

MAC Attacks



Dale Meredith

MCT | CEI | CEH | MCSA | MCSE
Cyber Security Expert

dalemeredith.com | [Twitter: @dalemeredith](https://twitter.com/dalemeredith) | [Linkedin: dalemeredith](https://www.linkedin.com/in/dalemeredith)



Sometimes you need to take what is rightfully yours. This is why I see the Hamburglar as the hero.

Frank Underwood



**Continually learning is
the key to success!**

What's a MAC?

Media Access Control

Unique ID for each
port on a device

12-Digits

First 6 are the “prefix”

00:13:10 /

00:25:9C / 68:7f:74

= Linksys



```
Description . . . . . : Hyper-V Virtual Et
Physical Address . . . . . : 08-60-6E-75-5C-6D
DHCP Enabled . . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::90a0:f828:93
IPv4 Address . . . . . : 10.10.10.35(Prefer
Subnet Mask . . . . . : 255.255.255.0
```

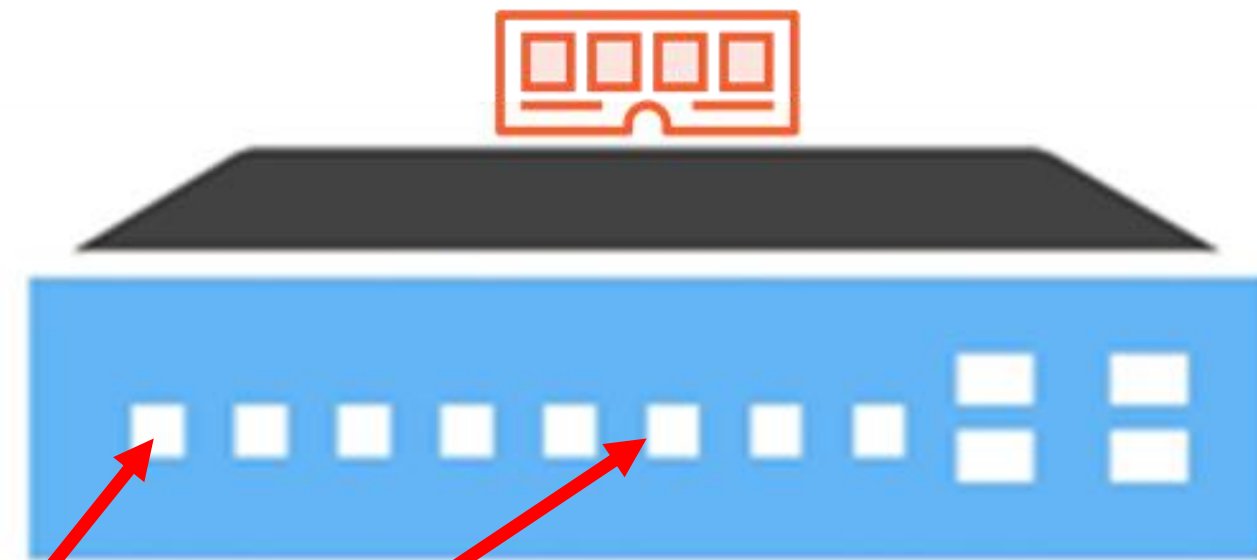


MAC Spelled Backwards = CAM

MAC Spelled Backwards = CAM

D: AA:BB:CC:DD:EE:FF

S: ZZ:YY:XX:VV:UU:TT



- AA:BB:CC:DD:EE:FF
- ZZ:YY:XX:VV:UU:TT
- _____

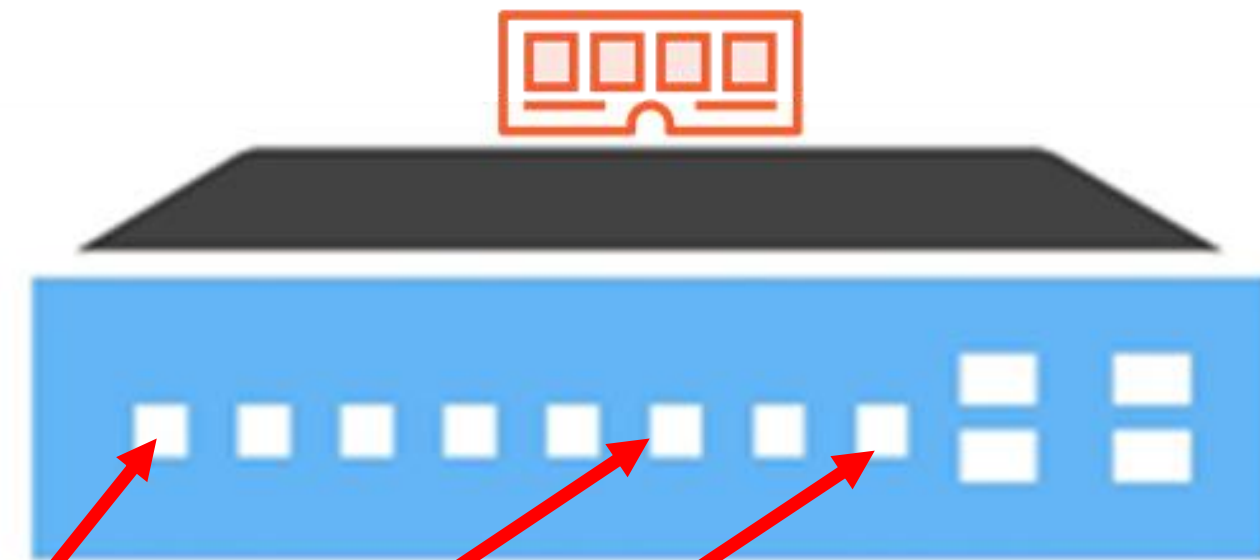
MAC Spelled Backwards = CAM

D: 12:34:56:78:90:A1

S: ZZ:YY:XX:VV:UU:TT

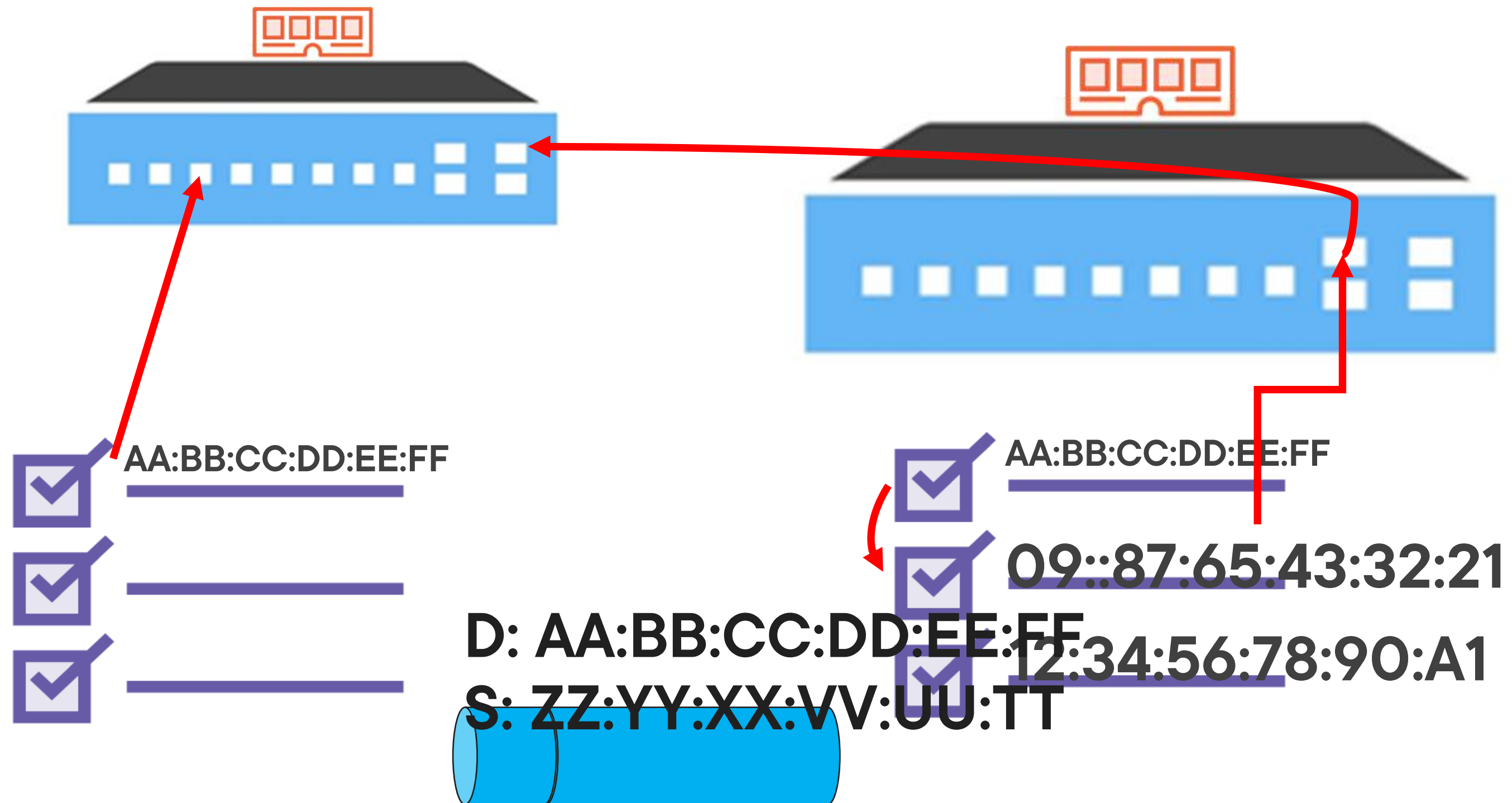


- AA:BB:CC:DD:EE:FF
- ZZ:YY:XX:VV:UU:TT
- 12:34:56:78:90:A1



