R&S Security Overview

Santiago, Chile

Mayo 2009

Agenda

- Introduccion
- Update de mercado
- Aplicando seguridad al R&S
  - Problematicas de clientes y potenciales soluciones
  - Demos
- Conclusiones

Seguridad: que hacer durante la crisis?

- Priorizacion basada en riesgo y recompensa
- Tener la correcta mezcla de gente en su grupo
- Construir procesos replicables
- Crear una estrategia optima de costos compartidos
- Automatizar y outsourcing – pero sabiamente

Market share - Routing – Total Enterprise

- High end + access routing
- Datos al Q4CY08

Total Enterprise Router Market (Dell'Oro Group)							
Position	Vendor	Share	Q/Q Share Change	Y/Y Share Change	Revenue	Q/Q Revenue Growth	Y/Y Revenue Growth
1	CISCO	80.8%	-1.7%	-1.1%	$794.9	-8.5%	-8.9%
2	JUNIPER	5.6%	0.4%	0.2%	$55.3	1.5%	-3.5%
3	HUAWEI	3.7%	0.8%	0.4%	$36.3	19.0%	4.5%
4	3COM/H3C	3.0%	0.7%	0.8%	$29.3	24.4%	28.4%
5	NORTEL	1.2%	-0.4%	-0.2%	$11.8	-28.4%	-20.3%
Total Market					**$983.4**	-6.6%	-7.6%

Market share - Switching

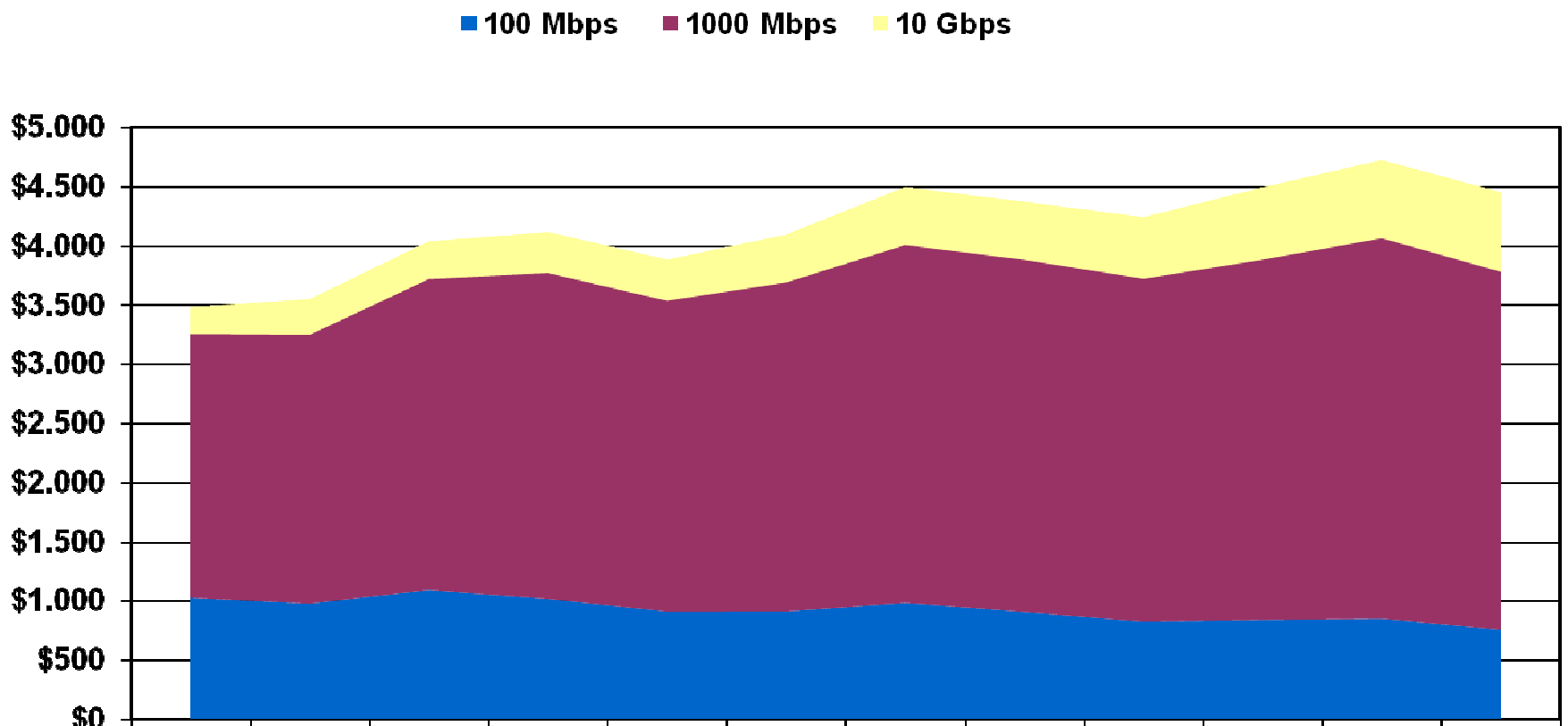
- Modular + fixed switching – managed only
- Datos al Q4CY08

Total L2+3 Total Managed Switch Revenue							Q4CY08
Position	Vendor	Share	Q/Q Share Change	Y/Y Share Change	Revenue ($M)	Q/Q Revenue Change	Y/Y Revenue Change
1	Cisco	76.0%	-0.4%	1.7%	$3,315.6	-6.0%	4.2%
2	HP ProCurve	5.0%	-0.1%	0.0%	$217.3	-6.5%	1.5%
3	Nortel	3.1%	0.1%	-1.0%	$136.2	-1.4%	-22.5%
4	3Com/H3C	2.2%	0.0%	-0.3%	$97.3	-6.5%	-8.5%
5	Foundry	1.9%	0.2%	-0.2%	$84.1	3.1%	-6.8%
Total Market					*$4,361.9*	*-5.5%*	*1.8%*

Market share – Switching
Unmanaged switches

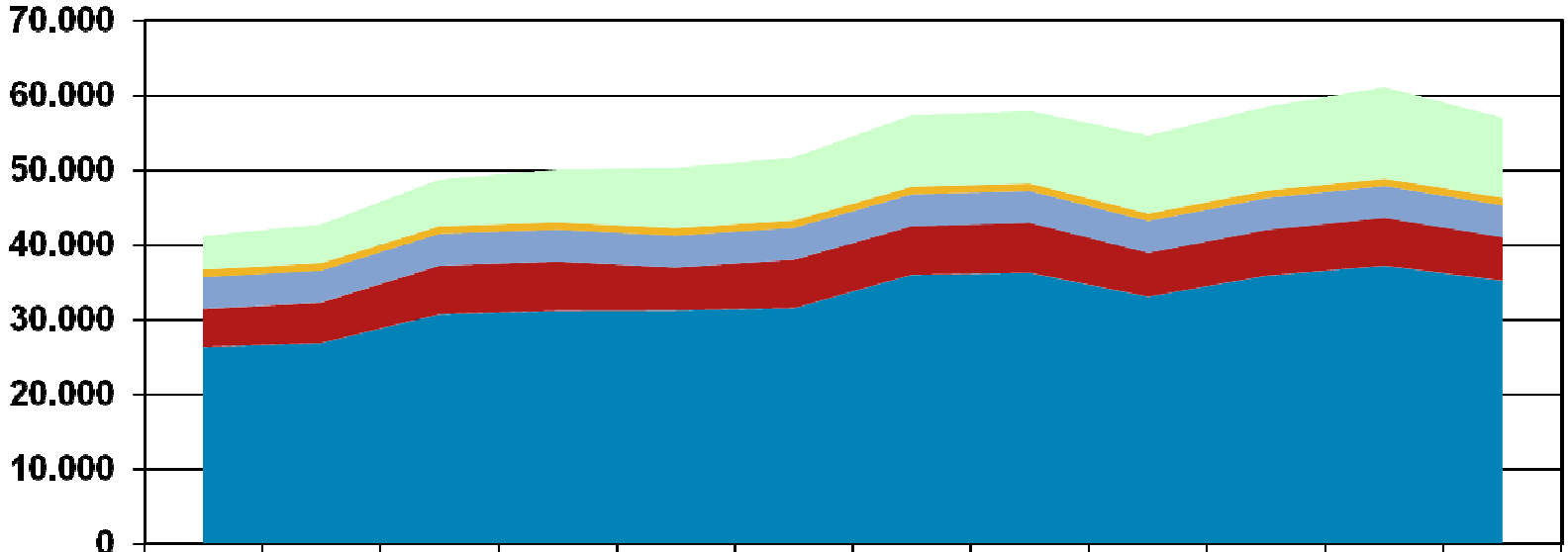
Total L2+3 Fixed Unmanaged Switch Revenue							Q4CY08
Position	Vendor	Share	Q/Q Share Change	Y/Y Share Change	Revenue ($M)	Q/Q Revenue Change	Y/Y Revenue Change
1	Netgear	22.3%	-1.8%	-3.9%	$20.5	-23.6%	-14.6%
2	D-Link	16.8%	-2.8%	1.6%	$15.4	-29.2%	10.7%
3	3Com/H3C	16.4%	-0.7%	-2.1%	$15.0	-20.6%	-10.7%
4	HP ProCurve	10.7%	1.8%	3.0%	$9.8	-1.1%	38.8%
5	Linksys	6.9%	1.1%	0.3%	$6.4	-2.0%	4.9%
Total Market					*$91.7*	*-17.3%*	*0.5%*

Switching – distribucion por velocidad



	1Q06	2Q06	3Q06	4Q06	1Q07	2Q07	3Q07	4Q07	1Q08	2Q08	3Q08	4Q08
10 Gbps	$ 228	$ 302	$ 320	$ 347	$ 348	$ 405	$ 490	$ 491	$ 520	$ 611	$ 660	$ 673
1000 Mbps	$ 2.231	$ 2.273	$ 2.628	$ 2.756	$ 2.627	$ 2.781	$ 3.025	$ 2.977	$ 2.899	$ 3.045	$ 3.215	$ 3.026
100 Mbps	$ 1.026	$ 976	$ 1.092	$ 1.016	$ 910	$ 910	$ 983	$ 906	$ 823	$ 839	$ 850	$ 755

12 Quarter Total L2+3 Port Summary
By Form Factor & PoE Capability



	1Q06	2Q06	3Q06	4Q06	1Q07	2Q07	3Q07	4Q07	1Q08	2Q08	3Q08	4Q08
Unmanaged	4.523	5.218	6.290	7.098	8.108	8.485	9.618	9.746	10.493	11.271	12.258	10.788
Modular PoE	1.027	1.027	1.027	1.027	1.027	1.027	1.027	1.027	1.027	1.027	1.027	1.027
Fixed Mgd PoE	4.315	4.315	4.315	4.315	4.315	4.315	4.315	4.315	4.315	4.315	4.315	4.315
Modular Non PoE	5.058	5.409	6.481	6.569	5.739	6.475	6.517	6.707	5.869	6.135	6.416	5.825
Fixed Mgd Non PoE	26.260	26.786	30.649	31.101	31.150	31.442	35.923	36.180	32.983	35.791	37.126	35.133

Routing y Switching Baseline

Routers

- IOS Firewall
- IOS VPN
- IOS IPS
- CoPP
- Routing
- uRPF

Switches

- STP Tookit
- DHCP snooping
- IP Source Guard
- DAI
- VACL
- CoPP

Seguridad infraestructura de red

Mejores prácticas

- Uso de SSH/SSL
- Rate limiting
- Gestión fuera de banda

Visibilidad

- Gestión centralizada
- Netflow
- IP SLA

Seguridad de infraestructura de red Decreto 83 [1/2]

d) Seguridad del personal:

Se aplicarán las secciones 6.1 y 6.3 del capítulo 6 de la norma NCh2777. La sección 6.2 se adoptará como recomendación.

