Ostoja

Wizualny poradnik rozwiązywania problemów UniFi

Od objawu do potwierdzonej naprawy



Ostoja · Drzewo diagnostyczne

Objaw: użytkownik zgłasza, że sieć nie działa.

Nie zakładaj od razu awarii internetu ani punktu dostępowego.

1. Test pierwszy: sprawdź drugiego klienta

w tym samym miejscu. Następnie porównaj klienta przewodowego z bezprzewodowym.



Decyzja:
jeśli problem dotyczy jednego urządzenia, badaj jego profil i konfigurację.



Decyzja:
jeśli wielu, przejdź do wspólnej infrastruktury.



2. Test drugi: sprawdź zasilanie, połączenie, poprawny adres, bramę i rozwiązywanie nazw.

Zatrzymaj się na pierwszym niespełnionym warunku.



3. Rozwiązanie wynika z gałęzi:

popraw przewód, drogę VLAN-u, usługę DHCP, DNS albo połączenie WAN.
Nie zmieniaj wszystkiego równocześnie.

4. Przykład: kabel działa, Wi-Fi nie.

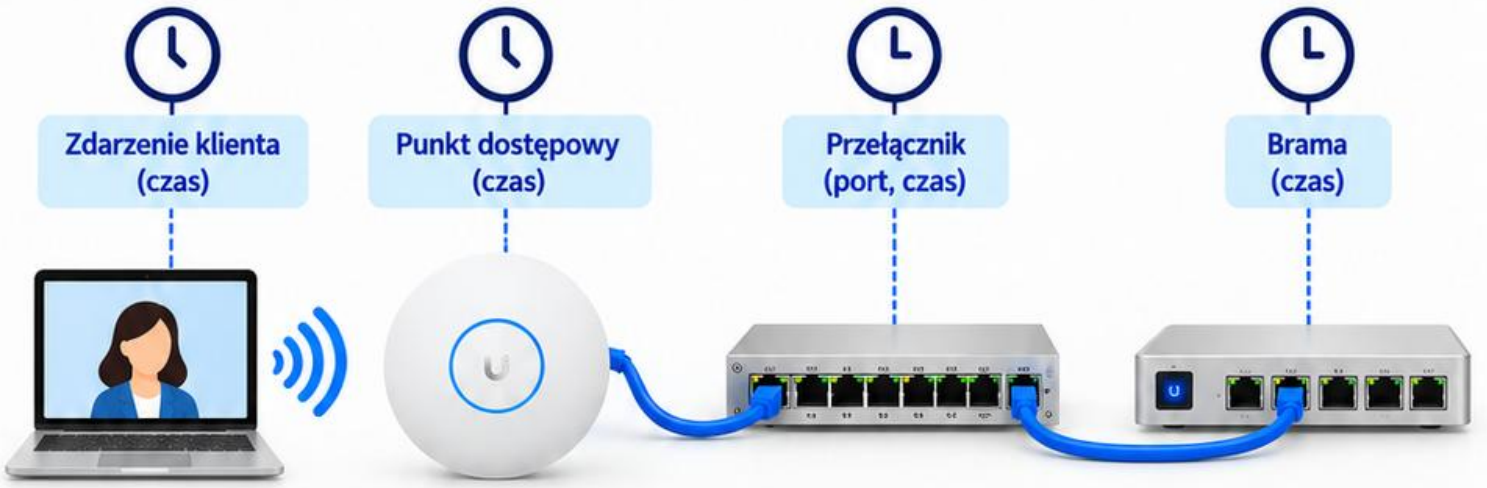
Zawęź badanie do ścieżki bezprzewodowej, ale pamiętaj o VLAN-ie przypisanym do SSID.

5. Walidacja: powtórz pierwotne zadanie użytkownika i test porównawczy.

Zapisz pierwszą przyczynę, wykonaną zmianę oraz wynik.

Źródła: [30], [31]

Ostoja • Zbierz dowody bez ujawniania danych



1. Objaw

Objaw: awaria występuje okresowo, a restart usuwa ślady. Najpierw zapisz czas, urządzenie i czynność, przy której pojawia się problem.



2. Test

Test: zestaw zdarzenia klienta z portem, AP, bramą i ostatnią zmianą. Używaj tej samej strefy czasowej w notatkach.



3. Decyzja

Decyzja: korelacja czasu wskazuje obszar badania, lecz nie dowodzi przyczyny. Wybierz próbę rozdzielającą co najmniej dwie hipotezy.



4. Rozwiązanie organizacyjne

Rozwiązanie organizacyjne: zapisz stan przed zmianą, wykonaj pojedyncze działanie i zachowaj dowód po nim. Ukryj zbędne identyfikatory oraz dane użytkowników.



5. Przykład

Przykład: Anna z recepcji zgłasza przerwy przy przejściu do sali. Zapis trasy i AP jest użyteczniejszy niż ogólny opis słabej sieci.



Nie dołączaj haseł, prywatnych kluczy ani pełnych profili VPN do publicznego zgłoszenia.

Pliki wsparcia przekazuj zatwierdzonym kanałem.



Walidacja

Walidacja: inny technik powinien odtworzyć próbę na podstawie notatki, bez dostępu do sekretów i bez dodatkowego zgadywania.

Źródła: [30], [8]

Urządzenie nie ma zasilania

Objaw:

Brak oznak uruchomienia AP, telefonu lub innego odbiornika.



1. Test:

Sprawdź zasilanie przełącznika, zgodność PoE i dostępny budżet. Zastąp patchcord sprawdzonym przewodem i użyj zgodnego portu.



2. Decyzja:

Jeżeli odbiornik uruchamia się na innym zgodnym porcie, badaj poprzedni tor. Jeżeli nie, sprawdź odbiornik i jego specyfikację.



3. Rozwiązanie:

Popraw zgodność zasilania lub uszkodzony odcinek. Nie próbuj przypadkowych trybów pasywnego PoE.



4. Przykład:

Po wymianie przewodu AP pozostaje aktywny także podczas normalnej pracy klientów.



