Przewodnik po sieciowych systemach telewizji dozorowej IP

Tłumaczenie „Technical guide to network video" Axis Communications

AXIS COMMUNICATIONS

5.5 Technologie sieciowe IP
Bezpieczeństwo sieci

Istnieje wiele sposobów zapewniania bezpieczeństwa w sieciach przewodowych i bezprzewodowych oraz między różnymi sieciami a klientami. Kontrolowane i zabezpieczone może być wszystko: od danych wysyłanych przez sieć po faktyczne wykorzystanie i dostępność sieci.

5.5.1. Bezpieczna transmisja

Zapewnienie bezpiecznej transmisji danych można porównać do korzystania z usługi kurierskiej do przesłania ważnego i tajnego dokumentu od jednej osoby do drugiej. Gdy kurier przyjeżdża do nadawcy, zwykle jest proszony o okazanie dokumentu tożsamości. Nadawca decyduje wtedy, czy kurier jest osobą, za którą się podaje, i czy można mu zaufać. Jeżeli wszystko jest w porządku, kurierowi wręczana jest zamknięta i zaplombowana teczka, którą ten ma dostarczyć do odbiorcy. U odbiorcy ma miejsce taka sama procedura kontroli tożsamości oraz sprawdzenie, czy plomba nie została uszkodzona. Po wyjściu kuriera odbiorca otwiera teczkę i wyjmuje dokument, aby go przeczytać.
Bezpieczna komunikacja jest tworzona w ten sam sposób; można ją podzielić na trzy etapy:

Uwierzytelnianie

Początkowym etapem jest przedstawienie się użytkownika (lub urządzenia) w sieci i u odbiorcy. Odbywa się to na zasadzie okazania sieci/systemowi swojego rodzaju dowodu tożsamości, np. nazwy użytkownika i hasła, certyfikatu X509 (SSL) i wykorzystania standardu 802.1x.

Uwierzytelniania wg standardu IEEE 802.1x

Pod naciskiem użytkowników sieci bezprzewodowych, domagających się silniejszych zabezpieczeń, standard 802.1x stał się obecnie najczęściej stosowaną metodą uwierzytelniania: IEEE 802.1x zapewnia uwierzytelnianie urządzeń podłączonych do portu sieci LAN, a następnie nawiązanie połączenia typu punkt-punkt *(point-to-point)* lub uniemożliwienie dostępu z tego portu przy braku uwierzytelnienia.

Jak to działa?

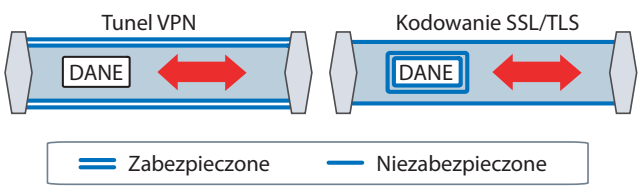
Klienci i serwery w sieci 802.1x uwierzytelniają się nawzajem za pomocą certyfikatów cyfrowych dostarczanych przez organy certyfikacji. Certyfikaty te są następnie potwierdzane przez jednostkę zewnętrzną, np. przez serwer uwierzytelniający nazywany serwerem RADIUS, którego przykładem jest usługa Microsoft Internet Authentication Service.
Urządzenie należące do sieciowego systemu wizyjnego Axis przedstawia swój certyfikat przełącznikowi sieciowemu, który z kolei przekazuje go do serwera RADIUS. Ten akceptuje lub odrzuca certyfikat, informuje o tym przełącznik, który udziela lub zabrania dostępu do sieci z określonego portu.
Dzięki temu porty sieciowe mogą pozostawać otwarte i dostępne: punkt dostępowy umożliwi połączenie z siecią tylko wtedy, gdy zostanie użyta prawidłowa tożsamość.

Autoryzacja
Kolejnym etapem jest autoryzacja i akceptacja uwierzytelnienia, czyli sprawdzenie, czy urządzenie jest tym, za które się podaje. Odbywa się to poprzez sprawdzenie tożsamości w bazie danych lub na liście prawidłowych i zaakceptowanych tożsamości. Po zakończeniu autoryzacji urządzenie zostaje całkowicie podłączone do systemu i może w nim pracować.

