



## Kapitola 2: Základné koncepty prepínačov a ich konfigurácie



## CCNA Exploration Semester 3 - Chapter 2

## Modul 2 pokrýva

- Koncept LAN IEEE802.3/Ethernet sietí
  - Zaradenie ISO OSI
  - Prístupová metóda
  - Adresovanie a komunikácia
- LAN prepínanie
- Konfigurácia prepínačov
  - Základná
  - Port security

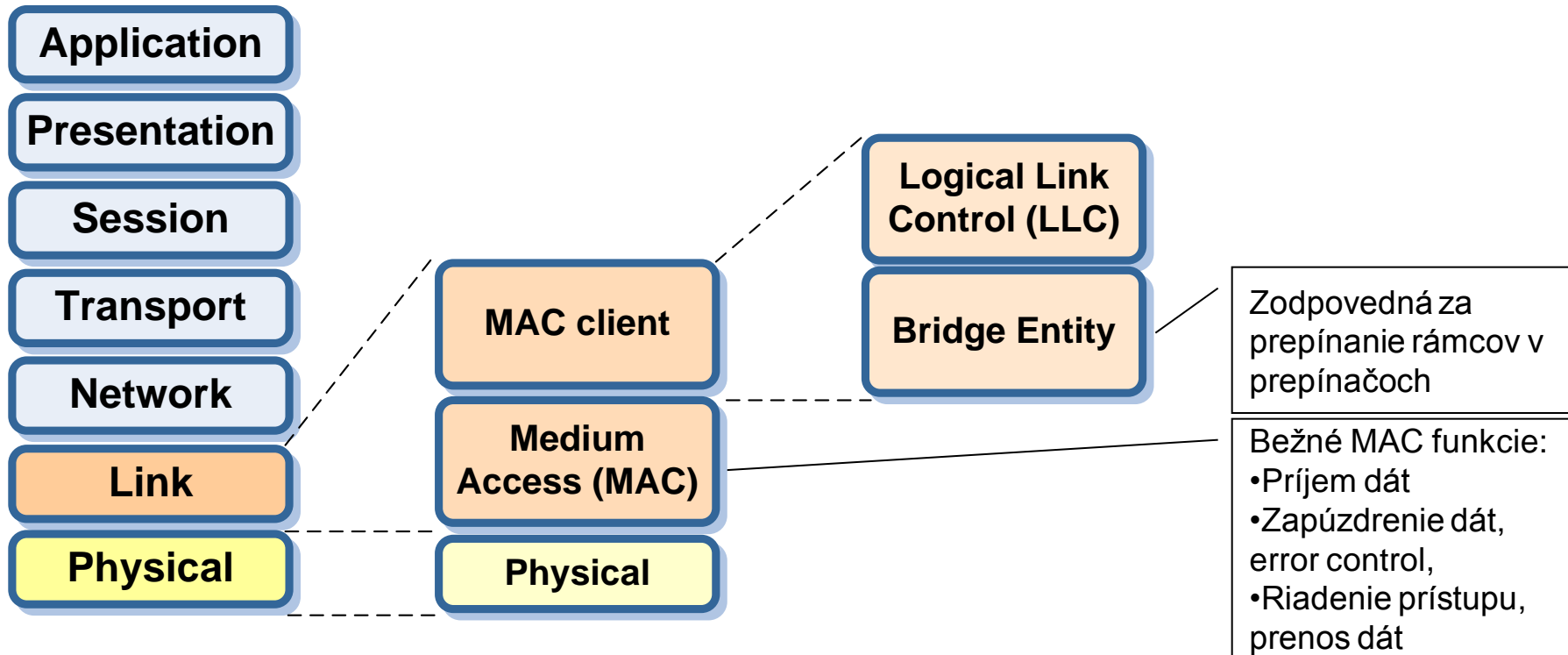
# Zopár otázok k Ethernetu

- Otázky na zamyslenie:
  - Ako sa volá PDU na ethernetete?
  - Aký má formát?
  - Aké adresovanie používa Ethernet a koľko typov adries má?
  - Koľko formátov rámca v Ethernete vlastne existuje?
  - Čo je to kolízna a broadcastová doména?
  - Prečo má rámec stanovenú minimálnu a maximálnu dĺžku?
  - Ako funguje CSMA/CD?
  - Ako pracuje full-duplex na TP kabeláži? Ako súvisí s CSMA/CD?
  - Čo je to kolízia? Aké druhy kolízií existujú?
  - Aké aktívne prvky sa v Ethernete bežne používali / používajú?
  - Ako funguje „autonegotiation“? Čo v prípade, že „nefunguje“?

# Ethernet – krátke pripomenutie

- Ethernet vznikol v prvej polovici 70. rokov v Xerox-e, jedným z autorov bol Bob Metcalfe, zakladateľ 3Com
  - Lacná, nenáročná, best-effort linková technológia
- V súčasnosti dominantná linková technológia v LAN, významne sa rozširuje v SAN i v MAN / WAN
  - Carrier Ethernet
  - Data Center Bridging
  - Synchronous Ethernet
- Rýchlosti od 10 Mbps do 100Gbps

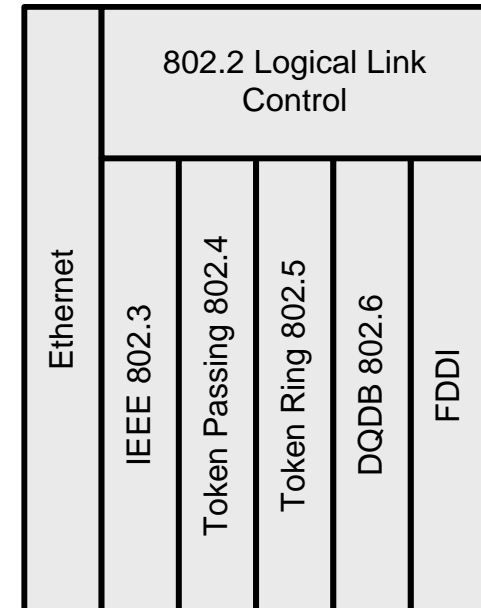
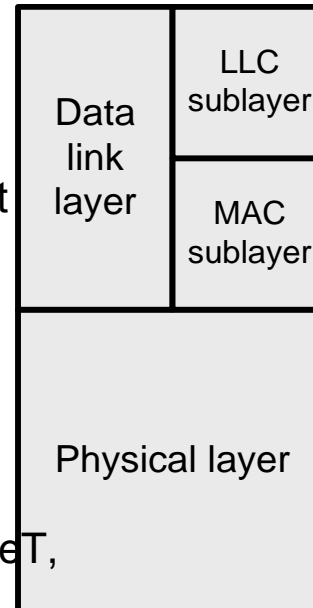
# Ethernet / IEEE 802.3 vs. ISO RM



- Ethernet / IEEE 802.3:
  - Definovaný na prvých dvoch vrstvách ISO OSI
  - Sú plne kompatibilné

# Ethernet - základy

- Použitá metóda riadenia prístupu
  - CSMA/CD (po 1 GigaEthernet vrátane)
    - 10GEthernet CSMA/CD nepoužíva
- Ethernet definuje vlastné PDU
  - Rámec
    - Použité na prenos používateľských dát
    - Min 64B - max. 1518B.
- Používa vlastné adresovanie
- Vyskytujúce sa topológie
  - Fyzická:
    - Bus (10Base2, 10Base5), Star (10BaseT, 100Base\_XX)
  - Logická:
    - Bus (CSMA/CD)
    - Point-to-Point (fullduplexný ethernet, žiadne CSMA/CD)



# Logical Link Control IEEE 802.2 (LLC)

- **Logical Link Control IEEE 802.2 sublayer (LLC)**

- Logicky oddeľuje vyššiu sieťovú vrstvu od nižšej, špecifickej podvrstvy prístupu k médiu (MAC)
  - Ako napr. IEEE 802.3, IEEE 802.5 a pod.
- Poskytuje jednotné rozhranie voči sieťovej vrstve

- **Funkcie:**

- Riadenie **toku** rámcov, riadenie **opravných procedúr** pri chybe prenosu, služby prenosu
- Poskytuje pre sieťové protokoly tzv. prístupové body k médiu
  - Service Access Points (SAP)
- SAP identifikuje sieťový protokol, ktorý predáva pakety na prenos LLC vrstve
  - Cez LLC môže komunikovať viacero sieťových protokolov naraz
    - IP, IPX, STP, NetBIOS apod.
    - Source SAP (SSAP), Destination SAP (DSAP)

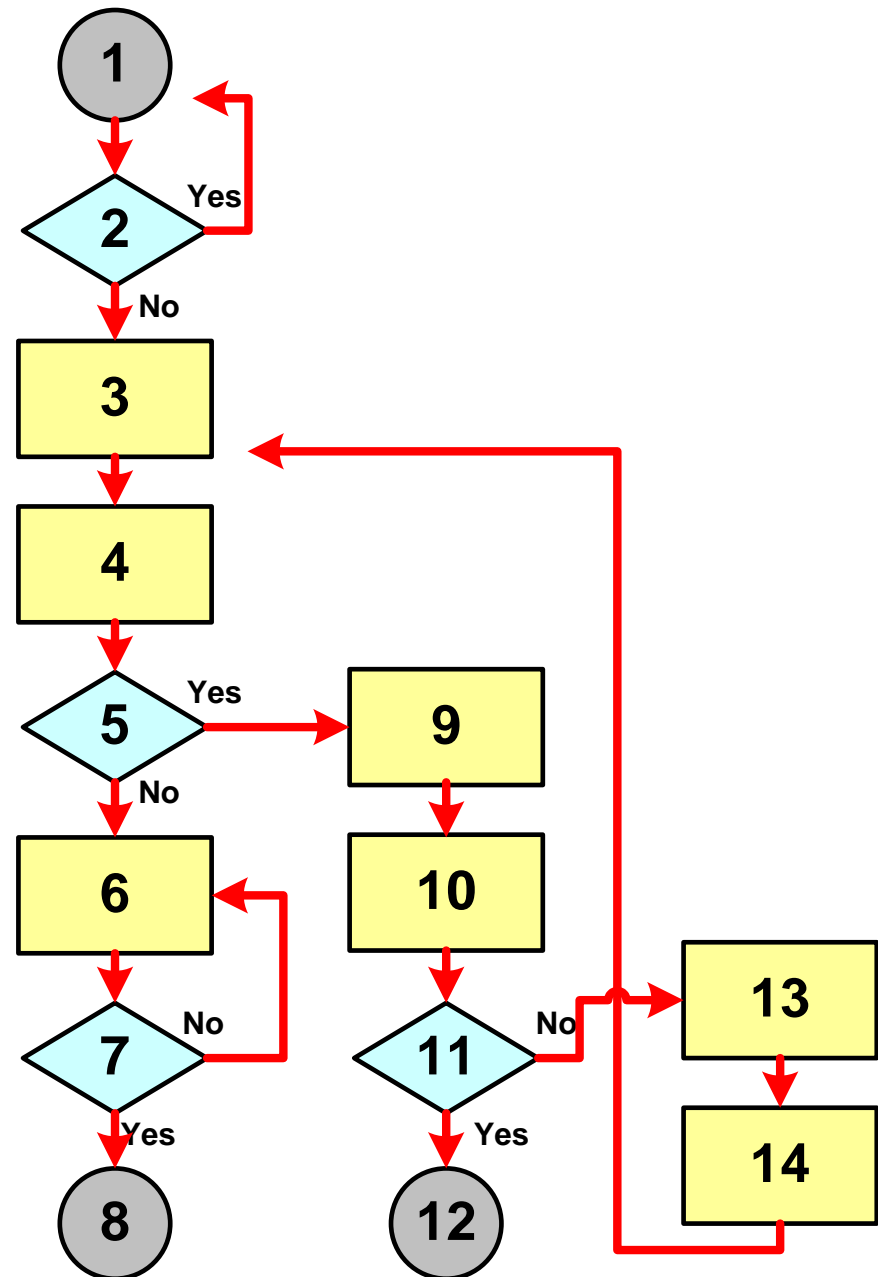
# Medium Access Control

- Medium Access Control sublayer (MAC)
  - Riadi prístup k médiu
    - Zabezpečuje zdieľanie prenosového média pre komunikujúcich
  - Riadi doručovanie dát cez sieť
    - **Adresovanie**
      - Doručovanie na základe identifikácie príjemcu a odosielateľa
      - Adresa predstavuje fyzickú adresu zariadenia
    - Funkcie **práce s rámcom**
      - Definícia formátu rámcov (štruktúry)
      - Rozpoznávanie typu a formátu rámcov
      - Zabezpečenie prenosu (počítanie FCS a kontrola FCS pri doručení)
- Niektoré MAC metódy
  - **CSMA/CD** (Carrier Sense Multiple Access / Collision Detect)
  - **CSMA/CA** (Carrier Sense Multiple Access / Collision Avoidance)
  - **Token Passing**



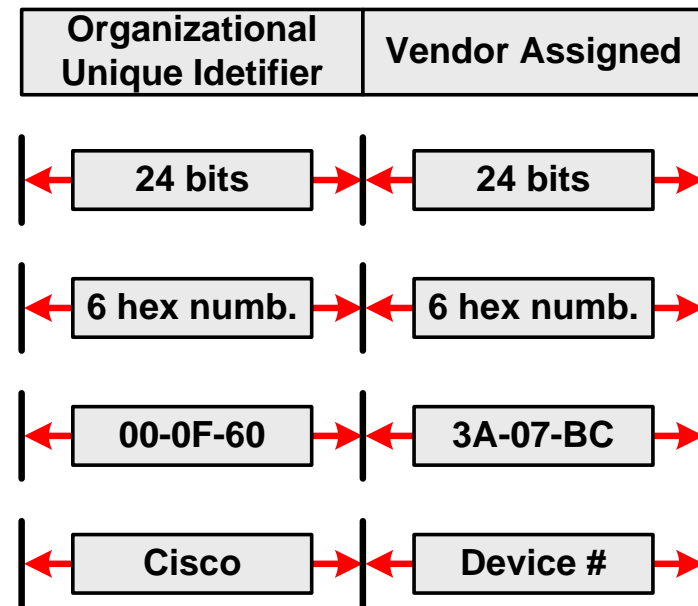
# CSMA/CD

1. Host wants to transmit?
2. Is carrier sensed?
3. Assemble frame.
4. Start transmitting.
5. Is a collision detected?
6. Keep transmitting.
7. Is the transmission done?
8. Transmission completed.
9. Broadcast JAM signal.
10. Attempts = Attempts + 1
11. Attempts > Too many
12. Too many collisions. Abort transmission.
13. Algorithm calculates backoff.
14. Wait for T microseconds.



