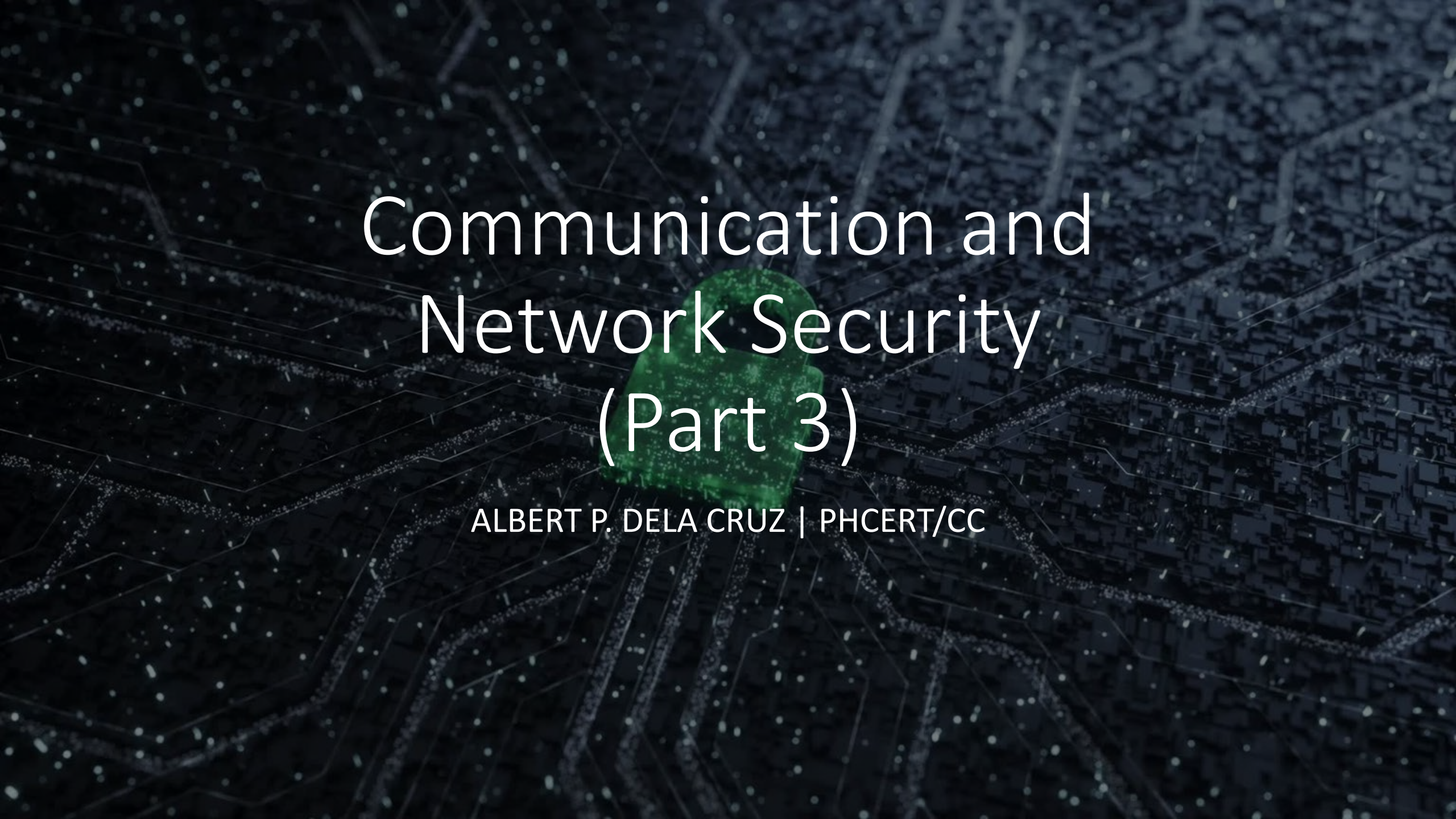
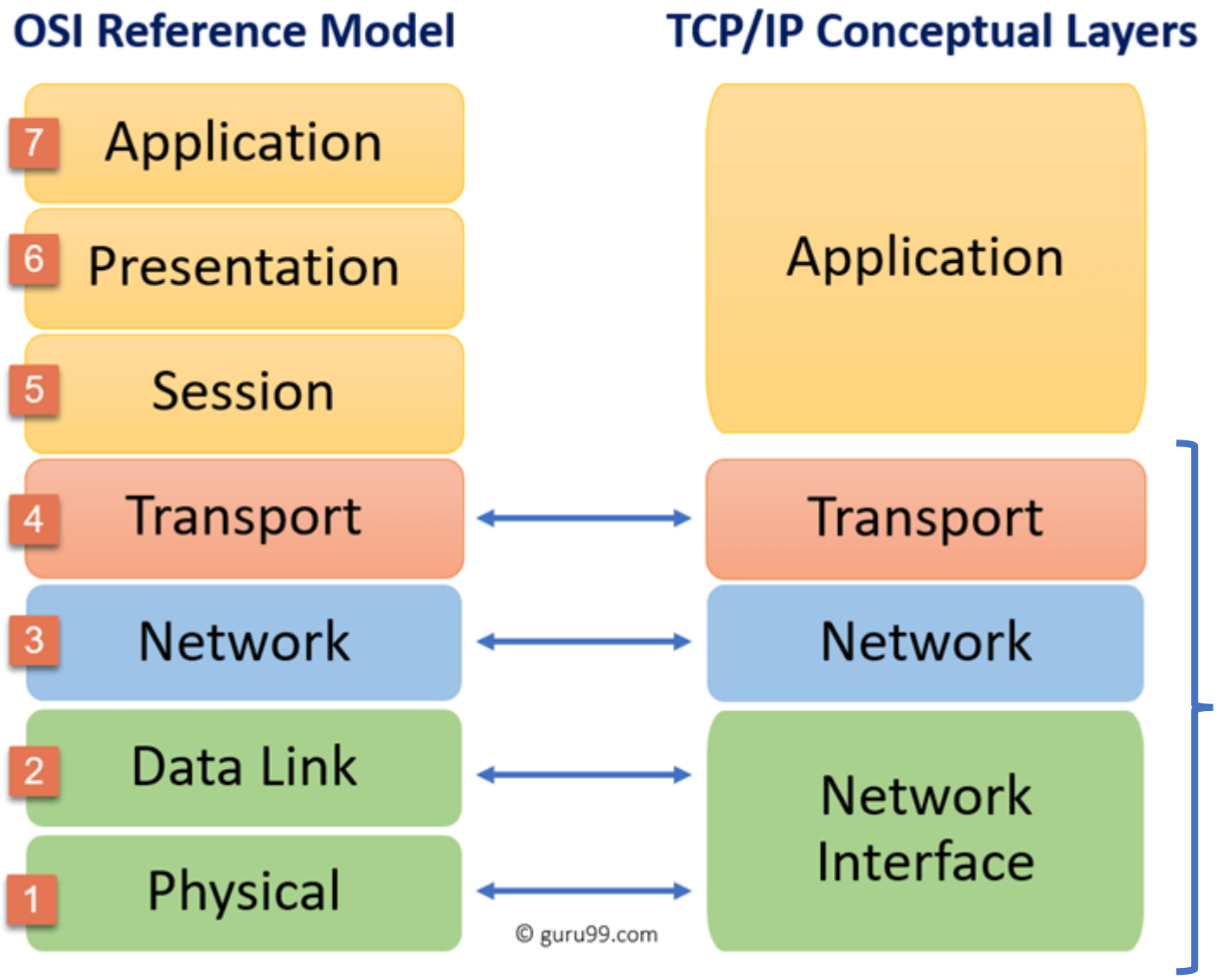


Communication and Network Security (Part 3)

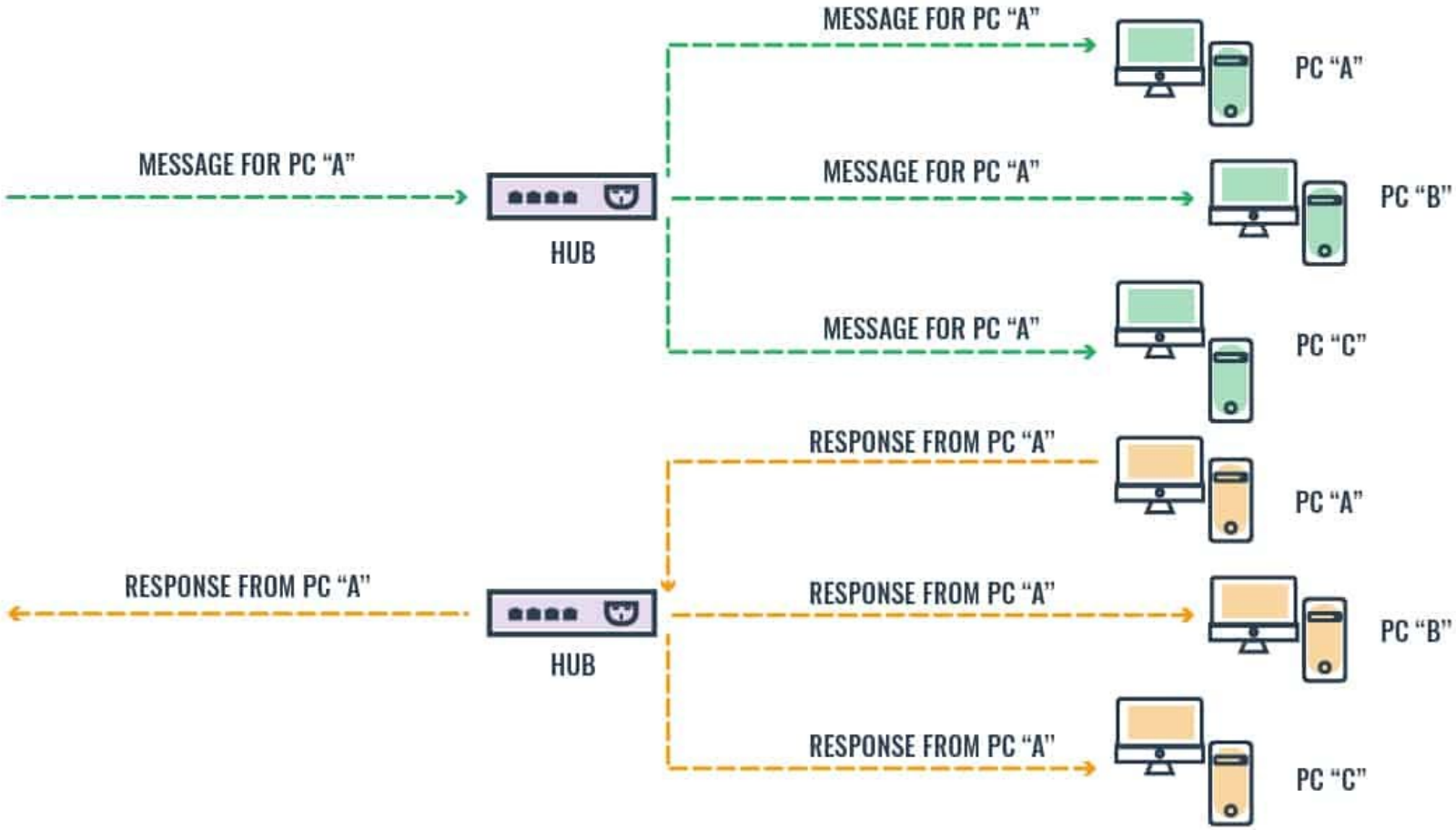
ALBERT P. DELA CRUZ | PHCERT/CC


OSI Reference Model
TCP/IP Conceptual Layers
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
Application
Transport
Network
Network Interface
© guru99.com

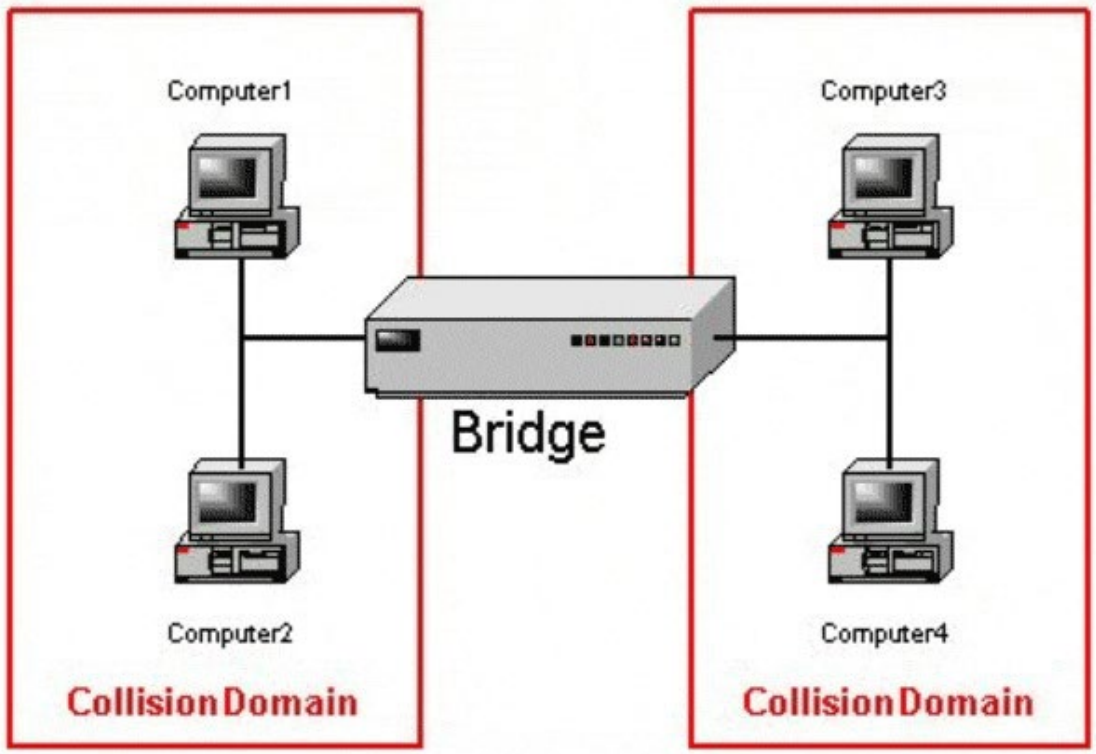
Secure Network Devices and Protocols

Repeaters and Hubs

- Repeater - simplest type of connectivity device that regenerates a digital signal
  - Operates in the Physical Layer
    - Cannot Improve or Correct Bad or Erroneous Signals
  - Regenerate signal over the entire segment
  - (Usually) One input and one output port
  - Suited only to bus topology networks
- Hubs – functions like a repeater but generally is a 'multiport' version
  - Used as a central device
  - Connects computers in a star topology
  - Cannot Filter network Traffic
  - Regenerates signals and broadcasts them to all ports



