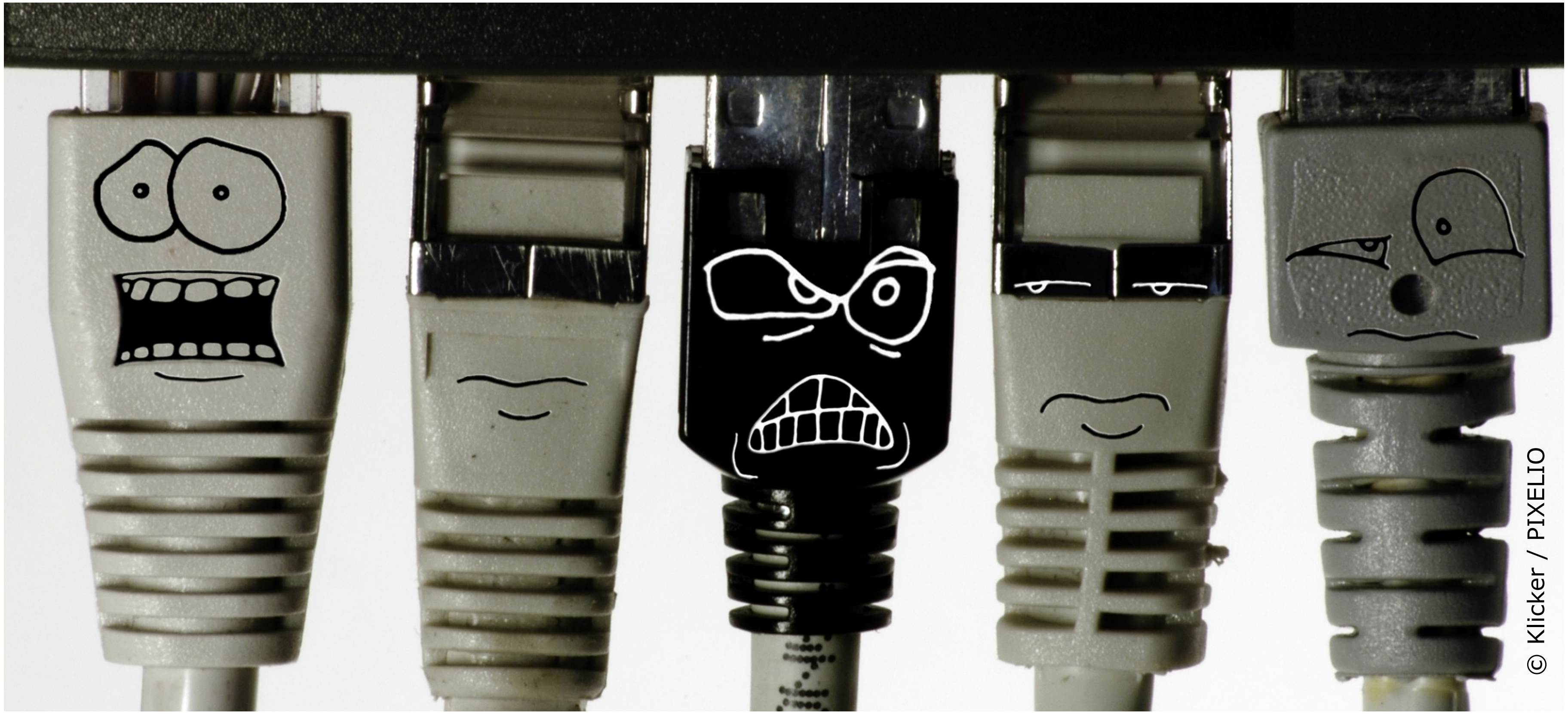
Network Security (NetSec)

TECHNISCHE UNIVERSITÄT DARMSTADT

Summer 2015
Virtual LAN (VLAN) Security



© Klicker / PIXELIO

CASED

Learning Objectives

Know the advantages and disadvantages of Virtual LANs

Understand the risks of a VLAN setup

Be able to mitigate the risks of using VLANs

Overview of this Module

(1) VLAN Introduction

- The idea behind Virtual LAN
- Typical setup
- IEEE 802.1Q

(2) Possible Attacks against 802.1Q VLANs

- Switch spoofing
- Double tagging

(3) Mitigation

(4) Other VLAN Technics

VLAN Basics

Networking Domains

Production

Accounting

Guests

Voice

System/Network Management

Storage (SAN)

