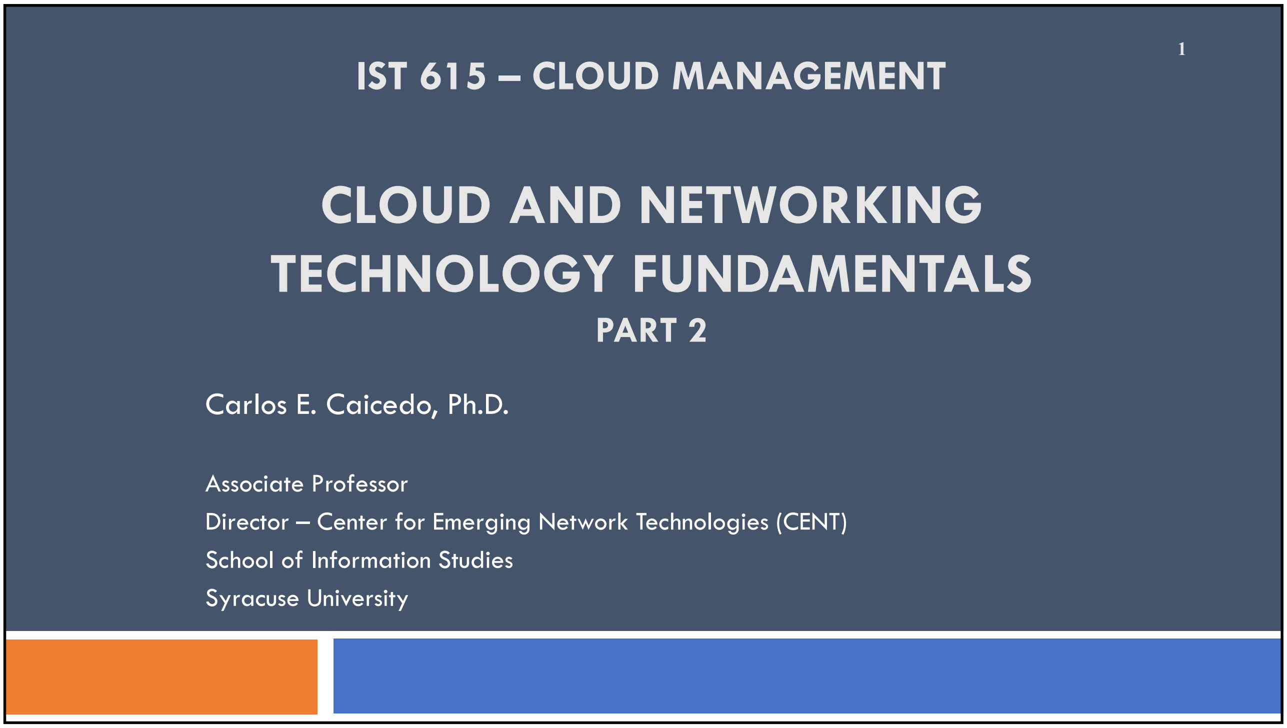


1

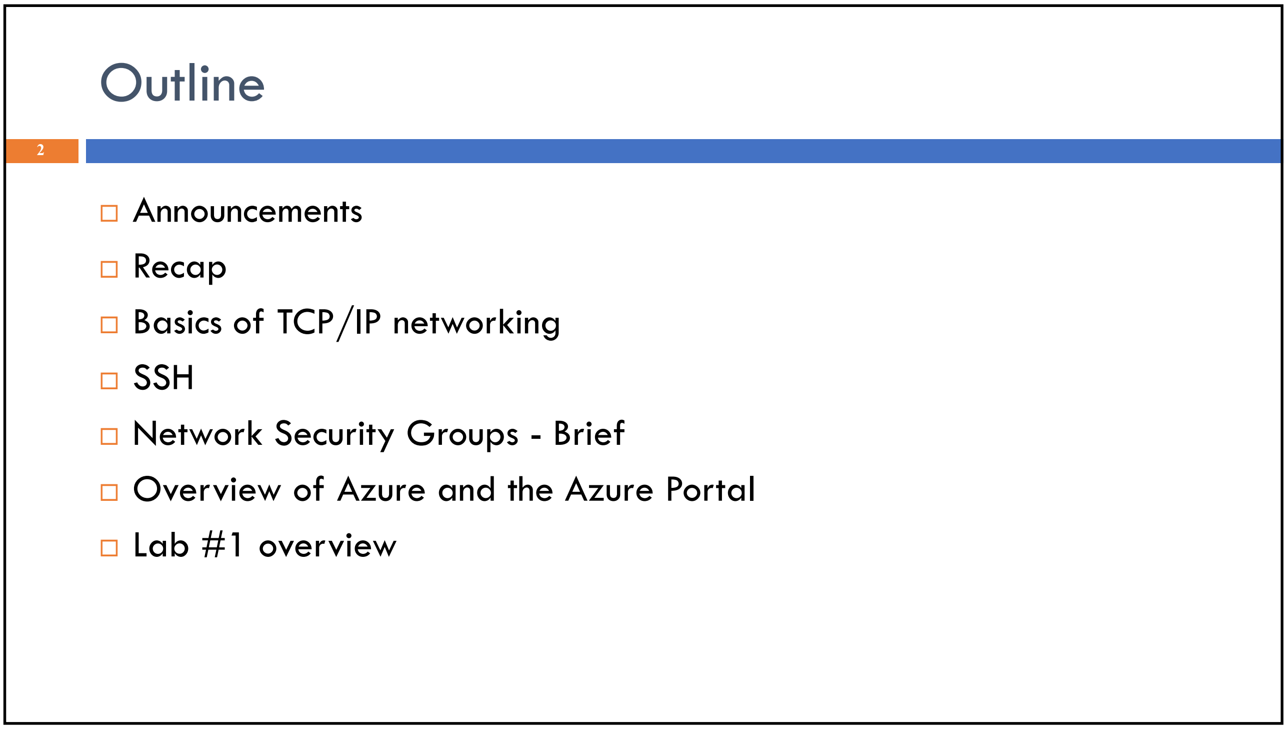
IST 615 – CLOUD MANAGEMENT

CLOUD AND NETWORKING TECHNOLOGY FUNDAMENTALS
PART 2

Carlos E. Caicedo, Ph.D.

Associate Professor
Director – Center for Emerging Network Technologies (CENT)
School of Information Studies
Syracuse University

1

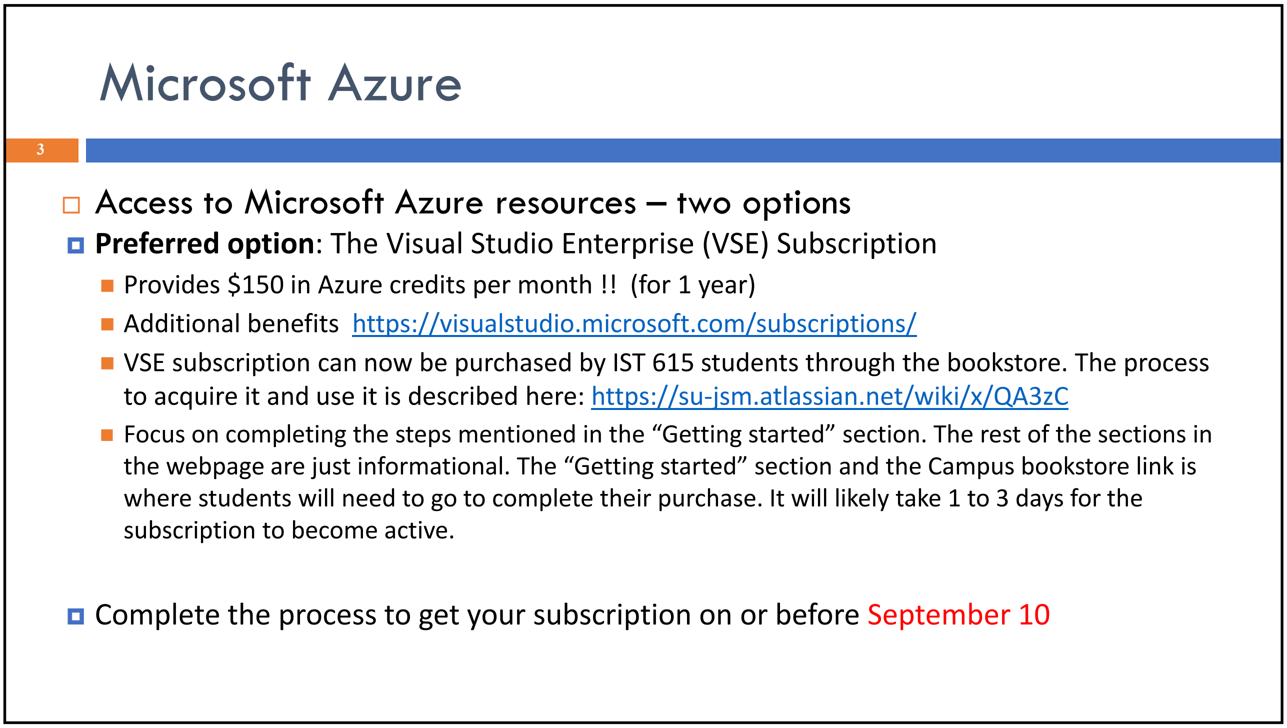


Outline

2

□ Announcements
□ Recap
□ Basics of TCP/IP networking
□ SSH
□ Network Security Groups - Brief
□ Overview of Azure and the Azure Portal
□ Lab #1 overview

2

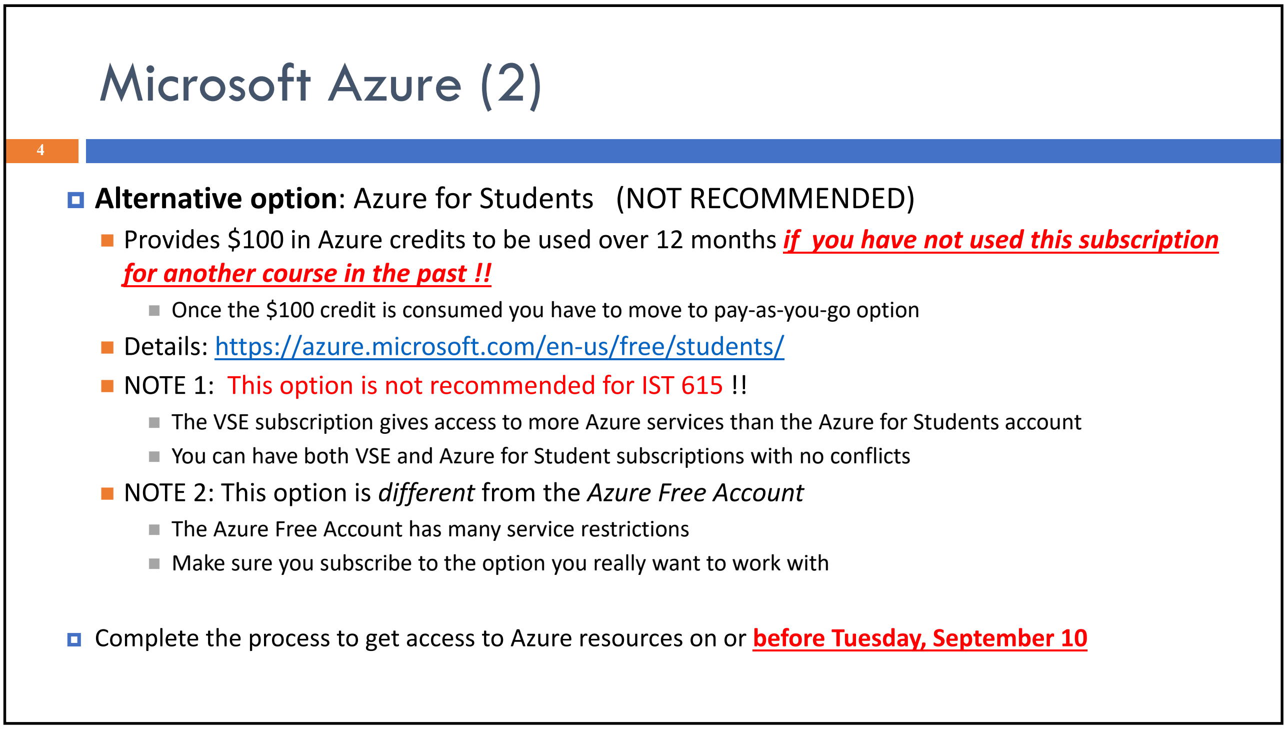


Microsoft Azure

3

- Access to Microsoft Azure resources – two options
- **Preferred option**: The Visual Studio Enterprise (VSE) Subscription
  - Provides $150 in Azure credits per month !! (for 1 year)
  - Additional benefits https://visualstudio.microsoft.com/subscriptions/
  - VSE subscription can now be purchased by IST 615 students through the bookstore. The process to acquire it and use it is described here: https://su-jsm.atlassian.net/wiki/x/QA3zC
  - Focus on completing the steps mentioned in the "Getting started" section. The rest of the sections in the webpage are just informational. The "Getting started" section and the Campus bookstore link is where students will need to go to complete their purchase. It will likely take 1 to 3 days for the subscription to become active.
- Complete the process to get your subscription on or before September 10

3

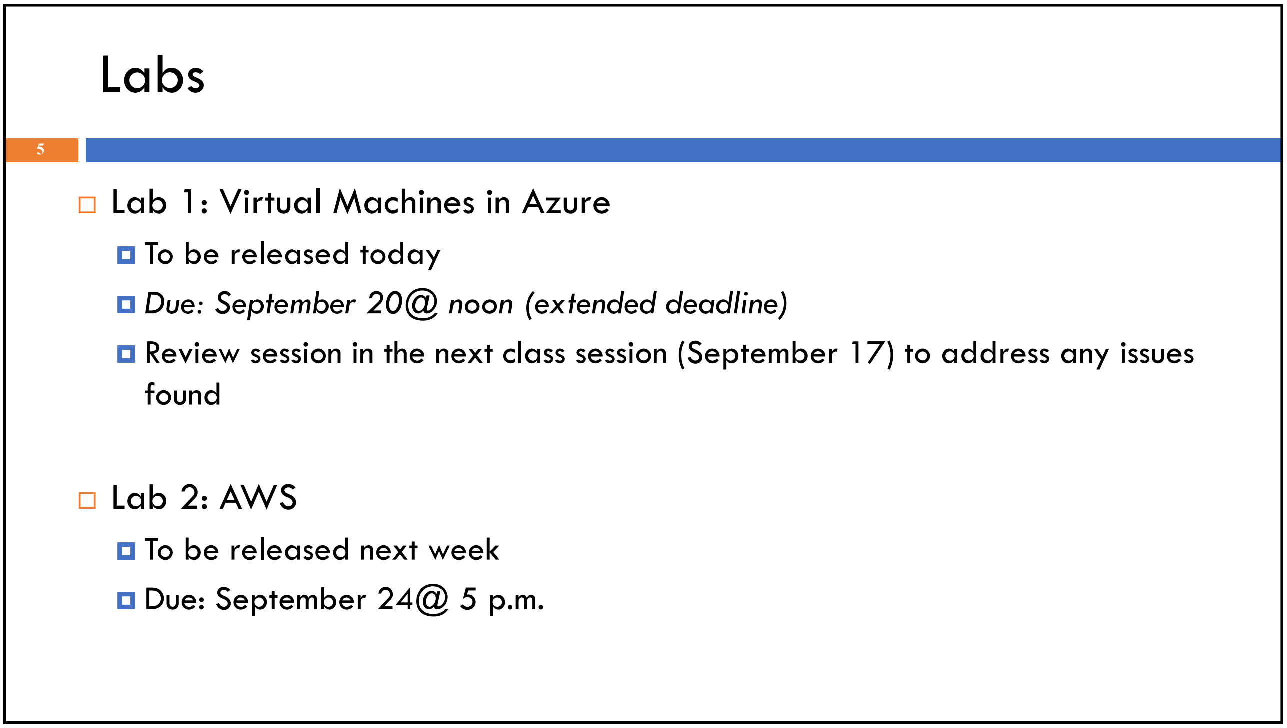


Microsoft Azure (2)

4

- **Alternative option**: Azure for Students (NOT RECOMMENDED)
  - Provides $100 in Azure credits to be used over 12 months ***if you have not used this subscription for another course in the past !!***
    - Once the $100 credit is consumed you have to move to pay-as-you-go option
  - Details: https://azure.microsoft.com/en-us/free/students/
  - NOTE 1: This option is not recommended for IST 615 !!
    - The VSE subscription gives access to more Azure services than the Azure for Students account
    - You can have both VSE and Azure for Student subscriptions with no conflicts
  - NOTE 2: This option is *different* from the *Azure Free Account*
    - The Azure Free Account has many service restrictions
    - Make sure you subscribe to the option you really want to work with
- Complete the process to get access to Azure resources on or **before Tuesday, September 10**

