

Network Services Delivery



Michal Mesaros

Agenda

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

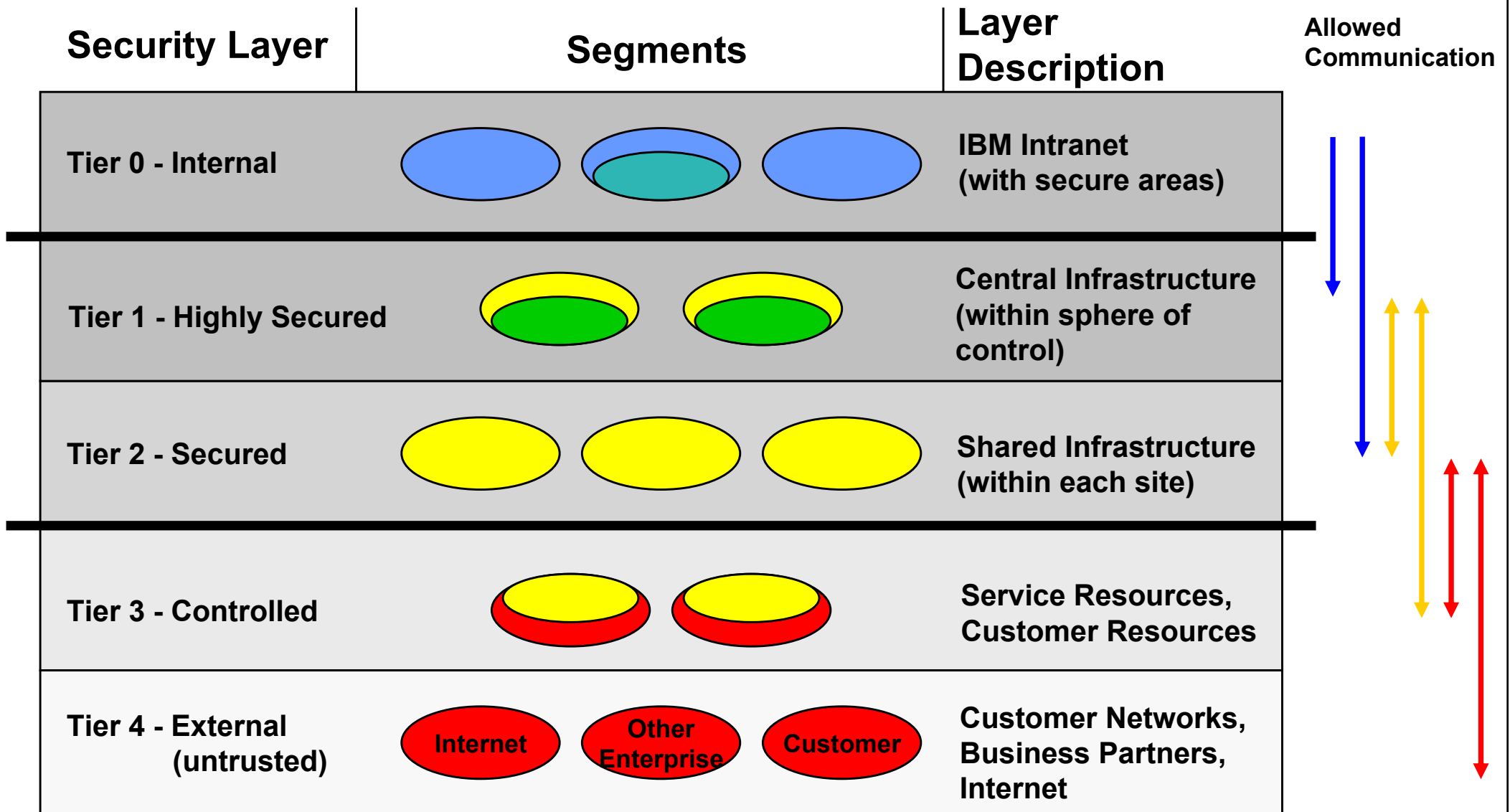
Agenda

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

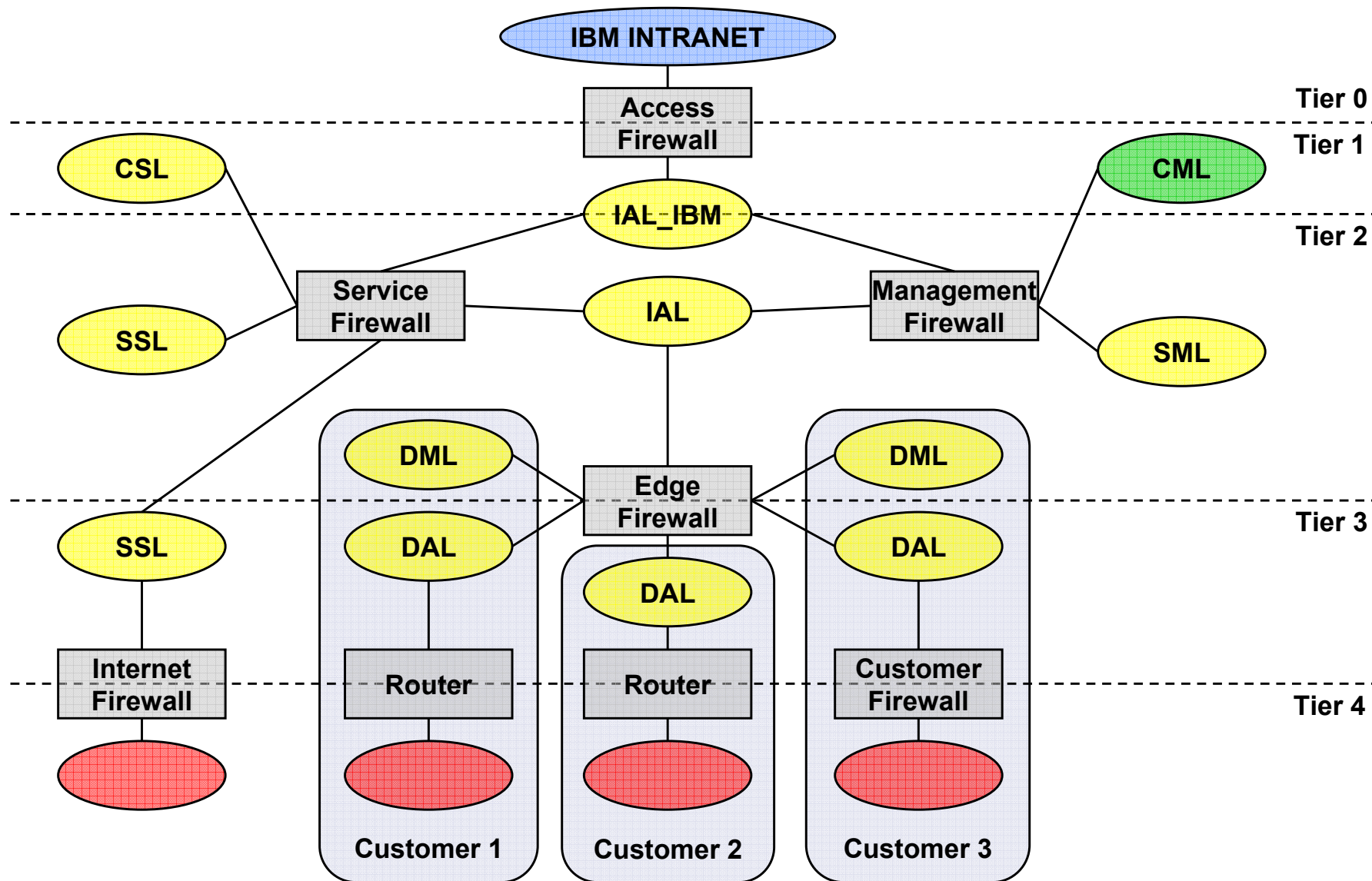
What is Shared Network Infrastructure (SNI)?

