Ostoja

Checklista wdrożenia sieci UniFi

Dowody, testy i odbiór konfiguracji krok po kroku



Ostoja

Jak zapisywać wynik i dowód

Jedna kratka oznacza jeden sprawdzony warunek. Zaznacz OK dopiero po teście; **NIE** oznacza błąd, **ND** wymaga uzasadnienia.



- ☐ **Tożsamość:** lokalizacja, wersja i urządzenie zgadzają się z kartą; dowód: numer wpisu lub odczyt panelu.
- ☐ **Stan początkowy zapisany:** znasz poprzednią wartość i sposób jej przywrócenia.
- ☐ **Kryterium określone przed testem:** wiadomo, jaki wynik jest poprawny i jaki dostęp ma być zablokowany.
- ☐ **Dowód powtarzalny:** wpis zawiera czas, klienta, IP oraz faktyczny wynik testu.
- ☐ **Dane chronione:** brak haseł, kodów MFA, kluczy prywatnych i danych zbędnych do odbioru.
- ☐ **Błąd ma właściciela:** termin poprawki oraz decyzja o kontynuacji lub wycofaniu są zapisane.

✓ **Przykład:** VLAN 30 | 10:20 | laptop T01 | HTTPS działa | panel UniFi zablokowany | dowód T-07 | OK.

Lokalizacja: _____ Data: _____ Wykonawca: _____

Test / kryterium: _____

Wynik / dowód / decyzja: _____

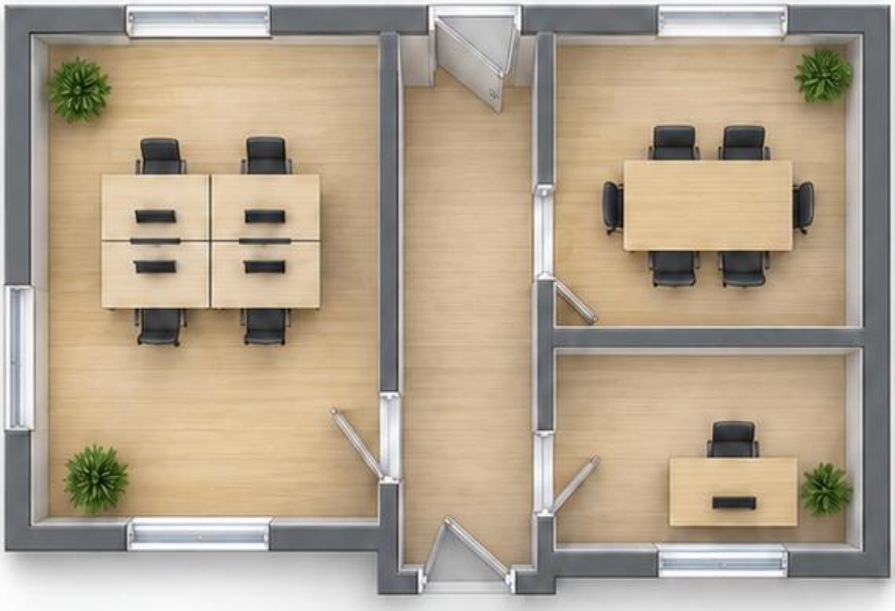
Źródła: [1], [8]

Ostoja

Rozpoznanie instalacji

Wypełnij przed podłączeniem nowej bramy. Źródłem są rozmowa z właścicielem, oględziny i odczyty działającej sieci.





1. ☐ **Zakres uzgodniony:** lista pomieszczeń, użytkowników i usług ma akceptację właściciela.
2. ☐ **Operator rozpoznany:** zapisano metodę WAN, zakończenie łącza i kontakt serwisowy; dane potwierdza dokument usługi.
3. ☐ **Role urządzeń ustalone:** wiadomo, gdzie działa routing, DHCP i aplikacja Network.
4. ☐ **Wersje zapisane:** model hosta, Network, UniFi OS lub system serwera odpowiadają faktycznemu odczytowi.
5. ☐ **Dostęp awaryjny sprawdzony:** laptop otwiera lokalny panel i właściwą lokalizację.
6. ☐ **Okno prac uzgodnione:** określono przerwę, osobę decyzyjną i warunek przerwania.

Przykład: Kraków, biuro 18 osób; CloudKey + router operatora; lokalny panel sprawdzony z T01.

