CompTIA Security+

Exam Preparation Training Course

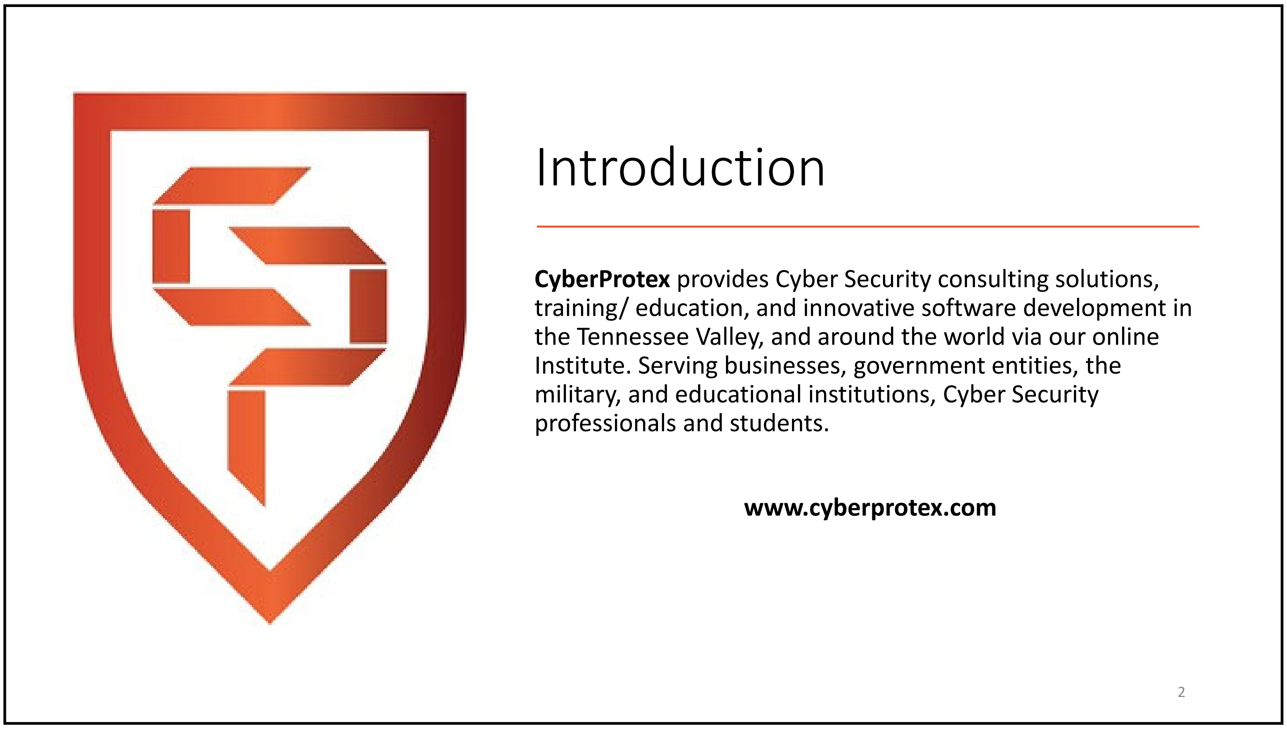
CyberProtex

Got Cyber?™

CompTIA AUTHORIZED PARTNER

CompTIA Security+

1

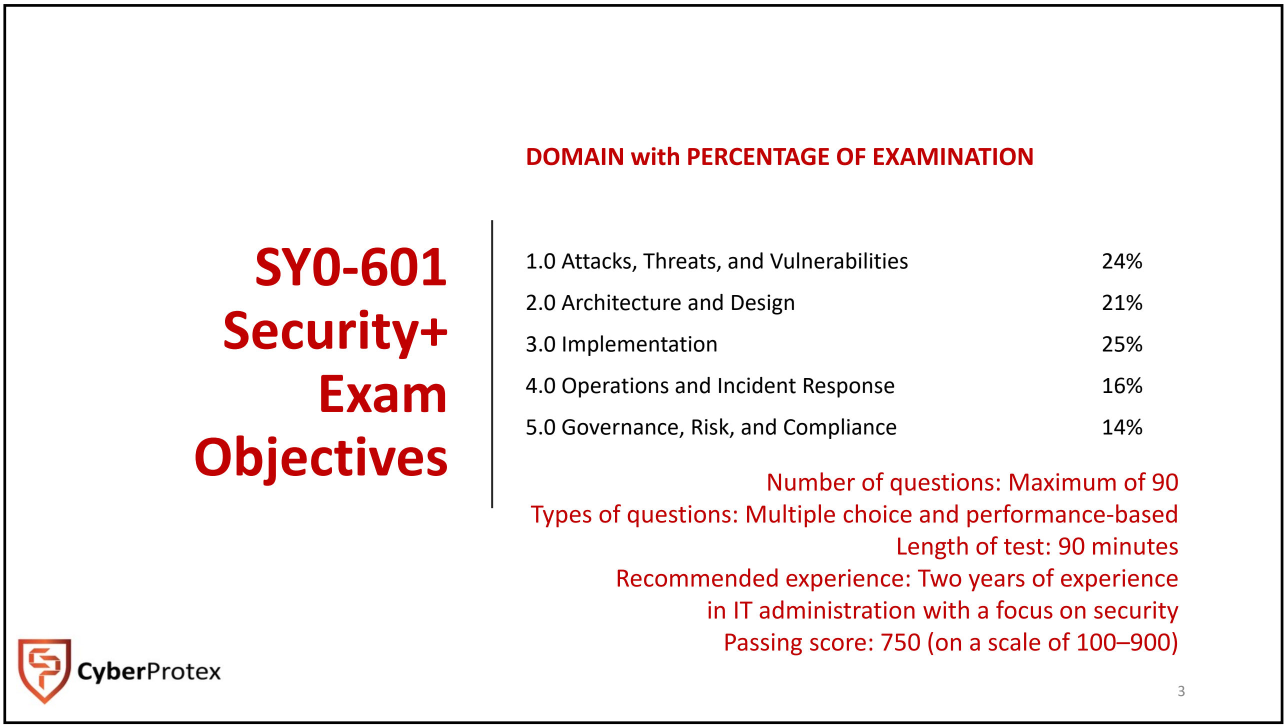


Introduction

CyberProtex provides Cyber Security consulting solutions, training/ education, and innovative software development in the Tennessee Valley, and around the world via our online Institute. Serving businesses, government entities, the military, and educational institutions, Cyber Security professionals and students.

