Monitorowanie sieci

(w oparciu o „Protokoły SNMP i RMON” W. Stallings)

Architektura monitorowania sieci

Obszary monitorowania sieci

- ***Dostępu do monitorowanych informacji***
  - w jaki sposób zdefiniować monitorowane informacje oraz jak pobrać te informacje z zasobów do zarządcy.
- ***Projektowania mechanizmów monitorowania***
  - w jaki sposób najlepiej uzyskać informacje z zasobów.
- ***Zastosowania monitorowanych informacji***
  - w jaki sposób używane są monitorowane informacje w różnych dziedzinach zarządzania.

Informacje nadzorowania sieci

- ***Statyczne*** – informacje te charakteryzują bieżącą konfigurację oraz jej elementy,
- ***Dynamiczne*** – informacje te są powiązane ze zdarzeniami w sieci,
- ***Statystyczne*** – są to informacje które można wywieść z informacji dynamicznych,

Informacja statyczna

- Informacja statyczna zazwyczaj jest generowana przez związany z nią element, np. router przechowuje swoją własną informację o konfiguracji.
- Informacja statyczna może być dostępna bezpośrednio dla nadzorcy, jeżeli dany element posiada własne oprogramowanie agenta lub udostępniana pełnomocnikowi, który przekaże ją nadzorcy.

Informacja dynamiczna

- Informacja dynamiczna jest zbierana i przechowywana przez odpowiedzialny za odpowiednie zdarzenia element sieci.
- Jeżeli dany system jest połączony z siecią LAN, wówczas większość jego działalności może być obserwowana przez inny system w tej sieci. Urządzenie w sieci LAN, które obserwuje cały ruch w sieci i gromadzi informacje o tym ruchu nazywane jest *zdalnym nadzorcą.*

Informacje statystyczne

- Informacje statystyczne mogą być generowane przez każdy system, który ma dostęp do informacji dynamicznych.
- Informacje statystyczne mogą być generowane przez samego nadzorcę sieci. Wymaga to jednak przesłania wszystkich nieopracowanych jeszcze danych do nadzorcy, gdzie zostaną przeanalizowane i podsumowane.

Konfiguracja monitoringu sieci

- Aplikacja monitoringu
- Funkcja zarządcy
- Funkcja agenta
- Zarządzane obiekty

Aplikacja monitoringu

- ***Aplikacja monitoringu*** – komponent ten zawiera funkcje monitoringu sieci, które są widoczne dla użytkownika, takie jak monitorowanie wydajności, monitorowanie sytuacji awaryjnych i monitorowanie wykorzystania obiektów.

Funkcja zarządcy

- ***Funkcja zarządcy*** – jest to model nadzorcy sieci, który wykonuje podstawową funkcję monitoringu, tj. odbiera dane z innych elementów konfiguracji.

Funkcja agenta

- ***Funkcja agenta*** – moduł ten zbiera i zapisuje informacje zarządzania z jednego lub więcej elementów sieciowych orz przekazuje te informacje do nadzorcy.

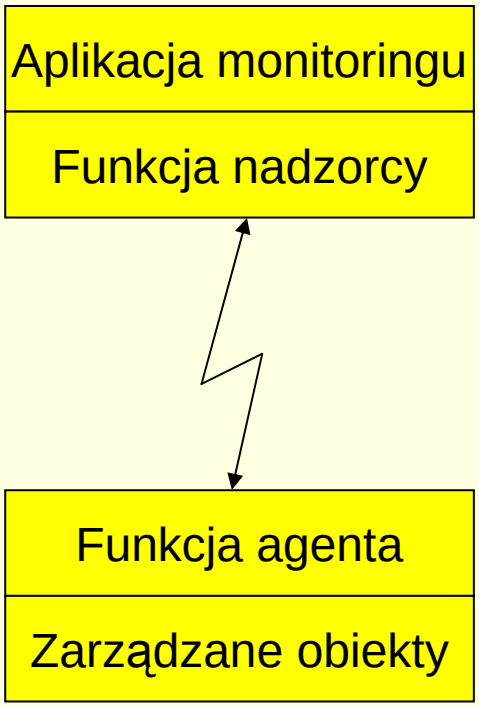
Zarządzane obiekty

- ***Zarządzane obiekty*** – jest to informacja zarządzania, która reprezentuje zasoby oraz ich działania.

