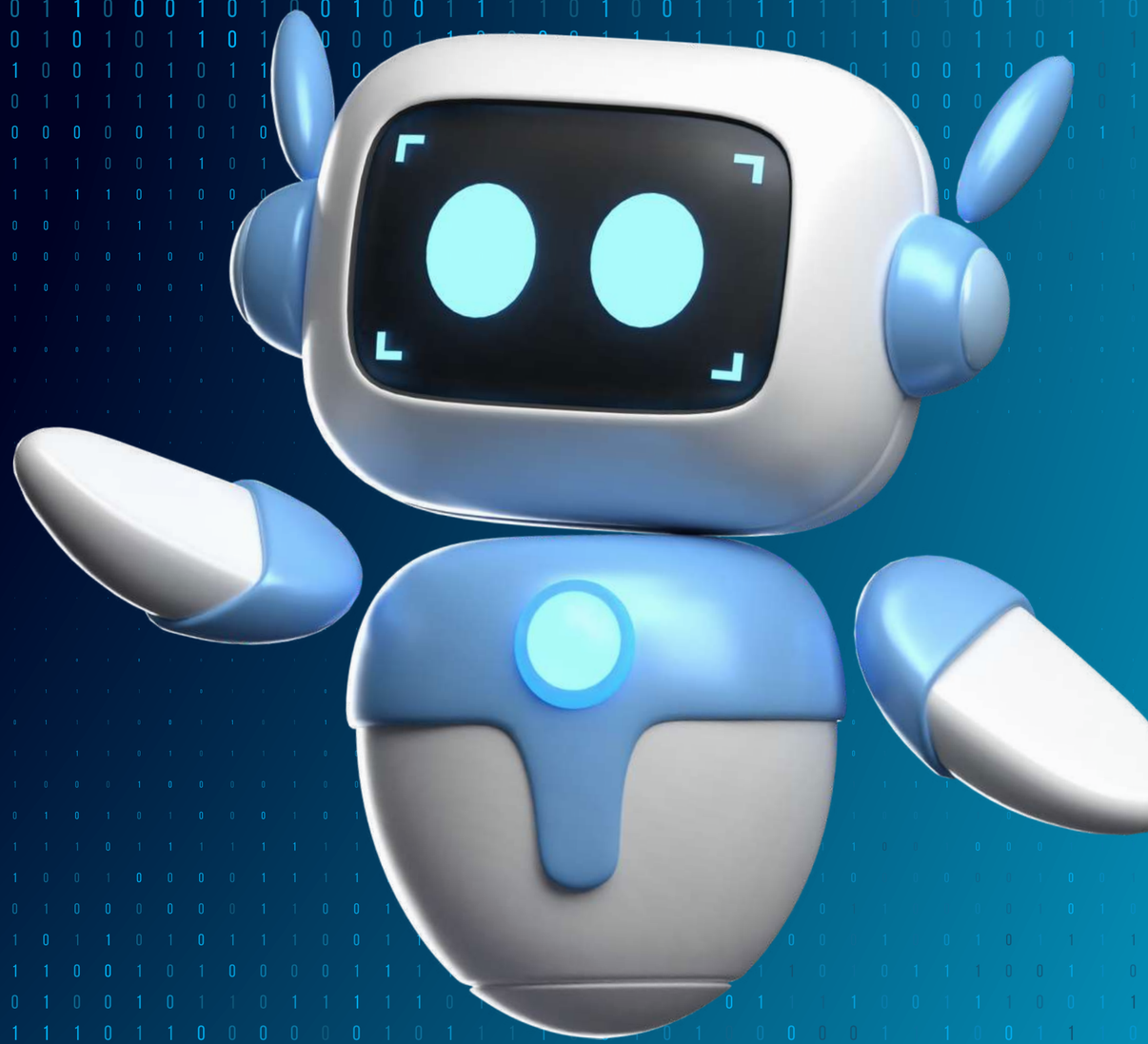
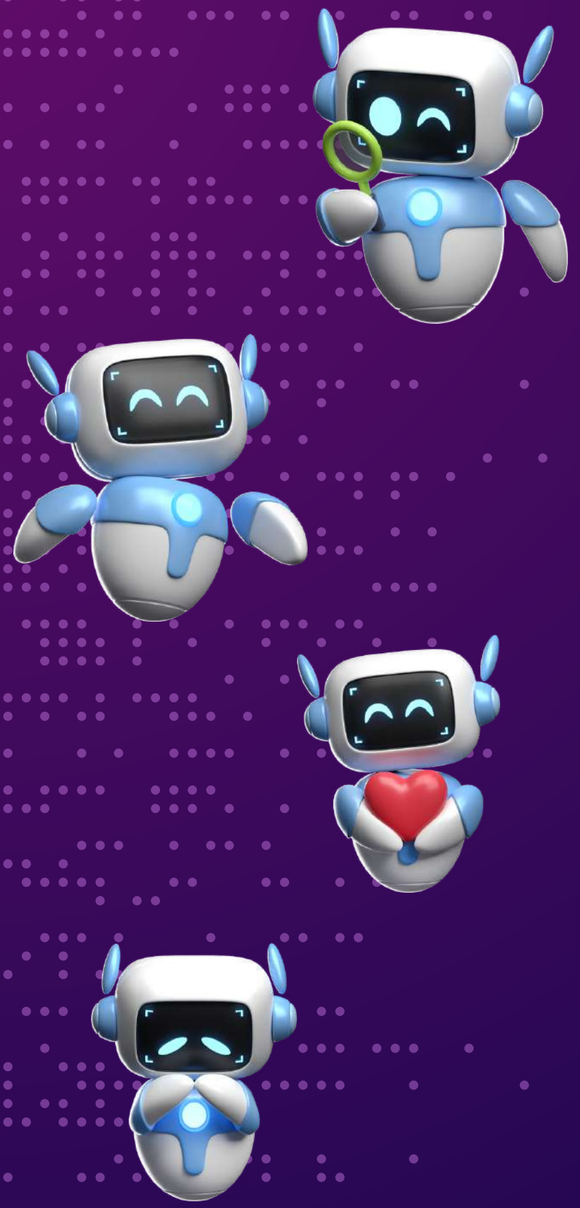
# ACL

## Access Control List



SIT "Empowering Bounciless Digital Transformation"
School of Information Technology
King Mongkut's University of Technology Thonburi



# LEARNING OUTCOME

An Access Control List (ACL) is a security measure commonly used in computer systems and networks to control which users or systems have access to specific resources or services.

ACLs typically list permissions associated with different objects, such as files, folders, or network devices, and define which entities are allowed or denied access to those resources.

By setting up and managing ACLs effectively, organizations can enhance their system security by restricting unauthorized access and ensuring that only authorized users can interact with sensitive data or services.