www.cyberprotex.com

2



SY0-601 Security+ Exam Objectives

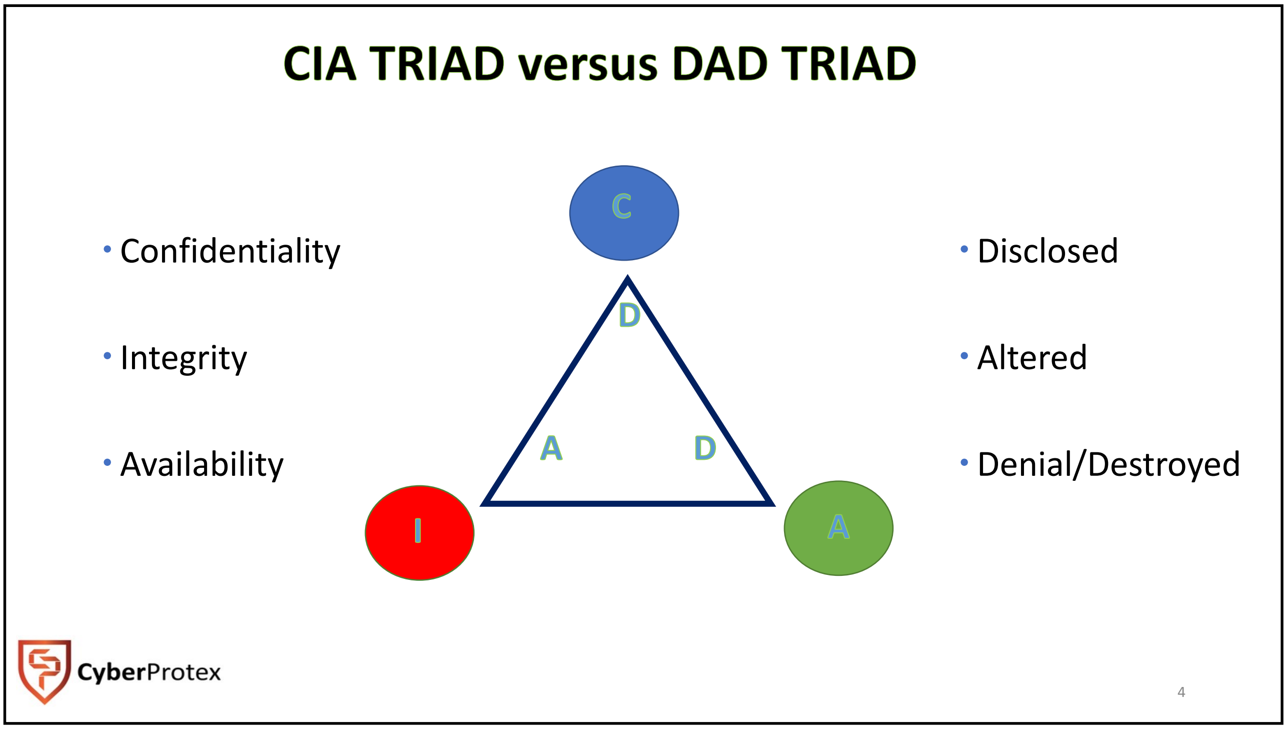
DOMAIN with PERCENTAGE OF EXAMINATION

1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%

Number of questions: Maximum of 90
Types of questions: Multiple choice and performance-based
Length of test: 90 minutes
Recommended experience: Two years of experience in IT administration with a focus on security
Passing score: 750 (on a scale of 100–900)

CyberProtex

3



CIA TRIAD versus DAD TRIAD

- Confidentiality
- Integrity
- Availability

- Disclosed
- Altered
- Denial/Destroyed

CyberProtex

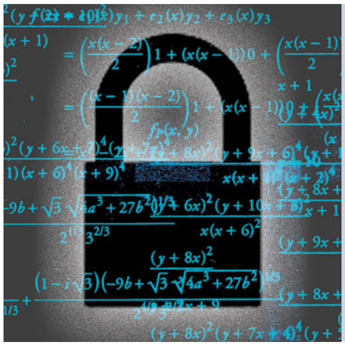
4

Confidentiality

- Confidentiality has been defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access" and is one of the cornerstones of information security.
- Confidential information must only be accessed, used, copied, or disclosed by users who have been authorized, and only when there is a genuine need.
- A confidentiality breach occurs when information or information systems have been, or may have been, accessed, used, copied, or disclosed, or by someone who was not authorized to have access to the information.

