Okablowanie strukturalne w budynku trzypiętrowym

Spis treści

[1. Opis struktury okablowania 5](#_Toc189603105)

[1.1. Szkielet sieci 5](#_Toc189603106)

[1.2. Okablowanie pionowe 7](#_Toc189603107)

[1.3. Okablowanie poziome 7](#_Toc189603108)

[1.4. Metodologia opisów 8](#_Toc189603109)

[2. Opis struktury logicznej 9](#_Toc189603110)

[2.1. Oddzielne pule adresowe dla każdego piętra i typu urządzeń. 9](#_Toc189603111)

[2.2. Schemat logiczny adresacji 10](#_Toc189603112)

[2.3. VLAN 69 – Zarządzanie (MGMT) 10](#_Toc189603113)

3[.Wykorzsytane technologie 11](#_Toc189603114)

[3.1..Trunking na styku warstw access i core 11](#_Toc189603114)

[3.2.Switching & Routing 11](#_Toc189603114)

[4.Podsumowanie zbiorcze 11](#_Toc189603114)

[Rzut z góry, piętro 1 3](#_Toc189603333)

[Rzut z góry, piętro 2 4](#_Toc189603334)

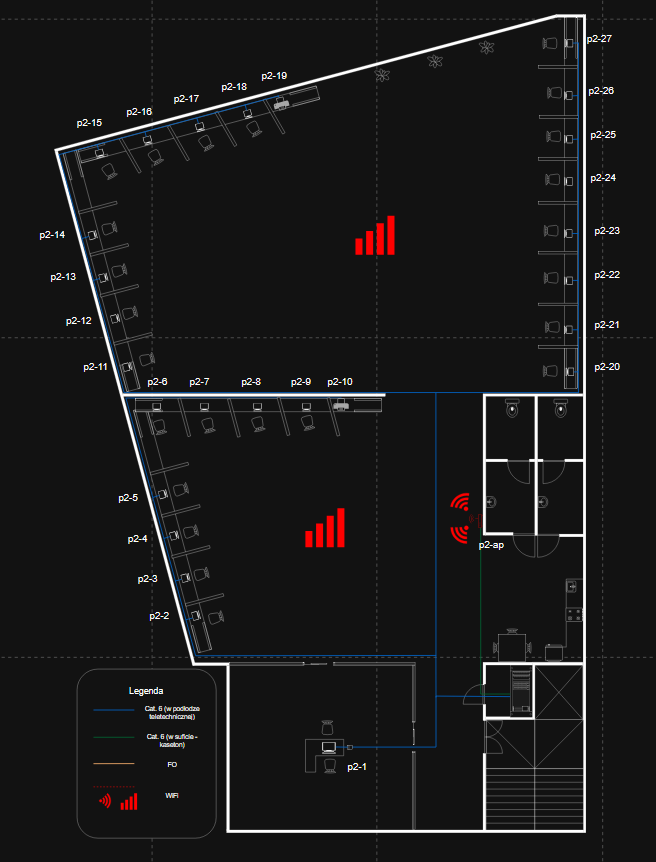
[Rzut z góry, piętro 3 5](#_Toc189603335)

[Rysunek 4 Wizualizacja szafy rack 10](#_Toc190032587)

