



# SSO, DCS and NSD



Petr Habarta

SSO+DCS + NSD MU FIT



# Vladimir Vagner message

- He will sent mail with more informations about ITSM
- Will share link and PDF for every presentation
- Share terms for the excursion in IBM CIC

# About lector

- Dr. Ing. Petr Habarta, Ph.D.
- 11 years spent on multiple universities
- Over 9 years in IBM
- Positions - started as 1<sup>st</sup> level technician, 2<sup>nd</sup> level production control, incident coordinator, shift leader, senior incident manager, problem manager
- In IBM organization GTS division – service management
- Senior Problem Manager with focus on strategic data centers
- Lector of Service Management University
- Experience in IT and computers 30 years (14 years as professional, before it was only hobby)



# Agenda

- SSO – System server operations
- DCS – Desktop Client services
- NSD – Network services delivery
- Organization structure
- 1st level, 2nd level and 3rd level support
- Tickets and ticketing tools
- Monitoring tools
- Tivoli infrastructure
- LAN and WAN management
- Security



# SSO – System Server Operation

- Managing IT infrastructure
- Managing and maintenance of customer servers – remotely (server monitoring)
- Coverage of functions and availability of servers
- Backups and data restores
- Applications



# DCS – Desktop Client Support

- 2<sup>nd</sup> level helpdesk
- Image services
- Managing of issues
- Coordination of installations, changes etc. (SCCM services)
- Disaster recovery – backups & restores
- Centralized support of end user stations



## NSD – Network services delivery

- Focus only to network IT infrastructure
- Proactive monitoring of different tools. Coordinates incident resolution and communication.
- Require best knowledge of processes, tools usage and got global overview of systems.
- Necessary 24/7 support
- About 70% of issues are network based



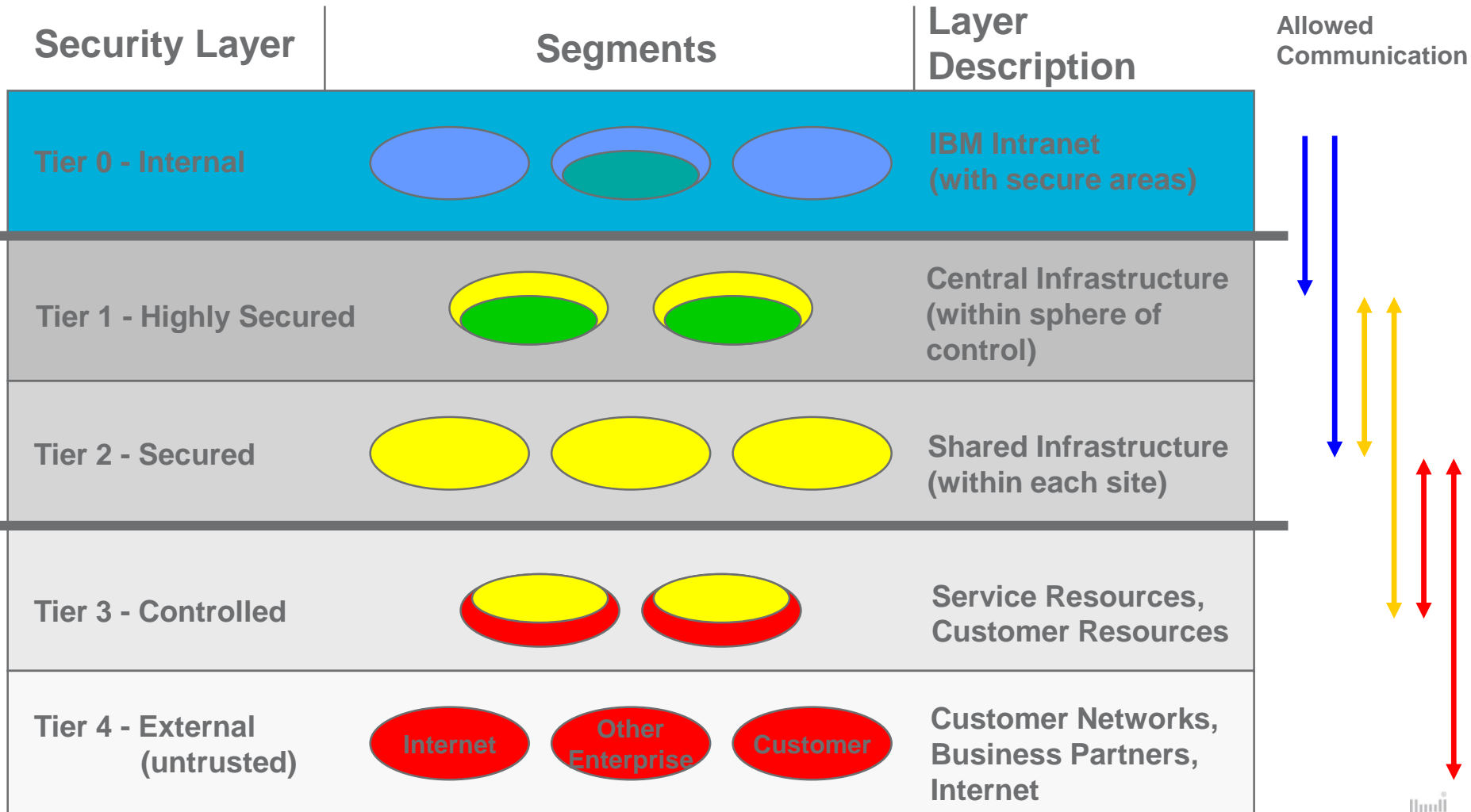
# What is Shared Network Infrastructure (SNI)?

- 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

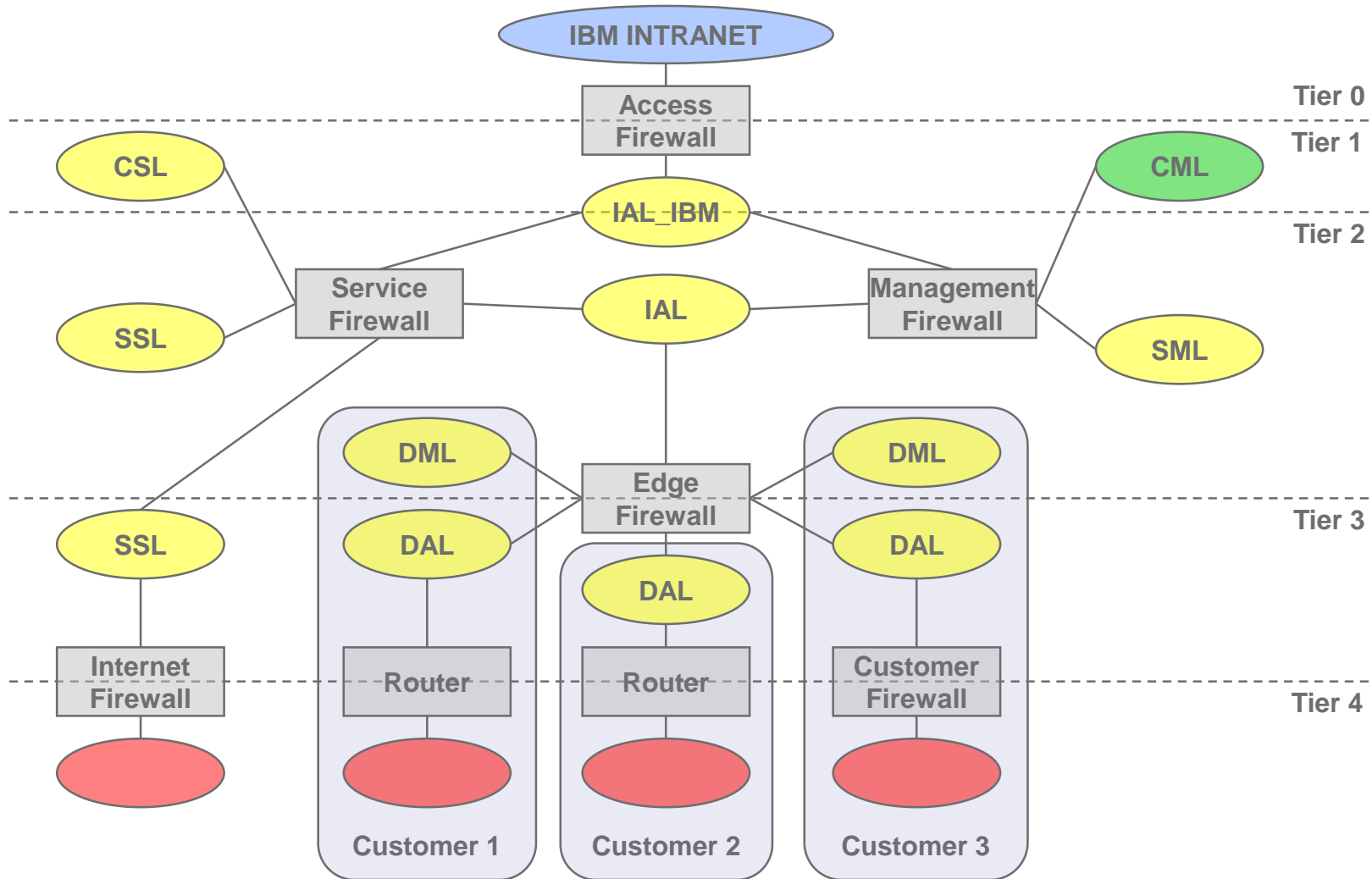




# Tier Definitions for SNI (e.g. eSNI “simplified”)



# 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



# Structure of teams

- 1<sup>st</sup> level support
  - Monitoring team
  - Basic and simple tasks
- 2<sup>nd</sup> level support
  - Managing more complex issues (installation, patching, changes etc.)
  - Application management
  - Divided based on their specialization – Windows, Unix, DB, Storage, DNS/DHCP, Firewalls etc.
- 3<sup>rd</sup> level support
  - Masters of their specialization
  - “Top guns” used for most critical and complex issues



# Ticketing tools

- Ticket is record (evidence & protocol) in ticketing tool – Basic communication tool
- Different names – Maximo, Remedy, Manage now, AOTS, HPSM, SNOW etc.
- 1 record = 1 ticket
- Advantages – every record is unique, simple escalation, recorded all activities and steps done

The screenshot displays a user interface for a ticketing system. On the left side, there are two main sections: 'Quick Insert' and 'Favorite Applications'. 'Quick Insert' contains four options: 'New Service Request' (with a document icon), 'New Incident' (with a warning triangle icon), 'New Problem' (with a warning triangle and circular arrows icon), and 'New Change' (with a document and circular arrows icon). 'Favorite Applications' lists various system components: 'Activities and Tasks', 'Service Requests', 'Incidents', 'Problems', 'Process Requests', 'Changes', 'Solutions', 'Configuration Items', 'Service Groups', 'Ticket Templates', and 'Job Plans'. On the right side, there are two sections: 'Bulletin Board' and 'Inbox / Assignments'. 'Bulletin Board' has a search bar labeled 'Subject' and a 'Filter' button. 'Inbox / Assignments' shows a 'Next Assignment Due: 4.4.16 10:02:00' and a list of tasks under the heading 'Description'. The tasks include 'Other approvers for Approval Level', 'Determine whether Change CH4009...', 'L3 - Approve or Reject Change CH4...', 'L4 - Approve or Reject the Change C...', and 'Provide Business Assessment Impa...'. A small logo is visible in the bottom right corner of the interface.

