

J.C. Mackin
Tony Northrup

Egzamin MCTS 70-642: Konfigurowanie infrastruktury sieciowej Windows Server® 2008 R2 Training Kit

Wydanie 2

Przekład: Maria Chaniewska, Janusz Machowski

APN Promise
Warszawa 2011

Egzamin MCTS 70-642: Konfigurowanie infrastruktury sieciowej Windows Server® 2008 R2
Training Kit, Wydanie 2
© 2011 APN PROMISE SA

Authorized Polish translation of English edition of
MCTS Self-Paced Training Kit (Exam 70-642): Configuring Windows Server® 2008 Network
Infrastructure (Second Edition), ISBN: 978-0-7356-5160-9
Copyright © 2011 by Tony Northrup and J.C. Mackin
This translation is published and sold by permission of O'Reilly Media, Inc., which owns
or controls all rights to publish and sell the same.

APN PROMISE SA, biuro: ul. Kryniczna 2, 03-934 Warszawa
tel. +48 22 35 51 600, fax +48 22 35 51 699
e-mail: mspress@promise.pl

Wszystkie prawa zastrzeżone. Żadna część niniejszej książki nie może być powielana
ani rozpowszechniana w jakiegokolwiek formie i w jakikolwiek sposób (elektroniczny,
mechaniczny), włącznie z fotokopiowaniem, nagrywaniem na taśmy lub przy użyciu innych
systemów bez pisemnej zgody wydawcy.

Książka ta przedstawia poglądy i opinie autora. Informacje i widoki przedstawione w tym
dokumencie, w tym adresy URL i inne odniesienia do witryn internetowych, mogą być
zmieniane bez powiadomienia. Państwo sami ponoszą ryzyko związane z ich wykorzystywaniem.
Przykłady firm, produktów, osób i wydarzeń opisane w niniejszej książce są fikcyjne i nie
odnoszą się do żadnych konkretnych firm, produktów, osób i wydarzeń. Ewentualne
podobieństwo do jakiegokolwiek rzeczywistej firmy, organizacji, produktu, nazwy domeny, adresu
poczty elektronicznej, logo, osoby, miejsca lub zdarzenia jest przypadkowe i niezamierzone.

Microsoft oraz znaki towarowe wymienione na stronie <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> są zastrzeżonymi znakami towarowymi grupy
Microsoft. Wszystkie inne znaki towarowe są własnością ich odnośnych właścicieli.

APN PROMISE SA dołożyła wszelkich starań, aby zapewnić najwyższą jakość tej publikacji.
Jednakże nikomu nie udziela się rękojmi ani gwarancji.
APN PROMISE SA nie jest w żadnym wypadku odpowiedzialna za jakiegokolwiek szkody
będące następstwem korzystania z informacji zawartych w niniejszej publikacji, nawet jeśli
APN PROMISE została powiadomiona o możliwości wystąpienia szkód.

ISBN: 978-83-7541-093-8

Przekład: Maria Chaniewska, Janusz Machowski
Redakcja: Marek Włodarz
Korekta: Ewa Swędrowska
Skład i łamanie: MAWart Marek Włodarz

Egzamin 70-642: MCTS: Windows Server® 2008 Network Infrastructure, Configuring

Zagadnienie	Rozdział	Lekcja
1. Konfigurowanie adresowania i usług IP		
1.1 Konfigurowanie adresowania IPv4 i IPv6	1	2, 3
1.2 Konfigurowanie DHCP (Dynamic Host Configuration Protocol)	4	1, 2
1.3 Konfigurowanie routingu	5	1
1.4 Konfigurowanie IPsec	6	1
	8	1
2. Konfigurowanie rozpoznawania nazw		
2.1 Konfigurowanie serwera DNS (Domain Name System)	2	2
2.2 Konfigurowanie stref DNS	3	1, 3
2.3 Konfigurowanie rekordów DNS	3	1
2.4 Konfigurowanie replikacji DNS	3	2
2.5 Konfigurowanie rozpoznawania nazw dla komputerów klienckich	2	3
3. Konfigurowanie dostępu sieciowego		
3.1 Konfigurowanie zdalnego dostępu	7	2, 3
3.2 Konfigurowanie NAP (Network Access Protection)	8	2
3.3 Konfigurowanie DirectAccess	7	4
3.4 Konfigurowanie Network Policy Server (NPS)	7	1
4. Konfigurowanie usług plików i drukowania		
4.1 Konfigurowanie serwera plików	11	1, 2
4.2 Konfigurowanie DFS (Distributed File System)	11	2
4.3 Konfigurowanie tworzenia i przywracania kopii zapasowych	11	3
4.4 Zarządzanie zasobami serwera plików	11	2
4.5 Konfigurowanie i monitorowanie usług drukowania	12	1
5. Monitorowanie i zarządzanie infrastrukturą sieci		
5.1 Konfigurowanie ustawień serwera WSUS (Windows Server Update Services)	9	1, 2
5.2 Konfigurowanie monitorowania wydajności	10	1, 2
5.3 Monitorowanie dzienników zdarzeń	10	1
5.4 Zbieranie danych sieciowych	10	1, 2, 3
	6	1

Uwaga: Przedstawione tu cele egzaminu są obowiązujące w momencie publikacji tej książki. Mogą ulec zmianie w dowolnym momencie i bez wcześniejszego powiadomienia. Najbardziej aktualna lista zagadnień egzaminacyjnych znajduje się na witrynie Web Microsoft Learning Certification (www.microsoft.com/learning/mcp/).

Spis treści

Wstęp	xv
Przygotowanie do egzaminu	xxi
1 Działanie i konfiguracja TCP/IP	1
Przed rozpoczęciem	1
Lekcja 1: Wprowadzenie do działania sieci w systemie Windows	3
Pojęcie warstw sieci	3
Warstwy modelu sieciowego TCP/IP	5
Konfigurowanie właściwości w systemie Windows Server 2008 R2.....	15
Zadanie: Konfigurowanie adresów TCP/IP	34
Podsumowanie lekcji	37
Pytania do lekcji	37
Lekcja 2: Adresowanie IPv4	38
Struktura adresów IPv4	39
Działanie routingu i bram domyślnych	48
Zakresy adresów IPv4	49
Co to jest dzielenie na podsieci?	58
Zalety dzielenia na podsieci	60
Identyfikator podsieci	61
Tworzenie podsieci tego samego rozmiaru	62
Korzystanie z masek VLSM (Variable-Length Subnet Masks)	64
Wyznaczanie parametrów podsieci w przestrzeni adresów	65
Sprawdzanie poprawności konfiguracji podsieci i przynależności adresów	72
Zadanie: Nauka pracy z blokami adresowymi	73
Podsumowanie lekcji	79
Pytania do lekcji	80
Lekcja 3: Adresowanie IPv6	82
Wprowadzenie do adresów IPv6	82
Typy adresów IPv6	83
Przejściowe technologie IPv6	87
Stosowanie podsieci IPv6	91
Zadanie: Testowanie łączności IPv6	95
Podsumowanie lekcji	97
Pytania do lekcji	98
Przegląd rozdziału	100
Podsumowanie rozdziału	100
Terminy kluczowe	101
Scenariusz przykładowy.....	101

Scenariusz przykładowy: Praca z blokami adresów IPv4	101
Proponowane zadania praktyczne	102
Konfigurowanie adresowania IP	102
Test ćwiczeniowy	102
2 Konfigurowanie rozpoznawania nazw	103
Przed rozpoczęciem	103
Lekcja 1: Rozpoznawanie nazw w sieciach Windows Server 2008	105
Metody rozpoznawania nazw w systemie Windows.....	105
Co to jest Link Local Multicast Name Resolution (LLMNR)?.....	106
Co to jest NetBIOS Name Resolution?.....	110
Co to jest rozpoznawanie nazw DNS?	114
Komponenty DNS.....	116
Sposób działania kwerend DNS.....	117
Sposób działania buforowania.....	124
Zadanie: Poznanie automatycznego rozpoznawania nazw w sieciach lokalnych.....	125
Podsumowanie lekcji	127
Pytania do lekcji	128
Lekcja 2: Wdrażanie serwera DNS.....	129
Wdrożenie serwera DNS na kontrolerze domeny	129
Wdrożenie DNS Server na samodzielnym komputerze lub na serwerze członkowskim	132
Wdrożenie DNS Server na instalacji Server Core systemu Windows Server 2008 R2	133
Konfigurowanie tylko buforującego serwera DNS.....	135
Konfigurowanie właściwości serwera	136
Konfigurowanie puli gniazd DNS.....	142
Konfigurowanie blokady pamięci podręcznej DNS.....	143
Zadanie: Eksplorowanie DNS w środowisku Active Directory.....	143
Podsumowanie lekcji	148
Pytania do lekcji	149
Lekcja 3: Konfigurowanie ustawień klienta DNS.....	150
Określanie serwerów DNS	150
Określanie nazwy komputera i sufiksów DNS.....	152
Konfigurowanie listy sufiksów wyszukiwania	154
Konfigurowanie ustawień aktualizacji dynamicznych	156
Wyświetlanie i czyszczenie bufora klienta DNS.....	159
Zadanie: Zarządzanie buforem klienta DNS.....	160
Podsumowanie lekcji	160
Pytania do lekcji	161
Przegląd rozdziału.....	163
Podsumowanie rozdziału	163
Określenia kluczowe	163
Scenariusze przykładowe	164

Scenariusz przykładowy 1: Rozwiązywanie problemów z klientami DNS.....	164
Scenariusz przykładowy 2: Wdrożenie serwera DNS.....	165
Proponowane zadania praktyczne	165
Konfigurowanie serwera DNS	165
Konfigurowanie rozpoznawania nazw dla komputerów klienckich	165
Test ćwiczeniowy	166
3 Konfigurowanie infrastruktury stref DNS.....	167
Przed rozpoczęciem	167
Lekcja 1: Tworzenie i konfigurowanie stref.....	169
Tworzenie stref	169
Sprawdzanie wbudowanych rekordów zasobów.....	177
Tworzenie rekordów zasobów.....	180
Włączanie rozpoznawania nazw WINS przez usługę DNS.....	186
Przedawianie i oczyszczanie.....	186
Korzystanie ze strefy GlobalNames	190
Zadanie: Wdrażanie strefy GlobalNames.....	191
Podsumowanie lekcji	193
Pytania do lekcji	194
Lekcja 2: Konfigurowanie replikacji, transferów i delegowania stref.....	195
Konfiguracja replikacji strefy dla stref zintegrowanych z Active Directory.....	195
Używanie transferów stref	200
Delegowanie stref.....	203
Implementacja stref skrótowych.....	206
Zadanie: Tworzenie partycji katalogu aplikacji dla DNS.....	208
Zadanie: Wdrażanie strefy pomocniczej	209
Podsumowanie lekcji	212
Pytania do lekcji	212
Lekcja 3: Implementowanie DNSSEC	214
Szyfrowanie z użyciem klucza publicznego w DNSSEC	214
Rozpoznawanie nazw DNSSEC	217
Konfigurowanie DNSSEC	224
Zadanie: Konfigurowanie DNSSEC.....	232
Podsumowanie lekcji	235
Pytania do lekcji	236
Przegląd rozdziału.....	237
Podsumowanie rozdziału	237
Określenia kluczowe	238
Scenariusze przykładowe	238
Scenariusz przykładowy 1: Zarządzanie przestarzałymi danymi strefy	239
Scenariusz przykładowy 2: Konfigurowanie transferów stref	239
Proponowane zadania praktyczne	239
Konfigurowanie infrastruktury DNS	239
Test ćwiczeniowy	240

4 Tworzenie infrastruktury DHCP	241
Przed rozpoczęciem	241
Lekcja 1: Instalacja serwera DHCP	242
Przyznawanie adresów DHCP	242
Dodawanie roli serwera DHCP	245
Zadanie: Wdrożenie serwera DHCP	254
Podsumowanie lekcji	256
Pytania do lekcji	256
Lekcja 2: Konfiguracja serwera DHCP	258
Wykonywanie zadań poinstalacyjnych	258
Klasy opcji DHCP	263
Kontrola dostępu do DHCP za pomocą filtrowania adresów MAC	266
Konfigurowanie opóźnienia usługi DHCP	268
Używanie kreatora konfiguracji podziału zakresu DHCP	268
Konfigurowanie wykonywania aktualizacji dynamicznych DNS przez DHCP dla klientów	270
Instalacja i konfiguracja DHCP na instalacji Server Core	273
Zadanie: Tworzenie zakresu wykluczania	274
Podsumowanie lekcji	274
Pytania do lekcji	275
Przegląd rozdziału	276
Podsumowanie rozdziału	276
Terminy kluczowe	276
Scenariusze przykładowe	277
Scenariusz przykładowy 1: Wdrożenie nowego serwera DHCP	277
Scenariusz przykładowy 2: Konfigurowanie opcji DHCP	277
Proponowane zadania praktyczne	278
Konfigurowanie DHCP	278
Test ćwiczeniowy	278
5 Konfigurowanie routingu IP	279
Przed rozpoczęciem	279
Lekcja 1: Routing	280
Omówienie doboru tras	280
Badanie tras w sieci	282
Protokoły routingu	283
Routing statyczny	288
Zadanie: Analizowanie i konfigurowanie routingu	293
Podsumowanie lekcji	297
Pytania do lekcji	297
Przegląd rozdziału	299
Podsumowanie rozdziału	299
Terminy kluczowe	299
Scenariusze przykładowe	299

Scenariusz przykładowy 1: Dodawanie drugiej bramy domyślnej	299
Scenariusz przykładowy 2: Dodawanie nowej podsieci	300
Proponowane zadania praktyczne	301
Test ćwiczeniowy	301
6 Ochrona ruchu sieciowego za pomocą IPsec	303
Przed rozpoczęciem	303
Lekcja 1: Konfigurowanie IPsec	305
Co to jest IPsec?	305
Stosowanie IPsec w trybie tunelu	310
Metody uwierzytelniania w IPsec	311
Przypisywanie predefiniowanej zasady IPsec	312
Tworzenie nowej zasady IPsec	313
Tworzenie i konfigurowanie reguły zabezpieczeń połączeń	318
Zadanie: Wdrażanie IPsec za pomocą zasad IPsec i reguły zabezpieczeń połączeń	323
Podsumowanie lekcji	329
Pytania do lekcji	330
Przegląd rozdziału	332
Podsumowanie rozdziału	332
Kluczowe terminy	332
Scenariusz przykładowy	333
Scenariusz przykładowy: Implementacja IPsec	333
Proponowane zadania praktyczne	333
Wdrożenie IPsec	333
Webcast	333
Test ćwiczeniowy	333
7 Przyłączanie się do sieci	335
Przed rozpoczęciem	336
Lekcja 1: Konfigurowanie serwera NPS	338
Standardy bezpieczeństwa bezprzewodowego	338
Sieci bezprzewodowe infrastrukturalne i ad hoc	340
Konfigurowanie infrastruktury klucza publicznego	341
Uwierzytelnianie sieci bezprzewodowych za pomocą Windows Server 2008 R2 342	350
Łączenie z sieciami bezprzewodowymi	350
Wdrożenie sieci bezprzewodowych z WPA-EAP	351
Zabezpieczenia sieci przewodowej	352
Zadanie: Konfigurowanie uwierzytelniania WPA-EAP dla beziprzewodowego punktu dostępowego	354
Podsumowanie lekcji	359
Pytania do lekcji	360
Lekcja 2: Konfigurowanie NAT	361
Koncepcje translacji adresów sieciowych	361
Konfigurowanie Internet Connection Sharing	363

Konfigurowanie NAT za pomocą Routing And Remote Access.....	365
Rozwiązywanie problemów z NAT	368
Zadanie: Konfigurowanie NAT	368
Podsumowanie lekcji	369
Pytania do lekcji	370
Lekcja 3: Łączenie ze zdalnymi sieciami.....	371
Opis ogólny dostępu zdalnego.....	371
Konfigurowanie połączeń telefonicznych	374
Konfigurowanie połączeń VPN	380
Rozwiązywanie problemów z połączeniami VPN	384
Konfigurowanie ograniczeń połączeń	385
Testowanie łączności	387
Zadanie: Ustanowienie połączenia zdalnego dostępu VPN	391
Podsumowanie lekcji	393
Pytania do lekcji	394
Lekcja 4: Konfigurowanie DirectAccess.....	395
Typy połączeń DirectAccess	396
Używanie DirectAccess w sieciach IPv4	398
DirectAccess i rozpoznawanie nazw	398
Serwer NLS (Network Location Server)	399
Wymagania DirectAccess.....	400
Ograniczenia DirectAccess	401
Konfiguracja zapory systemu	401
Uruchamianie kreatora instalacji DirectAccess	402
Zadanie: Konfigurowanie DirectAccess.....	404
Podsumowanie lekcji	412
Pytania do lekcji	412
Przegląd rozdziału.....	414
Podsumowanie rozdziału	414
Terminy kluczowe	414
Scenariusze przykładowe	415
Scenariusz przykładowy 1: Łączenie biura oddziału z Internetem.....	415
Scenariusz przykładowy 2: Planowanie dostępu zdalnego.....	415
Proponowane zadania praktyczne	416
Konfigurowanie dostępu bezprzewodowego.....	416
Konfigurowanie dostępu zdalnego.....	417
Konfigurowanie uwierzytelniania sieci.....	417
Konfigurowanie DirectAccess	417
Test ćwiczeniowy	418
8 Konfigurowanie zapory Windows i mechanizmu NAP	419
Przed rozpoczęciem	419
Lekcja 1: Konfigurowanie Windows Firewall	421
Dlaczego zapory są ważne	421
Profile zapory.....	422

Filtrowanie ruchu przychodzącego.....	422
Filtrowanie ruchu wychodzącego.....	424
Konfigurowanie zakresu.....	426
Autoryzowanie połączeń.....	427
Konfigurowanie ustawień zapory za pomocą zasad grupy	428
Włączanie rejestrowania dla Windows Firewall.....	429
Identyfikacja komunikacji sieciowej.....	430
Zadanie: Konfiguracja Windows Firewall	431
Podsumowanie lekcji	433
Pytania do lekcji.....	434
Lekcja 2: Konfigurowanie NAP	435
Koncepcje NAP.....	436
Planowanie wdrożenia NAP.....	440
Instalowanie i konfigurowanie Network Policy Server	441
Konfigurowanie wymuszania NAP	444
Konfigurowanie komponentów NAP	454
Rejestrowanie NAP	466
Zadanie: Konfigurowanie wymuszania DHCP NAP	468
Podsumowanie lekcji	473
Pytania do lekcji.....	473
Przegląd rozdziału.....	475
Podsumowanie rozdziału	475
Określenia kluczowe	475
Scenariusze przykładowe	475
Scenariusz przykładowy 1: Badanie ustawień zapory.....	476
Scenariusz przykładowy 2: Planowanie NAP.....	476
Proponowane zadania praktyczne	477
Konfigurowanie ustawień zapory.....	477
Konfigurowanie NAP (Network Access Protection).....	477
Test ćwiczeniowy	478
9 Zarządzanie aktualizacjami oprogramowania	479
Przed rozpoczęciem	479
Lekcja 1: Działanie Windows Server Update Services.....	481
Przegląd WSUS.....	481
Klient Windows Update	482
Architektura WSUS	484
Wymagania WSUS.....	486
Planowanie instalacji WSUS	487
Audyt aktualizacji.....	489
Podsumowanie lekcji	489
Pytania do lekcji.....	490
Lekcja 2: Korzystanie z WSUS.....	491
Instalacja Windows Server Update Services.....	491
Konfigurowanie Windows Server Update Services	492

Rozwiązywanie problemów z instalacją aktualizacji	503
Usuwanie aktualizacji.....	506
Zadanie: Wdrażanie aktualizacji z WSUS.....	506
Podsumowanie lekcji	509
Pytania do lekcji	510
Przegląd rozdziału.....	511
Podsumowanie rozdziału	511
Określenia kluczowe	511
Scenariusze przykładowe	512
Scenariusz przykładowy 1: Planowanie podstawowej infrastruktury WSUS	512
Scenariusz przykładowy 2: Planowanie złożonej infrastruktury WSUS.....	512
Proponowane zadania praktyczne	513
Konfigurowanie ustawień serwera WSUS (Windows Server Update Services) ...	513
Test ćwiczeniowy	514
10 Monitorowanie komputerów	515
Przed rozpoczęciem	515
Lekcja 1: Monitorowanie zdarzeń.....	517
Używanie Podglądu zdarzeń.....	517
Automatyczne reagowanie na zdarzenia.....	519
Konfigurowanie przekazywania zdarzeń.....	520
Rozwiązywanie problemów z przekazywaniem zdarzeń.....	526
Zadanie: Zbieranie zdarzeń i reagowanie na nie.....	529
Podsumowanie lekcji	532
Pytania do lekcji	533
Lekcja 2: Monitorowanie wydajności i niezawodności	534
Używanie monitora wydajności	534
Używanie monitora niezawodności	536
Używanie zestawów modułów zbierających dane.....	538
Konfigurowanie pamięci wirtualnej.....	544
Zadanie: Uruchamianie Data Collector Set i analiza wyników	546
Podsumowanie lekcji	547
Pytania do lekcji	548
Lekcja 3: Używanie monitora sieci i protokołu SNMP	549
Instalacja Network Monitor	549
Przechwytywanie i analiza komunikacji sieciowej	550
Zadanie: Przechwytywanie i analiza ruchu sieciowego.....	558
Podsumowanie lekcji	560
Pytania do lekcji	560
Przegląd rozdziału.....	561
Podsumowanie rozdziału	561
Terminy kluczowe	562
Scenariusze przykładowe	562
Scenariusz przykładowy 1: Rozwiązywanie problemu z wydajnością sieci	562

Scenariusz przykładowy 2: Monitorowanie komputerów w celu wykrycia niskiej pojemności dysku	563
Proponowane zadania praktyczne	563
Konfigurowanie dzienników zdarzeń	563
Konfigurowanie monitorowania wydajności	563
Zbieranie danych sieciowych	564
Test ćwiczeniowy	564
11 Zarządzanie plikami	565
Przed rozpoczęciem	565
Lekcja 1: Zarządzanie bezpieczeństwem plików	567
Uprawnienia plików NTFS	567
System szyfrowania plików EFS	570
Zadanie: Szyfrowanie i odzyskiwanie plików	580
Podsumowanie lekcji	582
Pytania do lekcji	582
Lekcja 2: Współdzielenie folderów	584
Instalowanie roli serwera File Services	584
Stosowanie limitów przydziału	585
Udostępnianie folderów	591
Zarządzanie klasyfikacją	594
Rozproszony system plików (DFS)	597
Pliki trybu offline	603
BranchCache	605
Zadanie: Praca z udostępnianymi folderami	610
Podsumowanie lekcji	613
Pytania do lekcji	614
Lekcja 3: Tworzenie kopii zapasowych i przywracanie plików	615
Kopie w tle	615
Windows Server Backup	616
Zadanie: Tworzenie kopii zapasowej i przywracanie plików	625
Podsumowanie lekcji	627
Pytania do lekcji	627
Przegląd rozdziału	628
Podsumowanie rozdziału	628
Terminy kluczowe	629
Scenariusze przykładowe	629
Scenariusz przykładowy 1: Planowanie usług plików	629
Scenariusz przykładowy 2: Planowanie odzyskiwania awaryjnego	629
Proponowane zadania praktyczne	630
Konfigurowanie serwera plików	630
Konfigurowanie systemu DFS	630
Konfigurowanie usług kopiowania w tle	631
Konfigurowanie tworzenia i przywracania kopii zapasowej	631
Zarządzanie zasobami serwera plików	631

Test ćwiczeniowy	632
12 Zarządzanie drukarkami	633
Przed rozpoczęciem	633
Lekcja 1: Zarządzanie drukarkami.....	635
Instalacja roli serwera Print And Document Services	635
Instalowanie drukarek	637
Udostępnianie drukarek.....	640
Konfigurowanie uprawnień dla serwera wydruku i drukarki.....	642
Dodawanie sterowników drukarek	643
Konfigurowanie puli drukarek.....	644
Konfigurowanie priorytetów drukarek.....	645
Zarządzanie drukowaniem internetowym	646
Generowanie powiadomień.....	647
Wdrażanie drukarek przy użyciu zasad grupy.....	648
Zarządzanie drukarkami	649
Zarządzanie drukarkami z wiersza polecenia lub skryptu.....	651
Monitorowanie drukarek	653
Zadanie: Instalowanie i udostępnianie drukarki.....	653
Podsumowanie lekcji	656
Pytania do lekcji	657
Przegląd rozdziału.....	658
Podsumowanie rozdziału	658
Terminy kluczowe	658
Scenariusz przykładowy.....	659
Scenariusz przykładowy: Zarządzanie drukarkami sieciowymi.....	659
Proponowane zadania praktyczne	659
Konfigurowanie i monitorowanie usług drukowania	659
Test ćwiczeniowy	660
Odpowiedzi	661
Słowniczek	697
Indeks	701

Wstęp

Podręcznik ten jest przeznaczony dla profesjonalistów technologii informacyjnych (IT), którzy pracują w złożonych środowiskach komputerowych od średnich do dużych firm i planują zdanie egzaminu MCTS (Microsoft Certified Technology Specialist) 70-642. Zakładamy, że przed rozpoczęciem korzystania z tego podręcznika Czytelnik posiada już podstawową wiedzę na temat systemów operacyjnych serwerów Microsoft Windows i popularnych technologii internetowych.

