Co siedzi w chmurce

czyli technologie sieciowe wykorzystywane w systemach dozorowych CCTV

Cz. 1. Przepustowość

Akademia CCTV IP

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

Na wstępie wyjaśnienie – określenie „w chmurce" zostało przeze mnie użyte celowo. Nie chodzi bowiem o trafiającą coraz powszechniej pod strzechy technologię korzystania z usług wyniesionych, dostarczanych przez usługodawców i umieszczonych w chmurze. Chodzi o chmurkę, która często jest symbolem sieci IP wykorzystywanym w projektach i schematach opisujących systemy CCTV IP. Uproszczenie schematu poprzez umieszczenie na nim chmurki zamiast realnej struktury sieciowej wynika zapewne z dość naiwnego przekonania, że jest to ta część systemu, którą zajmują się służby IT w danym obiekcie i one posiadają stosowną wiedzę oraz umiejętności, aby poprawnie przygotować sieć pod kątem współpracy z systemami CCTV. Podejście to jest o tyle niefrasobliwe, że w wielu przypadkach, znając chociażby podstawy działania sieci IP, można bez dodatkowych środków radykalnie zwiększyć jej wydajność i dostosować do wymagań stawianych jej przez systemy CCTV. Nie mówiąc już o prostej diagnostyce, której znajomość może znacznie skrócić proces uruchamiania systemu, co w oczywisty sposób przekłada się na obniżenie kosztów.

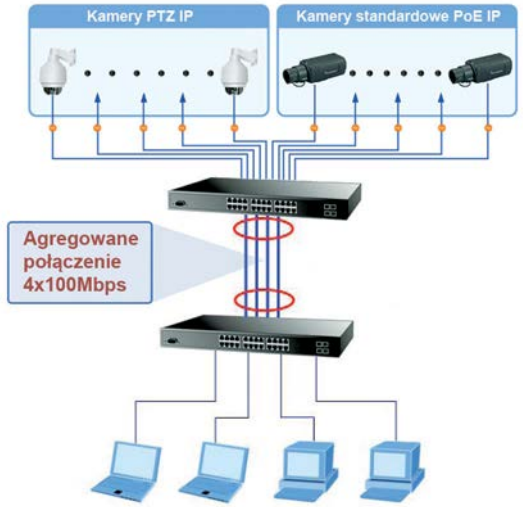
W serii krótkich artykułów przybliżymy ciekawe i przydatne w realnym środowisku funkcje oraz technologie zaimplementowane w przełącznikach sieciowych, wykorzystywanych przy budowaniu sieci IP przeznaczonych do transmisji danych, w tym także cyfrowych strumieni wizyjnych.

PRZEPUSTOWOŚĆ

Punktem wyjścia do analizy stosowanych technologii jest określenie wymagań, jakie stawiają systemy dozorowe CCTV sieciom LAN wykorzystywanym do transmisji strumieni wideo. Te wymagania można określić jednym słowem – przepustowość. Wynika to z faktu, że nawet dla rozdzielczości standardowych, znanych z rozwiązań analogowych (4CIF, D1) ilość informacji zawartej w sygnale wizyjnym jest bardzo duża i znacząco wzrasta dla rozdzielczości megapikselowych. Zależy od ustawień, takich jak liczba klatek na sekundę, rozdzielczość obrazu czy zastosowany algorytm kompresji.

W efekcie zapotrzebowanie na pasmo do przesłania strumienia IP zakodowanego do najnowszego, a co za tym idzie najefektywniejszego formatu H.264 może sięgnąć nawet kilkunastu megabitów na sekundę w odniesieniu do pojedynczego strumienia. Dla starszych i mniej efektywnych algorytmów kompresji pojedynczy strumień może sięgnąć nawet kilkudziesięciu megabitów.

