

Tomasz Żuk

PRZEŁĄCZNIKI SIECIOWE

KRWIOBIEG SYSTEMU CCTV IP



Rosnąca popularność systemów CCTV IP sprawia, że instalatorzy muszą zmierzyć się z dość trudną materią, jaką jest sieć IP. Trudność ta wynika przede wszystkim z faktu, że urządzenia służące do budowy sieci są naspikowane wieloma funkcjami najczęściej opisywanymi tajemniczo brzmiącymi skrótami. Niemal każda funkcja i technologia zawiera olbrzymią liczbę opcji i ustawień, co sprawia wrażenie skomplikowania. Bez znajomości technologii kryjących się za tymi skrótami trudno zrozumieć sposób działania przełączników oraz sieci jako takiej, choć w gruncie rzeczy jest on dość prosty.

Istnieje kilka kryteriów, wg których dokonuje się klasyfikacji przełączników. Podstawowym jest podział na **przełączniki zarządzalne** i **niezarządzalne**. Pierwsze z nich udostępniają dostęp do panelu administracyjnego, najczęściej w formie konsoli lub strony www, oferującego dodatkowe ustawienia, na które ma wpływ administrator. Przełączniki niezarządzalne zaś pracują zgodnie z ustawieniami fabrycznymi, na które nie ma wpływu i nie można ich korygować. Biorąc pod uwagę dość wysokie i specyficzne wymagania stawiane sieciom przez systemy telewizji dozorowej IP, nie ma wątpliwości, że do ich budowy warto i należy stosować urządzenia zarządzalne, ponieważ umożliwiają one realny wpływ na sposób obsługi ruchu sieciowego.

Z perspektywy zastosowań w systemach telewizji dozorowej IP, sieci powinny spełniać trzy istotne wymogi: przepustowość, niezawodność i bezpieczeństwo.

Pierwszy wymóg wynika z faktu, że strumienie wideo przesyłane z kamer (szczególnie o rozdzielczościach megapikselowych) do rejestratorów mogą osiągać wielkość kilku, a nawet kilkunastu Mb/s. Mnożąc tę wielkość przez liczbę kamer, których nawet w średniej wielkości systemie może być kilkadziesiąt, zapotrzebowanie na pasmo z łatwością osiąga kilkaset Mb/s, a nawet pojedyncze Gb/s ciągłego ruchu! W przeciętnym systemie telewizji dozorowej IP pracuje też kilka stacji graficznych służących do bieżącego monitoringu, przeglądania archiwum czy archiwizacji materiału wideo. Oznacza to, że całkowity ruch sieciowy może być kilkakrotnie większy od oszacowanego. Efektywne przesłanie takiej masy informacji wymaga odpowiednio szybkich urządzeń i dośpejności stosowanych protokołów.

Drugi wymóg – niezawodność – okazuje się szczególnie istotny, kiedy zdamy sobie sprawę, że bez sprawnie działającej sieci cały system telewizji dozorowej staje się bezużyteczny. Niezawodność należy w tym przypadku rozumieć jako takie połączenie odpowiedniej topologii i rozwiązań funkcjonalnych, które zapewnia ciągłość pracy nawet przy uszkodzeniu poszczególnych komponentów sieci. Profesjonalne, zarządzalne przełączniki sieciowe dysponują wieloma mechanizmami i funkcjami, które pozwalają na realizację powyższych wymogów. Co więcej, mogą to robić na wiele różnych sposobów, a od wiedzy i intuicji administratora zależy, który z nich uzna za najlepszy i najefektywniejszy.

Powszechnie stosowane w systemach CCTV IP profesjonalne przełączniki sieciowe oferują użytkownikom wiele technik podnoszących niezawodność. Przykładem może być możliwość pracy w topologii wielokrotnej pętli światłowodowej (standard IEEE 802.17). Technologia ta pozwala na zbudowanie dwóch równoległych, szybkich pętli światłowodowych, które realizują wymianę bardzo dużych ilości danych w dwóch kierunkach równocześnie, a oprócz szybkości oferują także odporność na uszkodzenie (podczas uszkodzenia jednej pętli, druga pozostaje w pełni funkcjonalna).

Z kolei wykorzystując dowolny z dostępnych protokołów agregujących, przełączniki można łączyć kilkoma przewodami, które są „widziane” przez te przełączniki jako pojedyncze linki logiczne. Takie połączenia spełniają oba wymogi: szybkość (przepustowość linku logicznego jest równa sumie przepustowości poszczególnych linków fizycznych) oraz bezpieczeństwo (w sytuacji uszkodzenia pojedynczego linku fizycznego link logiczny

mimo utraty części przepustowości nadal funkcjonuje).

Trzeci wymóg to bezpieczeństwo. Bezpieczeństwo sieci IP może być budowane na wiele sposobów. Opisane wcześniej mechanizmy budowania topologii wielokrotnych są także jednym z aspektów bezpieczeństwa. Istnieje wiele innych sposobów zabezpieczania sieci, począwszy od uwierzytelniania użytkowników i urządzeń, poprzez filtrowanie ruchu pod kątem nadawców i odbiorców czy grupowanie urządzeń pod kątem funkcjonalnym i separowaniu ruchu pomiędzy tak zbudowanymi grupami, skończywszy na tak prozaicznym działaniu, jak wyłączenie nieużywanych portów, by nie mogły posłużyć do nieautoryzowanego dostępu.

Należy zdawać sobie sprawę, że celowe lub przypadkowe sabotowanie sieci jest możliwe, ponieważ sieć IP jest z definicji środowiskiem otwartym – czyli takim, do którego dostęp może być dość łatwy. Konsekwencją tego faktu jest konieczność podjęcia odpowiednich kroków, które przystosują sieć do wymogów CCTV IP, zabezpieczając ją przed nieautoryzowanym dostępem.

Nie trzeba być ekspertem z zakresu sieci IP, by realnie wpływać na bezpieczeństwo i niezawodność sieci, a co za tym idzie także systemów CCTV, które na tej sieci opierają swoje funkcjonowanie.

Przemyślane wykorzystanie chociażby kilku podstawowych mechanizmów oraz sumienne stosowanie dobrych praktyk budowy sieci IP gwarantuje uzyskanie szybkich i niezawodnych struktur sieciowych. Będą one mogły z łatwością sprostać wysokim wymaganiom stawianym przez systemy telewizji dozorowej IP. ●