

ZyXEL Ethernet Switch

Security Switching in Layer 2+ und Layer 3+

Ulrich Eska

ZyXEL Deutschland GmbH

Oranienburg, 11. Oktober 2006



ZyXEL im Überblick

Gegründet: August 1989 von Dr. Shun-I Chu

Mitarbeiter: 2100 Angestellte weltweit (Dez. 2005)

Firmensitz: Hsinchu Science Park, Taiwan

ZyXEL Produktbereiche

Telco/ISP



- >> Multi-Service IP DSLAM
- >> VDSL Switch
- >> Edge Switch
- >> ADSL/G.SHDSL/VDSL CPE
- >> VoIP CPE
- >> Video/Multimedia CPE
- >> Multimedia Auto Provisioning Solution
- >> Central Mgmt Software

Businesses



- >> L2/L3 Switch
- >> Network Security Appliance
- >> Security Alert Platform
- >> Business WLAN Solution
- >> Hot Spot WLAN Solution
- >> Central Mgmt Software/Appliance
- >> Product & Service platform

Homes



- >> Broadband Router
- >> WLAN AP/Clients
- >> Desktop Switch
- >> VoIP Device

Agenda



Layer 2 Switching

- Standard
- VLAN

Layer 2+ Switching

- Security
- Port Mirroring
- Link Aggregation
- IGMP Multicast

Layer 3+ Switching

- Redundanz mit OSPF und VRRP

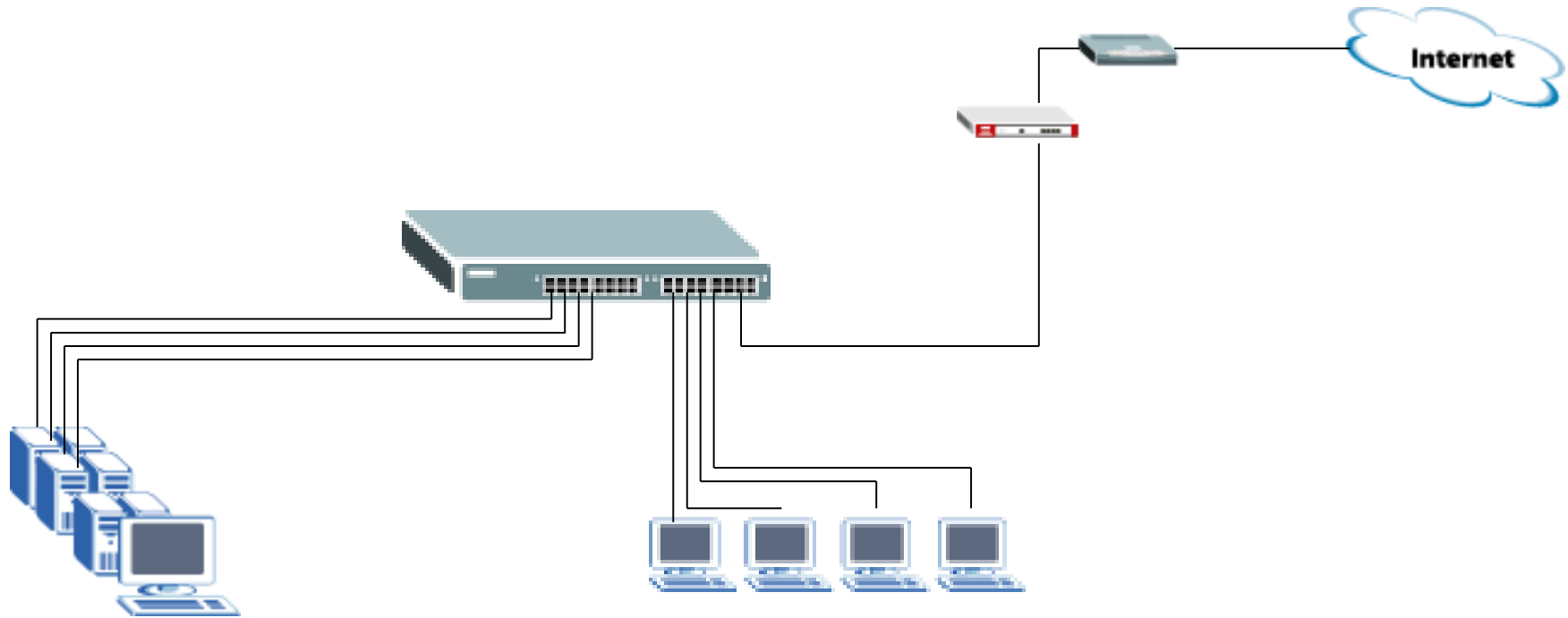
Layer 2 Switching

Security im L2 Ethernet Switch

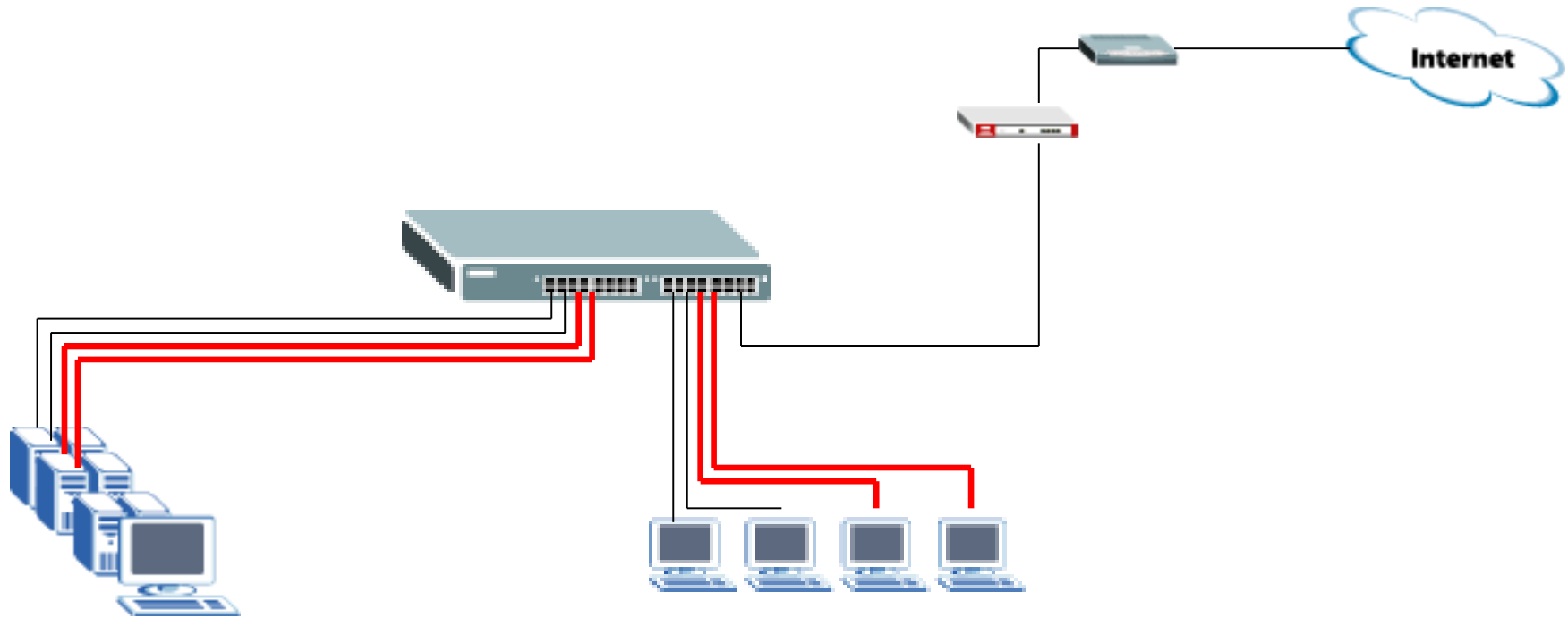
Wozu benötigen wir dies?