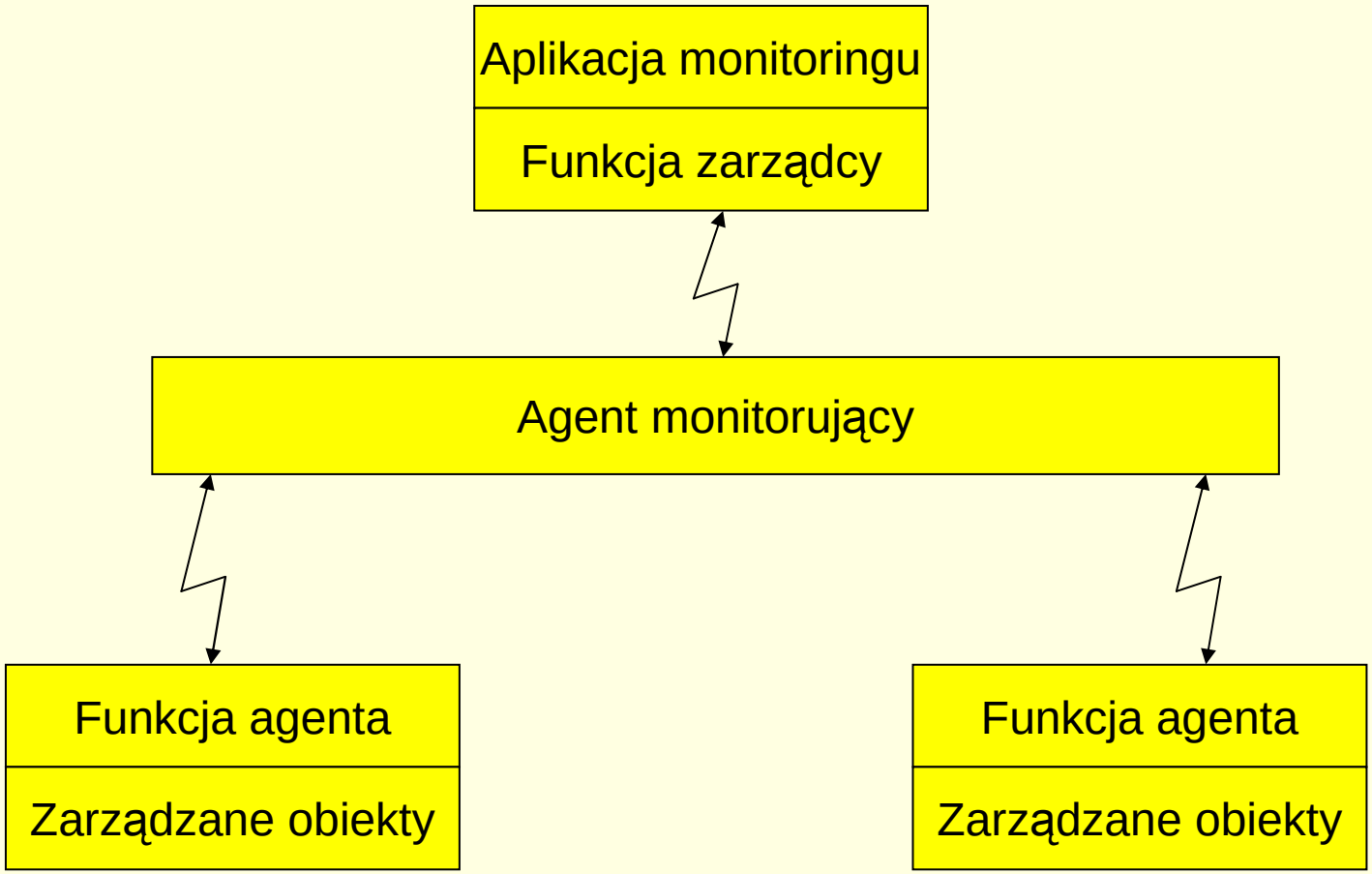
Agent monitorujący

- ***Agent monitorujący*** – przeprowadza podsumowania oraz analizy statystyczne informacji zarządzania. Jeżeli agent monitorujący nie jest zintegrowany z zarządcą, wówczas zachowuje się jak agent i przesyła podsumowane informacje do zarządcy.

