vmware® PRESS

VMware® dla administratorów sieci komputerowych

Christopher Wahl
Steven Pantol

Przedmowa **Ivan Pepelnjak**

Tytuł oryginału: Networking for VMware Administrators

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-0696-7

Authorized translation from the English language edition, entitled: NETWORKING FOR VMWARE ADMINISTRATORS, ISBN 0133511081; by Christopher Wahl and Steve Pantol; published by Pearson Education, Inc, publishing as VMWARE Press.

Wydawnictwo HELION
ul. Kościuszki 1c, 44-100 GLIWICE
tel. 32 231 22 19, 32 230 98 63
e-mail: *helion@helion.pl*
WWW: *http://helion.pl* (księgarnia internetowa, katalog książek)

Drogi Czytelniku!
Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres
http://helion.pl/user/opinie/vmwaad
Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

Spis treści

Część II. Przełączanie wirtualne

Część III. Twoja pamięć masowa znajduje się w mojej sieci: IP Storage

Część IV. Inne scenariusze projektowe

ROZDZIAŁ

9

vSphere Distributed Switch

Kluczowe zagadnienia omówione w tym rozdziale:

- uplinki dvUplink,
- protokół LLDP,
- NetFlow,
- Port Mirroring,
- prywatne sieci VLAN,
- kształtowanie ruchu *egress*,
- *Load Based Teaming*,
- sterowanie operacjami we/wy sieci (NIOC).

Wprowadzenie do przełącznika vSphere Distributed Switch

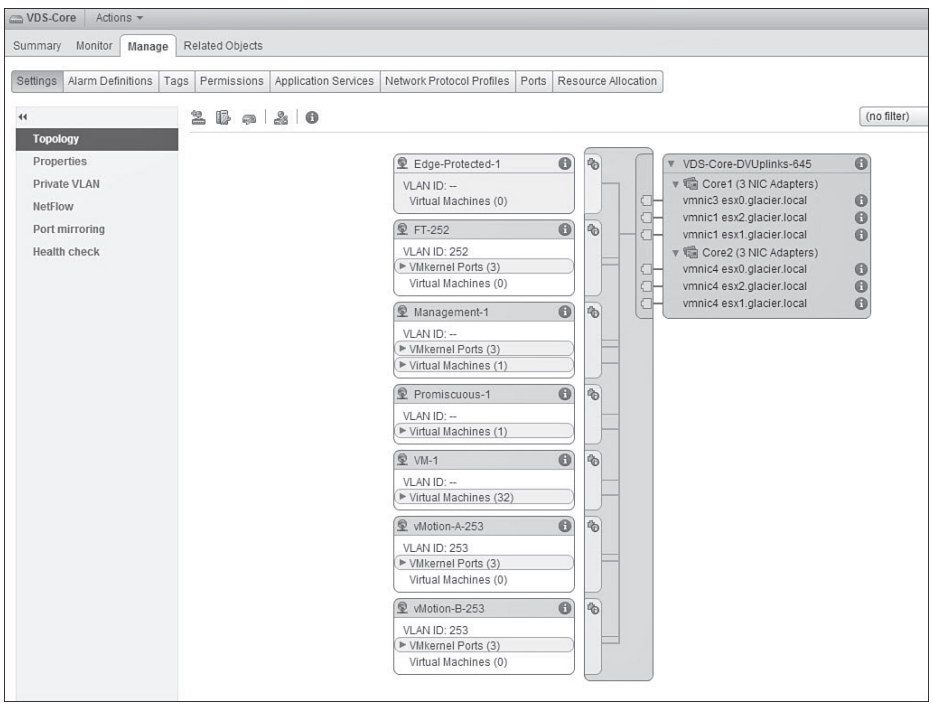
Przełącznik vSphere Distributed Switch (VDS) oferuje Tobie, jako klientowi, dwie główne korzyści. Po pierwsze, VDS zapewnia scentralizowaną płaszczyznę sterowania do zarządzania przełączaniem wirtualnym, zapobiegając konieczności wykonywania wielu niewdzięcznych zadań w codziennej administracji. Po drugie, VDS oferuje bardziej zaawansowane usługi i funkcje niż przełącznik standardowy.

VDS znajduje się pośrodku skali funkcjonalności, udostępniając więcej możliwości niż przełącznik standardowy, ale pozostawiając nieco miejsca dla przełączników innych producentów, takich jak Cisco Nexus 1000V. Przełącznikom typu vSwitch innych producentów poświęcimy więcej uwagi w następnym rozdziale. Na razie skupimy się na przełączniku VDS, różnicach w stosunku do przełącznika standardowego oraz niektórych przyjemnych funkcjach i gadżetach, w jakie został wyposażony.

Płaszczyzna sterowania

Płaszczyzna sterowania przełącznika VDS jest zlokalizowana w warstwie vCenter stosu. Oznacza to, że vCenter jest wehikułem wykorzystywanym do tworzenia, modyfikowania i usuwania przełączników VDS oraz ich grup portów wirtualnych. Innymi słowy, możesz jednorazowo utworzyć swój przełącznik VDS, a następnie wybrać, które hosty będą go używać. Jest to koncepcja podobna do klastra vSphere. Klaster sam w sobie nie pełni żadnej funkcji. Można skonfigurować opcje *High Availability* (HA) oraz *Distributed Resource Scheduler* (DRS) klastra, ale dopóki nie dodasz do niego kilku hostów, będzie po prostu pełnił funkcję dekoracyjną. Przełącznik VDS jest bezużyteczny do momentu dodania do niego hostów — i dopiero od tej chwili zaczyna działać magia.

Każdy przełącznik VDS ma zdefiniowaną określoną liczbę uplinków. Domyślnie każdy uplink ma nazwę **dvUplink**, po której podawany jest numer uplinku. Można jednak zmienić tę nazwę. Z perspektywy płaszczyzny sterowania nadawanie uplinkom niestandardowych nazw pomaga określić rolę poszczególnych uplinków wykorzystywanych przez każdy host do przenoszenia ruchu w kierunku do przełącznika VDS i w przeciwnym. Podczas dodawania hosta do przełącznika VDS fizyczne porty uplinków mapowane są na logiczne porty dvUplink. Na rysunku 9.1 widoczne są porty dvUplink przełącznika VDS, które wykorzystują niestandardowe nazwy „Core1” i „Core2”.



RYSUNEK 9.1. Porty dvUplink w przełączniku VDS

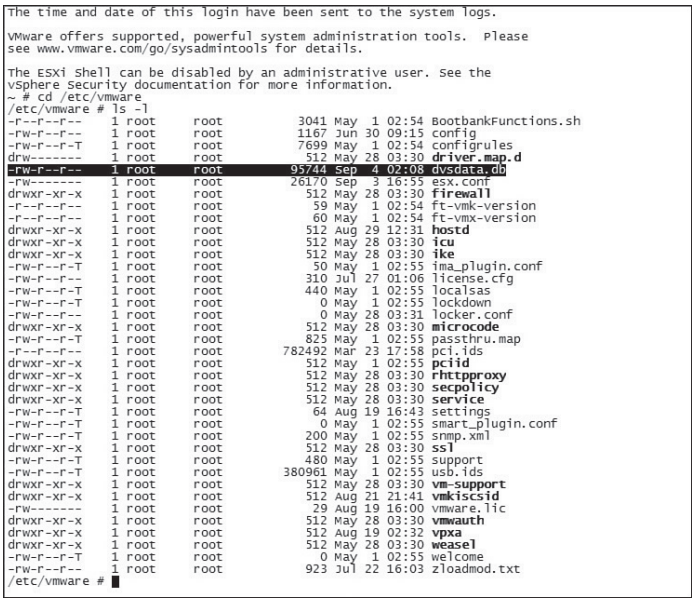
WSKAZÓWKA

Nazywaj swoje uplinki w sposób opisowy, który pomoże Ci w rozwiązywaniu problemów. Z reguły wybieram nazwy związane z zadaniem przełącznika VDS, np. „Core-##" lub „Storage-##". Można również jako podstawę nazewnictwa wykorzystać fizyczną infrastrukturę przełączania, np. „TOR-A" lub „TOR-B", aby rozróżnić, z którym przełącznikiem górnego poziomu w szafie rackowej (ang. *Top-of-Rack* — TOR) się łączysz. Należy unikać używania nazw konkretnych przełączników lub adresów IP, ponieważ te informacje i tak są śledzone przez protokoły CDP lub LLDP. Protokół LLDP zostanie omówiony w dalszej części rozdziału.

Obsługa awarii vCenter

To, że przełączniki VDS są zarządzane poprzez vCenter, może być przyczyną problemów, ponieważ zdaje się to implikować uzależnienie od dostępności vCenter. Można się zastanawiać, co się stanie w wypadku awarii serwera vCenter — wirtualne przełączanie zostanie po prostu zatrzymane?

Krótka odpowiedź brzmi: nie, przełączanie będzie kontynuowane bez zakłóceń. Skoro mamy jednak jeszcze kilkaset stron książki, możemy rozwinąć tę odpowiedź. Chociaż prawdą jest, że mózg przełącznika VDS znajduje się na serwerze vCenter, to w każdym hoście vSphere przechowywana jest w pamięci podręcznej kopia konfiguracji VDS, która jest aktualizowana co pięć minut. Jeśli serwer vCenter ulegnie awarii, host będzie korzystał z tej kopii konfiguracji przełącznika VDS zbuforowanej w pamięci podręcznej. Możesz zalogować się do swojego hosta vSphere za pomocą protokołu SSH i znaleźć ten plik w lokalizacji */etc/vmware/dvsdata.db*. Zbuforowana baza danych została przedstawiona na rysunku 9.2.



RYSUNEK 9.2. Lokalna kopia bazy danych VDS przechowywana w pamięci podręcznej

Gdy serwer vCenter powróci do trybu online, wyświetlonych zostanie kilka błędów informujących o tym, że konfiguracja VDS nie jest zsynchronizowana z niektórymi hostami. Błędy znikną zaraz po tym, gdy konfiguracja VDS z serwera vCenter zostanie wysłana do hosta vSphere podczas regularnego pięciominutowego interwału aktualizacji.

Płaszczyzna danych

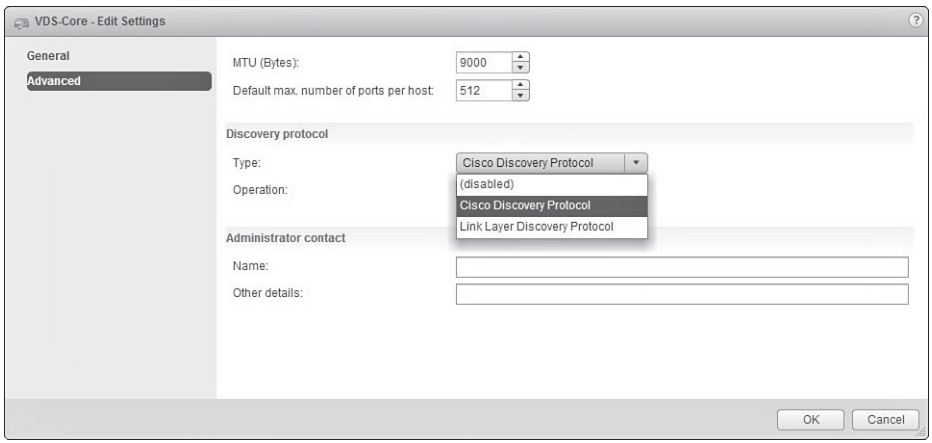
Podobnie jak w wypadku standardowego przełącznika cała aktywność płaszczyzny danych występuje nadal w warstwie hosta. Z założenia żadne dane nie są przesyłane za pośrednictwem serwera vCenter, ponieważ jest on po prostu punktem kontroli. Wszystkie decyzje przełączania nadal podejmowane są w samym hoście na podstawie tych samych zasad warstwy drugiej, które zostały omówione w rozdziale 3.

