ZESZYTY NAUKOWE POLITECHNIKI ŚLĄSKIEJ 1999
Seria: INFORMATYKA z. 36 Nr kol. 1414

Robert ZBYSIŃSKI
OPTIMUS S.A. Dział Integracji, Warszawa

ANALIZA I OPTYMALIZACJA OBCIĄŻENIA SIECI

Streszczenie. Przedstawione poniżej rozważania zawierają analizę i metody optymalizacji mechanizmów generujących obciążenie sieci lokalnych i rozległych. Analiza dotyczy sieci opartych na MS Windows NT Serwer używających do transmisji protokołu TCP/IP. Wybór ten jest spowodowany faktem, iż tak TCP/IP, jak i MS Windows występują w większości obecnie pracujących sieci.

THE ANALYSIS AND OBTAINING OPTIMUM OF NETWORK TRAFFIC CAPACITY

Summary. The following article contains the analysis and methods of obtaining the best results in mechanisms causing the LAN/WAN traffic. The analysis concerns the networks based on MS Windows NT Server that uses TCP/IP protocol for transmission. This choice is determined by the fact of using both TCP/IP and MS Windows in majority of presently active networks.

1. Analiza ruchu związanego z dynamicznym przydzielaniem adresu protokołu DHCP

W sieciach typu Internet pierwszą rzeczą, jaką stacja robocza musi zrobić, jest inicjalizacja protokołu TCP/IP. Najpierw należy nadać stacji adres i maskę podsieci. Adresy te mogą być skonfigurowane manualnie przez administratora albo przypisane automatycznie przy użyciu protokołu DHCP. Gdy rozpatrujemy ruch w sieci na przestrzeni długiego czasu (kilkanaście godzin i więcej), to udział ruchu związanego z protokołem DHCP nie jest znaczny. Jeżeli jednak ograniczymy okres rozpatrywania do kilkudziesięciu minut tuż po rozpoczęciu pracy przez użytkowników, to ruch ten staje się dość istotnym czynnikiem obciążenia sieci. Protokół DHCP generuje ruch tylko w momencie przydzielania adresu IP i odnowienia adresu IP.

1.1. Ramka protokołu DHCP

W czasie inicjalizacji protokołu DHCP pierwszą rzeczą, jaką musi zrobić klient, jest zdobycie adresu IP przy pomocy tego protokołu. Sprowadza się to do konwersacji pomiędzy klientem a serwerem DHCP. W procesie tym generowane są cztery pakiety (tabela 1) każdy po 342 bajty. Czas generacji tych ramek trwa około ¼ sekundy.

Tabela 1

Pakiety generowane w czasie nadawania adresu IP przy użyciu protokołu DHCP

Pakiet	Opis
DHCP Discover	Pierwsza ramka, kiedy komputer klienta wysyła *broadcast DHCP Discover* w celu zlokalizowania serwera DHCP. Klient nie ma żadnej wiedzy o jakichkolwiek serwerach DHCP i dlatego musi wysłać pakiet typu *broadcast*, aby taki serwer odnaleźć.
DHCP Offer	Gdy serwer DHCP odbierze pakiet *DHCP Discover* i zdecyduje, że może go obsłużyć, odpowiada pakietem *DHCP Offer* podającym adres, jaki klient może otrzymać.
DHCP Request	Klient odbiera pakiet *DHCP Offer* i po zaakceptowaniu adresu wysyła pakiet *DHCP Reguest* do serwera DHCP z potwierdzeniem przyjęcia zaproponowanego adresu.
DHCP ACK	Gdy serwer otrzyma *DHCP Request*, odpowiada pakietem *DHCP ACK* zawierającym czas użyczenia adresu oraz opcjonalnie inne parametry TCP/IP.

1.2. Odnowienie użyczenia adresu

Ilekroć klient DHCP jest restartowany, musi odnowić adres na serwerze DHCP. Podczas odnawiania adresu IP na serwerze DHCP konwersacja jest prostsza, gdyż ogranicza się do dwóch ostatnich pakietów, czyli fazy przydzielania adresu. Komputer klienta żąda pakietem *DHCP Request* odnowienia swojego aktualnego adresu i w przypadku pozytywnej weryfikacji serwer DHCP odpowiada Pakietem *DHCP ACK*.

Klient DHCP odnawia swój adres IP w połowie okresu użyczenia adresu; okres ten jest konfigurowalny. W tym czasie klient wysyła pakiet *DHCP Request* do serwera DHCP, a serwer odpowiada pakietem *DHCP ACK*, gdy zdecyduje, że klient może nadal używać tego adresu. Różnica pomiędzy pakietami *Request* i *ACK* w czasie odnawiania i w czasie pierwszego pobierania jest taka, że konwersacja jest punktowa (dla odnawiania), a nie *broadcast-owa* (jak dla pierwszego pobierania adresu), gdyż serwer i klient wiedzą o swoim istnieniu. Te dwie ramki generują 684 bajty w czasie około 50 milisekund.

2. Analiza ruchu w sieci podczas procesu logowania

Jedną z pierwszych funkcji, jaką użytkownik wykonuje w sieci, jest weryfikacja w czasie logowania. Jest ona wykonywana przez kontrolery domeny, do której należy użytkownik.

2.1. Znajdowanie serwera logowania

Pierwszą czynnością wykonywaną w trakcie procesu logowania jest poszukiwanie kontrolera domeny w celu weryfikacji konta użytkownika. Realizowane jest to następującymi metodami:

- zapytanie do usługi WINS o wszystkie zarejestrowane kontrolery domeny w domenie,
- wysłanie *broadcast-u* z zapytaniem do *Mail Slotu Netlogon*.

