Keysight Technologies

LOJAIN IDRIS

GLORY IMO

JOSHUA QUICK

Introduction

Keysight Technologies Inc focuses in electronic design and test solutions; it has its headquarters in Santa Rosa, California. It offers design, testing and validation tools and software for engineers and scientists in electronics and electrical products and systems. Their products are essential in maintaining the functionality and efficiency of various gadgets in use today starting with gadgets used in homes to highly developed communication systems.

Keysight was established in 1939 as an HP division, and has a long history in electronic measurement. It was only in 2014 that it became an independent company with its business model revolving around electronic measurement solutions. Today, Keysight operates in telecommunication, aerospace and defense, automotive, energy, and semiconductor manufacturing industries. They offer products and services that are crucial to firms that seek to introduce new electronic products and services to the market within short time and with great quality.

Keysight is present in the Americas, Europe and the Asia-Pacific region, through its offices and facilities. It also makes them capable of serving many customers and engaging in close cooperation with the clients all over the world. For more than a decade, they have been dedicated to the delivery of value, innovation, and quality to become a strategic partner in the electronics industry.

Keysight locations

Keysight technologies is headquartered in Santa Rose 1400 Fountaingrove Parkway, United States, and has 41 office locations.

- Calabasas 26601 Agoura Rd, United States
- Colorado Springs 1900 Garden of the Gods Rd, United States
- Mulgrave 745 Springvale Rd, Australia
- Vienna, Austria
- Rotselaar, Belgium

Security Components

Network Security ISO model:

- Physical Layer: securing data centers and server rooms, physical defenses such as locks, security guards, and biometric authentication.
- Data Link Access Layer: Mac addresses filtering, using VLAN for network segmentation.
- Network Layer: Firewalls, securing IP communication, Access control lists.
- Transport Layer: packet filtering to prevent unauthorized access.
- Session Layer: session management tools, securing VPNs, using
- Presentation Layer: Data encryption.
- Application Layer: Web application firewalls, antivirus software.

Network security TCP/IP model

- Network Access Layer: physical security, MAC filtering, Port Security.
- Internet Layer: Network Segmentation by using subnets and VLANs, ACLs managing and controls traffic and unauthorized access.
- Transport Layer: Firewall, Data Encryption, TCP/IP security.
- Application Layer: Web application firewalls, protocols security.

NIST Framework

Keysight is a large company that needs flexible and strong security measures to avoid security threats, therefore NIST security framework is the ideal security framework choice for our company due to our extensive range technology products and wide range of industries that need protection. NIST security framework provides the best practice that can be tailored to different industries and organizations sizes which apply to our company. Furthermore, NIST security framework covers all areas of cybersecurity which gives us a way to approach our security posture. NIST security framework is the best approach to regulatory standards and risk management.

NIST framework core function:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

Network Types & Their Importance

Wide Area Network (WAN)

Definition: Used to join offices/data centers in different cities or countries over large distances hence called long distance communication.

Importance: Crucial for communication between different centres such as R&D or production, as well as other administrative offices all over the world. Allows more secure real time sharing of files and docs and is convenient to manage through a single interface .

Local Area Network (LAN)

Definition: Connects devices in one building or a campus.

Importance: Enables fast connections of internal devices in the organization such as computers and lab devices for the proper functioning of the organization in every station.

Personal Area Network (PAN)

Definition: Used to link personal devices in a small space.

Importance: Provides mobility in lab or office environments where employees' own devices can be used to connect to the secure Wi-Fi.

Small Office Home Office or SOHO

Definition: Network for offices with lesser number of employees or for home-based offices.

Importance: Offers secure remote access connection for employees and contractors to connect to company resources from any location.

Optimized Network Design & IP Address Scheme

Network Structure for Keysight Technology Company

WAN: Puts together international locations such as offices and laboratories.

LAN: It supports high-speed connection within offices.

PAN: Supports the connection of the device in some extent.

SOHO: Remote access and assurance of security to the workers.

IP Address Scheme

Class A Private Range: 10.0.0.0/8 – big address space for large scale internetworking.

Subnetting:

HQ: 10.0.0.0/16 (65,536 IPs for the operations of the central network).

R&D Centers: 10./18 (16000 IPs per center)

Manufacturing: 10.2.0.0/20 which really means 4096 IPs per facility

Regional Offices: 10.3.0.0/22 (1,024 IPs per office)

SOHO: 10.10.0.0/24 (256 IPs per site)

Ensuring Security with Network Segmentation & VLANs

Subnet Security with VLANs

Segmentation Example:

VLAN 10: Human Resources

VLAN 20: Finance

VLAN 30: Research & Development

Purpose: Reduces the options for penetration and limits the consequences of the violation by means of the isolation of relevant departments.

