

**MURANG'A UNIVERSITY OF  
TECHNOLOGY  
DEPARTMENT OF IT  
SIT304: COMPUTER NETWORKING  
PRACTICUM  
CREDIT HOURS: 3 HOURS  
COURSE NOTES – 2020/2021**

# INTRODUCTION TO COMPUTER NETWORKS

## COMPARING LOGICAL AND PHYSICAL NETWORKS

A network is a **group** of computers and other devices connected together.

These **connections** can be with cables, wireless connections, or both.

Networks are discussed in both **logical** and **physical** terms.

The logical organization of a network identifies the overall **design** of a network.

It differentiates between local area networks (LANs) and wide area networks (WANs)

# COMPARING LOGICAL AND PHYSICAL NETWORKS CONT'D

The logical design of the network provides a **high-level** overview of the entire network and may not show smaller components such as all the switches, routers, and firewalls.

By contrast, the physical network infrastructure includes the **details** of the physical components.

The physical components are the **devices** and **cabling** that you can touch and feel.

# NETWORKING HOME COMPUTERS

Most home computers are part of a network today.

At the very least, home computers have the ability to connect to the **Internet**, which is a massive network of networks.

The computer has access to the Internet through a modem to an **Internet service provider** (ISP).

This could be a **cable** modem used in a broadband connection or a modem used for dial-up connections

Broadband connections are widely available in urban areas. This includes connections through cable TV systems, fiber-optic lines, and even phone connections such as ISDN and 3G/4G data services.

