

CO SIEDZI W CHMURCE?

„QoS (Quality of Service – jakość usługi) to (...) całość charakterystyk usługi telekomunikacyjnej, stanowiących podstawę do wypełnienia wyrażonych i zaspokajanych potrzeb użytkownika tej usługi” – tak krótko i lakonicznie popularny portal Wikipedia definiuje bogaty zestaw mechanizmów i funkcji, które mają ogromny wpływ na efektywność działania sieci. Jednocześnie podręcznik Cisco *Enterprise QoS Solution Reference Network Design Guide* ma bagatela ponad 330 stron. Obszerność, tej drugiej publikacji świadczy o tym, z jak skomplikowaną materią mamy do czynienia. Myślę jednak, że mimo ograniczonych ram niniejszego artykułu warto pokusić się o bliższe przyjrzenie się temu ciekawemu zagadnieniu zwłaszcza, że podstawowe mechanizmy QoS mogą być z powodzeniem wykorzystywane nawet przed początkujących adeptów trudnej sztuki administrowania sieciami IP. Jak więc działa QoS?

TECHNOLOGIE SIECIOWE WYKORZYSTYWANE W SYSTEMACH CCTV

Cz. 3. QoS – JAKOŚĆ USŁUGI

DEFINICJA QoS

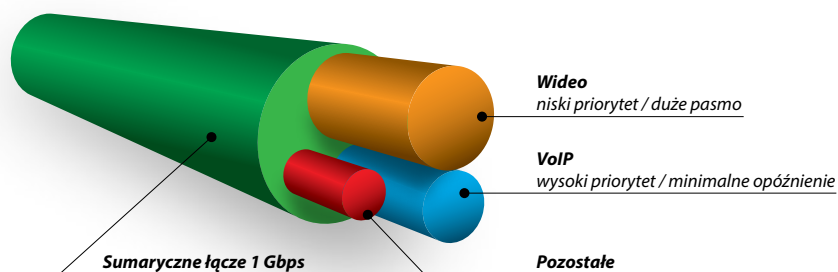
Problem z QoS wynika z faktu, że w skład mechanizmów i funkcji służących do sterowania i zarządzania ruchem w sieci należy wiele, z reguły skomplikowanych (posiadających wiele opcji) protokołów, które wzajemnie na siebie wpływają, nie zawsze w oczekiwany sposób. Od administratorów sieci zajmujących się QoS wymaga się – poza gruntowną wiedzą, znajomością protokołów i pełnego spektrum ich opcji – także intuicji pozwalającej na sprawne ich wykorzystanie. Można bowiem osiągnąć podobne efekty w różny sposób (za pomocą różnych mechanizmów), a niuanse decydują o tym, który z nich jest wydajniejszy i w jakiej sytuacji.

Należy także pamiętać, że administratorzy z reguły operują na czymś, co trudno sklasyfikować – na ruchu sieciowym, który często pochodzi z wielu źródeł z reguły znacząco róż-

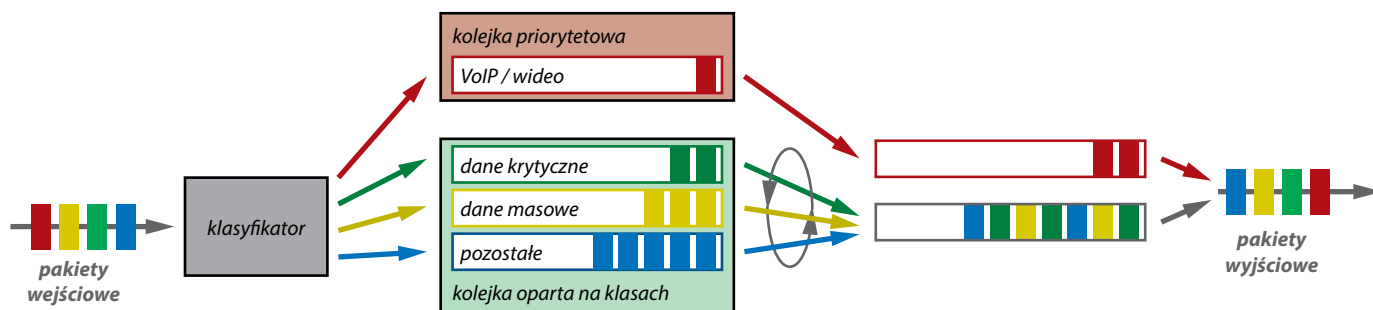
niących się, a ponadto ruch ten jest zmienny w czasie. W tym przypadku osoby zajmujące się sieciami głównie pod kątem zastosowań do systemów CCTV mają ułatwione zadanie, ponieważ tutaj ruch jest bardziej uporządkowany (pod warunkiem że jest to wyizolowana to-

