Obecna infrastruktura sieciowa boryka się z kilkoma problemami, które mają wpływ zarówno na bezpieczeństwo, jak i na stabilność pracy:

- **Brak wolnych adresów IP** – prywatne telefony pracowników oraz inne urządzenia łączą się przez Wi-Fi i pobierają adresy IP, co powoduje, że dla komputerów firmowych zaczyna ich brakować. Ze względu na zmienne identyfikatory tych urządzeń (dynamiczne adresy MAC) blokowanie ich jest nieskuteczne.
- **Drukarki sieciowe** – obecnie działają w jednej wspólnej sieci, wysyłając informacje o swoich usługach w każdym kierunku. Powoduje to niepotrzebny ruch, który obciąża infrastrukturę i spowalnia inne aplikacje.
- **Urządzenia dodatkowe (IoT)** – takie jak bramy, zamki czy instalacje fotowoltaiczne, także pracują w tej samej sieci. Powoduje to ryzyko, że potencjalnie mniej bezpieczne urządzenia mogą wpływać na działanie krytycznych systemów firmowych.

Rozwiązania wprowadzane w nowym projekcie

1. **Kontrola dostępu do sieci**
    - Do sieci będą wpuszczane wyłącznie urządzenia wcześniej zatwierdzone.
    - Urządzenia nieznane (np. prywatne telefony, laptopy gości) zostaną automatycznie izolowane i nie uzyskają dostępu do Internetu ani do zasobów firmowych.
2. **Segmentacja sieci (VLAN)**
    - Każda grupa urządzeń (komputery pracowników, serwery, drukarki, urządzenia IoT, goście) będzie posiadać wydzieloną podsieć.
    - Ruch z jednej podsieci nie będzie zakłócał pracy w innej. Drukarki będą widoczne tylko dla osób, które powinny z nich korzystać.
    - Urządzenia IoT zostaną odseparowane, aby ich praca nie wpływała na systemy biznesowe.
3. **Centralne zarządzanie**
    - Wszystkie przełączniki i punkty dostępowe Unifi będą obsługiwane z jednego panelu administracyjnego.
    - Pozwoli to na szybkie diagnozowanie problemów, monitorowanie obciążenia i natychmiastową reakcję w przypadku incydentu.
4. **Stabilność usług**
    - Zniknie problem braku adresów IP dla komputerów – każdy pracownik będzie miał zapewnione stabilne połączenie.
    - Ograniczenie zbędnego ruchu sieciowego zwiększy szybkość i niezawodność systemów biznesowych.

Wzrost bezpieczeństwa

- **Brak dostępu dla urządzeń nieautoryzowanych** – prywatne telefony, nieznane laptopy czy urządzenia IoT spoza listy zatwierdzonych nie będą miały żadnego dostępu do sieci.
- **Lepsza ochrona danych firmowych** – systemy sprzedażowe, serwery i kopie zapasowe będą oddzielone od ruchu użytkowników, drukarek i urządzeń IoT.
- **Minimalizacja ryzyka ataków wewnętrznych** – segmentacja i filtracja MAC ograniczają możliwość podsłuchu czy nieautoryzowanego dostępu do zasobów.
- **Większa odporność na błędy ludzkie** – nawet przypadkowe podłączenie nieautoryzowanego urządzenia nie wpłynie na działanie całej sieci.

👉 **Korzyści biznesowe:**
Nowa infrastruktura sieciowa zapewni stabilne środowisko pracy, wyeliminuje obecne problemy z adresacją, drukarkami i urządzeniami IoT, a przede wszystkim znacząco podniesie poziom bezpieczeństwa danych i systemów krytycznych dla działalności firmy.

Podsumowanie kosztów wg budynków

Renault

Mikrotik RB5009UG+S+IN	
Ubiquiti USW-Aggregation	
Ubiquiti USW-Pro-24 (bez PoE)	
Ubiquiti USW-Pro-24-PoE	
Patchcordy DAC (3x0,5m)	
Patchcordy RJ45 Cat6a + drobnica	
SUMA	**8100,00 zl**

Ferrari

Ubiquiti USW-Pro-24 (bez PoE)	
Ubiquiti USW-Pro-24-PoE	
Patchcordy DAC (3x0,5m)	
Patchcordy RJ45 Cat6a + drobnica	
SUMA	**6800,00 zl**

Ferrari Old

Patchcordy DAC (3x0,5m)	
Patchcordy RJ45 Cat6a + drobnica	
Ubiquiti USW-16-PoE	
SUMA	**2400,00 zl**

Peugeot

Ubiquiti USW-Pro-24 (bez PoE)	
Patchcordy DAC (3x0,5m)	
Patchcordy RJ45 Cat6a + drobnica	
SUMA	**2400,00 zl**

Lamborghini

Ubiquiti USW-Pro-24 (bez PoE)	
Ubiquiti USW-Pro-24-PoE	
Patchcordy DAC (3x0,5m)	
Patchcordy RJ45 Cat6a + drobnica	
SUMA	**5600,00 zl**

Łączna kwota netto sprzęt: 25300,00 zł

Robocizna liczona wg faktycznie wykorzystanych godzin