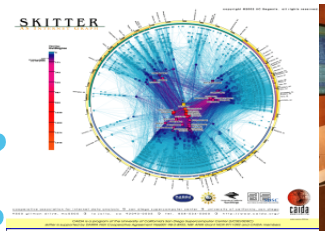
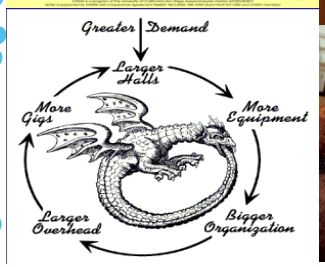
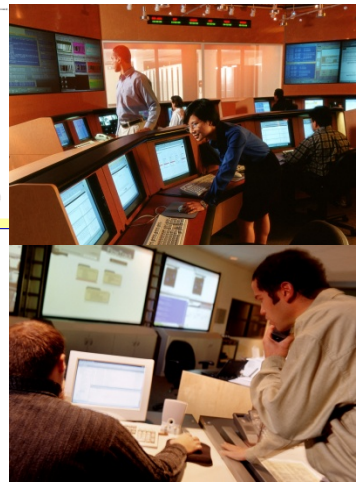
How to Respond to a DDOS Attack (Service Provider Edition)







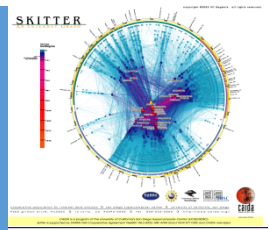
Outline

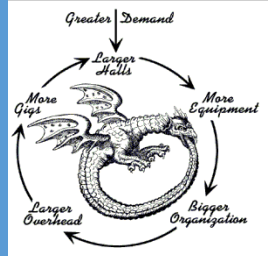
- Background Principles to Fighting a DoS Attack
- Putting the Tools to Work – DDOS Attack

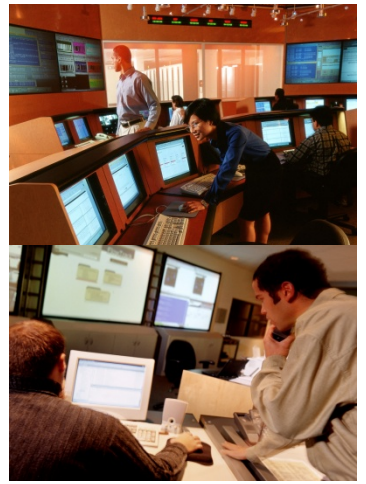
Long History – Online Training

- NANOG 23 – ISP Security – Real World Techniques II – by Barry Raveendran Greene, Cisco Systems; Chris Morrow, UUNET/Verizon; Brian W. Gemberling, UUNET
- NANOG 25 – BGP Security Update – by Barry Raveendran Greene, Cisco Systems
- NANOG 26 – ISP Security – Real World Techniques – by Barry Raveendran Greene, Cisco Systems; Kevin Houle, CERT
- NANOG 28 – ISP Security: Deploying and Using Sinkholes by Barry Raveendren Greene, Cisco Systems; Danny McPherson, Arbor Networks
- NANOG 36 – ISP Security 101 Primer by Barry Greene, Cisco Systems and Roland Dobbins, Cisco Systems
- NANOG 47 – NSP-SEC Top Ten Security Techniques by Barry Greene, Juniper Networks
- NANOG 54 – Service Provider “Security” Tool Kit by Barry Greene, ISC (Part 1) & (Part 2)
- **MAAWG 26 – SP Security Workshop**
- CommunicAsia 2015 Workshop

Background Principles to Fighting a DoS Attack

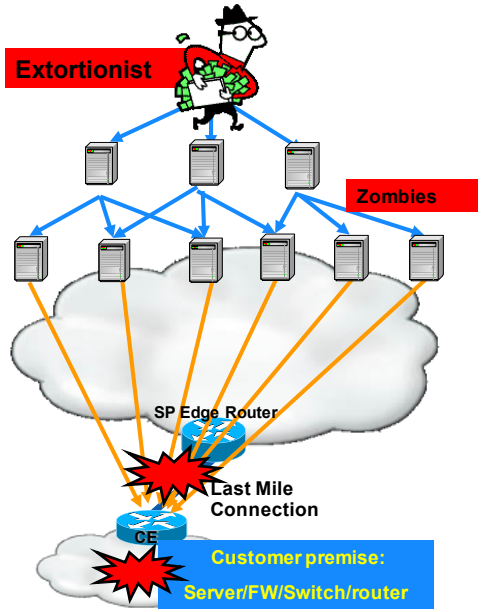






How do you really stop a DDOS Attack?

- Clean Pipes, Scrubbing Centers, and other “Anti-DDOS” tools *does not stop DDOS Attacks*.
- These tools are critical, but their should only be used to provide:
  - ✓ Full Service Restoration for selected mission critical services
  - ✓ Time to Remediate the DDOS Attack



- Stopping a DDOS Attack requires an ability to do:

1. Withstand the attack and not given in to the extortion/threat
2. Visibility/Traceback to the Sources of the Attack
3. Remediating the Tools used in the Attack (BOTNETs and Reflectors)
4. Backtracing to the C&C used to drive the attack.
5. Triangulating on the person(s) launching the attack.

Essential Principle for DoS Resilience

Building a Secure Infrastructure for Profitable Services

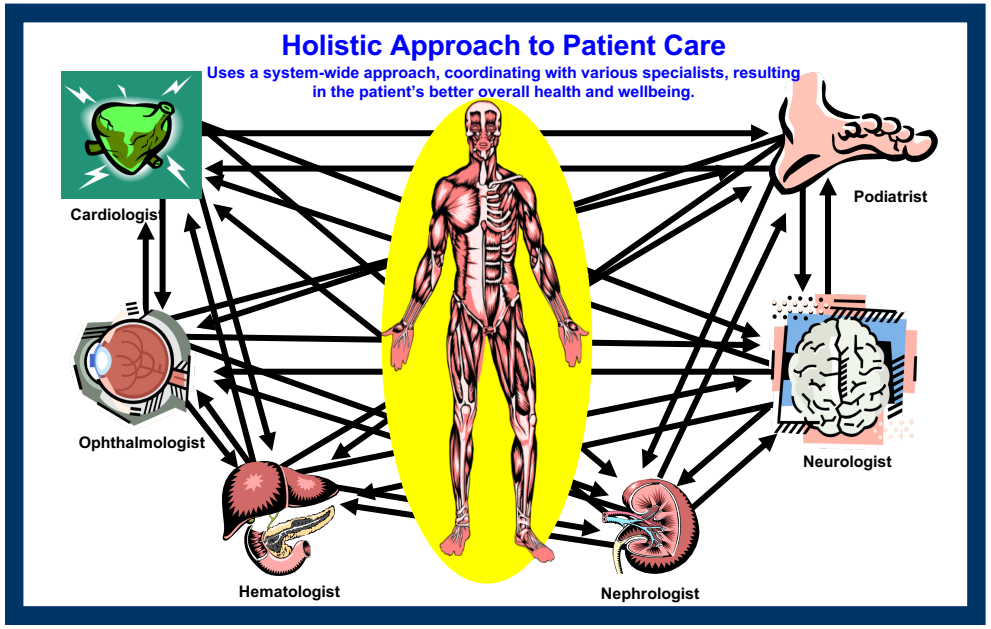
Complete Control over all traffic in the network.

Total Visibility in all aspects of the network.

Maximized Availability of all services.

What does Visibility Mean?

- Visibility is a business fundamental of the telecommunications industry.
- You need to know everything you customers are doing, what applications are driving your network, and understand the direction you business is being driven.
- MOST TELECOMMUNICATIONS COMPANIES TODAY DO NOT DO THIS WITH TCP/IP!

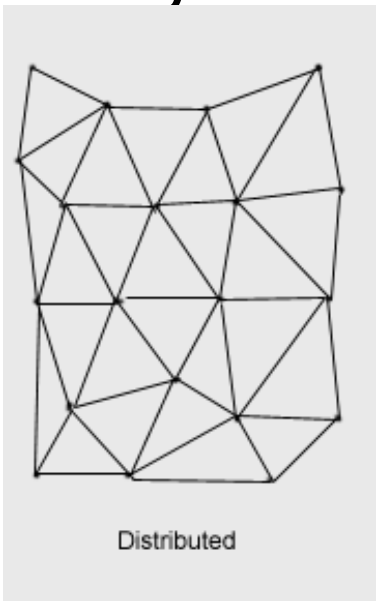


What does Control Mean?

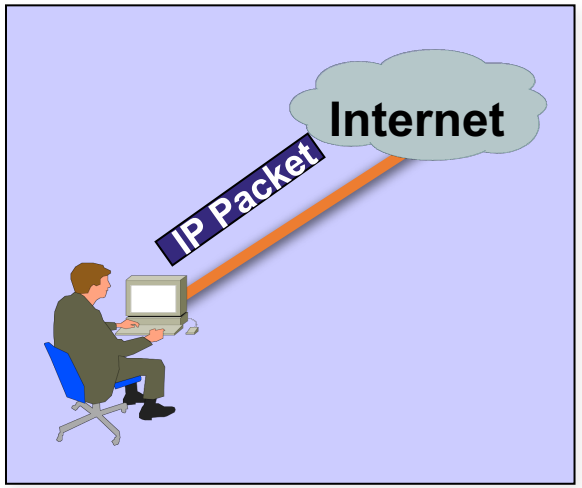
1. **You need to know Exactly what is going on with your customers and your network.**
2. **You need to be able to shape, manipulated, and serve your customers based on that knowledge.**
3. **You need to have your network stay up beyond *five 9s***

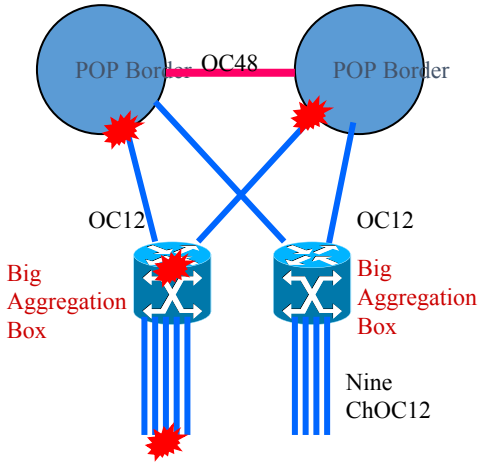
What does Availability Mean?

- The network must be up for 99.999%
- We do this with the Paul Baran Model of Availability and Resiliency.
- Problem: The majority of IP Engineers do not know the principles the Paul Baran Model of Availability and Resiliency.



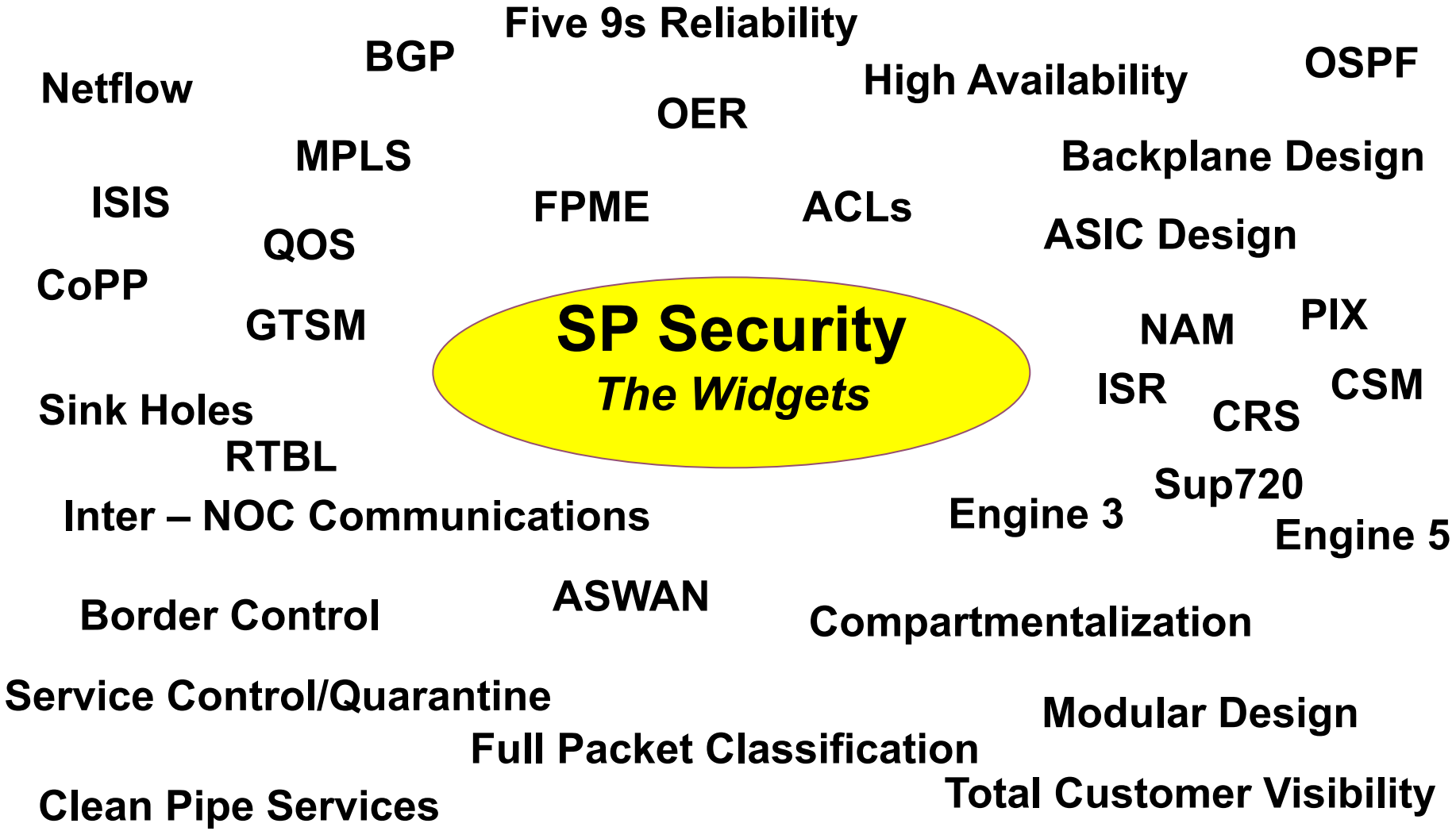
It is all about the packet ……..



