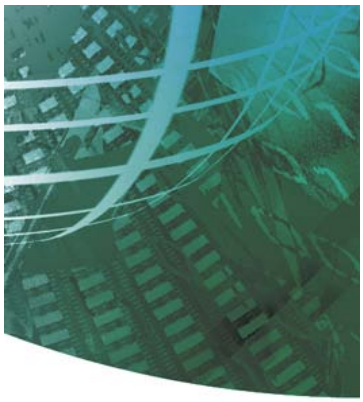
NIEZAWODNE ROZWIĄZANIA SYSTEMÓW AUTOMATYKI



Praca asix3 na stanowiskach w sieci Internet

Pomoc techniczna

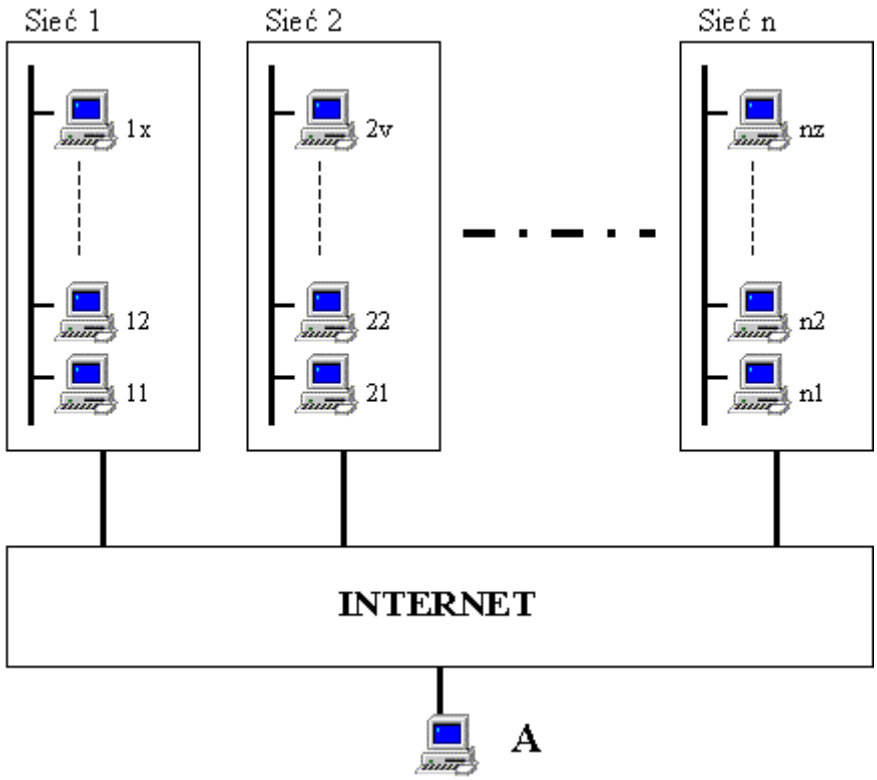
Dok. Nr PLP0008
Wersja: 24-11-2005

ASKOM Sp. z o. o., ul. Józefa Sowińskiego 13, 44-121 Gliwice,
tel. +48 (0) 32 3018100, fax +48 (0) 32 3018101,
http://www.askom.com.pl, e-mail: office@askom.com.pl

1. asix w Internecie

1.1. Pozyskiwanie danych z wykorzystaniem VPN

asix3 posiada mechanizmy umożliwiające wykorzystanie sieci Internet do pozyskiwania danych pomiarowych równocześnie z wielu sieci lokalnych ze stanowiskami **asix**. Niniejszy dokument przedstawia rozwiązanie pozwalające na transfer danych z serwerów **asix** znajdujących się w kilku sieciach lokalnych LAN (Local Area Network) przez klienta z zainstalowanym oprogramowaniem **asix** i podłączonym do sieci Internet (*patrz: rysunek 1*).



Rysunek 1. Ogólna koncepcja połączenia.

