Data Security Issues in SAN & Ethernet Fabrik

SAN和以太网Fabric中的数据安全问题

Jean-Luc Tarik Aslan 02.02.2012
PhD student Uni-Bonn FKIE Institute
波恩大学FKIE研究所博士生

Lecture content 讲座内容

Another view of the topic, namely from the production point of view.

- SAN Operation Problem is Known
- Lan operation problem is known
- SAN technologyInfrastructure
- Infrastructure Complexity & Data protection
- Ethernet Data Center Fabric

本课题的另一种观点，即从生产的角度。

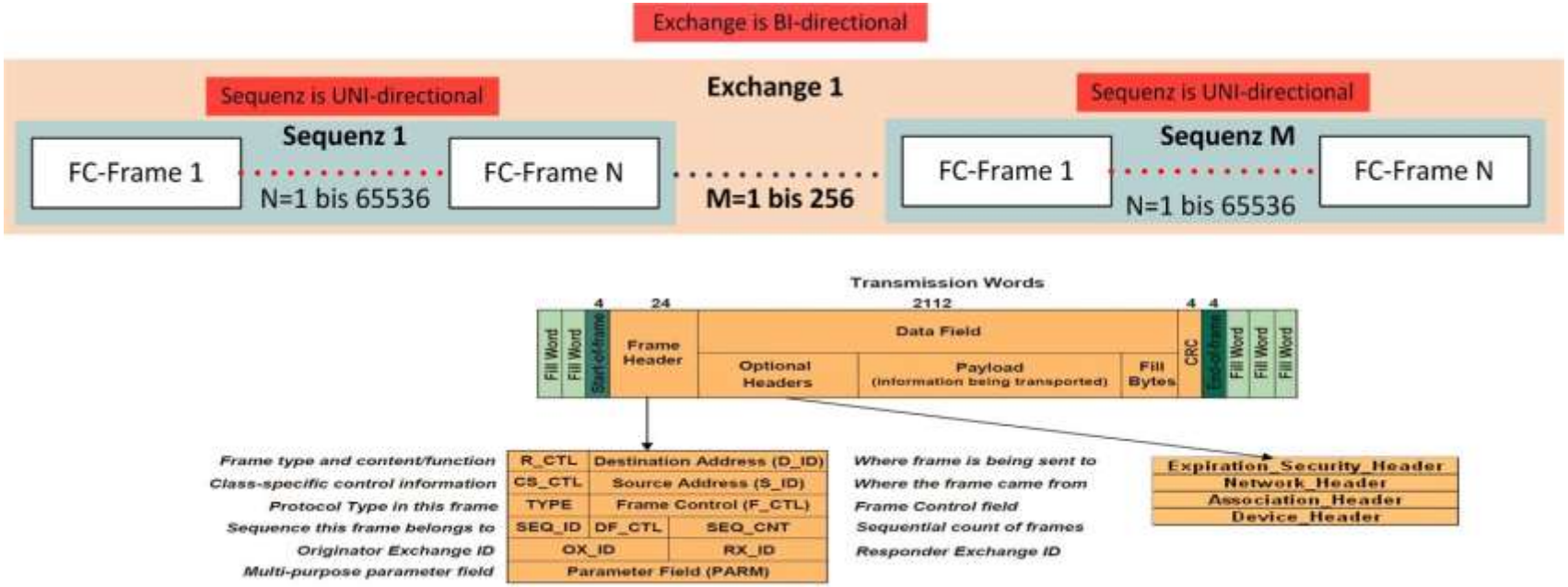
- 已知SAN操作问题
- 局域网操作问题已知
- SAN技术
- 基础设施
- 基础设施复杂性和数据保护
- 以太网数据中心结构

Technology SAN

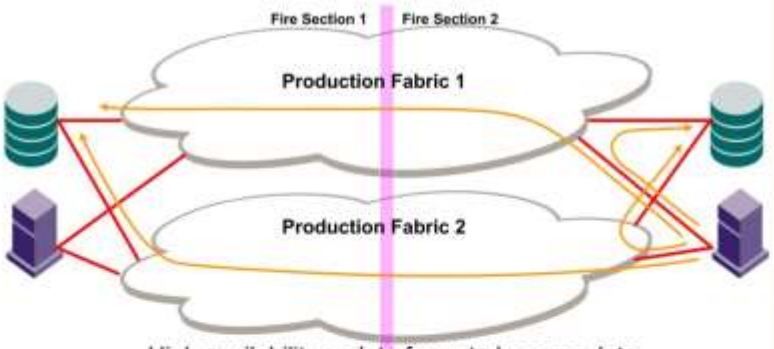
SAN : What is this?

- Networking of data storage systems
- Efficient transport of data
- Uses the old SCSI protocol to address device.
- Transport protocol may be different
- Transport protocol decision is often dependent on financial framework
- Is a summary of
  - **Daten-Storage Anlage**
  - **Server Interface (HBA) inkl Drivers**
  - **Transport Switch**
  - **Verkabelungsinfrastruktur**

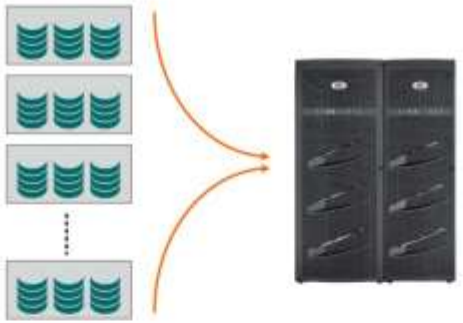
FC Exchange


Exchange is BI-directional
Exchange 1
Sequenz is UNI-directional
Sequenz 1
FC-Frame 1
N=1 bis 65536
FC-Frame N
M=1 bis 256
Sequenz is UNI-directional
Sequenz M
FC-Frame 1
N=1 bis 65536
FC-Frame N
Transmission Words
4
24
2112
4
4
Fill Word
Fill Word
Start-Of-Frame
Frame Header
Data Field
Optional Headers
Payload (information being transported)
Fill Bytes
CRC
End-Of-Frame
Fill Word
Fill Word
Fill Word
Frame type and content/function
Class-specific control information
Protocol Type in this frame
Sequence this frame belongs to
Originator Exchange ID
Multi-purpose parameter field
R_CTL
Destination Address (D_ID)
CS_CTL
Source Address (S_ID)
TYPE
Frame Control (F_CTL)
SEQ_ID
DF_CTL
SEQ_CNT
OX_ID
RX_ID
Parameter Field (PARM)
Where frame is being sent to
Where the frame came from
Frame Control field
Sequential count of frames
Responder Exchange ID
Expiration_Security_Header
Network_Header
Association_Header
Device_Header

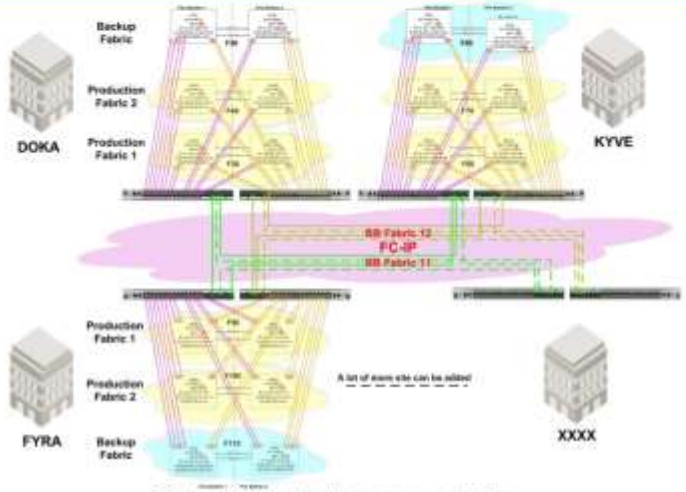
Operation Goal



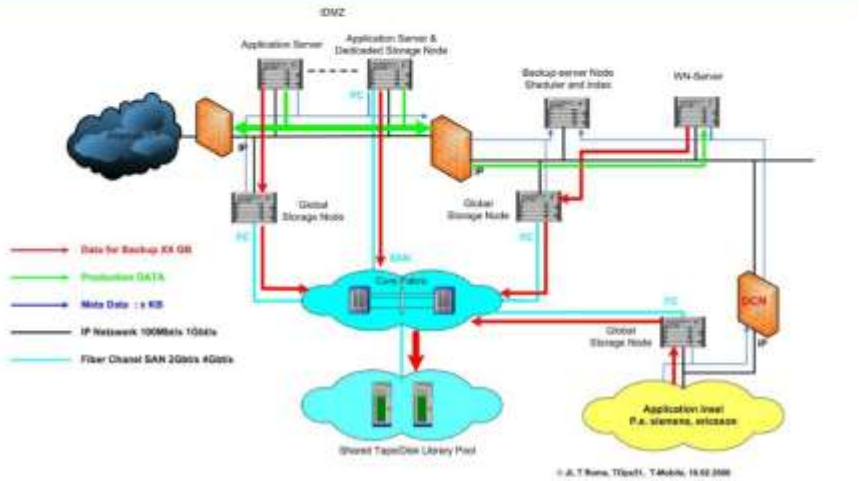
High availability : a lot of way to become data
Performance : 2, 4, 8 Gbits and security



Storage device Consolidation (speed, maintenace, availability)
Backup device Consolidation (xx tape Library→ 1 Disc Library virtualisation)

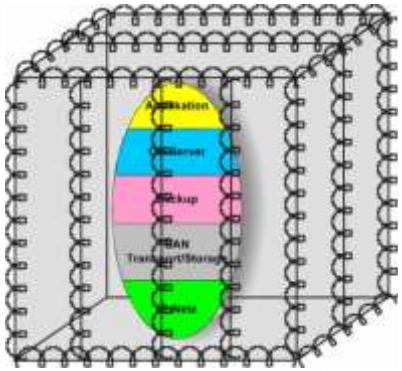


Global Disaster Recovery solution



Tape Library Consolidation
Central Backup and Sox - Reduce opex

Advantage: Optimization of data centers



Application and System Provider….