Monitorowanie

Przełącznik VDS obsługuje zarówno protokół CDP (ang. *Cisco Discovery Protocol*), jak i LLDP (ang. *Link Layer Discovery Protocol*).

Protokół CDP

Jak zapewne pamiętasz, standardowy przełącznik vSwitch obsługuje protokół CDP, ale konfiguracja tej funkcji i zarządzanie nią wymaga skorzystania z interfejsów ESXCLI, PowerCLI lub innych metod wiersza poleceń. W wypadku przełącznika VDS oprócz możliwości włączenia protokołu CDP lub LLDP można również ustawić tryb jednego z tych protokołów (*Listen*, *Advertise* lub *Both*) bezpośrednio z poziomu aplikacji vSphere Client lub vSphere Web Client. Jest to po prostu pole rozwijanej listy w sekcji *Discovery protocol*. Zgrabne, prawda? Wymienione pole rozwijanej listy zostało przedstawione na rysunku 9.3.



RYSUNEK 9.3. Włączenie protokołu CDP w przełączniku VDS za pomocą prostej rozwijanej listy

Protokół LLDP

Do szczęściarzy mogą zaliczyć się ci, którzy nie operują w środowisku przełączania Cisco. VDS obsługuje otwarty standard będący odpowiednikiem CDP, czyli protokół LLDP. Zapewnia on wszystko, czego można oczekiwać od CDP, ale działa na platformach szeregu różnych dostawców. Co ciekawe, obecnie coraz więcej przełączników Cisco również obsługuje protokół LLDP, co pomaga zapewnić heterogeniczność środowiska przełączania.

Jak pokazano na rysunku 9.3, opcję umożliwiającą włączenie protokołu LLDP można znaleźć w tym samym rozwijanym polu, w którym włącza się protokół CDP. Można również skonfigurować jeden z trzech trybów pracy: *Listen*, *Advertise* lub *Both*.

> **WSKAZÓWKA**
>
> Jedno z często pojawiających się pytań dotyczy potrzeby ustawienia trybów *Advertise* lub *Both* dla protokołu LLDP (lub nawet dla CDP) i tego, jakie mogą być wady takiej konfiguracji. Nie spotkaliśmy się jeszcze z żadnymi środowiskami, w których posiadanie dodatkowych informacji na temat danego środowiska (z perspektywy serwera lub sieci) byłoby czymś złym. Chociaż niektóre organizacje będą stosowały politykę zapobiegania włączaniu protokołu LLDP lub CDP w określonych środowiskach, w których ważna jest kwestia zgodności, to w większości wypadków nie będzie to stanowiło problemu. Skonsultuj się najpierw w tym zakresie z zespołami ds. bezpieczeństwa i sieci, ale najprawdopodobniej włączenie widzialności w wirtualnym środowisku sieciowym zostanie uznane za korzystne.

Funkcja NetFlow

Przechodzimy teraz do pewnych funkcji stanowiących wartość dodaną, które naprawdę cieszą użytkowników przełączników VDS. Pierwszą z nich jest dostępna w przełączniku VDS zaawansowana funkcja NetFlow. NetFlow tak naprawdę nie ma wiele wspólnego konkretnie z VMware. Funkcja ta została opracowana przez firmę Cisco i z rozsądnych względów stała się standardowym mechanizmem do przeprowadzania analizy sieci.

W rozdziale 7. wspomniana została koncepcja ruchu szarej strefy, czyli takiego ruchu, który może nigdy nie opuścić hosta. Dzieje się tak dlatego, że zarówno źródłowa, jak i docelowa maszyna wirtualna znajdują się na tym samym hoście. Być może dwie maszyny wirtualne komunikują się ze sobą w tej samej sieci VLAN i na tym samym hoście. W końcu czasem robi się to celowo, aby uniknąć dodatkowego obciążania sieci fizycznej, jak również dlatego, że ruch szarej strefy jest przełączany z wykorzystaniem znacznie większej szybkości procesora lub pamięci RAM hosta niż zapewniają to fizyczne prędkości sieci. NetFlow jest sposobem monitorowania i próbkowania ruchu IP odbywającego się w obrębie przełącznika VDS. Ta konfiguracja jest kontrolowalna aż do poziomu grupy portów. Ruch danych jest przesyłany do kolektora NetFlow, który działa w innym miejscu sieci. Funkcja NetFlow jest powszechnie stosowana w fizycznym świecie, aby pomóc zapewnić widoczność ruchu i ułatwić zrozumienie, kto wysyła jakie dane i gdzie one trafiają.

Funkcja NetFlow dostępna jest w różnych wersjach, od v1 do v10. VMware korzysta z funkcji NetFlow w wersji 10, która jest oparta na protokole IPFIX (ang. *Internet Protocol Flow Information eXport*). IPFIX to w rzeczywistości połączenie NetFlow w wersji 9 z pewnymi standardami stowarzyszenia IETF (ang. *Internet Engineering Task Force*) i z tego względu jest czasem określany jako „NetFlow 9 znormalizowany zgodnie ze standardami IETF". Jeśli czujesz się zdezorientowany tym, że wersja 10 jest czasem nazywana „IPFIX 9", nie jesteś sam. Dla uproszczenia najlepiej jest po prostu stosować nazwę IPFIX, a wszyscy będą wiedzieć, co masz na myśli.

WSKAZÓWKA

vSphere 5.0 wykorzystuje NetFlow w wersji 5, a vSphere 5.1 i nowsze wersje używają IPFIX (wersja 10). Jeśli używasz oprogramowania, które wymaga wersji 5 lub nie obsługuje protokołu IPFIX, możesz chcieć uniknąć aktualizacji hostów vSphere, dopóki nie znajdziesz rozwiązania tego problemu. vSphere 5.1 nie obsługuje NetFlow w wersji 5.

Aby skorzystać z funkcji NetFlow, należy wykonać dwie czynności. Pierwszą z nich jest skonfigurowanie ustawień NetFlow w samym przełączniku VDS, które opiszemy szczegółowo.

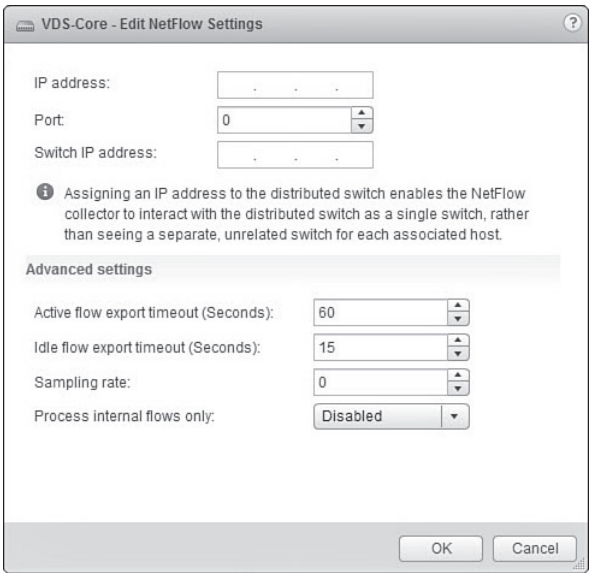
Konfiguracja NetFlow przełącznika jest określana przez następujące elementy:

- ***IP address*** (adres IP). Jest to adres IP kolektora NetFlow, do którego wysyłane są informacje o ruchu.
- ***Port***. Port używany przez kolektor NetFlow. Jest to zazwyczaj port UDP o numerze 2055, ale może się różnić w zależności od producenta zbierającego dane.
- ***Switch IP address*** (adres IP przełącznika). Na początku może to być mylące. W typowym środowisku sprzętowym każdy przełącznik ma jakiś identyfikator IP wykorzystywany do zarządzania. Dzięki przypisaniu za pomocą tego ustawienia adresu IP kolektor NetFlow potraktuje przełącznik VDS jako jeden podmiot. Nie musi to być poprawny, routowalny adres IP, służy bowiem jedynie jako identyfikator. Prawidłowym wpisem jest na przykład 1.1.1.1.

Opisane powyżej opcje zostały przedstawione na rysunku 9.4.

Istnieje również kilka zaawansowanych ustawień, które mogą być modyfikowane w razie potrzeby:

- ***Active flow export timeout (Seconds)*** (limit czasu dla eksportu aktywnego przepływu wyrażony w sekundach). Czas, jaki musi upłynąć, zanim przełącznik pofragmentuje przepływ i prześle go do kolektora. Pozwala to uniknąć wysyłania dużej ilości danych, gdy występuje szczególnie długi przepływ danych.
- ***Idle flow export timeout (Seconds)*** (limit czasu dla eksportu bezczynnego przepływu wyrażony w sekundach). Podobny do limitu czasu aktywnego przepływu, ale przeznaczony dla przepływów, które weszły w stan bezczynności. Możesz potraktować to jako czyszczenie konieczne, aby zapewnić, że bezczynny przepływ zostanie wysłany do kolektora w odpowiednim czasie.



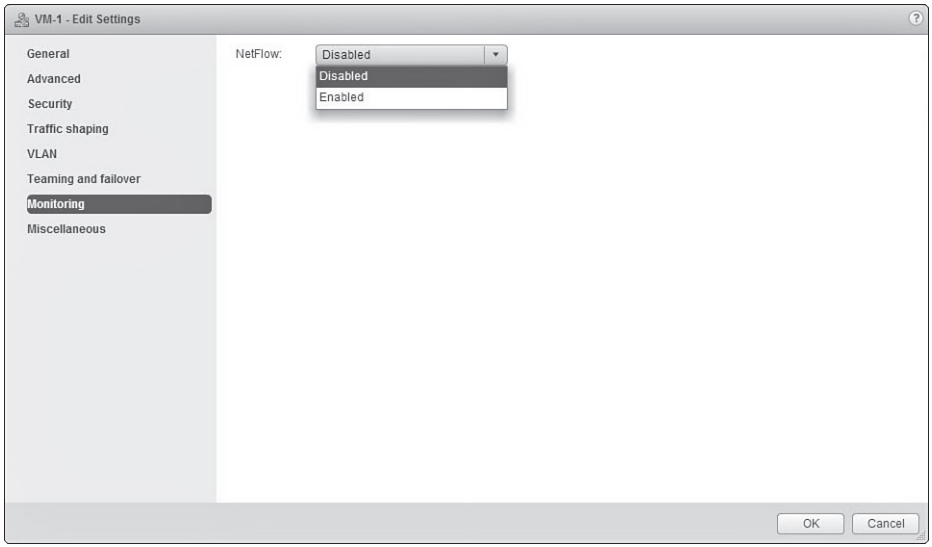
RYSUNEK 9.4. Opcje konfiguracji NetFlow w przełączniku VDS

- ***Sampling rate*** (częstotliwość próbkowania). Określa n-ty pakiet do zebrania. Domyślna wartość wynosi 0, co oznacza, że zbierane są wszystkie pakiety. Jeśli ustawisz wartość inną niż 0, zbierany będzie każdy n-ty pakiet, np. wartość 3 oznacza zbieranie tylko co trzeciego pakietu.
- ***Process internal flows only*** (przetwarzanie tylko przepływów wewnętrznych). Dla tej opcji dostępne są ustawienia *Enabled* (włączona) lub *Disabled* (wyłączona). To drugie ustawienie jest domyślne. Włączenie opcji zapewnia, że zbierane są tylko te przepływy, które mają miejsce pomiędzy maszynami wirtualnymi na samym hoście. Może to być pomocne, jeśli chcesz zbierać tylko przepływ ruchu szarej strefy, masz już skonfigurowaną funkcję NetFlow w infrastrukturze fizycznej i chcesz uniknąć dwukrotnego próbkowania ruchu (raz w warstwie wirtualnej i ponownie — w warstwie fizycznej).