Abgrenzung verschiedener Abteilungen durch VLAN

Layer 2 Switching



Layer 2 Switching VLAN



Layer 2 Switching **VLAN**

ZyXEL Status Logout Help

MENU
 Basic Setting
 Advanced Application
 Routing Protocol
 Management

VLAN Status
 The Number Of VLAN = 3

[VLAN Port Setting](#) [Static VLAN](#)

Index	VID	Port Number																Elapsed Time	Status
		2	4	6	8	10	12	14	16	18	20	22	24	26	28				
1	1	U	U	U	U	U	U	U	U	U	U	U	U	U	U	0:02:21	Static		
		U	U	U	U	U	U	U	U	U	U	U	U	U	U				
2	10	-	-	-	-	-	-	-	-	-	-	-	-	-	-	0:02:21	Static		
		U	U	-	-	-	-	-	-	-	-	-	-	-	-				
3	20	U	-	-	-	-	-	-	-	-	-	-	-	-	-	0:02:21	Static		
		-	U	-	-	-	-	-	-	-	-	-	-	-	-				

Poll Interval(s)

Change Pages

© Copyright 1995-2004 by ZyXEL Communications Corp.

Layer 2+ Switching

Erweiterte Security im L2+ Ethernet Switch

- static MAC Forwarding; So wird mein Server für den Angreifer unerreikbaar
- limited Number of learned MAC; Grenzen Sie die Useranzahl auf dem Switch ein
- Port Security; Legen Sie fest, wer Daten an den Switch senden darf
- dedizierte MAC Adressen; Grenzen Sie den Nutzer genau ein
- 802.1x; Bleiben Sie flexibel durch den Radius Login
- Port Mirroring; Wodurch wird der Traffic verursacht?

Static MAC Forwarding

MAC	VID	Port
00:a0:c5:00:00:01	10	1

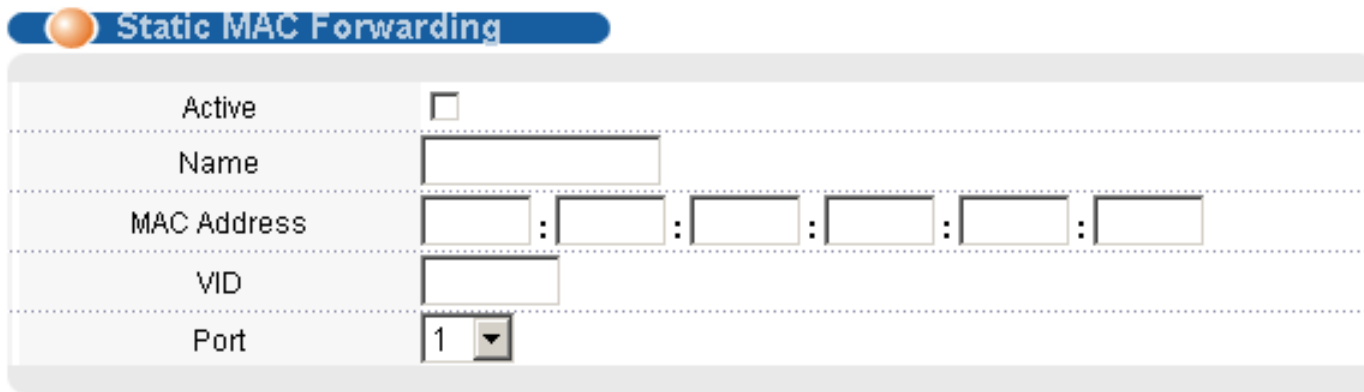
Wird weitergeleitet zu Port 1



Dest. 00:a0:c5:00:00:01 VID:10

00:a0:c5:00:00:01

Static MAC Forwarding

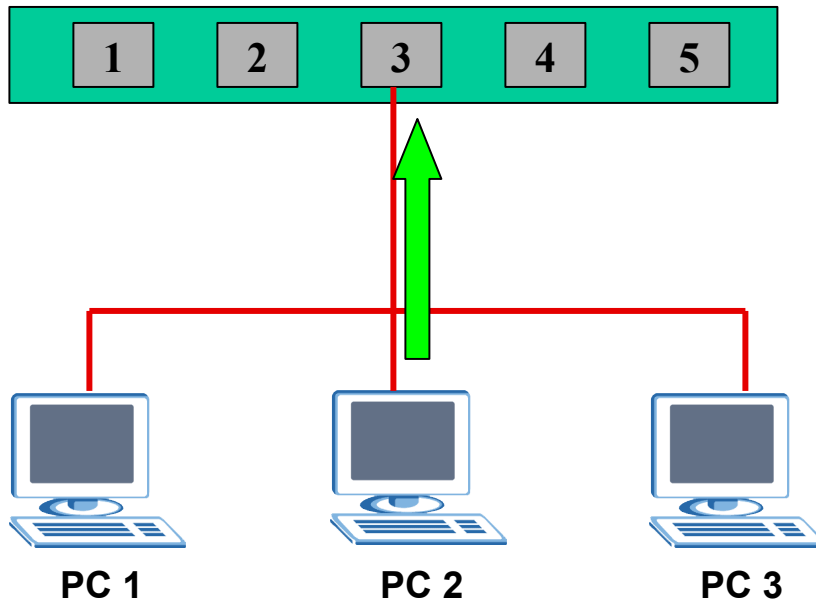
A configuration form for Static MAC Forwarding. It features a title bar with an orange sphere icon and the text 'Static MAC Forwarding'. Below the title bar is a table with five rows: 'Active' with a checkbox, 'Name' with a text input field, 'MAC Address' with six text input fields separated by colons, 'VID' with a text input field, and 'Port' with a dropdown menu showing '1'.