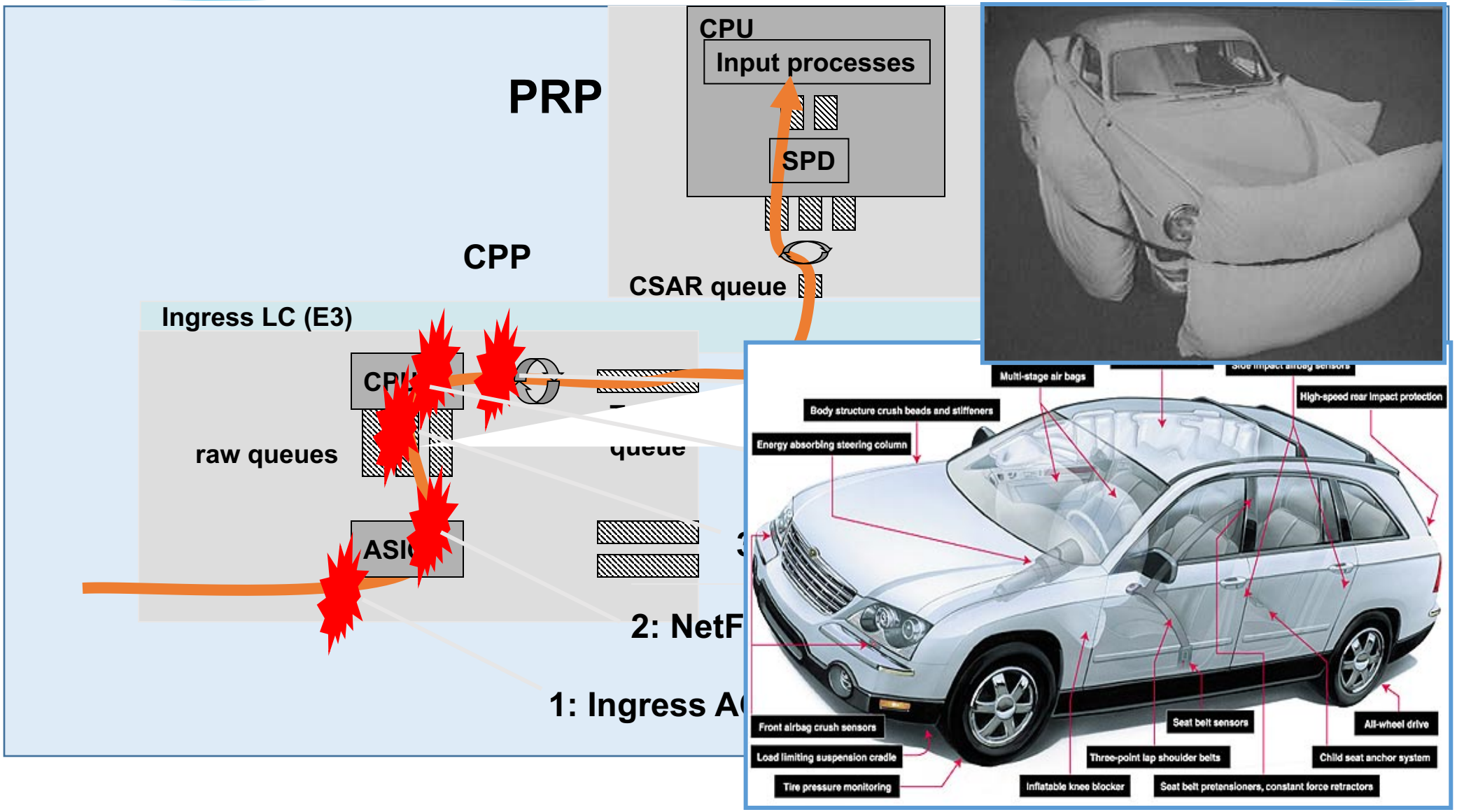


- **It is all about the packet …..**
- **Once a packet gets into the Internet, someone, somewhere has to do one of two things:**
  - ***Deliver the Packet***
  - ***Drop the Packet***
- **In the context of DoS attacks, the questions are *who* and *where* will the "drop the packet" action occur?**

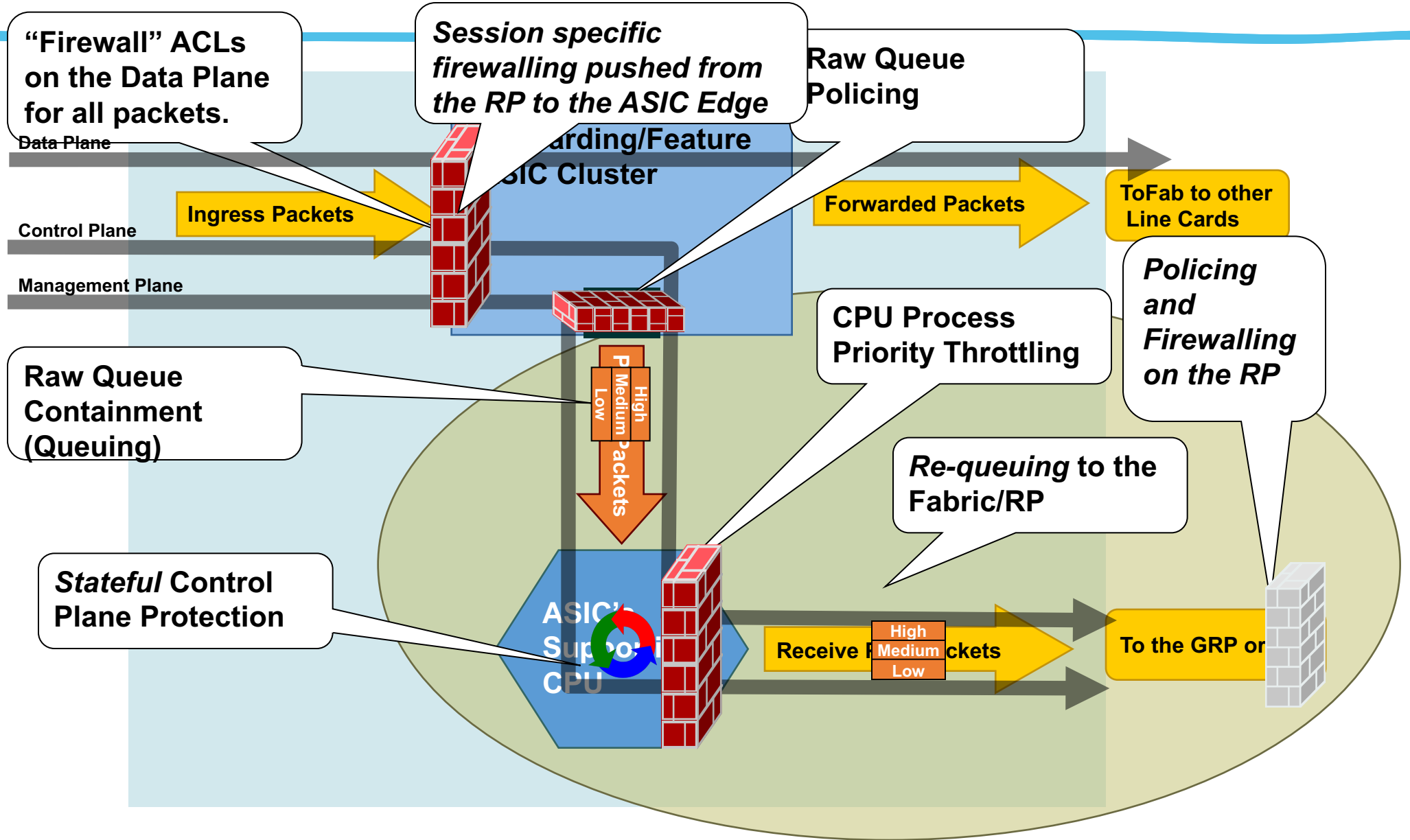
The Operator Security *Toolkit – Use Everything*



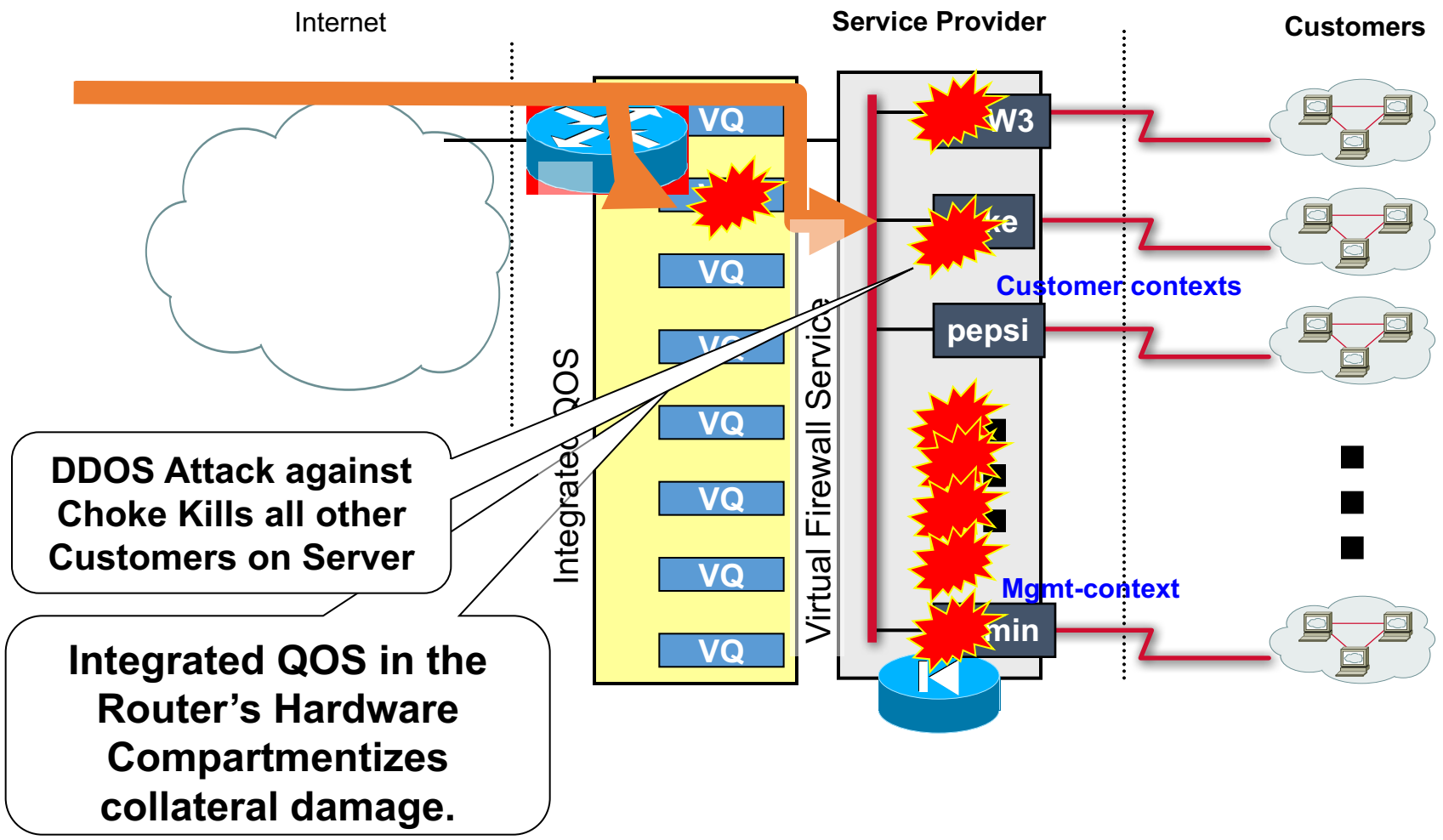
Security Cannot be an Afterthought!



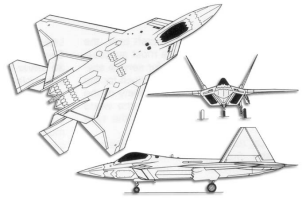
What can you do to protect inside a Router?



