|  |  |
| --- | --- |
|  | **Wyższa Szkoła**  **Ekonomii i Informatyki**  **w Krakowie** |

SEBASTIAN BZDEK, ŁUKASZ CHOJNACKI, KRYSTIAN JANAS

**[net-006-00]** **Przykład wykorzystania sieci VPN s2s do realizacji połączenia pomiędzy centralą i oddziałami**

**Kraków 2020-2021**

**Spis treści**

[1.Wstęp i cel projektu 2](#_Toc32403495)

[2.Wprowadzenie do zagadnień sieci Internetowej i zastosowanych technologii 3](#_Toc32403496)

[2.1.Sieć internetowa i jej struktura. 3](#_Toc32403497)

[2.2.Omówienie zagadnień Wirtualnych Sieci Prywatnych, protokołów sieciowych 12](#_Toc32403498)

[2.3.Charakterystyka i konfiguracja protokołu EIGRP 25](#_Toc32403499)

[3.Kolejny rozdział. 37](#_Toc32403500)

[4.Kolejny rozdział. 37](#_Toc32403501)

[Zakończenie 37](#_Toc32403502)

[Bibliografia 38](#_Toc32403503)

[Netografia 38](#_Toc32403504)

[Spis tabel 39](#_Toc32403505)

[Spis rysunków 39](#_Toc32403506)

# Wstęp i cel projektu

Bezpieczeństwo i prywatność przesyłanych informacji w obecnych czasach staje się coraz bardziej istotnym aspektem samego działania sieci. Niegdyś wyzwanie stanowiło samo przesyłanie danych z jednej lokalizacji, do drugiej. W obecnych czasach, gdzie przesyłane są terabajty danych wyzwaniem nie jest już sama możliwość przesyłania danych, a jej stabilność i bezpieczeństwo. Coraz to bardziej wyrafinowane urządzenia sieciowe i oprogramowanie do monitorowania sieci internetowych umożliwia sprawnie filtrowanie przesyłanych informacji. Otwarta wiedza i standaryzowane rozwiązania mają również swoje drugie dno.

Połączenia z ogólnodostępnymi, otwartymi lub nawet firmowymi, zamkniętymi sieciami niosą ze sobą zagrożenia. Nigdy nie jest wiadome czy informacje, które są wysyłane z urządzenia nie są przechwytywane i poddawane analizie. Z pozoru niegroźne prywatne wiadomości lub firmowe e-maile, mogą w odpowiednich rękach stanowić wartość. Mogą pomóc uzyskać dostęp do osobistych informacji lub wydarzeń, a w przypadku firm uzyskać dostęp do cen, kontaktów czy ustaleń związanych z projektami.

Jak zatem chronić informacje? W miarę rozrostu globalnej sieci internetowej oraz coraz to większego zaawansowania rozwiązań w obszarze informatyki, problem został dostrzeżony. Już w roku 1969[[1]](#footnote-1), czyli 30 lat po oficjalnym powstaniu sieci internetowej, powstały pierwsze sieci szyfrujące połączenie, nazwa potem Wirtualnymi Sieciami Prywatnymi (*ang. VPN, Virtual Private Networks*). Dzięki pierwszym próbom sprzed ponad 30 lat, możliwe jest w dniu dzisiejszym utworzenie bezpiecznych, często szyfrowanych połączeń, tuneli.

Projekt niniejszy, dotyczył będzie bezpiecznych, tunelowych połączeń pomiędzy dwoma lokalizacjami.

# Wprowadzenie do zagadnień sieci Internetowej i zastosowanych technologii

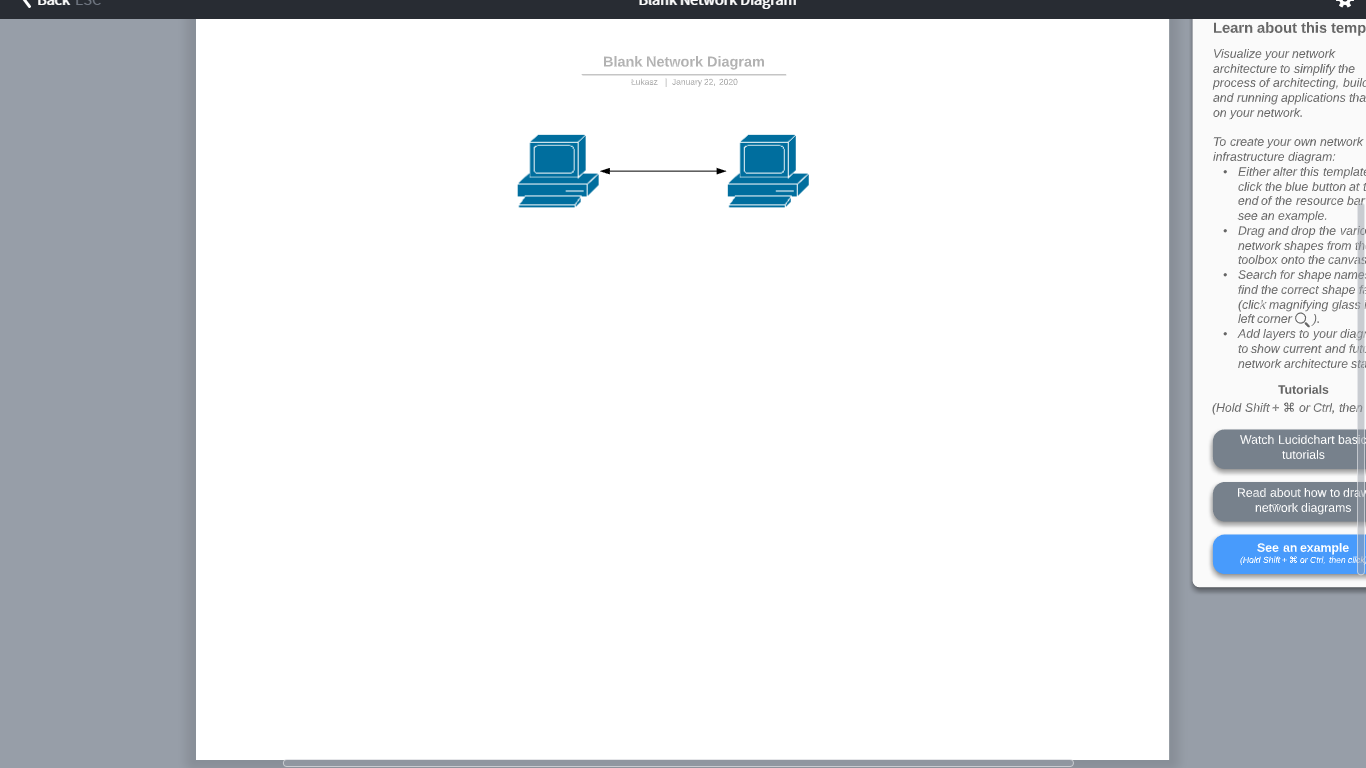
## Sieć internetowa i jej struktura.

Dziś w czasach powszechnego dostępu do informacji, trudno wyobrazić sobie dzień bez dostępu do sieci Internetowej. Obecnie sieć ta jest powszechnienie znana i dostępna z każdego przenośnego lub stacjonarnego. urządzenia posiadającego odpowiedni interfejs sieciowy. Swoje początki miała w latach 70 ubiegłego wieku jak projekt wojskowy. Dziś czasach postępującej digitalizacji, informatyzacji, automatyzacji i rozwijającej się technologii sztucznej inteligencji, informacja sama w sobie stanowi kluczową wartość. W roku 2017 sama informacja została okrzyknięta przez magazyn “The Economist” najdroższym zasobem na Ziemi, droższym niż ropa czy złoto[[2]](#footnote-2). Sam dostęp do sieci Internetowej staje się jedną z podstawowych potrzeb na Ziemi. Jako cywilizacja nie uporaliśmy się jeszcze z wyzwaniem zapewnienia dostępu do wody pitnej dla wszystkich mieszkańców planety. Nie stanowi to jednak przeszkody w planowaniu zapewnienia globalnego dostępu do sieci Internetowej, zapowiedzianej przez pioniera nowoczesnych rozwiązań Elona Muska. Częściowo działający już projekt oparty na 60 satelitach zawieszonych na orbicie okołoziemskiej, ma zapewnić darmowy dostęp do Internetu całej populacji globu[[3]](#footnote-3). Sam dostęp do informacji staje się zatem kluczową potrzebą, a jej zaspokojenie globalnym wyzwaniem.

Sieci komputerowe były pierwszym krokiem, dzięki któremu mógł powstać Internet. Połączenie umożliwiające komunikację, dwóch komputerów nie stanowiło, aż tak wielkiego wyzwania. Z biegiem czasu połączenia te, zwane topologia sieci komputerowej ewoluowały.

Pierwszym i najprostszym z nich jest połączenie bezpośrednie (ang. *Point-To-Point).* Przy wykorzystaniu fizycznego połączenia przewodami Ethernet, przy minimalnych kosztach możliwe jest zapewnienie bezpośredniej komunikacji dwóch komputerów, serwerów. Urządzenia połączone są za pomocą interfejsu sieciowego i przewodu. Jest to jedno z najprostszych, ale też najmniej użytecznych typów połączeń. Dwa urządzenia po zastosowaniu odpowiedniej konfiguracji, są w stanie komunikować się ze sobą. Praktyczne zastosowanie tych połączeń w obecnych czasach jest znikome, z racji braku możliwości szybkiego skalowania sieci.

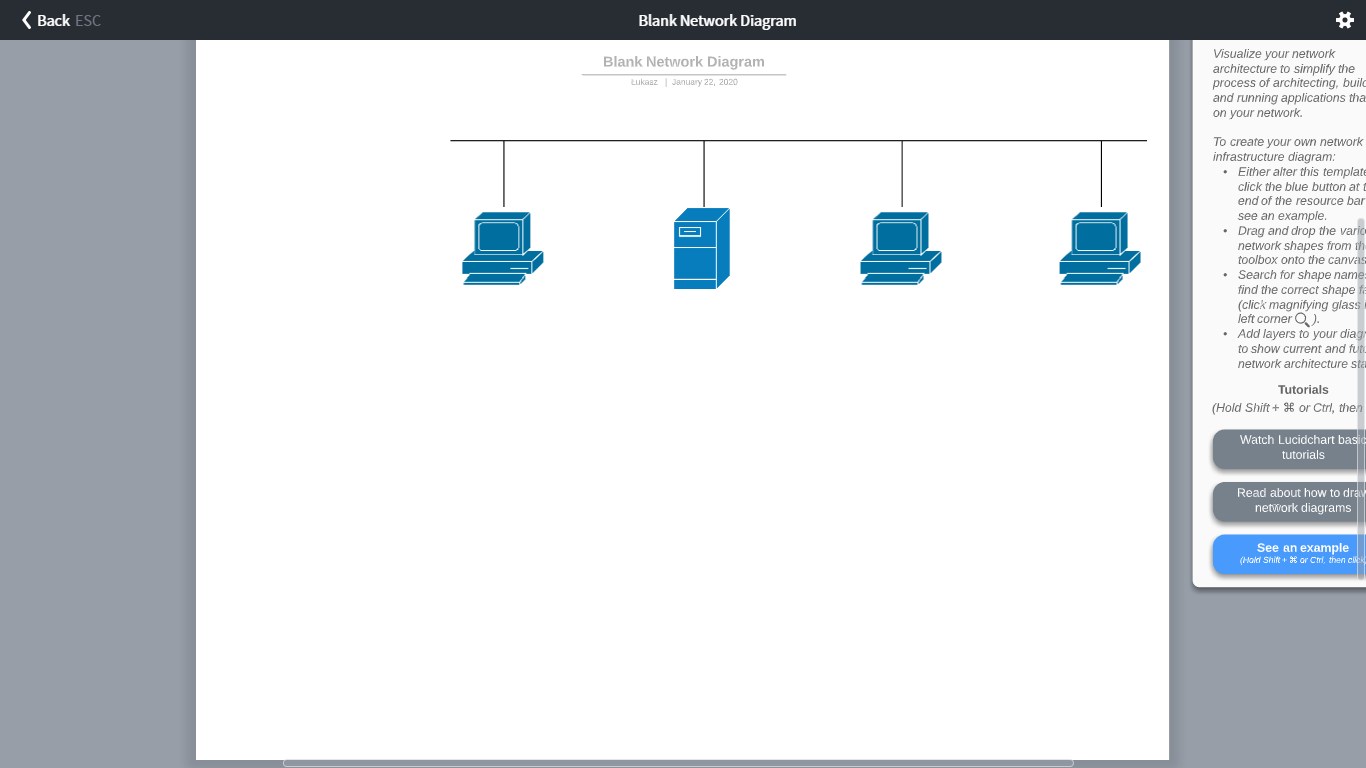
Rys. 1. Topologia połączenia bezpośredniego



źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Kolejnym typem połączenia jest topologia magistrali (*ang. Bus*). Poszczególne komputery lub serwery są połączone ze sobą liniowo wzdłuż ciągnącego się przewodu. Rozwiązanie to jest prostym sposobem na połączenie ze sobą kilku maszyn, jednak posiada istotną wadę. Uszkodzenie głównego przewodu w dowolnym miejscu, wzdłuż linii powoduje trudną do zlokalizowania usterkę, skutecznie wyłączającą całą sieć.