Materiał zawarty w tym podręczniku i objęty egzaminem 70-642 dotyczy podstawowych funkcji sieciowych, takich jak adresowanie, rozpoznawanie nazw, zdalny dostęp i drukowanie. Tematy omawiane w książce dotyczą wszystkiego, co trzeba wiedzieć, aby zdać egzamin 70-642, zgodnie z opisem dostępnym na stronie <http://www.microsoft.com/learning/en/us/exam.aspx?ID=70-642>.

Z tego podręcznika można nauczyć się, jak:

- Konfigurować adresowanie IP, routing i IPsec.
- Konfigurować rozpoznawanie nazw za pomocą DNS (Domain Name System).
- Konfigurować zdalny i bezprzewodowy dostęp do sieci.
- Konfigurować NAP (Network Access Protection).
- Konfigurować usługi plików i drukowania.
- Monitorować i zarządzać infrastrukturą sieciową.

Na początku książki znajduje się strona ze wskazaniem miejsca, w którym można znaleźć każdy temat egzaminu.

Wymagania systemowe

Poniżej opisane są minimalne wymagania sprzętowe i programowe, jakie muszą być spełnione, aby można było wykonać ćwiczenia praktyczne zawarte w tej książce oraz skorzystać z dołączonego dysku CD.

Wymagania sprzętowe

Do wykonania ćwiczeń zawartych w tej książce zalecane jest użycie jednego komputera fizycznego i oprogramowania do wirtualizacji. Komputer powinien spełniać następujące wymagania sprzętowe:

- Procesor klasy x64.
- Jeśli ma być używane oprogramowanie do wirtualizacji Hyper-V, to procesor musi obsługiwać wirtualizację wspomaganą sprzętowo, technologię bitu NX (No eXecute) oraz technologię DEP (Data Execution Prevention).

- 2 GB pamięci RAM (zalecane 8 GB)
- 100 GB wolnego miejsca na dysku twardym (25 GB dla każdej z trzech maszyn wirtualnych plus 25 GB dla systemu bazowego).

Wymagania programowe

Do wykonania ćwiczeń praktycznych potrzebne jest następujące oprogramowanie:

- System Windows Server 2008 R2. Można użyć wersji ewaluacyjnej, dostępnej do pobrania na stronie Microsoft Download Center o adresie <http://www.microsoft.com/downloads>.
- Przeglądarka internetowa, taka jak Windows Internet Explorer 7, Windows Internet Explorer 8 lub Windows Internet Explorer 9.
- Aplikacja do wyświetlania plików PDF, taka jak Adobe Acrobat Reader, którą można pobrać ze strony <http://www.adobe.com/reader>.

Instrukcja budowy laboratorium

Większość ćwiczeń w tym podręczniku wymaga dwóch komputerów lub maszyn wirtualnych z systemem Windows Server 2008 zainstalowanym z domyślnymi ustawieniami (ćwiczenia w rozdziale 6 i kilka ćwiczeń z lekcji 4. w rozdziale 7 wymagają trzeciego komputera lub maszyny wirtualnej). W większości lekcji wszystkie komputery laboratoryjne muszą być fizycznie połączone z tą samą siecią, jednak niektóre lekcje opisują inne konfiguracje sieci. Do wykonania zadań z tej książki zalecamy użycie izolowanej sieci, która nie jest częścią sieci produkcyjnej.

W celu minimalizacji czasu i kosztów konfiguracji komputerów fizycznych i sieci można użyć maszyn wirtualnych. Do uruchomienia komputerów jako maszyn wirtualnych w systemie Windows można użyć technologii Hyper-V lub produktu innej firmy, takiego jak bezpłatne oprogramowanie VirtualBox. Oba te produkty pozwalają uruchamiać 64-bitowe gościnne systemy operacyjne w środowisku wirtualnym, co jest niezbędne w przypadku systemu Windows Server 2008 R2, który występuje wyłącznie w wersji 64-bitowej. (Proszę pamiętać, że ani Virtual PC ani Virtual Server nie obsługują 64-bitowych systemów gościnnych). Więcej informacji o Hyper-V można znaleźć na stronie <http://www.microsoft.com/hyperv>. VirtualBox można pobrać ze strony <http://www.virtualbox.org>.

Użycie środowiska wirtualnego jest najprostszym sposobem przygotowania komputerów dla potrzeb ćwiczeń z tego podręcznika. Aby izolować komputery laboratoryjne w jednej sieci, należy tak skonfigurować ustawienia każdej maszyny wirtualnej, aby jej karta sieciowa była przypisana do sieci prywatnej lub wewnętrznej. Ponadto niektóre ćwiczenia wymagają dostępu do Internetu, co będzie oznaczało konieczność podłączenia karty sieciowej do sieci zewnętrznej. Aby wykonać te ćwiczenia, można tymczasowo podłączyć kartę sieciową do sieci zewnętrznej lub wykonać ćwiczenia na innym komputerze, mającym dostęp do Internetu.

Przygotowanie komputerów Windows Server 2008 R2

W celu przygotowania pierwszego komputera Windows Server 2008 do ćwiczeń w tym podręczniku należy wykonać poniższe czynności.

Na trzech komputerach laboratoryjnych należy wykonać domyślną instalację systemu Windows Server 2008 R2. Proszę nie dodawać żadnych ról ani nie zmieniać ustawień sieciowych. Używając apletu System w Panelu sterowania należy nadać pierwszemu komputerowi nazwę **Dcsrv1**, drugiemu **Boston**, a trzeciemu **Binghamton**.

W przypadku używania maszyn wirtualnych należy zapisać ich migawki zaraz po zakończeniu instalacji, aby móc szybko przywrócić je później do tego stanu.

Uwaga Wykonywanie migawek po każdym ćwiczeniu

Oprogramowanie maszyn wirtualnych pozwala wykonać migawkę takiej maszyny, stanowiącą kompletny zapis stanu maszyny w danym momencie. Po każdym ćwiczeniu należy wykonać migawkę wszystkich komputerów, w których zaszły jakieś zmiany. Trzeba zawsze wykonywać migawkę Dcsrv1 po podniesieniu tej maszyny wirtualnej do roli kontrolera domeny, nawet jeśli ćwiczenia są wykonywane na innych komputerach. (Zmiany dokonywane w serwerach członkowskich powodują często modyfikację ustawień w kontrolerze domeny).

Korzystanie z obrazu dysku CD

Obraz dysku CD towarzyszącego książce jest dostępny na stronie wydawcy przy opisie książki w zakładce Dodatkowe informacje, pod adresem:

<http://www.ksiazki.promise.pl/aspx/produkt.aspx?pid=58529>

Na podstawie tego obrazu można wykonać fizyczny dysk CD lub zainstalować go jako napęd wirtualny. Dysk ten zawiera:

- **Testy ćwiczeniowe** Można ugruntować wiedzę na temat konfiguracji infrastruktury sieciowej Windows Server 2008 R2, używając elektronicznych testów ćwiczeniowych, które można dostosować do własnych potrzeb, korzystając z puli pytań do lekcji zawartych w tej książce. Można też trenować do egzaminu certyfikacyjnego 70-642, używając testów utworzonych z puli około 200 realistycznych pytań egzaminacyjnych, które zapewnią dobre przygotowanie do praktycznego egzaminu.
- **Webcasty** Uzupełnieniem informacji zawartych w książce są webcasty o IPsec dołączone na dysku CD.

Instalowanie testów ćwiczeniowych

Należy wykonać następujące czynności, aby zainstalować oprogramowanie testów ćwiczeniowych z dołączonego CD na twardy dysk:

1. Włożyć dołączony dysk CD do napędu CD i zaakceptować umowę licencyjną. Na ekranie pojawi się menu CD.

Uwaga Jeżeli menu CD się nie pojawia

Jeżeli menu CD lub umowa licencyjna się nie pojawia, może to oznaczać wyłączenie opcji AutoRun na komputerze. Alternatywne instrukcje instalacyjne znajdują się w pliku Readme.txt na CD-ROM.

2. Kliknąć Practice Tests i wykonać instrukcje ukazujące się na ekranie.

Jak korzystać z testów ćwiczeniowych?

Aby uruchomić oprogramowanie testów ćwiczeniowych, należy wykonać następujące działania:

1. Kliknąć Start\All Programs\Microsoft Press Training Kit Exam Prep. Na ekranie pojawi się okno, które pokaże zainstalowany na komputerze zestaw przygotowawczy do egzaminu, dołączony do podręcznika Microsoft Press.
2. Kliknąć dwukrotnie Lesson review lub Practice test, którego chce się użyć.

Uwaga Pytania do lekcji a testy ćwiczeniowe

Opcja (70-642) Configuring Windows Server 2008 Network Infrastructure (2nd Edition) lesson review pozwala skorzystać z pytań w części „Pytania do lekcji” z tej książki (w języku angielskim). Opcja (70-642) Configuring Windows Server 2008 Network Infrastructure (2nd Edition) practice test pozwala skorzystać z puli 200 pytań podobnych do tych, które pojawiają się na egzaminie certyfikacyjnym 70-642.

Opcje pytań do lekcji

Po uruchomieniu pytań do lekcji pojawi się okno dialogowe Custom Mode, pozwalające na skonfigurowanie testu. Można kliknąć OK, aby zaakceptować wartości domyślne lub dostosować liczbę pytań, sposób działania oprogramowania testów, zagadnienia egzaminacyjne, których mają dotyczyć pytania, i możliwości pomiaru czasu. Przy ponownym wykonywaniu testu można wybrać, czy znowu mają być wyświetlane wszystkie pytania, czy tylko te, które zostały poprzednio pominięte lub pozostawione bez odpowiedzi.

Po kliknięciu OK uruchamiają się pytania do lekcji. Poniżej wymienione są podstawowe zasady obowiązujące w trakcie wykonywania testu:

- Podczas testu należy odpowiadać na pytania i używać przycisków Next, Previous i Go To, aby poruszać się pomiędzy nimi.
- Po udzieleniu odpowiedzi na pytanie można zobaczyć, które odpowiedzi są poprawne – wraz z wyjaśnieniami dla każdej poprawnej odpowiedzi – klikając Explanation.
- Jeżeli wolimy poczekać do końca testu i wtedy zobaczyć jego wynik, należy odpowiedzieć na wszystkie pytania i kliknąć Score Test. Pojawi się podsumowanie wybranych zagadnień egzaminacyjnych oraz procent prawidłowych pytań dla każdego zagadnienia z osobna i sumarycznie. Następnie można wydrukować kopię testu, przejrzeć odpowiedzi lub ponownie przeprowadzić test.

Opcje testów ćwiczeniowych

Po uruchomieniu testu ćwiczeniowego należy wybrać pomiędzy trybami Certification, Study i Custom:

- **Certification Mode (tryb certyfikacyjny)** Przypomina udział w egzaminie certyfikacyjnym. Test obejmuje określony zbiór pytań, czas jest mierzony i nie można zatrzymać ani ponownie uruchomić zegara.
- **Study Mode (tryb nauki)** Tworzy test bez pomiaru czasu, w którym można zobaczyć poprawne odpowiedzi i wyjaśnienia po odpowiedzi na każde pytanie.
- **Custom Mode (tryb dowolny)** Pozwala na pełną dowolność konfiguracji opcji testu.

We wszystkich trybach interfejs użytkownika wyświetlany podczas wykonywania testu jest podobny, ale różni się opcjami włączonymi lub wyłączonymi w zależności od trybu. Główne opcje są omówione we wcześniejszym podrozdziale „Opcje pytań do lekcji”.

Podczas sprawdzania odpowiedzi na poszczególne pytania testu ćwiczeniowego wyświetlana jest sekcja „References”, która informuje, gdzie w podręczniku można znaleźć wiadomości związane z tym pytaniem i zawiera łącza do innych zasobów informacyjnych. Po kliknięciu Test Results w celu oceny całego testu ćwiczeniowego można kliknąć kartę Learning Plan, aby zobaczyć listę odsyłaczy dla każdego zagadnienia.

Odinstalowywanie testów ćwiczeniowych

Aby odinstalować oprogramowanie testów ćwiczeniowych dla tego podręcznika, należy użyć opcji Add Or Remove Programs (Dodaj lub usuń programy) w systemie Windows XP, a w Windows 7 i Windows Server 2008 R2 opcji Program And Features (Programy i funkcje) w Windows Control Panel.

Podziękowania

Ta książka powstała przy udziale zespołu uznanych ekspertów i jako autorzy chcielibyśmy podziękować im za wspianą pracę, którą wykonali.

Ken Jones z firmy Microsoft przygotował nasze kontrakty, Karen Szall była redaktorem rozwojowym, a Carol Dillingham redaktorem projektu.

Kathy Krause z Online Training Solutions, Inc. zarządzała zespołem wydawniczym i produkcyjnym. Victoria Thulman była redaktorem tekstu odpowiedzialnym za zapewnienie, że książka będzie czytelna i spójna, a Jaime Odell dodatkowo ją sprawdził.

Bob Dean przejrzał książkę od strony technicznej i pomógł uczynić ją tak dokładną, jak to tylko możliwe. Jan Bednarczuk zrobił indeks, dostępny na końcu książki.

W powstaniu tej książki pomogło wiele osób, mimo że nie należeli formalnie do jej zespołu.

Tony Northrup chciałby podziękować swoim przyjaciołom. W szczególności są to: Brian i Melissa Rheame, Jose i Kristin Gonzales, Chelsea i Madelyn Knowles, Eddie i Christine Mercado, Papa Jose oraz Nana Lucy.

J.C. Mackin chciałby podziękować swoim przyjaciołom i rodzinie za oferowane stałe wsparcie.

To ogromna różnica, gdy ludzie, z którymi się pracuje, są jednocześnie przyjaciółmi. Posiadanie wspaniałego zespołu nie tylko poprawia jakość książki, ale sprawia, że jest to znacznie radośniejsze doświadczenie. Pisanie tej książki było ogromną przyjemnością i mamy nadzieję, że w przyszłości będziemy mieć jeszcze możliwość pracy ze wszystkimi tymi osobami.

Wsparcie technicznie i kontakt

W kolejnych podrozdziałach podane są informacje na temat erraty, wsparcia technicznego i przesyłania opinii oraz dane kontaktowe:

Errata

Podjęto wszelkie wysiłki, aby zapewnić dokładność tej książki i treści dołączonego dysku CD. W przypadku wykrycia błędu można zgłosić go na witrynie wydawnictwa Microsoft Press lub oreilly.com. W tym celu należy wykonać następujące działania:

1. Wejść na stronę <http://microsoftpress.oreilly.com>.
2. W polu Search wprowadzić tytuł książki lub jej numer ISBN.
3. Wybrać książkę z listy wyników.
4. Na stronie katalogowej książki, poniżej zdjęcia okładki, powinna widnieć lista łączy.
5. Kliknąć łącznie View/Submit Errata.

Na stronie katalogowej książki można znaleźć również inne informacje i usługi. Jeśli jest potrzebna dodatkowa pomoc, można wysłać wiadomość email do działu Microsoft Press Book Support na adres mspinput@microsoft.com.

Proszę pamiętać, że pod wymienionymi adresami nie można uzyskać pomocy technicznej na temat oprogramowania firmy Microsoft.

Czekamy na opinie

W firmie Microsoft Press najważniejsza jest satysfakcja klienta i najcenniejszy materiał stanowią opinie Czytelników. Dlatego prosimy o podzielenie się z nami swoją opinią na temat tej książki i wypełnienie ankiety na stronie <http://www.microsoft.com/learning/booksurvey>.

Ankieta jest krótka i czytamy wszystkie komentarze i pomysły. Z góry dziękujemy za udział!

Bądźmy w kontakcie

Kontynuujmy naszą rozmowę! Jesteśmy na Twitterze: <http://twitter.com/MicrosoftPress>

Przygotowanie do egzaminu

Certyfikaty Microsoft stanowią najlepszy sposób potwierdzenia opanowanych umiejętności i posiadanego doświadczenia w zakresie aktualnych produktów i technologii firmy Microsoft. Chociaż nic nie zastąpi doświadczeń zdobywanych poprzez pracę z produktami, przygotowanie poprzez naukę i proponowane ćwiczenia praktyczne ułatwia przygotowanie się do egzaminu. Zalecamy opracowanie planu przygotowywania się do egzaminu poprzez łączenie dostępnych materiałów i kursów. Na przykład, można zestaw szkoleniowy czy inny poradnik wykorzystywać do przygotowywania się „w domu” i brać udział w kursie Microsoft Official Curriculum, by nabyć doświadczeń na sali wykładowej. Wybierz połączenie, które Ci najbardziej odpowiada!

Microsoft®
CERTIFIED

*Technology
Specialist*

Rozdział 1

Działanie i konfiguracja TCP/IP

Sieci komputerowe, podobnie jak każdy system komunikacyjny, polegają na zbiorze standardów umożliwiających wysyłanie, odbieranie i interpretowanie komunikatów. Internet, sieci Windows i prawie wszystkie inne sieci komputerowe wykorzystują w tym celu protokoły TCP/IP (Transmission Control Protocol/Internet Protocol), których rdzennym protokołem jest IP.

W tym rozdziale poznamy podstawy protokołu TCP/IP oraz sposób konfigurowania systemów Windows Server 2008 i Windows Server 2008 R2 do łączenia się z sieciami TCP/IP.

Ważne **Czy przeczytałeś** **stronę xxi?**

Strona zawiera ważne informacje dotyczące umiejętności potrzebnych do zdania egzaminu.

Tematy egzaminacyjne w tym rozdziale:

- Konfiguracja adresowania IPv4 i IPv6

Lekcje w tym rozdziale:

Lekcja 1: Wprowadzenie do działania sieci w systemie Windows.	3
Lekcja 2: Adresowanie IPv4	38
Lekcja 3: Adresowanie IPv6	82

Przed rozpoczęciem

Do wykonania lekcji z tego rozdziału trzeba mieć:

- Dwie maszyny wirtualne lub komputery fizyczne o nazwach Dcsrv1 i Boston, połączone do tej samej izolowanej sieci z zainstalowanym systemem Windows Server 2008 R2. Żaden z tych komputerów nie powinien mieć dodanych ról serwera.
- Podstawową wiedzę na temat administracji Windows.



Z praktyki

JC Mackin

W celu rozwiązywania problemów z siecią dobrze jest mieć zapamiętany jeden publiczny adres IP.

W tej książce używamy w tym celu adresu 198.41.0.4, będący adresem głównego internetowego serwera nazw a.root-servers.net. Serwer ten zawsze działa. Wykonując w trybie znakowym polecenie `tracert 198.41.0.4` można natychmiast sprawdzić, czy i gdzie występuje przerwa w łączności TCP/IP między lokalnym komputerem a Internetem.

Lekcja 1: Wprowadzenie do działania sieci w systemie Windows

W ramach tej lekcji omówimy podstawowe pojęcia związane z działaniem sieci w systemie Windows. Na początku poznamy koncepcję modelu warstwowego sieci, a następnie przejdziemy do opisu TCP/IP – wielowarstwowego pakietu protokołów, na którym opiera się działanie sieci w systemie Windows. Następnie zobaczymy, jak wygląda konfigurowanie podstawowych właściwości połączeń sieciowych w systemach Windows Server 2008 i Windows Server 2008 R2, a na koniec omówimy podstawowe sposoby rozwiązywania problemów z połączeniami sieciowymi przy użyciu podstawowych narzędzi TCP/IP.

Po ukończeniu tej lekcji Czytelnik będzie umiał:

- Opisać cztery warstwy w stosie protokołów TCP/IP.
- Wyświetlić i skonfigurować konfigurację IP połączenia sieci lokalnej.
- Opisać koncepcję rozgłaszania w sieci.
- Rozwiązać problemy z łącznością sieciową z zastosowaniem narzędzi TCP/IP.

Przewidywany czas trwania lekcji: 100 minut

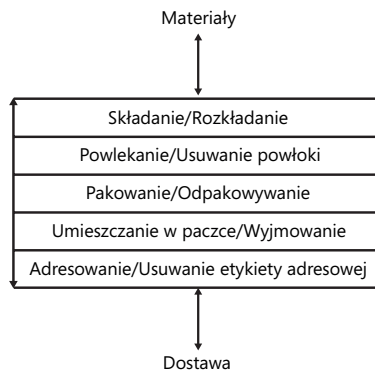
Pojęcie warstw sieci

Warstwy sieci to etapy funkcjonalne komunikacji sieciowej realizowane przez programy zwane *protokołami*. Rozważmy jako analogię linię produkcyjną. Jeżeli fabryka korzysta z linii produkcyjnej do tworzenia produktu, który jest na przykład składany, powlekany, pakowany, umieszczany w pudełku i etykietowany, możemy wyobrazić sobie te pięć kolejnych funkcji jako pionowo rozmieszczone warstwy w procesie produkcyjnym, jak pokazano na rysunku 1-1. Podążając za tą analogią, protokoły w linii produkcyjnej są konkretnymi maszynami (składającymi, malującymi, pakującymi itd.) służącymi do wykonania funkcji każdej warstwy. Chociaż każdy protokół jest przeznaczony do przyjmowania specyficznego wejścia i generowania specyficznego wyjścia, dowolną maszynę w systemie można wymienić na inną, o ile pozostanie ona kompatybilna z sąsiednimi maszynami na linii produkcyjnej.



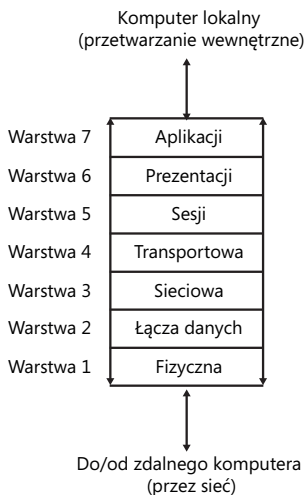
Rysunek 1-1 Warstwowy model działania linii produkcyjnej

W ten sposób komunikacja sieciowa rzeczywiście przypomina tworzenie pakowanych produktów na linii produkcyjnej, ponieważ komputery komunikują się ze sobą, tworząc i wysyłając kapsułkowane (opakowane) paczki nazywane *pakietami*. Natomiast, w przeciwieństwie do linii produkcyjnej, komunikacja pomiędzy komputerami jest dwukierunkowa. Oznacza to, że warstwy sieciowe wzięte razem opisują zarówno sposób konstruowania, jak i *demontowania* pakietów. Każda warstwa i każdy konkretny protokół muszą być w stanie wykonywać swoją funkcję w dwóch kierunkach. Taki dwukierunkowy model dla przykładowej linii produkcyjnej można przedstawić tak, jak na rysunku 1-2.



Rysunek 1-2 Warstwy w dwukierunkowej linii „składania-rozkładania”

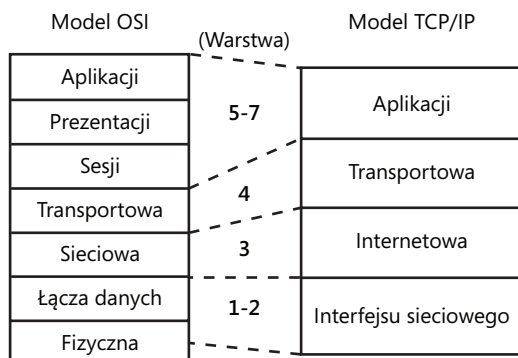
Tradycyjnie stosowany model warstwowy komunikacji w sieciach komputerowych, siedmiowarstwowy model OSI (Open Systems Interconnect), pokazano na rysunku 1-3. Widać na podstawie nazw, że każda z tych siedmiu warstw jest przeznaczona do wykonywania określonego kroku w procesie komunikacji, jak prezentacja lub transport informacji.



Rysunek 1-3 Model OSI komunikacji sieciowej

Chociaż protokoły, które tworzyły oryginalny model OSI, nie zostały nigdy w pełni zaadaptowane z praktyki, to nazwy warstw – a szczególnie ich numery – przetrwały do dzisiaj.

W efekcie, nawet jeśli TCP/IP jest oparty o własny model, cztery warstwy sieciowe TCP/IP są często definiowane w oparciu o model OSI, co widać na rysunku 1-4.

