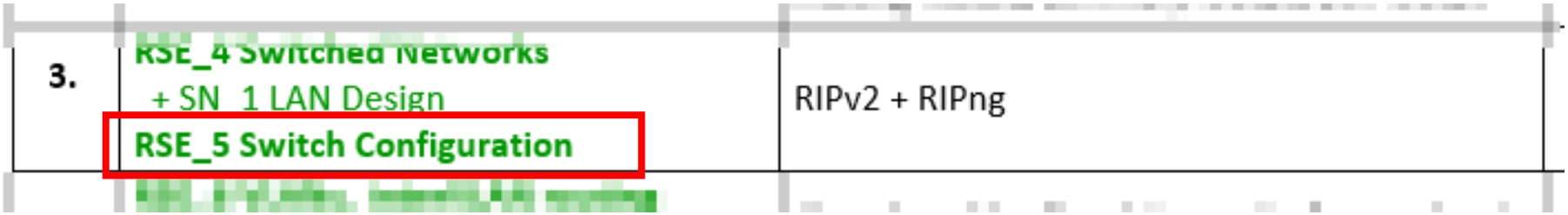
MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Module 5:
Konfigurácia prepínačov

CCNA2 (v6) - Chapter 5:
Switch Configuration

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Obsah prednášky



- Oboznámenie s „*exteriérom*“ prepínača
- Príprava práce
  - Premazanie prepínača
  - Obnova IOS a hesla
- Základná konfigurácia
- Zabezpečenie
  - SSH
  - Port security

Oboznámenie sa s prepínačom - Systém LED a boot proces

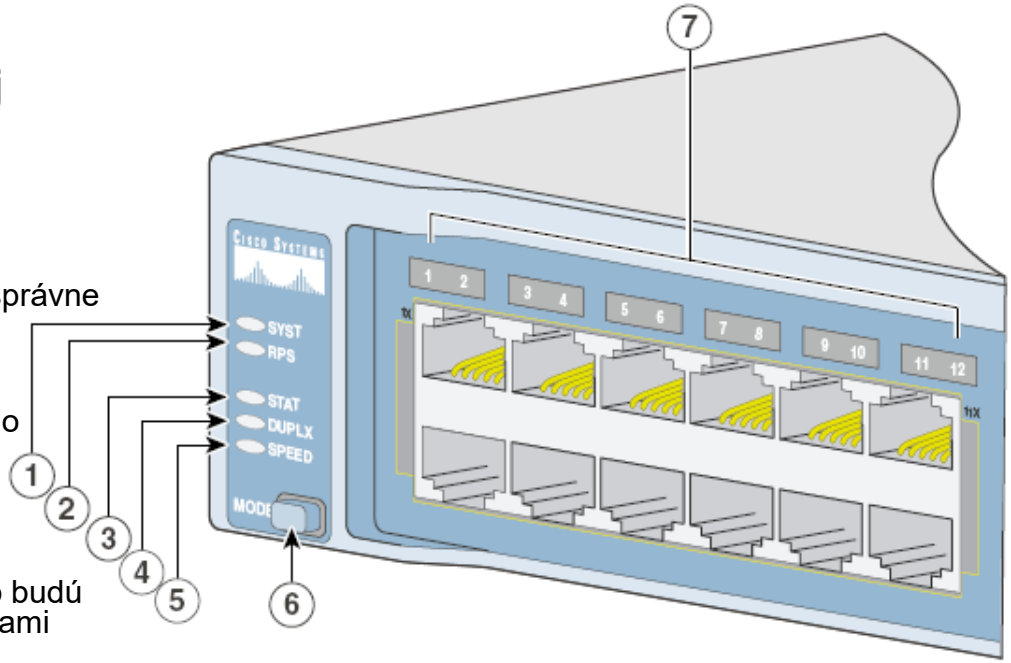
Vytvorené v rámci projektu KEGA 011STU - 4/2017.

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



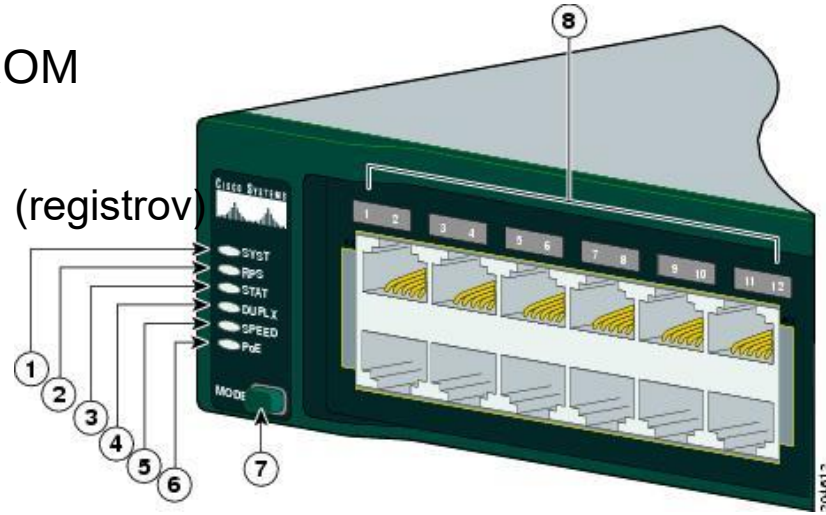
1	SYST LED	5	Speed LED
2	RPS LED	6	Mode button
3	Status LED	7	Port LEDs
4	Duplex LED		

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. **Note** 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	**10/100/1000 ports**	
	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.
	SFP module ports	
	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. **Note** 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 – boot sekvencia

- 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 následne natiahne konfigurák



- 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.

