



VMware® dla administratorów sieci komputerowych

Christopher Wahl
Steven Pantol

Przedmowa Ivan Pepelnjak



Tytuł oryginału: Networking for VMware Administrators

Tłumaczenie: Lech Lachowski

ISBN: 978-83-283-0696-7

Authorized translation from the English language edition, entitled: NETWORKING FOR VMWARE ADMINISTRATORS, ISBN 0133511081; by Christopher Wahl and Steve Pantol; published by Pearson Education, Inc, publishing as VMWARE Press.
Copyright © 2014 VMware, Inc.

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or by any information storage retrieval system, without permission from Pearson Education Inc.

Polish language edition published by HELION S.A. Copyright © 2015.

Wszelkie prawa zastrzeżone. Nieautoryzowane rozpowszechnianie całości lub fragmentu niniejszej publikacji w jakiegokolwiek postaci jest zabronione. Wykonywanie kopii metodą kserograficzną, fotograficzną, a także kopiowanie książki na nośniku filmowym, magnetycznym lub innym powoduje naruszenie praw autorskich niniejszej publikacji.

Wszystkie znaki występujące w tekście są zastrzeżonymi znakami firmowymi bądź towarowymi ich właścicieli.

Autor oraz Wydawnictwo HELION dołożyli wszelkich starań, by zawarte w tej książce informacje były kompletne i rzetelne. Nie biorą jednak żadnej odpowiedzialności ani za ich wykorzystanie, ani za związane z tym ewentualne naruszenie praw patentowych lub autorskich. Autor oraz Wydawnictwo HELION nie ponoszą również żadnej odpowiedzialności za ewentualne szkody wynikłe z wykorzystania informacji zawartych w książce.

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

Drogi Czytelniku!

Jeżeli chcesz ocenić tę książkę, zajrzyj pod adres

<http://helion.pl/user/opinie/vmwaad>

Możesz tam wpisać swoje uwagi, spostrzeżenia, recenzję.

Printed in Poland.

- [Kup książkę](#)
- [Poleć książkę](#)
- [Oceń książkę](#)

- [Księgarnia internetowa](#)
- [Lubię to! » Nasza społeczność](#)

Spis treści

Przedmowa	13
Wprowadzenie	15
O autorach	18
Podziękowania	19
O korektorach merytorycznych	20

Część I. Podstawy sieci fizycznych

Rozdział 1. Podstawy	21
Wprowadzenie	21
Wymyślanie koła od nowa	21
Podsumowanie	26
Rozdział 2. Opowieść o dwóch modelach sieciowych	27
Wprowadzenie	27
Zachowanie modelu	29
Warstwowanie	29
Kapsułkowanie	29
Model OSI	30
Model TCP/IP	32
Warstwa dostępu do sieci	32
Warstwa internetowa	32
Warstwa transportowa	33
Warstwa aplikacji	34
Porównanie modelu OSI z modelem TCP/IP	34
Podsumowanie	35
Rozdział 3. Sieci Ethernet	37
Wprowadzenie	37
Ethernet	37
Historia i teoria działania	38
Standardy i rodzaje kabli Ethernet	39
Adresowanie w sieci Ethernet	42

Rozszerzanie segmentów sieci Ethernet: regeneratory sygnału, koncentratory i przełączniki	43
Logika przełączania	45
Podsumowanie	45
Rozdział 4. Zaawansowane zagadnienia warstwy drugiej	47
Wprowadzenie	47
Koncepcje	47
Trunking	50
Unikanie pętli oraz Spanning Tree	51
Przegląd protokołu Spanning Tree	52
PortFast	54
Rapid Spanning Tree	55
Agregacja łączy	56
Co to jest agregacja łączy?	56
Dynamiczna agregacja łączy	59
Rodzaje dystrybucji obciążenia	60
Podsumowanie	61
Rozdział 5. Warstwa trzecia	63
Wprowadzenie	63
Warstwa sieciowa	63
Routing i forwarding	64
Trasy automatyczne, statyczne i dynamiczne	64
Trasa ostatniego wyboru	64
Adresowanie i podsieciowanie IP	65
Adresowanie klasowe	65
Adresowanie bezklasowe	66
Adresy zarezerwowane	67
Aplikacje wspierające warstwę sieciową	68
DHCP	68
DNS	68
ARP	69
Ping	69
Podsumowanie	69
Rozdział 6. Infrastruktura konwergentna	71
Wprowadzenie	71
Koncepcje	72
Zalety infrastruktury konwergentnej	72
Przykłady	73
UCS firmy Cisco	73
BladeSystem firmy HP	75
Virtual Computing Platform firmy Nutanix	76
Podsumowanie	78

Część II. Przełączanie wirtualne

Rozdział 7. Różnice pomiędzy przełączaniem wirtualnym i fizycznym	79
Wprowadzenie	79
Porównanie przełączników fizycznych z wirtualnymi	79
Podobieństwa	80
Różnice	80
Decyzje dotyczące przełączania	80
Uplinki fizyczne	82
Adapter sieciowy hosta	82
Porty wirtualne	83
Adaptory sieciowe maszyn wirtualnych	84
Porty VMkernel	84
Service Console	84
Sieci VLAN	85
Znakowanie EST	85
Znakowanie VST	85
Znakowanie VGT	86
Podsumowanie	86
Rozdział 8. vSphere Standard Switch	89
Wprowadzenie	89
Przełącznik vSphere Standard Switch	89
Podstawowa terminologia	90
Płaszczyzna sterowania	90
Płaszczyzna danych	90
Właściwości przełącznika vSwitch	91
Porty	91
Rozmiar największego datagramu (MTU)	92
Bezpieczeństwo	92
Tryb mieszany	93
Zmiany adresu MAC	93
Fałszywe transmisje	95
Wykrywanie	95
Protokół CDP	96
Kształtowanie ruchu	97
Matematyka kształtowania ruchu	99
NIC Teaming	99
Równoważenie obciążenia	100
Wykrywanie awarii sieci	102
Informowanie przełączników	103
Powrót po awarii	103
Kolejność przełączania awaryjnego	104
Nadpisywanie hierarchii	104
Porty VMkernel	105
Właściwości i usługi portów	105
Adresy IP	107
Grupy portów VM	107
Podsumowanie	108

Rozdział 9. vSphere Distributed Switch	109
Wprowadzenie do przełącznika vSphere Distributed Switch	109
Płaszczyzna sterowania	110
Obsługa awarii vCenter	111
Płaszczyzna danych	112
Monitorowanie	112
Protokół CDP	112
Protokół LLDP	113
Funkcja NetFlow	113
Port Mirroring	115
Prywatne sieci VLAN	121
VLAN podstawowy	121
VLAN mieszany	121
VLAN-y podrzędne	121
VLAN-y typu community	122
VLAN-y typu isolated	123
Rozproszone grupy portów	123
Porty VMkernel	124
Maszyny wirtualne	125
Kształtowanie ruchu	125
Egress	125
Równoważenie obciążenia	126
Route based on physical NIC load	126
Sterowanie operacjami we/wy sieci	129
Pule zasobów sieciowych	130
Udziały	131
Pule zasobów sieciowych definiowane przez użytkownika	132
Podsumowanie	134
 Rozdział 10. Przełączniki innych producentów — 1000V	135
Wprowadzenie	135
Integracja z vSphere	136
Różnice w zakresie architektury	137
Wirtualny moduł zarządzający	137
Profile portów	140
Wirtualny moduł ethernetowy	142
Tryb warstwy drugiej	143
Nexus 1000V w trybie warstwy trzeciej	144
Maksymalna liczba modułów VEM	145
Funkcje zaawansowane	145
Uwaga na temat systemu operacyjnego Nexus OS	145
Licencjonowane tryby pracy	146
Licencja Essential Edition	146
Licencja Advanced Edition	146
Podsumowanie	147

Rozdział 11. Scenariusz laboratoryjny	149
Wprowadzenie	149
Budowanie sieci wirtualnej	149
Decyzje architektoniczne	150
Projekt sieci	150
Projekt hostów	151
Projekt ruchu danych dla maszyn wirtualnych	152
Scenariusz laboratoryjny	153
Podsumowanie	156
 Rozdział 12. Projekt przełącznika Standard vSwitch	 157
Wprowadzenie	157
Projekt przełącznika Standard vSwitch	157
Przykładowy przypadek użycia	158
Konwencje nazewnictwa	158
Zapewnienie funkcjonalności Quality of Service	161
Adaptery sieciowe	162
Ruch maszyn wirtualnych	164
Grupy portów maszyn wirtualnych	164
Kolejność przełączania awaryjnego	167
Porty VMkernel	169
Usługa Management	169
Usługa vMotion	172
Usługa Fault Tolerance	176
Usługa NFS Storage	178
Przegląd ustawień przełączania awaryjnego dla portów VMkernel	181
Końcowa regulacja	182
Konfiguracja dodatkowych hostów vSphere	183
Podsumowanie	184
 Rozdział 13. Projekt przełącznika Distributed vSwitch	 185
Wprowadzenie	185
Projekt przełącznika Distributed vSwitch	185
Przypadek użycia	186
Konwencje nazewnictwa	187
Zapewnienie funkcjonalności Quality of Service	188
Sterowanie operacjami we/wy sieci	188
Znakowanie priorytetów w standardzie 802.1p	190
Usługa DSCP	191
Tworzenie przełącznika Distributed vSwitch	191
Adaptery sieciowe	194
Rozproszone grupy portów dla maszyn wirtualnych	195
Load Based Teaming	197
Rozproszone grupy portów dla portów VMkernel	200
Usługa Management	200
Usługa vMotion	202
Usługa Fault Tolerance	203

