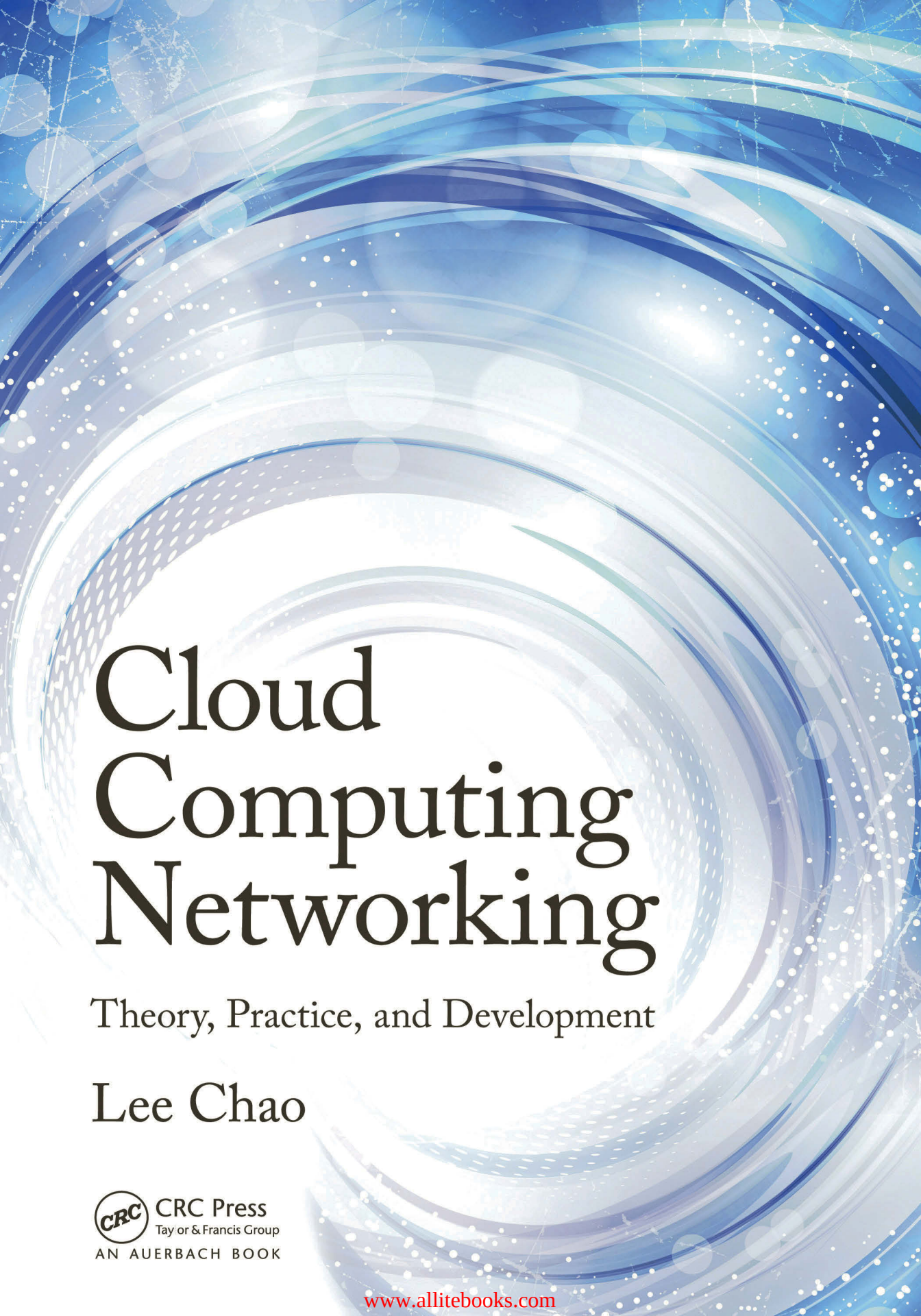

Cloud Computing Networking

Theory, Practice, and Development

Cloud Computing Networking

Theory, Practice, and Development

Lee Chao

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Version Date: 20150724

International Standard Book Number-13: 978-1-4822-5482-2 (eBook - PDF)

Contents

Preface

As the IT industry advances, cloud computing represents the next big computing platform change. It is the most significant transformation since the introduction of the Internet in the early 1990s. Cloud computing along with virtualization technology will literally revolutionize the way we run a business. The cloud provides a flexible, secure, scalable, and affordable IT infrastructure. E-commerce and educational institutions can particularly benefit from cloud-based IT infrastructures.

Through the Internet, cloud-based IT infrastructures allow companies and educational institutions to subscribe to software, an IT infrastructure, or an application development platform from a cloud provider. This way, it is not necessary for subscribers to build their own IT infrastructure for supporting their computation needs. As a result, subscribers can significantly reduce the cost of IT development and management. Companies and educational institutions can also develop their own private clouds to take advantage of the flexibility, security, availability, and affordability of a cloud computing environment.

To catch up on the cutting-edge technology such as cloud computing and network virtualization, this book is designed to provide enough networking theory and concepts for readers to understand cloud computing. In addition, the book provides hands-on practice in a cloud-based computing environment.

Motivation

More and more companies and educational institutions are planning to adopt a cloud-based IT infrastructure. Therefore, today's job market requires IT professionals to understand cloud computing and have hands-on skills for developing cloud-based IT infrastructures. Although professional development books in the cloud

computing field are available, they are usually for more experienced IT professionals. For many university students and entry-level IT professionals, there are a handful of challenges to master cloud technology. It is difficult for them to understand cloud computing without adequate knowledge of networking and system administration.

Understanding the needs of entry-level IP professionals and university students has motivated the author to write this book, which includes systematic coverage of networking and system administration for better understanding cloud computing.

Objectives of the Book

With this motivation, this book is designed with the following objectives. First, it provides IT professionals with the necessary networking and system administration knowledge to better understand cloud computing. Second, it helps IT professionals to get a quick start in deploying cloud services. The book provides detailed instructions on establishing a cloud-based computing environment where IT professionals can carry out all the hands-on activities in this book. The cloud-based computing environment allows readers to develop cloud services collaboratively or individually. Third, it enhances readers' hands-on skills by providing lab activities. Through these lab activities, readers can develop a fully functioning cloud-based IT infrastructure with Microsoft Azure. Last, this book demonstrates how networking plays a key role in a cloud-based IT infrastructure. It helps readers understand how to set up networks for a cloud-based IT infrastructure. It also demonstrates how networks are used to construct cloud services.

Features of the Book

This book integrates networking and cloud computing. Networking and system administration theory and concepts are used to explain cloud computing technology. Hands-on practice is conducted in the cloud computing environment. To help IT professionals catch up with the trend in cloud computing, the public cloud provider, Microsoft Azure, is used to establish a cloud computing environment. This book also illustrates the development of a private cloud with Hyper-V. After systematic coverage of networking theory and concepts such as virtual network, private network, and certification, this book leads the reader to the development of a hybrid cloud that integrates the public cloud and the private cloud.

The following are the features that make the book valuable for readers who are interested in learning about cloud-based IT infrastructures.

- *Cloud computing*: This book focuses on networking used to construct a cloud computing environment. Microsoft Azure is used to build and manage virtual networks.

- *Real-world approach*: Many hands-on activities are added to help readers develop a cloud-based IT infrastructure that can be used for a real-world business.
- *Combination of theory and hands-on practice*: This book provides adequate networking theory, enough for readers to understand cloud computing. Comprehensive lab activities are used to help readers make the connection between theory and practice.
- *Online development*: This book provides detailed instructions and resources for creating and managing online computer labs by using the Microsoft Azure academic account.
- *Instructional materials*: To help with teaching and learning, this book includes instructional materials such as an instructor's manual, PowerPoint presentations, and solutions.

The book focuses on its goal to make sure that readers learn how to develop a cloud-based network system for a real-world business. The content of the book is suitable for undergraduate and beginning graduate courses related to networking as well as for IT professionals who do self-study on cloud computing.

For the convenience of entry-level IP professionals and university students, the book is designed in the following manner:

- *Self-contained content*: For readers' convenience, the book is self-contained. It includes some necessary basic networking concepts, hands-on activities, and information about cloud-based network services.
- *Suitable for self-study*: This book provides detailed instructions that are suitable for self-study. It not only presents the theory and concepts but also explains them through examples, illustrations, and hands-on activities.
- *Designed for Microsoft Azure*: The book is specially designed for Microsoft Azure. All the hands-on activities can be conducted with the Windows Server operating system.
- *Step-by-step instructions*: For hands-on activities, the book provides step-by-step instructions and illustrations to help beginners. It also provides instructions on setting up a cloud environment for hands-on practice.

With these features, readers will be able to implement a cloud-based IT infrastructure and other cloud-based services in a short time.

Organization of the Book

This book includes 11 chapters. Each chapter contains an introduction of its content, the main body of the chapter, a "Summary" section to summarize the discussion in the chapter, and a "Review Questions" section to help readers review the knowledge

learned from the chapter. Each chapter also includes hands-on activities to help readers practice the skills learned in the chapter.

Chapter 1 introduces networking and network operating systems. It outlines the use of network operating systems in cloud computing. This chapter gives an overview of the commonly available public cloud providers and packages used for developing private clouds. The lab activity in this chapter prepares a cloud computing environment for the lab activities in later chapters.

Chapter 2 deals with the necessary network protocols to be used in cloud computing. Three hands-on activities are used to explore the network management tools provided by the Windows Server operating system.

Chapter 3 covers the topics related to network design and IP addressing. It describes how the Internet works. It also describes other types of networks used in implementing cloud computing. The hands-on practice of this chapter creates a virtual network on Microsoft Azure. The virtual network is used to illustrate the concepts of local area networking and subnetting.

Chapter 4 introduces directory services, which are the key components of cloud computing. The chapter describes how directory services are used in enterprise-level IT infrastructure management. It provides technical details on the development and implementation of directory services. In the hands-on practice of this chapter, the Active Directory service is implemented on virtual machines hosted by Microsoft Azure.

Chapter 5 introduces network services such as the dynamic host service and name service, which are often used in cloud computing. The theory and concepts of the dynamic host service and name service are described in detail. The hands-on activity in this chapter illustrates the implementation of the dynamic host service and name service in Microsoft Azure.

Chapter 6 demonstrates how to use Windows PowerShell for network and cloud management. This chapter introduces programming units such as cmdlets, PowerShell functions, and PowerShell Scripts. During hands-on activities, readers can experiment with such units in the Microsoft Azure cloud environment. This chapter also presents the use of Microsoft Azure PowerShell for cloud service management.

Chapter 7 discusses Internet data transaction protection. In the cloud computing environment, it is necessary to protect the data transaction between a cloud provider and a cloud service subscriber. The chapter introduces network security tools such as Secure Sockets Layer (SSL) and Certificate Services. The hands-on activity in this chapter implements Certificate Services in the Microsoft Azure cloud environment.

Chapter 8 covers IP Security (IPSec), which is used in later chapters to link the virtual networks created in Microsoft Azure to the on-premises network of an enterprise. IPSec is a security protocol to secure the network protocols above the Internet layer. The hands-on activities implement IPSec in the Microsoft Azure cloud environment.

Chapter 9 explains the theory and concepts of network routing. Routers are used to connect networks. In this book, the virtual networks in the cloud and the on-premises

networks of an enterprise are connected with routers. This chapter also discusses Network Address Translation (NAT), which allows the virtual machines on a private network to share a single Internet connection. There are two activities for this chapter's hands-on practice. The first one creates a routing service with Windows Server and second one implements a NAT service.

Chapter 10 discusses the virtual private network (VPN) architecture. VPN allows an enterprise to integrate its own network with a virtual network in a cloud. This chapter gives the pros and cons of different types of VPN technologies. It focuses on the IPSec-based VPN and SSL-based VPN, which are used by Microsoft Azure to remotely access the on-premises network of a company from a virtual network in a cloud or vice versa. Two hands-on activities are included in this chapter. The first one is used to create a point-to-site connection between a local computer and Microsoft Azure. The second one creates a site-to-site connection between Microsoft Azure and an on-premises network.

Chapter 11 covers the hybrid cloud, which integrates public clouds with private clouds. It introduces hybrid cloud technology and its application in a cloud-based enterprise network. With the System Center Virtual Machine Manager (SCVMM) package, the hands-on activity of this chapter creates a hybrid cloud that integrates Microsoft Azure with a private cloud created on a local network.

One or more hands-on activities are included in each of the chapters. It is recommended that readers complete the activities in the previous chapters before starting the hands-on activity in the next chapter because some of the hands-on activities may depend on the ones in the previous chapters.

Acknowledgments

I thank my family for their continuous and loving support, patience, and understanding of my work.

My special gratitude goes to my students and Dr. Jenny Huang for their participation in the book proofreading process. They carefully reviewed the content of the manuscript. Their constructive suggestions and corrections greatly improve the quality of the book.

I also thank the outstanding editorial staff members and other personnel at Auerbach Publications of Taylor & Francis Group for their support of this project. I truly appreciate the encouragement and collaboration of John Wyzalek, senior acquisitions editor, and all the other people who have been involved in the book's production. The book would not have been possible without their inspiration and great effort.

Author

Lee Chao, PhD, is currently a professor in the Science, Technology, Engineering, and Mathematics Division at the University of Houston, Victoria, Texas. He earned his PhD from the University of Wyoming, Laramie, Wyoming. He has been teaching IT courses for over 20 years. His current research interests are database system development and cloud computing. Dr. Chao is also the author of more than a dozen research articles and books in various areas of IT.

1

Overview on Cloud and Networking

Objectives

- Draw an overview of network servers.
- Understand the role of network servers in networking.
- Learn about the process of implementing networks.
- Set up a cloud-based lab for hands-on practice.

1.1 Introduction

In an enterprise, IT infrastructure is needed to provide employees with the necessary hardware and software to do their job. The key component of the IT infrastructure is the network that connects servers, desktop computers, and mobile devices. The IT infrastructure in an enterprise is a high-cost and high-maintenance unit. It requires expensive hardware and software and skilled IT service staff members to keep it running.

Cloud computing is a technology that can be used to support online IT infrastructure. Cloud computing has become the new trend in delivering business applications and services. The cloud is a cost-effective, flexible, reliable IT infrastructure to support e-commerce and e-learning. With the cloud, employees across the world are able to access the hardware and software provided by an enterprise. In addition, an enterprise can allow its contractors to create their own virtual IT infrastructures on the cloud. Cloud computing can also provide a collaboration platform for developers to participate in an application development project anywhere and anytime. When an enterprise develops a cloud for its own use, this type of cloud is called a private cloud. When a cloud provides cloud services for the public to subscribe, this type of cloud is called a public cloud. When a cloud integrates both the public and private clouds, it is called a hybrid cloud. A large enterprise usually has its IT infrastructure created on a hybrid cloud.

Since a cloud can be considered an online IT infrastructure, the network is also a key component of the cloud. Networking theories and practice have been widely used in cloud computing. To understand the usage of the cloud in an enterprise, one has to have a thorough understanding of networking theories and practice. At the end of this book, a hybrid cloud will be developed. To get there, the reader needs to be familiar with the cloud-related networking theories and practice.

As networks play a key role in today's IT industry, networking has become a required subject in the computer science and information systems curricula. Networking theories and practice are taught at different levels in high schools and higher education institutions. Students majoring in IT-related fields are required to have networking knowledge and skills.

This chapter will first introduce the types of networks. Then, it will introduce the operating systems that are able to provide network services and manage network devices. It will analyze the functionalities of these operating systems and present their functionalities through network architecture. This chapter will explain how cloud computing is supported by the operating systems. It will discuss the networking process and illustrate how to implement a network system. At the end of the chapter, instructions will be provided on how to develop a cloud-based lab environment for conducting hands-on activities in later chapters.

1.2 Networks

To transmit data from one computer to another computer, the two computers need to be connected via network hardware and software. Computers, printers, copiers, or storage devices linked by a network are called hosts. Each host has a network interface card (NIC) to which a network cable or another connection medium is connected. The network cable or connection medium carries binary electronic signals back and forth between two hosts. When there are multiple hosts on a network, these hosts are connected to a network device called a switch through which electronic signals are distributed to other hosts. The network device, router, is used to connect two different networks. In the IT industry, it is known that a switch is used to construct a network and a router is used to connect networks.

There are different types of networks such as the local area network (LAN), wide area network (WAN), Internet, and cloud-based network. A LAN is a type of network that exists within a room or a building as shown in Figure 1.1. A WAN is a type of network that is highly scalable and may cover a large geographic area (Figure 1.2). The Internet is a worldwide network system formed by interconnecting LANs and

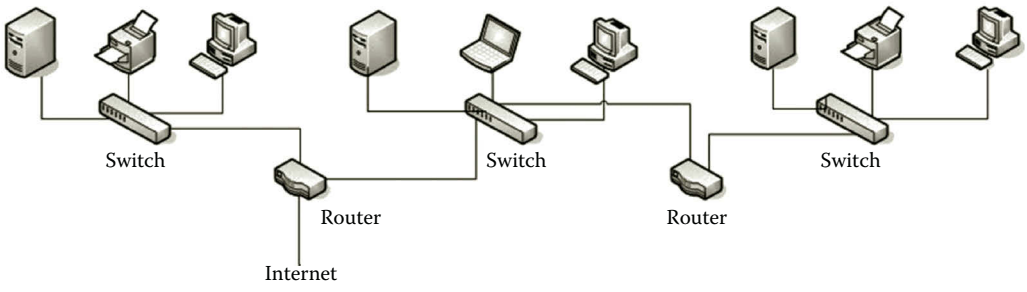

Figure 1.1 Local area network.

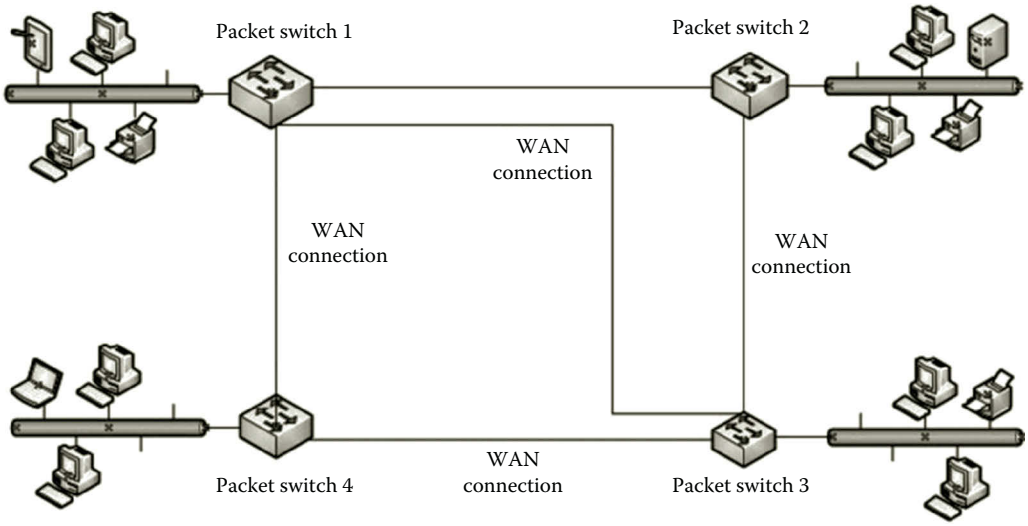

Figure 1.2 Wide area network.

WANs as shown in Figure 1.3. The LAN is connected to the Internet through one of the Internet Service Providers (ISPs). The ISP communicates with the regional network through an access point called a point of presence (POP). It can be a telecommunication facility rented by an ISP for accessing the global network, or it can be any facility used to access the Internet such as a dial-up server, router, or ATM switch. ISPs are connected through a network access point (NAP), which is a major Internet interconnection point.

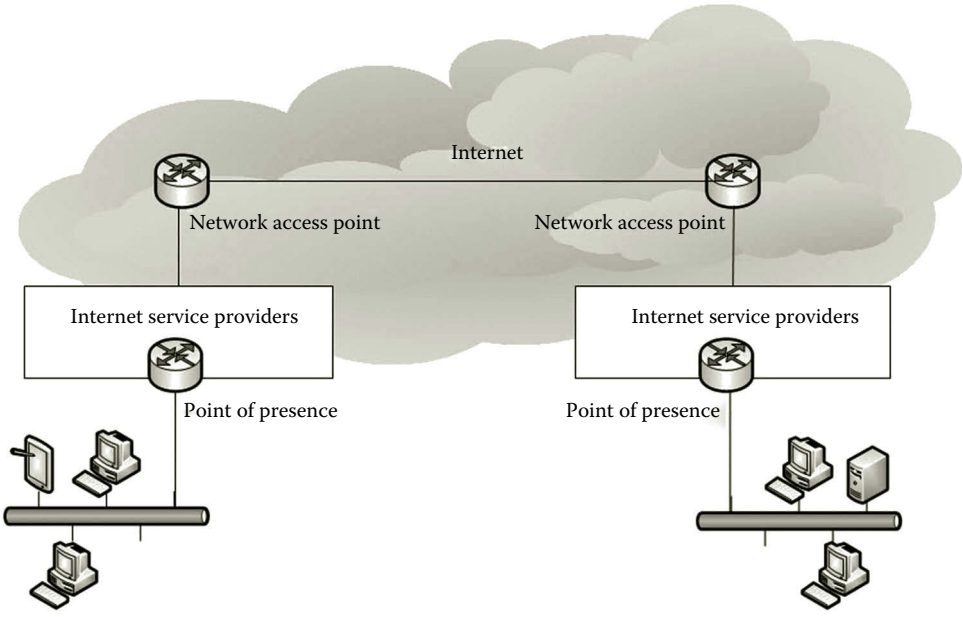

Figure 1.3 Internet.

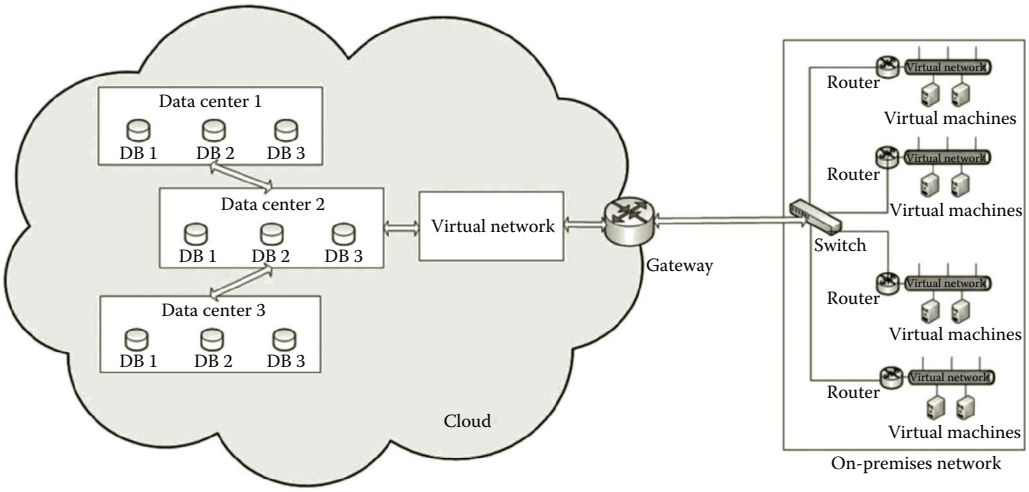

Figure 1.4 Cloud-based network.

A cloud-based network is an enterprise network that can be extended to the cloud shown in Figure 1.4. The cloud-based network allows an enterprise to distribute its network around the world. The cloud significantly simplifies the development of an enterprise network system. In the cloud, the underlying network is constructed by a cloud provider. All an enterprise needs to do is to connect its on-premises network to the network built in the cloud to form a global enterprise-class network system. There is no initial capital investment in this type of global network system.

Unlike the Internet, the cloud-based network provides centralized control over network visibility. Through the cloud-based network, the enterprise is able to provide a multitenant application, which is a software application that serves multiple tenants. Each tenant subscribes an instance of the application. Each tenant's data are isolated and remain invisible to other tenants. On the other hand, the maintenance and update of the application can be greatly simplified. The cloud-based network enables the enterprise to deploy IT infrastructures to remote locations in minutes (Figure 1.4).

The cloud-based network targets organizations with a large number of sites around the world. There could be a couple of hundred to ten thousand employees working in multiple sites such as branch offices, schools in a school district, clinics, manufacturing facilities, or retail stores. Through the management tools deployed in the cloud, network administrators are able to manage the enterprise-distributed networks anywhere and anytime. The management tools can be used to manage cloud-hosted virtual machines and mobile services. They are used to accomplish tasks such as centralized management, remote monitoring, remote software and app installation, remote wiping, and security auditing.

1.3 Network Operating Systems

Operating systems can be categorized as a server edition, desktop edition, and mobile edition based on the tasks performed by them. The server edition can be used to manage networks and is capable of providing network services. Here, our focus is on server edition operating systems. In the following, we will discuss several commonly available server edition operating systems that are capable of networking.

Most of the low-cost network server operating systems are developed to run on the ×86 platform, which is powered with the microprocessors from Intel and AMD. The ×86 platform was originally created for personal computers. Today's ×86 platform is built on multicore ×86 microprocessors, which can handle large-scale networking tasks. Popular operating systems such as Linux, Windows, and some versions of the UNIX operating system are all supported by the ×86 platform.

1.3.1 Windows Server 2012

For networking, Windows Server 2012 provides tools to accomplish the following tasks:

- *Network management*: The tasks may include network performance management, network device management, system backup and restoration, troubleshooting, and so on.
- *Network services*: The tasks may include developing and managing network services such as IP address management service, dynamic IP address assignment, name service, Web service, email service, VOIP service, and so on.
- *Network security*: The tasks may include user authentication, certification service, data encryption, network monitoring, setting up firewalls, virus protection, and so on.
- *Remote access and routing*: The tasks may include sharing network resources through VPN and DirectAccess. Windows Server 2012 can also accomplish tasks such as routing network traffic from one network to another network.
- *Cloud communication management*: The tasks may include extending a private cloud to a public cloud by securely connecting the private cloud to the public cloud. The public cloud can also be used to extend the data center located on the private cloud.
- *Virtualization*: Windows Server 2012 includes the virtualization tool, Hyper-V. With Hyper-V, we are able to accomplish the tasks of creating virtual machines, virtual networks, and virtual network devices such as virtual switches.

Compared with the older version of Windows Server, Windows Server 2012 was designed with the cloud concept in mind. New networking features have been added

mainly to support cloud computing. The new features such as failover clustering, virtualization, and file services have all been added for this purpose. The virtualization tool Hyper-V has been modified so that it can help set up environments in the cloud.

Hyper-V is broadly used to create and manage virtual machines and virtual network devices such as virtual switches. With Hyper-V, one can create virtual networks that are independent of the underlying physical network. For network security management, the virtual networks created with Hyper-V can be isolated from each other. For example, the virtual network for hands-on practice in a networking class can be made to isolate itself from that of the Admissions office. Also, deploying the workload to multiple virtual networks can improve the performance of a large project such as a datacenter.

Hyper-V has a feature called live migration; that is, virtual machines hosted by virtual networks can live migrate anywhere without service disruption. These virtual networks can be migrated to a cloud while preserving their existing IP addresses. With the IP addresses preserved, the virtual networks on the cloud can emerge into the on-premises network. All the services provided by these migrated virtual networks can continue to function without knowing where the underlying physical network is. With Hyper-V, a true hybrid cloud can be established by seamlessly integrating a public cloud and a private cloud running on an on-premises network.

In Windows Server 2012, most of the management tasks can be done through the Server Manager interface shown in Figure 1.5. Networking tasks such as active directory administration, dynamic IP addressing, name service, virtualization, and remote access can all be handled in Server Manager.

