Roger Access Control System 5v2

Nota aplikacyjna nr 008

Wersja dokumentu: Rev. A

Komunikacja sieciowa

Uwaga: Niniejszy dokument dotyczy RACS 5 v2.0.4 lub nowszy

Wprowadzenie

Sieć komputerowa (Ethernet) jest wykorzystywana w systemie RACS 5 do komunikacji pomiędzy kontrolerami MC16, oprogramowaniem zarządzającym VISO, serwerami (usługami Windows) z pakietu oprogramowania RogerSVC oraz bazą danych MS SQL Server. Do prawidłowego funkcjonowania systemu istotne jest, by transmisja sieciowa mogła być realizowana w sposób niezawodny i bez niepotrzebnych zakłóceń.

Uwaga: Zasadniczo kontroler MC16 może być użytkowany zarówno w sieci WAN jak i LAN, przy czym gwarancją producenta jest objęta tylko jego praca w wyizolowanej sieci LAN zarezerwowanej wyłącznie dla systemu kontroli dostępu, w którym ma pracować kontroler.

Uwaga: Przed decyzją o użyciu kontrolera w nieizolowanej sieci LAN lub WAN zaleca się przeprowadzenie testów potwierdzających prawidłowe działanie komunikacji w tej sieci. Należy przy tym mieć na uwadze, że pozytywny wynik testów w nie jest gwarancją poprawnej pracy urządzenia lub systemu gdyż, warunki panujące w danej sieci mogą ulegać znacznym zmianom a sieć być celem ataków cybernetycznych.

Komunikacja sieciowa

Ogólna koncepcja komunikacji

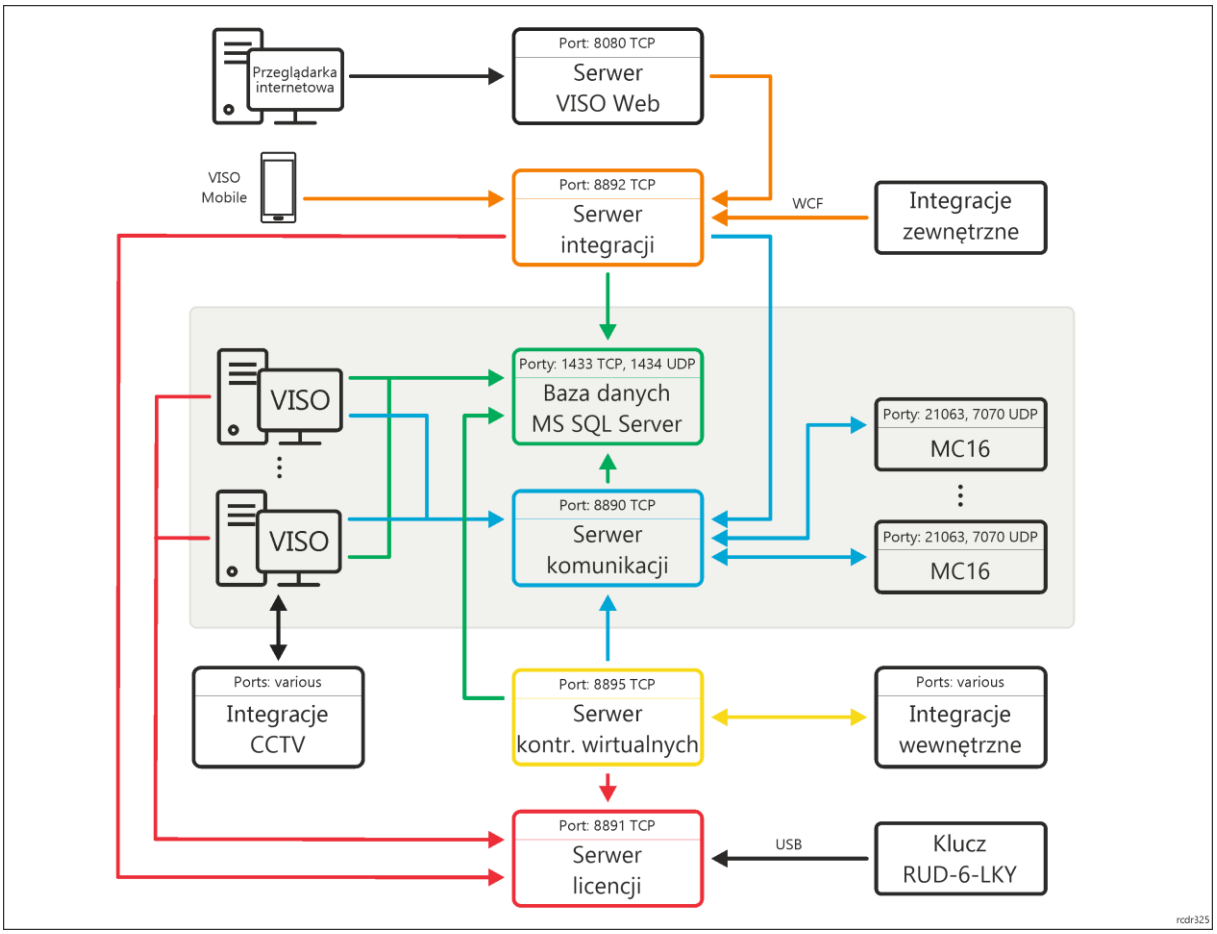
System RACS 5 od strony sprzętowej to przede wszystkim kontrolery MC16, czytniki MCT i ekspandery MCX. Z kolei od strony oprogramowania to przede wszystkim:

- VISO – oprogramowanie zarządzające systemem RACS 5
- RogerSVC – pakiet oprogramowania zawierający w sobie takie usługi Windows jak
  - Serwer komunikacji
  - Serwer licencji
  - Serwer integracji
  - Serwer kontrolerów wirtualnych
  - Serwer VISO Web

Spośród wymienionych serwerów koniecznym do funkcjonowania systemu jest Serwer komunikacji i ewentualnie Serwer licencji jeżeli system ma oferować funkcjonalności spoza podstawowego zakresu. Pozostałe serwery są opcjonalne i stosuje się je w określonych scenariuszach pracy. Dodatkowe konieczne jest utworzenie bazy danych MS SQL Server zgodnie z notą AN017.

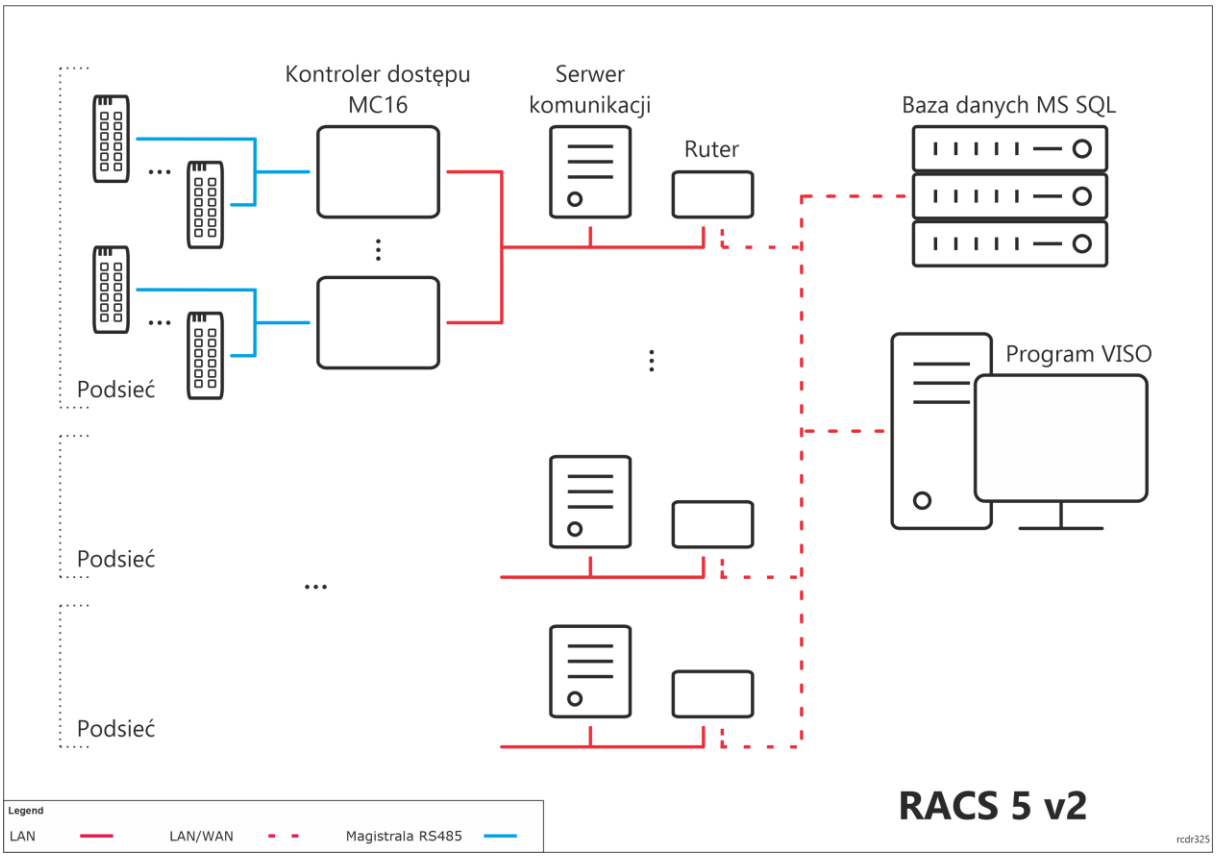
Na poniższym schemacie podano domyślne porty. Wszystkie porty oprócz portu 21063 UDP kontrolera MC16 są konfigurowalne za pomocą oprogramowania RogerSVC, VISO albo w ramach środowiska MS SQL Server. Serwery mogą funkcjonować na jednym komputerze lub na różnych

