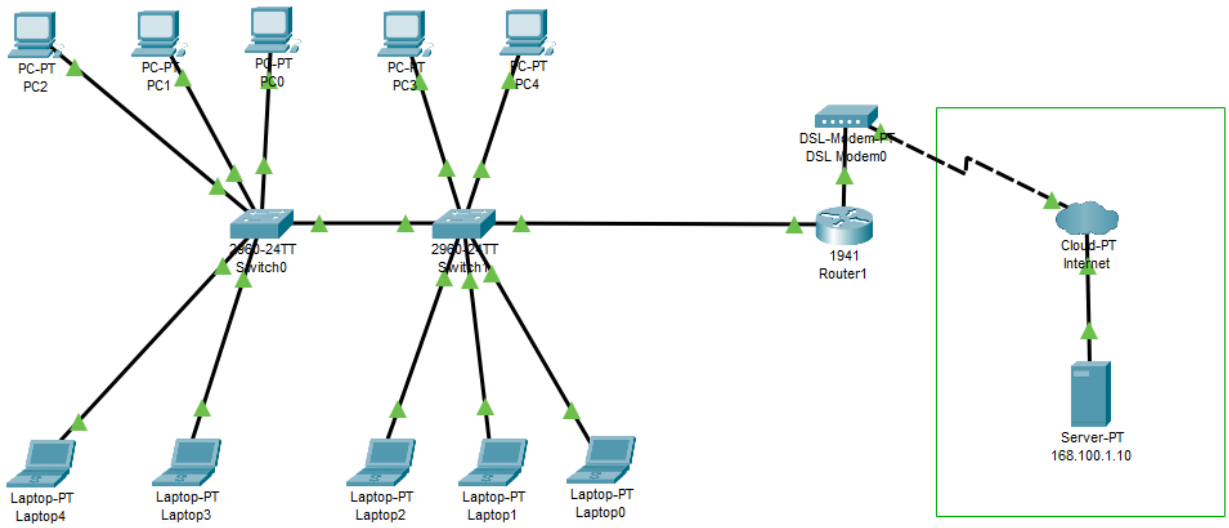
Router on a Stick / Inter VLAN Routing



Die jetzt durch VLAN Konfiguration auf Schicht 2 getrennten Netze sollen trotzdem beide in der Lage sein miteinander und auch mit dem Internet zu kommunizieren.
Leider steht nur ein physikalisches Router Interface zur Verfügung.
Um den beiden Netzen nun jeweils ein eigenes Gateway zur Verfügung zu stellen nutzen Sie folgende Syntax:
Beim wechseln in den Interface-Konfigurationsmodus ergänzen Sie die Interface Nr. durch .X wobei X = ganze natürliche Zahl beginnend bei 1

```
Router(config)#interface gigabitEthernet 0/0.1
Router(config-subif)#
%LINK-5-CHANGED: Interface GigabitEthernet0/0.1, changed
state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0.1, changed state to up
```

Dieses Sub-Interface soll nun genutzt werden als Gegenstück an einem VLAN Trunk die passend getaggten Frames erkennen zu können und wird dadurch auch als Gateqay eines bestimmten Subnetzes/VLANS zugeordnet. Hierfür nutzen wir den Befehl (hier mit der Zuordnung zum VLAN 10)

```
Router(config-subif)#encapsulation dot1Q 10
```

Die virtuellen Sub-Interfaces können nun wie gewohnt adressiert werden.

Das vom Switch1 zum Router zeigende Interface muss nun noch als Trunkport mit passender VLAN Erlaubnis konfiguriert werden.

Switchport Security

Um die Sicherheit auf Layer 1 und 2 weiter zu erhöhen fahren Sie alle ungenutzen Ports der beiden Switche runter.
Weiterhin soll es nicht so einfach möglich sein einfach ein fremdes Gerät an das Netzwerk anzuschliesen. Hierzu bieten die Switche eine einfache, auf der MAC Adressenerkennenung der Endgeräte basierende, Schutzfunktion.

`switchport mode access` → legt fest das es sich um einen einfachen Zugangsport für ein End-Device handelt ! Nur hier ist MAC-Filtern möglich !

`switchport port-security` → Die Sicherheitsoptionen werden angeschalten.

`switchport port-security mac-address xxxx.yyyy.zzzz` → manuelle Eingabe der erlaubten MAC

oder

`switchport port-security mac-address sticky` → automatisch lernen

Jetzt noch:

Dann Anzahl der MAC Adressen die jeder Port kennen darf einstellen (hier bitte auf 1)

`switchport port-security maximum N`

Dann einstellen wie sich der Port bei Fremd-MAC verhalten soll:

`switchport port-security violation protect/restrict/shutdown`

Die Einstellung protect: Pakete von nicht erlaubten Geräten werden nicht weitergeleitet/angenommen.
Beim Wiederanschluss eines erlaubten Gerätes funktioniert der Port wieder wie bisher → kein eingreifen erforderlich.

Die Einstellung shutdown: Der Port schaltet sich beim Nutzungsversuch durch nicht erlaubte Geräte ab. Vor der weiteren Nutzung muss der Port vom Administrtator wieder angeschalten werden.

Die Einstellung restrict: Pakete von nicht erlaubten Geräten werden nicht weitergeleitet/angenommen = protect
Hier wird aber ein Eintrag erzeugt der über die Sicherheitsverletzung informiert und gegebenfalls zurück gesetzt werden muss.

```
Switch#show port-security

Switch#clear port-security all
```

Aber ACHTUNG ! Hier werden alle MAC Einträge auf allen Ports mitgelöscht. Auch die durch Sticky gelernten.