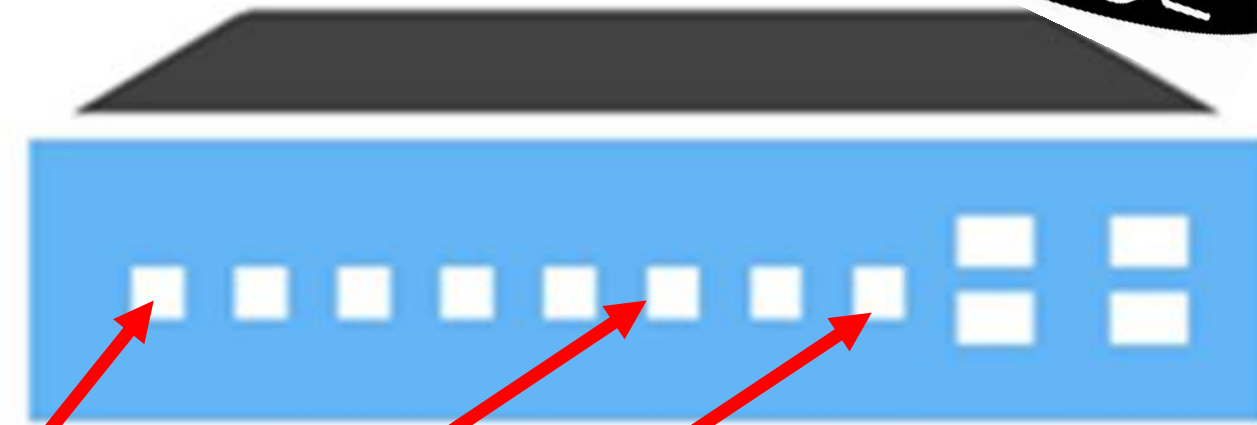
**FF:FF:FF:FF:FF:FF:
FF**

MAC Spelled Backwards = CAM



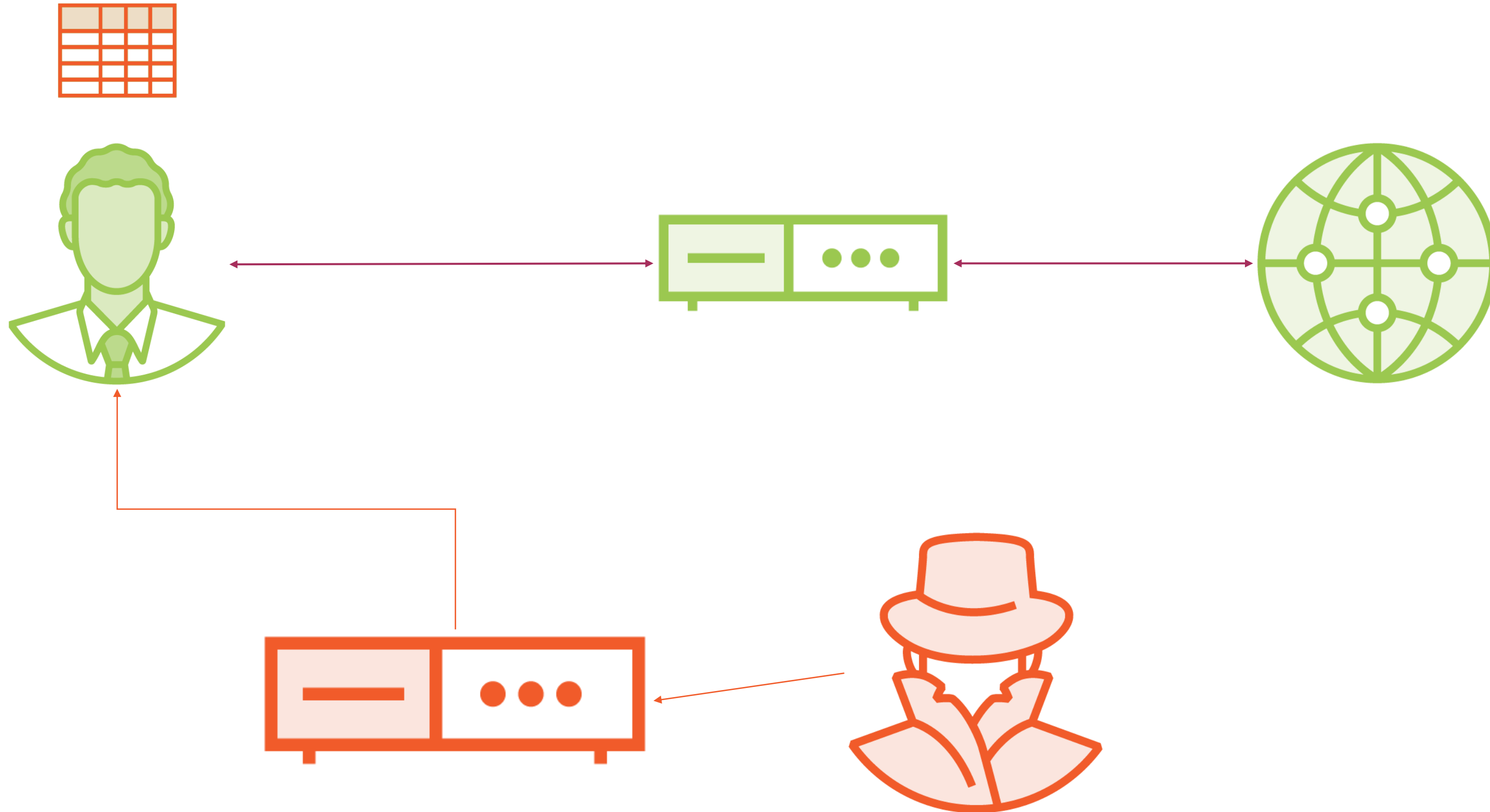
Flooding

I've Eaten Too Much, I'm Full



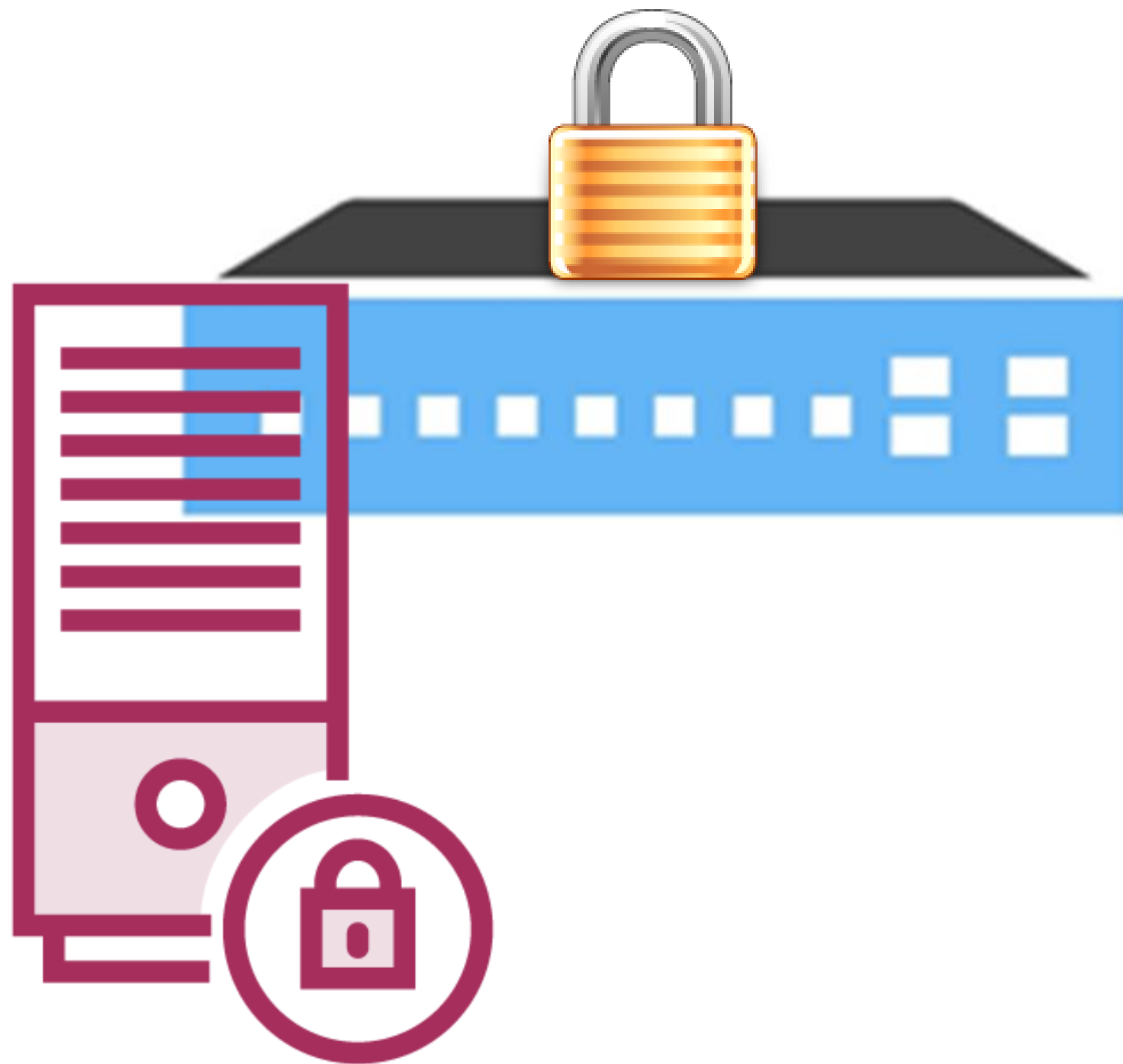
- AA:BB:CC:DD:EE:FF
- ZZ:YY:XX:VV:UU.TT
- 12:34:56:78:90:A1

IRDP Spoofing



Countermeasures

Repeat, Rinse, Repeat



- ❑ **Port Security?**
Secure MAC => Secure Port
- ❑ **Use AAA Server**

Summary



- ❑ **What's a MAC?**
- ❑ **MAC Spelled Backwards = CAM**
- ❑ **Flooding**
- ❑ **Countermeasures**

Stalking is such a strong word, I prefer intense research of an individual.

