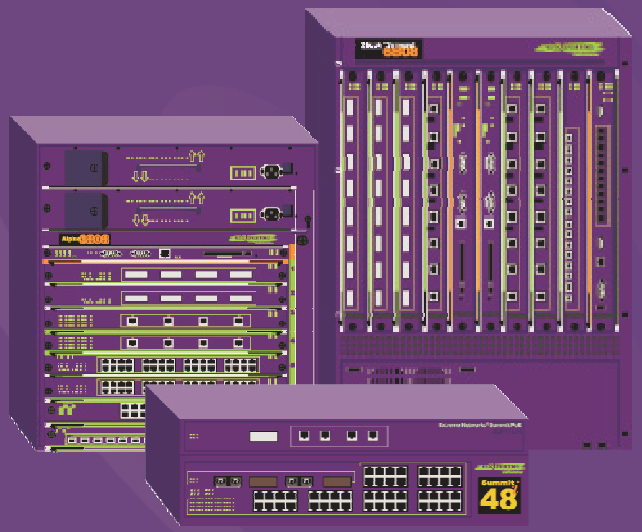
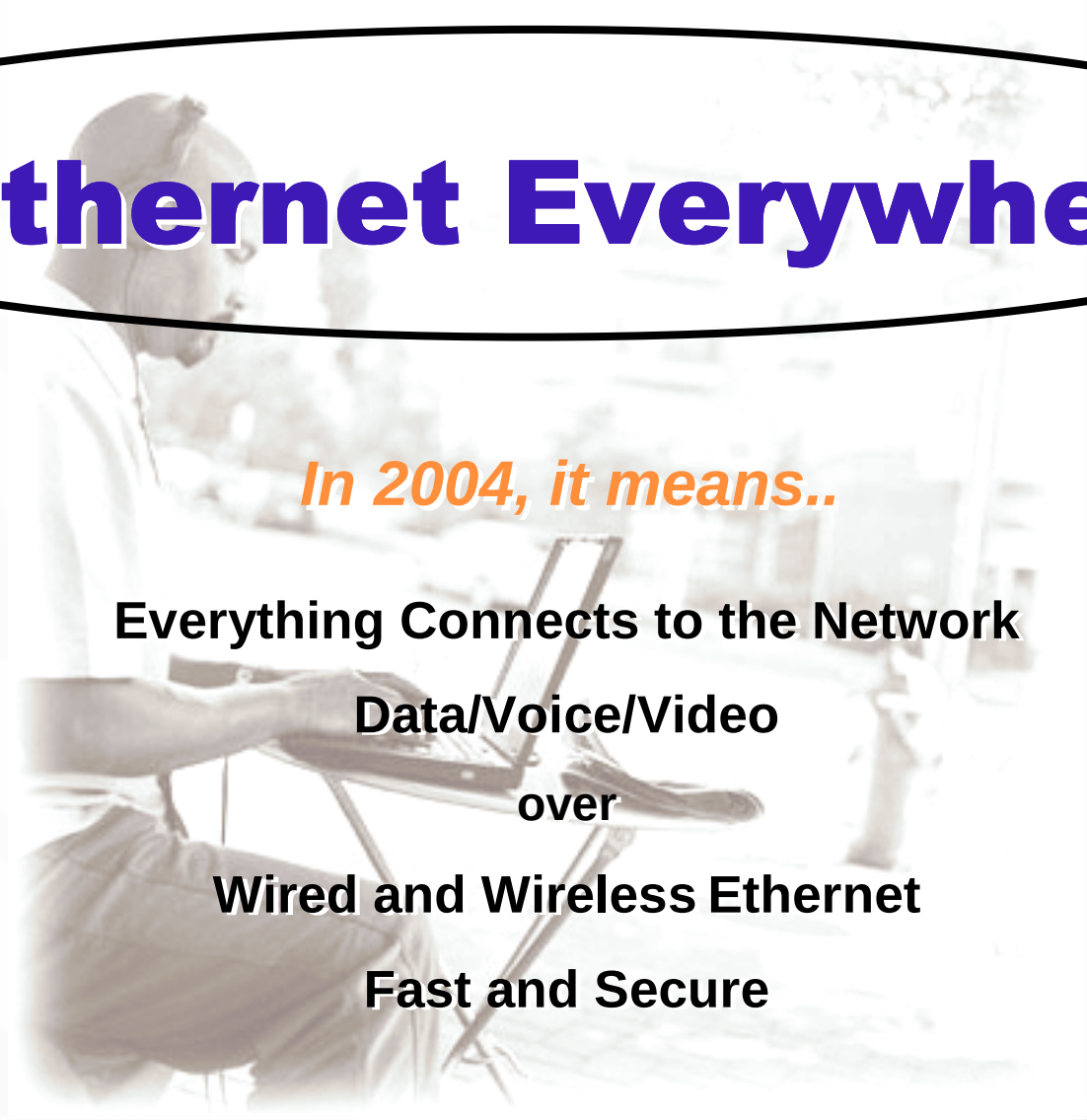
Tecnologias e Tendências nas Redes Metro Ethernet



Renier Souza
SE Manager - South America
rsouza@extremenetworks.com
Office : +55(11) 5185-2760

Our Vision Since Day 1

“Ethernet Everywhere”



In 2004, it means..

Everything Connects to the Network

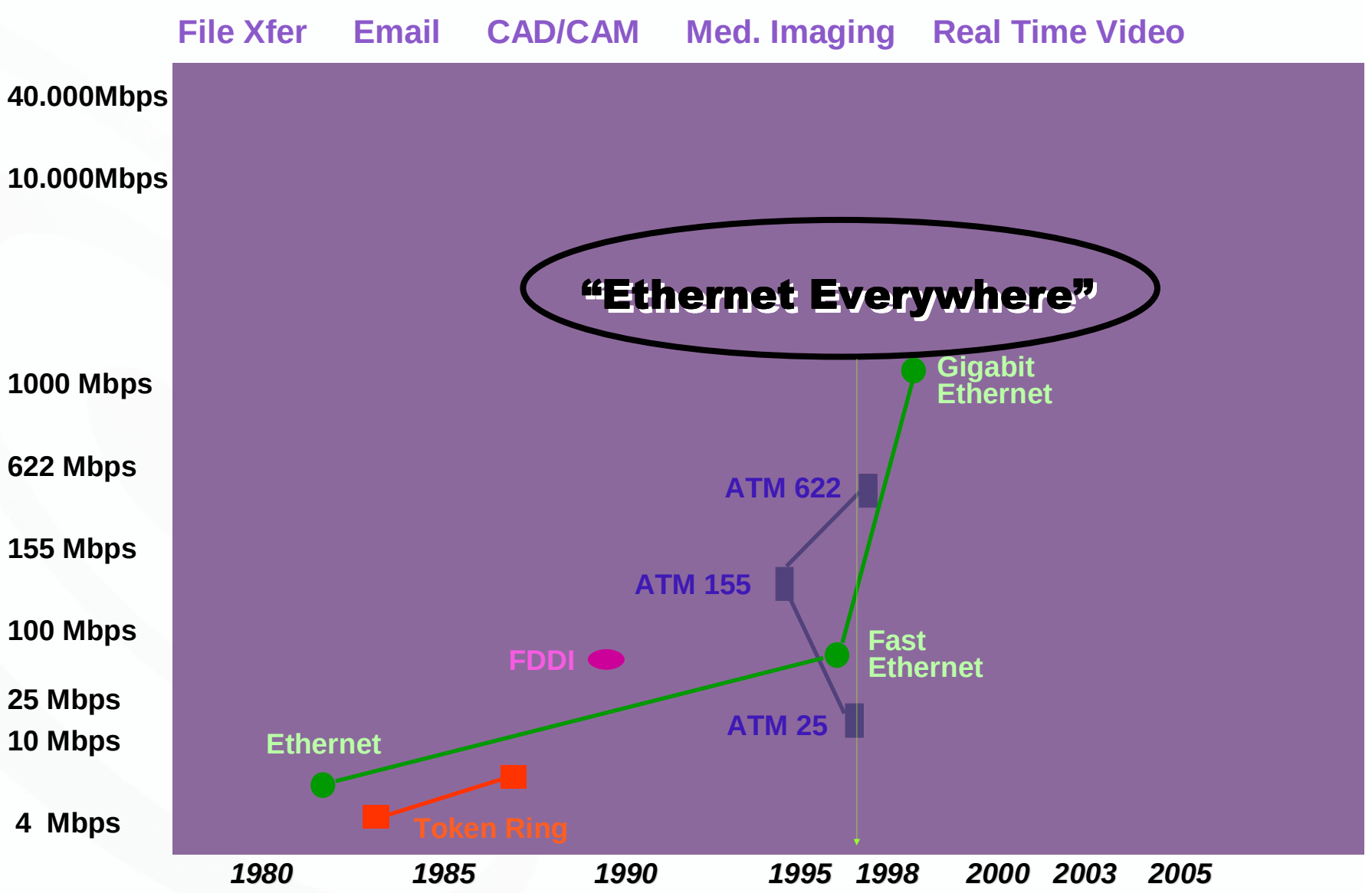
Data/Voice/Video

over

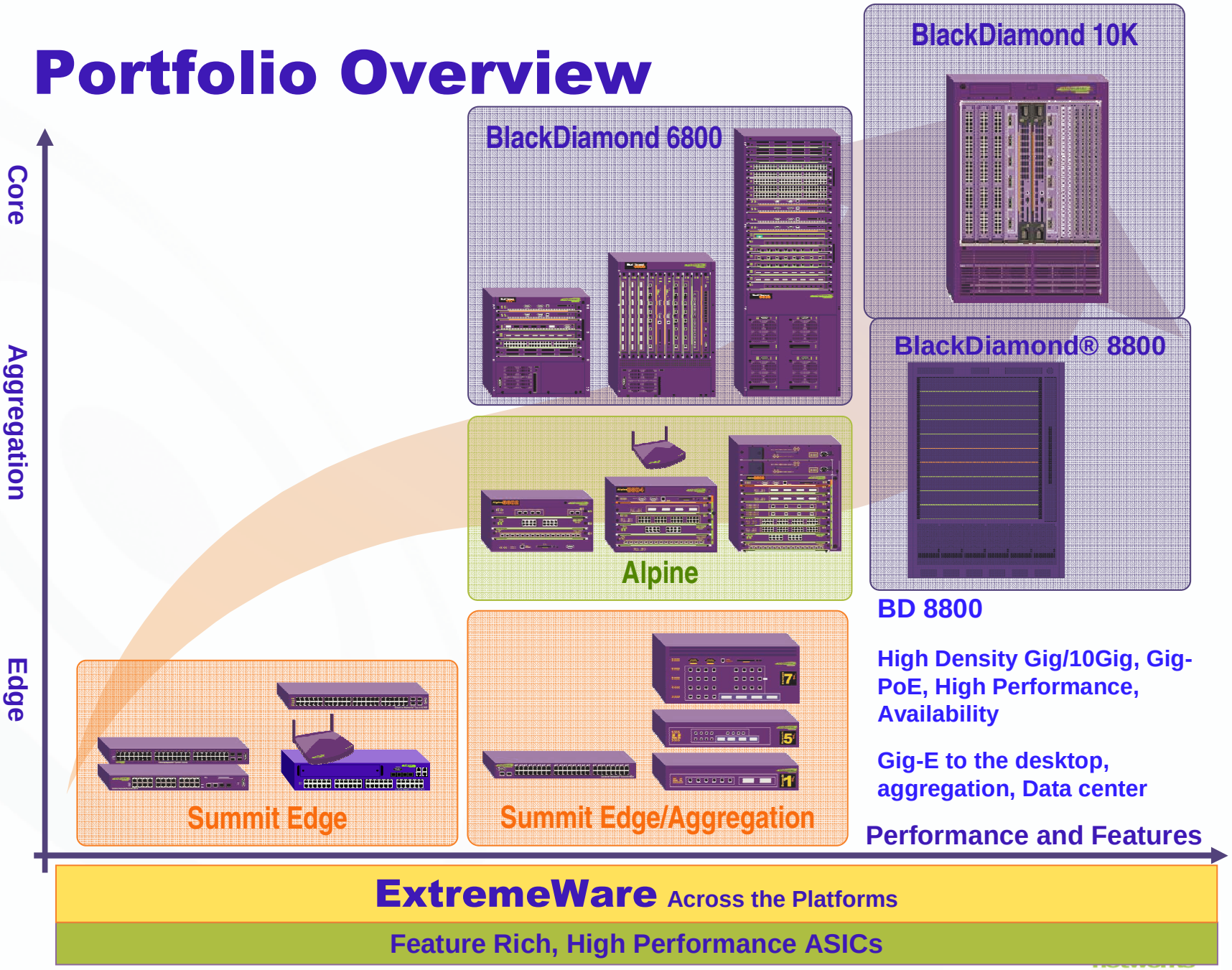
Wired and Wireless Ethernet

Fast and Secure

Para onde vão as redes !!



