INFRASTRUCTURE DESIGN AND MANAGEMENT

2110684 Information System Architecture

Natawut Nupairoj Ph.D.

Department of Computer Engineering, Chulalongkorn University

Agenda

- Capacity Planning
- System Availability and Monitoring
- Server Consolidation
- Security

CAPACITY PLANNING

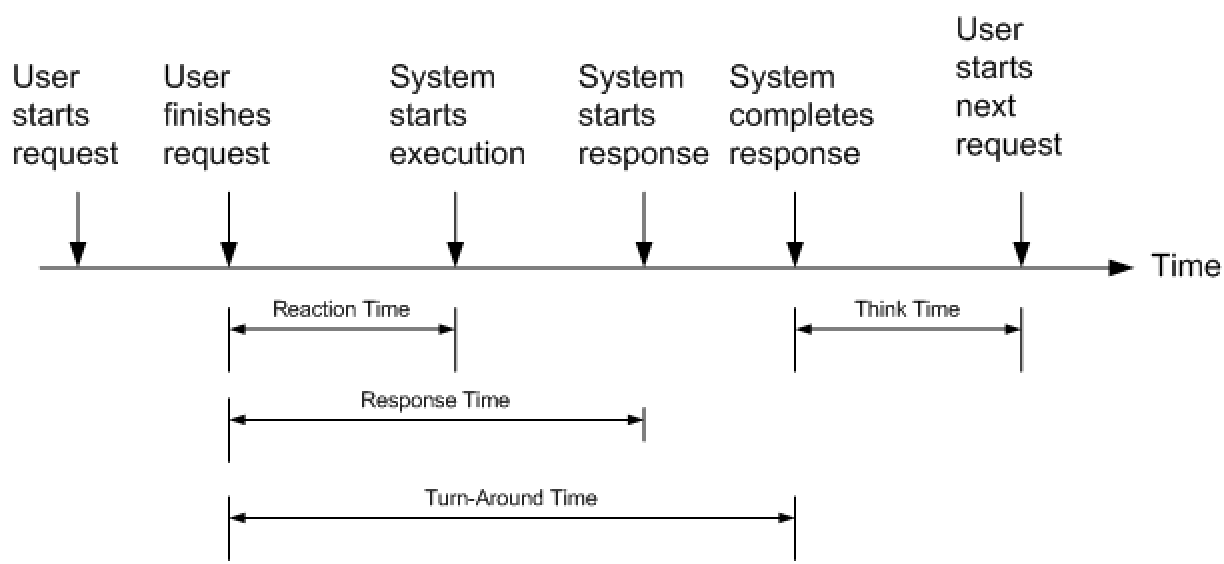
Capacity Planning

- Determining the production capacity needed by an organization to meet changing demands for its products
- Infrastructure Sizing
  - Servers, Network, Storage
  - Depends on to-be-deployed applications and hardware
  - Vendor can provide more accurate sizing
  - Can refer to standard benchmark for rough estimation
    - SPEC
    - TPC

Popular Metrics

- Time - Execution Time
- Rate - Throughput and Processing Speed
- Resource – Utilization
- Ratio - Cost Effectiveness
- Reliability – Error Rate
- Availability – Mean Time To Failure (MTTF)

Definition of Time



Throughput

- Number of jobs that can be processed in a unit time.
- Aka. Bandwidth (in communication).
- The more, the better.
- High throughput does not necessary mean low execution time.
  - Pipeline.
  - Multiple execution units.

Utilization

The percentage of resources being used

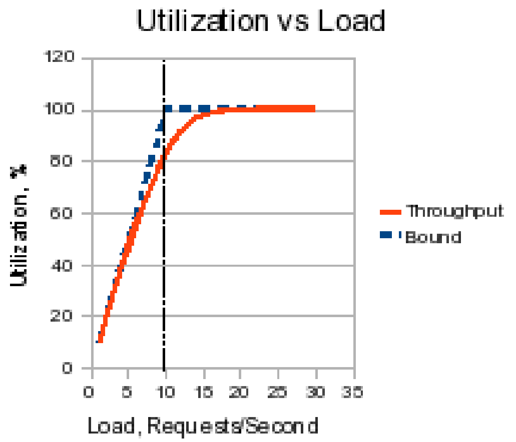
Ratio of

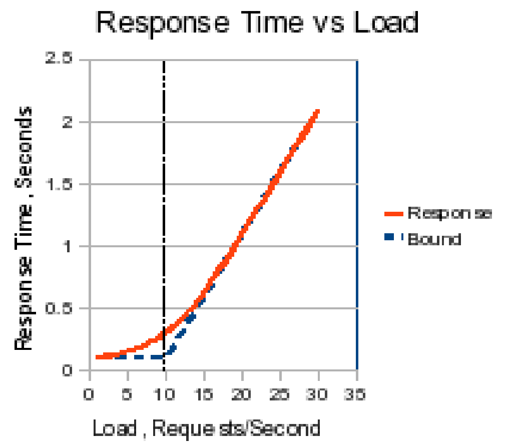
- busy time vs. total time
- sustained speed vs. peak speed

The more the better?

- True for manager
- But may be not for user/customer

Resource with highest utilization is the “bottleneck”

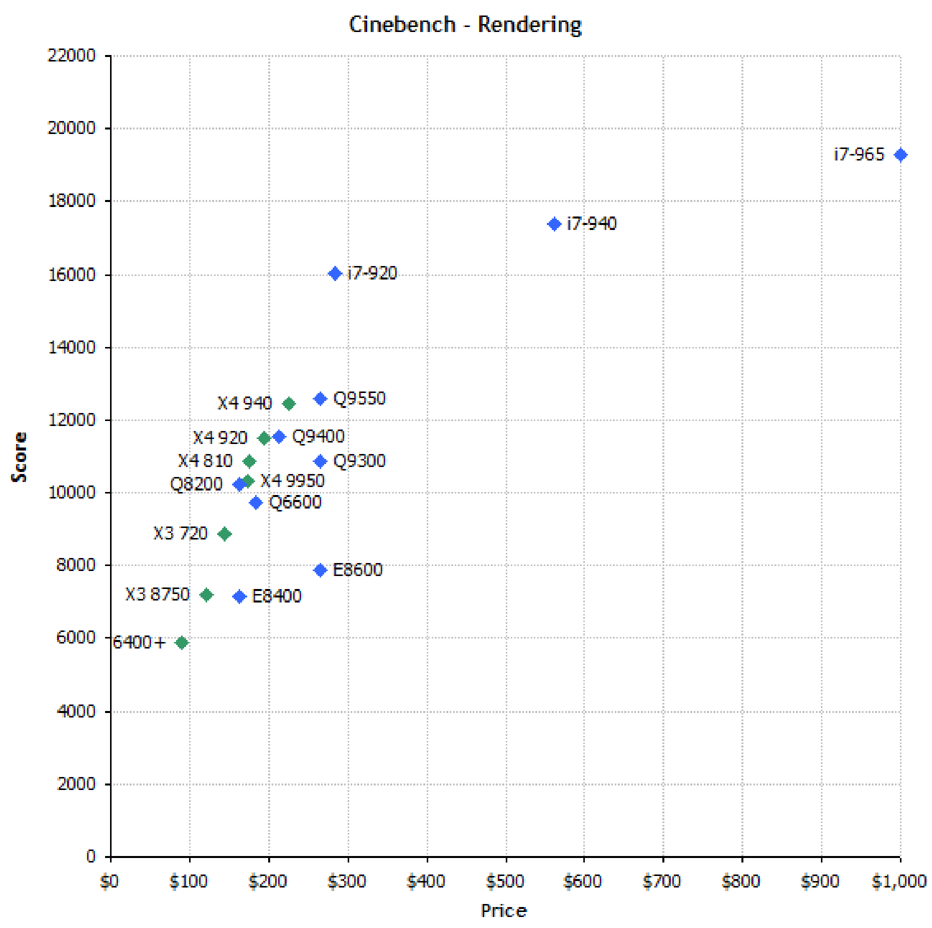




Cost Effectiveness

- Peak performance/cost ratio
- Price/performance ratio

Price/Performance Ratio



From Tom's Hardware Guide: CPU Chart 2009

SPEC

- By Standard Performance Evaluation Corporation
- Using real applications
- http://www.spec.org
- SPEC CPU2006
  - Measure CPU performance
    - Raw speed of completing a single task
    - Rates of processing many tasks
  - CINT2006 - Integer performance
  - CFP2006 - Floating-point performance

CINT2006

400.perlbench	C	PERL Programming Language
401.bzip2	C	Compression
403.gcc	C	C Compiler
429.mcf	C	Combinatorial Optimization
445.gobmk	C	Artificial Intelligence: go
456.hmmer	C	Search Gene Sequence
458.sjeng	C	Artificial Intelligence: chess
462.libquantum	C	Physics: Quantum Computing
464.h264ref	C	Video Compression
471.omnetpp	C++	Discrete Event Simulation
473.astar	C++	Path-finding Algorithms
483.xalancbmk	C++	XML Processing

CFP2006

410.bwaves	Fortran	Fluid Dynamics
416.gamess	Fortran	Quantum Chemistry
433.milc	C	Physics: Quantum Chromodynamics
434.zeusmp	Fortran	Physics / CFD
435.gromacs	C/Fortran	Biochemistry/Molecular Dynamics
436.cactusADM	C/Fortran	Physics / General Relativity
437.leslie3d	Fortran	Fluid Dynamics
444.namd	C++	Biology / Molecular Dynamics
447.dealII	C++	Finite Element Analysis
450.soplex	C++	Linear Programming, Optimization
453.povray	C++	Image Ray-tracing
454.calculix	C/Fortran	Structural Mechanics
459.GemsFDTD	Fortran	Computational Electromagnetics
465.tonto	Fortran	Quantum Chemistry
470.lbm	C	Fluid Dynamics
481.wrf	C/Fortran	Weather Prediction
482.sphinx3	C	Speech recognition

Top 10 CINT2006 Speed (as of 4 August 2010)

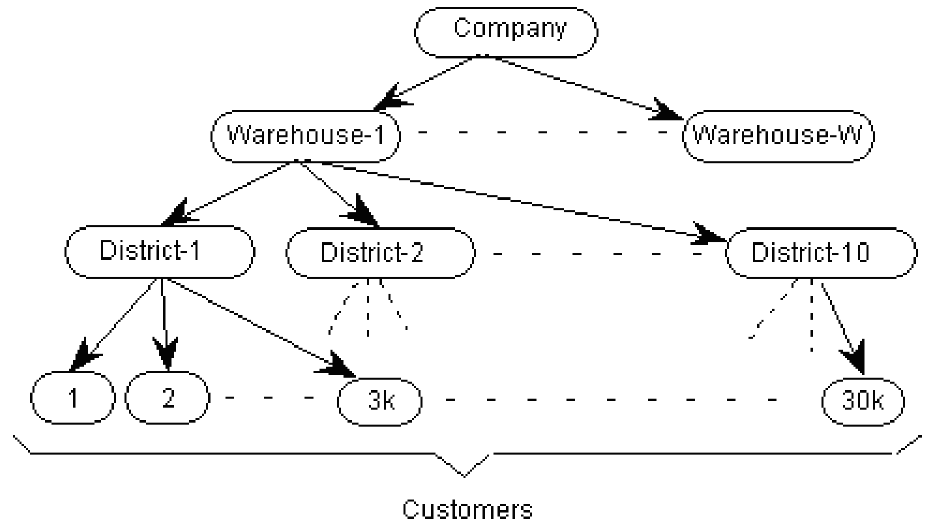
System	Result	# Cores	# Chips	Cores/Chip
IBM Power 780 Server (4.14 GHz, 16 core)	44	16	4	4
PRIMERGY RX200 S6, Intel Xeon X5677, 3.47 GHz	43.5	8	2	4
PRIMERGY BX922 S2, Intel Xeon X5677, 3.46 GHz	43.4	8	2	4
IBM System x3500 M3 (Intel Xeon X5677)	43.4	8	2	4
NovaScale R440 F2 (Intel Xeon X5677, 3.46 GHz)	43.4	8	2	4
PowerEdge R610 (Intel Xeon X5677, 3.46 GHz)	43.4	8	2	4
NovaScale T840 F2 (Intel Xeon X5677, 3.46 GHz)	43.3	8	2	4
PowerEdge T610 (Intel Xeon X5677, 3.46 GHz)	43.3	8	2	4
PRIMERGY BX924 S2, Intel Xeon X5677, 3.46 GHz	43.3	8	2	4
NovaScale R460 F2 (Intel Xeon X5677, 3.46 GHz)	43.3	8	2	4

Other Interesting SPECs

- SPEC jAppServer2004
  - Measure the performance of J2EE 1.3 application servers
- SPEC Web2009
  - Emulates users sending browser requests over broadband Internet connections to a web server
- SPECpower_ssj2008
  - Evaluates the power and performance characteristics of volume server class computers

TPC

- Transaction Processing Performance Council
- http://www.tpc.org
- TPC-C: performance of Online Transaction Processing (OLTP) system
  - tpmC: transactions per minute.
  - $/tpmC: price/performance.



