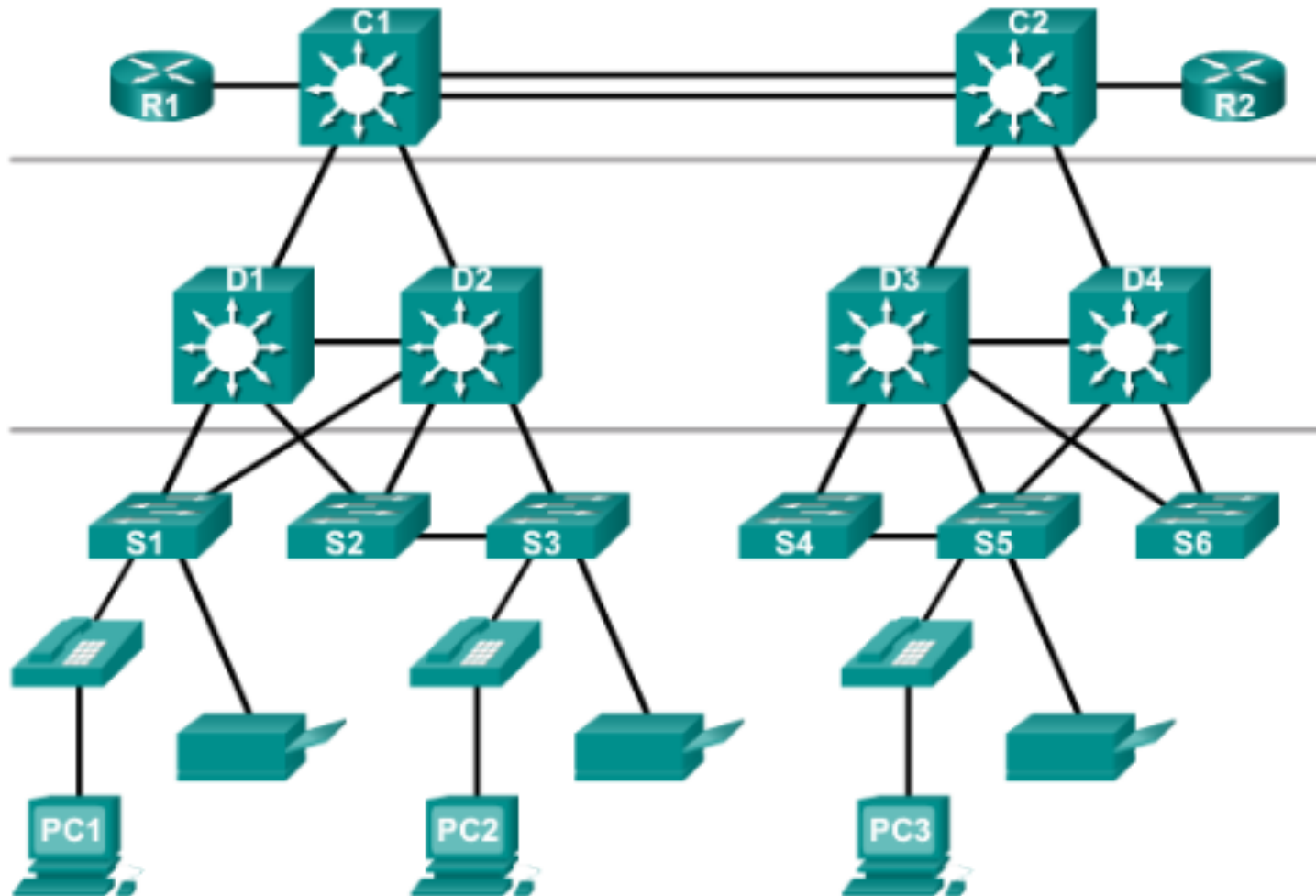
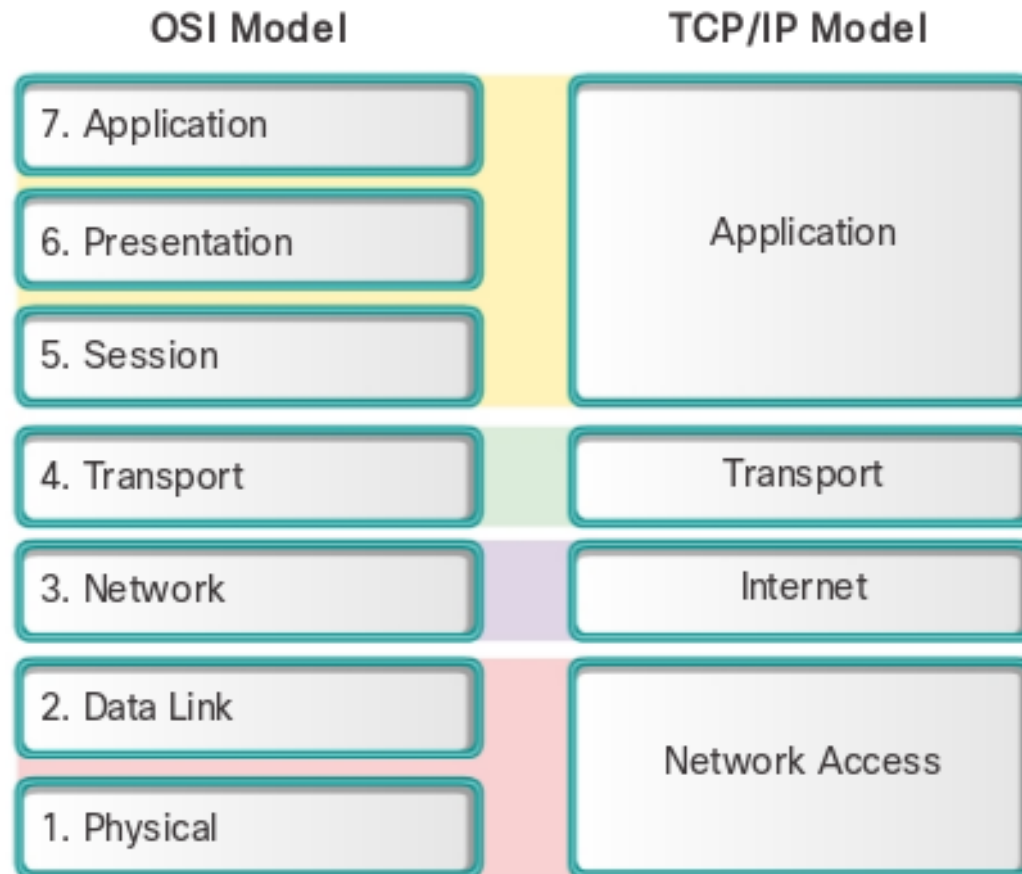


