

Cisco DDOS Solutions

Hank Nussbacher
IUCC – hank@mail.iucc.ac.il

Prague
Feb 24 & 25 2005

Appliances

Cisco Guard XT 5650:

- **Attack analysis & mitigation**
- **Diverts traffic for on-demand protection**
- **2 GE Fiber/Copper**



Cisco Guard XT 5650

Cisco Traffic Anomaly Detector XT 5600:

- **Attack detection & identification**
- **Monitors copy of traffic**
- **2 GE Fiber/Copper**



Cisco Traffic Anomaly Detector XT 5600

Also carrier grade versions (DC power, NEBS) planned

R4: Catalyst “Jaffa” Service Modules



Anomaly Guard Module

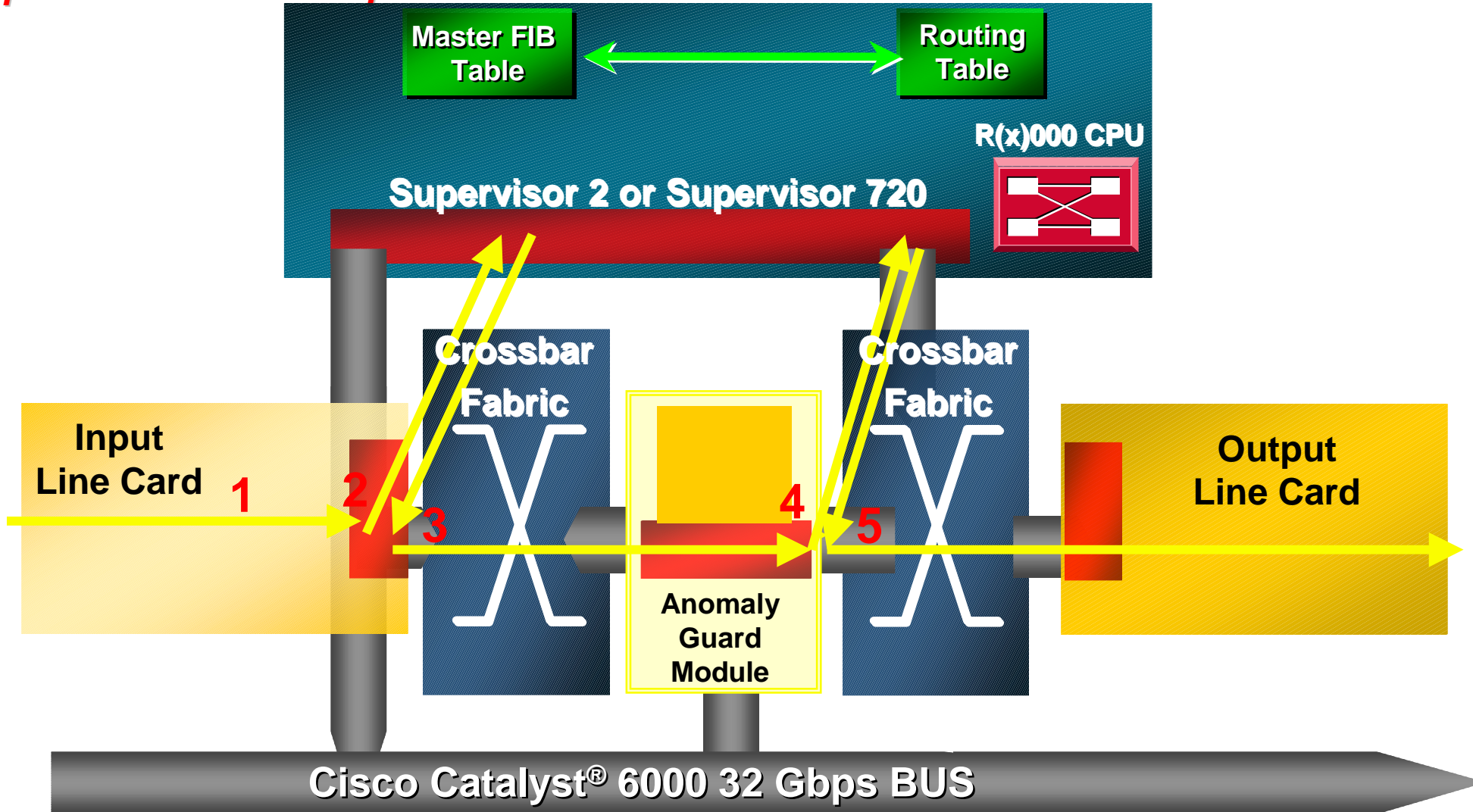


Traffic Anomaly Detector Module

- Single slot service modules for Cat 6K (7600 certification to follow)
- Similar performance and functionality to appliance
 - No on-board interfaces – uses line card or supervisor interfaces
 - No hard drive
 - Performance approximately 95% of appliance