# NETWORK DESIGN

SW-A

SW-B

Network Address
**1x.4.4.0 /24**

Network Address
**1x.1.1.0 /24**

Network Address
**1x.2.2.0 /24**

Network Address
**1x.3.3.0 /24**

# IP ADDRESS DESIGN

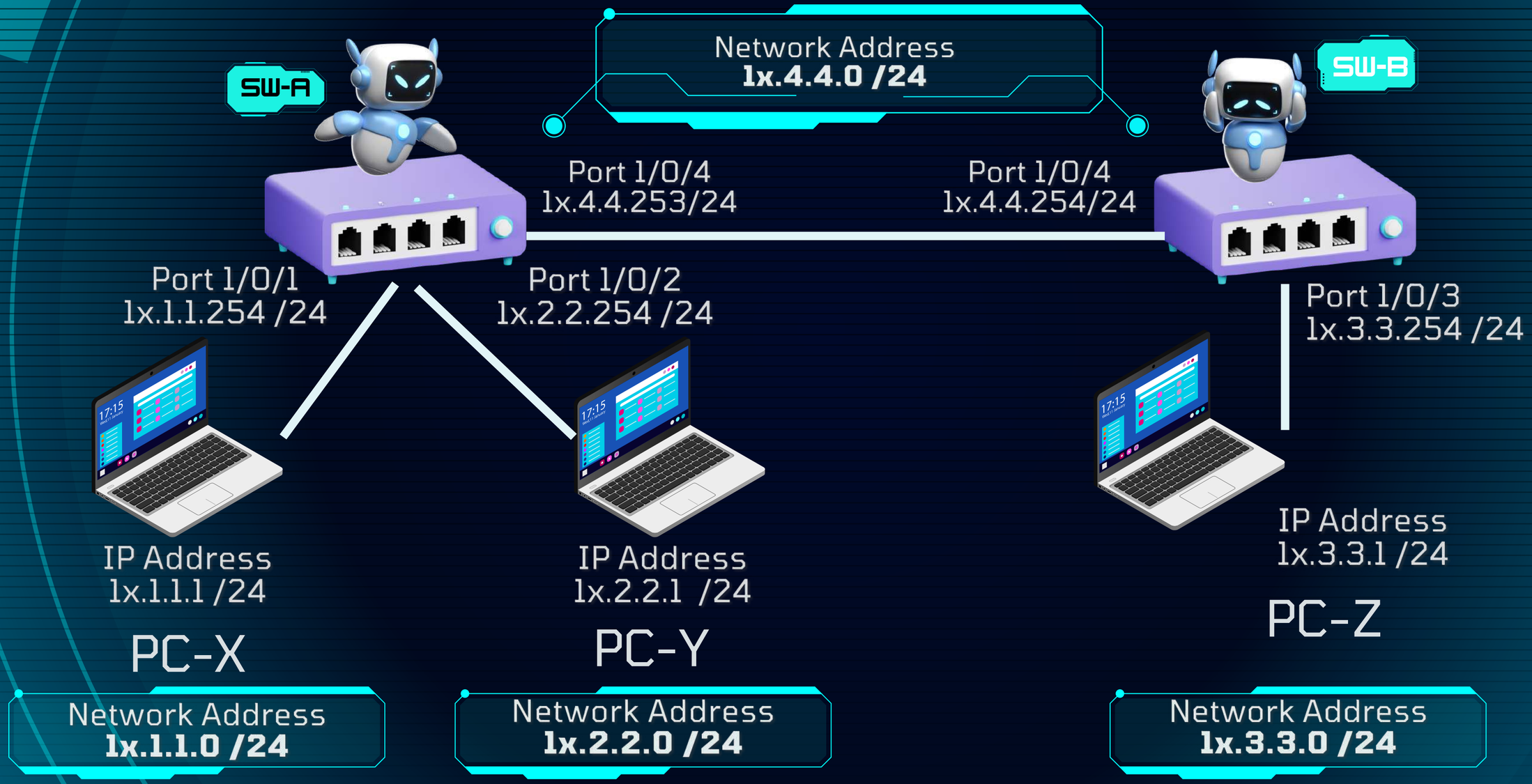
## Room 10-01

| | |
|---|---|
| 11.0.0.0 /8 | Rack 11 |
| 12.0.0.0 /8 | Rack 12 |
| 13.0.0.0 /8 | Rack 13 |
| 14.0.0.0 /8 | Rack 14 |
| 15.0.0.0 /8 | Rack 15 |

## Room 10-02

| | |
|---|---|
| 21.0.0.0 /8 | Rack 21 |
| 22.0.0.0 /8 | Rack 22 |
| 23.0.0.0 /8 | Rack 23 |
| 24.0.0.0 /8 | Rack 24 |
| 25.0.0.0 /8 | Rack 25 |

# PHYSICAL DESIGN



# OSPF CONFIGURATION COMMAND

## SW-A

```
system-view
sysname SW-A
#
interface gigabitethernet 1/0/1
port link-mode route
ip address xx.1.1.254 24
#
interface gigabitethernet 1/0/2
port link-mode route
ip address xx.2.2.254 24
#
interface gigabitethernet 1/0/4
port link-mode route
ip address xx.4.4.253 24
#
ospf 1
area 0
network xx.1.1.0 0.0.0.255
network xx.2.2.0 0.0.0.255
network xx.4.4.0 0.0.0.255
#
```

---

## SW-B [HP/H3C]

```
system-view
sysname SW-B
#
vlan 3
port gigabitethernet 1/0/3
interface vlan-interface 3
ip address xx.3.3.254 24
#
vlan 4
port gigabitethernet 1/0/4
interface vlan-interface 4
ip address xx.4.4.254 24
#
ospf 1
area 0
network xx.3.3.0 0.0.0.255
network xx.4.4.0 0.0.0.255
#
```

---

## SW-B [ARUBA]

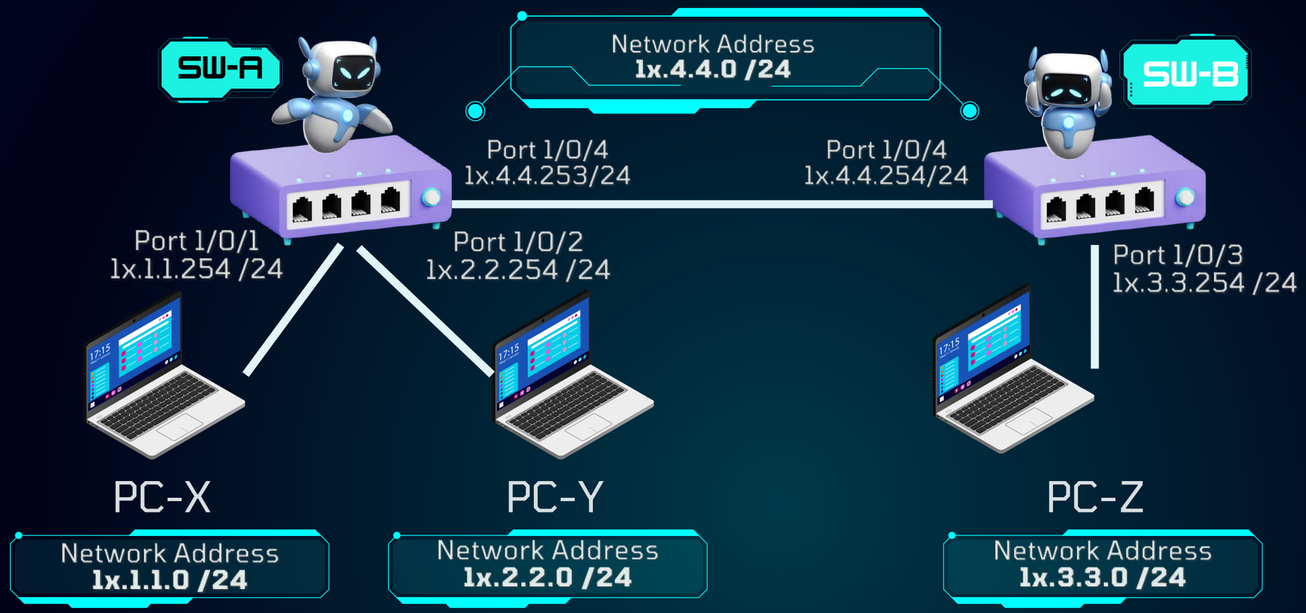
```
enable
configure terminal
hostname SW-B

vlan 3
untagged 3
ip address xx.3.3.254 255.255.255.0

vlan 4
untagged 4
ip address xx.4.4.254 255.255.255.0

ip routing
router ospf
area 0
enable

vlan 3
ip ospf
vlan 4
ip ospf
```

---

display ip interface brief
display ip routing-table
display ospf peer
display ospf

show ip route
show ip ospf

# DISPLAY IP ROUTING




## Routing table SW-A

| Dest NW | Mask | Protocol | Nexthop |
|---|---|---|---|
| 10.1.1.0 | /24 | direct | - |
| 10.2.2.0 | /24 | direct | - |
| 10.4.4.0 | /24 | direct | - |
| 10.3.3.0 | /24 | OSPF | 10.4.4.254 |