Usługa iSCSI Storage	204
Przegląd ustawień przełączania awaryjnego dla portów VMkernel	204
Dodawanie hostów vSphere	206
Tworzenie portów VMkernel	212
Przenoszenie maszyny wirtualnej vCenter	215
Kroki końcowe	220
Funkcja Health Check	220
Protokół wykrywania sieci	222
Inne względy konstrukcyjne	223
Projektowanie w pełni zautomatyzowane	223
Projektowanie hybrydowe automatyczne	224
Co jest właściwe?	224
Podsumowanie	224

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

Rozdział 14. Ogólne przypadki użycia protokołu iSCSI	225
Wprowadzenie	225
Protokół iSCSI	225
Protokoły bezstratne i typu best effort	226
Sterowanie przepływem oparte na priorytetach	226
Izolacja za pomocą sieci VLAN	228
iSCSI z ramkami jumbo	228
Komponenty iSCSI	229
Inicjatory	230
Cele	230
Nazewnictwo	231
Zabezpieczanie za pomocą protokołu CHAP	232
Adaptery iSCSI	234
Programowy adapter iSCSI	235
Zależny sprzętowy adapter iSCSI	236
Niezależny sprzętowy adapter iSCSI	237
Projektowanie iSCSI	238
Funkcja NIC Teaming	239
Wiązanie portu sieciowego	240
Projekt wielu przełączników vSwitch	241
Projekt pojedynczego przełącznika vSwitch	242
Bootowanie z iSCSI	243
Podsumowanie	245
 Rozdział 15. Projektowanie i konfiguracja pamięci masowej iSCSI	 247
Wprowadzenie	247
Projekt iSCSI	247
Przypadek użycia	248
Konwencje nazewnictwa	249
Adresy sieciowe	250

Konfiguracja przełącznika vSwitch	251
Rozproszone grupy portów iSCSI	251
Porty VMkernel	254
Wiązanie portu sieciowego	257
Ramki jumbo	260
Dodawanie urządzeń iSCSI	261
Serwer i cele iSCSI	261
Uwierzytelnianie za pomocą protokołu CHAP	263
Tworzenie magazynów danych VMFS	266
Reguły PSP	268
Podsumowanie	269
Rozdział 16. Ogólne przypadki użycia protokołu NFS	271
Wprowadzenie	271
Protokół NFS	271
Protokoły bezstratne i typu best effort	272
Izolacja za pomocą sieci VLAN	273
NFS z ramkami jumbo	273
Komponenty NFS	274
Plik exports	274
Demony	274
Punkty montowania	275
Zapewnianie bezpieczeństwa za pomocą list ACL	277
Adaptory sieciowe	278
Projekt NFS	278
Pojedyncza sieć	279
Wiele sieci	280
Grupa agregacji łączy	282
Podsumowanie	284
Rozdział 17. Projektowanie i konfiguracja pamięci masowej NFS	285
Wprowadzenie	285
Projekt NFS	285
Przypadek użycia	285
Konwencje nazewnictwa	286
Adresy sieciowe	287
Konfiguracja przełącznika vSwitch	288
Przełącznik vSwitch dla sieci NFS	288
Adaptory sieciowe	290
Porty VMkernel	291
Montowanie pamięci masowej NFS	293
Podsumowanie	295

Część IV. Inne scenariusze projektowe

Rozdział 18. Dodatkowe scenariusze projektowe przełącznika vSwitch	297
Wprowadzenie	297
Przypadek użycia	297
Standardy nazewnictwa	298
Dwa adaptory sieciowe	298
Model z pamięcią masową opartą na sieci Ethernet	299
Model bez pamięci masowej opartej na sieci Ethernet	299
Cztery porty sieciowe	299
Model z pamięcią masową opartą na sieci Ethernet	300
Model bez pamięci masowej opartej na sieci Ethernet	301
Sześć portów sieciowych	301
Model z pamięcią masową opartą na sieci Ethernet — sześć adapterów 1 Gb	302
Model bez pamięci masowej opartej na standardzie Ethernet — sześć adapterów 1 Gb	302
Model z pamięcią masową opartą na sieci Ethernet — cztery adaptory 1 Gb + dwa adaptory 10 Gb	303
Model bez pamięci masowej opartej na sieci Ethernet — cztery adaptory 1 Gb + dwa adaptory 10 Gb	304
Osiem adapterów sieciowych	305
Model z pamięcią masową opartą na sieci Ethernet — osiem adapterów 1 Gb	305
Model bez pamięci masowej opartej na sieci Ethernet — osiem adapterów 1 Gb	306
Model z pamięcią masową opartą na sieci Ethernet — cztery adaptory 1 Gb + cztery adaptory 10 Gb	306
Model bez pamięci masowej opartej na sieci Ethernet — cztery adaptory 1 Gb + cztery adaptory 10 Gb	308
Podsumowanie	308
Rozdział 19. Architektura multi-NIC vMotion	309
Wprowadzenie	309
Przypadki użycia multi-NIC vMotion	309
Projekt	310
Sprawdzanie dostępnej przepustowości	311
Kontrolowanie ruchu vMotion	312
Projekt rozproszonego przełącznika vSwitch	312
Projekt standardowego przełącznika vSwitch	315
Projekt fizycznego przełącznika upstream	315
Konfiguracja multi-NIC vMotion	316
Rozproszone grupy portów	316
Porty VMkernel	317
Kształtowanie ruchu	318
Podsumowanie	319
Dodatek A. Sieci dla administratorów VMware: organizacja VMware User Group	321
Organizacja VMware User Group	321
Skorowidz	322

vSphere Distributed Switch

Kluczowe zagadnienia omówione w tym rozdziale:

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

Wprowadzenie do przełącznika vSphere Distributed Switch

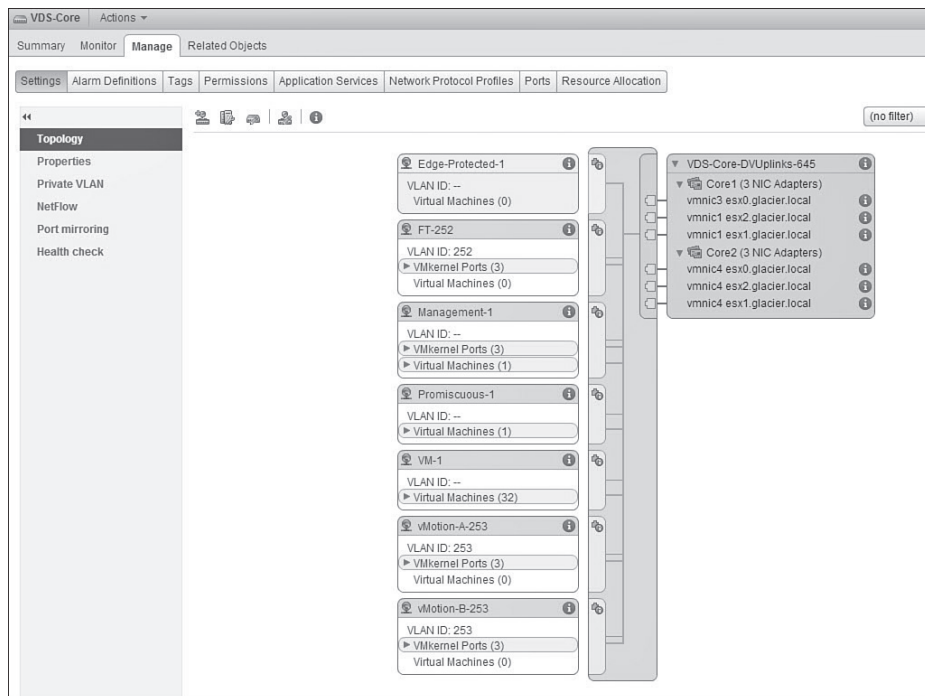
Przełącznik vSphere Distributed Switch (VDS) oferuje Tobie, jako klientowi, dwie główne korzyści. Po pierwsze, VDS zapewnia scentralizowaną płaszczyznę sterowania do zarządzania przełączaniem wirtualnym, zapobiegając konieczności wykonywania wielu niewdzięcznych zadań w codziennej administracji. Po drugie,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