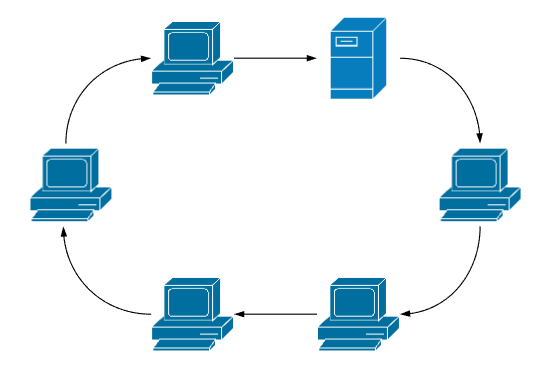
Rys. 2. Topologia magistrali



źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Kolejnym typem topologii, są topologie pierścienia. Sieć działa tutaj w oparciu o pierścień po obwodzie, którego podpięte są poszczególne komputery lub serwery. Sieci te posiadają większą dostępność niż dwa opisane już modele. Każde podłączone urządzenie końcowe jest podłączone do poprzedzającego i następującego po nim urządzenia. Powoduje to, że w przypadku awarii jednego połączenia, komunikacja może zostać zachowana.

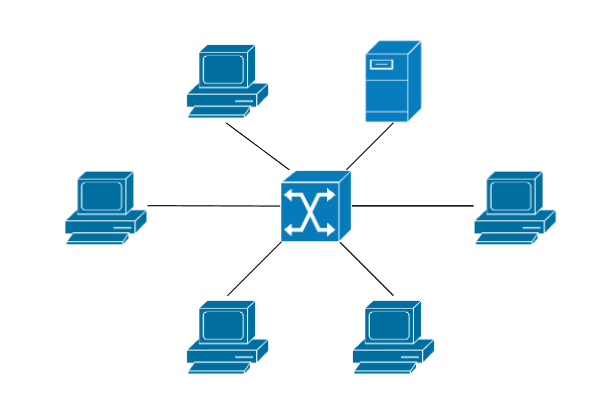
Rys. 3. Topologia pierścienia



źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Czwarty typ to topologie gwiazdy, ich struktura znacząco różni się od opisanych poprzednio topologii. Są one składową współcześnie stosowanych rozwiązań, opartych na przełączniku lub innym urządzeniu sieciowym. Centrum sieci, topologii stanowi urządzenie zarządzające ruchem w sieci. Takie rozwiązanie powoduje, że niedostępność którego z urządzeń końcowych, nie powoduje niedostępności całej sieci, jak w przypadku poprzednich typów topologii.

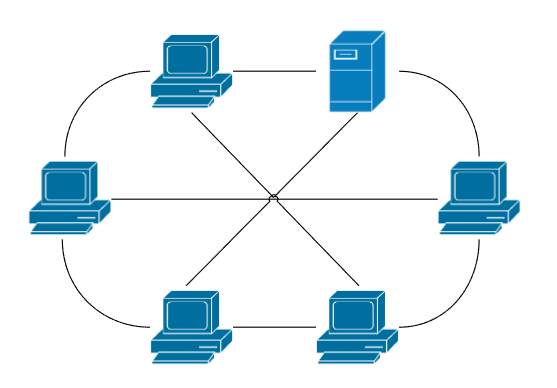
Rys. 4. Topologia gwiazdy



źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Topologia siatki, ta konfiguracja zapewnia zapasowe łącze, każdorazowo wybierana jest najkrótsza, najniższy koszt połączenia. W przypadku awarii jednego łącza, komunikacja może opierać się na pozostałych dostępnych połączeniach. W przypadku tej topologii, konkretne łącza mogą służyć konkretnym celom, np. jedne mogę służyć komunikacji, a drugie być stosowane do przesyłania danych.

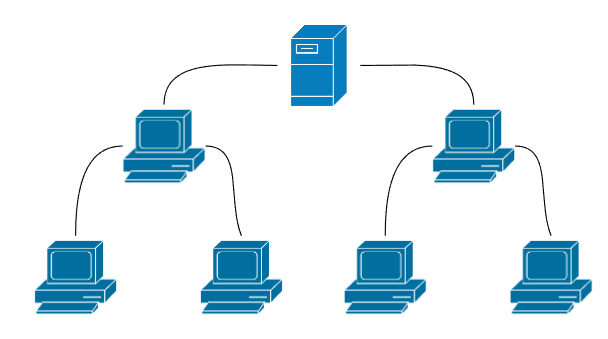
Rys. 5. Topologia siatki



źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Topologia drzewa, najczęściej wykorzystywana w obecnych środowiskach informatycznych ze względu na łatwą skalowalność. Dobrze sprawdza się w miejscach, gdzie zarządza się w grupami stacji komputerów lub serwerów. Cechą charakterystyczną tej topologii jest hierarchiczność. Pozwala również na segmentację sieci, łatwe zarządzanie oraz konfigurację danych poziomów w hierarchii..

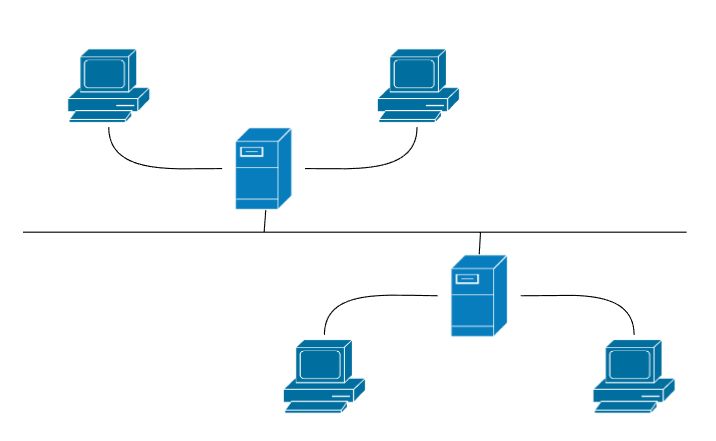
Rys. 6. Topologia drzewa



źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Topologia hybrydowa jest częściowym połączeniem wcześniejszych topologii. Jej plusem jest elastyczność i możliwość dostosowania konfiguracji do konkretnych zadań. Jednak jej złożoność oraz koszty stanowią wadę rozwiązania. Zaletą natomiast jest łatwe ustalenie usterki występującej w środowisku, przez weryfikację od góry do dołu, gdzie komunikacja szwankuje.

Rys. 7. Topologia hybrydowa



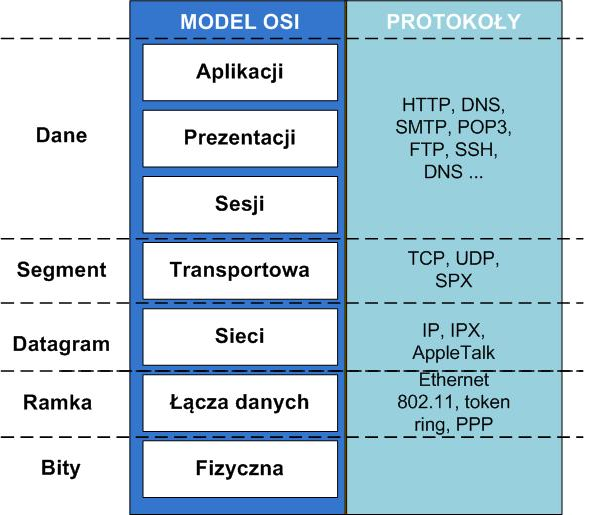
źródło: opracowanie własne na podstawie https://www.educba.com/types-of-network-topology/

Wielkość konkretnej sieci i jej konfiguracja stanowi o jej zaszeregowaniu. Na początku hierarchii sieci znajdują się sieci zwane LAN (*ang. Local Area Network)*. Są to lokalne sieci, w obrębie biura, budynku, stanowią połączenia dostępnych w danej lokalizacji urządzeń i są zarządzane lokalnie. Sieci lokalne, stanowią składową większej sieci miejskiej, nazwanej w skrócie MAN (*ang. Metropolitan Area Network).* Sieci te zarządzane są najczęściej przez dostawców usług Internetowych *(ang. ISP - Internet Service Providers)*. Sieci LAN i MAN są częścią WAN (*ang. Wide Area Network)*, dużych obszarów sieci. WAN nie są najczęściej zarządzane przez jedną organizację, najczęściej stanowią strukturę zarządzaną przez kolektyw.

Aby rozumienie działania sieci oraz jej analiza pod kątem problemów było prostsza, opracowane zostały modele segmentujące sieć. Najpopularniejszym na przestrzeni lat stał się model OSI[[4]](#footnote-4) *(ang. Open Systems Interconnection Model).* Wyróżnia on siedem warstw składających się na sieć Internetową:

* Warstwa 1. Fizyczna, odpowiada za transmisję danych przez sieć przy pomocy fizycznych połączeń.
* Warstwa 2. Łącza danych, kontroluje i nadzoruje przesyłane przez sieć informacje. Operuje na adresach MAC.
* Warstwa 3. Sieci, zapewnia możliwość komunikacji urządzeń między sobą. Określa ścieżki dostępowe od nadawcy do odbiorcy. Operuje na adresach IP.
* Warstwa 4. Transportowa, odpowiada za przesyłanie danych odpowiednimi protokołami TCP lub UDP. Analizuje zgubione pakiety i wymusza ich retransmisję.
* Warstwa 5. Sesji, odpowiada za utrzymuje połączenia i jego trwałość.
* Warstwa 6. Prezentacji, odpowiada za poprawną prezentację i strukturyzację danych.
* Warstwa 7. Aplikacji, warstwa wykorzystywana przez użytkowników końcowych, wykorzystywana przez np. aplikacje sieciowe do komunikacji człowiek-komputer.

Rys. 8. Model OSI i stosowane w warstwach protokoły



źródło http://edu.pjwstk.edu.pl/wyklady/sko/scb/w2.html

Do zaistnienia opisanych wcześniej topologii sieciowych, konieczne są odpowiednie urządzenia sieciowe. Odpowiadają one za zarządzanie i organizację infrastruktury sieciowej. Celowo pominięte zostaną opisy przewodów łączących urządzenia, ponieważ obszar ten nie dotyczy zagadnień projektu.

Sprzęt techniczny ewoluuje niezwykle szybko, coś co kilka, kilkanaście lat temu było szczytem techniki i budziło zachwyt, dziś już nie interesuje nikogo. Moc obliczeniowa komputerów, które wyniosły na orbitę okołoziemską rakiety Apollo, dziś używane jest do zasilania grających kartek-pozytywek. Popularne obecne smartfony posiadają już wydajność komputerów osobistych sprzed kilku lat, a postęp nadal trwa. Tak samo wygląda sytuacja na rynku sprzętu sieciowego. Producenci firm, których obecnie jest więcej niż kiedykolwiek wcześniej, starają się uzyskać jak największą część rynku dla siebie. Urządzenia ewoluują, interfejsy są upraszczane. Do samych urządzeń zaczyna się dołączać dodatkowo sprzęt analizujący, nierzadko połączony z rozwiązanymi chmurowymi (zdalne serwery o dużej mocy obliczeniowej). Wszystko to wymuszone jest postępem technologicznym oraz nowymi zagrożeniami i problemami, z którymi muszą mierzyć się współcześni administratorzy systemów i sieci. Zanim to wszystko się zaczęło, sprzęt sieciowy nieśmiało rozwijał się na początku lat 60 ubiegłego wieku, ewoluując w wieloprocesorowe od lat 90 ubiegłego stulecia, które rozwijają się nieustannie, aż po dziś dzień.