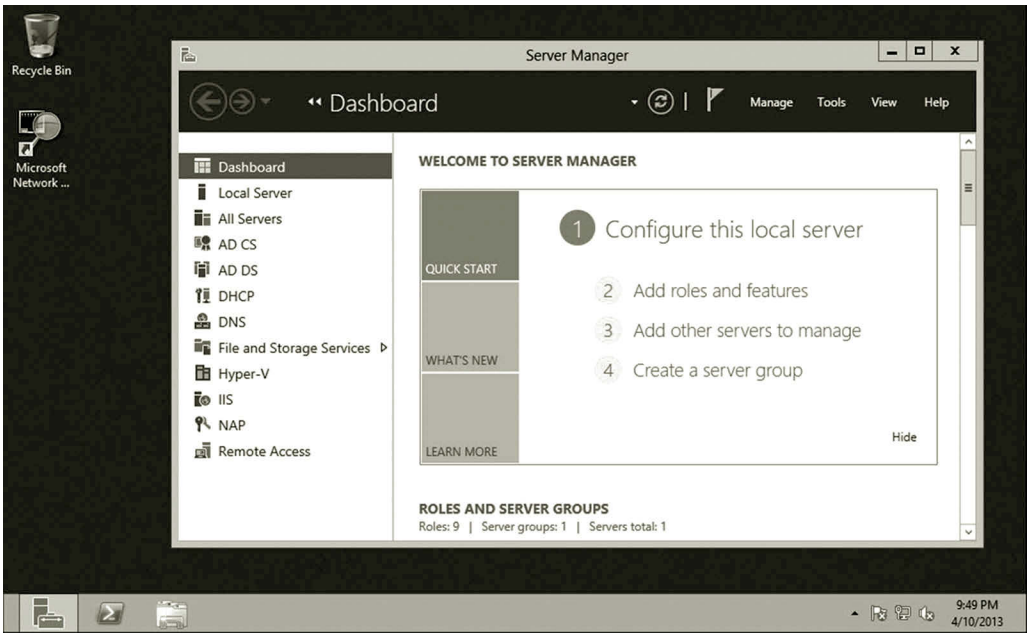

Figure 1.5 Server Manager.

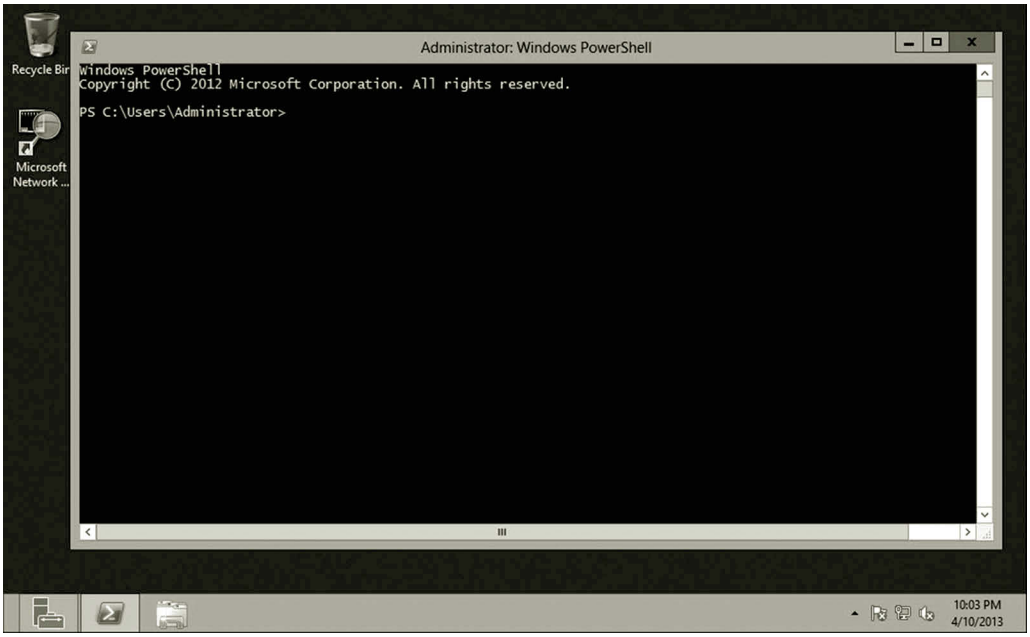

Figure 1.6 Windows PowerShell.

The management tasks can also be done through the command interface, Windows PowerShell (Figure 1.6). Windows PowerShell is a powerful management tool which includes 2430 cmdlets. A network administrator can write a script to automate a large task that needs to execute multiple cmdlets.

Windows Server 2012 uses a new Metro GUI design for touch-centric devices. In Metro GUI, the Start menu is a matrix of icons as shown in Figure 1.7.

1.3.2 Microsoft Azure

Microsoft Azure is a cloud computing platform built on a global network of Microsoft-managed datacenters. Microsoft Azure uses a customized version of Hyper-V known as Windows Azure Hypervisor to handle virtualization tasks. The operating system running on Microsoft Azure is used to manage computing and storage resources. It also provides security protection and remote access mechanisms. The Microsoft Azure development environment is highly scalable. Additional computation capacities can be added as desired until the subscription limit is reached. Microsoft Azure provides a highly available computing environment. With Microsoft Azure, IT professionals can work on their projects from anywhere and at any time. With Microsoft Azure, there is no initial cost on IT infrastructure development and management. However, users need to pay monthly for the storage and computing usage. Figure 1.8 shows the Microsoft Azure Management Portal.

Microsoft Azure provides three types of cloud services, Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). For data storage,

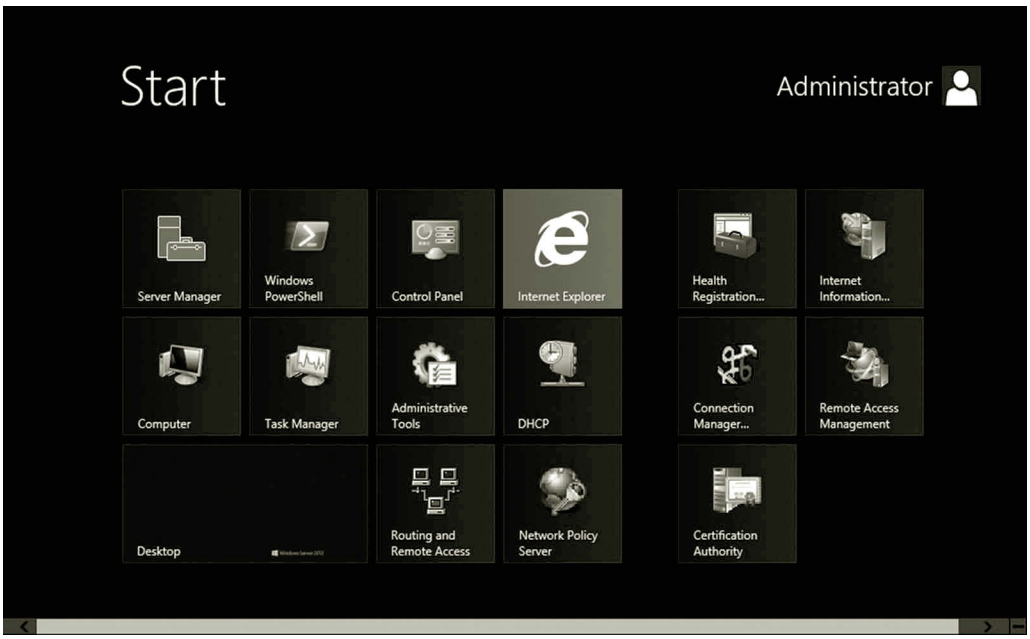

Figure 1.7 Metro GUI.

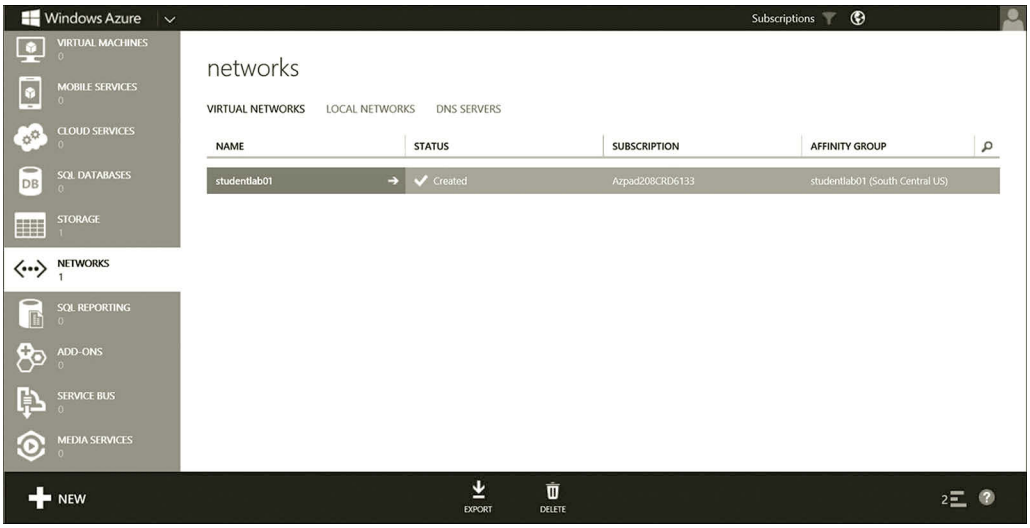

Figure 1.8 Windows Azure management portal.

Microsoft Azure offers Windows Azure SQL Database for storing and managing relational data and data storage services for storing and managing nonrelational data. Microsoft Azure provides software such as server operating systems like Windows Server 2012 and SUSE Linux Enterprise Server (SLES). It also provides database management system (DBMS) software such as Windows Azure SQL Database, which is the cloud version of Microsoft SQL Server. The Windows Azure emulation

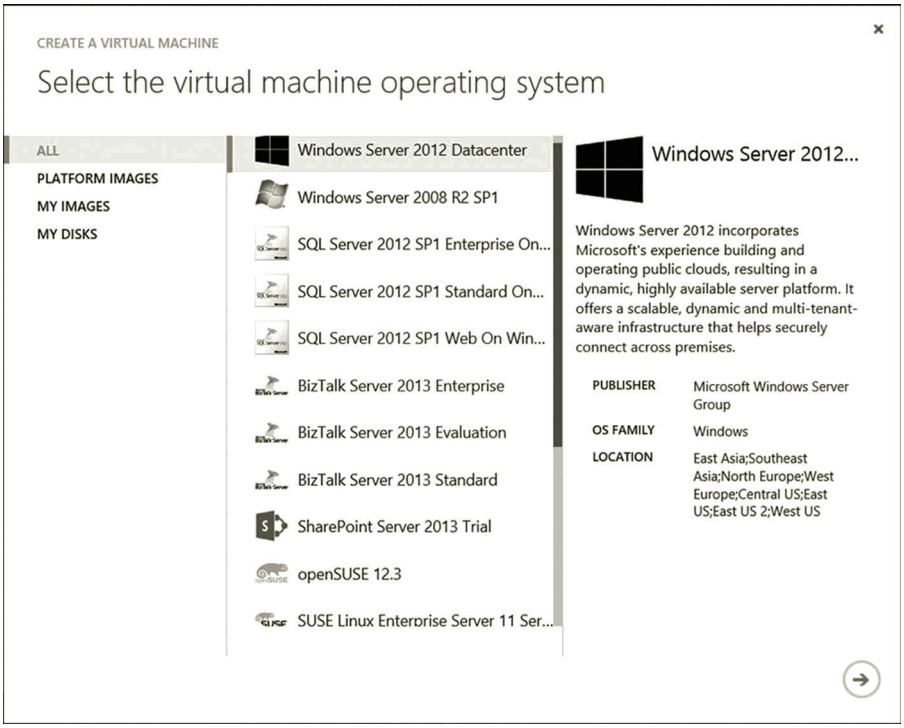

Figure 1.9 Operating systems provided by Windows Azure.

software and Windows Azure Software Development Kit (SDK) can be downloaded to students' home computers to emulate the Microsoft Azure cloud environment on a local computer. Figure 1.9 shows the operating system software provided by Microsoft Azure.

To help cloud subscribers to extend their existing networks into the public cloud, Microsoft Azure offers a range of networking capabilities such as Virtual Network, Windows Azure Connect, and Traffic Manager. Figure 1.10 shows the Virtual Network tools.

Windows Azure Virtual Network provisions and manages the VPN connection between the on-premises IT infrastructure and Microsoft Azure. Virtual Network is used to set up a hybrid cloud, which consists of the private cloud run on the on-premises network and the public Microsoft Azure cloud. With Virtual Network, an administrator can accomplish tasks such as setting up IP security service to provide a secure connection between the corporate VPN gateway and Microsoft Azure. Virtual Network can also be used to configure DNS service and IP address for virtual machines.

Windows Azure Connect is a tool used to connect the services provided by two machines; one is located on the on-premises network and the other one is on Microsoft Azure. This tool can be used to help application developers to build cloud applications hosted in a hybrid environment. It allows services such as Web service on

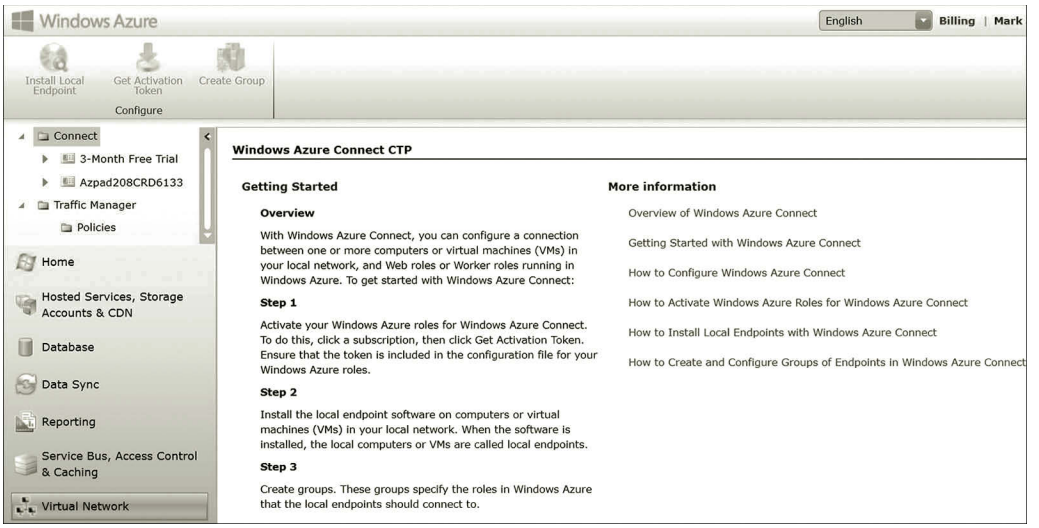

Figure 1.10 Virtual network tools.

Microsoft Azure to securely access an on-premise SQL Server database server. It can also authenticate users on Microsoft Azure against an on-premise Active Directory service. With this tool, application developers can use the debugging tools provided by the on-premises applications to do troubleshooting for the applications hosted on the Microsoft Azure cloud.

Traffic Manager is a tool used to balance the network traffic across multiple Microsoft Azure hosted services. This tool can help improve an application's performance, availability, and elasticity. To improve availability, Traffic Manager provides automatic failover capabilities when a service goes down. It also monitors Microsoft Azure hosted services. To improve performance, it allows the services to run at the datacenter closest to the end-user to reduce latency.

1.3.3 VMware vCloud Suite

The VMware vCloud Suite® is an integrated package used to provide a full cloud solution at the enterprise level. It includes the operating system, management software, and front-end user interface. The following are the main products included in the suite.

VMware vSphere: vSphere is a cloud computing virtualization operating system provided by VMware. vSphere provides a virtualization platform for enterprises to make use of both the public and private cloud services. One of VMware's goals is to be able to connect a private cloud to any public cloud provider. When there is a burst of workload, vSphere can seamlessly migrate some of the workload to a public cloud. To achieve this goal, VMware has developed the open-source standard, Open Virtualization Format (OVF), used for packaging and distributing virtual machines. Through OVF, VMware enables the sharing of virtual machines between

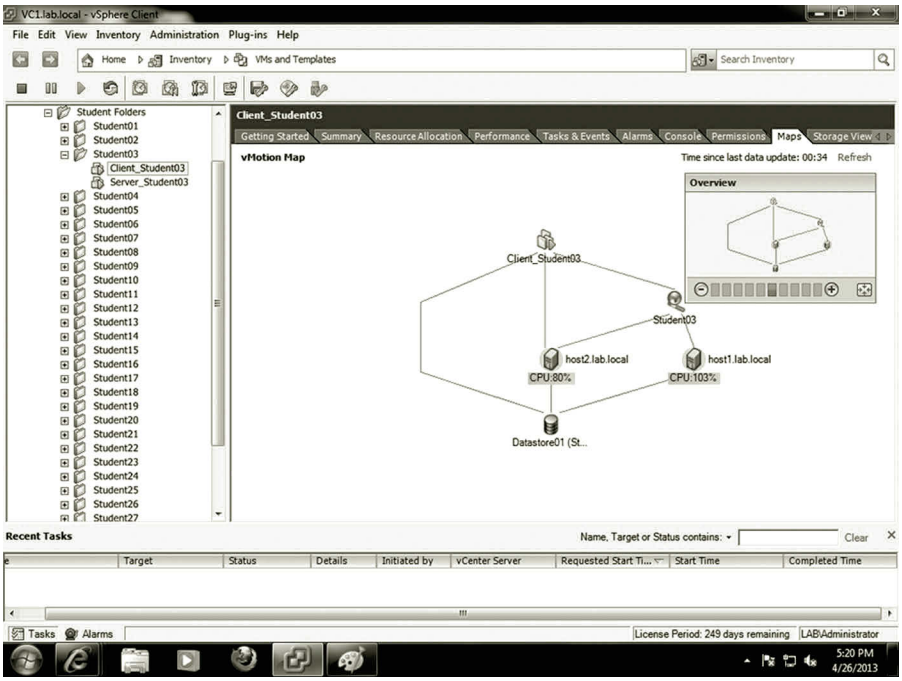

Figure 1.11 vMotion map.

two different virtual machine platforms and the sharing of virtual machines over the Internet. vSphere is able to migrate running virtual machines and attach storage devices to host servers. Figure 1.11 illustrates a map of host servers, virtual machines, and the centralized data store.

To enhance network security and manageability, VMware has been working on the new operating system NSX as the network and security virtualization platform. With NSX, to help with virtualization security, VMware provides tools to help users to store virtualized applications and data in a separated zone where no unauthorized user can access. NSX allows users to create virtual networks to accomplish tasks such as switching, routing, firewall setting, load-balancing, and so on. NSX also allows its partners to securely integrate their physical and virtual networks into the NSX platform. For security, NSX does not require disruptive hardware to be upgraded. To support virtual machines made by other server hypervisors, VMware is designed to support server hypervisors such as KVM and Xen. It can also work with any cloud management systems, for example, VMware vCloud, OpenStack, and CloudStack.

As a network operating system, vSphere can be used for datacenter-wide network integration by centralizing the network provision and network management. It provides management tools such as vSphere Distributed Resource Scheduler (DRS) for dynamically balancing computing resources and power consumption, vSphere High Availability for fault tolerance, data protection and replication, vShield Zones for securing vSphere with application-aware firewall and antivirus functions, and vSphere Auto Deploy for rapid deployment.

Applications developed by application developers such as those from Microsoft and Google all have their architectures, not to mention that many companies have their own applications. The architecture of an application may not match the architecture of a cloud provider. The difference in application architecture makes it hard to migrate these applications to the public cloud. Assisting the migration of applications to the cloud environment is another goal of VMware. VMware includes the plugins from application developers so that their applications can run on vSphere. VMware is also working on the technology that can help a company run their apps in a self-service provisioning enabled cloud. Self-service provisioning allows the end user to deploy and manage applications in the cloud computing environment.

For networking, vSphere provides four types of services for network system development:

- The first type of service is used to connect virtual network devices and virtual machines hosted by a vSphere server.
- The second type of service connects virtual network devices and virtual machines to the underlying physical network.
- The third type of service connects the services on the virtual network to the underlying physical network.
- The fourth type of service is used for managing the host server where the vSphere is installed.

VMware vSphere can virtualize network devices such as NICs and switches for connecting virtual machines. Figure 1.12 shows the virtual machines hosted by a vSphere server.

With VMware vSphere, various virtual IT infrastructures can be delivered as services. That is, the IT infrastructures designed for different types of businesses can be delivered without resetting the underlying physical network. VMware vSphere provides network performance analysis tools for network monitoring and management. Figure 1.13 shows a virtual machine performance chart and Figure 1.14 illustrates vSphere computing resources.

vCloud Director: This product is used to provide virtual datacenter services. It creates a secure multitenant environment to fully utilize the hardware capability and other computing resources. It allows the rapid cloning of the previously built virtualized IT infrastructure called vApps. It can also be used to deploy a virtualized multitier client–server IT infrastructure.

vCloud Networking and Security: This product offers a broad range of services including virtual firewalls, VPN, load balancing, and VXLAN extended networks. VXLAN is designed to allow an application to be scaled across clusters without any reconfiguration of a physical network. To protect data security, vCloud Networking and Security scans sensitive data and reports violations. The report can be used to assess the state of compliance with regulations.

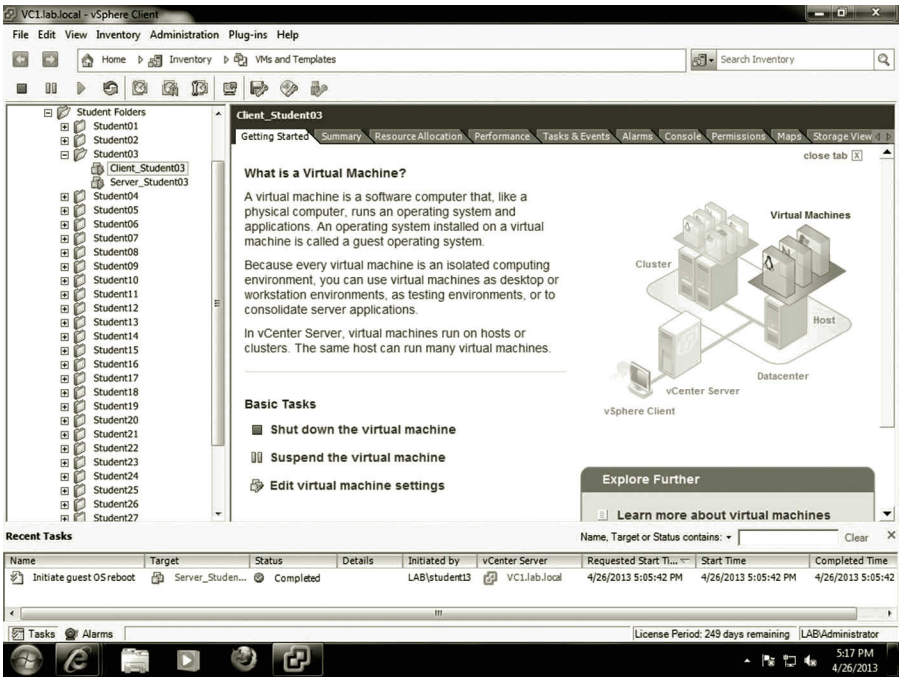

Figure 1.12 Virtual machines hosted by vSphere server.

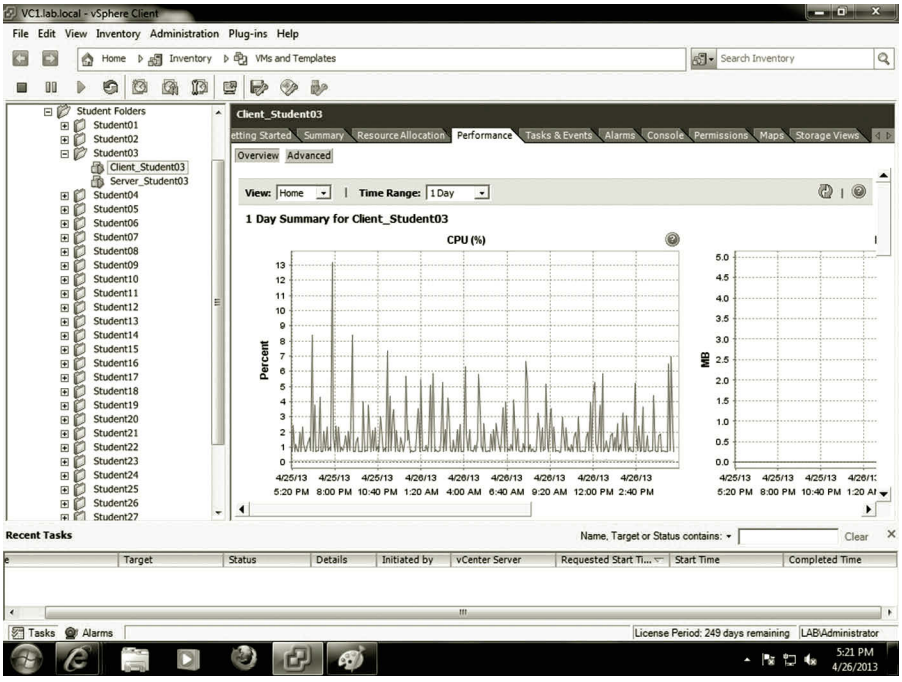

Figure 1.13 Performance monitoring.

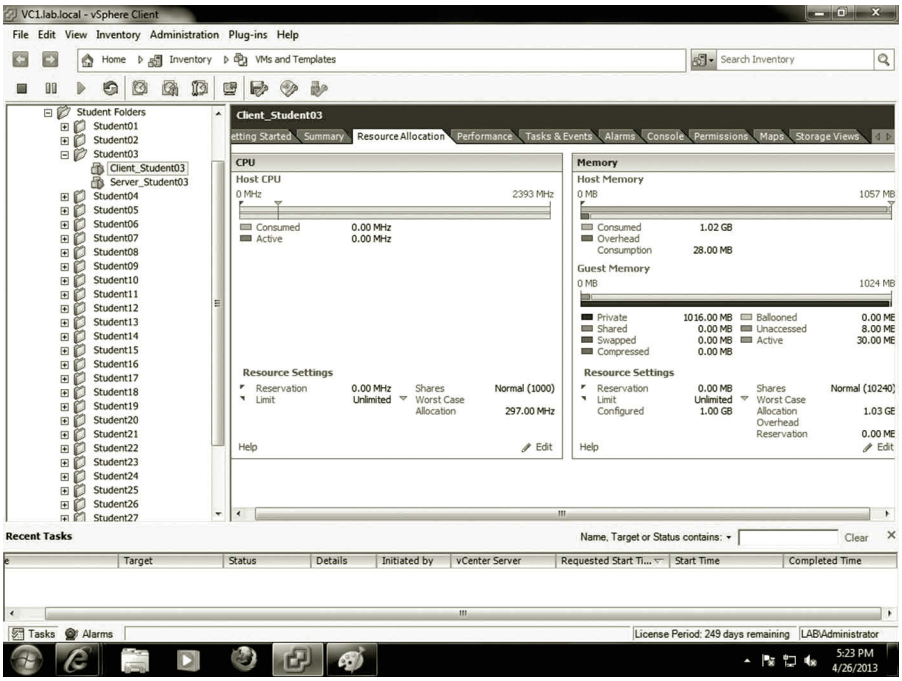

Figure 1.14 Computing resources.

vCenter Operations Management Suite: As a management tool, the product provides automated operations management through an integrated approach to performance, capacity, and configuration management. The vCenter Operations Management Suite enables IT organizations to get better visibility and actionable intelligence to proactively ensure service levels, optimum resource usage, and configuration compliance in dynamic virtual and cloud environments.

vFabric Application Director for Provisioning: It is a cloud-enabled application provisioning and maintenance solution. This tool simplifies the process of creating and standardizing application deployment across cloud services. With the tool, multitier applications can be deployed to any cloud.

vCloud Automation Center: With this tool, users can rapidly deploy and provide cloud services across private and public clouds, physical infrastructures, hypervisors, and public cloud providers. It provides user authentication service and helps to enforce business policies throughout the service lifecycle.

vSphere Client: vSphere Client is a GUI tool for managing vSphere. vSphere has two versions of vSphere Client, the regular vSphere Desktop Client, and the vSphere Web Client. Some of the new features of vSphere can only be managed with the vSphere Web Client. With the vSphere Desktop Client, a network administrator can accomplish tasks such as connecting to a vSphere host, VXLAN Networking, changing the guest OS on an existing virtual machine, editing virtual network attributes, viewing vCenter Server maps, and so on. Figure 1.15 demonstrates the guest operating system running on a vSphere host server.