Sekvencia bootovania prepínača

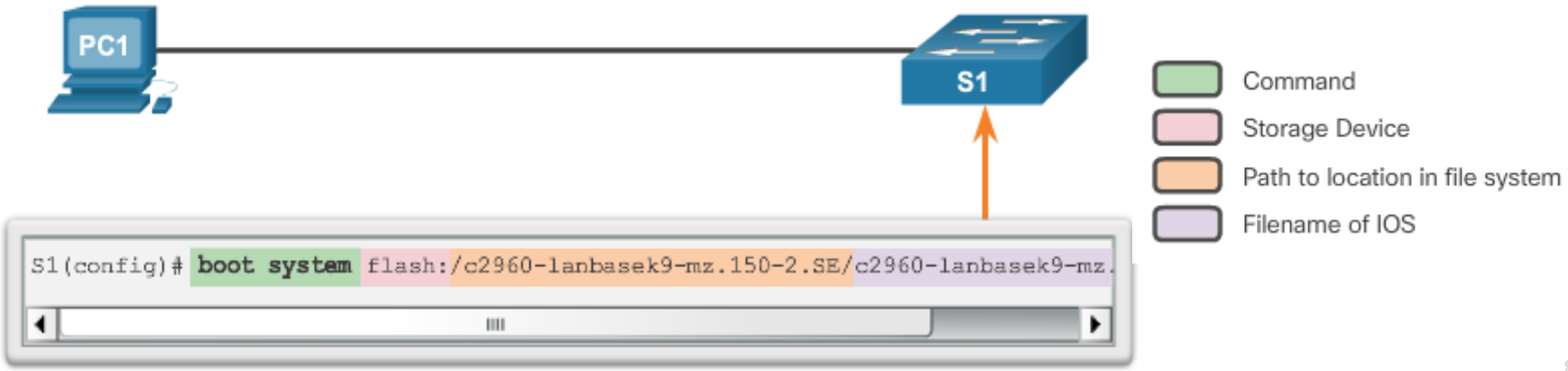
Vyhľadanie IOSu je riadené:

Krok 1. BootLoader sa snaží IOS automaticky spustiť pomocou informácií v premennej prostredia BOOT.

Krok 2. Ak táto premenná nie je nastavená, BL prehľadá flash súborový systém zhora nadol a načíta a spustí prvý spustiteľný súbor (ak je to možné)

Krok 3. IOS potom inicializuje rozhrania pomocou príkazov zo startup-config konfiguračného súboru z NVRAM

POZN: Príkazom **`boot system`** možno nastaviť hodnoty premennej prostredia BOOT, t.j. určiť aký súbosr IO S sa načíta pri boot-e



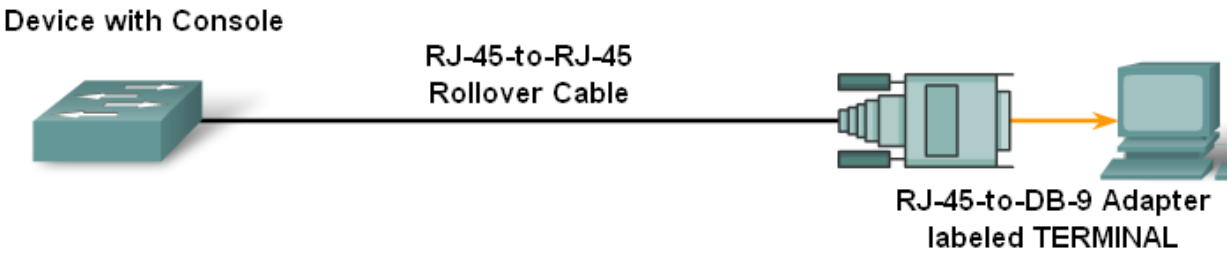
Základy práce a konfigurácie Cisco Catalyst prepínačov

2960-24TT-L a základná práca s prepínačom

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Príprava na konfiguráciu prepínača

Pripojenie na konzolu prepínača



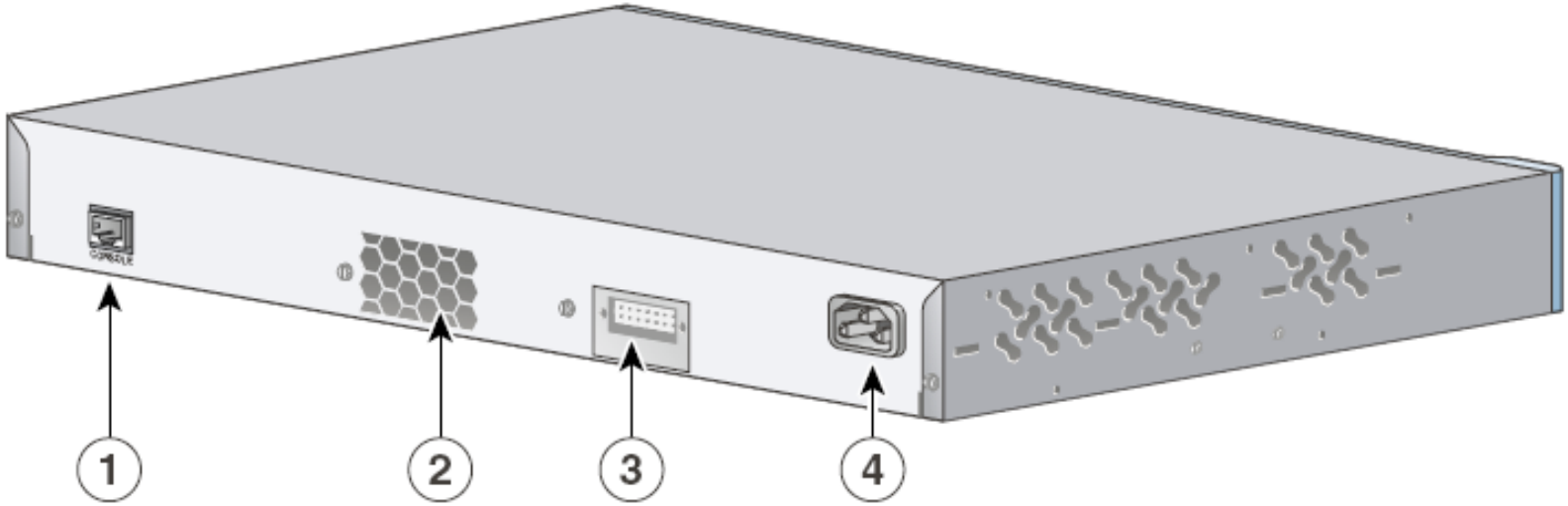
Prenosová cesta ako pri smerovači

- 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

Cisco prístupový prepínač 2960-24TT-L

Zadný pohľad – umiestnenie konzolového portu



1	RJ-45 console port	**3**	RPS connector
2	Fan exhaust	**4**	AC power connector

Príprava na konfiguráciu prepínača

Zotavenie po zlyhaní systému

- Zavádzač OS možno použiť aj na manažovanie prepínača:
  - keď sa nepodarí nabootovať štandardne IOS
  - alebo je zabudnuté heslo
- Ako sa k nemu dostať:
  1. Pripojiť PC konzolovým káblom k prepínaču na konzolový port. Odpojiť napájací kábel z prepínača.
  2. Naspať zapojiť napájací kábel k prepínaču, následne stlačiť a držať tlačidlo **Mode**.
  3. Systémová LED začne svietiť jantárovo a potom na zeleno, potom už treba pustiť tlačidlo **Mode**.
- V príkazovom riadku sa zobrazí zavádzač OS

```
switch:prompt
```

