Einführung in Switching

Kapitelaufbau

1.1 Konvergierte Netze

1.2 Hierarchischer Netzansatz

1.3 Switch Basis Konfiguration

1.4 Sicherheitsfunktionen

1.1 Konvergierte Netze

Lernziele:

- Sie kennen die Ansprüche, die man heute an konvergierte Netze im Switching Umfeld stellt
- Sie verstehen den Ansatz hierarchischer Netze.
- Sie wissen, wie ein Switch aufstartet
- Sie kennen die möglichen Einstellungen der Switch-Ports
- Sie können einen sicheren Remote-Zugang zum Switch erstellen
- Sie kennen die wichtigsten Angriffe auf Switch
- Sie können die grundlegenden Sicherheitseinstellungen für die Benutzerseite auf einem Switch vornehmen

1.1 Konvergierte Netze

Fragen:

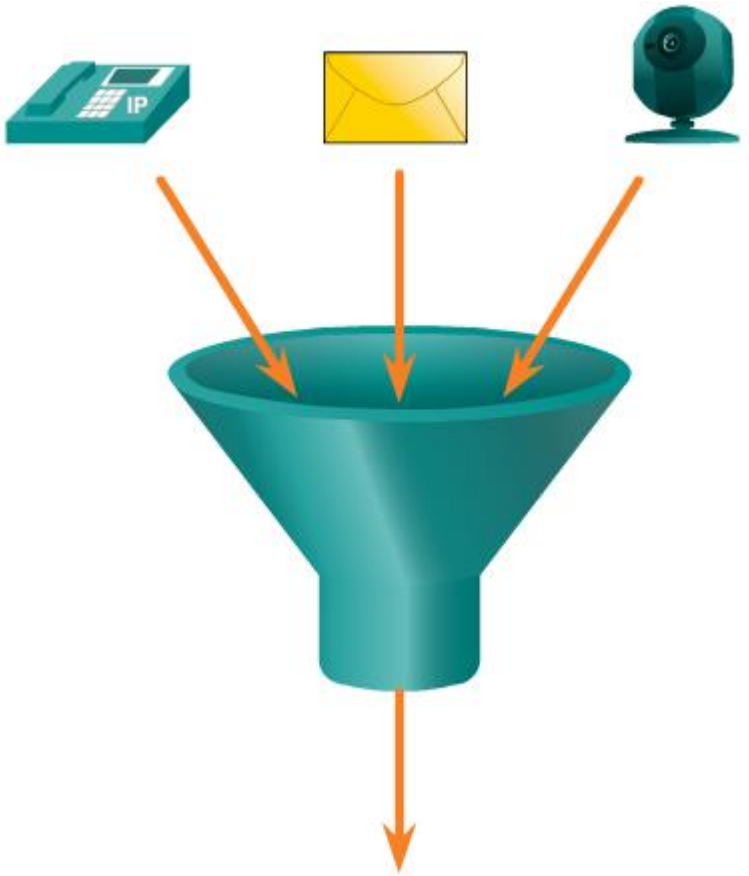
1. Was erwartet man von einem Firmen-LAN heute?
   Welche Dienste soll es unterstützen?

2. Welche Anforderungen ergeben sich daraus?

3. Wie muss man ein LAN entwerfen, damit es diese Anforderungen erfüllen kann?

1.1 Konvergierte Netze

Verschiedene Arten von Verkehr:

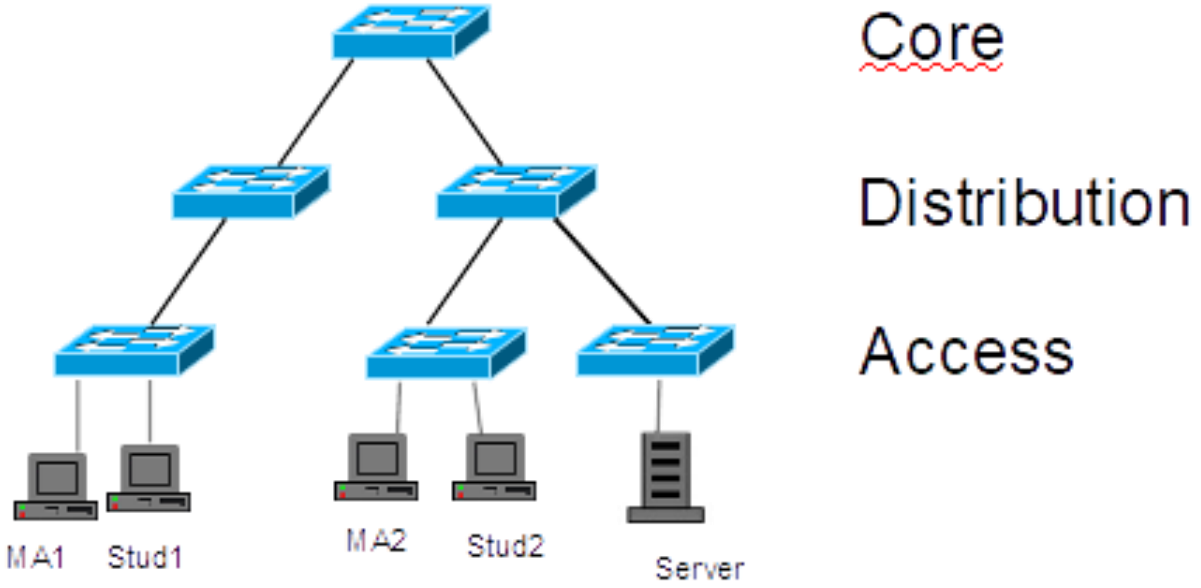


1.1 Konvergierte Netze

Anforderungen an ein LAN:

1.2 Hierarchischer Netzansatz

Ebenen in LANs



Switch werden nur ‘vertikal’ untereinander verbunden (d.h. von einer Ebene in die Nachbarebene). Horizontale Verbindungen sind nur im Core erlaubt.

(In dieser Zeichnung wurde absichtlich auf Redundanz verzichtet)

1.2 Hierarchischer Netzansatz

Vorteile des hierarchischen Netzansatzes:

- Skalierbarkeit
- Hoher Durchsatz
- Sicherheit
- Einfache Wartbarkeit
- Beschränkung der betroffenen Clients im Fehlerfall

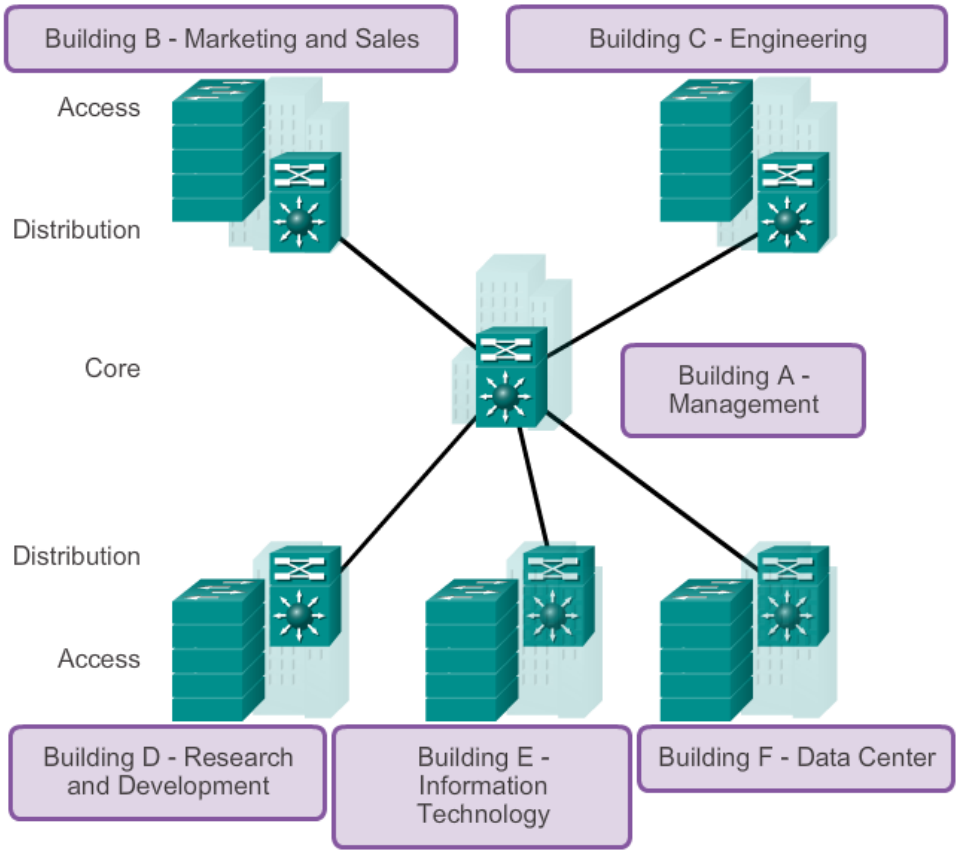
Nachteile:

- ?

1.2 Hierarchischer Netzansatz

Bsp:

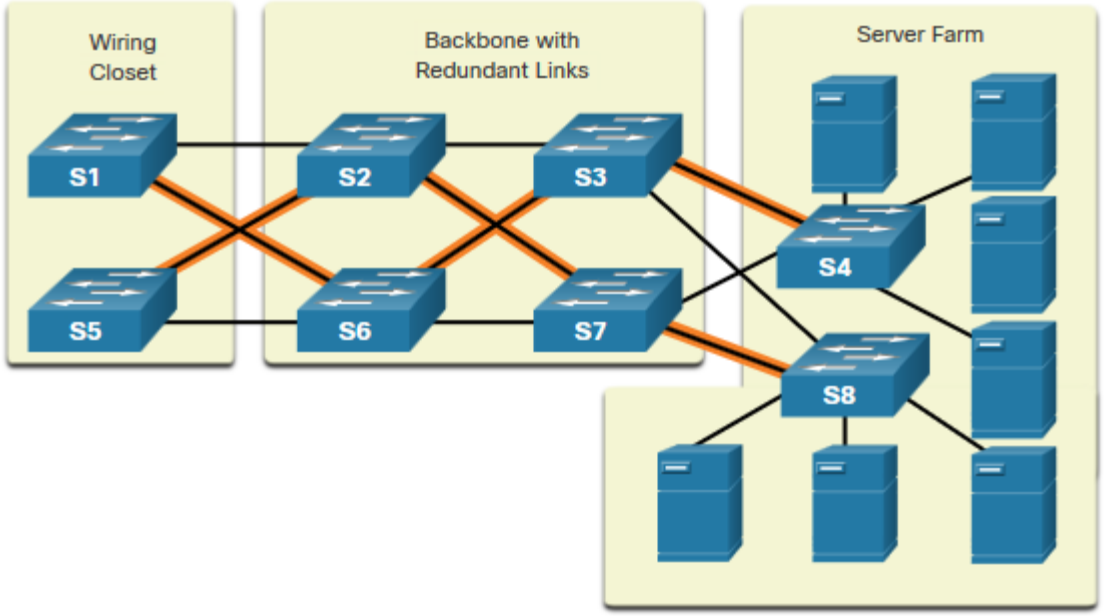
Verteilung der verschiedenen Switch auf die Gebäude