Lokalizacja / zakres: _____

Usługi krytyczne / właściciel: _____

WAN / dokument operatora: _____

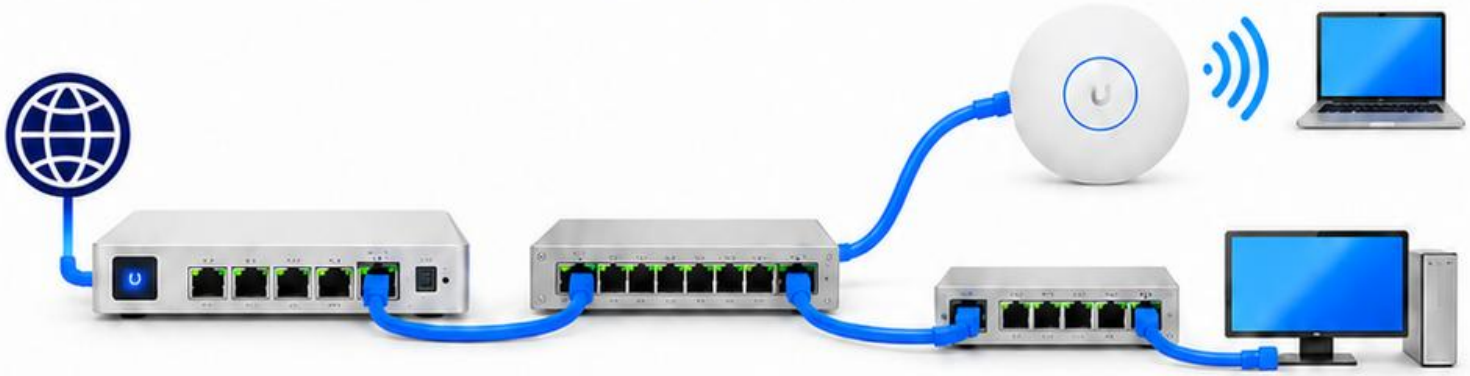
Okno / kontakt / dowód dostępu: _____

Źródła: [9], [10], [11]

Ostoja

Plan adresacji

Sprawdź cały plan łącznie z VPN i oddziałami. Każdy wiersz musi wskazywać sieć, VLAN, router i źródło konfiguracji klientów.



Podsieci rozłączne:
porównanie prefiksów nie wykazało przecięć LAN, WAN prywatnej i VPN.

Bramy poprawne:
należą do właściwych podsieci i nie są przydzielane klientom.

Pule DHCP wystarczające:
liczba adresów pokrywa uzgodnioną liczbę jednoczesnych klientów.

Adresy infrastruktury spisane:
rezerwacje i ustawienia ręczne nie powodują kolizji.

DNS określony:
znana jest obsługa nazw lokalnych i publicznych; testy mają wskazane nazwy.

IPv6 uwzględniony:
zapisano delegację i osobne /64 albo uzasadniono brak wdrożenia.

Przykład: Pracownicy | VLAN 20 | 192.168.20.0/24 | brama .1 | DHCP .100–.220.

