



# Fundamentos – Componentes de los Sistemas de TI

Ciberseguridad  
FPUNA



# Mapeo de las Redes de Computadoras



# Dispositivos

El mapeo identifica y categoriza todos los dispositivos conectados a la red, como:

- servidores,
- routers,
- switches,
- impresoras,
- puntos de acceso inalámbricos y
- workstations.



# Conectividad

- Se visualiza cómo se interconectan estos dispositivos, mostrando las rutas físicas y virtuales entre ellos. Esto incluye la topología de la red (cableado, switches, etc.) y la configuración de las subredes.

# Flujo de Información

- El mapeo puede mostrar el flujo de datos y tráfico en la red, incluyendo las rutas preferidas, la carga de tráfico y los puntos de congestión.

# Servicios

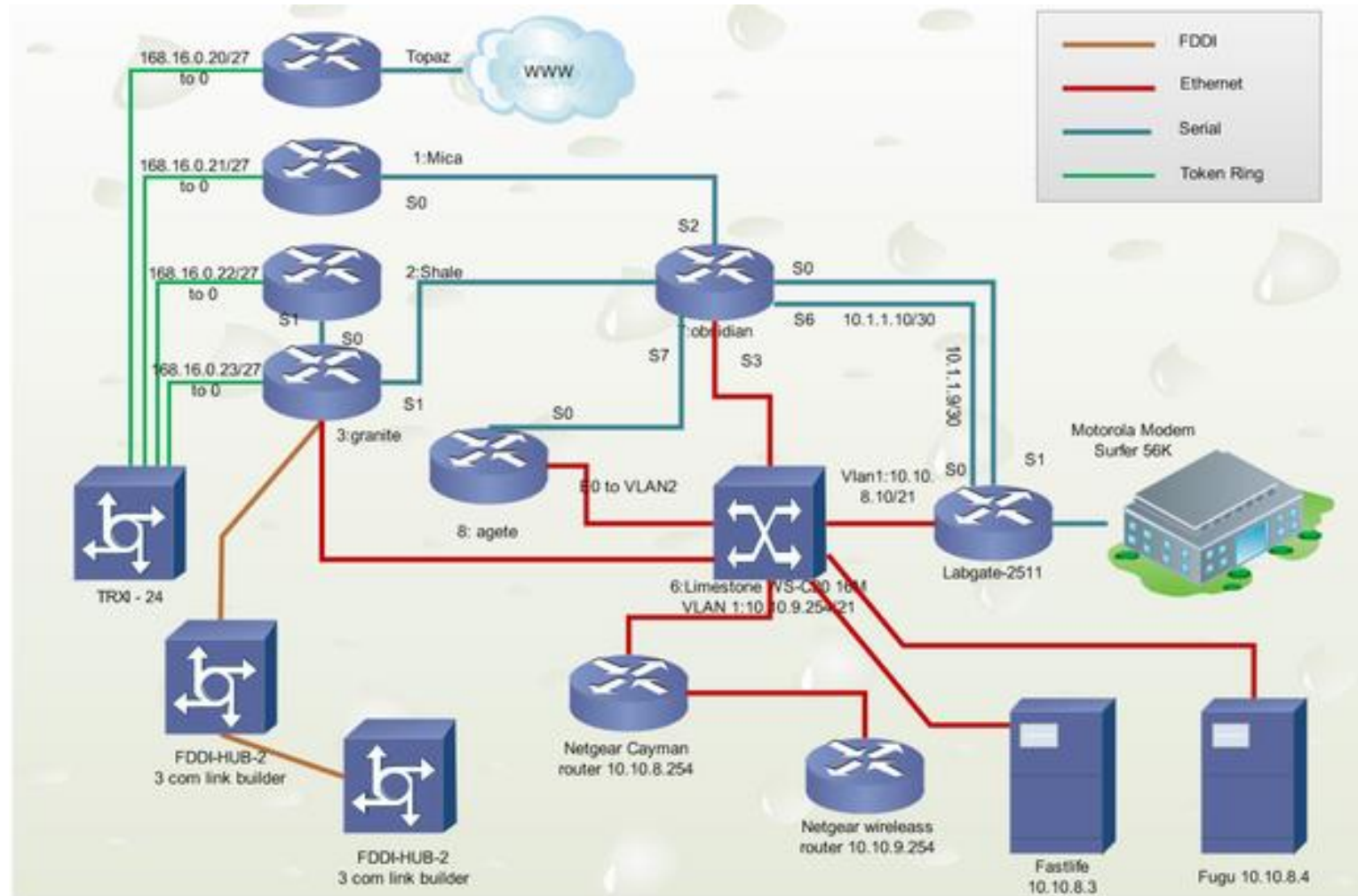
- Se pueden identificar y mapear los servicios de red disponibles, como DHCP, DNS, VPN, firewalls y servidores web.

