Projekt Standortvernetzung und IoT

**Rudnenko Dmytro und Prasser Tobias - 4AKIFT**

**Aufgabenstellung**: Die Firma YUPP Software Entwicklung GmbH. hat ein rasantes Wachstum hinter sich und siedelt mit dem Hauptsitz auf einen neuen Campus in 2 Gebäude. Zusätzlich sollen in einer weit entfernten Lagerhalle am Stadtrand verschiedene Internet-of-Things Überwachungselemente aufgestellt werden. Für diesen Zweck soll ein Firmennetzwerk (bzw. Teile daraus als Prototyp) projektiert und eine Dokumentation darüber angefertigt werden. Weiters sollen grundlegende Netzwerkfunktionen sichergestellt und Sicherheitsüberlegungen angestellt werden. Jetzt sind sie gefordert!

**Das Netzwerk in Cisco**:

Ein Bild, das Text, Diagramm, Reihe, Screenshot enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Das Netzwerk soll folgender groben Spezifikationen genügen**:

• Logisches Netzwerk: Um das logische Netzwerk zu implementieren sollen die IP-Adressen in den angegebenen Bereichen verteilt und mittels Subnetting unter Verwendung von VLSM in unterschiedlich große Netze aufgeteilt werden. Alle Arbeitsstationen sollen ihre IP-Adressen automatisch beziehen. Im gesamten Netzwerk werden private Adressen verwendet (z.B. ist der WEBServer nur über port-forwarding erreichbar).

• Ein korrektes Konfigurieren der Router, Switches und Endgeräte soll dann für einen Firmennetzwerk-Prototypen erfolgen.

• Switching: Die verschiedenen Netzwerke der Fa. (d.h. PCs-LANs und Server-LANs) sind logisch in VLANs zu strukturieren. Es sind die erforderlichen Switches, VLANs und Trunks einzurichten und zu konfigurieren. Zusätzlich ist auf LAN-Security zu achten!

• WANs: Es erfolgt am Campus eine Anbindung der Fa. an das Internet. Vom ISP haben sie dazu einen öffentlichen IP-Adressbereich zugeteilt bekommen, bzw. müssen den benötigten Bereich anfordern. Für die Anbindung an das Internet ist die Implementierung von NAT/PAT am Border Router erforderlich (zum Testen soll ein zusätzliches Web-Service ins Internet gestellt werden (Achtung: nur offizielle Adressen routen!)).

• IoT und IoT-Server: Die IoT-Elemente erhalten natürlich private IP-Adressen. Der Standort Lagerhalle ist auch an das Internet angebunden. Überlegen sie sich eine mögliche Implementierung, damit die IoT-Elemente auf den zentralen IoT-Server zugreifen können (um sich dort zu registrieren). Dieser IoT-(Registration)-Server ist am DNS-Server zu aktivieren. Nur PC22 darf auf den IoT-Server zugreifen und die Daten der IoT-Elemente ansehen.

## **IP-Adress Schema**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name des Netzwerks** | **Ip-Bereich** | **Prefix** | **Netzwerk Adresse** | **Broadcast Adresse** |
| IoT(max 254) | 10.2.0.1 - 10.2.1.254 | /24 | 10.2.0.0 | 10.2.0.255 |
| Production(99) | 10.2.1.1 - 10.2.1.126 | /25 | 10.2.1.0 | 10.2.1.127 |
| Office(14) | 10.2.1.129 - 10.2.1.158 | /27 | 10.2.1.128 | 10.2.1.159 |
| R1-R0(2) | 10.2.1.169 - 10.2.1.170 | /30 | 10.2.1.168 | 10.2.1.171 |
| R1-ISP(2) | 10.2.1.173 - 10.2.1.174 | /30 | 10.2.1.172 | 10.2.1.175 |
| ISP-Internet | 199.120.120.1 - 199.120.120.6 | /29 | 199.120.120.0 | 199.120.120.7 |
| IoT-Internet | 199.120.120.9 - 199.120.120.14 | /29 | 199.120.120.8 | 199.120.120.15 |
| Internet-Server | 199.120.120.17 -199.120.120.22 | /29 | 199.120.120.16 | 199.120.120.23 |
| DNS/IOT-ISP(>2) | 199.120.120.25 - 199.120.120.30 | /29 | 199.120.120.24 | 199.120.120.31 |
|  |  |  |  |  |

**DHCP-Konfiguration:**

Office:

**A screenshot of a computer

AI-generated content may be incorrect.**

Production:

A screenshot of a computer

AI-generated content may be incorrect.

