Počítačové siete
VLAN (IEEE 802.1Q)

Klasická LAN

- jednotlivé uzly pripojené k médiu môžu navzájom voľne komunikovať na linkovej vrstve
- kolízna doména
  - množina uzlov, z ktorých môže naraz vysielať len jeden, aby nedošlo ku kolízii
- broadcast-ová doména
  - množina uzlov, ktoré dostanú rámec určený všetkým uzlom (broadcast)

Klasická LAN

- Ethernet
  - hub(y)
    - jedna kolízna doména, jedna broadcast-ová doména
  - switch(e)
    - jedna broadcast-ová doména
    - každý port tvorí samostatnú kolíznu doménu
- WiFi
  - celá ESS je jedna broadcastová doména

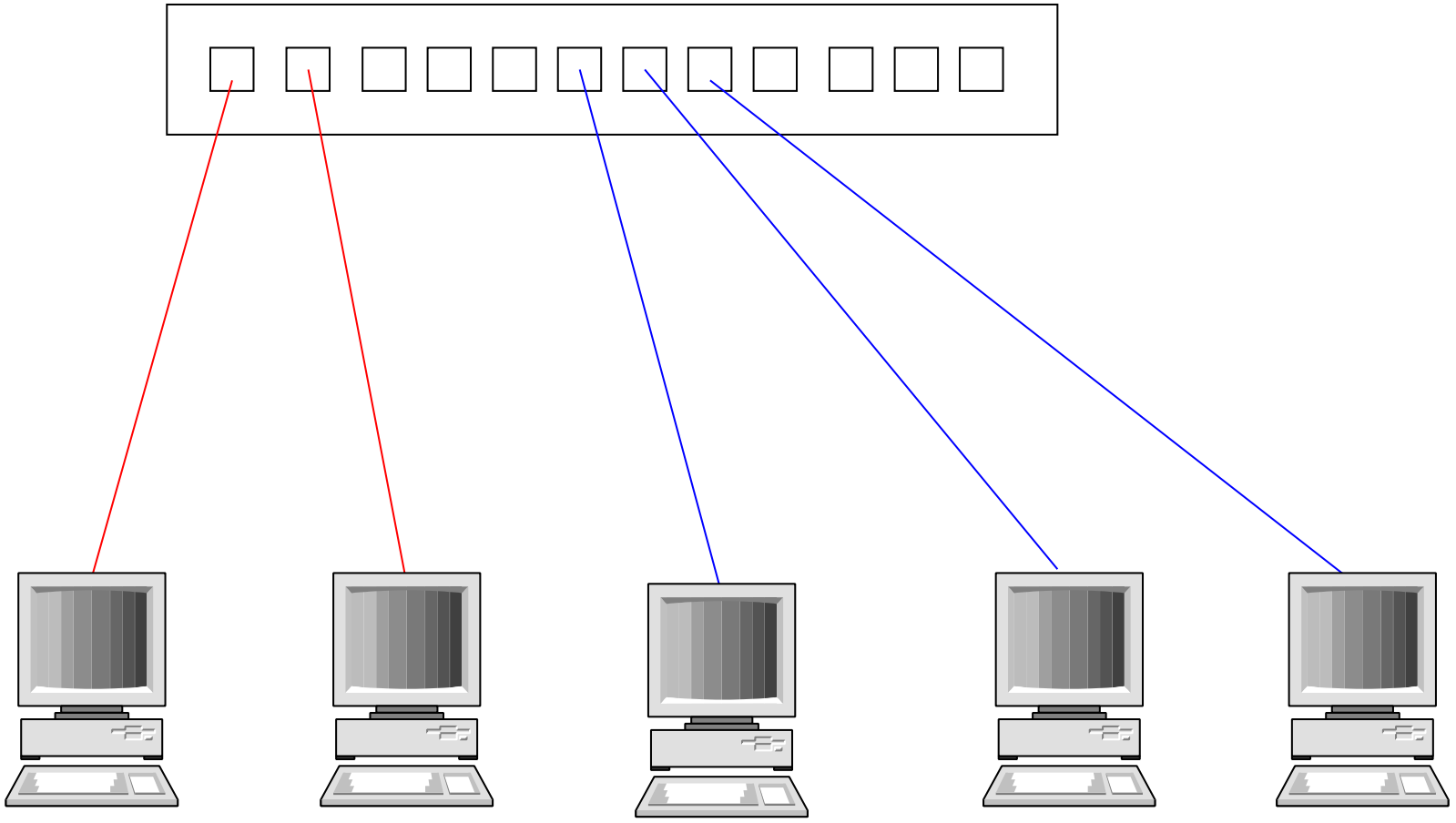
Virtual LAN

- rozdelenie fyzickej LAN na virtuálne
  - rámce sú prenášané len medzi portami patriacimi do jednej VLAN
    - prenos medzi VLAN je možný len cez prvok sieťovej vrstvy – router
- využitie
  - bezpečnosť
    - zariadenia môžu komunikovať len cez router – firewall
  - rozdelenie siete na samostatné broadcast-ové domény
    - zníženie záťaže siete

