it.schule
stuttgart

IT Schule Stuttgart Projekt Nr. 2

Projekt Messe Auftritt

Durchführung:

Holger Haack
Luis Scheurenbrand
Dennis Kreittner

Lehrer:

Hr. Serhan

20.1.2024

Abkürzungsverzeichnis

PT Packet Tracer

IP Internet Protokoll: Ein verbindungsloses Protokoll, dass die Adressierung von Computern und das Routing von Paketen ermöglicht.

wr Write memory: Ein wichtiger Befehl, bei der Konfiguration von Routern im Packet Tracer, genutzt damit Konfigurationen persistent sind.

RADIUS Remote Authentication Dial-In User Service: Client-Server-Protokoll zur Authentifizierung, Autorisierung und Accounting von Benutzern bei Einwahlverbindungen in Netzwerke.

AP Access Point: Schnittstelle für kabellose Kommunikationsgeräte.

LWAP Light Weight Access Point: Schnittstelle für kabellose Kommunikationsgeräte.

CIDR Classless Inter-Domain Routing: Verfahren zur effizienten Nutzung von IP-Adress-Räumen unter Verwendung von Subnetzmasken.

DHCP Dynamic Host Configuration Protocol: Ein Verfahren um von einem Server aus Netzwerkkonfigurationen an Clients zuzuweisen.

WPA2 Wi-Fi Protected Access 2: Sicherheitsstandard für Funknetze basierend auf AES.

AES Advanced Encryption Standard: Blockchiffre zur Verschlüsselung von Daten.

ACL Access Liste: Liste von zugelassenen und blockierten IP Adressen(-Bereichen).

TCP Transmission Control Protocol: Ein zuverlässiges, verbindungsorientiertes, paketvermitteltes Layer 4 Netzwerk Protokoll.

HTTPS Hypertext Transfer Protocl Secure: Ein Kommunikationsprotokoll im World Wide Web, das eine Transportverschlüsselung darstellt.

JSON JavsScript Object Notation: Ein kompaktes Datenformat in einer einfach lesbaren Textform unabhängig von Programmiersprachen.

SQL Structured Query Language: Eine Abfragesprache um auf Daten in einer relationalen Datenbank zuzugreifen und diese zu verwalten.

UI User Interface: Englische Bezeichnung für Benutzeroberfläche.

Inhaltsverzeichnis

1 Einführung

Für den Messeauftritt Ihres Unternehmens am 24.1.2024 soll eine WLAN-Infrastruktur und eine Software zur Erfassung von Kundendaten bereitgestellt werden.

2 Anforderungsanalyse

Dieser Abschnitt befasst sich mit der Ausgangssituation die vor Ort vorliegt und den Anforderungen, die an die zu erstellenden Netzwerkkomponenten und Softwarelösungen gestellt werden.

2.1 Situationsbeschreibung

Die Firma XYZ plant den Besuch einer Messe. Auf der Messe sollen neben den üblichen Tätigkeiten nach Möglichkeit auch Daten potenzieller Neukunden erhoben und gespeichert werden. Zu diesem Zweck kann der Messestand Gutscheine ausstellen, mit denen vergünstigte Angebote auf der Messe wahrgenommen werden können. Voraussetzung ist die Registrierung im Portal der Firma XYZ.

