



**Tomasz Żuk**  
**UTC Fire & Security Polska Sp. z o.o.**  
 ul. Sadowa 8, 80-771 Gdańsk  
 tel.: (58) 301-38-31, 760-64-80  
 faks: (58) 301-14-36  
 www.utcfireandsecurity.com



W dobie bezprecedensowego upowszechniania się sieci komputerowych w różnego rodzaju zastosowaniach dynamicznie rośnie również liczba systemów dozorowych CCTV IP. Wiąże się to z wprowadzaniem coraz doskonalszych i bardziej zaawansowanych kamer oraz rejestratorów IP. Olbrzymia ilość danych, jakie muszą zostać przesłane w systemach CCTV IP, sprawia, że sieć – jej wydajność, niezawodność i przede wszystkim bezpieczeństwo – staje się kluczowym czynnikiem, z którym muszą zmierzyć się projektanci i instalatorzy. Bezwzględnym wymogiem jest posiadanie wiedzy dotyczącej wymagań stawianych poszczególnym przełącznikom, by sieć mogła sprostać wysokim wymaganiom systemów CCTV IP.

# KRYTERIA DOBORU URZĄDZEŃ SIECIOWYCH DO SYSTEMÓW DOZOROWYCH CCTV IP

Dobór właściwych przełączników trzeba rozpocząć od określenia wymagań funkcjonalnych stawianych poszczególnym urządzeniom sieciowym w poszczególnych punktach sieci. Zacznijmy od poznania modelu opartego na cechach funkcjonalnych przełączników, zwanego modelem hierarchicznym. Choć nazwa tego sposobu prezentowania funkcjonalności sieci brzmi poważnie, sprowadza się on w zasadzie do podziału przełączników, z których jest zbudowana sieć, na trzy warstwy:

- dostępową – do której wpina się wszystkie urządzenia końcowe,
- dystrybucyjnej – do której trafia ruch zebrany w urządzeniach dostępowych,

- rdzenia – której zadaniem jest możliwie szybka wymiana danych pomiędzy poszczególnymi węzłami sieci.

Każda warstwa sieci charakteryzuje się innymi wymaganiami, a co za tym idzie innymi wymaganiami muszą charakteryzować się przełączniki stosowane w poszczególnych warstwach.

## PRZEŁĄCZNIKI DOSTĘPOWE

W pierwszej warstwie funkcjonalnej (*access-layer*) znajdują się przełączniki, których zadaniem jest wpięcie urządzeń końcowych (np. kamery) do sieci IP. Ponieważ kamera standardowej rozdzielczości jest w stanie wygenerować ruch na poziomie kilku MB/s, prędkości portów przełączników dostępowych,

do których są podłączone, nie muszą być duże. Jednak ze względu na pokaźną liczbę urządzeń pożądaną cechą przełączników jest duże upakowanie portów, dzięki czemu koszt pojedynczego portu maleje. Ważną i chętnie wykorzystaną funkcją jest także dostępność zasilania PoE. Umożliwia ono zasilanie kamer bez prowadzenia dodatkowych przewodów zasilających.

Prędkości pojedynczych portów są co prawda niewielkie, ale jeżeli pomnożyć niewielkie prędkości przez dużą liczbę portów, uzyskuje się spore ilości danych. Dlatego przełączniki dostępowe powinny umożliwiać skalowanie szybkości połączenia do kolejnej warstwy. Realizuje się to za pomocą mechanizmów agre-

Rys. 1. Profesjonalne przełączniki dostępowe IFS



Rys. 2. Przemysłowy przełącznik dostępowy NS3552-8P-2S



Rys. 3. Jednokanałowy konwerter światłowodowy MCR300-1T/1S



Rys. 4. Moduł wzmacniacza sygnału Ethernet POE302-EX

gacji, czyli łączenia kilku portów fizycznych w duży link logiczny, będący sumą przepustowości poszczególnych portów składowych. Służą do tego dedykowane protokoły, np. LACP, które niejako przy okazji realizują także funkcję redundancji, zabezpieczającą przed utratą komunikacji w razie awarii jednego z portów składowych agregowanego linku.