Prywatność
Ostatnim etapem jest zastosowanie wymaganego poziomu prywatności. Odbywa się to za pomocą szyfrowania komunikacji, uniemożliwiającego nieuprawnionym osobom użycie/odczyt danych. Szyfrowanie może powodować znaczny spadek wydajności, zależnie od rodzaju implementacji i zastosowanej metody szyfrowania.
Prywatność można zapewnić na różne sposoby. Dwie najczęściej stosowane metody to sieci VPN i protokół SSL/TLS (znany też jako HTTPS):

■ Sieci VPN (Virtual Private Network – wirtualna sieć prywatna)
Sieć VPN tworzy bezpieczny tunel między punktami w obrębie tej sieci. W sieci VPN mogą pracować tylko urządzenia z odpowiednim „kluczem". Urządzenia sieciowe pomiędzy klientem a serwerem nie mają dostępu do danych. W sieci VPN różne miejsca mogą być bezpiecznie połączone poprzez Internet.

■ Protokół SSL/TLS
Kolejnym sposobem zapewnienia bezpieczeństwa jest zastosowanie szyfrowania samych danych. W takim przypadku nie stosuje się bezpiecznego tunelu, jak w rozwiązaniu VPN, ale zabezpiecza przesyłane dane. Dostępnych jest wiele różnych technik szyfrowania, takich jak SSL, WEP i WPA; dwie ostatnie stosuje się w sieciach bezprzewodowych.



Gdy wykorzystywany jest protokół SSL, znany też jako HTTPS, urządzenie lub komputer instaluje certyfikat, który jest następnie udostępniany lokalnie przez użytkownika lub podmiot zewnętrzny, np. Verisign.

5.5.2. Bezpieczeństwo w sieciach bezprzewodowych

Ze względu na naturę komunikacji bezprzewodowej każda osoba z urządzeniem bezprzewodowym znajdująca się w zasięgu sieci może być jej użytkownikiem i korzystać z udostępnionych usług, stąd potrzeba zapewnienia bezpieczeństwa.

WEP
Standard WEP *(Wireless Equivalent Privacy)* szyfruje komunikację za pomocą algorytmu RSA RC4 i uniemożliwia dostęp do sieci osobom bez prawidłowego klucza.

Problem ze standardem WEP polega na tym, że jest on podatny na ataki, dlatego też nie jest w stanie zapewnić podstawowego poziomu bezpieczeństwa. Główną wadą standardu WEP jest statyczny klucz szyfrujący i krótki wektor początkowy. Ponieważ łatwo dokonać ataku na standard WEP za pomocą taniego sprzętu powszechnie dostępnego w sprzedaży, sieci bezprzewodowe nie powinny opierać się na zabezpieczeniach WEP.

WPA
Standard WPA *(WiFi Protected Access)* jest pozbawiony głównych wad WEP. W standardzie WPA klucz jest zmieniany dla każdej przesyłanej klatki za pomocą protokołu TKIP *(Temporal Key Integrity Protocol)*. Długość wektora początkowego jest zwiększona z 24 do 48 bitów. Standard WPA jest uznawany za podstawowy poziom zabezpieczeń sieci bezprzewodowych.
Aby zwiększyć bezpieczeństwo, należy stosować standard WPA2, który zamiast protokołu TKIP wykorzystuje standard szyfrowania AES *(Advanced Encryption Standard)*. Jest on najlepszym dostępnym obecnie zabezpieczeniem sieci bezprzewodowych. Standard WPA2 obejmuje też uwierzytelnianie 802.1x (patrz rozdział o standardzie 802.1x).