Ramka ta ma długość około 260 bajtów w zależności od długości nazwy komputera. Każdy serwer zarejestrowany w domenie, na którym jest uruchomiona usługa *NetLogon*, będzie odpowiadał klientom, a więc może przyjąć zapytanie logowania. Odpowiedź do pytającego komputera poprzez *mailslot\mailslot\temp\netlogon*.

Ramka ta ma długość około 230 bajtów w zależności od długości nazwy komputera.

2.2. Weryfikacja żądania logowania

Następnie w procesie logowania komputer klienta otrzymuje pierwszą odpowiedź i zaczyna się następujący ruch w sieci:

- Klient odnajduje nazwę wybranego serwera logowania (używając albo zapytania do WINS, albo przy użyciu *broadcast-ów*).
- W procesie *Handshake* zostaje nawiązana sesja TCP z serwerem logowania.
- Zostaje nawiązana sesja *NetBios* z serwerem logowania.
- Następuje negocjacja protokołu SMB.
- Zostaje nawiązane połączenie z "Serwerlogowania".
- Powyższy proces generuje 11 ramek o łącznej długości około 1280 bajtów.
- Na koniec klient rozpoczyna konwersacje z serwerem logowania przy pomocy zdalnych zapytań typu API w celu zweryfikowania logowania.
- Pierwsze zapytanie typu API (nazywane *NetWkstaUserLogon)* żąda potwierdzenia poprawności logowania.
- Drugie zapytanie API (*NetRemoteTOD*) pobiera informacje z serwera dotyczące czasu na serwerze w celu ustalenia strefy czasowej, daty plików i stempli czasowych. Wtedy serwer odpowiada właściwą godziną zgodną z godziną na kontrolerze domeny.

Proces ten (dwa zapytania API i dwie odpowiedzi) generuje cztery ramki, razem 765 bajtów.

Zaraz po uwiarygodnieniu użytkownika następują procesy: login skrypty, profile użytkownika i ustawienia systemowe. Oznacza to oczywiście ruch w sieci, np. zalogowanie użytkownika z Win95 do domeny generuje 35 dodatkowych ramek na: nawiązanie sesji z kontrolerem domeny, podłączenie do zasobu NETLOGON, wykonanie skryptu logowania i ustawienie polityki systemu. Proces ten nie tylko wygeneruje ruch w sieci, ale także wydłuży proces logowania o kilka sekund.

W końcu następuje zerwanie połączenia IPC$, a sesje NetBIOS i TCP zostają utrzymane. Wygeneruje to ruch około 360 bajtów.

3. Analiza obciążenia spowodowanego działaniem *browsera*

Po tym jak użytkownik zostanie zalogowany, zaczyna sięgać do zasobów sieci. W sieciach Microsoftu do przeglądania zasobów sieci używany jest mechanizm nazywany *browserem.*

3.1. Właściwości pakietów browsera

Browser w większości opiera swoje działanie na ramkach typu broadcast. Ramki mają rozmiar pomiędzy 200 a 300 bajtów – są to *broadcast-y* z warstwy MAC i IP.

3.2. Rodzaje ruchu związanego z browserem

Usługa *browser* generuje bardzo dużo ruchu w sieci. Ma to wpływ na przepustowość sieci, a z drugiej strony jest dużym ułatwieniem dla użytkowników przeszukujących zasoby sieci. Usługę *browser* realizuje serwer nazywany *Master Browser-em,* na którym to serwerze klienci dodawani są do listy *browsera. Master Browser-y* muszą komunikować się między sobą, aby użytkownicy mogli widzieć zasoby innych domen w sieci. *Backup (zapasowy) Browser* musi uaktualniać listę z *Master Browsera* w celu zapewnienia możliwie aktualnej listy klientom. Klienci muszą wiedzieć, które z serwerów są *Master,* a które *Backup Browser-ami.* Cały ten proces generuje ruch w sieci.

3.2.1. Ogłaszanie obecności stacji w sieci

Stacja, która chce udostępniać swoje zasoby w sieci, będzie ogłaszać swoją obecność co 12 minut, oczywiście w czasie inicjalizacji ogłaszanie będzie następować znacznie częściej w

celu zapewnienia wpisu na listę przeglądania (*browse list*). Takie rozgłoszenie generuje około 243 bajty obciążenia.

3.2.2. Przeszukiwanie listy przeglądania (Browse List)

Zaraz po tym, jak klient zgłosi swoją obecność, użytkownik może zażądać połączenia do udostępnianych w sieci zasobów. Aby to zrobić, stacja musi przeszukać listę dostępnych zasobów. Proces ten wymaga odnalezienia lokalnego *Master Browser-a* w celu wyszukania listy *Backup Browser-ów*, połączenia z *Backup Browser-em* i przeszukania listy (*Browse List*) na nim się znajdującej.

Aby znaleźć lokalny *Master Browser*, klient wysyła zapytanie (*Get Backup List Request*) do domeny. Zapytanie to ma rozmiar około 215 bajtów. Lokalny *Master Browser* odpowiada na „*Get Backup List Request*" listą dostępnych *Backup Browserów*. Ramki te mają bardzo różny rozmiar. Lista dwu serwerów ma rozmiar 234 bajtów. Następnie klient podłącza się do jednego z backup browserów z listy i przeszukuje listę przeszukiwań (*Browse List*). Cały ten proces generuje 19 ramek, razem 2150 bajtów. Opis generowanego ruchu przedstawia tabela 2.

