Network Services Delivery

Petr Habarta

SSO+DCS MU FIT

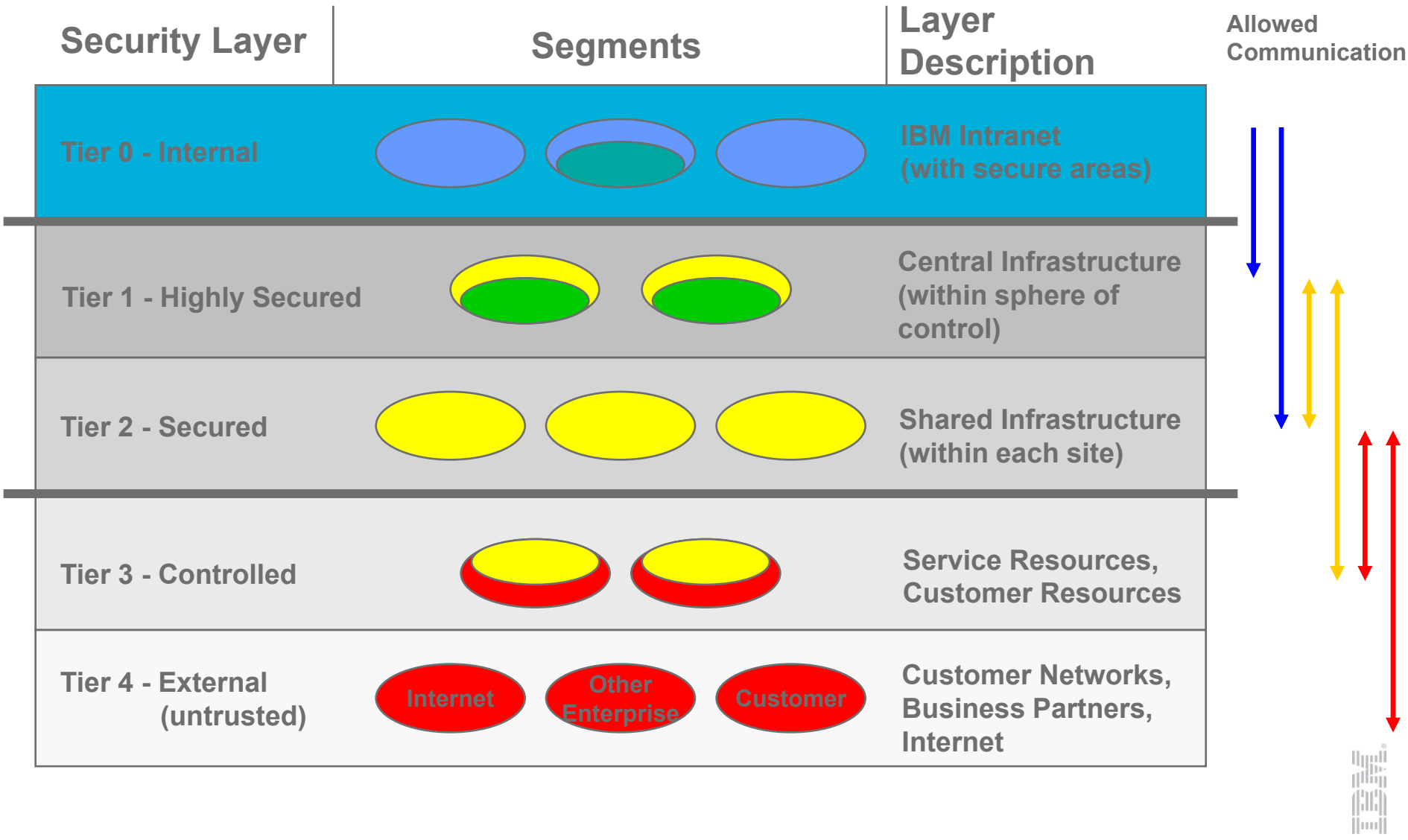
Agenda

- Shared Network Infrastructure
- Organization structure
- Network monitoring tools
- LAN Management
- WAN Management
- Firewall
- IP Services
- Network Security
- Typical issues - LAN/WAN
- Typical issues - FW, IPSE

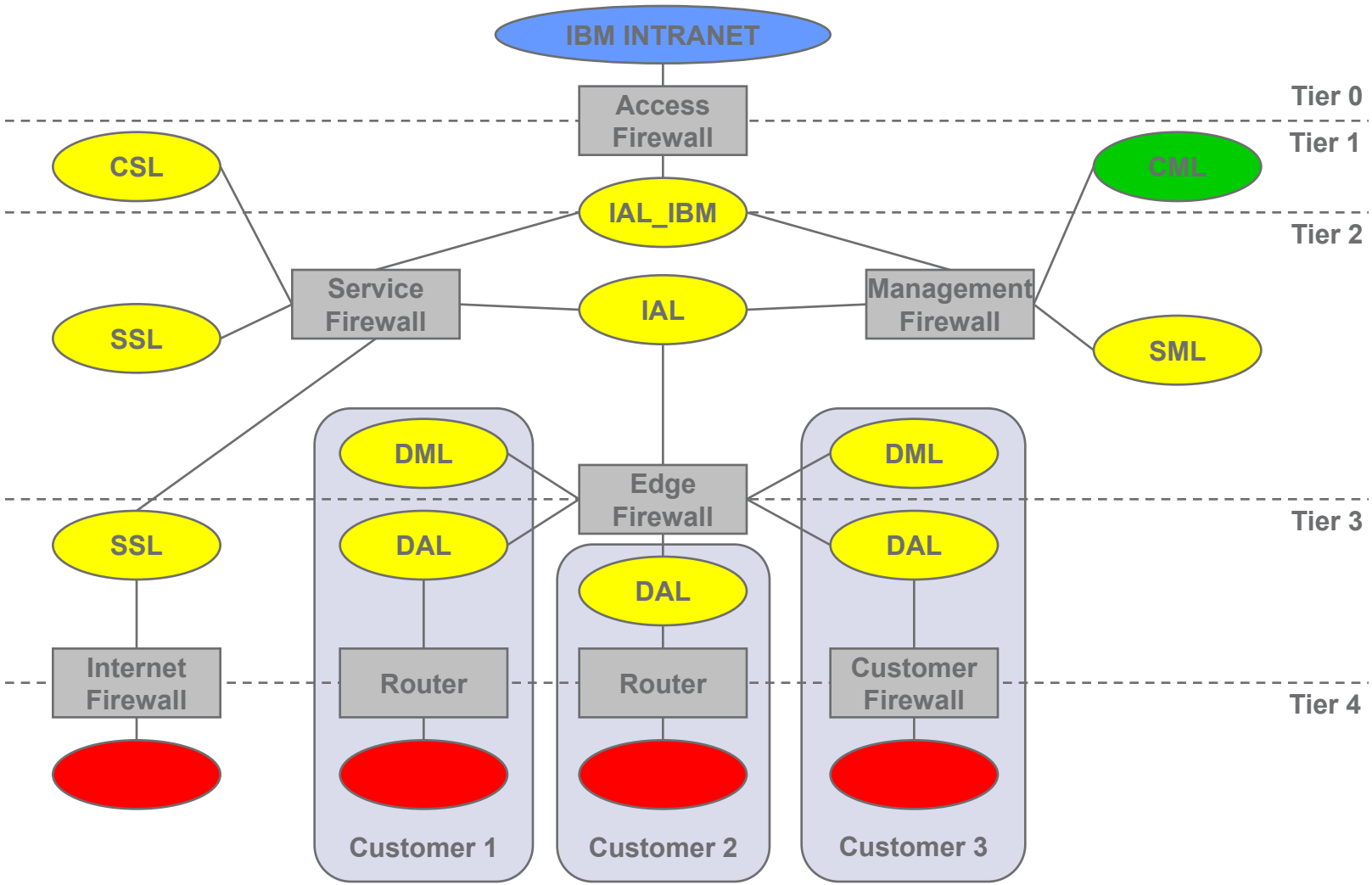
What is Shared Network Infrastructure (SNI)?

- Provides secure way how to connect from IBM internal network to customer network
- SNI is special network architecture inside IBM Global Services Data Center.
- Security requirements are very difficult
- Is based on few network segment with different security access levels

Tier Definitions for SNI (e.g. eSNI “simplified”)



Implementation Example (e.g. eSNI “simplified”)



Abbreviations

- CML – Central Management LAN
- CSL – Central Service LAN
- SML – Shared Management LAN
- SSL – Shared Service LAN
- DML – Dedicated Management LAN
- DAL – Dedicated Access LAN
- IAL – Infrastructure Access LAN
- IAL_IBM – Infrastructure Access LAN IBM

What Advantages/Disadvantages are there for SNI?

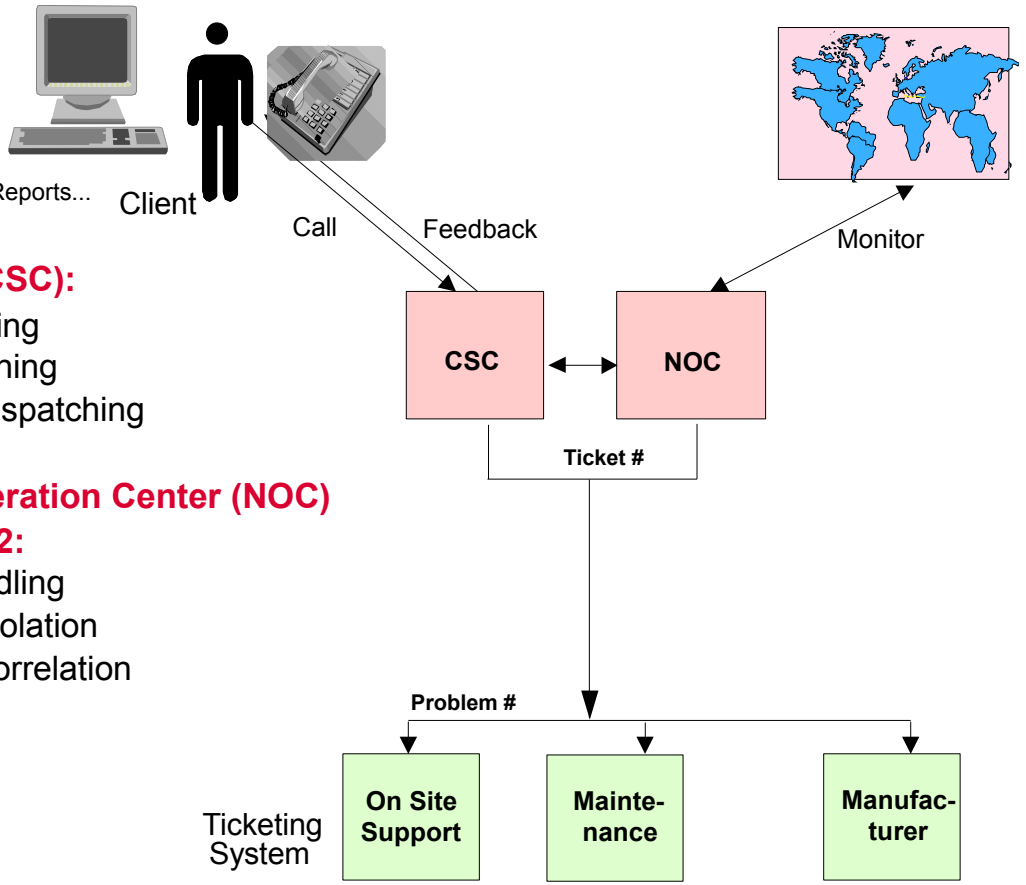
Advantages

- Standard solution
- Secure solution
- Reuse of environment
- Cost reduction

Disadvantages

- Sharing of network environment got much higher security and management requirement as single-customer one.
- It’s not always possible standardize all customer specific requests
- Possibility of conflicts in private IP address ranges

Organization Structure – Network management GNMC model



Help Desk (CSC):

- Call Handling
- Ticket opening
- Problem dispatching

Network Operation Center (NOC)
Level 1/level2:

- Ticket handling
- Problem isolation
- Problem correlation

NOC - Level 1 support

- Proactive monitoring of different tools. Coordinates incident resolution and communication.
- Use simple and clear processes. Require best knowledge of these processes, tools usage and got global overview of systems.
- Necessary 24/7 support

Examples

- Coordinates outages of WAN providers, communicate WAN related issues.
- Update problem tickets in ticketing systems and inform other teams in case of issue resolution
- Communication point for CSC – provide feedback for customer
- Coordinates HW replacement

NOC - Level 2 support

- Advanced problem resolution of troubles coming from 1st level.
- Processes are not so clear for 2nd level
- Level 2 require skills and experiences

Examples

- Analyze and correct routing problems
- Correct security findings in configuration, patch/upgrade OS on devices
- Setting and modifying configuration on devices, activation of new customers or devices
- Change of ACLs, cooperation with 3rd level and vendor support if needed

Level 3 support

- Level 3 support work with complex problems. 3rd level is involved in problems affecting huge infrastructure.
- Solving all not standard solutions
- Cooperating and coordinating complex changes in network structure.
- Act as Network Architects

Examples

- Providing prevention in wrong setup of routing protocols
- Finding solution for slow application performance
- Deploying new customer to SNI

Why we need proper NSD tools set?