# Základy Ethernet-u - adresovanie

- Komunikácia
  - Komunikujúci musí byť jednoznačne určený - **adresa**
- Ethernet adresovanie
  - Fyzické adresovanie
    - Napálená MAC adresa v NIC
  - Plošné adresovanie
    - Nie sú logické väzby medzi adresami
  - Adresa dlhá **48 bitov**
    - 24 bit OUI
      - Organizational Unique Identifier
      - Riadi IEEE
      - Pozri: <http://standards.ieee.org/regauth/oui/oui.txt>
    - +
    - 24 bitov (pridelených výrobcom)



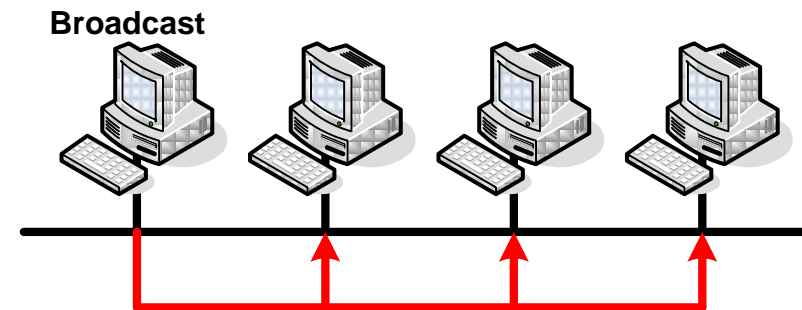
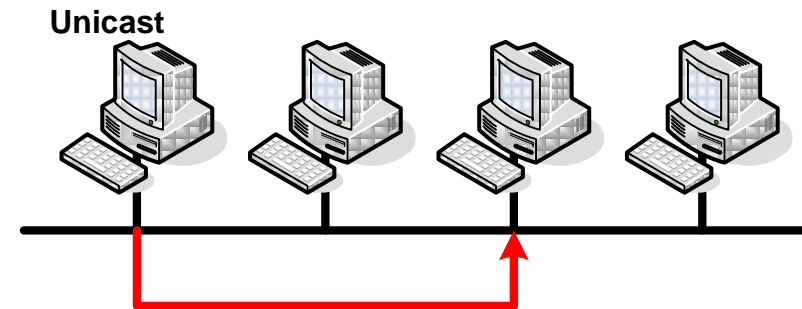
# Základy Ethernet-u - adresovanie

- Typy adries:
  - **Unicast:**
    - Určuje jedno zariadenie
  - **Multicast:**
    - Určuje skupinu zariadení, ale nie všetky
  - **Broadcast:**
    - Určuje všetky zariadenia na LAN
    - MAC (samé jednotky): FF-FF-FF-FF-FF-FF
- Z typov adries
  - Vyplývajú spôsoby komunikácie v Ethernet LAN

# Základy Ethernet-u - komunikácia

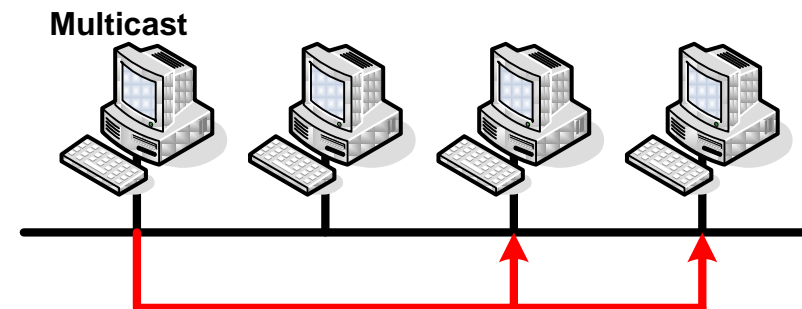
## ■ Unicast

- Najbežnejšia forma komunikácie
- Jeden odosielateľ, jeden príjemca
- Odosielateľ
  - Vyplní rámec s unicast adresou odosielateľa a unicast adresou prijímateľa
- Sieť doručí práve danému prijímateľovi



## ■ Broadcast

- Častá forma komunikácie
- Jeden rámec zaslaný všetkým LAN staniciam
  - LAN zariadenia kopírujú rámec na všetky svoje porty



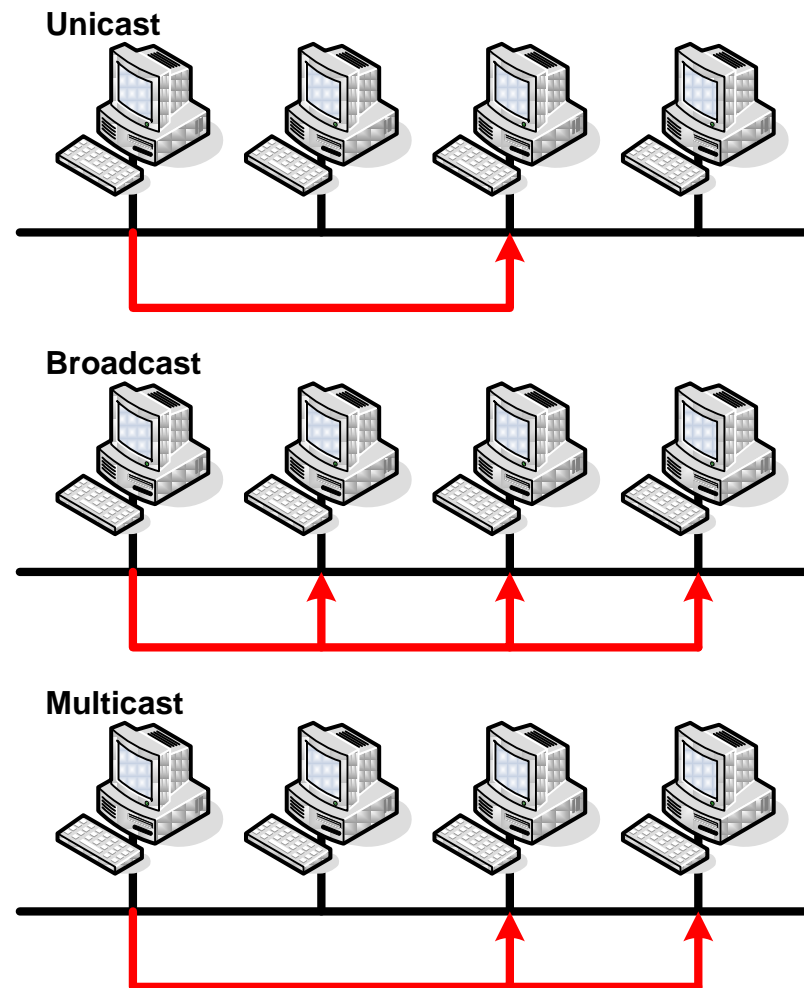
# Základy Ethernet-u - komunikácia

## ■ Broadcast cont.

- Odosielateľ
  - Vyplní rámec svojou unicast adresou a všetkých prijímateľov
  - Tzv. **Broadcast** adresa
    - FF-FF-FF-FF-FF-FF
- Sieť doručí všetkým uzlom

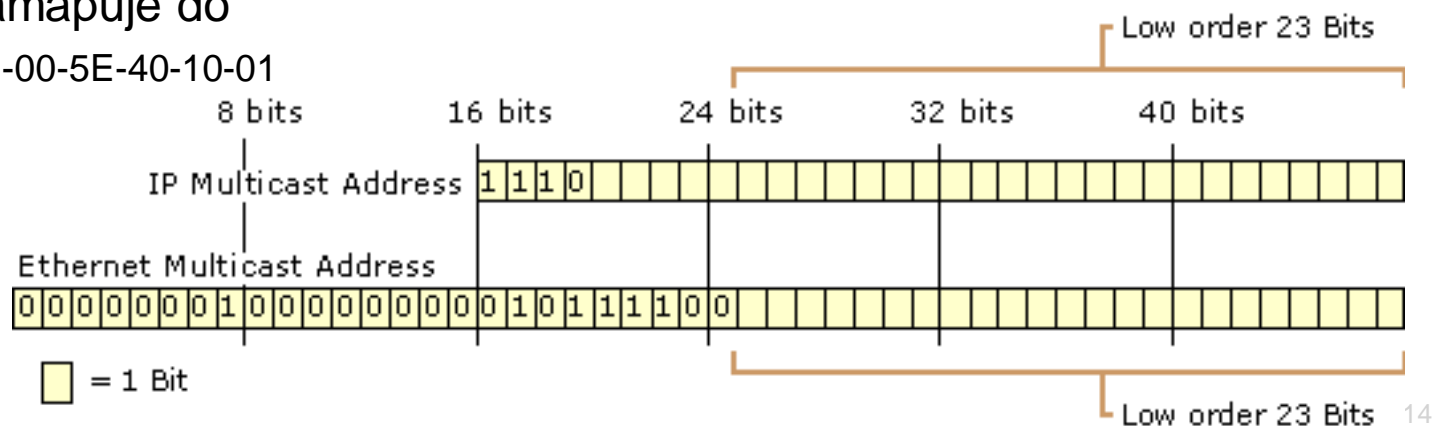
## ■ Multicast

- Skupinová komunikácia
- Jeden rámec zaslaný podskupine prijímateľov (nie všetkým)
- Sieť kopíruje rámec len na porty prijímateľov
- Odosielateľ
  - Vyplní rámec svojou unicast adresou a adresou pod skupiny prijímateľov



# Odvodzovanie mcast MAC adresy z IP mcast adresy

- Ethernet multicast rezervované adresy
  - 01-00-5E-00-00-00 do 01-00-5E-7F-FF-FF
    - 25 najvyšších bitov zo 48 je rezervovaných
- Pri mapovaní IPv4 mcast adresy sa mapuje najnižších 23 bitov
  - Sedem bitov druhého oktetu, celý tretí a štvrtý oktet
- Príklad
  - 224.192.16.1
    - 11100000.11000000.00010000.00000001
    - E0 -C0 -10 -01
  - Sa namapuje do
    - 01-00-5E-40-10-01



# Základy Ethernet-u - rámce

## Ethernet II

Preamble (8B)	Dest. Addr. (6B)	Source Addr. (6B)	Type (2B)	Data (46 - 1500B)	FCS (4B)
---------------	------------------	-------------------	-----------	-------------------	----------

## IEEE 802.3 LLC

Preamble (7B)	SFD (1B)	Dest. Addr. (6B)	Source Addr. (6B)	Length/Type (2B)	DSAP (1B)	SSAP (1B)	Control (1B)	Data (43 - 1497B)	FCS (4B)
---------------	----------	------------------	-------------------	------------------	-----------	-----------	--------------	-------------------	----------

## IEEE 802.3 LLC/SNAP

Preamble (7B)	SFD (1B)	Dest. Addr. (6B)	Source Addr. (6B)	Length/Type (2B)	DSAP (1B)	SSAP (1B)	Control (1B)	SNAP protocol ID (5B)	Data (38 - 1492B)	FCS (4B)
---------------	----------	------------------	-------------------	------------------	-----------	-----------	--------------	-----------------------	-------------------	----------

← LLC Header →

← SNAP Header →

- V súčasnosti existuje niekoľko druhov rámcov
- Najrozšírenejšie
  - Ethernet II
    - DIX štandard
    - Používaný v IP sieťach
      - Len jeden L3 protokol
  - IEEE 802.3 LLC
    - IEEE štandard
    - Používaný ak stanica má viac L3 protokolov
    - Nepoužíva sa pre IP
  - IEEE 802.3 LLC SNAP
    - Rozširuje 802.3 LLC – identifikujem viac protokolov ako  $2^8$  pomocou DSAP
    - Použitie aj pre IP

# Polia ethernet rámcov

- **Preamble: 7B IEEE802.3 or 8B (Ethernet)**
  - Bitová a rámcová synchronizácia
    - Opakujúca sa postupnosť jednotiek a núl
    - Časová synchronizácia
- **Start Of Frame Delimiter: 1B**
  - Oznamuje koniec časových informácií v preambule
    - Bitová vzorka: 10101011
- **Destination Address: 6B**
  - MAC adresa prijímateľa (adresáta)
- **Source Address: 6B**
  - MAC adresa odosielateľa
- **Length/Type: 2B**
  - **IEEE 802.3**
    - Ak hodnota < 0x600: Hodnota určuje dĺžku dátovej časti rámca
    - Ak hodnota > 0x600: Hodnota určuje typ sieťového protokolu



# Polia ethernet rámcov

- **Ethernet II**
  - **Type:** Hodnota určuje typ sieťového protokolu
  - Napr:
    - 0x0806: ARP protokol
    - 0x0800: IPv4 protokol
- **LLC Header**
  - **DSAP** (Destination Service Access Point): **1B**
    - Identifikuje cieľový L3 protokol
  - **SSAP** (Source Service Access Point): **1B**
    - Identifikuje zdrojový L3 protokol nesený v rámci
  - **Control: 1B**
    - Identifikuje typ LLC rámca
- **SNAP (SubNetwork Access Protocol) Header**
  - **Protocol ID: 5B**
    - Rozširuje možnosti na identifikáciu viac a ďalších protokolov ako umožňuje LLC

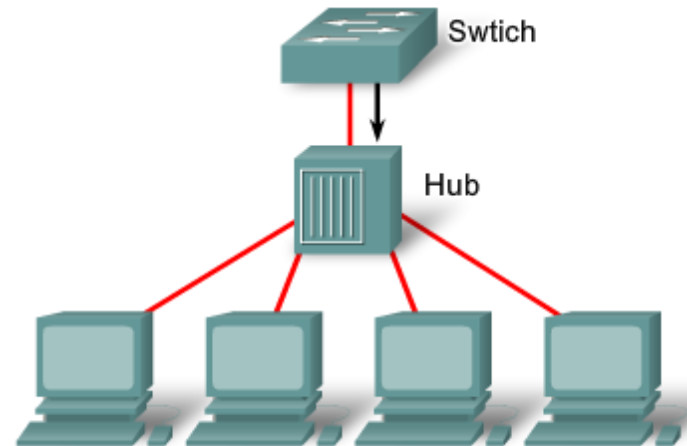
# Polia ethernet rámcov

- **Data: Variable Length**
  - Dátová časť
  - Dĺžka závisí od typu rámca
    - 46 až 1500 B dlhá
- **FCS (Frame Check Sequence): 4B**
  - Kontrolná suma (CRC) cez rámec
    - Nezahrňa sa preambula a SOF
  - Zabezpečenie voči chybám pri prenose

# Základy ethernetu - komunikácia

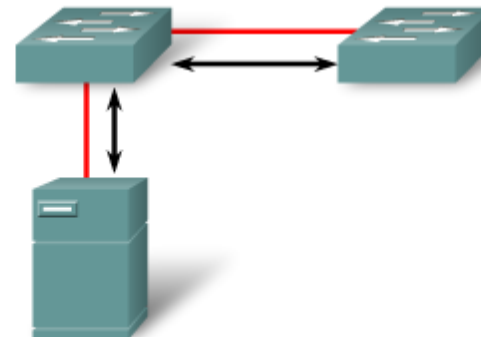
## Half Duplex (CSMA/CD)

- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

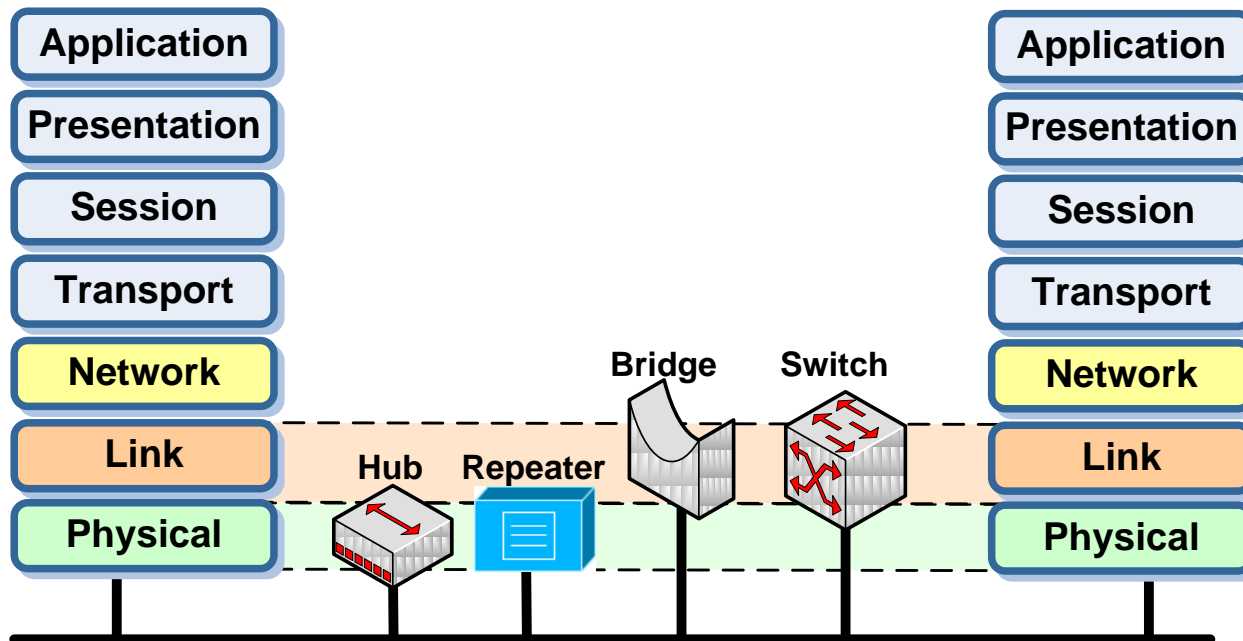


## Full Duplex

- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled



# Ethernet zariadenia



- **Repeater, Hub**
  - Pracujú na fyzickej vrstve (L1)
- **Bridge (Most), Switch (Prepínač), NIC (Sieťová karta)**
  - Pracujú na linkovej vrstve (L2)