2.1.1 Teilprojekt SAE: Datenerfassung Neukunden

Während des Messeauftritts sollen von Kunden im Self-Service Kundenkarten erstellt werden können, mit denen dann der Zugang zu weiteren Messeangeboten möglich wird. Dabei sollen Nachname, Vorname, Anschrift und ein Bild erfasst werden. Zusätzlich sollen ein oder mehrere Produktgruppen angegeben werden können, für die besonderes Interesse besteht. Bei Firmenvertretern soll zusätzlich ein Datensatz für die Firma angelegt werden. Die Speicherung der Daten soll langfristig in einer Datenbank erfolgen. Da die Zuverlässigkeit der Netzwerkverbindung während des Messeauftritts nicht immer sichergestellt werden kann, muss das Erfassungssystem auch offline funktionieren und in der Lage sein, die Daten auf Wunsch an die Firmenzentrale zu übermitteln. Die Übermittlung soll mit Hilfe einer REST-API an den Firmenserver erfolgen. Die gespeicherten Daten sollen von den MitarbeiterInnen auch abgerufen und durchsucht werden können. Da es sich um einen Self-Service handelt muss sichergestellt werden, dass nicht jede Person das System frei nutzen kann. Für die Erfassung des Fotos soll eine Webcam angebunden werden. Für die Erfassung der Daten sollen 4 firmeneigene Laptops zur Verfügung gestellt werden, die über WLAN an das Internet angebunden sind (siehe unten)
Folgende technische Rahmenbedingungen werden an die Softwarelösung gestellt:

- C# Applikation
- Rest API mit ASP.Net erstellen und konsumieren

- SQLite Datenbank
- Entity Framework Core
- Datenbankentwurf
- Prüfen: Design Pattern, Interface, Dependency Injection

2.1.2 Teilprojekt ITS: WLAN

Sie sollen für den Messeauftritt ein eigenes WLAN planen, da Sie nicht auf das dort verfügbare öffentliche WLAN zugreifen wollen. Zu diesem Zweck erhalten Sie vom Messeveranstalter einen internetfähigen Router mit der Auflage, nur Subnetze im Bereich 192.168.4.128/25 anzubieten. Das Netzwerk muss so aufgebaut sein, dass die im Teilprojekt SAE erfassten Daten bei Bedarf an die Firmenzentrale übermittelt werden können. Die insgesamt 16 firmeneigenen Endgeräte sollen über das WLAN angebunden werden. Die 4 für Kunden gedachten Laptops sollen sich in einem anderen Netz als die Geräte der Mitarbeiter befinden.
Folgende Anforderungen werden an die Netzwerkumsetzung gestellt:

- Subnetting
- Konfiguration WLAN
- Accesspoints
- Informieren: WLAN Controller, Radius, AAA-Server

3 Umsetzung Teilprojekt ITS

3.1 Netzwerkinfrastruktur Stand

3.1.1 Netzwerkaufbau

Zunächst wurde das Projekt mit dem Router 4331 und mit einem zusätzlichen Modul (NIM-ES2-4) gestartet, um den Router um 4 weitere Gigabit Ports erweitert, da jeweils ein AP einen Port belegt, der Radius Server einen Port belegt, und ein Port mit „dem Internet“ verbunden ist. Standardmäßig ist der Router allerdings nur mit zwei Gigabit Ports bestückt. Einen weiteren könnte man mit dem GLC-T Modul erweitern, dann wäre man aber nur bei 3 statt 4 Ports. Der Port, der „mit dem Internet“ verbunden ist, erhielt zusätzlich ein GLC-GE-100FX Modul, da man darüber über 2km Reichweite mit Glasfaser erreichen könnte, und das am ehesten der Realität entspricht. Dass mehr Ports benötigt werden, ist erst beim Aufbauen des Netzwerkes aufgefallen. Daher musste der Router einmal ausgeschaltet werden und mit den Modulen erweitert werden. Dabei hat sich der Befehl „wr“ bzw. „write memory“ als sehr wichtig herausgestellt, da andernfalls alle bisherigen Konfigurationen gelöscht werden, da sie flüchtig waren. Nachdem fast alle verkabelt war, außer der Radius Server, hat sich allerdings herausgestellt, dass das NIM-ES2-4 Modul nur auf Layer 2 arbeitet, also wie ein Switch. Es fehlte also ein Port für den Radius Server. Daher wurde der Router verworfen und es wurde ein PT-Empty mit 3x PT-ROUTER-NM-1CGE Modulen und einem PT-ROUTER-NM-1FGE Modul erweitert. Erstere werden verwendet, da die verwendeten AP nicht mit FastEthernet gearbeitet haben, und Letztere, um hohen Datentransfer zum Server zu gewährleisten. Vorteil: Der Router ist insgesamt günstiger als der ISR 4331, und er ist flexibel erweiterbar. Für diese Migration wurden die Konfigurations-Dateien der bisherigen Router exportiert, und in die neuen Router gemerged. Damit mussten die dhcp Konfigurationen nicht neu erstellt werden. Nachdem das Netzwerk soweit eingerichtet wurde, und es an die Konfiguration des RADIUS-Servers ging, hat sich herausgestellt, dass die im Vergleich zu den LWAPs günstigeren APs nicht direkt einen RADIUS-Server angeben können. Daher wurde ein PT-ROUTER-NM-1CGE und der RADIUS-Server als solcher entfernt, dass die Kosten abermals reduziert. Das fertige Projekt lässt sich Preis-Leistungstechnisch kaum weiter optimieren, da man trotz der geringen Gesamtkosten immer noch ein hohes Maß an sowohl Geschwindigkeit als auch Sicherheit erreicht. Näheres dazu unter dem Reiter WLAN, Zugang und Sicherheit. Im Folgenden die Tabelle für die Subnetze und die Netzwerkskizzen für das