Repeaters and Hubs

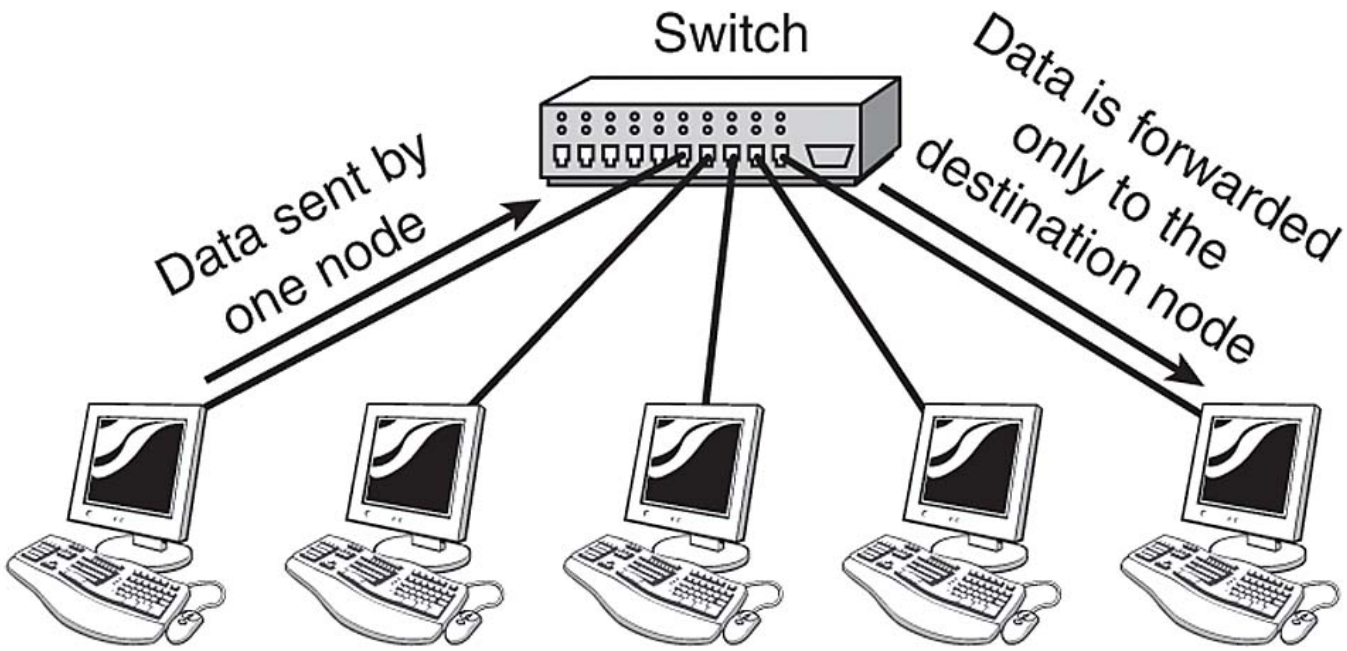


Bridges

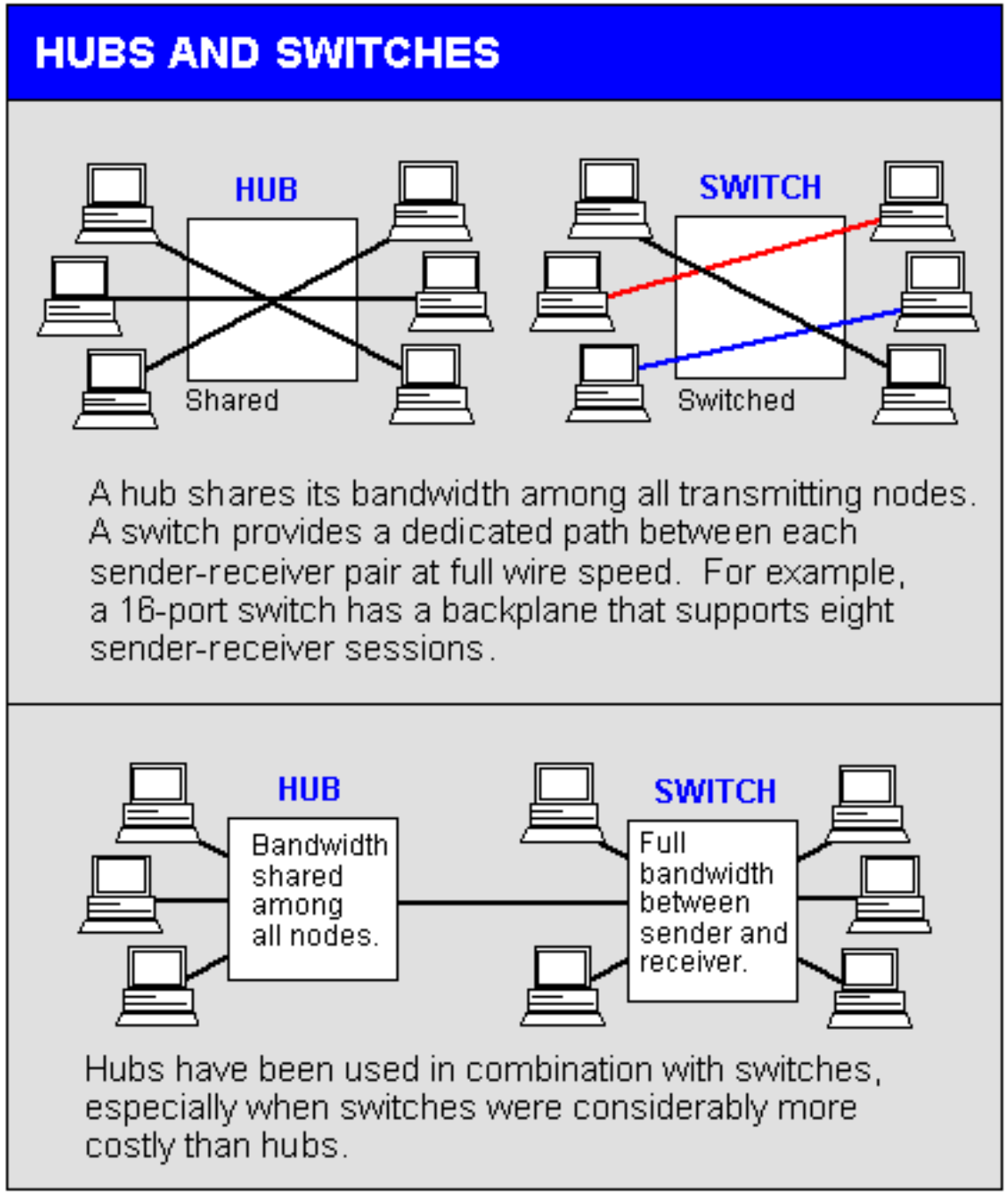
- A network bridge is a computer networking device that creates a single, aggregate network from multiple communication networks or network segments.

Switches

- A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device.
- A network switch is a multiport network bridge that uses MAC addresses to forward data at the data link layer of the OSI model