- Simulate the wholesale company environment
  - N warehouses, 10 sales districts each.
  - Each district serves 3,000 customers with one terminal in each district.

TPC Transactions

- An operator can perform one of the five transactions
  - Create a new order.
  - Make a payment.
  - Check the order’s status.
  - Deliver an order.
  - Examine the current stock level.
- Measure from the throughput of New-Order.
- Top 10 (Performance, Price/Performance).

Top 10 TPC-C Performance (as of 4 August 2010)

Rank	Company	System	tpmC	Price/tpmC	Watts/KtpmC	System Availability	Database	Operating System	TP Monitor	Date Submitted	Cluster
1	ORACLE	Sun SPARC Enterprise T5440 Server Cluster	7,646,486	2.36 USD	NR	03/19/10	Oracle Database 11g Ent. Ed. w/Real Application Clusters w/Partitionin	Sun Solaris 10 10/09	Tuxedo CFS-R	11/03/09	Y
2	IBM	IBM Power 595 Server Model 9119-FHA	6,085,166	2.81 USD	NR	12/10/08	IBM DB2 9.5	IBM AIX 5L V5.3	Microsoft COM+	06/10/08	N
***	Bull	Bull Escala PL6460R	6,085,166	2.81 USD	NR	12/15/08	IBM DB2 9.5	IBM AIX 5L V5.3	Microsoft COM+	06/15/08	N
3	hp invent	HP Integrity Superdome-Itanium2/1.6GHz/24MB iL3	4,092,799	2.93 USD	NR	08/06/07	Oracle Database 10g R2 Enterprise Edt w/Partitioning	HP-UX 11i v3	BEA Tuxedo 8.0	02/27/07	N
4	IBM	IBM System p5 595	4,033,378	2.97 USD	NR	01/22/07	IBM DB2 9	IBM AIX 5L V5.3	Microsoft COM+	01/22/07	N
5	IBM	IBM eServer p5 595	3,210,540	5.07 USD	NR	05/14/05	IBM DB2 UDB 8.2	IBM AIX 5L V5.3	Microsoft COM+	11/18/04	N
6	FUJITSU	PRIMEQUEST 580A 32p/64c	2,382,032	3.76 USD	NR	12/04/08	Oracle Database 10g R2 Enterprise Edt w/Partitioning	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	12/04/08	N
7	FUJITSU	PRIMEQUEST 580 32p/64c	2,196,268	4.70 USD	NR	04/30/08	Oracle 10g Enterprise Ed R2 w/ Partitioning	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	10/30/07	N
8	IBM	IBM System p 570	1,616,162	3.54 USD	NR	11/21/07	IBM DB2 Enterprise 9	IBM AIX 5L V5.3	Microsoft COM+	05/21/07	N
***	Bull	Bull Escala PL1660R	1,616,162	3.54 USD	NR	12/16/07	IBM DB2 9.1	IBM AIX 5L V5.3	Microsoft COM+	12/17/07	N
9	IBM	IBM eServer p5 595	1,601,784	5.05 USD	NR	04/20/05	Oracle Database 10g Enterprise Edition	IBM AIX 5L V5.3	Microsoft COM+	04/20/05	N
10	FUJITSU	PRIMEQUEST 540A 16p/32c	1,354,086	3.25 USD	NR	11/22/08	Oracle Database 10g release2 Enterprise Edt	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	11/22/08	N

Top 10 TPC-C Price/Performance (as of 4 August 2010)

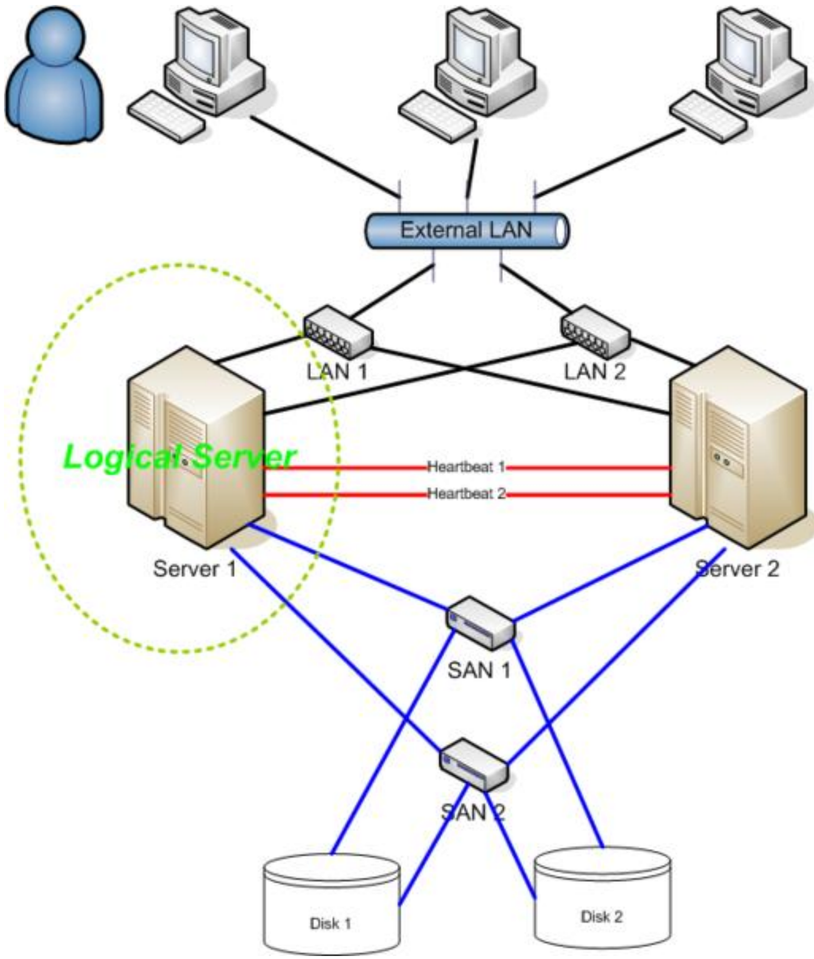
Rank	Company	System	tpmC	Price/tpmC	Watts/KtpmC	System Availability	Database	Operating System	TP Monitor	Date Submitted	Cluster
1	DELL	Dell PowerEdge T710	239,392	.50 USD	NR	11/18/09	Oracle Database 11g Standard Edition One	Microsoft Windows Server 2003 Enterprise x64 Edition	Microsoft COM+	11/18/09	N
2	hp invent	HP ProLiant ML350 G6	232,002	.54 USD	NR	05/21/09	Oracle Database 11g Standard Edition One	Oracle Enterprise Linux	Microsoft COM+	05/21/09	N
3	hp invent	HP ProLiant DL385G7	705,652	.60 USD	NR	09/01/10	Microsoft SQL Server 2005 Enterprise x64 Edition SP3	Microsoft Windows Server 2008 R2 Enterprise Edition	Microsoft COM+	04/08/10	N
4	DELL	Dell PowerEdge 2900	104,492	.60 USD	NR	02/20/09	Oracle Database 11g Standard Edition One	Microsoft Windows Server 2003 Standard Ed. x64	Microsoft COM+	02/20/09	N
5	DELL	Dell PowerEdge 2900	97,083	.68 USD	NR	06/16/08	Oracle Database 11g Standard Edition One	Microsoft Windows Server 2003 Standard Ed. x64	Microsoft COM+	06/16/08	N
6	hp invent	HP ProLiant DL380 G7	803,068	.68 USD	NR	09/01/10	Microsoft SQL Server 2005 Enterprise x64 Edition SP3	Microsoft Windows Server 2008 R2 Enterprise Ed for X64-Based Systems	Microsoft COM+	05/11/10	N
7	hp invent	HP ProLiant DL585 G7	1,193,472	.68 USD	5.93	09/01/10	Microsoft SQL Server 2005 Enterprise x64 Edition SP3	Microsoft Windows Server 2008 R2 Enterprise Edition	Microsoft COM+	06/21/10	N
8	IBM	IBM Power 780 Server Model 9179-MHB	1,200,011	.69 USD	NR	10/13/10	IBM DB2 9.5	AIX Version 6.1	Microsoft COM+	04/13/10	N
9	hp invent	HP ProLiant ML350G5	102,454	.73 USD	NR	12/31/07	Oracle Database 11g Standard Edition One	Microsoft Windows Standard x64 Etd. SP1 R2	Microsoft COM+	09/12/07	N
10	hp invent	HP ProLiant ML350G5	100,926	.74 USD	NR	06/08/07	Oracle Database 10g Standard Edition One	Oracle Enterprise Linux	Microsoft COM+	06/08/07	N

SYSTEM AVAILABILITY AND MONITORING

System Availability

- How to ensures a certain absolute degree of operational continuity during a given measurement period
- Availability includes ability of the user community to access the system, whether to submit new work, update or alter existing work, or collect the results of previous work
- Model of Availability
  - Active-Standby: HA Cluster or Failover Cluster
  - Active-Active: Server Load Balancing

HA Cluster

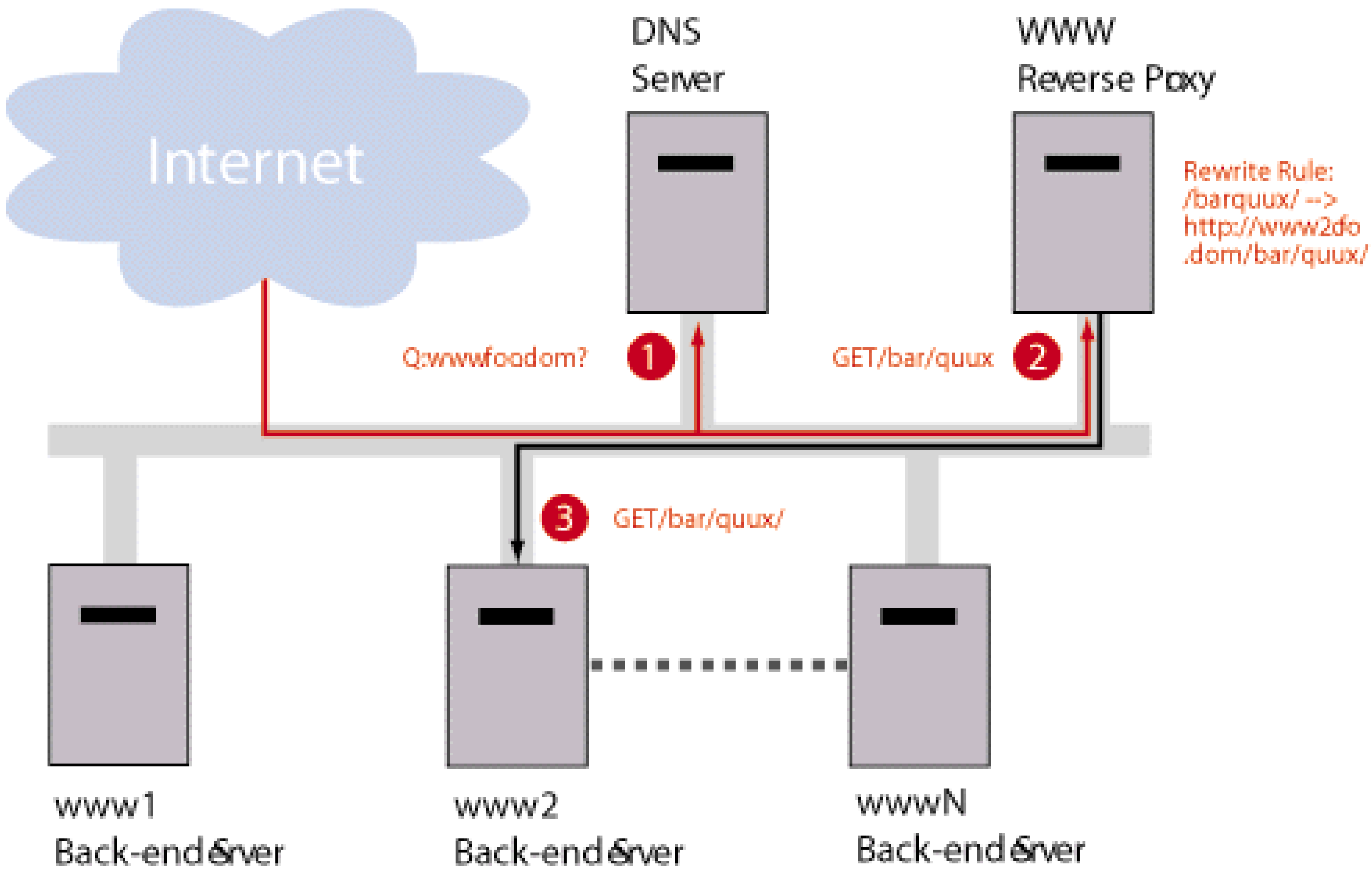


External LAN
LAN 1
LAN 2
Logical Server
Heartbeat 1
Heartbeat 2
Server 1
Server 2
SAN 1
SAN 2
Disk 1
Disk 2