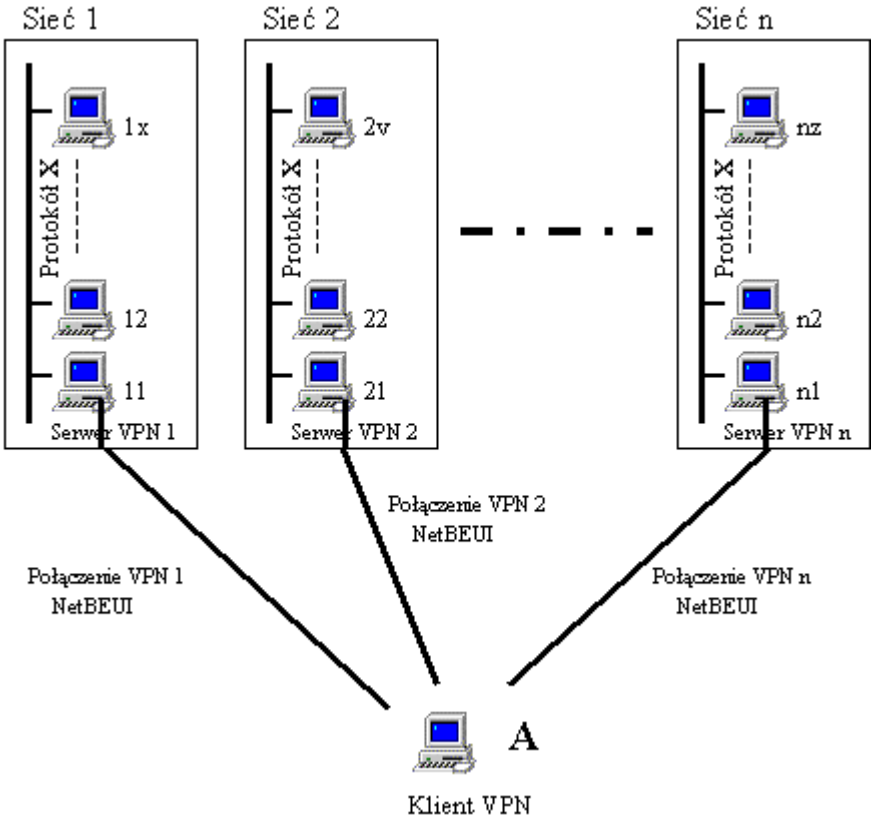
Rozwiązanie przewiduje wykorzystanie mechanizmu "wirtualnych sieci prywatnych" VPN (Virtual Private Network) opartych na protokołach PPTP (ang. Point to Point Tunneling Protocol) lub L2TP (ang. Layer Two Tunneling Protocol). W zależności od wymagań i uwarunkowań technicznych proponowane są dwie opcje rozwiązania:

- połączenie VPN jest realizowane pomiędzy klientem i serwerem **asix** pracującym w trybie *pomost*;
- połączenie VPN jest realizowane pomiędzy klientem i serwerem VPN, zapewniającym dostęp do całej sieci LAN.

W przypadku wykorzystywania wolnych łączy w dostępie do sieci Internet np. 24kbps, zaleca się wykorzystywanie metody połączenia VPN do serwera z pracującym w trybie *pomost* systemem **asix**. Metoda ta separuje ruch w sieci lokalnej, przez co zmniejsza ilość ramek przesyłanych do klienta.

1.1.1. Dostęp do danych poprzez serwer asix pracujący w trybie ‘pomost’

Stacja *klient VPN* posiada bezpośredni dostęp tylko do serwera VPN, na którym zainstalowany jest system **asix**, pracujący w trybie *pomost*. Taka konfiguracja umożliwia przesyłanie danych pomiarowych z pozostałych stacji.



Rysunek 2. Konfiguracja połączenia z wykorzystaniem serwera asix pracującego w trybie ‘pomost’.

Zaznaczony na rysunku 2 *Protokół X* służący do wymiany danych pomiędzy poszczególnymi stacjami sieci, może być protokołem TCPIP, NetBEUI lub IPX. Moduł sieciowy systemu **asix** pracujący na stacjach *serwer VPN* musi obsługiwać połączenia realizowane za pomocą sieci LAN oraz połączenia za pomocą protokołu NetBEUI do komunikacji ze stacją *klient VPN*. W związku z tym w sekcji [ASLINK] pliku inicjacyjnego aplikacji powinny znaleźć się następujące zapisy:

Adaptery = NetBEUI&wan, ProtokółX
Adaptery_Szukanie_Serwerow = ProtokółX

gdzie `ProtokółX` to jeden z tekstów: NetBEUI, TCPIP lub IPX.

