Vorgehensweise:

1. Grundkonfiguration
2. Serielle Konsole
3. SSH
4. VLAN
5. Hardening Guide kontrollieren / anpassen
6. ACL
7. Services (DHCP/Radius etc.)

Grundkonfig

device(config)# hostname <name>	Vergibt dem Gerät einen Namen
device(config)# enable secret <password>	Setzen des verschlüsselten Passwortes für den privilegierten Modus
device(config)# service password-encryption	Verschlüsselt alle Passwörter
(config)# username <name> [privilege 0-15] {secret|password} <password>	Legt einen Benutzer mit Passwort an
*..(config)#*no password	Kein anonymer Login
device(config-line)# login local	Aktiviert die angelegten Benutzer mit Passwort

Serielle Console absichern

Schnittstelle auswählen:	*..(config)#*line console 0
Passwort vergeben:	*..(config-line)#* password <password>
Kein anonymer Login:	*(config-line)#*login local
Konsole schließen:	*(config-line)#*exec timout <minuten> <sekunden>
Synchrone Protokollierung	*..(config-line)#* logging synchronous

Hardening Guide

Switch(config) # vtp mode transparent	VTP vermeiden
Unused VLAN:	VLAN 1 vermeiden
Switch(config)# vlan <id>	stattdessen "UNUSED VLAN" erstellen
Switch(config) #int range fa[0/X-Y]	Ports auswählen

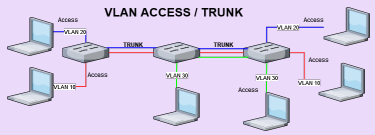
Hardening Guide (cont)

Switch(config-if)# switchport mode access	Switchport mode access
switch(config-if)# switchport access vlan <unusedVlan>	Ports in Vlan
VTY beschränken:	
device(config-line)# transport input none	keine Verbindung zulassen
exec-timeout <minuten> <sekunden>	
Allgemein:	
switchport nonegotiate	DTP
ACLs anpassen!	siehe ACL
ggfs. Inter-Vlan Routing	siehe Inter-Vlan Routing

VLAN

switch(config)# vlan <vlan-id>	Vlan anlegen
switch(config-vlan)# name <name>	Vergibt dem VLAN einen Namen
switch(config-if)# switchport mode {access|trunk	Access oder Trunk Mode
switch(config-if)# switchport access vlan <vlan-id>	Access Port (statisch) anlegen
switch(config-if)# switchport trunk allowed vlan <vlan-ids>	Trunk festlegen (VLANS)
switch# show vlan [brief]	! Gemäß Show Commands

VLAN Trunk & Access



Inter VLAN Routing

Router(config)# int fastEthernet 0/0.{VLAN}	Sub-Interface anlegen (Schnittstelle Router)
Router(config-subif)# encapsulation dot1Q {VLAN}	
Router(config-subif)# ip address <ip>.254 <SNM>	IP Adresse vergeben
Für jedes VLAN das Routen durchführen	
Switch# show vlan brief	Siehe Show Command

Wildcardmask

Invertierte Subnetzsmaske	
255.255.255.0 | /24	0.0.0.255
255.255.255.128 | 25	0.0.0.127

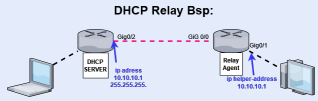
SSH

! Hostname vergebn	
device(config)# ip domain-name <dns-suffix>	Legt ein DNS-Suffix für das Gerät fest
!Benutzer muss angelegt sein	
device(config)# crypto key generate rsa	Erzegut Schlüssel mit RSA-Standard
device(config)# ip ssh version {2}	Legt die Version vom SSH Protokoll fest
device(config)# line vty 0 15	Wechselt auf die virtuellen Schnittstellen zum Fernwarten
device(config-line)# login local	Aktiviert die angelegten Benutzer mit Passwort
device(config-line)# transport input ssh	Zugriff über vty nur über SSH möglich
PC> ssh -l <username> <ip>	Aufbau einer SSH-Verbindung über die Konsole (nur in Packet Tracer)

DHCP

device(config)# ip dhcp pool <name>	DHCP Pool anlegen
device(config-dhcp)# network <net-id> <snm>	Netz ID dem Pool zuweisen
device(config-dhcp)# default-router <ip>	Gateway festlegen
device(config-dhcp)# dns-server <ip>	DNS Server festlegen
device(config-dhcp)# domain-name <domain>	DNS Suffix festlegen
router(dhcp-config)# lease {days hours minute|infinite}	Lease festlegen
device(config)# ip dhcp excluded--address <start-ip> <end-ip	IP-Adressbereiche die ausgeschlossen werden sollen
device# show ip dhcp lease	! Gemäß Show Commands
device#show ip <pool|binding|conflict>	! Gemäß Show Commands

DHCP RelayAgent



router(config-if)# ip helper-address <IP DHCP-SERVER>

Radius

! SSH einrichten	siehe SSH
!Benutzer muss angelegt sein	siehe Grundconfig
*Router(config)#*aaa new-model	Aktiveren des Dienstes
*Router(config)#*radius-server host {ip-address} auth-port {port-number}[retransmit retries] key {string} [alias {hostname | ip-address}]	Radius Server angeben inkl. Port
*Router(config)#*aaa authentication login default group radius local	Authentifizierungstyp festlegen (login)

Radius (cont)

Router(config)# aaa authentication enable default group radius local	Authentifizierungstyp festlegen (EnableModus)
Router(config)# line vty 0 15	VTY auswählen
Router(config-line)# login authentication default	Login mit Radius über VTY

SERVER (Dienst: AAA Konfigurieren)

Basic

device# copy <source> <destination>	Kopieren von Quelle nach Ziel

Show Commands

device# show running-config	Zeigt die aktuelle Konfiguration an
device# show startup-config	Zeigt die Start-Konfiguration an
L3switch# show ip interface brief	Zeigt den Status der physikalischen oder virtuellen Schnittstellen
device> show interfaces	Übersicht über Anzahl und Zustand der Schnittstellen
device# show ip interface [brief]	(Kurz-)Übersicht über die globalen Einstellungen der "IP-Schnittstellen"
device# show ip dhcp lease	Zeigt die DHCP Address Leases an
switch# show vlan [brief]	Übersicht über die VLAN-Konfiguration
switch# show interfaces trunk	Übersicht und Informationen über konfigurierte Trunks
device# show ip route	Zeigt die Routing-Tabelle an

Show Commands (cont)

device# show ip dhcp lease	Zeigt die DHCP Address Leases an
device# show access-list	Übersicht über ACL´s

ACL

Router(config)# ip access-list <standard | extended> <name>	Named-ACL erstellen
Router(config-ext-acl)# <permit | deny > <protocol> <source> <wildcardmask> <destination> <wildcardmask>	Extended--Named-ACL erstellen
Router(interface)# ip access-group <name> <in | out>	ACL auf Interface einbinden
Router()# show access-lest	ACL überprüfen