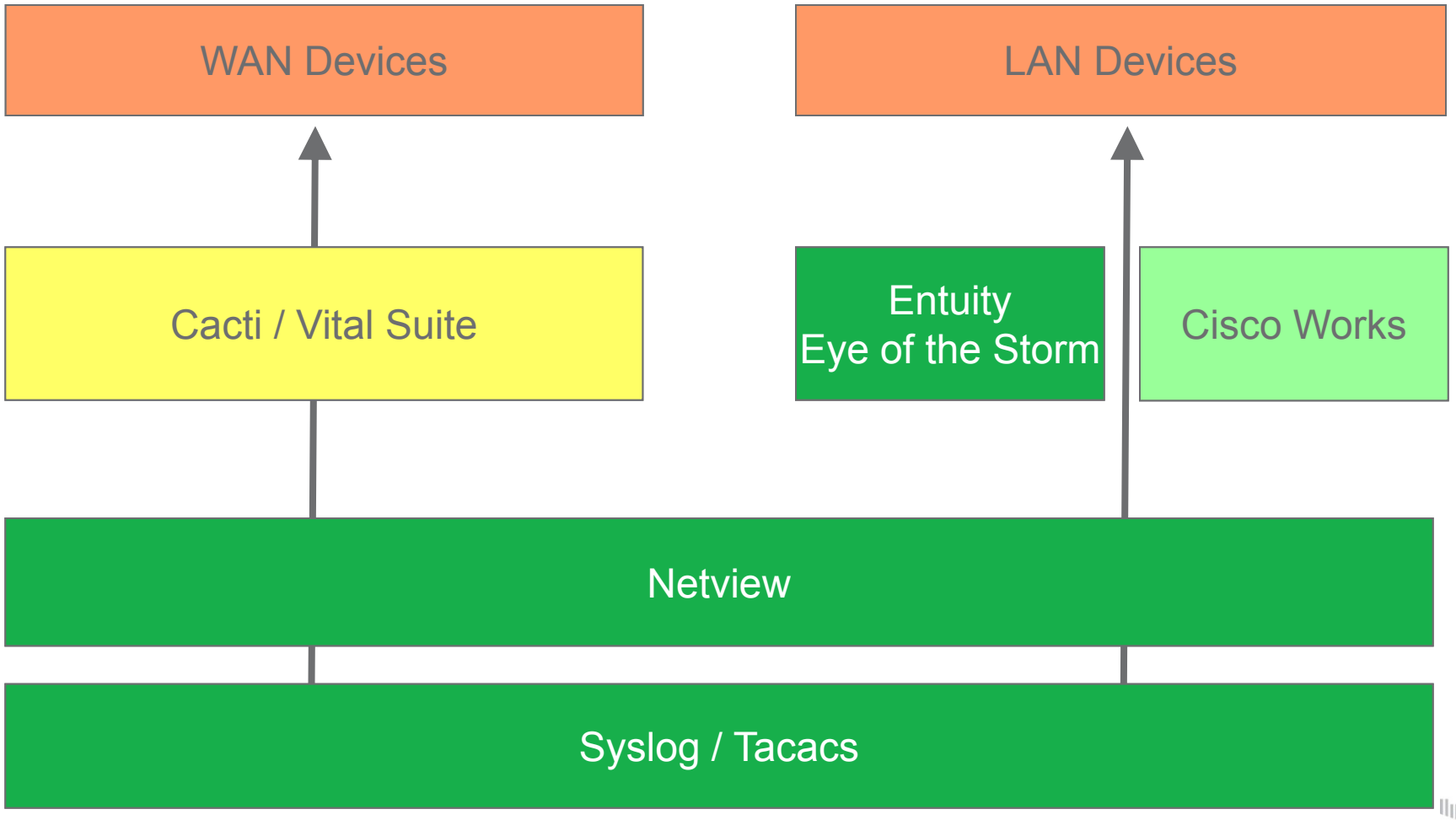
More than 80 percent of application performance and availability failures will be blamed on network problems, but the network will represent less than 20 percent of the root cause

- **With proper tools set you can**
  - With monitoring tool react before customer will recognize problem.
  - Locate problem much faster then by manual tracking
  - Update many devices by one click
  - By performance tools see the trend and recognize problem before it will occurred
  - Based on historical data prevent blaming application problems

Network Management Toolset

- Tivoli Netview
  - Detection of problems with implementation of L3 map
- Entuity Eye of the Storm
  - Performance and advanced monitoring / analysis
  - Monitor device with SNMP - can detect more than 70 type of errors.
- Cisco Works (CW)
  - Provides advanced configuration / problem detection for Cisco Platform
- CACTI / Vital suite Statistics
  - SNMP orientated performance management tool
- Other tools
  - TACACS/RADIUS/LDAP – Authentication services
  - Evidence databases – CEP+ / MAD / eAMT
  - Ticket tracking tools

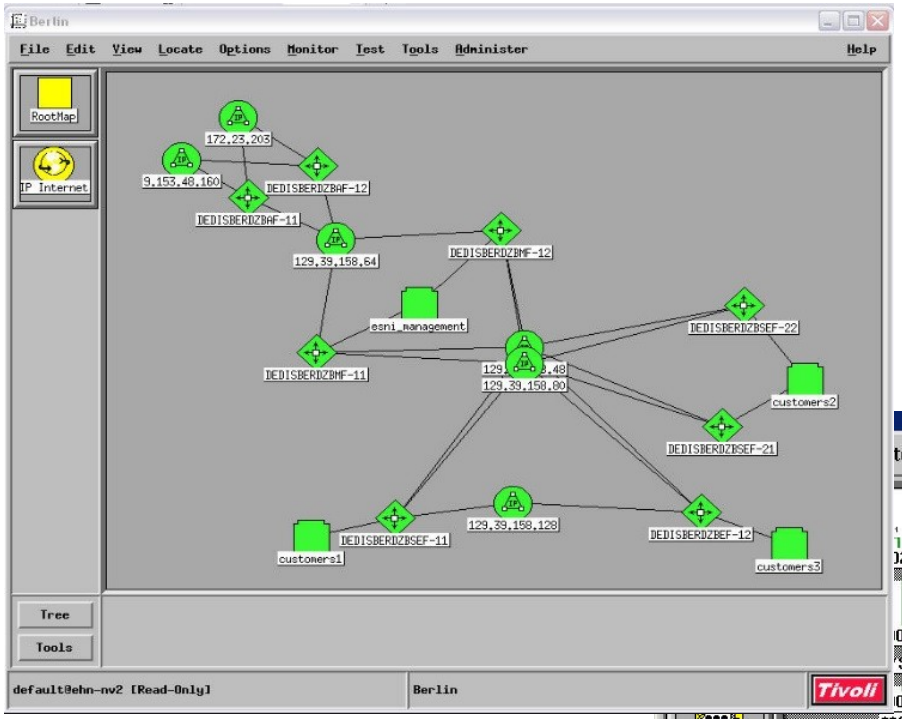
Network Management Toolset

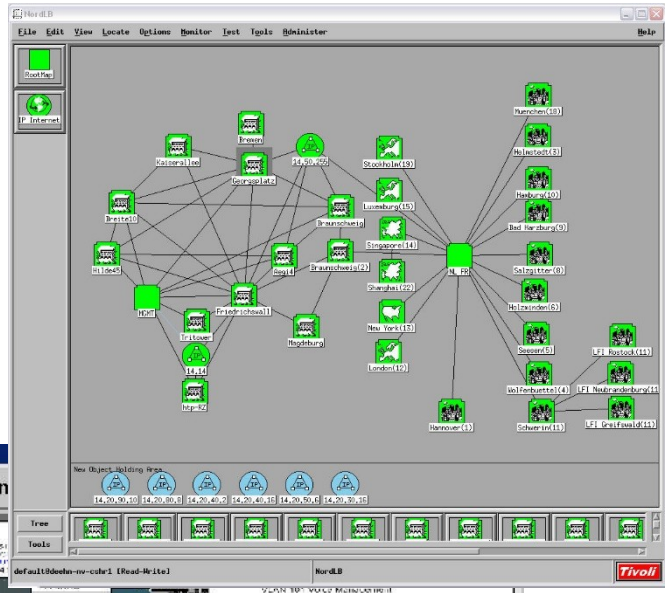


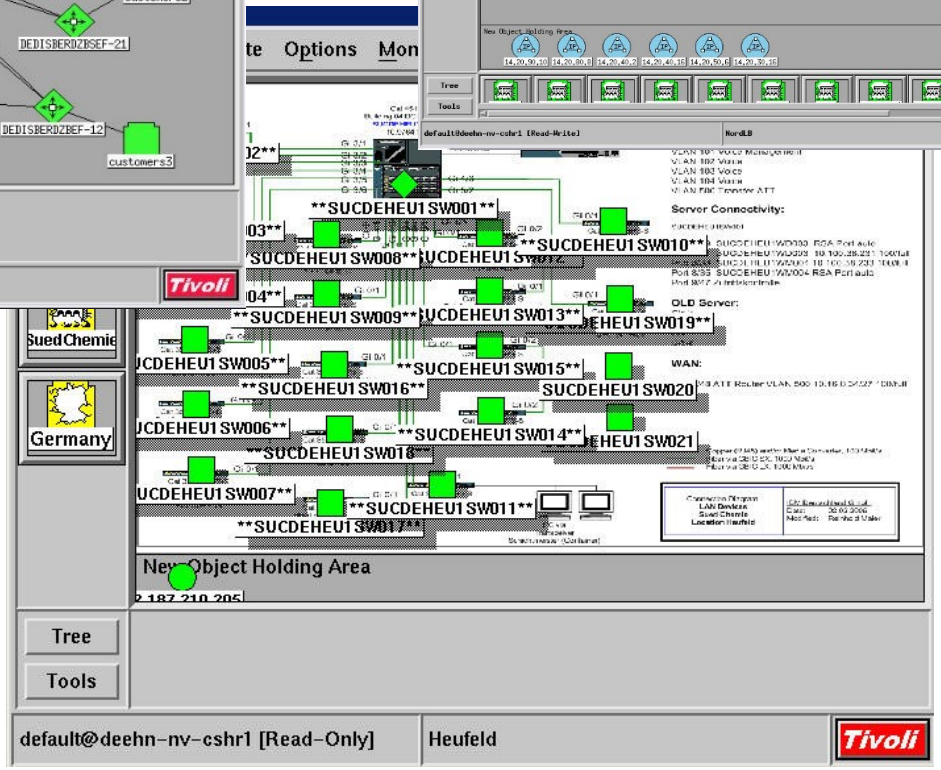
Fault detection with Netview

- Netview is standard tool used by IBM all over the world for most customers.
- Monitoring of device status
- Clear picture of network infrastructure
- Netview support easy implementation of various scripts which can automation work.
- With SNMP support of all devices provides advanced monitoring (not based only on UP/DOWN functionality with ICMP)
- Can receive/forward SNMP traps from/to other tools (EotS/Cacti…)