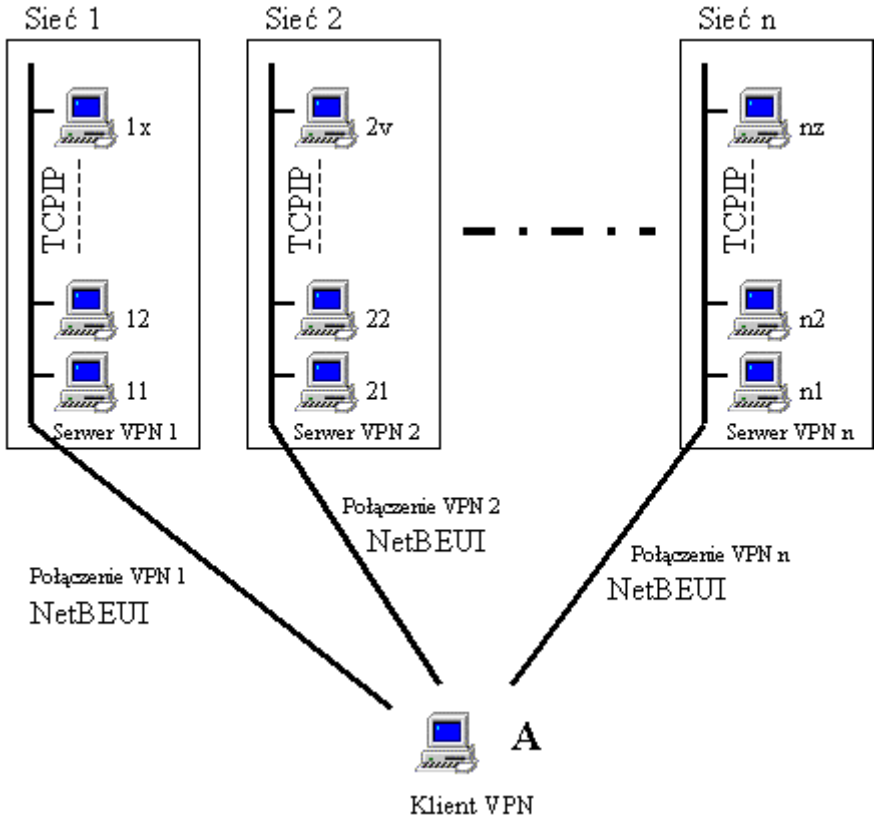
W sekcji [ASLINK] na stacji *klient VPN* należy umieścić zapis:

Adaptery=NetBEUI&wan
Czas_Szukania_Stacji=6000
Czas_Oczekiwania_Na_Odp = 10000
Aslink4=NIE
Timeout_Nadawczy = 60

W przypadku złych warunków połączenia VPN może być również konieczne zwiększenie wartości parametru *Timeout_nadawczy* na stacjach *serwer VPN* oraz *klient VPN*. Jego wartość nie może przekraczać wartości 240, co odpowiada dwóm minutom (parametr ma wartość wyrażoną w jednostkach równych 500 ms). Z tych samych powodów należy zwiększyć wartość parametru *Czas_Szukania_Stacji* oraz *Czas_Oczekiwania_Na_Odp*.

1.1.2. Dostęp do danych z wykorzystaniem połączenia VPN z siecią lokalną

Metoda druga zapewnia pełny i bezpośredni dostęp stacji *klient VPN* do wielu sieci LAN, w których znajdują się komputery z pracującym systemem **asix**. Systemy **asix** pracujące w tych sieciach komunikują się za pomocą protokołu TCPIP.



Rysunek 3. Konfiguracja połączenia VPN z sieciami lokalnymi.