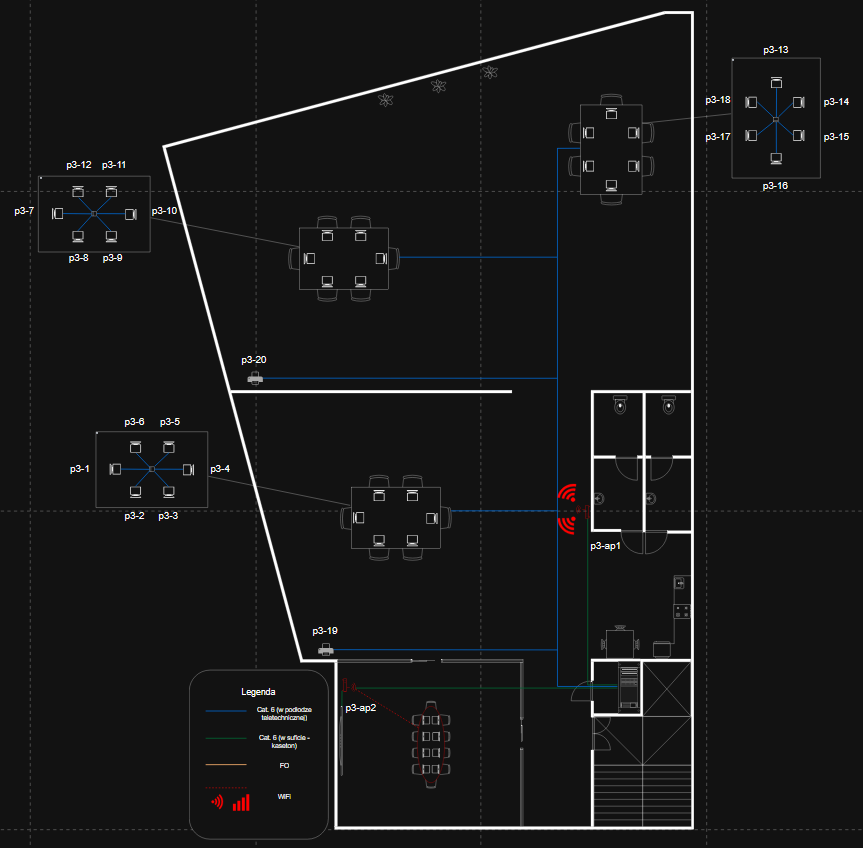
[Tabela 1 Urządzenia aktywne, pasywne i materiały 13](#_Toc189603153)



Rzut z góry, piętro 1



Rzut z góry, piętro 2



Rzut z góry, piętro 3

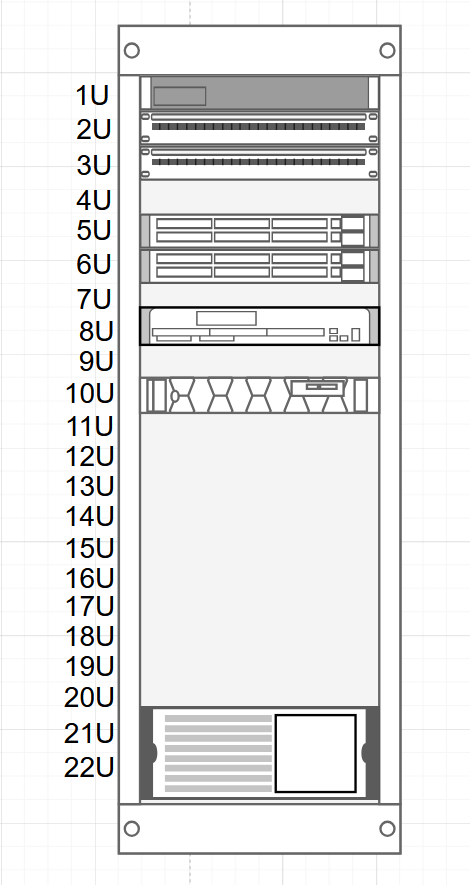
1. Opis struktury okablowania

1.1. Szkielet sieci

Podstawą infrastruktury teletechnicznej budynku jest wielomodowy światłowód, który gwarantuje wysoką przepustowość i niezawodność transmisji danych. Każde piętro posiada własną szafę dystrybucyjną, połączoną z centralnym punktem dystrybucyjnym (CPD) światłowodowymi patchcordami, biegnącymi przez dedykowane szachty.  
CPD ulokowany został na 2 piętrze, chroniony jest systemem monitoringu wizyjnego oraz kartą dostępową RFID wydawaną jedynie uprawnionym osobom. W szafie dystrybucyjnej CPD znaleźć można tożsame urządzenia z szaf dystrybucyjnych z innych pięter: 2 patchpanele, 2 switche access, 1 switch core, 1 APC, jednocześnie ekskluzywnie znajdziemy w niej przełącznicę FO, router oraz IDS\IPS.

