

Network Security With RouterOS



Wilmer Almazan
winet.ca

Career

Computer Systems & Network Engineer.

Software developer

Winet Canada: Master Distributor

Mikrotik Certified Trainer

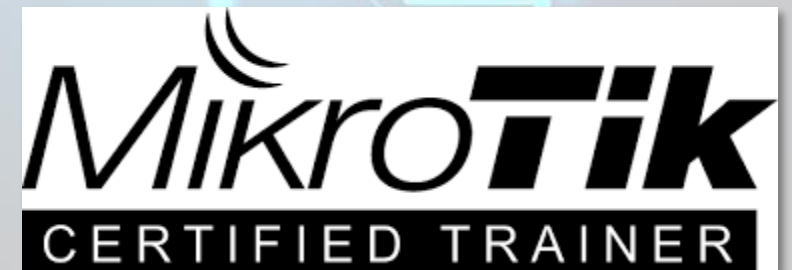
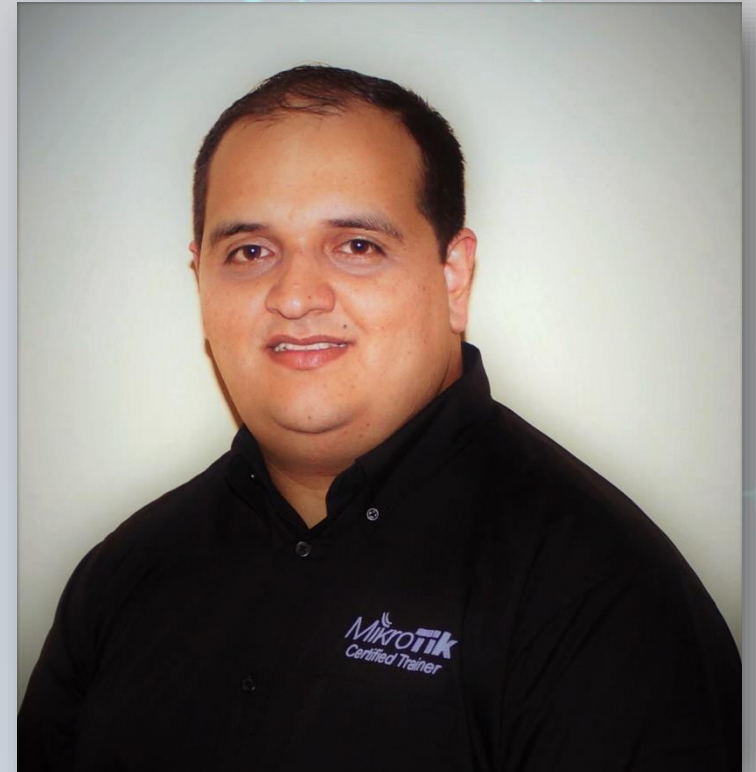
Certifications:

MTCNA – MTCRE – MTCSE – MTCTCE

MTCUME – MTCWE - Trainer

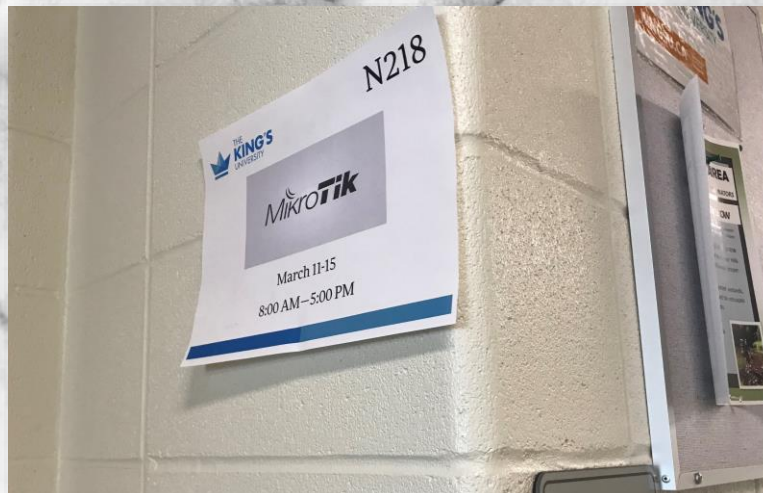
CompTIA Network+, Security+

Contact: www.winet.ca





Training Canada & Latin America





5 min

**Average amount of time it
takes for a device to be
attacked once plugged into
the Internet**



*Mikro**Tik***

**Network
Security**





Username : admin
Password : admin



CONSOLE

PWR

MikroTik

1000bps

500bps

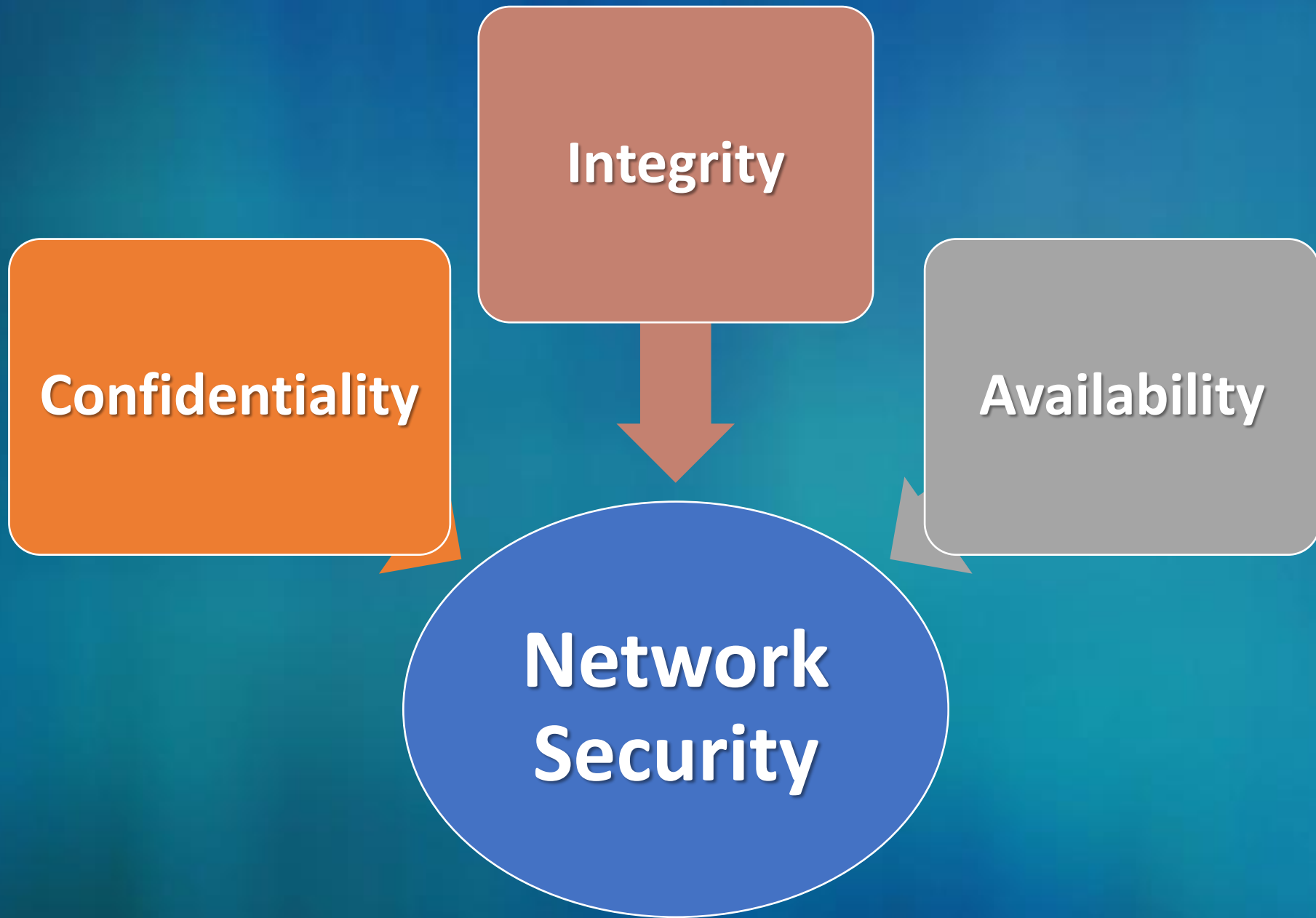
Resources

Storage: 879.0 MiB
CPU: 1 %
Memory: 15.0 GiB

Cloud Core Router
CCR1072-1G-8S

MikroTik

SMART CARD





**What Can
We Do?**

Types of Attacks

Attacks / Threats

Active

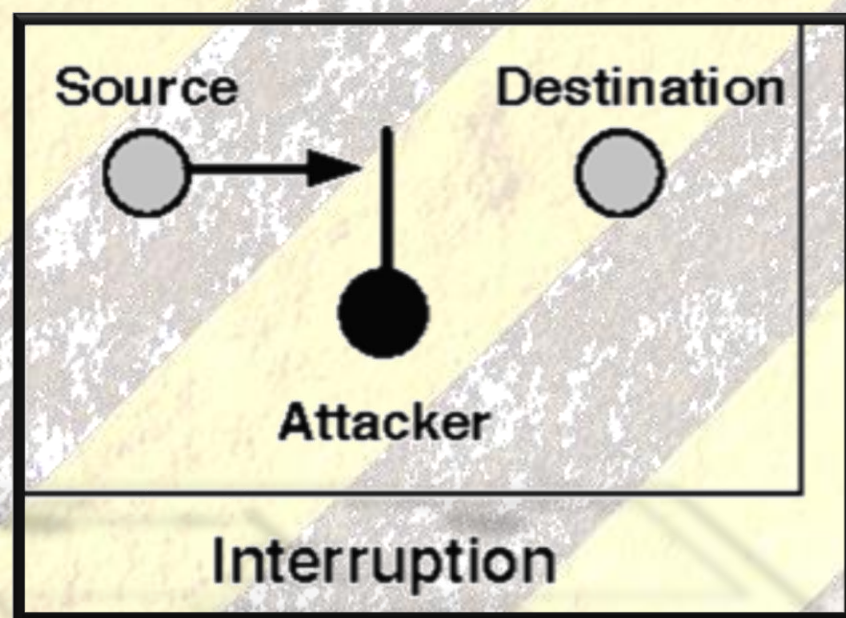
Passive

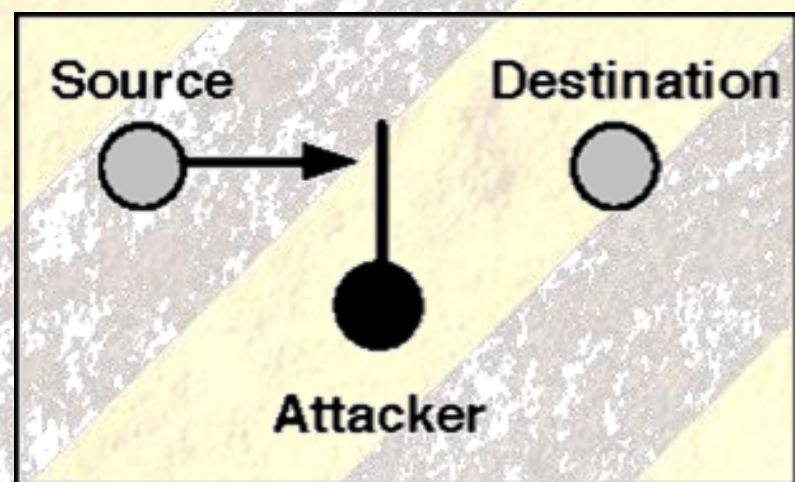
Interruption

Modification

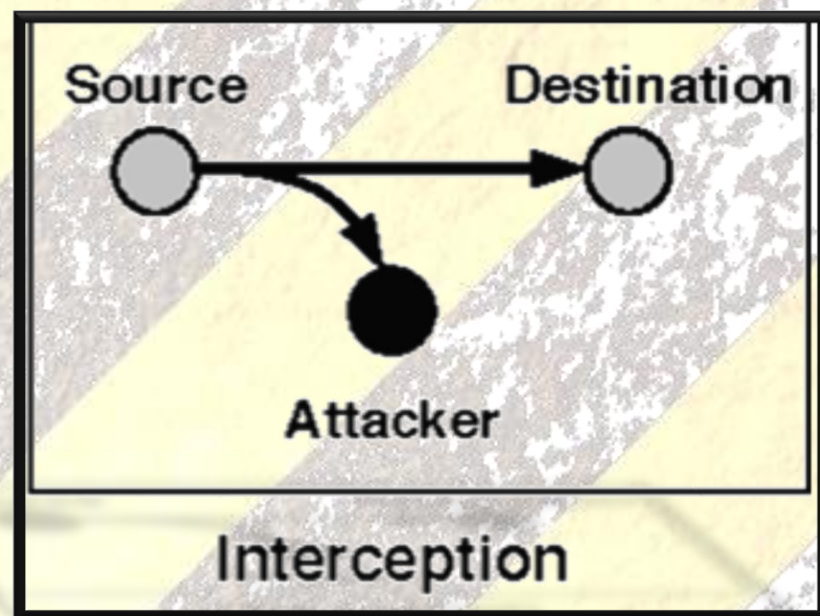
Fabrication

Interception

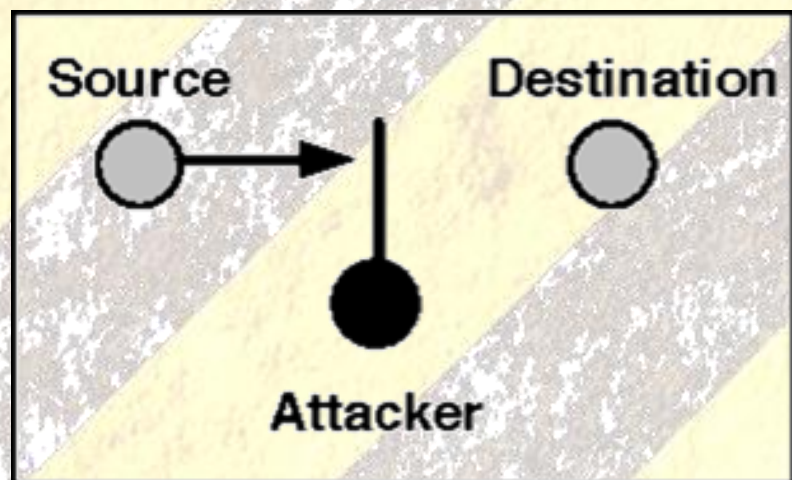




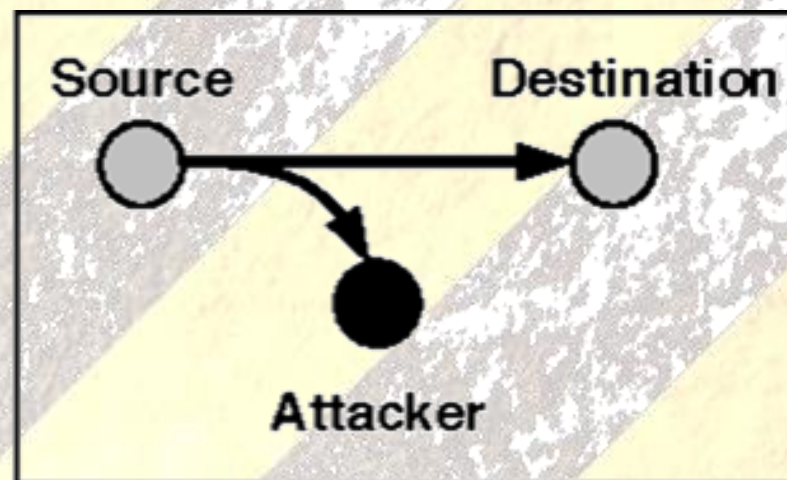
Interruption



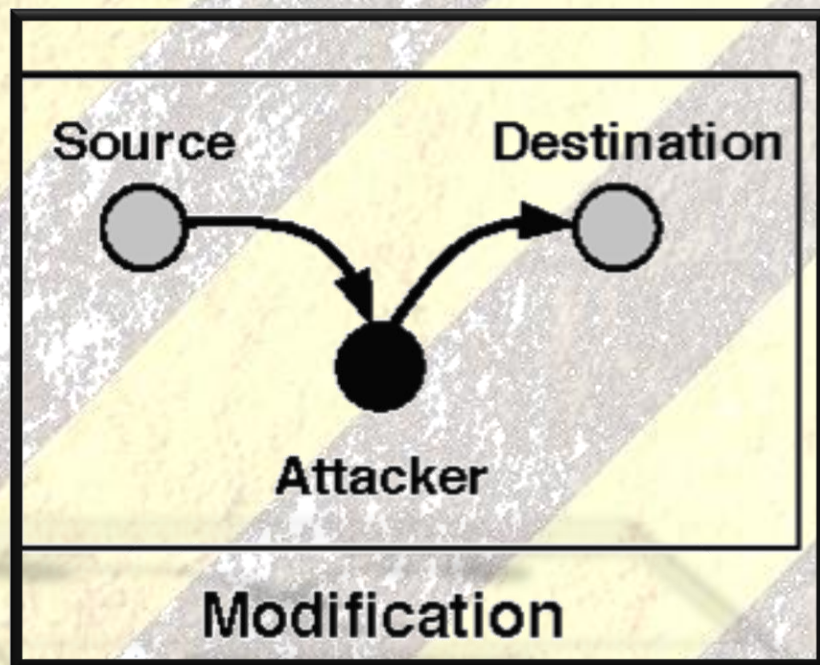
Interception