CyberProtex

Integrity

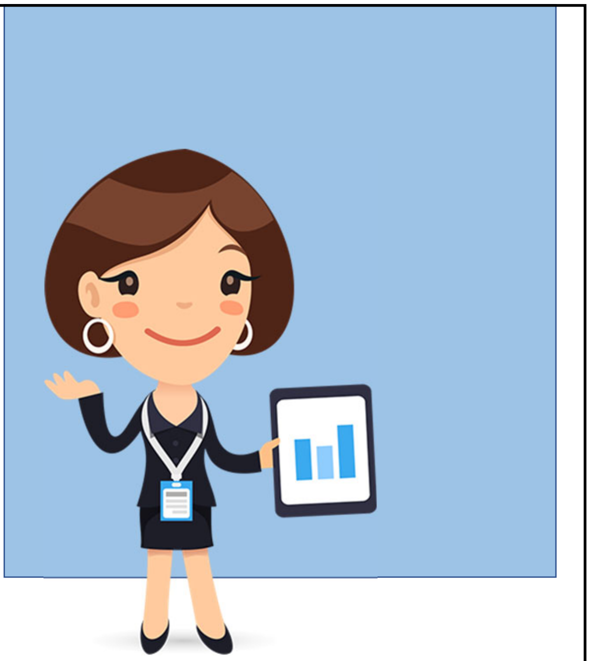


- ➢Integrity means data can not be created, changed, or deleted without proper authorization.
- ➢Data stored in one part of a database system is in agreement with other related data stored in another part of the database system (or another system).

CyberProtex

Availability

- Availability means that the information, the computing systems used to process the information, and the security controls used to protect the information are all available and functioning correctly when the information is needed.
- The opposite of availability is denial of service (DoS).

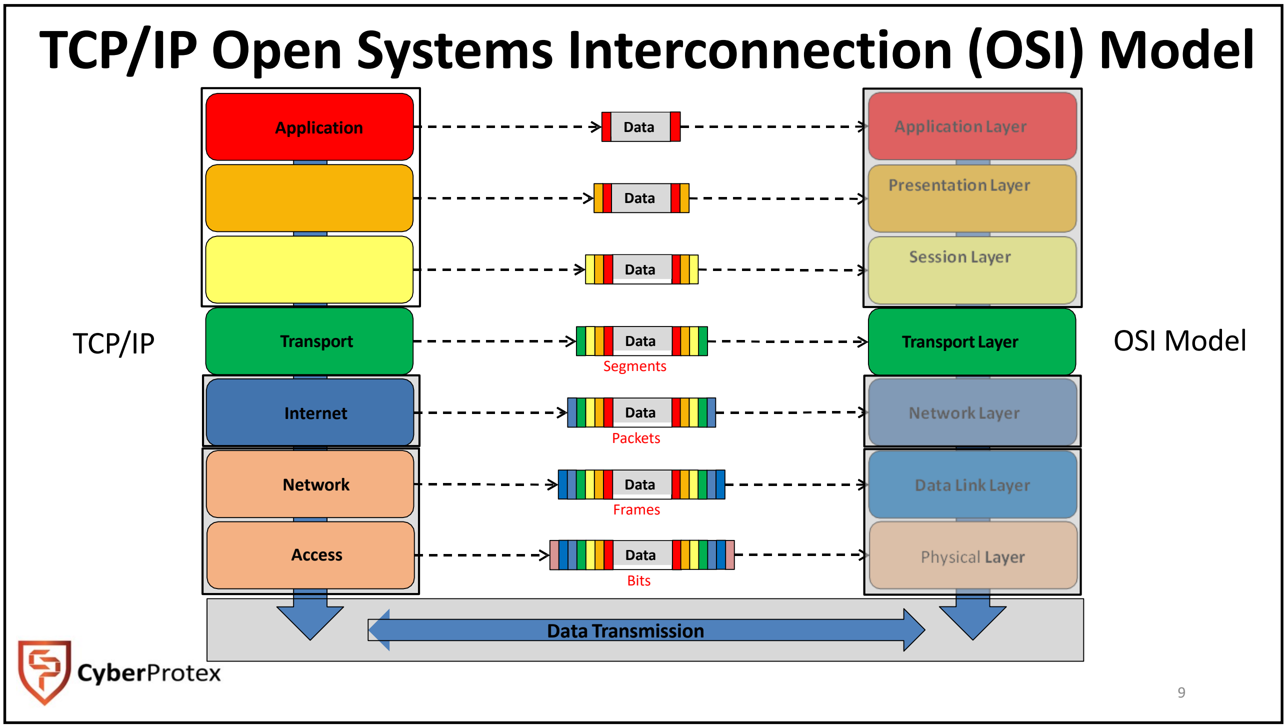


Transmission Control Protocol (TCP)/ Internet Protocol (IP)