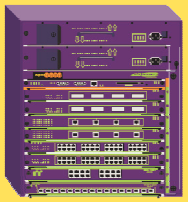
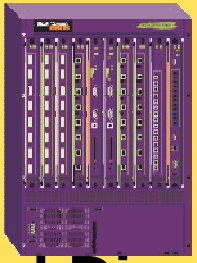
Portfolio Overview



Equipamentos

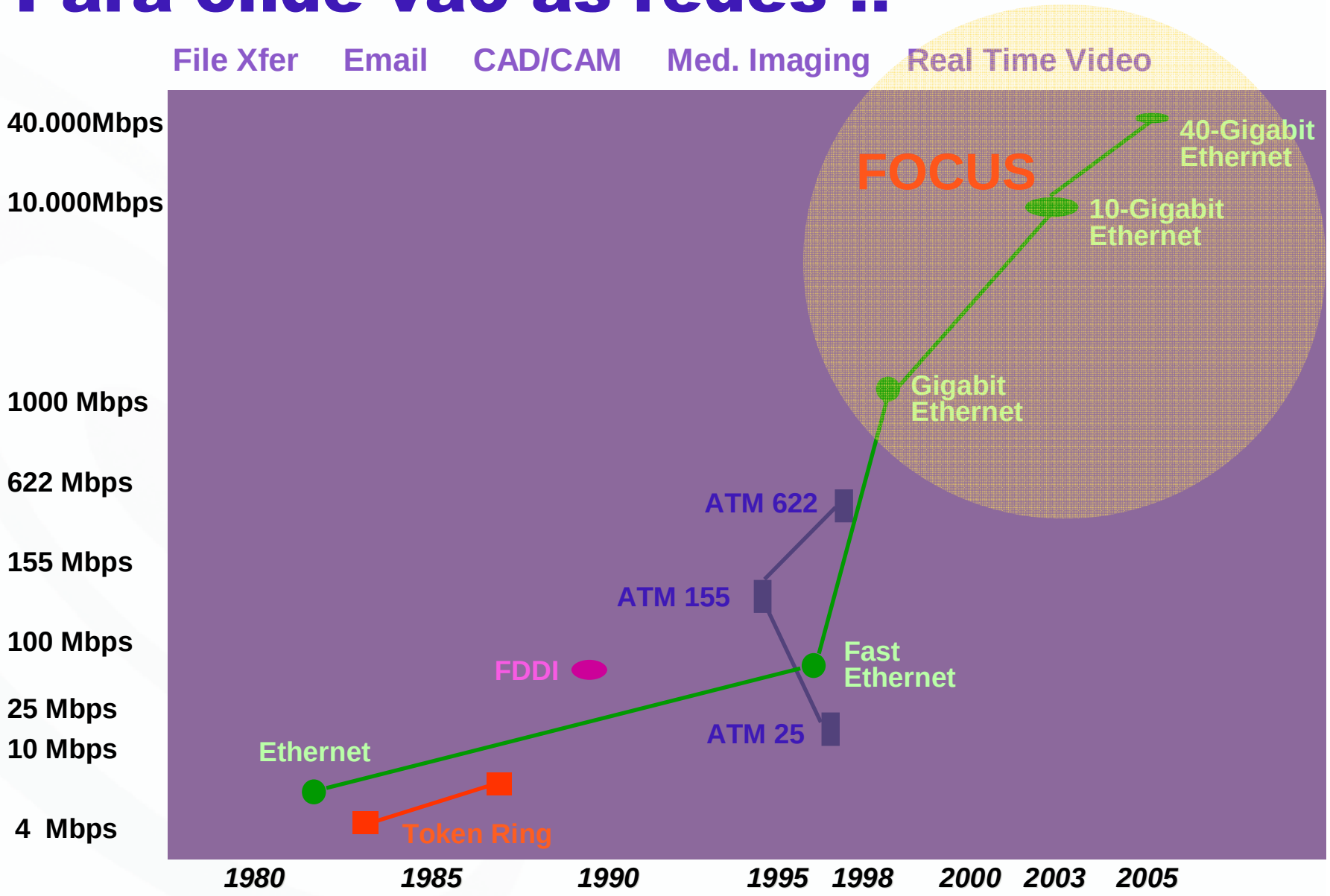
- Que tal um Switch com :
  - Alta performance / WireSpeed ?
  - Server Load Balance ?
  - Full IP : OSPF, BGP, ISIS, Multicast ?
  - Suporte a WireSpeed ACLs ?
  - Suporte a Web Cache Redirection
  - Suporte a ataques DOS
  - LPM !!!!!!

Nós já temos isto !!! Série “i”


Alpine, BlackDiamond, Summit

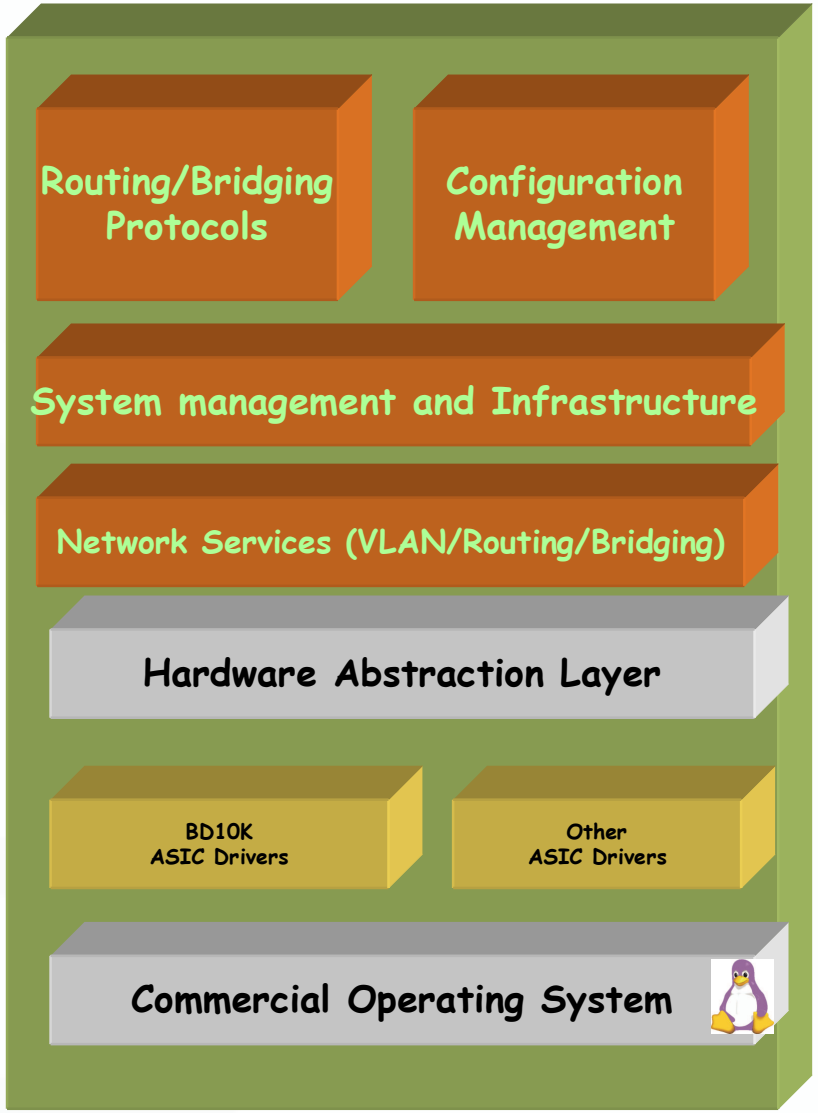
Para onde vão as redes !!



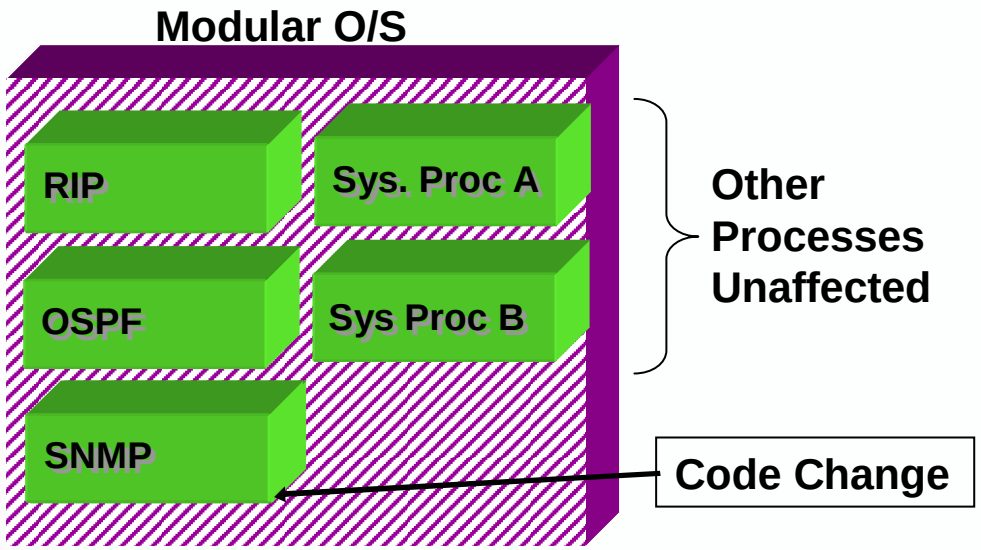
What's Really Needed

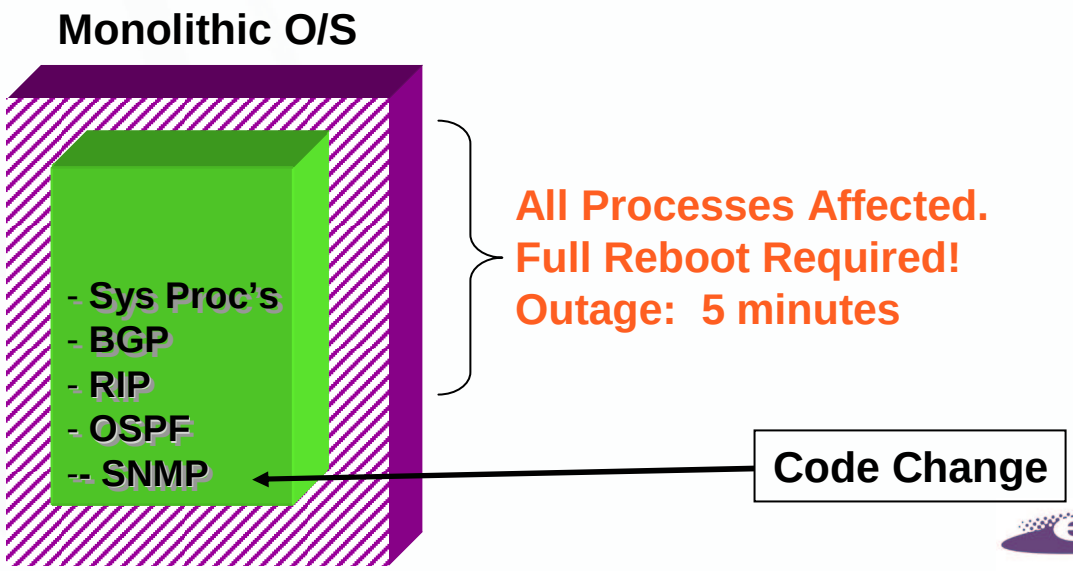
- Não se trata somente de portas 10Gig
  - Example: flow based architectures não vão escalar com 10 vezes o número de usuários
- É necessário inovar em Múltiplas dimensões !!!