Demilitarized Zone (DMZ)

v.de

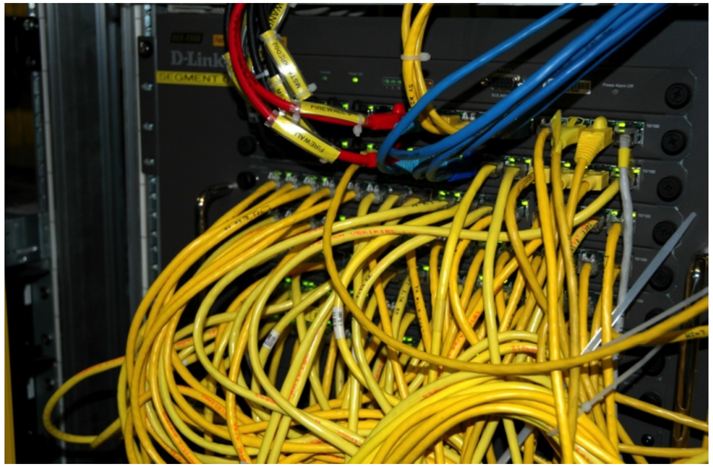
winnettcollege.com

C. Nöhren / pixelio.de

The idea behind a Virtual LAN

Before VLAN:

- One cable per subnet
- Moving hosts meant physical rewiring
- Adding a new subnet meant adding new wires **AND** switches
- Bandwidth not shared between subnets