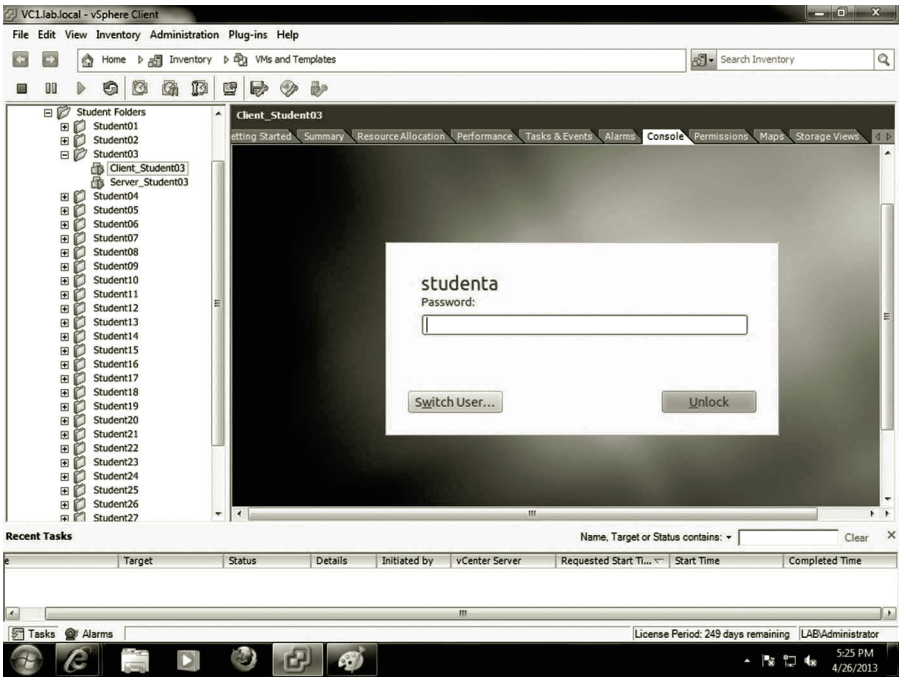

Figure 1.15 Guest operating system on host server.

By using the vSphere Web Client, the network administrator can perform tasks such as user authentication management, inventory management, vSphere replication, workflow management, virtual machine migration management, logging, virtual distributed switch management, and vSphere data protection.

1.3.4 Linux

Linux is an open source operating system, which is licensed under the GNU General Public License. The operating system source code can be freely modified, used, and redistributed by anyone. Since the World Wide Web and Internet-related protocols such as IP are open source technologies, it is convenient to include these protocols in the operating system. With these open source protocols, Linux is widely used as a network server to accomplish various networking tasks. Linux can be made to serve as an enterprise-level server operating system. It is built to multitask and allow multiple users to work on the same server computer at the same time. Therefore, a Linux operating system is often used in a grid system for distributed computing. As Linux is able to communicate with other network technologies such as Windows and Novell, Linux can also host the directory service. As an open source product, the total cost of using Linux is low. However, it requires technicians to have adequate knowledge to handle daily operations. The main cost of using Linux is the support and services offered by Linux distributions. In general, Linux requires less computing resources and is able to

work with older network devices. The Linux operating system is able to run on a broad range of computing architectures such as ×86, POWER, SAPRC, and Itanium 2. This feature is especially suitable for organizations that have a limited budget and are not able to upgrade their equipment frequently.

Next, we will look at some of the Linux operating systems that are capable of supporting cloud computing. Among these Linux operating systems, you can find virtual machines preinstalled with SUSE Linux Enterprise or Ubuntu Linux on Microsoft Azure. Also, you can download a readymade virtual machine with Red Hat Linux installed for VMware.

Red Hat Linux: Red Hat, Inc. was founded in 1993. Red Hat has two editions of operating systems, Fedora and Red Hat Enterprise Linux. Fedora is the open source version of the Linux operating system, which is managed by the Linux user community and Red Hat employees. Even though Fedora is free, it is a fully functioning operating system. Red Hat uses Fedora as a testing platform for many new services and innovation tools. During the testing period, programmers from the user community and Red Hat work together to fix problems found in the new products. As Linux is updated frequently, Fedora is updated every 4–6 months. Since Fedora is a free operating system, Red Hat does not provide training and support for Fedora.

Red Hat Enterprise Linux is known as the Linux operating system for supporting enterprise-level computation. It charges fees for support and services. The support and services are necessary for developing and managing an enterprise-level IT infrastructure. Red Hat Enterprise Linux provides 24 × 7 integrated service. Customers can often get response within 1 h. In addition to the support and services, Red Hat also provides various training and certification service on Red Hat Enterprise Linux. Red Hat Enterprise Linux is a more stable operating system. It only includes those new services and innovation tools that are proven to work. Red Hat Enterprise Linux will be upgraded to a new version after three new upgrades of Fedora. Red Hat Enterprise Linux is going to be fully supported by Red Hat for 7 years after it is upgraded. It is widely supported by computer hardware companies such as Dell, HP, and IBM. It is also supported by over a thousand application software companies such as Oracle, CA, IBM, and so forth. The software from these companies is tested on the Red Hat operating system. Although the Red Hat operating system often runs on the ×86 platform, it is also able to run on other platforms.

For cloud computing, Red Hat provides an open hybrid cloud solution. Red Hat allows its customers to create a hybrid cloud in their own way and there is no vendor lock-in. That is, the customer has the freedom to access data in various structures, to build any application or service regardless of technology and platform. The open cloud allows customers to add a variety of features, cloud providers, and technologies from different vendors. With Red Hat, customers can fully utilize the existing IT infrastructure and build a cloud solution piece by piece. They are able to connect their private clouds to a wide range of public clouds such as Amazon and IBM.

Red Hat can make applications and data portable across different clouds. It also allows the management of applications across heterogeneous infrastructures.

Red Hat provides a number of products for developing cloud services. Among these products, CloudForms can be used to develop IaaS service and OpenShift can be used to develop PaaS service. With CloudForms, one can construct a virtualized system with a mixture of hypervisors and virtualization management software, and the technologies from various public clouds. CloudForms allows users to create a pool of virtual machine images consisting of an operating system, applications, and associated supporting software. It also allows users to manage, deploy, and monitor virtualized systems. OpenShift has two versions, OpenShift Online and OpenShift Enterprise. OpenShift Online is a public cloud providing PaaS service. OpenShift Enterprise is a comprehensive enterprise development platform. With OpenShift Enterprise, a team of developers can develop, deploy, and execute enterprise applications in either a private or public cloud environment.

SUSE Linux: SUSE Linux is another major Linux distribution owned by Novell. Like Red Hat Linux, there are two editions of SUSE Linux, openSUSE and SUSE Linux Enterprise. openSUSE is available in a free-download open source package. It is also available in a retail package, which contains a printed manual, a DVD, and bundled software. openSUSE also includes some proprietary components such as Adobe Flash. After Novell acquired SUSE Linux from a SUSE UNIX consulting company in Germany, Novell added the GUI-based system management software YaST2 to SUSE Linux. Novell also provides two proprietary editions of the Linux operating system, SUSE Linux Enterprise Server (SLES) and SUSE Linux Enterprise Desktop (SLED). These two editions of SUSE Linux are designed for developing and managing enterprise-level IT infrastructure. As a server operating system, SLES can run on servers with platforms such as ×86, PowerPC, Itanium 2, and so on. SLES includes over 2000 proprietary application software packages from Microsoft, Oracle, SAP, and WebSphere. In addition, it includes over 1000 open source applications. SLES is a relatively stable operating system. It is usually upgraded to a new version every 2 years. The new version will be supported by SUSE for 7 years. Figure 1.16 displays the SUSE Linux Enterprise login interface.

As a desktop operating system, SLED is designed for enterprise use. Like SLES, it is relatively stable when compared with openSUSE. It also includes proprietary software such as the antivirus software McAffee. Both SLED and SLES include technical support from Novell and certification by hardware and software vendors. SUSE Linux Enterprise is often installed on servers sold by hardware vendors such as IBM, HP, Sun Microsystems, Dell, and SGI. These hardware vendors install, configure, and test SUSE Linux Enterprise before their computer systems are shipped to customers.

As for cloud computing, the SUSE Cloud package is an open source, enterprise cloud computing platform. The platform includes an administration server used for setting up the cloud. The administration server is also used for configuring and

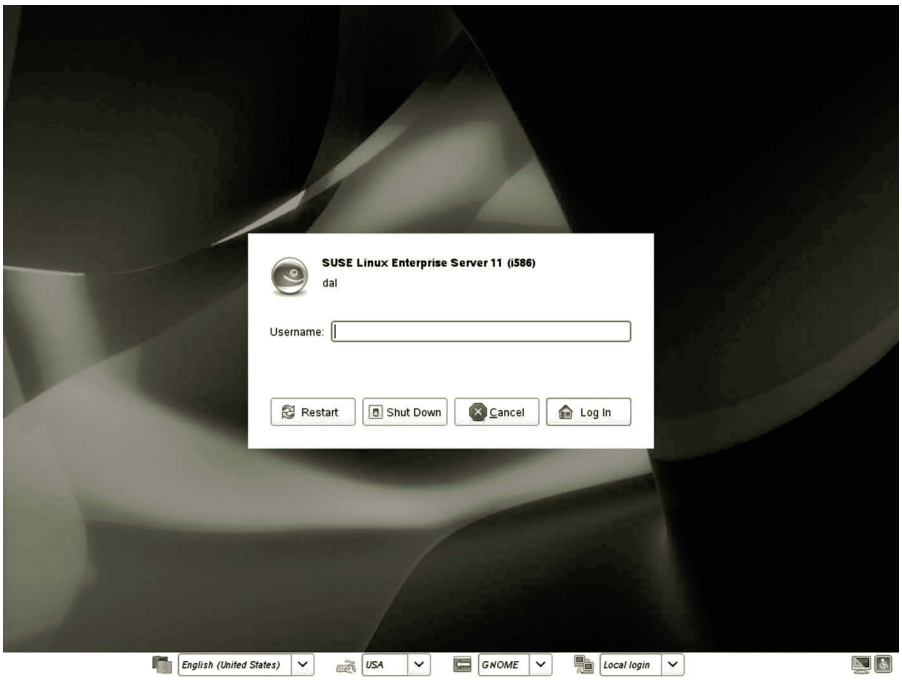

Figure 1.16 SUSE Linux enterprise server.

provisioning cloud control nodes and cloud compute or storage nodes. A control node automatically tracks the resource state of the cloud compute or storage nodes, identifies the available capacity within the cloud, and deploys workloads. The compute or storage nodes are physical servers that are either used to host virtual machines or to host storage devices.

SUSE Cloud is an OpenStack-based platform that supports multiple hypervisors such as Xen, KVM, QEMU, LXC, and Hyper-V. The support of Hyper-V enables enterprises to deploy their open source private clouds on the public cloud Microsoft Azure, or to be hosted by on-premises Windows Server machines. The collaboration with Hyper-V also facilitates the installation of compute nodes based on Hyper-V on the SUSE Cloud platform.

SUSE collaborates with the hardware vendor Dell to develop the enterprise-class private cloud infrastructure solution, which combines Dell's hardware and services with SUSE software. The Dell SUSE Cloud Solution gets support from both Dell and SUSE worldwide support organizations. It simplifies the IT infrastructure development process, enables an enterprise to set up clouds on an existing data center quickly, and reduces tasks needed to add capacity as the need continues to grow.

Ubuntu Linux: Ubuntu is also a major Linux distribution sponsored by Canonical Ltd., a private company from South Africa. The Ubuntu Linux operating system is free and consists of all open source products. It is updated every 6 months. It also provides a long-term support version of the operating system, which upgrades every 3 years.

The Ubuntu Linux operating system has three editions, the server edition, the desktop edition, and the mobile edition. The server edition of Ubuntu Linux includes the LAMP (Linux, Apache, MySQL, and PHP) package. The installation of Ubuntu is quick and simple. The LAMP package is installed automatically. The Ubuntu desktop edition is specially designed to be easy-to-use. It includes many utilities for handling multimedia content such as photo editing and media editing tools. Like the Windows operating system, it includes a large number of GUI tools for searching, calendaring, Web form spell checking, phishing detection, and system administration. It also includes e-mail and the latest Web browsing technology, the office suite OpenOffice.org, the instant messenger Pidgin, and the image editor GIMP. The mobile edition is designed to run multimedia content on mobile devices. The mobile edition operating system can run with small memory and storage space. It also delivers fast boot and resume time. Figure 1.17 illustrates the GUI interface of Ubuntu Server.

Ubuntu Cloud is designed to allow companies to provide fast and efficient cloud services. With Ubuntu Cloud, a pool of scalable compute and storage IT resources can be made available for on-demand access. Ubuntu is the reference operating system for OpenStack. That is, Ubuntu is the base operating system used by the developers of OpenStack. OpenStack is a free and open-source software platform on which cloud services can be built, tested, and deployed. As the reference operating system

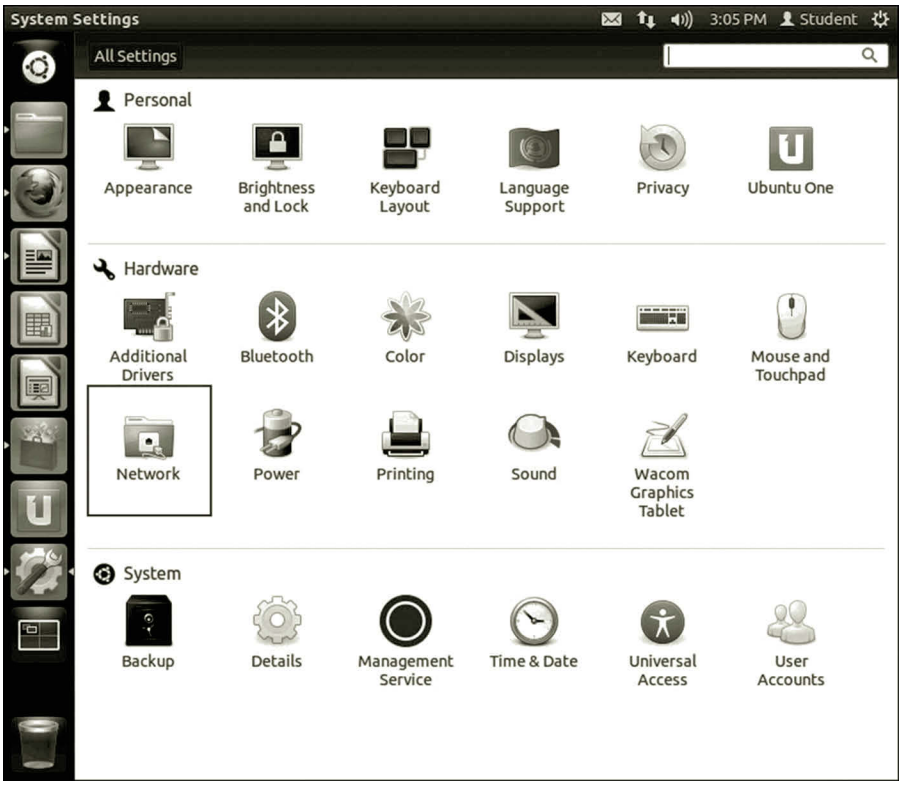

Figure 1.17 Ubuntu Server.

for OpenStack, Ubuntu cuts down the complexity in developing an OpenStack cloud, which stops the lock-in to a specific cloud vendor.

Ubuntu is broadly supported by public clouds such as Amazon Web Services, Rackspace Cloud, HP Public Cloud, and Microsoft Azure, and so on. It can be used either as an underlying infrastructure or as a guest operating system on virtual machines hosted in a cloud. Ubuntu works with the leading public cloud infrastructures to enhance performance, handle updates, and achieve compliance and reliability on the public clouds. Ubuntu has been creating tools such as cloud-init to ease the process of bringing up new instances on a public cloud.

Ubuntu can also be used to create cloud services that are deployed on private IT infrastructures. With Ubuntu Cloud Infrastructure, a company can deliver all its compute, network, and storage resources as cloud service. Ubuntu provides necessary tools for developing a private Infrastructure as a Service (IaaS) cloud service on an existing private IT infrastructure. With these tools, one can quickly set up scalable storage and integrate the features into a cloud service. The private cloud created with Ubuntu is compliant with some of the public cloud standards including Amazon EC2 and Rackspace APIs. Therefore, it has the freedom to migrate the cloud services between the public cloud and the private cloud.

With Ubuntu Cloud Infrastructure, a private cloud can be extended into the public cloud to form a hybrid cloud. When Ubuntu is on both the private cloud and the public cloud, Ubuntu Cloud Infrastructure enables users to burst workloads from their private clouds to the major public clouds, or vice versa. Ubuntu provides a service orchestration tool called Juju to accomplish tasks such as automated arrangement, coordination, and management of virtual machines, middleware, and services. With Juju, one can define the Software as a Service (SaaS) and deploy it to a cloud, either a private cloud or a public cloud or both. Juju is so designed that it is cloud provider independent; therefore, it can deploy services to different cloud providers.

Earlier, we have discussed several operating systems that are capable of cloud computing and network virtualization. There are many other operating systems that may also be capable of cloud development and network virtualization. The selection of an operating system for networking depends on the tasks to be accomplished, the flexibility, the scalability, ease-of-use, and the cost. For most networking-related tasks, the operating system mentioned in this section should be able to do the job. Next, we will focus on network architecture which is the logic model used by the networking capable operating systems.

1.4 Network Architecture

This section will discuss network architecture and the tasks to be accomplished during a networking process. It will introduce the major components in a network system. We will take a look at how network functionalities are designed and

implemented in an operating system. Network management tools will also be introduced in this section.

A network can be as small as two computers connected by a copper wire or as large as the Internet that links millions of computers and network devices. For computers to be able to communicate with each other through physical media, as an example, the Linux operating system provides four major components: application, service, protocol, and adapter.

A network system can be represented by a network model, also called network architecture, which is often presented as a layer system. The network architecture provides an overview of a network system by including the major components for a network and the interfaces between components. To be able to handle data transmission tasks on various networks, the network components in an operating system are built according to the network architecture. An operating system controls data transmission from the application software to the physical wire, which connects the computers. Figure 1.18 illustrates the network components in an operating system.

As a service interface between users and the operating system kernel, the application software manages data communication between the users and the operating system. It takes the users' requests for file transfer, database query, and message exchange, and then submits the requests to the operating system. Once the requests are submitted to the operating system, the network management component will collect the data and identify the network protocols to be used for data communication.

A network protocol serves as a service interface between the application software and the network driver. There are hundreds of protocols supported by an operating system.

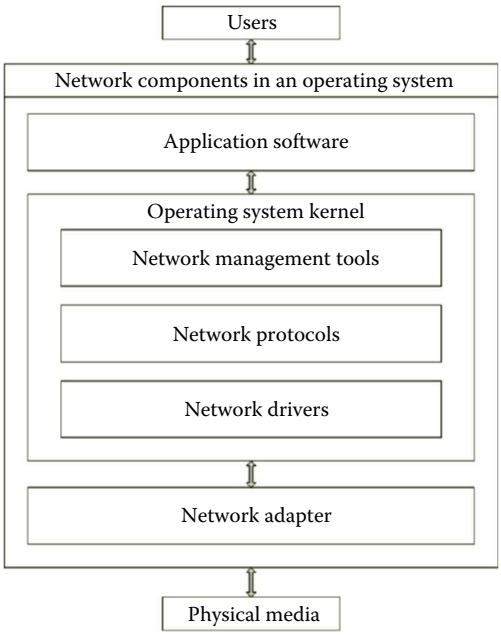

Figure 1.18 Network components.

The network protocols perform tasks such as establishing the communication ports, detecting data transmission errors, data formatting, controlling the data transmission process, resolving network addresses, maintaining network traffic, locating the destination computer and setting up the route to the destination, defining how the data are sent and received, and so on. For security, some of the protocols are used for data encryption and authentication.

A network driver serves as an interface between the software and the hardware. The driver enables the operating system to communicate with the NIC, which connects the physical data transmission media. Drivers can be used to handle I/O interrupts during a data transmission process. In addition to interacting with the operating system, drivers also interact with buffers, network protocols, and network adapters.

A network adapter is a piece of hardware that connects the physical media to a computer on the network. During data transmission, a network adapter communicates with its peer network adapter installed on another computer. Network adapters may be a wired Ethernet NIC, or it can also be a wireless network device. A network adapter serves as an interface between the operating system kernel and the physical media. Electrical signals are framed in a network adapter. The frame specifies the transmission rate and the shape and strength of the binary signals. By using a network adapter, the binary electric signals are sent to or received from physical transmission media. The network adapter is able to locate its peer network adapter through the hardware address. Once the data arrive at the receiving network adapter, the receiving network adapter informs the operating system to get ready to process the incoming binary signals.

The physical medium links two network hosts such as computers or network devices. The electric signals representing the binary bits are transmitted through the physical media such as copper cables, fiber glass, radio waves, etc. The physical media may also include network devices used to pass the electric signals to a particular destination.

A network can be presented in two different network architectures. The first one is the Open Systems Interconnection (OSI) architecture developed by the International Organization for Standardization (ISO). OSI is a network architecture that defines the communication process between two computers. OSI categorizes the entire communication process into seven layers as shown in Figure 1.19. The second one is the Internet architecture. This architecture is built around the Transmission Control Protocol and Internet Protocol (TCP/IP). Therefore, the Internet architecture is also called the TCP/IP architecture, which includes four layers as shown in Figure 1.20.

In the OSI network architecture, the top layer is the application. The protocols in the application layer are provided by application software. The application layer protocols handle requests from users for file transfer, database query, message exchange, and so on. The protocols in the application layer communicate with the protocols in the presentation layer.

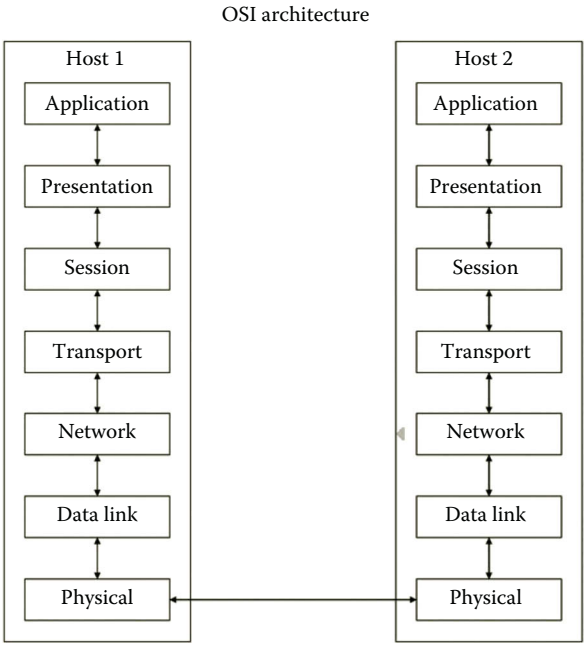

Figure 1.19 OSI architecture diagram.

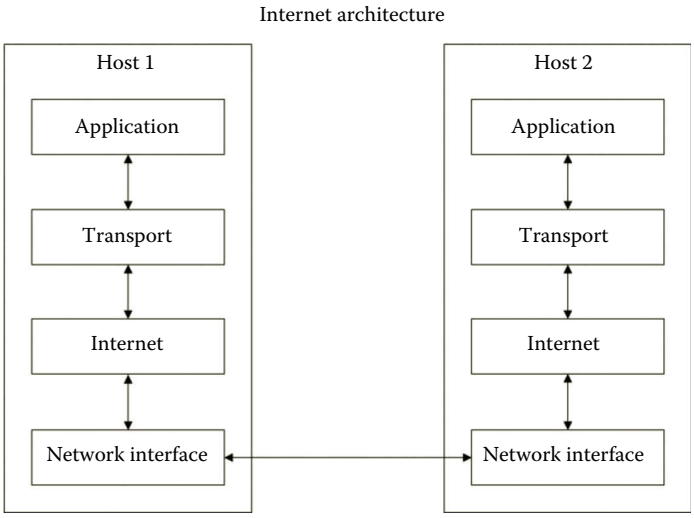

Figure 1.20 Internet architecture diagram.

The protocols in the presentation layer format the data so that the data meet certain transmission requirements. The tasks to be handled by this layer can be data compression, data encryption, video streaming, data format conversion, and so forth.

The protocols in the session layer establish the communication session between two applications such as a conference call or remote connection to a database server. These protocols can be used to start, manage, and terminate a communication session.

They also perform tasks such as requesting and responding during a data transmission process between applications.

The protocols in the transport layer establish and manage the connection between two hosts on the network. This layer handles tasks such as detecting transmission errors; controlling network flow; transporting data; and establishing, managing and terminating connections.

The protocols in the network layer can identify the destination network and establish the data transmission route to a destination host. This is the layer that works with routers and network logical address configuration tools. The routing protocols are able to calculate the shortest path to the destination host and update the routing table periodically.

The data link layer is often implemented in the network card driver. This layer defines the beginning and ending of a binary data transmission frame. It also defines data types. During the process of sending and receiving binary code, this layer also detects and corrects errors in the binary code.

The physical layer transmits electrical binary signals over the physical media that link two hosts. It also defines the shape of electronic signals. When an electrical binary signal arrives from the physical media, the physical layer passes the binary signal up to the data link layer.

Another commonly used network architecture, the Internet architecture, is designed for modeling data exchange through the Internet. The application layer in the Internet architecture includes the application layer, the presentation layer, and the session layer of the OSI architecture. The transport layer of the Internet architecture is equivalent to the transport layer of the OSI architecture. The Internet layer of the Internet architecture is similar to the network layer of the OSI architecture. The network interface layer of the Internet architecture includes data link layer and the physical layer of the OSI architecture. Figure 1.20 shows the diagram of the Internet (TCP/IP) architecture.

The OSI network architecture is the standard adopted by the U.S. government. Therefore, the hardware and software companies working for the U.S. government need to follow the OSI network architecture. On the other hand, many private companies have been traditionally using the TCP/IP architecture, which matches the network architecture used by the Berkeley UNIX operating system. The Microsoft Windows Server operating system uses the TCP/IP architecture to describe its network system.

Both Linux and Windows network systems can be implemented by closely following the TCP/IP network architecture. Comparing the network components in Figure 1.18 with the TCP/IP network architecture, one can see that the application layer in the TCP/IP network architecture matches the component of application software in Figure 1.18. Application software often carries out tasks such as data compression, data encryption, video streaming, and data format conversion. The application software component also includes network management tools. These tools are used

to handle tasks related to session establishment, maintenance, and termination. The operating system kernel manages protocols such as TCP and IP around which the TCP/IP architecture is constructed. The combination of network drivers, network adapters, and physical media in Figure 1.18 matches the network interface layer in the TCP/IP architecture.

Earlier, we briefly discussed the network architecture, which shows how data communication is carried out between applications over a network. The network architecture models the data communication process. In later chapters, more detailed discussion about each layer of the network architecture will be given.

Activity 1.1: Preparing for Hands-On Activities

To carry out the lab activities covered in this book, we need to install the operating system and virtualization software. We also need to prepare the cloud environment for the hands-on practice. As for the public cloud provider, we will choose Microsoft Windows Azure since it has a free trial period, academic support, and it supports both Linux and Windows operating systems. To develop virtual networks, we can use Microsoft Azure, or use Hyper-V if Windows Server 2012 or Windows 8, or use VMware Workstation, which can work with various desktop operating systems. The following tasks will be performed on Microsoft Azure.

Getting Started with Microsoft Azure

To be able to use Microsoft Azure, you need to first create a free account. You also need to create a storage account and virtual network on Microsoft Azure. Then, you will create a virtual machine on Microsoft Azure as shown in the following steps:

1. Assume that you have established the free trial account or academic account. First, you need to go to the following Web site to log on to Microsoft Azure (Microsoft Azure, The cloud for modern business, May, 2015): http://azure.microsoft.com/en-us/.
2. Log on to your Microsoft Azure Management Portal with your user name and password.
3. In the lower left-hand corner of your screen, click **New**. Then, click **NETWORK SERVICES**, and then click **VIRTUAL NETWORK**. Click **CUSTOM CREATE** as shown in Figure 1.21.
4. On the Virtual Network Details page, enter the information about the name and location as shown in Figure 1.22, and then click the **Next** arrow at the lower right corner.
5. On the DNS Server and VPN Connectivity page, leave DNS server blank as shown in Figure 1.23. Then, click the **next arrow** on the lower right.

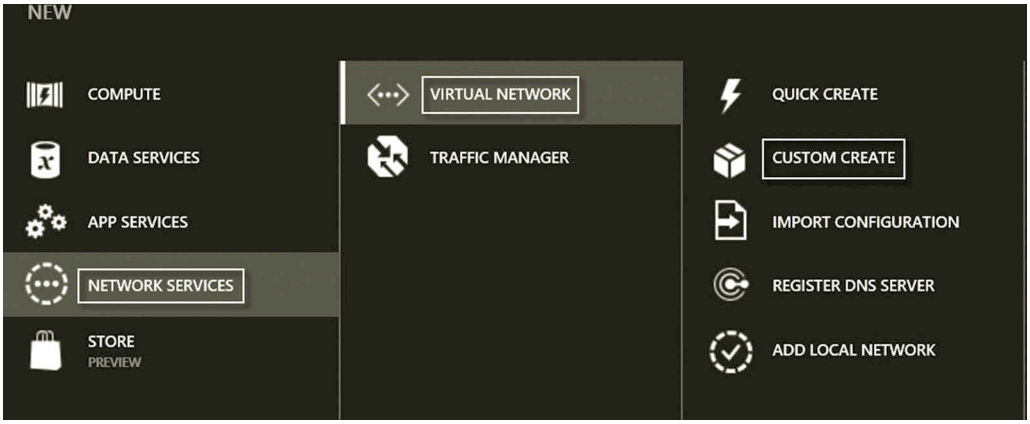

Figure 1.21 Creating new virtual network.

