LABORATORIUM SIECI WIELOUSŁUGOWYCH

POMIARY W SIECIACH IP

POLITECHNIKA WARSZAWSKA

INSTYTUT TELEKOMUNIKACJI

Warszawa, 2016

Spis treści

1 WPROWADZENIE 3

2 ROLA SYSTEMÓW MONITOROWANIA I POMIARÓW 3

3 METRYKI POMIAROWE 4

3.1 METRYKI ZDEFINIOWANE PRZEZ ITU-T 5
3.2 METRYKI ZDEFINIOWANE PRZEZ IETF 7

4 METODY POMIAROWE 8

4.1 POMIAR METODĄ AKTYWNĄ 9
4.2 POMIAR METODĄ PASYWNĄ 10
4.3 POMIAR METODĄ „OFF-LINE” 11
4.4 POMIAR METODĄ „ON-LINE” 12

5 NIEPEWNOŚĆ POMIARÓW 13

6 POMIARY W WIELOUSŁUGOWYCH SIECIACH IP 14

6.1 GRANICE KLAS OBSŁUGI W SIECI WIELO-DOMENOWEJ 15
6.2 PUNKTY ODNIESIENIA DLA LOKALIZACJI URZĄDZEŃ POMIAROWYCH 16

7 LITERATURA 19

8 PRZYKŁADOWE PYTANIA NA KOLOKWIUM 19

9 REALIZOWANE ZADANIA 20

9.1 ZADANIE 1: PRZYGOTOWANIE SIECI LABORATORYJNEJ 20
9.2 ZADANIE 2: PRZYGOTOWANIE I ZWERYFIKOWANIE NARZĘDZIA MGEN 22
9.3 ZADANIE 3: BADANIE SIECI IP 26

10 DODATEK A: ANALIZA WYNIKÓW POMIAROWYCH 27

10.1 WARTOŚĆ ŚREDNIA PRÓBKI 27
10.2 WARIANCJA PRÓBKI 27
10.3 PRZEDZIAŁY UFNOŚCI DLA WARTOŚCI ŚREDNIEJ 27

1 Wprowadzenie

W obecnych sieciach IP pomiary odgrywają znaczącą rolę jako jedna z podstawowych metod pozyskiwania wiedzy o stanie sieci. Informacja uzyskana z pomiarów umożliwia zarówno monitorowanie aktualnego stanu sieci, diagnozowanie sytuacji awaryjnych, jak również wspiera funkcje realizowane przez sieć, pozwalając na efektywne sterowanie ruchem w sieci, zarządzanie zasobami sieci, czy też jej odpowiednie planowanie.

Celem laboratorium jest zapoznanie studentów z podstawowymi metrykami pomiarowymi (w szczególności związanymi z jakością przekazu pakietów), metodami pomiarowymi wykorzystującymi pomiary aktywne oraz pasywne. W szczególności, w ramach ćwiczeń laboratoryjnych studenci wykonają pomiary charakterystyk przekazu pakietów, zbadają wpływ ruchu oraz ustawień sieci na charakterystyki przekazu. Ćwiczenia zostaną przeprowadzone z wykorzystaniem infrastruktury badawczej PLLAB2020.

2 Rola systemów monitorowania i pomiarów

Pomiary, oprócz metod analitycznych, są jednym z podstawowych narzędzi, które umożliwiają uzyskanie wiedzy o stanie sieci, jak również o zjawiskach w niej zachodzących. Przydatność metod pomiarowych wynika z następujących powodów: (1) obciążenie ruchem sieci IP jest trudne do przewidzenia, wynikające z różnorodności aplikacji, z których korzystają użytkownicy i braku kontroli dopuszczenia ruchu do sieci, (2) obecne sieci IP są strukturami coraz bardziej rozbudowanymi, opartymi na różnych, wzajemnie się przenikających technologiach; (3) dostępne i stosowane dotychczas modele analityczne nie umożliwiają dostarczenia wystarczającej wiedzy o stanie sieci; (4) wprowadzenie jakości obsługi do sieci pakietowych wymaga wiedzy o stanie obciążenia ruchowego w sieci, co biorąc pod uwagę (3) implikuje, iż systemy monitorowania i pomiarów w sieciach pakietowych mogą w istotny sposób wspierać pozyskiwanie wiedzy o stanie sieci niezbędnej dla potrzeb operatora, użytkownika, jak również dla mechanizmów sieciowych i aplikacji.

O znaczącej roli pomiarów w sieciach IP świadczy również intensywność prac mających na celu opracowanie efektywnych metod pomiarowych związanych z różnymi metrykami obrazującymi stan sieci. Prace te są prowadzone między innymi przez organizacje standaryzacyjne tj. IETF (Internet Engineering Task Force) [1] oraz ITU-T (International Telecommunication Union) [2], jak również projekty europejskie tj. IST-Intermon [4], IST-MoMe [5], IST-EuQoS [6].

W obecnych sieciach IP można wyróżnić trzy główne obszary zastosowania pomiarów, są to: (1) wsparcie wybranych funkcji sterowania ruchem oraz inżynierii ruchowej, (2) monitorowanie

stanu sieci oraz oferowanej jakości obsługi, oraz (3) testowanie sieci (urządzeń sieciowych) w warunkach laboratoryjnych.

Pomiary stosowane do wspierania funkcji sieciowych, np. funkcji przyjmowania nowych wywołań czy inżynierii ruchowej mają na celu uzyskanie informacji o stanie wykorzystania zasobów sieci (obciążenia łączy, zajętości buforów) oraz o ruchu przenoszonym w poszczególnych relacjach. Wiedza ta pozwala na zwiększenie efektywności mechanizmów sieciowych oraz mechanizmów zarządzania ruchem. Pomiar taki, powinien cechować się dużą wiarygodnością, przy założeniu najmniejszego wprowadzanego obciążenia do sieci (ruch pomiarowy przy pomiarach aktywnych). Zwykle pomiary tego typu są wykonywane w różnych skalach czasowych, w zależności od wymagań poszczególnych mechanizmów.

Dzięki pomiarom realizowanym w celu monitorowania sieci jest możliwe wykrywanie anomalii takich jak nieoczekiwany rozpływ ruchu, oferowanie obniżonej jakości oraz usterek sieci, np. awarii węzłów lub łączy. Wykrycie powyższych nieprawidłowości sieci może umożliwić podjęcie odpowiednich działań dla przywrócenia pożądanego stanu sieci.

Dodatkowy obszar zastosowania pomiarów jest związany z testowaniem sieci, urządzeń czy też poszczególnych mechanizmów lub protokołów. W przeciwieństwie do poprzednich zastosowań pomiarów, testowanie jest wykonywane w warunkach laboratoryjnych, w których pomiar jest wykonywany w ściśle określonych warunkach ruchowych, a jego wynik może być porównany z oczekiwanym rezultatem. Celem testów jest sprawdzenie czy sieć (urządzenie sieciowe) zachowuje się zgodnie z postawionymi wymaganiami dotyczącymi zgodności ze specyfikacją, sprawności oraz możliwości współpracy.

3 Metryki pomiarowe

Podstawą pomiarów jest precyzyjne zdefiniowanie metryk pomiarowych. Metryka zgodnie z definicją IETF metryka to „*clearly specified quantity related with the performance and reliability of the Internet that we'd like to know the value of*.” Metryki powinny charakteryzować się następującymi cechami:

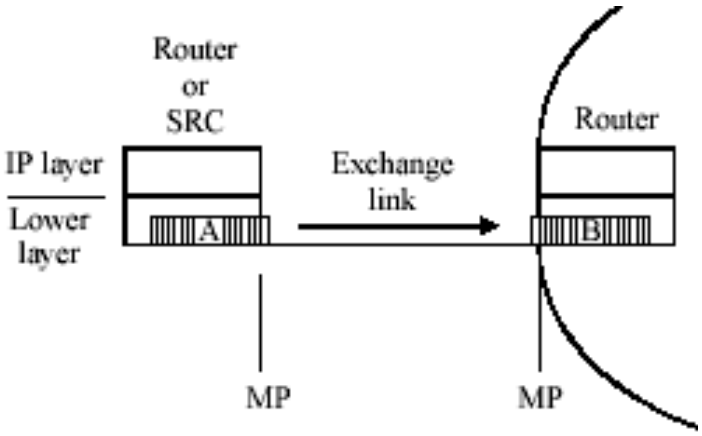
- metryki powinny być dobrze zdefiniowane,
- metoda pomiaru metryki powinna gwarantować, że wartość metryki zmierzonej w identycznych warunkach jest taka sama,
- odchyłka wartość metryki zmierzonej w odmiennych warunkach powinna być możliwa do wytłumaczenia,
- metryka powinna być użyteczna i odzwierciedlać zachodzące zjawisko w zrozumiały sposób,

Dzięki precyzyjnemu zdefiniowaniu metryk jest możliwe porównanie wyników uzyskanych w różnych pomiarach, np. prowadzonych w różnych laboratoriach pomiarowych. Metryki pomiarowe podlegają standaryzacji, którą zajmują się dedykowane grupy robocze w ramach organizacji IETF [1] oraz ITU-T [2]. W dalszej części rozdziału przedstawiono podstawowe metryki związane z przekazem pakietów w sieciach IP.