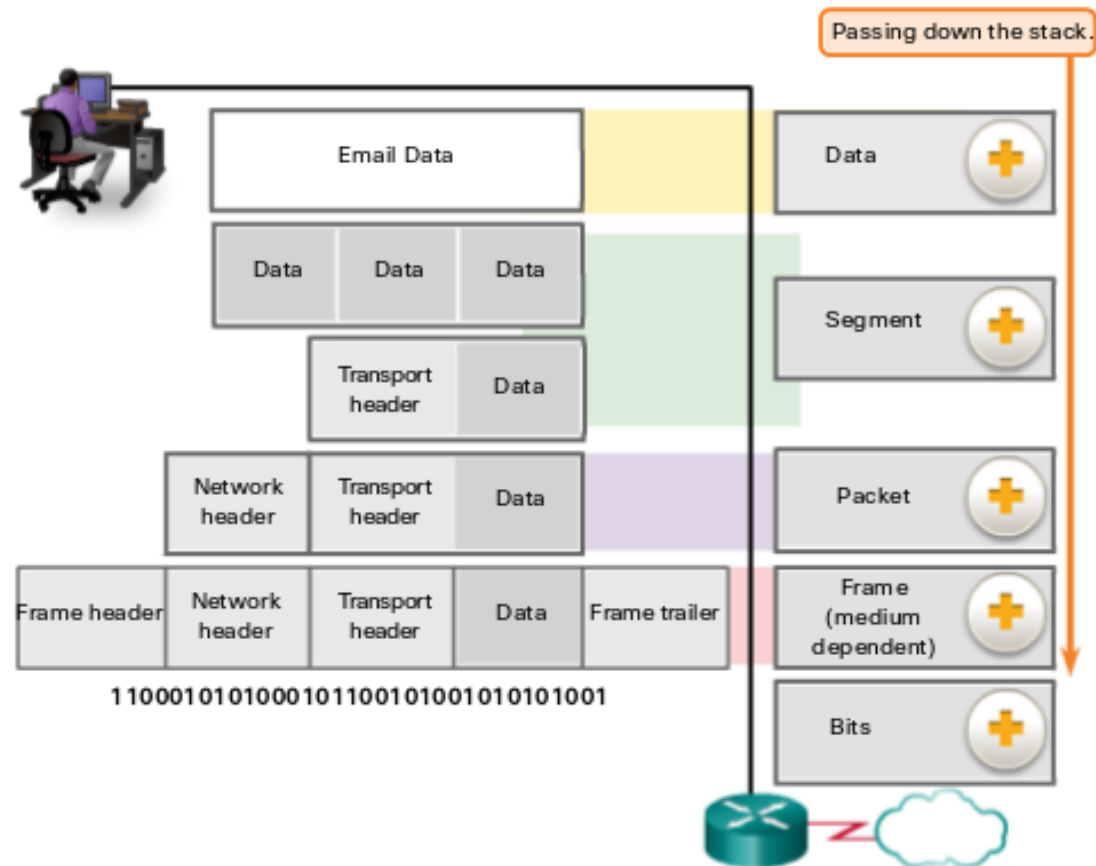
Hirarchisches Netzwerk



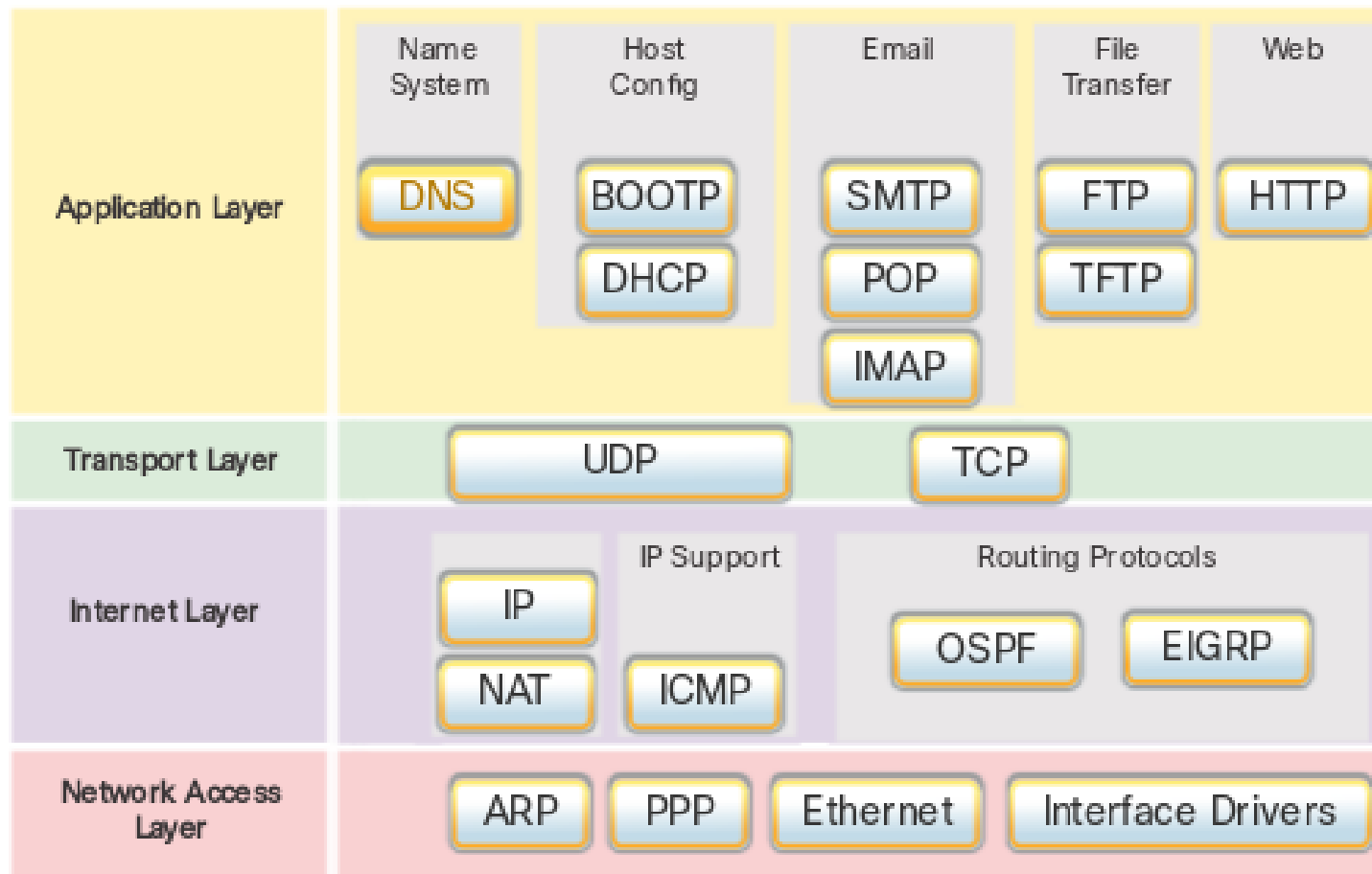
ISO/OSI vs. TCP/IP



Segmente, Pakete, Frames



Übersicht TCP/IP



Ethernet Frame



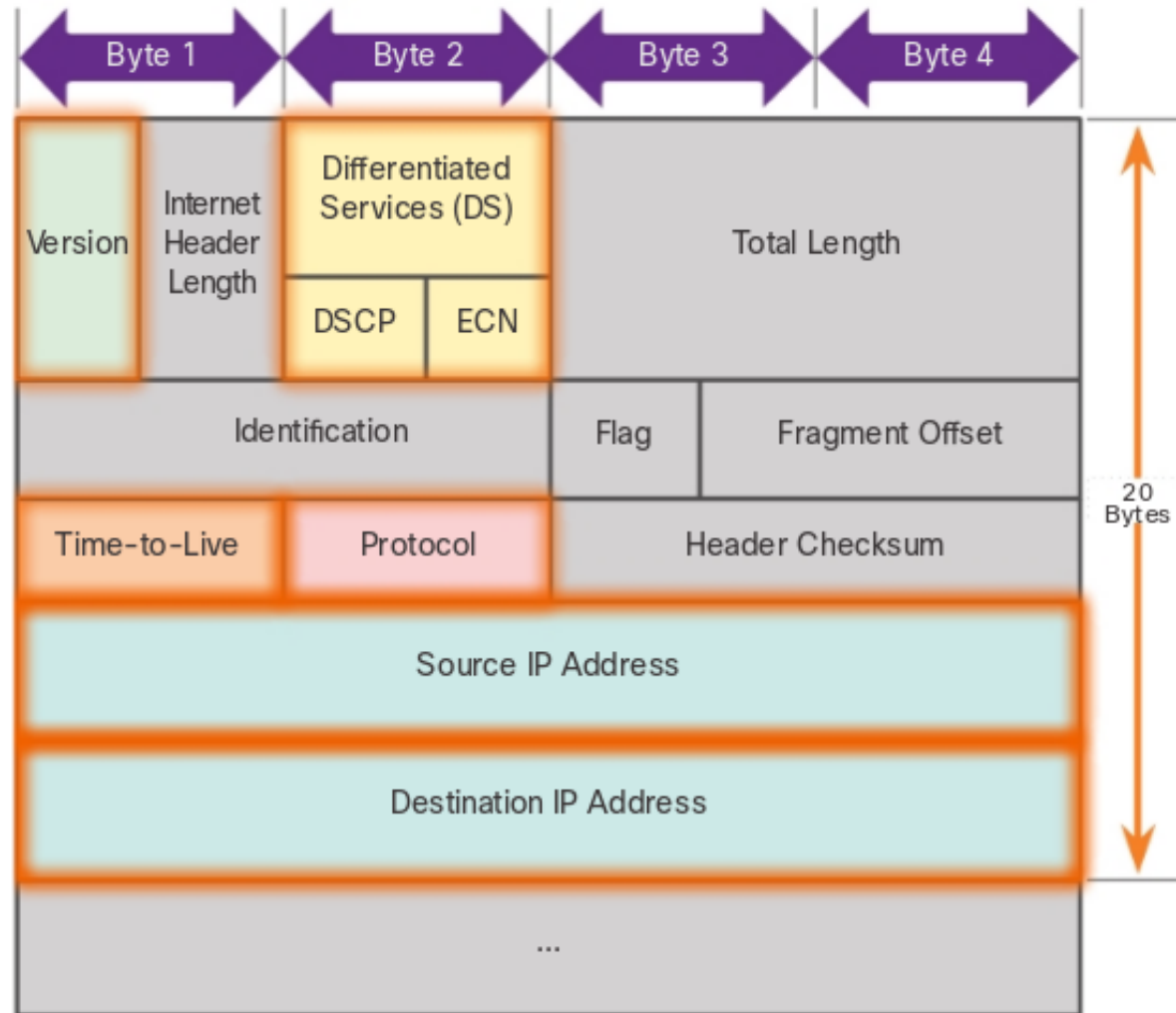
- Preamble: 01111110
- MAC Adressen: für den Switch
- EtherType: Protokoll der höheren Ebene,
 - Ip4, ip6 oder arp
- Data: IP Paket
- FCS: Prüfsumme (falls korrupt, wird das Frame verworfen)

Ethernet Frame

- Von Minimum 64 Bytes bis Maximum 1518 Bytes
- Kleiner als 64 Bytes bezeichnet man ein Frame als "runt frame" oder "collision fragment".
- Frames die größer sind als 1500 Bytes bezeichnet man als "jumbo" Frames.

```
Sl# show interfaces fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:06, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes);
Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
  25994 packets input, 2013962 bytes, 0 no buffer
    Received 22213 broadcasts (21934 multicasts)
      0 runs, 0 giants, 0 throttles
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
      0 watchdog, 21934 multicast, 0 pause input
      0 input packets with dribble condition detected
  7203 packets output, 771291 bytes, 0 underruns
<output omitted>
```