Active	<input type="checkbox"/>
Name	<input type="text"/>
MAC Address	<input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/> : <input type="text"/>
VID	<input type="text"/>
Port	1 <input type="button" value="v"/>

Limit Number of Learned MAC

MAC	VID	Port
00:a0:c5:00:00:01	10	3
00:a0:c5:00:00:03	10	3

Limit MAC Number = 2

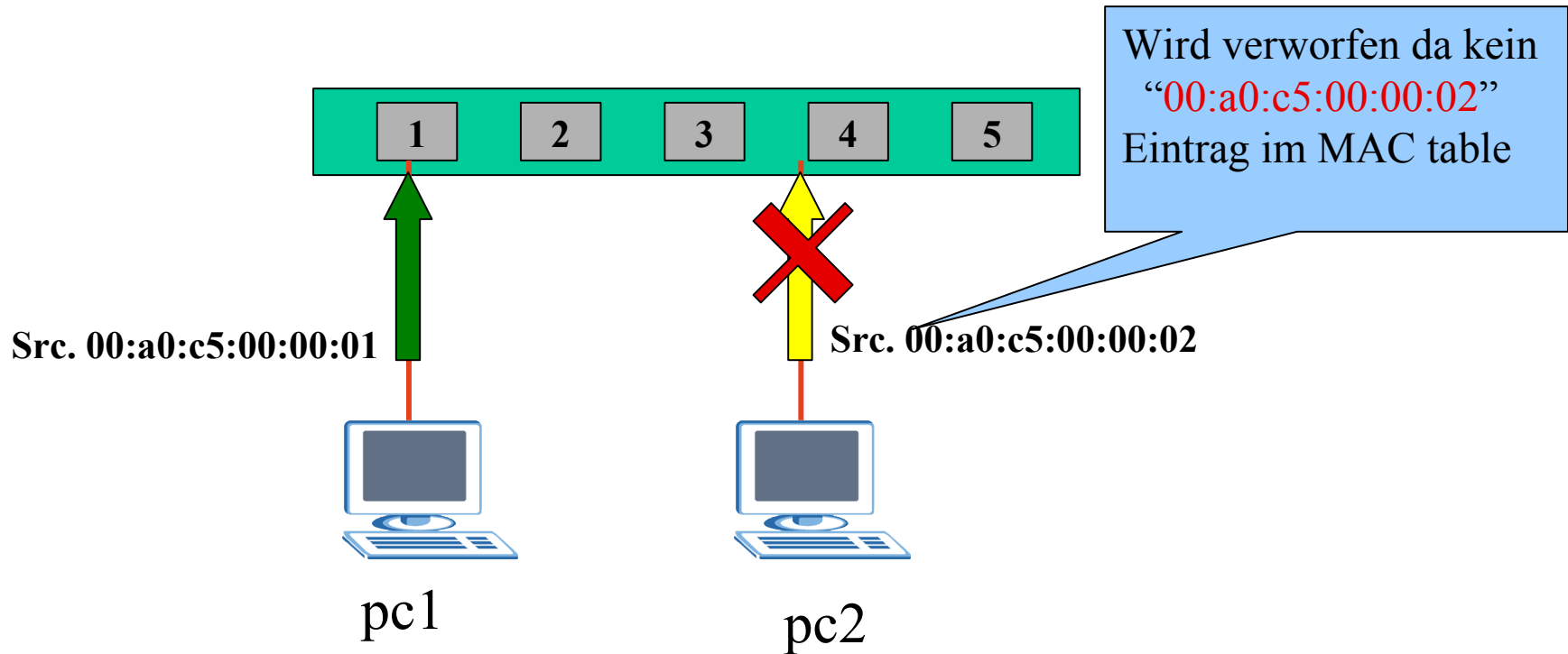


00:a0:c5:00:00:01 00:a0:c5:00:00:02 00:a0:c5:00:00:03

- Die MAC Adresse des PC1 und PC3 wurde durch den Switch erlernt
- Die MAC Adresse kann nicht vom Switch erlernt werden
- Der Traffic von PC 2 kann weiterhin zu allen Ports geleitet werden

Port Security

MAC	VID	Port
00:a0:c5:00:00:01	10	1



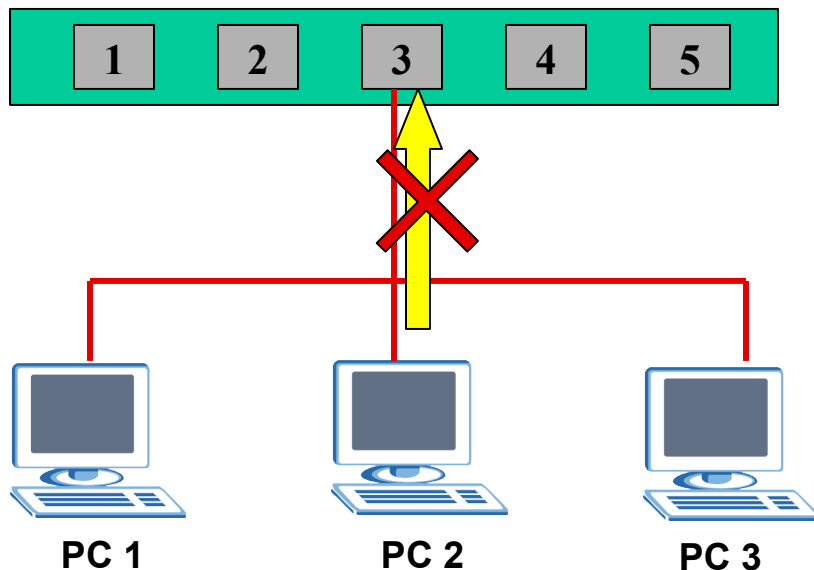
Port Security

Port Security

Port	Active	Address Learning	Limited Number of Learned MAC Address
1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="0"/>