Modular, Open Operating System

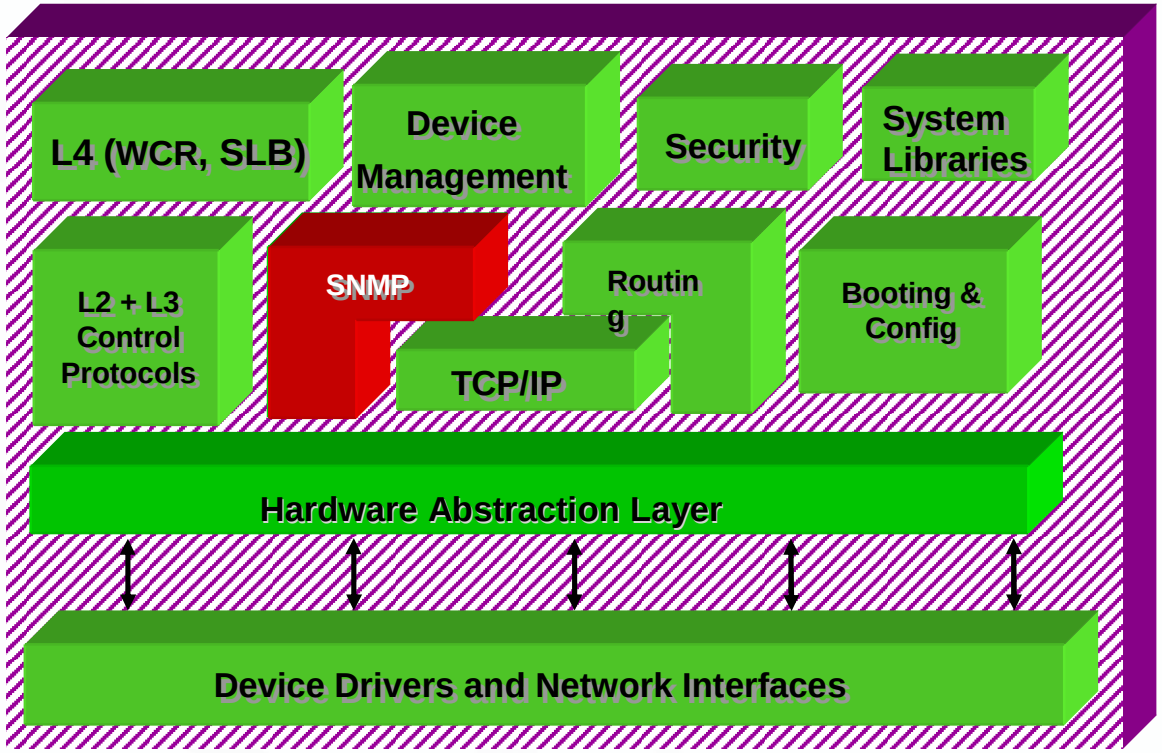


Modular vs. Monolithic O/S





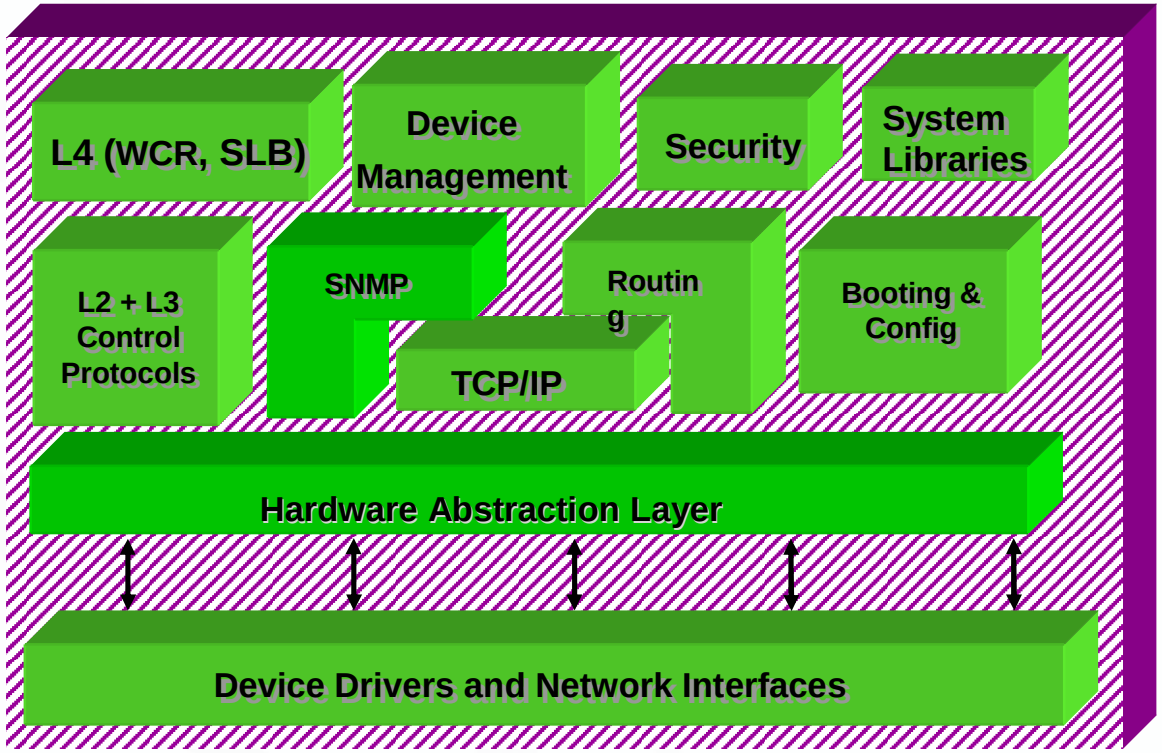
Process Restart



- (1) SNMP process gets into infinite loop.

- PROCESS RESTART:
  - Processes restart WITHOUT rebooting the switch.

Process Restart



- (1) SNMP process gets into infinite loop.
- (2) Multithreaded O/S continues to service other processes.
- (3) Watchdog detects problem in SNMP; kills process
- (4) O/S re-starts SNMP.

- PROCESS RESTART:
  - Processes restart WITHOUT rebooting the switch.

Access Lists

- Rule Syntax

```
entry <entry-name>  {
    if {
      <match-conditions>;
    } then {
      <action>;
      <action-modifiers>;
    }
}
```

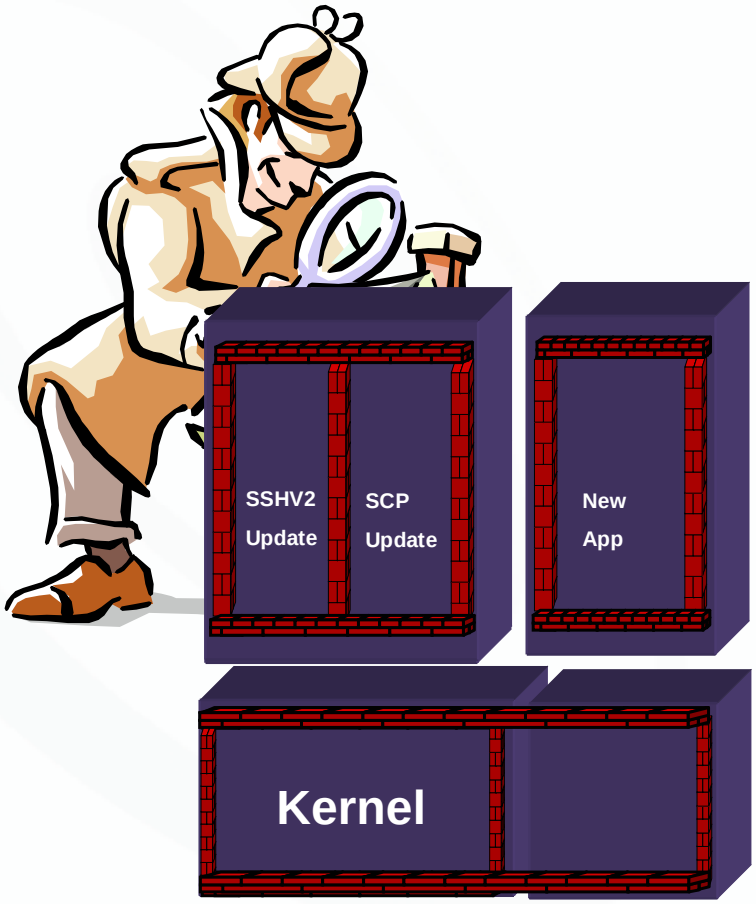
- *Match-condition*: values or fields which the packet must contain
- *Action*: what to do if a packet matches the condition(s), *accept* or *deny*
- *Action-modifier*: specifies the further actions to be taken, such as count etc.

Exemplo :

```
# ----------------------------------
#  Permitir Mac Específico
# ----------------------------------
entry ARPRenier  {
   if {
    ethernet-source-address 00:08:74:9F:2C:2A ;
     } then {
       permit;
       count pcrenier;
    }
}
# ----------------------------------
#  Permitir ARP's
# ----------------------------------
  if {
     ethernet-type 0x806;
      } then {
        permit;
        count permarp;
    }
}
# ----------------------------------
#  DENY ALL IS THE LAST
# ----------------------------------
entry default {
   if {
      }
   then {
     deny;
     count default;
```

Availability: Uptime instead of reboots

- Example using an application module consisting of multiple multithreaded processes



1) Functionality can be bundled in an application module, still in protected processes

2) Application modules can be upgraded during runtime

3) Kernel (driver) modules can be loaded during runtime

4) Application modules can be added during runtime

5) Processes are monitored and can be restarted if necessary

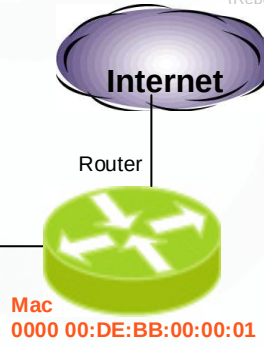
Examples

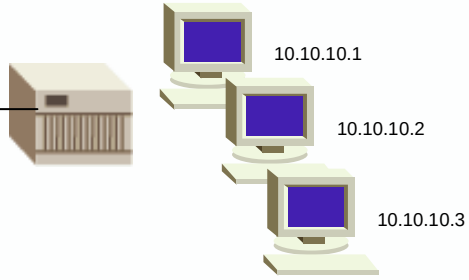
IPDA/LPM Disabled

```
Alpine3808:4 # sho iproute
Ori Destination      Gateway        Mtr Flags      VLAN       Duration
*d  1.1.1.0/24       1.1.1.1        1   U------u--- v1         0d:0h:00m:51s
*d  11.1.1.0/24      11.1.1.1       1   U------u--- Mgmt       0d:0h:00m:51s
*d  2.2.2.0/24       2.2.2.1        1   U------u--- v2         0d:0h:00m:51s
*s  10.10.10.0/24    2.2.2.2        1   UG---S-um-- v2         0d:0h:00m:51s     (Static /24 route)
*d  127.0.0.1/8      127.0.0.1      0   U-H----um-- Default    0d:0h:00m:51s
Alpine3808:5 #
```

```
Alpine3808:5 # sho ipfdb
 Dest IP Addr  TblIdx MacIdx  Flag Flow    MAC Address     VLAN Port
--------------- ------ ------  ---- ----  ----------------- ---- ----
1.1.1.1        0101.0 5FE3.0       0000 00:01:30:00:6D:00 4093 CPU
2.2.2.1        0102.0 5FE2.0       0000 00:01:30:00:6D:00 4092 CPU
2.2.2.2        0202.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2
10.10.10.1     010A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)
10.10.10.2     020A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)
10.10.10.3     030A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)
10.10.10.4     040A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)
10.10.10.5     050A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)
..
10.10.10.99    630A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)
10.10.10.100   640A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2   (Host Entry)

Total: 103 Static: 2 Dynamic: 101
IPFDB Aging time: 0 minutes
Alpine3808:6 #
Alpine3808:6 # enable ip-subnet-lookup                               (Enabling IPDA)
To be effective, system rebooting is needed
* Alpine3808:7 # reboot                                              (Reboot)
```