## Routing table SW-B

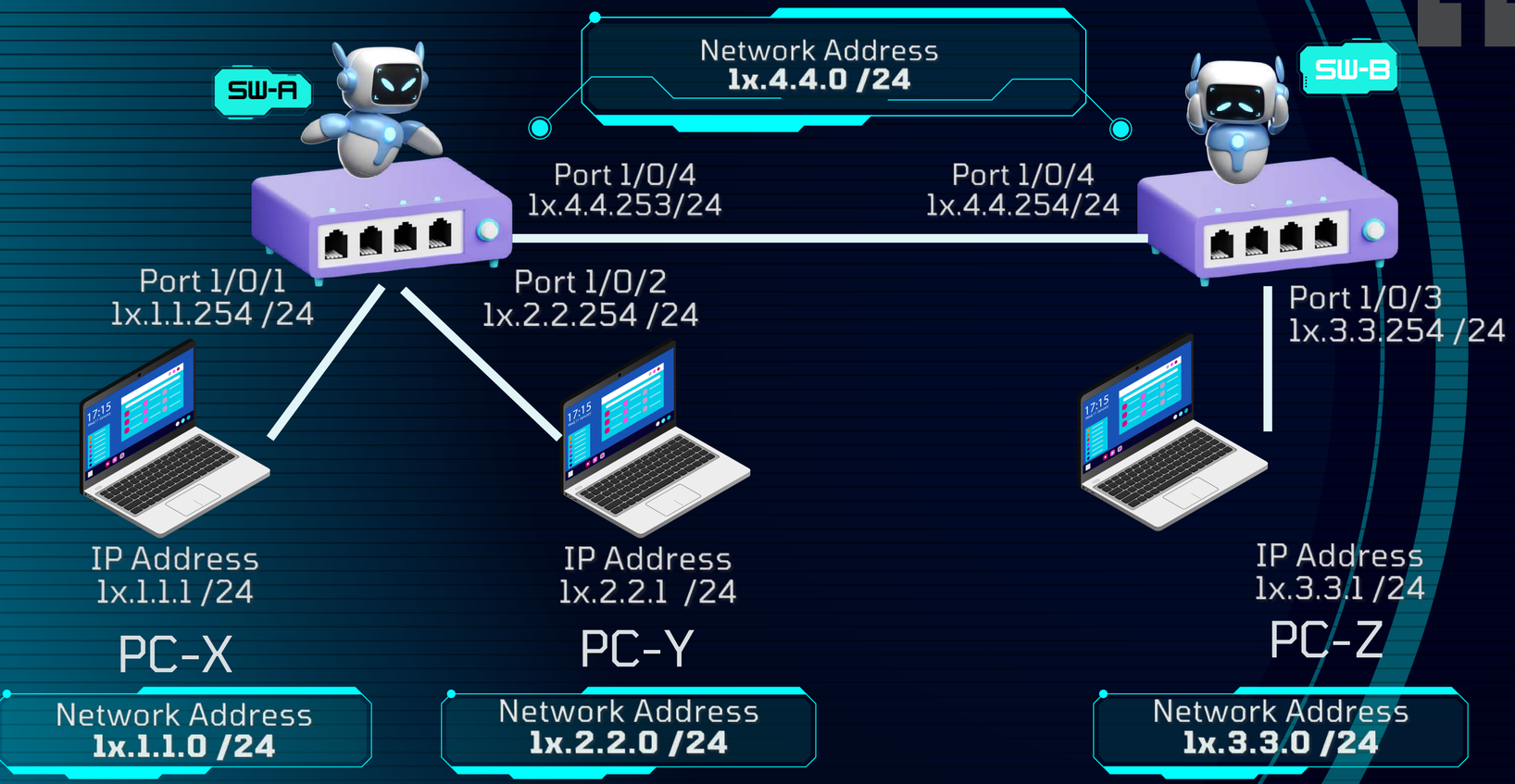
| Dest NW | Mask | Protocol | Nexthop |
|---|---|---|---|
| 10.3.3.0 | /24 | direct | - |
| 10.4.4.0 | /24 | direct | - |
| 10.1.1.0 | /24 | OSPF | 10.4.4.253 |
| 10.2.2.0 | /24 | OSPF | 10.4.4.253 |

# ACCESS CONTROL LIST

An access control list (ACL) is a set of for identifying traffic based on criteria such as source IP address, destination IP address, and port number.

ACLs are used for: packet filtering rules (permit or deny statements), QoS, IP routing, traffic classification and identification.

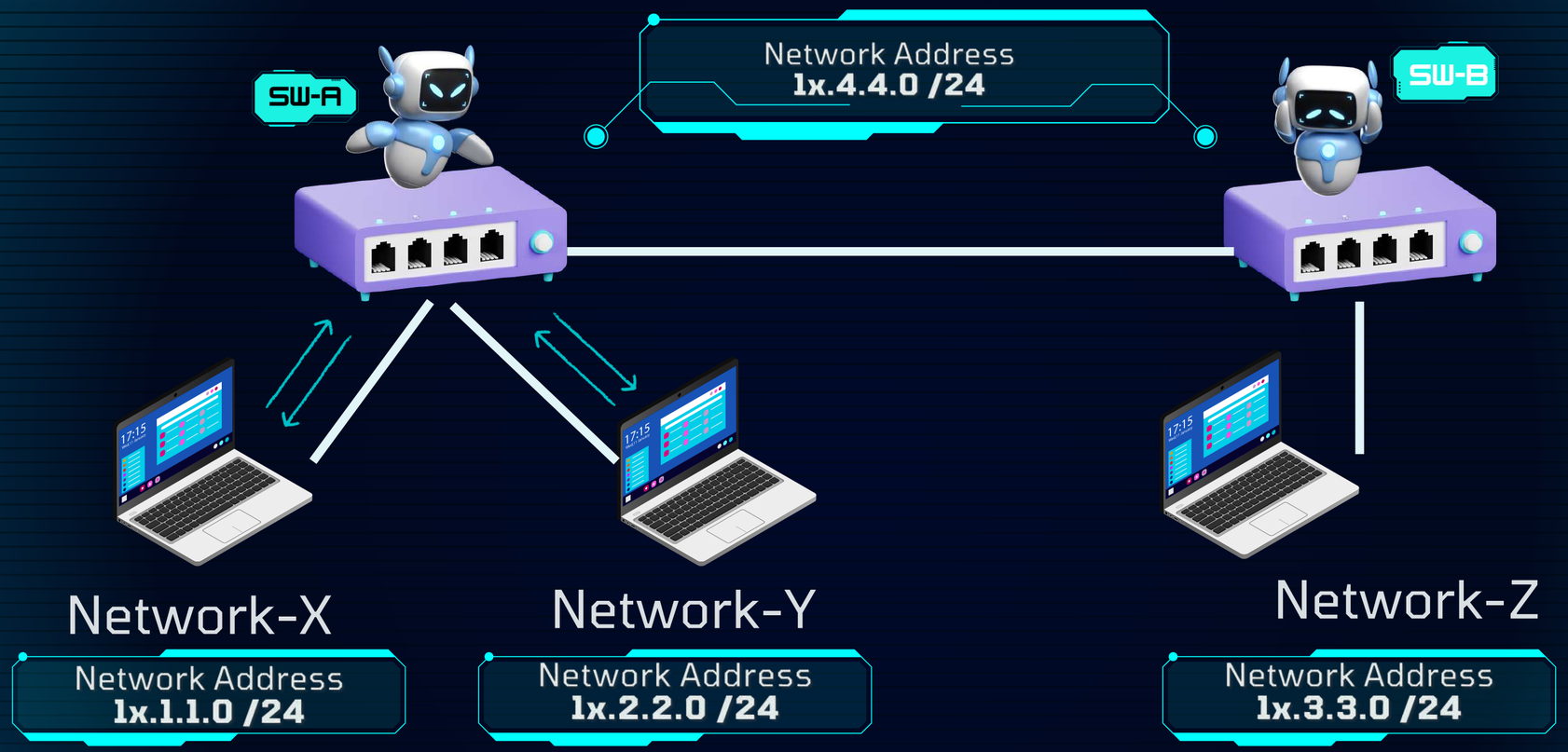
# ACCESS CONTROL LIST PLANNING




"What are the network traffic flow?

How to add the ACL to the interfaces or VLANs?"