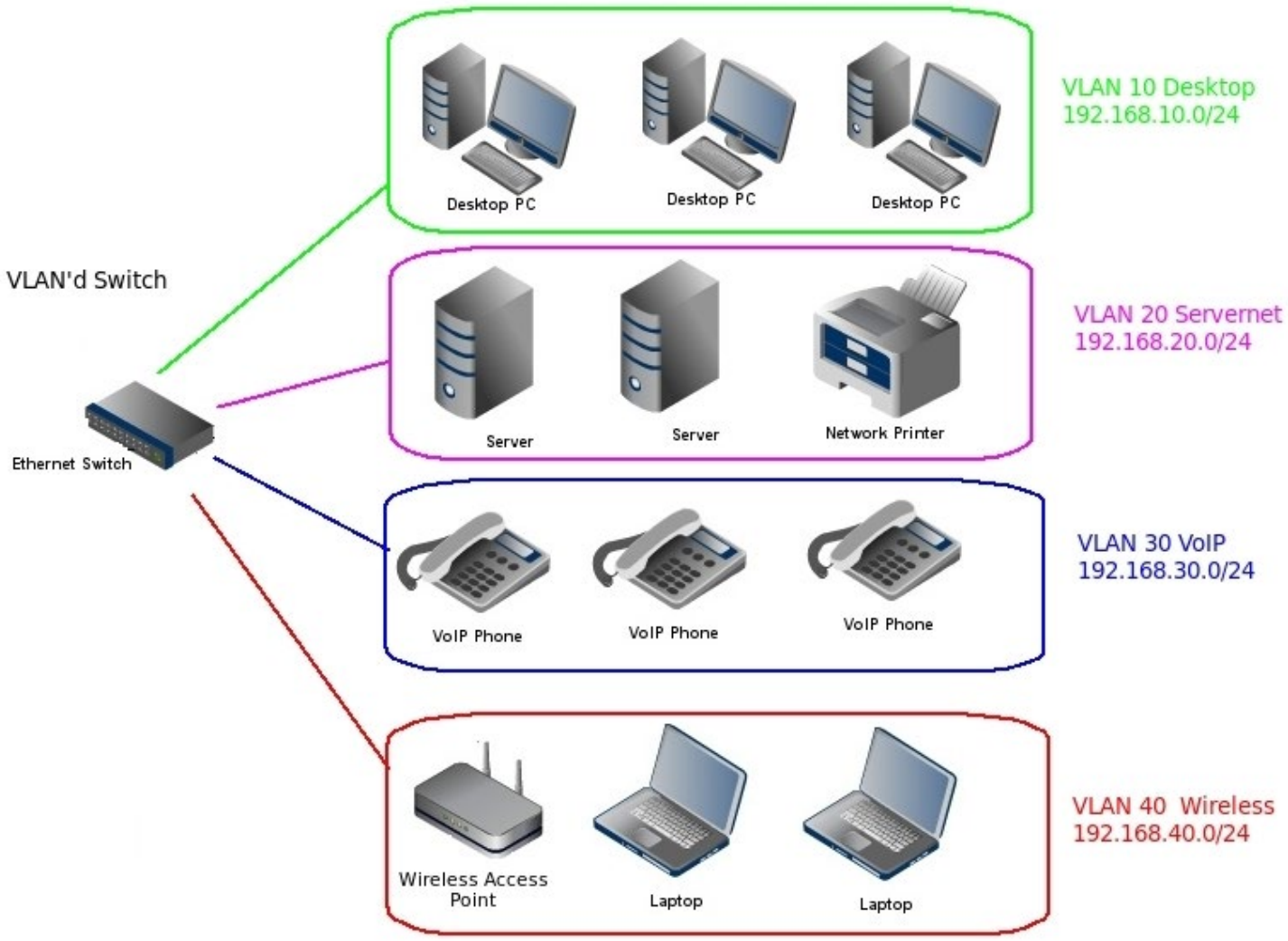


Switches vs Hubs

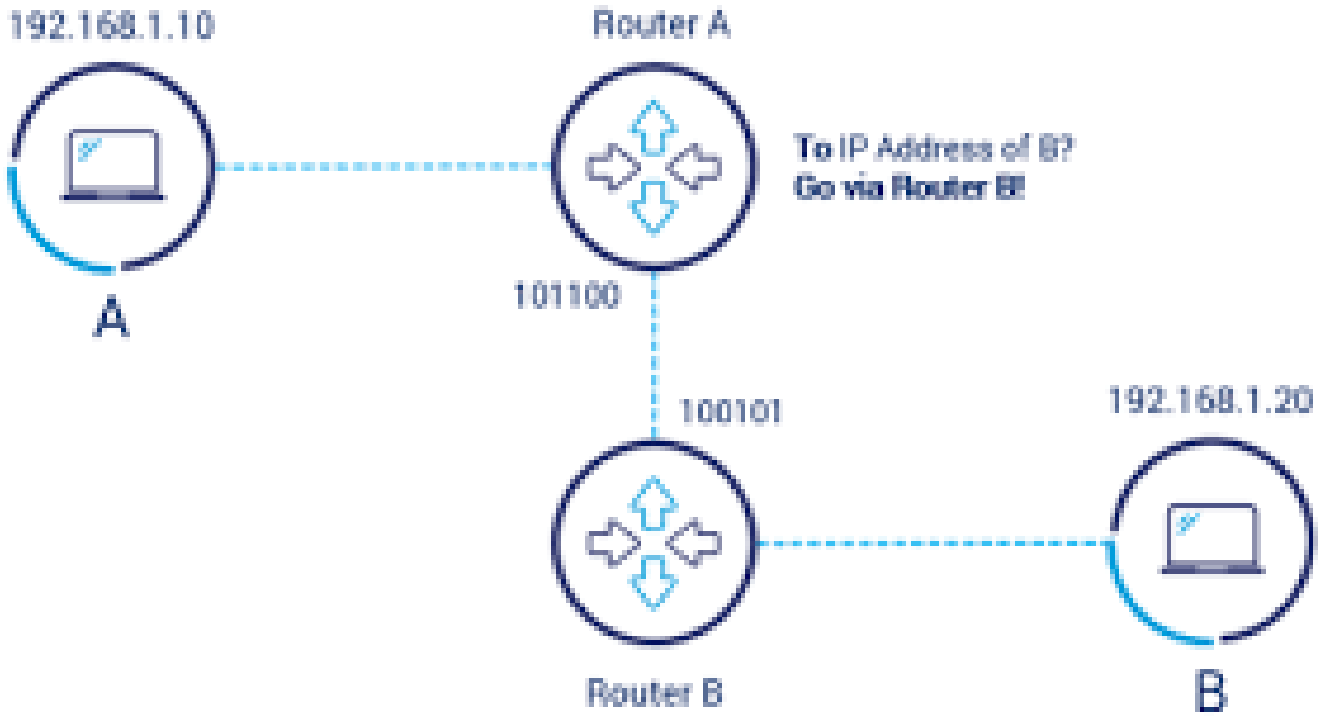


VLANs

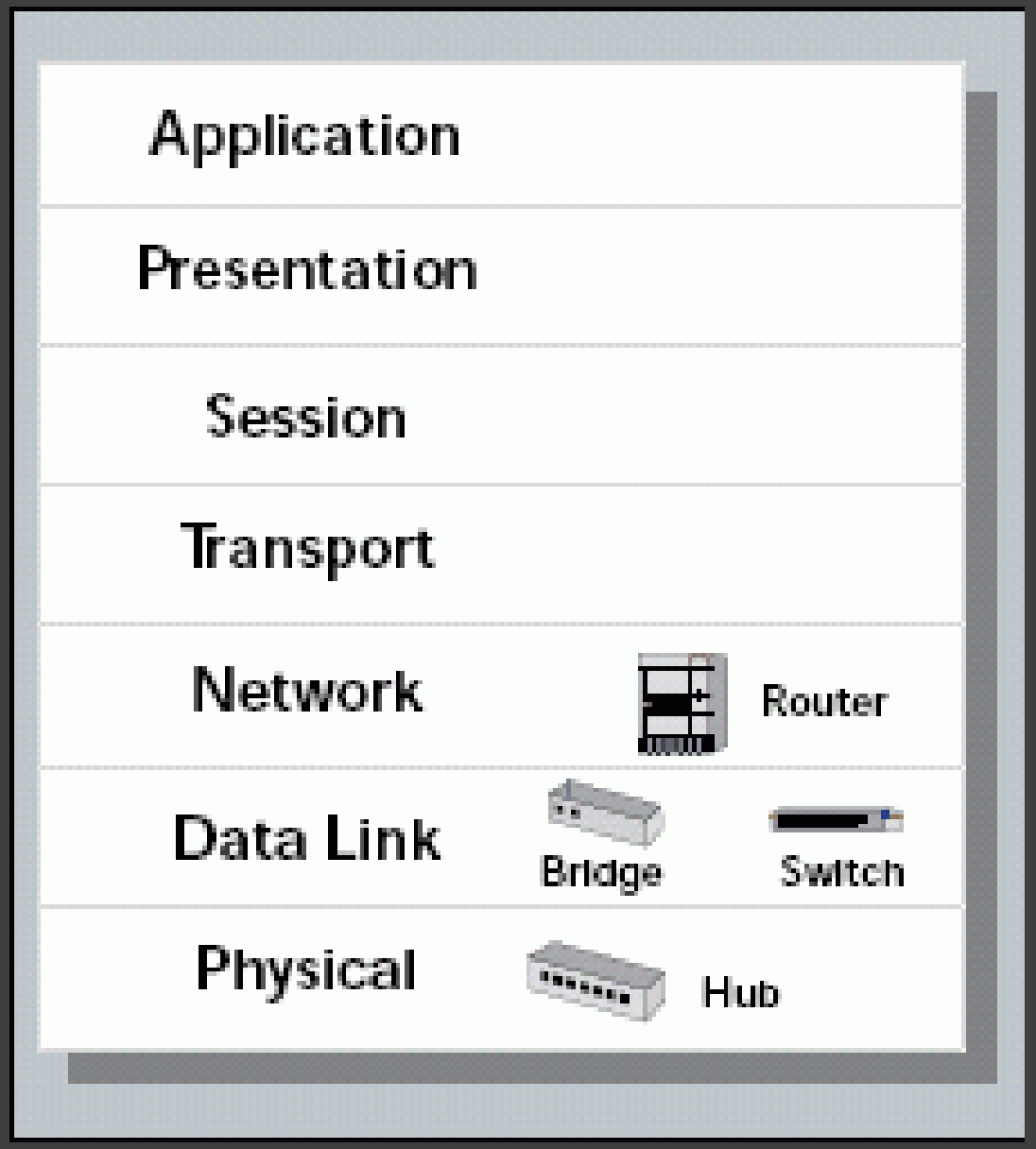
- A virtual LAN (VLAN) is a logical overlay network that groups together a subset of devices that share a physical LAN, isolating the traffic for each group.



Routers

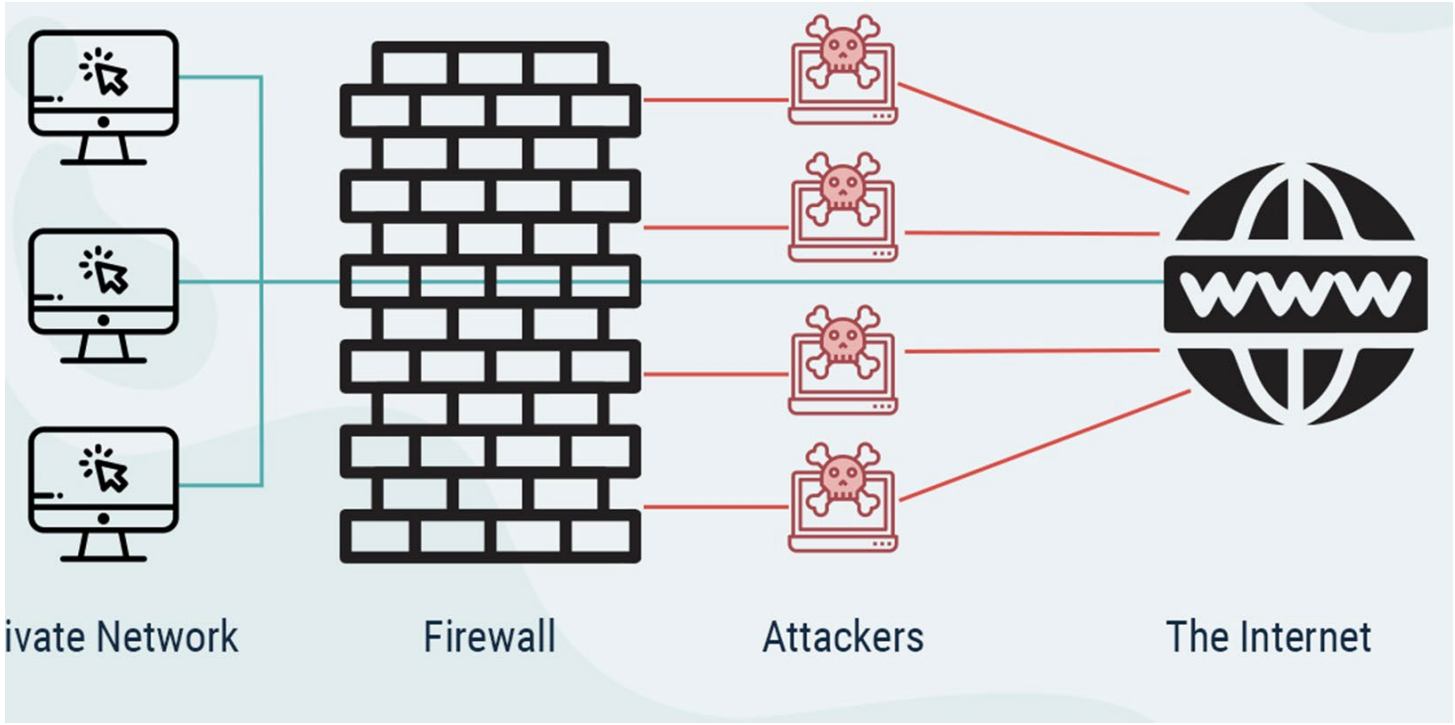


- A router is a device that connects two or more packet-switched networks or subnetworks. It serves two primary functions: managing traffic between these networks by forwarding data packets to their intended IP addresses, and allowing multiple devices to use the same Internet connection.

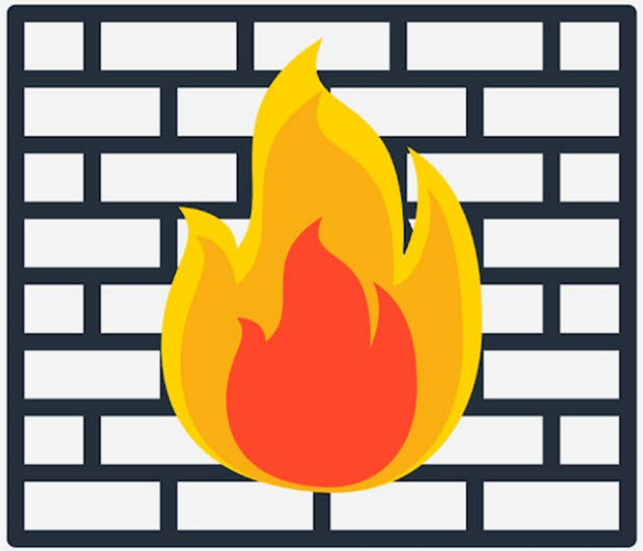


Network Devices and the OSI Model

Firewalls



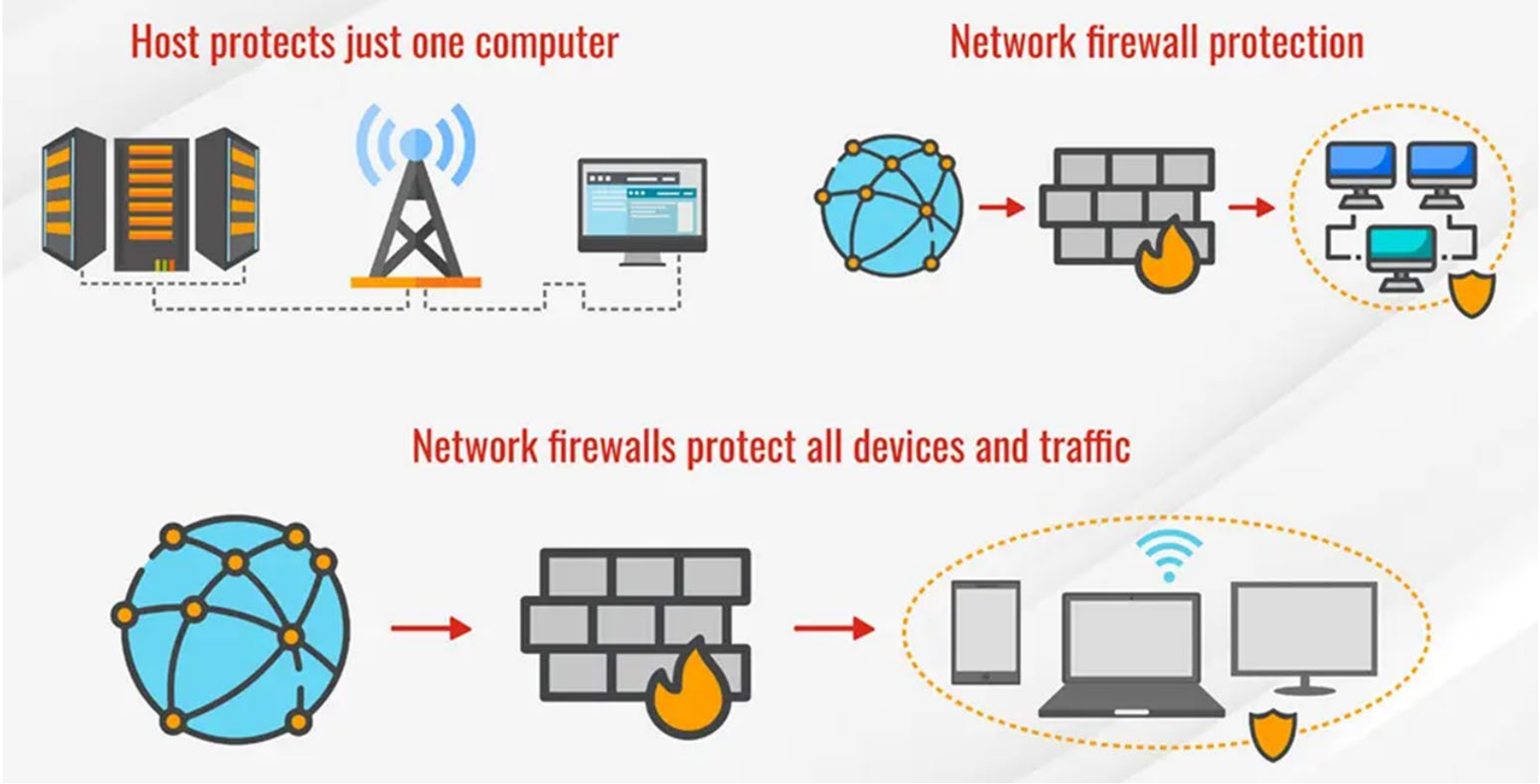
- A firewall is a network security device that monitors traffic to or from your network. It allows or blocks traffic based on a defined set of security rules.

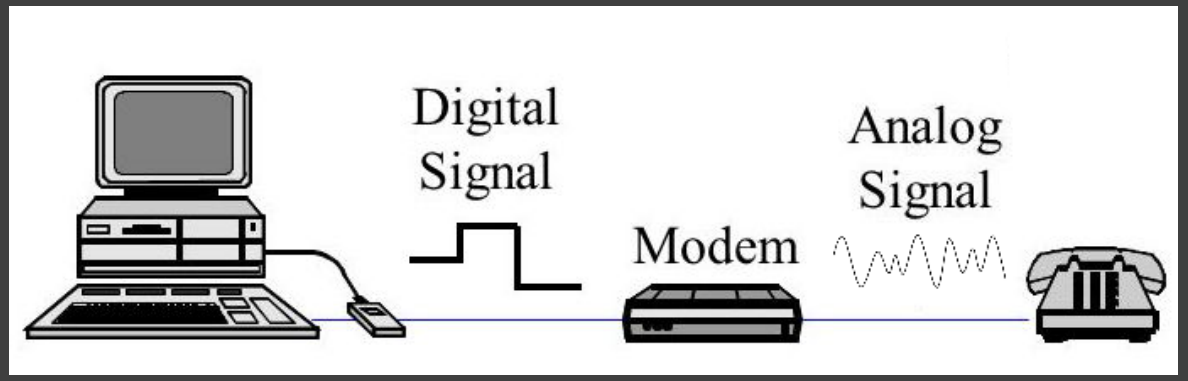


1. Defend resources
2. Validate access
3. Manage and control network traffic
4. Record and report on events
5. Act as an intermediary

Firewall Tasks

Host-based vs. Network-based Firewalls



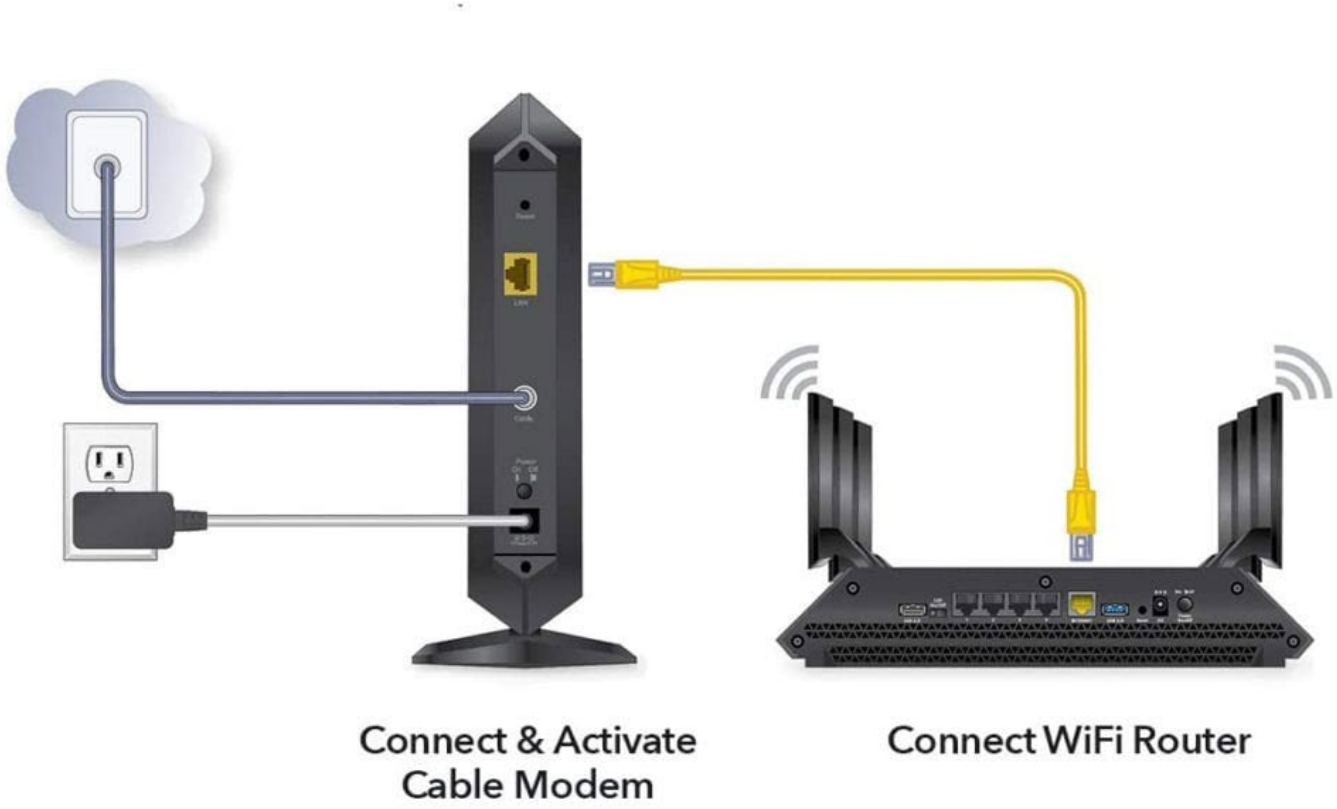


Modems

- BEFORE: A modulator-demodulator or modem is a computer hardware device that converts data from a digital format into a format suitable for an analog transmission medium such as telephone or radio.

