VLAN, VPN

E13

VLAN

- **VLAN (*ang. Virtual Local Area Network*)** - sieć komputerowa wydzielona logicznie w ramach innej, większej sieci fizycznej

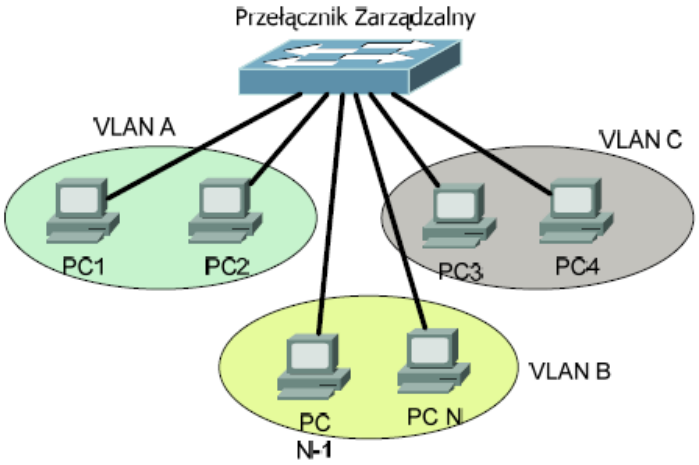
- Zastosowania VLAN
  - Dzielenie sieci na grupy użytkowe: Inżynierowie, Zarządzanie
  - Tworzenie typów użytkowników np. e-mail, WWW, itd.

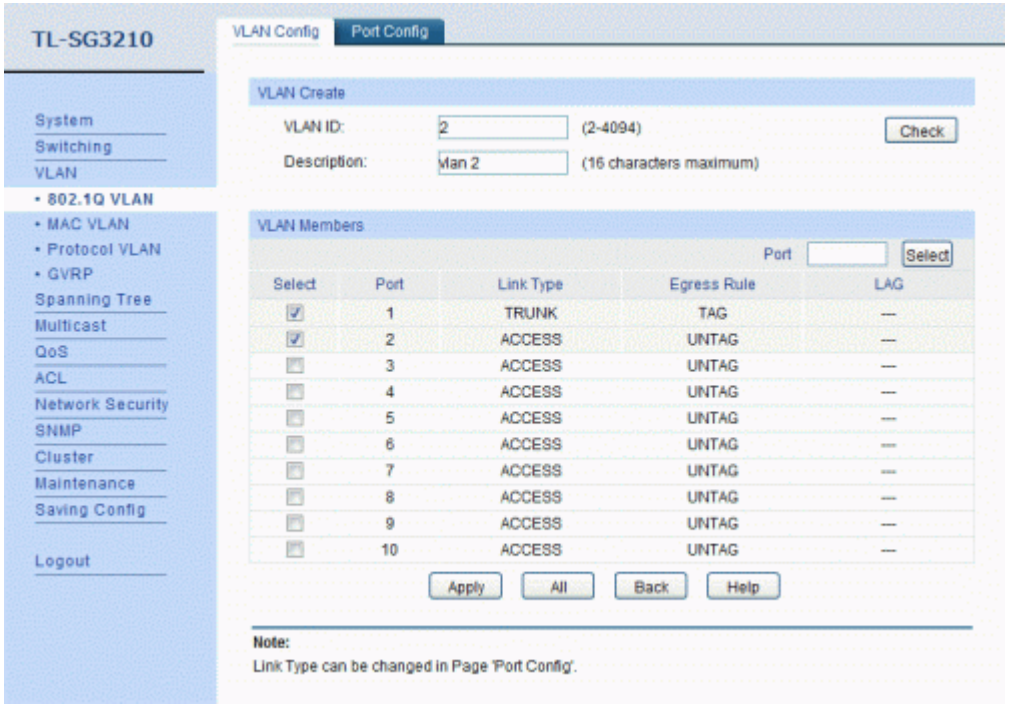
- Do tworzenia VLAN-ów wykorzystuje się **konfigurowalne lub zarządzalne przełączniki**, umożliwiające podział jednego fizycznego urządzenia na większą liczbę urządzeń logicznych, poprzez separację ruchu pomiędzy określonymi grupami portów.