-Unknown

What We'll Learn

**Explore sniffing
concepts**

DHCP Assaults

Big-MAC Attack

ARP Poisoning

DNS Poisoning

Countermeasures



Speaking of Sniffing

Let's get sniffing!

Old Method, Knew Technology

Wiretapping



Unofficial

Official

Direct line

Radio

Types of Tapping

Active

Man-in-the-middle

Monitor or record traffic

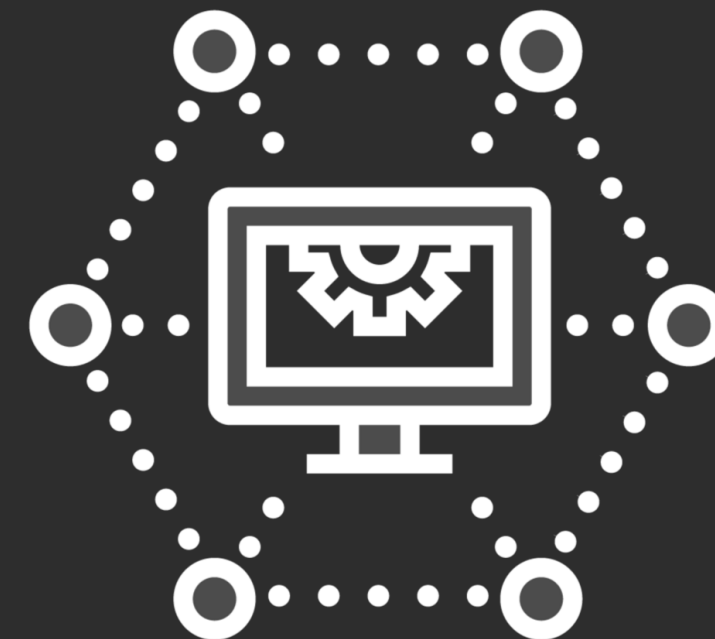
Change data

Passive

Eavesdropping or snooping

Monitor or record traffic

Doesn't change data





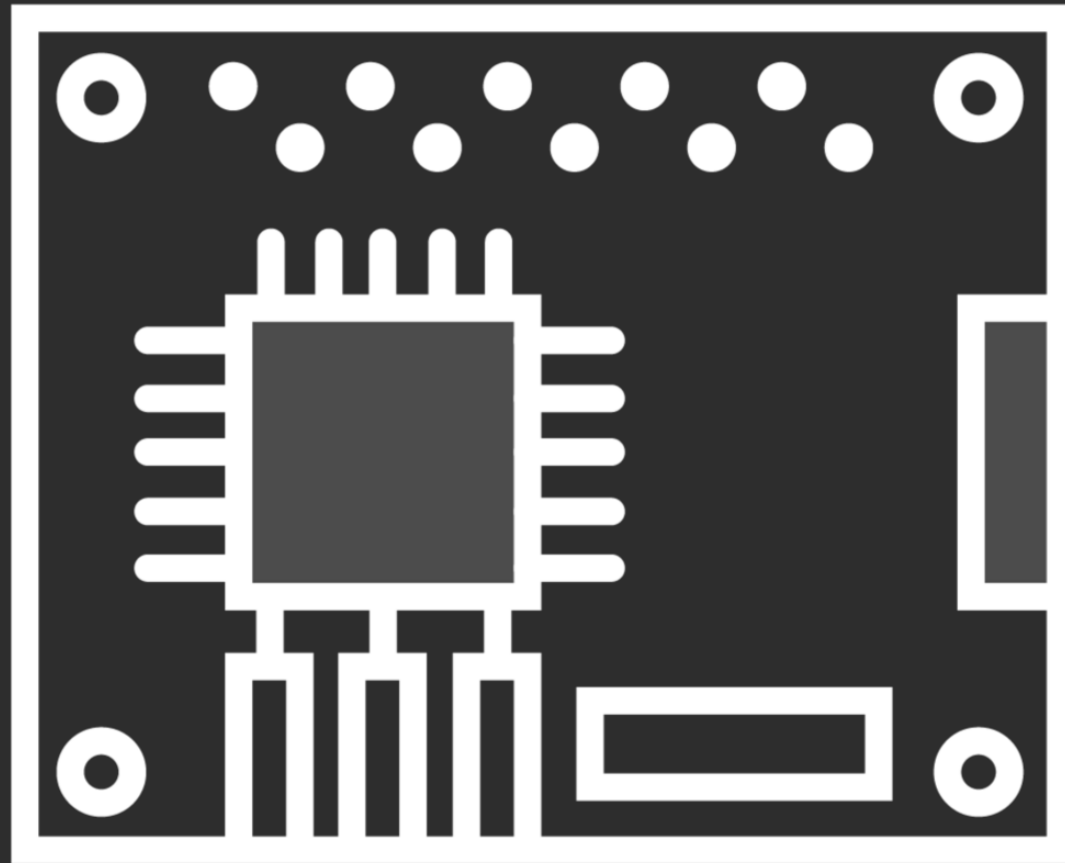
11101111001111
RAUD 00001111
0001 DANGER 0
01011111

Know the rules for your
environment.