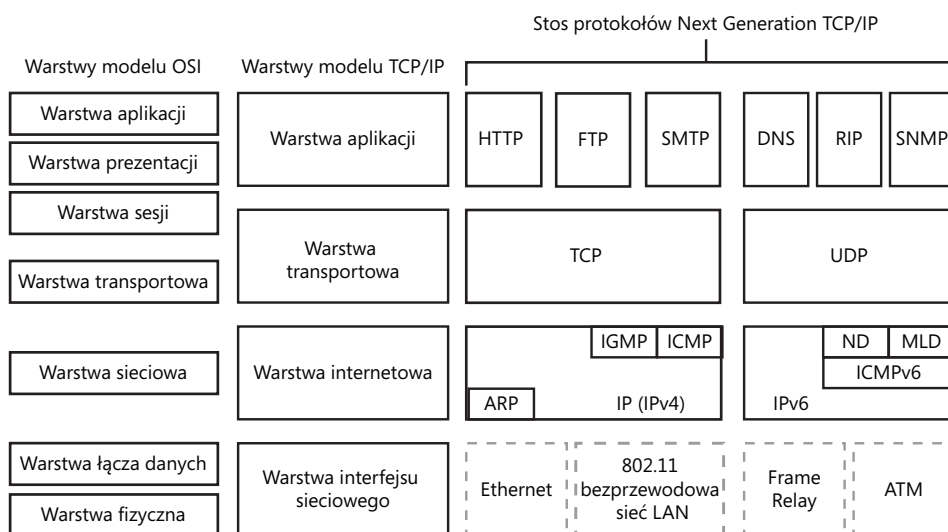


Rysunek 1-4 Warstwy sieciowe TCP/IP są zmapowane do modelu OSI

Warstwy modelu sieciowego TCP/IP

Idea warstwowego modelu sieciowego umożliwia modyfikowanie poszczególnych protokołów, o ile protokoły te będą nadal gładko współpracować z protokołami z sąsiednich warstw. Taka zmiana nastąpiła faktycznie niedawno w TCP/IP w sieciach Windows. Najpierw w systemach Windows Server 2008 i Windows Vista, a potem w Windows Server 2008 R2 i Windows 7 firma Microsoft wprowadziła nową implementację stosu protokołów TCP/IP, znaną jako Next Generation TCP/IP (stos TCP/IP nowej generacji). W wersji tej została na nowo zaprojektowana warstwa Internetu, natomiast sąsiadujące z nią warstwy pozostały zasadniczo takie same.

Stos TCP/IP nowej generacji pokazany jest na rysunku 1-5.



Rysunek 1-5 Stos Next Generation TCP/IP

Uwaga Numery warstw TCP/IP

Chociaż czasami możemy napotkać warstwy w modelu TCP/IP z przypisanymi własnymi numerami niezależnymi od modelu OSI, w tej książce stosujemy powszechniej stosowane numery warstw OSI. Kolejny podrozdział zawiera bardziej szczegółowy opis czterech warstw TCP/IP pokazanych na rysunku 1-5.

Warstwa interfejsu sieciowego

Warstwa *interfejsu sieciowego*, zwana często *warstwą 2* lub *warstwą łącza danych*, opisuje standardową metodę komunikacji między urządzeniami znajdującymi się w tym samym segmencie sieci. (Segment sieci składa się z interfejsów sieciowych rozdzielonych jedynie kablami, przełącznikami, koncentratorami lub bezprzewodowymi punktami dostępowymi). Interfejsy sieciowe używają protokołów tej warstwy do komunikowania się z innymi, sąsiadującymi interfejsami sieciowymi, identyfikowanymi na podstawie stałych adresów sprzętowych (takich jak adresy MAC). Warstwa interfejsu sieciowego specyfikuje także wymagania fizyczne dotyczące sygnałów, kart sieciowych, kabli, przełączników, koncentratorów i punktów dostępowych; ta czysto fizyczna specyfikacja jest czasem określana mianem warstwy fizycznej lub warstwy 1. Przykładami standardów zdefiniowanych w warstwie interfejsu sieciowego są Ethernet, Token Ring PPP (Point-to-Point Protocol) i FDDI (Fiber Distributed Data Interface).

Uwaga Przełącznik (switch) działa na poziomie warstwy 2

Ponieważ przełącznik odczytuje adres sprzętowy w sieci lokalnej i ogranicza propagację ruchu sieciowego tylko do tych adresów, które są potrzebne, zaliczany jest do urządzeń warstwy 2.

Rzut oka na protokół Ethernet

Pakiety ethernetowe znane są bardziej jako ramki. W tej części pokazana jest ramka ethernetowa przechwycona za pomocą analizatora protokołu Network Monitor, dostępnego na stronie firmy Microsoft.

UWAGA Szczegóły protokołu nie są poruszane na egzaminach firmy Microsoft

Nie trzeba znać budowy ramki żadnego typu protokołu, aby zdać egzamin 70-642. Tego typu wiedza może jednak pomóc w lepszym zrozumieniu protokołów.

Pierwszy wiersz, zaczynający się od wyrazu „Frame” (ramka), poprzedza przechwyconą ramkę i jest dodawany przez program Network Monitor, aby dostarczyć ogólną informację o tej ramce. Potem występują dane samego protokołu Ethernet (zwane nagłówkiem); zostały one rozwinięte i wyróżnione.

Poniżej nagłówka ethernetowego, badając lewą stronę treści ramki, widać, że zawiera ona nagłówki IPv4, TCP i HTTP.

Ostatnią część pakietu stanowi nagłówek HTTP wskazujący, że jest to żądanie „HTTP GET Request” skierowane do zdalnego serwera sieci Web. Ostatecznym celem całej tej ramki ethernetowej jest więc prośba o zawartość zdalnej strony sieci Web.

```
Frame: Number = 16, Captured Frame Length = 664, MediaType = ETHERNET
- Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-1E-2A-47-
C2-78], SourceAddress: [00-15-5D-02-03-00]
+ DestinationAddress: 001E2A 47C278 [00-1E-2A-47-C2-78]
+ SourceAddress: Microsoft Corporation 020300 [00-15-5D-02-03-00]
EthernetType: Internet IP (IPv4), 2048(0x800)

+ IPv4: Src = 192.168.2.201, Dest = 216.156.213.67, Next Protocol = TCP,
Packet ID = 1134, Total IP Length = 650
+ Tcp: Flags=...AP..., SrcPort=49197, DstPort=HTTP(80), PayloadLen=610,
Seq=776410322 - 776410932, Ack=829641496, Win=32850 (scale factor 0x2) =
131400
+ Http: Request, GET /
```

W środku rozwiniętego nagłówka ethernetowego widać wartości DestinationAddress (adres docelowy) i SourceAddress (adres źródłowy). Wartości te reprezentują adresy MAC, czyli stałe adresy fizyczne przypisane do konkretnych interfejsów sieciowych. Wartość SourceAddress ma dodaną przez program Network Monitor etykietę „Microsoft Corporation”, ponieważ pierwsza część tego adresu MAC (00-15-5D) jest przypisana do firmy Microsoft jako producenta interfejsu sieciowego. (Komputer lokalny jest w rzeczywistości maszyną wirtualną uruchomioną na platformie wirtualizującej Microsoft Hyper-V, tak więc w tym przypadku interfejs sieciowy jest po prostu oprogramowaniem). Druga połowa adresu MAC jest unikatowa dla tego konkretnego interfejsu.

Adres docelowy, „DestinationAddress”, odnosi się w tym przypadku do domyślnej bramy w sieci lokalnej (LAN), a nie do zdalnego serwera sieci Web, do którego zawartość pakietu ma być w ostateczności dostarczona. Protokoły, takie jak Ethernet, które działają w warstwie 2, nie widzą niczego poza siecią lokalną.

Pole EthernetType wskazuje w ramce protokół następnej warstwy. Gdy docelowy system operacyjny otrzymuje taką ramkę, wartość w tym polu określa protokół, który ma przetworzyć dane występujące po nagłówku ethernetowym. W naszym przypadku porcja danych w ramce ethernetowej zostanie przekazana do protokołu IPv4.

Podczas wędrówki pakietu przez sieć LAN oraz Internet w kierunku miejsca docelowego, którym jest zdalny serwer sieci Web, nagłówek warstwy 2 jest wielokrotnie przepisywany, aby uwzględnić nowe adresy miejsca źródłowego i docelowego na każdym łączu sieci. Może być także zmieniany w celu dostosowania go do różnych interfejsów sieciowych – technologii innych niż Ethernet, takich jak FDDI czy Token Ring, które mogą zostać napotkane po drodze.

Warstwa internetowa

Warstwa internetowa, nazywana także często *warstwą sieciową* lub *warstwą 3*, opisuje globalne i konfigurowalne oprogramowanie, którego zadaniem jest komunikacja między urządzeniami należącymi do różnych segmentów sieci. Głównym protokołem działającym w warstwie 3 jest IP, a urządzeniem - *router*. Router odczytuje adres docelowy zapisany w pakiecie i następnie przekazuje ten pakiet do miejsca docelowego po odpowiedniej

trasie. Jeśli na poziomie tej warstwy adres docelowy podany w pakiecie należy do sieci lokalnej lub oznacza lokalne rozgłaszanie, to router po prostu odrzuca taki pakiet. Z tego powodu mówi się, że routery blokują rozgłaszanie.

Jak zostało już wcześniej powiedziane, to właśnie w warstwie 3. dokonano głównych zmian w nowej implementacji TCP/IP firmy Microsoft. Tradycyjnie jedynym protokołem wykorzystywanym w tej warstwie był IPv4. Natomiast w stosie Next Generation TCP/IP stosowane są wspólnie protokoły IPv4 i IPv6. W ten sposób tylko jeden zestaw protokołów w sąsiadujących warstwach komunikuje się przy użyciu zarówno IPv4, jak i IPv6.

- **IPv4** Protokół IPv4 (lub po prostu IP) jest odpowiedzialny za adresowanie i przekazywanie pakietów pomiędzy hostami, które mogą być oddalone o wiele segmentów sieci. IPv4 polega na adresach 32-bitowych, a ponieważ ta przestrzeń adresowa jest relatywnie mała, adresy w sieciach IPv4 szybko się wyczerpują.
- **IPv6** IPv6 stosuje adresy 128 bitowe zamiast 32 bitowych adresów stosowanych w IPv4 i w wyniku tego może definiować znacznie więcej adresów. Ponieważ niewiele routerów w Internecie jest kompatybilnych z IPv6, dziś IPv6 jest stosowany w Internecie z pomocą protokołów tunelowania. Natomiast w sieciach lokalnych Windows Vista, Windows 7, Windows Server 2008 i Windows Server 2008 R2 IPv6 jest wspierany natywnie.

Domyślnie są włączone oba protokoły, IPv4 i IPv6. Dzięki tej dualnej architekturze IP komputery do komunikacji mogą używać IPv6, jeśli jest on obsługiwany przez klientów, serwery i infrastrukturę sieciową. Mogą się też komunikować z komputerami i usługami sieciowymi, które obsługują wyłącznie IPv4.

Rzut oka na protokół IP

Podana niżej ramka ethernetowa to ta sama, która występowała wcześniej w ramce „Rzut oka na protokół Ethernet”. Teraz jednak został w niej rozwinięty i wyróżniony nagłówek IPv4:

```
Frame: Number = 16, Captured Frame Length = 664, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4), DestinationAddress: [00-1E-2A-47-
C2-78], SourceAddress: [00-15-5D-02-03-00]

- Ipv4: Src = 192.168.2.201, Dest = 216.156.213.67, Next Protocol = TCP,
  Packet ID = 1134, Total IP Length = 650
+ Versions: IPv4, Internet Protocol; Header Length = 20
+ DifferentiatedServicesField: DSCP: 0, ECN: 0
  TotalLength: 650 (0x28A)
  Identification: 1134 (0x46E)
+ FragmentFlags: 16384 (0x4000)
  TimeToLive: 128 (0x80)
  NextProtocol: TCP, 6(0x6)
  Checksum: 0 (0x0)
  SourceAddress: 192.168.2.201
  DestinationAddress: 216.156.213.67
```

```
+ Tcp: Flags=...AP..., SrcPort=49197, DstPort=HTTP(80), PayloadLen=610,  
Seq=776410322 - 776410932, Ack=829641496, Win=32850 (scale factor 0x2) =  
131400
```

```
+ Http: Request, GET /
```

Tak jak w przypadku nagłówka ethernetowego najważniejszymi danymi w nagłówku IPv4 są pola SourceAddress (adres źródłowy) i DestinationAddress (adres docelowy), występujące na końcu wyróżnionej sekcji. Zwróćmy jednak uwagę, że w tym przypadku oba te adresy są adresami IP i że adresem docelowym jest adres końcowy (zdalnego serwera sieci Web).

Oprócz adresu źródłowego i docelowego nagłówek IP zawiera również informacje używane przez różne inne funkcje protokołu. Sekcja DifferentiatedServicesField składa się z dwóch pól, DSCP i ECN. Pole DSCP, odczytywane tylko przez niektóre specjalne routery, pozwala określić ruch do konkretnego adresu IP jako wymagający priorytetowej obsługi. Pole ECN sygnalizuje tłok w routerze wysyłającym pakiety do następnych routerów na trasie. TotalLength podaje całkowitą długość w bajtach pakietu IP (zwanego również „datagramem”). Długość ta obejmuje wszystkie dane z warstwy 3, 4 i wyższych, łącznie z wszystkimi danymi leżącymi za nagłówkami. W tym przypadku datagram IP ma długość 650 bajtów. Pole Identification zawiera numer nadany pakietowi, dzięki któremu można złożyć z powrotem dane poddane fragmentacji. (Pakiety są poddawane fragmentacji, gdy ich długość przekracza wartość zwaną rozmiarem MTU (Maximum Transmission Unit) określoną przez komputery, routery i inne urządzenia). Sekcja FragmentFlags dostarcza informacje, które pomagają ustalić i złożyć razem podzielone datagramy IP. Wartość TimeToLive (czas życia) ustawiana jest w systemie Windows standardowo na 128, a następnie zmniejszana o 1 przez każdy kolejny router obsługujący datagram IP. Po osiągnięciu wartości 0 datagram jest usuwany. Celem tego mechanizmu jest zapobieganie wpadaniu transmisji danych w nieskończoną pętlę w sieci. Pole NextProtocol określa protokół wyższej warstwy (warstwy 4.), który ma być użyty do przetworzenia zawartości datagramu IP. W naszym przypadku jest to protokół TCP. Pole Checksum (suma kontrolna) zawiera wynik funkcji matematycznej, której celem jest kontrola integralności nagłówka IP. Wartość 0 oznacza stan poprawny i potwierdza, że nagłówek nie został zmodyfikowany podczas transmisji.

Datagramy IP mogą występować w dwóch wersjach: IPv4 i IPv6. IPv6 jest nowszą, alternatywną wersją IP, wykorzystywaną w niektórych transmisjach sieciowych. Zamieszczona niżej ramka ethernetowa zawiera rozwinięty i wyróżniony nagłówek IPv6:

```
Frame: Number = 43, Captured Frame Length = 86, MediaType = ETHERNET
```

```
+ Ethernet: Etype = IPv6, DestinationAddress:[33-33-00-01-00-  
03], SourceAddress:[00-15-5D-02-03-05]
```

```
- Ipv6: Next Protocol = UDP, Payload Length = 32  
+ Versions: IPv6, Internet Protocol, DSCP 0  
  PayloadLength: 32 (0x20)  
  NextProtocol: UDP, 17(0x11)
```

```
HopLimit: 1 (0x1)
SourceAddress: FE80:0:0:0:D9C6:6B0E:BA3F:1FC9
DestinationAddress: FF02:0:0:0:0:0:1:3
```

```
+ Udp: SrcPort = 53047, DstPort = Linklocal Multicast Name
Resolution(5355), Length = 32
```

```
+ Llmnr: QueryId = 0x862D, Standard, Query for boston of type Host Addr
on class Internet
```

W nagłówku IPv6 pole PayloadLength podaje długość w bajtach danych przenoszonych przez datagram IPv6. Pole NextProtocol wskazuje protokół warstwy 4., do którego należy przekazać dane z datagramu IPv6. Wartość HopLimit oznacza to samo co TimeToLive w IPv4. Wartość 1 wskazuje, że pakiet jest skierowany tylko do sieci lokalnej (LAN). Wartości SourceAddress i DestinationAddress są 16-bajtowymi adresami IPv6. W naszym przykładzie adres docelowy jest przypadkowo adresem typu multicast, który może być przypisany do więcej niż jednego komputera w sieci LAN.

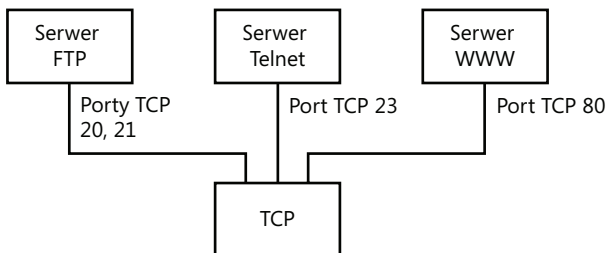
Warstwa transportowa

Warstwa transportowa modelu TCP/IP, zwana również warstwą 4., definiuje metodę wysyłania i odbierania danych między urządzeniami. Warstwa 4. służy również do oznakowywania danych jako przeznaczonych dla konkretnej aplikacji, takiej jak poczta elektroniczna czy WWW.

Dwoma protokołami warstwy transportowej w stosie TCP/IP są TCP i UDP.

- **TCP** TCP odbiera dane z warstwy aplikacji i przetwarza je na strumień bajtów. Te bajty są grupowane w segmenty, które TCP następnie numeruje i dostarcza sekwencyjnie do hostów sieciowych. Komunikacja TCP jest dwukierunkowa i niezawodna. Odbiorca potwierdza otrzymanie każdego segmentu danych i jeśli nadawca nie otrzyma takiego potwierdzenia, to ponownie wysyła dany segment.

Gdy TCP odbiera strumień danych z hosta sieciowego, wysyła dane do aplikacji wyznaczonej przez numer portu TCP. Porty TCP pozwalają różnym aplikacjom i programom na korzystanie z usług TCP na jednym hoście, jak pokazano na rysunku 1-6. Każdy program korzystający z portów TCP nasłuchuje komunikatów przybywających z opowiadającym mu numerem portu. W ten sposób dane wysyłane do określonego portu TCP są odbierane przez aplikację nasłuchującą na tym porcie.



Rysunek 1-6 Porty TCP

- **UDP** Wiele usług sieciowych (takich jak DNS) jako protokołu transportowego używa UDP zamiast TCP. UDP umożliwia szybki transport datagramów przez wyeliminowanie funkcji niezawodności TCP, takich jak gwarancja potwierdzenia dostarczenia i weryfikacja kolejności. W przeciwieństwie do TCP UDP jest usługą *bezpoleźniową*, przekazującą dane tak dobrze „jak się da”. Host źródłowy, który potrzebuje niezawodnej komunikacji, musi albo używać TCP, albo programu, który zapewnia własne usługi sekwencjonowania i potwierdzania.

Rzut oka na protokoły TCP i UDP

TCP i UDP są protokołami warstwy transportowej, ale tylko TCP jest protokołem połączeniowym. Komunikacja połączeniowa ma miejsce podczas sesji dwukierunkowej; gdy jeden komputer wysyła dane do drugiego przy użyciu protokołu TCP, odbiorca wysyła do nadawcy potwierdzenia odbioru danych.

Sesja TCP między dwoma komputerami jest najpierw nawiązywana za pomocą trójetapowej wymiany komunikatów. W pierwszym kroku pierwszy komputer wysyła wiadomość SYN, czyli „synchronizuj”. Drugi komputer odpowiada wówczas wysyłając pakiet TCP (zwany segmentem), który zawiera zarówno wiadomość ACK (potwierdzenie), jak i SYN. Na koniec pierwszy komputer wysyła drugiemu segment ACK.

Ta trójetapowa wymiana, przechwycona przez Network Monitor, pokazana jest na rysunku 1-7. Proszę zwrócić uwagę na trzy kolejne segmenty TCP. Segmenty te są wymieniane między komputerem o adresie 192.168.2.201 i komputerem o adresie 192.168.2.103.

Frame Summary				
Find ▾ ↓ ↑ Autoscroll				
Process Name	Source	Destination	Protocol Name	Description
			NetmonFilter	NetmonFilter:Updated Ca
			NetworkInfoEx	NetworkInfoEx:Network i
	192.168.2.3	255.255.255.255	UDP	UDP:SrcPort = 17500, Ds
	192.168.2.3	192.168.2.255	UDP	UDP:SrcPort = 17500, Ds
	192.168.2.201	192.168.2.103	ARP	ARP:Request, 192.168.2.
	192.168.2.103	192.168.2.201	ARP	ARP:Response, 192.168.
System	192.168.2.201	192.168.2.103	TCP	TCP:Flags=.....S., SrcP
System	192.168.2.103	192.168.2.201	TCP	TCP:Flags=...A..S., SrcP
System	192.168.2.201	192.168.2.103	TCP	TCP:Flags=...A....., SrcP
System	192.168.2.201	192.168.2.103	SMB	SMB:C; Negotiate, Dialect
System	192.168.2.103	192.168.2.201	SMB2	SMB2:R NEGOTIATE (0x
System	192.168.2.201	192.168.2.103	SMB2	SMB2:C NEGOTIATE (0x
System	192.168.2.103	192.168.2.201	SMB2	SMB2:R NEGOTIATE (0x

Rysunek 1-7 Wymiana komunikatów TCP

W pierwszym segmencie TCP wymiany zainicjowanej przez pierwszy komputer występuje komunikat SYN, pokazany przez Network Monitor jako „TCP:Flags=.....S.”.

Drugi komputer odpowiada na to segmentem SYN-ACK, reprezentowanym przez opis „TCP:Flags=...A..S.”. Na koniec pierwszy komputer odpowiada drugiemu wysyłając segment ACK, reprezentowany przez opis „TCP: Flags=...A....”.

Po ustanowieniu sesji protokół TCP może być wykorzystywany do transportu danych z jednego komputera do drugiego. Nagłówek segmentu TCP używany podczas takiej sesji pokazany jest poniżej. Zamieszczona ramka ethernetowa to ta sama ramka, która występowała wcześniej w tym rozdziale w ramce „Rzut oka na protokół Ethernet”. Tym razem jednak został rozwinięty i wyróżniony nagłówek TCP występujący w tej ramce:

```

Frame: Number = 16, Captured Frame Length = 664, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4),DestinationAddress:[00-1E-2A-47-
C2-78],SourceAddress:[00-15-5D-02-03-00]

+ Ipv4: Src = 192.168.2.201, Dest = 216.156.213.67, Next Protocol = TCP,
Packet ID = 1134, Total IP Length = 650

- Tcp: Flags=...AP..., SrcPort=49197, DstPort=HTTP(80), PayloadLen=610,
Seq=776410322 - 776410932, Ack=829641496, Win=32850 (scale factor 0x2) =
131400
  SrcPort: 49197
  DstPort: HTTP(80)
  SequenceNumber: 776410322 (0x2E4714D2)
  AcknowledgementNumber: 829641496 (0x31735318)
+ DataOffset: 80 (0x50)
+ Flags: ...AP...
  Window: 32850 (scale factor 0x2) = 131400
  Checksum: 0x73CE, Disregarded
  UrgentPointer: 0 (0x0)
  TCPPayload: SourcePort = 49197, DestinationPort = 80

+ Http: Request, GET /

```

W protokole TCP do rozróżniania strumieni danych wysyłanych z i do różnych aplikacji używane są porty. Dane zawarte w tym konkretnym segmencie TCP to żądanie HTTP GET Request od lokalnego komputera do zdalnego serwera sieci Web. O ile występujący w tym żądaniu port źródłowy, SrcPort, 49197 jest rzadko wybierany, to port docelowy, DstPort, musi mieć numer 80, ponieważ jest on zarezerwowany dla ruchu HTTP. Liczba SequenceNumber odnosi się do kolejności danych wychodzących w przypadku dużego strumienia obejmującego wiele segmentów. Liczba ta pozwala komputerowi docelowemu uporządkować dane, jeśli przyjdą w zmienionej kolejności. Liczba AcknowledgementNumber odnosi się do danych przychodzących: zasadniczo informuje nadawcę strumienia danych TCP o tym, które bajty danych zostały już odebrane. Wartość DataOffset wskazuje koniec nagłówka TCP i początek porcji danych.

Flags (flagi) to seria 8 bitów. Każdy pojedynczy bit ma konkretne znaczenie w przypadku jego ustawienia (na 1, a nie na 0). Na przykład ustawienie czwartego bitu oznacza flagę ACK, a siódmego – flagę SYN. W naszym przykładzie ustawione są flagi ACK i PSH (push). Ta druga powoduje zasadniczo natychmiastowe wysłanie

danych do protokołu wyższej warstwy (tutaj HTTP) przed wypełnieniem całego bufora TCP. Do innych ważnych flag należą RST (przerwanie sesji TCP), FIN (koniec sesji TCP) i URG (pilne dane).