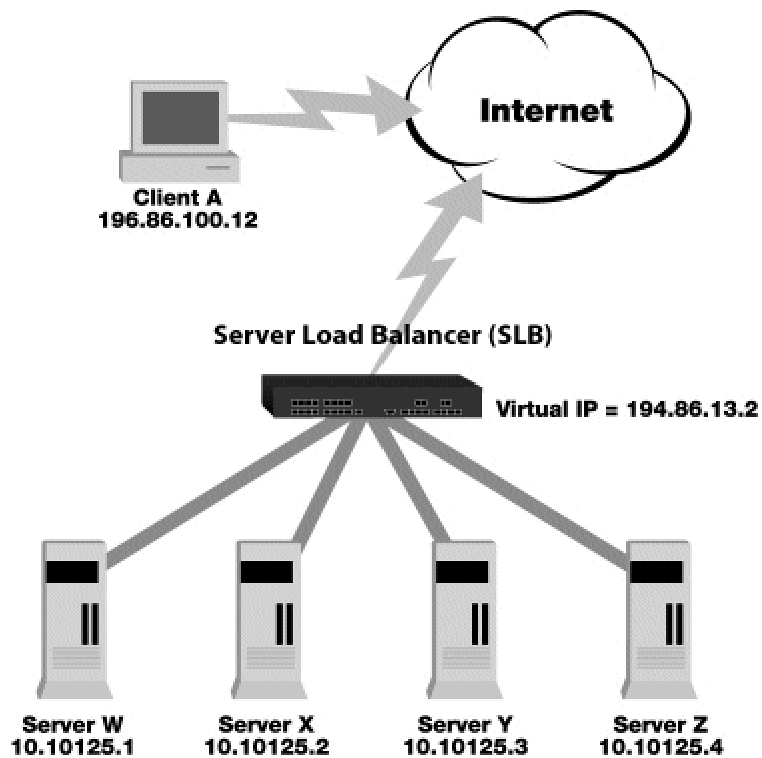
Server Load Balancing

- Spread work between two or more computers, network links, CPUs, hard drives, or other resources, in order to get optimal resource utilization, throughput, or response time
- Approaches
  - The DNS Approach
  - The Reverse Proxy Approach
  - Load balancer Approach

Reverse Proxy Approach



Server Load Balancing



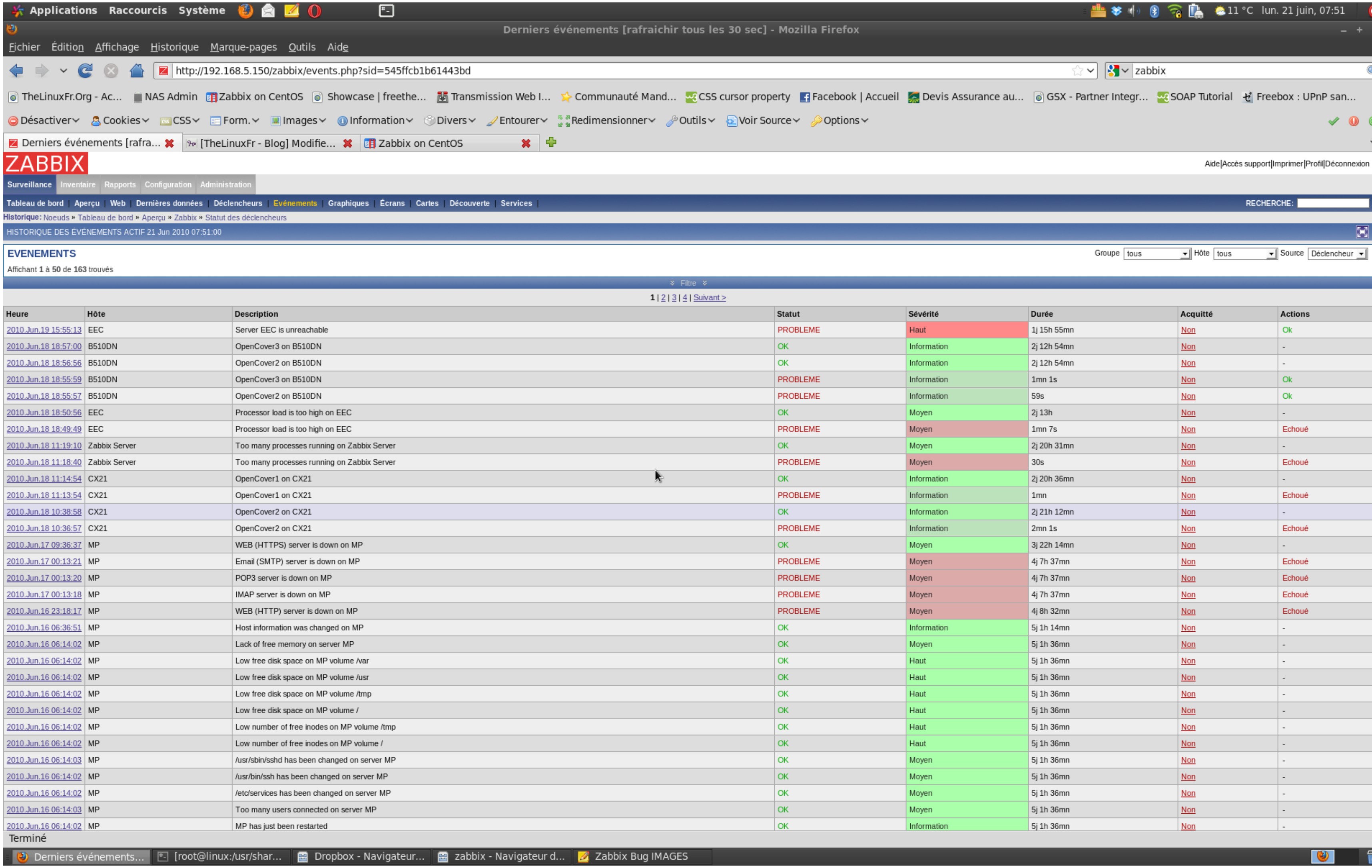
Downtime Table

Availability %	Downtime per year	Downtime per month*	Downtime per week
90%	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
98%	7.30 days	14.4 hours	3.36 hours
99%	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 min
99.8%	17.52 hours	86.23 min	20.16 min
99.9% ("three nines")	8.76 hours	43.2 min	10.1 min
99.95%	4.38 hours	21.56 min	5.04 min
99.99% ("four nines")	52.6 min	4.32 min	1.01 min
99.999% ("five nines")	5.26 min	25.9 s	6.05 s
99.9999% ("six nines")	31.5 s	2.59 s	0.605 s

Budget

Sample Network Monitoring Applications

- There are several network management applications
  - OS Tools
    - Ping, tracerout, netstat, etc.
  - Freewares
    - Zabbix, Nagios, MRTG, snort, etc.
  - Commercial
    - CA Unicenter, HP Openview, IBM Trivoli, CiscoWorks.



ZABBIX

Aide|Accès support|Imprimer|Profil|Déconnexion

Surveillance | Inventaire | Rapports | Configuration | Administration

Tableau de bord | Aperçu | Web | Dernières données | Déclencheurs | Événements | Graphiques | Écrans | Cartes | Découverte | Services

RECHERCHE:

Historique: Noeuds » Tableau de bord » Aperçu » Zabbix » Statut des déclencheurs

HISTORIQUE DES EVENEMENTS ACTIF 21 Jun 2010 07:51:00

EVENEMENTS

Groupe tous Hôte tous Source Déclencheur

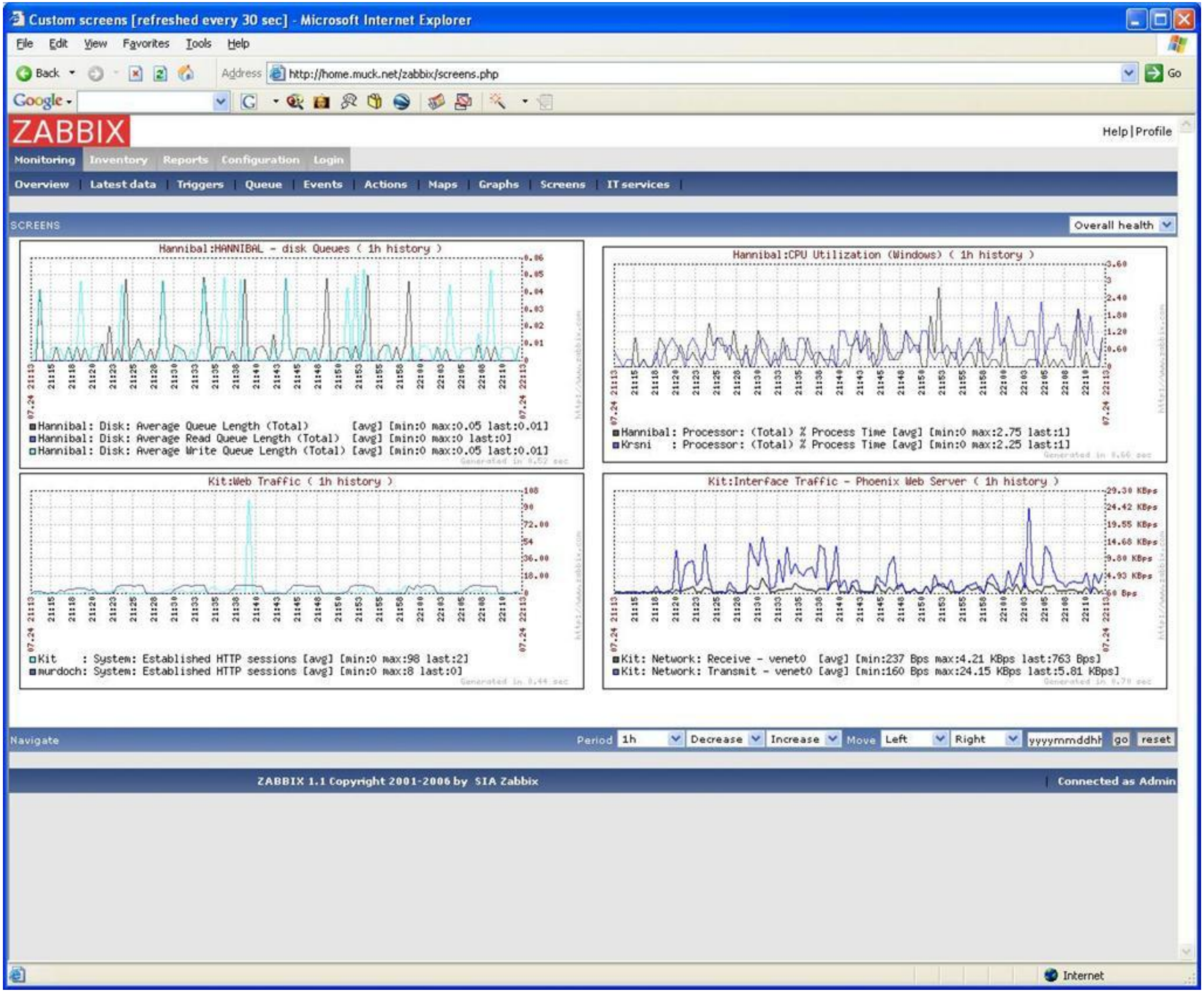
Affichant **1** à **50** de **163** trouvés