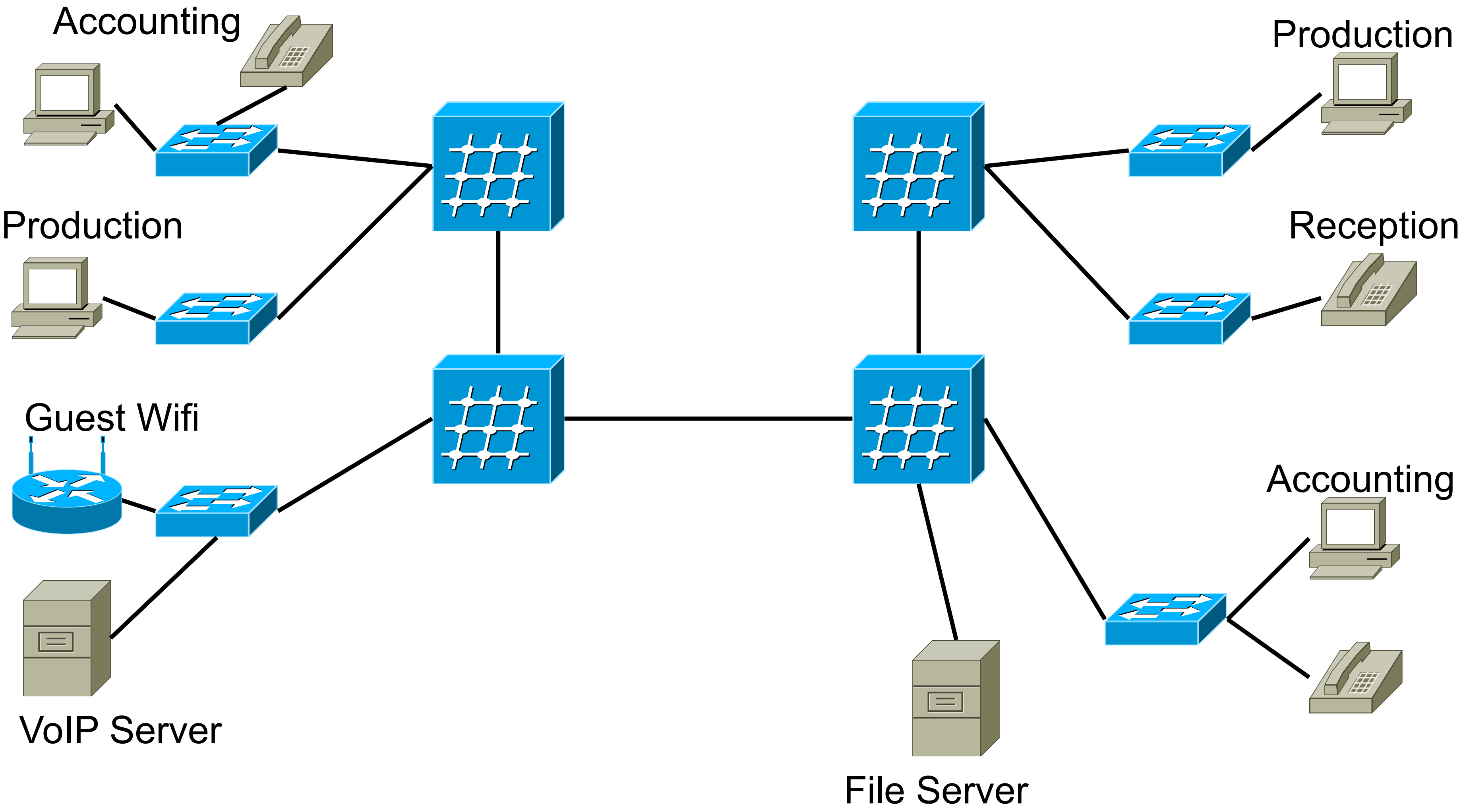


After VLAN:

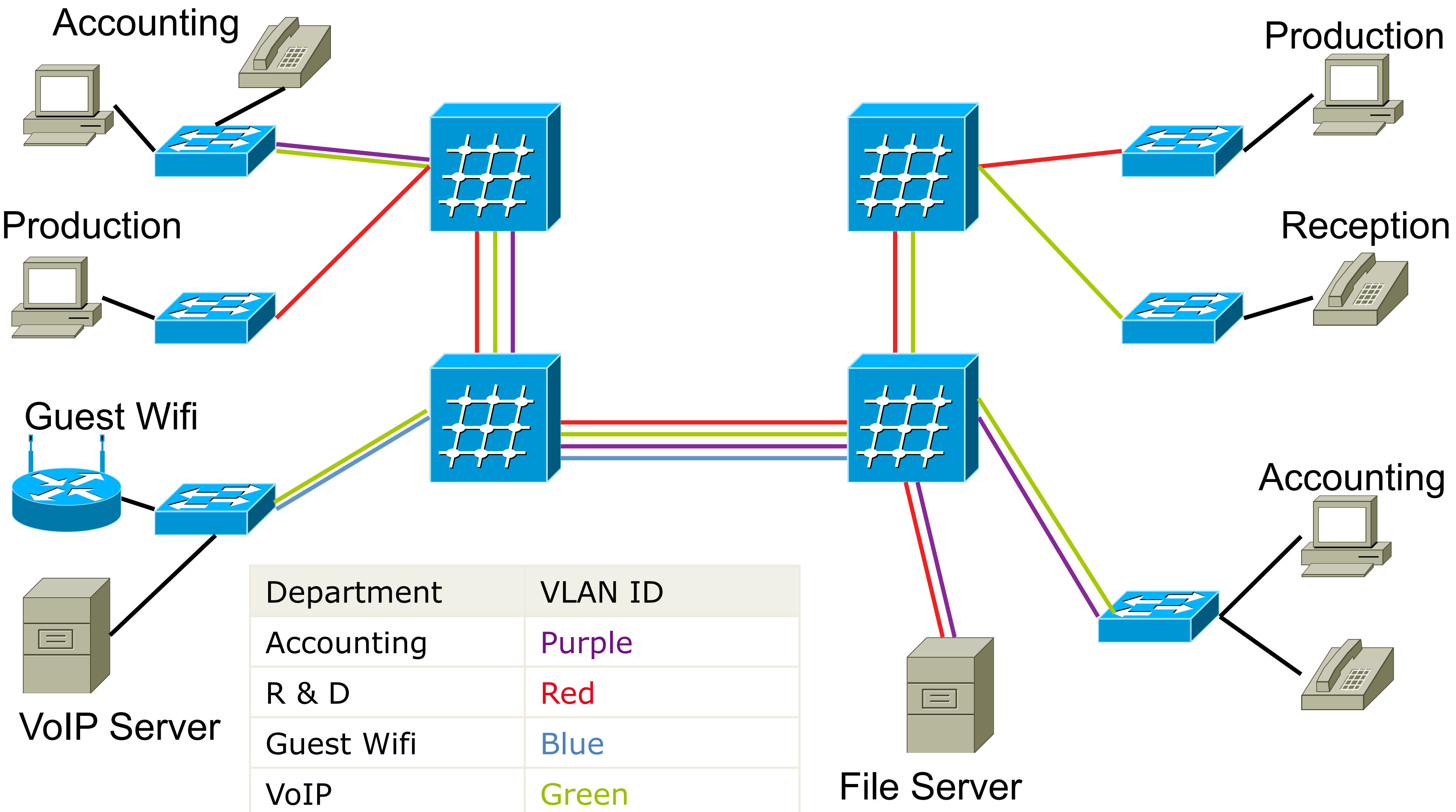
- The wires are virtual now
- Complete remote reconfiguration of networks
- Bandwidth on a wire can now be shared between subnets