komputerach i w takim układzie na danej stacji instaluje się jedynie wymagane elementy oprogramowania RogerSVC.



Serwery komunikacji

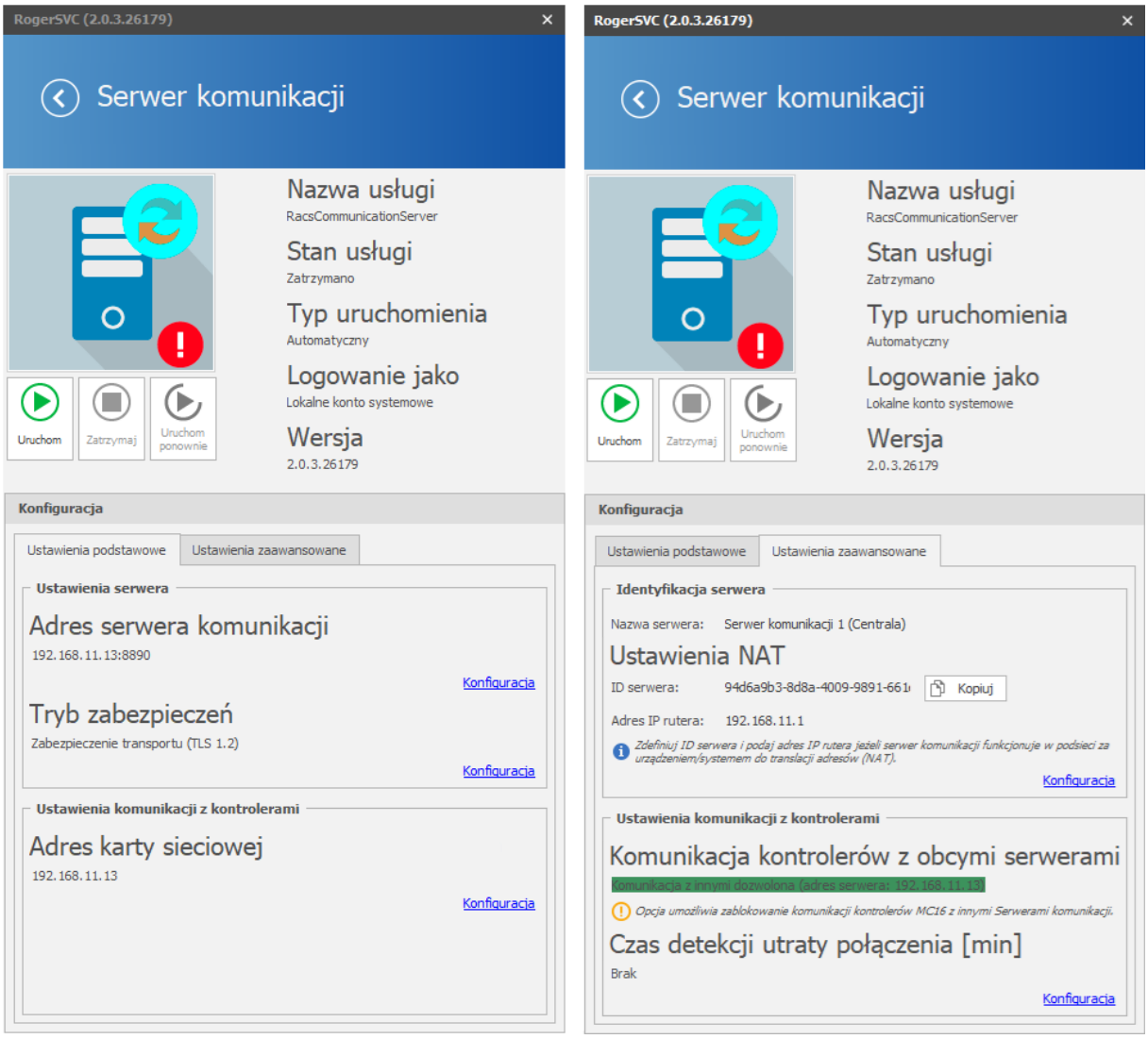
W systemie RACS 5 v1 konieczne było stosowanie jednego wspólnego dla całego systemu Serwera komunikacji. W systemie RACS 5 v2 jak na schemacie poniżej wprowadzona została możliwość stosowania wielu Serwerów komunikacji, czyli osobnych komputerów z zainstalowaną usługą z pakietu oprogramowania RogerSVC. W praktyce, stosowanie wielu takich serwerów ma przede wszystkim sens w systemach, które są rozproszone czyli np. takie gdzie poszczególne podsieci systemu RACS 5 funkcjonują w różnych budynkach/miastach/krajach.