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

Płaszczyzna sterowania

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

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



RYSUNEK 9.1. Porty dvUplink w przełączniku VDS

WSKAZÓWKA

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

Obsługa awarii vCenter

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

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

```
The time and date of this login have been sent to the system logs.
vmware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.

The ESXi shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
~ # cd /etc/vmware
/etc/vmware # ls -l
-rw-r--r-- 1 root root 3041 May 1 02:54 BootbankFunctions.sh
-rw-r--r-- 1 root root 1167 Jun 30 09:15 config
-rw-r--r-- 1 root root 7699 May 1 02:54 configrules
drwx----- 1 root root 512 May 28 03:30 driver_map.d
-rw-r--r-- 1 root root 95744 Sep 4 02:08 dvsdata.db
-rw----- 1 root root 26170 Sep 3 16:55 esx.conf
drwxr-xr-x 1 root root 512 May 28 03:30 firewall
-rw-r--r-- 1 root root 59 May 1 02:54 ft-vmx-version
-rw-r--r-- 1 root root 60 May 1 02:54 ft-vmx-version
drwxr-xr-x 1 root root 512 Aug 29 12:31 hostd
drwxr-xr-x 1 root root 512 May 28 03:30 icu
drwxr-xr-x 1 root root 512 May 28 03:30 ike
-rw-r--r-- 1 root root 50 May 1 02:55 ima_plugin.conf
-rw-r--r-- 1 root root 310 Jul 27 01:06 license.cfg
-rw-r--r-- 1 root root 440 May 1 02:55 localsas
-rw-r--r-- 1 root root 0 May 1 02:55 lockdown
-rw-r--r-- 1 root root 0 May 28 03:31 locker.conf
drwxr-xr-x 1 root root 512 May 28 03:30 microcode
-rw-r--r-- 1 root root 825 May 1 02:55 passthru.map
-rw-r--r-- 1 root root 782492 Mar 23 17:58 pci_ids
drwxr-xr-x 1 root root 512 May 1 02:55 pciid
drwxr-xr-x 1 root root 512 May 28 03:30 rhttpproxy
drwxr-xr-x 1 root root 512 May 28 03:30 secpolicy
drwxr-xr-x 1 root root 512 May 28 03:30 service
-rw-r--r-- 1 root root 64 Aug 19 16:43 settings
-rw-r--r-- 1 root root 0 May 1 02:55 smart_plugin.conf
-rw-r--r-- 1 root root 200 May 1 02:55 snmp.xml
drwxr-xr-x 1 root root 512 May 28 03:30 ssl
-rw-r--r-- 1 root root 480 May 1 02:55 support
-rw-r--r-- 1 root root 380961 May 1 02:55 usb.ids
drwxr-xr-x 1 root root 512 May 28 03:30 vm-support
drwxr-xr-x 1 root root 512 Aug 21 21:41 vmkscsid
-rw----- 1 root root 29 Aug 19 16:00 vmware.lic
drwxr-xr-x 1 root root 512 May 28 03:30 vmauth
drwxr-xr-x 1 root root 512 Aug 19 02:32 vpxa
-rw-r--r-- 1 root root 512 May 28 03:30 weasel
-rw-r--r-- 1 root root 0 May 1 02:55 welcome
-rw-r--r-- 1 root root 923 Jul 22 16:03 zloadmod.txt
/etc/vmware #
```

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

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

Płaszczyzna danych

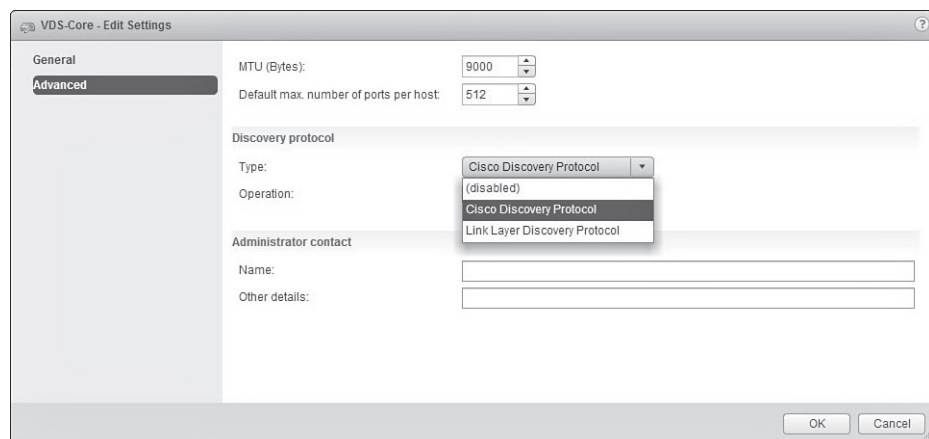
Podobnie jak w wypadku standardowego przełącznika cała aktywność płaszczyzny danych występuje nadal w warstwie hosta. Z założenia żadne dane nie są przesyłane za pośrednictwem serwera vCenter, ponieważ jest on po prostu punktem kontroli. Wszystkie decyzje przełączania nadal podejmowane są w samym hoście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

Monitorowanie

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

Protokół CDP

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



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

Protokół LLDP

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

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

WSKAZÓWKA

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

Funkcja NetFlow

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

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

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

WSKAZÓWKĄ

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

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

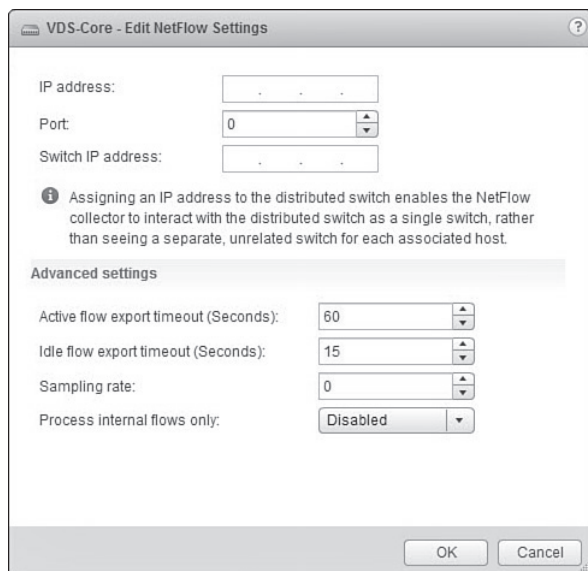
Konfiguracja NetFlow przełącznika jest określana przez następujące elementy:

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

Opisane powyżej opcje zostały przedstawione na rysunku 9.4.

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

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



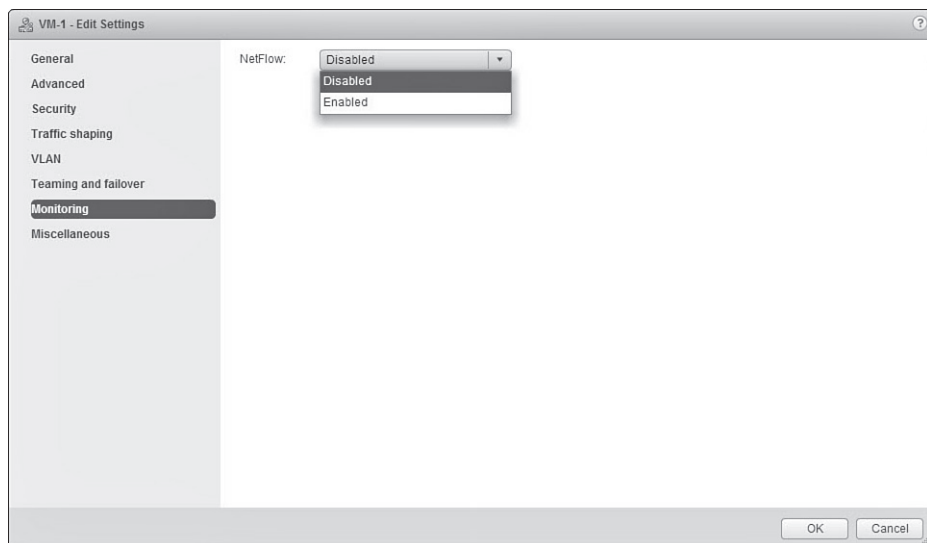
RYСУNEK 9.4. Opcje konfiguracji NetFlow w przełączniku VDS

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

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

Port Mirroring

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



RYSUNEK 9.5. Włączanie funkcji NetFlow dla grupy portów

ale często mają różne cele. Jeśli chodzi o **monitorowanie**, może być potrzeba związana na przykład z zachowaniem zgodności lub jakąś umową SLA (ang. *Service Level Agreement*), aby wiedzieć dokładnie, jaki ruch jest wysyłany z jednego konkretnego urządzenia do drugiego.

