DDOS Mitigation

Strategies for Large ISPs

Reykjavik, IS 2003 08 25

Sean Doran

smd@sprint.net

Large ISPs and DDOS

- A large ISP will have a different view of DDOS attacks than any other net entity
  - Floods are currently a process problem, not an engineering one
  - Floods quickly become non-scary with foreseeable engineering efforts
  - Scary DDOSes exist, and threaten the entire industry

Flood attacks

- Pure flood-based attacks are highly disruptive but are becoming extinct
  - Mitigation: minimize disruption to targets and topologically nearby non-targets alike
  - Flood-recovery techniques are improving
  - Preventing floods or making them undisruptive is computationally feasible

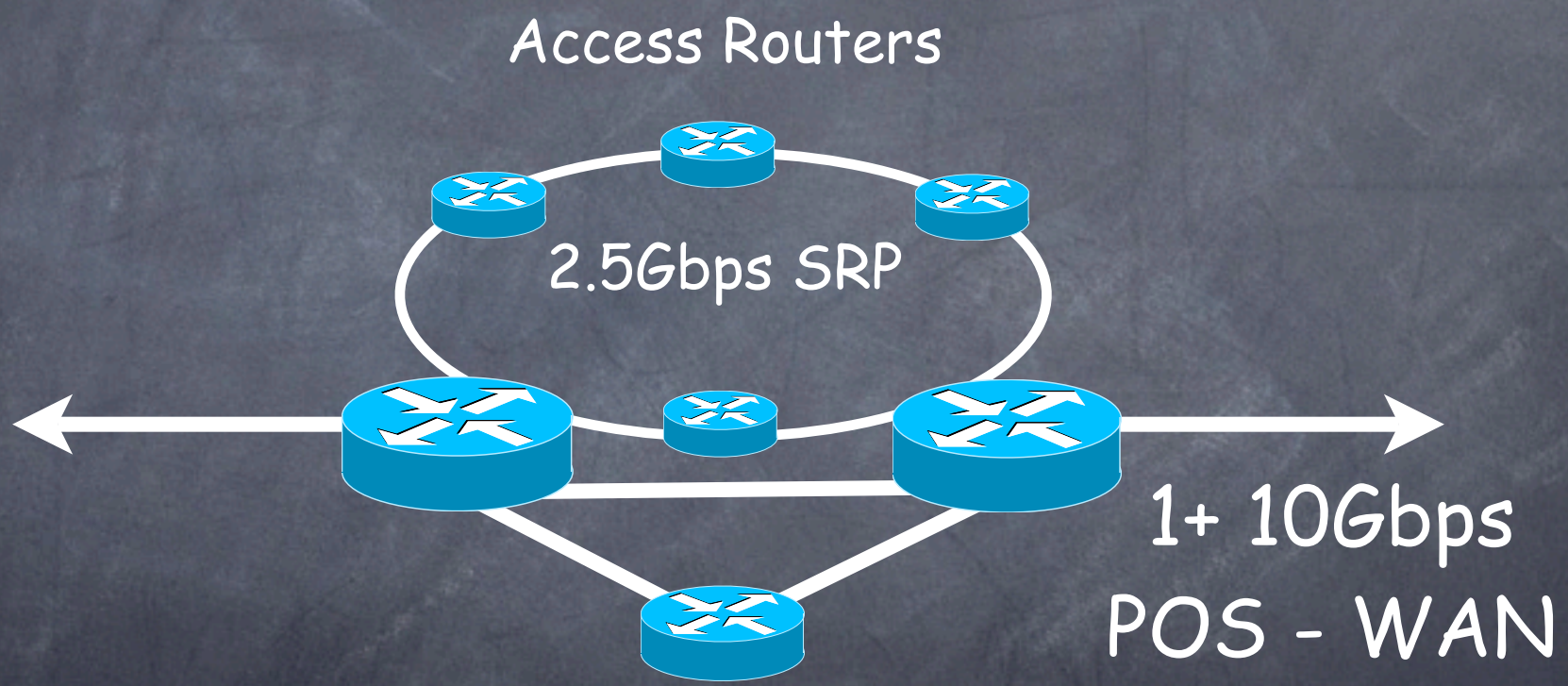
Worse than floods...