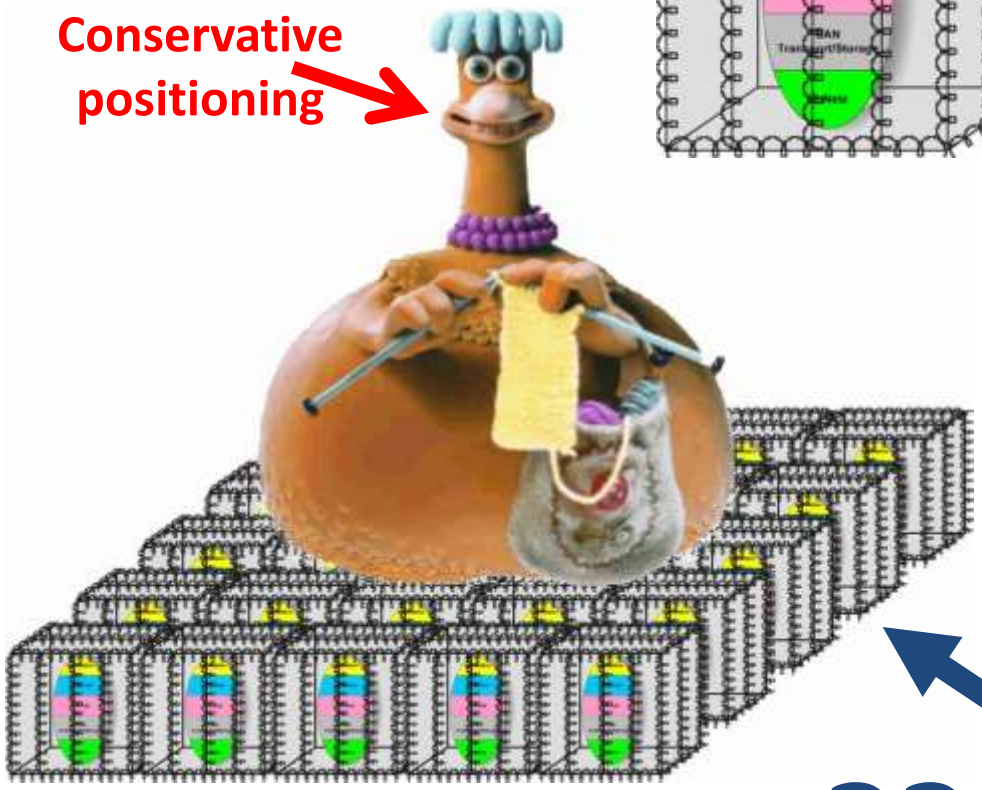
Project Manager …

My application, my server

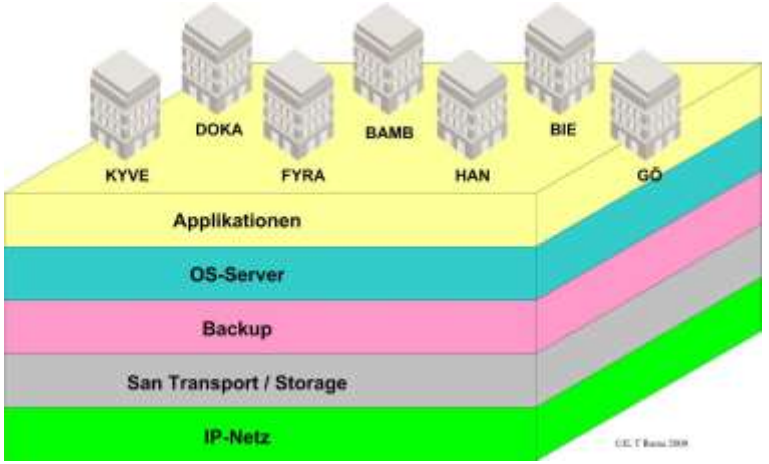
my storage, my network…..

Go away!!!

Conservative positioning



- ~70% memory usage
- Flexible
- Security??



??

- 20% memory usage??
- Inflexible
- Safe

Living technology

Major technology renewing
each 2 Year

Major Security renewing
each 6 Month

SAN Technology Evolurion last few Year

1997	First Fiber Channel Protocol
.....	.....
2004	2Gbits Technology
2005	iSCSI Technology & FCip
2006	4 Gbits Technology
2008	8 Gbits Technology
2008	FCoE Technology
2010	FCoE Technology & 16Gbits FC

1997	Fibre-Channel Protocol
1999	1Gbits Technology
2002	255 ports Core Switch 2Gbits
2003	2Gbits Technology
2004	FC Routing 2Gbits
2005	FC 4Gibts
2006	FC Director with 380Port
2006	FC Router 4Gbits
2007	opinion revising about san security
2007	Virtualization in SAN - Virtual WWN
2007	8Gbits Technology and HBA
2008	FCoE
2008	890Ports Datacenter Core MP 8Gbits
2008	Multiprotocol HBA: CNA (Converged Network Adaptor)
2009	FCoE Switch and Blade
2010	16Gbits Technology, 64/66bits, fillword mode 3
2011	Virtual Cluster switching & VDX

Price ←←← ja pro gbits übertragen aber Investition bleibt sehr hoch

Electric power ←←← wenn jede 2J man alle 2J alles erneuert $$$

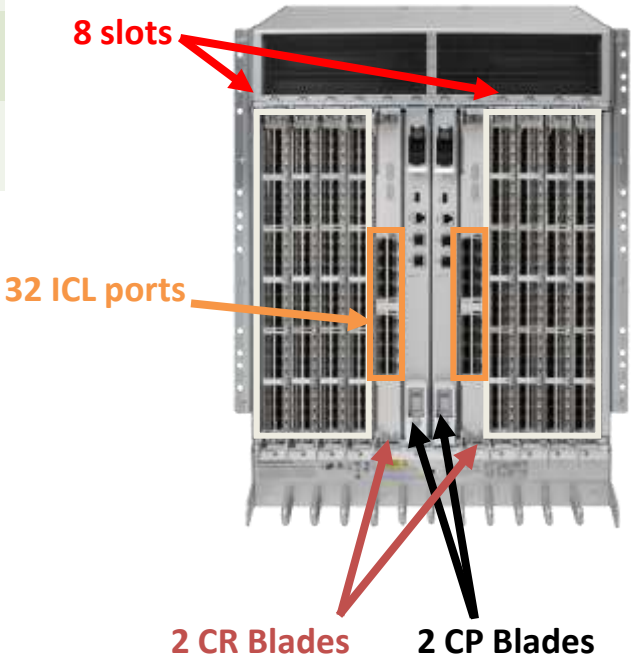
Gbits transmission ←←← wenn die Verkabelungsinfrastruktur es erlaubt

Security ←←← wenn richtig implementiert (zeit??)

New 16gbits Technology

	Condor-3	Condor-2
Technology	40/45nm	90nm
Data path	**64 bits**	**32 bits**
Number of Ports	48	40
FC Speeds	16-**10**-8-4-2	8-4-2-1
Power	40W	30W
Frames switching per second	**L2 = 420 M**	**L2 = 212 M**
FC Security	**32 Gbps encryption (6us latency)** **32 Gbps decryption(6us latency)**	No
FC Compression	**64 Gbps compression(6us latency)** **64 Gbps decompression(6us latency)**	No

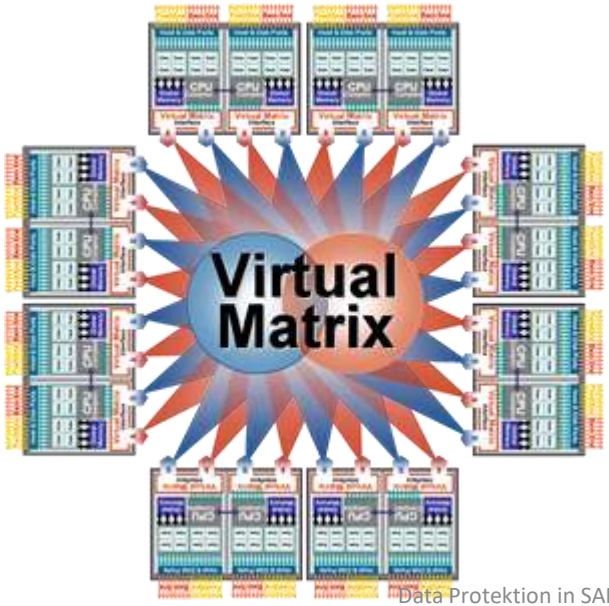
- Up to 384 ports at full 16 Gbps speed
- Up to 32 optical Inter-Chassis Link (ICL) ports
- 8.2 Tbps total chassis bandwidth
  - 6.1 Tbps universal ports
  - 2.1 Tbps ICL bandwidth
- 512 Gbps bandwidth per slot

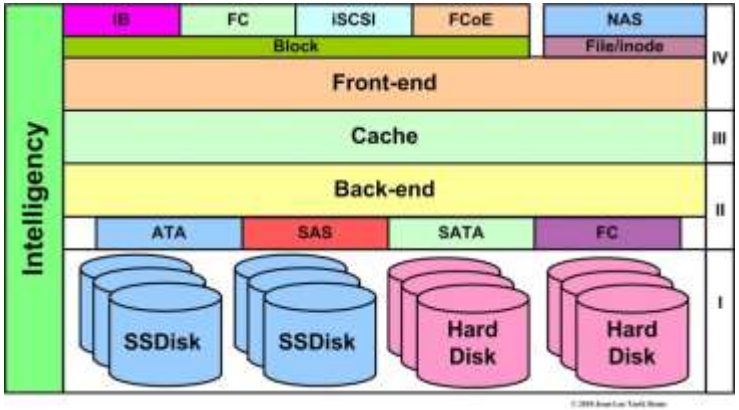


6 DCX in mesh with ICL gekoppelt ➔ fabric upto ~2300 ports 16gbits oder ~4000 ports 8gibts

Storage roadmap, turnaround time

- SSD drives are industry capable
- Tiering of data
- Local storage virtualization in storage
- Global storage virtualization in SAN engine
- Virtualization of Tape Library