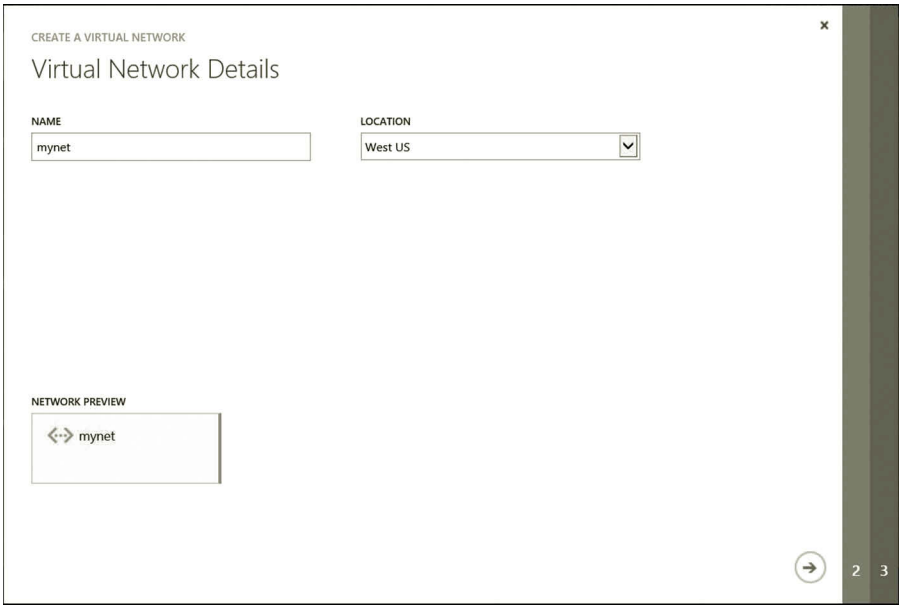

Figure 1.22 Virtual network configuration.

6. On the Virtual Network Address Spaces page, click **add subnet** button to create a subnet as shown in Figure 1.24. Then, click the **check mark** on the lower right.
7. In addition to the virtual network, you may create a storage account that provides the namespace for data storage. At the lower left-hand corner of the screen, click **New**.
8. In the navigation pane, click **DATA SERVICES, STORAGE**, and then **QUICK CREATE**. Specify the URL and Affinity group as shown in Figure 1.25. Then, click the **CREATE STORAGE ACCOUNT** check mark on the lower right.

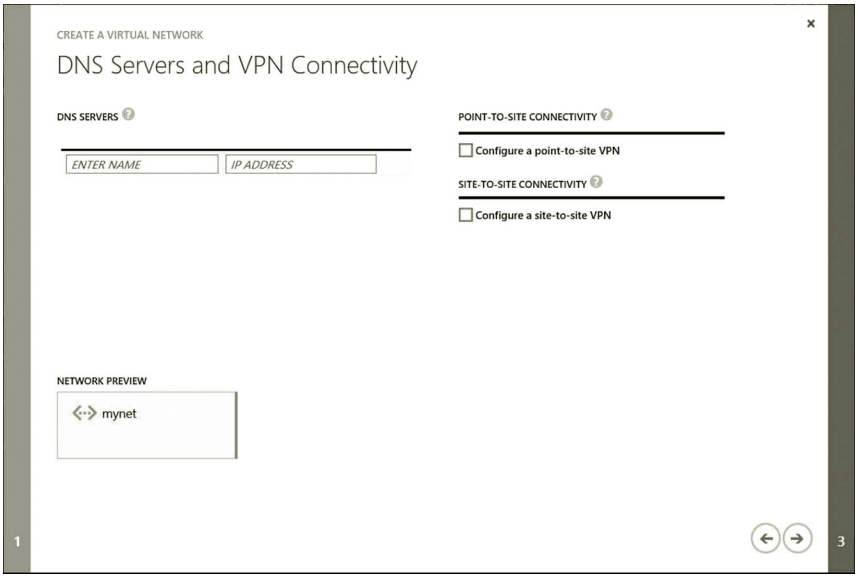

Figure 1.23 DNS server configuration.

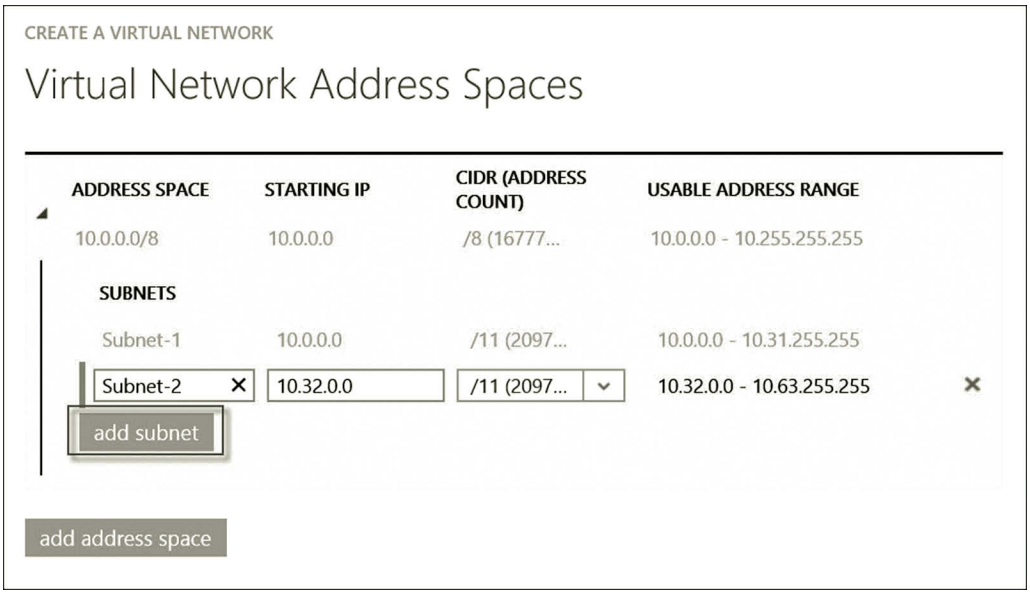

Figure 1.24 Adding virtual subnet.

9. Your next step is to create a virtual machine installed with Windows Server 2012. To do so, at the lower left-hand corner of your screen, click **New**. Then, click **COMPUTE, VIRTUAL MACHINE, FROM GALLERY** as shown in Figure 1.26.
10. On the Select virtual machine operating system page, click **Windows Server 2012 R2 Datacenter** (Figure 1.27) and then click the **Next** arrow on the lower right.

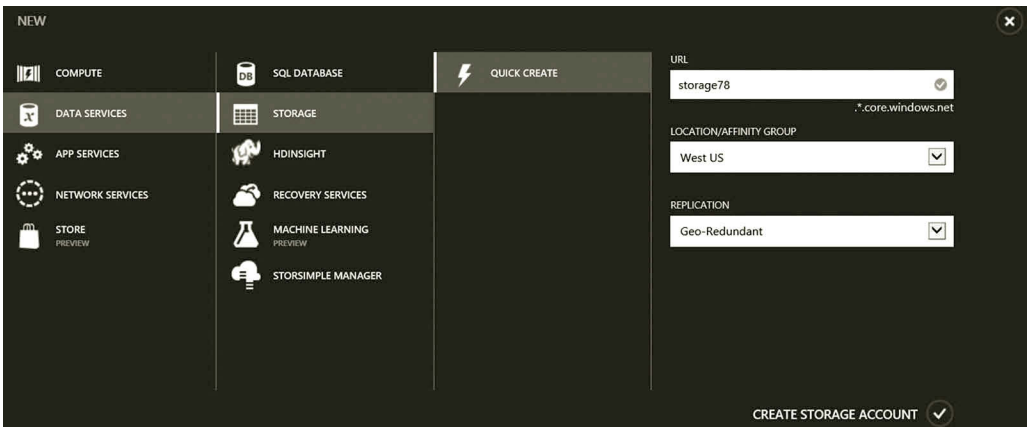

Figure 1.25 Creating storage account.

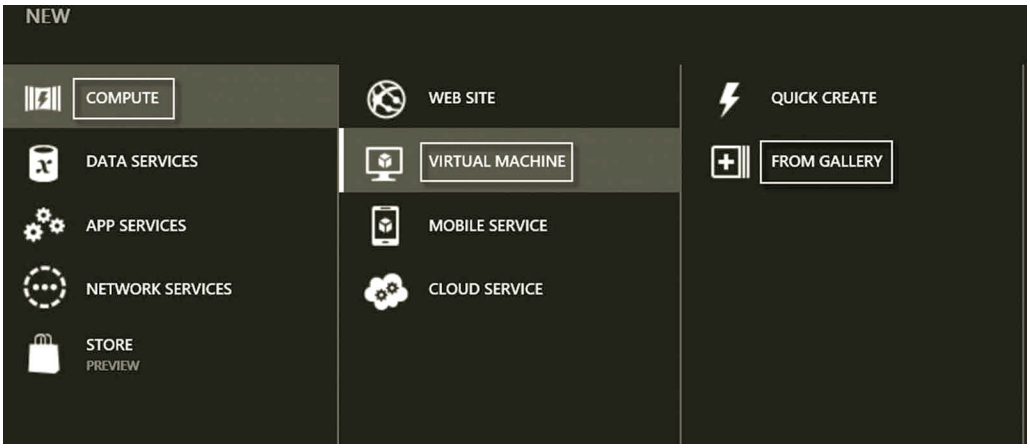

Figure 1.26 Selecting virtual machine.

11. On the Virtual machine configuration page, enter your virtual machine name **servera**, the user **student** and the password, confirm the password, and select the size of your virtual machine as shown in Figure 1.28. The A1 size is adequate for the hands-on activities in this book. Then, click the **Next** arrow.
12. On the Virtual machine configuration page, specify the virtual machine as shown in Figure 1.29.
13. Depending on the needs, you may add a few more communication protocols as shown in Figure 1.30. Then, click the **Next** arrow.
14. On the Virtual machine configuration page, click the **check mark** at the lower right corner to create the virtual machine.
15. After the virtual machine is created, click the **CONNECT** link at the bottom of your screen. Select the option **Use another account**. Enter the user name as **student** and the password for the user and then click **OK** to log on to the virtual machine (Figure 1.31).

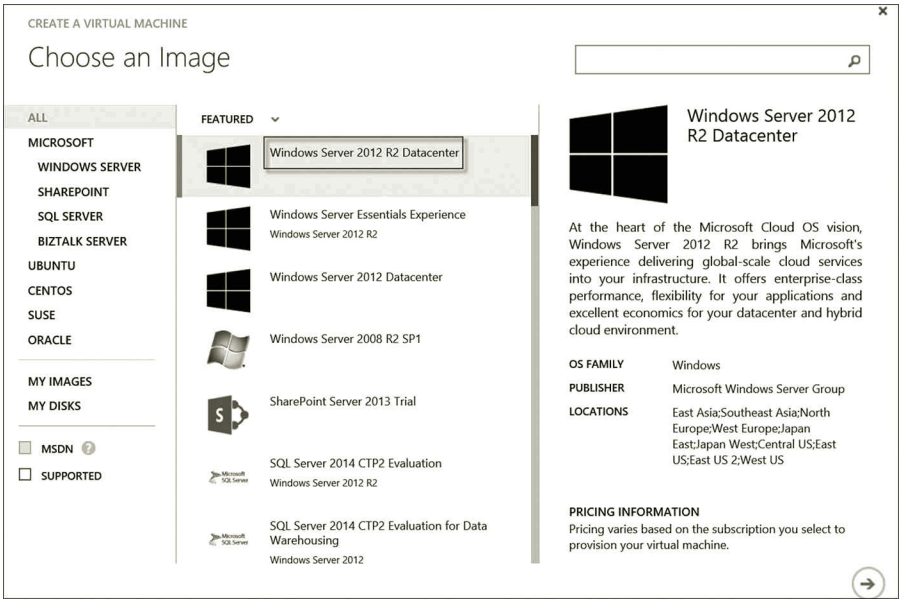

Figure 1.27 Selecting operating system.

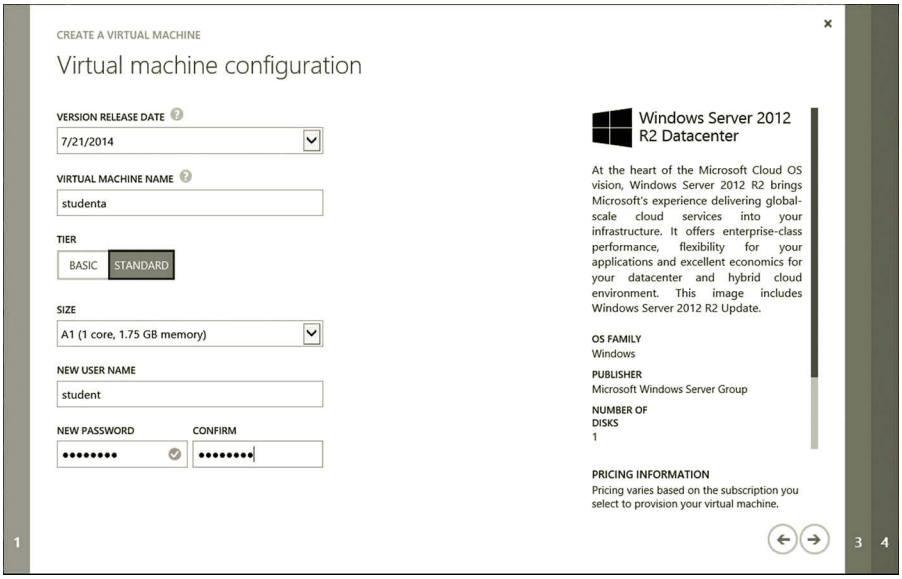

Figure 1.28 Configuring virtual machine.

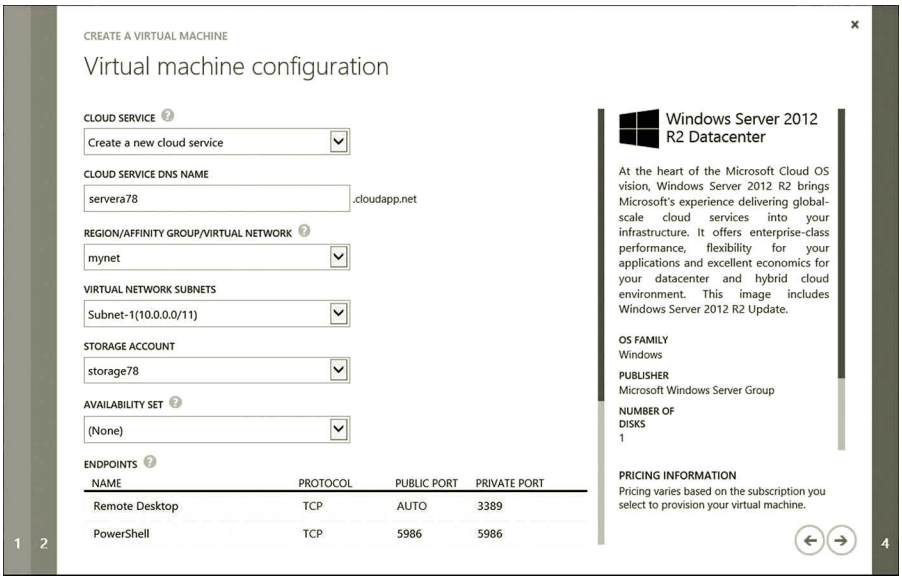

Figure 1.29 Virtual machine configuration.

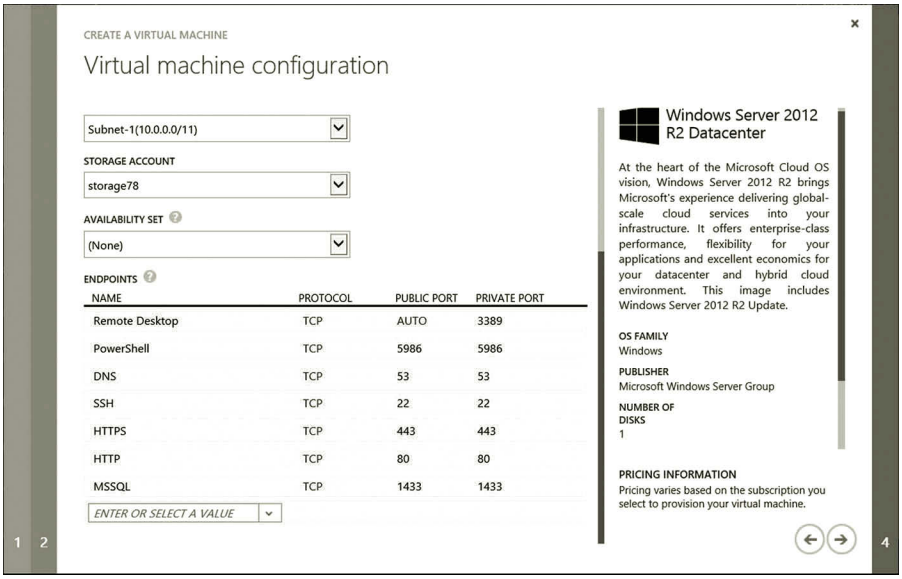

Figure 1.30 Adding network protocols.

16. After logging on to the virtual machine, you should be able to see Server Manager as shown in Figure 1.32.
17. For networking, you need to create another virtual machine. Assume that you are still logged on to the Microsoft Azure Management Portal. Click **NEW** at the bottom of the screen. Click **FROM GALLERY** and select **Windows Server 2012 R2 Datacenter**. Enter the virtual machine **serverb** and user

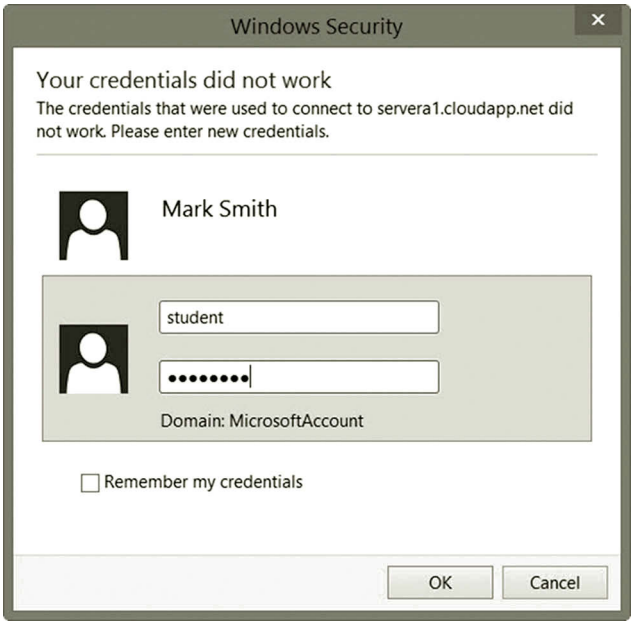

Figure 1.31 Remotely logging on to virtual machine.

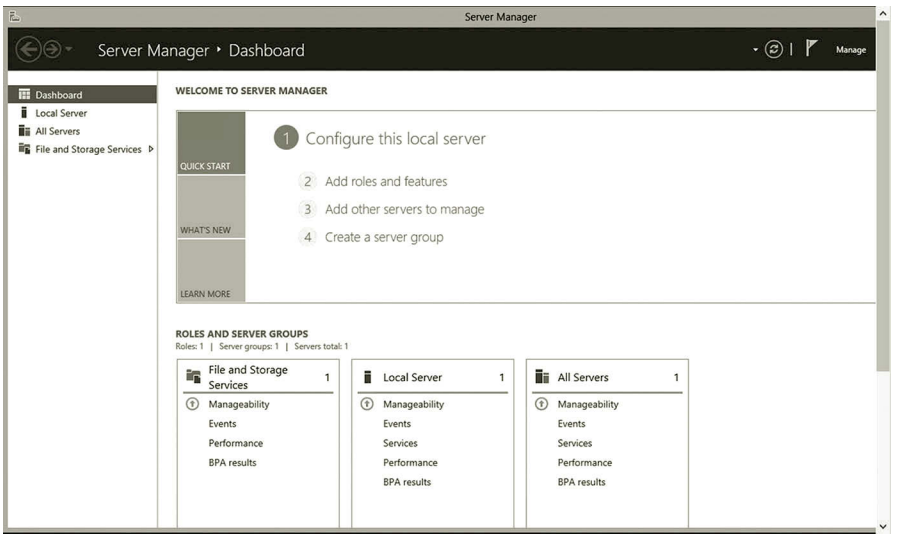

Figure 1.32 Server Manager.

name **student**. Enter your password as shown in Figure 1.33 and click the **Next arrow**.

18. On the Virtual Machine Configuration page, specify the virtual machine as shown in Figure 1.34. Similarly, add some network protocols as shown in Figures 1.30. Then, click the **Next arrow**.
19. On the Virtual machine option page, click the **check mark** at the lower right corner to create the virtual machine.

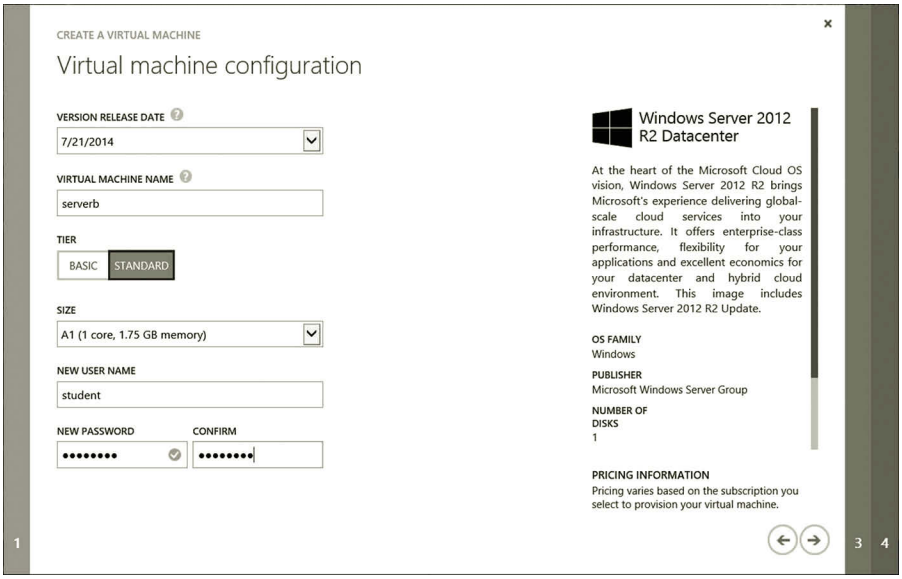

Figure 1.33 Configuring virtual machine server.

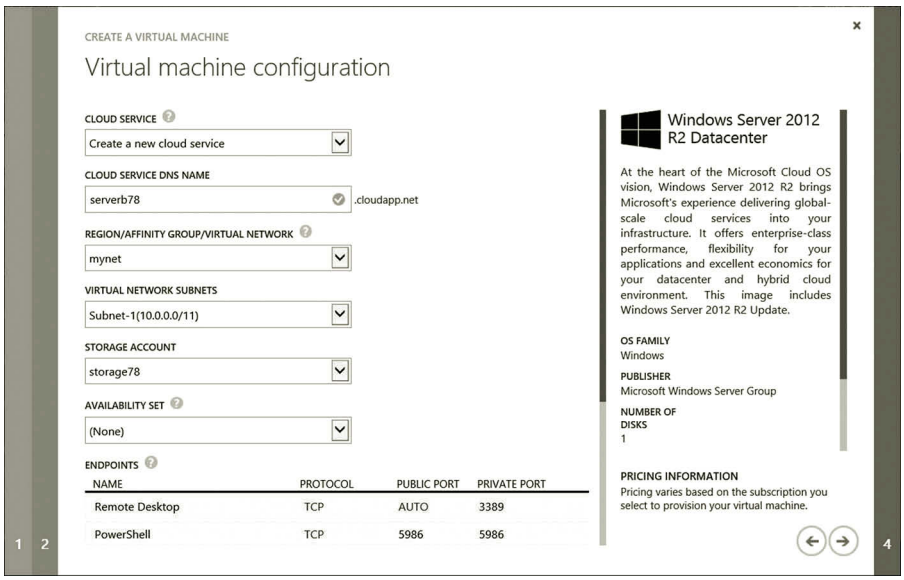

Figure 1.34 Configuring virtual machine.

20. Due to the spending limit on Azure, make sure to shutdown the virtual machines whenever you are not using them. In the Microsoft Azure Management Portal, you should shutdown both servera and serverb before exiting the Microsoft Azure Management Portal.

So far, you have created two virtual machines on Microsoft Azure. Later, you will perform networking on these two virtual machines.

1.5 Summary

This chapter introduces networking. It first provides an overview of networks. Then, it discusses network operating systems. It also provides information on how the operating systems handle virtualization and support cloud computing. This chapter reviews network architectures. Two abstract network architectures, the OSI network architecture and Internet network architecture, are introduced. The chapter then describes the role of operating systems in developing network systems.

To prepare the computing environment for the hands-on practice in later chapters, the activity of this chapter walked the reader through a process of creating virtual machines and installing a guest operating system on the virtual machines. Once the virtual machines are created, we are ready to discover how these virtual machines are used to accomplish various networking tasks.

Review Questions

1. What are hosts?
2. What is LAN?
3. What is WAN?
4. Describe the Internet.
5. What is POP?
6. What is NAP?
7. Which operating system mentioned in this chapter is designed for the cloud platform?
8. Which operating system mentioned in this chapter provides the virtualization tool, Hyper-V?
9. What do you do with Hyper-V?
10. What are cloud services provided by Microsoft Azure?
11. What is vSphere?
12. Name five hypervisors supported by OpenStack.
13. Describe the application layer in the OSI network architecture.
14. What tasks can be handled by the transport layer in the OSI network architecture?
15. What tasks can be handled by the network layer in the OSI network architecture?
16. Which layers in the OSI network architecture are included in the application layer of the TCP/IP network architecture?
17. Which layers in the OSI network architecture are included in the network interface layer of the TCP/IP network architecture?
18. What tasks can be accomplished by the TCP in the transport layer?
19. IP is in which layer of the TCP/IP network architecture?
20. Network drivers are in which layer of the TCP/IP network architecture?

2
Network Protocols

Objectives

- Learn about commonly used protocols in the Internet architecture.
- Understand the relationships among the protocols.
- Explore network tools.

2.1 Introduction

As described in Chapter 1, a networking process involves various protocols, which are used as communication languages. In a network, the data transfer is accomplished by multiple protocols; each protocol carries out a specific task. Various protocols will be used in later chapters. To enhance the understanding of how network devices communicate with each other, it is necessary to understand how the protocols are designed, what the responsibilities of these protocols are, and how these protocols are related. In this chapter, the commonly used protocols in cloud computing will be discussed in detail. Due to the fact that the network architecture used by Windows and UNIX-like operating systems is the Internet architecture (or Transmission Control Protocol/Internet Protocol [TCP/IP] architecture), the protocols introduced in this chapter will be grouped based on the TCP/IP architecture.

There are four layers in the TCP/IP network architecture: application layer, transport layer, Internet layer, and network interface layer. Each layer in the TCP/IP architecture may include dozens or even hundreds of protocols. In this chapter, a few commonly used protocols in each layer will be introduced. In the hands-on practice, some of the networking tools will be used to illustrate the protocols used in cloud computing.

2.2 Application Layer Protocols

Protocols in the application layer handle the communication of application software. They can carry out tasks such as responding to requests from web browsers, making conference calls, or connecting to remote database servers. Some of the protocols can be used to set up user authentication. Others can be used to set up agreements on data resources, data integrity, and data syntax rules. The protocols included in this layer can be used to establish, terminate, and manage sessions that handle requests and responses between hosts. In the application layer of the TCP/IP architecture, the

protocols also perform tasks such as data compression, data encryption, video streaming, and data format conversion.