W omawianej metodzie stacja *klient VPN* staje się logicznym członkiem każdej sieci LAN, do której została przyłączona (pomimo tego, że komunikacja po łączu VPN odbywa się za pomocą protokołu NetBEUI, zaś poszczególne stacje sieci LAN wykorzystują protokół TCPIP). Na stacji *serwer VPN* nie musi pracować system **asix**

W sekcji [ASLINK] każdej stacji sieci LAN, na której pracuje system **asix** należy umieścić zapis:

Adaptery = TCPIP

W sekcji [ASLINK] na stacji *klient VPN* należy umieścić zapis:

Adaptery=NetBEUI&wan
Czas_Szukania_Stacji=6000
Czas_Oczekiwania_Na_Odp = 10000
Aslink4=NIE
Timeout_Nadawczy = 60

W przypadku złych warunków połączenia VPN może być również konieczne zwiększenie wartości czasowych połączenia, które opisane są w rozdziale poświęconym metodzie dostępu do danych poprzez serwer **asix** pracujący w trybie *pomost* .

1.2. Konfiguracja łącza VPN

Rodzaj platformy serwer VPN jest uzależniony od wybranej metody pozyskiwania danych z systemu **asix**. W przypadku wybrania połączenia VPN realizowanego pomiędzy klientem i serwerem **asix** pracującym w trybie *pomost*, wymagane jest oprogramowanie Microsoft Windows NT 4.0 lub Microsoft Windows 2000. Natomiast wybór połączenia VPN realizowanego pomiędzy klientem i serwerem VPN i zapewniającym dostęp do całej sieci LAN, umożliwia zastosowanie dowolnej platformy programowej serwera VPN.

Serwer VPN niezależnie od wybranej opcji dostępu do danych **asix** powinien spełniać następujące kryteria:
- przesyłanie ramek protokołu NetBEUI
- przesyłanie ramek protokołu NetBIOS
- przesyłanie ramek typu Multicast

1.2.1. Konfiguracja Windows 2000 jako serwer VPN

Należy utworzyć połączenie przychodzące uruchamiając *Kreatora połączeń sieciowych* (*Połączenia sieciowe i telefoniczne* / *Utwórz nowe połączenie*). Po uruchomieniu kreatora należy wybrać pozycję *Zaakceptuj nadchodzące połączenie* i przycisnąć przycisk *Dalej*. Na kolejnej zakładce należy wybrać urządzenie odbierające połączenia przychodzące (modem, SDI itp.). Jeśli *serwer VPN* wykorzystuje sieć LAN do odbioru połączeń przychodzących, to wszystkie urządzenia listy należy pozostawić nie zaznaczone. Należy przycisnąć przycisk *Dalej*. Po przejściu do kolejnej zakładki zaznaczyć pozycję *Zezwalaj na wirtualne połączenia prywatne*. Następnie wybrać użytkownika, który będzie miał prawo nawiązywać połączenie VPN. Nazwa tego użytkownika będzie podawana na stacjach *klient VPN* w czasie nawiązywania połączenia VPN. Dalej zaznaczyć protokół NetBEUI oraz przycisnąć przycisk *Właściwości*. W otwartym okienku zaznaczyć pozycję *zezwalaj rozmówcom na dostęp do mojej sieci lokalnej* (dla metody 2) lub usunąć to zaznaczenie (dla metody 1). Należy również sparametryzować automatyczne nawiązywanie połączenia z Internetem (sposób jest zależny od typu połączenia z Internetem).

1.2.2. Modyfikacja rejestrów serwera VPN do pracy w trybie ‘pomost’

W celu usprawnienia pracy systemu Windows 2000 jako serwer VPN należy wprowadzić następujące poprawki w rejestrze systemowym:

Klucz
HKEY_LOCAL_MACHINE/SYSTEM/CurrentControlSet/Services/RemoteAccess/Parameters/Nbf musi zawierać następujące zapisy:

- DisableMcastFwdWhenSessionTraffic
  Jeśli wartość tego parametru jest równa 1, to przepływ datagramów typu multicast (wysyłanych przez moduł sieciowy ASLINK systemu **asix** w trakcie nawiązywania połączenia) będzie ograniczany na rzecz przepływu pakietów połączeń sesyjnych). Parametr należy ustawić na 0 tak, aby był zawsze możliwy przepływ datagramów, nawet przy znacznym obciążeniu połączenia VPN transmisją danych. Wartość 1 może spowodować trudności w nawiązywaniu kolejnych połączeń po łączu VPN.
  (wartość domyślna 1).
- EnableBroadcast
  Jeśli wartość tego parametru jest równa 1, to datagramy typu broadcast będą mogły przepływać pomiędzy siecią LAN a stacją *klient VPN*. ASLINK nie wykorzystuje tego typu pakietów i należy wartość tego parametru pozostawić ustawioną na 0.
  (wartość domyślna 0)
- MaxBcastDgBuffered
  Ilość datagramów typu broadcast i multicast buforowanych dla każdego łącza VPN. Należy ją zwiększyć w sytuacji "gubienia" datagramów. "Gubienie" datagramów objawia się trudnościami w nawiązywaniu połączeń, a okienko menedżera plików systemu **asix** nie zawsze pokazuje wszystkie dostępne stacje.
  (wartość domyślna 32)
- MaxDgBufferedPerGroupName
  Ilość datagramów buforowanych dla każdej nazwy grupowej. ASLINK używa tylko jednej nazwy grupowej. Uwagi jak dla parametru "MaxBcastDgBuffered"
  (wartość domyślna 10)
- MaxDynMem
  Ilość pamięci dynamicznej użytej do buforowania danych w połączeniach sesyjnych. Brak pamięci może skutkować zrywaniem połączeń sesyjnych W takiej sytuacji należy zwiększyć ilość pamięci dynamicznej lub zwiększyć wartości timeout'ow połączeń sesyjnych (*patrz: parametryzacja programu ASLINK w pliku pomocy ‘asix4. Podręcznik użytkownika’*)
  (wartość domyślna: 655350)
- MultiCastForwardRate
  Parametr określa odstęp czasu pomiędzy datagramami typu multicast. Ponieważ nawiązanie połączenia pomiędzy dwoma stacjami **asix** jest zazwyczaj poprzedzone wymianą datagramów typu multicast, to aby zdalna stacja *klient VPN* mogła w sposób pewny łączyć się ze stacjami w sieci LAN, parametr należy **bezwzględnie ustawić na wartość 0**.
  (wartość domyślna 5)
- NumRecvQueryIndications
  Ilość jednocześnie inicjowanych połączeń sesyjnych. Jeśli stacja *klient VPN* musi być połączona jednocześnie z wieloma stacjami sieci LAN, to parametr należy odpowiednio zwiększyć.
  (wartość domyślna 3)
- RcvDgSubmittedPerGroupName
  Ilość komend typu ReceiveDatagram inicjowanych równocześnie dla jednej nazwy grupowej.
  Jeżeli występuje „gubienie” datagramów, to wartość tego parametru należy zwiększyć. W

czasie testów wartość domyślna tego parametru okazała się być niewystarczająca już dla dwóch stacji przyłączonych do sieci LAN. Parametr należy ustawić na wartość większą niż podwójna ilość systemów **asix** w sieci LAN.
(wartość domyślna 3)

- RemoteListen
  Określa stopień dostępności stacji *klient VPN* dla stacji przyłączonych do sieci LAN. Jeśli zdalna stacja **asix** musi pełnić rolę serwera danych dla stacji przyłączonych do sieci LAN, to parametrowi *RemoteListen* **należy bezwzględnie przyporządkować wartość 2**.
  (wartość domyślna 1).

1.2.3. Konfiguracja Windows 2000 pracujących jako klient VPN

Należy utworzyć połączenie wychodzące uruchamiając *Kreatora połączeń sieciowych* (*Połączenia sieciowe i telefoniczne* / *Utwórz nowe połączenie*). Po uruchomieniu kreatora należy wybrać pozycję *Połącz z siecią prywatną za pośrednictwem Internetu* i przycisnąć przycisk *Dalej*. Nie należy zaznaczać pozycji *Automatycznie wybierz to połączenie początkowe*. Na kolejnej zakładce należy podać adres stacji *serwer VPN*. Po utworzeniu nowego połączenia wychodzącego należy je zaznaczyć i otworzyć okno dialogowe *Właściwości*. Na zakładce *Sieć* należy zaznaczyć protokół NetBEUI. Na zakładce *Opcje* należy wyłączyć pozycję *Monituj o nazwę użytkownika, hasło i certyfikat* oraz zaznaczyć opcję *wybierz numer ponownie po zerwaniu połączenia* (należy również sparametryzować odpowiednio ponowne wybieranie).