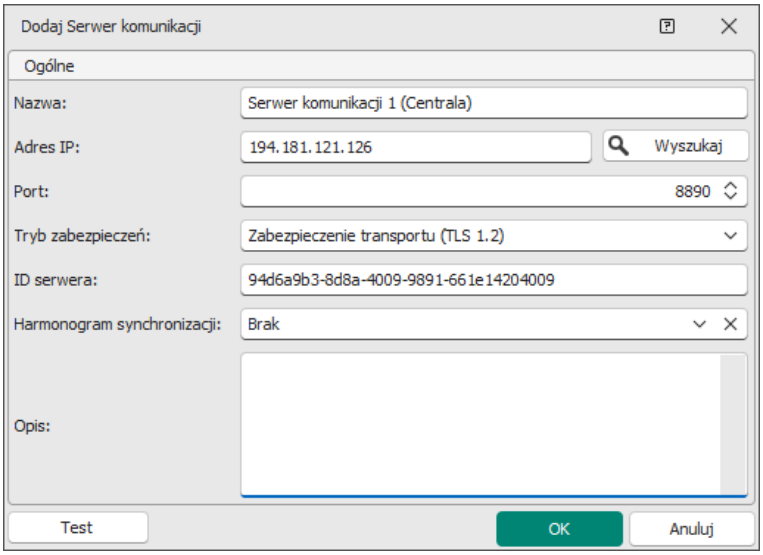
Komunikacja poprzez ruter (NAT)

W systemie RACS 5 v2 dodane zostało nowe rozwiązanie w zakresie komunikacji poprzez ruter (NAT), które zastąpiło wcześniej stosowane przekierowywanie portów dla poszczególnych kontrolerów MC16. Aby zdefiniować komunikację poprzez ruter (NAT) w systemie RACS 5 v2:

- Zainstaluj program RogerSVC zaznaczając Serwer komunikacji, uruchom program i kliknij jego ikonę w zasobniku Windows.
- Wybierz kafelek *Serwer komunikacji* i następnie zakładkę *Ustawienia podstawowe*.
- Kliknij *Konfiguracja* i wprowadź adres karty sieciowej komputera by zdefiniować adres IP serwera w sieci lokalnej (np. 192.168.11.13). W razie potrzeby zdefiniuj własny port zamiast domyślnego portu 8890 TCP.