Sieć / VLAN / prefiks: _____

Brama / DHCP / DNS: _____

Adresy stałe / rezerwacje: _____

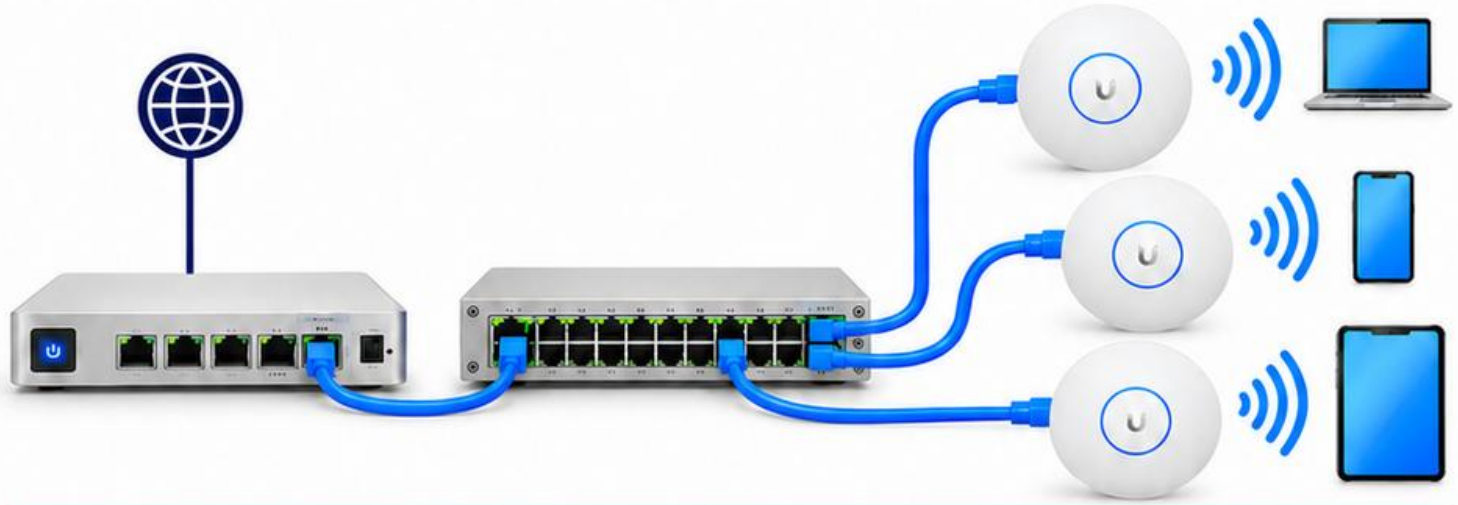
IPv6 / kolizje / dowód: _____

Źródła: [1], [12], [13]

Ostoja

Inwentarz i zasilanie

Porównaj rejestr z fizycznym sprzętem. Moc i standard zasilania sprawdzaj dla konkretnego modelu oraz używanego zasilacza.



- [ ] **1.** **Tożsamość potwierdzona:** model i MAC każdego urządzenia odpowiadają etykiecie.
- [ ] **2.** **Przewody opisane:** dla uplinków zapisano oba porty i lokalizację patchpanelu.
- [ ] **3.** **Standard PoE zgodny:** port lub injektor spełnia wymagania odbiornika z dokumentacji.
- [ ] **4.** **Budżet policzony:** suma mocy maksymalnych mieści się w dostępnym budżecie switcha.
- [ ] **5.** **Zaplecze energetyczne sprawdzone:** wskazano obwód zasilania, UPS i planowane zachowanie przy zaniku.
- [ ] **6.** **Próba jednoczesnego startu zakończona:** brak restartów odbiorników, a odczyt poboru zapisano jako dowód.

Przykład: 3 AP × 20 W = 60 W; budżet 80 W; zapas projektu 20 W.

1. Urządzenie / MAC / miejsce: _____
2. Port / przewód / standard PoE: _____
3. Maksimum / budżet / zapas: _____
4. Test startu / wynik / dowód: _____

Źródła: [6], [4]

Ostoja

Kontroler i dostęp

Sprawdź konta w oddzielnej sesji. Odbiór wymaga działającej ścieżki lokalnej oraz potwierdzonego zakresu uprawnień.

- ☐ **Host właściwy:** lokalizacja, model i wersja Network zgadzają się z dokumentacją.
- ☐ **Własność ustalona:** osoba odpowiedzialna ma dostęp i potwierdziła sposób przekazania instalacji.
- ☐ **Konta imienne działają:** każdy administrator loguje się własnym kontem.
- ☐ **Uprawnienia przetestowane:** potrzebne funkcje są dostępne, a zakres poza obowiązkami pozostaje niedostępny.
- ☐ **MFA i odzyskiwanie gotowe:** sprawdzono dodatkową metodę; w karcie zapisano wyłącznie miejsce przechowywania.
- ☐ **Dostęp lokalny potwierdzony:** logowanie po IP działa z laptopa serwisowego; zapisano port i adres hosta.



Przykład: Serwis widzi tylko GDN-Magazyn; właściciel zalogował się niezależnie; dowód A-03.