- 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

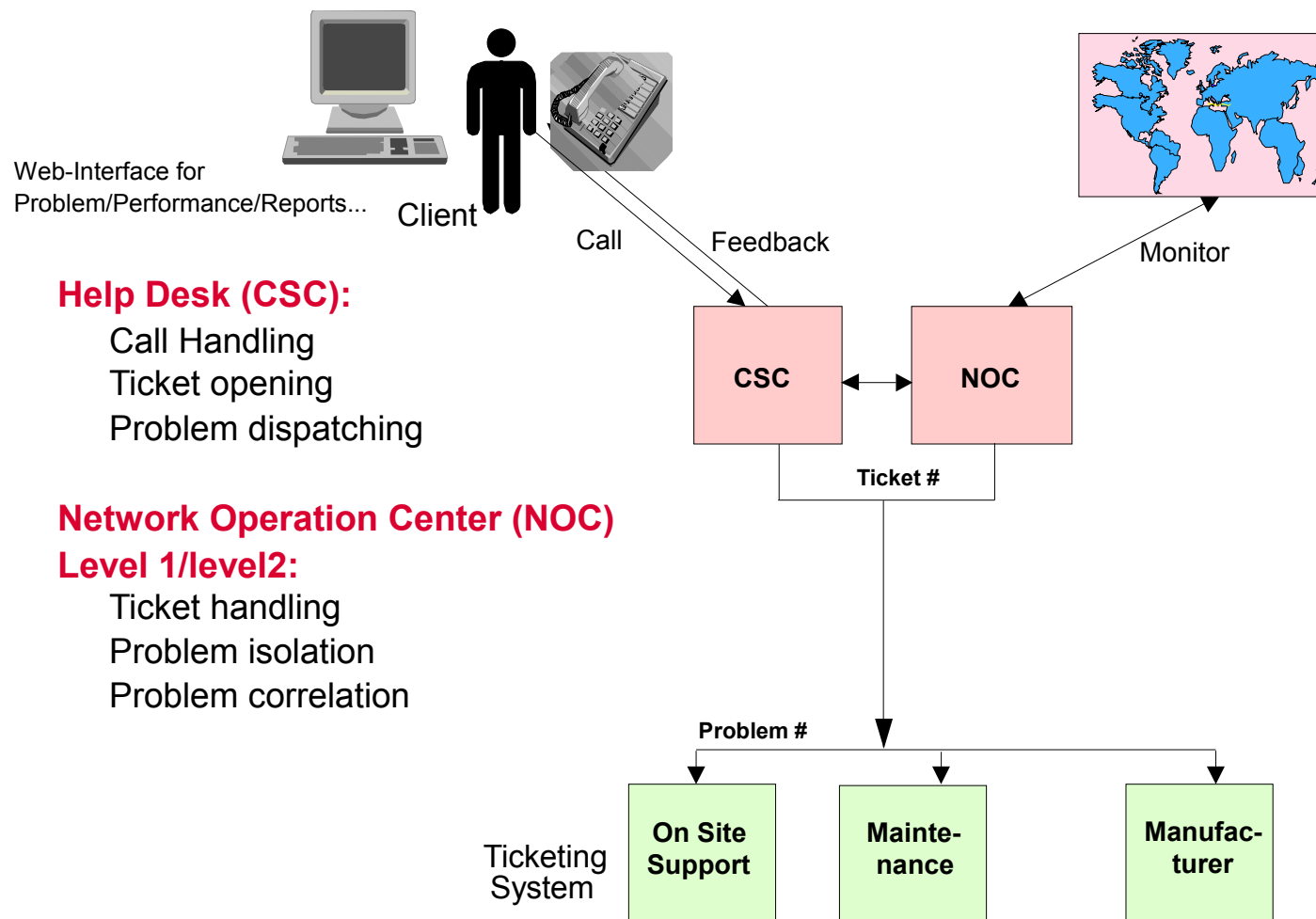
Disadvantages

- 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

Agenda

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

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

Ticketing System

NOC - Level 1 support

- **Proactive monitoring of different tools. Coordinates problem 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 problems.**
- **Update problem tickets in ticketing systems and inform other teams in case of problem 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**

Agenda

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

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

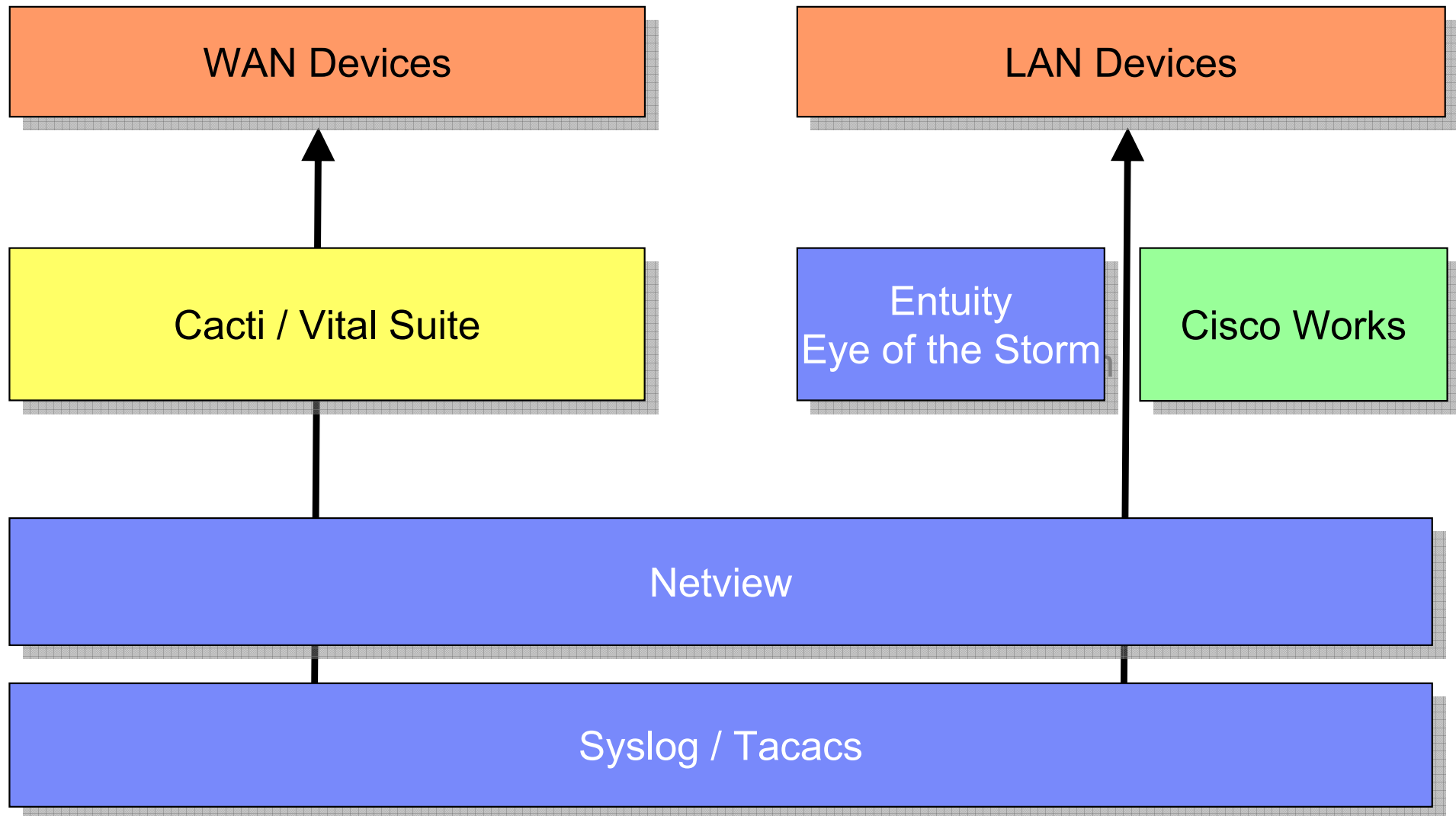
- **With proper tools set you can**

- 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

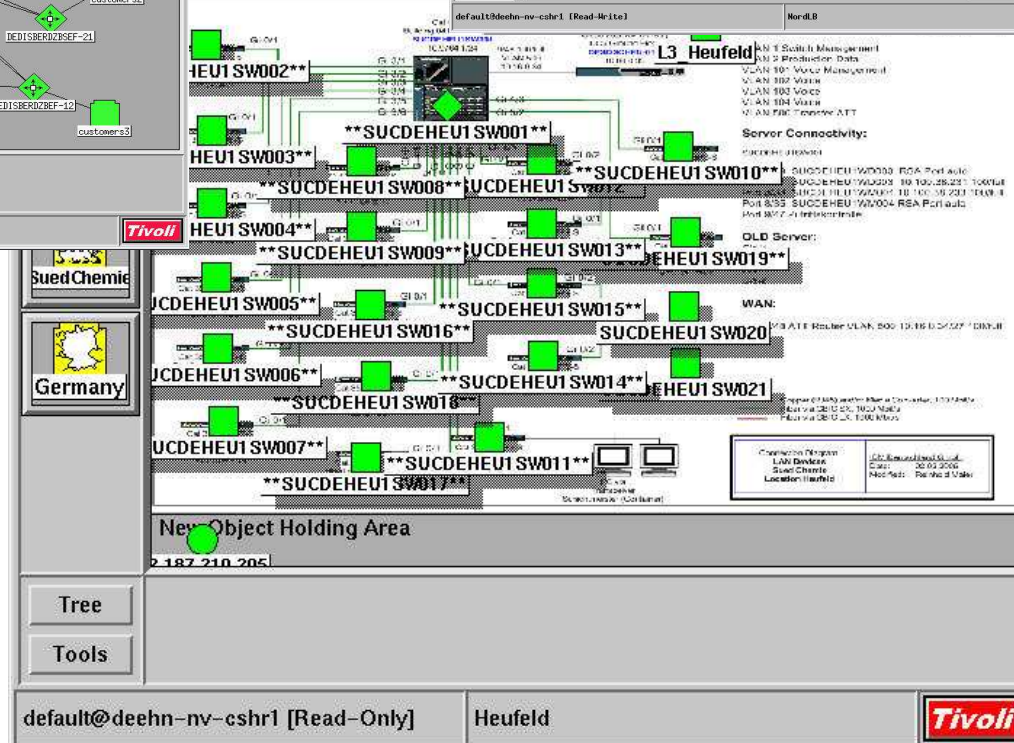
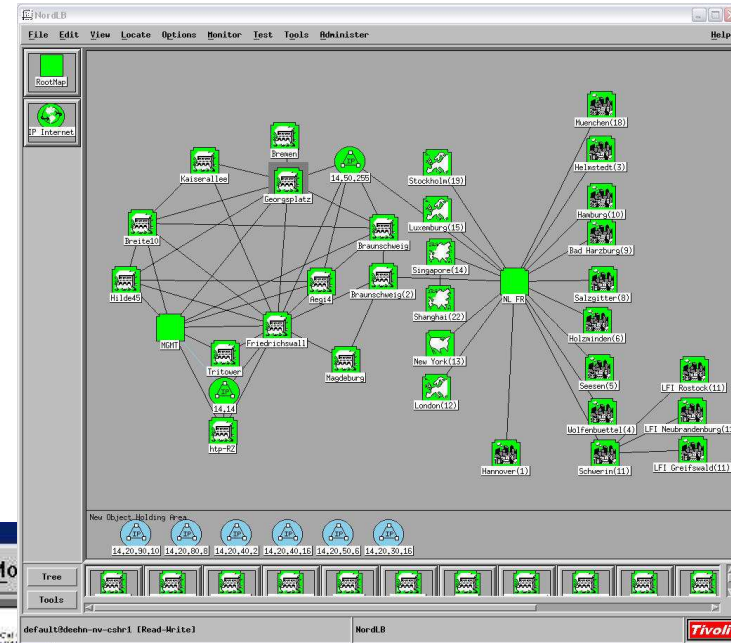
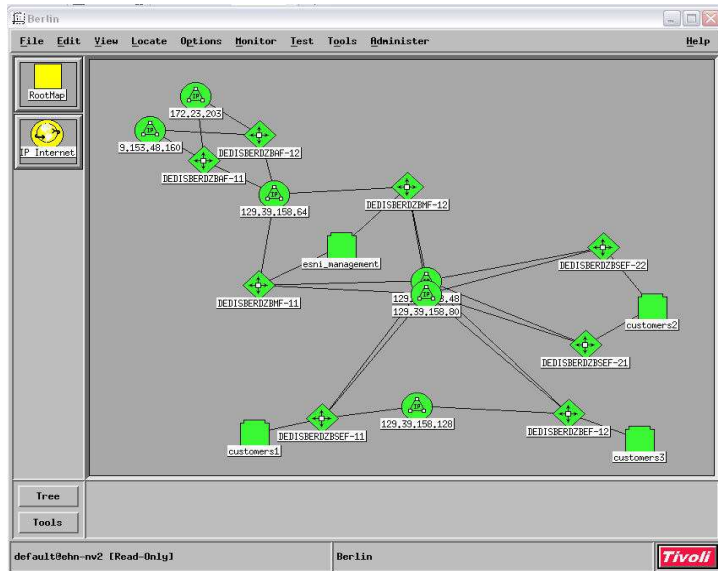
Network Management Toolset