Routing and Traffic Control

Layer 3 Switches/Routers: Local connectivity of subnets, which enables effective and secure exchange of information between different locations, such as research and development and production facilities.

Firewalls and Intrusion Detection Systems (IDS):

Located strategically in the network for the purpose of surveillance and regulation of data in the organization.

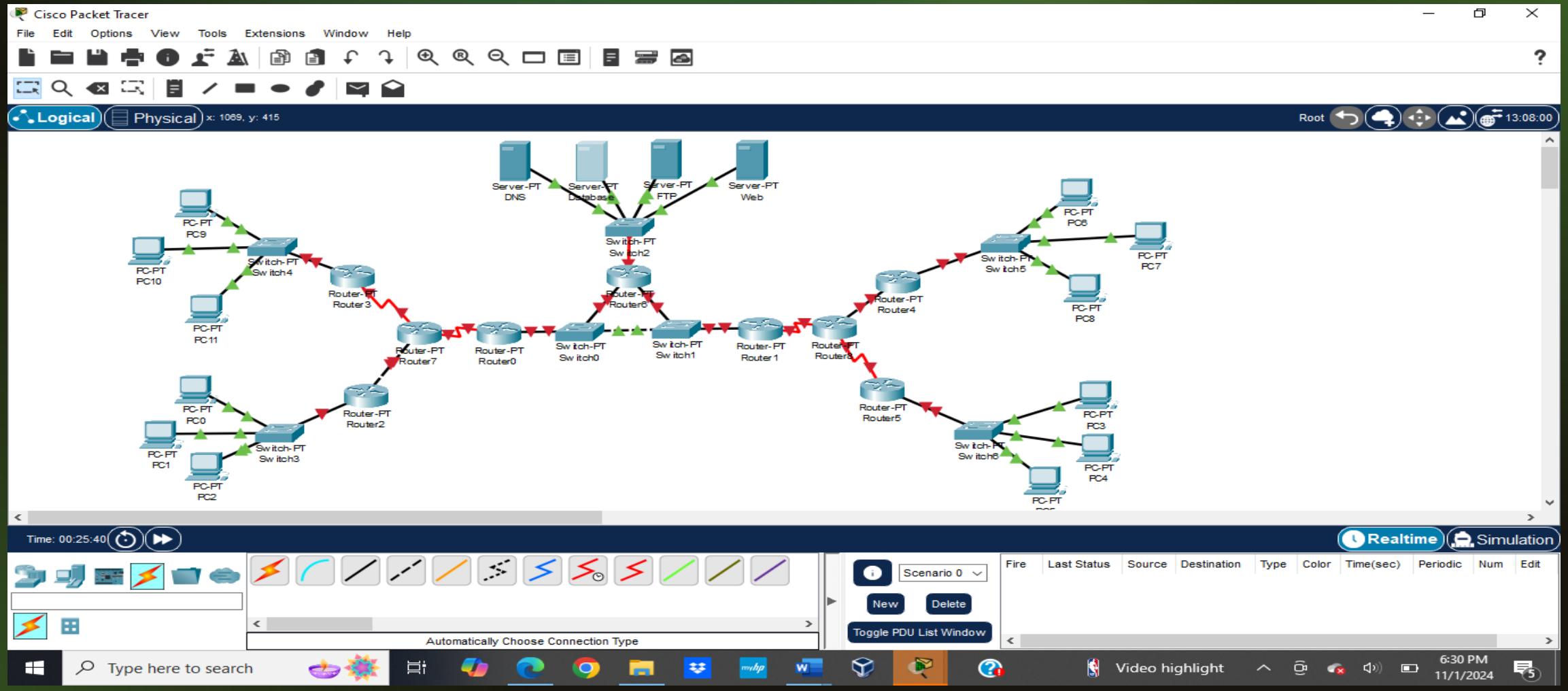
Safeguards against intrusions and gives added security measure to the computer system.

Conclusion:

Keysight's network uses WAN for long distance connection, LAN for connection with other devices in same area, SOHO for home office connection and PAN for convenient device connection.

An appropriate Class A IP address range together with effective subnetting helps to achieve scalability; VLAN and security measures help to protect data, which complies with Keysight's vision of secure and reliable work.

