Nick Marshall

Mike Brown, G. Blair Fritz,
Ryan Johnson

Przedmowa: Pat Gelsinger

VMware vSphere® 6.7
od podstaw

Helion

SYBEX
A Wiley Brand

Tytuł oryginału: Mastering VMware vSphere 6.7

Tłumaczenie: Lech Lachowski (rozdz. 1 – 7, dodatek), Andrzej Watrak (wprowadzenie, rozdz. 8 – 14, dodatek)

ISBN: 978-83-283-6349-6

Helion SA
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)

Printed in Poland.

Spis treści

Rozdział 5.

Tworzenie i konfigurowanie sieci vSphere

W ostatecznym rozrachunku wszystko sprowadza się do sieci. Posiadanie serwerów z uruchomionym hipernadzorcą VMware ESXi i z wirtualnymi maszynami przechowywanymi w wysoce redundantnej pamięci masowej to w sumie świetna sprawa, ale to wszystko będzie właściwie bezużyteczne, jeśli maszyny wirtualne nie będą mogły komunikować się poprzez sieć. Na nic nie zda się uruchomienie 10, 20, 30 czy nawet większej liczby serwerów produkcyjnych na pojedynczym hoście ESXi, jeśli te serwery nie będą dostępne dla klientów w sieci. Okazuje się więc, że dla każdego administratora vSphere kluczowa jest dogłębna znajomość zagadnień dotyczących sieci vSphere w ramach ESXi.

W TYM ROZDZIALE:

- komponenty sieci vSphere,
- tworzenie standardowych i rozproszonych przełączników vSphere,
- tworzenie grup kart sieciowych, VLAN-ów i prywatnych VLAN-ów oraz zarządzanie nimi,
- konfigurowanie reguł bezpieczeństwa przełączników wirtualnych.

Tworzenie sieci vSphere

Projektowanie i budowanie sieci vSphere z wykorzystaniem hipernadzorcy ESXi i serwera vCenter w pewnym stopniu przypomina projektowanie i budowanie sieci fizycznych, ale mimo wszystko te dwie dziedziny na tyle się różnią, że warto zrobić przegląd komponentów i terminologii związanych z sieciami wirtualnymi. Zanim zajmiemy się omawianiem czynników wpływających na projektowanie sieci w środowisku wirtualnym, zdefiniujmy najpierw komponenty, których można używać do budowania takiej sieci.

vSphere Standard Switch (standardowy przełącznik vSphere). Przełącznik programowy, który rezyduje w systemie operacyjnym VMkernel i zapewnia zarządzanie ruchem dla maszyn wirtualnych. Użytkownicy muszą zarządzać standardowymi przełącznikami vSphere niezależnie na poszczególnych hostach ESXi. W tej książce **standardowy przełącznik vSphere** będziemy nierzadko nazywać po prostu **przełącznikiem wirtualnym** (ang. *vSwitch*).

vSphere Distributed Switch (rozproszony przełącznik vSphere). Przełącznik programowy, który rezyduje w systemie operacyjnym VMkernel i zapewnia zarządzanie ruchem dla maszyn wirtualnych i systemu VMkernel. Rozproszone przełączniki vSphere są współdzielone i zarządzane przez różne hosty ESXi i klastry w obrębie centrum danych vSphere.

W tej książce **przełącznik rozproszony vSphere** będziemy nierzadko nazywać po prostu **przełącznikiem rozproszonym** lub używać skrótowca **VDS** pochodzącego od jego angielskiej nazwy.

Port/Port Group (port lub grupa portów). Logiczny obiekt w standardowym lub rozproszonym przełączniku vSphere, który zapewnia wyspecjalizowane usługi dla systemu VMkernel lub maszyn wirtualnych. Każdy wirtualny przełącznik może mieć port VMkernel lub grupę portów maszyn wirtualnych, które w rozproszonym przełączniku vSphere są nazywane rozproszonymi grupami portów.

VMkernel Port (port VMkernel). Wyspecjalizowany typ portu przełącznika wirtualnego skonfigurowany z adresem IP, który umożliwia hipernadzorcy rejestrowanie działania takich elementów jak ruch zarządzania, vMotion, VMware vSAN, pamięć masowa iSCSI, pamięć masowa NFS (ang. *Network File System*), vSphere Replication oraz vSphere Fault Tolerance (FT). Porty VMkernel są również tworzone dla punktów końcowych (VTEP) tunelu VXLAN, który jest używany przez platformę wirtualizacji i bezpieczeństwa sieci VMware NSX. Te porty VMkernel tworzy się ze stosem TCP/IP VXLAN, a nie przy użyciu stosu domyślnego. Stosy TCP/IP omówimy w dalszej części tego rozdziału. Port VMkernel jest również nazywany **vmknic**.

Virtual Machine Port Group (grupa portów maszyn wirtualnych). Grupa portów przełącznika wirtualnego, które posiadają wspólną konfigurację i umożliwiają maszynom wirtualnym dostęp do innych maszyn wirtualnych skonfigurowanych w tej samej grupie portów albo znajdujących się w dostępnej sieci PVLAN lub sieci fizycznej.

Virtual LAN (wirtualna sieć LAN, tzw.VLAN). Logiczna sieć lokalna skonfigurowana na przełączniku wirtualnym lub fizycznym, która dzięki dostarczaniu ruchu tylko do portów skonfigurowanych dla określonego VLAN-u zapewnia wydajną segmentację ruchu, kontrolę ruchu broadcastowego (rozgłoszeniowego), bezpieczeństwo oraz efektywne wykorzystanie przepustowości.

Trunk Port (port trunkowy, tzw. trunking). Port na fizycznym przełączniku, który nasłuchuje ruchu przeznaczonego dla różnych VLAN-ów i wie, jak ten ruch do nich przekazać. W tym celu wykorzystuje znaczniki VLAN-ów zgodne ze standardem 802.1q dla ruchu przechodzącego przez port trunkowy do podłączonych urządzeń. Porty trunkowe są zwykle używane do połączeń między przełącznikami, aby umożliwić VLAN-om swobodny przepływ między nimi. Wirtualne przełączniki obsługują sieci VLAN, a używanie dla nich trunków umożliwia VLAN-om swobodny przepływ do tych przełączników.

TRUNKING I AGREGACJA ŁĄCZY

W zależności od dostawcy internetowego możesz spotkać się z tym, że termin *trunk* będzie również używany do opisania agregacji wielu pojedynczych łączy w jedno łącze logiczne. W tej książce słowo *trunk* opisuje połączenie, które transmituje znaczniki wielu VLAN-ów. **Agregacja łączy** (ang. *link aggregation*) odnosi się do praktyki łączenia ze sobą wielu indywidualnych łączy.

Access Port (port dostępu). Port na fizycznym przełączniku, który przekazuje ruch tylko dla jednego VLAN-u. W przeciwieństwie do portu trunkowego, który dla przechodzącego przez niego ruchu wykorzystuje identyfikację VLAN-ów, port dostępu usuwa dla przechodzącego przez niego ruchu informacje o VLAN-ach.

Network Interface Card Team (grupa kart sieciowych). Agregacja fizycznych kart interfejsów sieciowych (ang. *network interface card* — NIC), która tworzy pojedynczy logiczny kanał komunikacji. Różne typy grup kart sieciowych (ang. *NIC team*) zapewniają różne poziomy równoważenia obciążenia ruchem i odporności na awarie.

VMXNET Adapter (karta sieciowa VMXNET). Zwirtualizowana karta sieciowa działająca w systemie operacyjnym gościa. Karta sieciowa VMXNET jest zoptymalizowana pod kątem wydajności maszyny wirtualnej. Aby zapewnić sterownik karty sieciowej VMXNET, w systemie operacyjnym gościa muszą być zainstalowane narzędzia VMware. Karta sieciowa VMXNET jest czasem określana mianem **sterownika parawirtualizowanego**.

VMXNET 2 Adapter (karta sieciowa VMXNET 2). Jest oparta na karcie sieciowej VMXNET, ale zapewnia część funkcjonalności wysokiej wydajności powszechnie stosowanych w nowoczesnych sieciach, takich jak ramki jumbo i odciążenia sprzętowe. Aby zapewnić sterownik karty sieciowej VMXNET 2, w systemie operacyjnym gościa muszą być zainstalowane narzędzia VMware.

VMXNET 3 Adapter (karta sieciowa VMXNET 3). Jest to parawirtualizowana karta sieciowa nowej generacji, zaprojektowana pod kątem wydajności i nie jest związana z kartami sieciowymi VMXNET lub VMXNET 2. Oferuje wszystkie funkcjonalności dostępne w VMXNET 2 i dodaje kilka nowych funkcji, takich jak obsługa wielokolejkowania (w systemie Windows znanego również jako skalowanie po stronie odbierającej, ang. *Receive Side Scsling*), odciążenia IPv6 i dostarczanie przerwań MSI/MSI-X. Aby zapewnić sterownik karty sieciowej VMXNET 3, wymagany jest sprzęt maszyn wirtualnych w wersji co najmniej 7, a w systemie operacyjnym gościa muszą być zainstalowane narzędzia VMware.

E1000 Adapter (karta sieciowa E1000). Zwirtualizowana karta sieciowa, która emuluje gigabitową kartę sieciową Intel 82545EM. Zazwyczaj system operacyjny gościa zapewnia wbudowany sterownik dla tej karty.

Adapter E1000e (karta sieciowa E1000e). Zwirtualizowana karta sieciowa, który emuluje gigabitową kartę sieciową Intel 82574. E1000e wymaga sprzętu maszyn wirtualnych w wersji co najmniej 8. Ta karta sieciowa jest dostępna dla systemów operacyjnych Windows 8 i nowszych; nie jest dostępna dla systemu Linux.

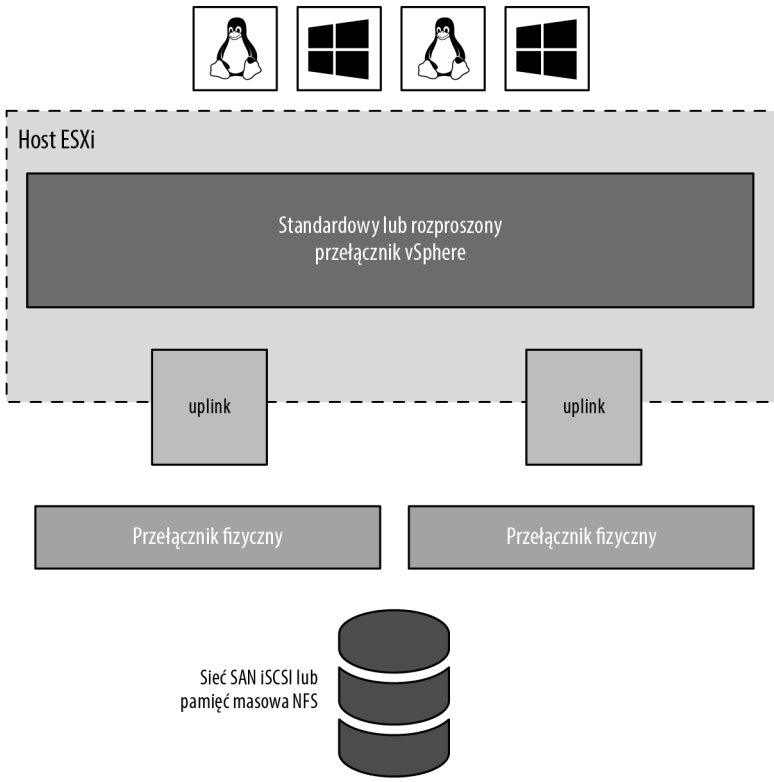
Skoro masz już pewną wiedzę na temat komponentów i terminologii, z którymi będziesz miał do czynienia w tym rozdziale, zobaczmy, jak te komponenty współpracują ze sobą w celu wspierania działania maszyn wirtualnych, pamięci masowej opartej na protokole IP oraz hostów ESXi.

Odpowiedzi na poniższe pytania w dużej mierze determinować będą Twoje projekty sieci vSphere:

- Czy potrzebujesz dedykowanej sieci dla ruchu zarządzania lub może ją masz, na przykład do zarządzania przełącznikami fizycznymi?
- Czy masz dedykowaną sieć lub może jej potrzebujesz dla ruchu vMotion?
- Czy masz sieć pamięci masowej IP? Czy ta sieć pamięci masowej IP jest siecią dedykowaną? Korzystasz z protokołu iSCSI czy NFS? Czy planujesz zaimplementowanie VMware vSAN?
- Ile kart sieciowych ma standardowo Twój projekt hosta ESXi?
- Czy karty sieciowe w hostach obsługują Gigabit Ethernet, 10 Gigabit Ethernet, 25 Gigabit Ethernet, czy 40 Gigabit Ethernet?
- Czy potrzebujesz bardzo wysokich poziomów odporności na awarie dla maszyn wirtualnych?
- Czy istniejąca sieć fizyczna składa się z VLAN-ów?
- Czy chcesz rozszerzyć wykorzystanie sieci VLAN na przełączniki wirtualne?
- Czy korzystając z NSX, będziesz do swojej sieci wprowadzać nakładki, takie jak VXLAN lub Geneve?

Jako prekursor konfiguracji architektury sieciowej vSphere musisz zidentyfikować i udokumentować komponenty sieci fizycznej i wymagania bezpieczeństwa dla tej sieci. Ważne jest także poznanie architektury istniejącej sieci fizycznej, ponieważ ma to również duży wpływ na projekt sieci vSphere. Jeśli sieć fizyczna nie obsługuje na przykład VLAN-ów, wówczas projekt sieci vSphere musi uwzględniać to ograniczenie.

W tym rozdziale omówimy szczegółowo różne komponenty sieci vSphere. Otrzymasz również wskazówki dotyczące tego, w jaki sposób różne komponenty wpasowują się w ogólny projekt sieci vSphere. Udany projekt sieci vSphere łączy ze sobą sieć fizyczną, karty sieciowe i przełączniki wirtualne, jak pokazano na rysunku 5.1.



RYSUNEK 5.1. Udany projekt sieci vSphere to połączenie wirtualnych i fizycznych kart sieciowych oraz przełączników

Ponieważ implementacja sieci vSphere zapewnia dostęp do maszyn wirtualnych, kluczowe jest, aby ta sieć została skonfigurowana w sposób zapewniający niezawodną i wydajną komunikację pomiędzy różnymi komponentami infrastruktury sieciowej.

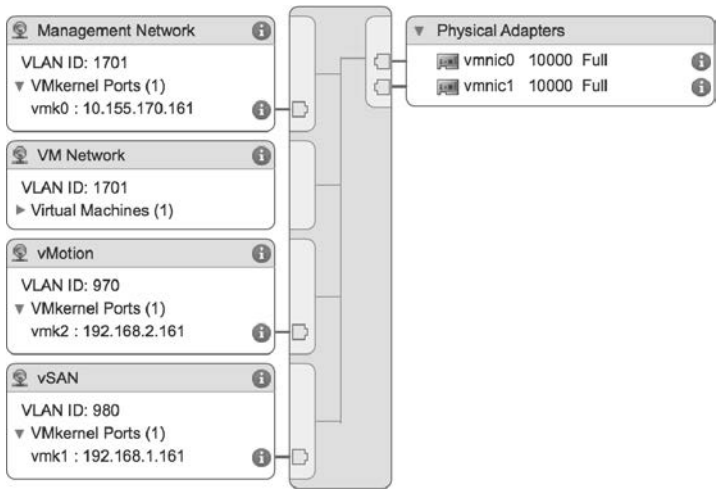
Praca ze standardowymi przełącznikami vSphere

Architektura sieciowa ESXi obraca się wokół tworzenia i konfigurowania wirtualnych przełączników. Te przełączniki wirtualne to standardowe przełączniki vSphere lub rozproszone przełączniki vSphere. Najpierw omówimy standardowe, a potem rozproszone przełączniki vSphere.

Standardowe przełączniki vSphere są tworzone i zarządzane za pośrednictwem klienta internetowego vSphere lub interfejsu CLI vSphere przy użyciu polecenia `esxcli`, ale działają w systemie operacyjnym VMkernel. Przełączniki wirtualne zapewniają komunikację sieciową pomiędzy różnymi komponentami, na przykład:

- między maszynami wirtualnymi na danym hoście ESXi,
- między maszynami wirtualnymi na różnych hostach ESXi,
- między maszynami wirtualnymi oraz innymi wirtualnymi lub fizycznymi identyfikatorami sieciowymi podłączonymi za pośrednictwem sieci fizycznej,
- między systemem VMkernel i sieciami w celu rejestrowania aktywności różnych funkcjonalności, takich jak Management, vMotion, VMware vSAN, iSCSI, NFS, vSphere Replication lub Fault Tolerance.

Spójrz na rysunek 5.2, na którym pokazano, w jaki sposób klient internetowy vSphere przedstawia standardowy przełącznik vSphere na hoście ESXi. Na tym rysunku widzimy jednak nie tylko sam standardowy przełącznik vSphere; mamy tam również grupy portów i uplinki służące do komunikacji zewnętrznej względem hosta. Bez uplinków przełącznik wirtualny nie mógłby komunikować się z siecią upstreamową, a bez grup portów standardowy przełącznik vSphere nie mógłby zapewnić łączności dla systemu VMkernel lub maszyn wirtualnych. Właśnie dlatego, omawiając przełączniki wirtualne, będziemy koncentrować się w dużej mierze na grupach portów i uplinkach.



RYSUNEK 5.2. Same standardowe przełączniki vSphere nie zapewnią łączności; potrzebują grup portów i uplinków, aby zapewnić łączność zewnętrzną względem hosta ESXi

Najpierw przyjrzyjmy się jednak wirtualnym przełącznikom oraz ich podobieństwom i różnicom w stosunku do fizycznych przełączników w sieci.

Porównywanie przełączników wirtualnych i fizycznych

Przełączniki wirtualne w ESXi są konstruowane przez system operacyjny VMkernel i w nim działają. Ponadto nie są przełącznikami zarządzalnymi i nie zapewniają tych wszystkich zaawansowanych funkcjonalności oferowanych przez wiele nowoczesnych przełączników fizycznych. Z przełącznikiem wirtualnym nie można na przykład połączyć się za pomocą telnetu, aby zmodyfikować jego ustawienia. Oprócz poleceń interfejsu vSphere CLI, takich jak `esxcli`, lub poleceń PowerCLI, takich jak `New-VirtualPortGroup`, przełącznik wirtualny nie ma żadnego interfejsu wiersza poleceń

(ang. *command-line interface* — CLI). Mimo to pod pewnymi względami działanie przełącznika wirtualnego przypomina działanie przełącznika fizycznego. Przełącznik wirtualny, podobnie jak jego fizyczny odpowiednik, działa w warstwie drugiej: utrzymuje tablice adresów MAC, przekazuje ramki do portów innych przełączników na podstawie adresów MAC, obsługuje konfiguracje VLAN-ów, zapewnia trunking VLAN-ów przy użyciu znaczników IEEE 802.1q i może ustanawiać kanały zwane port channel. Przełącznik rozproszony vSphere obsługuje również PVLAN-y, pod warunkiem że są one obsługiwane na fizycznych przełącznikach upstreamowych. Podobnie jak przełączniki fizyczne, przełączniki wirtualne są skonfigurowane z określoną liczbą portów.

Pomimo tych podobieństw przełączniki wirtualne różnią się nieco od przełączników fizycznych. Standardowy przełącznik vSphere nie obsługuje dynamicznych protokołów negocjacyjnych, takich jak DTP (ang. *Dynamic Trunking Protocol*) lub LACP (ang. *Link Aggregation Control Protocol*), wykorzystywanych do ustanawiania trunków 802.1q lub kanałów port channel. Jednak rozproszony przełącznik vSphere obsługuje LACP w obu trybach: aktywnym i pasywnym. Przełącznika wirtualnego nie można podłączyć do innego przełącznika wirtualnego, co eliminuje potencjalne skonfigurowanie pętli. Ponieważ nie ma możliwości powstania pętli, przełączniki wirtualne nie stosują protokołu STP (ang. *Spanning Tree Protocol*), czyli protokołu drzewa rozpinającego.

PROTOKÓŁ DRZEWA ROZPINAJĄCEGO

W przełącznikach fizycznych protokół STP oferuje redundancję dla ścieżek i zapobiega powstawaniu pętli w topologii sieci, blokując redundantne ścieżki i utrzymując je w trybie gotowości. STP aktywuje będącą w trybie gotowości redundantną ścieżkę tylko wtedy, gdy jakaś używana ścieżka przestaje być dostępna.

Istnieje pewna możliwość połączenia ze sobą przełączników wirtualnych za pomocą maszyny wirtualnej z oprogramowaniem mostkującym (ang. *bridging software*) warstwy drugiej i wieloma wirtualnymi kartami sieciowymi, ale skonfigurowanie i uruchomienie tej opcji wymagałoby nieco wysiłku.

- Przełączniki wirtualne i przełączniki fizyczne różnią się od siebie również pod innymi względami: przełącznik wirtualny posiada autorytatywną wiedzę o adresach MAC podłączonych do niego maszyn wirtualnych, więc nie ma potrzeby, aby uczył się adresów MAC z sieci.
- Ruch odbierany przez przełącznik wirtualny na jednym uplinku nigdy nie jest przekazywany dalej przez inny uplink. Jest to kolejny powód, dla którego przełączniki wirtualne nie korzystają z protokołu drzewa rozpinającego.
- Przełącznik wirtualny nie musi stosować szpiegowania IMGP (ang. *Internet Group Management Protocol snooping* — IGMP snooping), ponieważ wie, jakie transmisje multicastowe będą przeprowadzać podłączone do niego maszyny wirtualne.

Jak widać na podstawie tej listy różnic, przełączników wirtualnych po prostu nie można używać w ten sam sposób, w jaki wykorzystuje się przełączniki fizyczne. Nie można na przykład użyć przełącznika wirtualnego jako ścieżki tranzytowej między dwoma przełącznikami fizycznymi, ponieważ ruch odbierany na jednym uplinku nie będzie przekazywany dalej na drugi uplink.

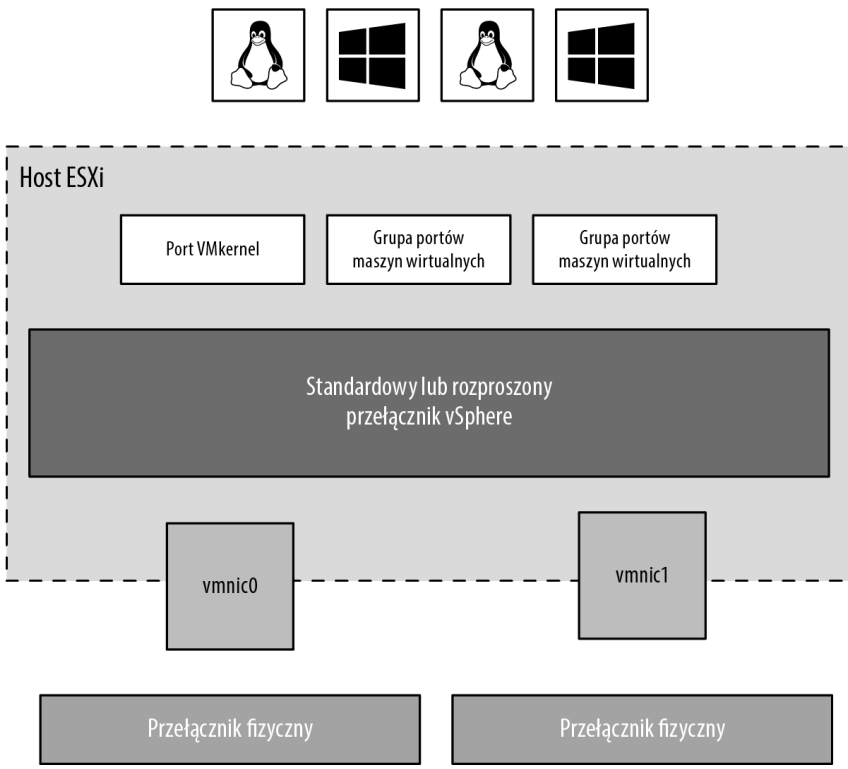
Posiadając tę podstawową wiedzę na temat działania przełączników wirtualnych, przyjrzyjmy się teraz portom i grupom portów.

Porty i grupy portów

Jak wyjaśniliśmy wcześniej, przełącznik wirtualny umożliwia kilka różnych rodzajów komunikacji, w tym komunikację w kierunku VMkernel i odwrotną oraz między maszynami wirtualnymi. Aby łatwiej było rozróżnić te różnorakie typy komunikacji, hosty ESXi używają portów i grup portów. Standardowy przełącznik vSphere bez portów lub grup portów jest jak przełącznik fizyczny, który nie ma fizycznych portów. Do takiego przełącznika nie można w żaden sposób nic podłączyć, więc nie służy on żadnemu celowi.

Grupy portów określają typy ruchu przechodzącego przez przełącznik wirtualny, a ponadto działają jako granice wykorzystywane w konfiguracji komunikacji i (lub) reguł bezpieczeństwa. Rysunki 5.3 i 5.4 pokazują dwa różne typy portów i grup portów, które można skonfigurować na przełączniku wirtualnym:

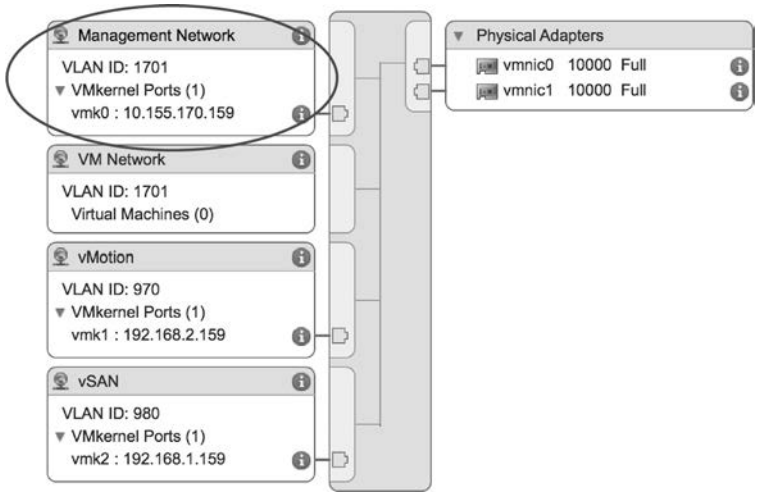
- port VMkernel,
- grupa portów maszyn wirtualnych.



RYSUNEK 5.3. Przełączniki wirtualne mogą zawierać dwa typy połączeń: port VMkernel i grupę portów maszyn wirtualnych

Ponieważ przełącznika wirtualnego nie można używać w żaden sposób bez przynajmniej jednego portu lub grupy portów, przekonasz się, że klient internetowy łączy tworzenie nowych przełączników wirtualnych z tworzeniem nowych portów lub grup portów.

Jak pokazano wcześniej na rysunku 5.2, porty i grupy portów stanowią tylko część całościowego rozwiązania. Jego kolejną częścią są uplinki, o których również należy pamiętać, ponieważ zapewniają łączność pomiędzy zewnętrzną siecią i przełącznikami wirtualnymi.



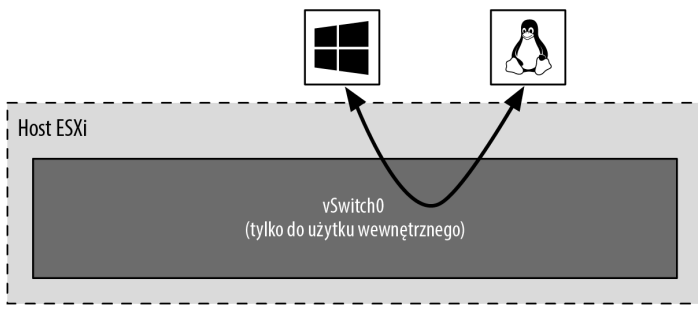
RYSUNEK 5.4. Możesz tworzyć przełączniki wirtualne posiadające jednocześnie oba typy połączeń

Uplinki

Chociaż przełącznik wirtualny umożliwia komunikację między podłączonymi do niego maszynami wirtualnymi, nie może komunikować się z siecią fizyczną bez tak zwanych uplinków. Podobnie jak fizyczny przełącznik musi być podłączony do innych przełączników w celu zapewnienia komunikacji w sieci, tak przełączniki wirtualne muszą być podłączone do fizycznych kart sieciowych hosta ESXi, aby zapewnić uplinki wykorzystywane do komunikacji z resztą sieci.

W przeciwieństwie do portów i grup portów uplinki nie są wymagane do działania przełącznika wirtualnego. Fizyczne systemy podłączone do wyizolowanego przełącznika fizycznego bez żadnych uplinków do innych przełączników fizycznych z sieci nadal mogą komunikować się ze sobą — po prostu nie mogą komunikować się z innymi systemami, które nie są podłączone do tego samego wyizolowanego przełącznika. Podobnie maszyny wirtualne podłączone do przełącznika wirtualnego bez żadnych uplinków mogą komunikować się ze sobą, ale nie mogą komunikować się z maszynami wirtualnymi z innych przełączników wirtualnych lub systemami fizycznymi.

Ten rodzaj konfiguracji jest znany jako przełącznik wirtualny **tylko do użytku wewnętrznego** (ang. *internal-only vSwitch*) lub po prostu wewnętrzny przełącznik wirtualny. Umożliwienie maszynom wirtualnym komunikowania się tylko między sobą może być użyteczne. Maszyny wirtualne, które się komunikują za pośrednictwem wewnętrznego przełącznika wirtualnego, nie przekazują żadnego ruchu przez fizyczną kartę sieciową hosta ESXi. Jak pokazano na rysunku 5.5, komunikacja między maszynami wirtualnymi podłączonymi do wewnętrznego przełącznika wirtualnego odbywa się wyłącznie na płaszczyźnie oprogramowania i z prędkością, z jaką VMkernel może wykonać dane zadanie.



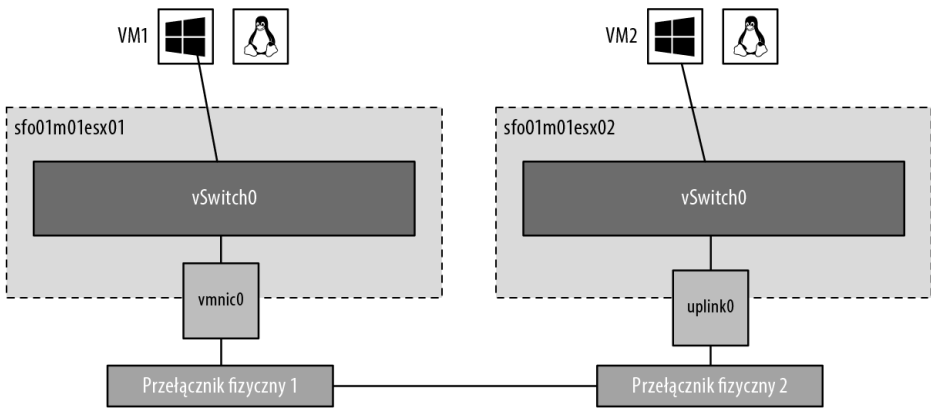
RYSUNEK 5.5. Maszyny wirtualne komunikujące się poprzez wewnętrzny przełącznik wirtualny nie przekazują żadnego ruchu przez fizyczną kartę sieciową

BEZ UPLINKU NIE MOŻNA KORZYSTAĆ Z VMOTION?

W starszych wersjach vSphere maszyny wirtualne podłączone do wewnętrznego przełącznika wirtualnego nie były w stanie obsługiwać vMotion. Chociaż w nowszych wersjach vSphere wymagania dotyczące uplinków zostały złagodzone, dopiero w vSphere 6 zmieniony został przepływ pracy związany z migracją maszyny za pomocą vMotion. Gdy chcesz przeprowadzić migrację vMotion, możesz wybrać docelową grupę portów. Ta grupa portów może znajdować się na standardowym lub rozproszonym przełączniku wirtualnym i jest to prawidłowe miejsce docelowe niezależnie od tego, czy przełącznik wirtualny, o którym mowa, ma jakiekolwiek uplinki. Pełne wymagania dotyczące vMotion zostały omówione w rozdziale 12. „Równoważenie wykorzystania zasobów".

Aby maszyny wirtualne mogły komunikować się z zasobami znajdującymi się poza maszynami wirtualnymi hostowanymi na lokalnym hoście ESXi lub gdy włączony jest PVLAN, przełącznik wirtualny musi być skonfigurowany do korzystania z co najmniej jednej fizycznej karty sieciowej, czyli uplinku. Przełącznik wirtualny można powiązać z pojedynczą kartą sieciową lub z kilkoma.

Przełącznik wirtualny powiązany z co najmniej jedną fizyczną kartą sieciową pozwala maszynom wirtualnym ustanowić komunikację z serwerami fizycznymi w sieci lub z maszynami wirtualnymi na innych hostach ESXi. Zakładamy przy tym oczywiście, że wspomniane maszyny wirtualne na innych hostach ESXi są podłączone do przełącznika wirtualnego powiązanego z co najmniej jedną fizyczną kartą sieciową. Podobnie jak sieć fizyczna, tak i sieć wirtualna wymaga łączności na obu krańcach. Rysunek 5.6 pokazuje ścieżkę komunikacji dla maszyn wirtualnych podłączonych do przełącznika wirtualnego powiązanego z fizyczną kartą sieciową. Na tym schemacie *vm1* na *sfo01m01esx01* musi komunikować się z *vm2* na *sfo01m01esx02*, a ruch z maszyny wirtualnej przechodzi przez *vSwitch0* (poprzez grupę portów maszyny wirtualnej) do fizycznej karty sieciowej, z którą powiązany jest ten przełącznik wirtualny. Z fizycznej karty sieciowej ruch dociera do fizycznego przełącznika (*Przełącznik fizyczny 1*). Ten przełącznik fizyczny przekazuje ruch do drugiego przełącznika fizycznego (*Przełącznik fizyczny 2*), który przekazuje ruch poprzez fizyczną kartę sieciową powiązaną z przełącznikiem wirtualnym na *sfo01m01esx02*. Na ostatnim etapie komunikacji przełącznik wirtualny przekazuje ruch do docelowej maszyny wirtualnej *vm2*.



RYSUNEK 5.6. Przełącznik wirtualny z przypisaną jedną kartą sieciową pozwala maszynom wirtualnym komunikować się z fizycznym serwerami i innymi maszynami wirtualnymi w sieci

Przełącznik wirtualny powiązany z fizyczną kartą sieciową zapewnia maszynom wirtualnym taką ilość przepustowości, jaką potrafi obsługiwać dana karta sieciowa. Podczas komunikowania się z maszynami fizycznymi lub maszynami wirtualnymi na innych hostach ESXi wszystkie maszyny

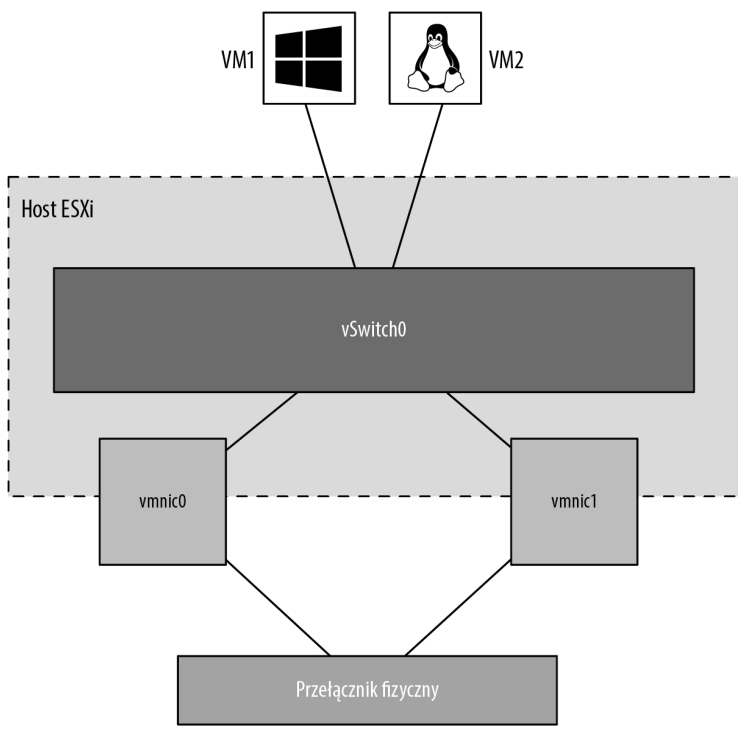
wirtualne będą współdzielić tę przepustowość. Tym samym przełącznik wirtualny po raz kolejny wykazuje podobieństwo do przełącznika fizycznego. Przełącznik wirtualny skonfigurowany na przykład z pojedynczą kartą sieciową 1 Gb/s zapewni podłączonym do niego maszynom wirtualnym do 1 Gb/s przepustowości. Podobnie fizyczny przełącznik z uplinkiem 1 Gb/s do innego przełącznika fizycznego zapewni pomiędzy tymi dwoma przełącznikami do 1 Gb/s przepustowości dla podłączonych do nich systemów.

Przełącznik wirtualny można również skonfigurować z wieloma fizycznymi kartami sieciowymi.

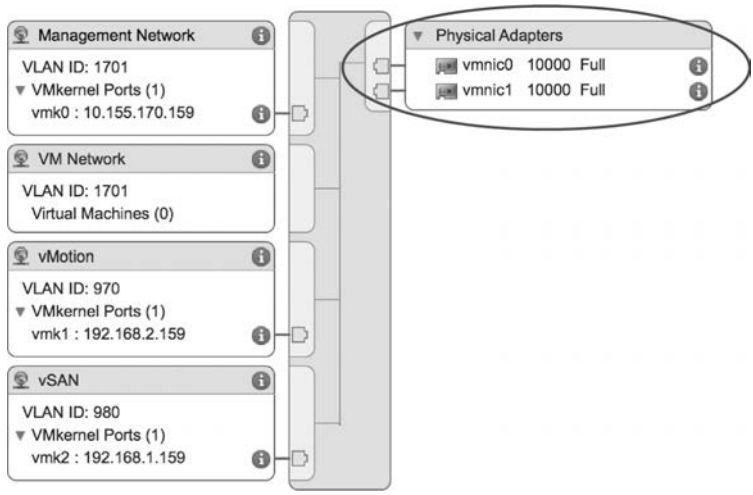
LIMITY UPLINKÓW

Chociaż pojedynczy przełącznik wirtualny może być skonfigurowany z wieloma fizycznymi kartami sieciowymi, pojedynczej fizycznej karty sieciowej nie można przypisać do wielu przełączników wirtualnych. Hosty ESXi mogą mieć wiele kart sieciowych z różnymi prędkościami. Liczba kart sieciowych zależy od chipsetu. Informacje na temat liczby kart sieciowych obsługiwanych przez konkretne chipsety znajdziesz w przewodniku *vSphere Maximums* (*https://configmax.vmware.com*).

Rysunki 5.7 i 5.8 pokazują przełącznik wirtualny skonfigurowany z wieloma fizycznymi kartami sieciowymi. Przełącznik wirtualny może mieć maksymalnie 32 uplinki. Innymi słowy, pojedynczy przełącznik wirtualny może używać nawet 32 fizycznych kart sieciowych do wysyłania ruchu do sieci fizycznej i odbierania go z niej. Skonfigurowanie na przełączniku wirtualnym wielu fizycznych kart sieciowych ma tę zaletę, że zapewnia redundancję i dystrybucję obciążenia. Tego rodzaju konfiguracją przełącznika wirtualnego zajmiemy się szczegółowo w punkcie „Konfigurowanie grupowania kart sieciowych" w dalszej części tego rozdziału.



RYSUNEK 5.7. Przełącznik wirtualny korzystający z grupy kart sieciowych ma dostępnych wiele interfejsów do transferu danych. Grupowanie kart sieciowych oferuje redundancję i dystrybucję obciążenia



RYSUNEK 5.8. Przełączniki wirtualne korzystające z grupowania kart sieciowych można poznać po tym, że przypisanych jest do nich wiele fizycznych adapterów

UWAGA

Należy zwrócić uwagę, że grupowanie kart sieciowych określa sposób obsługi ruchu na wielu uplinkach i nie należy go traktować jako typu agregacji łączy, takiego jak LACP.

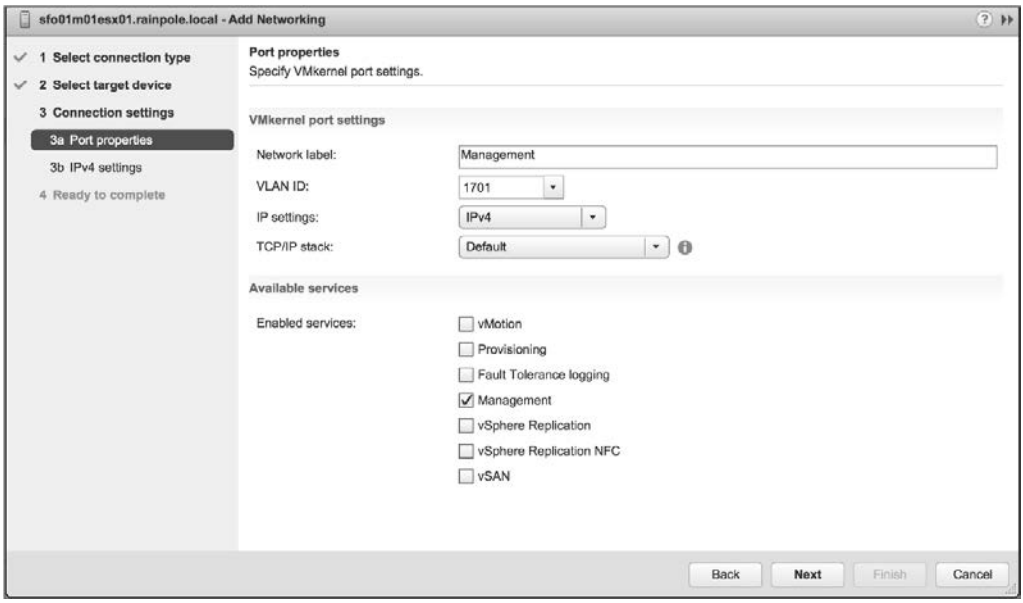
Przyjrzeliśmy się przełącznikom wirtualnym, portom i grupom portów oraz uplinkom. Powinieneś mieć już podstawowe wyobrażenie o tym, w jaki sposób te elementy zaczynają się ze sobą łączyć, tworząc wirtualną sieć. Następny krok polega na zagłębieniu się w konfigurację różnych typów portów i grup portów, ponieważ są one niezbędne w sieciach vSphere. Zaczniemy od omówienia sieci zarządzania.