Host / IP / port / wersja: _____

Właściciel / zastępca: _____

Rola / lokalizacja / test: _____

MFA / dostęp lokalny / dowód: _____

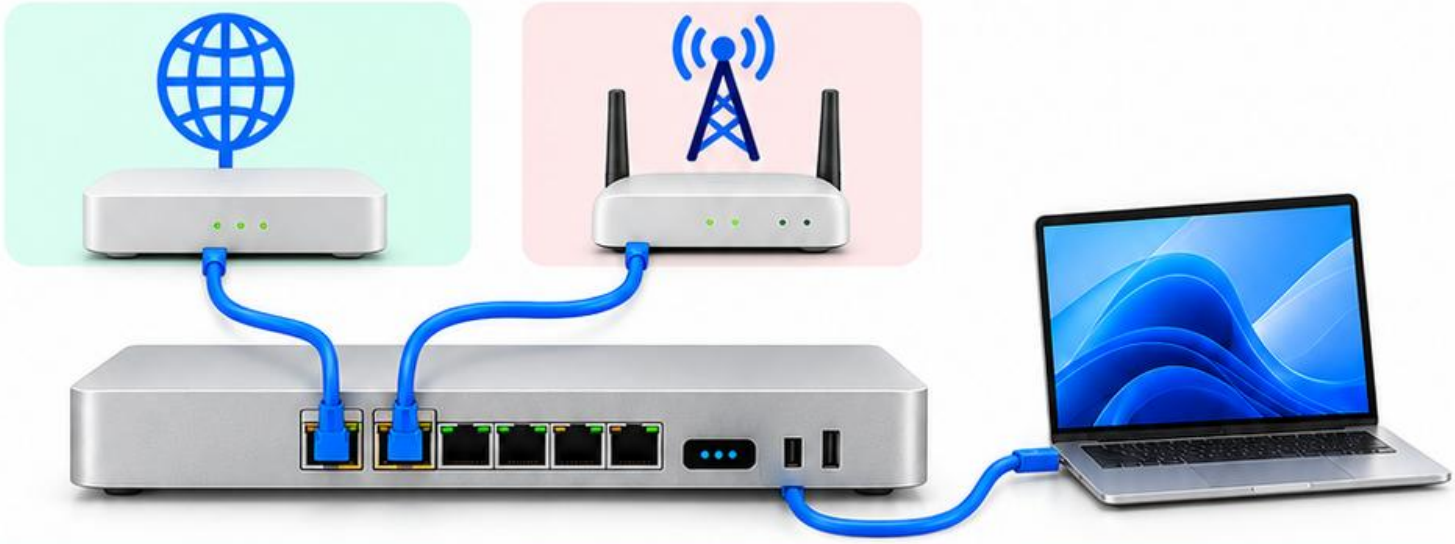
Źródła: [14], [15], [10]

Ostoja

Brama i internet

Testuj z klienta przewodowego oraz zapisuj stan WAN. Sprawdź rzeczywistą usługę, a nie tylko ikonę dostępności.

- ☐ **Parametry zgodne:** metoda IP, ewentualny VLAN i dane PPPoE odpowiadają dokumentowi operatora.
- ☐ **DNS odpowiada:** udokumentowano zapytanie oraz udane otwarcie uzgodnionej strony HTTPS.
- ☐ **Adresacja WAN poprawna:** IP, brama i prefiks nie kolidują z LAN.
- ☐ **Zapasowy WAN sprawdzony, jeśli istnieje:** nowe połączenie działa po kontrolowanej awarii podstawowego.
- ☐ **NAT rozpoznany:** zapisano obecność routera pośredniego i potwierdzenie CGNAT lub publicznego adresu.
- ☐ **Powrót odebrany:** po przywróceniu łącza działają usługi krytyczne; IPv6 sprawdzono osobno, jeżeli używane.





Przykład: WAN1 DHCP; WAN2 LTE failover; po teście HTTPS działa; usługa przychodząca wymaga publicznego IPv4.