IPDA/LPM Enabled

```
Alpine3808:1 # sh iproute
Ori Destination      Gateway        Mtr Flags      VLAN       Duration
*d  1.1.1.0/24       1.1.1.1        1   U------u--- v1         0d:0h:00m:14s
*d  11.1.1.0/24      11.1.1.1       1   U------u--- Mgmt       0d:0h:00m:14s
*d  2.2.2.0/24       2.2.2.1        1   U------u--- v2         0d:0h:00m:14s
*s  10.10.10.0/24    2.2.2.2        1   UG---S-um-- v2         0d:0h:00m:14s
*d  127.0.0.1/8      127.0.0.1      0   U-H----um-- Default    0d:0h:00m:14s
Alpine3808:2 #
```

```
Alpine3808:2 # sho ipfdb
 Dest IP Addr  TblIdx MacIdx  Flag Flow    MAC Address     VLAN Port          (No more host entries)
--------------- ------ ------  ---- ----  ----------------- ---- ----
1.1.1.1        0101.0 5FE3.0       0000 00:01:30:00:6D:00 4093 CPU
2.2.2.1        0102.0 5FE2.0       0000 00:01:30:00:6D:00 4092 CPU
2.2.2.2        0202.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2
Total: 3 Static: 2 Dynamic: 1
IPFDB Aging time: 0 minutes
Alpine3808:3 #
Alpine3808:3 # show ip-subnet-lookup fdb
 Dest IP Addr     TblIdx  MacIdx  Flag Flow    MAC Address     VLAN Port
------------------ ------- ------  ---- ----  ----------------- ---- ----
10.10.10.0     /24 1000A.0 38B1.0       0000 00:DE:BB:00:00:01 4092 3:2     (IPDA HW entry)
Total number of entries = 1
IPFDB SUBNET Lookup Maskbits: [24]                                          (Static Subnet mask)
```

Network Monitoring Problem

- Existing Traffic Monitoring Techniques:

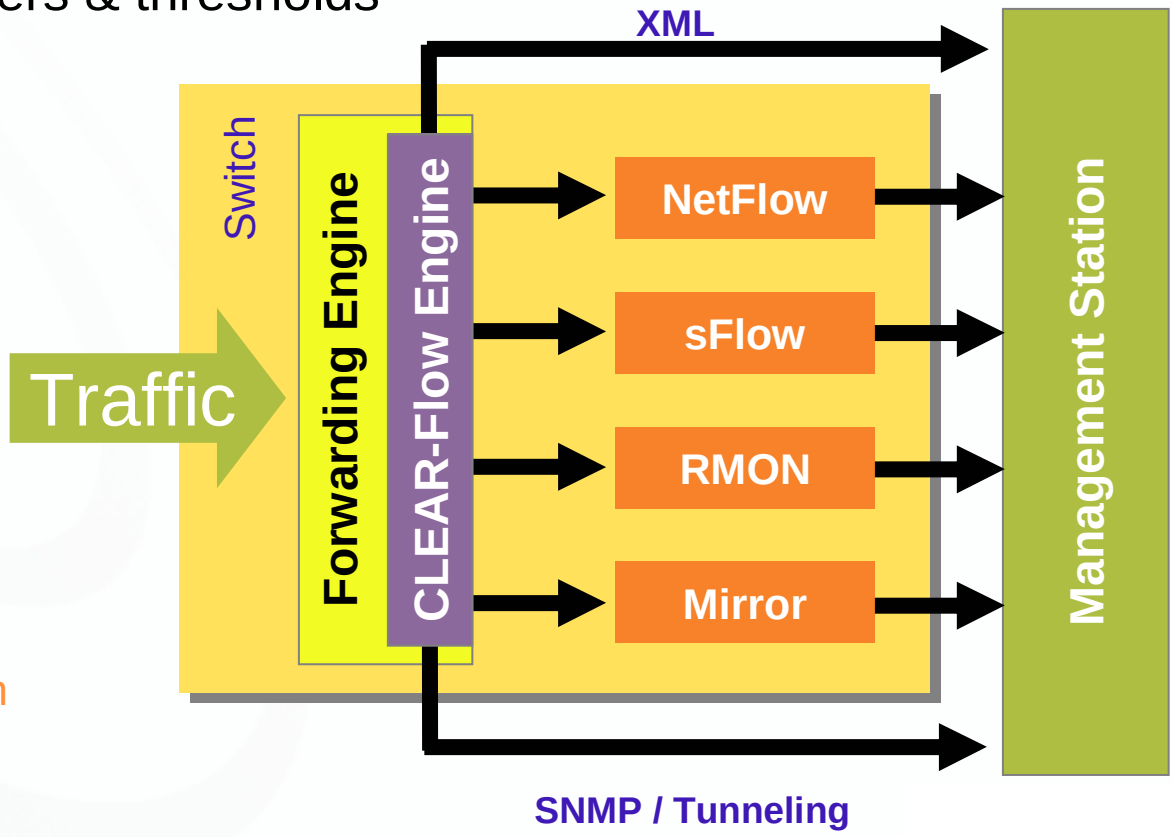
Technology	How it operates
Port Mirroring	Sends data to external capture system
RMON	Counts packets
sFlow	Looks at 1 packet a second (statistical)
NetFlow	Accumulates flow-based accounting data

- Nenhuma delas é efetiva para análise detalhada de todo o tráfego.
- Tudo é feito em CPU !

extreme networks

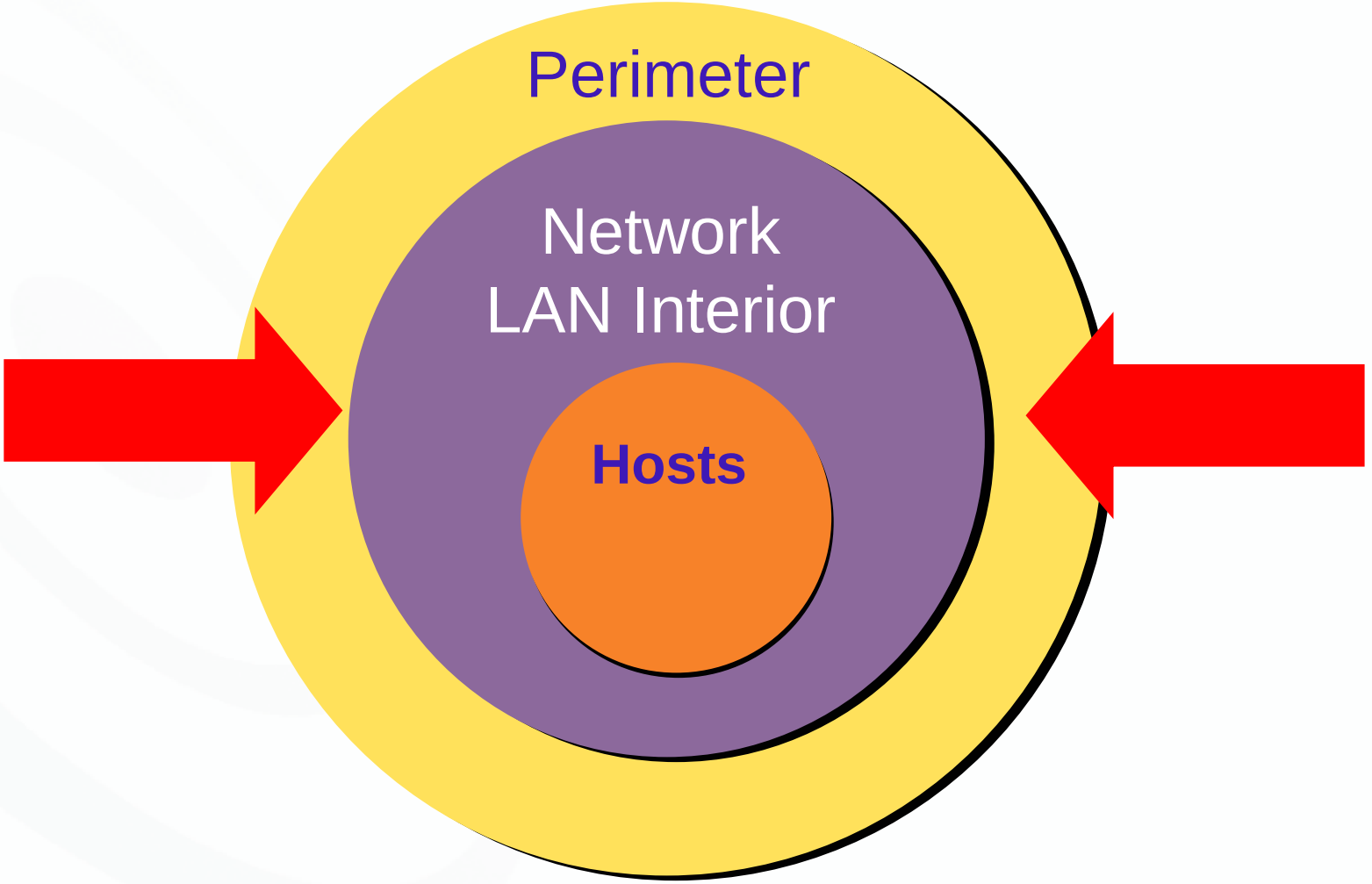
Solution : Traffic Analysis: CLEAR-Flow™

- Network pre-processes traffic before measuring
- Network can pinpoint anomalies
  - Counters & thresholds