There are hundreds of protocols included in this layer. Some of the well-known application protocols are Hypertext Transfer Protocol (HTTP), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), Simple Mail Transfer Protocol (SMTP), Post Office Protocol Version 3 (POP3), Internet Message Access Protocol (IMAP), Telecommunication Network (Telnet), Secure Shell (SSH), Lightweight Directory Access Protocol (LDAP), Secure Sockets Layer (SSL), Secure Shell (SSH), Secure Socket Tunneling Protocol (SSTP), and Simple Network Management Protocol (SNMP).

An application protocol communicates through a dedicated port number. For example, HTTP communicates through the port 80, DNS communicates through the port 53, and DHCP communicates through the port 67.

The following gives general descriptions of the commonly used protocols in the application layer. In later chapters, more specific application protocols will be introduced.

Hypertext Transfer Protocol (HTTP): The protocol HTTP is used for transferring data between web browsers and web servers. HTTP can carry data in various formats such as text, graphic images, sound, video, and other multimedia files. To manage data transferring, HTTP provides a set of commands. With these commands, HTTP handles how a web browser requests data stored on a web server and how the web server responds to the request from the web browser. HTTP also handles how a web browser uploads files to a web server and how the web server executes scripts to support a dynamic web page. For example, suppose that a user enters a URL in a web browser. After the user presses the Enter key, HTTP carries the GET command to the web server through Port 80. By executing the GET command, the web server finds the requested web page. Then, HTTP carries the web page back to the web browser. If the user uploads a file to the web server, HTTP sends the web page and the PUT command to the web server. By executing the PUT command, the web server stores the web page in a proper place. In addition to telling the web server how to respond to a request from a client, HTTP can instruct the web server to place requested data in an application. It can also instruct the web server to run scripts.

Domain Name System (DNS): DNS is a protocol used to find the corresponding IP address for a given host name, or vice versa. It communicates with UDP through Port 53. In a network, each host needs to have an IP address for data communication. However, it is not easy for a user to remember the host's IP address. The host in a network needs a user-friendly name such as www.windowsazure.com. When accessing a web server, the data communication process needs the web server's IP address to contact the web server. DNS works like finding a phone number in a telephone directory. Based on the URL entered by the user, DNS finds the corresponding IP address in a

DNS server. Then, it returns the IP address to the host with the web browser installed for connecting to the web server.

DNS is implemented with two components, the DNS client and DNS server. The DNS client is the host that requests the IP address. The DNS server stores a database that contains pairs of host names and corresponding IP addresses. As you can imagine, for all the hosts on the Internet, the DNS database can be a really large one. Therefore, the database has to be distributed to many DNS servers; each of them stores only part of the database.

Dynamic Host Configuration Protocol (DHCP): As described earlier, each host in a network needs to have a unique IP address. It can be a tedious task to manually assign each host an IP address. DHCP is a protocol that can be used to automatically assign an IP address and other network parameters to a computer or a network device. In addition to assigning IP addresses, DHCP can also be used to deliver network parameters such as the subnet mask, the IP address of the router used as the default gateway, and the DNS server, and so on. Later chapters will provide more information about these parameters. DHCP greatly reduces the amount of configuration time spent on these network hosts such as computers and network devices.

Here is an example to illustrate how DHCP works. If a computer is configured to automatically receive an IP address and other network parameters from a DHCP server, as the computer is booted up, it sends out a broadcast message to look for the DHCP server on a network. Once the DHCP server receives the request broadcasted by the client computer, it offers an IP address and a set of network parameters to the client computer. When the client computer receives the offer from the DHCP server, it accepts the offer by sending a response to the DHCP server. If the DHCP client receives multiple offers from multiple DHCP servers, the client computer will inform the DHCP servers to let them know which offer has been accepted. Then, the chosen DHCP server sends an acknowledgment to the client computer and informs the client computer that the IP address and other network parameters are ready for data communication.

Simple Mail Transfer Protocol (SMTP): Sending and receiving e-mail message need different protocols. SMTP is a protocol used to send messages to e-mail servers. It can also be used to deliver e-mail messages between two e-mail servers. However, SMTP is not used to receive messages from e-mail servers for reading due to its limited ability on user authentication and queuing messages at the receiving end.

As a simple text-based protocol, SMTP has about 10 commands in order to reduce bandwidth and improve performance. SMTP has no authentication measure to verify who is sending the message. Therefore, it cannot tell if the message is sent by a real sender or a hacker. SMTP communicates through Port 25. To improve security and performance, the Enhanced Simple Mail Transfer Protocol (ESMTP) has been developed to enforce security. ESMTP adds many features for authentication, reduces bandwidth, and does error recovery.

Post Office Protocol Version 3 (POP3): POP3 is one of the protocols used for receiving e-mail messages. It can check the mail box on an e-mail server and download the e-mails from the server. It has the user authentication mechanism so that only the qualified user can receive the e-mails that belong to that user. POP3 is included in most of the e-mail client software and web browsers. The disadvantage of POP3 is that it only supports a single inbox, so the user cannot place related e-mails into different folders. POP3 communicates through Port 110.

Internet Message Access Protocol (IMAP): IMAP is another protocol used for receiving e-mail messages. Unlike POP3, IMAP supports multiple folders on the server side. These folders can be used for organizing e-mail messages. IMAP allows users to select which messages to download. It uses Port 143 to download e-mail messages from an e-mail server.

Secure Sockets Layer (SSL): SSL is a security protocol used for protecting sensitive information transferred between a web server and a web browser. When a web browser connects to an SSL server hosted by a web server, it requests the server to provide a digital Certificate of Authority (CA). The CA is usually validated by a third party authority agency such as VeriSign. This CA is used to authenticate the SSL server to make sure that the server is not a hacker. The web browser also checks if the name of the server matches the domain name provided by the CA and if the digital signature is valid. When a web browser uses the URL starting with https, it means that the SSL protocol is used to connect to the SSL server. Sensitive information will be protected during data communication. For web applications, SSL runs on the port number 443. However, for other applications, SSL runs on different ports. Also, the network administrator can choose to run SSL on a different port number.

Secure Shell (SSH): SSH is another protocol used to secure the access of a remote network host. With SSH, a user can securely log on to a remote computer to carry out tasks such as executing commands and transferring files. With the built-in authentication and encryption mechanism, SSH can protect the network from attacks such as IP spoofing or IP source routing. The authentication mechanism only allows the connection from trusted hosts. The encryption mechanism encrypts SSH commands and passwords for confidentiality. During transmission, SSH establishes a secure channel between two hosts on the network. By default, SSH uses the port 22 for information exchange.

Secure Socket Tunneling Protocol (SSTP): SSTP is a protocol designed to allow two application programs to engage in bidirectional, asynchronous communication. For example, it can be used to establish a virtual private network (VPN), which is a private network constructed over the public Internet. Even though the data communication is carried out in the public network, the communication between two hosts in the private network is protected by using encryption and authentication mechanisms. SSTP depends on SSL to provide the security mechanism. SSTP uses TCP Port 443 for relaying SSTP traffic. In later chapters, SSTP is used to connect a host on a

home network to a virtual network on a cloud. The advantage of SSTP is that it is not blocked by the firewall, so the virtual machine on the cloud can communicate with the hosts behind the router in your home network.

Lightweight Directory Access Protocol (LDAP): A directory service is used to store and organize the authentication information about network resources such as users, groups, computers, printers, files, domains, and organization units. LDAP is a protocol used to manage the directory service. With LDAP, the network administrator can perform tasks such as implementing centralized user authentication, arranging users according to an organization's structure, and configuring group policies. LDAP is often used by other services, such as web service and e-mail service for authentication.

Simple Network Management Protocol (SNMP): SNMP is a protocol for network management. It can be used to improve network performance, detect and correct network problems, and monitor network activities. The commands provided by SNMP are used to perform management tasks such as obtaining information from network devices and controlling the behavior of network devices. To accomplish the management tasks, SNMP needs information about the network devices and software that is stored in a management information base (MIB). In the MIB, the names of network objects and the information about their locations are stored on a tree structure and are coded in the Abstract Syntax Notation One (ASN.1) language. SNMP provides the security measures called SNMP Community Strings to protect the data being transmitted.

Earlier, a few commonly used application protocols were introduced. More application protocols will be introduced in later chapters. The list of application protocols introduced in this book is far from complete. There are about 100 known application protocols available. Also, there is no consistent definition on which protocol should be qualified as an application layer protocol.

2.3 Transport Layer Protocols

Protocols in the transport layer transfer data from one application to another. To prepare data transferring, protocols in the transport layer break the data into small units called packets. The transport layer protocols also handle tasks such as data transmission error checking; network flow control; and establishing, managing, and terminating a connection between hosts. The transport protocols process requests from the application layer protocols and issue the requests to the protocols in the Internet layer. While communicating with the protocols in the application layer, the transport layer protocols have the ability to identify the ports in the destination hosts. In such a way, the packets can be delivered to the proper ports of the destinations. The two commonly used transport layer protocols are Transmission Control Protocol (TCP) and User Datagram Protocol (UDP).

2.3.1 Transmission Control Protocol

TCP is a well-known transport layer protocol. It controls and manages data communication between ports. The following TCP features make TCP a core protocol in the TCP/IP architecture:

- *Connection orientation*: Once TCP receives a connection request from an application layer protocol, it establishes a reliable connection between the hosts that have agreed to communicate. Before the data communication begins, this feature makes sure that the application layer ports on the hosts are properly linked.
- *Point-to-point communication*: TCP views ports as connection end points. Data communication takes place between two end points.
- *Complete reliability*: This feature guarantees no data missing during transmission.
- *Full duplex communication*: TCP allows simultaneous communication in both directions just like a 2-way street.
- *3-Way handshake connection*: To initiate and terminate a connection, TCP uses a 3-way handshake process, which guarantees that the connection is reliable and the termination is graceful.

The aforementioned features can be implemented by accomplishing the following tasks:

- TCP divides a data file to be transmitted into small units called packets.
- A reliable TCP connection is established by using the 3-way handshake process.
- The termination of a TCP connection is also done through the 3-way handshake process.
- The 3-way handshake is implemented with a three-packet process.
- During the transmission process, a window mechanism is used to control the packet transmission flow.
- Based on the network capacity, TCP determines the proper packet transmission rate to avoid network congestion.
- TCP tracks packets to make sure that all the packets arrive at the destination host.
- TCP keeps the transmitted packets in order so that the packets can be reassembled back to the original file.
- TCP creates checksum used for detecting any transmission error.
- TCP resends the packets that are lost or that have transmission errors detected during the transmission.
- TCP discards duplicated packets.

To see how TCP can accomplish the aforementioned tasks, read the next few paragraphs for detailed descriptions.

The reasons for TCP to break a data block to be transmitted over a network into small units are listed:

- It needs some time to coordinate the protocol and hardware involved in a data transmission process.
- When the network transmission media are shared by multiple computers, the use of packets allows these computers transfer data in turns.

Packets are formed by combining each small data unit with a header and a trailer. In a packet, the small data unit is called a payload. The header includes information about the data to be transferred. It also includes information about the network used to carry out the transmission. It general, the header may include the following:

- The header includes the source and destination information for delivering a packet to the destination host and for receiving response from the destination host.
- It contains a packet sequence number used as the packet identification.
- It contains a synchronization bit, which can be turned on and off to synchronize network transmission.
- It has a packet type indicator to identify the type of information to be carried by the packet.
- It also has the information about the packet length, which is the size of the packet.

In practice, the header of a protocol may include more or less information than the basic information listed earlier. As a complicated protocol, TCP has much more information in its header. The following is the diagram of a typical TCP header (Figure 2.1).

In the diagram, each row represents a unit of 32 binary bits transmitted through a network. The following briefly describes each field in the diagram:

- Source and Destination Ports: These two fields identify the end points of a TCP connection for delivering and receiving packets.
- Sequence Number: Assigned to the outgoing packet, this number is used for reordering packets and calculating the acknowledgment number(s).

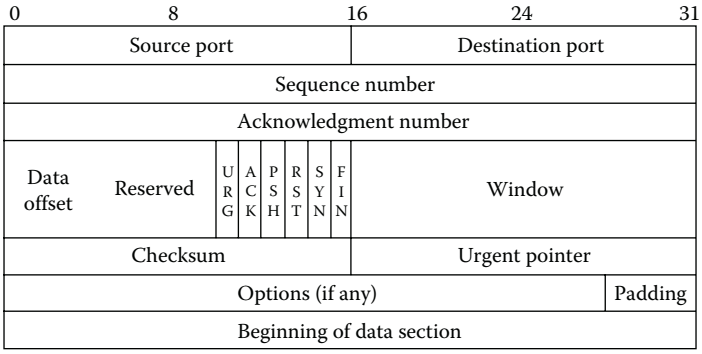

Figure 2.1 TCP header diagram.

- Acknowledgment Number: The acknowledgment number is used by the receiving host to inform the sending host that the transmitted data have been received successfully. This number is expected to be sent after the sequence number.
- Data Offset: This field specifies the number of 32-bit words in the header. The minimum size is five words. Each word has 32 bits, which are equal to 4 bytes. Therefore, the smallest TCP header contains 20 bytes of information.
- Reserved: This field is reserved for future use.
- Control Bits: This field has 6 information control bits described in the following list:
  - URG: This flag is used for validating the urgent pointer.
  - SYN: This flag synchronizes the sequence of numbers that is used to indicate the beginning a 3-way handshake connection process.
  - ACK: This flag is a signal to acknowledge the receipt of data. It can be used for establishing a 3-way handshake connection.
  - PSH: This flag indicates that the data must be pushed out immediately.
  - RST: This is the reset flag.
  - FIN: This flag means that there are no more data from the sender.
- Window: This field specifies the size of the receiving window, which limits the sender to send up to n bytes of data before waiting for the acknowledgment from the receiver. The size of the receiving window is determined by the buffer space available for the incoming data.
- Checksum: Checksum is used to verify if the header is damaged during transmission.
- Urgent Pointer: This field contains a pointer that points to the data that needs to be processed as soon as possible. The data will be processed if the URG control bit is turned on.
- Options: This field can be used to deal with various TCP options such as the maximum segment size and the window scale.
- Padding: The padding field is used to create a 32-bit boundary between the header and the data section.

The data section is placed after the header. The data section typically contains 1000–1500 bytes of message. It is also called the payload or packet body. Depending on the size of the data, the length of the data section may vary. If a packet is set to have a fixed length, the data section will be padded with blanks.

The packet trailer is placed after the data section. It is used to indicate the end of a packet. The error checking mechanism called Cyclic Redundancy Check (CRC) may be included in the packet trailer. During transmission, binary signals can be wrongly altered by outside interference. CRC can be used for detecting this type of transmission error. It can also be used to detect damaged binary signals caused by hardware failure.

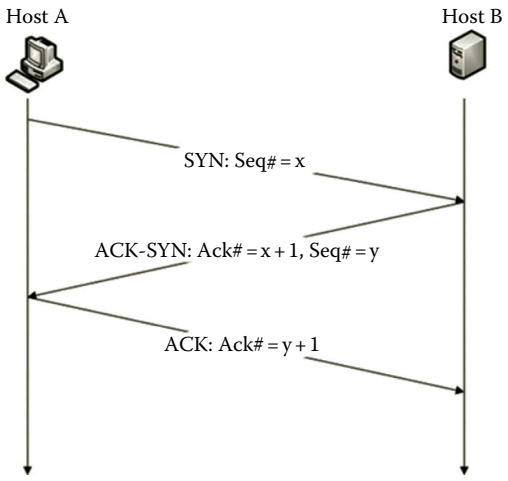

Figure 2.2 3-Way handshake process.

A reliable TCP connection is established through a 3-way handshake process. As illustrated in Figure 2.2, the 3-way handshake is implemented with three packets. The following are the steps used by the 3-way handshake process:

- To establish a reliable connection, the 3-way handshake process is started by the sender Host A. Host A first sends a packet to Host B with the control bit SYN turned on. When the SYN bit is turned on, it means that this packet is asking for a connection negotiation. In addition to turning on the SYN bit, the first packet also contains several network connection parameters such as the sequence number, say x, called the Initial Send Sequence (ISS). Therefore, the first packet is sometimes called the SYN packet.
- Once Host B receives the SYN packet, it responds with a packet with both the ACK and SYN control bits turned on. The turned on ACK bit is used as the acknowledgment of the connection negotiation request from Host A. The second packet also contains an acknowledgment sequence number x+1, which is the increment of the sequence number in the first packet. In addition to the acknowledgment sequence number, the second packet includes several network connection parameters such as another sequence number, say y. Therefore, the second packet is also called the ACK- SYN packet.
- When Host A receives the ACK- SYN packet and if it accepts the negotiation parameters, Host A will return a packet with the ACK bit turned on and the acknowledgment sequence number, which is updated to y + 1. Once the third package arrives at Host B, the 3-way handshake process is completed and the data transmission process can be started.

Similarly, the 3-way handshake process is also used in the process of terminating a connection. It makes sure that the communication between two hosts is terminated in a graceful way.

After sending out a packet, the sender waits for the acknowledgment from the receiver. When a packet gets lost or delayed during the transmission, a retransmit mechanism provided by TCP will resend the packet. If TCP waits for the acknowledgment from the receiver long enough, it will resend the same packet to the receiver. The waiting period is estimated by TCP according to the network transmission rate. TCP collects the round-trip time for sending a packet and getting the acknowledgment back. Based on the collected round-trip time, TCP then calculates the estimated mean and standard deviation of the round-trip time. The waiting period for retransmission can be determined by the following rules:

- When the measures of the round-trip time remain close to the mean, it means that the round-trip time is relatively consistent. In such a case, the waiting period for retransmission can be a time period value that is slightly longer than the mean. With such a length of waiting time, TCP waits long enough for most of the sending–receiving round trips to complete before retransmission.
- When the measures of the round-trip time vary significantly from the mean, it means that the round-trip time is not consistent. The waiting period value should be set as the mean plus two times the standard deviation. According to the statistics theory, such a waiting period is long enough for 95% of the round-trip transmissions to complete their journeys. In fact, such a calculated waiting period is suitable to any type of network traffic environments.

After the waiting period is over, TCP assumes that the packet is lost and resends the packet.

During packet transmission, there could be a situation where the sender sends more packets than the receiver can handle. To prevent this from happening, TCP uses a window mechanism to control the traffic flow so that the receiver is not overwhelmed. Once the incoming data arrive, the receiver uses a buffer to store the incoming data. The available buffer is also called the window. To not over feed the receiver, it is necessary for the sender to adjust the packet transmission rate according to the receiver's window size. Before the data transmission starts, the receiver sends out a notification about its buffer size. This notification is also called the window advertisement. According to the window advertisement, the sender delivers packets. When the receiver receives the packets from the sender, it will recalculate its window advertisement. Then, it sends the updated window advertisement to the sender with the acknowledgment. When the buffer is full, the receiver will send a zero window advertisement to inform the sender to stop sending packets. After the receiver informs the sender with a positive window advertisement, the sender can restart the data sending process.

When a packet transmission gets too crowded in one section of a network, the delivery of packets may be delayed. Some of the packets may even get lost. Such a phenomenon is called network congestion. When network congestion occurs, TCP's resending mechanism will resend those packets that get delayed or lost. Resending the packets will add more traffic on the network. In the end, little or no meaningful

communication can be carried out by the network. Such a phenomenon is called network congestion collapse. To prevent the network congestion collapse, TCP provides several congestion control mechanisms. TCP is able to adjust the packet transmission rate according to the packet loss rate. When many packets get lost or delayed in a short time, instead of resending all the missing packets immediately, TCP will resend one packet first. If no packet gets lost during the transmission, the sender will get the acknowledgment back from the receiver. In such a case, TCP will double the retransmission rate. If there is still no packet that is lost during the transmission, TCP will double the retransmission rate again. By doing this, the retransmission rate will increase exponentially. The retransmission can quickly reach about half of the advertised window size. After that, if there is still no packet lost, TCP will increase the retransmission rate one packet at a time until the whole retransmission process is done. In such a way, TCP can control how much traffic to add to the network and thereby avoid a network congestion collapse.

This section describes some of the main TCP features during packet transmission. In addition to TCP, UDP is another important protocol in the transport layer. A brief discussion of UDP is given in the next section.

2.3.2 User Datagram Protocol

Like TCP, UDP is a transport layer protocol used for sending and receiving packets between ports. Unlike TCP, UDP does not provide mechanisms to establish a reliable connection between network hosts. Also, it does not provide transmission control mechanisms such as the error correction mechanism and packet resending mechanism. The way that UDP delivers packets resembles mail delivery. It delivers a packet without the permission of the receiver. With UDP, packets are sent out without establishing a connection first. Therefore, UDP is said to be a connectionless network protocol. The advantage of UDP is that it has better performance than TCP. On the other hand, UDP is a less reliable protocol. Therefore, UDP is suitable for a situation that requires high performance but not high reliability in packet delivering. UDP is commonly used in delivering multimedia content such as streaming media in online digital games, Voice over IP (VoIP), and IP Television (IPTV). Due to its high performance feature, UDP is also used by some network protocols, applications, and services such as Trivial File Transfer Protocol (TFTP), Domain Name System (DNS), and broadcasting messages over the network.

TCP and UDP are two main transport layer protocols. In addition to TCP and UDP, there are a few dozen other less known transport layer protocols. In the TCP/IP architecture, transport protocols handle service requests from application protocols. Based on the requests from the protocols in the application layer, the transport protocols instruct the protocols in the Internet layer to prepare packet delivery to the destination hosts. In the next section, we will discuss the protocols in the Internet layer.

2.4 Internet Layer Protocols

In the TCP/IP architecture, protocols in the Internet layer are used to deliver packets from a source host to a destination host across a network. The IP is a well-known Internet layer protocol. It is the core protocol in the TCP/IP architecture. IP is the protocol that carries packets to the destination host. The journey may cross various types of networks. Another significant Internet layer protocol is the Internet Control Message Protocol (ICMP) used by network operating systems to get responses from remote hosts. The Address Resolution Protocol (ARP) relates an IP address with its hardware address, and IP Security (IPSec) is for securing IP communication. There is an argument on which layer the routing protocols should belong to. Since BGP and RIP use UDP in data transmission, some authors think BGP and RIP should belong to the application layer. Since OSPF uses IP in data transmission, some authors believe OSPF should belong to the transport layer. Sometimes, OSPF is listed in the network interface layer. Also, some authors think ARP should belong to the network interface layer. So far, there is no convincing answer to the argument. Here, for convenience, these protocols will be described in the Internet layer.

2.4.1 Internet Protocol

IP relies on TCP to establish a reliable connection. It also relies on TCP to provide mechanisms to control the transmission flow and check for transmission errors. IP depends on TCP to provide connection-oriented service to accomplish packet delivery tasks. IP's main function is to deliver packets from one host to another host. Therefore, IP should be able to keep track of the destination host's IP address. IP should also be able to find the destination host. IP formats packets, called Internet packets, so that these packets can be delivered across the Internet. An Internet packet is also called a datagram.

Currently, there are two versions of IP, IPv4 and IPv6, used on the Internet. IPv4 has been widely deployed for delivering data across the Internet. IPv4 uses a 32-bit binary number to specify the address of a network host. This means that IPv4 can identify at most 2^{32} = 4,294,967,296 network hosts uniquely. However, not all the 32-bit numbers are available for identifying hosts. Some of the 32-bit numbers are used for indentifying networks and others are used for broadcasting and multicasting, and also some of the numbers are reserved for testing or experiments. On the other hand, the number of hosts on the Internet grows exponentially. Nowadays, we are facing a shortage of 32-bit numbers to address the hosts on the Internet.

Originally, IPv4 is designed as a data-oriented protocol. It is not able to provide a high quality path for transmitting audio and video signals. In many ways, IPv4 is not very efficient for delivering packets in a large network. For example, IPv4 uses a broadcasting process to contact an unknown host in a network. During the broadcasting process, IPv4 delivers the packets to every host in the network. This can create a large amount of network traffic in the network.

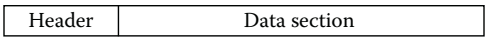

Figure 2.3 Internet packet.

The next generation IP protocol IPv6 is designed to overcome the limitations of IPv4. To make sure that we do not run out of IP addresses for many years to come, IPv6 uses 128-bit binary numbers to identify the hosts on the Internet. The set of 2^{128} binary numbers is large enough so that each atom on the surface of the earth can be assigned an IP address. IPv6 is also designed to be able to establish an optimized path to transmit the audio and video signals over the Internet. IPv6 is more efficient by eliminating the broadcast. It is also designed to simplify the network configuration and management tasks.

The Internet packet or datagram is formed with a header and a data section (Figure 2.3).

The header contains information used to send data across a network. The size of the data section may vary depending on the specification of an application. For IPv4, the maximum size of an Internet packet is 64K bytes including both the data and the header.

Since IP is designed to carry data across the Internet, it must be able to deliver a packet through heterogeneous networks. To accommodate heterogeneity, IP must accomplish the following tasks:

- Format packets with an addressing scheme.
- Pass data from one type of network to another type of network.
- Fragment packets into smaller packets to pass through the networks with low data transmission rates and reassemble the fragments at the ultimate destinations.

IP formats packets with both the destination IP addresses and source IP addresses. It must format the packets with the destination addresses so that it will know where to deliver the packets. Also, IP must format a packet with the sender's address called the source address in order to get response from the receiver. Both the source and destination addresses are included in the header of the IP packet. An IP address is assigned to each network interface device, such as a network interface card. The IP address for each host on the Internet must be unique.

In order for an Internet packet to be transmitted through a network, the Internet packet needs to be enclosed in a frame, which is a sequence of bits or symbols used to define the beginning and end of an Internet packet. The frame is formed by a specific network hardware technology in the network interface layer. Different types of networks form different types of frames. The process to load a datagram to a frame is called encapsulation. Figure 2.4 illustrates the encapsulation process.

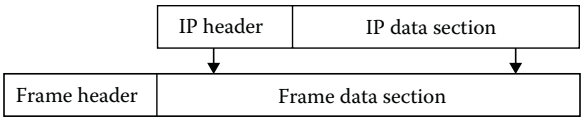

Figure 2.4 Encapsulation.

If the destination host is located within the same network, the frame will carry the Internet packet or datagram to its destination directly. However, if the destination host is located in a different type of network, the frame can only carry the datagram to the border between the two networks where the datagram will be reloaded to a different type of frame formed by a different type of network technology. This is how the datagram can be carried through different types of networks.

When a datagram is delivered across the Internet, it may need to travel through multiple networks to get to the destination. Different networks may have different data transmission rates. The data transmission rate is specified by the parameter Maximum Transmission Unit (MTU). The MTU refers to the maximum amount of data that a frame can carry. It may happen that the MTU of a network in the middle of the delivery path is less than that of the network which the sender belongs to. In such a case, the amount of data originally loaded in the frame formed by the sender's network is too much to be carried by the frame formed by the network with the lower MTU. Therefore, the originally loaded data unit needs to be divided into smaller units so that they can be carried by the frame formed by the network with the lower MTU. The process of dividing the original data unit into several small units is called fragmentation. The header of each fragment is so constructed that all the fragments can be reassembled back to the original datagram. As the fragments may be transmitted through different routes to the ultimate destination, it is difficult to reassemble them in the middle of the delivery path. Also, the fragments may need to be further fragmented if there is a network with an even smaller MTU in the delivery path. Therefore, the fragments are reassembled at the ultimate destination.

An IP header is constructed to accomplish the aforementioned tasks. Figure 2.5 illustrates an IP header's structure.

The following briefly describes the main fields in the IP header:

- H. Len: This field specifies the length of the IP packet header. The minimum length of an IP header is five words and each word contains 32 bits. Therefore, the smallest IP header contains 20 bytes of information.

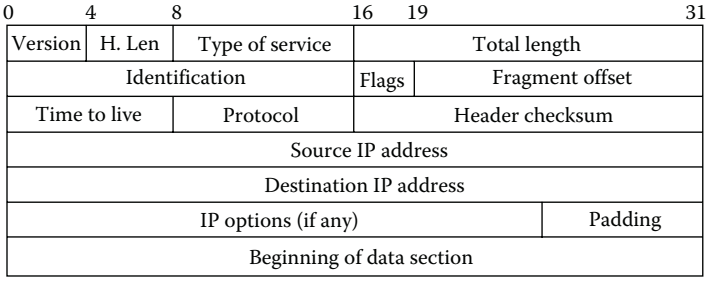

Figure 2.5 IP header.