Tabela 2

Pakiety generowane w procesie przeszukiwania sieci

Rodzaj obciążenia	Opis
Proces ogłaszania	W procesie ogłaszania rozsyłanych jest wiele różnych pakietów, a usługa *Browser* generuje wiele różnorodnych wiadomości ogłaszanych. Komputery z uruchomionymi usługami serwera będą zgłaszać swoją obecność do *Master Browser-a* ich domeny. Jest to realizowane przez ogłaszanie stacji i ma na celu poinformowanie sieci o zasobach udostępnionych przez stację. Zaraz po tym, jak stacja *Browser-a* zostanie uruchomiona, musi ustalić, kto jest *Master Browser*-em jego domeny. Realizuje to żądaniem ogłoszenia. Żądanie ogłoszenia używane jest także do wymuszenia ogłaszania stacji, gdy nowy *Master Browser* rozpoczyna pracę. *Master Browser* odpowiada na ogłoszenia informacją o lokalnym *Master Browse-rze*. Gdy *Master Browser* zostanie wybrany, musi on ogłosić siebie jako *Master Browser-a* domeny. Robi to przy pomocy ogłoszenia grupowego (Workgroup Announcment). W ten sposób *Master Browser* dowiaduje się o innych *Master Browser-ach* w sieci lokalnej.
Wybór *Browsera*	W przypadku gdy nie można znaleźć *Master Browser-a*, komputer, który pierwszy odkrył brak *Master Browser-a*, inicjalizuje proces wyboru w celu wypromowania nowego *Master Browser-a*. W procesie promowania stacja inicjująca wybór *Browser-a* wysyła ramkę wyborczą informującą o rozpoczęciu wyboru, zawierającą dodatkowo informacje o kryteriach wyboru. Wszystkie stacje w sieci odbierają ramkę elekcyjną, analizują ją i stacja o wyższym statusie wg kryteriów wyborów

	wysyła ramkę elekcyjną zawierającą jej parametry elekcyjne. Ostatecznie komputer o najwyższych parametrach wyborów wygrywa elekcję i zostaje *Master Browser-em*.
Przeglądanie międzysieciowe	Często użytkownicy potrzebują sięgnąć do zasobów z innej sieci. Aby to umożliwić, każda domena posiada *Master Browser* dla każdej podsieci. *Browser-y* te synchronizują wzajemnie swoje listy przeglądania (*browse list*) co 15 minut. Efekt tej synchronizacji jest widoczny dla klientów za pośrednictwem *Backup Browser-ów*.
Zapytania *Browsera*	Kiedy klient próbuje wyświetlić listę zasobów sieciowych, lista ta jest pobierana z *Backup Browser-a*. Aby znaleźć *Backup Browser-a*, klient musi wysłać zapytanie "Get Backup List Request" do *Master Browser-a*. Tam klient odnajduje na liście *Backup Browser*, nawiązuje z nim sesję i odczytuje listę przeszukiwań (*browse list*).

4. Analiza obciążenia generowanego przez sesje plikowe

Jednym z nadrzędnych celów analizy i optymalizacji obciążenia jest zapewnienie większej przepustowości w transferze plików, drukowaniu i uruchamianiu aplikacji. Każda aplikacja generuje specyficzne obciążenie. W przypadku transferu plików część transmisji jest bardzo podobna. Z tego też powodu może być ona łatwo mierzona i analizowana. W tabeli 3 przedstawiono rodzaje ruchu towarzyszącego sesjom plikowym.

Tabela 3

Pakiety generowane w czasie sesji plikowych

Element sesji plikowej	Opis
Konwersja Adresu IP	Ruch generowany przez klienta próbującego konwertować adres IP na adres sprzętowy. Konwersja adresu IP generuje dwie 60-bajtowe ramki.
Ustanowienie sesji TCP	W czasie ustanawiania sesji TCP pomiędzy klientem a serwerem generowane są trzy ramki po 60 bajtów każda.
Ustanowienie sesji NetBIOS	Ustanowienie sesji NetBios pomiędzy serwerem a klientem generuje dwie ramki łącznej długości 186 bajtów.
Negocjacja protokołu SMB	Negocjacja protokołu SMB ma na celu ustalenie, jakie komendy SMB mogą być użyte. Generowane są dwie ramki o rozmiarze pomiędzy 300 a 400 bajtów w zależności od poziomu SMB i systemu operacyjnego na pracującego na stacji klienta.
Połączenie	Podłączenie do konkretnego udostępnionego zasobu generuje dwie ramki o długości około 350 bajtów.
Rozłączenie sesji	Zakończenie sesji generuje dwie 93-bajtowe ramki.

Ustanowienie sesji i zestawienie połączenia z plikiem generuje 11 ramek o łącznej długości 1000 bajtów. Od momentu rozpoczęcia sesji i nawiązania połączenia (z plikami) ruch w sieci zależy od typu (rozmiaru) pliku i używanej aplikacji.

5. Analiza ruchu związanego z synchronizacją kont

W sieciach opartych na Microsoft Windows NT weryfikacja logowania użytkownika jest realizowana przez PDC (Primary Domain Controller) lub BDC (Backup Domain Controller). Przeważnie weryfikacji dokonuje BDC, gdyż BDC jest zwykle mniej obciążony, więc odpowiada szybciej niż PDC.