Repeater[[5]](#footnote-5) (*pol. Wzmacniacz sieciowy*) - działa na fizycznej warstwie sieci. Zadaniem tego urządzenia jest powielanie otrzymanego sygnału sieciowego danej sieci oraz pakietów i przesyłanie ich dalej. Stosowany jest w miejscach, gdzie występuje słaby zasięg, który należy przedłużyć np. sieci WiFi.

Hub (*pol. Koncentrator sieciowy*) - jest wieloportowym urządzeniem powielającymi sygnał. Może być stosowany np. do łączenia kilku typów przewodów, gdzie stosowane jest jednocześnie wiele topologii. Urządzenie to nie filtruje ruchu sieciowego, zatem pakiety przesyłane do wszystkich pozostałych urządzeń. Urządzenia te nie posiadają również mocy obliczeniowej oraz możliwości odnajdywania najkorzystniejszych ścieżek połączeń. Te dwie wady powodują, że generują dużo niepotrzebnego ruchu w sieci. Urządzenia typu Hub dzielą się na aktywne, posiadające niezależne zasilanie i możliwość powtarzania i wzmacniania sygnału oraz pasywne, nieposiadające tych funkcji.

Bridge (*pol. Most sieciowy*), urządzenie działa na warstwie danych. Jest posiada on możliwość wzmacniania i powtarzania sygnału. Dodatkowo pozwala na filtrowanie zawartości za pomocą adresów MAC źródłowego i docelowego. Za jego pomocą można łączyć różne sieci LAN.

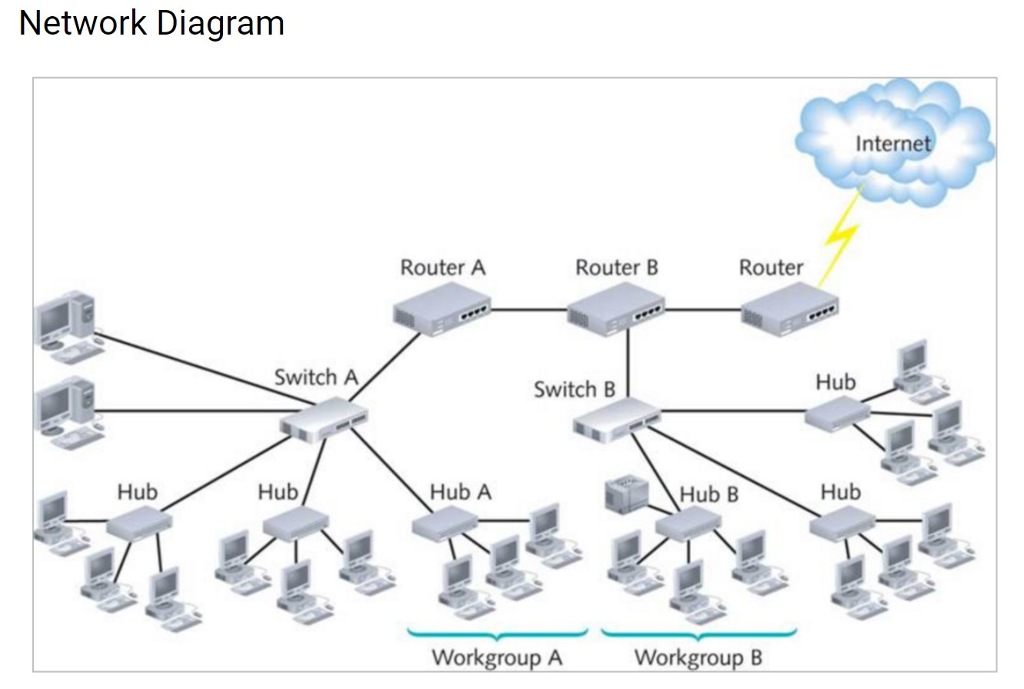
Switch (*pol. Przełącznik sieciowy*), switch jest rodzajem mostu sieciowego pozwalającym na zwiększenie wydajności sieci. Posiada więcej portów i wydajność niż zwykły most. Działa na warstwie danych modelu OSI, przesyłając pakiety i ramki. Rozpoznaje urządzenia za pomocą adresów MAC urządzeń, w obszarze sieci LAN. Istotną cechą jest walidacja sieci pod kątem błędów przed przesyłaniem pakietów dalej. Switch posiada znacznie większą ilość dostępnych dla połączeń portów, zazwyczaj 24 lub 48.

Router (*pol. Trasownik*), jest urządzeniem podobnym do przełącznika sieciowego, jednak jego praca opiera się na adresach IP przechowując adresy w pamięci zwanej tabelą routingu. Operuje on głównie w zakresie warstwy sieciowej modelu OSI. Dzięki routerom, możliwe jest połączenie sieci LAN i WAN. Routery mogą pomóc sprawie zarządzać siecią, jej wydajnością, bezpieczeństwu oraz analizie ruchu. Domowe routery pełnią zazwyczaj również funkcję Access Point i Firewall. Ze względu na zastosowane podzespoły trasownik działa i przetwarza dane szybciej niż przełącznik sieciowy.

Wireless Access Point lub Access Point (*pol. Bezprzewodowy Punkt dostępu),* urządzenie sieciowe zapewniające możliwość połączenia urządzeń za pomocą sieci bezprzewodowej Wi-Fi. Urządzenie połączone jest z trasownikiem za pomocą fizycznych przewodów, dzięki niemu możliwe jest przekonwertowanie sygnału otrzymywanego za pomocą przewodów na sygnał sieci bezprzewodowej. Dzięki czemu bez dodatkowych fizycznych połączeń zasięg sieci LAN może zostać rozszerzony. Większość punktów dostępu zapewnia bezprzewodowe połączenie dla 255 urządzeń.

Firewall (*pol. Zapora sieciowa)*, urządzenie sieciowe zapewniające filtrację przychodzącego lub wychodzącego ruchu w sieci przez przesiewanie ruchu na podstawie adresów IP, MAC lub konkretnych portów. Zapora sieciowa stanowi podstawę zabezpieczenia większości sieci LAN. Nowoczesne i zaawansowane urządzenia pozwalają dodatkowo na analizę ruchu pod kątem “zachowania się” danego połączenia, zwaną heurystyką.. Coraz więcej firm wprowadza na rynek zapory sieciowe nowej generacji (*ang. Next-Generation Firewall)*. Zapewniają one funkcje wykrywania intruzów (niechcianych połączeń). Umożliwiają dodatkowo szyfrowanie ruchu wewnątrz sieci, inspekcję ruchu, filtrowanie zawartości Internetu dostępnej dla użytkowników sieci LAN.

Rys. 9. Przykład schemat topologii sieciowej ze wskazaniem urządzeń sieciowych



źródło: https://www.chegg.com/homework-help/questions-and-answers/simple-network-problem-router-lan- wan-please-help-thanks-1-diagram-router-master-router-ro-q24721095

## 

## Omówienie zagadnień Wirtualnych Sieci Prywatnych, protokołów sieciowych

Bezpieczeństwo w sieci jest istotnym zagadnieniem dla wielu firm jak i użytkowników końcowych. Od kilku dekad cyberbezpieczeństwo jest ciągle udoskonalane, hakerzy również rozwijają swoje umiejętności i stosują coraz to nowe techniki łamania zabezpieczeń. Zanim dostęp do Internetu stał się łatwy i tani, duże przedsiębiorstwa wydawały majątek tworząc właśnie rozwiązania sieciowe zapewniające bezpieczeństwo. Używanie usług telekomunikacyjnych takich jak linie dzierżawione, Frame Relay czy Asynchronus Transfer Mode (ATM) do połączenie rozrzuconych siedzib było na porządku dziennym. Wzrost popularności Internetu przyśpieszył prace nad tą technologia oferując coraz szybszy dostęp przy jednoczesnym malejącym koszcie dostępu. Pozwoliło to zrezygnować z drogich rozwiązań tunelowania połączenia, przerzucając ruch na publiczną sieć Wide Area Network (WAN). Powstanie VPN było kluczową technologia służącą do Technologia VPN została opracowana, aby umożliwić zdalnym użytkownikom i oddziałom dostęp do aplikacji i zasobów korporacyjnych. Aby zapewnić bezpieczeństwo, prywatne połączenie sieciowe jest ustanawiane za pomocą szyfrowanego protokołu tunelowania warstwowego, a użytkownicy VPN używają metod uwierzytelniania, w tym haseł lub certyfikatów, aby uzyskać dostęp do VPN. W innych aplikacjach użytkownicy Internetu mogą zabezpieczyć swoje połączenia za pomocą sieci VPN, aby obejść ograniczenia geograficzne i cenzurę lub połączyć się z serwerami proxy w celu ochrony tożsamości osobistej i lokalizacji w celu zachowania anonimowości w Internecie.

Inwigilacja z każdym dniem jest coraz większa. Użytkownicy w trosce o swoją prywatność coraz częściej decydują się na korzystanie z Internetu za pośrednictwem połączenia VPN. Czym tak naprawdę jest ten VPN ?

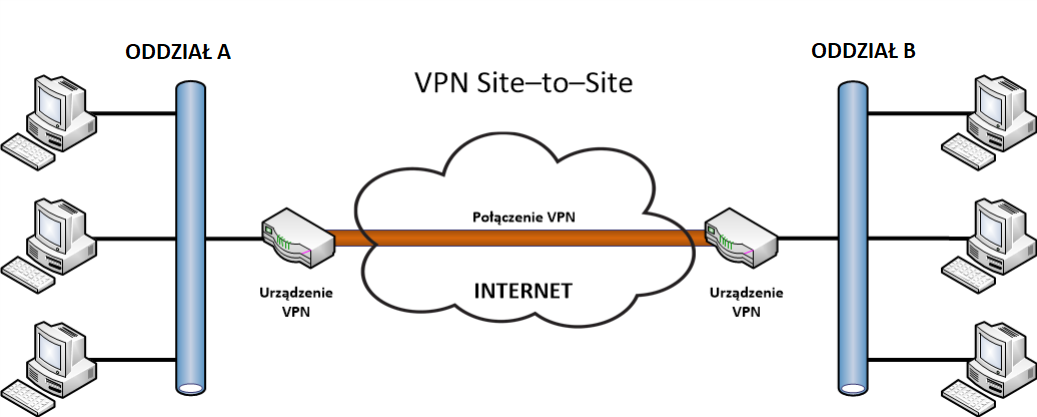
VPN (ang. *Virtual Private Network*, Wirtualna Sieć Prywatna) – tunel, przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet) w taki sposób, że węzły tej sieci są przezroczyste dla przesyłanych w ten sposób pakietów. Można opcjonalnie kompresować lub szyfrować przesyłane dane w celu zapewnienia lepszej jakości lub większego poziomu bezpieczeństwa. Określenie „wirtualna” oznacza, że sieć ta istnieje jedynie jako struktura logiczna działająca w rzeczywistości w ramach sieci publicznej, w odróżnieniu od sieci prywatnej, która powstaje na bazie specjalnie dzierżawionych w tym celu łącz. Pomimo takiego mechanizmu działania stacje końcowe mogą korzystać z VPN dokładnie tak, jak gdyby istniało pomiędzy nimi fizyczne łącze prywatne. Początki tego protokołu sięgają 1996 roku, kiedy to Microsoft stworzył protokół Point-to-Point Tuneneling Protocol (PPTP). W 1999 roku technologia ta została udostępniona. Od tamtej pory technologia ta znacznie się rozwinęła, tworząc to kolejne sposoby zdalnego bezpiecznego połączenia[[6]](#footnote-6).