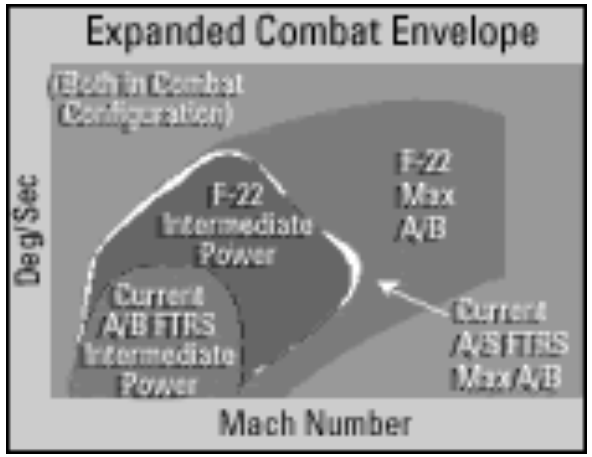
Throwing Hardware at the Problem?

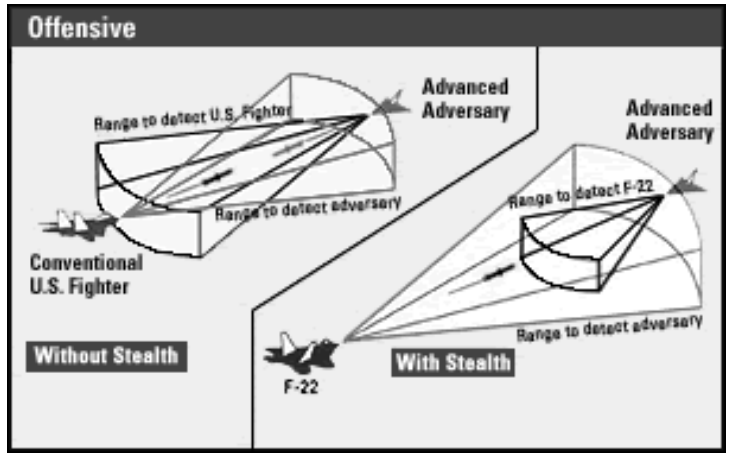


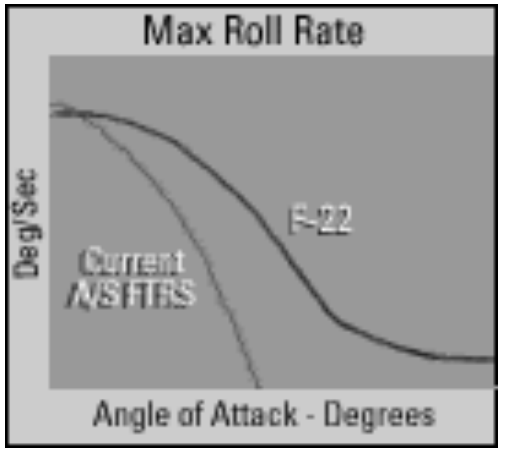
Are You Pushing the Envelop?



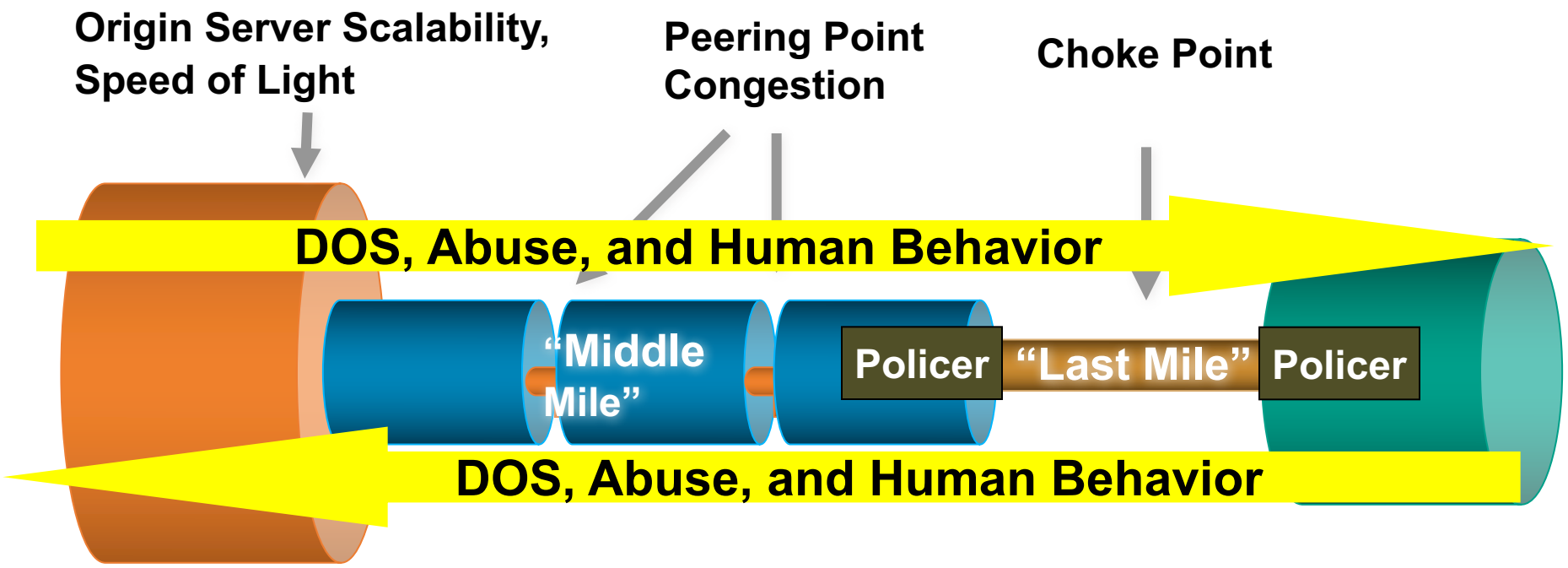
- Know your equipment and infrastructure:
  - Know the Performance Envelop of all your equipment (routers, switches, workstation, etc). You need to know what your equipment is really capable of doing. If you cannot do it your self, make is a purchasing requirement.
  - Know the capabilities of your network. If possible, test it. Surprises are not kind during a security incident.