Przechwytywanie (ang. *capturing*) jest najczęściej spotykane w wypadku konieczności spełnienia wymagań dotyczących rejestrowania rozmów, np. przy przechwytywaniu ruchu VoIP, aby w *call center* rejestrowane były rozmowy telefoniczne.

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

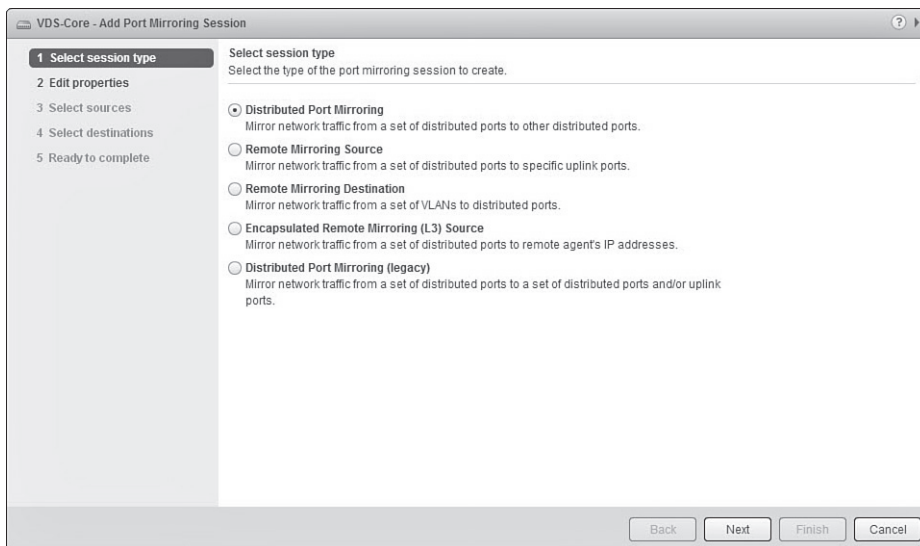
Dodanie środowisk wirtualnych stworzyło pewne problemy związane z funkcją Port Mirroring. Pojedynczy port przełącznika podłączony do hosta vSphere może teraz przekazywać ruch dla dziesiątek, a nawet setek serwerów wirtualnych. Dla pojedynczego serwera wirtualnego funkcjonującego poza rozbudowanymi topologiami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

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

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

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

Opcje te zostały przedstawione na rysunku 9.6.



RYСУNEK 9.6. Opcje funkcji Port Mirroring w przełączniku VDS 5.1

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

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

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

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

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

Te zaawansowane właściwości zostały przedstawione na rysunku 9.7.

RYСУNEK 9.7. Elementy konfiguracyjne dla sesji Port Mirroring

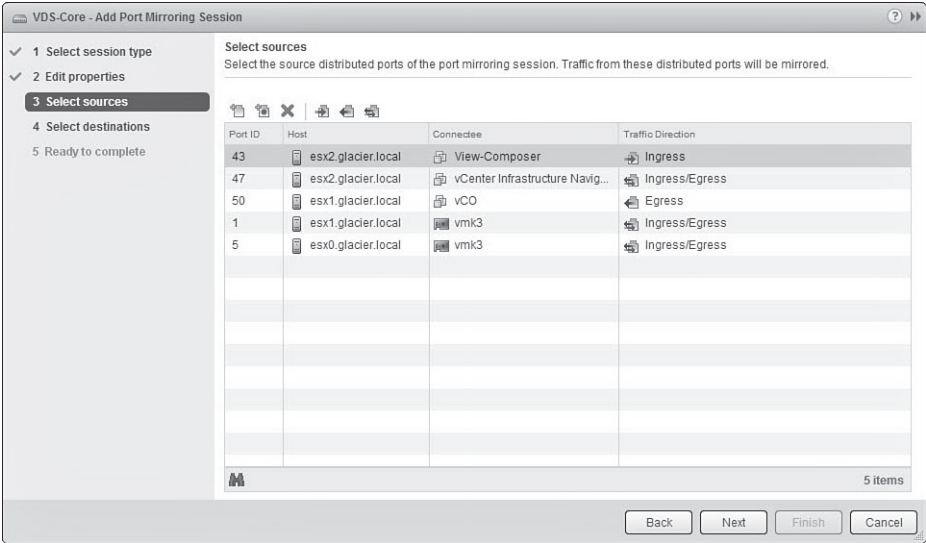
Źródłem dla sesji Port Mirroring mogą być: jeden port rozproszony, wiele portów rozproszonych, a nawet zakres portów. Porty mogą być wykorzystywane przez maszyny wirtualne lub porty VMkernel. Każdy identyfikator portu (ang. *port ID*) wskazuje host, który obsługuje identyfikator portu wirtualnego, element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

Opcje źródeł zostały przedstawione na rysunku 9.8.

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

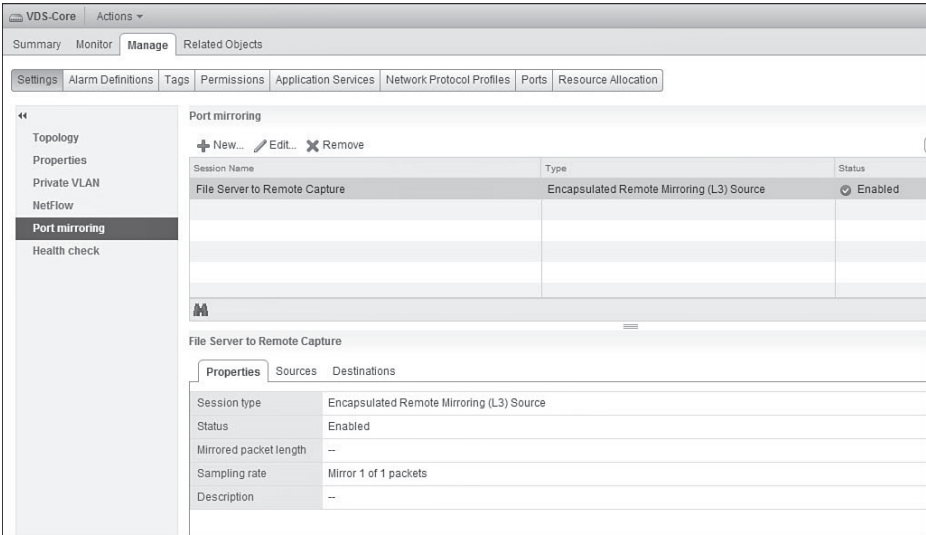
Wybór miejsca docelowego dla sesji Port Mirroring jest najbardziej zróżnicowany. Oto lista dostępnych opcji związanych z miejscami docelowymi dla każdego rodzaju Port Mirroring:

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



RYSUNEK 9.8. Próbkowanie źródeł do sesji funkcji Port Mirroring

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



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

Prywatne sieci VLAN

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

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

VLAN podstawowy

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

VLAN mieszany

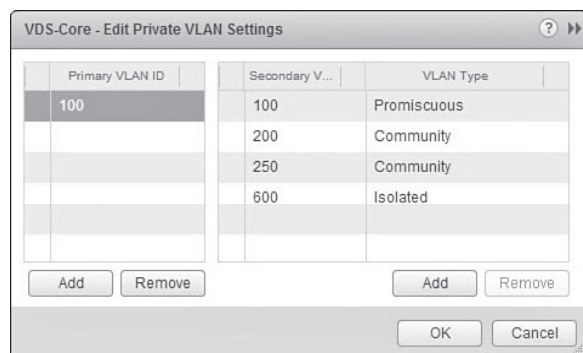
VLAN podstawowy jest połączony z resztą infrastruktury sieciowej za pomocą jednego portu mieszanego (ang. *promiscuous port* — P-Port) lub kilku takich portów. Możesz potraktować P-Port jako wejście do budynku z apartamentami — każdy ma do niego dostęp, a przez ten port wchodzi się do prywatnego zbioru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

VLAN-y podrzędne

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

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

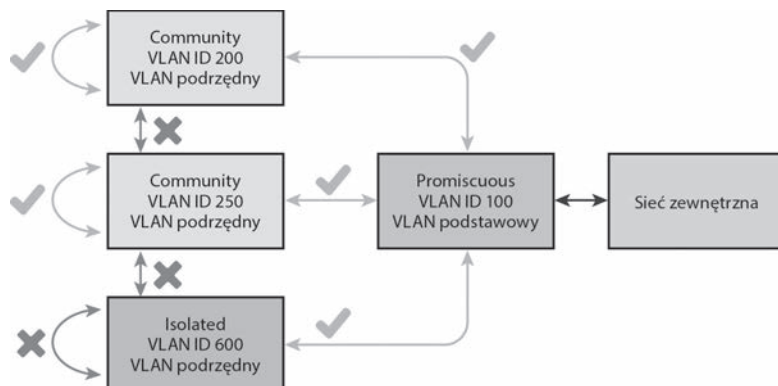
Na rysunku 9.10 przedstawiony został proces tworzenia VLAN-u prywatnego w przełączniku VDS.