## Tipos de Mapeo de Redes

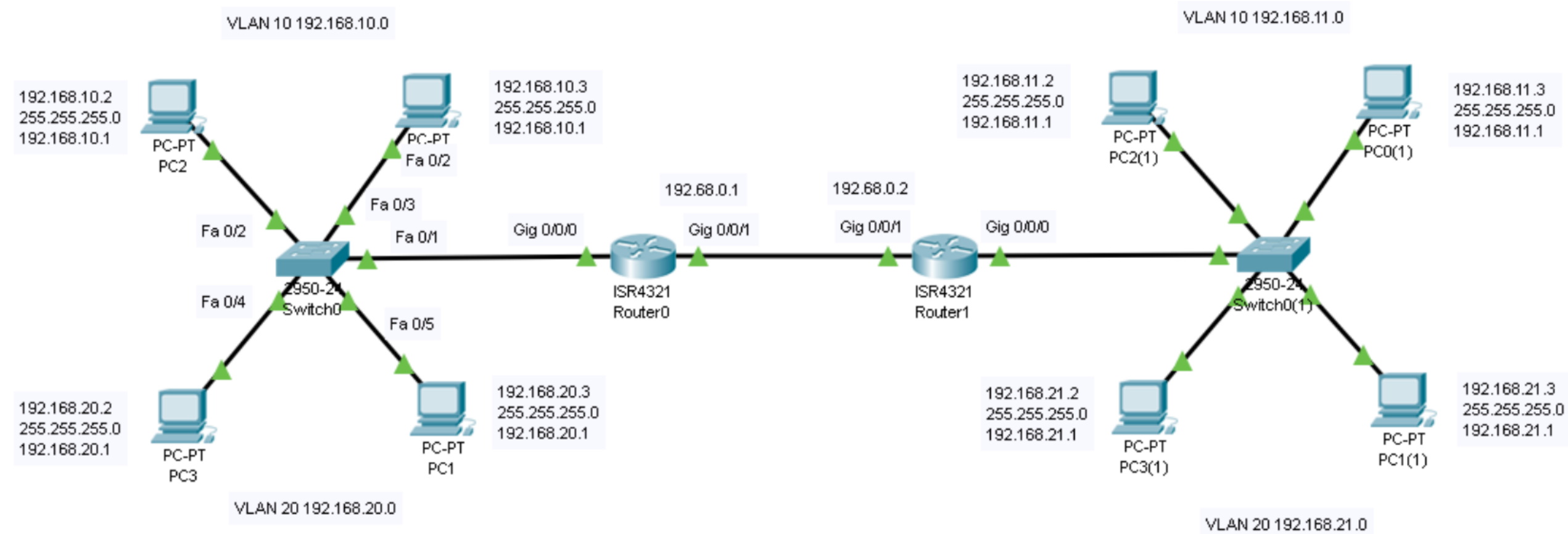
- **Mapeo físico:** Representa la ubicación física de los dispositivos y el cableado.
- **Mapeo lógico:** Muestra la organización lógica de la red, como subredes, dominios y VLANs.
- **Mapeo de aplicaciones:** Se enfoca en el flujo de datos y las relaciones entre las aplicaciones que se ejecutan en la red.