Drugą czynnością wymaganą do tego, aby skorzystać z funkcji NetFlow, jest włączenie monitorowania (ang. *monitoring*) we wszystkich grupach portów, które mają być monitorowane. Szybko możesz się zorientować, że jest to konieczne, jeśli skonfigurujesz funkcję NetFlow, ale nie zobaczysz żadnych informacji o przepływie ruchu — robiliśmy to nie jeden raz. Odpowiednie okno dialogowe zostało przedstawione na rysunku 9.5.

Port Mirroring

Czasami pojawia się potrzeba klonowania ruchu na określonym porcie do innego portu. Wykracza to poza samo monitorowanie portu — funkcja Port Mirroring klonuje cały ruch do skonfigurowanego miejsca docelowego. Istnieją dwa główne przypadki użycia dla tej funkcji: monitorowanie i przechwytywanie. Te dwa przypadki użycia są ściśle ze sobą powiązane,



RYSUNEK 9.5. Włączanie funkcji NetFlow dla grupy portów

ale często mają różne cele. Jeśli chodzi o **monitorowanie**, może być potrzeba związana na przykład z zachowaniem zgodności lub jakąś umową SLA (ang. *Service Level Agreement*), aby wiedzieć dokładnie, jaki ruch jest wysyłany z jednego konkretnego urządzenia do drugiego. **Przechwytywanie** (ang. *capturing*) jest najczęściej spotykane w wypadku konieczności spełnienia wymagań dotyczących rejestrowania rozmów, np. przy przechwytywaniu ruchu VoIP, aby w *call center* rejestrowane były rozmowy telefoniczne.

Jest to dość proste do zrobienia w świecie fizycznym i może występować pod wieloma nazwami, np. porty SPAN (ang. *Switched Port ANalyzer*), Port Mirroring lub monitorowanie portów. Dla danej konfiguracji wybierany jest określony port źródłowy lub VLAN, a każdy ruch, który płynie przez ten port, jest klonowany do portu docelowego. Proces klonowania jest zazwyczaj „obojętny" na rzeczywisty ruch i tworzy po prostu dokładną kopię ruchu na porcie docelowym. Sprawdza się to, gdy każdy port przełącznika przenosi ruch dla pojedynczego podłączonego serwera lub pojedynczej podłączonej stacji roboczej.

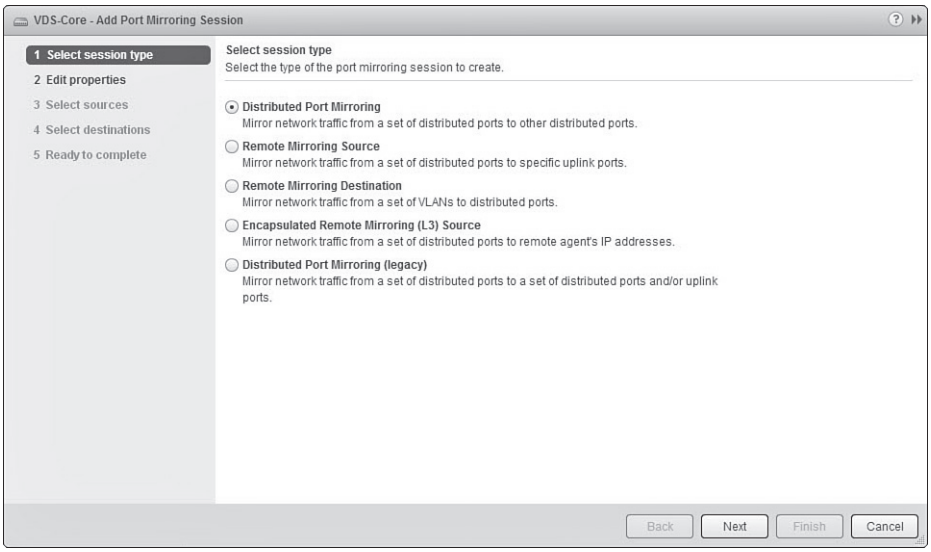
Dodanie środowisk wirtualnych stworzyło pewne problemy związane z funkcją Port Mirroring. Pojedynczy port przełącznika podłączony do hosta vSphere może teraz przekazywać ruch dla dziesiątek, a nawet setek serwerów wirtualnych. Dla pojedynczego serwera wirtualnego funkcjonującego poza rozbudowanymi topologiami sieci (np. w przypadku podłączenia maszyny wirtualnej do specjalnie przeznaczonego portu uplink hosta) mirrorowanie ruchu stało się trudne — jest to działanie rozrzutne i dodatkowo ograniczające mobilność maszyny wirtualnej. Inne technologie, takie jak zastosowanie zewnętrznego przełącznika Nexus 1000V, mogą pomóc rozwiązać ten problem, ale tradycyjnie zależne są od specjalnych umiejętności konfigurowania sieci oraz wyższej ceny zakupu.

Począwszy od vSphere 5.0 przełącznik rozproszony zaczął oferować możliwość mirrorowania ruchu dla portów wirtualnych. Pozwoliło to administratorowi dokładnie kontrolować Port Mirroring dla określonego rozproszonego portu (lub portów). Z początku przełącznik VDS 5.0 oferował prostą konfigurację, która umożliwiała mirrorowanie rozproszonych portów na inne porty rozproszone lub uplink. W przełącznikach VDS 5.1 i nowszych funkcja ta jest znana jako *Distributed Port Mirroring (Legacy)* i jest już przestarzała. Należy pamiętać, że aktualizacja środowiska vSphere nie oznacza automatycznej aktualizacji istniejącego przełącznika VDS. Aby cieszyć się funkcjami dostępnymi w nowszych wersjach VDS, należy również wykonać aktualizację tego przełącznika.

Od wprowadzenia wersji VDS 5.1 dostępne są cztery różne rodzaje sesji Port Mirroring:

1. ***Distributed Port Mirroring***. Mirrorowanie pakietów z dowolnej liczby rozproszonych portów na dowolną liczbę innych rozproszonych portów na tym samym hoście. Jeśli źródło i miejsce docelowe znajdują się na różnych hostach, ten rodzaj sesji nie działa.
2. ***Remote Mirroring Source***. Mirrorowanie pakietów z wielu rozproszonych portów na konkretne porty uplink odpowiedniego hosta.
3. ***Remote Mirroring Destination***. Mirrorowanie pakietów z wielu sieci VLAN na rozproszone porty.
4. ***Encapsulated Remote Mirroring (L3) Source***. Mirrorowanie pakietów z wielu rozproszonych portów na adres IP zdalnego klienta. Ruch maszyn wirtualnych jest mirrorowany do zdalnego fizycznego miejsca docelowego poprzez tunel IP. Jest to podobne do funkcji ERSPAN (ang. *Encapsulated Remote Switched Port Analyzer*).

Opcje te zostały przedstawione na rysunku 9.6.



RYSUNEK 9.6. Opcje funkcji Port Mirroring w przełączniku VDS 5.1

Chociaż dla każdego rodzaju sesji funkcji Port Mirroring różne są źródło i miejsce docelowe, to wszystkie właściwości są stosunkowo podobne. Aby skonfigurować dowolną sesję Port Mirroring, należy zdefiniować kilka standardowych właściwości. Zestaw właściwości, które trzeba skonfigurować, będzie się zmieniać w zależności od rodzaju wybranego trybu Port Mirroring:

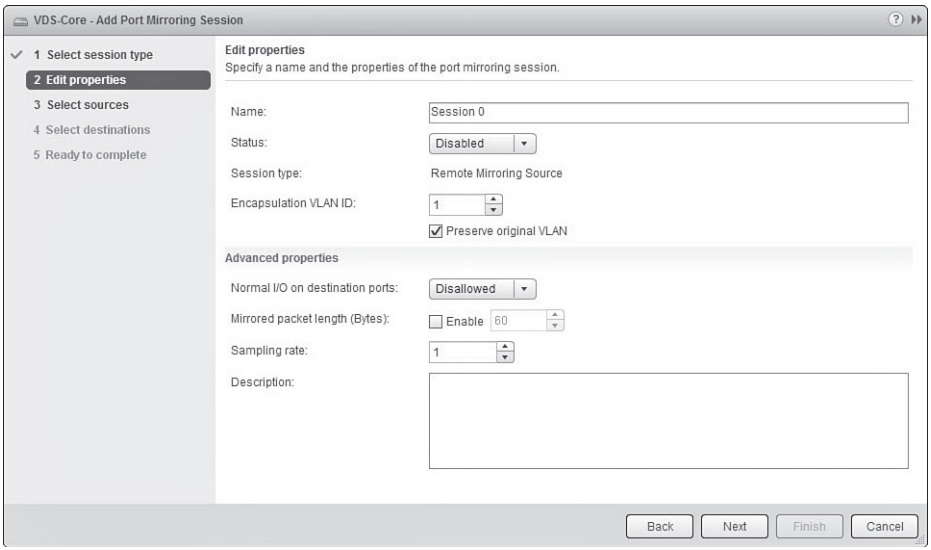
- ***Name***. Nazwa opisująca sesję Port Mirroring. Postaraj się, aby była możliwie jak najbardziej opisowa, ale przy tym nie była rozwlekła, np. „Mirroring serwera X na cel Y" lub „Serwer X na zdalne IP".
- ***Status***. Domyślnie sesja Port Mirroring będzie wyłączona. Możesz zostawić sesję wyłączoną podczas jej tworzenia i włączyć później. Możesz też włączyć sesję podczas konfiguracji.
- ***Session type***. Wybór rodzaju sesji Port Mirroring. Można wybrać jeden z czterech rodzajów sesji opisanych powyżej.
- ***Encapsulation VLAN ID***. Określony w tej właściwości VLAN będzie wykorzystywany do kapsułkowania mirrorowanych ramek. Umożliwi to wysyłanie poprzez uplink ramek, które używają różnych znaczników VLAN ID. Jeśli chcesz, aby sesja Port Mirroring pamiętała oryginalny VLAN ID wykorzystywany przez dany ruch, zaznacz opcję *Preserve original VLAN* (zachowaj oryginalny VLAN). W przeciwnym razie zastosowany zostanie zdefiniowany VLAN kapsułkowania.