Choke Points = Collateral Damage



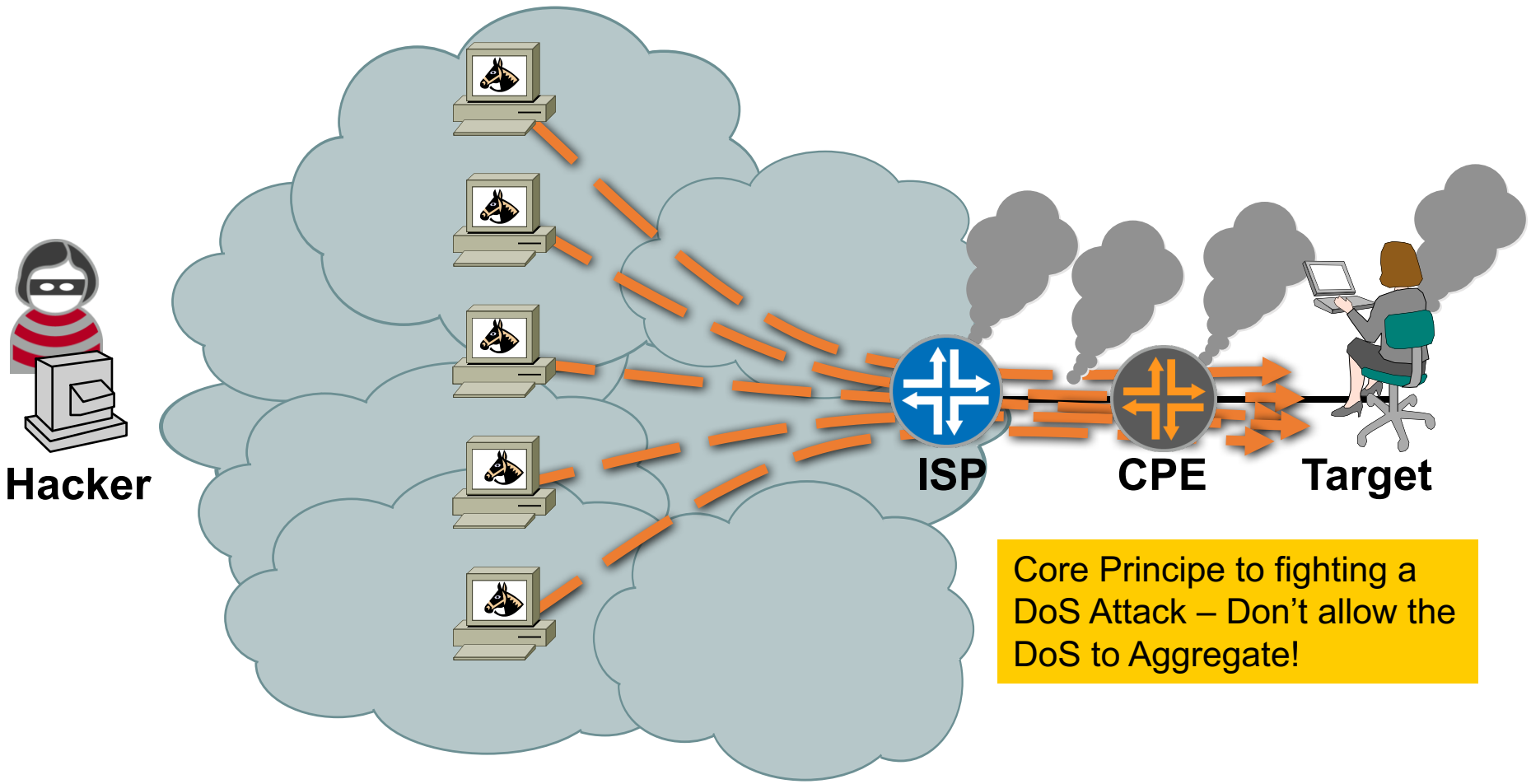
Internet Backbone

Cross-Internet connections

Local Loop

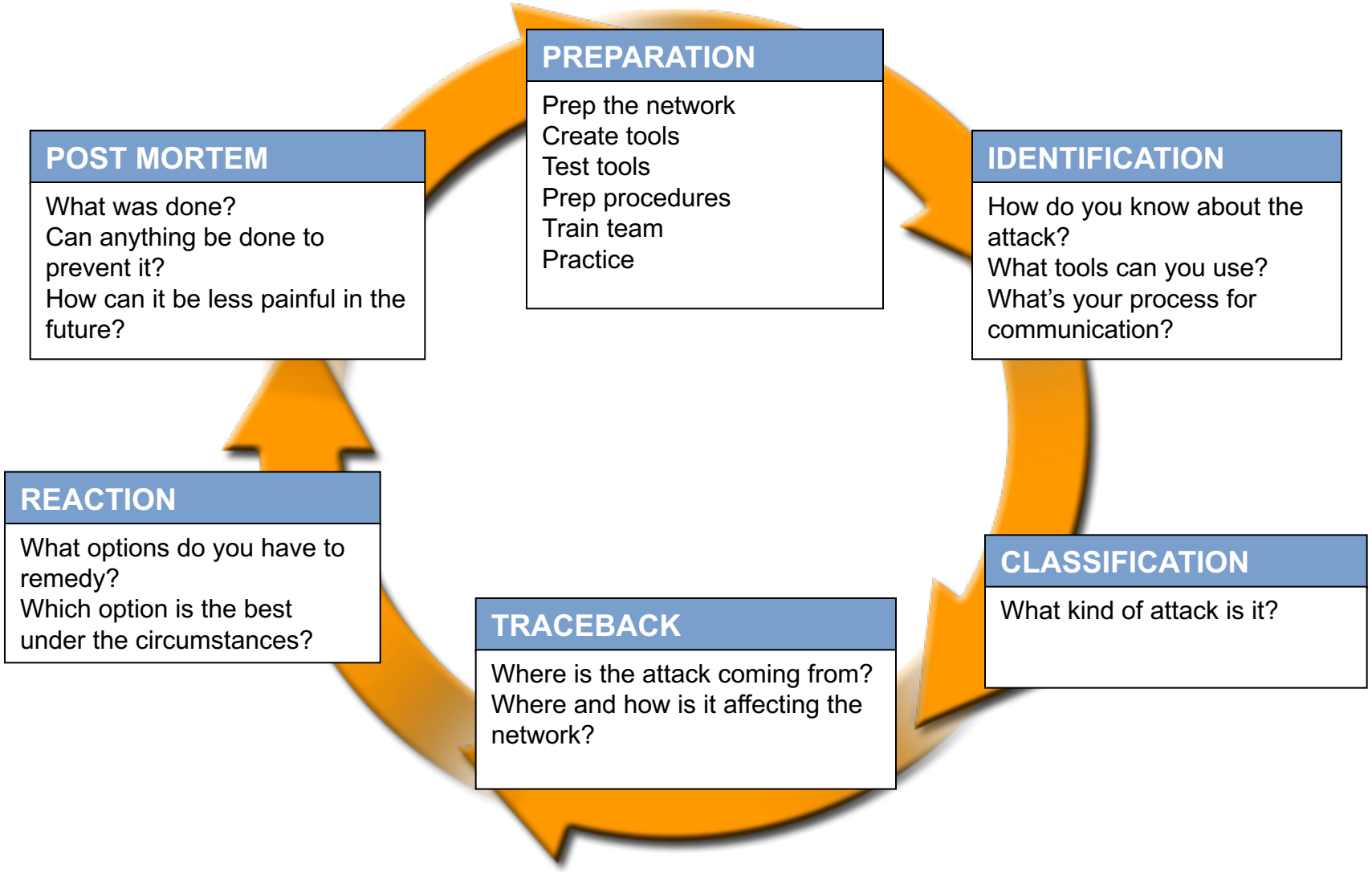
Premises Network

DoS Aggregation Point

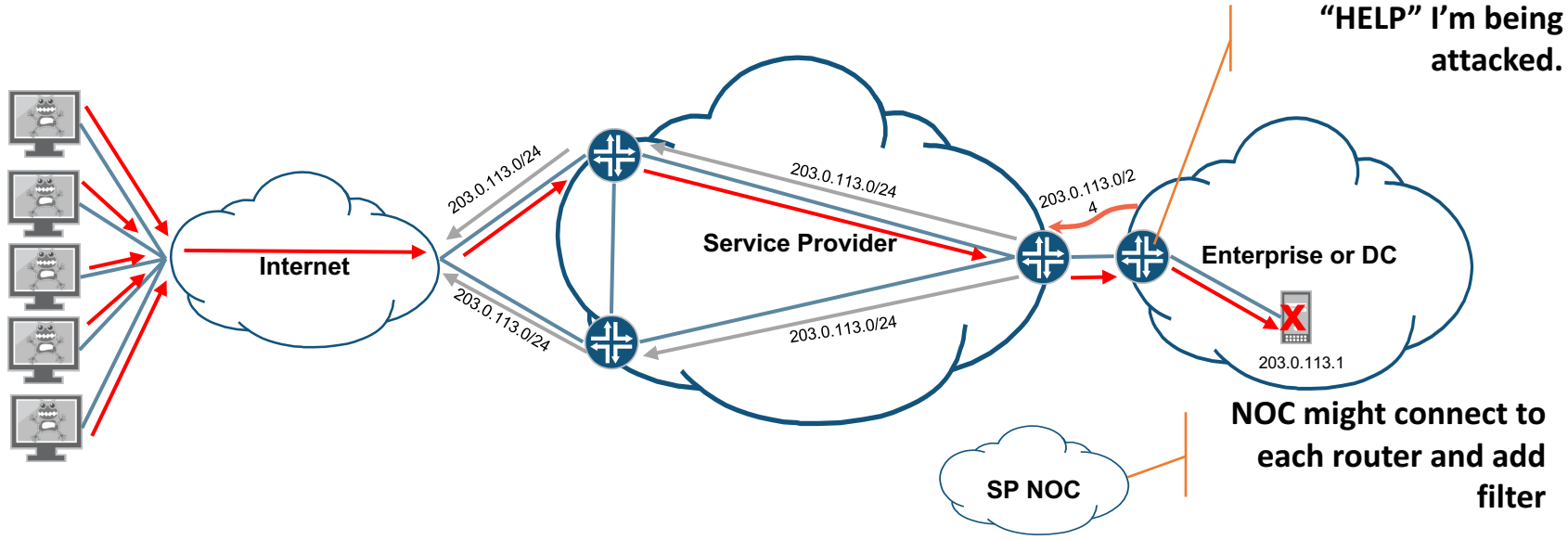


Core Principe to fighting a DoS Attack – Don't allow the DoS to Aggregate!

Six Phases of Incident Response

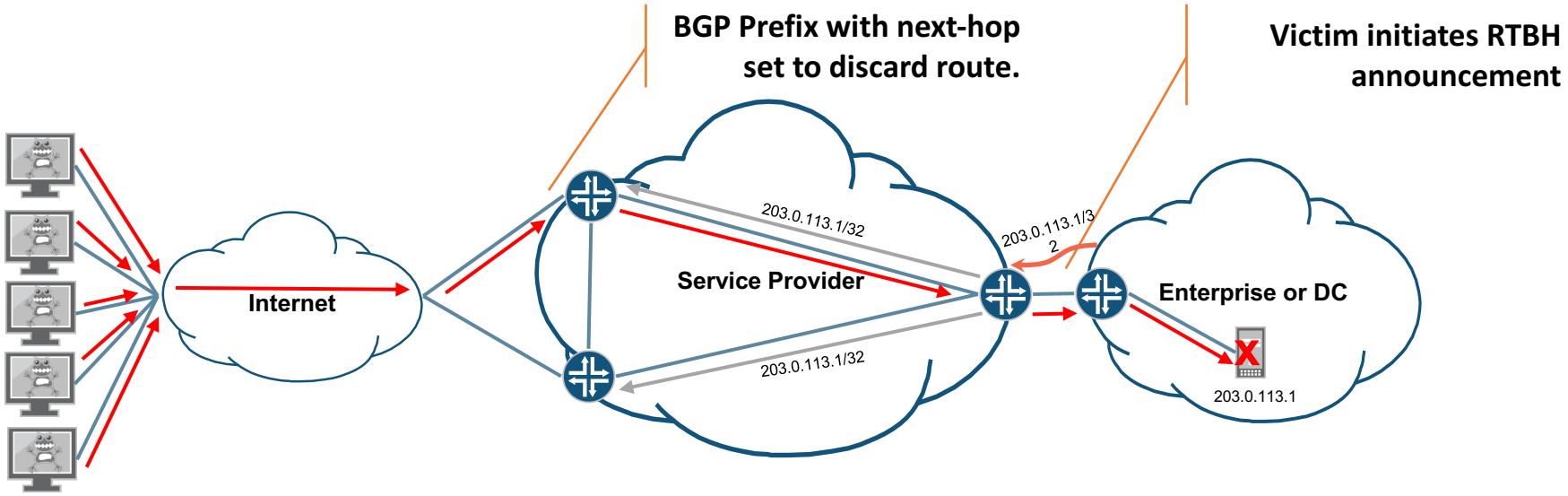


Blocking DDoS in the “Old” Days



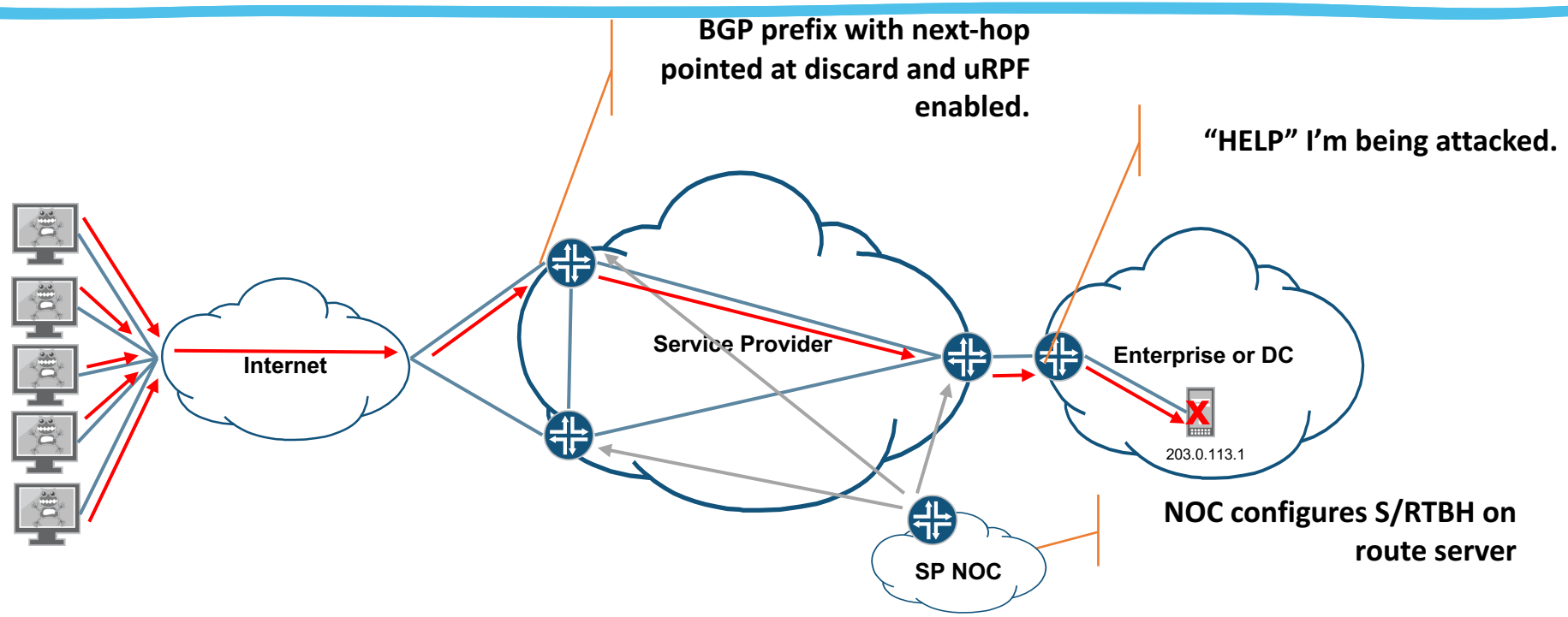
- Ease of implementation and uses well understood constructs
- Requires high degree of co-ordination between customer and provider
- Cumbersome to scale in a large network perimeter
- Mis-configuration possible and expensive

Destination Remotely Triggered Black Hole (D/RTBH)



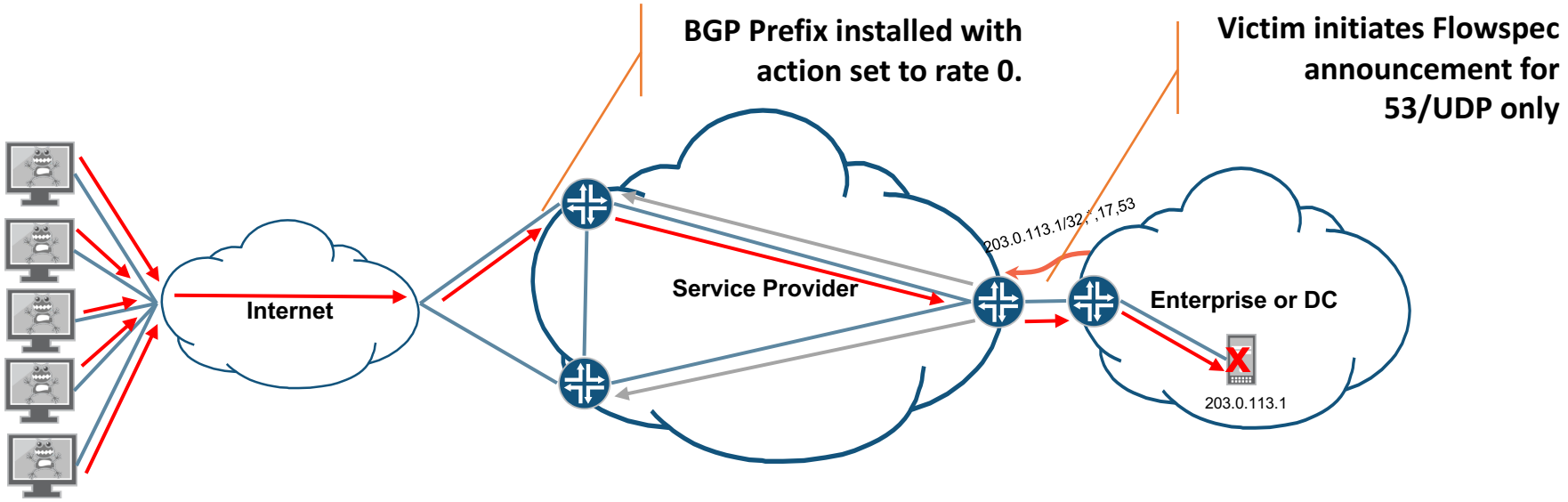
- RFC 3882 circa 2000
- Requires pre-configuration of discard route on all edge routers
- Victim's destination address is completely unreachable but attack (and collateral damage) is stopped.