# NETWORKING HOME COMPUTERS CONT'D

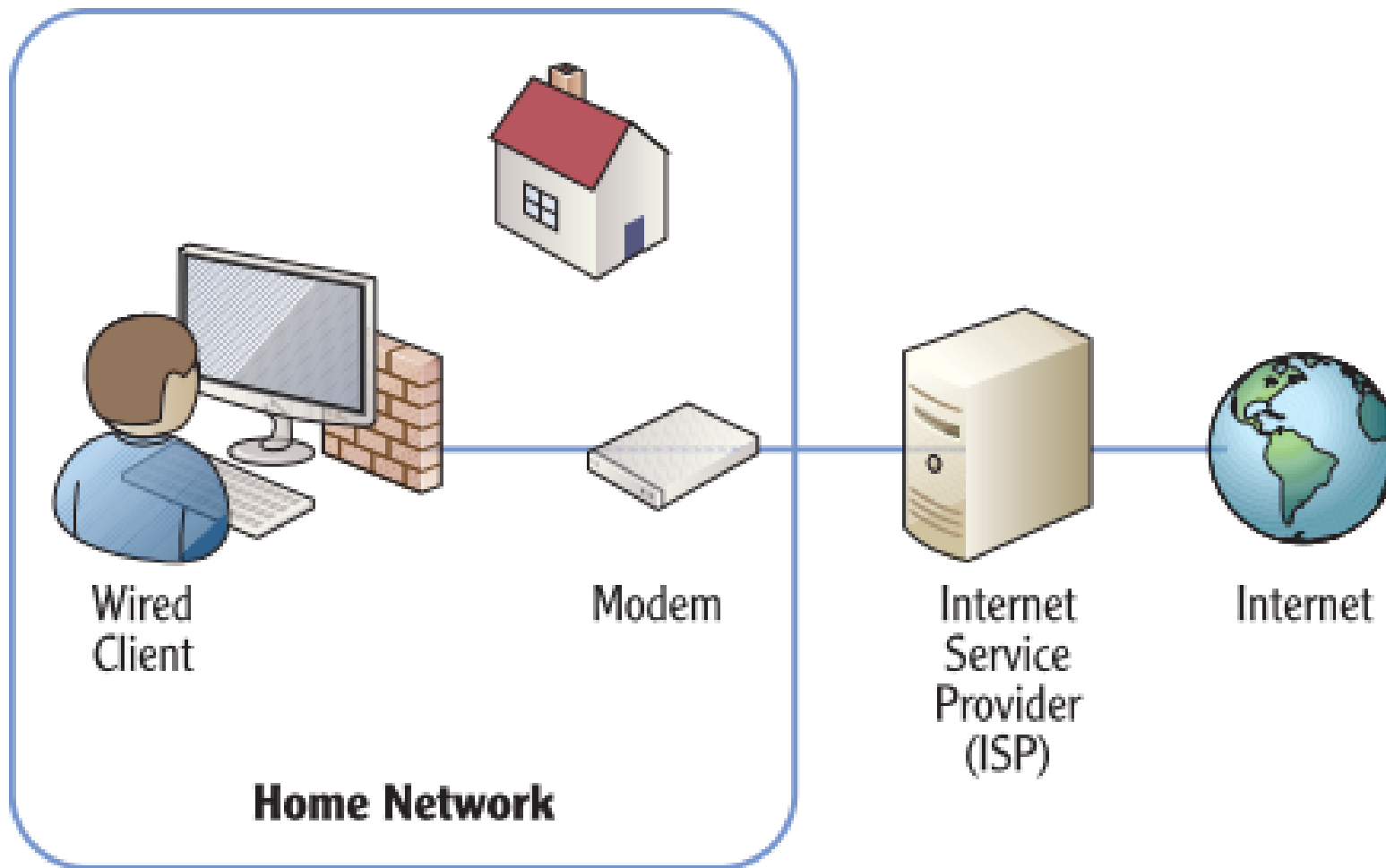


Figure 1: Home computer with access to Internet

# NETWORKING HOME COMPUTERS CONT'D

## ENABLE THE LOCAL FIREWALL

When a computer connects directly to the Internet through an ISP (without going through an internal router or wireless access point), it is at significant **risk**.

The computer has a **public IP address** and is **accessible** from any other computer on the Internet, anywhere in the world. Attackers often prowl the Internet looking for unprotected computers.

Enabling the **software firewall** on this computer provides a layer of protection

# NETWORKING HOME COMPUTERS CONT'D

When home users add additional computers into their home, they typically want to network these computers.

Users on the network are then able to **share** resources. For example, consider figure 2 which shows a typical home network connected to **each** other and the **Internet** using both wired and wireless connections.

In the figure, the wired user is connected to a wireless router directly with a cable, and another user is connected via a wireless connection.

A wireless printer is added that can be shared by any users with access to the wired network. An