# Ticket tools

https://129.39.225.188 - ManageNow : R2 Problem Management - Problem Details - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Resolve Close Edit Transfer Assign Add Note Severity Target Date Team Info Outages Call Back Refresh Help Close Window

General Notes Associated Changes View Attachments

---

**Problem Details**

**Problem Number:** IBM-04348854      **Problem Abstract:** ██████████-CPPEA13:\*Attention\* Contact your hardware service

Problem Information	Contact Information	Problem Date Information
<b>Status:</b> TRANSFERRED	<b>Contact:</b> FLQFAAA1FCCIS01	<b>Occurred Date and Time:</b> SEP 17,2006 04:00:16
<b>Problem Type:</b> PROBLEM	<b>Organization:</b> FLQFAAA1FAURECI	<b>Open Date and Time:</b> SEP 17,2006 04:00:08
<b>Call Code:</b> Outgoing Call	<b>Last Name:</b> CGC IS COMMAND CENTER	<b>Original Target Date and Time:</b> SEP 24,2006 04:00:16
<b>Severity:</b> 3	<b>First Name:</b> ██████████	<b>Current Target Date and Time:</b> SEP 24,2006 04:00:16
<b>Original Severity:</b> 3	<b>Middle Name:</b>	<b>Resolved Date and Time:</b>
<b>System:</b> FLQ_COMMON-APP	<b>External Phone:</b> 1	<b>Close Date and Time:</b>
<b>Component:</b> OPERATINGSYS	<b>Alternate Contact:</b>	<b>Duration:</b>
<b>Item:</b> OS/400	<b>Department:</b> CC	<b>Call Back Date and Time:</b>
<b>Module:</b> ERROR-MESG	<b>Division:</b> NA	<b>Reminder Date and Time:</b>
<b>User:</b>	<b>Site:</b> FLQFA-IBM COMMAND CENTER	
<b>Group:</b> FLQ-IFRISTI	<b>Address:</b> IBM COMMAND CENTER	<b>Bridging Information</b>
<b>Owning User:</b>	<b>Floor:</b>	Not Bridged
<b>Owning Group:</b>	<b>Location:</b> 000000000131954	<b>Bridge Ticket Number:</b>
<b>Resolver User:</b>	<b>City:</b> FRANCE	
<b>Resolver Group:</b>	<b>State:</b> FRANCE	
<b>Reporter User:</b> CZZJUC01		
<b>Last Name:</b> ██████████	<b>Zip:</b> NA	
<b>First Name:</b> ██████████		
<b>Reporter Group:</b> FLQ-ICZOPIOCALM		
<b>Cause Change Number:</b>		
<b>Cause Code:</b>		
<b>Node:</b>	<b>Additional Contact Information</b>	<b>Lock Status</b>
<b>Number Times Reassigned:</b> 1	No Additional Contact Information	<b>Locked By:</b>
<b>Duplicate Problem Number:</b>		<b>User:</b>

---

**Description**

AA1 - ██████████ MsgID:CPPEA13:\*Attention\* Contact your hardware service provider.  
 Receive date . 2006/09/17 03:36:14

A critical system hardware problem has occurred. Critical Message Handler has been run.  
 Receive date . 2006/09/17 03:36:16

Done Internet

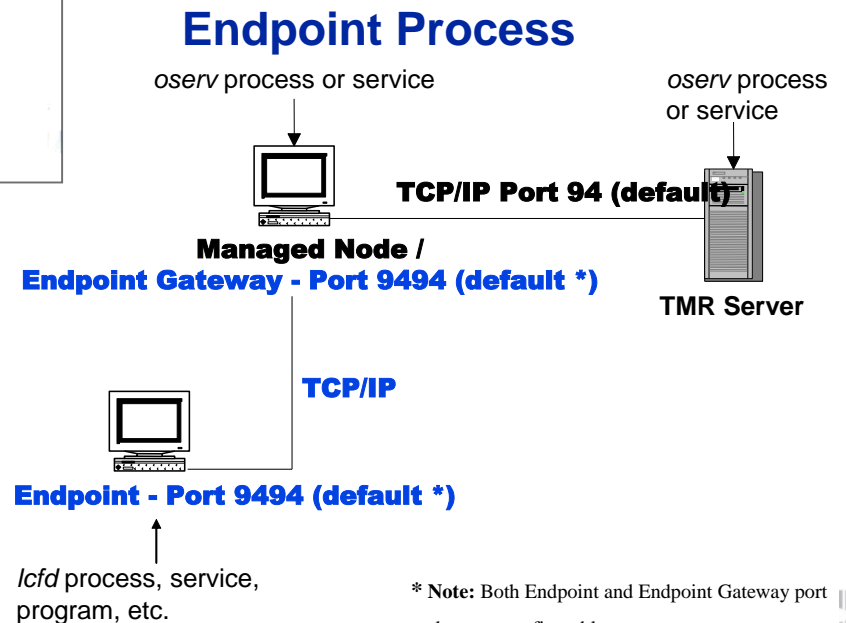
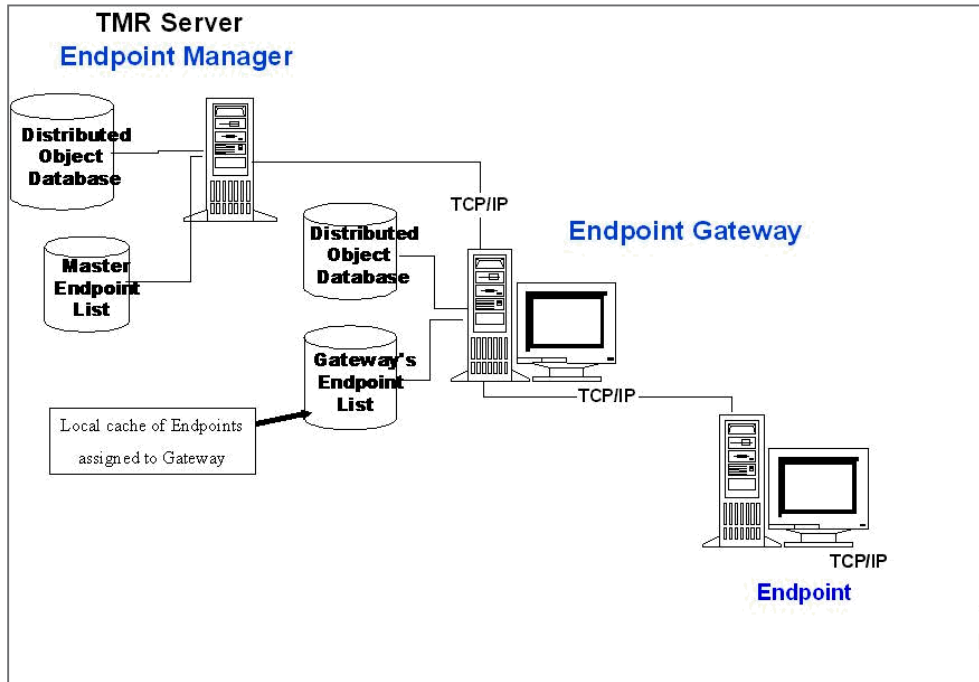


# Monitoring - Tivoli

- Tivoli is IBM product
- Set of tools with many features
- One of them is monitoring of OS, SW, HW, NSD etc.



# Tivoli monitoring infrastructure



\* Note: Both Endpoint and Endpoint Gateway port values are configurable.