Port Security mit Static MAC

MAC	VID	Port
00:a0:c5:00:00:01	10	3
00:a0:c5:00:00:03	10	3

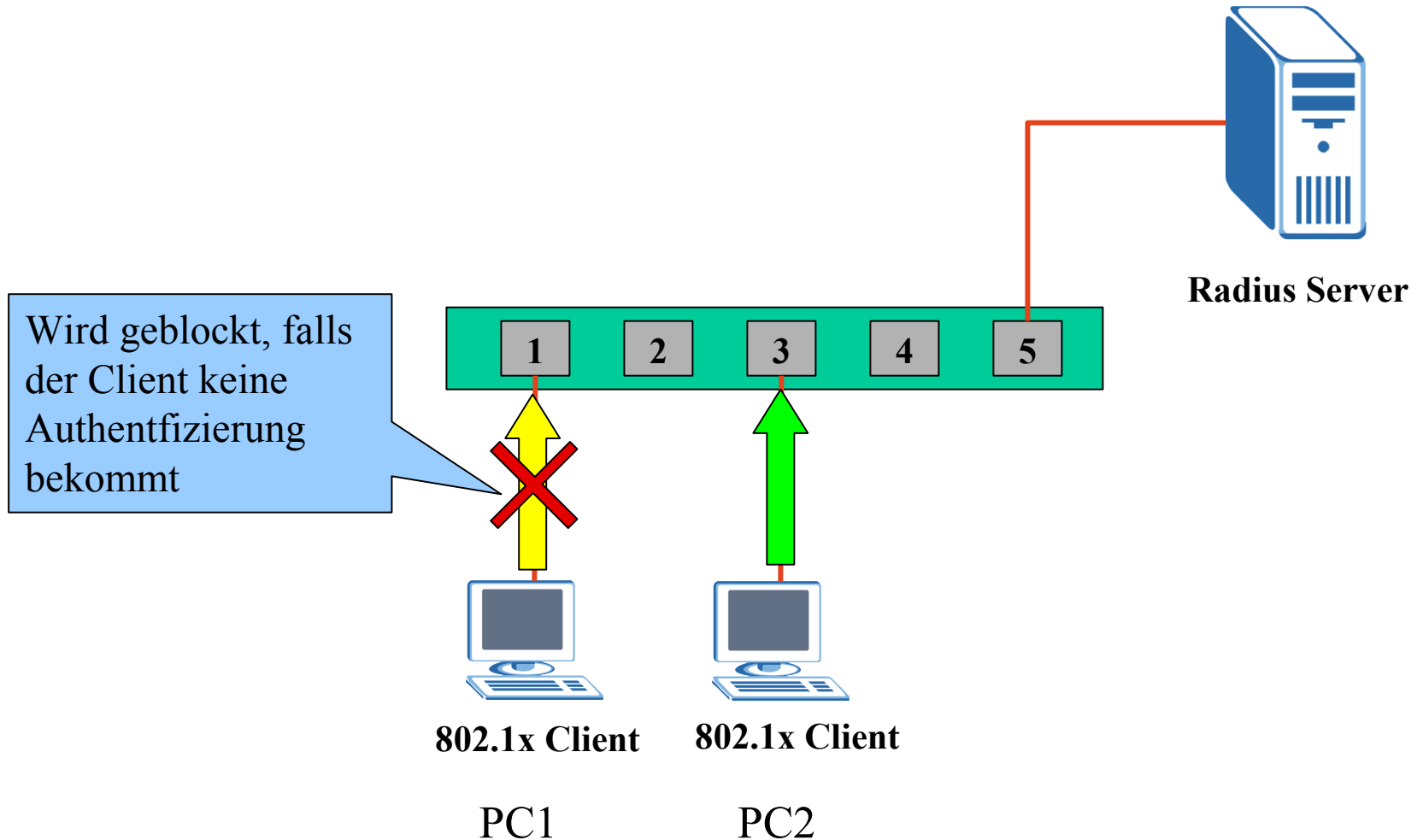


Port Security = Enable
Address Learning = **disable**

- Die MAC Adresse des PC 1 und PC 3 sind durch den Admin erfasst.
- Die Adress-Learning Funktion des Port 3 ist ausgeschaltet, dadurch kann die MAC Adresse des PC2 nicht erlernt werden.
- Der Traffic von PC2 wird geblockt, da der PC nicht in der MAC Tabelle erfasst wurde

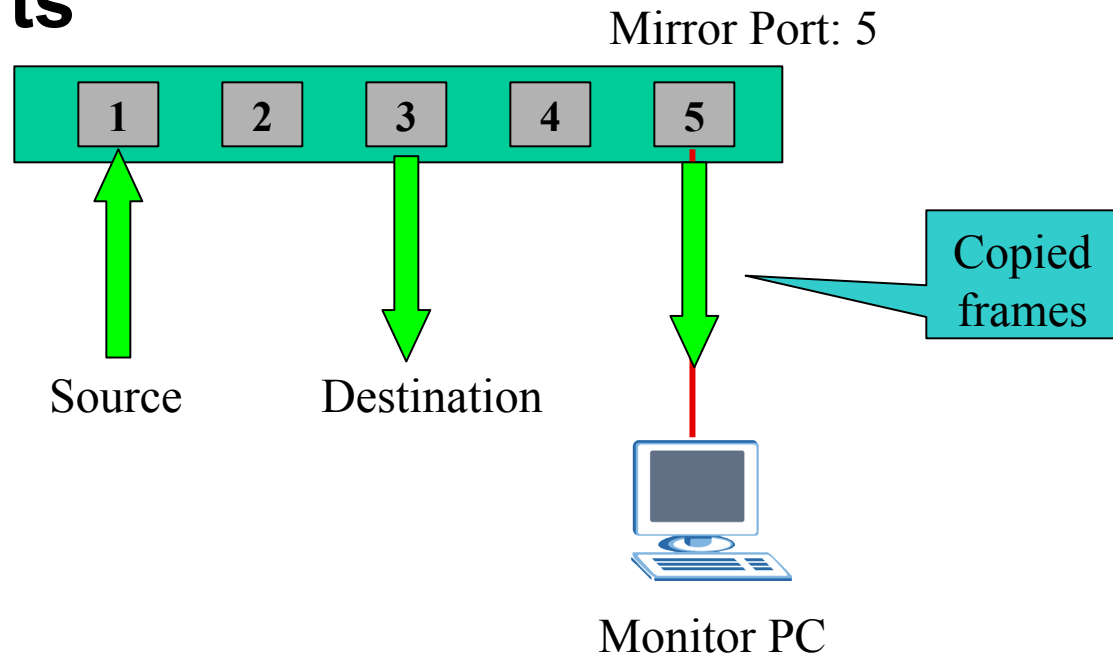
00:a0:c5:00:00:01 00:a0:c5:00:00:02 00:a0:c5:00:00:03