# NETWORKING HOME COMPUTERS CONT'D

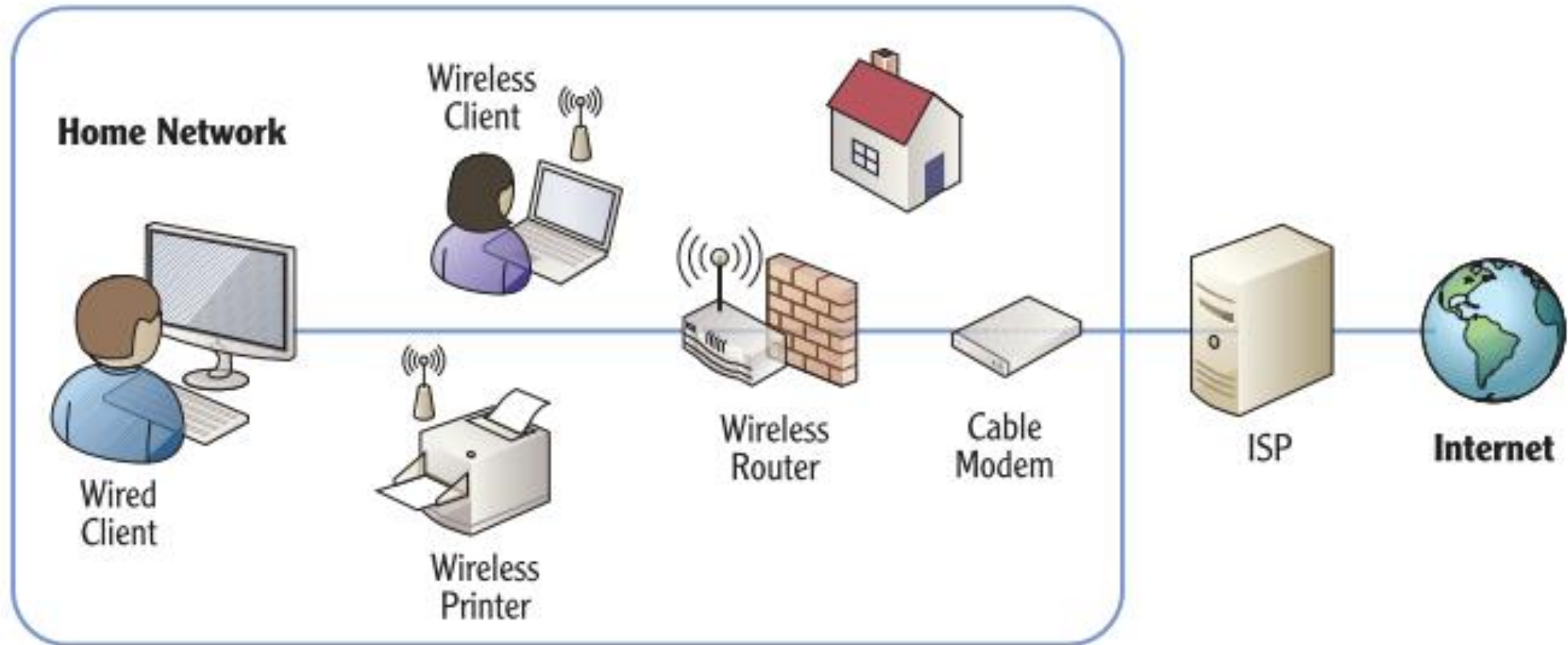


Figure 2: Typical home network



# NETWORKING HOME COMPUTERS CONT'D

ISP **provides** connectivity to the Internet, just as it would for a single user. A single cable modem connects to the ISP, and then the cable modem connects to a wireless router.

Without a network, each individual computer would need to connect to the Internet separately, incurring individual access charges.

However, the single Internet connection can be shared by adding the **wireless router**. A great benefit of wireless is that you don't have to install cables to each computer. Most wireless routers include several additional capabilities.

# NETWORKING HOME COMPUTERS CONT'D

It's common for a wireless router used in most home networks to include the following:

## Wireless Access Point (WAP)

The core purpose of the wireless device is to support connectivity for wireless clients. The WAP provides this connectivity.

## Routing Capabilities

A built-in router will route data from the internal network to the Internet and from Internet data back to the internal network.

# NETWORKING HOME COMPUTERS CONT'D

## Network Address Translation (NAT)

NAT translates the public IP addresses used on the Internet to private IP addresses on the internal network, and vice versa.

If NAT wasn't used, you'd have to purchase or lease public IP addresses for each internal computer.

Additionally, each computer would be directly on the Internet and exposed to unnecessary risks.

NAT hides the internal computers from Internet attackers

# NETWORKING HOME COMPUTERS CONT'D

## Dynamic Host Configuration Protocol (DHCP)

DHCP provides clients with IP addresses and other TCP/IP configuration information. The other TCP/IP information includes the address of the DNS server and the address of the router that provides a path to the Internet. The router address is also known as the default gateway.

## Firewall

A WAP will provide basic firewall capabilities. This blocks unwanted traffic from the Internet, providing a layer of protection for internal clients.

# NETWORKING SMALL OFFICES AND HOME OFFICES

Small offices and home offices (SOHOs) are very similar to the sophisticated home network.

They are both considered LANs.

SOHOs have access to the Internet and can have either wireless clients, wired clients, or both.

Figure 3 shows the configuration of sample SOHO network. The primary difference is that a SOHO will typically have a server to provide additional capabilities for the office.

For example, the server can be used as a file server to store files used within the business.