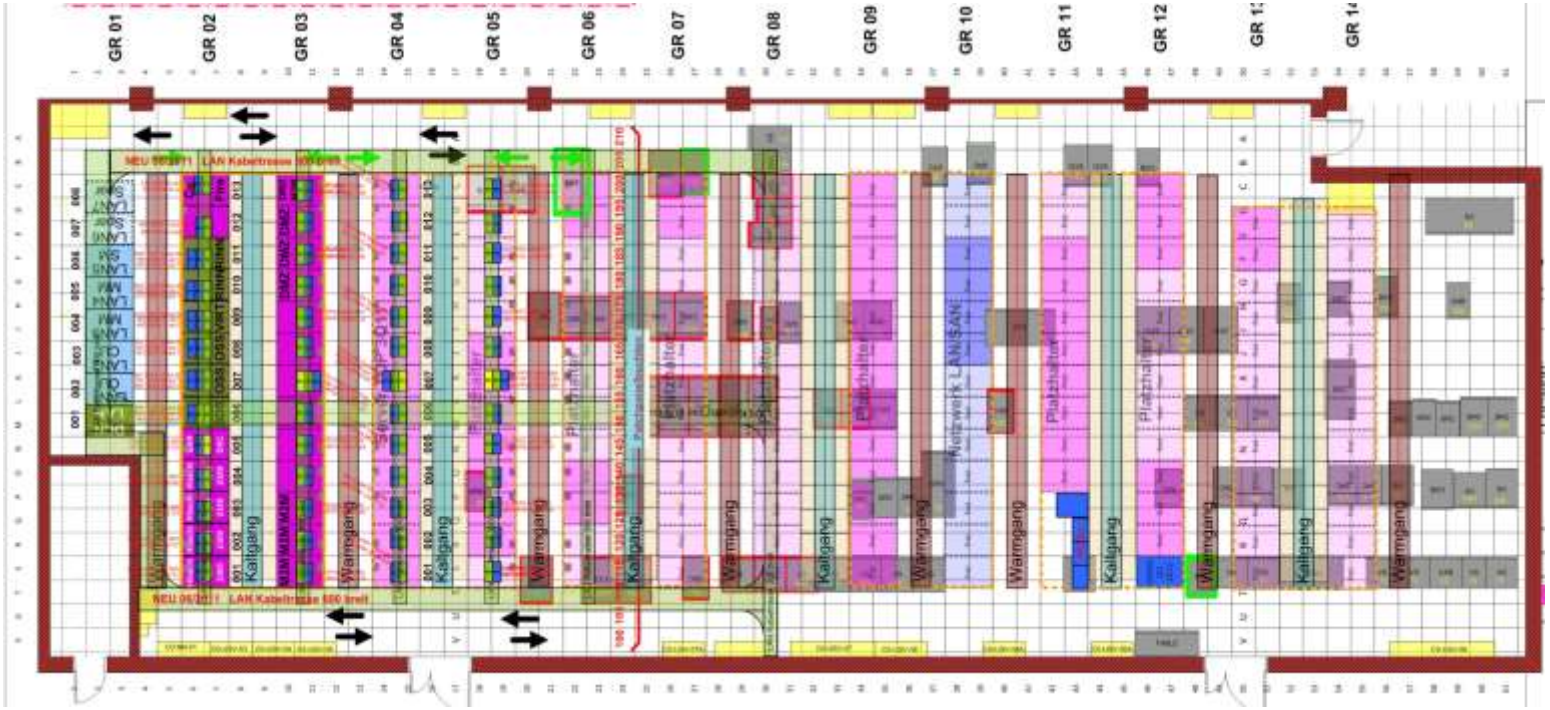
Infrastructure

Infrastructure costs and complexity

Zwischen GR01-GR05 :

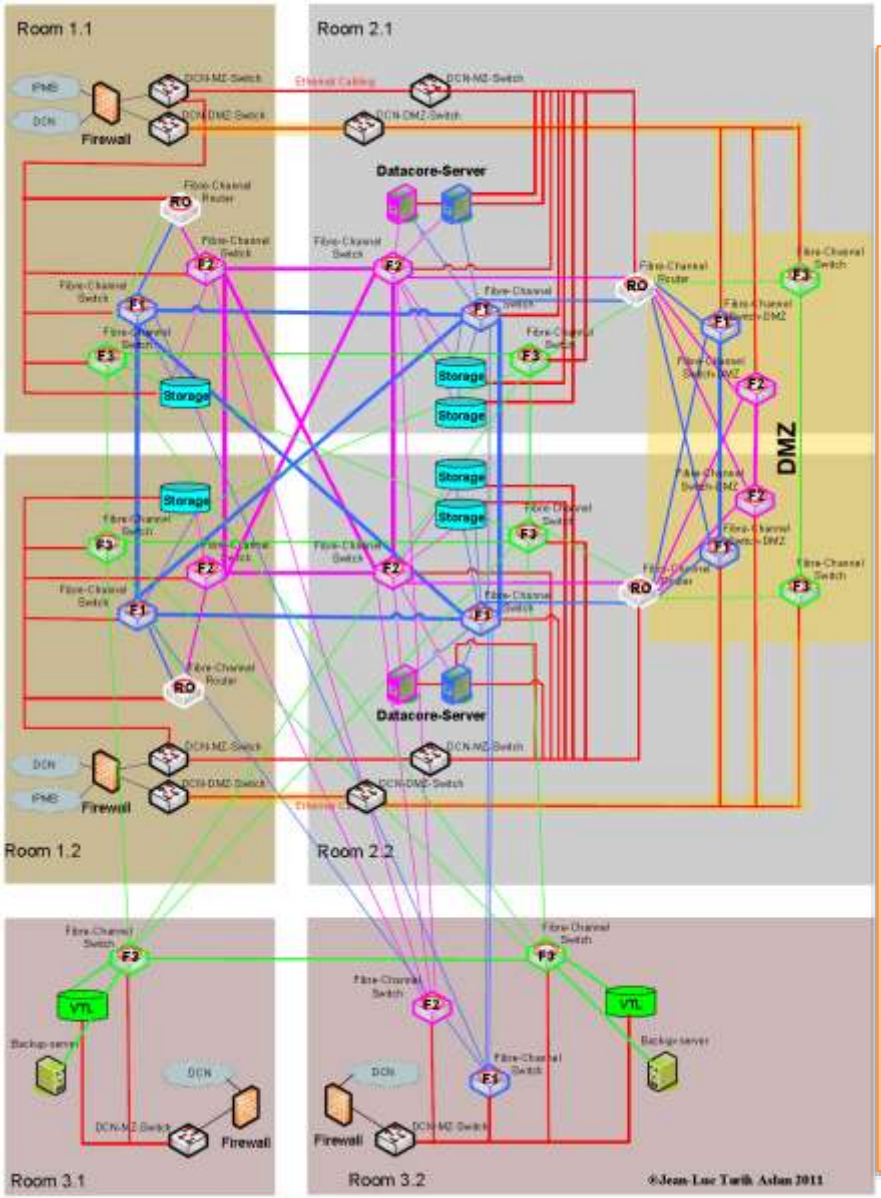
- about 1500 cu & FC Ports (OM4)
- Structured cabling costs(inkl. Trassen) ~750T€
- plan till GR14
- 1 room over 10 in SK4 Location
- Multi-fabric SAN inter-room coupled
- **1 Rack($$m²)~10kw~6 ESX server~40-60 cu ~24FC**

Who can pay for that?



Infrastructure Complexity Data Protection

San Infrastructure Complexity



Brocade DCX:

- up to 384 16Gbits ports
- Up to 512 8gbits ports

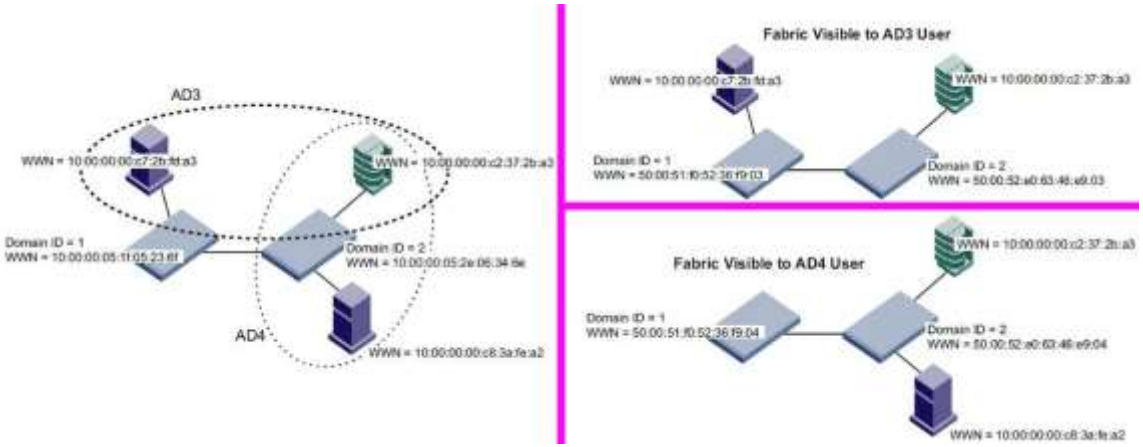
- DCX chassis can be coupled via ICL
- 4x ICLs deliver 256 Gbps (16 x 16 Gbps ISLs)
- ICL Trunking can accommodate up to 4 ICL Ports in a Trunk

By storage virtualization engine, you canthe data is everywhere, the data trafficIt's impossible to predict.

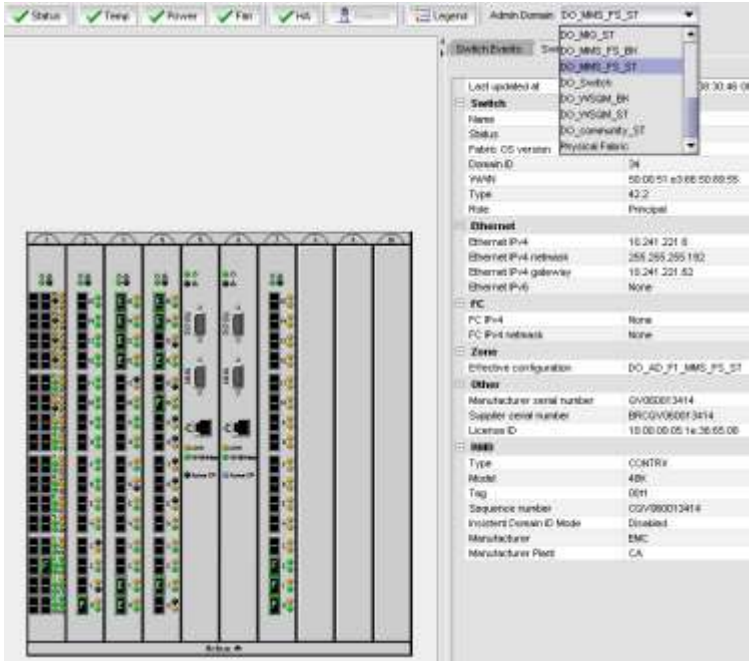
Normal traffic and backup traffic mustthe one that allows aoversubscription 1/7 der andere 1/1 (Streaming)