5.5.3. Ochrona pojedynczych urządzeń

Bezpieczeństwo oznacza też ochronę pojedynczych urządzeń przed włamaniem, np. uzyskaniem dostępu do urządzenia przez nieuprawnionego użytkownika, przed wirusami i innymi tego typu niepożądanymi elementami.
Dostęp do komputerów lub serwerów może być zabezpieczony za pomocą nazwy użytkownika i hasła o długości co najmniej 6 znaków (im dłuższe hasło, tym lepsze), zawierającego cyfry i litery (zarówno małe, jak i wielkie). Dla zwiększenia bezpieczeństwa i przyspieszenia logowania komputera można zastosować takie narzędzia, jak czytnik linii papilarnych lub karta mikroprocesorowa.
Do zabezpieczenia urządzenia przed wirusami, robakami i innym złośliwym oprogramowaniem zalecane jest używanie dobrego skanera antywirusowego z zaktualizowaną bazą wirusów. Skaner antywirusowy należy zainstalować na wszystkich komputerach. Systemy operacyjne powinny być regularnie aktualizowane o dodatki serwisowe i poprawki udostępniane przez producentów.
W przypadku podłączenia sieci LAN do Internetu bardzo ważne jest zastosowanie zapory *(firewall)*. Pełni ona rolę „strażnika", blokując lub ograniczając ruch do/z Internetu. Może też służyć do filtrowania przechodzących przez nią danych lub ograniczania dostępu.

5.6. QoS *(Quality of Service* – jakość usługi)

Obecnie zupełnie różne sieci łączą się w jedną sieć wykorzystującą protokół IP. Na przykład sieci telefoniczne i telewizyjne (CCTV) migrują w stronę sieci IP. W sieciach tych potrzebna jest kontrola sposobu udostępniania zasobów sieciowych w celu spełnienia wymagań wszystkich usług. Jednym z rozwiązań jest umożliwienie routerom i przełącznikom sieciowym różnego zachowania w przypadku różnych rodzajów usług (głosowych, danych, wideo), gdy ruch odbywa się w sieci. Technika ta jest nazywana *Differentiated Services (DiffServ)*. Dzięki zastosowaniu mechanizmu QoS różne aplikacje sieciowe mogą współistnieć w tej samej sieci, bez wzajemnego odbierania sobie przepustowości.

Definicja

Termin *Quality of Service* odnosi się do wielu technologii zapewniających określoną jakość różnych usług w sieci. Jakością taką może być np. zachowany poziom przepustowości, małe opóźnienie, brak utraty pakietów itp. Głównymi zaletami sieci z mechanizmem QoS są:

- możliwość hierarchizowania ruchu, czyli umożliwienia transmisji ważnych danych wcześniej niż tych o niższym priorytecie;
- większa niezawodność w sieci dzięki sterowaniu przepustowością, jaką może wykorzystywać dana aplikacja; można więc kontrolować „rywalizację" o przepustowość między aplikacjami.

QoS i sieciowe systemy wizyjne: wymagania

Aby można było zastosować mechanizm QoS w sieci z sieciowymi produktami wizyjnymi, muszą być spełnione następujące warunki:

- Wszystkie routery i przełączniki sieciowe muszą obsługiwać mechanizm QoS. Jest to ważne dla uzyskania pełnej funkcjonalności mechanizmu QoS.
- Sieciowe produkty wizyjne muszą mieć włączoną funkcję QoS.

Informacje o ruchu PTZ (przesunięcie, nachylenie, zbliżenie)