Modems

- NOW: A device that takes the signals that come from your Internet Service Provider, or ISP, and translates them into an Internet connection for your Wi-Fi router to broadcast.




Secure Communications

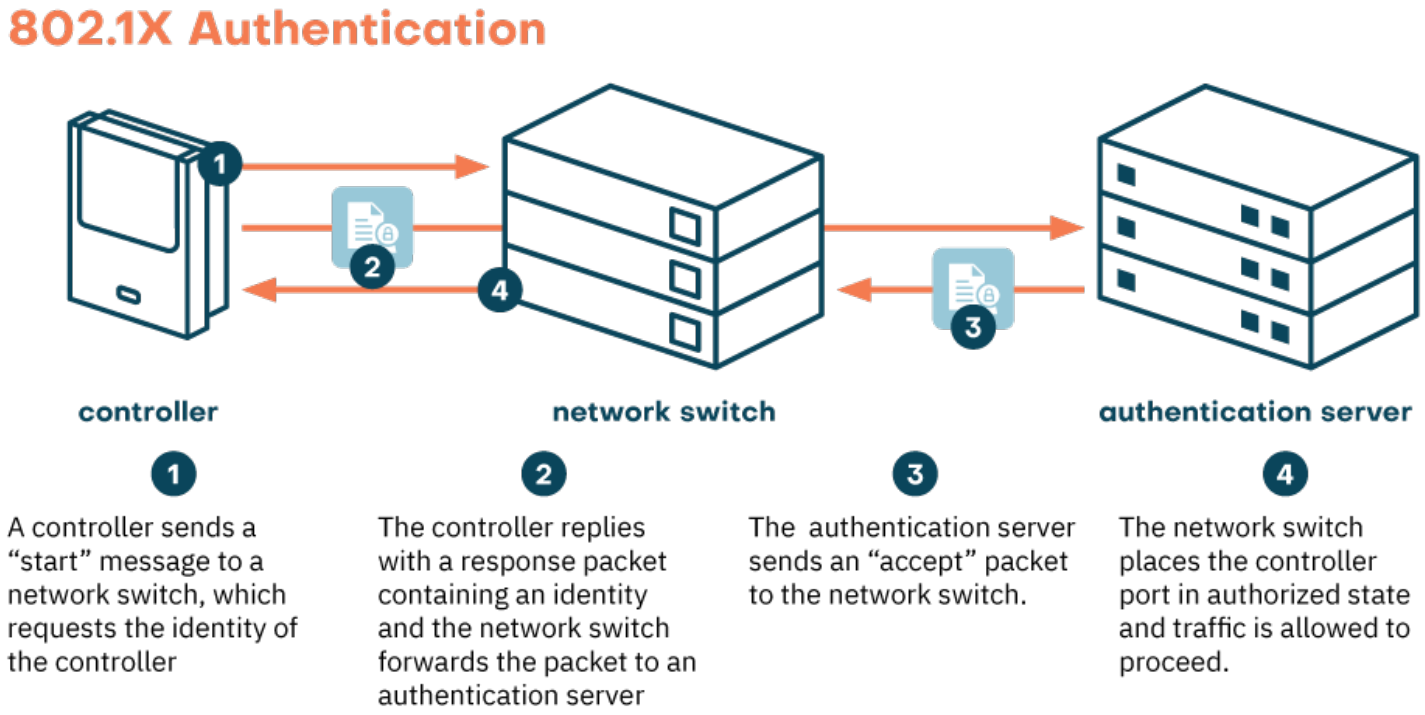
Authentication Protocols and Frameworks

EAP

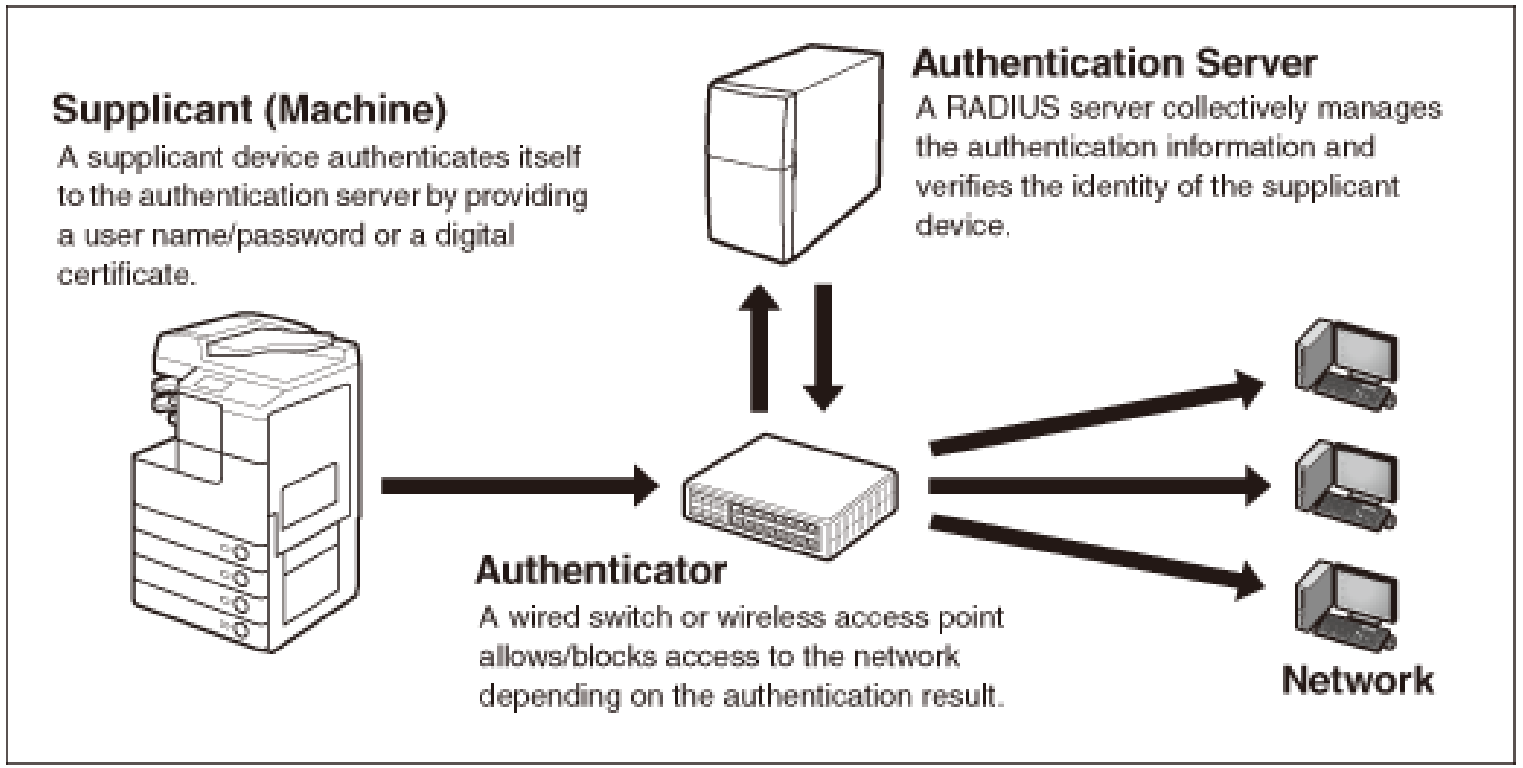
- Extensible Authentication Protocol (EAP) is an authentication framework, not a specific authentication mechanism, frequently used in wireless networks and point-to-point connections. It provides some common functions and negotiation of authentication methods called EAP methods.
- It supports various authentication methods, including as token cards, smart cards, certificates, one-time passwords and public key encryption.

802.1x

- 802.1X is a network authentication protocol that opens ports for network access when an organization authenticates a user's identity and authorizes them for access to the network. The user's identity is determined based on their credentials or certificate, which is confirmed by the RADIUS server.

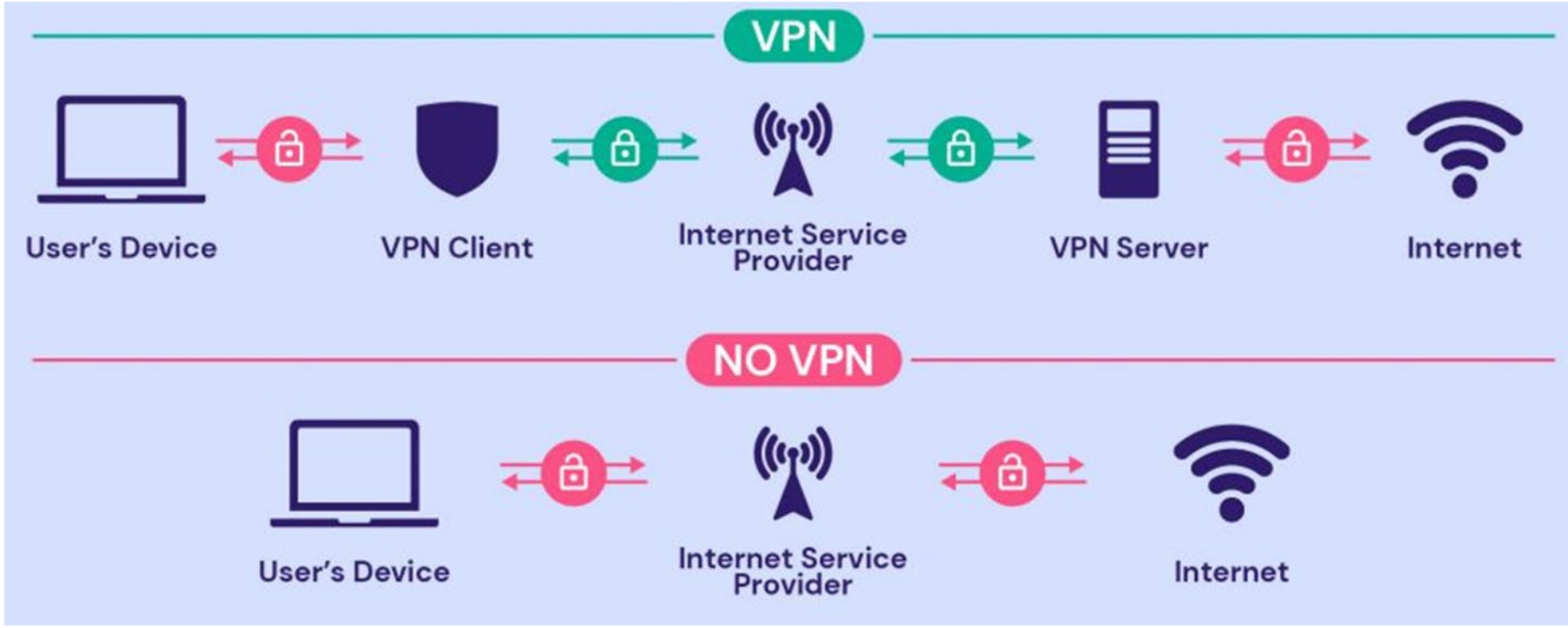


802.1x


Supplicant (Machine)
A supplicant device authenticates itself to the authentication server by providing a user name/password or a digital certificate.
Authentication Server
A RADIUS server collectively manages the authentication information and verifies the identity of the supplicant device.
Authenticator
A wired switch or wireless access point allows/blocks access to the network depending on the authentication result.
Network

VPN

- A virtual private network, or VPN, is an encrypted connection over the Internet from a device to a network. The encrypted connection helps ensure that sensitive data is safely transmitted. It prevents unauthorized people from eavesdropping on the traffic and allows the user to conduct work remotely. VPN technology is widely used in corporate environments.