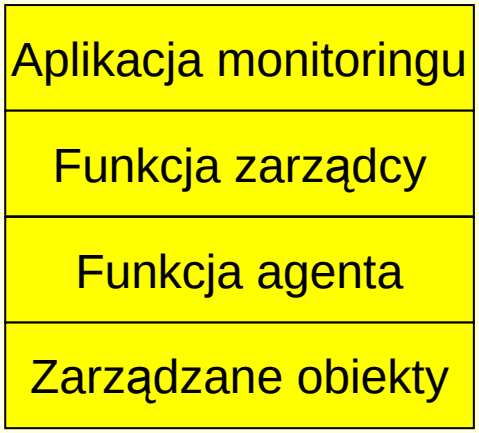
Model zarządca - agent



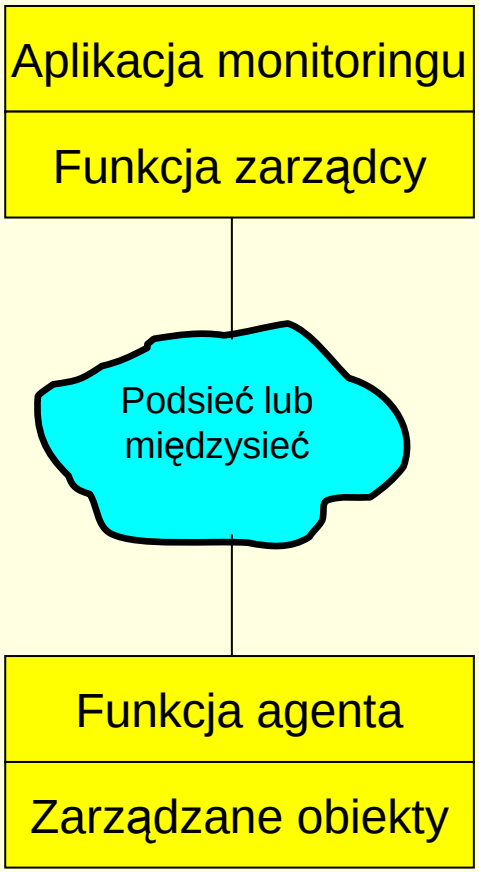
Model z podsumowaniem



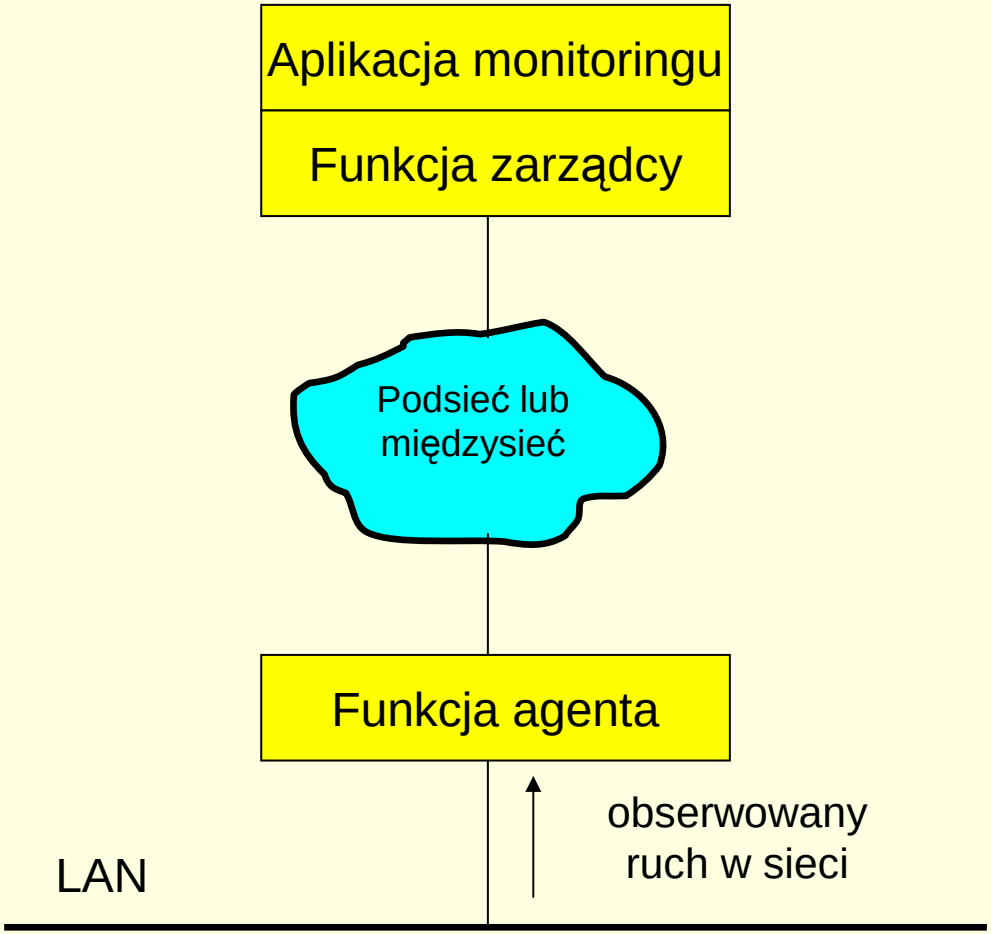
Zarządzanie zasobami w systemie zarządcy