# NETWORKING SMALL OFFICES AND HOME OFFICES

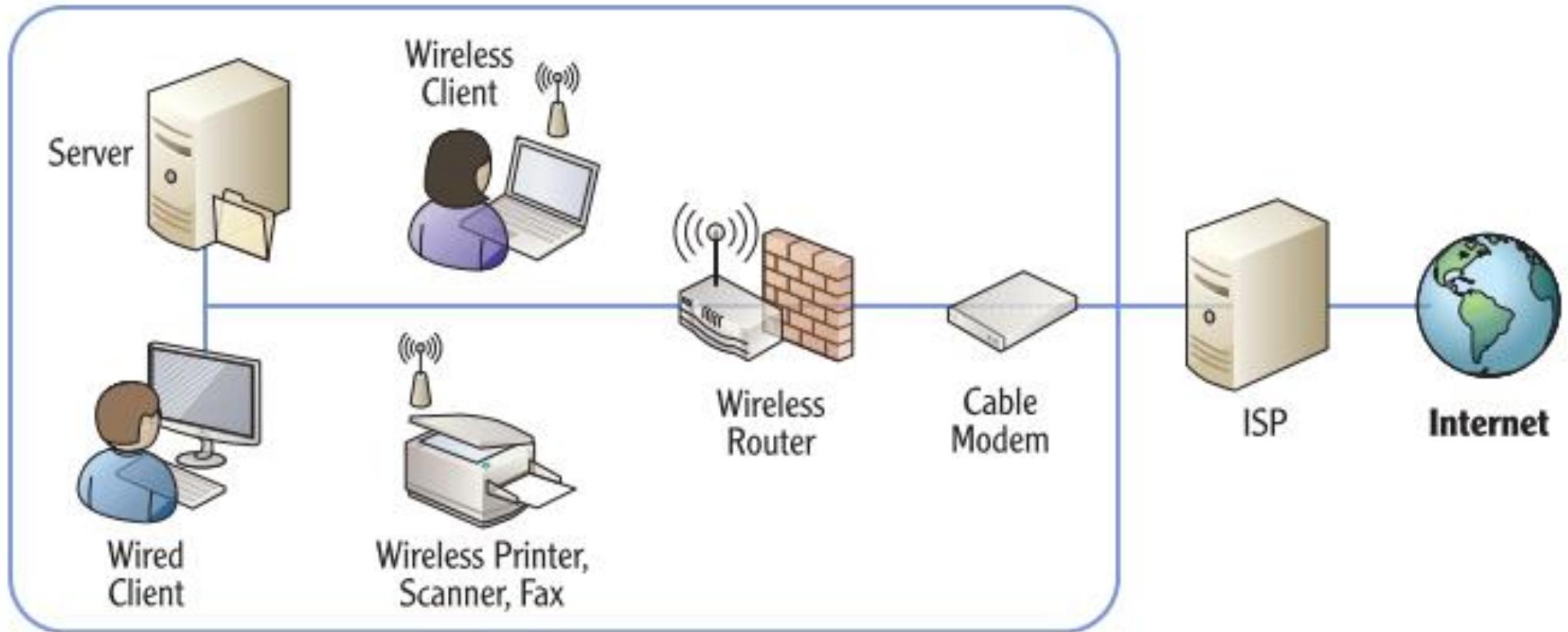


Figure 3: SOHO network

# NETWORKING SMALL OFFICES AND HOME OFFICES CONT'D

Although most offices will have a server, it's not necessary. Important files could be stored on a primary **user's** computer and shared to other users from there if needed.

However, if important files are stored on multiple computers, it becomes harder to back up these files.

Additionally, a business may have a wireless **multifunction printer** that can print, scan, and fax documents to meet the needs of the business.

It's not necessary to have a wireless printer. However, these are becoming more popular in SOHOs because they are easier to share between the network users.

# NETWORKING SMALL OFFICES AND HOME OFFICES CONT'D

## SECURE WIRELESS NETWORKS

It's very important to lock down wireless networks with the best security available.

The primary method of security for wireless networks is **WPA2** (or 802.11i) If the network is not locked down, an attacker can use a simple laptop with a wireless NIC while driving by in a car to compromise it.