Konfigurowanie sieci zarządzania

Ruch zarządzania to specjalny rodzaj ruchu sieciowego, który jest przesyłany przez port VMkernel. Porty VMkernel zapewniają dostęp sieciowy dla stosu TCP/IP systemu VMkernel. Jest to osobny ruch niezależny od ruchu sieciowego generowanego przez maszyny wirtualne. Sieć zarządzania hostami ESXi jest jednak pod dwoma względami traktowana nieco inaczej niż pozostałe porty VMkernel:

- Po pierwsze port VMkernel służący do zarządzania hostami ESXi jest tworzony automatycznie podczas instalacji ESXi. Aby host ESXi był dostępny w sieci, port VMkernel zarządzania musi być skonfigurowany i działający.
- Po drugie Direct Console User Interface (DCUI) — czyli interfejs użytkownika, o którym mówimy, kiedy pracujesz na fizycznej konsoli serwera z uruchomionym ESXi — zapewnia mechanizm do konfigurowania lub rekonfigurowania sieci zarządzania (portu Management VMKernel). Poza kilkoma opcjami resetowania konfiguracji sieciowej nie umożliwia on jednak konfigurowania żadnych innych form sieci na tym hoście.

Chociaż klient internetowy vSphere oferuje możliwość włączenia ruchu zarządzania podczas konfigurowania sieci (jak widać na rysunku 5.9), mało prawdopodobne, abyś często korzystał z tej opcji. W końcu do skonfigurowania sieci zarządzania z poziomu klienta internetowego vSphere host ESXi musi już mieć działającą sieć zarządzania (serwer vCenter komunikuje się z hostami ESXi za pośrednictwem sieci zarządzania). Tej opcji mógłbyś użyć, gdybyś tworzył dodatkowe interfejsy zarządzania. W tym celu skorzystałbyś z procedury opisanej w dalszej części rozdziału (w punkcie „Konfigurowanie sieci VMkernel"), aby za pomocą klienta internetowego vSphere utworzyć porty VMkernel, włączając po prostu ruch *Management* w sekcji *Enable Services* (włączone usługi) podczas tworzenia portu VMkernel.



RYSUNEK 5.9. Klient internetowy vSphere oferuje sposób włączenia sieci Management podczas konfigurowania ustawień sieciowych

Gdy host ESXi jest nieosiągalny — i dlatego nie można go skonfigurować za pomocą klienta internetowego vSphere — do skonfigurowania sieci zarządzania należy użyć interfejsu DCUI.

Aby skonfigurować sieć zarządzania ESXi za pomocą DCUI, wykonaj następujące czynności:

1. W fizycznej konsoli serwera lub za pomocą narzędzia zdalnej konsoli, takiego jak HP iLO lub Dell DRAC, naciśnij przycisk *F2*, aby przejść do menu *System Customization* (dostosowywanie systemu).

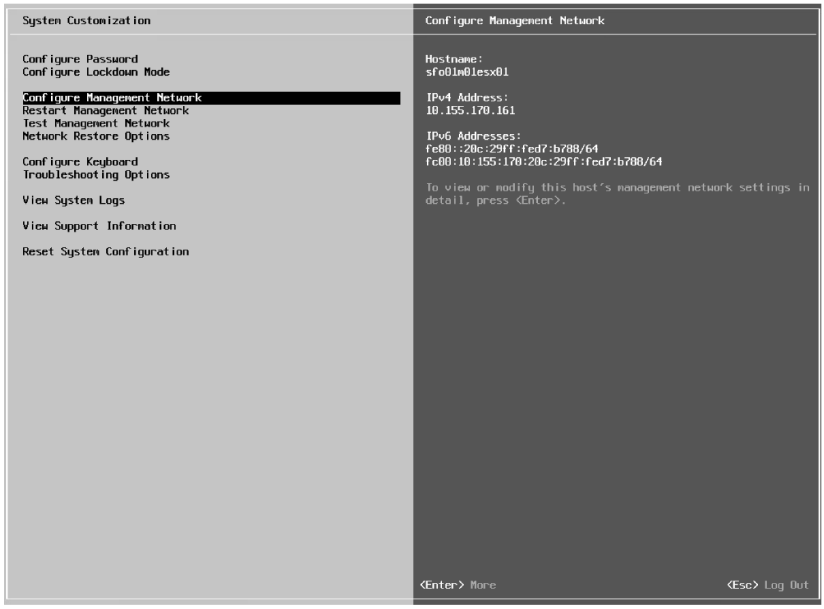
   Po wyświetleniu monitu o zalogowanie się wprowadź odpowiednie poświadczenia.

2. Użyj przycisków strzałek, aby podświetlić opcję *Configure Management Network* (konfigurowanie sieci zarządzania), jak pokazano na rysunku 5.10, i naciśnij *Enter*.

3. Z menu *Configure Management Network* wybierz odpowiednią opcję dla skonfigurowania sieci zarządzania ESXi, jak pokazano na rysunku 5.11.

   Nie można stąd tworzyć dodatkowych interfejsów sieci zarządzania; możesz tylko zmodyfikować istniejący interfejs sieci zarządzania.

4. Po zakończeniu postępuj zgodnie z instrukcjami wyświetlanymi na ekranie, aby wyjść z konfiguracji sieci zarządzania.

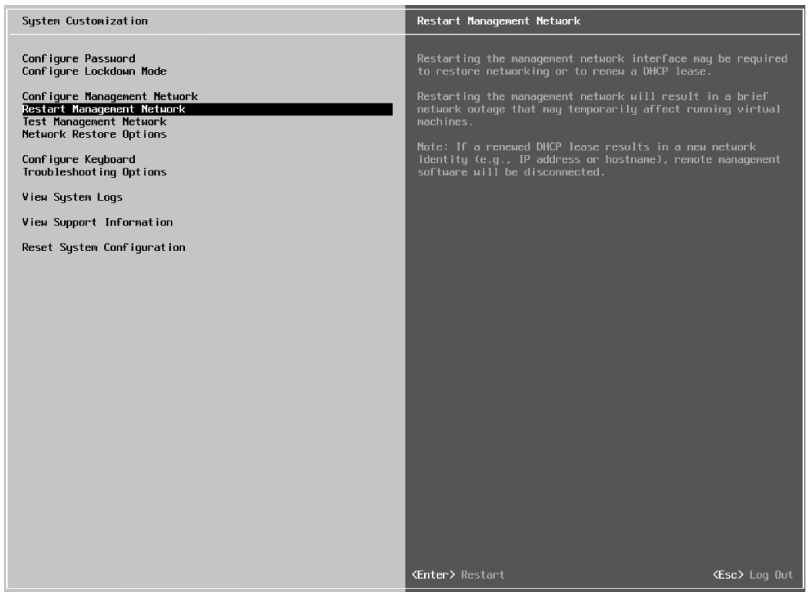


RYSUNEK 5.10. Konfigurowanie sieci zarządzania ESXi za pomocą opcji Configure Management Network w menu System Customization

RYSUNEK 5.11. Z poziomu menu Configure Management Network użytkownicy mogą modyfikować przypisane karty sieciowe, zmieniać identyfikator VLAN-u, adres IP, serwery DNS oraz konfigurację wyszukiwania DNS

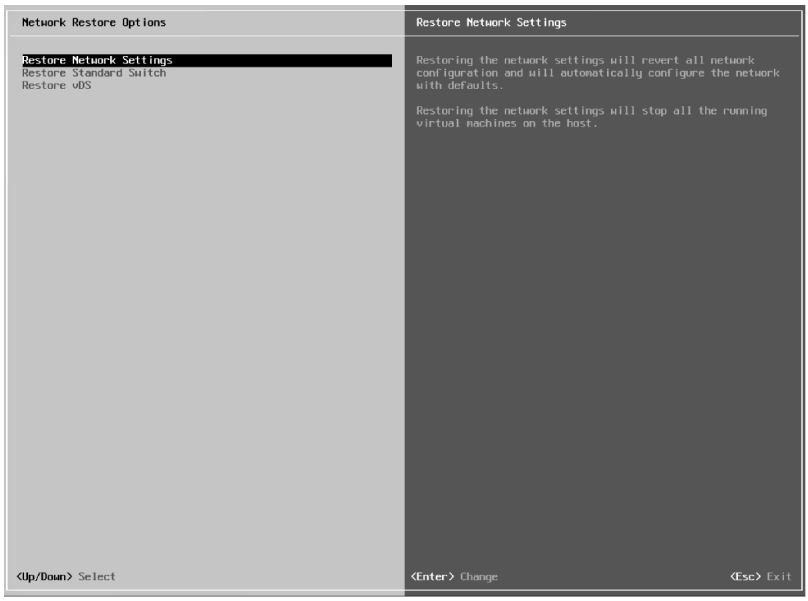
Jeśli wyświetlone zostanie zapytanie o ponowne uruchomienie sieci zarządzania, wybierz *Yes* (tak); w przeciwnym razie zrestartuj sieć zarządzania z menu *System Customization*, jak pokazano na rysunku 5.12.

Przyglądając się rysunkom 5.10 i 5.12, zauważysz także opcje testowania sieci zarządzania, które pozwalają sprawdzić, czy jest ona poprawnie skonfigurowana. To bardzo przydatne, jeśli nie jesteś pewien identyfikatora VLAN-u lub kart sieciowych, których powinieneś użyć.



RYSUNEK 5.12. Opcja Restart Management Network powoduje zrestartowanie sieci zarządzania ESXi i zastosowanie wszelkich wprowadzonych zmian

Zwróć także uwagę na ekran *Network Restore Options* (opcje przywracania ustawień sieciowych), pokazany na rysunku 5.13. Dostępne tu opcje pozwalają przywrócić domyślną konfigurację sieci, standardowy przełącznik vSphere, a nawet rozproszony przełącznik vSphere — wszystkie są bardzo przydatne w przypadku rozwiązywania problemów związanych z łącznością sieci zarządzania z hostem ESXi.

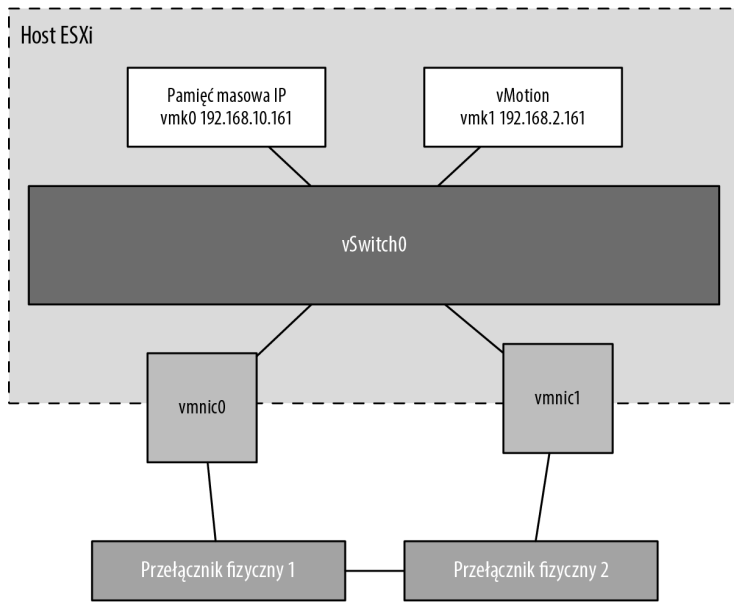


RYSUNEK 5.13. Użyj ekranu Network Restore Options do zarządzania łącznością sieciową z hostem ESXi

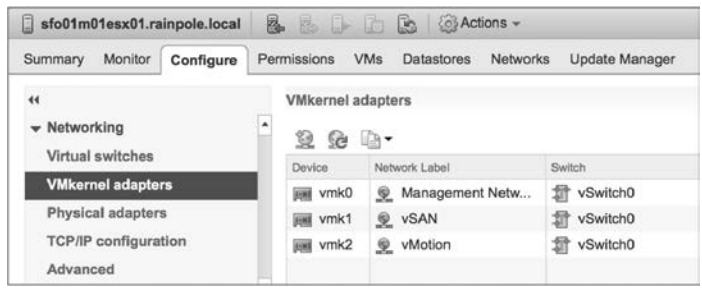
Jednak sieć VMkernel to nie tylko sam ruch zarządzania. Przyjrzyjmy się teraz innym typom ruchu VMkernel oraz sposobom tworzenia i konfigurowania portów VMkernel.

Konfigurowanie sieci VMkernel

Sieć VMkernel przenosi nie tylko ruch związany z zarządzaniem, ale także wszystkie inne typy ruchu, które pochodzą z samego hosta ESXi (tzn. każdy ruch, który nie jest generowany przez maszyny wirtualne działające na tym hoście ESXi). Jak pokazano na rysunkach 5.14 i 5.15, porty VMkernel są używane do takich typów ruchu jak Management, vMotion, vSAN, iSCSI, NFS, vSphere Replication i vSphere FT — czyli w zasadzie do wszystkich rodzajów ruchu generowanego przez samego hipernadzorcę. Rozdział 6. „Tworzenie i konfigurowanie urządzeń pamięci masowej" szczegółowo opisuje konfiguracje iSCSI i NFS oraz konfigurację vSAN. Z kolei rozdział 12. zawiera szczegółowe informacje na temat procesu vMotion i działania vSphere FT. Oba te rozdziały dotyczą więc przepływu ruchu między systemem VMkernel a urządzeniami pamięci masowej (iSCSI, NFS, vSAN) lub innymi hostami ESXi (dla celów vMotion lub vSphere FT). W tym momencie powinieneś przejmować się jednak tylko konfiguracją sieci VMkernel.

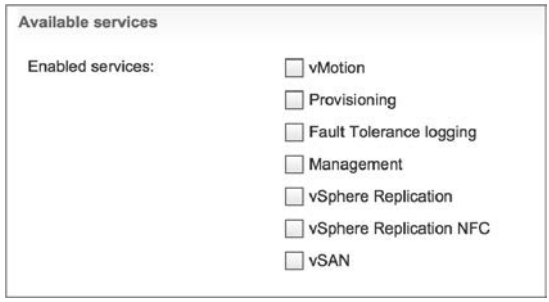


RYSUNEK 5.14. Do adaptera VMkernel przypisano adres IP w celu zapewnienia dostępu do urządzeń pamięci masowej iSCSI lub NFS lub innych usług zarządzania



RYSUNEK 5.15. Do interfejsu VMkernel zaleca się dodawać tylko jeden typ ruchu

W vSphere 6.0 wiele odpowiedzialnych wcześniej za ruch usług zarządzania zostało podzielonych na odrębne usługi, które można podłączyć do unikatowego interfejsu VMkernel. Jak pokazano na rysunku 5.16, te usługi to Provisioning, vSphere Replication i vSphere Replication NFC (Network File Copy).



RYSUNEK 5.16. Typy ruchu VMkernel w vSphere 6.7. Począwszy od wersji vSphere 6.0, porty VMkernel mogą przenosić również ruch Provisioning, vSphere Replication i vSphere Replication NFC

Provisioning obsługuje transfer danych dla klonowania maszyn wirtualnych, migracji wyłączonych lub wstrzymanych maszyn wirtualnych (tzw. migracji na zimno) i tworzenia migawek. Ten proces może generować intensywny ruch, szczególnie gdy nie jest wykorzystywany interfejs VMware vStorage API for Array Integration (VAAI). Może się to zdarzyć w wielu różnych sytuacjach, o czym mowa w artykule 1021976 bazy wiedzy VMware.

vSphere Replication przesyła zreplikowane bloki z hosta ESXi do urządzenia wirtualnego vSphere Replication, natomiast vSphere Replication NFC obsługuje sieciowe kopiowanie plików z urządzenia wirtualnego vSphere Replication do docelowego magazynu danych za pośrednictwem hosta ESXi.

Port VMkernel składa się z dwóch komponentów: grupy portów na przełączniku wirtualnym (vSwitch) i interfejsu sieciowego VMkernel (vmknic).

Aby dodać port VMkernel do istniejącego przełącznika wirtualnego za pomocą klienta internetowego vSphere, wykonaj następujące czynności:

1. Jeśli nie jesteś jeszcze podłączony, otwórz obsługiwaną przeglądarkę internetową i zaloguj się do instancji serwera vCenter. Jeżeli Twoja instancja serwera vCenter nazywa się na przykład *vcenter*, musisz połączyć się z adresem *https://vcenter.domain.name/vsphere-client*, a następnie zalogować się za pomocą odpowiednich poświadczeń.
2. W kliencie internetowym vSphere wybierz *Hosts and Clusters* (hosty i klastry).
3. Rozwiń drzewo *vCenter Server* i wybierz host ESXi, na którym chcesz dodać nowy port VMkernel.
4. Kliknij zakładkę *Configure* (konfigurowanie).
5. Kliknij opcję *VMkernel Adapters* (karty sieciowe VMkernel).
6. Kliknij ikonę *Add Host Networking* (dodaj sieć hosta). Spowoduje to uruchomienie kreatora dodawania sieci.
7. Wybierz *VMkernel Network Adapter* (karta sieciowa VMkernel), a następnie kliknij *Next* (dalej).
8. Ponieważ dodajesz port VMkernel do istniejącego przełącznika wirtualnego, upewnij się, że zaznaczona jest opcja *Select An Existing Standard Switch* (wybierz istniejący przełącznik standardowy); następnie kliknij *Browse* (przeglądaj), aby wybrać przełącznik wirtualny, do którego należy dodać nowy port VMkernel. W oknie dialogowym *Select Switch* (wybierz przełącznik) kliknij *OK* i kliknij *Next*, aby kontynuować.
9. W polu tekstowym *Network Label* (etykieta sieciowa) wpisz nazwę portu.
10. W razie potrzeby określ identyfikator VLAN-u dla portu VMkernel.
11. Wybierz, czy ten port VMkernel będzie obsługiwał protokół IPv4, IPv6, czy oba.

12. Wybierz stos TCP/IP, którego powinien używać ten port VMkernel. Jeżeli nie utworzyłeś żadnego niestandardowego stosu TCP/IP, jedynymi wymienionymi tutaj opcjami będą *Default* (domyślny), *Provisioning* i *vMotion*. (Stosy TCP/IP omówimy w dalszej części rozdziału, w punkcie „Konfigurowanie stosów TCP/IP").
13. Wybierz usługi, które zostaną włączone na tym porcie VMkernel, a następnie kliknij *Next*. W przypadku portu VMkernel, który będzie używany tylko dla ruchu iSCSI lub NFS, należy usunąć zaznaczenie wszystkich pól *Services*. W przypadku portu VMkernel, który będzie działał jako dodatkowy interfejs zarządzania, należy wybrać tylko *Management Traffic*.
14. W przypadku protokołu IPv4 (jeśli w poprzednim kroku w ustawieniach IP wybrałeś *IPv4* lub *IPv4 and IPv6*) możesz wybrać automatyczne pobieranie konfiguracji (za pośrednictwem DHCP) lub wprowadzić konfigurację statyczną.

NADPISYWANIE BRAMY DOMYŚLNEJ NA KARCIE SIECIOWEJ

Jeżeli wybierzesz statyczny adres IPv4, będziesz miał możliwość nadpisania bramy domyślnej i podania bramy specjalnie dla tej karty sieciowej VMkernel. Nie powoduje to jednak dodania wpisu do tabeli routingu hostów ESXi. Z tej bramy będą korzystać tylko usługi, które określają ten VMkernel jako interfejs wyjściowy. Zapewnia to dodatkowe opcje łączności warstwy trzeciej dla usług, które potrzebują wielu bram. Może to być przydatne dla usługi takiej jak vSphere Replication, w przypadku której nie chcemy, aby ruch przechodził przez sieć zarządzania lub nie chcemy tworzyć statycznych tras na hostach ESXi.

SERWERÓW DNS NIE MOŻNA EDYTOWAĆ

Zwróć uwagę, że adresy serwerów DNS są kontrolowane przez konfigurację stosu TCP/IP i nie mogą być tutaj zmieniane. Aby zmienić ustawienia serwera DNS, musisz dokonać edycji ustawień stosu TCP/IP, jak opisano w punkcie „Konfigurowanie stosów TCP/IP".

15. W przypadku protokołu IPv6 (jeśli wcześniej w ustawieniach IP wybrałeś *IPv6* lub *IPv4 and IPv6*) możesz wybrać opcję automatycznego pobierania konfiguracji poprzez DHCPv6, automatycznego pobierania konfiguracji za pośrednictwem rozgłoszeń routera i (lub) przypisać co najmniej jeden adres IPv6. Aby dodać adres IPv6 odpowiedni dla sieci, do której zostanie podłączony ten interfejs VMkernel, użyj zielonego symbolu plusa.
16. Kliknij *Next*, aby przejrzeć podsumowanie konfiguracji, a następnie kliknij *Finish* (zakończ).

Po wykonaniu tych czynności możesz użyć polecenia `Get-VMHostNetworkAdapter PowerCLI`, aby wyświetlić nowy port VMkernel i nową kartę sieciową VMkernel, które zostały utworzone:

```
Connect-VIServer <nazwa_hosta_ESXi>
```

Po wyświetleniu monitu o zalogowanie się wprowadź odpowiednie poświadczenia.

```
Get-VMHostNetworkAdapter -VMkernel | Format-list
```

Aby lepiej zilustrować różne elementy tworzone podczas tego procesu, czyli port VMkernel oraz kartę sieciową VMkernel (vmknic), omówmy jeszcze raz kroki, które pozwalają utworzyć port VMkernel za pomocą PowerCLI.

Aby utworzyć port VMkernel na istniejącym przełączniku wirtualnym za pomocą wiersza poleceń, wykonaj następujące czynności:

1. Otwórz PowerCLI i połącz się z hostem ESXi, wprowadzając następujące polecenie:

   ```
   Connect-VIServer <nazwa_hosta_ESXi>
   ```

   Po wyświetleniu monitu o zalogowanie się wprowadź odpowiednie poświadczenia.

2. Wpisz poniższe polecenie, aby dodać grupę portów o nazwie *VMkernel* do przełącznika *vSwitch0*:

   ```
   New-VirtualPortGroup -Name VMkernel -VirtualSwitch vSwitch0
   ```

3. Użyj poniższego polecenia, aby wyświetlić listę grup portów na przełączniku *vSwitch0*. Zwróć uwagę, że grupa portów istnieje, ale nic nie zostało do niej podłączone (kolumna *Port* jest pusta).

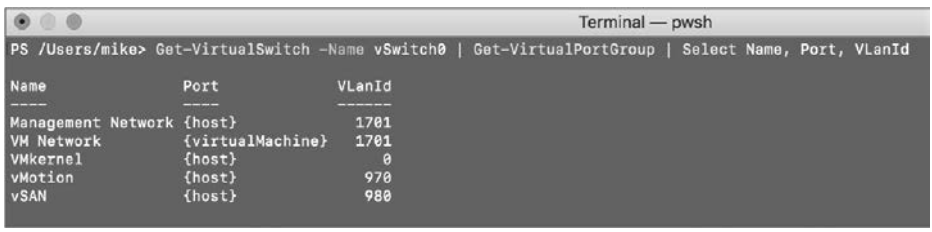
   ```
   Get-VirtualSwitch -Name vSwitch0 | Get-VirtualPortGroup | Select Name,
   Port, VLanId
   ```

4. Wpisz następujące polecenie, aby utworzyć port VMkernel z określonym adresem IP i dołączyć go do grupy portów utworzonej w kroku 2.:

   ```
   New-VMHostNetworkAdapter -PortGroup VMkernel -VirtualSwitch vSwitch0 -IP
   <Adres_IP> -SubnetMask <Maska_podsieci>
   ```

5. Powtórz polecenie z kroku 3. Zwróć uwagę, że w kolumnie *Port* wyświetlana jest teraz wartość *{host}*.

   Oznacza to, że karta sieciowa VMkernel została podłączona do wirtualnego portu w tej grupie portów. Rysunek 5.17 pokazuje dane wyjściowe z polecenia PowerCLI po wykonaniu kroku 5.

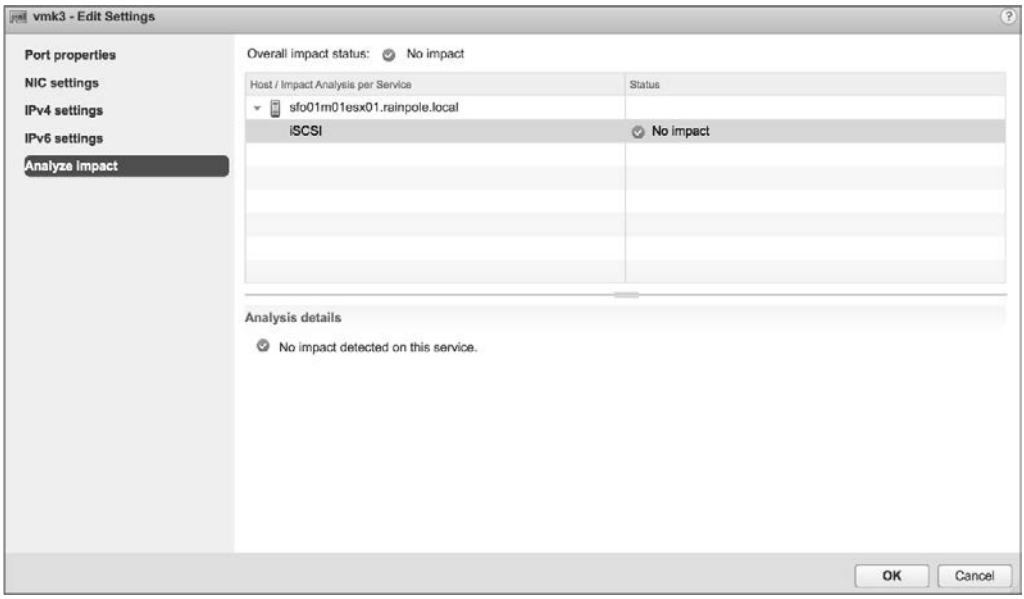


RYSUNEK 5.17. Korzystanie z CLI pomaga sprawdzić, czy grupa portów i port VMkernel to oddzielne obiekty

Poza domyślnymi portami wymaganymi dla sieci zarządzania podczas instalacji ESXi nie są tworzone żadne porty VMkernel, więc musisz utworzyć porty VMkernel dla usług wymaganych w Twoim środowisku. W tym celu możesz skorzystać z klienta internetowego vSphere lub interfejsu CLI.

Oprócz dodawania portów VMkernel konieczna może być edycja portu VMkernel, a nawet jego usunięcie. Oba te zadania możesz wykonać w tym samym miejscu, w którym dodałeś port VMkernel, czyli w sekcji *Networking* zakładki *Configure* dla hosta ESXi.

Aby edytować żądany port VMkernel, wybierz go z listy i kliknij ikonę *Edit Settings* (edycja ustawień), która wygląda jak ołówek. Spowoduje to wyświetlenie okna dialogowego *Edit Settings*, umożliwiającego zmianę usług, dla których ten port jest włączony, zmianę wartości MTU (ang. *maximum transmission unit*) oraz modyfikowanie ustawień IPv4 i (lub) IPv6. Szczególnie interesująca jest tutaj sekcja *Analyze Impact* (analiza wpływu) pokazana na rysunku 5.18. Pomaga ona wskazać zależności na porcie VMkernel w celu uniknięcia niepożądanych efektów ubocznych, które mogą wynikać z modyfikacji konfiguracji portu VMkernel.



RYSUNEK 5.18. Sekcja Analyze Impact pokazuje zależności administracyjne na portach VMkernel

Aby usunąć żądany port VMkernel, wybierz go z listy i kliknij przycisk *Remove Selected Virtual Network Adapter* (usuń wybraną wirtualną kartę sieciową), który wygląda jak czerwony znak *X*. W wyświetlonym oknie dialogowym potwierdzenia zobaczysz opcję służącą do analizy wpływu (tak samo jak w przypadku modyfikacji portu VMkernel). Kliknij przycisk *OK*, aby usunąć ten port VMkernel.

Włączanie rozszerzonych funkcji multicastowych

W vSphere 6.0 do przełączników wirtualnych vSphere zostały dodane dwa nowe tryby filtrowania ruchu multicastowego: podstawowe filtrowanie multicastowe i snooping multicastowy.

Standardowy przełącznik vSphere obsługuje tylko podstawowe filtrowanie multicastowe, więc snooping multicastowy zostanie omówiony w podrozdziale „Praca z rozproszonymi przełącznikami vSphere" w dalszej części rozdziału.

W trybie podstawowego filtrowania multicastowego standardowy przełącznik będzie przekazywał ruch multicastowy dla maszyn wirtualnych zgodnie z docelowym adresem MAC grupy multicastowej. Kiedy maszyna wirtualna dołącza do grupy multicastowej, działający w niej system operacyjny wysyła do standardowego przełącznika adres MAC tej grupy. Standardowy przełącznik zapisuje w lokalnej tabeli przekazywania mapowanie między portem, do którego podłączona jest maszyna wirtualna, a docelowym multicastowym adresem MAC.

Standardowy przełącznik odpowiada za wysyłanie komunikatów IGMP bezpośrednio do lokalnego routera multicastowego, który następnie interpretuje żądanie dołączenia maszyny wirtualnej do grupy lub usunięcia jej z grupy.

Oceniając podstawowe filtrowanie multicastowe, należy wziąć pod uwagę pewne ograniczenia:

- Przełącznik wirtualny nie jest zgodny ze specyfikacją IGMP w wersji 3, dotyczącą filtrowania pakietów zgodnie z jego adresem źródłowym.

- Adres MAC grupy multicastowej może być współdzielony przez maksymalnie 32 różne grupy, co może spowodować, że maszyna wirtualna będzie odbierać pakiety, którymi nie jest zainteresowana.
- Ze względu na ograniczenia w modelu przekazywania, jeśli maszyna wirtualna zostanie zasubskrybowana do ponad 32 multicastowych adresów MAC, będzie otrzymywać niechciane pakiety.

Dużą zaletą podstawowego filtrowania multicastowego jest to, że jest domyślnie włączone, więc nie trzeba poświęcać czasu na jego konfigurowanie!

Konfigurowanie stosów TCP/IP

Przed wydaniem vSphere 5.5 wszystkie interfejsy VMkernel współużytkowały pojedynczą instancję stosu TCP/IP. W rezultacie współdzieliły tę samą tabelę routingu i konfigurację DNS. W niektórych środowiskach tworzyło to ciekawe wyzwania. Mogło dojść na przykład do sytuacji, w której potrzebowałeś bramy domyślnej dla sieci zarządzania, ale potrzebna była również brama domyślna dla ruchu vMotion. Jedynym obejściem było użycie pojedynczej bramy domyślnej, a następnie wypełnienie tablicy routingu statycznymi trasami. Oczywiście nie jest to zbyt skalowalne rozwiązanie, jeśli trzeba zapewnić solidną lub unikatową sieć VMkernel.

Obecnie vSphere umożliwia tworzenie wielu stosów TCP/IP, a zostało to wprowadzone w vSphere 5.5. Każdy stos ma własną tablicę routingu i własną konfigurację DNS.

Przyjrzyjmy się, jak tworzyć stosy TCP/IP. Po utworzeniu co najmniej jednego dodatkowego stosu TCP/IP dowiesz się, jak przypisać interfejs VMkernel do określonego stosu.

Tworzenie stosu TCP/IP

Nowe instancje stosu TCP/IP można tworzyć tylko z poziomu wiersza poleceń, używając polecenia `esxcli`.

Aby utworzyć nowy stos TCP/IP, użyj poniższego polecenia:

```
esxcli network ip netstack add --netstack=<Nazwa_nowego_stosu_TCP/IP>
```

Gdybyś chciał na przykład utworzyć osobny stos TCP/IP dla ruchu NFS, polecenie mogłoby wyglądać mniej więcej tak:

```
esxcli network ip netstack add --netstack=NFS
```

Listę wszystkich skonfigurowanych stosów TCP/IP możesz uzyskać za pomocą bardzo podobnego polecenia `esxcli`:

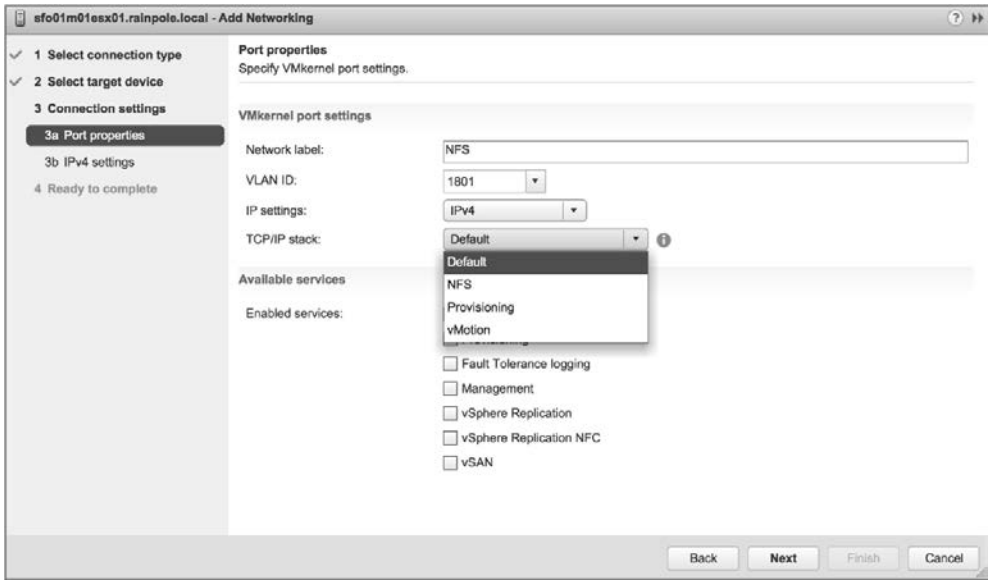
```
esxcli network ip netstack list
```

Po utworzeniu nowego stosu TCP/IP możesz kontynuować konfigurowanie go za pomocą polecenia `esxcli`. Prawdopodobnie łatwiej będzie jednak skorzystać w tym celu z klienta internetowego vSphere, jak opisano w następnym podpunkcie.

Przypisywanie portów do stosu TCP/IP

Aby móc edytować ustawienia stosu TCP/IP, należy mu przypisać port VMkernel. Niestety porty VMkernel można przypisywać do stosu TCP/IP tylko w momencie ich tworzenia. Innymi słowy, po utworzeniu portu VMkernel nie można zmienić stosu TCP/IP, do którego został on przypisany. Musisz usunąć port VMkernel, a następnie ponownie go utworzyć, przypisując go do żądanego stosu TCP/IP. Tworzenie i usuwanie portów VMkernel opisaliśmy już wcześniej, więc nie będziemy omawiać tych zadań ponownie.

Zwróć uwagę, że w kroku 12. procesu tworzenia portu VMkernel opisanego w punkcie „Konfigurowanie sieci VMkernel" możesz wybrać określony stos TCP/IP, aby powiązać z nim dany port. Zostało to zilustrowane na rysunku 5.19, na którym widać dostępne do wyboru stosy: *Default*, *vMotion*, *Provisioning* i utworzony wcześniej niestandardowy *NFS*.



RYSUNEK 5.19. Porty VMkernel można przypisywać do stosu TCP/IP tylko w momencie ich tworzenia

NIESTANDARDOWE STOSY VMOTION

vSphere 6.0 było pierwszą wersją zawierającą systemowy stos TCP/IP dla vMotion. Niestety niestandardowych stosów TCP/IP nie można używać do obsługi rejestrowania Fault Tolerance oraz ruchów zarządzania, VMware vSAN, vSphere Replication i vSphere Replication NFC. Po wybraniu niestandardowego stosu TCP/IP zobaczysz, że pola umożliwiające włączenie tych usług automatycznie przestaną być dostępne. Niestandardowych stosów TCP/IP można używać tylko do obsługi pamięci masowych IP, takich jak iSCSI i NFS.

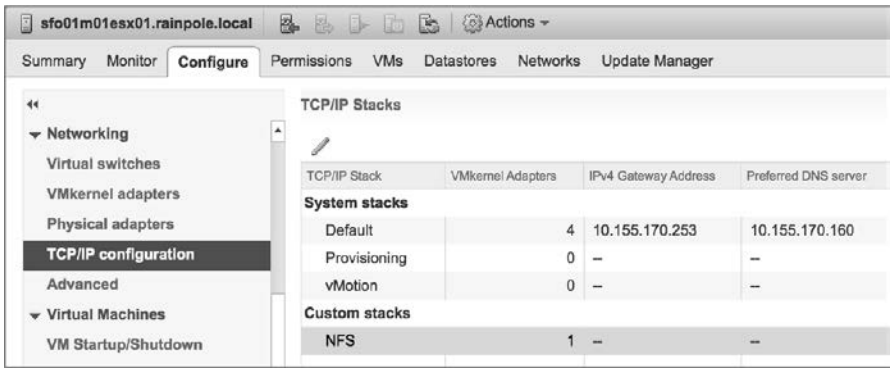
Konfigurowanie ustawień stosu TCP/IP

Ustawienia stosów TCP/IP znajdują się w tym samym miejscu, w którym tworzy się i konfiguruje inne ustawienia sieciowe hosta: w sekcji *Networking* zakładki *Configure* dla obiektu hosta ESXi, jak pokazano na rysunku 5.20.

Na rysunku 5.20 możesz zobaczyć nowy stos TCP/IP o nazwie *NFS*, który został utworzony w poprzednim podpunkcie. Aby edytować ustawienia tego stosu, wybierz go z listy i kliknij znajdującą się nad listą stosów TCP/IP ikonę *Edit TCP/IP Stack Configuration* (edytowanie konfiguracji stosu TCP/IP), która wygląda jak ołówek. Spowoduje to wyświetlenie okna dialogowego *Edit TCP/IP Stack Configuration* pokazanego na rysunku 5.21.

W oknie dialogowym *Edit TCP/IP Stack Configuration* wprowadź wymagane zmiany w nazwie, konfiguracji DNS, routingu lub innych zaawansowanych ustawieniach. Po zakończeniu kliknij *OK*.

Nadszedł czas, aby od ustawień sieciowych hosta przejść do ustawień sieciowych maszyn wirtualnych.



RYSUNEK 5.20. Ustawienia stosu TCP/IP są dostępne wraz z innymi opcjami konfiguracji sieciowej hosta

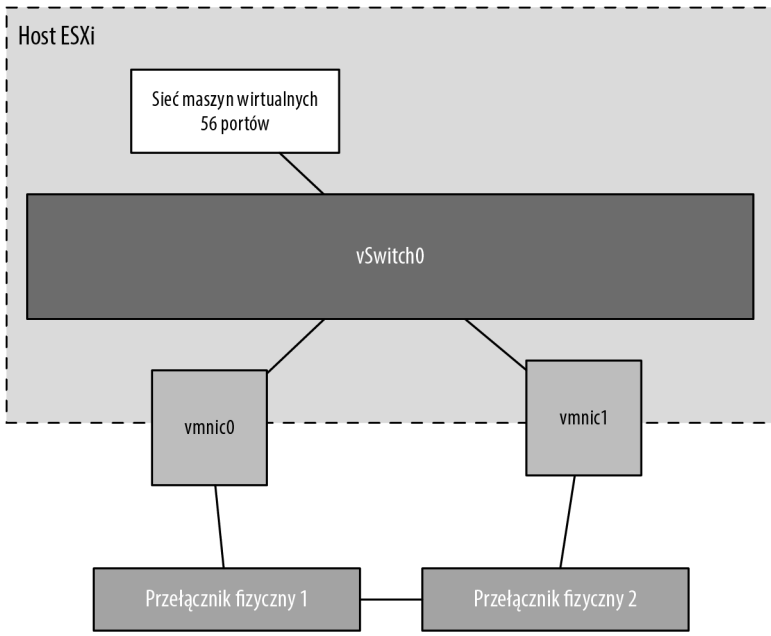
RYSUNEK 5.21. Każdy stos TCP/IP może mieć własną konfigurację DNS, własne informacje o routingu i inne zaawansowane ustawienia

Konfigurowanie sieci maszyn wirtualnych

Omówimy teraz kolejny typ grup portów, czyli grupę portów maszyn wirtualnych, która jest odpowiedzialna za sieć dla wszystkich maszyn wirtualnych. Grupa portów maszyn wirtualnych znacznie różni się od portu VMkernel. W sieci VMkernel istnieje relacja „jeden do jednego" z interfejsem: każda karta sieciowa VMkernel (vmknic) wymaga odpowiadającej jej grupy portów VMkernel na przełączniku wirtualnym. Ponadto interfejsy te wymagają adresów IP dla celów zarządzania lub zapewniania dostępu do sieci VMkernel.

Natomiast grupa portów maszyn wirtualnych nie ma relacji „jeden do jednego" i nie wymaga adresu IP. Zapomnijmy na chwilę o przełącznikach wirtualnych i weźmy pod uwagę standardowe przełączniki fizyczne. Gdy dodajesz do środowiska sieciowego niezarządzalny przełącznik fizyczny, nie wymaga on adresu IP. Po prostu instalujesz przełącznik i podpinasz odpowiednie uplinki, które połączą go z resztą sieci.

Przełącznik wirtualny utworzony z grupą portów maszyn wirtualnych niczym się nie różni. Działa jak dodatkowy niezarządzalny przełącznik fizyczny. Wystarczy podpiąć tylko odpowiednie uplinki — w tym przypadku fizyczne karty sieciowe — które połączą ten przełącznik wirtualny z resztą sieci. Aby połączyć porty przełącznika wirtualnego z portami przełącznika fizycznego, nie trzeba konfigurować adresu IP dla grupy portów maszyn wirtualnych, podobnie jak w przypadku niezarządzalnego przełącznika fizycznego. Rysunek 5.22 ilustruje bezpośrednie połączenie między przełącznikiem wirtualnym i przełącznikiem fizycznym.



RYSUNEK 5.22. Przełącznik wirtualny z grupą portów maszyn wirtualnych wykorzystuje powiązane z nim fizyczne karty sieciowe do ustanowienia bezpośrednich połączeń z przełącznikami fizycznymi

Aby utworzyć przełącznik wirtualny z grupą portów maszyn wirtualnych za pomocą klienta internetowego vSphere, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter przy użyciu klienta internetowego vSphere.
2. W widoku *Hosts and Clusters* rozwiń drzewo *vCenter Server*.
3. Wybierz host ESXi, na którym chcesz dodać przełącznik wirtualny, kliknij zakładkę *Configure* i w sekcji *Networking* kliknij *Virtual Switches* (przełączniki wirtualne).
4. Aby uruchomić kreator dodawania sieci, kliknij ikonę *Add Host Networking* (dodaj sieć hosta), która wygląda jak mała kula ziemska ze znakiem plus.
5. Zaznacz przycisk opcji *Virtual Machine Port Group For A Standard Switch* (grupa portów maszyn wirtualnych dla przełącznika standardowego) i kliknij *Next*.
6. Ponieważ tworzysz nowy przełącznik wirtualny, zaznacz przycisk opcji *New Standard Switch* (nowy przełącznik standardowy). Kliknij *Next*.
7. Kliknij zieloną ikonę ze znakiem plus, aby dodać fizyczne karty sieciowe do nowego przełącznika wirtualnego, który tworzysz. W oknie dialogowym *Add Physical Adapters To The Switch* (dodawanie do przełącznika fizycznych kart sieciowych) wybierz kartę lub karty sieciowe, które mogą przenosić odpowiedni ruch dla maszyn wirtualnych.