pologia sieciowa) i nie zawieruszły się w niej żadne inne dane. Czym zatem jest mityczne *Quality of Service*?

Quality of Service (QoS) jest zestawem zaawansowanych mechanizmów służących do ustalenia priorytetu ruchu sieciowego, co pozwala na



Rys.1. Quality of Service – podział pasma i ustalenie priorytetu wg rodzaju ruchu w sieci



Rys. 2. Klasyfikowanie pakietów do poszczególnych poziomów obsługi

efektywne zarządzanie przesyłaniem danych w sieci. QoS umożliwia przypisywanie wszystkich przesyłanych danych wg zdefiniowanych kryteriów do różnego rodzaju klas i różne sposoby obsługi w zależności od tego, do której klasy dane należą.

Oto przykład. Porównajmy dwa rodzaje ruchu – połączenie telefoniczne VoIP (*Voice over IP*) oraz zdalną archiwizację materiału wideo z rejestratora na macierz sieciową. W pierwszym wymagane pasmo nie jest duże (sięga kilkunastu kb/s), opóźnienie transmisji natomiast musi być minimalne, aby rozmawiające ze sobą osoby nie odczuwały niewygodny związanej z opóźnieniami słyszanych odpowiedzi. Drugi przypadek opisuje rodzaj aktywności sieciowej, która zaalokuje maksymalne dostępne pasmo (konieczne jest zarchiwizowanie bardzo dużej ilości danych), przy jednoczesnym braku wymagań dotyczących czasu realizacji usługi – w skrajnych przypadkach dopuszcza się chwilowe wstrzymanie transmisji bez negatywnych skutków dla całego procesu. Jeżeli więc oba rodzaje ruchu mają być zrealizowane za pomocą jednego przełącznika, musi on „rozumieć”, z jakim ruchem ma do czynienia, i obsłużyć go w inny sposób.

Każda aplikacja pracująca w środowisku sieciowym wymienia dane z innymi urządzeniami, wysyłając je przez sieć w formie pakietów IP. Podczas wysyłania do ich nagłówków wpisywana jest informacja w postaci znacznika DSCP o tym, jakiego rodzaju dane zawiera dany pakiet. Pakiet trafia do przełącznika, który najpierw kieruje go do klasyfikatora. Klasyfikator weryfikuje typ wpisanych danych i na tej podstawie kieruje go do odpowiedniej kolejki. Współczesne urządzenia sieciowe realizują co najmniej dwie kolejki – priorytetową, oznaczoną jako LLQ (*Low-latency queuing* – kolejowanie o niskim opóźnieniu), do której trafia ruch wymagający możliwie najszybszej obsługi (np. VoIP, interaktywne wideo), oraz kolejkę opartą na klasach CBWFQ (*Class-based weighted fair queuing* – ważone, właściwe kolejowanie oparte na klasach), do której trafiają wszystkie pozostałe typy ruchu. Przełącznik przesyła odebrane pakiety dalej wg kolejności wynikającej z typu ruchu oraz przypisanego mu poziomu usługi, dbając o to, aby w pierwszej kolejności zostały przesłane pakiety znajdujące się w kolejce priorytetowej.