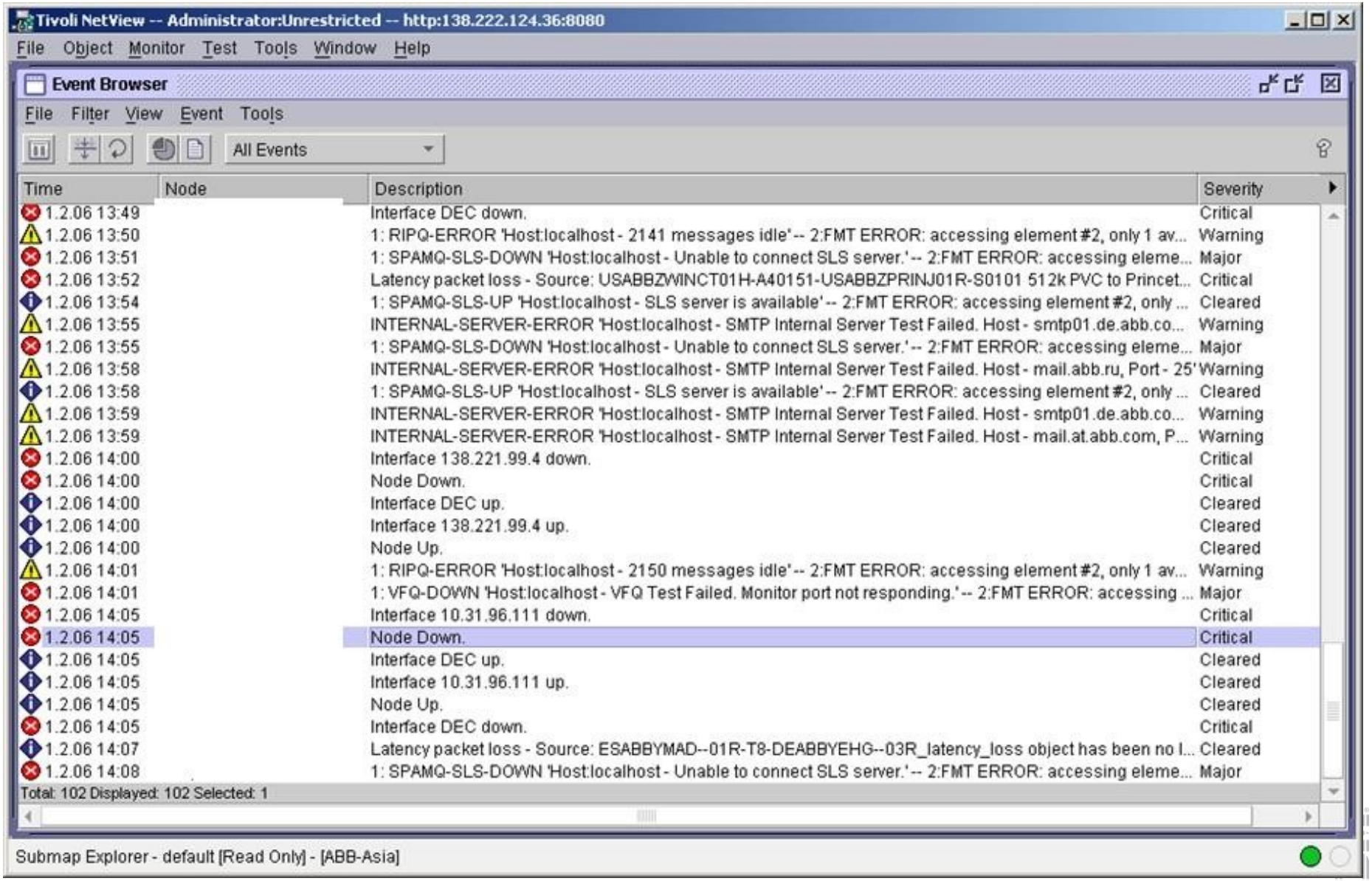
Fault detection - Netview







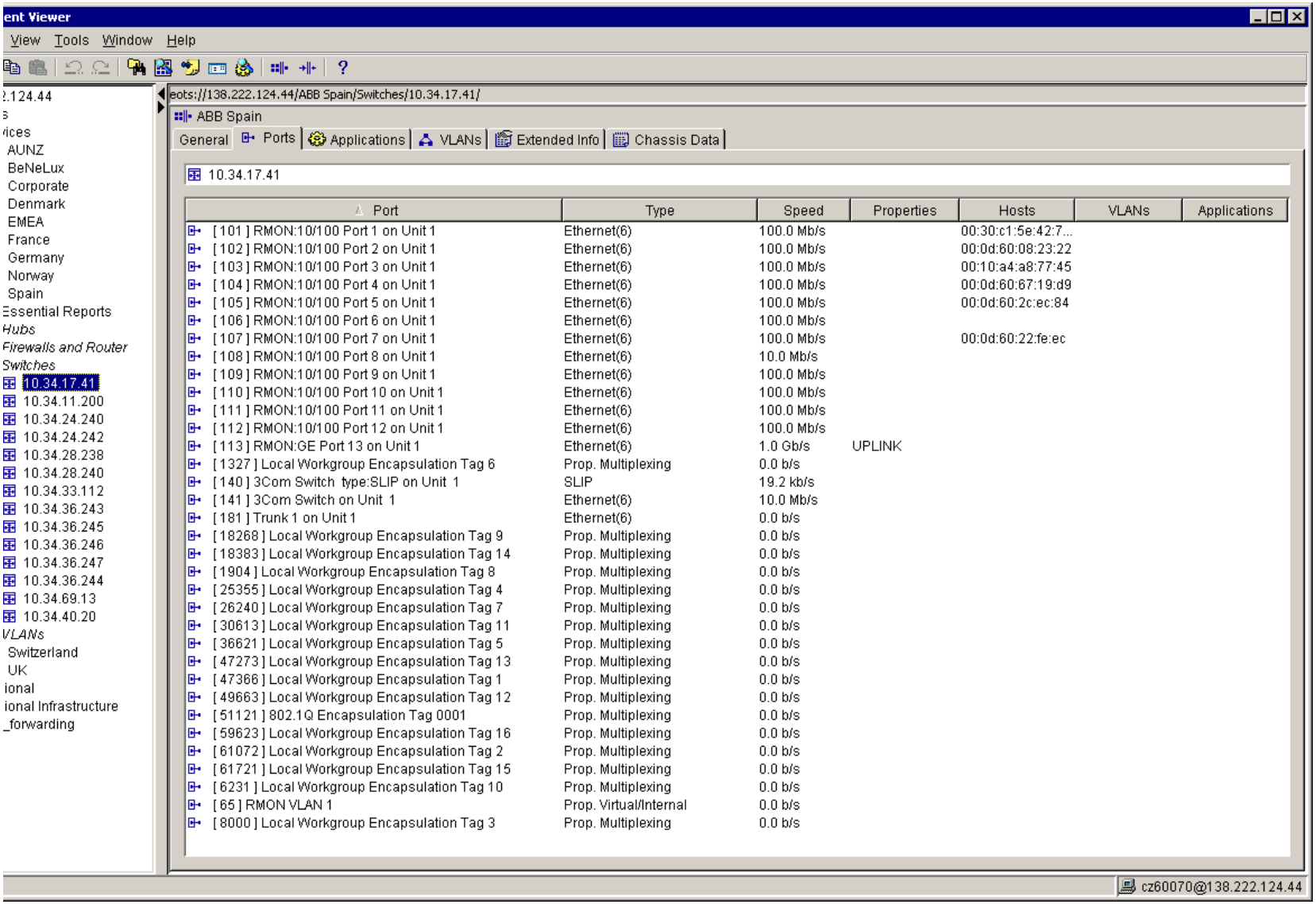
Tivoli Netview – Event Browser



Entuity Eye of the Storm

- Advanced monitoring of devices (LAN, WAN and firewalls) with SNMP
- Forward major issues to netview
- Provides advanced troubles finding
- Feature performance monitoring gives us possibility for prevention in outages based on wrong implementation
- Provides statistic for core lines (Trunks, Etherchannels)
- Availability management
- Keeps historical data

Entuity Eye of the Storm – port listing



Port	Type	Speed	Properties	Hosts	VLANs	Applications
[101] RMON:10/100 Port 1 on Unit 1	Ethernet(6)	100.0 Mb/s		00:30:c1:5e:42:7...		
[102] RMON:10/100 Port 2 on Unit 1	Ethernet(6)	100.0 Mb/s		00:0d:60:08:23:22		
[103] RMON:10/100 Port 3 on Unit 1	Ethernet(6)	100.0 Mb/s		00:10:a4:a8:77:45		
[104] RMON:10/100 Port 4 on Unit 1	Ethernet(6)	100.0 Mb/s		00:0d:60:67:19:d9		
[105] RMON:10/100 Port 5 on Unit 1	Ethernet(6)	100.0 Mb/s		00:0d:60:2c:ec:84		
[106] RMON:10/100 Port 6 on Unit 1	Ethernet(6)	100.0 Mb/s				
[107] RMON:10/100 Port 7 on Unit 1	Ethernet(6)	100.0 Mb/s		00:0d:60:22:fe:ec		
[108] RMON:10/100 Port 8 on Unit 1	Ethernet(6)	10.0 Mb/s				
[109] RMON:10/100 Port 9 on Unit 1	Ethernet(6)	100.0 Mb/s				
[110] RMON:10/100 Port 10 on Unit 1	Ethernet(6)	100.0 Mb/s				
[111] RMON:10/100 Port 11 on Unit 1	Ethernet(6)	100.0 Mb/s				
[112] RMON:10/100 Port 12 on Unit 1	Ethernet(6)	100.0 Mb/s				
[113] RMON:GE Port 13 on Unit 1	Ethernet(6)	1.0 Gb/s	UPLINK			
[1327] Local Workgroup Encapsulation Tag 6	Prop. Multiplexing	0.0 b/s				
[140] 3Com Switch type:SLIP on Unit 1	SLIP	19.2 kb/s				
[141] 3Com Switch on Unit 1	Ethernet(6)	10.0 Mb/s				
[181] Trunk 1 on Unit 1	Ethernet(6)	0.0 b/s				
[18268] Local Workgroup Encapsulation Tag 9	Prop. Multiplexing	0.0 b/s				
[18383] Local Workgroup Encapsulation Tag 14	Prop. Multiplexing	0.0 b/s				
[1904] Local Workgroup Encapsulation Tag 8	Prop. Multiplexing	0.0 b/s				
[25355] Local Workgroup Encapsulation Tag 4	Prop. Multiplexing	0.0 b/s				
[26240] Local Workgroup Encapsulation Tag 7	Prop. Multiplexing	0.0 b/s				
[30613] Local Workgroup Encapsulation Tag 11	Prop. Multiplexing	0.0 b/s				
[36621] Local Workgroup Encapsulation Tag 5	Prop. Multiplexing	0.0 b/s				
[47273] Local Workgroup Encapsulation Tag 13	Prop. Multiplexing	0.0 b/s				
[47366] Local Workgroup Encapsulation Tag 1	Prop. Multiplexing	0.0 b/s				
[49663] Local Workgroup Encapsulation Tag 12	Prop. Multiplexing	0.0 b/s				
[51121] 802.1Q Encapsulation Tag 0001	Prop. Multiplexing	0.0 b/s				
[59623] Local Workgroup Encapsulation Tag 16	Prop. Multiplexing	0.0 b/s				
[61072] Local Workgroup Encapsulation Tag 2	Prop. Multiplexing	0.0 b/s				
[61721] Local Workgroup Encapsulation Tag 15	Prop. Multiplexing	0.0 b/s				
[6231] Local Workgroup Encapsulation Tag 10	Prop. Multiplexing	0.0 b/s				
[65] RMON VLAN 1	Prop. Virtual/Internal	0.0 b/s				
[8000] Local Workgroup Encapsulation Tag 3	Prop. Multiplexing	0.0 b/s				