Same Story - Different Platform



Monitors Both Hardware and Software

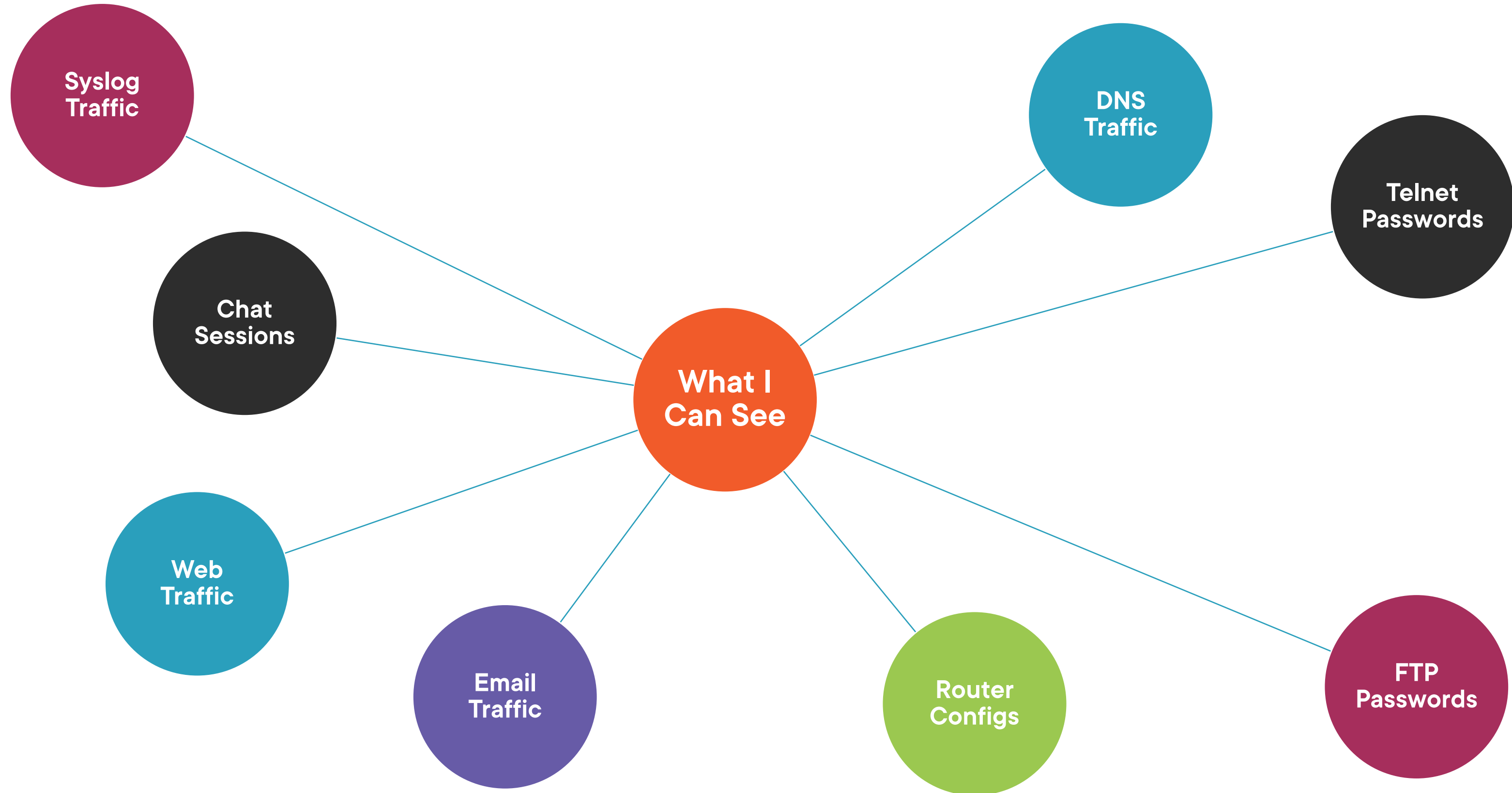


What Are We Looking For?



How Dangerous Is Sniffing?

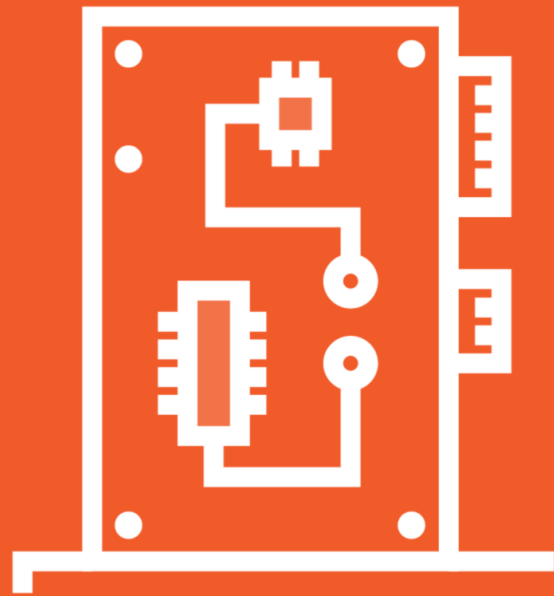
It's All There!



Ala' Mode



Ala' Mode



Promiscuous



Ala' Mode



Promiscuous

Passes traffic to the CPU instead of discarding frames intended for the NIC card



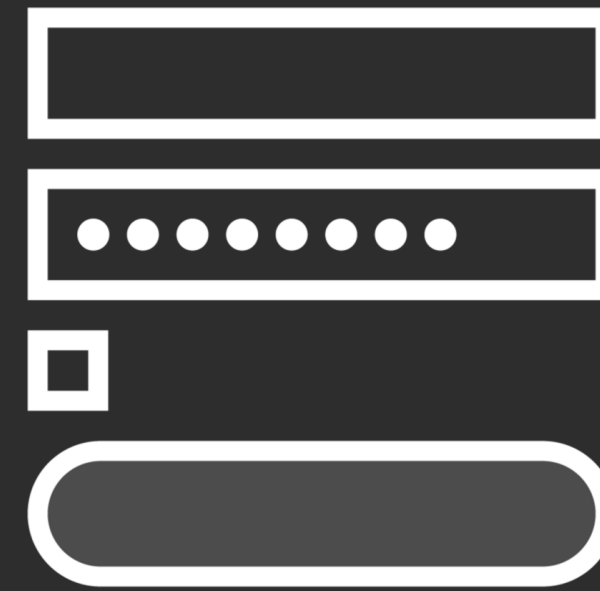
Yes, most networks today employ switch technology

Packet sniffing is still useful

Installing remote sniffing programs on networks with heavy traffic flow is relatively easy