Filtre

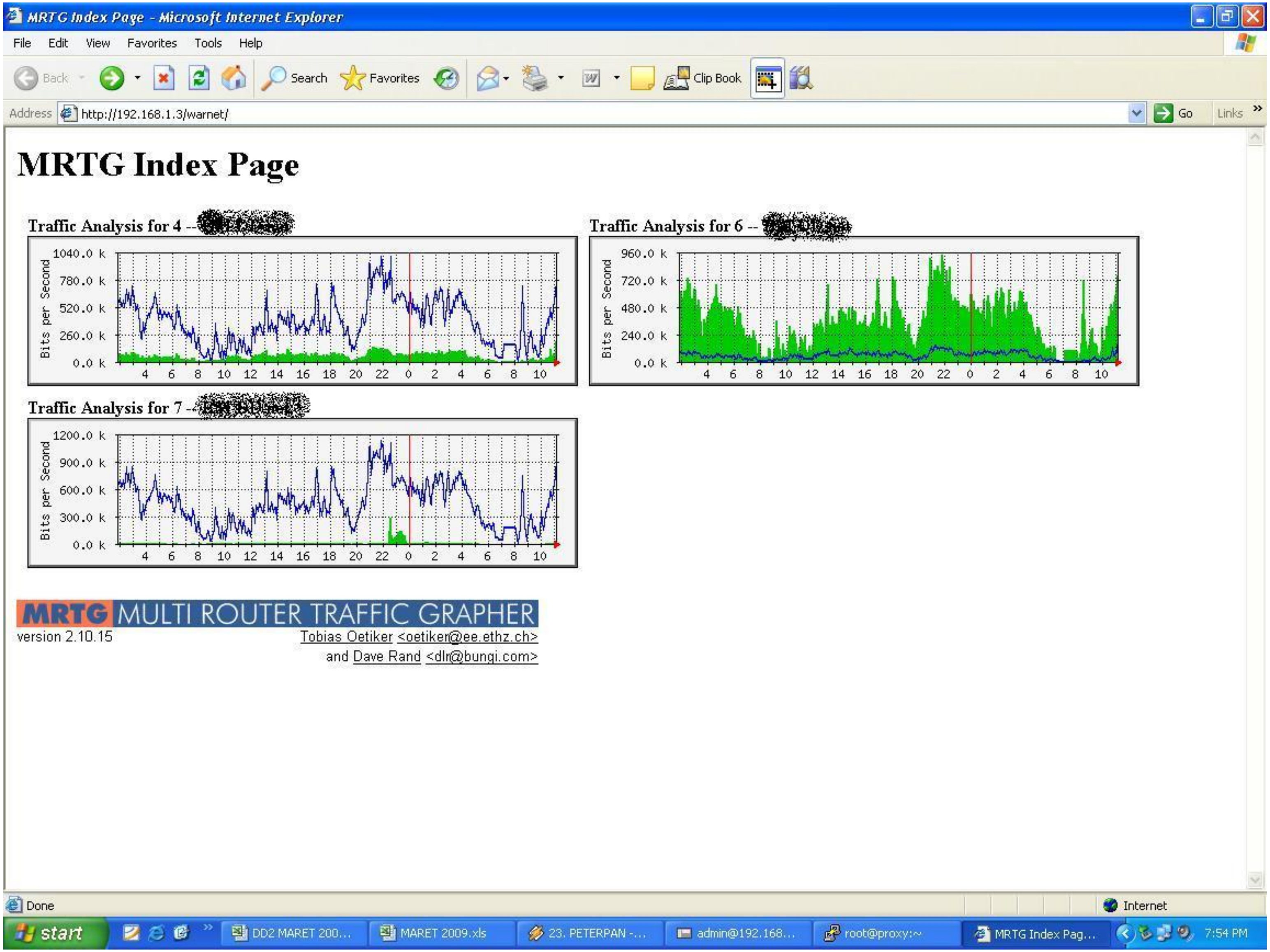
1 | 2 | 3 | 4 | Suivant >

Heure	Hôte	Description	Statut	Sévérité	Durée	Acquitté	Actions
2010.Jun.19 15:55:13	EEC	Server EEC is unreachable	PROBLEME	Haut	1j 15h 55mn	Non	Ok
2010.Jun.18 18:57:00	B510DN	OpenCover3 on B510DN	OK	Information	2j 12h 54mn	Non	-
2010.Jun.18 18:56:56	B510DN	OpenCover2 on B510DN	OK	Information	2j 12h 54mn	Non	-
2010.Jun.18 18:55:59	B510DN	OpenCover3 on B510DN	PROBLEME	Information	1mn 1s	Non	Ok
2010.Jun.18 18:55:57	B510DN	OpenCover2 on B510DN	PROBLEME	Information	59s	Non	Ok
2010.Jun.18 18:50:56	EEC	Processor load is too high on EEC	OK	Moyen	2j 13h	Non	-
2010.Jun.18 18:49:49	EEC	Processor load is too high on EEC	PROBLEME	Moyen	1mn 7s	Non	Echoué
2010.Jun.18 11:19:10	Zabbix Server	Too many processes running on Zabbix Server	OK	Moyen	2j 20h 31mn	Non	-
2010.Jun.18 11:18:40	Zabbix Server	Too many processes running on Zabbix Server	PROBLEME	Moyen	30s	Non	Echoué
2010.Jun.18 11:14:54	CX21	OpenCover1 on CX21	OK	Information	2j 20h 36mn	Non	-
2010.Jun.18 11:13:54	CX21	OpenCover1 on CX21	PROBLEME	Information	1mn	Non	Echoué
2010.Jun.18 10:38:58	CX21	OpenCover2 on CX21	OK	Information	2j 21h 12mn	Non	-
2010.Jun.18 10:36:57	CX21	OpenCover2 on CX21	PROBLEME	Information	2mn 1s	Non	Echoué
2010.Jun.17 09:36:37	MP	WEB (HTTPS) server is down on MP	OK	Moyen	3j 22h 14mn	Non	-
2010.Jun.17 00:13:21	MP	Email (SMTP) server is down on MP	PROBLEME	Moyen	4j 7h 37mn	Non	Echoué
2010.Jun.17 00:13:20	MP	POP3 server is down on MP	PROBLEME	Moyen	4j 7h 37mn	Non	Echoué
2010.Jun.17 00:13:18	MP	IMAP server is down on MP	PROBLEME	Moyen	4j 7h 37mn	Non	Echoué
2010.Jun.16 23:18:17	MP	WEB (HTTP) server is down on MP	PROBLEME	Moyen	4j 8h 32mn	Non	Echoué
2010.Jun.16 06:36:51	MP	Host information was changed on MP	OK	Information	5j 1h 14mn	Non	-
2010.Jun.16 06:14:02	MP	Lack of free memory on server MP	OK	Moyen	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	Low free disk space on MP volume /var	OK	Haut	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	Low free disk space on MP volume /usr	OK	Haut	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	Low free disk space on MP volume /tmp	OK	Haut	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	Low free disk space on MP volume /	OK	Haut	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	Low number of free inodes on MP volume /tmp	OK	Haut	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	Low number of free inodes on MP volume /	OK	Haut	5j 1h 36mn	Non	-
2010.Jun.16 06:14:03	MP	/usr/sbin/sshd has been changed on server MP	OK	Moyen	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	/usr/bin/ssh has been changed on server MP	OK	Moyen	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	/etc/services has been changed on server MP	OK	Moyen	5j 1h 36mn	Non	-
2010.Jun.16 06:14:03	MP	Too many users connected on server MP	OK	Moyen	5j 1h 36mn	Non	-
2010.Jun.16 06:14:02	MP	MP has just been restarted	OK	Information	5j 1h 36mn	Non	-

Terminé



Custom screens [refreshed every 30 sec] - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address http://home.muck.net/zabbix/screens.php
Go
ZABBIX
Help | Profile
Monitoring Inventory Reports Configuration Login
Overview | Latest data | Triggers | Queue | Events | Actions | Maps | Graphs | Screens | IT services |
SCREENS
Overall health
Hannibal:HANNIBAL - disk Queues (1h history)
Hannibal: Disk: Average Queue Length (Total) [avg] [min:0 max:0.05 last:0.01]
Hannibal: Disk: Average Read Queue Length (Total) [avg] [min:0 max:0 last:0]
Hannibal: Disk: Average Write Queue Length (Total) [avg] [min:0 max:0.05 last:0.01]
Hannibal:CPU Utilization (Windows) (1h history)
Hannibal: Processor: (Total) % Process Time [avg] [min:0 max:2.75 last:1]
Krsni : Processor: (Total) % Process Time [avg] [min:0 max:2.25 last:1]
Kit:Web Traffic (1h history)
Kit : System: Established HTTP sessions [avg] [min:0 max:98 last:2]
murdoch: System: Established HTTP sessions [avg] [min:0 max:8 last:0]
Kit:Interface Traffic - Phoenix Web Server (1h history)
Kit: Network: Receive - veneto [avg] [min:237 Bps max:4.21 KBps last:763 Bps]
Kit: Network: Transmit - veneto [avg] [min:160 Bps max:24.15 KBps last:5.81 KBps]
Navigate
Period 1h Decrease Increase Move Left Right yyyymmddhh go reset
ZABBIX 1.1 Copyright 2001-2006 by SIA Zabbix
Connected as Admin
Internet


MRTG Index Page - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Clip Book
Address http://192.168.1.3/warnet/
Go Links
MRTG Index Page
Traffic Analysis for 4 -- [redacted]
Traffic Analysis for 6 -- [redacted]
Traffic Analysis for 7 -- [redacted]
Bits per Second
1040.0 k 780.0 k 520.0 k 260.0 k 0.0 k
960.0 k 720.0 k 480.0 k 240.0 k 0.0 k
1200.0 k 900.0 k 600.0 k 300.0 k 0.0 k
4 6 8 10 12 14 16 18 20 22 0 2 4 6 8 10
MRTG MULTI ROUTER TRAFFIC GRAPHER
version 2.10.15
Tobias Oetiker <oetiker@ee.ethz.ch>
and Dave Rand <dlr@bungi.com>
Done
Internet
start
DD2 MARET 200...
MARET 2009.xls
23. PETERPAN -...
admin@192.168...
root@proxy:~
MRTG Index Pag...
7:54 PM