We forget here the location coupling via FCIP or DWDM dark-fiber

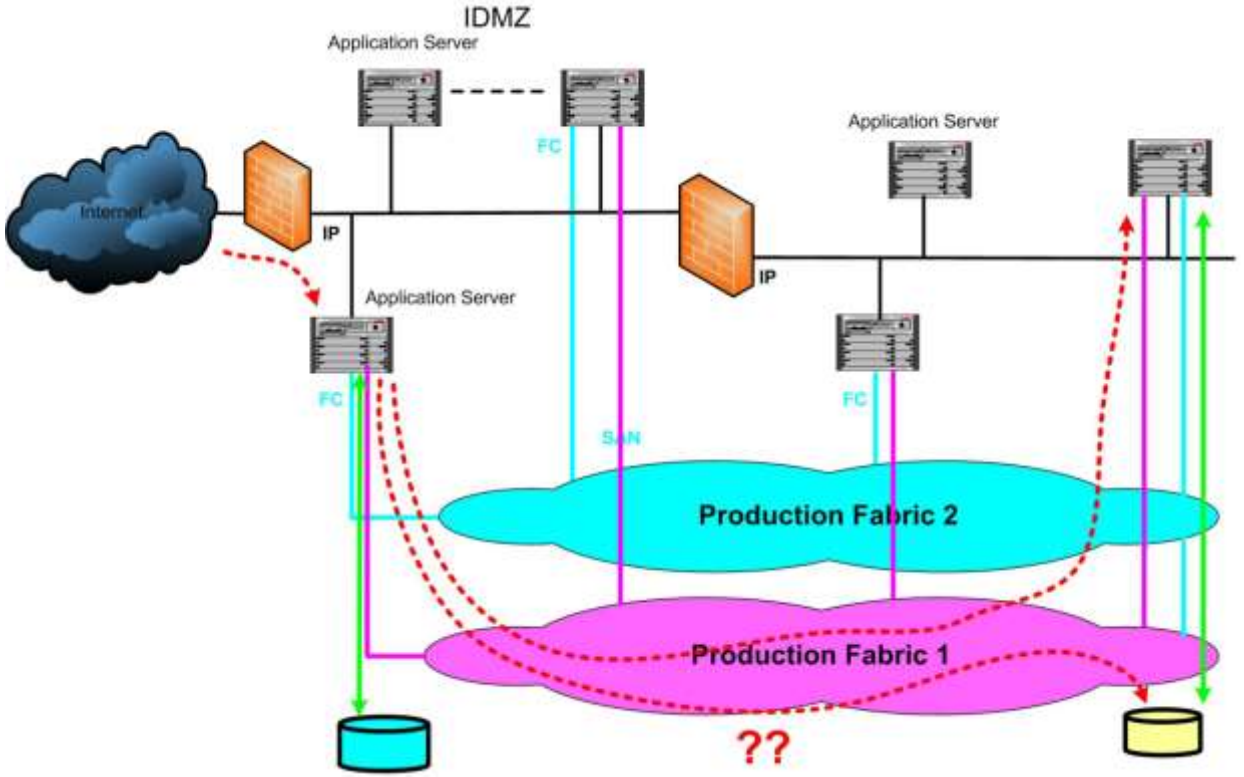
Admin Domain, Virtual Fabric, VSan



- 2000 san ports
  → über 4000 SAN zones
- AD Domain/VF/VS partitionnieren
  die menge
- VF & VS brauchen inter Fabric routing
- AD Domain share devices



SAN-DMZ Issue

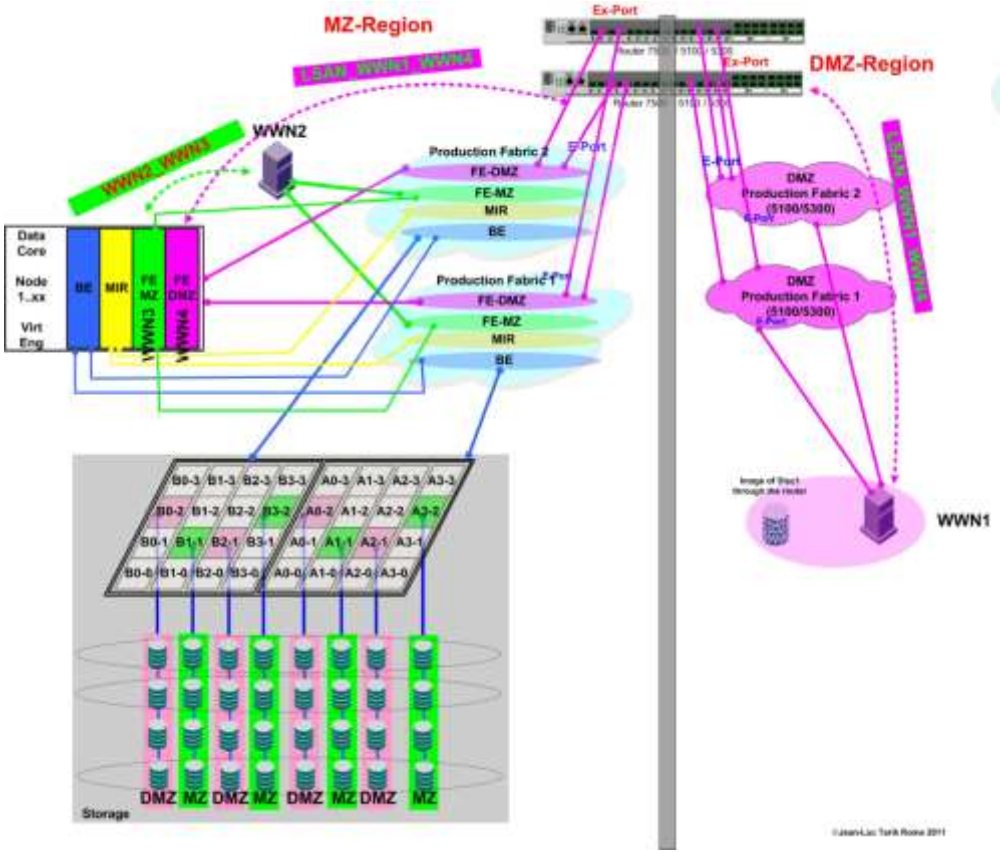


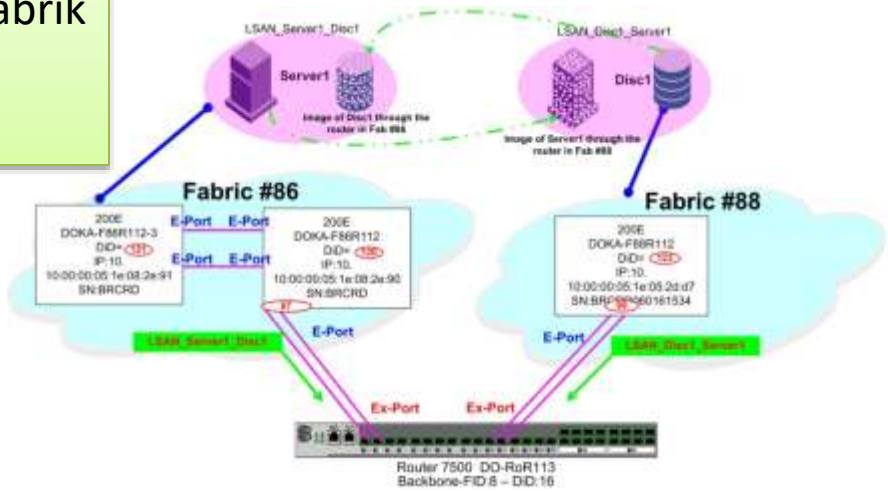
- Broadcast Attack
- WWN spoofing von MZ server
- RSCN attack auf storage
- Primitive attack auf fabrik dienst → Fabric not ready
- Chassis attack → Fabric not ready
- Bad zoning configuration erlaubt daten zugriff

Etc.. Etc…

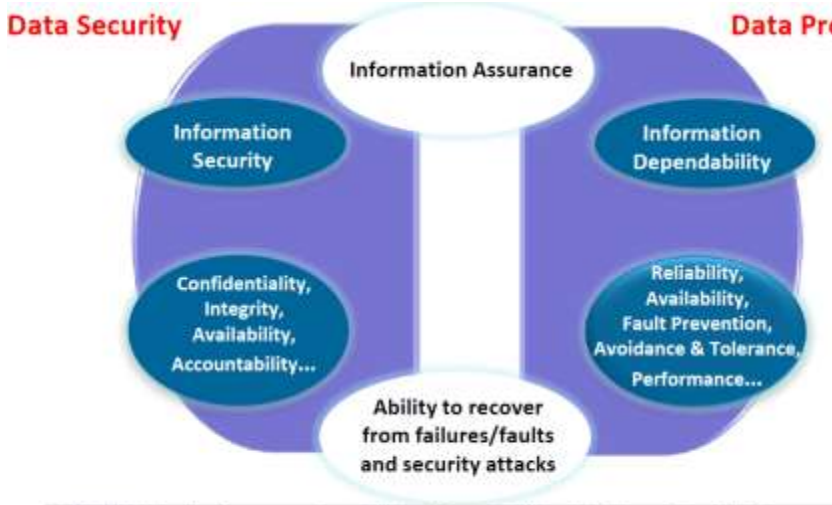
SAN-DMZ Solution

Doppel zoning Konfiguration nötigt MZ & DMZ
Port hardening
DMZ Fabrik Problem haben kein Wirkung auf MZ Fabrik
Durch sharing von WWN Port müssen dedizierter
Front-End Port für DMZ reserviert werden