Wartość Window (okno) dotyczy kontroli przepływu danych. Wartość ta jest wysyłana przez odbiorcę strumienia bajtów w celu powiadomienia nadawcy, ile bajtów danych może aktualnie przyjąć odbiorca. Ponieważ wartość ta może się różnić dla poszczególnych segmentów, mówi się, że TCP ma przesuwne okno. Wartość Checksum (suma kontrolna) kontroluje spójność danych i działa tak samo jak suma kontrolna w nagłówku IP. Wartość UrgentPointer wskazuje lokalizację pilnych danych w przypadku ustawionej flagi URG.

A teraz porównamy bogaty w funkcje, połączeniowy protokół TCP z jego bezpołączeniowym odpowiednikiem UDP. W pokazanej niżej ramce ethernetowej został rozwinięty i wyróżniony nagłówek UDP:

```
Frame: Number = 11, Captured Frame Length = 72, MediaType = ETHERNET

+ Ethernet: Etype = Internet IP (IPv4), DestinationAddress:[00-1F-C6-72-80-C2], SourceAddress:[00-15-5D-02-03-00]

+ Ipv4: Src = 192.168.2.201, Dest = 192.168.2.2, Next Protocol = UDP,
Packet ID = 1131, Total IP Length = 58

- Udp: SrcPort = 65265, DstPort = DNS(53), Length = 38
  SrcPort: 65265
  DstPort: DNS(53)
  TotalLength: 38 (0x26)
  Checksum: 31269 (0x7A25)
  UDPPayload: SourcePort = 65265, DestinationPort = 53

+ Dns: QueryId = 0xDF04, QUERY (Standard query), Query for www.bing.com
of type Host Addr on class Internet
```

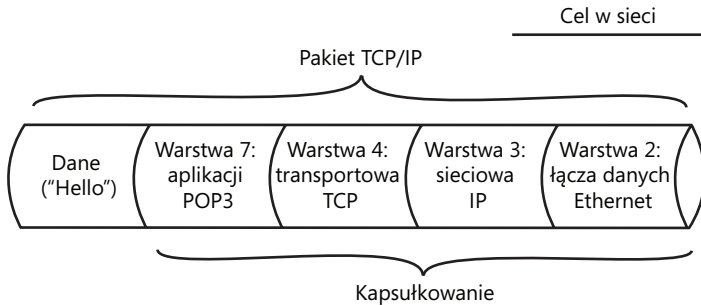
Tym, co najbardziej uderza w nagłówku UDP, jest jego prostota w porównaniu z TCP. Powodem tej prostoty jest skromna liczba funkcji zapewnianych przez UDP. Nie ma tu informacji o kolejności, nie ma potwierdzeń, nie ma kontroli przepływu ani żadnych flag. UDP nie stosuje również wymiany komunikatów ani sesji dwukierunkowej, która ma początek i koniec. Dane transportowane przy użyciu protokołu UDP są po prostu wysyłane na adres i port docelowy i jeśli odbiorca ich nie otrzyma, to strumień bajtów przepada.

Warstwa aplikacji

Warstwa aplikacji – nazywana czasem warstwą 7. – jest etapem, na którym ma miejsce standaryzacja usług sieciowych. Do protokołów warstwy aplikacji należą na przykład protokoły poczty elektronicznej zapewniające określone usługi użytkownikom i różnym aplikacjom. Oprócz protokołów związanych z pocztą elektroniczną, takich jak POP3, SMTP czy IMAP4, do przykładów protokołów warstwy aplikacji natywnych dla pakietu TCP/IP należą HTTP, Telnet, FTP, TFTP (Trivial File Transfer Protocol), SNMP (Simple Network Management Protocol), DNS i NNTP (Network News Transfer Protocol).

Kapsułkowanie TCP/IP

Poprzez kapsułkowanie danych przez każdą z opisanych powyżej czterech warstw TCP/IP tworzy pakiet, taki jak pokazany na uproszczonym przykładzie na rysunku 1-8. Na rysunku tym komunikat e-mail „Hello” jest kapsułkowany w nagłówki POP3 email (warstwa 7), TCP (warstwa 4), IP (warstwa 3) i Ethernet (warstwa 2).



Rysunek 1-8 Przykład pakietu TCP/IP

Uwaga Liczba protokołów w każdym pakiecie może się zmieniać

Pakiet pokazany na rysunku 1-8 jest uproszczony, ponieważ nie każdy pakiet rzeczywiście zawiera dane kapsułkowane przez dokładnie cztery protokoły. Na przykład wiele pakietów jest przeznaczonych wyłącznie do komunikacji w niższych warstwach, takich jak TCP, i dlatego zawiera mniej protokołów. Inne pakiety mogą zawierać więcej niż cztery protokoły, jeśli w jakiejś warstwie istnieje więcej niż jeden protokół. Na przykład w warstwie 4 w jednym pakiecie może występować razem wiele usług i protokołów aplikacji wysokiego poziomu.



Pytania kontrolne

1. W jakiej warstwie sieciowej znajduje się Ethernet?
2. Co robią domyślne routery z rozgłoszeniami w sieci?

Odpowiedzi

1. W warstwie 2.
2. Routery domyślnie blokują rozgłoszenia.

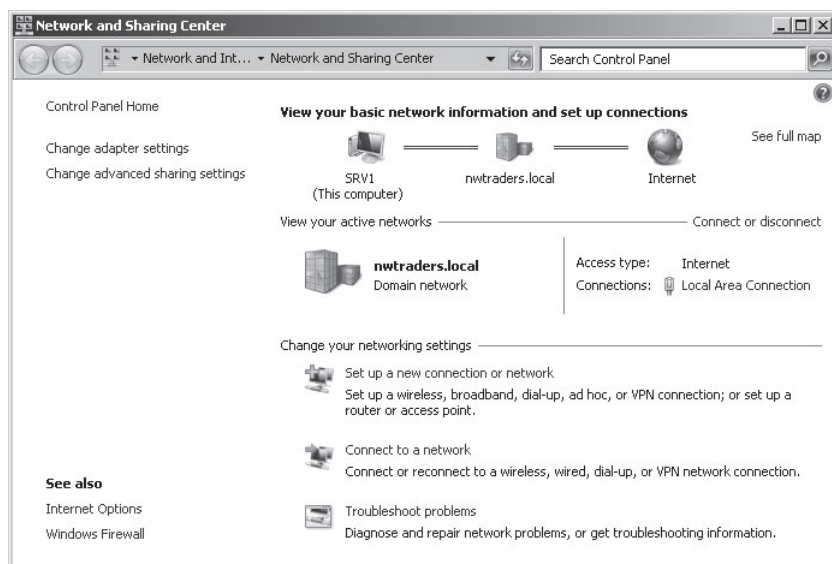
Konfigurowanie właściwości w systemie Windows Server 2008 R2

Konfigurację właściwości sieciowych w interfejsie systemu Windows Server 2008 R2 wykonuje się w dwóch głównych obszarach: Network and Sharing Center (Centrum sieci i udostępniania) i Network Connections (Połączenia sieciowe). Kolejne podrozdziały opisują te obszary w interfejsie Windows Server 2008 R2 i ustawienia, jakie możemy w nich konfigurować.

Network and Sharing Center

Network and Sharing Center to główne narzędzie konfiguracji ustawień sieciowych w Windows Server 2008 R2. Aby otworzyć Network and Sharing Center z menu Start, klikamy prawym przyciskiem myszy Network (Sieć) i wybieramy Properties (Właściwości). Alternatywnie w obszarze Notification klikamy prawym przyciskiem myszy ikonę sieci i wybieramy Network And Sharing Center z menu podręcznego. Trzecią opcją jest także znalezienie Network and Sharing Center po przejściu do Control Panel\Network and Internet\Network and Sharing Center (Panel sterowania\Sieć i Internet\Centrum sieci i udostępniania).

Network and Sharing Center pokazano na rysunku 1-8.



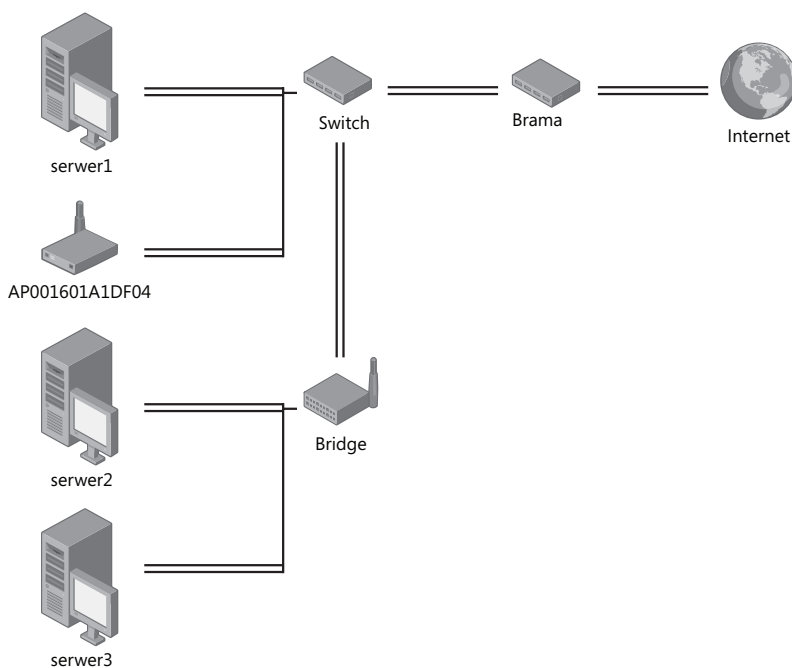
Rysunek 1-9 Network and Sharing Center

Używając Network and Sharing Center można sprawdzić podstawową konfigurację sieci i dostęp do Internetu. Można również skorzystać z dostępnych łączy i uruchomić kreator rozwiązywania problemów, otworzyć stronę Local Area Connection (lub innego aktywnego połączenia), utworzyć nowe połączenie oraz wykonać wiele innych zadań.

Większość opcji dostępnych w oknie Network and Sharing Center nie wymaga wyjaśnienia. Dwie z nich mogą być jednak mniej zrozumiałe.: Change Advanced Sharing Settings (zmień zaawansowane ustawienia udostępniania) i See Full Map (zobacz pełną mapę).

Opcja Change Advanced Sharing Settings w Network and Sharing Center odnosi się do standardowych ustawień lokalnego komputera w takich profilach sieciowych, jak Home (dom), Work (praca) czy Public (publiczna). W każdym z tych profili sieciowych można tak skonfigurować komputer lokalny, aby miał włączony lub wyłączony protokół Network Discovery (protokół umożliwiający przeglądanie), File and Printer Sharing, Public Folder Sharing oraz Media Streaming. Ustawienia te dotyczą jednak głównie środowiska pracy grupowej i nie są sprawdzane na egzaminie 70-642. W środowisku Domain (Domena) serwery mają automatycznie ustawiany profil sieciowy Domain, a standardowe funkcje włączone w tym profilu powinny być ustawione dla całej domeny za pomocą Zasad grupy.

Opcja See Full Map w Network and Sharing Center pozwala zobaczyć, jakie urządzenia są w lokalnej sieci i jak te urządzenia są połączone pomiędzy sobą i z Internetem. Opcja ta jest standardowo wyłączona w profilu sieciowym Domain, ale można ją włączyć w Zasadach grupy. Przykładowa mapa sieci jest pokazana na rysunku 1-10.



Rysunek 1-10 Mapa sieci

Network Map bazuje na dwóch komponentach:

- Komponent Link Layer Topology Discovery (LLTD) Mapper odpytuje sieć o urządzenia do uwzględnienia w mapie.
- Komponent LLTD Responder odpowiada na zapytania z Mapper I/O.

Chociaż komponenty te są zawarte tylko w systemach Windows Vista, Windows 7, i Windows Server 2008 R2, możemy zainstalować komponent LLTD Responder na komputerach z systemem Windows XP, aby mogły pojawiać się na Network Map w innych komputerach.

Wskazówka egzaminacyjna

Pamiętajmy, że aby komputer z systemem Windows XP pojawiał się na mapie sieci, trzeba instalować na nim LLTD Responder.

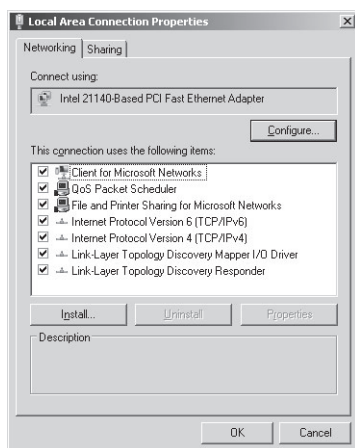
Przeglądanie połączeń sieciowych

Windows Server 2008 R2 automatycznie wykrywa i konfiguruje połączenia związane z kartami sieciowymi zainstalowanymi w lokalnym komputerze. Te połączenia są następnie wyświetlane w Network Connections wraz z dodatkowymi połączeniami, takimi jak połączenia dial-up, które trzeba dodawać ręcznie, klikając opcję Set Up A New Connection Or Network (Skonfiguruj nowe połączenie lub sieć) w Network and Sharing Center.

Okno Network Connections możemy otworzyć na wiele sposobów. Po pierwsze, możemy wybrać węzeł *Server Manager (Menedżer serwera)* w Server Manager, a następnie kliknąć View Network Connections (Wyświetl połączenia sieciowe). Możemy również kliknąć Configure Networking (Konfiguruj sieć) w oknie Initial Configuration Tasks (Zadania konfiguracji początkowej). Możemy też kliknąć Change Adapter Settings (Zmień ustawienia karty sieciowej) w Network and Sharing Center. W końcu możemy wpisać polecenie **ncpa.cpl** w wierszu polecenia, w polu Start Search (Rozpocznij wyszukiwanie) lub w polu Run (Uruchom).

Przeglądanie domyślnych komponentów Network Connections Połączenia same w sobie nie umożliwiają komunikacji hostom sieciowym. Komunikację za pośrednictwem połączenia zapewniają natomiast klienci sieciowi, usługi i protokoły związane z połączeniami. Po otwarciu właściwości konkretnego połączenia w Network Connections (Połączenia sieciowe), na karcie Networking okna dialogowego Properties można zobaczyć klientów, usługi i protokoły związane z tym połączeniem.

Rysunek 1-11 ukazuje domyślne komponenty zainstalowane na lokalnym połączeniu Windows Server 2008. Pola wyboru obok każdego komponentu wskazują, że komponent jest związany z połączeniem.



Rysunek 1-11 Domyślne komponenty połączenia

Poniższa lista zawiera opis trzech rodzajów składników sieciowych, które mogą być związane z połączeniem.

- **Klienci sieci** W Windows *klienci sieci (network clients)* to komponenty programowe, takie jak Client For Microsoft Networks (Klient sieci Microsoft Networks), które pozwalają lokalnemu komputerowi na łączenie się z konkretnym sieciowym systemem operacyjnym. Domyślnie Client For Microsoft Networks jest jedynym klientem sieciowym powiązanym ze wszystkimi lokalnymi połączeniami. Client For Microsoft Networks pozwala komputerom klienckim Windows na łączenie się ze współdzielonymi zasobami udostępnianymi na innych komputerach Windows.
- **Usługi sieciowe** Usługi sieciowe to komponenty programowe, które dostarczają dodatkowe funkcje połączeń sieciowych. File And Printer Sharing For Microsoft Networks (Udostępnianie plików i drukarek w sieciach Microsoft Networks) i QoS Packet Scheduler (Harmonogram pakietów QoS) są dwiema usługami sieciowymi domyślnie związanymi ze wszystkimi połączeniami sieci lokalnych. File And Printer Sharing For Microsoft Networks pozwala komputerowi lokalnemu na udostępnienie folderów przez sieć. QoS Packet Scheduler zapewnia kontrolę ruchu sieciowego w tym usługi tempa przepływu i nadawania priorytetów.
- **Protokoły sieciowe** Komputery mogą komunikować się przez połączenie tylko za pomocą protokołów sieciowych związanych z tym połączeniem. Domyślnie z każdym połączeniem sieciowym są instalowane i łączone cztery protokoły sieciowe: IPv4, IPv6, LLTD (Link-Layer Topology Discovery) Mapper i LLTD Responder.

Mostkowanie połączeń sieciowych

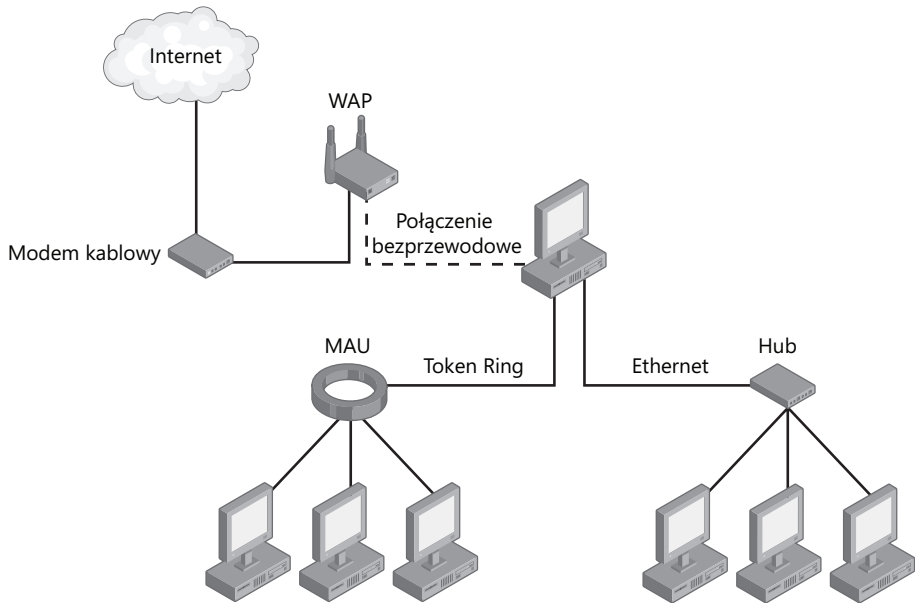
W niektórych przypadkach możemy chcieć połączyć wiele połączeń sieciowych na danym komputerze, aby system Windows traktował je, jakby były w tej samej sieci (w jednej domenie rozgłoszeniowej). Na przykład możemy chcieć współdzielić jeden punkt dostępu bezprzewodowego (WAP) z wieloma różnymi topologiami połączeń, jak pokazano na rysunku 1-12.

W tym przykładzie połączenie internetowe jest połączone do pojedynczego WAP. Następnie WAP komunikuje się z bezprzewodową kartą sieciową (NIC) w serwerze. Dodatkowo serwer ma połączenia Ethernet i Token Ring połączone z innymi sieciami.

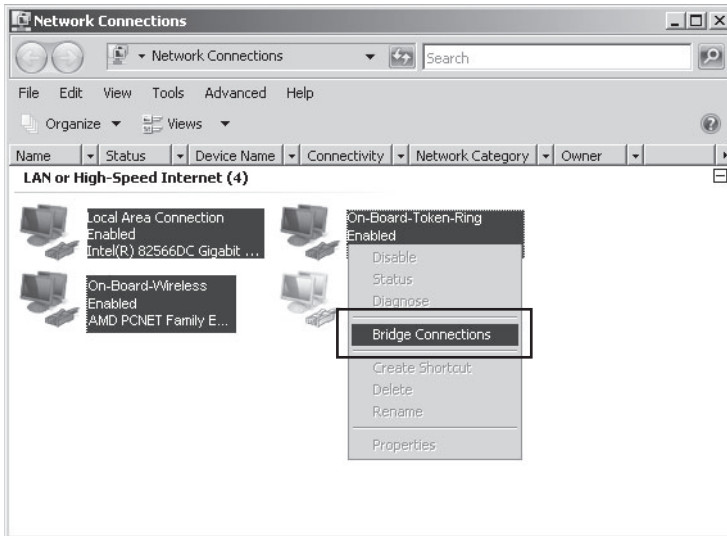
Gdy włączy się *mostkowanie sieci (network bridging)* na tym połączeniu, wszystkie punkty wejścia do serwera (bezprzewodowe, Token Ring i Ethernet) pojawiają się w tej samej sieci. Stąd mogą one wszystkie współdzielić połączenie i wyjście do Internetu.

Aby mostkować sieci, wciskamy Ctrl i wybieramy wiele połączeń sieciowych na serwerze. Następnie klikamy prawym przyciskiem myszy i wybieramy Bridge Connections (Połączenia mostkowe), jak pokazano na rysunku 1-13.

Skonfigurowanie mostkowania sieci pozwala na współdzielenie tej samej przestrzeni sieciowej przez karty bezprzewodowe, Ethernet i Token Ring. W ten sposób jedna karta bezprzewodowa ma stanowić bramę wychodzącą do całkiem odmiennych sieci.



Rysunek 1-12 Przykład mostkowania sieci



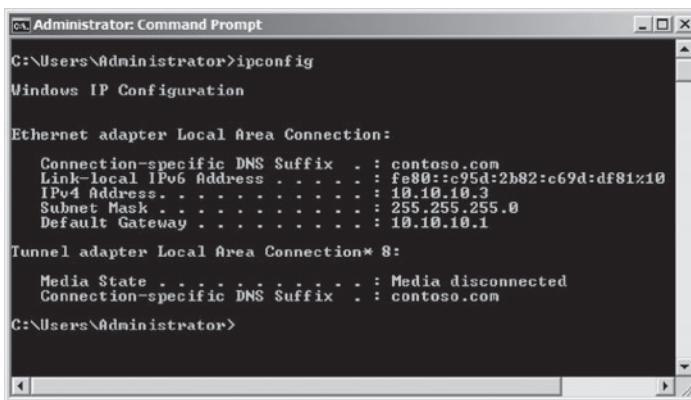
Rysunek 1-13 Mostkowanie sieci

Wyświetlanie konfiguracji adresu

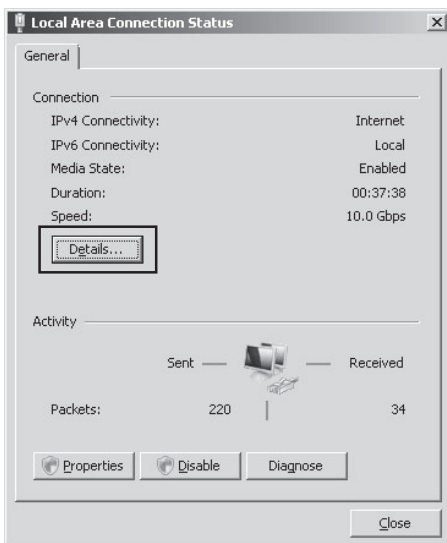
Konfiguracja IP połączenia składa się co najmniej z adresu IPv4 i maski podsieci lub adresu IPv6 i prefiksu podsieci. Poza tymi minimalnymi ustawieniami konfiguracja IP może także objąć takie informacje, jak brama domyślna, adresy serwerów DNS, sufiks nazwy DNS i adresy serwerów WINS.

Aby zobaczyć konfigurację adresu IP danego połączenia, możemy skorzystać z polecenia *Ipconfig* lub z okna dialogowego Network Connection Details (Szczegóły połączenia sieciowego).

W pierwszym wypadku wpisujemy **ipconfig** w wierszu polecenia. Rezultat będzie podobny do tego z rysunku 1-14. Klikamy najpierw połączenie w Network Connections, aby otworzyć okno dialogowe Status (Stan). Następnie w oknie dialogowym Status klikamy przycisk Details (Szczegóły), jak to jest pokazane na rysunku 1-15.

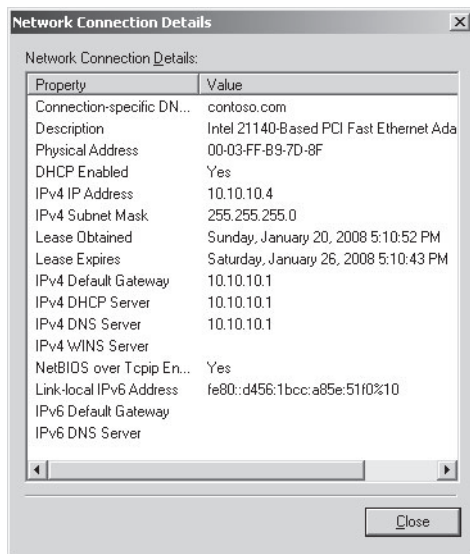


Rysunek 1-14 Wyświetlanie adresu IP



Rysunek 1-15 Okno dialogowe Local Area Connection Status

To ostatnie działanie powoduje otwarcie okna dialogowego Network Connection Details (Szczegóły połączenia sieciowego), pokazanego na rysunku 1-16.