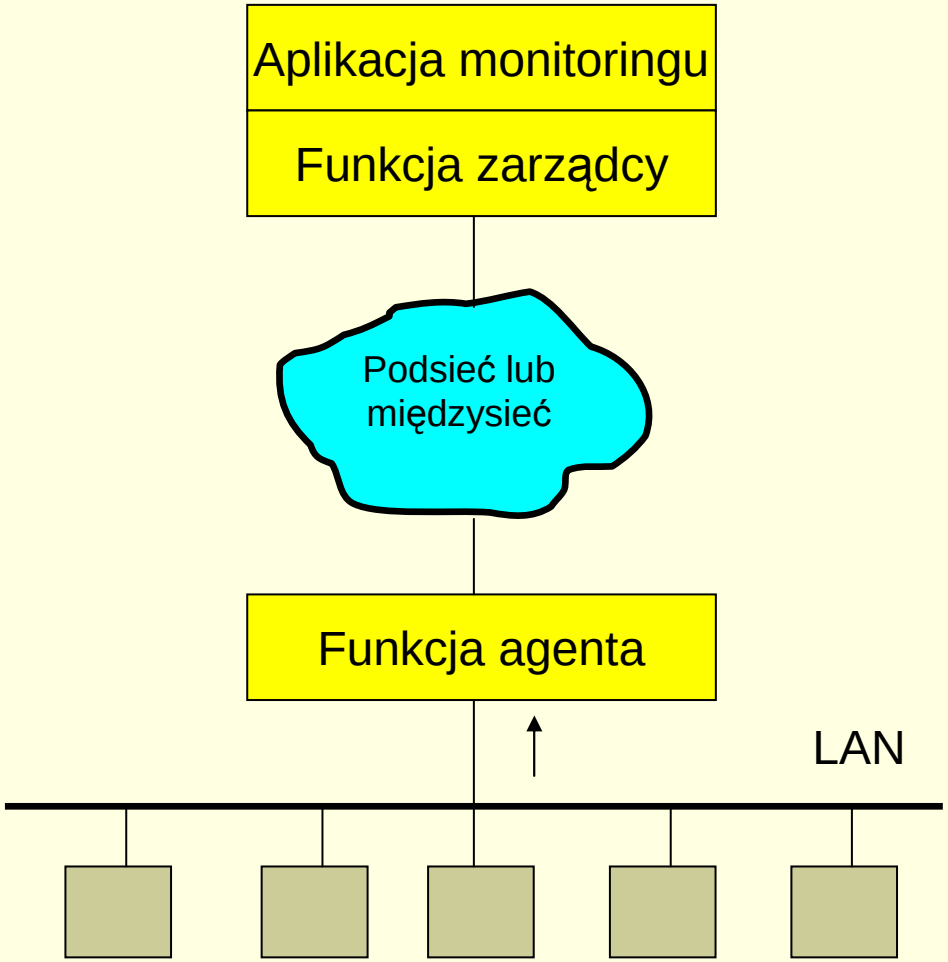
Zasoby w systemie agenta



Zewnętrzny nadzorca



Agent proxy nadzorcy



Odpytywanie i raportowanie zdarzeń

Informacje wykorzystywane przy monitorowaniu sieci są zbierane i udostępniane jednemu lub kilku systemom zarządzania

Używane są dwie techniki udostępniania zarządcy informacji pochodzących od agenta:

- Odpytywanie
- Raportowanie zdarzeń

Odpytywanie

- Odpytywanie *(Polling)* - jest współdziałaniem zarządcy z agentem na zasadzie pytanie – odpowiedź.
- Zarządca może pytać każdego agenta (do którego posiada uprawnienia) o wartości różnych elementów informacji.
- Agent odpowiada informacjami z własnej bazy MIB.

Raportowanie zdarzeń

- Raportowanie zdarzeń *(Event Reporting)* – tu inicjatywa należy do agenta, a zarządca pełni rolę nasłuchującego, czekając na nadchodzące informacje.
- Agent może generować raporty regularnie aby przedstawić zarządcy swój aktualny stan.
- Agent może także generować raport, kiedy wystąpi jakieś ważne wydarzenie (np.. zmiana stanu) lub niezwyczajne zdarzenie (np..awaria)

Wybór metody zależy od:

- Ilości ruchu sieciowego generowanego przez każdą z metod,
- Odporności w sytuacjach krytycznych,
- Opóźnienia czasowego przy powiadamianiu zarządcy sieci,
- Stopnia przetwarzania w zarządzanych urządzeniach,
- Wyboru między pewnymi i niepewnymi metodami wymiany danych,
- Rodzaju stosowanych aplikacji nadzorczych,
- Wymaganych w przypadku uszkodzenia urządzeń środków zaradczych (zanim zdąży ono wysłać raport)

Monitorowanie sieci

(w oparciu o „Protokoły SNMP i RMON” W. Stallings)

Monitorowanie wydajności

Wskaźniki wydajności sieci

- Zorientowane na usługi
  - Dostępność,
  - Czas odpowiedzi,
  - Dokładność,
- Zorientowane na wydajność
  - Przepustowość,
  - Wykorzystanie,

Wskaźniki wydajności sieci

(Zorientowane na usługi)

- ***Dostępność*** – procent czasu przez który dany system, komponent czy aplikacja są dostępne dla użytkownika.
- ***Czas odpowiedzi*** – ilość czasu upływająca od momentu wydania polecenia przez użytkownika do chwili pojawienia się odpowiedzi na terminalu.
- ***Dokładność*** – procent czasu w którym nie wystąpiły błędy w transmisji ani w dostarczaniu informacji.

Wskaźniki wydajności sieci
(Zorientowane na wydajność)

- ***Przepustowość*** – Częstość występowania zdarzeń powiązanych z aplikacją (np. przesłanie komunikatów, transfer plików).

- ***Wykorzystanie*** – procent wykorzystania teoretycznej pojemności zasobu (np. multipleksera, linii przesyłowej, przełącznika).