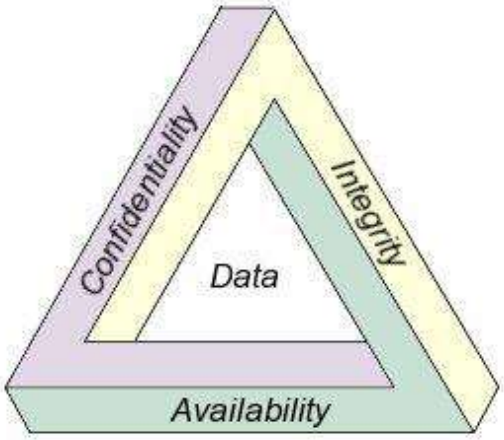


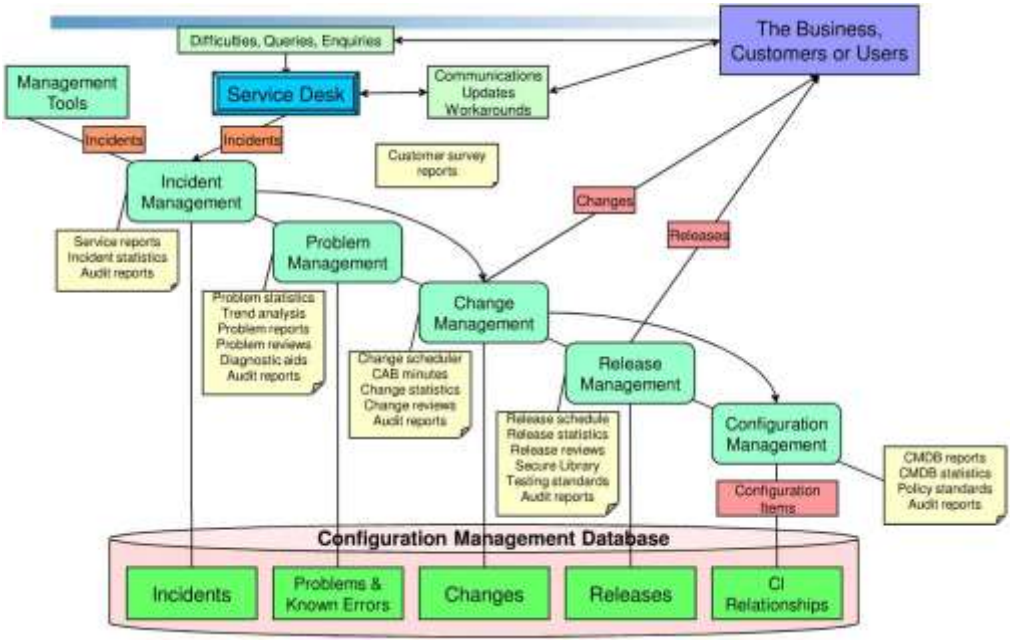
Daten Protection Thema



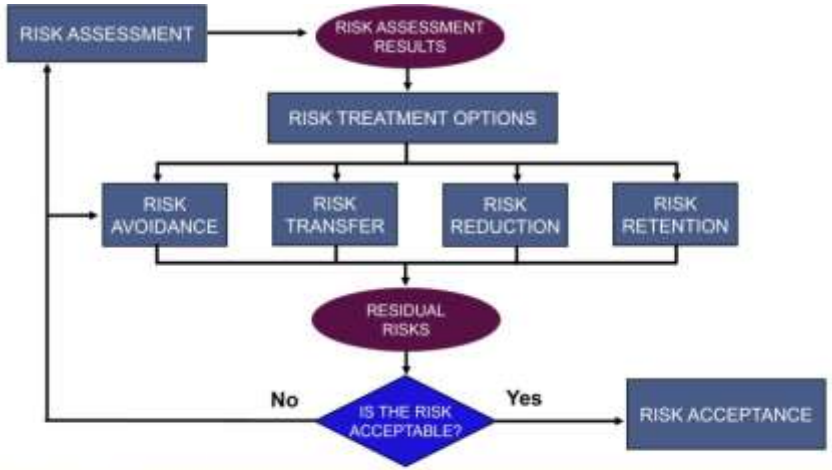
SOURCE: *Information Assurance – Dependability and Security in Networked Systems*, Qian, Joshi, Tipper, Krishnamurthy, 2008, New York, ISBN: 978-0-12-373566-9.

We make money with our data
We earn money by trusting customers
We earn money from service reliability
We make money with data security
Change /Incident/Problem Management are important large infrastructure





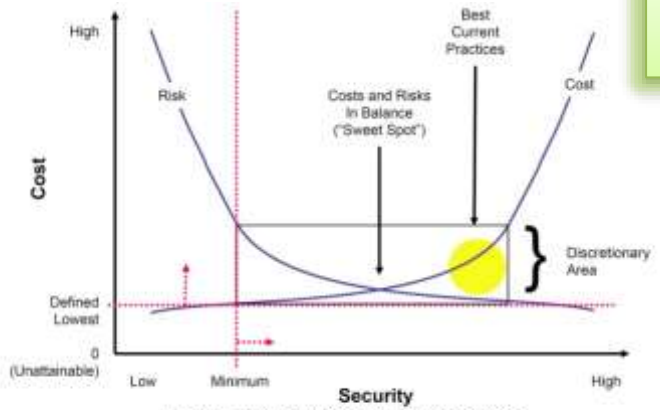
Rest Risiko Thema



BASED ON: ISO/IEC 27005:2008, *Information technology -- Security techniques – Information Security Risk Management*, http://www.iso.ch

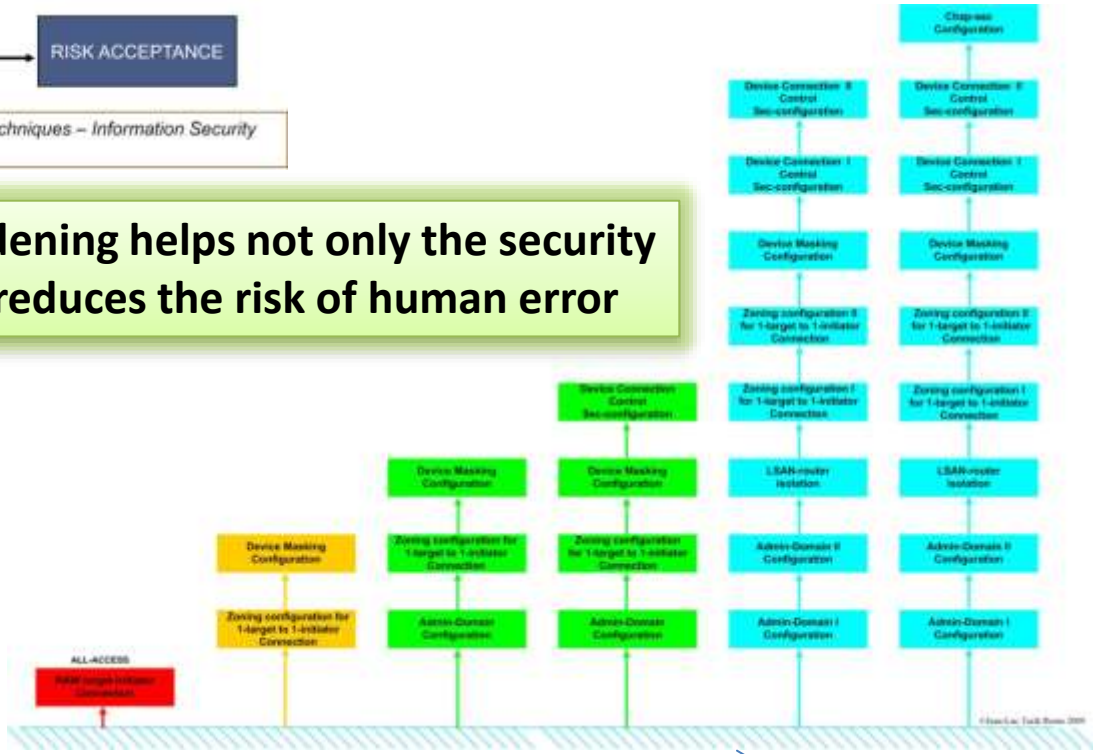
When is too little
When is too much
When is it priceless?
When is the risk tolerable
for the data class?

Hardening helps not only the security but reduces the risk of human error



© 1996 – 2000 Ray Kaplan All Rights Reserved

Source: Ray Kaplan, CISSP, *A Matter of Trust*, Information Security Management Handbook, 5th Edition. Tipton & Krause, editors.



We are among the best

DATALOSS db
open security foundation

login | signup CREDANT

About | Search | Submit New | Primary Sources | Laws | Reports | Stats | Analysis | Mail Lists | The Blotter | Fringe | Supporters

Main | Latest Incidents | Largest Incidents | Most Discussed Incidents | Recently Updated Incidents

HACK
ID: 1518: Malicious Software/Hack compromises unknown number of credit cards at fifth largest credit card processor
Date: 2009-01-20 Records Lost: 130,000,000 Source: Outside Submitted by: michaelcordes Location: Princeton NJ, US
Organizations: Heartland Payment Systems, Tower Federal Credit Union, Beverly National Bank

HACK
ID: 548: Hack exposes 94 million credit card numbers and transaction details
Date: 2007-01-17 Records Lost: 94,000,000 Source: Outside Submitted by: admin Location: US
Organizations: TJX Companies Inc.

HACK
ID: 2061: Hackers access credit-reporting database.
Date: 1984-06-01 Records Lost: 90,000,000 Source: Outside Submitted by: Dissent Location: US
Organizations: TRW, Sears Roebuck

HACK
ID: 3634: 77 million names, addresses, email addresses, birthdates, PlayStation Network/Qriocity passwords and logins, handle/PSN online ID, profile data, purchase history and possibly credit cards obtained.
Date: 2011-04-26 Records Lost: 77,000,000 Source: Outside Submitted by: jkouns Location: US
Organizations: Sony Corporation

HACK
ID: 110: Major card processor breached losing millions of credit card numbers
Date: 2005-06-19 Records Lost: 40,000,000 Source: Outside Submitted by: admin Location: Tucson AZ, US
Organizations: CardSystems, Visa, MasterCard, American Express

HACK
ID: 5285: 40 million forum members' usernames and clear-text passwords leaked online by hackers
Date: 2011-12-26 Records Lost: 40,000,000 Source: Outside Submitted by: Dissent Location: CN
Organizations: Tianya

HACK
ID: 4521: Personal information of 35 million users including names, email addresses, phone numbers and encrypted resident registration numbers and passwords accessed by hacker
Date: 2011-07-26 Records Lost: 35,000,000 Source: Outside Submitted by: Dissent Location: KR
Organizations: SK Communications, Nate, Cyworld

HACK
ID: 4942: Database containing user names, hashed and salted passwords, game purchases, email addresses, billing addresses and encrypted credit card information accessed by hacker(s).
Date: 2011-11-10 Records Lost: 35,000,000 Source: Outside Submitted by: Dissent Location: Washington DC, US
Organizations: Steam (Valve, Inc.)

HACK
ID: 3755: Hackers breached database and accessed username and password information on more than 30 million individuals
Date: 2009-12-14 Records Lost: 32,000,000 Source: Outside Submitted by: jkouns Location: Redwood City CA, US
Organizations: RockYou Inc.

STOLEN COMPUTER
ID: 289: Names, Social Security numbers, and dates of birth of 26.5 million U.S. military veterans stolen
Date: 2006-05-22 Records Lost: 26,500,000 Source: Outside Submitted by: admin Location: US
Organizations: U.S. Department of Veterans Affairs

LOST MEDIA
ID: 841: Two missing CDs contained over 25 million names, addresses, dates of birth and National Insurance numbers of the entire HMRC child benefit database as well as 7 million banking details
Date: 2007-11-20 Records Lost: 25,000,000 Source: Outside Submitted by: admin Location: GB
Organizations: HM Revenue and Customs, TNT

HACK
ID: 3661: 24.6 million customer dates of birth, email addresses and phone numbers, including 12,700 non-U.S. credit or debit card numbers and expiration dates and about 10,700 direct debit records including bank account numbers accessed by hacker
Date: 2011-05-02 Records Lost: 24,600,000 Source: Outside Submitted by: Dissent Location: US
Organizations: Sony Online Entertainment, Sony Corporation

HACK
ID: 5489: 24 million email addresses, billing and shipping addresses, phone numbers, the last four digits from credit cards, passwords and more illegally accessed
Date: 2012-01-15 Records Lost: 24,000,000 Source: Outside Submitted by: arex1337 Location: Henderson NV, US
Organizations: Zappos

HACK
ID: 5282: Data for 20,000,000 game site users reportedly leaked by hackers
Date: 2011-12-22 Records Lost: 20,000,000 Source: Outside Submitted by: Dissent Location: ??? ???, CN
Organizations: 7k7k