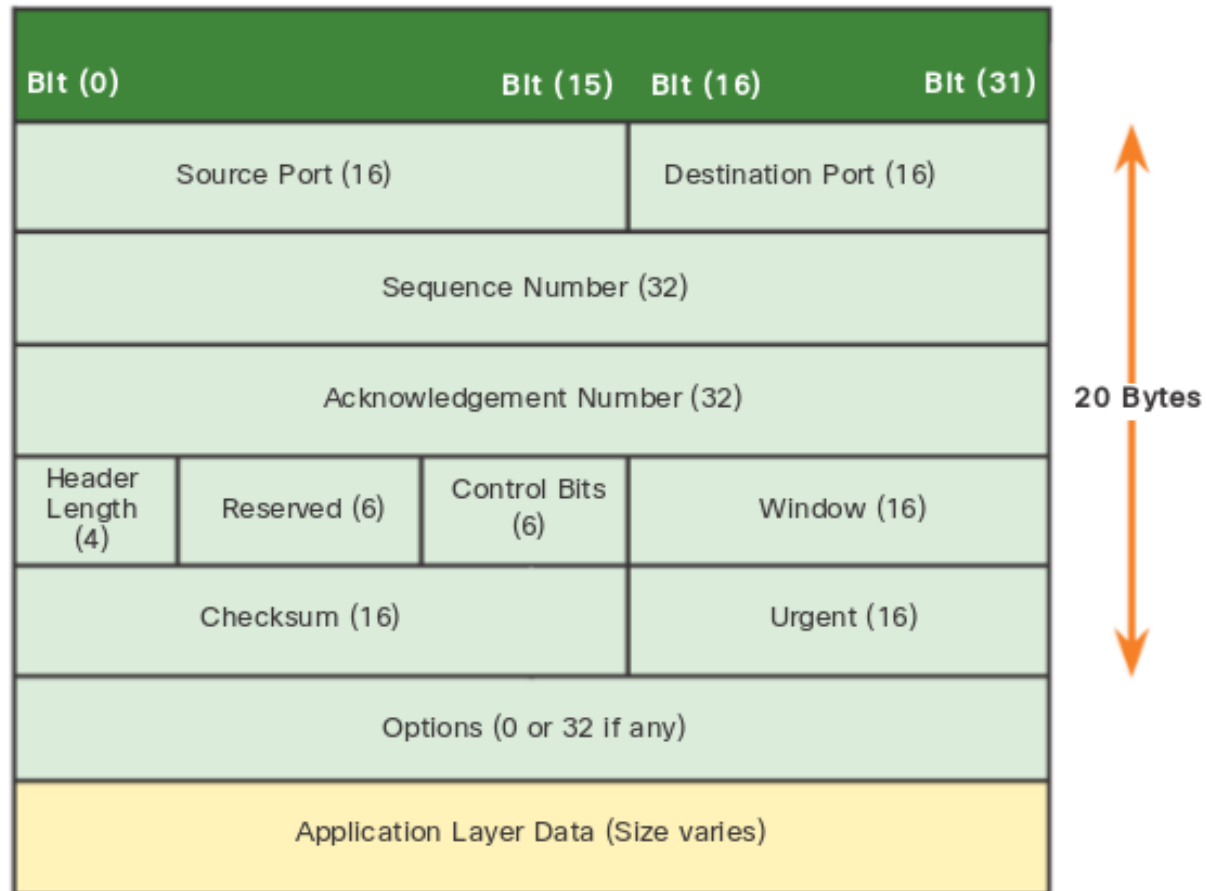
IP Pakete



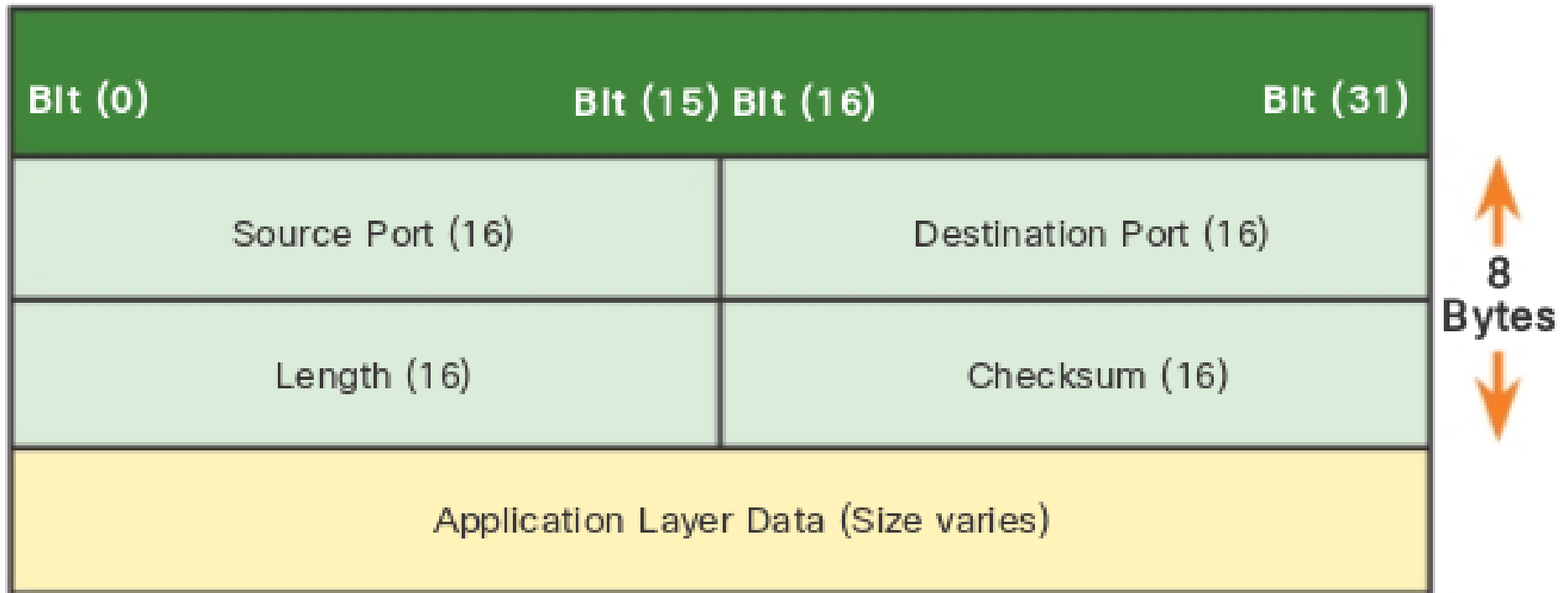
IP Pakete

- Version: IPv4 oder IPv6
- Time to Live (TTL): jeder Router dekrementiert dieses Feld, bei 0 wird das Paket verworfen. Es entstehen somit keine Loops.
- Protokoll: verwendetes Protokoll auf der nächsthöheren Ebene
 - TCP, UDP oder ICMP
- IP Adressen für die Router

TCP Segment



UDP Datagram



Funktionsweise Switch

- Ein Switch schaut sich die Source und Destination MAC eines Frames an.
 - Mittels Source MAC "lernt" der Switch an welchem Port ein PC angeschlossen ist.
 - Mittels Destination MAC wird das Frame an den Empfänger weitergeleitet ("forward")
 - Wenn ein Switch nicht weiß, wohin ein Frame weiterleiten, dann flutet ("flooding") er das Frame

Funktionsweise Switch



Store and Forward Switch

- Das gesamte Frame wird vom Switch empfangen.
- Der Switch berechnet die Prüfsumme (CRC), ist diese falsch, wird das Frame verworfen.
- Ist die Prüfsumme richtig, wird kontrolliert, ob die Source MAC in der MAC Tabelle eingetragen ist.
- Dann wird das Frame weitergeleitet

Store and Forward Switch



Cut- through Switch

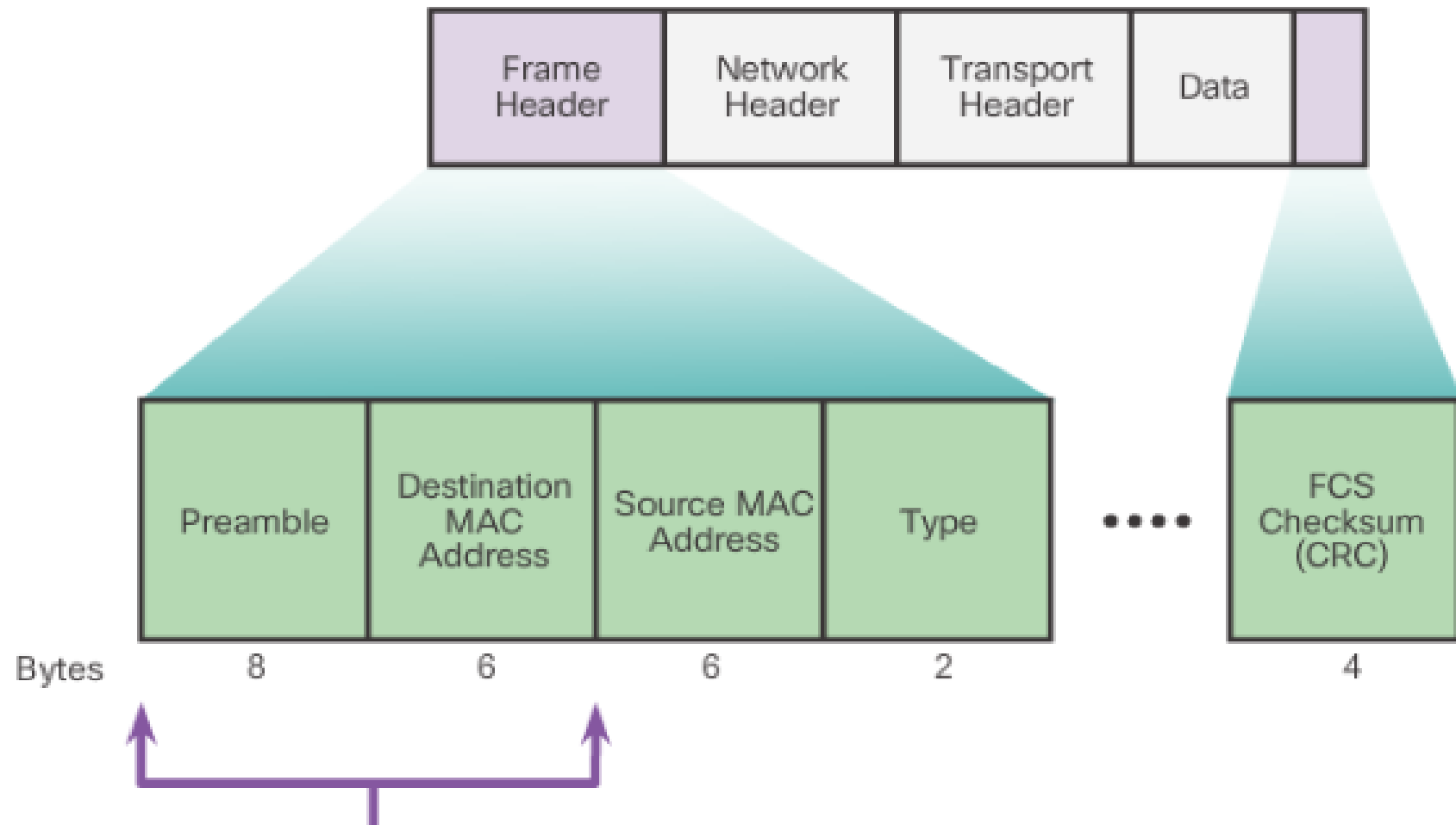
- Bei einem cut- through Switch wird nur die Destination MAC Adresse kontrolliert.
- Der Switch leitet sofort jedes Bit weiter.
- Das Frame wird ohne Kontrolle weitergeleitet.
- Die Source MAC Adresse wird nachwievor gelernt.
- Die Kontrolle, ob das Frame nicht korrupt ist, wird den Clients überlassen.

Cut- through Switch



Cut- through Switch

Cut-Through Switching



Frames can begin to be forwarded as soon as the Destination MAC is received.

Broadcast Domäne

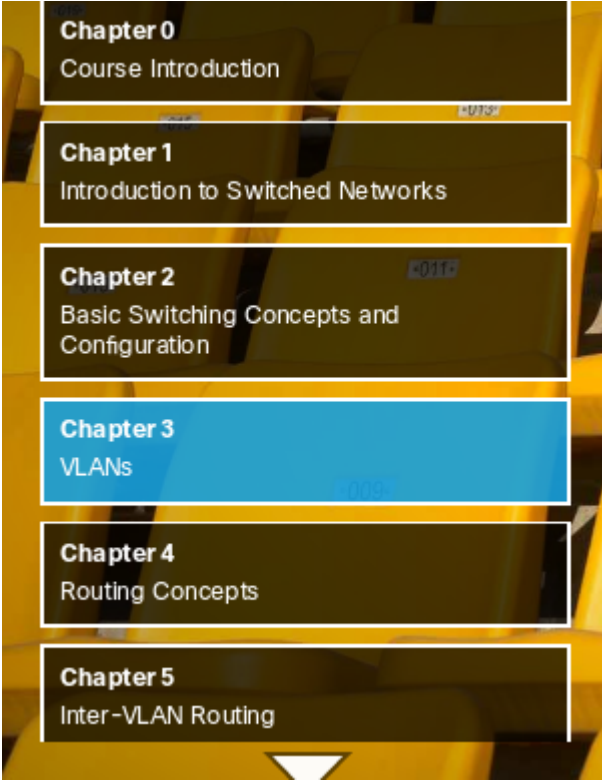
- Wenn die Destination MAC Adresse alles Einsen beinhaltet, (FF:FF:FF:FF:FF:FF), dann nennt man es ein Broadcast Paket auf Layer 2.
- Dieses Paket wird an alle Geräte weitergeleitet, die an einem Switch hängen.
- Unterschied Broadcast, Multicast:
 - Alle beide werden an alle Geräte (z.B. PCs) verschickt
 - Die NIC des angeschlossenen Geräts (z.B. PC) löst bei einem Broadcast immer einen Interrupt aus, bei einem Multicast nur dann, wenn die NIC teil der Multicast-Gruppe ist.