# Činnost' Hub (swf)

- [Link – HTTP](#)
- [Link - PT](#)



Created using **Wink**

# Činnosť LAN prepínača

- L2 prepínače vykonávajú nasledovné funkcie
  - Učia sa MAC adresy z poľa zdrojovej adresy hlavičiek prichádzajúcich rámcov
  - Budujú a udržujú si tabuľku MAC adries a k nim asociovaných portov
  - Rámce prepínajú na základe L2 adries (hardware based bridging)
  - Broadcastové a multicastové rámce sú záplavovo posielané von cez všetky porty okrem portu na ktorom bol rámec prijatý
  - Rámce určené pre neznáme MAC adresy sú záplavovo posielané von cez všetky porty okrem portu na ktorom bol rámec prijatý
  - Bridges a switches komunikujú s inými L2 zariadeniami za účelom ochrany L2 slučiek
    - Nie je súčasť 802.3 štandardu
- Implementácia
  - ASIC (*application-specific integrated circuits*)
    - Hardvérovo vykonávané prepínanie

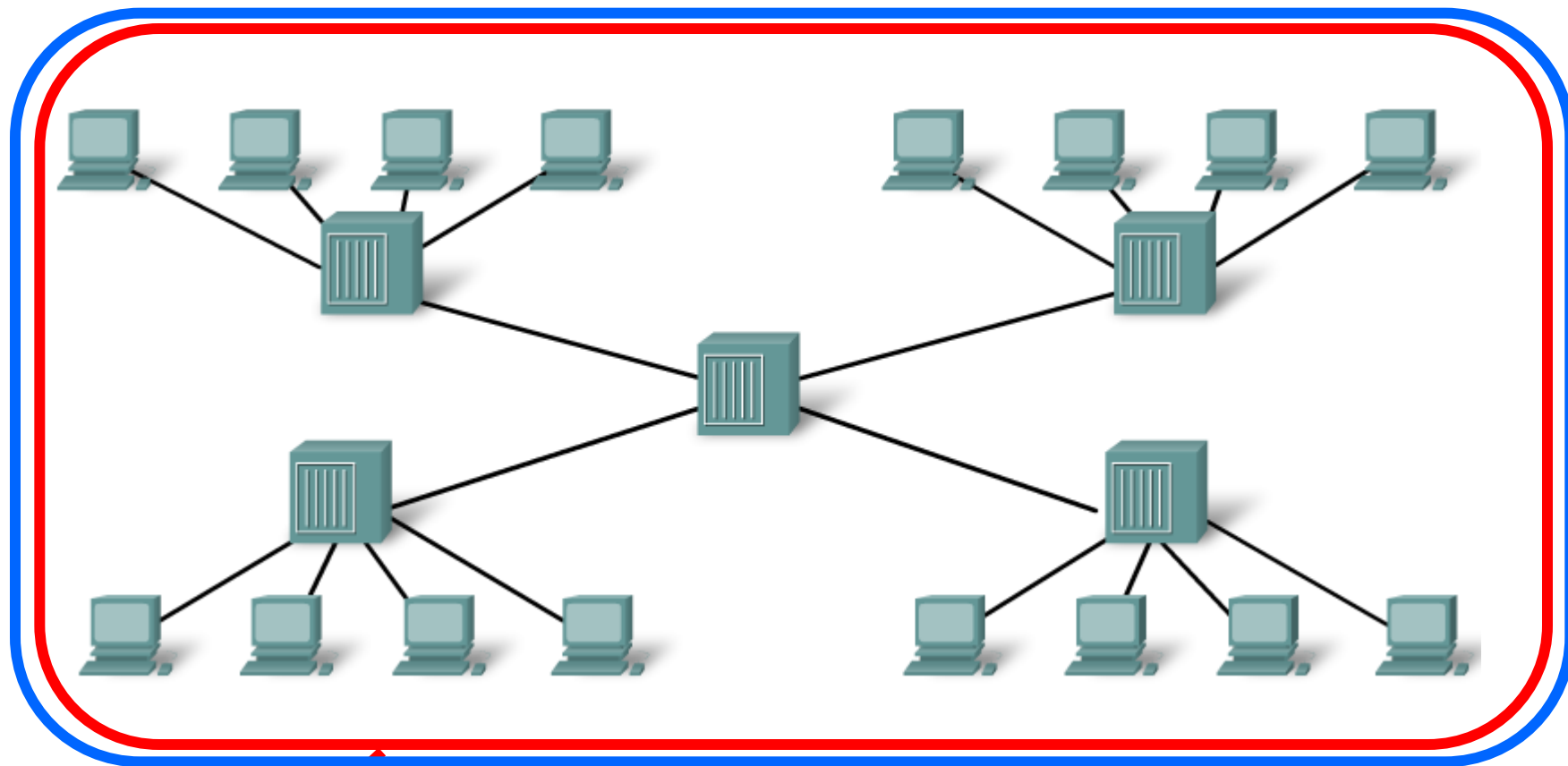
# Činnost LAN prepínača (swf)

- [Link – HTTP](#)
- Link - PT



Created using **Wink**

## Dizajn - Kolízna a broadcast doména - Hub



Kolízna  
doména

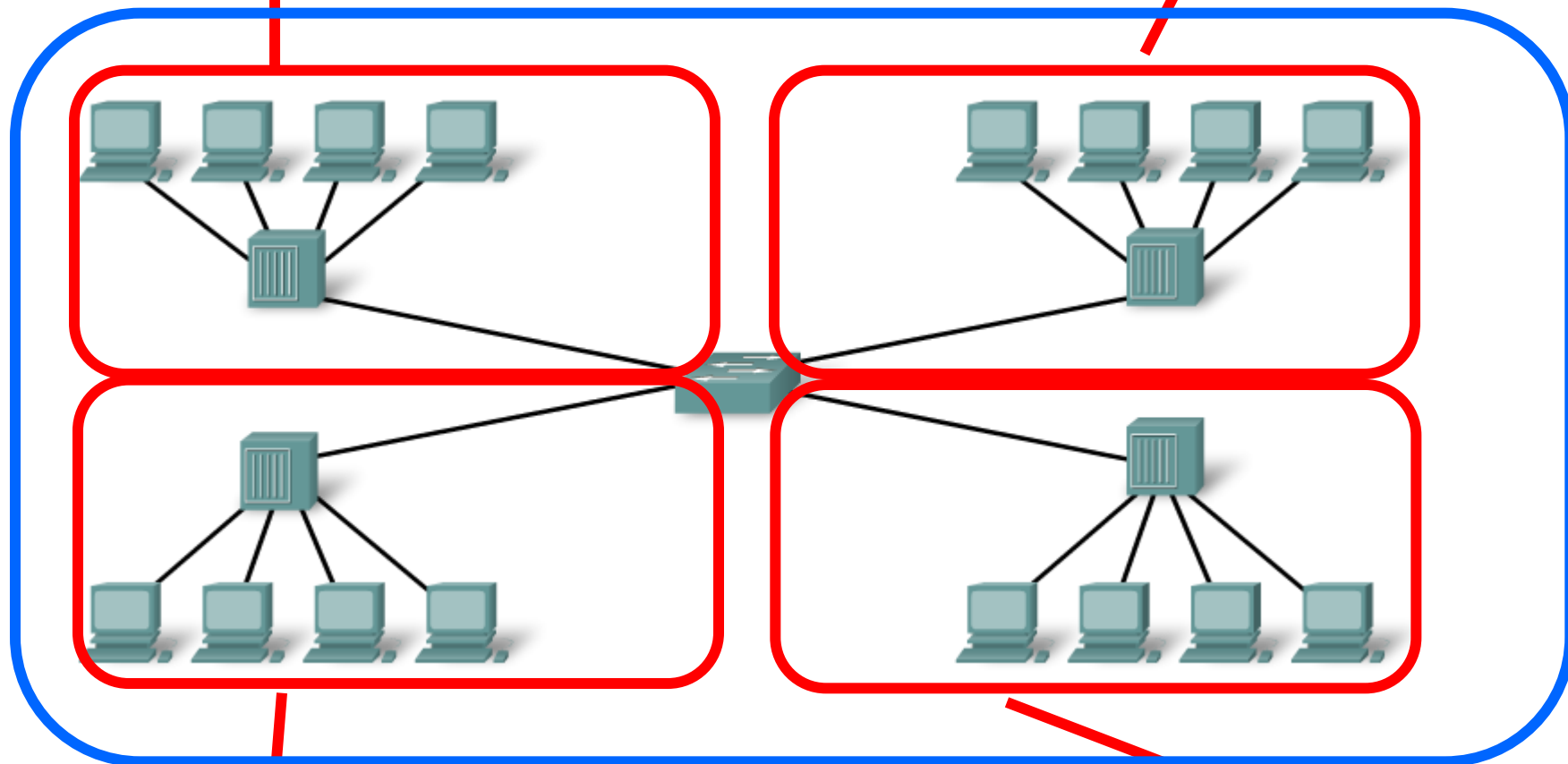
Broadcastová  
doména



Kolízna  
doména

Kolízna  
doména

## Dizajn - Kolízna a broadcast doména – Segmentácia na L2



Kolízna  
doména

Broadcastová  
doména

Kolízna  
doména

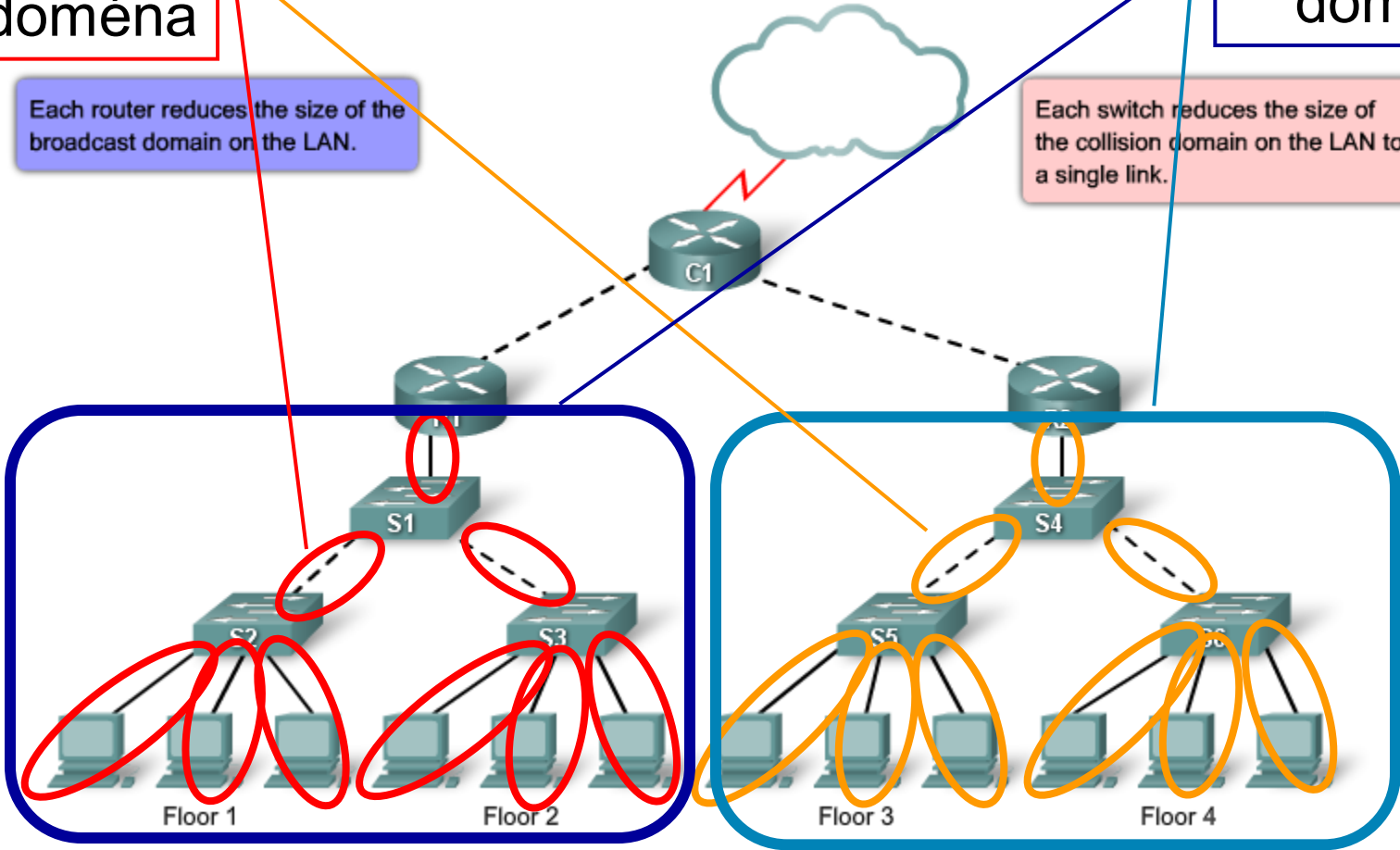
# Dizajn - Kolízna a broadcast doména – Segmentácia na L3

Kolízna doména

Each router reduces the size of the broadcast domain on the LAN.

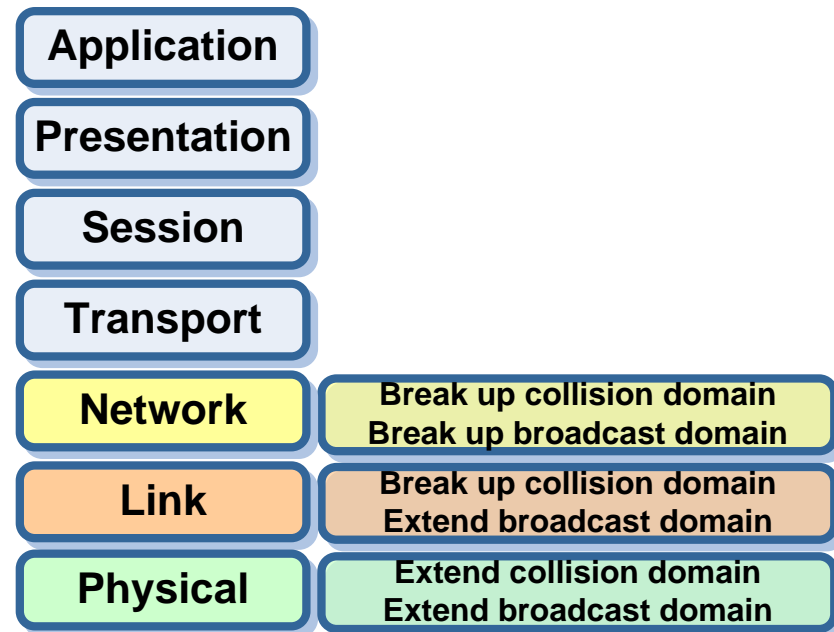
Broadcast doména

Each switch reduces the size of the collision domain on the LAN to a single link.