Powyższa definicja dokładnie opisuje mechanizm i sens używania tej technologii. Niestety nie wskazuje jak bardzo jest potrzeba z punktu widzenia firm. Dostęp do zasobów firmy i jej sieci jest elementem kluczowym, bez którego większość pracowników nie byłaby w stanie realizować swoich podstawowych zdań. Czasy, w których pracownik musiał być fizycznie w firmie, żeby mieć dostęp do swoich plików już dawno minął. Teraz może to zrobić z dowolnego miejsca, za pośrednictwem Internetu i prywatnego komputera. Tak więc największą zaletą połączenia VPN dla firm, jest możliwość zdalnej pracy pracownika tak jakby znajdował się w oddziale firmy.

Kolejnym istotnym zagadnieniem dla całości projektu, są Metody połączenia zdalnego. Rozróżniamy dwa główne typy połączeń dostępu zdalnego.

Pierwszym z nich jest połączenie typu *Site-to-site.* Znajduje głownie zastosowanie w korporacjach przez rodzaj stosowanego połączenia. Jest to połączenie router-router. Faktem jest to, że wiele firm ma swoje biura w różnych lokalizacjach, w różnych miastach czy nawet innych państwach. *Site-to-site* służy do połącznie głównej sieci z sieciami innych biur. Ten system zwany jest również VPN oparty o *Intranet*. Odwrotne rozwiązanie również jest możliwe, połączenie z innymi w firmami w ten sam sposób, co klasyfikowane jest pod nazwą *Extranet* VPN. Podsumowując, omawiana forma połączenia pozwala zbudować wirtualny most, który łączy sieci w różnych miejscach za pośrednictwem Internetu oraz utrzymuję bezpieczną i prywatną komunikację miedzy tymi sieciami

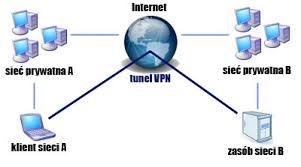
Rys. 10. Połączenie Site-to-Site



Źródło: http://slow7.pl/sieci-komputerowe/item/117-konfiguracja-polaczenia-vpn-w-srodowisku-windows-lecz-nie-tylko

Drugim typem połączenia jest konfiguracja typu Client-site, również często używana przez firmy, w celu zdalnego dostępu pracownika z komputera do zasobów firmy bądź firmowej infrastruktury

Rys. 11. Połączenie Client-Site

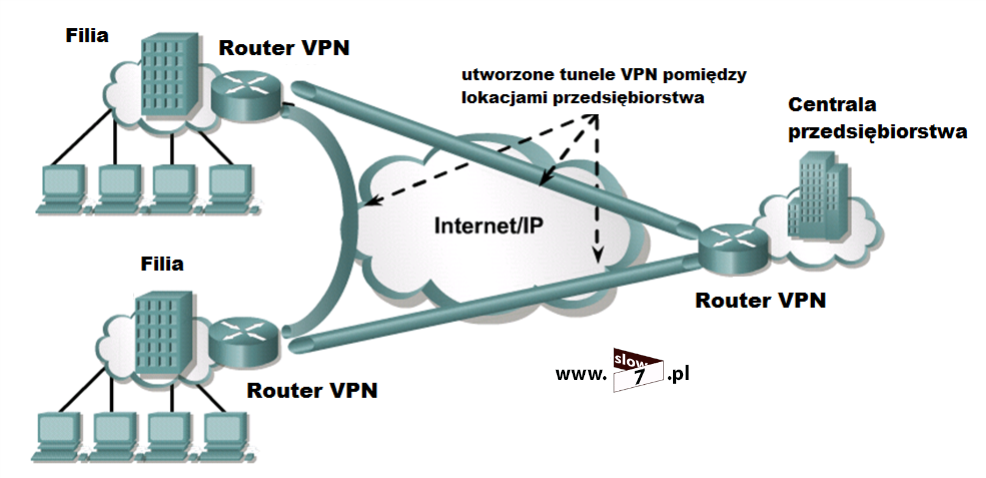
****

źródło: http://www.haxnet.pl/pages-print-114.html

Wachlarz możliwości VPN jest dosyć rozległe. Każda osoba może użyć sieci vpn do zorganizowania sieci firmowej: od dużych korporacji po małe firmy. Wirtualna sieć prywatna może również połączyć wnętrze kamery monitoringu, systemu alarmowe czy kontrole dostępu. Jest dość wygodne rozwiązanie, z powodu braku konieczności ciągnięcia fizycznie kabla. Można postawić sieć na istniejącej już sieci lub podzielić ja na kilka innych. Używa się również do łączenia serwerów klastrów obliczeniowych, aby zwiększyć ich dostępność i redundancję.

Częstym przypadkiem użycia tuneli jest łączenie zdalnych, geograficznie odseparowanych stron przez istniejącą sieć, w szczególności routing przez infrastrukturę publiczną (taką jak Internet). Gdy są używane w ten sposób, tunele tworzą sieci nakładkowe VPN między zdalnymi witrynami. Pakiety przeznaczone do zdalnych sieci prywatnych są enkapsulowane w nowym nagłówku IP, który jest wykorzystywany do przechodzenia przez publiczny Internet

Rys. 12. Schemat połaczenia VPN



źródło : omsosik.cba.pl

Inna forma wykorzystania omawianej formy łączności opiera się na sesji. Sesja używana jest głownie w celu dostępu do wielu usług, w tym takich które przetwarzają wrażliwe dane ( związane z finansami, opieką zdrowotną czy prawem). Nawet zwykły użytkownik może używać owego połączenia, zalecane jest dla zabezpieczenia urządzeń z systemem android i iOS, aby podczas łączenia z jakąś siecią publiczną używać bezpiecznego węzła ( jak dom, router, czy dostawca VPN) w celu ukrycia swojego ruchu przez potencjalnym przechwyceniem.

Praktycznym przypadkiem użycia VPN’a jest obejście pewnych ograniczeń dostępu. Mowa tutaj o uzyskaniu dostępu do zablokowanych zasobów sieciowych, które są niedostępne dla użytkownika danego rejonu (np. na terenie Chin). Według raportu sporządzonego przez 2014 roku przez firmę GlobalWeblndex, ponad 166 milionów ludzi użyło VPN-a do uzyskania dostępu do sieci społecznościowych.

Rys. 13. Wizualizacja braku dostępu do treści po połączeniu VPN



źródło : shutterstock.com

Równie istotnym zagadnieniem co protokoły, jest samo bezpieczeństwo połączenia zdalnego. Współczesne implementacje sieci VPN dysponują wieloma mechanizmami, które pozwalają na bardzo wysoki poziom bezpieczeństwa. Wydawać by się mogło, ze hasło i odpowiednio skonfigurowane szyfrowanie wystarczy. Możemy wyróżnić 3 główne filary:

* Uwierzytelnienie (*ang. Authentication*) – jest kontrolą czy dany system komputerowy jest rzeczywiście tym za który się podaje. Jest to weryfikacja przeprowadzana po stronie klienta jak i serwera VPN. Zapobiega to dwóm niebezpiecznym sytuacjom – kiedy ktoś wejdzie w posiadanie elementu do autoryzacji (np.: hasła) oraz kiedy następuje próba podszycia się pod serwer, tak zwany koncentrator VPN.
* Autoryzacja (ang. *Authorisation*) – weryfikuje czy dany klient ma prawo do wybranej sieci lub zasobu. Jest wiele sposobów jak może się odbywać, na podstawie hasła czy zestawu kluczy. Często jest to implementowane w postaci – autoryzowany jest klient uwierzytelniony – jeśli ustalimy tożsamość klienta VPN , dopuszczamy do dostępu do naszych zasobów.
* Szyfrowanie *(ang.Cipher*) – podstawa działania tunelu VPN. Polega na zabezpieczeniu transportowanych pakietów danych w taki sposób aby nikt nie mógł ich podsłuchać, również nie pozwala na ich modyfikacje czy wstrzyknięcia obcej transmisji.

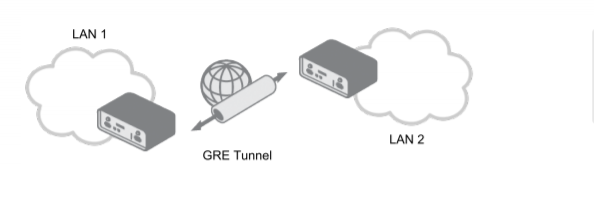
Nie licząc wymienionych trzech filarów istnieje wiele innych mechanizmów, które zapewniają bezpieczeństwo przesyłanej transmisji. Przykładowo *OpenVPN* zawiera ciekawy mechanizm o nazwie HMAC (*Keyed-Hash Message Authentication Code*).

Mechanizm wykorzystuje osobny klucz do podpisania każdego pakietu kontrolnego przy uruchamianiu transmisji. Dane, które nie zostaną podpisane takim kluczem są automatycznie odrzucane. Dzięki temu dla osób z zewnątrz OPENVPN będzie niewidoczny, z tego powodu że będzie odrzucał wszystkie próby połączenia nie podpisane certyfikatem. Stanowi to doskonałe zabezpieczenie przed atakami DoS (*Denial of Service)*, a także blokuje wszystkie próby szpiegowania. Minusem tego rozwiązania jest małe utrudnienie dla nowych klientów, które utrudnia diagnostykę i wysyła fałszywe komunikaty o niedostępności usługi.

Trzeba pamiętać, że sieci VPN są tylko narzędziem, które pozwalają uzyskać założony cel. Dostarczają nam różnych mechanizmów szyfrowania, autoryzacji i uwierzytelnienia. Zapewniają bezpieczeństwo i integralność przesyłanych danych. Nawet najlepsze zabezpieczenia mogą nic nie dać w starciu z nieostrożnym użytkownikiem. To właśnie on, jest zawsze najsłabszym ogniwem całego systemu i to na jego zachowania trzeba zawsze zwracać największą uwagę.

Kolejnym ważnym protokołem jest Generic Routing Encapsulation w skrócie GRE, jest on protokołem komunikacyjnym używanym do ustanowienia bezpośredniego połączenia punkt-punkt między węzłami sieci. Będąc prostą i skuteczną metodą przesyłania danych przez sieć publiczną, taką jak Internet, GRE pozwala dwóm uczestnikom współdzielić dane, których nie byliby w stanie udostępnić przez samą sieć publiczną. Tunel GRE tworzy połączenie dwóch sieci LAN w jedną.

Rys. 14. Wizualizacja działania tunelu GRE



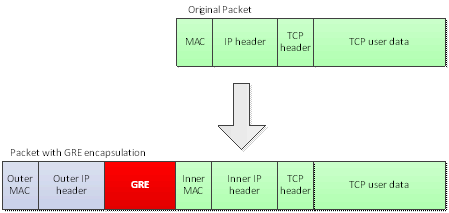
Zródło support.elmark.com.pl

Tunel GRE służy do enkapsulacji dowolnego protokołu warstwy na innym protokole dowolnej warstwy. Ogólnie GRE pozwala na utworzenie tunelu przy użyciu określonego protokołu, który następnie ukrywa zawartość innego protokołu przenoszonego w tunelu. Tunelowanie zapewnia mechanizm transportu pakietów jednego protokołu w ramach innego protokołu. Protokół, który jest przenoszony, nazywany jest protokołem pasażera, a protokół używany do przewozu protokołu pasażera nazywany jest protokołem transportowym. Generic Routing Encapsulation jest jednym z dostępnych mechanizmów tunelowania, który wykorzystuje protokół IP jako protokół transportowy i może być używany do przenoszenia wielu różnych protokołów pasażerskich. Tunele zachowują się jak wirtualne połączenia punkt-punkt, które mają dwa punkty końcowe zidentyfikowane przez źródło tunelu i adresy docelowe tunelu w każdym punkcie końcowym.

Aby pakiet enkapsulowany został przesłany, konieczne jest utworzenie tunelu. Po założeniu tunelu pakiet GRE może podróżować bezpośrednio między dwoma punktami końcowymi. To, że tunel jest wirtualny, oznacza, że ​​nawet gdy pakiet podróżuje przez inne routery, nie ma interakcji z jego ładunkiem. Zamiast tego pakiet jest wypychany do przodu, aż osiągnie punkt końcowy tunelu, gdzie pakiet zewnętrzny jest dekapsułkowany, a ładunek parsowany.