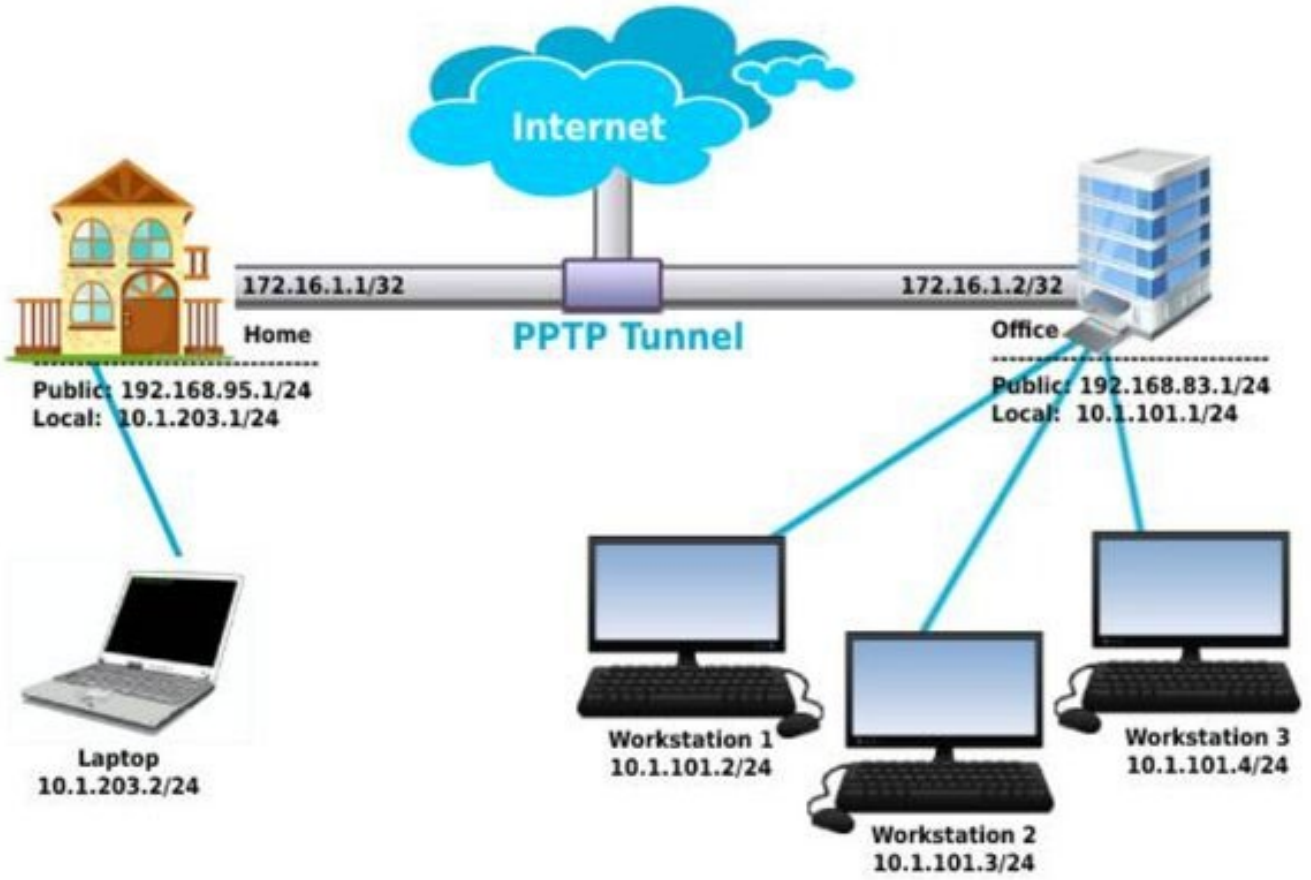


VPN


VPN
Secures your Data
YOU
THE INTERNET
GOVERNMENT
HACKERS
SNOOPERS

PPP

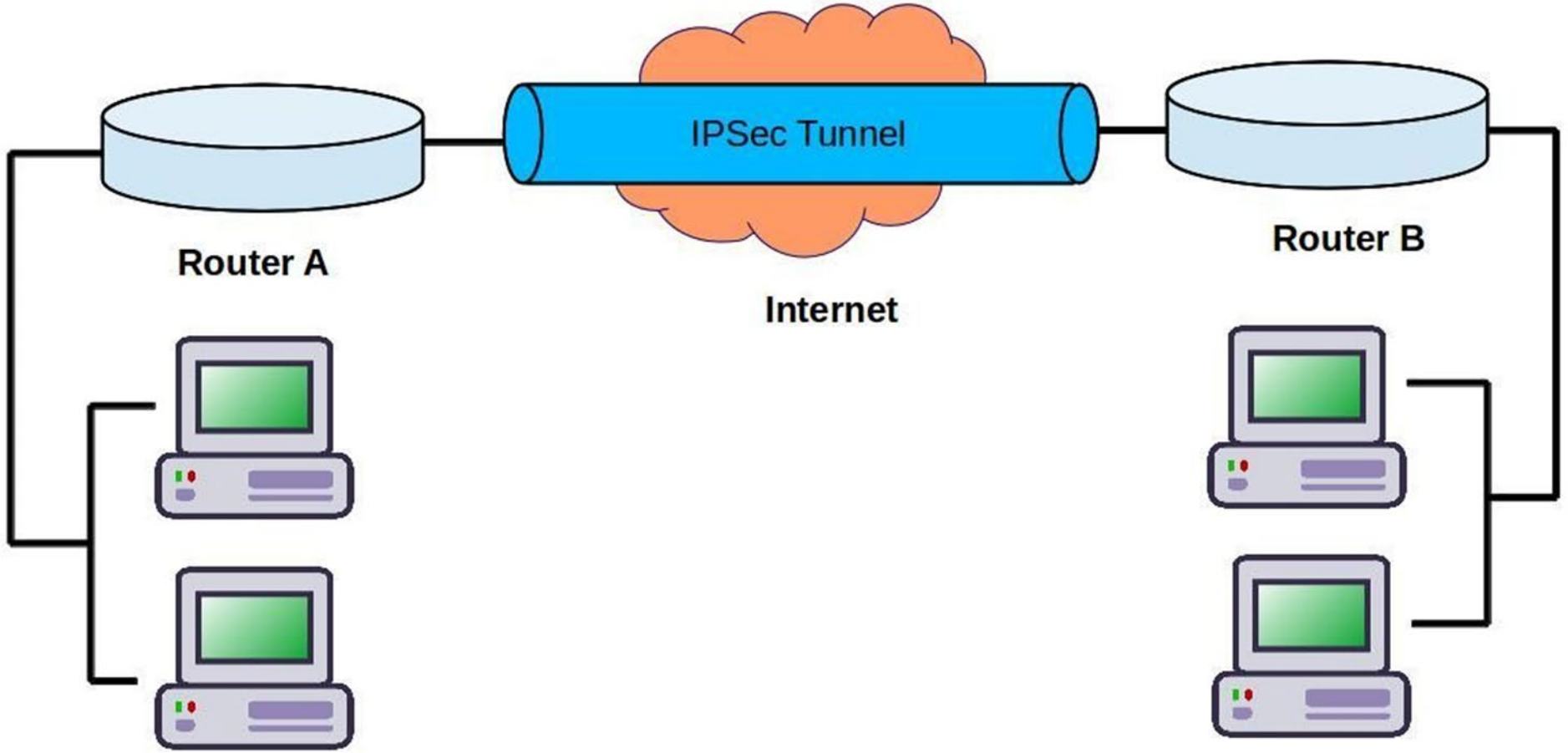
- Point-to-Point Protocol (PPP) is a TCP/IP protocol that is used to connect one computer system to another. Computers use PPP to communicate over the telephone network or the Internet. A PPP connection exists when two systems physically connect through a telephone line. You can use PPP to connect one system to another.



IPSec

- IPsec is a suite of protocols that are used to secure internet communications—in fact, the name itself is an abbreviation for Internet Protocol Security.
- IPsec was first codified in the '90s, spurred on by the dawning realization that internet traffic needed to be protected: the early internet mostly connected secured government and university buildings, and the internet protocol (IP) that defined how communications online worked sent information whizzing around unsecured and unencrypted.
- IPsec was designed to create a universal standard for internet security and enabled some of the first truly secure internet connections. IPsec isn't the most common internet security protocol you'll use today, but it still has a vital role to play in securing internet communications.

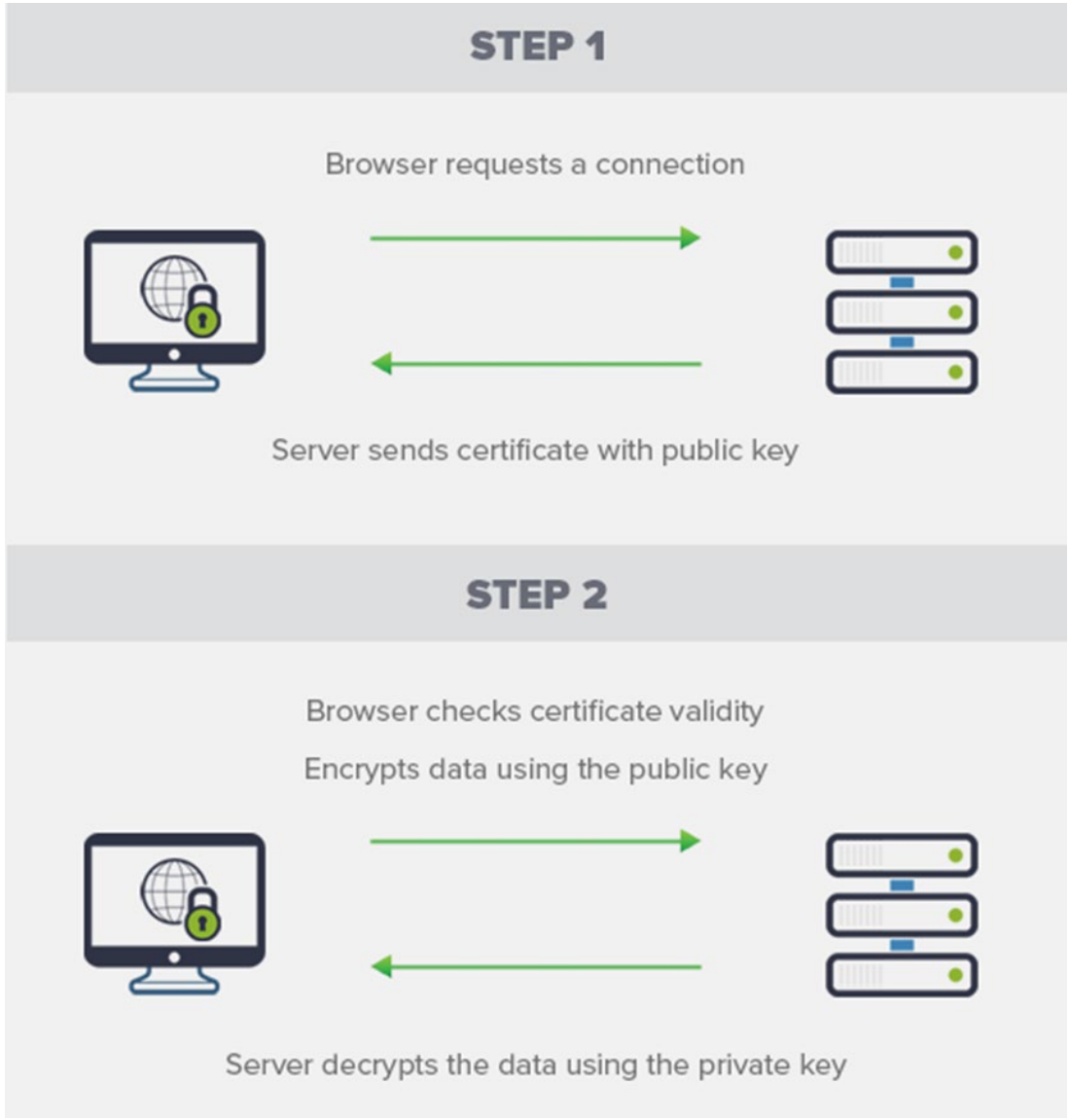
IPSec



SSL

- SSL stands for Secure Sockets Layer and, in short, it's the standard technology for keeping an internet connection secure and safeguarding any sensitive data that is being sent between two systems, preventing criminals from reading and modifying any information transferred, including potential personal details.