Broadcast Domäne



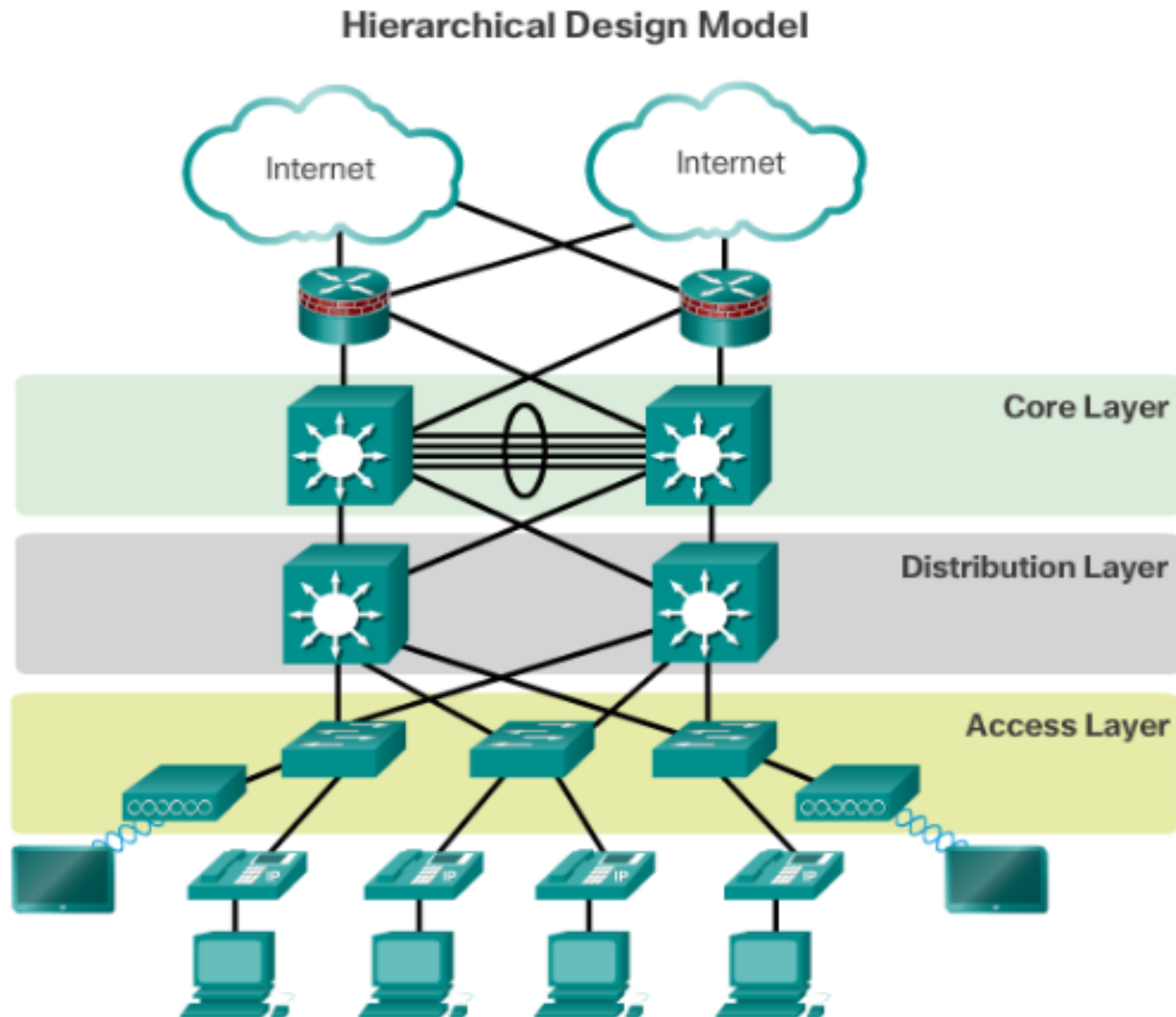
VLAN

- todo

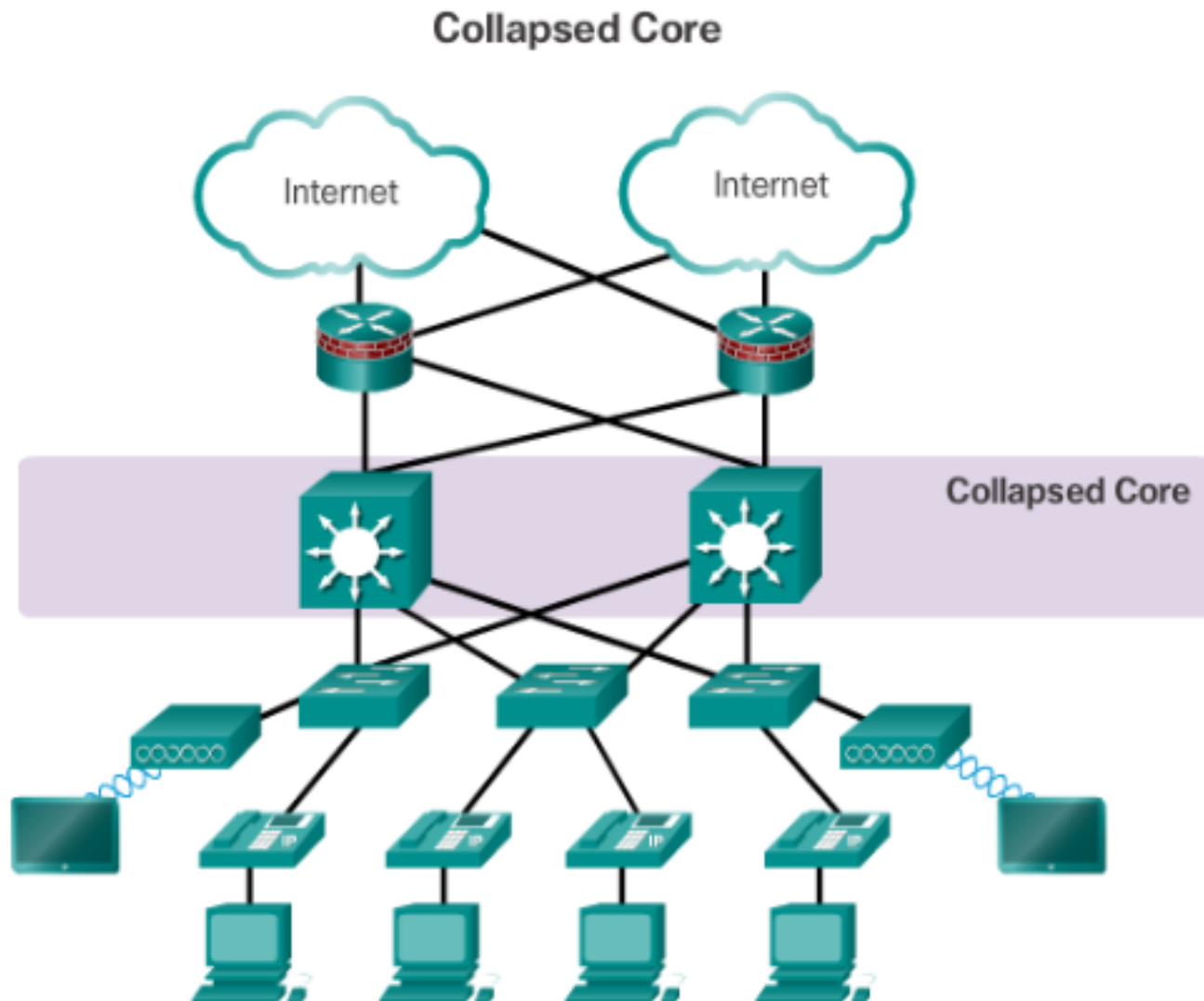


Chapter 0 Course Introduction
Chapter 1 Introduction to Switched Networks
Chapter 2 Basic Switching Concepts and Configuration
Chapter 3 VLANs
Chapter 4 Routing Concepts
Chapter 5 Inter-VLAN Routing

Hirarchisches Netzwerk Design



Hirarchisches Netzwerk Design



Spanning Tree

- Durch ein hierarchisches Netzwerkdesign entstehen auch Schleifen.
 - Wir haben gesehen, dass diese fatale Folgen für ein Netzwerk haben können
 - Broadcast storm
 - Multiple Unicast Frames
 - Instable MAC Tables
- Durch das Spanning Tree Protokoll werden diese Probleme eliminiert und es entstehen redundante Wege.
 - Sehr gut für die Ausfallsicherheit!!!

FHRP

- First Hop Redundancy Protokoll
 - Das Problem mit dem default Gateway.
 - Ein Gerät hat nur einen default Gateway.
 - Deshalb gibt es einen "single point of failure"
 - Fällt der default Gateway aus, ist das lokale Netz von der Außenwelt abgeschnitten.
- Man bräuchte also einen zweiten Gateway, der im Falle eines Ausfalls die Pakete weiterleitet.