3.1 Metryki zdefiniowane przez ITU-T

Przedstawione poniżej metryki dotyczą efektywności przekazu pakietów przez sieć IP.

1. **Opóźnienie przekazu pakietów - IPTD** (IP Packet Transfer Delay) jest określane jako zbiór próbek dotyczących czasu upływającego pomiędzy wysłaniem pierwszego bitu a odebraniem ostatniego bitu pakietu pomiarowego przesyłanego pomiędzy dwoma punktami pomiarowymi (Measurement Points) umieszczonymi w mierzonej sieci lub jej części. Należy zwrócić uwagę, iż w przypadku straty pakietu lub znacznego opóźnienia pakietu wartość opóźnienia powinna zostać pominięta w obliczeniu statystyk metryki IPTD.



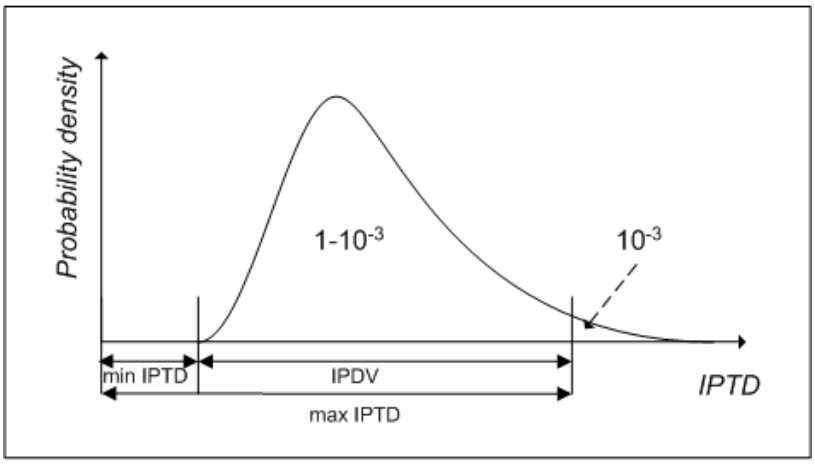
Rysunek 3-1: Definicja metryki IPTD

Wartość tej metryki podaje się w postaci parametrów statystycznych próbki, tj.:

1. minimalne opóźnienie (min IPTD),
2. maksymalne opóźnienie (max IPTD),
3. średnie opóźnienie (mean IPTD).

2. **Zmienność opóźnienia przekazu pakietów – IPDV** (IP Packet Delay Variation). Metryka ta określa zmienność opóźnienia doświadczanego przez pakiety w sieci i jest zdefiniowana jako różnica pomiędzy kwantylem rzędu α rozkładu opóźnienia przekazu pakietów IPTD a

wartością minimalnego opóźnienia minIPTD zmierzoną dla danej próby (okresu pomiarowego).



Rysunek 3-2: Ilustracja definicji zmienności opóźnienia IPDV (ITU-T)

W losowej próbie o liczności n, wartość kwantyla rzędu α można wyznaczyć jako wartość k-tego elementu, posortowanej rosnąco listy elementów X_k, gdzie $k = \lceil (n-1) * \alpha + 1 \rceil$

3. **Poziom strat pakietów - IPLR** (IP Packet Loss Ratio) jest zdefiniowany jako stosunek liczby pakietów odebranych do liczby pakietów wysłanych w danym okresie pomiarowym. Przy czym za stracone uznaje się pakiety, które nie zostały odebrane (np. w wyniku przepełnienia buforów lub uszkodzenia nagłówka pakietu) lub są znacznie opóźnione (zwykle więcej niż 3s).

$$IPLR = \frac{liczba\ wyslanych\, pakietow - liczba\ odebrnaych\ \ pakietow}{liczba\ wyslanych\, pakietow}$$

4. **Poziom błędnych pakietów – IPER** (IP Packet Error Ratio) jest zdefiniowany jako stosunek liczby pakietów z błędami w polu danych pakietu (przy czym poprawnym nagłówkiem) do liczby pakietów wysłanych w danym okresie pomiarowym.

5. **Przepływność na poziomie pakietów – IPPT** (IP Packet Throughput) określa stosunek liczby pakietów odebranych w danym okresie pomiarowym do długości tego okresu pomiarowego.

6. **Przepływność bajtowa IPOT** (Octet-based IP Packet Throughput) określa stosunek liczby bajtów zawartych w pakietach odebranych w danym punkcie sieci w pewnym okresie pomiarowym do długości tego okresu.

7. **Dostępność usługi IP** (IP service availability). Usługa jest uważana za dostępną jeśli w danym okresie pomiarowy poziom strat pakietów jest mniejszy od założonego progu (IPLR < c_1). Przy czym w przypadku sieci IP wspierającej różne klasy [3] usług wartość progu c_1 jest uzależniona od rodzaju klasy usługi i wynosi: dla klasy standard c_1=0.75, dla klasy 0 i 1 odpowienio c_1 = 0.03 lub 0.2

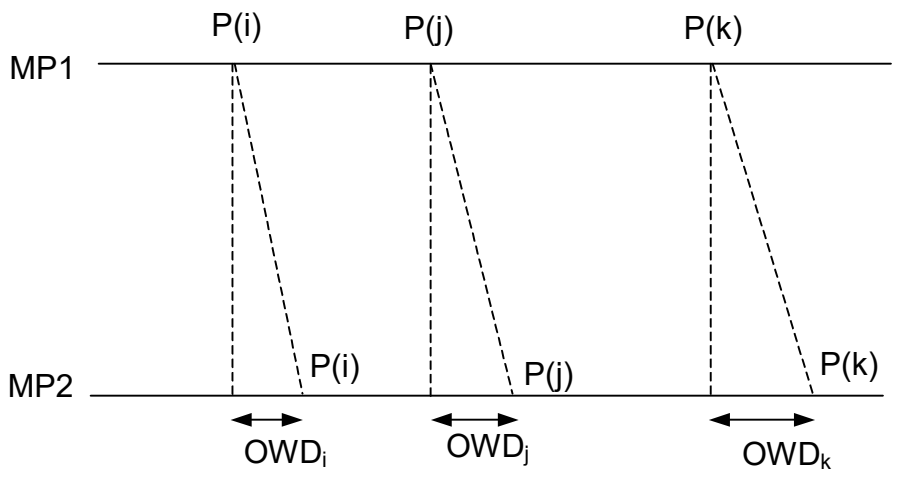
3.2 Metryki zdefiniowane przez IETF

Poniżej przedstawiono najważniejsze metryki zdefiniowane w ramach IETF [6].

1. **Dostępność** (Connectivity) [8] określa możliwość przekazu pakietów pomiędzy danym źródłem a urządzeniem docelowym. Urządzenie docelowe jest uznawane za dostępne jeśli pakiet wysłany ze źródło dotrze do urządzenia docelowego w określonym czasie.

2. **Opóźnienie w jednym kierunku OWD** (One Way Delay) [9] określa czas przekazu pakietu pomiędzy dwoma punktami w sieci. Matryka ma wartość ΔT, jeśli źródło wysłało pierwszy bit danego pakietu w chwili T, a urządzenie docelowe odebrało ostatni bit tego pakietu w chwili T+ΔT. Wartość tej metryki dla danego zbioru pakietów (próbki) podaje się w postaci parametrów statystycznych tj.:
   - Minimalne opóźnienie OWD (One-way-Delay-Minimum), zdefiniowane jako najmniejsza wartość opóźnienia w danej próbce.
   - Średnie opóźnienie OWD (Mean One-way-Delay), zdefiniowane jako średnia wartość opóźnienia w danej próbce.
   - Percentyl opóźnienia OWD (One-way-Delay-Percentile) określony jako x-ty percentyl opóźnienie danej próbki
   - Mediana opóźnienia OWD (One-way-Delay-Median) zdefiniowane jako wartośc mediany danej próbki,

3. **Zmienność opóźnienia przekazu pakietów – IPDV** (IP Packet Delay Variation) [12] jest określone jako różnica pomiędzy wartością OWD dla dwóch pakietów w mierzonej próbce pakietów. Zwykle przyjmuje się jako zmienność opóźnienia różnicę opóźnienia sąsiednich pakietów.



Rysunek 3-3: Ilustracja definicji zmienności opóźnienia IPDV wg. IETF

W przykładzie przedstawionym Rysunek 3-3, wartość zmienności opóźnienia wynosi: $IPDV_j = OWD_j - OWD_i$ oraz $IPDV_k = OWD_k - OWD_j$

4. **Opóźnienie pakietów w pętli –** (Round Trip Delay) [11] określa opóźnienie przekazu pakietu mierzone w jednym punkcie na drodze pomiędzy źródłem-przeznaczeniem-źródłem. Matryka ma wartość ΔT, jeśli źródło wysłało pierwszy bit danego pakietu w chwili T, urządzenie docelowe po odebraniu pakietu natychmiast odesłało pakiet do źródła a źródło odebrało ostatni bit tego pakietu w chwili $T+\Delta T$.

5. **Straty pakietów - OWL** (One Way Packet Loss) [10]. Metryka ta przyjmuje wartość 0 w przypadku poprawnego odebrania pakietu lub wartość 1 w przeciwnym przypadku. Wartości oczekiwana metryki OWL wyznaczona dla danej próbki oznacza poziom strat pakietów (IPLR).