This “**war driving**” technique allows an attacker to tap into the network and access the network's resources if the network isn't secured.



# NETWORKING SMALL OFFICES AND HOME OFFICES CONT'D

Historically, wireless networks were notoriously **insecure**.

However, technologies available today make it possible to provide **sufficient** security for most wireless networks. Similarly, the **WAP** used in the SOHO will provide many of the same capabilities to the office as a WAP provides for a home network.

This includes routing, NAT, DHCP, and a firewall

# UNDERSTANDING LOCAL AREA NETWORKS

The **home** network and the **SOHOs** are both considered local area networks.

A LAN is a group of computers and/or other devices that are connected in a single physical location (such as a home, office, or corporate building).

LANs have **fast** network connectivity between the different devices in the LAN.

Common speeds of wired LANs today are **100 Mbps** or **1000 Mbps** (1 Gbps) and 54 Mbps or 300 Mbps for wireless

# UNDERSTANDING LOCAL AREA NETWORKS CONT'D

## MEGABIT AND GIGABIT

LAN speeds identify how much data they can **transfer**. Mbps is short for **megabit per second**, and a megabit represents a **million bits**.

A LAN with a speed of 100 Mbps can transfer data at a rate of **100 million** bits per second.

A gigabit LAN (1 Gbps or 1000 Mbps) transfers data at a rate of **1 billion** bits per second

# UNDERSTANDING LOCAL AREA NETWORKS CONT'D

Occasionally, data is measured in **bytes** instead of bits.

A byte consists of **8 bits**.

When bytes are mentioned, a **capital B** is used.

For example, a system may have 4 gigabytes (GB) of random access memory (RAM).

This is commonly listed as 4 GB. It is not accurate to list this as 4 Gb (with a lowercase b).

Similarly, it not accurate to list a 100 Mbps LAN as 100 MBps (with a capital B).

# UNDERSTANDING LOCAL AREA NETWORKS CONT'D

A LAN is an **internal** network.

Most LANs will have connectivity to the Internet through a **router** or **firewall**, but the LAN itself is internal.

Traffic **back** and **forth** through a firewall to the Internet is filtered for **security** purposes.

However, traffic within the LAN itself is usually not filtered.

The internal network is considered a **high trust** area, so any traffic on the network is allowed

# COMPARING WORKGROUPS AND DOMAINS

A SOHO will typically include from one to ten workers and will usually be configured as a **workgroup**.

A workgroup is a group of networked computers that share a **common** workgroup name.

The default name of a Microsoft workgroup is simply Workgroup, and all computers in the workgroup will share the **same** workgroup name.