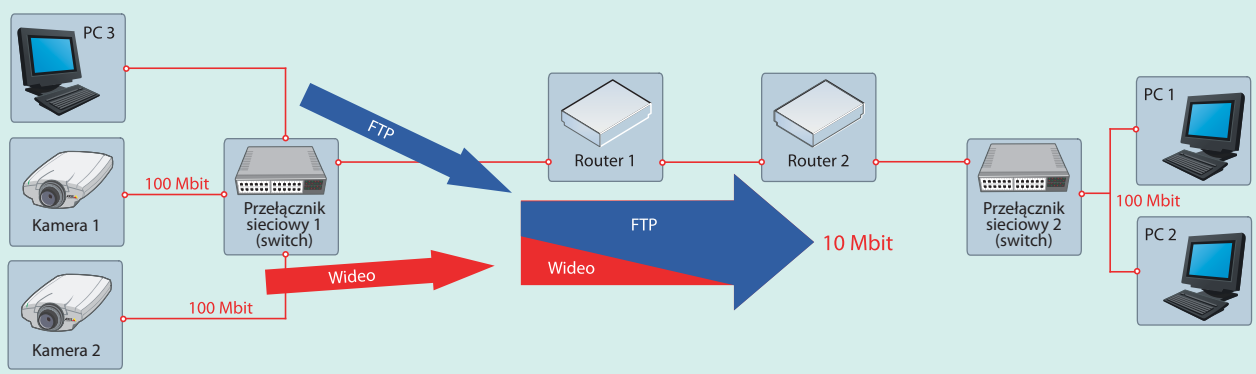
Ruch PTZ jest często uznawany za bardzo ważny, wymaga więc małego opóźnienia w celu zagwarantowania szybkiej reakcji na żądania zmian. Jest to typowy przypadek, w którym można zastosować mechanizm QoS w celu zagwarantowania niezbędnych parametrów transmisji. Mechanizm QoS sterowania ruchem PTZ w sieciowych produktach wizyjnych firmy Axis jest obsługiwany przez kontrolkę ActiveX AXIS Media Control (AMC), która jest instalowana automatycznie przy pierwszym uzyskaniu dostępu do produktu Axis za pomocą przeglądarki Microsoft Internet Explorer.

5.7. Więcej informacji o technologiach i urządzeniach sieciowych

Koncentratory, przełączniki i mosty *(hubs, switches and bridges)*

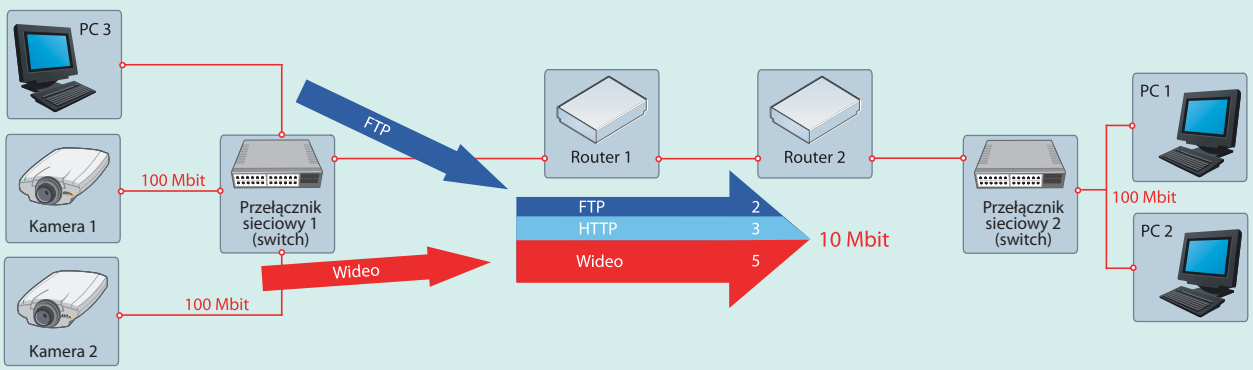
Urządzenia te są stosowane jako skrzynki przyłączeniowe, umożliwiające różnym elementom systemu współużytkowanie jednego połączenia ethernetowego. Do jednego koncentratora można podłączyć zwykle od 5 do 24 urządzeń. Jeżeli używanych jest więcej urządzeń, można dodać kolejny koncentrator. W celu przyspieszenia sieci można

Scenariusz QoS



Rys. 1.: Sieć zwykła (bez mechanizmu QoS)

W tym przykładzie PC1 czuwa nad dwoma strumieniami wizji z kamer 1 i 2; obie kamery przesyłają strumień danych z szybkością 2,5 Mb/s. Nagle PC2 rozpoczyna transfer plików z PC3. W tym scenariuszu transfer plików będzie próbował wykorzystać pełną przepustowość 10 Mb/s pomiędzy routerami 1 i 2, natomiast strumienie wideo będą próbowały zachować swoją całkowitą szybkość transmisji wynoszącą 5 Mb/s. Przepustowość przypisana systemowi dozorowemu nie może być już zagwarantowana, a liczba klatek na sekundę prawdopodobnie spadnie. W najgorszym przypadku ruch FTP wykorzysta całą dostępną przepustowość.