Messe-Netzwerk und das Netzwerk in der Firmenzentrale:

Netzwerk-Adresse	Subnetzmaske	Beschreibung
192.168.4.128	255.255.255.224	Dieses Netzwerk ist für die Firmengeräte auf der Messe gedacht. Es hat einen CIDR von /27, sodass alle 16 Geräte + Netzwerkadresse + Broadcastadresse in das Netz passen
192.168.4.161	255.255.255.248	Dieses Netzwerk ist für die Kunden-Geräte auf der Messe gedacht. Es hat einen CIDR von /29, sodass alle 4 Geräte + Netzwerkadresse + Broadcastadresse in das Netz passen
142.250.183.0	255.255.255.0	Dieses Netzwerk dient der Kommunikation zwischen dem Messe Router und dem Router der Firmenzentrale. Sie ist willkürlich gewählt, da sie normalerweise vom ISP vergeben wird, da das gleichzeitig auch die öffentliche IP-Adresse ist
172.16.0.0	255.255.255.0	Dieses Netzwerk soll das private Netzwerk innerhalb der Firmenzentrale darstellen. Da dieses nicht näher beschrieben wurde, wurde auch dieses willkürlich gewählt

Tabelle 3.1: Netzwerke für das Subnetting

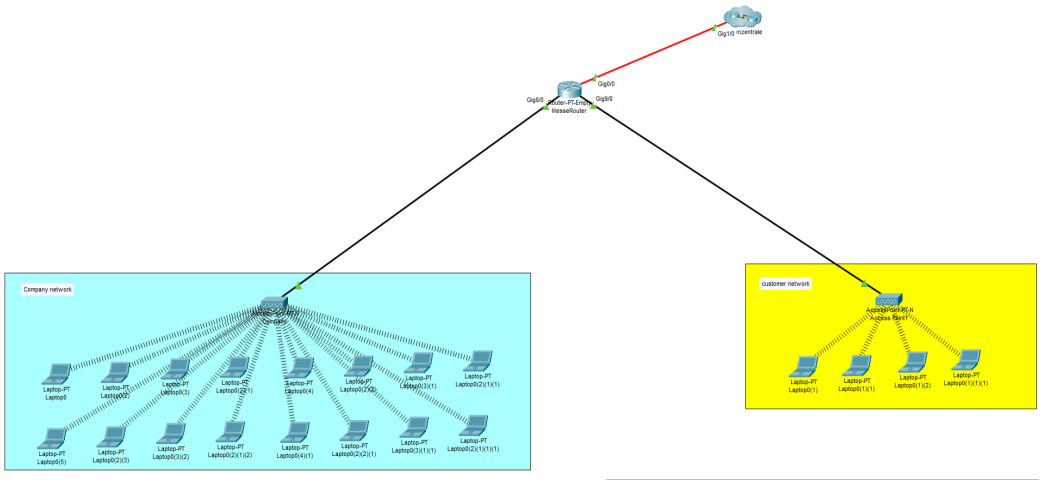

Abbildung 3.1: Netzwerkskizze Messe-Netzwerk

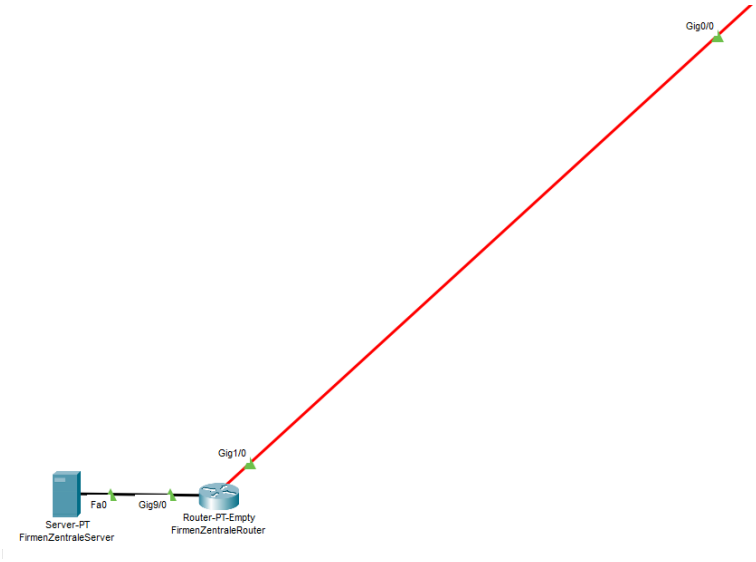

Abbildung 3.2: Netzwerkskizze Firmenzentrale-Netzwerk

3.1.2 Anbindung Messenetzwerk

Messe Router Interface Konfiguration

Das linke, untere Interface gig 8/0 befindet sich im company network, es ist also das größere Subnetz, da 16 Geräte benötigt werden. Die IP-Adresse lautet: 192.168.4.129 /27 (255.255.255.224). Die Subnetzmaske /28 konnte nicht verwendet werden, da neben den 