# Tivoli Enterprise Console - TEC

Tivoli Enterprise Console

3 2 5 2 3 1

Time Received	Classes	Hostname	Severity	Status	Message	Sub-source	Sub-origin
May 31, 2006 22:43:04 UTC	NT_Monitored_Logs_Report	TIVOLIUSER	Unknown	Open	NT_Log_Space_Low	Primary:TIVOLIUSER:NT	Application
May 31, 2006 23:05:30 UTC	NT_Event_Log	BIGGEST	Unknown	Open	NT_Service_Error	Primary:BIGGEST:NT	Error
May 31, 2006 23:19:11 UTC	ITM_Generic	TIVOLIUSER	Minor	Open	TEMS <TIVOILUSER> restarted	Primary:TIVOLIUSER:NT	
June 4, 2006 1:45:34 UTC	ITM_NT_Physical_Disk	TIVOLIUSER	Warning	Reopened	NT_Physical_Disk_Busy_Warning	Primary:TIVOLIUSER:NT	C:
June 4, 2006 2:15:17 UTC	NT_Monitored_Logs_Report	TIVOLIUSER	Unknown	Open	NT_Log_Space_Low	Primary:TIVOLIUSER:NT	System
June 4, 2006 2:21:34 UTC	ITM_NT_Process	BIG	Critical	Open	CPU_Critical(%_Processor_Time)>=90	Primary:BIG:NT	java
June 4, 2005 2:47:55 UTC	ITM_NT_Process	BIG	Critical	Open	CPU_Critical(%_Processor_Time)>=90	Primary:BIG:NT	oserv
June 4, 2005 3:05:58 UTC	ITM_NT_Process	BIG	Critical	Acknowledged	CPU_Critical(%_Processor_Time)>=90	Primary:BIG:NT	services
June 4, 2005 4:55:40 UTC	TEC_ITS_NODE_STATUS	Little	Harmless	Open	Node Up	NET	
June 4, 2005 5:22:16 UTC	TEC_ITS_NODE_STATUS	Little	Warning	Open	Node Down	NET	
June 4, 2005 5:37:18 UTC	TEC_ITS_NODE_STATUS	Little	Warning	Open	Node Down	NET	
June 4, 2005 7:15:24 UTC	TEC_ITM_ConfigSys	Accounts	Warning	Open	Sending updates		
June 4, 2005 9:36:25 UTC	EVENT		Fatal	Closed	Outage		
June 5, 2005 0:30:00 UTC	TEC_Stop	Backroom	Minor	Open	TEC Event Server shut down		
June 5, 2005 8:01:02 UTC	TEC_Start	Backroom	Harmless	Open	TEC Event Server initialized		
June 6, 2005 21:59:05 UTC	TEC_Generic	Backroom	Warning	Open	Resync events		

Acknowledge Close Details Information



# Netcool monitoring tool

Netcool/OMNIBUS Event List : Filter="Node-RED", View="Default"

File Edit View Alerts Tools Help

Node-RED Default Top [ OFF ] 0

Node	Alert Group	AlertKey	Demand	Summary	Last Occurrence
National Grid	Spike Alarm	NI_to_GB		Alert: NI_to_GB transfer has changed by more than 5%	28/02/14 11:35:56
National Grid	Spike Alarm	Netherlands_to_GB		Alert: Netherlands_to_GB transfer has changed by more than 5%	28/02/14 11:35:56
National Grid	Trend Warning	demand		Warning: Demand has risen by more than 5% in the last thirty minutes	27/02/14 16:55:47
National Grid	Spike Alarm	France_to_GB		Alert: France_to_GB transfer has changed by more than 5%	27/02/14 16:35:46
National Grid	Threshold Breach	frequency		Warning: Frequency below 50Hz	28/02/14 11:35:56
National Grid	Trend Warning	demand		Warning: Demand has been rising for the last thirty minutes	27/02/14 18:25:48
National Grid	Trend Warning	demand		Warning: Demand has been rising for the last thirty minutes	27/02/14 17:55:47
National Grid	Trend Warning	demand		Warning: Demand has been rising for the last thirty minutes	27/02/14 17:25:49
National Grid	Trend Warning	demand		Warning: Demand has been rising for the last thirty minutes	27/02/14 16:10:46
National Grid	Trend Warning	demand		Warning: Demand has been rising for the last thirty minutes	24/02/14 08:01:37
National Grid	Trend Alarm	NI_to_GB		Information: NI_to_GB transfer spike of more than 5% has reduced	23/02/14 18:34:23
National Grid	Spike Alarm	Netherlands_to_GB		End of Alert: Netherlands_to_GB transfer spike of more than 5% has stayed at new value	28/02/14 11:05:54
National Grid	Spike Alarm	NI_to_GB		End of Alert: NI_to_GB transfer spike of more than 5% has stayed at new value	28/02/14 10:50:53
National Grid	Threshold Breach	frequency		Clear: Frequency now above 50Hz	27/02/14 18:40:48
National Grid	Spike Alarm	France_to_GB		End of Alert: France_to_GB transfer spike of more than 5% has returned to base value	27/02/14 17:05:47
National Grid	Trend Warning	demand		Information: Demand has been falling for the last thirty minutes	27/02/14 14:55:47

5 0 1 6 4 0 All Events

No rows modified. 28/02/14 11:41:06 netcool NCOMS[PRJ]

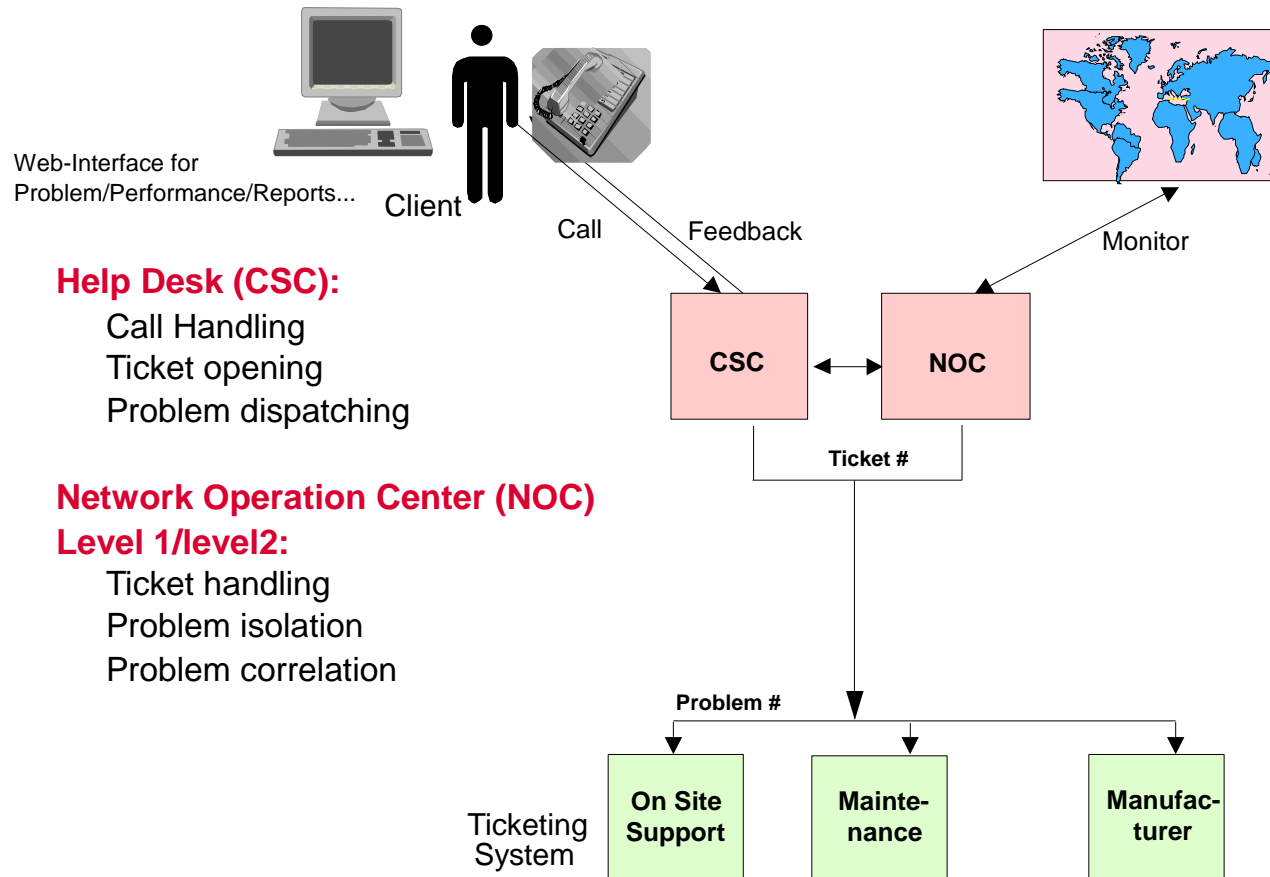


# Tivoli features

- TEC – Tivoli Enterprise Console
- TSM – Tivoli Storage Manager
- TWS – Tivoli Workload Scheduler
- Tivoli Configuration Manager
- Tivoli License Manager
- Tivoli Access Manager



# Organization Structure – Network management GNMC model



# 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

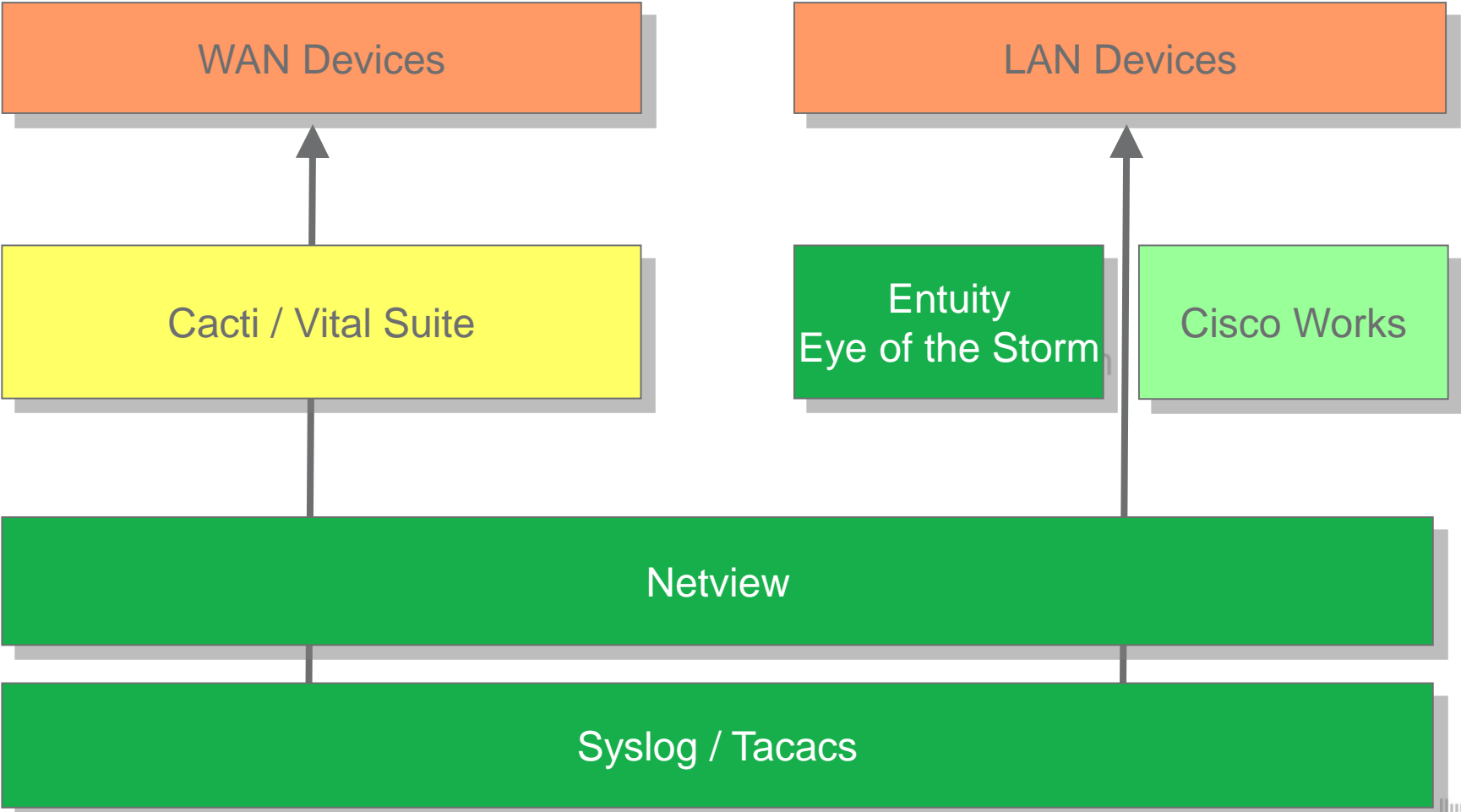


# Network Management Toolset

- 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...)