Istnieje również kilka zaawansowanych właściwości, które mogą być modyfikowane. Nie wszystkie z nich będą dostępne dla każdego rodzaju funkcji Port Mirroring, ale omówimy je wszystkie:

- ***Normal I/O on destination ports*** (normalny tryb we/wy na portach docelowych). Opis tej właściwości jest nieco niejasny. Chodzi o to, aby zdecydować, czy port docelowy ma działać tylko jako port funkcji Port Mirroring, czy powinien akceptować ruch przychodzący. Domyślnie właściwość jest ustawiona jako *Disallowed* (niedozwolone), co zapobiega przyjmowaniu przez port docelowy ruchu wchodzącego i dedykuje go funkcji Port Mirroring. Dla większości zastosowań monitoringowych, które po prostu mają za zadanie badanie ruchu, pożądane jest pozostawienie dla tej właściwości wartości *Disallowed*. Należy pamiętać, że zapobiega to również przekazywaniu ruchu przez port docelowy.
- ***Mirror packet length (Bytes)*** (długość mirrorowanego pakietu wyrażona w bajtach). Jest to ograniczenie rozmiaru nakładane na mirrorowany ruch. Pakiety przekraczające zdefiniowany rozmiar zostaną przycięte do podanej wartości. Może to być przydatne, jeśli monitorujesz ruch zawierający ramki jumbo (np. ruch pamięci masowej), ale chcesz przechwytywać tylko ramki normalnych rozmiarów lub nagłówki zamiast pełnego bloku danych. Zazwyczaj to pole pozostawia się puste, a wszelkie ograniczenia długości pakietów definiuje się w oprogramowaniu do przechwytywania.
- ***Sampling rate*** (częstotliwość próbkowania). Podobnie jak miało to miejsce w konfiguracji częstotliwości próbkowania funkcji NetFlow, ta właściwość określa, jak dużo pakietów ma być próbkowanych. Domyślna wartość *1* oznacza przechwytywanie wszystkich pakietów. Każda inna wartość *n* oznacza przechwytywanie co n-tego pakietu, np. częstotliwość próbkowania *7* oznacza próbkowanie co siódmego pakietu i pomijanie pozostałych sześciu.

- ***Description*** (opis). Opis sesji Port Mirroring. Nie wiadomo, dlaczego jest to wymienione w sekcji właściwości zaawansowanych, ponieważ jest to sposób przekazywania informacji o celu sesji, ale właśnie tu się znajduje.

Te zaawansowane właściwości zostały przedstawione na rysunku 9.7.



RYSUNEK 9.7. Elementy konfiguracyjne dla sesji Port Mirroring

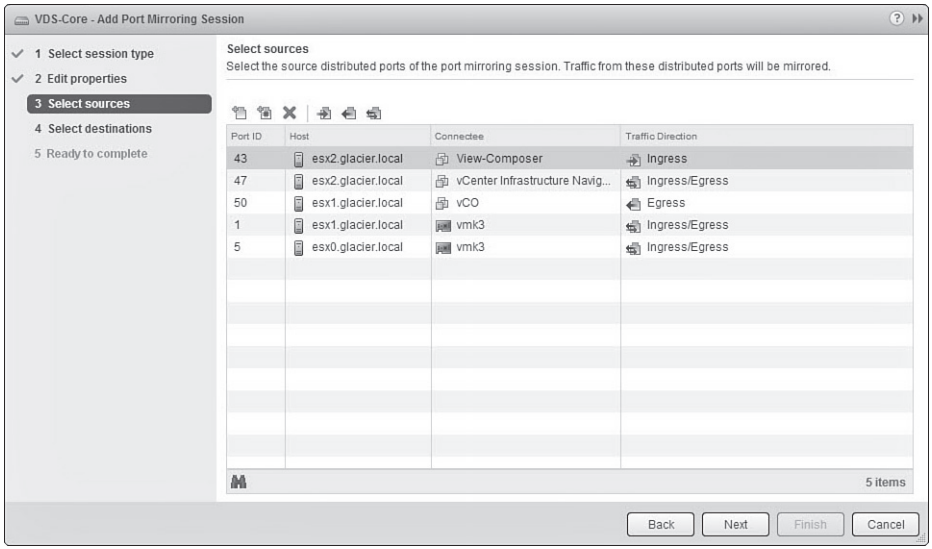
Źródłem dla sesji Port Mirroring mogą być: jeden port rozproszony, wiele portów rozproszonych, a nawet zakres portów. Porty mogą być wykorzystywane przez maszyny wirtualne lub porty VMkernel. Każdy identyfikator portu (ang. *port ID*) wskazuje host, który obsługuje identyfikator portu wirtualnego, element podłączony do portu wirtualnego oraz kierunek ruchu, który chcesz przechwytywać. Należy pamiętać, że kierunek jest oparty na następującej perspektywie: *ingress* wchodzi na port, natomiast *egress* wychodzi z portu. Gdy dwie osoby prowadzą konwersację, z ust osoby mówiącej „wychodzą" informacje (*egress*), które „wchodzą" (*ingress*) do ucha osoby słuchającej.

Opcje źródeł zostały przedstawione na rysunku 9.8.

Jedynym wyjątkiem jest rodzaj sesji *Remote Mirroring Destination*, który wykorzystuje jako źródło jeden VLAN ID lub kilka.

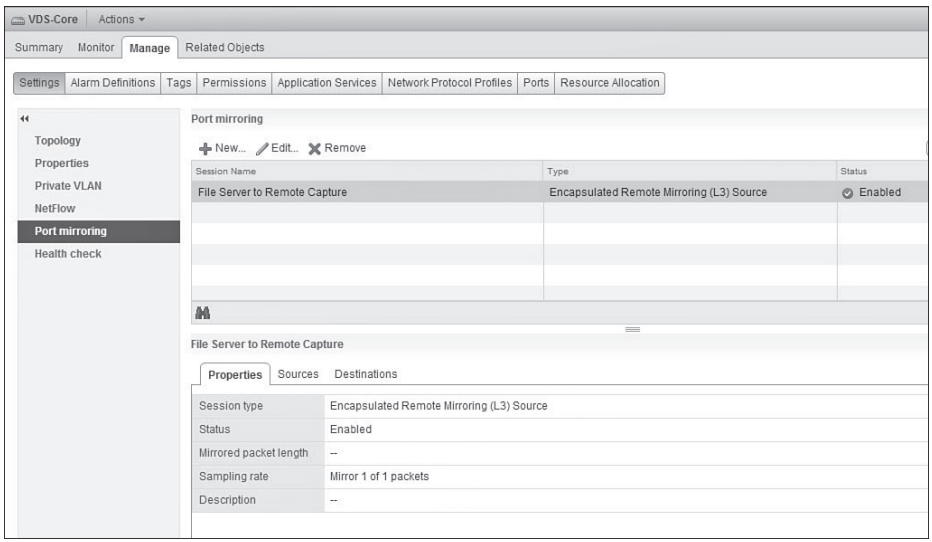
Wybór miejsca docelowego dla sesji Port Mirroring jest najbardziej zróżnicowany. Oto lista dostępnych opcji związanych z miejscami docelowymi dla każdego rodzaju Port Mirroring:

- ***Distributed Port Mirroring***: wirtualne porty,
- ***Remote Mirroring Source***: uplink,
- ***Remote Mirroring Destination***: wirtualne porty,
- ***Encapsulated Remote Mirroring (L3) Source***: zdalny adres IP.



RYSUNEK 9.8. Próbkowanie źródeł do sesji funkcji Port Mirroring

Efektem jest wpis w sekcji *Port mirroring* przełącznika VDS, pokazujący listę wszystkich sesji. W górnym panelu okna wyświetlane są: nazwa, rodzaj i status każdej sesji, a w dolnym panelu — właściwości, źródła i miejsca docelowe. Aktywna sesja funkcji Port Mirroring została przedstawiona na rysunku 9.9.



RYSUNEK 9.9. Aktywna sesja Encapsulated Remote Mirroring (L3) Source funkcji Port Mirroring

Prywatne sieci VLAN

Czasami zastosowanie sieci VLAN nie jest wystarczające do spełnienia wymagań projektowych. Być może będziesz chciał uniknąć niepotrzebnego wykorzystania swoich 4094 znaczników VLAN ID lub będziesz miał jakieś specjalne wymagania związane z dzierżawą, które uzasadniają tworzenie izolowanych środowisk. Tutaj do gry wchodzi koncepcja prywatnej sieci VLAN (ang. *private VLAN*). Różnice architektoniczne można zilustrować za pomocą porównania domu jednorodzinnego z wielopiętrowym apartamentowcem.

W scenariuszu dotyczącym domu jednorodzinnego wszyscy mieszkają razem w jednym domu, ale zajmują różne pokoje. Jeśli masz dostęp do domu, zakładamy, że przynależysz do niego, i nie zabraniamy Ci zaglądać do cudzych pokoi — chociaż nie jest to zwykle zbyt uprzejme zachowanie. Jest to sytuacja bardzo podobna do standardowej sieci VLAN. Jeśli chcesz przenieść się z domu jednej osoby do domu drugiej osoby lub z jednego VLAN-u do drugiego, musisz użyć urządzenia routującego — nie możesz po prostu przechodzić między domami.

VLAN podstawowy

W apartamentowcu każde mieszkanie jest odizolowanym środowiskiem znajdującym się w obrębie większego budynku. Wszyscy mają dostęp do drzwi frontowych apartamentowca, ale nie mają dostępu do cudzych mieszkań. Mniej więcej w ten sposób działa prywatna sieć VLAN. Do oznaczenia wspólnej sieci VLAN, która jest wykorzystywana jako wejście do prywatnego zbioru sieci VLAN, używamy terminu „VLAN podstawowy” (ang. *primary VLAN*).

VLAN mieszany

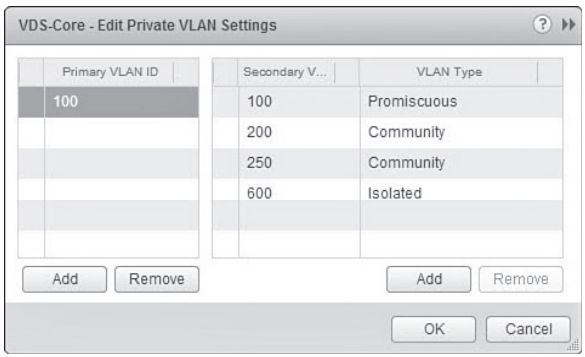
VLAN podstawowy jest połączony z resztą infrastruktury sieciowej za pomocą jednego portu mieszanego (ang. *promiscuous port* — P-Port) lub kilku takich portów. Możesz potraktować P-Port jako wejście do budynku z apartamentami — każdy ma do niego dostęp, a przez ten port wchodzi się do prywatnego zbioru sieci VLAN i z niego wychodzi. Każdy VLAN prywatny potrzebuje VLAN-u podstawowego z portem P-Port, w przeciwnym razie nie byłoby możliwości transmitowania ruchu do tego segmentu sieci i w odwrotnym kierunku.