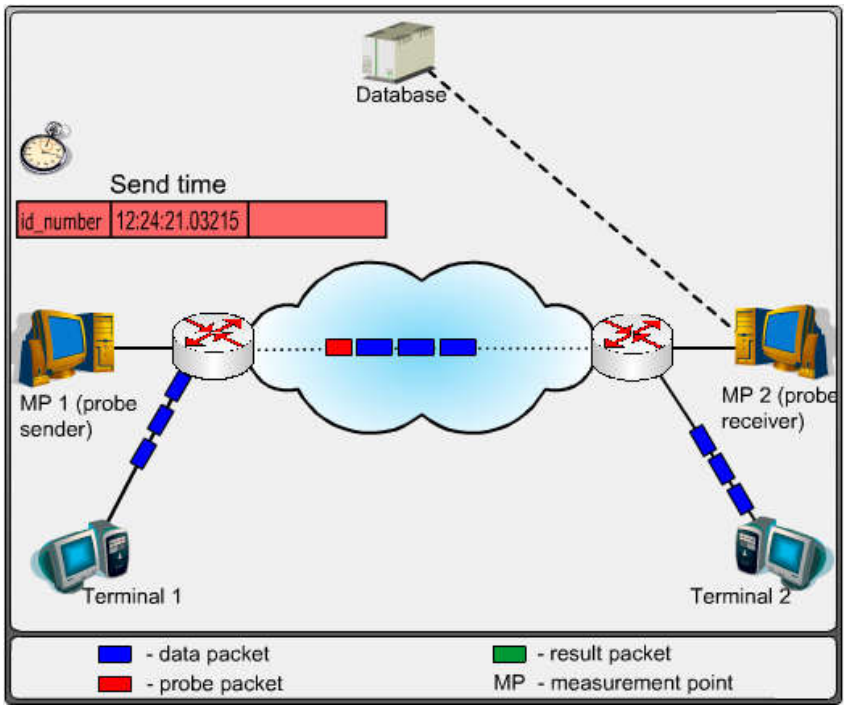
4 Metody pomiarowe

Podstawowa klasyfikacja metod pomiarowych obejmuje tzw.: metody „aktywne” oraz metody „pasywne”. Dodatkowo, pod względem sposobu zarządzania pomiarami i zbierania wyników, można wyróżnić narzędzia działające w jednym z dwóch trybów: pomiaru w planowanych eksperymentach (ang. „off-line”) oraz pomiar działającej sieci (ang. „on-line”).

Przedstawione dwa kryteria klasyfikacji są niezależne od siebie, tzn. metoda pomiaru aktywnego bądź też pasywnego może być wykorzystywana zarówno przez narzędzia pomiarowe pracujące w trybie „off-line” jak i „on-line”.

4.1 Pomiar metodą aktywną

Metoda pomiaru aktywnego (Rysunek 4-1) pozwala zmierzyć wartości metryk QoS (opóźnienie, zmienność opóźnienia, poziom strat pakietów, przepływności) poprzez wysyłanie specjalnych pakietów pomiarowych (ang. „probing packets") w ramach monitorowanego strumienia ruchu. Metoda aktywna zakłada, że pakiety pomiarowe są przesyłane tą samą drogą i obsługiwane dokładnie w ten sam sposób, co pakiety użytkowników. Dzięki temu, można uznać, że wartość metryk zmierzonych dla ruchu pomiarowego jest przybliżeniem wartości odpowiednich metryk dla pakietów użytkowników. Jednakże należy zwrócić uwagę, iż pomiar metodą aktywną pozwala jedynie estymować parametry populacji generalnej na podstawie wartości elementów próby (kolejnych wyników pomiaru).



Rysunek 4-1: Pomiar metodą aktywną.

Metoda aktywna zakłada, że nadajnik nadaje wysyłanym pakietom znacznik czasowy, który jest zapisywany w polu danych. Drugi znacznik czasowy jest nadawany przez odbiornik natychmiast po odebraniu pakietu pomiarowego. Porównanie wartości tych dwóch znaczników pozwala obliczyć wartości metryk związanych z opóźnieniem przesłania pakietu w sieci. Należy zwrócić uwagę na to, że kluczowym warunkiem poprawności pomiaru jest zapewnienie wspólnej podstawy czasu w nadajniku i odbiorniku, co można uzyskać np. synchronizując zegary korzystając z systemu GPS (Global Positioning System) lub protokołu NTP (Network Time Protocol).

Niekorzystną konsekwencją stosowania aktywnej metody pomiaru jest wprowadzenie na

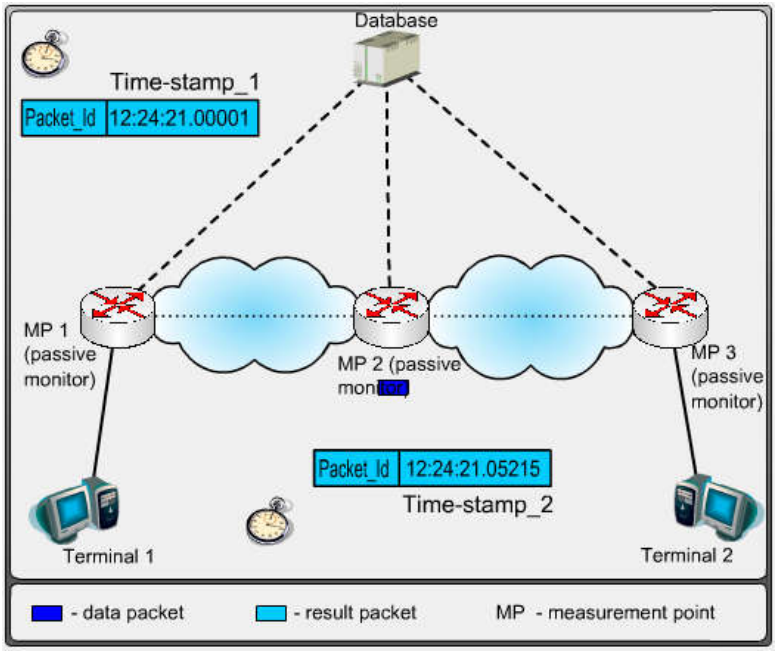
monitorowanym odcinku sieci dodatkowego obciążenia ruchowego związanego z pakietami pomiarowymi.

Głównym problemem zastosowanie metody aktywnej jest odpowiedni dobór wielkości ruchu pomiarowego oraz jego profilu. Ruch pomiarowy powinien być tak dobrany, aby można było uzyskać informacje na temat mierzonej ścieżki. Z drugiej strony wprowadzony ruch pomiarowy powinien być na tyle mały, aby wprowadzone dodatkowe obciążenie sieci zniekształcało wartości mierzonej metryki. Oprócz odpowiedniego doboru wielkości ruchu pomiarowego istotny jest dobór odpowiedniego profilu ruchu pomiarowego. Profil ten powinien być zbliżony do profilu ruchu mierzonego. W szczególności w praktyce stosuje się ruch pomiarowy o stałej szybkości bitowej lub generowany w sposób losowy. Istotną kwestią jest również dobranie odpowiedniej długości pakietów pomiarowych.

Ze względu na stosunkowo łatwą implementację i zarządzanie pomiarami, metoda aktywna jest wykorzystywana przez większość znanych narzędzi i systemów pomiaru parametrów QoS w komercyjnych i badawczych sieciach IP.

4.2 Pomiar metodą pasywną

Pasywna metoda pomiaru polega na obserwacji pakietów w danym punkcie pomiarowym (lub w wielu punktach) i odpowiedniej analizie zarejestrowanego zapisu ruchu. W przypadku obserwacji w jednym tylko punkcie pomiar może dotyczyć charakterystyki przesyłanego ruchu, jak np. średniej szybkości bitowej ruchu na danym łączu. W przypadku, kiedy rozważamy dwa punkty pomiarowe, metoda pasywna może też być wykorzystana do pomiaru wartości metryk jakości przekazu pomiędzy tymi punktami.



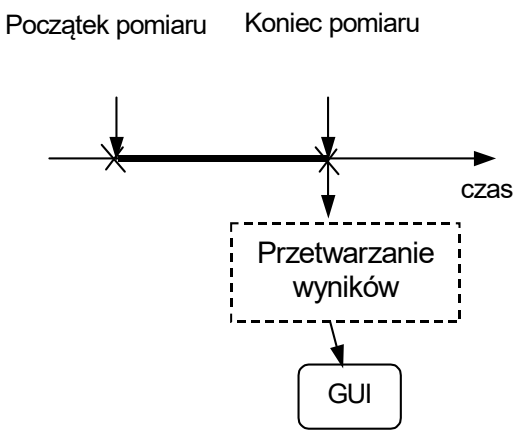
Rysunek 4-2: Pomiar metodą pasywną.

Pasywna metoda pomiaru parametrów QoS wymaga rejestrowania (ang. „trace”) zaobserwowanych pakietów i odpowiadających im znaczników czasowych w dwóch punktach pomiarowych. Następnie, zbiory zebrane w poszczególnych punktach pomiarowych są przesyłane do serwera zarządzającego pomiarami, gdzie są analizowane. Porównując znaczniki czasowe nadane danemu pakietowi w dwóch różnych punktach pomiarowych można obliczyć czas przesłania tego pakietu pomiędzy rozważanymi punktami. Oczywiście, zapewnienie synchronizacji zegarów w poszczególnych punktach pomiarowych jest kluczowe dla uzyskania poprawnego wyniku.