SERVER CONSOLIDATION

Based on "Virtualization Assessment" by Matt Behrens

Main Problems

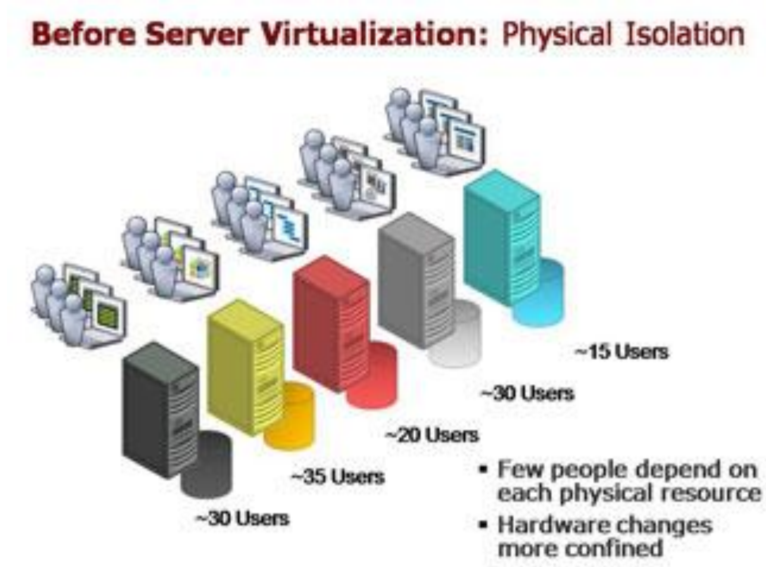
Old applications rely on many servers

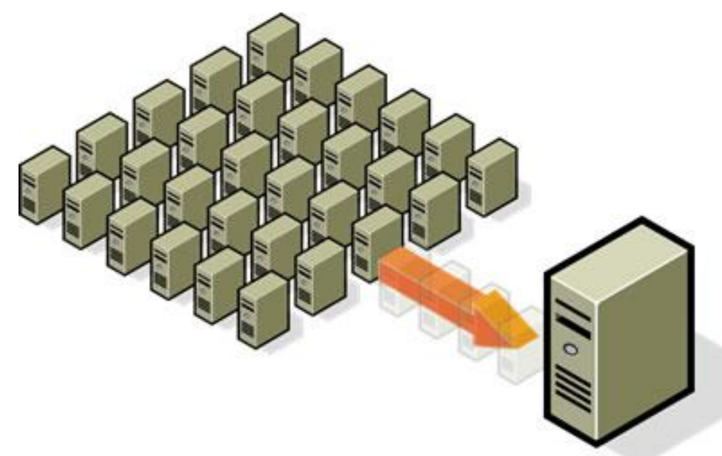
- High operation cost: maintenance, electricity, etc.
- Heterogeneous environments
- Difficult to migrate

New servers are very powerful and under-utilized

- Some resources remain idle

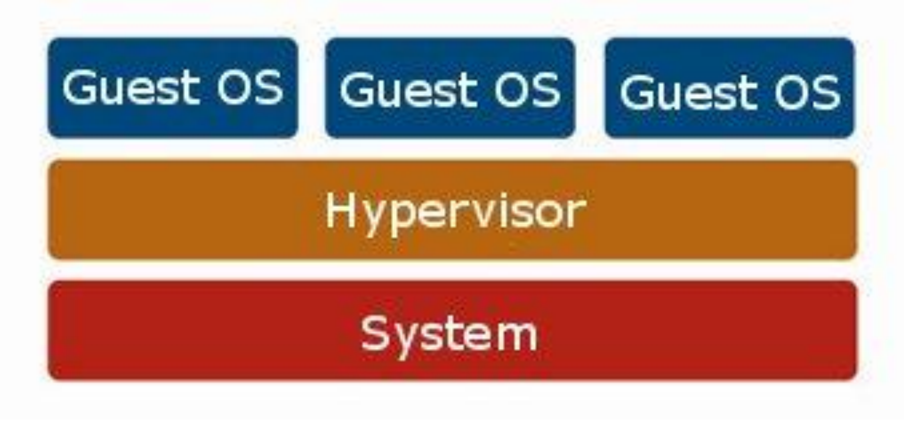
Reduce costs by consolidating servers





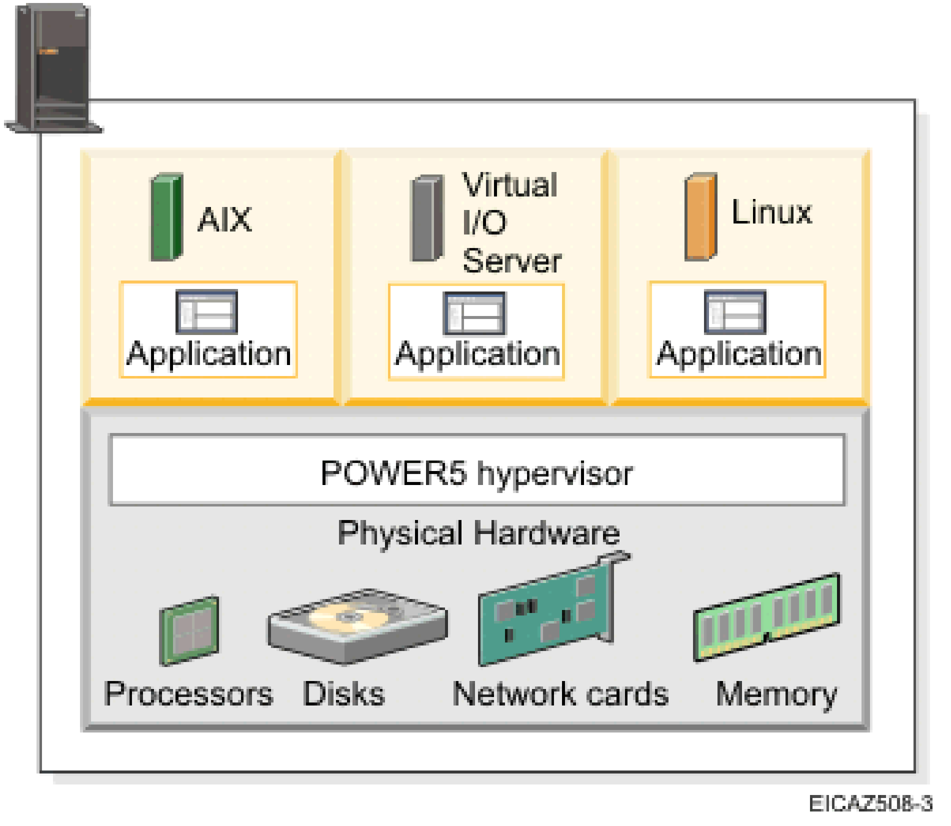
The Hypervisor

- The role of the Hypervisor in supporting Guest Operating Systems on a single machine.



Hardware Virtualization (example)

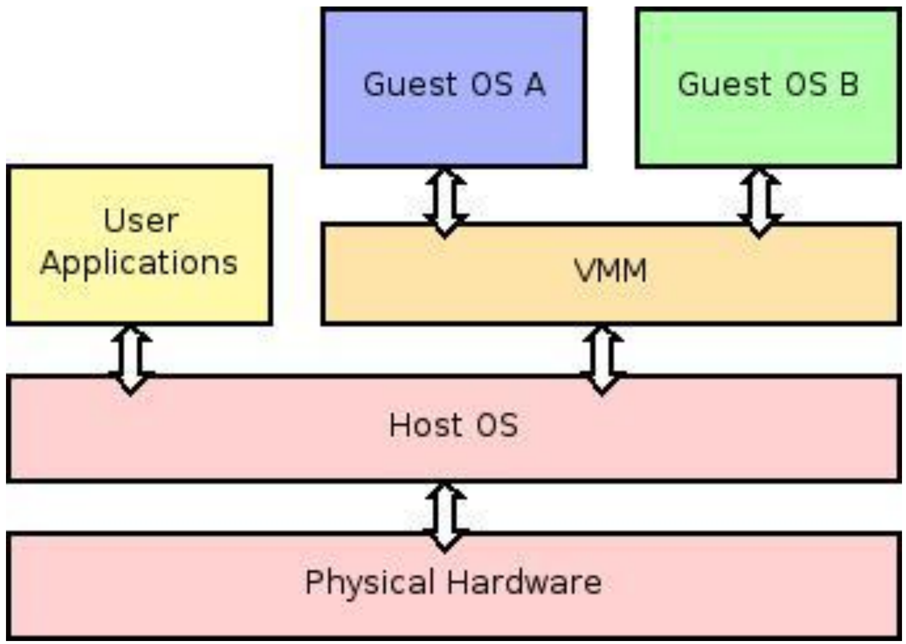
- IBM pSeries Servers



http://publib.boulder.ibm.com/infocenter/eserver/v1r2/topic/eicaz/eicaz508.gif

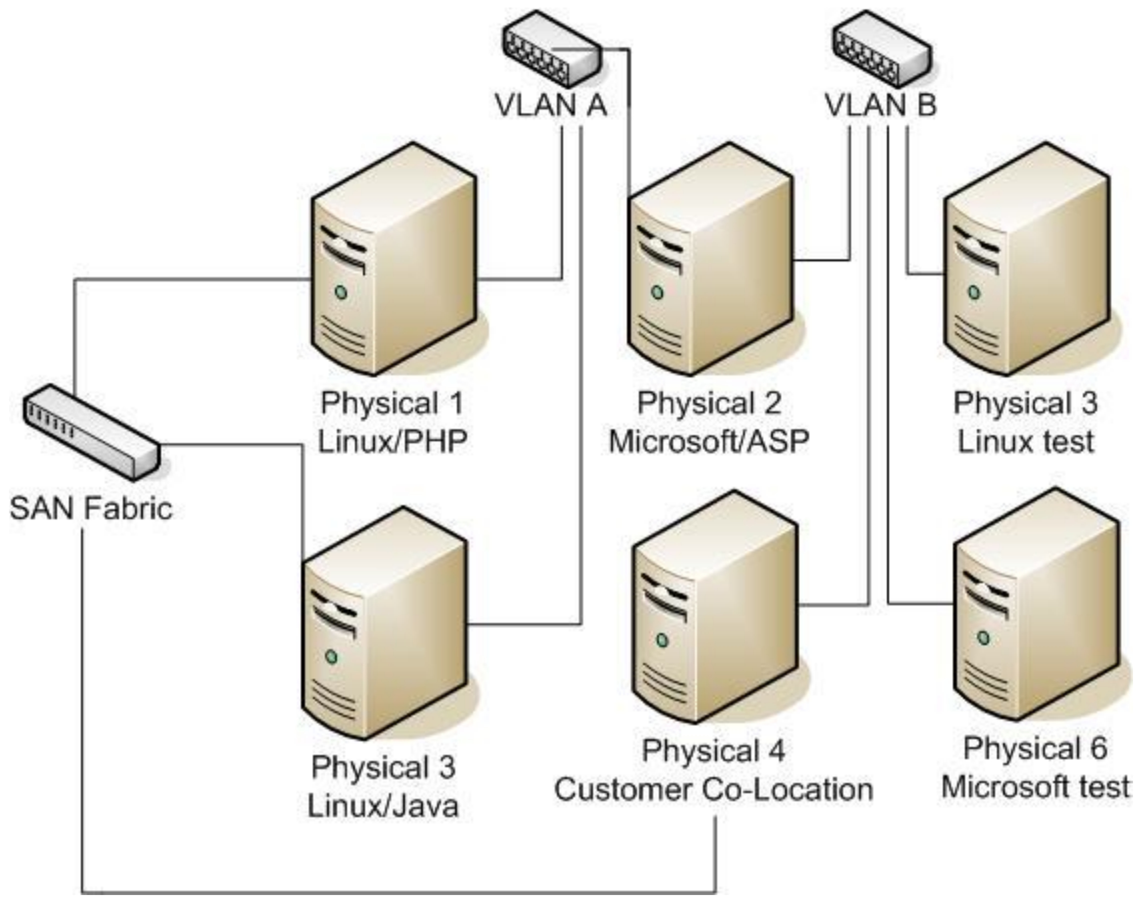
Software Virtualization (example)

- VMware Server (GSX)