Entuity Eye of the Storm – device report

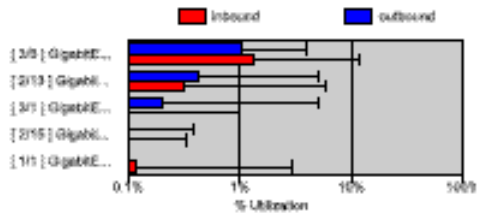
10.49.29.130

Cisco Internetwork Operating System Software IOS (tm) c6sup1_rp Software (c6sup1_rp-DSV-M), Version 12.1(23)E2, RELEASE SOFTW

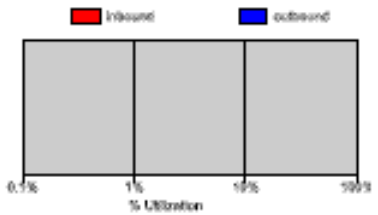
Speed	Total	Spare
10/100Mb	48	43 (90%)
1Gb	66	18 (27%)

Availability: 100%
Outages: 0
Monitored Servers: 0
Monitored Applications: 0

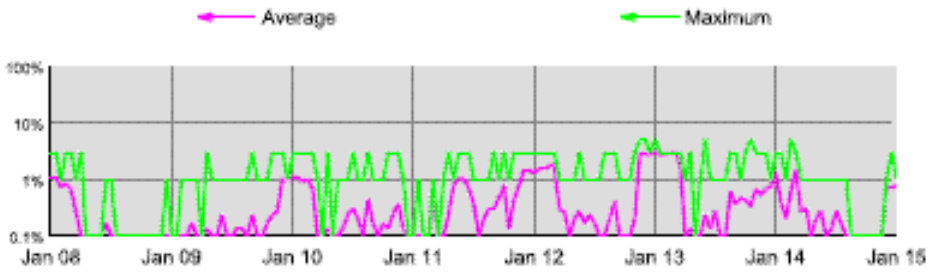
Top trunk ports



Top server ports



Bus Utilization



Entuity Eye of the Storm

Availability Summary

Over the 4 week period Wed Feb 01 2006 - Wed Mar 01 2006

Generated at 00:42 on Wed Mar 01 2006 for the Germany view

Based on data from **28 availability samples** each covering **1 day**

OVERALL AVAILABILITY SUMMARY
Application: -- (Application: --, Server: --, Network: --)
Server: -- (Server: --, Network: --)
WAN link: 94.17%

NETWORK AVAILABILITY SUMMARY		
IP Address Outages: 320 on 186 elements (585 being monitored)	MTBF: 458.9hours	MTTR: 9,949.3minutes
Router Outages: 25 on 8 devices (23 being monitored)	MTBF: 321.6hours	MTTR: 45minutes
Switch Outages: 6 on 6 devices (82 being monitored)	MTBF: 655.7hours	MTTR: 26,505minutes

APPLICATION AVAILABILITY SUMMARY		
Application Outages: none (0 being monitored)	MTBF: --	MTTR: --

SERVER AVAILABILITY SUMMARY		
Server Outages: none (0 being monitored)	MTBF: --	MTTR: --

WAN LINK AVAILABILITY SUMMARY		
Wan Link Outages: 108 on 38 links (106 being monitored)	MTBF: 333.2hours	MTTR: 6,995.4minutes

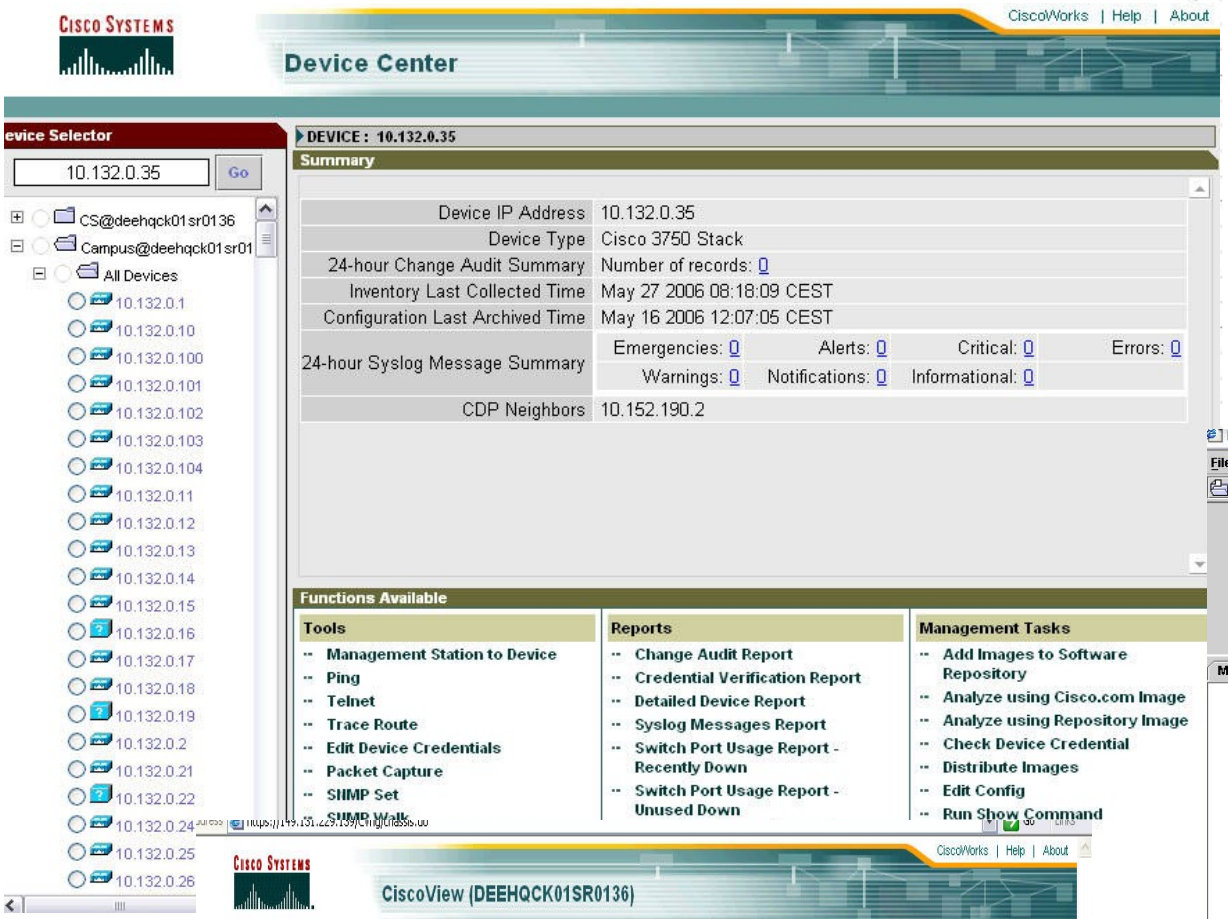
Top problem WAN links (sorted by number of outages)	Outage count	Downtime (minutes)
138.228.192.222 : [22] DEABBYEHG--03R-T65002-SGABBYSI[illegible]	15	155.7minutes
138.228.192.222 : [17] att-unman DEABBYEHG-03R-T9-ZAABBYJNB--01[illegible]	13	1,717.6minutes
138.228.192.222 : [12] DEABBYEHG-03R-T4-CZABBYBRQ--01[illegible]	10	340.6minutes
138.228.192.222 : [19] DEABBYEHG-03R-T11-CHABBYBAD--0[illegible]	8	21.8minutes
138.228.192.222 : [15] DEABBYEHG-03R-T7-PTABBYPCS--01[illegible]	7	26minutes

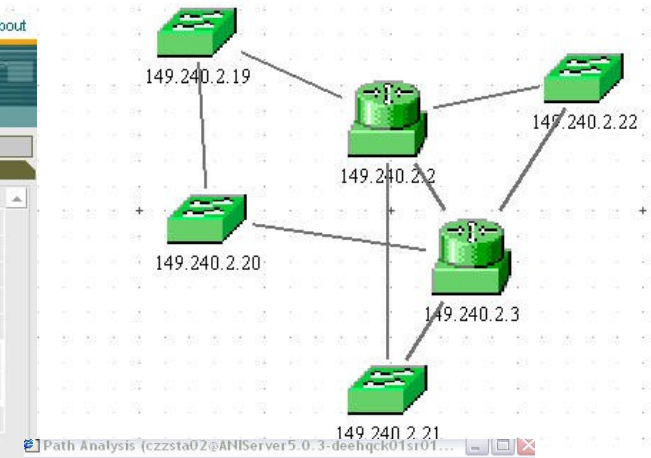
Top problem WAN links (sorted by downtime)	Outage count	Downtime (minutes)
10.49.127.199 : [124] Vlan120	1	39,600minutes
10.49.240.3 : [206] Vlan51	1	39,600minutes
10.49.240.2 : [107] Vlan1	1	39,600minutes
10.49.127.75 : [135] Vlan101	1	39,600minutes
10.49.240.3 : [203] Vlan1	1	39,600minutes

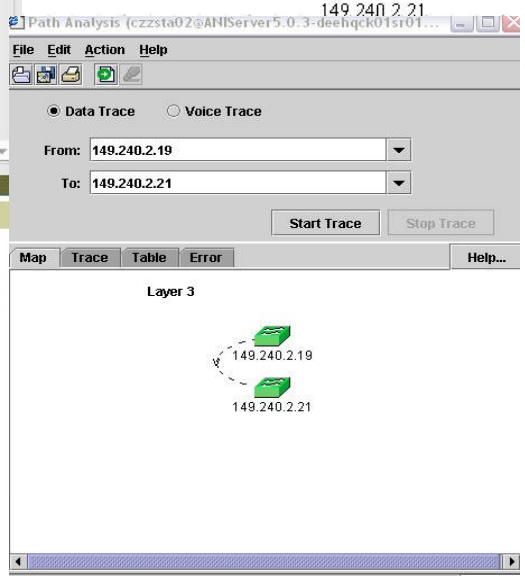
Configuration with Cisco Works

- CW support mapping devices in network made by Cisco devices.
- CW is able to download configs but it also allow to upload them to device, modify directly on CW which allow to made small common changes by “one click” on many devices
- CW give you chance to work with device like with real (show physical surface)
- Data colleting from devices / mass changes / security activities
- Can create reports for Cisco platform