# Riešenie kolíznych a bcast domén

- Rozdelenia kolíznej domény
  - Použitie L2 alebo L3 zariadenia
- Rozdelenie broadcast domény
  - Použitie Virtuálnych LAN (VLAN)
  - Použitie L3 zariadenia
    - Smerovač, L3 prepínač



# Parametre, ktoré treba brať do úvahy pri dizajne

- Oneskorenie (delay, latency)
- Zabltenie

# End-to-End oneskorenie

- Doba prenesenia prvého bitu prvého paketu po dobu prijatia posledného bitu prvého paketu
- **Oneskorenie je tvorené**
  - **Propagation and serialization delay:**
    - oneskorenie média; pridáva linka
  - +
  - **Processing and queuing delay:**
    - spracovanie paketu v sieťovom prvku
- **Ťažko predpovedateľné!!!**
  - Podľa zaťaženia, počtu paketov, veľkosti paketov a pod.

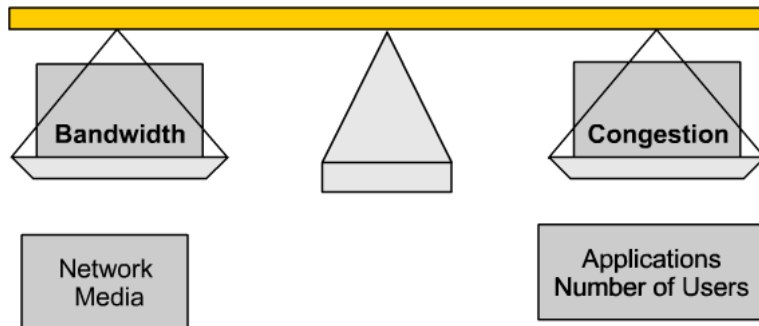
# End-to-End oneskorenie

- **Propagation delay:**
  - Čas prenesenia paketu linkou
  - Závisí na šírke pásma (priepustnosti) linky
- **Serialization delay:**
  - Doba umiestnenia bitov paketu na linku
- **Processing (forwarding) delay:**
  - Čas potrebný smerovačom/prpeínačom na prenesenie paketu zo vstupného rozhrania do výstupnej fronty výstupného rozhrania (zahŕňa aj spracovanie paketu)
  - Ovplyvňujú viaceré faktory:
    - Rýchlosť a vyťaženosť CPU, architektúra smerovača a pod.
- **Queuing delay:**
  - Čas, ktorý strávi paket vo výstupnej fronte smerovača
  - Závisí od:
    - Veľkosti a počtu paketov vo fronte pred ním
    - Na priepustnosti rozhrania (rýchlosti)

# Príklad: One-way delay

- Propagation delay:
  - ~5ms/1000km for fibre
- Switching / processing delay:
  - typically 10-20µs per packet
- Serialisation delay:
  - dependent upon line rate: 6ms for 1500 byte packet at 2Mbps, 80µs at STM-1, 1.25µs at STM-64
- Typicky:
  - Čím na vyššej vrstve zariadenie pracuje
  - Tým viac oneskorenia do cesty vnáša

# Zahltenie siete – faktory vplyvajúce naň



Balance depends on having enough bandwidth to meet the needs of the users and the applications.

- Nárast aplikácii so vzdialeným prístupom, alebo zdieľaním
  - Multitasking operačné systémy
    - Windows, UNIX, and Mac
  - Rýchlejšie desktop OS
    - Viac sieťovej aktivity





## LAN switching – prepínanie v LAN



# LAN prepínanie podľa priepustnosti

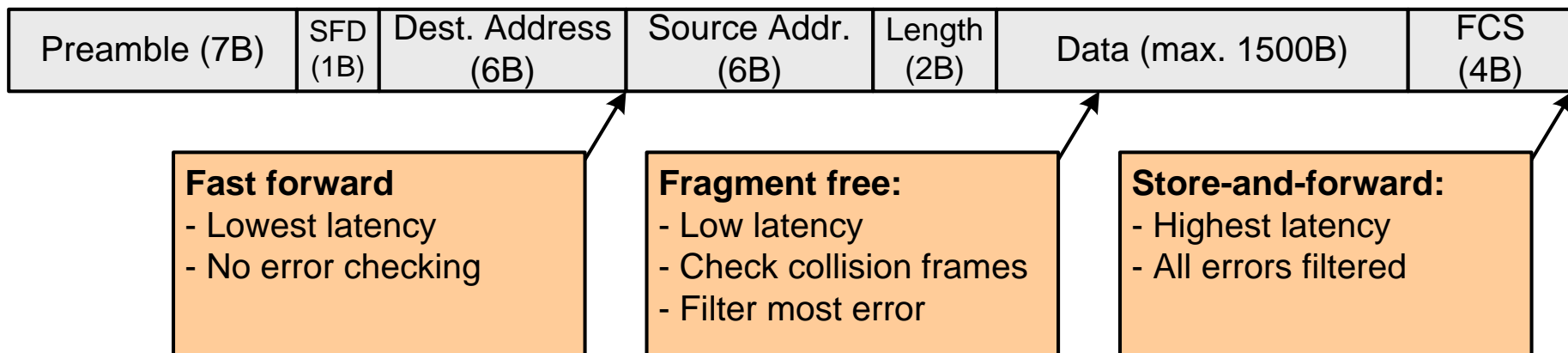
- LAN prepínače môžu byť charakterizované podľa priepustnosti pridelovanej na porty prepínača (**LAN bandwidth switching**)
  - **Symmetric switching** (symetrické prepínanie)
    - Poskytuje prepínanú, rovnako distribuovanú priepustnosť pre všetky porty
  - **Asymmetric switching** (asymetrické prepínanie)
    - Poskytuje mechanizmy prepínania medzi portami rôznych prenosových rýchlostí

# Vyrovnávacia pamäť

- Je použitá vyrovnávacia pamäť (**Memory buffer**)
  - Na uloženie a prepnutie rámca (store and forward)
  - Ak výstupný port je obsadený
    - Prebieha na ňom komunikácia
- Dva druhy použitia vyrovnávacích pamätí:
  - **Port-based memory buffering**
    - Rámce sú ukladané do fronty, ktorá je spojená so špecifickým vstupným portom
  - **Shared-memory buffering**
    - Všetky rámce a porty požívajú a zdieľajú jednu zdieľanú pamäť (memory buffer)
    - Rámce v pamäti sú dynamicky mapované na daný výstupný port.
    - Táto technika napomáha balansovať 10 a 100Mbps porty

# Prepínacie metódy rámcov

- LAN prepínač môže pracovať s viacerými prepínacími metódami
  - **Store and Forward switching**
    - Rámec je prijatý celý do pamäte prepínača kým sa prepne
  - **Cut through switching (Fast Forward / Fragment free)**
    - Rámec je prepínaný na výstup skôr ako je celý prijatý



# Store and Forward

- LAN prepínač používajúci Store and Forward:
  - Prijme a uloží do pamäte celý rámec
  - Skontroluje dĺžku rámca
    - Ak veľkosť rámca je **menšia ako 64 bytov – Runt** – rámec je **zahodený**
    - Ak veľkosť rámca je **väčšia ako 1518 bytov – Giant** - rámec je **zahodený**
  - Skontroluje CRC
    - Kontrola chybovosti
    - Ak je detekovaná neopraviteľná chyba rámec je **zahodený**
  - Prečíta cieľovú a zdrojovú MAC adresu
  - Aplikuje filtrovacie pravidlo (ak existuje)
  - Prehľadá prepínaciu tabuľku podľa cieľovej MAC a zistí výstupné rozhranie
  - Prepne rámec
- **Nevýhody**
  - Vnáša do prenosovej cesty oneskorenie
    - Celý rámec musí byť prijatý
    - Oneskorenie väčšie pri väčších rámcoch
- **Výhody:**
  - Detekcia chýb, prenášané sú len korektné rámce
  - Šetrenie kapacity siete

# Cut through

- LAN prepínač používajúci Cut through:
  - Prepne rámec na výstupný port skôr ako je prijatý celý rámec
  - Minimálne musí byť prijatá cieľová MAC adresa
- Cut through znižuje oneskorenie
  - Prepína rámce čo najskôr
- Cut through znižuje možnosti detekcie chybných rámcov
  - Nerobí sa CRC kontrola
  - Prenášajú sa aj chybné rámce
- Existujú dve varianty Cut through:
  - **Fast forward**
  - **Fragment free**

# Cut through

- **Fast forward:**

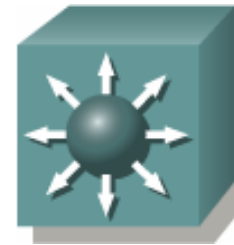
- Poskytuje najnižšie možné oneskorenie pri prepínaní rámcov
- Rámec je prepínaný okamžite po prečítaní **cieľovej MAC adresy** (prvých 6 bytov)

- **Fragment free:**

- Kolízne fragmenty rámcov (chybné rámce)
  - Bývajú zvyčajne menšie ako 64B
- Rámec je prepnutý, ak bolo prijatých **viac** ako 64B
  - Berie sa do úvahy predpoklad, že teda nie je potom kolízny

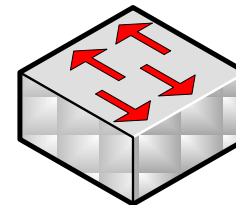
# MultiLayer switching

- Nová problematika
- Prepínanie môže nastať na L2 a L3 vrstve
  - Rozdiel na základe akej informácie sa prepína
- **Layer 2 switching**
  - Pracuje na L2 vrstve
  - Prepínanie na základe MAC adresy
  - Používajú prepínače a bridge
  - Flat siete (Fyzická segmentácia)
- **Layer 3 switching**
  - Pracuje na L3 vrstve
  - Prepínanie na základe IP adresy
  - Používajú smerovače a L3 prepínače
  - L2 prepínače so smerovacími modulmi
  - Fyzická aj logická segmentácia



## L3 switch

- Hardware-based packet forwarding
- High-performance packet switching
- High speed scalability
- Low latency
- Low cost per port
- Uses IP addresses
- Flow accounting
- Security
- QoS



## L2 switch

- Hardware based switching
- Wire speed performance
- Low latency
- Uses MAC addresses
- Low cost



# L3 routing

- L3 smerovače vykonávajú nasledovné funkcie
  - Pakety sú doručované medzi sieťami na základe L3 adres
  - Pre pakety vyberá optimálnu cestu daný router na základe jeho lokálnych informácií a doručuje ho susedovi po ceste
    - Smerovacie rozhodnutie zahŕňa prehľadanie smerovacej tabuľky na základe cieľovej siete, výber next hop smerovača a výstupného rozhrania
  - Výber optimálnej cesty môže byť podmienený mnohými možnosťami
  - Smerovače komunikujú s inými smerovačmi pomocou smerovacích protokolov.
- Smerovanie vykonávané CPU

# Smerovač vs. L3 prepínač

## ■ Smerovač

- Pracuje na L3
- Spracovanie každého paketu softvérovo
  - Smerovacím modulom
- Potom prepnutie

## ■ L3 prepínač

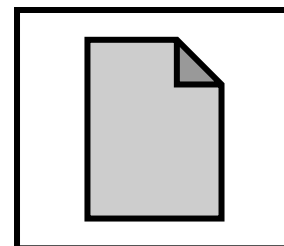
- Pracuje na L2/L3
- Spracovanie prvého paketu toku ako na smerovači
  - Smerovacím modulom
- Ďalšie rámce toho istého toku spracované v hardvéri
  - Použitie Application specific integrated circuit (ASIC) HW



# Konfigurácia prepínačov



P2



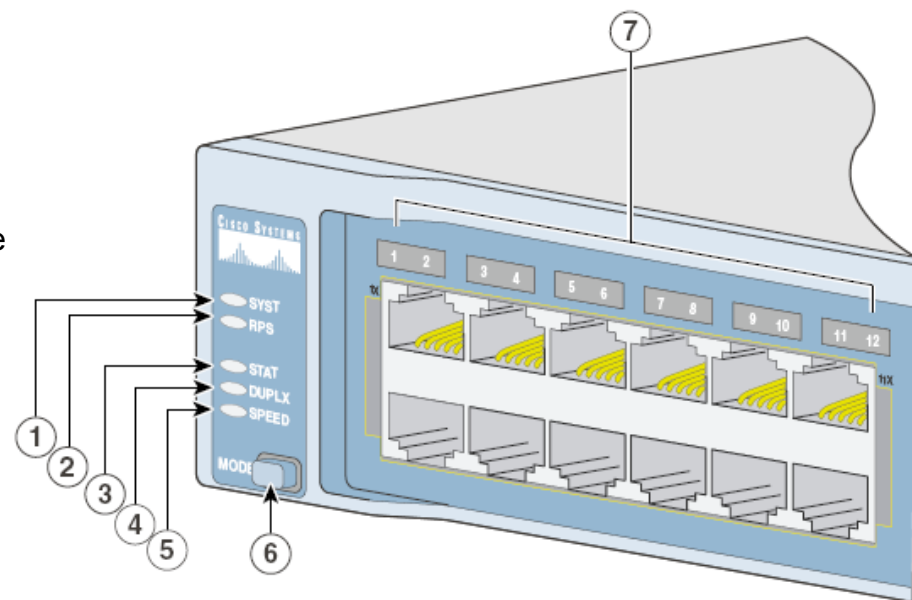
# Zapnutie prepínača

- Prepínače zvyčajne nemajú napájacie tlačidlo
- Zapínajú a vypínajú sa pripojením napájacieho kábla do napätia



# LED indikátory na prepínači

- Predný panel prepínača má sériu LED indikátorov pre zobrazenie systémovej aktivity a stavu zariadenia
- LED na prednom paneli:
  - **System LED**
    - Indikuje, či je zariadenie zapnuté a či správne pracuje
  - **Remote Power Supply (RPS) LED**
    - Indikuje použitie záložného napájacieho zdroja
  - **Port Mode LED**
    - Zobrazuje súčasný stav tlačidla Mode
    - Tlačidlom Mode je možné vybrať si, čo budú signalizovať LED nad jednotlivými portami prepínača
- Režimy tlačidla Mode
  - **Status LED**
    - Stav portu
  - **Duplex LED**
    - Režim duplexu (full alebo half)
  - **Speed LED**
    - Súčasná prenosová rýchlosť portu



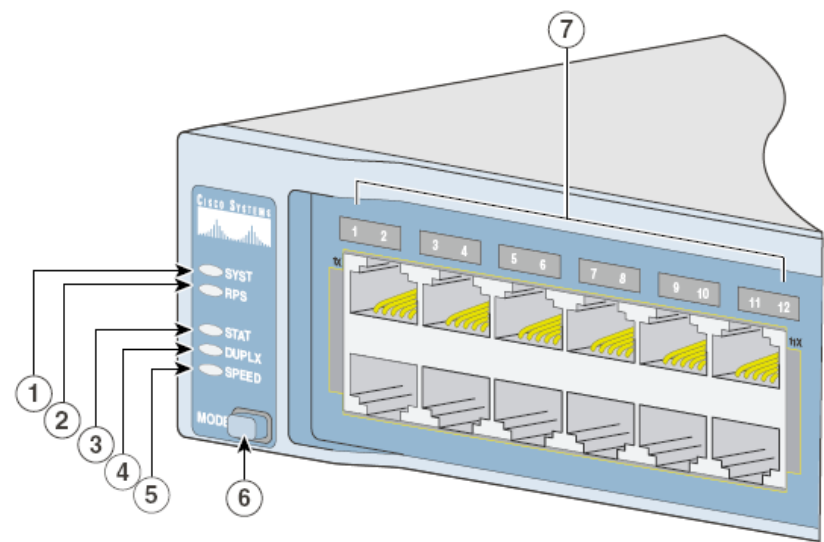
1	SYST LED	5	Speed LED
2	RPS LED	6	Mode button
3	Status LED	7	Port LEDs
4	Duplex LED		

# Význam LED pre jednotlivé porty

Port Mode	LED Color	Meaning
STAT (port status)	Off	No link, or port was administratively shut down.
	Green	Link present.
	Blinking green	Activity. Port is sending or receiving data.
	Alternating green-amber	Link fault. Error frames can affect connectivity, and errors such as excessive collisions, cyclic redundancy check (CRC) errors, and alignment and jabber errors are monitored for a link-fault indication.
	Amber	Port is blocked by Spanning Tree Protocol (STP) and is not forwarding data.  <b>Note</b> After a port is reconfigured, the port LED can remain amber for up to 30 seconds as STP checks the switch for possible loops.
	Blinking amber	Port is blocked by STP and is sending or receiving packets.
DUPLX (duplex)	Off	Port is operating in half duplex.
	Green	Port is operating in full duplex.
SPEED	<b>10/100/1000 ports</b>	
	Off	Port is operating at 10 Mb/s.
	Green	Port is operating at 100 Mb/s.
	Blinking green	Port is operating at 1000 Mb/s.
	<b>SFP module ports</b>	
	Off	Port is operating at 10 Mb/s.
	Green	Port is operating at 100 Mb/s.
	Blinking green	Port is operating at 1000 Mb/s.
		<b>Note</b> 1000BASE-T SFP modules can operate at 10, 100, or 1000 Mb/s in full-duplex mode or at 10 or 100 Mb/s in half-duplex mode in the Catalyst 2960 switches.

