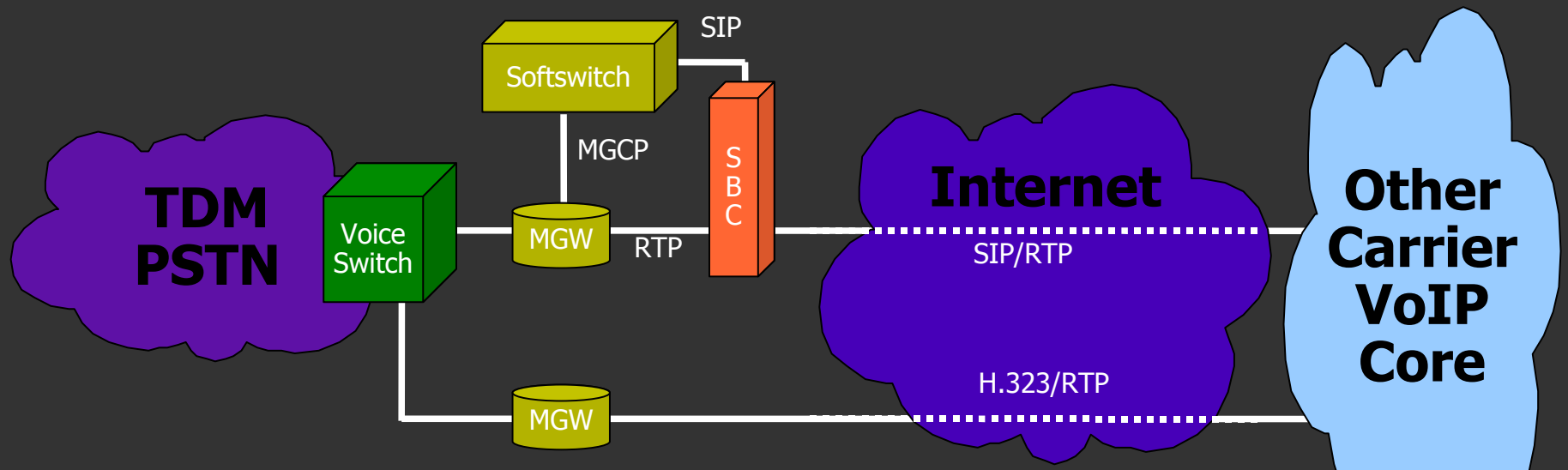
PBX Trunking over IP



Wholesale Voice over IP

POTS

VoIP/ToIP



Security challenges

- VoIP protocols
  - No, VoIP isn't just SIP
  - SIP is a driver for IMS services and cheap CPEs
  - H.323 and MGCP (still) rock the carrier world
- Security issues
  - VoIP dialects
  - Only a couple of OEM VoIP stacks (think x-vendor vulnerabilities)
  - FWs / SBCs: do they solve issues or introduce complexity ?
  - Are we creating backdoors into customer networks ?
  - CPS and QoS

Session Border Controller

- What the role of an SBC ?
  - Security
  - Hosted NAT traversal (correct signalling / IP header)
  - Signalling conversion
  - Media Conversion
  - Stateful RTP pin-holing based on signalling
- Can be located at different interfaces: Customer/Provider, inside customer LAN, Provider/Provider (VoIP peering)
- What can be done on a FW with ALGs ?

IMS services

- IMS = IP Multimedia Subsystem
- Remember when the mobile operators built their WAP and 3G networks ?
  - Mostly “open” (aka terminal is trusted)
  - Even connected with their “internal”/IT network
- IMS services with MVNOs, 3G/4G: overly complex architecture with tons of interfaces
- Large attack surface: registration/tracking servers, application servers, etc
- Firewalling: complex if not impossible

IMS Future Threats

- FMC: Attack Fixed<->Mobile handover (GSM<->WiFi)
- “Vishing” (VoIP Phishing): risks associated with IVR
- Abusing IN systems

MSP and IP DSLAM

- Multi-Service Platform aka Carrier Ethernet
- IP/Ethernet DSLAMs
- Remember all the “LAN only” layer 2 attacks ?
- dsniff is not dead ;-)
- VLANs, TCAM, etc.
- Basic IP features DSLAMs

Conclusion

- Last 5 years : infrastructure security
- Next 5 years : NGN security
- In a couple of years : learn the hard way that NGN needs stable and secure underlying infrastructure