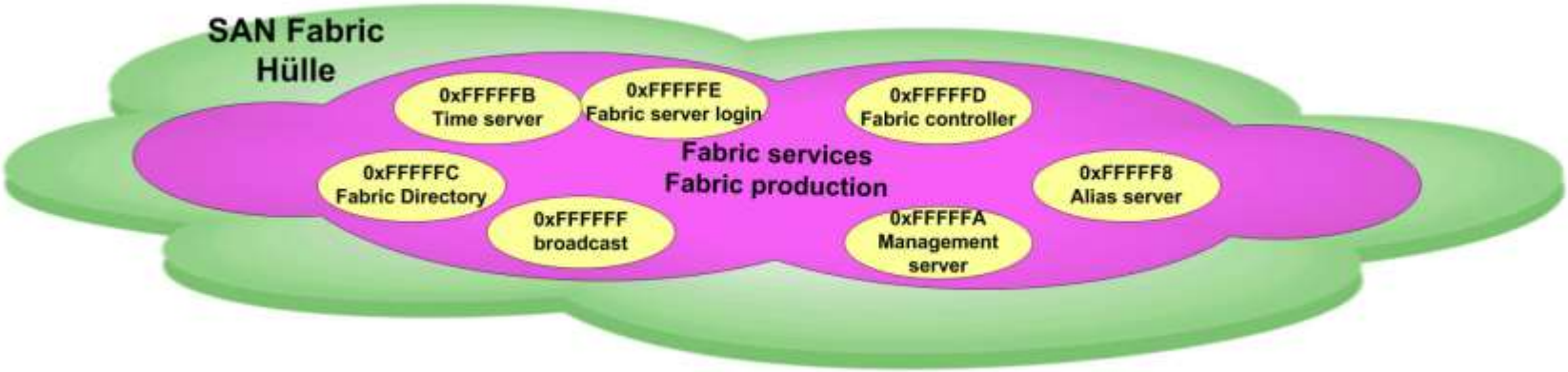
HACK
ID: 5306: 17,900,617 members notified of forced password reset after hacker accesses "limited number" of users' logins
Date: 2011-12-28 Records Lost: 17,900,617 Source: Outside Submitted by: Dissent Location: Redwood City CA, US
Organizations: Care2

LOST DISK DRIVE
ID: 1172: T-Mobile lost disk containing data on 17 million customers
Organizations: T-Mobile, Deutsche Telekom

Share Services Fabrik

FCIA, SNIA, IEEE define protocol.
In SAN, all distributed services with well-known addresses are directly accessible.
This also means that these services are also very easy to attack.
Often these services are completely open, such as management servers,
name server (simple name server).

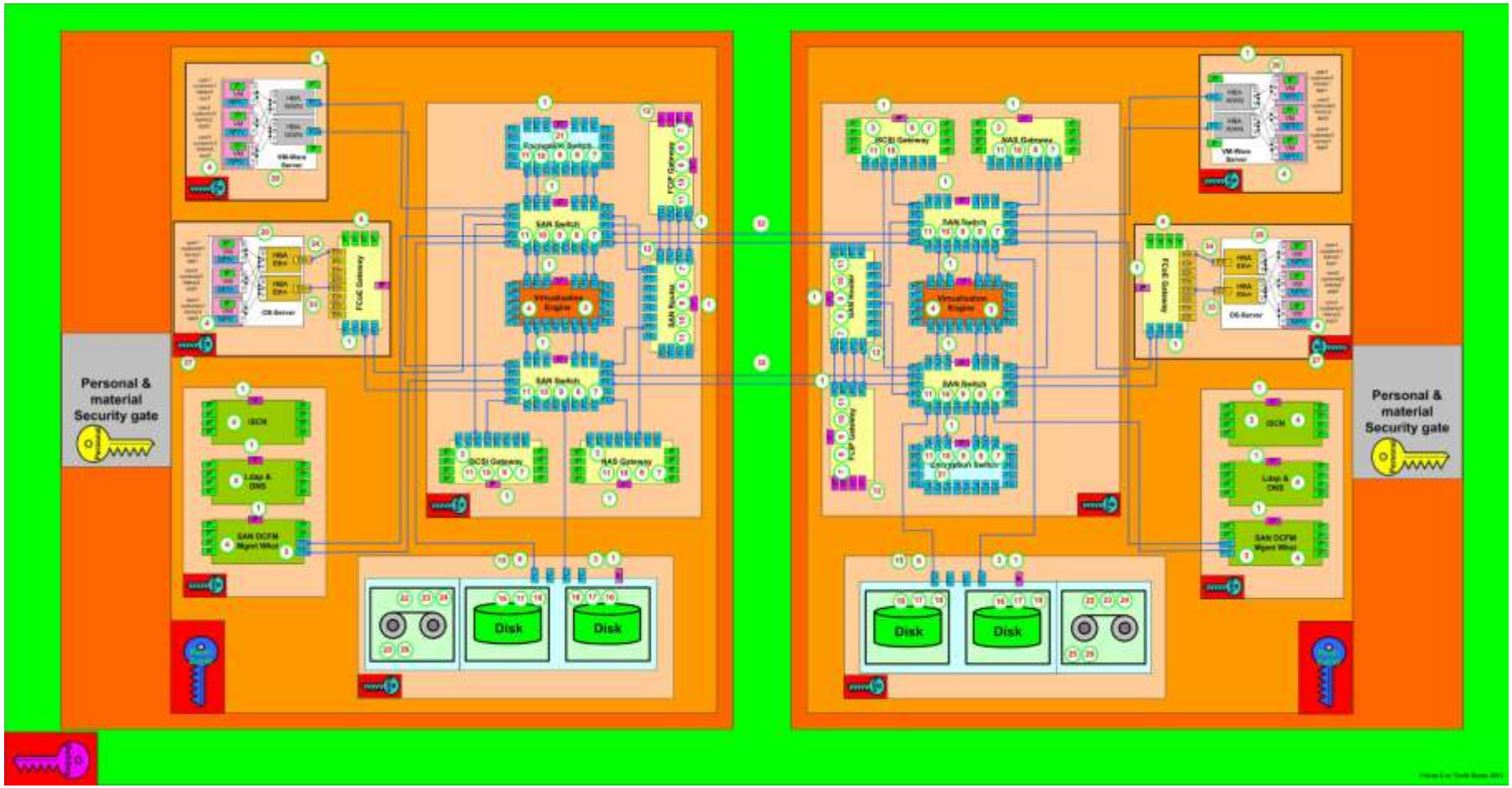
FCIA, SNIA , IEEE never define how to implement a protocol,Suppliers are free to implement what they want as they want.



Z Example: PID of the port are fixed with Brocade.
At Cisco, they are assigned by the switch

Logical Data Storage Network

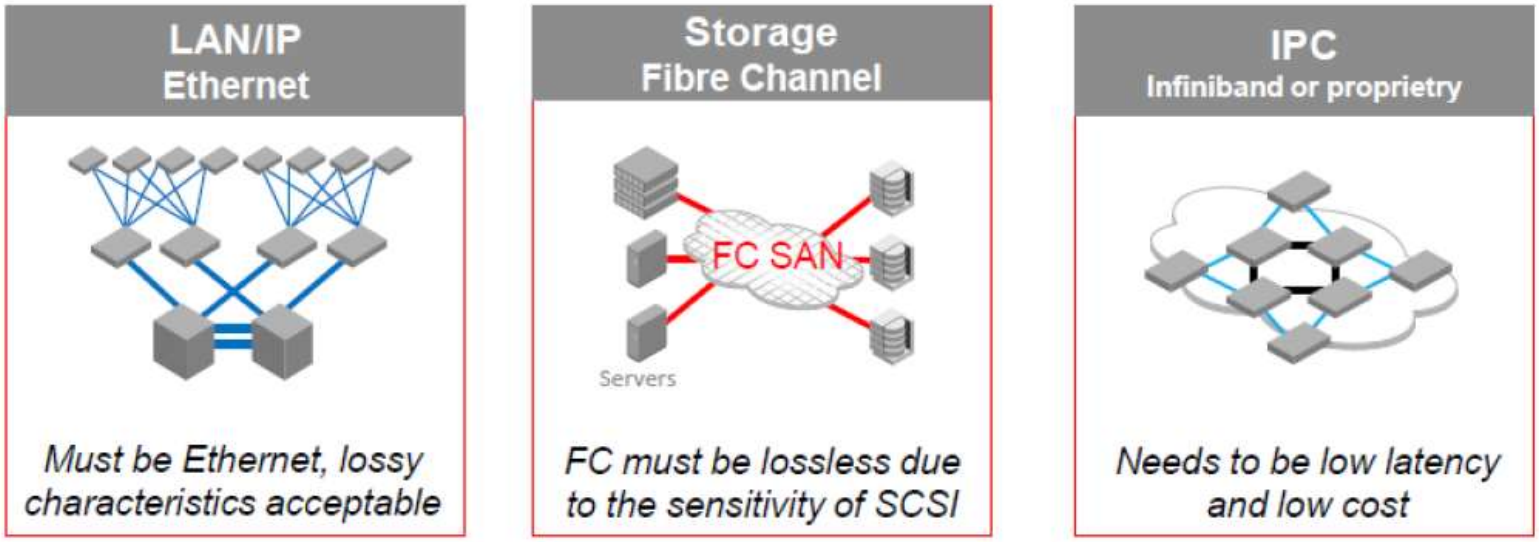
Now IP ports are separated from FC ports, but later with Datacenter Ethernet??



Data Center Ethernet/Fabric

Goal

- Capex reduction (infrastructure costs)
- Same availability/reliability as FC
- Joint transport infrastructure for all protocols



Datacenter Ethernet

IEEE

802.1Qbb Priority Flow Control (PFC)

802.1Qaz Enhanced Transmission Selection (ETS)

DCBX Data Center Bridging Exchange protocol proposal for 802.1Qaz

802.1Qau congestion notification

T11 ANSI

FCoE

SPMA FPMA address discovery

IETF

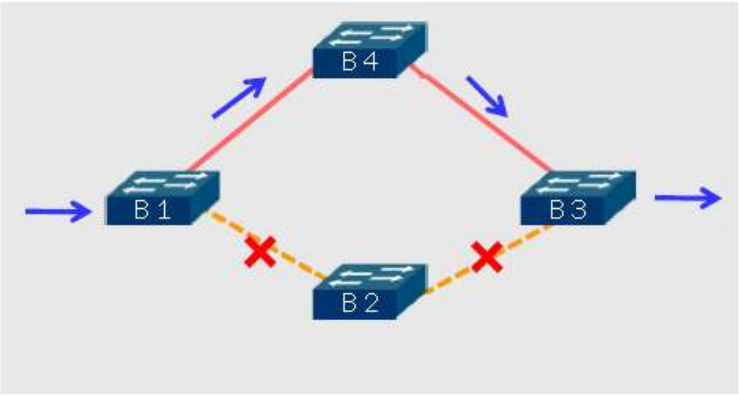
TRILL - Transparent Interconnection of Lots of Links