Aby BDC mógł w sposób właściwy uwierzytelnić logowanie użytkownika, ważne jest, aby BDC dysponował dokładną i aktualną kopią bazy klientów znajdującej się na PDC. Synchronizacją tych baz zajmuje się usługa NetLogon. Synchronizacja odbywa się:

- gdy BDC jest instalowany lub restartowany w domenie,
- gdy wymuszana jest w procesie administracji z poziomu *Server Manager-a*,
- gdy jest automatycznie uruchamiana przez kontrolery domeny zgodnie z zapisami w rejestrach.

5.1. Znajdowanie PRIMARY DOMAIN CONTROLLER

Po tym jak BDC zainicjalizuje swój protokół, zarejestruje się w domenie i uruchomi swoje usługi sieciowe, musi znaleźć PDC, aby uaktualnić bazę właściwości zasobów sieciowych.

5.1.1. Zapytanie o Primary Domain Controler

Aby znaleźć PDC, klient zapytuje WINS, wysyłając zapytanie o nazwę domeny. Nazwa ta jest jednoznacznie przypisana do PDC, więc serwer WINS odpowiada na to zapytanie, podając adres IP PDC. Te dwie ramki mają łączną długość 196 bajtów.

Następnie BDC wysyła komunikat „Query for PDC" do adresu wskazanego przez WINS jako właściciela nazwy NAZWADOMENY. Zapytanie to ma na celu ustalenie nazwy komputera pełniącego rolę PDC. Komunikat ten wysyłany jest do "\MAILSLOT\NET\NET-LOGON". Ramka ta ma rozmiar około 270 bajtów.

5.1.2. Odpowiedź ze strony PDC

PDC odpowiada na powyższe zapytanie ramką *„Response ToPrimary Query"*. Nazwa PDC na liście jest umieszczona jako *Primary DC Name* podobnie jak nazwa domeny. Ramka ta ma koło 275 bajtów.

Ustalenie nazwy PDC generuje cztery ramki o łącznej długości około 545 bajtów.

5.2. Weryfikacja bazy Directory Services

Gdy BDC znajdzie PDC, rozpoczyna weryfikację wersji bazy zasobów (Directory Services Database). W procesie tym nawiązuje on sesję z PDC w celu przygotowania weryfikacji i synchronizacji bazy zasobów (Directory Services Database). Generuje to 11 ramek, łącznie 1200 bajtów.

5.3. Zestawienie Secure Channel

Zanim DBC rozpocznie weryfikację, musi zestawić bezpieczny kanał transmisji z PDC. Wysyła przy tym osiem ramek o długości 1550 bajtów.

5.4. Weryfikacja bazy

Następnie wysyłane są ramki z zapytaniem RPC przekazujące do PDC numer seryjny lub wersję każdej z baz. Ramki te mają łącznie około 1344 bajtów.

5.5. Okresowe uaktualnianie bazy

Domyślnie PDC weryfikuje bazy zasobów co 5 minut, przeszukując pod kątem zmian. Kiedy zauważy zmianę, wysyła komunikat do wszystkich DBC, które powinny być poinformowane o uaktualnieniu bazy. PDC dysponuje tablicą zawierającą informacje o wszystkich BDC i wersjach ich baz. BDC, który posiada aktualną bazę, nie jest informowany o konieczności uaktualnienia.

Gdy zostanie utworzone nowe konto użytkownika w bazie kont użytkowników, PDC rejestruje tę zmianę. Od momentu, gdy ta zmiana zostanie zauważona, rozpoczyna się następujący proces:

- PDC zgłasza tę zmianę do SAM (ramka o długości około 390 bajtów).
- BDC łączy się z IPC$ na PDC.
- DBC zestawia bezpieczny kanał do PDC i weryfikuje bazę kont przy pomocy usługi Net Logon.
- DBC transportuje zaktualizowane dane przy pomocy SMB lub zapytań RPC (w zależności od rozmiaru danych).

Gdy dodajemy dwóch użytkowników, proces powyższy trwa poniżej sekundy i generuje 12 ramek o łącznej długości 4 411 bajtów. Zawierają one informacje o koncie użytkownika, takie jak: pełna nazwa, komentarz, przynależność do grup itp.

6. Analiza ruchu związanego ze związkami zaufania

Prawidłowo zaprojektowane struktury sieciowe powinny mieć scentralizowaną administrację zasobami sieci, gdzie jeden departament zajmuje się zarządzaniem zasobami sieciowymi. W środowisku MS Windows NT jest to realizowane przez utworzenie jednej domeny kont z wieloma domenami zasobów. Rozwiązanie takie wymaga ustanowienia związków zaufania pomiędzy domeną kont a domenami zasobów. W tabeli 4 przedstawiono ruch generowany w trakcie ustalania związków zaufania.

Tabela 4

Pakiety generowane w trakcie ustalania związków zaufania pomiędzy domenami

Ruch generowany przez	Opis
Przekazywanie prawa pomiędzy domenami	Domena ufająca przekazuje prawa domenie zaufanej, po czym domena zaufana potwierdza przyjęcie tych praw. Proces ten trwa około trzech sekund. W tym czasie transportowanych jest około 100 ramek o długości łącznej około 15000 bajtów.
Przekazywanie zaufanych kont	Domena ufająca importuje konta użytkowników w celu przypisaniu uprawnień do lokalnych zasobów. Proces ten trwa około dziesięciu sekund i generuje 100 ramek o długości 24 000 bajtów.
Weryfikacja zaufanego użytkownika	Gdy użytkownik z domeny zaufanej próbuje sięgnąć do zasobów domeny ufającej, musi być zweryfikowany pod kątem uprawnień. Proces ten trwa około 0,2 sekundy, generuje 20 ramek o długości 3700 bajtów.