- Distributed computation -> smarter DDOS
  - Protocol-specific attacks which use massive parallel computations can out-scale any computational response
  - These can take place without triggering "out-of-profile" alarms near a diffuse number of non-concealed sources

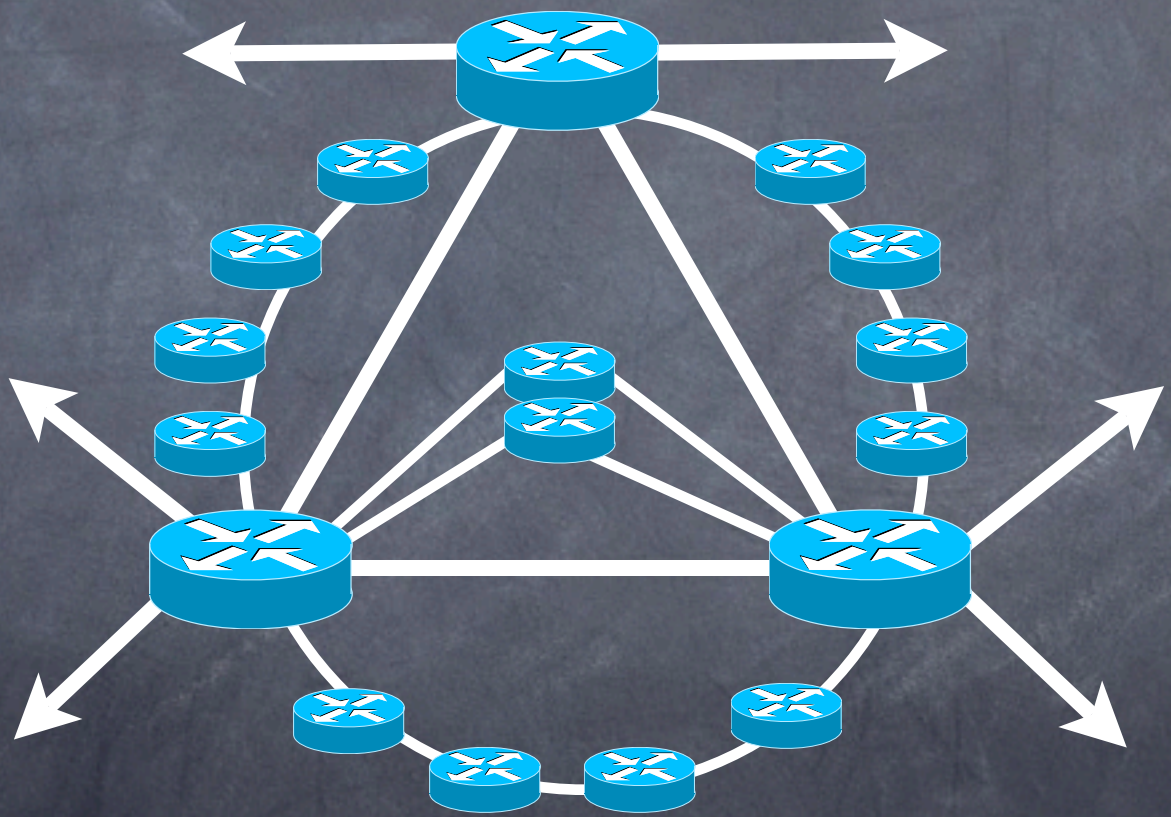
What's a large ISP?

- Consider a defintion of large as: a network which can "just deliver" feasible traffic floods towards a customer for sustained periods, with minimal effect on other customers
- People often laugh at me here, so a quick overview of Sprintlink follows...

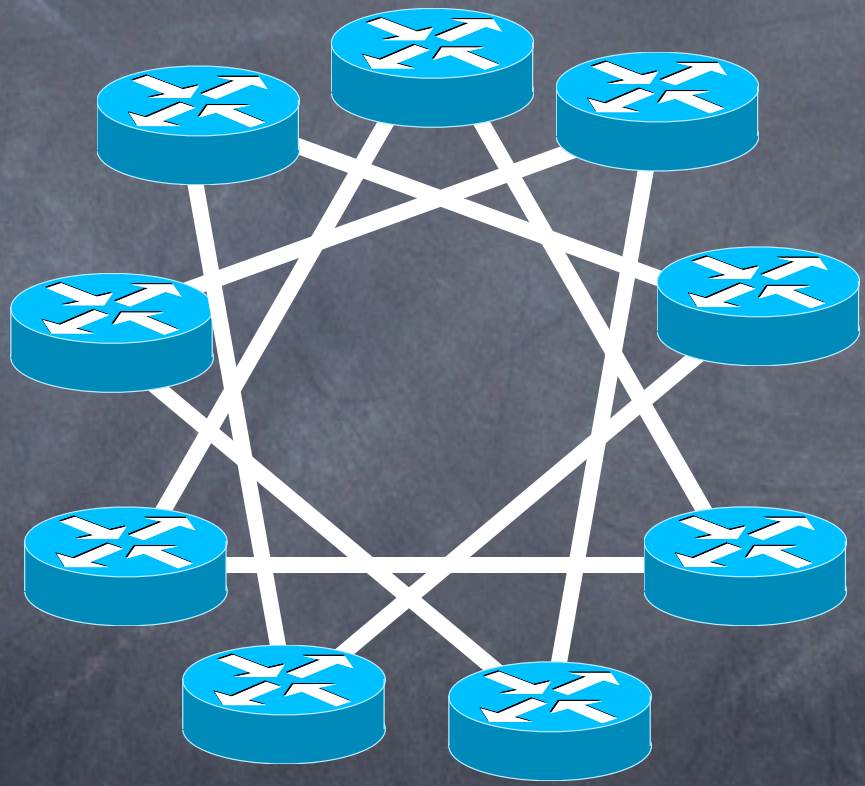
Small Sprintlink POP



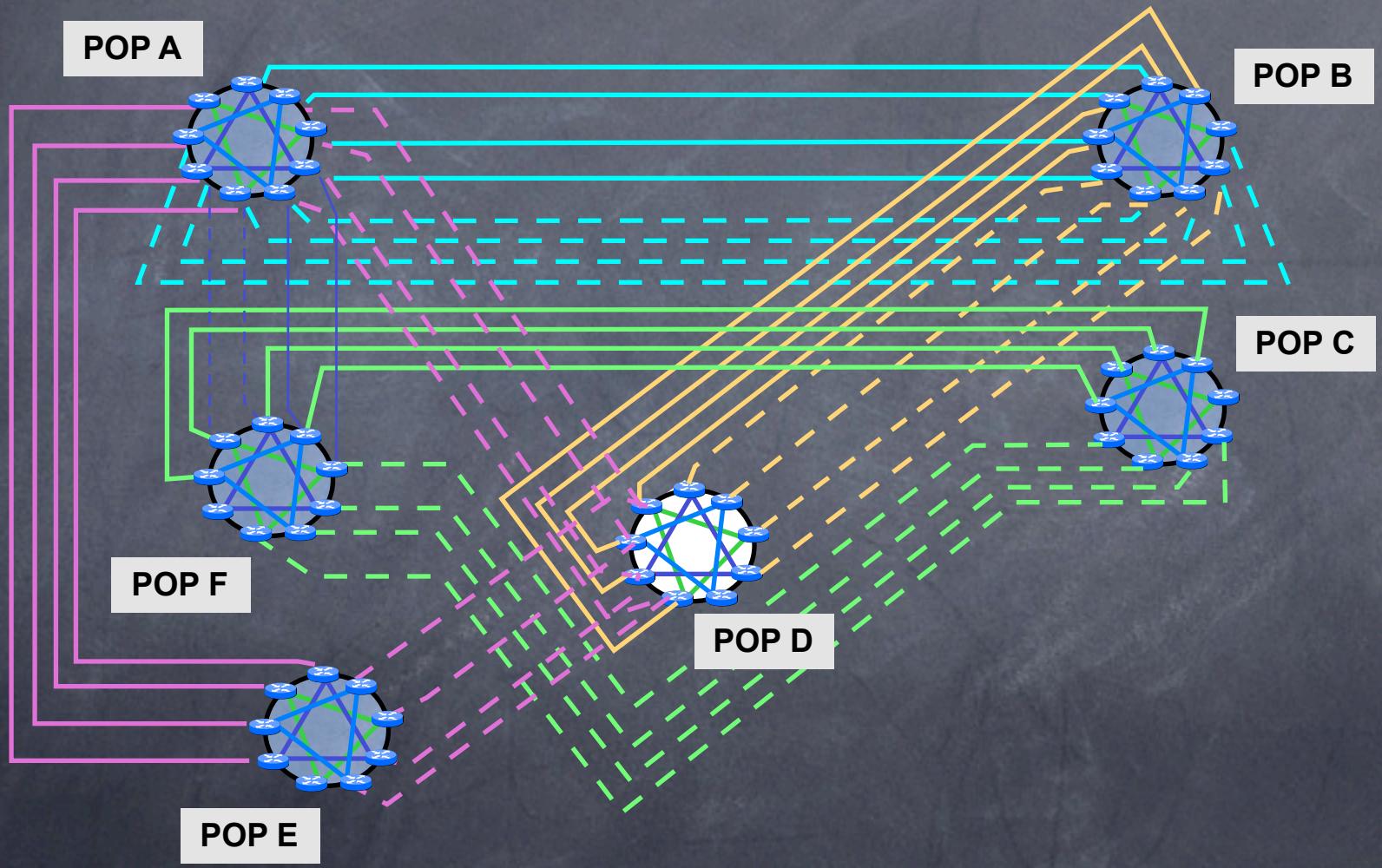
One-layer, Sprintlink Rosette

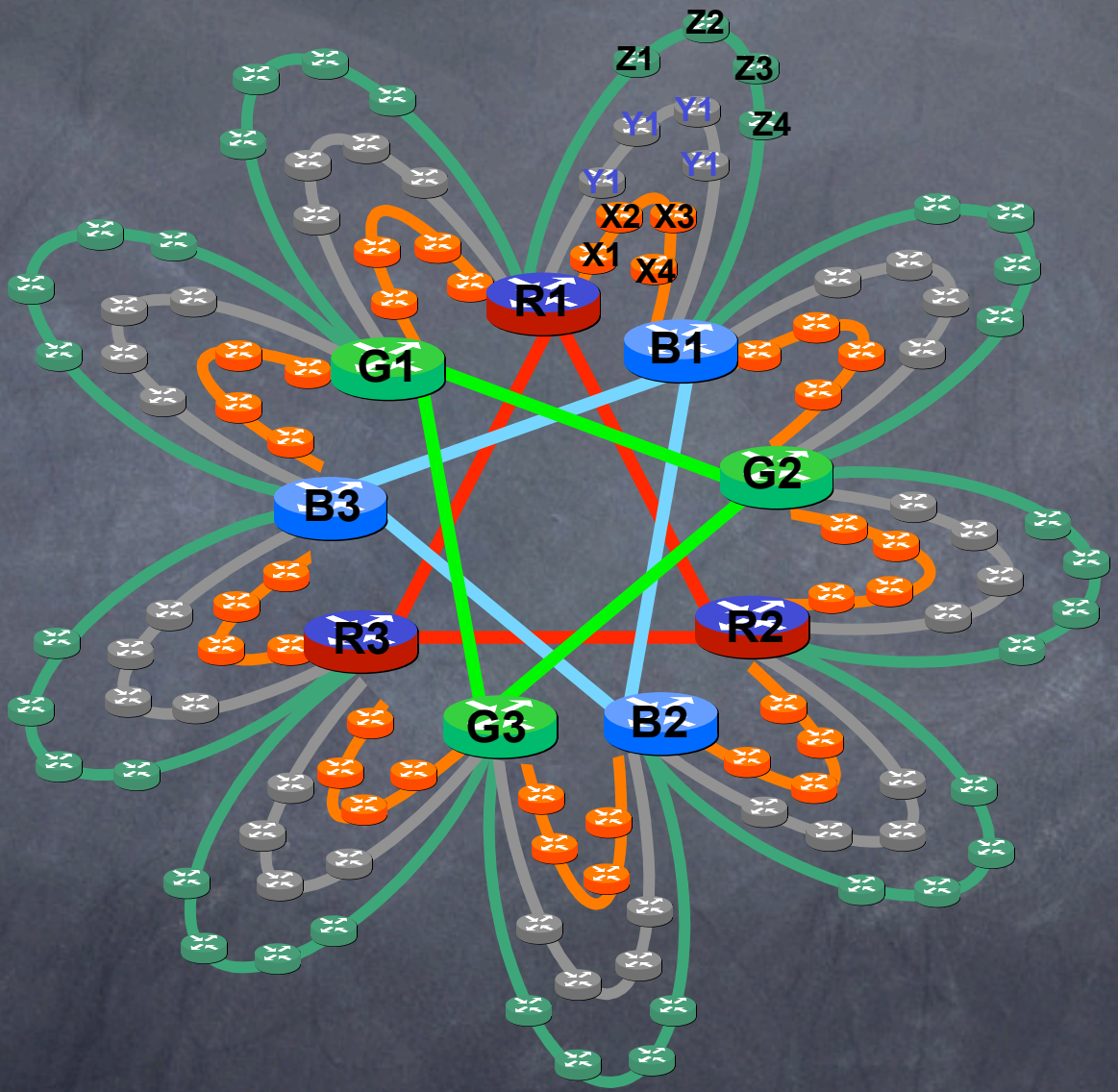


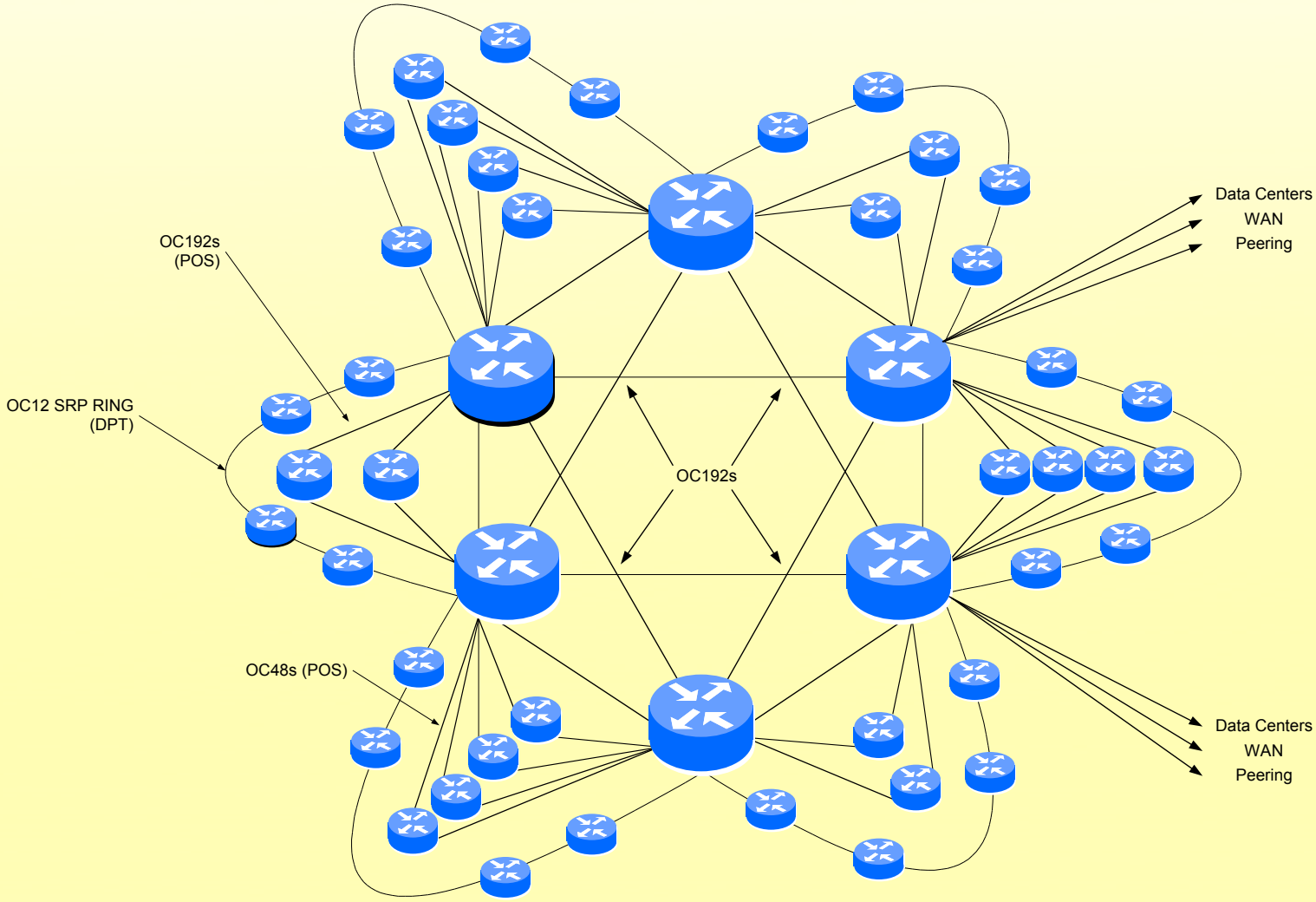
Three-layer Rosette Core



Inter-city connectivity driven by rosette + fibre paths




Z2
Z1
Z3
Y1
Y1
Z4
Y1
Y1
X2
X3
X1
X4
R1
B1
G1
G2
B3
R3
R2
G3
B2


OC192s
(POS)
OC12 SRP RING
(DPT)
OC48s (POS)
OC192s
Data Centers
WAN
Peering
Data Centers
WAN
Peering

2003 POP Max. Scale

- 9 Core Routers, 108 Access
- Trunk capacity 45 x 10Gbps
- 2.5:1 overbooking between small access router rings (mostly lightly-aggregating customers like corporate end users) and core routers
- Customer capacity eqiv. of 3456 STM-1

Traffic floods

- We observe brute-force flooding rates of several hundred Mbps today.
- The bottlenecks attacked are (in order of decreasing probability):
  - Small customer connection to Sprintlink
  - Something downstream of large customer
  - SRP ring segment / netwk infrastructure

What does this mean to us?

- When they are not the target itself, most customers are unaffected by even enormous flood attacks
- Mitigation is an edge problem:
  - Increasingly fine-grained filters can be applied on a customer access router
  - "Sealing all borders" likely unnecessary

A reactive SLA

- In principle we could frame an SLA with time intervals between events:
  - T0: ticket opened by report or detection
  - T1: initial "coarse-grained" filter
  - T2...Tn-4: report on filter activity, traffic composition, and any steps taken to "narrow" the filter

- Tn-3: observation that the attack has ceased
- Tn-2: notification to customer
- Tn-1: removal of filter
- Tn: normal service

Some cleverer attacks

- Protocol-specific attacking is growing, thanks to the increasing prevalence of Own3d h0st3z
- A million scattrered hosts generating what looks to an observer near them like ordinary, legitimate traffic, but which clogs things up at or near the victim, is very scary

Mitigation technology:
Distributed Recovery of Service systems

- Riverhead and other companies have been evolving "washing-machine" devices which effectively narrow filters as algorithms declare specific traffic flows "good"
- This is a useful evolutionary direction, because attacks are getting to be smarter than brute-force flooding

Problems with DROSs

- However, all of these devices need to touch real traffic destined for the victim, so using them poses problems:
  - moving traffic through them can be awkward
  - they usually only handle a few hundred Mbps at most... and may not be able to distribute nearly as well as attacks

A market?

- These platforms are also not without cost
- Some risk too: they may be out-evolved by attackers
- In short: limited proactivity

Conclusions

- Attacks keep coming, and are evolving
- Defenses evolve too; mostly procedural, but some analytical tools are getting greater use
- Brute force floods are amenable to in-router proactive prevention but
- Owned hosts are the next obvious worry, and there is no obvious defence

Thanks for listening!

Sean Doran
smd@sprint.net