Rys. 1. Agregacja połączeń sieciowych (port trunk)



Wielkość strumieni wideo w zależności od rozdzielczości i szybkości zapisu

Rozdzielczość	H	V	Megapiksele	Szybkość zapisu kl/s dla standardu H.264					
				1	2	5	10	15	25
CIF (PAL)	352	288	0.1	60 kbps	100 kbps	130 kbps	200 kbps	300 kbps	500 kbps
4CIF (PAL)	704	576	0.4	250 kbps	370 kbps	500 kbps	800 kbps	1.1 Mbps	1.7 Mbps
720p	1280	720	0.9	550 kbps	800 kbps	1.1 Mbps	1.8 Mbps	2.5 Mbps	3.9 Mbps
SXGA	1280	1024	1.3	800 kbps	1.2 Mbps	1.6 Mbps	2.6 Mbps	3.5 Mbps	5.5 Mbps
UXGA	1600	1200	1.9	1.2 Mbps	1.7 Mbps	2.3 Mbps	3.7 Mbps	5.2 Mbps	8.1 Mbps
Full HD (1080p)	1920	1080	2.1	1.2 Mbps	1.9 Mbps	2.5 Mbps	4.0 Mbps	5.6 Mbps	8.7 Mbps
WUXGA	1920	1200	2.3	1.4 Mbps	2.1 Mbps	2.8 Mbps	4.5 Mbps	6.2 Mbps	9.7 Mbps
QXGA	2048	1536	3.1	1.9 Mbps	2.8 Mbps	3.8 Mbps	6.1 Mbps	8.5 Mbps	13.0 Mbps

Standard Ethernet stosowany do budowania lokalnych sieci komputerowych definiuje kilka standardów szybkości złączy, które można uzyskać niezależnie od medium, z jakiego są wykonane (miedź, światłowód). Szybkości te wynoszą 10, 100 (obecnie najpopularniejszy standard 100Base-T), 1000 oraz 10 000 Mb/s. Poszczególne prędkości można uzyskać, stosując przewody o odpowiednich kategoriach (im wyższa kategoria, tym większa możliwa przepustowość). Ponieważ większość przełączników sieciowych oferuje od kilku nawet do kilkudziesięciu (najczęściej 8, 16, 24 lub 32) złączy RJ45 pracujących z szybkością 100 Mb/s, sumaryczny ruch do i z urządzenia może sięgnąć kilkuset Mb/s i przewyższyć prędkość pojedynczego portu.

Czy w takiej sytuacji są dostępne proste metody umożliwiające zwiększenie przepustowości oferowanych przez przełączniki lub zmiany charakterystyki ruchu, która poprawiłaby możliwości przesyłania danych? Oczywiście są, a ich włączenie sprowadza się do kilku kliknięć. Oto kilku z nich.

AGREGACJA ŁĄCZY

Istnieje kilka sposobów zwiększenia szybkości wymiany ruchu pomiędzy przełącznikami. Często stosowaną metodą jest połączenie kilku niezależnych portów w logiczny link oznaczony symbolem LAG *(Link Aggregated Group)* – mechanizm ten nazywamy agregacją. Porty, które zostały połączone w grupę, mogą pracować z wykorzystaniem różnych mediów (np. połączenie miedziana + światłowód), ale powinny pracować z tą samą prędkością. Funkcjonalność ta, poza zwiększeniem przepustowości, zapewnia także redundancję połączenia, ponieważ uszkodzenie pojedynczego portu w LAG-u nie powoduje utraty połączenia całości.

Połączenie agregowane może być wykonywana zarówno statycznie, poprzez ręczne wskazanie portów, które mają być zagregowane *(Port Trunk),* jak i automatycznie za pomocą odpowiednich protokołów, np. LACP *(Link Aggregation Control Protocol),* EtherChanel lub SMLT *(Split Multi-Link Trunking).* Zasada działania powyższych protokołów wprawdzie różni się w szczegółach, zasadniczo realizują one identyczną funkcjonalność.

Stosując agregację łączy, można zwiększać przepustowość łączy pomiędzy przełącznikami w newralgicznych miejscach sieci., Wówczas sumaryczna przepustowość jest równa sumie przepustowości poszczególnych portów. Przykładowo, jeżeli jeden link logiczny zostanie zbudowany z czterech linków 1 Gb/s każdy, to sumaryczna osiągnięta w ten sposób przepustowość osiągnie poziom 4 Gb/s.

W zależności od modelu przełącznika, a dokładnie – od protokołu wykorzystywanego do agregowania, istnieją różne ograniczenia dotyczące liczby portów należących do jednego linku logicznego. Najczęściej do jednego linku może należeć od 4 nawet do 16 pracujących równolegle portów.