802.1X Port Authentication



Port Mirroring

Monitor the traffic on other ports



Port Mirroring

 **Mirroring**

Active

Monitor Port

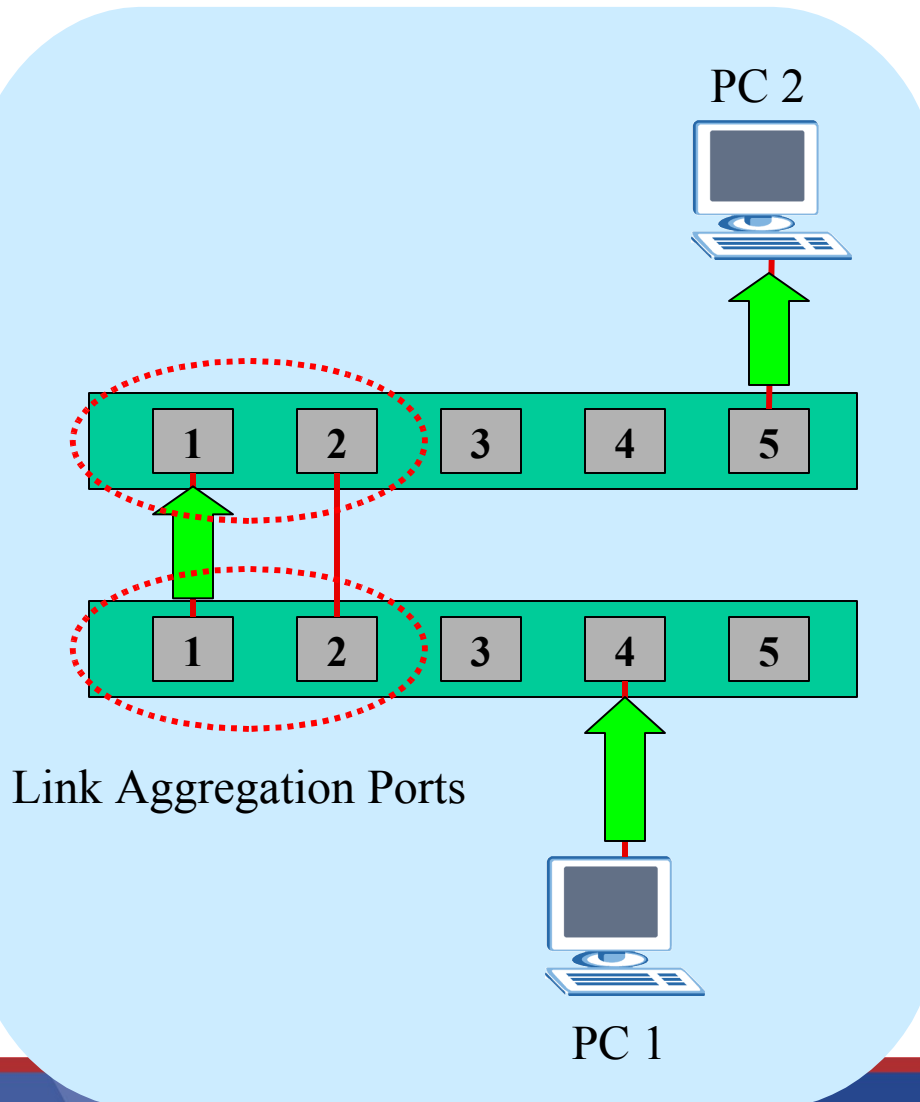
Port	Mirrored	Direction
1	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
2	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
3	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
4	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
5	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
6	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
7	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
8	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
9	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
10	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
11	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
12	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
13	<input type="checkbox"/>	Ingress <input type="button" value="v"/>
14	<input type="checkbox"/>	Ingress <input type="button" value="v"/>

Layer 2+ Switching

Erweiterte Funktionen im L2+ Ethernet Switch




- Link Aggregation; Bündeln Sie die Bandbreite
- IGMP Snooping; Nutzen Sie die Intelligenz des Netzes um Bandbreiten zu schonen

Link Aggregation

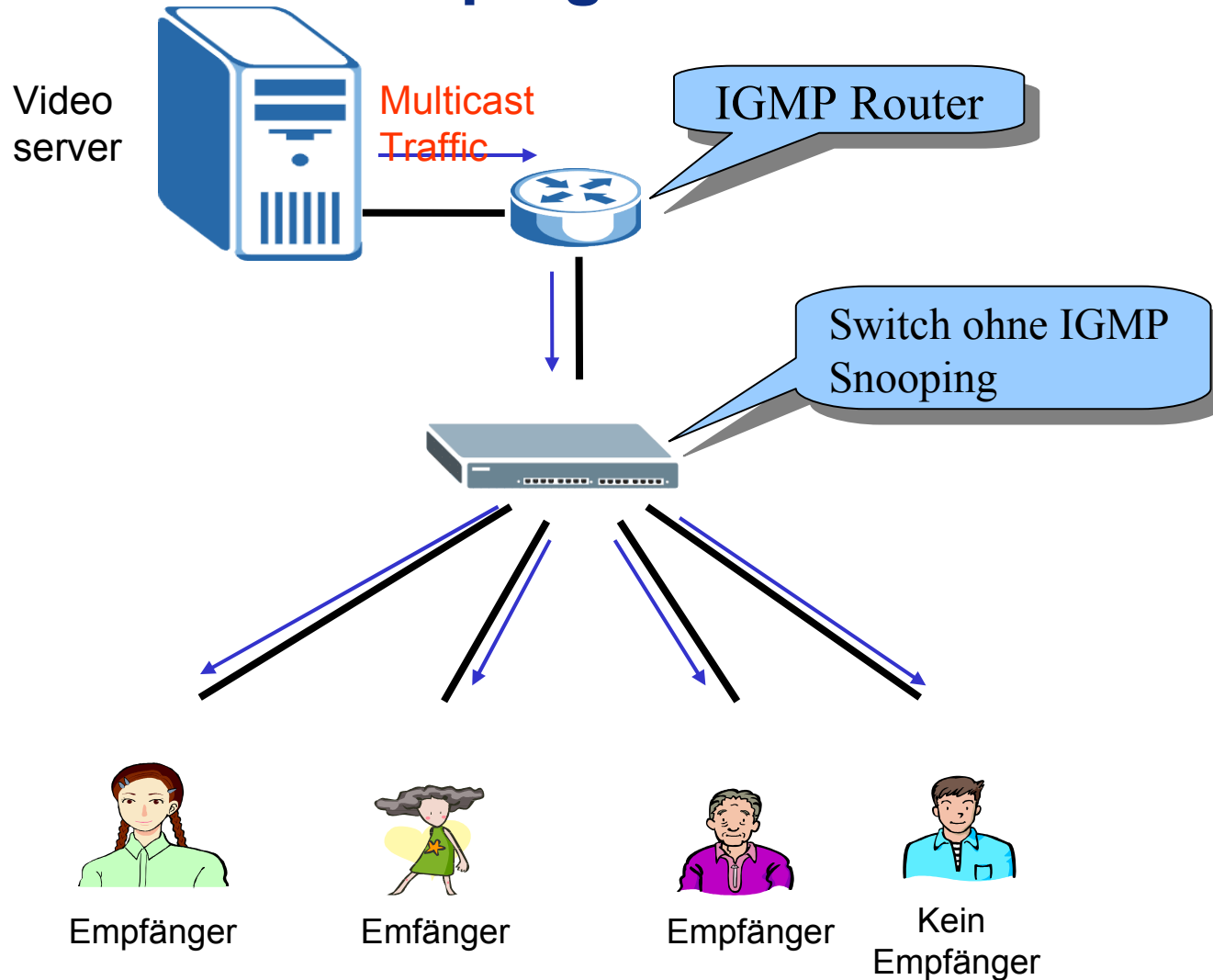


- Die Verteilung des Traffic ist basierend Auf der Quell- und Ziel- MAC Adresse des Ethernet frames.
- Der Traffic von mehreren Clients wird über eine Trunk Group Verbindung geleitet.