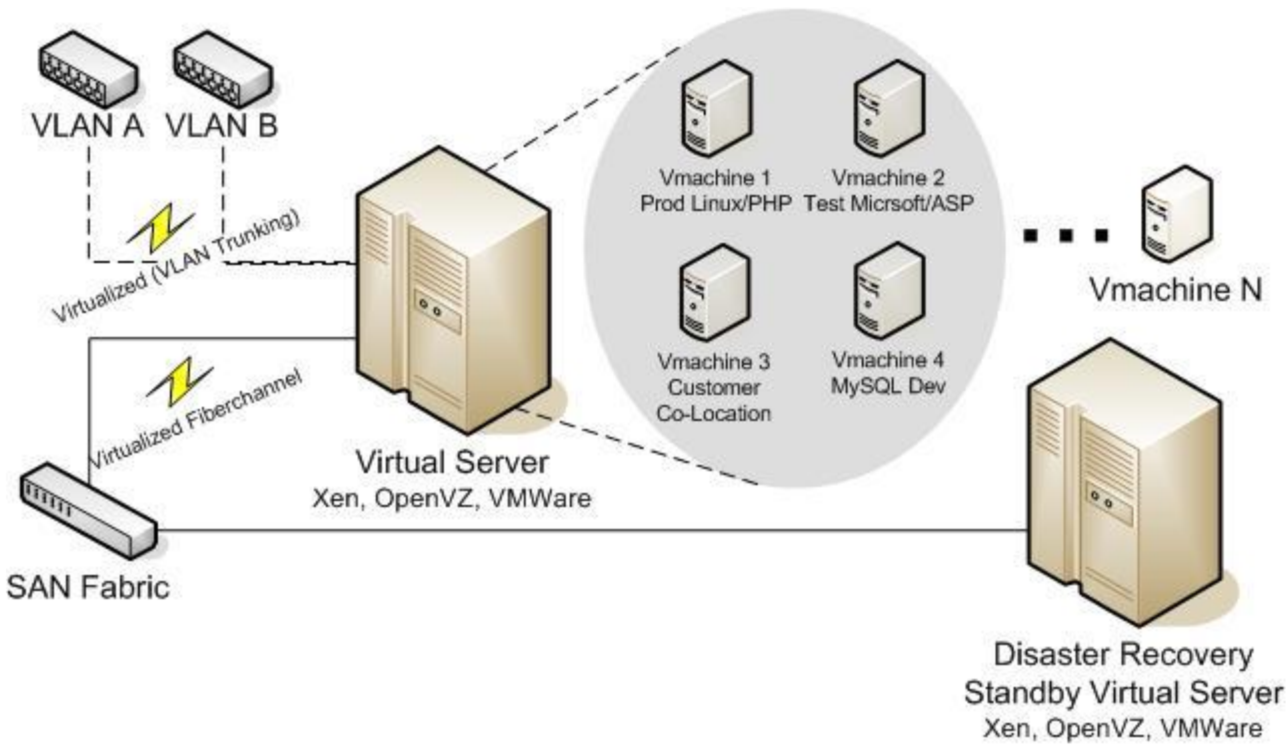


http://openlab-mu-internal.web.cern.ch/openlab-mu-internal/openlab-II_Projects/Platform_Competence_Centre/Virtualization/Virtualization.asp

Current Architecture



Virtualized Architecture



SECURITY

Based on Kurose and Ross,

"Computer Networking: A Top-Down Approach"

Security Management

- Security must be considered both at infrastructure level and application level
- Infrastructure level
  - Control physical access
  - Operating system level = “hardening”
  - Secure coding
    - Avoid certain coding patterns to remove vulnerbilities
  - Network security

Security Equipment

- Firewall
- IDS / IPS
- Anti-Virus
- Spam Filter
- Authentication

Two-Factor Authentication

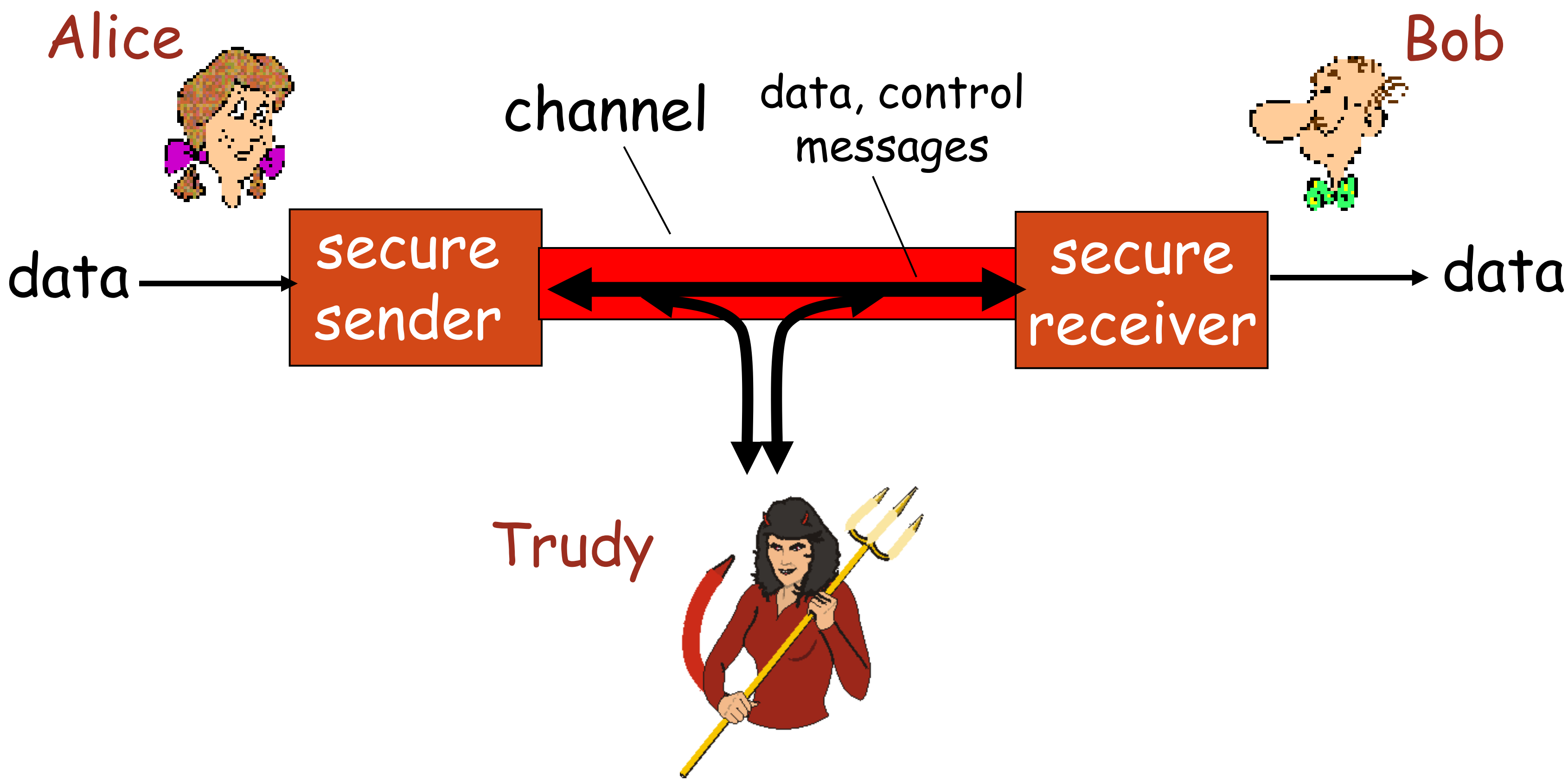
- Something you know
  - Password
- Something you have
  - ID Card, Credit Card, Mobile Phone
- Something you are
  - Biometric: retina, voice, fingerprint, etc.

Authentication Devices

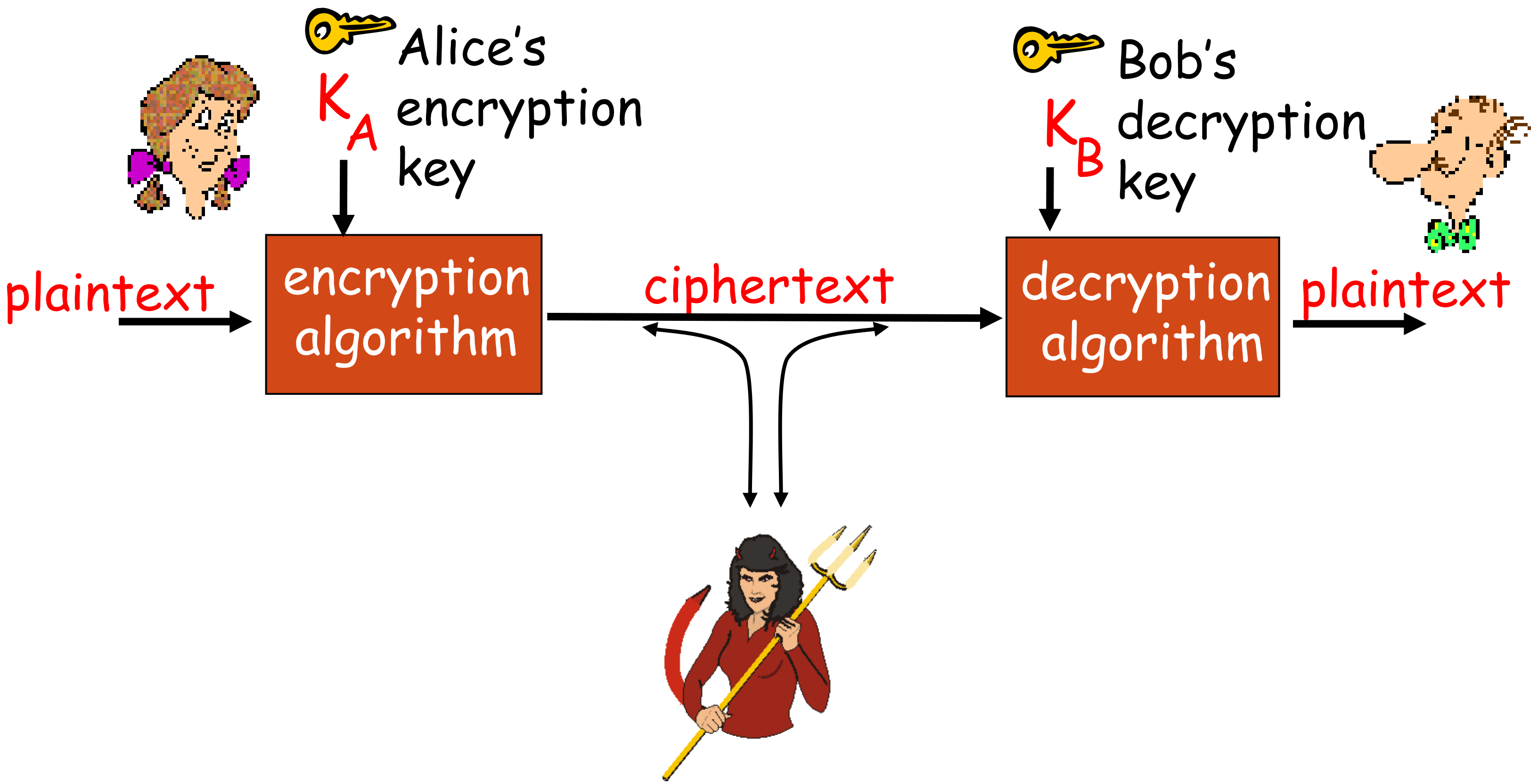
What is Network Security?

- Confidentiality: only sender, intended receiver should "understand" message contents.
- Authentication: confirm identity of each other.
- Message Integrity: ensure message not altered (in transit, or afterwards) without detection.

Friends and Enemies: Alice, Bob, Trudy



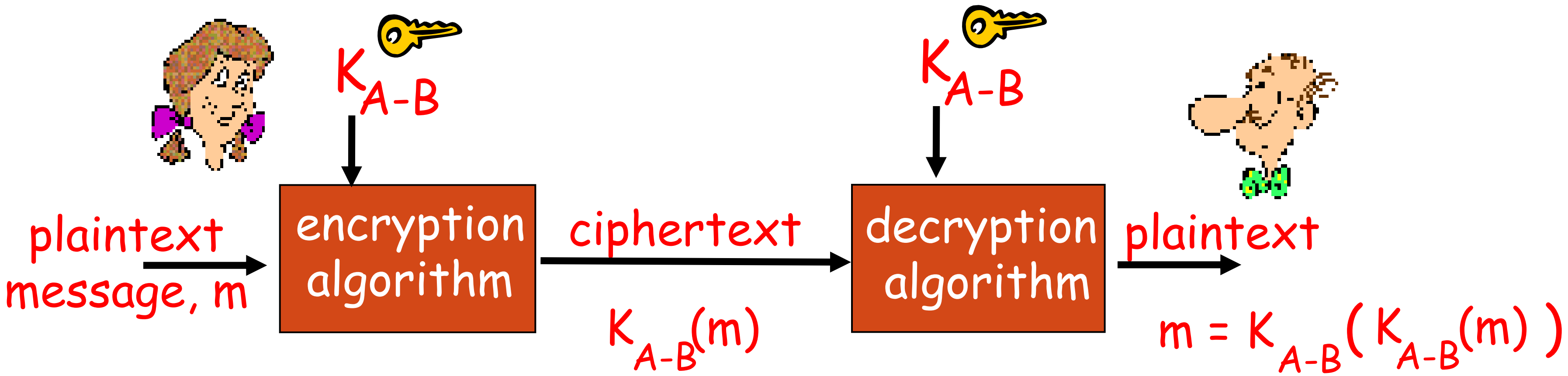
The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

Symmetric key cryptography



- symmetric key crypto:
  Bob and Alice share same (symmetric) key: K_{A-B}
- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- Q: how do Bob and Alice agree on key value?