WAN / metoda / dokument: _____

Adres / NAT / DNS: _____

Awaria / przełączenie / powrót: _____

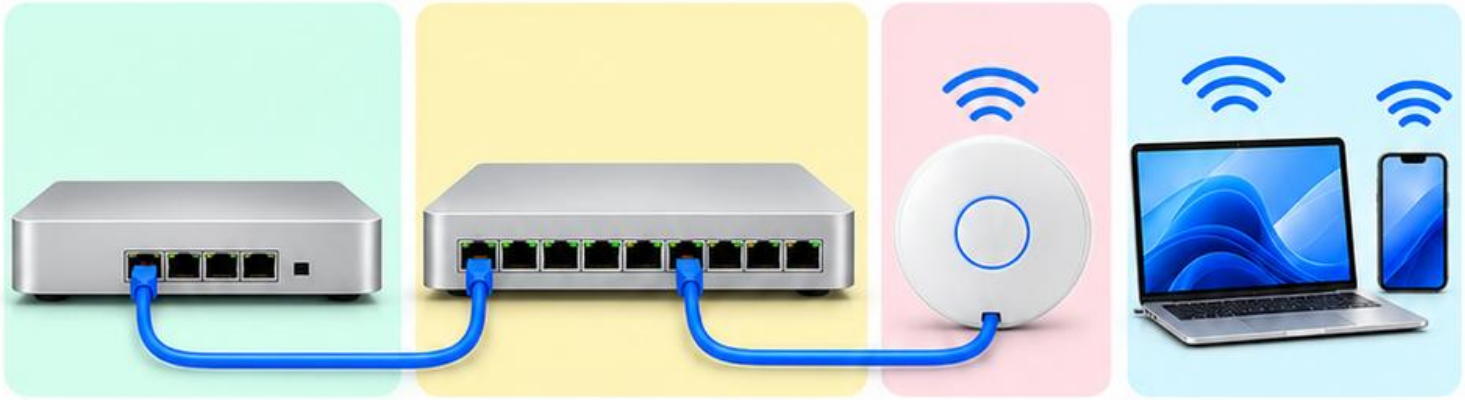
IPv6 / usługa / dowód: _____

Źródła: [16], [17], [18], [13]

Ostoja

VLAN-y i porty

Porównaj konfigurację całej ścieżki: router, uplink, switch, port końcowy lub AP. Testuj po jednym reprezentatywnym kliencie na segment.



- [ ] **VLAN ID spójne:** numery odpowiadają planowi na wszystkich urządzeniach.
- [ ] **Router wskazany:** wiadomo, gdzie działają DHCP i polityki między sieciami.
- [ ] **Uplinki przenoszą wymagane tagi:** nie ma brakującego VLAN na żadnym odcinku.
- [ ] **Porty dostępowe poprawne:** klient trafia do zamierzonej sieci i otrzymuje właściwe parametry.
- [ ] **Porty AP zgodne z projektem:** sieć zarządzania i VLAN-y SSID mają działającą drogę.
- [ ] **Dostęp administracyjny zachowany:** po zmianie nadal działa lokalny panel oraz zarządzanie urządzeniami.

Przykład: SW01/8 → AP02; zarządzanie VLAN 10; SSID pracowników VLAN 20 i gości VLAN 30.

Trasa / oba porty: _____

VLAN natywny / tagowane: _____

Klient / IP / DHCP: _____

Dostęp lokalny / wynik / dowód: _____

Źródła: [1], [4], [10]

Ostoja

Wi-Fi i goście

Sprawdź urządzenia reprezentujące rzeczywistych użytkowników.
Wydziel próbę łączności od testu izolacji oraz od pomiaru pokrycia.



- ☐ **SSID przypisane:** nazwa, VLAN i lista nadających AP odpowiadają projektowi.
- ☐ **Zabezpieczenia zgodne:** klient testowy łączy się przy przyjętej konfiguracji WPA i PMF.
- ☐ **Adresacja działa:** klient Wi-Fi otrzymuje właściwe DHCP, bramę i DNS.
- ☐ **Zasięg zmierzony:** zapisano wynik w punktach krytycznych, model klienta oraz pasmo.
- ☐ **Goście odizolowani:** internet działa, a zabronione usługi LAN i komunikacja między klientami nie przechodzą.
- ☐ **Kraj i pasma potwierdzone:** instalacja w Polsce korzysta ze zgodnych ustawień modelu i miejsca montażu.

Przykład: Recepcja: telefon T02 łączy się z Goście; HTTPS działa; panel Network pozostaje niedostępny.