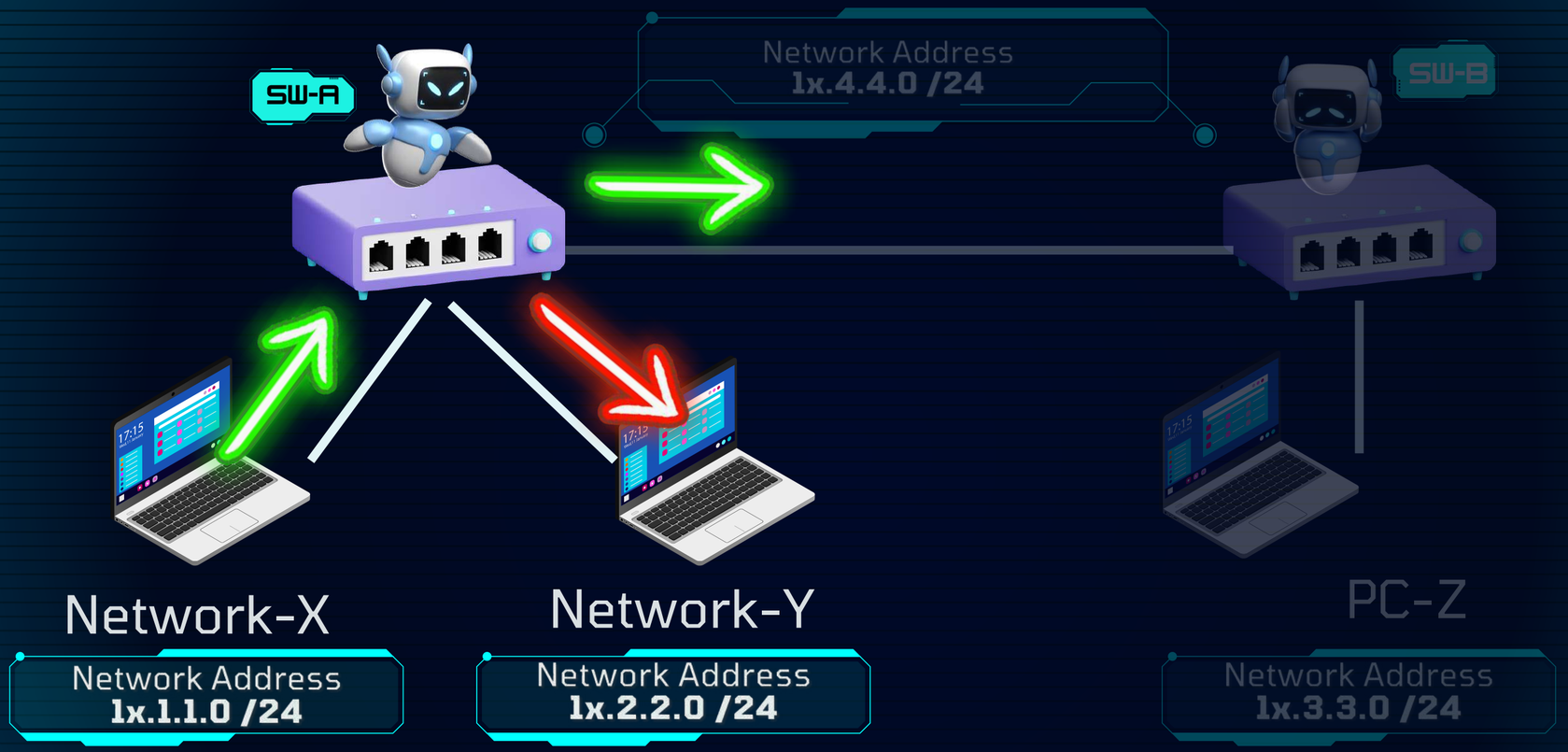
# THE SECURITY POLICY




**Policy 1: Block the Network X to Network Y**

***1.What are the network traffic flow?***
***2.How to add the ACL to the interfaces or VLANs?***

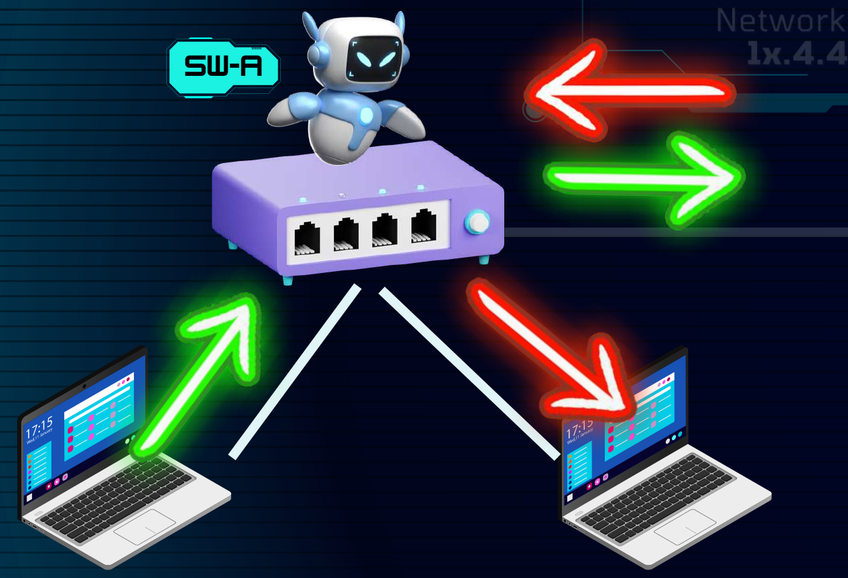
# THE SECURITY POLICY




**Policy 1: Block the network X to network Y**

***1.What are the network traffic flow?***

# WHAT ARE THE NETWORK TRAFFIC FLOW?




An adaptation of this policy to a language that a computer can understand might look something like the following:

**inbound**

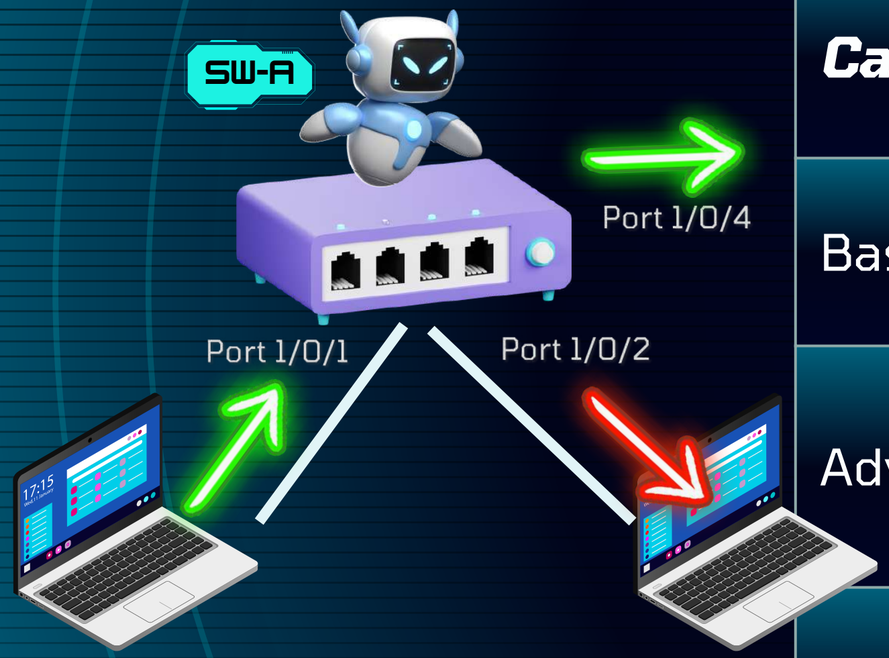
Permit IP from any to any return-traffic
Permit IP from any to Web-server protocol equal http
(implicit deny all)

**outbound**

Permit IP from any to any
(implicit deny all)

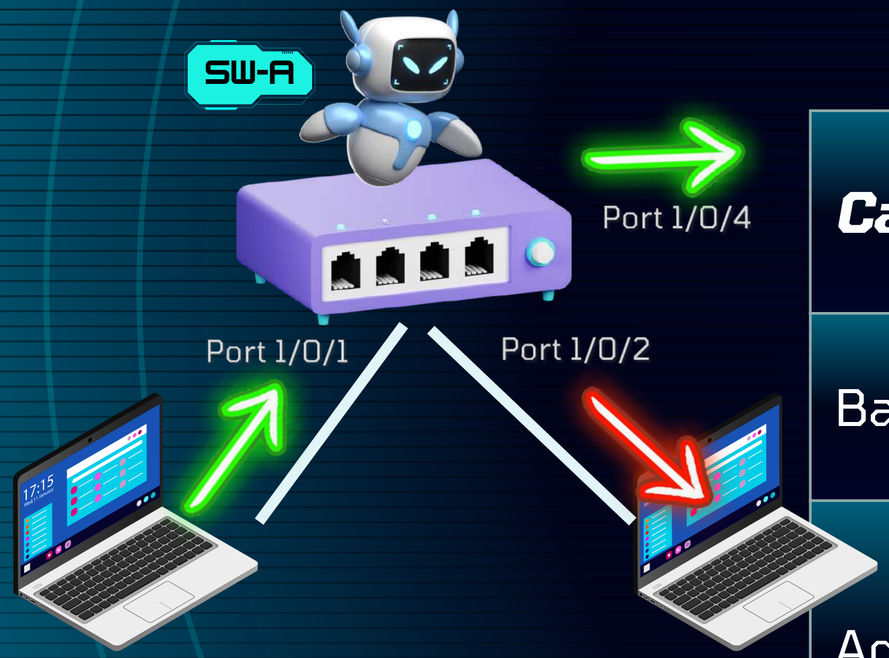
**Policy 1: Block the network X to network Y**