© Paul-Georg Meister / PIXELIO

Typical Setup



Typical Setup



Department	VLAN ID
Accounting	Purple
R & D	Red
Guest Wifi	Blue
VoIP	Green

Airport IT

Lufthansa
Kein Eingang
Please do not enter
Anmeldefreie Waren
Nothing to declare
Tobacco & Liquor
Fragrance

Frankfurt Airport

20 000 people working at the airport

Air traffic, security checks, logistics, retail

450 mission critical services

22 000 network outlets, 466 Wifi access points

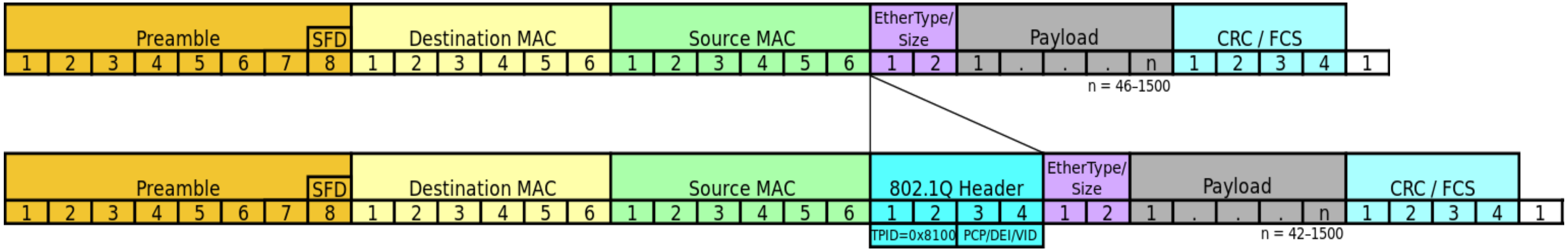
Thousands of desktop PCs

Hundreds of mobile devices

All on one physical network (including surveillance, phone etc.)

IEEE 802.1Q

802.1Q: Overview



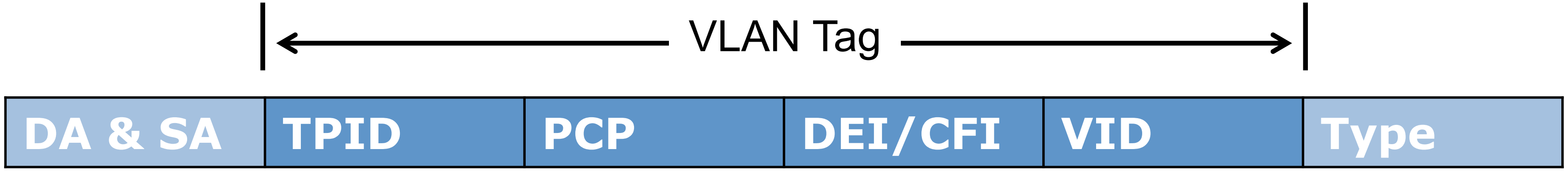
A layer 2 extension (IEEE 802 group defines Ethernet)

- Adds an additional 32 bit field after the source MAC address
- Also provides Class of Service (CoS)

Each packet gets its own tag

If a packet is not tagged the switch will add the default tag (for the ingress port)

802.1Q: Header



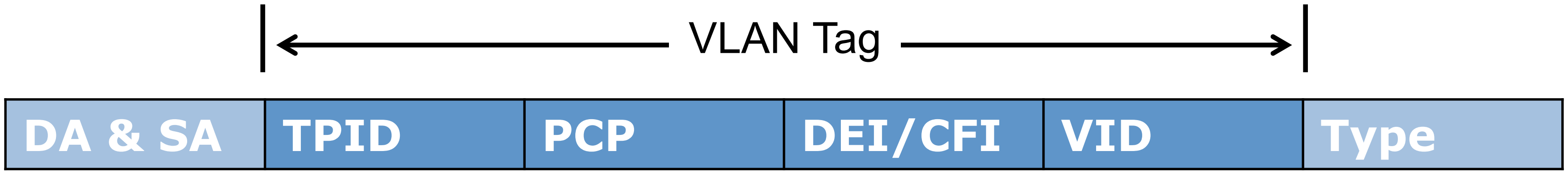
TPID - Tag Protocol Identifier (16 Bit)