Source Remotely Triggered Black Hole (S/RTBH)



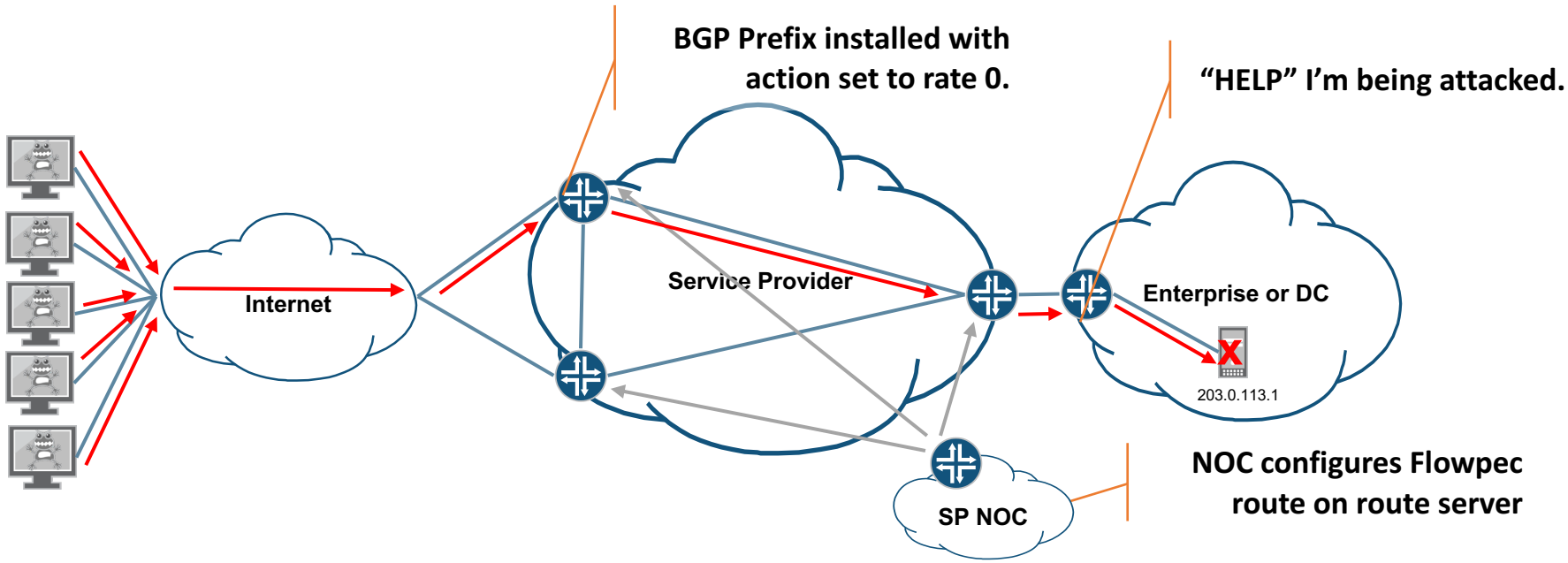
- RFC 5635 circa 2005
- Requires pre-configuration of discard route and uRPF on all edge routers
- Victim's destination address is still useable
- Only works for single (or small number) source.

Inter-domain DDoS Mitigation Using Flowspec



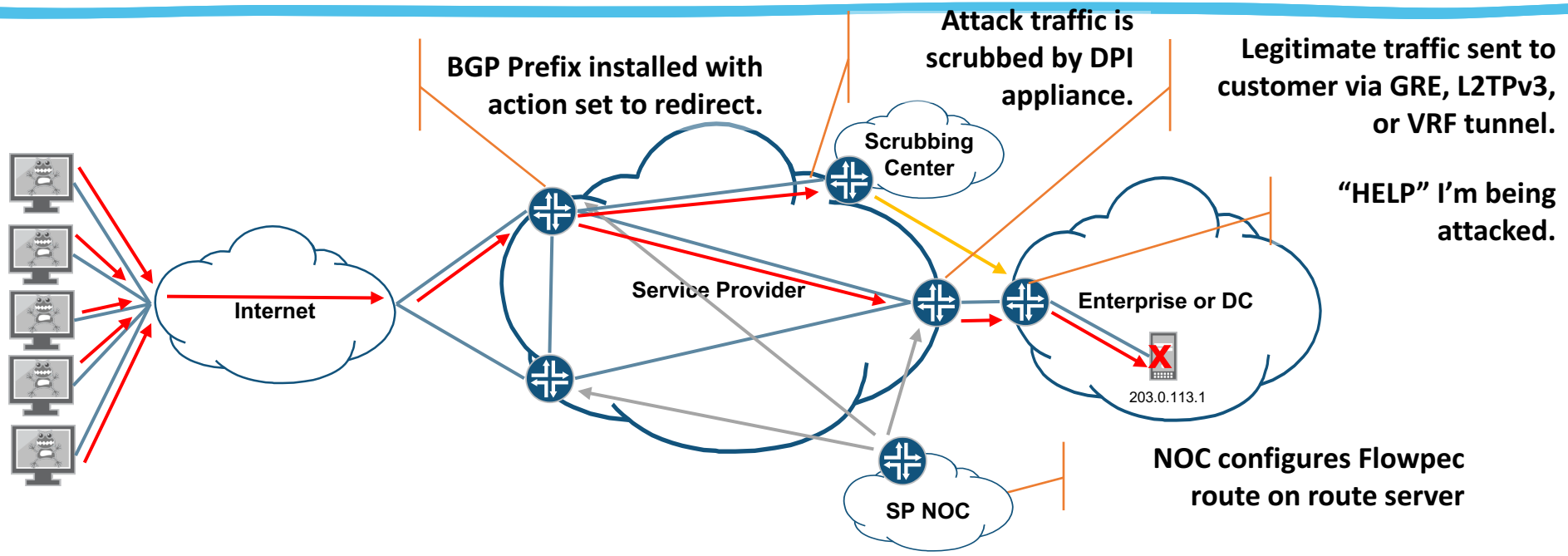
- Allows ISP customer to initiate the filter.
- Requires sane filtering at customer edge.

Intra-domain DDoS Mitigation Using Flowspec



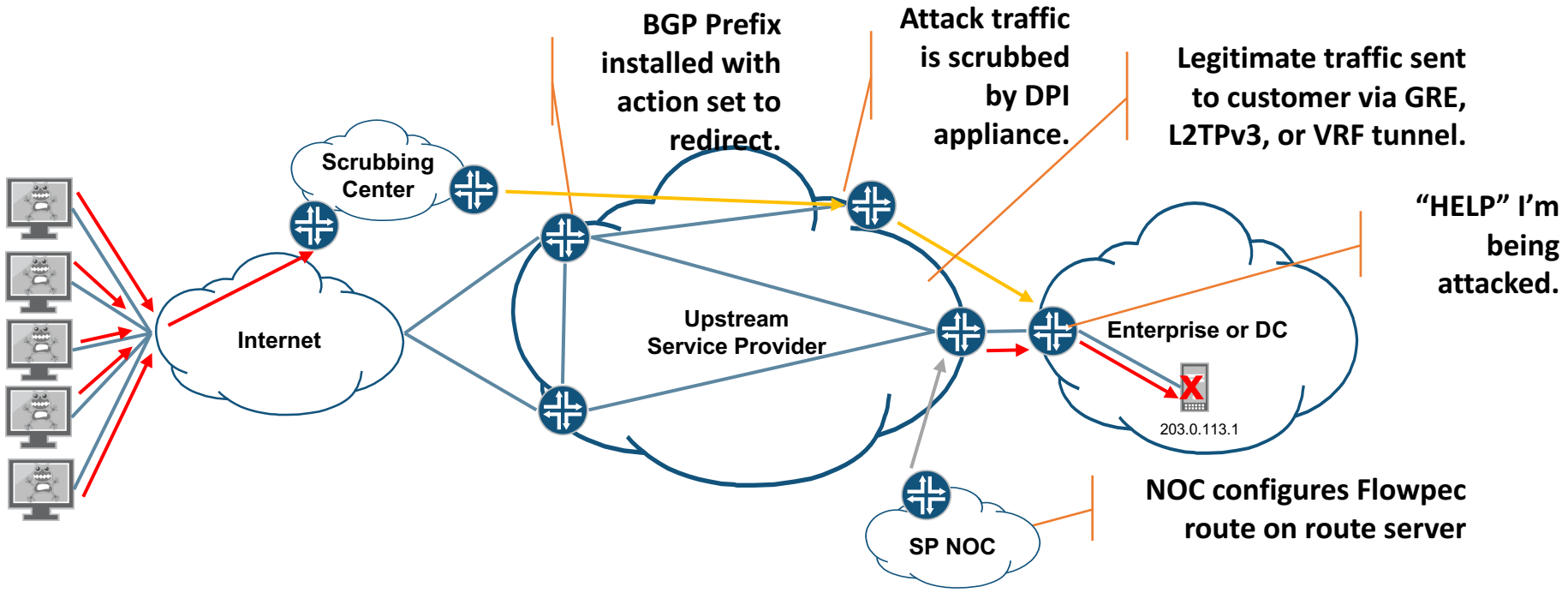
- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Requires co-ordination between customer and provider.

DDoS Mitigation Using Scrubbing Center



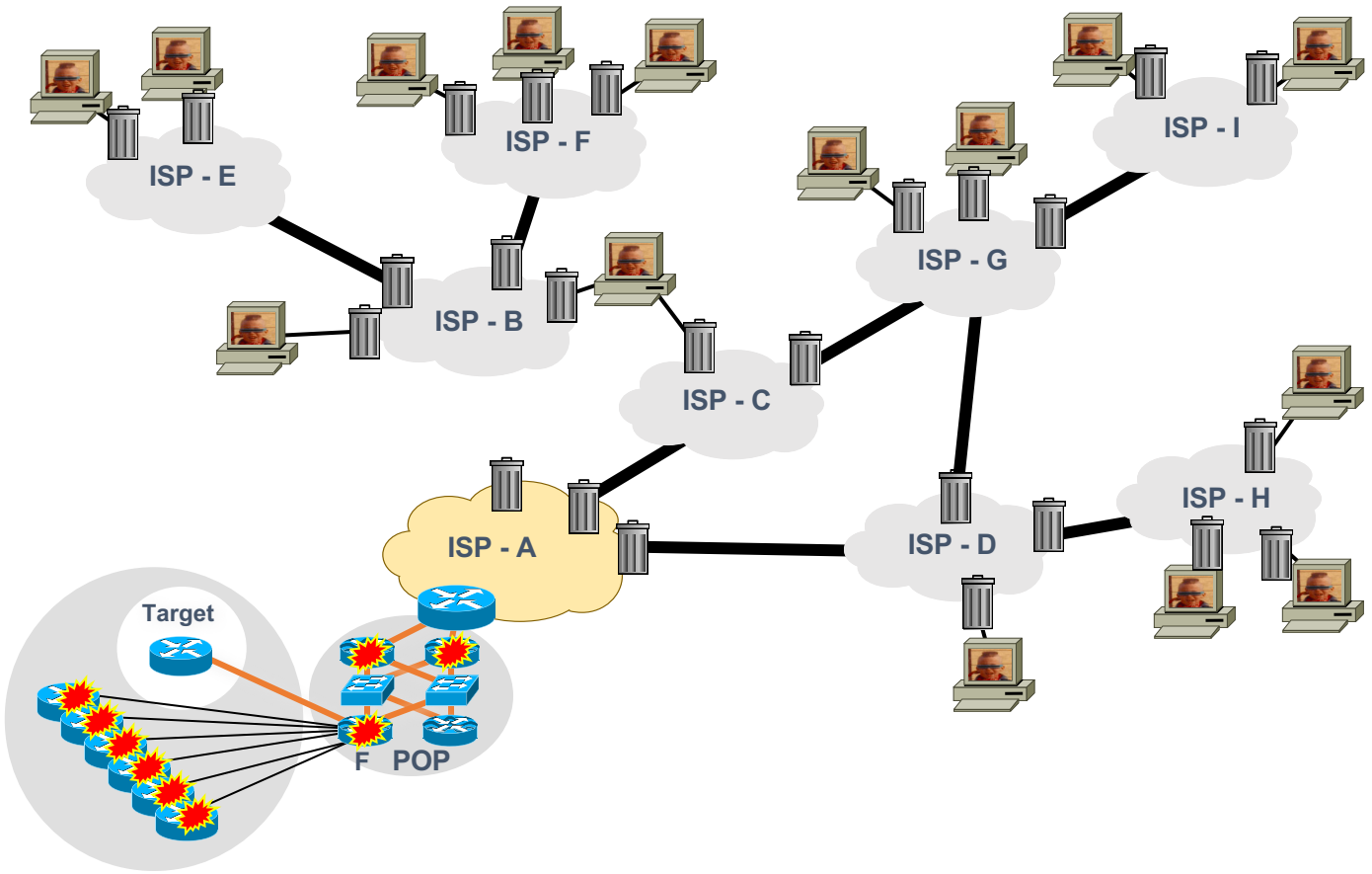
- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Allows for mitigating application layer attacks without completing the attack.