Sección 6.1 de la Norma Chilena de Seguridad 2777

6.1 Seguridad en la definición del trabajo y recursos

Objetivo: Reducir los riesgos de error humano, robos, fraudes o mal uso de las instalaciones.
Las responsabilidades de seguridad se deberían asignar en la etapa de contratación del personal, incluirlas en los contratos, y monitorearlas durante el empleo de la persona.
Los potenciales postulantes se deberían seleccionar adecuadamente (ver 6.1.2), especialmente para trabajos sensibles. Todos los empleados y los usuarios de terceras partes de los equipos de procesamiento de la información, deberían firmar un acuerdo de confidencialidad (no divulgación).

Seguridad de infraestructura de red
Decreto 83 [2/2]

i) Gestión de la continuidad del negocio: Se aplicarán las estipulaciones del capítulo 11 de la norma NCh2777, en su integridad.

Artículo Segundo.- La presente norma deberá ser implementada por los diferentes órganos de la Administración del Estado dentro de los siguientes plazos:

- El Nivel 1, a más tardar en el año 2004.
- El Nivel 2, a más tardar en el año 2009.

Capítulo 11 de la Norma Chilena de Seguridad 2777

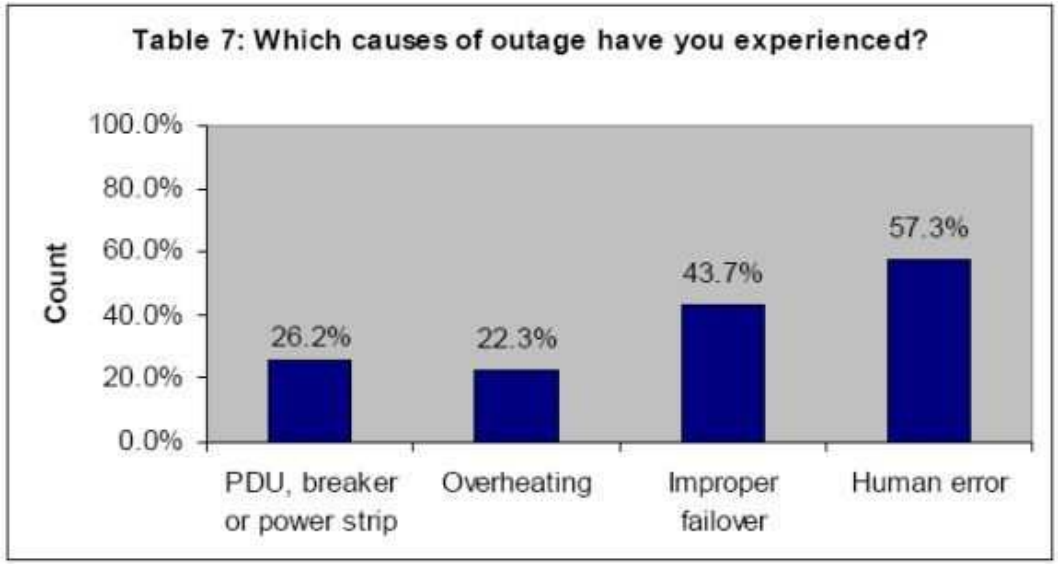
11 Gestión de la continuidad del negocio

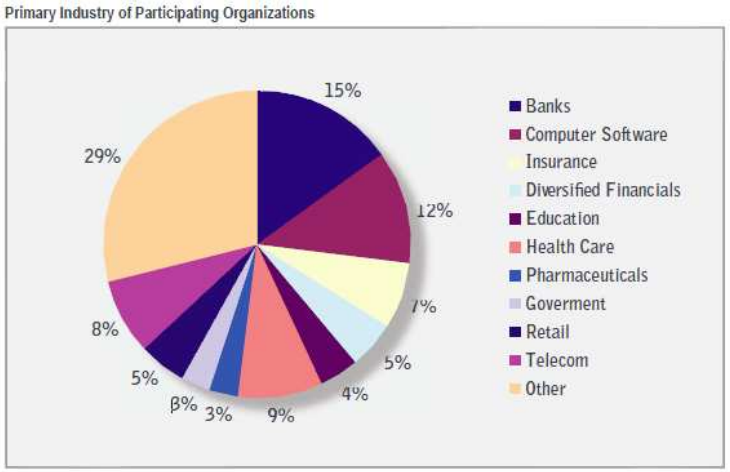
11.1 Aspectos de la gestión de la continuidad del negocio

Objetivo: Contrarrestar las interrupciones de las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres.
Se debería implementar un proceso de gestión de la continuidad del negocio para reducir las interrupciones que causan los desastres y fallas de seguridad (los que pueden ser resultado de, por ejemplo, desastres naturales, accidentes, fallas de equipos, y acciones deliberadas) a un nivel aceptable, como una combinación de controles preventivos y recuperativos.
Se deberían analizar las consecuencias de los desastres, fallas de seguridad y pérdidas de servicio. Se deberían desarrollar e implementar planes de contingencia para asegurar que los procesos del negocio se puedan restablecer dentro de una escala de tiempo necesaria. Tales planes se deberían mantener y practicar para que lleguen a ser una parte integral de todos los otros procesos de gestión. La gestión de la continuidad del negocio debería incluir los controles para identificar y reducir los riesgos, limitar las consecuencias de daños de incidentes y asegurar a tiempo la reanudación de las operaciones esenciales.

Aplicando Seguridad en switching

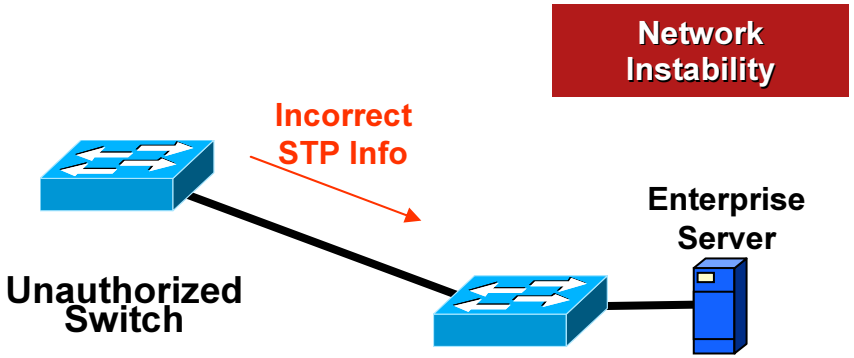
Desafio:
Inestabilidad de redes en L2

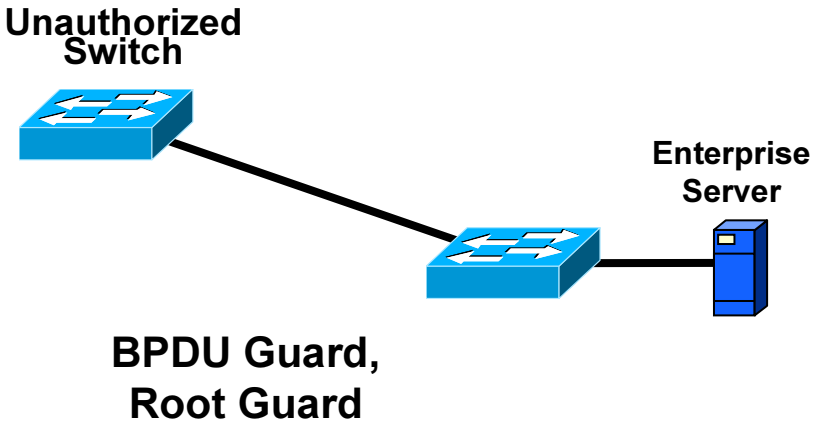




Fuente: Aperture Research

Desafio:
Inestabilidad de redes en L2





Problem:

- Rogue switches or routers can insert incorrect routing/STP info and inadvertently bring down the entire network

Solution:

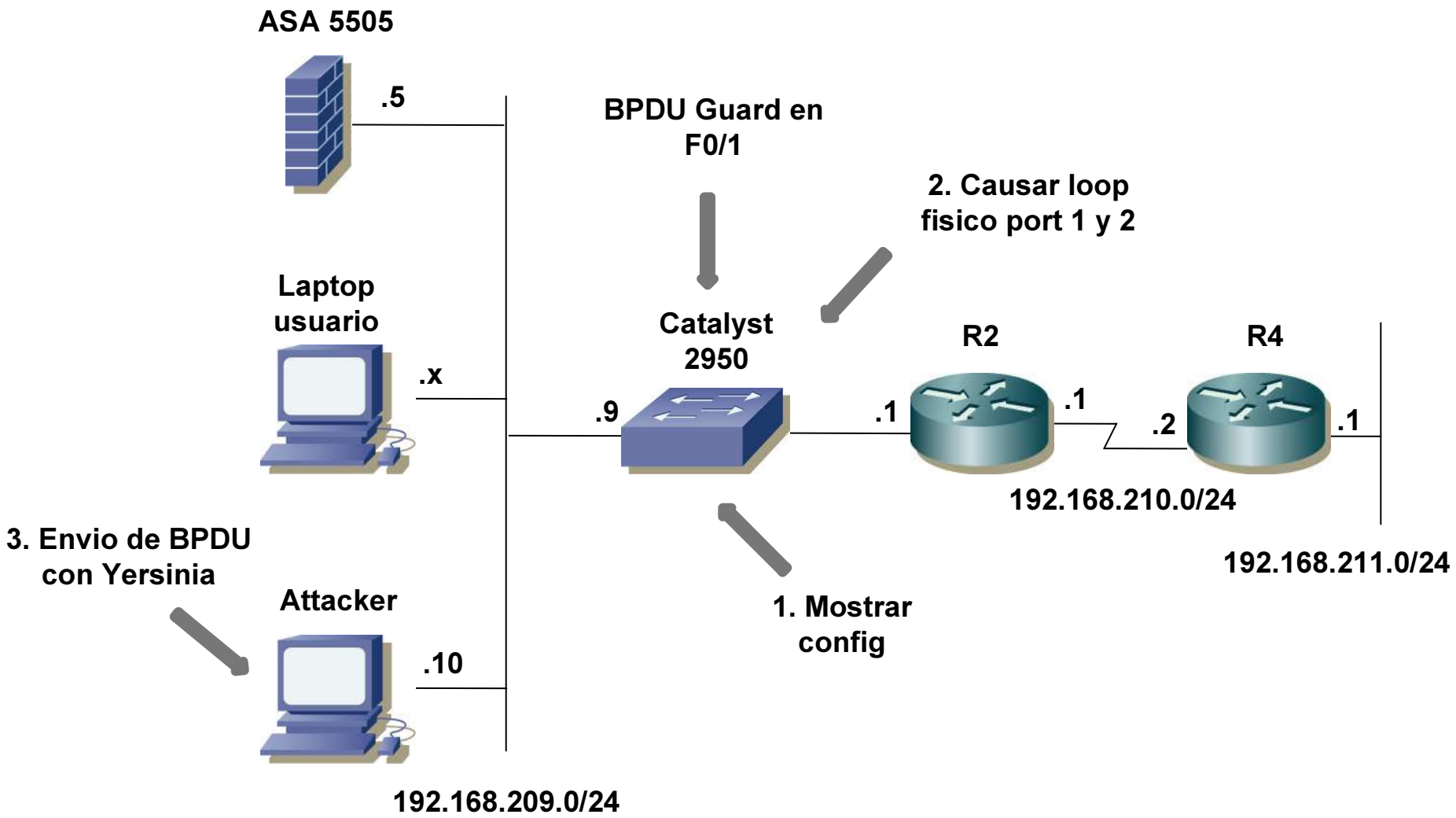
- Catalyst Switches support BPDU-Guard and authenticated routing updates: BPDU Guard, Root Guard, etc.