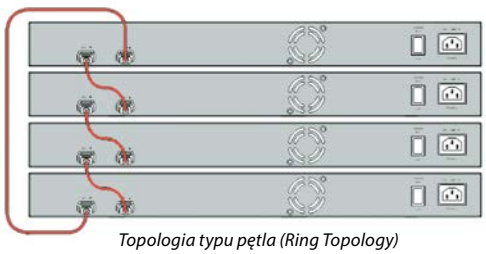
STOSY URZĄDZEŃ *(STACK)*

Inną metodą zapewnienia szybkiej wymiany danych pomiędzy przełącznikami jest tworzenie stosów przełączników (STACK). Tę metodę można stosować jedynie na przełącznikach mających odpowiednie dedykowane złącza – nie może być zrealizowana na normalnie dostępnych portach RJ45. Czołowi producenci opracowali więc własne protokoły i standardy okablowania. Wśród najpowszechniejszych technologii można wymienić np. StackWise czy StackWise Plus firmy Cisco. Urządzenia połączone w pojedynczy stos zachowują się jak jeden przełącznik o znacznie większym zagęszczeniu portów. Oznacza to, że wszystkie przełączniki spięte w stos są dostępne pod wspólnym adresem IP i można zarządzać wszystkimi urządzeniami w stosie za pomocą jednego interfejsu operacyjnego.

Najważniejszą korzyścią płynącą z zastosowania stosu urządzeń jest szybkość wymiany danych pomiędzy urządzeniami w stosie, która może sięgnąć kilkudziesięciu Gb/s, co jest szybkością

Rys. 2. Stos urządzeń sieciowych

Topologia typu szereg (Chaing Topology)



Topologia typu pętla (Ring Topology)

kilkadziesiąt razy większą od szybkości pojedynczego portu.
Z punktu widzenia konfiguracji zestawienie stosu urządzeń sprowadza się najczęściej jedynie do spięcia ich za pomocą odpowiedniego przewodu połączeniowego, a urządzenia automatycznie dokonują reszty ustawień, wybierając spośród siebie urządzenie główne *(Master),* które staje się odpowiedzialne za komunikację i ustawienia wszystkich pozostałych urządzeń. Numer IP tego właśnie urządzenia głównego staje się numerem dla całego stosu przełączników.
Z punktu widzenia topologii sieci połączenie wszystkich przełączników w stosie może być szeregiem *(chain topology)* lub pętlą *(ring topology).* Stosując połączenie typu pętla, zyskuje się dodatkowo funkcję redundancji. Uszkodzenie pojedynczego połączenie nie powoduje utraty komunikacji, może natomiast wpłynąć na znaczne obniżenie przepustowości. W takim przypadku przełączniki mogą sygnalizować stan uszkodzenia do systemów monitorujących.

SIECI WIRTUALNE VLAN

Opisane metody powiększania przepustowości poszczególnych segmentów sieci stanowią jedną z głównych, ale nie jedyną metodą jej optymalizacji pod kątem współpracy ze specyficznymi urządzeniami, jakimi są kamery i rejestratory CCTV.