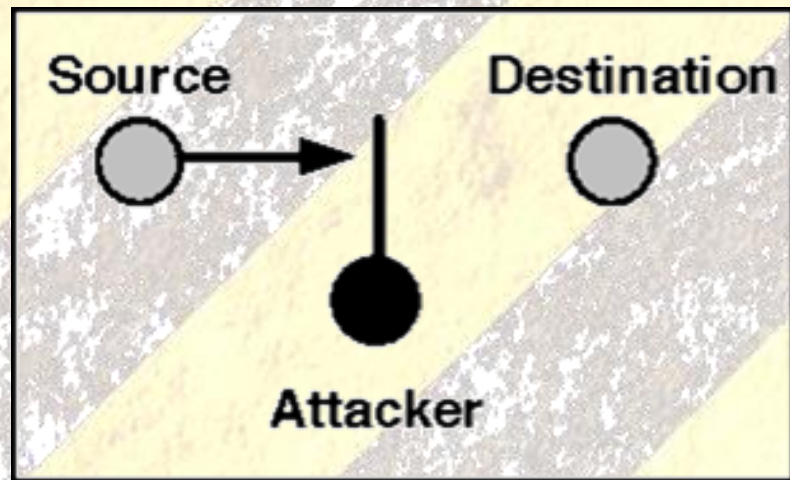


Interruption

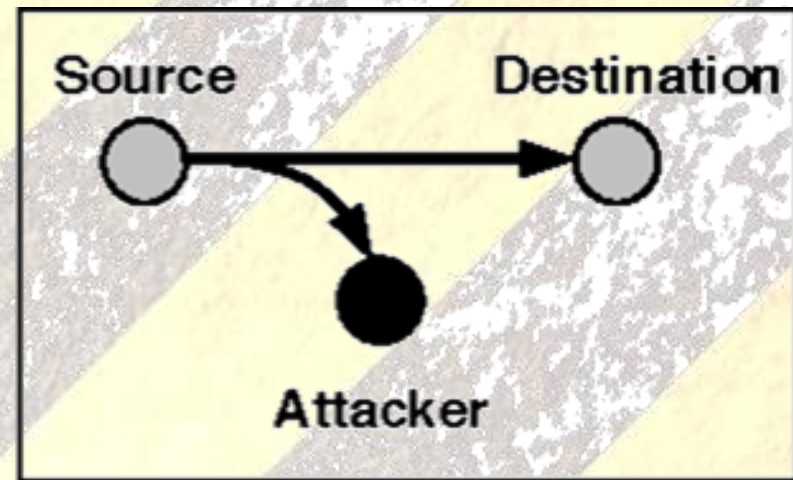


Interception

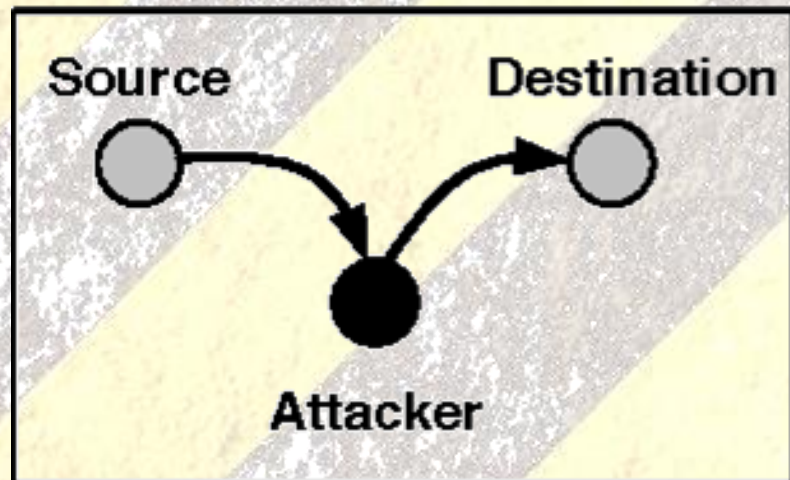




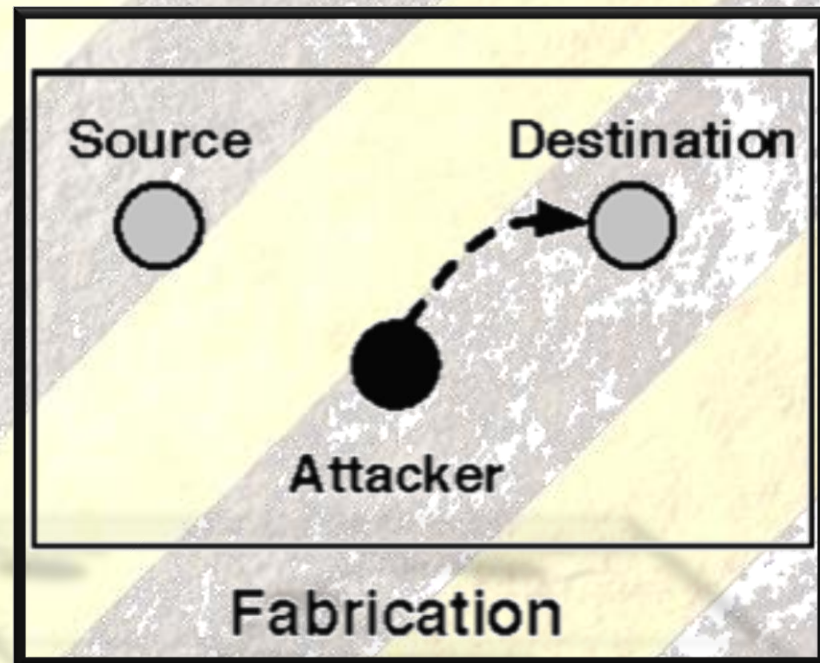
Interruption



Interception



Modification

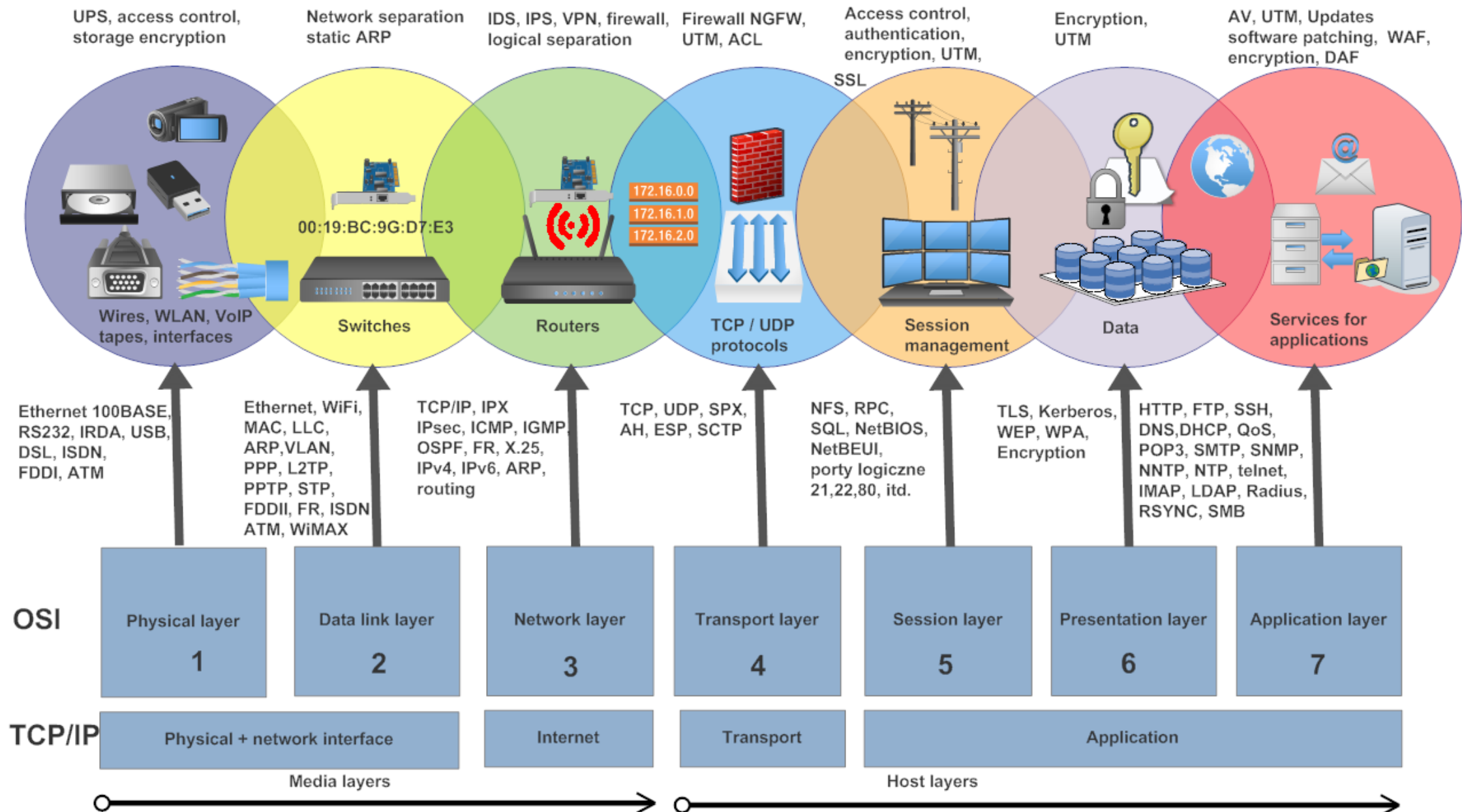


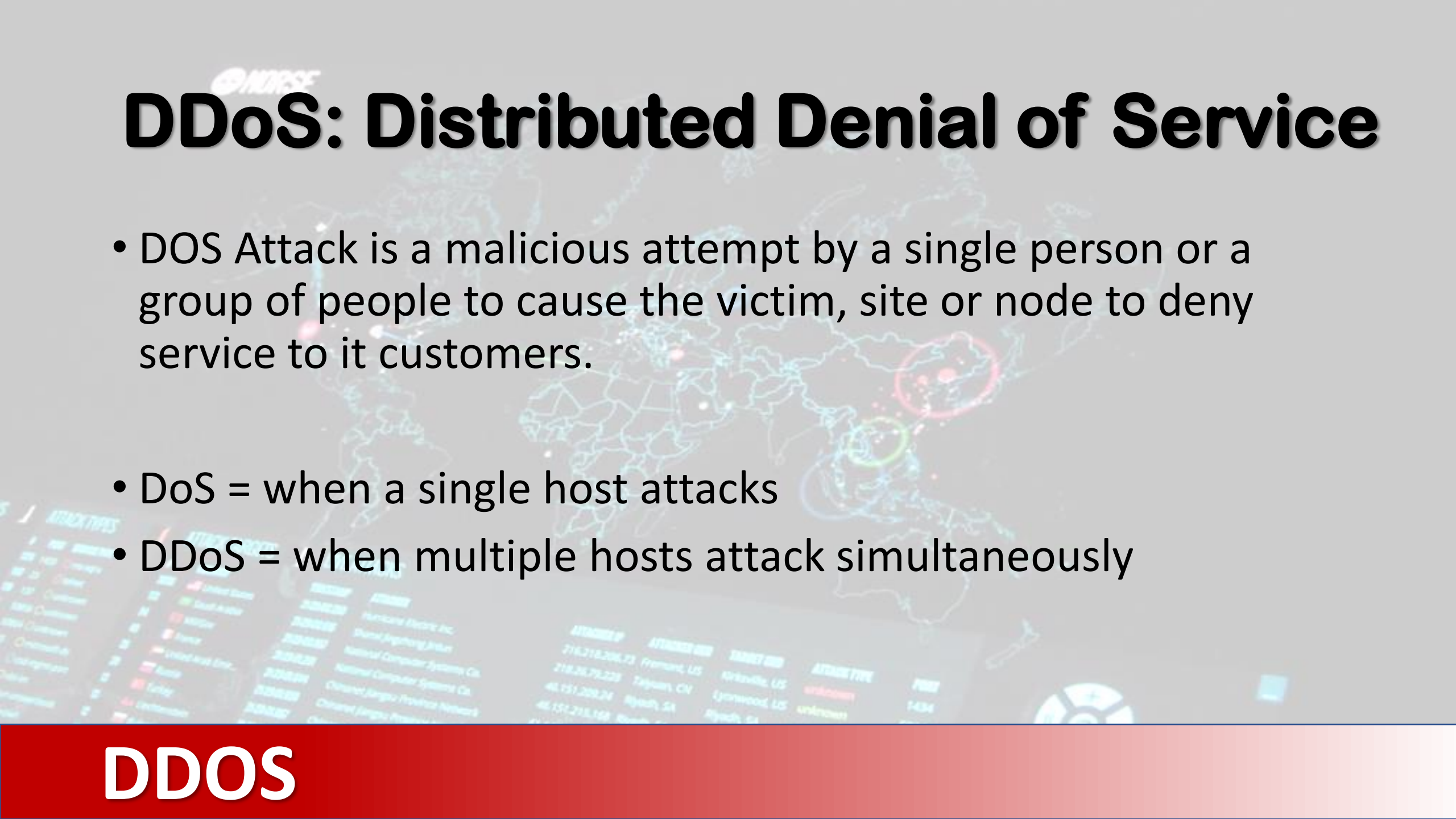
Fabrication



Threats

OSI / TCP/IP MODELS - THREATS, PROTECTION





DDoS: Distributed Denial of Service

- DOS Attack is a malicious attempt by a single person or a group of people to cause the victim, site or node to deny service to its customers.
- DoS = when a single host attacks
- DDoS = when multiple hosts attack simultaneously

DDOS

How to detect?

Are there too many connections with SYN-SENT state?

```
/ip firewall connection print
```

DDOS

How to detect?

High traffic (pps) passing through any interface?

```
/interface monitor-traffic interface_name
```

DDOS

How to detect?

CPU

100%

/system resource monitor

DDOS

How to detect?

Torch

Basic

Interface: ether1

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address

☒ Dst. Address

☐ VLAN Id

☒ Protocol

☒ Port

Filters

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Protocol: any

Port: any

VLAN Id: any

Start

Stop

Close

Find

Eth.	Protocol	Prot...	Src. Address	Src. Port	Dst. Address	Dst. Port	Tx Rate	Rx Rate	Tx Packet...	Rx Packet...
		6 (tcp)	209.68.35.17	80 (http)	10.0.1.18	55056	3.7 kbps	21.7 kbps	3	3
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	58074	0 bps	170 bps	0	0
		47	10.0.1.2		10.0.1.18		0 bps	829 bps	0	1
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	56655	165 bps	920 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	58579	165 bps	165 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	10.0.1.18	57912	165 bps	920 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	58429	173 bps	1429 bps	0	0
		6 (tcp)	64.74.98.80	80 (http)	10.0.1.18	55569	2.0 kbps	1376 bps	1	1
		6 (tcp)	10.5.8.1	53 (dns)	173.16.16.242	54018	669 bps	1893 bps	1	1
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	58417	173 bps	173 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	63366	160 bps	397 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	56255	160 bps	354 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	10.0.1.18	40995	160 bps	397 bps	0	0
		17 (...)	10.5.8.1	53 (dns)	173.16.16.242	60854	186 bps	1413 bps	0	0
		6 (tcp)	10.5.6.196	80 (http)	10.0.1.18	43415	2.0 kbps	7.7 kbps	1	1

23 items

Total Tx: 14.9 kbps

Total Rx: 46.7 kbps

Total Tx Packet: 8

Total Rx Packet: 9

Malicious Connections?

/tool torch

DDOS

DDOS : MITIGATION

- Connection Limit

```
/ip firewall filter  
add chain=input protocol=tcp connection-limit=LIMIT,32  
action=add-src-to-address-list  
address-list=blocked-addr address-list-timeout=1d
```

DDOS

TCP SYN Attack

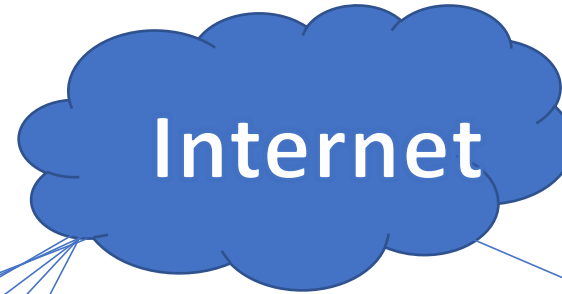
- TCP SYN flood is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.
- Essentially, with SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation.

TCP SYN

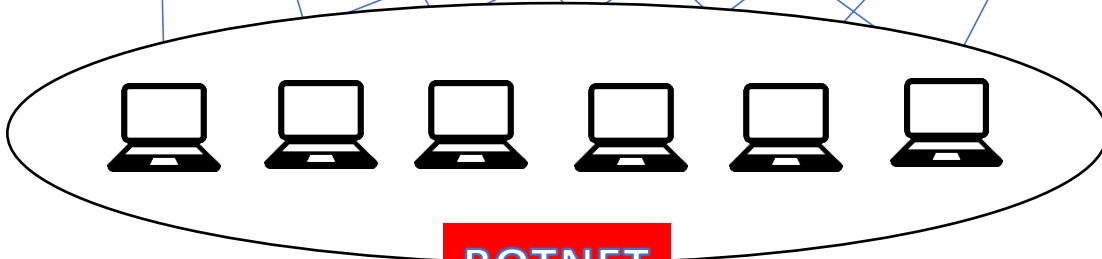
TCP SYN ATTACK



BOT MASTER



SYN FLOOD



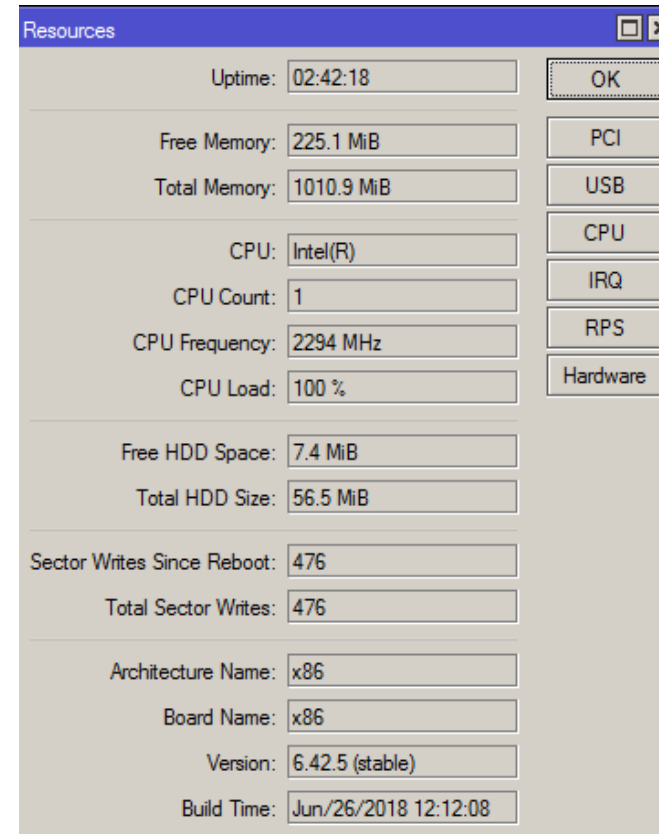
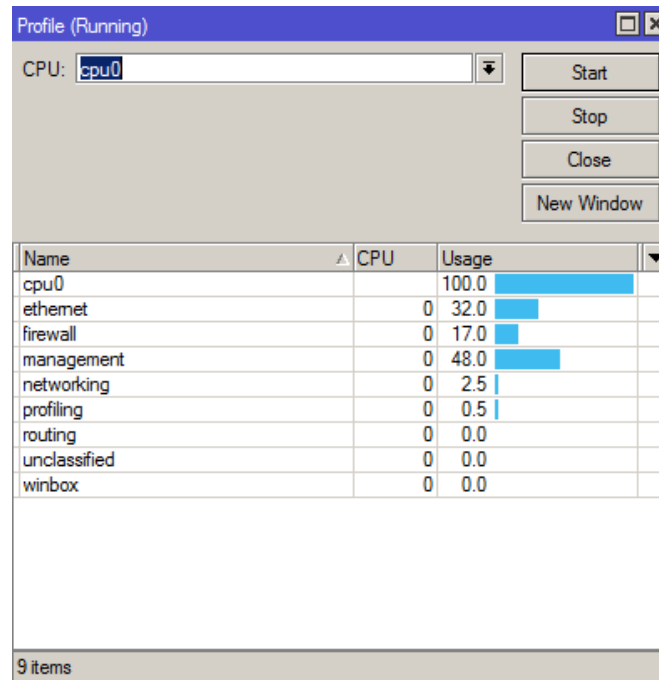
BOTNET



SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN
SYN

TCP SYN

- It's exhausting a router resource and dropped router's performance.



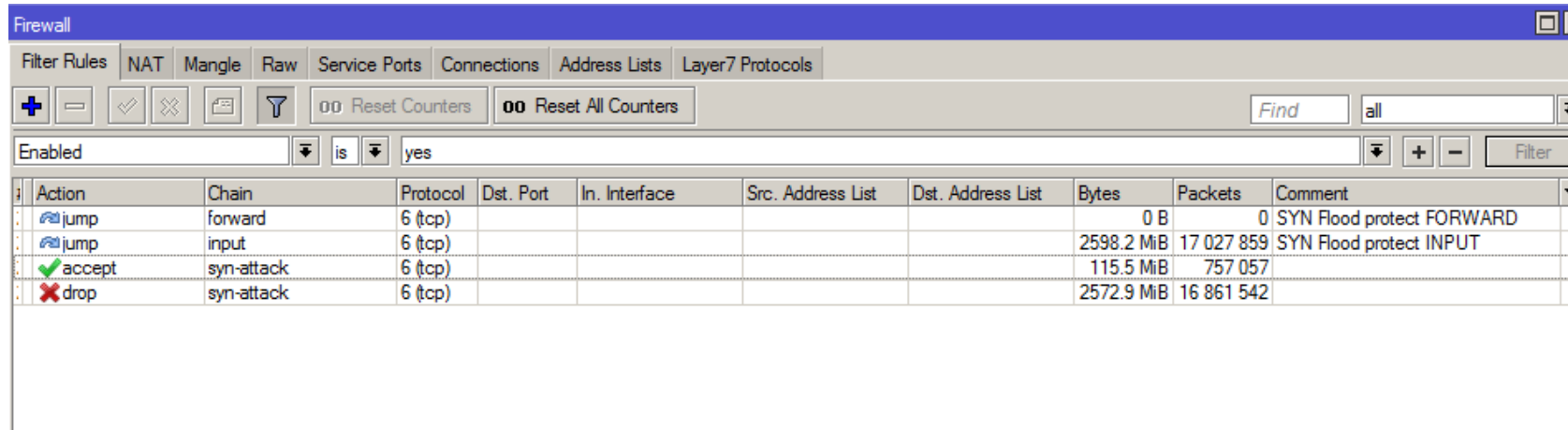
TCP SYN

Preventing TCP SYN Attack

- Rate-limiting for each new tcp connection
- Reduce syn-received timer
- And setup tcp syn-cookies

Preventing TCP SYN Attack

- Creating firewall for preventing tcp SYN flood



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. The filter is named 'Enabled' and is currently disabled. The action is set to 'yes'. The table below shows the configured rules:

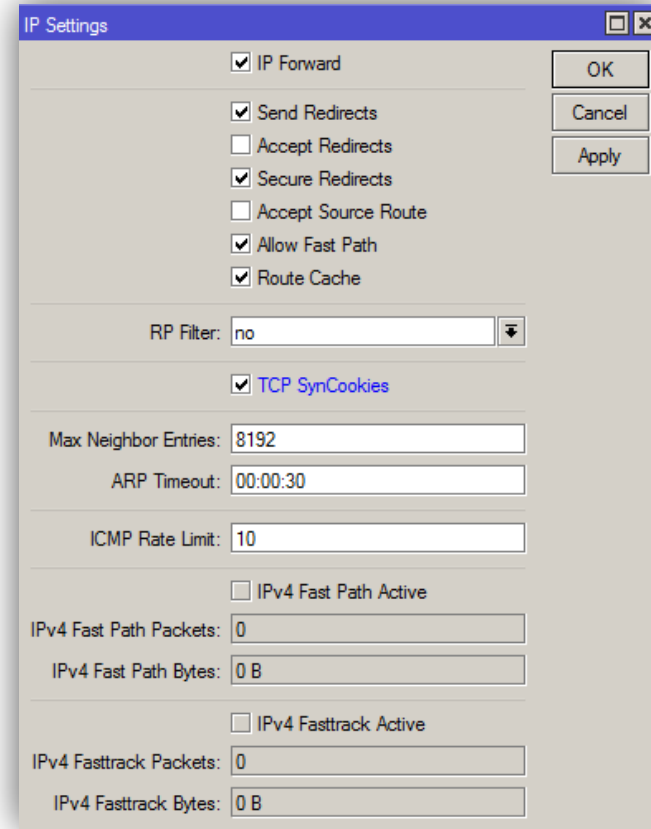
Action	Chain	Protocol	Dst. Port	In. Interface	Src. Address List	Dst. Address List	Bytes	Packets	Comment
jump	forward	6 (tcp)					0 B	0	SYN Flood protect FORWARD
jump	input	6 (tcp)					2598.2 MiB	17 027 859	SYN Flood protect INPUT
accept	syn-attack	6 (tcp)					115.5 MiB	757 057	
drop	syn-attack	6 (tcp)					2572.9 MiB	16 861 542	

```
/ip firewall filter
add action=jump chain=forward comment="SYN Flood protect FORWARD" connection-state=new jump-
target=syn-attack protocol=tcp tcp-flags=syn
add action=jump chain=input comment="SYN Flood protect INPUT" connection-state=new jump-
target=syn-attack protocol=tcp tcp-flags=syn
add action=accept chain=syn-attack connection-state=new limit=400,5:packet protocol=tcp tcp- flags=syn
add action=drop chain=syn-attack connection-state=new protocol=tcp tcp-flags=syn
```

TCP SYN

Preventing TCP SYN Attack

- IP > Settings and enable “TCP SynCookies”



```
/ip settings set tcp-syncookies=yes
```

TCP SYN

Raw Table Syn-flood Attack

```
/ip firewall raw  
chain=input action=drop tcp-flags=syn protocol=tcp
```

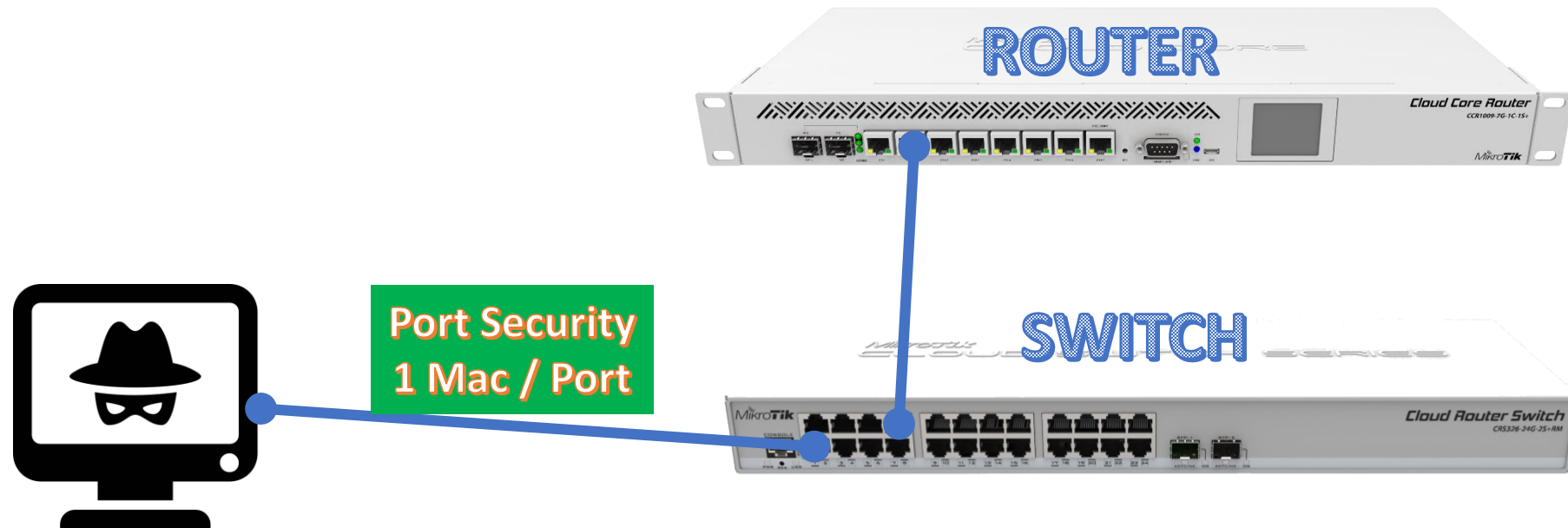
TCP SYN

- Target: DHCP servers
- Objective:
 - Exhaust all available IP addresses that can be allocated by the DHCP server.
- Under this attack, legitimate network users can be denied service.

DHCP Starvation

Preventing DHCP Starvation

- Restrict the number of MAC addresses on the port of the switch



DHCP Starvation

How? Port Security on CRS3xxx

Create a rule to allow the given MAC address and drop all other traffic on **ether1** (for ingress traffic):

```
/interface ethernet switch rule
```

```
add ports=ether1 src-mac-address= AA:BB:CC:DD:EE:FF /FF:FF:FF:FF:FF:FF switch=switch1
```

```
add new-dst-ports="" ports=ether1 switch=switch1
```

DHCP Starvation

How? Port Security on CRS3xxx

- Switch all required ports together
- Disable MAC learning
- Disable unknown unicast flooding on ether1

```
/interface bridge add name=bridge1
```

```
/interface bridge port
```

```
add bridge=bridge1 interface=ether1 hw=yes learn=no unknown-unicast-flood=no
```

```
add bridge=bridge1 interface=ether2 hw=yes
```

DHCP Starvation

Add a static hosts entry for 64:D1:54:81:EF:8E (for egress traffic):

```
/interface bridge host  
add bridge=bridge1 interface=ether1 mac-address=AA:BB:CC:DD:EE:FF
```

DHCP Starvation

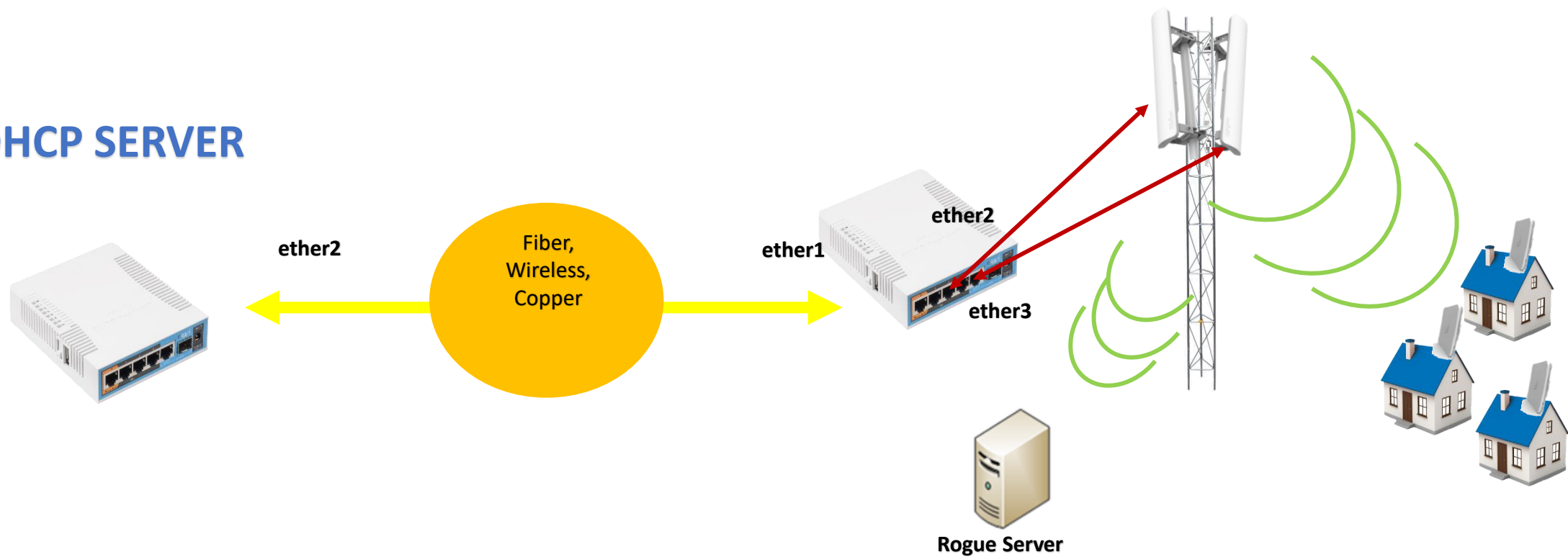
DHCP server on a network which is not under the administrative control of the network staff



DHCP Rogue

OUR TOWER (WISP, HOTSPOT, ETC)

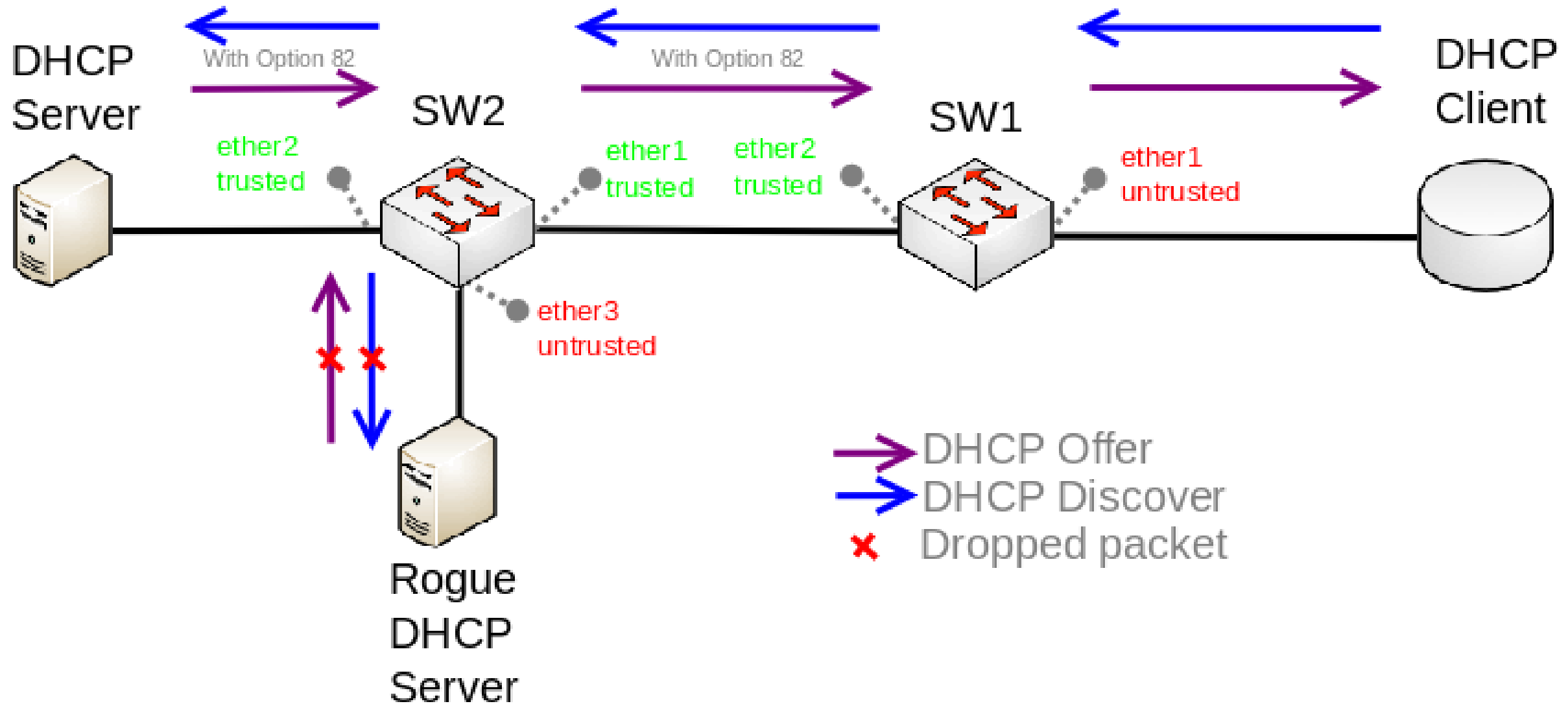
DHCP SERVER



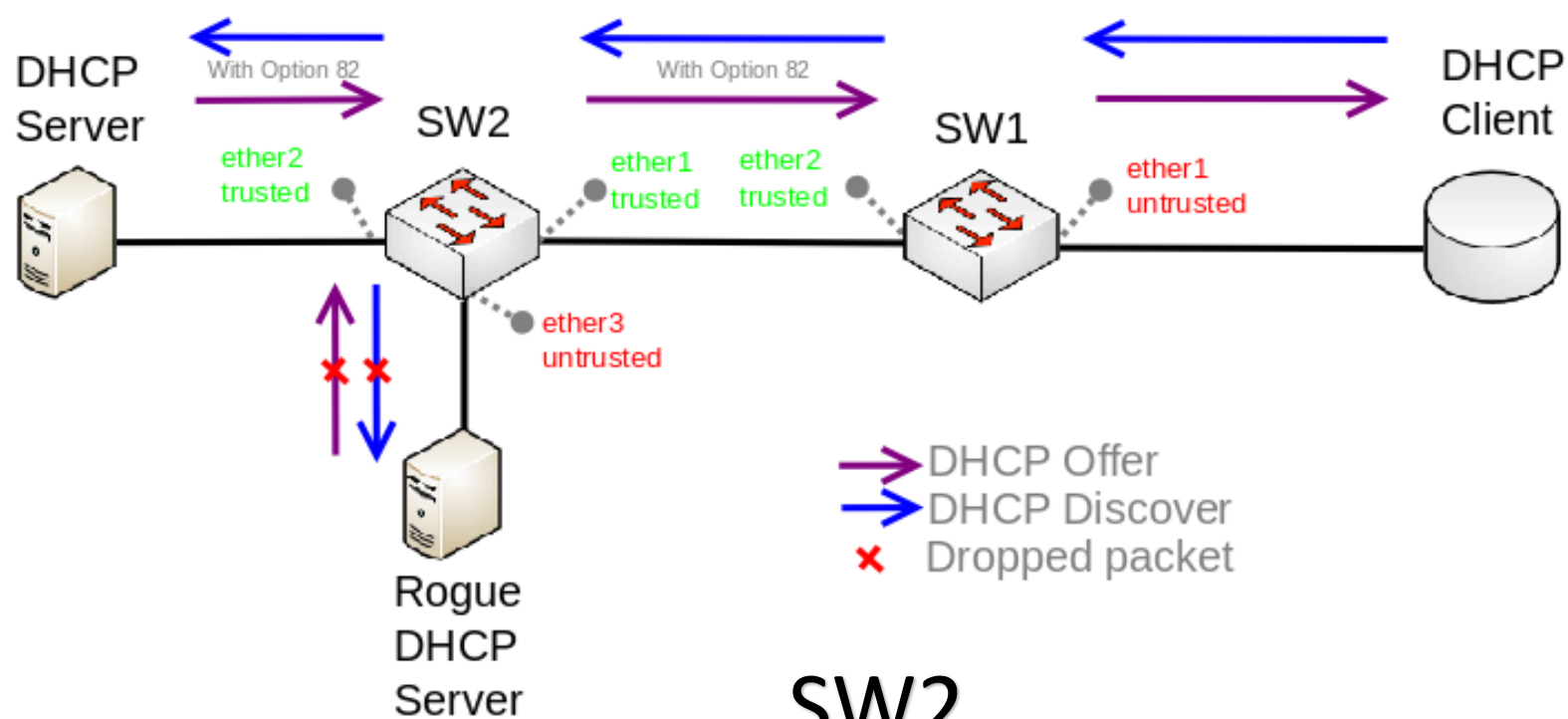
DHCP Rogue

Solution: DHCP Snooping (6.43+)

- The DHCP Snooping is a Layer2 security feature, that limits unauthorized DHCP servers from providing a malicious information to users.
- **How?**
- In RouterOS you can specify which bridge ports are trusted (where known DHCP server resides and DHCP messages should be forwarded) and which are untrusted (usually used for access ports, received DHCP server messages will be dropped).



DHCP Rogue



SW1

```
/interface bridge
add name=bridge
/interface bridge port
add bridge=bridge interface=ether1
add bridge=bridge interface=ether2 trusted=yes
/interface bridge
set [find where name="bridge"] dhcp-snooping=yes
add-dhcp-option82=yes
```

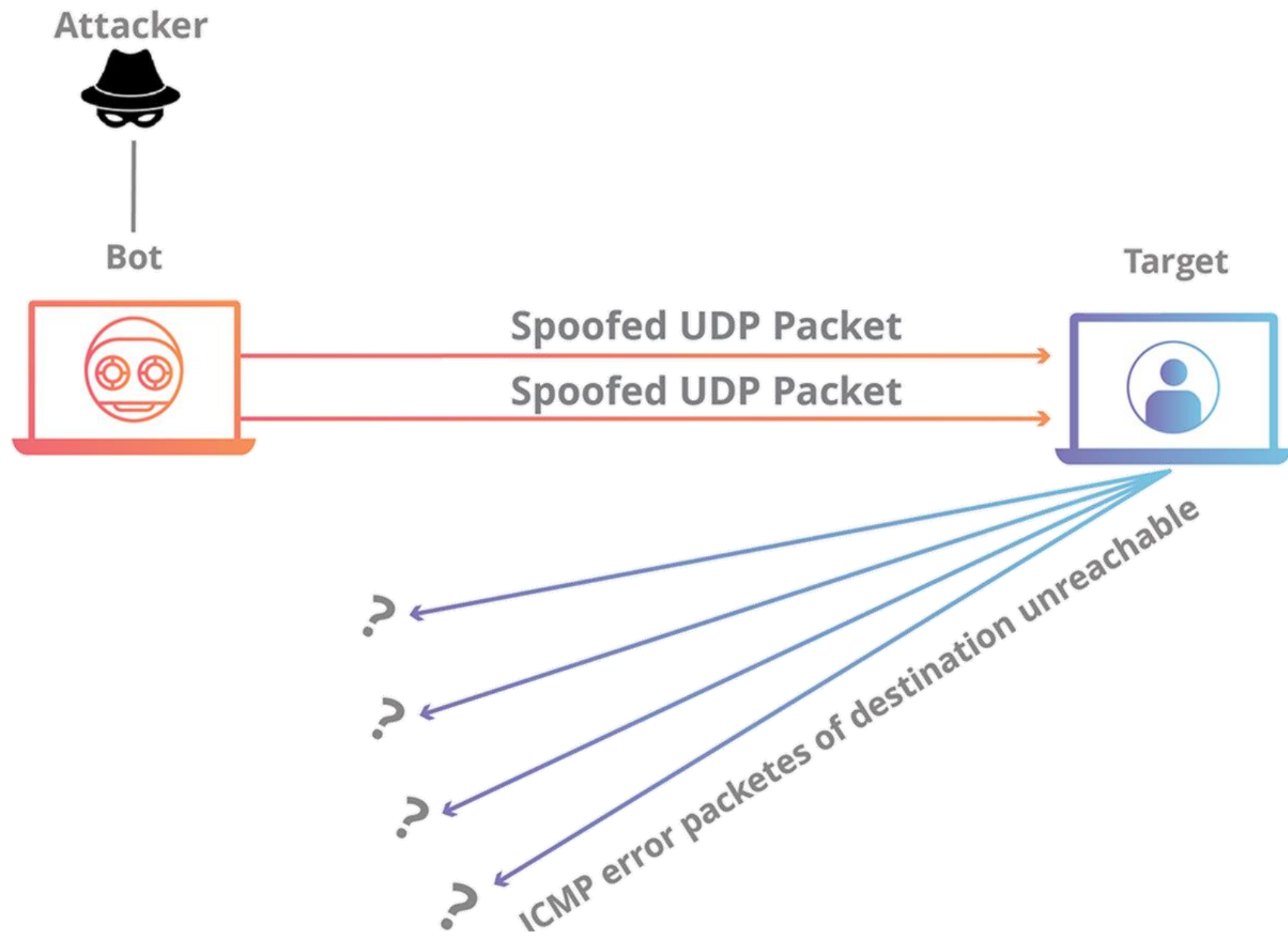
SW2

```
/interface bridge
add name=bridge
/interface bridge port
add bridge=bridge interface=ether1 trusted=yes
add bridge=bridge interface=ether2 trusted=yes
add bridge=bridge interface=ether3
/interface bridge
set [find where name="bridge"] dhcp-snooping=yes
add-dhcp-option82=yes
```

DHCP Rogue

UDP Flood

- UDP flood is a type of Denial of Service (DoS) attack in which the attacker overwhelms random ports on the targeted host with IP packets containing UDP datagrams.



UDP Flood

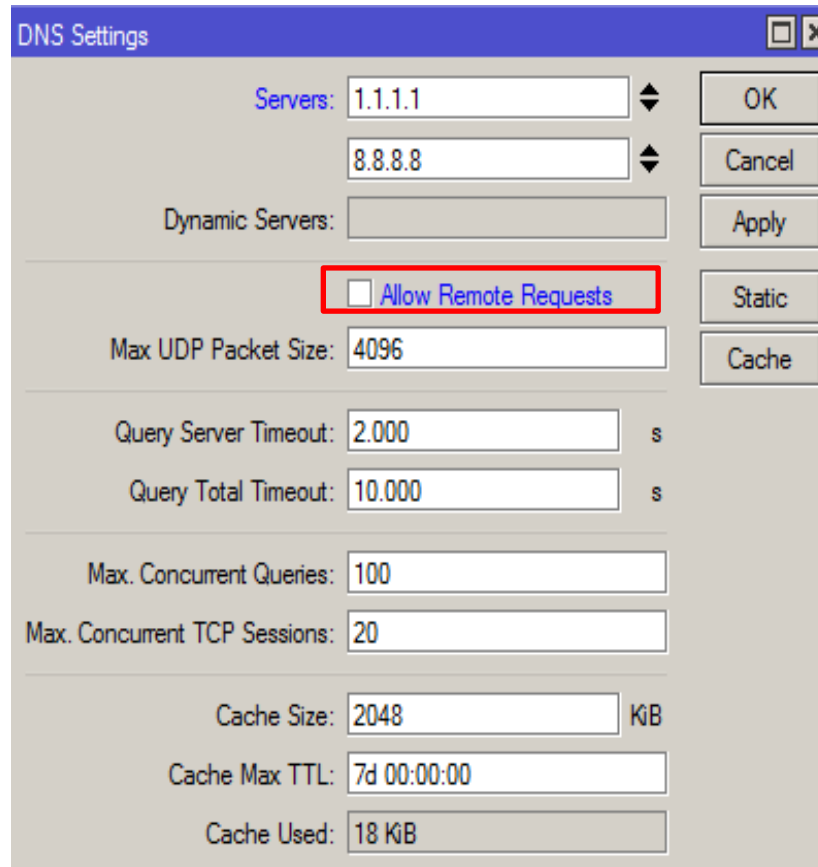
How to mitigate UDP Flood Attack

- Disable DNS forwarder on MikroTik if not required.
- If “IP -> DNS” – *Allow remote request* is enabled, make sure appropriate filter rule is set to prevent incoming DNS attacks.
- Rate-limiting for each new udp connection.
- Block UDP Traffic from outside

UDP Flood

- Disable

“Allow Remote Requests on router” if not required

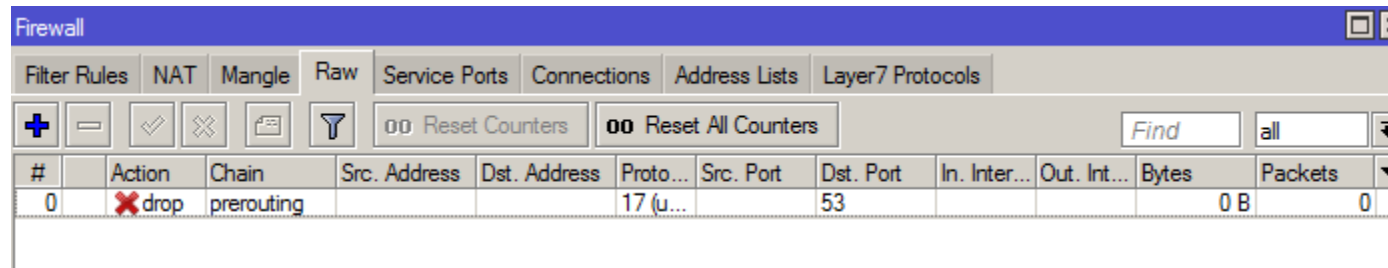


The image shows a 'DNS Settings' window with various configuration options. The 'Servers' field contains '1.1.1.1' and '8.8.8.8'. The 'Dynamic Servers' field is empty. The 'Allow Remote Requests' checkbox is unchecked and highlighted with a red rectangle. The 'Max UDP Packet Size' is set to 4096. The 'Query Server Timeout' is 2.000 s and the 'Query Total Timeout' is 10.000 s. The 'Max. Concurrent Queries' is 100 and the 'Max. Concurrent TCP Sessions' is 20. The 'Cache Size' is 2048 KiB, the 'Cache Max TTL' is 7d 00:00:00, and the 'Cache Used' is 18 KiB. Buttons for 'OK', 'Cancel', 'Apply', 'Static', and 'Cache' are on the right.

Setting	Value
Servers	1.1.1.1, 8.8.8.8
Dynamic Servers	
Allow Remote Requests	☐
Max UDP Packet Size	4096
Query Server Timeout	2.000 s
Query Total Timeout	10.000 s
Max. Concurrent Queries	100
Max. Concurrent TCP Sessions	20
Cache Size	2048 KiB
Cache Max TTL	7d 00:00:00
Cache Used	18 KiB

UDP Flood

- Block dns request “udp/53” traffic from outside



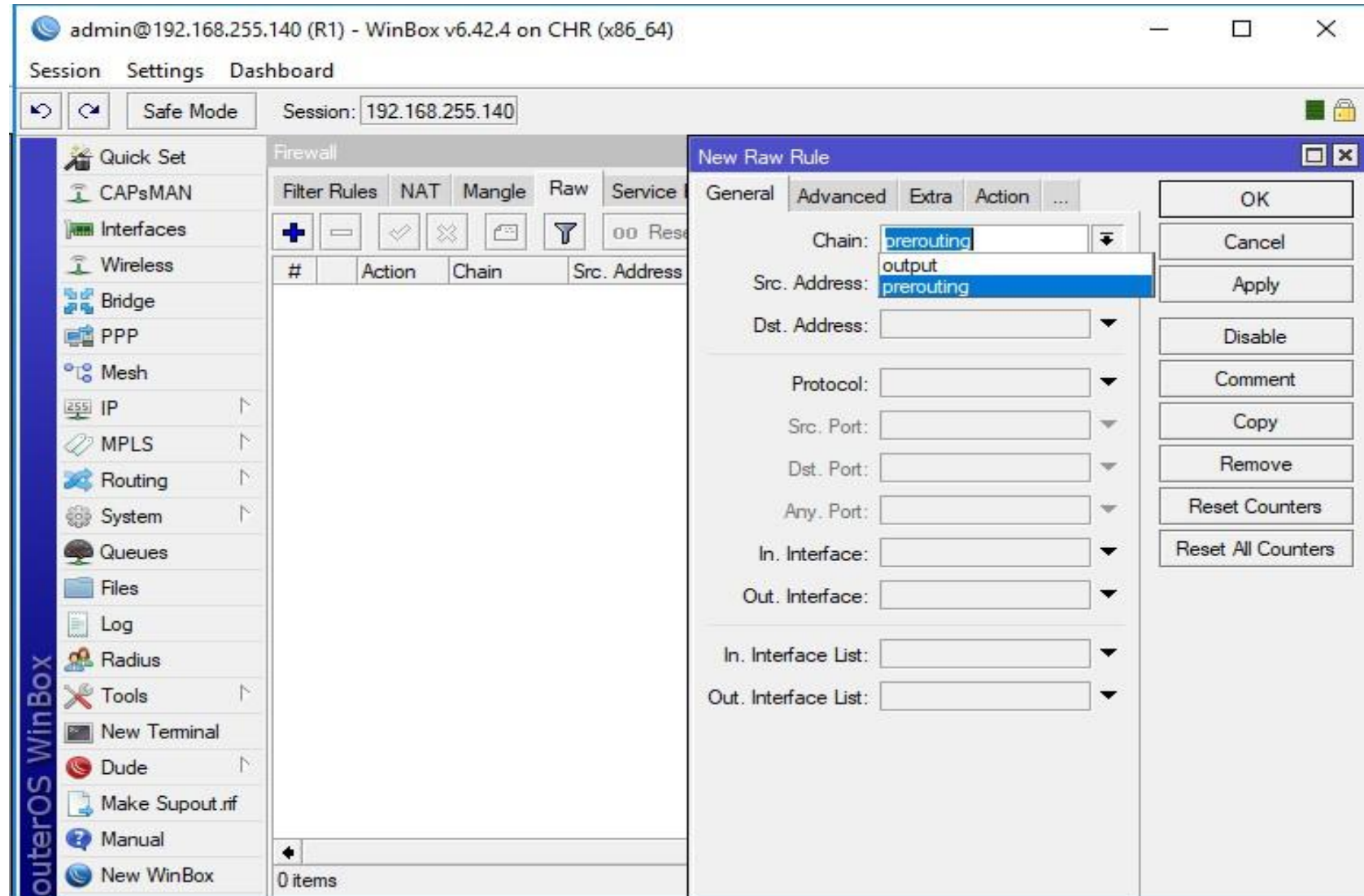
```
/interface list add name=WAN
```

```
/interface list member add interface=ether3-internet list=WAN
```

```
/ip firewall raw add action=drop chain=prerouting dst-port=53 in-interface-list=WAN  
protocol=udp
```

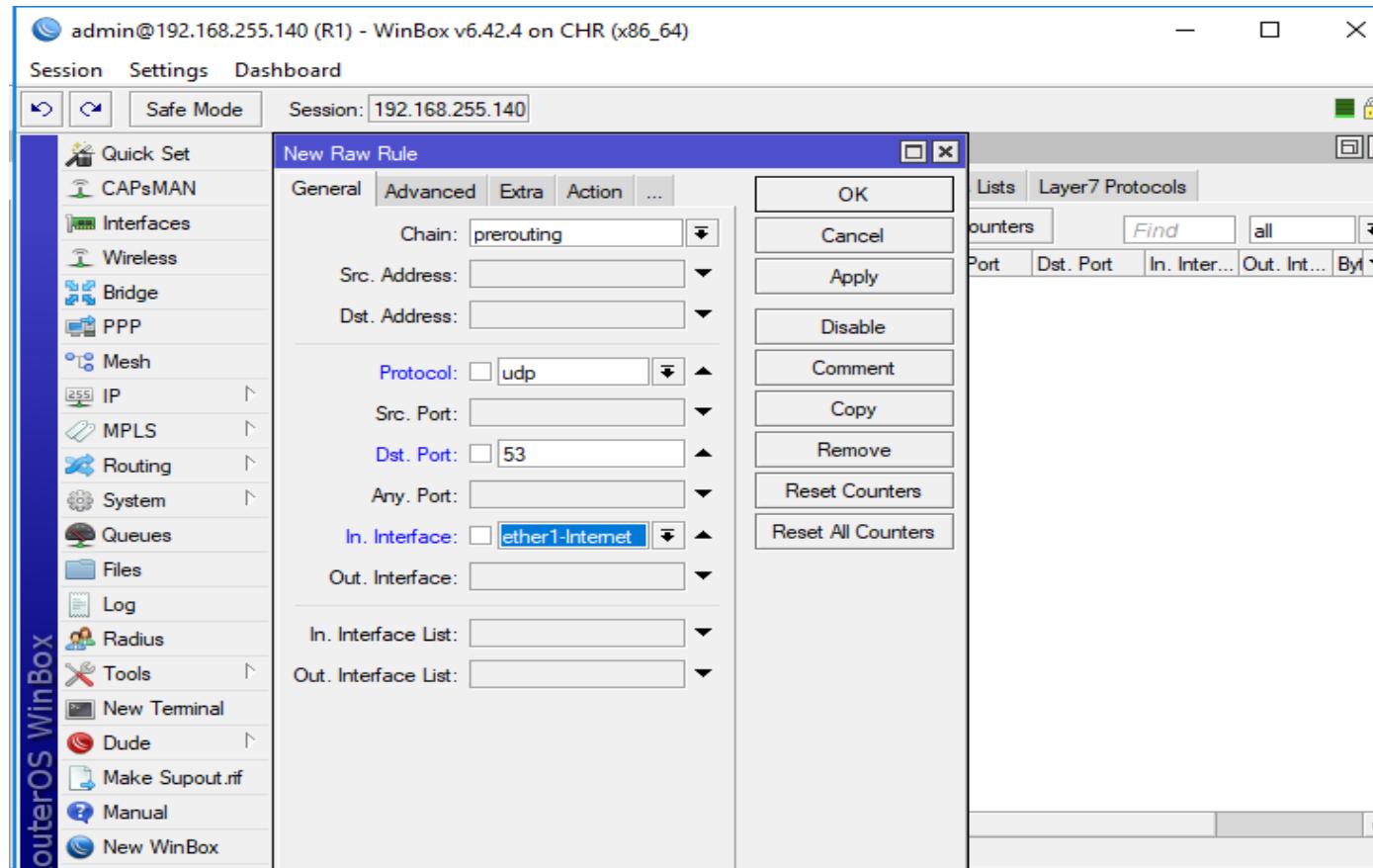
UDP Flood

Raw table



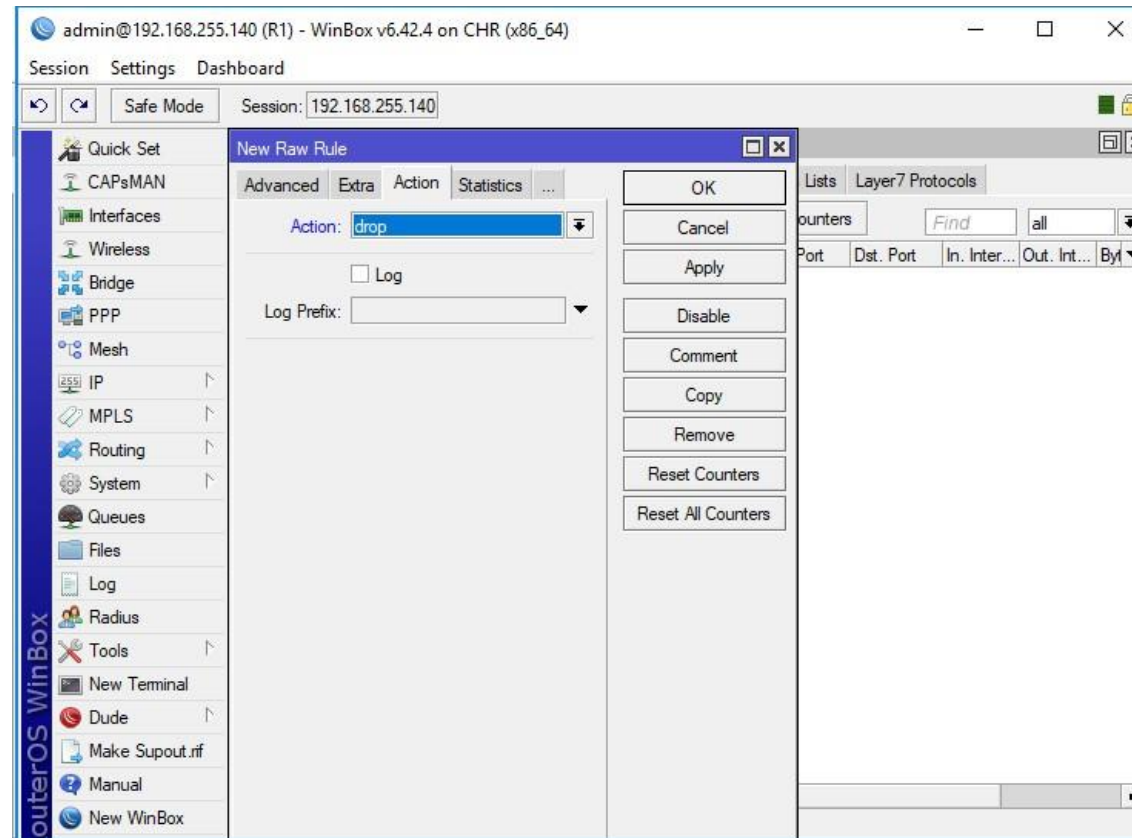
UDP Flood

Raw table. Drop packets



UDP Flood

Raw table. Drop packets



UDP Flood

Brute Force Attack

- A Brute Force Attack is the simplest method to gain access to a site or server (or anything that is password protected). It tries various combinations of usernames and passwords again and again until it gets in.
- This repetitive action is like an army attacking a fort.

Brute Force

Prevention: Brute Force Attack

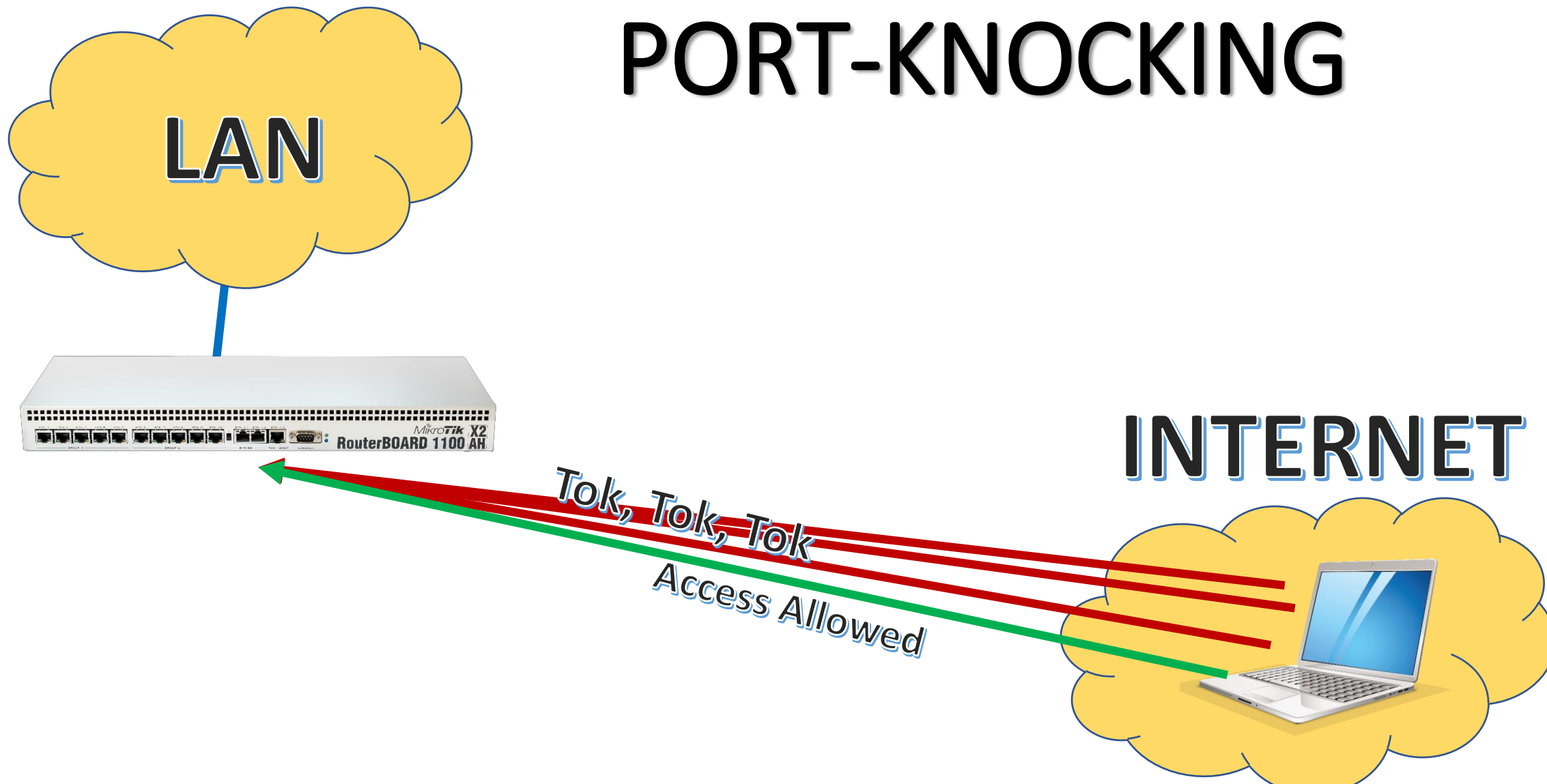
- Limit Failed Login Attempts and lock out users with a maximum number of failed attempts.
- Don't use a default ports.
- Limit Logins to a Specified IP Address or Range
- Use complex password and change it periodically

Brute Force

- Port knocking is a method that enables access to the router only after receiving a sequenced connection attempts on a set of “pre-specified” open ports.
- Once the correct sequence of the connection attempts is received, the RouterOS dynamically adds a host source IP to the allowed address list and You will be able to connect your router.

Port Knocking

PORT-KNOCKING



Port Knocking

/ip firewall filter

```
add action=add-src-to-address-list address-list="stage1" address-list-timeout=1m  
chain=input dst-port=8000 protocol=tcp
```

```
add action=add-src-to-address-list address-list="stage2" address-list-timeout=1m  
chain=input dst-port=7000 protocol=tcp src-address-list="stage1"
```

```
add action=add-src-to-address-list address-list="allowed" address-list-timeout=30m  
chain=input dst-port=6000 protocol=tcp src-address-list="stage2"
```

```
add chain=input src-address-list=allowed action=accept  
add action=drop chain=input
```

Questions?