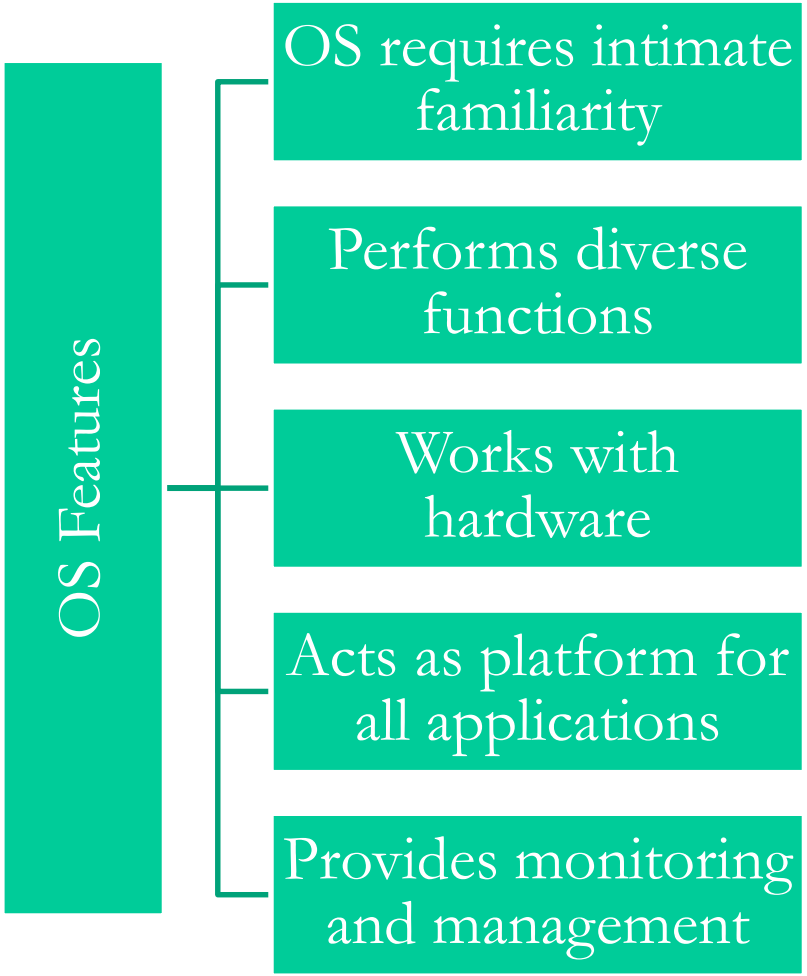
System Fundamentals

Chapter 2

SYBEX

Operating Systems

The operating system provides many features, but look underneath the interface and you will find the platform responsible for the applications being executed.



SYBEX

Common OS Features

- Graphical User Interface
- Network Support
- Multitasking
- Application Support
- Hardware Interface

SYBEX

Microsoft Windows

The majority of the systems will be running Microsoft Windows in some form.

- The dominate OS
- Debuted in 1980s
- Installed on PCs and other devices
- Installed on 90% of computers

