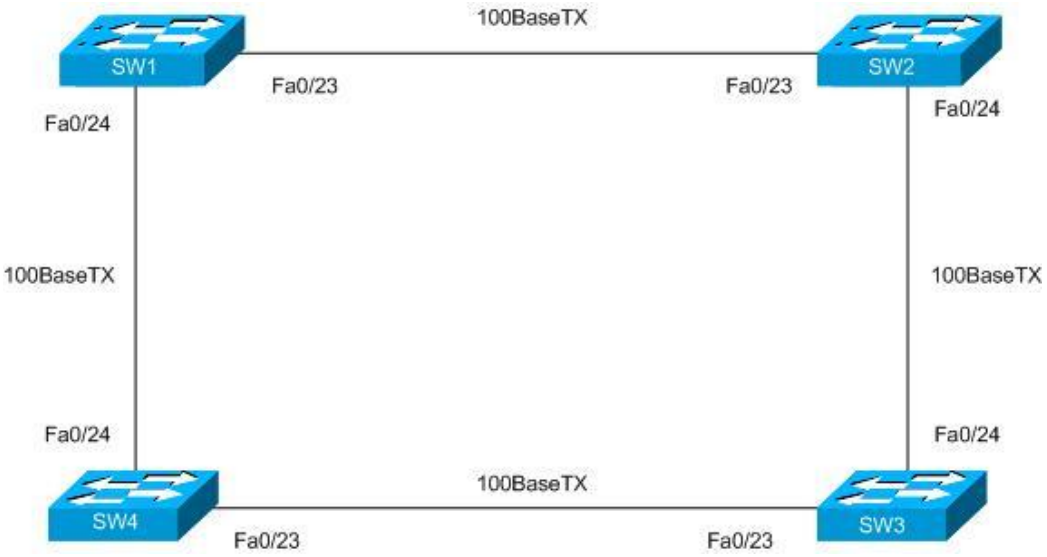
Komplettaufgabe Switching

Diese Komplettaufgabe basiert auf 4 Layer-2-Switches, die im Kreis zusammengeschlossen sind:



Die Teilnehmer verteilen sich gleichmäßig auf alle Switches und führen die Aufgaben als Team aus. Die folgenden Aufgaben umfassen die folgenden Themengebiete:

- Password-Recovery
- Switch-Grundkonfiguration
- VLAN-Konfiguration und Portkonfiguration
- Trunks konfigurieren
- VTP-Konfiguration
- Spanning-Tree-Konfiguration
- Port-Security

Wenn keine Angaben gemacht werden, können Sie eigenständige Entscheidungen treffen, ggf. müssen Sie sich mit anderen Teilnehmern abstimmen.
Hinweis: Patchen Sie den Admin-PC (Laptop) an fa0/1.

Password Recovery

Szenario: Die Switches sollen mit ihrer vorhandenen Konfiguration in einem Netzwerk eingesetzt werden. Leider sind die Zugangsdaten verloren gegangen, so dass zunächst ein Password Recovery durchgeführt werden muss:

1. Starten Sie den Switch im Recovery-Modus.
2. Führen Sie die notwendigen Schritte durch, um den Switch so zu starten, dass er beim Neustart die gespeicherte Konfiguration umgeht und den Initial Configuration Dialog anzeigt.
3. Beenden Sie den Initial Configuration Dialog mit „no“ und begeben Sie sich in den Privileged Mode.
4. Laden Sie die vorhandene, gespeicherte Konfiguration in die Running-Config.
5. Passen Sie das Passwort für den Privileged Mode an und setzen Sie das Passwort auf „cisco“.

6. Erstellen Sie einen Benutzer „asterix“ mit dem Passwort „cisco“. Nutzen Sie zum Festlegen des Passwortes die sichere Variante mit dem Schlüsselwort „secret“.
7. Stellen Sie sicher, dass sowohl der Konsolenzugriff als auch der Zugriff über die VTY-Lines 0 bis 15 über die Abfrage der lokal gespeicherten Benutzerkennungen gesichert ist.
8. Testen Sie den Zugriff auf die Konsole, in dem Sie sich ausloggen und wieder einloggen. Auch der Zugriff auf den Privileged Mode sollte nun wieder funktionieren.