# Tivoli Netview – Event Browser

Tivoli NetView -- Administrator:Unrestricted -- http:138.222.124.36:8080

File Object Monitor Test Tools Window Help

Event Browser

File Filter View Event Tools

All Events

Time	Node	Description	Severity
1.2.06 13:49		Interface DEC down.	Critical
1.2.06 13:50		1: RIPQ-ERROR 'Host:localhost - 2141 messages idle'-- 2:FMT ERROR: accessing element #2, only 1 av...	Warning
1.2.06 13:51		1: SPAMQ-SLS-DOWN 'Host:localhost - Unable to connect SLS server.'-- 2:FMT ERROR: accessing eleme...	Major
1.2.06 13:52		Latency packet loss - Source: USABBZWINCT01H-A40151-USABBZPRINJ01R-S0101 512k PVC to Princet...	Critical
1.2.06 13:54		1: SPAMQ-SLS-UP 'Host:localhost - SLS server is available'-- 2:FMT ERROR: accessing element #2, only ...	Cleared
1.2.06 13:55		INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - smtp01.de.abb.co...	Warning
1.2.06 13:55		1: SPAMQ-SLS-DOWN 'Host:localhost - Unable to connect SLS server.'-- 2:FMT ERROR: accessing eleme...	Major
1.2.06 13:58		INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - mail.abb.ru, Port - 25'	Warning
1.2.06 13:58		1: SPAMQ-SLS-UP 'Host:localhost - SLS server is available'-- 2:FMT ERROR: accessing element #2, only ...	Cleared
1.2.06 13:59		INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - smtp01.de.abb.co...	Warning
1.2.06 13:59		INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - mail.at.abb.com, P...	Warning
1.2.06 14:00		Interface 138.221.99.4 down.	Critical
1.2.06 14:00		Node Down.	Critical
1.2.06 14:00		Interface DEC up.	Cleared
1.2.06 14:00		Interface 138.221.99.4 up.	Cleared
1.2.06 14:00		Node Up.	Cleared
1.2.06 14:01		1: RIPQ-ERROR 'Host:localhost - 2150 messages idle'-- 2:FMT ERROR: accessing element #2, only 1 av...	Warning
1.2.06 14:01		1: VFQ-DOWN 'Host:localhost - VFQ Test Failed. Monitor port not responding.'-- 2:FMT ERROR: accessing ...	Major
1.2.06 14:05		Interface 10.31.96.111 down.	Critical
1.2.06 14:05		Node Down.	Critical
1.2.06 14:05		Interface DEC up.	Cleared
1.2.06 14:05		Interface 10.31.96.111 up.	Cleared
1.2.06 14:05		Node Up.	Cleared
1.2.06 14:05		Interface DEC down.	Critical
1.2.06 14:07		Latency packet loss - Source: ESABBYMAD--01R-T8-DEABBYEHG--03R_latency_loss object has been no l...	Cleared
1.2.06 14:08		1: SPAMQ-SLS-DOWN 'Host:localhost - Unable to connect SLS server.'-- 2:FMT ERROR: accessing eleme...	Major

Total: 102 Displayed: 102 Selected: 1

Submap Explorer - default [Read Only] - [ABB-Asia]

# 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

ent Viewer

View Tools Window Help

138.222.124.44

Roots://138.222.124.44/ABB Spain/Switches/10.34.17.41/

ABB Spain

General Ports Applications VLANs Extended Info Chassis Data

10.34.17.41

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				

10.34.11.200

10.34.24.240

10.34.24.242

10.34.28.238

10.34.28.240

10.34.33.112

10.34.36.243

10.34.36.245

10.34.36.246

10.34.36.247

10.34.36.244

10.34.69.13

10.34.40.20

VLANs

Switzerland

UK

ional

ional Infrastructure

\_forwarding

cz60070@138.222.124.44



# Entuity Eye of the Storm – device report

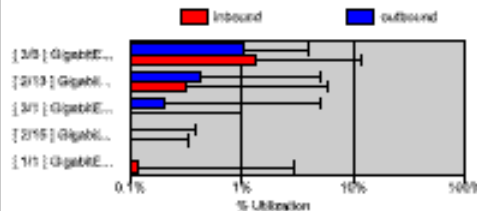
**10.49.29.130**

**Cisco Internetwork Operating System Software IOS (tm)  
c6sup1\_rp Software (c6sup1\_rp-DSV-M), Version  
12.1(23)E2, RELEASE SOFTW**

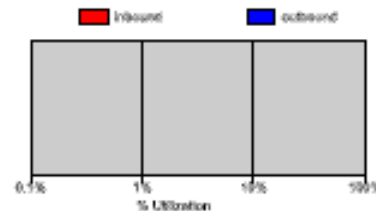
Speed	Total	Spare
10/100Mb	48	43 (90%)
1Gb	66	18 (27%)

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

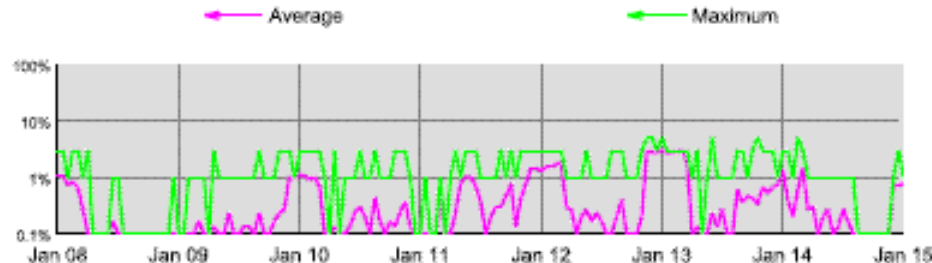
Top trunk ports



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 (62 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)	Top problem WAN links (sorted by downtime)		Downtime (minutes)
138.228.192.222 : [ 22 ] DEABBYEHG-03R-T65002-SGABBY-S1		15	155.7minutes	10.49.127.199 : [ 124 ] Vlan120		39,600minutes
138.228.192.222 : [ 17 ] att-unman DEABBYEHG-03R-T9-ZAABBYJNB-01		13	1,717.6minutes	10.49.240.3 : [ 208 ] Vlan51		39,600minutes
138.228.192.222 : [ 12 ] DEABBYEHG-03R-T4-CZABBYBRQ-01		10	340.6minutes	10.49.240.2 : [ 107 ] Vlan1		39,600minutes
138.228.192.222 : [ 19 ] DEABBYEHG-03R-T11-CHABBYBAD-01		8	21.8minutes	10.49.127.75 : [ 135 ] Vlan101		39,600minutes
138.228.192.222 : [ 15 ] DEABBYEHG-03R-T7-PTABBYPCS-01		7	26minutes	10.49.240.3 : [ 203 ] Vlan1		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

**Device Center**

DEVICE: 10.132.0.35

**Summary**

Device IP Address	10.132.0.35
Device Type	Cisco 3750 Stack
24-hour Change Audit Summary	Number of records: 0
Inventory Last Collected Time	May 27 2006 08:18:09 CEST
Configuration Last Archived Time	May 16 2006 12:07:05 CEST
24-hour Syslog Message Summary	Emergencies: 0 Alerts: 0 Critical: 0 Errors: 0 Warnings: 0 Notifications: 0 Informational: 0
CDP Neighbors	10.152.190.2