RYСУNEK 9.10. Tworzenie VLAN-u prywatnego w przełączniku rozproszonym

VLAN-y typu community

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



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

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

VLAN-y typu *isolated*

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

WSKAZÓWKA

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

Rozproszone grupy portów

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

WSKAZÓWKA

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

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

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

Porty VMkernel

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

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

The screenshot shows the vSphere Web Client interface for configuring a Distributed Virtual Switch (VDS). The left sidebar shows the navigation tree with 'Virtual adapters' selected. The main panel displays a table of virtual adapters and their properties.

Device	Network Label	Switch	IP Address	vMotion Traffic	FT Logging	Management	vSphere
vmk0	Management-1	VDS-Core	10.0.0.50	Disabled	Disabled	Disabled	Disabled
vmk1	vMotion-A-253	VDS-Core	10.0.253.50	Enabled	Disabled	Disabled	Disabled
vmk2	vMotion-B-253	VDS-Core	10.0.253.150	Enabled	Disabled	Disabled	Disabled
vmk3	FT-252	VDS-Core	10.0.252.50	Disabled	Enabled	Disabled	Disabled
vmk4	NFS-A-251	VDS-Storage	10.0.251.50	Disabled	Disabled	Disabled	Disabled

Below the table, the configuration for the selected virtual network adapter 'vmk0' is shown. The configuration includes:

- IPV6 addresses:** fe80::250:56ff:fe63:470a/64
- Default gateway for IPv6:** --
- NIC settings:**
 - MAC address: 00:50:56:83:47:0a
 - MTU: 1500
- Security:**
 - Promiscuous mode: Reject
 - MAC address changes: Reject
 - Forged transmits: Reject
- Ingress traffic shaping:**
 - Status: Disabled
 - Average bandwidth: --
 - Peak bandwidth: --
 - Burst size: --
- Egress traffic shaping:**

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

Maszyny wirtualne

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

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

Kształtowanie ruchu

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

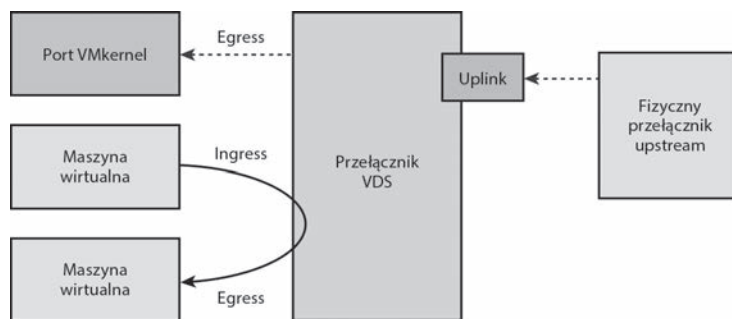
W tym rozdziale powracamy do kwestii kształtowania ruchu z uwagi na dodatkową funkcję, która pojawiła się w przełączniku Distributed vSwitch. Jest to zdolność do kształtowania zarówno ruchu *ingress*, jak i *egress*. Standardowy przełącznik vSwitch umożliwia jedynie kształtowanie ruchu *ingress*.

Egress

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

UWAGA

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



RYСУNEK 9.13. Różne przypadki występowania ruchu egress w przełączniku VDS

Równoważenie obciążenia

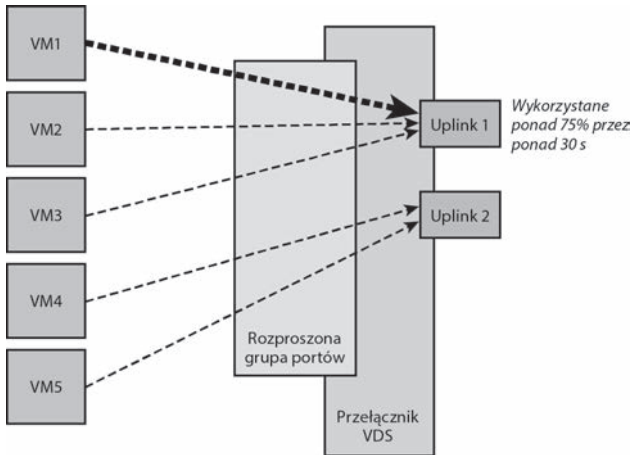
Kolejną funkcją dostępną tylko w przełączniku Distributed vSwitch jest nowa forma równoważenia obciążenia o nazwie *Route based on physical NIC load* (trasa oparta na obciążeniu fizycznego adaptera sieciowego), często określana jako *Load Based Teaming* (LBT). Te reguły routingu zostały wprowadzone w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

Route based on physical NIC load

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

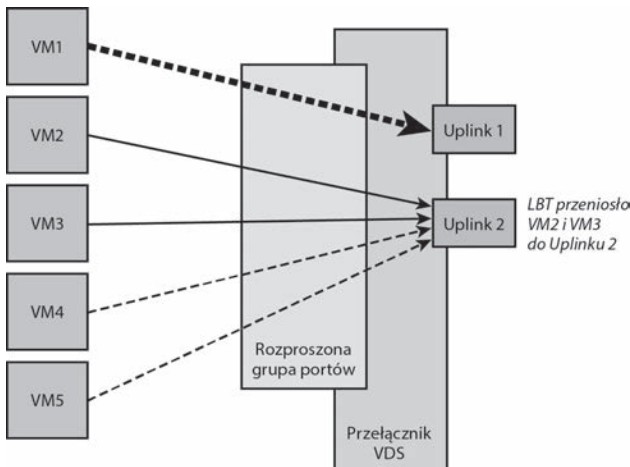
W wypadku każdej innej zasady równoważenia obciążenia nasycenie na *Uplinku 1* będzie się utrzymywać, dopóki VM1 nie zakończy wysyłania danych przez sieć. Tymczasem *Uplink 2* może doświadczać bardzo niewielkiego ruchu, a nawet pozostawać w stanie bezczynności. Co za marnotrawstwo!

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



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

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



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

Ważne jest, aby zrozumieć kilka ograniczeń związanych z LBT:

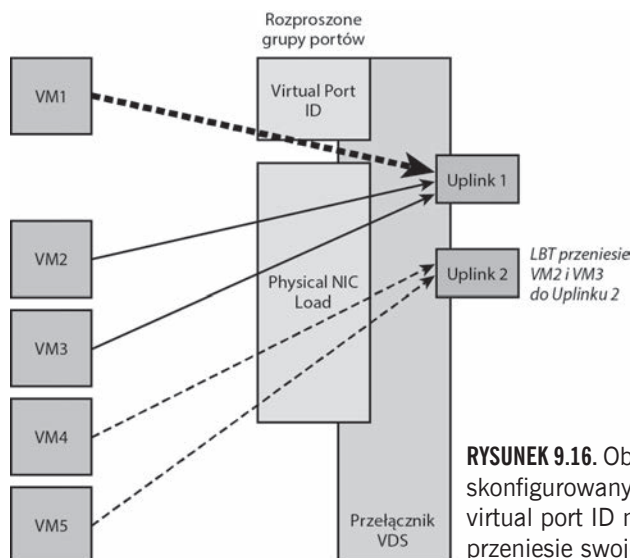
- Wirtualny adapter sieciowy maszyny wirtualnej nie może korzystać z wielu uplinków w tym samym czasie. Reguły równoważenia obciążenia w wypadku rywalizacji o przepustowość przenoszą adapter wirtualny z jednego uplinku do drugiego, ale nie rozkładają ruchu sieciowego pojedynczej maszyny wirtualnej na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

UWAGA

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

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

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



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

Sterowanie operacjami we/wy sieci

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

UWAGA

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

Network Resource Pool	Host Limit (Mbps)	Physical Adapter Sha...	Shares Value	QoS Priority Tag
System network resource pools				
vMotion Traffic	500	Normal	50	
Fault Tolerance (FT) Traffic	Unlimited	Normal	50	
vSphere Replication (VR) Traffic	Unlimited	Normal	50	
iSCSI Traffic	Unlimited	Normal	50	
Management Traffic	Unlimited	Normal	50	
NFS Traffic	Unlimited	Normal	50	
Virtual Machine Traffic	Unlimited	High	100	
vSphere Storage Area Network Traffic	Unlimited	Normal	50	