Rysunek 1-16 Okno dialogowe Network Connection Details

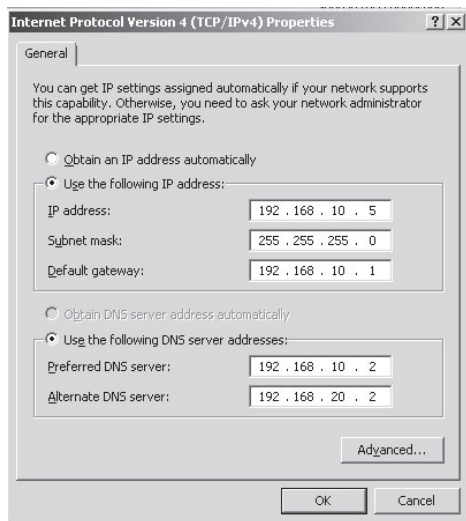
Ręczne określanie konfiguracji IP

Możemy ręcznie lub automatycznie skonfigurować IP połączenia sieciowego. W tym podrozdziale pokażemy, jak ręcznie zdefiniować konfigurację IPv4 i IPv6.

Ręczne nadawanie konfiguracji IPv4 Ręcznie skonfigurowany adres jest nazywany adresem statycznym, ponieważ pozostaje stały po ponownym uruchomieniu komputera. Takie statyczne adresy są odpowiednie dla ważnych serwerów infrastrukturalnych, takich jak kontrolery domen, serwery DNS, serwery DHCP, serwery WINS i routery.

Statyczne adresy i inne parametry konfiguracji IPv4 możemy ręcznie przypisać do połączeń sieciowych, korzystając z okna dialogowego Internet Protocol Version 4 (TCP/IP) Properties (Właściwości: Protokół internetowy w wersji 4 (TCP/IPv4)). W celu uzyskania dostępu do tego okna dialogowego otwieramy właściwości połączenia sieciowego, którego konfigurację IPv4 chcemy określić. (W tym celu można kliknąć prawym przyciskiem myszy konkretne połączenie w oknie Network Connections i wybrać polecenie Properties. Można też kliknąć to połączenie w oknie Network and Sharing Center, a następnie kliknąć Properties w oknie Status). W oknie dialogowym właściwości połączenia klikamy dwukrotnie Internet Protocol Version 4 (TCP/IPv4) (Protokół internetowy w wersji 4 (TCP/IPv4)) na liście komponentów.

Rysunek 1-17 przedstawia okno dialogowe Internet Protocol Version 4 (TCP/IPv4) Properties.



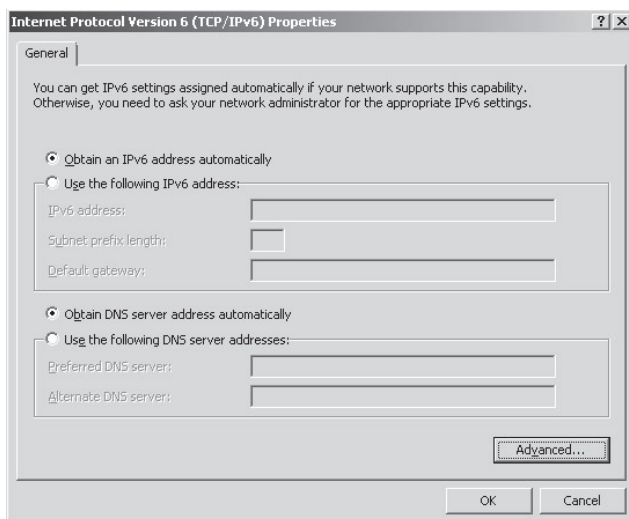
Rysunek 1-17 Ręczne przypisywanie konfiguracji IPv4

Domyślnie połączenia sieciowe są konfigurowane, aby uzyskiwały adres IP i adres serwera DNS automatycznie. Dlatego, aby zmienić to standardowe ustawienie i skonfigurować statyczny adres IP, wybieramy opcję *Use The Following IP Address* (Użyj następującego adresu IP), a następnie określamy adres IP, maskę podsieci i (opcjonalnie) bramę domyślną. Wybieramy opcję *Use The Following DNS Server Addresses* (Użyj następujących adresów serwerów DNS), a następnie określamy preferowany i (opcjonalnie) alternatywny adres serwera DNS, aby określić statyczne parametry serwera DNS dla tego połączenia.

Ręczne określanie konfiguracji IPv6 Na ogół adresu IPv6 nie trzeba konfigurować ręcznie, ponieważ statyczne adresy IPv6 są typowo przypisywane tylko do routerów, a nie do hostów. Zwykle konfiguracja IPv6 jest przypisywana do hosta za pomocą autokonfiguracji.

Możemy jednak określić ręcznie adres IPv6 za pomocą okna dialogowego *Internet Protocol Version 6 (TCP/IPv6) Properties* (Właściwości: Protokół internetowy w wersji 6 (TCP/IPv6)). Otwieramy to okno dialogowe, dwukrotnie klikając *Internet Protocol Version 6 (TCP/IPv6)* (Protokół internetowy w wersji 6 (TCP/IPv6)) we właściwościach połączenia sieciowego. Rysunek 1-18 ukazuje okno dialogowe *Internet Protocol Version 6 (TCP/IPv6) Properties*.

Tak jak w przypadku IPv4, połączenia sieciowe są konfigurowane do automatycznego uzyskiwania adresu IPv6 i do automatycznego uzyskiwania adresu serwera DNS. Wybieramy opcję *Use The Following IPv6 Address* (Użyj następującego adresu IPv6) i określamy adres IPv6, długość prefiksu podsieci (typowo 64) i (opcjonalnie) bramę domyślną, aby skonfigurować statyczny adres IPv6. Zauważmy, że jeśli skonfigurowaliśmy statyczny adres IPv6, musimy także określić statyczny adres serwera DNS dla IPv6.



Rysunek 1-18 Konfigurowanie ustawień IPv6

Ręczne konfigurowanie ustawień IPv4 i IPv6 z wiersza polecenia Konfigurację IP połączenia możemy wykonać ręcznie w wierszu polecenia tekstowego, korzystając z narzędzia Netsh. Oto polecenie, które wpisujemy w wierszu polecenia, aby określić stały adres IPv4 i maskę podsieci dla połączenia, gdzie *Connection_Name* jest nazwą połączenia (taką jak Local Area Connection), *Address* to adres IPv4, a *Subnet_Mask* to maska podsieci.

```
netsh interface ipv4 set address "Connection_Name" static Address Subnet_Mask
```

Na przykład, aby określić adres IPv4 połączenia Local Area Connection na 192.168.33.5 z maską podsieci 255.255.255.0, możemy wpisać polecenie:

```
netsh interface ipv4 set address "local area connection" static 192.168.33.5  
255.255.255.0
```

Jeśli wraz z konfiguracją IPv4 chcemy dodatkowo skonfigurować bramę domyślną, możemy dodać tę informację na końcu polecenia. Na przykład, aby skonfigurować ten sam adres IPv4 dla połączenia local area connection z bramą domyślną 192.168.33.1, wpisujemy:

```
netsh interface ip set address "local area connection" static 192.168.33.5  
255.255.255.0 192.168.33.1
```

Uwaga Alternatywna składnia Netsh

Istnieje wiele poprawnych odmian składni Netsh. Na przykład możemy wpisać **netsh interface ip** zamiast **netsh interface ipv4**. Więcej informacji znajduje się w Netsh Help.

Oto co wpisujemy w wierszu polecenia, aby przypisać stały adres IPv6 do połączenia, gdzie *Connection_Name* to nazwa połączenia, a *Address* to adres IPv6.

```
netsh interface ipv6 set address "Connection_Name" Address
```

Na przykład, aby przypisać adres 2001:db8:290c:1291::1 do Local Area Connection (pozostawiając domyślny prefiks podsieci o długości 64), wpisujemy:

```
netsh interface ipv6 set address "Local Area Connection" 2001:db8:290c:1291::1
```

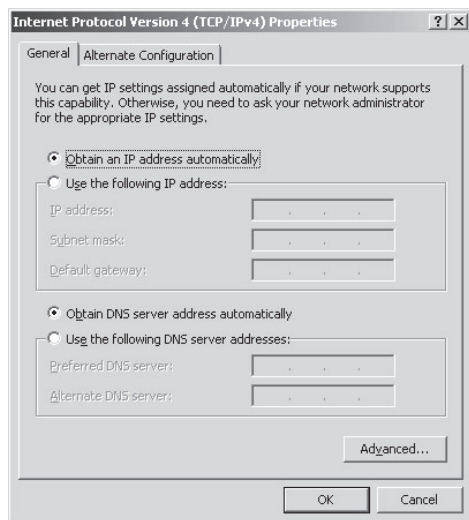
Narzędzie Netsh udostępnia wiele innych opcji do konfigurowania zarówno IPv4, jak i IPv6. Więcej informacji na temat opcji i składni znajduje się w Netsh Help.

Konfigurowanie połączenia IPv4 do automatycznego uzyskiwania adresu

W domyślnej konfiguracji połączenia uzyskują automatycznie adresy IPv4. Komputer z tak skonfigurowanym połączeniem jest nazywany klientem DHCP.

W efekcie tego ustawienia wszystkie połączenia sieciowe będą dostawać adres IPv4 od serwera DHCP, jeśli jest on dostępny. Jeżeli nie ma dostępnych żadnych serwerów DHCP, połączenie będzie automatycznie przypisywać sobie uprzednio zdefiniowaną alternatywną konfigurację. Jeżeli nie zdefiniuje się żadnej alternatywnej konfiguracji, połączenie będzie automatycznie przypisywać sobie adres APIPA (Automatic Private IP Addressing) dla IPv4.

Chcąc skonfigurować połączenie do automatycznego uzyskiwania adresu IPv4, wybieramy odpowiednią opcję w oknie Internet Protocol Version 4 (TCP/IPv4) Properties, jak pokazano na rysunku 1-19.



Rysunek 1-19 Konfigurowanie połączenia w celu automatycznego uzyskania adresu IPv4 (ustawienie domyślne)

Możemy także użyć narzędzia Netsh, aby skonfigurować klienta do automatycznego uzyskania adresu IPv4. W tym celu w wierszu polecenia wpisujemy poniższe polecenie, gdzie *Connection_Name* to nazwa połączenia sieciowego:

```
netsh interface ip set address "Connection_Name" dhcp
```

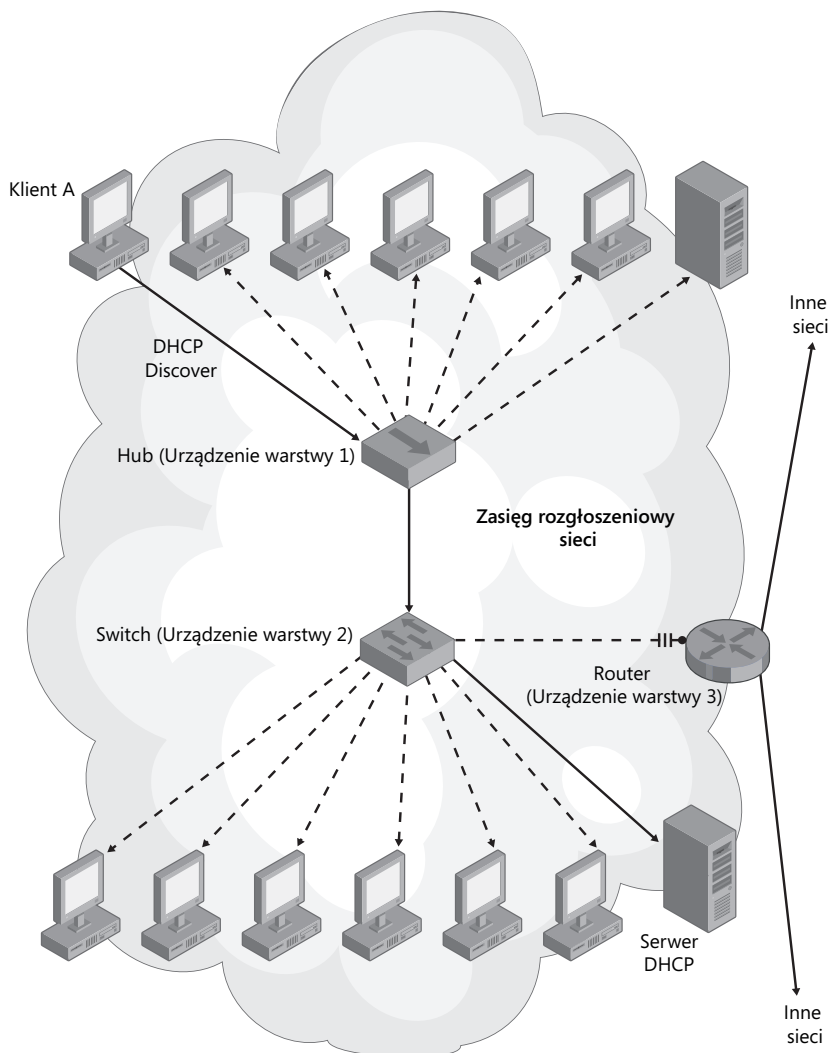
Na przykład, aby skonfigurować połączenie Local Area Connection do automatycznego uzyskiwania adresu, wpisujemy:

```
netsh interface ip set address "Local Area Connection" dhcp
```

Adresy przypisywane przez DHCP Adresy przypisywane przez DHCP zawsze mają priorytety wyższe niż inne automatyczne metody konfiguracji IPv4. Host w sieci IP może otrzymać adres IP z serwera DHCP, gdy serwer DHCP (lub DHCP Relay Agent) jest zlokalizowany w jego domenie rozgłoszeniowej.

Rozgłaszanie sieciowe to transmisja, która jest kierowana do wszystkich lokalnych adresów. Takie rozgłoszenie propaguje się przez wszystkie sieci urządzenia warstw 1 i 2 (takie jak kable, repeatery, huby, bridge i switche), ale jest blokowane przez urządzenia warstwy 3 (routery). Komputery, które mogą komunikować się ze sobą przez rozgłoszenia, są nazywane zlokalizowanymi w tej samej domenie rozgłoszeniowej.

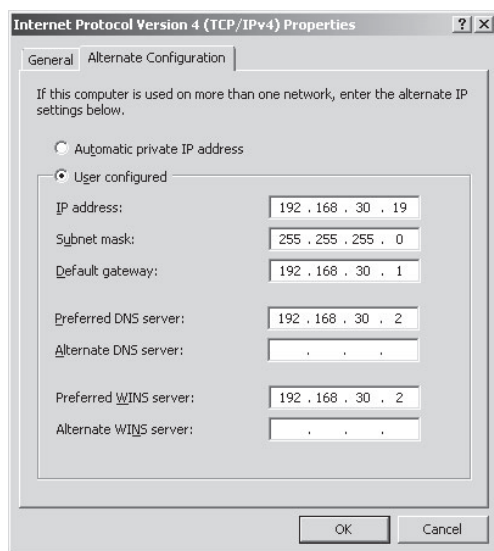
Rozgłaszanie sieciowe zilustrowano na rysunku 1-20.



Rysunek 1-20 Klient A może otrzymać adres IP z serwera DHCP, ponieważ te dwa komputery leżą w tej samej domenie rozgłoszeniowej. Zauważmy, że obszar rozgłoszeniowy dochodzi tylko do routera.

Definiowanie konfiguracji alternatywnej Jeżeli żaden serwer DHCP nie jest dostępny w domenie rozgłoszeniowej klienta, klient skonfigurowany do automatycznego uzyskiwania adresu domyślnie przyjmie konfigurację alternatywną, jeżeli ją zdefiniujemy.

Możemy przypisać alternatywną konfigurację do połączenia, wybierając kartę Alternate Configuration (Konfiguracja alternatywna) w oknie dialogowym Internet Protocol Version 4 (TCP/IPv4) Properties. Tę kartę pokazano na rysunku 1-21. Zauważmy, że alternatywna konfiguracja pozwala na określanie adresu IP, maski podsieci, bramy domyślnej, serwera DNS i serwera WINS.



Rysunek 1-21 Definiowanie alternatywnej konfiguracji IPv4

Ponieważ alternatywna konfiguracja pozwala na nadanie komputerowi specyficznej szczegółowej konfiguracji IP, gdy nie można znaleźć żadnego serwera DHCP, definiowanie alternatywnej konfiguracji jest użyteczne w przypadku komputerów przenośnych, które podłącza się do sieci z serwerami DHCP i bez nich.

Wskazówka egzaminacyjna

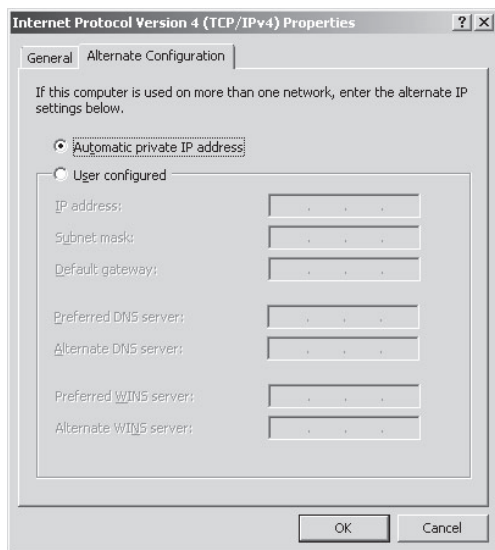
Zrozumienie zalet konfiguracji alternatywnej jest konieczne do egzaminu 70-642.

Zrozumienie adresowania APIPA (Automatic Private IP Addressing) APIPA to funkcja automatycznego adresowania użyteczna w pewnych sieciach ad hoc i tymczasowych. Kiedy komputer Windows jest skonfigurowany do uzyskiwania adresu IP automatycznie, a nie jest dostępny żaden serwer DHCP, ani nie jest określona alternatywna konfiguracja, komputer korzysta z APIPA do przypisania sobie prywatnego adresu IP z zakresu od 169.254.0.1 do 169.254.255.254 i maski podsieci 255.255.0.0.

Domyślnie wszystkie połączenia sieciowe przyjmują adresy APIPA, gdy żaden serwer DHCP nie jest dostępny. To ustawienie pokazano na rysunku 1-22.

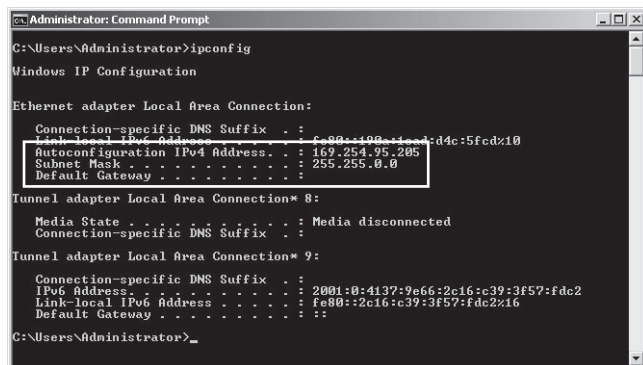
Funkcja APIPA jest bardzo użyteczna, ponieważ umożliwia komunikację dwu lub więcej komputerom Windows zlokalizowanym w tej samej domenie rozgłoszeniowej, w której nie

ma serwera DHCP, bez konieczności ręcznego wykonywania konfiguracji przez użytkownika. Umożliwia to także komunikację klientom DHCP w razie awarii DHCP. Gdy serwer DHCP później stanie się dostępny, adres APIPA będzie zastąpiony przez adres otrzymany od serwera DHCP.



Rysunek 1-22 Domyślnie połączenia sieciowe mają konfigurowany adres APIPA w razie nieobecności serwera DHCP.

Rysunek 1-23 ukazuje konfigurację adresu APIPA.



Rysunek 1-23 Adres APIPA jest oznaką problemu w sieci.

Wskazówka egzaminacyjna

Gdy dwa komputery klienckie mogą widzieć się nawzajem, ale nie mogą połączyć się z niczym innym w sieci (lub Internecie), możemy podejrzewać konfigurację APIPA. Występuje wtedy problem z serwerem DHCP w naszej sieci lub uszkodzenie połączenia z tym serwerem.

Chociaż adres APIPA umożliwia pewną komunikację w sieci lokalnej, ma znaczne ograniczenia. Połączenia z przypisanymi adresami APIPA mogą komunikować się tylko z innymi komputerami korzystającymi z adresów APIPA w obrębie domeny rozgłoszeniowej sieci. Takie komputery nie mogą mieć dostępu do Internetu. Zauważmy także, że w konfiguracji APIPA nie możemy określić adresu serwera DNS, adresu bramy domyślnej ani adresu serwera WINS.

Naprawianie połączenia sieciowego za pomocą *Ipconfig /renew* i funkcji Diagnose (Diagnostuj) Typowo adres APIPA przypisany do połączenia jest oznaką, że to połączenie nie otrzymało właściwego adresu IP z serwera DHCP. Ponieważ połączenia z przypisanymi adresami APIPA mogą komunikować się tylko z pobliskimi komputerami, które także mają przypisane adresy APIPA, takie adresy są zwykle niepożądane. W przypadku połączeń z adresami APIPA należy się spodziewać braku łączności lub jej ograniczeń.

Jeżeli połączenie ma przypisany adres APIPA, a w sieci nie jest dostępny żaden serwer DHCP, możemy albo zainstalować serwer DHCP, albo przypisać połączeniu statyczną konfigurację IP lub konfigurację alternatywną.

Jeżeli połączenie ma przypisany adres APIPA w sieci, w której działa już serwer DHCP, spróbujemy najpierw odnowić konfigurację IP lub użyć funkcji Diagnose dla tego połączenia. Aby odnowić konfigurację, korzystając z wiersza polecenia, wpisujemy **ipconfig /renew**. Natomiast jeśli chcemy skorzystać z Network Connections, klikamy prawym przyciskiem myszy połączenie, do którego został przypisany adres APIPA, a następnie wybieramy Diagnose z menu podręcznego (można też kliknąć Troubleshoot Problems w Network and Sharing Center). Mamy wtedy szansę naprawy połączenia.

Gdy ta strategia nie przyniesie efektu w postaci przypisania nowego adresu IP hosta, powinniśmy sprawdzić, czy serwer DHCP działa właściwie. Jeżeli serwer DHCP działa, przejdźmy do sprawdzania problemów sprzętowych, takich jak uszkodzone lub odłączone kable, huby i switchy, które mogą występować pomiędzy serwerem DHCP a klientem.

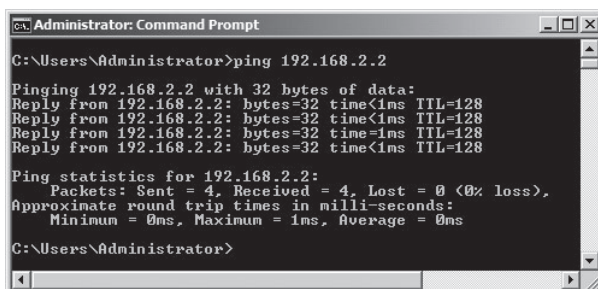
Uwaga Odnawianie konfiguracji IPv6

Wpisujemy `ipconfig /renew`, aby odnowić konfigurację IPv6.

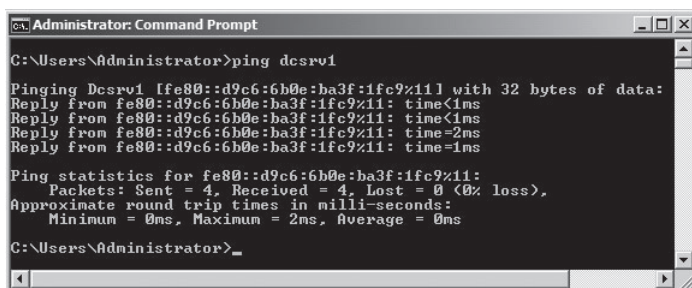
Rozwiązywanie problemów z łącznością sieciową za pomocą Ping, Tracert, PathPing i Arp Jeżeli ani zastosowanie funkcji Diagnose, ani polecenia *Ipconfig /renew* nie rozwiązało problemu sieciowego, użyjmy w tym celu takich narzędzi, jak Ping, Tracert, PathPing i Arp, opisanych dalej w tej lekcji.

■ **Ping** Ping to kluczowe narzędzie stosowane do testowania łączności sieciowej. Wpisujemy **ping remote_host** w wierszu polecenia, gdzie *remote_host* to nazwa lub adres IP zdalnego komputera, serwera lub routera, z którymi chce się sprawdzić łączność. Jeżeli komputer zdalny odpowiada na polecenie ping, wiadomo, że mamy z nim łączność. Rysunek 1-24 ukazuje pomyślną próbę użycia polecenia ping do komputera o adresie 192.168.2.2.