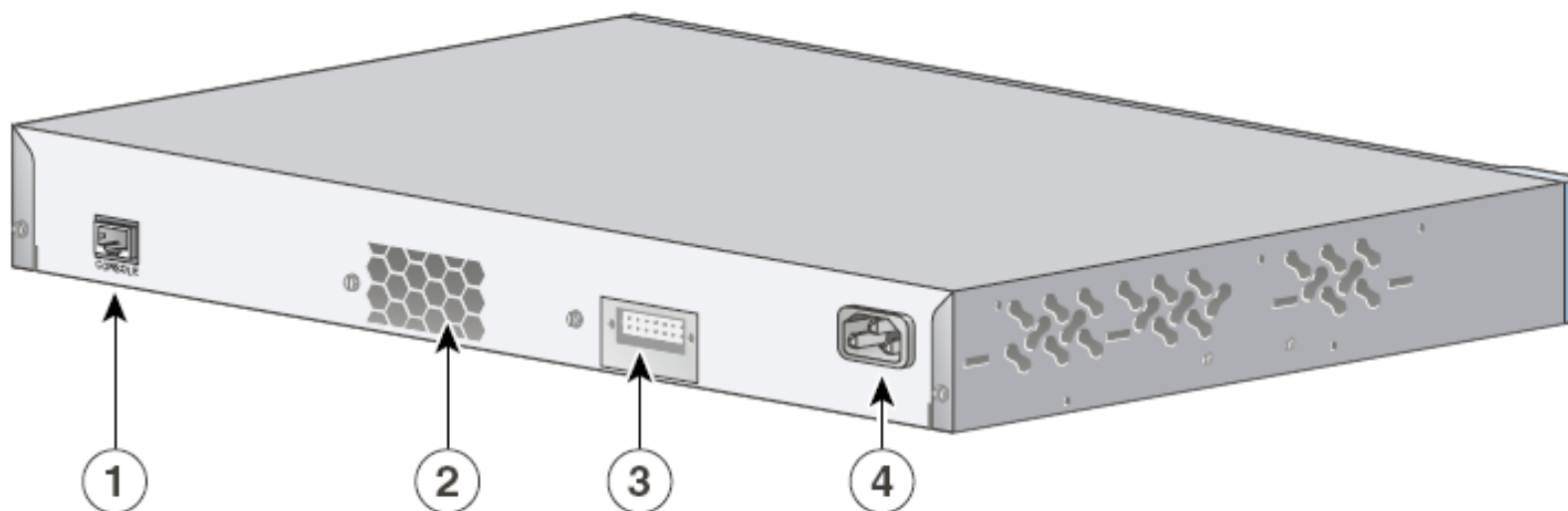
# Význam systémových LED počas štartu prepínača

- Prepínač po zapnutí prechádza sériou interných testov,
  1. Prepínač natiahne boot loader soft z ROM
  2. Boot Loader
    1. Vykoná nízkoúrovňovú inicializáciu CPU (registrov)
    2. Vykoná tzv. **power-on self test** (POST)
    3. Inicializuje flash systém
    4. Natiahne IOS
  3. IOS natiahne konfiguračný
- Ak System LED je **OFF**, prepínač nie je zapnutý
- Ak System LED je **zelená**, POST prebehol úspešne
- Ak System LED je **jantárová**, počas behu POST testov sa zistila chyba. POST chyba sa považuje za kritickú poruchu.



1	SYST LED	5	Speed LED
2	RPS LED	6	Mode button
3	Status LED	7	Port LEDs
4	Duplex LED		

# Cisco prístupový prepínač 2960-24TT-L – zadný pohľad – umiestnenie konzolového portu



<b>1</b>	RJ-45 console port	<b>3</b>	RPS connector
<b>2</b>	Fan exhaust	<b>4</b>	AC power connector





# Základy konfigurácie Cisco prepínačov



**2960-24TT-L**

# Základné informácie o ovládaní

- Prepínač má z hľadiska ovládania veľa vecí podobných smerovačom:
  - Spravuje sa cez CLI
  - Riadenie prístupových práv
    - Používateľský prístup
    - Privilegovaný prístup

```
Switch>enable  
Switch#disable  
Switch>
```

# Základné informácie o ovládaní

## ■ Systém nápovedy

```
Switch#?
```

```
Exec commands:
```

access-enable	Create a temporary Access-List entry
access-template	Create a temporary Access-List entry
archive	manage archive files
cd	Change current directory
clear	Reset functions
clock	Manage the system clock

```
... Output omitted ...
```

```
Switch#configure ?
```

memory	Configure from NV memory
network	Configure from a TFTP network host
terminal	Configure from the terminal
<cr>	

```
Switch#configure terminal
```

# Základné informácie o ovládaní

- Dopisovanie príkazov cez <TAB>
- Zadávanie príkazov
  - Šípka nahor, nadol, vľavo, vpravo, <Backspace>, Ctrl-A, Ctrl-E, Enter
- Štrukturovanie CLI
  - Používateľský mód
  - Privilegovaný mód
  - Globálny konfiguračný mód (režim) a podrežimy

```
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
Switch(config) #
```

# Základné informácie o ovládaní

## ■ Systém nápovedy chyby

```
Switch>configure terminal
```

```
^
```

```
% Invalid input detected at '^' marker.
```

```
... <neplatný príkaz pre daný režim>
```

```
Switch>show
```

```
% Type "show ?" for a list of subcommands
```

```
... <chýba časť príkazu za show>
```

```
Switch#show rumming-config
```

```
^
```

```
% Invalid input detected at '^' marker.
```

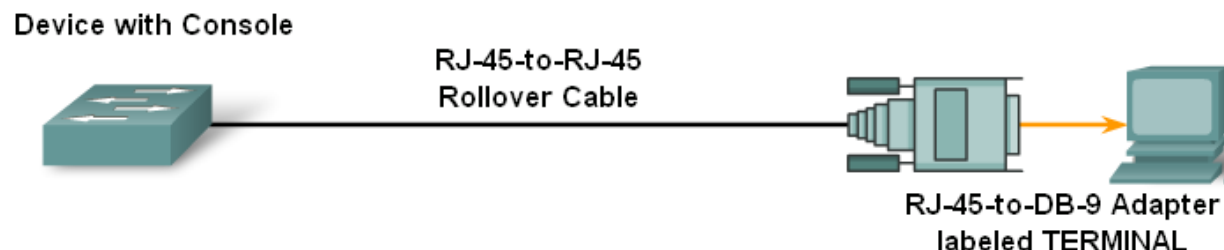
```
... <zle zadaná položka príkazu show>
```



## Práca s prepínačom



# Pripojenie na konzolu prepínača



## Prenosová cesta ako pri smerovači

- PCs require an RJ-45 to DB-9 or RJ-45 to DB-25 adapter.
- COM port settings are 9600 bps, 8 data bits, no parity, 1 stop bit, no flow control.
- This provides out-of-band console access.
- AUX switch port may be used for a modem-connected console.

- Postup, komunikačný softvér a nastavenia ako pri smerovači 1
- **Poznámka:** Konzolový port sa nachádza na zadnej strane prepínača
  - Bit 9600, Data bits 8, Parity none, Stop bits 1, Flow control none

# Pozorovanie výpisu pri bootovaní prepínača

- Prepínač vypisuje pri bootovaní hlášky na konzolu
- Získanie základných informácií o prepínači
  - Procesor, pamäte, rozhrania, IOS a pod

```
... Output omitted
Processor board ID FOC1136X2P0
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.

64K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:1D:E5:9B:2E:00
Motherboard assembly number     : 73-10390-04
Power supply part number        : 341-0097-02
Motherboard serial number       : FOC11361MFY
Power supply serial number      : DCA113483VD
Model revision number           : D0
Motherboard revision number     : A0
Model number                    : WS-C2960-24TT-L
System serial number            : FOC1136X2P0
Top Assembly Part Number        : 800-27221-03
Top Assembly Revision Number    : B0
Version ID                      : V03
CLEI Code Number                : COM3L00BRB
Hardware Board Revision Number  : 0x01
... Output omitted ...
```



# Overenie základnej konfigurácie prepínača

- **show running-config**
  - Zobrazí aktuálne používaný konfiguračný súbor
- **show interface**
  - Zobrazí stav všetkých rozhraní prepínača
- **show vlan**
  - Zobrazí informácie o Virtuálnych sieťach
- **show flash**
  - Zobrazí informácie o Flash pamäti
- **show version**
  - Zobrazí informácie o verzii používaného OS

# show running-config

```
Switch>enable
Switch#show running-config
Building configuration...

Current configuration : 1215 bytes
!
version 12.2
service config
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname Switch
!
... Output omitted ...
!
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
```

# show interface

```
Switch#show interfaces fastEthernet 0/1
FastEthernet0/1 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 001d.e59b.2e01 (bia
001d.e59b.2e01)
  MTU 1500 bytes, BW 100000 Kbit, DLY 100 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:55, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    692 packets input, 57874 bytes, 0 no buffer
    Received 30 broadcasts (0 multicasts)
    0 runs, 0 giants, 0 throttles
... Output omitted ...
```

# show vlan

```
Switch#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5, Fa0/6, Fa0/7, Fa0/8, Fa0/9, Fa0/10, Fa0/11, Fa0/12, Fa0/13, Fa0/14, Fa0/15, Fa0/16, Fa0/17, Fa0/18, Fa0/19, Fa0/20, Fa0/21, Fa0/22, Fa0/23, Fa0/24 Gi0/1, Gi0/2
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

... Output omitted ...

Default nastavenie na cisco prepínačoch

# show flash

```
Switch#show flash
```

```
Directory of flash:/
```

2	-rwx	616	Mar 1 1993 00:01:17 +00:00
vlan.dat			
7	drwx	192	Mar 1 1993 00:06:41 +00:00
c2960-lanbase-mz.122-35.SE5			

```
32514048 bytes total (24179200 bytes free)
```

# show version

```
Switch#show version
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(35)SE5,
RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Thu 19-Jul-07 20:06 by nachen
Image text-base: 0x00003000, data-base: 0x00D40000

ROM: Bootstrap program is C2960 boot loader
BOOTLDR: C2960 Boot Loader (C2960-HBOOT-M) Version 12.2(25r)SEE1, RELEASE
SOFTWARE (fc1)

Switch uptime is 1 hour, 1 minute
System returned to ROM by power-on
System image file is "flash:c2960-lanbase-mz.122-35.SE5/c2960-lanbase-
mz.122-35.SE5.bin"

cisco WS-C2960-24TT-L (PowerPC405) processor (revision D0) with
61440K/4088K bytes of memory.
Processor board ID FOC1136X2P0
Last reset from power-on
1 Virtual Ethernet interface
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
The password-recovery mechanism is enabled.
... Output omitted ...
```

# Začiatok konfigurácie prepínača

## - zmazanie cudzej konfigurácie

- Pred začiatkom práce ak tam ostala cudzia konfigurácia môžeme vymazať nastavenia prepínača nasledujúcim spôsobom
  - Potrebne vymazať všetky VLAN informácie vymazaním VLAN databázy vlan.dat z Flash pamäte
    - **delete vlan.dat**
    - **POZOR: nerobiť erase flash:**
      - **Zmaže IOS!!!!!!!**

```
Switch#show flash
Directory of flash:/

   2  -rwx           616   Mar 1 1993 00:01:17 +00:00  vlan.dat
   7  drwx           192   Mar 1 1993 00:06:41 +00:00  c2960-lanbase-
mz.122-35.SE5

32514048 bytes total (24179200 bytes free)
Switch#delete vlan.dat
Delete filename [vlan.dat]?
Delete flash:vlan.dat? [confirm]
Switch#
```

# Vymazanie prepínača pripojeného do väčšej živej siete

- Môže nastať situácia kedy zmazané VLAN (vlan.dat) sa nám neustále nanovo objavujú na prepínači (znovu naučením)

```
Switch#conf t
Switch(config)#
Switch(config)#interface range FastEthernet 0/1 -24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range GigabitEthernet
0/1 -2
Switch(config-if-range)#shutdown
15:45:59: %LINK-5-CHANGED: Interface GigabitEthernet0/2,
changed state to administratively down
Switch(config-if-range)#exit
Switch(config)#no vlan ID_VLANY
Switch(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
```



# Začiatok konfigurácie prepínača

## - zmazanie cudzej konfigurácie

- Vymaž štartovací konfiguračný súbor startup-config
  - `erase startup-config`
- Reštartuj prepínač
  - `reload`

```
Switch#erase startup-config
```

```
Erasing the nvram filesystem will remove all  
configuration files! Continue? [confirm]
```

```
[OK]
```

```
Erase of nvram: complete
```

```
Switch#reload
```

```
Proceed with reload? [confirm]
```

# Konfigurácia prepínača

- Odporúčaný postup pre konfiguráciu prepínača
  1. Nastavenie mena zariadenia
  2. Zabezpečenie prístupu k privilegovanému módu
    1. Použi heslo: **class**
  3. Zabezpečenie prístupu k prepínaču cez konfiguračné rozhrania pomocou hesiel
    1. Použi heslo: **cisco**
  4. Zabezpečenie IP prístupu na prepínač
  5. Konfigurácia bannerov
- Tento postup nie je záväzný, ale je osvedčený

# Nastavenie mena prepínača, ošetrenie prístupu k privilegovanému módu a prístupov

```
Switch#configure terminal
Enter configuration commands, one per line.  End with
CNTL/Z.
```

```
Switch(config)#hostname Tristan
Tristan(config)#enable secret TajneHeslo1234
Tristan(config)#
```

```
Tristan(config)#line console 0
Tristan(config-line)#password cisco
Tristan(config-line)#login
Tristan(config-line)#exit
```

```
Tristan(config)#line vty 0 15
Tristan(config-line)#password cisco
Tristan(config-line)#login
Tristan(config-line)#exit
```

```
Tristan(config)#
```

# Konfigurácia SSH prístupu

```
Switch(config)#username Meno password Heslo
```

! Doména musí byť zadefinovaná

```
Switch(config)#ip domain-name pepe.sk
```

```
Switch(config)# crypto key generate rsa
```

The name for the keys will be: Switch.pepe.sk

Choose the size of the key modulus in the range of 360 to 2048 for your General Purpose Keys. Choosing a key modulus greater than 512 may take a few minutes.

How many bits in the modulus [512]:

% Generating 512 bit RSA keys, keys will be non-exportable...[OK]

```
Switch(config)#ip ssh version 2
```

\*III 1 0:1:9.780: %SSH-5-ENABLED: SSH 1 has been enabled