RYSUNEK 9.17. W oknie z zakładką Resource Allocation pokazane wszystkie wartości konfiguracji NIOC. Zobaczmy, za co odpowiedzialne są różne ustawienia konfiguracyjne NIOC:

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

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

Pule zasobów sieciowych

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

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

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

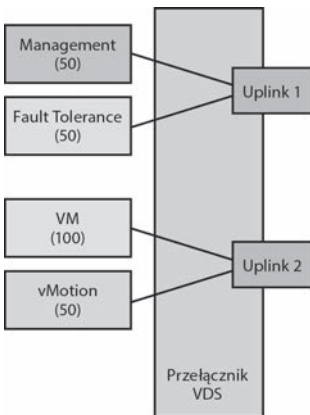
- **Host Limit (Mbps)** (limit hosta w Mb/s). Limit ruchu określony w megabitach na sekundę, który nie może zostać przekroczony przez daną pulę zasobów sieciowych. W wersji vSphere 5.1 jest to limit dla każdego uplinku, podczas gdy w wersjach wcześniejszych był to limit dla każdego hosta. Jeśli w przełączniku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

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

Udziały

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

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



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

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

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

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

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

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

Pule zasobów sieciowych definiowane przez użytkownika

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

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

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

The screenshot shows the 'VDS-Core' interface with the 'Manage' tab selected. The 'Resource Allocation' sub-tab is active, displaying a table of network resource pools. The table is divided into 'System network resource pools' and 'User-defined network resource pools'.

Network Resource Pool	Host Limit (Mbps)	Physical Adapter Shares	Shares Value	QoS Priority Tag
System network resource pools				
Fault Tolerance (FT) Traffic	Unlimited	Normal	50	
vSphere Replication (VR) Traffic	Unlimited	Normal	50	
iSCSI Traffic	Unlimited	Normal	50	
Management Traffic	Unlimited	Normal	50	
NFS Traffic	Unlimited	Normal	50	
Virtual Machine Traffic	Unlimited	High	100	
vMotion Traffic	500	Normal	50	
vSphere Storage Area Network Traffic	Unlimited	Normal	50	
User-defined network resource pools				
Production VMs	Unlimited	Custom	100	

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

The screenshot shows the 'VM-1 - Edit Settings' dialog box. The 'General' tab is selected. The 'Network resource pool' dropdown menu is open, showing the selection of 'Production VMs'.

Fields visible in the dialog:

- Name: VM-1
- Port binding: Static binding
- Port allocation: Elastic
- Number of ports: 40
- Network resource pool: Production VMs
- Description: (empty)

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

Podsumowanie

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

Skorowidz

A

ACL, Access Control List, 277
adapter, 104
 HBA, 72, 258
 iSCSI, 234, 258
 niezależny sprzętowy, 237
 programowy, 235
 zależny sprzętowy, 236
sieciowy, 82, 162, 194, 278,
 290, 298, 305
wirtualny, 84, 105
adres
 IP, 107
 IPv4, 215, 256
 MAC, 42
 efektywny, 94
 multicast, 43
 początkowy, 94
 MAC, 42
 uruchomieniowy, 94
adresowanie, 42, 65
 bezklasowe, 66
 klasowe, 65
adresy
 sieci iSCSI, 250
 sieci NFS, 287
 zarezerwowane, 67
agregacja łącz, 47, 56, 282
algorytm
 back-off, 39
 CSMA/CD, 38

LBT, 197

Round Robin, 269
szeregowania WRRS, 190
aplikacje vSphere Web Client, 156
architektura
 Cisco UCS, 74
 multi-NIC vMotion, 309
 SAN, 245
 sieci, 27
ARP, Address Resolution
 Protocol, 33, 69
ARPANET, 28
awaria uplinku, 103
awarie sieci, 102

B

bezklasowy routing
 międzydomenowy, 66
bezpieczeństwo, 277
bezpieczeństwo vSwitch, 93
 fałszywe transmisje, 95
 tryb mieszany, 93
 zmiany adresu MAC, 93
BladeSystem firmy HP, 75
błąd PEBKAC, 31
bootowanie
 z architektury SAN, 245
 z iSCSI, 243
brama domyślna, 64
burza broadcastowa, 51

C

CAM, Content Addressable
 Memory, 45
CDP, Cisco Discovery Protocol,
 96, 112, 222
cele iSCSI, 261, 263
CHAP, Challenge Handshake
 Authentication Protocol, 233
CIDR, Classless Inter-Domain
 Routing, 66
CLI, Command Line Interface,
 288
CNA, Converged Network
 Adapter, 237
CoS, Class of Service, 226, 272
Cross-Stack EtherChannel, 58
czas życia pakietu, TTL, 51

D

demon SSH, 288
demony, 274
DHCP, Dynamic Host
 Configuration Protocol, 68
DHCP snooping, 135
DNS, Domain Name System, 68
dodawanie
 adapterów sieciowych, 290
 hostów, 207
 hostów vSphere, 206
 urządzeń iSCSI, 261

domena
kolizyjna, 44
rozgłoszeniowa, 45

dostępność, 56

dupleks, 44

dvUplink, 110

dynamiczna

agregacja łączy, 59

grupa LAG, 59

dynamiczny EtherChannel, 58

dystrybucja obciążenia, 61

działanie

przełącznika, 45, 90

Spanning Tree, 52

E

efekt sieci, 23

egress, 49

EST, External Switch Tagging, 85

EtherChannel, 57

Ethernet, 37

EUC, End User Computing, 278

F

falszywe transmisje, 95

FEX, fabric extender, 74

fiber, 39

forwarding, 64

funkcja

Add Networking, 173

Health Check, 220, 221

iBFT, 244

Manage host networking, 213

NetFlow, 113

NIC Teaming, 239

NIOC, 129, 190

Port Mirroring, 115, 117, 118

PortFast, 54, 55

Teaming and failover, 100

TOE, 278

funkcje

przełącznika, 90

zaawansowane adapterów

sieciowych, 151

zaawansowane Nexus
1000V, 145
funkcjonalność QoS, 161, 188

G

Gigabit Ethernet, 39

grupa

agregacji łączy, 282

portów, 316

dla maszyn wirtualnych,
195

iSCSI, 251

rozproszona, 195

VM, 107, 164, 195

H

HBA, Host Bus Adapter, 258

HCL, Hardware Compatibility
List, 152, 244, 278

hub, 24

I

ICMP, Internet Control
Message Protocol, 33, 69

identyfikator

mostka, 52

OUI, 43

VLAN ID, 164, 166

IGMP, Internet Group Message
Protocol, 33

informowanie przełączników,
103

infrastruktura konwergentna, 71

ingress, 49

inicjatory, 230

interfejs

DCUI, 212

logiczny, 58

Port Channel, 58

interfejsy sieciowe, 105

IP, Internet Protocol, 28

IQN, 232

iSCSI, 225

cele, 230

inicjatory, 230

nazewnictwo, 231

izolacja za pomocą sieci VLAN,
228, 273

J

jednostka LUN, 266, 267

K

kabel

DAC, 40

Ethernet, 39

miedziany, 40

światłowodowy, 39

twinakowy, 40, 42

UTP, 41

kanał EtherChannel, 59

kapsułkowanie, encapsulation, 29

klasa

A, 65

B, 65

C, 65

klastrowanie, 77

klient NFS, 276

klucz tajny, 233

kolejność przełączania

awaryjnego, 104, 167, 205, 254

kolizja, 38

komponenty

iSCSI, 229

NFS, 274

koncentrator, 24, 43

konfiguracja

adaptera sieciowego, 256

hostów vSphere, 183

magazynu danych NFS, 294

multi-NIC vMotion, 316

NetFlow, 114

NIC Teaming, 100

NIOC, 129

pamięci masowej iSCSI, 247

pamięci masowej NFS, 285

przełącznika vSwitch, 251, 288

reguł bezpieczeństwa, 183

sieci, 162

konfiguracja

- sieci wirtualnej, 149
- sześciouplinkowa
 - przełącznika, 303
- uwierzytelniania, 265
- uwierzytelniania CHAP, 234
- właściwości portu, 292
- znacznika VLAN, 87

konserwacja hosta, 310

konwergentny adapter sieciowy,
CNA, 237

konwerter interfejsu
gigabitowego, 40

kopia bazy danych, 111

koszt STP, 53

kreator dodawania nowego
portu, 291

kształtowanie ruchu, 97, 99,
125, 318

Egress, 125

L

laboratorium demonstracyjne,
153

LACP, Link Aggregation
Control Protocol, 59

LAG, Link Aggregation Group,
57, 282

LAN, 47

LBT, Load Based Teaming, 197

licencja

- Advanced Edition, 146
- Essential Edition, 146

liczba modułów VEM, 145

lista

- ACL, 277
- adapterów sieciowych, 244
- adapterów VMkernel, 255
- portów VMkernel, 175