1.2 Hierarchischer Netzansatz

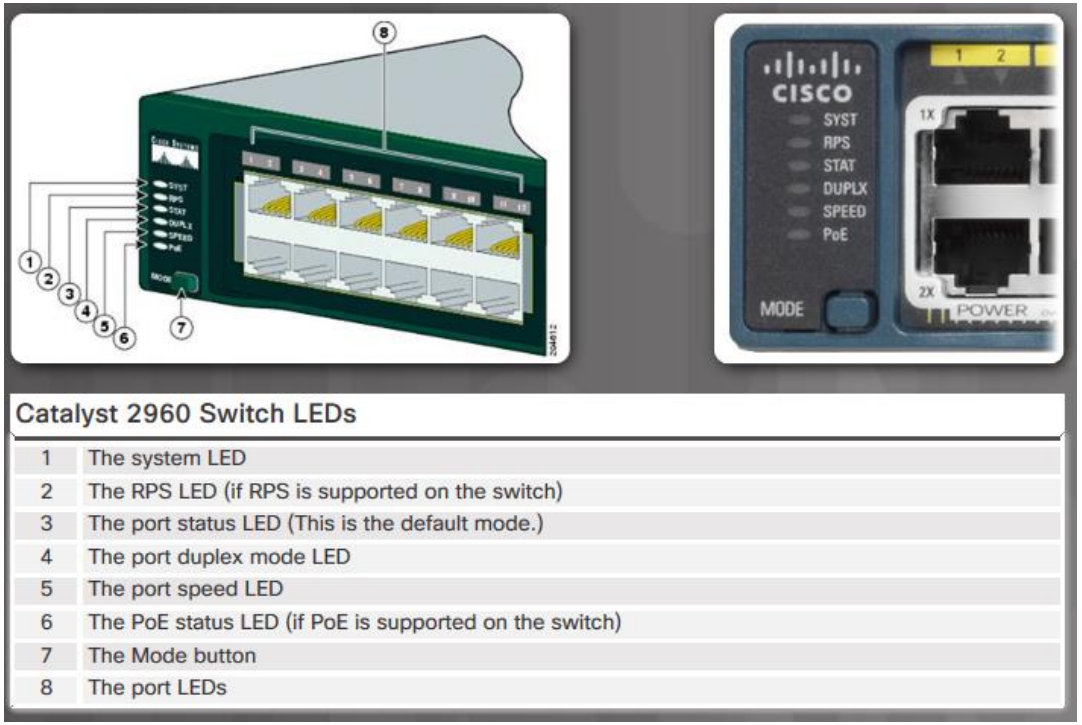
Ansatz für hohe Verfügbarkeit:

- Jeder Switch wird gegen den Core doppelt angebunden



1.3 Switch Basis Konfiguration

Anzeigen auf einem Switch



Catalyst 2960 Switch LEDs	
1	The system LED
2	The RPS LED (if RPS is supported on the switch)
3	The port status LED (This is the default mode.)
4	The port duplex mode LED
5	The port speed LED
6	The PoE status LED (if PoE is supported on the switch)
7	The Mode button
8	The port LEDs

Im Fehlerfall kontrollieren Sie zuerst die LEDs. Ist ein Port ‚up‘?

1.3 Switch Basis Konfiguration

Remote Management von Switches mit Telnet

Notwendige Konfigurationen:

```
AS-1(conf)#enable password class
AS-1(conf)# interface Vlan1
AS-1(conf-if)#ip address 192.168.5.22 255.255.255.0
AS-1(conf-if)#no shutdown
AS-1(conf-if)#exit
AS-1(conf)# ip default-gateway 192.168.5.1
AS-1(conf)# line vty 0 4
AS-1(conf-line)# password cisco
AS-1(conf-line)#^z
AS-1#
```

1.3 Switch Basis Konfiguration

Freiheitsgrade auf den Switch Ports:

- Duplex mode
- Datenrate

```
Switch(config)#interface f0/1
Switch(config-if)#duplex full
Switch(config-if)#speed 100
```

- MDIX Autoconfiguration

```
Switch(config)#interface f0/1
Switch(config-if)#duplex auto
Switch(config-if)#speed auto
Switch(config-if)#mdix auto
```