- Type of Service: This field is used to specify if a datagram passes through a route with the minimum delay, the maximum throughput, the maximum reliability, or the minimum cost.
- Total Length: This field specifies the length of a datagram, including both the header and the data section.
- Identification: This field is used to identify the datagram to which the fragments belong. Together with the source address, the value in the identification field can be used to reassemble the fragments back to the original datagram.
- Flags: This field is used to set and display fragment-related properties.
- Fragment Offset: The content of this field is used to instruct the receiver how to reassemble a fragmented datagram.
- Time to Live (TTL): The value in this field represents the lifetime of a datagram. Each time a datagram passes through a network, the lifetime number will be reduced by one. When the lifetime number is down to zero, the datagram is discarded. TTL is used to prevent a datagram from traveling in an infinite loop.
- Protocol: This field specifies the protocol to be encapsulated.
- Header Checksum: This field contains an IP header checksum, which is used to detect transmission errors in the IP header.
- Source Address: This field contains the sender's IP address.
- Destination Address: This field contains the receiver's IP address.
- Options: This field specifies various IP options such as MTU replay and experimental flow control.
- Padding: This field is used to create a 32-bit boundary between the header and the data section.

In the TCP/IP architecture, TCP and IP are the core protocols. During data transmission, these two protocols work together and are often denoted as TCP/IP. In addition to IP, the Internet layer also includes several other protocols, which are introduced next.

2.4.2 Internet Control Message Protocol

ICMP is a protocol used to report network operation status and network errors. The following are some of the tasks accomplished by ICMP:

- Report Network Status: ICMP can be used to send an echo request message to the receiver. Then, it carries the reply of the receiver back to the sender. ICMP can also be used to report how packets are redirected to different networks.
- Report Network Errors: ICMP can be used to report network problems such as an unreachable host or network. It also carries network parameters that may reveal an improperly functioning network.

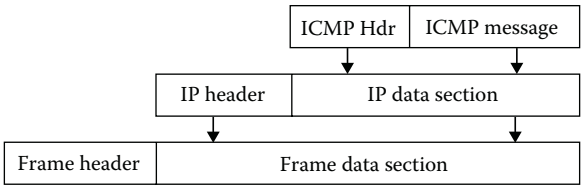

Figure 2.6 Encapsulation of ICMP.

- Report Network Congestion: When a receiving device on a network cannot process the incoming data fast enough, ICMP will deliver a source quench message to the sender for adjustment. ICMP can also be used to probe the MTU of a network and send the result back to the sender.
- Assist Network Troubleshooting: ICMP can be used with network troubleshooting commands. When used with a network management command such as ping, ICMP reports if a packet can be sent to a dedicated destination. ICMP can also report the round-trip time and the percentage of packet loss during the transmission. When used with the tracert command, ICMP reports what networks the packet has passed through. The report also includes the TTL value. A time expired message will be returned by ICMP when TTL drops to zero.

To deliver an ICMP message through different networks, a network device creates an IP datagram first and then encapsulates the ICMP message in the IP datagram as shown in Figure 2.6.

2.4.3 Address Resolution Protocol

For the data communication between two hosts, the IP header includes the source and destination IP addresses. However, a frame uses the hardware address (also called MAC address) to deliver packets. When the frame reaches the destination network, each host in the destination network compares its hardware address with the destination hardware address included in the frame. If there is a match, the frame will be processed by the destination host. Therefore, the destination IP address in the datagram needs to be correctly converted to the hardware address. Otherwise, the frame will not be able to find its destination. ARP is the protocol used to resolve the IP address to the hardware address.

The commonly used address resolution scheme is called message exchange, which can be accomplished in three steps. When a host needs to resolve a destination IP address, it first broadcasts an ARP request to ask which host in the destination network has the IP address that matches the destination IP address. After the destination host discovers that its IP address matches the destination IP address, it will respond with an ARP reply, which contains the corresponding hardware address to the host that issued the ARP request. After the ARP reply arrives, the host that issued the

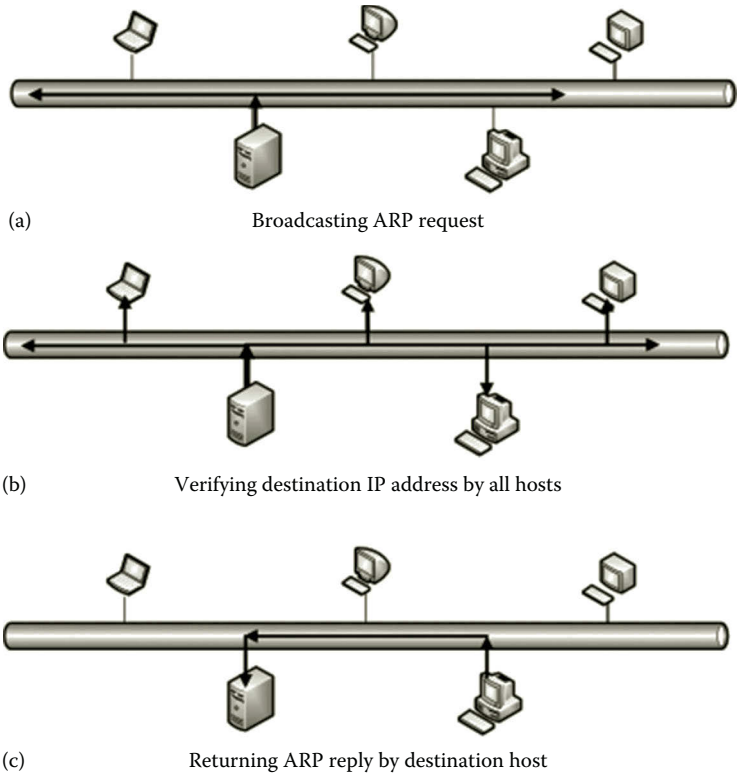

Figure 2.7 Address resolution process.

ARP request places the destination hardware address to the frame. Now, the frame is ready to be sent. Figure 2.7 illustrates the three-step process.

To make the address resolution process more efficient, the host operating system saves the pair of the IP address and its matching hardware address in a cache. Next time, if the host needs to resolve a destination IP address to a hardware address, it will search the cache first. If there is no match in the cache, then the host will start the message exchange process.

2.4.4 IP Security

While traveling across a network, packets can be captured by unauthorized individuals or hackers. The unauthorized individuals can read or intentionally alter the data content in the packets. IPSec is a protocol that provides protection against hackers. It provides authentication, encryption, and digital signature mechanism for securing TCP/IP communication. The authentication mechanism is used to make sure that the computers or network devices on both ends of a communication path are trusted. After a secure connection is established, IPSec hides the IP address. The encryption mechanism is used to make the content carried by IP packets unreadable. With IPSec, even if the packets are captured by hackers during the transmission,

the hackers cannot figure out the data content. The IPSec digital signature is used to make sure that the content of an IP packet is not altered during the transmission. Since IPSec is an Internet layer protocol, it can protect all the protocols in the transport layer and application layer so that those protocols do not have to have their own protection. The disadvantage of IPSec is that it slows down the network traffic. Later chapters will show how IPSec is used to connect an on-premises network to a virtual network on a cloud. The advantage of IPSec is that the data communication between two networks is highly secured.

2.4.5 Internet Routing Protocols

Routing protocols such as Routing Information Protocol (RIP), Open Shortest Path First (OSPF) protocol, and Border Gateway Protocol (BGP) are used to create and update routing tables. A routing table stores information about the routes from one network to other networks. The routing protocols can also be used to calculate the shortest path from one network to another.

BGP is a protocol used to manage routes among autonomous systems. An autonomous system is a heterogeneous network system typically governed by a large organization such as an Internet service provider (ISP). Each ISP may create its own autonomous system. The networks included in an autonomous system adopt the same routing policy. BGP is often used by ISPs to establish routes among them. The Internet routing protocol that manages routes among autonomous systems is also called Exterior Gateway Protocol (EGP). The Internet routing protocol that manages routes within an autonomous system is called Interior Gateway Protocol (IGP). To accomplish the routing management tasks, BGP has the following features:

- BGP is a type of EGP as well as IGP.
- BGP allows the sender and the receiver in different autonomous systems to negotiate routing policies.
- BGP uses the reliable TCP to update the routing table.
- With BGP, an autonomous system can be defined as a transit system, which allows the network traffic to pass through, or can be defined as a stub system, which blocks the network traffic from passing through.
- BGP can be used to dynamically update the routing tables of neighboring autonomous systems.
- BGP can be used to program routing policies and route filters.
- BGP allows network administrators to inject specific routes into the routing table.

RIP is used as an Internet routing protocol within an autonomous system. RIP is a simple protocol and requires very little configuration. However, RIP is not suitable for large networks since it can only manage up to 15 subnetworks and it takes a lot of network resources to update routing tables. Therefore, RIP is usually used in

small network systems or used for education purposes. The following are some of the RIP features:

- RIP is used as IGP.
- RIP uses UDP to update routing tables, which is faster but less reliable.
- RIP does not check transmission faults while updating routing tables.
- RIP uses broadcasting to update routing tables. Although the use of broadcasting may take less effort, it is much less efficient.
- RIP measures the distance of a route by counting the number of networks the route traverses. RIP can only count up to 15 networks. This feature makes RIP a protocol that updates routing tables locally.
- To update routing tables, RIP broadcasts a packet that contains a complete routing table every 30 s. The broadcasted routing table is used by other routers to update their own routing tables. Broadcasting routing tables to one another every 30 s can significantly slow down network performance if there are many routers used in the network. Therefore, RIP is not designed for large networks.

The OSPF protocol is designed to handle the routing needs of large companies and ISPs. It has the following features:

- OSPF is used as IGP.
- OSPF has a hierarchical structure. With the hierarchical structure, OSPF can divide a large autonomous system into areas and update the routing tables within an area. The use of areas can significantly reduce the size of a routing table.
- OSPF uses Dijkstra's algorithm to find the shortest path inside each area. OSPF allows the network administrator to define the criteria of the shortest path.
- By using OSPF, more IP addresses are available to be assigned to networks and hosts in a network.
- OSPF provides the authentication mechanism to secure the updating of routing tables.
- OSPF can import routes created by other routing protocols.
- Instead of using broadcasting, OSPF uses multicasting within an area for routing table updating. Multicasting is more efficient than broadcasting.
- When updating a routing table, instead of sending out the entire routing table, OSPF only sends out what has been changed in the routing table to other routing tables in an area. Changes are sent only when they occur, not every 30 s.

With the aforementioned features, OSPF is a more sophisticated Internet routing protocol. The disadvantages of OSPF are the complexity in configuration, which takes more time for one to learn how to configure the protocol.

2.5 Network Interface Layer Protocols

Protocols in the network interface layer are implemented by combining the hardware and software. In some of the textbooks, the network interface layer is broken into two layers. One is the network interface layer, which contains protocols that are used to form frames. The other layer is the physical layer, which includes the network hardware. Here, for convenience, the hardware and the protocols are all combined into a single network interface layer. There are more than a dozen protocols and network technologies included in this layer. The commonly used protocols and network technologies in the network interface layer are Point-to-Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Protocol (PPP), Ethernet, Wireless Fidelity (Wi-Fi), Worldwide Interoperability for Microwave Access (WiMAX), the network interface card, twisted pair cable, optical fiber, electromagnetic radio wave, and so forth.

The network interface layer protocols convert packets into raw binary bits and transport the binary bits across the network media. The binary bits are then formed into code words. After that, the code words are converted into physical electric signals. Through the network media, the electric signals are then transmitted to the destination host. Once the electric signals arrive at the destination host, they are reorganized into packets for protocols in the upper layers to process. Some of the protocols in the network interface layer have the mechanism to verify if the physical electric signals have been correctly transferred to the destination.

Point-to-Point Tunneling Protocol (PPTP): PPTP is sometimes listed as the application layer protocol. Again, there is no convincing answer to this. PPTP is also a protocol used for VPN connections. PPTP was jointly developed by several companies such as Microsoft, 3COM, US Robotics, and others. By using PPTP, users can securely remotely access their companies' or universities' network devices and computers through the Internet. PPTP provides both user authentication and encryption to secure the communication on the Internet. It is relatively easy to configure PPTP. The disadvantage of PPTP is that it only authenticates users but not network hosts. This means that the users are able to access the VPN server through any host, which may cause some security concern. For better security, one can consider using L2TP.

Layer 2 Tunneling Protocol (L2TP): L2TP can also be used to support VPN connections. The data to be transmitted are encapsulated into L2TP packets. To protect the data's confidentiality, L2TP relies on IPSec to provide the encryption mechanism. In order to do so, the L2TP packet is encapsulated into an IPSec. Then, the IPSec packet is delivered over the public Internet. The L2TP/IPSec pair requires more configurations. Both the VPN client and VPN server are required to use the IPSec authentication. L2TP/IPSec improves authentication by providing both the user level authentication and the computer level authentication.

Point-to-Point Protocol (PPP): PPP is a protocol commonly used for transferring Internet packets over a serial link such as a telephone line or an optical link. TCP/IP

protocols do not work well over a serial link. Therefore, PPP is designed for this purpose. For example, since IP packets cannot be transmitted through a modem line on their own, an ISP uses this protocol to connect their customers to the Internet. PPP also provides error checking and authentication mechanisms.

Ethernet: The Ethernet technology does two tasks. The first task specifies the format of a frame to be transmitted across a network. The second task defines the wiring and signaling standards. In an Ethernet network, the network media such as cables are designed according to the Ethernet standards. The network hardware used to connect to cables, such as cable plugs and network interface cards, is also designed to follow the Ethernet wiring and signaling standards. The Ethernet technology is widely used in both the wired networks and wireless networks. Originally, the transmission rate supported by the Ethernet technology was 10 megabits per second (Mbps). Later, the Fast Ethernet technology supported the transmission rate of 100 Mbps. The Gigabit Ethernet technology can support the transmission rate up to 1000 Mbps. Recently, 10G Gigabit Ethernet has become available. All these Ethernet technologies are designed to share the same frame format; this makes the current Ethernet technology backward compatible with the early versions of Ethernet.

Wireless Fidelity (Wi-Fi): Wi-Fi is well known for short distance wireless communication. It is commonly used in local area networks, cordless phones, video games, and so on. Wi-Fi network devices are widely installed in laptop computers and mobile devices. In a data communication process, a Wi-Fi adapter converts the binary code into radio signals, and then transmits the radio signals through an antenna. When a Wi-Fi access point receives the radio signals, it converts the radio signals back to the binary code and transmits the code through a wired network media. A Wi-Fi access point is typically available in a home network. It may also be available in many public locations such as student dormitories, restaurants, airports, and hotels. The Wi-Fi technology makes networking more flexible by avoiding the cabling process. Without cabling, Wi-Fi also reduces the cost on network deployment. The main disadvantage of Wi-Fi is the short communication range. It may also cause some security concerns.

Network Interface Card (NIC): Physically, an NIC connects the bus system in a computer and the network media. A computer bus is an array of wires with a connector on each end of the bus. The computer bus shared by different electric devices is used to transmit binary signals from one device to another device inside a computer. Through NICs, binary signals can be passed on to the network media such as the copper wire, fiber optic cable, or radio wave for wireless networks. Each NIC has a unique serial number, which is often used as the hardware address. In a data transmission process, after a frame is formed, the CPU sends the frame through the computer bus to the NIC and instructs the NIC to forward the frame to the network media. The NIC handles all the details of frame transmission and reception. After the frame reaches the receiver, the receiving computer's CPU allocates buffer space in the memory and tells the receiving computer's NIC to read the incoming frame. After all parts of the frame have been received, the NIC verifies the checksum.

If there is no error, the NIC will compare the destination address in the received frame with its own hardware address. If there is a match, the NIC will inform the CPU to make a copy of the frame in the memory and begin to process the frame. If the hardware address does not match the destination address, the received frame will be discarded. The communication between the NIC and CPU is handled by the network card driver, which handles the interaction between the computer and the attached hardware.

Twisted pair cable: A twisted pair cable is a type of network media. It is a type of wire used to transmit electric signals to the destination host through a pair of copper wires. The pair of insulated copper wires is twisted together to minimize the electric interference. The use of the copper wire is due to its low resistance to electric currents.

Optical fiber: Optical fiber is another type of network media. It is made with flexible glass fiber that can be used to transmit data to a remote destination. To transmit data over optical fiber, the sender first converts the binary signals into light pulses and then transmits the light pulses by using a light emitting diode (LED). When the light pulses reach the destination, the receiver uses a phototransistor to detect the light pulses and converts them into electric currents. Then, the network adapter converts the electric currents to binary code. Compared with the copper wire, optical fiber has the following advantages:

- The light pulses transmitted by optical fiber are not susceptible to electric interference.
- The transmission of light pulses in optical fiber is much faster than the transmission of electric signals in a copper wire.
- Optical fiber can transmit data over much longer distance than what a copper wire can do. During long distance travel, a light pulse has very little loss.
- Light pulses can be encoded with much more information than electric currents.

The disadvantage is that it is difficult to install and repair optical fiber.

Electromagnetic radio wave: An electromagnetic radio wave is a type of wireless network transmission media. It can be used to transmit data over the air. With radio waves, senders and receivers send and receive data through antennae. Radio waves can be converted into binary signals or vice versa. Different sections of radio wave frequencies are reserved for different types of wireless technologies. For example, Wi-Fi uses radio frequencies between 2.4 and 5.6 GHz. The higher the frequency, the faster the transmission rate is.

This section has briefly introduced some of the network interface layer protocols and technologies. Some of the protocols and technologies in the network interface layer are responsible for physically transferring data between hosts. Some of them are also responsible for interacting with the protocols in the Internet layer. In the next section, we will take a closer look at how these protocols relate to each other.

2.6 Network Protocol Graph

In this section, a protocol graph will be used to illustrate the relationships among the protocols. The protocols in the application layer handle data communication requests and responses by application software. However, the protocols in the application layer cannot deliver or receive data through a network by themselves. To deliver the data to a destination host in a network, the data block needs to be chopped into small units and carried by the IP protocol to the destination host. To reach the destination host, one needs a protocol such as TCP to create a connection between two hosts on the network. Also, other protocols may be needed to convert IP packets to electric signals so that they can be physically transmitted over the network media. Therefore, data transmission over a network is accomplished by multiple protocols working together. Figure 2.8 illustrates the relationships among these protocols.

As shown in Figure 2.8, when a client needs certain information from the server, the request is initiated by an application layer protocol. The request will be passed on to a transport protocol such as TCP through a dedicated communication port. Then, TCP will establish a reliable connection to the port dedicated to the application on the server.

IP delivers packets to destination hosts across the Internet. IP itself does not create a connection to a remote host. It relies on TCP to establish the connection and control the data flow. ICMP is used to get error messages from remote hosts. Protocols such as ICMP and ARP are encapsulated in IP so that messages can be delivered through different types of networks. To deliver an Internet packet or datagram, IP depends on the protocols or technologies in the network interface layer. For example, to transmit an Internet packet across an Ethernet network, the

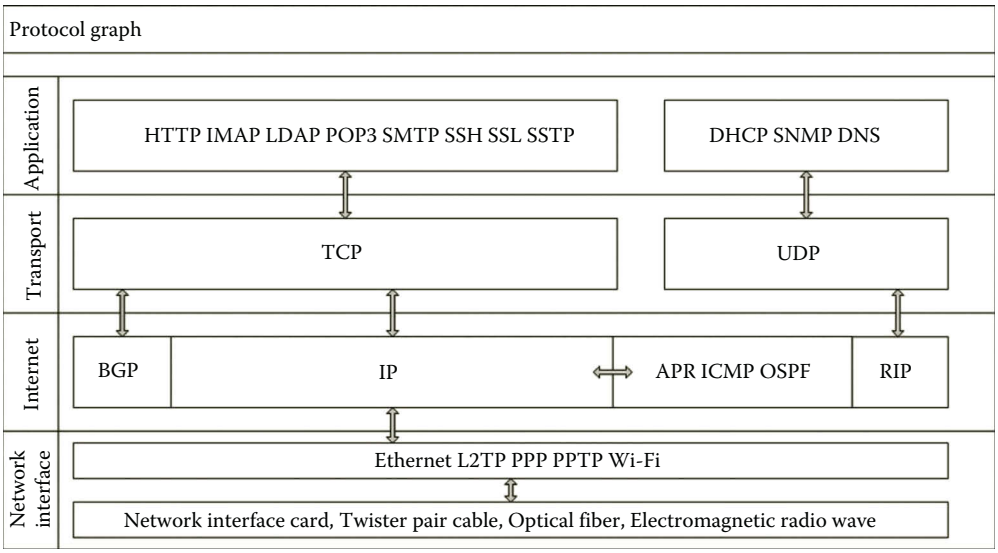

Figure 2.8 Protocol graph.

Table 2.1 Communication Ports

APPLICATION LAYER PROTOCOL	PORT NUMBER	TRANSPORT LAYER PROTOCOL
HTTP	80	TCP
IMAP	143	TCP
LDAP	389	TCP
POP3	110	TCP
SMTP	25	TCP
SSH	22	TCP
SSTP	443	TCP
DHCP	67	UDP
SNMP	161	UDP
DNS	53	UDP

Internet packet will be carried by a frame formed by the Ethernet technology. By using a network interface card, the frame is then converted to binary signals and is transmitted by electric currents, light pulses, or electromagnetic radio waves to the remote destination. Once the binary signals reach the destination host, the network interface card on the destination host will verify the destination address with its own hardware address. If there is a match, the binary signals will be reassembled to get the Internet packet back. At the destination, TCP will perform error checking and decide if a resend is necessary. If there is no error, the TCP on the destination host will pick up the request and forward the message to the protocol related to the server side application through the corresponding port. Table 2.1 lists the port numbers used by the application layer protocols for communicating with the transport layer protocols mentioned in Figure 2.8.

Earlier, we have examined the relationships among some commonly used protocols in each layer of the TCP/IP architecture through a graph. Next, we are going to explore some networking tools and view some of the protocols through hands-on activities.

Activity 2.1: Exploring Windows Server 2012

The objective of this activity is to get familiar with the networking tools provided by Windows Server 2012.

Task 1: Exploring Windows Server 2012 Operating System

1. Log on to the Microsoft Azure Management Portal with your user name and password.
2. Select your virtual machine **servera** and click **CONNECT**.
3. Log on to your **servera** server as **student** with your password.
4. Click **Local Server**, you should be able to see the configuration of the local server shown in Figure 2.9. In Figure 2.9, you can find the computer name,

Figure 2.9 Information about local server.

workgroup name, firewall status, information about the Ethernet cards, and the version of your operating system.

5. You can configure the name of the local server. Click **servera**, you will see the **System Properties** dialog where you can configure the computer name and workgroup as shown in Figure 2.10. Click **Cancel** to close the System Properties dialog.

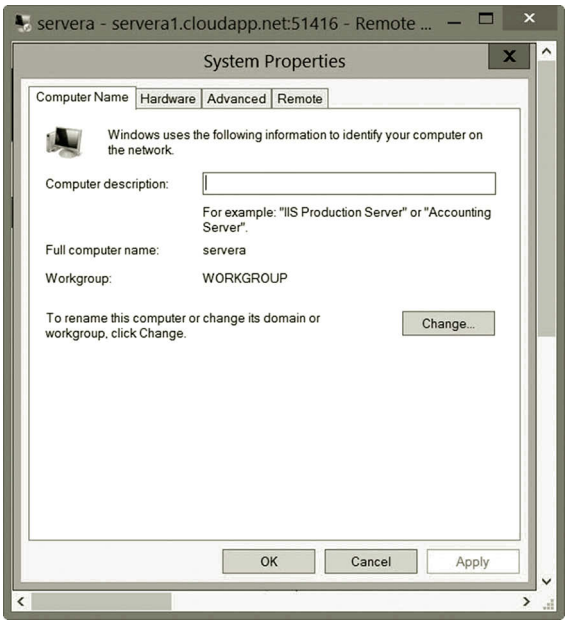

Figure 2.10 System properties dialog.

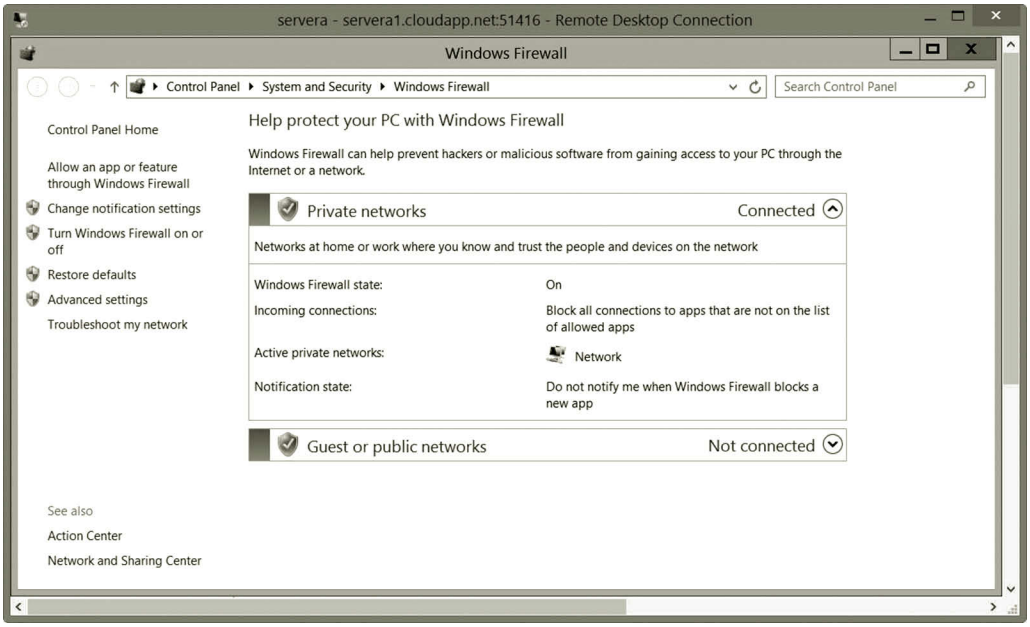

Figure 2.11 Windows firewall dialog.

6. For firewall configuration, click the link **Public: On**. You should be able to see the Windows Firewall dialog shown in Figure 2.11. You can change the firewall settings in the Windows Firewall dialog. Close the **Windows Firewall** dialog.
7. To configure the network adapter, click the link **IPv4 address assigned by DHCP, IPv6 enabled**. Right click the **Ethernet** icon and select **Properties**. Select **Internet Protocol Version 4 (TCP/IPv4)** and click the **Properties** button. You should be able to see the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog shown in Figure 2.12.
8. To be able to access the Internet from your virtual machine, click the option **Use the following DNS server addresses** as shown in Figure 2.13. Enter a public know DNS server IP address such **8.8.8.8** and click **OK**.
9. You should be able to see the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog shown in Figure 2.14. Click **Cancel** to close the dialog.

Task 2: Viewing Ethernet Properties

1. Assume that you have logged on to your Windows Server 2012. Click the link **Local Computer**. Then, click **IPv4 address assigned by DHCP, IPv6 enabled**.
2. Right click the **Ethernet** icon and select **Properties.** In the Ethernet Properties dialog, as you can see, the network protocols TCP/IPv4 and TCP/IPv6 are installed. Click the **Install** button (Figure 2.15).

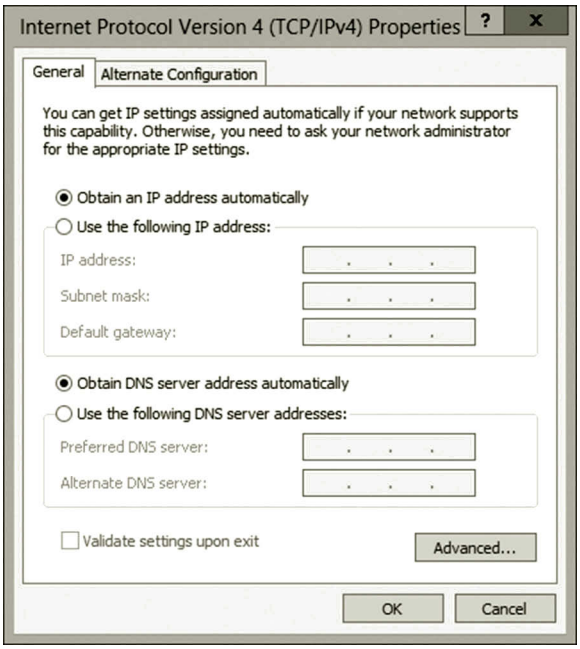

Figure 2.12 IPv4 properties dialog.