8. Po zakończeniu wybierania fizycznych kart sieciowych kliknij *OK*. Spowoduje to powrót do ekranu *Create A Standard Switch* (tworzenie przełącznika standardowego), w którym możesz kliknąć *Next*, aby kontynuować.
9. W polu tekstowym *Network Label* (etykieta sieciowa) wpisz nazwę grupy portów maszyn wirtualnych.
10. W razie potrzeby podaj identyfikator VLAN-u i kliknij *Next*.
11. Kliknij *Next*, aby przejrzeć konfigurację przełącznika wirtualnego, a następnie kliknij *Finish*.

Jeśli jesteś zwolennikiem wiersza poleceń, grupę portów maszyn wirtualnych możesz utworzyć również za pomocą PowerCLI.

Aby utworzyć przełącznik wirtualny z grupą portów maszyn wirtualnych przy użyciu wiersza poleceń, wykonaj następujące czynności:

1. Otwórz PowerCLI i połącz się z serwerem vCenter:

   ```
   Connect-VIServer <nazwa_hosta_vCenter>
   ```

   Po wyświetleniu monitu o zalogowanie się wprowadź odpowiednie poświadczenia.
2. Wpisz poniższe polecenie, aby dodać wirtualny przełącznik o nazwie *vSwitch1* do hosta ESXi o nazwie *sfo01m01esx01*:

   ```
   New-VirtualSwitch -VMhost sfo01m01esx01 -Name vSwitch1
   ```
3. Aby dodać fizyczną kartę sieciową *vmnic1* do przełącznika *vSwitch1*, wpisz następujące polecenie:

   ```
   Set-VirtualSwitch -VirtualSwitch vSwitch1 -Nic vmnic1
   ```

   Dodając fizyczną kartę sieciową do przełącznika wirtualnego, zapewniasz podłączonym do niego maszynom wirtualnym fizyczną łączność z resztą sieci. Pamiętaj, że daną fizyczną kartę sieciową możesz przypisać tylko do jednego przełącznika wirtualnego (ale przełącznik wirtualny może mieć przypisanych jednocześnie wiele fizycznych kart sieciowych).
4. Wpisz poniższe polecenie, aby na przełączniku *vSwitch1* utworzyć grupę portów maszyn wirtualnych o nazwie *ProductionLAN*:

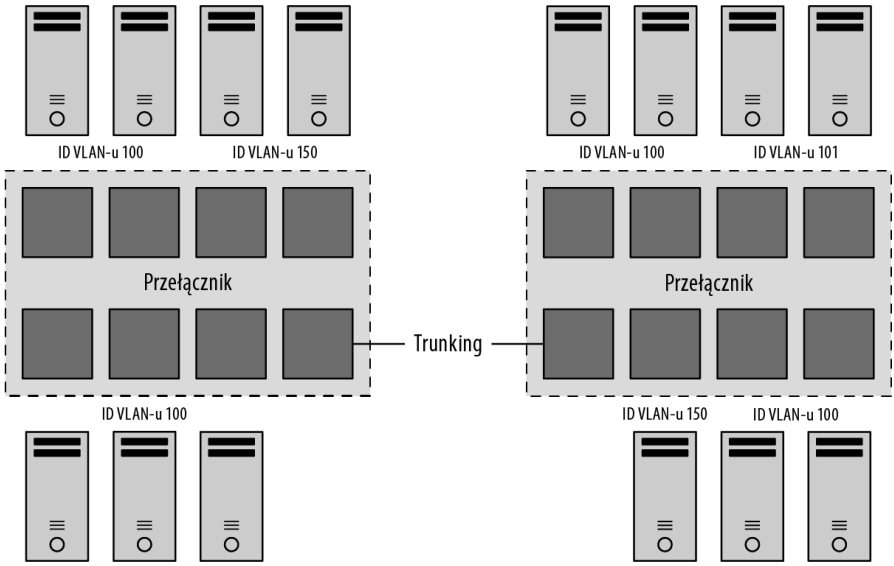
   ```
   New-VirtualPortGroup -VirtualSwitch vSwitch1 -Name ProductionLAN
   ```

Wśród różnych typów połączeń, takich jak porty VMkernel i grupy portów maszyn wirtualnych, administratorzy vSphere z reguły większość czasu poświęcają na tworzenie, modyfikowanie i usuwanie grup portów maszyn wirtualnych oraz zarządzanie nimi.

Konfigurowanie VLAN-ów

Wirtualna sieć LAN (ang. *Virtual LAN* — VLAN) to logiczna sieć lokalna, która zapewnia wydajną segmentację, bezpieczeństwo i kontrolę transmisji broadcastowych (rozgłoszeniowych), pozwalając jednocześnie, aby ruch współdzielił te same fizyczne segmenty sieci LAN lub te same przełączniki fizyczne. Rysunek 5.23 pokazuje typową konfigurację VLAN-ów między przełącznikami fizycznymi.

Sieci VLAN korzystają ze standardu IEEE 802.1q do **znakowania** ruchu należącego do określonych VLAN-ów. Znacznik VLAN, nazywany również identyfikatorem VLAN-u, jest wartością liczbową z przedziału od 1 do 4094 i w sposób jednoznaczny identyfikuje daną sieć VLAN w sieci. Przełączniki fizyczne, takie jak te przedstawione na rysunku 5.23, muszą być skonfigurowane z portami służącymi do trunkingu sieci VLAN między przełącznikami. Porty te zwane są portami **trunkowymi**. Porty, które nie zostały skonfigurowane do trunkingu sieci VLAN, nazywamy portami *dostępu* i mogą one przenosić ruch tylko dla jednego VLAN-u jednocześnie.



RYSUNEK 5.23. Wirtualne sieci LAN zapewniają bezpieczną segmentację ruchu bez ponoszenia kosztów dodatkowego sprzętu

KORZYSTANIE Z IDENTYFIKATORA VLAN-U 4095

Zwykle identyfikator VLAN-u będzie miał wartość z przedziału od 1 do 4094. Jednak w środowisku vSphere prawidłowy jest identyfikator VLAN-u 4095. Użycie tego identyfikatora z ESXi powoduje, że informacje o znakowaniu VLAN-ów są przekazywane poprzez przełącznik wirtualny aż do systemu operacyjnego gościa. Nazywa się to **znakowaniem wirtualnych gości** (ang. *virtual guest tagging* — VGT) i jest użyteczne tylko dla systemów operacyjnych gości, które obsługują i rozumieją znaczniki VLAN-ów.

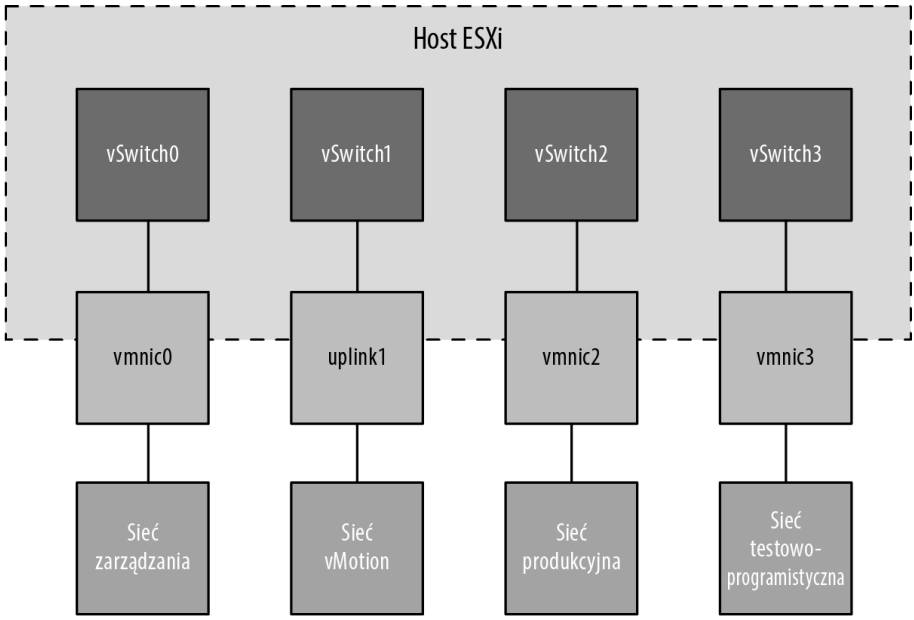
VLAN-y są ważną częścią sieci ESXi ze względu na wpływ, jaki mają na liczbę wymaganych przełączników wirtualnych i uplinków. Rozważmy następującą konfigurację:

- Sieć zarządzania potrzebuje dostępu do segmentu sieci przenoszącego ruch zarządzania.
- Pozostałe porty VMkernel, w zależności od ich przeznaczenia, mogą wymagać dostępu do wyizolowanego segmentu vMotion lub segmentu sieci przenoszącego ruch iSCSI i NFS.
- Grupy portów maszyn wirtualnych potrzebują dostępu do odpowiednich segmentów sieci dla maszyn wirtualnych działających na hostach ESXi.

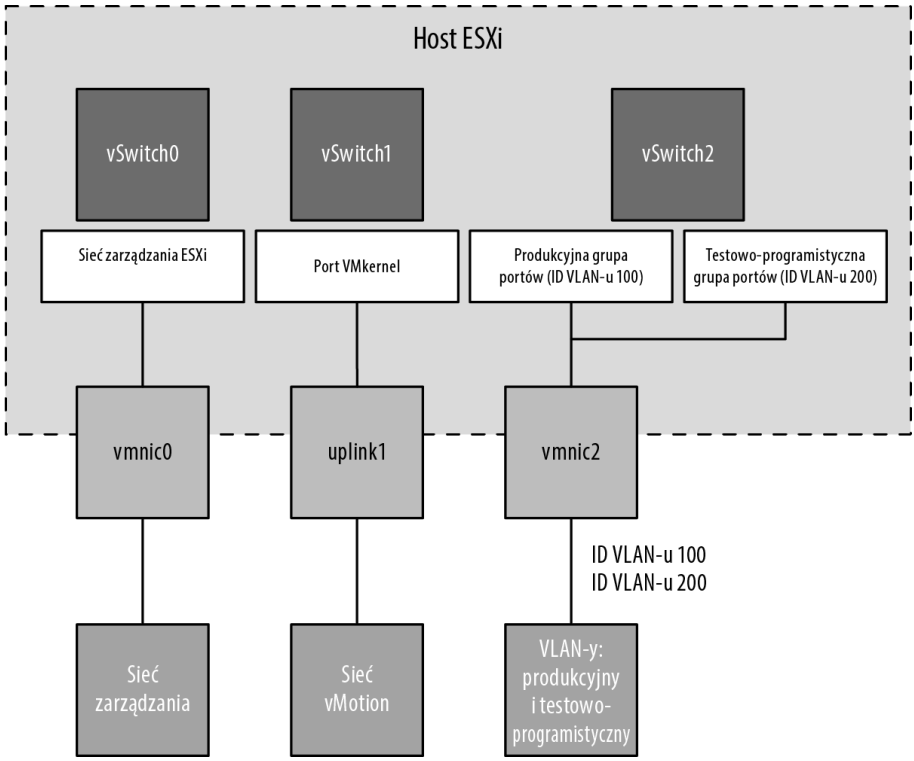
Bez VLAN-ów ta konfiguracja wymagałaby co najmniej trzech osobnych przełączników wirtualnych, z których każdy byłby powiązany z inną fizyczną kartą sieciową, a każda fizyczna karta sieciowa musiałaby być fizycznie podłączona do właściwego segmentu sieci, jak pokazano na rysunku 5.24.

Jeśli dodamy jeszcze sieć pamięci masowej IP i kilka innych sieci maszyn wirtualnych, które muszą być obsługiwane, liczba wymaganych przełączników wirtualnych szybko się zwiększy. A nie uwzględniliśmy jeszcze nawet redundancji uplinków.

Rozwiązaniem tego problemu są VLAN-y. Rysunek 5.25 pokazuje sieć z rysunku 5.24, ale tym razem z VLAN-ami.



RYSUNEK 5.24. Obsługa wielu sieci bez VLAN-ów może zwiększyć liczbę wymaganych przełączników wirtualnych i uplinków oraz ilość okablowania



RYSUNEK 5.25. VLAN-y mogą zmniejszyć liczbę wymaganych przełączników wirtualnych i uplinków oraz ilość okablowania

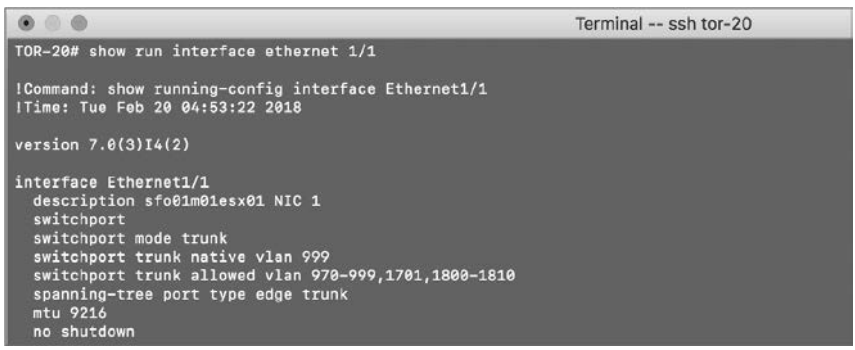
Chociaż na rysunku 5.25 redukcja w stosunku do rysunku 5.24 to tylko jeden przełącznik wirtualny i jeden uplink, do tej konfiguracji łatwo możesz dodać więcej sieci maszyn wirtualnych, dołączając po prostu kolejną grupę portów z innym identyfikatorem VLAN-u. Serwery kasetowe to doskonały przykład tego, że VLAN-y oferują ogromne korzyści. Ze względu na niewielki rozmiar obudowy serwery kasetowe zawsze oferowały ograniczoną liczbę gniazd rozszerzeń dla fizycznych kart sieciowych. VLAN-y pozwalają tym serwerom kasetowym obsługiwać więcej sieci, niż mogłyby obsłużyć standardowo.

VLAN-Y NIE SĄ NIEZBĘDNE

Wirtualne przełączniki w systemie VMkernel nie potrzebują VLAN-ów, jeśli host ESXi ma wystarczającą liczbę fizycznych kart sieciowych, aby podłączyć się do wszystkich segmentów sieci. VLAN-y zapewniają jednak dodatkową elastyczność w dostosowywaniu się do przyszłych zmian w sieci, więc zaleca się korzystanie z nich wszędzie tam, gdzie jest to możliwe.

Jak pokazano na rysunku 5.25, VLAN-y są obsługiwane poprzez konfigurowanie różnych grup portów na przełączniku wirtualnym. Relacja między VLAN-ami i grupami portów nie jest relacją „jeden do jednego". Dana grupa portów może być powiązana tylko z jednym VLAN-em, ale pojedynczy VLAN może mieć przypisanych wiele grup portów. W podrozdziale „Konfigurowanie zabezpieczeń przełącznika wirtualnego" w dalszej części tego rozdziału zobaczysz kilka przykładów sytuacji, w których z pojedynczym VLAN-em może być powiązanych wiele grup portów.

Aby VLAN-y działały poprawnie z grupą portów, uplinki dla danego przełącznika wirtualnego muszą być podłączone do portu przełącznika fizycznego skonfigurowanego jako port trunkowy. Port trunkowy jest w stanie przekazywać ruch z wielu VLAN-ów naraz, zachowując przy tym jego identyfikatory VLAN-ów. Rysunek 5.26 pokazuje fragment konfiguracji przełącznika z serii Cisco Nexus 9000 dla portu skonfigurowanego jako port trunkowy.



RYSUNEK 5.26. Aby przekazywać do hostów ESXi informacje o VLAN-ach, które będą wykorzystywane przez grupy portów, porty przełącznika fizycznego muszą być skonfigurowane jako porty trunkowe

Konfiguracja przełączników innych producentów będzie się różnić, więc koniecznie zapoznaj się z podręcznikiem użytkownika dla konkretnego przełącznika, aby uzyskać szczegółowe informacje na temat konfiguracji portów trunkowych.

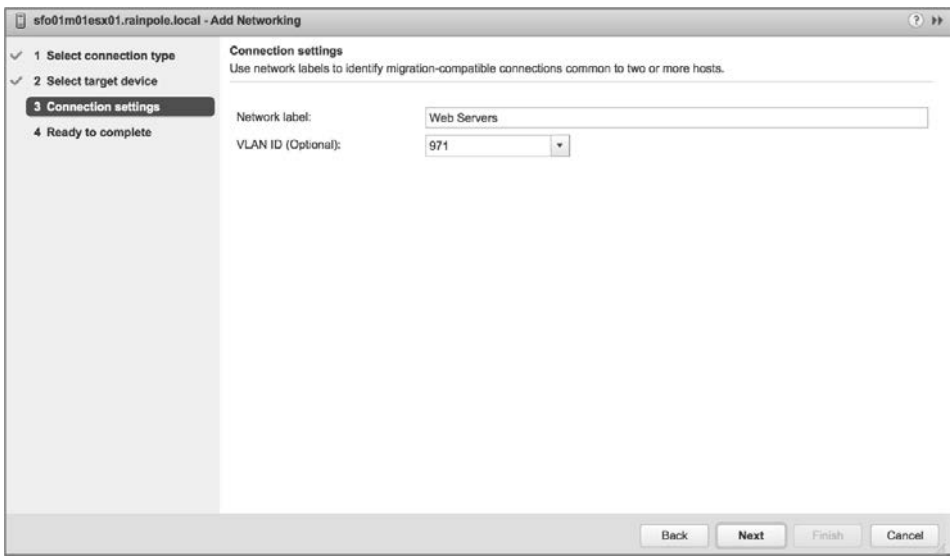
Gdy porty przełącznika fizycznego są poprawnie skonfigurowane jako porty trunkowe, przełącznik ten przekazuje znaczniki VLAN-ów do serwera ESXi, gdzie przełącznik wirtualny kieruje ruch do grup portów z przypisanymi odpowiednimi identyfikatorami VLAN-ów. Jeśli z danym identyfikatorem VLAN-u nie została skonfigurowania żadna grupa portów, ruch jest odrzucany.

VLAN NATYWNY

Na rysunku 5.26 można zauważyć polecenie `switchport trunk native vlan 999`. Na większości przełączników domyślnym VLAN-em natywnym (zwanym również VLAN-em nieoznakowanym) jest VLAN 1. Jeśli musisz przekazywać ruch do hostów ESXi na VLAN-ie 1, powinieneś wyznaczyć inny VLAN jako natywny za pomocą tego polecenia (lub jego odpowiednika). Zalecamy utworzenie atrapy VLAN-u, takiej jak 999, i ustawienie jej jako VLAN-u natywnego. Gwarantuje to, że podczas przekazywania do hostów ESXi wszystkie VLAN-y będą oznakowane odpowiednim identyfikatorem. Należy pamiętać, że może to wpływać na zachowania takie jak bootowanie PXE, które zasadniczo wymaga ruchu nieoznakowanego.

Aby skonfigurować grupę portów maszyn wirtualnych przy użyciu identyfikatora VLAN-u 971, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do hosta ESXi, do którego chcesz dodać grupę portów maszyn wirtualnych, kliknij zakładkę *Configure*, a następnie w sekcji *Networking* wybierz *Virtual Switches* (przełączniki wirtualne).
3. Wybierz przełącznik wirtualny, na którym ma zostać utworzona nowa grupa portów.
4. Kliknij ikonę *Add Host Networking* (wygląda jak globus ze znakiem plus w rogu), aby uruchomić kreatora dodawania sieci.
5. Zaznacz przycisk opcji *Virtual Machine Port Group For A Standard Switch* i kliknij *Next*.
6. Upewnij się, że zaznaczony jest przycisk opcji *Select An Existing Standard Switch* i w razie potrzeby użyj przycisku *Browse*, aby wybrać, który przełącznik wirtualny będzie hostował nową grupę portów maszyn wirtualnych. Kliknij *Next*.
7. W polu tekstowym *Network Label* wpisz nazwę grupy portów maszyny wirtualnej.
8. W polu tekstowym VLAN ID (Optional) wpisz **971**, jak pokazano na rysunku 5.27.



RYSUNEK 5.27. Musisz podać poprawny identyfikator VLAN-u, aby grupa portów otrzymywała ruch przeznaczony dla określonego VLAN-u

Powinieneś użyć tutaj wartości, która jest poprawna dla Twojej sieci.

9. Kliknij *Next*, aby przejrzeć konfigurację przełącznika wirtualnego, a następnie kliknij *Finish*.

Jak już się zapewne zorientowałeś, do tworzenia lub modyfikowania ustawień VLAN-ów dla portów lub grup portów możesz również użyć PowerCLI. Nie będziemy tutaj omawiać szczegółowo tych czynności, ponieważ polecenia są bardzo podobne do tego, co już pokazaliśmy.

Chociaż VLAN-y zmniejszają koszty budowy wielu logicznych podsieci, należy pamiętać, że nie usuwają ograniczeń ruchu. Chociaż VLAN-y oddzielają logicznie segmenty sieci, pod spodem cały ruch nadal przechodzi przez tę samą sieć fizyczną. Aby uwzględnić operacje sieciowe wymagające transmitowania dużej ilości danych, upewnij się, że fizyczne karty sieciowe i przełączniki są w stanie zapewnić żądaną przepustowość.

KONTROLOWANIE VLAN-ÓW PRZEKAZYWANYCH PRZEZ KANAŁ TRUNKOWY

W niektórych konfiguracjach przełączników Cisco możesz zobaczyć również polecenie `switchport trunk allowed vlan`. Pozwala ono kontrolować, które VLAN-y są przekazywane przez kanał trunkowy do urządzenia znajdującego się na drugim końcu łącza — w tym przypadku hosta ESXi. Musisz upewnić się, że wszystkie VLAN-y zdefiniowane na przełącznikach wirtualnych zostały również uwzględnione w poleceniu `switchport trunk allowed vlan`; VLAN-y nieuwzględnione w tym poleceniu nie będą działać.

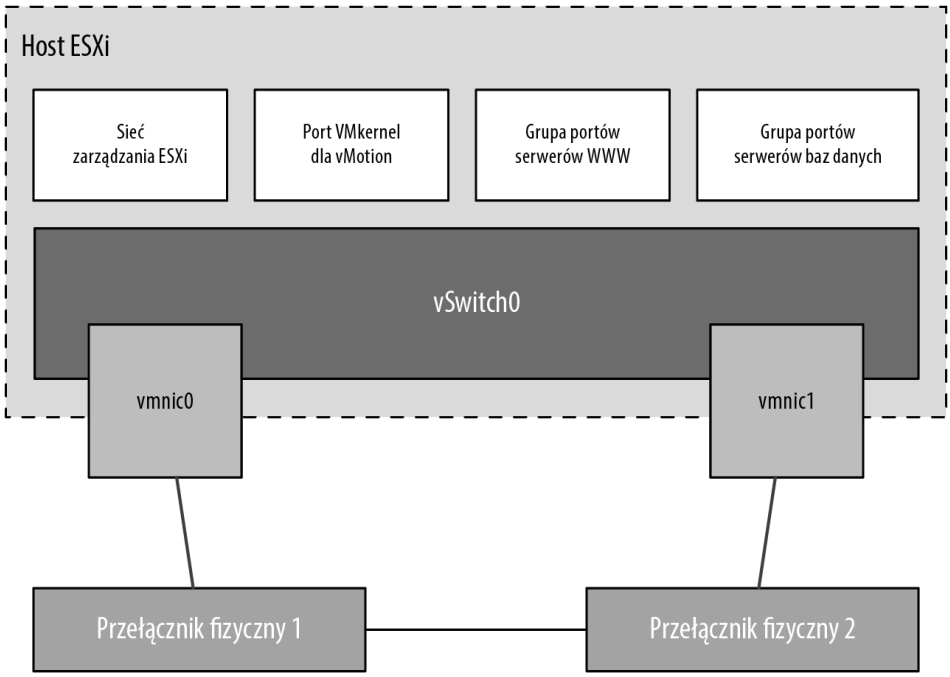
Konfigurowanie grup kart sieciowych

Aby przełącznik wirtualny i powiązane z nim porty lub grupy portów mogły komunikować się z innymi hostami ESXi lub systemami fizycznymi, przełącznik wirtualny musi mieć co najmniej jeden uplink. **Uplink** to fizyczna karta sieciowa powiązana z przełącznikiem wirtualnym i podłączona do fizycznego przełącznika sieciowego. Gdy jest ona podłączona do fizycznej sieci, zapewnia łączność z systemem VMkernel i maszynami wirtualnymi podłączonymi do danego przełącznika wirtualnego. Co się jednak stanie, gdy awarii ulegnie fizyczna karta sieciowa, kabel łączący ten uplink z fizyczną siecią lub upstreamowy fizyczny przełącznik, do którego podłączony jest ten uplink? Przy pojedynczym uplinku utracone zostanie połączenie sieciowe z całym przełącznikiem wirtualnym i wszystkimi jego portami lub grupami portów. Właśnie tutaj do gry wchodzą grupy kart sieciowych.

Grupowanie kart sieciowych (ang. *NIC teaming*) polega na podłączeniu wielu fizycznych kart sieciowych do pojedynczego przełącznika wirtualnego. Grupy kart sieciowych zapewniają redundancję i równoważenie obciążenia dla komunikacji sieciowej z systemem VMkernel i maszynami wirtualnymi.

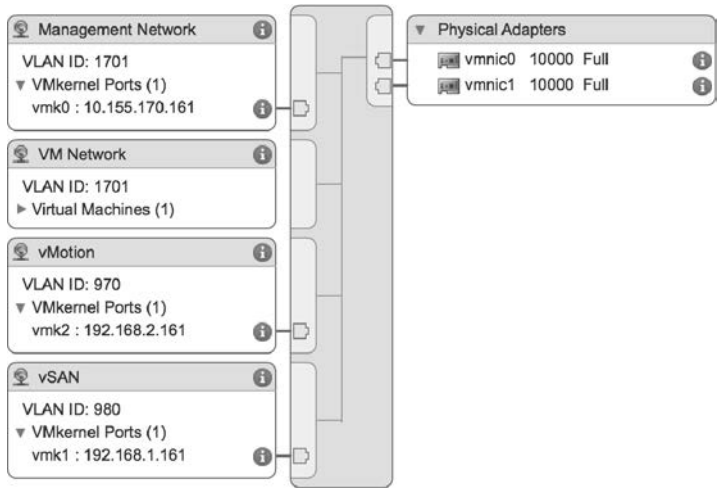
Koncepcję grupowania kart sieciowych ilustruje rysunek 5.28. Przełącznik wirtualny ma dwa uplinki, a każdy uplink jest podłączony do innego przełącznika fizycznego. Zwróć uwagę, że grupy kart sieciowych obsługują różne typy połączeń, więc można ich używać z siecią zarządzania ESXi, siecią VMkernel oraz siecią maszyn wirtualnych.

Rysunek 5.29 pokazuje, jak wygląda grupa kart sieciowych z poziomu klienta internetowego vSphere. W tym przykładzie przełącznik wirtualny został powiązany z kilkoma fizycznymi kartami sieciowymi (uplinkami). Jak wspomnieliśmy wcześniej, host ESXi może mieć maksymalnie 32 uplinki. Mogą one być rozproszone na wiele przełączników wirtualnych lub połączone w grupę na jednym przełączniku wirtualnym. Pamiętaj, że każdą fizyczną kartę sieciową możesz podłączyć za każdym razem tylko do jednego przełącznika wirtualnego.



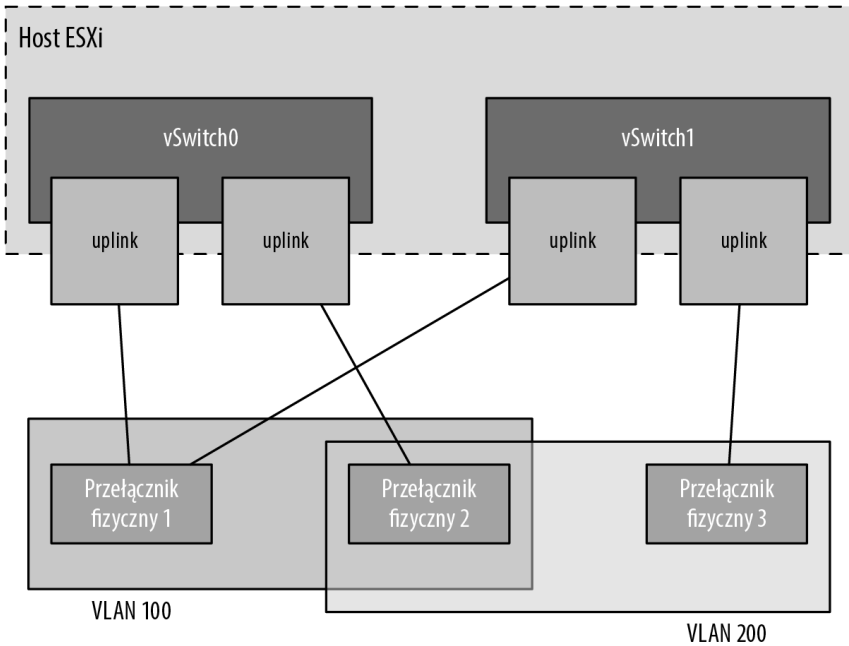
RYSUNEK 5.28. Przełączniki wirtualne z wieloma uplinkami oferują redundancję i równoważenie obciążenia

RYSUNEK 5.29. Klient internetowy vSphere pokazuje, kiedy z przełącznikiem wirtualnym powiązanych jest wiele fizycznych kart sieciowych tworzących grupę



Zbudowanie funkcjonalnej grupy kart sieciowych wymaga, aby wszystkie uplinki były podłączone do fizycznych przełączników znajdujących się w tej samej domenie rozgłoszeniowej. Jeśli używane są VLAN-y, na wszystkich przełącznikach należy skonfigurować trunking VLAN-ów, a kanał trunkowy musi dopuszczać przekazywanie odpowiedniego podzbioru VLAN-ów. W przełącznikach Cisco zwykle jest to kontrolowane za pomocą instrukcji `switchport trunk allowed vlan`.

Na rysunku 5.30 grupa kart sieciowych dla przełącznika wirtualnego *vSwitch0* będzie działać, ponieważ oba fizyczne przełączniki współdzielą VLAN 100. Nie będzie jednak działać grupa kart sieciowych dla przełącznika wirtualnego *vSwitch1*, ponieważ fizyczne przełączniki, do których podłączone są karty sieciowe, nie przenoszą tych samych VLAN-ów: jeden przenosi VLAN 100, a drugi VLAN 200.



RYSUNEK 5.30. Wszystkie fizyczne karty sieciowe w grupie muszą przenosić te same VLAN-y

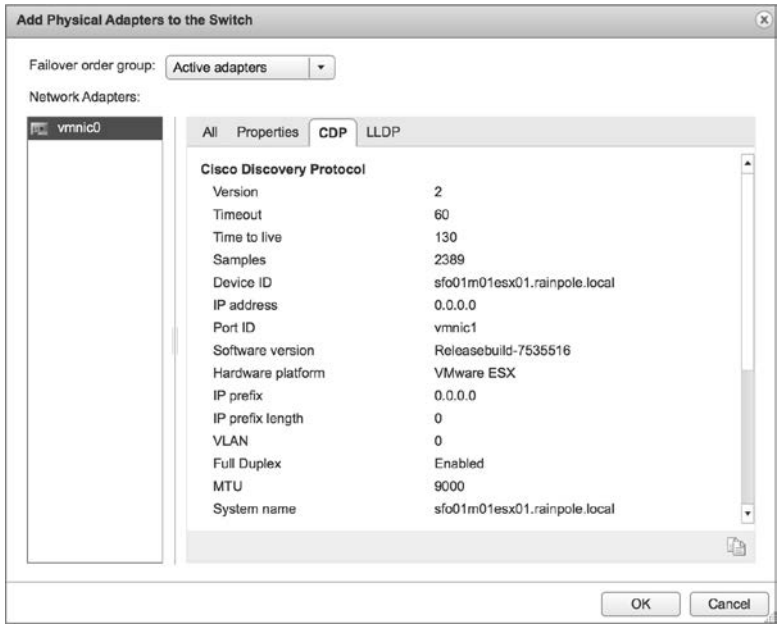
KONSTRUOWANIE GRUP KART SIECIOWYCH

Grupy kart sieciowych należy budować na fizycznych kartach sieciowych zlokalizowanych na osobnych magistralach. Jeśli host ESXi zawiera na przykład dwie zintegrowane karty sieciowe i czteroportową kartę sieciową PCI Express, grupa kart sieciowych powinna zostać skonstruowana przy użyciu jednej wbudowanej karty sieciowej i jednej karty sieciowej działającej na magistrali PCI. Taki projekt eliminuje pojedynczy punkt awarii.

Aby utworzyć grupę kart sieciowych dla istniejącego przełącznika wirtualnego za pomocą klienta internetowego vSphere, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter przy użyciu klienta internetowego vSphere.
2. Przejdź do sekcji *Networking* w zakładce *Configure* dla hosta ESXi, na którym chcesz utworzyć grupę kart sieciowych.
3. Wybierz *Virtual Switches*, a następnie wybierz przełącznik wirtualny, do którego ma zostać przypisana dana grupa kart sieciowych, i kliknij ikonę *Manage The Physical Adapters Connected To The Selected Virtual Switch* (zarządzanie fizycznymi kartami podłączonymi do wybranego przełącznika wirtualnego) wyglądającą jak karta sieciowa z kluczem.
4. W oknie dialogowym *Manage Physical Network Adapters* (zarządzanie fizycznymi kartami sieciowymi) kliknij zieloną ikonę *Add Adapters* (dodawanie kart sieciowych).
5. W oknie dialogowym *Add Physical Adapters To The Switch* (dodawanie fizycznych kart sieciowych do przełącznika) wybierz z listy odpowiednią kartę (lub karty), jak pokazano na rysunku 5.31.

RYSUNEK 5.31. Tworzenie grupy kart sieciowych poprzez dodawanie kart sieciowych, które należą do tej samej domeny rozgłoszeniowej warstwy drugiej, co pierwotna karta sieciowa



UMIESZCZANIE NOWYCH KART SIECIOWYCH W INNEJ GRUPIE PRZEŁĄCZANIA AWARYJNEGO

Okno dialogowe *Add Physical Adapters To The Switch* pokazane na rysunku 5.31 umożliwia dodawanie kart sieciowych do listy aktywnych kart oraz do listy kart rezerwowych lub nieużywanych. Wystarczy zmienić żądaną grupę przy użyciu rozwijanej listy *Failover order group*.

6. Kliknij *OK*, aby powrócić do okna dialogowego *Manage Physical Network Adapters*.
7. Kliknij *OK*, aby zakończyć proces i powrócić do sekcji *Virtual Switch* wybranego hosta ESXi. Zwróć uwagę, że aktualizacja wyświetlanych informacji w celu uwzględnienia nowej fizycznej karty sieciowej może chwilę potrwać.

Po skonfigurowaniu kart sieciowych dla przełącznika wirtualnego ESXi może dla niego włączyć równoważenie obciążenia. Równoważenie obciążenia w grupie kart sieciowych nie działa tak samo jak równoważenie obciążenia zaawansowanych protokołów routingu. Nie wynika ono z identyfikowania ilości ruchu przesyłanego przez kartę sieciową i przenoszenia ruchu w celu wyrównania przepływu danych przez wszystkie dostępne karty. Algorytm równoważenia obciążenia dla grup kart sieciowych na przełączniku wirtualnym polega na wyrównywaniu liczby połączeń, a nie natężenia ruchu. Grupy kart sieciowych na przełączniku wirtualnym można skonfigurować z jedną z następujących czterech reguł równoważenia obciążenia:

- równoważenie obciążenia oparte na wirtualnych portach pochodzenia (domyślne),
- równoważenie obciążenia oparte na źródłowych adresach MAC,
- równoważenie obciążenia oparte na skrótach IP,
- bezpośrednia kolejność przełączania awaryjnego.

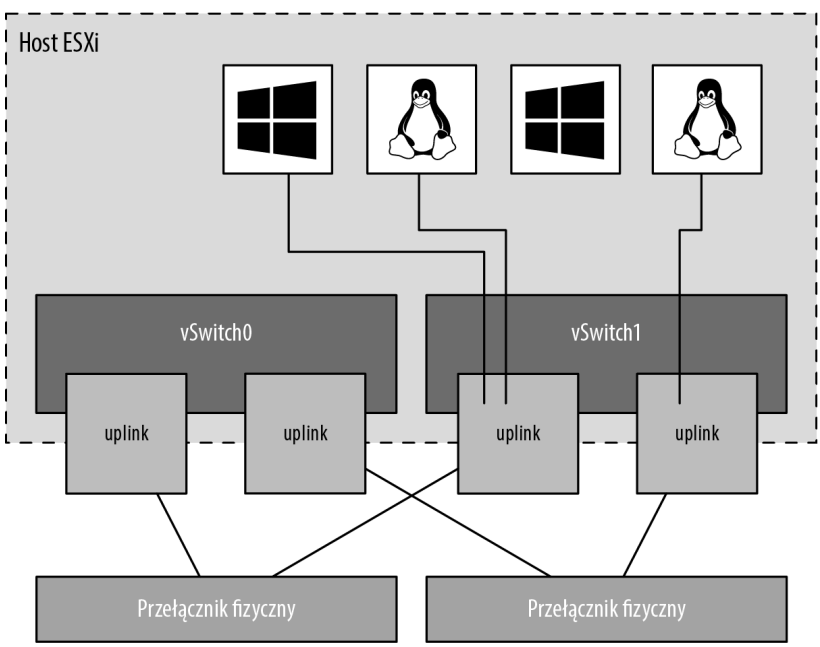
Ostatnia opcja, bezpośrednia kolejność przełączania awaryjnego, nie jest tak naprawdę regułą „równoważenia obciążenia". Stosuje ona przydzieloną przez administratora kolejność przełączania awaryjnego, przy czym wykorzystywany jest pierwszy w kolejności uplink z listy aktywnych kart sieciowych, które spełniają kryteria wykrywania przełączania awaryjnego. Więcej informacji na temat kolejności przełączania awaryjnego znajdziesz w podpunkcie „Konfigurowanie wykrywania i reguł przełączania awaryjnego" w dalszej części tego rozdziału. Zwróć również uwagę, że podana przeze mnie lista dotyczy tylko standardowych przełączników vSphere. Rozproszone przełączniki vSphere, które zostaną omówione nieco dalej w podrozdziale „Praca z rozproszonymi przełącznikami vSphere", mają dodatkowe opcje równoważenia obciążenia i przełączania awaryjnego.

UWAGA

Funkcjonalność równoważenia obciążenia grup kart sieciowych na przełączniku wirtualnym dotyczy tylko ruchu wychodzącego.

Równoważenie obciążenia oparte na wirtualnych portach pochodzenia

Domyślna reguła równoważenia obciążenia jest oparta na źródłowych portach wirtualnych i korzysta z algorytmu, który przypisuje każdy port przełącznika wirtualnego do określonego uplinku powiązanego z tym przełącznikiem. Algorytm ten próbuje utrzymać na wszystkich uplinkach taką samą liczbę przypisań portu do uplinku, aby osiągnąć równoważenie obciążenia. Jak pokazano na rysunku 5.32, ta reguła gwarantuje, że ruch z określonej wirtualnej karty sieciowej podłączonej do portu przełącznika wirtualnego będzie konsekwentnie używać tej samej fizycznej karty sieciowej. W przypadku awarii jednego z uplinków jego ruch jest przełączany awaryjnie na inną fizyczną kartę sieciową.



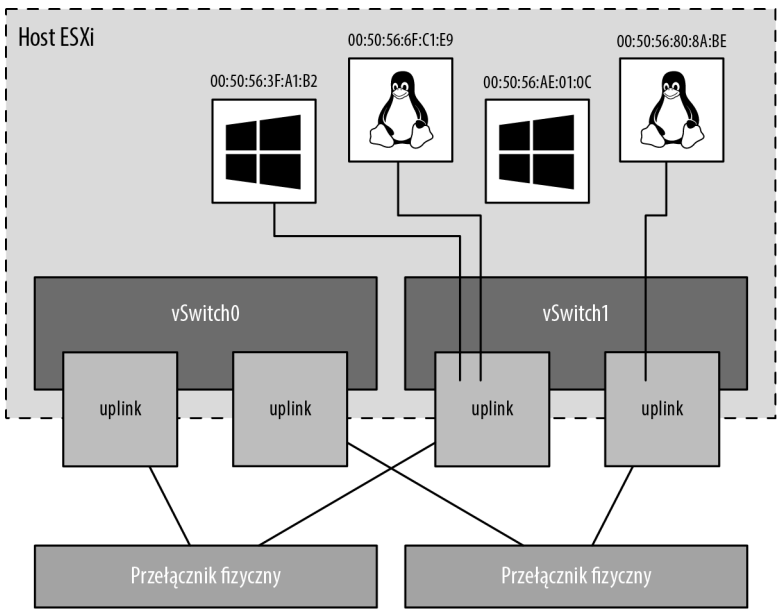
RYSUNEK 5.32. Reguła równoważenia obciążenia oparta na wirtualnych portach pochodzenia przypisuje każdy port przełącznika wirtualnego do określonego uplinku. Przełączenie awaryjne na inny uplink ma miejsce wtedy, gdy jedna z fizycznych kart sieciowych doznaje awarii

Chociaż ta reguła nie zapewnia dynamicznego równoważenia obciążenia, gwarantuje redundancję. Ponieważ port dla maszyny wirtualnej nie zmienia się, to niezależnie od natężenia ruchu sieciowego każda maszyna wirtualna jest powiązana z fizyczną kartą sieciową do momentu przełączenia awaryjnego lub przeprowadzenia migracji vMotion. Patrząc na rysunek 5.32, wyobraź sobie, że maszyna wirtualna z systemem Linux i maszyna wirtualna z systemem Windows znajdujące się po lewej stronie to dwie najbardziej obciążające sieć maszyny wirtualne. W tym przypadku reguła oparta na portach wirtualnych przypisała oba porty dla tych maszyn wirtualnych do tej samej fizycznej karty sieciowej. W takiej sytuacji jedna fizyczna karta sieciowa może być znacznie bardziej obciążona niż pozostałe karty sieciowe w grupie.