7. Analiza ruchu związanego replikacją katalogów

Usługa replikacji katalogów realizuje automatyczną replikację drzewa katalogów pomiędzy wieloma komputerami bez interwencji administratora. Używana jest ona do replikowania *Logon Script-ów* z PDC do BDC. Dzięki temu *Logon Script* będzie wykonywany niezależnie od tego, który kontroler weryfikował użytkownika.

7.1. Replikacja

Replikacja drzewa katalogów następuje, gdy serwer eksportowy zarejestruje zmianę w replikowanym drzewie (domyślnie REPL$nazwaudostepnienia). Informuje wtedy wszystkie stacje ze swojej listy eksportowej o tym, że zawartość katalogów uległa zmianie. Ogłaszanie to ma około 340 bajtów.

Stacje importujące zestawiają połączenie SMB z serwerem eksportującym. Wysyłanych jest przy tym dziewięć ramek o długości łącznej 1286 bajtów. Następnie serwer importujący zweryfikuje katalogi używając 22 ramek o długości 3710 bajtów. Gdy okaże się, że potrzebne

jest uaktualnienie, to w tym połączeniu zostanie wykonana replikacja plików. Ruch generowany przez uaktualnianie zależy od wielkości uaktualnianych danych.

8. Optymalizacja ruchu związanego z przydzielaniem adresów DHCP

Korzystanie z DHCP nie zwiększa znacząco obciążenia sieci. Cały proces zdobywania adresu IP za pośrednictwem protokołu DHCP generuje cztery ramki 342 bajtów i przy nie obciążonej sieci nie trwa dłużej niż pół sekundy.

Komunikacja DHCP występuje w następujących przypadkach:

- gdy klient zapytuje po raz pierwszy (cztery ramki),
- podczas automatycznego uaktualnienia użyczenia, wykonywanego w połowie czasu użyczenia (standardowy czas użyczenia trwa 3 dni, czyli automatyczne odnowienie co 18 godzin); dwie ramki: zapytania DHCP i DHCP ACK trwają około 200 milisekund,
- gdy klient zostaje przeniesiony do nowej podsieci – cztery ramki jak dla nowego klienta,
- gdy zostanie wymieniona karta sieciowa na stacji klienta – cztery ramki jak dla nowego klienta
- każdorazowo, gdy klient ręcznie odnawia lub ustawia adres.

8.1. Czas użyczenia

W celu zredukowania obciążenia związanego z protokołem DHCP można zmieniać czas użyczenia adresu IP. Wykonywane jest to z poziomu *DHCP Manager-a* w opcji *Properties*. Zwiększenie czasu użyczenia z trzech dni (wartość domyślna) do na przykład 30 dni w znaczący sposób zmniejszy częstotliwość odnowień adresu DHCP. Długi czas użyczenia ma tylko wtedy sens, gdy liczba adresów przydzielanych przez DHCP jest znacznie większa od liczby stacji korzystających z DHCP. W przypadku gdy liczba stacji jest zbliżona do liczby osiągalnych adresów, zalecane jest stosowanie krótkiego czasu użyczenia.

9. Optymalizacja ruchu związanego z przesyłaniem plików

W skład ruchu związanego z transferem plików wchodzi ruch związany z zestawieniem połączenia i ruch bezpośrednio związany z transferem plików. W przypadku transferu plików ruch potrzebny na zestawienie połączenia jest niewielki, ale ruch związany z właściwym transferem plików w sposób znaczący obciąża sieć.

Proces zestawienia sesji TCP, sesji NetBIOS, negocjacji protokołu SMB generuje 10 ramek, 1169 bajtów i trwa około 238 milisekund. Proces rozłączania trwa siedem milisekund i generuje 360 bajtów w pięciu ramkach.

9.1. Sposoby optymalizacji

Nie da się wiele zrobić w kierunku zoptymalizowania ruchu związanego z zestawianiem i rozłączaniem sesji transferu plików. Prawdopodobnie najlepszym sposobem jest usunięcie nadmiarowych protokołów, aby zapytania połączeniowe nie były wysyłane przez wszystkie protokoły jednocześnie. Usunięcie protokołów zmniejszy liczbę takich pakietów w sieci.

10. Optymalizacja ruchu domenowego

Optymalizacja ruchu związanego z usługami katalogowymi dotyczy kontroli ruchu generowanego w czasie synchronizacji bazy usług katalogowych. W tym celu należy ustalić kompromis pomiędzy weryfikacją logowania użytkowników a pasmem WAN dla zdalnych użytkowników. W dużych przedsiębiorstwach (organizacjach) można zaimplementować pojedynczą domenę obejmującą wiele różnych lokalizacji. Należy pamiętać, że w takiej konfiguracji weryfikacja logowania użytkownika będzie zależna od stanu łącza WAN. W tym przypadku, aby zapewnić sprawną weryfikację logowania na wypadek utraty połączenia WAN, konieczne jest zdefiniowanie BDC w każdej odległej lokalizacji. Gdy DBC są zlokalizowane w każdej odległej lokalizacji, należy sprawdzić, czy synchronizacja kont w bazach (directory services) usług katalogowych nie zajmuje całego pasma WAN. Zajęcie całego pasma WAN na synchronizację kont spowoduje uniemożliwienie użytkownikom dostępu do zdalnych zasobów w czasie synchronizacji. Zsynchronizowanie nowo utworzonych kont dwóch użytkowników generuje 28 ramek i 5654 bajtów.