Obsługa dla wielu protokołów i typów pakietów sprawia, że ​​jest on idealny do rozwiązywania wielu problemów napotykanych podczas próby utworzenia sieci VPN przez Internet. Najbardziej oczywistym problemem jest to, że prywatne adresy używane w przedsiębiorstwie nie mogą być kierowane przez publiczny Internet. GRE rozwiązuje to poprzez obudowanie nagłówka IP prywatnym adresowaniem za pomocą zewnętrznego nagłówka IP, który wykorzystuje adresowanie publiczne.

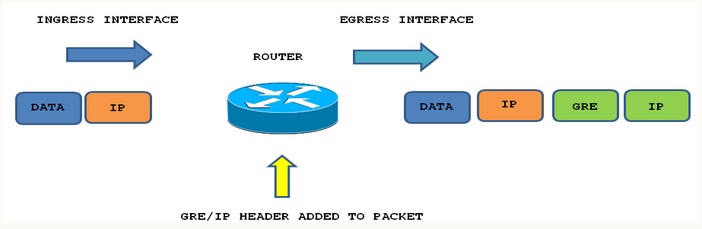
Rys. 15. Struktura pakietu z GRE



Źródło:https://docs.microsoft.com/pl-pl/windows-hardware/drivers/network/

Protokół ten jest podobny do wieloaspektowej usługi dostawy, która może obsługiwać każdy rodzaj paczki transportując je od drzwi do drzwi. Po prostu bierze wszystko, co zostało wprowadzone, umieszcza to w jednym ze swoich pudełek, przykleja etykietę adresową i zabiera ją do miejsca docelowego.

Rys. 16. Przekierowanie pakietu GRE



Źródło:https://docs.microsoft.com/pl-pl/windows-hardware/drivers/network/

Tunele GRE zostały tak zbudowane, aby być całkowicie bezstanowe. W praktyce oznacza to, że każdy punkt końcowy tunelu nie przechowuje żadnych informacji o stanie ani dostępności zdalnego punktu końcowego tunelu. Efektem tego jest brak możliwości obniżenia linii interfejsu tunelu GRE przez lokalny router punktu końcowego kiedy zdalny koniec tunelu jest nieosiągalny. Nie pozwala to na usunięcie wszelkich tras (szczególnie tras statycznych) z tabeli routinugu pozwalając na instalacje alternatywnej trasy w celu wybrania alternatywnego następnego przeskoku lub interfejsu. Interfejs tunelu GRE pojawia się, gdy tylko zostanie poprawnie skonfigurowany o pozostaję włączony, dopóki istnieje prawidłowy adres źródłowy tunelu. Docelowy adres IP tunelu musi być uwzględniony w routingu. Oznacza to, że GRE pozostaje aktywny, nawet jeśli pakiety tuneli nie docierają do drugiego końca tunelu.

Kluczowym jest połączeń VPN jest protokół IPSec (*Internet Protocol Security*) jest protokołem sieciowy stosowanym do uwierzytelniania i szyfrowania pakietów danych w celu zapewnienia bezpiecznej szyfrowanej komunikacji między dwoma komputerami za pośrednictwem sieci VPN. Protokół IPSec obejmuje protokoły wzajemnego uwierzytelniania między klientami na początku sesji oraz negocjowania kluczy kryptograficznych używanych podczas sesji. Protokół IPSec może chronić przepływy danych między parą hostów (host-host), między parą bram bezpieczeństwa (sieć-sieć) lub między bramą bezpieczeństwa a hostem (sieć-host). Wykorzystuje usługi bezpieczeństwa kryptograficznego do ochrony komunikacji w sieciach protokołu internetowego (IP). Obsługuje uwierzytelnianie równorzędne na poziomie sieci, uwierzytelnianie pochodzenia danych, integralność danych, poufność danych (szyfrowanie) i ochronę odtwarzania.

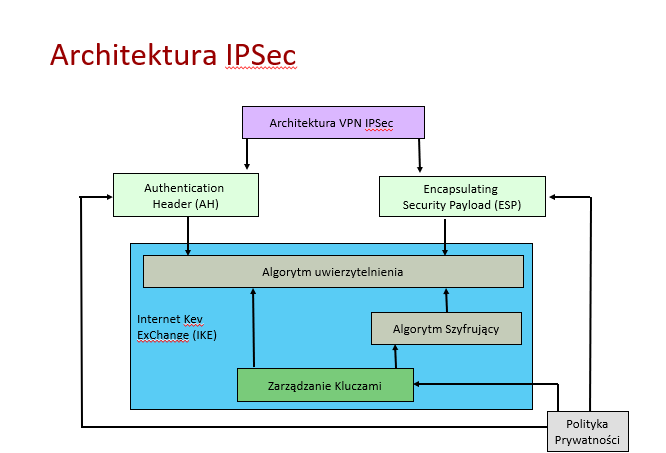
Początkowy pakiet IPv4 został opracowany z kilkoma przepisami bezpieczeństwa. W ramach rozszerzenia IPv4, IPSec to model OSI warstwy trzeciej , podczas gdy inne powszechnie stosowane systemy zabezpieczeń internetowych działają powyżej warstwy trzeciej, takie jak TLS (*Transport Layer Security)* i SSH (*Secure Shell)*, które działają na warstwie transportowej. IPSec może automatycznie zabezpieczyć aplikacje w warstwie IP. Począwszy od wczesnych lat siedemdziesiątych Agencja Zaawansowanych Projektów Badawczych sponsorowała serię eksperymentalnych urządzeń szyfrujących ARPANET , najpierw do natywnego szyfrowania pakietów ARPANET, a następnie do szyfrowania pakietów TCP / IP; niektóre z nich były certyfikowane i wystawiane. W latach 1986–1991 NSA sponsorowała opracowywanie protokołów bezpieczeństwa dla Internetu w ramach programu Secure Data Network Systems (SDNS). W ten sposób zebrali się różni dostawcy, w tym Motorola, którzy wyprodukowali urządzenie do szyfrowania sieci w 1988 r. Prace zostały opublikowane od około 1988 r. Przez NIST, a protokół bezpieczeństwa w warstwie 3 (SP3) ostatecznie przekształciłby się w standardową sieć ISO Layer Security Protocol (NLSP).

W latach 1992-1995 różne grupy badawcze ulepszyły wersję SPNS SDNS. W 1992 r. w NRL (*Naval Research Laboratory*) rozpoczęło projekt SIPP(*Single Inline Pin Package)* dotyczący badań i wdrożenia szyfrowania IP. W grudniu 1993 r. Eksperymentalny software IP Encryption Protocol został opracowany na SunOS w Columbia University i AT&T Bell Labs przez Johna Loannidisa i innych. Wei Xu z Trusted Information Systems (TIS) podążył za badaniami i ulepszył protokoły bezpieczeństwa IP. Opracował sterownik urządzenia Data Encryption Standard. Do grudnia 1994 r. Jego zespół wypuścił produkt TIS Gauntlet Firewall ze zintegrowanym sprzętowym szyfrowaniem 3DES i zapewnił komercyjne bezpieczeństwo IP przy prędkościach T1 , zabezpieczając sieci między wschodnim i zachodnim wybrzeżem Stanów Zjednoczonych. W tym okresie Grupa Robocza ds. Bezpieczeństwa IP w Internet Engineering Task Force (IETF) utworzyła, swobodnie dostępny zestaw rozszerzeń bezpieczeństwa, zwany IPSec . W 1995r.opublikowała RFC-1825 za pośrednictwem RFC-1827, a NRL miał pierwszą roboczą implementację.

Architektura IPSec VPN składa się z pakietów protokołu Authentication Header (*AH*), Encapsulation Security Payload (*ESP*) i protokołu Internet Key Exchange (*IKE*). IPSec zapewnia ochronę bezpieczeństwa pakietów IP przez AH i ESP, gwarantuje poufność transmisji danych IP przez ESP, a także zapewnia kontrolę integralności danych, uwierzytelnianie źródła danych oraz funkcje zapobiegające odtwarzaniu przez AH / ESP. ESP i AH definiują protokół i format nagłówka ładunku oraz świadczone usługi, ale nie określają metod transkodowania wymaganych do wdrożenia zdolności. Metody transkodowania obejmują metody konwersji danych, takie jak algorytm i długość klucza. IKE upraszcza korzystanie z IPSec i zarządzanie nim poprzez automatyczne negocjowanie wymiany kluczy oraz ustanawianie i utrzymywanie skojarzeń zabezpieczeń dla IPSec. Szczegóły są następujące:

* AH - protokół uwierzytelniania nagłówka pakietu, który zapewnia uwierzytelnianie źródła danych, sprawdzanie integralności danych i funkcje zapobiegające odtwarzaniu, ale nie obsługuje szyfrowania.
* ESP - protokół bezpieczeństwa enkapsulacji, który zapewnia szyfrowanie, uwierzytelnianie źródła danych, sprawdzanie integralności danych oraz funkcje zapobiegające odtwarzaniu.
* IKE: ustanowiony w oparciu o (ISAKMP Internet Security Association i Key Management Protocol), przy użyciu DH (Diffie-Hellman) w celu wdrożenia bezpiecznej dystrybucji kluczy i uwierzytelniania tożsamości w niezabezpieczonych sieciach, co zapewnia bezpieczeństwo transmisji danych. IKE poprawia bezpieczeństwo klucza i zmniejsza złożoność zarządzania IPSec.

Rys. 17. Model architektury IPSec

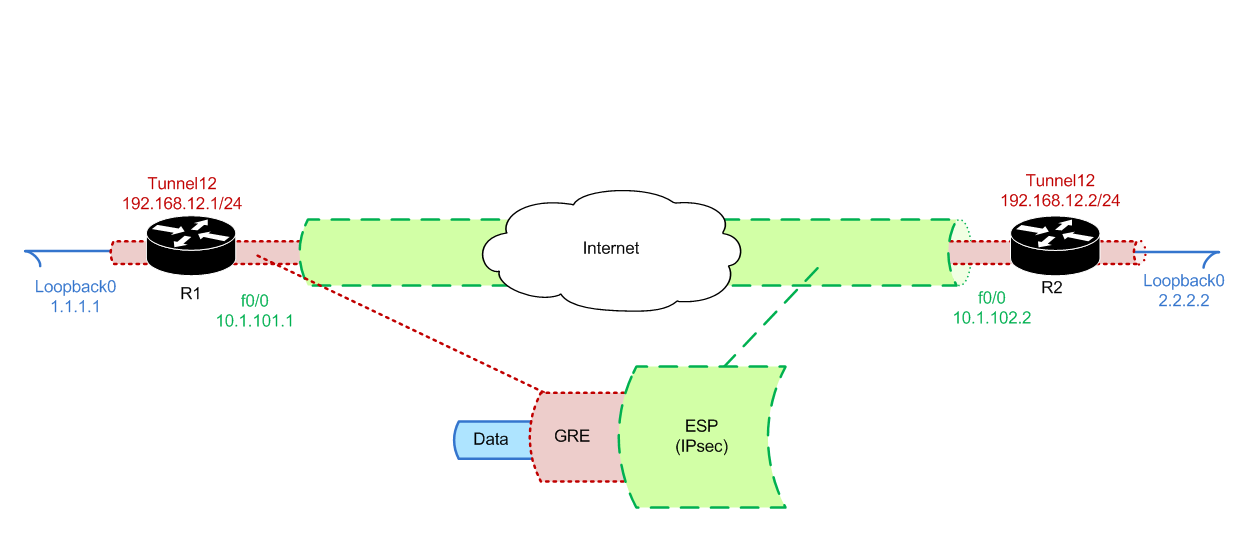


Źródło: https://www.vsx.pl/

Technologia GRE over IPSec wykorzystuje protokół IPSec do enkapsulacji pakietów, które zostały enkapsulowane przez GRE. Ponieważ GRE nie ma własnego mechanizmu szyfrowania ruchu, wykonanie zadania szyfrowania zależy od IPsec. Chodzi o to, aby GRE przez IPsec szyfrował to, co jest zawarte w GRE. GRE over IPSec implementuje szyfrowanie IPSec na fizycznych interfejsach. System wykrywa przepływy danych GRE, które muszą być szyfrowane na fizycznych interfejsach (lista ACL jest skonfigurowana tak, aby pasowała do przepływów danych GRE między dwiema bramami). W ten sposób wszystkie przepływy danych przesyłane przez tunel GRE są chronione przez IPSec. Tunel GRE jest również chroniony przez IPSec podczas konfiguracji.