VLAN-y podrzędne

Każdy apartament w budynku stanowiłby „VLAN podrzędny” (ang. *secondary VLAN*), inaczej sub-VLAN, który może ponownie wykorzystywać identyfikatory VLAN ID istniejące poza prywatną siecią VLAN. Oznacza to, że jeśli masz gdzieś w swojej sieci VLAN ID 100, możesz mieć również w obrębie VLAN-u podstawowego VLAN podrzędny, który wykorzystuje identyfikator VLAN ID 100. VLAN podstawowy musi być jednak unikatowy w obu sieciach. W przeciwnym razie sieć będzie miała problemy z rozstrzygnięciem, dla którego VLAN-u przeznaczony jest ruch.

Podrzędne identyfikatory VLAN ID istnieją tylko w środowisku VLAN-u prywatnego, a znaczniki zostają zastąpione podstawowym VLAN ID, gdy ruch opuszcza prywatną sieć VLAN. W przełączniku VMware Distributed Switch zdefiniowane są trzy typy VLAN-ów podrzędnych: VLAN *Promiscuous* (który już omówiliśmy), VLAN *Community* oraz VLAN *Isolated*.

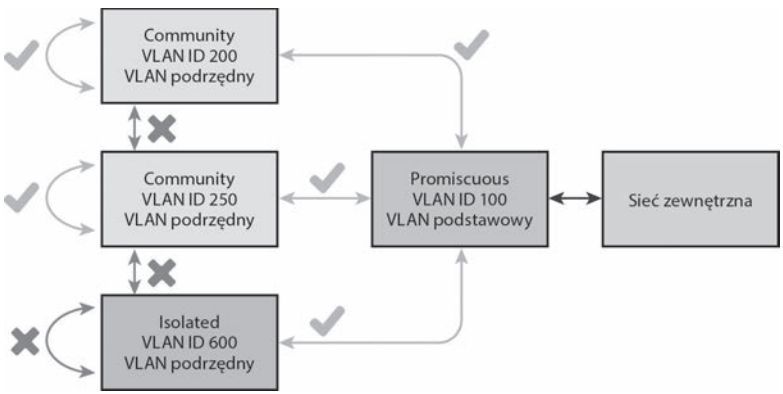
Na rysunku 9.10 przedstawiony został proces tworzenia VLAN-u prywatnego w przełączniku VDS.



RYSUNEK 9.10. Tworzenie VLAN-u prywatnego w przełączniku rozproszonym

VLAN-y typu community

VLAN *Community* pozwala swoim członkom komunikować się ze sobą oraz z VLAN-em *Promiscuous*. Możesz potraktować to jak pokój konferencyjny — wszyscy w tym pokoju mogą komunikować się ze sobą, ale nie mogą bez pomocy rozmawiać z nikim na zewnątrz. Na rysunku 9.10 przedstawione zostały na przykład dwa VLAN-y *Community*: 200 i 250. Wszystkie maszyny wirtualne umieszczone w *Community* VLAN 200 będą mogły komunikować się ze sobą oraz wysyłać ruch do sieci *Promiscuous* VLAN. Nie będą mogły jednak wysyłać ruchu do *Community* VLAN 250 lub *Isolated* VLAN 600 bez bezpośredniego wsparcia ze strony urządzenia routującego, znajdującego się w sieci *Promiscuous* VLAN lub na wyższym poziomie w stosie sieciowym. Na rysunku 9.11 zilustrowano przepływ ruchu między VLAN-ami podrzędnymi.



RYSUNEK 9.11. Przepływ ruchu pomiędzy VLAN-nami podrzędnymi w VLAN-nie prywatnym

Można mieć dowolną liczbę VLAN-ów *Community*, a jedynym ograniczeniem jest liczba dostępnych znaczników VLAN ID, czyli 4094.

VLAN-y typu isolated

Ostatnim typem VLAN-u podrzędnego jest VLAN *Isolated*. Mają tu zastosowanie reguły dotyczące VLAN-ów *Community*, ale dodatkowo maszyny wirtualne wewnątrz VLAN-u *Isolated* nie mogą nawet komunikować się między sobą. Każdy ruch warstwy drugiej, który będzie próbował przedostać się z jednej maszyny wirtualnej do drugiej, będzie po prostu zrzucany. Maszyny wirtualne mogą komunikować się tylko z VLAN-em *Promiscuous* i środowiskiem zewnętrznym.

WSKAZÓWKA

Dlaczego warto korzystać z VLAN-ów typu *isolated*? Ten szczególny rodzaj sieci VLAN ma fantastyczne zastosowania dla obciążeń roboczych, które będą współdzielone przez gościnnych użytkowników, takich jak kioski. Jeśli umieścisz bramkę internetową w VLAN-nie *Promiscuous*, możesz zapewnić, aby każdy kiosk był izolowany od pozostałych, ale wciąż miał dostęp do Internetu. W rzeczywistości w większości zastosowań hotelowych wdrażane są VLAN-y typu *isolated* właśnie z tego powodu. Mimo to należy uważać, co robi się w Internecie — ktoś prawdopodobnie monitoruje Twoją aktywność.

Rozproszone grupy portów

Ponieważ przełącznika VDS może używać wiele hostów, grupy portów również muszą być rozproszone. Oznacza to, że żaden host nie jest właścicielem jakiejkolwiek części przełącznika VDS, włączając w to rozproszone grupy portów. W rzeczywistości, jeśli port VMkernel ma znajdować się w przełączniku VDS, musi skorzystać z rozproszonej grupy portów. Różni się to od konfiguracji standardowego przełącznika vSwitch pod tym względem, że trzeba utworzyć specjalne adaptery sieciowe VMkernel bezpośrednio w przełączniku vSwitch. Ponadto wiele portów VMkernel może współdzielić tę samą rozproszoną grupę portów.

WSKAZÓWKA

VDS jest własnością kontenera vCenter Datacenter, a nie hosta, i nie może obejmować więcej niż jednego kontenera Datacenter. Oznacza to, że można w przełączniku VDS tworzyć grupy portów, które będą wykorzystywane przez hosty w każdym klastrze znajdującym się w kontenerze Datacenter lub nawet przez hosty niebędące w klastrze. Te grupy portów nie mogą być jednak używane przez hosty innego kontenera Datacenter. To sprawia, że rozproszone grupy portów są niezwykle wszechstronne i wysoce skalowalne.

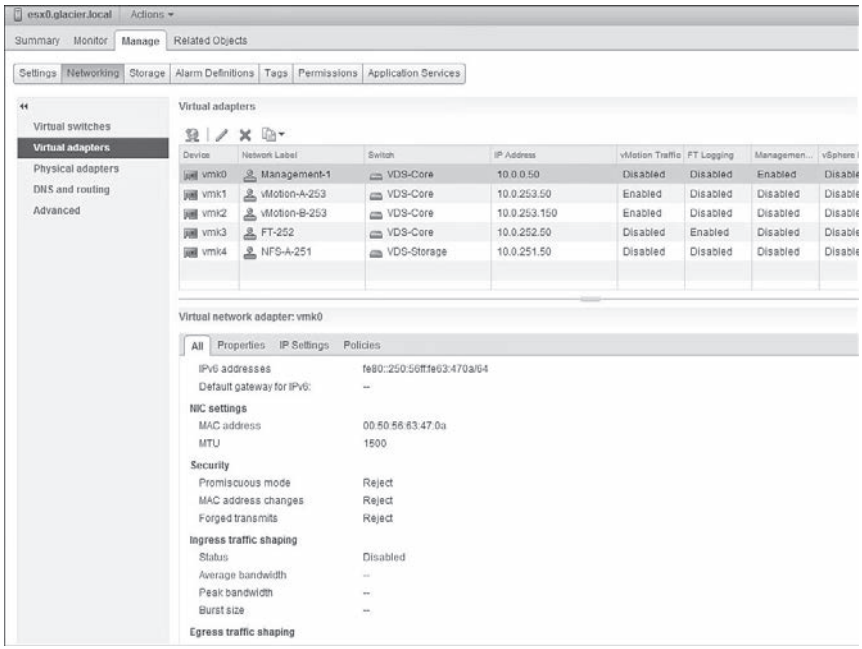
Każda rozproszona grupa portów posiada dostęp do wszystkich uplinków powiązanych z przełącznikiem VDS. Ponadto ustawienia i reguły konfiguracyjne (takie jak wartości zabezpieczeń i teamingu) są stosowane bezpośrednio do rozproszonej grupy portów.

Oznacza to, że jedna rozproszona grupa portów ma wszystkie uplinki skonfigurowane jako aktywne i używa VLAN-u 100, podczas gdy druga grupa portów ma konfigurację mieszaną aktywny-pasywny w VLAN-ie 200. Powszechne jest tworzenie projektów modułowych z szeregiem grup portów do różnych zadań, np. po jednej dla każdego VLAN-u, którego będą używać gościnne maszyny wirtualne, ruchu *vMotion*, *Management*, *Fault Tolerance logging*. Więcej informacji na ten temat znajdziesz w rozdziale 13.

Porty VMkernel

Ponieważ host wciąż potrzebuje portów VMkernel (wirtualnych adapterów) do obsługi zadań, takich jak zarządzanie ruchem i *vMotion*, nadal jest zapotrzebowanie na porty VMkernel w przełączniku VDS. Tutaj wszystko może stać się nieco bardziej skomplikowane. Porty VMkernel są unikatowe dla każdego hosta, ponieważ każdy host ma własne: schemat numerowania vmk i szczegóły konfiguracji IP. Dlatego porty VMkernel są konfigurowane na każdym hoście w vCenter, podobnie jak w wypadku standardowego przełącznika vSwitch.

Różnica polega na tym, że każdy port VMkernel istnieje w rozproszonej grupie portów. Kiedy do przełącznika VDS zostanie dodany host, pojawiają się opcje umieszczenia jego portów VMkernel w rozproszonej grupie portów. Port VMkernel do funkcjonowania wykorzystuje bazowe reguły z rozproszonej grupy portów. Dlatego bazowa konfiguracja sprzętowa jest definiowana przez reguły rozproszonej grupy portów, a tożsamość portu VMkernel (adres IP, maska podsieci, MTU itd.) są definiowane przez sam host. Na rysunku 9.12 pokazane zostały porty VMkernel hosta w przełączniku VDS.



RYSUNEK 9.12. Porty VMkernel w hoście vSphere dodanym do przełącznika Distributed vSwitch

Maszyny wirtualne

Jeśli chodzi o maszyny wirtualne podłączone do przełącznika VDS, to wymagane są niewielkie zmiany operacyjne. Maszyny wirtualne mogą korzystać z portów dowolnej rozproszonej grupy portów, nawet tej, która została przeznaczona do wykorzystywania przez porty VMkernel. Zazwyczaj najlepiej jest utworzyć konkretne grupy portów tylko dla maszyn wirtualnych i zastosować schemat nazewnictwa, który najlepiej opisuje sieć, np. zakres segmentu IP oraz VLAN ID.

Dodatkową korzyścią (należy o tym pamiętać, ponieważ grupy portów są rozproszone) z umieszczenia maszyny wirtualnej w rozproszonej grupie portów jest zmniejszone ryzyko, że *vMotion* zrobi spustoszenie z powodu reguł lub błędnej konfiguracji VLAN ID hosta docelowego. Host ma dokładnie takie same ustawienia grupy portów. Ułatwia to nieco rozwiązywanie problemów z siecią, ponieważ często przy niewielkim wysiłku można ustalić, że fizyczna sieć w hoście nie jest poprawnie skonfigurowana.