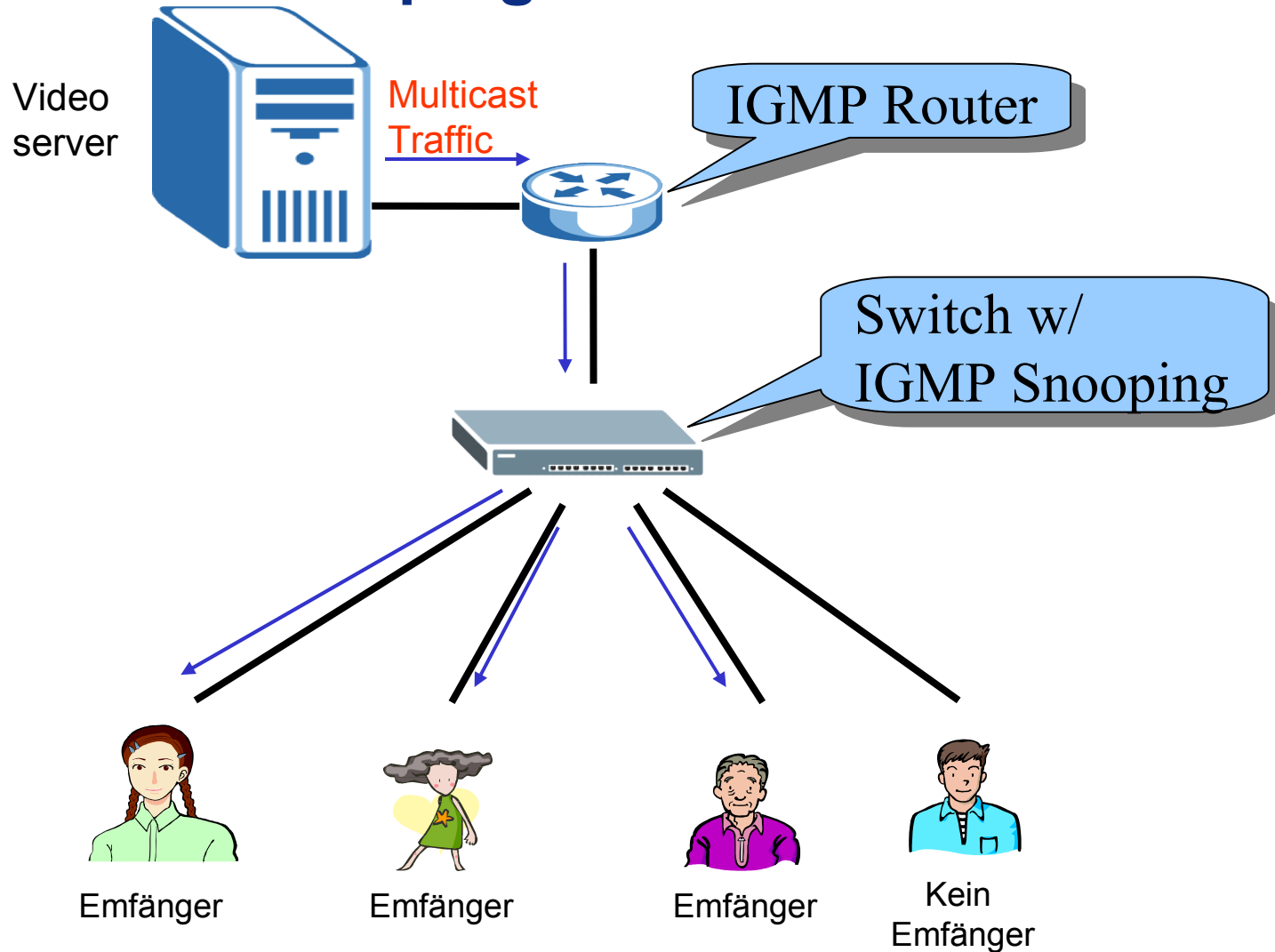
IGMP / Multicast

	Quelle	Ziel
Unicast	Eine 	Ein
Broadcast	Eine 	Alle
Multicast	Eine 	Gruppe

Ohne IGMP Snooping



Mit IGMP Snooping



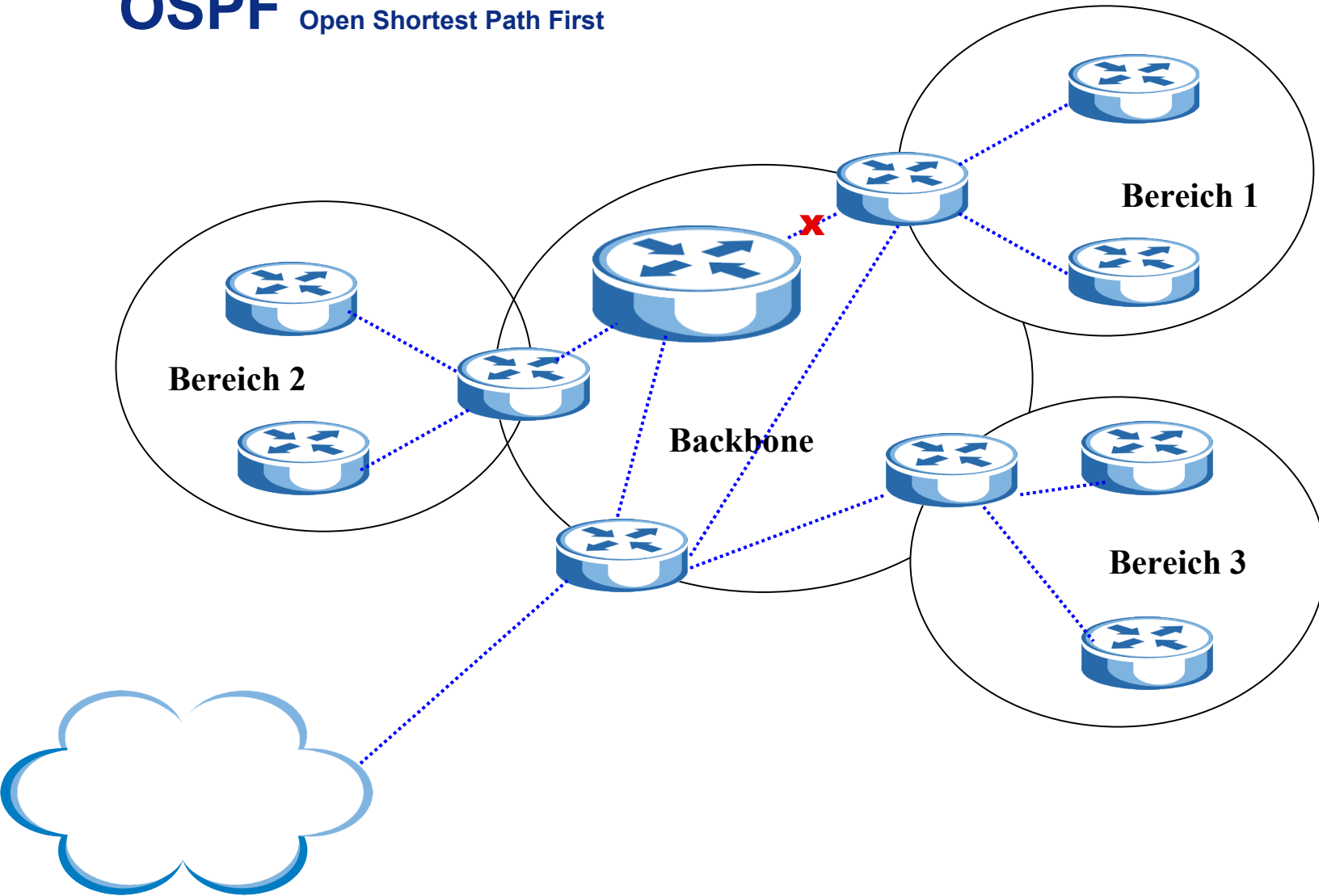
Layer 3+ Switching

Q: Warum L3 Switching?