**User** accounts are located on each individual computer.

# COMPARING WORKGROUPS AND DOMAINS CONT'D

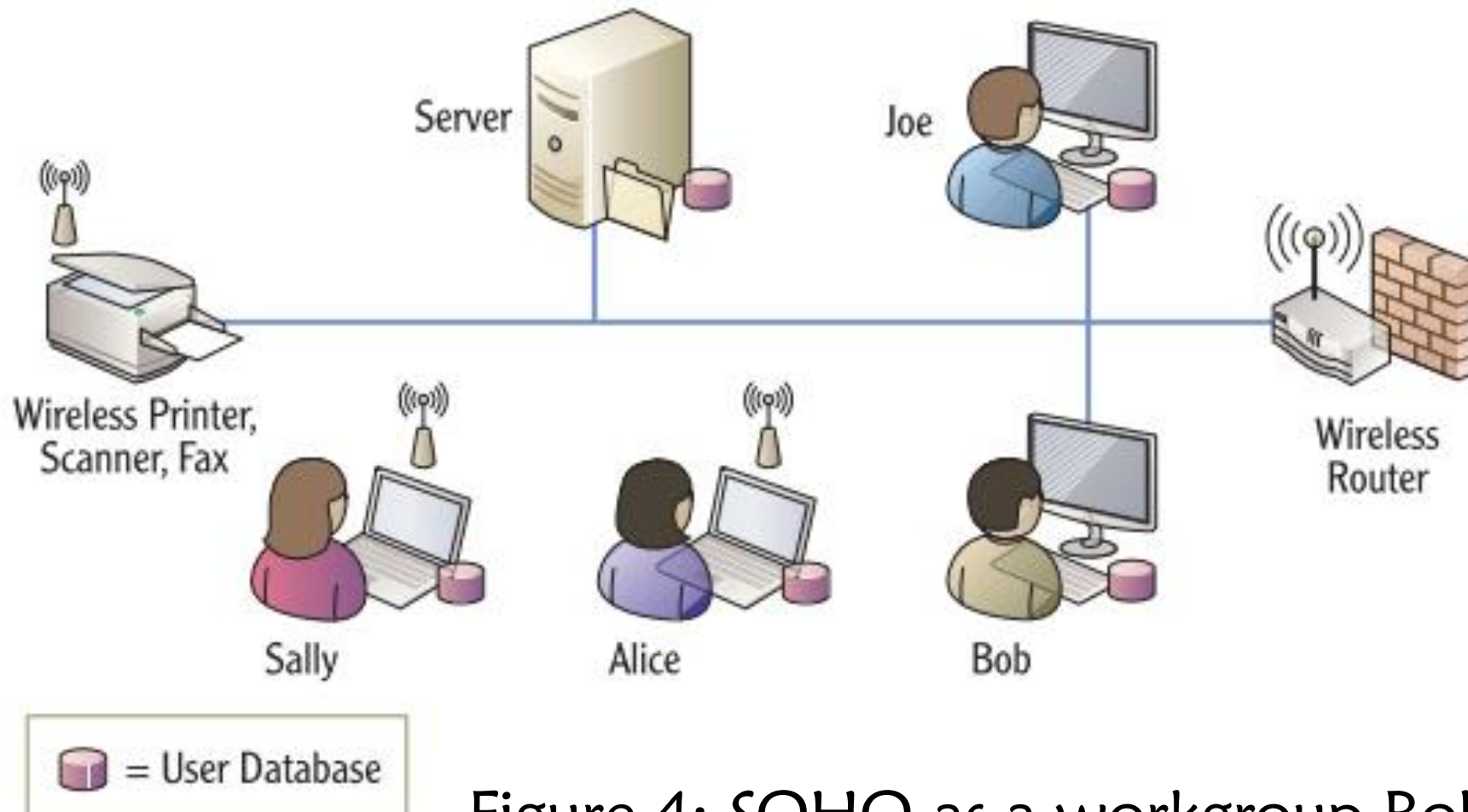


Figure 4: SOHO as a workgroup Bob

# COMPARING WORKGROUPS AND DOMAINS CONT'D

Each of the users in figure 4 have their **own** computer, and an additional server is available to them.

For Sally to log onto her computer, she needs a computer account on **her** computer.

However, this account **won't** work on Bob's, Alice's, or Joe's computers.

If Sally needs to log onto any other computer in the workgroup, she must have a **separate** account on that computer



# COMPARING WORKGROUPS AND DOMAINS CONT'D

In this scenario, there are five separate user databases—one on the server and one on each of the four computers.

Similarly, each user would need to remember five **usernames** and five **passwords** to log onto each of the five computers.

However, most users in a SOHO will typically log onto only one computer in the network and will need only one user account.

If users had to remember five usernames and five passwords, they would probably break a **cardinal** rule of security. They would probably start writing down the usernames and passwords.

When offices get larger than 10 computers or whenever offices need to have more centralized user and computer management, they move into a **domain configuration**.

# COMPARING WORKGROUPS AND DOMAINS CONT'D

You can add a server and promote it to a **domain controller** or promote an existing server to a domain controller.

In Microsoft domains, the domain controller hosts **Active Directory Domain Services** (AD DS). AD DS includes objects such as user and computer accounts. Each user would have one user account in the domain, and each computer would have one computer account.

Figure 5 shows a SOHO configured as a domain. It has eight users with nine computers connected to the LAN.