➢TCP / IP is the underlying suite of protocols that aids in the creation, transmission, and reception of internet traffic

➢ TCP / IP contains four layers
  - ✓ Application Layer
  - ✓ Transport Layer
  - ✓ Internet Layer
  - ✓ Network Access Layer

➢ Host: Any device on a network that runs the TCP / IP protocol suite



TCP/IP Open Systems Interconnection (OSI) Model

TCP/IP

Application

Transport

Internet

Network

Access

Data

Data

Data

Data

Segments

Data

Packets

Data

Frames

Data

Bits

Application Layer

Presentation Layer

Session Layer

Transport Layer

Network Layer

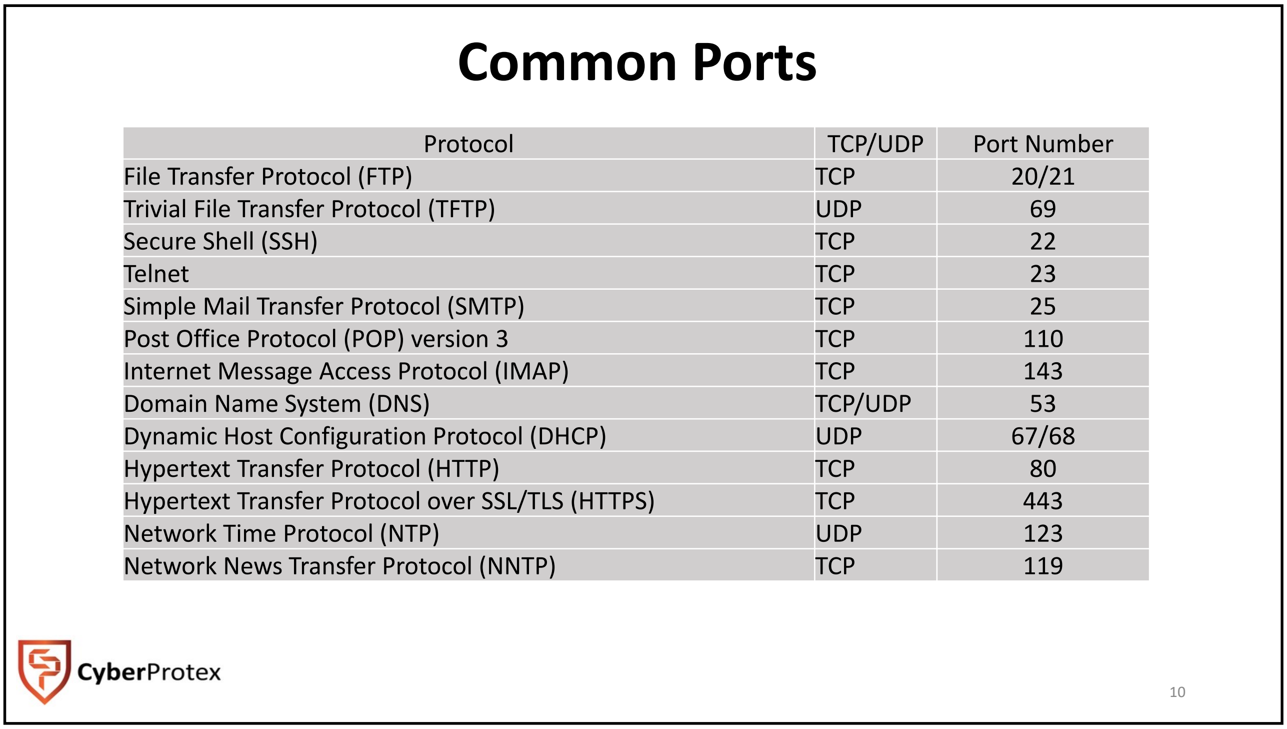
Data Link Layer

Physical Layer

OSI Model

Data Transmission

CyberProtex



Common Ports

Protocol	TCP/UDP	Port Number
File Transfer Protocol (FTP)	TCP	20/21
Trivial File Transfer Protocol (TFTP)	UDP	69
Secure Shell (SSH)	TCP	22
Telnet	TCP	23
Simple Mail Transfer Protocol (SMTP)	TCP	25
Post Office Protocol (POP) version 3	TCP	110
Internet Message Access Protocol (IMAP)	TCP	143
Domain Name System (DNS)	TCP/UDP	53
Dynamic Host Configuration Protocol (DHCP)	UDP	67/68