Príprava na konfiguráciu prepínača

Obnova IOS-u na prepínačoch

- Mnoho študentov si rado zmýli „erase startup-config“ resp. „delete flash:vlan.dat“ s príkazom „erase flash:“
- Catalyst prepínače dokážu po reštarte zmazaný IOS obnoviť iba cez COM port, nie cez Ethernet
  - Pozor: Max rýchlosť je 115200 baud, upload trvá „nekonečne“ dlho!
- Po nabootovaní do bootloadera je potrebné zadať:

```
switch: flash_init
switch: load_helper ! S novším IOSom už nie je potrebné
switch: set BAUD 115200 ! Zrýchli konzolu na 115.2 kbps
switch: format flash: ! Nie je nevyhnutné
switch: copy xmodem:<MENO> flash:<MENO>
switch: unset BAUD ! Vráti rýchlosť konzoly na 9.6 kbps
switch: boot
```

Príprava na konfiguráciu prepínača

Obnova hesla (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
```

Príprava na konfiguráciu prepínača

Zmazanie cudzej konfigurácie

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

```
Switch# show startup-config
 .... MAZ-LEN-AK-TU-NIECO-JE ....
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]
```

Príprava na konfiguráciu prepínača

Premazanie cuudzaj konfigurácie VLAN vo vlan.dat

- Potrebné vymazať všetky VLAN informácie vymazaním VLAN databázy vlan.dat z flash pamäte
  - **delete vlan.dat**
  - **POZOR: nerobiť erase flash:**
    - **Zmaže sa 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# reload
```

Odstránenie konfigurácie z rozhrania

- Rozhranie (je možné vrátiť do východzieho stavu)

```
! Zmaz konfig na interface
Switch# conf t
Switch (config)# default interface NAZOV X/Y
```

- Samozrejme vždy je možné odstrániť príkaz z running-config použitím negácie „no“

```
! Zmaz konfig na interface
Switch# conf t
Switch (config)# interface NAZOVO X/Y
Switch (config-if)# ip address 1.1.1.1 255.255.255.0
Switch (config-if)# no ip address
```

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.
```

Základná konfigurácie prepínača

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Ovládanie IOS z CMD - repete

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>
```

Ovládanie IOS z CMD - repete

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
```

Ovládanie IOS z CMD - repete

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)#
```

Ovládanie IOS z CMD - repete

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>
```

Overenie stavu prepínača

Výpis boot procesu prepínača

- Prepínač vypisuje pri bootovaní hlášky na konzolu
- Získanie základných informácii 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 ...
```

Základná konfigurácia prepínača s IOS

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Základná konfigurácia prepínača

Konfigurácia prepínača

- Odporúčaný postup pre konfiguráciu prepínača
  1. Základné nastavenia
     - Nastavenie mena zariadenia, DNS, systémové hlásenia, ochrana hesiel
  2. Nastavenie výstražných hlásení pred nepovolaným vstupom
  3. Zabezpečenie prístupu k prepínaču pomocou hesiel
     - Zabezpečenie prístupu k privilegovanému módu (Použi heslo: class)
     - Zabezpečenie prístupu cez konfiguračné rozhrania pomocou hesiel Použi heslo: cisco
  4. Zabezpečenie IP prístupu na prepínač pre vzdialenú správu + konfigurácia IP default gateway
  5. Overenie
  6. Iné konfigurácie
     - Tu rozumej konfigurácia módu a rýchlosti portu
- Tento postup nie je záväzný, ale je osvedčený

Základné nastavenia

Nastavenie mena prepínača a DNS

```
! Pristup do global konfig rezimu (GKR)
Switch# configure terminal

! Nastavenie mena, bez medzier, manej ako 64 znakov
Switch(config)# hostname ALS1

! Nastavenie domenoveho mena
ALS1(config)# ip domain-name netlab.uniza.sk

! Nastavenie DNS servera
ALS1(config)# ip name-server 8.8.8.8

! Vypnutie/zapnutie domain lookup
ALS1(config)# no ip domain-lookup
```

```
! Overenie
Show running-config
Show run | include HLADANY_STRING
```

Základné nastavenia

Ochrana hesiel v konfigurácii

- Okrem príkazu enable secret budú všetky ostatné heslá v konfigurácii uložené ako **plaintext**, t.j. viditeľné kedykoľvek pri jej zobrazení
- Ochranu týchto hesiel je možné dodatočne aktivovať v GKR príkazom `service password-encryption`
  - Od tohto momentu všetky existujúce i v budúcnosti zadané heslá v konfigurácii budú zašifrované (slabou) vratnou šifrou
  - Zrušenie príkazu ponechá existujúce heslá zašifrované

Pred príkazom:

```
line con 0
 password TajneHeslo
 login
line aux 0
 password TajneHeslo
 login
line vty 0 15
 password TajneHeslo
 login
```

Po príkaze:

```
line con 0
 password 7 09784F0317003F1718000B
 login
line aux 0
 password 7 053F07052F49660C0A0918
 login
line vty 0 15
 password 7 073B2046400C3100041E04
 login
```

Základná konfigurácia prepínača

Nastavenie výstražných hlásení - Banery

- Účelom výstražných hlásení je upozorniť nepovolané osoby pred pokusmi o neoprávnený vstup na zariadenie
  - Môže byť rozhodujúce v právnych sporoch pri bezpečnostných incidentoch
  - Tvorený príkazom, oddeľovacím znakom a textom

```
! Message-of-the-day banner, zobrazi sa vsetkym
! pred nalogovanim, nad banner login
ALS1(config)# banner motd #This is a secure site. Only
authorized users are allowed.For access, contact
technical support.#

! Login banner so spravou pred prihlasenim
Switch(config)# banner login $Access for authorized users
only. Please enter your username and password.$

! Banner po prihlaseni
Switch(config)# banner exec $ TEXT $
```

Zabezpečenie prístupu k príkazovému riadku

Ošetrenie prístupu k privilegovanému módu

```
! Zabezpecenie pristupu z pouzivatelskeho do
! privilegovaneho rezimu, heslo je v config-u sifrovane
ALS1(config)# enable secret TajneHeslo1234

! Overenie
! ----------------
ALS1(config)# end
ALS1# disable
ALS1> enable
Password: TajneHeslo456
ALS1#
```

```
! Nepouzivaj nezabezpecenu formu
ALS1(config)# enable password TajneHeslo1234
```