4

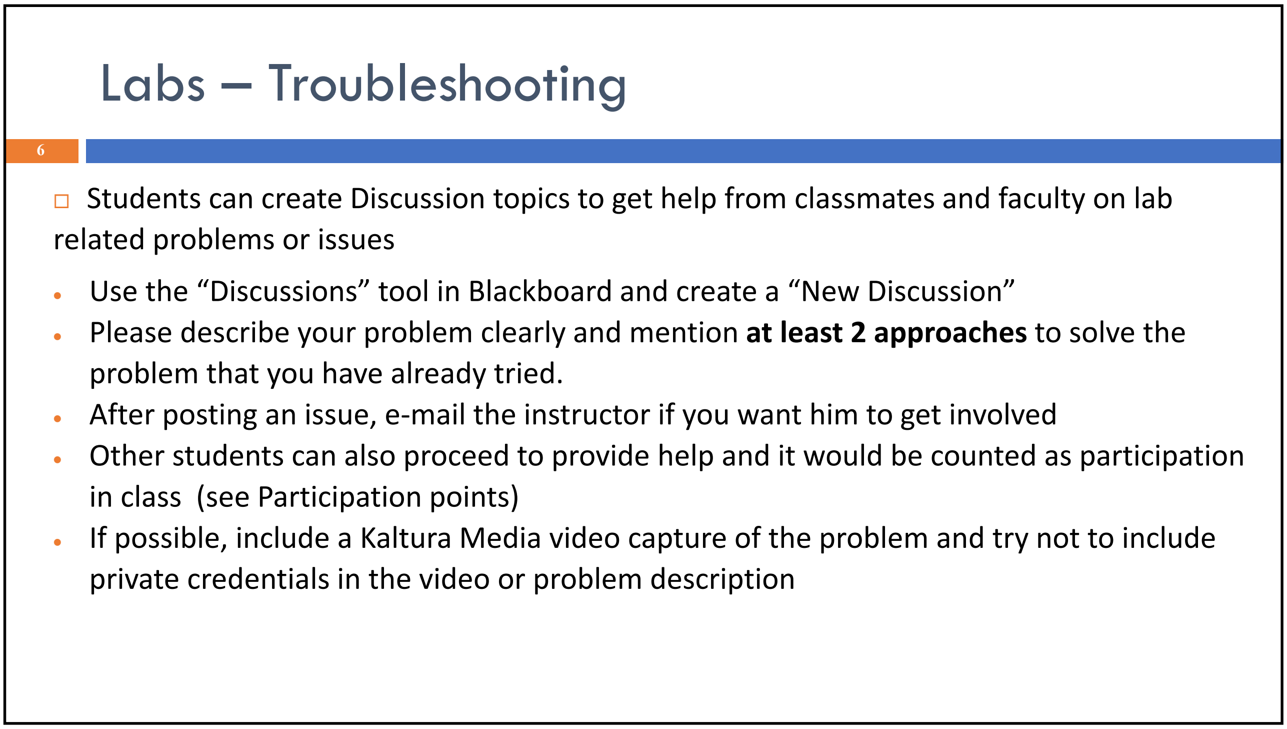


Labs

5

- Lab 1: Virtual Machines in Azure
  - To be released today
  - *Due: September 20@ noon (extended deadline)*
  - Review session in the next class session (September 17) to address any issues found
- Lab 2: AWS
  - To be released next week
  - Due: September 24@ 5 p.m.

5

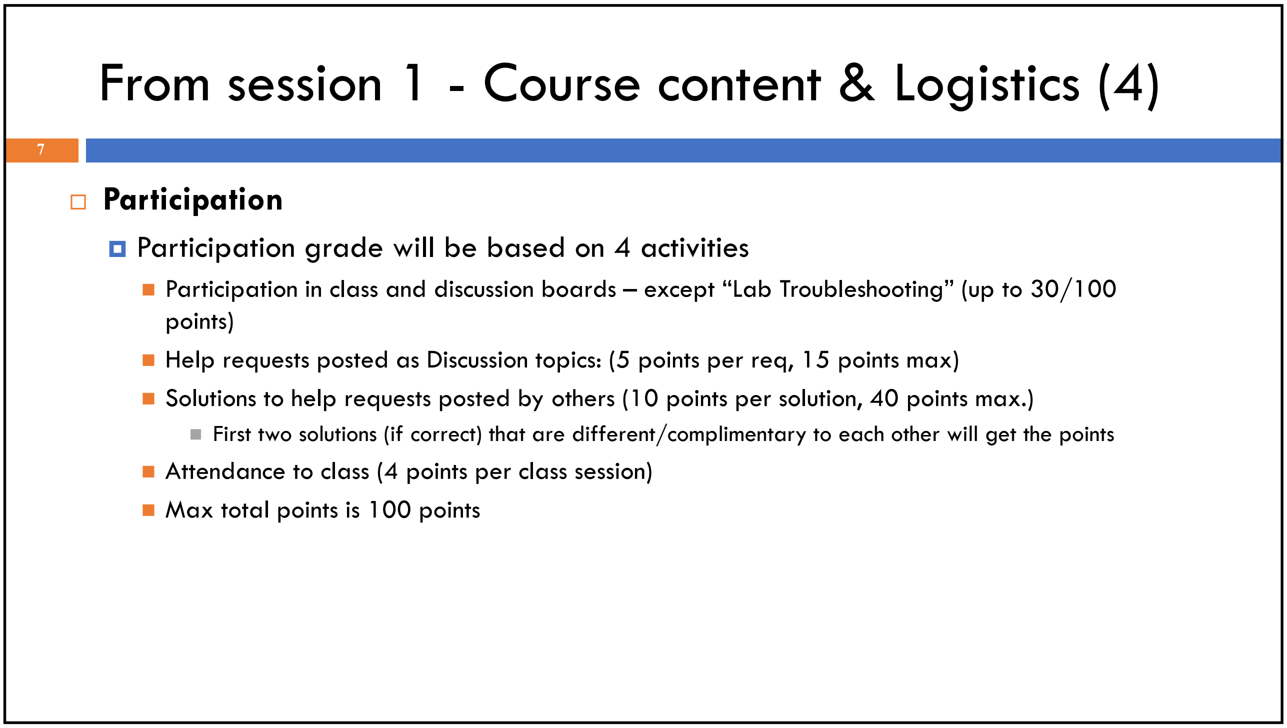


Labs – Troubleshooting

6

- Students can create Discussion topics to get help from classmates and faculty on lab related problems or issues
- Use the “Discussions” tool in Blackboard and create a “New Discussion”
- Please describe your problem clearly and mention **at least 2 approaches** to solve the problem that you have already tried.
- After posting an issue, e-mail the instructor if you want him to get involved
- Other students can also proceed to provide help and it would be counted as participation in class (see Participation points)
- If possible, include a Kaltura Media video capture of the problem and try not to include private credentials in the video or problem description

6

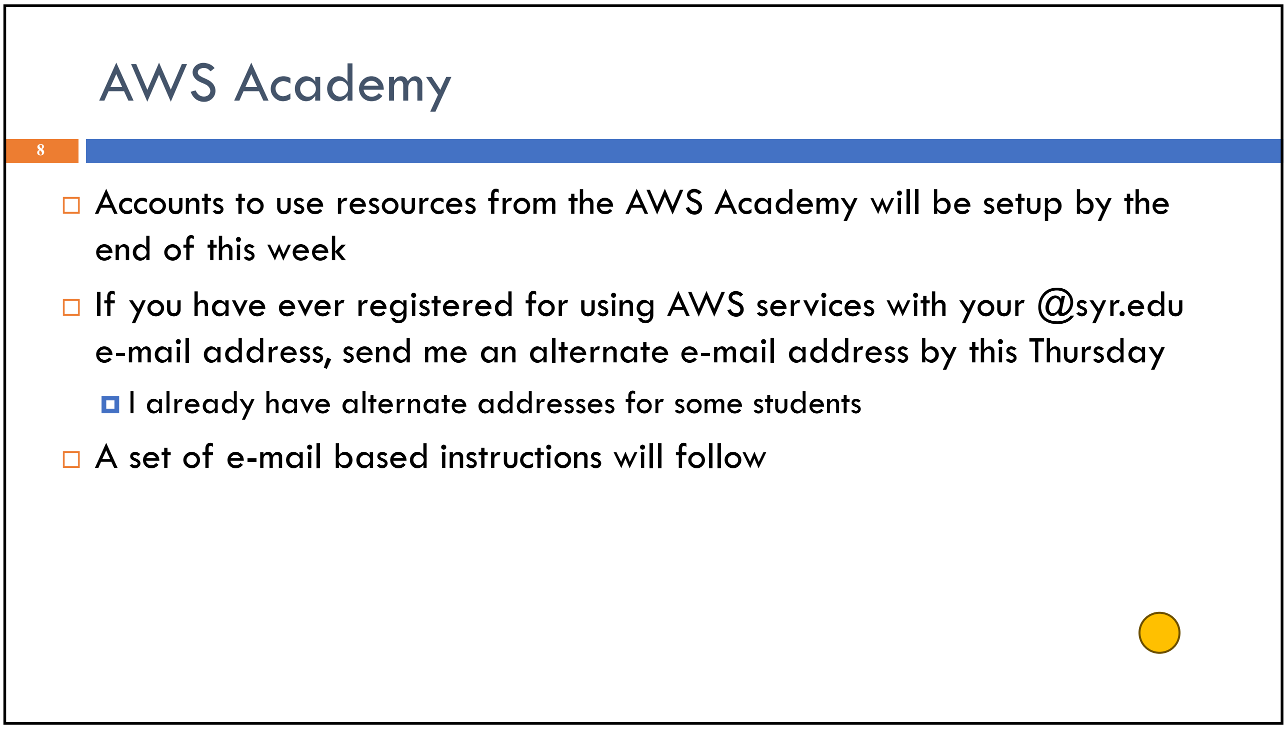


From session 1 - Course content & Logistics (4)

7

- **Participation**
  - Participation grade will be based on 4 activities
    - Participation in class and discussion boards – except “Lab Troubleshooting” (up to 30/100 points)
    - Help requests posted as Discussion topics: (5 points per req, 15 points max)
    - Solutions to help requests posted by others (10 points per solution, 40 points max.)
      - First two solutions (if correct) that are different/complimentary to each other will get the points
    - Attendance to class (4 points per class session)
    - Max total points is 100 points

7

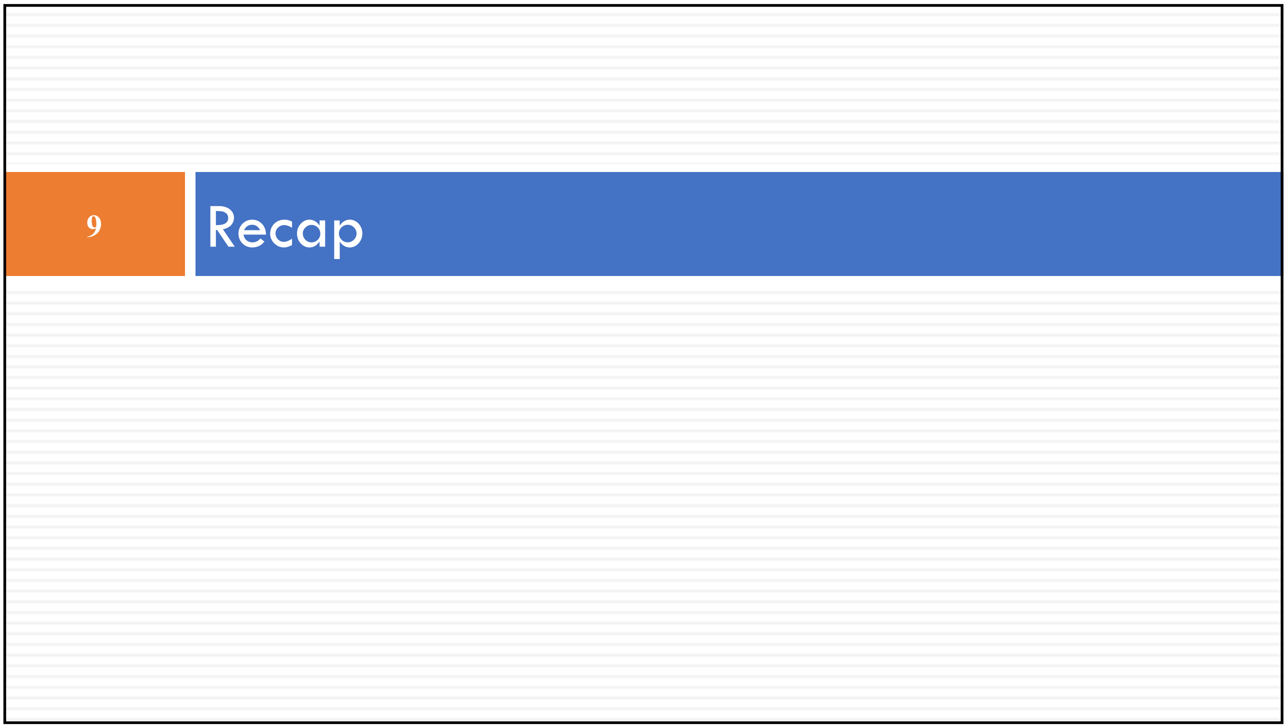


AWS Academy

8

- Accounts to use resources from the AWS Academy will be setup by the end of this week
- If you have ever registered for using AWS services with your @syr.edu e-mail address, send me an alternate e-mail address by this Thursday
  - I already have alternate addresses for some students
- A set of e-mail based instructions will follow

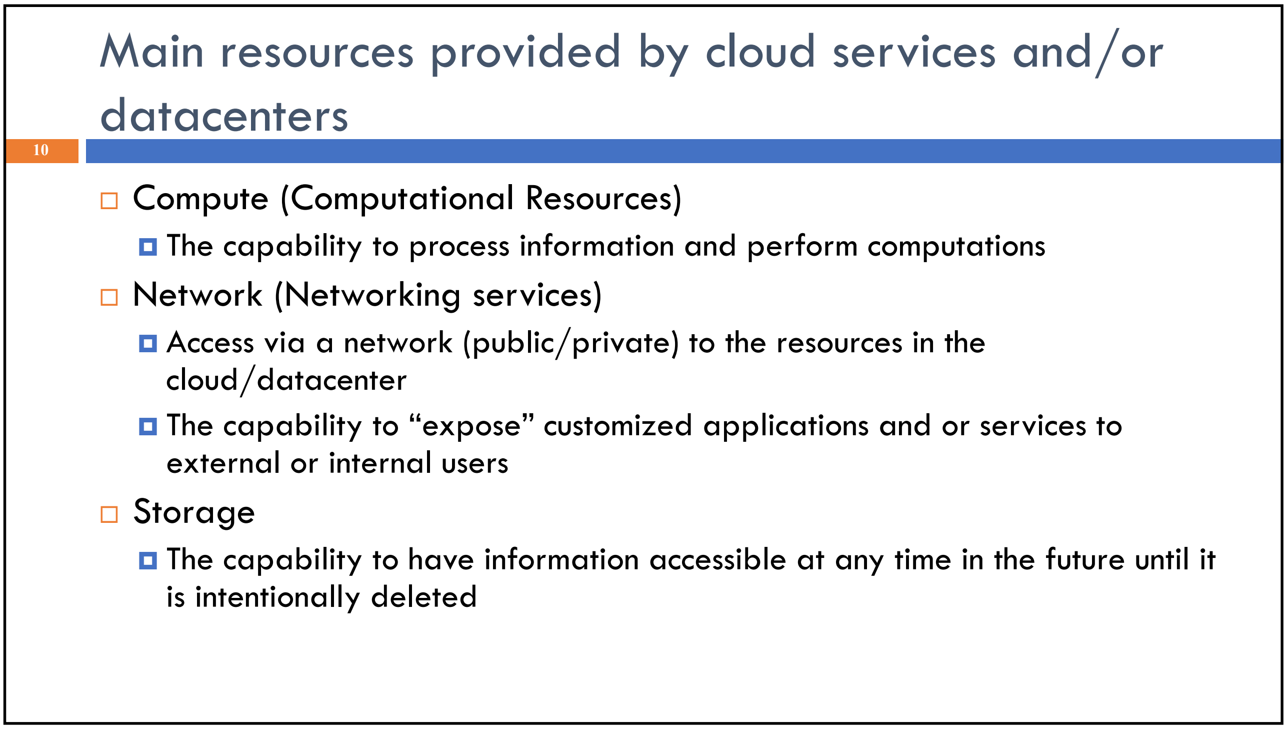
8



9

Recap

9

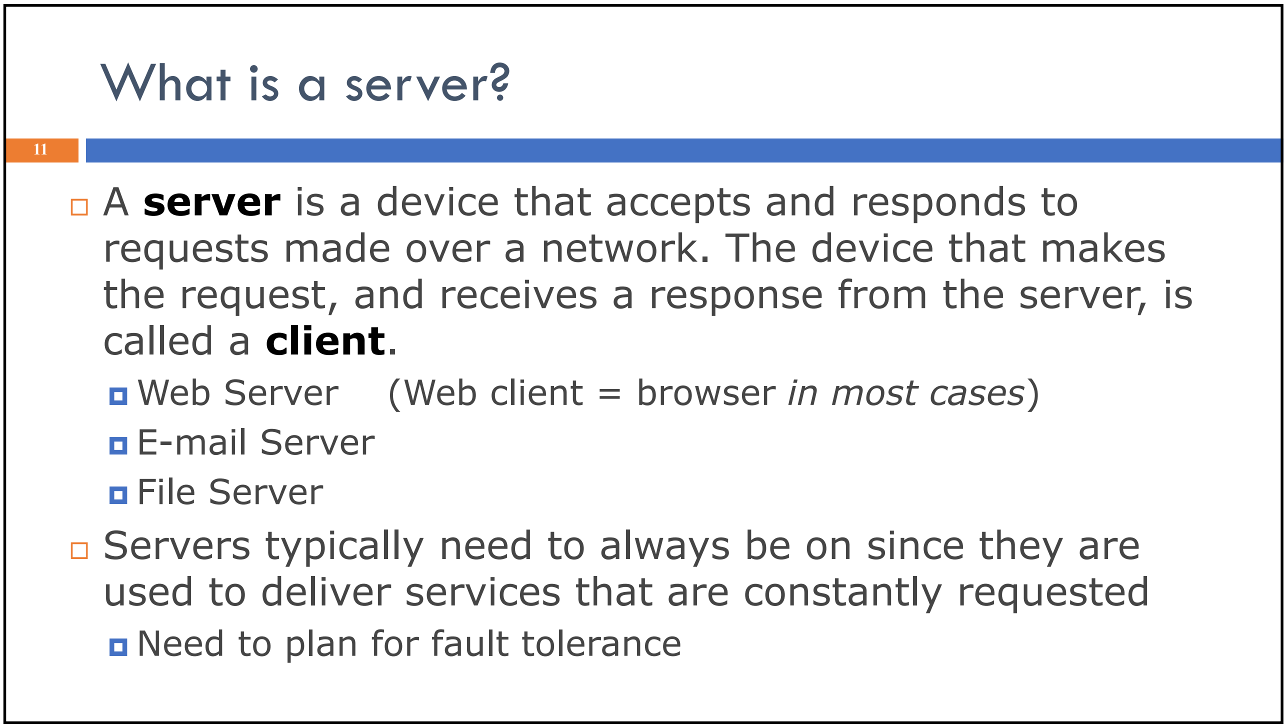


Main resources provided by cloud services and/or datacenters

10

- Compute (Computational Resources)
  - The capability to process information and perform computations
- Network (Networking services)
  - Access via a network (public/private) to the resources in the cloud/datacenter
  - The capability to "expose" customized applications and or services to external or internal users
- Storage
  - The capability to have information accessible at any time in the future until it is intentionally deleted