Przełącznik fizyczny przekazujący ruch uczy się powiązania portów i dlatego wysyła odpowiedzi przez tę samą fizyczną kartę sieciową, z której zainicjowano żądanie. Regułę opartą na portach wirtualnych najlepiej stosować wtedy, gdy więcej jest wirtualnych kart sieciowych niż fizycznych kart sieciowych, czyli w przypadku ruchu maszyn wirtualnych prawie zawsze. Kiedy jest mniej wirtualnych kart sieciowych, niektóre karty fizyczne nie będą używane. Jeśli do przełącznika wirtualnego z sześcioma uplinkami podłączonych jest na przykład pięć maszyn wirtualnych, tylko pięć portów tego przełącznika zostanie przypisanych do dokładnie pięciu uplinków, a jeden uplink pozostanie niewykorzystany.

Równoważenie obciążenia oparte na źródłowych adresach MAC

Drugą regułą równoważenia obciążenia dostępną dla grup kart sieciowych jest reguła oparta na źródłowych adresach MAC, zilustrowana na rysunku 5.33. Ma ona te same wady, co reguła oparta na wirtualnych portach pochodzenia, a wynika to z prostego faktu, że źródłowe adresy MAC mają tak samo statyczny charakter jak przypisania portów wirtualnych. Reguły opartej na źródłowych adresach MAC również najlepiej używać wtedy, gdy więcej jest wirtualnych kart sieciowych niż fizycznych kart sieciowych. Ponadto maszyny wirtualne i tak nie będą mogły używać wielu kart fizycznych, jeśli nie zostaną skonfigurowane z wieloma kartami wirtualnymi. Wiele wirtualnych kart sieciowych w systemie operacyjnym gościa maszyny wirtualnej zapewni wiele źródłowych adresów MAC i umożliwi korzystanie z wielu fizycznych kart sieciowych.



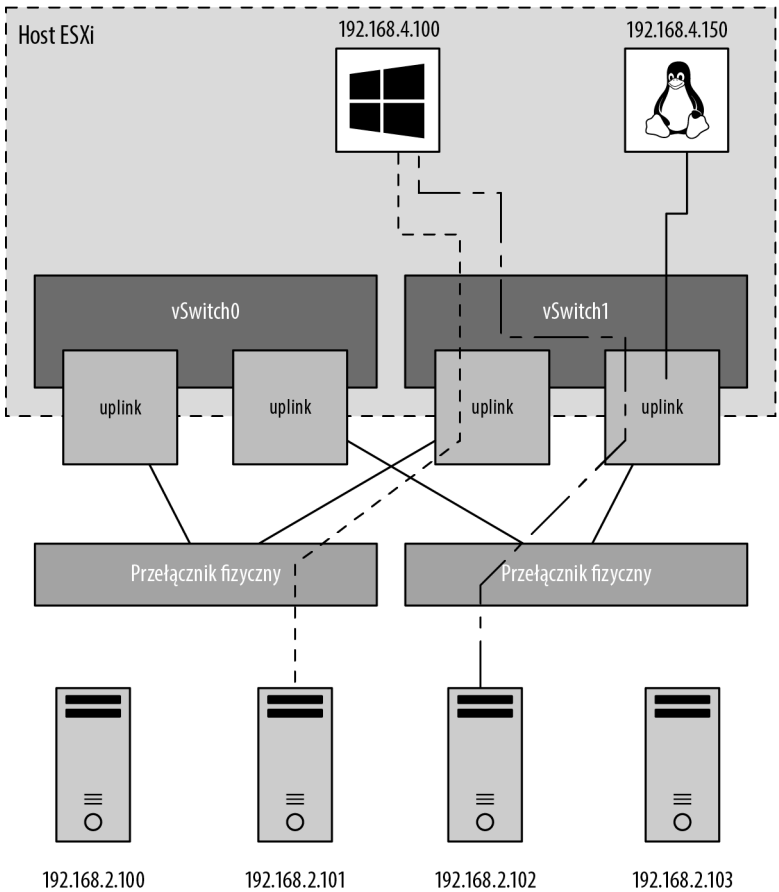
RYSUNEK 5.33. Jak sama nazwa wskazuje, reguła równoważenia obciążenia oparta na źródłowych adresach MAC wiąże wirtualną kartę sieciową z fizyczną kartą sieciową na podstawie adresu MAC

POŁĄCZENIE PRZEŁĄCZNIKA WIRTUALNEGO Z FIZYCZNYM

Aby wyeliminować pojedynczy punkt awarii, fizyczne karty sieciowe w grupach skonfigurowanych do korzystania z reguł równoważenia obciążenia opartych na portach wirtualnych lub źródłowych adresach MAC możesz podłączyć do różnych przełączników fizycznych. Z żadną z tych reguł równoważenia obciążenia nie jest obsługiwana agregacja łączy zgodna ze standardem 802.3ad.

Równoważenie obciążenia oparte na skrótach IP

Trzecią metodą równoważenia obciążenia dostępną dla grup kart sieciowych jest reguła oparta na skrótach IP, zwana także regułą **out-IP**, która została zilustrowana na rysunku 5.34. Adresuje ona statyczne ograniczenia pozostałych dwóch reguł. Reguła oparta na skrótach IP wykorzystuje źródłowe i docelowe adresy IP do obliczania skrótów określających fizyczną kartę sieciową używaną do komunikacji. Różne kombinacje źródłowego i docelowego adresu IP będą w naturalny sposób generować różne skróty. Na podstawie takiego skrótu algorytm może następnie umożliwić pojedynczej maszynie wirtualnej komunikację z różnymi miejscami docelowymi za pośrednictwem różnych fizycznych kart sieciowych, przy założeniu, że obliczone wartości skrótów nie wyznaczają tej samej fizycznej karty sieciowej.



RYSUNEK 5.34. Reguła oparta na skrótach IP jest bardziej skalowalną metodą równoważenia obciążenia, która pozwala maszynom wirtualnym używać więcej niż jednej fizycznej karty sieciowej podczas komunikacji z wieloma hostami docelowymi

Przełącznik wirtualny z grupą kart sieciowych, która ma skonfigurowaną regułę równoważenia obciążenia opartą na skrótach IP, musi mieć wszystkie fizyczne karty sieciowe podłączone do tego samego przełącznika fizycznego lub stosu przełączników fizycznych. Ponadto ten przełącznik musi być skonfigurowany do agregacji łączy. ESXi skonfigurowany do korzystania ze standardowego przełącznika vSphere obsługuje agregację łączy 802.3ad w trybie statycznym (manualnym), nazywaną niekiedy kanałem EtherChannel, ale nie obsługuje protokołów agregacji łączy w trybie dynamicznym, takich jak LACP. Agregacja łączy może potencjalnie zwiększyć ogólną, zagregowaną przepustowość, łącząc przepustowości wielu fizycznych kart sieciowych do wykorzystania przez pojedynczą wirtualną kartę sieciową maszyny wirtualnej.

Podczas korzystania z opartej na haszowaniu IP zasady równoważenia obciążenia należy również wziąć pod uwagę, że wszystkie fizyczne karty sieciowe muszą być aktywne. Wynika to ze sposobu, w jaki równoważenie obciążenia oparte na haszowaniu IP działa między przełącznikiem wirtualnym i przełącznikiem fizycznym.

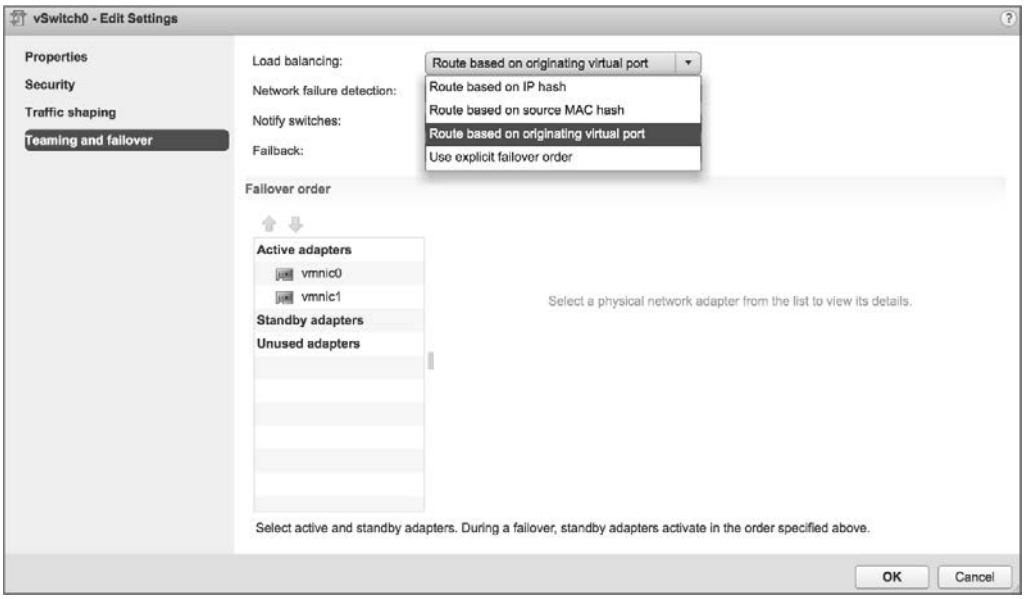
RÓWNOWAŻENIE OBCIĄŻENIA DLA DUŻYCH TRANSFERÓW DANYCH

Chociaż reguła równoważenia obciążenia oparta na skrótach IP może bardziej równomiernie rozkładać ruch dla pojedynczej maszyny wirtualnej, nie zapewnia żadnych korzyści w przypadku dużych transferów danych, które mają miejsce między tym samym systemem będącym i źródłowym, i docelowym. Ponieważ skrót źródłowo-docelowy będzie taki sam przez cały czas trwania sesji, dane tej sesji będą przepływać jedynie przez jedną fizyczną kartę sieciową, zamiast przechodzić karuzelowo przez wszystkie dostępne karty obsługujące daną grupę portów.

Aby zmienić regułę równoważenia obciążenia dla grupy kart sieciowych przełącznika wirtualnego, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do konkretnego hosta ESXi posiadającego przełącznik wirtualny, którego konfigurację grupy kart sieciowych chcesz zmodyfikować.
3. Po wybraniu hosta ESXi przejdź do zakładki *Configure* i wybierz *Virtual Switches*.
4. Z listy przełączników wirtualnych wybierz nazwę żądanego przełącznika, a następnie kliknij ikonę *Edit* (edytowanie), która wygląda jak ołówek.
5. W oknie dialogowym *Edit Settings* (edytowanie ustawień) wybierz *Teaming and Failover* (grupy kart sieciowych i przełączanie awaryjne), a następnie wybierz żądane ustawienie równoważenia obciążenia z rozwijanej listy *Load Balancing*, jak pokazano na rysunku 5.35.
6. Kliknij *OK*, aby zapisać zmiany.

Wyjaśniliśmy już reguły równoważenia obciążenia, ale zanim przejdziemy do metody bezpośredniej kolejności przełączania awaryjnego, przyjrzyjmy się dokładniej przełączaniu awaryjnemu uplinków w grupie kart sieciowych oraz przywracaniu ich stanu po usunięciu awarii. Musimy rozważyć dwie kwestie: wykrywanie przełączania awaryjnego i reguły przełączania awaryjnego. Obie omówimy w następnym podpunkcie.



RYSUNEK 5.35. Wybór reguły równoważenia obciążenia dla przełącznika wirtualnego w sekcji Teaming and Failover

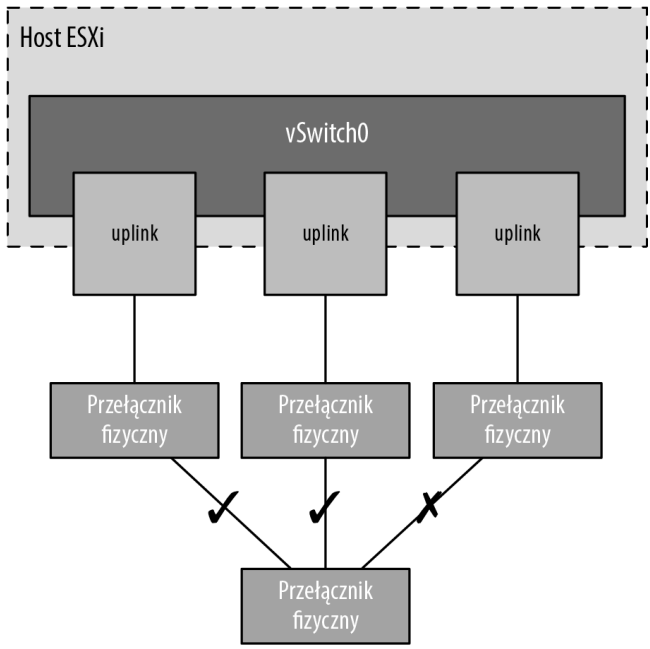
Konfigurowanie wykrywania i reguł przełączania awaryjnego

W grupie kart sieciowych można skonfigurować wykrywanie przełączania awaryjnego korzystające z metody stanu łącza lub sondowania ramek nawigacyjnych (ang. *beacon frames*).

Metoda wykrywania przełączania awaryjnego oparta na stanie łącza działa tak, jak sugeruje nazwa. Status łącza fizycznej karty sieciowej wskazuje awarię uplinku. W takim przypadku awaria jest wykrywana dla takich zdarzeń jak odłączenie kabli lub awaria zasilania przełącznika fizycznego. Minusem ustawienia wykrywania przełączania awaryjnego na podstawie stanu łącza jest jego niezdolność do zidentyfikowania błędnych konfiguracji lub wypiętych kabli łączących przełącznik z innymi urządzeniami sieciowymi (na przykład kabla łączącego dany przełącznik z przełącznikiem upstreamowym).

Z kolei metoda wykrywania przełączania awaryjnego oparta na sondowaniu sygnału nawigacyjnego, która obejmuje również status łącza, polega na rozsyłaniu rozgłoszeniowych ramek ethernetowych ze wszystkich fizycznych kart sieciowych z grupy. Te ramki rozgłoszeniowe pozwalają przełącznikowi wirtualnemu wykrywać awarie upstreamowego połączenia sieciowego i wymuszają przełączanie awaryjne, gdy porty zostaną zablokowane przez STP, porty zostaną skonfigurowane z niewłaściwym VLAN-em lub awarii ulegnie połączenie między przełącznikami. Kiedy na fizycznej karcie sieciowej przestaje być zwracany sygnał nawigacyjny, przełącznik wirtualny wysyła powiadomienie o przełączaniu awaryjnym i zgodnie z regułą przełączania awaryjnego przekierowuje ruch z uszkodzonej karty sieciowej na inną dostępną kartę sieciową.

Rozważmy przełącznik wirtualny z grupą kart sieciowych składającą się z trzech fizycznych kart, gdzie każda karta jest podłączona do innego przełącznika fizycznego, a wszystkie te przełączniki fizyczne są podłączone do przełącznika upstreamowego, jak pokazano na rysunku 5.36. Gdy dla grupy kart sieciowych ustawiona zostanie metoda wykrywania przełączania awaryjnego na podstawie sondowania ramek nawigacyjnych, ramki te będą wysyłane przez wszystkie trzy uplinki.



RYSUNEK 5.36. Reguła wykrywania przełączania awaryjnego oparta na wysyłaniu sygnału nawigacyjnego polega na wysyłaniu ramek nawigacyjnych przez wszystkie fizyczne karty sieciowe w grupie w celu identyfikowania awarii sieci upstreamowej lub błędnych konfiguracji przełącznika

INNE SPOSOBY WYKRYWANIA AWARII UPSTREAMOWYCH

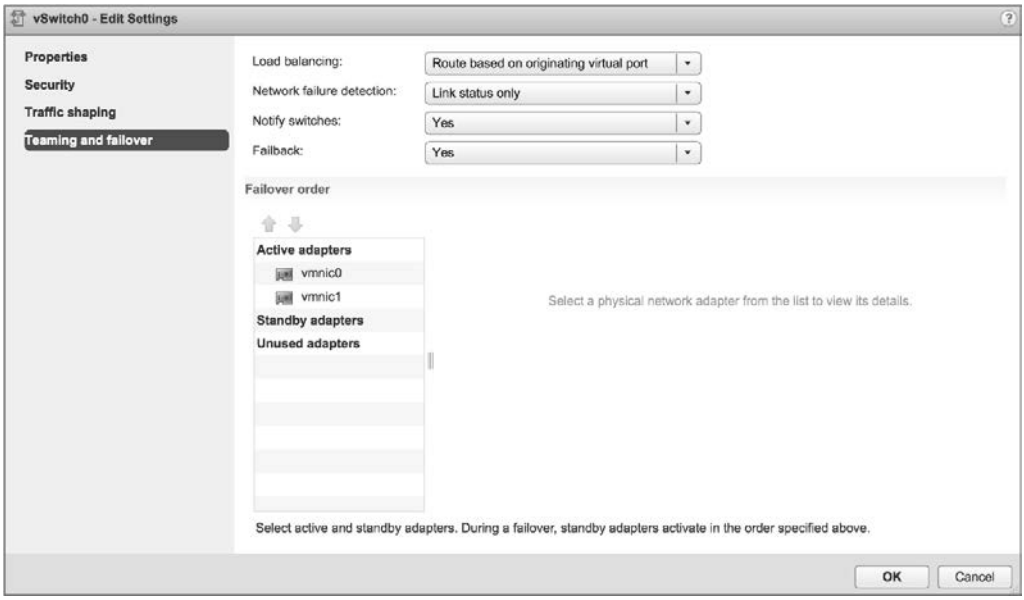
Niektórzy producenci przełączników sieciowych dodali do swoich urządzeń funkcjonalności, które pomagają wykrywać awarie sieci upstreamowej. W linii produktów Cisco dostępna jest na przykład funkcjonalność znana jako **śledzenie stanu łącza** (ang. *link state tracking*), która umożliwia przełącznikowi wykrywanie wyłączenia portu upstreamowego i odpowiednie reagowanie.

Po wykryciu awarii (na podstawie stanu łącza lub sondowania sygnału nawigacyjnego) następuje przełączenie awaryjne. Ruch z maszyn wirtualnych lub portów VMkernel jest przekierowywany do innego członka grupy kart sieciowych. Wybór członka grupy zależy jednak przede wszystkim od skonfigurowanej kolejności przełączania awaryjnego.

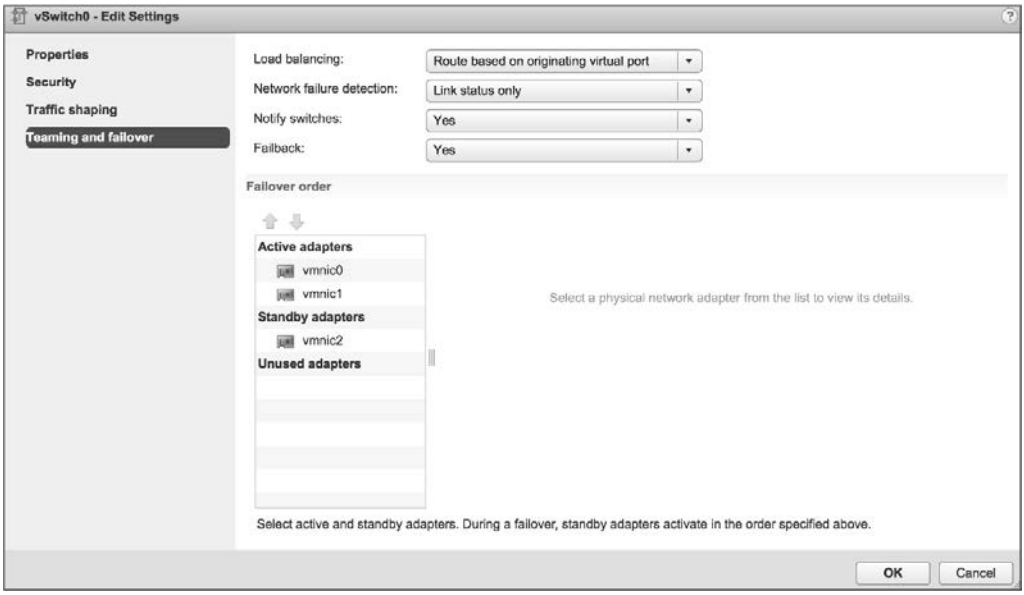
Rysunek 5.37 pokazuje konfigurację kolejności przełączania awaryjnego dla przełącznika wirtualnego z dwoma kartami sieciowymi w grupie. W tej konfiguracji obie karty sieciowe są skonfigurowane jako aktywne w dowolnym momencie do obsługi ruchu dla tego przełącznika wirtualnego i dla wszystkich powiązanych z nim portów lub grup portów używana może być jedna z tych dwóch kart lub obie.

Spójrz teraz na rysunek 5.38. Pokazano na nim przełącznik wirtualny z trzema fizycznymi kartami sieciowymi w grupie. W tej konfiguracji jedna z kart sieciowych jest skonfigurowana jako rezerwowa. Żadne karty sieciowe wymienione jako rezerwowe (*Standby adapters*) nie będą używane, dopóki nie dojdzie do awarii jednej z aktywnych kart sieciowych (*Active adapters*) — wtedy rezerwowe karty sieciowe są aktywowane w podanej kolejności.

Powinno to być oczywiste, ale dla jasności wspomnijmy jeszcze, że karty sieciowe wymienione w sekcji *Unused adapters* (nieużywane karty sieciowe) nie będą używane w przypadku awarii.



RYSUNEK 5.37. Kolejność przełączania awaryjnego pomaga określić sposób używania kart sieciowych z grupy, kiedy następuje przełączenie awaryjne



RYSUNEK 5.38. Rezerwowe karty sieciowe są aktywowane automatycznie, gdy dochodzi do awarii aktywnej karty sieciowej

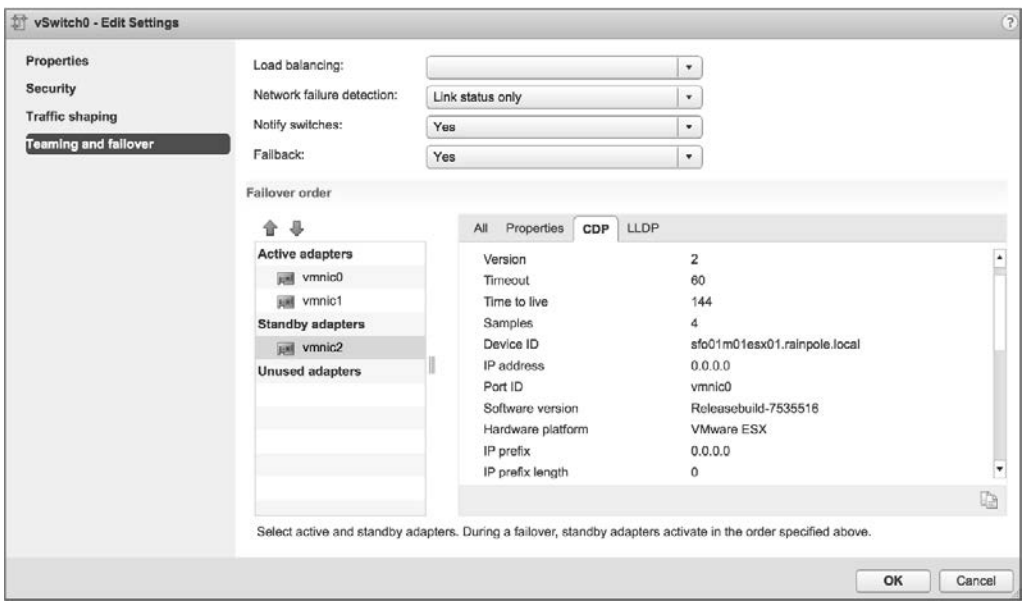
Teraz ponownie rzuć okiem na rysunek 5.35. Zobaczysz tam opcję *Use Explicit Failover Order*. Jest to reguła bezpośredniej kolejności przełączania awaryjnego wspomniana wcześniej na początku punktu „Konfigurowanie grup kart sieciowych". Jeśli wybierzesz tę opcję zamiast jednej z reguł równoważenia obciążenia, ruch będzie przenoszony do następnego dostępnego uplinku na liście aktywnych kart sieciowych. Jeżeli nie będą dostępne żadne aktywne karty sieciowe, ruch zostanie przeniesiony do pierwszej dostępnej karty z listy kart rezerwowych. Jak sugeruje nazwa opcji,

do określenia sposobu umieszczania ruchu na fizycznych kartach sieciowych ESXi użyje kolejności kart zdefiniowanej w kolejności przełączania awaryjnego. Ponieważ ta opcja nie przeprowadza zupełnie żadnego równoważenia obciążenia, na ogół nie jest zalecana i powinieneś raczej użyć jednej z pozostałych trzech dostępnych opcji.

Opcja *Failback* kontroluje sposób, w jaki ESXi będzie obsługiwać kartę sieciową, gdy odzyska ona sprawność po usunięciu awarii. Pokazane na rysunkach 5.37 i 5.38 ustawienie domyślne *Yes* (tak) wskazuje, że karta sieciowa zostanie przywrócona do stanu aktywności natychmiast po odzyskaniu sprawności i zastąpi ewentualną rezerwową kartę sieciową, która mogła zająć jej miejsce podczas awarii. Ustawienie *Failback* na *No* (nie) oznacza, że po odzyskaniu sprawności karta sieciowa pozostanie nieaktywna, dopóki inna karta sieciowa nie ulegnie awarii, co spowoduje zastąpienie nowo uszkodzonej karty.

Aby skonfigurować kolejność przełączania awaryjnego dla grupy kart sieciowych, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do hosta ESXi posiadającego przełącznik wirtualny, dla którego chcesz zmienić kolejność przełączania awaryjnego. Po wybraniu hosta ESXi wybierz zakładkę *Configure* i kliknij *Virtual Switches*.
3. Wybierz przełącznik wirtualny, który chcesz edytować, i kliknij ikonę *Edit Settings*.
4. Wybierz opcję *Teaming and Failover*.
5. Użyj przycisków *Move Up* (przenieś w górę) i *Move Down* (przenieś w dół), aby dostosować kolejność oraz położenie kart sieciowych na listach *Active Adapters*, *Standby Adapters* i *Unused Adapters*, jak pokazano na rysunku 5.39.



RYSUNEK 5.39. Kolejność przełączania awaryjnego dla grupy kart sieciowych jest określona przez kolejność kart na listach Active Adapters, Standby Adapters i Unused Adapters

6. Kliknij *OK*, aby zapisać zmiany.

Przełącznik wirtualny, na którym dochodzi do przełączenia awaryjnego, ma informacje o tym zdarzeniu. Natomiast fizyczny przełącznik, do którego podłączony jest dany przełącznik wirtualny, nie dowiaduje się od razu. Jak widać na rysunku 5.39, przełącznik wirtualny zawiera ustawienie *Notify Switches* (powiadamianie przełączników), które po ustawieniu na *Yes* pozwoli fizycznemu przełącznikowi natychmiast dowiadywać się o takich zmianach jak:

- włączenie maszyny wirtualnej (lub każdorazowe zarejestrowanie się klienta na przełączniku wirtualnym),
- ruch vMotion,
- zmiana adresu MAC,
- przełączenie awaryjne lub odzyskanie sprawności po awarii w grupie kart sieciowych.

W przypadku każdego z tych zdarzeń przełącznik fizyczny jest powiadamiany o zmianie przy użyciu protokołu RARP (ang. *Reverse Address Resolution Protocol*). RARP aktualizuje tablice wyszukiwania na fizycznych przełącznikach i zapewnia najkrótsze opóźnienie w przypadku wystąpienia zdarzenia przełączenia awaryjnego.

WYŁĄCZANIE POWIADOMIEŃ PRZEŁĄCZNIKÓW

Opcja *Notify Switches* powinna być ustawiona na *No*, gdy dana grupa portów obejmuje maszyny wirtualne korzystające z funkcjonalności sieciowego równoważenia obciążenia (ang. *Network Load Balancing* — NLB) firmy Microsoft w trybie unicastowym. Zapobiega to wysyłaniu pakietów RARP przez przełącznik wirtualny lub grupę portów.

Chociaż VMkernel działa proaktywnie, to aby utrzymać przepływ ruchu z komponentów sieci wirtualnej do komponentów sieci fizycznej w celu zminimalizowania opóźnień w sieci VMware zaleca podjęcie następujących działań:

- wyłączenie PAgP i LACP na przełącznikach fizycznych,
- wyłączenie DTP lub negocjacji trunkingu,
- wyłączenie STP.

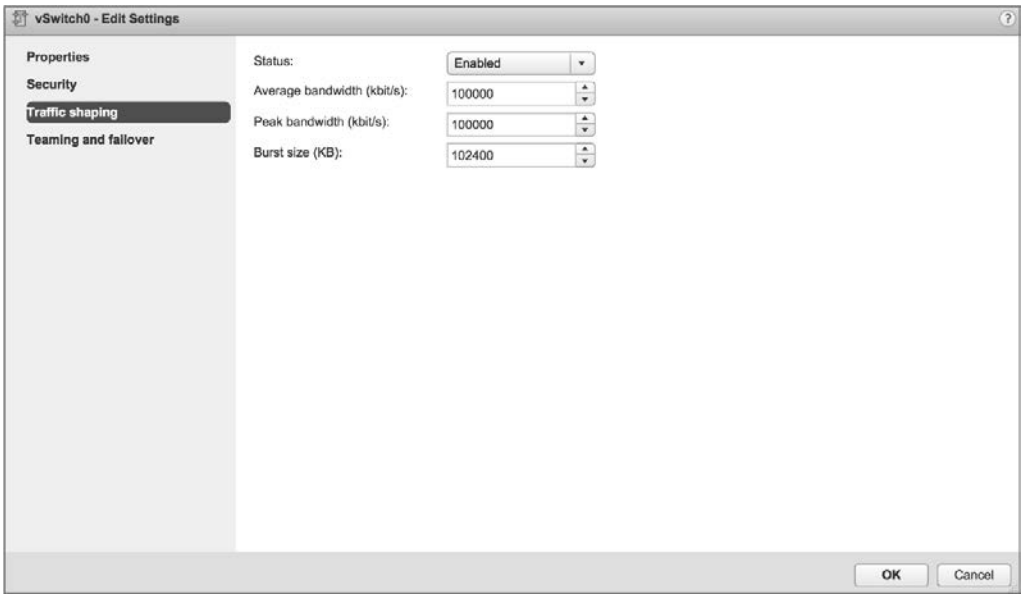
PRZEŁĄCZNIKI WIRTUALNE Z PRZEŁĄCZNIKAMI CISCO

VMware zaleca skonfigurowanie urządzeń Cisco do korzystania z trybu PortFast dla portów dostępu lub trybu trunkowego PortFast dla portów trunkowych.

Używanie i konfigurowanie kształtowania ruchu

Domyślnie wszystkie wirtualne karty sieciowe podłączone do przełącznika wirtualnego mają dostęp do pełnej przepustowość fizycznej karty sieciowej, z którą powiązany jest ten przełącznik. Innymi słowy, jeśli przełącznik wirtualny ma przypisaną kartę sieciową 10 Gb/s, każda maszyna wirtualna skonfigurowana do korzystania z tego przełącznika ma dostęp do przepustowości 10 Gb/s. Oczywiście jeśli rywalizacja o przepustowość stanie się wąskim gardłem ograniczającym wydajność maszyn wirtualnych, pomocna będzie grupa kart sieciowych. Jednak jako uzupełnienie grupy kart sieciowych możesz także włączyć i skonfigurować kształtowanie ruchu (*Traffic shaping*). Ustanawia ono stałe limity dla maksymalnej przepustowości, średniej przepustowości i wielkości serii w celu ograniczenia możliwości maszyn wirtualnych do okupowania przepustowości wychodzącej.

Jak pokazano na rysunku 5.40, wartości maksymalnej (*Peak bandwidth*) i średniej przepustowości (*Average bandwidth*) są określane w kilobitach na sekundę, a wartość wielkości serii (*Burst size*) jest konfigurowana w kilobajtach. Wartość wprowadzona dla średniej przepustowości dyktuje ilość danych przesyłanych na sekundę na całym przełączniku wirtualnym. Wartość maksymalnej przepustowości określa maksymalną ilość danych, jaką może przekazywać przełącznik wirtualny bez porzucania pakietów. Natomiast wartość wielkości serii definiuje maksymalną ilość danych w serii. Wielkość serii oblicza się, mnożąc przepustowość przez czas. Jeżeli w okresach wysokiego wykorzystania przepustowości wielkość serii przekracza skonfigurowaną wartość, pakiety są porzucane na korzyść innego ruchu. Jeśli jednak kolejka do przetwarzania ruchu sieciowego nie jest pełna, pakiety są zachowane do przesłania w późniejszym terminie.



RYSUNEK 5.40. Kształtowanie ruchu ogranicza wychodzącą przepustowość dostępną dla grupy portów

KSZTAŁTOWANIE RUCHU JAKO OSTATECZNOŚĆ

Z funkcjonalności kształtowania ruchu należy korzystać oszczędnie. Powinna być zarezerwowana dla sytuacji, w których maszyny wirtualne konkurują o przepustowość i nie można już dodać kolejnych fizycznych kart sieciowych. Z uwagi na niskie koszty kart sieciowych warto poświęcić czas na budowanie przełączników wirtualnych z grupami kart sieciowych, zamiast zmniejszać przepustowości dostępne dla określonych zestawów maszyn wirtualnych. Ponadto sterowanie operacjami we-wy jest znacznie łatwiejsze w zarządzaniu i zapewnia sprawiedliwy podział między grupami portów maszyn wirtualnych i grupami portów VMkernel.

Aby skonfigurować kształtowanie ruchu, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do hosta ESXi, na którym chcesz skonfigurować kształtowanie ruchu. Na wybranym hoście ESXi przejdź do sekcji *Virtual Switch* w zakładce *Configure*.
3. Wybierz przełącznik wirtualny, na którym chcesz włączyć kształtowanie ruchu, a następnie kliknij ikonę *Edit Settings*.

4. Wybierz *Traffic shaping* (kształtowanie ruchu).
5. Z rozwijanej listy *Status* wybierz opcję *Enabled* (włączone).
6. Dostosuj wartość *Average bandwidth* do żądanej liczby kilobitów na sekundę.
7. Dostosuj wartość *Peak bandwidth* do żądanej liczby kilobitów na sekundę.
8. Dostosuj wartość *Burst size* do żądanej liczby kilobajtów.

Należy pamiętać, że kształtowanie ruchu na standardowym przełączniku vSphere dotyczy tylko ruchu wychodzącego.

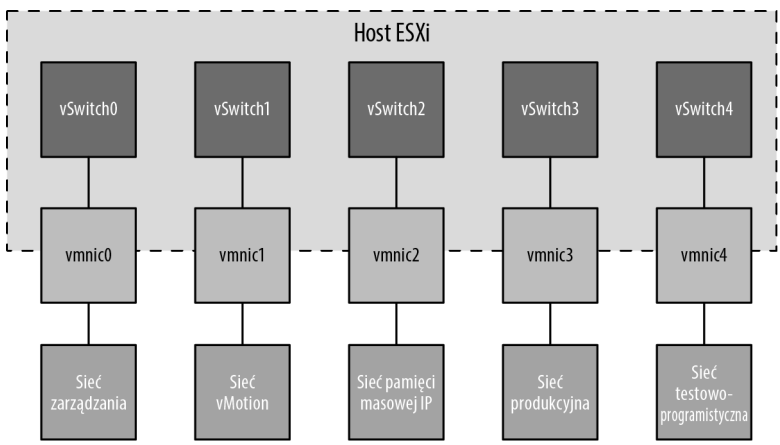
Złożenie w całość wszystkich elementów

Zobaczyłeś już, jak współdziałają ze sobą różne komponenty wirtualnej sieci ESXi, i dowiedziałeś się, czym są przełączniki wirtualne, porty, grupy portów, uplinki, grupy kart sieciowych oraz VLAN-y. Ale jak te wszystkie elementy złożyć w użyteczną całość?

Liczba i konfiguracja przełączników wirtualnych i grup portów zależy od kilku czynników, w tym liczby kart sieciowych na hoście ESXi, liczby podsieci IP, istnienia VLAN-ów i liczby sieci fizycznych. Jeśli chodzi o konfigurację przełączników wirtualnych i grup portów maszyn wirtualnych, nie ma jednej poprawnej konfiguracji, która spełniłaby wymagania wszystkich scenariuszy. Jednak im większa liczba fizycznych kart sieciowych na hoście ESXi, tym większą elastyczność będziesz mieć w swojej architekturze sieci wirtualnej.

W dalszej części rozdziału omówimy kilka zaawansowanych czynników projektowych, ale na razie pozostańmy przy kilku podstawowych uwarunkowaniach dotyczących projektu. Jeśli przełączniki wirtualne nie będą skonfigurowane z VLAN-ami, musisz utworzyć osobny przełącznik wirtualny dla każdej podsieci IP lub sieci fizycznej, z którą chcesz się połączyć. Zostało to zilustrowane wcześniej na rysunku 5.24 podczas omawiania VLAN-ów. Aby zrozumieć tę koncepcję, przeanalizujmy jeszcze dwa przykłady.

Rysunek 5.41 pokazuje scenariusz z pięcioma podsieciami IP, z którymi muszą łączyć się komponenty infrastruktury wirtualnej. Maszyny wirtualne ze środowiska produkcyjnego muszą mieć łączność z produkcyjną siecią LAN, maszyny wirtualne ze środowiska testowego muszą mieć łączność z testową siecią LAN, VMkernel musi mieć dostęp do sieci LAN pamięci masowej IP i vMotion, a host ESXi musi mieć dostęp do sieci LAN zarządzania. W tym scenariuszu bez VLAN-ów i grup portów host ESXi musi mieć pięć różnych przełączników wirtualnych i pięć różnych fizycznych kart sieciowych. (Oczywiście nie uwzględnia to redundancji lub grup kart sieciowych dla przełączników wirtualnych).



RYSUNEK 5.41. Bez VLAN-ów każda podsieć IP będzie wymagać osobnego przełącznika wirtualnego z odpowiednim typem połączenia

PO CO TO TAK PROJEKTOWAĆ?

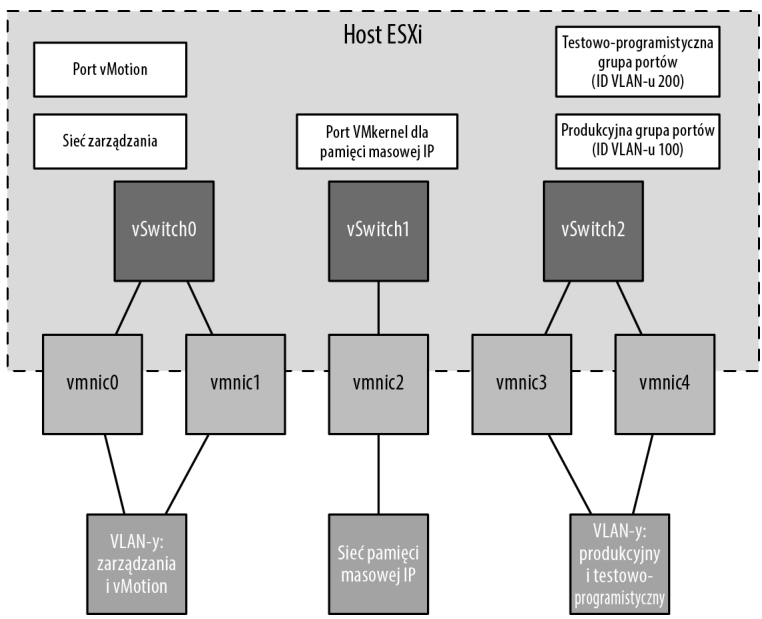
Podczas procesu projektowania sieci wirtualnej ludzie często pytają, dlaczego nie tworzyć przełączników wirtualnych z jak największą liczbą portów, aby pozostawić miejsce na rozwój, albo dlaczego należy używać wielu przełączników wirtualnych zamiast jednego (lub odwrotnie). Na niektóre z tych pytań łatwo udzielić odpowiedzi, natomiast odpowiedzi na inne pytania są kwestią doświadczenia i, szczerze mówiąc, osobistych preferencji.

Zastanów się nad pytaniem dotyczącym kwestii tworzenia przełączników wirtualnych z możliwie największą liczbą portów. Jak zobaczysz w tabeli 5.1 w dalszej części tego rozdziału, maksymalna liczba portów wirtualnego przełącznika sieciowego na host wynosi 4096. Oznacza to, że jeśli tworzone będą przełączniki wirtualne z 1024 portami, będzie można ich utworzyć tylko 4. Pomnóż 1024 przez 4, a otrzymasz maksymalną liczbę 4096 portów na host. (Należy pamiętać, że przełączniki wirtualne tak naprawdę mają 8 portów zarezerwowanych, więc przełącznik 1016-portowy w rzeczywistości ma 1024 porty).

Odpowiedzi na inne pytania niekoniecznie są tak jednoznaczne. Korzystanie z wielu przełączników wirtualnych może ułatwić przeniesienie niektórych sieci do dedykowanych sieci fizycznych. Jeśli klient będzie chciał na przykład przenieść sieć zarządzania do dedykowanej fizycznej sieci zarządzania w celu zapewnienia większego bezpieczeństwa, znacznie łatwiej będzie to osiągnąć za pomocą dedykowanego przełącznika wirtualnego dla sieci zarządzania niż przy użyciu pojedynczego przełącznika wirtualnego. To samo można powiedzieć o używaniu VLAN-ów. Należy jednak pamiętać o zasadzie, że liczba przełączników wirtualnych powinna być jak najmniejsza, aby implementacja była prostsza i łatwiejsza w utrzymaniu.

Ostatecznie jednak wiele obszarów projektowania sieci wirtualnych to po prostu obszary osobistych preferencji lub wyborów podyktowanych polityką zespołu ds. infrastruktury sieciowej, a nie koniecznością techniczną. Umiejętność określania, do której kategorii należą poszczególne obszary, może być bardzo pomocna w zrozumieniu zwirtualizowanego środowiska sieciowego.