How SSL Works

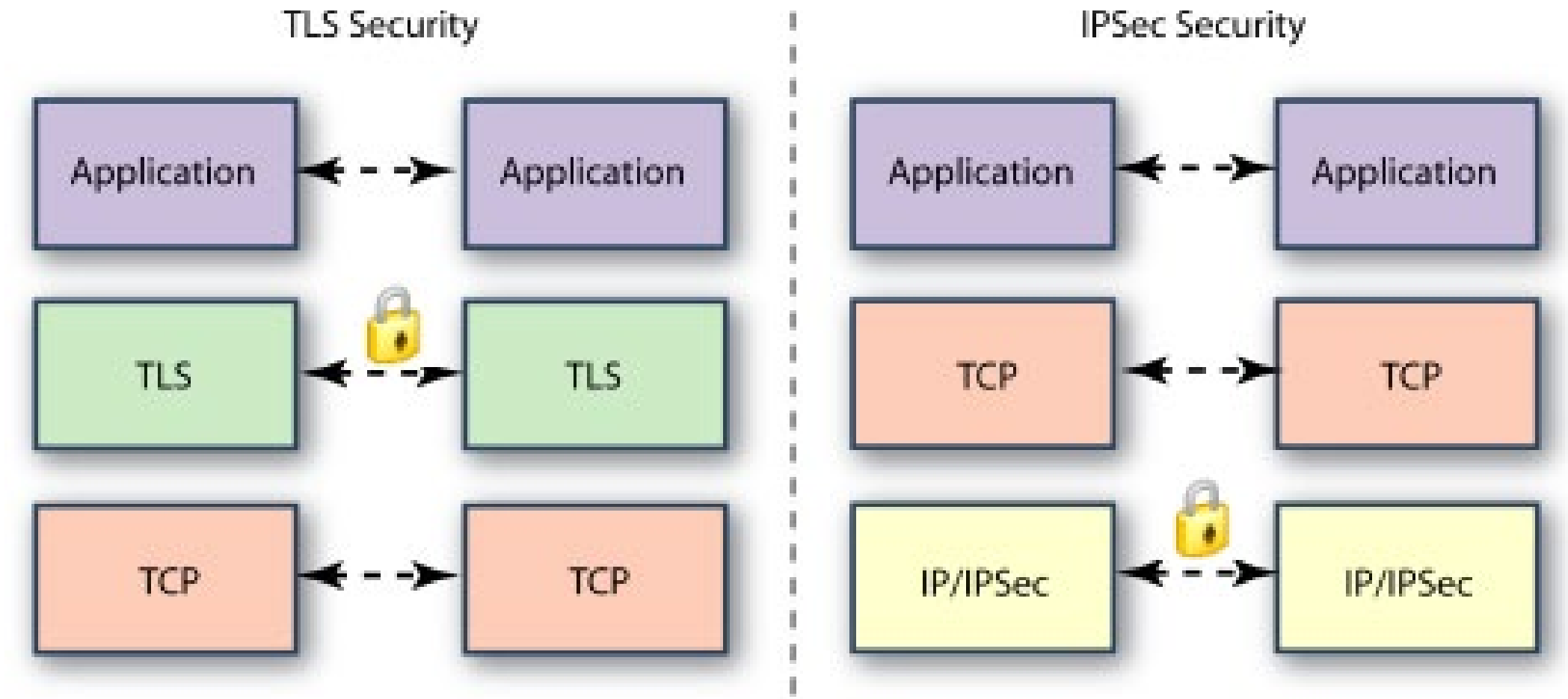


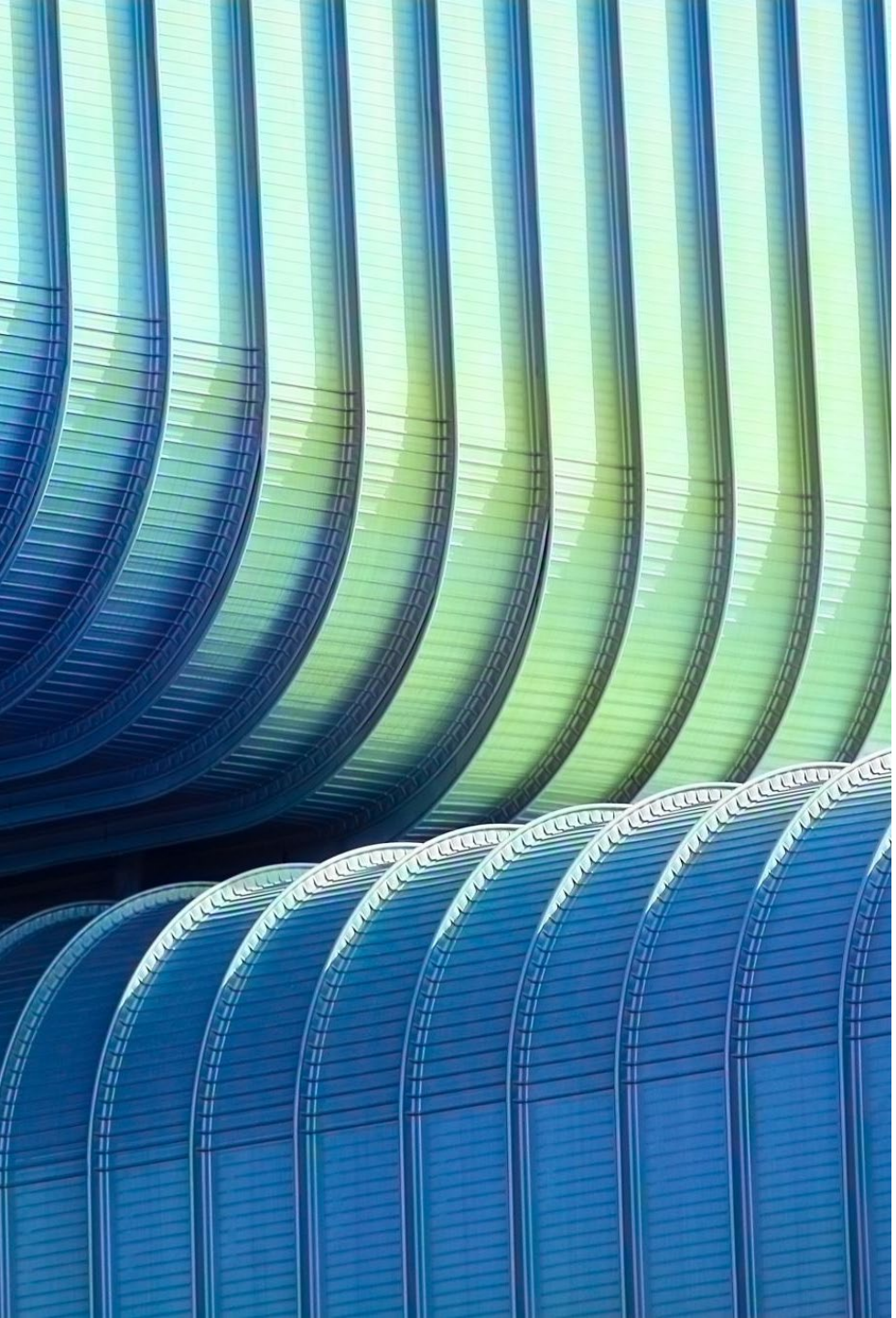
SSL and TLS

- Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as the SSL, using encryption to protect the transfer of data and information. The two terms are often used interchangeably in the industry although SSL is still widely used.

TLS	SSL
More secure in comparison to SSL.	Less secure in comparison to TLS.
TLS 1.0 and 1.1 are currently deprecated but TLS 1.2 and TLS 1.3 are actively used as of 2022.	All the SSL versions are deprecated now.
Provides more alert messages than SSL.	Less alert messages in comparison to TLS.
Provides support to the alert messages generated by SSL.	No support provided for the alert messages.
Uses HMAC for data integrity. TLS 1.3 uses AEAD for both encryption and authentication.	Uses MD5 and SHA1 based on a MAC.
Doesn't support the Fortezza cipher suite	Supports the Fortezza cipher suite.
Client sends an insecure Hello request and once secure connection is made communication switches to a port like 443 in case of HTTPS.	An explicit secure connection is made at a port. For example explicit HTTPS connection is made at port 443.

TLS vs IPSec

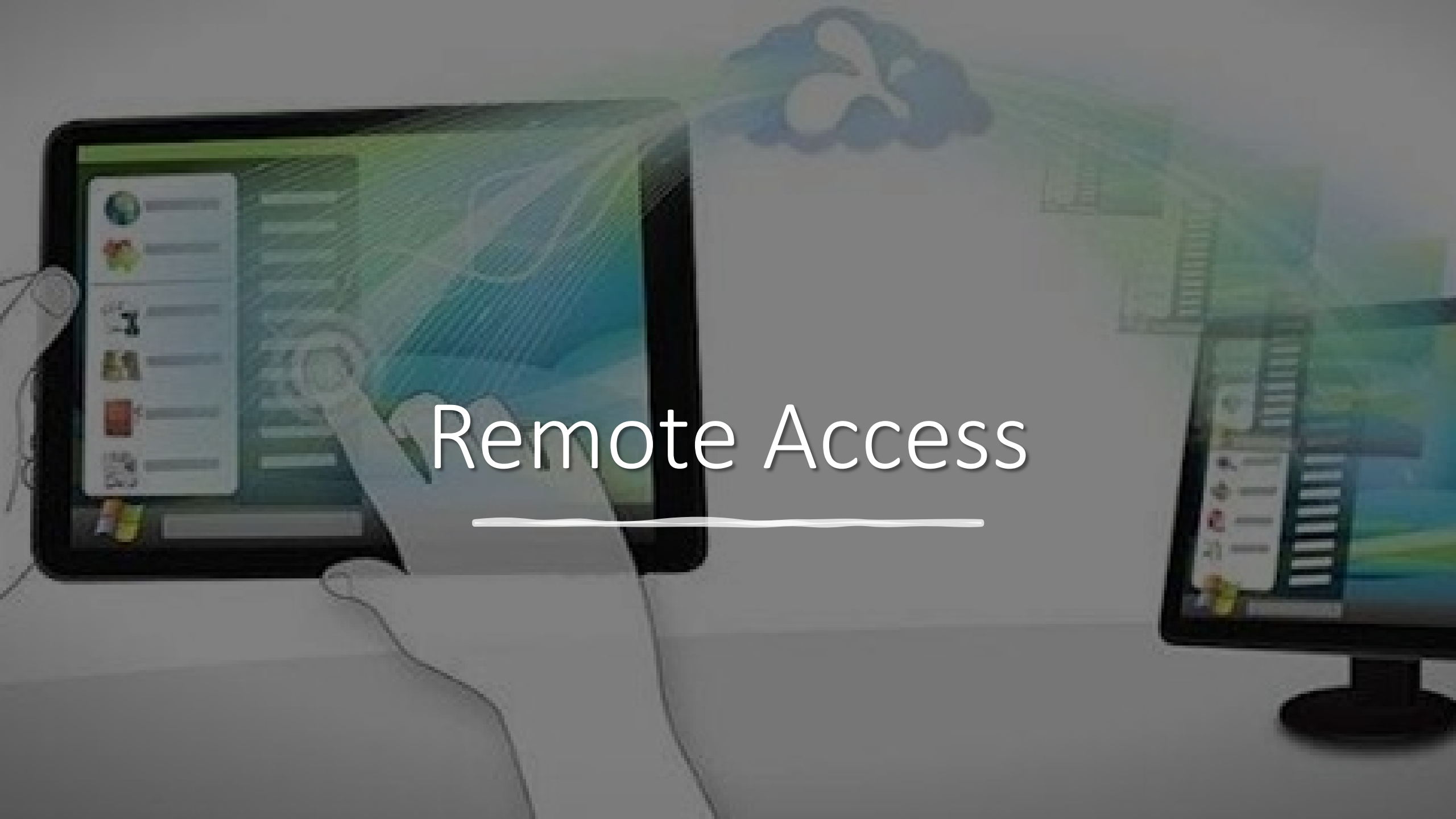

TLS Security
Application
Application
TLS
TLS
TCP
TCP
IPSec Security
Application
Application
TCP
TCP
IP/IPSec
IP/IPSec



HTTP? HTTPS? SSL?

HTTPS and SSL are similar things but not the same. HTTPS basically a standard Internet protocol that makes the online data to be encrypted and is a more advanced and secure version of the HTTP protocol. SSL is a part of the HTTPS protocol that performs the encryption of the data.

HTTPS is HTTP with encryption. The only difference between the two protocols is that HTTPS uses TLS (SSL) to encrypt normal HTTP requests and responses. As a result, HTTPS is far more secure than HTTP. A website that uses HTTP has http:// in its URL, while a website that uses HTTPS has https://.



Remote Access

xDSL

- A technology for high-speed network or Internet access over voice lines. There are various types but are generally called xDSL

xDSL Types

- HDSL (High-Bit-Rate DSL)
  - Standardized in 1994, HDSL uses two pairs of 24 AWG copper wires to provide symmetric E1/T1 data rates to distances up to 3657 meters. Its successors are HDSL2 and HDSL4, the latter using four pairs of wire instead of two.
- SDSL (Symmetric DSL)
  - SDSL succeeded HDSL as the two-wire (single-pair) type of symmetric DSL. SDSL is also known within ANSI as HDSL2.
  - Essentially offering the same capabilities as HDSL, SDSL offers T1 rates (1.544 Mbps) at ranges up to 10,000 feet and is primarily designed for business applications.

xDSL Types

- ADSL: Asymmetric DSL
  - ADSL provides transmission speeds ranging from downstream/upstream rates of 9 Mbps/640 kbps over a relatively short distance to 1.544 Mbps/16 kbps as far as 18,000 feet. The former speeds are more suited to a business, the latter more to the computing needs of a residential customer.
  - ADSL's substantial bandwidth accommodates large downstream transmissions, such as receiving data from a host computer or downloading multimedia files.
  - Its lopsided nature and various speed/distance options available within this range make ADSL attractive for use in high-speed internet access. Like most DSL services standardized by ANSI as T1.413, ADSL enables you to lease and pay for only the bandwidth you need.

xDSL Types

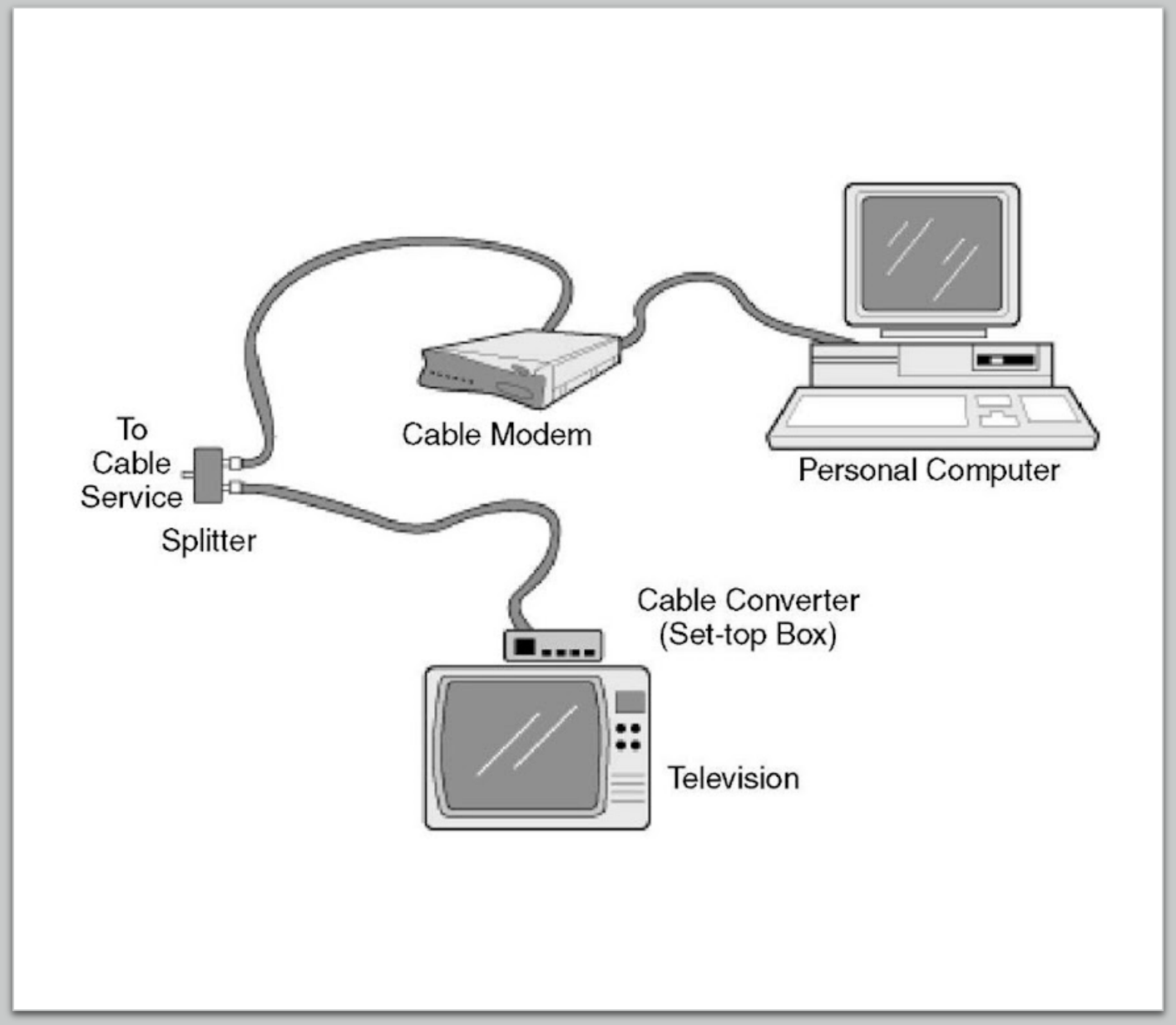
- SHDSL: Single-Pair, High-Speed Digital Subscriber Line
  - Also known as G.SHDSL, this type of DSL transmits data at much higher speeds than older types of DSL. It enables faster transmission and connections to the internet over regular copper telephone lines than traditional voice modems can provide. Support of symmetrical data rates makes SHDSL a popular choice for businesses using PBXs, private networks, web hosting and other services.
  - SHDSL can be used effectively in enterprise LAN applications. When interconnecting sites on a corporate campus, buildings and network devices are often beyond the reach of a standard Ethernet segment. Now you can use existing copper network infrastructure to connect remote LANs across longer distances and at higher speeds than previously thought possible.
  - Ratified as a standard in 2001, SHDSL combines ADSL and SDSL features for communications over two or four (multiplexed) copper wires. SHDSL provides symmetrical upstream and downstream transmission with rates ranging from 192 kbps to 2.3 Mbps. As a departure from older DSL services designed to provide higher downstream speeds, SHDSL specified higher upstream rates, too. Higher transmission rates of 384 kbps to 4.6 Mbps can be achieved using two to four copper pairs. The distance varies according to the loop rate and noise conditions.
  - For higher-bandwidth symmetric links, newer G.SHDSL devices for four-wire applications support 10-Mbps rates at distances up to 1.3 miles (2 km). Equipment for two-wire deployments can transmit up to 5.7 Mbps at the same distance.
  - SHDSL (G.SHDSL) is the first DSL standard to be developed from the ground up and to be approved by the International Telecommunication Union (ITU) as a standard for symmetrical digital subscriber lines. It incorporates features of other DSL technologies, such as ADSL and SDS, and is specified in the ITU recommendation G.991.2.