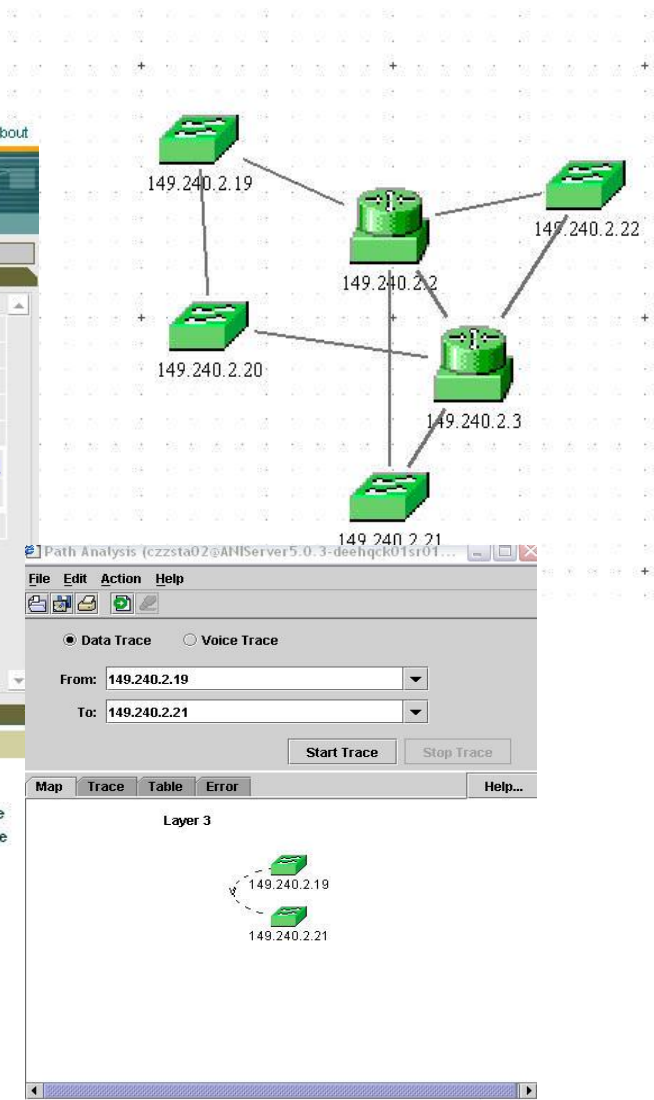
**Functions Available**

Tools	Reports	Management Tasks
<ul style="list-style-type: none"><li>Management Station to Device</li><li>Ping</li><li>Telnet</li><li>Trace Route</li><li>Edit Device Credentials</li><li>Packet Capture</li><li>SIIMP Set</li><li>SIIMP Walk</li></ul>	<ul style="list-style-type: none"><li>Change Audit Report</li><li>Credential Verification Report</li><li>Detailed Device Report</li><li>Syslog Messages Report</li><li>Switch Port Usage Report - Recently Down</li><li>Switch Port Usage Report - Unused Down</li></ul>	<ul style="list-style-type: none"><li>Add Images to Software Repository</li><li>Analyze using Cisco.com Image</li><li>Analyze using Repository Image</li><li>Check Device Credential</li><li>Distribute Images</li><li>Edit Config</li><li>Run Show Command</li></ul>

**CiscoView (DEEHQCK01SR0136)**

Device Name/IP: 149.240.50.95

Catalyst 2950 SERIES



# Cisco Works – example of report

Resource Manager Essentials - Microsoft Internet Explorer

File Edit View Favorites Tools Help

**Reloads Report - 1 Day**

Back Close Save As CSV Format Reports 1 Day

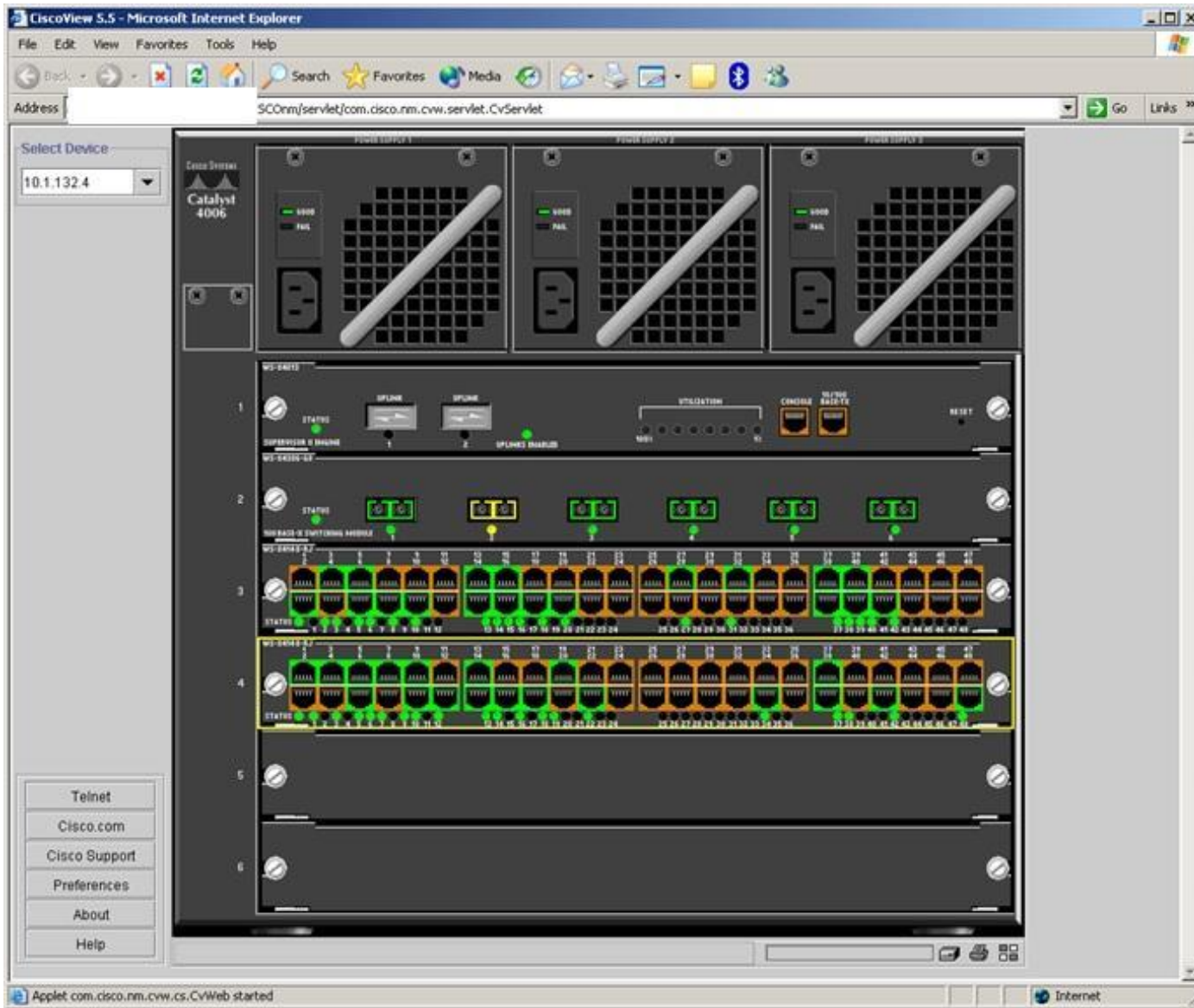
<u>Device Name</u>	<u>Device Type</u>	<u>Reload Reason</u>	<u>Reload Time</u>
<a href="#">10.49.84.132</a>	Catalyst IOS 3508	power-on	25 Mar 2006 22:38:14 MEST
<a href="#">10.49.84.133</a>	Catalyst IOS 3548	power-on	25 Mar 2006 21:59:02 MEST
<a href="#">10.49.84.134</a>	Catalyst IOS 3548	power-on	25 Mar 2006 21:50:20 MEST
<a href="#">10.49.84.135</a>	Catalyst IOS 3548	power-on	25 Mar 2006 21:57:19 MEST
<a href="#">10.49.84.140</a>	Catalyst IOS 3548	Reload !! Warning:Possible Sysuptime wrap detected	26 Mar 2006 00:02:02 MEST
<a href="#">10.49.84.143</a>	Catalyst IOS 3524	Reload !! Warning:Possible Sysuptime wrap detected	26 Mar 2006 00:07:39 MEST

Generated: 26 Mar 2006 15:14:12 MEST  
Cisco Systems, Inc. ©

Done Internet



# Cisco Works – Cisco View

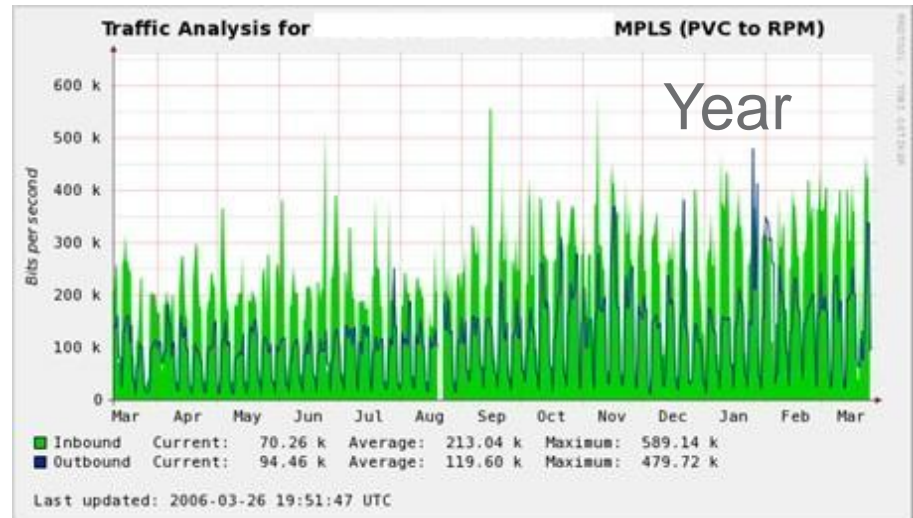
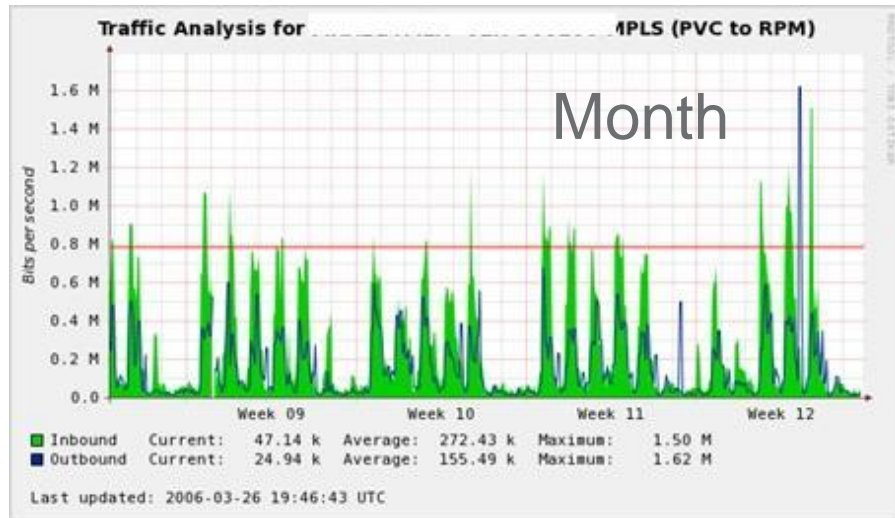
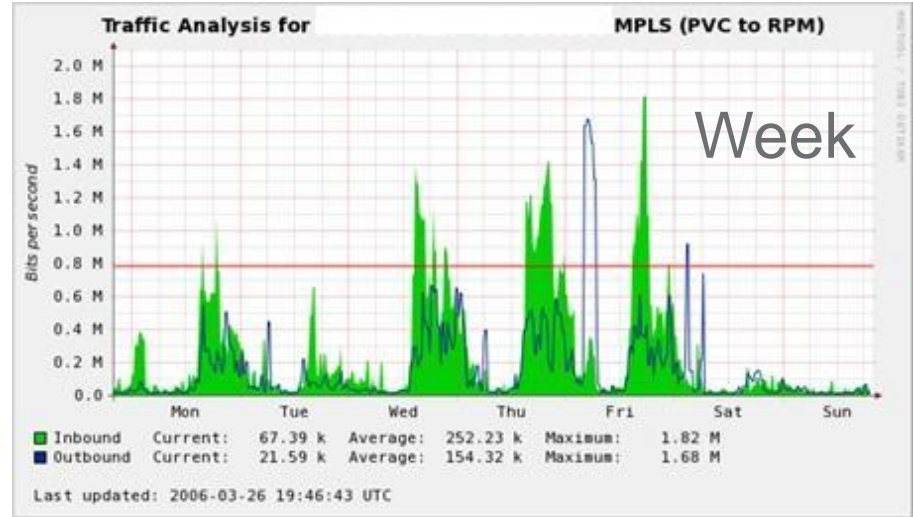
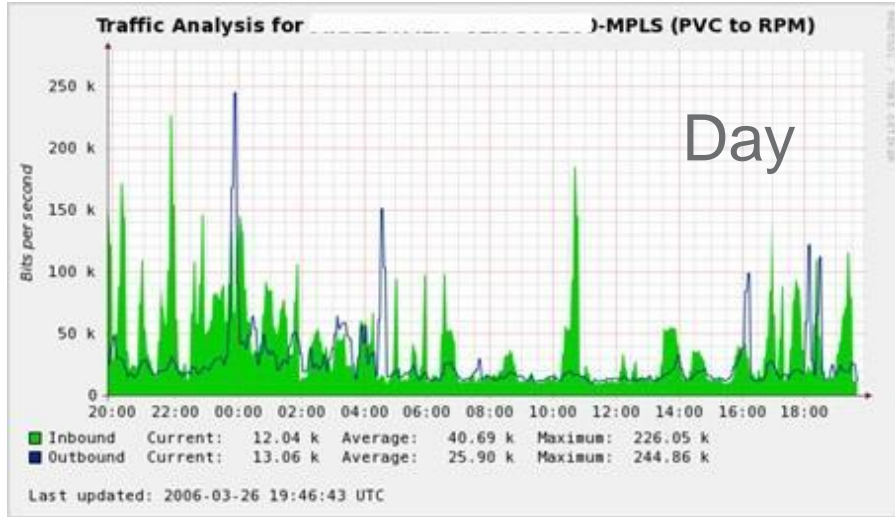


