Switch-Grundkonfiguration

Ein Switch ist „Out-of-the-Box“ funktionsfähig. Um in einer Produktivumgebung sinnvoll und sicher eingesetzt zu warden, benötigt ein Switch jedoch eine passende Grundkonfiguration. Die folgenden Befehle sind Grundbefehle, müssen aber je nach Szenario angepasst werden.

Allgemeine globale Konfiguration:

Hostnamen auf SW1 konfigurieren:

```
Switch(config)#hostname SW1
```

Domänennamen-Suche deaktivieren:

```
SW1(config)#no ip domain-lookup
```

Enable-Passwort auf Pa$$w0rd setzen:

```
SW1(config)#enable secret Pa$$w0rd
```

Passwort-Verschlüsselung aktivieren:

```
SW1(config)#service password-encryption
```

Domänennamen auf atracon.local setzen (für SSH notwendig):

```
SW1(config)#ip domain-name atracon.local
```

SSH-Schlüsselpaar erstellen (Schlüssellänge mind. 1024 Bit für SSHv2!):

```
SW1(config)#crypto key generate rsa
```

Benutzer Asterix [Optional: mit Admin-Privilegien] erstellen:

```
SW1(config)#username asterix [privilege 15] secret Pa$$w0rd
```

Konsolen-, Telnet und SSH-Zugriff konfigurieren:

Variante 1: Nur Passwortabfrage:

```
SW1(config)#line con 0
SW1(config-line)#password Pa$$w0rd
SW1(config-line)#login
```

Variante 2: Lokale Benutzerdatenbank abfragen:

```
SW1(config)#line con 0
SW1(config-line)#login local
```

Störung der Logmeldungen “abmildern”:

```
SW1(config-line)#logging synchronous
```

In Laborumgebungen(!) Logout vermeiden:

```
SW1(config-line)#exec-timeout 0
```

Dieselbe Konfiguration gilt auf den Terminal-Lines vty 0-4 bzw. 0-15. Zusätzlich muss hier ggf. der Zugriff für Telnet deaktiviert werden:

```
SW1(config-line)#transput input ssh
```

Management-IP-Konfiguration erstellen (mit Beispiel-IP-Adressen):

```
SW1(config)#ip default-gateway 192.168.1.254
SW1(config)#int vlan1
SW1(config-if)#ip address 192.168.1.1 255.255.255.0
SW1(config-if)#no shutdown
```

Grundkonfiguration für Switchports

Portfast-Default aktivieren:

```
SW1(config)#spanning-tree portfast default
```

Ports, an denen Endgeräte angeschlossen sind, als Access-Ports definieren:

```
SW1(config)#int range fa0/1 – 20
SW1(config-range-if)#switchport mode access
```

BPDU-Guard oder -Filter auf Access-Ports aktivieren, um Rogue-Switches zu verhindern:

```
SW1(config-range-if)#spanning-tree bpduguard|bpdufilter enable
```

Nicht genutzte Interfaces deaktivieren:

```
SW1(config-if)#shutdown
```

Trunkports ohne DTP (wenn Auswahl vorhanden ggf. auf 802.1Q) festlegen:

```
SW1(config)#int fa0/24
SW1(config-if)#switchport trunk encapsulation dot1q
SW1(config-if)#switchport mode trunk
SW1(config-if)#switchport nonegotiate
```

Syslog konfigurieren:

Protokollierung in den Geräte-internen Puffer (50.000 Bytes, Severity: Notification):

```
SW1(config)#logging on
SW1(config)#logging buffered 50000 notification
```

Betrachten des lokalen Log-Puffers:

```
SW1(config)#show log
```

Protokollierung auf einen Syslog-Server mit der IP 192.168.1.1, Severity: Informational:

```
SW1(config)#logging on
SW1(config)#logging trap informational
SW1(config)#logging 192.168.1.1
```

Beide Varianten können parallel genutzt werden!