16 Hosts auch eine Adresse für das Netzwerk und eine als Broadcastadresse verwendet wird. Das rechte, untere Interface gig 9/0 befindet sich im customers network für die Kunden-Geräte. Dessen IP-Adresse lautet: 192.168.4.161 /29 (255.255.255.248). Die nächstkleinere Subnetzmaske konnte aufgrund obiger Beschreibung ebenfalls nicht verwendet werden. Das obere Inter-

face gig 0/0, ist das Interface, das „ins Internet“ führt, und über das dann der Server in der Firmenzentrale erreicht werden soll. Seine IPv4 lautet: 142.250.183.14 /24 (generisch, da diese IP-Adresse normalerweise vom ISP bereitgestellt wird und es gemäß Aufgabenstellung keine weitere Einschränkung in Bezug auf diese Adresse gibt).

Firmenzentrale Router Interface Konfiguration

Der Port, der „aus dem Internet“ zugreifbar ist, ist Gig 1/0 zusammen mit einem PT-ROUTER-NM-1FGE Modul. Er hat die IPv4: 142.250.183.16 (generisch, da diese IP-Adresse normalerweise vom ISP bereitgestellt wird). Es wurde absichtlich eine Adresse innerhalb des gleichen Netzwerkes gewählt, da dies am ehesten der Simulation einer VPN-Verbindung entspricht. Aufgrund dieser Annahme, und da es sich nur um eine Simulation des Firmenservers handelt, wurde ansonsten keine weitere Konfiguration zum Beispiel in Form einer ACL angefertigt. Der Port, der mit dem Server der Firmenzentrale verbunden ist, hat den Port Gig 9/0 und das Modul PT-ROUTER-NM-1CGE. Er hat die IPv4: 172.16.0.10 /24 (generische, private IP-Adresse mit generischer Subnetzmaske).