10

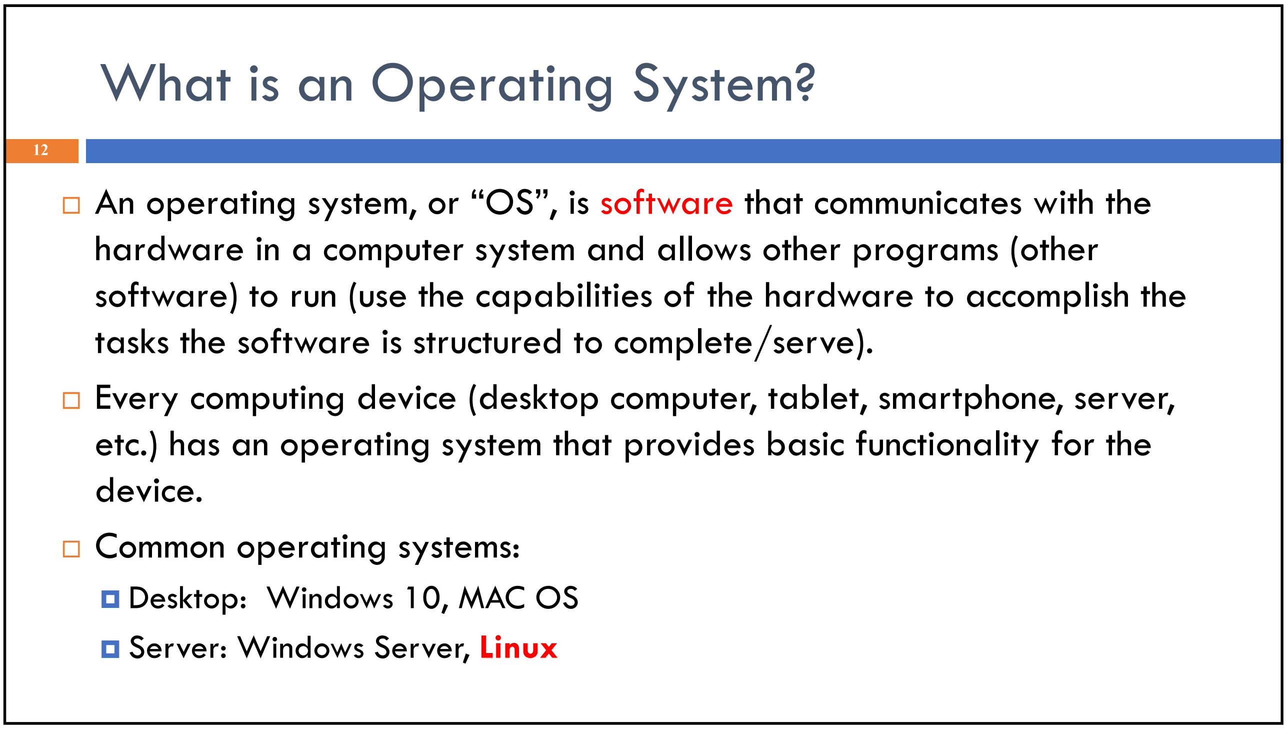


What is a server?

11

- A **server** is a device that accepts and responds to requests made over a network. The device that makes the request, and receives a response from the server, is called a **client**.
  - Web Server (Web client = browser *in most cases*)
  - E-mail Server
  - File Server
- Servers typically need to always be on since they are used to deliver services that are constantly requested
  - Need to plan for fault tolerance

11



What is an Operating System?

12

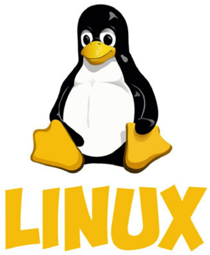
- An operating system, or “OS”, is software that communicates with the hardware in a computer system and allows other programs (other software) to run (use the capabilities of the hardware to accomplish the tasks the software is structured to complete/serve).
- Every computing device (desktop computer, tablet, smartphone, server, etc.) has an operating system that provides basic functionality for the device.
- Common operating systems:
  - Desktop: Windows 10, MAC OS
  - Server: Windows Server, **Linux**

12

Linux

13

- Main components
  - Linux Kernel
  - GNU (GNU is Not Unix) Software
  - Software Package management
  - Other packages



- Has been ported from Intel x86 architecture processors to many others
  - Alpha, VAX, PowerPC, IBM S/390, MIPS, IA-64,…
  - “Embedded” in many commercial devices
    - Wearables, cameras, etc.

13

Application Program Interface (API)

14

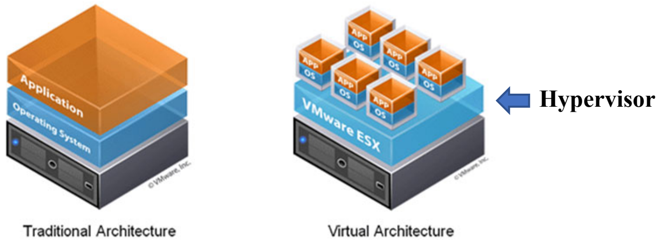
- An ***a****pplication* ***p****rogram* ***i****nterface* (**API**) is a set of routines, protocols, and tools for building software applications.
  - Specifies how software components should interact
  - Simplifies application development by abstracting the underlying implementation details and only exposing information (objects) or actions that the developer needs.
  - Includes specifications for some or all of:
    - software routines (functions)
    - data structures
    - object classes
    - variables
    - remote procedure calls
  - https://www.youtube.com/watch?v=s7wmiS2mSXY

14

Virtualization

15

- What is Virtualization?
  - Virtualization is the creation of a virtual resource or device on a platform where the operational environment of the platform divides the resource into one or more execution environments
- Examples of Virtualization
  - Virtual drives
  - Virtual memory
  - Virtual machines
  - Virtual servers



15

Hypervisor

16

- Also called a virtual machine manager (VMM)
- Software that allows multiple operating systems to share a single hardware host
  - Each operating system appears to have the host's processor, memory, and other resources all to itself
- Controls the host system processor and resources (memory, disk, network), allocating what is needed to each operating system
- Makes sure that each guest system (each *virtual machine*) does not affect other guest systems

16

Containers – Introduction

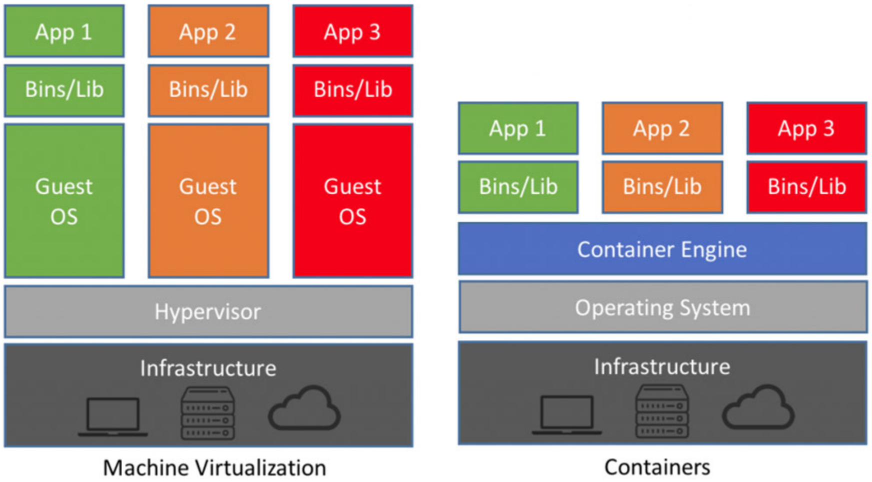
17

- Containers virtualize the OS just like hypervisors virtualizes the hardware
- Containers wrap up a piece of software in a complete filesystem that contains everything it needs to run such as : code, runtime, system tools, libraries etc.
- Containers share the OS kernel, binaries and/or libraries where needed
  - Any differences are limited to each container

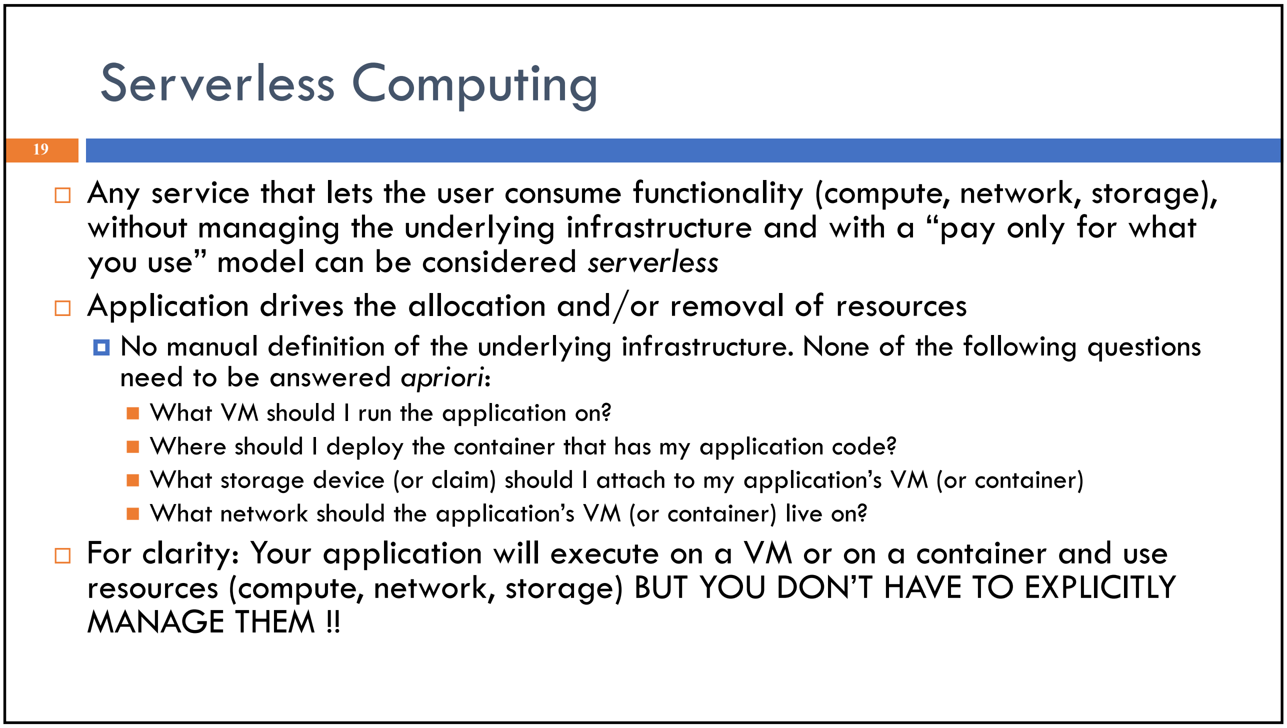
17

VMs vs. Containers

18



18

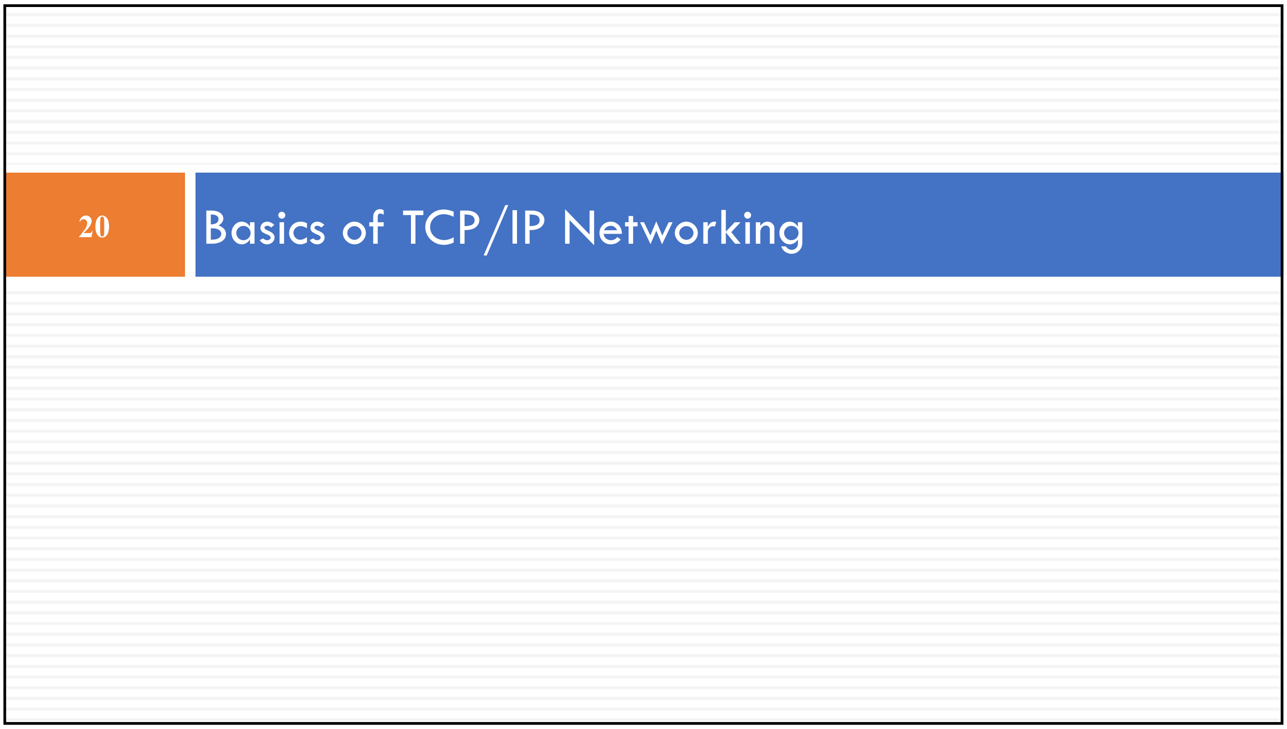


Serverless Computing

19

- □ Any service that lets the user consume functionality (compute, network, storage), without managing the underlying infrastructure and with a "pay only for what you use" model can be considered *serverless*
- □ Application drives the allocation and/or removal of resources
  - No manual definition of the underlying infrastructure. None of the following questions need to be answered *apriori*:
    - What VM should I run the application on?
    - Where should I deploy the container that has my application code?
    - What storage device (or claim) should I attach to my application's VM (or container)
    - What network should the application's VM (or container) live on?
- □ For clarity: Your application will execute on a VM or on a container and use resources (compute, network, storage) BUT YOU DON'T HAVE TO EXPLICITLY MANAGE THEM !!