GRE przez IPSec obsługuje enkapsulację zarówno w trybie tunelowym, jak i transportowym. W trybie tunelowym do pakietów wstawiany jest nagłówek pakietu IPSec, który szyfruje dane zawarte w tunelu.

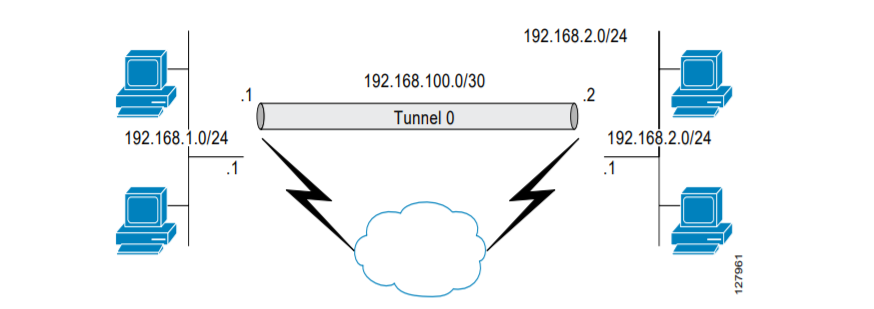
Rys. 18. Wizualizacja połączenia GRE z IPSec



Źródło: https://www.proprofs.com/discuss/q/1667635/what-is-the-difference-between-ipsec-and-gre

Interfejs wirtualnego tunelu IPSec znacznie upraszcza proces konfiguracji, gdy trzeba go zapewniać ochrona zdalnego dostępu i stanowi prostszą alternatywę dla tuneli GRE lub L2TP dla enkapsulacja i map kryptograficzne z IPSec. Główna zaleta związana z VTI IPSec o zmniejszenie narzutu, ponieważ konfiguracja nie wymaga statycznego mapowania sesji IPSec i jest podpięty do interfejsu fizycznego. VTI IPSec pozwala na elastyczność wysyłania i odbierania zarówno IP unicast jak zaszyfrowanej emisji multicast na dowolnym interfejsie fizycznym. Wykorzystywana w przypadku wielu ścieżek dla pakietu ( multicast routing). Istnieją dwa rodzaje interfejsów VTI: statyczne VTI (SVTI) i dynamiczne VTI (DVTI). Statyczne VTI (SVTI) - można włączyć protokoły routingu w interfejsie tunelu, aby informacje o routingu mogły być propagowane przez wirtualny tunel. Router może nawiązywać relacje sąsiedzkie za pośrednictwem interfejsu wirtualnego tunelu. Pakiety multicast mogą być szyfrowane, a współdziałanie ze standardowymi instalacjami IPSec dzięki wykorzystaniu IP ANY ANY proxy.

Rys. 19. Przykład połączenia statycznego VTI

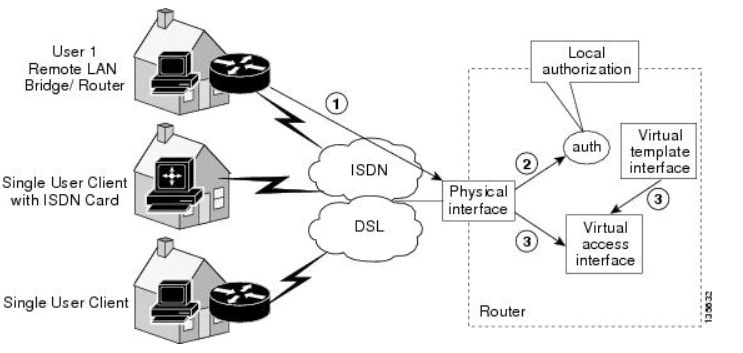


Źródło: https://support.zyxel.eu/hc/pl/articles/360000707399-Jak-mog%C4%99-skonfigurowa%C4%87-VPN-site-to-site-IPSec-za-pomoc%C4%85-VTI-na-USG-

Dynamiczne VTI (DVTI) mogą zapewniać wysoce bezpieczną i skalowalną łączność dla sieci VPN z dostępem zdalnym. Technologia DVTI zastępuje dynamiczne mapy kryptograficzne i dynamiczną metodę hub-and-speak do ustanawiania tuneli. Dynamicznych VTI można używać zarówno do konfiguracji serwera, jak i zdalnej. Tunele zapewniają oddzielny interfejs wirtualnego dostępu na żądanie dla każdej sesji VPN. Konfiguracja wirtualnych interfejsów dostępu jest klonowana z konfiguracji wirtualnego szablonu, która obejmuje konfigurację IPsec i dowolną funkcję oprogramowania Cisco IOS skonfigurowaną w interfejsie wirtualnego szablonu, taką jak QoS(Qualiti of Service) lub ACL.

DVTI działają jak każdy inny rzeczywisty interfejs, dzięki czemu można zastosować QoS, firewall i inne usługi bezpieczeństwa, gdy tylko tunel jest aktywny. Funkcje QoS mogą być wykorzystane do poprawy wydajności różnych aplikacji w sieci. Dowolna kombinacja funkcji QoS oferowanych w oprogramowaniu Cisco IOS może być wykorzystana do obsługi aplikacji głosowych, wideo lub przesyłu danych. Konfiguracja jest minimalna, która można później sklonować i użyć na innych urządzeniach.

Rys. 20. Przykład połączenia dynamicznego VTI



Źródło: https://support.zyxel.eu/hc/pl/articles/360000707399-Jak-mog%C4%99-skonfigurowa%C4%87-VPN-site-to-site-IPSec-za-pomoc%C4%85-VTI-na-USG-

W powyższej grafice, proces połączenia wygląda następująco:

1. Użytkownik wywołuje router.
2. Router uwierzytelnia użytkownika.
3. Ipsec klonuje interfejs wirtualnego dostępu virtual template interface.

# Charakterystyka i konfiguracja protokołu EIGRP

Enhanced Interior Gateway Routing Protocol (w skrócie EIGRP) to lepsza wersja protokołu IGRP która została stworzona przez firmę Cisco Systems. EIGRP zostawił taką samą długość wektora, informacje metryki oraz algorytm długości wektora jak oryginalny IGRP, ale szybkość synchronizacji i inne atrybuty regulacji zostały bardzo poprawione. EIGRP posiada opcje które nie znajdują się w jego starszej wersji, na przykład podsumowywanie trasy oraz obsługę VLMS. Ta technologia dysponuje również funkcjami które są właściwe dla protokół takich jak OSPF. EIGRP scala ze sobą zalety protokołów stanu łącza z zaletami protokołów wektora odległości[[7]](#footnote-7).

Analogicznie do IGRP, EIGRP komunikuje wzmiankę o tablicy routingu tylko ruterom sąsiednim ale w przeciwieństwie do IGRP, sąsiedzi odnajdywani są dzięki wymianie protokołu hello dokonywaną miedzy urządzeniami w tej samej sieci fizycznej. Po odnalezieniu sąsiednich routerów, EIGRP korzysta z wyjątkowego protokołu transportu na skutek tego zapewnia prawidłowe i uporządkowane informacje z tablicy routingu oraz uaktualnienie. Router widzi nie tylko scalone z nim trasy, ale także wszystkie trasy ogłaszane przez sąsiadów. Na podstawie tych komunikatów, EIGRP potrafi efektywnie oraz szybko wybrać drogę docelową o najmniejszym koszcie i zadeklarować że nie jest ona częścią pętli trasowania. Przy użyciu informacji od sąsiadujących routerów, algorytm może szybciej oszacować trasę zamienną w przypadku kiedy nastąpi awaria łącza albo innego wydarzenia transformującego topologię. Informacje routingu oraz komunikaty hello protokołu EIGRP są przekazywane w protokole transportowym EIGRP. Transport EIGRP kreuje rzetelne ogłoszenia oraz twierdzenia odbioru i nadawać żądania, pozwala to komunikatom hello i informacjom routingu prawidłowo wysyłać do wszystkich sąsiednich urządzeń.

W hybrydowym protokole IGRP zaprezentować można 5 rodzajów pakietów które w odniesieniu do swojego przeznaczenia mogą być wysłane na adres unicastowy lub multicastowy.

1. Powitanie (*ang. Hello*)
   1. Wykorzystywane odkrywania sąsiadów.
   2. Wysyłane bez potwierdzenia.
   3. Wysyłane na adres multicast.
2. Aktualizacja *(ang. Update)*
   1. Wysyłane za potwierdzeniem.
   2. Wysyłane na adres unicast lub multicast.
   3. Wykorzystywane do propagowania informacji.
3. Zapytanie *(ang. Query )*
   1. Wysyłane w odpytania o konkretną trasę.
   2. Wysyłane na adres unicast lub multicast.
4. Odpowiedź *(ang. Reply)*
   1. Odbiorca oczekuje na potwierdzenie otrzymania.
   2. Wysyła w odpowiedzi na pakiety Query.
   3. Wysyłane na adres unicast.
5. Potwierdzenie *(ang. Acknowledgement)*
   1. Wysyłane w celu potwierdzenia otrzymania danych
   2. Wysyłane na adres unicast

Protokół EIGRP wykorzystuje algorytm *Diffusing Update Algorith* (DUAL) w celu zapewnienia ścieżek (podstawowej oraz zapasowej) do danej podsieci w uwzględnieniem braku pętli routingu. Proces decyzyjny dla obliczania każdej ścieżki jest wykonywany przez DUAL *Finite State Machine* (FSM). Śledzi on wszystkie trasy i w oparciu o metryki EIGRP wybiera najefektywniejsze ( o najniższej metryce) ścieżki do umieszczenia w tablicy routingu.

Przeliczanie metryk jest operacją mocno obciążającą procesor i z tego powodu EIGRP stara się dokonywać takich przeliczeń jak najrzadziej jest to możliwe poprzez przechowywanie zapasowych tras w tablicy topologii. W przypadku awarii podstawowej trasy, kolejna może zostać natychmiast przeniesiona z tablicy topologii do tablicy routingu.

Proces DUAL zapewnia:

* Szybką zbieżność
* Minimalne użycie łącza poprzez aktualizacje protokołu
* Ścieżki wolne od pętli routingu
* Zapasowe ścieżki które mogą być natychmiastowo użyte

Protokół EIGRP składa się z wielu innych, pomniejszych składowych. Każda nowa technologia przynosi poprawę efektywności działania, tempa osiągania zbieżności lub funkcjonalności protokołu EIGRP w porównaniu z IGRP i innymi protokołami routingu. Rozwiązania te można zakwalifikować do jednej z czterech kategorii:

* Wykrywanie nowych sąsiadów i odtwarzanie relacji z byłymi sąsiadami,
* Protokół RTP (*Reliable Transport Protocol*),
* Algorytm automatu skończonego DUAL,
* Moduły zależne od protokołów.

Proste routery wykorzystujące mechanizm wektora odległości nie nawiązują żadnych relacji z sąsiednimi urządzeniami. Routery wyposażone w protokoły RIP i IGRP jedynie rozgłaszają lub rozsyłają grupowo aktualizacje przez skonfigurowane w tym celu interfejsy. W odróżnieniu od nich routery z protokołem EIGRP aktywnie ustanawiają relacje z sąsiadującymi urządzeniami, bardzo podobnie do sposobu, w jaki czynią to routery OSPF.

Routery EIGRP tworzą relacje przylegania. W tym celu wykorzystują niewielkie pakiety hello. Pakiety te są wysyłane domyślnie co 5 sekund. Router EIGRP zakłada, że tak długo, jak otrzymuje pakiety hello od znanych sąsiadów, sąsiedzi ci oraz obsługiwane przez nie trasy funkcjonują prawidłowo, czyli pozostają pasywne. Gdy routery EIGRP tworzą relacje przylegania, możliwe są następujące scenariusze:

* Dynamicznie dowiadują się o nowych trasach, które pojawiły się w sieci,
* Wykrywają routery, które stały się niedostępne lub przestały działać,
* Ponownie wykrywają routery, które wcześniej były niedostępne.