Disponibilidad - BPDU Guard

Cisco Catalyst Switches: **FEATURE COMPARISON**

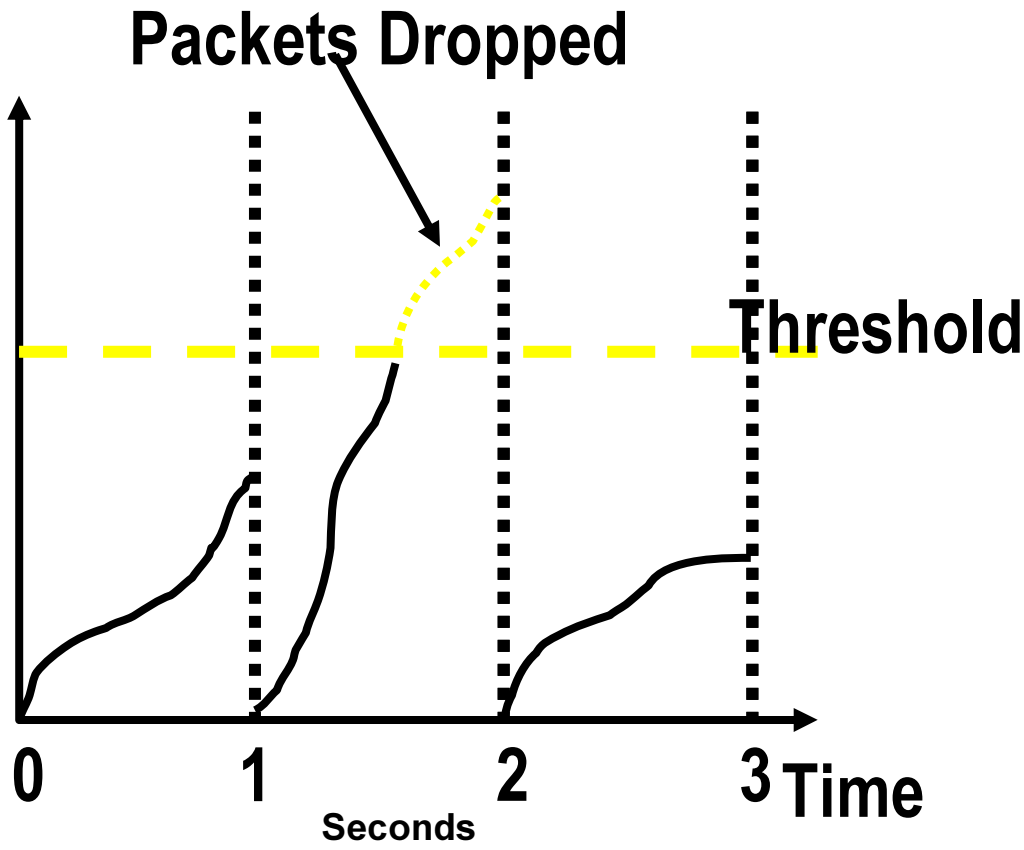
	MODULAR SWITCHES		FIXED-CONFIGURATION SWITCHES								
	Catalyst 6500	Catalyst 4500	Catalyst 4900	Catalyst 3750-E	Catalyst 3750	Catalyst 3650-E	Catalyst 3560	Catalyst 2960	Catalyst 2950	Catalyst 2940	Catalyst Express 500
AVAILABILITY AND RESILIENCY											
Switch Redundancy											
IOS Software Modularity	•										
Non-stop Forwarding/Stateful Switchover (NSF/SSO)	•	•		•	•						
NSF-aware	•	•	•	•	•	•	•				
Redundant Power Supplies	•	•	•	External only	External only	External only	External only	External only	External only		External
Redundant Fans	•	•	•								
Redundant Fan Trays	•										
Redundant Supervisors	•	•									
Generic Online Diagnostics (GOLD)	•			•	•	•	•				
Basic Support for GOLD Services	•	•	•	•	•	•	•				
Power Supply Failure Redundancy	•	•	•	•	•	•	•	•	•		24, PC only
Power Circuit Failure Redundancy	•	•	•								
Network Protocols											
Unidirectional Link Detection (UDLD)	•	•	•	•	•	•	•	•	•	•	•
Gateway Load Balancing Protocol (GLBP)	•										
Hot Standby Routing Protocol (HSRP)	•	•	•	•	•	•	•				
Virtual Router Redundancy Protocol (VRRP)	•	•	•								
UplinkFast	•	•	•	•	•	•	•	•	•	•	•
BackBoneFast	•	•	•	•	•	•	•	•	•	•	•
RSTP (802.1w)	•	•	•	•	•	•	•	•	•	•	•
PortFast	•	•	•	•	•	•	•	•	•	•	•
Per VLAN STP (PVSTP)	•	•	•	•	•	•	•	•	•	•	•
Per VLAN RSTP (PVRSTP)	•			•	•	•	•	•	•	•	•
Multiple Instance STP (MISTP)	•	•	•	•	•	•	•	•	•	•	•
MSTP (802.1s)	•	•	•	•	•	•	•	•	•	•	
STP Root Guard	•	•	•	•	•	•	•	•	•	•	•
BDPU Guard	•	•	•	•	•	•	•	•	•	•	•
Loop Guard	•	•	•	•	•	•	•	•	•	•	•
IP Event Dampening	•										
Bidirectional Forwarding Detection	•										

Demo – BPDU Guard

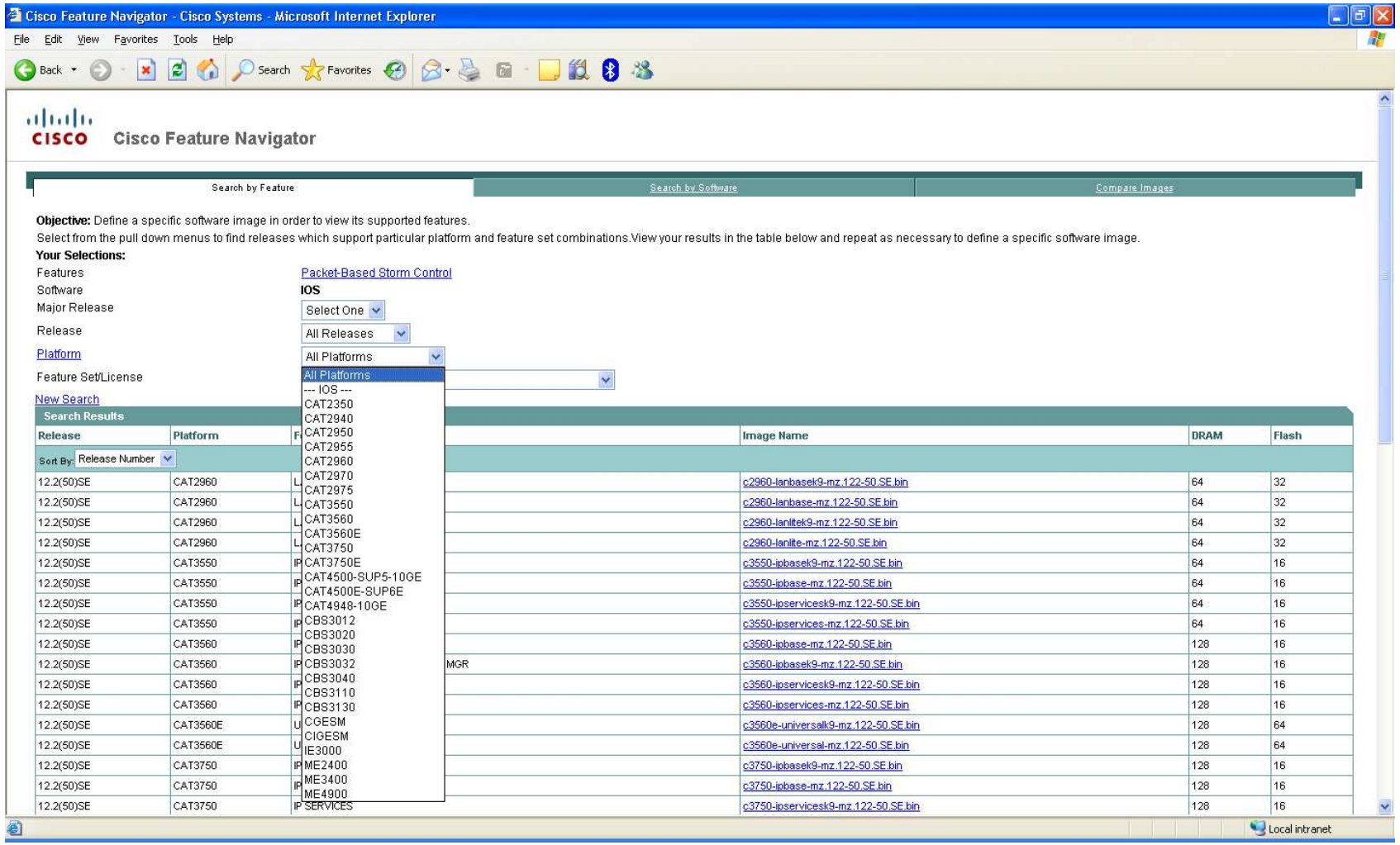


Storm Control

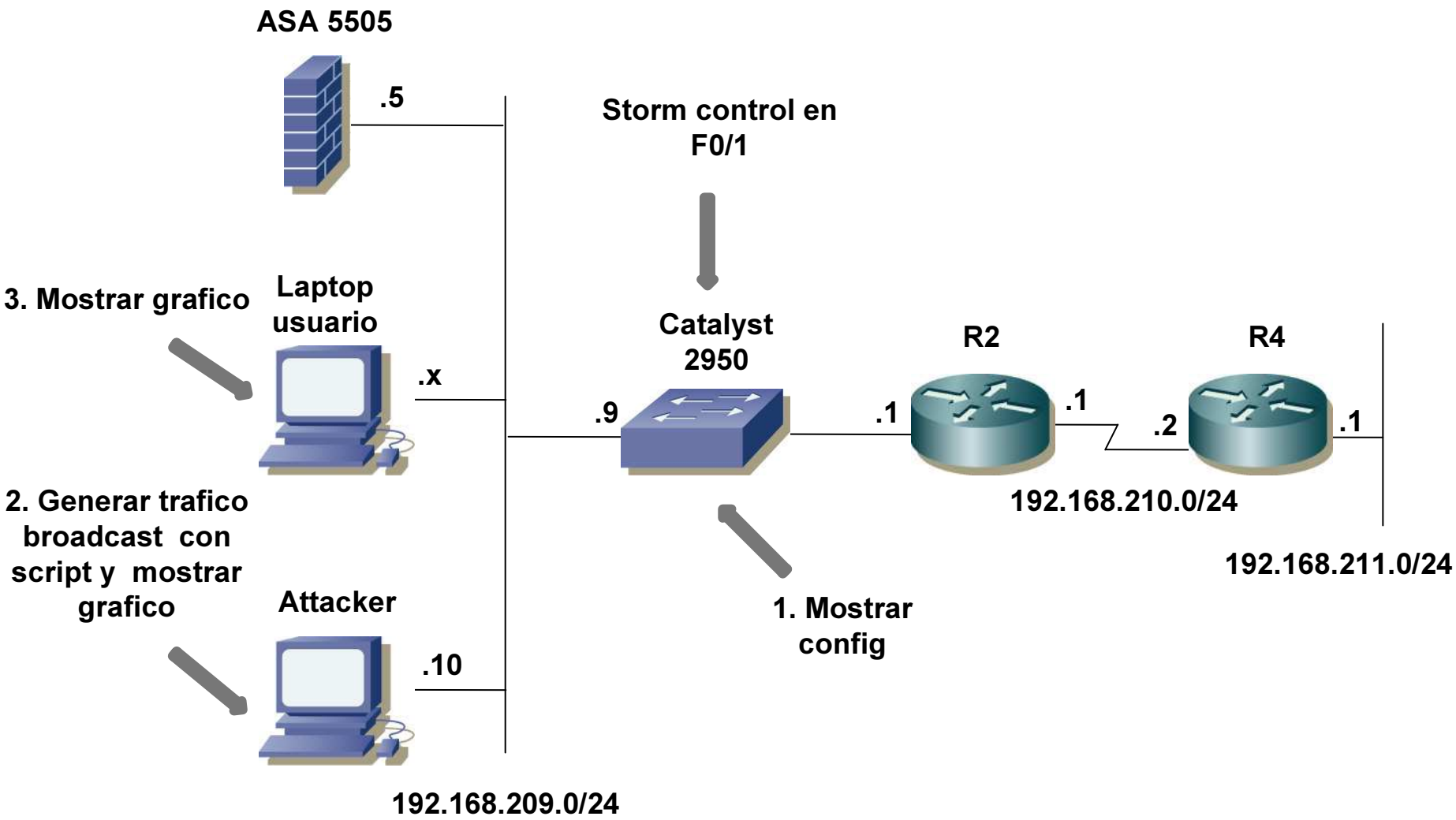
- Storm Control is also known as Broadcast suppression
- Able to limit the volume of broadcast, multicast and/or unicast traffic
- Protect the network from intentional and unintentional flood attacks i.e. STP loop
- Limit the combined rate of broadcast & multicast traffic to normal peak loads