19



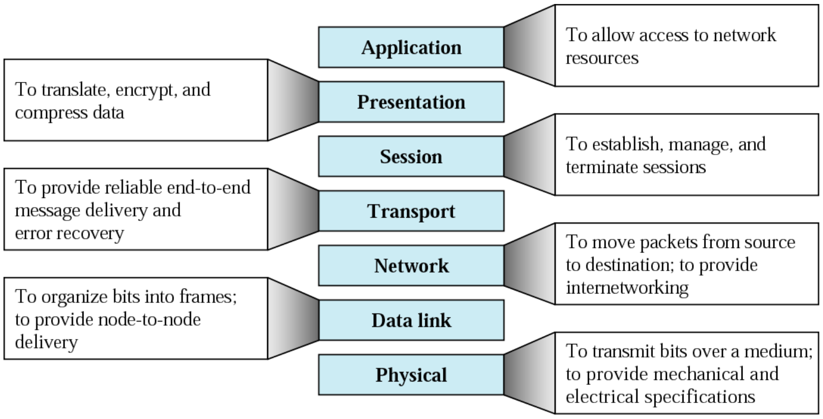
20

Basics of TCP/IP Networking

20

Summary of the OSI Reference Model

21



To allow access to network resources

To translate, encrypt, and compress data

To establish, manage, and terminate sessions

To provide reliable end-to-end message delivery and error recovery

To move packets from source to destination; to provide internetworking

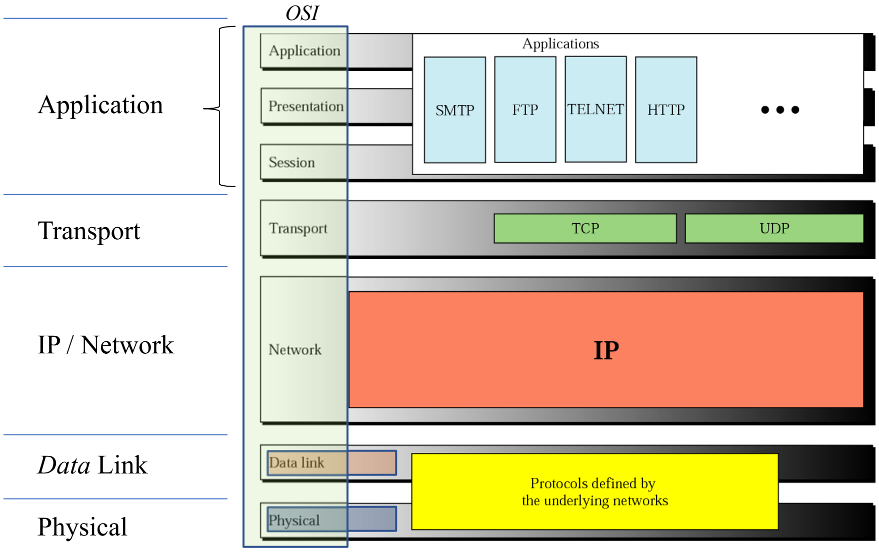
To organize bits into frames; to provide node-to-node delivery

To transmit bits over a medium; to provide mechanical and electrical specifications

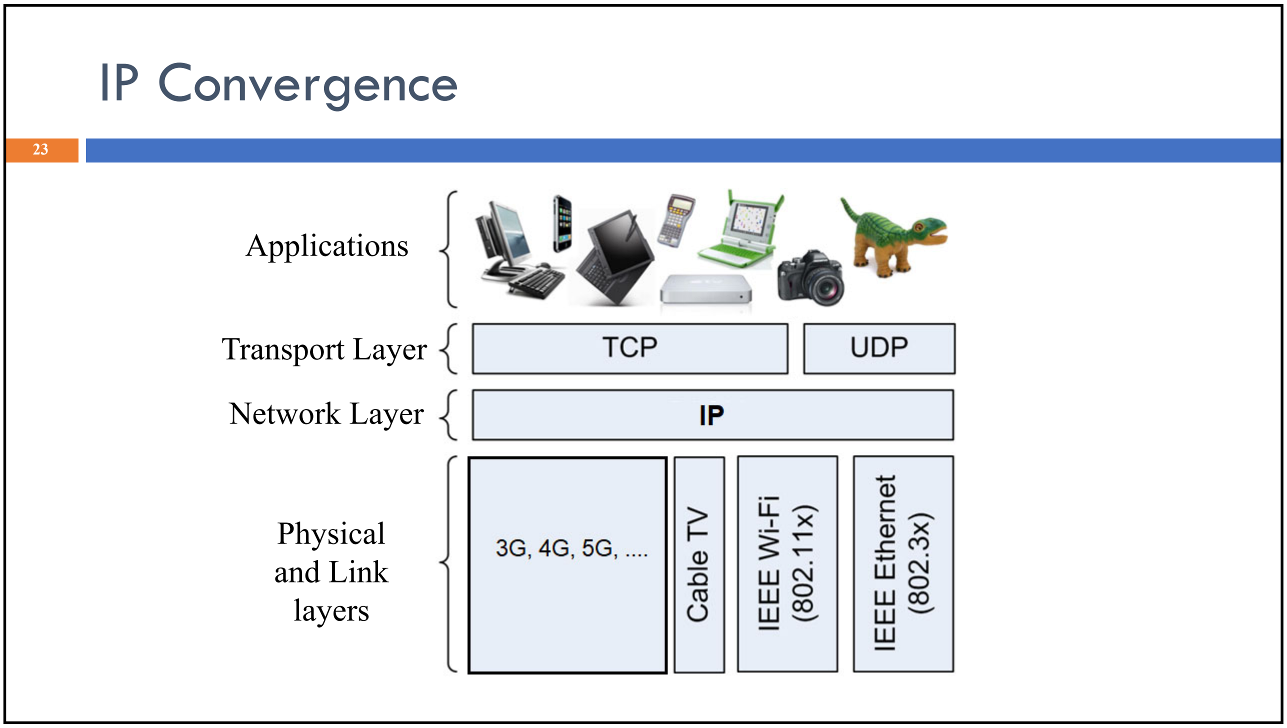
21

Internet Architecture

22



22



IP Convergence

23

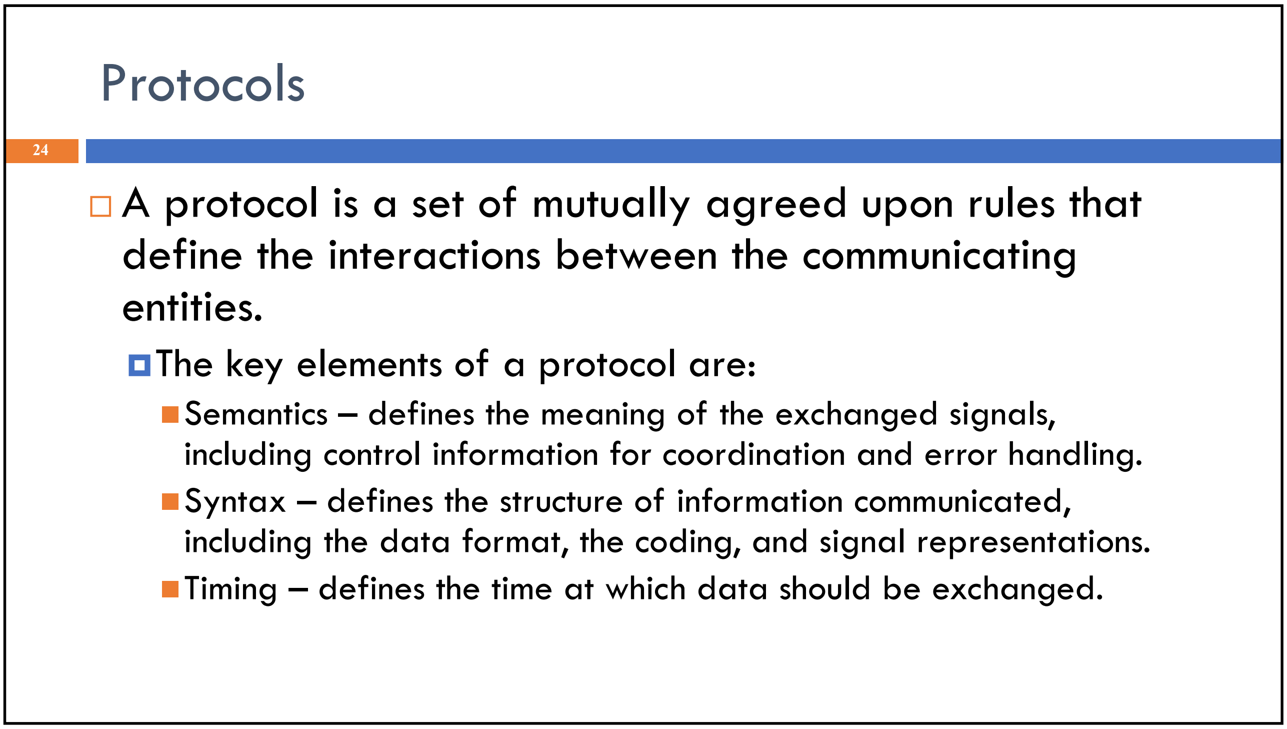
Applications

Transport Layer: TCP | UDP

Network Layer: IP

Physical and Link layers: 3G, 4G, 5G, ... | Cable TV | IEEE Wi-Fi (802.11x) | IEEE Ethernet (802.3x)

23

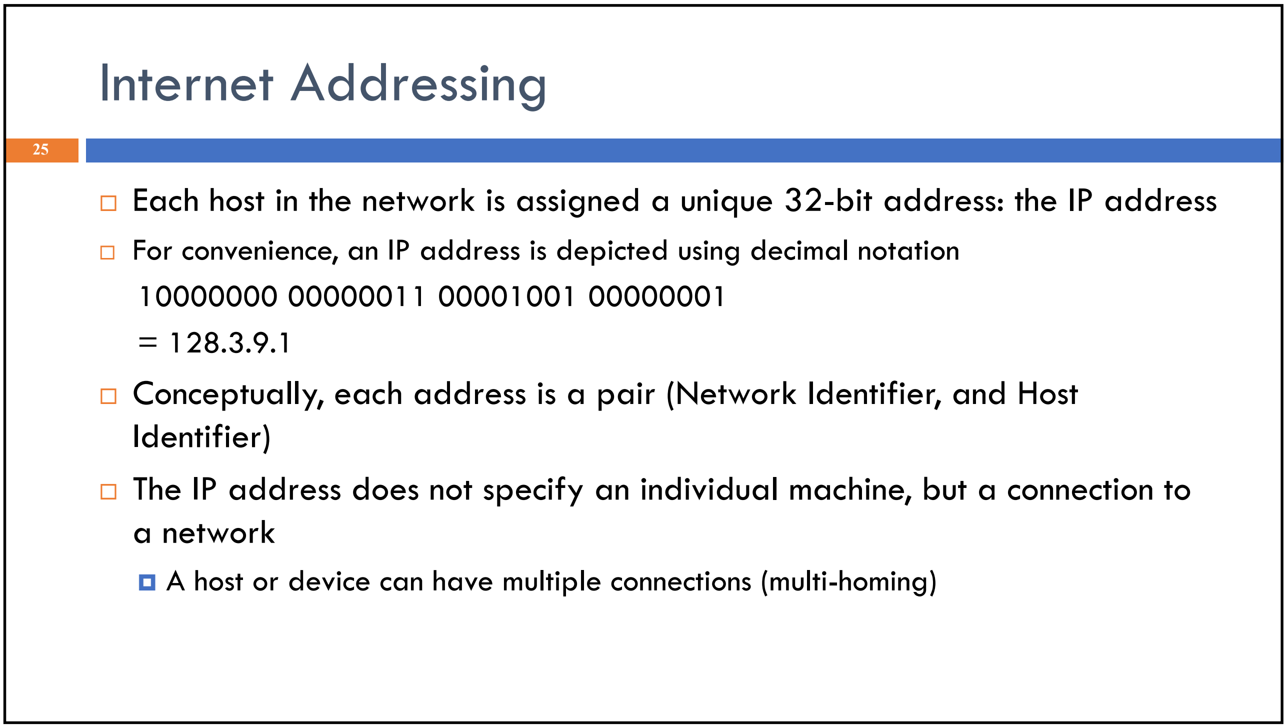


Protocols

24

- A protocol is a set of mutually agreed upon rules that define the interactions between the communicating entities.
  - The key elements of a protocol are:
    - Semantics – defines the meaning of the exchanged signals, including control information for coordination and error handling.
    - Syntax – defines the structure of information communicated, including the data format, the coding, and signal representations.
    - Timing – defines the time at which data should be exchanged.

24



Internet Addressing

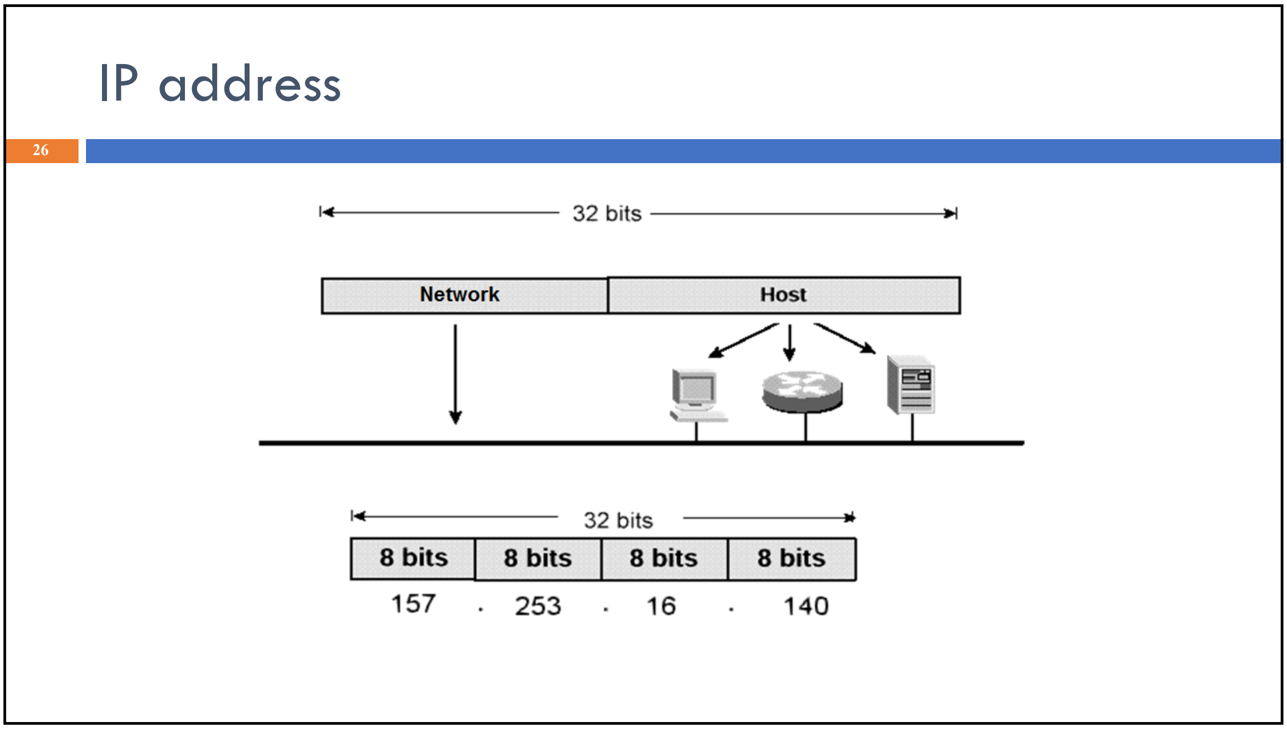
25

- □ Each host in the network is assigned a unique 32-bit address: the IP address
- □ For convenience, an IP address is depicted using decimal notation

  10000000 00000011 00001001 00000001

  = 128.3.9.1
- □ Conceptually, each address is a pair (Network Identifier, and Host Identifier)
- □ The IP address does not specify an individual machine, but a connection to a network
  - ◘ A host or device can have multiple connections (multi-homing)