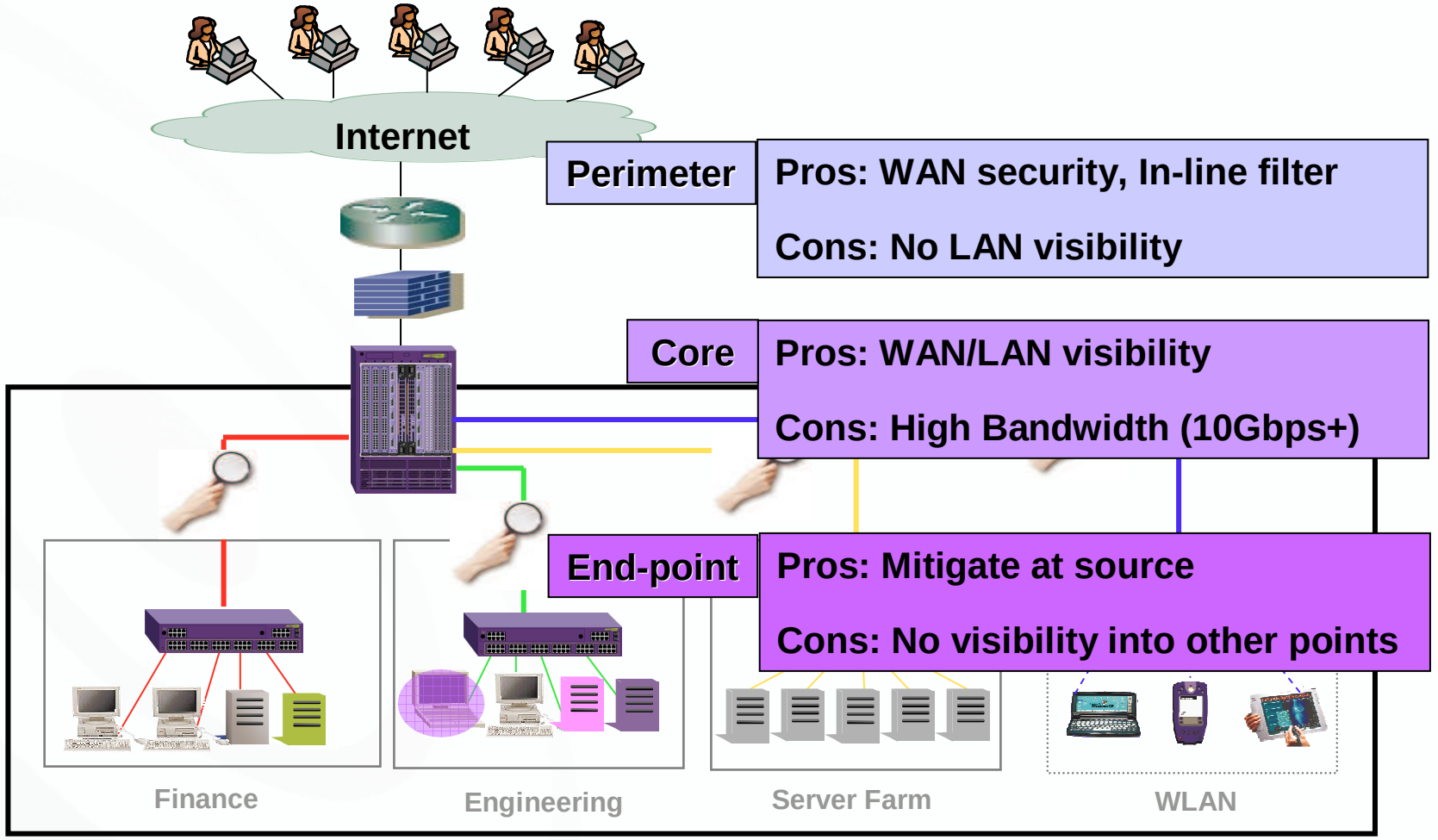


Continuous
Learning
Examination
Action &
Reporting

Traditionally Threats Enter Via Internet



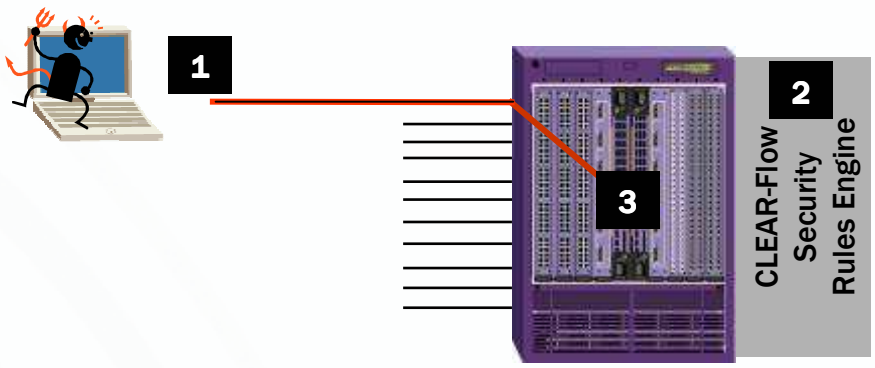
Defense-in-Depth Overview



Challenges: Multi-gigabit rates, Increased mobility, Manual mitigation

CLEAR-Flow

Instantaneous first order threat mitigation



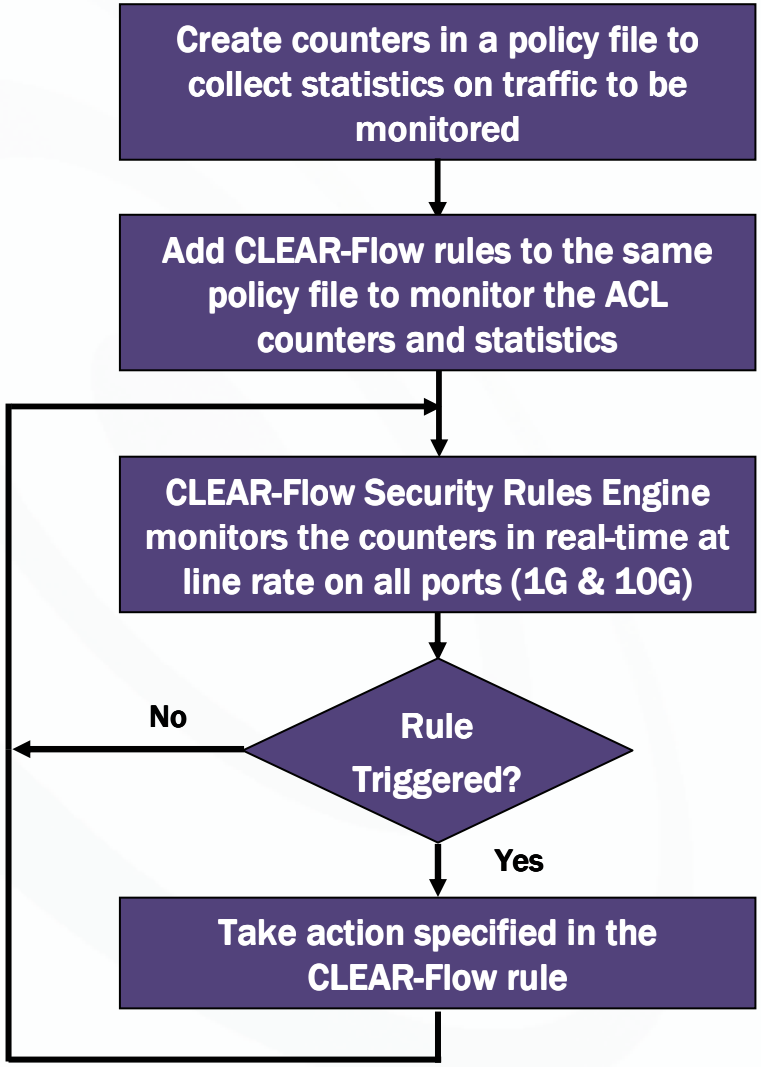
1 An infected source or malicious hacker launches an attack into the network

2 BlackDiamond 10K ACLs and CLEAR-Flow Security Rules Engine detect the attack traffic

3 CLEAR-Flow Security Rules Engine takes appropriate action to mitigate the attack

CLEAR-Flow

How the Security Rules Engine works



Sample: ACL Counters

- SYN
- SYN_ACK
- ARP_REQUEST
- ARP_RESPONSE

Sample: CLEAR-Flow Rules

Check for the following counter thresholds and detect anomalous behavior in real-time

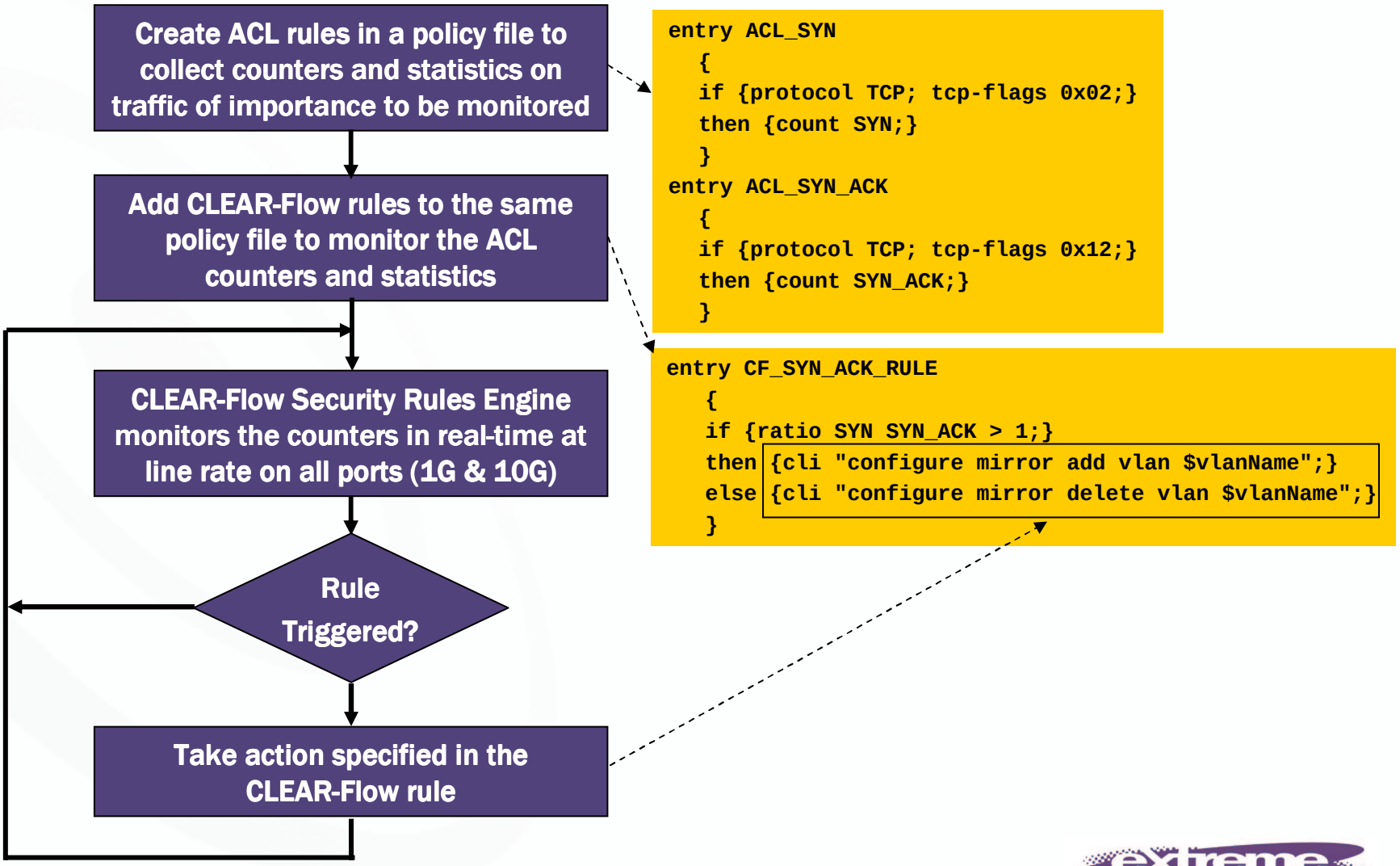
- count – Cumulative counter
- delta – The change in a cumulative counter
- ratio – Ratio of two cumulative counter values
- deltaratio – Ratio of the Change in two different counters

Sample: CLEAR-Flow Action Types

- permit <ACLRuleName>
- deny <ACLRuleName>
- qosprofile <ACLRuleName> <QPx>
- mirror add|delete <ACLRuleName>
- snmptrap <id> <message> {period}
- syslog <message> <level> {period}
- cli <clicommand>

CLEAR-Flow

A real example



CLEAR-Flow

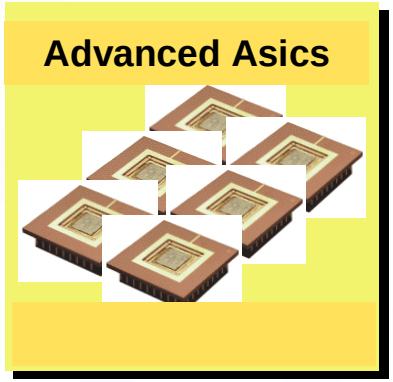
First order threats that can be mitigated

Denial of Service Attacks
Smurf attack
Ping of death
Ping sweep
Ping flood
Port sweep
TCP Flood (Syn, Syn-Ack, Ack, Fin, Xmas, Rst)
Syn attack: RFC-2827

Flood attacks against ports
Login services
RPC, NFS
File sharing
X windows
Name services
Mail services
Web services
ICMP messages

■ ■ ■

Next Generation Core



+

=

BlackDiamond 8810

Industry's First Extensible Switching Platform

BlackDiamond 10K

Summit 450-24 / 24X

IPv6 : Up and runnig

- RFC 2460, Internet Protocol, Version 6 (IPv6) Specification
- RFC 2461, Neighbor Discovery for IP Version 6, (IPv6)
- RFC 2462, IPv6 Stateless Address Auto configuration - Router Requirements
- RFC 2463, Internet Control Message Protocol (ICMPv6) for the IPv6 Specification
- RFC 2466, MIB for ICMPv6
- RFC 1981, Path MTU Discovery for IPv6, August 1996 - Router requirements
- RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture
- RFC 3587, Global Unicast Address Format
- RFC 2464, Transmission of IPv6 Packets over Ethernet Networks
- RFC 2710, IPv6 Multicast Listener Discovery v1 (MLDv1) Protocol
- RFC 3810, IPv6 Multicast Listener Discovery v2 (MLDv2) Protocol
- RFC 2740, OSPF for IPv6
- RFC 2080, RIPng
- RFC 2893, Configured Tunnels
- RFC 3056, 6to4
- Static Unicast routes for IPv6
- Telnet over IPv6 transport
- SSH-2 over IPv6 transport
- Ping over IPv6 transport
- Traceroute over IPv6 transport