Logical Topology: Star



Logical Topology: Star

- **Redundancy and Reliability**
  - **Two Core Routers**: Having two core routers ensures that if one router fails, the other can take over, minimizing downtime and maintaining network availability.
  - **Two Core Switches**: Similar to the routers, two core switches provide redundancy, allowing traffic to be rerouted if one switch encounters an issue. This enhances the reliability of internal communications.
- **Load Balancing**
  - **Core Routers and Switches**: With multiple core devices, traffic can be balanced between them. This prevents any single device from becoming a bottleneck, improving overall network performance.
  - **Edge Routers**: Two edge routers can distribute incoming and outgoing internet traffic, optimizing bandwidth usage and enhancing response times for users.

Logical Topology: Star

- **Increased Capacity**
  - **Scalability**: Having additional core and edge devices allows for higher capacity and scalability as the organization grows. More connections and devices can be supported without significant reconfiguration.
  - **Segmented Traffic**: The arrangement allows different types of traffic (e.g., internal vs. external) to be handled efficiently, improving performance for critical applications.
- **Improved Security**
  - **Layered Security**: The architecture allows for multiple security measures to be implemented at various points (e.g., edge routers for external traffic, core routers for internal traffic), enhancing overall security.
  - **Isolation of Services**: The use of separate edge routers for handling public-facing services allows for better control and monitoring of external threats, providing an additional layer of security.

Logical Topology: Star

- **Enhanced Performance**
  - **Local Traffic Management**: The presence of switches at each location helps in managing local traffic efficiently, reducing congestion on the core network.
  - **Faster Response Times**: With dedicated routers and switches, devices can communicate more quickly, leading to better performance for applications used at each location.
- **Failover Capabilities**
  - **Automatic Failover**: In the event of hardware failure, having multiple routers and switches allows for automatic failover, ensuring continuous service availability.
  - **Redundant Paths**: Multiple paths for data to travel through the network enhance resilience, preventing single points of failure.

Logical Topology: Star Security

- First, we have the **perimeter firewall**, which is positioned between the ISP and our edge routers. This firewall serves as the first line of defense against external threats, filtering incoming and outgoing traffic based on predefined security policies. Its primary role is to prevent unauthorized access to our internal network.
- Next, we have the **Intrusion Detection and Prevention Systems (IDS/IPS)**, located between the edge routers and the core routers. The IDS monitors traffic for suspicious activities and provides alerts, while the IPS actively blocks or mitigates identified threats. This placement is crucial as it protects our internal network from both external and internal threats.

Logical Topology: Star Security

- The **Demilitarized Zone (DMZ)** is positioned between the edge routers and core routers. This area hosts our publicly accessible servers, such as web servers, while isolating them from our internal network. The DMZ enhances security by protecting sensitive internal resources from direct exposure to the internet.
- In the data center, we have our **Security Information and Event Management (SIEM)** system. This component aggregates and analyzes logs from various network devices, enabling us to monitor for suspicious activities and security incidents in real time. It plays a vital role in our centralized incident response and compliance efforts.

Logical Topology: Star Security

- **Encryption** is implemented both in transit and at rest. For in-transit encryption, we ensure that all communications between servers, particularly those involving sensitive data, are encrypted. At rest, we apply encryption to sensitive data stored on our file and database servers. This dual-layer approach protects data from unauthorized access during transmission and ensures its confidentiality when stored.
- Next, we have **antivirus and endpoint security**, which are installed on all endpoints across the network, including workstations and servers. This layer of security protects against malware, viruses, and other threats, ensuring that all devices connected to our network are secure.

Logical Topology: Star Security

- **Virtual Local Area Networks (VLANs)** are configured on our core switches to segment network traffic based on departments or functions. This segmentation enhances security by isolating sensitive data and resources while also improving overall network performance by reducing broadcast traffic.
- Finally, **access control** measures are implemented on routers, switches, and servers throughout the network. We utilize Role-Based Access Control (RBAC) to restrict access to resources based on user roles and enforce Multi-Factor Authentication (MFA) for critical systems. This ensures that only authorized users can access sensitive information.

References

- https://craft.co/keysight-technologies/locations
- Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J., & Wolber, D. (1989). A network security monitor (No. UCRL-CR-105095). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States); California Univ., Davis, CA (USA). Dept. of Electrical Engineering and Computer Science.
- https://www.bitsight.com/blog/7-cybersecurity-frameworks-to-reduce-cyber-risk.
- https://www.keysight.com/us/en/home.html
- https://www.keysight.com/us/en/cmp/2022/private-network-solutions.html
- https://www.keysight.com/us/en/solutions/data-center-infrastructure.html
- https://www.keysight.com/us/en/products/network-test/network-modeling.html