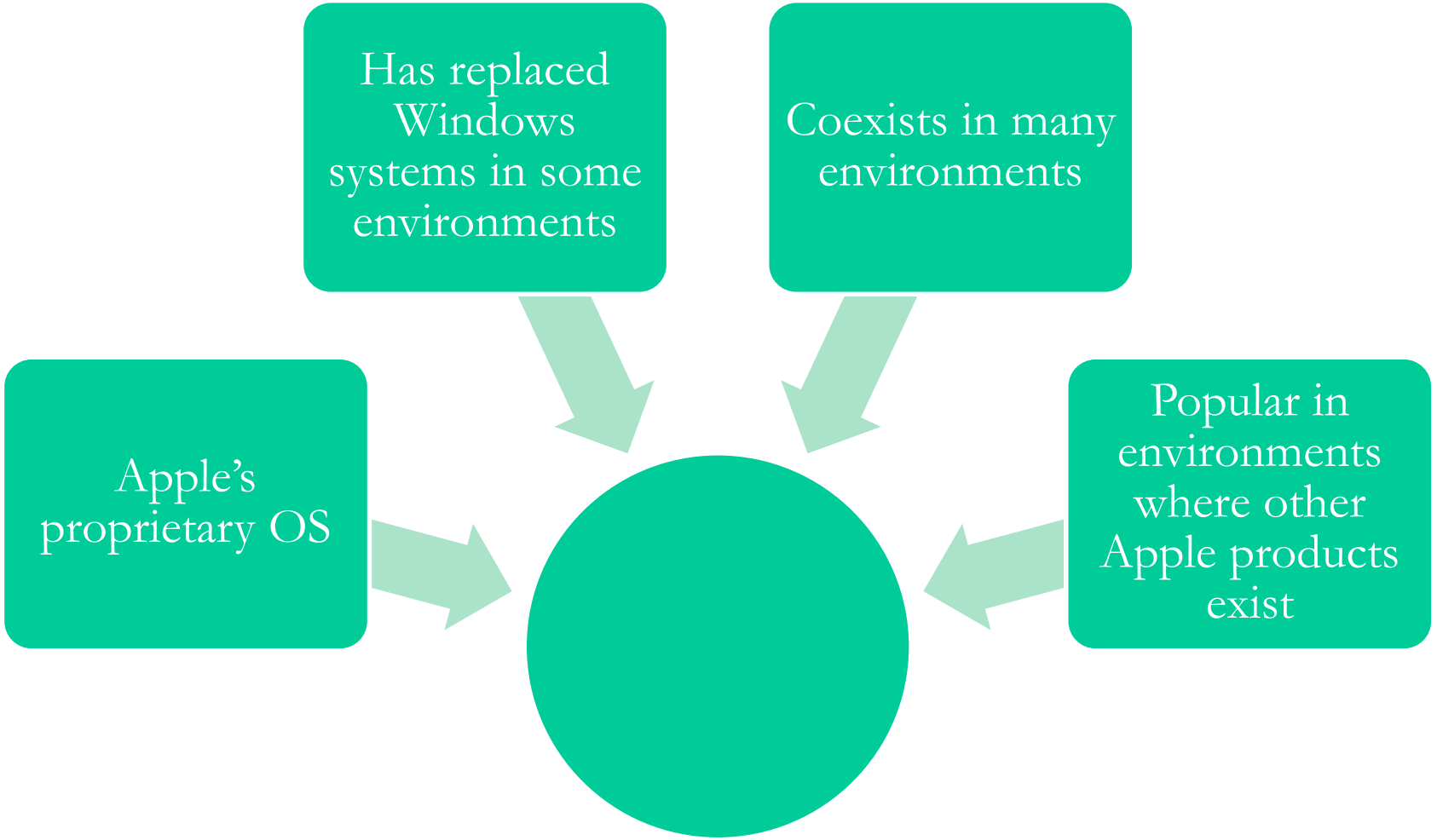
SYBEX

Windows Security Issues

- Windows is a huge target because of a large installed base.
- An endless stream of countless updates are hard to keep track of.
- The default configurations is left in place by many consumers.
- A large number of older or legacy systems still exist.

SYBEX

Apple's Mac OS X



Issues with Mac OS X

- The security solutions are lacking versus other platforms.
- There is naivety among users who feel that vulnerabilities do not exist.
- Features are generally all enabled and ready to use even if the user is not using them.

SYBEX

Linux

- Advanced operating system suited to tech enthusiasts
- Popular among techies, but also useful as a desktop OS
- Popular with pen testers
- Widely used as a server OS

SYBEX

Facts About Linux

- Higher level of knowledge required
- Least privilege is the default security model
- Open source allows for scrutiny by public
- Extremely flexible
- Present on many embedded devices

SYBEX

Next Step, Networks

A pen tester must understand the dynamics of networks.

Networks have clients and servers.

Servers provide services and data.

Clients are where users work.

SYBEX

Networks Types

Personal Area Network (PAN) → Local Area Network (LAN) → Municipal Area Network (MAN) → Wide Area Network (WAN)

Networks come in four different sizes, with each based on scale. Knowing each of the different types of networks is absolutely essential in planning and executing a successful penetration test.