Zabezpečenie prístupu k príkazovému riadku

Zdieľané heslo pre konzolu, vty (telnet/ssh)

```
! Konzola
ALS1(config)# line console 0
ALS1(config-line)# password Heslo123
ALS1(config-line)# login
! Cas neaktivity na ukoncenie exec
ALS1(config-line)# exec-timeout 30
! Ochrana proti zmiesavaniu vstupu a vystupu CMD
ALS1(config-line)# logging synchronous
ALS1(config-line)# exit

! Telnet / SSH - Musi byt IP konektivita na prepinac
ALS1(config)# line vty 0 15
ALS1(config-line)# password Heslo123
ALS1(config-line)# login
ALS1(config-line)# exit
```

```
Press RETURN to get started.

User Access Verification

Password: Heslo123
ALS1> enable
Password: TajneHeslo456
ALS1#
```

Zabezpečenie prístupu k príkazovému riadku

Overenie prístupu voči lokálnej autent. DB

- Lokálna databáza je na každom zariadení zadefinovaný zoznam mien a hesiel s pridelenou úrovňou prístupu
  - **username** *NAME* **privilege** *LEVEL* **secret** *HESLO*

```
! Definovanie poloziek pouzivatelov v lokalnej DB
ALS1(config)# username admin privilege 15 secret
  ADMIN_HESLO
ALS1(config)# username palo secret PALOVE_HESLO
ALS1(config)# username juro secret JUROVE_HESLO

ALS1(config)# line con 0
ALS1(config-line)# login local
ALS1(config-line)# exit
ALS1(config)# line vty 0 15
ALS1(config-line)# login local
```

Základná konfigurácia prepínača

Zabezpečenie IP prístupu na prepínač

- Prečo má mať prepínač ako L2 zariadenie IP adresu?
  - Nastavenie IP adresy a def. gw umožňuje pristupovať k manažmentu prepínača cez telnet, web, ssh apod.
- IP adresa sa prideľuje tzv. virtuálnemu rozhraniu, volanému Switch Virtual Interface (SVI)
  - Je to virtuálne L3 rozhranie
    - T.j. má IP adresu, avšak bežný L2 stále nevie smerovač pakety
    - Pozn. v skutočnosti obmedzene vie, ale zatiaľ je to mimo CCNA2
  - K SVI je priradená buď VLAN alebo fyzický port/rozhranie
- Na cisco prepínačoch default:
  - Každý prepínač dodávaný s VLAN1 a máme SVI Vlan1
    - Všetky porty priradené do VLAN1
    - VLAN1 – tzv. „**manažovacia VLAN**“
      - Lebo poskytuje IP prístup k manažmentu

Základná konfigurácia prepínača

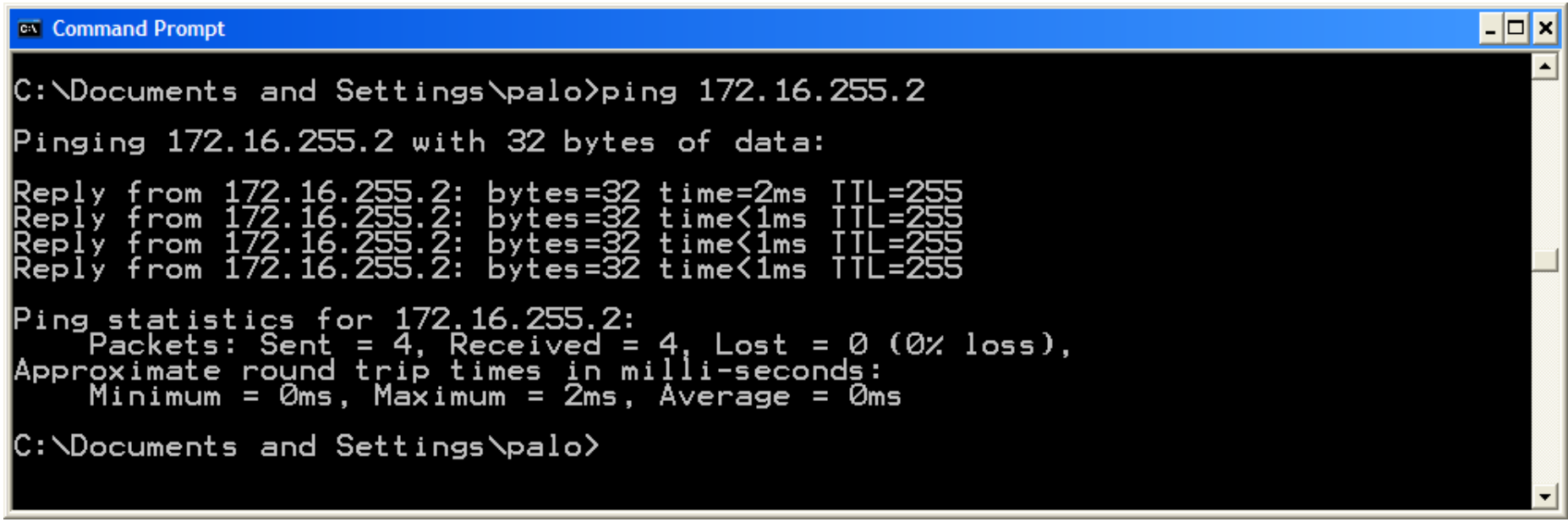
Zabezpečenie IP prístupu na prepínač - VLAN1