Disponibilidad – Storm control



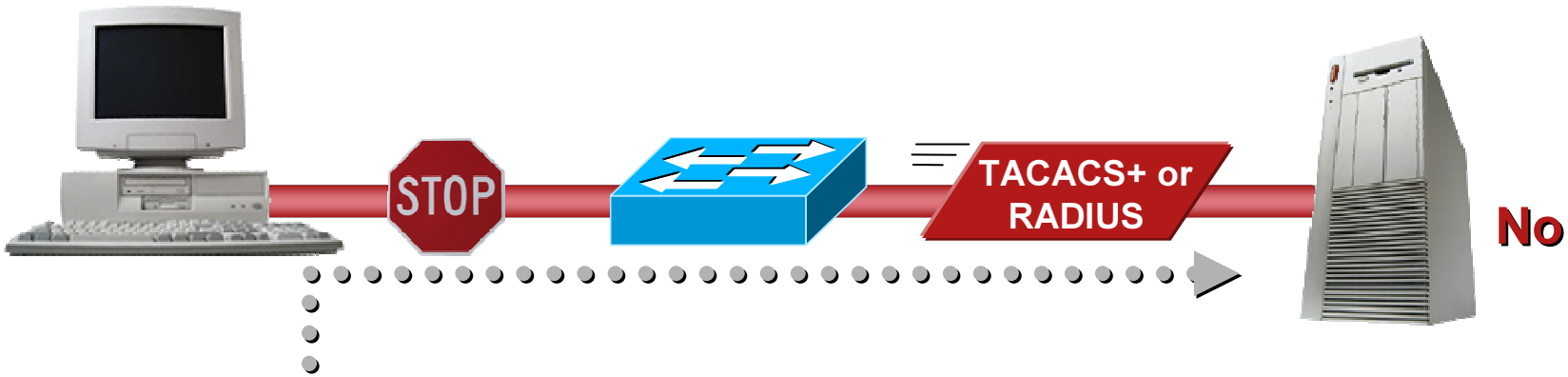
Demo – Storm Control Broadcast



Autenticacion en redes – 802.1x

How It Works:

Each person trying to enter the network must receive authorization based on their personal username and password.



Client Accessing Switch (802.1x Suplicant)

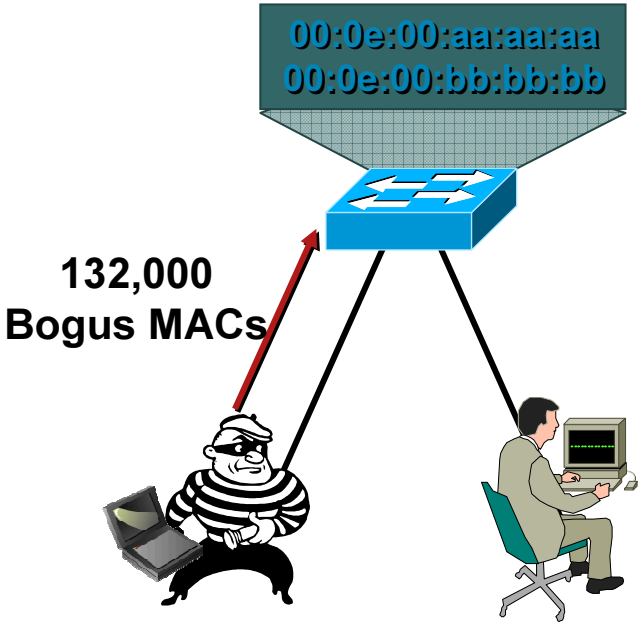
TACACS+ or Radius Server

Disponibilidad – 802.1x

Cisco Catalyst Switches: **FEATURE COMPARISON**

	MODULAR SWITCHES		FIXED-CONFIGURATION SWITCHES								
	Catalyst 6500	Catalyst 4500	Catalyst 4900	Catalyst 3750-E	Catalyst 3750	Catalyst 3650-E	Catalyst 3560	Catalyst 2960	Catalyst 2950	Catalyst 2940	Catalyst Express 500
INTEGRATED SECURITY continued											
Attack Mitigation continued											
Dynamic ARP Inspection	•	•	•	•	•	•	•				
MAC Address Notification	•	•	•	•	•	•	•	•	•	•	•
Port Security	•	•	•	•	•	•	•	•	•	•	•
H/W-based uRFP Check	•			•		•					
H/W-based MAC Learning	•										
H/W-assisted MAC Aging	•			•		•					
PIM Accept Register—Rogue Multicast Server Protection	•			•		•					
Routing Protocol Pass Through	•										
ARP Policing	•										
H/W-based Directed Broadcast	•										
Trust and Identity Management											
802.1x Identity-based Networking Port Authentication	•	•	•	•	•	•	•	•	•	•	•
802.1x with VLAN assignment	•	•	•	•	•	•	•	•	•	•	
802.1x with Guest VLAN	•	•	•	•	•	•	•	•	•	•	
802.1x with Aux. VLAN Support	•	•	•	•	•	•	•	•	•	•	
802.1x Port Description	•										
TACACS+/RADIUS	•	•	•	•	•	•	•	•	•	•	RADIUS only
Web Authentication Proxy	•			•	•	•	•	•			
MAC Authentication	•	•	•	•	•	•	•	•		•	
Unidirectional Control Port	•										
Inaccessible Authentication	•	•	•	•	•	•	•	•			
Secure Connectivity											
H/W-based NAT/PAT	•										
MD5 Route Authentication	•	•	•	•	•	•	•				
Multilevel Account Privilege	•	•	•	•	•	•	•				

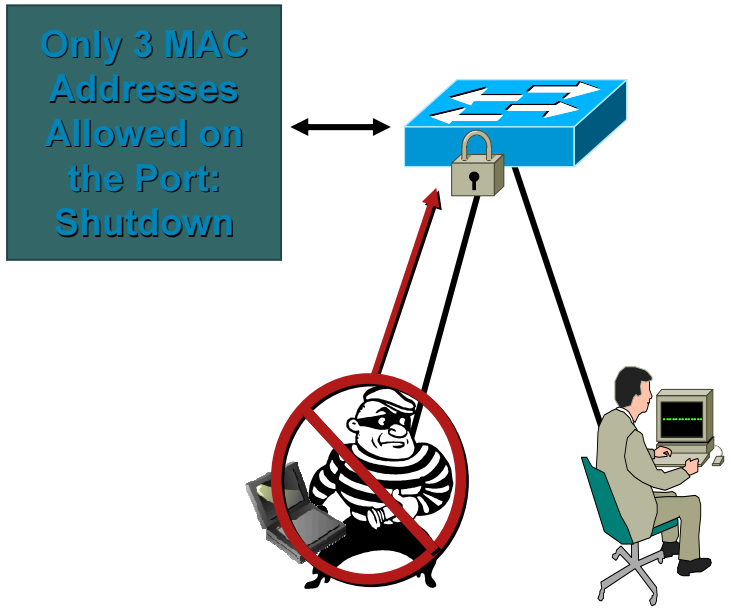
Desafio:
Protegiendo confidencialidad de datos en capa 2



Problem:

"Script Kiddie" Hacking Tools Enable Attackers Flood Switch CAM Tables with Bogus Macs; Turning the VLAN into a "Hub" and Eliminating Privacy

Switch CAM Table Limit of 32K Mac Addresses



Solution:

Port Security Limits MAC Flooding Attack and Locks down Port and Sends an SNMP Trap

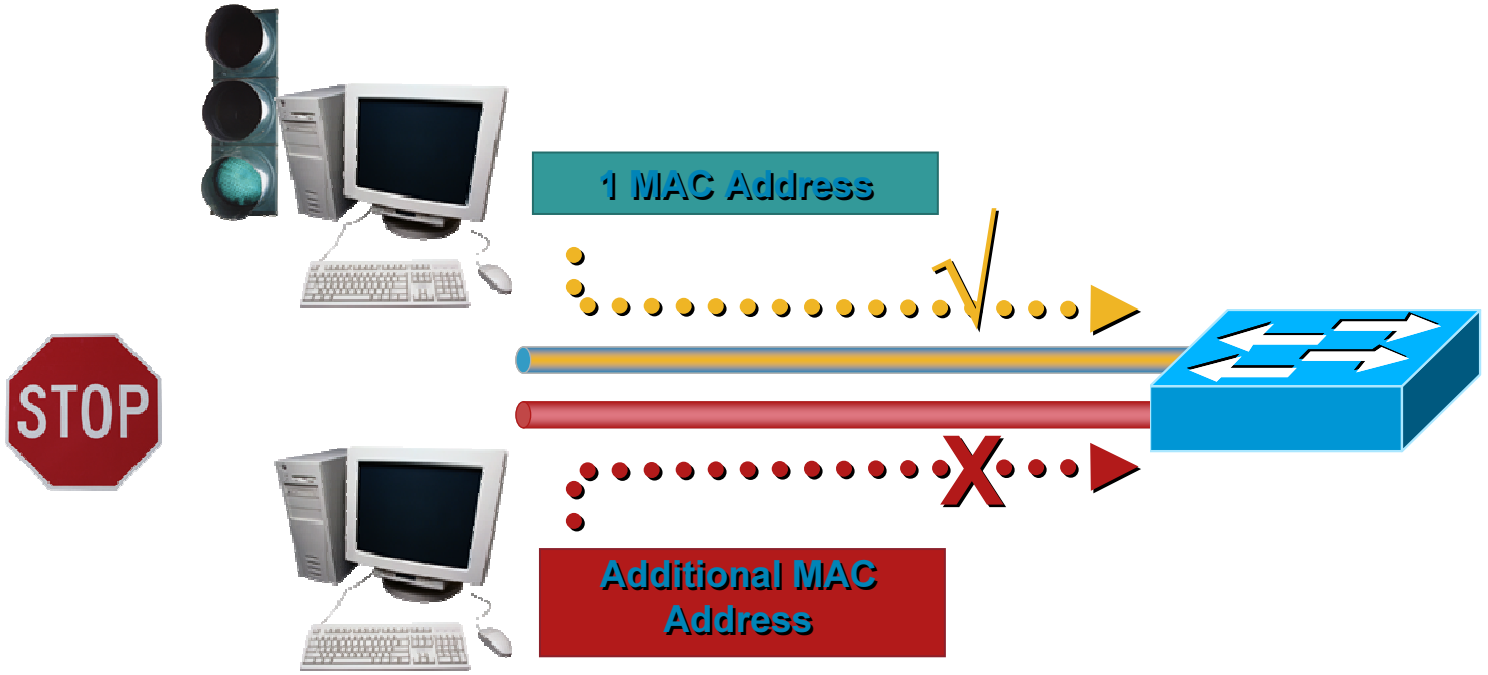
Port Security

What It Does:

Limits the number of MAC addresses that are able to connect to a switch and ensures only approved MAC addresses are able to access the switch.

Benefit:

Ensures only approved users can log on to the network.