xDSL Types

- VDSL: Very-High-Bit-Rate DSL
  - Also approved in 2001, VDSL as a DSL service enables downstream/upstream rates up to 52 Mbps/16 Mbps. Extenders for local networks boast 100-Mbps/60-Mbps speeds when communicating at distances up to 500 feet (152.4 m) over a single voice-grade twisted pair. As a broadband solution, VDSL enables the simultaneous transmission of voice, data, and video, including HDTV, video on demand and high-quality video conferencing. Depending on the application, you can set VDSL to run symmetrically or asymmetrically.
- VDSL2: Very-High-Bit-Rate DSL 2
  - Standardized in 2006, VDSL2 provides higher bandwidth (up to 100 Mbps) and higher symmetrical speeds than VDSL, enabling its use for Triple Play services (data, video, voice) at longer distances. While VDSL2 supports upstream/downstream rates similar to VDSL, at longer distances, the speeds don't deteriorate as much as those transmitted with ordinary VDSL equipment.

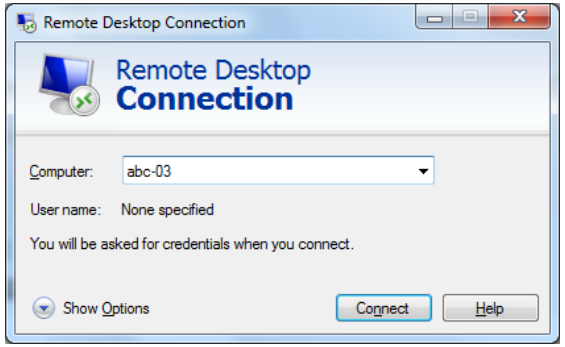
Cable Modems

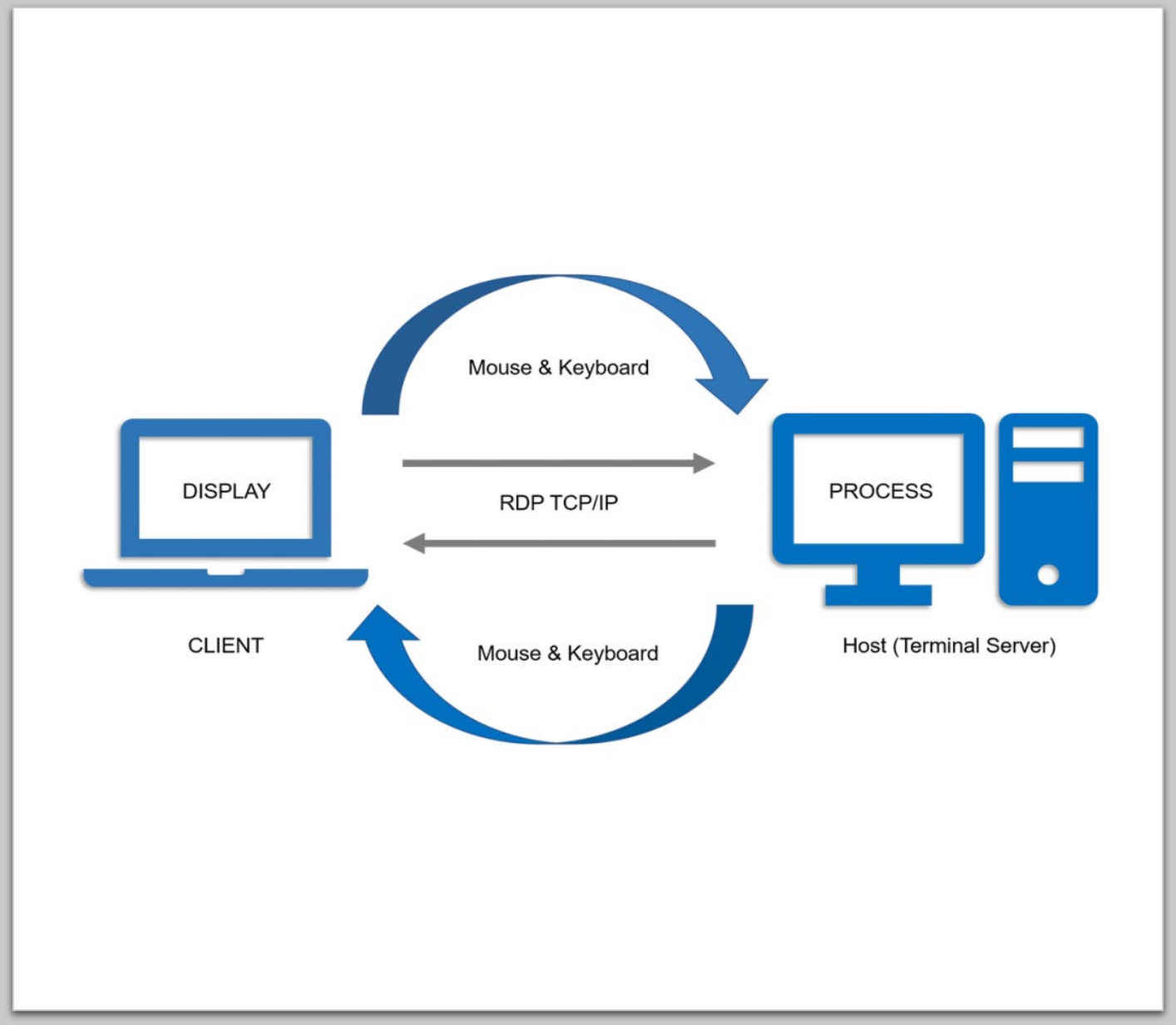
- a type of modem that connects a computer or local network to broadband internet service through the same cable that supplies cable television service. "a cable-modem connection"



Remote Desktop Console Access

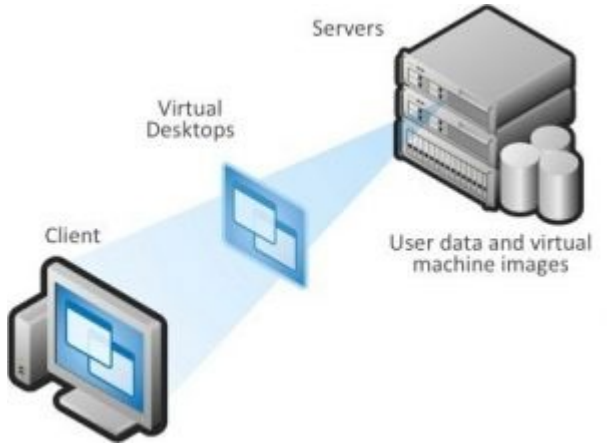
- A remote desktop is a program or an operating system feature that allows a user to connect to a computer in another location, see that computer's desktop and interact with it as if it were local.

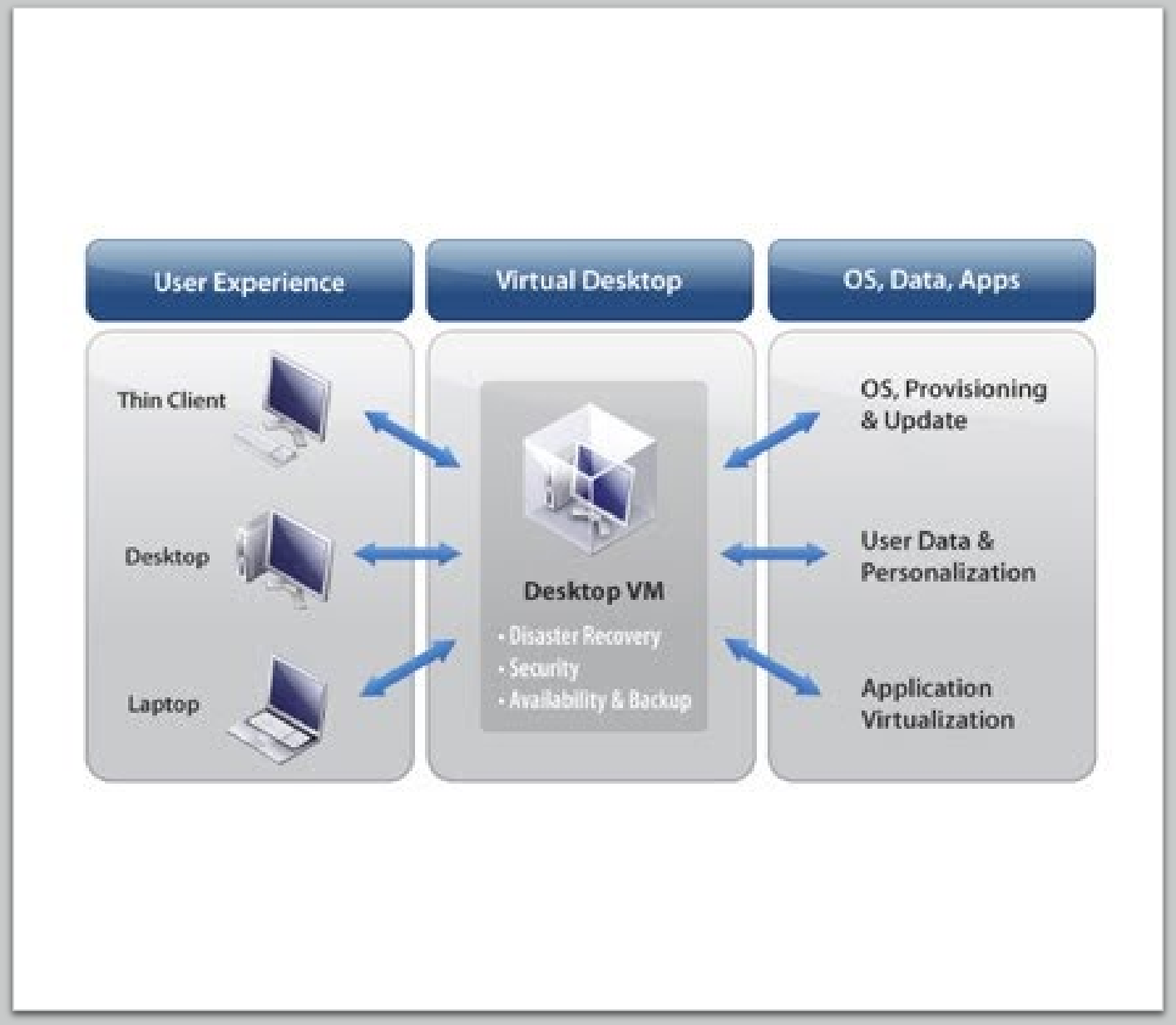




Desktop Virtualization

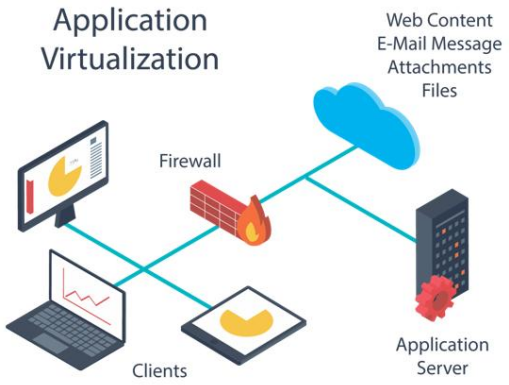
- Desktop virtualization is a technology that lets users simulate a workstation load to access a desktop from a connected device remotely or locally.

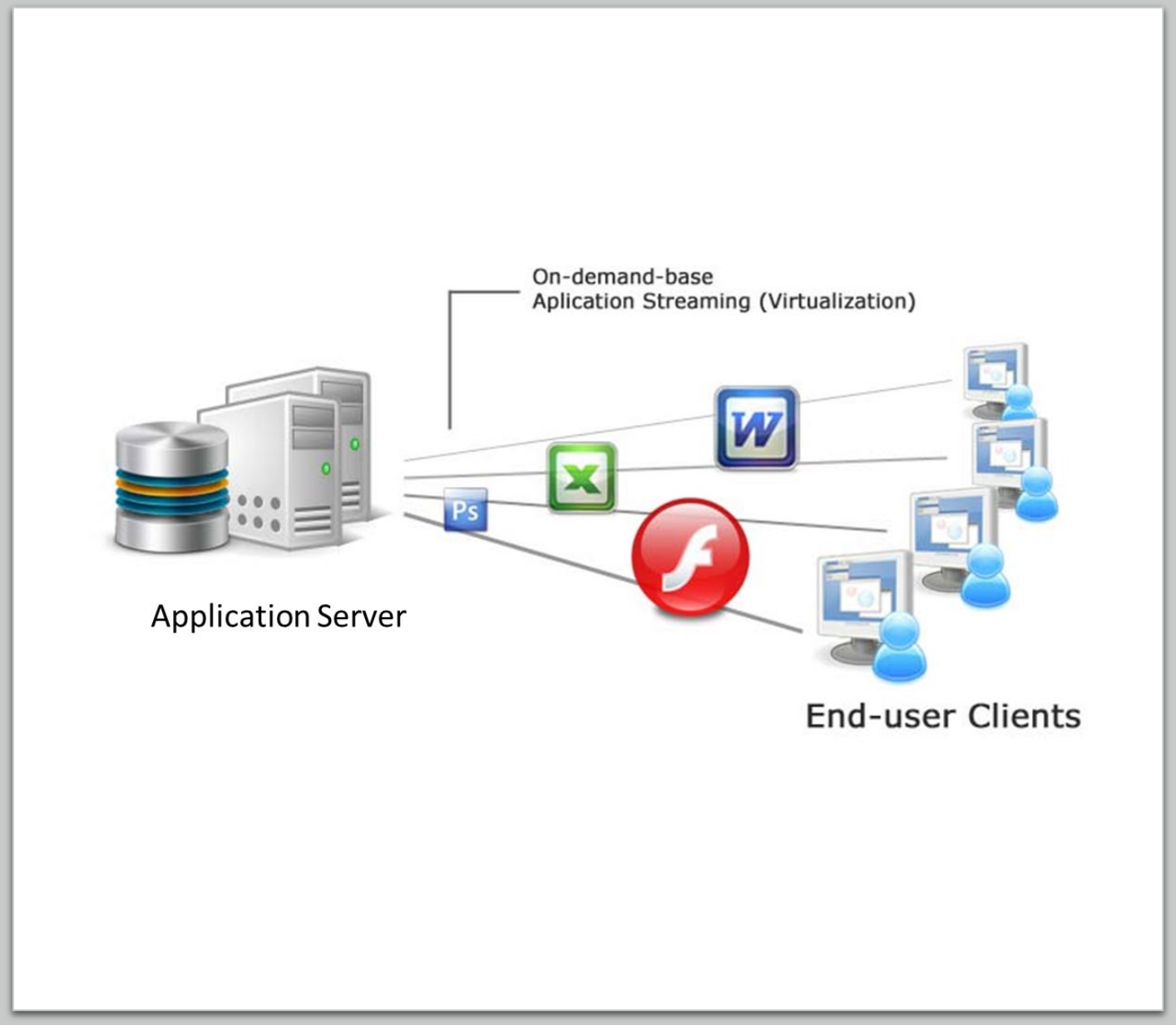




Application Virtualization

- Application virtualization is a process that deceives a standard app into believing that it interfaces directly with an operating system's capacities when, in fact, it does not. This ruse requires a virtualization layer inserted between the app and the OS.