10.1. Synchronizacja baz kont przez WAN

Synchronizacja bazy *Directory Services* generuje 1kB dla każdej zmiany w bazie. Przy połączeniu 56 kb synchronizacja 30000 kont użytkowników zajmie około 24 godzin. Pomimo zastosowania mechanizmów zmniejszających konieczność częstego wykonywania pełnej synchronizacji i kontroli ruchu związanego z synchronizacją, to i tak w przypadku niepomyślnego dokonania synchronizacji przyrostowej konieczne jest wykonanie pełnej synchronizacji. Sytuacja taka może mieć miejsce w przypadku niestabilnego łącza WAN

(częściowo ukończona synchronizacja). W przypadku uaktualnienia kont obciążenie to może być mniejsze.

Należy też pamiętać, że domyślnie usługa NetLogon w przypadku nasycenia pliku rejestru zmian zaczyna kompresję tego pliku, a BDC wymusza pełną synchronizację kont.

10.2. Zarządzanie replikacją

Prawdopodobnie najczęściej modyfikowanym parametrem usługi NetLogon jest: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters\ReplicationGovernor. Parametr ten definiuje i kontroluje procent użycia pasma, jaki może usługa NetLogon wykorzystać w czasie operacji synchronizacji bazy kont. Domyślnie parametr ten ma wartość 100%, co oznacza, że w czasie synchronizacji usługa NetLogon może wykorzystać 100% przepustowości sieci. Może to mieć katastrofalne skutki, gdy jednocześnie w tym czasie użytkownicy będą próbowali korzystać z tego samego łącza WAN. Dodanie powyższego parametru i ustawienie jego wartości na 50 spowoduje obciążenie łącza WAN maksymalnie tylko w 50% transmisją związaną z synchronizacją.

Pozostałe parametry NetLogon związane z generowaniem ruchu w sieci podczas synchronizacji przedstawiono w tabeli 5.

Tabela 5

Parametry klucza "NetLogon" w rejestrach MS Windows NT

Nazwa parametru Netlogon	Opis
Pulse	Kontroluje, jak często PDC sprawdza zmiany w swojej bazie *Directory Sevices*, i wysyła je do odpowiednich BDC. Domyślnie przyjmuje wartość 5 minut i może być zwiększona do 60 minut.
PulseMaximum	Kontroluje, jak często PDC wysyła *Pulse* do wszystkich BDC, nawet jeśli posiadają one aktualną bazę. Domyślnie przyjmuje wartość 2 godziny i może być zwiększona do 24 godzin, co wydatnie zmniejszy liczbę wiadomości *Pulse*.
ChangeLogSize	Kontroluje liczbę zmian w bazie *Directory Services* potrzebnych do tego, aby zainicjować pełną synchronizację. Wartość domyślna jest 64 kB, co oznacza około 2000 zmian (zmiana to około 32 bajty). W sieci z dużą liczbą użytkowników, którzy często zmieniają hasło, bardzo łatwo osiągnąć tę wartość i wymusić pełną synchronizację. Wtedy to wzrasta ruch w sieci i wysyłanych jest do BDC znacznie więcej informacji, niż jest rzeczywiście potrzebne.

Właściwa analiza synchronizacji *Directory Services* i wdrożenie odpowiedniej techniki optymalizacyjnej mogą wydatnie zredukować ruch generowany przez synchronizację, a co za tym idzie – zwolnić więcej pasma dla użytkowników.

11. Optymalizacja ruchu związanego z *Browser-em*

Każdy komputer, na którym uruchomiona jest usługa "serwer", zgłasza swoją obecność jako jednostki przeglądającej do *Master Browser-a*. Generuje przy tym jedną 250-bajtową ramkę. Aby komputer pozostawał na liście przeglądania (browse list), operacja zgłaszania obecności jest powtarzana co 12 minut. Wyłączenie tej usługi serwera na każdym komputerze, który nie pracuje jako serwer, wyeliminuje ten ruch w sieci.

W środowisku TCP/IP w każdej podsieci znajduje się *Master Browser* dla każdej domeny. Wszystkie *Master Browser-y* danej domeny aktualizują listę przeglądania co 15 minut. Ta aktualizacja dotyczy zarówno komputerów z lokalnej domeny, ale także z innych domen ogłoszonych w innych podsieciach.

Przeszukiwanie listy przeglądania generuje sześć ramek, dwie do ustalenia listy *Backup Browser-ów* i cztery do wyszukania listy domen i serwerów.

11.1. Uaktualnianie rejestrów

Większość ruchu generowanego przez przeglądanie jest inicjowane automatycznie przez poszczególne komputery przeglądające, *Master Browser* i *Backub Browser-y*. Ruch generowany przez *Browser-y* możemy regulować za pośrednictwem dwóch parametrów w rejestrach.

Parametry te znajdziemy w rejestrach w miejscu:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Browser\Parameters.

11.1.1. MasterPeriodicity

Parametr ten definiuje, jak często *Master Browser* łączy się z *Master Browser-em* domeny. Domyślnie przyjmuje on wartość 900 sekund (15 minut), minimalna wartość to 300 sekund (5 minut), a maksymalna to 4294967295 sekund (HFFFFFFFF). Parametr ten jest typu REG_DWORD i może być zmieniany bez konieczności restartu komputera. Parametr ten ma wpływ na ruch WAN, gdy do domeny należy kilka podsieci, a w każdej podsieci znajduje się jej *Master Browser*.

11.1.2. BackupPeriodicity

Parametr ten definiuje, jak często *Backup Browser* łączy się z *Master Browser-em*.