1.3 Switch Basis Konfiguration

Statusabfragen

```
S1#show interfaces [if-id]
S1#show startup-config
S1#show flash
S1#show version
S1#show history
S1#show ip interface brief
S1#show mac-address-table
```

1.4 Sicherheitsfunktionen

Frage:

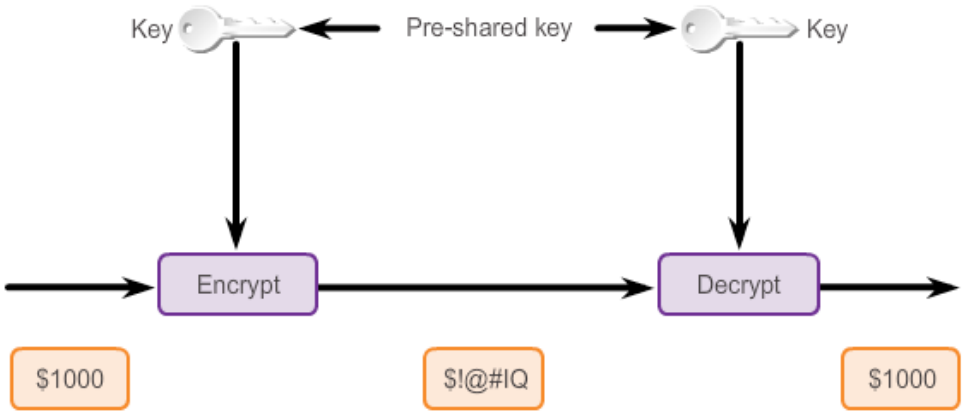
Welche Angriffe auf ein LAN können Sie sich vorstellen?

Kann sie man unterbinden?

1.4 Sicherheitsfunktionen

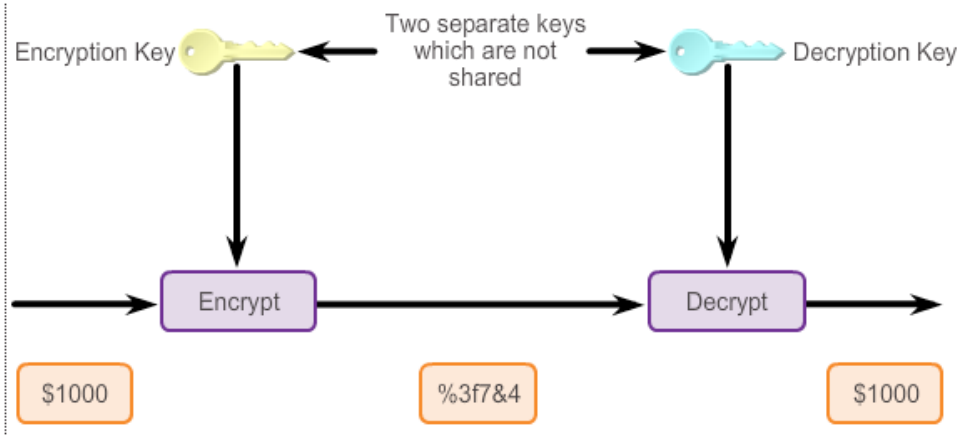
Symmetrische Verschlüsselung:

- An beiden Enden wird der gleiche Schlüssel verwendet
- Kurze Schlüssel, effizient
- Verschlüsselung von Daten