Advanced, Aggregation: Summit X450-24x, Summit X450-24t

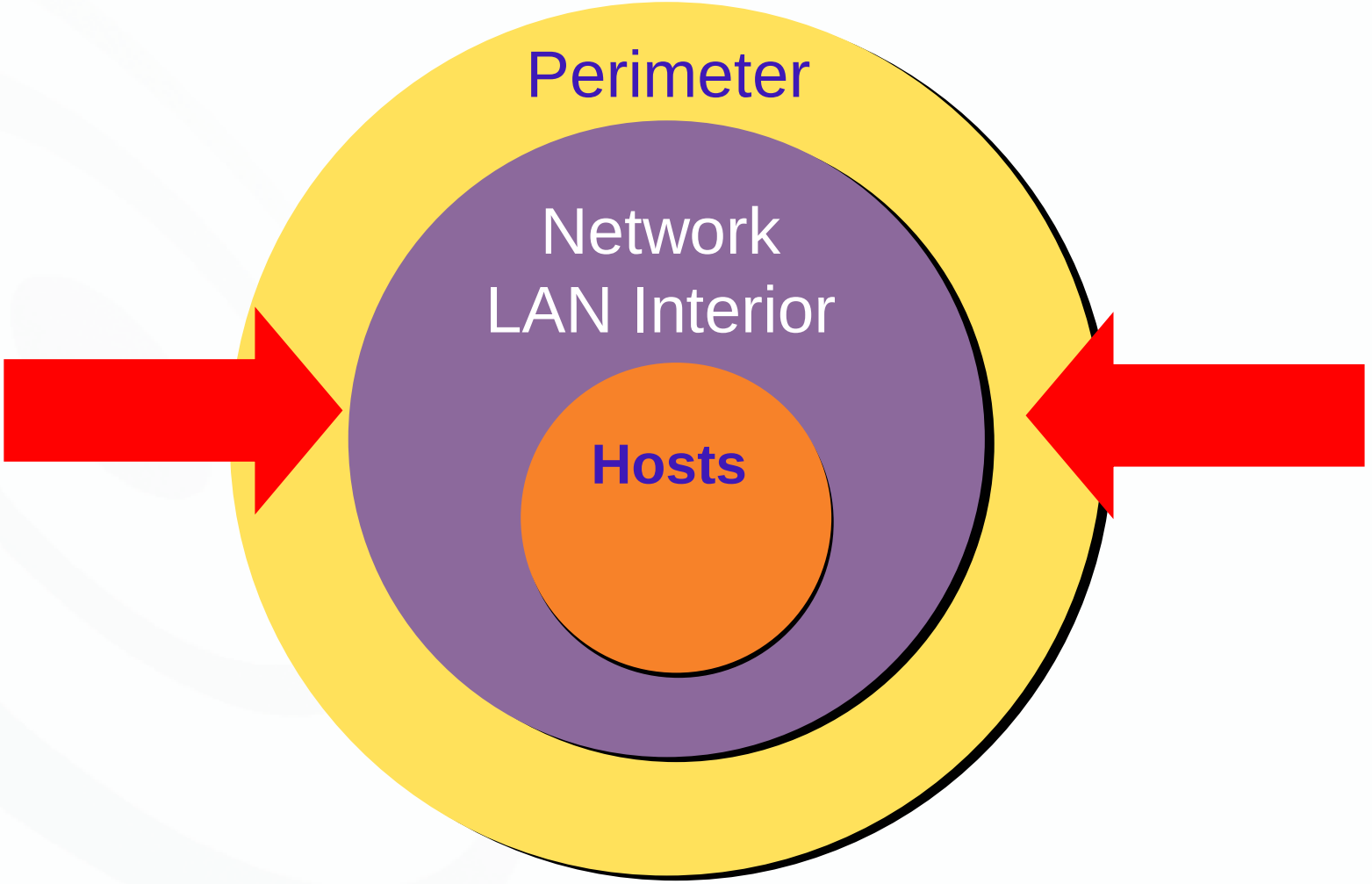
Summit X450-24x:

Summit X450-24t

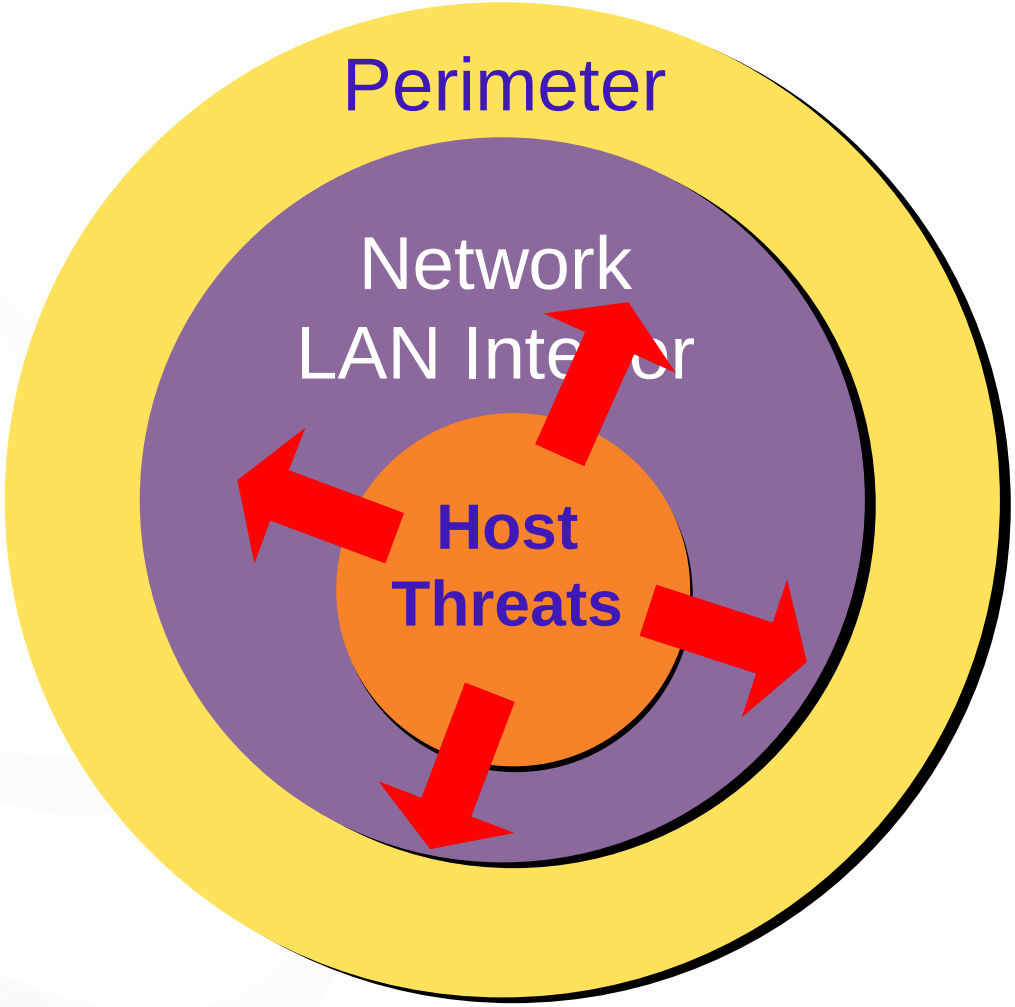
Rear

- Summit X450-24x - Fiber (SFP) aggregation switch
- Summit X450-24t - 10/100/1000Base-T advanced switch
- Option slot for XEN card for dual 10-Gigabit uplinks
- XOS modular operating system
  - Advanced Edge license bundled
  - Option Core license (BGP/IPV6)

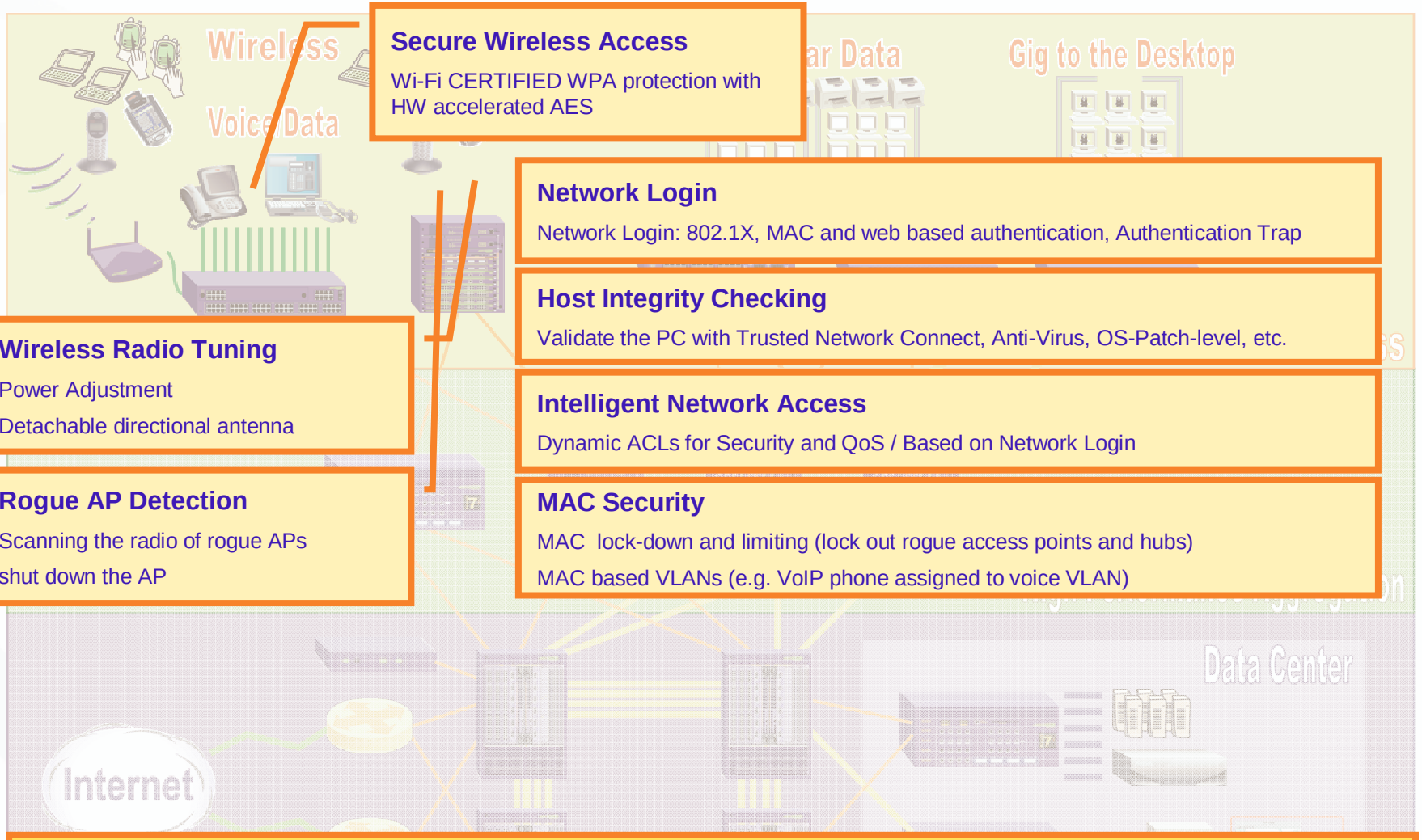
Traditionally Threats Enter Via Internet



Now threats are appearing on the inside



Security ~ Secure Unified Access ~



Secure Wireless Access

Wi-Fi CERTIFIED WPA protection with HW accelerated AES

Network Login

Network Login: 802.1X, MAC and web based authentication, Authentication Trap

Host Integrity Checking

Validate the PC with Trusted Network Connect, Anti-Virus, OS-Patch-level, etc.