```
Switch(config)#line vty 0 15
```

```
Switch(config-line)#transport input ssh
```

```
Switch(config-line)#login local
```

! Obnovenie telnet prístupu

```
Switch(config)#line vty 0 15
```

```
Switch(config-line)#transport input telnet
```

! Or

```
Switch(config-line)#transport input all
```

# Šifrovanie hesiel v konfigurácii

- Bez dodatočnej konfigurácie sú heslá v konfigurácii uvedené presne tak, ako sme ich zadali
  - Výnimkou je príkaz **enable secret**
- Toto je fragment konfiguračného súboru po nakonfigurovaní hesiel pre prístup k príkazovému riadku

```
line con 0
  password IneTajneHeslo
  login
line vty 0 15
  password IneTajneHeslo
  login
```

# Šifrovanie hesiel v konfigurácii

- Heslá sa takto ľahko kontrolujú, ale nie sú bezpečné – je ich možné vidieť
- Šifrovanie hesiel v konfigurácii je možné preto zapnúť osobitným príkazom v GKR

```
Tristan(config)#service password-encryption  
Tristan(config)#
```

- Ten istý fragment konfigurácie po zadaní tohto príkazu už vyzerá inak

```
line con 0  
password 7 11211C161B1D5A5E57  
login  
line vty 0 4  
password 7 123100041E045D5679  
login
```

# Zabezpečenie IP prístupu na prepínač

- Prečo má mať prepínač ako L2 zariadenie IP adresu?
  - Nastavenie IP adresy a def. gw umožňuje prístupovať k manažmentu prepínača cez telnet, web, ssh apod.
- IP adresa sa prideliuje tzv. virtuálnemu rozhraniu, volanému Virtual LAN (VLAN)
  - K VLAN rozhraniu by mal existovať priradený port pre prístup
- Na cisco prepínačoch default:
  - Každý prepínač dodávaný s VLAN1
  - Všetky porty priradené do VLAN1
  - VLAN1 – tzv. „**manažovacia VLAN**“
    - Lebo poskytuje IP prístup k manažmentu

# Zabezpečenie IP prístupu na prepínač - VLAN1

```
Tristan(config)#interface vlan 1
Tristan(config-if)#ip address 172.16.255.2 ?
    A.B.C.D   IP subnet mask

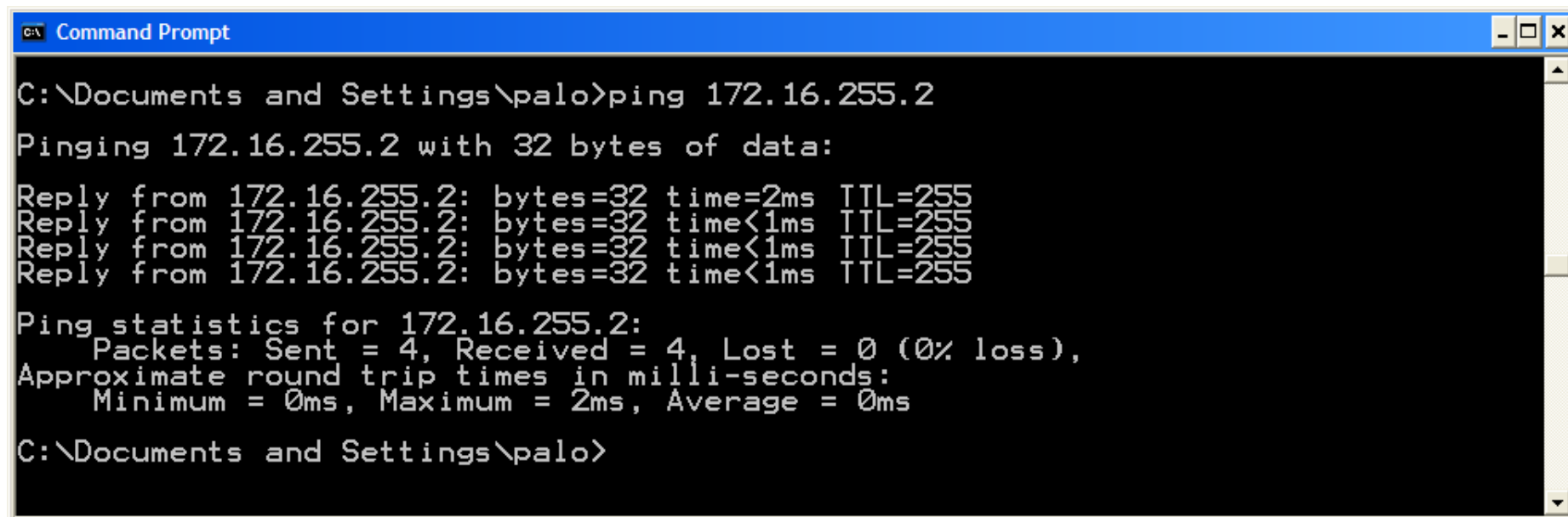
Tristan(config-if)#ip address 172.16.255.2 255.255.255.128
Tristan(config-if)#no shutdown
00:53:16: %LINK-3-UPDOWN: Interface Vlan1, changed state to up
00:53:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed
state to up
Tristan(config-if)#exit
Tristan(config)#ip default-gateway 172.16.255.1
Tristan(config)#
```

```
Tristan#show run
! Output omitted
!
interface Vlan1
    ip address 172.16.255.2 255.255.255.128
    no ip route-cache
!
ip default-gateway 172.16.255.1
```



# Overenie dostupnosti prepínača

- Ping, telnet z ethernetom pripojeného PC, smerovača



```
C:\> Command Prompt

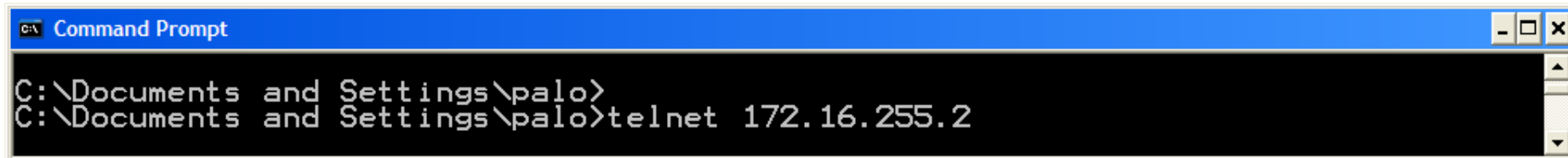
C:\Documents and Settings\palo>ping 172.16.255.2

Pinging 172.16.255.2 with 32 bytes of data:

Reply from 172.16.255.2: bytes=32 time=2ms TTL=255
Reply from 172.16.255.2: bytes=32 time<1ms TTL=255
Reply from 172.16.255.2: bytes=32 time<1ms TTL=255
Reply from 172.16.255.2: bytes=32 time<1ms TTL=255

Ping statistics for 172.16.255.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms

C:\Documents and Settings\palo>
```



```
C:\> Command Prompt

C:\Documents and Settings\palo>
C:\Documents and Settings\palo>telnet 172.16.255.2
```

# Zabezpečenie IP prístupu na prepínač – iná manažovacia VLAN – VLAN99

```
Tristan(config)#interface vlan 99
Tristan(config-if)#ip address 192.168.1.2 255.255.255.0
Tristan(config-if)#no shutdown
00:53:16: %LINK-3-UPDOWN: Interface Vlan99, changed state to up
00:53:17: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan99, changed
state to up
Tristan(config-if)#exit
Tristan(config)#ip default-gateway 192.168.1.1
Tristan(config)#interface fa 0/18
Tristan(config-if)#switchport mode access
Tristan(config-if)#switchport access vlan 99
```

Priradenie fyzického portu do vlan99

- Odporúčaný bezpečnostný postup – zmeniť manažovaciú VLAN z VLAN 1 na inú

# Overenie konfigurácie

```
Tristan# sh ip int brief
```

```
...  
FastEthernet0/17      unassigned      YES manual down      down  
FastEthernet0/18      unassigned      YES manual up         up  
FastEthernet0/19      unassigned      YES manual down      down  
...  
Vlan1                 unassigned      YES manual administratively down down  
Vlan99                192.168.1.2     YES manual up         up
```

```
Tristan#show run
```

```
! Output omitted
```

```
!
```

```
interface FastEthernet0/18  
  switchport access vlan 99  
  switchport mode access
```

```
!
```

```
! Output omitted
```

```
interface Vlan99  
  ip address 192.168.1.2 255.255.255.0  
!  
ip default-gateway 192.168.1.1
```

# Konfigurácia bannerov MOTD a login

```
Switch(config)#banner motd c
Enter TEXT message. End with the character 'c'.
*****
      ACCESS DENY!
*****
C
```

```
Switch(config)#banner login c
Enter TEXT message. End with the character 'c'.
*****
      Dna 30.1.2009 udrzba
*****
C
```

```
PC>telnet 192.168.1.1
Trying 192.168.1.1 ...

*****
      ACCESS DENY!
*****

*****
      Dna 30.1.2009 udrzba
*****

User Access Verification
Password:
```

# Výpis histórie príkazov

## Configure the Command History buffer

Cisco IOS CLI Command Syntax	
Enable terminal history. This command can be run from either user or privileged EXEC mode.	switch# <b>terminal history</b>
Configures the terminal history size. The terminal history can maintain 0 to 256 command lines.	switch# <b>terminal history size 50</b>
Resets the terminal history size to the default value of 10 command lines.	switch# <b>terminal no history size</b>
Disables terminal history.	switch# <b>terminal no history</b>

```
Switch#show history
```

```
ena
sh history
sh run
sh start
conf t
sh history
Switch#
```

# Spustenie http služby

- Spustenie interného web servera
  - Umožňuje manažment prepínača cez web prehliadač

```
Tristan(config)#ip http ?
  access-class          Restrict http server access by access-class
  active-session-modules Set up active http server session modules
  authentication         Set http server authentication method
  client                Set http client parameters
  max-connections       Set maximum number of concurrent http server
                        connections
  path                  Set base path for HTML
  port                  Set http port
  server                Enable http server
  session-module-list   Set up a http(s) server session module list
  timeout-policy        Set http server time-out policy parameters
```

```
Tristan(config)#ip http server
```

```
Tristan(config)#
```

# The GUI Interface

158.193.152.20 : Cisco Device Manager - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://158.193.152.20/xhome.htm

Ako začať Prehľad správ Getting Started Latest Headlines

Wireshark: Go deep. Pravda.sk - Homepage - Správy ktorý... 158.193.152.20 : Cisco Device Ma... NASA - Home

**Catalyst 2950 Series Device Manager - sw\_2950T\_kis**

Refresh Print Smartports Legend Help

Uptime: 19 weeks, 7 hours, 10 minutes

Next refresh in 5 seconds

View: Status

**Catalyst 2950 SERIES**

10Base-T/100Base-TX

10/100/1000Base-T

Move the pointer over the ports for more information.

**Contents**

- Dashboard
- Configure
  - Smartports
  - Port Settings
  - Express Setup
  - Restart / Reset
- Monitor
  - Trends
  - Port Status
  - Port Statistics
- Maintenance
  - Telnet
- Network Assistant

**Dashboard**

**Switch Information**

Host Name:	sw_2950T_kis
Product ID:	WS-C2950T-24
IP Address:	158.193.152.20
MAC Address:	00:06:52:58:01:00
Version ID:	B0
Serial Number:	FOC0524X0F5
Software:	12.1(22)EA8a
Contact:	Palo Segec
Location:	304

**Switch Health** [View Trends](#)

<b>Bandwidth Used</b>	<b>Packet Error</b>	<b>Fan</b>
0%	0%	OK

**Port Utilization** [View Trends](#) | [View Port Statistics](#)

# Nastavenie rýchlosti portu a duplexu

- Rozhrania prepínača sú default autosensed:
  - auto-speed
  - auto-duplex
- Existuje však možnosť manuálne to zmeniť

```
Tristan(config)#interface fa 0/1
Tristan(config-if)#speed ?
  10      Force 10 Mbps operation
  100     Force 100 Mbps operation
  auto    Enable AUTO speed configuration
```

```
Tristan(config-if)#speed 100
```

```
01:05:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down fu
```

```
01:05:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```

```
Tristan(config-if)#duplex full
```

```
01:05:37: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to down
```

```
01:05:39: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1,
changed state to up
```





# MAC tabuľka



# Budovanie a zobrazenie MAC tabuľky

- Prepínače sa dynamicky učia o výskyte MAC adries na svojich rozhraniach
  - Položky sa automaticky nulujú po 300 sekundách
- Zobrazenie MAC (CAM) tabuľky

```
Tristan# show mac-address-table
```

# Zobrazenie prepínacej tabuľky

- CAM tabuľka je prázdna

```
Tristan#show mac-address-table dynamic
```

```
Mac Address Table
```

```
-----  
Vlan      Mac Address      Type      Ports  
----      -
```

```
Tristan#
```

- Ping z PC na smerovač: >ping 172.16.255.1

```
Tristan#show mac-address-table dynamic
```

```
Mac Address Table
```

```
-----  
Vlan      Mac Address      Type      Ports  
----      -  
1         001c.2320.3a28    DYNAMIC    Fa0/2  
1         001e.1375.8fbd    DYNAMIC    Fa0/1
```

```
Total Mac Addresses for this criterion: 2
```

# Vymazanie prepínacej tabuľky

- Položky môžeme zmazať manuálne, ak nechceme čakať na vyradenie (age out)

```
Tristan#clear mac-address-table dynamic
```

- Or -

```
Tristan#clear mac-address-table dynamic ?
```

```
address      address keyword
```

```
interface    interface keyword
```

```
vlan         vlan keyword
```

```
<cr>
```

# Konfigurácia statickej MAC adresy

- Dôvody na pridelenie statickej MAC adresy na port?
  - Adresa sa nebude automaticky mazať z portu po age-out čase
  - Zvýšená bezpečnosť
    - Stanica s danou MAC adresou sa môže pripojiť len na daný port (musí), inde nie
      - Podmienené správaním prepínača, ktorý umožňuje mapovanie jednej konkrétnej MAC adresy len na jeden port (nie na viaceré)

# Konfigurácia statickej MAC adresy

```
Switch(config)# mac-address-table static <MAC-  
ADDRESS OF HOST> interface FastEthernet <ETHERNET  
NUMBER> vlan VLAN_NUMBER
```

```
Switch(config)# mac-address-table ?  
  aging-time      Set MAC address table entry maximum age  
  notification    Enable/Disable MAC Notification on the switch  
  static          static keyword  
Switch(config)# mac-address-table static 00e0.a3e8.8de7 interface  
Fa 0/1 vlan 1  
Switch(config)# exit  
%SYS-5-CONFIG_I: Configured from console by console  
Switch#sh mac-address-table  
      Mac Address Table  
-----  
Vlan    Mac Address      Type        Ports  
----    -  
1       00e0.a3e8.8de7   STATIC      Fa0/1  
Switch#
```