Hypertext Transfer Protocol (HTTP)	TCP	80
Hypertext Transfer Protocol over SSL/TLS (HTTPS)	TCP	443
Network Time Protocol (NTP)	UDP	123
Network News Transfer Protocol (NNTP)	TCP	119

CyberProtex

Common Ports

Protocol	TCP/UDP	Port Number
Network Basic Input/Output System (NetBIOS)	TCP/UDP	135/137/138/139
Simple Network Management Protocol (SNMP)	TCP/UDP	161/162
Lightweight Directory Access Protocol (LDAP)	TCP/UDP	389
Lightweight Directory Access Protocol over TLS/SSL (LDAPS)	TCP/UDP	636
Kerberos	TCP	88
Syslog	TCP	514
TCP SMB	TCP	445
Remote Desktop Protocol (RDP)	TCP	3389
MSSQL	TCP	1433
MYSQL	TCP	3306

CyberProtex

Encapsulation/Decapsulation

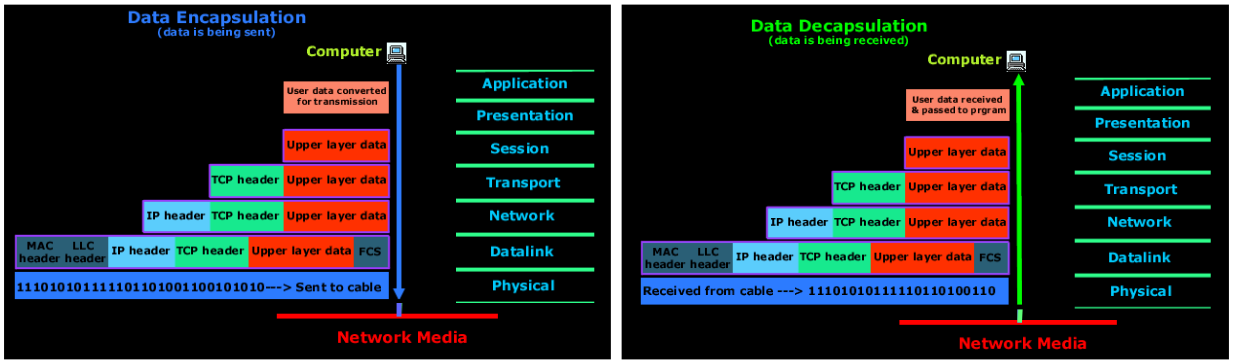


Image Courtesy of: Data Encapsulation & Decapsulation in the OSI Model. http://www.firewall.cx/networking-topics/the-osi-model/179-osi-data-encapsulation.html

CyberProtex

Encapsulation/Decapsulation

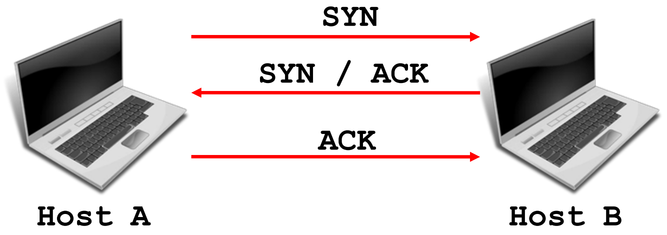
						A						
					P	A	P					
				S	P	A	P	S				
			T	S	P	A	P	S	T			
		N	T	S	P	A	P	S	T	N		
	DL	N	T	S	P	A	P	S	T	N	DL	
P	DL	N	T	S	P	A	P	S	T	N	DL	P