Metoda pasywna, w odróżnieniu od metody aktywnej, nie wprowadza dodatkowego ruchu pomiarowego. Oczywiście, przesłanie zbioru z zapisem ruchu zaobserwowanego w punkcie pomiarowym do serwera zarządzającego także wiąże się z dodatkowym ruchem, ale nie obciąża on bezpośrednio monitorowanej ścieżki i może być przesyłany np. z niższym priorytetem obsługi niż ruch użytkowników. Należy zwrócić uwagę na to, że metoda pasywna pozwala na bezpośredni pomiar jakości przekazu uzyskiwanej przez pakiety użytkowników. Z drugiej strony, jej podstawową wadą jest trudność implementacji, co jest związane z koniecznością rejestracji całego ruchu w danym punkcie pomiarowym i stosunkowo skomplikowanym przetwarzaniem uzyskanych w ten sposób zbiorów.

4.3 Pomiar metodą „off-line”

Różnica pomiędzy metodami “off-line” i “on-line” dotyczy sposobu zarządzania pomiarami, czyli rozpoczynania i zakończania procesu pomiarowego. Nie ma tutaj znaczenia sposób realizacji samego pomiaru, który może być wykonywany zgodnie z metodą aktywną bądź też pasywną. W przypadku narzędzi pomiarowych działających w trybie „off-line” wyniki są zbierane, umieszczane w bazie danych i ewentualnie przetwarzane dopiero po całkowitym zakończeniu procesu pomiarowego (Rysunek 4-3). W związku z tym, wyniki są dostępne dla użytkownika z pewnym opóźnieniem, które zależy od przyjętego czasu trwania eksperymentu.



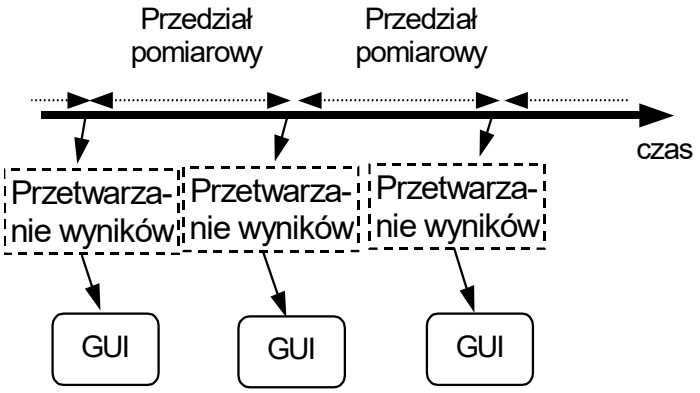
Rysunek 4-3: Schemat pomiaru „off-line”

Narzędzia pomiarowe działające w trybie „off-line” są zwykle wykorzystywane dla przeprowadzenia planowanych testów zgodnie ze ściśle określonym scenariuszem badawczym, w kontrolowanym środowisku. Przykładem takich pomiarów są testy nowych urządzeń i mechanizmów dla zapewnienia QoS, przeprowadzane w sieciach laboratoryjnych. Metodologia testowania QoS obejmuje następujące punkty:

1. Wytworzenie najgorszych możliwych warunków ruchowych na badanym łączu w sieci, poprzez generowanie ruchu zbiorczego o obciążeniu odpowiadającym maksymalnej liczbie połączeń dopuszczanej przez mechanizm sterowania przyjmowaniem wywołań. Charakterystyka generowanego ruchu powinna odpowiadać profilowi ruchu związanemu z aplikacjami reprezentatywnymi dla danej klasy ruchu.
2. Pomiar parametrów QoS (opóźnienie, zmienność opóźnienia, poziom strat) pomiędzy odpowiednimi punktami pomiarowymi. Jeśli wynik testu jest pozytywny, tzn. sieć oferuje wymagane gwarancje QoS w najgorszych dopuszczalnych warunkach ruchowych, to można wnioskować, że w każdych innych warunkach zastosowane mechanizmy będą działały poprawnie.

4.4 Pomiar metodą „on-line”

Metoda pomiaru „on-line” wykorzystuje zwykle tzw. mechanizm przesuwającego się okna pomiarowego. Wyniki są zbierane z punktów pomiarowych w określonych odstępach czasowych, bez przerywania procesu pomiarowego (Rysunek 4-4). Oczywiście długość okna może być różna, dostosowana do wymaganej skali czasu pomiaru. Wyniki z ostatniego okna pomiarowego mogą być natychmiast przetwarzane (np. metodami analizy statystycznej dla wyznaczenia wartości średniej i innych parametrów) i udostępniane operatorowi bez potrzeby zatrzymania procesu pomiarowego. Następnie, okno pomiarowe „przesuwa się” w czasie i cały proces jest powtarzany.

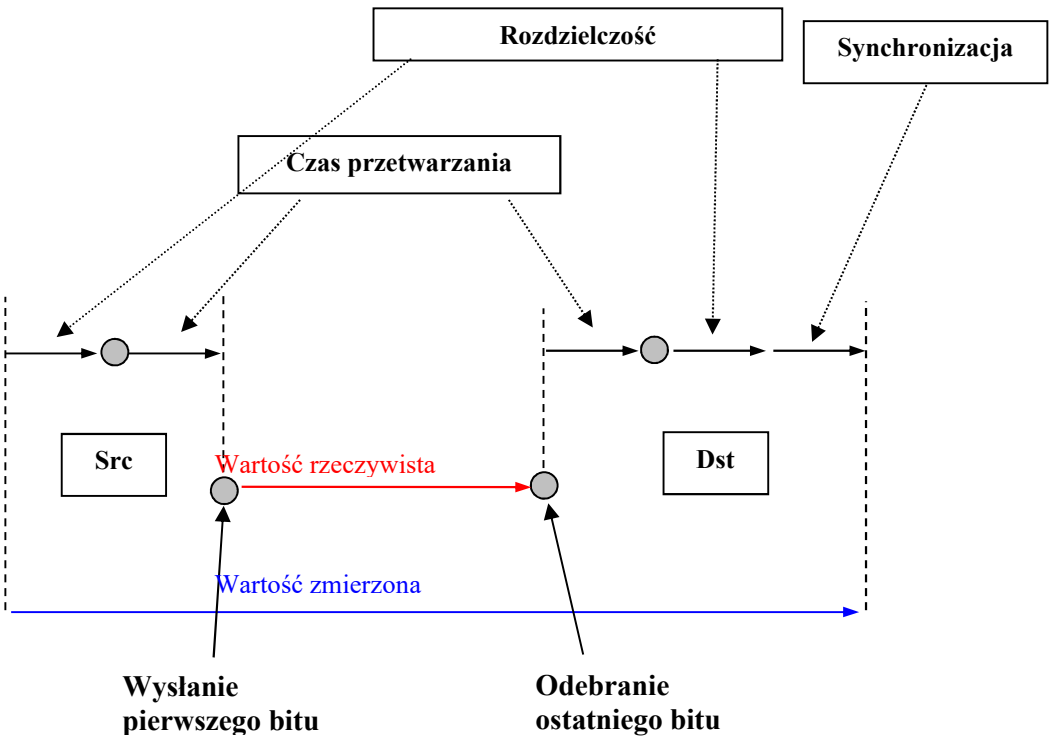


Rysunek 4-4: Schemat pomiru „on-line”

Pomiar odbywa się w sposób ciągły, zatem narzędzia pomiarowe korzystające z metody pomiaru „on-line” mogą być wykorzystywane do monitorowania na bieżąco działającej sieci. Dzięki temu, operator może mieć niemal natychmiastowy dostęp do bieżących wyników pomiarowych, które niosą informację o aktualnym stanie sieci i o jakości przekazu odczuwanej przez użytkowników.

5 Niepewność pomiarów

Każdy pomiar jest obarczony błędem. Źródłem błędów w pomiarach jest niedoskonałość metod pomiarowych oraz urządzeń pomiarowych. W szczególności w przypadku pomiarów aktywnych dodatkowy ruch zwiększa obciążenie sieci, co jest przyczyną wzrostu opóźnienia, jego zmienności, a także poziomu strat doświadczanych przez pakiety użytkowników. Również przyczyną błędów pomiarowych jest niedoskonałość urządzeń pomiarowych. W szczególności w przypadku pomiaru opóźnień przekazu pakietów należy uwzględnić wpływ czasu przetwarzania pakietów w urządzeniu pomiarowym, rozdzielczość zegara, synchronizację zegarów. Wartości te zostały zilustrowane na rysunku 33



Rysunek 5-1: Czynniki wpływające na niepewność pomiaru opóźnienia

Oprócz niepewności związanych z dokładnością zegarów używanych do mierzenia czasów, na podstawie których obliczane jest opóźnienie pakietu, istnieje niepewność związana fizycznymi własnościami interfejsów sieciowych. Ponieważ opóźnienie mierzone jest pomiędzy wysłaniem pakietu przez interfejs sieciowy ze źródła do odebrania tego pakietu przez interfejs sieciowy odbiornika, zachodzi potrzeba przeanalizowania jeszcze jednej kwestii związanej z niepewnością poprawności mierzonego czasu. Jeżeli czas wysłania zapisywany jest przez odpowiednio przystosowany do tego program, czas ten jest w rzeczywistości czasem tuż przed wysłaniem tego pakietu przez interfejs sieciowy. Jest to spowodowane tym, że interfejsowi musi jeszcze zostać przydzielone przerwanie przez system operacyjny, jak również występują opóźnienia przy przesyłaniu danych po szynie PCI, a dopiero wtedy pakiet ten zostanie wysłany do sieci. Czas ten nazywa się czasem przetwarzania.