Schemat mocowań rack jest wspólny dla wszystkich pięter:

|  |  |  |
| --- | --- | --- |
| 1U | Przełącznica światłowodowa | Uplink budynku |
| 2U | Patchpanel 1 | Organizacja kabli sieciowych |
| 3U | Patchpanel 2 | Organizacja kabli sieciowych |
| 4U | Pusty (dla organizacji kabli) | Zapewnia lepszy przepływ powietrza |
| 5U | Switch Access (Cisco 2960) | Blisko patchpaneli dla krótszych patchcordów |
| 6U | Switch Access (Cisco 2960) | Blisko patchpaneli dla krótszych patchcordów |
| 7U | Switch Core (Cisco 3650) | Blisko patchpaneli dla krótszych patchcordów |
| 8U | Pusty | Przestrzeń wentylacyjna |
| 9U | Router Cisco 2911 | Odbiór usługi, dostęp do Internetu, NAT |
| 10U | Pusty | Przestrzeń wentylacyjna |
| 11U | IDS\IPS | Ochrona sieci |
| … | Pusty | Dystans od UPS dla chłodzenia, miejsce na rozbudowę. |
| 21U | UPS APC SMT1500RM2UC | Podtrzymanie zasilania |
| 22U |



Rysunek 4 Wizualizacja szafy rack

1.2. Okablowanie pionowe

Okablowanie pionowe zostało poprowadzone w specjalnie zaplanowanych szachtach teletechnicznych i szybach instalacyjnych, umiejscowionych w bezpośrednim sąsiedztwie szybu podnośnika dźwigowego. To rozwiązanie zapewnia łatwy dostęp serwisowy, jednocześnie chroniąc przewody przed przypadkowym uszkodzeniem i izolując od wpływu użytkowników oraz warunków zewnętrznych. W szachtach biegną magistrale oparte o światłowód wielomodowy zakończone złączami LC/PC do modułów SFP+ 10G, co uodparnia sieć na fragmentację i kolejkowanie transmisji, zapewnia pasmo zdolne przenieść pełne obciążenie pojedynczych użytkowników bez wpływu na pracę na resztę sieci i zagwarantuje odpowiednią przepustowość.

1.3. Okablowanie poziome

W ramach infrastruktury poziomej zastosowano 3 systemy prowadzenia kabli i ustanawiania gniazd abonenckich, dostosowane do specyfiki montażu urządzeń oraz stanowisk pracy:

* **Podłoga teletechniczna i korytka kablowe**  
  Tam, gdzie kable biegną w obrębie stanowisk roboczych, zostały one ukryte w metalowych trasach kablowych i peszlach, prowadzonych pod plastrami podłogi teletechnicznej. Takie rozwiązanie zapewnia łatwość modernizacji, gdy zajdzie potrzeba dostosowania infrastruktury do nowych wymagań użytkowników.
* **Gniazda abonenckie i floorboxy**  
  W miejscach, gdzie biurka są ustawione przy ścianach, zastosowano standardowe gniazda abonenckie, montowane na wysokości roboczej. Natomiast w przestrzeniach typu open space, gdzie stanowiska oddalone są od ścian, przewidziano floorboxy – estetyczne, wbudowane w podłogę moduły, wyposażone w gniazda keystone, umożliwiające łatwe podłączenie sprzętu bez konieczności prowadzenia kabli „na widoku”.
* **Okablowanie w sufitach podwieszanych**  
  Urządzenia montowane powyżej 1 metra od poziomu podłogi, takie jak punkty dostępowe WiFi (AP), zostały podłączone za pomocą UTP kat. 6A, prowadzonych w przestrzeni sufitu kasetonowego. To rozwiązanie zapewnia minimalną ingerencję w estetykę pomieszczeń, a jednocześnie umożliwia łatwe dostosowanie i ewentualne rozbudowywanie sieci bez konieczności kucia ścian.