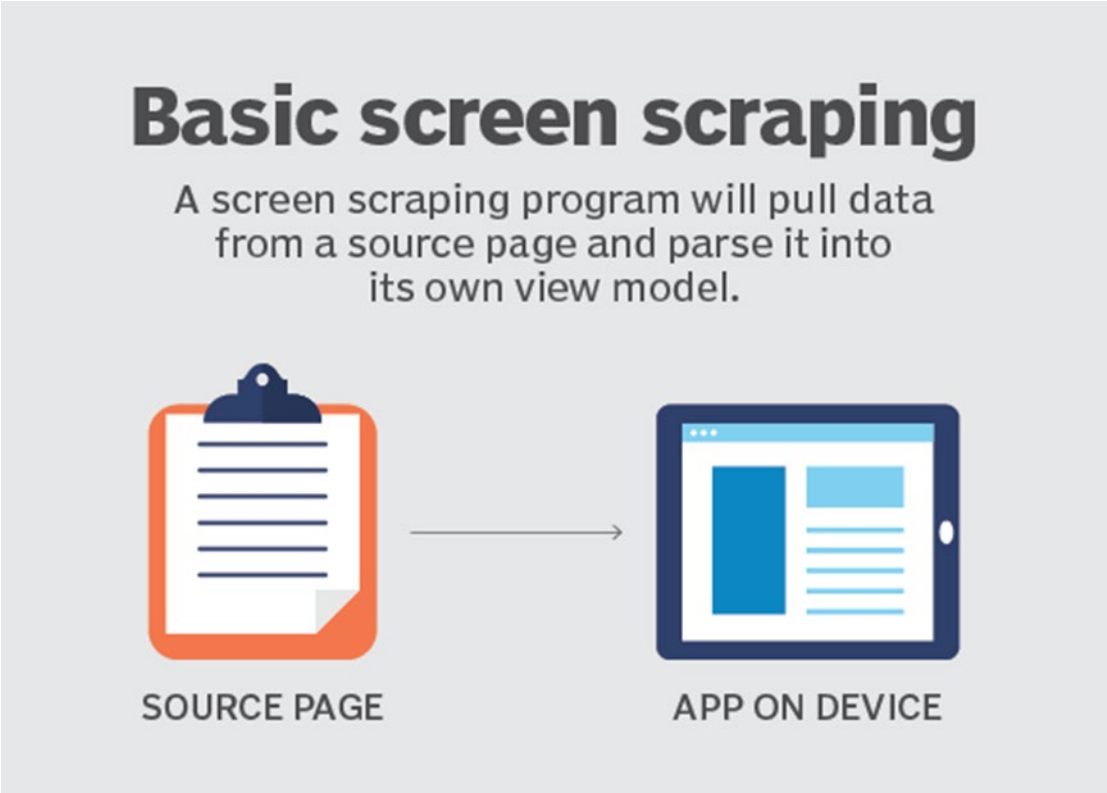


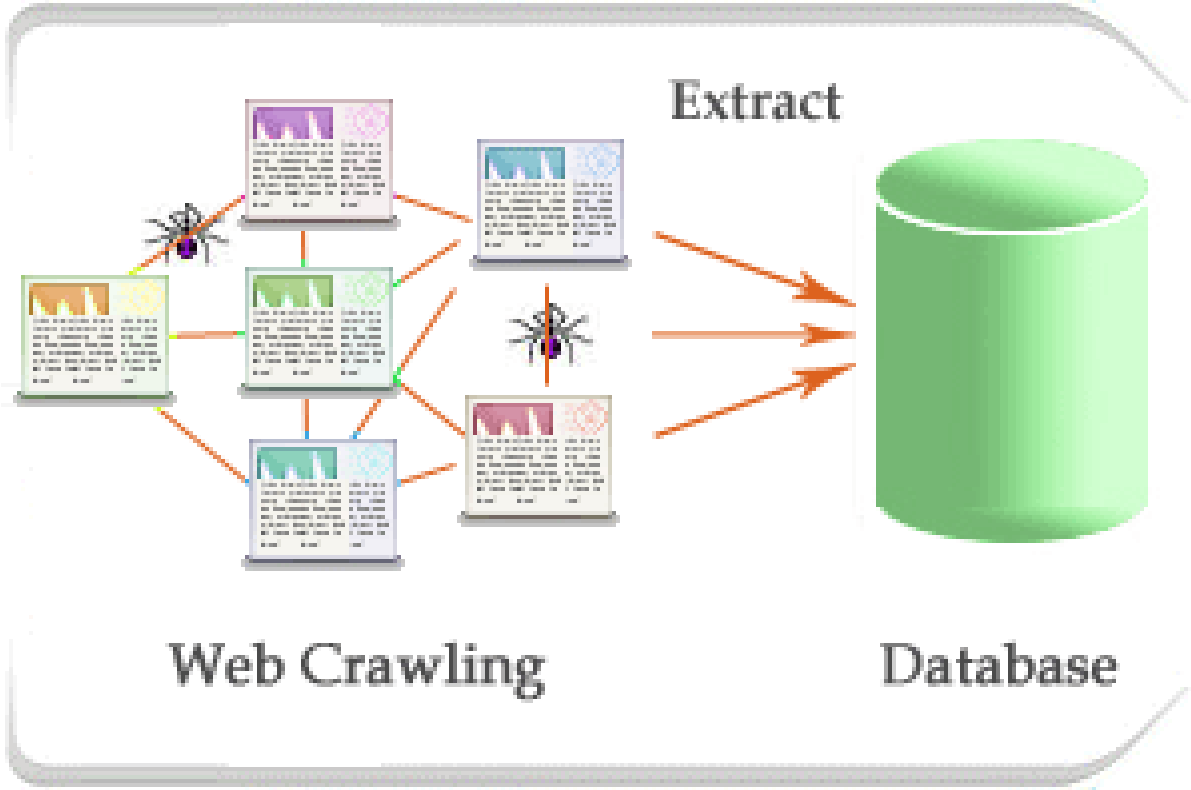


Screen Scraping

- Screen scraping is the act of copying information that shows on a digital display so it can be used for another purpose. Visual data can be collected as raw text from on-screen elements such as a text or images that appear on the desktop, in an application or on a website. Screen scraping can be performed automatically with a scraping program or manually with an individual extracting data.
- Screen scraping has a variety of uses, both ethical and unethical. Brief examples of both include either an app for banking, for gathering data from multiple accounts for a user, or for stealing data from applications. A developer might be tempted to steal code from another application to make the process of development faster and easier for themselves.

Screen Scraping





Instant Messaging

- Instant messaging, often shortened to IM or IM'ing, is the exchange of near-real-time messages through a standalone application or embedded software.

Remote Conferencing

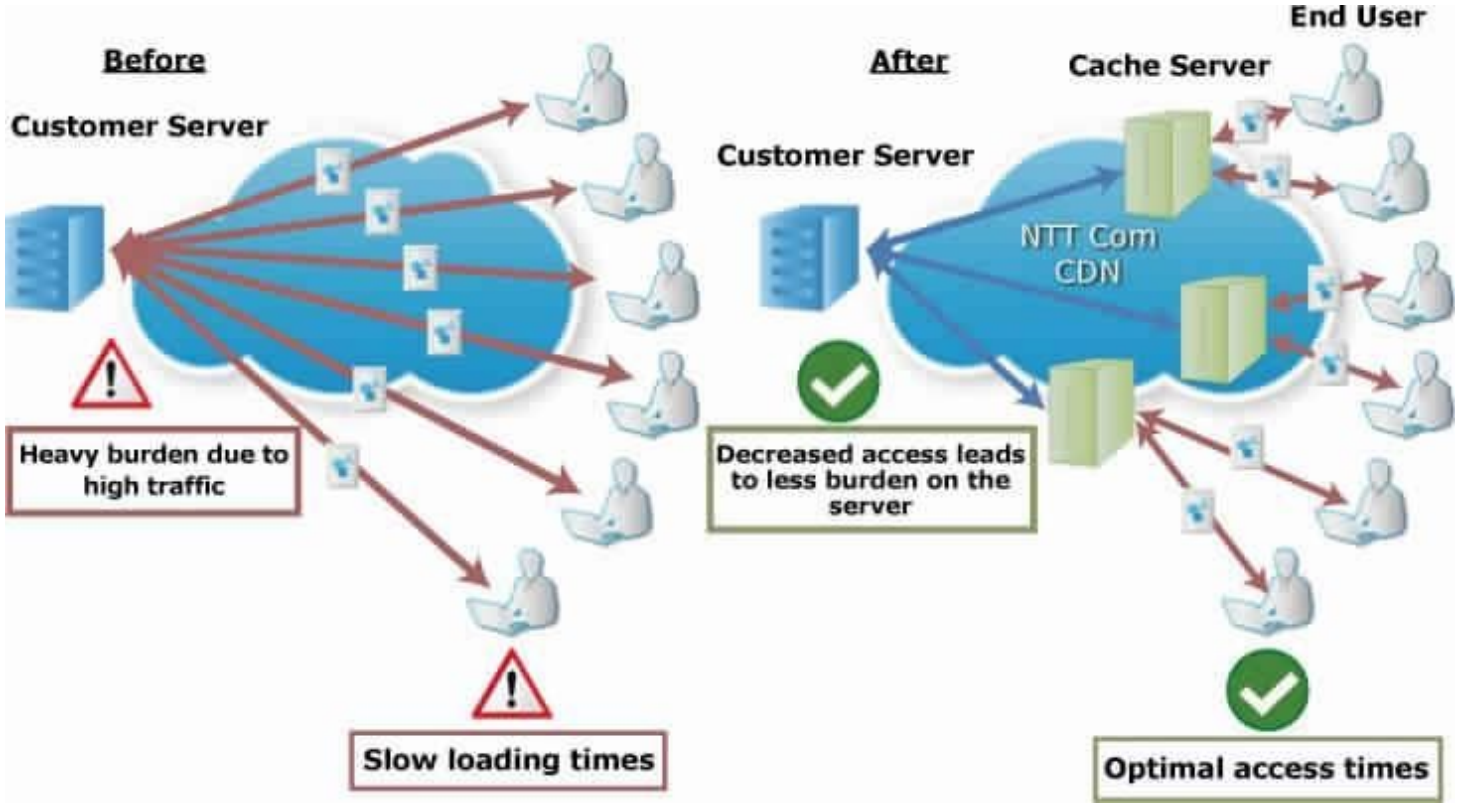
- A remote meeting, also known as a virtual meeting, occurs when a group of people, who are dispersed across different locations, use video and audio to connect online. This type of meeting is used by organizations with remote or hybrid teams.

PDA

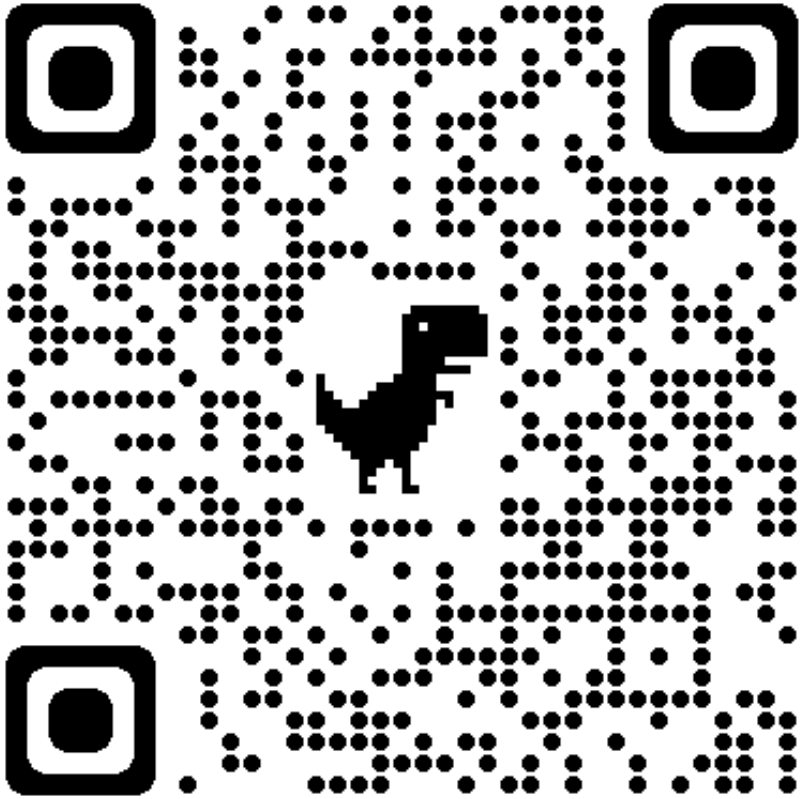
- Short for Personal Digital Assistant, PDA is a computer that fits in the palm of your hand to help collect such information as contacts, appointments, files, and programs

Content Distribution Network (CDN)

- A content delivery network (CDN) refers to a geographically distributed group of servers that work together to provide fast delivery of Internet content.



PH CERT
Philippine Computer Emergency Response Team Coordinating Center



ALBERT P. DELA CRUZ <albertdc@phcert.cc>

https://phcert.cc

twitter.com/phcert

fb.me/phcert