Protokół RTP (*Reliable Transport Protocol*) to protokół warstwy transportowej, który gwarantuje dostarczanie pakietów EIGRP w odpowiedniej kolejności do wszystkich sąsiednich urządzeń. W sieci opartej na protokole IP do wyznaczenia kolejności pakietów i zapewnienia ich terminowego dostarczenia hosty wykorzystują protokół TCP. Protokół EIGRP ma tę zaletę, że jest niezależny od protokołu bazowego. Oznacza to, że w celu wymiany informacji o routingu nie używa TCP/IP, jak to jest w przypadku protokółów RIP, IGRP i OSPF.

Żeby możliwe było pozostanie niezależnym od protokołu IP, do przesyłania informacji o routingu protokół EIGRP używa protokołu RTP jako własnego protokołu warstwy transportowej. Protokół RTP może obsługiwać protokół EIGRP w sposób gwarantowany lub bez gwarancji, zależnie od wymagań danej sytuacji. Na przykład dla pakietów hello można zrezygnować z dodatkowych obciążeń wynikających z dostawy gwarantowanej, ponieważ są one często wysyłane i powinny być jak najmniejsze. Dostarczanie pozostałych informacji o routingu w trybie gwarantowanym może w praktyce przyspieszyć osiąganie zbieżności, ponieważ routery EIGRP nie muszą czekać z rozpoczęciem ich przekazywania na upłynięcie limitu czasu ustawionego w zegarze. Dzięki protokołowi RTP protokół EIGRP może wysyłać dane do innych urządzeń jednocześnie w formie transmisji pojedynczej i grupowej. Zapewnia to maksymalną efektywność rozsyłania.

Kluczowym elementem protokołu EIGRP jest algorytm DUAL – mechanizm obliczania tras używany przez ten protokół. Pełna nazwa tej technologii to automat skończony DUAL FSM (*Finite-state Machine*). FSM to automat algorytmiczny, a nie urządzenie z ruchomymi częściami. Moduły FSM określają zbiór możliwych stanów, przez które może przechodzić dany obiekt, zdarzenia powodujące te stany oraz zdarzenia będące efektem zaistnienia tych stanów. Projektanci wykorzystują koncepcję automatu o skończonej liczbie stanów do opisywania reakcji urządzenia, programu komputerowego lub algorytmu routingu na zbiór zdarzeń. Automat FSM protokołu DUAL jest wyposażony we wszystkie funkcje logiczne potrzebne do obliczania i porównywania tras w sieci EIGRP.

Algorytm DUAL śledzi wszystkie trasy ogłaszane przez sąsiednie routery. W celu ich porównania używa złożonych metryk każdej z tras. Algorytm gwarantuje również brak zapętleń we wszystkich ścieżkach. W tablicy routingu umieszcza ścieżki o najniższych kosztach. Te trasy główne są nazywane podstawowymi opłacalnymi trasami.

Protokół EIGRP zapewnia łatwy dostęp do ważnych informacji o trasach i topologii dzięki umieszczeniu ich w tablicy sąsiadów i tablicy topologii. Tablice te dostarczają algorytmowi DUAL kompleksowych informacji o trasach na wypadek zakłóceń funkcjonowania sieci. Na podstawie tych informacji algorytm może szybko wybrać trasy alternatywne. Jeśli dane łącze ulegnie awarii, algorytm DUAL poszukuje w tablicy topologii alternatywnej ścieżki, tzw. następnej opłacalnej trasy.

Jedną z korzystnych cech protokołu EIGRP jest jego modułowa konstrukcja. Praktyka pokazuje, że konstrukcje modułowe (warstwowe) są najbardziej skalowalne i elastyczne. Obsługę protokołów routowanych, takich jak IP, IPX i AppleTalk, zapewniają w protokole EIGRP moduły PDM. Teoretycznie można dodawać kolejne moduły PDM, które umożliwią obsługę nowych lub zmodernizowanych protokołów routowanych, takich jak IPv6.

Każdy moduł PDM odpowiada za obsługę wszystkich funkcji związanych z konkretnym protokołem routowanym. Moduł IP-EIGRP odpowiada za realizację następujących funkcji:

* Wysyłanie i odbieranie pakietów EIGRP zawierających dane IP,
* Powiadamianie algorytmu DUAL o otrzymywanych nowych informacjach o routingu IP,
* Przechowywanie decyzji o routingu podejmowanych przez algorytm DUAL w tablicy routingu protokołu IP,
* Rozprowadzanie informacji o routingu uzyskanych przez inne protokoły routingu obsługujące protokół IP.

Struktura danych protokołu EIGRP wygląda podobnie jak w przypadku protokołu OSPF. Do utrzymywania tabel i nawiązywania relacji z sąsiednimi routerami protokół EIGRP wykorzystuje różne rodzaje pakietów.

Wyróżnia się pięć typów pakietów protokołu EIGRP:

* Powitanie *(ang. Hello)*,
* Potwierdzenie (*ang.Acknowledgment*),
* Aktualizacja (*ang.Update*),
* Zapytanie (*ang.Query*),
* Odpowiedź (*ang.Reply*).

Pakiety hello są wykorzystywane do wykrywania, weryfikowania i ponownego wykrywania sąsiednich routerów. Ponowne wykrywanie ma miejsce w sytuacji, gdy routery EIGRP nie otrzymują od siebie pakietów hello przez czas przetrzymania, ale potem ponownie nawiązują komunikację.

Routery EIGRP wysyłają pakiety hello w stałych, ale konfigurowalnych odstępach czasu. Domyślny czas między pakietami hello zależy od szerokości pasma interfejsu. W sieciach IP routery EIGRP wysyłają pakiety hello pod adres grupowy 224.0.0.10.

Routery EIGRP przechowują informacje o sąsiednich urządzeniach w tablicy sąsiadów. Tablica sąsiadów zawiera pole Seq No (*Sequence Number*, numer sekwencyjny), w którym jest zapisywany numer ostatniego otrzymanego pakietu EIGRP wysłanego przez dane urządzenie. Istnieje również pole Hold Time (Czas przetrzymania), w którym jest rejestrowany czas otrzymania ostatniego pakietu. Aby trasa pozostała w stanie pasywnym, pakiety muszą być otrzymywane przed upłynięciem czasu przetrzymania. Stan pasywny oznacza, że trasa jest dostępna i funkcjonuje prawidłowo.

Jeśli protokół EIGRP nie otrzyma pakietu od sąsiedniego urządzenia w wyznaczonym czasie przetrzymania, uzna, że urządzenie to nie działa. W tym momencie algorytm DUAL zaczyna weryfikację tablicy routingu. Domyślnie czas przetrzymania to trzykrotność czasu między pakietami hello, ale administrator może ustawiać obie wartości w dowolny sposób.

Aby była możliwa komunikacja między dwoma sąsiednimi routerami obsługiwanymi przez protokół OSPF, muszą mieć one takie same przedziały pakietów hello i czasy nieaktywności. Protokół EIGRP nie narzuca takiego ograniczenia. Sąsiednie routery dowiadują się o swoich wzajemnych ustawieniach zegarów przez wymianę pakietów hello. Następnie wykorzystują te informacje do ustanowienia trwałej relacji, niezależnie od różnic między wartościami zegarów. Pakiety hello zawsze są wysyłane bez gwarancji. Oznacza to, że nie towarzyszą im żadne pakiety potwierdzeń.

Routery EIGRP używają pakietów potwierdzeń podczas wymiany gwarantowanej do poinformowania, że otrzymały pakiety EIGRP. Protokół RTP umożliwia gwarantowaną komunikację między hostami EIGRP. W tym celu są wykorzystywane pakiety potwierdzeń. Są to pakiety hello pozbawione danych. W odróżnieniu od pakietów hello rozsyłanych grupowo, pakiety potwierdzeń są rozsyłane pojedynczo. Potwierdzenia mogą być dołączane do innych rodzajów pakietów EIGRP, np. pakietów odpowiedzi.

Pakiety aktualizacyjne są używane w sytuacji, gdy router wykryje nowe urządzenie sąsiednie. Routery EIGRP wysyłają wtedy do takiego routera pakiety aktualizacyjne w trybie transmisji pojedynczej (*unicast*), które umożliwią mu uzupełnienie tablicy topologii. Przekazanie wszystkich informacji może wymagać przesłania kilku pakietów. Pakiety aktualizacyjne są również wykorzystywane w przypadku wykrycia przez router zmian w topologii. Wtedy router EIGRP wysyła do wszystkich sąsiadów pakiet w trybie multiemisji (*multicast*), który informuje je o zaistniałej zmianie. Wszystkie pakiety aktualizacyjne są wysyłane z gwarancją.

Jeśli router utraci swoją podstawową opłacalną trasę i nie będzie mógł znaleźć następnej opłacalnej trasy, algorytm DUAL nada trasie stan aktywny. Następnie router podejmie próbę ustalenia innej podstawowej opłacalnej trasy do miejsca docelowego, rozsyłając grupowo do wszystkich sąsiednich routerów odpowiednie zapytanie. Sąsiednie urządzenia muszą przysłać odpowiedzi, które będą zawierały informacje o dostępnych trasach albo stwierdzenie braku żądanych informacji.

Proste routery wykorzystujące mechanizm wektora odległości nie nawiązują żadnych relacji z sąsiednimi urządzeniami. Routery wyposażone w protokoły RIP i IGRP jedynie rozgłaszają lub rozsyłają grupowo aktualizacje przez skonfigurowane w tym celu interfejsy. W odróżnieniu od nich routery z protokołem EIGRP aktywnie ustanawiają relacje z sąsiadującymi urządzeniami, analogicznie do routerów używających protokołu OSPF.

Najważniejszą tablicą w routingu EIGRP jest tablica sąsiadów. Każdy router EIGRP utrzymuje tablicę sąsiadów, w której są wymienione sąsiadujące z nim routery. Dla każdego protokołu obsługiwanego przez protokół EIGRP istnieje osobna tablica sąsiadów.

Routery EIGRP ustanawiają relacje przylegania z sąsiednimi routerami za pomocą niewielkich pakietów hello. Pakiety te są wysyłane domyślnie co 5 sekund. Tworzenie relacji przylegania daje routerom EIGRP następujące możliwości:

* Dynamiczne uzyskiwanie informacji o nowych trasach pojawiających się w sieci;
* Wykrywanie routerów, które stały się niedostępne lub przestały działać;
* Ponowne wykrywanie routerów, które wcześniej były niedostępne.
* Tablica sąsiadów zawiera następujące pola:
* Adres sąsiedniego urządzenia (*neighbor address*) – adres warstwy sieci sąsiedniego routera.
* Czas przetrzymania (*hold time*) – czas oczekiwania bez otrzymania jakiegokolwiek sygnału od sąsiedniego urządzenia, zanim łącze zostanie uznane za niedostępne. Pierwotnie oczekiwanym pakietem był pakiet hello, jednak w obecnych wydaniach systemu Cisco IOS zegar jest resetowany po otrzymaniu jakiegokolwiek pakietu protokołu EIGRP po pierwszym pakiecie hello.
* Zegar SRTT (*Smooth Round-Trip Timer*) – średni czas od wysłania pakietu do sąsiedniego urządzenia do otrzymania pakietu odpowiedzi. Zegar jest wykorzystywany do ustalania interwału retransmisji RTO.
* Wielkość kolejki Q Cnt (*Queue count*) – liczba pakietów oczekujących w kolejce na wysłanie. Jeśli wartość ta jest regularnie większa od zera, na routerze może występować przeciążenie. Liczba 0 oznacza brak pakietów protokołu EIGRP w kolejce.
* Numer sekwencyjny Seq No (*Sequence Number*) – numer ostatniego pakietu otrzymanego od danego sąsiedniego urządzenia. W tym polu protokół EIGRP potwierdza transmisję z sąsiedniego urządzenia oraz identyfikuje pakiety, które dotarły bez zachowania właściwej kolejności. Tablica sąsiadów służy do zapewnienia gwarantowanej, sekwencyjnej wysyłki pakietów. Można ją porównywać do protokołu TCP używanego do gwarantowanego dostarczania pakietów IP.

Routery EIGRP przechowują informacje o trasach i topologii w pamięci RAM, dzięki czemu mogą szybko reagować na zmiany. Podobnie jak routery OSPF, routery EIGRP zapisują te informacje w kilku tablicach i bazach danych.