SYBEX

Enter the OSI Model

Stands for Open System Interconnect

Old but useful model

Conceived in 1970s

Defines a common set of rules for vendors of hardware and software

Useful in placing attacks and other components into proper context

SYBEX

Seven Layers of OSI

- Application
- Presentation
- Session
- Transport
- Network
- Data Link
- Physical

SYBEX

TCP/IP

A suite of networking protocols used to exchange information

OSI influenced, but didn't create TCP/IP

Is one of many network protocols

- Is most popular
- Other protocols are essentially extinct

SYBEX

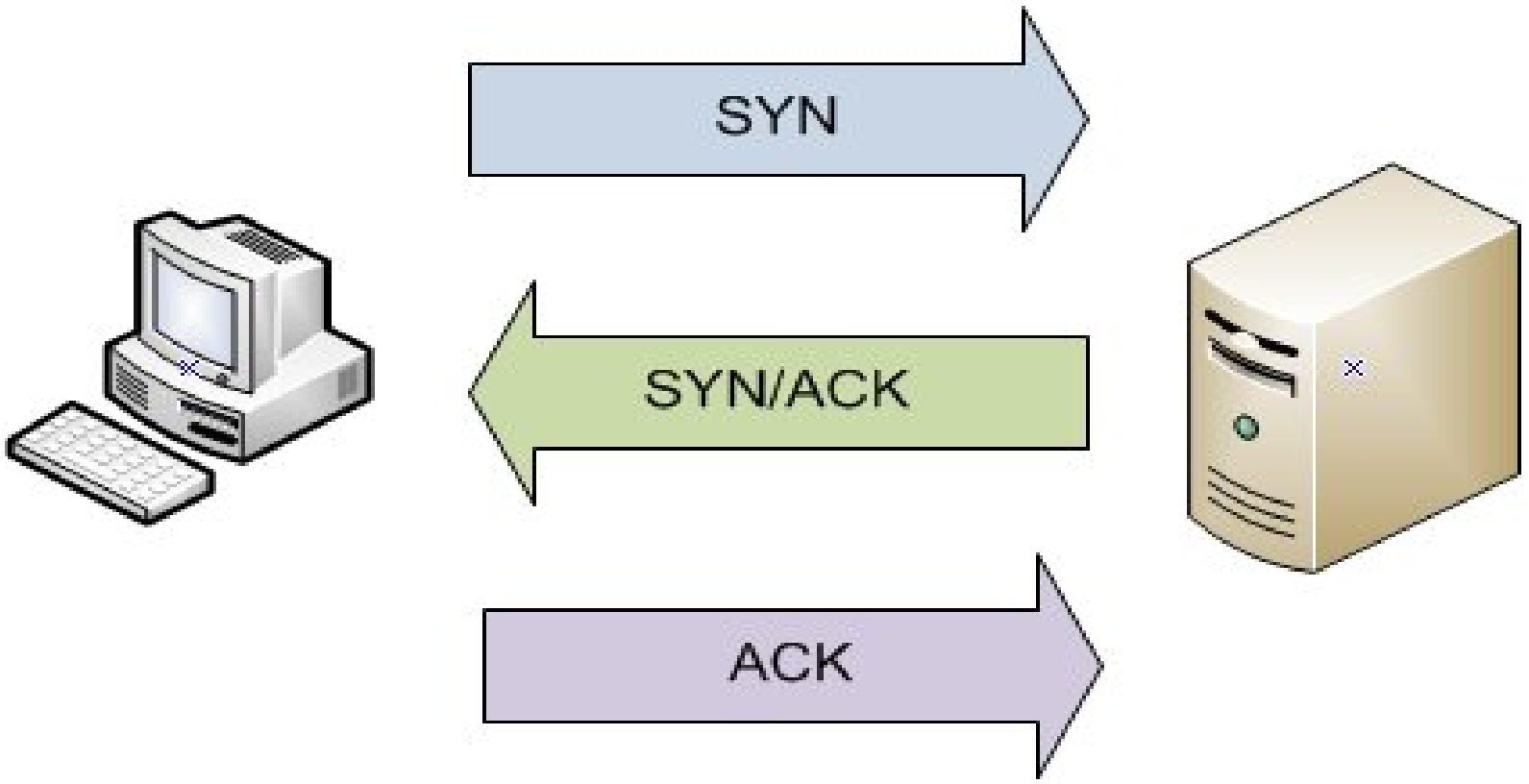
TCP vs. UDP

Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Reliable	Unreliable
Connection Oriented	Connectionless

A packet is a chunk of information transmitted over the network

SYBEX

TCP Three-Way Handshake



The three-way handshake is a process that TCP uses to initiate a connection between two points.