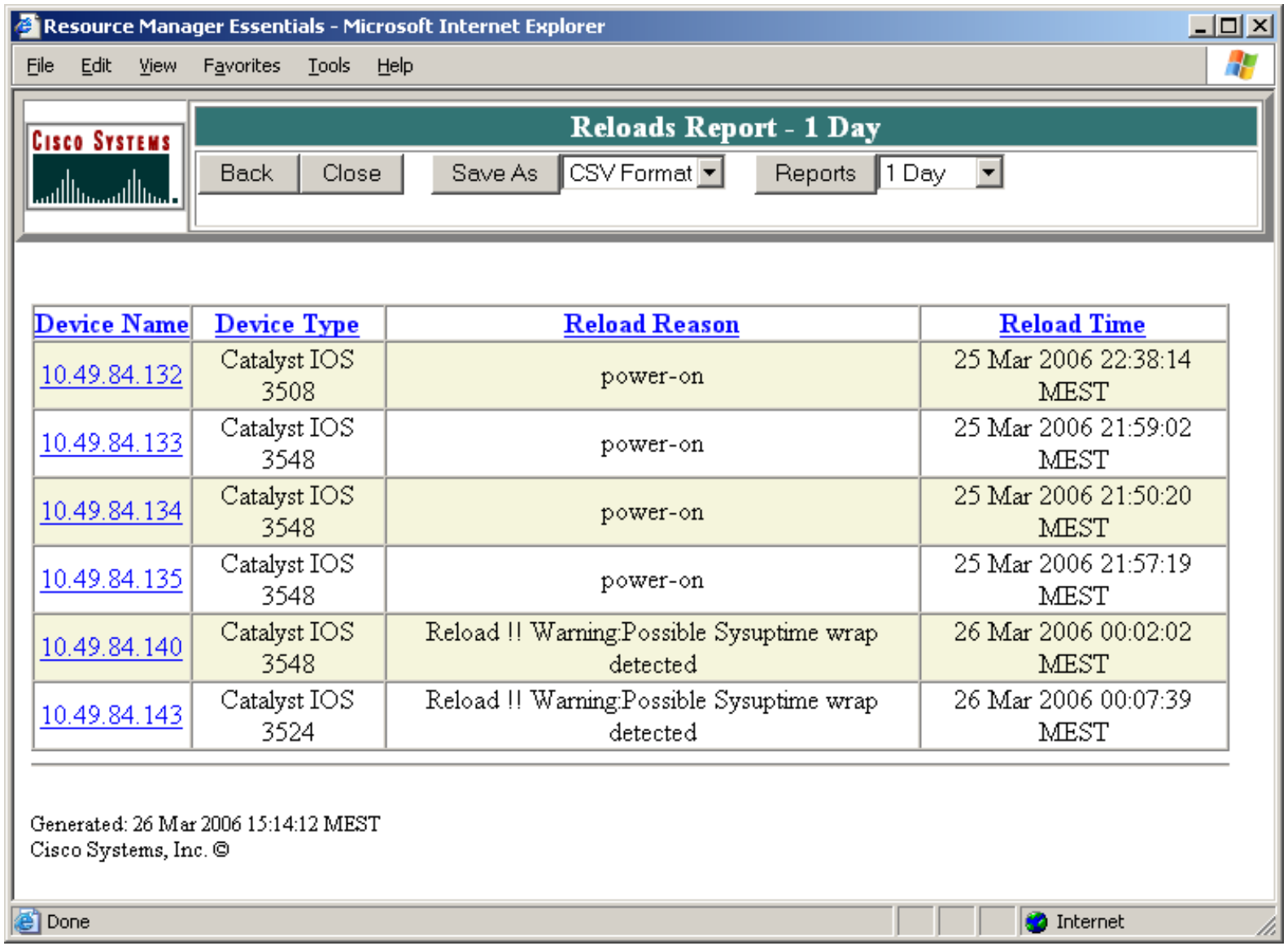
Configuration – Cisco works



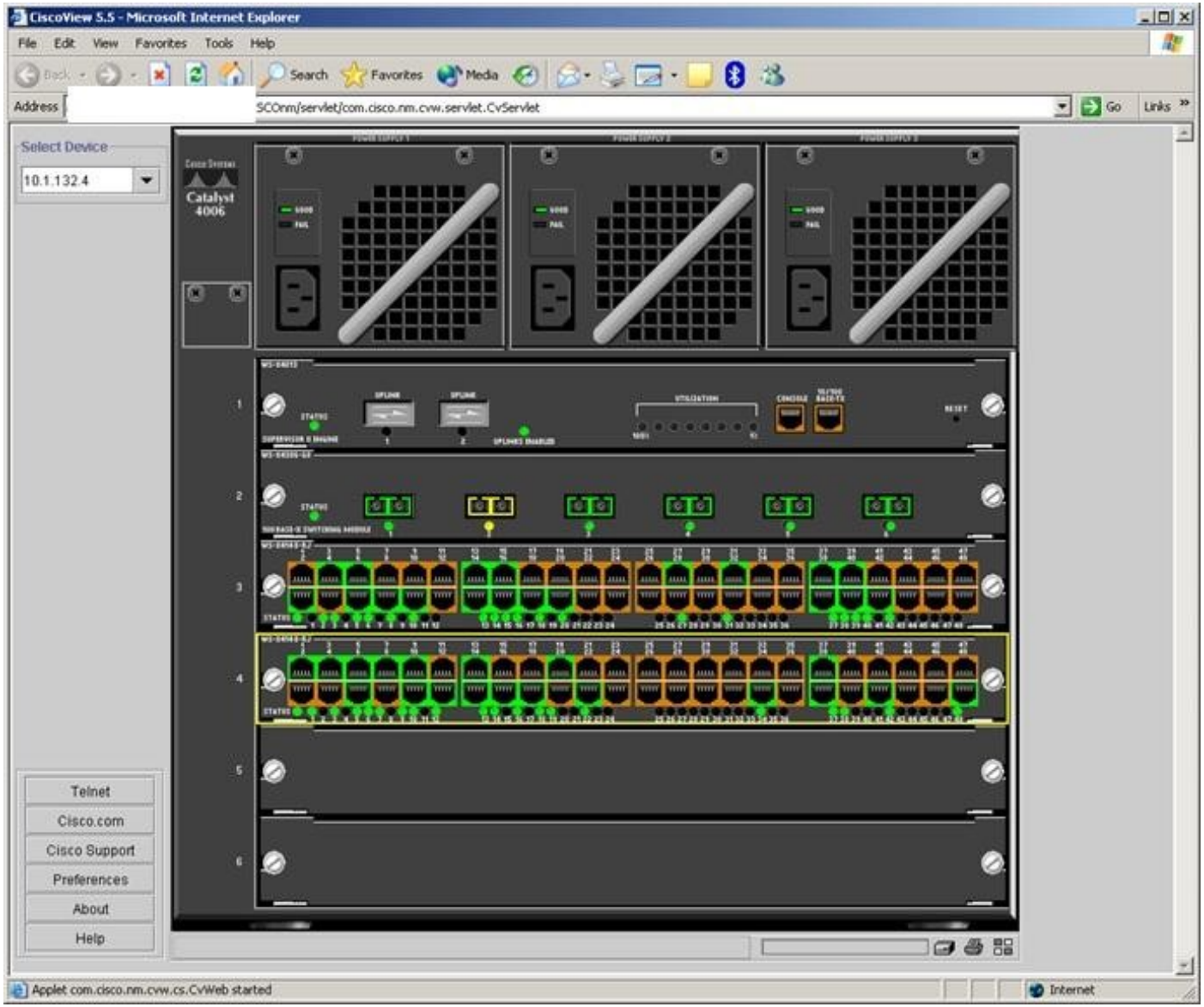




Cisco Works – example of report



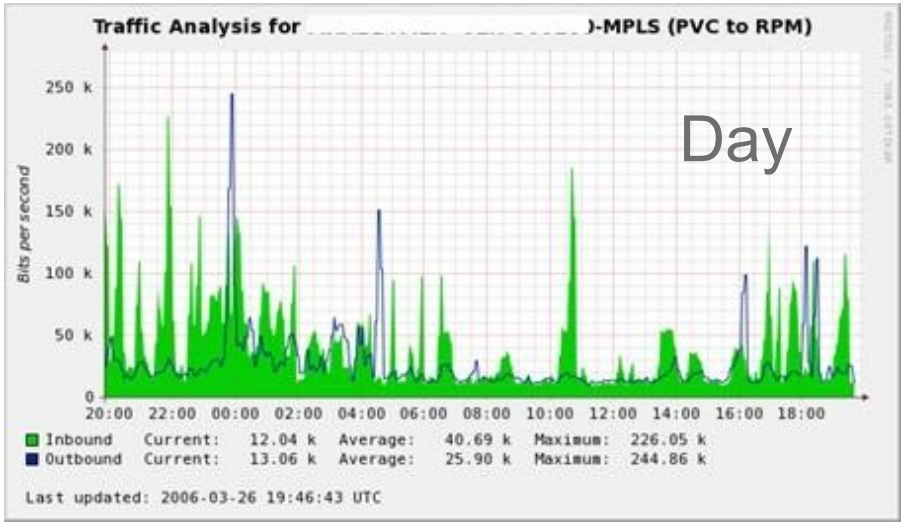
Cisco Works – Cisco View

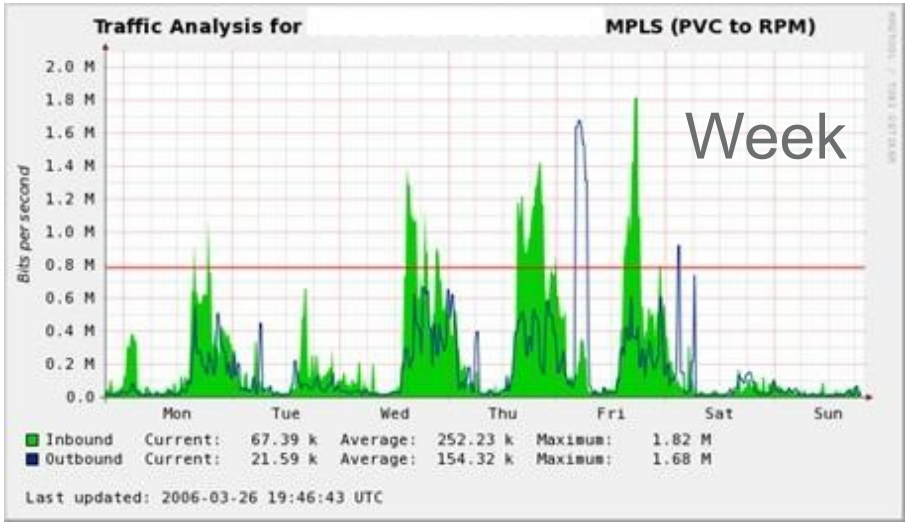


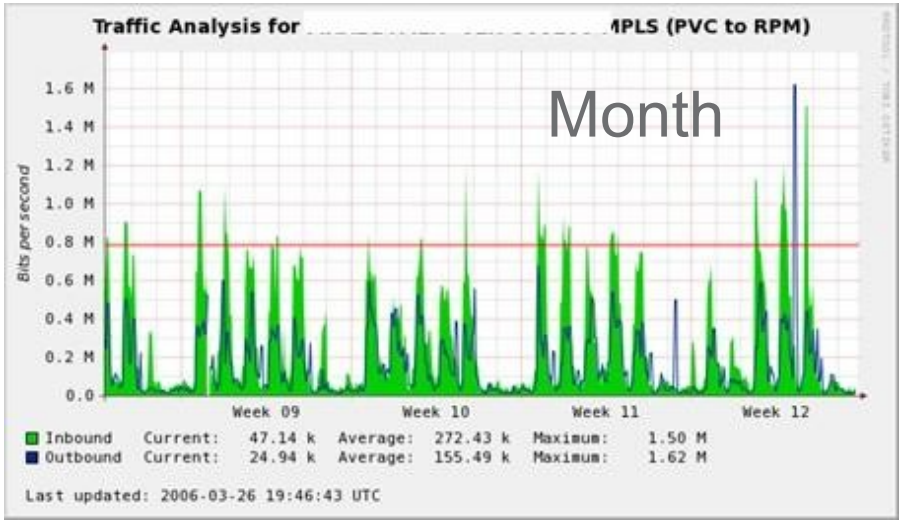
Performance with Lucent Vital suite / CACTI

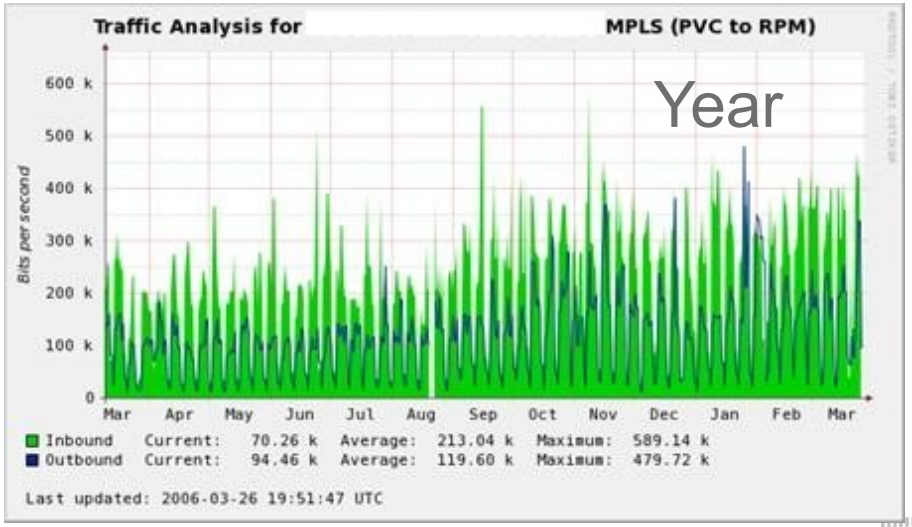
- One of the most important part of our work is troubleshooting are network performance problems.
- Collect variable information from device and store them for analyze (historical data)
- Fast analyze of network performance situations
  - On which point is network overload.
  - And what kind of traffic is overloading it.
- Proactive Information to prevent overload of WAN / LAN networks
- Lucent vital suite are the standard tool for Performance
- Can analyze QoS separately
- List of TOP talkers