Na rysunku 1-25 polecenie ping odnosi się do adresu IPv4 i odpowiedź pochodzi z tego samego adresu. Jednak w niektórych przypadkach polecenie ping może odnosić się do adresu IPv6, na przykład w środowisku grupy roboczej, w którym komputer docelowy jest wskazywany przez nazwę. Taka sytuacja pokazana jest na rysunku 1-25.



Rysunek 1-24 Pomyślne działanie polecenia ping ukazuje, że lokalny komputer może komunikować się z komputerem o adresie 192.168.2.2.



Rysunek 1-25 Polecenie ping używa czasem adresu IPv6 do komunikacji ze zdalnym komputerem.

Rzut oka na ruch typu Ping

Narzędzia Ping, Tracert i Pathping są oparte na protokole komunikatów warstwy 3 o nazwie ICMP (Internet Control Message Protocol). Na rysunku 1-26 pokazany jest przechwycony ruch w sieci dla polecenia ping z rysunku 1-24.

Frame Summary			
Source	Destination	Protocol Name	Description
		NetmonFilter	NetmonFilter:Updated Capture Filter: Nor
		NetworkInfoEx	NetworkInfoEx:Network info for , Networ
192.168.2.201	192.168.2.2	ICMP	ICMP:Echo Request Message, From 192.168.2.201
192.168.2.2	192.168.2.201	ICMP	ICMP:Echo Reply Message, From 192.168.2.2
192.168.2.201	192.168.2.2	ICMP	ICMP:Echo Request Message, From 192.168.2.201
192.168.2.2	192.168.2.201	ICMP	ICMP:Echo Reply Message, From 192.168.2.2
192.168.2.201	192.168.2.2	ICMP	ICMP:Echo Request Message, From 192.168.2.201
192.168.2.2	192.168.2.201	ICMP	ICMP:Echo Reply Message, From 192.168.2.2
192.168.2.201	192.168.2.2	ICMP	ICMP:Echo Request Message, From 192.168.2.201
192.168.2.2	192.168.2.201	ICMP	ICMP:Echo Reply Message, From 192.168.2.2
192.168.2.2	192.168.2.201	ARP	ARP:Request, 192.168.2.2 asks for 192.168.2.201
192.168.2.201	192.168.2.2	ARP	ARP:Response, 192.168.2.201 at 00-15-57-00-00-00

Rysunek 1-26 Ruch sieciowy dla pomyślnej próby użycia polecenia Ping

Na rysunku widać osiem komunikatów ICMP. Tych osiem komunikatów dotyczy czterech kolejnych prostych wymian ICMP. Pierwszy komunikat, Echo Request Message (prośba o echo), jest wysyłany z lokalnego komputera (192.168.2.201) do zdalnego komputera o adresie 192.168.2.2. Następnie zdalny komputer 192.168.2.2 wysyła do lokalnego komputera drugi komunikat – Echo Reply Message (odpowiedź-echo). To właśnie takie cztery odpowiedzi widać w przechwyconym ruchu i odpowiadają one czterem komunikatom „Reply from...” wyświetlanym w kolejnych wierszach po wykonaniu polecenia ping. (Ping nie wyświetla oddzielnie każdej kolejnej prośby o echo). Występuje specjalna wersja ICMP o nazwie ICMPv6, która jest używana do protokołu IPv6. Ruch sieciowy przechwycony dla polecenia ping w przypadku protokołu IPv6 wygląda bardzo podobnie do przypadku IPv4, co widać na rysunku 1-27. Rysunek ten przedstawia ruch sieciowy przechwycony dla tego samego polecenia ping, co rysunek 1-25.

Source	Destination	Protocol Name	Description
Dcsrv1	FE80:0:0:0:5C46:F4DD:7A11:50F9	LLMNR	LLMNR:QueryId = 0x...
FE80:0:0:0:5C46:F4DD:7A11:50F9	Dcsrv1	ICMPv6	ICMPv6:Echo request
Dcsrv1	FE80:0:0:0:5C46:F4DD:7A11:50F9	ICMPv6	ICMPv6:Echo reply, II
FE80:0:0:0:5C46:F4DD:7A11:50F9	Dcsrv1	ICMPv6	ICMPv6:Echo request
Dcsrv1	FE80:0:0:0:5C46:F4DD:7A11:50F9	ICMPv6	ICMPv6:Echo reply, II
FE80:0:0:0:5C46:F4DD:7A11:50F9	Dcsrv1	ICMPv6	ICMPv6:Echo request
Dcsrv1	FE80:0:0:0:5C46:F4DD:7A11:50F9	ICMPv6	ICMPv6:Echo reply, II
FE80:0:0:0:5C46:F4DD:7A11:50F9	Dcsrv1	ICMPv6	ICMPv6:Echo request
Dcsrv1	FE80:0:0:0:5C46:F4DD:7A11:50F9	ICMPv6	ICMPv6:Echo reply, II
Dcsrv1	FF02:0:0:0:0:1:2	DHCPv6	DHCPv6:MessageTyp...

Rysunek 1-27 Ruch sieciowy przechwycony dla pomyślnej próby użycia polecenia Ping w wersji IPv6

WAŻNE ICMP, zapory i Ping

ICMP jest domyślnie blokowany przez Windows Firewall (Zaporę systemu Windows), a także przez niektóre routery i samodzielne zapory. W konsekwencji, aby skutecznie użyć poleceń Ping, Tracert i PathPing, trzeba zapewnić, że ICMP nie będzie blokowany przez zdalny host. Aby włączyć wyjątek zapory dla ICMP w komputerze z systemem Windows Server 2008 R2, należy za pomocą konsoli Windows Firewall with Advanced Security (Zapora systemu Windows z zabezpieczeniami zaawansowanymi) włączyć regułę zapory File and Printer Sharing (Echo Request – ICMPv4-In). Aby włączyć wyjątek zapory dla wersji ICMPv6, należy włączyć regułę File and Printer Sharing (Echo Request – ICMPv6-In). Można również włączyć te reguły dla całej domeny za pomocą Zasad grupy.

- **Tracert** Tracert to narzędzie sieciowe, które śledzi ścieżkę od komputera lokalnego do zdalnego i testuje stan każdego routera po drodze. Na przykład, jeżeli ścieżka z serwera ServerA do ServerE przechodzi przez RouterB, RouterC i RouterD, możemy użyć Tracert do testowania, czy każdy z tych pośrednich routerów (a także docelowy serwer ServerE) może odpowiadać na komunikaty ICMP. Celem tego testu jest zlokalizowanie przerwy w łączności znajdującej się pomiędzy lokalnym komputerem a odległym celem.

W wierszu polecenia wpisujemy **tracert remote_host**, gdzie *remote_host* jest nazwą lub adresem docelowego komputera, serwera lub routera.

Poniżej pokazano rezultat polecenia Tracert. Zauważmy, że przełącznik **-d** służy do przyspieszenia testu przez zapobieganie tłumaczenia każdego adresu IP na nazwę.

```
C:\Users\jcmackin>tracert -d 69.147.114.210
```

```
Tracing route to 69.147.114.210 over a maximum of 30 hops
```

1	1 ms	<1 ms	<1 ms	192.168.2.1
2	822 ms	708 ms	659 ms	67.142.148.2
3	708 ms	649 ms	658 ms	67.142.131.209
4	632 ms	619 ms	629 ms	67.142.131.254
5	726 ms	698 ms	619 ms	67.142.128.246
6	732 ms	679 ms	709 ms	65.46.24.177
7	713 ms	650 ms	679 ms	207.88.81.245
8	732 ms	719 ms	719 ms	71.5.170.41
9	957 ms	739 ms	719 ms	71.5.170.34
10	734 ms	736 ms	677 ms	64.212.107.85
11	723 ms	690 ms	862 ms	64.208.110.166
12	824 ms	849 ms	739 ms	216.115.101.137
13	781 ms	799 ms	869 ms	216.115.101.152
14	822 ms	719 ms	678 ms	216.115.108.72
15	759 ms	709 ms	799 ms	216.115.108.61
16	724 ms	819 ms	1479 ms	68.142.238.65
17	775 ms	859 ms	739 ms	69.147.114.210

```
Trace complete.
```

- **PathPing** PathPing przypomina Tracert, ale w przeciwieństwie do niego ma na celu znajdowanie łączy, które powodują *sporadyczne* straty danych. PathPing wysyła przez pewien czas pakiety do każdego routera na drodze do końcowego celu, a następnie oblicza procent pakietów zwróconych z każdego przeskoku. Ponieważ PathPing ukazuje stopień strat pakietów na każdym routerze lub łączy, możemy użyć tego polecenia do wskazania, które routery lub łączy mogą powodować problemy z siecią.

Wpisujemy **PathPing remote_host** w wierszu polecenia, przy czym *remote_host* to nazwa lub adres docelowego komputera, serwera lub routera, gdzie na ścieżce prowadzącej do niego chcemy testować sporadyczne straty danych.

Oto przykład wyników polecenia PathPing:

```
D:\>pathping -n testpc1
Tracing route to testpc1 [7.54.1.196]
over a maximum of 30 hops:
0 172.16.87.35
1 172.16.87.218
2 192.168.52.1
3 192.168.80.1
4 7.54.247.14
5 7.54.1.196
Computing statistics for 25 seconds...
Source to Here This Node/Link
Hop RTT Lost/Sent = Pct Lost/Sent = Pct Address
0 0/ 100 = 0% | 172.16.87.35
1 41ms 0/ 100 = 0% 0/ 100 = 0% 172.16.87.218
```

```

      13/ 100 = 13% |
2    22ms 16/ 100 = 16% 3/ 100 = 3%      192.168.52.1
      0/ 100 = 0% |
3    24ms 13/ 100 = 13% 0/ 100 = 0%      192.168.80.1
      0/ 100 = 0% |
4    21ms 14/ 100 = 14% 1/ 100 = 1%      7.54.247.14
      0/ 100 = 0% |
5    24ms 13/ 100 = 13% 0/ 100 = 0%      7.54.1.196
Trace complete.

```

Zauważmy, że powyższe wyniki najpierw ukazują pięć przeskoków na ścieżce do określonego celu, a następnie obliczenia procenta strat danych pomiędzy każdym z tych przeskoku. W tym przypadku PathPing ukazuje 13 procent straty danych pomiędzy lokalnym komputerem (172.16.87.35) a pierwszym przeskoku (172.16.87.218).

- **Arp** Arp jest nazwą zarówno narzędzia, jak i protokołu. Protokół ARP (Address Resolution Protocol) służy do tłumaczenia adresów IPv4 (programowych) komputera lub routera w domenie rozgłoszeniowej na adresy MAC (sprzętowe) konkretnych interfejsów w sieci. Innymi słowy, protokół ARP pozwala komputerowi fizycznie komunikować się z sąsiednim komputerem lub routerem reprezentowanym przez adres IPv4. Narzędzie Arp pełni związaną z tym funkcję. Możemy korzystać z niego do wyświetlania lub zarządzania buforem ARP komputera, który przechowuje mapowanie adresów IPv4 na adresy MAC innych komputerów w sieci lokalnej.

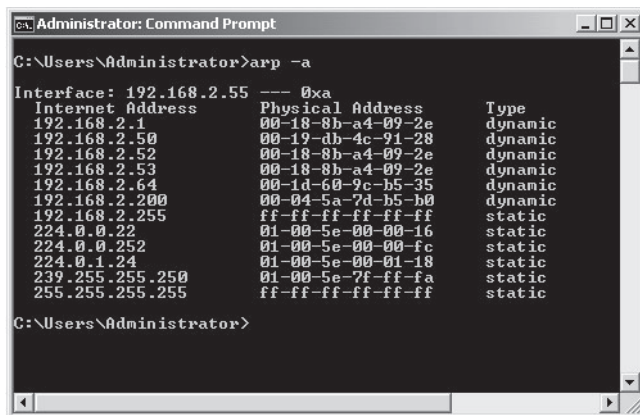
Ponieważ połączenie z komputerem w domenie rozgłoszeniowej zależy od poprawnego mapowania adresu IPv4 na adres MAC komputera w lokalnym buforze ARP, narzędzie Arp może pomóc naprawić te problemy z siecią, których przyczyną jest niewłaściwe mapowanie. Wyświetlając bufor za pomocą polecenia **arp -a**, możemy wykryć problem – na przykład z dwiema sąsiednimi wirtualnymi maszynami, które mają przypisany ten sam wirtualny adres MAC (jest to całkiem częste). Możemy także użyć polecenia **arp -d** do usunięcia wpisu w buforze ARP komputera lub maszyny wirtualnej, której adres MAC został już zmieniony i wiemy, że stary jest nieprawidłowy.

W rzadkich sytuacjach możemy także użyć narzędzia Arp do wykrycia próby zatrucia bufora ARP poprzez przypisanie niektórych lub wszystkich lokalnych adresów IPv4, szczególnie adresu IPv4 lokalnego routera, z własnym adresem MAC używanym przez lokalnego hakera. Jest to dobrze znana technika, która pozwala hakerowi potajemnie przeprowadzać połączenia sieciowe przez jego własny komputer.

Przykład zatrutego bufora ARP pokazano na rysunku 1-28. Zauważmy, że adresy IPv4 192.168.2.1, 192.168.2.52 i 192.168.2.53 są wszystkie związane z tym samym adresem MAC. Jeżeli komputer hakera jest reprezentowany przez 192.168.2.52, ten bufor ARP może umożliwić przechwytywanie wszystkich połączeń do 192.168.2.1 i 192.168.2.53. Jeżeli 192.168.2.1 reprezentuje adres IPv4 lokalnego routera, mogą być przechwytywane wszystkie komunikaty internetowe.

Uwaga Czy zawsze duplikaty adresów w buforze ARP oznaczają problem?

O ile nie ma się przypisanych dwóch lub więcej adresów IPv4 do pojedynczej karty sieciowej gdzieś w sieci lokalnej (jest to rzadkie, ale możliwe), każdy adres IPv4 w buforze ARP powinien być związany jednoznacznie z jednym adresem fizycznym.



Rysunek 1-28 Zatruty bufor ARP

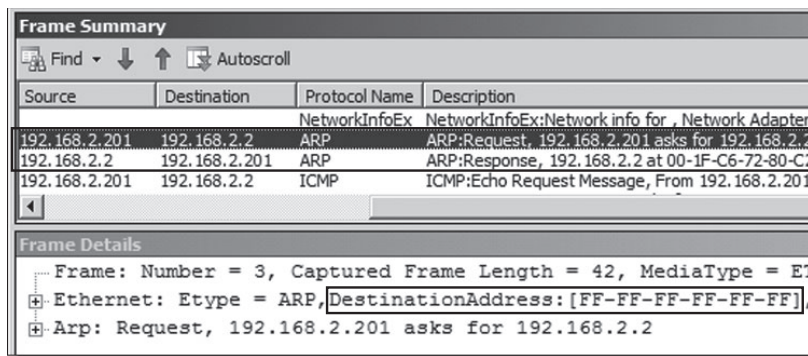
Uwaga IPv6 zapobiega zatruciu bufora Arp

IPv6 korzysta z protokołu Neighbor Discovery (ND) zamiast z protokołu ARP używanego w IPv4, aby rozpoznać mapowania adresów IP do MAC. Z tego powodu przyjemną zaletą sieci stosującej jedynie IPv6 jest to, że zapobiega ona możliwości zatrucia bufora Arp.

Rzut oka na ruch ARP

Komunikacja między dwoma komputerami w tej samej sieci odbywa się przy użyciu protokołu warstwy 2, takiego jak na przykład Ethernet. Jeśli pierwszy komputer zna tylko adres IP (warstwa 3) drugiego komputera lokalnego, to pierwszy komputer musi najpierw przetłumaczyć docelowy adres IP na adres warstwy 2 (sprzętowy), zanim skomunikuje się z drugim komputerem. Takiego tłumaczenia dokonuje protokół ARP.

Na rysunku 1-29 pokazany jest przechwycony ruch sieciowy dla wymiany ARP służącej do ustalenia adresu sprzętowego komputera 192.168.2.2.



Rysunek 1-29 Wymiana ARP składa się z rozgłaszanej prośby, po której następuje odpowiedź typu unicast.

Na wymianę ARP składają się dwa pakiety. Pierwszy pakiet to komunikat ARP Request z komputera 192.168.2.201. Chociaż miejsce docelowe komunikatu ARP Request jest pokazane jako 192.168.2.2 w okienku Frame Summary, to w okienku Frame Details widać, że adres docelowy ARP Request ma postać FF-FF-FF-FF-FF-FF. Ten ethernetowy adres jest adresem rozgłaszania, który gwarantuje odbiór komunikatu przez każdą kartę sieciową w sieci LAN. W drugim pakiecie wymiany ARP karta sieciowa o adresie IP 192.168.2.2 wysyła komunikat ARP Response z powrotem do komputera 192.168.2.201. Komunikat ten zawiera żadaną informację: 00-1F-C6-72-80-C2, czyli adres sprzętowy komputera 192.168.2.2. Po otrzymaniu tego adresu sprzętowego jest on zapisywany w lokalnym buforze ARP przez komputer, który wysłał komunikat ARP Request.

Zadanie Konfigurowanie adresów TCP/IP

W tym zadaniu skonfigurujemy statyczny adres IPv4 połączeń sieci lokalnych na komputerze Dcscr1, alternatywny adres dla lokalnego połączenia na komputerze Boston, i w końcu korzystając z wiersza polecenia określimy statyczny adres komputera Boston. Do tej pory te połączenia miały przypisane adresy APIPA. Po skonfigurowaniu tych adresów możemy włączyć udostępnianie plików na obu komputerach i przetestować łączność przy użyciu Ping.

W tym ćwiczeniu zakładamy, że dysponujemy laboratorium komputerowym skonfigurowanym zgodnie z opisem we wstępie do tej książki. Na Dcscr1 Local Area Connection musi być połączone z prywatną siecią laboratorium, a *Local Area Connection 2* musi być wyłączona. Na Boston Local Area Connection musi być połączone z tą samą prywatną siecią laboratorium. Żadne inne komputery ani serwery nie powinny występować w tej sieci prywatnej.

Żadne role serwera nie powinny być instalowane na żadnym komputerze.

► Ćwiczenie 1: Weryfikacja aktualnego adresu IP

W tym ćwiczeniu sprawdzamy bieżącą konfigurację IP na komputerze Dcscr1.

1. Zaloguj się na Dcscr1 jako administrator.
2. Otwórz wiersz polecenia, klikając Start, a następnie wybierając Command Prompt.
3. W wierszu polecenia wpisz **ipconfig**, a następnie wciśnij Enter. To polecenie służy do pokazania konfiguracji adresu IP.

Wyniki ukazują połączenia sieciowe. Pod „Ethernet adapter Local Area Connection” i obok Autoconfiguration IPv4 Address widać adres 169.254.y.z, gdzie y i z odpowiadają ID hosta aktualnie przypisanego do tego połączenia. Maską podsieci jest domyślna i wynosi 255.255.0.0. Ponieważ domyślna instalacja Windows Server 2008 R2 określa, że adres IP hosta jest przypisywany automatycznie, pod nieobecność serwera DHCP, host korzysta z adresu APIPA (zakładając, że żadna alternatywna konfiguracja nie została zdefiniowana). Zauważmy także, że temu samemu połączeniu został przypisany adres lokalny łącza IPv6 zaczynający się od fe80::.. Ten adres jest odpowiednikiem IPv6 adresu APIPA.

W końcu widać także połączenia lokalne dla karty tunelowej. Są one związane z IPv6 i będą dokładnie opisane w lekcji 3 „Adresowanie IPv6”.

► Ćwiczenie 2: Ręczne konfigurowanie adresu

W tym ćwiczeniu przypisujemy statyczny adres IP do Local Area Connection na Dcsrv1. Styczny adres IP jest potrzebny komputerom, na których będą później działać usługi infrastruktury sieciowej, takie jak DNS lub DHCP.

1. Będąc nadal zalogowanym na Dcsrv1 jako administrator, w wierszu polecenia wpisz **ncpa.cpl**.
2. Kliknij prawym przyciskiem myszy Local Area Connection w oknie Network Connections i wybierz Properties. To połączenie znajduje się w prywatnej sieci laboratorium.
3. Kliknij dwukrotnie Internet Protocol Version 4 (TCP/IPv4) w oknie dialogowym Local Area Connections Properties w obszarze This Connection Uses The Following Items.
4. Wybierz Use The Following IP Address na karcie General okna dialogowego Internet Protocol Version 4 (TCP/IPv4) Properties.
5. Wpisz **192.168.0.1** w polu tekstowym IP Address.
6. Wybierz pole tekstowe Subnet Mask umieszczając w nim kursor. W tym polu pojawi się maska podsieci 255.255.255.0. Kliknij OK.
7. W oknie dialogowym Local Area Connection Properties kliknij OK.
8. W wierszu polecenia wpisz **ipconfig**.
Zobaczymy nowy stały adres IPv4 związany z Local Area Connection.

► Ćwiczenie 3: Definiowanie konfiguracji alternatywnej

W tym ćwiczeniu zmienimy konfigurację IP na komputerze Boston, aby w razie braku serwera DHCP w prywatnej sieci laboratorium ten komputer miał zdefiniowany adres 192.168.0.200 dla Local Area Connection.

1. Zaloguj się na Boston jako administrator.
2. Kliknij View Network Connections w Server Manager.
3. Otwórz właściwości Local Area Connection w Network Connections.
4. Otwórz właściwości Internet Protocol Version 4 (TCP/IPv4) w oknie dialogowym Local Area Connection Properties.
Zauważmy, że na karcie General okna dialogowego Internet Protocol (TCP/IP) Properties są zaznaczone opcje dotyczące automatycznego uzyskiwania adresów – Obtain An IP Address Automatically oraz Obtain DNS Server Address Automatically.
5. Kliknij zakładkę karty Alternate Configuration.
Wybrana jest opcja Automatic Private IP Address (Automatyczny adres prywatny IP). Ponieważ żaden serwer DHCP nie jest dostępny, a to ustawienie jest włączone domyślnie, Boston ma do Local Area Connection automatycznie przypisany adres APIPA.
6. Wybierz User Configured (Ustawienia konfigurowane przez użytkownika).
7. Wpisz **192.168.0.200** w polu tekstowym IP Address.
8. Kliknij pole tekstowe Subnet Mask, aby umieścić w nim kursor. Wtedy w tym polu pojawi się domyślna maska podsieci 255.255.255.0. Pozostaw ten wpis.

9. Usuń zaznaczenie pola wyboru Validate Settings If Changed Upon Exit. W ten sposób skonfigurowaliśmy adres IP 192.168.0.200/24 komputera Boston. Możemy używać tej konfiguracji do czasu, gdy w naszej sieci skonfigurujemy serwer DHCP.

10. Kliknij OK.

11. Kliknij OK w oknie dialogowym Local Area Connection Properties.

12. Otwórz wiersz polecenia i wpisz **ipconfig /all**. W wynikach Ipconfig poszukaj wartości IPv4 Address. Znajdziesz tu nowy, alternatywny adres przypisany komputerowi Boston. Następnie poszukaj wartości Autoconfiguration Enabled (Autokonfiguracja włączona). Zwróć uwagę, że jest ustawiona na Yes (Tak).

► **Ćwiczenie 4: Konfigurowanie statycznego adresu IPv4 za pomocą polecenia tekstowego**

W kolejnym ćwiczeniu do konfiguracji na komputerze Boston statycznego adresu IPv4 192.168.0.2 i maski podsieci 255.255.255.0 użyjemy wiersza polecenia.

1. Będąc zalogowanym na komputerze Boston jako administrator, otwórz wiersz polecenia z podniesionymi uprawnieniami (ten krok nie jest konieczny, jeżeli jesteś zalogowany na konto o nazwie Administrator wiersz polecenia z podniesionymi uprawnieniami otwieramy klikając Start, potem klikając prawym przyciskiem myszy Command Prompt (Wiersz polecenia), a następnie wybierając Run As Administrator (Uruchom jako administrator)).

2. W wierszu polecenia wpisz, co następuje:

```
netsh interface ip set address "local area connection" static 192.168.0.2
255.255.255.0
```

3. W wierszu polecenia wpisz **ipconfig**.
Wyniki Ipconfig ukazują nowy adres IPv4.

► **Ćwiczenie 5: Włączanie udostępniania plików**

Włączenie udostępniania plików w systemie Windows Server 2008 R2 powoduje utworzenie wyjątku zapory dla protokołu ICMP, który pozwala komputerowi odpowiadać na polecenia Ping. Dlatego wykonamy teraz ten krok w Network and Sharing Center na obu komputerach Dcsrv1 i Boston.

1. Będąc zalogowany na Dcsrv1 jako administrator, otwórz Network and Sharing Center, klikając prawym przyciskiem myszy ikonę sieci w obszarze powiadomień i wybierając Network And Sharing Center (obszar powiadomień znajduje się po prawej stronie paska zadań).

