T: Metody pomiarów sieci logicznej.

Zadanie1:

Odszukaj w serwisie internetowym Wikipedii informacje na temat modelu ISO/OSI.

Różnorodność istniejących protokołów sieciowych, zróżnicowanie architektury sieci stacjonarnych LAN/WAN oraz bezprzewodowych WLAN oraz stosowanych technologii w łączach telekomunikacyjnych powodują, że diagnozowanie poprawności działania sieci stało się bardzo trudne.

Zadanie2:

Zapoznaj się z zawartością następującej witryny internetowej:
http://www.computerworld.pl/artykuly/276800_1/Sprawdzanie.sieci.html.

Diagnozowanie sieci komputerowych może przebiegać według następujących metod:
- testowanie oddolne (bottom up) – zaczynamy sprawdzając połączenia fizyczne i stopniowo przechodzimy do kolejnych warstw sieciowych,
- testowanie odgórne (top down) – zaczynamy sprawdzając najwyższą warstwę sieci, np. sprawdzając poprawność aplikacji między głównymi węzłami sieci, a następnie diagnozowane są niższe warstwy sieci.

W strategii testowania oddolnego (bottom up), testowanie sieci rozpoczyna się od warstwy najniższej, czyli sprawdzania kabli i połączeń fizycznych, i stopniowo przechodzi do diagnozowania coraz wyższych warstw. Chociaż testowanie oddolne stosuje się zwykle podczas uruchamiania sieci nowych, w praktyce używa się naprzemiennie obydwóch sposobów diagnozowania sieci teleinformatycznej.

Strategia testowania odgórnego (top down) zakłada początek testowania od najwyższej warstwy sieciowej, po czym kolejno są diagnozowane coraz niższe warstwy sieci. Jest ona stosowana głównie w sieciach już działających, nawet współbieżnie z eksploatacją sieci. W tym sposobie testowania najpierw sprawdza się poprawność aplikacji między głównymi węzłami sieciowymi, następnie komunikację węzłów pośredniczących i dopiero na końcu poprawność poszczególnych kanałów fizycznych sieci teletransmisyjnej.

Do najczęściej stosowanych procedur lokalizujących uszkodzenia i diagnozujących sieci komputerowe należą:
- testowanie okablowania,
- analiza pakietów i protokołów,
- testowanie połączeń między węzłami sieci,
- statystyczna analiza trafiku sieciowego,
- analiza konfiguracji sieci,
- analiza stanu sieci,
- testowanie funkcji i realizacja procedur samotestowania.

Zgodnie z warstwową architekturą sieci można wydzielić następujące rodzaje pomiarów sieci komputerowych:
- pomiary parametrów fizycznych okablowania (miedzianego i światłowodowego),
- pomiary pasywne dokonywane wyłącznie przez obserwację i monitorowanie funkcjonowania sieci za pośrednictwem analizatorów,
- aktywne pomiary logiczne z możliwością iniekcji do sieci wybranych zestawów testowych.

Infrastruktury telekomunikacyjne:
- SDH (Synchronous Digital Hierarchy),
- ATM (Asynchronous Transfer Mode).

W sieci synchronicznej SDH można wydzielić kilka grup testowych, sprawdzających poszczególne obszary funkcjonowania sieci, wśród których można wyróżnić:
- testy poprawności odwzorowania plezjochronicznych sygnałów PDH w modułach transportowych STM (Synchronous Transport Mode),
- pomiary i testowanie sprawności wbudowanych alarmów programowych,
- zasadnicze pomiary jakości przekazów, czyli określenie stopy błędów transmisji w sieci,

- pomiary sprawności styków optycznych i elektrycznych w interfejsach,
- pomiary wartości fluktuacji fazy (jitter) i wędrówki (wander),
- pomiary układów zegarowych i synchronizacji,
- testowanie systemu zarządzania.

Zadanie3:

Odszukaj w serwisie internetowym dobreprogramy.pl informacje na temat programów inSSIDer oraz Retina Network Security Scanner, WirelessNetView.

inSSIDer Office to niewielki i prosty w obsłudze program do skanowania pasma radiowego wykorzystywanego przez sieci bezprzewodowe (Wi-Fi). Za pomocą programu po przeskanowaniu pasma radiowego zobaczymy jakie kanały wykorzystują sieci z najbliższego otoczenia, jaka jest moc ich sygnału oraz szereg innych informacji. Wszystkie informacje podawane są w bardzo czytelny sposób dzięki czemu nie dysponując żadną wiedzą możemy łatwo ustalić, które kanały sieci są wolne i jaki z nich najlepiej wybrać dla własnego urządzenia dostępowego (Access Point).

Retina Network Security Scanner to bezpłatny program, który służy do skanowania sieci bezprzewodowych. Retina WiFi Scanner pozwala między innymi na wykrycie i zlokalizowane bezprzewodowych punktów dostępowych oraz na zlokalizowanie wszystkich użytkowników korzystających z sieci WiFI. Dzięki Retinie uzyskamy informacje na temat dostępności publicznej punktu dostępowego. Poza tym, program udostępnia wiele istotnych informacji dotyczących sieci i sprzętu. Aplikacja generuje także eleganckie raporty z przeprowadzonych testów.