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

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	AUREG-WRH3	Interface DEC down.	Critical
1.2.06 13:50	smtp02.de.abb.com	1: RIPQ-ERROR 'Host:localhost - 2141 messages idle'-- 2:FMT ERROR: accessing element #2, only 1 av...	Warning
1.2.06 13:51	smtp03.de.abb.com	1: SPAMQ-SLS-DOWN 'Host:localhost - Unable to connect SLS server.'-- 2:FMT ERROR: accessing eleme...	Major
1.2.06 13:52	USABBZWINCT01H	Latency packet loss - Source: USABBZWINCT01H-A40151-USABBZPRINJ01R-S0101 512k PVC to Princet...	Critical
1.2.06 13:54	smtp03.de.abb.com	1: SPAMQ-SLS-UP 'Host:localhost - SLS server is available'-- 2:FMT ERROR: accessing element #2, only ...	Cleared
1.2.06 13:55	smtp02.de.abb.com	INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - smtp01.de.abb.co...	Warning
1.2.06 13:55	smtp03.de.abb.com	1: SPAMQ-SLS-DOWN 'Host:localhost - Unable to connect SLS server.'-- 2:FMT ERROR: accessing eleme...	Major
1.2.06 13:58	apsmtp01.sg.abb.com	INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - mail.abb.ru, Port - 25'	Warning
1.2.06 13:58	smtp03.de.abb.com	1: SPAMQ-SLS-UP 'Host:localhost - SLS server is available'-- 2:FMT ERROR: accessing element #2, only ...	Cleared
1.2.06 13:59	apsmtp01.sg.abb.com	INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - smtp01.de.abb.co...	Warning
1.2.06 13:59	apsmtp01.sg.abb.com	INTERNAL-SERVER-ERROR 'Host:localhost - SMTP Internal Server Test Failed. Host - mail.at.abb.com, P...	Warning
1.2.06 14:00	NK00069	Interface 138.221.99.4 down.	Critical
1.2.06 14:00	NK00069	Node Down.	Critical
1.2.06 14:00	AUREG-WRH3	Interface DEC up.	Cleared
1.2.06 14:00	NK00069	Interface 138.221.99.4 up.	Cleared
1.2.06 14:00	NK00069	Node Up.	Cleared
1.2.06 14:01	smtp02.de.abb.com	1: RIPQ-ERROR 'Host:localhost - 2150 messages idle'-- 2:FMT ERROR: accessing element #2, only 1 av...	Warning
1.2.06 14:01	smtp02.de.abb.com	1: VFQ-DOWN 'Host:localhost - VFQ Test Failed. Monitor port not responding.'-- 2:FMT ERROR: accessing ...	Major
1.2.06 14:05	NLRTM-CFW0	Interface 10.31.96.111 down.	Critical
1.2.06 14:05	NLRTM-CFW0	Node Down.	Critical
1.2.06 14:05	AUREG-WRH3	Interface DEC up.	Cleared
1.2.06 14:05	NLRTM-CFW0	Interface 10.31.96.111 up.	Cleared
1.2.06 14:05	NLRTM-CFW0	Node Up.	Cleared
1.2.06 14:05	AUREG-WRH3	Interface DEC down.	Critical
1.2.06 14:07	ESABBYMAD--01R	Latency packet loss - Source: ESABBYMAD--01R-T8-DEABBYEHG--03R_latency_loss object has been no l...	Cleared
1.2.06 14:08	smtp03.de.abb.com	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

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				

cz60070@138.222.124.44

Entuity Eye of the Storm – device report

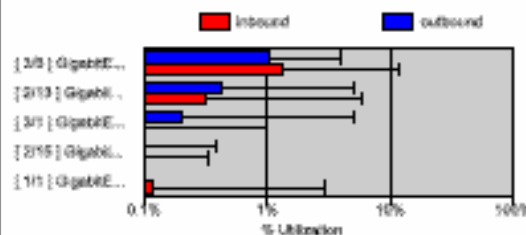
10.49.29.130

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

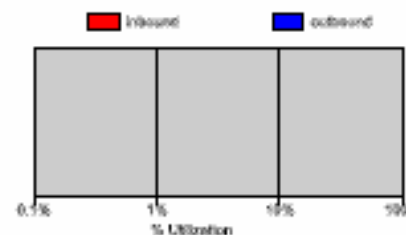
Speed	Total	Spare
10/100Mb	48	43 (90%)
1Gb	66	18 (27%)