Cacti – graphs









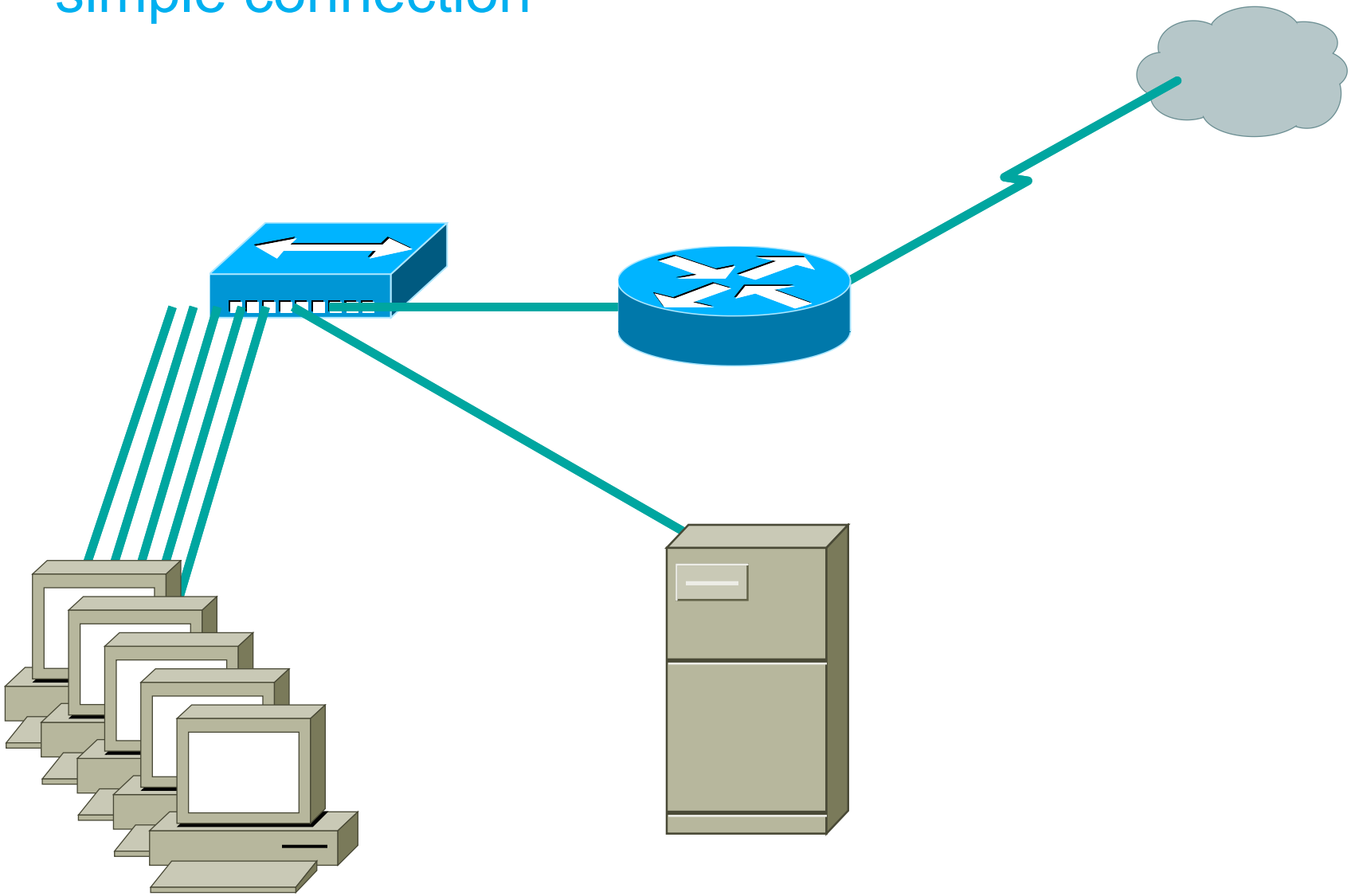
Evidence Databases & Other Databases

- All databases are bind
- Asset Evidence (eAMT)
- Central Evidence of all devices
  - Device type/hardware information
  - Location information
  - IP address, hostname, interfaces
  - Contacts for other support groups / provider / on-site support
  - Security Evidence with historical data
  - Etc.
- Evidence for Security findings
  - Keeps OS bugs
  - With each finding in configuration bug reports to responsible support

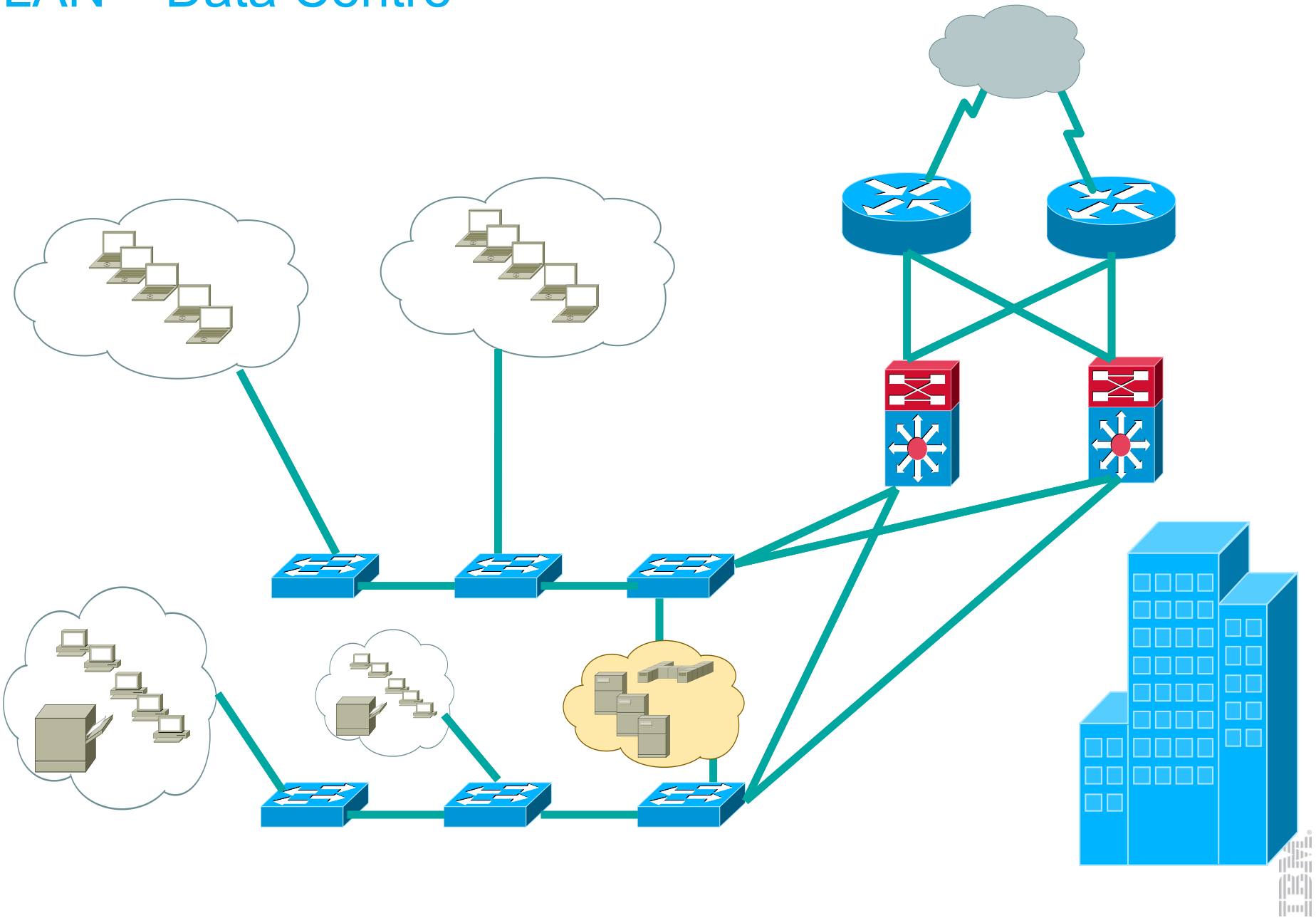
LAN Management

- LAN = Local Area Network
- Device's vendors
  - Cisco, Nortel, 3com, Alel, Allied Telesyn, Blue Coat, Digital, D-link, Edimax, Enterasys, HP, IBM, Intel, Intermac, Kingston, KTI Networks, LANart, LinkSys, Netgear, Nokia, Olicom, Planet, Symbol, Synoptics, Xtreme
  - **Migration of all existing platforms to Cisco for providing best centralized support**
- Device's categories
  - Firewalls
  - Routers
  - Switches