RODZAJE RUCHU W SIECIACH – MODELE KLAS

Dla uporządkowania i unifikacji technologii wykorzystywanych przez urządzenia sieciowe do realizacji zadań QoS firma Cisco, dostawca urządzeń sieciowych, opracowała modele klas ruchu, które obrazują typy ruchu i ich podział ze względu na sposób realizacji QoS. Najbardziej rozbudowany model 11-klasowy, zwany modelem bazowym, zawiera zestaw rekomendacji inżynierów tej firmy, pomagający zapewnić odpowiednią jakość usług sieciowych niezależnie od wykorzystywanych technologii i topologii.

Poszczególne klasy zawierają typy ruchu powszechnie występujące w sieciach LAN i charakteryzujące się różnymi wymaganiami dotyczącymi sposobu obsługi.

Poszczególne klasy zawierają:

1. VoIP – wszelki ruch sieciowy realizujący przesyłanie strumieni audio w czasie rzeczywistym. Dla takiego ruchu wymogi dotyczące obsługi są najbardziej restrykcyjne:

- utrata pakietów poniżej 1%;
- opóźnienie, rozumiane jako czas upływający od momentu wypowiedzenia słowa do jego dotarcia do ucha odbiorcy, nie dłuższe niż 150 ms;
- zniekształcenia sygnału cyfrowego (*Jitter*) poniżej 30 ms;
- gwarantowane pasmo dla pojedynczej transmisji 21-310 kb/s;

2. interaktywne wideo – ruch generowany podczas wideokonferencji. Ponieważ strumień wideokonferencji zawiera także ścieżkę audio, wymogi dotyczące opóźnień i zniekształceń sygnału pozostają takie jak w punkcie 1.:

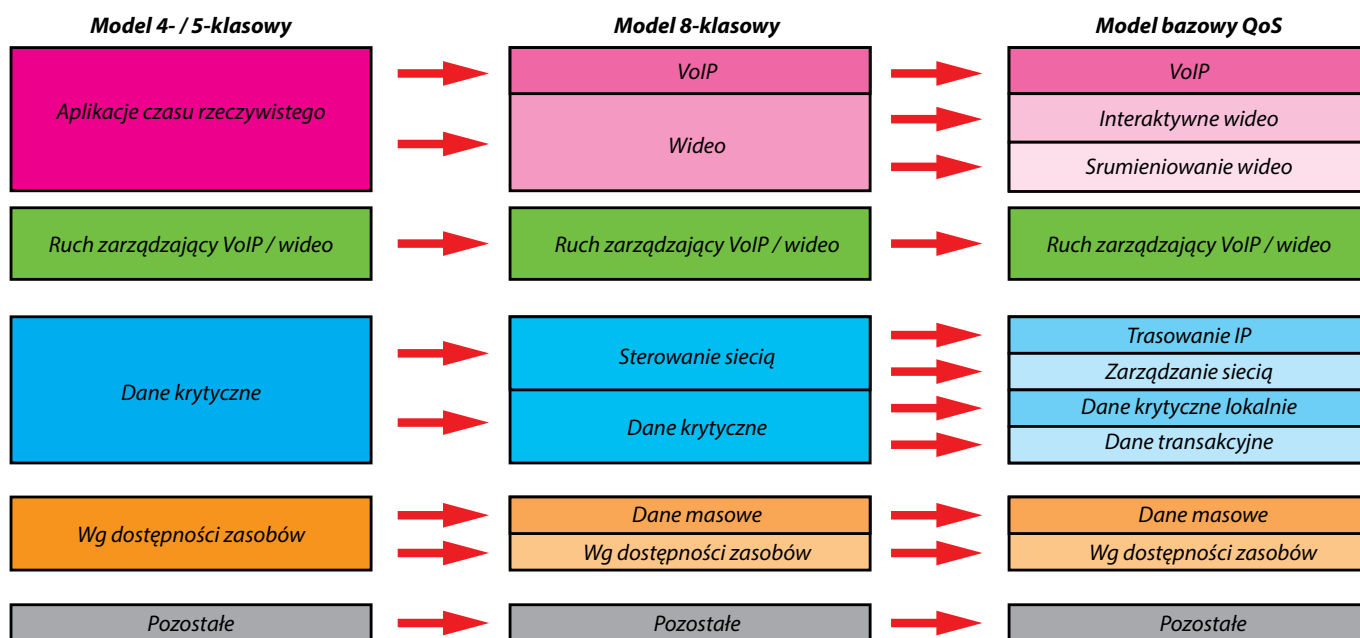
- utrata pakietów poniżej 1%;
- opóźnienie rozumiane, jako czas upływający od momentu wypowiedzenia słowa do jego dotarcia do ucha odbiorcy nie dłuższy niż 150 ms;
- zniekształcenia sygnału (*Jitter*) poniżej 30 ms;
- rezerwa dla dynamicznej zmiany sygnału interaktywnego 20%;