Przełączniki warstwy dostępowej muszą także spełniać niezwykle istotne zadanie zabezpieczenia sieci przed nieautoryzowanym dostępem i ewentualnym sabotażem. Profesjonalne przełączniki stosowane w warstwie dostępowej udostępniają funkcje podnoszące poziom bezpieczeństwa sieci. Są to m.in.:

- **listy dostępowe ACL (Access Control List)** – mechanizm bezpieczeństwa polegający na utworzeniu grupy reguł (filtrów) opisujących sposób obsługi ruchu pochodzącego od pojedynczego użytkownika lub grupy użytkowników i przypisania tych reguł do poszczególnych portów w przełączniku. Każdy pakiet przychodzący do interfejsu przełącznika jest sprawdzany pod kątem spełnienia poszczególnych reguł i jedynie te pakiety, które spełnią odpowiednie kryteria, zostaną obsłużone przez przełącznik. Do filtrowania ruchu mogą być wykorzystane takie elementy, jak adresy IP oraz MAC nadawcy i odbiorcy pakietu, typ ramki (ARP, Ethernet, IPv4 itp.), numer VLAN czy nawet rodzaj protokołu, jakim są wysyłane (ICMP,

UDP, TCP itp.). Implementacja list dostępowych może przyjmować skomplikowane formy, szczególnie w sytuacji, gdy są im nadawane priorytety pod kątem obsługi różnego rodzaju ruchu sieciowego. Listy dostępowe działają podobnie jak znane z wielu rozwiązań informatycznych ściany ogniowe (*firewall*);

- **VLAN** – przypisywanie poszczególnych portów (a więc także urządzeń podłączonych do tych portów) do poszczególnych sieci wirtualnych. Zasada pracy wynikająca z konstrukcji Ethernetu mówi, że tylko urządzenia należące do jednej sieci (fizycznej lub wirtualnej) mogą się komunikować bezpośrednio ze sobą. Umieszczając wszystkie kamery w jednej sieci wirtualnej i przypisując pozostałe porty przełącznika do innej sieci wirtualnej, osoby nieautoryzowane nie mają dostępu do kamer;
- **port security** – zespół mechanizmów umożliwiających tworzenie list autoryzowanych adresów MAC, które mogą nawiązać komunikację z przełącznikiem. Jedynie urządzenia, które znajdują się na listach przypisanych do wskazanych portów, mogą się na tych portach (i tylko na nich) komunikować. Inne próby nawiązania komunikacji są odrzucane;
- **uwierzytelnienie** – często stosowanym mechanizmem znacząco zwiększającym poziom bezpieczeństwa jest uwierzytelnienie

urządzeń podłączonych do przełącznika na etapie nawiązywania połączenia. Powszechnym rozwiązaniem jest stosowanie protokołu 802.1x, który zapewnia bezpieczne i scentralizowane uwierzytelnianie użytkowników i urządzeń. Zasada działania protokołu 802.x polega na tym, że zanim przełącznik umożliwi nawiązanie komunikacji z innym urządzeniem w sieci, poprosi o podanie danych (loginu i hasła) umożliwiających potwierdzenie, z kim lub czym ma do czynienia. Dane te są wysyłane do specjalnego serwera, np. RADIUS (*Remote Authentication Dial In User Service*). Jeżeli serwer potwierdzi, że dane urządzenie jest uwierzytelnione, przełącznik pozwoli na dalszą komunikację. Do czasu poprawnego uwierzytelnienia przełącznik blokuje wszelką komunikację z urządzeniem.