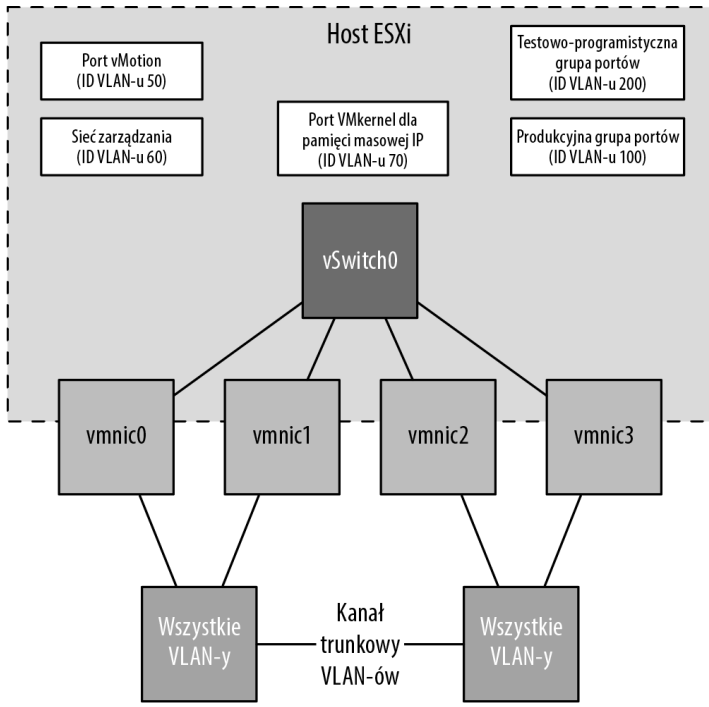
Rysunek 5.42 pokazuje tę samą konfigurację, ale tym razem z zastosowaniem VLAN-ów do sieci zarządzania, vMotion, produkcyjnej oraz testowo-programistycznej. Sieć pamięci masowej IP pozostaje fizycznie oddzielną siecią (co jest typową konfiguracją dla iSCSI w wielu środowiskach).



RYSUNEK 5.42. Użycie fizycznie oddzielnej sieci dla pamięci masowej IP ogranicza redukcję liczby przełączników wirtualnych i uplinków

Konfiguracja pokazana na rysunku 5.42 nadal wykorzystuje trzy karty sieciowe, ale tym razem możesz zapewnić grupy kart sieciowych dla wszystkich sieci.

Gdyby sieć pamięci masowej IP została skonfigurowana jako VLAN, można by jeszcze bardziej zmniejszyć liczbę przełączników i uplinków. Rysunek 5.43 pokazuje możliwą konfigurację, która obsługiwałaby taki scenariusz.



RYSUNEK 5.43. Dzięki użyciu grup portów i VLAN-ów na przełącznikach wirtualnych wymagana byłaby jeszcze mniejsza liczba przełączników wirtualnych i uplinków

Tym razem możesz zapewnić grupy kart sieciowych dla wszystkich rodzajów ruchu — zarządzania, vMotion, pamięci masowej IP i maszyn wirtualnych — za pomocą tylko jednego przełącznika wirtualnego z wieloma uplinkami.

Oczywiste jest więc, że istnieje ogromna elastyczność w sposobie łączenia ze sobą przełączników wirtualnych, uplinków i grup portów w celu utworzenia sieci wirtualnej zdolnej do obsługi danej infrastruktury. Nawet przy tej całej elastyczności istnieją jednak pewne ograniczenia. Tabela 5.1 zawiera listę niektórych ograniczeń sieci ESXi.

TABELA 5.1. Limity konfiguracyjne dla komponentów sieciowych ESXi (w standardowych przełącznikach vSphere)

Element konfiguracji	Maksimum
Liczba portów na przełącznik wirtualny	4088
Liczba portów na host (przełącznik standardowy/rozproszony)	4096
Liczba grup portów na przełącznik wirtualny	512
Liczba uplinków na przełącznik wirtualny	32
Liczba aktywnych portów na host (przełącznik standardowy/rozproszony)	1016

KONFIGURACJE PRZEŁĄCZNIKÓW WIRTUALNYCH — NIE POPADAJ W SKRAJNOŚCI

Chociaż można utworzyć przełącznik wirtualny z maksymalną liczbą 4088 portów (tak naprawdę 4096), nie zalecamy praktykowania tego, jeżeli przewiduje się rozwój. Hosty ESXi nie mogą mieć więcej niż 4096 portów, jeśli więc utworzysz przełącznik wirtualny z 4088 portami, będziesz ograniczony do jednego przełącznika wirtualnego na tym hoście. Z pojedynczym przełącznikiem wirtualnym możesz nie być w stanie połączyć się ze wszystkimi potrzebnymi sieciami. Gdy skończą Ci się porty na hoście ESXi, a będziesz musiał utworzyć nowy przełącznik wirtualny, możesz zmniejszyć liczbę portów na istniejącym przełączniku. Zastosowanie tej zmiany wymaga ponownego uruchomienia, ale vMotion pozwala przenieść maszyny wirtualne na inny host, aby zapobiec ich przestojom.

Pamiętaj również o uwzględnieniu scenariuszy, takich jak awaria hosta, gdy maszyny wirtualne są restartowane na innych hostach przy użyciu funkcjonalności vSphere HA (opisanej szczegółowo w rozdziale 7. „Zapewnienie wysokiej dostępności i ciągłość działania"). Jeśli w tym przypadku przełącznik wirtualny okaże się zbyt mały (na przykład będzie miał za mało portów), również możesz napotkać problem.

Pamiętaj, że rozmiar przełącznika wirtualnego jest wypadkową wielu zmiennych, które należy wziąć pod uwagę, więc planuj starannie! Zalecamy tworzenie wirtualnych przełączników z tak dużą liczbą portów, aby zaspokoić bieżące potrzeby i prognozowany wzrost oraz zapewnić zdolność przełączania awaryjnego.

Dzięki dużej elastyczności zapewnianej przez różne komponenty sieciowe vSphere możesz mieć pewność, że bez względu na to, z jaką konfiguracją sieci fizycznej będziesz mieć do czynienia, zawsze istnieje kilka sposobów jej integracji z siecią vSphere. To, co skonfigurujesz dzisiaj, może ulec zmianie w przyszłości, gdy zmieni się infrastruktura lub sprzęt. ESXi zapewnia wystarczającą liczbę narzędzi i opcji, aby zagwarantować schemat skutecznej komunikacji między vSphere a sieciami fizycznymi.

Praca z rozproszonymi przełącznikami vSphere

Do tej pory koncentrowaliśmy się wyłącznie na standardowych przełącznikach vSphere (czyli po prostu przełącznikach wirtualnych). Począwszy od wersji vSphere 4.0, dostępna jest też druga opcja: rozproszone przełączniki vSphere.

Podczas gdy standardowymi przełącznikami vSphere zarządza się na poszczególnych hostach, rozproszony przełącznik vSphere Distributed Switch działa jako pojedynczy przełącznik wirtualny na wszystkich powiązanych hostach ESXi w obiekcie centrum danych. Między rozproszonym i standardowym przełącznikiem vSphere istnieje wiele podobieństw:

- Rozproszony przełącznik vSphere zapewnia łączność dla maszyn wirtualnych i interfejsów VMkernel.
- Rozproszony przełącznik vSphere wykorzystuje fizyczne karty sieciowe jako uplinki, aby zapewnić łączność z zewnętrzną siecią fizyczną.
- Rozproszony przełącznik vSphere może wykorzystywać VLAN-y do logicznej segmentacji sieci.
- Na rozproszonym przełączniku vSphere dostępna jest większość tych samych reguł równoważenia obciążenia, odzyskiwania sprawności po awarii, bezpieczeństwa i kształtowania ruchu, co na standardowym przełączniku. Dostępnych jest też kilka dodatków, które zwiększają funkcjonalność przełącznika rozproszonego w porównaniu ze standardowym.

Oczywiście istnieją również różnice, a najważniejsza z nich polega na tym, że rozproszony przełącznik vSphere może obejmować wiele hostów w centrum danych vSphere — w przypadku standardowych przełączników każdy host ma własny zestaw niezależnych przełączników wirtualnych i grup portów. Zmniejsza to znacznie złożoność w klastrowych środowiskach ESXi i upraszcza dodawanie nowych serwerów do klastra ESXi.

Oficjalnym skrótowcem VMware dla rozproszonego przełącznika vSphere jest VDS (ang. *vSphere Distributed Switch*). W tym rozdziale będziemy używać jego pełnej nazwy (rozproszony przełącznik vSphere) lub skrótowca VDS, a czasem będziemy nazywać go po prostu przełącznikiem rozproszonym, aby wskazać tę konkretną jego funkcjonalność.

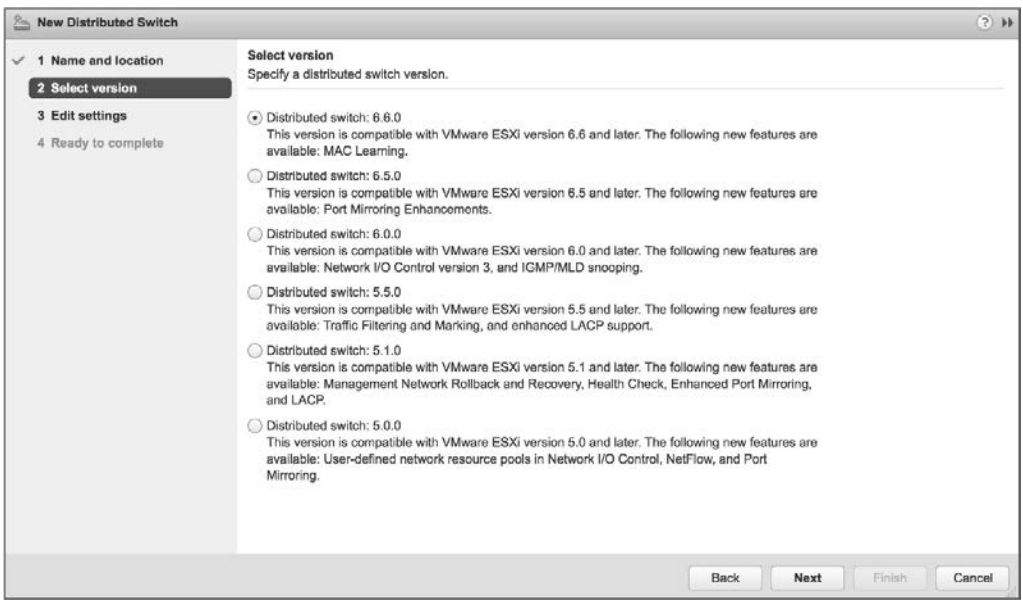
Tworzenie rozproszonego przełącznika vSphere

Proces tworzenia i konfigurowania przełącznika rozproszonego jest dwuetapowy. Najpierw tworzy się przełącznik rozproszony na poziomie obiektu centrum danych, a następnie dodaje się do niego hosty ESXi.

Aby utworzyć nowy rozproszony przełącznik vSphere, wykonaj następujące czynności:

1. Uruchom klienta internetowego vSphere i połącz się z instancją serwera vCenter.
2. Na ekranie głównym klienta internetowego vSphere wybierz *Networking* (sieci) w panelu nawigatora.
3. Kliknij prawym przyciskiem myszy obiekt centrum danych, przejdź do *Distributed Switch* (przełącznik rozproszony) i wybierz *New Distributed Switch* (nowy przełącznik rozproszony).

   Spowoduje to uruchomienie kreatora nowego przełącznika rozproszonego.
4. Podaj nazwę nowego przełącznika rozproszonego i kliknij *Next* (dalej).
5. Wybierz wersję przełącznika rozproszonego, który chcesz utworzyć. Rysunek 5.44 pokazuje dostępne opcje dla wersji przełączników rozproszonych.



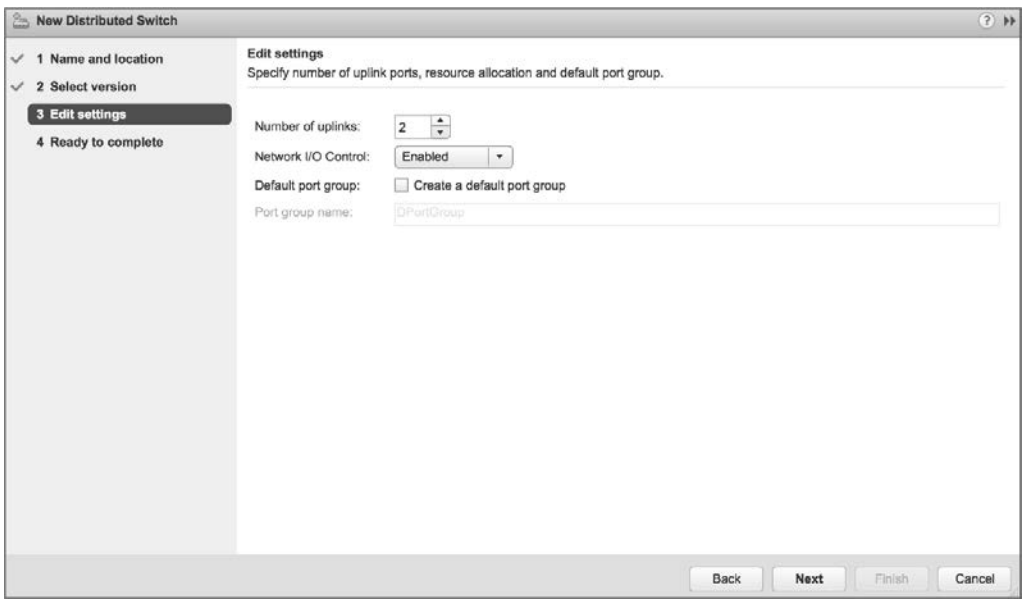
RYSUNEK 5.44. Jeśli chcesz zapewnić wsparcie dla wszystkich funkcjonalności dostępnych w vSphere 6.7, musisz użyć wersji 6.6.0 przełącznika rozproszonego

Dostępnych jest sześć opcji:

- *Distributed switch: 5.0.0* — wersja kompatybilna z platformą vSphere 5.0 i nowszą. Dodaje obsługę takich funkcjonalności jak zdefiniowane przez użytkownika pule zasobów sieciowych w sterowaniu operacjami we-wy sieci, NetFlow i mirroring portów.
- *Distributed switch: 5.1.0* — wersja kompatybilna z platformą vSphere 5.1 lub nowszą. Ten przełącznik rozproszony dodaje obsługę przywracania i odzyskiwania sieci, sprawdzania kondycji, rozszerzonego mirroringu portów i LACP.
- *Distributed switch: 5.5.0* — wersja obsługiwana przez platformę vSphere 5.5 lub nowszą. Ten przełącznik rozproszony dodaje filtrowanie i oznaczanie ruchu oraz rozszerzoną obsługę LACP.
- *Distributed switch: 6.0.0* — wersja obsługiwana przez platformę vSphere 6.0 lub nowszą. Ta wersja przełącznika rozproszonego dodaje obsługę NIOC3, snoopingu multicastowego i filtrowania multicastowego.
- *Distributed switch: 6.5.0* — wersja obsługiwana przez platformę vSphere 6.5 lub nowszą. Ta wersja przełącznika rozproszonego obsługuje protokół mirroringu portów ERSPAN.
- *Distributed switch: 6.6.0* — najnowsza wersja obsługiwana tylko przez platformę vSphere 6.7. Ta wersja przełącznika rozproszonego obsługuje uczenie się adresów MAC.

W tym przypadku wybierz rozproszony przełącznik vSphere w wersji 6.6.0 i kliknij *Next*.

6. Określ liczbę portów uplinkowych (*Number of uplinks*), jak pokazano na rysunku 5.45.



RYSUNEK 5.45. Liczba uplinków kontroluje, ile fizycznych kart sieciowych z każdego hosta może służyć jako uplinki przełącznika rozproszonego

7. Na tym samym ekranie pokazanym na rysunku 5.45 wybierz włączenie (*Enabled*) lub wyłączenie (*Disabled*) sterowania operacjami we-wy sieci (*Network I/O Control*). Określ także, czy chcesz utworzyć domyślną grupę portów (*Default port group*), a jeśli tak, wpisz nazwę dla domyślnej grupy portów. W tym przykładzie pozostaw włączone sterowanie operacjami we-wy i utwórz domyślną grupę portów o wybranej nazwie. Kliknij *Next*.
8. Przejrzyj ustawienia nowego przełącznika rozproszonego. Jeśli wszystko wygląda poprawnie, kliknij *Finish*. W przeciwnym razie użyj przycisku *Back* (wstecz), aby wrócić i zmienić ustawienia w razie potrzeby.

Po zakończeniu pracy kreatora w kliencie internetowym vSphere pojawi się nowy przełącznik rozproszony. Możesz kliknąć ten nowy przełącznik rozproszony, aby zobaczyć podłączone do niego hosty ESXi (jeszcze żadnych nie ma), hostowane na nim maszyny wirtualne (jeszcze żadnych nie ma), rozproszone grupy portów (jest tylko jedna — ta utworzona przez Ciebie podczas korzystania z kreatora) i grupy portów uplinkowych (również jest tylko jedna).

Wszystkie te informacje można również uzyskać przy użyciu interfejsu vSphere CLI lub PowerCLI, ale ze względu na sposób działania polecenia `esxcli` w tym celu musisz najpierw dodać jakiś host ESXi do przełącznika rozproszonego. Zobaczmy, jak to się robi.

ROZPROSZONE PRZEŁĄCZNIKI VSPHERE WYMAGAJĄ SERWERA VCENTER

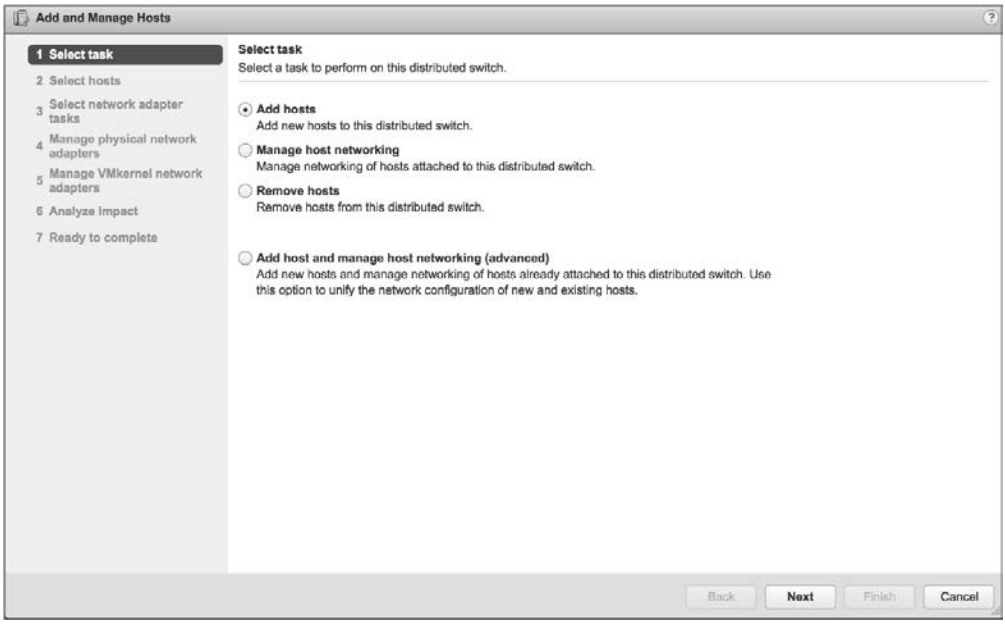
Może się to wydawać oczywiste, ale należy zaznaczyć, że ze względu na współdzieloną naturę rozproszonego przełącznika vSphere wymagany jest serwer vCenter. Innymi słowy, w środowisku, które nie jest zarządzane przez serwer vCenter, nie można utworzyć rozproszonego przełącznika vSphere ani nim zarządzać. Jednak w przypadku awarii serwera vCenter ruch będzie nadal płynął. Oprócz tego będziesz także potrzebować licencji Enterprise Plus.

Po utworzeniu przełącznika rozproszonego dodanie hosta ESXi jest stosunkowo łatwe. Kiedy host ESXi zostanie dodany, wszystkie rozproszone grupy portów zostaną automatycznie propagowane do tego hosta z prawidłową konfiguracją. Ponieważ zmiany konfiguracji są wprowadzane za pośrednictwem klienta internetowego vSphere, serwer vCenter przesyła te zmiany do wszystkich wymaganych hostów ESXi — na tym właśnie polega rozproszona natura tego przełącznika. Administratorzy VMware, którzy są przyzwyczajeni do zarządzania dużymi klastrami ESXi i konieczności ciągłego tworzenia przełączników wirtualnych i grup portów oraz zachowywania spójności w tych grupach portów na wszystkich hostach, docenią zredukowanie narzutu administracyjnego oferowane przez przełączniki rozproszone.

Aby dodać host ESXi do istniejącego przełącznika rozproszonego, wykonaj następujące czynności:

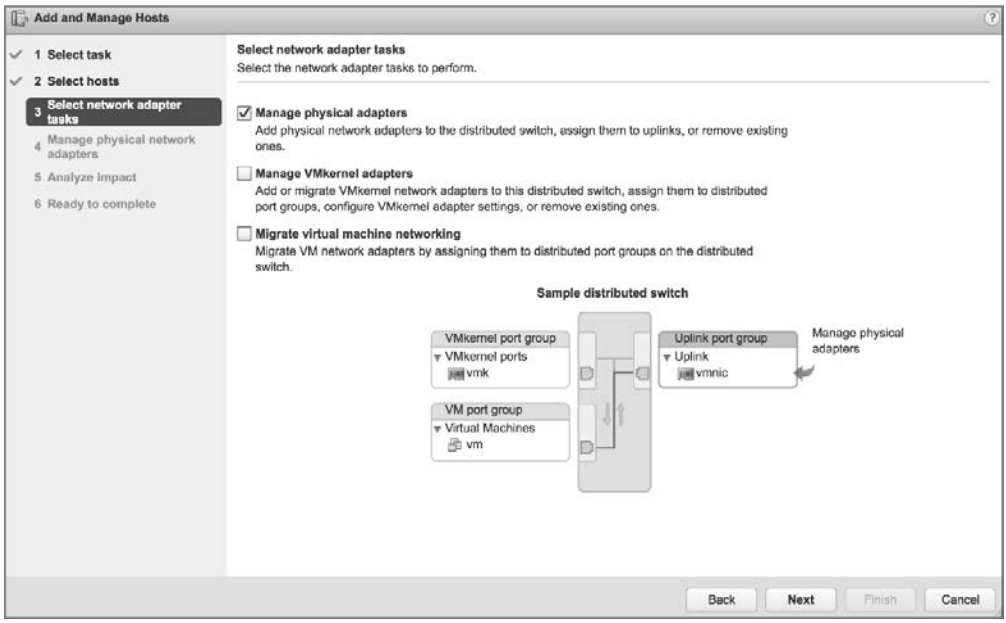
1. Uruchom klienta internetowego vSphere i połącz się z instancją serwera vCenter.
2. W nawigatorze kliknij *Networking*.
3. Wybierz istniejący przełącznik rozproszony, a następnie z menu *Actions* (działania) wybierz opcję *Add and Manage Hosts* (dodawanie hostów i zarządzanie nimi).

   Spowoduje to uruchomienie kreatora dodawania hostów i zarządzania nimi, pokazanego na rysunku 5.46.
4. Wybierz przycisk opcji *Add hosts* (dodawanie hostów) i kliknij *Next*.
5. Kliknij zieloną ikonę znaku plus, aby dodać host ESXi. Spowoduje to otwarcie okna dialogowego *Select New Host* (wybór nowego hosta).
6. Na liście nowych hostów do dodania zaznacz pole wyboru obok nazwy każdego hosta ESXi, który chcesz dodać do przełącznika rozproszonego. Gdy skończysz, kliknij *OK*, a następnie kliknij *Next*, aby kontynuować.



RYSUNEK 5.46. Kiedy pracujesz z przełącznikami rozproszonymi, klient internetowy vSphere oferuje pojedynczy kreator, który umożliwia dodawanie hostów, usuwanie hostów lub zarządzanie siecią hostów

7. Następny ekran oferuje do wykonania trzy różne zadania związane z kartami sieciowymi, jak pokazano na rysunku 5.47. W tym przypadku upewnij się, że wybrana jest tylko opcja *Manage physical adapters* (zarządzanie fizycznymi kartami sieciowymi). Kliknij *Next*, aby kontynuować.



RYSUNEK 5.47. Wszystkie opcje wprowadzania na przełączniku rozproszonym zmian związanych z kartami sieciowymi są skonsolidowane w jednym kreatorze

Opcja *Manage VMkernel adapters* (zarządzanie kartami sieciowymi VMkernel) pozwala dodawać, migrować, edytować lub usuwać karty sieciowe VMkernel (porty VMkernel) z tego przełącznika rozproszonego.

Opcja *Migrate virtual machine networking* (migrowanie sieci maszyn wirtualnych) umożliwia przeprowadzenie migracji kart sieciowych maszyny wirtualnej do tego przełącznika rozproszonego.

8. Następny ekran pozwala wybrać fizyczne karty sieciowe hostów, które powinny być podłączone do grupy portów uplinkowych przełącznika rozproszonego. Kliknij fizyczną kartę sieciową, którą chcesz dodać, a następnie kliknij dla niej opcję *Assign uplink* (przypisz uplink). Zostaniesz poproszony o potwierdzenie uplinku, do którego powinna zostać podłączona ta fizyczna karta sieciowa. Powtórz ten proces dla tylu fizycznych kart sieciowych, ile uplinków skonfigurowałeś dla przełącznika rozproszonego.

UWAGA

Dopóki nie przeprowadzisz migracji portu VMkernel zarządzania, pozostaw przynajmniej jedną fizyczną kartę sieciową podłączoną do standardowego przełącznika vSphere. Jeśli na tym etapie spróbujesz przenieść wszystkie karty, operacja zakończy się niepowodzeniem, ponieważ nie będzie łączności z hostami ESXi.

9. Powtórz krok 8. dla każdego hosta ESXi, który chcesz dodać do przełącznika rozproszonego. Kliknij *Next*, kiedy skończysz dodawać uplinki dla wszystkich hostów ESXi.
10. Ekran *Analyze Impact* (analiza wpływu) wyświetla potencjalne skutki zmian zaproponowanych przez kreator. Jeśli wszystko wydaje się być w porządku, kliknij *Next*. W przeciwnym razie kliknij *Back*, aby wrócić i zmienić ustawienia.
11. Kliknij *Finish*, aby zakończyć działanie kreatora.

Będziesz miał okazję ponownie zobaczyć ten kreator nieco później. W punkcie „Zarządzanie kartami sieciowymi VMkernel" w dalszej części tego rozdziału będziemy na przykład omawiać szczegółowo opcje zarządzania fizycznymi kartami sieciowymi i kartami VMkernel.

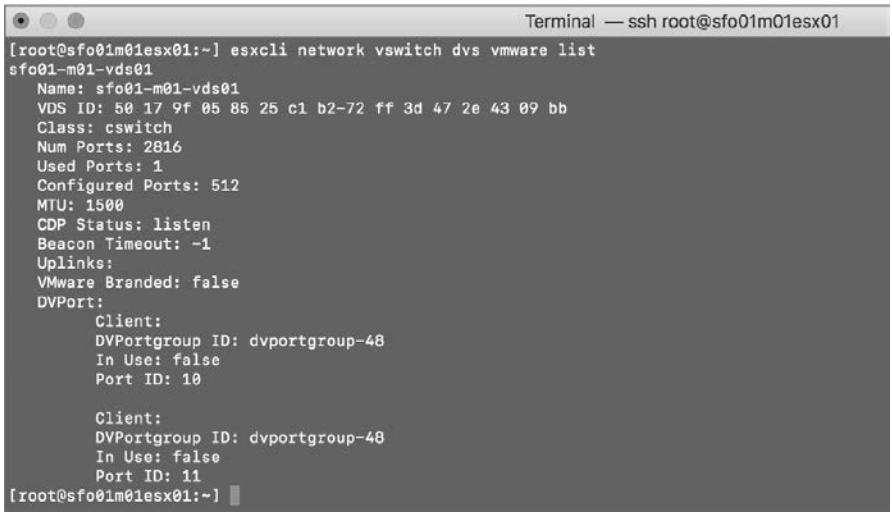
Wspomnieliśmy wcześniej w tym punkcie, że po dodaniu hosta do przełącznika rozproszonego w celu uzyskania informacji o przełączniku rozproszonym możesz użyć interfejsu vSphere CLI. Poniższe polecenie spowoduje wyświetlenie listy przełączników rozproszonych, do których należy dany host ESXi:

```
esxcli network vswitch dvs vmware list
```

Dane wyjściowe z tego polecenia będą wyglądać mniej więcej jak dane pokazane na rysunku 5.48.

Aby zobaczyć, jakie inne zadania związane z przełącznikami rozproszonymi vSphere możesz wykonać za pomocą interfejsu vSphere CLI, użyj parametru `--help` z poleceniem `network vswitch dvs vmware namespace`.

Przyjrzyjmy się teraz kilku innym zadaniom związanym z przełącznikami rozproszonymi. Zaczniemy od usunięcia hosta ESXi z przełącznika rozproszonego.



RYSUNEK 5.48. Polecenie esxcli powoduje wyświetlenie pełnych informacji na temat konfiguracji przełącznika rozproszonego

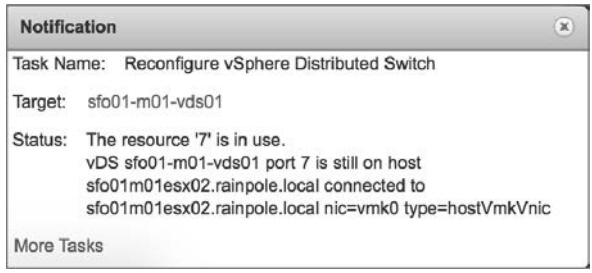
Usuwanie hosta ESXi z przełącznika rozproszonego

Oczywiście można również usuwać hosty ESXi z przełącznika rozproszonego. Usunięcie hosta z przełącznika rozproszonego jest niemożliwe w przypadku, kiedy jakieś jego maszyny wirtualne są nadal podłączone do rozproszonej grupy portów na tym przełączniku. Jest to analogiczne do próby usunięcia standardowego przełącznika lub grupy portów, gdy nadal podłączona jest maszyna wirtualna. To również jest niemożliwe. Aby umożliwić usunięcie hosta ESXi z przełącznika rozproszonego, musisz przenieść wszystkie maszyny wirtualne na standardowy przełącznik lub inny przełącznik rozproszony.

Aby usunąć pojedynczy host ESXi z przełącznika rozproszonego, wykonaj następujące czynności:

1. Uruchom klienta internetowego vSphere i połącz się z instancją serwera vCenter.
2. Przejdź do listy przełączników rozproszonych i wybierz ten, z którego chcesz usunąć pojedynczy host ESXi.
3. Z menu *Actions* wybierz *Add and Manage Hosts*. Spowoduje to wyświetlenie okna dialogowego *Add and Manage Hosts*, pokazanego wcześniej na rysunku 5.47.
4. Zaznacz przycisk opcji *Remove Hosts* (usuwanie hostów). Kliknij *Next*.
5. Kliknij zieloną ikonę znaku plus, aby wybrać hosty do usunięcia z przełącznika rozproszonego.
6. W oknie dialogowym *Select Member Hosts* (wybór hostów członkowskich) zaznacz pola wyboru obok każdego hosta ESXi, który chcesz usunąć z przełącznika rozproszonego. Gdy skończysz wybierać hosty, kliknij *OK*.
7. Kliknij *Finish*, aby usunąć wybrane hosty ESXi.
8. Jeśli do przełącznika rozproszonego nadal podłączone są jakieś maszyny wirtualne, klient internetowy vSphere wyświetli błąd podobny do pokazanego na rysunku 5.49.

RYSUNEK 5.49.
Klient internetowy vSphere nie pozwoli na usunięcie hosta z przełącznika rozproszonego, jeśli nadal podłączona jest jakaś maszyna wirtualna



Aby pozbyć się tego błędu, przekonfiguruj odpowiednią maszynę wirtualną (lub maszyny wirtualne), aby używała innego przełącznika rozproszonego lub przełącznika standardowego. Potem kontynuuj usuwanie hosta z przełącznika rozproszonego.

Jeśli do przełącznika rozproszonego nie są podłączone żadne maszyny wirtualne lub przekonfigurowałeś ewentualne podłączone maszyny wirtualne, aby używały innego przełącznika rozproszonego lub przełącznika standardowego, host zostanie usunięty.

Oprócz usuwania poszczególnych hostów ESXi z przełącznika rozproszonego możesz także usunąć cały przełącznik rozproszony.

Usuwanie przełącznika rozproszonego

Usunięcie ostatniego hosta ESXi z przełącznika rozproszonego nie powoduje usunięcia samego przełącznika. Nawet jeśli z przełącznika rozproszonego zostały usunięte wszystkie maszyny wirtualne i (lub) hosty ESXi, ten przełącznik nadal istnieje w inwentarzu vCenter. Musisz usunąć sam obiekt przełącznika rozproszonego.

Przełącznik rozproszony można usunąć tylko wtedy, gdy żadne maszyny wirtualne nie są przypisane do rozproszonej grupy portów na tym przełączniku. W przeciwnym razie usuwanie zostanie zablokowane i wyświetlony zostanie komunikat błędu podobny do pokazanego wcześniej na rysunku 5.49. I tym razem przed kontynuowaniem operacji musisz przekonfigurować maszynę wirtualną (lub maszyny wirtualne) do używania innego przełącznika standardowego lub rozproszonego. Więcej informacji na temat modyfikowania ustawień sieciowych maszyny wirtualnej znajdziesz w rozdziale 9. „Tworzenie maszyn wirtualnych i zarządzanie nimi".

Jeśli żadne maszyny wirtualne nie są podłączone do żadnej rozproszonej grupy portów na przełączniku rozproszonym, wykonaj następujące czynności, aby usunąć ten przełącznik rozproszony:

1. Uruchom klienta internetowego vSphere i połącz się z instancją serwera vCenter.
2. W nawigatorze wybierz *Networking*.
3. Wybierz istniejący rozproszony przełącznik vSphere.
4. Z menu *Actions* wybierz *Delete* (usuwanie).

   Przełącznik rozproszony i wszystkie powiązane grupy portów rozproszonych zostaną usunięte z inwentarza i ze wszystkich podłączonych hostów.

Większość konfiguracji przełącznika rozproszonego nie jest wykonywana dla niego samego, ale raczej dla rozproszonych grup portów na tym przełączniku. Niemniej jednak przyjrzyjmy się najpierw zarządzaniu samymi przełącznikami rozproszonymi.

Zarządzanie przełącznikami rozproszonymi

Jak stwierdziliśmy wcześniej, zdecydowana większość zadań, które administrator VMware wykonuje przy przełączniku rozproszonym, obejmuje pracę z rozproszonymi grupami portów. Rozproszone grupy portów omówimy później, a na razie zajmijmy się zarządzaniem przełącznikiem rozproszonym.

Zakładkę *Configure* już widziałeś i zobaczysz ponownie w tym rozdziale. Będziesz w szczególności dość dużo pracować w sekcji *Settings* (ustawienia) zakładki *Configure*. Będziesz kontynuować pracę w tej sekcji, gdy zaczniesz tworzyć rozproszone grupy portów. Zakładka *Configure* obejmuje również sekcję *Resource Allocation* (alokacja zasobów).

Sekcja *Resource Allocation* służy do przydzielania zasobów dla ruchu systemowego i tworzenia pul zasobów sieciowych do użytku z funkcją sterowania operacjami we-wy sieci. Temat ten omówiono w rozdziale 11. „Zarządzanie alokacją zasobów".

W zakładce *Monitor* (monitorowanie) znajdują się trzy sekcje:

- Sekcja *Issues* (problemy) pokazuje problemy i (lub) alarmy dotyczące przełącznika rozproszonego.
- Sekcje *Tasks* (zadania) i *Events* (zdarzenia) zapewniają wgląd w ostatnio wykonane zadania oraz listę zdarzeń, które miały miejsce i mogą być wynikiem działania użytkownika lub systemu. W tych sekcjach możesz na przykład sprawdzić, który użytkownik wykonał określone zadanie, lub przejrzeć różne zdarzenia dotyczące wybranego przełącznika rozproszonego.
- Sekcja *Health* (kondycja) centralizuje informacje o kondycji przełącznika rozproszonego, takie jak kontrola stanu VLAN-ów, MTU i inne.

Sekcja *Health* zawiera kilka dość ważnych funkcji, więc przyjrzyjmy się jej bliżej.

Korzystanie z kontroli kondycji i przywracania sieci

Funkcjonalność kontroli kondycji rozproszonego przełącznika vSphere została dodana w vSphere 5.1 i jest dostępna tylko wtedy, gdy używasz przełącznika rozproszonego w wersji co najmniej 5.1.0. Ma ona pomóc administratorom VMware w identyfikacji niezgodnych konfiguracji VLAN-ów, konfiguracji MTU i reguł grup kart sieciowych — są to typowe źródła problemów z łącznością.

Powinieneś poznać wymagania dotyczące korzystania z funkcjonalności kontroli kondycji. Są one następujące:

- Musisz używać przełącznika rozproszonego w wersji co najmniej 5.1.0.
- Kontrole VLAN-ów i MTU wymagają co najmniej dwóch kart sieciowych z aktywnymi łączami.
- Kontrole reguł grup kart sieciowych wymagają co najmniej dwóch kart sieciowych z aktywnymi łączami i przynajmniej dwóch hostów.

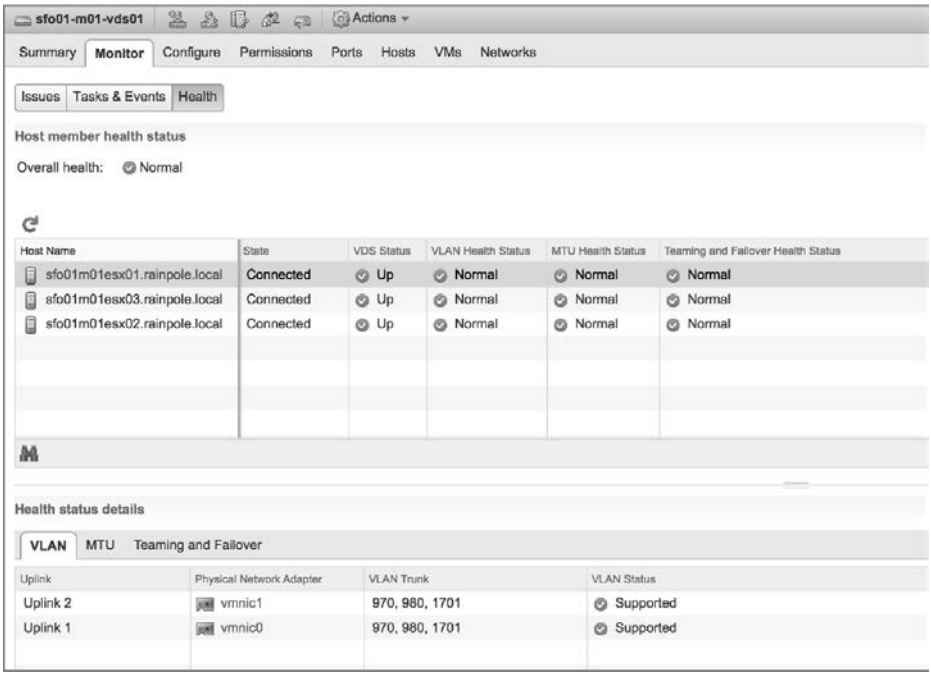
Domyślnie kontrola kondycji rozproszonego przełącznika vSphere jest wyłączona. Aby przeprowadzać kontrole, musisz włączyć tę funkcjonalność.

Aby włączyć kontrolę kondycji rozproszonego przełącznika vSphere, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking* i wybierz przełącznik rozproszony, na którym chcesz włączyć funkcjonalność kontroli kondycji.
3. Kliknij zakładkę *Configure*, a następnie wybierz *Health Check* (kontrola kondycji).

4. Kliknij przycisk *Edit* (edytowanie).
5. W oknie dialogowym *Edit Health Check Settings* (edytowanie ustawień kontroli kondycji) możesz niezależnie włączyć kontrolę VLAN-ów i MTU, grup kart sieciowych i przełączania awaryjnego, albo obie. Gdy skończysz, kliknij *OK*.

Kiedy funkcjonalność kontroli zostanie włączona, informacje o kondycji będziesz mógł przeglądać w zakładce *Monitor* przełącznika rozproszonego. Rysunek 5.50 pokazuje informacje o kondycji dla przełącznika rozproszonego po włączeniu kontroli.



RYSUNEK 5.50. Kontrola kondycji rozproszonego przełącznika vSphere pomaga identyfikować potencjalne problemy w konfiguracji

Z funkcjonalnością kontroli kondycji ściśle związana jest funkcjonalność o nazwie vSphere Network Rollback, czyli przywracanie ustawień sieciowych. Zadaniem przywracania sieci jest automatyczna ochrona środowisk przed takimi zmianami, które odłączyłyby hosty ESXi od serwera vCenter. Jej działanie polega na wycofywaniu zmian, jeśli są one nieprawidłowe. Przykładami zmian, których wprowadzanie jest weryfikowane, są zmiany szybkości lub dupleksu fizycznej karty sieciowej, aktualizowanie reguł grup kart sieciowych i przełączania awaryjnego dla przełącznika zawierającego interfejs zarządzania hosta ESXi lub zmiana ustawień IP interfejsu zarządzania hosta. Jeśli zmiana spowodowałaby utratę łączności dla zarządzania hostem, jest automatycznie wycofywana.

Wycofywanie może odbywać się na dwóch poziomach: na poziomie ustawień sieciowych hosta lub na poziomie przełącznika rozproszonego. Przywracanie sieci jest domyślnie włączone.

Oprócz automatycznego wycofywania zmian administratorzy VMware mają również możliwość wykonywania tych operacji ręcznie. Przeprowadzania ręcznego wycofywania zmian na poziomie hosta nauczyłeś się wcześniej w punkcie „Konfigurowanie sieci zarządzania", w którym omawialiśmy obszar *Network Restore Options* (opcje przywracania sieci) interfejsu DCUI hosta ESXi. Do wykonywania ręcznego wycofywania zmian w ustawieniach przełącznika rozproszonego używa się tego samego procesu, co w przypadku przywracania ustawień z zapisanej konfiguracji, czym zajmiemy się w następnym podpunkcie.

Importowanie i eksportowanie konfiguracji przełączników rozproszonych

Wersja vSphere 5.1 dodała możliwość eksportowania (zapisywania) i importowania (ładowania) konfiguracji przełącznika rozproszonego. Ta funkcjonalność może służyć wielu celom. Jednym z nich jest ręczne „wracanie" do poprzednio zapisanej konfiguracji.

Aby wyeksportować (zapisać) konfigurację przełącznika rozproszonego do pliku, wykonaj następujące czynności:

1. Zaloguj się do instancji serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do przełącznika rozproszonego, którego konfigurację chcesz zapisać.
3. Z menu *Actions* wybierz *Settings/Export Configuration* (ustawienia/eksport konfiguracji). Spowoduje to otwarcie okna dialogowego *Export Configuration*.
4. Zaznacz odpowiedni przycisk opcji, aby wyeksportować konfigurację przełącznika rozproszonego i wszystkich rozproszonych grup portów lub konfigurację samego przełącznika rozproszonego.
5. Opcjonalnie podaj opis eksportowanej (zapisywanej) konfiguracji. Następnie kliknij *OK*.
6. Po wyświetleniu zapytania, czy chcesz zapisać eksportowany plik konfiguracyjny, kliknij *Yes* (tak).
7. Użyj okna dialogowego zapisywania pliku Twojego systemu operacyjnego, aby wybrać lokalizację, w której powinien zostać zapisany eksportowany plik konfiguracyjny (o nazwie *backup.zip*).