Algorytm protokołu EIGRP wykorzystujący wektor odległości DUAL na podstawie informacji zawartych w tablicy sąsiadów i tablicy topologii oblicza najtańszą trasę do miejsca docelowego. Trasa główna jest nazywana podstawową opłacalną trasą. Obliczoną trasę główną algorytm DUAL umieszcza w tablicy routingu, a jej kopię – w tablicy topologii.

DUAL próbuje również obliczyć trasę zapasową na wypadek, gdyby trasa główna zawiodła. Trasa zapasowa jest nazywana zapasową trasą główną. Obliczoną następną opłacalną trasę algorytm umieszcza w tablicy topologii. Gdy trasa główna do miejsca docelowego stanie się niedostępna lub niewiarygodna, można skorzystać z zapasowej trasy głównej.

Jeśli w tablicy nie zostanie odnaleziona następna opłacalna trasa, dana trasa jest oznaczana jako aktywna, czyli bezużyteczna w danym momencie. Do sąsiednich routerów są wysyłane pakiety zapytań z żądaniem informacji o topologii. Na podstawie otrzymanych informacji algorytm DUAL ponownie oblicza podstawową i zapasową trasę główną do miejsca docelowego. Po przeprowadzeniu obliczeń trasa główna jest zapisywana w tablicy routingu. Następnie obie trasy główne – podstawowa i zapasowa – są zapisywane w tablicy topologii. Stan docelowej trasy do miejsca docelowego ulegnie teraz zmianie z aktywnego na pasywny. Oznacza to, że trasa działa i jest wiarygodna. Każda tablica zawiera następujące informacje:

* Protokół routingu EIGRP,
* Najniższy koszt trasy, zwany opłacalną odległością FD,
* Koszt trasy ogłaszany przez sąsiedni router, zwany zgłaszaną odległością RD.

Należy zwrócić uwagę, że istnienie następnej opłacalnej trasy jest opcjonalne.

Algorytm DUAL śledzi wszystkie trasy ogłaszane przez sąsiednie routery. W celu ich porównania używa złożonych metryk każdej z tras. Algorytm gwarantuje również brak zapętleń we wszystkich ścieżkach.

Następnie algorytm wstawia ścieżki o najniższym koszcie do tablicy routingu. Te trasy główne są nazywane podstawowymi opłacalnymi trasami. Kopia informacji o trasach głównych jest również umieszczana w tablicy topologii. Tablice te dostarczają algorytmowi DUAL kompleksowych informacji o trasach na wypadek zakłóceń funkcjonowania sieci. Na podstawie tych informacji algorytm może szybko wybrać trasy alternatywne.

Jeśli dane łącze ulegnie awarii, algorytm DUAL poszukuje w tablicy topologii alternatywnej ścieżki, tzw. następnej opłacalnej trasy. Jeśli odpowiedni wpis nie zostanie znaleziony w tablicy, dana trasa jest oznaczana jako aktywna. Do sąsiednich routerów są wysyłane pakiety zapytań z żądaniem informacji o topologii. Na podstawie otrzymanych informacji algorytm DUAL ponownie oblicza podstawową i zapasową trasę główną do miejsca docelowego.

Po zakończeniu obliczeń stan docelowej trasy do miejsca docelowego ulegnie zmianie z aktywnego na pasywny. Oznacza to, że trasa działa i jest wiarygodna.

Wykrycie nowego urządzenia w sąsiedztwie powoduje zapisanie informacji o jego adresie i interfejsie. Dane te są zapisywane w strukturze danych urządzeń sąsiadujących. Gdy sąsiednie urządzenie wysyła pakiet hello, ogłasza swój czas przetrzymania. Innymi słowy, jeśli w tym okresie nie zostanie otrzymany pakiet hello, czas przetrzymania wygasa. Po wygaśnięciu czasu przetrzymania algorytm DUAL jest informowany o zmianach w topologii i musi ponownie obliczyć nową topologię.

Aby włączyć protokół EIGRP należy wpisać następującą komendę: *Router(config)# router eigrp 10*. Liczba 10 oznacza w tym wpisie numer autonomicznego systemu (AS), jest to konieczne ponieważ na jednym routerze można uruchomić kilka procesów EIGRP. Numer ten musi być taki sam na każdym routerze należącym do tego samego autonomicznego systemu co nasz, a więc na każdym routerze, z którym chcemy utrzymywać wymianę informacji na temat tras.

Następnie pokazano jak dodaje się sieć do protokołu EIGRP : *Router(config)# router eigrp 10, Router(config-router)# network 172.20.0.0*

Ponieważ w powyższej komendzie nie została podana maska podsieci, router uwzględni w procesie EIGRP (a więc także w pakietach aktualizacyjnych wysyłanych do innych routerów) wszystkie znane mu podsieci mieszczące się w sieci klasy B 172.16.0.0/16. Aby zadeklarować wyłącznie wybranej sieci, potrzebna jest odwrócona maska podsieci (wildcard mask) określająca dokładnie, która sieć ma być użyta: *Router(config-router)# network 172.20.0.8 0.0.0.3*

Komenda wpisana powyżej dodała sieć 172.20.0.8 255.255.255.252 do protokołu EIGRP. Żeby obliczyć odwróconą maskę podsieci (*wildcard mask*), trzeba od adresu 255.255.255.255 odjąć maskę podsieci. Wykonując równanie na adresach IP 255.255.255.255 -255.255.255.252= 0.0.0.3

Aby urządzenie mogło wysyłać i odbierać komunikaty które aktualizują wiadomości o trasach do innych sieci, najpierw musi ustanowić zależność z przyległości z routerem po drugiej stronie.

Aby router mógł wysyłać i odbierać pakiety aktualizujące informacje o trasach do innych sieci, najpierw musi ustanowić zależność przyległości z routerem po drugiej stronie. Do tego celu używane są pakiety hallo. Do weryfikacji, czy taka zależność została utworzona, służy następująca komenda: *Router# show ip eigrp neighbors*

Informacja uzyskana po wydaniu tej komendy będzie zawierała m.in. adres IP przyległych routerów, lokalny interfejs, na którym dany router został wykryty, czas trwania zależności przyległości i licznik timera hold. W przypadku protokołu EIGRP należy zwrócić uwagę, aby nie wydawać komendy passive-interface na interfejsach łączących z innymi routerami, gdyż uniemożliwi to routerom wymianę informacji na temat tras. Natomiast tak samo jak w innych protokołach, ogólne informacje o procesie EIGRP na lokalnym routerze można uzyskać wydając komendę show ip protocols. Kiedy zbudujemy sieć składającą się z więcej niż jednego routera, możemy zweryfikować tablicę trasowania na naszym routerze następującą komendą: *Router# show ip route.*

Zastosowany do wirtualnej konfiguracji VPN zostanie zastosowany symulator GNS3. Skrót w jego nazwie podchodzi od Graphical Network Simulator. Jest to darmowy program a dokładniej emulator sieci dzięki któremu możemy całościowo tworzyć i testować sieci złożone z wirtualnego sprzętu, w naszym przypadku będzie to CiscoDo zaprezentowania naszego projektu wykorzystamy emulator GNS3 ( Graphical Network Simulation -3 ). GNS3 istnieje od ponad 10 lat. Pozwala na kombinacje wirtualnych urządzeń sieciowych, dzięki czemu można odtworzyć działanie prawdziwej sieci. Ze względu na typ oprogramowania (open source) służy do emulacji nie tylko urządzeń firmy Cisco ( np.: Mikrotik, AT&T). W naszym projekcie wykorzystamy go do pokazania działania połączenia c2s w oparciu o urządzenia Cisco.

Oto jedne z ciekawszych opcji GNS3 i narzędzi z nim współpracujących:

* Wysokiej jakości implementacja wielu rozwiązań sieciowych, dzięki czemu można testować złożone topologie sieciowe
* Dynamips pozwala emulację prawdziwych systemów Cisco IOS
* Qemu umożliwia testowanie wykorzystując obrazy prawdziwych systemów wirtualnych
* Emulacja Routerów Cisco, IPS, firewalli PIX/ASA, JUNOSów
* Dokładna emulacja ruchu Ethernet, ATM, Framerelay na przełącznikach
* Możliwość integracji (i dalszej emulacji) prawdziwych sieci i Internetu

Do czego można wykorzystać GNS3? Aby poszerzyć swoją wiedzę na temat sieci komputerowych lub żeby stworzyć swoją prawdziwą sieć komputerową od zera (wraz z wyborem Hardware’u i jego konfiguracją) – oraz przetestować jej działanie. Ponadto pozawala Symulować bezpieczeństwo sieci i przeprowadzać ataki sieciowe oraz testować planowane do wdrożenia urządzenia sieciowe oraz ich wpływ na działanie sieci.

# Kolejny rozdział.

Tekst

# Kolejny rozdział.

Tekst

# Zakończenie

Tekst

# Bibliografia

1. Leinwand A., Pinsky B., *Konfiguracja Routerów Cisco Podstawy*, wydanie drugie, MIKOM, Polska, 2002

# 

# Netografia

1. Historia sieci VPN, zasoby internetu: https://www.le-vpn.com/history-of-vpn/, dostęp 22.01.2020
2. The world’s most valuable resource is no longer oil, but data 2017, zasoby internetu: https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data, dostęp 20.01.2020
3. Starlink: SpaceX’s satellite internet projekt, zasoby internetu: https://www.space.com/spacex-starlink-satellites.html, dostęp 20.01.2020
4. Model OSI/ISO, zasoby internetu: http://edu.pjwstk.edu.pl/wyklady/sko/scb/w2.html, dostęp 25.01.2020
5. Network Devices, zasoby internetu: https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/, dostęp 25.01.2020

# Spis tabel

Tekst

# Spis rysunków

[Rys. 1. Topologia połączenia bezpośredniego 4](#_Toc32403248)

[Rys. 2. Topologia magistrali 4](#_Toc32403249)

[Rys. 3. Topologia pierścienia 5](#_Toc32403250)

[Rys. 4. Topologia gwiazdy 5](#_Toc32403251)

[Rys. 5. Topologia siatki 6](#_Toc32403252)

[Rys. 6. Topologia drzewa 6](#_Toc32403253)

[Rys. 7. Topologia hybrydowa 7](#_Toc32403254)

[Rys. 8. Model OSI i stosowane w warstwach protokoły 8](#_Toc32403255)

[Rys. 9. Przykład schemat topologii sieciowej ze wskazaniem urządzeń sieciowych 11](#_Toc32403256)

[Rys. 10. Połączenie Site-to-Site 14](#_Toc32403257)

[Rys. 11. Połączenie Client-Site 14](#_Toc32403258)

[Rys. 12. Schemat połaczenia VPN 15](#_Toc32403259)

[Rys. 13. Wizualizacja braku dostępu do treści po połączeniu VPN 16](#_Toc32403260)

[Rys. 14. Wizualizacja działania tunelu GRE 17](#_Toc32403261)

[Rys. 15. Struktura pakietu z GRE 18](#_Toc32403262)

[Rys. 16. Przekierowanie pakietu GRE 19](#_Toc32403263)

[Rys. 17. Model architektury IPSec 22](#_Toc32403264)

[Rys. 18. Wizualizacja połączenia GRE z IPSec 23](#_Toc32403265)

[Rys. 19. Przykład połączenia statycznego VTI 24](#_Toc32403266)

[Rys. 20. Przykład połączenia dynamicznego VTI 25](#_Toc32403267)

1. Historia VPN, https://www.le-vpn.com/history-of-vpn/, dostęp 20.01.2020 [↑](#footnote-ref-1)
2. https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-isno-longer-oil-but-data, dostęp 20.01.2020 [↑](#footnote-ref-2)
3. https://www.space.com/spacex-starlink-satellites.html, dostęp 20.01.2020 [↑](#footnote-ref-3)
4. Model ISO/OSI, http://edu.pjwstk.edu.pl/wyklady/sko/scb/w2.html, dostęp 25.01.2020 [↑](#footnote-ref-4)
5. Network Devices, https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/, dostęp 25.01.2020 [↑](#footnote-ref-5)
6. https://pl.wikipedia.org/wiki/Wirtualna\_sie%C4%87\_prywatna, dostęp 01.02.2020 [↑](#footnote-ref-6)
7. Leinwand A., Pinsky B., Konfiguracja Routerów Cisco Podstawy, s.150 [↑](#footnote-ref-7)