Symmetric key crypto: DES

DES: Data Encryption Standard

- US encryption standard [NIST 1993]
- 56-bit symmetric key, 64-bit plaintext input
- How secure is DES?
  - DES Challenge: 56-bit-key-encrypted phrase ("Strong cryptography makes the world a safer place") decrypted (brute force) in 4 months
  - no known "backdoor" decryption approach
- making DES more secure:
  - use three keys sequentially (3-DES) on each datum
  - use cipher-block chaining

Public Key Cryptography

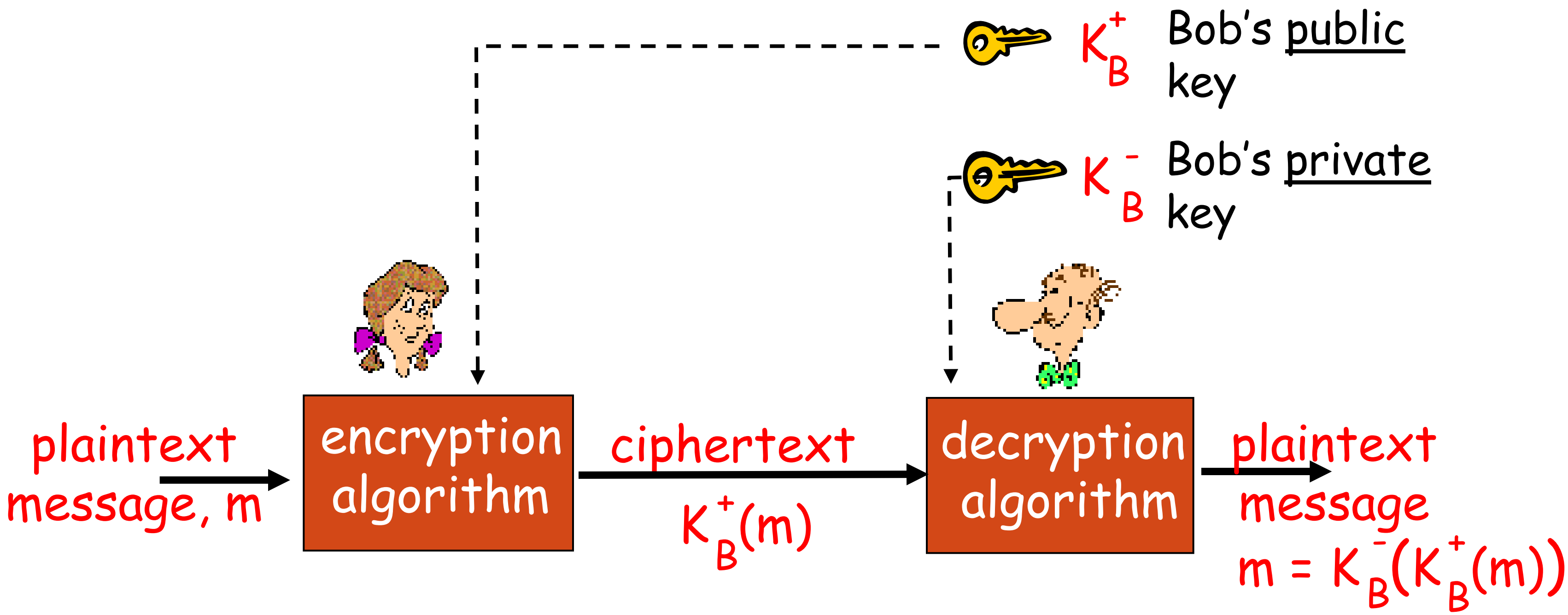
symmetric key crypto

- Sender and receiver know shared secret key
- Q: how to agree on key in first place (particularly if never "met")?

public key cryptography

- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver

Public key cryptography



Digital Signatures

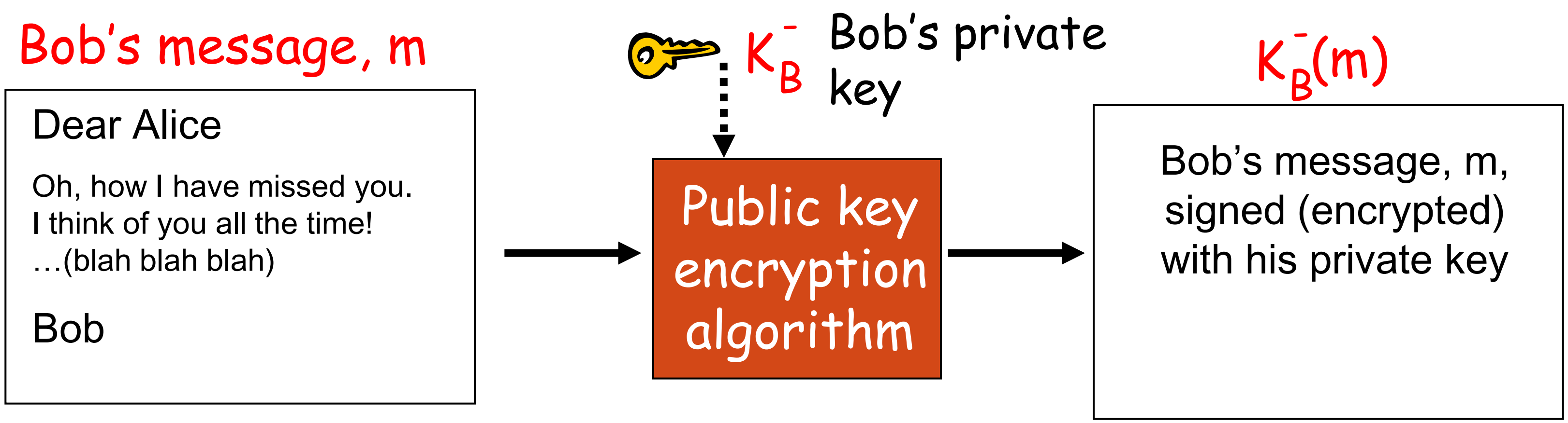
Cryptographic technique analogous to hand-written signatures.

- sender (Bob) digitally signs document
  - establishing he is document owner/creator.
- verifiable, nonforgeable:
  - recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document

Digital Signatures

Simple digital signature for message m:

- Bob signs m by encrypting with his private key K_B^-, creating "signed" message, $K_B^-(m)$



Digital Signatures (more)

- Suppose Alice receives msg m, digital signature $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- If $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

- ✓ Bob signed m.
- ✓ No one else signed m.
- ✓ Bob signed m and not m'.

Non-repudiation:

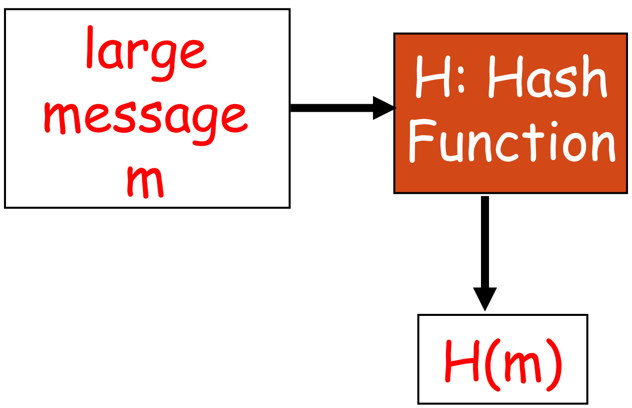
- ✓ Alice can take m, and signature $K_B^-(m)$ to court and prove that Bob signed m.

Message Digests

Computationally expensive to public-key-encrypt long messages

Goal: fixed-length, easy- to-compute digital "fingerprint"

- apply hash function H to *m*, get fixed size message digest, *H(m).*



Hash function properties:

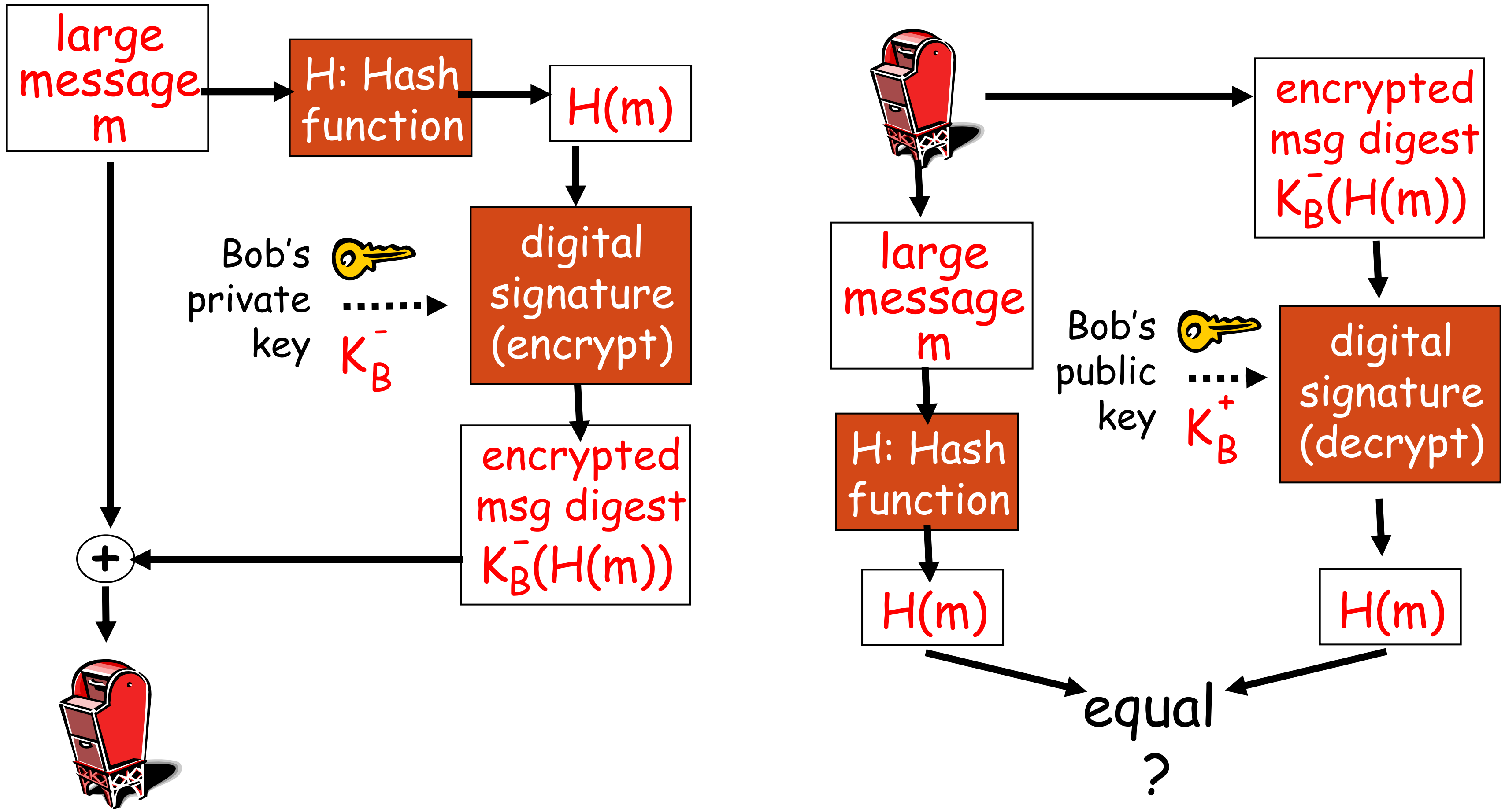
- many-to-1
- produces fixed-size msg digest (fingerprint)
- given message digest x, computationally infeasible to find m such that x = H(m)