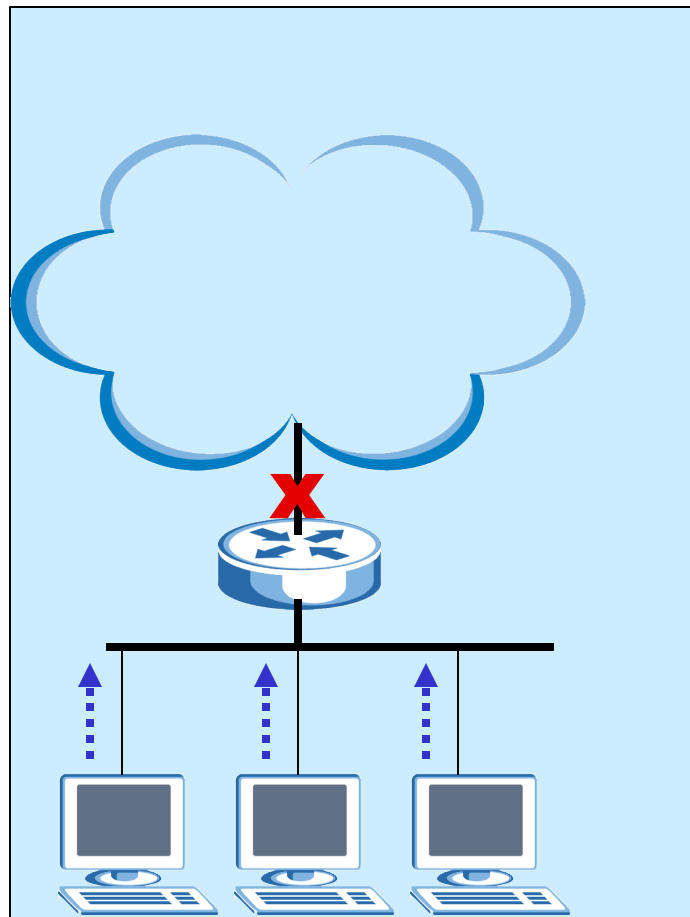
A: Redundanz

OSPF

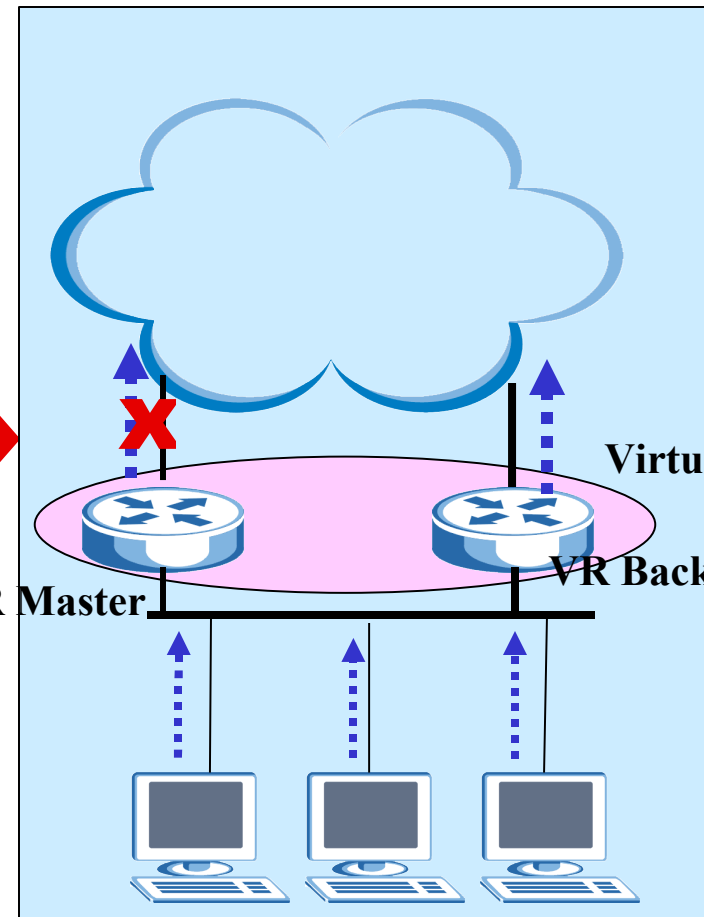
Open Shortest Path First



VRRP Virtual Router Redundancy Protocol



Ohne VRRP