# Performance with Lucent Vital suite / CACTI

- 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

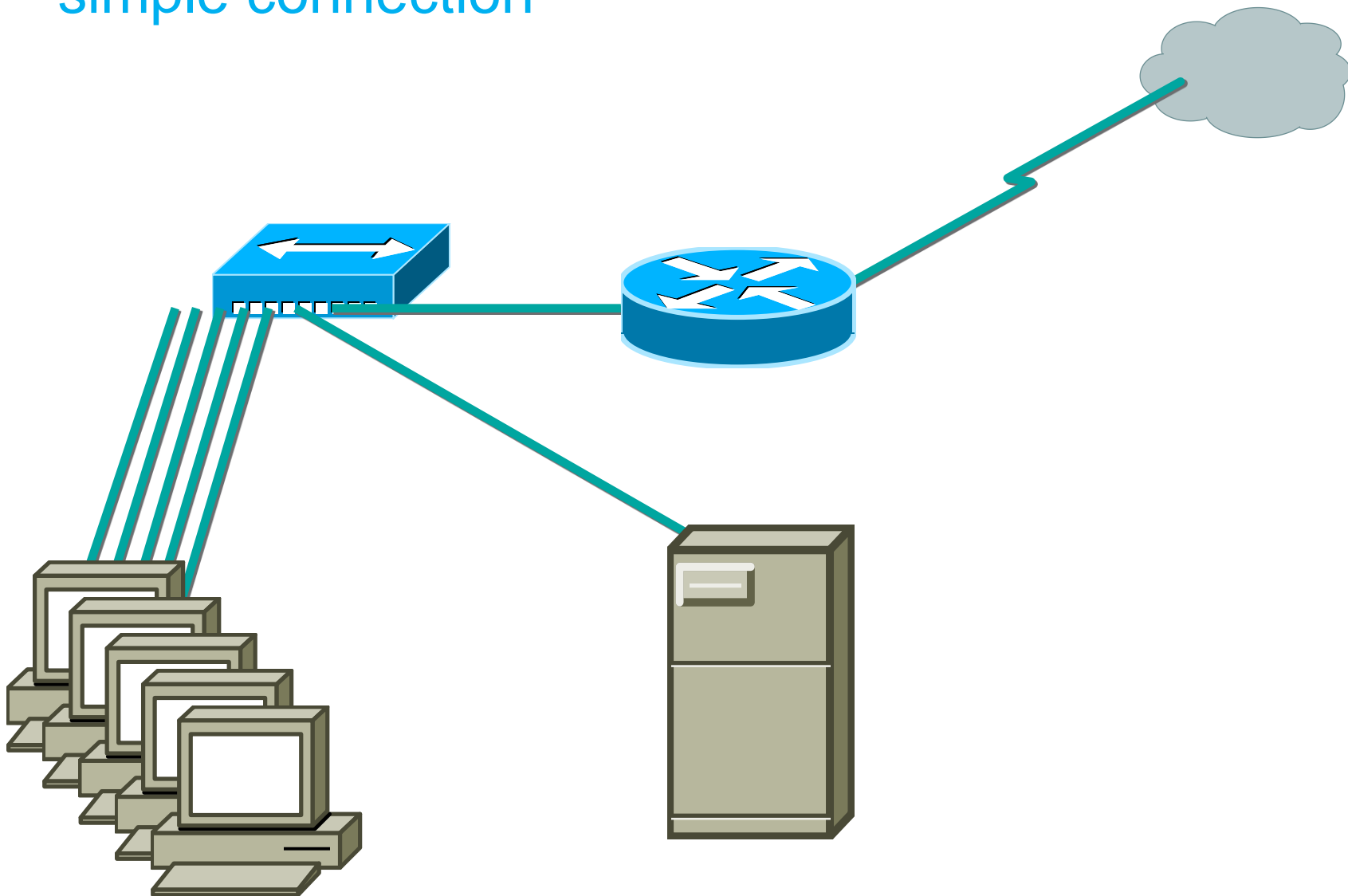


# LAN Management

- 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

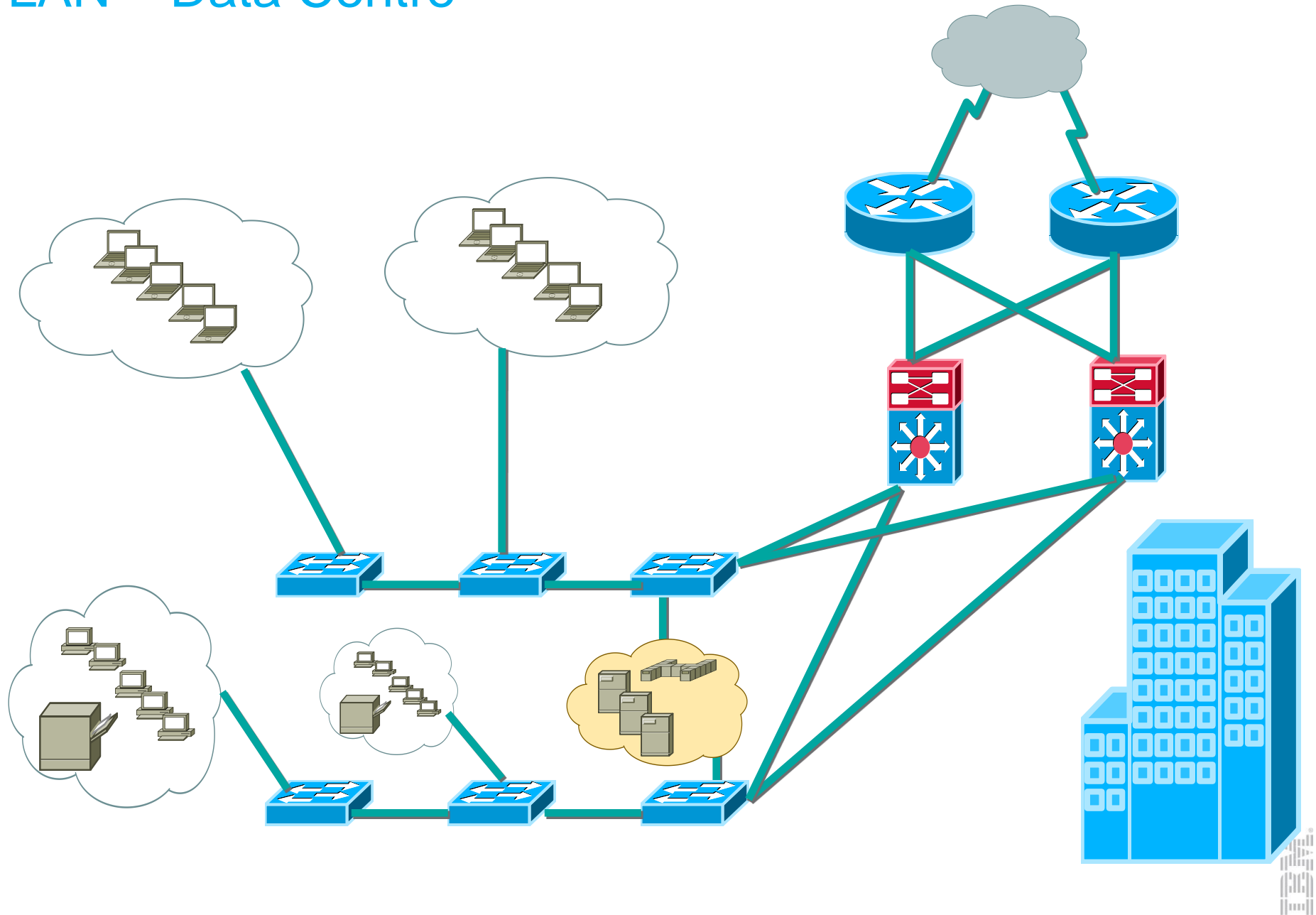


# LAN – simple connection

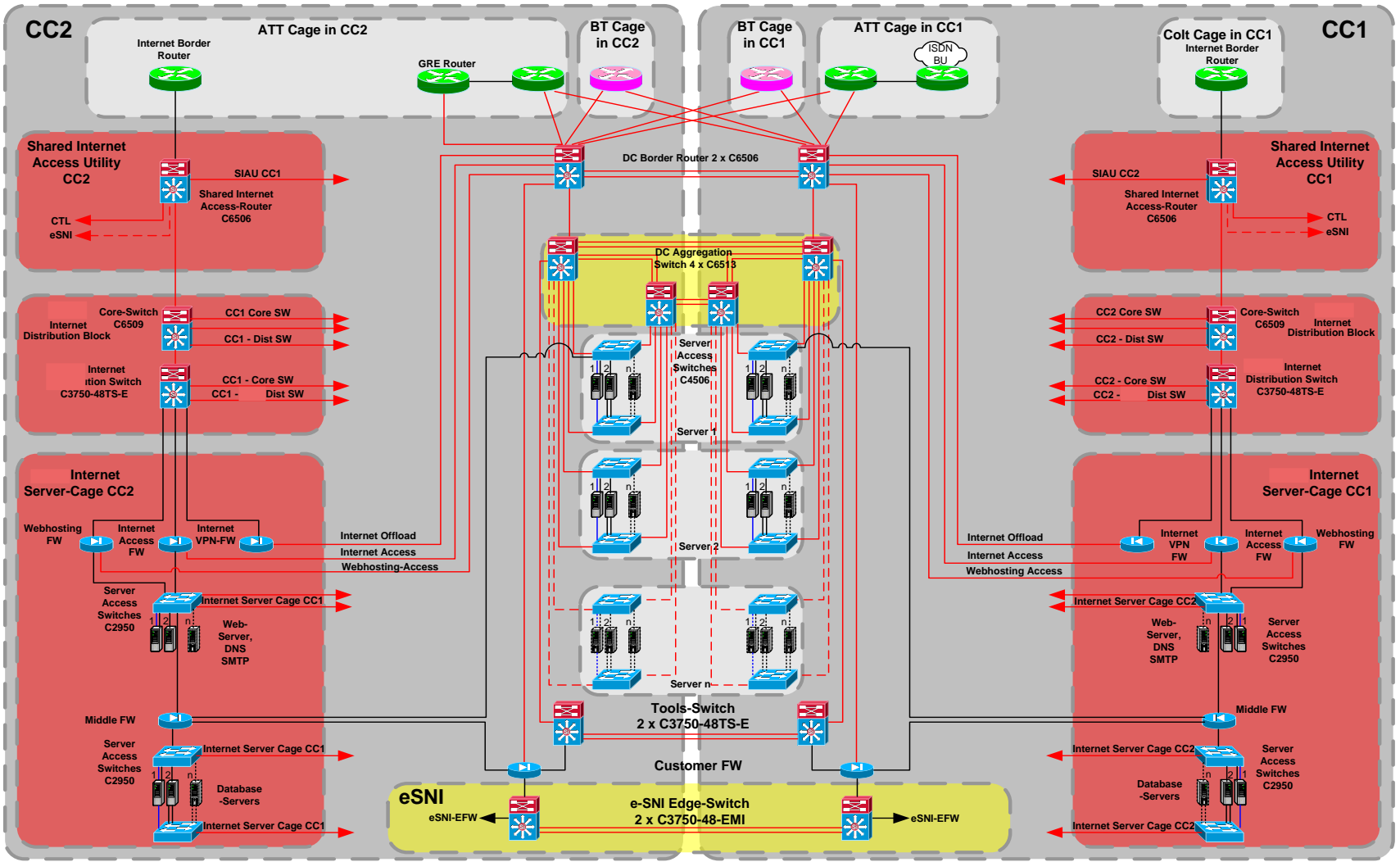