Automatyczne nawiązywanie połączenia VPN nie powinno następować częściej niż co dwie minuty. Należy połączyć się ze stacją *serwer VPN* podając nazwę użytkownika i hasło zaznaczając pozycję *zapisz hasło*. W przypadku otwierania przez system dodatkowych okien informacyjnych należy zaznaczać pozycję *nie pokazuj ponownie tego okna*.

Ww. ustawienia wybierania powinny sprawić, że odtworzenie zerwanego połączenia dokona się automatycznie bez potrzeby interwencji operatora. Oprócz automatycznego nawiązywania połączenia VPN, wymagane jest również sparametryzowanie automatycznego nawiązywania połączenia z Internetem. W przypadku wielu połączeń VPN, automatycznego nawiązywania tych połączeń nie należy wiązać z automatycznym nawiązaniem połączenia z Internetem tj. nie należy zaznaczać pozycji *Automatycznie wybierz to połączenie początkowe* (Właściwości połączenia VPN - zakładka *Ogólne*). Automatyczne nawiązywanie połączenia z Internetem należy sparametryzować oddzielnie.

1.2.4. Porty wykorzystywane przez VPN

Jeśli połączenie VPN wykorzystuje protokół PPTP, to są wykorzystywane porty protokołu TCPIP o numerach 1723 i 47. W przypadku protokołu L2TP porty te mają numery 500 i 50.

Rodzaj wykorzystywanego protokołu ustawia się na stacji *klient VPN* w parametrach połączenia VPN (zakładka *Sieć* / *typ wywoływanego serwera VPN*). Należy wybrać protokół PPTP lub *Automatyczny*.

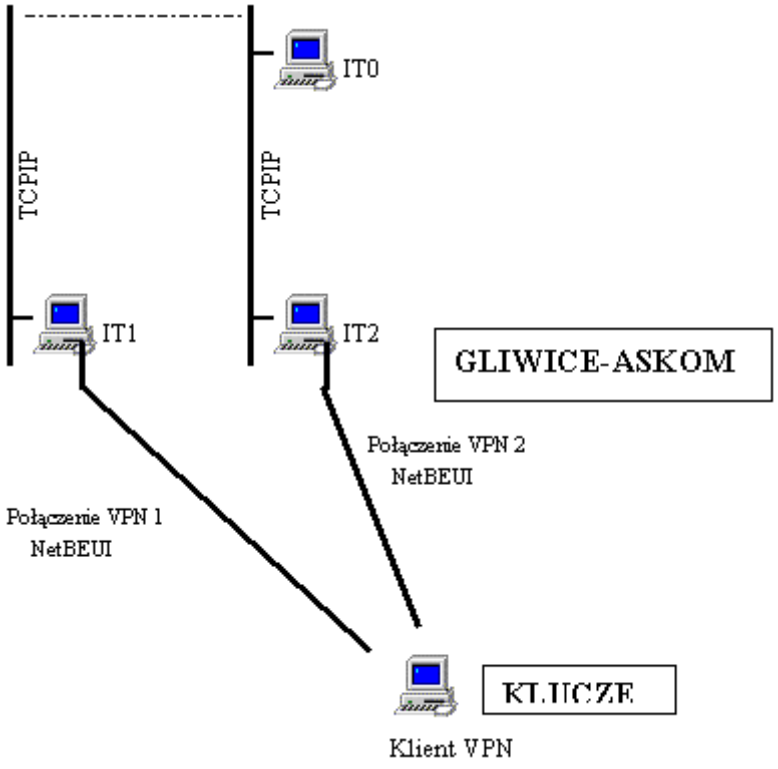
Połączenie z Internetem musi umożliwiać wykorzystanie ww. portów. Ma to znaczenie zwłaszcza w przypadku połączenia z Internetem za pośrednictwem *firewall*. Komputer pełniący funkcję *firewall* musi zezwalać na obsługę ww. portów.