25



IP address

26

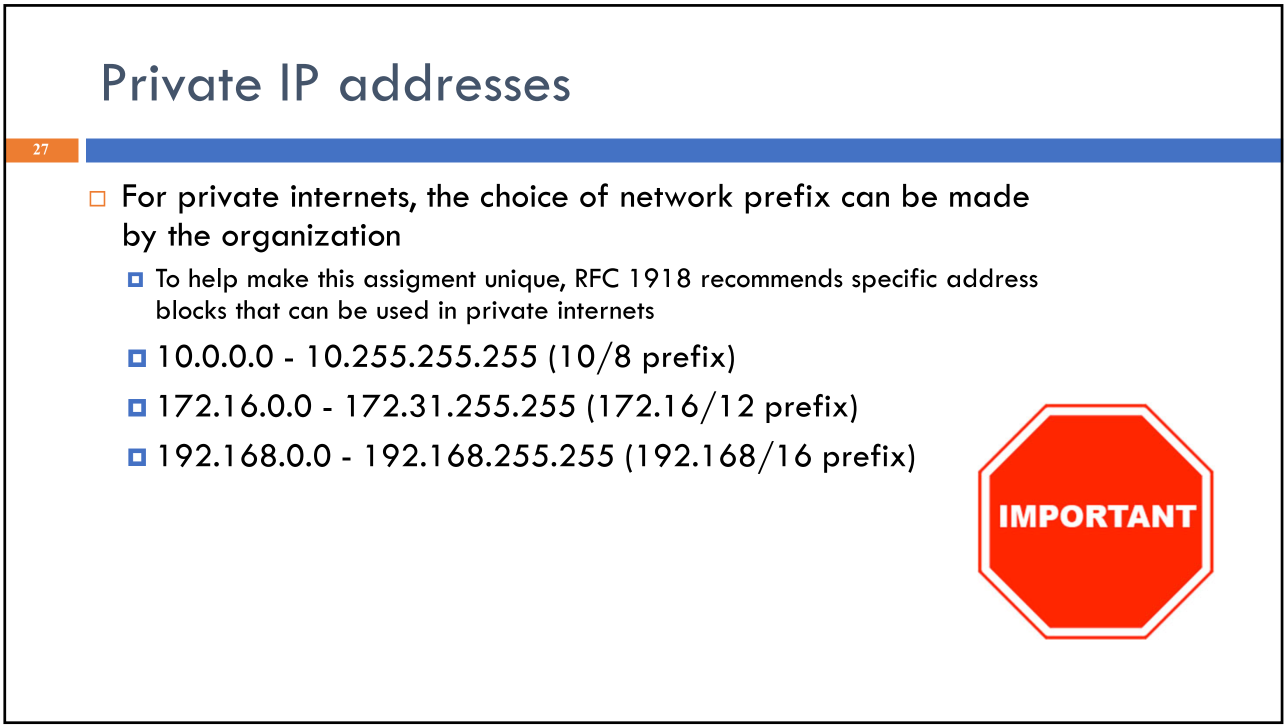
32 bits

Network | Host

32 bits

8 bits	8 bits	8 bits	8 bits
157 .	253 .	16 .	140

26

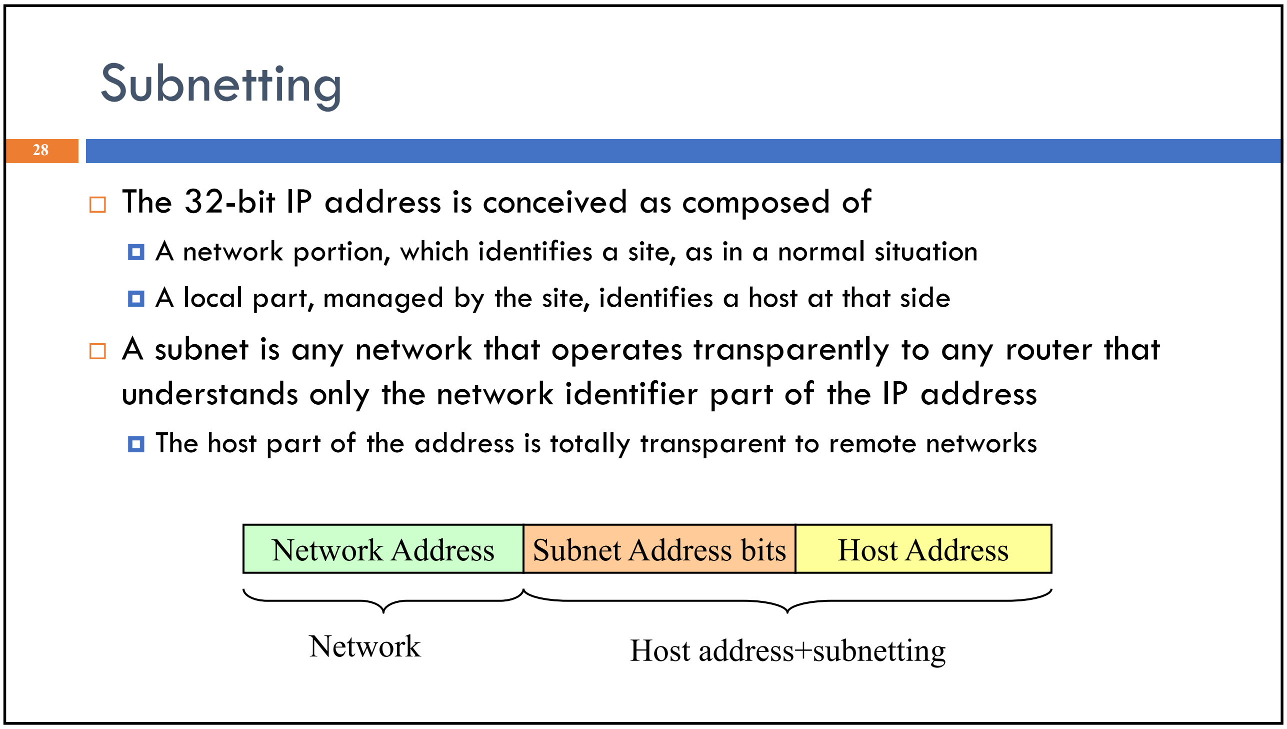


Private IP addresses

27

- For private internets, the choice of network prefix can be made by the organization
  - To help make this assigment unique, RFC 1918 recommends specific address blocks that can be used in private internets
  - 10.0.0.0 - 10.255.255.255 (10/8 prefix)
  - 172.16.0.0 - 172.31.255.255 (172.16/12 prefix)
  - 192.168.0.0 - 192.168.255.255 (192.168/16 prefix)

27



Subnetting

28

- The 32-bit IP address is conceived as composed of
  - A network portion, which identifies a site, as in a normal situation
  - A local part, managed by the site, identifies a host at that side
- A subnet is any network that operates transparently to any router that understands only the network identifier part of the IP address
  - The host part of the address is totally transparent to remote networks

Network Address	Subnet Address bits	Host Address

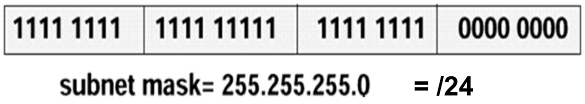
Network

Host address+subnetting

28

Subnet Masks

- By convention
  - Binary 1s, identify the network address portion of the IP address
  - Binary 0s, identify the host address portion of the IP address
- For example, a subnet mask for a "/16 (slash 16)" network that uses the third octet to identify the physical network and the fourth to identify the host is defined as:

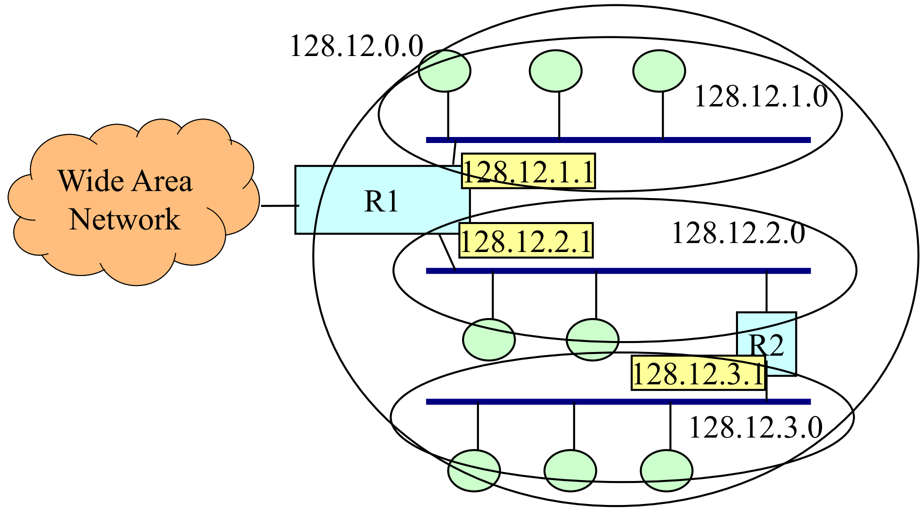


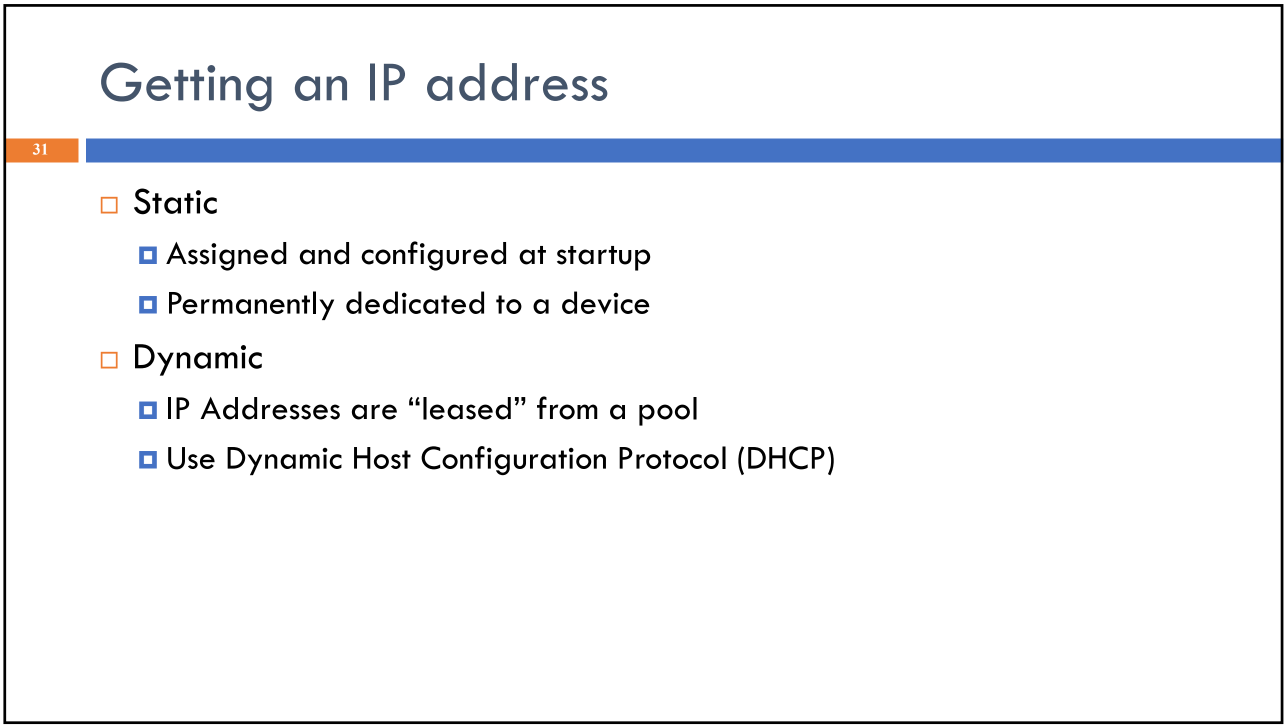
1111 1111	1111 11111	1111 1111	0000 0000

subnet mask= 255.255.255.0 = /24

- Two types of subnetting are possible
  - Static subnetting
  - Variable length subnetting

Subnet Addresses



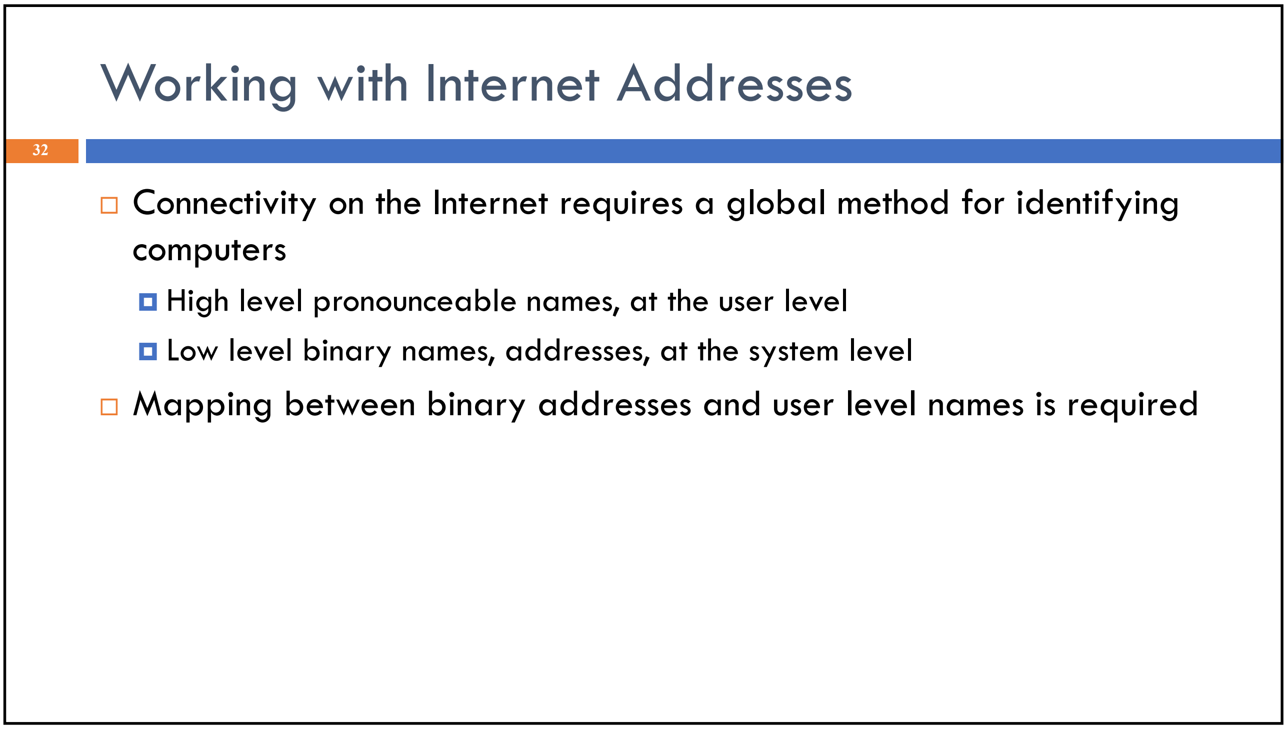


Getting an IP address

31

- Static
  - Assigned and configured at startup
  - Permanently dedicated to a device
- Dynamic
  - IP Addresses are “leased” from a pool
  - Use Dynamic Host Configuration Protocol (DHCP)

31

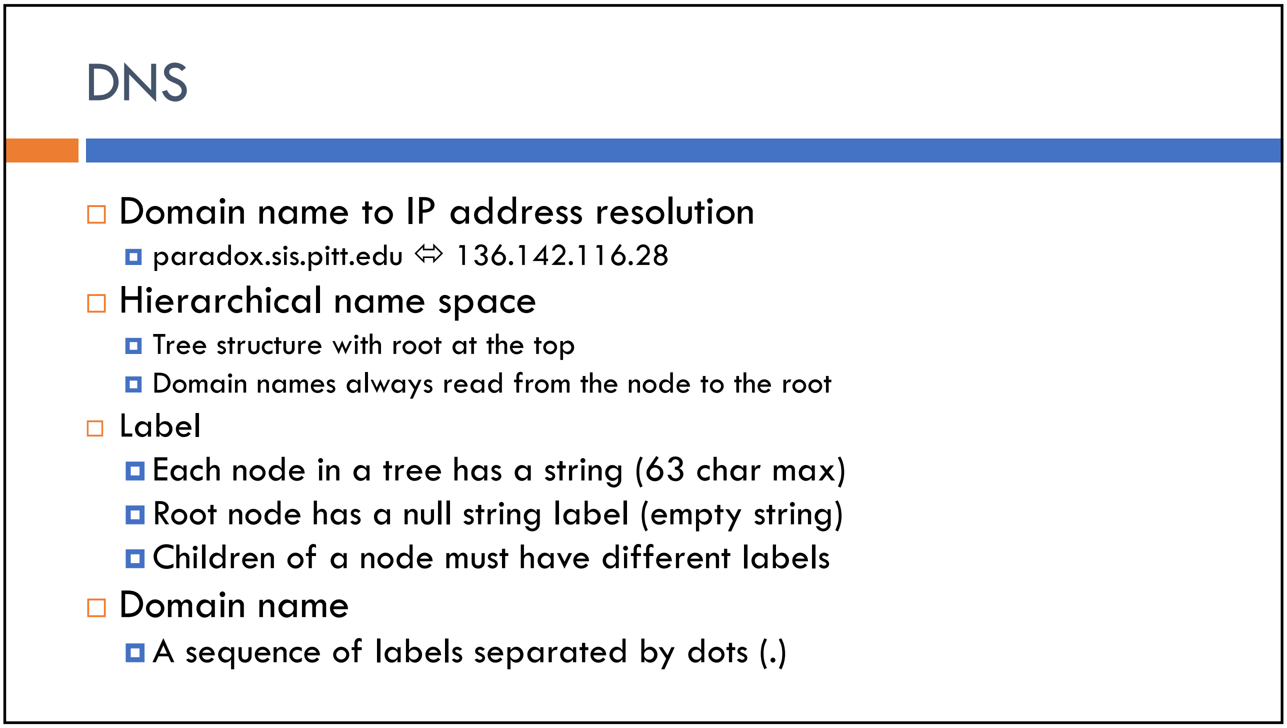


Working with Internet Addresses

32

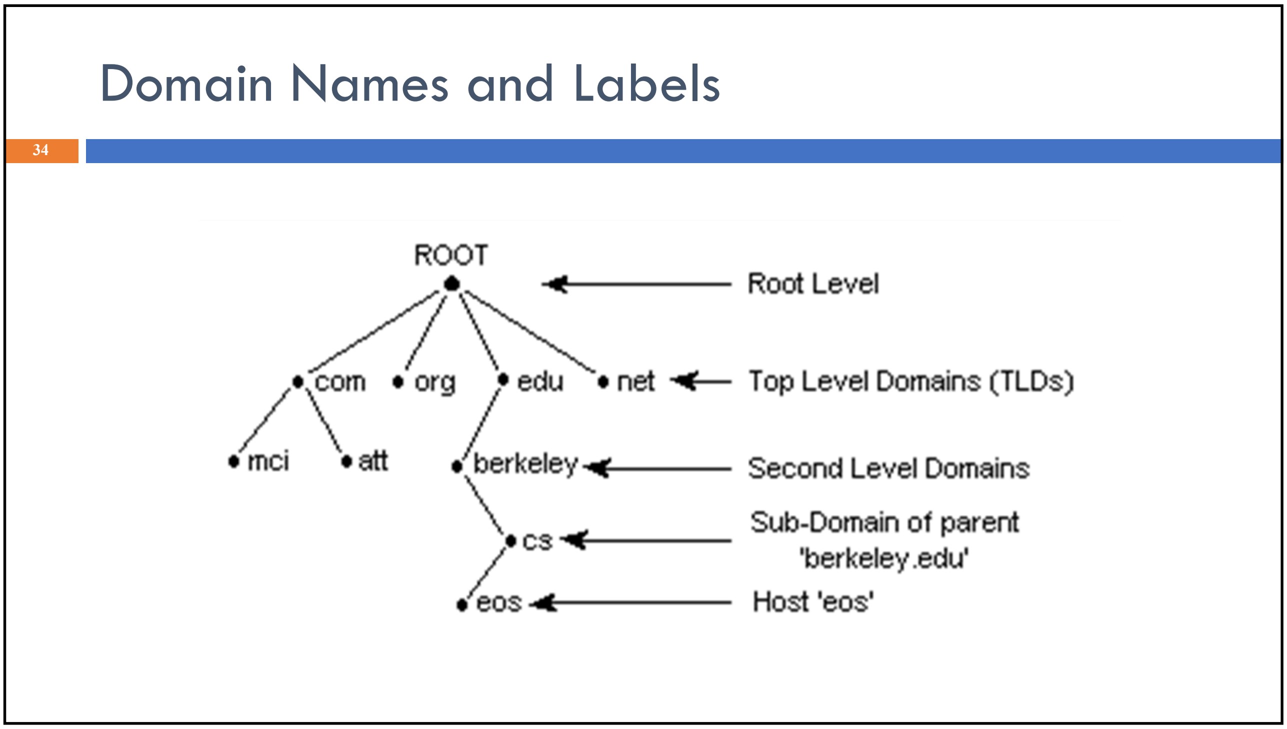
- Connectivity on the Internet requires a global method for identifying computers
  - High level pronounceable names, at the user level
  - Low level binary names, addresses, at the system level
- Mapping between binary addresses and user level names is required

32



DNS

- □ Domain name to IP address resolution
  - paradox.sis.pitt.edu ⇔ 136.142.116.28
- □ Hierarchical name space
  - Tree structure with root at the top
  - Domain names always read from the node to the root
- □ Label
  - Each node in a tree has a string (63 char max)
  - Root node has a null string label (empty string)
  - Children of a node must have different labels
- □ Domain name
  - A sequence of labels separated by dots (.)