Intelligent Network Access

Dynamic ACLs for Security and QoS / Based on Network Login

MAC Security

MAC lock-down and limiting (lock out rogue access points and hubs)

MAC based VLANs (e.g. VoIP phone assigned to voice VLAN)

Wireless Radio Tuning

Power Adjustment

Detachable directional antenna

Rogue AP Detection

Scanning the radio of rogue APs

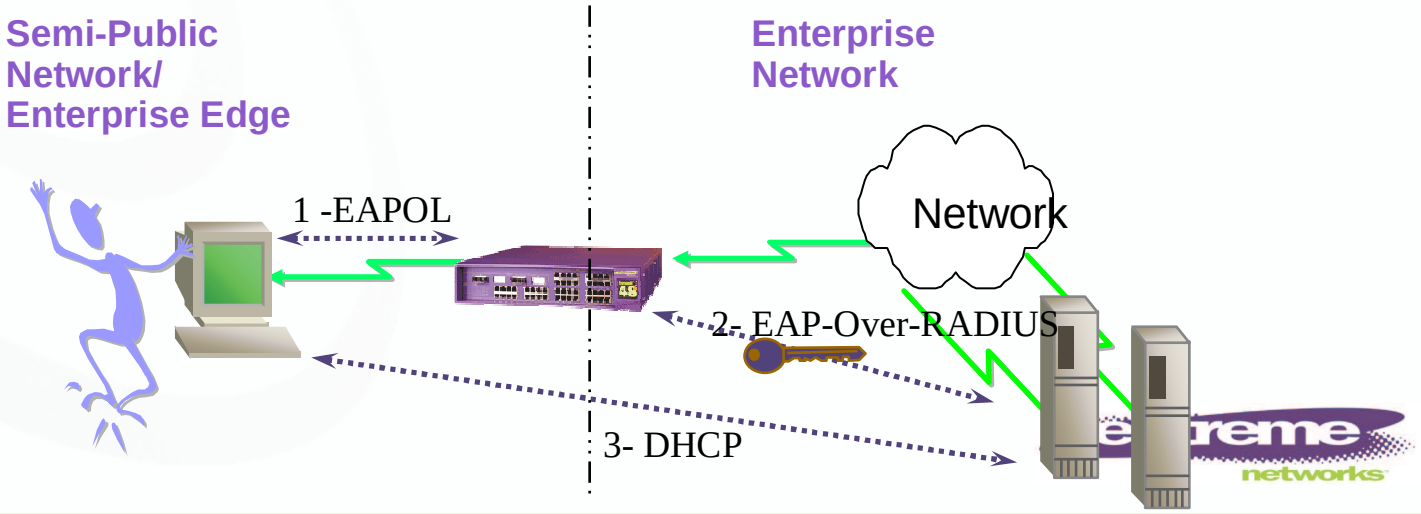
shut down the AP

Secure Unified Access

Prevent abuser or un-authorized device from connecting to the network

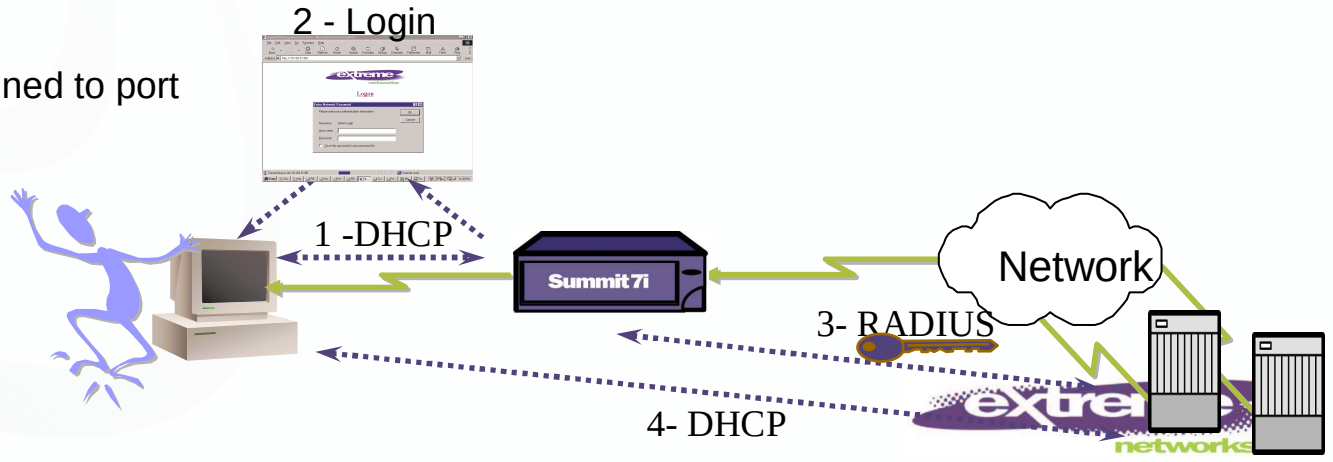
Access Security - 802.1x

- Many variants, standard is extensible. Extreme's authenticator implementation provides the most popular variants
  - MD5, TLS, TTLS
- Requires client software/OS support. Most popular clients in compatibility test
  - Windows XP (TLS)
  - Funk Software Odyssey client (TLS/TTLS)
- Uses EAP (Extensible Authentication protocol) as transport protocol
- Uses RADIUS authentication servers. Most popular authentication servers in test
  - Funk Steel Belted RADIUS (TLS/TTLS), MS-2000 IAS (MD5, TLS)
- Standard defines "port-based". Extreme can do "user based" (multiple supplicants)



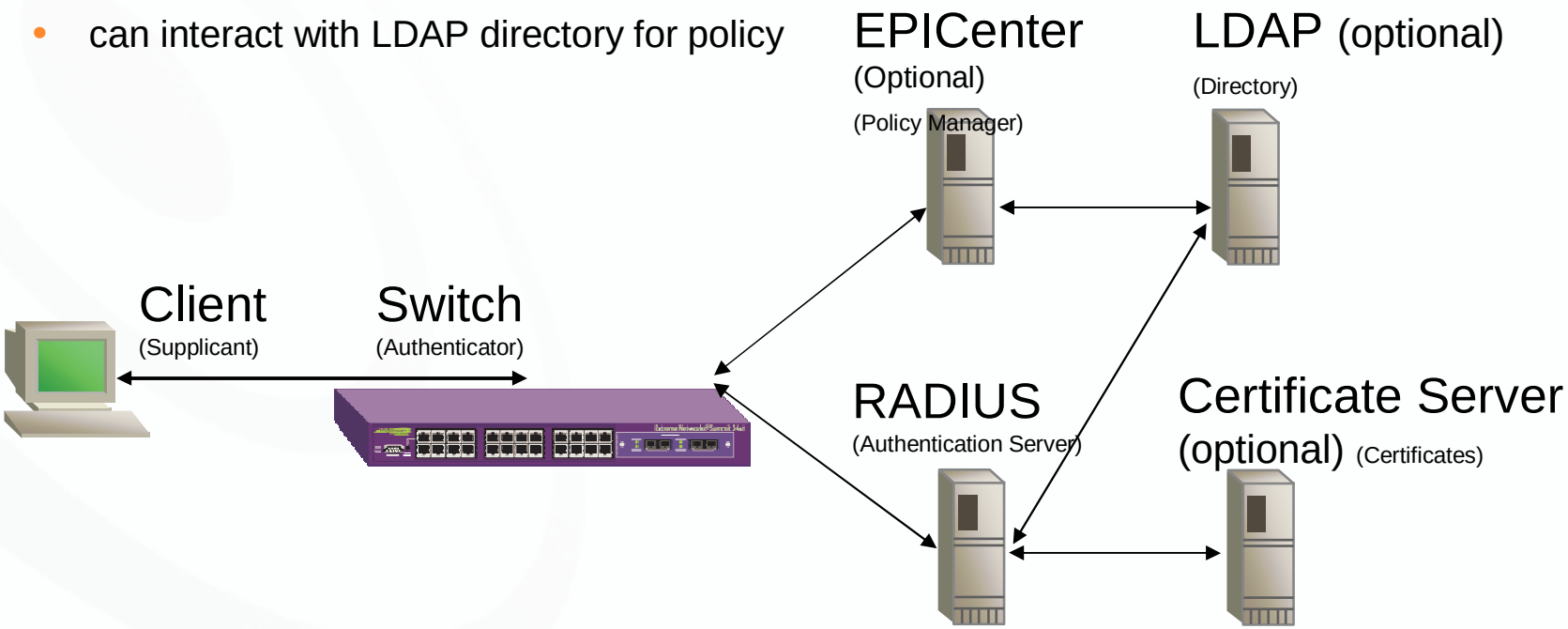
Network Login – alternative

- Control user admission and access rights to a network
  - Prevents unauthorized access and network abuse
  - 2 modes: “Campus”, “ISP”
- No client software is needed, supports PCs, Apple, Unix, …
  - DHCP/Browser based, URL-hijacking automatically redirects to login page
  - Presents Web interface and requests user login
  - Access granted to users authenticated by RADIUS server
- Login page text is configurable (HTML body, text), for guest access and localization
- Inactivity (configurable) and manual logout for security and accounting
- Mode: Campus
  - Ideal for “open” networks - Edu, Gov, Healthcare
  - VLAN is assigned based on configuration set on RADIUS server, ideal for roaming users
- Mode: ISP
  - VLAN pre-assigned to port



How INA Works

- Switch authenticates via RADIUS (Web-Based or 802.1X based Network Login)
- RADIUS server will send authentication
  - can interact with LDAP for user information and use a central certificate server
  - Can supply group or user-based VLAN ID tag
- Switch sends traps / syslog on Network Login
- EPICenter Policy Manager applies policy
  - can interact with LDAP directory for policy



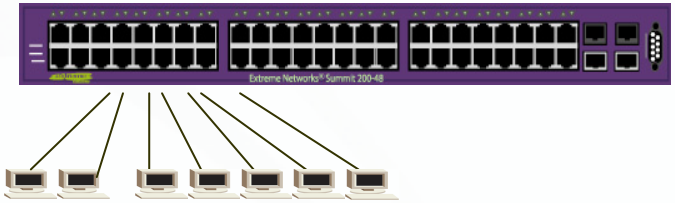
Network Login Modes

- Mode: “Campus”
  - Ideal for “open” networks - Edu, Gov, Healthcare
  - VLAN is assigned based on configuration set on RADIUS server
  - ideal for roaming users with different VLAN access needs
  - Can use ports even for guest access via an internet-only VLAN
  - If users share the port, they need to have the same VLAN assignment as the first authenticated user or will not be let in
- Mode: “ISP”
  - VLAN pre-assigned to port
  - Seamless support even for multiple users on the same port (hotspot)

Network Login

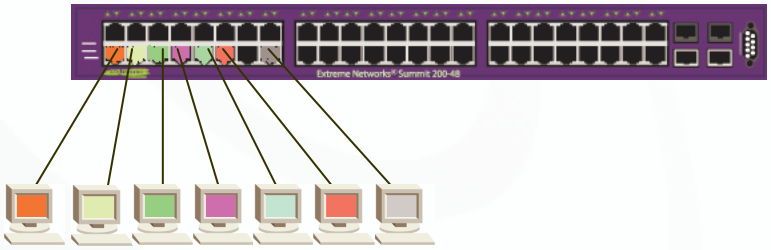
Campus Mode

Before Login



ALL Ports Blocked

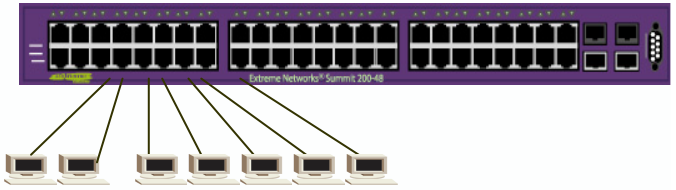
After User Login



- Ports Unblocked
- Ports **CHANGE** to User Difined Vlan
- All vlans must be in the Uplink(s) Port(s)