SSID / VLAN / AP: _____

Klient / pasmo / punkt pomiaru: _____

DHCP / DNS / izolacja: _____

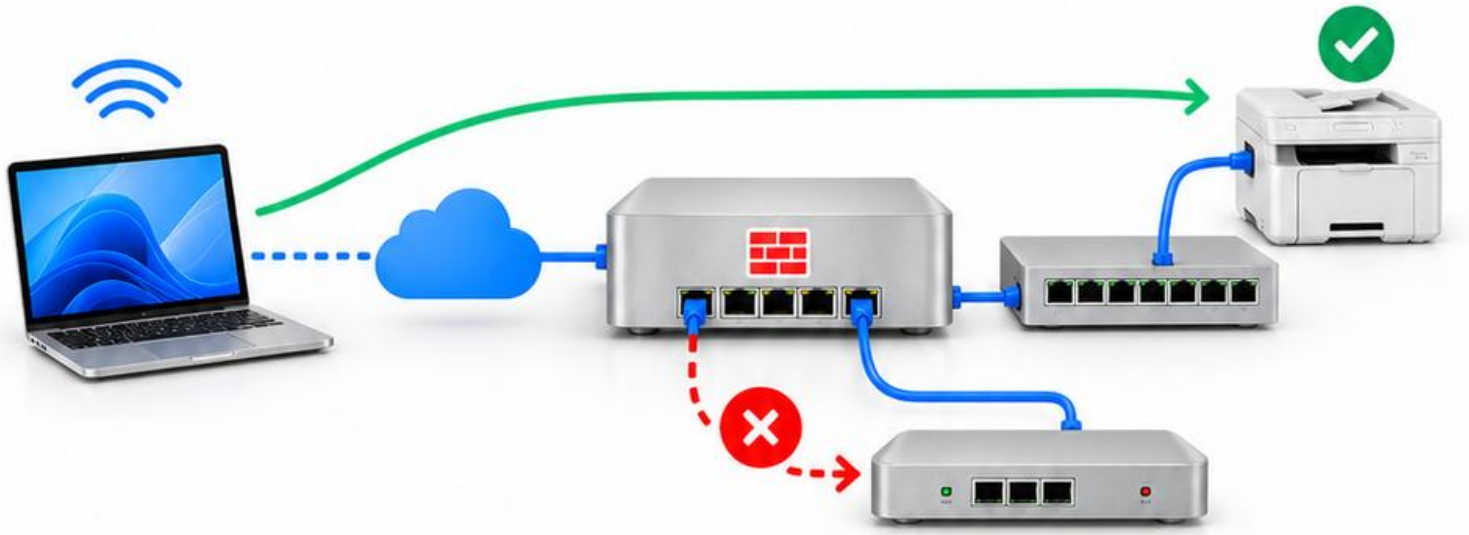
Kraj / wynik / dowód: _____

Źródła: [2], [19], [20], [21]

Ostoja

Firewall i VPN

Porównaj reguły z uzgodnioną macierzą dostępu. Tunel aktywny nie oznacza jeszcze poprawnego routingu, DNS ani właściwego zakresu uprawnień.



- [ ] **Typ zapory ustalony:** udokumentowano strefy albo konfigurację starszą zgodną z wersją.
- [ ] **Kierunki poprawne:** źródło, cel, protokół i port każdej wymaganej usługi odpowiadają macierzy.
- [ ] **Kolejność sprawdzona:** potrzebny wyjątek nie jest przesłonięty wcześniejszą blokadą.
- [ ] **IPv4 i IPv6 przetestowane:** zakazane połączenia nie omijają polityki drugim protokołem.
- [ ] **VPN działa spoza LAN:** klient zestawia tunel i dociera do wskazanej usługi, używając właściwego DNS.
- [ ] **Zakres VPN ograniczony:** próba dostępu poza uprawnieniami nie przechodzi; klucze prywatne nie trafiają do protokołu.

Przykład: Pracownik VPN drukuje do wybranej drukarki; dostęp do panelu bramy jest zablokowany.

Reguła / źródło / cel / port: _____

VPN / klient / sieć zewnętrzna: _____

Test dozwolony / zakazany: _____

IPv6 / wynik / dowód: _____

Źródła: [3], [22], [13]

Ostoja

Wydajność i izolacja

Ustal kryteria przed pomiarem. Porównuj ten sam serwer, klienta i warunki; zapisz osobno wynik lokalny oraz wynik przez internet.