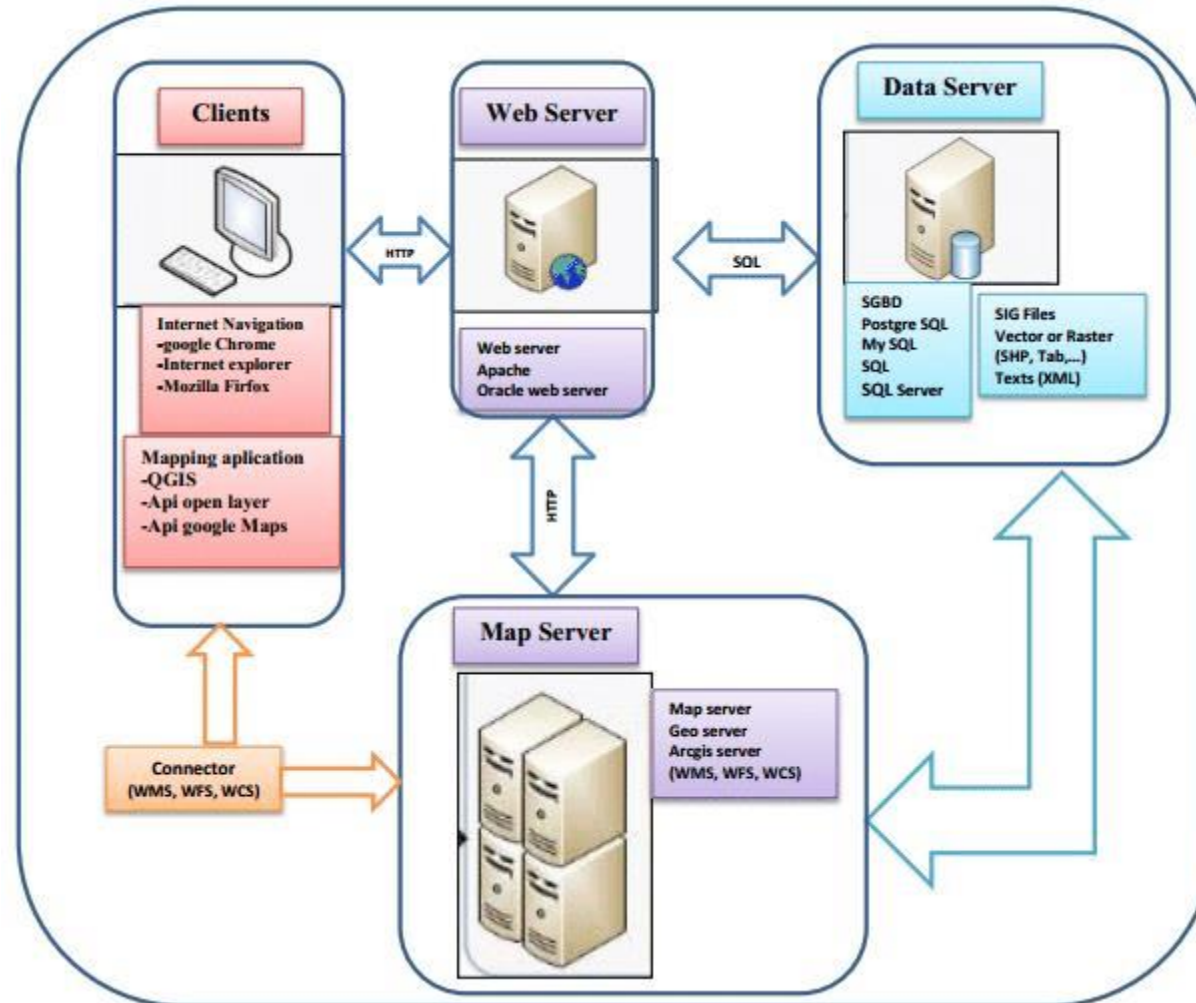
# Ejemplo de Mapeo Físico



# Ejemplo de Mapeo Lógico



# Ejemplo de Mapeo de Aplicaciones



# Beneficios del mapeo de redes

- **Visibilidad:** Facilita la comprensión de la estructura y el funcionamiento de la red.
- **Solución de problemas:** Permite identificar y solucionar problemas de conectividad, rendimiento y seguridad de forma rápida y eficiente.
- **Planificación y escalabilidad:** Ayuda a planificar el crecimiento y la expansión de la red de manera eficiente.
- **Documentación:** Proporciona una documentación precisa y actualizada de la red.
- **Seguridad:** Permite identificar vulnerabilidades y mejorar la seguridad de la red.

# Herramientas para el mapeo de redes

Existen diversas herramientas para realizar el mapeo de redes, desde software gratuito de código abierto hasta soluciones comerciales más sofisticadas. Algunas opciones populares son:

- **Nmap:** Herramienta gratuita para el escaneo de puertos y la detección de dispositivos.
- **Spiceworks:** Software gratuito de gestión de redes que incluye herramientas de mapeo.
- **Microsoft Visio:** Software de diagramación que se puede utilizar para crear mapas de red.
- **SolarWinds Network Performance Monitor:** Solución comercial avanzada para el monitoreo y mapeo de redes.

# Screenshot nmap

```
root@kali: ~  
root@kali: ~ 80x24  
root@kali:~# nmap -sV -Pn 192.168.10.100  
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-31 19:00 IST  
Nmap scan report for 192.168.10.100  
Host is up (0.0097s latency).  
Not shown: 995 closed ports  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          (protocol 2.0)  
80/tcp    open  http         Apache httpd 2.4.25 ((Raspbian))  