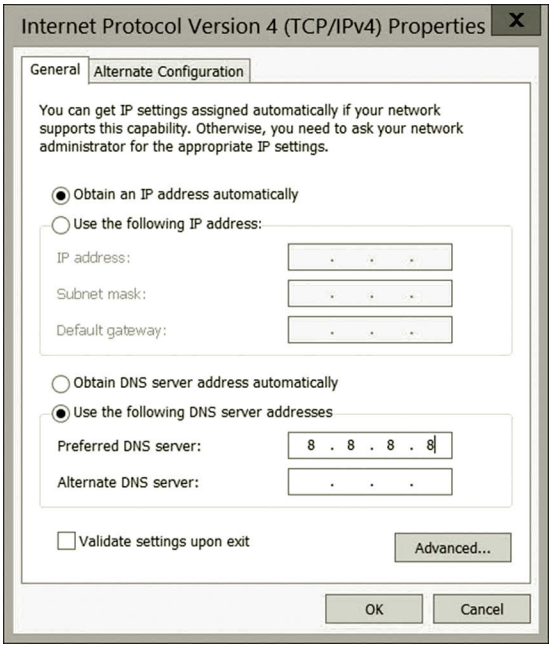

Figure 2.13 Specifying DNS server.

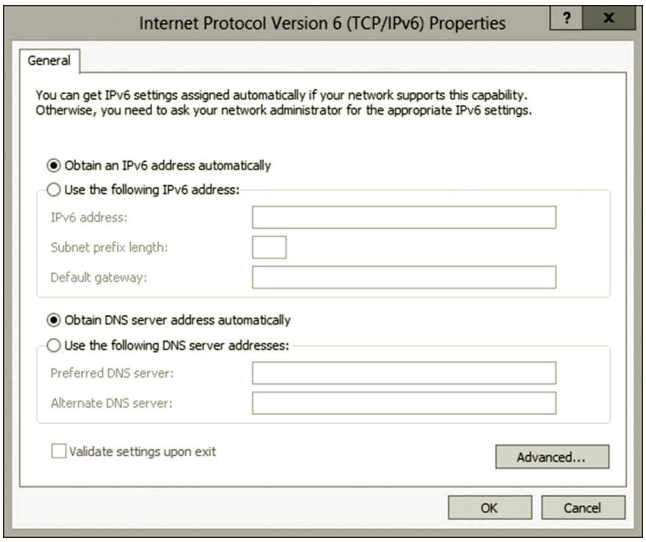

Figure 2.14 IPv6 properties dialog.

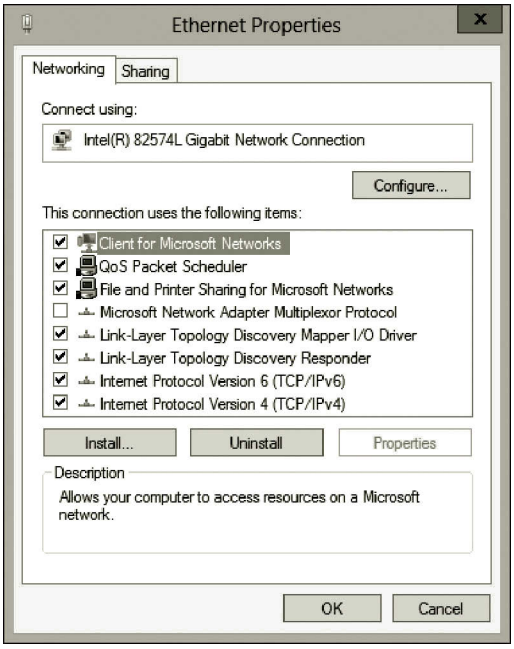

Figure 2.15 Ethernet properties.

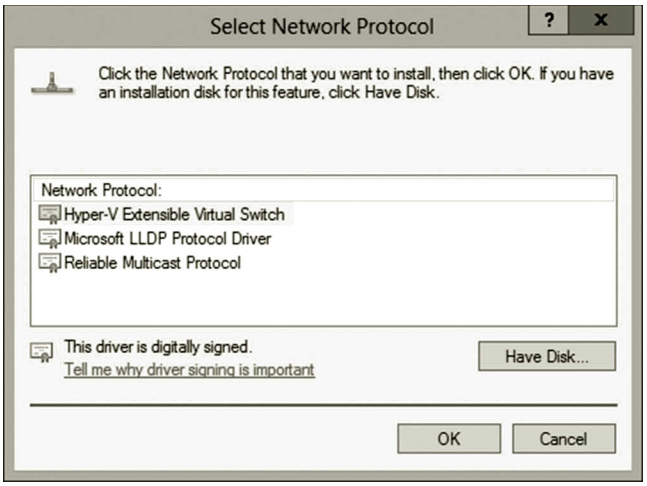

Figure 2.16 Available network protocols.

3. To see more protocols available to install, in the Select Network Feature Type dialog, select **Protocols** and click the **Add** button. You will see a few protocols available for installation as shown in Figure 2.16.
4. After you have viewed the protocols, click the **Cancel** button.

Task 3: Viewing Available Roles and Features

You will be using ICMP to test the connection between two virtual machines. By default, the ICMP protocol is blocked by the firewall. You need to enable ICMP. The following are the steps to enable ICMP:

1. Log on to your Microsoft Azure Management Portal with your user name and password.
2. Select your virtual machine **servera** and click **CONNECT**.
3. Log on to your **servera** server as **student** with your password.
4. In Server Manager, click the **Tools** menu and select **Windows Firewall with Advanced Security** as shown in Figure 2.17.
5. After the configuration dialog is opened, click **Inbound Rules** on the left-hand side of your screen. Use the **Ctrl** key to select **File and Printer Sharing (Echo Request - ICMPv4-In)** and **File and Printer Sharing (Echo Request - ICMPv6-In)**. Right click the selected items and click **Enable Rule** as shown in Figure 2.18.
6. In the configuration dialog, click **Outbound Rules** on the left hand side of your screen. Use the Ctrl key to select **File and Printer Sharing (Echo Request - ICMPv4-Out)** and **File and Printer Sharing (Echo Request - ICMPv6-Out)**. Right click the selected items and click **Enable Rule** as shown in Figure 2.19. After the outbound rules are configured, close the configuration dialog.

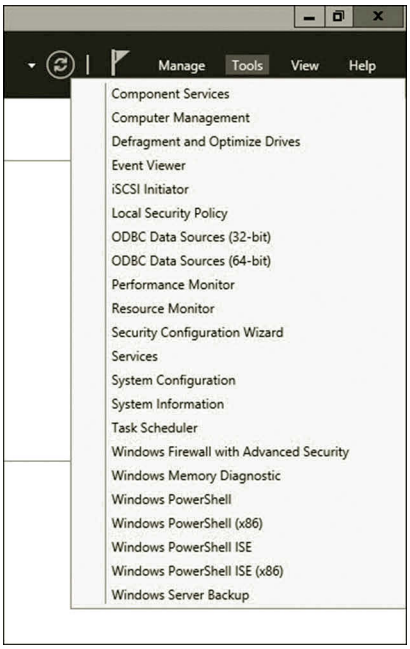

Figure 2.17 Configuring firewall.

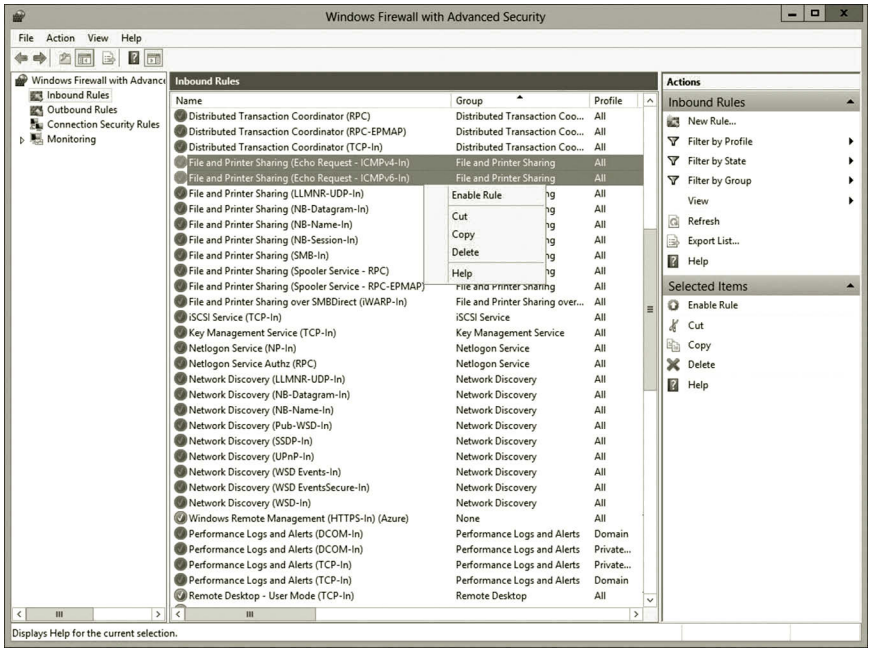

Figure 2.18 Configuring inbound rules.

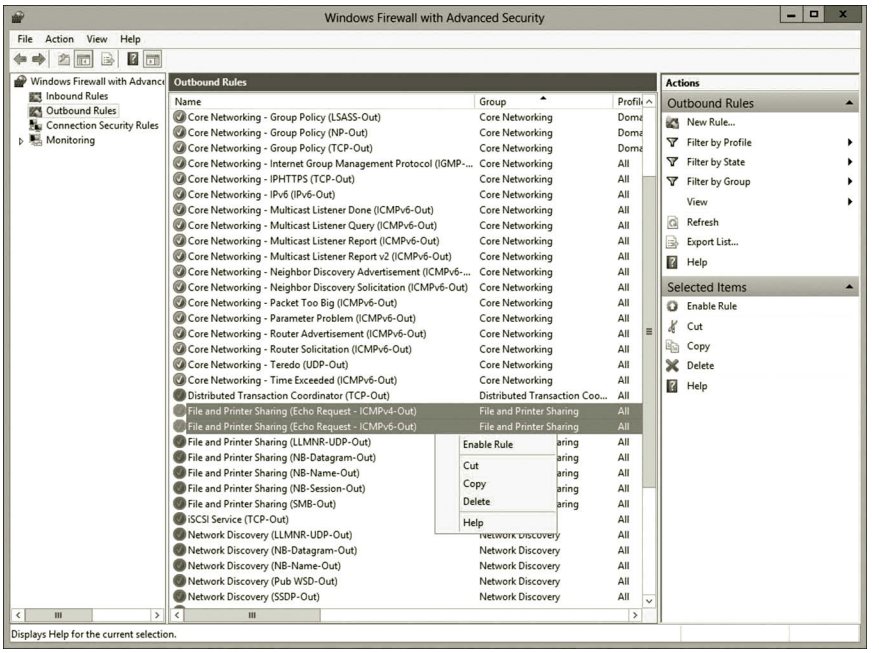

Figure 2.19 Configuring outbound rules.

7. Similarly, enable ICMP in serverb.
8. Assume that you have logged on to your Windows Server 2012. To view the available roles, on the Server Manager page, click the link **Dashboard**.
9. On the Dashboard, click the link **Add roles and features** as shown in Figure 2.20.

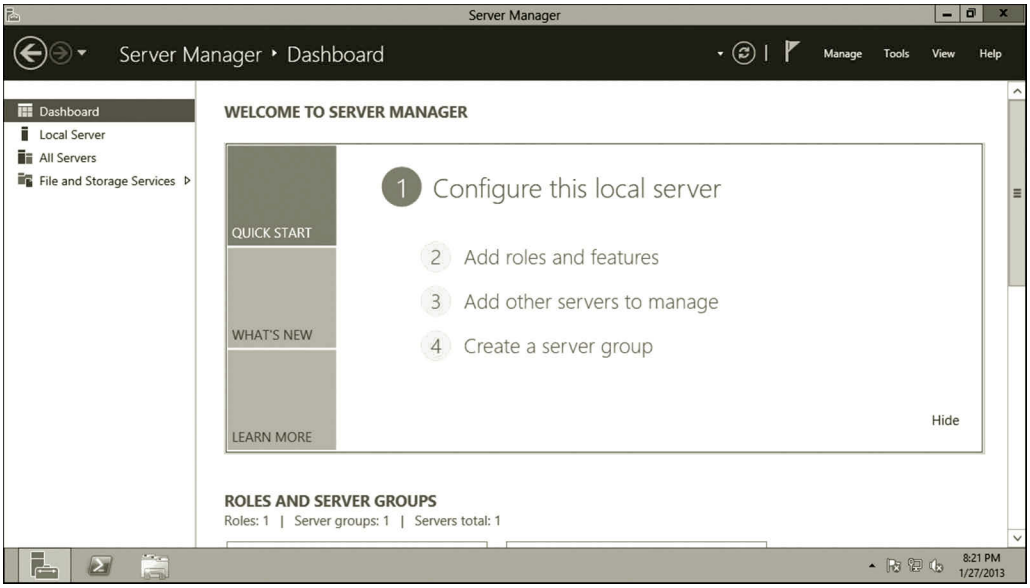

Figure 2.20 Dashboard.

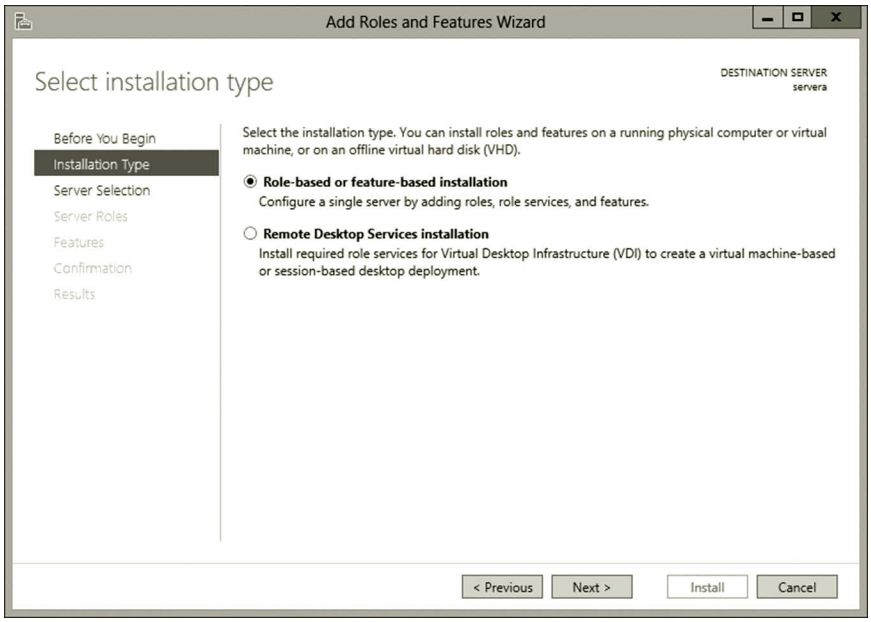

Figure 2.21 Select installation type page.

10. After the Add Roles and Features Wizard is opened, click the **Next** button.
11. On the Select installation type page, select the option **Role-based or feature-based installation** and click the **Next** button as shown in Figure 2.21.
12. On the Select destination server page, select your server as shown in Figure 2.22, and then click the **Next** button.

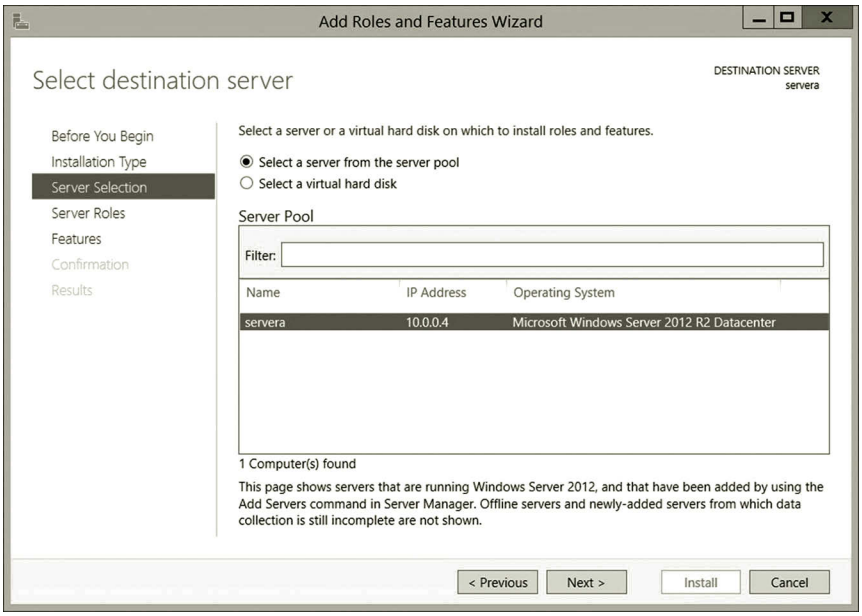

Figure 2.22 Select destination server page.

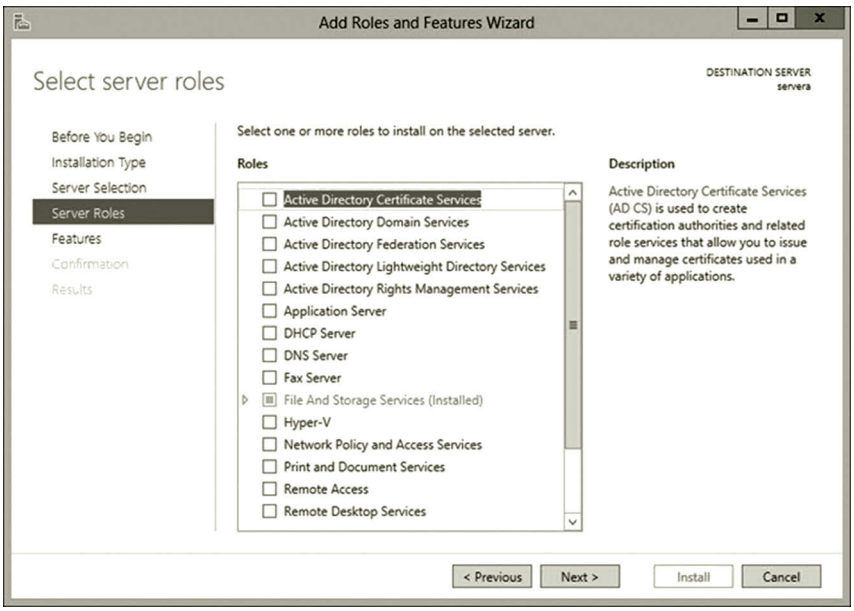

Figure 2.23 Select server roles page.

13. On the Select server roles page, you can see a number of service roles available for installation as shown in Figure 2.23. Then, click the **Next** button.
14. On the Select features page, you can see a number of features available for installation as shown in Figure 2.24. After viewing the features, click the **Cancel** button.

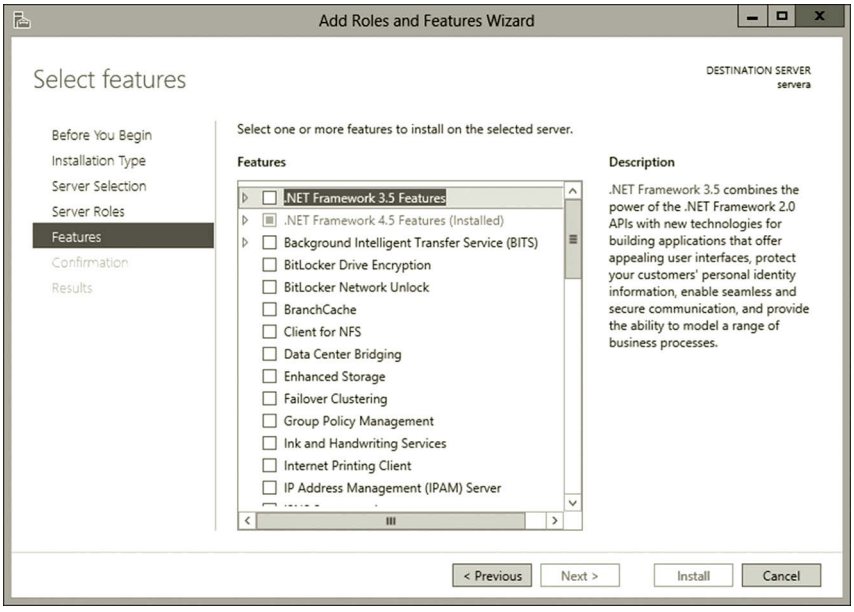

Figure 2.24 Select features page.

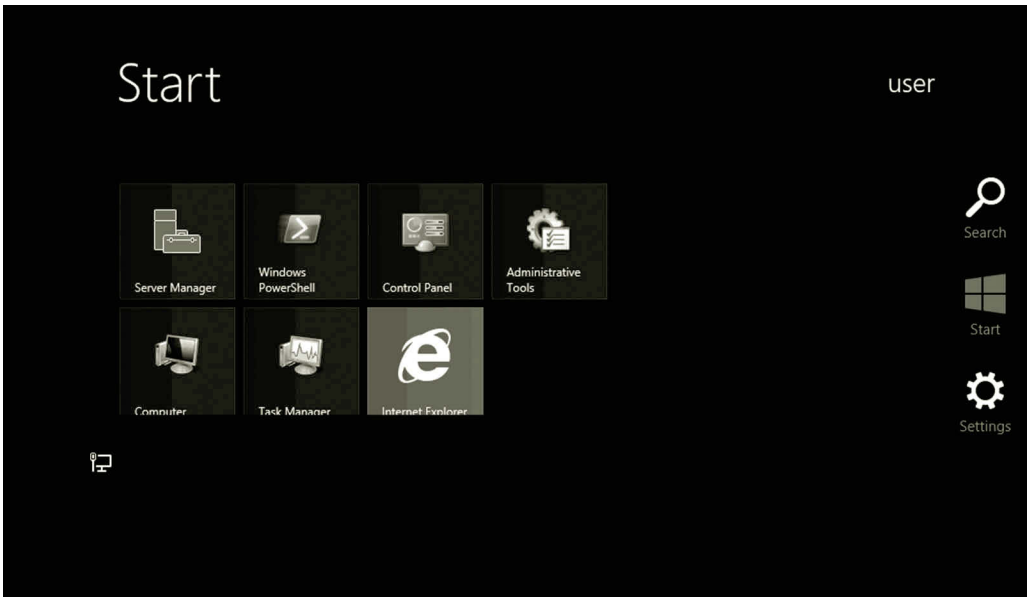

Figure 2.25 Pop-up start screen.

Task 4: Viewing Installed Roles and Features

To view the installed services on Windows Server 2012, you may follow the steps given here:

1. Move the mouse along the border at the lower right corner of your Windows Server screen. After the pop-up menu is displayed on the screen, click the **Start** icon as shown in Figure 2.25. You may also get the Start menu by clicking the **Start** icon on the task bar.
2. On the Settings menu, click **Administrative Tools** tile.
3. On the Administrative Tools page, double click **Services**. Then, you will see the installed services shown in Figure 2.26.
4. After you have viewed the installed services, close the Services window.

Activity 2.2: Viewing IP Configuration in the Command Prompt Window

In this activity, you will use the Command Prompt window to view IP configuration:

1. If you have not done so, log on to your Microsoft Azure account and connect to your virtual machine servera.
2. Press the **Windows logo** key. Type **cmd** and then click the **Command Prompt** tile as shown in Figure 2.27.
3. In the Command Prompt window, enter the command **ipconfig/all** as shown in Figure 2.28 and press **Enter**. From the printout, you can find the information about the Windows IP configuration and Ethernet Adapter configuration.

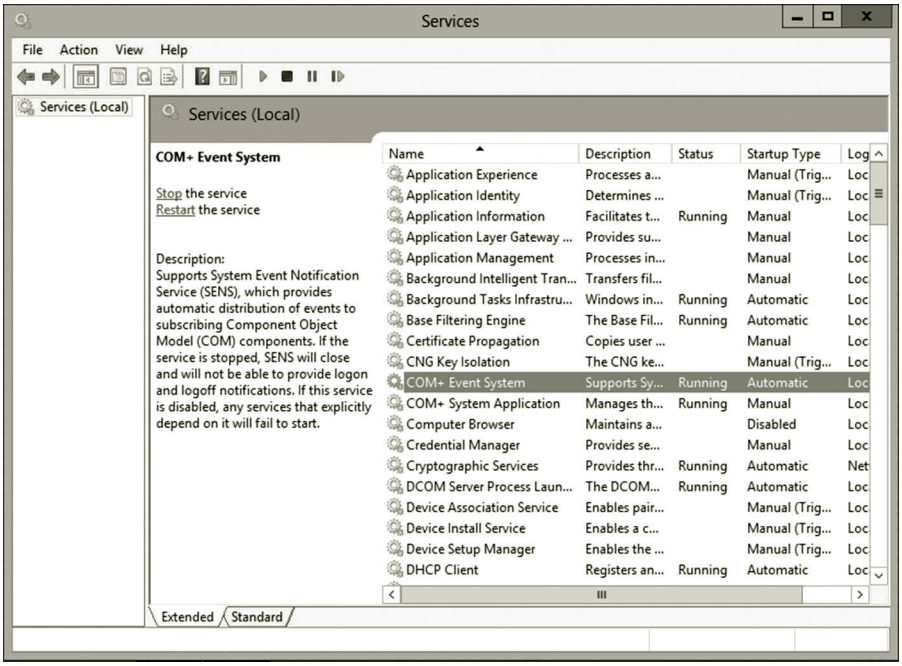

Figure 2.26 Installed services.

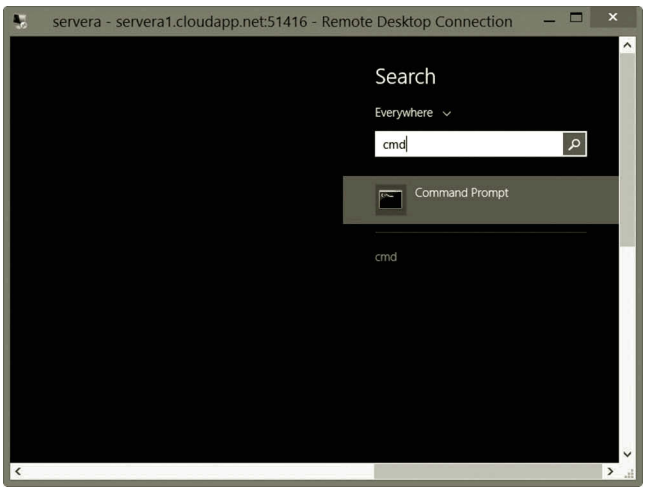

Figure 2.27 Open command prompt.

4. As shown in Figure 2.29, the information about Ethernet Adaptor 2 of servera is displayed. The information includes the IPv4 IP address and IPv6 IP address.
5. Close the command prompt window.
6. Similarly, you can get the IP information from serverb as shown in Figure 2.30.

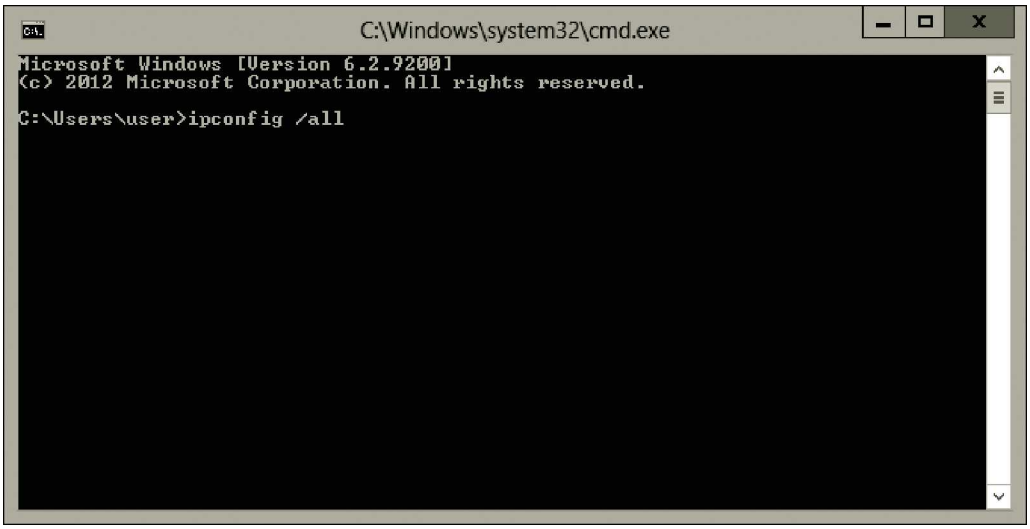

Figure 2.28 Command prompt.