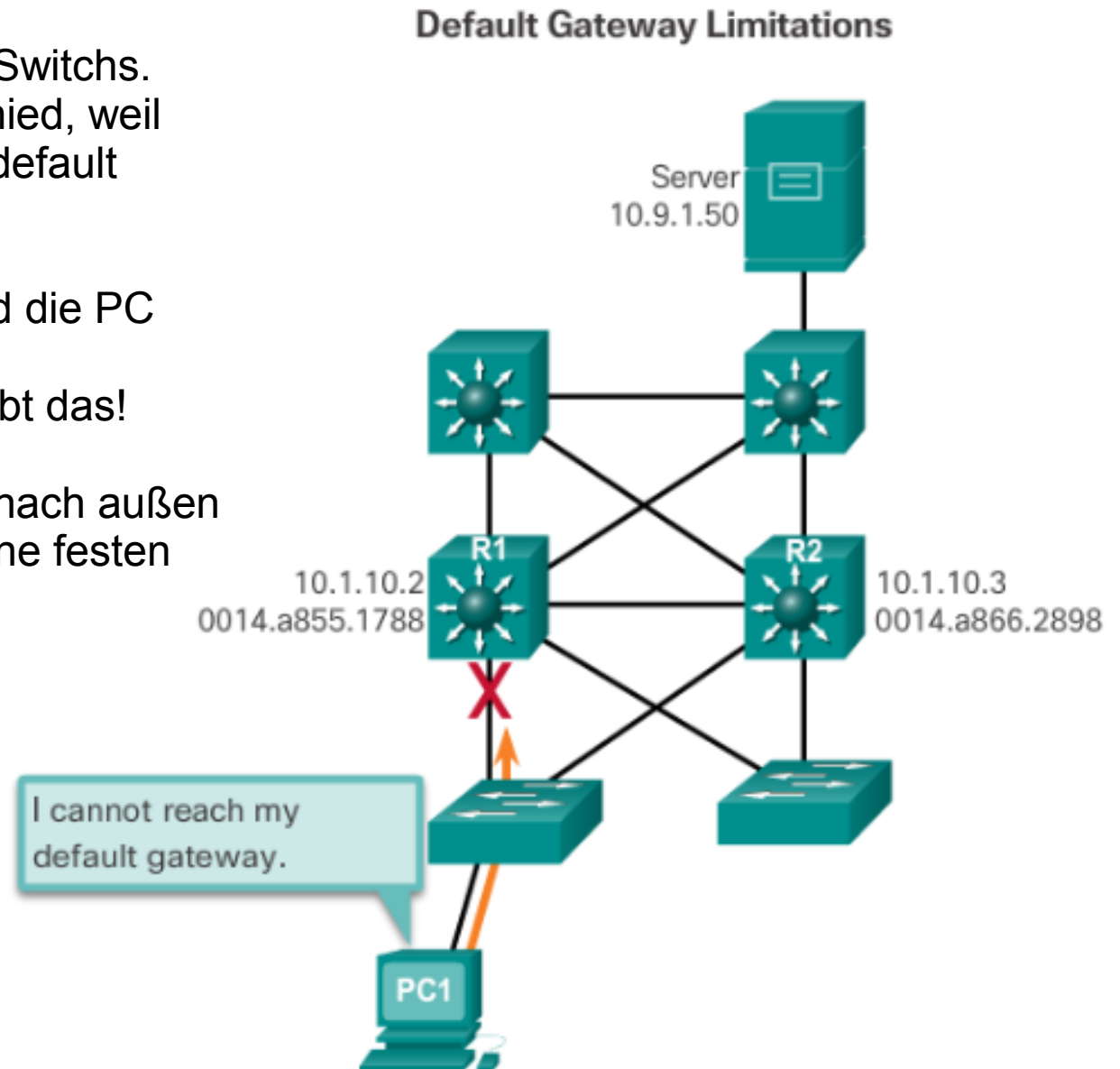
FHRP

Alle Router im Bild sind Layer 2 Switchs.
Das macht aber keinen Unterschied, weil normalerweise in L2 Switch der default Gateway für ein VLAN ist.

Wenn der Router R1 ausfällt sind die PC von außen noch erreichbar.

Das Routing Protokoll erlaubt das!

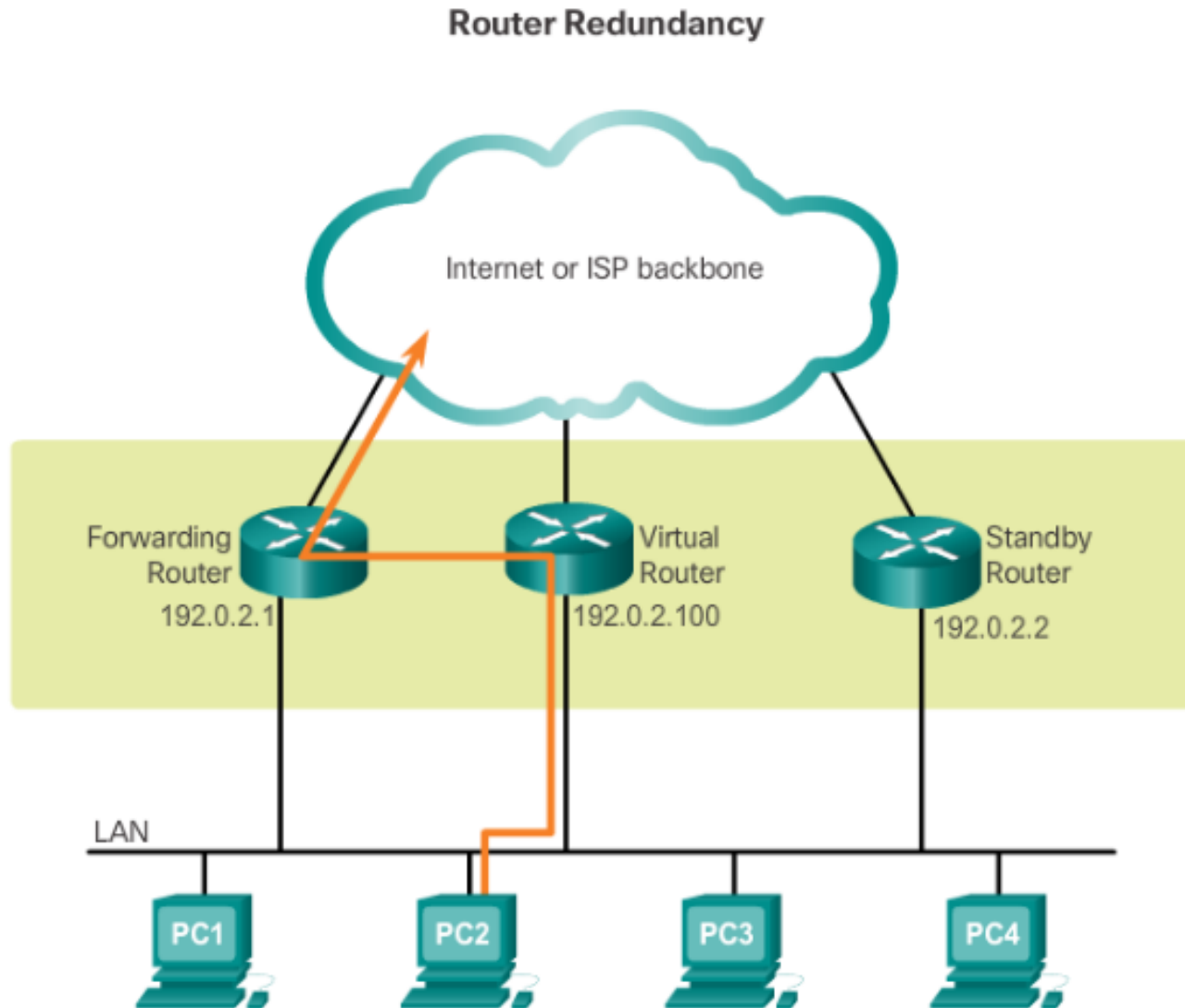
Die PC können aber nicht mehr nach außen kommunizieren, weil jeder PC eine festen default Gateway eingestellt hat.



Router Redundanz

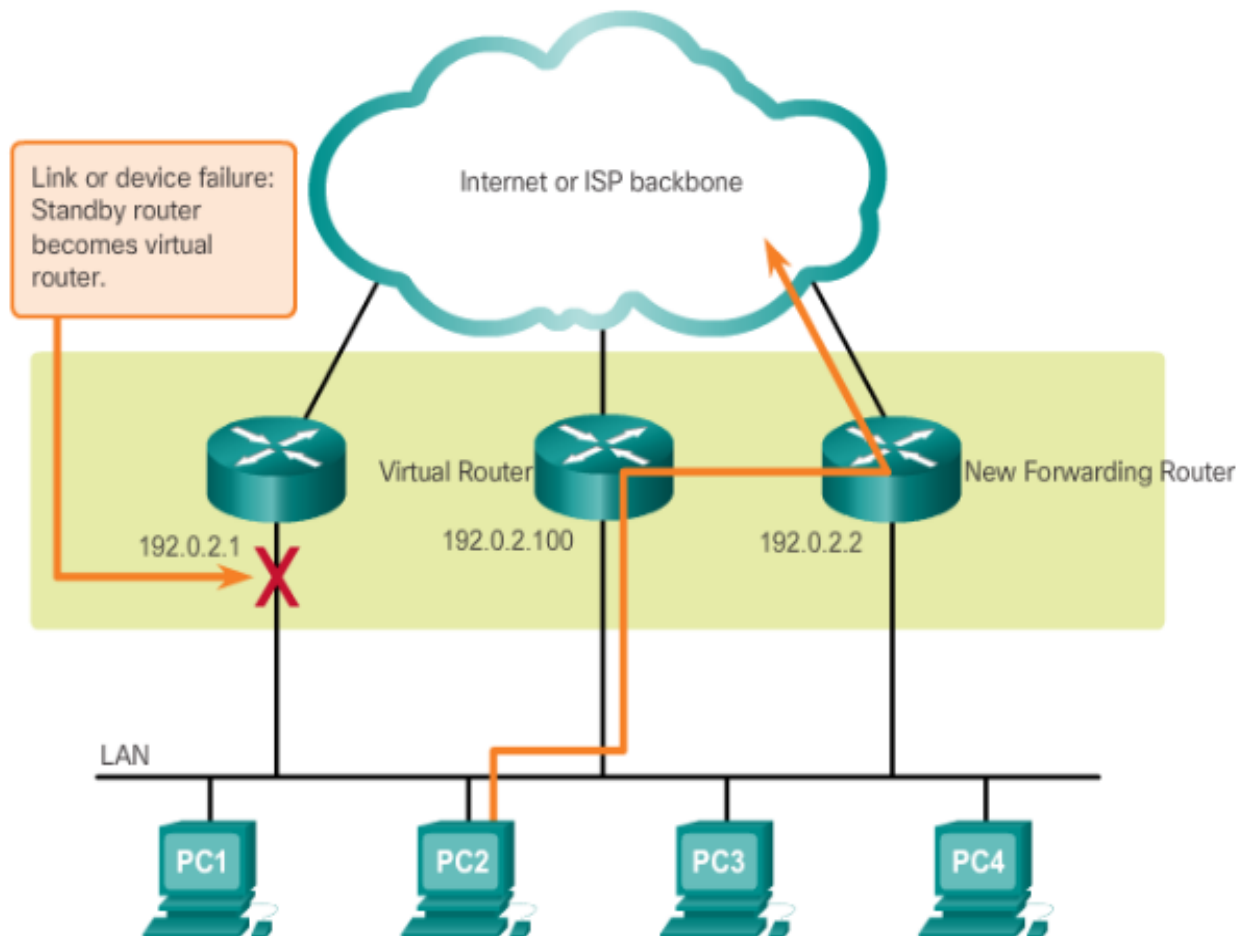
- Man konfiguriert mehrere Router als eine Gruppe und definiert einen virtuellen Router.
- Der virtuelle Router leitet die Pakete nicht direkt in Internet weiter, sondern an einen Forward Router.
- Fällt der Forward Router aus, gibt es eine Standby Router, der einspringt.
- Normalerweise gibt es für eine Gruppe eine Virtuellen Gateway ID und Virtuelle Gateway MAC

Router Redundanz



Router Redundanz

Steps for Router Failover



Router Redundanz

- Wenn der Forward Router ausfällt, macht das Protokoll folgendes:
 - Der Standby Router erhält keine Hello Pakete vom Forward Router mehr.
 - Der Standby Router übernimmt die Rolle des Forward Router
 - Der neue Forward Router hat dieselbe virtuelle MAC und IP Adresse des "alten" Forward Router.
 - Die PCs merken somit den Ausfall nicht, da sie als default Gateway die virtuelle Gateway IP eingestellt haben.