WirelessNetView to darmowe narzędzie służące do monitorowania sieci bezprzewodowej, który umożliwia zidentyfikowanie sieci będących w zasięgu naszego komputera. Aplikacja potrafi odczytać szczegółowe dane o znalezionych sieciach, takie jak identyfikator SSID, siła sygnału oraz sposób zabezpieczenia sieci.

Zadanie4:

Przeprowadź skanowanie pasma radiowego w szkolnej pracowni i określ używane w sieciach bezprzewodowych urządzenia.

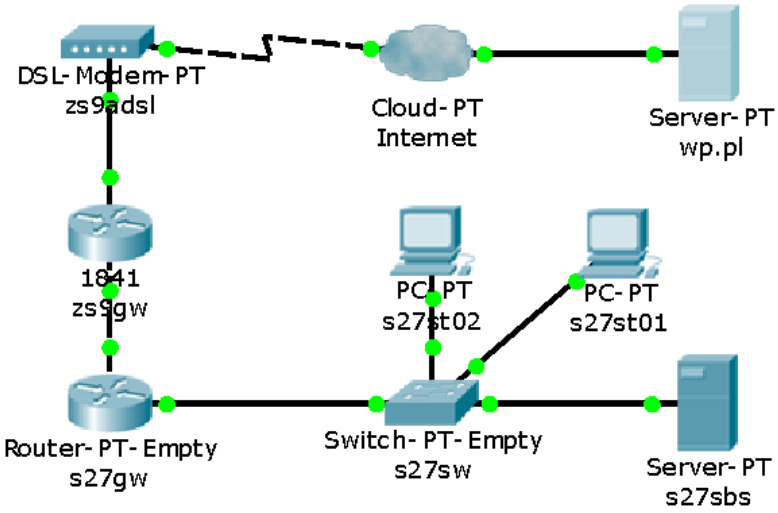
Zadanie5:

Uruchom w maszynie wirtualnej VirtualBox system Linux BackTrack lub Kali Linux i przeprowadź skanowanie dostępnych w szkole sieci bezprzewodowych. Opis konfiguracji maszyny wirtualnej bądź systemów znajdziesz na poniższych stronach internetowych:
http://backtrack.pl/2012/10/06/backtrack-na-maszynie-wirtualnej-problemy-vmware-virutalbox-qemu-kvm/
http://kali-linux.pl/uruchamianie-kali-linux-na-virtualbox_2013/

Zadanie6:

Wykorzystując dostępne w pracowni komputerowej wyposażenie oraz oprogramowanie przeprowadź pełną diagnozę szkolnej sieci komputerowej. Sporządź ze swoich działań sprawozdanie, w którym umieścisz wyniki testów i pomiarów sieci. Pracę zachowaj w pliku pod nazwą **$nazwisko_monitoring.odt** oraz prześlij pocztą elektroniczną do nauczyciela w postaci załącznika na adres greszata@zs9elektronik.pl. Sprawozdanie powinno zawierać następujące pomiary:

- warstwy fizycznej,
- opis konfiguracji urządzenia sieciowego w systemie,
- warstwy łącza danych,
- warstwy sieciowej,
- warstwy transportowej,
- warstwy sesji,
- warstwy prezentacji,
- warstwy aplikacji.



Ramki (warstwa 2) zawierają pakiety, pakiety (warstwa 3) zawierają datagramy, a datagramy (warstwa 4) zawierają segmenty sieci (warstwy 5 do 7).

Elementy ramki danych przesyłanych w sieciach standardu Ethernet (26 B oraz dane, ramka), warstwa łącza danych:
- 7 B – preambuła, naprzemienne jedynki i zera (10101010…),
- 1 B – SFD, znacznik początkowy ramki,
- 6 B – adres stacji odbiorczej MAC,
- 6 B – adres stacji nadawczej MAC,
- 2 B – typ protokołu lub długość ramki,
- 46 – 1500 B – dane,
- 4 B – FCB, suma kontrolna.

Elementy nagłówka IP (24 B oraz dane, pakiet), warstwa sieciowa:
- 4 b – wersja,
- 4 b – długość nagłówka,
- 1 B – typ usługi,
- 2 B – całkowita długość pakietu,
- 2 B – numer identyfikacyjny,
- 3 b – flagi,
- 13 b – przesunięcie,
- 1 B – czas życia,
- 1 B – protokół warstwy wyższej,
- 2 B – suma kontrolna nagłówka,
- 4 B – adres źródłowy IP,
- 4 B – adres docelowy IP,
- 3 B – opcje IP (niewymagane),
- 1 B – wypełnienie (niewymagane),
- X B - dane.

Elementy segmentu TCP (20 B oraz dane, datagram):
- 2 B – port nadawcy,
- 2 B – port odbiorcy,
- 4 B – numer sekwencyjny,
- 4 B – numer potwierdzenia,
- 4 b – długość nagłówka,
- 3 b – zarezerwowane,
- 9 b – flagi,

- 2 B – szerokość okna,
- 2 B – suma kontrolna,
- 2 B – wskaźnik priorytetu,
- 4 B – opcje, uzupełnione zerami,
- X B – dane.