 - Future software license upgrade for multi-processor 2-3X performance increase
- Sup 2 and Sup 720 IOS support (Rockies 1.3 = 12.2(18)SXD3) no Cat OS
 - Rockies 2 for 7600 support
- Multiple Guards (and Detectors) per chassis
 - Protecting non-overlapping zones or clustered for single zone
 - Min 4 each initially; follow on testing to 8+
 - Uses CEF level 3 hash per src-dst pair to load balance
- WBM, CLI and SNMP at FCS

Anomaly Guard Module Packet Flow

Supervisor 2/SFM or Supervisor 720



Performance

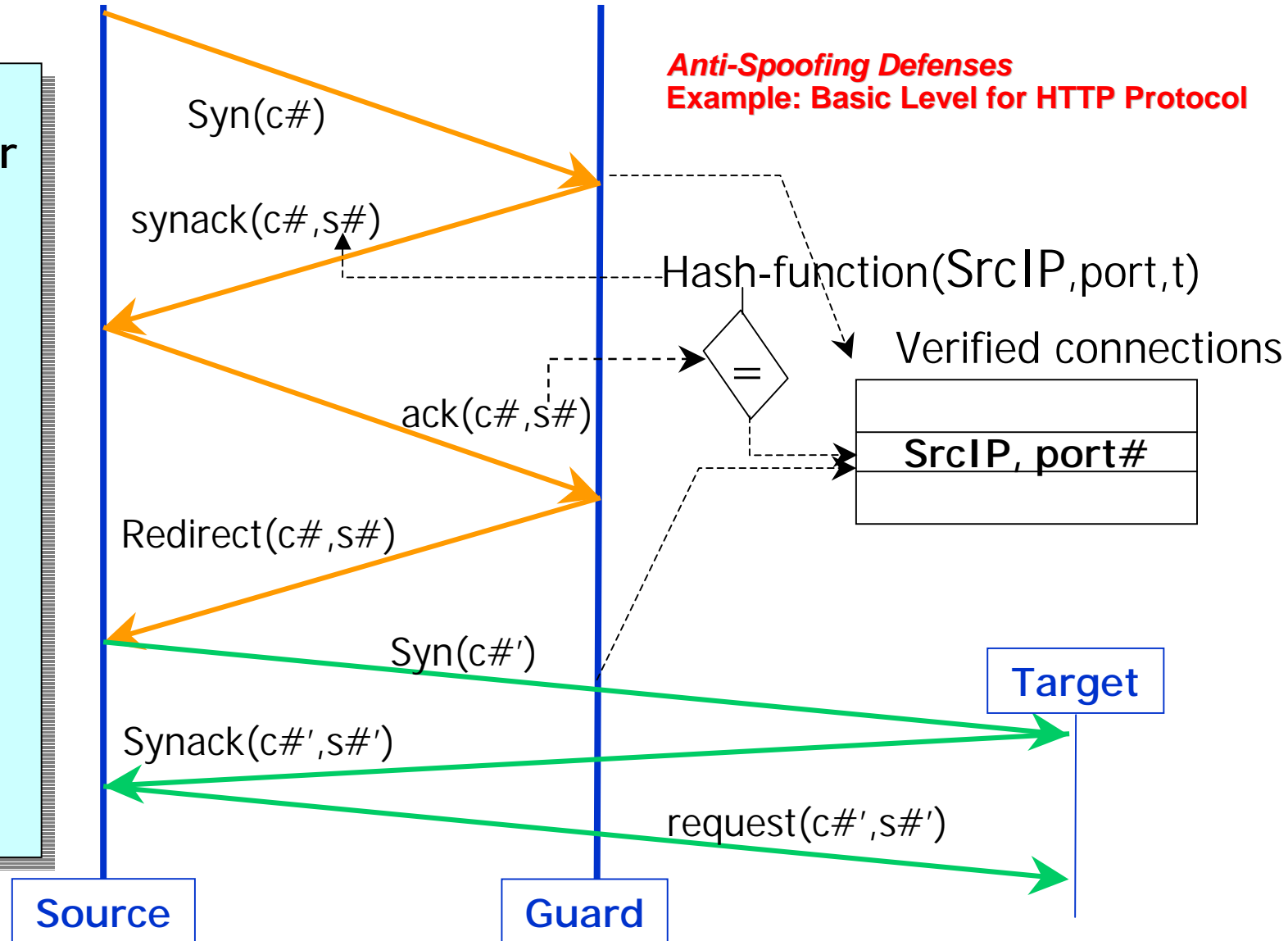
- **Detector XT**
 - Can detect on both GE interfaces
 - 3.0Mpps for detection
- **Guard XT**
 - 1.25Mpps for most attack conditions
 - 1.48Mpps optimal or 1Gbps
 - Protects 30 concurrently attacked “zones”
 - Minimum 1.5 million concurrent connections
 - 150,000 blocked sources (dynamic filters)
 - Can add 1000 sources/sec
 - < 1 msec latency & jitter