# LAN – Data Centre



# Datacentre example



# WAN Management

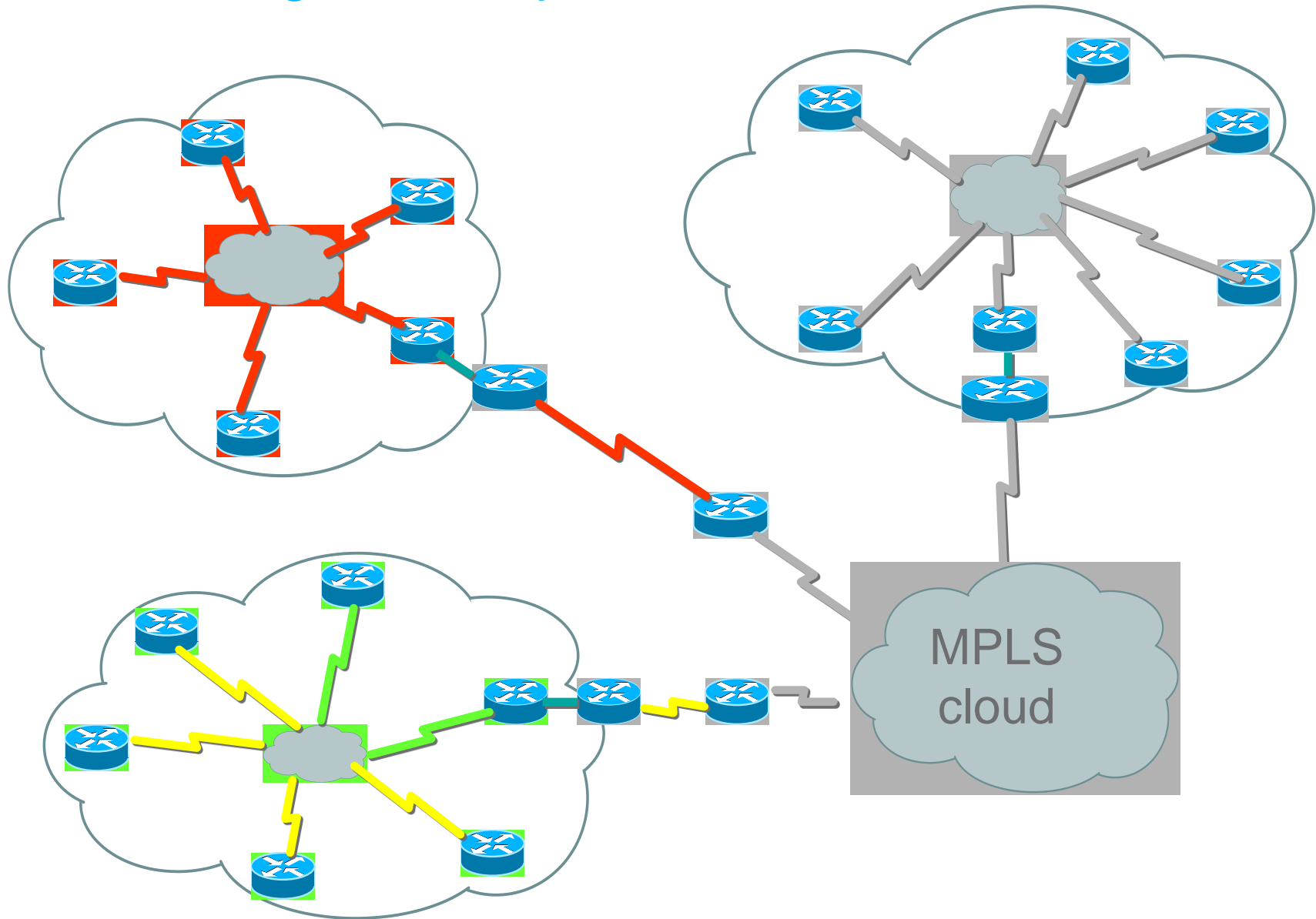
- WAN = Wide Area Network
- Used solutions
  - Leased line
  - ATM/Frame Relay
  - MPLS
  - DSL/ADSL/ISDN
  - Internet tunnel (iVPN)
- WAN lines are usually provided by external companies (BT, AT&T, HP, Colt...)
- NOC (1<sup>st</sup> level) is contact point between customer and provider