**IoT-Server Konfiguration**:

1. Man muss den IoT-Server im Browser, vom IoT-Server aus(solange noch keine anderen PCs/Server verbunden sind), aufrufen und dann „Sign up now“ auswählen um einen neuen User zu erstellen:

A screenshot of a computer

Description automatically generated

Danach muss man das IOT Gerät öffnen und in die Konfiguration gehen:

A diagram of a network

Description automatically generated

Und dann muss man unter IoT-Server die IP-Adresse des IoT-Servers eingeben und den Username und das Passwort des Accounts, den man vorher beim IoT-Server erstellt hat, eingeben. In unserem Fall war es: username: „admin“, passwort: „admin“:

A screenshot of a computer

Description automatically generated

Anschließend drückt man auf „Connect“ und wenn die Verbindung erfolgreich ist, steht dann „Refresh“. Wenn man dann über den Webbrowser wieder den IoT-Server aufruft und sich mit dem vorher erstellten Account anmeldet, kann man die IoT-Geräte, die mit dem IoT-Server verbunden sind, ansehen und verwalten:

A screenshot of a computer

Description automatically generated

**NAT-Konfiguration**:

Wir haben NAT am ISP-Router konfiguriert, weil er als Router zwischen privaten IP-Adressen und öffentlichen IP-Adressen dient. Die Konfiguration:

A screenshot of a computer

Description automatically generated

Nach der NAT-Konfiguration kann man sehen, dass die privaten IP-Adressen in die öffentliche IP-Adresse des Routers übersetzt werden:

A close-up of a number

Description automatically generated

Da nur PC22 und die IoT-Geräte Zugriff auf den IoT-Server haben sollen, wurde am ISP-Router eine Access-List an Serial0/1/0(interface nach innen) und Serial0/1/1(interface nach außen) erstellt:

ACL 110(HTTPS/HTTPS nur PC22; Domain-Auflösung alle; Rest zu DNS/IoT gesperrt; Rest erlaubt):

Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

KI-generierte Inhalte können fehlerhaft sein.

A close up of numbers

AI-generated content may be incorrect.

ACL 111(IP nur HomeRouter auf DNS/IoT):



A number and date on a white background

AI-generated content may be incorrect.

Durch Static Routing Konfiguration an jedem Router kann man dann von PC22 auf die IoT-Geräte zugreifen:

PC21:

A screenshot of a computer

AI-generated content may be incorrect.

PC22:

A screenshot of a computer

AI-generated content may be incorrect.

**Schutz vor Internet**

Access-List am Router konfigurieren:

A computer screen shot of a computer code

Description automatically generated

Dann kann ein Gerät z.B. PC den Web-Server erreichen:

A computer screen with white text

Description automatically generated

Aber der Web-Server kann andere Geräte z.B. PC nicht erreichen:

A screen shot of a computer

Description automatically generated

**SSH-Konfiguration:**

Man muss SSH an allen Routern/Switches konfigurieren.

Router-Konfiguration:  
Ein Bild, das Text, Screenshot, Schrift, Reihe enthält.

KI-generierte Inhalte können fehlerhaft sein.



Switch-Konfiguration:  
Ein Bild, das Text, Screenshot, Dokument, Schrift enthält.

KI-generierte Inhalte können fehlerhaft sein.

Danach kann man die Geräte von einem PC aus remote konfigurieren:

Ein Bild, das Text, Screenshot, Software, Multimedia-Software enthält.

KI-generierte Inhalte können fehlerhaft sein.

Um die Switches über SSH zu konfigurieren muss erst ein Passwort auf den Switches eingestellt werden.