3.1.3 Netzwerk Einrichtung und IP-Zuweisung

Die interface Adressen wurden den ip dhcp excluded adressen hinzugefügt, auch wenn das beim int gig 0/0 nicht notwendig gewesen wäre, da er nicht in die dhcp pools eingreift. Default Router sind entsprechend die ip adressen der Schnittstellen des Routers für die dhcp pools, also 192.168.4.129 für den company dhcp pool und 192.168.4.161 für den customers dhcp pool. Der dhcp pool company ist wie oben beschrieben für die Firmengeräte gedacht und hat das Netzwerk 192.168.4.128 255.255.255.224. Der dhcp pool customers ist für die Kunden-Geräte gedacht und hat das Netzwerk 192.168.4.160 255.255.255.248.

3.1.4 Routing

Theoretisch hätte man auch OSPF auf den Routern konfigurieren können, da dies eher dem Szenario entspricht, dass man erst „über das Internet“ geht und dann auf den Firmen-Server zugreift, wenn es aber darum geht, dass man sich über einen VPN-Tunnel mit dem Firmen-Server verbindet, und die Laptops ausschließlich mit dem Firmen-Server kommunizieren sollen und sonst nichts anderes können sollen, dann entsprechen statische Routen eher dem Anwendungsfall, weswegen wir uns dafür entschieden haben. Aufgrund der statischen Routen, müssen sowohl

für den Messe Router als auch für den Firmenzentrale Router Tabellen angefertigt werden.

Ziel-Netzwerk	Ziel-Subnetzmaske	Next Hop	Quell-Port
172.16.0.0	255.255.255.0	142.250.183.16	Gig 0/0

Tabelle 3.2: Messe Router Routing Tabelle

Ziel-Netzwerk	Ziel-Subnetzmaske	Next Hop	Quell-Port
192.168.4.128	255.255.255.224	142.250.183.14	Gig 1/0
192.168.4.160	255.255.255.248	142.250.183.14	Gig 1/0

Tabelle 3.3: Firmenzentrale Router Routing Tabelle

3.2 WLAN

3.2.1 Zugang und Sicherheit

Der Zugriff auf das Netzwerk wurde mithilfe WPA2-PSK gesichert. Dieses Protokoll nutzt die AES-Verschlüsselung, die deutlich sicherer ist als TKIP, was noch von WPA verwendet wurde, und sich als Standard-Verschlüsselung etabliert hat. Da es sich nur um einen Messe-Aufenthalt handelt, muss man sich keine Gedanken über das zyklische tauschen des Schlüssels machen, was normalerweise der Fall wäre, um die Sicherheit zu erhöhen. Der Schlüssel wurde außerdem sehr lang gewählt, und wird in KeePass verschlüsselt gespeichert. Die Schlüssellänge wurde bewusst sehr lang gewählt, da es sowohl für die Firmengeräte als auch die Kundengeräte verwendet werden soll, was Administratoren die Arbeit erleichtert, da Sicherheit auch immer ein Abwägen zwischen Aufwand und Ertrag ist. Wie im Kapitel „Routing“ bereits erwähnt, wird davon ausgegangen, dass nur über eine VPN-Verbindung der Firmenzentrale Server erreicht werden kann, was ein großes Plus an Sicherheit für die Kommunikation zwischen dem Messer Router und dem Firmenzentrale Netzwerk bedeuten würde. Diese Sicherheit, und die gesicherte Verbindung zwischen den APs wurde durch die beiden ACLs erreicht, die auf dem Messe Router konfiguriert wurden:

ACL 1

Situationsbeschreibung

Nur Requests vom Server an die Netzwerke sollen erlaubt werden. Die Kommunikation zwischen den Netzwerken und die Paket-Weiterleitung der Pakete an

die Netzwerke von anderen IP-Adressen als der Server-Adresse sollen gestoppt werden. Für diesen Anwendungsfall reicht eine einfache ACL, da keine Protokolle spezifiziert werden müssen.