Anti-Spoofing

- **Specific support for protocols:**
 - HTTP, DNS
 - General TCP support (L5 - L7 independent) adapted and tested with many protocols: SMTP, IRC, HTTPS and many customer-proprietary protocols, ...
- **Authenticates:**
 - SYNs, SYNACKs, FINs, regular TCP packets
 - DNS requests, DNS replies, Zone transfers
 - UDP traffic via correlated TCP control sessions
- **Techniques for different protocols & level of authentication**
 - SYN cookie
 - Safe reset
 - TTL
 - DNS authentication techniques
 - Various Redirection methods

Antispoofing only when under attack

- Authenticate source on initial query
- No state kept for all flows; only for legitimate sources
- Subsequent queries verified



Anomaly Detection

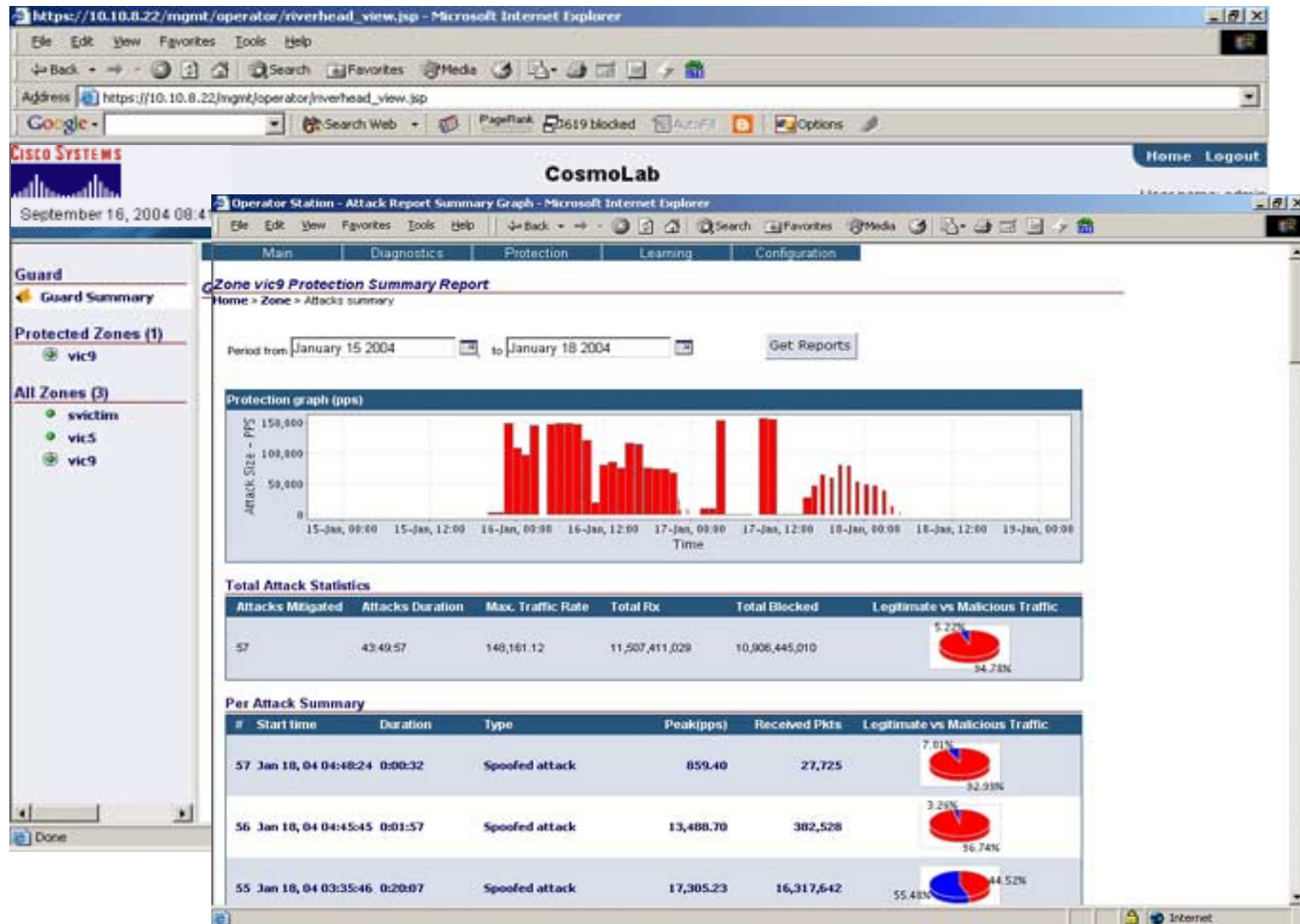
- **Flow Classification: Extensive profiling within global traffic to a zone**
 - From individual src-ips and src-nets
 - To individual dst-ips and dst-ports
 - By protocol
- **What: Depth of profiles**
 - Packets, syns and requests, fragments
 - Ratios eg SYNs to FINs
 - Unauthenticated vs authenticated pkts
 - Connection count by total and no-data
 - Number of non-spoofed sources
 - DNS reply and query pkts
- **Default normal baselines with site specific learning**
 - Baselines for typical as well as top sources and proxies

