ACLs-Dossier

4.1 Zweck von #ACL s

- **Was ist eine ACL?**
  - Eine Access Control List (ACL) ist eine Reihe von #OS-Befehlen, die verwendet werden, um Datenpakete basierend auf Informationen im Paketheader zu filtern. ACLs bestehen aus einer sequentiellen Liste von "Permit" oder "Deny"-Anweisungen, die als Access Control Entries (#ACE s) bezeichnet werden. Wenn eine ACL auf eine Schnittstelle angewendet wird, entscheidet der Router, ob ein Paket weitergeleitet oder verworfen wird.
- **Paketfilterung**
  - Die #Paketfilterung steuert den Zugriff auf ein Netzwerk, indem sie inbound und outbound Pakete analysiert und entscheidet, ob sie weitergeleitet oder verworfen werden. Die Filterung kann auf Layer 3 und Layer 4 erfolgen.
  - Cisco-Router unterstützen zwei Arten von ACLs:
    - **Standard-ACLs**: Filtern nur auf Layer 3 basierend auf der Quell-IP-Adresse.
    - **Extended ACLs**: Filtern auf Layer 3 und 4 basierend auf Quell- und Ziel-IP-Adresse, TCP/UDP-Ports und Protokollen.
- **Funktionsweise von ACLs**
  - ACLs analysieren Pakete, die durch eingehende (inbound) oder ausgehende (outbound) Schnittstellen des Routers geleitet werden. Eingehende ACLs filtern den Verkehr vor der Weiterleitung, während ausgehende ACLs den Verkehr nach der Weiterleitung filtern.

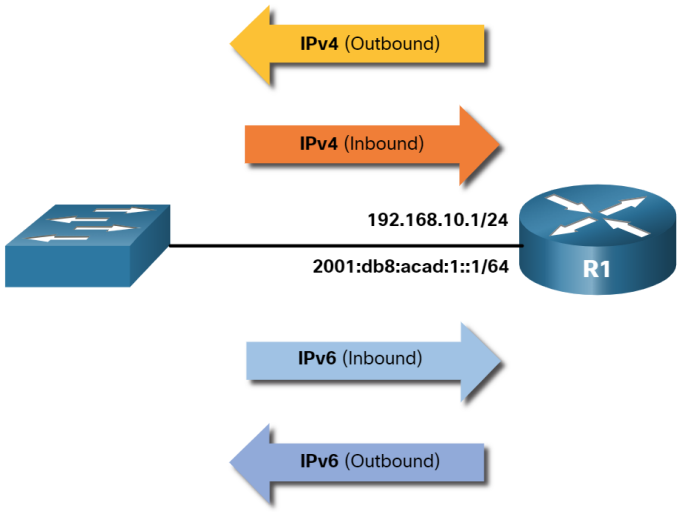
  - Alle ACLs haben eine **"deny all"**-Anweisung am Ende, was bedeutet, dass jeder Datenverkehr, der nicht explizit zugelassen wird, standardmäßig abgelehnt wird. Auch genannt **"implictit deny"**.

4.2 Wildcard-Masken in ACLs

- **Wildcard-Masken Überblick**
  - #Wildcard-Masken geben an, welche Teile einer IP-Adresse für die Filterung übereinstimmen müssen. Also genau das Gegenteil wie eine Subnetzmaske
- **Wildcard-Masken Berechnung**
  - Um eine Wildcard-Maske zu berechnen, subtrahiert man die Subnetzmaske von 255.255.255.255. Zum Beispiel ergibt das für ein Netzwerk 192.168.3.0/24 die Wildcard-Maske 0.0.0.255.
- **Wildcard-Masken-Schlüsselwörter**
  - **host**: Steht für eine bestimmte IP-Adresse
  - **any**: Erlaubt alle IP-Adressen

4.3 Erstellung von ACLs

- **Anzahl der ACLs pro Schnittstelle**
  - Eine Router-Schnittstelle kann bis zu 4 ACLs haben: eine eingehende und eine ausgehende für sowohl IPv4 als auch IPv6.



- **Best Practices für ACLs**
  - Zu den besten Praktiken gehören das Erstellen von ACLs, bevor sie angewendet werden, das Testen der ACLs in einer sicheren Umgebung und die Dokumentation der ACLs zur späteren Nachverfolgung.

4.4 Arten von IPv4-ACLs

- **Standard- und erweiterte ACLs**
  - **Standard-ACLs**: Filtern den Datenverkehr basierend auf der Quell-IP-Adresse.
  - **Extended ACLs**: Filtern den Datenverkehr basierend auf der Quell- und Ziel-IP-Adresse, sowie auf Protokoll- und Portnummern.
- **Nummerierte und benannte ACLs**
  - Nummerierte ACLs haben einen bestimmten Zahlenbereich (1-99 für Standard, 100-199 für erweiterte ACLs). Benannte ACLs werden bevorzugt, da sie leichter zu verwalten und zu ändern sind.
- **Platzierung von ACLs**
  - **Standard-ACLs**: Sollten so nah wie möglich am Ziel platziert werden.
  - **Extended ACLs**: Sollten so nah wie möglich an der Quelle platziert werden, um unerwünschten Datenverkehr frühzeitig zu blockieren.