Switch-Grundkonfiguration

Szenario: Die vorhandene Konfiguration eignet sich nach eingehender Prüfung nicht für eine Integration in das vorhandene Netzwerk. Daher muss der Switch zunächst in seinen Initialzustand versetzt und anschließend mit einer Grundkonfiguration versehen werden, bevor spezielle und angepasste Konfigurationsschritte unternommen werden:

<u>Den Switch auf den Initial-Zustand zurücksetzen:</u>

1. Löschen Sie die gespeicherte Konfiguration und die VLAN-Datenbank.
2. Starten Sie den Switch anschließend neu und beenden den Initial Configuration Dialog mit „no“. Überprüfen Sie, dass tatsächlich nur noch eine Initialkonfiguration ist und keine VLAN-Datenbank im Flash vorhanden ist.

<u>Allgemeine Grundkonfiguration des Switches:</u>

1. Setzen Sie den Hostnamen auf SW<X>, wobei X für Ihre Gruppen-Nummer steht.
2. Das Passwort zum Schutz des Privileged Mode soll „cisco“ lauten.
3. Alle Passwörter sollen verschlüsselt werden.
4. Verhindern Sie die Domain-Namen-Suche.
5. Erstellen Sie einen Benutzer „asterix“ mit Admin-Privilegien und Passwort „cisco“. Nutzen Sie die sichere Verschlüsselung für das Passwort.
6. Erstellen Sie einen Benutzer „caesar“ ohne Admin-Privilegien und Passwort „cisco“. Nutzen Sie die sichere Verschlüsselung für das Passwort.
7. Stellen Sie sicher, dass sowohl der Konsolenzugriff als auch der Zugriff über die VTY-Lines 0 bis 15 über die Abfrage der lokal gespeicherten Benutzerkennungen gesichert ist.
8. Legen Sie VLAN 10 als Management-VLAN fest und definieren Sie hierfür eine IP-Adresse gemäß des Adress-Schemas (192.168.1.x 255.255.255.0).
9. Konfigurieren Sie ein Default-Gateway mit der IP-Adresse 192.168.1.254.
10. Stellen Sie sicher, dass der Admin-PC (-Laptop) die IP-Adresse des Switches anpingen kann. Denken Sie daran, den Port des Admin-PCs dem VLAN 10 zuzuweisen.
11. Testen Sie den Zugriff über Konsole und über Telnet. In beiden Fällen testen Sie beide Benutzerkennungen.
12. Installieren Sie auf Ihrem Admin-PC einen Syslog-Server (z.B. Kiwi-Syslog). Konfigurieren Sie das Logging auf Ihrem Switch so, dass die Logmeldungen auf den Syslog-Server übertragen werden.
13. Testen Sie die Übertragung, in dem Sie ein nicht genutztes Interface deaktivieren und anschließend wieder aktivieren.
14. Überprüfen Sie die Running-Config und speichern Sie diese anschließend als Startup-Config.
15. *Optional:* Legen Sie den Domain-Name auf cisco.local fest, um SSH konfigurieren zu können.
16. *Optional:* Wenn der Switch es unterstützt, erstellen Sie einen SSH-Schlüssel

17. *Optional:* Testen Sie den Zugriff auf den Switch via SSH
18. *Optional:* Stellen Sie sicher, dass ausschließlich SSH erlaubt und der Telnet-Zugriff abgelehnt wird. Testen Sie anschließend den Zugriff über Telnet und SSH.

VLAN-Konfiguration und Portkonfiguration

Szenario: Nachdem der Switch eine Grundkonfiguration erhalten hat, müssen VLANs erstellt und den Interfaces zugewiesen werden:

1. Erstellen Sie die folgenden VLANs:
    a. VLAN 100 -> Name: Kundenservice
    b. VLAN 200 -> Name: Buchhaltung
    c. VLAN 300 -> Name: Personal
    d. VLAN 400 -> Name: IT
    e. VLAN 500 -> Name: Leitung
    f. VLAN 50 -> Name: Voice
2. Vergeben Sie dem vorhandenen Management-VLAN 10 den Namen: „Management-VLAN“.
3. Konfigurieren Sie die Ports fa0/1 – 5 als Access-Ports und für VLAN 10.
4. Konfigurieren Sie die Ports fa0/6 – 10 als Access-Ports und für VLAN 100.
5. Konfigurieren Sie die Ports fa0/11 – 15 als Access-Ports und für VLAN 200.
6. Konfigurieren Sie für die Ports fa0/1 – 15 das Voice-VLAN 50.
7. Deaktivieren Sie alle nicht genutzten Ports
8. Überprüfen Sie mit den geeigneten Show-Befehlen Ihre Konfiguration (mindestens 3!).
9. Überprüfen Sie die Running-Config und speichern Sie diese als Startup-Config.