Problemy wyboru i wykorzystania wskaźników

- Używanie zbyt wielu wskaźników,
- Niedostateczne rozumienie znaczenia wszystkich wskaźników,
- Udostępnianie i wspieranie niektórych wskaźników jedynie przez część protokołów,
- Niedostosowanie większości wskaźników do porównania ich z innymi,
- Niepoprawna interpretacja wskaźników (przy dokładnym pomiarze),
- Zbyt czasochłonne obliczanie wskaźników, utrudniające wykorzystanie końcowego wyniku do kontrolowania otoczenia,

Dostępność

- ***Dostępność (Availability)*** – określa jaki procent czasu może być udostępniony użytkownikowi przez system sieciowy, komponent lub aplikację.
  Dostępność systemu zależy od dostępności poszczególnych komponentów i dodatkowo od organizacji systemu.

Dostępność jest oparta na niezawodności poszczególnych komponentów sieci.

Awaryjność komponentu

- Awaryjność komponentu jest wyrażana wzorem:

$$A = \frac{MTBF}{MTBF + MTTR}$$

- Gdzie:
  MTBF – średni czas między uszkodzeniami,
  MTTR – średni czas naprawy,

Czas odpowiedzi

- ***Czas odpowiedzi (Response Time)*** – jest to czas jakiego potrzebuje system, aby zareagować na dane żądanie.

  W przypadku transakcji interaktywnej, jest to czas między ostatnim uderzeniem w klawisz przez użytkownika a chwilą rozpoczęcia wyświetlania wyniku na ekranie.

Składowe czasu odpowiedzi

- Wejściowe opóźnienie stacji roboczej,
- Wejściowy czas oczekiwania w kolejce,
- Wejściowy czas obsługi,
- Opóźnienie procesora
- Wyjściowy czas kolejkowania,
- Wyjściowy czas obsługi,
- Wyjściowe opóźnienie stacji roboczej,

Wejściowe opóźnienie stacji roboczej

- ***Wejściowe opóźnienie stacji roboczej*** – opóźnienie powstające podczas przesyłania pytania z terminala do linii komunikacyjnej.
- Najczęściej opóźnienie w samym terminalu jest niezauważalne i zależy bezpośrednio od szybkości transmisji od terminala do kontrolera.

  Dla szybkości 2400b/s wynosi 3,33 ms/znak.

Wejściowy czas oczekiwania w kolejce

- ***Wejściowy czas oczekiwania w kolejce*** – czas potrzebny na przetworzenie wiadomości przez kontroler. Kontroler obsługuje informacje przychodzące z wielu terminali oraz dane z sieci przeznaczone dla nich. Nadchodząca wiadomość zostanie umieszczona w buforze i obsłużona gdy nadejdzie jej kolej. Tak więc im bardziej obciążony kontroler, tym dłuższy czas przetwarzania.

Wejściowy czas obsługi

- ***Wejściowy czas obsługi*** – czas potrzebny na przesyłanie danych od komputera poprzez łącze komunikacyjne, sieć lub inne obiekty komunikacyjne do procesora *Front – End* hosta.

Opóźnienie procesora

- ***Opóźnienie procesora*** – czas który procesor *front – end,* procesor hosta, sterowniki dysków i tym podobne urządzenia poświęcają na przygotowanie w centralnym komputerze odpowiedzi na zadanie pytanie.

  Składnik ten zwykle jest poza kontrolą zarządcy sieci.

Wyjściowy czas kolejkowania

- ***Wyjściowy czas kolejkowania*** – czas jaki odpowiedź spędza na wyjściu hosta w oczekiwaniu na wysłanie do sieci lub linii komunikacyjnej.

  Opóźnienie jest tym większe im większa liczba odpowiedzi czekających na obsłużenie.