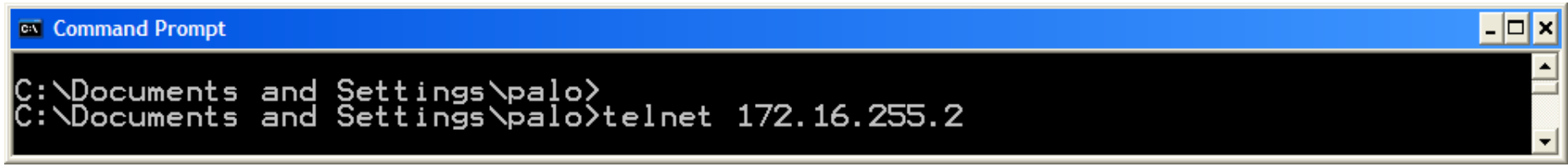
```
Tristan(config)# interface vlan 1
Tristan(config-if)#ip address 172.16.255.2 ?
  A.B.C.D  IP subnet mask

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





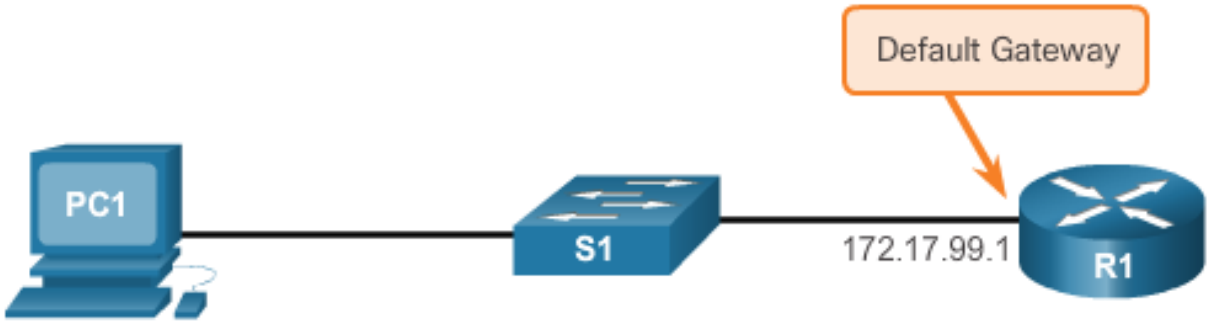
Zabezpečenie IP prístupu na prepínač

Použitie inej manažovacej VLAN – VLAN99

```
Tristan(config)#interface vlan 99
Tristan(config-if)#ip address 172.17.99.2 255.255.255.0
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
```

Konfigurácia predvolenej brány (def. gw)

```
Tristan(config)# ip default-gateway 172.17.99.1
```



Zabezpečenie IP prístupu na prepínač

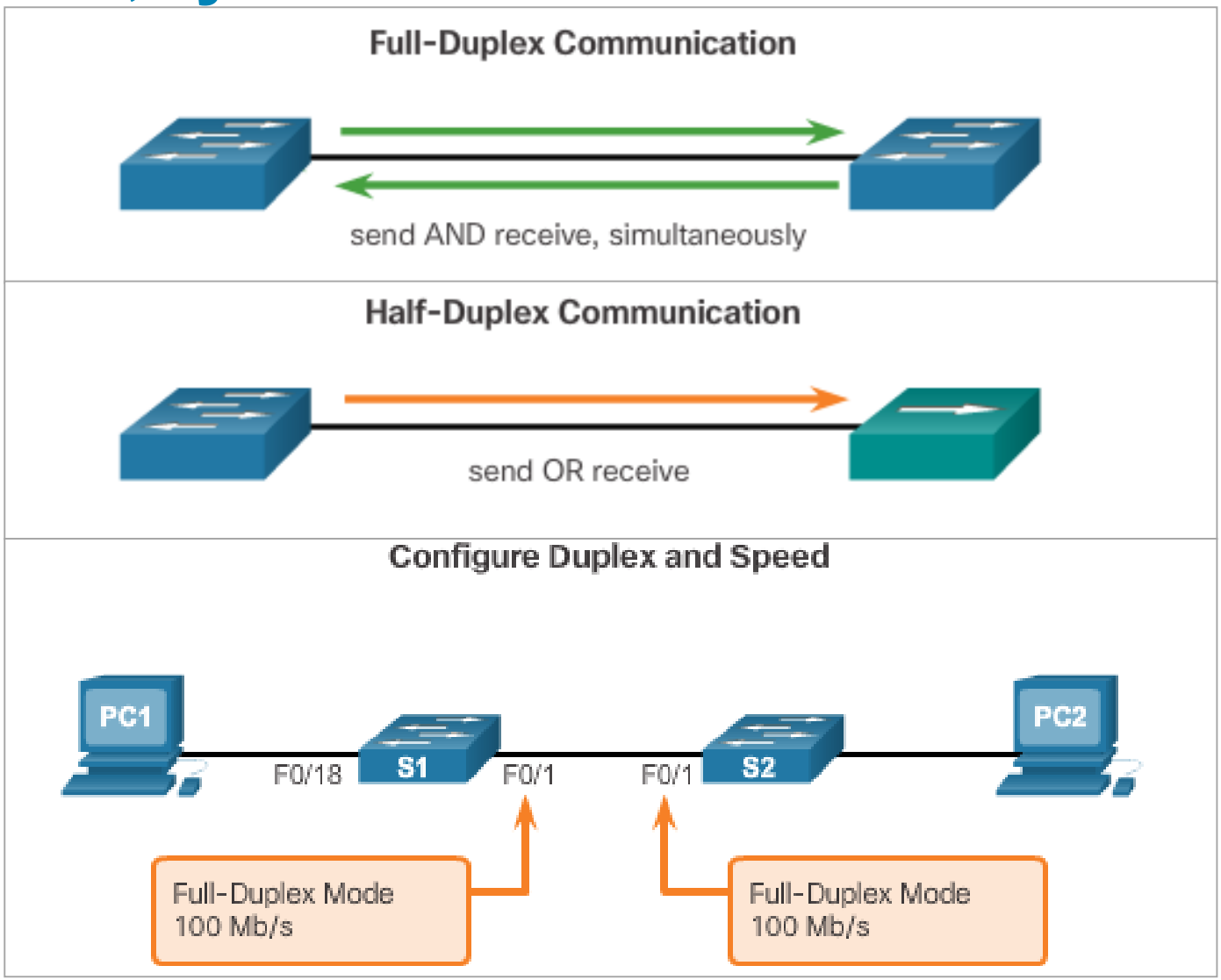
Overenie

```
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                 172.17.99.2     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 172.17.99.2 255.255.255.0
!
ip default-gateway 172.17.99.1
```

Konfigurácia portov na prepínači

Duplex, rýchlosť komunikácie



Konfigurácia portov na prepínači

Funkcia auto-MDIX

- Príslušné typy káblov (priamy/krížený) bolo v minulosti potrebné dodržiavať pri pripojení k zariadeniam.
- Dnes ale tento problém rieši **auto-MDIX**
  - *automatic medium-dependent interface crossover*.
- Keď je povolená (na rozhraní), automaticky deteguje požadovaný typ káblového prepojenia a vhodne ho nakonfiguruje.
- Ak ju používam, rýchlosť aj duplex musia byť nastavené na automatické vyjednanie ba oboch stranách:
  - T.j. **auto** (autonegotiate)
- Overenie:

```
switch# show controllers ethernet-controller gigabitEthernet 0/1 phy |
include Auto-MDXI
```

Základná konfigurácia portov prepínača

```
Switch(config)# interface gig 3/1
Switch(config-if)# description Printer in Bldg A, room 213
! Switch(config-if)# speed {10 | 100 | 1000 | auto}
Switch(config-if)# speed auto
! Switch(config-if)# duplex {auto | full | half}
Switch(config-if)# duplex auto
```

- Ak je aspoň jeden z týchto parametrov ponechaný na auto, na porte zostáva bežať autonegociácia
  - V „capabilities“, ktoré port ohlasuje, sú len tie alternatívy, ktoré zahŕňajú fixne nastavený parameter
- Ak sú oba parametre nastavené fixne, autonegociácia sa na viacerých typoch Catalyst switchov vypína
  - Dôsledkom je, že ak sa druhá strana spolieha na autonegociáciu, rýchlosť odhadne z kanálového kódovania a duplex nastaví na half (fallback hodnota)
  - Možnosť veľmi nepríjemných problémov kvôli nezhode duplexu
  - Je rozdiel „vypnutá autonegociácia“ a „autonegociácia, ktorá uvádza iba jedinú alternatívu“
  - Ak je vypnutá autonegociácia, nefunguje ani auto-MDIX
  - Praktická skúsenosť: 3560V2 nevypínajú autonegotiation, iné modely switchov (2960) áno – poučenie: ak je potrebné nastaviť rýchlosť a duplex fixne, najlepšie je to urobiť na oboch koncoch linky súčasne

Overenie stavu prepínača

Overenie základnej konfigurácie

- **`show running-config`**
  - Zobrazí aktuálne používaný konfiguračný súbor
- **`show vlan`**
  - Zobrazí informácie o Virtuálnych sieťach
- **`show flash`**
  - Zobrazí informácie o Flash pamäti
- **`show version`**
  - Zobrazí informácie o verzii používaného OS
- **`show interface status`**
  - Zobrazí stav portov prepínača, rýchlosť, duplex a médium
- **`show interface`**
  - Zobrazí stav všetkých rozhraní prepínača

Overenie stavu prepínača

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
```

Overenie stavu prepínača

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

Overenie stavu prepínača

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)
```

Overenie stavu prepínača

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 ...
```

Overenie stavu prepínača

Show interfaces status

```
switch# show interface status

Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          a-full  a-100 10/100BaseTX
Fa0/2                        connected    1          a-full  a-100 10/100BaseTX
Fa0/3                        connected    1          a-full  a-100 10/100BaseTX
Fa0/4                        notconnect   1            auto   auto 10/100BaseTX
Fa0/5                        notconnect   1            auto   auto 10/100BaseTX
Fa0/6                        notconnect   1            auto   auto 10/100BaseTX
Fa0/7                        notconnect   1            auto   auto 10/100BaseTX
Fa0/8                        connected    1          a-full  a-100 10/100BaseTX
Fa0/9                        notconnect   1            auto   auto 10/100BaseTX
Fa0/10                       notconnect   1            auto   auto 10/100BaseTX
```