LLDP, Link Layer Discovery
Protocol, 112

logika

- dystrybucji obciążenia, 60
- przełączania, 45

LOM, LAN On Motherboard, 152

LSB, Least Significant Bit, 283

M

macierz pamięci masowej,
179, 275

magazyn danych
NFS, 294
VMFS, 266

magistrala, 38

maska podsieci, 66, 215, 256

maskowanie, 230

maszyna wirtualna, 61, 125
vCenter Server, 215, 217

mechanizm PFC, 226

medium

- komunikacyjne, 38, 39
- transmisyjne, 43

metoda

- białych rękawiczek, 207
- młota, 207

metody implementacji, 57

migracja maszyny wirtualnej,
211, 220

migracja

- portu, 210, 219
- sieci, 211

mirrorowanie, 117

model sieciowy, 27

- OSI, 30
- TCP/IP, 28, 32

moduł

- GBIC, 42
- SFP/SFP+, 42
- VEM, 137, 142
- VSM, 138

monitorowanie, 116

- pamięci masowej NFS, 293

mostek główny, 52

MTU, Maximum Transmission
Unit, 92, 152, 228, 260

Multi-Chassis Link
Aggregation, 58

multi-NIC vMotion, 309

N

nadpisywanie hierarchii, 104
najmniej znaczący bit, 283

narzędzie

- BPDU, 55
- BPDU Guard, 55
- Filtering, 55

nazwa

- sieci, 153
- IQN, 232

NFS, Network File System, 271,
273, 285

NIC bonding, 58

NIC teaming, 58, 99

NIOC, 129, 188, 190, 312

O

obciążenie typu src-dst-ip, 61

obsługa awarii vCenter, 111

odciążenie segmentacji TCP, 151

odczytywanie nośnej, 39

odrzućcie ramek, discarding, 55

oktet, 65

opcje

- funkcji Port Mirroring, 117
- konfiguracji NetFlow, 115

operacje we/wy sieci, 129, 188

opóźnienie, latency, 226

organizacja

- ICANN, 34
- IEEE, 43

VMware User Group, 321

OUI, Organizationally Unique
Identifier, 43

P

PAGP, Port Aggregation
Protocol, 58, 60

pamięć

- CAM, 45
- masowa
- sieci Ethernet, 300
- masowa NFS, 279–285

panel obudowy HP

- BladeSystem, 77

parametr MTU, 260

PCP, Priorytet Code Point, 190

PDU, Protocol Data Unit, 29

- pętla warstwy drugiej, 47
- PFC, Priority-based Flow Control, 226, 272
- platforma BladeSystem, 75
- plik exports, 274
- pliki .vmdk, 272
- podsielowanie IP, 65
- pole VLAN ID, 50
- polecenie
 - no ip classless, 65
 - ping, 52, 69
- połączenia typu upstream, 40
- porównanie
 - modeli sieciowych, 34
 - przełączników, 79
- port, 34
 - 0, 34
 - aktywny, 53
 - alternatywny, 55
 - brzegowy, 54
 - dostępu, access port, 49
 - dvUplink, 110
 - elastyczny, 84
 - FT, 177
 - główny, 53
 - iSCSI, 251
 - Management VMkernel, 172
 - maszyny wirtualnej, 164, 197
 - NFS Storage, 180
 - prywatny, 34
 - przełączania awaryjnego, 57
 - sieciowy, 299, 301
 - usługi, 105
 - vmk0, 170
 - VMkernel, 84, 105, 124, 169, 173, 200, 212, 254, 291, 317
 - vMotion, 174
 - w trybie trunkingowym, 50
 - wirtualny, 83
 - właściwości, 105
 - wyznaczony, 53
 - zablokowany, 53
 - zapasowy, 55
 - zarejestrowany, 34
- PortFast, 54
- poświadczenia
 - uwierzytelniania, 265
- poziom zabezpieczeń, 233
- półdupleks, 44
- prawo Metcalfe'a, 23
- prędkość transmisji, 53
- prorytetyzowane sterowanie przepływem, 226
- profile portów, 140
- programowy adapter iSCSI, 258
- projekt
 - fizycznego przełącznika upstream, 315
 - hostów, 151
 - iSCSI, 206, 238, 247
 - adresy sieciowe, 250
 - konwencje nazewnictwa, 249
 - przypadek użycia, 248
 - LAG, 283
 - NFS, 278
 - adaptory sieciowe, 290
 - adresy sieciowe, 287
 - konwencje nazewnictwa, 286
 - porty VMkernel, 291
 - przypadek użycia, 285
 - OSI, 28
 - pojedynczego przełącznika vSwitch, 242
 - pojedynczej sieci, 279
 - przełącznika
 - adaptory sieciowe, 163, 194, 298
 - dodawanie hostów, 183, 206
 - Distributed vSwitch, 185, 191
 - funkcja Health Check, 220
 - funkcjonalność QoS, 161, 188
 - konwencje nazewnictwa, 158, 187
 - model bez pamięci masowej, 302
 - model z pamięcią masową, 302
 - przypadek użycia, 158, 186, 297
 - rozproszony vSwitch, 312
 - standardowego vSwitch, 157, 241, 315
 - standardy nazewnictwa, 298
 - sześć portów, 301
 - usługa DSCP, 191
 - usługa Fault Tolerance, 176, 203
 - usługa iSCSI Storage, 204
 - usługa Management, 169, 200
 - usługa NFS Storage, 178
 - usługa vMotion, 172, 202
 - ustawienia
 - bezpieczeństwa, 182
 - ruchu danych, 152
 - sieci, 150
 - vMotion, 310
 - kontrolowanie ruchu, 312
 - kształtowanie ruchu, 318
 - przepustowość, 311
 - wielu sieci, 281
 - projektowanie
 - hybrydowe automatyczne, 224
 - zautomatyzowane, 223
 - protokoły
 - bezzstratne, 226, 272
 - typu best effort, 226, 272
- protokół, 27
 - ARP, 33, 69
 - CDP, 96, 112, 222
 - CHAP, 232, 264
 - DHCP, 68
 - Fibre Channel, 39
 - ICMP, 33, 69
 - IGMP, 33
 - IP, 33
 - iSCSI, 225
 - LACP, 57, 59
 - LLDP, 113
 - NFS, 271
 - PagP, 60
 - RSTP, 55
 - Spanning Tree, 172
 - STP, 52
 - TCP, 33
 - TCP/IP, 28
 - UDP, 33

próbkowanie źródeł, 120
 prywatne sieci VLAN, 121
 przechwytywanie, 116
 przekazywanie ramek,
 forwarding, 55
 przełączanie
 awaryjne, 104
 kolejność, 167, 205
 ustawienia, 181, 204
 fizyczne, 79
 wirtualne, 79
 przełącznik, 43
 aktualizowanie tablicy
 adresów, 103
 architektura Nexus 1000V,
 137
 Cisco, 57
 dodawanie hostów, 207
 dodawanie nowej sieci, 165
 dwuuplinkowy, 299
 fabric interconnect, 73–77
 fałszywe transmisje, 95
 funkcja NetFlow, 113
 funkcja Port Mirroring, 115
 funkcje zaawansowane, 145
 grupy portów, 107
 kształtowanie ruchu, 97, 125
 moduł VEM, 142
 moduł VSM, 137
 monitorowanie, 112
 MTU, 92
 nadpisywanie hierarchii, 104
 Nexus 1000V, 135
 obsługa awarii, 111
 opcja Failback, 103
 opcja Notify switches, 103
 ośmiouplinkowy, 307
 płaszczyzna danych, 90, 112
 płaszczyzna sterowania,
 90, 110
 porty, 91
 profile portów, 140
 projekt Distributed
 vSwitch, 185
 projekt Standard vSwitch,
 157

przełączanie awaryjne, 104,
 167
 rozproszone grupy portów,
 123
 rozproszony vSwitch, 197
 równoważenie obciążenia,
 100, 126
 sondowanie ramek beacon,
 102
 sterowanie operacjami
 we/wy, 129
 Storage_Switch, 289, 293
 tryb mieszany, 93
 tryb warstwy drugiej, 143
 tryb warstwy trzeciej, 144
 tryby licencjonowania, 146
 upstream, 75, 77, 315
 ustawienia bezpieczeństwa,
 92
 VMware, 89
 vSphere Distributed Switch,
 109–134
 vSphere Standard Switch,
 89–108
 vSwitch, 135, 251, 288, 297,
 312, 315
 wirtualny, 61, 81
 wykrywanie, 95
 zmiany adresu MAC, 93
 przenoszenie maszyny
 wirtualnej, 215
 przepustowość, 56
 szczytowa, 98
 średnia, 97
 przypadki użycia
 protokołu iSCSI, 225
 protokołu NFS, 271
 multi-NIC vMotion, 309
 pule zasobów sieciowych, 130,
 132
 punkty montowania, 275
 PXE, Preboot Execution
 Environment, 54