Specyfika systemów dozorowych CCTV IP wymusza stosowanie w warstwie dostępowej różnych rozwiązań umożliwiających wykonanie niestandardowej topologii fizycznej. O ile w typowej serwerowni wszystkie urządzenia dostępowe (np. komputery, routery, firewalles sprzętowe) są skupione w jednym miejscu i odległość do najbliższego punktu dostępowego jest niewielka, o tyle w przypadku systemów CCTV IP często zachodzi konieczność podłączenia pojedynczych kamer wyniesionych na znaczną odległość do struktury sieciowej. W tym celu stosuje się niewielkie przełączniki przemysłowe, najczęściej posiadające

możliwość montaż na szynie DIN w lokalnych rozdzielnicach elektrycznych. Tego typu przełączniki są zwykle wykonane w sposób pozwalający na ich wykorzystanie w niesprzyjających warunkach atmosferycznych (kurz, szerszy zakres temperatury pracy). Przykładem takiego urządzenia jest przełącznik NS3552-8P-2S (rys. 2.).

Do podłączenia pojedynczych urządzeń wyniesionych na znaczne odległości standardowo stosuje się dwa rozwiązania. Pierwsze polega na zastosowaniu konwerterów światłowodowych, umożliwiających wydłużenie pojedynczej nitki sieci na odległość nawet kilkudziesięciu kilometrów (rys. 3). Konwertery mogą pracować ze światłowodami zarówno jedno-, jak i wielomodowych.

Tam, gdzie wymagane odległości sięgają kilkuset metrów, a budżet lub możliwości techniczne nie pozwalają na użycie światłowodu, stosuje się moduły wzmacniaczy sygnału Ethernet. Przykładem takiego urządzenia jest moduł POE302-EX (rys. 4), który umożliwia łączenie trzech modułów w kaskadzie, dzięki czemu można uzyskać pojedynczą linię Ethernet o długości do 400 m.

Ciekawostką jest fakt, że moduły wzmacniaczy POE302-EX nie wymagają dodatkowego zasilania lokalnego (są zasilane za pomocą PoE), a ponadto na końcu nitki wciąż istnieje możliwość zasilania kamery za pomocą technologii PoE.

### PRZEŁĄCZNIKI DYSTRYBUCYJNE

W warstwie drugiej, dystrybucji (*distribution-layer*), wymogi stawiane przełącznikom są nieco inne. Tutaj ruch wpływający z pojedynczych portów jest równy sumie ruchu poszczególnych portów przełączników dostępowych. Każdy przełącznik dostępowy agreguje (sumuje) ruch ze wszystkich swoich portów dostępowych i przesyła go do pojedynczego portu przełącznika warstwy dystrybucji.

Z powyższego wynika, że jedno z podstawowych wymagań dotyczy prędkości matrycy przełączającej przełącznika. Liczba pojedynczych portów oraz wyposażenie ich w funkcję PoE nie jest kluczowe. Ważne, aby przełącznik mógł agregować pojedyncze łącza w grupy agregowane za pomocą agregacji statycznych (*Static Aggregation*) lub przy użyciu szybkich protokołów agregujących (LACP lub PAGP).

Istotną cechą jest także dostępność szybkich portów połączeniowych do innych przełączników warstwy dystrybucji, zwanych uplinkami. Powszechnie są tu stosowane grupy agregowane o prędkości kilku Gb/s, a nierzadko także szybkie połączenia o prędkości 10 GB/s – szczególnie do wykonywania wysokowydajnych połączeń wielokrotnych do urządzeń warstwy rdzenia.

Z punktu widzenia funkcjonalności co do zasady w warstwie dystrybucji następuje terminacja (domykanie) VLAN-ów, czyli usuwanie znaczników VLAN ze wszystkich pakietów, które trafiają do warstwy niższej. Wynika to z fak-

Rys. 5. Przełącznik dystrybucyjny NS3702-24P-4S



Rys. 6. Ultraszybkie przełączniki rdzeniowe IFS



tu, że przełączniki z warstwy rdzenia mają tak dużo danych do przesłania, że nie mają czasu na „zagłądanie” do każdego z pakietów w celu określenia, do jakiego VLAN danych należy pakiet.