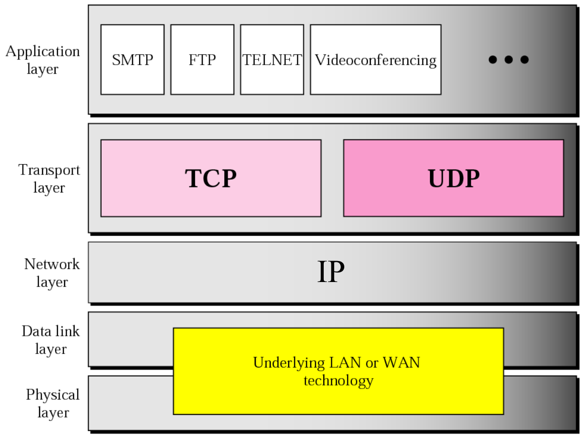


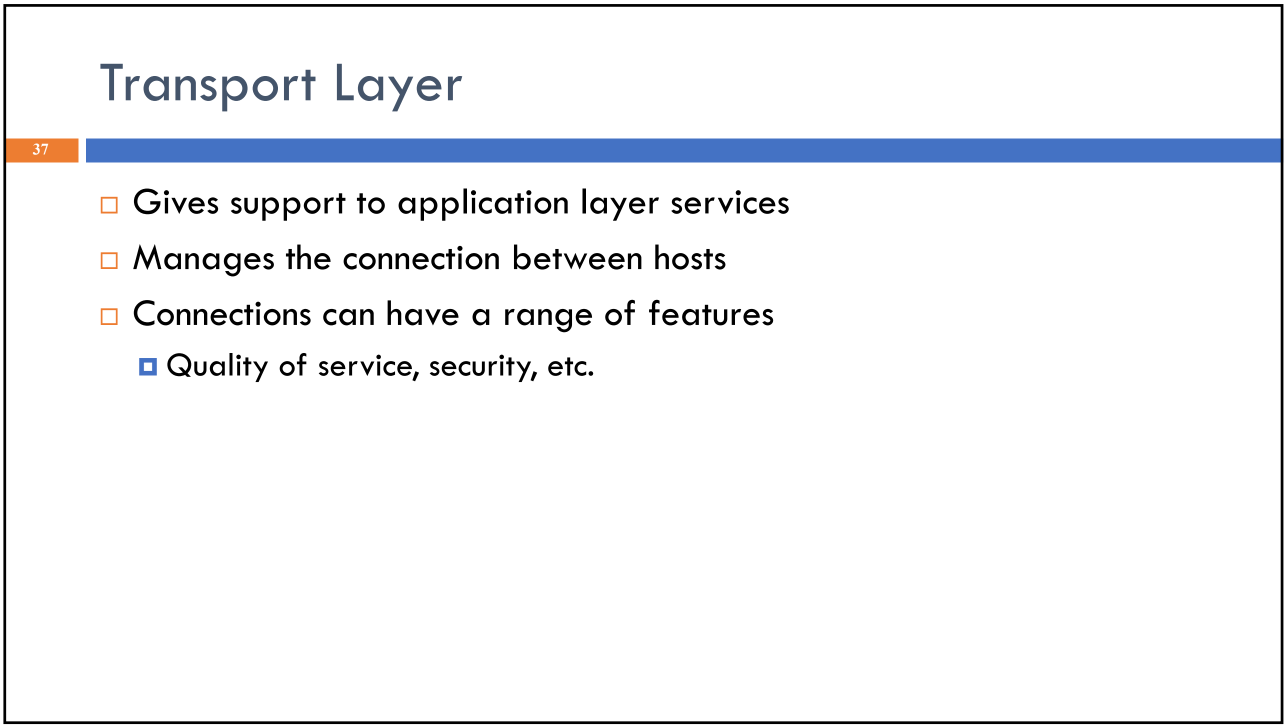
Domain Names and Labels

IPv6 Addressing

- IPv6 address is 128 bits
- ***x:x:x:x:x:x:x:x,*** where "**x**" represents 16 bit hexadecimal field
- Leading zeros in a field are optional:
  - 2031:0:130F:0:0:9C0:876A:130B
- Successive fields of 0 can be represented as ::, but only once per address
- Examples:
  - **FF01:0:0:0:0:0:0:1 >>> FF01::1**
  - **0:0:0:0:0:0:0:1 >>> ::1**
- IPv6 addresses are usually divided into two equal parts with the high-order 64 bits identifying a network address and the low-order 64 bits identifying the node. Many other address arrangements are also possible

Transport Layer



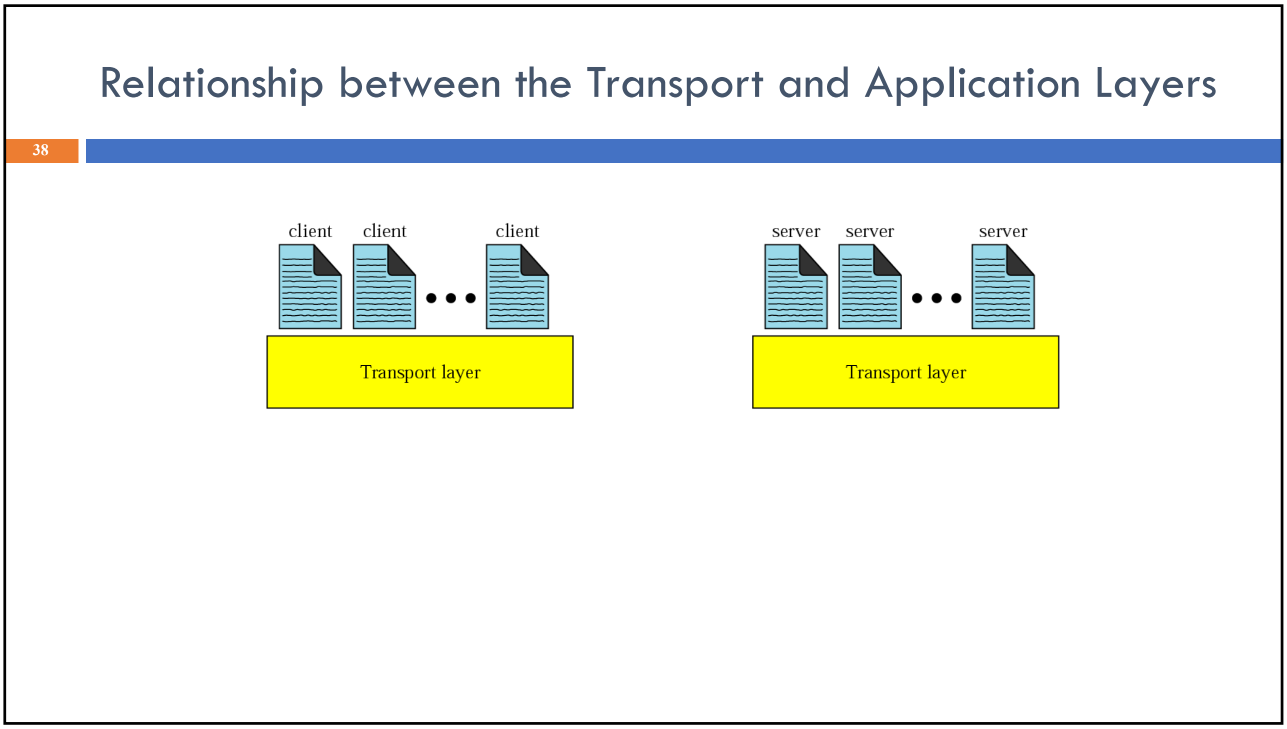


Transport Layer

37

- □ Gives support to application layer services
- □ Manages the connection between hosts
- □ Connections can have a range of features
  - Quality of service, security, etc.

37

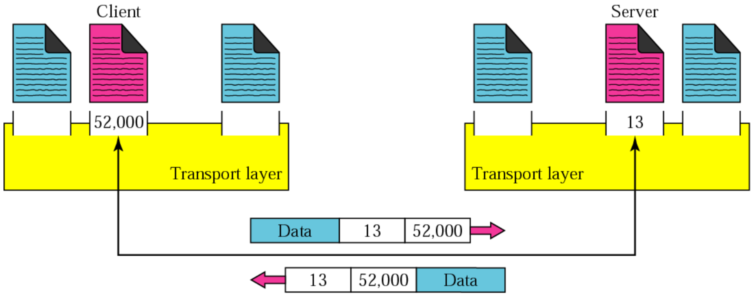


Relationship between the Transport and Application Layers

38

38

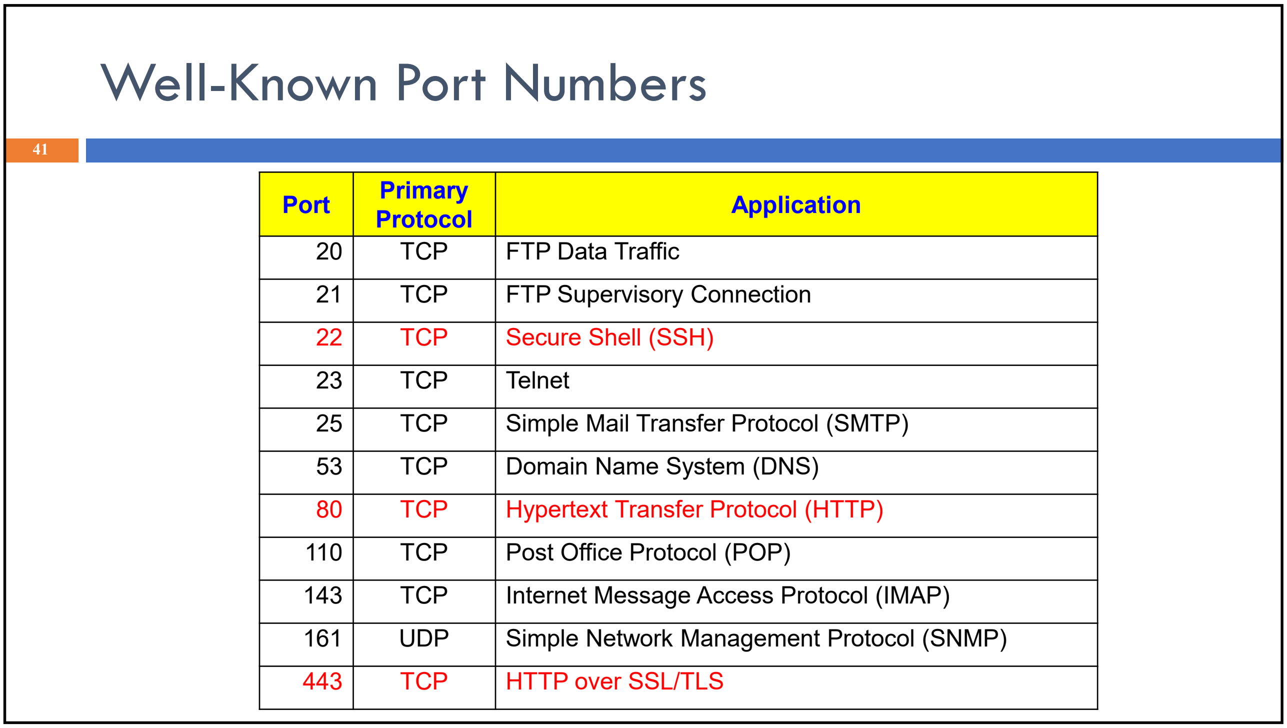
Port Numbers



- □ Clients use temporary port numbers
- □ Servers use well-know port numbers

Transport Layer (in the Internet Reference Model)

- □ TCP and UDP
- □ TCP
  - Connectivity is between ports on hosts
  - These addresses need only be locally unique
  - In TCP, some standard ports are defined
    - For well-known services (Telnet, FTP, e-Mail, HTTP, etc)

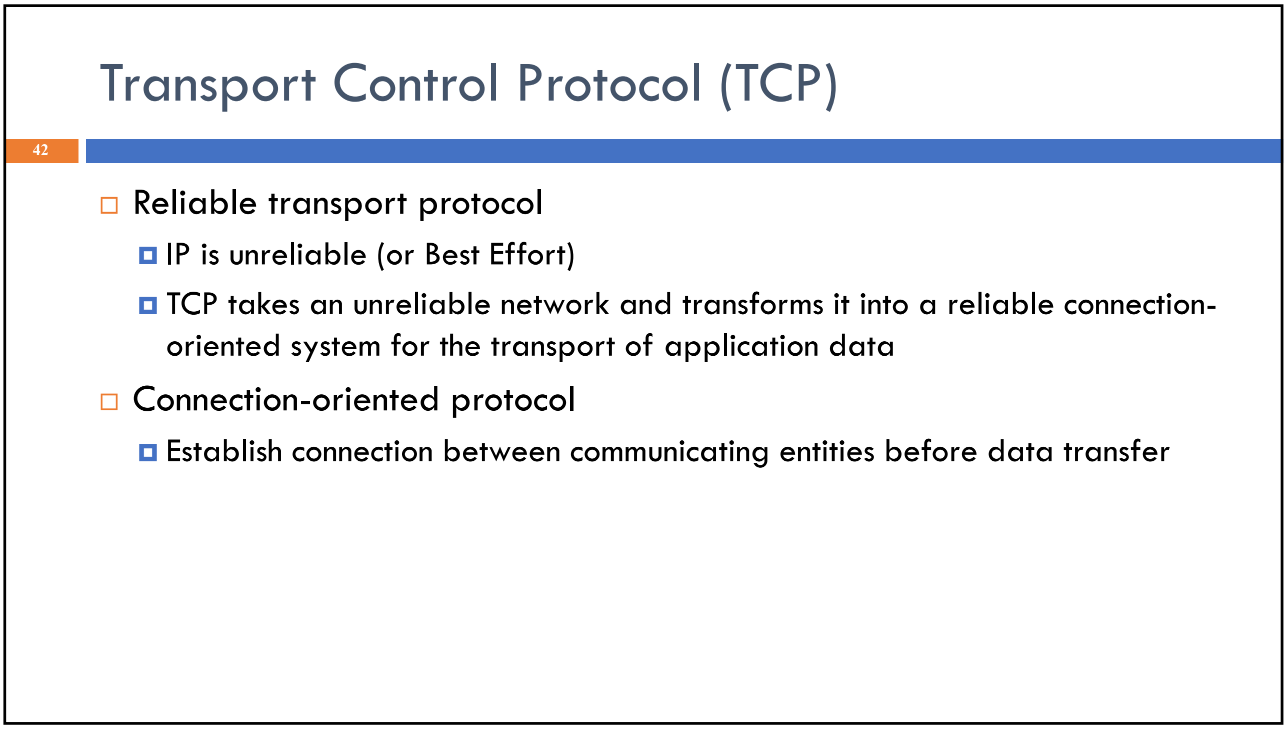


Well-Known Port Numbers

41

Port	Primary Protocol	Application
20	TCP	FTP Data Traffic
21	TCP	FTP Supervisory Connection
22	TCP	Secure Shell (SSH)
23	TCP	Telnet
25	TCP	Simple Mail Transfer Protocol (SMTP)
53	TCP	Domain Name System (DNS)
80	TCP	Hypertext Transfer Protocol (HTTP)
110	TCP	Post Office Protocol (POP)
143	TCP	Internet Message Access Protocol (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)
443	TCP	HTTP over SSL/TLS

41



Transport Control Protocol (TCP)

42

- Reliable transport protocol
  - IP is unreliable (or Best Effort)
  - TCP takes an unreliable network and transforms it into a reliable connection-oriented system for the transport of application data
- Connection-oriented protocol
  - Establish connection between communicating entities before data transfer

42

Connecting to a “node” on the Internet (in the Cloud)