- [ ] **Warunki zapisane:** model klienta, łącze, pasmo, miejsce i czas umożliwiają powtórzenie testu.
- [ ] **Punkt odniesienia zmierzony:** przewodowy klient działa poprawnie przed oceną Wi-Fi.
- [ ] **Usługa docelowa spełnia kryterium:** zapisano rzeczywisty wynik, a nie samą prędkość połączenia radiowego.
- [ ] **Opóźnienie i utrata pakietów ocenione:** test ma uzgodniony cel oraz czas pomiaru.
- [ ] **Izolacja sprawdzona pozytywnie i negatywnie:** dozwolona usługa działa, zabroniony konkretny port pozostaje niedostępny.
- [ ] **Obciążenie reprezentatywne:** wynik powtórzono przy typowej liczbie użytkowników albo zapisano ograniczenie próby.

Przykład: Kryterium projektu: plik 500 MB do serwera LAN w czasie ≤60 s; wynik 42 s; dowód P-04.

Klient / serwer / warunki: _____

Kryterium / pomiar: _____

Test zakazany / konkretny port: _____

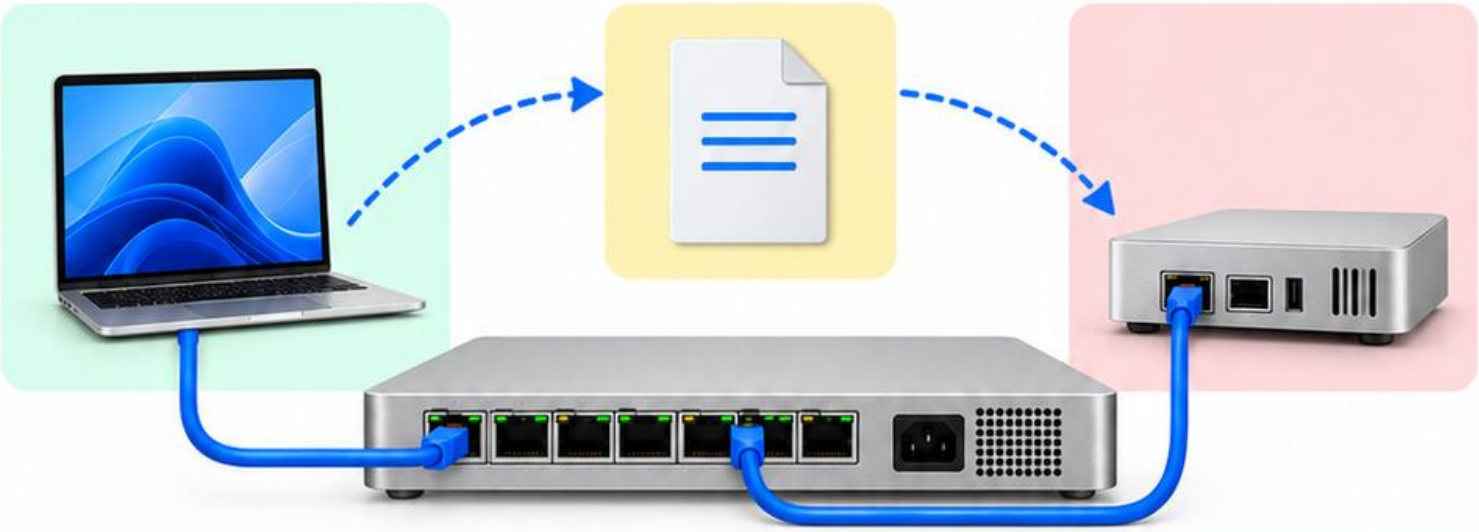
Ograniczenie / wynik / dowód: _____

Źródła: [19], [20], [18]

Ostoja

Kopia i odzyskiwanie

Kopia ma umożliwiać uzgodnione odtworzenie instalacji. Testuj w odseparowanym środowisku i nie uruchamiaj dwóch konkurujących hostów zarządzających.



- [ ] **Zakres kopii znany:** zapisano, czy obejmuje konsolę, czy aplikację Network.
- [ ] **Kopia aktualna:** data, wersja źródłowa i nazwa pliku odpowiadają ostatniej zaakceptowanej konfiguracji.
- [ ] **Przechowywanie bezpieczne:** plik znajduje się poza odtwarzanym urządzeniem i ma kontrolowany dostęp.
- [ ] **Dane odzyskiwania dostępne:** upoważniona osoba zna miejsce przechowywania, bez ujawniania sekretów w karcie.
- [ ] **Próba wykonana:** host testowy przyjął kopię zgodną z procedurą i wersją; wynik zapisano.
- [ ] **Powrót do pracy określony:** opisano kolejność podłączeń, kryteria sukcesu oraz czas odtworzenia.