Broadest Attack Protection

- Random spoofed attacks (eg SYN,...)
 - **Removes spoofed flows that evade statistical detection**
- Focused spoofed of good source (eg AOL proxy)
 - **Distinguishes good vs bad flows with same src-IP**
- Non-spoofed distributed attack
 - **Capacity for high volume, massive and morphing botnets of attackers**
- Non-spoofed client attack (eg http 1/2 open)
 - **Identifies low volume, protocol anomaly attacks that evade sampled flow data**

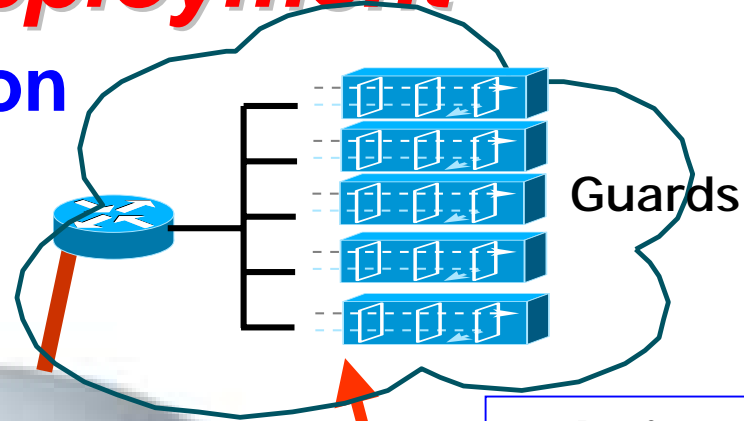
Management Features

- Cisco-like CLI
- Web (html) embedded device manager
 - At-a-glance operations management
 - Detailed attack data
 - Per-customer (zone) summary reports
- DDoS SNMP MIB and traps
- Interactive recommendations
- Extensive reporting
 - XML export
- HW environmental monitoring