Trunks konfigurieren

Szenario: Die Trunks zwischen den Switches müssen explizit konfiguriert werden, um einen sicheren Trunk sicherzustellen. Für die folgenden Übungen müssen Sie entweder fa0/23 oder fa0/24 *durchgängig* nutzen:

1. Konfigurieren Sie auf *beiden* Seiten des Trunks fa0/23 (fa0/24) als Trunk-Port im Mode „Dynamic Auto“. Überprüfen Sie den Trunk-Status. Dieser sollte nicht zustande kommen. Warum?
2. Konfigurieren Sie auf einer Seite des Trunks fa0/23 (fa0/24) als Trunk-Port im Mode „Dynamic Desirable“. Überprüfen Sie den Trunk-Status. Der Trunk sollte zustande kommen. Warum?
3. Konfigurieren Sie auf einer Seite des Trunks fa0/23 (fa0/24) als Trunk-Port im Mode „Trunk“. Überprüfen Sie den Trunk-Status. Der Trunk sollte zustande kommen. Warum?
4. Überprüfen Sie den Trunk-Status mit mindestens 3 Show-Befehlen.
5. Verbinden Sie Ihre Admin-PCs mit dem Port fa0/6, um zu überprüfen, ob Sie auch im VLAN 100 miteinander kommunizieren können. Patchen Sie den Admin-PC anschließend wieder zurück auf fa0/1.
6. Überprüfen Sie die Running-Config und speichern Sie diese als Startup-Config.

VTP-Konfiguration

Szenario: Die Erstellung der VLANs auf jedem Switch ist mühsam und fehleranfällig. VTP soll für einen automatischen Abgleich der VLANs auf allen Switches sorgen:

1. Erstellen Sie auf Ihrem Switch die VTP-Domain „CISCO“. Beachten Sie die Groß- und Kleinschreibung.
2. Legen Sie als VTP-Passwort „cisco“ fest.
3. Aktivieren Sie VTP-Version 2.
4. Stellen Sie sicher, dass Ihr Switch im Modus „Server“ läuft.
5. Aktivieren Sie VTP-Pruning.
6. Überprüfen Sie Ihre VTP-Konfiguration und das gesetzte Passwort.
7. Handeln Sie mit Ihren Mit-Teilnehmern aus, welche beiden Switches im VTP-Server-Modus laufen. Einer der beiden anderen Switches wird in den Client-Modus versetzt und der andere in den Transparent-Modus.
8. Auf einem der beiden VTP-Server erstellen Sie nun VLAN 600, Name: Lab1.
9. Überprüfen Sie auf den anderen Switches, wie sich diese Änderung auswirkt. Der Switch im Transparent-Modus sollte die Änderung nicht vollzogen haben, während sowohl der andere Server als auch der Client die Änderungen übernommen haben.
10. Löschen Sie auf dem zweiten VTP-Server das VLAN 600 und erstellen das VLAN 700, Name: Lab2.
11. Überprüfen Sie auf den anderen Switches, wie sich diese Änderung auswirkt. Der Switch im Transparent-Modus sollte die Änderung wiederum nicht vollzogen haben, während der VTP-Server und –Client die Änderungen übernommen haben. Das VLAN 600 sollte nun nicht mehr existieren.

Spanning-Tree-Konfiguration

Szenario: Die Switches sind redundant angebunden. Daher muss eine schleifenfreie Kommunikation sichergestellt werden. Hierzu dient STP. Dies läuft zwar ohne weiteres Zutun, sollte aber optimiert werden:

1. Überprüfen Sie Ihre Spanning-Tree-Konfiguration und erstellen Sie zusammen mit Ihren Mit-Teilnehmern ein Netzwerk-Chart, in dem die folgenden Informationen erfasst werden:
    a. Uplink-Ports
    b. MAC-Adressen jedes Switches
    c. Root-Switch (Root-Bridge)
    d. Uplink-Kosten (z.B. 100BaseTX=19)
    e. Root-Port jedes Nicht-Root-Switches
    f. Designated Port und Non-Designated Port (Blocking-Port)
2. Konfigurieren Sie:
    a. SW1 als Root-Bridge für VLAN 100, SW2 als Secondary Root.
    b. SW2 als Root-Bridge für VLAN 200, SW3 als Secondary Root.
    c. SW3 als Root-Bridge für VLAN 300, SW4 als Secondary Root.
    d. SW4 als Root Bridge für VLAN 400, SW1 als Secondary Root.