Q

QoS, Quality of Service, 161

R

ramka
 beacon, 102
 Ethernet, 49
 IEEE 802.3, 80
 iSCSI, 227
 jumbo, 229, 260, 273
 RARP, 103
 Rapid Spanning Tree, 55
 RARP, Reverse Address
 Resolution Protocol, 103
 RDM, Raw Device Mapping, 269
 redundancja, 56, 151
 regenerator sygnału, 43
 reguła
 bezpieczeństwa, 183
 egress, 314
 przełączania awaryjnego, 171
 PSP, 241, 268
 reprezentacja binarna adresu, 67
 rodzaje
 dystrybucji obciążenia, 60
 kabli, 39
 reguł PSP, 241
 role STP, 53, 54
 routing, 64
 ogłoszeniowy adres
 docelowy, 43
 rozłożenie obciążenia, 56
 rozmiar
 największego datagramu, 92
 serii, 98
 rozproszone
 grupy portów, 123, 205, 316
 iSCSI, 251
 VM, 199
 uplinki, 209
 rozproszony przełącznik, 197
 vSwitch, 207–209, 312
 równoległy NFS, 278
 równoważenie obciążenia, 100,
 126
 RSTP, Rapid Spanning Tree
 Protocol, 55

ruch

- Fibre Channel, 227
- ingress, 130
- Management, 172
- maszyn wirtualnych, 164
- szarej strefy, 83
- vMotion, 173
- wchodzący, 49
- wychodzący, 49

S

scenariusz laboratoryjny, 153

Service Console, 84

serwer

- DHCP, 68
- DNS, 68
- iSCSI, 262, 263
- vCenter, 155

sesja Encapsulated Remote

- Mirroring, 120

sieci klasowe, 66

sieć

- DMZ, 305
- Ethernet, 37
- iSCSI, 251
- pakietowa, 138
- sterowania, 139
- typu single-link, 23
- VLAN, 85, 121
- zarządzania, 138

skanowanie programowego

- adaptera, 263

skrętka nieekranowana, 39

sneakernet, 22

sondowanie ramek beacon, 102

Spanning Tree, 51, 52

sprawdzanie przepustowości,
311

SSH, Secure Shell, 169

standard

- Gigabit Ethernet, 39
- IEEE 802.1ax, 57
- IEEE 802.1D, 52
- IEEE 802.1p, 190
- IEEE 802.1Qbb, 226
- IEEE 802.3ad, 57
- SFP+, 40

standardy sieci Ethernet, 41

stany adapterów, 104

status VLAN-ów, 222

statyczna grupa LAG, 59

statyczny EtherChannel, 57

sterowanie

- operacjami we/wy sieci, 188
- przepływem, 226

STP, Spanning Tree Protocol, 51

switch, *Patrz* przełącznik

system

- operacyjny Nexus OS, 145
- plików, 272
- UCS, 73

Ś

środowisko

- inżynieryjne, 261
- produkcyjne, 261
- projektowania, 261
- PXE, 54

światłowód, 39

- jednomodowy, 40

- wielomodowy, 40

T

tabela routingu, 64, 240

tablica adresów MAC, 103

TCP, Transmission Control
Protocol, 28

teaming, 99

technologia Virtual Connect, 76

tłumienie, 43

TOE, TCP Offload Engine, 237,
278

topologia sieci, 229

transceivery SFP, 40

transmisja, 39

trasa

- automatyczna, 64
- domyślna, 64
- dynamiczna, 64
- ostatniego wyboru, 64
- statyczna, 64

Trunk, 58

trunking, 50

tryb

- mieszany, 93
- warstwy drugiej, 143
- pracy licencjonowany, 146

trzepotanie, 280

TSO, TCP Segmentation

- Offload, 151

tworzenie

- magazynów danych, 266
- portów VMkernel, 212, 213
- sieci wirtualnej, 149

typy

- adapterów sieciowych
- iSCSI, 234
- adresów MAC, 43
- sieci, 138
- użytkowników, 277

U

UCNA, Universal CNA, 237

UCS, Unified Computing
System, 73

uczenie się adresów MAC, 55

udziały, 131

unikatowe adresy MAC, 42

uplink, 110

uplinki fizyczne, 82

uruchamianie demona SSH, 288

usługa

- DSCP, 191
- Fault Tolerance, 176, 203
- iSCSI Storage, 204
- Management, 169, 200
- NFS Storage, 178
- SSH, 288
- vMotion, 172, 202
- vMotion traffic, 214
- VMkernel, 150

usługi portów, 105

ustawienia

- IPv4, 175
- przełączania awaryjnego, 181

uwierzelnianie, 263

- celu, 264

- CHAP, 234, 265

- wykrywania, 264

V

VBCA, Virtual Business Critical Application, 278
 VEM, Virtual Ethernet Module, 137
 VGT, Virtual Guest Tagging, 86
 Virtual Computing Platform, 76
 Virtual Connect, 76
 VLAN, Virtual LAN, 47
 mieszany, 121
 natywny, 51
 podstawowy, 121
 podrzędny, 121
 typu community, 122
 typu isolated, 123
 VLSM, Variable-Length Subnet Masking, 66
 VM, virtual machines, 61
 VMFS, Virtual Machine File System, 266, 272
 VMware User Group, 321
 VSM, Virtual Supervisor Module, 137
 vSphere Distributed Switch, 109
 vSphere Standard Switch, 89
 VST, Virtual Switch Tagging, 85

W

warstwa
 aplikacji, 31, 34
 czwarta, 31
 dostępu, 26
 dostępu do sieci, 32
 druga, 31, 47
 dystrybucji, 25
 fizyczna, 30
 internetowa, 32
 łącza danych, 31
 ósma, 31
 piąta, 31
 pierwsza, 30
 prezentacji, 31
 rdzenia, 25
 sesji, 31
 sieciowa, 31, 63, 68
 siódma, 31
 szósta, 31
 transportowa, 31, 33
 trzecia, 31, 63
 warstwowanie, 29
 warstwy
 modelu OSI, 30
 modelu TCP/IP, 32
 wbudowany adapter sieciowy, 152
 wiązanie portu sieciowego, 240, 257
 wielodostęp, 39
 wirtualne
 karty sieciowe, 127
 sieci LAN, 47, 48

wirtualny

 klaster obliczeniowy, 76
 moduł ethernetowy, VEM, 142
 moduł zarządzający, VSM, 137
 własna sieć wirtualna, 149
 właściwości
 portu, 105, 173, 292
 portu VMkernel, 174, 177, 180
 przełącznika vSwitch, 91
 współdzielone łącze, 38
 WWN, World Wide Name, 75
 wykrywanie
 awarii sieci, 102
 dynamiczne, 231
 kolizji, 39
 sieci, 222
 statyczne, 231

Z

zabezpieczenia CHAP, 233
 zagnieżdżona wirtualizacja, 95
 zalety infrastruktury
 konwergentnej, 72
 zarządzanie
 hostem, 170
 warstwą, 29
 zdalna karta liniowa, 74
 złącza kablowe, 42
 złącze
 RJ-45, 40
 światłowodowe LC, 41
 światłowodowe SC, 41
 zmiany adresu MAC, 93
 znacznik VLAN, 87
 znakowanie
 EST, 85
 priorytetów, 190
 VGT, 86
 VLAN-ów, 152
 VST, 85

PROGRAM PARTNERSKI

GRUPY WYDAWNICZEJ HELION



1. ZAREJESTRUJ SIĘ
2. PREZENTUJ KSIĄŻKI
3. ZBIERAJ PROWIZJĘ

Zmień swoją stronę WWW
w działający bankomat!

Dowiedz się więcej i dołącz już dzisiaj!

<http://program-partnerski.helion.pl>

GRUPA WYDAWNICZA



Helion SA

Obowiązkowa lektura dla administratorów sieci komputerowych!

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

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

DZIĘKI TEJ KSIĄŻCE:

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

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

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



35313 numer katalogowy
księgarnia internetowa

<http://helion.pl>

zamówienia telefoniczne



0 801 339900



0 601 339900

Informatyka w najlepszym wydaniu

Sprawdź najnowsze promocje:
❶ <http://helion.pl/promocje>
❷ książki najchętniej czytane:
❸ <http://helion.pl/bestsellery>
Zamów informacje o nowościach:
❹ <http://helion.pl/nowości>

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

sięgnij po WIĘCEJ



KOD KORZYŚCI

ISBN 978-83-283-0696-7



9 788328 306967

cena: 67,00 zł