Po wyeksportowaniu konfiguracji do pliku możesz później zaimportować ją z powrotem do środowiska vSphere, aby przywrócić zapisaną konfigurację. Możesz również zaimportować tę konfigurację do innego środowiska vSphere, na przykład zarządzanego przez osobną instancję serwera vCenter.

Aby zaimportować zapisaną konfigurację, wykonaj następujące czynności:

1. Zaloguj się do instancji serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do przełącznika rozproszonego, którego konfigurację chcesz przywrócić.
3. Z menu *Actions* wybierz *Settings/Restore Configuration* (ustawienia/przywracanie konfiguracji). Spowoduje to uruchomienie kreatora przywracania konfiguracji.
4. Użyj przycisku *Browse*, aby wybrać zapisany plik konfiguracji utworzony wcześniej za pomocą funkcji eksportu.
5. Zaznacz odpowiedni przycisk opcji, aby przywrócić konfigurację przełącznika rozproszonego i wszystkich rozproszonych grup portów lub konfigurację samego przełącznika rozproszonego.
6. Kliknij *Next*.
7. Przejrzyj ustawienia, które ma zaimportować kreator. Jeśli wszystko jest w porządku, kliknij *Finish*. W przeciwnym razie kliknij *Back*, aby wrócić i wprowadzić zmiany.

Zarówno funkcjonalność vSphere Network Rollback, jak i możliwość ręcznego eksportowania lub importowania konfiguracji przełącznika rozproszonego to ważne kroki naprzód w zarządzaniu przełącznikami rozproszonymi w środowisku vSphere.

Większość pracy, którą musi wykonać administrator VMware, będzie dotyczyła rozproszonych grup portów, więc skupmy naszą uwagę na nich.

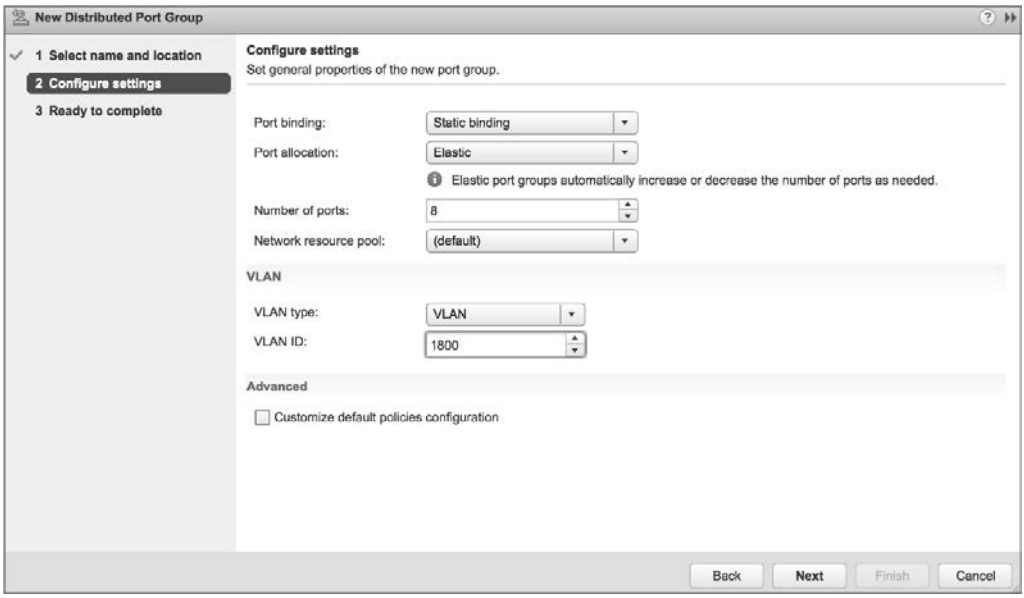
Praca z rozproszonymi grupami portów

W przypadku standardowych przełączników vSphere grupy portów są kluczem do zapewnienia łączności dla systemu VMkernel i maszyn wirtualnych. Bez portów i grup portów na przełączniku wirtualnym niczego nie można do tego przełącznika podłączyć. To samo dotyczy rozproszonych przełączników vSphere. Bez rozproszonej grupy portów do przełącznika rozproszonego nie można niczego podłączyć i taki przełącznik jest bezużyteczny. W kolejnych podpunktach przyjrzymy się bliżej tworzeniu, konfigurowaniu i usuwaniu rozproszonych grup portów.

Tworzenie rozproszonych grup portów

Wykonaj następujące kroki, aby utworzyć nową rozproszoną grupę portów:

1. Zaloguj się do instancji serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking*.
3. Wybierz istniejący rozproszony przełącznik vSphere, a następnie z menu *Actions* wybierz *Distributed Port Group/New Distributed Port Group* (rozproszona grupa portów/nowa rozproszona grupa portów).
4. Podaj nazwę nowej rozproszonej grupy portów. Naciśnij *Next*, aby kontynuować.
5. Pokazany na rysunku 5.51 ekran *Configure settings* (konfigurowanie ustawień) pozwala określić różne ustawienia dla nowej rozproszonej grupy portów.



RYSUNEK 5.51. Kreator nowej rozproszonej grupy portów oferuje szerokie możliwości dostosowywania ustawień tej grupy

Opcje *Port binding* (wiązanie portów) i *Port allocation* (alokacja portów) umożliwiają szczegółową kontrolę sposobu przydzielania portów z rozproszonej grupy portów do maszyn wirtualnych.

- Gdy wiązanie portów jest ustawione na domyślną wartość *Static binding*, porty są statycznie przypisywane do maszyn wirtualnych, gdy te maszyny są podłączane do przełącznika rozproszonego. Możesz także ustawić alokację portów na *Elastic* (w takim przypadku rozproszona grupa portów będzie miała na początku 8 portów i razie potrzeby ich liczba będzie zwiększana w przyrostach 8-portowych) lub *Fixed* (w takim przypadku domyślnie jest 128 portów).
- Gdy wiązanie portów jest ustawione na wartość *Dynamic binding* (wiązanie dynamiczne), określasz, ile portów powinna mieć rozproszona grupa portów (domyślnie jest to 128). Pamiętaj, że ta opcja jest przestarzała i niezalecana. Jeśli ją wybierzesz, klient internetowy vSphere wyświetli ostrzeżenie z tą informacją.
- Gdy wiązanie portów jest ustawione na wartość *Ephemeral binding* (wiązanie efemeryczne), nie można określić liczby portów ani metody alokacji portów.

Opcja *Network resource pool* (pula zasobów sieciowych) pozwala podłączyć tę rozproszoną grupę portów do puli zasobów sterowania operacjami we-wy sieci. Sterowanie operacjami we-wy sieci i pule zasobów sieciowych zostały opisane szczegółowo w rozdziale 11.

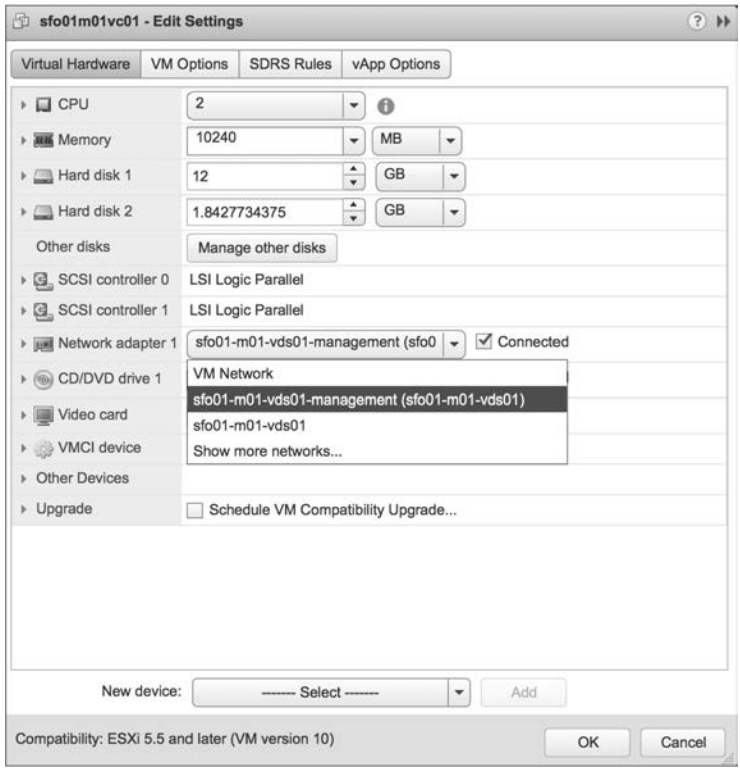
Opcje *VLAN type* (typ VLAN-ów) również mogą wymagać nieco wyjaśnień:

- Gdy typ VLAN-ów jest ustawiony na *None* (brak), rozproszona grupa portów będzie odbierać tylko nieoznakowany ruch. W takim przypadku uplinki muszą łączyć się z portami przełącznika fizycznego skonfigurowanymi jako porty dostępu do portów lub będą odbierać tylko nieoznakowany (natywny) ruch VLAN-ów.
- Gdy typ VLAN-ów jest ustawiony na *VLAN* (tj. 802.1Q VST), musisz podać identyfikator VLAN-u. Rozproszona grupa portów będzie odbierać ruch oznaczony tym identyfikatorem VLAN-u. Uplinki muszą łączyć się z portami przełącznika fizycznego skonfigurowanymi jako trunki VLAN-ów.
- Gdy typ VLAN-ów jest ustawiony na *VLAN Trunking* (tj. 802.1Q VGT), musisz określić zakres dozwolonych VLAN-ów. Rozproszona grupa portów będzie przekazywać znaczniki VLAN-ów do systemów operacyjnych gości na wszystkich podłączonych maszynach wirtualnych.
- Gdy typ VLAN-ów jest ustawiony na *Private VLAN*, musisz określić prywatny VLAN. Prywatne VLAN-y zostały opisane szczegółowo w dalszej części rozdziału, w punkcie „Konfigurowanie VLAN-ów prywatnych”.

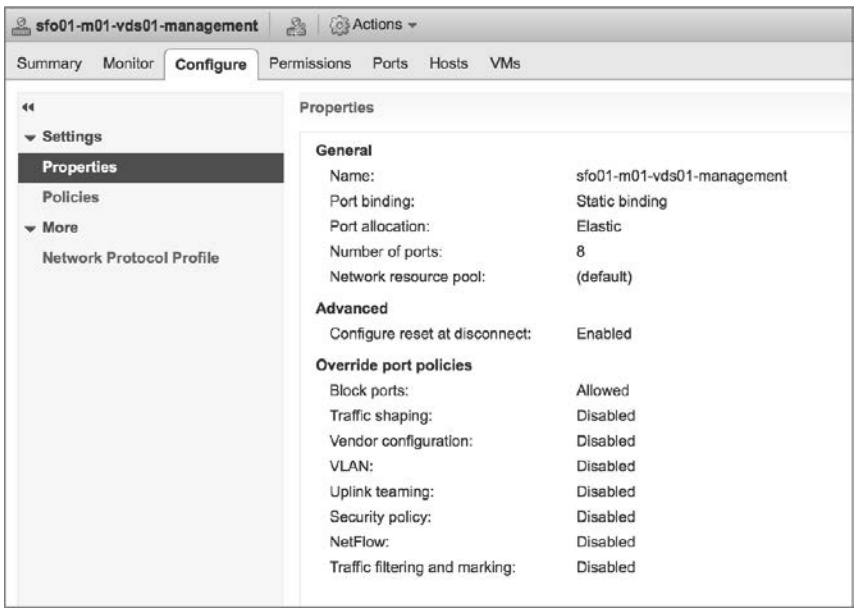
6. Wybierz żądane ustawienie wiązania portów (i alokacji portów, jeśli jest to konieczne), żądaną pulę zasobów sieciowych i żądany typ VLAN-ów, a następnie kliknij *Next*.
7. Na ekranie podsumowania przejrzyj ustawienia i kliknij *Finish*, jeśli wszystko jest w porządku. W przeciwnym razie kliknij przycisk *Back*, aby wrócić i wprowadzić niezbędne zmiany.

Po utworzeniu rozproszonej grupy portów możesz ją wybrać w konfiguracji maszyny wirtualnej jako możliwe połączenie sieciowe, jak pokazano na rysunku 5.52.

Gdy utworzysz rozproszoną grupę portów, pojawi się ona w widoku *Topology* (topologia) dla przełącznika rozproszonego, który ją hostuje. W kliencie internetowym vSphere ten widok jest dostępny w obszarze *Settings* zakładki *Configure* dla danego przełącznika rozproszonego. Kliknij w tym miejscu ikonę *Info* (mała litera *i* w niebieskim kółku) — uzyskasz więcej informacji o rozproszonej grupie portów i jej bieżącym stanie. Rysunek 5.53 pokazuje niektóre informacje dostarczone przez klienta internetowego vSphere na temat rozproszonej grupy portów.



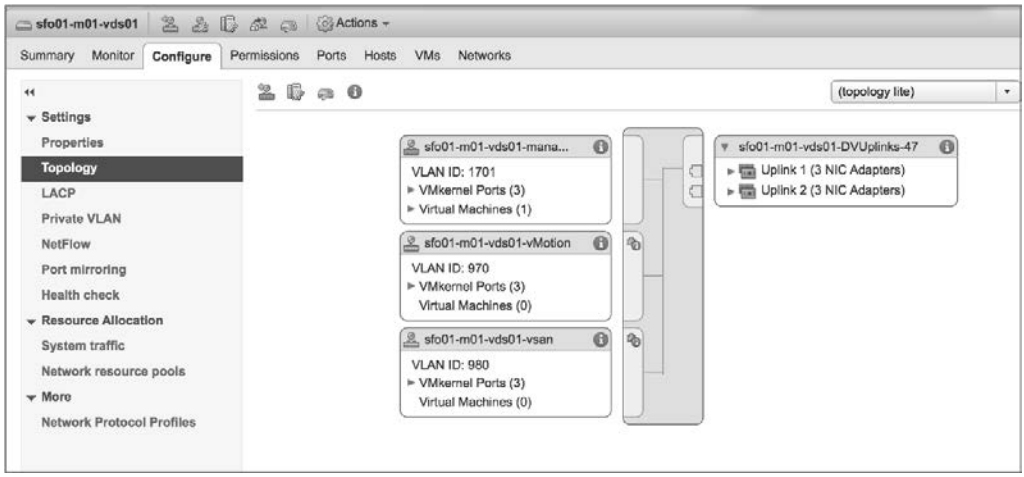
RYSUNEK 5.52. Rozproszona grupa portów wybrana jako połączenie sieciowe dla maszyn wirtualnych, podobnie jak grupy portów na standardowym przełączniku vSphere



RYSUNEK 5.53. Klient internetowy vSphere zapewnia podsumowanie konfiguracji rozproszonej grupy portów

Edytowanie rozproszonej grupy portów

Aby edytować konfigurację rozproszonej grupy portów, użyj linku *Edit Distributed Port Group Settings* w widoku *Topology* dla danego przełącznika rozproszonego. W kliencie internetowym vSphere możesz przejść do tego miejsca, wybierając przełącznik rozproszony, a następnie przechodząc do obszaru *Settings* zakładki *Configure*. Na koniec wybierz *Topology*, aby wygenerować widok topologii pokazany na rysunku 5.54.



RYSUNEK 5.54. Widok Topology dla przełącznika rozproszonego zapewnia łatwy dostęp do przeglądania i edycji rozproszonej grupy portów

Na razie skupmy się na modyfikowaniu ustawień VLAN-ów, kształtowania ruchu i grupy kart sieciowych dla rozproszonej grupy portów. Ustawienia reguł bezpieczeństwa i monitorowania omówimy w dalszej części tego rozdziału.

RÓŻNE OPCJE W ZALEŻNOŚCI OD WERSJI ROZPROSZONEGO PRZEŁĄCZNIKA VSPHERE

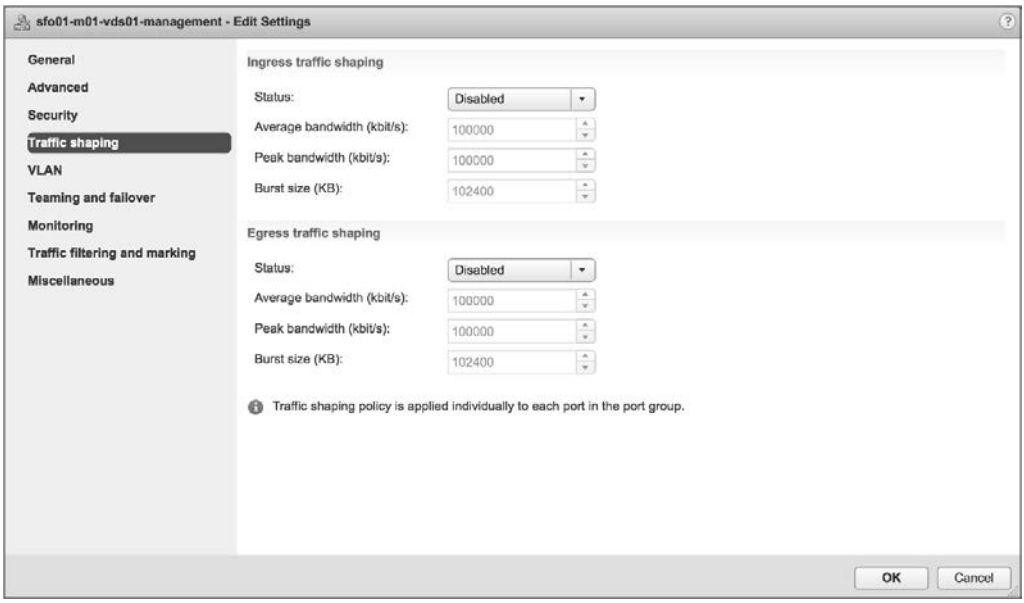
Jak pewnie pamiętasz, w kliencie internetowym vSphere można tworzyć różne wersje przełączników rozproszonych. Dostępne opcje konfiguracji zależą od wersji przełącznika.

Aby zmodyfikować ustawienia VLAN-ów dla rozproszonej grupy portów, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do rozproszonej grupy portów, którą chcesz edytować.
3. Kliknij ikonę *Edit Distributed Port Group Settings* (edytowanie ustawień rozproszonej grupy portów).
4. W oknie dialogowym *Edit Settings* (edytowanie ustawień) wybierz opcję *VLAN* z listy opcji po lewej stronie.
5. Zmodyfikuj ustawienia VLAN-ów, zmieniając identyfikator VLAN-u lub zmieniając typ VLAN-u na *VLAN Trunking* lub *Private VLAN*.
6. Gdy skończysz wprowadzanie zmian, kliknij *OK*.

Aby zmodyfikować reguły kształtowania ruchu dla rozproszonej grupy portów, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do rozproszonej grupy portów, którą chcesz edytować.
3. Kliknij ikonę *Edit Distributed Port Group Settings*.
4. Wybierz opcję *Traffic Shaping* (kształtowanie ruchu) z listy opcji po lewej stronie okna dialogowego ustawień rozproszonej grupy portów, jak pokazano na rysunku 5.55.



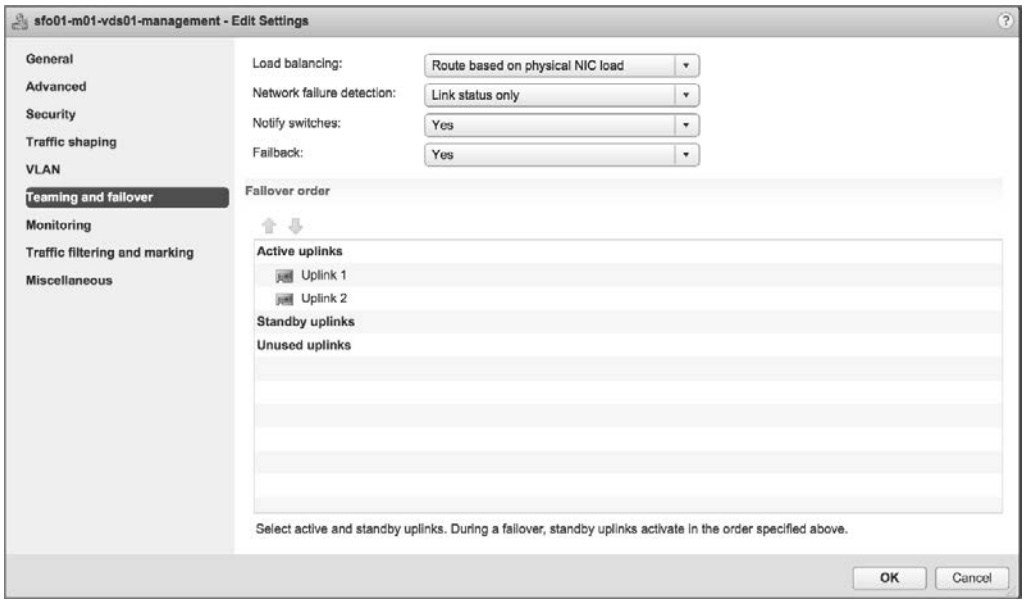
RYSUNEK 5.55. Do rozproszonej grupy portów na przełączniku rozproszonym możesz zastosować reguły kształtowania ruchu zarówno dla ruchu przychodzącego, jak i wychodzącego

Kształtowanie ruchu zostało opisane szczegółowo wcześniej w punkcie „Używanie i konfigurowanie kształtowania ruchu". W przypadku przełącznika rozproszonego istotna różnica polega na tym, że reguły kształtowania ruchu możesz stosować do ruchu przychodzącego i wychodzącego. W standardowych przełącznikach vSphere reguły kształtowania ruchu możesz stosować tylko do ruchu wychodzącego. Pozostałe ustawienia tej funkcji dla rozproszonej grupy portów są takie same, jak opisano wcześniej.

5. Gdy skończysz wprowadzanie zmian, kliknij *OK*.

Aby zmodyfikować reguły grupy kart sieciowych i przełączania awaryjnego dla rozproszonej grupy portów, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do grupy portów rozproszonych, którą chcesz edytować.
3. Kliknij ikonę *Edit Distributed Port Group Settings*.
4. Wybierz opcję *Teaming and Failover* z listy opcji po lewej stronie okna dialogowego *Edit Settings*, jak pokazano na rysunku 5.56.



RYSUNEK 5.56. Ustawienia Teaming and failover w oknie dialogowym Edit Settings dla rozproszonej grupy portów zapewniają opcje dla modyfikowania sposobu używania uplinków przez tę rozproszoną grupę portów

Ustawienia te zostały opisane szczegółowo w punkcie „Konfigurowanie grup kart sieciowych" z jednym istotnym wyjątkiem — od wersji 4.1 przełączniki rozproszone obsługują regułę równoważenia obciążenia na podstawie obciążenia fizycznych kart sieciowych (*Route Based On Physical NIC Load*). Gdy ustawiona jest ta reguła równoważenia obciążenia, ESXi sprawdza wykorzystanie uplinków pod kątem ewentualnych przeciążeń co 30 sekund. W tym przypadku przeciążenie jest zdefiniowane jako transmitowany lub odbierany ruch większy niż średnie wykorzystanie 75% przez okres dłuższy niż 30 sekund. W razie wykrycia przeciążenia uplinku ESXi dynamicznie zmienia przypisanie ruchu maszyny wirtualnej lub systemu VMkernel, kierując go do innego uplinku.

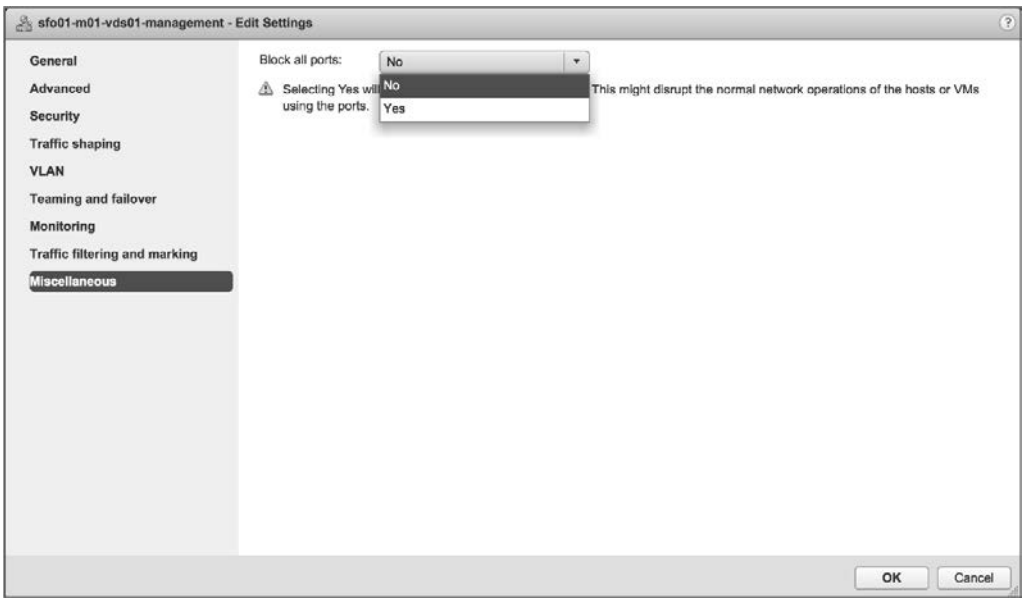
WYMAGANIA DLA GRUPOWANIA KART SIECIOWYCH OPARTEGO NA OBCIĄŻENIU

Grupowanie kart sieciowych oparte na obciążeniu (ang. *Load Based Teaming* — LBT) wymaga, aby wszystkie upstreamowe przełączniki fizyczne były częścią tej samej domeny warstwy drugiej (rozgłoszeniowej). Ponadto VMware zaleca włączenie opcji PortFast lub PortFast Trunk na wszystkich portach przełącznika fizycznego podłączonych do przełącznika rozproszonego korzystającego z LBT.

5. Gdy skończysz wprowadzanie zmian, kliknij *OK*.

Obsługa protokołu LACP (ang. *Link Aggregation Control Protocol*) w vSphere i sposób konfiguracji przełącznika rozproszonego do korzystania z LACP zostały omówione szczegółowo w dalszej części tego rozdziału, w punkcie „Konfigurowanie LACP". Punkt ten odwołuje się również do niektórych omówionych tutaj kwestii dotyczących modyfikowania ustawień grup kart sieciowych i przełączania awaryjnego.

Przeglądając dostępne ustawienia, możesz zauważyć opcję *Blocked Policy* (reguła blokowania). Jest to ekwiwalent wyłączania grupy portów w rozproszonej grupie portów. Rysunek 5.57 pokazuje, że ustawienie *Block all ports* (zablokuj wszystkie porty) może mieć wartość *Yes* (tak) lub *No* (nie). Jeśli ustawisz regułę blokowania na *Yes*, cały ruch wchodzący do tej rozproszonej grupy portów i wychodzący z niej będzie porzucany.



RYSUNEK 5.57. Reguła blokowania może być ustawiona na Yes lub No. Ustawienie tej reguły na Yes powoduje wyłączenie wszystkich portów w danej rozproszonej grupie portów

SKUTKI USTAWIENIA REGUŁY BLOKOWANIA NA YES

Nie zmieniaj reguły blokowana na *Yes*, chyba że jesteś przygotowany na przestój sieciowy dla wszystkich maszyn wirtualnych podłączonych do tej rozproszonej grupy portów!

PRZYDATNA FUNKCJONALNOŚĆ

Załóżmy, że przypadkowo ustawiłeś regułę blokowania na *Yes* w rozproszonej grupie portów, która zawiera interfejs zarządzania. Czy napotkałeś już jakąś funkcjonalność, która może pomóc w tej sytuacji? Tak! Pomocne byłoby tutaj przywracanie ustawień sieciowych (vSphere Network Rollback).

Usuwanie rozproszonej grupy portów

Aby usunąć rozproszoną grupę portów, najpierw wybierz tę grupę. Następnie w menu *Actions* kliknij *Delete* (usuwanie). Kliknij *Yes*, aby potwierdzić zamiar usunięcia danej rozproszonej grupy portów.

Jeśli do tej rozproszonej grupy nadal podłączone są jakieś maszyny wirtualne, klient internetowy vSphere uniemożliwi jej usunięcie i zarejestruje powiadomienie o błędzie.

Aby usunąć rozproszoną grupę portów, do której podłączona jest maszyna wirtualna, musisz najpierw przekonfigurować maszynę wirtualną do używania innej rozproszonej grupy portów na tym samym przełączniku rozproszonym, rozproszonej grupy portów na innym przełączniku rozproszonym lub standardowego przełącznika vSphere. Możesz użyć polecenia *Migrate Virtual Machines To Another Network* (migrowanie maszyn wirtualnych do innej sieci) z menu *Actions* lub po prostu bezpośrednio przekonfigurować ustawienia sieciowe maszyn wirtualnych.

Po przeniesieniu wszystkich maszyn wirtualnych z rozproszonej grupy portów możesz usunąć tę grupę przy użyciu procesu opisanego w poprzednich akapitach.

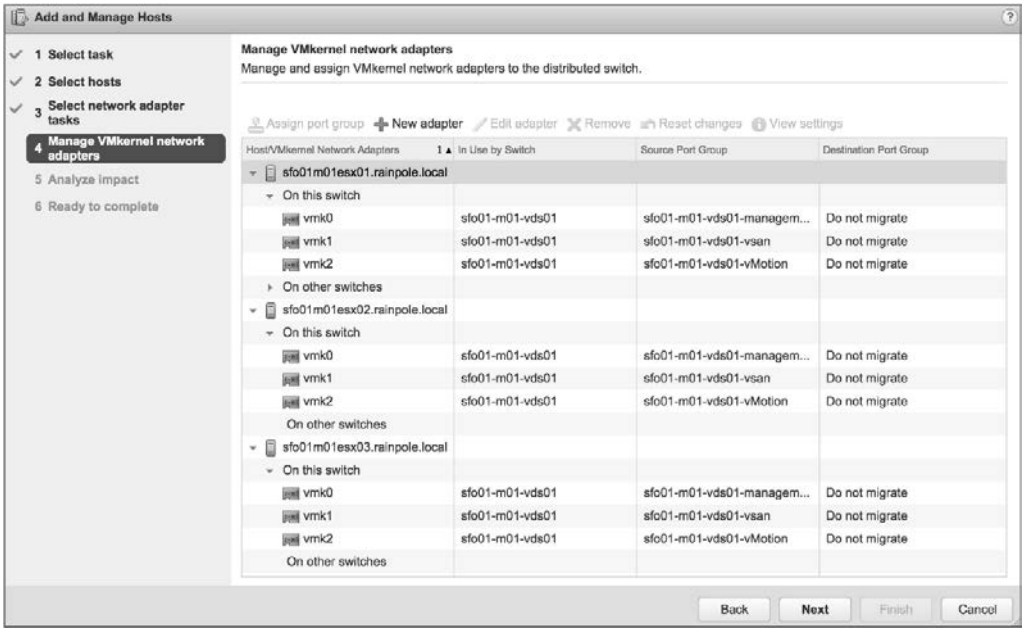
Następny punkt rozdziału koncentruje się na zarządzaniu kartami sieciowymi, zarówno fizycznymi, jak i wirtualnymi, podczas pracy z rozproszonym przełącznikiem vSphere.

Zarządzanie kartami sieciowymi VMkernel

W przełączniku rozproszonym zarządzanie kartami sieciowymi VMkernel i fizycznymi jest obsługiwane zupełnie inaczej niż w przypadku standardowego przełącznika vSphere. Karty sieciowe VMkernel to interfejsy VMkernel, więc gdy mówimy o zarządzaniu **kartami sieciowymi VMkernel**, tak naprawdę chodzi nam o zarządzanie **ruchem VMkernel**. Management, vMotion, pamięć masowa IP, vSAN, vSphere Replication, vSphere Replication NFC i rejestrowanie Fault Tolerance — to wszystko to typy ruchu VMkernel. Fizyczne karty sieciowe to oczywiście te karty, które służą jako uplinki dla przełącznika rozproszonego. Zarządzanie fizycznymi kartami sieciowymi obejmuje dodawanie lub usuwanie fizycznych kart podłączonych do portów w uplinkowej rozproszonej grupie portów na przełączniku rozproszonym.

Aby dodać kartę sieciową VMkernel do przełącznika rozproszonego, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking*.
3. Wybierz przełącznik rozproszony, do którego chcesz dodać kartę sieciową VMkernel.
4. Z menu *Actions* wybierz *Add and Manage Hosts* (dodawanie hostów i zarządzanie nimi).
5. Zaznacz przycisk opcji *Manage Host Networking* (zarządzanie siecią hosta), a następnie kliknij *Next*.
6. Na ekranie *Select Hosts* (wybierz hosty) użyj zielonej ikony ze znakiem plus, aby dodać hosty do listy hostów, które zostaną zmodyfikowane podczas tego procesu. Chociaż wydaje się, że kreator prosi o dodanie hostów do przełącznika rozproszonego, tak naprawdę dodajesz hosty do listy hostów, które mają być zmodyfikowane. Kliknij *Next*, gdy będziesz gotowy przejść do następnego kroku.
7. W tym przypadku modyfikujemy karty sieciowe VMkernel, więc upewnij się, że zaznaczone jest tylko pole wyboru *Manage VMkernel adapters* (zarządzanie kartami sieciowymi VMkernel). Kliknij *Next*.
8. Przy wybranym hoście ESXi kliknij link *New adapter* (nowa karta sieciowa) u góry okna *Manage VMkernel network adapters*, pokazanego na rysunku 5.58. Spowoduje to uruchomienie kreatora dodawania sieci.
9. W kreatorze dodawania sieci kliknij przycisk *Browse*, aby wybrać istniejącą rozproszoną grupę portów, do której należy dodać tę nową wirtualną kartę sieciową. (Zapoznaj się z ramką „Najpierw utwórz rozproszoną grupę portów”). Po wybraniu istniejącej rozproszonej grupy portów kliknij *OK*, a następnie kliknij *Next*.



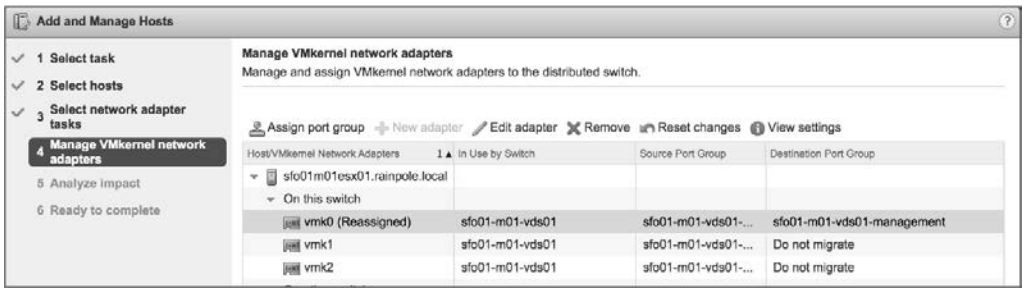
RYSUNEK 5.58. Ekran Manage VMkernel network adapters kreatora pozwala dodawać nowe karty sieciowe oraz przeprowadzać migracje istniejących

10. Na ekranie *Port Properties* (właściwości portu) wybierz, czy chcesz włączyć obsługę protokołu IPv4, IPv6, czy obu.
11. Włącz żądane usługi, takie jak vMotion, vSAN, vSphere Replication lub Fault Tolerance Logging, które powinny być uruchomione na tej nowej wirtualnej karcie sieciowej. Kliknij *Next*.
12. W zależności od tego, czy wybrałeś IPv4, IPv6, czy IPv4 i IPv6, na kilku kolejnych ekranach powinieneś skonfigurować odpowiednie ustawienia sieciowe.
    - Jeśli wybrałeś tylko IPv4, podaj żądane ustawienia IPv4.
    - Jeśli wybrałeś tylko IPv6, podaj prawidłowe ustawienia IPv6 dla swojej sieci.
    - Jeśli wybrałeś IPv4 i IPv6, w kreatorze będą dwa ekrany konfiguracyjne: jeden dla IPv4, a drugi osobny ekran dla IPv6.
13. Po wprowadzeniu poprawnych ustawień protokołu sieciowego wyświetlony zostanie ostatni ekran kreatora, przedstawiający ustawienia, które zostaną zastosowane. Jeśli wszystko jest w porządku, kliknij przycisk *Finish*. W przeciwnym razie kliknij przycisk *Back*, aby wrócić i w razie potrzeby zmienić ustawienia.
14. Spowoduje to powrót do kreatora dodawania hostów i zarządzania nimi, gdzie zobaczysz teraz nową wirtualną kartę sieciową, która zostanie dodana. Jeśli chcesz w tym samym czasie dodać wirtualną kartę sieciową dla innego hosta ESXi, powtórz kroki od 8. do 13. W przeciwnym razie kliknij *Next*.
15. Ekran *Analyze Impact* pokaże potencjalny wpływ wprowadzanych zmian. W razie potrzeby kliknij przycisk *Back*, aby wrócić i wprowadzić modyfikacje niwelujące negatywne skutki. Gdy będziesz gotowy kontynuować, kliknij *Next*.
16. Kliknij *Finish*, aby zatwierdzić zmiany w wybranym przełączniku rozproszonym i hostach ESXi.

NAJPIERW UTWÓRZ ROZPROSZONĄ GRUPĘ PORTÓW

Gdy dodajesz nowe karty sieciowe VMkernel do przełącznika rozproszonego, najpierw upewnij się, że utworzyłeś już rozproszoną grupę portów, której ma używać ta nowa wirtualna karta sieciowa. Kreator dodawania nowej wirtualnej karty sieciowej nie zapewnia sposobu tworzenia rozproszonej grupy portów jako części procesu.

Migracja istniejącej wirtualnej karty sieciowej, takiej jak port VMkernel w istniejącym standardowym przełączniku vSphere, odbywa się dokładnie w taki sam sposób. Jedyną różnicą jest to, że w kroku 8. musisz wybrać istniejącą wirtualną kartę sieciową, a następnie kliknąć u góry link *Assign port group* (przypisz grupę portów). Wybierz istniejącą grupę portów i kliknij *OK*, aby powrócić do kreatora, którego ekran będzie wyglądał podobnie do tego, co pokazano na rysunku 5.59.



RYSUNEK 5.59. Migracja wirtualnej karty sieciowej wymaga przypisania jej do istniejącej rozproszonej grupy portów

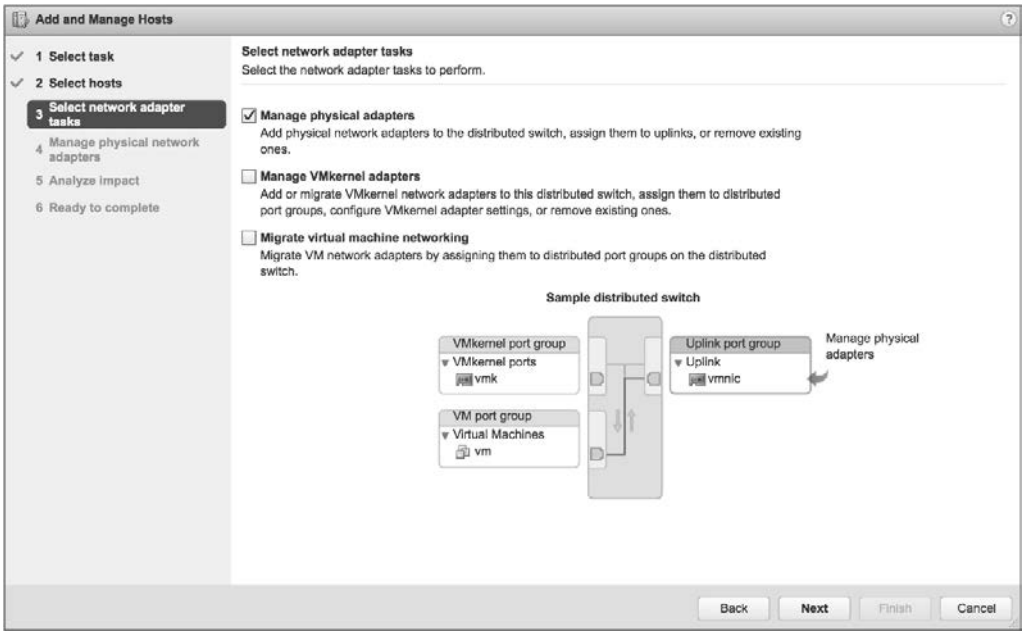
Po utworzeniu lub przeprowadzeniu migracji wirtualnej karty sieciowej używasz tego samego kreatora, aby w tym porcie wirtualnym wprowadzić zmiany — takie jak modyfikacja adresu IP, zmiana rozproszonej grupy portów, do której karta sieciowa jest przypisana — lub włączyć funkcjonalności, takie jak vMotion lub Fault Tolerance Logging. Aby edytować istniejącą wirtualną kartę sieciową, wybierz link *Edit Adapter* (edytuj kartę sieciową) widoczny na rysunku 5.59. Za pomocą tego kreatora możesz również usuwać karty sieciowe VMkernel, korzystając z linku *Remove* na ekranie *Manage VMkernel network adapters*.

Nie jest zadziwiające, że klient internetowy vSphere umożliwia także dodawanie lub usuwanie fizycznych kart sieciowych podłączonych do portów w uplinkowej grupie portów na przełączniku rozproszonym. Chociaż jak pokazano wcześniej, możesz określić fizyczne karty sieciowe podczas dodawania hosta do przełącznika rozproszonego, czasami konieczne może być podłączenie fizycznej karty sieciowej do przełącznika rozproszonego po tym, jak host zostanie już do niego dodany.

Aby dodać fizyczną kartę sieciową hosta ESXi do przełącznika rozproszonego, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Na ekranie głównym klienta internetowego vSphere przejdź do przełącznika rozproszonego, który chcesz modyfikować.
3. Z menu *Actions* wybierz *Add and Manage Hosts*.
4. Zaznacz przycisk opcji *Manage Host Networking*, a następnie kliknij przycisk *Next*.
5. Użyj zielonej ikony ze znakiem plus, aby dodać hosty ESXi do listy hostów, na które będą mieć wpływ zmiany wprowadzone w kreatorze. Po zakończeniu dodawania hostów ESXi do listy kliknij *Next*.

6. Upewnij się, że wybrana jest tylko opcja *Manage physical adapters* (zarządzanie fizycznymi kartami sieciowymi), jak pokazano na rysunku 5.60, i kliknij *Next*.