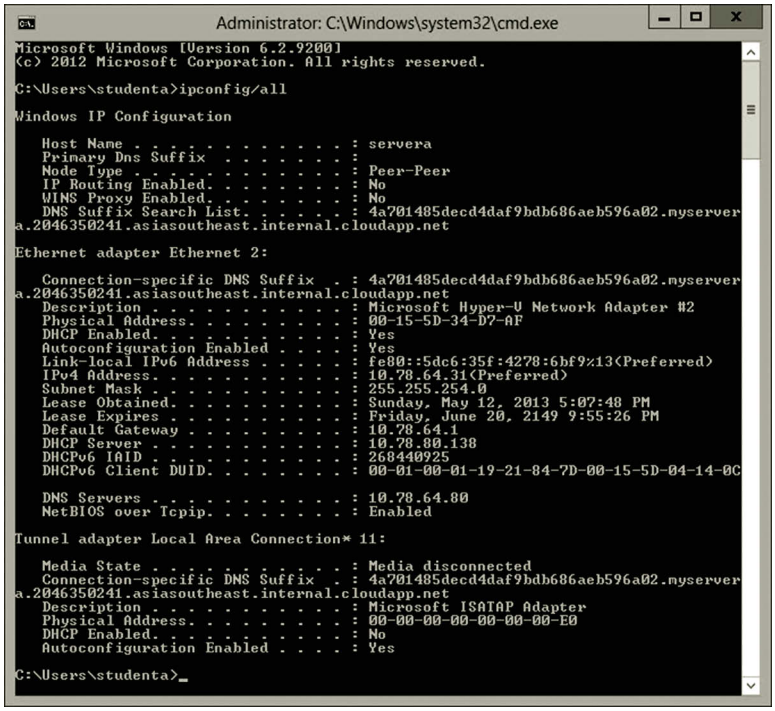

Figure 2.29 IP Information from servera.

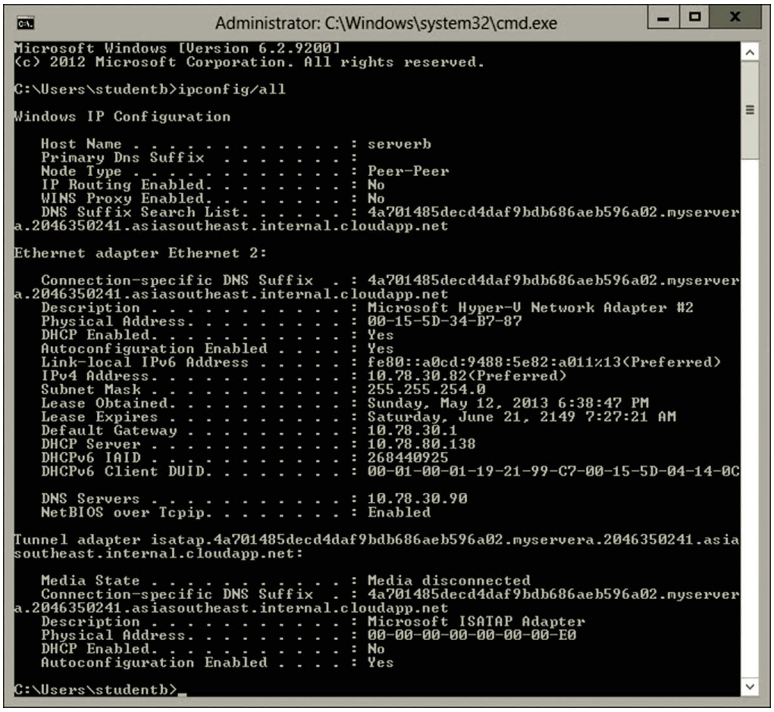

Figure 2.30 IP Information from serverb.

As shown in Figures 2.29 and 2.30, the private IP address for servera is 10.78.64.31 and the IP address for serverb is 10.78.30.82. Note that your IP address should be different from the ones illustrated in Figures 2.29 and 2.30.

Activity 2.3: Viewing Protocols with Network Monitor

The goal of this activity is to install the Network Monitor. Then, use Network Monitor to view some of the protocols introduced in this chapter.

Task 1: Installing Network Monitor

1. Assume that you have logged on to **servera**.
2. Click the **Start** icon on the Taskbar to open the Start menu. Then, click **Internet Explorer**.
3. After the browser is opened, click **Tools** icon and **Internet options**.
4. After the Internet Options dialog is opened, click the **Security** tab and click the **Internet** icon.
5. Click the **Custom level** button. Find the **File download** node on the list of security settings. Click the **Enable** option as shown in Figure 2.31.
6. Click **OK** twice to complete the configuration of Internet options.

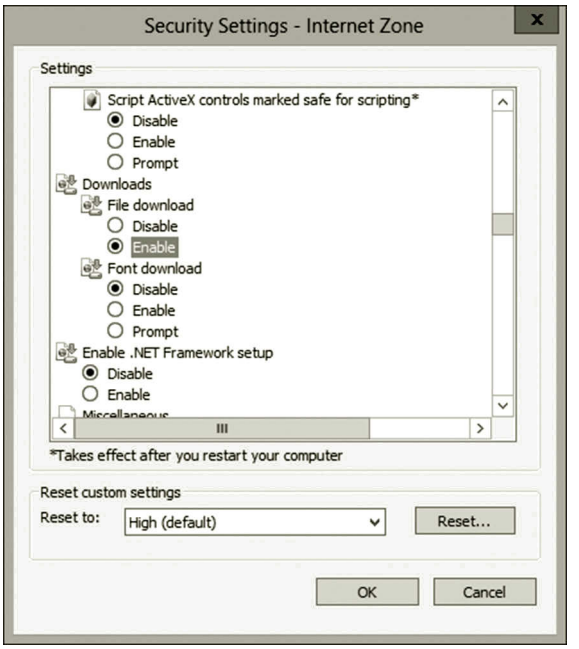

Figure 2.31 Enabling file download.

7. You may also need to temporarily turn off the IE Enhanced Security Configuration. To do so, On the Server Manager page, click **Local Server**. Then, turn off **IE Enhanced Security Configuration**.
8. You can now download Network Monitor from the following website (Microsoft Azure, Download Center, May, 2015). http://www.microsoft.com/en-us/download/?id%20=%204865.
9. From the website, download the **NM34_x64.exe** file. Then, **run** the file to install the **Typical** version of Microsoft Network Monitor.
10. Double click the icon of **Microsoft Network Monitor 3.4** on Desktop.
11. Network Monitor will be opened as shown in Figure 2.32. Then, close the Network Monitor window.

Task 2: Viewing TCP and HTTP

1. On your desktop, right click the **Network Monitor** icon and select **Run as administrator**.
2. Make sure **Ethernet** is checked as shown in Figure 2.33.
3. Click the link **New Capture** tab. Then, click **Start** on the menu bar (Figure 2.34).
4. Assume that Internet Explorer is still open, type the URL **http://go.microsoft.com**.
5. In the Network Monitor window, click the **Stop** menu.
6. Select the first **HTTP** packet under the Protocol Name column as shown in Figure 2.35.

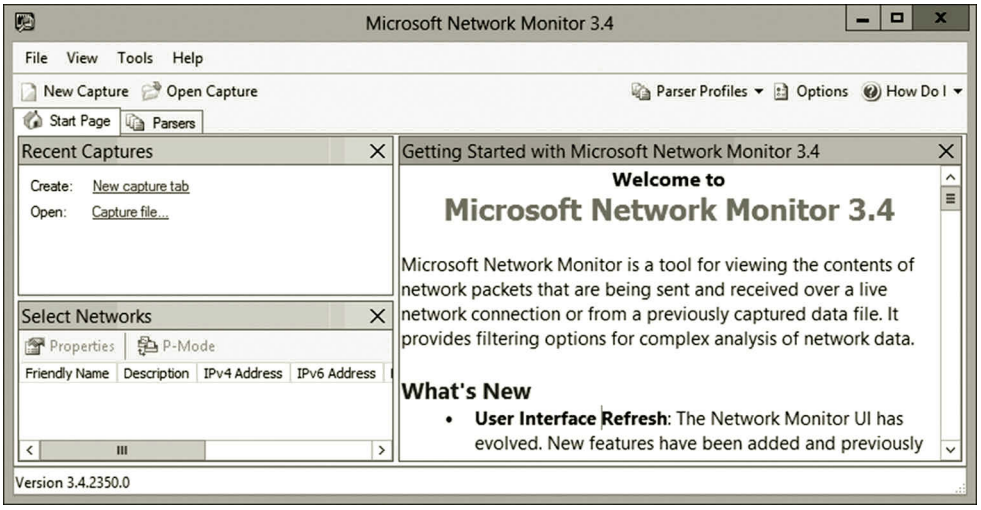

Figure 2.32 Network monitor.

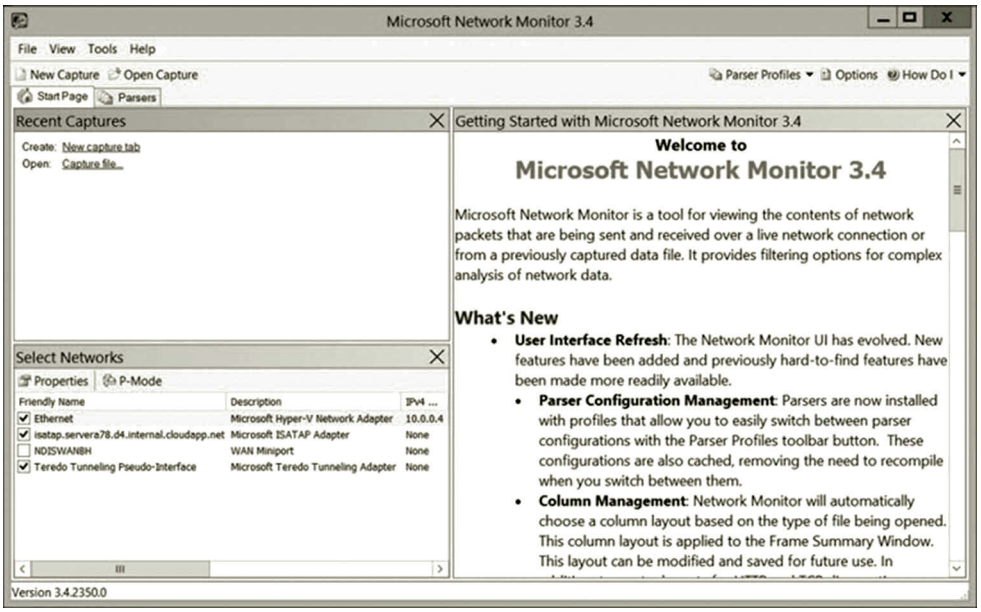

Figure 2.33 Checking exterior NIC for monitoring.

7. Then, expand the **HTTP** node in the Frame Details pane. As you can see in Figure 2.35, the protocol HTTP sends a requested file to the web server and the command GET is used to retrieve the data requested by the HTTP client.
8. In the Frame Summary pane, click the first **TCP** after HTTP under the Protocol Name column. Then, expand the **TCP** node in the Frame Details pane. As shown in Figure 2.36, the source port number is HTTP(80), and the destination port number is 49162. In the Frame Details pane, you can also find information of other items included in the TCP header.

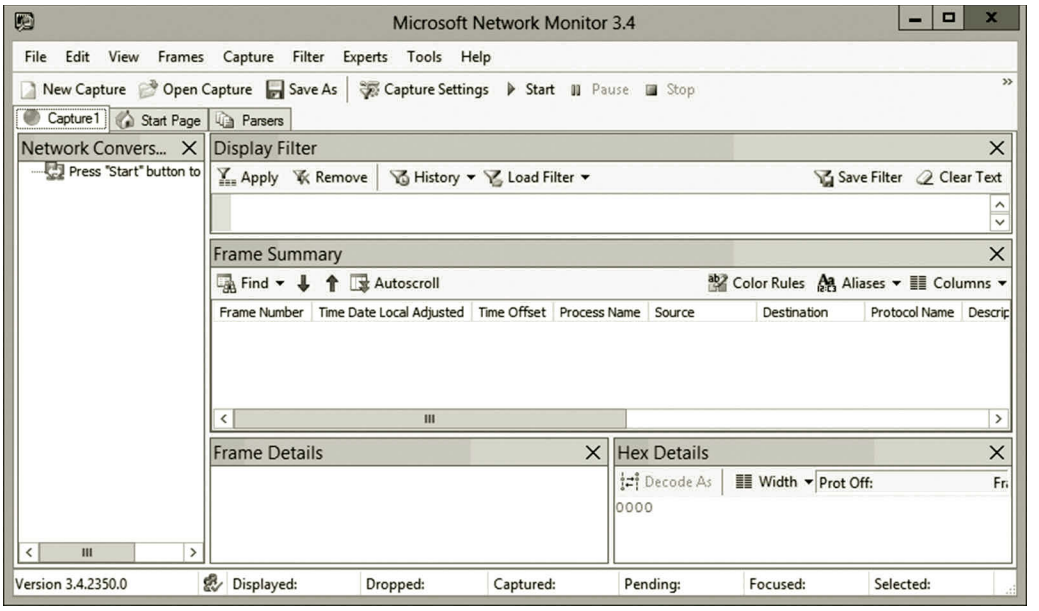

Figure 2.34 Starting to capture packets.

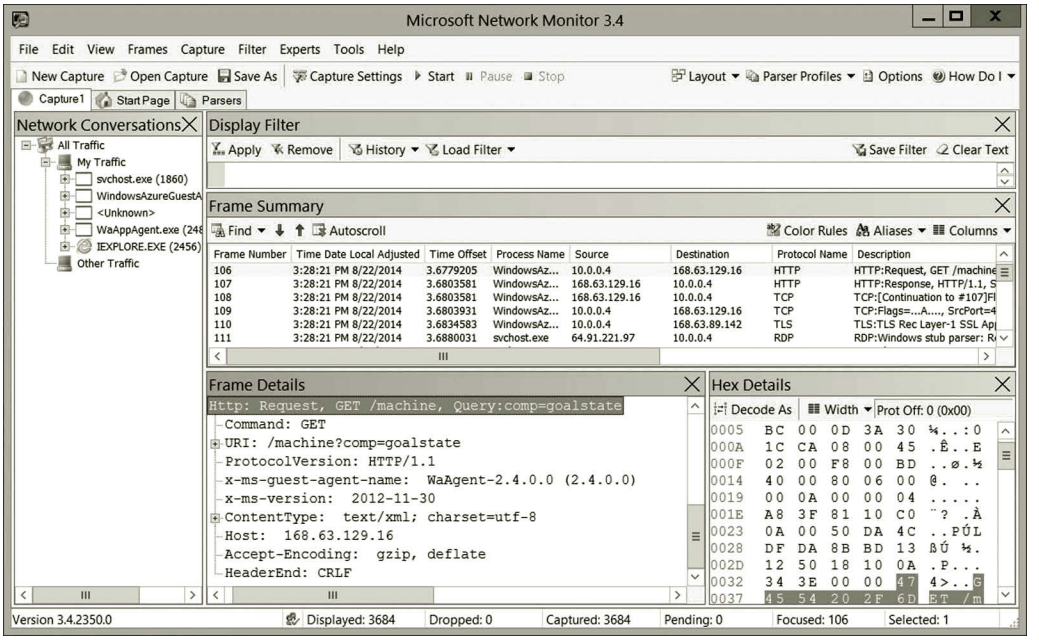

Figure 2.35 HTTP protocol.

Task 3: Viewing ARP and ICMP

1. To start the Command Prompt window, press the **Windows logo + r** key combination. In the Run dialog box, type **cmd** and then click **OK**.
2. In the Network Monitor window, click **Start** on the menu bar.

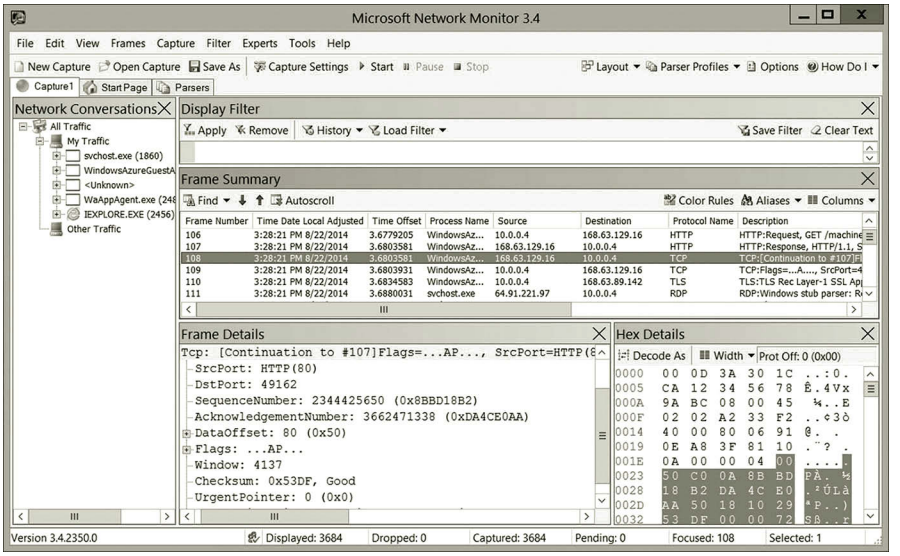

Figure 2.36 TCP protocol.

3. In command prompt window, type **ping 10.0.0.5**. Then, in the Network Monitor window, click the **Stop** menu.
4. Expand the ARP node as shown in Figure 2.37. The IP address has a corresponding MAC address (hardware address or physical address). Note that your IP address should be different from the one illustrated in Figure 2.37.
5. To view the ICMP protocol, click the **ICMP** packet under the Protocol Name column. Expand the **Icmp** node in the Frame Details pane. As shown in Figure 2.38, the message type is Echo Request Message.

Task 4: Viewing IP and UDP

1. To view the IP protocol, in the Network Monitor window, click **Start** on the menu bar. In Internet Explorer, enter the URL **http://go.microsoft.com**. In the Network Monitor window, click the **Stop** menu.
2. Click the first **DNS** packet under the Protocol Name column. Expand the **Ipv4** node in the Frame Details pane. As shown in Figure 2.39, the source IP address and destination IP address are specified in the IPv4 protocol. In the Frame Details pane, you can also view the configuration of other items in the IP header.
3. To view the UDP protocol, expand the **Udp** node in the Frame Details pane. As you can see, the UDP protocol communicates through the source port 62215 and the destination port 53 (Figure 2.40).
4. Close the Network Monitor window. When prompted to save the captured packets, click **No**.
5. In the Microsoft Azure Management Portal, shutdown both servera and serverb before exiting the Microsoft Azure Management Portal.

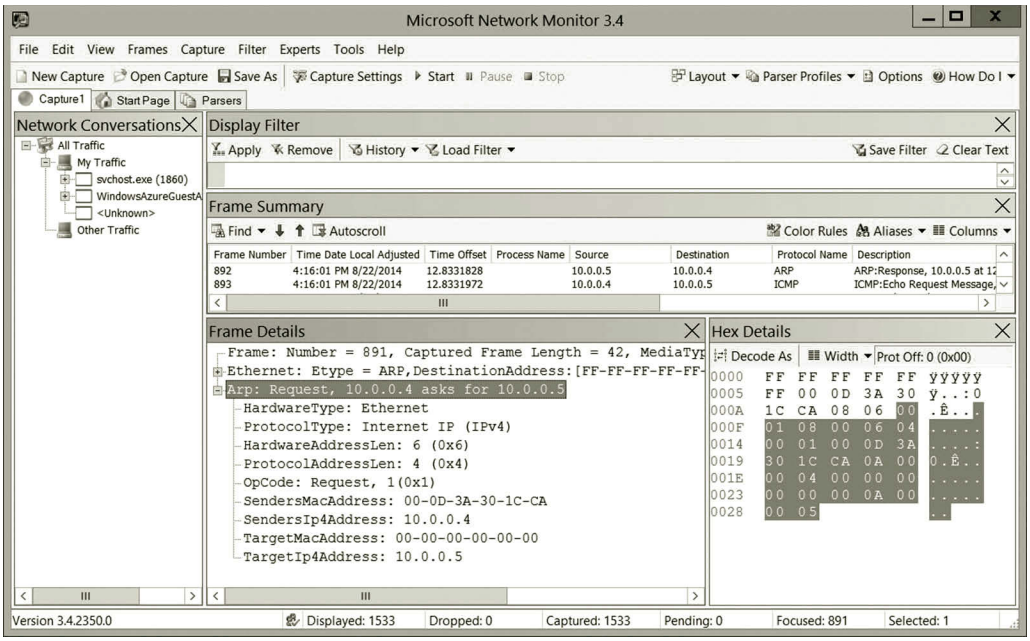

Figure 2.37 ARP protocol.

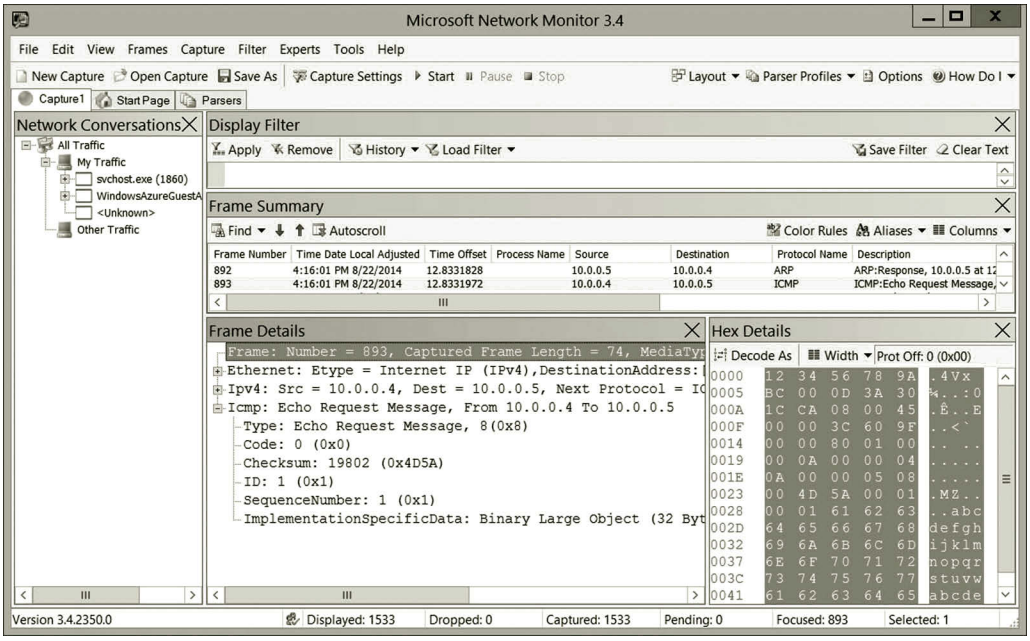

Figure 2.38 ICMP protocol.

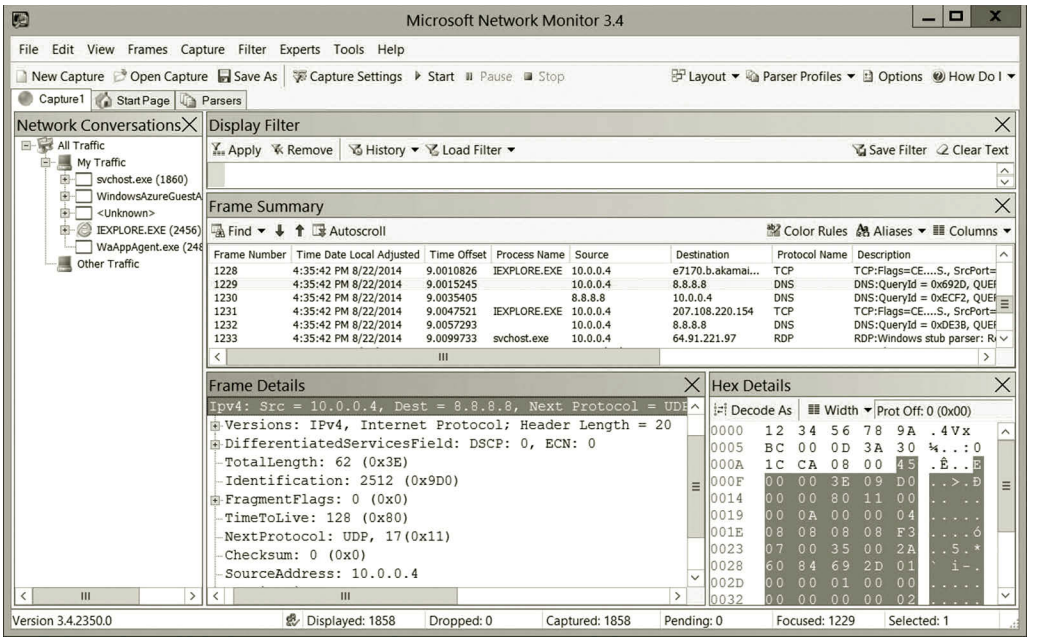

Figure 2.39 IPv4 protocol.

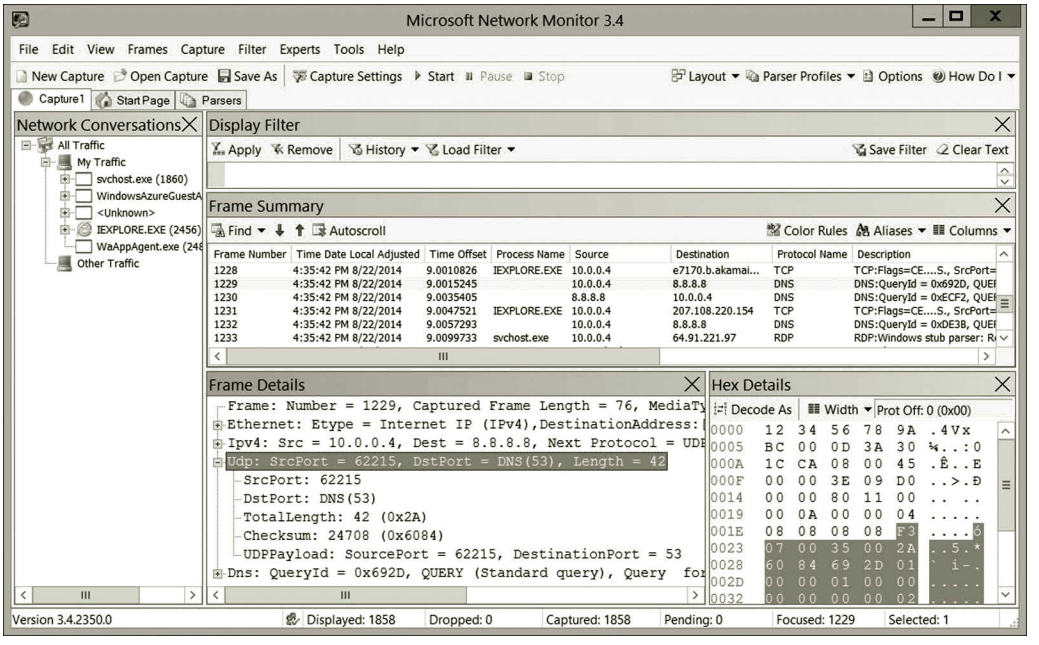

Figure 2.40 UDP protocol.

2.7 Summary

This chapter introduces some of the commonly used protocols in the TCP/IP architecture. Protocols are used to handle data communication between network hosts. This chapter shows how different protocols work together to deliver or receive data across networks. The relationships among these protocols are also illustrated through a protocol graph. The hands-on activities in this chapter explore various network management tools such as Server Manager, Command Prompt, and Network Monitor. The knowledge of protocols and network management tools covered in the next chapter will help design and develop networks.

Review Questions

1. What are the core protocols in the TCP/IP architecture?
2. What is HTTP used for?
3. What is DHCP used for?
4. The protocols SMTP, POP3, and IMAP are e-mail-related protocols. What are the differences among these protocols?
5. What makes SSH safer?
6. What can the network administrator do with LDAP?
7. What are the TCP features mentioned in this chapter?
8. What tasks discussed in this chapter can be handled by TCP?
9. What makes a TCP connection reliable?
10. How does TCP decide the waiting time before resending a packet?
11. What is the difference between UDP and TCP?
12. What is ARP used for?
13. Why do we need to replace IPv4 with IPv6?
14. What tasks mentioned in this chapter can be accomplished by IP?
15. What is encapsulation?
16. How can ICMP packets be transmitted across heterogeneous networks?
17. Describe the differences among the IP routing protocols: RIP, OSPF, and BGP.
18. What is the concern when we use PPTP for a VPN?
19. How does Ethernet work?
20. Compared with the copper wire, what are the advantages of optical fiber?