DDoS Mitigation Using Scrubbing Center

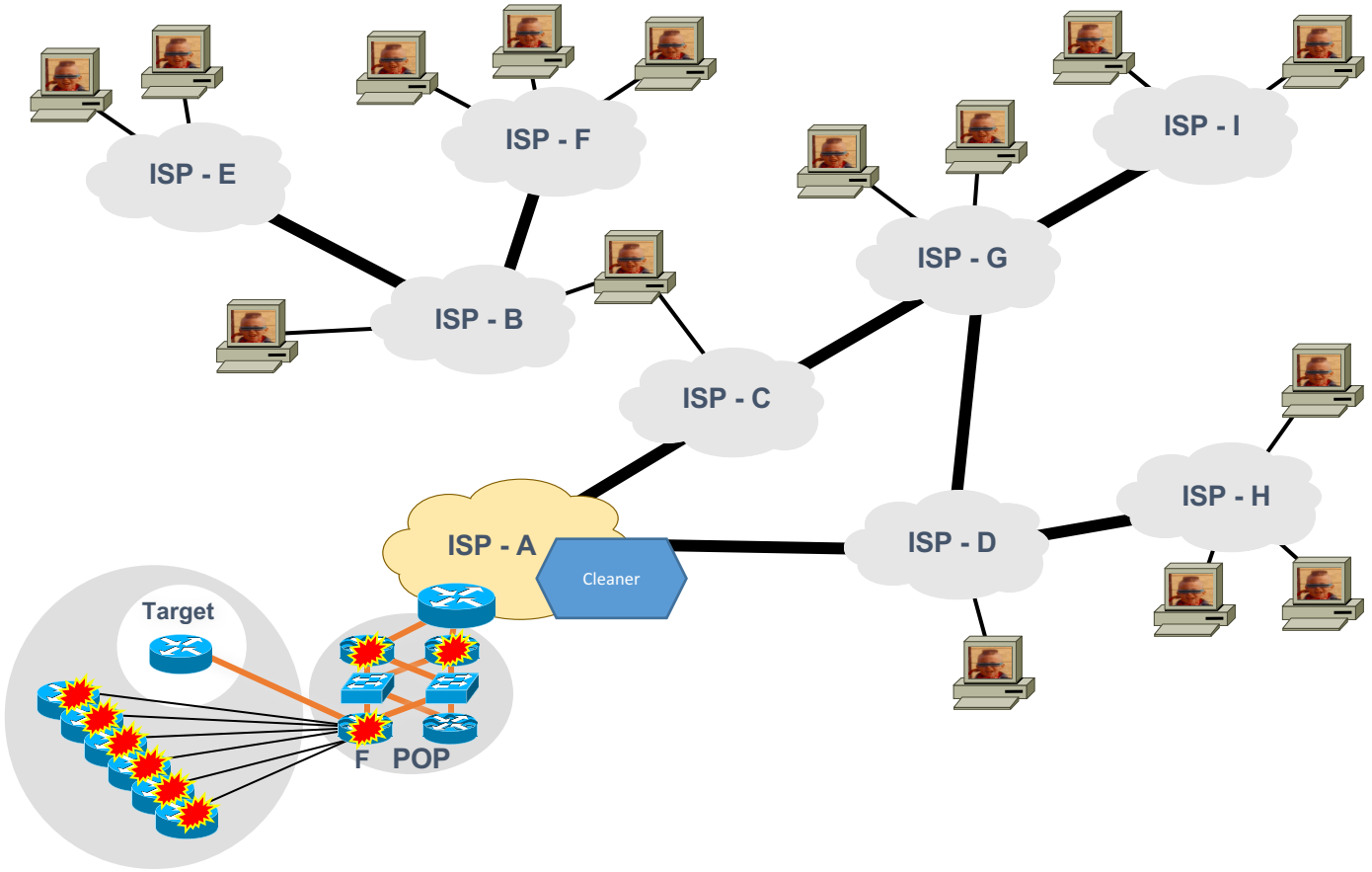


- Could be initiated by phone call, detection in SP network, or a web portal for the customer.
- Allows for mitigating application layer attacks without completing the attack.

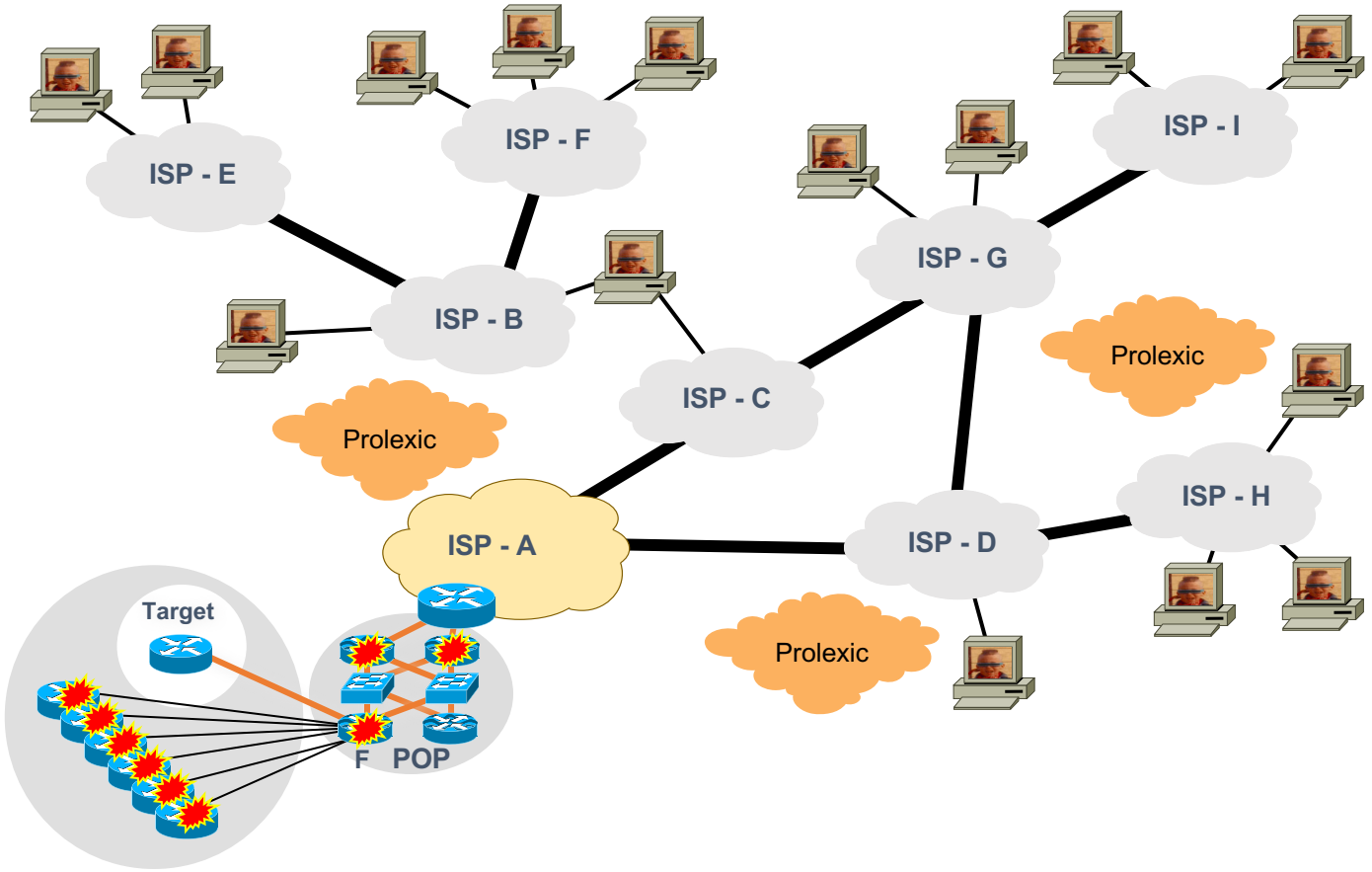
DDOS Today – We can push back with RTBH



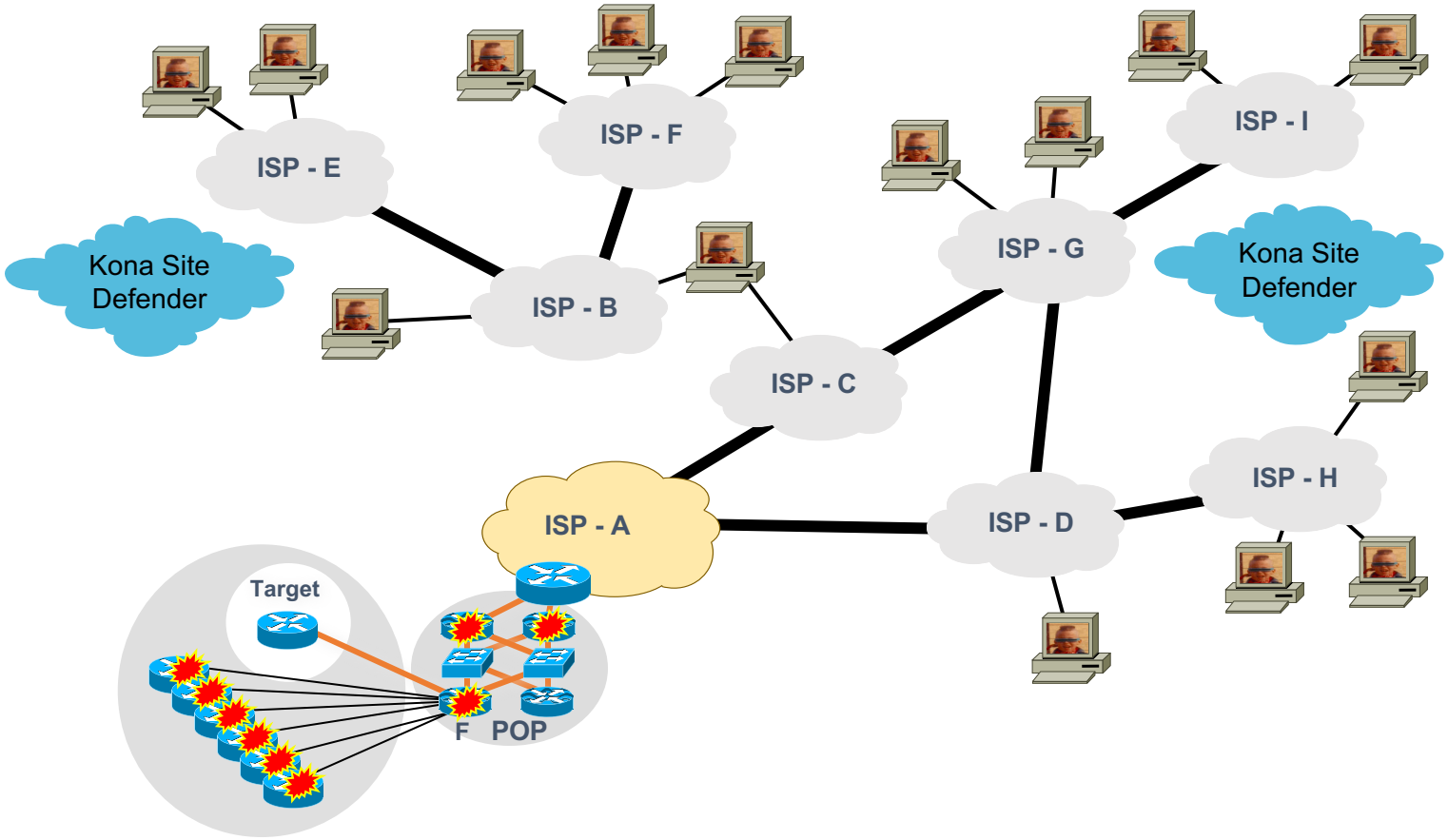
DDOS Today – Ride out the Attack – On Premise Scrubbing



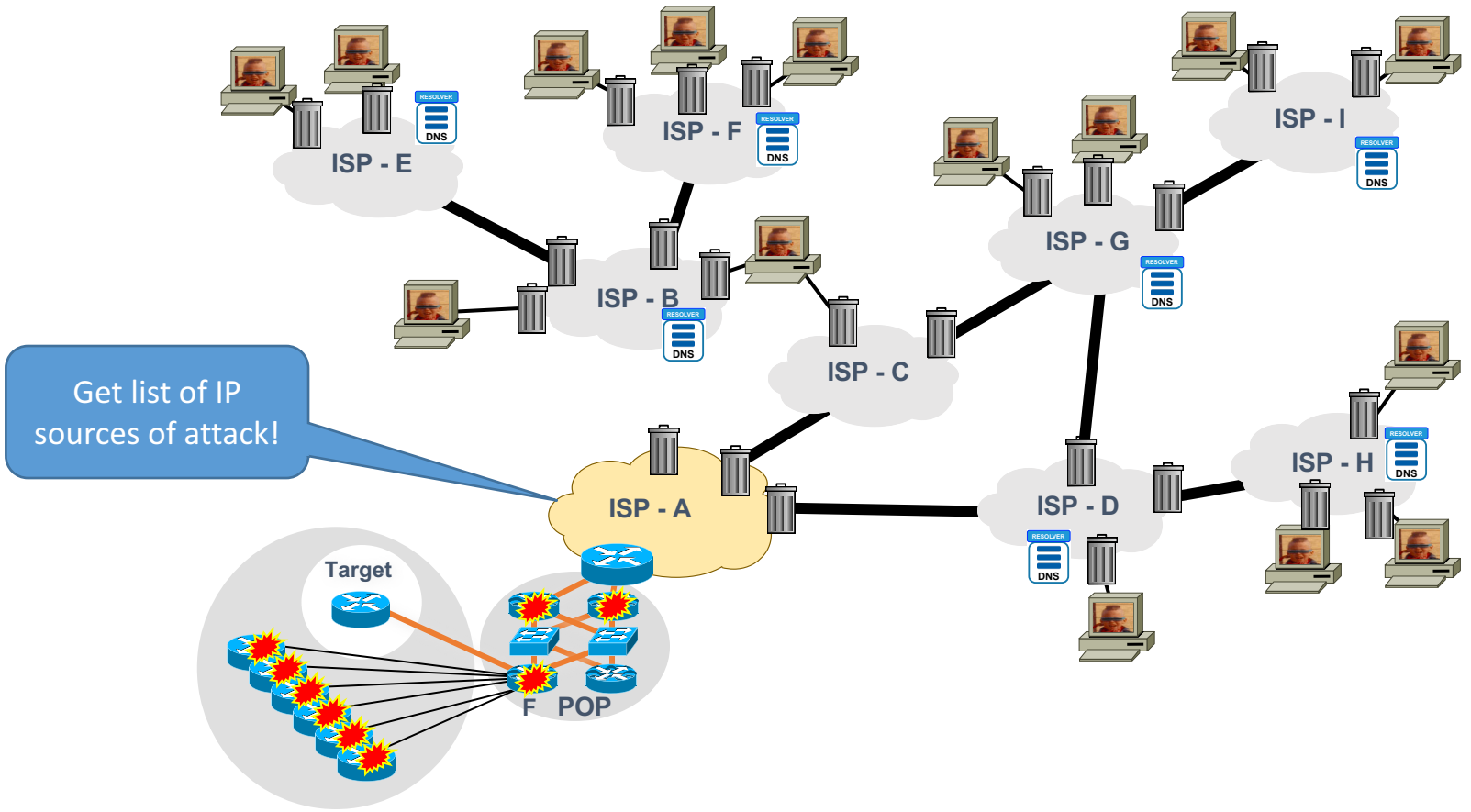
DDOS Today – Ride out the Attack – Off Premise