Example: MD5 and SHA-1

Digital signature = signed message digest

Bob sends digitally signed message:

Alice verifies signature and integrity of digitally signed message:



PKI Devices

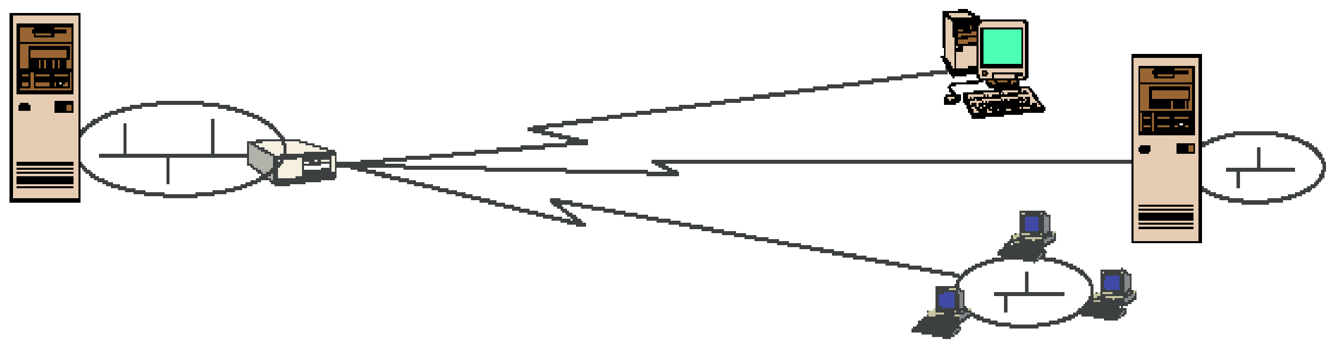
Smart Card

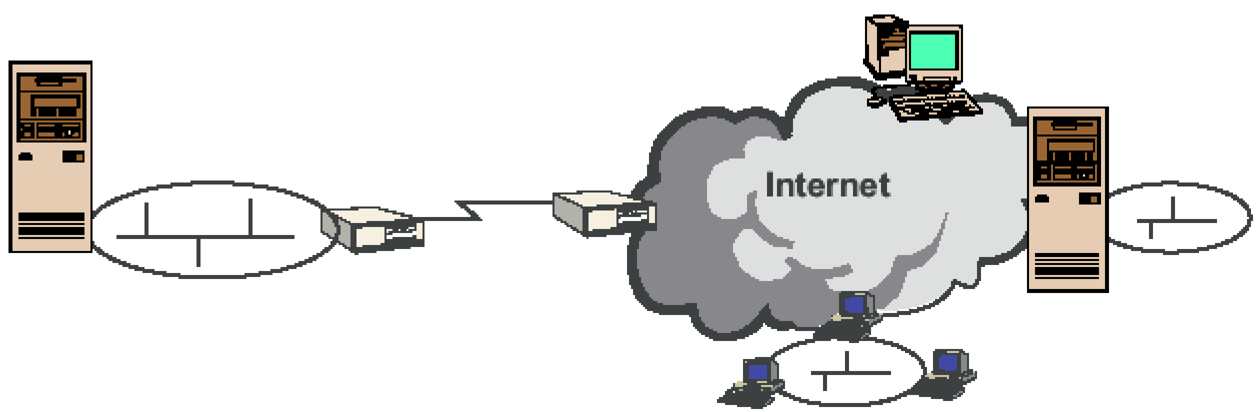
- Pocket-size card with circuit to process information
- Private & public keys
- Digital signing

USB Token

- USB type device
- Provide functions similar to smart card
- No need for readers

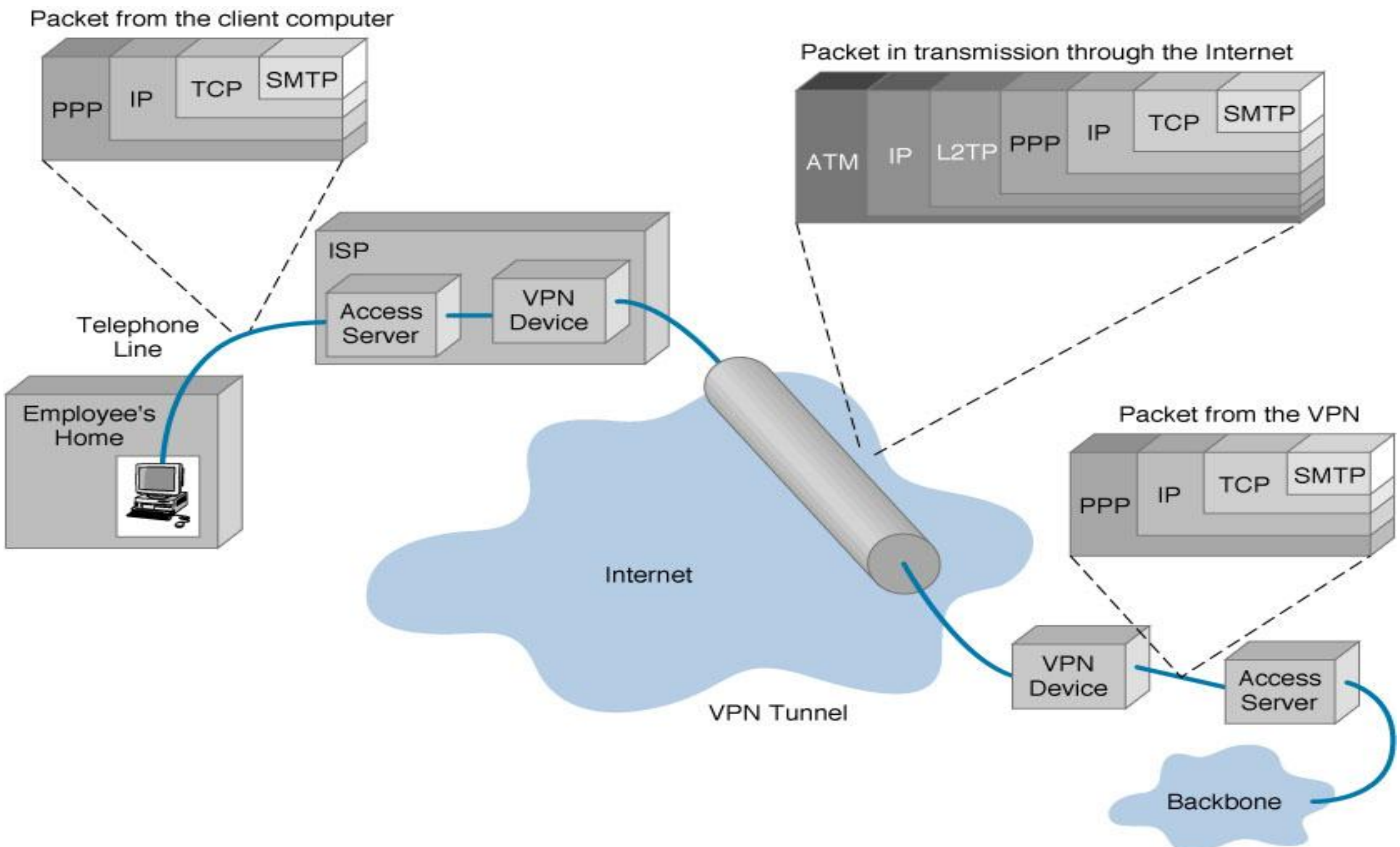
VPN





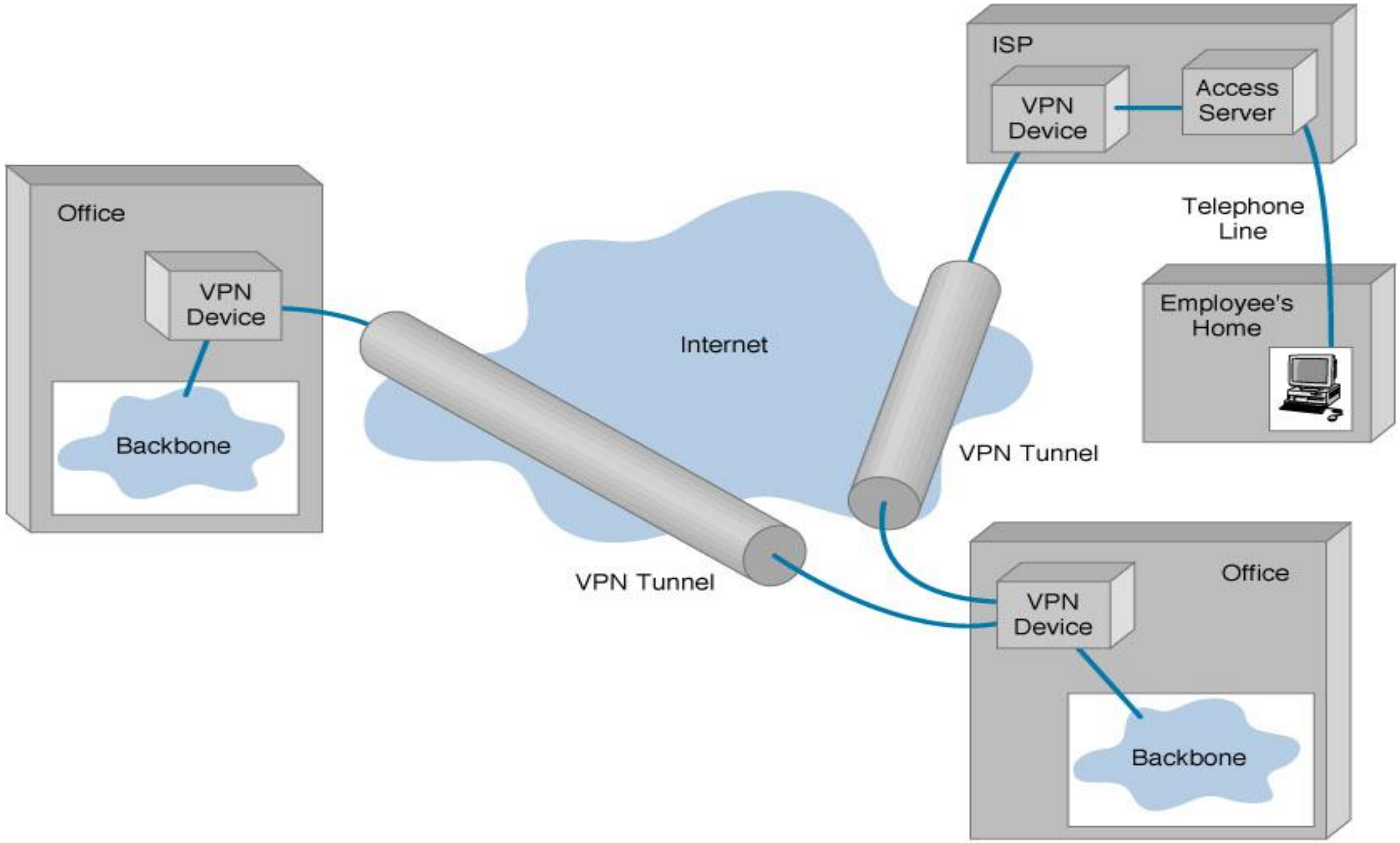
From: Fred Baker, "Virtual Private Networks"

VPN Encapsulation of Packets



From: D. Ashikyan et al, "Virtual Private Networks (VPN)"

VPN: Basic Architecture



From: D. Ashikyan et al, "Virtual Private Networks (VPN)"

References

- J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, 5[nd] Edition, Addison Wesley, 2010.
- Netsaint, http://www.netsaint.org.

References

- J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison Wesley, 2001.
- The SimpleWeb Tutorials, http://www.simpleweb.org/tutorials/.
- Electronic and telecommunication Institute, *Lessons about SNMP*, http://www.et.put.poznan.pl/snmp/main/mainmenu.html.
- Yoram Cohen, *SNMP – Simple Network Management Protocol*, http://www.rad.com/networks/1995/snmp/snmp.htm.