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

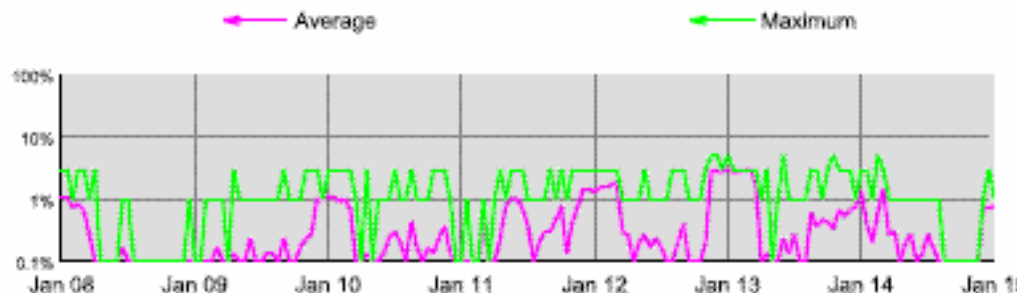
Top trunk ports



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																																			
<table border="1"> <thead> <tr> <th>Top problem WAN links (sorted by number of outages)</th> <th>Outage count</th> <th>Downtime (minutes)</th> </tr> </thead> <tbody> <tr> <td>138.228.192.222 : [22] DEABBYEHG-03R-T65002-SGABBYSP-01</td> <td>15</td> <td>155.7minutes</td> </tr> <tr> <td>138.228.192.222 : [17] att-unman DEABBYEHG-03R-T9-ZAABBYJNS-01</td> <td>13</td> <td>1,717.6minutes</td> </tr> <tr> <td>138.228.192.222 : [12] DEABBYEHG-03R-T4-CZABBYBRQ-01</td> <td>10</td> <td>340.6minutes</td> </tr> <tr> <td>138.228.192.222 : [19] DEABBYEHG-03R-T11-CHABBYBAD-01</td> <td>8</td> <td>21.8minutes</td> </tr> <tr> <td>138.228.192.222 : [15] DEABBYEHG-03R-T7-PTAABBYPCS-01</td> <td>7</td> <td>26minutes</td> </tr> </tbody> </table>	Top problem WAN links (sorted by number of outages)	Outage count	Downtime (minutes)	138.228.192.222 : [22] DEABBYEHG-03R-T65002-SGABBYSP-01	15	155.7minutes	138.228.192.222 : [17] att-unman DEABBYEHG-03R-T9-ZAABBYJNS-01	13	1,717.6minutes	138.228.192.222 : [12] DEABBYEHG-03R-T4-CZABBYBRQ-01	10	340.6minutes	138.228.192.222 : [19] DEABBYEHG-03R-T11-CHABBYBAD-01	8	21.8minutes	138.228.192.222 : [15] DEABBYEHG-03R-T7-PTAABBYPCS-01	7	26minutes	<table border="1"> <thead> <tr> <th>Top problem WAN links (sorted by downtime)</th> <th>Outage count</th> <th>Downtime (minutes)</th> </tr> </thead> <tbody> <tr> <td>10.49.127.199 : [124] Vlan120</td> <td>1</td> <td>39,600minutes</td> </tr> <tr> <td>10.49.240.3 : [206] Vlan51</td> <td>1</td> <td>39,600minutes</td> </tr> <tr> <td>10.49.240.2 : [107] Vlan1</td> <td>1</td> <td>39,600minutes</td> </tr> <tr> <td>10.49.127.75 : [135] Vlan101</td> <td>1</td> <td>39,600minutes</td> </tr> <tr> <td>10.49.240.3 : [203] Vlan1</td> <td>1</td> <td>39,600minutes</td> </tr> </tbody> </table>	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
Top problem WAN links (sorted by number of outages)	Outage count	Downtime (minutes)																																			
138.228.192.222 : [22] DEABBYEHG-03R-T65002-SGABBYSP-01	15	155.7minutes																																			
138.228.192.222 : [17] att-unman DEABBYEHG-03R-T9-ZAABBYJNS-01	13	1,717.6minutes																																			
138.228.192.222 : [12] DEABBYEHG-03R-T4-CZABBYBRQ-01	10	340.6minutes																																			
138.228.192.222 : [19] DEABBYEHG-03R-T11-CHABBYBAD-01	8	21.8minutes																																			
138.228.192.222 : [15] DEABBYEHG-03R-T7-PTAABBYPCS-01	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**

CISCO SYSTEMS CiscoWorks | Help | About

Device Center

Device Selector

10.132.0.35

- CS@deehqck01sr0136
 - Campus@deehqck01sr01
 - All Devices
 - 10.132.0.1
 - 10.132.0.10
 - 10.132.0.100
 - 10.132.0.101
 - 10.132.0.102
 - 10.132.0.103
 - 10.132.0.104
 - 10.132.0.11
 - 10.132.0.12
 - 10.132.0.13
 - 10.132.0.14
 - 10.132.0.15
 - 10.132.0.16
 - 10.132.0.17
 - 10.132.0.18
 - 10.132.0.19
 - 10.132.0.2
 - 10.132.0.21
 - 10.132.0.22
 - 10.132.0.24
 - 10.132.0.25
 - 10.132.0.26

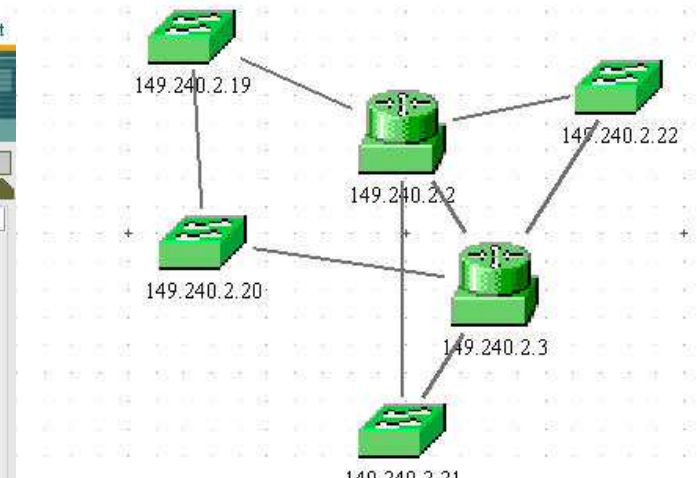
DEVICE: 10.132.0.35

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
	Warnings: 0	Notifications: 0	Informational: 0
Errors: 0			
CDP Neighbors	10.152.190.2		

Functions Available

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



Path Analysis (czzsta02@ANIServer5.0.3-deehqck01sr01...)

File Edit Action Help

Data Trace Voice Trace

From: 149.240.2.19

To: 149.240.2.21

Map Trace Table Error Help...

Layer 3

CISCO SYSTEMS CiscoWorks | Help | About

CiscoView (DEEHQCK01SR0136)

Device Name/IP: 149.240.50.95

Cisco Works – example of report

Resource Manager Essentials - Microsoft Internet Explorer

File Edit View Favorites Tools Help

CISCO SYSTEMS

Reloads Report - 1 Day

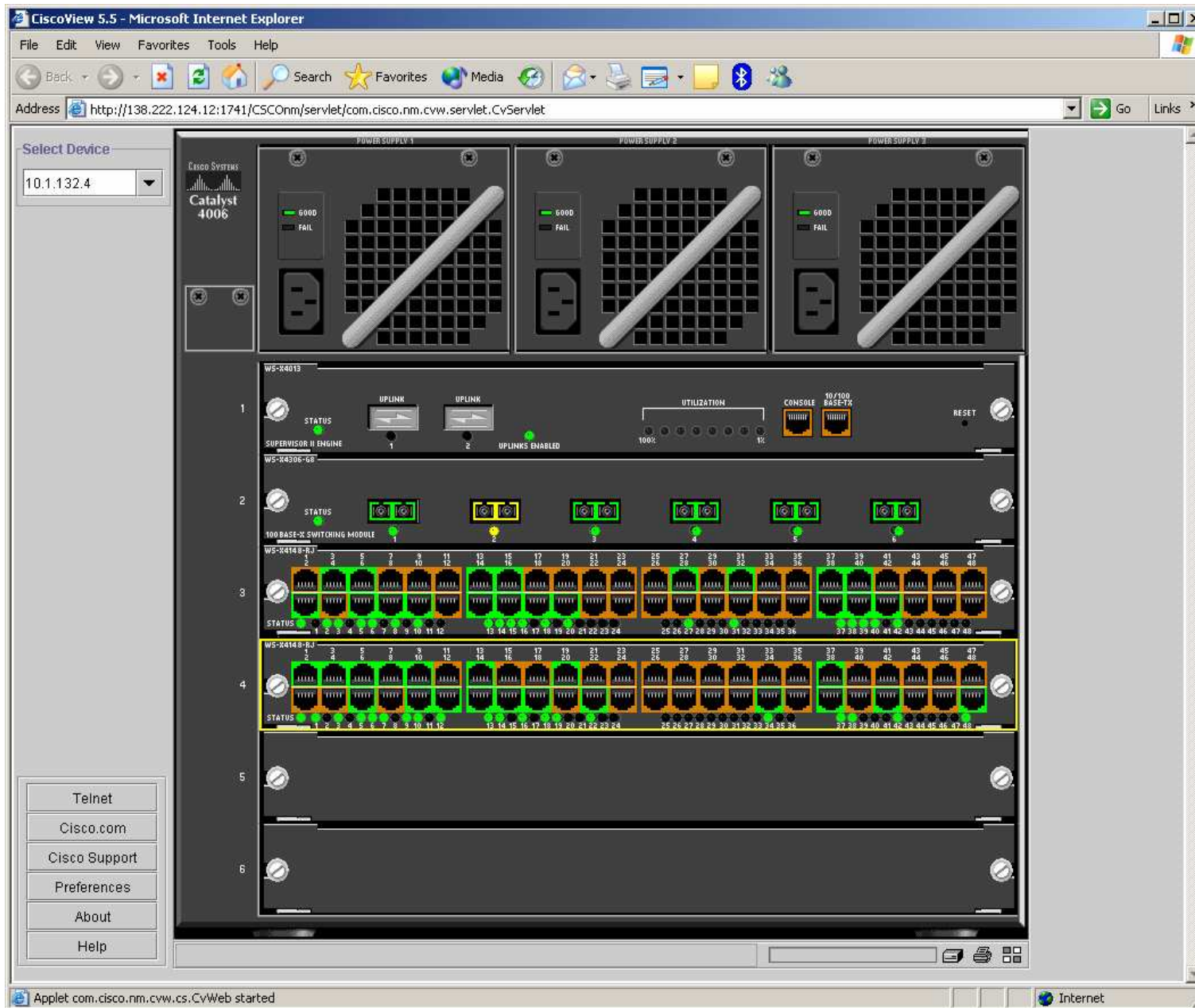
Back Close Save As CSV Format Reports 1 Day