SYBEX

Working with UDP

User Datagram Protocol

Does not have error checking or acknowledgments like TCP

Stateless or connectionless protocol

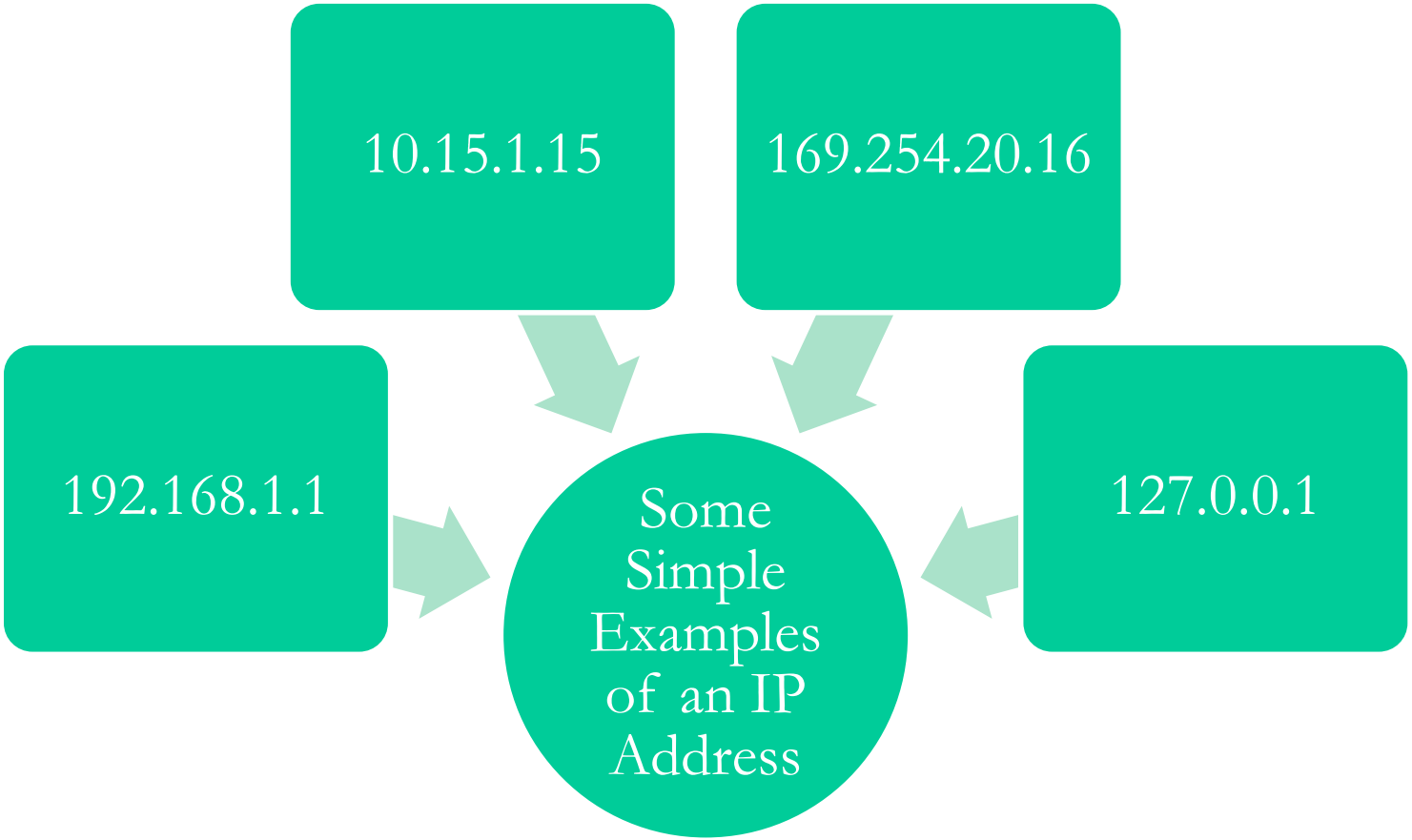
Less overhead than TCP

IP Addresses

- An IP address is a unique numeric identifier assigned to a host.
- Hosts are something attached to a network.
- A device attached to a network with an IP address is a host.
- Every packet has a source IP and destination IP.

SYBEX

Examples of IP Addresses



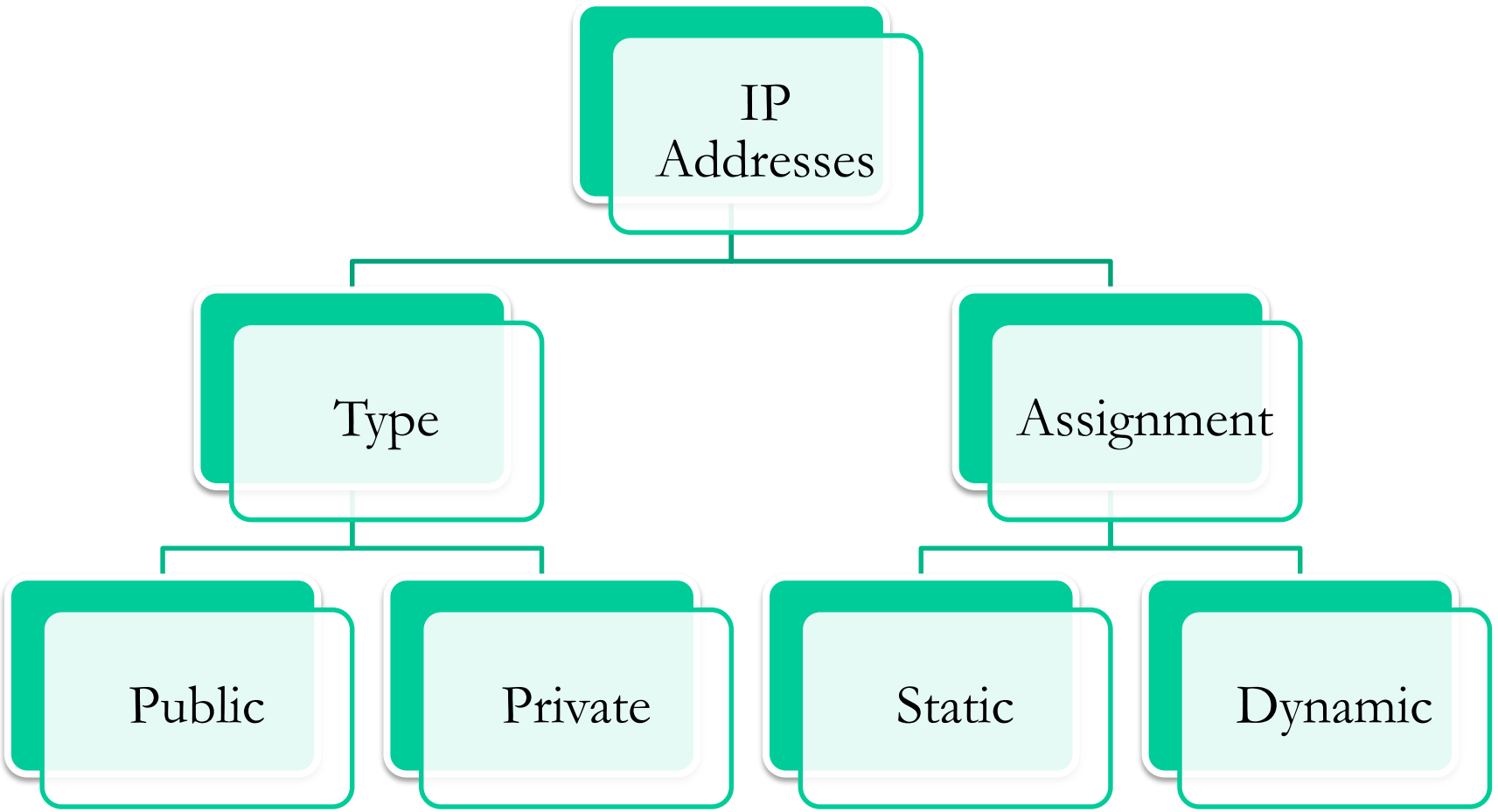
Each one of these addresses is considered a valid IP address, and each would be legal in their own individual situation.

IP Address Format

Written in dotted decimal format	• Separated by periods
Four numbers separated by decimal points	• 210.168.69.2
IP address is made up of network and host	• Network, Then Host

SYBEX

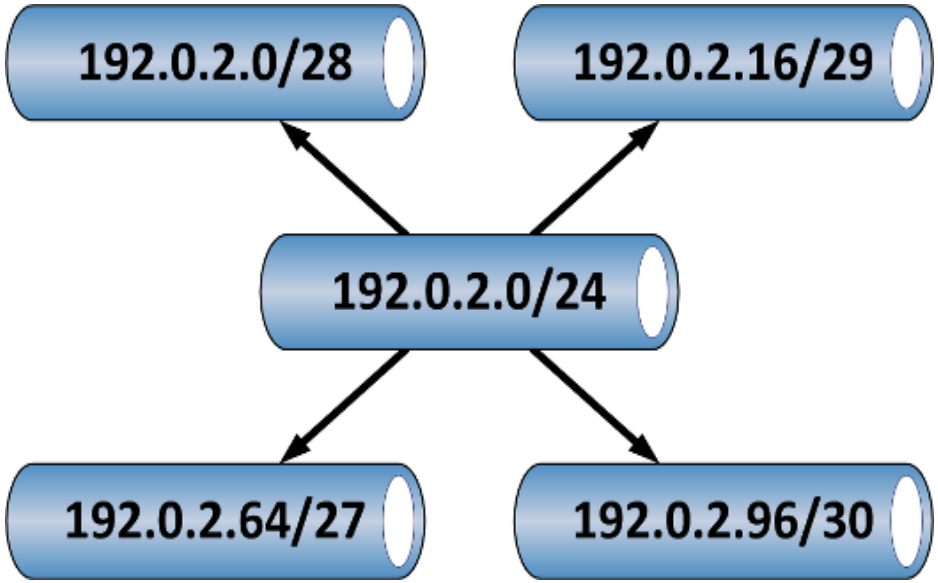
Types of IP Addresses



SYBEX

Types of IP Addresses

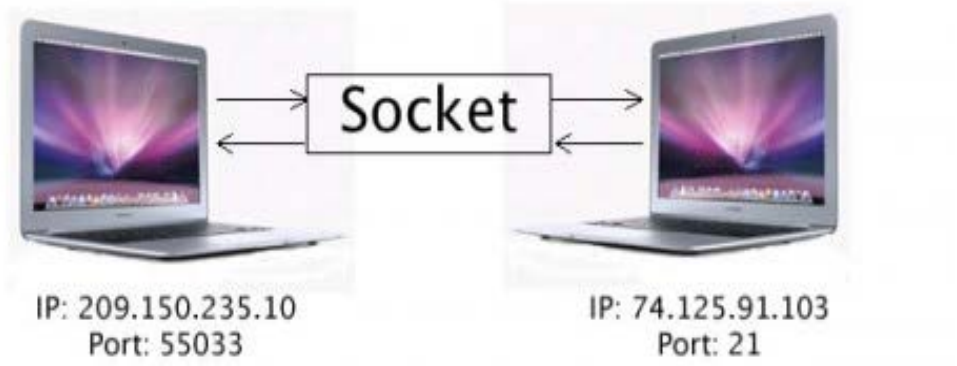
Subnetting is the logical breakdown of a network address space into smaller subnetworks.



SYBEX

About Ports

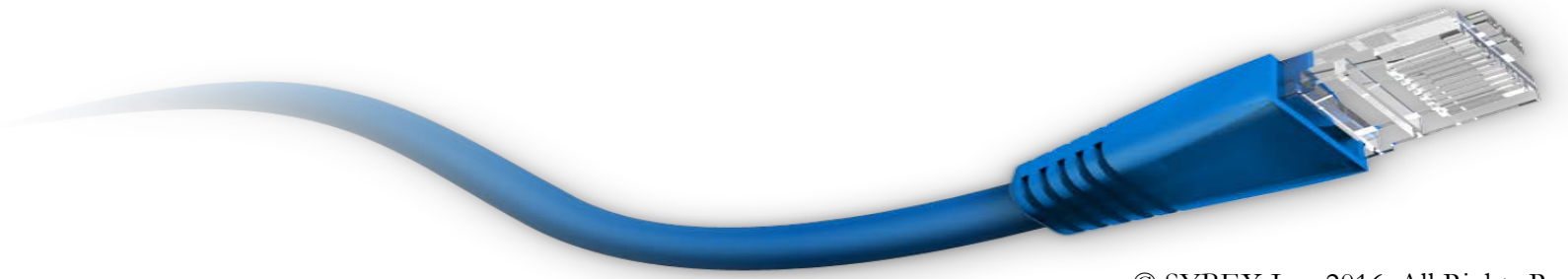
- Ports identify and categorize types of traffic.
- Each port is associated with a protocol or application.
- Ports ensure traffic will end up at the right location.
- They are represented in the format 192.168.1.10:80.



SYBEX

Port Ranges (TCP and UDP)

TCP and UDP		
Well-known ports	Registered ports	Dynamic ports
1 to 1024	1025 to 49151	49152 to 65535



SYBEX

Network Hardware

Networks contain various appliances.

Each controls the flow of traffic.

Having a basic overview of each is essential to a penetration tester.

SYBEX

Routers and Switches

Routers and switches are commonly used devices in networks.

Routers create and connect networks.

Switches create multiple broadcast domains.

A solid understanding of the functions of routers and switches will give you a substantial edge when ferreting out information on a target network.

SYBEX

What Is a Router?

Directs packets to the proper network and address

Works at the network layer

Works as a gateway between networks

Routers can use Network Address Translation (NAT)

- Used to translate a few public IPs to numerous private IPs

SYBEX

Looking at Switches

Deliver data based on hardware or physical address

- MAC addresses are physical addresses in a network card
- Come in the form of six pairs of characters in hexadecimal form
  - C0-cb-38-ad-2b-c4

Create collision and broadcast domains

SYBEX

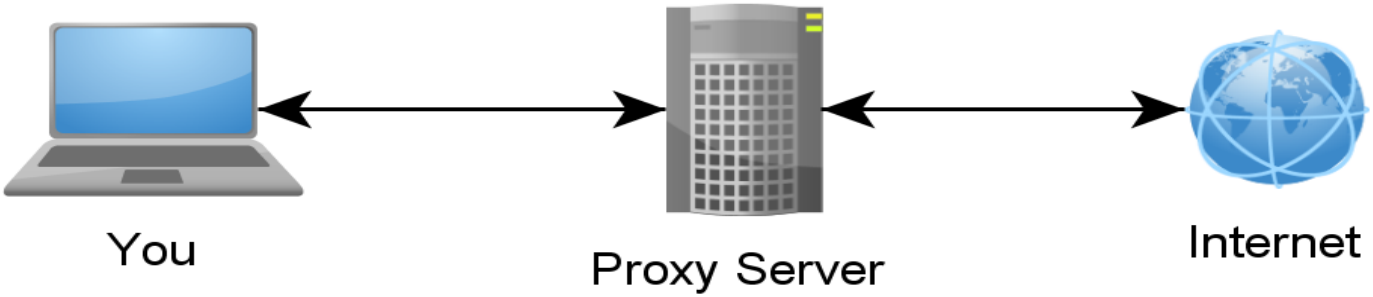
Proxies

Protect internal systems

Intermediaries between internal and external networks

Can filter content such as websites or other aspects

Can cache content



Firewalls

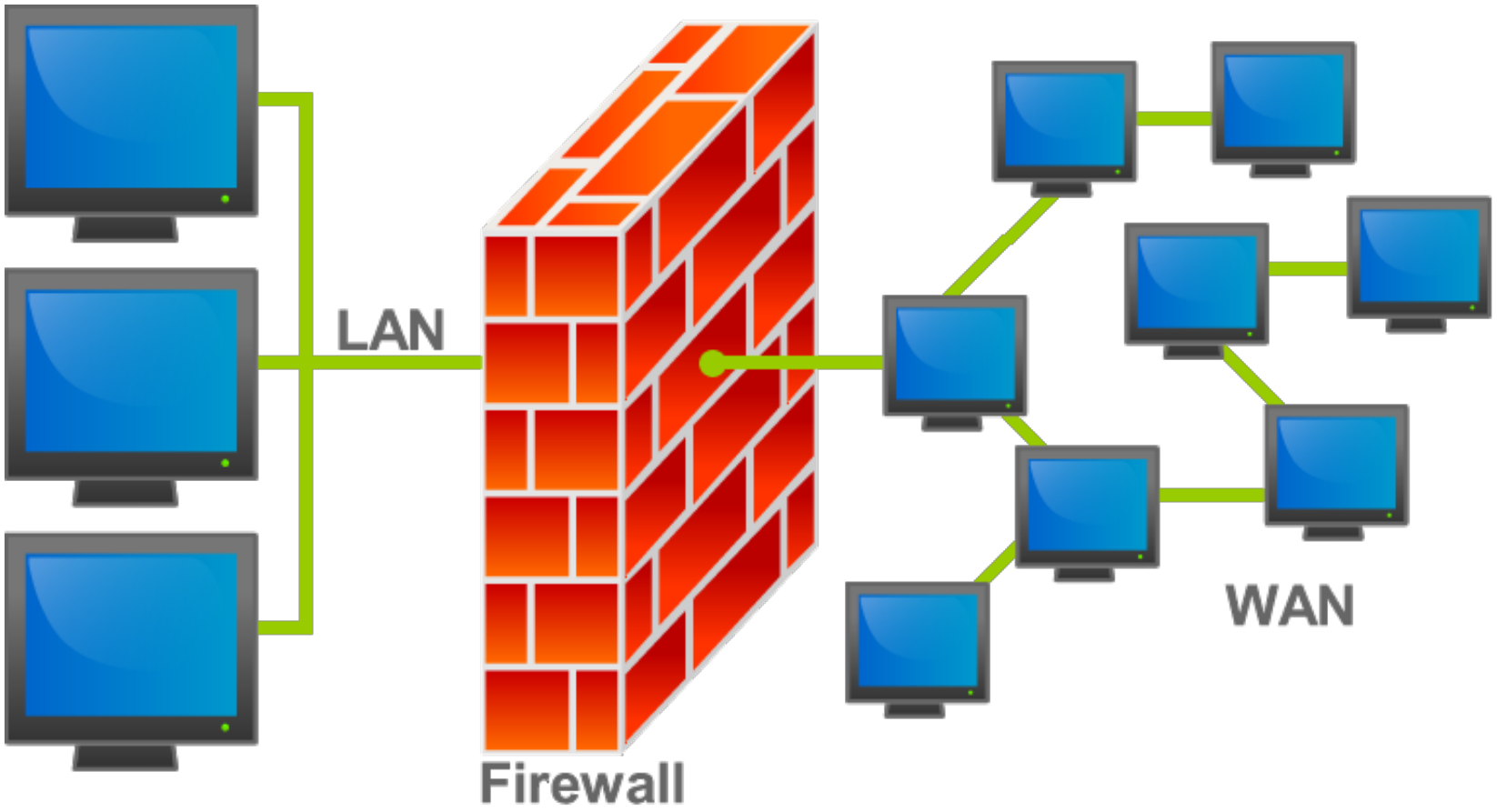
Control flow of traffic

- Caching of content
- Content filtering
- Examine traffic headers

Come in two main types

- Packet filtering
- Stateful packet filtering

Placement of a Firewall



SYBEX

Intrusion Detection System

- Intrusion detection system (IDS)
- Detects but doesn't stop malicious activity
- Can send an alert of logging an event
- Is a passive device
- Intrusion prevention systems (IPSs) are like IDSs but react to activity