3389/tcp  open  ms-wbt-server xrdp  
5901/tcp  open  vnc          VNC (protocol 3.8)  
6001/tcp  open  X11          (access denied)  
1 service unrecognized despite returning data. If you know the service/version,  
please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :  
SF-Port22-TCP:V=7.70%I=7%D=12/31%Time=5C2A19F8%P=x86_64-pc-linux-gnu%r(NUL  
SF:L,29,"SSH-2\0-OpenSSH_7\4p1\X20Raspbian-10\+deb9u4\n");  
MAC Address: B8:27:EB:4B:D5:FA (Raspberry Pi Foundation)  
  
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .  
Nmap done: 1 IP address (1 host up) scanned in 16.11 seconds  
root@kali:~#
```

# Screenshot Spiceworks

spiceworks

Find answers, products, resources

CommunityTools & AppsLearnProduct Reviews

Device Inventory

Devices from all scanners & agents

All Devices107

Devices with tickets0

Agent Download

All Devices (107)

☐ Last Updated

Name

IP Addresses

OS

☐ 2m ago

aaron-pc

101.251.2.2

Windows 8 Pr

☐ 3m ago

frank-pc

101.251.2.21

Windows 7 Pr

☐ 3m ago

george-pc

101.251.2.15

Windows 7 Pr

☐ 3m ago

xander-pc

101.251.2.8

Windows 7 Pr

☐ 2d ago\*

carolyn-pc

101.251.2.4

Windows 7 Pr

☐ 21m ago

davidb-mbp

101.251.2.5

OSX El Capita

☐ 3m ago

greg-mbp

101.251.2.18

OSX Yosemite

☐ 3m ago

stephanie-mbp

101.251.2.19

OSX El Capita

☐ 3m ago\*

terry-pc

101.251.2.24

Windows 7 U

☐ 5m ago

ursula-pc

101.251.2.25

Windows 7 Pr

☐ 6m ago

james-pc

101.251.2.27

Windows 7 Pr

☐ 2m ago

ted-pc

101.251.2.22

Windows 7 Pr

☐ 6m ago

judit-pc

101.251.2.29

Windows 7 Pr

☐ 10m ago

frances-pc

101.251.2.2

Windows 7 Pr

xander-pc

General Info

Antivirus

Hardware

Storage

Memory

Network

Software

Tickets

Hardware

Manufacturer

QEMU

Model

Standard PC (i440FX + PIIX, 1996)