## Today's trends for WAN

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



# WAN Management – providers



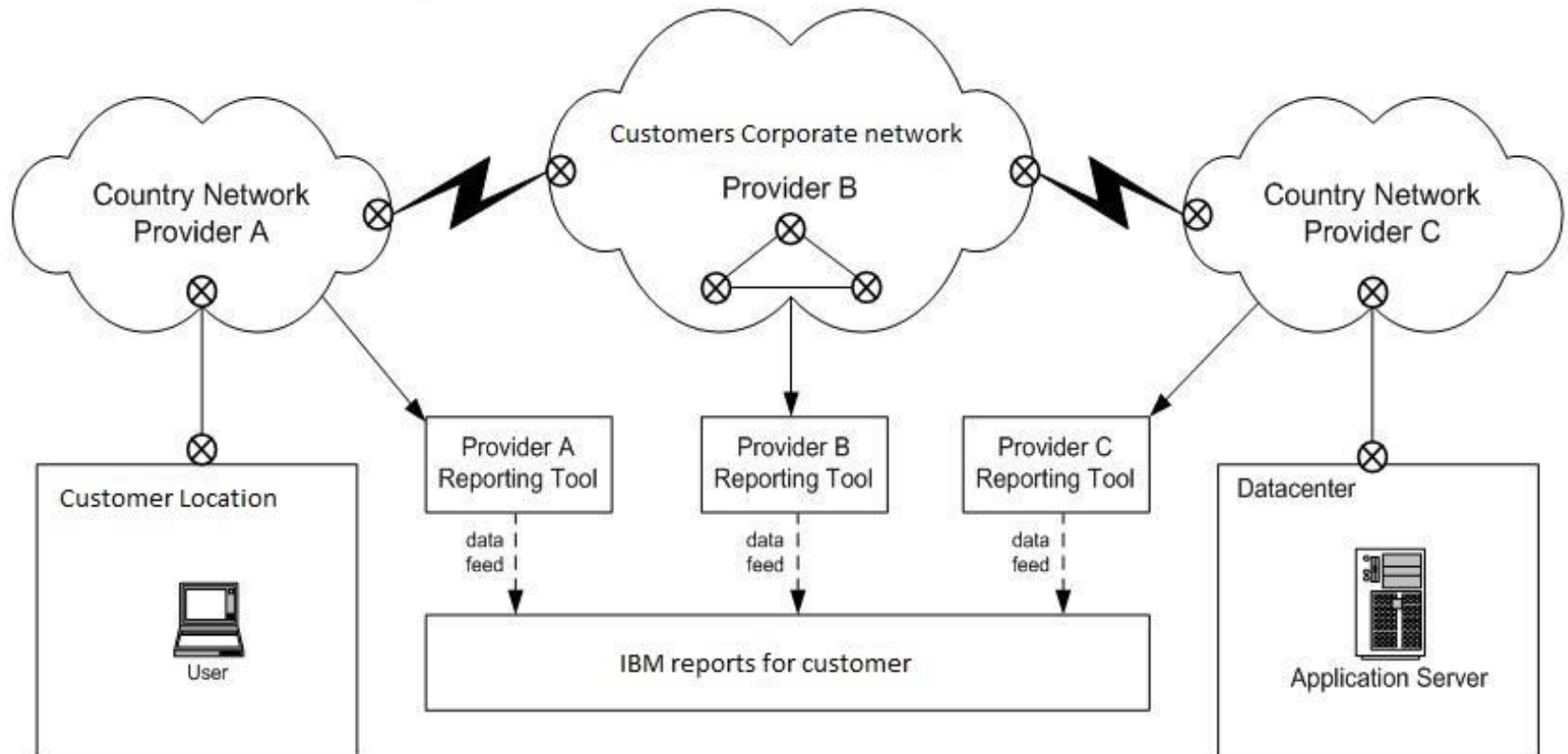
# WAN Specifications and requirements

- 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

There are many different providers and routers where issue can occur.



# IP Services (IPSE)

- DNS/DHCP
- NTP
- Proxy

# QIP – central management for DNS/DHCP

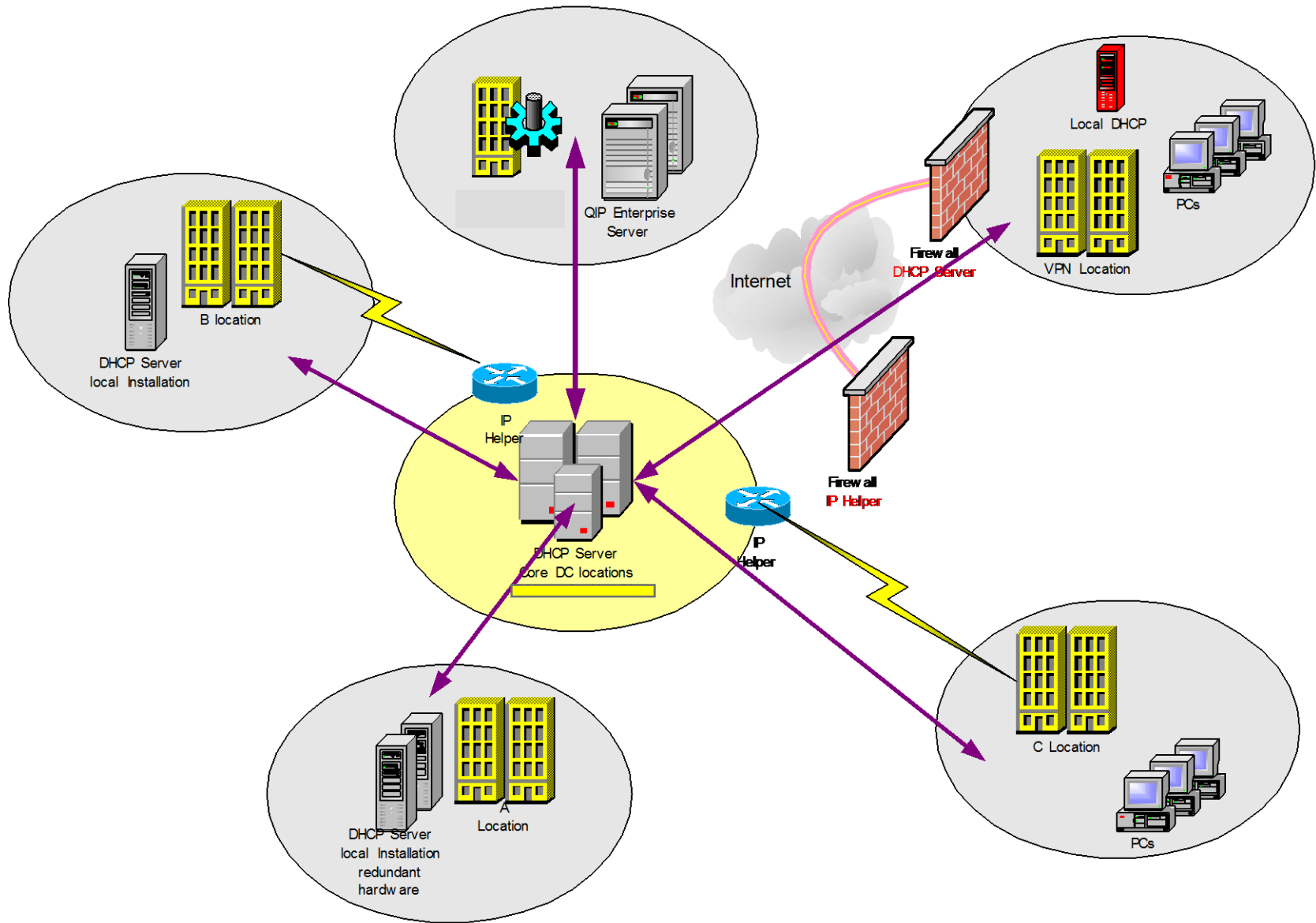
- One central (with backup feature) QIP management server
- Structure-based implementation of QIP provides opportunity to use other QIP servers which are reporting to QIP management server
- Location types:
  - Less than 250 users DHCP – IP helper
  - Less than 499 users local DHCP server or IP helper
  - 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
  - 2<sup>nd</sup> level domain (customer.com)
  - Sub-domains (location.customer.com)
- Domain management can be delegated to another server







# 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



# 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

Check Point SmartView Status

File View Tree Products System Alert Tools Window Help

System Status System Alert

Check Point Gateways	Status	Updated
camtr-cpfw0-cluster	Disconnected	15:27:11
esmad-cfw0-cluster	OK	15:27:03
CHBAD-Cluster2	OK	15:27:02
nlrtm-cfw0-cluster	OK	15:27:02
gbgr-cfw0-cluster	OK	15:27:03
gbgr-cfw0	OK	15:27:03
FireWall-1	OK	15:27:03
VPN-1	OK	15:27:03
ClusterXL	OK	15:27:03
SVN Foundation	OK	15:27:03
gbgr-cfw1	OK	15:27:03
CMA_US	OK	15:26:56
ushou-cpfw2-projfw	OK	15:26:59
uswnd-cpfw2-altdmz	OK	15:26:58
ushou-cpfw1-phono	OK	15:26:58
noosl-cfw0	OK	15:27:02
camtr-cpfw1-montreal	OK	15:26:59
usbvo-cpfw1-scada	Disconnected	15:26:47
uswnd-cpfw1-alt	OK	15:26:50
gbbil-cfw0	OK	15:27:04
esmad-cfw1	Disconnected	15:27:04
frchi-cfw0	OK	15:27:34
frchi-cfw1_	OK	15:27:17
frps-cfw1	OK	15:27:08

FireWall-1 Details	
Status:	OK
Policy Name:	gbgr-20060314
Installed At:	Mon Mar 27 12:03:20 2006
Packets	
Accepted:	136166300
Dropped:	1020878
Logged:	503498
Active Connections:	335
UFP Cache	
Hit ratio (%):	0
Connections inspected:	0
Hits:	0
Hash Kernel Memory	
Total memory allocated:	19922944 bytes using 4858 blocks in 6 pools
Total memory used:	1034080 bytes used (5%); peak was 8258164 bytes
Total blocks used:	361 blocks used (7%); peak was 2083 blocks
Allocations:	1103367655
Allocation failures:	0
Frees:	1103354754
Free failures:	0
System Kernel Memory	
Total memory used:	33834944 bytes used; peak was 58433224 bytes
Allocations:	1706764329
Allocation failures:	0
Frees:	1706762535
Free failures:	0

Critical Notifications

camtr-cpfw2-stlaurent    usbvo-cpfw1-scada    esmad-cfw1    camtr-cpfw1-stlaurent    mxmex-cfw0

For Help, press F1      System Alert Not Started    Read-Write Mode



# 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



# Used shortcuts

- IBM = International Business Machines
- CIC = Client Innovation Center
- GSDC = Global Services Delivery Center
- SSO = Server System Operation
- DCS = Desktop Client Support
- HW = Hardware
- SW = Software
- OS = Operating System
- SLA = Service Level Agreement
- IT = Information Technologies
- SNMP = Simple Network Management Protocol
- TCP/IP = Transmission Control Protocol/Internet Protocol
- OSS = On Site Support
- ERP = Enterprise Resource Planning
- PC = Personal Computer
- CC = Command Center
- HD = HelpDesk
- TEC = Tivoli Enterprise Console
- OSS = On Site Support
- RSA = Remote Supervisor Adapter
- LAN = Local area network
- WAN = Wide area network
- TMR = Tivoli Management Region
- Icfcd = Lightweight Client Framework Daemon
- SME = Service Matter Expert



# Questions ?