Rys. 2.: Sieć z wykorzystaniem mechanizmu QoS

Router 1 został tak skonfigurowany, aby przeznaczyć maksymalnie 5 Mb/s z dostępnych 10 Mb/s na przesyłanie strumienia wideo. Ruch FTP może wykorzystywać maksymalnie 2 Mb/s, a HTTP i wszelki inny ruch – maksymalnie 3 Mb/s. Dzięki temu podziałowi strumienie wideo będą zawsze dysponowały konieczną przepustowością. Transfer plików jest uważany za mniej ważny i uzyskuje mniejszą przepustowość, nadal jednak będzie dostępna przepustowość wykorzystywana do przeglądania stron internetowych i na inny ruch. Należy zwrócić uwagę, że te wartości maksymalne mają zastosowanie wtedy, gdy sieć jest przeciążona. Jeżeli część przepustowości nie jest wykorzystywana, może zostać użyta przez inny typ ruchu.

użyć koncentratorów przełączanych, umożliwiających jednoczesne przesyłanie wielu pakietów danych.

Bramy i routery *(gateways and routers)*

Bramy i routery są przekaźnikami pakietów działającymi w warstwie 3. sieci (w warstwie IP)*. Decyzje dotyczące przekazywania pakietów są podejmowane na podstawie adresów IP i tablic tras IP. Brama umożliwia połączenie dwóch sieci o odmiennych technologiach w jedną. Na przykład sieć Ethernet może być połączona z siecią typu Token Ring.

Routery NAT

Wszystkie urządzenia łączące się bezpośrednio z Internetem muszą mieć unikatowy publiczny adres IP. Publiczne adresy IP są sprzedawane przez dostawców usług internetowych. Urządzenie NAT *(Network Address Translator)* umożliwia połączenie sieci LAN z adresami prywatnymi z Internetem poprzez dokonanie translacji (mapowania) wewnętrznych adresów prywatnych na adresy publiczne.

Bramy *(gateways)*

Bramy stanowią wygodny sposób tworzenia sieci lokalnej. Działają jako połączenie routera, przełącznika i urządzenia NAT; są oferowane przez wielu producentów.

Serwery DHCP

Zarządzanie adresami IP dużej liczby urządzeń w sieci zajmuje sporo czasu. W celu skrócenia tego czasu i utrzymania jak najmniejszej liczby adresów IP można zastosować serwer DHCP. Ten typ serwera automatycznie przypisuje adresy IP urządzeniom, gdy podłączają się do sieci.

Serwery nazw domen DNS *(Domain Name Server)*

W większych sieciach jest instalowany serwer nazw domen. Jest to dosłownie serwer „nazw". Przypisuje nazwy do odpowiednich adresów IP i zapamiętuje je. Na przykład kamera sieciowa monitorująca drzwi może być łatwiej zapamiętana za pomocą słowa „drzwi" niż adresu internetowego, np. 192.36.253.80.

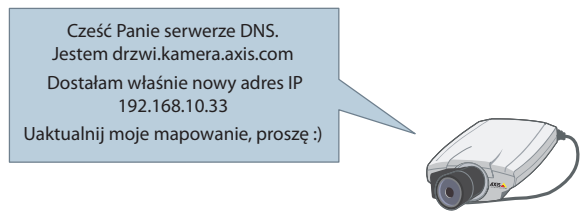
Zapora *(firewall)*

Zapora służy do ochrony przed nieuprawnionym dostępem do i z sieci prywatnej. Zapory mogą być instalowane sprzętowo, programowo lub jako kombinacja obu tych typów. Zapory stosuje się często w celu uniemożliwienia nieuprawnionym użytkownikom Internetu dostępu do sieci prywatnych podłączonych do Internetu, zwłaszcza sieci intranetowych. Wszystkie wiadomości wchodzące lub opuszczające intranet przechodzą przez zaporę, która sprawdza je i blokuje te, które nie spełniają określonych kryteriów bezpieczeństwa. Dzięki zastosowaniu zapory można np. upewnić się, że terminale wizyjne mają dostęp do kamer, podczas gdy komunikacja komputerów z kamerami będzie blokowana.