Kształtowanie ruchu

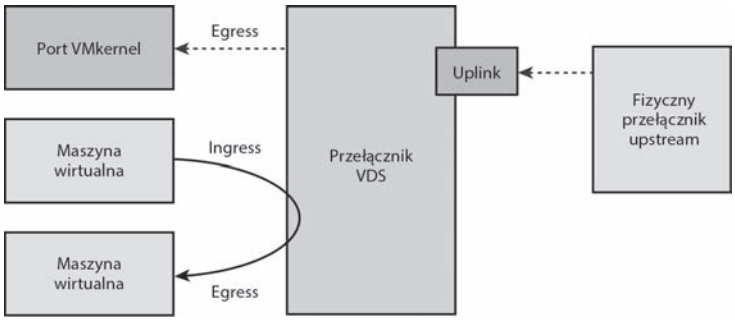
W rozdziale 8. omówiliśmy już dość szeroko koncepcję kształtowania ruchu oraz sposób wyliczania wartości dla parametrów konfiguracyjnych. Powinieneś się dobrze orientować, w jaki sposób zdefiniować średnią przepustowość, szczytową przepustowość oraz rozmiar serii — jeśli tak nie jest, wróć do tego rozdziału i ponownie przeczytaj fragment dotyczący kształtowania ruchu.

W tym rozdziale powracamy do kwestii kształtowania ruchu z uwagi na dodatkową funkcję, która pojawiła się w przełączniku Distributed vSwitch. Jest to zdolność do kształtowania zarówno ruchu *ingress*, jak i *egress*. Standardowy przełącznik vSwitch umożliwia jedynie kształtowanie ruchu *ingress*.

Egress

Egress jest koncepcją kształtowania ruchu, który opuszcza przełącznik VDS. Może to być ruch z przełącznika VDS do maszyny wirtualnej lub portu VMkernel, a nawet ruch przepływający z jednej maszyny wirtualnej do drugiej. Opcje konfiguracji kształtowania ruchu są takie same jak w wypadku ruchu *ingress*, ale są stosowane dla ruchu przepływającego w kierunku przeciwnym. Taki ruch został przedstawiony na rysunku 9.13.

> **UWAGA**
>
> Jednym z doskonałych sposobów na wykorzystanie kształtowania ruchu *egress* jest kontrolowanie przepustowości, która może być zastosowana do ruchu *multi-NIC vMotion*. Z patologicznym przypadkiem mamy do czynienia, gdy wiele hostów źródłowych przenosi za pomocą *vMotion* maszyny wirtualne do pojedynczego hosta docelowego. Bez kształtowania ruchu *egress* lub jakiegoś fizycznego kształtowania ruchu na przełączniku upstream możesz doświadczyć nietrywialnej ilości ruchu na uplinkach hosta. Ta kwestia zostanie omówiona szczegółowo w rozdziale 19.



RYSUNEK 9.13. Różne przypadki występowania ruchu egress w przełączniku VDS

Równoważenie obciążenia

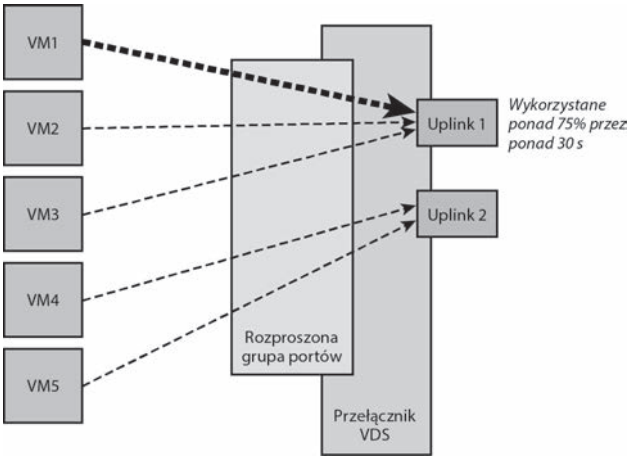
Kolejną funkcją dostępną tylko w przełączniku Distributed vSwitch jest nowa forma równoważenia obciążenia o nazwie *Route based on physical NIC load* (trasa oparta na obciążeniu fizycznego adaptera sieciowego), często określana jako *Load Based Teaming* (LBT). Te reguły routingu zostały wprowadzone w wersji vSphere 4.1 i jest to jedyna dostępna, naprawdę aktywna polityka równoważenia obciążenia. Wszystkie inne reguły wykorzystują arbitralny czynnik do określenia ścieżki uplinku (np. adres IP albo wirtualny port), natomiast LBT aktywnie monitoruje ruch i przenosi go do różnych uplinków, gdy zostają spełnione pewne kryteria.

Route based on physical NIC load

Przyjrzyjmy się bliżej działaniu tych reguł równoważenia obciążenia na podstawie przykładowego scenariusza. Wyobraź sobie, że na tym samym fizycznym hoście vSphere masz pięć maszyn wirtualnych, które wysyłają i odbierają ruch Ethernet na tej samej rozproszonej grupie portów. Ta grupa portów posiada losowo przypisane maszyny wirtualne VM1, VM2 i VM3 do *Uplinku 1*, podczas gdy maszyny wirtualne VM4 i VM5 używają *Uplinku 2*. Nagle VM1 rozpoczyna wysyłanie ogromnej ilości ruchu, który nasyca całe dostępne pasmo na *Uplinku 1* przez ponad 30 sekund, tak jak zostało to przedstawione na rysunku 9.14.

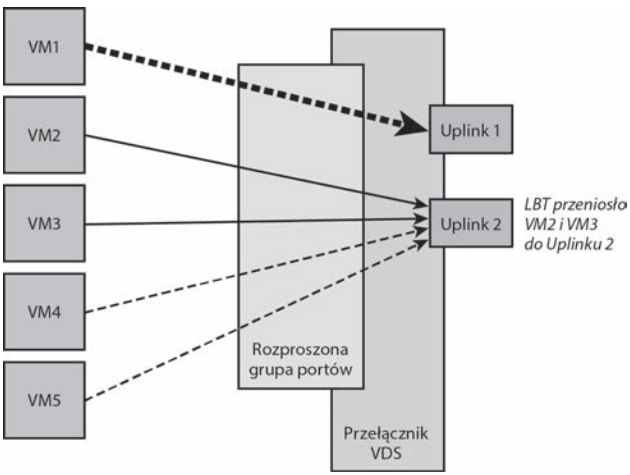
W wypadku każdej innej zasady równoważenia obciążenia nasycenie na *Uplinku 1* będzie się utrzymywać, dopóki VM1 nie zakończy wysyłania danych przez sieć. Tymczasem *Uplink 2* może doświadczać bardzo niewielkiego ruchu, a nawet pozostawać w stanie bezczynności. Co za marnotrawstwo!

LBT będzie monitorować uplinki i uruchamiać równoważenie obciążenia, gdy któryś z uplinków będzie nasycony w co najmniej 75% przez co najmniej 30 sekund (wartości progowe nie mogą być modyfikowane). W takiej sytuacji podejmowana będzie decyzja o przeniesieniu niektórych wirtualnych kart sieciowych VM do innego aktywnego uplinku, pod warunkiem, że ma on wystarczającą niewykorzystaną przepustowość, aby zaakceptować nową maszynę wirtualną. Należy pamiętać, że LBT nie przeniesie ruchu do uplinku będącego w stanie gotowości lub nieużywanego, więc nie musisz się martwić o zakłócenie zdefiniowanej kolejności przełączania awaryjnego.



RYSUNEK 9.14. Maszyna wirtualna VM1 powoduje, że *Uplink 1* przekracza 75% swojego maksymalnego poziomu wykorzystania przez ponad 30 sekund

W przykładowym scenariuszu przedstawionym na rysunku 9.15 LBT przeniosło maszyny wirtualne VM2 i VM3 do *Uplinku 2*. Jest to spowodowane sytuacją „hałaśliwego sąsiada", w której maszyna wirtualna VM1 była przyczyną powstania rywalizacji o przepustowość sieci.



RYSUNEK 9.15. LBT przeniosło wirtualne karty sieciowe maszyn wirtualnych VM2 i VM3 do Uplinku 2

Ważne jest, aby zrozumieć kilka ograniczeń związanych z LBT:

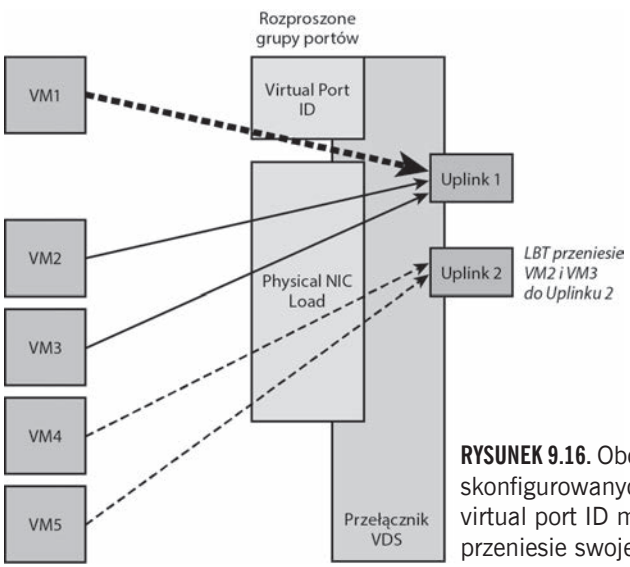
- Wirtualny adapter sieciowy maszyny wirtualnej nie może korzystać z wielu uplinków w tym samym czasie. Reguły równoważenia obciążenia w wypadku rywalizacji o przepustowość przenoszą adapter wirtualny z jednego uplinku do drugiego, ale nie rozkładają ruchu sieciowego pojedynczej maszyny wirtualnej na wiele uplinków.
- Jeśli masz bardzo impulsowy ruch, który kończy się przed upływem 30 sekund, LBT nie uruchomi migracji. Ten 30-sekundowy próg jest stosowany, aby zapobiec thrashingowi, czyli wykonywaniu bezużytecznej, powtarzającej się i kosztownej pracy.

UWAGA

Chociaż niemal w całej dokumentacji dla LBT mówi się o możliwości migrowania wirtualnych adapterów sieciowych maszyn wirtualnych, należy zrozumieć, że można również przenosić porty VMkernel. Jeśli pracujesz w środowisku konwergentnej infrastruktury z ograniczoną liczbą uplinków, korzystne może być stosowanie LBT do przenoszenia portu VMkernel przypisanego do zarządzania lub *vMotion* w wypadkach nasycenia przepustowości uplinku. Nie zapominaj, że LBT nie może spowodować, aby ruch dla portu VMkernel korzystał z wielu uplinków jednocześnie — port VMkernel jest jedynie przenoszony z jednego uplinku do drugiego.