Port based VLAN

- každý port je priradený do nejakej VLAN
  - je izolovaný od portov v inej VLAN
- nie je možné prenášať viac VLAN cez jednu linku
  - nie je vhodné pre VLAN, ktorá má porty vo viacerých switch-och
- nevyžaduje žiadne zmeny formátu rámcov
  - nie je potrebný žiadny štandard na zaistenie interoperability
- komunikácia možná len medzi portami jednej VLAN

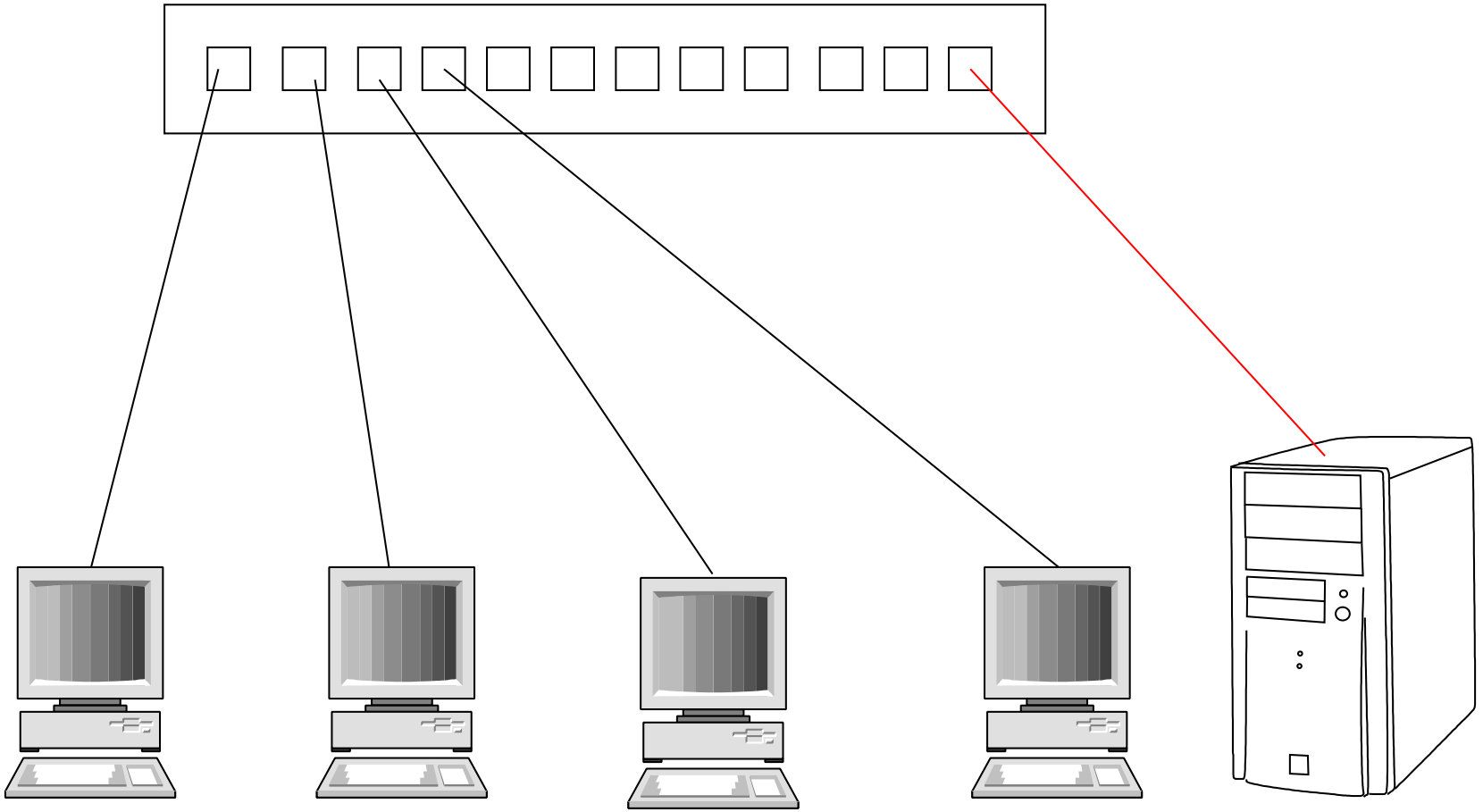
Port based VLAN



Izolované porty a uplink

- jeden port switch-a je definovaný ako uplink
- ostatné porty sú navzájom izolované
- možná komunikácia
  - izolovaný port -> uplink
  - uplink -> izolovaný port
- nemožná komunikácia
  - izolovaný port -> iný izolovaný port

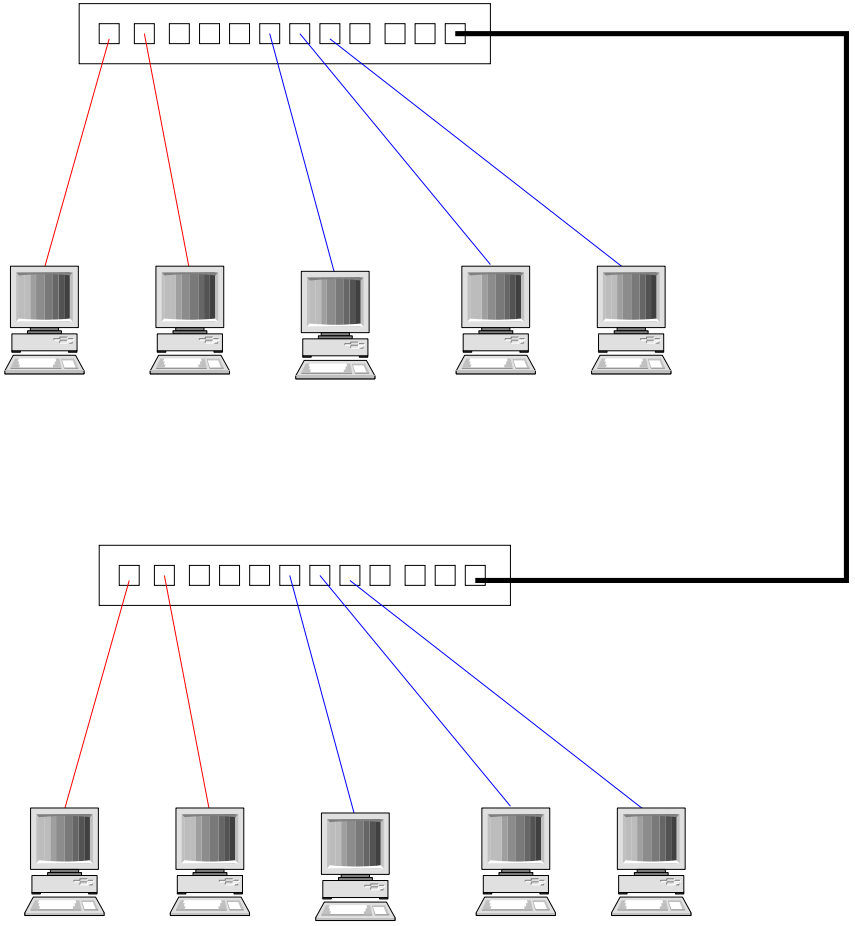
Izolované porty a uplink



802.1Q VLAN

- umožňuje, aby VLAN obsahovala porty na rôznych switch-och
- umožňuje zdieľanie prepojov viacerými VLAN

802.1Q VLAN



802.1Q VLAN

- každá VLAN má pridelené číslo – VID
  - 12 bitov
  - 0 = žiadna
  - 1 = default
  - 4095 = neplatná hodnota
  - 2 – 4094 = použiteľné VID
    - niektoré switch-e (napr. CISCO) majú ďalšie obmedzenia

802.1Q VLAN

- rámce
  - netagované (untagged)
    - bežné (napr. Ethernet) rámce
  - tagované (tagged)
    - typ protokolu = 0x8100
    - Tag Control Information
      - 3 bity priorita
      - 1 bit indikuje kandidáta na zahodenie (od 802.1Q-2014, voliteľne zapnuteľné)
      - 12 bitov VID

Porovnanie Ethernet rámcov

- cieľová adresa (6B)
- zdrojová adresa (6B)
- typ (protokol sieťovej vrstvy) (2B)
  - 0x0800 = IPv4
  - 0x86DD = IPv6
  - 0x0806 = ARP
- dáta
- FCS