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

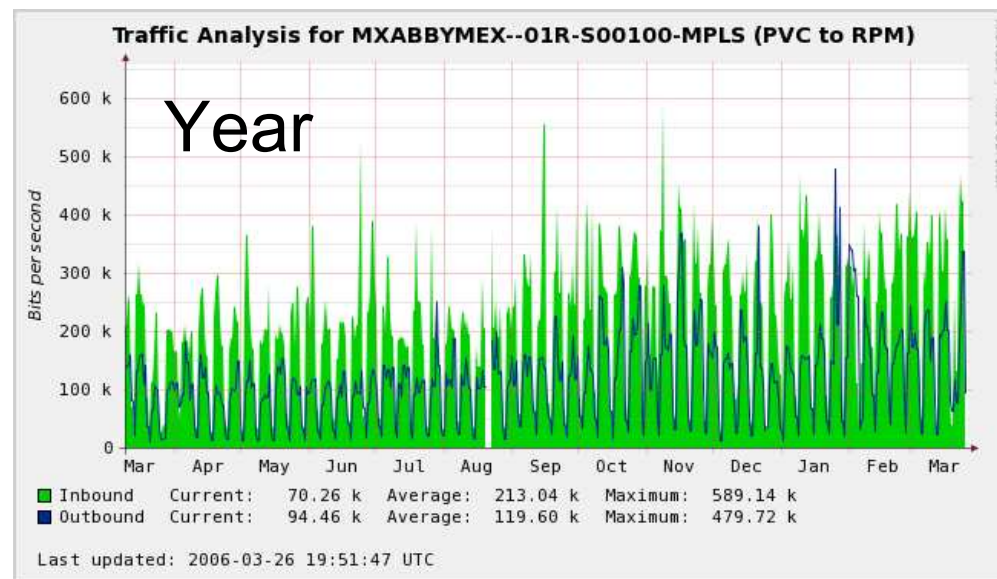
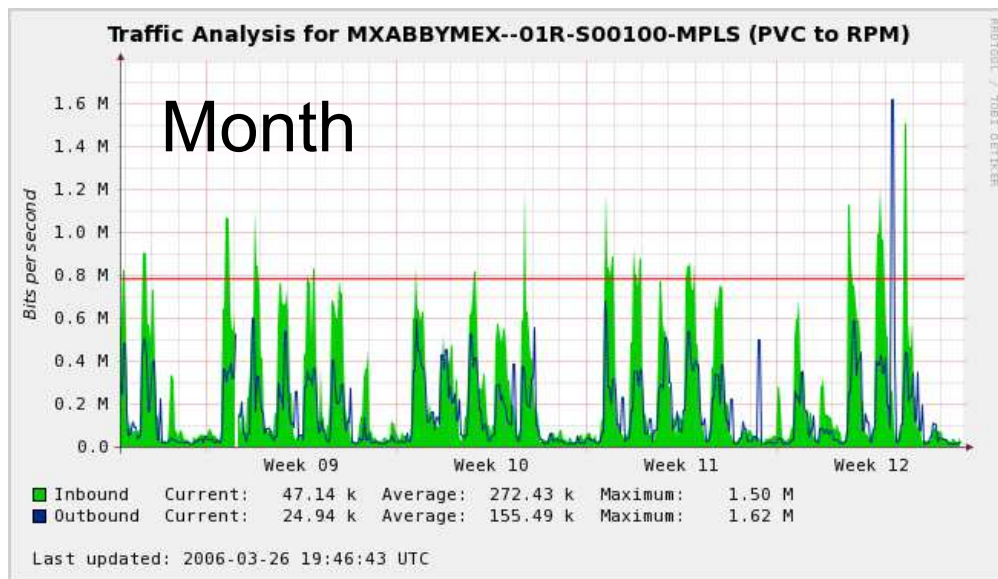
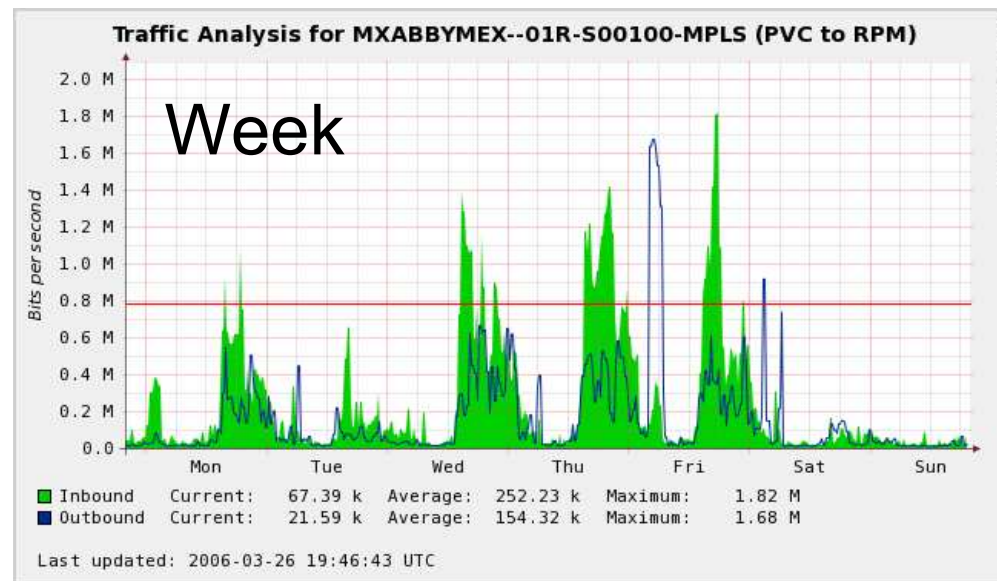
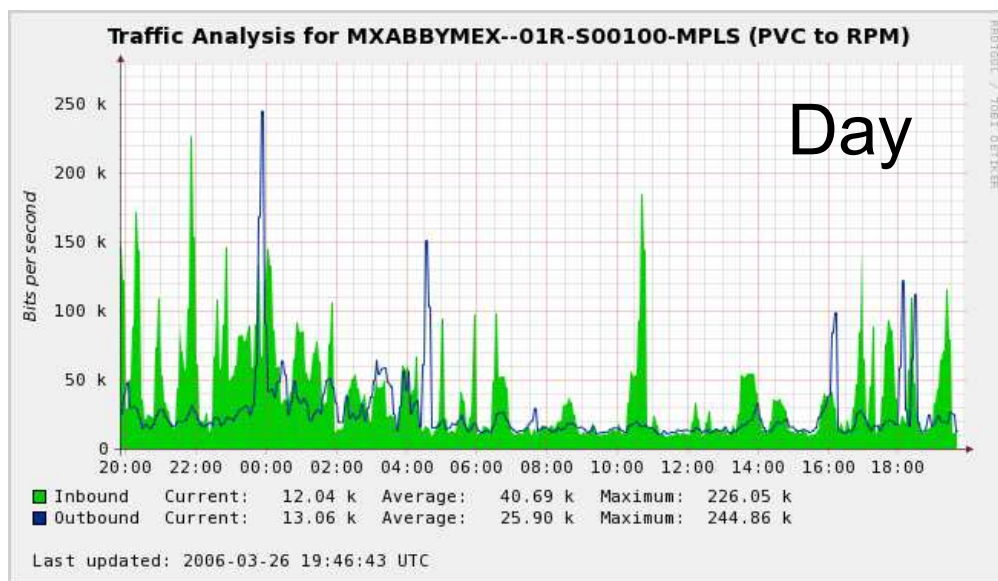
Cisco Works – Cisco View



Performance with Lucent Vital suite / CACTI

- **One of the most important part of our work is troubleshooting are network performance problems.**
- **Requirements for Performance Tools:**
- **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