# COMPARING WORKGROUPS AND DOMAINS CONT'D

The server has been **promoted** to a domain controller and is hosting Active Directory. Instead of requiring users to **memorize** passwords for each computer, each user has **a single account** hosted on the domain controller.

This supports **single sign-on** (SSO) where a user needs to sign on **only once**.

All access to domain resources for the user is **granted** using this single account. Additionally, this one account is used to log onto almost **any** computer in the domain

# COMPARING WORKGROUPS AND DOMAINS CONT'D

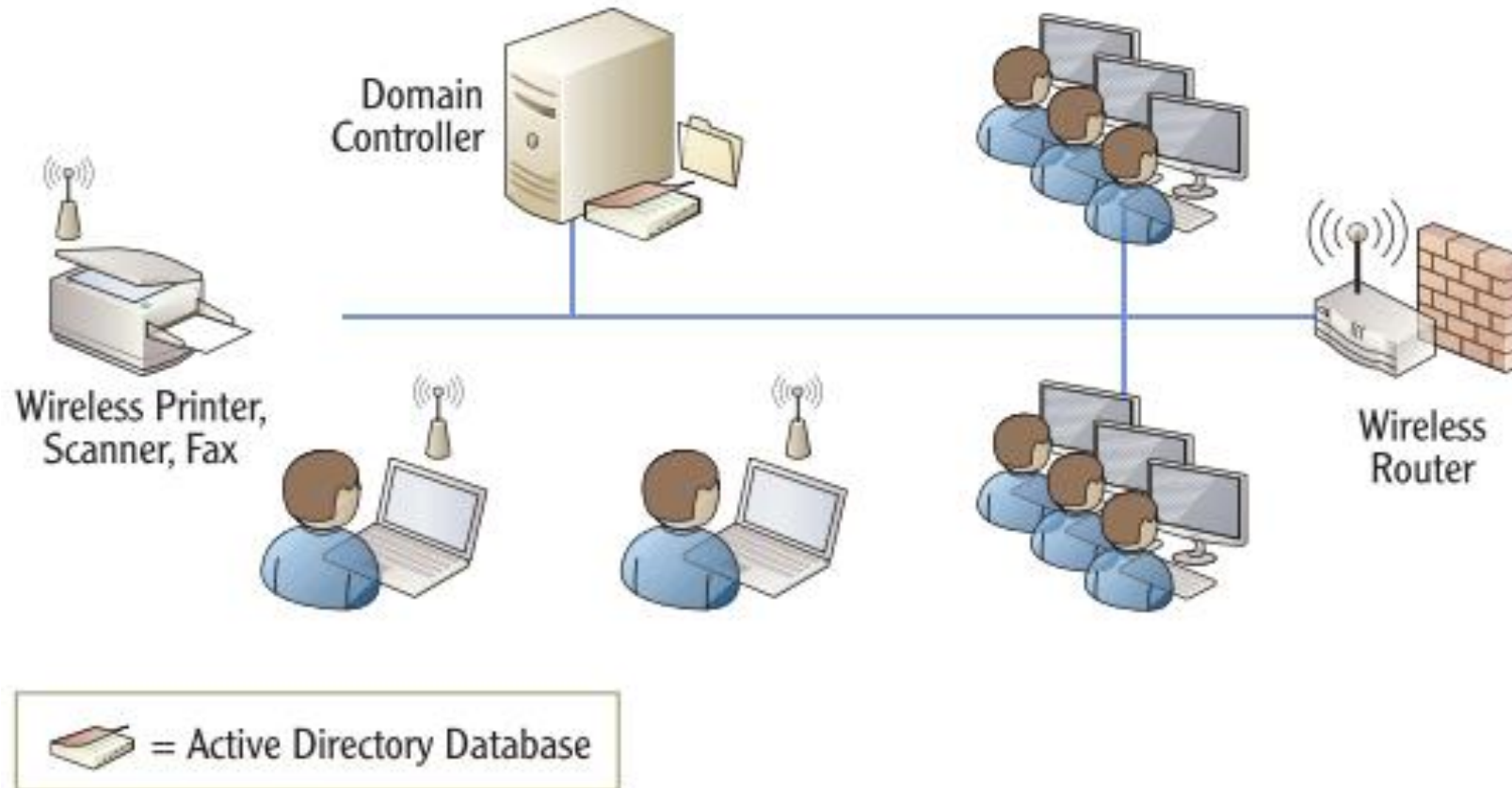


Figure 5: SOHO as a domain

# COMPARING WORKGROUPS AND DOMAINS CONT'D

By default, domain users are **authorized** to log onto any computer in the domain **except** for domain controllers. **Administrators** are granted the right to log onto domain controllers.

However, it is possible to **restrict** users from logging onto other computers within the domain if necessary. Even though the server has been promoted to a domain controller, it can still perform other **functions** on the network. For example, a domain controller can still host files as a file server.

# WHEN TO SWITCH FROM A WORKGROUP TO A DOMAIN

There isn't a specific number defining when networks must change from a workgroup to a domain. It's based on **preference** and **usability**. However, most offices switch over when the number of users **reaches** between 10 and 20.

Multiple reasons encourage the switch.

=> The **primary** reason to switch is when users have to remember multiple user accounts to perform their job. The domain provides single sign-on capabilities where users need to remember only a single user account to log on.

# WHEN TO SWITCH FROM A WORKGROUP TO A DOMAIN CONT'D

=> A **secondary** reason is to help administrators **reduce** their workload. A domain provides **centralized** administration through Active Directory. It also includes advanced administration tools such as **Group Policy**.

Group Policy **allows** an administrator to configure a setting once in a domain and have it apply to many or all of the computers and users.

=> Another reason is to allow more **concurrent connections** from other devices on the LAN.

# WHEN TO SWITCH FROM A WORKGROUP TO A DOMAIN CONT'D

In older **operating systems** such as Windows XP, each computer was restricted to only 10 concurrent connections. For example, if a computer shared a printer, only 10 other users could send print jobs to it at a time. The 11th connection was refused.