A screenshot of a computer program

AI-generated content may be incorrect.

In dem Netzwerk soll nur PC22 die Netzgeräte über SSH konfigurieren können, daher hat jedes Gerät eine Access-List für VTY.

A screenshot of a computer program

AI-generated content may be incorrect.

Versuch von PC21:  
A screenshot of a computer

AI-generated content may be incorrect.

PC22:

A screenshot of a computer

AI-generated content may be incorrect.

**VLAN-Konfiguration:**

Zuerst wurden Office und Production in ein eigenes VLAN unterteilt.

Office(VLAN 20):  
Ein Bild, das Text, Screenshot, Schrift, Zahl enthält.

KI-generierte Inhalte können fehlerhaft sein.

Production(VLAN 10):

Ein Bild, das Text, Screenshot enthält.

KI-generierte Inhalte können fehlerhaft sein.

**Layer 2 Security:**

Auf beiden Switches wurde auf allen Ports, mit Ausnahme der Uplinks, Port-Security sowie BPDU Guard aktiviert.  
Zusätzlich wurde DHCP Snooping konfiguriert. Dabei wurde ausschließlich der Port zum jeweiligen DHCP-Server als vertrauenswürdig (trusted) markiert, während auf den übrigen aktiven Ports eine Rate-Limitierung für DHCP-Anfragen aktiviert wurde.  
Alle nicht genutzten Ports wurden deaktiviert (shutdown).

Hier der Office Switch:

Ein Bild, das Text, Elektronik, Screenshot, Software enthält.

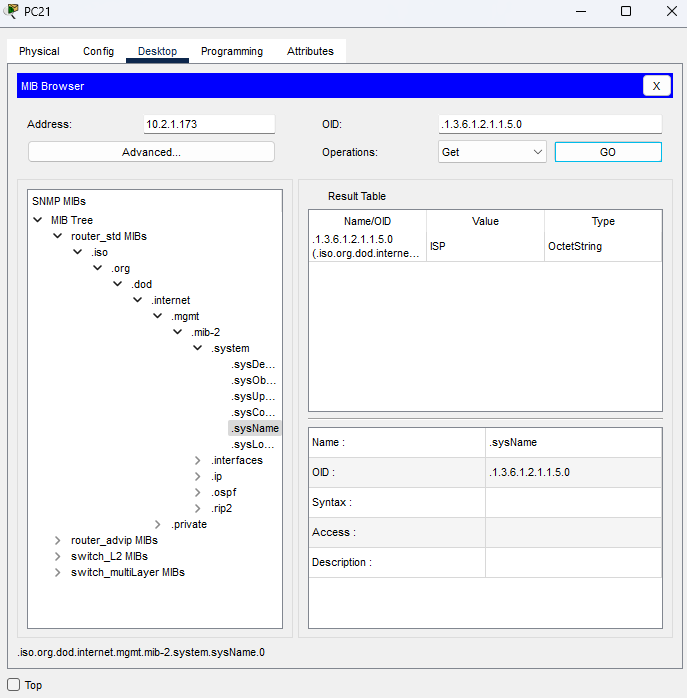
KI-generierte Inhalte können fehlerhaft sein.

**SNMP-Konfiguration:**

Die SNMP Communities für Read-Only und Read/Write Zugriff müssen in jedem Netzwerkgerät erstellt werden:



Nach der Konfiguration können die Netzgeräte im MIB-Browser über SNMP erreicht werden:



**Check Matrix:**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | PC11 | PC21 | DNS/IoT-Server | PC22 | WEB-Server | Internet | IoT-Laptop | ISP-Router |
| PC11 | - | y | y(53) | y | y | y | x | x(ssh) |
| PC21 | y | - | y(53) | y | y | y | x | x(ssh) |
| WEB-Server | x | x | x | x | - | y | x | x(ssh) |
| Internet | x(nat) | x(nat) | x | x(nat) | y | - | x | x(ssh) |
| IoT-Laptop | x | x | y | x | y | y | - | x(ssh) |
| PC22 | y | y | y(80,443,53) | - | y | y | x | y(ssh) |