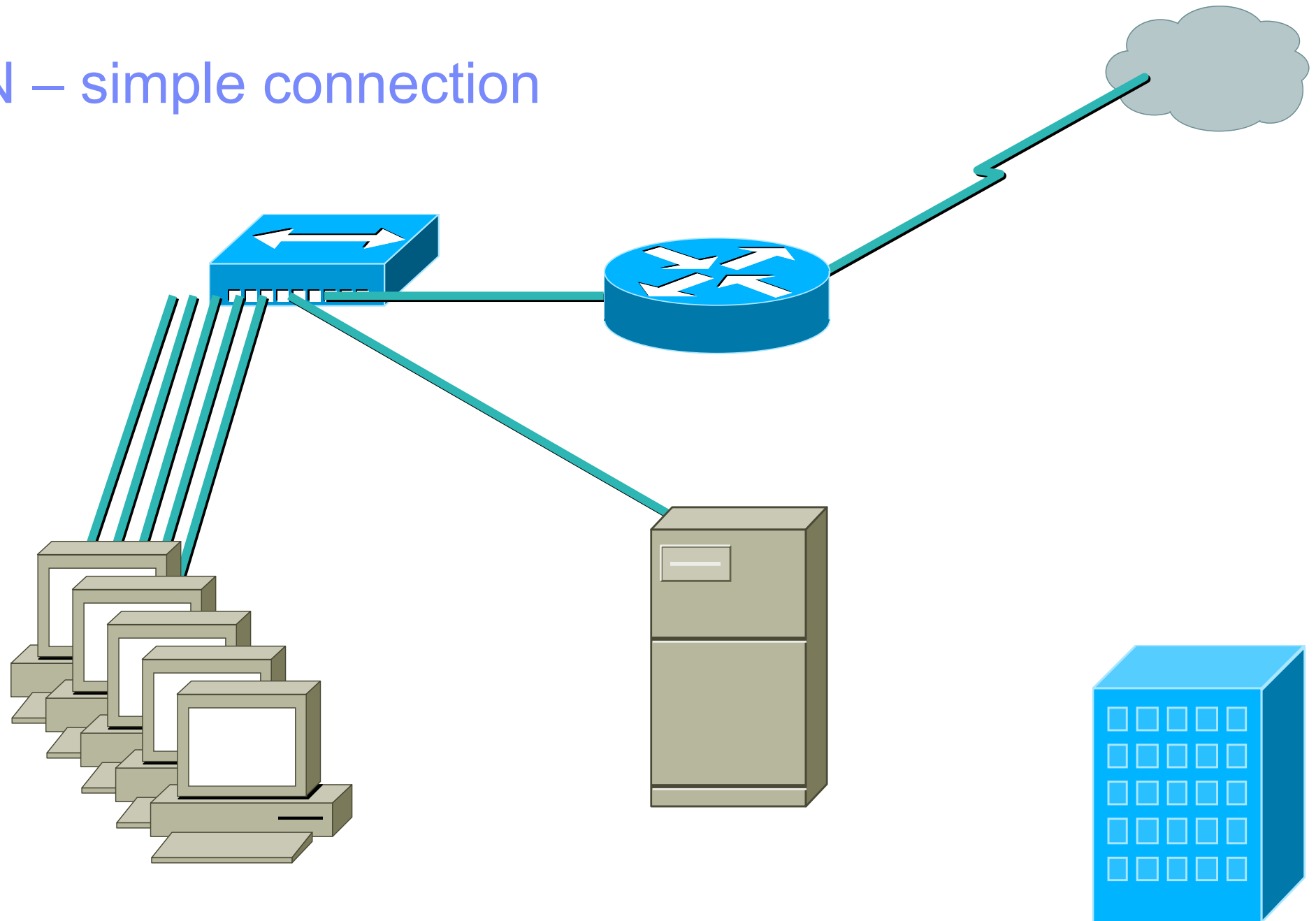
Agenda

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

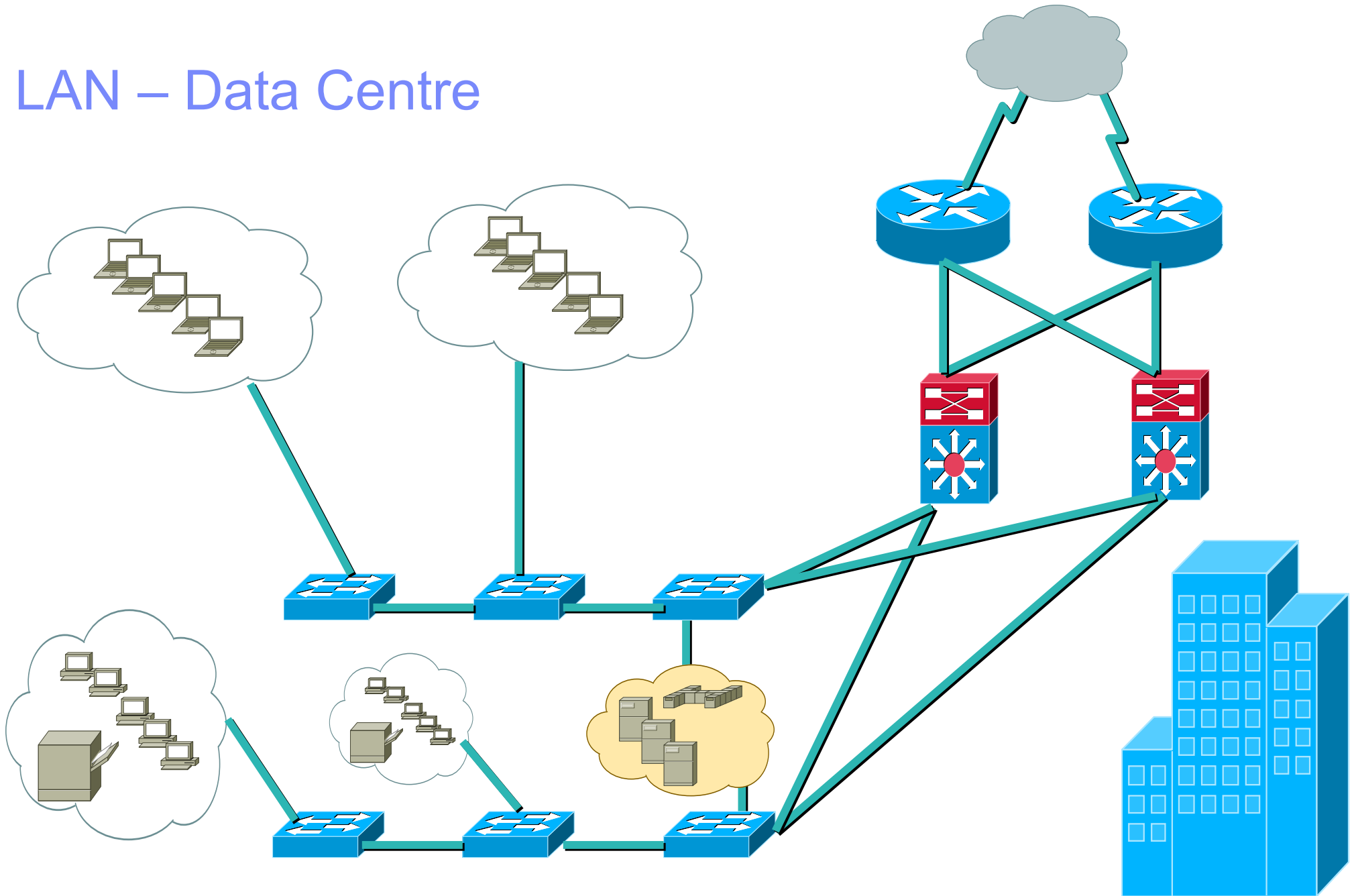
LAN Management

- LAN = Local Area Network
- Device's vendors
 - Cisco, Nortel, 3com, Altel, Allied Telesyn, Blue Coat, Digital, D-link, 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