Protokolle redundante Router

- Hot Standby Router Protocol (HSRP)
 - Cisco proprietär
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
 - Offenes Protokoll
- Gateway Load Balancing Protocol (GLBP)
 - Cisco proprietär
 - Erlaubt zudem Load Balancing

Hot Standby Router Protocol

First-Hop Router Redundancy Options



Hot Standby Router Protocol

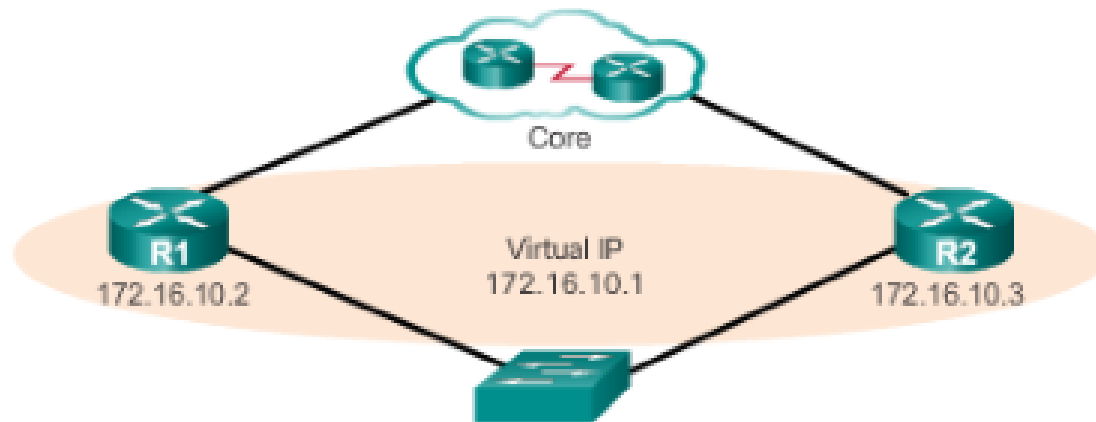
- Eigenschaften Active Router
 - Antwortet auf ein ARP Paket mit der virtuellen MAC Adresse.
 - Leitet alle erhaltenen Pakete weiter ins Internet
 - Sendet in regelmäßigen Abständen Hello Pakete an der Standby Router
 - Kennt die virtuelle IP Adresse

Hot Standby Router Protocol

```
Router# show standby
Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
    Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
    Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
    Gratuitous ARP 14 sent, next in 7.412 secs
    Preemption enabled, min delay 50 sec, sync delay 40 sec
    Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  Group name is "HSRP1" (cfgd)
Follow by groups:
Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.666)
Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

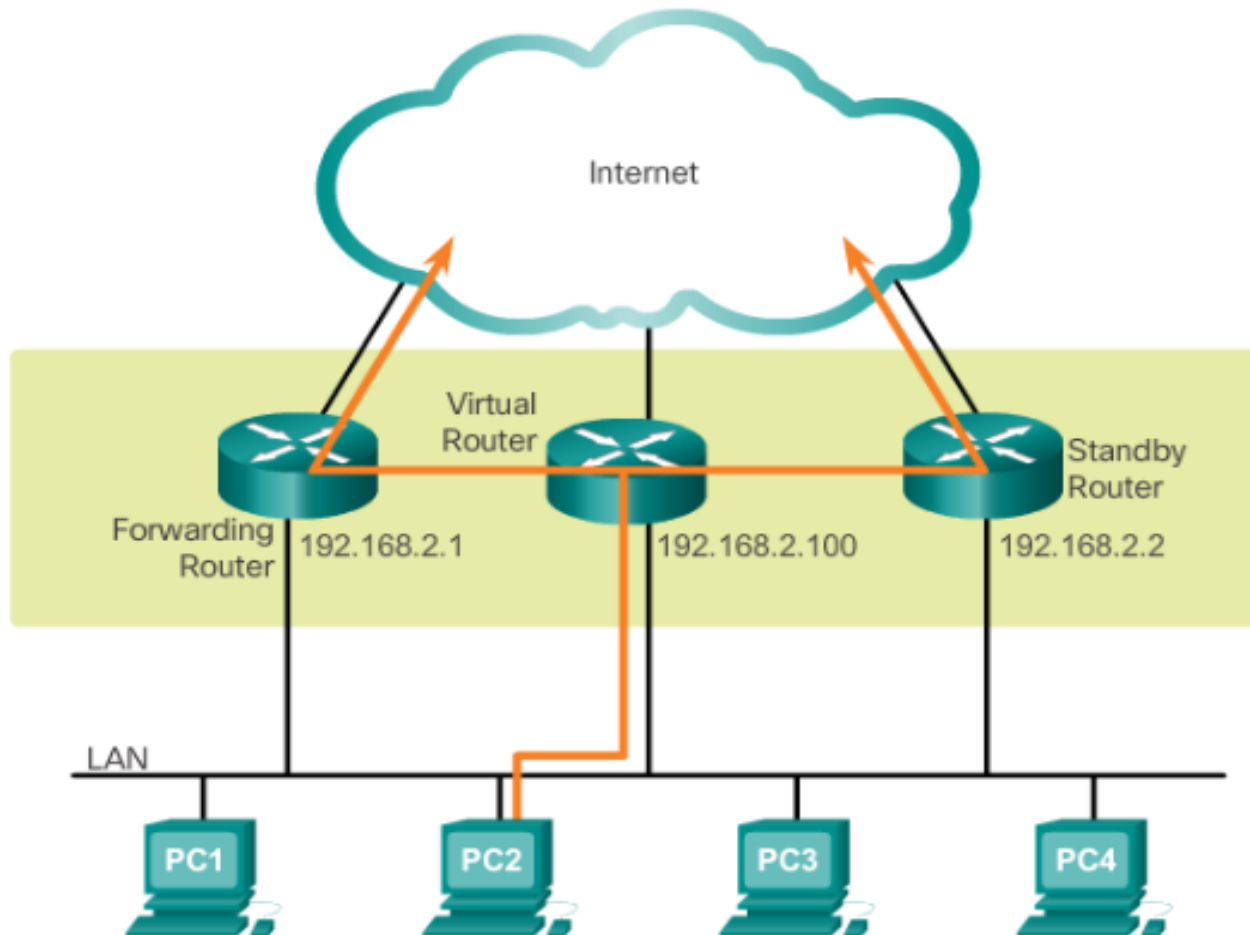
Hot Standby Router Protocol

- Was macht der standby Router?
 - Horcht auf die periodischen Hello Pakete
 - Übernimmt die aktive Rolle, wenn er keine Hello Pakete bekommt



Gateway Load Balancing Protocol

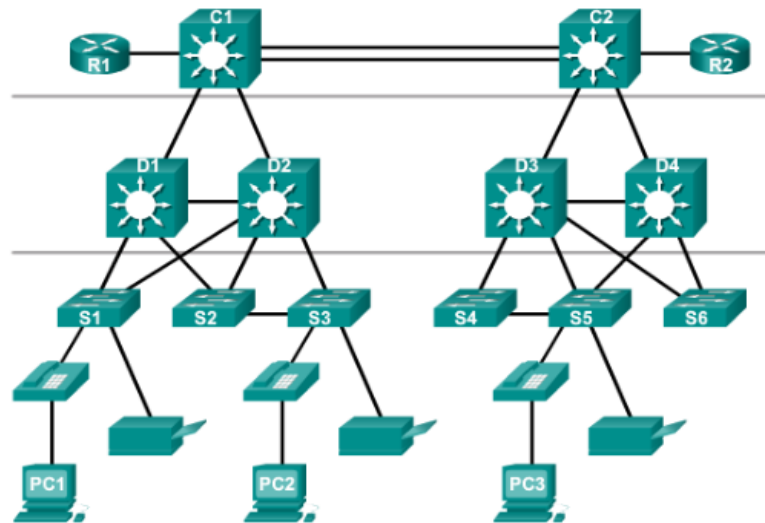
Gateway Load Balancing Protocol



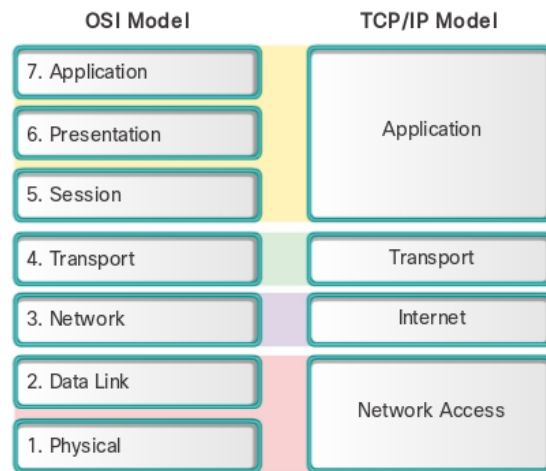
Übung

- Mache die Übung

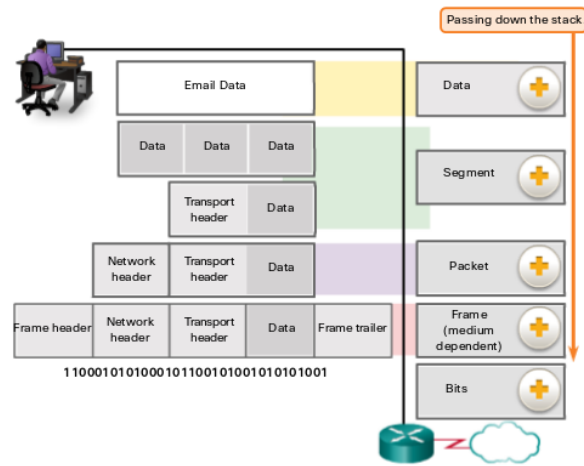
Hirarchisches Netzwerk



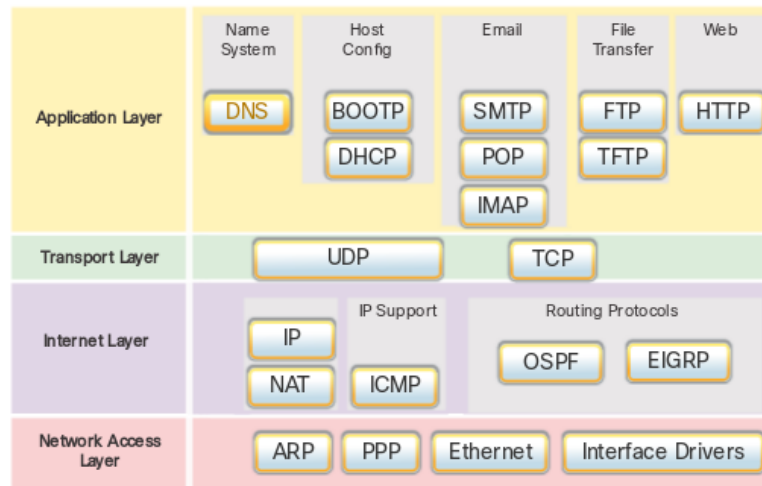
ISO/OSI vs. TCP/IP



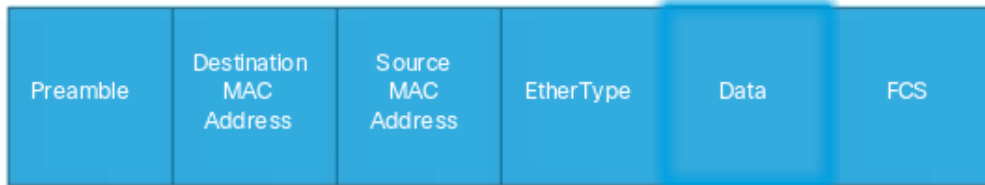
Segmente, Pakete, Frames



Übersicht TCP/IP



Ethernet Frame



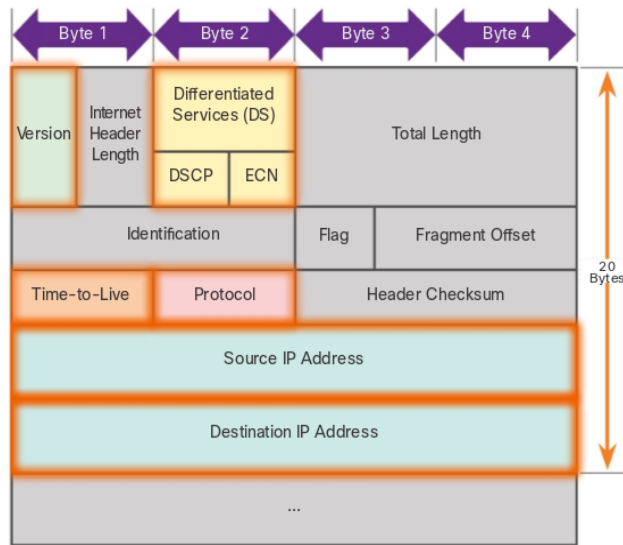
- Preamble: 01111110
- MAC Adressen: für den Switch
- EtherType: Protokoll der höheren Ebene,
 - Ip4, ip6 oder arp
- Data: IP Paket
- FCS: Prüfsumme (falls korrupt, wird das Frame verworfen)

Ethernet Frame

- Von Minimum 64 Bytes bis Maximum 1518 Bytes
- Kleiner als 64 Bytes bezeichnet man ein Frame als "runt frame" oder "collision fragment".
- Frames die größer sind als 1500 Bytes bezeichnet man als "jumbo" Frames.