1.4. Metodologia opisów.

Sieć cechuje się czytelnym i konsekwentnym nazewnictwem, które ułatwia zarządzanie i diagnostykę.

* Każde gniazdo posiada unikalną nazwę zgodną z formatem:

numer piętra - numer portu w patchpanelu, np. p1-1, p3-27.

* Okablowanie w szafie utrzymane jest w schemacie "1 do 1", co oznacza, że porty switcha odpowiadają numerom portów w patchpanelu w jak największym stopniu.
* Wszystkie patchcordy są opisane na obu końcach, aby uniknąć konieczności ręcznego śledzenia trasy przewodów w szafie rack.
* Każdy switch i router w sieci otrzymuje oznaczenie według schematu:

numer piętra - s/r (switch/router) numer urządzenia

* Komputery, drukarki, punkty dostępu WiFi i inne urządzenia klienckie oznaczane są według wzoru:   
  typ urządzenia - numer piętra - numer gniazda abonenckiego, np. PC-p2-6.

Poniżej znajduje się spis wszystkich połączeń w okablowaniu poziomym sieci. Uwzględniono w nim ww. nazewnictwo, numery portów, długości kabli, numery gniazd oraz typy urządzeń odbiorczych. W spisie **nie znajduje się okablowanie pionowe**, ponieważ wszystkie patchcordy światłowodowe prowadzone są przez wcześniej przygotowane szachty i prowadzą od portu do portu urządzeń aktywnych szkieletu. Do zapoznania z ich logiką posłużyć może dołączony plik Cisco Packet Tracer (.pkt).

2. Opis struktury logicznej.

2.1. Oddzielne pule adresowe dla każdego piętra i typu urządzeń.

| **Piętro** | **VLAN** | **Podsieć** | **Przeznaczenie** |
| --- | --- | --- | --- |
| 1 | 110 | 10.1.10.0/24 | PC piętro 1 |
| 1 | 120 | 10.1.20.0/24 | Drukarki piętro 1 |
| 1 | 130 | 10.1.30.0/24 | Wi-Fi piętro 1 |
| 2 | 210 | 10.2.10.0/24 | PC piętro 2 |
| 2 | 220 | 10.2.20.0/24 | Drukarki piętro 2 |
| 2 | 230 | 10.2.30.0/24 | Wi-Fi piętro 2 |
| 3 | 310 | 10.3.10.0/24 | PC piętro 3 |
| 3 | 320 | 10.3.20.0/24 | Drukarki piętro 3 |
| 3 | 330 | 10.3.30.0/24 | Wi-Fi piętro 3 |

**Uzasadnienie:**

1. **Izolacja pionowa** (między piętrami) – zapobiega rozprzestrzenianiu się ruchu broadcastowego warstwy 2 i zwiększa bezpieczeństwo.
2. **Izolacja pozioma** (wewnątrz pięter) – separuje różne typy urządzeń, ułatwiając zarządzanie politykami sieciowymi.
3. **Skalowalność** – łatwe dodawanie nowych pięter lub typów urządzeń bez przebudowy całej sieci.

Każdy VLAN jest osobną **domeną broadcastową**, co izoluje ruch między piętrami.

2.2. Schemat logiczny adresacji

|  |  |  |  |
| --- | --- | --- | --- |
|  | VLAN PC (y) | VLAN Drukarki (y) | VLAN Wi-Fi (y) |
| Piętro 1 (x) | 10.1.10.0/24 | 10.1.20.0/24 | 10.1.30.0/24 |
| Piętro 2 (x) | 10.2.10.0/24 | 10.2.20.0/24 | 10.2.30.0/24 |
| Piętro 3 (x) | 10.3.10.0/24 | 10.3.20.0/24 | 10.3.30.0/24 |