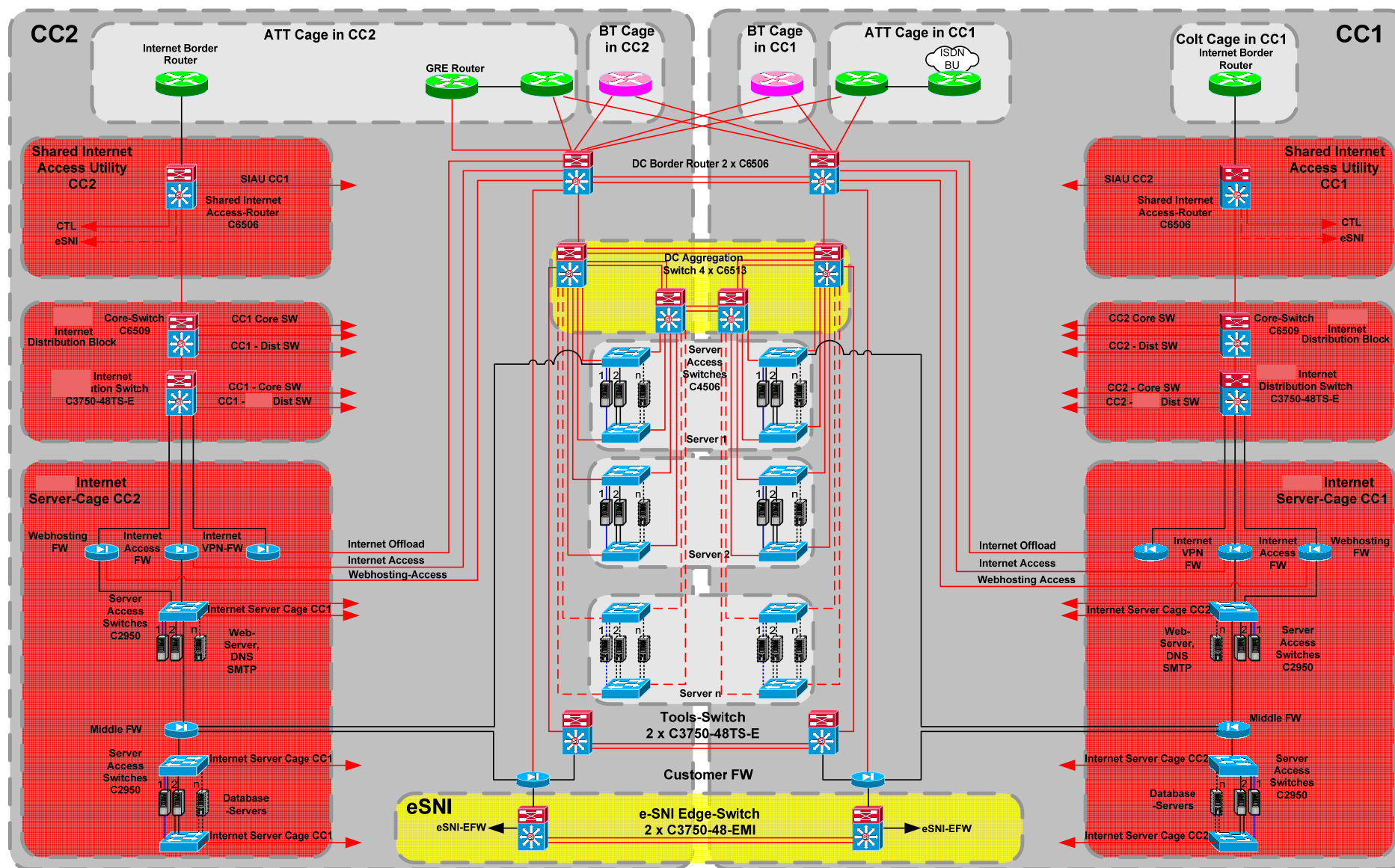
LAN – simple connection



LAN – Data Centre



Datacentre example



Agenda

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

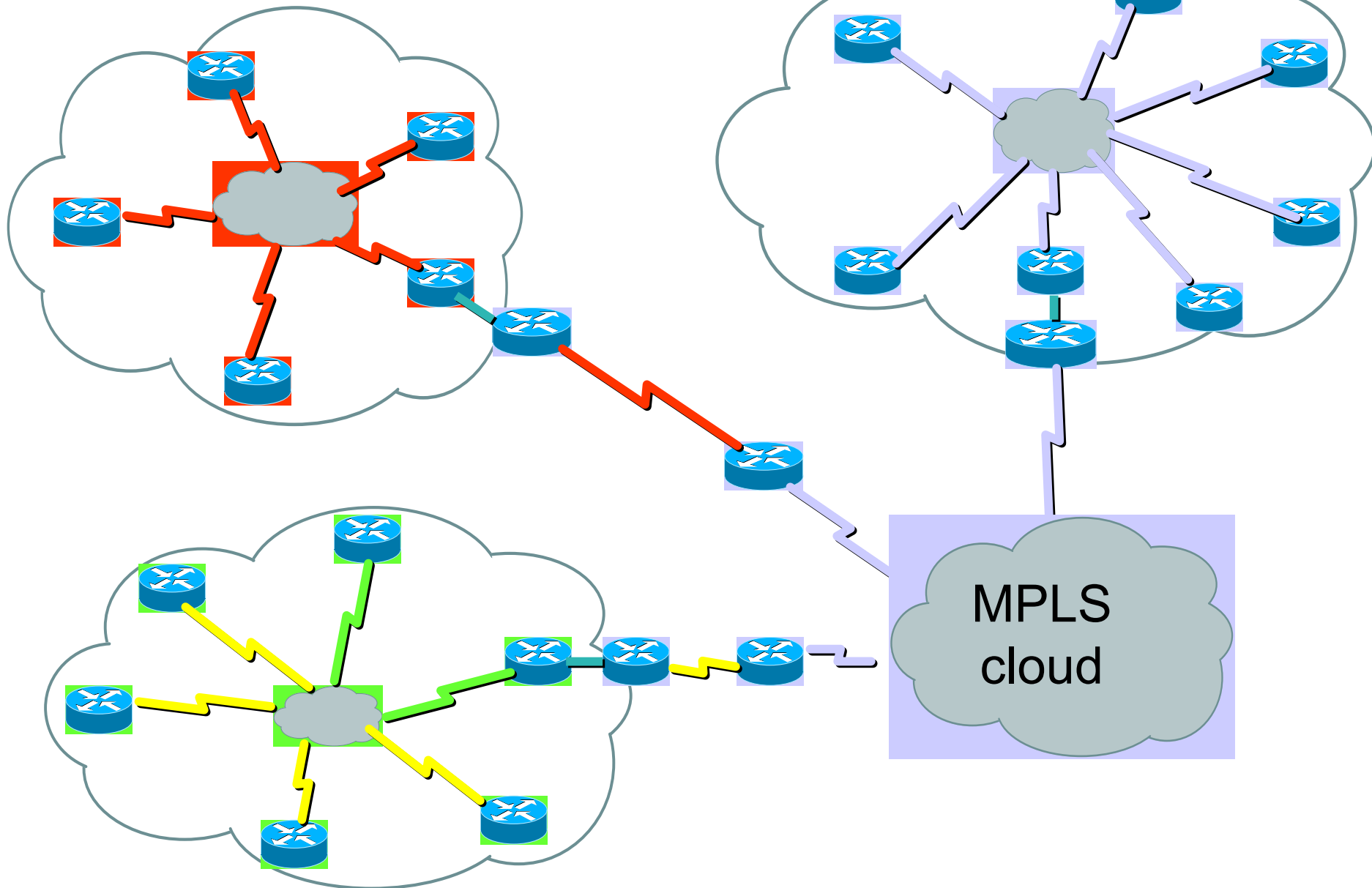
WAN Management

- 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, DT...)
- NOC (1st level) is contact point between customer and provider

Today's trends for WAN

- MPLS = Multiprotocol Label Switching (<http://www.isdn.cz/clanek.php?cid=3869>)
- QoS = Quality of Service (<http://eldar.cz/manasek/felbox/36mps/qos/index.htm>)

WAN Management – providers



WAN Specifications and requirements

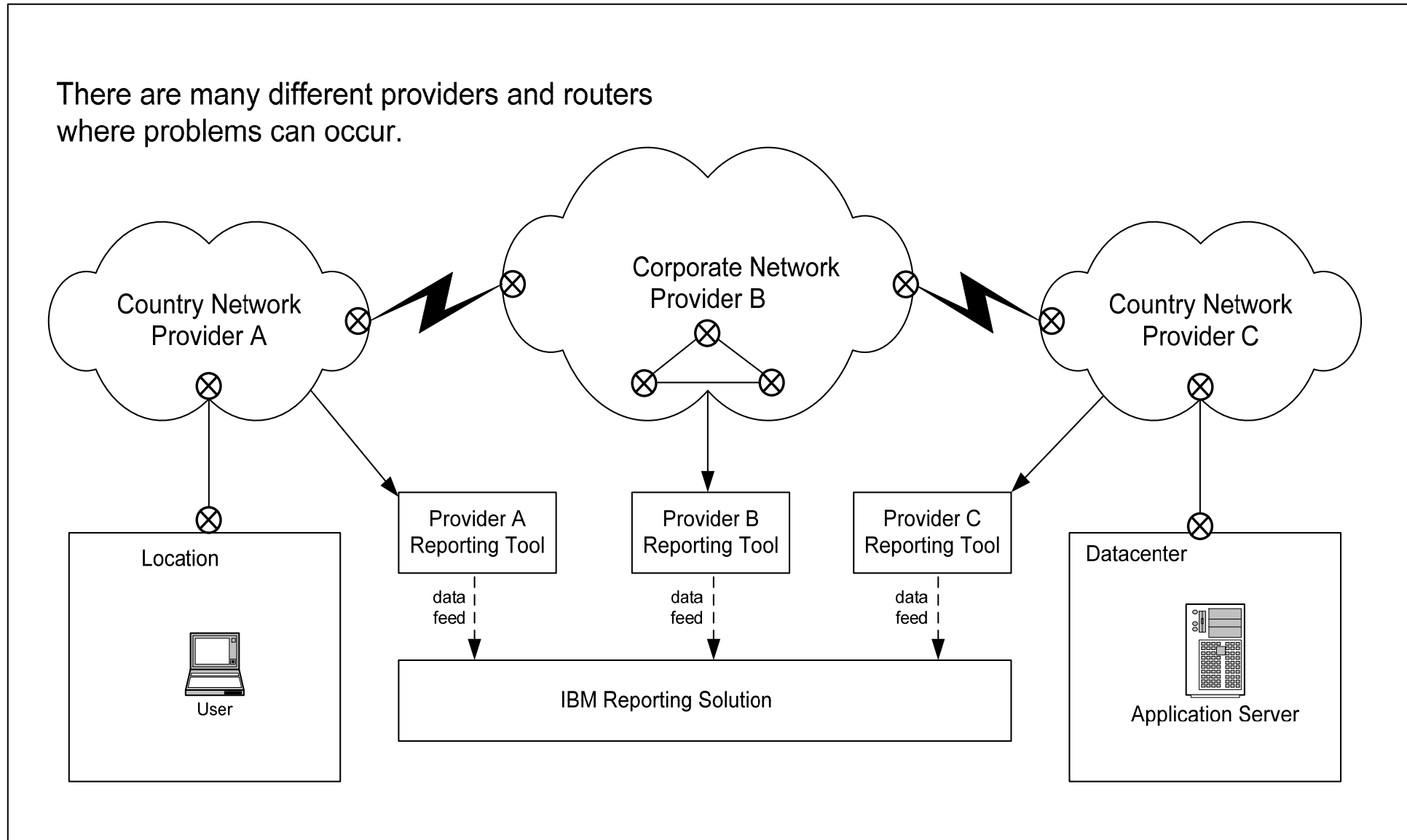
- Setting QoS on WAN lines leads to better performance and usage of line
- 80 – 100 % WAN link utilization (“we pay 100, we use 100”)
- For monitoring of QoS we need good tools

QoS – Basic categorization

- Category 1
 - interactive applications with non-packet burst traffic (e.g. telnet, VoIP)
 - Packet loss should be avoided
- Category 2
 - Interactive applications with packet bursty traffic (e.g. http)
 - Few packet loss
- Category 3
 - Non-interactive batch traffic (e.g. replication, UDP packets)
 - Packet loss possible
- Category Default
 - Non classified traffic
 - High packet loss on congestions, best effort

WAN Problem determination

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



Agenda

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

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
- Hardware
 - PC Architecture
 - Sun
 - Nokia
 - Cisco PIX

Firewall Standard for all replaced and new build firewalls

- Software
 - Checkpoint Firewall-1 Next Generation with Application Intelligence
 - Cisco PIX
- Operating Systems
 - Checkpoint Secure Platform
 - Cisco PIX Firewall OS
- Hardware
 - IBM x-Series Servers
 - Cisco PIX

Checkpoint - ProviderOne

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

Checkpoint - ProviderOne

The screenshot shows the Checkpoint ProviderOne management console. The main window displays a table of Customer Contents under the heading 'General - Customer Contents'. The table has columns for Customer Contents, IP Address, Multi Domain Server, Status, and Active/Standby. A context menu is open over the 'esmad-cfw1' entry, with the 'Launch on Active CMA' option selected, which has opened a sub-menu.