5. Waidacja:

Sprawdź stabilne uruchomienie i dostępność urządzenia. Odczytaj pobór, a następnie ponów próbę w warunkach zgłaszanej awarii.

Jeśli próba nie rozstrzyga przyczyny, zachowaj dowody i przekaż je osobie odpowiedzialnej za wskazany odcinek.

Źródła: [6]

Adopcja pozostaje oczekująca

Objaw: Urządzenie jest widoczne, lecz nie kończy adopcji w UniFi Network.

Test: Sprawdź adres urządzenia, jego sieć zarządzającą i osiągalność właściwej instancji Network. Porównaj stan urządzenia z uruchomioną aplikacją.

Decyzja: Brak poprawnego adresu kieruje do DHCP i VLAN-u. Poprawna adresacja bez komunikacji z aplikacją kieruje do drogi i filtrów.

Rozwiązanie: Przywróć wymaganą komunikację między urządzeniem a kontrolerem. Adopcję między podsieciami przygotuj według scenariusza warstwy trzeciej.

Przykład: Nowy AP działa w sieci montażowej, ale nie w docelowej szafie; porównaj konfigurację jej uplinku.

Walidacja: Potwierdź stan online, możliwość zmiany nazwy i utrzymanie połączenia. Nie resetuj działającej instalacji przed zebraniem dowodów.



1. Sprawdź adres urządzenia
Urządzenie ma poprawny adres IP w sieci zarządzającej?

Nie

2. Sprawdź DHCP i VLAN
Czy urządzenie otrzymuje adres w sieci zarządzającej?



Tak

3. Sprawdź komunikację z aplikacją
Czy urządzenie może połączyć się z właściwą instancją Network?



4. Przywróć wymaganą komunikację
Zastosuj odpowiednie zasady routingu i filtrów, aby urządzenie mogło połączyć się z kontrolerem. Adopcję między podsieciami przygotuj według scenariusza warstwy trzeciej.

5. Zweryfikuj działanie
Potwierdź stan online, możliwość zmiany nazwy i utrzymanie połączenia.



Jeśli próba nie rozstrzyga przyczyny, zachowaj dowody i przekaż je osobie odpowiedzialnej za wskazany odcinek.

Źródła: [24]

Urządzenie ma inny kontroler

Objaw: Widoczny jest komunikat o zarządzaniu przez inną konsolę.

Test: Ustal właściciela i historię urządzenia. Sprawdź, czy stara instancja Network nadal działa oraz czy istnieje jej kopia zapasowa.

Decyzja: Jeśli przenosisz istniejącą instalację, wybierz właściwą migrację. Jeśli urządzenie ma zostać wyczyszczone, przygotuj ponowną konfigurację i okno serwisowe.

Rozwiązanie: Użyj zatwierdzonej migracji lub przywrócenia zgodnej kopii. Reset fabryczny pozostaw jako świadomą operację usuwającą konfigurację.

Przykład: Przełącznik po wymianie kontrolera nadal pamięta poprzednie zarządzanie. Kolejna instalacja aplikacji nie przejmuje go automatycznie.

Walidacja: Potwierdź zarządzanie z nowej instancji i dostępność odbiorników. Usuń ryzyko powrotu do starej instancji zgodnie z procedurą migracji.

1. Stara konsola

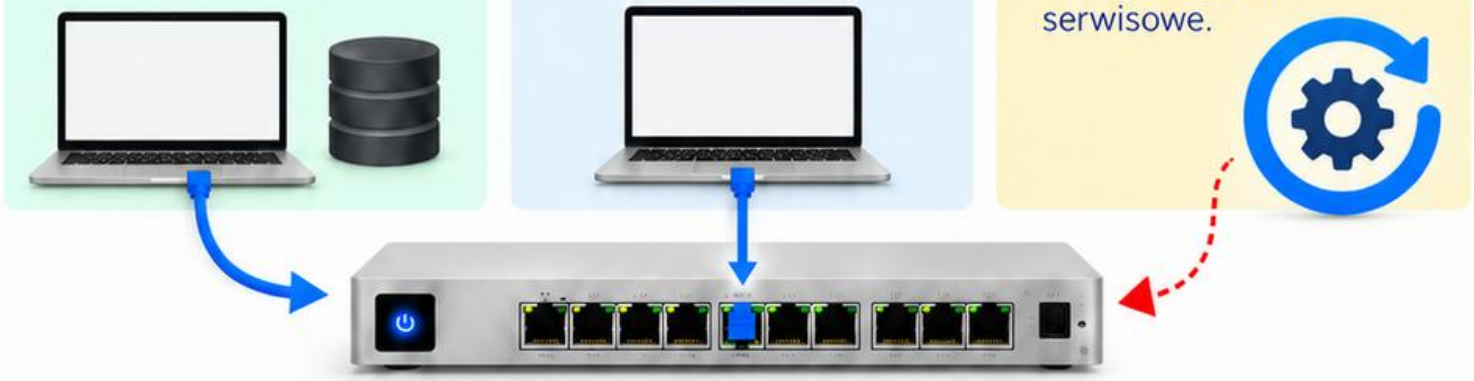
Sprawdź, czy instancja Network nadal działa i czy istnieje jej kopia zapasowa.

2. Nowa konsola

Wykonaj migrację lub przywróć zgodną kopię na nowej instancji.

3. Reset fabryczny

Użyj tylko gdy urządzenie ma zostać wyczyszczone. Przygotuj ponowną konfigurację i okno serwisowe.



Problem: urządzenie zarządzane przez inną konsolę

Przełącznik nadal pamięta poprzednie zarządzanie. Kolejna instalacja aplikacji nie przejmuje go automatycznie.



Po migracji lub przywróceniu

Urządzenie jest zarządzane z nowej instancji i odbiorniki są dostępne.



Jeśli próba nie rozstrzyga przyczyny, zachowaj dowody i przekaż je osobie odpowiedzialnej za wskazany odcinek.

Źródła: [8]

Urządzenie jest rozłączone

Zarządzanie nie działa



Zarządzanie działa



1. Objaw

AP lub przełącznik nie jest online, choć część usług nadal działa.



2. Test

Sprawdź zasilanie, port i adres zarządzający. Porównaj ostatnią zmianę VLAN-u, podsieci lub reguł z czasem rozłączenia.



3. Decyzja

Jeśli klient na tym samym kablu także nie otrzymuje adresu, badaj tor przewodowy i DHCP. Jeśli działa, sprawdź urządzenie i zarządzanie.



4. Rozwiązanie

Cofnij potwierdzoną błędną zmianę albo popraw drogę do kontrolera. Nie utożsamiaj działającego SSID z prawidłowym połączeniem zarządzającym.



5. Przykład

AP nadal obsługuje klientów według ostatniej konfiguracji, ale nie odbiera zmian z Network. Taki stan nie potwierdza sprawności zarządzania.



6. Walidacja

Sprawdź powrót online, aktualizację statusu oraz rzeczywiste zastosowanie bezpiecznej zmiany testowej. Zapisz odcinek odpowiedzialny za przerwę.



Źródła: [31]

Klient nie otrzymuje DHCP

Objaw: Po połączeniu klient nie ma poprawnego adresu z oczekiwanej sieci.



1. Test:

Sprawdź konfigurację IP klienta, sieć portu lub SSID, drogę VLAN-u i dostępność puli DHCP. Porównaj innego klienta.

2. Decyzja:

Jeśli drugi klient też nie uzyskuje adresu, szukaj problemu wspólnego. Jeśli działa, sprawdź profil, statyczne ustawienia i zachowanie pierwszego klienta.

3. Rozwiązanie:

Popraw wykazany błąd przypisania lub usługi DHCP. Nie przydzielaj przypadkowego statycznego adresu jako docelowego obejścia.

4. Przykład:

Laptop pracuje na porcie rdzenia, lecz nie na piętrze. Sprawdź VLAN na odcinku między przełącznikami, zanim zmienisz serwer.

5. Walidacja:

Odnów dzierżawę i porównaj adres, maskę, bramę oraz DNS. Powtórz próbę po ponownym podłączeniu i uruchom aplikację użytkownika.

Źródła: [32]

Występuje konflikt adresu IP



1. Objaw

Łączność jest niestabilna lub system zgłasza zajęty adres.



2. Test

Zapisz adres i identyfikatory obu podejrzanych urządzeń. Porównaj dzierżawy DHCP, rezerwacje i statyczną konfigurację odbiorników.



3. Decyzja

Jeśli statyczny adres pokrywa się z pulą dynamiczną, popraw plan adresacji. Jeśli problem dotyczy rezerwacji, sprawdź właściwy identyfikator klienta.



4. Rozwiązanie

Nadaj urządzeniom jednoznaczne adresy zgodnie z planem. Zmień potwierdzone źródło konfliktu, zachowując dostęp do urządzenia infrastruktury.



5. Przykład

Drukarka ma ręcznie ustawiony adres przydzielany także laptopowi. Wyłączenie laptopa usuwa objaw chwilowo, lecz nie przyczynę.



6. Walidacja

Odnów dzierżawę i sprawdź równoczesną pracę obu urządzeń. Potwierdź poprawne mapowanie adresów oraz brak ponownego komunikatu konfliktu.



Jeśli próba nie rozstrzyga przyczyny, zachowaj dowody i przekaż je osobie odpowiedzialnej za wskazany odcinek.

Źródła: [1]

DNS nie odpowiada

Objaw: Połączenie istnieje, lecz usługi po nazwie nie działają.

Przykład: Komputer otwiera usługę po znanym adresie, lecz nie po nazwie firmowej. Publiczny resolver nie musi znać prywatnej nazwy.



1. Test

Odczytaj resolver klienta i wykonaj kontrolowane zapytanie do niego. Porównaj osiągalność znanego celu oraz wynik z innego klienta.



2. Decyzja

Jeśli połączenie do celu działa, ale rozwiązywanie nazwy nie, badaj DNS. Jeśli oba zawodzą, wróć do adresacji, bramy i WAN.



3. Rozwiązanie

Popraw przekazywany resolver lub potwierdzoną blokadę jego usługi. Zachowaj wymagania lokalnych nazw, zanim zastąpisz wewnętrzny serwer zewnętrznym.



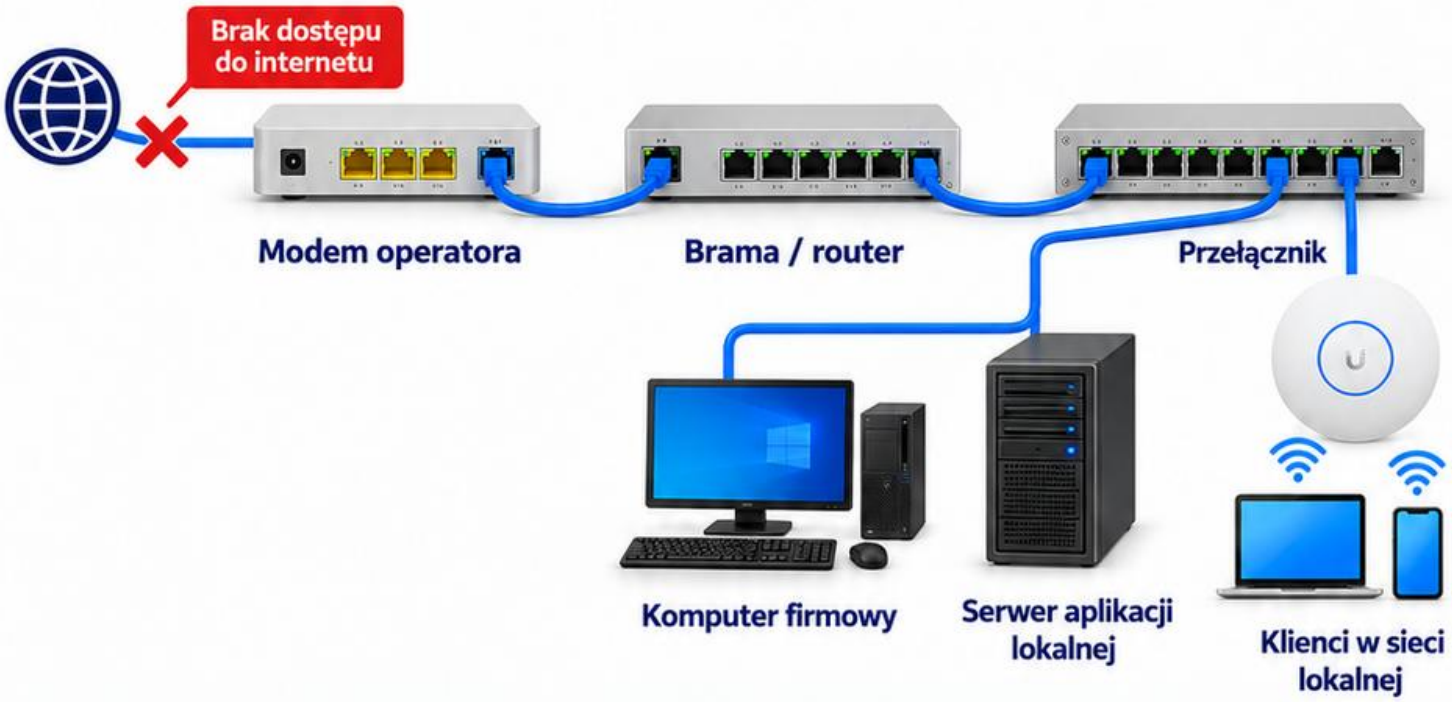
4. Walidacja

Ponów zapytanie do właściwego serwera i zadanie użytkownika. Sprawdź nową dzierżawę, jeśli zmiana DNS jest przekazywana przez DHCP.



Źródło: [18]

WAN jest niedostępny



1. Objaw

Wiele poprawnie skonfigurowanych klientów jednocześnie traci dostęp do internetu.

2. Test

Sprawdź lokalną bramę, stan fizycznego WAN i parametry otrzymane od operatora. Porównaj zasięg problemu z komunikatem operatora.

3. Decyzja

Jeśli LAN działa, a WAN nie ma wymaganej konfiguracji, badaj usługę operatora i jej ustawienia. Jeśli LAN też nie działa, zacznij lokalnie.

4. Rozwiązanie

Popraw wykazaną niezgodność dostępu lub zgłoś operatorowi awarię z czasem i dowodami. Nie zmieniaj LAN, aby obejść problem WAN.

5. Przykład

Całe biuro otwiera lokalną aplikację, ale nie usługi internetowe. Działająca sieć wewnętrzna zawęża obszar awarii.

6. Walidacja

Sprawdź z bramy i klienta połączenie oraz DNS. Potwierdź aplikację biznesową i obserwuj stabilność po powrocie usługi.

Źródła: [16]

PPPoE nie zestawia połączenia



1. Objaw

Łącze fizyczne jest aktywne, lecz sesja dostępu nie powstaje.

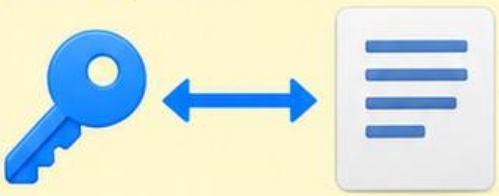
2. Test

Porównaj typ połączenia i wymagania operatora z zatwierdzonymi danymi instalacji. Sprawdź wymagany VLAN dostępu i informacje o błędzie sesji.



3. Decyzja

Błąd uwierzytelniania kieruje do danych i uprawnień usługi. Brak komunikacji wymaga kontroli toru oraz warunków po stronie operatora.



4. Rozwiązanie

Popraw konkretną rozbieżność i ponów połączenie. Sekrety porównuj w bezpiecznym miejscu, bez wpisywania ich do karty zgłoszenia.



5. Przykład

Po wymianie bramy pominięto wymaganie operatora. Skopiowanie przypadkowej konfiguracji z innego lokalu nie jest wiarygodną metodą naprawy.



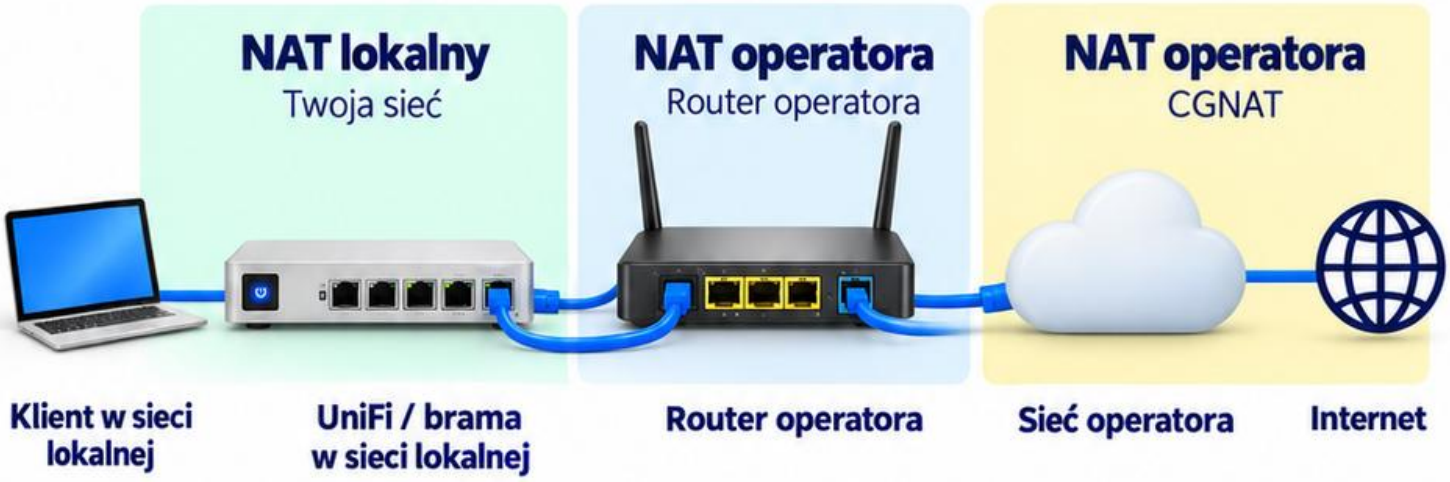
6. Walidacja

Potwierdź utworzenie sesji, przydzieloną konfigurację i działanie klienta. Przy eskalacji podaj typ błędu oraz czas, bez hasła dostępowego.



Źródła: [16]

Podwójny NAT albo CGNAT



1. Objaw

Usługi wychodzące działają, ale dostęp przychodzący lub serwer VPN nie jest osiągalny.



2. Test

Porównaj adres WAN z informacją o adresacji operatora i topologią urządzeń przed bramą. Ustal, kto kontroluje każdą warstwę NAT.



3. Decyzja

Dodatkowy router lokalny wskazuje możliwy podwójny NAT. Translacja u operatora wymaga uzgodnienia usługi; nie usuniesz jej samą regułą na UniFi.

4. Rozwiązanie

Uporządkuj uzgodnioną topologię lub zamów właściwą osiągalność u operatora. Alternatywny dostęp dobierz do wymagań i zgodności urządzeń.

5. Przykład

Brama stoi za routerem operatora. Samo przekierowanie na UniFi nie otwiera drogi przez urządzenie nadrzędne ani NAT operatora.

6. Walidacja

Wykonaj próbę z zewnętrznej sieci. Zapisz granicę odpowiedzialności i wynik, zamiast oceniać dostęp publiczny wyłącznie z lokalnego Wi-Fi.

Źródła: [22]

VLAN nie ma łączności

Objaw: Klient trafia do segmentu, ale oczekiwana usługa nie działa.

Test: Sprawdź adres, port dostępowy, przypisanie SSID i kolejne uplinki. Porównaj próbę z portu bezpośrednio przy urządzeniu routującym.



1. Sprawdź adres u klienta

Klient powinien otrzymać adres z oczekiwanej sieci VLAN.
Jeśli otrzymuje adres z innej sieci, sprawdź przypisanie lub natywny VLAN.



Klient otrzymuje adres z innej sieci niż oczekiwana.

2. Sprawdź port dostępowy

Upewnij się, że port, do którego podłączony jest punkt dostępowy, ma prawidłowe przypisanie VLAN.



3. Sprawdź przypisanie SSID

Zweryfikuj, że SSID jest przypisane do właściwego VLAN.



4. Sprawdź kolejne uplinki

Sprawdź łączność VLAN-u na kolejnych uplinkach.
Porównaj próbę z portu bezpośrednio przy urządzeniu routującym.



5. Porównaj wynik przy bramie

Jeśli przy bramie działa, a dalej nie, badaj ścieżkę warstwy drugiej.
Jeśli nie działa nigdzie, sprawdź sieć i usługi bramy.



6. Rozwiązanie

Popraw pierwszą potwierdzoną rozbieżność VLAN-u lub usługi. Nie otwieraj wszystkich segmentów, zanim wykażesz rzeczywistą blokadę firewalla.

7. Walidacja

Odnów adres, sprawdź bramę i usługę. Wykonaj również próbę zabronionego dostępu, aby naprawa łączności nie zniosła segmentacji.

8. Przykład

Klient otrzymuje adres z innej sieci niż oczekiwana. To wskazuje przypisanie lub natywny VLAN, a nie brak przepustowości internetu.

Źródła: [32]

Ostoja · Diagnoza · Brakuje VLAN-u na uplinku

Brakuje VLAN-u na uplinku

Objaw: Wybrana sieć działa na jednym przełączniku, a za kolejnym przestaje działać.



1. Test

W Port Manager porównaj Tagged VLAN Management po obu stronach połączenia. Sprawdź też zgodność ruchu nietagowanego i rzeczywistą trasę przewodu.

2. Decyzja

Brak wymaganego tagu na jednym końcu wskazuje przerwę ścieżki. Jeśli lista jest zgodna, przejdź do kolejnego odcinka i przypisania klienta.

3. Rozwiązanie

Dopuść wyłącznie potrzebny VLAN na potwierdzonym uplinku. Zachowaj sieć zarządzającą, aby nie odciąć przełącznika podczas poprawki.

4. Przykład

Goście działają przy rdzeniu, a nie na piętrze. Uzupełnienie właściwej listy na uplinku rozwiązuje problem bez zmiany SSID.

5. Walidacja

Przetestuj świeżą dzierżawę i dostęp do usługi. Udokumentuj oba końce połączenia oraz wymagany zestaw VLAN-ów dla dalszej obsługi.



Źródła: [4]

Klient nie łączy się z Wi-Fi

Objaw: Sieć jest widoczna, ale urządzenie nie kończy połączenia.



1. Test

Sprawdź dane profilu, obsługiwane pasma i metody zabezpieczeń. Porównaj drugiego klienta na tym samym SSID i AP.



2. Decyzja

Jeśli inne urządzenie działa, sprawdź profil i sterownik pierwszego. Jeśli wszystkie zawodzą, porównaj wspólne ustawienia SSID i AP.



3. Przykład

Starszy terminal widzi nazwę, lecz nie obsługuje wybranego zestawu zabezpieczeń. Widoczność SSID nie oznacza zgodności uwierzytelniania.



4. Rozwiązanie

Popraw wykazaną niezgodność lub odtwórz profil testowy. Nie obniżaj ochrony całej sieci bez sprawdzenia przyczyny.



5. Walidacja

Potwierdź nowe połączenie, adres i działanie aplikacji. Zapisz etap niepowodzenia, aby nie mylić odmowy uwierzytelniania z problemem DHCP.



6. Jeśli próba nie rozstrzyga

Jeśli próba nie rozstrzyga przyczyny, zachowaj dowody i przekaż je osobie odpowiedzialnej za wskazany odcinek.



Źródła: [33]

Ostoja · Diagnoza · **WPA lub PMF są niezgodne**

Część klientów nie może się połączyć po zmianie zabezpieczeń



1. Objaw

Po zmianie zabezpieczeń część klientów przestaje się łączyć.



2. Test

Porównaj działający i niedziałający model oraz poprzednie ustawienie. Sprawdź wymagania WPA3, PMF, pasma i aktualność sterownika.



3. Decyzja

Jeśli awaria dotyczy konkretnej grupy klientów, wykonaj próbę zgodności na kontrolowanym SSID. Nie zakładaj problemu sygnału.



4. Rozwiązanie

Zastosuj zatwierdzony wariant zabezpieczeń lub oddziel starsze urządzenia w ograniczonej sieci. Zachowaj ochronę wymaganą dla pozostałych odbiorników.



5. Przykład

Po zmianie PMF nowy laptop działa, a skaner nie. Porównanie możliwości skanera uzasadnia dalszą decyzję bez przypadkowych zmian kanału.



6. Walidacja

Ponów połączenie z czystego profilu na obu modelach. Potwierdź także poprawną sieć docelową i niedostępność zabronionych zasobów.



7.

Jeśli próba nie rozstrzyga przyczyny, zachowaj dowody i przekaż je osobie odpowiedzialnej za wskazany odcinek.



Źródła: [33]

Pokrycie jest niewystarczające



1. Objaw

Przerwy występują w określonym miejscu, mimo poprawnego działania bliżej AP.



2. Test

Przejdź stałą trasę z tym samym klientem. Zapisz sygnał, AP i działanie aplikacji po obu stronach przeszkody.



3. Decyzja

Jeśli objaw zależy od miejsca, sprawdź pokrycie i przeszkody. Jeśli od modelu urządzenia, porównaj zdolność komunikacji w obu kierunkach.



4. Rozwiązanie

Popraw położenie AP lub projekt pokrycia na podstawie pomiaru. Samo zwiększenie mocy AP nie wzmacnia nadajnika klienta.



5. Przykład

Pracownik w magazynie traci połączenie za regałem. Dobry wynik przy drzwiach nie opisuje stanowiska między metalowymi półkami.



6. Walidacja

Powtórz trasę podczas typowej pracy magazynu. Potwierdź stabilność aplikacji w miejscu zgłoszenia i brak pogorszenia przechodzenia do sąsiedniego AP.



Źródła: [30]

Zakłócenia i zajętość radia

Przed spotkaniem



Podczas warsztatów



1. Objaw

Sygnał jest wystarczający, lecz opóźnienia i retransmisje rosną w godzinach pracy.



2. Test

W Radios > AirView porównaj zajętość, retransmisje i otoczenie kanałów. Zestaw wyniki z liczbą klientów i ich aktywnością.



3. Decyzja

Wysoka zajętość może wynikać z konkurencji lub własnego ruchu. Rozdziel obce zakłócenia od obciążenia, zanim zmienisz plan kanałów.



4. Rozwiązanie

Dostosuj kanał, szerokość lub rozkład obciążenia zgodnie z pomiarem. Zmieniaj jeden element i zachowaj kraj instalacji.



5. Przykład

Sala jest szybka przed spotkaniem, a wolna podczas warsztatów. Pomiar bez uczestników nie rozstrzyga o rzeczywistych warunkach pracy.



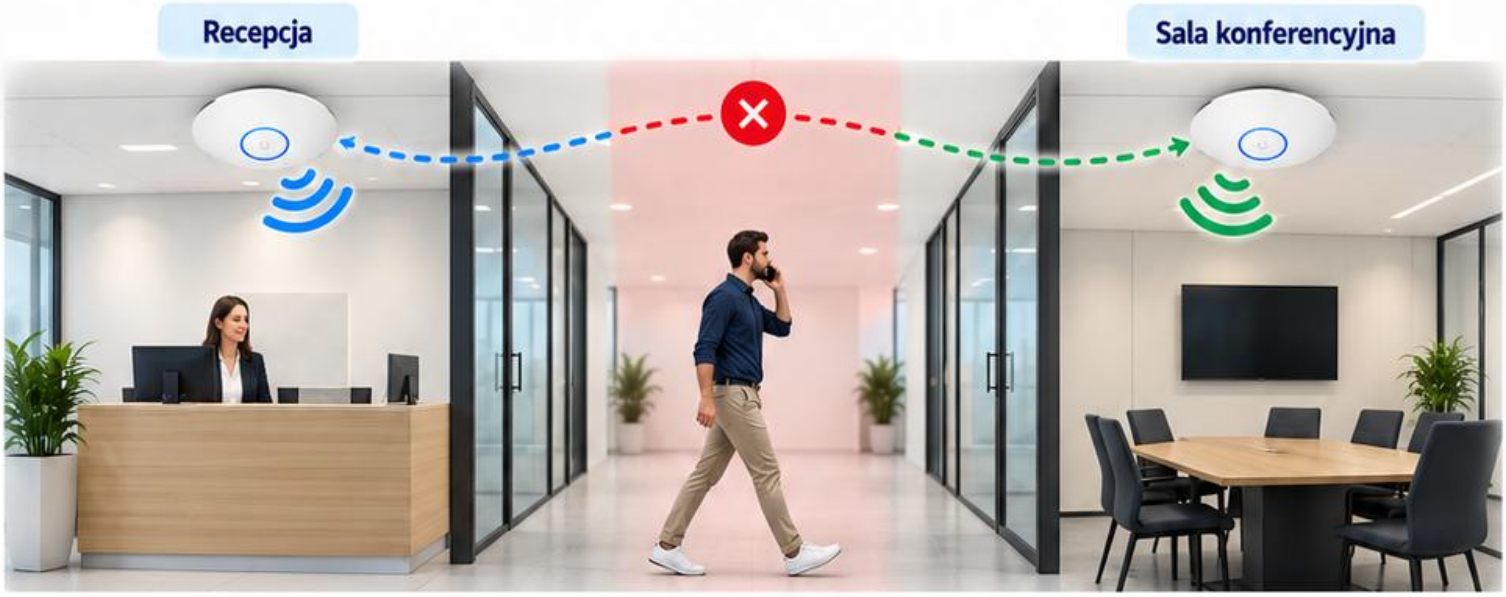
6. Walidacja

Porównaj aplikację, retransmisje i opóźnienia przy podobnym obciążeniu. Sam większy wynik pojedynczego testu prędkości nie potwierdza rozwiązania problemu.



Źródła: [30]

Przerwy podczas zmiany AP



1. Objaw

Rozmowa lub aplikacja przerywa przy przechodzeniu między pomieszczeniami.



2. Test

Zapisz trasę, moment zmiany AP i zachowanie aplikacji. Powtórz ją na drugim modelu klienta oraz w odwrotnym kierunku.



3. Decyzja

Brak pokrycia wskazuje projekt radiowy. Pozostawanie przy dalekim AP wymaga oceny nakładania komórek, klienta i zgodności opcji roamingu.



4. Rozwiązanie

Popraw potwierdzoną przyczynę i testuj opcje roamingu oddzielnie. Nie stosuj agresywnego odłączania klienta jako zamiennika pokrycia.



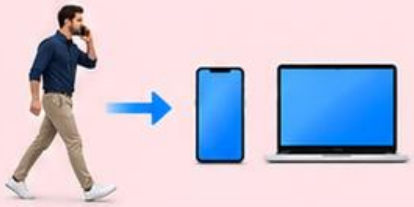
5. Przykład

Telefon pracownika trzyma połączenie z recepcją w sali konferencyjnej. Najpierw sprawdź oba sygnały i faktyczną zmianę AP.



6. Walidacja

Powtórz przejście z aktywną usługą. Potwierdź ciągłość i zapisz obsługiwany model; decyzja roamingowa klienta może różnić się między urządzeniami.



Źródła: [19]

Brakuje budżetu PoE



1. Objaw

Urządzenia restartują się po dołączeniu kolejnego odbiornika lub po powrocie zasilania.



2. Test

Porównaj budżet przełącznika, limity portów i wymagania wszystkich odbiorników. Sprawdź także zasilacz oraz przewody.



3. Decyzja

Jeśli problem pojawia się wraz z obciążeniem, badaj budżet i zgodność. Jeśli dotyczy jednego toru, przetestuj go osobno.



4. Rozwiązanie

Rozdziel obciążenie lub zastosuj zgodne źródło o wymaganych parametrach. Nie przyjmuj chwilowego niskiego poboru za maksymalne zapotrzebowanie.



5. Przykład

Po zaniku prądu wszystkie AP uruchamiają się naraz i część wraca do restartów. Test pojedynczego AP nie odtwarza tej sytuacji.



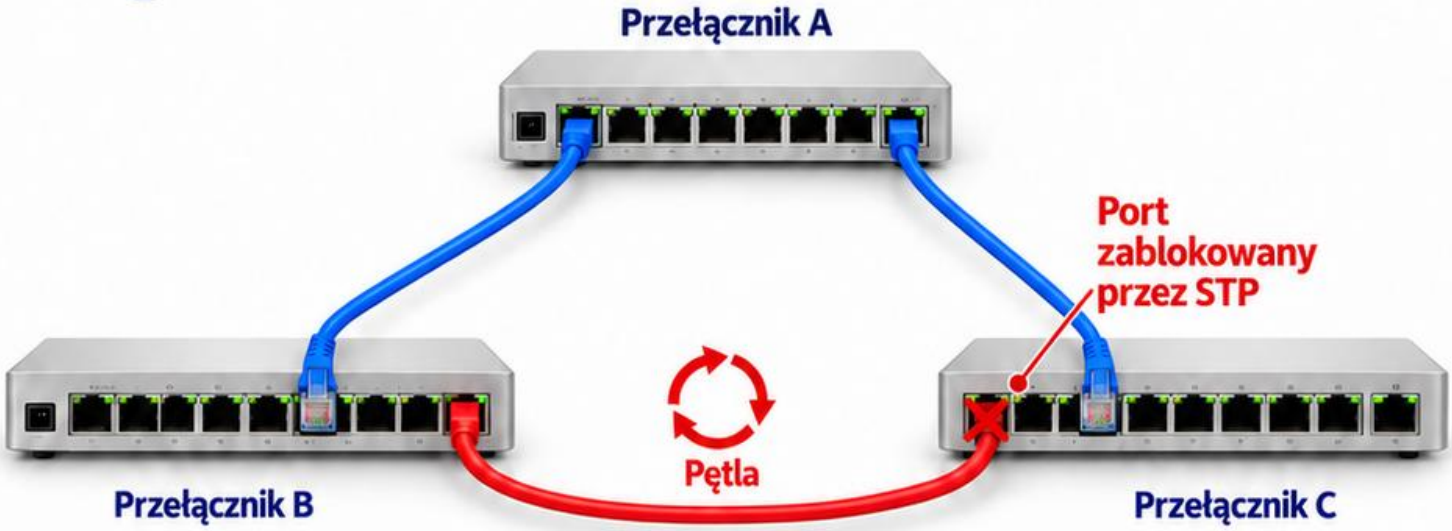
6. Walidacja

Sprawdź równoczesne uruchomienie oraz normalną pracę odbiorników. Zapisz stabilny wynik i rzeczywistą rezerwę wynikającą ze specyfikacji sprzętu.



Źródło: [6]

Pętla i blokada STP



1. Objaw

Wiele urządzeń rozłącza się albo pojawia się nieoczekiwana blokada portu.



2. Test

Sprawdź ostatnie połączenia kablowe, stan STP i topologię. Odróżnij zamierzoną zapasową ścieżkę od przypadkowego pierścienia.



3. Decyzja

Prawidłowo zablokowany nadmiarowy link może chronić sieć. Niezaplanowany obieg wymaga usunięcia, zamiast wyłączania ochrony.

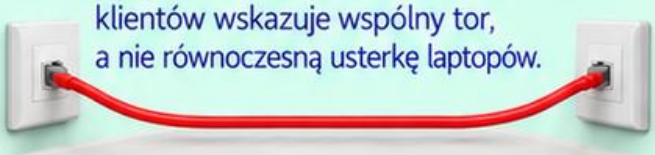
4. Rozwiązanie

Odłącz potwierdzony niepotrzebny przewód i uporządkuj topologię. Przywróć właściwe RSTP i plan korzenia; zachowaj podstawową drogę zarządzania.



5. Przykład

Po sprzątaniu dwa gniazda w sali połączono patchcordem. Awaria wielu klientów wskazuje wspólny tor, a nie równoczesną usterkę laptopów.



6. Walidacja

Potwierdź stabilność ruchu, właściwy korzeń i oczekiwane stany portów. Udokumentuj, dlaczego zapasowa ścieżka jest blokowana albo dlaczego została usunięta.

Źródła: [5]

VPN nie ma handshake

Objaw: Klient WireGuard jest uruchomiony, ale nie ma potwierdzonej wymiany z serwerem.



1 Test

Sprawdź połączenie klienta z internetem, właściwy profil, punkt końcowy i osiągalność serwera z zewnętrznej sieci. Porównaj ostatnią zmianę WAN.



2 Decyzja

Brak osiągalności kieruje do NAT, operatora i drogi serwera. Błędny profil wymaga porównania konfiguracji oraz uprawnień klienta.



3 Rozwiązanie

Popraw konkretny parametr lub warunek osiągalności. Sekrety sprawdzaj w bezpiecznej konfiguracji; nie wklejaj kluczy do zgłoszenia.



4. Przykład

Serwer działa za dodatkowym routerem operatora. Samo uruchomienie VPN na UniFi nie tworzy automatycznie drogi przychodzącej przez urządzenie nadrzędne.



5. Walidacja

Potwierdź świeży handshake po wygenerowaniu ruchu. Następnie wykonaj osobny test zasobu, ponieważ zestawienie tunelu nie dowodzi dostępu do aplikacji.



Źródła: [22]

Ostoja · Diagnoza · Tunel działą, zasób nie odpowiada

Objaw: VPN ma aktualny handshake, ale użytkownik nie otwiera potrzebnej usługi.

Test: Sprawdź adres celu, trasę klienta, nakładanie podsieci, DNS i politykę między VPN a zasobem. Porównaj próbę po nazwie i adresie.

Decyzja: Jeśli adres działa, a nazwa nie, badaj DNS. Jeśli oba zawodzą, sprawdź trasę, politykę i samą usługę docelową.

Rozwiązanie: Popraw wykazaną brakującą trasę, resolver lub wąskie uprawnienie. Nie otwieraj całej sieci wewnętrznej w celu naprawienia jednego dostępu.

Przykład: Domowa podsieć użytkownika pokrywa się z firmową. Ruch może pozostać lokalny mimo aktywnego tunelu, dlatego sprawdź faktyczną drogę.

Walidacja: Potwierdź dozwoloną usługę i próbę zabronioną. Zapisz wynik z zewnętrznej sieci oraz upewnij się, że naprawa nie rozszerzyła uprawnień.



1. Sprawdź adres celu

Porównaj połączenie po nazwie i adresie. Jeśli adres działa, a nazwa nie, badaj DNS.



2. Sprawdź trasę klienta

Upewnij się, że ruch do zasobu idzie przez tunel VPN, a nie pozostaje w sieci lokalnej klienta.



3. Sprawdź nakładanie podsieci

Jeśli domowa podsieć pokrywa się z firmową, ruch może pozostać lokalny mimo aktywnego tunelu.



4. Sprawdź DNS

Jeśli adres działa, a nazwa nie, sprawdź resolver dostępny przez VPN i jego odpowiedź dla tej nazwy.



5. Sprawdź politykę i usługę

Jeśli oba sposoby zawodzą, sprawdź reguły między VPN a zasobem oraz samą usługę docelową.



Walidacja

Potwierdź dozwoloną usługę i próbę zabronioną. Zapisz wynik z zewnętrznej sieci oraz upewnij się, że naprawa nie rozszerzyła uprawnień.



Źródła: [22]

Ostoja · Karta incydentu i eskalacja

Objaw: problem pozostaje po kontrolowanych próbach albo wraca okresowo.

Przygotuj zgłoszenie, które pozwala kontynuować diagnozę bez zaczynania od zera.

1. **Wpisz:** czas i strefa czasowa _____.
2. **Wpisz:** urządzenie, model i wersja _____.
3. **Wpisz:** oczekiwane działanie oraz objaw _____.
4. **Wpisz:** wykonany test, wynik i ostatnia zmiana _____.
5. **Wpisz:** wpływ na użytkowników i obejście _____.

Przykład: recepcja, telefon testowy, utrata rozmowy na przejściu do sali; komputer przewodowy działa; problem powtórzony w obu kierunkach.

Decyzja: wskaż gałąź, której nie udało się potwierdzić, oraz dowód potrzebny od kolejnej osoby. Nie wpisuj domniemanej przyczyny jako faktu.



Rozwiązanie: przekaż zanonimizowane dowody zatwierdzonym kanałem. Walidacja po naprawie obejmuje pierwotną czynność użytkownika i test kontrolny, z datą zamknięcia.



Źródła: [30], [31]

Źródła

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

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

5 Pętle i STP
https://help.ui.com/hc/en-us/articles/24292724428311

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

16 Failover i porty WAN
https://help.ui.com/hc/en-us/articles/360052548713

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

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

24 Adopcja urządzeń
https://help.ui.com/hc/en-us/articles/360012622613

30 Diagnostyka Wi-Fi
https://help.ui.com/hc/en-us/articles/32064585817495

31 Łączność urządzeń UniFi
https://help.ui.com/hc/en-us/articles/7258465146519

32 Diagnostyka VLAN
https://help.ui.com/hc/en-us/articles/9592924981911

33 Ustawienia SSID i AP
https://help.ui.com/hc/en-us/articles/32065480092951