DDNS i dynamiczne adresy IP

Dynamiczne DNS to metoda zachowania nazwy domeny powiązanej ze zmiennym adresem IP, jako że nie wszystkie komputery używają statycznych adresów IP. Zwykle gdy użytkownik łączy się z Internetem, jego dostawca usług internetowych przypisuje mu nieużywany adres IP z puli adresów IP; adres ten jest stosowany tylko podczas konkretnego połączenia. Ta metoda dynamicznego przypisywania adresów rozszerza użyteczną pulę dostępnych adresów IP. Dostawca usług dynamicznego DNS używa specjalnego programu, który jest uruchamiany na komputerze użytkownika, kontaktując się z usługą DNS za każdym razem, gdy adres IP przypisany przez dostawcę usług internetowych zmieni się, a następnie aktualizuje bazę danych DNS w celu uwzględnienia zmiany adresu IP. W ten sposób nawet gdy adres IP nazwy domeny często się zmienia, inni użytkownicy nie muszą znać zmienionego adresu IP, aby połączyć się z danym komputerem.

W sieciowych systemach wizyjnych kamera obserwująca drzwi wejściowe może być łatwo zapamiętana jako np. „drzwi.kamera.axis.com". W przypadku stosowania DHCP adres kamery IP może się jednak zmieniać w czasie. Tak więc odwzorowanie nazwy „drzwi.kamera.axis.com" na adres IP kamery „192.36.253.80" po jakimś czasie może być nieaktualne. DDNS zapewnia rozwiązanie tego problemu: za każdym razem, gdy kamera zmieni adres IP, skontaktuje się z serwerem DNS i uaktualni odwzorowanie.



SNMP

Protokół SNMP *(Simple Network Management Protocol)* jest zestawem protokołów do zarządzania złożonymi sieciami oraz do zdalnego sterowania i zarządzania urządzeniami podłączonymi do sieci.

IPSec

Protokół IPSec *(IP Security)* składa się z zestawu protokołów obsługujących bezpieczną wymianę pakietów w warstwie IP. Zestaw protokołów IPsec jest rozpowszechniony w prywatnych sieciach wirtualnych (VPN).

UPnP

Standard UPnP *(Universal Plug and Play)* to architektura sieciowa zapewniająca zgodność urządzeń sieciowych, peryferyjnych i oprogramowania ponad 400 dystrybutorów, będących członkami Universal Plug and Play Forum. Standard UPnP działa w sieciach przewodowych i bezprzewodowych; może być obsługiwany przez dowolny system operacyjny. Umożliwia łatwe podłączanie urządzeń oraz upraszcza wdrażanie sieci w domu i firmie.

UPnP jest najczęściej wykorzystywany do wykrywania kamer sieciowych. Po pierwszym podłączeniu kamery standard ten może pobrać z serwera DHCP adres, którego użytkownik w ogóle nie musi znać. Za pomocą UPnP można wyszukiwać kamery i wyświetlać je w wyskakujących oknach.

Więcej informacji na temat technologii i urządzeń sieciowych znajdują się na stronie internetowej:
www.axis.com/products/video/about_networkvideo/

* Od red.: W schemacie budowy sieci wyróżnia się kolejne jej warstwy: fizyczną (fizyczne przesyłania danych, np. kablami), łącza danych (adresowanie danych uwzględniające topologię sieci) oraz warstwę sieci (zapewniającą łączność i wybór ścieżek między dwoma hostami dzięki definiowaniu sposobu przesyłu danych).