Overenie stavu prepínača show interface TYP X/Y

```
Sw-FRI-3560-A213#sh interfaces gigabitEthernet 0/3
GigabitEthernet0/3 is up, line protocol is up (connected)
  Hardware is Gigabit Ethernet, address is 001b.8f8f.de03 (bia
001b.8f8f.de03)
  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 10/100/1000BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:00:01, 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 4000 bits/sec, 6 packets/sec
     2830675 packets input, 185209120 bytes, 0 no buffer
     Received 4199 broadcasts (0 multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
     0 input packets with dribble condition detected
     15980351 packets output, 1277847091 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

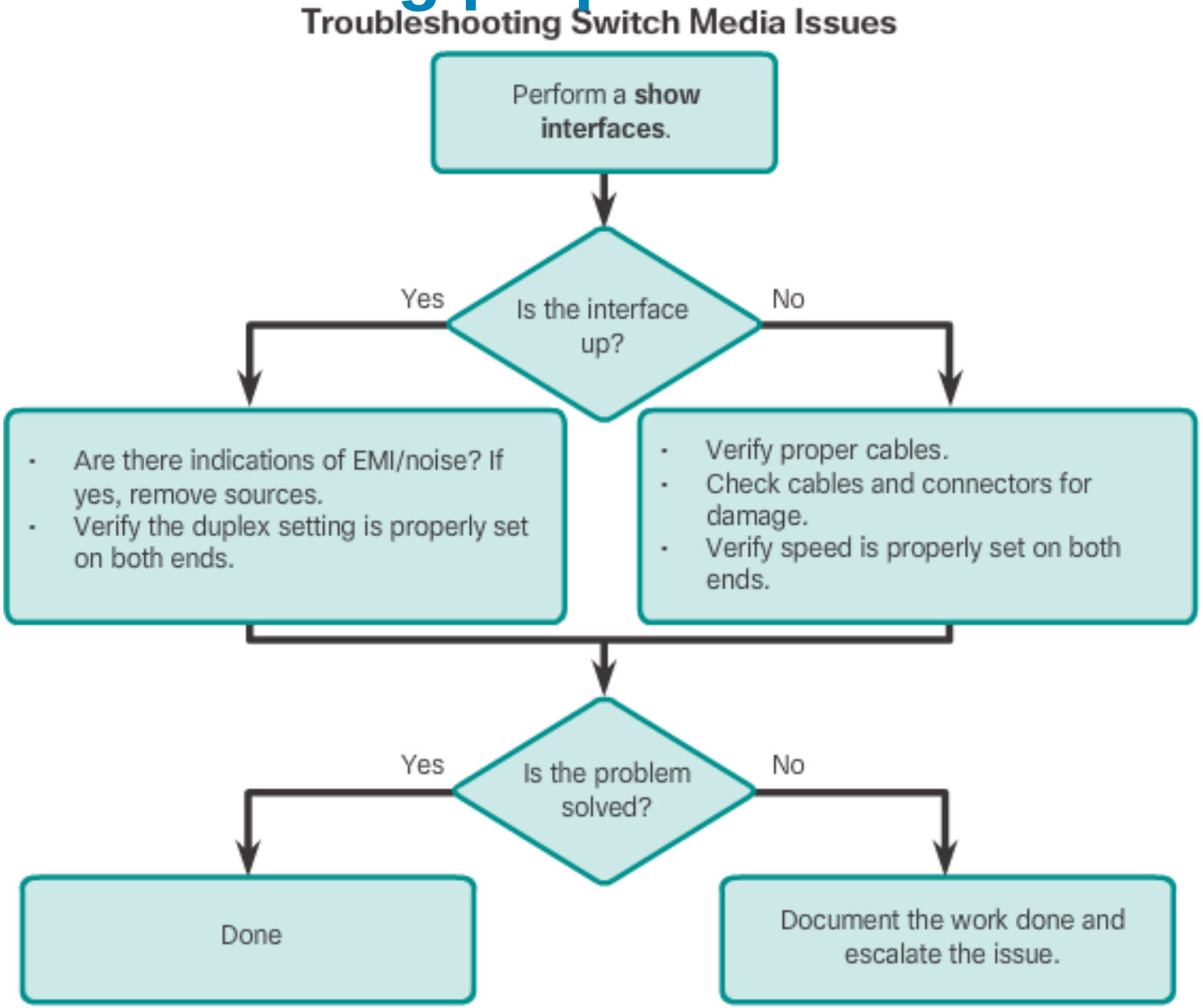
Konfigurácia portov na prepínači

Problémy na 1. vrstve - Network Access

Parameter	Description
Runts	Packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.
Giants	Packets that are discarded because they exceed the maximum packet size for the medium. For example, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Input errors	Total number of errors. It includes runts, giants, no buffer, CRC, frame, overrun, and ignored counts.
CRC	CRC errors are generated when the calculated checksum is not the same as the checksum received.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface that is being examined.
Collisions	Number of messages retransmitted because of an Ethernet collision.
Late collisions	Jammed signal could not reach to ends.

Konfigurácia portov na prepínači

Troubleshooting pri problémoch 1. vrstvy



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#**terminal history**
Configures the terminal history size. The terminal history can maintain 0 to 256 command lines.	switch#**terminal history size 50**
Resets the terminal history size to the default value of 10 command lines.	switch#**terminal no history size**
Disables terminal history.	switch#**terminal no history**

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

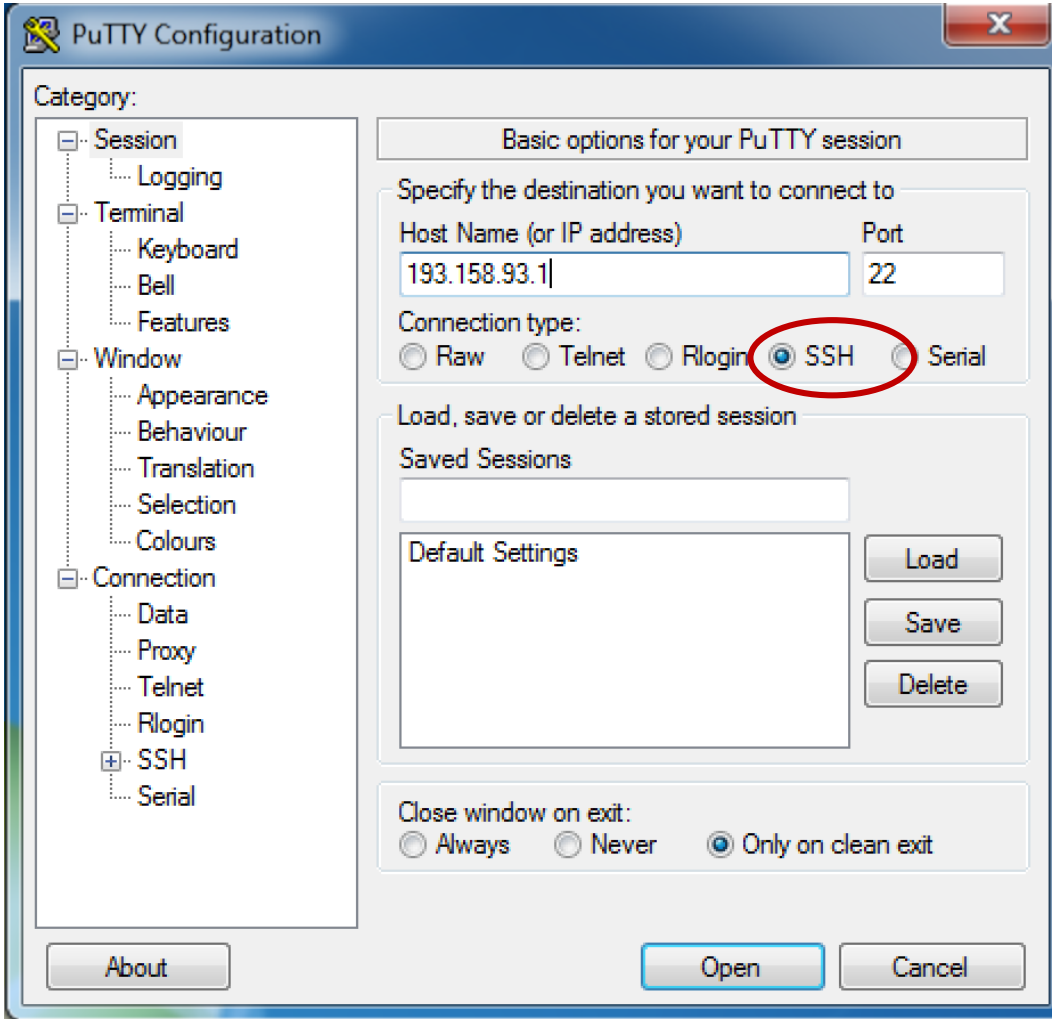
Bezpečnosť na prepínači: Manažment a implementácia

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Bezpečný vzdialený prístup k prepínaču

Secure Shell (SSH)

- Umožňuje šifrovaný prístup k príkazovému riadku na vzdialenom zariadení
- Bežne sa používa v UNIX systémoch
- Podporuje ho aj Cisco IOS
- Kvôli bezpečnosti ho treba vždy uprednostniť pred Telnetom
- SSH používa TCP port 22, Telnet používa TCP port 23



Bezpečný vzdialený prístup k prepínaču

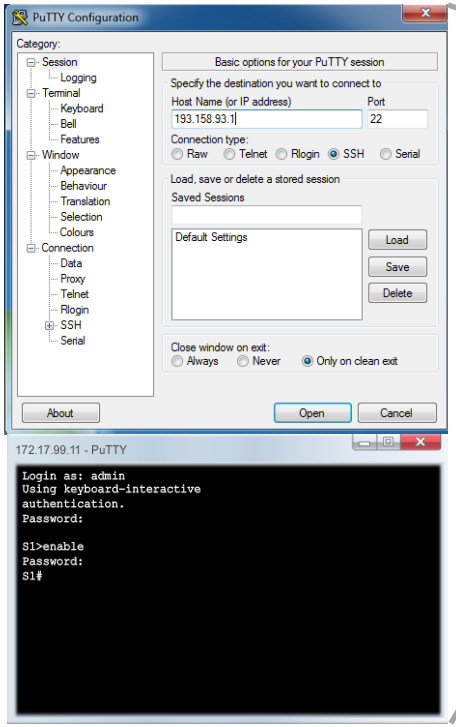
Konfigurácia SSH prístupu

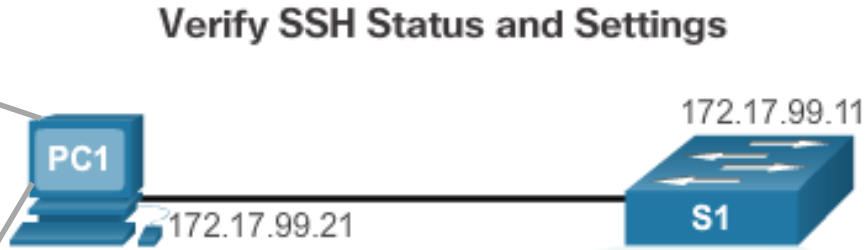
```
Switch(config)# username Meno password Heslo
! Domena musi byt zadefinovana
Switch(config)# ip domain-name pepe.sk
Switch(config)# crypto key generate rsa
The name for the keys will be: Switch.pepe.sk
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 1024
% Generating 1024 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 2 has been enabled
Switch(config)# line vty 0 15
Switch(config-line)# transport input ssh
Switch(config-line)# login local
```