Processor

Common KVM Processor

Memory

4 GB

Video Controller

Microsoft Basic Display Adapter

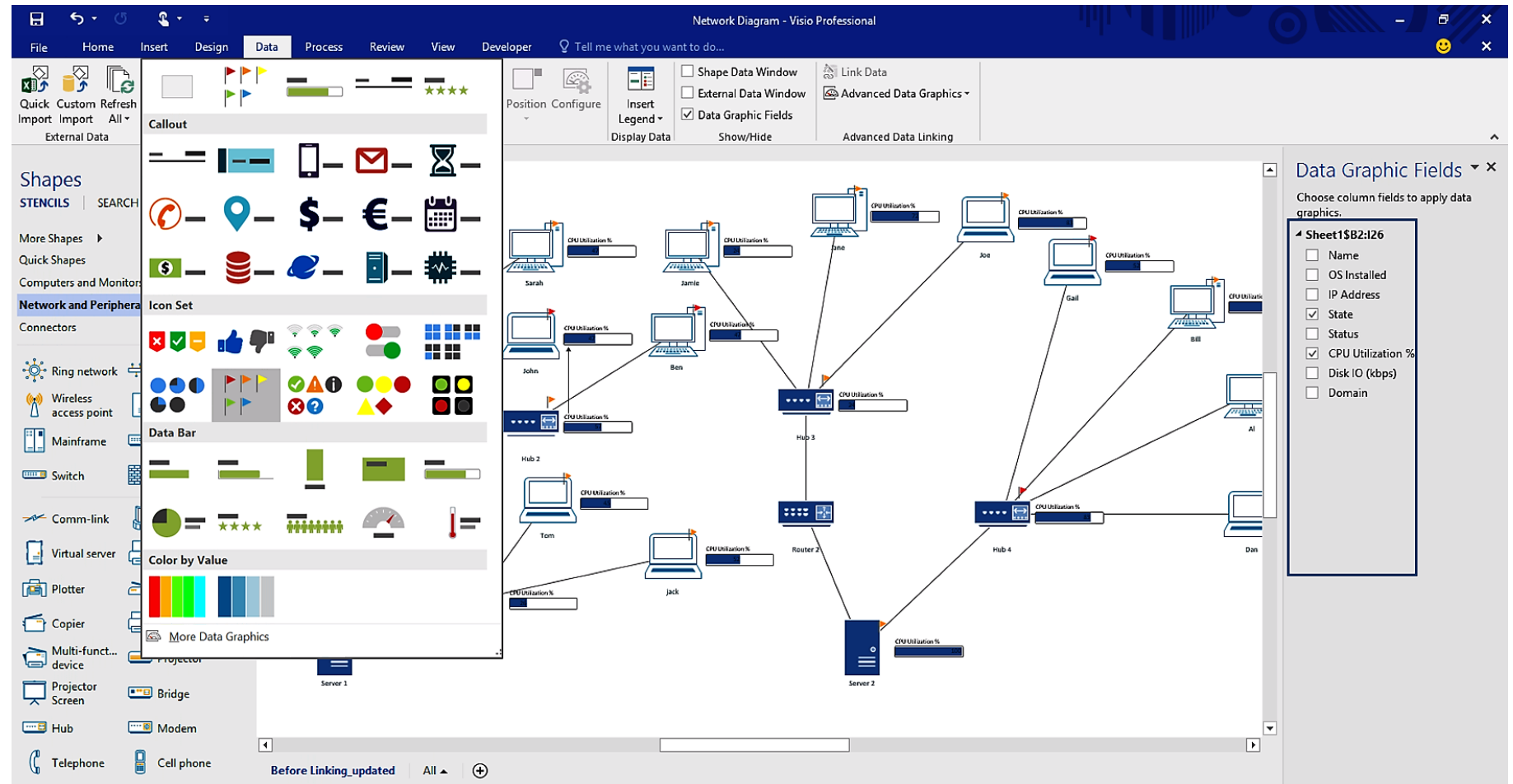
D:

C:

35 GB free



# Screenshot Microsoft VISIO





# Screenshot SolarWinds Network Performance Monitor

## NPM Summary

**All Nodes managed by NPM**

GROUPED BY VENDOR, STATUS

MANAGE NODES HELP

- American Power Conversion Corp.
- Avaya Communication
- Cisco
  - Up
    - AUS-SUB-01
    - bgp-2651-01
    - Cisco APIC

**CISCO APIC**

COMMANDS ▾

IP Address	10.199.4.70
Machine Type	Cisco APIC
Average Response Time	158 ms
City	
Show more custom properties	
    - EAST-2821-
    - EAST-3750-
    - EAST-4506-
    - EAST-FW-A
    - EAST-FW-B
    - EAST-testW
    - ew-3560e.l
    - FIBRE-Tex-M
    - LOSA-2821
    - MUS-NX7K
    - NEWY-2811-WAN
    - Nexus-1
    - Nexus-2
    - NWTIC2ACS5548C
    - NX-7K-A-admin1
    - NX-7K-B-admin

## Interfaces with High Percent Utilization

HELP

NODE	INTERFACE	RECEIVE	TRANSMIT
Nexus-2	port-channel31 · Po31	90%	60%
Nexus-1	Ethernet1/11 · Eth1/11	90%	30%
Nexus-2	mgmt0 · management0	30%	85%
Nexus-1	mgmt0 · management0	30%	85%
EAST-RPi	eth0	86%	24%

◀ | ◁ | Page 1 of 2 | ▷ | ▶ | Items on page 5 | Show all |

Displaying objects 1 - 5 of 9

## Hardware Health Overview

HELP

Critical

Warning

Up

**Nodes Count: 43**

35 Up 3 Warning 5 Critical 0 Undefined

# Enumeración e identificación de componentes de redes de computadoras

# Introducción

La enumeración e identificación de componentes de redes de computadoras es un proceso fundamental para comprender y gestionar la infraestructura de red. Se trata de identificar y catalogar todos los dispositivos físicos y virtuales que forman parte de la red, incluyendo:

- **Dispositivos físicos**
- **Dispositivos virtuales**
- **Información de identificación**
- **Herramientas para la enumeración e identificación**
- **Beneficios de la enumeración e identificación**

# Dispositivos físicos

- **Routers:** Enrutan el tráfico de red entre diferentes redes o subredes.
- **Switches:** Conectan dispositivos a la red y permiten la comunicación entre ellos.
- **Puntos de acceso inalámbrico:** Permiten que los dispositivos inalámbricos se conecten a la red.
- **Firewalls:** Protegen la red de accesos no autorizados y ataques cibernéticos.
- **Servidores:** Proporcionan recursos y servicios a los usuarios de la red, como archivos, aplicaciones, correo electrónico, etc.
- **Impresoras:** Permiten imprimir documentos desde los dispositivos conectados a la red.
- **Cámaras de seguridad:** Monitorean la red y sus alrededores.
- **Otros dispositivos:** Teléfonos IP, dispositivos IoT, etc.

# Dispositivos virtuales

- **Máquinas virtuales:** Ejecutan sistemas operativos y aplicaciones en un entorno virtualizado.
- **Contenedores:** Agrupan aplicaciones y sus dependencias en un paquete portátil.
- **Controladores de dominio:** Gestionan la autenticación y autorización de usuarios en redes Windows.
- **Switches virtuales:** Permiten la segmentación de la red en subredes virtuales.
- **Firewalls virtuales:** Protegen las redes virtuales de accesos no autorizados.