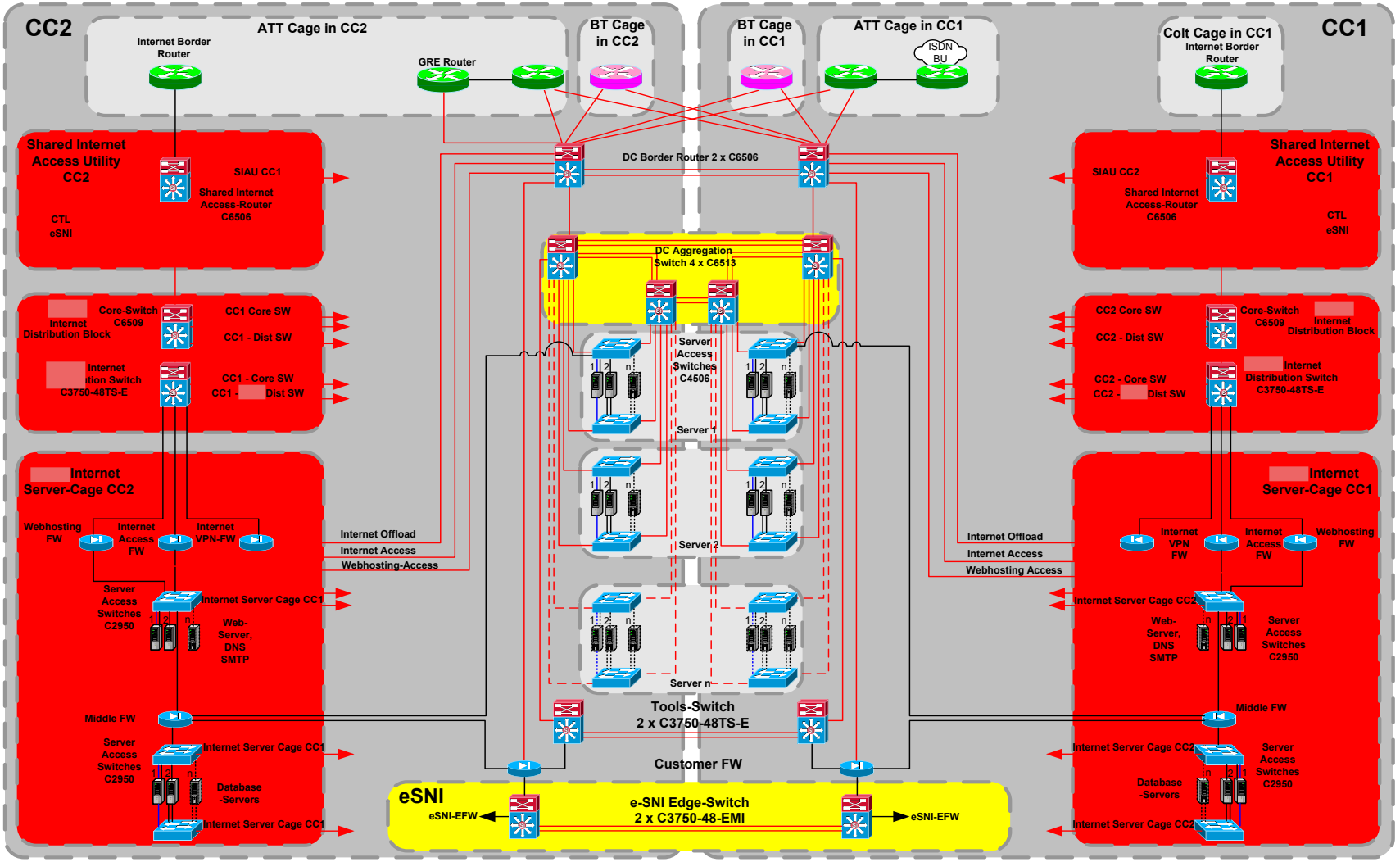
LAN – simple connection



LAN – Data Centre



Datacentre example



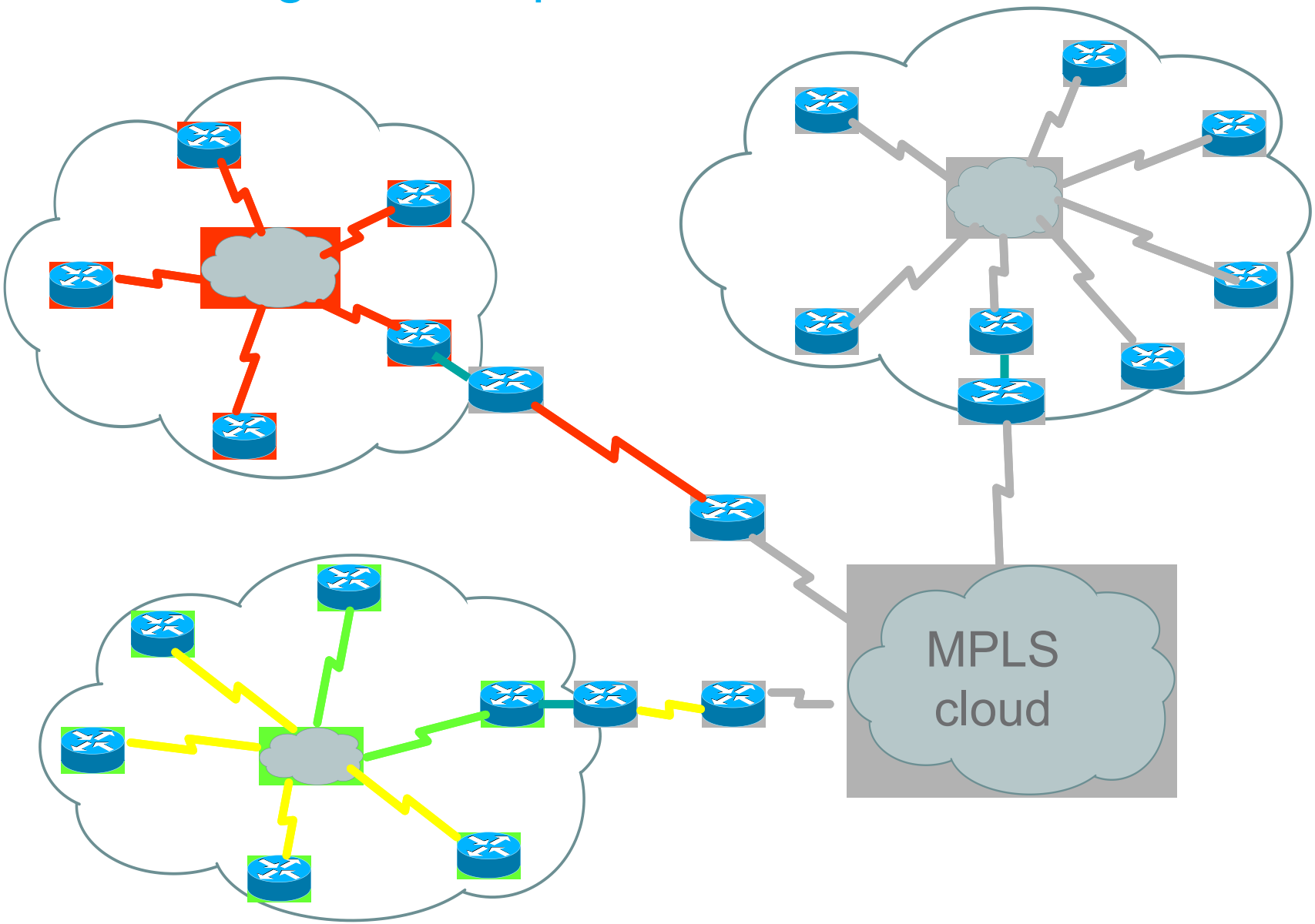
WAN Management

- WAN = Wide Area Network
- Used solutions
  - Leased line
  - ATM/Frame Relay
  - MPLS
  - DSL/ADSL/ISDN
  - Internet tunnel (iVPN)
- WAN lines are usually provided by external companies (BT, AT&T, HP, Colt…)
- NOC (1st level) is contact point between customer and provider

Today's trends for WAN

- MPLS = Multiprotocol Label Switching
- QoS = Quality of Service
- SaS = Solution as Service
- Cloud solutions

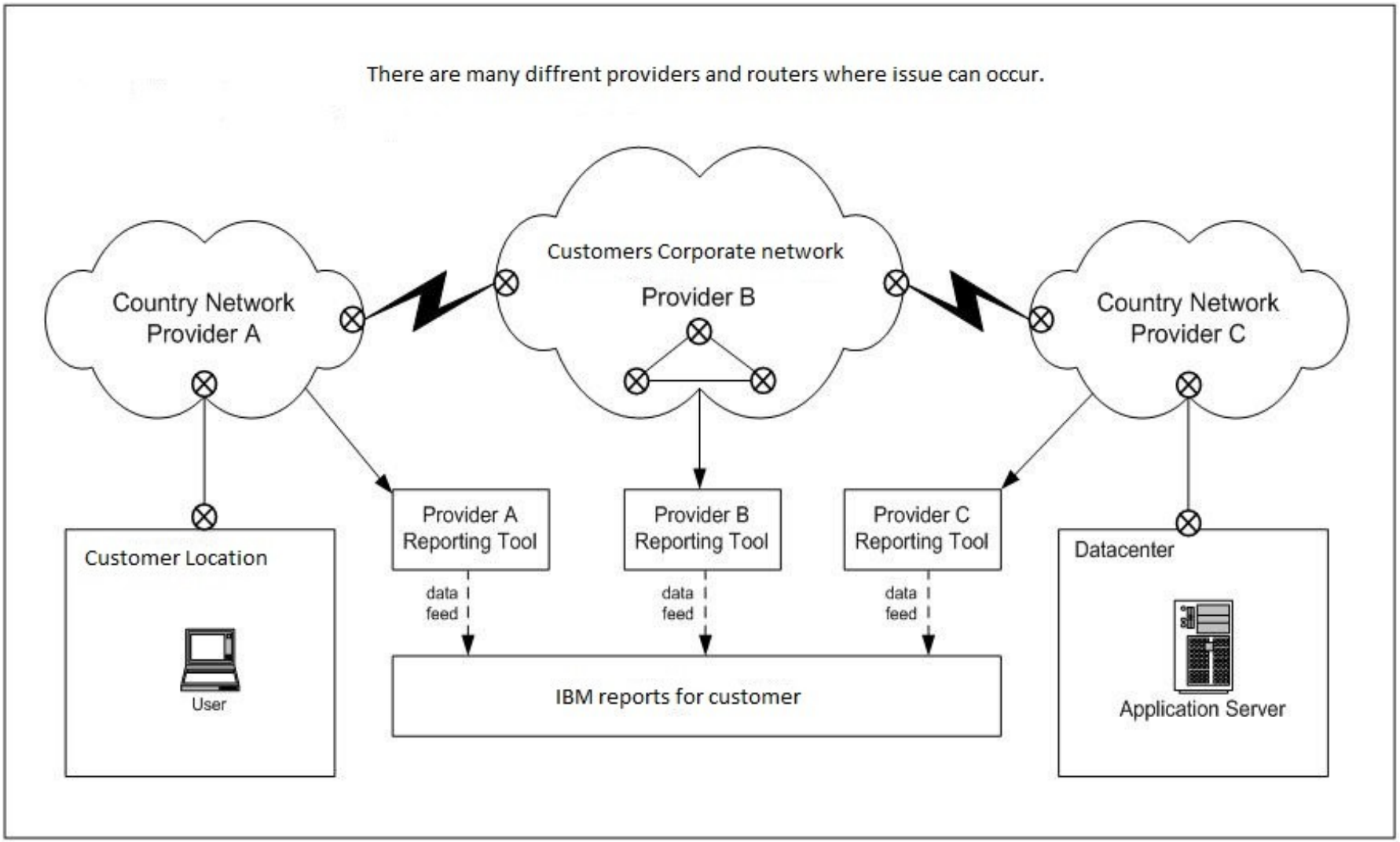
WAN Management – providers



WAN Specifications and requirements

- Setting QoS on WAN lines leads to better performance and usage of line
- 80 – 100 % WAN link utilization (“we pay 100, we use 100”)
- For monitoring of QoS we need good tools

WAN incident determination



Firewall

- Firewall types
- Standard used FW
- Checkpoint ProviderOne
- Usage of FW

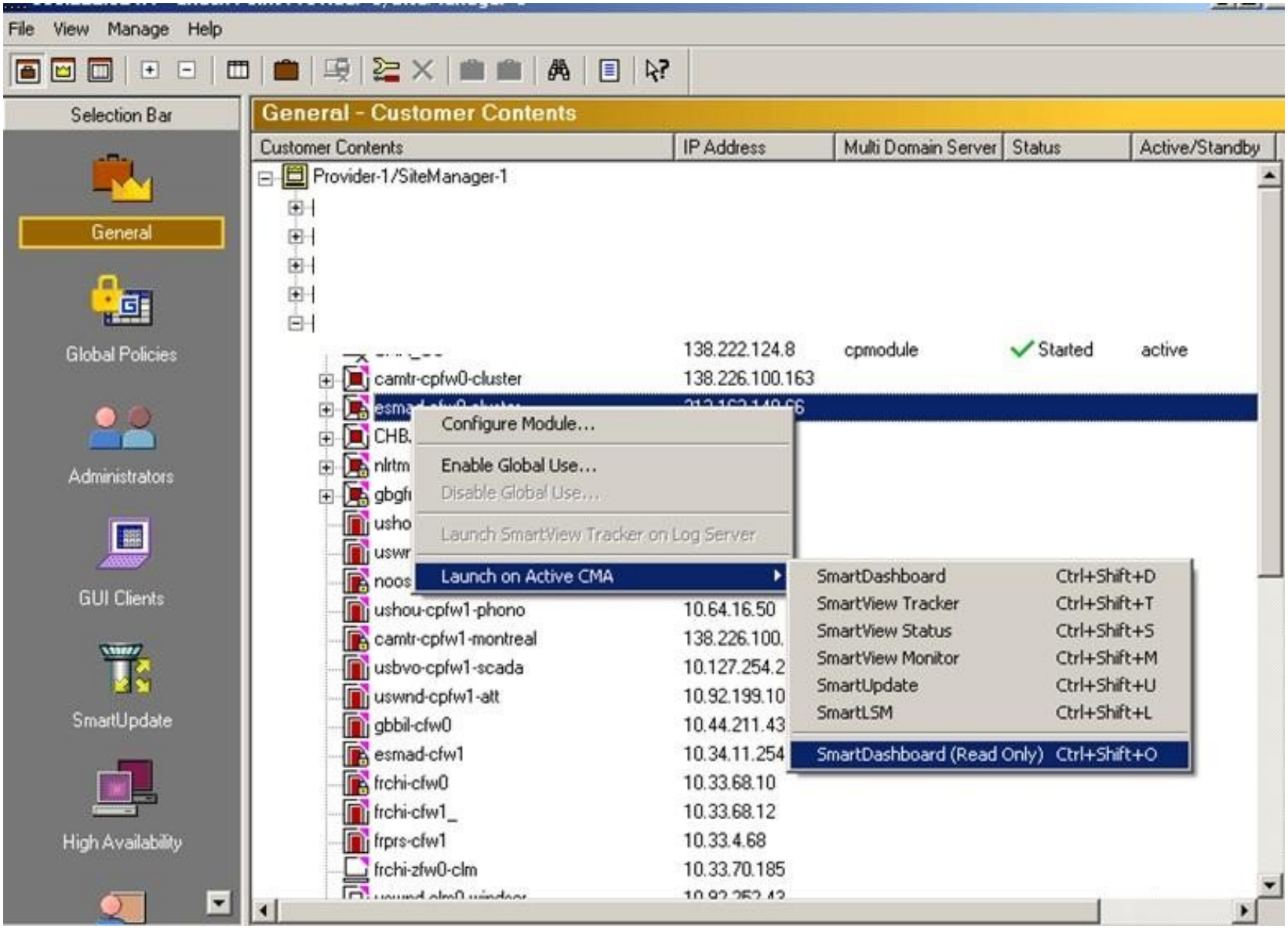
Types of existing Firewalls

- Software
  - Checkpoint Firewall-1 (diverse versions)
  - Cisco PIX
- Operating Systems
  - Checkpoint Secure Platform (SPlat)
  - Sun Solaris
  - Microsoft Windows
  - Linux
  - Nokia IPSO
  - Cisco PIX Firewall OS
- Hardware
  - PC Architecture
  - Sun
  - Nokia
  - Cisco PIX
  - IBM x-Series Servers