# ACL CATEGORIES [HP/H3C]



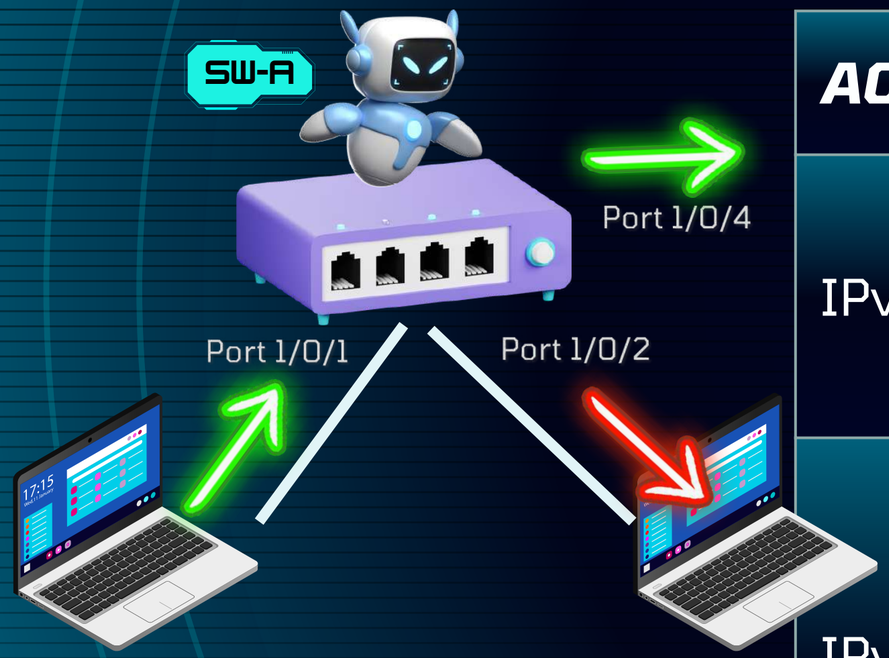

| Category | ACL number | Match criteria |
|---|---|---|
| Basic ACLs | 2000 to 2999 | Source IPv4 address |
| Advanced ACLs | 3000 to 3999 | Source IPv4 address, destination IPv4 address, protocols over IPv4, and other Layer 3 and Layer 4 header fields |
| Ethernet frame header ACLs | 4000 to 4999 | Layer 2 header fields, such as source and destination MAC addresses, 802.1p priority, and link layer protocol type |

# ACL CATEGORIES [ARUBA]



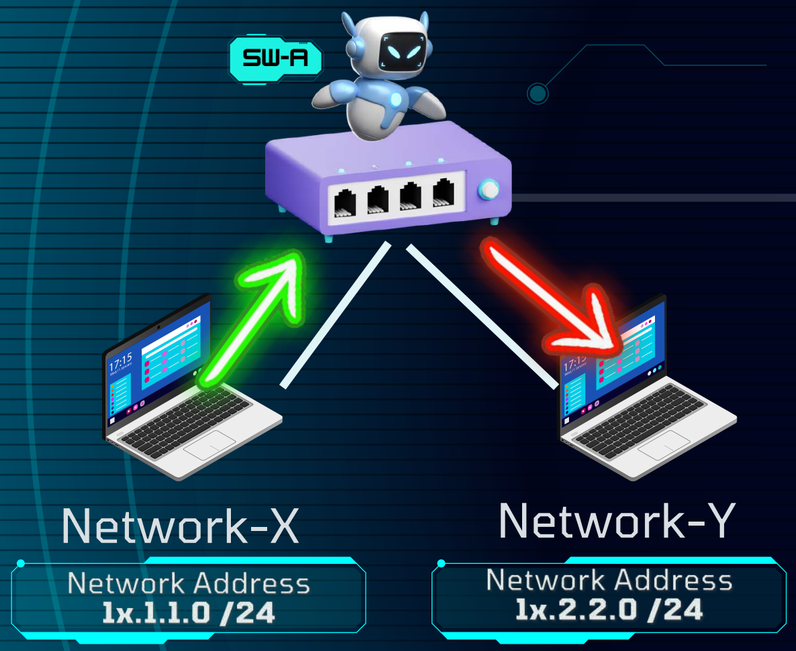

| Category | ACL number | Match criteria |
|---|---|---|
| Basic ACLs | 1 to 99 | Source IPv4 address |
| Advanced ACLs | 100 to 199 | Source IPv4 address, destination IPv4 address, protocols over IPv4, and other Layer 3 and Layer 4 header fields |

# SORT ACL RULES IN DEPTH-FIRST ORDER




| ***ACL Category*** | ***Sequence of tie breakers*** |
|---|---|
| IPv4 basic ACL | 1. VPN instance<br>2. More 0s in the source IP address wildcard (more 0s means a narrower IP address range)<br>3. Smaller rule ID |
| IPv4 advanced ACL | 1. VPN instance<br>2. Specific protocol type rather than IP (IP represents any protocol over IP)<br>3. More 0s in the source IP address wildcard mask<br>4. More 0s in the destination IP address wildcard<br>5. Narrower TCP/UDP service port number range<br>6. Smaller ID |

# ACL CONFIGURATION [ STEP 2.1 ]




Create an IPv4 basic / advanced ACL and enter its view

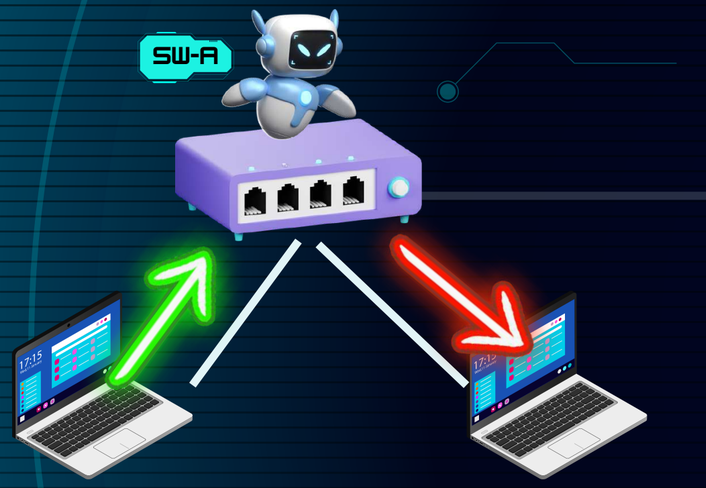
```
[HP] acl number acl-number [name acl-name]
[match-order {auto | config}]
```

–After creating an ACL with a name,
–Use the acl name acl-name command to enter the view of a named ACL.
–ACLs cannot rename it or delete its name.

**Policy 1: Block the network X to network Y**

## 2.How to add the ACL to the interfaces or VLANs?

# ACL CONFIGURATION [ STEP 2.2 ]




•Create or edit a rule in basic ACL

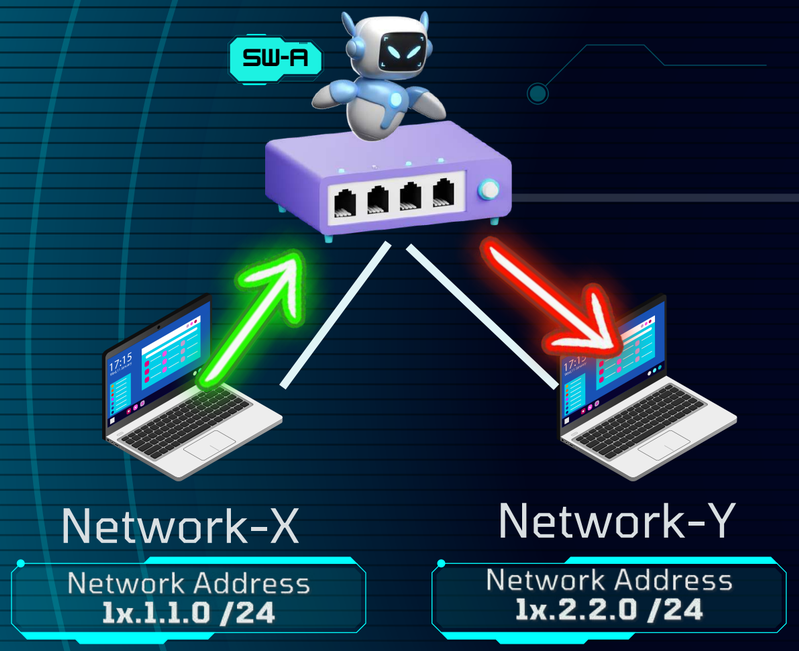
```
[HP acl] rule [rule-id] {deny | permit}
[counting | fragment | logging | source
{source-addr source-wildcard | any} | time-
range time-rangename | vpn-instance vpn-
instancename ]*
```

–IPv4 basic ACLs are numbered in the range 2000 to 2999.
–To create or edit multiple rules, repeat this step.