- W przełącznikach zarządzanych zgodnych z IEEE 802.1Q możliwe jest znakowanie ramek (tagowanie) poprzez doklejenie do nich informacji o VLAN-ie, do którego należą. Dzięki temu możliwe jest transmitowanie ramek należących do wielu różnych VLAN-ów poprzez jedno fizyczne połączenie (trunking).

- **Zalety:**
  - Podniesienie bezpieczeństwa – komunikować się mogą tylko uprawnione podsieci. Np. operator jest logicznie odseparowany od pionu zarządzania
  - Uporządkowanie ruchu sieciowego

VLAN





http://www.rogaski.org/cisco/sem3/wirtualne_sieci_lan.html

Tunelowanie

- **tunelowanie** – tworzenie połączenia pomiędzy dwoma odległymi hostami dające wrażenie połączenia bezpośredniego.
- tunel wykorzystuje technikę **enkapsulacji** jednego protokołu w innym, umożliwia zastosowanie mechanizmów szyfrowania lub translacji transmitowanych danych.
- **umożliwia translację protokołów** i technologii - łączenie ze sobą sieci IPX, TCP/IP za pośrednictwem publicznych sieci rozległych (np. FrameRelay, ATM, X.25, IP, ...)
- umożliwia wykorzystanie metod kryptograficznych celem utworzenia bezpiecznego kanału
- tunelowania pozwala omijać blokowannie portów i usług (np. poprzez dozwolony port firewalla) http-tunnel

Techniki datagramowe:

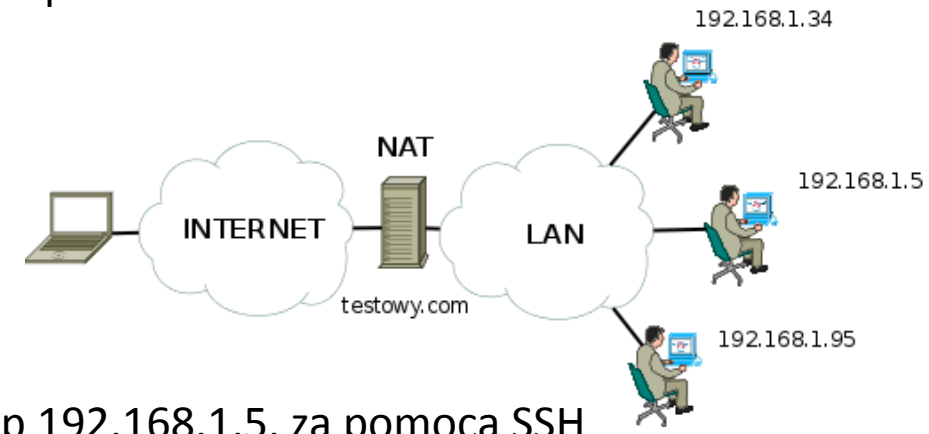
- L2TP (Layer2 TunnelingProtocol),
- GRE (GenericRoutingEncapsulation),
- GTP (GPRS TunnellingProtocol),
- PPTP (Point-to-PointTunnelingProtocol),
- PPPoE(Point-to-PointProtocoloverEthernet),
- PPPoA(Point-to-PointProtocoloverATM),
- IP-IPTunneling,
- IPsec,
- IEEE 802.1Q (Ethernet VLANs),

Techniki strumieniowe:

- TLS (Transport LayerSecurity),
- SSL (SecureSocketLayer)

Tunele oparte na SSH

- Tunelowanie, czyli inaczej przekierowywanie portów polega na przesyłaniu niezabezpieczonych pakietów protokołów TCP (POP3, SMTP czy HTTP) przez bezpieczny protokół SSH.
- Istnieją dwa rodzaje przekierowania portów: lokalne (wychodzące) oraz zdalne (przychodzące).
- OpenSSH - zestaw programów komputerowych zapewniających szyfrowaną komunikację w sieci komputerowej dzięki protokołowi SSH.



Połączenie z laptopa do klienta o adresie ip 192.168.1.5. za pomocą SSH

$ ssh -L port_lokalny:192.168.1.5:port_hosta user@testowy.com

Założenie: posiadamy konto na routerze realizującym NAT. W naszym przykładzie testowy.com.