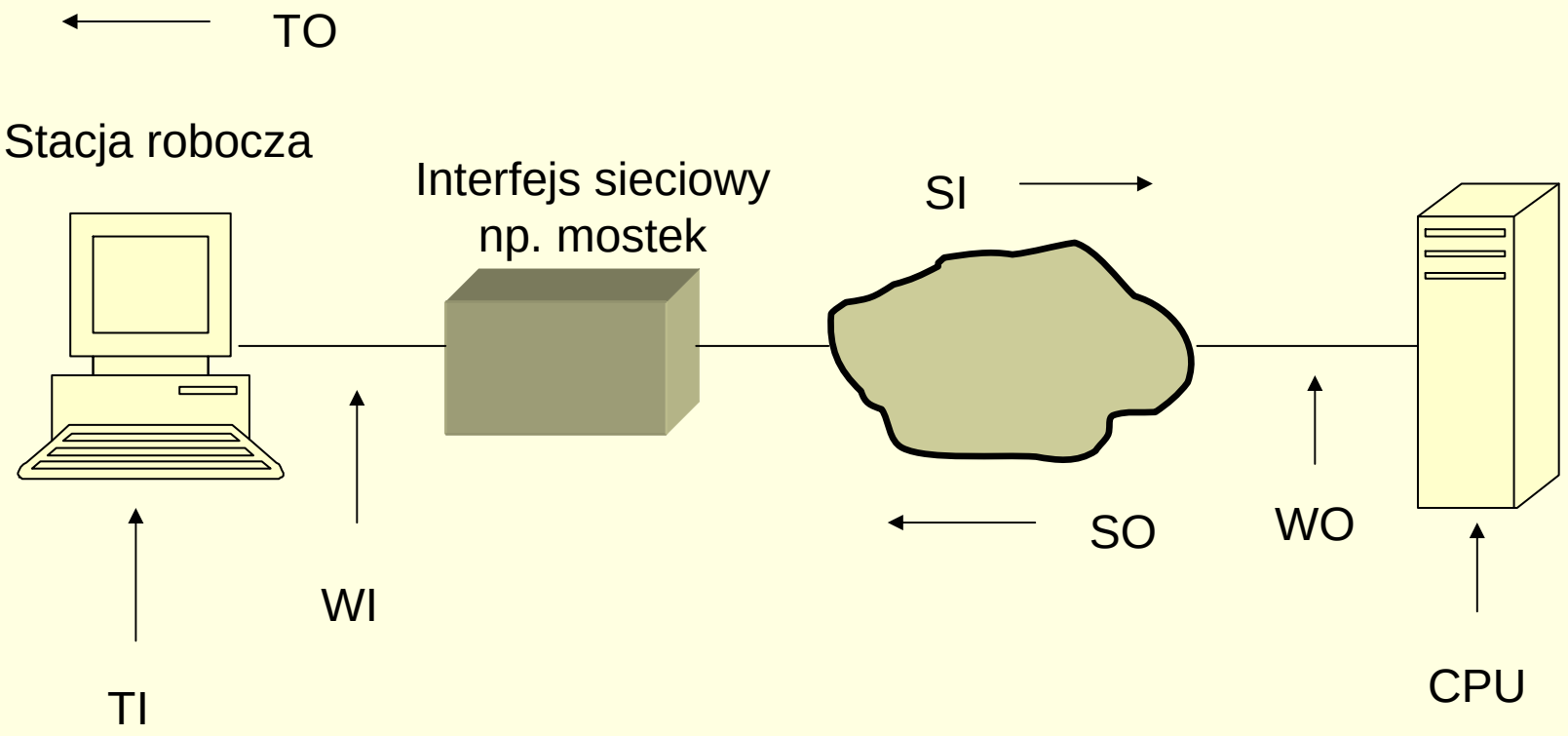
Wyjściowy czas obsługi

- ***Wyjściowy czas obsługi*** – czas potrzebny na przesłanie danych urządzeniem komunikacyjnym od procesora typu *front – end* hosta do kontrolera.

Wyjściowe opóźnienie stacji roboczej

- ***Wyjściowe opóźnienie stacji roboczej*** – opóźnienie w samym terminalu. Podobnie jak w przypadku *wejściowego opóźnienia stacji roboczej* zależy ono głównie od prędkości linii.

Składowe czasu odpowiedzi



RT=TI+WI+SI+CPU+WO+SO+TO

Transakcje

- Transakcję można podzielić na dwa etapy:
  - ***Czas odpowiedzi użytkownika (User Response Time)*** – czas pomiędzy momentem gdy użytkownik otrzyma kompletną odpowiedź na jedno polecenie, a chwilą gdy wprowadzi kolejne; tzw. *czas namysłu,*
  - ***Czas odpowiedzi systemu (System Response Time)*** – czas pomiędzy chwilą, gdy użytkownik wprowadzi polecenie a momentem gdy cała odpowiedź pojawi się na terminalu,

Koszty czasu odpowiedzi

- ***Moc przetwarzania komputera (Computer Processing Power)*** – im szybszy komputer, tym krótszy czas odpowiedzi, ale wzrost mocy komputera oznacza wzrost kosztów.
- ***Wymagania współzależności (Computing Requirements)*** – zapewnienie szybszego czasu odpowiedzi jednym procesom może pogorszyć czas odpowiedzi w innych procesach.

Koszt pracy

- Transakcja składa się z rozkazu użytkownika wydanego z terminala oraz odpowiedzi systemu.
- Gdy maleje czas odpowiedzi systemu, maleje też czas odpowiedzi użytkownika.
- Najlepsze wyniki uzyskuje się gdy ani komputer ani użytkownik nie czekają na siebie; tzn. wydajność wzrasta a koszt pracy maleje.

Czas

- Czas odpowiedzi powinien być dobierany w zależności od kosztów jego uzyskania.

Dokładność

- Chociaż protokoły takie jak łącza danych czy transportowe mają wbudowane mechanizmy korekcji błędów, przydatne jest monitorowanie ilości błędów które trzeba było skorygować.
- Duży wskaźnik błędów wskazuje na uszkodzenia linii, istnienie źródła szumów lub interferencji które należy wyeliminować.