**Policy 1: Block the network X to network Y**

## 2.How to add the ACL to the interfaces or VLANs?

# ACL CONFIGURATION [ STEP 2.3 ]




Enter Layer 2/3 Ethernet or VLAN interface view

```
[HP] interface interface-type interface-number
```

Apply an IPv4 ACL to the interface

```
[HP-interface] packet-filter {acl-number | name acl-name} {inbound | outbound}
```

SW-B

PC-Z

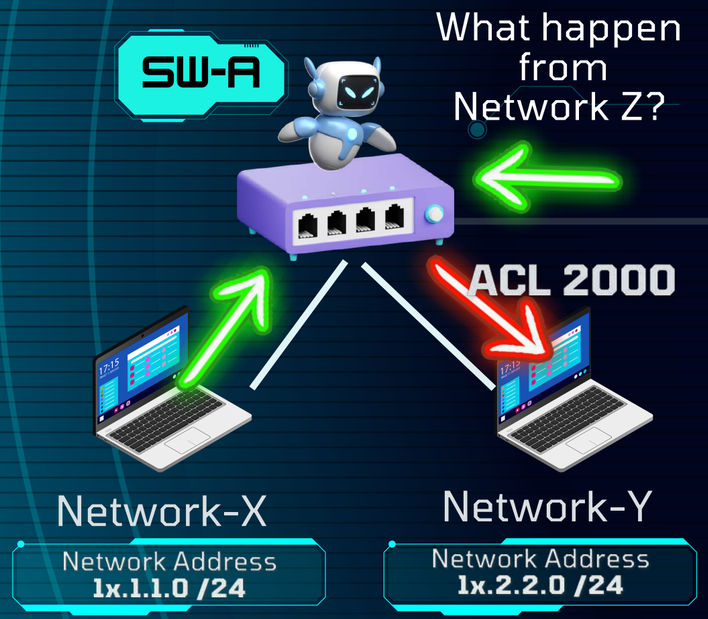
Network Address
1x.3.3.0 /24

**Policy 1: Block the network X to network Y**

## 2.How to add the ACL to the interfaces or VLANs?

# ACL CONFIGURATION GUIDE

## Policy 1: Block the network X to network Y




Step 2.1 Create the Basic ACL

```
[SW-A] acl number 2000
```

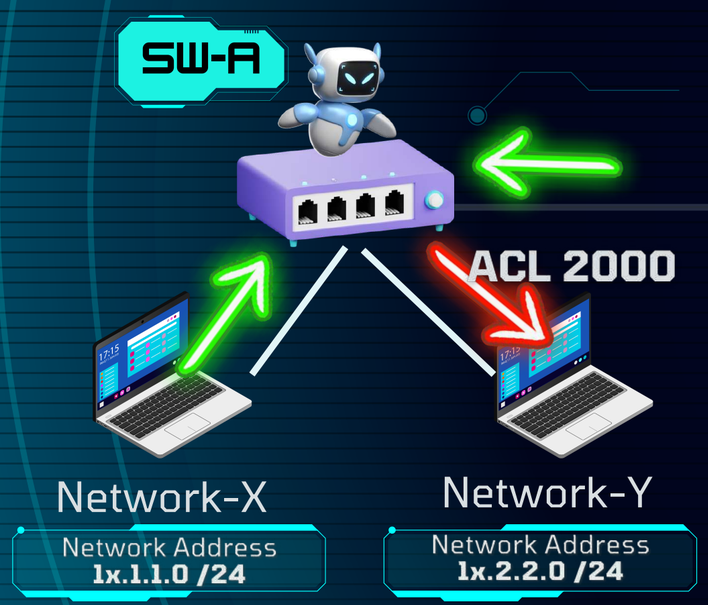
Step 2.2 Create the ACL rules

```
[SW-A-acl-bas-2000] rule 100 deny source
xx.1.1.0 0.0.0.255
[SW-A-acl-bas-2000] rule 200 permit source any
```

Step 2.3 Apply the ACL to interface

```
[SW-A] interface gigabitethernet 1/0/1
[SW-A-intG1/0/1] packet-filter 2000 inbound

[SW-A] interface gigabitethernet 1/0/2
[SW-A-intG1/0/2] packet-filter 2000 outbound
```

# DISPLAY THE ACL



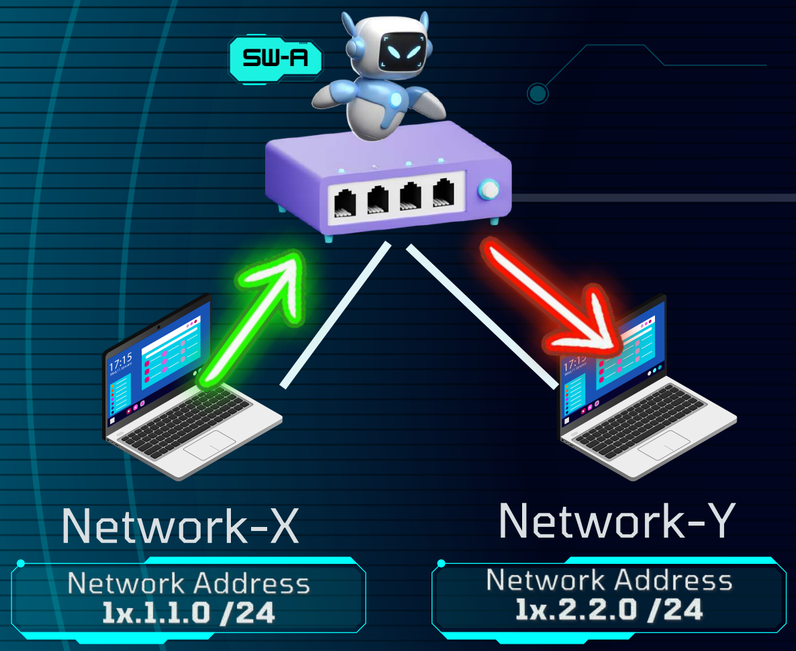

Display configuration and match statistics for one or all IPv4 ACLs

```
[HP] display acl {acl-number | all | name
aclname } [slot slot-number] [ | { begin |
exclude | include} regular-expression ]
```

Display the application status of packet filtering ACLs on interfaces

```
[HP] display packet-filter {{all | interface
interface-type interface-number} [inbound |
outbound] |  interface vlan-interface
vlaninterface-number [inbound | outbound]
[slot slot-number]} [ |  {begin | exclude |
include} regular-expression]
```

# ACL CONFIGURATION [ STEP 2.2 ]




Create or edit a rule in Advanced ACL

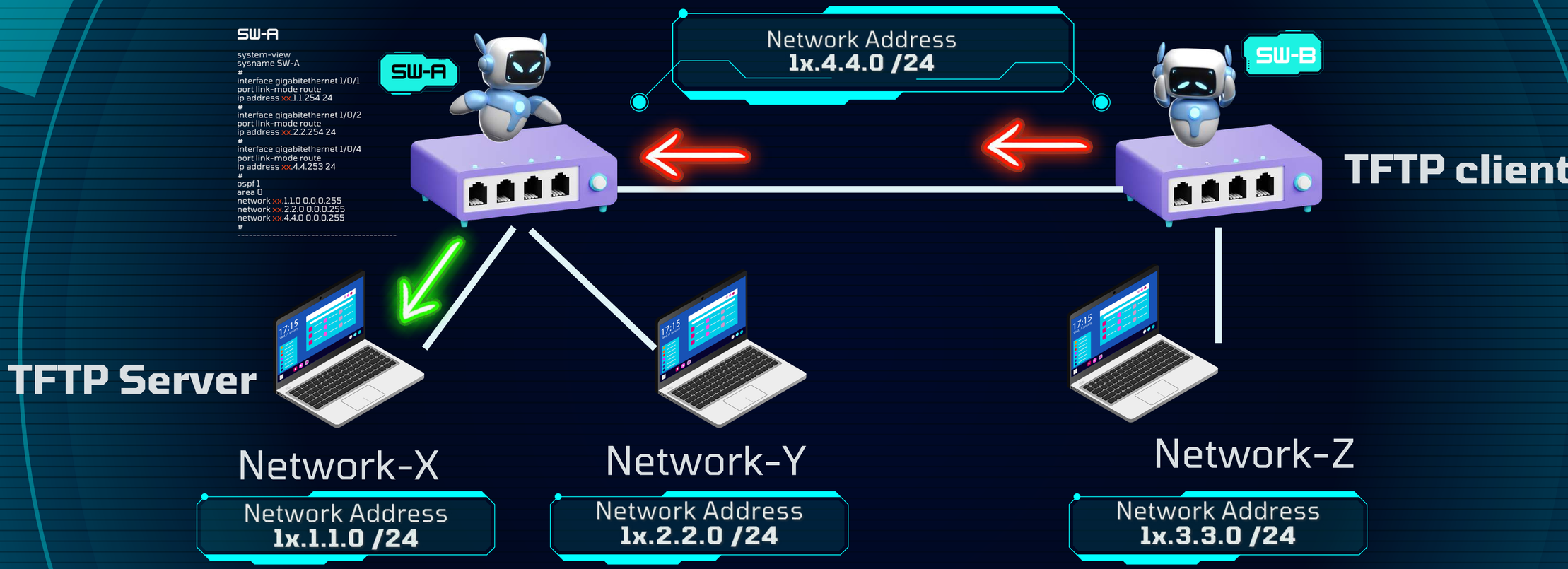
```
[HP acl] rule [rule-id] {deny | permit}
protocol [{{ ackack-value | fin fin-value |
pshpsh-value | rstrstvalue | synsyn-value |
urgurgvalue }* | established} | counting |
destination {dest-addrdest-wildcard | any} |
destination-port operator port1 [port2] |
dscpdscp | fragment | icmp-type {icmp-type
icmp-code | icmp-message} | logging |
precedence precedence | reflective | source
{sour-addr sour-wildcard| any} | source-port
operator port1 [port2] | time-range time-
range-name | tostos | vpn-instance vpn-
instance-name]*
```

–IPv4 basic ACLs are numbered in the range 3000 to 3999.
–To create or edit multiple rules, repeat this step.