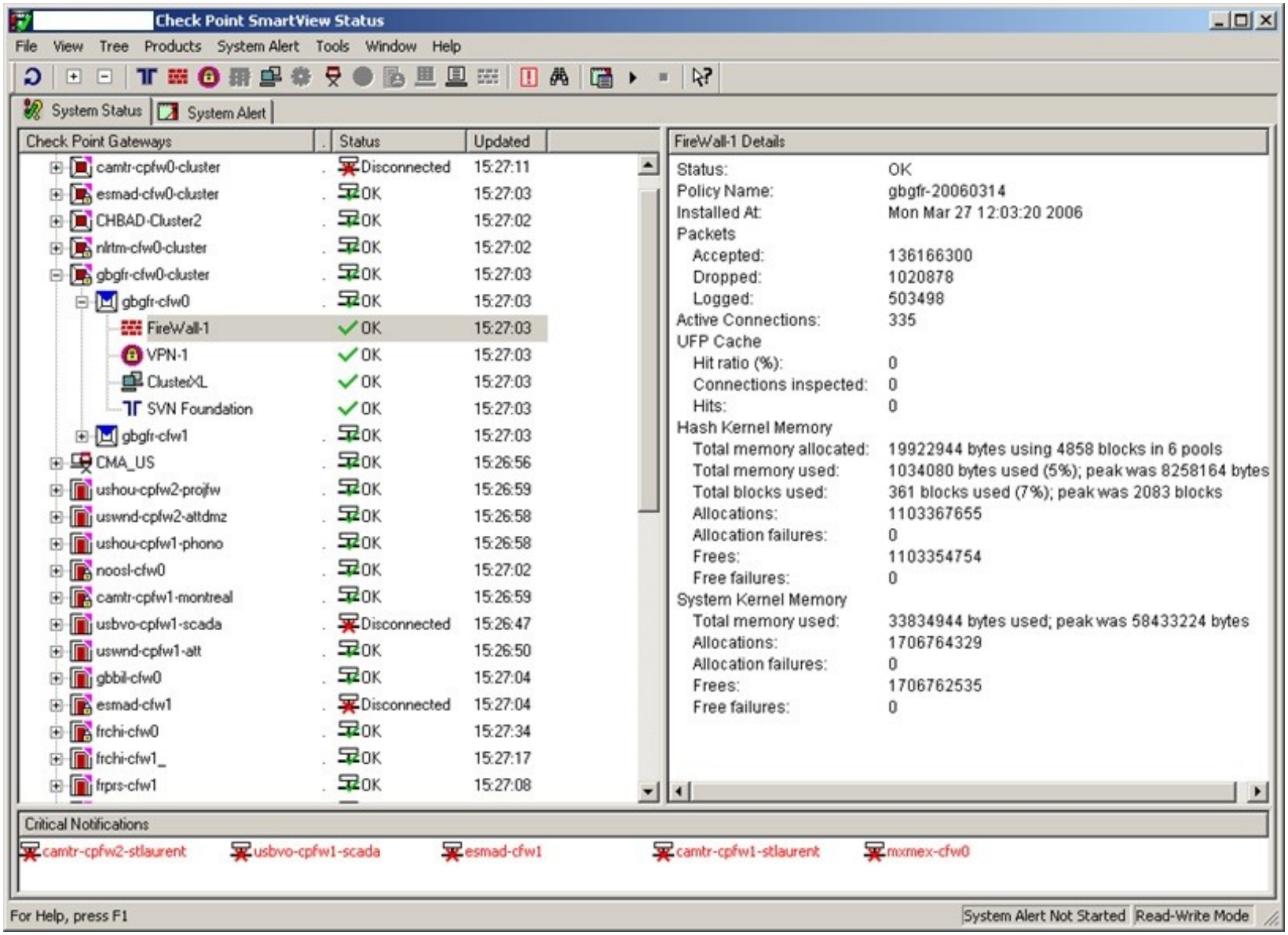
Checkpoint - ProviderOne

- Easy centralized management
- Saved all FW rule sets
- Central Logging
- Multi-platform management (Nokia, Splat)

Checkpoint - ProviderOne



Checkpoint - ProviderOne



Usage of Firewalls

- All network environments (Internet/DMZ/Corporate networks)
- Secure separation of networks
- Advanced security (not only ACLs – access control list)
- Implementation of statefull FW
- VPN implementation – VPN concentrators

IP Services (IPSE)

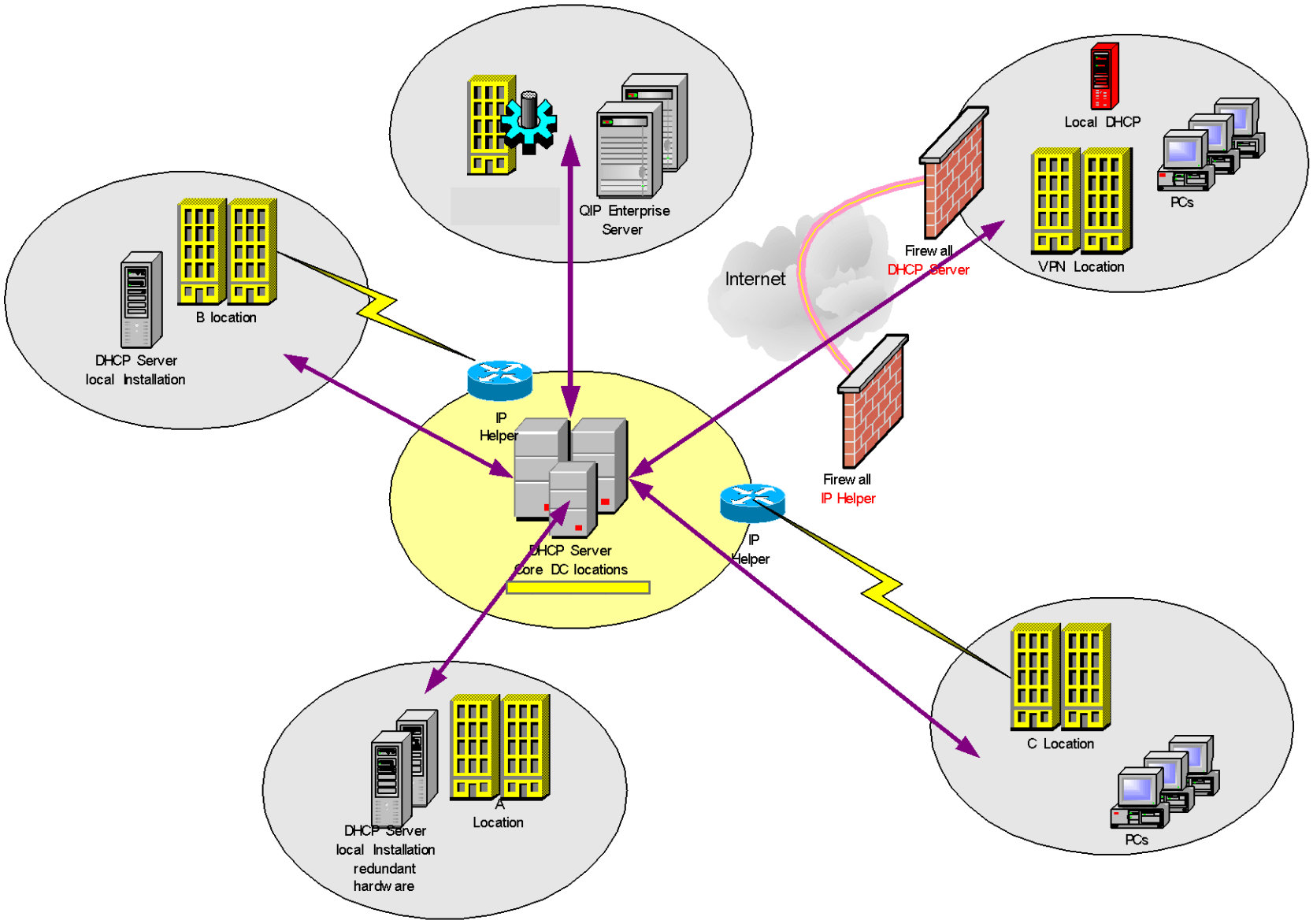
- DNS/DHCP
- NTP
- Proxy

QIP – central management for DNS/DHCP

- One central (with backup feature) QIP management server
- Structure-based implementation of QIP provides opportunity to use other QIP servers which are reporting to QIP management server
- Location types:
  - Less than 250 users DHCP – IP helper
  - Less than 499 users local DHCP server or IP helper
  - More than 500 users (Super location), local DHCP is provided by redundant servers
- Rules
  - Static Addresses for Servers and active network devices
  - Dynamic addresses for PCs and Printers

DNS management

- Central management of all DNS records
  - 2nd level domain (customer.com)
  - Sub-domains (location.customer.com)
- Domain management can be delegated to another server


QIP Enterprise Server
Local DHCP
PCs
VPN Location
Firew all
DHCP Server
Internet
B location
DHCP Server
local Installation
IP
Helper
Firew all
IP Helper
DHCP Server
Core DC locations
IP
Helper
C Location
PCs
A
Location
DHCP Server
local Installation
redundant
hardw are

NTP

- Time synchronization service
- NTP is installed on Intranet DNS servers
- NTP could be distributed for each domain to different servers (location based)
- More NTP for one location provide redundancy. Also internet backup is possible.

Proxy Solution

- In past main scope of proxy servers was to provide better usage of WAN lines (http proxy)
- Today's usage of Proxy servers is to provide secure and balanced connection
- We can recognize two types of proxies
  - Transparent (act as proxy for any traffic – mainly socks proxies)
  - Passive (use proxy feature only if application provide such functionality – http/ftp)

Network Security

- Configuration standards
- Checking or real configuration
- Actualized SW/HW
- User revalidation

Network Security – Standard configuration

- General Rules
- Applicable for different HW/OS
- Pre-defined standards pro Cisco, Nortel, IPSO and other platforms

Network Security – Checking actual configuration

- Correct setup for new device in network
- Revalidation is made at least each half of year
- Documentation of findings
- Corrective actions if applicable

Network security – Actual versions SW/HW

- Monitoring for new information/releases
  - Patches
  - New versions
- Risk management
- Planning upgrade

Typical problems LAN/WAN

- Slow network
  - LAN
  - Internet/WAN
- Device unreachable - LAN
- Location unreachable - WAN

Questions ?