Customer Contents	IP Address	Multi Domain Server	Status	Active/Standby
Provider-1/SiteManager-1				
ABB_Others				
ABB_ASPA				
ABB_EMEA				
ABB_NORDIC				
CMA_US				
CMA_US	138.222.124.8	cpmodule	Started	active
camtr-cpfw0-cluster	138.226.100.163			
esmad-cfw1	10.34.11.254			
esma-cfw0-cluster	10.33.68.10			
CHB...				
nrltm				
gbgf				
usho				
uswr				
noos				
ushou-cpfw1-phono	10.64.16.50			
camtr-cpfw1-montreal	138.226.100.			
usbvo-cpfw1-scada	10.127.254.2			
uswnd-cpfw1-att	10.92.199.10			
gbbil-cfw0	10.44.211.43			
esmad-cfw1	10.34.11.254			
frchi-cfw0	10.33.68.10			
frchi-cfw1_	10.33.68.12			
frprs-cfw1	10.33.4.68			
frchi-zfw0-clm	10.33.70.185			
uswnd-cfw0-windoc	10.92.252.42			

The context menu for 'Launch on Active CMA' includes the following options:

- SmartDashboard (Ctrl+Shift+D)
- SmartView Tracker (Ctrl+Shift+T)
- SmartView Status (Ctrl+Shift+S)
- SmartView Monitor (Ctrl+Shift+M)
- SmartUpdate (Ctrl+Shift+U)
- SmartLSM (Ctrl+Shift+L)
- SmartDashboard (Read Only) (Ctrl+Shift+O)**

Checkpoint - ProviderOne

The screenshot displays the 'Check Point SmartView Status' window for IP 138.222.124.8. The interface is divided into several sections:

- System Status / System Alert:** Shows a list of Check Point Gateways with their status and last update time.
- FireWall-1 Details:** Provides specific statistics for the selected 'FireWall-1' gateway.
- Critical Notifications:** Lists several gateways with red 'X' icons indicating they are disconnected or in error.

Check Point Gateways	Status	Updated
camtr-cpww0-cluster	Disconnected	15:27:11
esmad-cfw0-cluster	OK	15:27:03
CHBAD-Cluster2	OK	15:27:02
nrltm-cfw0-cluster	OK	15:27:02
gbgfr-cfw0-cluster	OK	15:27:03
gbgfr-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
gbgfr-cfw1	OK	15:27:03
CMA_US	OK	15:26:56
ushou-cpww2-projfw	OK	15:26:59
uswnd-cpww2-atdmz	OK	15:26:58
ushou-cpww1-phono	OK	15:26:58
noosl-cfw0	OK	15:27:02
camtr-cpww1-montreal	OK	15:26:59
usbvo-cpww1-scada	Disconnected	15:26:47
uswnd-cpww1-att	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
frprs-cfw1	OK	15:27:08

FireWall-1 Details	
Status:	OK
Policy Name:	gbgfr-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-cpww2-stlaurent
- usbvo-cpww1-scada
- esmad-cfw1
- camtr-cpww1-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)
- Implementation of statefull FW
- VPN implementation – VPN concentrators

Agenda

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

IP Services (IPSE)

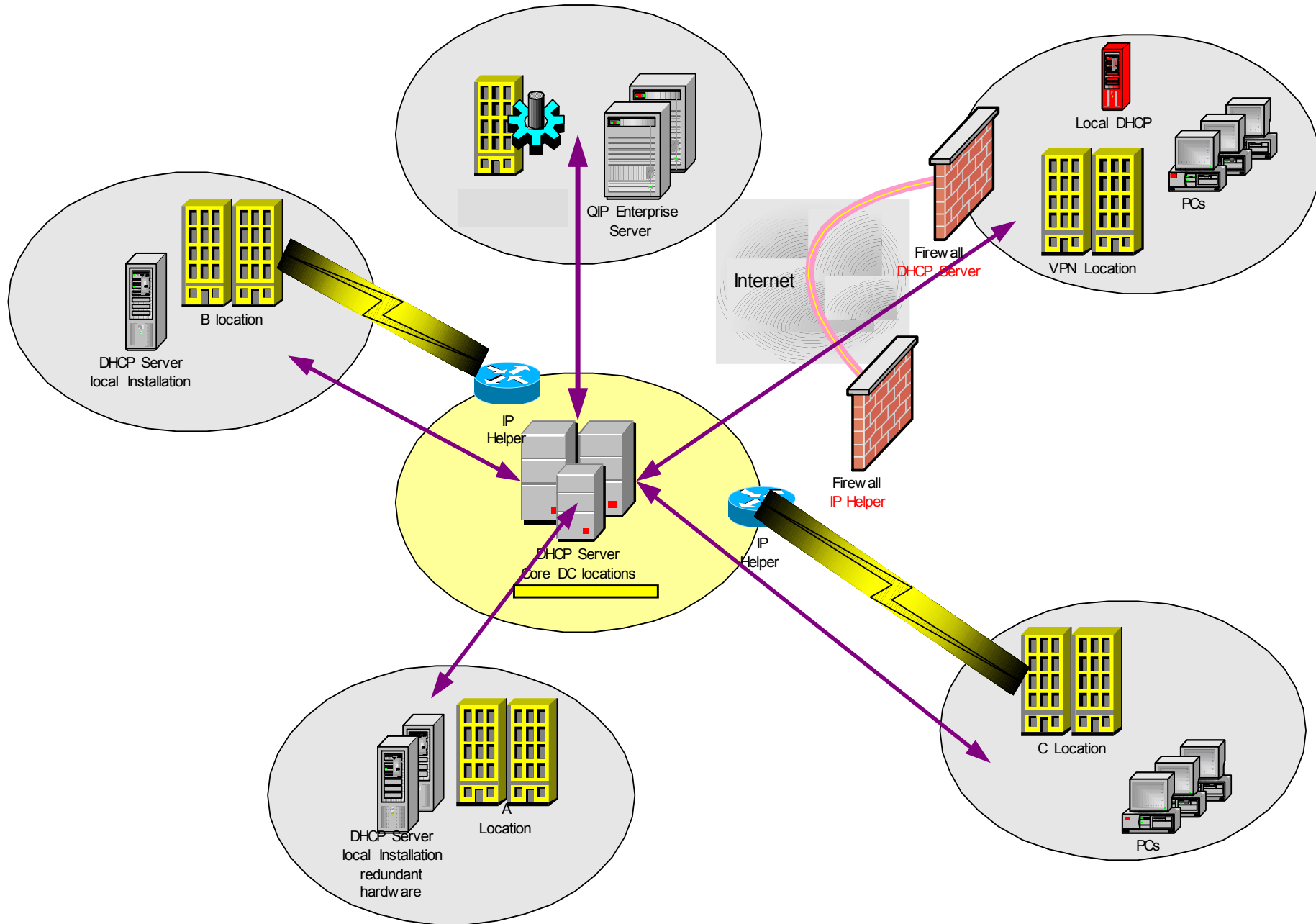
- DNS/DHCP
- NTP
- Proxy

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



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)

Agenda

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

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

Network Security – User revalidation

- Quarterly revalidation if users still exists – User verification
- Yearly revalidation if users still needs access – Business need
- Storing of evidence

Agenda

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

Typical problems LAN/WAN

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

Example 1 – Slow LAN network

- User reports slow network
- It's needed to identify if problem occurs on local server or remote site/internet
- Find port settings (speed/duplex) on switch and settings on user PC and server.
- Find statistic data for port errors
- Cooperate with Server support group to eliminate possible server problems
- Replace cable if port settings are not showing any incorrect settings and errors are shown on port report

Example 2 – Slow Internet/WAN network

- Up/Down Management
 - Find if there is no WAN issue (only backup running)
- QoS Statistics and Reports
 - Find if there are peak on network or load near threshold
- Netflow Traffic Analysis
 - Find which traffic cause big network load

Example 3 – Device unreachable

- Incoming event in NW management tool (Netview, ...)
- Event verification (Ping, SNMP request)
- Try to connect from different location (using different paths)
- Contact On-Site Support to eliminate power outage or cabling problems
- Manual restart (cold reboot)
- Console connect
- HW replacement

Example 4 – Location unreachable

- Incoming event in NW management tool (Netview, ...)
- Contact On-Site Support to eliminate power outage or cabling problems
- Connect via manual backup solution if available (dial up)
- Contact WAN provider for check line problems

Agenda

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

Example 1 – User can't connect to network

- Check IP address
- If IP don't correspond to location there could be problem with IPSE
- Check DHCP service on server
- Check if there are free IPs in pool

Example 2 – User can't connect to service

- Check IP addresses and locations (source / destination)
- Check if there is no network / server / service outage)
- Find route
- Check all rules on FW - ProviderOne
- Check all ACLs on routers / Switches
- Check VLANs

Example 3 – New server in location

- Get necessary approvals
- Find required connections
- Find data flow in network
- Correct all FW rules and ACLs

Questions & Answers