```
SI# show interfaces fastethernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
Hardware is Fast Ethernet, address is 0cd9.96e8.8a01 (bia 0cd9.96e8.8a01)
MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA, loopback not set
Keepalive set (10 sec)
Full-duplex, 100Mb/s, media type is 10/100BaseTX
input flow-control is off, output flow-control is unsupported
ARP type: ARPA, ARP Timeout 04:00:00
Last input 00:00:01, output 00:00:06, output hang never
Last clearing of "show interface" counters never
Input queue: 0/75/0/0 (size/max/drops/flushes);
Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
25994 packets input, 2013962 bytes, 0 no buffer
Received 22213 broadcasts (21934 multicasts)
0 runs, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
0 watchdog, 21934 multicast, 0 pause input
0 input packets with dribble condition detected
7203 packets output, 771291 bytes, 0 underruns
<output omitted>
```

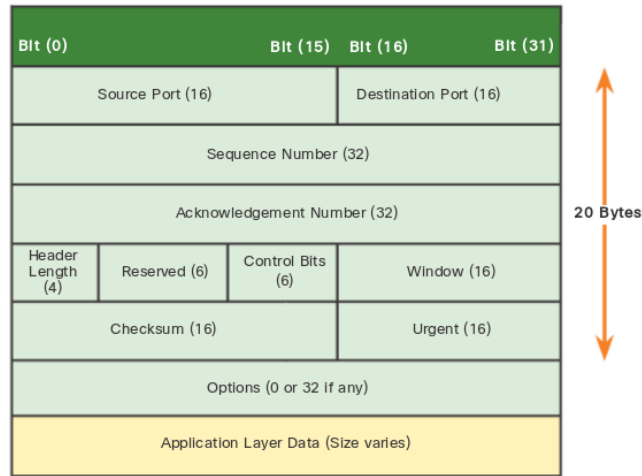
IP Pakete



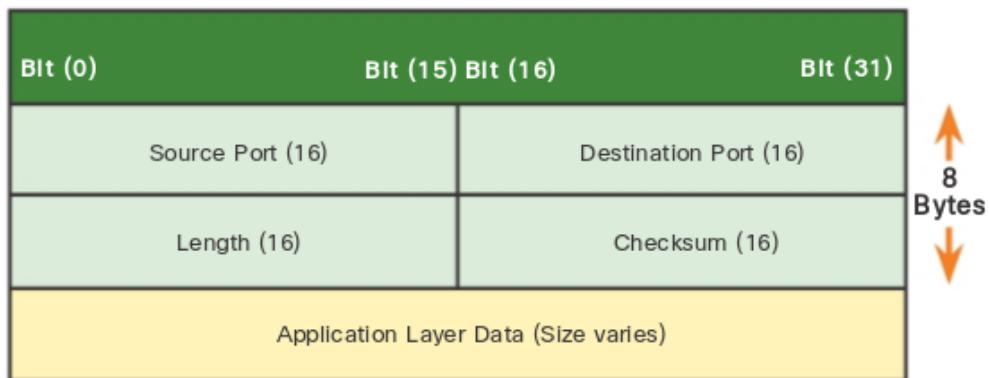
IP Pakete

- Version: IPv4 oder IPv6
- Time to Live (TTL): jeder Router dekrementiert dieses Feld, bei 0 wird das Paket verworfen. Es entstehen somit keine Loops.
- Protokoll: verwendetes Protokoll auf der nächsthöheren Ebene
 - TCP, UDP oder ICMP
- IP Adressen für die Router

TCP Segment



UDP Datagram



Funktionsweise Switch

- Ein Switch schaut sich die Source und Destination MAC eines Frames an.
 - Mittels Source MAC "lernt" der Switch an welchem Port ein PC angeschlossen ist.
 - Mittels Destination MAC wird das Frame an den Empfänger weitergeleitet ("forward")
 - Wenn ein Switch nicht weiß, wohin ein Frame weiterleiten, dann flutet ("flooding") er das Frame

Funktionsweise Switch



Store and Forward Switch

- Das gesamte Frame wird vom Switch empfangen.
- Der Switch berechnet die Prüfsumme (CRC), ist diese falsch, wird das Frame verworfen.
- Ist die Prüfsumme richtig, wird kontrolliert, ob die Source MAC in der MAC Tabelle eingetragen ist.
- Dann wird das Frame weitergeleitet

Store and Forward Switch



Cut- through Switch

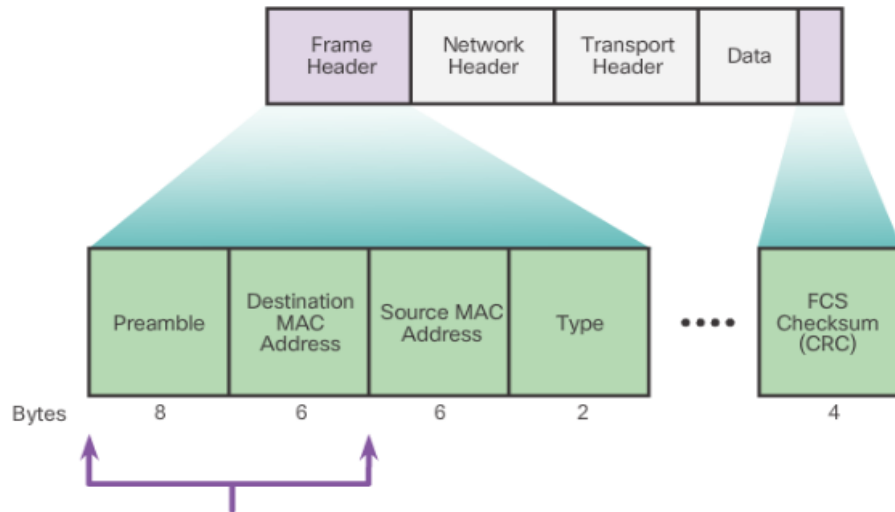
- Bei einem cut- through Switch wird nur die Destination MAC Adresse kontrolliert.
- Der Switch leitet sofort jedes Bit weiter.
- Das Frame wird ohne Kontrolle weitergeleitet.
- Die Source MAC Adresse wird nachwievor gelernt.
- Die Kontrolle, ob das Frame nicht korrupt ist, wird den Clients überlassen.

Cut- through Switch



Cut- through Switch

Cut-Through Switching



Frames can begin to be forwarded as soon as the Destination MAC is received.

Broadcast Domäne

- Wenn die Destination MAC Adresse alles Einsen beinhaltet, (FF:FF:FF:FF:FF:FF), dann nennt man es ein Broadcast Paket auf Layer 2.
- Dieses Paket wird an alle Geräte weitergeleitet, die an einem Switch hängen.
- Unterschied Broadcast, Multicast:
 - Alle beide werden an alle Geräte (z.B. PCs) verschickt
 - Die NIC des angeschlossenen Geräts (z.B. PC) löst bei einem Broadcast immer einen Interrupt aus, bei einem Multicast nur dann, wenn die NIC teil der Multicast-Gruppe ist.

Broadcast Domäne



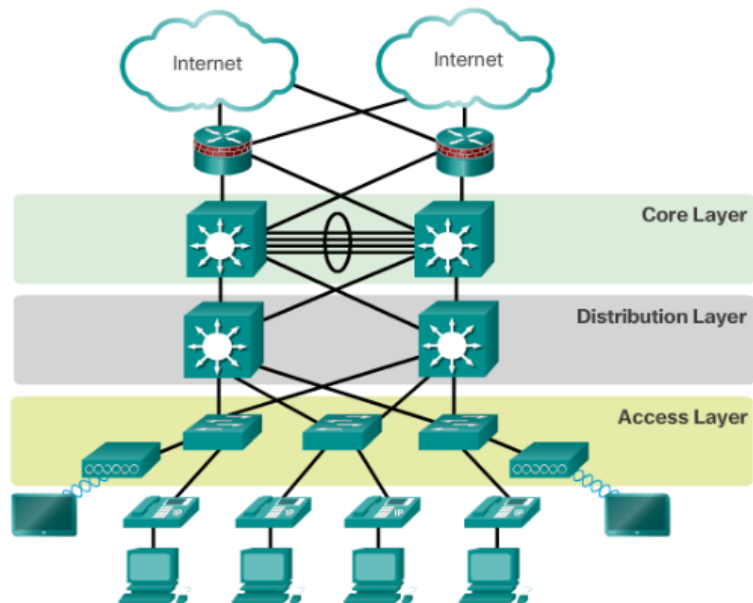
VLAN

- todo

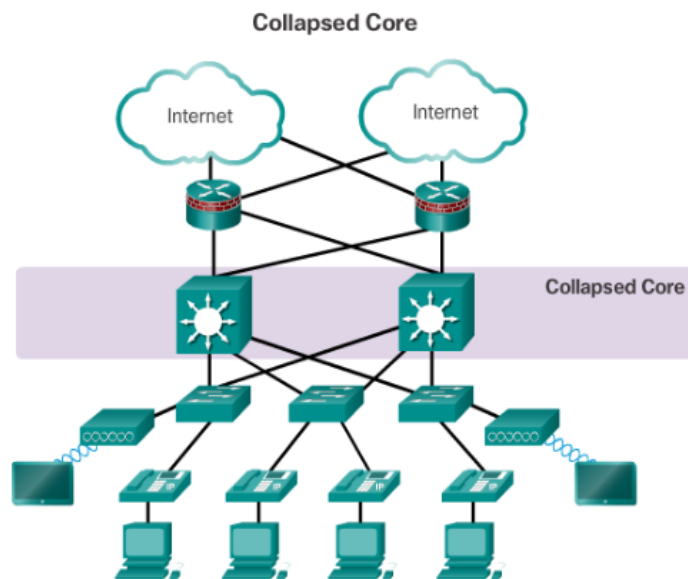
Chapter 0	Course Introduction
Chapter 1	Introduction to Switched Networks
Chapter 2	Basic Switching Concepts and Configuration
Chapter 3	VLANs
Chapter 4	Routing Concepts
Chapter 5	Inter-VLAN Routing

Hirarchisches Netzwerk Design

Hierarchical Design Model



Hirarchisches Netzwerk Design



Spanning Tree

- Durch ein hierarchisches Netzwerkdesign entstehen auch Schleifen.
 - Wir haben gesehen, dass diese fatale Folgen für ein Netzwerk haben können
 - Broadcast storm
 - Multiple Unicast Frames
 - Instable MAC Tables
- Durch das Spanning Tree Protokoll werden diese Probleme eliminiert und es entstehen redundante Wege.
 - Sehr gut für die Ausfallsicherheit!!!

FHRP

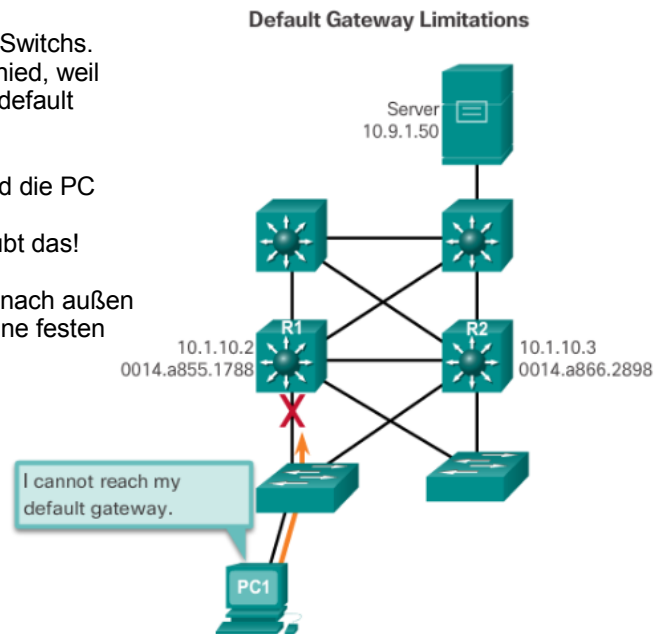
- First Hop Redundancy Protokoll
 - Das Problem mit dem default Gateway.
 - Ein Gerät hat nur einen default Gateway.
 - Deshalb gibt es einen "single point of failure"
 - Fällt der default Gateway aus, ist das lokale Netz von der Außenwelt abgeschnitten.
- Man bräuchte also einen zweiten Gateway, der im Falle eines Ausfalls die Pakete weiterleitet.

FHRP

Alle Router im Bild sind Layer 2 Switchs.
Das macht aber keinen Unterschied, weil normalerweise in L2 Switch der default Gateway für ein VLAN ist.

Wenn der Router R1 ausfällt sind die PC von außen noch erreichbar.
Das Routing Protokoll erlaubt das!

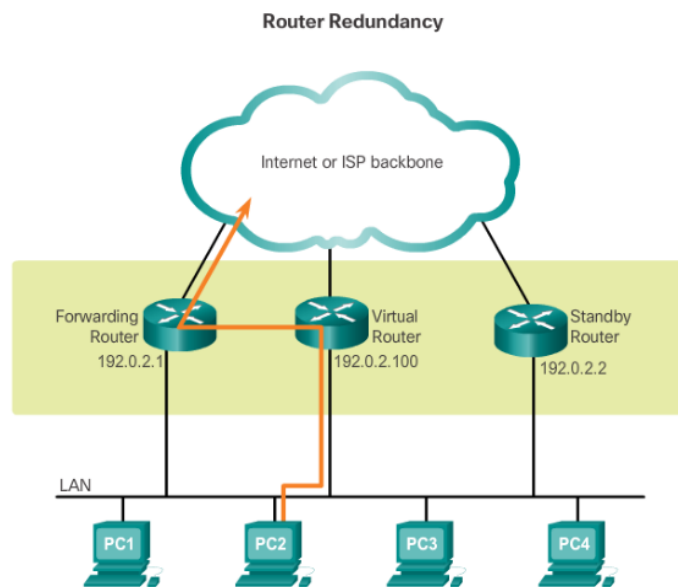
Die PC können aber nicht mehr nach außen kommunizieren, weil jeder PC eine festen default Gateway eingestellt hat.



Router Redundanz

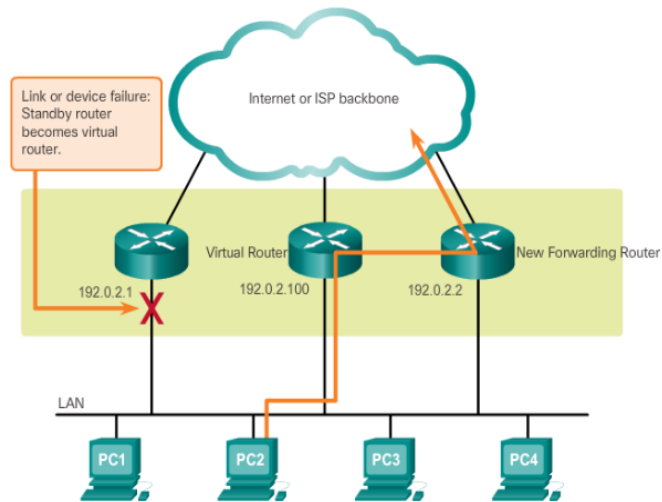
- Man konfiguriert mehrere Router als eine Gruppe und definiert einen virtuellen Router.
- Der virtuelle Router leitet die Pakete nicht direkt in Internet weiter, sondern an einen Forward Router.
- Fällt der Forward Router aus, gibt es eine Standby Router, der einspringt.
- Normalerweise gibt es für eine Gruppe eine Virtuellen Gateway ID und Virtuelle Gateway MAC

Router Redundanz



Router Redundanz

Steps for Router Failover



Router Redundanz

- Wenn der Forward Router ausfällt, macht das Protokoll folgendes:
 - Der Standby Router erhält keine Hello Pakete vom Forward Router mehr.
 - Der Standby Router übernimmt die Rolle des Forward Router
 - Der neue Forward Router hat dieselbe virtuelle MAC und IP Adresse des "alten" Forward Router.
 - Die PCs merken somit den Ausfall nicht, da sie als default Gateway die virtuelle Gateway IP eingestellt haben.

Protokolle redundante Router

- Hot Standby Router Protocol (HSRP)
 - Cisco proprietär
- Virtual Router Redundancy Protocol version 2 (VRRPv2)
 - Offenes Protokoll
- Gateway Load Balancing Protocol (GLBP)
 - Cisco proprietär
 - Erlaubt zudem Load Balancing

Hot Standby Router Protocol

First-Hop Router Redundancy Options



Hot Standby Router Protocol

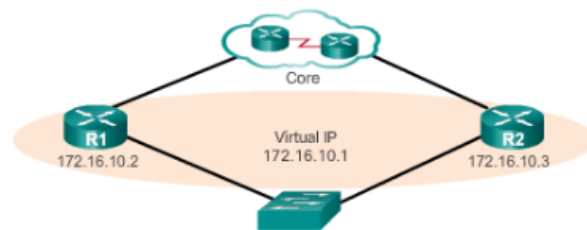
- Eigenschaften Active Router
 - Antwortet auf ein ARP Paket mit der virtuellen MAC Adresse.
 - Leitet alle erhaltenen Pakete weiter ins Internet
 - Sendet in regelmäßigen Abständen Hello Pakete an der Standby Router
 - Kennt die virtuelle IP Adresse

Hot Standby Router Protocol