3. Überprüfen Sie Ihre Spanning-Tree-Konfiguration und stellen Sie sicher, dass die richtigen Root-Bridges aktiv sind. Finden Sie mindestens 3 Befehle, um die STP-Konfiguration zu überprüfen.
4. Testen Sie die Ausfallzeit bei einem Endlos-Ping (Windows-Option: -t) auf einen benachbarten Admin-PC, in dem Sie das Patchkabel ziehen und anschließend wieder einstecken, an dem einer der Admin-PCs angeschlossen ist (fa0/1). Die Ausfallzeit sollte 30 Sekunden betragen. Warum?
5. Konfigurieren Sie für den Access-Port fa0/1:
    a. für Portfast
    b. als Access-Port
    c. mit BPDUGuard
6. Testen Sie die Ausfallzeit, wenn Sie nun das Patchkabel ziehen und wieder einstecken. Sie sollte bei minimal sein. Warum?
7. Nachdem Sie die Verbindung wieder hergestellt haben, ziehen Sie bei laufendem Ping den Uplink zum benachbarten Switch, an dem der Partner-PC (das Ziel des Pings) hängt. Wie lang ist die Ausfallzeit? Auch hier sollte der Zeitraum ca. 30 Sekunden betragen.
8. Überprüfen Sie, welche Version von STP auf Ihrem Switch läuft. Konfigurieren Sie auf allen Switches Rapid-STP, bzw. Rapid-PVST. Überprüfen Sie, dass die Änderung übernommen wurde durch den entsprechenden Show-Befehl.
9. Überprüfen Sie nun die Ausfallzeit, wenn Sie einen Dauerping auf einen benachbarten Admin-PC senden und das Uplink-Kabel ziehen. Die Ausfallzeit sollte minimal sein.
10. Optional: Konfigurieren Sie einen weiteren Switch SW5, dessen fa0/24-Interface im Modus Dynamic Desirable stehen sollte. Stellen Sie sicher, dass dieser Switch für VLAN 1 eine höhere Bridge-ID hat, als der bisherige Root-Switch.
11. Optional: Aktivieren Sie Port fa0/16 (bisher ungenutzt und im VLAN 1). Verbinden Sie SW5 über fa0/24 mit Port fa0/16 Ihres Switches und lassen Sie sich den STP-Status für VLAN 1 anzeigen. Der neue Switch sollte die Root-Bridge-Funktion übernommen haben.
12. Optional: Entfernen Sie SW5 vorübergehend wieder. Konfigurieren Sie Port fa0/16 nun als Access-Port in VLAN 1 und mit BPDUGuard. Was passiert, wenn Sie nun SW5 erneut mit fa0/16 verbinden? Mit welchen Befehlen können Sie den Port-Status überprüfen. Finden Sie mindestens 2! Der Port sollte in den err-disabled-State gehen. Wie können Sie diesen Status wieder aufheben?
13. Optional: Entfernen Sie ggf. SW5. Ersetzen Sie den BPDUGuard-Befehl mit BPDUFilter. Wie wirkt sich dies auf den Portstatus aus, wenn Sie nun SW5 wieder anschließen? Der Port sollte seinen Status nicht verändern und als normaler Access Port angezeigt werden. Warum ist dieses Verhalten in der Praxis u. U. problematisch?
14. Optional: Entfernen Sie SW5. Konfigurieren Sie fa0/16 als festen Trunk-Port. Außerdem konfigurieren Sie RootGuard auf diesem Port. Schließen Sie nun SW5 wieder an fa0/16 an. Wie reagiert fa0/16? Der Port sollte in den Status Root Inconsistent gehen, was mit sh span vlan 1 angezeigt wird. Gilt dieser Status für alle VLANs bzw. den physischen Port oder nur für ein bestimmtes VLAN? Wie können Sie diesen Status ändern?