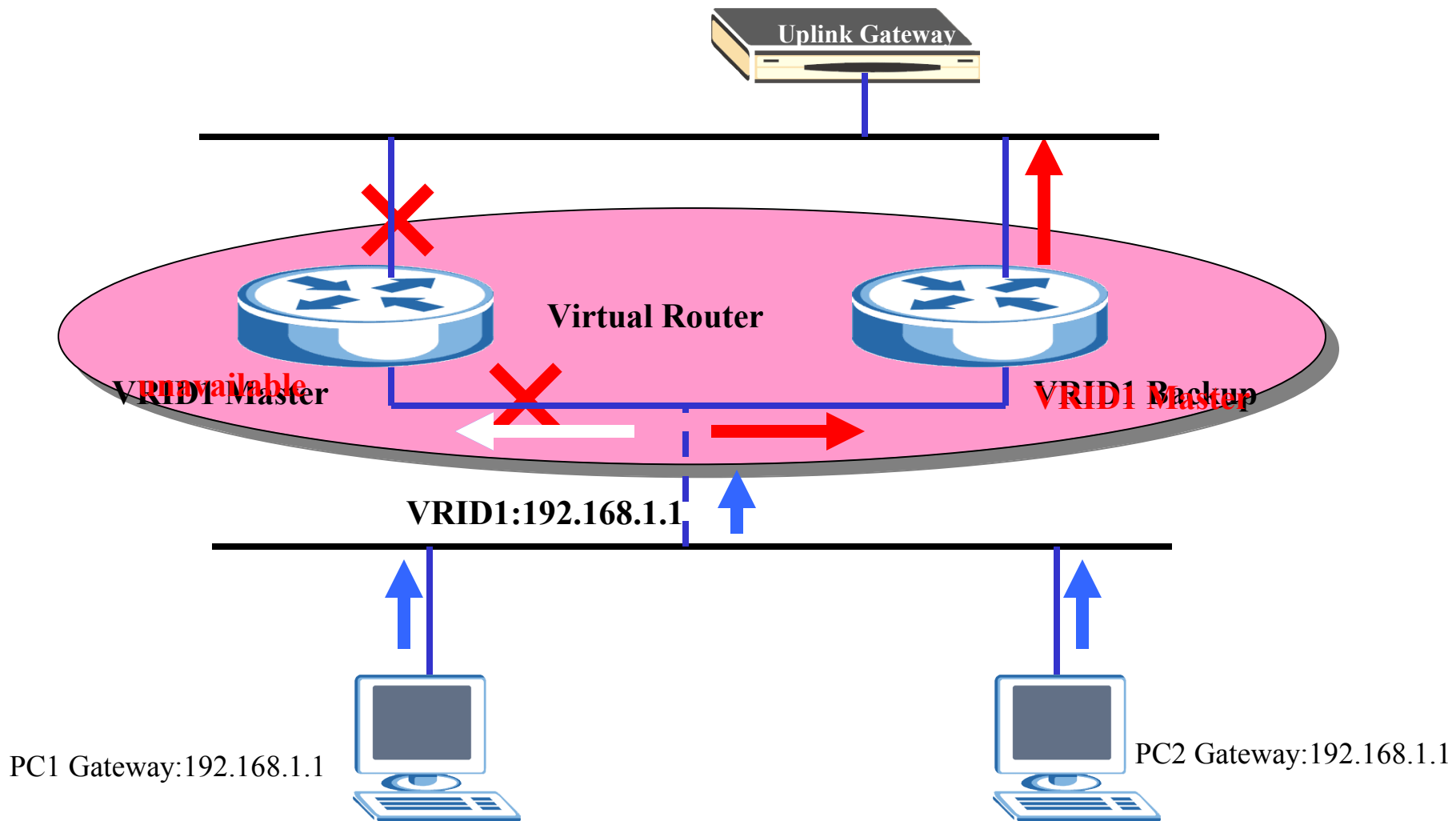
VR Master

VR Backup

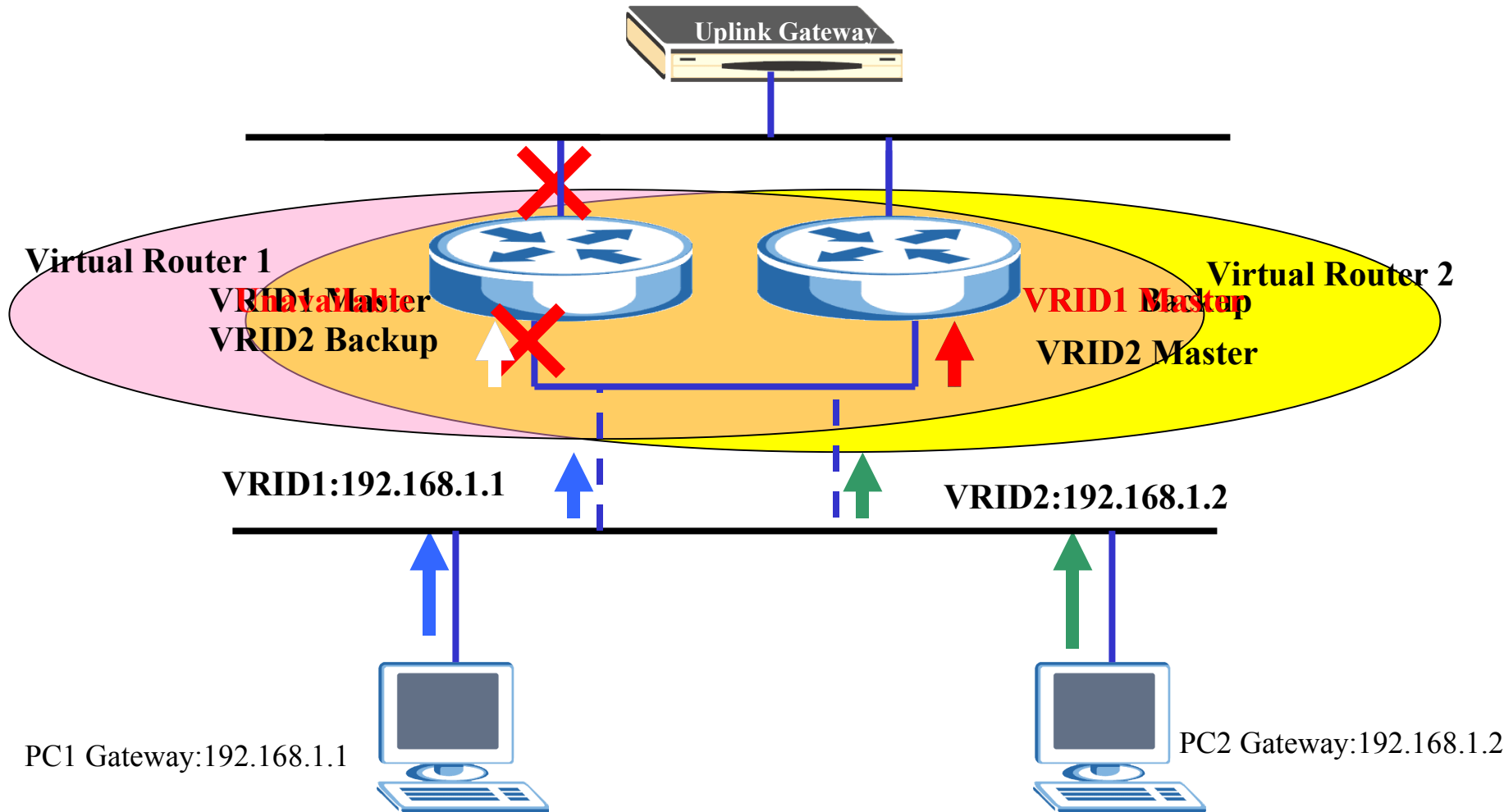
Virtual router

Mit VRRP

VRRP / Backup



VRRP / Load Sharing



Exceed the Limits

Enrich the Service