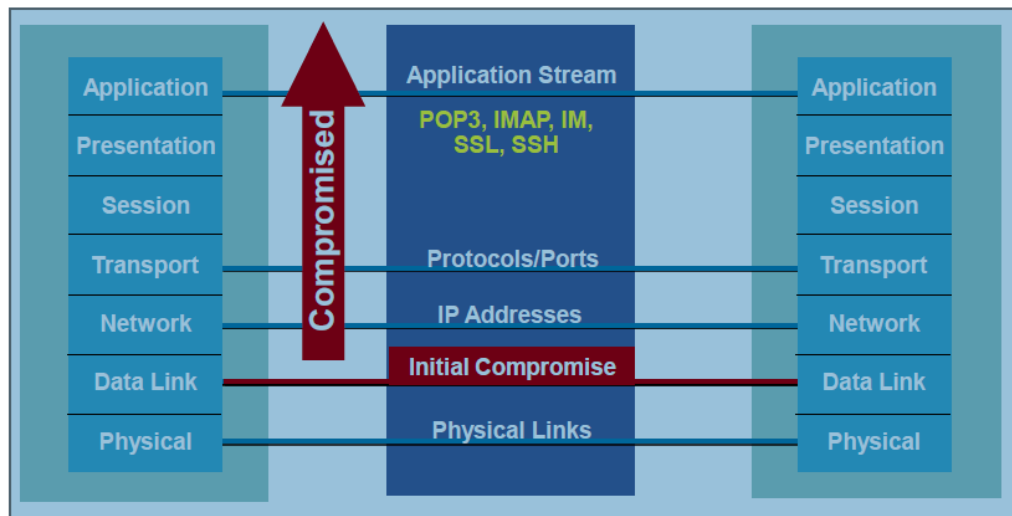


# Bezpečnostné útoky



# Zabezpečenie LAN infraštruktúry

- Bezpečnosť je väčšinou tlačaná na perimeter siete
  - Firewall, smerovač
    - Defaultne nastavené na zakázanie komunikácie, ktorú treba povoľovať
- Prepínače
  - Nastavané def. na povolenie komunikácie
  - Veľmi vhodné na útok zvnútra
    - Ak kompromitujem vnútro, zvyšok pôjde rýchlo
- Implementácia L2 security





# Zabezpečenie L2 infraštruktúry

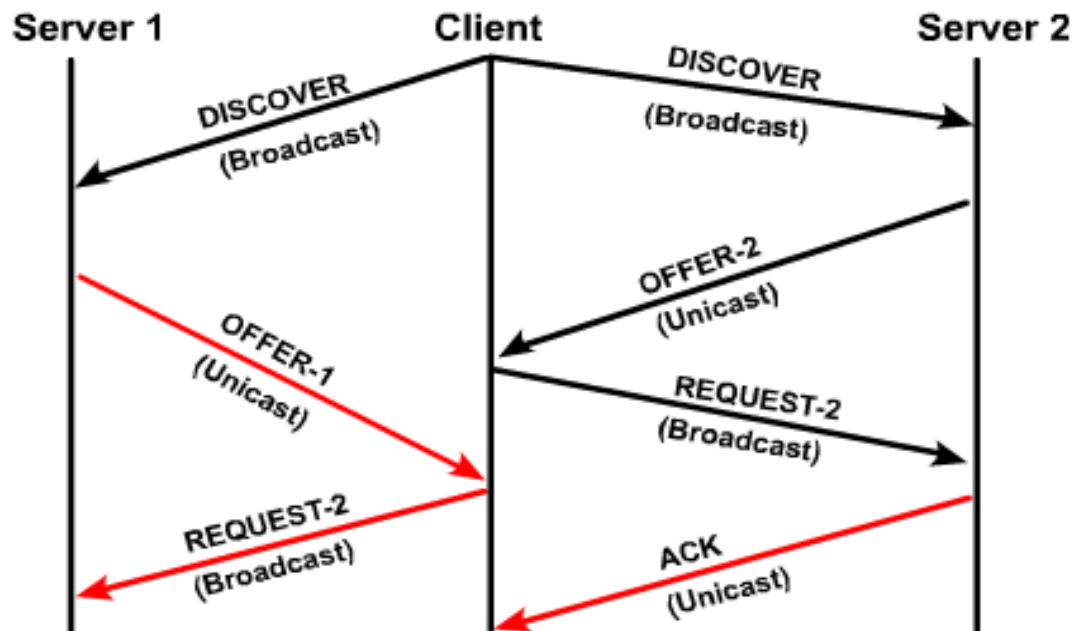
- Core
    - Nie je vhodné implementovať bezpečnostné mechanizmy
    - Musí rýchlo spracovávať pakety/rámce
  - Distribution
    - Vykonáva inter VLAN routing
    - Vhodné aplikovať packet filtering.
  - Access
    - Riadenie prístupu do siete na úrovni portu
  - Server farm
    - Poskytuje aplikačné služby
    - Vhodné aplikovať sieťový manažment
- 
- The diagram illustrates a multi-tier network architecture with four main layers, each with specific security considerations:
- Building Access:** This layer connects end-user devices (laptops and desktops) to the network. A security recommendation is to "Use switch port security to control access to the network."
  - Building Distribution:** This layer provides local aggregation and routing. A security recommendation is to "Use access lists to provide security."
  - Campus Core:** This layer handles high-speed forwarding and inter-VLAN routing. A security recommendation is to "Do not implement packet manipulation here."
  - Server Farm:** This layer contains critical services. A security recommendation is to "Use host- and network-based IPS, private VLANs, access control lists and secure password." The server farm includes:
    - Network Management:** Represented by a cloud icon.
    - Internal E-Mail:** Represented by a mail icon.
    - Corporate Server:** Represented by a server rack icon.
    - Cisco Unity CallManager:** Represented by a server rack icon.
- Additional security considerations for the Server Farm layer include:
- Use authentication server, OTPs, IPS and logging to minimize security threats.



# Útoky na DHCP



# DHCP činnost'



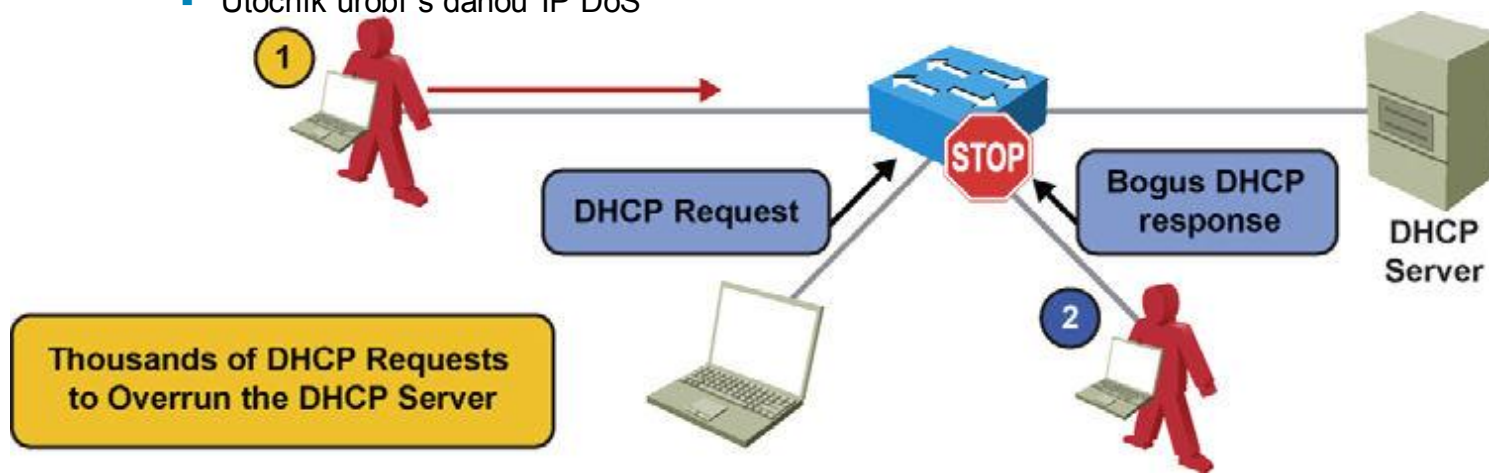
- DHCP client broadcasts DHCP DISCOVER packet on local subnet
- DHCP servers send OFFER packet with lease information
- DHCP client selects lease and broadcasts DHCP REQUEST packet
- Selected DHCP server sends DHCP ACK packet

# Vyčerpanie DHCP rozsahu

- Útok typu Denial of Service (DoS)
  - Nazývaný aj ***DHCP Starvation***
- Útočník sa snaží vyčerpať DHCP rozsah zapožičaním všetkých IP adries
  - Generuje množstvo DHCP discover správ s falošnými zdrojovými MAC adresami
    - yersinia
- Ochrana
  - Port Security
  - IP DHCP snooping limit rate

# DHCP spoofing – popis útoku

- DHCP spoofing je zapojenie neautorizovaného DHCP servera (rogue DHCP server) do siete
  - Môže sa jednať o zlomyseľnú aktivitu
    - Podvrhnutý DHCP Server odpovedá klientom nesprávnymi parametrami
  - Mnohokrát však ide skôr o nedbalosť – vlastný access point, notebook so sieťovým softvérom a podobne
- Útočník môže podvrhnúť:
  - Nesprávny default gateway
    - Útočník je Gateway (M-i-M)
  - Nesprávny DNS server
    - Útočník je DNS
  - Nesprávnu IP adresu
    - Útočník urobí s danou IP DoS





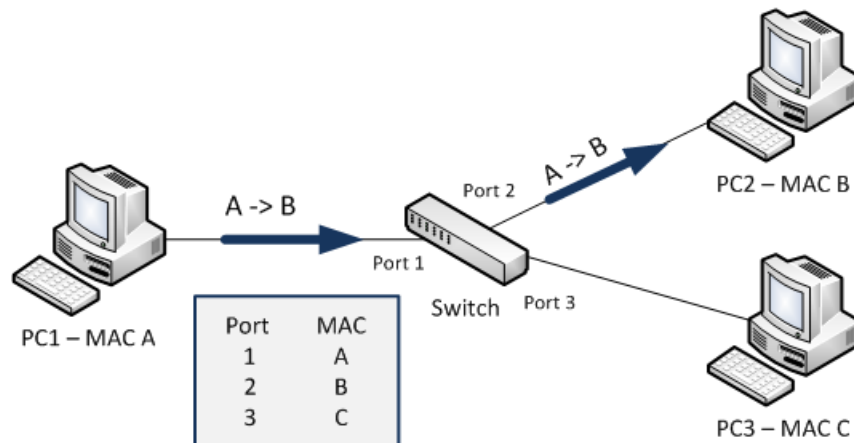
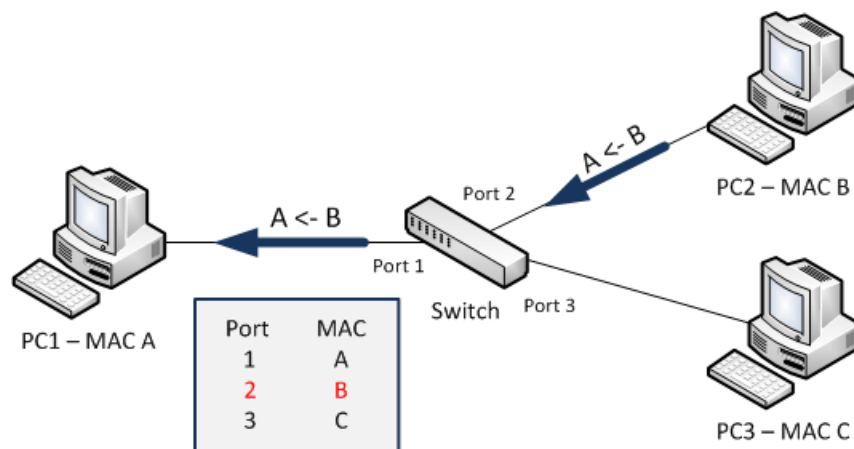
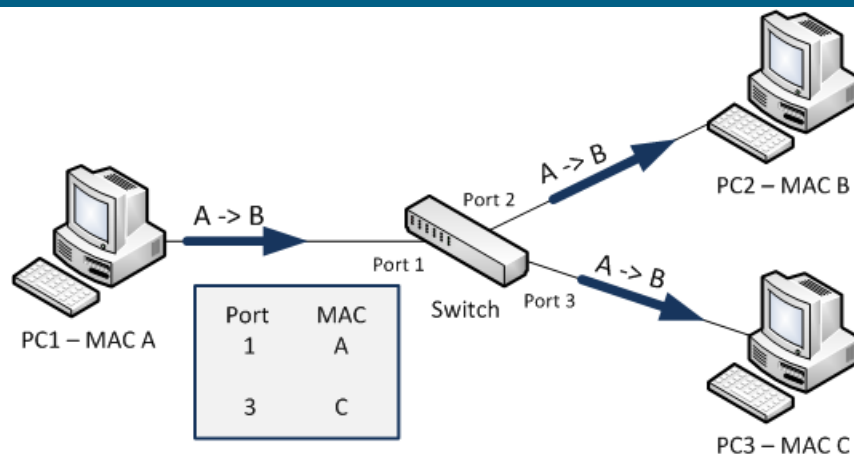
## Útoky na MAC/CAM



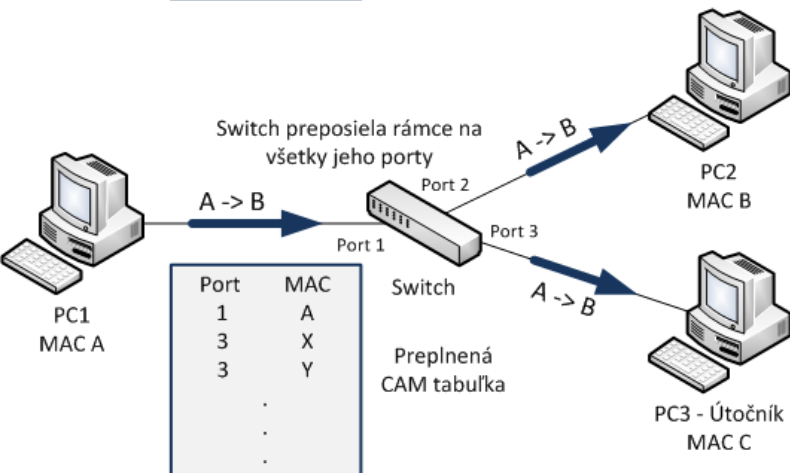
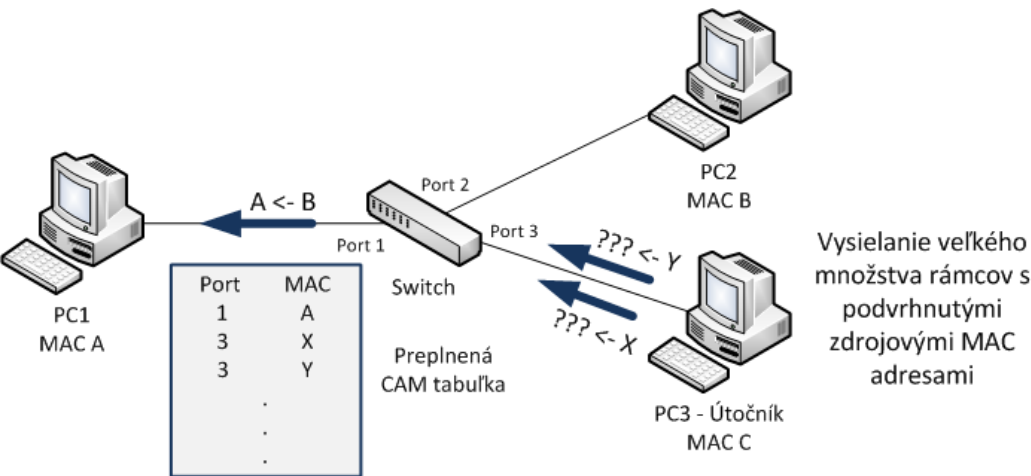
## Útoky na CAM

# CAM činnosť - Hrozba

- Bežný postup učenia sa L2 prepínača – Budovanie CAM
- Hrozba
  - Veľkosť CAM tabuľky a početnosť položiek v nej je **obmedzená**



# Útok na CAM – CAM overflow



- Útočník zasielaním veľkého počtu rámcov s rôznymi falošnými zdrojovými MAC adresami spôsobí zaplnenie CAM
  - Macof, yersinia
- Nové položky nie je kam písať
  - Útok často realizovaný pred začatím práce väčšiny
- Prepínač začne tieto rámce záplavovo šíriť