This worked the same if a computer **hosted** a shared application. Ten users could connect, but the 11th connection was refused.

This became a **logical** reason to switch to a domain when the office had more than 10 computers. Windows 7 Professional and Ultimate editions support 20 concurrent connections



# EXPLORING THE BENEFITS OF DOMAINS AND DOMAIN CONTROLLERS

Promoting a server to a domain controller provides several benefits beyond **single** sign-on.

These include the following:

## **i) Simplified Management**

Managing accounts in a domain is done with a group of centralized tools. For example, Active Directory Users and Computers is used to perform common administration tasks for all the users and computers in the domain.

Additionally, user and computer accounts are organized in organizational **units** within the domain.

# EXPLORING THE BENEFITS OF DOMAINS AND DOMAIN CONTROLLERS CONT'D

## ii) Group Policy

Group Policy is used in a domain to **configure**, **control**, and **manage** users and computers. For example, Group Policy can be used to configure **password-protected** screen savers for all computers in the domain.

An administrator can configure the setting **one time** in Group Policy, and the setting is configured **on all** the computers in the domain. It doesn't matter if the organization has 20 users or 20,000 users; the setting is configured once, and Group Policy does the rest.

Thousands of settings can be configured through Group Policy.



# EXPLORING THE BENEFITS OF DOMAINS AND DOMAIN CONTROLLERS CONT'D

## iii) Built-in Redundancy and Fault Tolerance

If you have at least two domain controllers, the domain data is automatically **replicated** to each domain controller. If an account is added on one domain controller, it's copied to the other. If a user changes a password, the change is copied. This ensures you always have a redundant **copy** of Active Directory providing fault tolerance.

In other words, if one domain controller develops a **fault or fails**, the domain can tolerate the fault. The other domain controller will carry the load.

Microsoft domains require a **Domain Name System** (DNS) server. DNS is used primarily to resolve computer names to IP addresses, but it's also used to **locate** domain controllers within a domain. If you don't have DNS or DNS fails, Active Directory fails.



# The end

## Q & A