- Indicates that the frame is VLAN tagged
- Value is 0x8100 for 802.1Q tagged frames
- For VLAN unaware devices it looks just like the *EtherType/Length* field

PCP - Priority Code Point (3 Bit)

- Frame priority according to IEEE 802.1p
- From 0 (best effort) to 7 (highest priority)
- Used for CoS

802.1Q: Header


VLAN Tag

DA & SA | TPID | PCP | DEI/CFI | VID | Type

DEI - Drop Eligible Indicator (1 Bit)

- Field formerly used as CFI (Canonical Format Indicator) for Token Ring compatibility
- Indicates if a frame can be dropped in case of congestion
- Normally used together with the PCP field

VID – VLAN Identifier (12 Bit)

- Specifies the actual VLAN
- Offers 4094 VLANs
- 0x000 (priority frames - CoS) and 0xFFF are reserved

Modes of Operation

Each port of a switch can either be:

Untagged (Access):

- Only regular Ethernet Frames are accepted
- The connected system is not allowed to add Tags
- Switch adds a defined Tag

Tagged (Trunk):

- Switch expects a frame with VLAN ID / extension
- Connected system can set the Tag themselves

Mixed (General):

- Both tagged and untagged packets are accepted
- Untagged packets get the Native/Port VID configured

Possible Attacks

Switch Spoofing

Switches allow for automatic/dynamic configuration

- Using 802.1ak: **Multiple VLAN Registration Protocol (MVRP)**
- or **VLAN Trunking Protocol (VTP)** with Cisco hardware
- When a new switch enters the network or the configuration is changed it announces the VLANs to the uplink
- Only the switch facing the end system needs to be configured

An attacker can use MVRP to announce himself as a switch

1. Use MVRP to announce all VIDs as configured
2. Uplink switches will reconfigure its downlink port accordingly
3. Attacker becomes part of all VLANs

Double Tagging

An Ethernet frame can carry two VLAN extensions

- Specified in IEEE 802.1ad
- Used by ISPs to mix tagged frames from different clients
- TPID for the outer (service provider) tag is 0x88a8
- The receiving entity is in fact the entity to which the sender wanted to send the packet

An attacker can send frames to other VLANs

1. A second tag is added to the frame before sending
2. The first switch removes the tag which the attacker is really a member of
3. The second switch only sees the second (false) tag and outputs the packet to the second VID

- Answers to the packet sent are not getting back to the attacker

Attack Mitigation

Get your config right

1. Disable automatic trunk negotiation
2. Explicitly set all non-trunk ports as access ports
3. Do not use VLAN 1 (the default Port-VID on most switches)
4. Set the Port-VID on trunk ports to an unused VLAN
5. Explicitly tag all packets on a trunk port with the Port-VID
6. Use PCP to allow mission critical systems to communicate while under a flooding (DoS) attack

Other VLAN Technics

MAC VLAN

Use the MAC address of the connected system to assign a VLAN

Can be used even if the users are roaming

Problems:

- MAC addresses can be spoofed even easier than VLAN tags
- Only the system is authenticated, not the user.
- When deploying new hardware the MAC address has to be added to the configuration of every switch

Solution:

- Use IEEE 802.1X authentication

Protocol VLAN

Use the protocol type in upper layers to assign a VLAN

Used to separate different Layer 3 or even Layer 5 protocols

- Apple Talk, IPX, DECnet, Banyan
- Create a Voice LAN

Helps to create different administrative domains

Prevents conflicts in upper layer protocols

Allows for regulatory compliance

- i.e. recording all voice calls

Private VLAN

Each port can only talk to specific ports

Separation into two VLANs for one subnet:

- Primary VLAN: the IEEE 802.1Q VLAN
- Secondary VLAN: a group of systems belonging to the VLAN
- Reduces the broadcast domain within a single subnet

Use cases:

- Network Segregation: Assign hosts to VLANs without changing their IP address
- Secure Hosting: Allow hosted servers to only talk to the firewall
- Secure VDI: Terminals are only allowed to talk to the server
- Backup Network: Hosts are only allowed to talk to their backup system

VXLAN – Virtual eXtensible LAN

Developed by VMWare and Cisco

Now an IETF draft

A step towards Software Defined Networking (SDN)