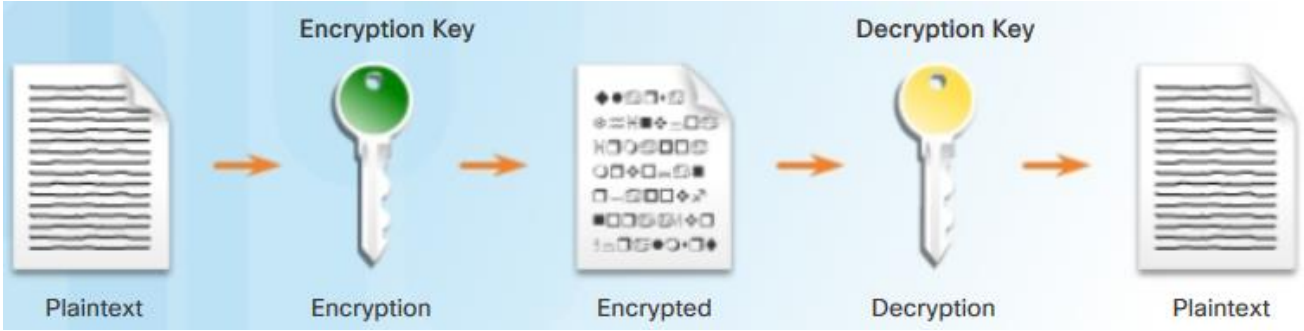
Asymmetrische Verschlüsselung

- Längere Schlüssel, aufwändige Berechnungen
- Nur kurze Nachrichten
- Authentisierung des Gegenübers



1.4 Sicherheitsfunktionen

- Asymmetrische Algorithmen (oder Public Key Verfahren) verwenden zwei verschiedene zueinander passende Schlüssel:



- Wird die Nachricht mit dem ersten Schlüssel (grün) verschlüsselt, so kann sie mit dem zweiten Schlüssel (gelb) - und nur mit diesem - entschlüsselt werden.
- Das Umgekehrte gilt auch: Wird eine Nachricht mit dem zweiten Schlüssel (gelb) verschlüsselt, so kann sie der Besitzer des ersten Schlüssels (grün) entschlüsseln. Und nur er kann die Nachricht entschlüsseln.
- Asymmetrische Verfahren werden zur Authentisierung des Gegenübers benützt, wenn zuvor kein gemeinsames Geheimnis ausgetauscht wurde.

1.4 Sicherheitsfunktionen

Konfiguration des Zugangs per SSH

1.Credentials für Benützer konfigurieren

```
S1(config)#username admin1 password Passw0rd
```

2.Generierung eines symmetrischen Schlüsselpaares

```
S1(config)# ip domain-name beispiel.ch
S1(config)#crypto key generate rsa
```

//Schlüssellänge mindestens 1024

1.SSH konfigurieren und verlangen

```
S1(config)#line vty 0 4
S1(config-line)# transport input ssh
S1(config-line)#login local
S1(config)#ip ssh version 2
```

1.4 Sicherheitsfunktionen

Switch und IPv6 Adressen

Kann man einem Switch eine IPv6 Adresse konfigurieren?

Per Default geht es nicht. Der IPv6 stack muss zuerst aktiviert werden:

```
Switch#configure terminal
Switch(conf)#sdm prefer dual-ipv4-and-ipv6 default
Switch(conf)#exit
Switch#reload
```

Man geht davon aus, dass Switch gewöhnlich per IPv4 gewartet werden.

1.4 Sicherheitsfunktionen

Angriffe auf Switch: MAC-flooding

- Kennen Sie den Angriff?
- Erklären Sie, wie der Angriff funktioniert.
- In welche Kategorie gehört dieser Angriff?

1.4 Sicherheitsfunktionen

Bekämpfung von MAC-Flooding

```
S1(config-if)#switchport mode access
S1(config-if)#switchport port-security
```

Statische Zulassung von einzelnen MAC-Adressen:

```
s1(config)#switchport port-security mac-address AB.CD.EF
```

Dynamisch:

```
S1(config-if)#switchport port-security maximum n
S1(config-if)#switchport port-security mac-address sticky
```

‘Sticky’ bedeutet, dass die MAC-Adresse für diesen Port gespeichert wird.

1.4 Sicherheitsfunktionen

Wie soll mit Zuwiederhandlung umgegangen werden?

Es gibt drei Arten darauf zu reagieren: Restrict, Protect, Shutdown

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	Yes	No	Yes	Yes

Bsp:

```
S1(config-if)#switchport port-security violation
protect
```