# Información de identificación

Para cada dispositivo, se debe recopilar información relevante como:

- **Dirección IP:** La dirección única que identifica al dispositivo en la red.
- **Nombre de host:** Un nombre que identifica al dispositivo de forma más fácil de recordar.
- **Marca y modelo:** El fabricante y modelo del dispositivo.
- **Sistema operativo:** El sistema operativo que ejecuta el dispositivo.
- **Fecha de instalación:** La fecha en que se instaló el dispositivo en la red.
- **Ubicación física:** La ubicación física del dispositivo en la red.
- **Función:** La función que cumple el dispositivo en la red.

# Herramientas para la enumeración e identificación

Existen diversas herramientas para realizar la enumeración e identificación de componentes de redes, como:

- **Nmap:** Herramienta gratuita para el escaneo de puertos y la detección de dispositivos.
- **Spiceworks:** Software gratuito de gestión de redes que incluye herramientas de detección de dispositivos.
- **Nessus:** Solución comercial para la evaluación de vulnerabilidades que incluye la detección de dispositivos.
- **Microsoft System Center Configuration Manager:** Solución de gestión de sistemas que incluye herramientas para la detección e inventario de dispositivos.

# Screenshot Nessus

Nessus / Scans / Hosts

Nessus Scans Schedules Policies Users paul

Basic Network Scan Audit Trail Filter Hosts

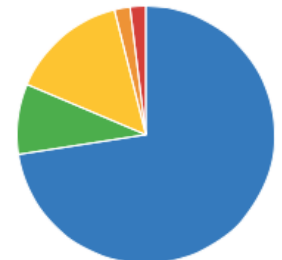
Scans > Hosts 24 Vulnerabilities 102 Remediations 5 Hide Details

Host	Vulnerabilities ▲	
192.168.1.1	18 7 57	✓
192.168.1.242	4 41	✓
192.168.1.16	6 40	✓
192.168.1.81	3 31	✓
192.168.1.98	2 4 24	✓
192.168.1.10	3 21	✓
192.168.1.67	2 23	✓
192.168.1.20	2 14	✓
192.168.1.21	2 14	✓
192.168.1.22	2 14	✓

**Scan Details**

Name: Basic Network Scan  
Folder: My Scans  
Status: Running  
Policy: Basic network scan  
Targets: 192.168.1.0/24  
Start time: Sun Dec 8 09:46:36 2013

**Vulnerabilities**



- Info
- Low
- Medium
- High
- Critical



# Screenshot Microsoft System Center Configuration Manager

System Center Configuration Manager (Connected to P01 - windows-noob primary site) (Evaluation, 89 days left)

Home

History Check for updates Refresh Saved Searches Install Update Pack Run prerequisite check Retry installation Ignore prerequisite warnings Promote Pre-production Client Download

Updates and Servicing Updates Search Install Download

Administration Overview Updates and Servicing

Updates and Servicing 0 items

Name	Date Released	State	Prereq Only	Ignore...	Full Version	Client Version	Last U
Configuration Manager Technical Preview 1810	10/1/2018 12:00 AM	Installed	No	Yes	5.00.8729.1000	5.00.8729.1000	10/8/
Configuration Manager Technical Preview 1810.2	10/16/2018 12:00 AM	Ready to install	No	No	5.00.8735.1000	5.00.8735.1000	10/17

Configuration Manager Technical Preview 1810.2

General Information Contents Related Objects

Description: New update for Configuration Manager. This update includes new Configuration Manager site server updates Configuration Manager console updates Configuration Manager client updates Fixes for known issues

Summary Features

Ready

## Beneficios de la enumeración e identificación

- **Visibilidad:** Permite tener una visión completa de la infraestructura de red.
- **Gestión:** Facilita la gestión de dispositivos, como la instalación de actualizaciones, la configuración de seguridad y la resolución de problemas.
- **Seguridad:** Ayuda a identificar dispositivos no autorizados o vulnerables en la red.
- **Planificación:** Permite planificar el crecimiento y la expansión de la red de manera eficiente.