Przełączniki mają często implementowane mechanizmy związane z QoS (*Quality Of Service*) umożliwiające nadawanie priorytetu ruchowi sieciowemu w celu określenia, jaki ruch należy obsłużyć w pierwszej kolejności. W zależności od tego, z jakiego źródła dany ruch pochodzi, przełącznik może go stosownie oznaczyć i obsłużyć w kolejce standardowej lub priorytetowej (szybszej). Daje to możliwość realnego wpływania na sposób obsługi transmisji.

### PRZEŁĄCZNIKI RDZENIA

Przełączniki stosowane w warstwie rdzenia (*core-layer*) mają wykonywać jedno kluczowe zadanie: jak najszybciej obsłużyć i przesłać możliwie największą ilość danych. Do tego celu stosuje się najszybsze, najbardziej zaawansowane przełączniki wyposażone najczęściej w szybkie łącza światłowodowe o prędkości 10 Gb/s.

Konieczność przesyłania ogromnych ilości danych oraz najczęściej bliska lokalizacja fizyczna tych urządzeń powoduje, że często do połączeń pomiędzy tymi urządzeniami stosuje się specjalne złącza (czołowi producenci opracowali w tym zakresie własne standardy i rozwiązania najczęściej niekompatybilne z innymi), zwane stosami (*STACK*). Urządzenia połączone w stos potrafią przesyłać dane między sobą z prędkością sięgającą kilkudziesięciu (a w niektórych przypadkach nawet kilkuset) Gb/s.

Co również istotne z punktu widzenia zarządzania, połączone w stos zachowują się jak jeden przełącznik o znacznie większym zagęszczeniu portów. Oznacza to, że wszystkie przełączniki w stosie są dostępne pod wspólnym adresem IP i można nimi zarządzać za pomocą jednego interfejsu operacyjnego.

Częstym rozwiązaniem wykorzystywanym w tej warstwie, wynikającym z konieczności

uzyskania dużych przepustowości, jest użycie przełączników o dużej liczbie portów światłowodowych. W innych warstwach stosuje się najczęściej urządzenia z przewagą złączy miedzianych RJ45 (np. 24 porty RJ25 i 2/4 porty SFP), tymczasem w warstwie rdzenia często działają urządzenia mające 24 porty SFP oraz 4/8 portów RJ45. Urządzenia te pełnią funkcję koncentratorów światłowodowych, umożliwiających koncentrowanie ruchu z wielu przełączników warstw wyższych połączonych za pomocą agregowanych połączeń światłowodowych.

Alternatywą dla połączeń typu STACK jest topologia pętli (*RING*). Jest dostępnych kilka protokołów umożliwiających wykonanie fizycznej topologii pętli. Do najpopularniejszych należą RPR (*Resilient Packet Ring*) oraz ERPS (*Ethernet Ring Protection Switching*). W przypadku topologii pętlowych do połączenia przełączników wykorzystuje się standardowe porty RJ45 lub złącza światłowodowe SFP.

Obie te technologie umożliwiają budowanie ultraszybkich pętli światłowodowych, dla których czas przywracania transmisji w przypadku awarii któregośkolwiek z łączy składowych wynosi od kilkunastu do kilkudziesięciu ms.

### UWAGI KOŃCOWE

Zbudowanie szybkiej, niezawodnej i bezpiecznej sieci nie jest łatwe, zwłaszcza w kontekście bardzo wysokich wymagań, jakie stawiają przed nią systemy CCTV IP. Projektowanie należy rozpocząć od określenia potrzeb funkcjonalnych i technicznych, by w kolejnym kroku dobrać i zastosować odpowiednie urządzenia mające wymagane cechy i funkcjonalności.

Choć zagadnienia te pozornie wydają się trudne, ich poznanie jest możliwe, wymaga jedynie przyswojenia odpowiedniej wiedzy, którą najłatwiej zdobyć na profesjonalnych szkoleniach organizowanych przez UTC Fire & Security Polska w ramach Akademii CCTV IP.

Szczegółowe informacje znajdują się na stronie internetowej [www.akademiactvvp.pl](http://www.akademiactvvp.pl)