2. W Network and Sharing Center kliknij Change Advanced Sharing Settings (Zmień zaawansowane ustawienia udostępniania).

3. W oknie Advanced Sharing Settings w obszarze aktualnego profilu kliknij Turn On File And Printer Sharing (Włącz udostępnianie plików i drukarek).

4. Kliknij przycisk Save Changes (Zapisz zmiany).

Proszę pamiętać, że ta metoda włączania wyjątku zapory dla ICMP jest zalecana tylko w sieciach testowych. W sieciach produkcyjnych lepiej jest włączać reguły zapory przy użyciu konsoli Windows Firewall With Advanced Security lub za pomocą zasad grupy.

5. Powtórz kroki 1 do 4 na komputerze Boston.

► Ćwiczenie 6: Sprawdzanie połączenia

W tym ćwiczeniu zweryfikujemy, że dwa komputery mogą się teraz komunikować przez prywatną sieć laboratorium.

1. Otwórz wiersz polecenia, będąc zalogowanym na komputerze Boston jako Administrator.
2. Wpisz ping **192.168.0.1** w wierszu polecenia.
Wynik potwierdza, że Dcsrv1 i Boston komunikują się przez IP.
3. Wyloguj się z obu komputerów.

Podsumowanie lekcji

- TCP/IP (Transmission Control Protocol/Internet Protocol) definiuje czterowarstwową architekturę, w tym warstwę interfejsu sieciowego (Network Interface), czyli łącza danych (Data Link), warstwę internetową (Internet), czyli siećową (Network), warstwę transportową (Transport) i warstwę aplikacji (Application). Z powodu ich położenia w modelu sieciowym OSI warstwy te są znane jako 2, 3, 4 i 7, odpowiednio.
- Network and Sharing Center to główne narzędzie konfiguracji sieci w Windows Server 2008 i Windows Server 2008 R2. Możemy korzystać z Network and Sharing Center do wykonania takich funkcji, jak określanie lokalizacji sieci, przeglądanie mapy sieci, konfigurowanie odnajdowania sieci oraz udostępniania plików i drukarek, bądź sprawdzanie stanu połączeń sieciowych.
- Korzystając z właściwości połączenia sieciowego możemy skonfigurować komputer z adresem statycznym lub automatycznie konfigurowanym. Automatycznie konfigurowane adresy są otrzymywane od serwera DHCP, jeżeli jest on dostępny.
- Gdy połączenie ma dostawać adres automatycznie, a żaden serwer DHCP nie jest dostępny, połączenie domyślne przypisuje sobie adres w formie 169.254.x.y. Możemy zdefiniować także alternatywną konfigurację, którą połączenie będzie sobie przypisywać pod nieobecność serwera DHCP.
- Pewne podstawowe narzędzia TCP/IP służą do testowania i rozwiązywania problemów z łącznością sieciową. Wśród tych narzędzi znajdują się Ipconfig, Ping, Tracert, PathPing i Arp.

Pytania do lekcji

Poniższe pytania mają posłużyć sprawdzeniu znajomości informacji zawartych w tej lekcji.

Uwaga Odpowiedzi

Odpowiedzi na te pytania i wyjaśnienia, dlaczego poszczególne opcje są poprawne lub błędne, znajdują się w części „Odpowiedzi” na końcu książki.

1. Użytkowniczka w organizacji narzeka, że nie może połączyć się z żadnymi zasobami sieciowymi. Po uruchomieniu polecenia *Ipconfig* na jej komputerze okazuje się, że adres przypisany do Local Area Connection to 169.254.232.21.
Które z następujących poleceń powinien najpierw wprowadzić administrator?
 - A. `Ipconfig /renew`
 - B. `ping 169.254.232.21`
 - C. `tracert 169.254.232.21`
 - D. `Arp -a`
2. Który z następujących typów adresów najlepiej pasuje do serwera DNS?
 - A. Adres przypisany przez DHCP
 - B. Adres APIPA
 - C. Adres konfiguracji alternatywnej
 - D. Adres określony ręcznie

Lekcja 2: Adresowanie IPv4

IPv4 jest do tej pory najpopularniejszym protokołem. Chociaż łączenie komputerów do ustanowionej sieci IPv4 jest proste (i często całkowicie automatyczne), aby implementować i konfigurować te sieci oraz rozwiązywać problemy związane z IPv4, musimy rozumieć podstawowe pojęcia adresowania IPv4.

Po ukończeniu tej lekcji Czytelnik będzie umiał:

- Opisać strukturę adresu IPv4, w tym ID sieci i ID hosta.
- Opisać funkcję maski podsieci.
- Konwertować maskę podsieci pomiędzy notacją dziesiętną z kropkami a notacją z ukośnikiem.
- Konwertować 8-bitową wartość pomiędzy notacjami binarną a dziesiętną.
- Opisać funkcję bramy domyślnej w routingu IP.
- Opisać i rozpoznawać zakresy adresów prywatnych IPv4.
- Opisać pojęcie bloków adresów.
- Wyznaczyć liczbę adresów w danym bloku adresów.
- Wyznaczyć rozmiar bloku adresów potrzebny dla danego numeru adresów.
- Opisać zalety dzielenia na podsieci.
- Ustalić liczbę podsieci na podstawie potrzeb sieciowych i zadanej przestrzeni adresów.
- Ustalić, czy dwa adresy są skonfigurowane w tej samej podsieci.

Przewidywany czas trwania lekcji: 180 minut

Struktura adresów IPv4

Adresy IPv4 mają długość 32 bitów i składają się z 4 *oktetów* o długości 8 bitów każdy. Przyjętą reprezentacją adresu IPv4 jest notacja *dziesiętna z kropkami*, w której każdy z czterech numerów reprezentuje oktet oddzielony od innych kropką – na przykład 192.168.23.245. Jednak ta notacja dziesiętna z kropkami jest powszechnie stosowana tylko dla ludzkiej wygody. Komputery rzeczywiście czytają adresy IPv4 w ich natywnej 32-bitowej notacji binarnej, takiej jak

```
11000000 10101000 00010111 11110101
```

Jest to ważne, jeżeli chcemy zrozumieć, jak działa IPv4.

IPv4 to system adresowania – system umożliwiający *znajdowanie* urządzeń – a nie jedynie system identyfikacyjny. Każdy adres IPv4 w sieci musi być jednoznaczny. Adres nie może być przypisany do urządzenia sieciowego losowo, ponieważ nie pozwalałoby to odnajdywać urządzeń. IPv4 zapewnia jednoznaczność adresów i możliwość wyszukiwania poprzez podział adresów na dwie części: *ID sieci* i *ID hosta*.

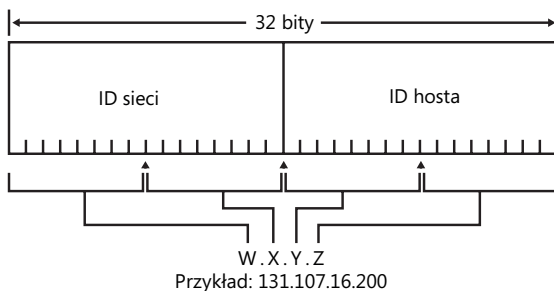
ID sieci i ID hosta

Pierwszą częścią adresu IPv4 jest *ID sieci*. Rolą ID sieci jest identyfikacja konkretnej sieci w większej złożonej sieci IPv4 (takiej jak Internet). Pozostała część adresu IPv4 to *ID hosta*. ID hosta identyfikuje host IPv4 (komputer, router lub inne urządzenie IPv4) wewnątrz sieci zidentyfikowanej przez ID sieci.

Uwaga ID sieci + ID hosta = 32 bity

Jeżeli n = liczba bitów w ID sieci, a h = liczba bitów w ID hosta, to $n + h$ jest równe 32.

Rysunek 1-30 ukazuje przykładowy widok adresu IPv4 (131.107.16.200) podzielonego na sekcje ID sieci i ID hosta. Litery w, x, y i z często służą do wyznaczania czterech oktetów w adresie IPv4. W tym przykładzie część ID sieci (131.107) jest określona przez oktety w i x. Część ID hosta (16.200) jest określona przez oktety y i z.



Rysunek 1-30 ID sieci i ID hosta

Porównanie adresów IPv4 i ZIP+4 System dzielenia adresu IPv4 na ID sieci i ID hosta przypomina system „ZIP+4” stosowany w większości urzędów pocztowych w systemie pocztowym USA. Ten system służy do kierowania i dostarczania poczty do poszczególnych skrzynek urzędów pocztowych w kraju.

Uwaga ZIP+4

Dla celów naszej analogii zakładamy, że cyfry +4 zawsze reprezentują indywidualne skrzynki urzędów pocztowych.

Razem wzięte 5-cyfrowy kod ZIP (znany także jako kod pocztowy) i 4-cyfrowy numer skrzynki reprezentują unikalny 9-cyfrowy adres ZIP+4 podobny w strukturze i funkcji do 32-bitowego adresu IPv4. Pierwsza część adresu ZIP+4 – pięciocyfrowy kod – reprezentuje wyszukany obszar, a nie konkretny adres. Druga część reprezentuje określoną 4-cyfrową skrzynkę pocztową wewnątrz 5-cyfrowego obszaru kodu ZIP – skrzynkę pocztową, do której urząd pocztowy reprezentowany przez kod ZIP dostarcza korespondencję.

Jednak adresy ZIP+4 są znacznie prostsze od adresów IPv4 pod jednym względem. Gdy przyglądamy się adresowi ZIP+4, wiadomo, która konkretna część adresu reprezentuje urząd pocztowy (kod ZIP), a która reprezentuje indywidualną skrzynkę (+4). Linia dzieląca pomiędzy nimi nigdy się nie zmienia. Pierwsze cztery cyfry i ostatnie pięć cyfr zawsze mają tę samą funkcję.

Trik w adresach IPv4 polega na tym, że rozmiar ID sieci i rozmiar ID hosta jest zmienny. Patrząc na sam adres IPv4, taki jak 192.168.23.245, nie potrafimy określić, które z 32 bitów określają ID sieci, a które ID hosta. Potrzebna jest dodatkowa informacja. Tą informacją jest maska podsieci.

**Z praktyki**

J.C. Mackin

W tej lekcji opisana jest ręczna metoda wyliczania sposobu adresowania IP. Taka technika pomaga lepiej zrozumieć to adresowanie i jest najbardziej przydatna pod kątem egzaminu. W praktyce do wykonywania tego typu obliczeń – ustalania masek podsieci, rozmiarów bloków, zakresów podsieci – można wykorzystywać odpowiednie oprogramowanie. Aby łatwo znaleźć tego typu narzędzia, najlepiej jest wpisać hasło typu „kalkulator podsieci” lub „kalkulator VLSM”.

Maski podsieci

Maska podsieci decyduje, która część 32-bitowego adresu IPv4 ma być uważana za ID sieci. Na przykład, gdy napiszemy 192.168.23.245/24, to /24 reprezentujące maskę podsieci informuje, że ID sieci jest zdefiniowane przez pierwsze 24 z 32 bitów w adresie IPv4. W adresie IPv4 131.107.16.200, pokazanym wcześniej na rysunku 1-29, ID sieci jest określone przez pierwszych 16 bitów. Dlatego odpowiednią maską do zastosowania na hoście, któremu przydzielono ten adres, jest /16.

Te dwie wymienione przed chwilą maski podsieci – /16 i /24 – są względnie łatwe do interpretacji. Ponieważ ich wartości są podzielne przez 8, te maski podsieci informują, że ID sieci składa się odpowiednio z pierwszych dwóch pełnych oktetów i pierwszych trzech pełnych oktetów adresu IPv4. Innymi słowy, ID sieci hosta przypisanego do adresu 131.107.16.200 /16 jest 131.107, a adres sieci hosta wynosi dlatego 131.107.0.0. ID sieci

hosta z przypisanym adresem 192.168.23.245/24 to 192.168.23, a adres sieci hosta wynosi 192.168.23.0. Jednak maski podsieci nie zawsze są podzielne przez 8 i nie zawsze tak łatwe do interpretacji, co wkrótce zobaczymy.

Notacje maski podsieci Do tej pory koncentrowaliśmy się na maskach podsieci w notacji z ukośnikiem – znanej także jako notacja CIDR (Classless Inter Domain Routing) lub notacja prefiksu sieci. Notacja z ukośnikiem jest częstym sposobem definiowania masek podsieci zarówno na egzaminie 70-642, jak i w świecie rzeczywistym. Natomiast równie często maski podsieci są przedstawiane w 32-bitowej notacji dziesiętnej z kropkami.

W notacji dziesiętnej z kropkami maska podsieci przyjmuje formę podobną do 32-bitowego adresu IPv4. Na przykład maska podsieci /16 jest przedstawiana w tej notacji jako 255.255.0.0, a maska podsieci /24 jako 255.255.255.0.

Aby zrozumieć związek maski podsieci wyrażonej w notacji z ukośnikiem z jej odpowiednikiem dziesiętnym z kropkami, musimy najpierw przetłumaczyć notację z ukośnikiem na binarną. Na początek weźmy wartość po ukośniku w notacji z ukośnikiem – na przykład 16 w /16 – i przedstawmy ją jako odpowiednią liczbę jedynek w notacji binarnej ze spacją po każdym 8 bitach – czyli oktetcie.

```
11111111 11111111
```

Następnie uzupełnijmy maskę podsieci w notacji binarnej do 32 bitów, dodając na końcu ciąg zer (ze spacją po każdym 8 bitach):

```
11111111 11111111 00000000 00000000
```

W końcu konwertujemy tę notację binarną na dziesiętną z kropkami. Ponieważ 11111111 jest binarnym odpowiednikiem dziesiętnej liczby 255, a 00000000 jest binarnym odpowiednikiem dziesiętnej liczby 0, możemy reprezentować każdy oktet jako 255 lub 0. Z tego powodu /16 jest równoważne 255.255.0.0.

Ważne Co stało się z klasami adresów?

Czasami słyszymy, że adres /8 jest nazywany adresem *klasy A*, adres /16 należy do *klasy B*, a adres /24 do *klasy C*. Te terminy odnoszą się do starszego systemu routingu IPv4 i nie są już stosowane, chociaż to słownictwo jest często używane nieformalnie. Te terminy nie pojawią się na egzaminie 70-642, ponieważ technicznie nie funkcjonują.

Konwertowanie pomiędzy notacją binarną a dziesiętną z kropkami

Rzadko zachodzi potrzeba konwersji między systemem dwójkowym (binarnym) i dziesiętnym i w takiej sytuacji można użyć kalkulatora. Jeśli jednak nie mamy pod ręką kalkulatora, dobrze jest wiedzieć, jak zrobić to ręcznie. Opis tej procedury pomoże również zrozumieć logikę adresowania IP.

Kluczem do zrozumienia notacji dwójkowej jest znajomość wartości bitu na każdej pozycji. Tak jak w systemie dziesiętnym, w którym poszczególne miejsca wyznaczają inne zakresy wielkości – jedynki, dziesiątki, setki itd. – wartości poszczególnych bitów rosną od prawej do lewej. W tabeli 1-1 pokazany jest zapis naukowy i dziesiętny wartości skojarzonych z kolejnymi miejscami oktetu binarnego. Zauważmy, że idąc od prawej do lewej każdy kolejny bit reprezentuje dwa razy większą wartość od poprzedniego. Daje to maksymalną wartość 128 ostatniego bitu po lewej. Znajomość tego wzoru pozwala łatwo wyznaczyć wartość bitu na każdym miejscu.

Tabela 1-1 Potencjalne wartości bitów w okcie binarnym

pozycja bitu	1. bit	2. bit	3. bit	4. bit	5. bit	6. bit	7. bit	8. bit
zapis naukowy	27	26	25	24	23	22	21	20
zapis dziesiętny	128	64	32	16	8	4	2	1

Pamiętajmy, że wartości podane dla poszczególnych pozycji obowiązują tylko wtedy, gdy dany bit jest ustawiony na 1. Gdy oktet zawiera na jakiejś pozycji 0, to wartość dla tej pozycji jest pusta. Na przykład, gdy bit na pierwszej pozycji (od lewej) ma wartość 1, to reprezentuje liczbę dziesiętną 128. Tam, gdzie bit jest ustawiony na 0, reprezentuje wartość dziesiętną równą 0. Gdy wszystkie bity oktetu są ustawione na 1, to oktet ma wartość dziesiętną 255. Gdy na wszystkich pozycjach oktetu występują 0, to jego wartość dziesiętna również wynosi 0.

Przykład konwersji z systemu binarnego na dziesiętny

Podany niżej ciąg zer i jedynek reprezentuje oktet, który może wystąpić w adresie IPv4:P

10000011

Aby ustalić dziesiętny odpowiednik tego oktetu, można użyć prostej tabeli konwersji, takiej jak zamieszczona poniżej, i wpisać do niej kolejne bity oktetu.

128	64	32	16	8	4	2	1
1	0	0	0	0	0	1	1

Dodając za pomocą tej tabeli wartości dziesiętne odpowiadające pozycjom kolejnych bitów można obliczyć sumę dziesiętną całego oktetu:

$$128 + 2 + 1 = 131$$

Oznacza to, że oktet o wartości binarnej 10000011 ma wartość dziesiętną równą 131.

Przykład konwersji z systemu dziesiętnego na binarny

Aby dokonać konwersji wartości dziesiętnej na oktet binarny, trzeba narysować tabelę konwersji i ustawić 1 w kolejnych bitach oktetu (od lewej do prawej), aż do uzyskania żądanej wartości dziesiętnej. Jeśli ustawienie 1 na kolejnej pozycji oktetu powoduje przekroczenie żądanej wartości dziesiętnej, należy ustawić 0 i przejść do następnej pozycji. Istnieje zawsze tylko jedna kombinacja zer i jedynek, która daje docelową wartość dziesiętną.

Przypuśćmy, że chcemy zamienić na oktet binarny wartość 209. Najpierw rysujemy na kartce pokazaną niżej tabelę konwersji:

128	64	32	16	8	4	2	1

Następnie ustalamy wartość pierwszego bitu (od lewej). Czy liczba 128 jest mniejsza od 209? Ponieważ jest mniejsza, zapisujemy 1 poniżej 128 i następnie zapisujemy 128 z boku kartki, aby liczyć sumę częściową.

128	64	32	16	8	4	2	1	Suma częściowa
1								128

Przechodzimy teraz do następnej pozycji oktetu. Czy suma $128 + 64$ jest mniejsza od 209? Ponieważ suma ta wynosi tylko 192, ponownie wpisujemy 1 poniżej 64 i dopisujemy 64 w kolumnie sumy częściowej.

128	64	32	16	8	4	2	1	Suma częściowa
1	1							128 +64 =192

Wartość dziesiętna następnej pozycji to 32, ale jeśli postawimy tu 1, to otrzymamy sumę częściową 224, przekraczającą naszą wartość docelową 209. Należy więc wpisać 0 i nie dodawać niczego do sumy częściowej.

128	64	32	16	8	4	2	1	Suma częściowa
1	1	0						128 +64 =192

Wartość dziesiętna następnej pozycji to 16 i dodanie tej wartości do 192 daje liczbę 208. Czy liczba 208 jest mniejsza od 209? Ponieważ jest mniejsza, należy wpisać 1 poniżej 16 i dodać 16 do sumy częściowej.

128	64	32	16	8	4	2	1	Suma częściowa
1	1	0	1					128 64 +16 =208

Ponieważ brakuje już tylko liczby 1 do uzyskania docelowej wartości, wystarczy wpisać 1 na ostatniej pozycji oktetu i na tym zakończyć konwersję.

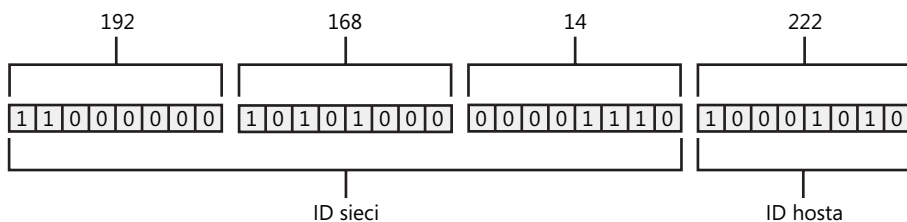
128	64	32	16	8	4	2	1	Suma częściowa
1	1	0	1	0	0	0	1	128 64 16 +1 =209

Tak więc oktet binarny reprezentujący liczbę dziesiętną 209 ma postać 11010001.

Pośrednie wartości maski podsieci Maski podsieci, jakim się przyglądaliśmy w notacji dziesiętnej z kropkami, składają się z oktetów, których wartości są reprezentowane jako 255 lub 0. Ogranicza to naszą dyskusję do tylko trzech możliwych masek podsieci: /8 (255.0.0.0), /16 (255.255.0.0) i /24 (255.255.255.0). Faktycznie są to najbardziej typowe maski podsieci stosowane w Internecie (szczególnie /24 czyli 255.255.255.0).

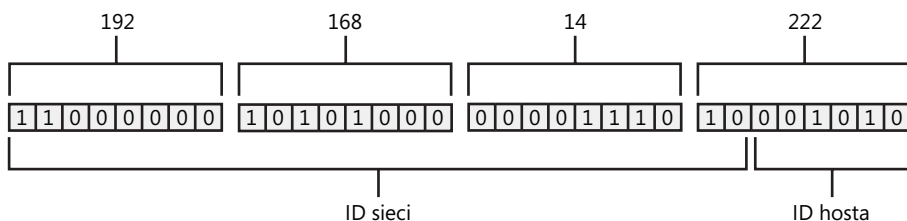
Jednak zarówno na egzaminie 70-642, jak i w świecie rzeczywistym napotkamy także maski podsieci, takie jak /25 lub /22, które wyrażone w notacji dziesiętnej z kropkami obejmują pośrednie wartości oktetów, takie jak 128 czy 252. Ta sytuacja występuje zawsze, gdy długość ID sieci (wyrażana w bitach) nie jest podzielna przez 8.

Na przykład rysunek 1-31 pokazuje binarną reprezentację adresu IPv4 192.168.14.222 z maską podsieci /24 czyli 255.255.255.0. W tym adresie ID sieci jest reprezentowane przez pierwsze 24 bity (pierwsze trzy oktety), a ID hosta jest reprezentowane przez ostatnie 8 bitów (ostatni oktet).



Rysunek 1-31 Adres IPv4 z maską podsieci /24

Teraz rozważmy ten sam adres IPv4 z 26-bitową maską podsieci, widoczną na rysunku 1-32. W tym przykładzie ID sieci korzysta z dwóch pierwszych bitów z ostatniego oktetu. Ostatni oktet jest więc częściowo dedykowany ID sieci, a częściowo ID hosta. Binarnie ID sieci jest po prostu 26-bitową liczbą, podczas gdy ID hosta jest liczbą 6-bitową.



Rysunek 1-32 Ten sam adres IPv4 z maską podsieci /26

Tabela 1-2 porównuje notacje z ukośnikiem, binarną i dziesiętną z kropkami wszystkich masek podsieci od /8 do /30. Są to jedyne maski podsieci, jakie możemy zobaczyć. Natomiast maski podsieci, jakie napotyka się najczęściej (zarówno na egzaminie 70-642, jak i w świecie rzeczywistym) są z zakresu /20 to /30.

Ważne Przestudiujmy tę tabelę

Ta tabela przedstawia informacje, które większość administratorów sieci musi rozumieć. Upewnijmy się, że spędziliśmy wystarczająco dużo czasu, przeglądając tę tabelę, aby mieć komfort znajomości wartości masek podsieci i tego, jak te trzy notacje odnoszą się do siebie nawzajem.

Tabela 1-2 Porównanie notacji masek podsieci

Notacja z ukośnikiem	Notacja binarna	Notacja dziesiętna z kropkami
/8	11111111 00000000 00000000 00000000	255.0.0.0
/9	11111111 10000000 00000000 00000000	255.128.0.0
/10	11111111 11000000 00000000 00000000	255.192.0.0
/11	11111111 11100000 00000000 00000000	255.224.0.0
/12	11111111 11110000 00000000 00000000	255.240.0.0
/13	11111111 11111000 00000000 00000000	255.248.0.0
/14	11111111 11111100 00000000 00000000	255.252.0.0
/15	11111111 11111110 00000000 00000000	255.254.0.0
/16	11111111 11111111 00000000 00000000	255.255.0.0

Tabela 1-2 Porównanie notacji masek podsieci

Notacja z ukośnikiem	Notacja binarna	Notacja dziesiętna z kropkami
/17	11111111 11111111 10000000 00000000	255.255.128.0
/18	11111111 11111111 11000000 00000000	255.255.192.0
/19	11111111 11111111 11100000 00000000	255.255.224.0
/20	11111111 11111111 11110000 00000000	255.255.240.0
/21	11111111 11111111 11111000 00000000	255.255.248.0
/22	11111111 11111111 11111100 00000000	255.255.252.0
/23	11111111 11111111 11111110 00000000	255.255.254.0
/24	11111111 11111111 11111111 00000000	255.255.255.0
/25	11111111 11111111 11111111 10000000	255.255.255.128
/26	11111111 11111111 11111111 11000000	255.255.255.192
/27	11111111 11111111 11111111 11100000	255.255.255.224
/28	11111111 11111111 11111111 11110000	255.255.255.240
/29	11111111 11111111 11111111 11111000	255.255.255.248
/30	11111111 11111111 11111111 11111100	255.255.255.252

Wartości oktetów masek podsieci Znajomość sekwencji dziewięciu możliwych wartości oktetu, które mogą wystąpić w masce, jest pomocna przy ustalaniu rozmiaru istniejących lub planowanych sieci. Na ogół od administratora sieci oczekuje się wręcz zdolności wykonywania tych obliczeń w głowie (metodę opisano dalej w tej lekcji w części zatytułowanej „Wyznaczanie maksymalnej ilości hostów w bloku”).

W zapamiętaniu tego wszystkiego może pomóc tabela 1-3. Zaczniemy od zakrycia górnego wiersza tabeli. Gdy będziemy potrafili bez wahania recytować dziesiętne wartości związane z dowolną ilością bitów o wartości 1 lub wartością binarną wybraną losowo z dolnych dwóch wierszy, przejdźmy do zakrycia dwóch dolnych wierszy. Gdy będziemy mogli już bez wahania wyrecytować ilość jedynek związanych z dziesiętną wartością wybraną losowo z górnego wiersza, przejdźmy do zapamiętania sekwencji dziesiętnych wartości od lewa do prawa i od prawa do lewa.

Powinniśmy znać te sekwencje od początku i od końca tak dobrze, żebyśmy mogli spojrzeć na liczbę, taką jak 192, i byśmy wiedzieli, że przechodząc od lewej strony do prawej ta wartość jest druga po 0 i dlatego 2 bity są przesunięte w prawo z wartości oktetu 0. W ten sam sposób będziemy w stanie spojrzeć na 248 i wiedzieć, że gdy przenosimy się od prawej do lewej, są to trzy miejsca przed 255 i dlatego trzy bity są przesunięte z lewej od 255.

Tabela 1-3 Wartości oktetów masek podsieci

Wartość dziesiętna	0	128	192	224	240	248	252	254	255
Liczba bitów	0	1	2	3	4	5	6	7	8
Wartość	0000	1000	1100	1110	1111	1111	1111	1111	1111
binarna	0000	0000	0000	0000	0000	1000	1100	1110	1111

Konwertowanie masek podsieci pomiędzy notacją ukośnikową a dziesiętną

Jeśli nie ma dostępu do odpowiedniego oprogramowania, to do konwersji zapisu maski podsieci należy używać odpowiedniej tabelki lub robić to w pamięci. Kogoś może jednak zainteresować, jak to robić bez tabelki, zapamiętywania wartości pośrednich i posługiwania się systemem binarnym. Taka metoda wymaga pewnej wprawy i nie powinna być używana podczas egzaminu 70-642.

Aby dokonać konwersji maski podsieci z notacji /n na zapis dziesiętny z kropkami, należy wykonać następujące działania:

1. Zapisać oktet 255 tyle razy, ile 8 mieści się w n.

Na przykład, dla sieci /19, będzie to dwa razy (8 mieści się dwa razy w 19). Tak więc należy zapisać „255.255.”.

2. Odjąć resztę z poprzedniego działania od 8, podnieść 2 do potęgi równej tej różnicy, a następnie odjąć tę nową wartość od 256. Działanie to można wyrazić matematycznie jako $256 - 2^{[8 - (n \bmod 8)]}$, gdzie n oznacza naszą wartość /n, a mod jest operatorem działania dającego resztę z dzielenia liczby poprzedzającej ten operator przez liczbę stojącą za tym operatorem. Wynik tej operacji należy umieścić w następnym okciecie. Jeśli pozostaną jeszcze jakieś oktety, należy ustawić ich wartość na 0.

Kontynuując ostatni przykład $256 - 2^{[8 - (19 \bmod 8)]} = 256 - 2^{[8 - 3]} = 256 - 2^5 = 256 - 32 = 224$. Tak więc należy zapisać „224” jako trzeci oktet i „0” jako czwarty. W efekcie sieć /19 ma maskę podsieci 255.255.224.0

Aby dokonać konwersji maski podsieci w zapisie dziesiętnym na maskę podsieci wyrażoną jako /n, należy wykonać następujące działania:

1. Mnożymy 8 przez liczbę oktetów w masce podsieci, które są ustawione na 255. Jeśli wszystkie pozostałe oktety są ustawione na 0, to stawiamy ukośnik przed wynikiem mnożenia i to koniec. W przeciwnym razie zachowujemy tę wartość jako sumę pośrednią i przechodzimy do następnego kroku.

Na przykład maska 255.255.255.192 zawiera trzy oktety 255. $8 * 3 = 24$.

Ponieważ czwarty oktet jest różny od 0, zachowujemy 24 jako sumę pośrednią.

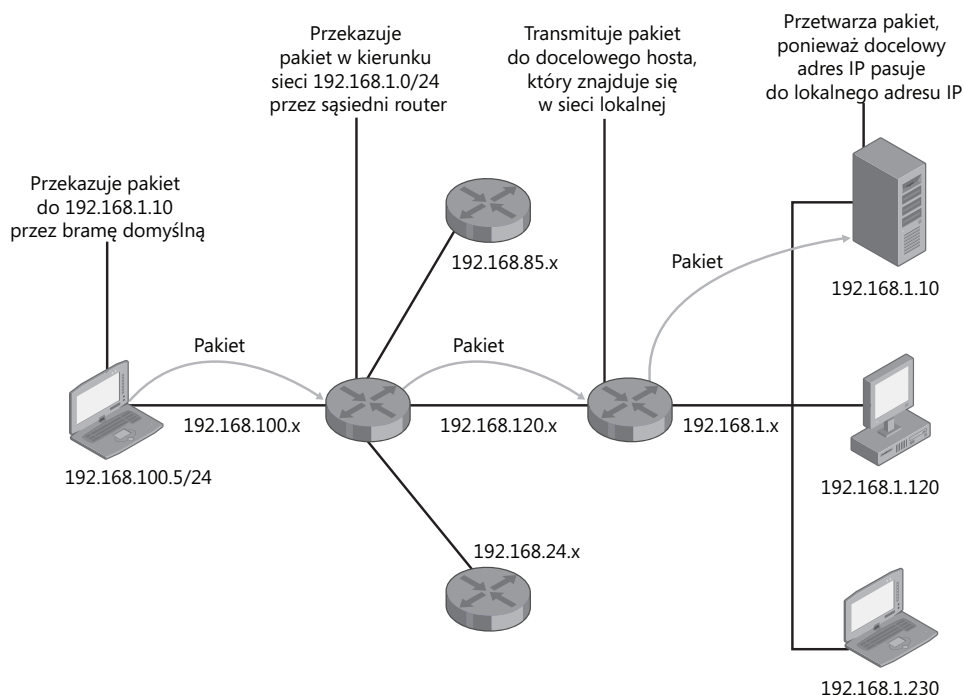
2. W przypadku oktetu o wartości między 0 i 255 odejmujemy tę wartość od 256, konwertujemy wynik na wyrażenie 2 do potęgi i na koniec odejmujemy wykładnik od liczby 8. Operację tę można wyrazić matematycznie jako $8 - \log_2(256 - y)$, gdzie y jest wartością oktetu, a $\log_2$ jest logarytmem dwójkowym, czyli potęgą dwójki, która daje następny składnik wyrażenia. Wynik tej operacji dodajemy do sumy pośredniej z kroku 1. Po dopisaniu na początku ukośnika otrzymujemy maskę w notacji /n.

Kontynuując poprzedni przykład z wartością 192 mamy: $8 - \log_2(256 - 192) = 8 - \log_2(64) = 8 - 6 = 2$. Dodajemy 24 z poprzedniego kroku do 2 i otrzymujemy rezultat końcowy /26. Tak więc odpowiednikiem maski podsieci 255.255.255.192 jest /26.

Działanie routingu i bram domyślnych

Ustalanie ID sieci przy użyciu maski podsieci jest ważnym krokiem w komunikacji IPv4, ponieważ ID sieci istotnie mówi komputerowi, jak ma obsłużyć pakiet IPv4. Gdy komputer w sieci ma wysłać pakiet do zdanego adresu, komputer porównuje najpierw własne ID sieci z tym ID, które jest określone w pakiecie IPv4 (do wyznaczenia tych ID sieci, komputer zawsze korzysta z lokalnie skonfigurowanej maski podsieci). Jeżeli te dwa ID sieci są identyczne, komunikat jest rozpoznawany jako lokalny i wysyłany do komputera w sieci lokalnej. Jeżeli te dwa ID sieci nie pasują do siebie, komputer wysyła pakiet do lokalnego routera o adresie znanym jako adres bramy domyślnej. Router znajdujący się pod adresem bramy domyślnej przekazuje następnie datagram IPv4 w sposób wyznaczony przez jego tabele routingu.

Rysunek 1-33 ilustruje ten proces routingu IP. Na rysunku komputer, którego adres wynosi 192.168.100.5/24, ma wysłać pakiet IP przeznaczony dla adresu 192.168.1.10. Ponieważ identyfikatory sieci tych dwóch adresów nie pasują do siebie, komputer wysyła pakiet do routera wskazanego przez adres bramy domyślnej. Ten router sprawdza swoje tabele routingu i wysyła pakiet do routera połączanego bezpośrednio z siecią 192.168.1.0. Ostatni router wysyła pakiet wprost do komputera z adresem 192.168.1.10, czyli do komputera, który odpowiedział na rozgłoszone w sieci lokalnej pytanie o ten adres, zgodnie z protokołem ARP opisanym wcześniej w tym rozdziale.



Rysunek 1-33 Routing pakietu IP przez złożoną sieć

Zapamiętajmy następujące ważne punkty dotyczące routingu i bram domyślnych:

- Brama domyślna musi mieć ten sam identyfikator sieci i znajdować się w tej samej domenie rozgłoszeniowej co wysyłający host.
- Jeżeli host nie ma skonfigurowanego ustawienia bramy domyślnej, nie będzie w stanie łączyć się ani z Internetem, ani z żadnymi komputerami poza zakresem rozgłoszeniowym. Na przykład prywatny wewnętrzny serwer, który czasami ma pobrać dane z Internetu, musi mieć zdefiniowaną bramę domyślną.
- Pozostawienie ustawienia bramy domyślnej nieskonfigurowanego na hoście zapobiega dostępowi do tego hosta ze wszystkich punktów poza lokalną podsiecią. Dlatego w pewnych sytuacjach możemy faktycznie zechcieć pozostawić nieskonfigurowane ustawienie bramy domyślnej z powodów bezpieczeństwa.

Zakresy adresów IPv4

Zdecydowana większość adresów IPv4 są to adresy pojedynczej emisji (typ unicast), co oznacza, że każdy z nich jest przypisany w danym momencie tylko do jednego hosta. Adresy IPv4 typu unicast możemy podzielić na trzy kategorie: zakresy publiczne, zakresy prywatne i zakresy APIPA (wprowadzone w lekcji 1). Podczas gdy adresy APIPA służą tylko jako adresy tymczasowe lub dla izolowanych komputerów, zakresy publiczny i prywatny są podzielone na bloki, które mogą być przypisywane całym sieciom. Te publiczne i prywatne zakresy, wraz z pojęciem bloków adresów omówiono w kolejnych częściach tej lekcji.

Korzystanie z publicznych adresów IPv4

W publicznym Internecie każdy adres IPv4 jest niepowtarzalny. Organizacja IANA (Internet Assigned Numbers Authority) podzieliła niezarezerwowaną przestrzeń adresów IPv4 i delegowała odpowiedzialność za przydział adresów do pewnej liczby regionalnych rejestrów na świecie, aby umożliwić sieciom uzyskiwanie niepowtarzalnych adresów internetowych. Te rejestry obejmują APNIC (Asia-Pacific Network Information Center), ARI (American Registry for Internet Numbers) i RIPE NCC (Réseaux IP Européens). Następnie te regionalne rejestry przydzielają *bloki* adresów niewielkiej liczbie większych dostawców usług internetowych (ISP), którzy z kolei przyznają mniejsze bloki swoim klientom i mniejszym ISP, którzy następnie dostarczają adresy publiczne do organizacji płacących za usługi internetowe. Wewnątrz tych organizacji adresy publiczne są zwykle zarezerwowane dla routerów i serwerów widocznych z Internetu.

Korzystanie z prywatnych adresów IPv4

Organizacja IANA zarezerwowała także pewną liczbę adresów IPv4, które nigdy nie są używane w globalnym Internecie. Te prywatne adresy IPv4 służą hostom, które wymagają łączności IPv4, ale nie są widoczne w sieci publicznej. Na przykład nie należy pozyskiwać publicznych adresów IPv4 do użytku wewnątrz sieci prywatnych, takich jak sieć domowa czy prywatna sieć firmowa. W sieciach prywatnych należy przydzielać hostom adresy z zakresów podanych w tabeli 1-4.

Tabela 1-4 Prywatne zakresy adresów

Adres początkowy	Adres końcowy
10.0.0.0	10.255.255.254
172.16.0.0	172.31.255.254
192.168.0.0	192.168.255.254

Hosty adresowane prywatnymi adresami IPv4 łączą się z Internetem przez serwer lub router dokonujący translacji adresów (Network Address Translation – NAT). Router pełniący rolę NAT może być komputerem Windows Server 2008 R2 lub urządzeniem dedykowanym do routingu.

Bloki adresów i podsieci

Większość organizacji korzysta z kombinacji adresów publicznych i prywatnych. Adresy publiczne są zwykle zarezerwowane dla routerów i serwerów widocznych z Internetu, takich jak serwery poczty czy sieci Web, które wymagają dostępu z zewnątrz. Sieci wewnętrzne składające się z wewnętrznych routerów, serwerów i klientów powinny korzystać z prywatnych zakresów adresów. Ważne jest to, że każda organizacja, która chce się komunikować z Internetem, musi mieć przynajmniej jeden adres publiczny. Ten jeden adres publiczny może służyć wielu klientom znajdującym się za urządzeniem NAT.

Publiczne adresy IPv4 są pobierane od dostawcy Internetu (w skrócie ISP) dla każdego komputera bezpośrednio podłączonego do Internetu. Chociaż małej organizacji może wystarczyć tylko jeden publiczny adres IPv4, wiele organizacji potrzebuje ich znacznie więcej. Organizacje potrzebujące więcej niż jeden publiczny adres kupują zwykle adresy od swojego ISP w postaci bloków.

Blok adresów to pełna grupa kolejnych adresów IP, które współdzielą pojedynczy identyfikator sieci. Na przykład organizacja może otrzymać od ISP blok adresów /24 z identyfikatorem sieci 206.73.118. Zakresem adresów związanych z tym blokiem byłoby wtedy 206.73.118.0 – 206.73.118.255.

Uwaga Co to jest przestrzeń adresowa?

Zakres adresów związanych z danym blokiem jest nazywany *przestrzenią adresową* bloku.

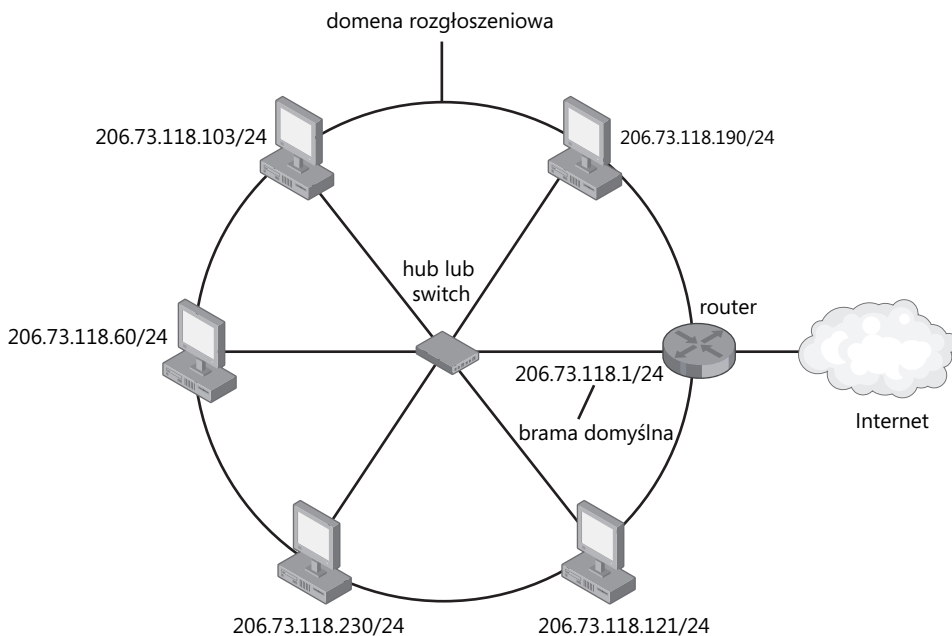
Istotne jest zrozumienie, że adresy w bloku adresów tworzą jedną sieć i dopóki ta sieć nie jest podzielona na podsieci – możliwość, którą rozważymy dalej w tej lekcji – taki blok adresów będzie stanowił *jedną domeną rozgłoszeniową* z pojedynczym routerem, czyli drogą wyjścia z sieci. *Brama domyślna* to adres w tej samej domenie rozgłoszeniowej przypisany do tego routera.

Inaczej mówiąc, blok adresów domyślnie jest przeznaczony do obsługi pojedynczej *podsieci*. Podsieć to grupa hostów w pojedynczej domenie rozgłoszeniowej, które współdzielą ten sam identyfikator sieci i ten sam adres bramy domyślnej.

Rysunek 1-34 przedstawia sieć obsługiwaną przez blok adresów 206.73.118.0/24.

Uwaga Jaka jest różnica pomiędzy siecią a podsiecią?

Terminy sieć i podsieć są często stosowane wymiennie. Różnica pomiędzy nimi jest taka, że podsieć zawsze wskazuje pojedynczą domenę rozgłoszeniową, która jest niepodzielona. Natomiast termin sieć może dotyczyć pojedynczej podsieci lub grupy połączonych podsieci.



Rysunek 1-34 Sieć z jedną podsiecią

Tworzenie tabeli odniesienia dla bloku adresów IPv4

Gdy trzeba wykonać obliczenia związane z blokami adresów IPv4 i nie można skorzystać z pomocy programu narzędziowego, należy utworzyć tabelę odniesienia. Taka tabela pozwala szybko rozwiązywać problemy z adresowaniem i jest szczególnie przydatna – wręcz niezbędna – na egzaminie.

Wskazówka egzaminacyjna

Podczas egzaminu warto utworzyć tabelę odniesienia na jakiejś kartce do notowania jeszcze przed kliknięciem przycisku Start i rozpoczęciem testu. Dzięki temu łatwiej będzie potem wyznaczyć szybko prawidłowe wartości, nie tracąc czasu przeznaczonego na egzamin.

Najpierw obracamy kartkę, tak aby dłuższy bok był ustawiony poziomo i zaczynamy wypełniać tabelę odniesienia wpisując od prawej do lewej kolejne potęgi 2 aż do wartości 256. Należy zostawić dużo miejsca z lewej strony kartki, gdyż później trzeba będzie tam wpisać więcej wartości.

← 256	128	64	32	16	8	4	2	1
-------	-----	----	----	----	---	---	---	---

Następnie rysujemy linię poziomą nad tym wierszem liczb i kreskę pionową na lewo od liczby 256. Z lewej strony wiersza wpisujemy etykietę „Rozmiar blok”, jak to jest pokazane niżej:

Rozmiar bloku	256	128	64	32	16	8	4	2	1
------------------	-----	-----	----	----	----	---	---	---	---

Następnie nad wierszem z rozmiarami bloków wpisujemy od lewej do prawej kolejne wartości od /24 do /32. Po tej czynności tabela powinna wyglądać następująco:

	/24	/25	/26	/27	/28	/29	/30	/31	/32
Rozmiar bloku	256	128	64	32	16	8	4	2	1

Każda kolumna tej tabeli reprezentuje sieć o innym rozmiarze. Rozmiar bloku informuje o liczbie adresów dostępnych w danej sieci. Na przykład zgodnie z tabelą sieć /28 zapewnia 16 adresów.

Teraz rysujemy poziomą linię poniżej rozmiarów bloku. Odejmujemy każdą z tych wartości od 256 i zapisujemy wynik poniżej nowej linii (wynikiem tej operacji są te same wartości oktetów maski podsieci, co w tabeli 1-3. Jeśli ktoś zna te wartości na pamięć, to etap ten powinien mu zająć niewiele czasu). Nowemu wierszowi nadajemy etykietę „Maska”.

	/24	/25	/26	/27	/28	/29	/30	/31	/32
Rozmiar bloku	256	256	256	256	256	256	256	256	256
	<u>-256</u>	<u>-128</u>	<u>-64</u>	<u>-32</u>	<u>-16</u>	<u>-8</u>	<u>-4</u>	<u>-2</u>	<u>-1</u>
Maska	0	128	192	224	240	248	252	254	255

Wartości w wierszu Maska informują o ostatnim okciecie w masce podsieci każdej sieci. Dla wszystkich sieci na prawo od kreski pionowej pierwsze trzy oktety są to 255.255.255. Aby ustalić na przykład maskę podsieci dla sieci /29, należy wpisać 255.255.255 i jako ostatni oktet dodać wartość Maski podaną w tabeli dla sieci /29 (248). Tak więc pełna maska podsieci dla sieci /29 ma postać 255.255.255.248.

W tym momencie, w zależności od potrzeb, można wypełnić trzy lub cztery dodatkowe kolumny na lewo od kreski pionowej. Sieci na lewo od tej kreski są inne, ponieważ trzeci oktet maski podsieci ma w nich wartość mniejszą od 255.

W naszym przykładzie wpisujemy wartości dla czterech dodatkowych sieci. Na początek wpisujemy w górnym wierszu, na lewo od /24, wartości od /20 do /23.

	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
Rozmiar bloku					256	128	64	32	16	8	4	2	1
Maska					0	128	192	224	240	248	252	254	255

W wierszu Rozmiar bloku dopisujemy od prawej do lewej kolejne podwojone wartości. Tym razem należy jednak uwzględnić drugie wyrażenie w rozmiarze każdego

bloku – wielokrotność 256, jak to jest pokazane niżej. Oba te składniki będą używane do obliczania trzeciego oktetu adresu. Na przykład użyjemy ich do obliczania zakresów adresów przy dużych rozmiarach bloków i do wypełniania wartości Maski w następnym kroku.

	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
Rozmiar bloku	4096 256 x 16	2048 256 x 8	1024 256 x 4	512 256 x 2	256	128	64	32	16	8	4	2	1
Maska					0	128	192	224	240	248	252	254	255

Dla każdego czynnika w parze z liczbą 256 w wierszu Rozmiar bloku należy odjąć ten czynnik od 256. (Możemy sobie wyobrazić, że zastępujemy wszędzie znak mnożenia znakiem odejmowania). Innymi słowy wykonujemy działania 256-16, 256-8, 256-4 i 256-2, a następnie umieszczamy wyniki tych czterech działań w odpowiednich polach wiersza Maski.

Gotowa tabela odniesienia powinna wyglądać tak, jak na rysunku 1-35.

	/20	/21	/22	/23	/24	/25	/26	/27	/28	/29	/30	/31	/32
Rozmiar bloku	4096 256 x 16	2048 256 x 8	1024 256 x 4	512 256 x 2	256	128	64	32	16	8	4	2	1
Maska	240	248	252	254	0	128	192	224	240	248	252	254	255

Rysunek 1-35 Tabela odniesienia bloków adresów IPv4

Wskazówka egzaminacyjna

W przypadku ręcznego wykonywania obliczeń związanych z adresowaniem IP dobrze jest nauczyć się na pamięć kolejnych potęg dwójki do wartości 2^{12} . Jeśli ktoś nie zna tych wartości, powinien przed egzaminem utworzyć na kartce do notowania stosowną tabelę. Wszystkie te wartości są podane na zamieszczonej niżej liście. Taką tabelę można szybko i łatwo utworzyć, ponieważ każda kolejna wartość jest dwukrotnie większa od poprzedniej. Zauważmy też, że są to takie same wartości, jak kolejne rozmiary bloków, jeśli więc ktoś woli, może umieścić te wyrażenia u góry tabeli odniesienia.

$$2^1=2$$

$$2^2=4$$

$$2^3=8$$

$$2^4=16$$

$$2^5=32$$

$$2^6=64$$

$$2^7=128$$

$$2^8=256$$

$$2^9=512$$

$$2^{10}=1024$$

$$2^{11}=1038$$

$$2^{12}=4096$$