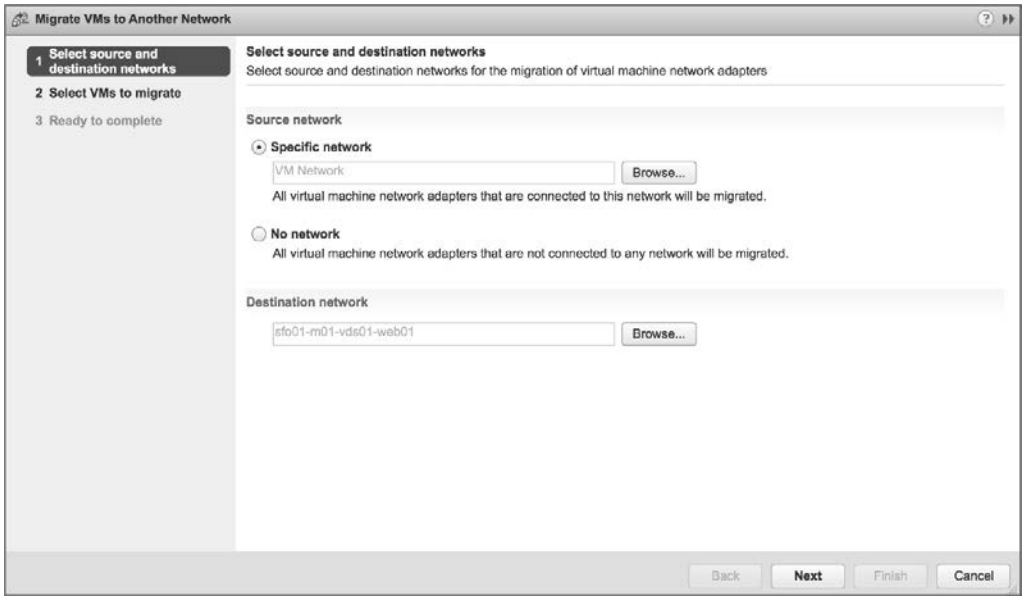


RYSUNEK 5.60. Aby zarządzać uplinkami na przełączniku rozproszonym, upewnij się, że zaznaczona jest tylko opcja Manage physical adapters

7. Na ekranie *Manage physical network adapters* możesz dodawać fizyczne karty sieciowe do wybranego przełącznika rozproszonego lub usuwać je z niego.
   - Aby dodać fizyczną kartę sieciową jako uplink, wybierz nieprzypisaną kartę sieciową z listy i kliknij link *Assign uplink* (przypisz uplink). Linku *Assign uplink* możesz użyć również do zmiany uplinku, do którego przypisana jest dana fizyczna karta sieciowa (na przykład aby przenieść ją z uplinku 2 do uplinku 3).
   - Aby usunąć fizyczną kartę sieciową jako uplink, wybierz przypisaną kartę z listy i kliknij link *Unassign adapter* (usuń przypisanie).
   - Aby przeprowadzić migrację fizycznej karty sieciowej z innego przełącznika do tego przełącznika rozproszonego, wybierz już przypisaną kartę sieciową i użyj linku *Assign uplink*. Spowoduje to automatyczne usunięcie karty z drugiego przełącznika i przypisanie jej do wybranego przełącznika rozproszonego.

   Powtórz ten proces dla każdego hosta na liście. Gdy będziesz gotowy kontynuować, kliknij *Next*.
8. Na ekranie *Analyze Impact* klient internetowy vSphere przedstawi informacje zwrotne na temat przewidywanego wpływu zmian. Jeśli wpływ zmian jest niepożądany, użyj przycisku *Back*, aby wrócić i dokonać niezbędnych modyfikacji. W przeciwnym razie kliknij *Next*.
9. Kliknij *Finish*, aby zakończyć działanie kreatora i zatwierdzić zmiany.

Oprócz przeprowadzania migracji kart sieciowych VMkernel i modyfikowania fizycznych kart sieciowych serwer vCenter umożliwia również wykonywanie migracji kart sieciowych maszyn wirtualnych, co oznacza migrację sieci maszyn wirtualnych między standardowymi przełącznikami vSphere i rozproszonymi przełącznikami vSphere, jak pokazano na rysunku 5.61.



RYSUNEK 5.61. Kreator migracji sieci maszyn wirtualnych automatyzuje proces migracji maszyn wirtualnych między siecią źródłową a siecią docelową

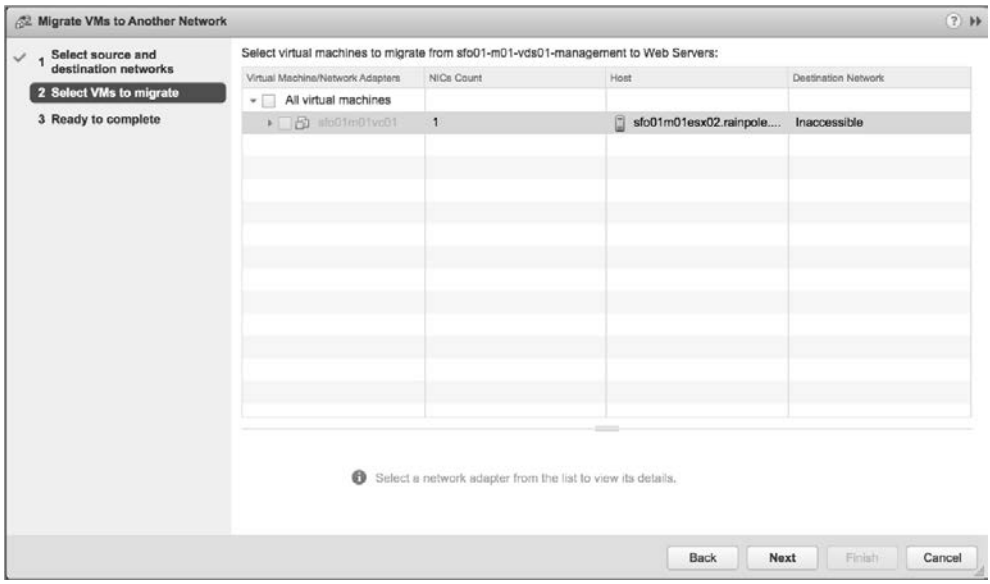
To narzędzie, dostępne w menu Actions po wybraniu przełącznika rozproszonego, przekonfiguruje wszystkie wybrane maszyny wirtualne, aby korzystały ze wskazanej sieci docelowej. Jest to o wiele łatwiejsze niż indywidualne rekonfigurowanie maszyn wirtualnych! Ponadto to narzędzie pozwala łatwo migrować maszyny wirtualne zarówno **do** przełącznika rozproszonego, jak i **z** przełącznika rozproszonego. Przejdźmy teraz przez cały proces, abyś mógł zobaczyć, jak to działa.

Aby przeprowadzić migrację maszyn wirtualnych ze standardowego przełącznika vSphere do rozproszonego przełącznika vSphere, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking*.
3. Wybierz przełącznik rozproszony z drzewa inwentarza po lewej stronie, a następnie z menu *Actions* wybierz *Migrate VMs To Another Network* (migracja maszyn wirtualnych do innej sieci). Spowoduje to uruchomienie kreatora migracji sieci maszyn wirtualnych.
4. Użyj przycisku *Browse*, aby wybrać sieć źródłową zawierającą maszyny wirtualne, które chcesz migrować. W razie potrzeby możesz użyć pól wyszukiwania *Filter* (filtruj) i *Find* (znajdź), aby ograniczyć wyniki. Po wybraniu sieci źródłowej kliknij *OK*.
5. Kliknij przycisk *Browse*, aby wybrać sieć docelową, do której chcesz przeprowadzić migrację maszyn wirtualnych. I tym razem w razie potrzeby użyj pól wyszukiwania *Filter* i *Find*, aby ułatwić sobie zlokalizowanie żądanej sieci docelowej. Po wybraniu sieci docelowej kliknij *OK*, aby wrócić do kreatora.
6. Po zakończeniu wybierania sieci źródłowej i docelowej kliknij *Next*.

7. Wygenerowana zostanie lista pasujących maszyn wirtualnych, a każda maszyna wirtualna zostanie przeanalizowana w celu ustalenia, czy sieć docelowa jest dla niej dostępna.

   Rysunek 5.62 pokazuje listę z dostępnymi i niedostępnymi sieciami docelowymi. Sieć docelowa może pojawić się jako niedostępna, jeśli host ESXi, na którym działa dana maszyna wirtualna, nie jest częścią wybranego przełącznika rozproszonego. Wybierz wirtualne maszyny, które chcesz migrować, a następnie kliknij *Next*.



RYSUNEK 5.62. Nie możesz przeprowadzić migracji maszyn wirtualnych odpowiadających wybranej przez Ciebie sieci źródłowej, jeśli sieć docelowa jest wymieniona jako niedostępna

8. Kliknij *Finish*, aby rozpocząć migrację wybranych maszyn wirtualnych z określonej sieci źródłowej do wskazanej sieci docelowej.

   W panelu *Task*s (zadania) zobaczysz uruchomione zadanie *Reconfigure Virtual Machine* (rekonfiguracja maszyny wirtualnej) dla każdej maszyny wirtualnej, której migracja ma zostać przeprowadzona.

Należy pamiętać, że to narzędzie może przeprowadzać migracje maszyn wirtualnych ze standardowego przełącznika vSphere do rozproszonego przełącznika vSphere lub odwrotnie — wystarczy określić odpowiednio sieć źródłową i docelową.

Skoro omówiliśmy już podstawy przełączników rozproszonych, przejdźmy do kilku zaawansowanych kwestii. Na pierwszy ogień weźmiemy monitorowanie sieci za pomocą NetFlow.

Korzystanie z NetFlow na rozproszonych przełącznikach vSphere

NetFlow to mechanizm efektywnego raportowania informacji o ruchu IP jako serii **przepływów ruchu** (ang. *traffic flows*). Przepływy ruchu są definiowane jako kombinacja źródłowego i docelowego adresu IP, źródłowych i docelowych portów TCP lub UDP, IP oraz typu usługi IP (ang. *Type of Service* — ToS). Urządzenia sieciowe obsługujące NetFlow będą śledzić i raportować informacje o przepływach ruchu, zwykle wysyłając je do kolektora NetFlow. Korzystając z zebranych danych, administratorzy sieci zyskują szczegółowy wgląd w rodzaje oraz ilość przepływów ruchu w sieci.

W vSphere 5.0 firma VMware wprowadziła obsługę NetFlow w rozproszonych przełącznikach vSphere (tylko w przypadku przełączników rozproszonych w wersji co najmniej 5.0.0). Dzięki temu hosty ESXi mogą gromadzić szczegółowe informacje o poszczególnych przepływach i raportować je do kolektora NetFlow.

Konfiguracja NetFlow jest procesem dwuetapowym:

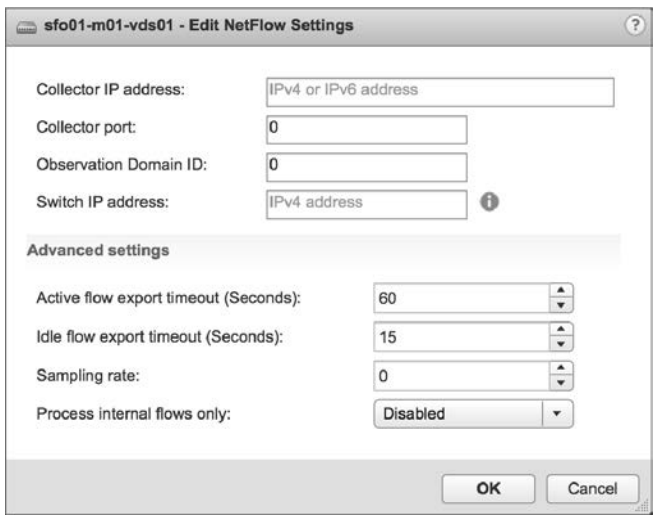
1. Skonfiguruj właściwości NetFlow na przełączniku rozproszonym.
2. Włącz lub wyłącz NetFlow (domyślnie jest wyłączony) dla poszczególnych rozproszonych grup portów.

Aby skonfigurować właściwości NetFlow dla przełącznika rozproszonego, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do listy przełączników rozproszonych i wybierz przełącznik, na którym chcesz włączyć NetFlow.
3. Po wybraniu żądanego przełącznika rozproszonego z menu *Actions* wybierz *Settings/Edit NetFlow* (ustawienia/edytowanie NetFlow).

   Spowoduje to otwarcie okna dialogowego *Edit NetFlow Settings* (edytowanie ustawień NetFlow).
4. Jak pokazano na rysunku 5.63, podaj adres IP kolektora NetFlow, port na kolektorze NetFlow oraz adres IP do identyfikacji przełącznika rozproszonego.

RYSUNEK 5.63. Aby wysyłać informacje o przepływie z przełącznika rozproszonego, potrzebujesz adresu IP i numeru portu dla kolektora NetFlow



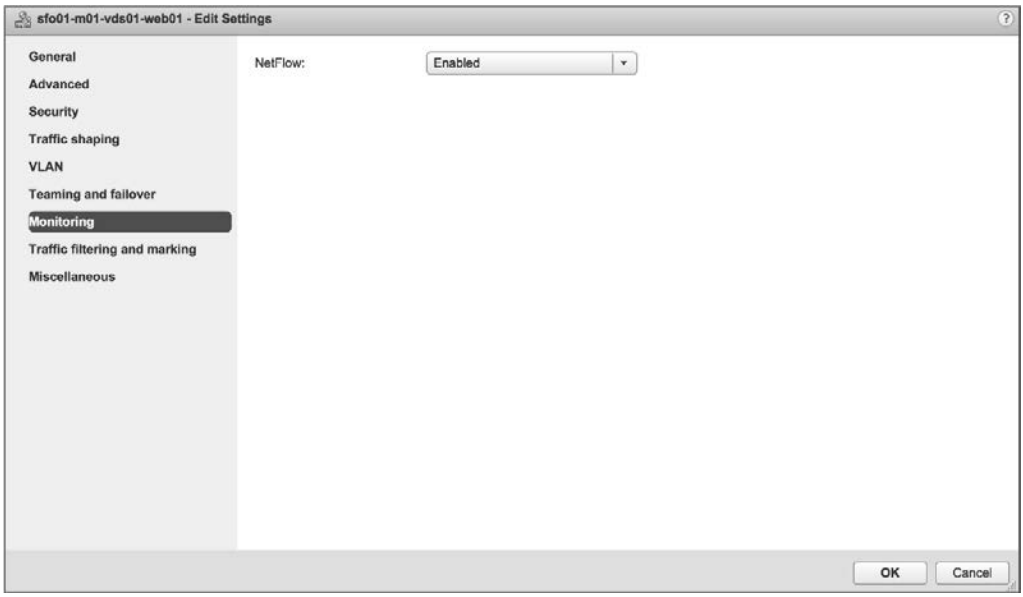
5. Możesz zmodyfikować ustawienia zaawansowane (*Advanced settings*), jeśli wymaga tego kolektor NetFlow.
6. Jeśli chcesz, aby przełącznik rozproszony przetwarzał tylko wewnętrzne przepływy ruchu, czyli ruch przepływający między maszynami wirtualnymi na tym samym hoście ESXi, ustaw *Enabled* (włączone) dla opcji *Process internal flows only*.
7. Kliknij *OK*, aby zatwierdzić zmiany i powrócić do klienta internetowego vSphere.

Gdy skonfigurujesz właściwości NetFlow dla przełącznika rozproszonego, włącz NetFlow dla poszczególnych rozproszonych grup portów. Domyślnie jest on wyłączony.

Aby włączyć NetFlow na określonej rozproszonej grupie portów, wykonaj następujące czynności:

1. W kliencie internetowym vSphere przejdź do przełącznika rozproszonego hostującego rozproszoną grupę portów, dla której chcesz włączyć NetFlow. Warunkiem wstępnym jest wykonanie najpierw poprzedniej procedury konfiguracji NetFlow na tym przełączniku rozproszonym.
2. Z menu *Actions* wybierz *Distributed Port Groups/Manage Distributed Port Groups* (rozproszone grupy portów/zarządzanie rozproszonymi grupami portów). Spowoduje to uruchomienie kreatora zarządzania rozproszonymi grupami portów. Możesz to również osiągnąć, klikając prawym przyciskiem myszy rozproszoną grupę portów i wybierając z menu kontekstowego opcję *Edit Settings* (edytowanie ustawień).
3. Zaznacz pole wyboru przy pozycji *Monitoring* (monitorowanie), a następnie kliknij *Next*.
4. W oknie *Select port groups* (wybieranie grup portów) kliknij ikonę *Select Distributed Port Groups* (wybieranie rozproszonych grup portów), wybierz rozproszone grupy portów do edycji i kliknij *OK*.

   Po wybraniu żądanych rozproszonych grup portów kliknij *Next*.
5. Na pokazanym na rysunku 5.64 ekranie *Monitoring* ustaw *NetFlow* na *Enabled* (włączone), a następnie kliknij *Next*.



RYSUNEK 5.64. Domyślnie NetFlow jest wyłączony. Włączasz go dla poszczególnych rozproszonych grup portów

6. Kliknij *Finish*, aby zapisać zmiany w rozproszonej grupie portów.

Ta rozproszona grupa portów rozpocznie przechwytywanie statystyk NetFlow i przesyłanie tych informacji do określonego kolektora NetFlow.

Kolejną przydatną w środowisku vSphere funkcjonalnością jest obsługa protokołów wykrywania przełączników, takich jak CDP (ang. *Cisco Discovery Protocol*) i LLDP (ang. *Link Layer Discovery Protocol*). W następnym punkcie zobaczymy, jak włączyć te protokoły w vSphere.

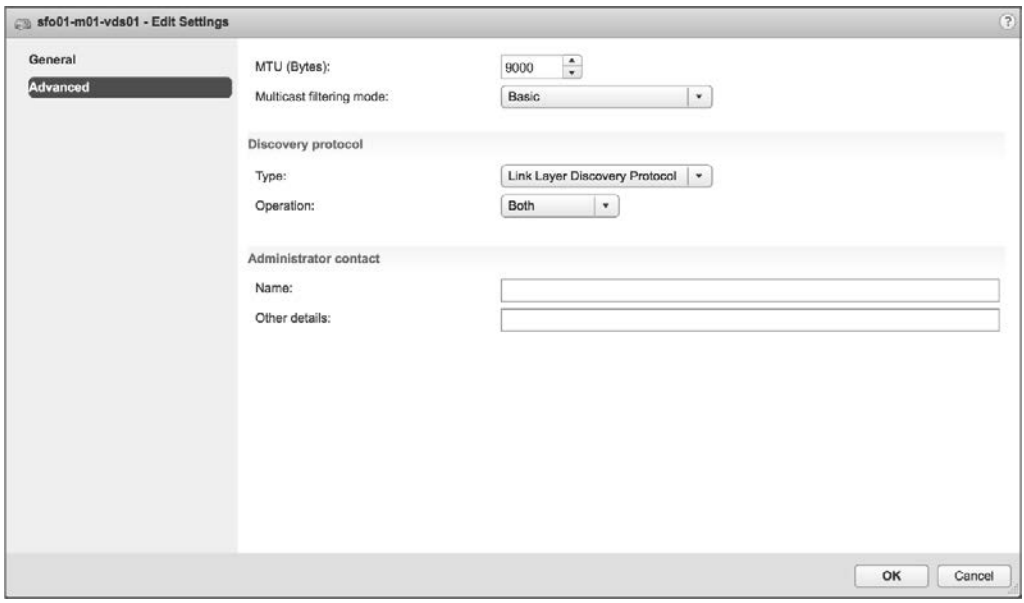
Włączanie protokołów wykrywania przełączników

Poprzednie wersje vSphere obsługiwały Cisco Discovery Protocol, który jest protokołem wymiany informacji między urządzeniami sieciowymi. Włączenie i skonfigurowanie CDP wymagało jednak użycia wiersza poleceń.

W vSphere 5.0 firma VMware dodała wsparcie dla standardowego protokołu wykrywania LLDP i zapewniła w kliencie internetowym vSphere lokalizację, w której można skonfigurować obsługę CDP/LLDP.

Aby skonfigurować obsługę wykrywania przełączników, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Po wybraniu przełącznika rozproszonego wybierz zakładkę *Configure*.
3. W obszarze *Settings* wybierz *Properties* (właściwości).
4. Kliknij przycisk *Edit*, a następnie w oknie dialogowym *Edit Settings* wybierz opcję *Advanced* (zaawansowane), aby skonfigurować przełącznik rozproszony do obsługi CDP lub LLDP, jak pokazano na rysunku 5.65.



RYSUNEK 5.65. Obsługa LLDP pozwala przełącznikom rozproszonym wymieniać przez sieć informacje o wykrywaniu z innymi obsługującymi LLDP urządzeniami

Ten rysunek pokazuje przełącznik rozproszony skonfigurowany do obsługi LLDP z ustawioną opcją *Operation* na *Both*, czyli nasłuchujący (odbierający informacje LLDP z innych podłączonych urządzeń) i rozgłaszający (wysyłający informacje LLDP do innych podłączonych urządzeń).

5. Kliknij *OK*, aby zapisać zmiany.

Gdy hosty ESXi będące członkami tego przełącznika rozproszonego zaczną wymieniać informacje o wykrywaniu, będziesz mógł przeglądać te informacje z poziomu przełączników fizycznych. W większości przełączników Cisco informacje o urządzeniach sieciowych z włączoną obsługą CDP, w tym hostach ESXi, wyświetla na przykład polecenie `show cdp neighbor`. Wpisy dotyczące hostów ESXi będą zawierać informacje na temat używanej fizycznej karty sieciowej i używanego przełącznika wirtualnego.

Przełączniki standardowe vSphere obsługują tylko protokół CDP (nie mają wsparcia dla LLDP), ale nie zapewniają GUI do jego skonfigurowania. Musisz użyć polecenia `esxcli`. Poniższe polecenie konfiguruje CDP na przełączniku wirtualnym do nasłuchiwania i rozgłaszania:

```
esxcli network vswitch standard set --cdp-status=both --vswitch-name=vSwitch0
```

Włączanie rozszerzonych funkcji multicastowych

Oprócz podstawowego filtrowania multicastowego obsługiwanego przez standardowy przełącznik vSphere, rozproszony przełącznik vSphere obsługuje również snooping multicastowy.

W tym trybie przełącznik rozproszony uczy o przynależności maszyny wirtualnej dynamicznie. Osiąga się to poprzez monitorowanie ruchu maszyn wirtualnych i przechwytywanie komunikatów IGMP lub MLD (ang. *Multicast Listener Discovery*), gdy maszyna wirtualna wysyła pakiety zawierające te informacje. Przełącznik rozproszony tworzy następnie rekord docelowego adresu IP grupy, a dla IGMPv3 rejestruje również źródłowy adres IP, z którego maszyna wirtualna „preferuje" odbierać ruch. Przełącznik rozproszony usuwa wpis zawierający informacje o grupie, jeśli maszyna wirtualna nie odnowi swojego członkostwa w określonym przedziale czasu.

TRZYMANIE SIĘ STANDARDÓW

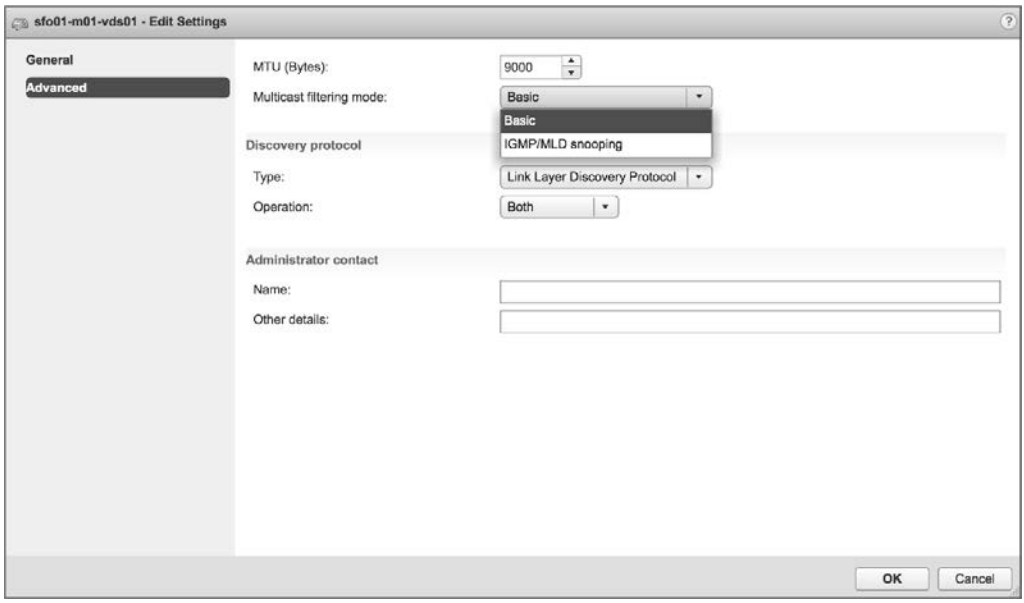
Snooping multicastowy w vSphere 6 został zaimplementowany zgodnie z dokumentem RFC 4541 i obsługuje IGMPv1, IGMPv2 oraz IGMPv3 dla grup multicastowych IPv4, a także MLDv1 i MLDv2 dla grup multicastowych IPv6.

Aby włączyć snooping multicastowy na przełączniku rozproszonym vSphere, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking*.
3. Wybierz istniejący przełącznik rozproszony, kliknij go prawym przyciskiem myszy i wybierz *Settings/Edit Settings*.
4. W wyświetlonym oknie dialogowym wybierz *Advanced*, a następnie zmień tryb filtrowania multicastowego na *IGMP/MLD snooping*, jak pokazano na rysunku 5.66.

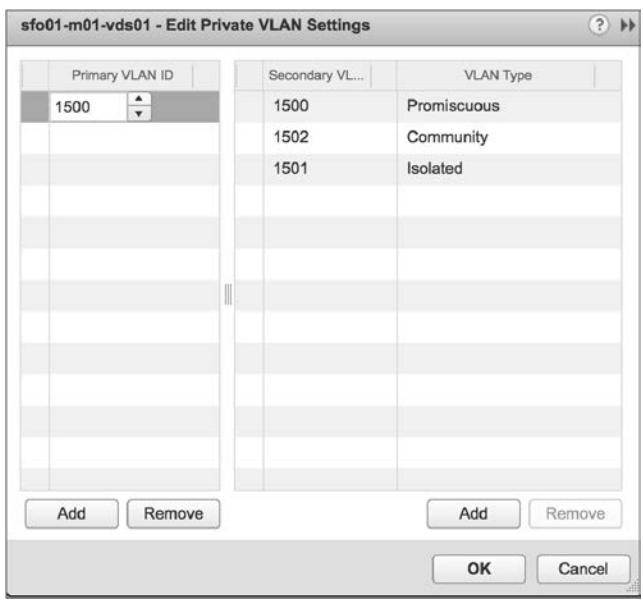
Konfigurowanie VLAN-ów prywatnych

VLAN-y prywatne (ang. *Private VLAN* — PVLAN) to zaawansowana funkcja sieciowa vSphere oparta na funkcjonalności przełączników rozproszonych. W środowisku vSphere PVLAN-y są dostępne tylko z przełącznikami rozproszonymi i nie działają z przełącznikami standardowymi. Ponadto musisz upewnić się, że PVLAN-y są również obsługiwane przez fizyczne przełączniki upstreamowe, do których podłączone jest Twoje środowisko vSphere.



RYSUNEK 5.66. Przełącznik rozproszony vSphere obsługuje zarówno podstawowe filtrowanie multicastowe, jak i snooping IGMP/MLD

Oto krótki przegląd prywatnych VLAN-ów. PVLAN-y to sposób na dalszą izolację portów w danym VLAN-ie. Weźmy na przykład scenariusz hostów w strefie zdemilitaryzowanej (ang. *demilitarized zone* — DMZ). Hosty w strefie DMZ rzadko muszą komunikować się między sobą, ale z wielu powodów używanie VLAN-u dla każdego hosta szybko staje się nieporęczne. Korzystanie z PVLAN-ów pozwala odizolować hosty od siebie nawzajem, jednocześnie utrzymując je w tej samej podsieci IP. Rysunek 5.67 ilustruje sposób działania PVLAN-ów.



RYSUNEK 5.67. Wpisy dla VLAN-ów prywatnych składają się z wpisu dla VLAN-u podstawowego (Primary VLAN) i co najmniej jednego wpisu dla VLAN-ów dodatkowych (Secondary VLAN)

PVLAN-y są konfigurowane parami: VLAN podstawowy i któryś z VLAN-ów dodatkowych. VLAN podstawowy jest uważany za **downstreamowy**, co oznacza, że po nim płynie ruch skierowany do hosta. VLAN dodatkowy jest uważany za **upstreamowy**, co oznacza, że po nim płynie ruch z hosta.

Aby użyć PVLAN-ów, najpierw skonfiguruj je na fizycznych przełącznikach łączących się z hostami ESXi, a następnie dodaj wpisy PVLAN-ów do przełącznika rozproszonego na serwerze vCenter.

Aby zdefiniować wpisy PVLAN-ów na przełączniku rozproszonym, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking*.
3. Wybierz istniejący przełącznik rozproszony i kliknij zakładkę *Configure*.
4. Wybierz *Private VLAN*, a następnie kliknij przycisk *Edit*.
5. W oknie dialogowym *Edit Private VLAN Settings* (edytowanie ustawień VLAN-ów prywatnych) kliknij *Add*, aby dodać identyfikator VLAN-u podstawowego do listy widocznej po lewej stronie.
6. Dla każdego identyfikatora VLAN-u podstawowego na liście po lewej stronie dodaj co najmniej jeden VLAN dodatkowy do listy po prawej stronie, jak pokazano wcześniej na rysunku 5.67.

   VLAN-ny dodatkowe są klasyfikowane jako jeden z dwóch następujących typów:

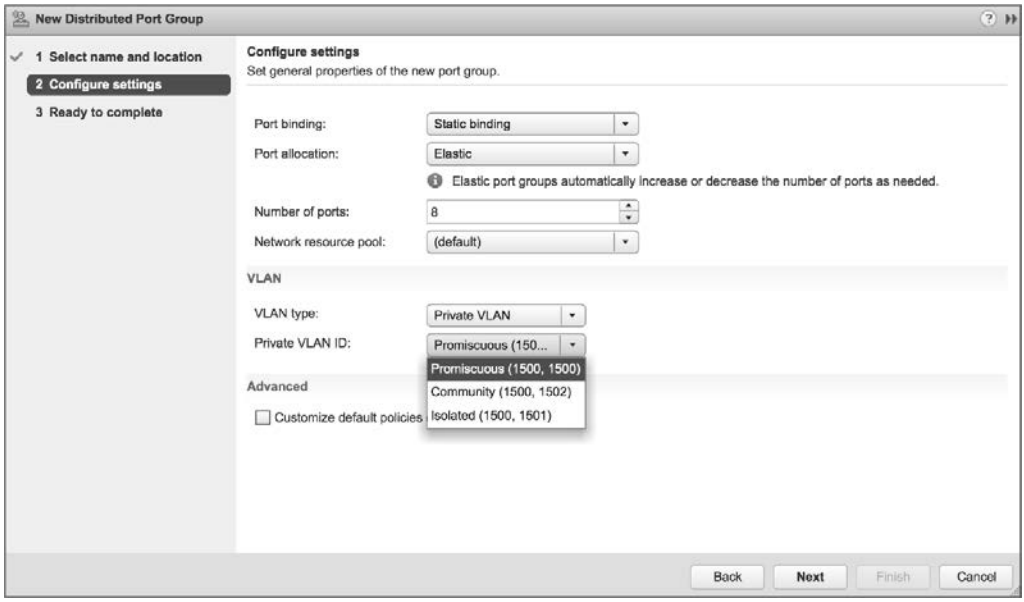
   - Izolowane (ang. *isolated*) — porty umieszczone w PVLAN-ach dodatkowych skonfigurowanych jako izolowane mogą komunikować się tylko z portami mieszanymi (ang. *promiscuous ports*) w tym samym VLAN-ie dodatkowym. (Porty mieszane omówimy w dalszej części tego rozdziału).
   - Wspólnotowe (ang. *community*) — porty w PVLAN-ie dodatkowym mogą komunikować się z innymi portami w tym samym PVLAN-ie dodatkowym oraz z portami mieszanymi.

   Dla każdego VLAN-u podstawowego dozwolony jest tylko jeden izolowany VLAN dodatkowy, natomiast dozwolonych jest wiele VLAN-ów dodatkowych skonfigurowanych jako wspólnotowe.
7. Gdy skończysz dodawanie wszystkich par PVLAN-ów, kliknij *OK*, aby zapisać zmiany i wrócić do klienta internetowego vSphere.

Po wprowadzeniu identyfikatorów PVLAN-ów dla przełącznika rozproszonego należy utworzyć rozproszoną grupę portów korzystającą z konfiguracji PVLAN-ów. Proces tworzenia rozproszonej grupy portów został opisany wcześniej. Rysunek 5.68 pokazuje kreator nowej rozproszonej grupy portów dla grupy, która wykorzystuje PVLAN-y.

Na rysunku 5.68 ponownie widać termin *promiscuous*, oznaczający port mieszany. W języku PVLAN-ów port mieszany może wysyłać i odbierać ramki warstwy drugiej z dowolnego innego portu w VLAN-ie. Ten typ portu jest zwykle zarezerwowany dla bramy domyślnej dla podsieci IP, na przykład routera warstwy trzeciej.

PVLAN-y to potężne narzędzie konfiguracyjne, ale także złożony i potencjalnie trudny do zrozumienia temat, nie mówiąc już o rozwiązywaniu problemów z komunikacją. Dodatkowe informacje na temat PVLAN-ów znajdziesz w artykule z bazy wiedzy VMware na stronie *https://kb.vmware.com/s/article/1010691*.



RYSUNEK 5.68. Gdy tworzona jest rozproszona grupa portów z PVLAN-ami, zostaje ona powiązana zarówno z identyfikatorem VLAN-u podstawowego, jak i dodatkowego

Podobnie jak standardowe przełączniki vSphere, również rozproszone przełączniki vSphere zapewniają ogromną elastyczność w projektowaniu i konfigurowaniu sieci wirtualnej. Jak zawsze, istnieją jednak ograniczenia tej elastyczności. Tabela 5.2 przedstawia niektóre konfiguracyjne wartości maksymalne dla przełączników rozproszonych vSphere.

TABELA 5.2. Wartości maksymalne dla konfiguracji komponentów sieciowych ESXi (dla rozproszonych przełączników vSphere)

Element konfiguracji	Maksimum
Liczba przełączników na serwer vCenter	128
Liczba portów na host (przełącznik standardowy/rozproszony)	4096
Liczba portów przełącznika rozproszonego na instancję serwera vCenter	60 000
Liczba hostów ESXi na przełącznik rozproszony	2000
Liczba statycznych grup portów na instancję serwera vCenter	10 000
Liczba efemerycznych grup portów na instancję serwera vCenter	1016

Konfigurowanie LACP

LACP (ang. *Link Aggregation Control Protocol*) to znormalizowany protokół do obsługi agregacji, czyli łączenia wielu łączy sieciowych w pojedyncze logiczne łącze sieciowe. Zwróć uwagę, że obsługa LACP jest dostępna tylko wtedy, gdy korzystasz z rozproszonego przełącznika vSphere. Standardowe przełączniki vSphere nie obsługują LACP.

CZY LACP TO JEDYNY SPOSÓB?

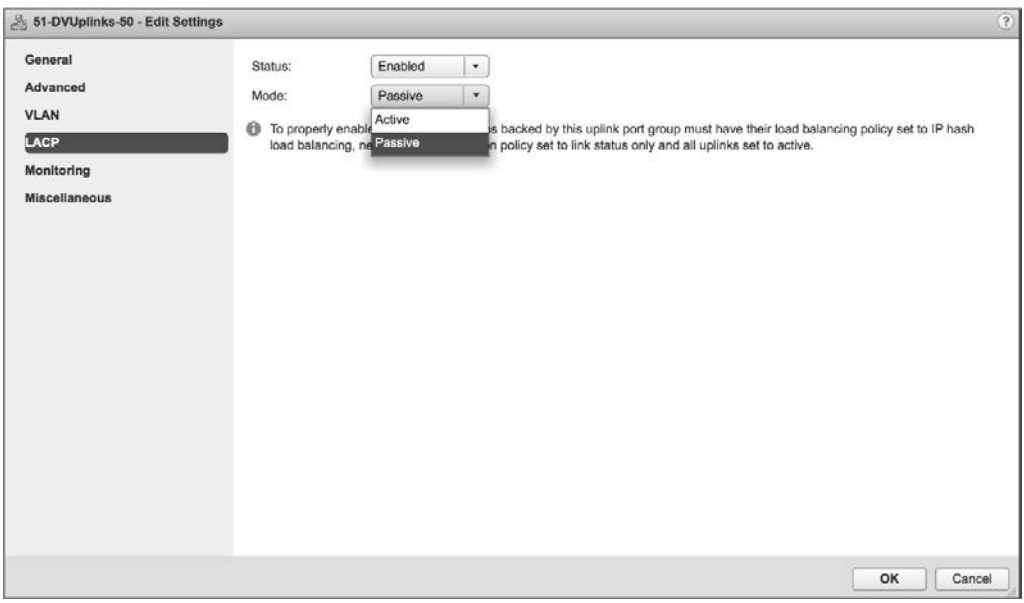
Stosowanie agregacji łączy bez LACP jest możliwe. Gdy używasz standardowego lub rozproszonego przełącznika vSphere, agregację łączy umożliwia ustawienie dla grup kart sieciowych reguły *Route Based on IP Hash*, czyli opartej na skrótach IP. Mimo że ta konfiguracja zapewnia agregację łączy, nie korzysta z protokołu LACP. Jest to jedyny sposób użycia agregacji łączy ze standardowym przełącznikiem vSphere.

Zaczniemy od przeglądu sposobu konfigurowania podstawowej obsługi LACP na rozproszonym przełączniku vSphere w wersji 5.1.0. Następnie pokażemy Ci, jak ulepszono obsługę LACP w vSphere 5.5 i w nowszych wersjach.

Jeśli używasz rozproszonego przełącznika vSphere w wersji 5.1.0, musisz skonfigurować następujące cztery elementy:

- Włączyć LACP we właściwościach dla grupy uplinków przełącznika rozproszonego.
- Ustawić dla wszystkich rozproszonych grup portów regułę grup kart sieciowych *Route Based On IP Hash*.
- Ustawić dla wszystkich rozproszonych grup portów regułę wykrywania sieci tylko na podstawie stanu łącza.
- Skonfigurować wszystkie rozproszone grupy portów w taki sposób, aby wszystkie uplinki były aktywne, a nie rezerwowe lub nieużywane.

Rysunek 5.69 pokazuje okno dialogowe Edit Settings dla grupy uplinków na rozproszonym przełączniku vSphere w wersji 5.1.0. Możesz zobaczyć tutaj ustawienie włączające LACP oraz pozostałe wymagane ustawienia.



RYSUNEK 5.69. Podstawowa obsługa LACP w wersji 5.1.0 rozproszonego przełącznika vSphere jest włączana w grupie uplinków, ale wymaga również innych ustawień

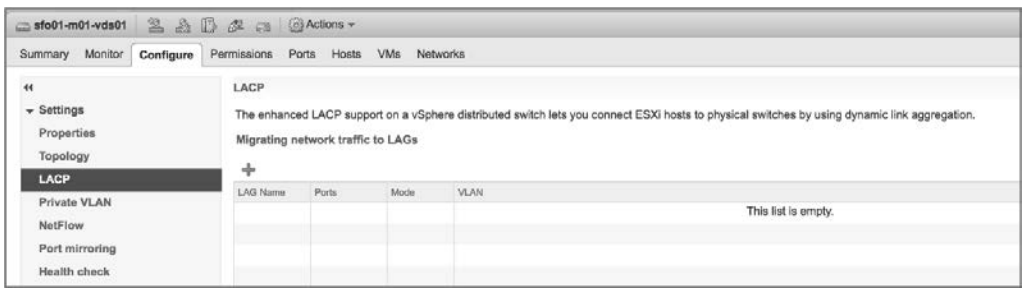
Musisz skonfigurować LACP na fizycznym przełączniku, do którego podłączony jest host ESXi. Dokładny sposób włączania LACP będzie różnił się w zależności od producenta sprzętu. Ustawienie trybu (*Mode*) pokazane na rysunku 5.69, które może być aktywne (*Active*) lub pasywne (*Passive*), pomaga zdefiniować sposób komunikowania się hosta ESXi z przełącznikiem fizycznym w celu ustanowienia agregacji łączy:

- Gdy ustawiony jest pasywny tryb LACP, host ESXi nie inicjuje żadnej komunikacji z przełącznikiem fizycznym. To przełącznik musi zainicjować negocjacje.
- Gdy ustawiony jest aktywny tryb LACP, host ESXi aktywnie inicjuje negocjacje agregacji łączy z przełącznikiem fizycznym.

Z tego, co do tej pory napisaliśmy na temat korzystania z LACP w wersji 5.1.0 rozproszonego przełącznika vSphere, możesz prawdopodobnie wywnioskować, że obsługiwana jest tylko jedna grupa zagregowanych łączy (pojedynczy pakiet łączy wynegocjowany przez LACP), a LACP włącza się lub wyłącza dla całego rozproszonego przełącznika vSphere.

Jeśli jednak zaktualizujesz rozproszony przełącznik vSphere do wersji 5.5.0 lub 6.0.0, otrzymasz ulepszoną obsługę LACP, która eliminuje te ograniczenia. Od wersji 5.5.0 przełączniki rozproszone obsługują wiele grup LACP, a sposób używania (lub nieużywania) tych grup można skonfigurować dla poszczególnych rozproszonych grup portów. Rzućmy okiem na sposób konfiguracji obsługi LACP na przełączniku rozproszonym w wersji 6.6.

Od wersji 5.5.0 przełącznika rozproszonego w obszarze *Settings* w zakładce *Configure* pojawia się nowa sekcja *LACP*, pokazana na rysunku 5.70. W tej sekcji możesz zdefiniować co najmniej jedną grupę agregacji łączy (ang. *link aggregation group* — LAG), a każda skonfigurowana grupa pojawi się jako logiczny uplink do rozproszonych grup portów na tym przełączniku rozproszonym. Od wersji 5.5 vSphere obsługuje wiele grup LAG na pojedynczym przełączniku rozproszonym, co pozwala administratorom zapewnić więcej niż jeden interfejs sieciowy dla przełączników rozproszonych (czyli podłączyć przełączniki rozproszone do wielu fizycznych przełączników upstreamowych) i nadal korzystać z LACP. Istnieje kilka ograniczeń, które zostaną omówione na końcu tego punktu rozdziału.