6 Pomiary w wielousługowych sieciach IP

W tym rozdziale przedstawiona zostanie zarys metodologii pomiarów wielousługowych sieci IP dotyczący lokalizacji lokalizacji punktów pomiarowych. Podstawą przeprowadzenia pomiarów jest odpowiednia lokalizacja tzw. punktów pomiarowych (ang. MP – Measurement Points), w których zainstalowane są narzędzia pomiarowe. Przypomnijmy, że w sieci z jakością przekazu

pakiety w ramach poszczególnych połączeń są obsługiwane w ramach tzw. klas obsługi CoS (ang. Class of Service), które oferują przekaz pakietów z zapewnieniem odpowiednich gwarancji QoS. Dlatego, punkty pomiarowe powinny być tak zlokalizowane, aby pozwalać na monitorowanie jakości przekazu pakietów w ramach klas obsługi zdefiniowanych na poszczególnych odcinkach danego połączenia.

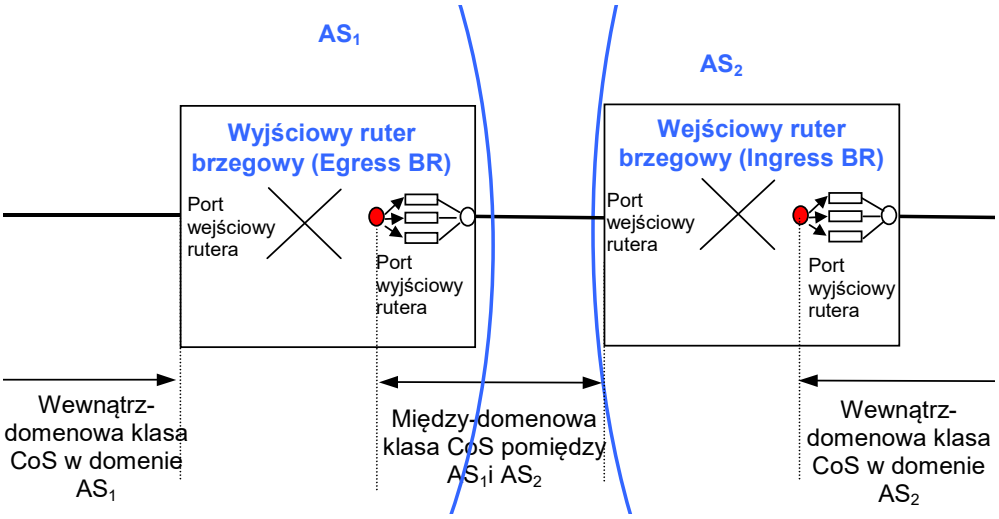
Należy zaznaczyć, że poszczególne domeny mogą wykorzystywać różne techniki sieciowe. W szczególności, sieci dostępowe mogą być budowane w oparciu o różne technologie, np. xDSL, UMTS, WiFi, LAN/Ethernet. Co więcej, klasy obsługi CoS mogą nieco różnić się w poszczególnych sieciach, oczywiście pod warunkiem, że złączenie CoS w sieciach obsługujących dane połączenie pozwala na zapewnienie odpowiednich gwarancji QoS w relacji od końca do końca. Pomiar jakości przekazu dla połączeń między-domenowych powinien zakładać korzystanie ze wspólnego zestawu parametrów (metryk) opisujących QoS w sposób spójny we wszystkich rozważanych rodzajach sieci. Dlatego zakładamy, że pomiar powinien być realizowany w warstwie sieci, która wykorzystuje protokół IP i jest wspólna dla wszystkich rodzajów rozważanych technik.

6.1 Granice klas obsługi w sieci wielo-domenowej

Przed zdefiniowaniem punktów odniesienia dla lokalizacji punktów pomiarowych wprowadzimy uproszczony model wielo-domenowej sieci IP. Model ten jest skonstruowany z punktu widzenia określonego połączenia typu punkt-punkt. Zakładamy, że połączenie to rozpoczyna się w terminalu w sieci dostępowej, przechodzi przez pewną liczbę domen szkieletowych i kończy się w terminalu podłączonym do innej sieci dostępowej. Punkty pomiarowe powinny być zlokalizowane w wybranych punktach wzdłuż całej ścieżki, tak, aby pozwalać na pomiar jakości przekazu oferowanej przez klasy CoS zaimplementowane w poszczególnych odcinkach sieci oraz na łączach między-domenowych. Zatem, oczywistym rozwiązaniem wydaje się umieszczenie punktów pomiarowych tam, gdzie klasy obsługi CoS zaczynają i kończą swoje działanie. W szczególności, klasa CoS w danej domenie zaczyna działać w wejściowym (ang. ingress) ruterze brzegowym na wejściu do kolejek na porcie wyjściowym rutera, czyli tam, gdzie pakiety podlegają klasyfikacji do poszczególnych klas CoS. Zakładamy, że kończy ona swoje działanie na porcie wejściowym tego rutera brzegowego, w którym pakiety opuszczają daną domenę (ang. egress).

Z kolei, na porcie wyjściowym tego rutera brzegowego rozpoczynają działanie między-domenowe klasy CoS. Między-domenowa klasa CoS kończy swoje działanie na porcie wejściowym rutera brzegowego w sąsiedniej domenie. W ten sposób wytyczono granice działania klas usług w

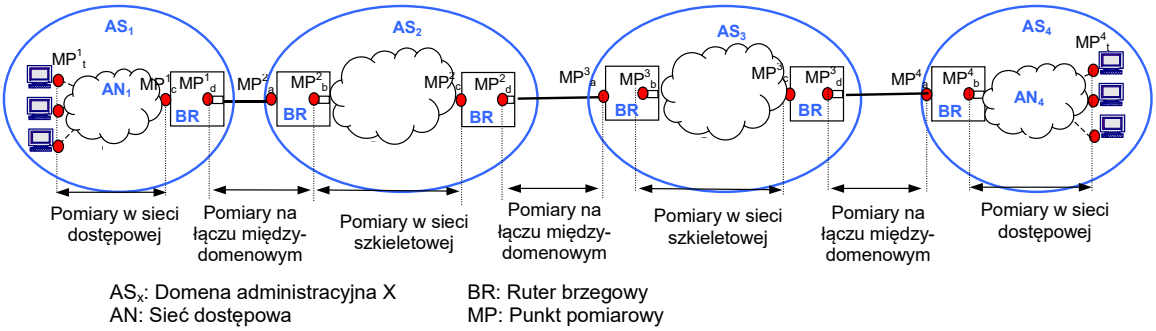
ramach poszczególnych domen oraz na łączach między-domenowych, co ilustruje Rysunek 6-1.



Rysunek 6-1: Granice klas obsługi (CoS) wewnątrz domeny i na łączach między-domenowych

6.2 Punkty odniesienia dla lokalizacji urządzeń pomiarowych

W tym rozdziale wyjaśnimy strategię lokalizacji punktów pomiarowych na przykładzie sieci składającej się z czterech domen administracyjnych, AS_X, X=1,...,4 (patrz Rysunek 6-2). Domeny AS_1 i AS_4 obejmują sieci dostępowe, natomiast domeny AS_2 i AS_3 to domeny obejmujące tylko sieci szkieletowe.



Rysunek 6-2: Lokalizacja punktów pomiarowych w przykładowej sieci składającej się z czterech domen

Zgodnie z przyjętą strategią lokalizacji punktów pomiarowych, w domenach pełniących rolę sieci szkieletowych (AS_1 i AS_2 na Rysunek 6-2) możemy wyróżnić następujące punkty odniesienia dla punktów pomiarowych:

1. MP^X_a: w wejściowym (ang. ingress) ruterze brzegowym domeny AS_X, na jego porcie wejściowym. Jest to punkt, w którym pakiety opuszczają obszar działania między-domenowej klasy usług CoS pomiędzy domenami AS_{X-1} i AS_X.

2. MP^X_b: w wejściowym (ang. ingress) ruterze brzegowym w domenie AS_X, w punkcie, gdzie pakiety wchodzą do kolejki na porcie wyjściowym. W tym właśnie punkcie pakiety wchodzą w obszar działania wewnątrz-domenowej klasy CoS.
3. MP^X_c: w wyjściowym (ang. egress) ruterze brzegowym domeny AS_X, w jego porcie wejściowym. W tym właśnie punkcie pakiety opuszczają obszar działania wewnątrz-domenowej klasy CoS w domenie AS_X.
4. MP^X_d: w wyjściowym (ang. egress) ruterze brzegowym w domenie AS_X, w punkcie, gdzie pakiety wchodzą do kolejki na porcie wyjściowym. W tym właśnie punkcie pakiety wchodzą w obszar działania między-domenowej klasy CoS zaimplementowanej na łączu pomiędzy domenami AS_X i AS_{X+1}.