1.3. Wyniki testów wykonanych przez firmę Askom

W przeprowadzonych testach przyjęto następujące założenia:

- stacja *klient VPN* pracuje pod systemem Windows 2000 Professional;
- stacje *serwer VPN* pracują pod systemem Windows 2000 Professional;
- stacje *serwer VPN* są "osiągalne" w sieci Internet poprzez stały adres IP lub nazwę DNS;
- stacje *klient VPN* i *serwer VPN* skonfigurowane są w ten sposób, że komunikacja po łączu VPN odbywa się za pomocą protokołu NetBEUI;
- konto użytkownika na rzecz, którego jest ustanawiane połączenie VPN musi posiadać na stacji *serwer VPN* uprawnienia do dokonywania takich połączeń;
- wszystkie systemy **asix** mają wersję 3.0 lub wyższą;
- połączenie z siecią Internet odbywa się poprzez połączenie modemowe z ogólnopolskim dostawcą usług teleinformatycznych. Prędkość połączenia z siecią Internet to 32kbit/s.

Na poniższym rysunku przedstawiono konfigurację połączeń przeprowadzonych testów.



Rysunek 4. Konfiguracja połączenia zrealizowanego podczas testów.

Stacja *klient VPN* połączona jest łączami VPN z wykorzystaniem protokołu NetBEUI ze stacjami IT1 oraz IT2. Stacja *klient VPN* nie miała bezpośredniego dostępu do stacji IT0. Dostęp do stacji IT0 odbywał się za pośrednictwem stacji IT2 z modułem ASMEN pracującym w trybie POMOST.

Stacja *klient VPN* pobierała 42 zmienne ze stacji IT2, 32 zmienne ze stacji IT0 (za pośrednictwem IT2) oraz 132 zmiennych ze stacji IT1. Daje to w sumie 206 zmiennych. Wszystkie zmienne miały czasokres odświeżania wynoszący 2 sekundy, co daje 103 zmienne na sekundę. Dodatkowo moduł ASPAD odczytywał po dwie zmienne z archiwum sieciowego na stacji IT1 oraz IT2. Zmienne te były wyświetlane na wykresach.

Wg wskazań AslView średni transfer wahał się w granicach 3000-3500 B/s, a w czasie transferu plików alarmów historycznych dochodził chwilowo do 4900 B/s.

W czasie trwania testu przeprowadzono transfer alarmów historycznych ze stacji, co wiązało się z transferem plików o sumarycznej wielkości 2,5 MB. Transfer plików trwał ponad 20 min.

Przeglądanie zmiennych archiwizowanych w archiwach na stacjach IT1 i IT2 przebiegało prawidłowo. Odświeżenie pola wykresu zawierającego 10 min. okres czasu (300 pomiarów) trwało kilka sekund (nie więcej niż 7).

Menadżer plików systemu **asix** pokazywał zawsze oba serwery IT1 i IT2 - nie zaobserwowano gubienia datagramów.

Stacja *klient VPN* pracowała jako klient serwera czasu. Zaobserwowano jedną zmianę czasu.

Przeprowadzono wielokrotne próby zrywania połączenia z Internetem. Połączenia były odtwarzane poprawnie. Sztuczne zrywanie połączenia z Internetem prowadziło do jego automatycznego nawiązywania.

2. Spis rysunków

Rysunek 1. Ogólna koncepcja połączenia. *3*
Rysunek 2. Konfiguracja połączenia z wykorzystaniem serwera asix pracującego w trybie 'pomost'. *4*
Rysunek 3. Konfiguracja połączenia VPN z sieciami lokalnymi. *5*
Rysunek 4. Konfiguracja połączenia zrealizowanego podczas testów. *9*

Spis treści

1. ASIX W INTERNECIE 3

1.1. POZYSKIWANIE DANYCH Z WYKORZYSTANIEM VPN 3
1.1.1. Dostęp do danych poprzez serwer asix pracujący w trybie "pomost" 4
1.1.2. Dostęp do danych z wykorzystaniem połączenia VPN z siecią lokalną 5
1.2. KONFIGURACJA ŁĄCZA VPN 6
1.2.1. Konfiguracja Windows 2000 jako serwer VPN 6
1.2.2. Modyfikacja rejestrów serwera VPN do pracy w trybie 'pomost' 7
1.2.3. Konfiguracja Windows 2000 pracujących jako klient VPN 8
1.2.4. Porty wykorzystywane przez VPN 8
1.3. WYNIKI TESTÓW WYKONANYCH PRZEZ FIRMĘ ASKOM 9

2. SPIS RYSUNKÓW 11