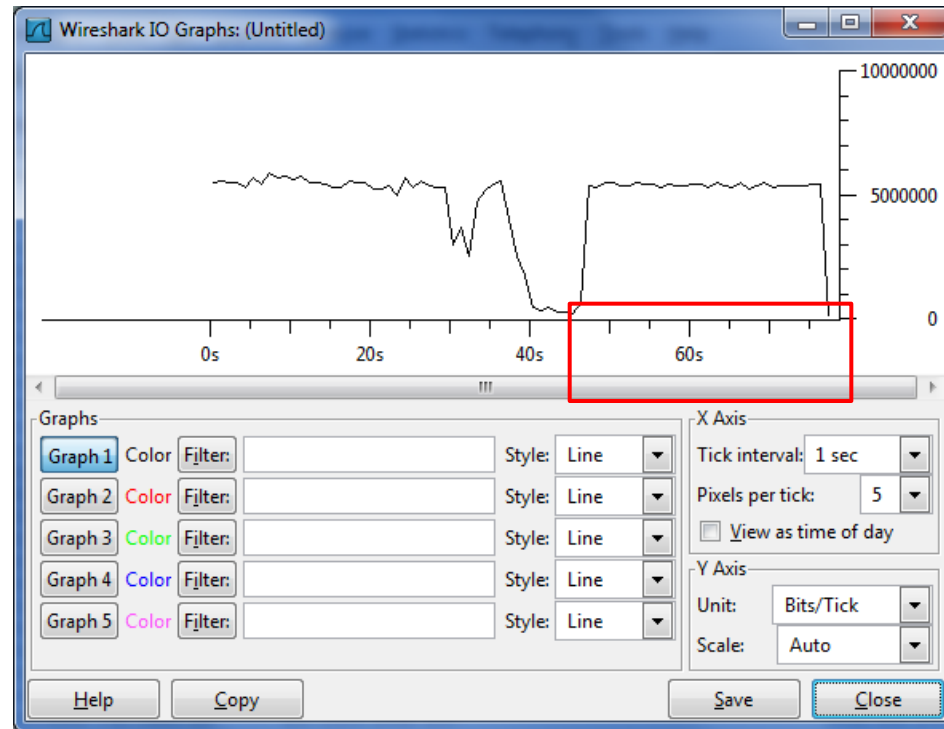
# Realizácia - macof

- Príkaz

macof -i eth0

- Agresívnejší režim (výpis do dev/null)

macof -i eth0 2>/dev/null



```
macof -i eth0
9:9e:3b:44:5:20 bd:35:99:23:1d:80 0.0.0.0.41911 > 0.0.0.0.3042: S 535014429:535014429(0) win 512
77:3e:75:40:79:fd 83:78:23:47:5e:6d 0.0.0.0.37577 > 0.0.0.0.16073: S 1654749076:1654749076(0) win 512
1d:2b:8c:65:14:ed 2:ce:2e:1a:8e:3e 0.0.0.0.39944 > 0.0.0.0.65129: S 902864306:902864306(0) win 512
9e:91:d4:77:97:b6 c3:41:e8:33:c9:e2 0.0.0.0.17930 > 0.0.0.0.23148: S 73203385:73203385(0) win 512
f0:78:1f:59:2:82 86:4e:ff:40:b6:11 0.0.0.0.17666 > 0.0.0.0.555: S 1988508690:1988508690(0) win 512
b9:8a:3e:6d:41:c3 6f:40:de:4b:28:60 0.0.0.0.61444 > 0.0.0.0.40408: S 370775209:370775209(0) win 512
d7:ea:a7:8:35:34 66:b0:b8:49:2a:69 0.0.0.0.24670 > 0.0.0.0.56585: S 115082340:115082340(0) win 512
ee:73:27:7b:4f:dd 23:83:53:62:9a:fe 0.0.0.0.29291 > 0.0.0.0.46088: S 1238142262:1238142262(0) win 512
df:56:62:7c:fa:4e e0:a2:65:45:8f:df 0.0.0.0.35816 > 0.0.0.0.40744: S 224492172:224492172(0) win 512
af:ba:0:28:6c:7b cb:34:15:36:ce:dc 0.0.0.0.36257 > 0.0.0.0.17653: S 1640037673:1640037673(0) win 512
2a:1f:3f:9:ff:cd 85:a:ad:6b:e1:d 0.0.0.0.58040 > 0.0.0.0.16133: S 2028675158:2028675158(0) win 512
```

# CAM table - Preplnenie

- Ak nastane preplnenie CAM tabuľky
  - Prevádzka bez položky v CAM je floodovaná na všetky porty danej VLAN
- Tento útok preplní CAM tabuľky aj ostatných prepínačov

10.1.1.22 -> (broadcast) ARP C Who is 10.1.1.1, 10.1.1.1 ?

10.1.1.22 -> (broadcast) ARP C Who is 10.1.1.19, 10.1.1.19 ?

10.1.1.26 -> 10.1.1.25 ICMP Echo request (ID: 256 Sequence number: 7424) ← OOPS

10.1.1.25 -> 10.1.1.26 ICMP Echo reply (ID: 256 Sequence number: 7424) ← OOPS



# Port security



# Port security

- Stáva sa, že príde nepovolaná osoba a len tak si pripojí svoj notebook alebo počítač do voľnej zásuvky
  - Nechránené porty sú potenciálnym miestom pre vstup nepovolaných osôb alebo zariadení do siete
- Cisco prepínače ponúkajú funkciu, ktorá sa volá **port security**
- Pomocou nej je možné
  - Obmedziť počet zariadení, ktoré môžu byť pripojené k jednému rozhraniu prepínača
  - Definovať zoznam MAC adries staníc, ktoré smú byť pripojené k danému rozhraniu prepínača
  - Definovať, čo sa stane, ak dôjde k porušeniu niektorého z týchto bezpečnostných pravidiel

# Port Security

- Funkcia Port Security umožňuje na porte definovať zoznam tzv. bezpečných (secure) MAC adries
  - Zabezpečený port povolí komunikovať len staniciam, ktorých MAC adresa sa nachádza v zozname
- Bezpečné adresy môžu byť troch druhov:
  - **Static secure MAC**: manuálne nakonfigurovaná adresa
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
  - **Dynamic secure MAC**: dynamicky získaná adresa z CAM
    - Nachádza sa len v CAM tabuľke
    - Po odpojení portu alebo reštarte prepínača sa stráca
  - **Sticky secure MAC**: hybrid medzi statickou a dynamickou adresou
    - Získava sa dynamicky, no prepínač automaticky vygeneruje záznam do bežiackej konfigurácie
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie

# Port Security

- Na porte je možné definovať maximálny počet bezpečných adries
  - Statické adresy sa započítavajú do počtu bezpečných adries
  - Prepínač automaticky pridá každú novú neznámu MAC adresu do zoznamu bezpečných adries ako *dynamickú* resp. *sticky*
  - Ak by sa však pridaním novej adresy prekročil maximálny počet bezpečných adries, nastáva tzv. **porušenie bezpečnosti** (**security violation**)
- Na bezpečnostné porušenie možno zareagovať trojakým spôsobom
  - **Protect**: rámec s nepovolenou MAC adresou sa zahodí
  - **Restrict**: rámec s nepovolenou MAC adresou sa zahodí a zároveň sa incident zaznamená (hláška na konzolu, syslog, SNMP trap...)
  - **Shutdown**: port sa pri prijatí rámca s nepovolenou MAC adresou automaticky uvedie do stavu err-disabled

# Konfigurácia Port Security

- Port Security sa konfiguruje individuálne na prepínaných portoch
- Odporúčany postup:
  - Port nastaviť do režimu „access“ alebo „trunk“
    - Nevyhnutné – Port Security nie je podporovaná na dynamických portoch
  - Nastaviť maximálny povolený počet MAC adries
    - Nepovinné, predvolený počet je 1
  - Definovať statické bezpečné adresy, prípadne sticky learning
    - Nepovinné
  - Určiť reakciu pri porušení bezpečnosti
    - Nepovinné, predvolená reakcia je shutdown
  - Určiť spôsob expirácie bezpečných adries
    - Nepovinné. Bez dodatočného nastavenia statické a sticky adresy neexpirujú vôbec, dynamické expirujú až pri odpojení portu
  - Aktivovať port security
    - Nevyhnutné a často prehliadnuté!

# Konfigurácia a kontrola Port Security

```
Sw(config)# interface fa0/2
Sw(config-if)# switchport mode access
Sw(config-if)# switchport port-security maximum 5
Sw(config-if)# switchport port-security mac-address 001c.2320.3a28
Sw(config-if)# switchport port-security violation restrict
Sw(config-if)# switchport port-security aging time 10
Sw(config-if)# switchport port-security
```

```
Sw# show port-security
```

Secure Port	MaxSecureAddr (Count)	CurrentAddr (Count)	SecurityViolation (Count)	Security Action
-------------	--------------------------	------------------------	------------------------------	-----------------

-----

Fa0/2	5	3	0	Restrict
-------	---	---	---	----------

-----

Total Addresses in System (excluding one mac per port) : 2

Max Addresses limit in System (excluding one mac per port) : 8192



# Konfigurácia a kontrola Port Security

```
Sw# show port-security address
```

## Secure Mac Address Table

Vlan	Mac Address	Type	Ports	Remaining Age (mins)
1	01c.2320.3a28	SecureConfigured	Fa0/2	-
1	00e0.4c3b.b787	SecureDynamic	Fa0/2	8
1	0200.0000.0001	SecureDynamic	Fa0/2	8

```
Total Addresses in System (excluding one mac per port) : 2
```

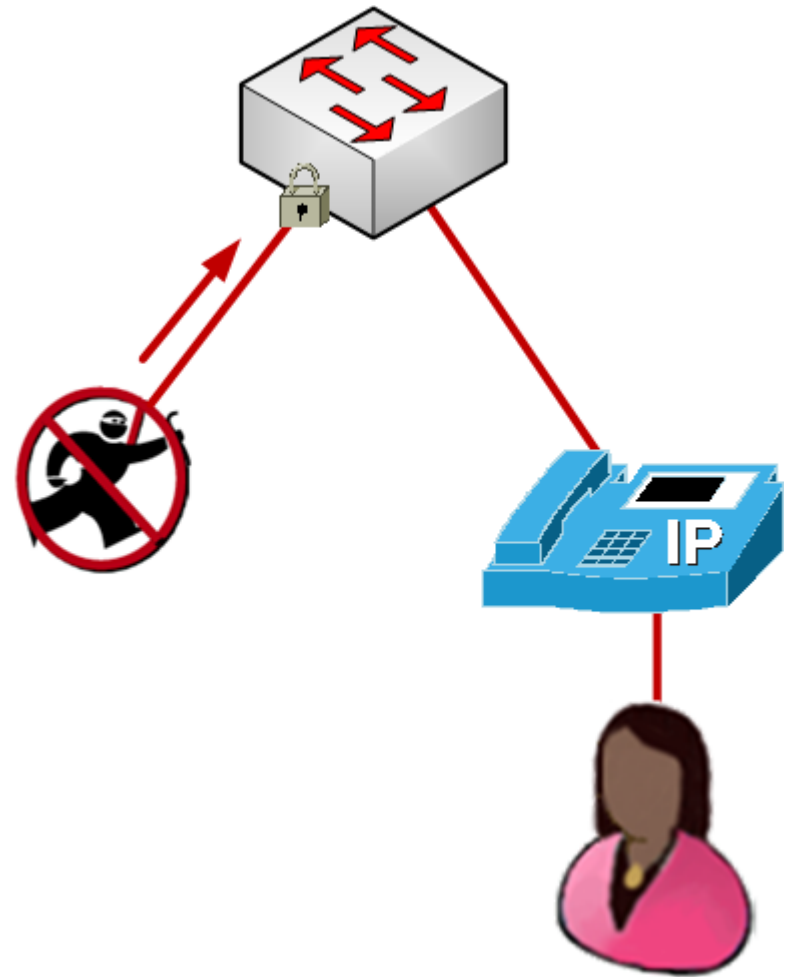
```
Max Addresses limit in System (excluding one mac per port) : 8192
```

# Konfigurácia a kontrola Port Security

```
Sw# show port-security interface fa0/2
Port Security                : Enabled
Port Status                  : Secure-up
Violation Mode                : Restrict
Aging Time                    : 10 mins
Aging Type                    : Absolute
SecureStatic Address Aging    : Disabled
Maximum MAC Addresses         : 5
Total MAC Addresses           : 3
Configured MAC Addresses      : 1
Sticky MAC Addresses          : 0
Last Source Address:Vlan      : 00e0.4c3b.b787:1
Security Violation Count      : 0
```

# Port security s VoIP

- VoIP telefóny môžu používať 2 až 3 MAC adresy
  - Podľa HW
  - Ak používajú CDP tak tri
  - Ak nepoužívajú CDP tak dve
- Zváž akciu pri porušení na
  - Vhodné **Restrict**
  - Akceptovateľné shutdown (podľa politik)
- Cieľom nie je riadiť prístup ale ochrániť službu a prepínač



# Zálohovanie konf. úborov

## Backup and Restore Switch Configurations

Cisco IOS CLI Command Syntax	
Formal version of Cisco IOS copy command. Confirm the destination file name. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	S1# <b>copy system:running-config flash:startup-config</b> Destination filename [ startup-config]?
Informal version of the copy command. The assumptions are that the running-config is running on the system and that the startup-config file that will be stored in flash NVRAM. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	S1# <b>copy running-config startup-config</b> Destination filename [ startup-config]?
Backup the startup-config to a file stored in flash NVRAM. Confirm the destination file name. Press the Enter key to accept and use the Ctrl+C key combination to cancel.	S1# <b>copy startup-config flash:config.bak1</b> Destination filename [ config.bak1]?

# Copying IOS from TFTP Server

```
ALSwitch#copy tftp flash
Address or name of remote host []? 192.168.1.3
Source filename []? c2950-c3h2s-mz.120-5.3.WC.1.bin
Destination filename [c2950-c3h2s-mz.120-5.3.WC.1.bin]? [enter]
%Warning: There is a file already existing with this name

Do you want to over write? [confirm] [enter]
Accessing tftp://192.168.1.3/c2950-c3h2s-mz.120-5.3.WC.1.bin...
Loading c2950-c3h2s-mz.120-5.3.WC.1.bin from 192.168.1.3 (via VLAN1):
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1674921 bytes]
1674921 bytes copied in 51.732 secs (32841 bytes/sec)
ALSwitch#
```

# Erasing and Reloading the Switch

Remove the VLAN database information file.

```
Switch#delete flash:vlan.dat  
Delete filename [vlan.dat]? [Enter]  
Delete flash:vlan.dat? [confirm] [Enter]
```

```
Switch(config)#reload
```

The responding line prompt will be:

```
System configuration has been modified. Save? [yes/no]:
```

Type **n** and then press **Enter**.

The responding line prompt will be:

```
Proceed with reload? [confirm] [Enter]
```

# Password recovery

```
switch: flash init
switch: load_helper
switch: dir flash:
Directory of flash:
  13  drwx           192   Mar 01 1993 22:30:48  c2960-lanbase-
mz.122-25.FX
  11  -rwx           5825   Mar 01 1993 22:31:59  config.text
  18  -rwx           720   Mar 01 1993 02:21:30  vlan.dat
16128000 bytes total (10003456 bytes free)

switch: rename flash:config.text flash:config.text.old
switch: boot
...
Continue with the configuration dialog? [yes/no]: N
Switch> enable
Switch# rename flash:config.text.old flash:config.text
Switch# copy flash:config.text system:running-config
Source filename [config.text]?
Destination filename [running-config]?
Switch# configure termina
Switch (config)# enable secret password
```

# Password recovery

- Netacad.uniza.sk -> Na stiahnutie -> Semester CCNA3
- Nil.uniza.sk
  - (<http://nil.uniza.sk/netacad/ccna3/catalyst-2960-password-recovery>)