Analogicznie powinna wyglądać strategia lokalizacji punktów pomiarowych w domenach obejmujących sieci dostępowe (AS_1 i AS_4 na Rysunek 6-2). Zatem, w domenie AS_1 mamy:

1. MP^1_t: w terminalu użytkownika.
2. MP^1_c: w wyjściowym (ang. egress) ruterze brzegowym domeny AS_1, w jego porcie wejściowym. W tym właśnie punkcie pakiety opuszczają obszar działania wewnątrz-domenowej klasy CoS w domenie AS_1.
3. MP^1_d: w wyjściowym (ang. egress) ruterze brzegowym w domenie AS_1, w punkcie, gdzie pakiety wchodzą do kolejki na porcie wyjściowym. W tym właśnie punkcie pakiety wchodzą w obszar działania między-domenowej klasy CoS zaimplementowanej na łączu pomiędzy domenami AS_1 i AS_2.

Z kolei, w domenie AS_4 można zdefiniować następujące punkty pomiarowe:

1. MP^4_a: w wejściowym (ang. ingress) ruterze brzegowym domeny AS_4, na jego porcie wejściowym. Jest to punkt, w którym pakiety opuszczają obszar działania między-domenowej klasy usług CoS pomiędzy domenami AS_3 i AS_4.
2. MP^X_b: w wejściowym (ang. ingress) ruterze brzegowym w domenie AS_4, w punkcie, gdzie pakiety wchodzą do kolejki na porcie wyjściowym. W tym właśnie punkcie pakiety wchodzą w obszar działania wewnątrz-domenowej klasy CoS w domenie AS_4.
3. MP^4_t: w terminalu użytkownika.

Dzięki lokalizacji punktów pomiarowych w zdefiniowanych powyżej punktach odniesienia możemy w rozważanej sieci wielo-domenowej przeprowadzać następujące pomiary:

1. Pomiary QoS pomiędzy dwoma punktami pomiarowymi:
   - Pomiędzy MP^X_t i MP^X_c: pomiar parametrów QoS w sieci dostępowej (kierunek „uplink”)

- Pomiędzy MP^X_b i MP^X_t: pomiar parametrów QoS w sieci dostępowej (kierunek „downlink”)
- Pomiędzy MP^X_b i MP^X_c: pomiar parametrów QoS w wewnątrz-domenowej klasie CoS w domenie AS_X.
- Pomiędzy MP^X_d i MP^{X+1}_a: pomiar parametrów QoS w między-domenowej klasie CoS na łączu pomiędzy domenami AS_X i AS_{X+1}.
- Pomiędzy MP^X_t i MP^Y_t: pomiar parametrów QoS od końca do końca.
- Oczywiście, można także wykonywać pomiary parametrów QoS na ścieżkach składających się z kliku domen i łączy między-domenowych.

2. Pomiary ilości i charakterystyki ruchu przesyłanego w danym punkcie pomiarowym:

- W punkcie MP^X_t: pomiar ruchu generowanego przez dany terminal
- W punkcie MP^X_a: pomiar ruchu wchodzącego do domeny AS_X danym łączem między-domenowym
- W punkcie MP^X_b: pomiar ruchu wchodzącego do usługi wewnątrz-domenowej w domenie AS_X
- W punkcie MP^X_c: pomiar ruchu wychodzącego z usługi wewnątrz-domenowej w domenie AS_X
- W punkcie MP^X_d: pomiar ruchu wychodzącego z domeny AS_X danym łączem między-domenowym

7 Literatura

[1] IETF IPPM (IP Performance Metrics) Working Group, http://www.ietf.org/html.charters/ippm-charter.html

[2] ITU-T Recommendation Y.1540, Internet protocol data communication service – IP packet transfer and availability performance parameters, December 2002

[3] ITU-T Recommendation Y.1541, Internet protocol data communication sernice - Quality of service and network performance objectives for IP-based services, May 2002

[4] IST-Intermon, Advanced architecture for INTER-domain quality of service MONitoring, modelling and visualisation, Project web page: www.ist-intermon.org

[5] IST-MOME, Monitoring and Measurement Luster, project web site: www.ist-mome.org

[6] IST-EuQoS, End-to-end Quality of Service support over heterogeneous networks, Project web page: www.ist-euqos.org

[7] IETF RFC 2330, "Framework for IP Performance Metrics", May 1998

[8] IETF RFC 2678, "IPPM Metrics for Measuring Connectivity", September 1999

[9] IETF RFC 2679, "A One-way Delay Metric for IPPM", September 1999

[10] IETF RFC 2680, "A One-way Packet Loss Metric for IPPM", September 1999

[11] IETF RFC 2681, "A Round-trip Delay Metric for IPPM", September 1999

[12] IETF RFC 3393, "IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)", November 2002

[13] IETF RFC 3763, "A One-way Active Measurement Protocol (OWAMP) Requirements", April 2004

8 Przykładowe pytania na kolokwium

1. Na czym polega metoda aktywna pomiaru?
2. Na czym polegają pomiary pasywne?
3. Opisz różnice między definicjami metryki IPTD pomiędzy ITU a IETF.
4. Opisz przyczyny błędów pomiarowych na przykładzie pomiaru opóźnienia.

9 Realizowane zadania

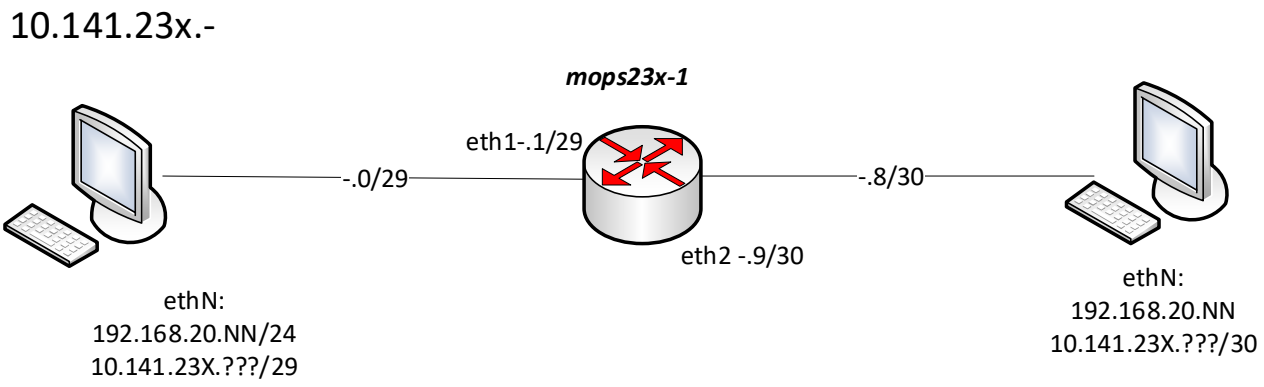
Celem ćwiczenia jest zbadanie charakterystyk przekazu pakietów w sieci IP oraz ocena wpływu parametrów sieci, np. obciążenia, pojemności buforów w węzłach, na charakterystyki przekazu. Badanie będzie realizowane przez pomiar podstawowych metryk dotyczących przekazu pakietów tj.

- **Opóźnienie przekazu pakietów, IPTD (IP Packet Transfer Delay),** jest zdefiniowane jako czas upływający pomiędzy chwilą wysłania pierwszego bitu a momentem odebrania ostatniego bitu danego pakietu w mierzonej sieci lub jej części.
- **Zmienność opóźnienia przekazu pakietów, IPDV (IP Packet Delay Variation)**, jest zdefiniowana jako różnica wartości percentyla 99.9% rozkładu opóźnienia przekazu pakietów a minimalną zmierzoną wartością.
- **Poziom strat pakietów, IPLR (IP Packet Loss Ratio)** jest zdefiniowany jako stosunek liczby pakietów straconych do liczby pakietów wysłanych w danym okresie pomiarowym. Przy czym za stracone uznaje się pakiety, które nie zostały odebrane (np. w wyniku przepełnienia buforów lub uszkodzenia nagłówka pakietu) lub są znacznie opóźnione.

Realizacja ćwiczenia obejmuje następujące zadania.

9.1 Zadanie 1: Przygotowanie sieci laboratoryjnej

W ramach przygotowania sieci laboratoryjnej należy skonfigurować urządzenia pomiarowe zgodnie ze schematem przedstawionym na rys. 1. Stanowisko składa się z 2 komputerów oraz rutera (maszyna wirtualna tiny core uruchomiona w PLLAB). X to numer zespołu podany przez prowadzącego, 192.168.20.NN to adres wyznaczony przez DHCP, natomiast ??? to adres urządzenia pomiarowego wyznaczony samodzielnie przez zespół laboratoryjny.



Rysunek 3: Schemat sieci laboratoryjnej

Przygotowanie sieci obejmuje:

I. Przydzielenie i skonfigurowanie adresów IP urządzeń pomiarowych (zgodnych z adresacją podsieci interfejsu do rutera) oraz rutingu dla adresów przeznaczenia zgodnie z przyjętym schematem sieci. (Należy skonfigurować oba urządzenia pomiarowe!)