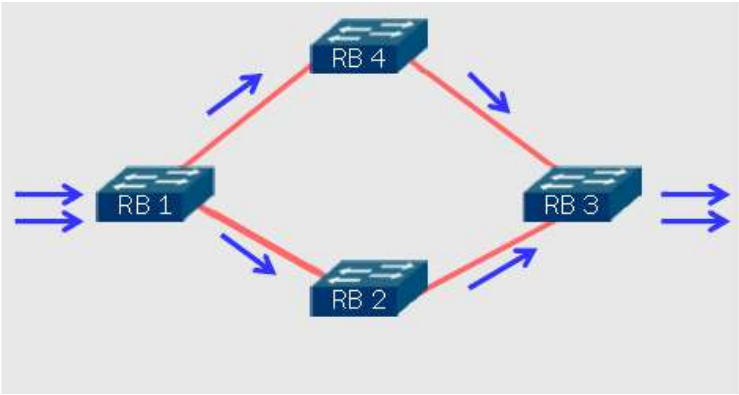
Implementation Agreement | Approved | In Development

TRILL (Transparent Interconnection of lots of links (Layer 2)

- Is the successor of spanning-tree protocol
- Tension tree protocol:
- No multipath support
- Inefficient use of the path
- Complex debugging (no deterministic failure mode)
- Slow re-convergence after failover – partitioningIdle
- ifraTRILL :
  - Enables L2 multiple paths via load splitting among paths
  - Reclaims network bandwidth and improves utilization
  - Improves efficiency with L2 shortest path and ECMP
  - Faster response to failures
  - TRILL is backward-compatible with existing infrastructures
  - Delivers multiple hop FCoE with Routing Bridges and link state routing protocols

Rbridge (switch mit Trill)

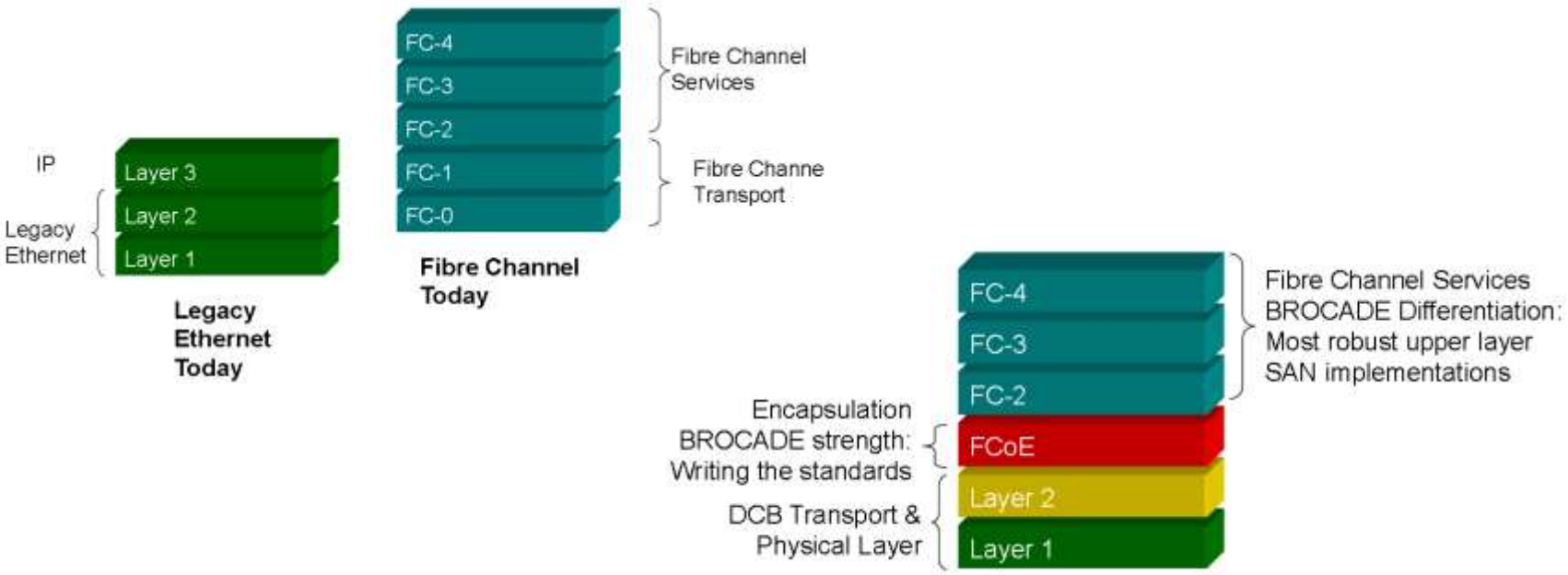




- Classische Switch benutzen Spanning-tree Protokoll
- Spanning-tree protocol verhindert loop durch abschalten von links

- Rbridge Switch benutzen Trill routing Protokoll
- Rbridge support multipathing der links

FCoE



FCF: Fibre Channel Forwarder

FCoE_LEP:

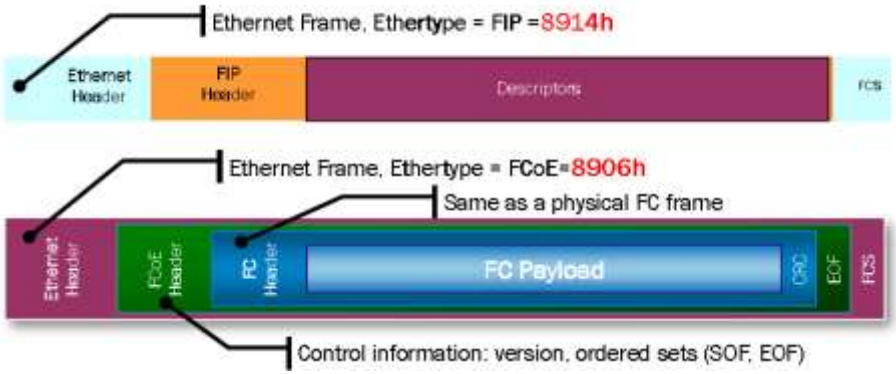
- terminate FCoE Link
- deals with de-&entcapsulation of FC Frame

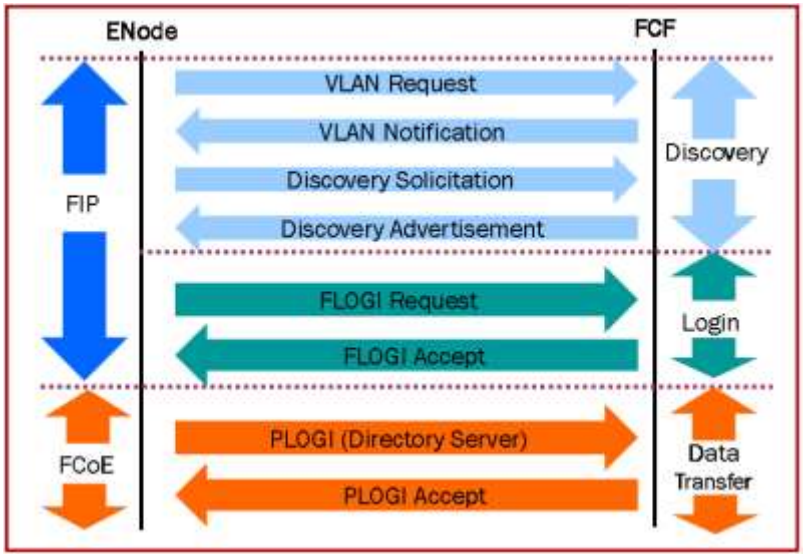
FcoE Controller: exists in VE-Node (VF/VN) and in FCFs

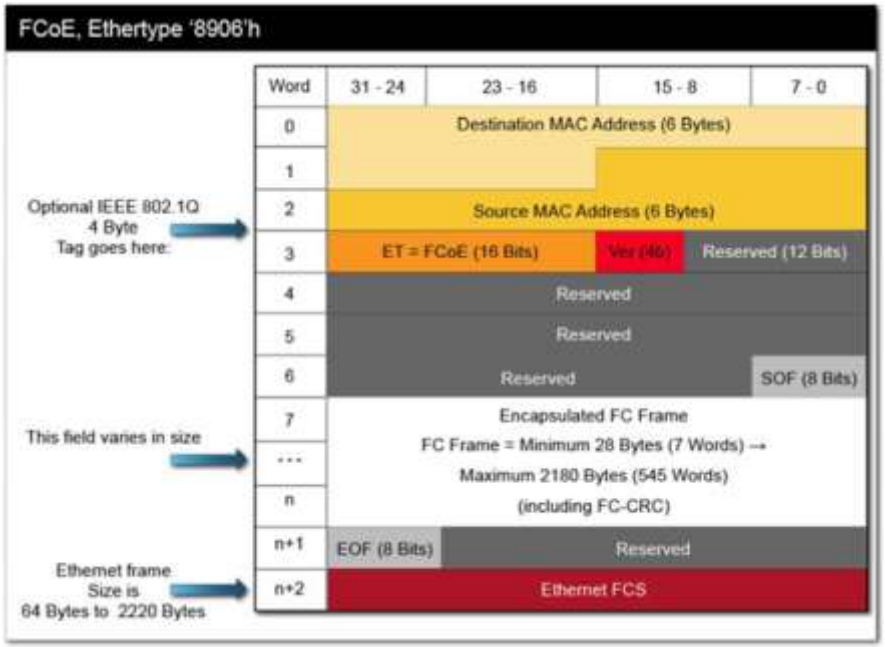
Participate in discovery

Are responsible for creation/delation/monitoring of virtual link

FIP – FCoE Frames

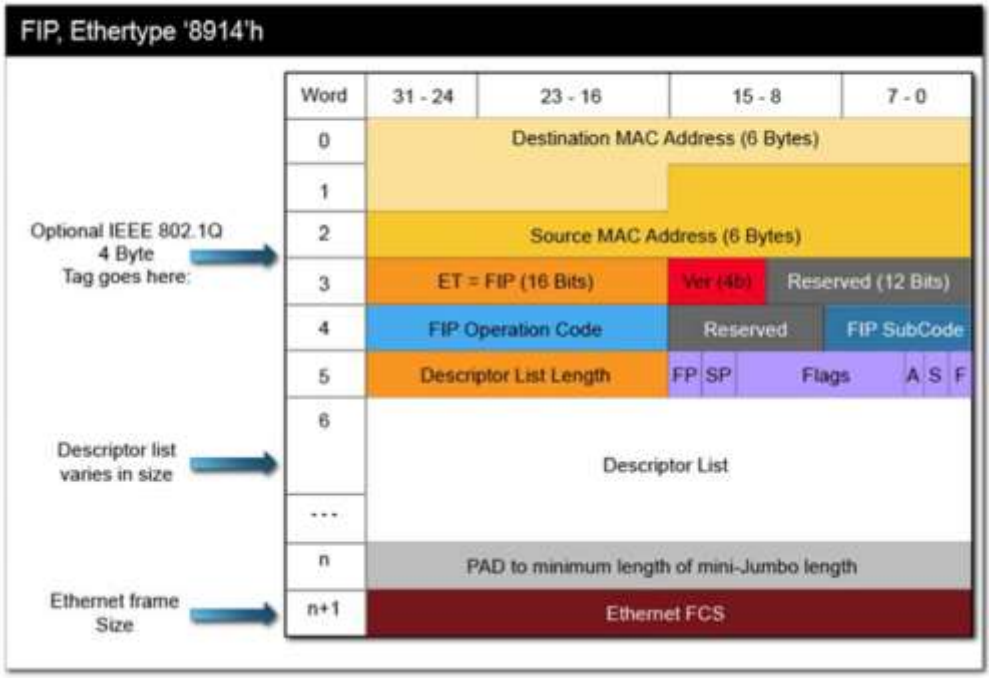






FIP (FCoE initialistaion Protocol)

