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 Schema von Netzwerk in Cisco**:

A diagram of a network

Description automatically generated

**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-LAN(>2) | 199.120.120.25 - 199.120.120.30 | /29 | 199.120.120.24 | 199.120.120.31 |
|  |  |  |  |  |

**IOT-Server Konfiguration**:

1.Zuerst muss man ins IOT-Server gehen

A diagram of a network

Description automatically generated

2. Danach muss man ins IOT-Server in Webserver gehen und IP-Adresse von IOT-Server schreiben und dann „Sign up now“ auswählen um neue User zu erstellen:

A screenshot of a computer

Description automatically generated

Danach muss man ins Gerät Konfiguration gehen:

A diagram of a network

Description automatically generated

Und dann muss man in IoT-Server Bereich richtiges IP-Adresse von Server-IoT schreiben und die Daten von neue User, die wir erstellt haben, nämlich user Name und Passwort in unserem Fall es war: „admin“, „admin“:

A screenshot of a computer

Description automatically generated

Und wenn man Login erfolgreich gemacht hast an IoT-Server mit Webbrowser, dann kann man die Geräte, die verbunden mit diesem IoT-Server sind ansehen und verwalten:

A screenshot of a computer

Description automatically generated

**NAT Konfiguration**:

Wir haben NAT an Router ISP konfiguriert, weil er als Router zwischen private Ip-Adresse und öffentliche Ip-Adresse dient. Konfiguration:

A screenshot of a computer

Description automatically generated

Nach dem NAT-Konfiguration kann man erfolgreich ansehen, wie das funktioniert wenn man von PC Server0 pingt:

A close-up of a number

Description automatically generated

Durch Static Routing Konfiguration an jedem Router kann man dann von PC alle IoT-Geräte zugreifen:

A screenshot of a computer

Description automatically generated

**Security**

Access-List an Router konfigurieren:

A computer screen shot of a computer code

Description automatically generated

Dann kann Gerät z.B. PC Internet Server erreichen:

A computer screen with white text

Description automatically generated

Aber Internet-Server kann nicht Geräte z.B. PC erreichen:

A screen shot of a computer

Description automatically generated

Internet Server kann nur IoT-Server erreichen:

A computer screen with white text

Description automatically generated