Przykładowe polecenia do konfiguracji:

adresu IP: *ip addr add 10.141.23X.nnn/29 dev eth0*

rutingu: *ip route add 10.141.23X.nnn /24 via 10.141.23X.1*

II. Konfigurację ograniczenia rozmiaru bufora, przepływności oraz opóźnienia w ruterze na łączu do komputera dołączonego do podsieci 10.141.23X.8/30

Konfiguracja ta wymaga :

- zalogowania się do rutera (użytkownik root, hasło: cafe),

  ssh root@10.141.23X.1
- uruchomienia skryptu impariment.sh podając odpowiedni interfejs wyjściowy oraz wartości: np. przepływność 2 Mbps, bufor=5, 20 lub 50 pakietów. Na ruterze należy ustawić 5ms opóźnienia.

III. Weryfikację poprawności konfiguracji sieci przez wykonanie testów osiągalności pomiędzy:

a. terminalami pomiarowymi
b. terminalami a serwerem NTP (w przypadku ich użycia)

Przykładowe polecenia dla zweryfikowania:

- osiągalności:

  ping 10.141.23X.nnn

  ping 10.141.23X.nnn
- rutingu

  traceroute 10.141.23X.nnn

  traceroute 10.141.23X.nnn

Uwaga: Weryfikację należy wykonać z obu urządzeń pomiarowych.

IV. Synchronizacja zegarów urządzeń pomiarowych. Synchronizację należy wykonać zgodnie z poleceniem prowadzącego. Wykonujemy synchronizację do serwerów NTP o adresach:

- time.coi.pw.edu.pl
- ntp.itl.waw.pl (*193.110.137.171)*

Przykładowe polecenia:

Uruchomienie/ zatrzymanie usługi synchronizacji

/etc/init.d/ntp [start/stop]

Sprawdzenie stanu synchronizacji zegarów urządzeń pomiarowych

ntpq –p

Ręczna synchronizacja

ntpdate –u 193.110.137.171

9.2 Zadanie 2: Przygotowanie i zweryfikowanie narzędzia MGEN

Pomiary będą realizowane z wykorzystaniem narzędzia MGEN v5. Narzędzie to umożliwia pomiar metryk związanych z przekazem pakietów tj. IPTD, IPDV, IPLR. MGENv5 mierzy metodą aktywną z wykorzystaniem dwóch punktów pomiarowych. Pomiar wymaga wygenerowania strumienia ruchu pomiarowego o zadanym profilu na jednym urządzeniu pomiarowym, a następnie odebrania tego strumienia przez narzędzie MGENv5 uruchomione w trybie odbiornika na drugim urządzeniu pomiarowych. Należy zwrócić uwagę, iż pomiar wymaga utrzymania synchronizacji zegarów urządzeń pomiarowych.

Narzędzie MGENv5 umożliwia generowanie równoległych strumieni ruchu, z których każdy jest opisywany niezależnie. Generator umożliwia wygenerowanie ruchu zgodnie z pięcioma profilami ruchowymi. W czasie laboratorium wykorzystany zostanie profil Poisson oraz CBR.

- **Ruch typu CBR**, nazywany profilem PERIODIC. Profil ten umożliwia generowanie pakietów o stałej długości w stałych odstępach czasu. Parametry strumienia typu CBR podaje się w postaci `... PERIODIC [<rate> <size>]...,` gdzie `<rate>` oznacza liczbę pakietów generowanych w ciągu jednej sekundy, natomiast `<size>` oznacza rozmiar pola danych pakietu w bajtach. Należy zwrócić uwagę, iż rozmiar pola danych, nie może być mniejszy niż 28 bajtów, ani większy niż 8192 bajty.

- **Ruch typu Poisson,** nazwany profilem POISSON. Profil ten umożliwia generowanie pakietów o stałej długości w dostępach określonych rozkładem wykładniczym. Parametry strumienia typu POISSON podaje się w postaci `... POISSON [<aveRate (msg/sec)> <size (bytes)>]...,` gdzie `<aveRate (msg/sec)>` oznacza średnią liczbę pakietów

generowanych w ciągu jednej sekundy, natomiast `<size>` oznacza rozmiar pola danych pakietu w bajtach. Podobnie jak w przypadku profilu PERIODIC, rozmiar pola danych, nie może być mniejszy niż 28 bajtów, ani większy niż 8192 bajty.

- **Ruch typu ONOFF,** nazwany profilem BURST. Profil ten umożliwia generowanie ruchu typu ONOFF, w którym momenty rozpoczęcia stanu ON, profil ruchu generowanego w stanie ON oraz czas trwania stanu ON mogą być określone w sposób deterministyczny lub rozkładem wykładnicznym. Parametry strumienia typu BURST podaje się w postaci `... BURST [REGULAR|RANDOM <aveInterval (sec)> <patternType> [<patternParams>] FIXED|EXPONENTIAL <aveDuration (sec)>] ...,` gdzie parametr `REGULAR|RANDOM <aveInterval (sec)>` określa odstępy pomiędzy rozpoczęciem kolejnych stanów ON, parametry `<patternType> [<patternParams>]` dotyczą profilu ruchowego generowanego w stanie ON, natomiast parametry `FIXED|EXPONENTIAL <aveDuration (sec)>,` określają czas trwania stanu ON. Należy zwrócić uwagę, iż w stanie ON możemy generować dowolny z profili, tj. PERIODIC, POISSON oraz BURST.
- **Ruch o zmiennej szybkości,** nazwany profilem JITTER. Profil ten umożliwia generowanie pakietów o stałej długości w dostępach czasu zdefiniowanych dwoma parametrami, tj. średnią szybkością oraz współczynnikiem zmiany szybkości. Parametry strumienia typu JITTER podaje się w postaci `... JITTER [<rate> <size> <jitterFraction]...,` gdzie `<rate>` oznacza sazybkość generowania pakietów, `<size>` oznacza rozmiar pola danych pakietu, natomiast `<jitterFraction>` oznacza współczynnik zmian szybkości generowania pakietów, który musi zawierać się w przedziale (0 ; 0,5). Rozmiar pola danych pakietu nie może być mniejszy niż 28 bajtów, ani większy niż 8192 bajty.
- **Ruch odtwarzany na podstawie zapisanego zbioru pakietów,** nazywany CLONE. Ten typ źródła umożliwia odtworzenie uprzednio zapisanego strumienia pakietów. Parametry tego typu źródła są podawane w postaci `... CLONE [<fileType> <fileName> [<repeatCount>]]... Z...` gdzie `<fileType>` oznacza format zapisanego zbioru pakietów (obecnie jedyny dostępny format to tcpdump, `<fileName>` jest nazwą zbioru, natomiast `<repeatCount>` oznacza liczbę powtórzeń tego samego zbioru. Wartość *-1* oznacza, że ruch będzie powtarzany aż do momentu zatrzymania źródła, wartość 0 oznacza, że zapisany zbiór pakietów będzie odtworzony tylko raz, natomiast dowolna wartość większa niż 0, oznacza liczbę powtórzeń.

Uruchomienie generatora wymaga przygotowania pliku konfiguracyjnego, w którym zawarty jest opis generowanych strumieni ruchu. Każdy wiersz pliku konfiguracyjnego określa parametry strumienia zgodnie z następującą składnią:

```
[<eventTime>] <eventType> <parameters ...> [<options ...>],
```

gdzie `[<eventTime>]`, określa czas upływający od uruchomienia generatora w którym ma zostać wykonana operacja określona przez `<eventType>`, natomiast `<parameters ...> [<options ...>]` definiują parametry właściwe dla danej operacji. Rysunek 4 przedstawia przykładowy plik konfiguracyjny dla generatora MGENv5, w którym zdefiniowano trzy strumienie odpowiednio o profilu CBR, POISSON oraz ONOFF.

```
##################################################
# Example MGEN script
##################################################
# These are some "Transmission Event" script lines

# Here is a constant bit rate flow to the loopback interface
0.0 ON  1 UDP SRC 5001 DST 127.0.0.1/5000 PERIODIC [1 1024]

# Here is a series of Poisson distributed packet transmissions
0.0 ON  2 UDP SRC 5000 DST 192.168.1.1/5001 POISSON [1 4096]

# Here is a "burst" transmission flow to the loopback interface
# The bursts are at regular 10 sec. intervals with fixed 5 sec. duration
0.0 ON  3 UDP DST 127.0.0.1/5000 \
BURST [REGULAR 10.0 PERIODIC [10.0 256] FIXED 5.0]

# To modify parameters of flow #2
4.0 MOD 2 PERIODIC [10 1024]

# To terminate flows after 10.0 seconds
10.0 OFF 1
10.0 OFF 2
30.0 OFF 3
```

Rysunek 4 Przykładowy plik konfiguracyjny dla generatora MGENv5.

W ramach każdego strumienia należy określić: numer strumienia, rodzaj protokołu transportowego (UDP lub TCP), numer portu źródłowego, docelowy adres IP/numer portu, a także parametry generowanego profilu ruchu.
Uruchomienie generatora jest możliwe z poziomu poleceń w trybie konsoli ekranowej

```
mgen input <nazwa pliku konfiguracyjnego>
```

Pomiar wartość i metryk wymaga odebrania generowanego strumienia pakietów w odbiorniku. W tym celu należy uruchomić narzędzie MGENv5 w trybie odbiornika. Jest możliwe z poziomu poleceń w trybie konsoli ekranowej

```
mgen port <port number>
```

lub za pomocą pliku konfiguracyjnego, którego przykładowy format przedstawia Rysunek 5.

```
##################################################
# Example MGEN script
##################################################
#Monitor UDP port numbers 5000, 5003, 5004, 5005, 5009
#and TCP port number 6000, 6003, 6004, 6005
#beginning at time 0.0

0.0 LISTEN UDP 5000,5003-5005,5009

0.0 LISTEN TCP 6000,6003-6005
```

Rysunek 5 Przykładowy plik konfiguracyjny dla narzędzia MGENv5 uruchomionego w trybie odbiornika.