Można zastanawiać się, jak działa LBT, gdy mamy wiele rozproszonych grup portów, z których wszystkie współdzielą ten sam zestaw uplinków. Przecież każda grupa portów może mieć wprowadzone inne reguły teamingu: niektóre wykorzystują LBT, inne — identyfikator wirtualnego portu, a jeszcze inne — bezpośrednio zdefiniowaną kolejność przełączania awaryjnego. Na szczęście LBT może bardzo dobrze mieszać się z innymi regułami, ponieważ monitoruje nasycenie uplinków. Jeśli nasycenie któregokolwiek uplinku w przełączniku VDS osiągnie poziom co najmniej 75% przez 30 sekund, każda rozproszona grupa portów ze skonfigurowanymi regułami LBT uruchomi równoważenie obciążenia. Nie ma potrzeby posiadania jednej dużej grupy portów z wszystkimi maszynami wirtualnymi wewnątrz.

Na rysunku 9.16 maszyny wirtualne zostały podzielone na dwie grupy portów: zieloną (jaśniejszą), wykorzystującą reguły *Route based on originating virtual port ID* (domyślne), i pomarańczową (ciemniejszą), wykorzystującą LBT. Gdy VM1 zacznie wysyłać ogromne ilości ruchu, które spowodują, że *Uplink 1* osiągnie poziom nasycenia co najmniej 75% przez minimum 30 sekund, pomarańczowa grupa portów (LBT) będzie mogła nadal przenieść VM2 i VM3 do *Uplinku 2*, aby złagodzić nasycenie.



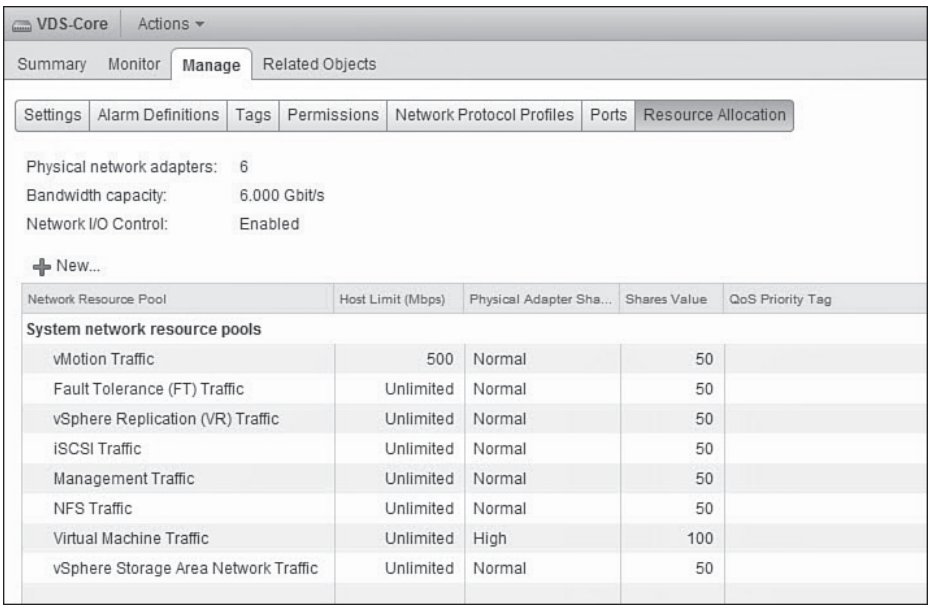
RYSUNEK 9.16. Obciążenie robocze na grupie portów skonfigurowanych z regułą Route based on originating virtual port ID może nadal spowodować, że LBT przeniesie swoje obciążenia robocze w inne miejsce

Sterowanie operacjami we/wy sieci

Ostatnią funkcją przełącznika Distributed vSwitch, którą się zajmiemy, jest *Network I/O Control* (NIOC), czyli sterowanie operacjami we/wy sieci. NIOC jest świetnym sposobem zwiększania kontroli ruchu w sieci. Podobnie jak jest to w wypadku pul zasobów tworzonych dla obciążeń obliczeniowych, ideą stojącą za NIOC jest umożliwienie konfigurowania limitów i udziałów w sieci zarówno dla pul zasobów sieci generowanych przez system, jak i definiowanych przez użytkownika. Ruch sieciowy jest grupowany w pule zasobów w zależności od rodzaju ruchu, a dla każdej puli zasobów można wybrać zastosowanie ograniczenia przepustowości, skonfigurowanie wartości udziałów, a nawet przypisanie znacznika priorytetów QoS.
Na rysunku 9.17 pokazano, gdzie można włączyć NIOC.

UWAGA

W aplikacji vSphere Web Client funkcja ta ukrywa się w menu *Resource Allocation* (alokacja zasobów). Spowodowało to pewną dezorientację wielu użytkowników, którzy szukali konkretnie zakładki *NIOC*.



RYSUNEK 9.17. W oknie z zakładką Resource Allocation pokazane wszystkie wartości konfiguracji NIOC

Zobaczmy, za co odpowiedzialne są różne ustawienia konfiguracyjne NIOC:

- ***Physical network adapters*** (fizyczne adaptery sieciowe). Liczba uplinków, które każdy host przeznacza dla tego konkretnego przełącznika VDS. W naszym wypadku przełącznik VDS wykorzystuje 3 hosty, a każdy ma 2 uplinki. Tak więc 3 hosty×2 uplinki = 6 fizycznych kart sieciowych.

- ***Bandwidth capacity (Gbit/s)*** (całkowita przepustowość w Gb/s). Każdy z 6 uplinków wykrytych w pozycji *Physical network adapters* pracuje z prędkością 1 Gb/s. Dlatego całkowita przepustowość dla całego przełącznika VDS wynosi 6 Gb/s. Należy pamiętać, że wartość ta jest podawana w gigabitach na sekundę (małe „b"), a nie gigabajtach na sekundę (wielkie „B").
- ***Network I/O Control*** (kontrola we/wy sieci). Domyślnie ta opcja jest wyłączona (ang. *disabled*) i wtedy wartości konfiguracyjne NIOC nie mają wpływu na ruch.

Pule zasobów sieciowych

Na rysunku 9.17 możesz również zauważyć listę ośmiu systemowych pul zasobów sieciowych (ang. *system network resource pools*). Każda z pul odpowiada określonemu rodzajowi ruchu oraz umożliwia skonfigurowanie wartości, które wpływają na ruch *ingress*, czyli z przełącznika VDS na jego porty uplink. Nie można usunąć żadnej z predefiniowanych pul zasobów, do których należą:

- *vMotion Traffic* (ruch *vMotion*).
- *Fault Tolerance (FT) Traffic* (ruch *Fault Tolerance*).
- *vSphere Replication (VR) Traffic* (ruch *vSphere Replication*). Pula używana przez urządzenia VR, w tym *VMware Site Recovery Manager* (SRM).
- *iSCSI Traffic* (ruch iSCSI).
- *Management Traffic* (ruch zarządzania).
- *NFS Traffic* (ruch NFS).
- *Virtual Machine Traffic* (ruch maszyn wirtualnych). Pula wykorzystywana dla wszystkich maszyn wirtualnych, choć można tworzyć własne, definiowane przez użytkownika pule zasobów. Zajmiemy się tym w dalszej części tego rozdziału.
- *vSphere Storage Area Network Traffic* (ruch *vSphere SAN*). Pula używana przez technologię Virtual SAN, którą firma VMware przedstawiła na konferencji „VMworld 2013" (tylko wersja vSphere 5.5 lub wyższa).

Skoro wiesz już, jakie rodzaje ruchu możemy kontrolować, przyjrzyjmy się dostępnym dla każdego z nich opcjom konfiguracyjnym:

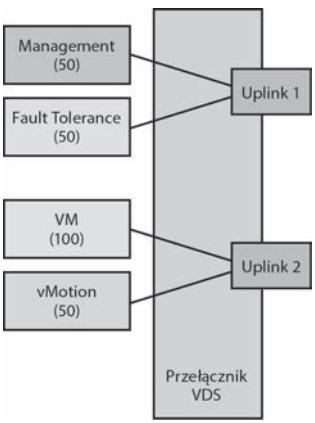
- ***Host Limit (Mbps)*** (limit hosta w Mb/s). Limit ruchu określony w megabitach na sekundę, który nie może zostać przekroczony przez daną pulę zasobów sieciowych. W wersji vSphere 5.1 jest to limit dla każdego uplinku, podczas gdy w wersjach wcześniejszych był to limit dla każdego hosta. Jeśli w przełączniku VDS w wersji 5.1 chciałbyś na przykład ograniczyć pulę zasobów sieciowych *vMotion* do 2000 Mb/s, ale masz zdefiniowanych wiele portów *vMotion* VMkernel na wielu uplinkach, to każdy uplink będzie mógł wysłać ruch z prędkością 2000 Mb/s. Używaj limitów oszczędnie, ponieważ mogą one sztucznie tworzyć połączenie sieciowe bez powodu.

- ***Physical Adapter Shares*** (udziały fizycznego adaptera). Skonfigurowane udziały dla adaptera (portu uplink). Dostępne są ustawienia *High* (100 udziałów), *Normal* (50 udziałów), *Low* (25 udziałów) lub *Custom*, które pozwala zdefiniować niestandardową liczbę udziałów — do 100. Udziały są w ostateczności stosowane do obliczenia, jaki procentowy udział w fizycznym adapterze (uplinku) może wykorzystać każda pula zasobów sieciowych. Prędkość uplinku nie wpływa na zwiększenie ani na zmniejszenie liczby udziałów, ponieważ wartości procentowe odnoszą się do prędkości uplinku.
- ***Shares Value*** (liczba udziałów). Liczba udziałów określonych dla puli zasobów sieciowych.
- ***QoS Priority Tag*** (znacznik priorytetu QoS). To pole daje możliwość ustawienia znacznika QoS IEEE 802.1p. Priorytet może przyjmować wartości od 0 (najniższy) do 7 (najwyższy). Wiele urządzeń warstwy drugiej działających w sieci fizycznej sprawdza tę część ramki Ethernet i na podstawie przypisanej wartości znacznika QoS priorytetyzuje lub zrzuca ruch. Przy konfiguracji tej opcji należy zachować ostrożność i skonsultować się z zespołem sieciowym.

Udziały

Jeśli chodzi o pule zasobów, to udziały powodują najwięcej nieporozumień. Przeanalizujmy więc wartości udziałów ustawiane dla pul zasobów sieciowych. Po pierwsze, udziały mają wartość względną. Nie reprezentują konkretnej, określonej ilości ruchu i nie są używane, dopóki uplink nie zostanie nasycony ruchem.

Po drugie, gdy uplink zostanie nasycony ruchem, uruchamia się funkcja NIOC i rozpoczyna sprawdzanie dwóch elementów: skonfigurowanej liczby udziałów oraz tego, które pule zasobów sieciowych są wykorzystywane przez uplink. W przykładzie przedstawionym na rysunku 9.18 mamy dwa uplinki skonfigurowane w przełączniki VDS z włączoną kontrolą NIOC. Jeden służy jako aktywny uplink dla grup portów *Management* i *Fault Tolerance*, podczas gdy drugi służy jako aktywny uplink dla grup portów VM i *vMotion*.