Przepustowość

- ***Przepustowość (Throughput)*** – jest pomiarem dotyczącym aplikacji np.:
  - liczba transakcji danego typu w określonym przedziale czasu,
  - liczba sesji klienta z daną aplikacją w danym przedziale czasu,
  - liczba odwołań klienta do środowiska z komutacją pakietów,

Wykorzystanie

- ***Wykorzystanie (Utilization)*** – jest pomiarem dokładniejszym niż przepustowość. Odnosi się ono do określenia procentu czasu, w jakim dany zasób jest wykorzystywany w przeciągu określonego przedziału czasu.
- Najważniejszym zastosowaniem **wykorzystania** jest poszukiwanie potencjalnych zatorów i obszarów przeciążenia.

Monitorowanie wydajności

- Monitorowanie wydajności obejmuje trzy składniki:
  - *pomiar wydajności* – czyli rzeczywistego gromadzenia statystyk o ruchu i czasach jego realizacji,
  - *analizę wydajności* – oprogramowania do redukowania i prezentowania danych,
  - *sztuczne wytwarzanie ruchu* – które pozwala na obserwowanie sieci przy kontrolowanym obciążeniu.

Pomiar wydajności

- Pomiar wydajności jest częściowo realizowany poprzez moduły agenckie wewnątrz urządzeń sieciowych (hostów, routerów, mostów, itp.).
- We współdzielonej sieci, takiej jak LAN, większość potrzebnych informacji może być zbierana przez zewnętrznego lub zdalnego nadzorcę, który po prostu obserwuje ruch w sieci.

Typowe pomiary w sieci LAN dotyczące błędów i nieefektywności

- Czy ruch wywołany przez poszczególnych użytkowników jest w miarę równomierny, czy może istnieją szczególne pary nadawca-odbiorca powodujące niezwykle duże obciążenie?
- Jaki jest udział procentowy poszczególnych typów pakietów? Czy pakiety któregoś typu pojawiają się ze zbyt dużą częstotliwością, co sygnalizowałoby błąd lub niesprawność protokołu?

Typowe pomiary w sieci LAN dotyczące błędów i nieefektywności c.d.

- Jaki jest rozmiar pakietów danych?
- Jaki jest rozkład czasów przejmowania kanałów i opóźnień komunikacyjnych? Czy czasy te nie są zbyt długie?
- Czy współczynniki kolizji przy transmitowaniu pakietów wskazują na uszkodzenie sprzętu lub wadliwy protokół?
- Jakie jest wykorzystanie kanałów i przepustowość?

Typowe pomiary w sieci LAN dotyczące obciążenia i ruchu

- Jaki jest wpływ obciążenia ruchu na wykorzystanie, przepustowość i czasy opóźnień?
  Jaki poziom obciążenia powoduje obniżenie wydajności systemu?
- Jaka jest maksymalna pojemność kanału w normalnych warunkach działania?
  Ilu aktywnych użytkowników potrzeba aby osiągnąć to maksimum?

Typowe pomiary w sieci LAN dotyczące obciążenia i ruchu c.d.

- Czy większe pakiety zwiększą lub zmniejszą przepustowość i opóźnienia?
- Jak na wykorzystanie i opóźnienia wpływają pakiety o stałych rozmiarach?

Monitorowanie uszkodzeń

- Celem monitorowania uszkodzeń jest jak najszybsze wykrywanie ich wystąpienia oraz identyfikowanie przyczyn tych błędów, tak aby mogły być podjęte odpowiednie działania naprawcze.

Problemy przy monitorowaniu uszkodzeń

- ***Uszkodzenia nieobserwowalne*** – pewne uszkodzenia są w naturalny sposób niemożliwe do zauważenia lokalnie. Na przykład niemożliwe jest lokalne stwierdzenie sytuacji *zakleszczenia (Deadlock)* między współpracującymi procesami rozproszonymi. Niektóre uszkodzenia mogą być nieobserwowalne ponieważ producent nie wyposażył danego sprzętu w odpowiednie mechanizmy wykrywające dany błąd.

Problemy przy monitorowaniu uszkodzeń c.d.

- ***Uszkodzenia częściowo obserwowalne*** – uszkodzenie węzła jest możliwe zaobserwowania, ale obserwacja może być niewystarczająca do dokładnego wskazania problemu. Na przykład węzeł może przestać odpowiadać na skutek uszkodzenia niskopoziomowego protokołu w przyłączonym urządzeniu.

Problemy przy monitorowaniu uszkodzeń c.d.

- ***Niepewność obserwacji*** – nawet jeżeli możliwe są szczegółowe obserwacje uszkodzeń, to mogą być one nie pewne lub nawet niekonsekwentne.
  Na przykład brak odpowiedzi od zdalnego urządzenia może oznaczać, że urządzenie to jest zblokowane, nastąpiło rozdzielenie sieci, opóźnienie odpowiedzi spowodował zator lub uszkodzony jest lokalny zegar.