Befehle

- access-list 1 permit 142.250.183.16 255.255.255.0
- (int 8/0) ip access-group 1 out → Das Paket darf nur von diesem Netzwerk in das Netzwerk kommen.
- (int 9/0) ip access-group 1 out

ACL 101

Situationsbeschreibung

Nur Anfragen an den Server aus den Netzwerken sollen erlaubt werden. Alle anderen Anfragen sollen fallen gelassen werden. Von den Anfragen, die zugelassen werden, sollen wiederum nur eine HTTPS Verbindung erlaubt werden, um zu gewährleisten, dass die Kommunikation verschlüsselt stattfindet. Dafür wird eine erweitere ACL benötigt, die TCP auf dem Standard-Port 443 erlaubt.

Befehle

- access-list 101 permit tcp 192.168.4.129 0.0.0.31 172.16.0.10 0.0.0.255 eq 443
- access-list 101 permit tcp 192.168.4.161 0.0.0.7 172.16.0.10 0.0.0.255 eq 443
- (int gig 0/0) ip access-group 101 out

Folgen

Aufgrund dieser restriktiven Einstellung war es zeitweise nicht möglich, die Notebooks über dhcp zu konfigurieren, da die dhcp discovery packages gedroppt wurden.

Lösung

Daher müssen die UDP-Ports, die für DHCP verwendet werden, ebenfalls erlaubt werden, und da die Notebooks zu dem Zeitpunkt noch keine IP haben, und das interface nicht kennen, wird any any verwendet:

- access-list 101 permit udp any any eq 67
- access-list 101 permit udp any any eq 68

3.2.2 Anbindung von Clients

Die Laptops haben standardmäßig ein Modul verbaut, welches nur einen Ethernet Port anbietet. Daher musste das integrierte Module der Laptops ausgebaut werden und durch ein WPC300N ersetzt werden, da dieses WLAN unterstützt. Um sich nun mit dem Netzwerk zu verbinden, muss man unter Desktop, PC Wireless, den nächsten AP auswählen und den Schlüssel eingeben. Ansonsten ist keine Verbindung mit dem Netzwerk möglich.

3.3 Inbetriebnahme

Die für den Stand auf der Messe verantwortlichen Mitarbeiter, werden mit den vier Laptops, die von Kunden zur Datenerfassung genutzt werden sollen, auf die Messe geschickt. Dabei befindet sich die dafür genutzte Software auf eben diesen Laptops. Die Mitarbeiter werden entsprechend geschult, wie das Programm zu bedienen ist (siehe Kapitel zu Anleitungen). Sollte von den Messebetreibern ein Access-Point bereits gestellt sein, kann dieser genutzt werden um eine Verbindung zum Internet und damit zum Firmenserver herzustellen. Wird kein Access-Point gestellt, so ist zumindest mit einem Router zu rechnen da sonst stark an der der Verfügbarkeit von Internet an diesem Standort gezweifelt werden muss. Sollte dies kein WLAN-fähiger Router sein, werden die Mitarbeiter ein entsprechendes Gerät mitführen und dieses per Ethernet Kabel mit dem dortigen Router verbinden. Anschließende werden die vier Laptops mit den gestellten oder mitgebrachten Access-Points verbunden unter Verwendung des vereinbarten Passworts.

4 Umsetzung Teilprojekt SAE

4.1 Datenbank

4.1.1 Datenbankmodell

4.2 Aufbau und Funktionsweise

4.2.1 Architektur

4.2.2 USE Case und UML Diagramme

4.2.3 Prerequisites: Bibliotheken und Komponenten

4.2.4 Inbetriebnahme vor Ort

4.2.5 Technische Beschreibung der WebCam Anbindung

4.2.6 Anleitung Bedienung durch den Kunden

4.2.7 Anleitung Datenabruf und Übermittlung

4.2.8 Testszenarien

Zusammenfassung