Types of Sniffing

Types of Sniffing



Spoofing attacks

Types of Sniffing



DHCP attack

Types of Sniffing



MAC Flooding

Types of Sniffing



DNS poisoning

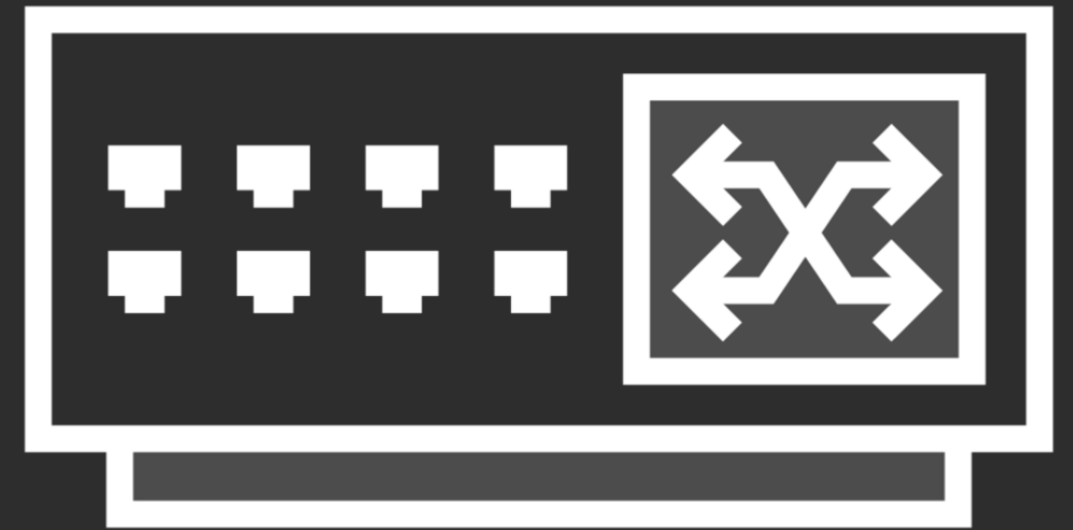
More Vectors



ARP poisoning



Password sniffing



**Switch-port
stealing**



More Vectors

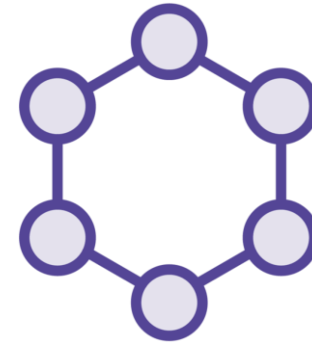
Dale switchport is pretty long- add icons here if you want to build out more slides