Jest on typu REG_DWORD, domyślnie przyjmuje wartość 720 sekund (12 minut), a maksimum i minimum ma takie jak *MasterPeriodicity*. Po zmianie natomiast wymaga restartu komputera. Parametr ten nie ma wpływu na ruch WAN, cały ruch zamyka się w danej podsieci.

12. Optymalizacja ruchu związanego z replikacją katalogów

Usługa replikacji katalogów w Windows NT pozwala na automatyczne powielenie źródłowego katalogu do wielu innych komputerów. Proces ten może wygenerować wiele pakietów w zależności od ilości replikowanych danych. Serwer eksportujący co 5 minut (domyślnie) sprawdza, czy są dane do zreplikowania. Czas ten może być wydłużony. Dopóki dane na serwerze eksportującym nie zostaną zmienione, proces ten generuje niewielki ruch.

W przypadku zmiany danych eksportowych ruch zależy od ich wielkości. Dla przykładu katalog z 16 plikami wielkości 426000 bajtów wygeneruje 1425 ramek, a replikacja zajmie około 42 sekund, podczas gdy skasowanie jednego pliku z tej samej listy eksportowej wygeneruje tylko 251 ramek i 48 sekund na weryfikację i uaktualnienie.

12.1. Struktura katalogów

Najlepszym sposobem na zminimalizowanie ruchu związanego z replikacją katalogów jest stosowanie płaskiej i płytkiej struktury katalogów. Stosowanie dużych, głębokich, o często zmienianej zawartości katalogów wydatnie obciąża usługę replikacji katalogów. Usługa replikacji katalogów sprawdza i kopiuje cały katalog, jeżeli jakikolwiek plik w tym katalogu uległ zmianie. Z tego powodu stosowanie większej liczby mniej rozbudowanych (zagłębionych) katalogów zamiast małej liczby katalogów o głębokiej strukturze wydatnie zmniejszy obciążenie związane z replikacją katalogów. Głęboką strukturę katalogów replikowanych można stosować, gdy zmiany w zawartości katalogów zdarzają się sporadycznie.

12.2. Server Manager

Istnieje możliwość zabezpieczenia przed replikacją katalogu w ciągu dnia poprzez zablokowanie katalogu. Realizuje się to w *Serwer Manager-rze* albo *Control Panel-Serwer*. Trzeba wybrać *Properties*, potem *Replication*. W okienku *Replication Directory* w opcji *Export Directories* wybierz *Manage*. Następnie wybierz katalog i wybierz *Add Lock*. Spowoduje to przesunięcie ruchu związanego z replikacją, na czas gdy pracuje mniej użytkowników.

W okienku *Replication Directory* dla każdego katalogu znajduje się także opcja *"Wait Until Stabilized"*. Opcja ta powoduje, że serwer importujący kopiuje cały podkatalog, jeżeli jakikolwiek plik w katalogu uległ zmianie. Wyłączenie tej opcji spowoduje, że serwer importujący będzie sprawdzał datę, godzinę, nazwę, atrybuty, rozmiar każdego pliku i będzie kopiował tylko te pliki, które uległy zmianie.

12.3. Parametry rejestrów

Wpisy związane z replikacją można znaleźć w rejestrach:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Replicator\Parameters

Najczęściej modyfikowane parametry związane z replikacją katalogów to *Interval* i *Pulse*.

Interval - definiuje, jak często serwer eksportujacy sprawdza, czy nastąpiły zmiany w replikowanym katalogu i powiadamia importujące serwery o konieczności uaktualnienia. Domyślnie przyjmuje wartość 5 minut. Można zwiększyć jego wartość do 60 minut. Zmniejszy się wówczas częstość replikacji, ale jednocześnie wzrośnie opóźnienie w uaktualnianiu pojedynczych zmian.

Pulse - jest parametrem, który podobnie jak licznik kontroluje, jak często serwer importujący kontaktuje się z serwerem eksportującym. Jeżeli serwer importujący nie otrzyma jakiejkolwiek informacji od serwera eksportującego po czasie *Pulse* * *Interval* minut, to samodzielnie wyśle żądanie uaktualnienia do serwera eksportującego. Domyślna wartość *Pulse* to 2, co oznacza, że po 10 minutach (2 <pulse> * 5 minut <interval>) milczenia ze strony serwera eksportującego serwer importujący zainicjuje komunikację z serwerem eksportującym. Zwiększenie wartości parametru *Pulse* zwiększy odstępy czasu, po jakich serwer importujący będzie inicjował komunikację z serwerem eksportującym, dając tym samym więcej czasu serwerowi eksportującemu na zainicjowanie komunikacji.

13. Podsumowanie

Powyższe rozważania dotyczące sieci typu Windows NT pozwoliły wyodrębnić kilka czynników, jakie mają wpływ na obciążenie sieci.

Tabela 6

Zestawienie mechanizmów generujących ruch w sieci i częstotliwość ich występowania

Usługa	Ruch w sieci /obciążenie	Częstotliwość
DHCP	Nadanie nowego adresu IP - 4 ramki - 1368 bajtów. Przedłużenie użyczenia adresu IP - 2 ramki - 684 bajty.	Dla każdego klienta. Przy każdym starcie komputera i w połowie czasu użyczenia.
Klient WINS	Rejestracja - 2 ramki = 214 bajtów. Odnowienie - 2 ramki = 214 bajtów. Konwersja - 2 ramki 196 bajtów.	Każdorazowo, gdy aplikacja lub usługa startuje. Dla każdego serwisu lub aplikacji w połowie czasu TTL. Różna częstotliwość.