VPN

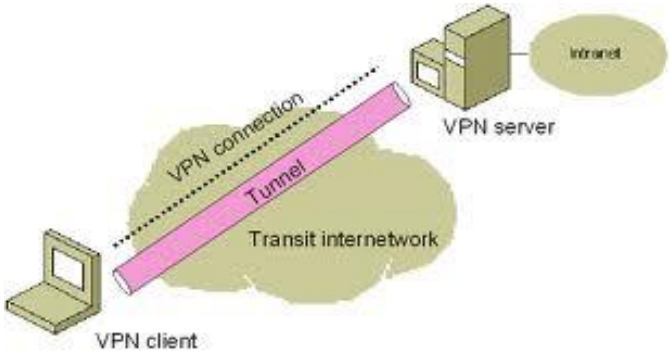
- **VPN (*ang. Virtual Private Network)*** - wirtualna sieć prywatna (tunel), przez który płynie ruch w ramach sieci prywatnej pomiędzy klientami końcowymi za pośrednictwem publicznej sieci (takiej jak Internet)

- Rozwiązania oparte na VPN stosowane są np. w sieciach korporacyjnych firm, których zdalni użytkownicy pracują ze swoich domów na niezabezpieczonych łączach. Wirtualne Sieci Prywatne charakteryzują się dość dużą efektywnością, nawet na słabych łączach (dzięki kompresji danych) oraz wysokim poziomem bezpieczeństwa (ze względu na szyfrowanie). Rozwiązanie to sprawdza się w firmach, których pracownicy często podróżują lub korzystają z możliwości telepracy

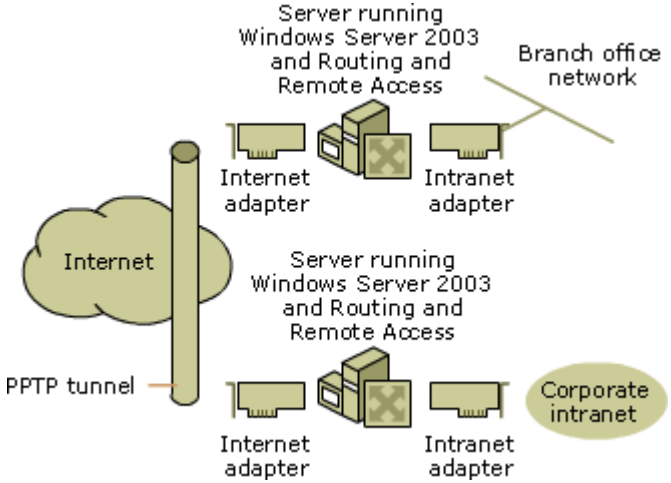
- Zastosowania:
  - sieci dostępowe - łączą zdalnych użytkowników: czyli pracowników mobilnych, konsultantów, sprzedawców, lokalne filie, z siedzibą firmy;
  - intranet - łączy odległe oddziały tej samej firmy;
  - ekstranet -zapewnia ograniczony dostęp do sieci firmowej zaufanym partnerom biznesowym.

VPN

- Wirtualna sieć prywatna VPN korzysta z publicznej infrastruktury telekomunikacyjnej, która dzięki stosowaniu protokołów tunelowania, szyfrowania i procedur bezpieczeństwa zachowuje poufność danych.
- Najczęściej spotykane rodzaje:
  - PPTP (Point ot Point Tunneling Protocol), L2TP (Layer Two Tunneling) – używane w MS Windows
  - Ipsec - (ang. Internet Protocol Security, IP Security) – zbiór protokołów służących implementacji bezpiecznych połączeń oraz wymiany kluczy szyfrowania pomiędzy komputerami. Protokoły tej grupy mogą być wykorzystywane do tworzenia Wirtualnej Sieci Prywatnej
  - SSTP (ang. Secure Socket Tunneling Protocol)
  - Tunelowanie SSL/TLS



połączenia klienta VPN do sieci firmowej intranet



połączenie PPTP sieci VPN typu router-router na komputerze z systemem operacyjnym Windows Server 2003.

Tworzenie VPN

- OpenVPN - jest ciekawą alternatywą dla klasycznych rozwiązań VPN opartych o protokół IPsec. Konfiguracja połączeń VPN jest bardzo prosta i zrozumiała nawet dla użytkownika nieobeznanego z technologią sieci VPN.