Wyniki pomiaru są przedstawione w postaci tekstowej zawierające informację o każdym odebranym pakiecie. Informacje te zawierają między innymi czas wysłania i odebrania pakietu, numer strumienia, numer sekwencyjny pakietu, długość pakietu. Przykładowy wynik pomiaru przedstawia Rysunek 6 oraz Rysunek 7.

```
18:39:44.984376  RECV  proto>UDP  flow>1  seq>0  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:44.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:45.984376  RECV  proto>UDP  flow>1  seq>1  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:45.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:46.984376  RECV  proto>UDP  flow>1  seq>2  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:46.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:47.984376  RECV  proto>UDP  flow>1  seq>3  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:47.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:48.984376  RECV  proto>UDP  flow>1  seq>4  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:48.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:49.984376  RECV  proto>UDP  flow>1  seq>5  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:49.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:50.984376  RECV  proto>UDP  flow>1  seq>6  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:50.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:51.984376  RECV  proto>UDP  flow>1  seq>7  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:51.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:52.984376  RECV  proto>UDP  flow>1  seq>8  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:52.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:53.984376  RECV  proto>UDP  flow>1  seq>9  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:53.984375 size>28 gps>INVALID,0.000000,0.000000,0
18:39:54.984376  RECV  proto>UDP  flow>1  seq>10  src>192.168.1.106/7001  dst>192.168.1.106/5000
sent>18:39:54.984375 size>28 gps>INVALID,0.000000,0.000000,0
```

Rysunek 6 Przykładowy wynik pomiaru dla strumieni UDP.

```
19:08:44.703125 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.687500 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.703125 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.703125 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.703125 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.703125 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.718750 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.703125 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.718750 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.718750 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.734375 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.718750 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.734375 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.734375 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.734375 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.734375 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.750000 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.734375 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.750000 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
sent>19:08:44.750000 size>65535 gps>INVALID,999.000000,999.000000,-999 flags>0x01
19:08:44.765625 RECV proto>TCP flow>1 seq>0 src>192.168.1.106/7001 dst>192.168.1.106/6000
```

Rysunek 7 Przykładowy wynik pomiaru dla strumieni TCP.

Ponadto, uzyskanie wartości metryk, tj. mean IPTD, IPDV, IPLR, wymaga odpowiedniego przetworzenia wyników pomiarowych za pomocą narzędzi analizujących pliki wyjściowe, np. `calc-mgen`. Narzędzie `calc-mgen` oblicza wartości następujących metryk: min IPTD, mean IPTD, max IPTD, IPDV (w oparciu o percentyl 99,9%, 99% oraz 95%), jak również metrykę IPLR.

Przykładowe polecenia:

calc-mgen test.txt

Należy zwrócić uwagę, iż MGENv5 realizuje pomiary metodą dwupunktową. Z tego względu prawidłowy pomiar opóźnienia przekazu pakietów oraz zmienności opóźnienia wymaga synchronizacji czasu pomiędzy punktami pomiarowymi.
Szczegółowy opis generatora MGENv5 jest dostępny w instrukcji obsługi zawartej w katalogu mops *mgen.html*.

Zadania do wykonania w sieci lokalnej:

1. Zweryfikować zgodność profilu ruchu generowanego przez narzędzie MGENv5 za pomocą narzędzia tcpdump lub Wireshark dla kilku szybkości generowania, różnych długości pakietów, np. 100B, 1400B
2. Zweryfikować poprawność pomiaru metryk IPTD, IPDV, IPLR w sieci lokalnej.

9.3 Zadanie 3: Badanie sieci IP

W ramach tego zadania należy zbadać własności sieci IP przez pomiar charakterystyk przekazu pakietów, tj. wartości metryk IPTD, IPDV, IPLR za pomocą metody aktywnej dla rozmiaru bufora w ruterze (rozmiar bufora = 5, 20 i 50 pakietów), różnego obciążenia sieci (rho=0.2, 0.8, 0.95), oraz dwóch profili ruchu (Poisson i CBR). Na ruterze należy ustawić dodatkowe 5ms opóźnienia. Ruch powinien być generowany od komputera lewego (dołączonego do sieci 10.141.23X.0/29) do komputera prawego (dołączonego do sieci 10.141.23X.8/30)

Na podstawie uzyskanych wyników należy określić wpływ na charakterystyki przekazu pakietów IPTD (min, avg, max), IPDV, IPLR:

- rozmiarów bufora
- obciążenie ruchowego
- profilu ruchowego

We wnioskach należy wyjaśnić przyczyny obserwowanych zjawisk.

10 Dodatek A: Analiza wyników pomiarowych

W rozdziale tym omówiono metody analizy wyników pomiarowych oraz ich prezentacji. Metody te są „narzędziem”, które umożliwiają uzyskanie wiedzy o badanym zjawisku na podstawie wyników pomiarowych dostarczonych przez system pomiarowy. Należy przy tym zwrócić uwagę, iż pomiary dostarczają jedynie pewną próbkę z populacji występującej w badanym procesie. Przykładowo mierząc opóźnienie przekazu pakietów, system pomiarowy dostarcza nam wartości opóźnień doświadczanych przez pakiety testowe, które są jednie pewną próbką opóźnień wprowadzanych przez badany system. Poniżej przedstawiono podstawowe miary stosowane dla analizy wyników pomiarowych

10.1 Wartość średnia próbki

Wartość średnią próbki nazywamy średnią arytmetyczną wartości elementów próbki, określoną jako:

$$\bar{x} = \frac{1}{n}\sum_{i=1}^{n} x_i \tag{10.1}$$

gdzie: n – oznacza liczności próbki; xi – oznacza wartość i-tego elementu próbki

10.2 Wariancja próbki

Wariancją próbki, oznaczoną jako s2 nazywamy wielkość określona jako:

$$s^2 = \frac{1}{n-1}\sum_{i=1}^{n} (x_i - \bar{x})^2 \tag{10.2}$$

gdzie: n – oznacza liczności próbki, xi – oznacza wartość i-tego elementu próbki;

10.3 Przedziały ufności dla wartości średniej

Biorąc pod uwagę, iż pomiar dostarcza jedynie pewną próbkę z populacji, zatem powstaje pytanie czy wyznaczona wartość średniej dla próbki (4.1) jest dobrym estymatorem wartości oczekiwanej wyznaczonej dla populacji. O ile wyznaczenie dokładnej wartości oczekiwanej wymagałoby próbki zawierającej całą populację, jednakże na podstawie próbki oraz znając rozkład

mierzonej wartości możemy łatwo określić pewien przedział (c1, c2), w którym z zadanym prawdopodobieństwem, 1-α, zawarta jest wartość oczekiwana populacji (4.3).

$$\Pr\{c_1 \le \overline{X} \le c_2\} = 1 - \alpha \qquad (10.3)$$

Przedział ten nazywamy przedziałem ufności, natomiast wartość 100*(1-α) poziomem ufności. Zwykle wyniki pomiarów przedstawia się zakładając 95% lub 99% poziom ufności.

Wartości przedziału ufności dla dowolnego rozkładu zmiennej losowej można wyznaczyć w przybliżeniu korzystając z właściwości centralnego twierdzenia granicznego. Na mocy tego twierdzenia, jeśli poszczególne elementy próbki było mierzone niezależnie oraz wartość średnia dla populacji wynosi μ, a wariancja dla populacji wynosi σ2 to wartość średnią dla próbki można przybliżyć z rozkładu normalnego o parametrach:

$$\overline{x} \approx N\left(\mu, \frac{\sigma}{\sqrt{n}}\right) \qquad (10.4)$$

gdzie σ - oznacza odchylenie standardowe dla populacji, σ /√n jest błędem standardowym oraz n licznością próbki.

Stosując warunek standaryzacji zmiennej losowej o rozkładzie normalnym funkcją

$$Z = \frac{\overline{x} - \mu}{\frac{\sigma}{\sqrt{n}}} \qquad (10.5)$$

Przedział ufności można wyznaczyć z zależności (4.6):

$$\Pr\{-z_{1-\alpha/2} \le \frac{\overline{x} - \mu}{\frac{\sigma}{\sqrt{n}}} \le z_{1-\alpha/2}\} = 1 - \alpha \qquad (10.6)$$

gdzie z1-α/2 jest kwantylem rzędu 1-α/2 standardowego rozkładu normalnego N(0,1)

Zatem przedział ufności dla wartości średniej μ na poziomie 100*(1-α) wynosi:

$$\left[\ \overline{x} - z_{1-\alpha/2} * \frac{\sigma}{\sqrt{n}} \quad ; \quad \overline{x} + z_{1-\alpha/2} * \frac{\sigma}{\sqrt{n}}\ \right] \qquad (10.7)$$