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

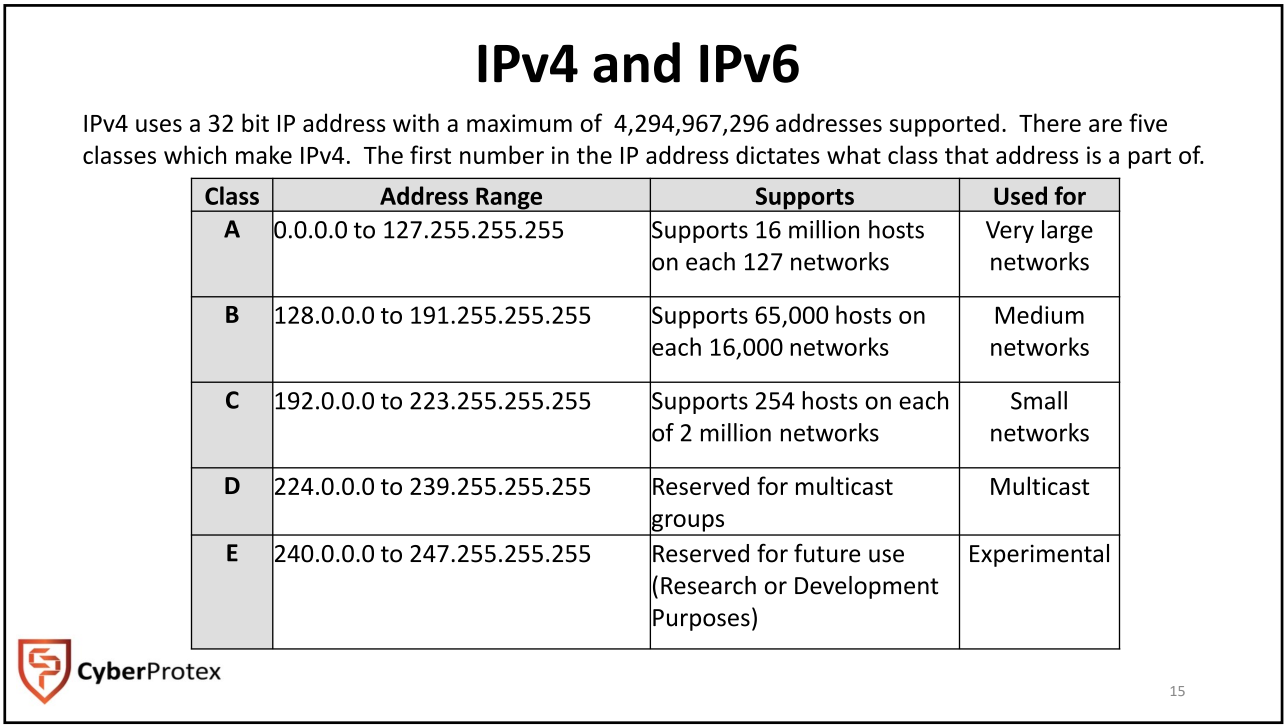
CyberProtex

TCP Connection Process

- ➢ In order to communicate with TCP, hosts must first establish a connection
- ➢ This is achieved with a "three-way" handshake