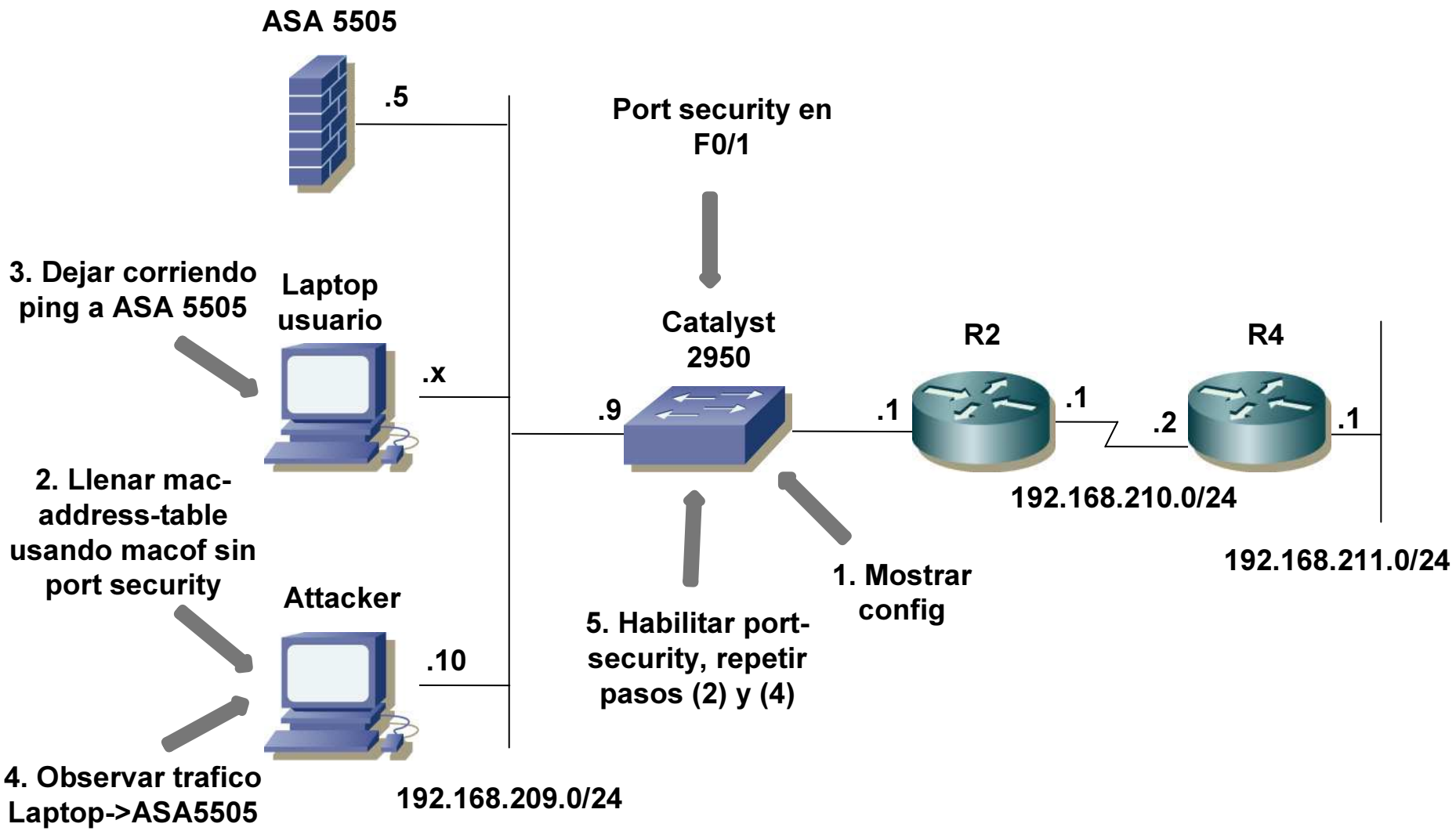


Disponibilidad – port security

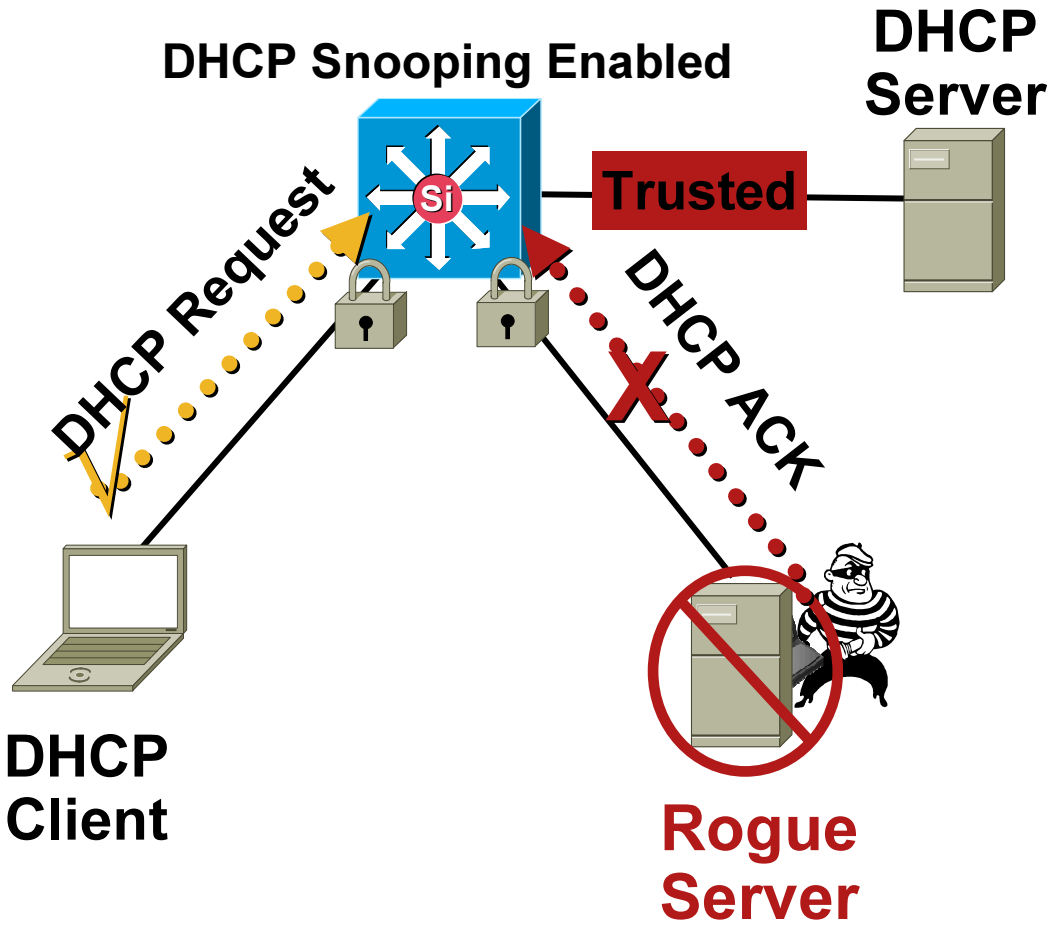
Cisco Catalyst Switches: **FEATURE COMPARISON**

	MODULAR SWITCHES		FIXED-CONFIGURATION SWITCHES								
	Catalyst 6500	Catalyst 4500	Catalyst 4900	Catalyst 3750-E	Catalyst 3750	Catalyst 3650-E	Catalyst 3560	Catalyst 2960	Catalyst 2950	Catalyst 2940	Catalyst Express 500
INTEGRATED SECURITY continued											
Attack Mitigation continued											
Dynamic ARP Inspection	•	•	•	•	•	•	•				
MAC Address Notification	•	•	•	•	•	•	•	•	•	•	•
Port Security	•	•	•	•	•	•	•	•	•	•	•
H/W-based uRFP Check	•			•		•					
H/W-based MAC Learning	•										
H/W-assisted MAC Aging	•			•		•					
PIM Accept Register—Rogue Multicast Server Protection	•			•		•					
Routing Protocol Pass Through	•										
ARP Policing	•										
H/W-based Directed Broadcast	•										
Trust and Identity Management											
802.1x Identity-based Networking Port Authentication	•	•	•	•	•	•	•	•	•	•	•
802.1x with VLAN assignment	•	•	•	•	•	•	•	•	•	•	
802.1x with Guest VLAN	•	•	•	•	•	•	•	•	•	•	
802.1x with Aux. VLAN Support	•	•	•	•	•	•	•	•	•	•	
802.1x Port Description	•										
TACACS+/RADIUS	•	•	•	•	•	•	•	•	•	•	RADIUS only
Web Authentication Proxy	•			•	•	•	•	•			
MAC Authentication	•	•	•	•	•	•	•	•		•	
Unidirectional Control Port	•										
Inaccessible Authentication	•	•	•	•	•	•	•	•			
Secure Connectivity											
H/W-based NAT/PAT	•										
MD5 Route Authentication	•	•	•	•	•	•	•				
Multilevel Account Privilege	•	•	•	•	•	•	•				

Demo – Port security



Desafio
Protección de LAN frente a DHCP servers no autorizados



What It Does:

- **Switch forwards only DHCP requests from untrusted access ports, drops all other types of DHCP traffic.**
- **Allows only designated DHCP ports or uplink ports trusted to relay DHCP Messages**
- **Builds a DHCP binding table containing client IP address, client MAC address, port, VLAN number**

Benefit:

Eliminates rogue devices from behaving as the DHCP server

Disponibilidad – DHCP snooping

Cisco Catalyst Switches: **FEATURE COMPARISON**

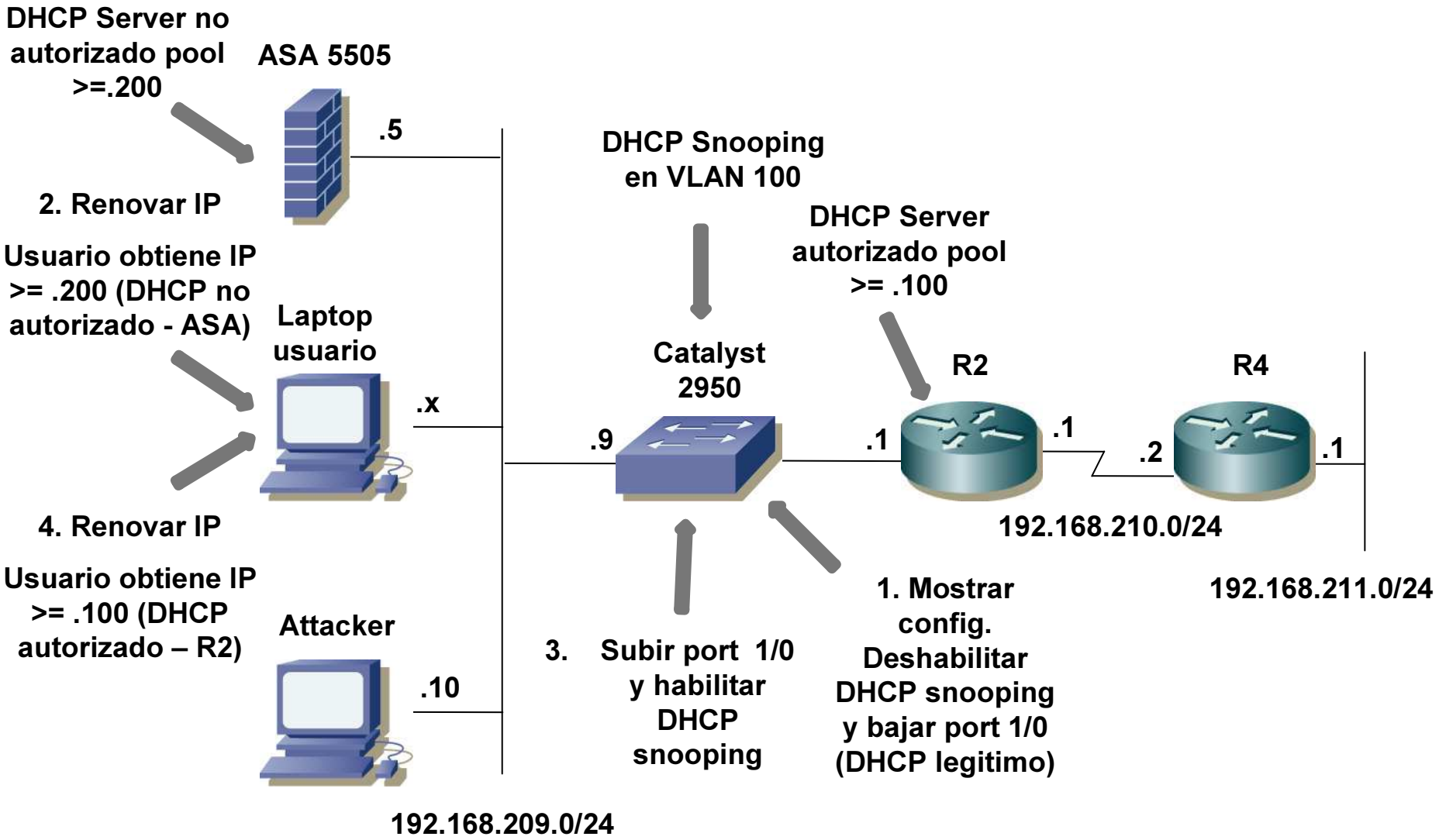
	MODULAR SWITCHES		FIXED-CONFIGURATION SWITCHES								
	Catalyst 6500	Catalyst 4500	Catalyst 4900	Catalyst 3750-E	Catalyst 3750	Catalyst 3650-E	Catalyst 3560	Catalyst 2960	Catalyst 2950	Catalyst 2940	Catalyst Express 500
LAN SWITCHING FEATURES continued											
Layer 3 continued											
RIP, RIPv2	•	•	•	•	•	•	•				
Static Routes	•	•	•	•	•	•	•				
IS-IS	•	•	•								
H/W-based IPv6 Routing	•	In software	In software	•	•	•	•				
H/W-based Policy Routing IPv4	•	•	•	•	•	•	•				
H/W-based Policy Routing IPv6	•			•	•	•	•				
Multiprotocol Routing (IPX, AppleTalk)	•	•	•								
Cisco Express Forwarding (CEF)	•	•	•	•	•	•	•				
H/W FIB Entries	Up to 1,000,000	Up to 128,000	Up to 128,000	Up to 20,000	Up to 20,000	Up to 11,000	Up to 11,000				
VRF Lite	IP Services	IP Services	IP Services	IP Services	IP Services	IP Services	IP Services				
INTEGRATED SECURITY											
Access Control Lists											
Reflexive ACL	•										
Port ACL	•	•	•	•	•	•	•	•	EI only		
Time-based ACL	•	•	•	•	•	•	•	•	•		
Router ACL	•	•	•	•	•	•	•				
VLAN ACL	•	•	•	•	•	•	•				
VACL with Redirect/Capture/ Logging of Denied Traffic	•	•*	•*	Capture and Logging	Capture and Logging	Capture and Logging	Capture and Logging				
Context-based Access Control	•										
H/W-based Access Control Entry (ACE) Counters	•										
Order-dependent ACL Merge	•										
Dedicated Hardware Resources for Security ACLs	•	•	•								
ACL Scalability (ACE entries)	32,000	32,000	32,000	2000	2000	2000	2000	512	300 ACP—EI only		
Attack Mitigation											
Flexible Packet Matching	•										
Control Plane Policing (Multiple CPU Rate Limiters)	•	•	•								
IP Source Guard											
DHCP Snooping/Option 82	•	•	•	•	•	•	•	•	•	•	

12

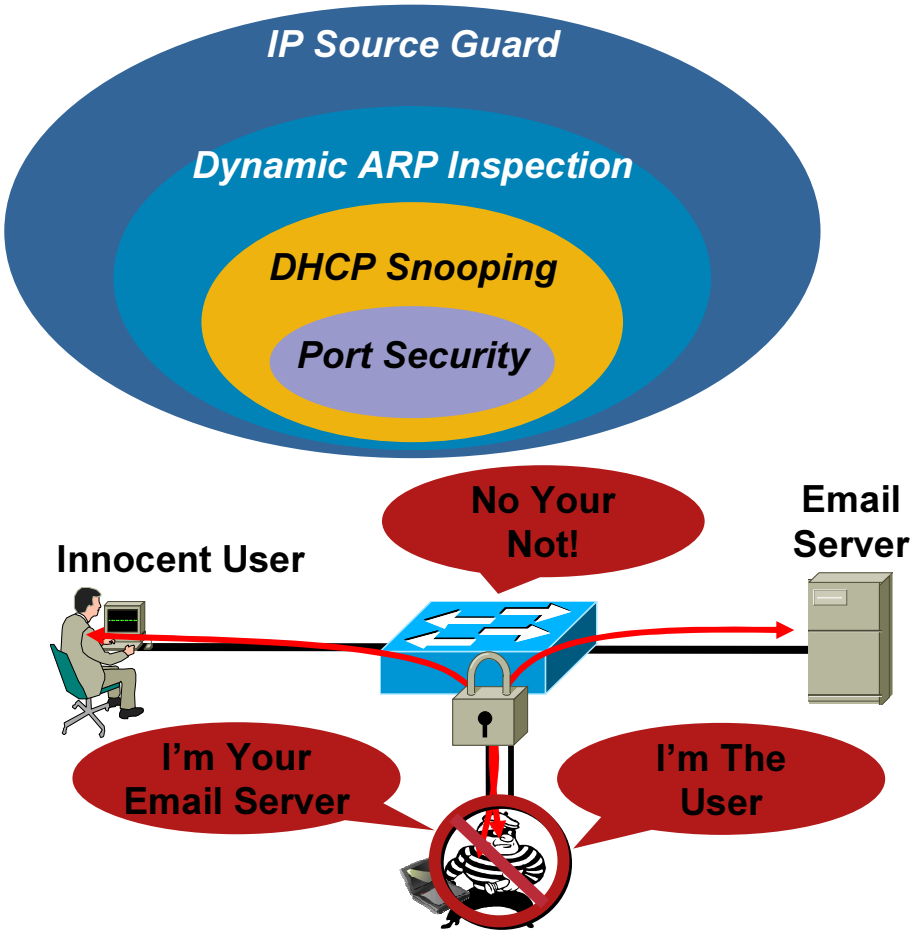
*As part of IP ACL in VLAN MAP but not for the entire VACL.

13

Demo – DHCP snooping



Otras herramientas para prevencion de ataques en L2



Attack	Catalyst Feature
MAC Address Flooding	Port Security
DHCP Rogue Server for Default Gateway Interception	DHCP Snooping
ARP Spoofing or ARP Poisoning	Dynamic ARP Inspection
IP Spoofing	IP Source Guard

Aplicando Seguridad en routing

Desafio:
Inestabilidad en redes WAN

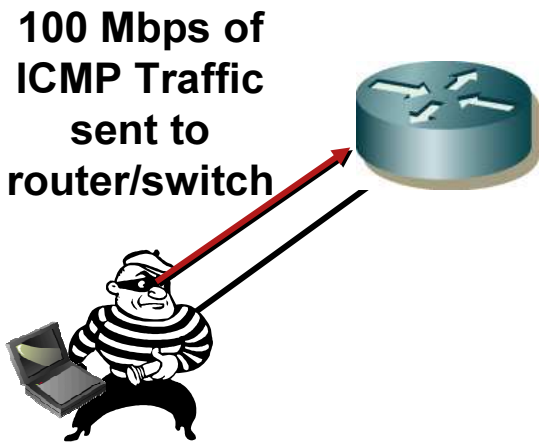
Experimental Study of Internet Stability and Backbone Failures *

Craig Labovitz, Abha Ahuja, Farnam Jahanian
University of Michigan
Department of Electrical Engineering and Computer Science
1301 Beal Ave.
Ann Arbor, Michigan 48109-2122
{labovit, ahuja, farnam}@umich.edu

Outage Category	Number of Occurrences	Percentage
Maintenance	272	16.2
Power Outage	270	16
Fiber Cut/Circuit/Carrier Problem	261	15.3
Unreachable	215	12.6
Hardware problem	154	9
Interface down	105	6.2
Routing Problems	104	6.1
Miscellaneous	86	5.9
Unknown/Undetermined/No problem	32	5.6
Congestion/Sluggish	65	4.6
Malicious Attack	26	1.5
Software problem	23	1.3

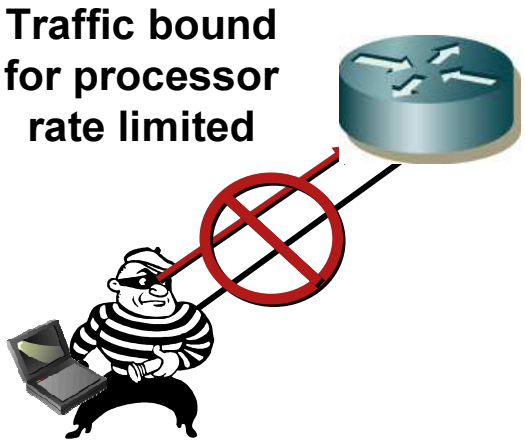
(a) Failure Categories

Control Plane Policying



Problem:

- **DoS Attacks at infrastructure devices generate rogue IP traffic streams destined to the Route Processor at very high data rates.**
- **Affects routing protocols, STP updates, which in turn severely affect network stability**



Solution:

Route Processor Rate Limiting provides hardware-based mechanism for limiting traffic destined to RP, including:

Ingress/Egress ACLs

CEF Receive and Glean

ICMP Redirects/Unreachable

TTL Failure

CEF No Route

RPF Failure

VACL Logging

CoPP Deployment Example

Undesirable -- Explicitly “bad” or “malicious” traffic to be denied access to the RP

- ip fragments, slammer, etc.
- “police” action is “drop/drop”
- This policy comes first!

Routing -- Traffic crucial to the operation of the network

- E.g. BGP, OSPF (remember, ISIS is not ‘classifiable’ today), PIM, LDP, APS, etc.
- “police” action is “transmit/transmit”

Management -- Traffic necessary for day-to-day operations

- E.g. ssh, (telnet :<(, snmp, ftp, ntp, dns, arp, etc.
- “police” action is “transmit/transmit” (medium rate)

Normal -- Traffic expected but not essential for network operations

- E.g. icmp, udp >10000, etc.
- “police” action is “transmit/drop” (low-ish rate)