RYSUNEK 9.18. Przykład przełącznika VDS z dwoma uplinkami i czterema grupami portów z różnymi rodzajami ruchu

Jeśli *Uplink1* zostanie nasycony ruchami *Management* i *Fault Tolerance*, to funkcja NIOC zbada ten uplink i wykryje następujące informacje:

- *Uplink 1*, który jest połączeniem o prędkości 1 Gb/s z przełącznikiem upstream, jest aktywnym uplinkiem dla ruchów *Management* (50 udziałów) i *Fault Tolerance* (50 udziałów).
- 50 działów+50 udziałów = 100 wszystkich udziałów dla tego uplinku.
- Ruch *Management* otrzyma 50 ze 100 udziałów, co stanowi 50% całego linku 1 Gb/s, czyli w sumie 0,5 Gb/s lub około 500 Mb/s.
- Ruch *Fault Tolerance* otrzyma 50 ze 100 udziałów, co stanowi 50% całego linku 1 Gb/s, czyli w sumie 0,5 Gb/s lub około 500 Mb/s.

To było łatwe. Zróbmy coś trudniejszego i sprawdźmy, co się stanie, jeśli *Uplink 2* zostanie nasycony ruchem VM i *vMotion*:

- *Uplink 2*, który jest połączeniem o prędkości 1 Gb/s z przełącznikiem upstream, jest aktywnym uplinkiem dla ruchów VM (100 udziałów) i *vMotion* (50 udziałów).
- 100 udziałów+50 udziałów = 150 wszystkich udziałów dla tego uplinku.
- Ruch VM otrzyma 100 ze 150 udziałów, co stanowi 66,7% całego linku 1 Gb/s, czyli w sumie 0,667 Gb/s lub około 667 Mb/s.
- Ruch *vMotion* otrzyma 50 ze 150 udziałów, co stanowi 33,3% całego linku 1 Gb/s, czyli w sumie 0,333 Gb/s lub około 333 Mb/s.

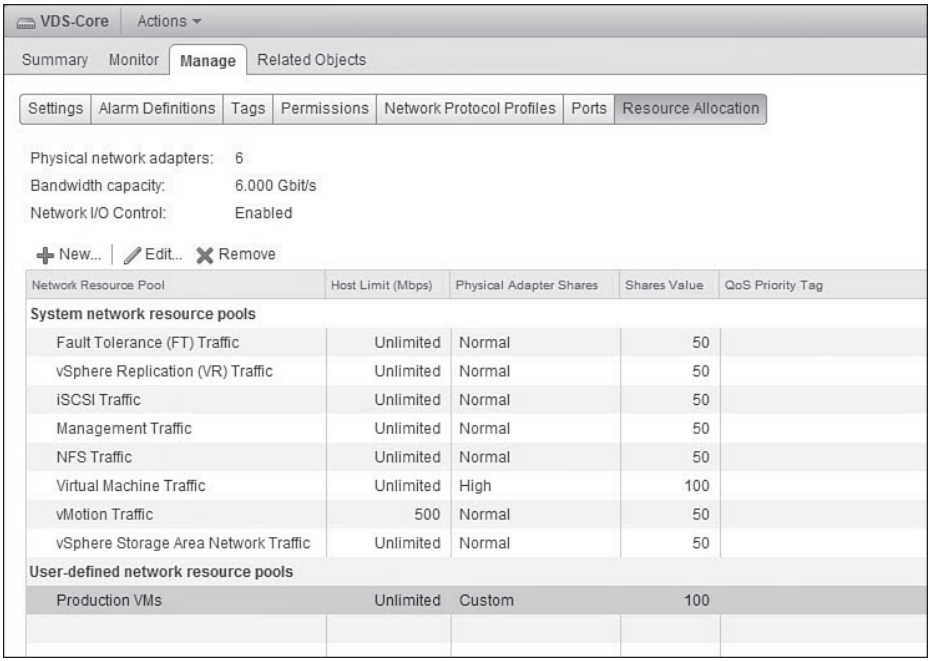
Pamiętaj, że udziały mają zastosowanie tylko w kontrolowaniu aktywnego ruchu. W scenariuszu, który właśnie omówiliśmy, zakładamy, że ruchy VM i *vMotion* były aktywne i powodowały rywalizację. Jeśli cały uplink byłby zajęty tylko przez ruch VM i nie występowałby żaden ruch *vMotion*, nie miałoby miejsce ograniczenie ruchu — byłby tylko jeden rodzaj aktywnego ruchu (ruch VM). Ruch VM otrzymywałby 100% przepustowości uplinku aż do pojawienia się ruchu *vMotion*.

Pule zasobów sieciowych definiowane przez użytkownika

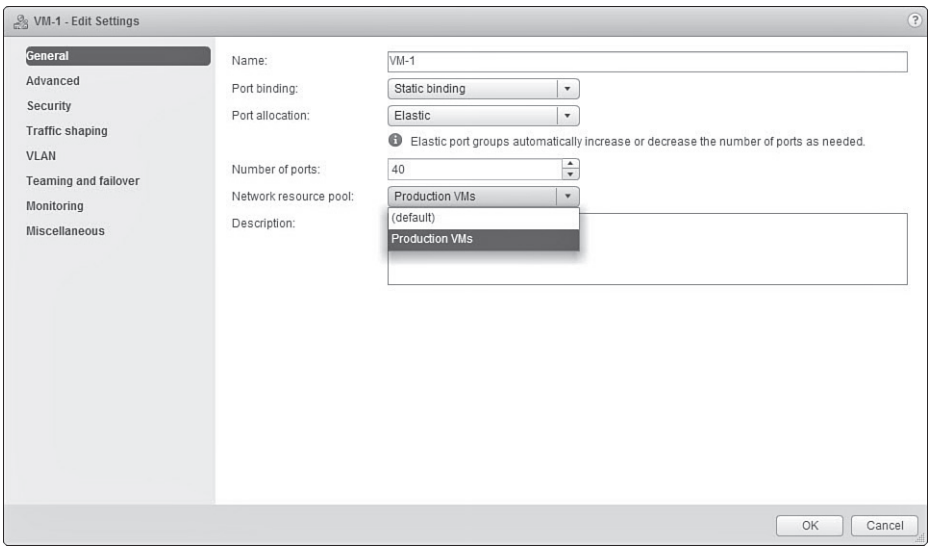
Poza systemowymi pulami zasobów sieciowych, które są predefiniowane w vSphere i nie mogą być usunięte, otrzymujesz możliwość tworzenia własnych niestandardowych pul zasobów. Są one używane przez wybrane przez Ciebie grupy portów VM, takie jak te przeznaczone dla celów produkcyjnych, programistycznych czy dla kluczowych maszyn wirtualnych. Pula zasobów zdefiniowana przez użytkownika została przedstawiona na rysunku 9.19.

Następnie można zastosować daną pulę zasobów sieciowych bezpośrednio do grupy portów, aby upewnić się, że wszystkim maszynom wirtualnym, które wykorzystują tę grupę portów, zostaną przyznane wartości konfiguracji NIOC. Ten proces został przedstawiony na rysunku 9.20.

Wszystkie maszyny wirtualne, które nie zostały przypisane do zdefiniowanej przez użytkownika puli zasobów sieciowych, będą korzystać ze zdefiniowanej systemowo puli o nazwie *Virtual Machine Traffic*. Można ją wykorzystać jako uniwersalną pulę zasobów dla wszystkiego, co nie ma zdefiniowanych żadnych konkretnych reguł.



RYSUNEK 9.19. Moja nowo utworzona niestandardowa pula zasobów sieciowych o nazwie „Production VMs”



RYSUNEK 9.20. Zastosowanie utworzonej puli zasobów sieciowych o nazwie „Production VMs” do rozproszonej grupy portów VM-1

Podsumowanie

W tym rozdziale opisano architekturę przełącznika vSphere Distrubuted Switch oraz wskazano, jakie dodatkowe funkcje oferuje on w stosunku do przełącznika standardowego. Należą do nich: obsługa protokołu LLDP, NetFlow, Port Mirroring, prywatne sieci VLAN, kształtowanie ruchu *egress*, ulepszone mechanizmy równoważenia obciążenia oraz kontrola NIOC. W następnym rozdziale omówione zostaną: przełącznik Cisco Nexus 1000V oraz funkcje, którymi różni się on od przełącznika VDS.

Skorowidz

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

V

W

Z

Obowiązkowa lektura dla administratorów sieci komputerowych!

Rosnący ruch sieciowy i coraz większa ilość przetwarzanych danych sprawiają, że wciąż rośnie także liczba serwerów, które trzeba zaprząc do pracy. Czy musi się to wiązać z koniecznością rozbudowy serwerowni? Stawianiem nowych budynków oraz zwiększeniem przestrzeni? Niekoniecznie! Na pomoc przychodzi wirtualizacja systemów komputerowych. Dzięki wirtualnym środowiskom administratorzy są w stanie zapanować nad infrastrukturą oraz zapewnić ciągłość działania centrów danych czy chmur obliczeniowych.

Jeżeli jesteś administratorem, a do Twoich obowiązków należy dbanie o wirtualne systemy, trafiłeś na doskonałą książkę. Znajdziesz w niej najistotniejsze informacje dotyczące wirtualnych środowisk opartych na rozwiązaniach firmy VMware — jednego z liderów na rynku wirtualizacji. Lektura tej fantastycznej książki pozwoli Ci przypomnieć sobie model TCP/IP oraz OSI, a następnie przejść do zgłębiania wiedzy na temat najróżniejszych protokołów sieciowych. Ponadto przekonasz się, jak budować VLAN-y w wirtualnym świecie, używać różnych urządzeń sieciowych oraz rozwiązywać typowe problemy. Książka ta jest doskonałą i obowiązkową lekturą dla wszystkich administratorów korzystających z dobrodziejstw wirtualizacji lub chcących się tego nauczyć.

DZIĘKI TEJ KSIĄŻCE:

- stworzysz własne laboratorium do testowania różnych konfiguracji sieciowych
- poznasz protokoły wykorzystywane we współczesnych sieciach
- opanujesz techniki kształtowania ruchu
- skonfigurujesz VLAN-y
- Twoja sieć będzie bardziej niezawodna

Christopher Wahl — ma bogate, ponad 10-letnie doświadczenie w branży IT. W swojej karierze zajmował się projektowaniem i wdrażaniem skomplikowanych infrastruktur klasy enterprise. Przyczynił się do powstania wielu centrów danych oraz prywatnych chmur obliczeniowych. Aktualnie pracuje jako starszy architekt w firmie Ahead.

Steven Pantol — od 14 lat pełni różne funkcje w świecie IT. Większość z nich dotyczy technologii VMware. Na co dzień pracuje jako starszy architekt w firmie Ahead. Zajmuje się budowaniem coraz lepszych centrów danych oraz propagowaniem technologii chmury.

Helion

35313 numer katalogowy

księgarnia internetowa

http://helion.pl

zamówienia telefoniczne

0 801 339900

0 601 339900

Sprawdź najnowsze promocje:
http://helion.pl/promocje
Książki najchętniej czytane:
http://helion.pl/bestsellery
Zamów informacje o nowościach:
http://helion.pl/nowosci

Helion SA
ul. Kościuszki 1c, 44-100 Gliwice
tel.: 32 230 98 63
e-mail: helion@helion.pl
http://helion.pl

Informatyka w najlepszym wydaniu

sięgnij po WIĘCEJ

KOD KORZYŚCI

ISBN 978-83-283-0696-7

9 788328 306967

cena: 67,00 zł