FIP, Ethertype '8914'h



FIP Operation Codes

Operation Code	Subcode	Operation
0001h	01h	Discovery, Solicitation
	02h	Discovery, Advertisement
0002h	01h	Virtual Link Instantiation Request
	02h	Virtual Link Instantiation Response
0003h	01h	FIP Keep Alive
	02h	FIP Clear Virtual Link
FFF8h .. FFFEh	00h .. FFh	Vendor Specific
All others	All others	Reserved

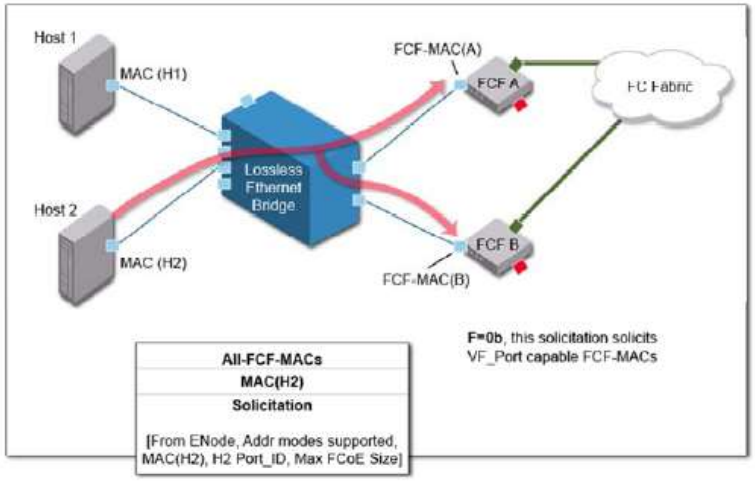
FIP operation descriptor

Range	Type	FIP Descriptor	Reference
Critical	0	Reserved	
	1	Priority	7.7.5.3.2
	2	MAC address	7.7.5.3.3
	3	FC-MAP	7.7.5.3.4
	4	Name_Identifier	7.7.5.3.5
	5	Fabric	7.7.5.3.6
	6	Max FCoE Size	7.7.5.3.7
	7	FLOGI[a]	7.7.5.3.8
	8	FDISC_NPIV[a]	7.7.5.3.9
	9	LOGO[a]	7.7.5.3.10
	10	ELP[a]	7.7.5.3.11
	11	VN_Port Identification	7.7.5.3.12
	12	FKA_ADV_Period	7.7.5.3.13
	13	Vendor_ID	7.7.5.3.14
	14-127	Reserved	
Non-critical	128-240	Reserved	
	241-254	Vendor Specific	7.7.5.3.15
	255	Reserved	

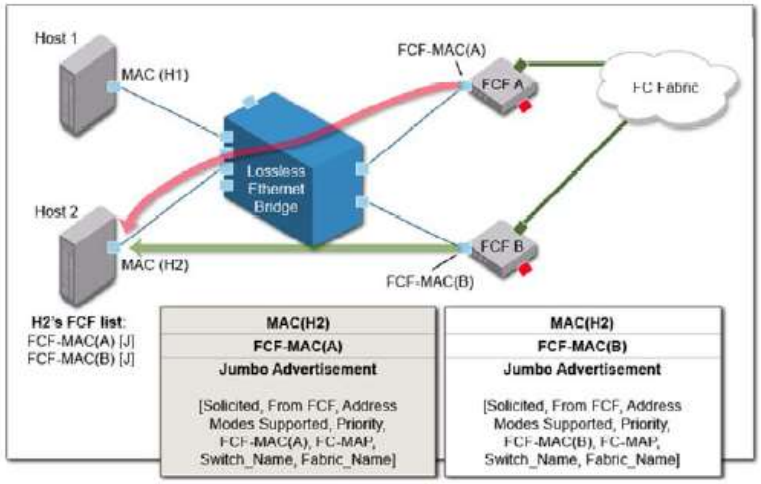
a The FC CRC, SOF, and EOF shall not be included in the FIP descriptor.

FIP (FCoE initialistaion Protocol)

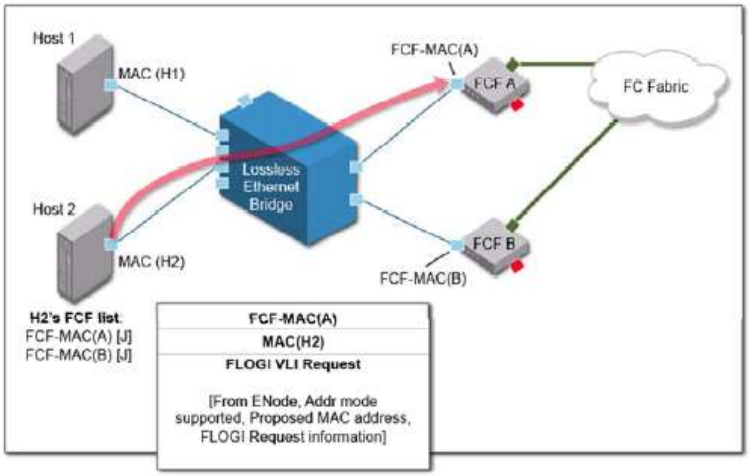
Multicast Solicitation from Host 2



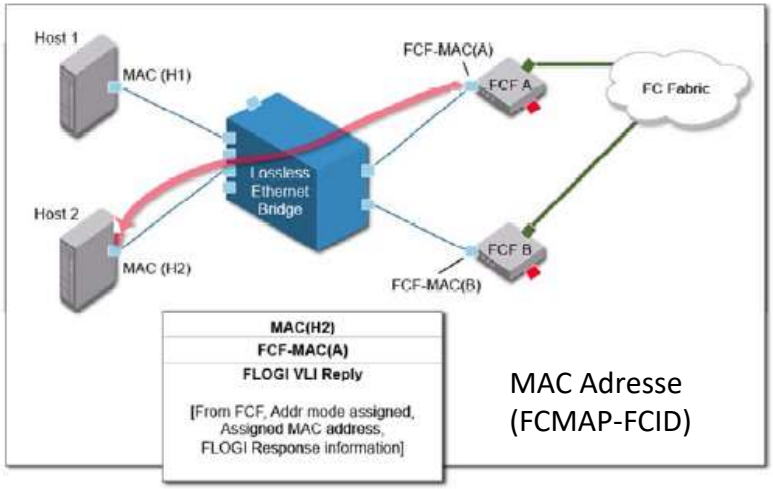
Unicast Advertisements from FCFs



Host 2 FLOGIs to FCF_A



FCF FLOGI Response to Host 2



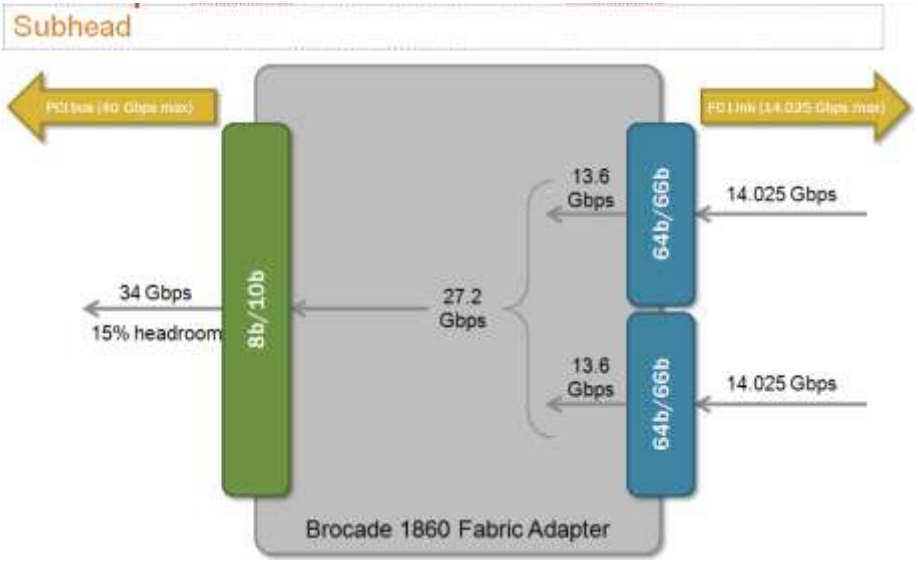
MAC Adresse
(FCMAP-FCID)

VDX Switch – VCS

- VDX switch are Datacenter Ethernet Switch
- VDX Switch working with VLAN
- VCS (virtual cluster switching) is a layer 2 Ethernet technology
- Edge port support industry standard Link Aggregation Groups (LAGs) with the LAPC protocol (IEEE 802.1ad)
- ISL do not use LAGs but special trunk protocol (upto 8 links)under VCS mode,
- the switch discovers its neighbor and mergesVLAN 40934095are reserved for VCS control traffic

Product Comparison	Brocade VDX 6720	Juniper EX4500	Cisco NX5020
Street price per port	$670	$1800 1st 40, then $1K	$670
Power per port	Max 6W	Max 12W	Max 14.5W
Latency	0.6–1.8 us	4.7 us	3.2–2.3 us
10 GbE ports	60	48	52
Throughput	1200 Gbps	960 Gbps	1040 Gbps
DCB/TRILL	Yes/Yes	No/No	Yes/Yes
Layer 3	Mid-2011	Yes	No

Interface HBA any I/O



Extends Ethernet and Fibre Channel fabric services

- •Brocade Server Application Optimization (SAO): QoS, N_Port Trunking
- •Brocade vFLink I/O virtualization, SR-IOV, VEB/VEPA

Brocade AnyIO Technology

- •16/8/4/2 Gbps Fibre Channel, 10 GbE Data Center Bridging (DCB), TCP/IP, FCoE, and/or iSCSI
- •Configurable on a per-port basis
- •All protocols supported concurrently, no licensing required

Summary

- We have looked at the problem of FC and already know where there was problem.
- We know that suppliers have high levels of implementation freedom
- We know that some parts of the Minutes have not yet been adopted.
- More detailed analysis of the protocol is needed

Issue

- Is datacenter Ethernet/Fabric operational?
- Does datacenter guarantee Ethernet/Fabric Data Protection?
- How are the protocols vulnerable?
- Allows to change routing information
- How to guarantee the separation of transport type……

How to proceed……