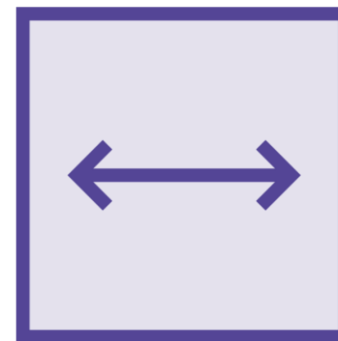
Types of Sniffing Continued



Passive Sniffing



Monitors packets flowing across the network



Networks that use hubs will use passive sniffing



Not often used



Passing Sniffing Methods

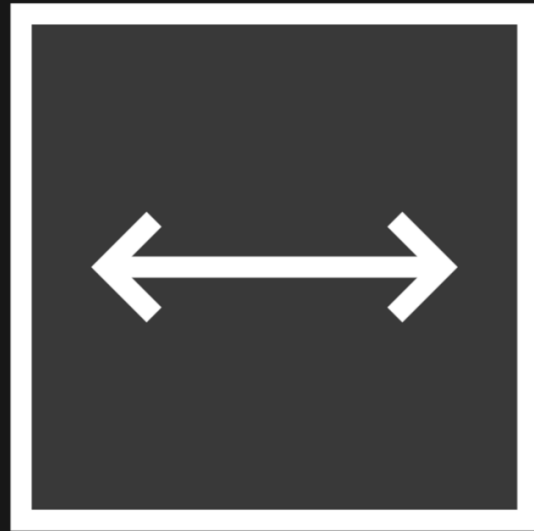
Compromising physical security

Using a Trojan horse



Passive sniffing provides
significant stealth advantages
over active sniffing

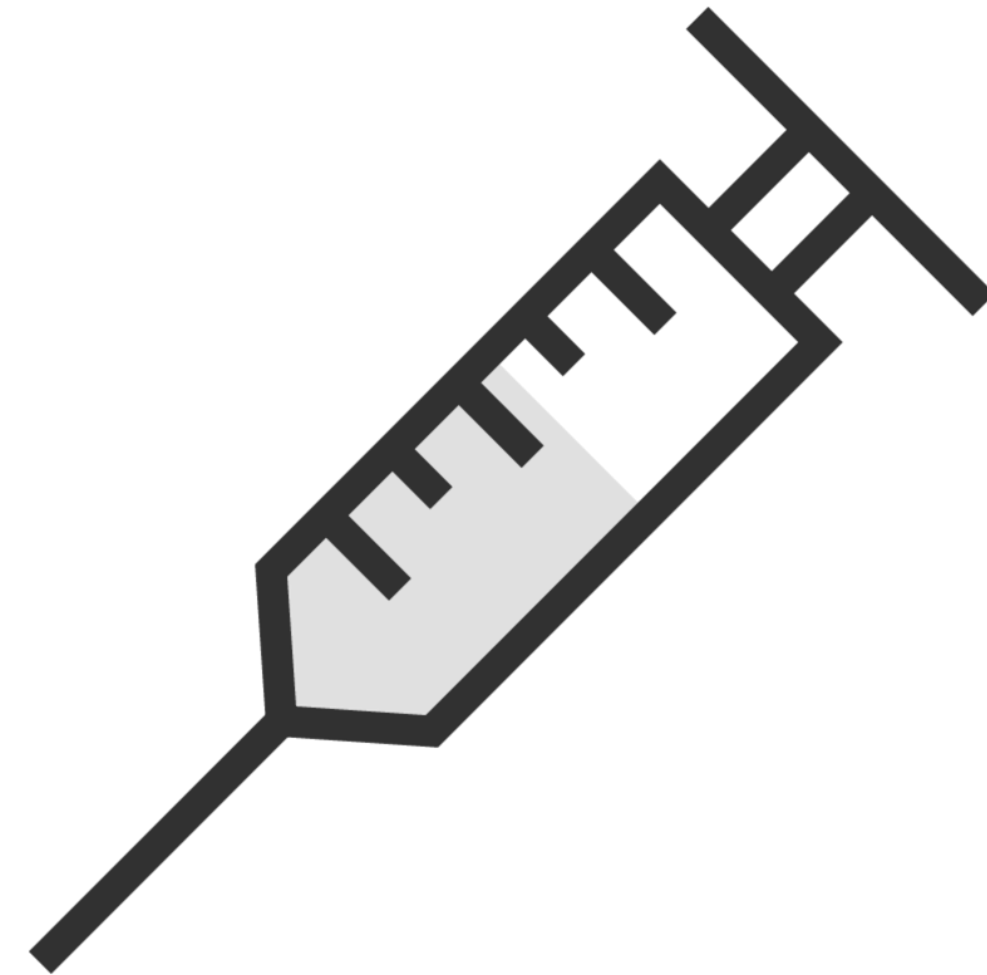




Sniffing through a switch

Active Sniffing

Searches for traffic by actively injecting traffic into it



CAM: Content Addressable Memory

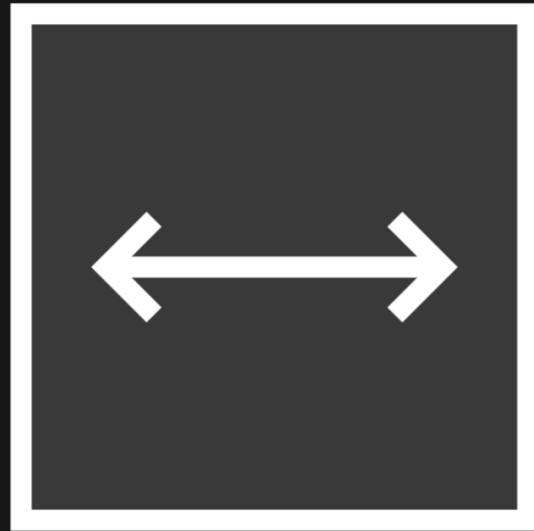
DHCP Starvation

MAC Duplication

ARP Spoofing

Mac Flooding

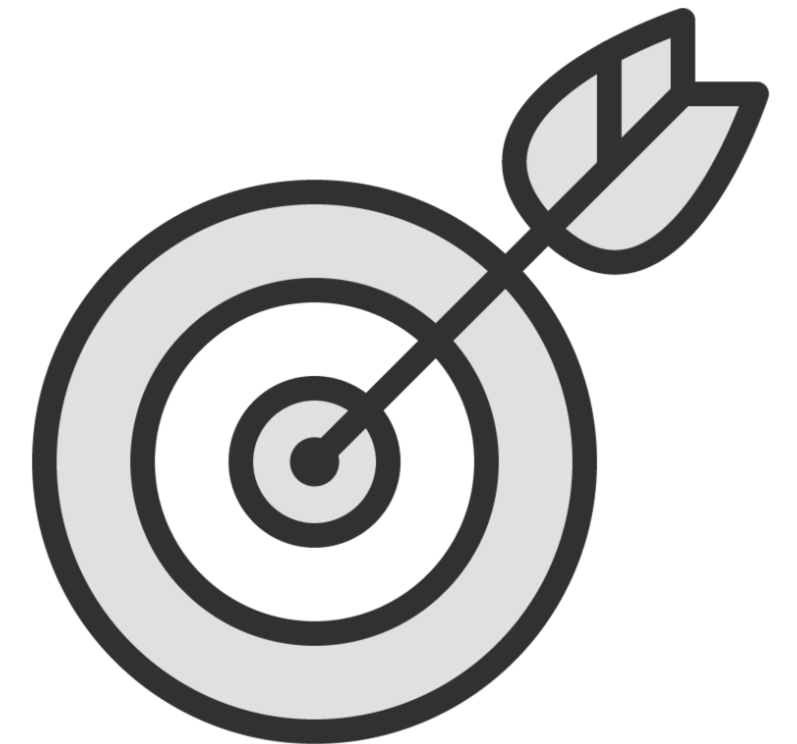
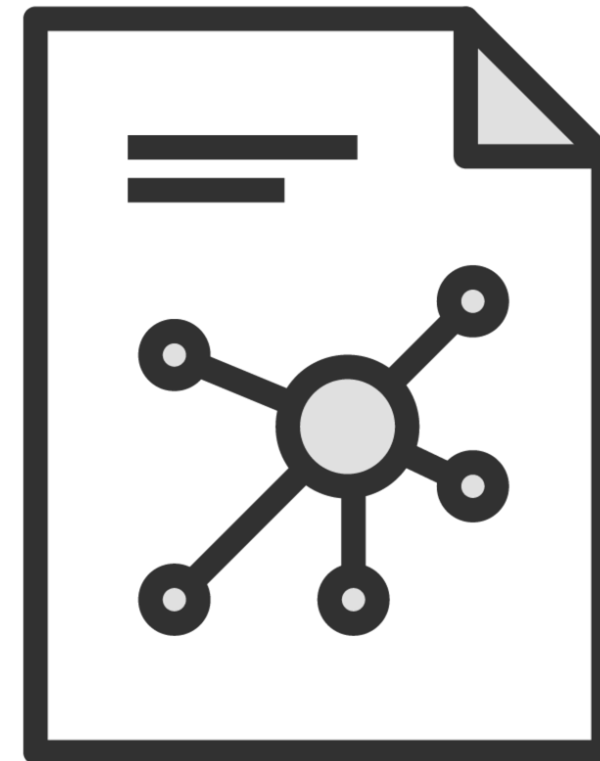