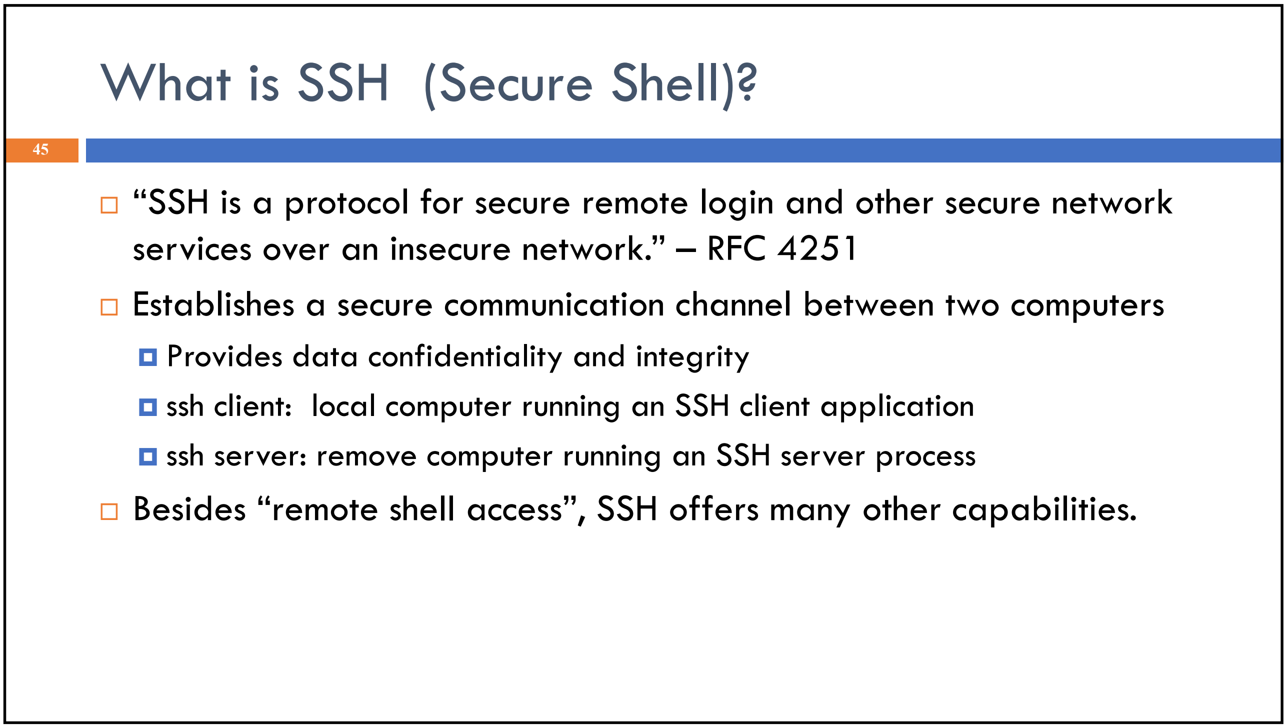
- You need to know the IP address of the “node” (e.g., a virtual machine)
  - OR know its *full name* and have DNS find the IP address

AND

- You need to know the (transport layer) port number over which the connection is supported
  - Typically, SSH runs on TCP port 22

- Note: All of this assumes that you have the proper permissions and system configuration to access the node

SSH – Remote connection to VMs in the cloud

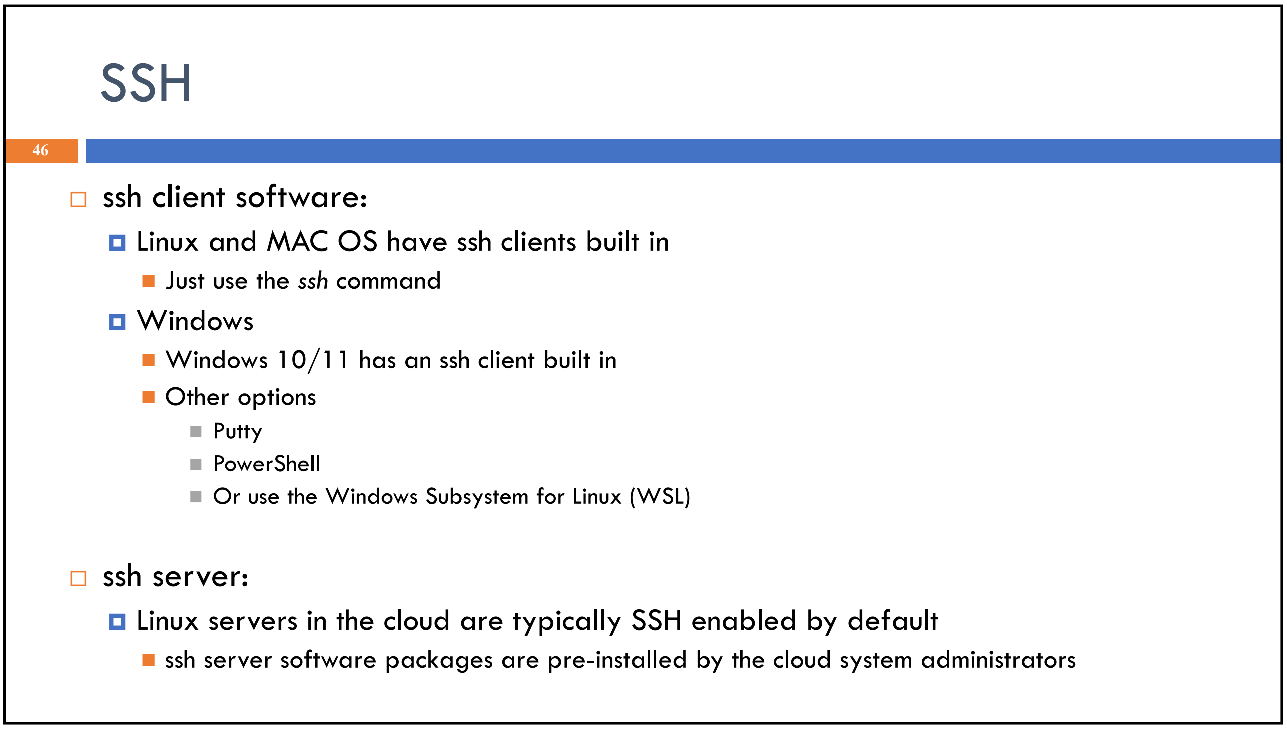


What is SSH (Secure Shell)?

45

- “SSH is a protocol for secure remote login and other secure network services over an insecure network.” – RFC 4251
- Establishes a secure communication channel between two computers
  - Provides data confidentiality and integrity
  - ssh client: local computer running an SSH client application
  - ssh server: remove computer running an SSH server process
- Besides “remote shell access”, SSH offers many other capabilities.

45

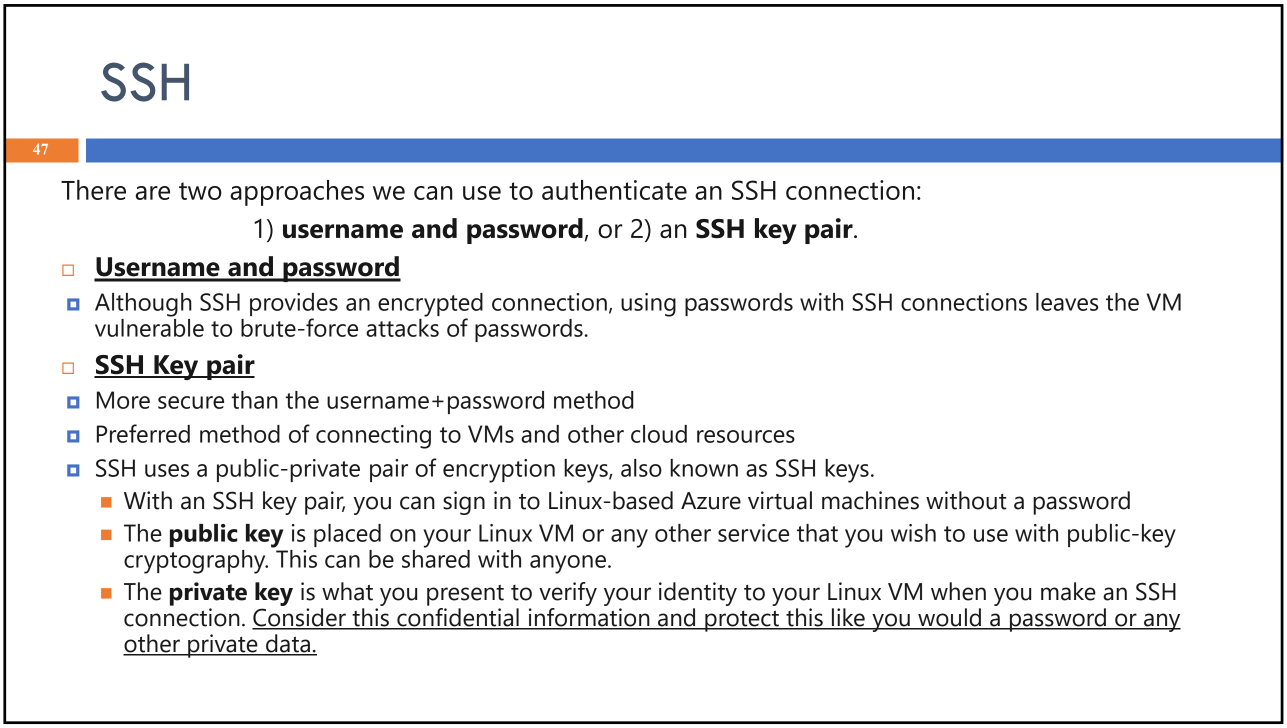


SSH

46

- ssh client software:
  - Linux and MAC OS have ssh clients built in
    - Just use the *ssh* command
  - Windows
    - Windows 10/11 has an ssh client built in
    - Other options
      - Putty
      - PowerShell
      - Or use the Windows Subsystem for Linux (WSL)
- ssh server:
  - Linux servers in the cloud are typically SSH enabled by default
    - ssh server software packages are pre-installed by the cloud system administrators

46



SSH

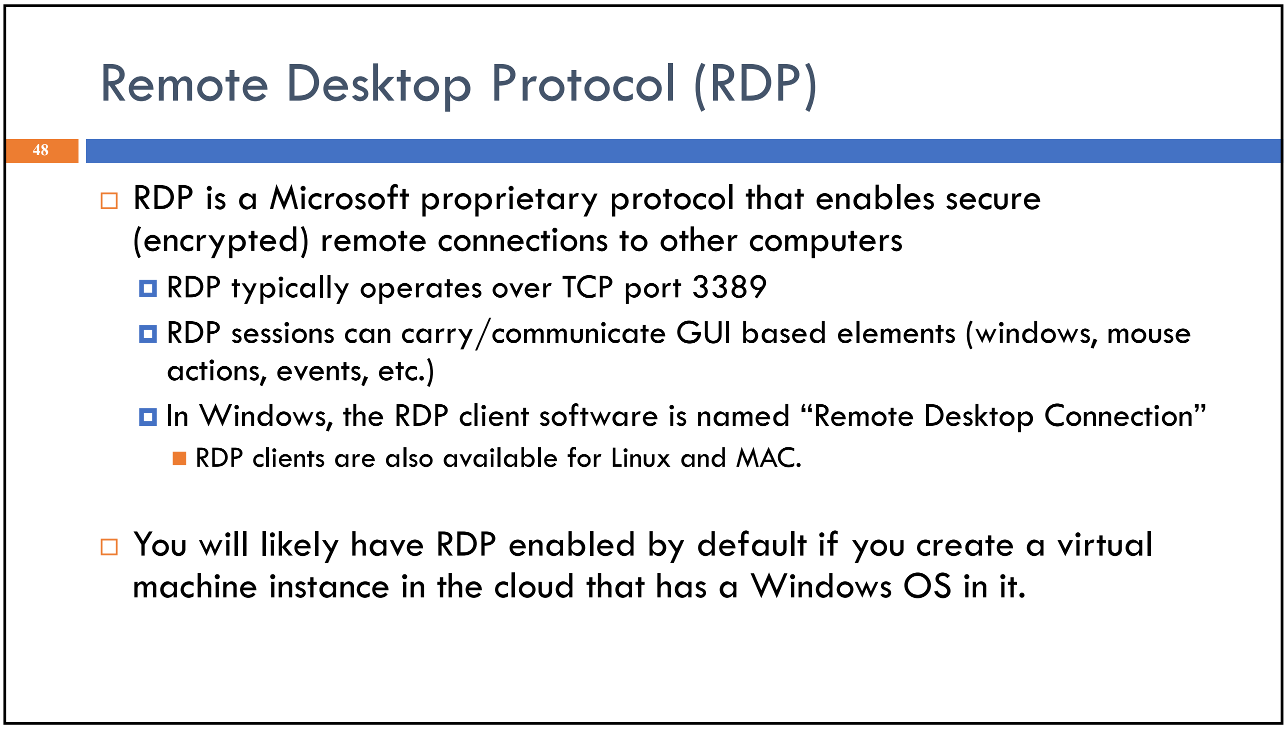
47

There are two approaches we can use to authenticate an SSH connection:

1) **username and password**, or 2) an **SSH key pair**.

- **Username and password**
  - Although SSH provides an encrypted connection, using passwords with SSH connections leaves the VM vulnerable to brute-force attacks of passwords.
- **SSH Key pair**
  - More secure than the username+password method
  - Preferred method of connecting to VMs and other cloud resources
  - SSH uses a public-private pair of encryption keys, also known as SSH keys.
    - With an SSH key pair, you can sign in to Linux-based Azure virtual machines without a password
    - The **public key** is placed on your Linux VM or any other service that you wish to use with public-key cryptography. This can be shared with anyone.
    - The **private key** is what you present to verify your identity to your Linux VM when you make an SSH connection. Consider this confidential information and protect this like you would a password or any other private data.

47

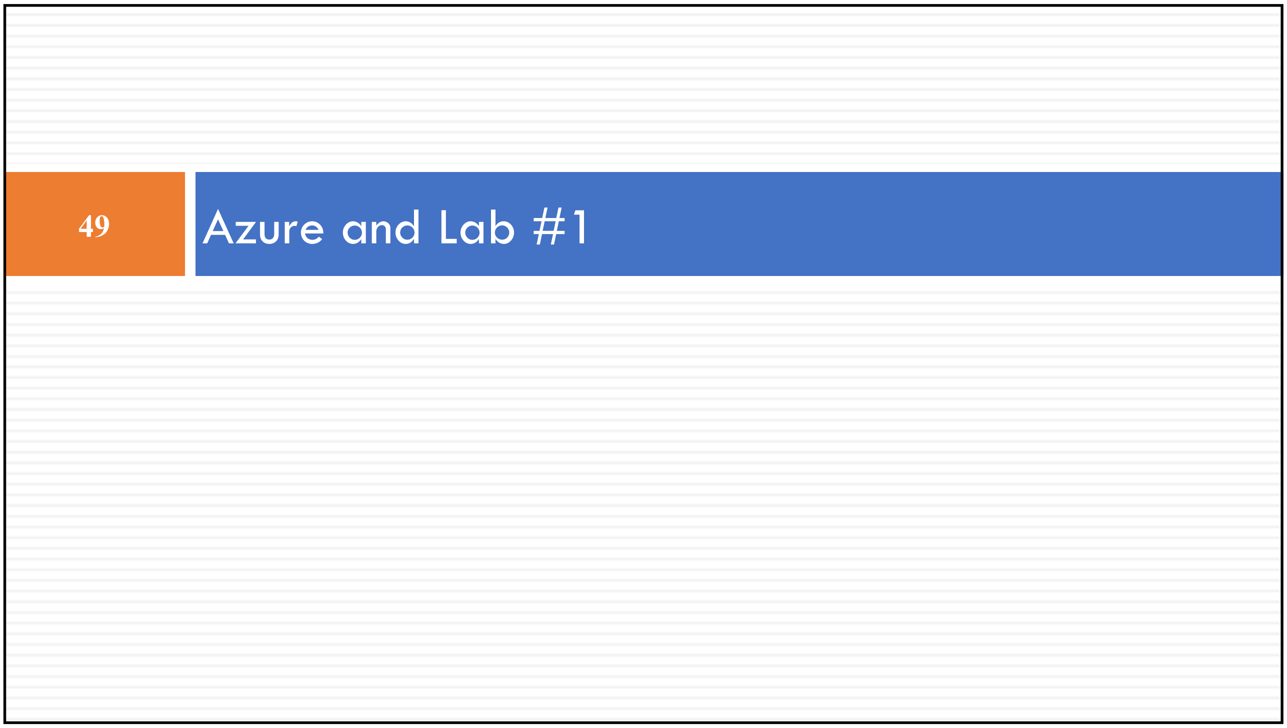


Remote Desktop Protocol (RDP)

48

- RDP is a Microsoft proprietary protocol that enables secure (encrypted) remote connections to other computers
  - RDP typically operates over TCP port 3389
  - RDP sessions can carry/communicate GUI based elements (windows, mouse actions, events, etc.)
  - In Windows, the RDP client software is named “Remote Desktop Connection”
    - RDP clients are also available for Linux and MAC.
- You will likely have RDP enabled by default if you create a virtual machine instance in the cloud that has a Windows OS in it.

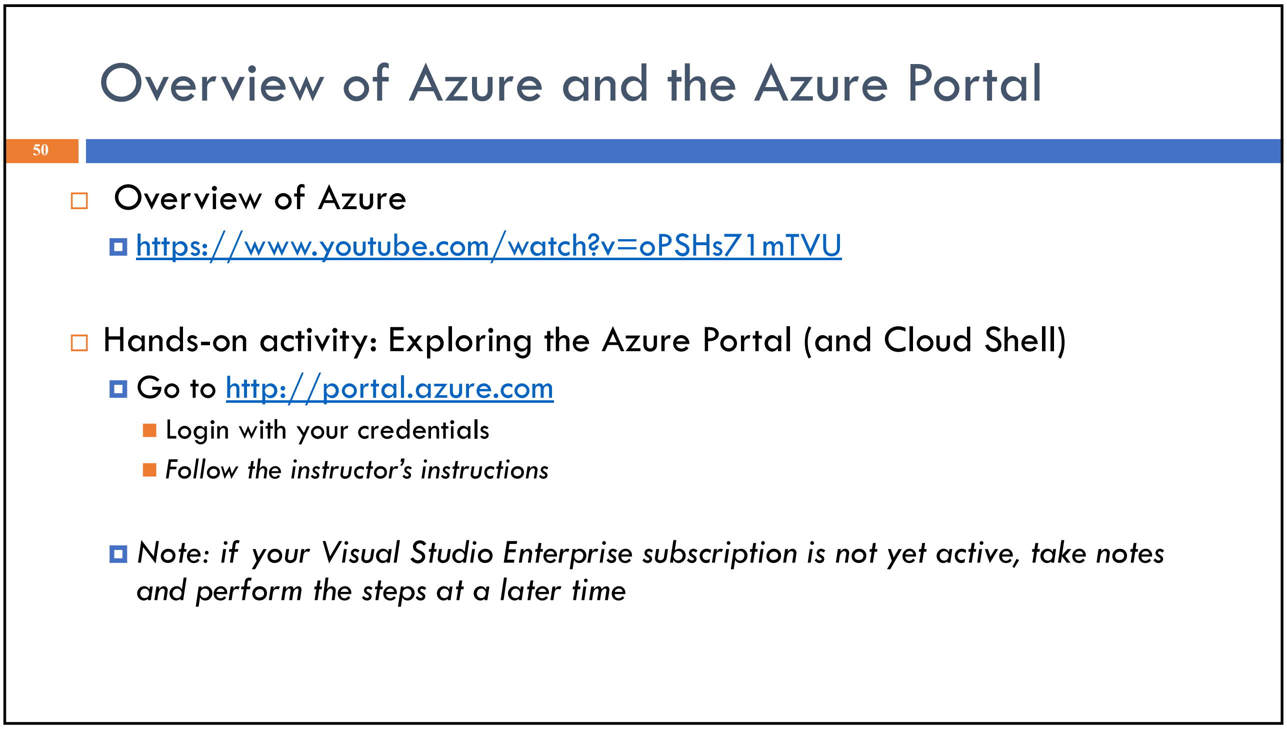
48



49

Azure and Lab #1

49

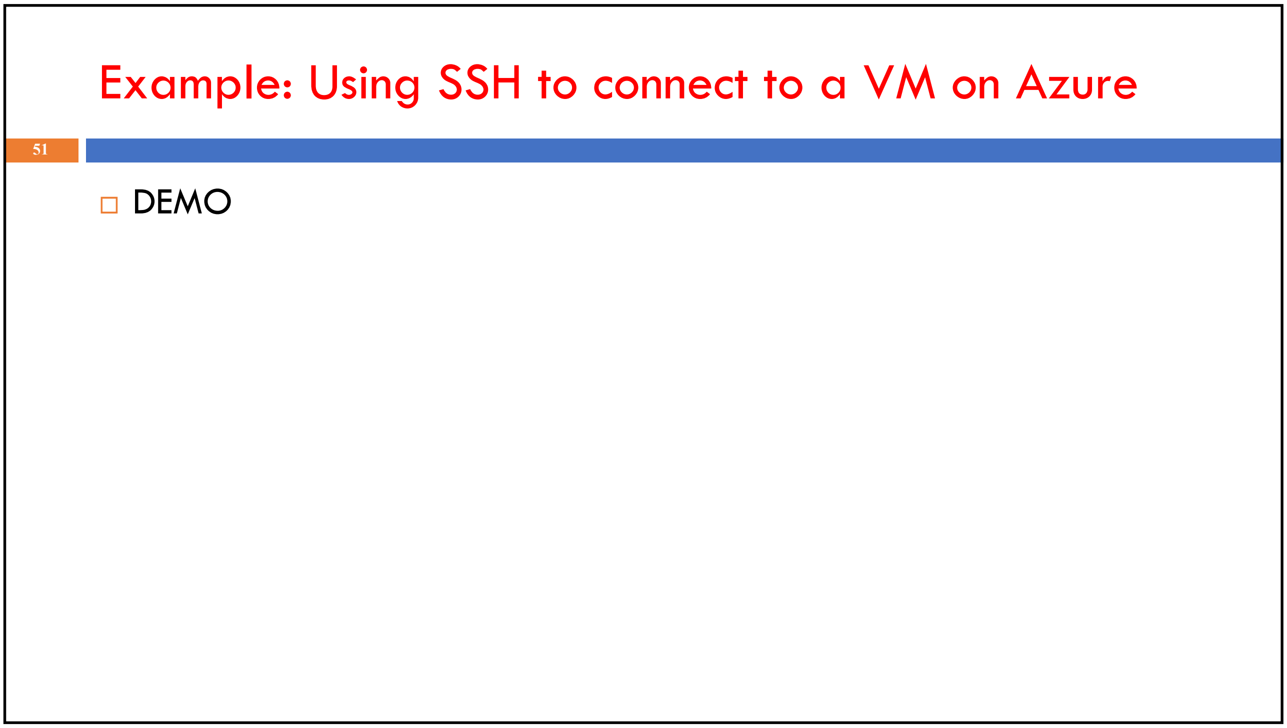


Overview of Azure and the Azure Portal

50

- Overview of Azure
  - https://www.youtube.com/watch?v=oPSHs71mTVU
- Hands-on activity: Exploring the Azure Portal (and Cloud Shell)
  - Go to http://portal.azure.com
    - Login with your credentials
    - *Follow the instructor's instructions*
  - *Note: if your Visual Studio Enterprise subscription is not yet active, take notes and perform the steps at a later time*

50

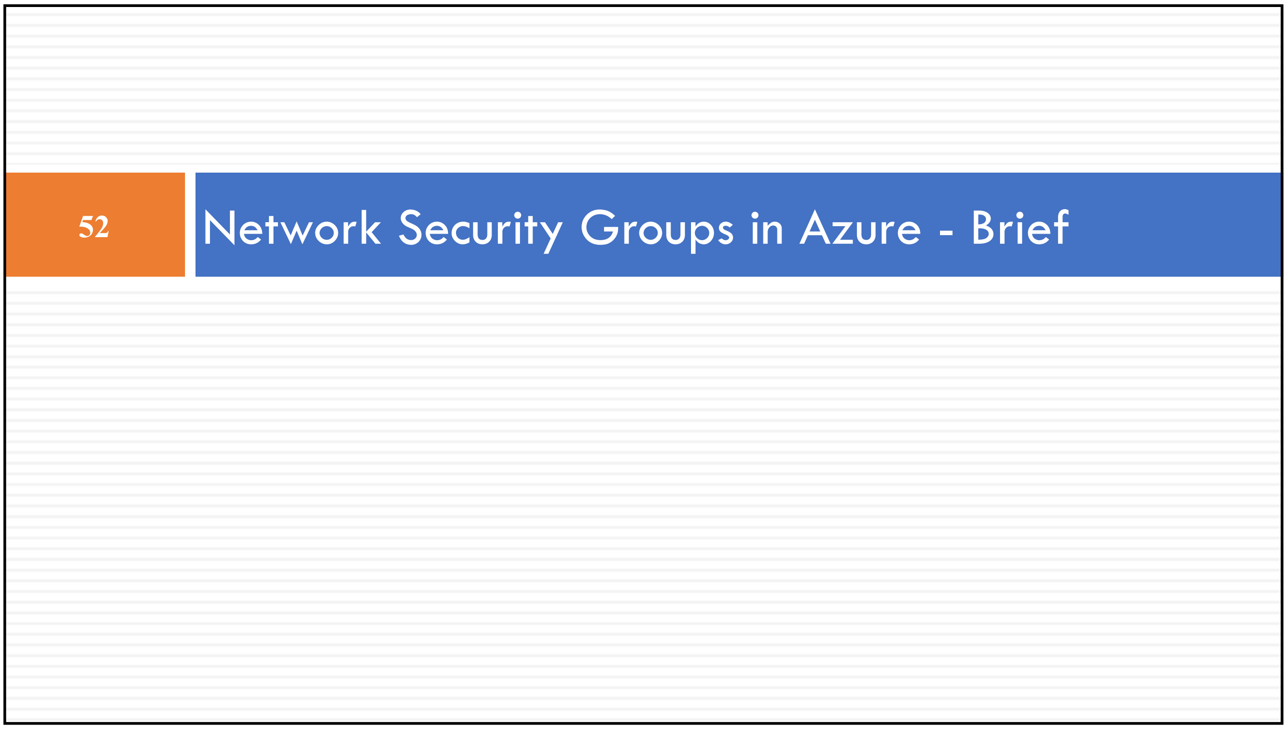


Example: Using SSH to connect to a VM on Azure

51

- □ DEMO

51

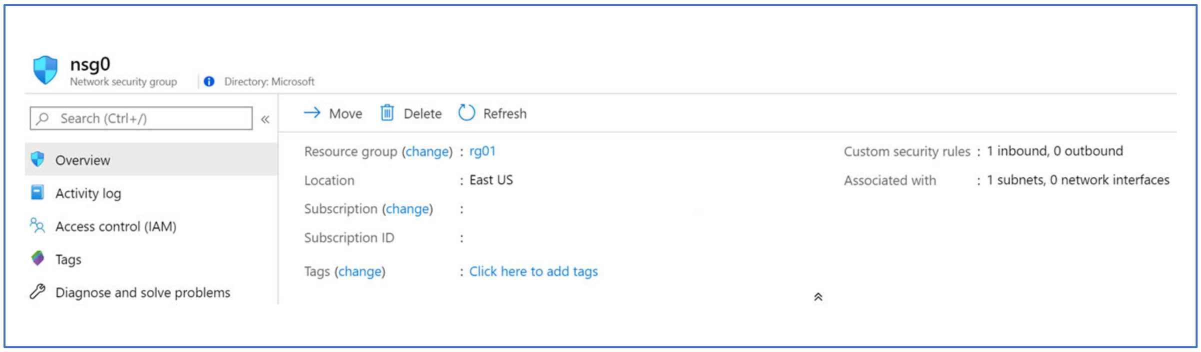


52

Network Security Groups in Azure - Brief

52

Implement Network Security Groups (NSGs)



Resource group (change) : rg01

Location : East US

Subscription (change) :

Subscription ID :

Tags (change) : Click here to add tags

Custom security rules : 1 inbound, 0 outbound

Associated with : 1 subnets, 0 network interfaces

Limits network traffic to resources in a virtual network

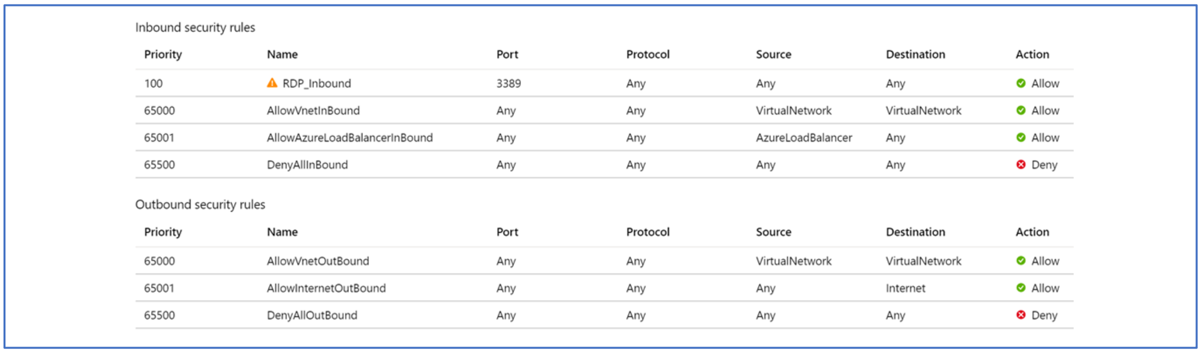
Lists the security rules that allow or deny inbound or outbound network traffic

Associated to a subnet or a network interface

Can be associated multiple times

53

Determine NSG Rules



Inbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
100	⚠ RDP_Inbound	3389	Any	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny

Outbound security rules

Priority	Name	Port	Protocol	Source	Destination	Action
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

Security rules in NSGs enable you to filter network traffic that can flow in and out of virtual network subnets and network interfaces

There are default security rules. You cannot delete the default rules, but you can add other rules with a higher priority

54

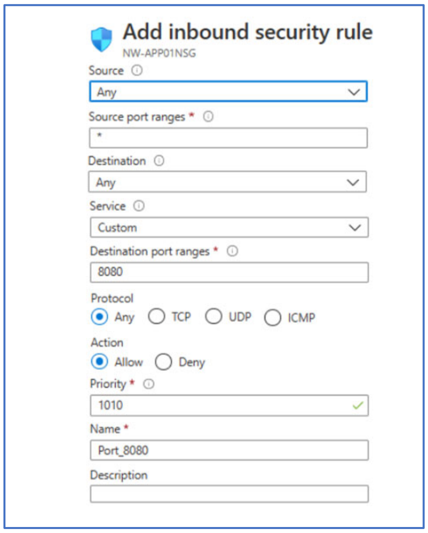
Create NSG rules

Source (Any, IP addresses, service tags, application security group)

Destination (Any, IP addresses, virtual network, application security group)

Service (HTTPS, SSH, RDP, DNS, POP3, custom, …)

Priority – The lower the number, the higher the priority



Add inbound security rule

NW-APP01NSG

Source: Any

Source port ranges *: *

Destination: Any

Service: Custom

Destination port ranges *: 8080

Protocol: ● Any ○ TCP ○ UDP ○ ICMP

Action: ● Allow ○ Deny

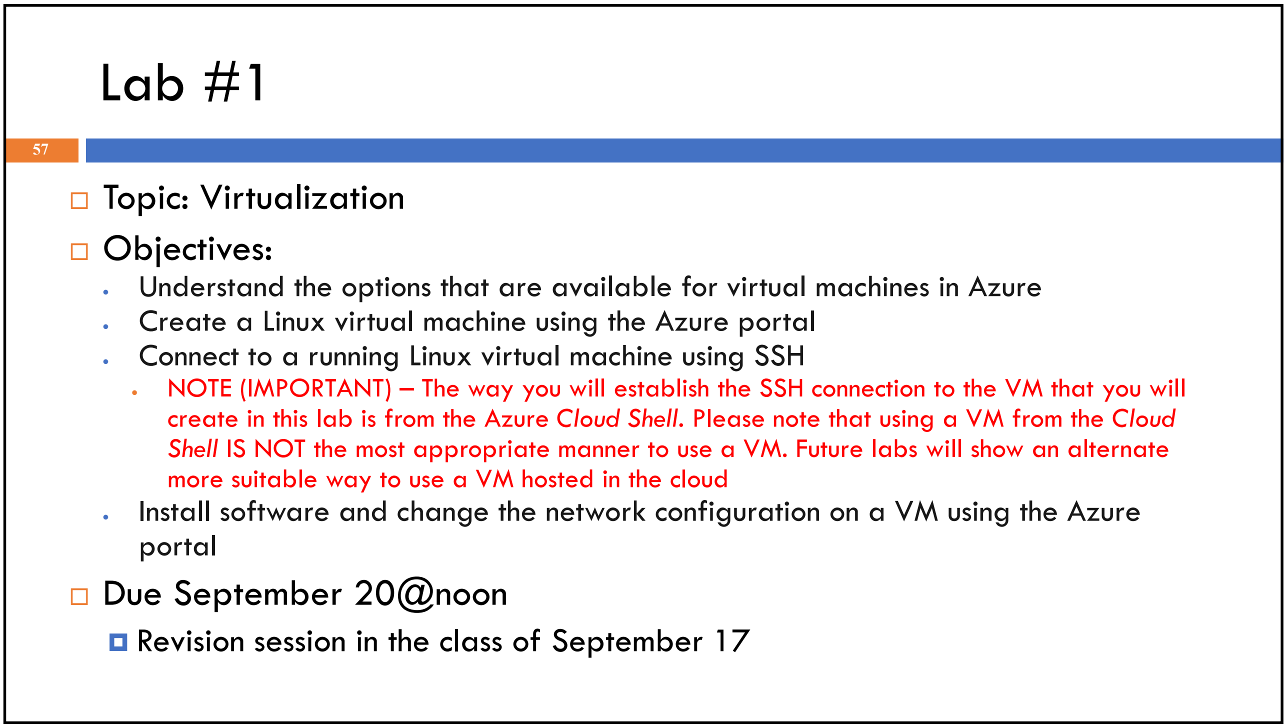
Priority *: 1010

Name *: Port_8080

Description:

Lab #1: Overview

- Explore the lab guide with the instructor
  - Questions ?



Lab #1

- Topic: Virtualization
- Objectives:
  - Understand the options that are available for virtual machines in Azure
  - Create a Linux virtual machine using the Azure portal
  - Connect to a running Linux virtual machine using SSH
    - NOTE (IMPORTANT) – The way you will establish the SSH connection to the VM that you will create in this lab is from the Azure *Cloud Shell*. Please note that using a VM from the *Cloud Shell* IS NOT the most appropriate manner to use a VM. Future labs will show an alternate more suitable way to use a VM hosted in the cloud
  - Install software and change the network configuration on a VM using the Azure portal
- Due September 20@noon
  - Revision session in the class of September 17