- W tym samym oknie wybierz zakładkę *Ustawienia zaawansowane*.
- Kliknij *Konfiguracja* i w otwartym oknie wygeneruj ID serwera oraz podaj wewnętrzny adres IP rutera (np. 192.168.11.1) pośredniczącego w komunikacji z Serwerem komunikacji.
- Uruchom lub zrestartuj Serwer komunikacji.
- W ustawieniach rutera ustaw przekierowanie dla portu usługi Serwera komunikacji (domyślnie 8890 TCP).
- Uruchom program VISO i podczas dodawania Serwera komunikacji wprowadź ten sam parametr ID serwer ID co w RogerSVC oraz podaj zewnętrzny adres IP rutera (np. 194.181.121.126) pośredniczącego w komunikacji.
- Kliknij *Test* by zweryfikować połączenie z Serwerem komunikacji.



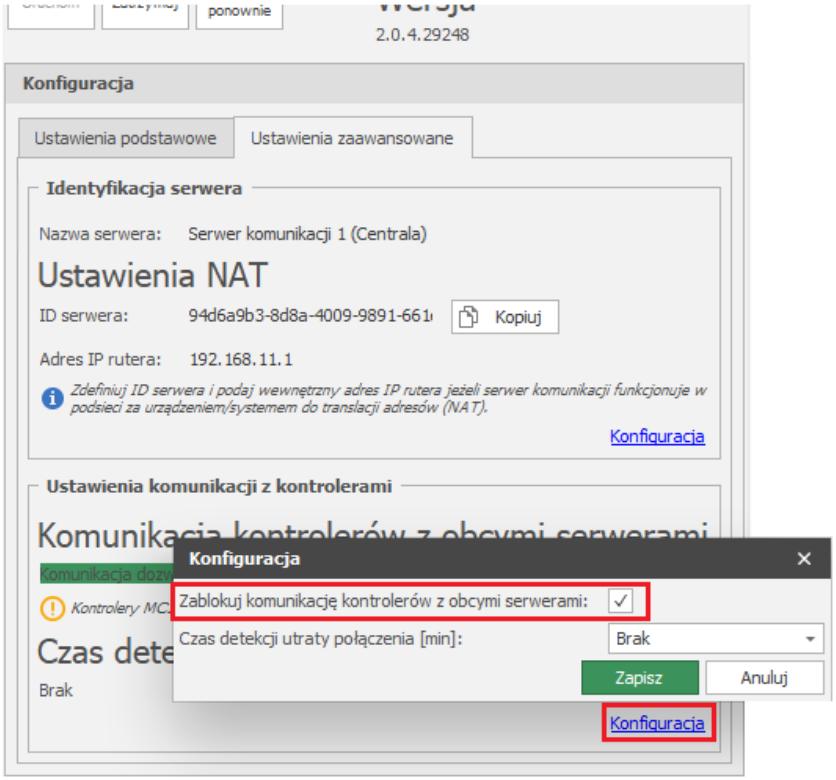
Alternatywnie możliwe jest zastosowanie sieci typu VPN zamiast przekierowywania komunikacji przez ruter.

Zabezpieczenie komunikacji

Komunikację z Serwerem komunikacji może być szyfrowana jedną z dostępnych metod poprzez wskazanie *Trybu zabezpieczeń* podczas konfiguracji Serwera komunikacji w programie RogerSVC w zakładce *Ustawienia podstawowe*. Ten sam Tryb zabezpieczeń trzeba również załączyć podczas dodawania Serwera komunikacji w programie VISO.

Komunikacja z kontrolerami MC16 jest szyfrowaną metodą AES128 CBC z zastosowaniem klucza komunikacyjnego definiowanego indywidualnie dla każdego kontrolera MC16. Dodatkowo w systemie RACS 5 v2 możliwe jest powiązanie kontrolera z Serwerem komunikacji o określonym adresie IP. W takim układzie zapytania z innych serwerów będą odrzucane przez kontroler nawet jeżeli stosowany jest prawidłowy klucz komunikacyjny. Takie powiązanie kontrolerów może być przydatne w dużych systemach gdzie może istnieć potrzeba wyraźnego pogrupowania kontrolerów jak też istnieje potrzeba zabezpieczenia systemu przed tym by kolejny Serwer komunikacji, który został dodany w sposób nieupoważniony nie ingerował w działanie systemu. Powiązanie kontrolerów z danym Serwerem komunikacji realizuje się poprzez zaznaczenie opcji *Zablokuj komunikację kontrolerów z obcymi serwerami* w ramach Serwera komunikacji w programie RogerSVC. Kontrolery, które zostaną wykryte w programie VISO po dodaniu Serwera komunikacji zostaną z nim na stałe powiązane. Odwiązanie można zrealizować poprzez odznaczenia wspomnianej wcześniej opcji w programie RogerSVC albo poprzez reset pamięci danego kontrolera MC16.