Weryfikacja logowania	Przygotowanie - 15 ramek = 2000 bajtów. Sprawdzanie wiarygodności - 4 ramki = 760 bajtów. Analiza sesji 5 ramek = 360 bajtów. Skrypty, profile itd. Zróżnicowany ruch.	Jednokrotnie dla każdego logowania.
Browser	Ogłoszenie stacji 1 ramka = 243 bajty. Ogłoszenie lokalnego *Master Browsera* 1 ramka = 250 bajtów. Ogłoszenie grupy 1 ramka = 250 bajtów. Elekcja – wiele ramek każda po 235 bajtów. Poszukiwanie *Backup Browser-a* 2 ramki ~ 450 bajtów.	Co 12 minut przez każdy komputer. Każdorazowo po elekcji *Master Browser-a.* Co 15 minut. Po inicjalizacji każdego komputera mogącego być *Master Browser-em.* Raz w czasie pierwszego przeglądania sieci przez komputer.
Transfer plików	Rozpoznanie adresu -2 ramki = 120 bajtów. Sesja TCP – 3 ramki = 180 bajtów. Sesja NetBIOS - 2 ramki = 186 bajtów. Negocjacja protokołu SMB - 2 ramki = 350 bajtów. Połączenie – 2 ramki = 350 bajtów. Rozłączenie - 5 ramek = 360 bajtów.	Przy każdej próbie komunikacji z inną stacją TCP/IP. Jednokrotnie dla każdej docelowej stacji TCP przy pierwszym połączeniu. Jednokrotnie dla połączenia NetBIOS przy pierwszym połączeniu. Jednokrotnie przy pierwszym połączeniu SMB ze stacją docelową. Jednokrotnie dla pojedynczego sięgnięcia do poszczególnego zasobu. Jednokrotnie dla ostatniego pakietu z sesji TCP w celu odłączenia stacji.
Synchronizacja bazy *Directory Services*	Poszukiwanie PDC - 4 ramki ~ 45 bajtów. Ustanowienie sesji 11 ramek = 1 200 bajtów. Zestawienie *Secure Channel* - 8 ramek= 1550 bajtów. Weryfikacja bazy - 6 ramek = 1350 bajtów. Informacja o uaktualnieniu PDC - 1 ramka ~ 400 bajtów.	Jednokrotnie w czasie uruchamiania BDC. W czasie każdej synchronizacji. W czasie każdej synchronizacji. W czasie każdej synchronizacji. W czasie każdej synchronizacji.
Ustanowienie związków zaufania	Około 100 ramek ~ 15000 bajtów.	Raz dla każdego utworzonego związku zaufania.
Import zaufanych kont	Około 100 ramek = 24000 bajtów dla 11 kont.	Każdorazowo w trakcie importu zaufanych kont.

Uwierzytelnienie zaufanego dostępu	20 ramek ~ 3700 bajtów.	Raz dla każdego dostępu do zasobów ufającej domeny.
Replikacja katalogów	Powiadomienie - 1 ramka ~ 340 bajtów. Zestawienie sesji - 9 ramek ~ 1300 bajtów. Weryfikacja katalogów 22 ramki ~ 3700 bajtów. Uaktualnienie katalogów - różnej wielkości obciążenie sieci	Jednokrotnie dla importującej domeny dla każdego importowanego drzewa katalogów. Jednokrotnie z każdego serwera importującego dla każdej operacji uaktualniania. Jednokrotnie z każdego serwera importującego dla każdej operacji uaktualniania.
Replikacja WINS	Weryfikacja bazy - 12 ramek ~ 900 bajtów. Uaktualnienie bazy - około 14 ramek ~ 2100 bajtów (zależnie od liczby zmian uaktualnień).	Jednokrotnie dla każdego zapytania do partnera replikacji. Jednokrotnie dla każdego zapytania do partnera replikacji.

LITERATURA

1. Sheldon T.: Wielka Encyklopedia Sieci Komputerowych. Wydawnictwo Robomatic ISBN 83-900945-5-X.
2. Brzeziński K. M.: Sieci Lokalne. Oficyna Wydawnicza Pol. Warszawskiej, Warszawa 1995.
3. MS Windows NT Resource Kit.
4. Microsoft Developer Network.
5. Miller A. M.: Sieci Internetworking. Wydawnictwo RM, Warszawa 1998.

Recenzent: Prof. dr hab. inż. Andrzej Grzywak

Wpłynęło do Redakcji 26 kwietnia 1999 r.

Abstract

The development of both Intranet and Extranet as well as growing popularity of multimedia applications results in networks, especially WAN networks, overload. As far as the individual user is concerned, it makes his system very slow and in the extreme conditions it

makes the communication impossible. The situation described above is an example of the analysis and optimisation in typical computer network traffic. The article presents the traffic analysis including DHCP activity as well as the log-in process, browser function, file transportation sessions, directory services data base synchronicity and catalogues replication.

The number of packages generated by DHCP can be regulated through the changes of IP address lease time. The traffic connected to data base accounts synchronicity or to browser activity could be optimised through the changes in the parameters of system registers. The number of packages generated by the catalogues replication depends on both the value of the parameters in system registers and on the structure of the catalogues being replicated itself. The proper analysis of the network packages and the optimisation allowing for unique characteristics of the networks may contribute to improvement in networks effectiveness. The presented above analysis concerned MS Windows NT network using TCP/IP protocol and may not be true in regard to the networks co-operating with different operating systems.