Sniffing through a switch

Active Sniffing

Purpose is to overload the switch and turn it into a HUB



Vulnerable Protocols

HTTP

Telnet

SNMP

POP

NNTP

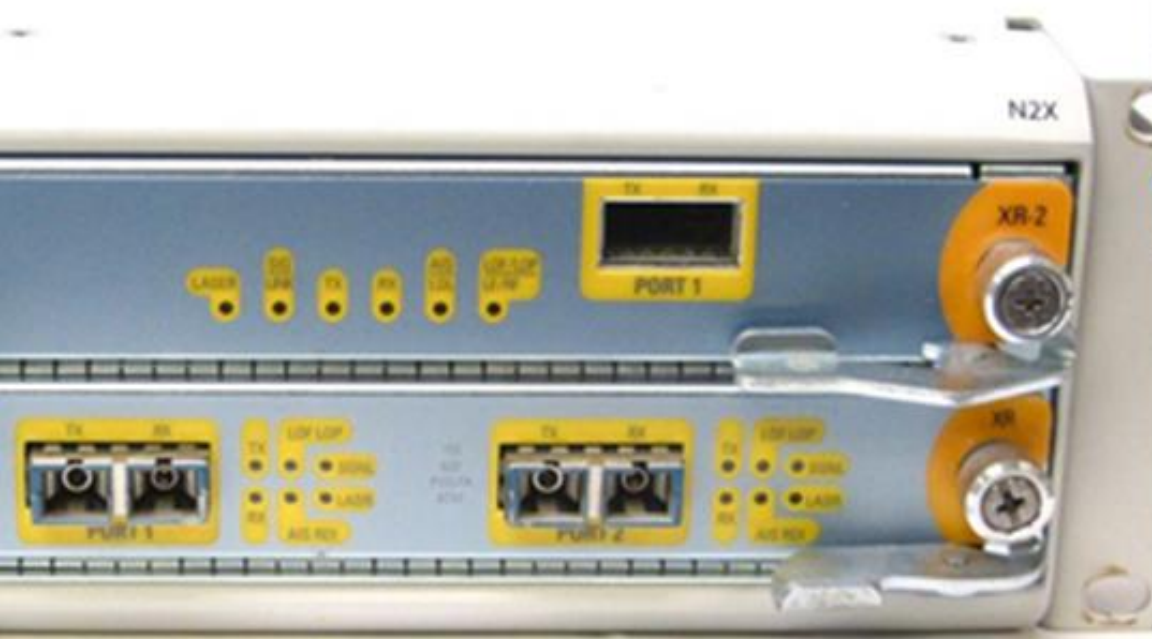
IMAP

FTP

rlogin

Hardware vs. Software

Analyzers



Monitor
Analyze
Capture
Data Packet

Software

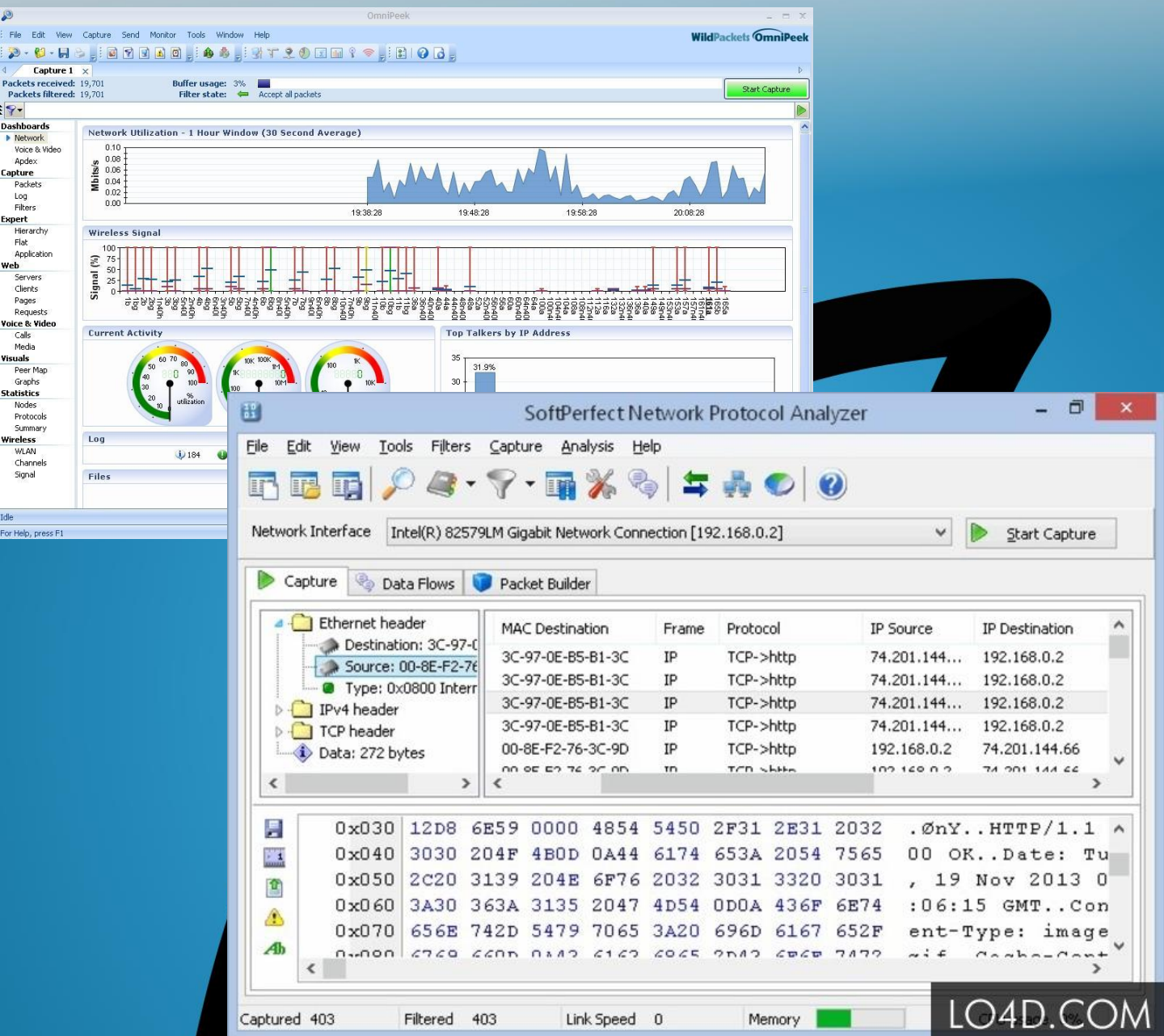
Wireshark

OmniPeek

SoftPerfect NPA

Microsoft Network Monitor

“The Dark Side”...



Add demo about wireshark and lift up PS
wireshark course

IS THIS SUPPOSED TO SAY
MOBILE??

Sniffing Module Apps

No laptop no problem!

Add demo of shopping for apps

I KNOW YOU'RE NOT DOING SUMMARY SLIDES-
BUT CONTENT YOU SHARE IN THIS SUMMARY
IS INTERESTING- MAYBE A STORY YOU WANT
TO KEEP TO CLOSE OUT THIS MODULE

IF YOU DO MAYBE ADD A SLIDE THAT SAYS
STORY TIME OR SOMETHING

Learning Check

Learning Check



Up Next:
