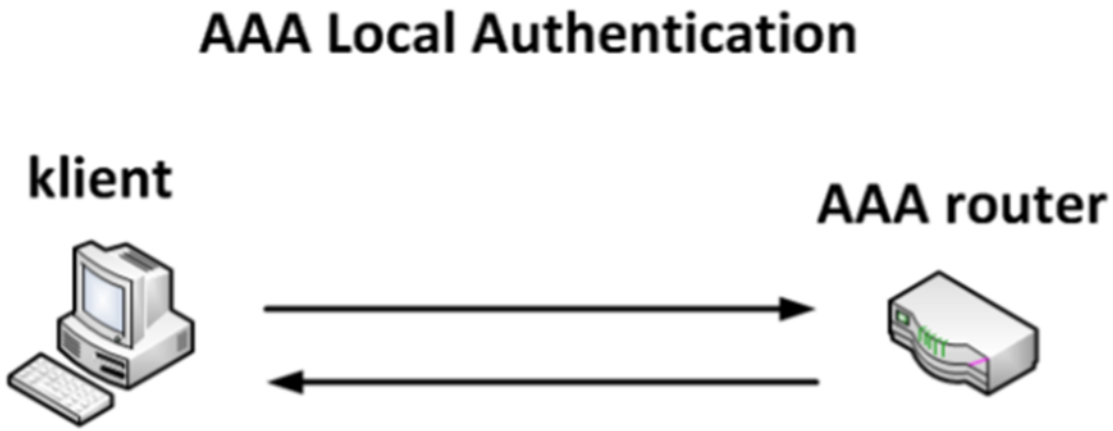
Podstawy sieci

BEZPIECZEŃSTWO PROTOKOŁÓW I USŁUG SIECIOWYCH

Uwierzytelnianie w Cisco IOS

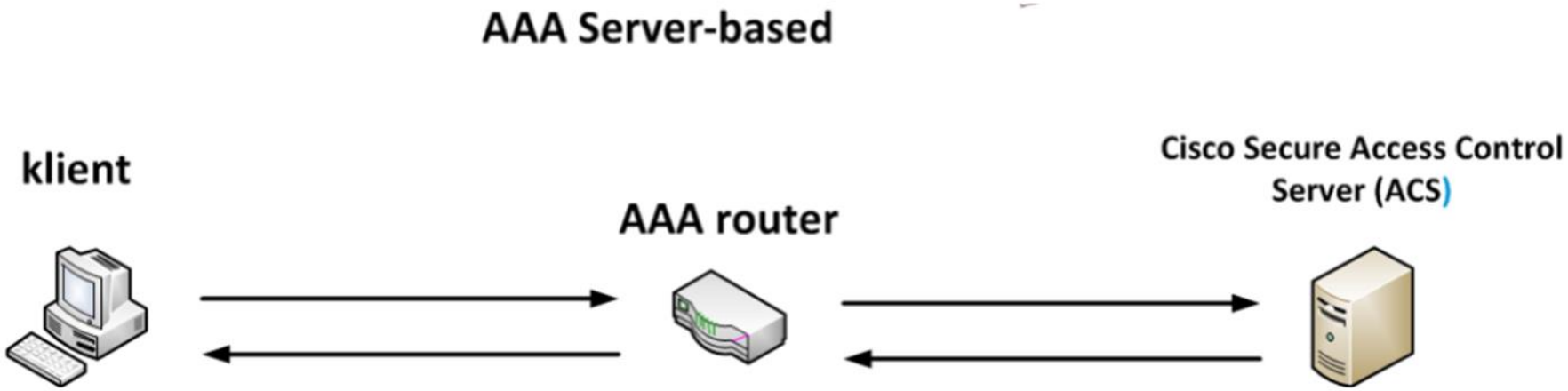
LOKALNE UWIERZYTELNIANIE UŻYTKOWNIKÓW



AAA (Authentication Authorization Accounting) - model ten stanowi spójny system w obrębie którego działają mechanizmy odpowiedzialne za bezpieczny dostęp do sieci i jej zasobów. Modułowy charakter mechanizmu pozwala wpływać na konfigurację trzech głównych usług: autentykacji-uwierzytelnianie **(authentication),** autoryzacji **(authorization)** oraz raportowania **(accounting).** Model ten może opierać się na lokalnej bazie użytkowników - **AAA Local Authentication (self-contained AAA)** oraz na bazie opartej o serwery uwierzytelniające - **AAA Server-based**

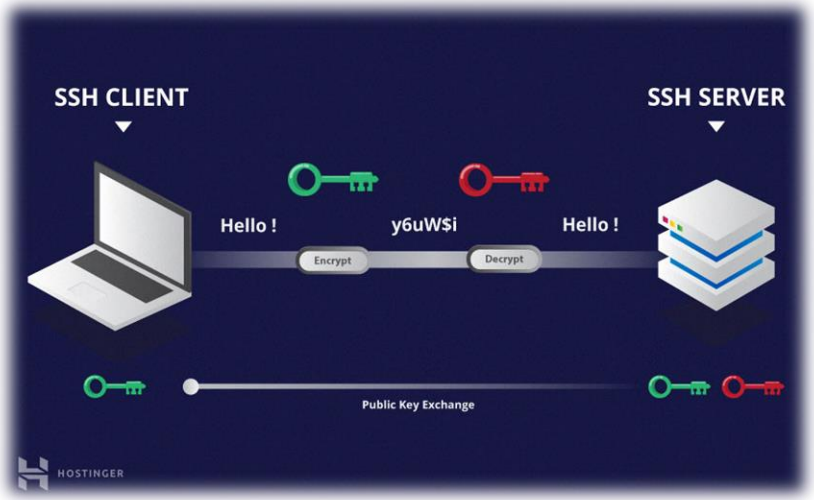
Uwierzytelnianie w Cisco IOS

UWIERZYTELNIANIE ZA POMOCĄ SERWERA CENTRALNEGO



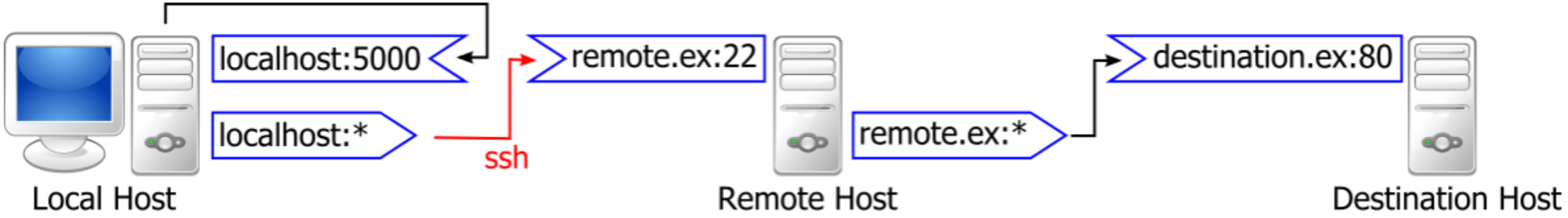
Metoda korzystająca z lokalnego uwierzytelnienia użytkowników jest przeciwieństwem autentykacji opartej na odwołaniach do centralnego serwera (bądź serwerów – redundancja na wypadek niedostępności serwera) na którym to znajduje się wspólna baza użytkowników dostępna dla wszystkich urządzeń. Na podstawie informacji zawartych w tej bazie przeprowadzane jest uwierzytelnienie i nadanie uprawnień. Korzystanie z zdalnej bazy zwalnia nas z konfiguracji bazy na każdym z urządzeń z osobna.

SSH (Secure Shell)



Cechy protokołu SSH:

- Działa w warstwie sesji modelu ISO/OSI oraz w warstwie aplikacji modelu TCP/IP
- Opera się na protokole transportu strumieniowego (TCP)
- Zapewnia dodatkowo kompresję
- Zapewnia tunelowanie sesji terminala
- Zapewnia tunelowanie protokołu X11 oraz innych.
- Zapewnia negocjację algorytmów kryptograficznych.



Szyfrowanie w IOS

- Typ 0 (jawny tekst) hasła widoczne dla wszystkich użytkowników

  switch(config)# line vty 0 15
  switch(config-line)# password cisco
  switch(config-line)# login

- Typ 5 (zaszyfrowany) – hasła są nieodwracalnie zaszyfrowane algorytmem MD5

  switch(config)# usename *uzytkownik* secret *haslo*

- Typ 7 (ukryty) – hasła są kodowane algorytmem Cisco i możliwe jest ich odkodowanie (www, key chain)

  switch(config)# service password-encryption

- Typ 4 (zaszyfrowany) – wykorzystywany do tego celu jest algorytm SHA256 z solą (salt)

VLAN (Virtual LAN)

VLANy specjalne:

Natywny VLAN – dzięki niemu ramki nieoznakowane, nie pochodzące od żadnego VLANu, są przesyłane przez porty typu trunk. Łącza trunkowe, czasami nazywane magistralami 802.1Q, potrafią obsługiwać ruch pochodzący właśnie z różnych sieci VLAN, ruch oznakowany, otagowany, ale również ruch z poza sieci VLAN.

VLAN zarządzający (ang. management VLAN), to rodzaj sieci wirtualnej, która utworzona jest na przełącznikach sieciowych po to aby odseparować ruch, tak zwany zarządzający (ang. management traffic), od faktycznego ruchu sieciowego, który generują komputery użytkowników.

VLAN typu czarna dziura (ang. black hole VLAN). Nieaktywne, nieużywane porty możemy dodać do jakiegoś fałszywego VLANu, w którym nie pracują żadne maszyny. Dzięki temu nawet jeśli jakiś intruz się do niego dostał, nie będzie mógł za wiele namieszać.

DHCP snooping

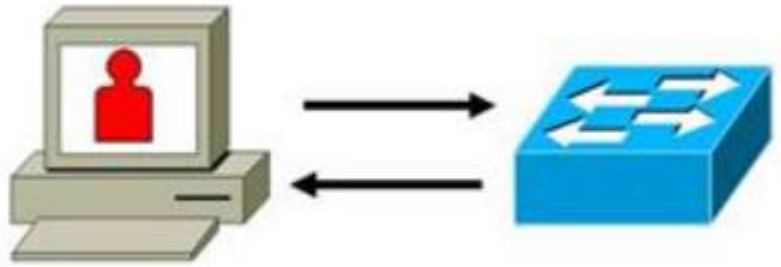
- Funkcjonalność DHCP snooping, polega na przypisaniu do konkretnego portu zaufanego serwera DHCP, a co za tym idzie, uniemożliwi podłączenie „lewego" serwera, do któregoś z innych portów. Dodatkowo funkcjonalność pozwala na ograniczenie ilości możliwych do wysłania z inny portów komunikatów – żądań DHCP Discover, co uniemożliwi wykonanie ataku.
- DHCP to usługa bazująca na transmisji broadcastowej, czyli rozgłoszeniowej i w związku z tym narażona jest na różnego rodzaju ataki. Korzystając z odpowiednich narzędzi, można spowodować, że serwer zostanie zalany komunikatami DHCP Discover i przestanie działać. Podłączony wówczas do sieci niezaufany serwer można zacząć przydzielać swoje adresy IP.

Tryby portów na switchu

- **switchport mode access** – w tej opcji port zawsze pozostanie w trybie nontrunking, będzie również próbował zmienić połączenie na nontrunking, jeśli mu się nie uda i tak pozostanie jako access
  switchport mode trunk – ten port zawsze będzie w trybie trunk, będzie również próbował zmienić połączenie na trunk, jeśli mu się nie uda i tak pozostanie jako trunk, jest to tryb domyślny dla trybów trunk i ma też nazwę On
  switchport mode dynamic auto – powoduje, że port zmienia się w port trunk, jeśli port po drugiej stronie jest skonfigurowany jako trunk lub desirable
  switchport mode dynamic desirable (dəˈzī(ə)rəbəl) – w tym trybie port aktywnie stara zmienić łącze na trunk, staje się łączem trunk w momencie gdy port sąsiadujący jest w trybie trunk, desirable lub auto
  switchport nonnegotiate – permanentny stan trunk, nie podlega żadnym negocjacjom, do powstania połączenia trunk port sąsiadujący musi być ustawiony w tryb trunk, połączenie w momencie gdy mamy switche od dwóch producentów

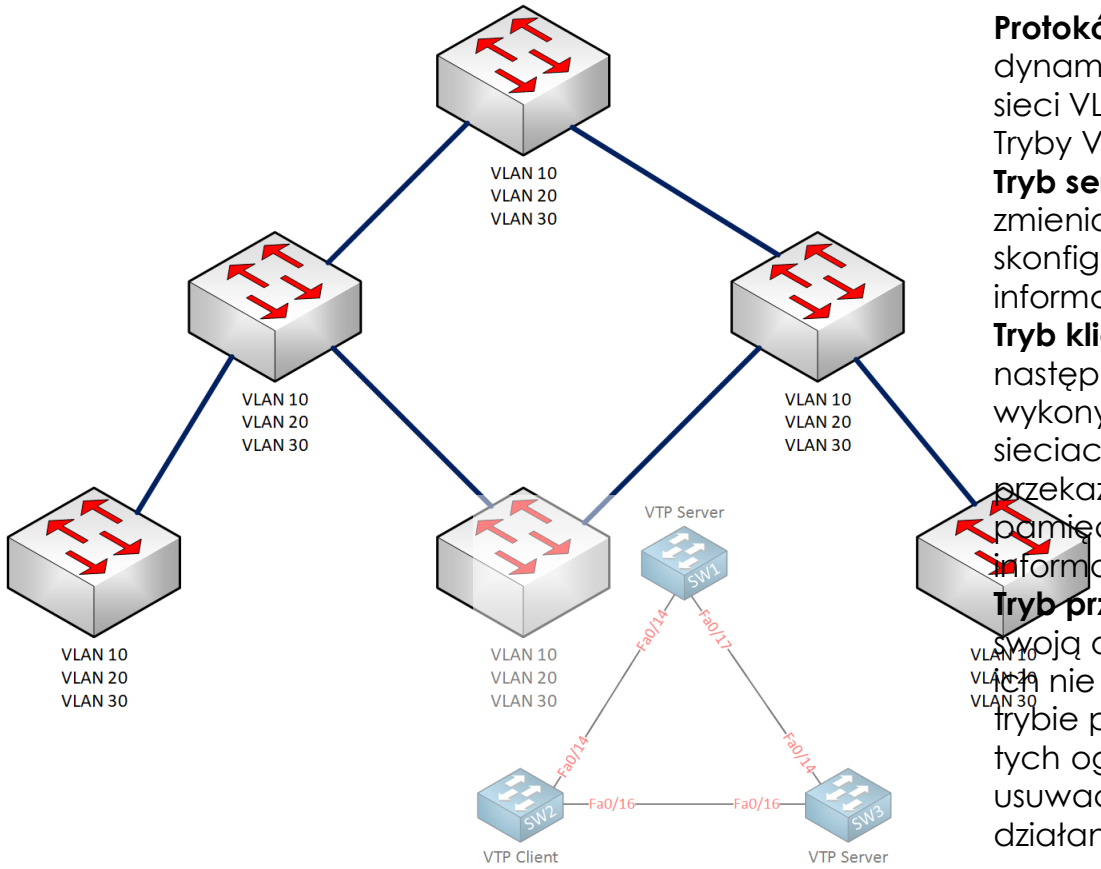
PORT-SECURITY

Port security restricts port access by MAC address.



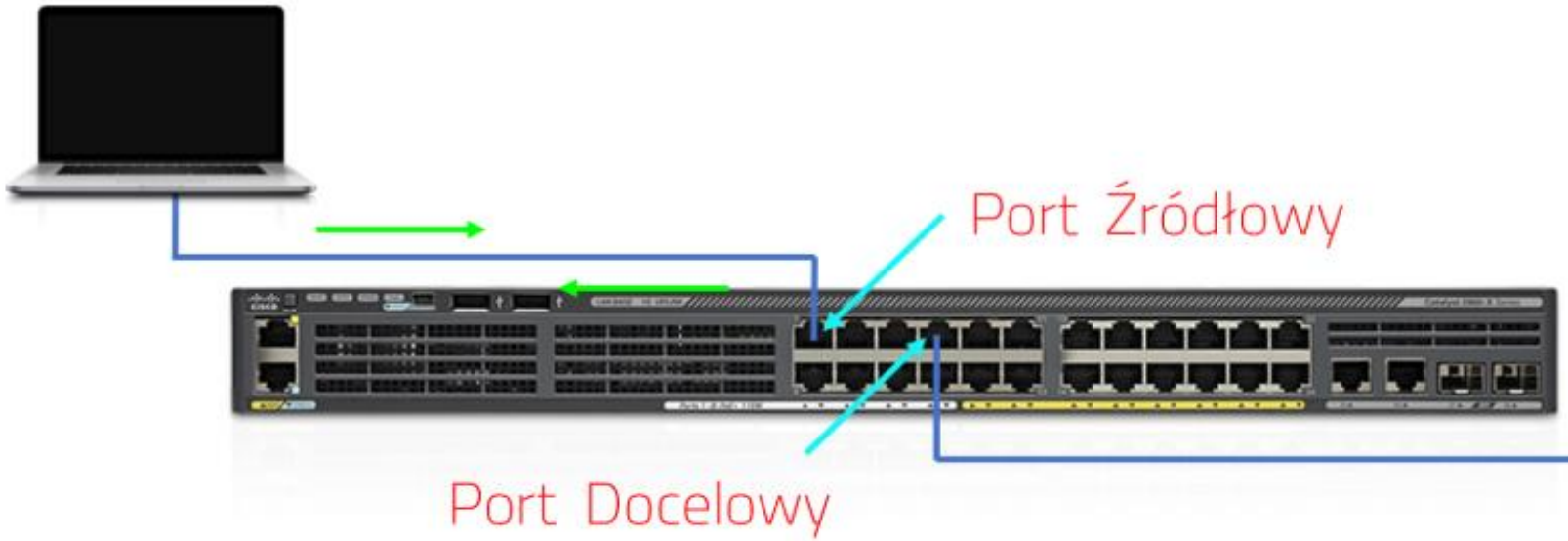
Port Security umożliwia określenie adresów MAC, które mogą komunikować się na danym interfejsie przełącznika a pomaga w tym protokół DTP (Discover Trunk Protocol).