QoS NAJWAŻNIEJSZE POJĘCIA

DSCP (*Differentiated services Code Point*) – specjalnie dodana i oznaczona grupa dodatkowych 6 bitów w nagłówku pakietu IP, umożliwiającą przypisanie temu pakietowi odpowiadającego mu poziomu usług. Każdy przesyłany przez sieć pakiet ma w nagłówku w polu DSCP informację o wymaganym sposobie obsługi (np. bez opóźnień dla VoIP lub wg dostępnych zasobów dla transmisji niekrytycznych itp.)

klasyfikator (*Classifier*) – mechanizm nadający ruchowi sieciowemu odpowiednie priorytety. Klasyfikatory funkcjonują w oparciu o różne kryteria, takie jak typ protokołu, rodzaj aplikacji, adres źródłowy/docelowy i są konfigurowane przez administratorów sieci w różnych punktach sieci. Każdy przychodzący pakiet jest przez mechanizm klasyfikujący analizowany i kierowany do kolejki o odpowiadającym poziomie usługi (*Service Level*)

poziomy usługi (*Service Level*) – definiuje priorytet, z jakim będzie obsługiwany dany rodzaj ruchu. Poziomy usługi są definiowane i modyfikowane przez administratorów urządzeń



Rys. 3. Model bazowy klas obsługi QoS opracowany przez Cisco

3. strumieniowanie wideo – przesyłanie strumieni wideo bez rygoru interaktywności. Tutaj wymogi QoS są już nieco inne:

- utrata pakietów do 5%;
- opóźnienie nie większe niż 4-5 s;
- brak wymagań dla maksymalnego poziomu zniekształceń cyfrowych;
- gwarantowane pasmo (zależne od parametrów przesyłanego strumienia);

4. ruch zarządzający VoIP/wideo – ruch wykorzystywany przez protokoły obsługujące zestawianie i realizację usług VoIP oraz wideokonferencji np. Skinny, SIP, H.323;

5. trasowanie IP – pakiety wysyłane przez wszelkie protokoły wykorzystywane do trasowania (*routing*), np. IGP (*Interior Gateway Protocol*), RIP/RIPv2 (*Routing Information Protocol*), OSPF (*Open Shortest Path First*) czy EIGRP (*Enhanced Interior Gateway Routing Protocol*). Ruch tej klasy wymaga jedynie wyraźnego zagwarantowania pasma na potrzeby realizacji ww. usług;

6. zarządzanie siecią – do realizacji wszelkich protokołów wykorzystywanych do zarządzania siecią, np. SNMP, NTP, Syslog, NFS – wymagana jest jedynie minimalna przepustowość na potrzeby realizacji usług;

7. dane krytyczne lokalnie (transmisja w sieci LAN) – przykładem takiego rodzaju ruchu jest wymiana danych z lokalną bazą danych. Choć globalnie wymiana ruchu z bazami danych jest traktowana jako ruch o niewielkim priorytecie, administrator może taki ruch „oznaczyć” jako „ważny lokalnie” i w ten sposób nadać mu wyższy priorytet;