# THE SECURITY POLICY

**SW-A**

```
system-view
sysname SW-A
#
interface gigabitethernet 1/0/1
port link-mode route
ip address xx.1.1.254 24
#
interface gigabitethernet 1/0/2
port link-mode route
ip address xx.2.2.254 24
#
interface gigabitethernet 1/0/4
port link-mode route
ip address xx.4.4.253 24
#
ospf 1
area 0
network xx.1.1.0 0.0.0.255
network xx.2.2.0 0.0.0.255
network xx.4.4.0 0.0.0.255
#
----------------------------------------
```

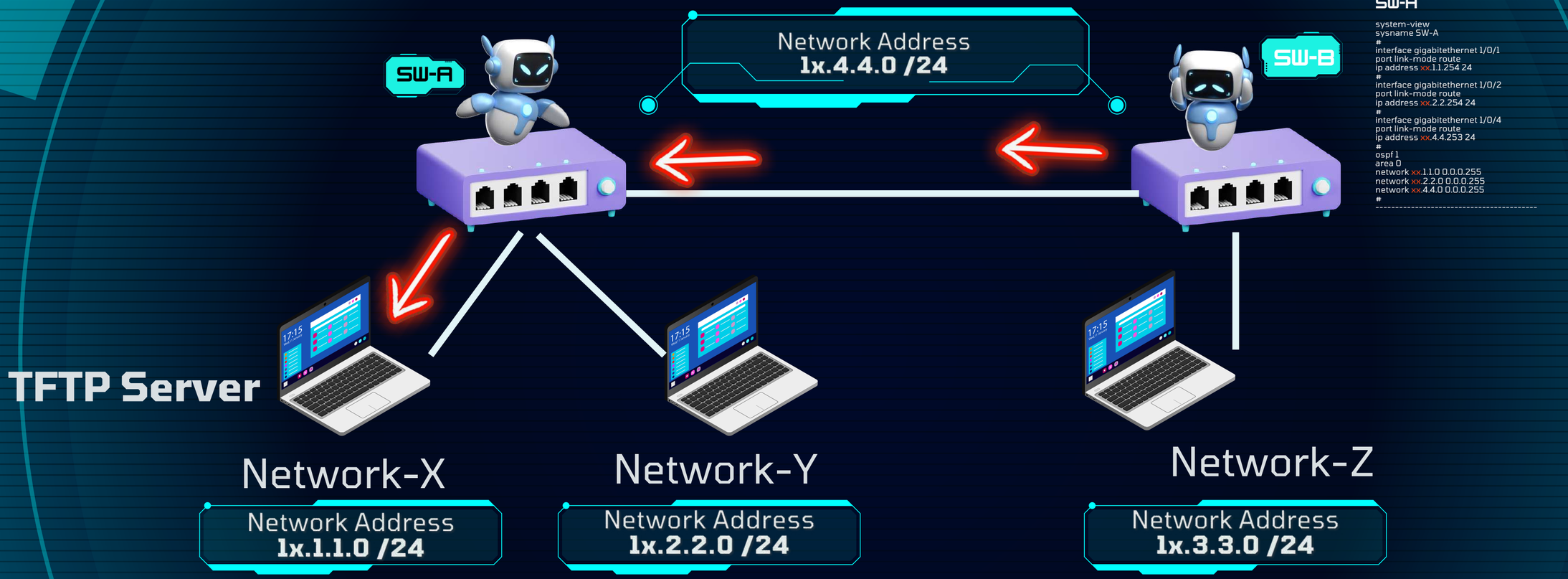



## Policy 2: Block the TFTP to network Z

***1.What are the network traffic flow?***

***2.How to add the ACL to the interfaces or VLANs?***

# THE SECURITY POLICY




**SW-A**

```
system-view
sysname SW-A
#
interface gigabitethernet 1/0/1
port link-mode route
ip address xx.1.1.254 24
#
interface gigabitethernet 1/0/2
port link-mode route
ip address xx.2.2.254 24
#
interface gigabitethernet 1/0/4
port link-mode route
ip address xx.4.4.253 24
#
ospf 1
area 0
network xx.1.1.0 0.0.0.255
network xx.2.2.0 0.0.0.255
network xx.4.4.0 0.0.0.255
#
-----------------------------------------
```

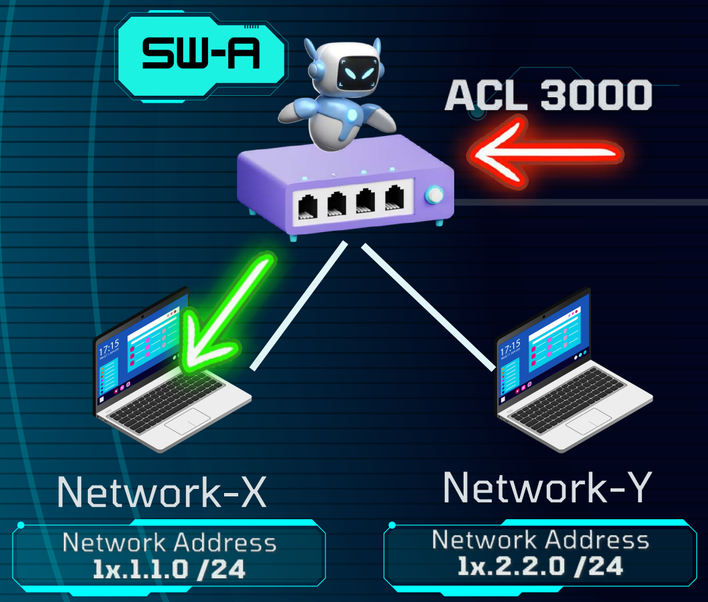
**TFTP client (Switch) upload file to the TFTP server**

```
[SW-B] quit
<SW-B> dir
<SW-B> tftp xx.3.3.1 put system.xml
```