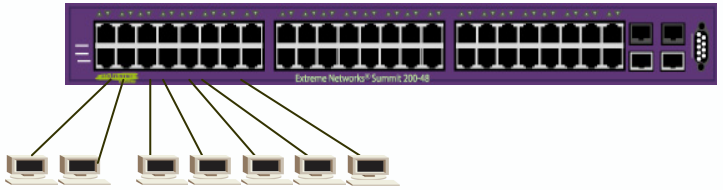
ISP Mode

Before login



ALL Ports Blocked

After User Login



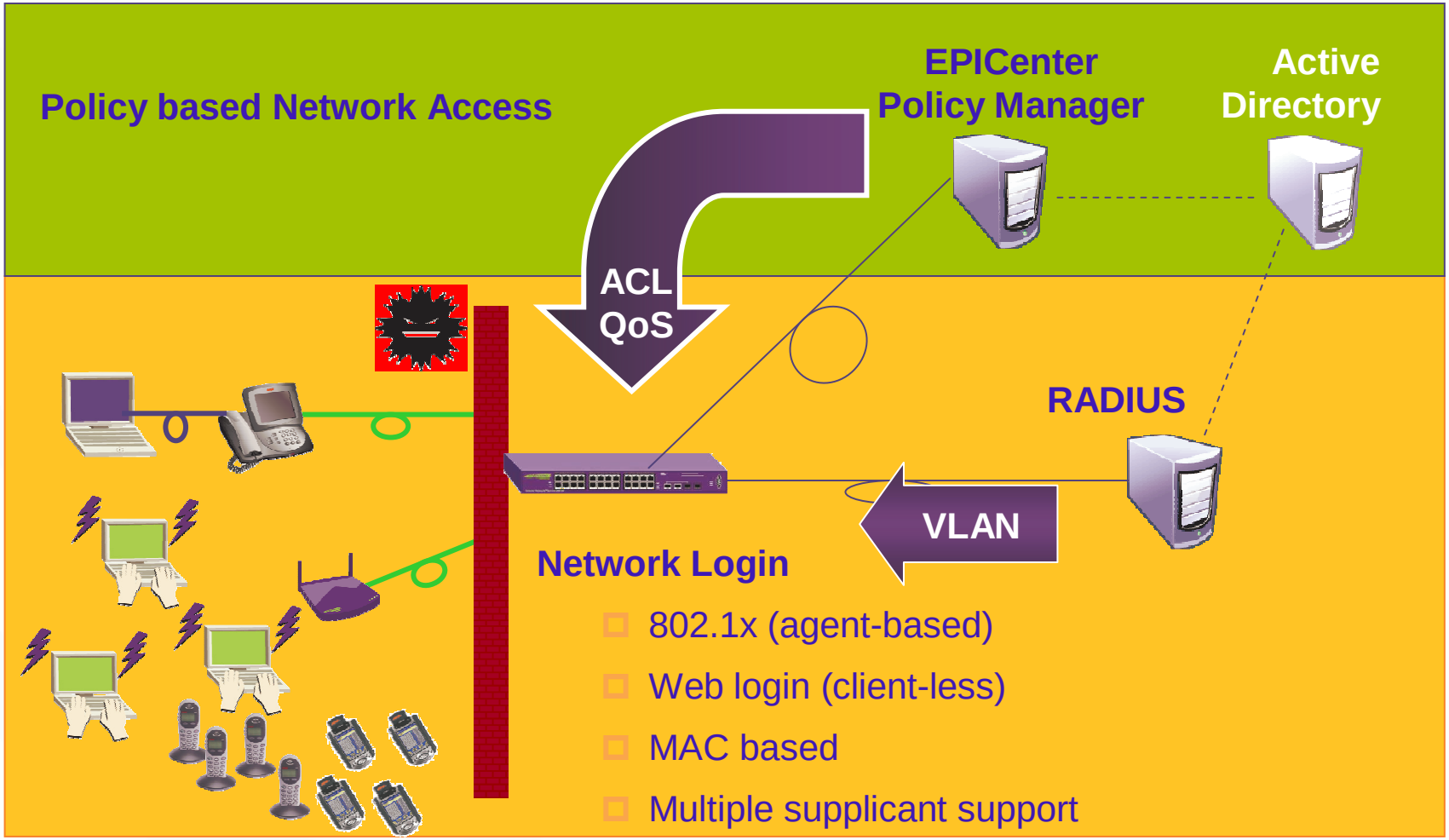
- Ports Unblocked
- Ports keep in the same vlan
- No changes on Vlan Port

Weblogin versus 802.1x

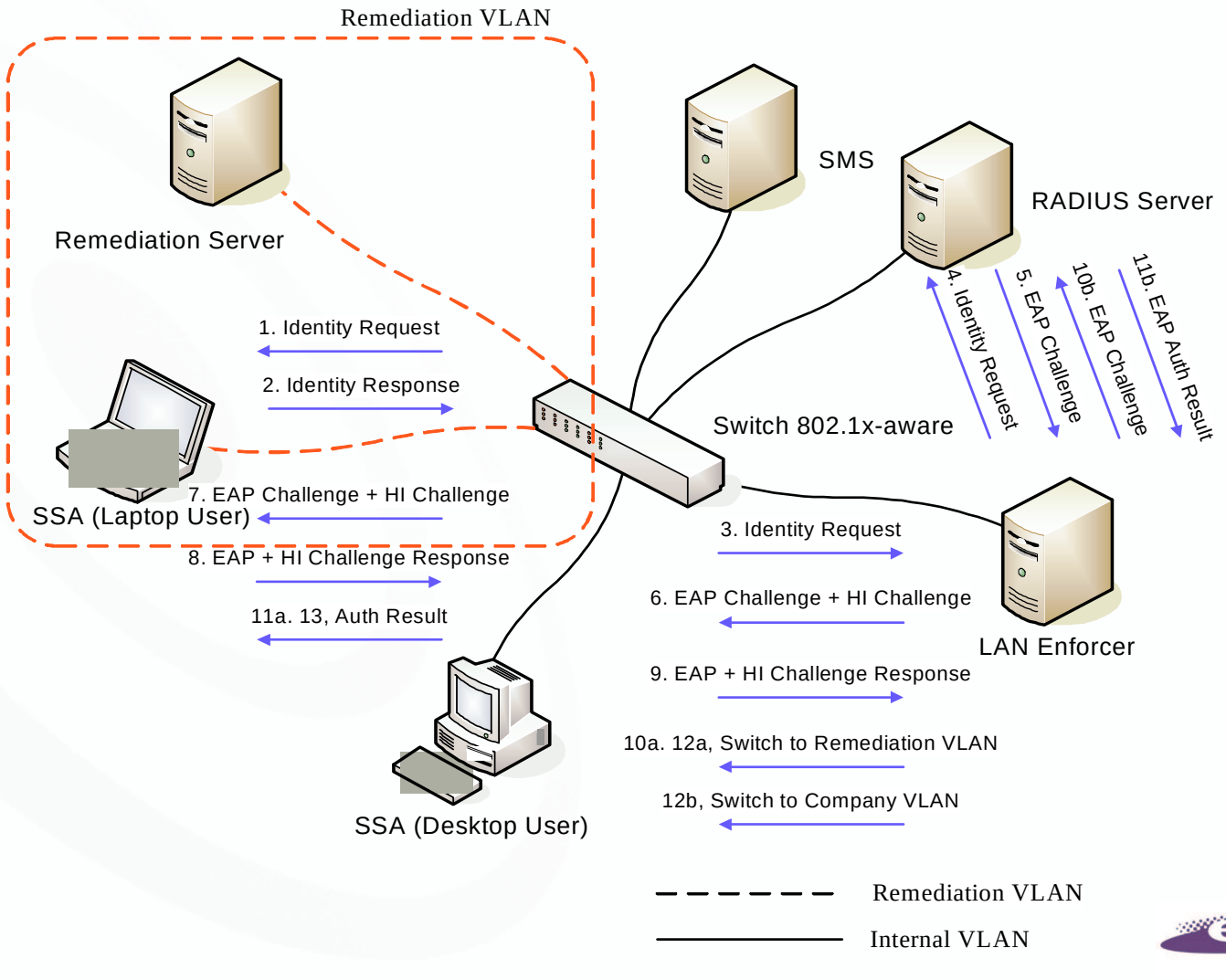
	Vantagens	Desvantagens
▸ Weblogin	*Não é necessário configurar ou instalar nada no Client Recomendação : Redes Corporativas & Usuários **Visitantes**	*Não é transparente
▸ 802.1x	*Após Configurado é transparente Recomendação : Redes Corporativas & Usuários **Corporativos**	*É é necessário configurar ou instalar SW no Client (Ver Sisoper)

Ideal : Ambos Simultâneamente na mesma porta.

Intelligent Network Access



802.1x EAP Authentication Example with Host Integrity Checking



Agenda

- **Case Studies**

Brasil

Comeco das operações : Abril/2000

Key Customers in Brazil

Goverment

CINDACTA II
STF Supremo Tribunal Federal
Ministério Público - RS
TRT 9ª REGIÃO
JUS J4 net TRT4
INFRAERO AEROPORTOS BRASILEIROS
Educação Ministério da Educação
TRE TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO
TRF 4
CELEPAR
Camara dos Deputados
Poder Judiciário Tribunal de Justiça do Estado do Rio Grande do Sul
POLÍCIA FEDERAL
CET Companhia de Engenharia de Tráfego São Paulo • SP • Brasil

Metro

RNP
CPqD
PROCERGS
BrasilTelecom
Itaú
CEEE COMPANHIA ESTADUAL DE ENERGIA ELÉTRICA-RS
CTBC
COPEL Companhia Paranaense de Energia
NET Virtua
Sercomtel
Impsat

Universidades / Research

UNIVERSIDADE FEDERAL DE MINAS GERAIS
UFPR
CPqD
UNICAMP
UNIVERSIDADE SALVADOR
UEMS
UFRGS
PUC RIO
LA SALLE
UFPel ufpel.edu.br 35 anos
ISP Universidade de São Paulo BRASIL
CBPF
SESC CEARÁ
UFSM
INPE
MINISTÉRIO DA CIÊNCIA E TECNOLOGIA INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS
Universidade Federal do Ceará

Enterprise

DAMOVO
gradiente
COMPAQ
RENNER
c.vale Cooperativa Agroindustrial
COAMO AGROINDUSTRIAL COOPERATIVA
ATENTO: Brasil
Abbott Laboratories
ERICSSON
ask!
www.dp.com.br
NOVAMPAN
unimed
BrasilTelecom
SICREDI
bompreço
HQ GLOBAL WORKPLACES
BR PETROBRAS
AGRARIA
avanade
Electrolux

Service Providers / Carriers

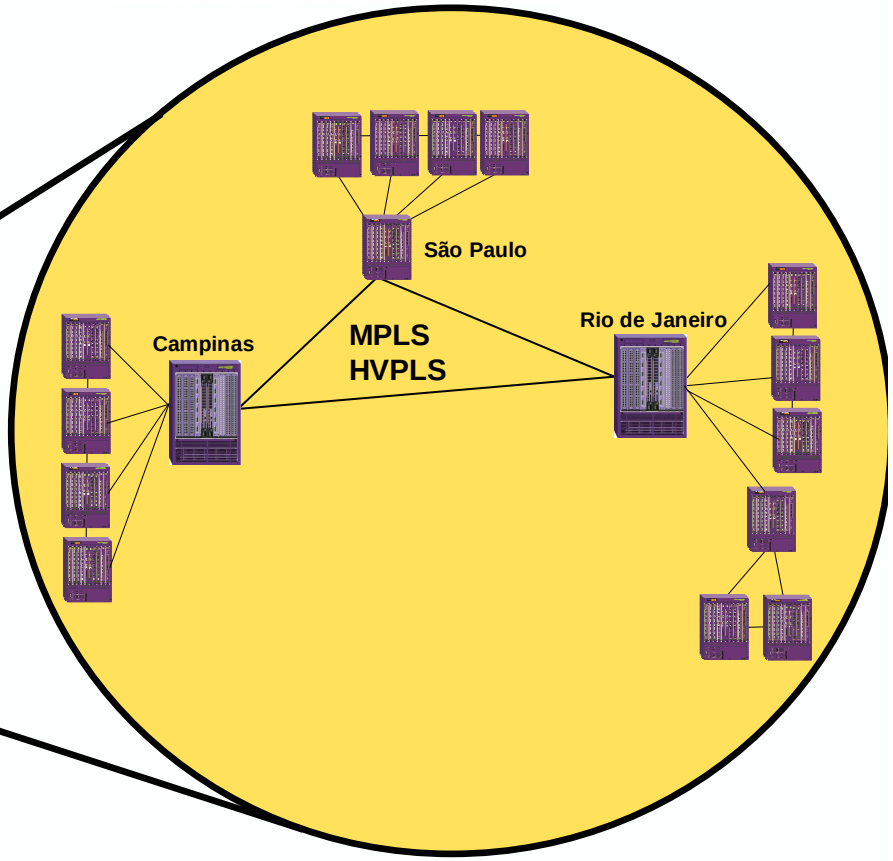
NET Virtua
Porto Digital
TELEMAR 100% brasileira
TNEXT data center
BrasilTelecom
BrTurbo.com
optiglobe
.comDominio
EDS
terra
TCO CENTRO OESTE celular
clicRBS
TIM timnet.com
iG
Telefônica
21 Embratel
registro.br

RNP

Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador
de redes avançadas no Brasil

CPqD
Telecom & IT Solutions

Projeto Giga



extreme networks

Rede Nacional de Ensino e Pesquisa
Promovendo o uso inovador
de redes avançadas no Brasil

New Gen

- Equipamentos Alpine em :
  - Porto Alegre
  - Salvador
  - Belo Horizonte
  - Fortaleza
  - Recife
  - Curitiba
  - Florianópolis
  - Brasília
  - Rio de Janeiro
  - São Paulo

- Programa de Parcerias
  - Certificação e treinamento de técnicos
  - Utitização anual dos Laboratórios da Extreme para testes avançados
  - Inclusao da RNP no CAC (Customer Advisor Council)

Muito Obrigado !!!!!!

Renier Edward Souza
SE Manager – South America
Rsouza@extremenetworks.com