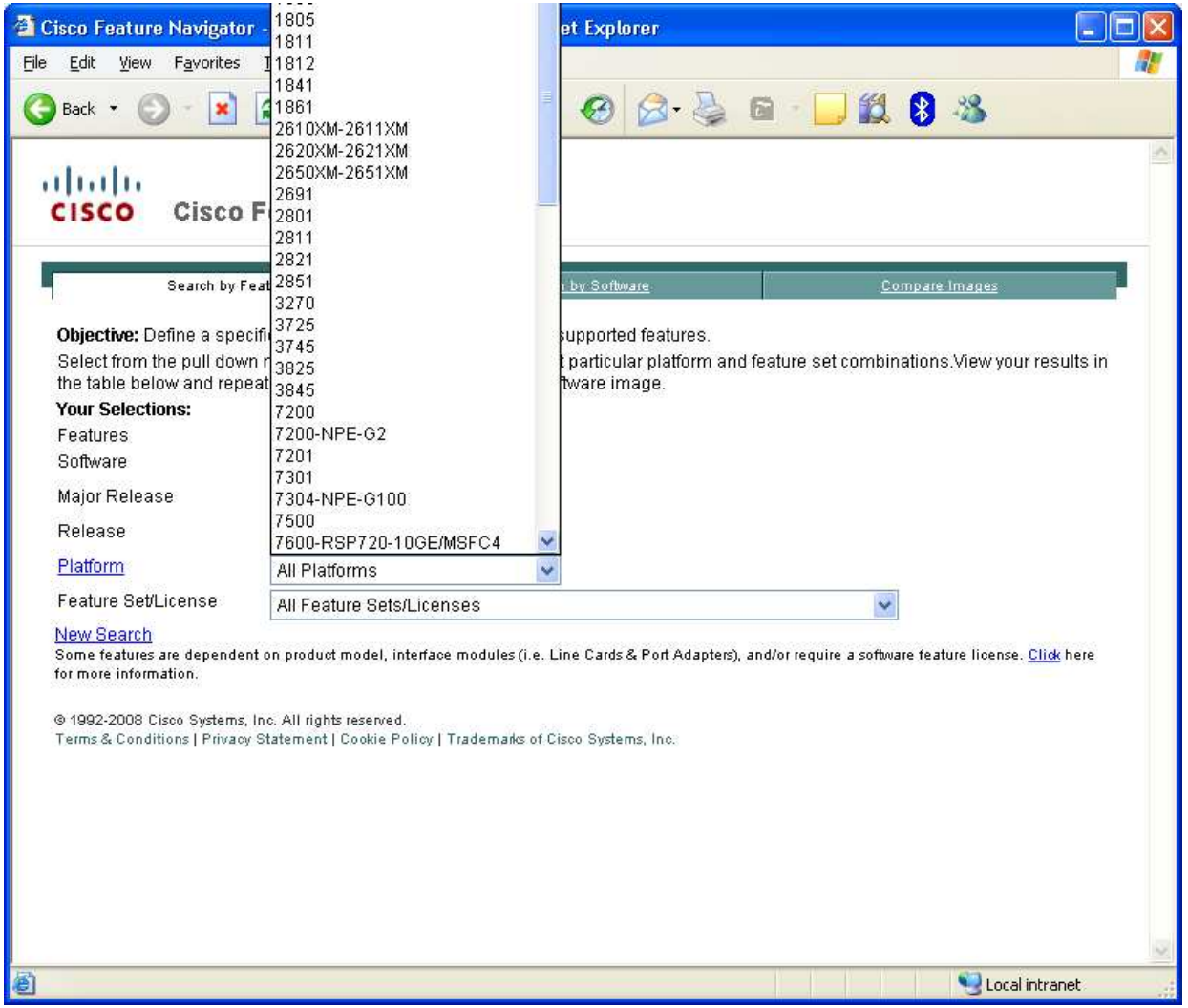
Remaining IP -- All remaining IP traffic destined to RP that has not been identified

- “permit ip any any”
- “police” action is “transmit/drop” (low-ish rate)

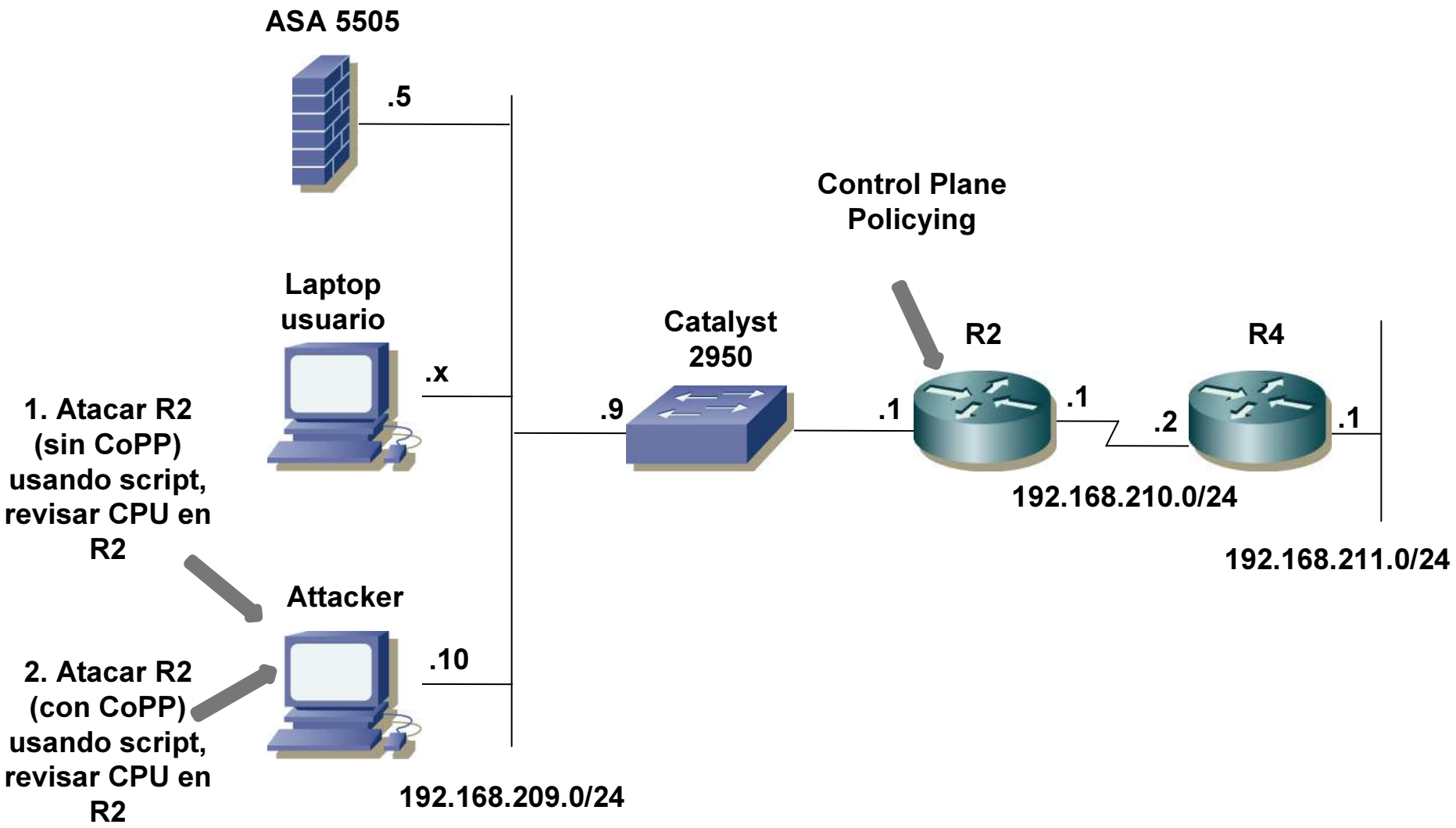
Class-default – “the rest”

- ISIS, ARP (if not matched above), CDP, etc.
- “police” action MUST BE “transmit/transmit”

Disponibilidad – Control Plane Policying



Demo – Control Plane Policying



Gradual Start with CoPP

start with:

"New" Deployment Control Plane Policing Service Policy			
Traffic Class	**Rate (bps)**	**Conform Action**	**Exceed Action**
Routing	N/A	Transmit	Transmit
Management	50,000	Transmit	Transmit
Normal	15,000	Transmit	Transmit
Undesirable	8,000	Drop	Drop
Remaining_IP	8,000	Transmit	Transmit
class-default	8,000	Transmit	Transmit

full deployment:

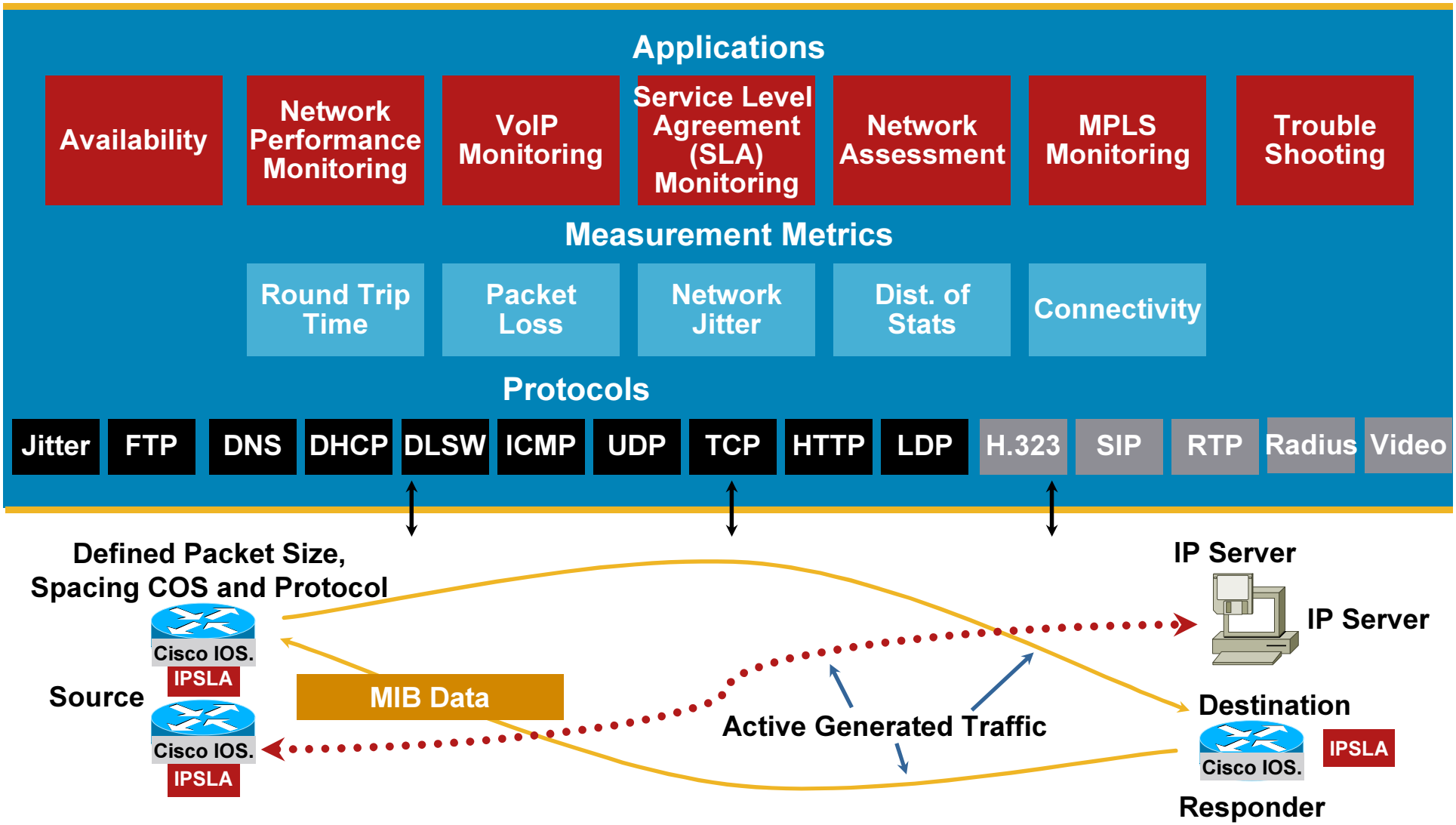
"Mature" Deployment Control Plane Policing Service Policy			
Traffic Class	**Rate (bps)**	**Conform Action**	**Exceed Action**
Routing	N/A	Transmit	Transmit
Management	50,000	Transmit	Drop
Normal	15,000	Transmit	Drop
Undesirable	8,000	Drop	Drop
Remaining_IP	8,000	Drop	Drop
class-default	8,000	Transmit	Transmit

rates are examples only; depend on your set-up

Otras funcionalidades de seguridad en Routing

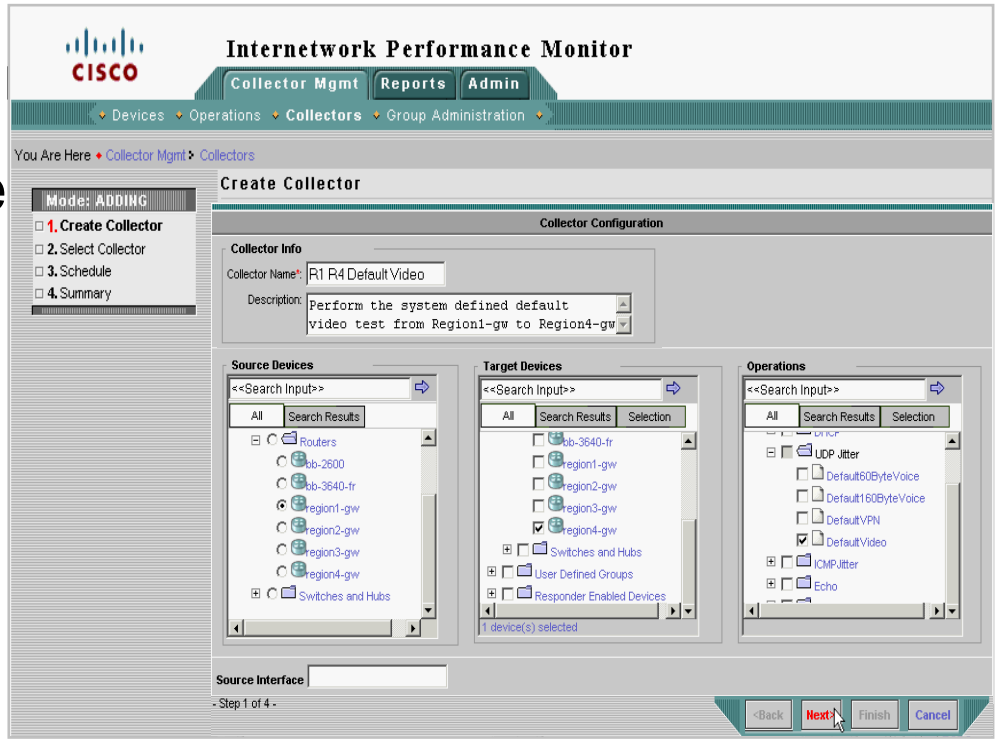
- Routing - filtros de entrada (*)
- IOS Firewall (*)
- Routing - autenticacion
- IOS IPS
- TCP Intercept
- Unicast Reverse Path Forwarding (clientes full BGP)
- Policy Based Routing (ej: blackholing)
- NBAR – Network Based Application Recognition
- ……