8. dane transakcyjne – najczęściej są to dane wymieniane pomiędzy poszczególnymi ele-

mentami w aplikacjach klient-serwer, np. Microsoft SQL, IBM Bus 2 Bus, DLSw+ (*Data Link Switching*) czy powszechnie wykorzystywana poczta elektroniczna;

9. dane obsługiwane wg dostępności zasobów – zakwalifikowano dwie podklasy o bardzo podobnych cechach i wymaganiach QoS: „dane masowe” i „dane realizowane wg dostępności zasobów” – to ruch niestawiający w zasadzie żadnych wymagań dotyczących opóźnień czy gwarantowanego pasma. Odbywa się niejako „w tle” pozostałych klas, w sytuacji dostępności zasobów. Przykładem tego typu ruchu jest zdalna archiwizacja bazy danych czy transfer dużych ilości danych z serwera FTP;

10. pozostałe – ruch, który ma najniższe priorytety z punktu widzenia obsługi. Są to najczęściej różnego rodzaju aplikacje P2P (*Peer-To-Peer*) na potrzeby rozrywki, takie jak KaZaa, Morpheus, Grokster, Napster, iMesh oraz – ku wielkiemu rozczarowaniu licznych miłośników rozrywki – gry komputerowe, np. Doom czy Quake.

PRIORYTETOWA OBSŁUGA RUCHU CCTV W PRAKTYCE

Pojawia się następane pytanie: w jaki sposób można wykorzystać mechanizmy QoS do zapewnienia odpowiedniego poziomu usługi w sieciach wykorzystywanych do przesyłania ruchu CCTV. Skonfigurowanie przełącznika do realizacji takiego zadania może okazać się proste. Zarządzalne przełączniki umożliwiają zdefiniowanie dla każdego swojego portu list kontrolnych QCL (*QoS Control List*), które działają na podobnej zasadzie jak listy stosowane w mechanizmach bezpieczeństwa przełączników („sa” nr 6/2013). W ramach list kontrolnych QoS przełącznik może analizować ruch

na danym porcie i nadawać mu odpowiedni priorytet (odpowiednią klasę ruchu) oparty na znaczniku VLAN. Wystarczy wówczas przypisać odpowiednio wysoki priorytet obsługi dla VLAN, w którym pracuje system CCTV, aby ruch w tym VLAN był obsługiwany priorytetowo.

Innym sposobem wykorzystania mechanizmów QoS do wsparcia pracy sieci CCTV jest zagwarantowanie odpowiedniego pasma strumieniom wideo wysyłanym przez kamery. Jest to szczególnie istotne, jeżeli w sieci, w której pracuje system CCTV, działają też innego rodzaju aplikacje. W takim przypadku można tak skonfigurować przełącznik, aby niezależnie od ilości ruchu w sieci rezerwował odpowiednie pasmo dla urządzeń CCTV (kryterium dostępu do zarezerwowanego pasma może być przynależność do VLAN).

UWAGI KOŃCOWE

Opisanie mechanizmów QoS było jednym z większych wyzwań, przed jakimi stanąłem jako autor publikacji dotyczących sieci IP. Wynika to z faktu, że mnogość technologii i mechanizmów funkcjonujących w ramach tego niezwykle szerokiego pojęcia jest przeogromna, a pojemność artykułu nader skromna. Zdaję sobie sprawę, że jedynie zasygnalizowałem tę arcydziełową, ale też trudną tematykę. Mam jednak nadzieję, że zawarte informacje zaciekały Czytelnika i choć o krok przybliżyły do prób samodzielnego skonfigurowania QoS i wykorzystania go w praktyce.

Literatura

1. *The QoS Baseline At-A-Glance*, Cisco Systems, 2005.
2. *Vanguard Applications Ware IP and LAN Feature Protocols – Quality of Service*, Vanguard Networks, 2004
3. *Enterprise QoS Solution Reference Network Design Guide*, Cisco Systems, 2005.
4. *IFS NS3601-24P/4S User Manual*, Interlogix, 2010.