Create overlay networks

Logical layer 2 networks are encapsulated in layer 3 packets

Uses a **Segment-ID** to differentiate the different networks

No 802.1Q VLAN tags required

Summary

VLANs help to split the network into domains

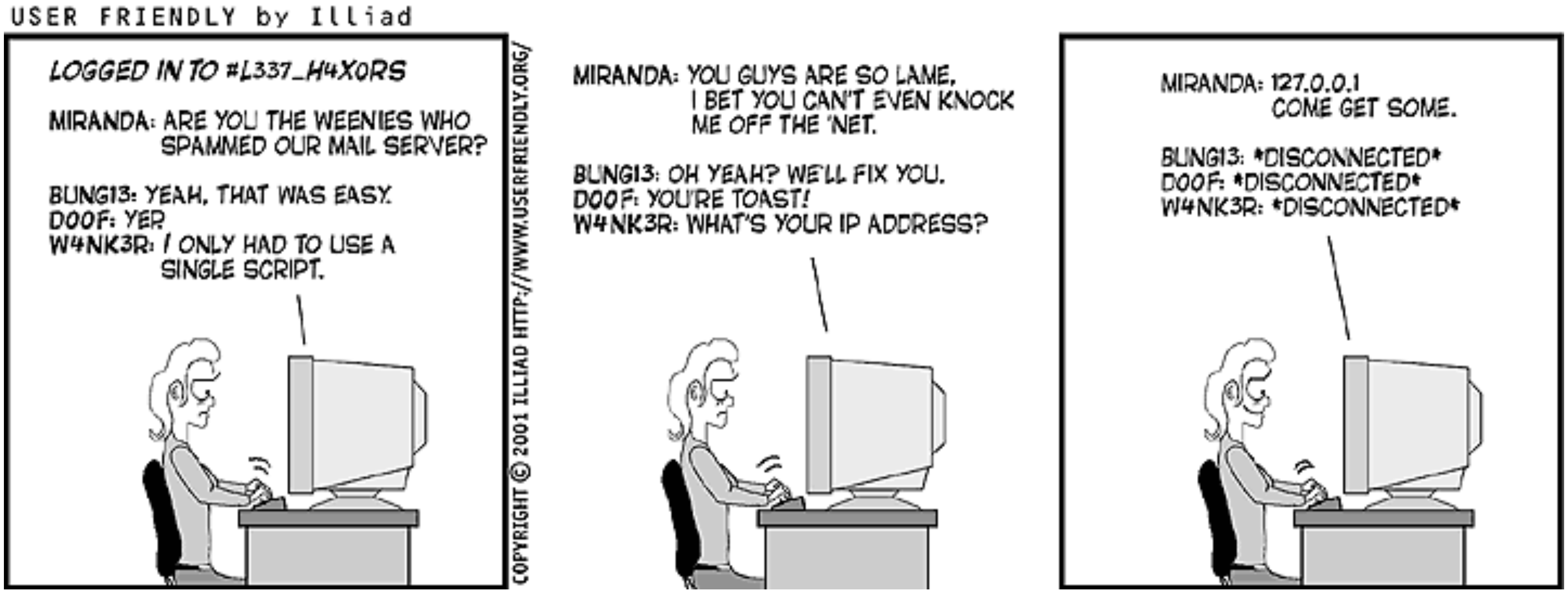
Reduce the networking costs

VLANs are not a security feature

Can help to implement security

- DoS mitigation using priority tags
- IEEE 802.1X authentication

VLAN enabled hardware is configured for convenience not security


USER FRIENDLY by Illiad
LOGGED IN TO #L337_H4X0RS
MIRANDA: ARE YOU THE WEENIES WHO SPAMMED OUR MAIL SERVER?
BUNG13: YEAH, THAT WAS EASY.
DOOF: YEP.
W4NK3R: I ONLY HAD TO USE A SINGLE SCRIPT.
COPYRIGHT © 2001 ILLIAD HTTP://WWW.USERFRIENDLY.ORG/
MIRANDA: YOU GUYS ARE SO LAME. I BET YOU CAN'T EVEN KNOCK ME OFF THE 'NET.
BUNG13: OH YEAH? WE'LL FIX YOU.
DOOF: YOU'RE TOAST!
W4NK3R: WHAT'S YOUR IP ADDRESS?
MIRANDA: 127.0.0.1 COME GET SOME.
BUNG13: *DISCONNECTED*
DOOF: *DISCONNECTED*
W4NK3R: *DISCONNECTED*

Copyright Notice