CyberProtex

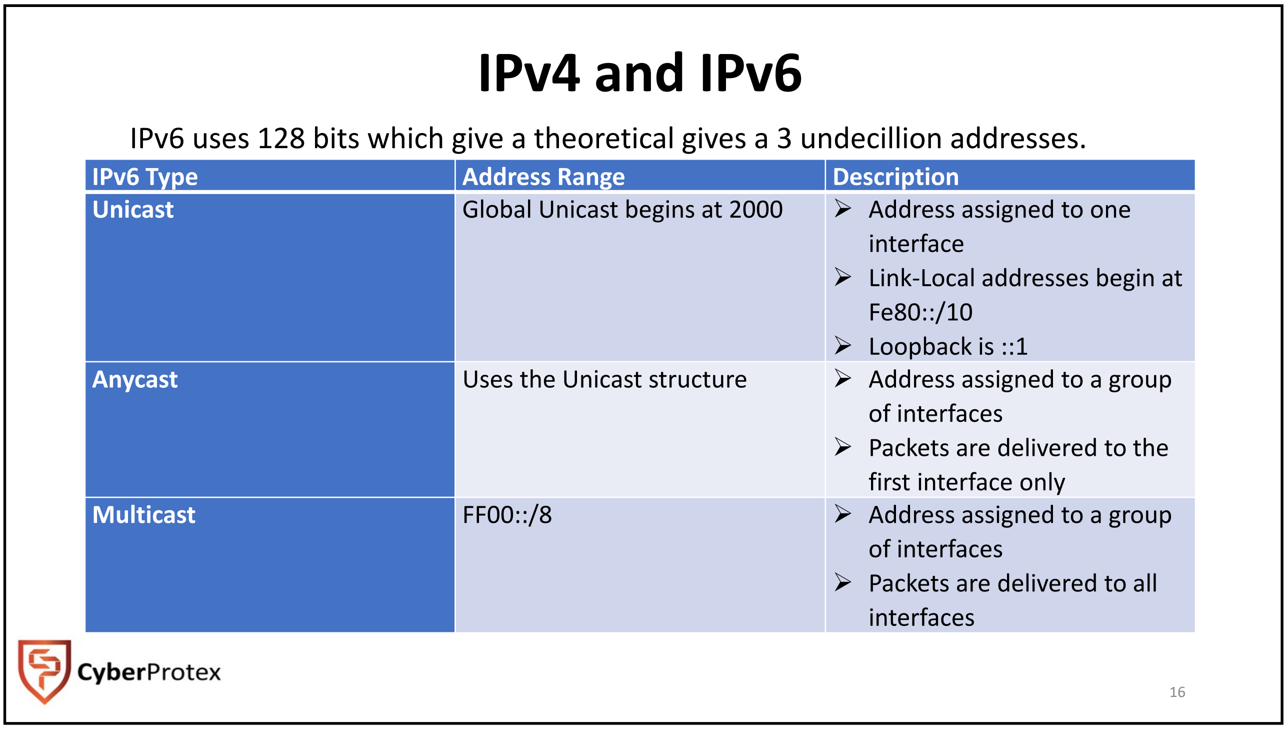


IPv4 and IPv6

IPv4 uses a 32 bit IP address with a maximum of 4,294,967,296 addresses supported. There are five classes which make IPv4. The first number in the IP address dictates what class that address is a part of.

Class	Address Range	Supports	Used for
A	0.0.0.0 to 127.255.255.255	Supports 16 million hosts on each 127 networks	Very large networks
B	128.0.0.0 to 191.255.255.255	Supports 65,000 hosts on each 16,000 networks	Medium networks
C	192.0.0.0 to 223.255.255.255	Supports 254 hosts on each of 2 million networks	Small networks
D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups	Multicast
E	240.0.0.0 to 247.255.255.255	Reserved for future use (Research or Development Purposes)	Experimental

CyberProtex



IPv4 and IPv6

IPv6 uses 128 bits which give a theoretical gives a 3 undecillion addresses.

IPv6 Type	Address Range	Description
Unicast	Global Unicast begins at 2000	➢ Address assigned to one interface ➢ Link-Local addresses begin at Fe80::/10 ➢ Loopback is ::1
Anycast	Uses the Unicast structure	➢ Address assigned to a group of interfaces ➢ Packets are delivered to the first interface only
Multicast	FF00::/8	➢ Address assigned to a group of interfaces ➢ Packets are delivered to all interfaces

CyberProtex