**10.x.y.z/24**, gdzie:  
**x** – numer piętra

**y** – rodzaj urządzenia

**z** – numer gniazda na piętrze

2.3. VLAN 69 – Zarządzanie (MGMT)

* **Adresacja**: 172.16.69.0/24
* **Przypisanie**: Wszystkie urządzenia, do których potrzeba zdalnego zarządzania (przełączniki, routery) mają adresy w tej podsieci.

| **VLAN** | **Podsieć** | **Przeznaczenie** |
| --- | --- | --- |
| 69 | 172.16.69.1/24 | Switch p1-s1-core |
| 69 | 172.16.69.2/24 | Switch p2-s1-core |
| 69 | 172.16.69.3/24 | Switch p3-s1-core |
| 69 | 172.16.69.11/24 | Switch p1-s2-access |
| 69 | 172.16.69.12/24 | Switch p1-s3-access |
| 69 | 172.16.69.21/24 | Switch p2-s2-access |
| 69 | 172.16.69.22/24 | Switch p2-s3-access |
| 69 | 172.16.69.31/24 | Switch p3-s2-access |
| 69 | 172.16.69.32/24 | Switch p3-s3-access |
| 69 | 172.16.69.10/24 | Router p2-r1-core |
| 69 | 172.16.69.20/24 | Router p2-r2-core |

2.3. VLAN 100 – Internet Access

* **Adresacja**: 10.100.100.0/24
* **Przypisanie**: Urządzenia biorące udział w trasowaniu do zewnątrz/wewnątrz sieci (przełącznik p2-s1-core oraz routery) i

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 100 | | | | 10.100.100.1/24 | Wirtualny interfejs HSRPv2. |
| 100 | | | | 10.100.100.2/24 | Interfejs trunk p2-s1-core vlan 100. |
| 100 | | | | 10.100.100.10/24 | Subinterfejs gig0/3/0.100 p2-r1-core. |
| 100 | | | | 10.100.100.20/24 | Subinterfejs gig0/3/0.100 p2-r2-core. |
|  |  |  |

3. Wykorzystane technologie.

3.1. Trunking na styku warstw access i core.  
  
W sieci zaimplementowany został ether-channel zwiększający przepustowość ze 100 do 800Mbps między warstwami access-core (Na sprzęcie fizycznym wykonałbym switch-stack master-slave, ale packet tracer nie obsługuje takiego rozwiązania). W ten sposób każdy host ma do dyspozycji 100Mbps i w przypadku zainfekowania i próby ataku DoS przez wysycenie łącza, maksymalnie jest w stanie wysycić 100Mbps, a pozostałe 700Mbps jest współdzielone pomiędzy resztę hostów. Rozwiązanie jest również przyjazne kosztowo, korzystamy z tańszych, setkowych switchów Cisco, np. Catalyst 2960.

3.2. Switching & Routing.

Intervlan routing odbywa się na switchach L3 klasy enterprise, tu Catalyst 3650, na nim również działa serwer DHCP rozdysponowujący adresy wewnątrz vlanów. Wykorzystanie tych switchów oznacza utworzenie warstwy core, w której istnieje dostęp zarządzający, switche są adresowane. Urządzenia brzegowe działają w oparciu o HSRP, oferując pojedynczy, wirtualny interfejs bramy domyślnej. Taki router służy przede wszystkim, jako brama do bezpiecznych zdalnych połączeń VPN oraz do trasowania ruchu w relacji in-out, potocznie zwanej NATownicą, dzięki czemu bezpieczna, skalowalna sieć ma dostęp do Internetu.

HSRP działa w wersji 2, jako jeden adres ustawiony na portach dwóch routerów, od strony LAN. Warto nadmienić, że zastosowano technikę „router-on-a-stick”, aby zachować routing intervlanowy na switchach core oraz wykorzystać pojedynczy interfejs routera do trasowania ruchu z vlanu zarządzającego 69 oraz vlanu dostępu do Internetu 100. Po drugiej stronie routera na gig0/1/0 ustawiono fikcyjny adres od ISP, dla większej czytelności skorzystano z adresów prywatnych klasy C, w realiach zawodowych, na interfejsach brzegowych obydwu routerów w HSRP widniałyby dedykowane adresy IP. W warunkach laboratoryjnych posłużyłem się symulatorem Internetu w postaci hopki – routera – na którym wykonałem routing statyczny.

**Routing statyczny:**209.165.200.0/24 via 192.168.1.1 to ruch z naszej sieci w stronę serwera, bez tego nie ma komunikacji na zewnątrz.  
10.100.100.0/24 via 192.168.1.1 to ruch od strony serwera do naszej sieci, bez tego nie ma komunikacji powrotnej.

Pingi do serwera szły wyłącznie z routerów w HSRP, ale na p2-s1-core ustawiłem:

Ip route 209.165.200.0/24 via 10.100.100.1 (adres wirtualny routera).

Ponadto trasa domyślna 0.0.0.0 0.0.0.0 10.100.100.1 zapewniła trasowanie ruchu przez interfejs wirtualny, a na routerach w HSRP utworzono **dedykowane access-listy** dla adresacji vlanów:

access-list 1 permit 10.1.30.0 0.0.0.255 oraz dopisano do nat:

ip nat inside source list 1 interface gig0/1/0 overload, ze wskazaniem na interfejs brzegowy routera dla ruchu wychodzącego. Dodano dedykowane adresacjom vlanów trasy powrotne:   
ip route 10.1.30.0 255.255.255.0 10.100.100.2, we wskazaniem na interfejs switcha p2-s1-core, w vlanie 100 (dostępu do Internetu).

3.2. Port-security, DHCP snooping, Dynamic ARP Inspection.

* **Port-security:** Jako zabezpiecznie m.in. przed MAC Flooding oraz podpinaniem nieautoryzowanego sprzętu do sieci wprowadzono port-security na portach access. Ze względu na to, że adresy alokowane są statycznie na każdym hoście połączonym kablowo, zdecydowałem się na ograniczenie do 1 adresu na port z parametrem sticky oraz trybem reagowania jako shutdown.
* **DHCP Snooping:** Dynamiczna alokacja adresów występuje jedynie w VLANACH 130,230,330, tam wprowadzono mechanizm DHCP Snooping mający za zadanie ograniczyć wpływ ataku DHCP spoofing/starvation. Porty zaufane aktywowano jedynie na łączach uplinkowych, pozostałe porty znajdują się w stanie untrusted.
* **DAI:** Przed atakami ARP spoofing/posoning i łączącymi się z nimi MITM, chroni wprowadzone zabezpieczenie Dynamic ARP Inspection, korzystające z wprowadzonego wcześniej DHCP Snooping Binding.

4.Podsumowanie zbiorcze

Tabela 1 Urządzenia aktywne, pasywne i materiały

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Rodzaj urządzenia** | **Zastosowany model** |
| 1 | Router core | Cisco 2911 |
| 2 | IDS/IPS | Palo Alto PA-850 |
| 3 | Switch access | 3x Cisco Catalyst 3650 |
| 4 | Switch core | 6x Cisco Catalyst 2960 |
| 5 | UPS | 3x UPS APC SMT1500RM2UC |
| 6 | Patchpanel | 6x Netrack 24 port cat. 6A |
| 7 | WiFi AP | 4x Ubiquiti Unifi U6+ 802.11ax + Unifi Controler |
| 8 | Drukarka sieciowa | 6x Brother HL-B2080DW |
| 9 | Okablowanie FO | 4x 20m Patchcord FO LC/PC |
| 10 | Okablowanie UTP | 1262m Bitner UTP cat. 6A |
| 11 | Moduły keystone | 72x Keystone RJ45 Digitus DN-93502 |
| 12 | RJ45 | 96x UTP RJ45 |
| 13 | Szafa rack | 3x szafa Rack 19'' 22U S6122DPII |