Przykład: Kopia Network pobrana po odbiorze; test na odseparowanym hoście; odtworzono listę sieci i urządzeń.

Plik / data / zakres / wersja: _____

Miejsce / odpowiedzialny: _____

Test / czas / wynik: _____

Dostęp awaryjny / dowód: _____

Źródła: [8], [10]

Ostoja

Odbiór i pozostałe zadania

Podpis potwierdza sprawdzony zakres oraz jawnie zapisane ograniczenia. Niezakończone zadanie musi mieć właściciela, termin i wpływ na użytkowników.



- [ ] **Zakres wdrożenia zgodny:** lista przekazanych sieci, urządzeń i usług odpowiada zamówieniu.
- [ ] **Testy zakończone:** każdy wymagany warunek ma wynik i identyfikator dowodu.
- [ ] **Dokumentacja przekazana:** mapa, inwentarz, adresacja i porty odpowiadają stanowi końcowemu.
- [ ] **Dostęp przekazany:** właściciel loguje się samodzielnie; nadmiarowe konta serwisowe objęto uzgodnioną decyzją.
- [ ] **Kopia i procedura dostępne:** wskazana osoba potwierdziła miejsce przechowywania i sposób użycia.
- [ ] **Zadania otwarte uzgodnione:** wpisano odpowiedzialnego, termin, obejście i kryterium zamknięcia.

Przykład: Zadanie Z-02; pomiar magazynu po dostawie regałów; Jan; 28.10; brak wpływu na odebrane biuro.

Zadanie / wpływ / właściciel / termin: _____

Zakres / protokół testów: _____

Przekazane pliki / dostęp / kopia: _____

Odbierający / wykonawca / data: _____

Źródła: [8], [14], [1]

Ostoja • Źródła • 1/2

Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w materiale.

[1] Tworzenie sieci VLAN

https://help.ui.com/hc/en-us/articles/9761080275607

[2] Tworzenie sieci Wi-Fi

https://help.ui.com/hc/en-us/articles/26136823938583

[3] Zapora strefowa

https://help.ui.com/hc/en-us/articles/115003173168

[4] Ustawienia przełączników

https://help.ui.com/hc/en-us/articles/33402927617047

[6] Tryby i dostępność PoE

https://help.ui.com/hc/en-us/articles/115000263008

[8] Kopie i migracja

https://help.ui.com/hc/en-us/articles/360008976393

[9] Pierwsze uruchomienie UniFi

https://help.ui.com/hc/en-us/articles/4416276882327

[10] Zarządzanie lokalne

https://help.ui.com/hc/en-us/articles/28457353760919

[11] Wybór hosta zarządzania

https://help.ui.com/hc/en-us/articles/30127033090071

[12] Serwer DHCP

https://help.ui.com/hc/en-us/articles/360012097513

Źródła • 2/2

Ostoja • Źródła • 2/2

Dokumentacja Ubiquiti. Stan sprawdzenia: 21.10.2026. Numery odpowiadają odwołaniom w materiale.

[13] Konfiguracja IPv6

https://help.ui.com/hc/en-us/articles/115005868927

[14] Dodawanie administratorów

https://help.ui.com/hc/en-us/articles/28692158912279

[15] Uwierzytelnianie wieloskładnikowe

https://help.ui.com/hc/en-us/articles/115012986607

[16] Failover i porty WAN

https://help.ui.com/hc/en-us/articles/360052548713

[17] Dynamiczny DNS

https://help.ui.com/hc/en-us/articles/9203184738583

[18] Diagnostyka DNS

https://help.ui.com/hc/en-us/articles/17484948645015

[19] Stabilność i opóźnienia Wi-Fi

https://help.ui.com/hc/en-us/articles/221029967

[20] Izolacja sieci i klientów

https://help.ui.com/hc/en-us/articles/18965560820247

[21] Regiony obsługujące 6 GHz

https://help.ui.com/hc/en-us/articles/8691786444567

[22] Serwer WireGuard

https://help.ui.com/hc/en-us/articles/115005445768