- cieľová adresa (6B)
- zdrojová adresa (6B)
- 0x8100
- TCI (2B)
- typ (protokol sieťovej vrstvy) (2B)
- dáta
- FCS

802.1Q VLAN

- pre každú definovanú VLAN má switch
  - VID
  - pre každý port
    - či je alebo nie je súčasťou VLAN, prípadne či sa môže stať súčasťou VLAN
    - či majú byť odoslané rámce do VLAN tagované alebo nie
- pre každý port
  - PVID (Port VID)
  - typ prijímaných rámcov
    - len tagované, len netagované, oboje

802.1Q VLAN

- príslušnosť prijatého rámca k VLAN
  - netagovaný (untagged) rámec
    - PVID
  - tagovaný rámec
    - VID uvedený v tagu

802.1Q VLAN

- ingress filtering
  - kontroluje, či prijatý rámec patrí do VLAN, ktorej súčasťou je prijímajúci port
  - dôležité pre bezpečnosť
    - inak je možné posielať rámce do cudzej VLAN
  - voliteľná vlastnosť
- egress filtering
  - rámec patriaci do VLAN switch pošle len na porty, ktoré do danej VLAN patria

802.1Q VLAN

- učenie sa MAC adries na portoch
  - okrem MAC adresy sa berie do úvahy aj VID
- rámec na známu MAC adresu vo VLAN
  - pošle sa len na správny port
- rámec na neznámu MAC adresu
  - pošle sa na všetky porty príslušnej VLAN
    - teda nie na porty, ktoré do VLAN nepatria
  - rovnako aj broadcast

802.1Q VLAN

- automatická konfigurácia VLAN
  - protokoly MVRP (802.1Q-2014), GVRP
  - umožňuje výmenu informácií o VLAN medzi switch-mi
    - nie je potrebné konfigurovať VLAN na všetkých switch-och

Priorita

- umožňuje prioritizovať niektorú komunikáciu
  - každý port môže mať niekoľko výstupných radov (queue)
    - každý určený pre nejakú triedu komunikácie (traffic class)
    - každý má definovanú prioritu
  - najprv sa odosielajú rámce z radu s vyššou prioritou
  - VLAN tag podporuje 8 úrovní priority (3 bity)
    - tie sa mapujú na triedy komunikácie

Priorita

		počet tried							
		1	2	3	4	5	6	7	8
priorita	0	0	0	0	0	0	1	1	1
	1	0	0	0	0	0	0	0	0
	2	0	0	0	1	1	2	2	2
	3	0	0	0	1	1	2	3	3
	4	0	1	1	2	2	3	4	4
	5	0	1	1	2	2	3	4	5
	6	0	1	2	3	3	4	5	6
	7	0	1	2	3	4	5	6	7

Priorita

počet tried	typy komunikácie
1	{*Best Effort*, Background, Excellent effort, Critical Applications, Voice, Video, Internetwork Control, Network Control}
2	{*Best Effort*, Background, Excellent effort, Critical Applications} {*Voice*, Video, Internetwork Control, Network Control}
3	{*Best Effort*, Background, Excellent effort, Critical Applications} {*Voice*, Video} {*Network Control*, Internetwork Control}
4	{*Best Effort*, Background} {*Critical Applications*, Excellent effort} {*Voice*, Video} {*Network Control*, Internetwork Control}
5	{*Best Effort*, Background} {*Critical Applications*, Excellent effort} {*Voice*, Video} {*Internetwork Control*} {*Network Control*}
6	{*Background*} {*Best Effort*} {*Critical Applications*, Excellent effort} {*Voice*, Video} {*Internetwork Control*} {*Network Control*}
7	{*Background*} {*Best Effort*} {*Excellent effort*} {*Critical Applications*} {*Voice*, Video} {*Internetwork Control*} {*Network Control*}
8	{*Background*} {*Best Effort*} {*Excellent effort*} {*Critical Applications*} {*Video*} {*Voice*} {*Internetwork Control*} {*Network Control*}

802.1Q VLAN

- bežne používané pojmy (CISCO)
  - access port
    - port, ktorý je netagovaný a patrí len do 1 VLAN
  - trunk port
    - port, ktorý môže patriť do viac VLAN, typicky tagovaný
    - native VLAN
      - netagovaná VLAN trunk portu, PVID
    - allowed VLAN
      - tagovaná VLAN povolená na trunk porte
      - default = všetky