Protokół VTP (ang. VLAN Trunking Protocol)



Protokół VTP (ang. VLAN Trunking Protocol) został stworzony tak aby zapewnić obsługę dynamicznego informowania sąsiednich przełączników o zmianach dokonanych w konfiguracji sieci VLAN. Zmiany te dotyczą dodania, usunięcia i zmiany nazwy sieci VLAN.
Tryby VTP:
Tryb serwera VTP (ang. VTP Server) może tworzyć, modyfikować i usuwać sieci VLAN a także zmieniać parametry konfiguracyjne sieci VLAN. Zadaniem serwera jest ogłoszenie informacji o skonfigurowanych sieciach VLAN innym przełącznikom a także synchronizowanie tych informacji. Jest to domyślny tryb pracy przełącznika.
Tryb klienta VTP (ang. VTP Client)- otrzymują od serwera informację o konfiguracji sieci VLAN i następnie ją stosują. Na przełączniku, który jest skonfigurowany jako klient nie można wykonywać operacji związanych z tworzeniem, modyfikowaniem i usuwaniem informacji o sieciach VLAN. Przełącznik w tym trybie ogłoszenia VTP przesyła dalej - przełącznik działa jako przekaźnik komunikatów VTP. Informacja o konfiguracji sieci VLAN jest przechowywana w pamięci przełącznika tylko podczas jego normalnej pracy. Po restarcie urządzenia bieżąca informacja o stanie sieci VLAN jest kasowana.
Tryb przezroczysty (ang. VTP Transparent) jest przeznaczony dla przełączników, które mają swoją odrębną konfigurację związaną z sieciami VLAN bądź konfiguracja dotycząca sieci VLAN ich nie dotyczy. Przełącznik działający w tym trybie nie bierze udziału w VTP. Przełącznik w tym trybie przekazują ogłoszenia protokołu VTP lecz wszystkie parametry konfiguracyjne zawarte w tych ogłoszeniach są przez niego ignorowane. W trybie tym można tworzyć, modyfikować i usuwać sieci VLAN lecz wprowadzona konfiguracja ma charakter lokalny czyli nie wpływa na działanie przełączników w skonfigurowanej domenie zarządzania.

Port Monitor (Port Mirroring)



Port mirroring (w przypadku urządzeń CISCO Port Monitor) jest funkcją, która pozwala na kopiowanie danych z danego, konkretnego portu lub grupy portów na inny. Funkcja te może być wykorzystywana w celach diagnostycznych przy analizowaniu ruchu sieciowego. Port mirroring może również zostać wykorzystany w celach dla nas niepożądanych. Hacker, który skonfiguruje kopiowanie danych na port, do którego podłączony jest jego komputer będzie miał dostęp do wszystkich informacji administracyjnych.

EtherChannel (Link Aggregation)

- **Agregacja łączy** (ang. link aggregation) polega na połączeniu ze sobą wielu portów fizycznych przełącznika w jedną logiczną całość. Dzięki takiemu połączeniu otrzymujemy grupę portów przez, które będą przesyłane dane przy czym od strony systemu IOS tak utworzona grupa będzie widoczna jako jeden port.

Tworząc grupę portów należy mieć na uwadze kilka zależności:

- porty muszą pracować z tą samą szybkością,
- powinny być w trybie pełnego duplexu,
- maksymalnie możemy utworzyć na przełączniku do 6 grup portów, przy czym maksymalna liczba portów w grupie wynosi 8;
- biorąc pod uwagę algorytm rozdzielający obciążenia na poszczególne porty lepiej tworzyć grupy, na które składają się 2, 4 albo 8 portów.

Protokół PAgP	
auto	Port pracujący w tym trybie samodzielnie nie inicjuje łącza, kanał zostaje utworzony pasywnie na zainicjowaną konfigurację.
desirable	Port pracujący w trybie desirable aktywnie negocjuje utworzenie kanału.
Protokół LACP	
passive	Port w sposób pasywny uczestniczy w procesie tworzenia łącza, negocjacja w tym trybie nie jest inicjonowana.
active	Port pracujący w trybie active aktywnie negocjuje utworzenie kanału.