**TFTP client (Aruba) upload file to the TFTP server**

```
SW-B# copy running tftp
```

# ACL CONFIGURATION GUIDE




## Policy 2: Block the TFTP to network Z

Step 2.1 Create the Advanced ACL

```
[SW-A] acl number 3000
```

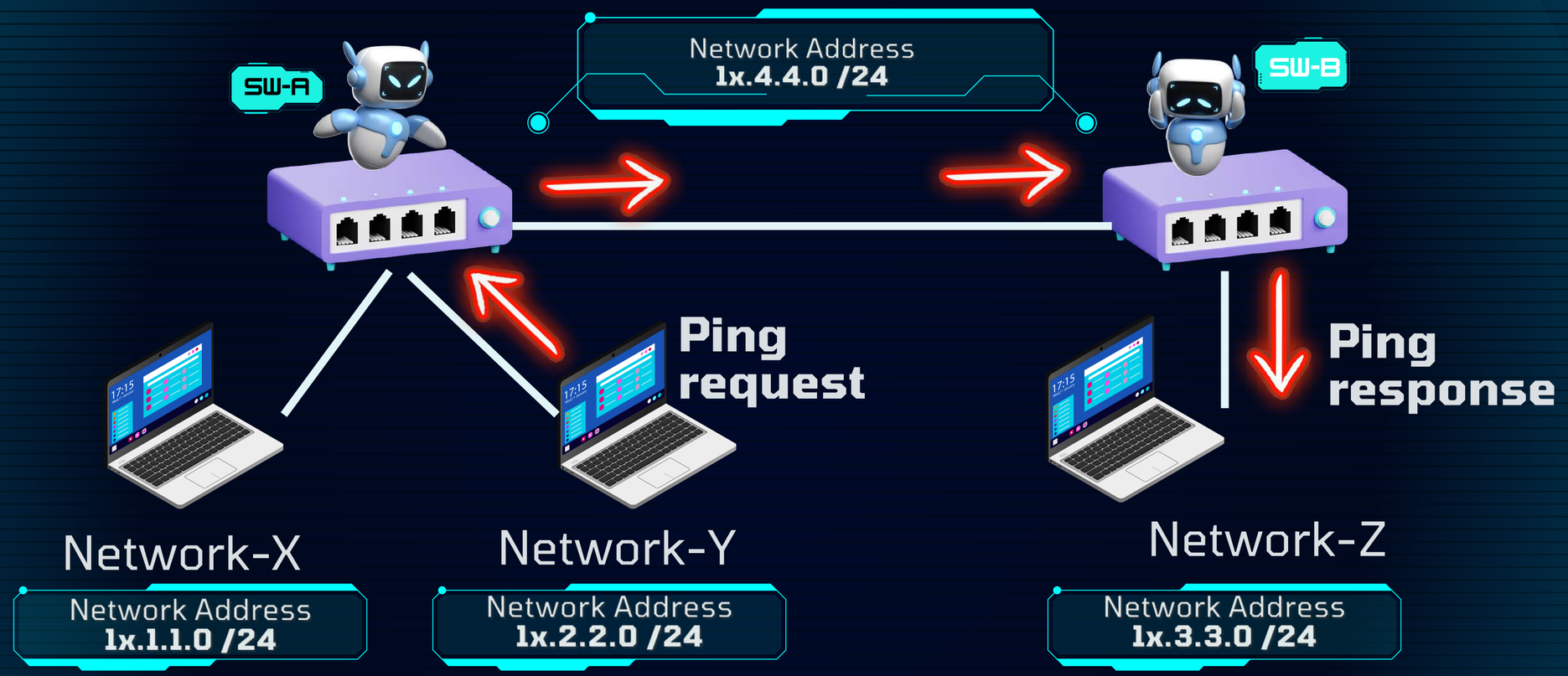
Step 2.2 Create the ACL rules

```
[SW-A-acl-adv-3000] rule 100 deny udp source any
destination xx.1.1.0 0.0.0.255 destination-port eq
69
[SW-A-acl-adv-3000] rule 200 permit ip source any
destination any
```

Step 2.3 Apply the ACL to interface

```
[SW-A] interface gigabitethernet 1/0/4
[SW-A-intG1/0/4] packet-filter 3000 inbound
```

# THE SECURITY POLICY

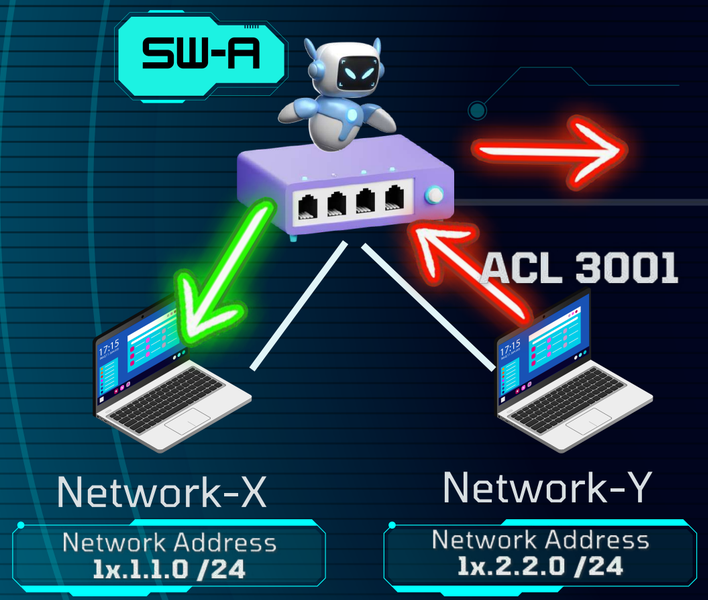



## Policy 3: Block the icmp Network Y to network Z

***1.What are the network traffic flow?***

***2.How to add the ACL to the interfaces or VLANs?***

# ACL CONFIGURATION GUIDE




## Policy 3: Block the icmp Network Y to network Z

Step 2.1 Create the Advanced ACL

```
[SW-A] acl number 3001
```

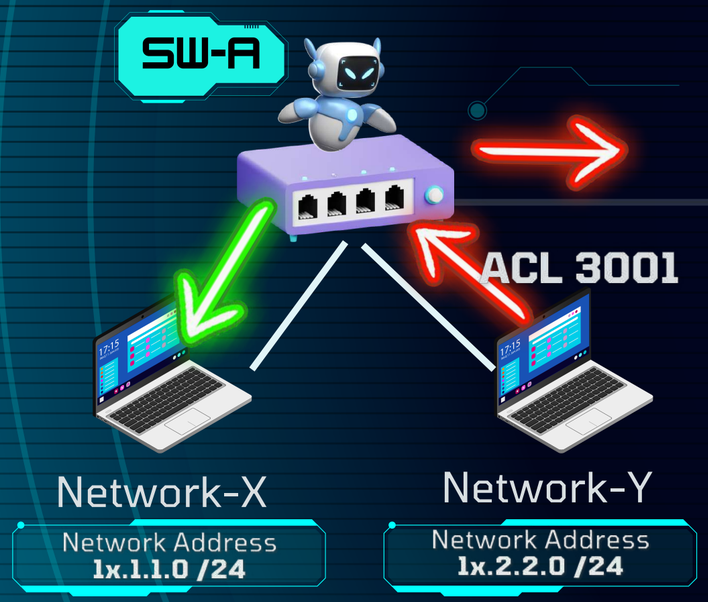
Step 2.2 Create the ACL rules

```
[SW-A-acl-adv-3001] rule 100 deny icmp source
xx.2.2.0 0.0.0.255 destination xx.3.3.0 0.0.0.255
[SW-A-acl-adv-3001] rule 200 permit ip any any
```

Step 2.3 Apply the ACL to interface

```
[SW-A] interface gigabitethernet 1/0/2
[SW-A-intG1/0/2] packet-filter 3001 inbound
```

# ACL CONFIGURATION GUIDE




## Policy 3+: Block the icmp Network Y to network Z [option + time-based ACL]

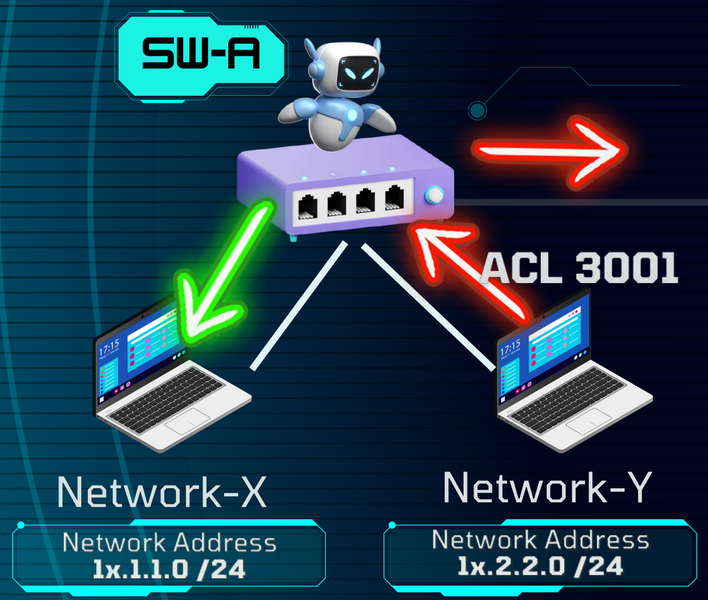
Configure a time range

```
[HP] time-range time-range-name start-timeto end-time days [from time1date1] [to time2 date2]
```

–time: ranges from 00:00 to 23:59
–date: in MM/DD/YYYY or YYYY/MM/DD format
–days: specifies the days of the week in words or digits, i.e., sun, mon, tue, wed, thu, fri, and sat (or 0-6).
- working-day for Monday through Friday.
- off-day for Saturday and Sunday.
- daily for the whole week.

–Repeat this command with the same time range name to create multiple statements for a time range.

# ACL CONFIGURATION GUIDE




## Policy 3+: Block the icmp Network Y to network Z [option + time-based ACL]

```
[SW-A] time-range blockping 00:01 to 00:02
```

Step 2.1 Create the Advanced ACL

```
[SW-A] acl number 3001
```

Step 2.2 Create the ACL rules

```
[SW-A-acl-adv-3001] rule 100 deny icmp source xx.2.2.0 0.0.0.255
destination xx.3.3.0 0.0.0.255 time-range blockping
[SW-A-acl-adv-3001] rule 200 permit ip any any
```

Step 2.3 Apply the ACL to interface

```
[SW-A] interface gigabitethernet 1/0/2
[SW-A-intG1/0/2] packet-filter 3001 inbound
```