DDOS Today – Build more Resilient Services

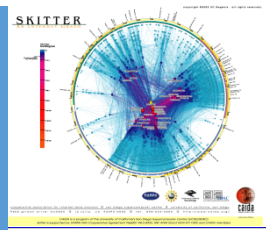


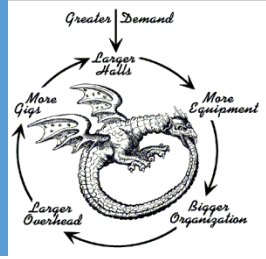
Now we can remediate as part of a Federation

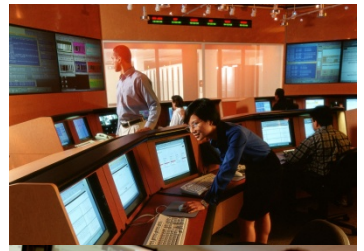


Pause for Questions

Putting the Tools to Work – DDOS Attack



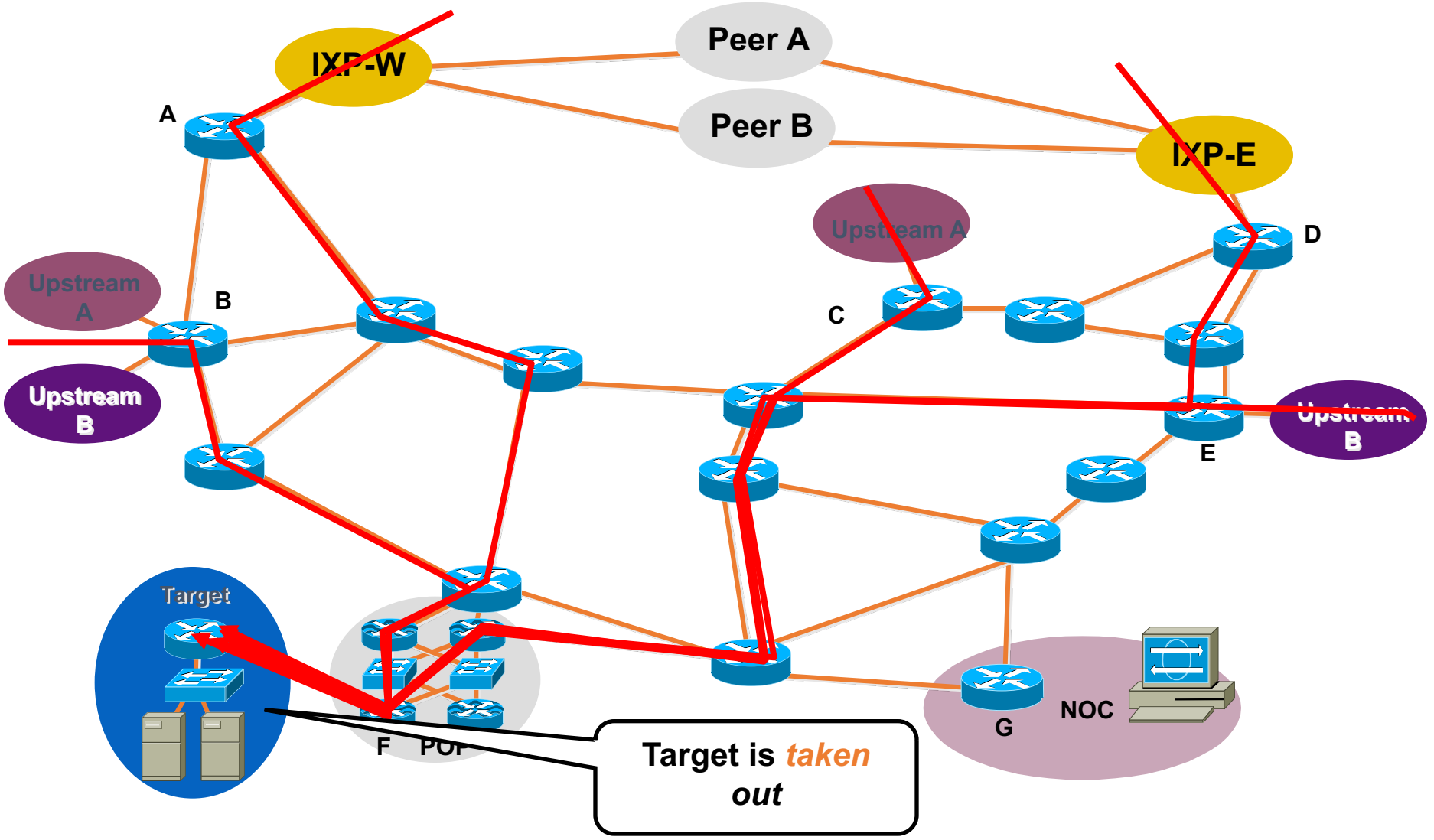




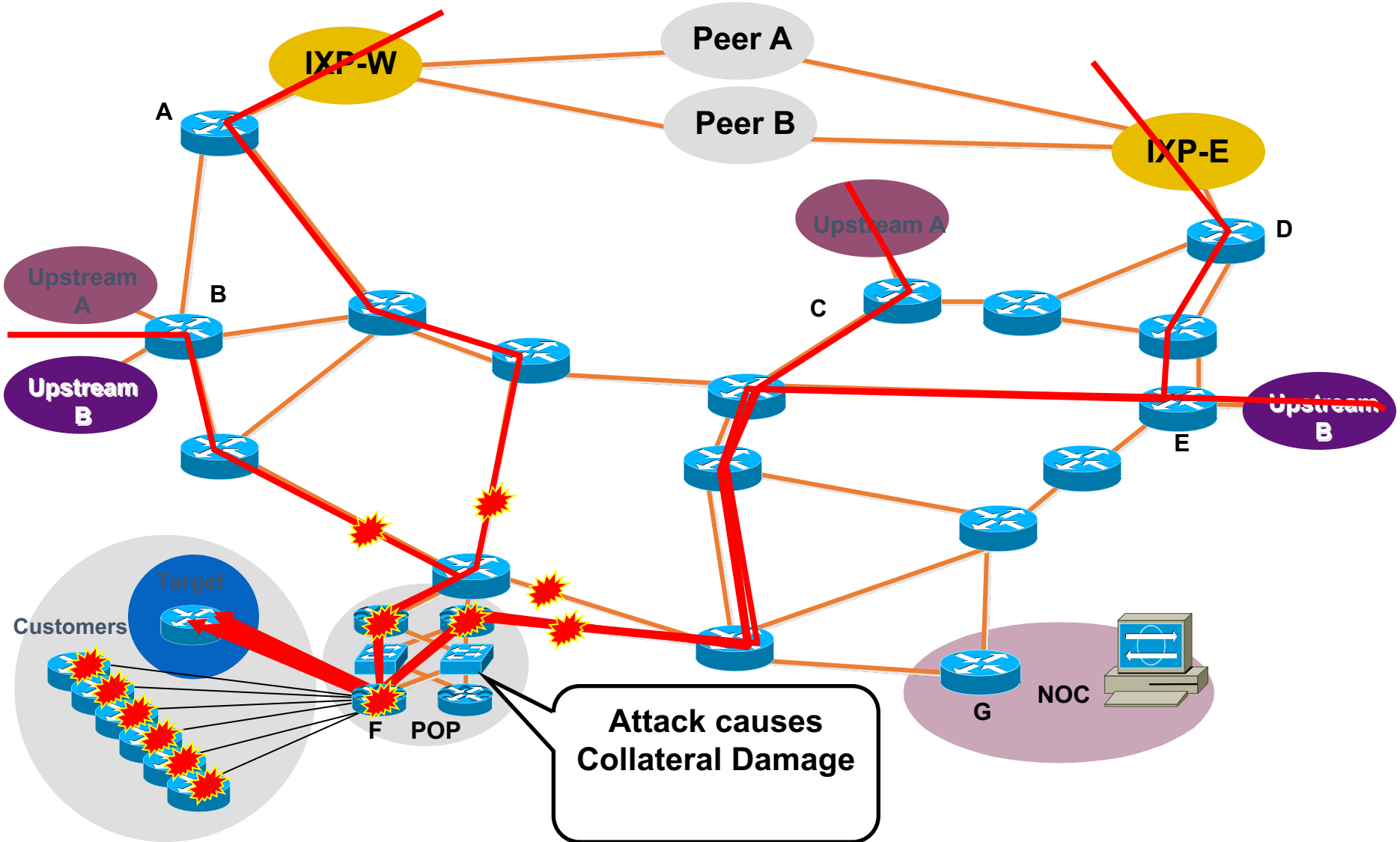
SITREP

- Everything is normal in the Network.
- Then alarms go off – something is happening in the network.

Customer Is DOSed—Before



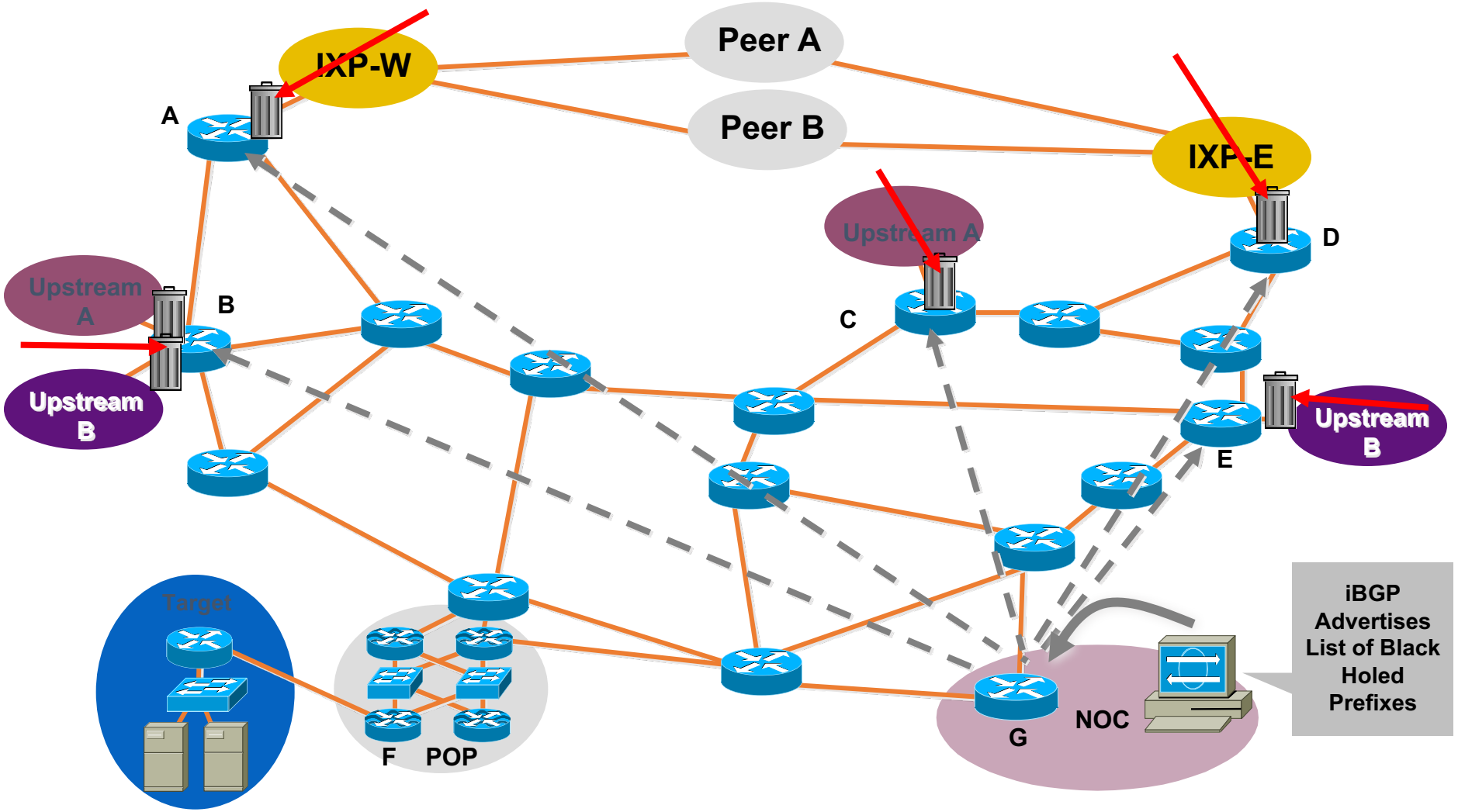
Customer Is DOSed—Before—Collateral Damage



SITREP – Attack in Progress

- Attack on a customer is impacting a number of customers.
- COLATERAL DAMAGE INCIDENT!
- Immediate Action: Solve the Collateral Damage issues.