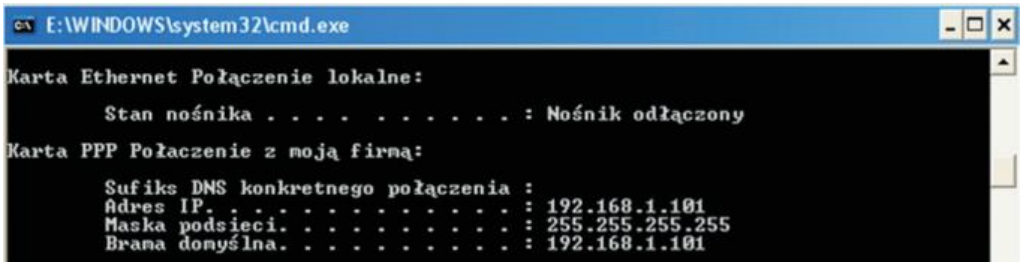
1. Windowa Server2003 → menu Start → Zarządzanie tym serwerem
2. Zaznaczamy Dodaj lub usuń rolę.
3. Zaznaczamy instalację Serwera dostępu zdalnego VPN
4. Zaznaczmy opcję Dostęp zdalny (połączenie telefoniczne lub sieć VPN)
5. W następnym etapie wybieramy Serwer sieci VPN. (W przypadku, gdy w komputerze, na którym pracuje Windows Server 2003 mamy tylko jedną kartę sieciową, (co właściwie nie powinno się zdarzyć) pojawi się komunikat ,w którym otrzymamy informacje, że serwer VPN wymaga, co najmniej dwóch interfejsów.
6. Wybieramy przypisywanie automatyczne DHCP
7. Zezwalamy użytkownikowi na dostęp zdalny. W tym celu klikamy prawym klawiszem myszki na użytkowniku wybieramy właściwości i przechodzimy do zakładki Telefonowanie i zaznaczamy opcję Zezwalaj na dostęp

Tworzenie VPN – Windows XP

- W Windows XP klikamy na Moje miejsce sieciowe prawym klawiszem myszki
- wybieramy właściwości i w menu po lewej stronie zaznaczamy Utwórz nowe połączenie.
- Otworzy się kreator nowego połączenia. W następnym oknie wybieramy Połącz się z siecią w miejscu pracy a w kolejnym zgodnie z tym, co chcemy skonfigurować Połączenie wirtualnej sieci prywatnej.
- Przechodzimy dalej i wpisujemy nazwę dla naszego połączenia (np. moja firma).
- Kolejny krok jest bardzo ważny gdyż podajemy adres IP serwera VPN, czyli inaczej mówiąc adres IP (oczywiście zewnętrzny) komputera z Windows Server 2003 gdzie postawiliśmy nasz serwer VPN.

Połączenie VPN

Dodatkowy interfejs PPP tworzący tunel VPN. (cmd → ipconfig/all)



- Aby sprawdzić czy wszystko działa z poziomu Windows XP wykonujemy ping do jednego z komputerów, który znajduje się w sieci wewnętrznej serwera Windows Server 2003.
- Jeśli okaże się, że w systemie klienta (Windows XP) nie mamy Internetu
  - klikamy na nasze połączenie prawym klawiszem myszki
  - wybieramy Właściwości i przechodzimy do zakładki Sieć.
  - Zaznaczamy protokół internetowy (TCP/IP) → Właściwości/Zaawansowane i odznaczamy pole Użyj domyślnej bramy w sieci zdalnej.

Pytania kontrolne

1. Co to jest sieć VLAN i jakie są korzyści ze stosowania tej technologii?
2. Jaka jest różnica pomiędzy VLAN i VPN?
3. Które z pojęć VLAN/VPN odpowiada stwierdzeniu:
   a) dzieli sieć fizyczną na wirtualne podsieci.
   b) łączy zalety sieci prywatnych i publicznych, umożliwiając firmom o wielu ośrodkach korzystanie z systemu zachowującego się jak w pełni prywatna sieć, lecz przesyłającego dane między ośrodkami siecią publiczną