Uwaga: Należy zachować ostrożność podczas stosowanie opcji *Zablokuj komunikację kontrolerów z obcymi serwerami* bo jej nieumiejętne stosowanie może całkowicie zablokować komunikację z danymi kontrolerami MC16 w systemie RACS 5 i konieczny będzie wtedy reset pamięci urządzeń. Przykładowo komunikacja może zostać zablokowana gdy zmieniony zostanie adres IP Serwera komunikacji bez wcześniejszego odwiązania kontrolerów jak też gdy usunięty zostanie kontroler w programie VISO bez wcześniejszego odwiązania od serwera a następnie podjęta zostanie próba jego dodania do innego Serwera komunikacji.



Typowe problemy komunikacji sieciowej

Dla optymalnego i w pełni funkcjonalnego działania systemu RACS 5 istotna jest przede wszystkim prawidłowa i nieprzerywana komunikacja sieciowa między kontrolerami, serwerami oprogramowania RogerSVC i bazą danych. W tym celu należy wykonać okablowanie przy zachowaniu norm i założeń dotyczących sieci komputerowych. Podczas eksploatowania systemu RACS 5 można napotkać typowe problemy komunikacyjne wynikające z:

- Pojawiających się zakłóceń elektromagnetycznych pochodzących od kabli i przewodów elektrycznych/energetycznych.
- Wykorzystania tego samego fizycznego łącza sieciowego do komunikacji systemu RACS 5, kamer CCTV IP oraz strumieniowania audio/video.
- Wykonania instalacji sieci standardu Fast/Gigabit Ethernet przy użyciu nieodpowiedniej jakości oraz standardu okablowania.
- Pojawiania się fizycznych zapętleń i załamań kabli sieciowych.
- Powstania zdublowanego fizycznego połączenia urządzeń sieciowych, czego wynikiem jest zapętlenie sieci i drastyczny spadek jej przepustowości.
- Zastosowania mało wydajnych i niepoprawnie skonfigurowanych urządzeń sieciowych.

Metody rozwiązywania problemów sieciowych

Aby uniknąć wspomnianych wcześniej problemów zaleca się:

- Wykonanie fizycznie wyodrębnionej sieci komputerowej do komunikacji między kontrolerami a Serwerem komunikacji.
- Zwrócenie szczególnej uwagi na bliskość kabli elektrycznych/energetycznych i ich potencjalne negatywne oddziaływanie.
- Stosowanie w sieciach LAN okablowania światłowodowego łączącego punkty dystrybucyjne.
- Stosowanie dobrej jakości okablowania miedzianego.
- Stosowanie urządzeń sieciowych uznanych producentów.

- Łączenie sieci systemu RACS 5 z pozostałymi sieciami na poziomie urządzeń trasujących (ruter).
- Wydzielenie stanowiska operatorskiego/administratora wyłącznie dla systemu RACS 5.

Incydentalnie można natknąć się na problemy niepoprawności konfiguracji urządzeń sieciowych, do których zaliczyć można:

- Niepoprawną konfigurację członkostwa sieci VLAN.
- Niewłaściwe użycie mechanizmów QoS.
- Niepoprawne wykorzystanie funkcji agregacji portów.
- Niewłaściwe użycie protokołu RSTP.
- Obecność w sieci hostów wykorzystujących sieci torrent i peer-to-peer.
- Niewłaściwe wykorzystywanie Muliticast IP.

Trzeba również mieć na uwadze, iż na jakość połączeń sieciowych ma wpływ wiele czynników zewnętrznych, które należy uwzględnić, przeanalizować i wyodrębnić już na etapie planowania sieci komputerowej.

Kontakt:
Roger sp. z o.o. sp.k.
82-400 Sztum
Gościszewo 59
Tel.: +48 55 272 0132
Faks: +48 55 272 0133
Pomoc tech.: +48 55 267 0126
Pomoc tech. (GSM): +48 664 294 087
E-mail: pomoc.techniczna@roger.pl
Web: www.roger.pl