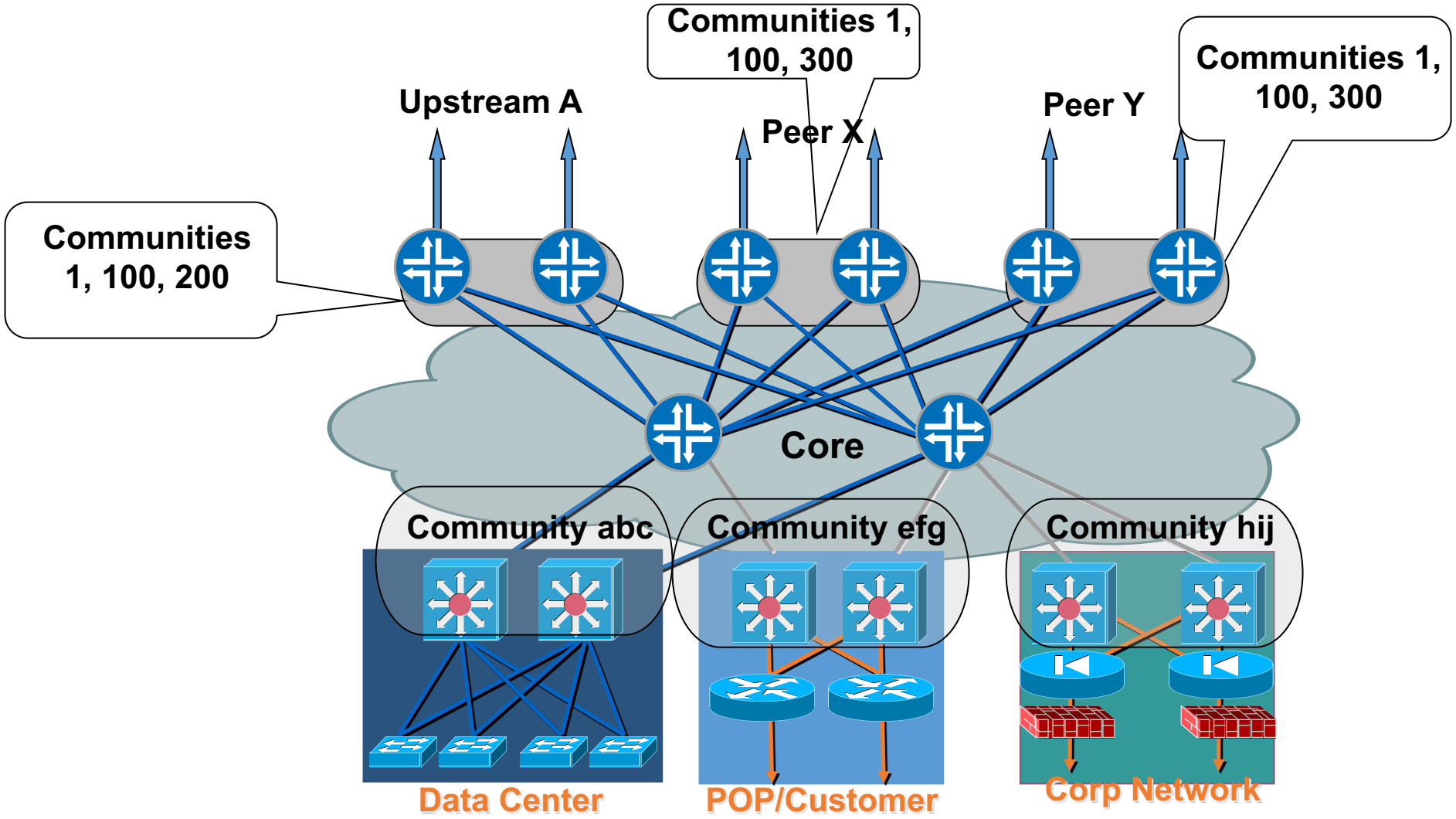
Customer Is DOSed—After—
Packet Drops Pushed to the Edge



SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Options:
  - Sink Hole a part of the traffic to analyze.
  - Watch the DOS attack and wait for Attack Rotation or cessation.
  - Activate “Clean Pipes” for a Full Service Recovery.

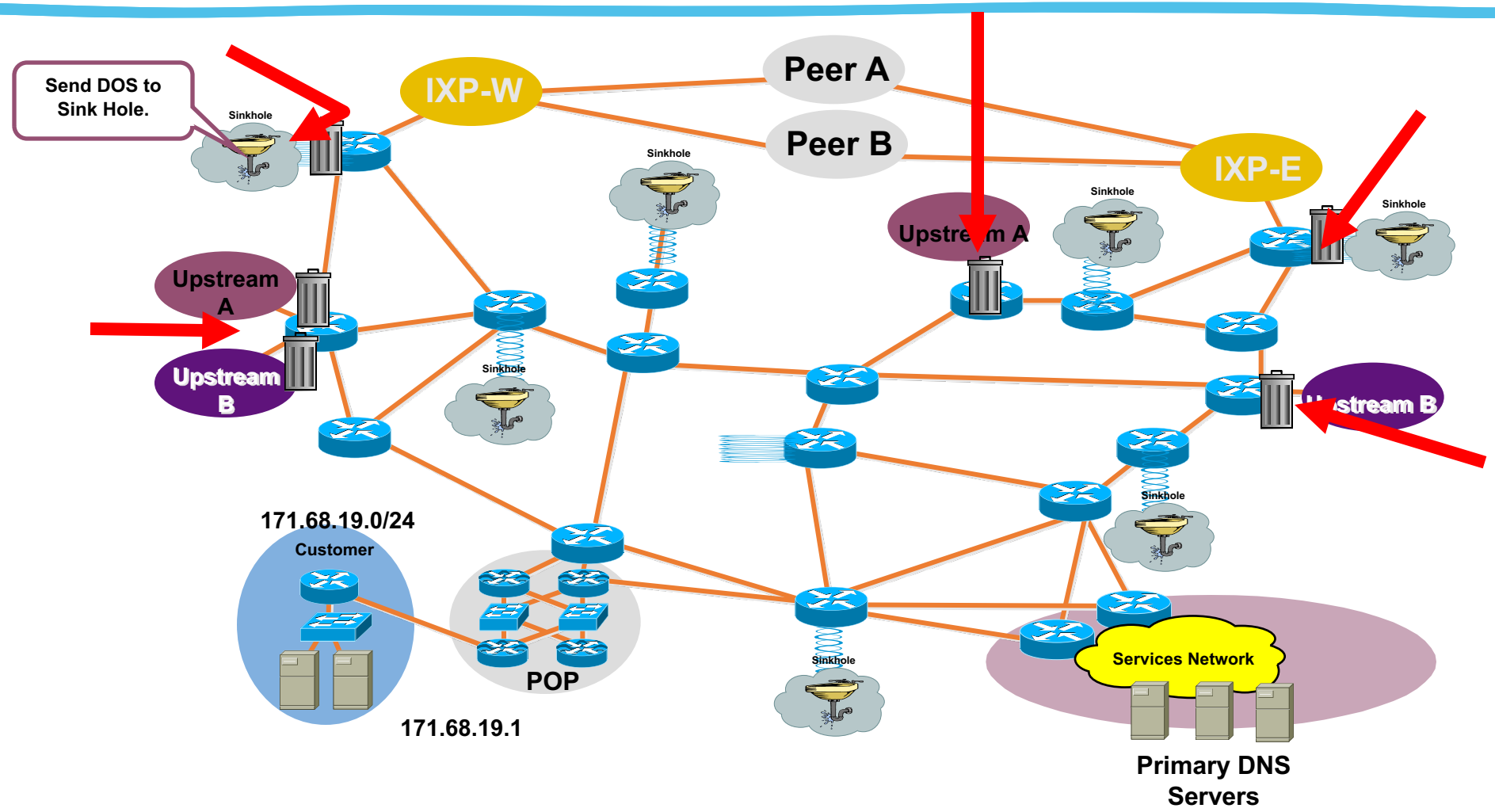
Remote Triggered Drops & BGP Communities



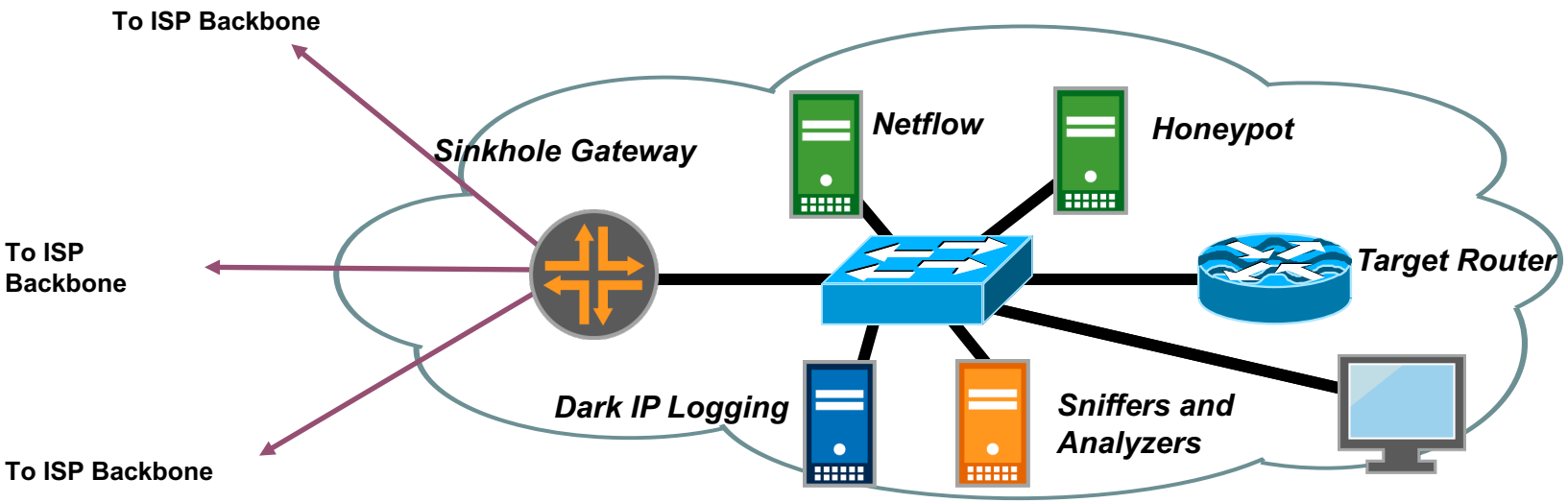
SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Action: Monitor the Attack & Get more details on the Attack – Use BGP Community based triggering to send one regions flow into a Sink Hole

BGP Community Trigger to Sinkhole



Analyze the Attack



- Use the tools available on the Internet and from Vendors to analyze the details of the attack.
- This will provide information about what you can or cannot do next.

SITREP – Attack in Progress

- Collateral Damage mitigated
- Customer who was attacked has PARTIAL SERVICE.
- DOS Attack is Still Active
- Action: Provide the Customer who is the victim with a Clean Pipes FULL SERVICE RECOVERY (off to vendor specific details).

What is Full Service Recovery

- “Clean Pipes” is a term used to describe *full service recovery*. The expectations for a full service recovery is:
  - DDOS Attack is in full force and ALL customer services are operating normally – meeting the contracted SLA.
  - The Device used for the full service recovery is not vulnerable to the DDOS & the infrastructure is not vulnerable to collateral damage.
- Full Service Recovery/Clean Pipes products are very specialized. Talk to the appropriate vendor.

Full vs Partial Service Recovery

- Partial Service Recovery is easy … push back the attack to the ASN Edge.

- Full Service Recover requires focused planning around the key services.

Pause for Questions

What's Next?

- Download White Papers, Blogs, Workshop Materials from www.senki.org

- Connect! Barry connects to peers, colleagues and aspiring talent via Linkedin (www.linkedin.com/in/barryrgreene/). You can also follow on Barry on Twitter (@BarryRGreene) or his blogs on Senki (www.senki.org).