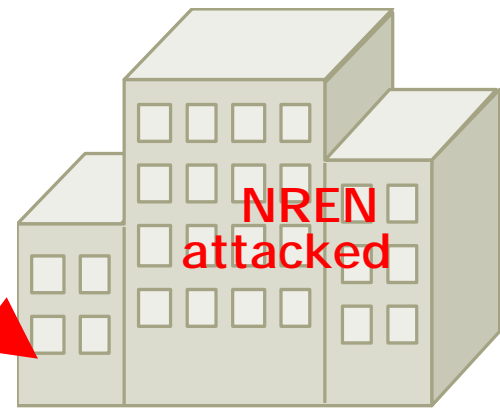
DDoS mitigation Deployment

DDoS protection Cluster



2. Activate: Auto/Manual

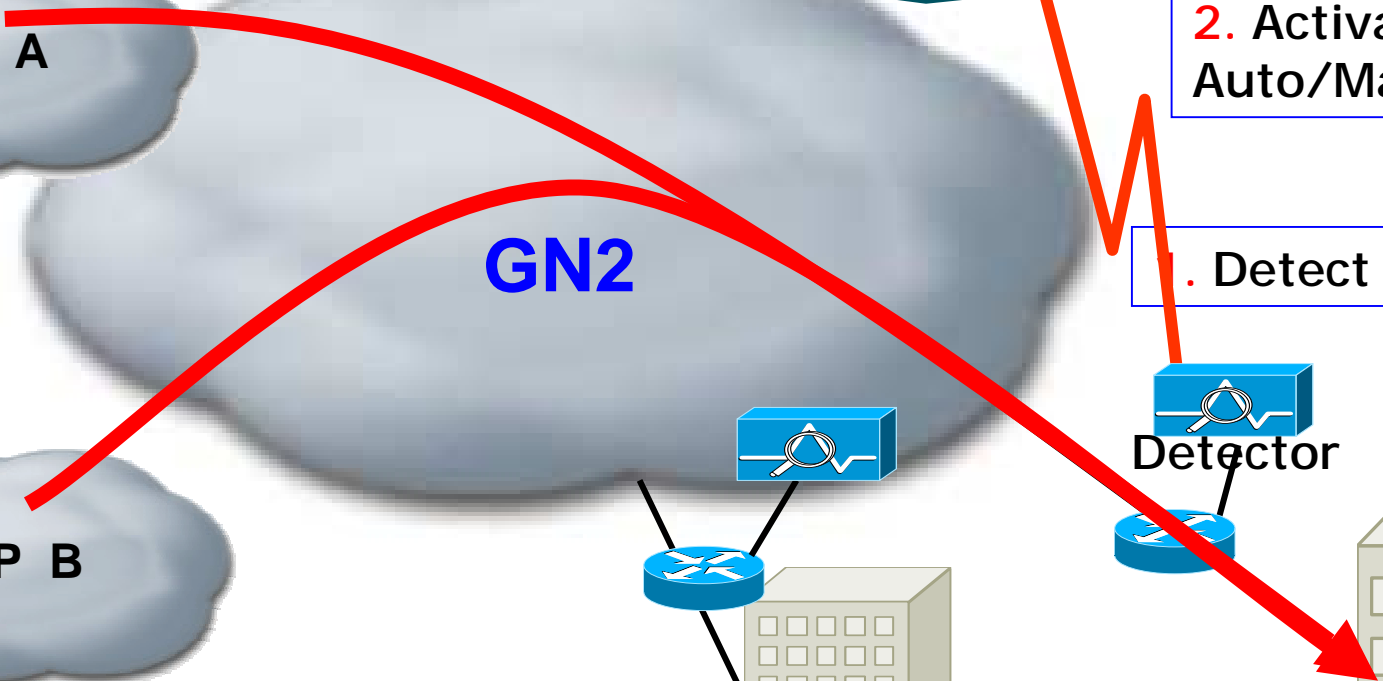
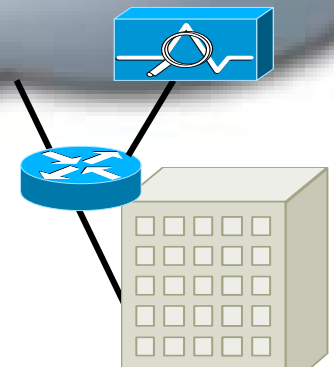
1. Detect



ISP A

ISP B

GN2



DDoS Mitigation Deployment

DDoS protection Cluster

3. Divert only target's traffic

4. Identify and filter the malicious

5. Forward the legitimate, via MPLS or GRE Tunnel