Desafio:
Gestión y visibilidad de SLAs – IOS IP SLA

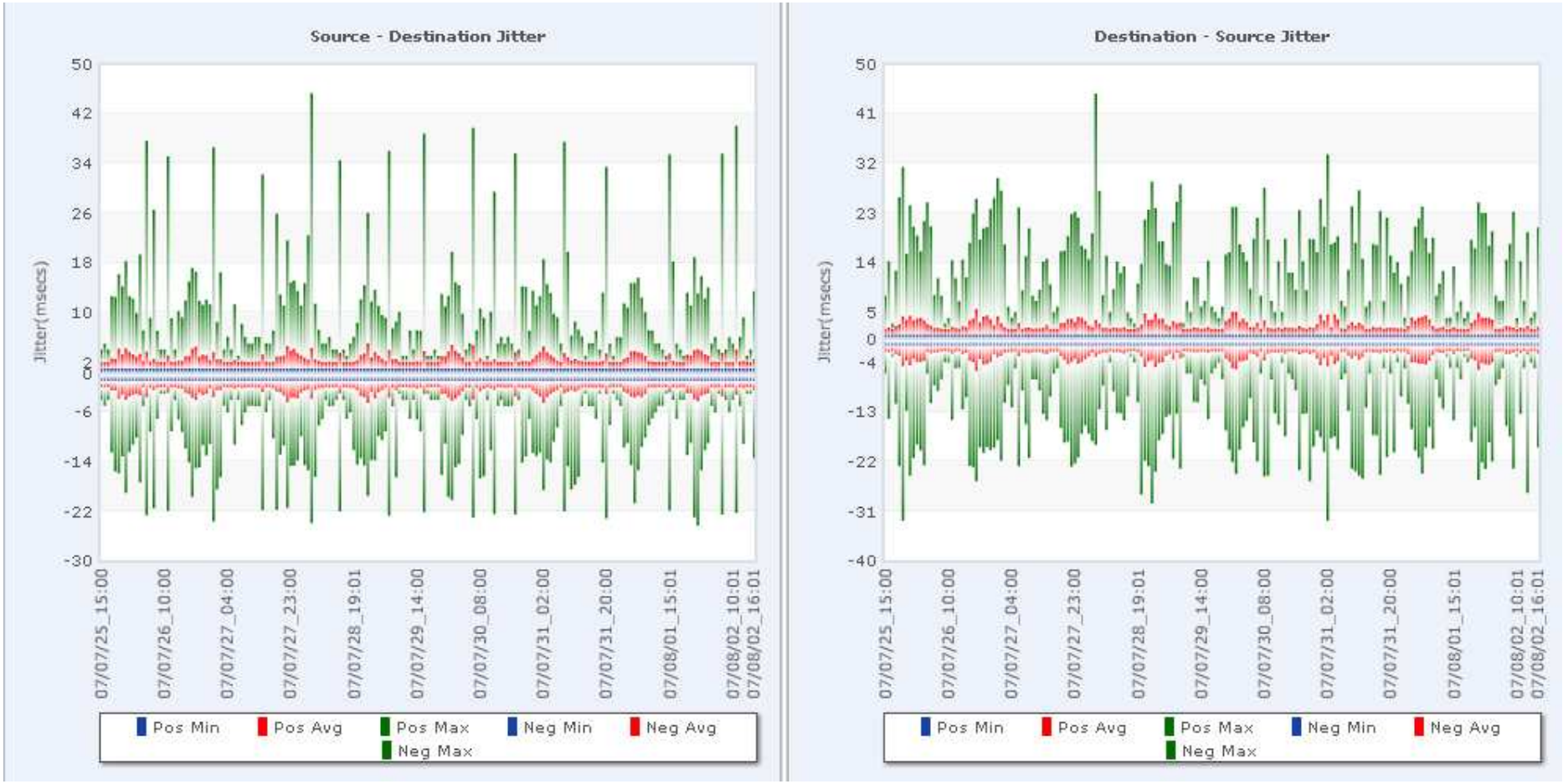


LMS - Internetwork Performance Monitor Collector

- Supports a single wizard-based approach to create multiple collectors at one step.
- Multiple collectors can be created by choosing more than one target and operations.
- For “m” target devices and “
- m*n collectors will be create

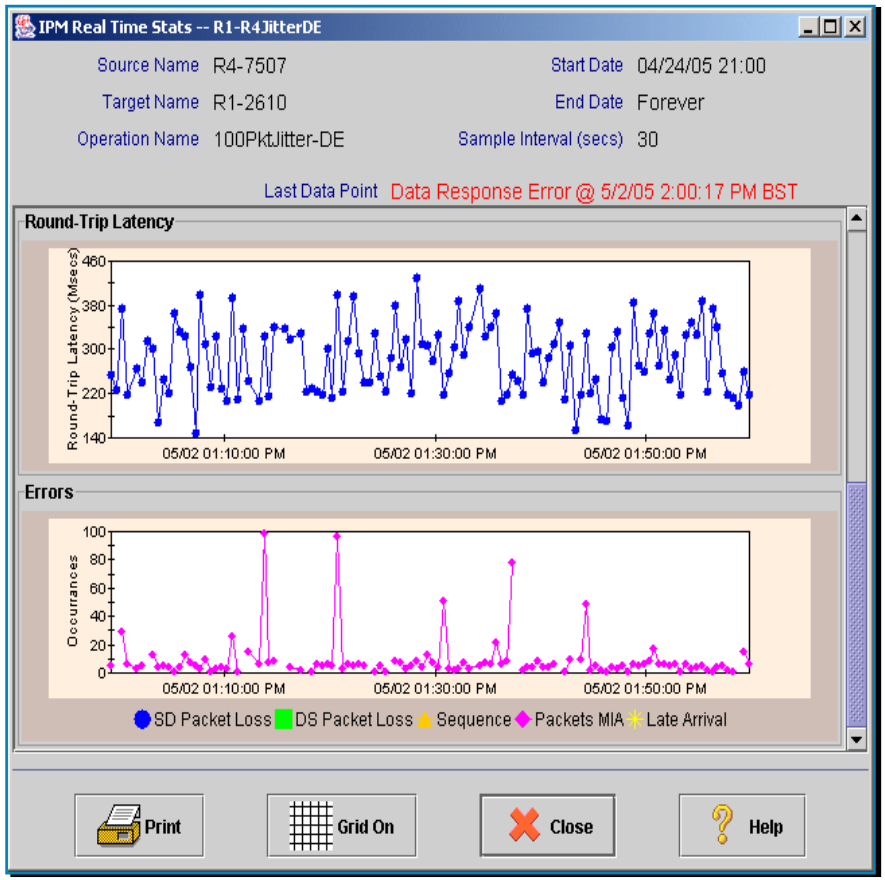


IPM - Rich Graphs – Hourly Jitter Graphs



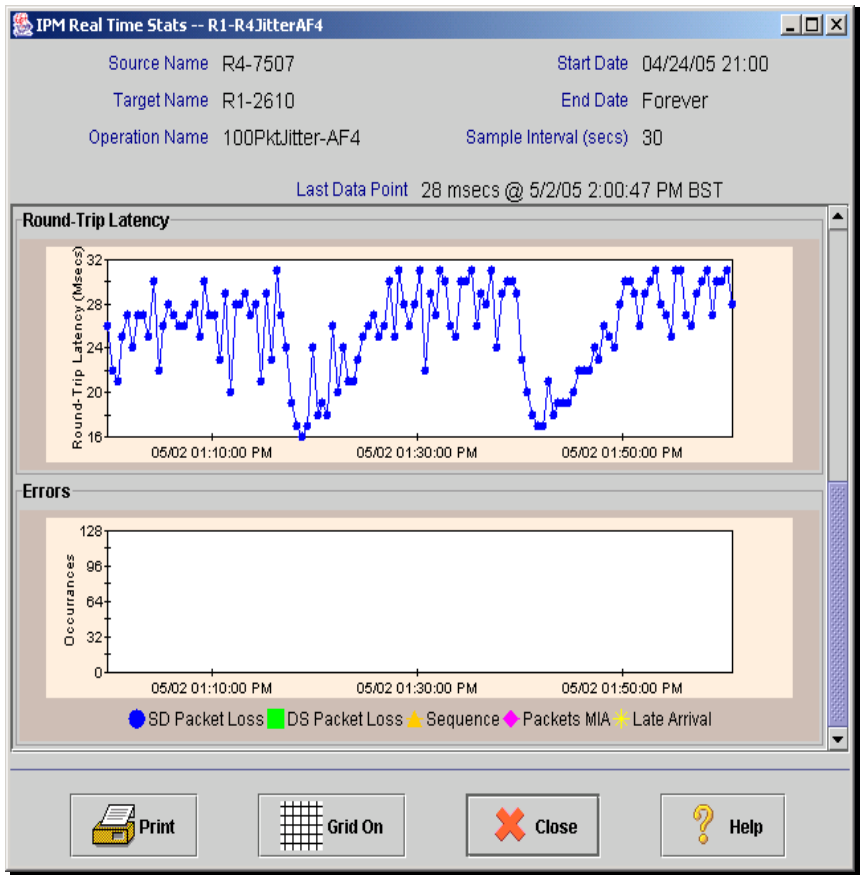
IP SLAs and IPM

IP SLAs Jitter BE



Response 200–400ms
Excessive Packet Loss

IP SLAs Jitter AF4

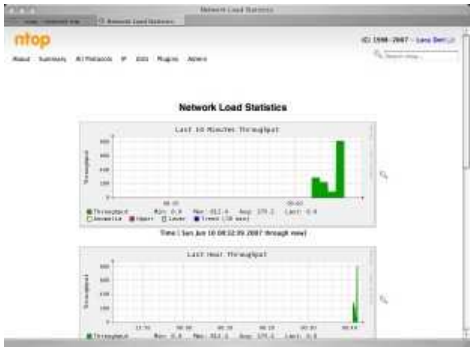


Response 20–30ms
No Packet Loss

Visibilidad de red – alternativas Open Source

- Demo ntop

  Netflow & sniffing



Conclusiones

- Herramientas del tipo “script-kiddie” existentes constituyen una amenaza, no se requiere expertise
- Las tecnologías presentadas permiten posicionar mejor el valor de la infraestructura Cisco de routing y switching
- Traducible en propuestas de servicios de optimización de red a clientes existentes – extensa base instalada
- Herramienta competitiva!