RYSUNEK 5.70. Ulepszona obsługa LACP wprowadzona w wersji 5.5 vSphere eliminuje wiele z ograniczeń wersji 5.1

Aby użyć LACP z przełącznikiem rozproszonym w wersji 5.5.0 lub nowszej, musisz wykonać trzy czynności:

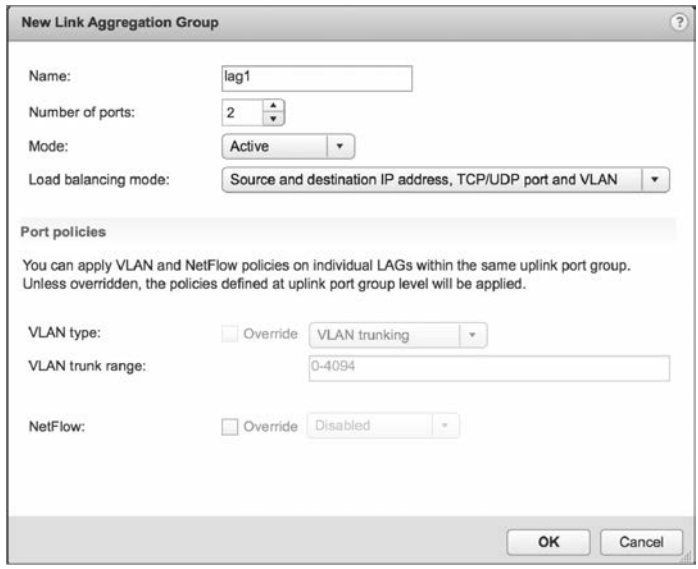
1. Zdefiniuj co najmniej jedną grupę LAG w sekcji *LACP* w obszarze *Settings* zakładki *Configure*.
2. Dodaj fizyczne karty sieciowe do utworzonych grup LAG.
3. W konfiguracji grup kart sieciowych i przełączania awaryjnego dla rozproszonych grup portów zmodyfikuj rozproszone grupy portów, aby używały tych grup LAG jako uplinków.

Przyjrzyjmy się każdej z tych czynności szczegółowo.

Aby utworzyć grupę LAG, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do przełącznika rozproszonego, dla którego chcesz skonfigurować grupę agregacji łączy LACP.
3. Po wybraniu przełącznika rozproszonego kliknij zakładkę *Configure*, a następnie kliknij *LACP*. Spowoduje to wyświetlenie ekranu pokazanego wcześniej na rysunku 5.70.
4. Aby dodać grupę LAG, kliknij zielony znak plus. Spowoduje to wyświetlenie okna dialogowego *New Link Aggregation Group* (nowa grupa agregacji łączy), pokazanego na rysunku 5.71.

RYSUNEK 5.71. Od wersji 5.5.0 przełącznika rozproszonego właściwości LACP są konfigurowane dla poszczególnych grup LAG, a nie dla całego przełącznika rozproszonego

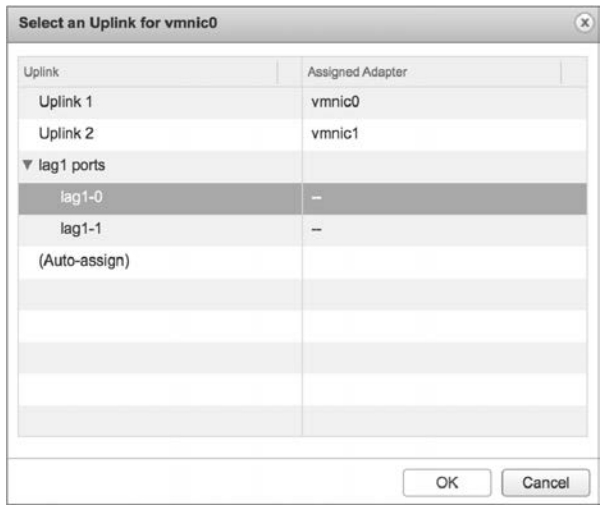


5. W oknie dialogowym *New Link Aggregation Group* podaj nazwę dla nowej grupy LAG.
6. Określ liczbę fizycznych portów, które będą uwzględnione w grupie LAG.
7. Określ tryb LACP (aktywny lub pasywny, jak opisaliśmy wcześniej), którego powinna używać ta grupa LAG.
8. Wybierz tryb równoważenia obciążenia. Zwróć uwagę, że ten tryb równoważenia obciążenia wpływa tylko na ruch wychodzący. Ruch przychodzący będzie równoważony pod względem obciążenia zgodnie z trybem równoważenia obciążenia skonfigurowanym na przełączniku fizycznym. (Aby uzyskać najlepsze wyniki i ułatwić rozwiązywanie problemów, w miarę możliwości ta konfiguracja powinna odpowiadać konfiguracji przełącznika fizycznego).
9. Jeśli musisz nadpisać reguły portów dla tej grupy LAG, możesz to zrobić na dole tego okna dialogowego.
10. Kliknij *OK*, aby utworzyć nową grupę LAG i powrócić do obszaru LACP klienta internetowego vSphere.

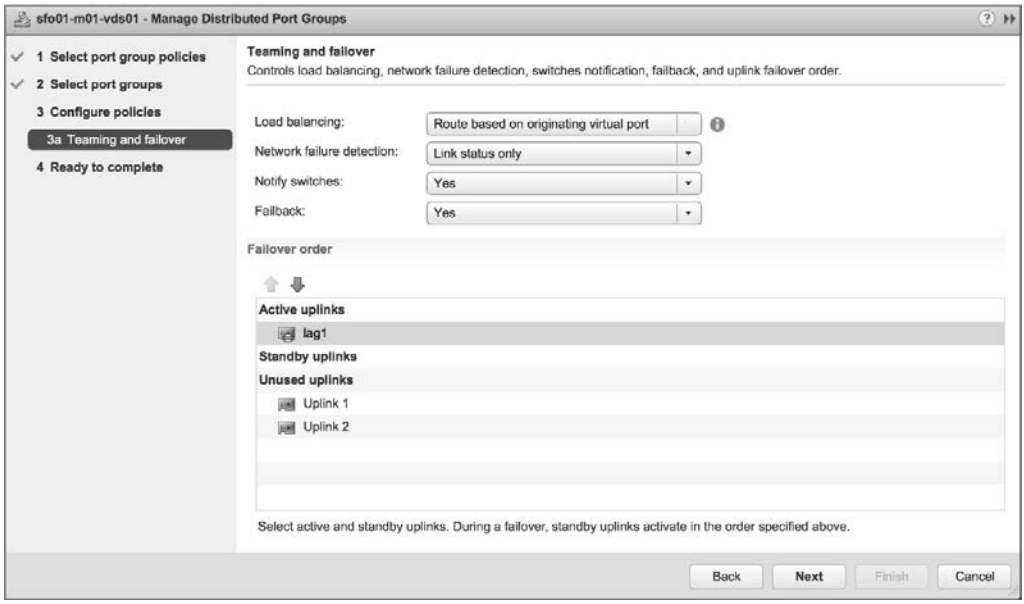
Skoro utworzyłeś już co najmniej jedną grupę LAG, musisz przypisać do niej fizyczne karty sieciowe. W tym celu musisz zastosować opisaną wcześniej procedurę zarządzania fizycznymi kartami sieciowymi (szczegółowe informacje na ten temat znajdziesz w punkcie „Zarządzanie kartami sieciowymi VMkernel"). Jedyna zmiana, którą zauważysz, polega na tym, że kiedy klikniesz

link *Assign Uplink* (przypisz uplink) dla wybranej fizycznej karty sieciowej, teraz zobaczysz opcję przypisania tej karty sieciowej do jednego z dostępnych portów uplinkowych z utworzonej przez Ciebie grupy (lub grup) LAG. Rysunek 5.72 pokazuje okno dialogowe do przypisywania uplinku dla przełącznika rozproszonego z dwiema grupami LAG.

RYSUNEK 5.72. Gdy grupa LAG zostanie utworzona, można dodać do niej fizyczne karty sieciowe



Po dodaniu fizycznych kart sieciowych do grupy (lub grup) LAG możesz przejść do ostatniego kroku: konfigurowania grupy (lub grup) LAG jako uplinków dla rozproszonych grup portów na tym przełączniku rozproszonym. Szczegółowe instrukcje dotyczące tego procesu podaliśmy wcześniej w podpunkcie „Edytowanie rozproszonej grupy portów". Zwróć uwagę, że grupy LAG pojawią się jako fizyczne uplinki w konfiguracji grup kart sieciowych i przełączania awaryjnego, jak widać na rysunku 5.73. Grupę LAG możesz przypisać jako aktywny, rezerwowy lub nieużywany uplink.



RYSUNEK 5.73. Grupy LAG pojawiają się jako fizyczne uplinki do rozproszonych grup portów

Korzystając z grup LAG, należy pamiętać o następujących ograniczeniach:

- Niektórych funkcjonalności vSphere, takich jak profile hostów, mirroring portów, sprawdzanie kondycji grup kart sieciowych i kolektor Netdump, nie można używać z grupami LAG. Więcej informacji na ten temat znajdziesz w bazie wiedzy VMware w artykule 2051307.
- Korzystając z grup LAG na przełączniku rozproszonym, tracisz korzyści wynikające ze stosowania algorytmu równoważenia obciążenia grup kart sieciowych opartego na obciążeniu fizycznych kart sieciowych.
- Nie można łączyć grup LAG i fizycznych uplinków dla danej rozproszonej grupy portów. Wszelkie fizyczne uplinki muszą być ustawione jako nieużywane karty sieciowe.
- Nie można używać wielu aktywnych grup LAG na pojedynczej rozproszonej grupie portów. Jedną grupę LAG umieść na liście aktywnych uplinków, a pozostałe grupy LAG na liście nieużywanych uplinków.
- VMware obsługuje tylko grupy LAG podłączone do tego samego przełącznika fizycznego lub stosu przełączników. W połączeniu z poprzednim punktem możesz zauważyć, że do momentu awarii przełącznika lub grupy LAG ruch może korzystać tylko z jednego przełącznika fizycznego. Więcej informacji na ten temat znajdziesz w bazie wiedzy VMware w artykule 1001938.

Zwróć uwagę, że niektóre z tych ograniczeń dotyczą poszczególnych rozproszonych grup portów. Z innymi rozproszonymi grupami portów możesz użyć innych aktywnych grup LAG lub autonomicznych uplinków, ponieważ konfiguracja grup kart sieciowych i przełączania awaryjnego jest ustawiana dla poszczególnych rozproszonych grup portów.

KORZYSTAJĄC Z GRUP LAG, NALEŻY ZIGNOROWAĆ USTAWIENIE RÓWNOWAŻENIA OBCIĄŻENIA

Gdy korzystasz z protokołu LACP i grup LAG z przełącznikiem rozproszonym w wersji 5.5 lub nowszej, możesz zignorować ustawienie równoważenia obciążenia (*Load balancing*) widoczne na rysunku 5.73. Jest ono nadpisywane przez regułę równoważenia obciążenia ustawianą dla grup LAG.

Konfigurowanie zabezpieczeń przełącznika wirtualnego

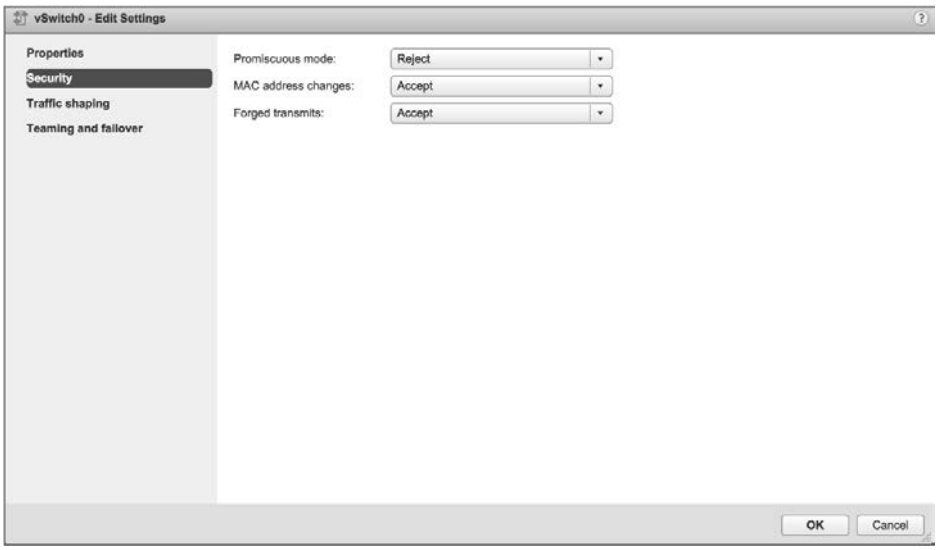
Chociaż przełączniki wirtualne i przełączniki rozproszone są uważane za „przełączniki niezarządzalne", możesz skonfigurować dla nich reguły bezpieczeństwa, aby zwiększyć lub zapewnić bezpieczeństwo w warstwie drugiej. W przypadku standardowych przełączników vSphere reguły bezpieczeństwa można zastosować na poziomie przełącznika lub grupy portów. Dla rozproszonych przełączników vSphere reguły bezpieczeństwa stosuje się tylko na poziomie rozproszonych grup portów. Ustawienia bezpieczeństwa obejmują następujące trzy opcje:

- tryb mieszany,
- zmiany adresów MAC,
- sfałszowane transmisje.

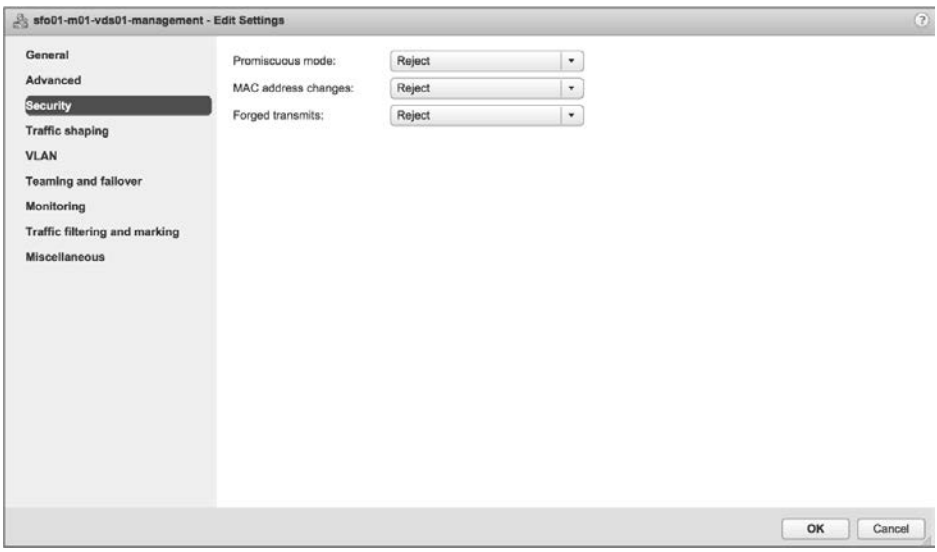
Zastosowanie zasad bezpieczeństwa do przełącznika wirtualnego jest domyślnie skuteczne dla wszystkich typów połączeń na tym przełączniku. Jeśli jednak na tym przełączniku wirtualnym jakaś grupa portów zostanie skonfigurowana z rywalizującą regułą bezpieczeństwa, nadpisze ona regułę ustawioną dla przełącznika. Jeżeli przełącznik wirtualny zostanie na przykład skonfigurowany z regułą bezpieczeństwa, która odrzuca zmiany adresów MAC, ale grupa portów na tym przełączniku zostanie

skonfigurowana do akceptowania zmian adresów MAC, wtedy każda maszyna wirtualna podłączona do tej grupy portów będzie mogła się komunikować, nawet jeśli będzie używać adresu MAC, który różni się od adresu skonfigurowanego w jej pliku *VMX*.

Pokazana na rysunku 5.74 domyślna reguła bezpieczeństwa dla przełącznika wirtualnego jest ustawiona na odrzucanie (*Reject*) trybu mieszanego (*Promiscuous mode*) oraz akceptowanie (*Accept*) zmian adresów MAC (*MAC address changes*) i sfałszowanych transmisji (*Forged transmits*). Rysunek 5.75 pokazuje natomiast domyślną regułę bezpieczeństwa dla rozproszonej grupy portów na przełączniku rozproszonym.



RYSUNEK 5.74. Domyślny profil bezpieczeństwa dla przełącznika standardowego nie dopuszcza trybu mieszanego, zezwala na zmiany adresów MAC i sfałszowane transmisje



RYSUNEK 5.75. Domyślny profil bezpieczeństwa dla rozproszonej grupy portów na przełączniku rozproszonym nie dopuszcza również zmian adresów MAC i sfałszowanych transmisji

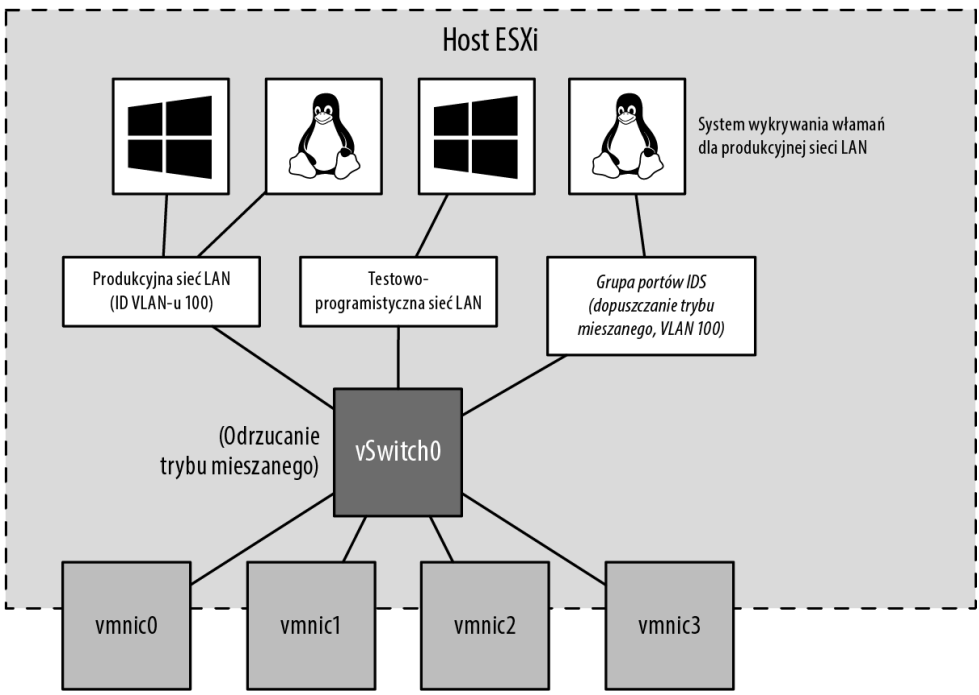
Każdą z tych opcji zabezpieczeń omówimy szczegółowo w kolejnych punktach.

Korzystanie z trybu mieszanego

Opcja trybu mieszanego jest domyślnie ustawiona na odrzucanie, aby uniemożliwić wirtualnym kartom sieciowym obserwowanie ruchu przesyłanego poprzez przełącznik wirtualny lub przełącznik rozproszony. Dla zapewnienia zwiększonego bezpieczeństwo nie jest zalecane dopuszczanie trybu mieszanego, ponieważ nie jest to bezpieczny tryb działania, który umożliwia wirtualnym kartom sieciowym uzyskiwanie dostępu do ruchu innego niż ich własny. Pomimo względów bezpieczeństwa istnieją ważne powody, aby zezwolić przełącznikowi na działanie w trybie mieszanym. Przykładem może być system wykrywania włamań (ang. *intrusion-detection system* — IDS), który musi być w stanie identyfikować cały ruch w celu wykrywania anomalii i złośliwych wzorców ruchu.

Wcześniej w tym rozdziale pisaliśmy o tym, że grupy portów i VLAN-y nie mają relacji „jeden do jednego" i może dojść do sytuacji, w których będziesz miał na przełączniku standardowym lub rozproszonym wiele grup portów skonfigurowanych z tym samym identyfikatorem VLAN-u. To jest dokładnie jedna z tych sytuacji — potrzebujesz, żeby pewien system, w tym przypadku IDS, widział ruch przeznaczony dla innych wirtualnych kart sieciowych. Zamiast przyznawać te uprawnienia wszystkim systemom w grupie portów, możesz utworzyć dedykowaną grupę portów tylko dla systemu IDS. Będzie ona miała ten sam identyfikator VLAN i te same inne ustawienia, ale będzie dopuszczać tryb mieszany zamiast go odrzucać. Pozwala to administratorowi starannie kontrolować, które systemy będą mogły korzystać z tej potężnej i potencjalnie zagrażającej bezpieczeństwu funkcjonalności.

Jak pokazano na rysunku 5.76, reguła bezpieczeństwa przełącznika wirtualnego pozostanie na domyślnym poziomie odrzucania trybu mieszanego, podczas gdy grupa portów maszyn wirtualnych dla systemu IDS będzie akceptować ten tryb. To ustawienie nadpisze przełącznik wirtualny, umożliwiając systemowi IDS monitorowanie całego ruchu dla tego VLAN-u.

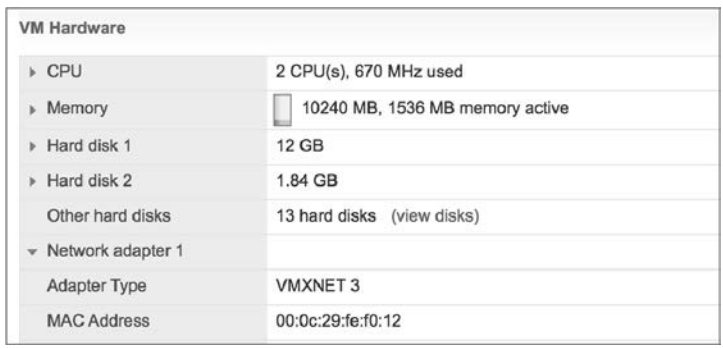


RYSUNEK 5.76. Chociaż tryb mieszany zmniejsza bezpieczeństwo, jest wymagany podczas korzystania z systemu wykrywania włamań

Zezwalanie na zmiany adresów MAC i sfałszowane transmisje

Gdy tworzona jest maszyna wirtualna z co najmniej jedną wirtualną kartą sieciową, dla każdej wirtualnej karty generowany jest adres MAC. Tak samo jak Intel, Broadcom i inni producenci kart sieciowych, którzy wyposażają je w unikatowe adresy MAC, również firma VMware jest producentem kart sieciowych posiadającym swój własny prefiks MAC, aby zapewnić unikatowość. Oczywiście VMware w rzeczywistości niczego nie produkuje, ponieważ produkt istnieje jako wirtualna karta sieciowa na maszynie wirtualnej. 6-bajtowe losowo generowane adresy MAC dla maszyny wirtualnej możesz zobaczyć w jej pliku konfiguracyjnym (*VMX*) oraz w pokazanym na rysunku 5.77 obszarze *Settings* (ustawienia) dla maszyny wirtualnej w kliencie internetowym vSphere. Adres MAC przypisany do VMware zaczyna się od prefiksu 00:50:56 lub 00:0C:29. Piąty i szósty zestaw (YY:ZZ) są generowane losowo na podstawie unikatowego identyfikatora uniwersalnego (ang. *universally unique identifier* — UUID) maszyny wirtualnej powiązanego z jej lokalizacją. Z tego powodu po zmianie lokalizacji maszyny wirtualnej przed jej uruchomieniem wyświetlane jest zapytanie o zachowanie UUID lub wygenerowanie nowego, co pomaga zapobiegać konfliktom adresów MAC.

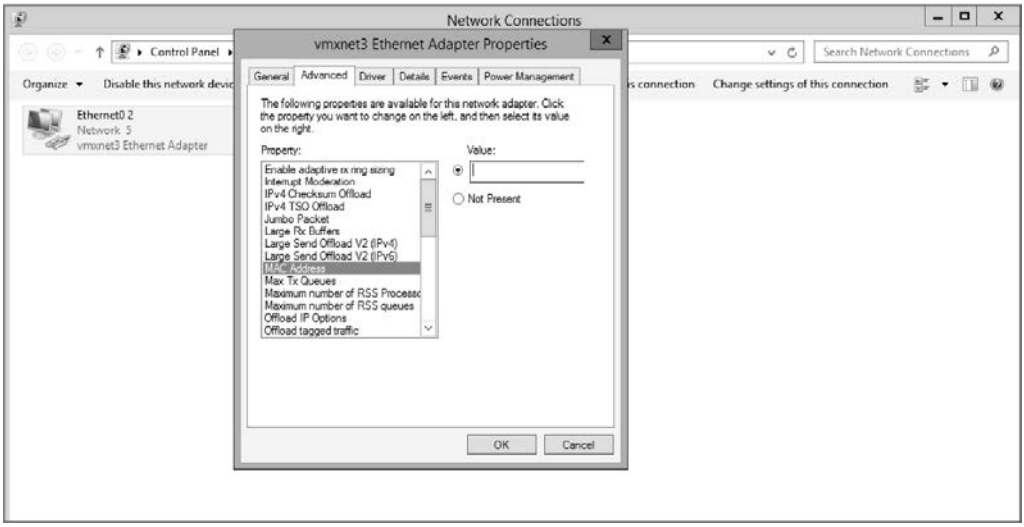
RYSUNEK 5.77. Początkowy adres MAC maszyny wirtualnej jest generowany automatycznie i umieszczany w jej pliku konfiguracyjnym oraz wyświetlany w kliencie internetowym vSphere



RĘCZNE USTAWIANIE ADRESU MAC

Ręczne skonfigurowanie adresu MAC w pliku konfiguracyjnym maszyny wirtualnej nie zadziała, jeśli pierwsze trzy bajty nie będą prefiksami dostarczanymi przez VMware, a ostatnie trzy bajty nie będą unikatowe. Jeżeli w pliku konfiguracyjnym zostanie wprowadzony prefiks MAC inny niż prefiks VMware, maszyna wirtualna nie włączy się.

Wszystkie maszyny wirtualne mają dwa adresy MAC: początkowy i efektywny. Początkowy adres MAC to adres MAC omówiony w poprzednim akapicie, który jest generowany automatycznie i znajduje się w pliku konfiguracyjnym. System operacyjny gościa nie ma kontroli nad początkowym adresem MAC. Efektywny adres MAC to adres MAC skonfigurowany przez system operacyjny gościa, który jest używany podczas komunikacji z innymi systemami. Efektywny adres MAC jest umieszczany w komunikacji sieciowej jako źródłowy adres MAC maszyny wirtualnej. Domyślnie te dwa adresy są identyczne. Aby dla systemu operacyjnego gościa wyegzekwować adres MAC nieprzypisany przez VMware, zmień efektywny adres MAC z poziomu systemu operacyjnego gościa, jak pokazano na rysunku 5.78.

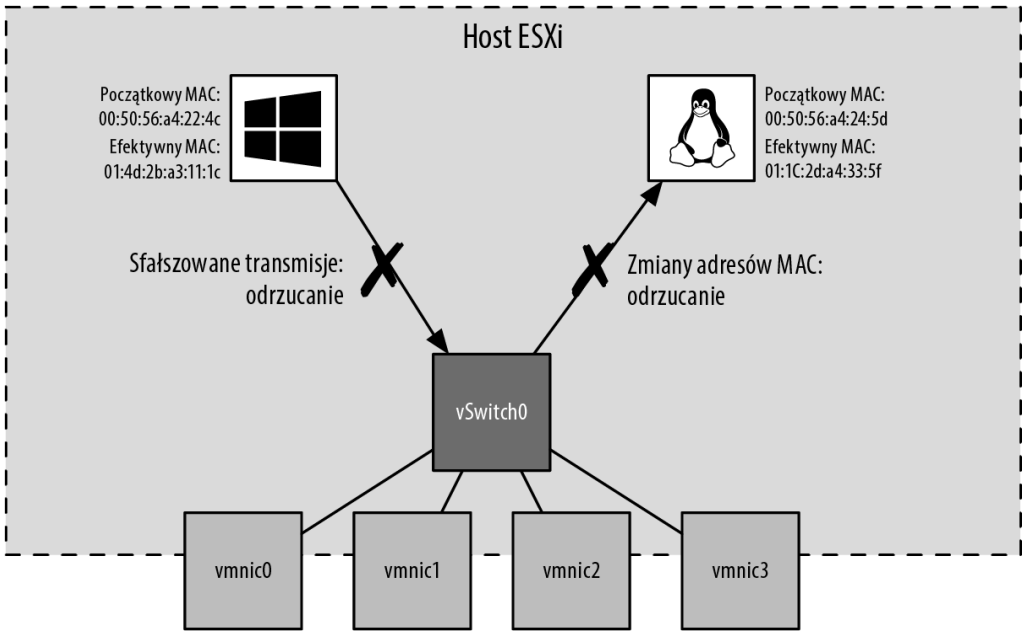


RYSUNEK 5.78. Źródłowy adres MAC maszyny wirtualnej to efektywny MAC adres, który domyślnie odpowiada początkowemu adresowi MAC skonfigurowanemu w pliku VMX. System operacyjny gościa może jednak zmienić efektywny adres MAC

Nie można usunąć możliwości zmiany efektywnego adresu MAC z systemu operacyjnego gościa. Możesz jednak odmówić lub zezwolić systemowi na działanie z tym zmienionym adresem MAC poprzez regułę bezpieczeństwa przełącznika standardowego lub rozproszonej grupy portów. Pozostałe dwa ustawienia reguły bezpieczeństwa przełącznika wirtualnego to zmiany adresów MAC i sfałszowane transmisje. Te ustawienia określają, czy początkowy adres MAC z pliku konfiguracyjnego i efektywny adres MAC w systemie operacyjnym gościa mogą się różnić. Jak wspomnieliśmy wcześniej, domyślną regułą bezpieczeństwa jest akceptowanie różnic i przetwarzanie ruchu zgodnie z potrzebami.

Różnica między ustawieniami bezpieczeństwa dotyczącymi zmian adresów MAC i sfałszowanymi transmisjami jest związana z kierunkiem ruchu. Zmiany adresów MAC dotyczą integralności ruchu przychodzącego. Gdy ta opcja jest ustawiona na odrzucanie, ruch nie będzie przekazywany poprzez przełącznik standardowy lub rozproszoną grupę portów do maszyny wirtualnej (ruch przychodzący), jeśli początkowy i efektywny adres MAC nie są zgodne. Ustawienie dla sfałszowanych transmisji nadzoruje natomiast integralność ruchu wychodzącego, i gdy ta opcja jest ustawiona na odrzucanie, ruch nie będzie przekazywany z maszyny wirtualnej do przełącznika standardowego lub rozproszonej grupy portów (ruch wychodzący), jeśli początkowy i efektywny adres MAC nie są zgodne. Rysunek 5.79 pokazuje ograniczenia bezpieczeństwa zaimplementowane, gdy opcje zmian adresów MAC i sfałszowanych transmisji są ustawione na odrzucanie.

Aby zapewnić najwyższy poziom bezpieczeństwa, VMware zaleca ustawienie zmian adresów MAC, sfałszowanych transmisji i trybu mieszanego na każdym przełączniku standardowym lub na każdej rozproszonej grupie portów na odrzucanie. Jeśli jest to uzasadnione lub konieczne, należy użyć grup portów, aby zmniejszyć poziom bezpieczeństwa dla pewnego podzbioru maszyn wirtualnych, które będą się łączyć z daną grupą portów.



RYSUNEK 5.79. Opcje bezpieczeństwa dotyczące zmian adresów MAC i sfałszowanych transmisji są związane odpowiednio z ruchem przychodzącym i wychodzącym

REGUŁY PRZEŁĄCZNIKÓW WIRTUALNYCH DLA FUNKCJONALNOŚCI RÓWNOWAŻENIA OBCIĄŻENIA SIECIOWEGO MICROSOFTU

Podobnie jak jest w przypadku innych rzeczy, istnieją oczywiście wyjątki od ogólnych zaleceń dotyczących tego, jak powinien być skonfigurowany przełącznik wirtualny. Zalecenia pozwalające na zmianę adresów MAC i sfałszowane transmisje są świetnymi przykładami. Dla maszyn wirtualnych, które zostaną skonfigurowane jako część klastra równoważenia obciążenia sieciowego (ang. *Network Load Balancing* — NLB) Microsoftu ustawionego w trybie unicastowym, grupa portów maszyn wirtualnych musi zezwalać na zmiany adresów MAC i sfałszowane transmisje. Systemy wchodzące w skład klastra NLB będą współdzielić adres IP i wirtualny adres MAC.

Współdzielony wirtualny adres MAC jest generowany przy użyciu algorytmu zawierającego statyczny komponent na podstawie konfiguracji trybu unicastowego lub multicastowego klastra NLB oraz szesnastkowej reprezentacji czterech oktetów tworzących adres IP. Ten wspólny adres MAC z pewnością będzie się różnić od adresu MAC zdefiniowanego w pliku *VMX* maszyny wirtualnej. Jeśli grupa portów maszyn wirtualnych nie zezwala na różnice między adresami MAC z pliku *VMX* i systemu operacyjnego gościa, NLB nie będzie działać zgodnie z oczekiwaniami. VMware zaleca uruchamianie klastrów NLB w trybie multicastowym z powodu tych problemów z klastrami NLB w trybie unicastowym.

Aby edytować profil bezpieczeństwa przełącznika wirtualnego, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do hosta ESXi posiadającego standardowy przełącznik vSphere, który chcesz edytować.

3. Po wybraniu hosta ESXi na liście inwentarza po lewej stronie kliknij zakładkę *Configure*, a następnie kliknij *Virtual Switches*.
4. Z listy przełączników wirtualnych wybierz standardowy przełącznik vSphere, który chcesz edytować, i kliknij link *Edit* (wygląda jak ołówek). Spowoduje to otwarcie okna dialogowego *Edit Settings* dla wybranego przełącznika wirtualnego.
5. Kliknij *Security* (bezpieczeństwo) na liście po lewej stronie okna dialogowego i wprowadź niezbędne modyfikacje.
6. Kliknij *OK*.

Aby edytować profil bezpieczeństwa grupy portów na przełączniku wirtualnym, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. Przejdź do określonego hosta ESXi i standardowego przełącznika vSphere zawierającego grupę, którą chcesz edytować.
3. Kliknij nazwę grupy portów pod graficzną reprezentacją przełącznika wirtualnego, a następnie kliknij link *Edit*.
4. Kliknij *Security* i wprowadź niezbędne modyfikacje. Musisz zaznaczyć pole wyboru *Override* (nadpisywanie), aby zezwolić grupie portów na użycie innego ustawienia, niż używa jej nadrzędny przełącznik wirtualny.
5. Kliknij *OK*, aby zapisać zmiany.

Aby edytować profil bezpieczeństwa rozproszonej grupy portów na rozproszonym przełączniku vSphere, wykonaj następujące czynności:

1. Połącz się z instancją serwera vCenter za pomocą klienta internetowego vSphere.
2. W nawigatorze wybierz *Networking*.
3. Wybierz istniejącą grupę portów rozproszonych, a następnie kliknij ikonę *Edit Distributed Port Group Settings*.
4. Wybierz *Security* z listy opcji reguł po lewej stronie okna dialogowego.
5. Wprowadź niezbędne modyfikacje w regułach bezpieczeństwa.
6. Kliknij *OK*, aby zapisać zmiany.

Jeśli musisz wprowadzić tę samą zmianę związaną z bezpieczeństwem w wielu rozproszonych grupach portów, możesz użyć opcji *Manage Distributed Port Groups* (zarządzanie rozproszonymi grupami portów) z menu *Actions*, aby wykonać to samo zadanie konfiguracyjne dla wielu rozproszonych grup portów jednocześnie.

Zarządzanie bezpieczeństwem architektury sieci wirtualnej jest bardzo podobne do zarządzania bezpieczeństwem każdej innej części systemów informatycznych. Reguły bezpieczeństwa powinny dyktować konfigurowanie możliwie jak najbezpieczniejszych ustawień, aby dmuchać na zimne. Poziom bezpieczeństwa należy obniżać tylko przy odpowiednich procesach autoryzacji, dokumentowania i zarządzania zmianami. Ponadto zmniejszenie poziomu bezpieczeństwa powinno być maksymalnie kontrolowane, aby miało wpływ na jak najmniejszą liczbę systemów, a najlepiej tylko na systemy wymagające modyfikacji.

W następnym rozdziale zajmiemy się szczegółowo pamięcią masową w środowisku vSphere VMware, która jest jego kluczowym komponentem.

Podsumowanie

Zidentyfikuj komponenty sieci wirtualnej. Sieci wirtualne to połączenie przełączników wirtualnych, przełączników fizycznych, sieci VLAN, fizycznych kart sieciowych, kart sieciowych VMkernel, uplinków, grup kart sieciowych, maszyn wirtualnych i grup portów.

Ćwiczenie. Jakie czynniki mają wpływ na projektowanie sieci wirtualnej i związanych z nią komponentów?

Twórz przełączniki wirtualne i rozproszone przełączniki wirtualne. vSphere obsługuje zarówno standardowe przełączniki vSphere, jak i rozproszone przełączniki vSphere. Przełączniki rozproszone wprowadzają do środowiska sieciowego vSphere nowe funkcjonalności, w tym prywatne sieci VLAN i scentralizowany punkt zarządzania klastrami ESXi.

Ćwiczenie. Poprosiłeś innego zaznajomionego administratora vSphere o utworzenie za Ciebie rozproszonego przełącznika vSphere, ale nie może on wykonać zadania, ponieważ nie wie, jak zrobić to przy hoście ESXi wybranym w kliencie internetowym vSphere. Co powinieneś powiedzieć temu administratorowi?

Twórz grupy kart sieciowych, VLAN-y oraz prywatne VLAN-y i zarządzaj nimi. Grupy kart sieciowych umożliwiają przełącznikom wirtualnym posiadanie redundantnych połączeń sieciowych z resztą sieci. Przełączniki wirtualne zapewniają także obsługę VLAN-ów, które oferują logiczną segmentację sieci, oraz prywatnych VLAN-ów, które gwarantują dodatkowe bezpieczeństwo istniejącym VLAN-om, jednocześnie pozwalając systemom współużytkować tę samą podsieć IP.

Ćwiczenie. Chcesz użyć grup kart sieciowych, aby jak najlepiej wykorzystać fizyczne uplinki do zapewnienia zarówno większej redundancji, jak i lepszej przepustowości, nawet w przypadku rywalizacji o przepustowość. Jakich reguł równoważenia obciążenia na przełączniku rozproszonym powinieneś użyć?

Ćwiczenie. Jak skonfigurować zarówno standardowy przełącznik vSphere, jak i rozproszony przełącznik vSphere do przekazywania znaczników VLAN aż do systemu operacyjnego gościa?

Skonfiguruj reguły bezpieczeństwa przełącznika wirtualnego. Przełączniki wirtualne obsługują reguły bezpieczeństwa dla akceptowania lub odrzucania trybu mieszanego, zmian adresów MAC oraz sfałszowanych transmisji. Wszystkie te opcje bezpieczeństwa mogą pomóc zwiększyć zabezpieczenia warstwy drugiej.

Ćwiczenie. Masz aplikację sieciową, która musi widzieć w sieci wirtualnej ruch przeznaczony dla innych systemów produkcyjnych w tym samym VLAN-ie. Aplikacja dokonuje tego za pomocą trybu mieszanego. Jak można zaspokoić potrzeby tej aplikacji sieciowej bez poświęcania bezpieczeństwa całości przełącznika wirtualnego?

Ćwiczenie. Inny administrator vSphere z Twojego zespołu próbuje skonfigurować reguły bezpieczeństwa na przełączniku rozproszonym, ale ma pewne trudności. Co może stanowić problem?

VMware vSphere: zostań mistrzem wirtualizacji!

Termin *wirtualizacja* jest od jakiegoś czasu bardzo modny. Oznacza abstrakcję zasobów obliczeniowych opartą na innych zasobach, jednak specjaliści IT słowo to kojarzą z abstrakcją sprzętu (serwerów), czyli oddzieleniem systemu operacyjnego od sprzętu, na którym jest uruchomiony. Dzięki temu na jednym fizycznym serwerze można jednocześnie uruchamiać wiele systemów operacyjnych. W takiej właśnie technologii działa rodzina produktów VMware vSphere. Tego rodzaju wirtualizacja przynosi sporo różnych korzyści, od oszczędności wynikających z mniejszej liczby potrzebnego sprzętu po lepszy dostęp do sieci i puli zasobów, które można wykorzystywać z dużo większą efektywnością.

W książce znalazły się wszelkie informacje potrzebne do instalowania, konfigurowania i monitorowania wirtualnego środowiska z wykorzystaniem VMware vSphere 6.7. Zaprezentowano tu szeroki zakres możliwości vSphere, opisano też przydatne funkcjonalności i udogodnienia. Dokładnie przedstawiono zagadnienie instalacji i konfiguracji sieci wraz z magazynami danych vSphere. Kolejne rozdziały poświęcono wysokiej dostępności, nadmiarowości i wykorzystaniu zasobów. Nie zabrakło opisu tworzenia maszyn wirtualnych i zarządzania nimi, a także monitorowania ich pracy i diagnozowania problemów. To wyczerpujące kompendium wiedzy o implementowaniu, utrzymywaniu i diagnozowaniu środowisk wirtualnych klasy korporacyjnej.

W książce między innymi:

- **planowanie wdrożenia i proces wdrażania środowiska VMware vSphere**
- **konfigurowanie sieci, maszyn wirtualnych oraz pamięci masowych**
- **zarządzanie przydzielaniem i wykorzystaniem zasobów**
- **monitorowanie wydajności i dostępności infrastruktury**
- **zapewnienie ciągłości działania**
- **automatyzowanie typowych operacji administracyjnych**

Nick Marshall jest starszym architektem integracji rozwiązań SDDC. Obecnie pracuje w firmie VMware, w dziale zintegrowanych systemów biznesowych. Jest pasjonatem wirtualizacji. Udziela się jako prelegent na branżowych konferencjach, między innymi VMworld, VMUG (VMware User Group) i PEX (Partner Exchange). Mieszka z rodziną w Melbourne w Australii.

Helion
helion.pl
HELION SA
ul. Kościuszki 1c
44-100 Gliwice
tel.: 32 230 98 63
helion@helion.pl

KOD KORZYŚCI
Sięgnij po więcej!
ISBN 978-83-283-6349-6
9 788328 363496
INFORMATYKA W NAJLEPSZYM WYDANIU
Cena: 149,00 zł
SYBEX
A Wiley Brand