Lokalizacja uszkodzenia

- Po zaobserwowaniu uszkodzenia konieczne jest ustalenie konkretnego komponentu odpowiedzialnego za jego powstanie. Przy lokalizacji konkretnego komponentu mogą powstać problemy typu:
  - *różnorodne potencjalne przyczyny,*
  - *zbyt wiele powiązanych obserwacji,*
  - *interferencja między diagnozą a lokalnymi procedurami naprawczymi,*
  - *brak narzędzi automatycznego testowania,*

Różnorodne potencjalne przyczyny

- Gdy wykorzystuje się różnorodne technologie, rośnie liczba potencjalnych miejsc i rodzajów uszkodzeń. Utrudnia to lokalizację źródła uszkodzenia.

Zbyt wiele powiązanych obserwacji

- Pojedyncze uszkodzenie może dotykać wielu aktywnych tras komunikacyjnych.
- Ponieważ pojedyncze uszkodzenie może generować wiele uszkodzeń pochodnych, rozpowszechnianie i nawarstwianie się informacji o uszkodzeniach, które powstają w ten sposób może przesłonić właściwą przyczynę problemu.

Interferencja między diagnozą a lokalnymi procedurami naprawczymi

- Lokalne procedury naprawcze mogą zniszczyć ważne dowody dotyczące natury uszkodzenia, uniemożliwiając właściwą diagnozę.

Brak narzędzi automatycznego testowania

- Testowanie w celu wyizolowania uszkodzeń jest trudne i kosztowne w administraci.

Funkcje monitorowania uszkodzeń

- Pierwszym wymaganiem stawianym systemowi monitorowania uszkodzeń jest zapewnienie możliwości wykrywania i raportowania uszkodzeń.
- W najgorszym przypadku agent monitorowania uszkodzeń będzie przechowywał dzienniki znaczących zdarzeń i błędów.

Dodatkowe możliwości

- Poza zgłaszaniem znanych i istniejących błędów, dobry system monitoringu uszkodzeń może je przewidywać.
- System monitorowania uszkodzeń powinien także pomagać izolować i rozpoznawać uszkodzenia.

Typowe testy systemu monitorowania

- test łączności,
- test integralności danych,
- test integralności protokołu,
- test nasycenia danych,
- test nasycenia połączenia,
- test czasu odpowiedzi,
- test pętli zwrotnej,
- test funkcjonalny,
- test diagnostyczny,

Monitorowanie wykorzystania *(Accounting Monitoring)*

- Monitorowanie wykorzystania dotyczy głównie śledzenia sposobu wykorzystania zasobów sieciowych przez użytkowników.
  - Jaką częścią kosztów należy obciążyć różne działy,
  - Podzielenie kosztów na poszczególne projekty i konta,
  - Obciążyć użytkowników zewnętrznych kosztami wykorzystania zasobów,

Zasoby poddawane monitorowaniu wykorzystania

- ***Urządzenia komunikacyjne*** – sieci LAN, WAN, łącza dzierżawione, łącza komutowane, systemy prywatnych central PBX,
- ***Sprzęt komputerowy*** – stacje robocze i serwery,
- ***Systemy i oprogramowanie*** – aplikacje oraz oprogramowanie narzędziowe,
- ***Usługi*** – wszystkie dostępne usługi komunikacyjne i informacyjne,

Informacje o wykorzystaniu

- Dla każdego użytkownika mogą być gromadzone i oraz przechowywane dane dotyczące wykorzystania zasobów komunikacyjnych.

Typowe typy zasobów

- W zależności od danej organizacji informacje zbierane są dla różnych typów zasobów np.
  - *identyfikacja użytkownika,*
  - *odbiorca,*
  - *liczba pakietów,*
  - *poziom bezpieczeństwa,*
  - *znaczniki czasu,*
  - *kody stanu sieci,*
  - *używane zasoby*

Monitorowanie sieci

Podsumowanie

Monitorowanie sieci

- Monitorowanie sieci jest najbardziej fundamentalnym aspektem zautomatyzowanego zarządzania siecią.
- Celem monitoringu sieci jest zbieranie informacji o stanie i zachowaniu elementów sieciowych.
  - *informacje statyczne,*
  - *informacje dynamiczne,*
  - *informacje statystyczne,*

Monitorowanie uszkodzeń

- Celem monitorowania uszkodzeń jest jak najszybsze wykrywanie ich wystąpienia oraz identyfikowanie przyczyn ich wystąpienia tak aby mogły być podjęte odpowiednie działania naprawcze.

Monitorowanie wykorzystania

- Monitorowanie zasobów wykorzystania sieci dotyczy zbierania informacji o jej wykorzystaniu na poziomie szczegółowości wymaganym dla poprawnego oszacowania kosztów.

Najważniejsze informacje zarządzania

- Dostępność,
- Czas odpowiedzi,
- Dokładność,
- Przepustowość,
- Wykorzystanie,