```
Router# show standby
Ethernet0/1 - Group 1
  State is Active
    2 state changes, last state change 00:30:59
  Virtual IP address is 10.1.0.20
    Secondary virtual IP address 10.1.0.21
    Active virtual MAC address is 0004.4d82.7981
    Local virtual MAC address is 0004.4d82.7981 (bia)
    Hello time 4 sec, hold time 12 sec
    Next hello sent in 1.412 secs
    Gratuitous ARP 14 sent, next in 7.412 secs
    Preemption enabled, min delay 50 sec, sync delay 40 sec
    Active router is local
  Standby router is 10.1.0.6, priority 75 (expires in 9.184 sec)
  Priority 95 (configured 120)
    Tracking 2 objects, 0 up
      Down Interface Ethernet0/2, pri 15
      Down Interface Ethernet0/3
  Group name is "HSRP1" (cfgd)
Follow by groups:
Et1/0.3 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.666)
Et1/0.4 Grp 2 Active 10.0.0.254 0000.0c07.ac02 refresh 30 secs
(next 19.491)
  Group name is "HSRP1", advertisement interval is 34 sec
```

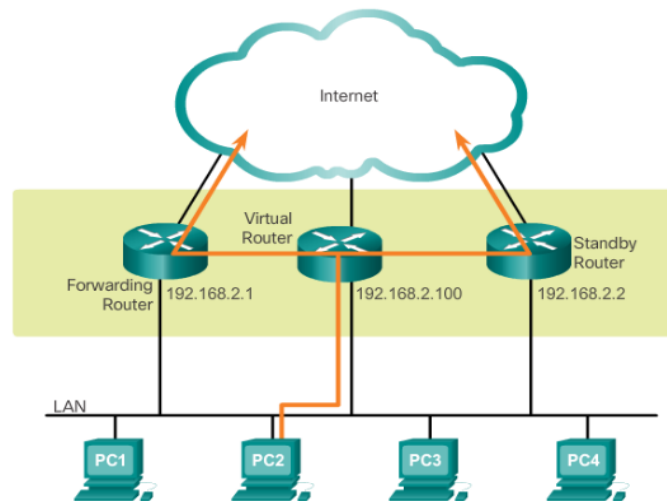
Hot Standby Router Protocol

- Was macht der standby Router?
 - Hört auf die periodischen Hello Pakete
 - Übernimmt die aktive Rolle, wenn er keine Hello Pakete bekommt



Gateway Load Balancing Protocol

Gateway Load Balancing Protocol



Übung

- Mache die Übung