Rys. 3. Separowanie domen rozgłoszeniowych poprzez zastosowanie VLAN

Potrzeba przesłania dużych ilości danych poprzez nieraz skomplikowane struktury sieciowe oraz zapewnienie bezpieczeństwa tym danym wymaga zastosowania także innych metod. W takich przypadkach powszechnie są wykorzystane sieci wirtualne VLAN *(Virtual Local Area Network),* które umożliwiają pogrupowanie portów przełączników oraz podłączonych do nich odbiorników i nadajników wg zadanych kryteriów, a także tworzenie logicznie zdefiniowanych grup roboczych. Ruch sieciowy pochodzący z każdej z takich grup może być obsługiwany w inny sposób, zależnie od jego priorytetu, może podlegać ograniczeniom lub – jeżeli jest taka potrzeba – można mu przydzielić dodatkowe zasoby sieciowe.
Podstawową korzyścią płynącą z zastosowania VLAN-ów jest możliwość segmentacji sieci LAN i dzielenie jej na mniejsze domeny rozgłoszeniowe. Chcąc wyjaśnić, czym jest domena rozgłoszeniowa (broadcast domain), należy zdefiniować sieć lokalną LAN. Sieć lokalna definiuje zbiór urządzeń, komputerów, przełączników itp., należących do wspólnej przestrzeni administracyjnej i geograficznej – najczęściej jest to budynek lub zbiór budynków.
Struktura taka, pomimo stosunkowo niedużej wielkości w sensie fizycznym, może zawierać olbrzymią liczbę komunikujących się ze sobą urządzeń. Aby zapewnić bezproblemowy dostęp do medium transmisyjnego, sieć lokalna jest podzielona najczęściej za pomocą przełączników na segmenty, w których odbywa się transmisja. Taki właśnie logiczny segment sieci nosi nazwę domeny rozgłoszeniowej. Wszelki ruch rozgłoszeniowy *(broadcast)* – czyli taki, który jest rozsyłany do wszystkich urządzeń w sieci – jest faktycznie ograniczony tylko do urządzeń należących do wspólnej domeny rozgłoszeniowej.

Dlaczego segmentacja sieci fizycznej realizowana za pomocą sieci wirtualnych VLAN ma korzystny wpływ na wydajność jej pracy? Powodów jest kilka:
- segmentacja obniża ilość ruchu broadcastowego i multicastowego (wysyłanego do wszystkich urządzeń w każdym kierunku), co obniża zajętość sieci i podnosi jej efektywność;
- podnosi poziom bezpieczeństwa, ponieważ wymiana ruchu następuje tylko w obrębie grupy Przypadkowe lub celowe wpięcie się komputerem do dowolnego portu przełącznika w celu podsłuchania transmisji, jeżeli port ten nie należy do danego VLAN-u, jest nieskuteczne;
- upraszcza administrowanie, dzięki czemu skraca czas eliminowania potencjalnych błędów konfiguracyjnych, mogących niekorzystnie wpływać na transmisję w obrębie sieci;
- separuje uszkodzenia w domenie rozgłoszeniowej – podział sieci na mniejsze domeny rozgłoszeniowe umożliwia ograniczenie wpływu awarii na pracę pozostałej części sieci.

Przydzielenie portów i użytkowników do grup roboczych nie musi być ograniczone wyłącznie do jednego przełącznika. Można budować sieci wirtualne VLAN obejmujące wiele struktur lokalnych – segmentacja sieci za pomocą VLAN jest możliwa także w sieciach rozległych WAN.

Dla ścisłości należy dodać, że administrowanie urządzeniami i portami należącymi do danego VLAN może się odbywać w jednym z dwóch trybów:
- statycznie – administrator w sposób jawny przypisuje dany port do VLAN-u. Port ten pozostaje w danym VLAN-ie dopóty, dopóki administrator nie zmieni odpowiedniego wpisu w parametrach portu;
- dynamicznie – mechanizm bazujący na adresie MAC urządzenia końcowego. Po podłączeniu urządzenia do portu przełącznik sprawdza w bazie danych przynależność urządzenia do VLAN i ustawia parametry portu do VLAN wskazanego w bazie danych. W celach przeprowadzenia weryfikacji urządzenia konieczne jest wykorzystanie odpowiedniej usługi, np. VMPS *(VLAN Management Policy Serwer).*

UWAGI KOŃCOWE

Wszystkie trzy opisane technologie stanowią jedynie ułamek możliwości, jakie obecnie oferują dostępne na rynku profesjonalne przełączniki sieciowe, ale to właśnie te mechanizmy zastosowane w odpowiednich miejscach umożliwiają znaczące zwiększenie przepustowości sieci.
W sytuacji braku technicznych możliwości zwiększenia przepustowości można także bardziej precyzyjnie zarządzać dostępnymi zasobami poprzez wyodrębnianie i separowanie ruchu z poszczególnych grup roboczych, co dodatkowo poprawia wydajność sieci. Technologie te są łatwe w implementacji i nie powinny nastręczyć problemów wdrożeniowych nawet początkującym administratorom sieci. Warto o nich pamiętać i z nich korzystać. □