```
! Obnovenie telnet pristupu
Switch(config)#line vty 0 15
Switch(config-line)#transport input telnet
! Or
Switch(config-line)#transport input all
```

Bezpečný vzdialený prístup k prepínaču

Overenie SSH






```
S1# show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 90 secs; Authentication retries: 2
Minimum expected Diffie Hellman key size : 1024 bits
IOS Keys in SECSH format(ssh-rsa, base64 encoded):
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAAAgQCdLksVz2QlREsoZt2f2scJHbW3aMDM8
/8jg/srGFNL
i+f+qJWwxt26BWmy694+6ZIQ/j7wUfIVNlQhI8GUOVIuKNqVMOMtLg8Ud4qAiLbGJfAa
P3fyrKmViPpO
eOZof6tnKgKKvJz18Mz22XAf2u/7Jq2JnEFXycGMO88OUJQL3Q==

S1# show ssh
Connection Version Mode Encryption  Hmac      State          Username
0          2.0     IN   aes256-cbc  hmac-sha1 Session started admin
0          2.0     OUT  aes256-cbc  hmac-sha1 Session started admin
%No SSHv1 server connections running.
S1#
```

MAC tabuľka

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

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 NUMER> vlan VLAN_NUMBER
```

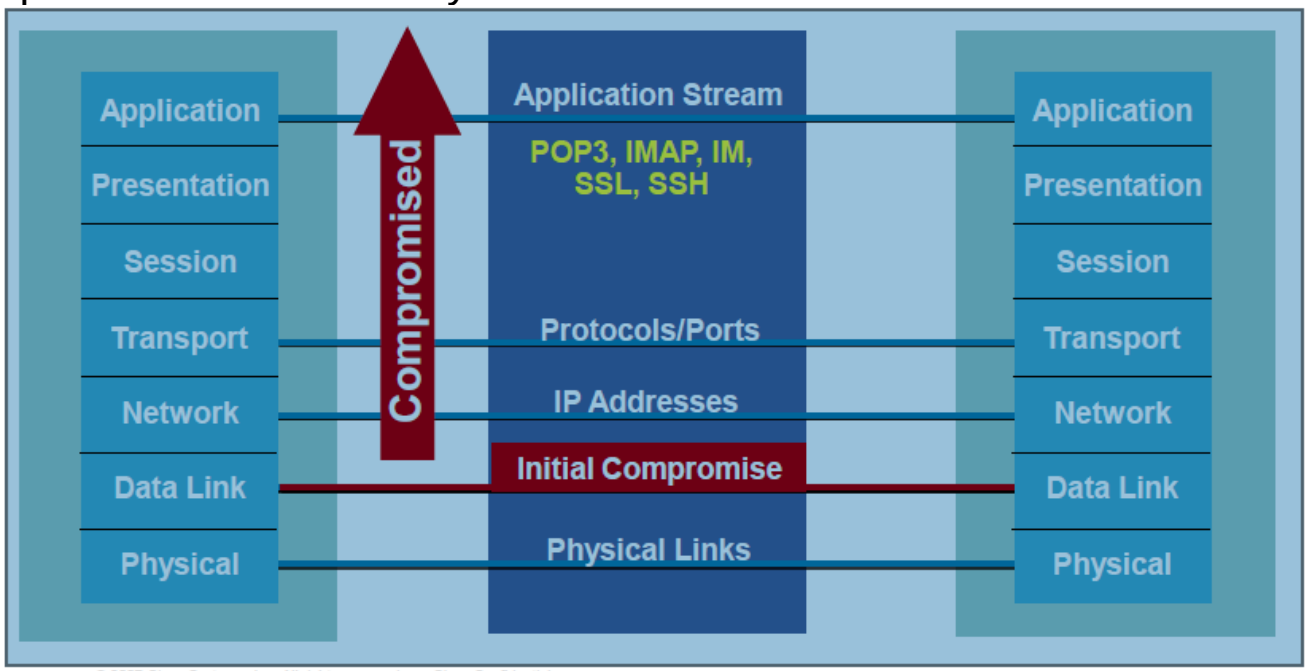
```
Switch(config)# mac-address-table ?
  aging-time     Set MAC address table entry maximum age
  notification   Enable/Disable MAC Notification on the switch
  static         static keyword
Switch(config)#mac-address-table static 00e0.a3e8.8de7 interface
Fa 0/1 vlan 1
Switch(config)#exit
%SYS-5-CONFIG_I: 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

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

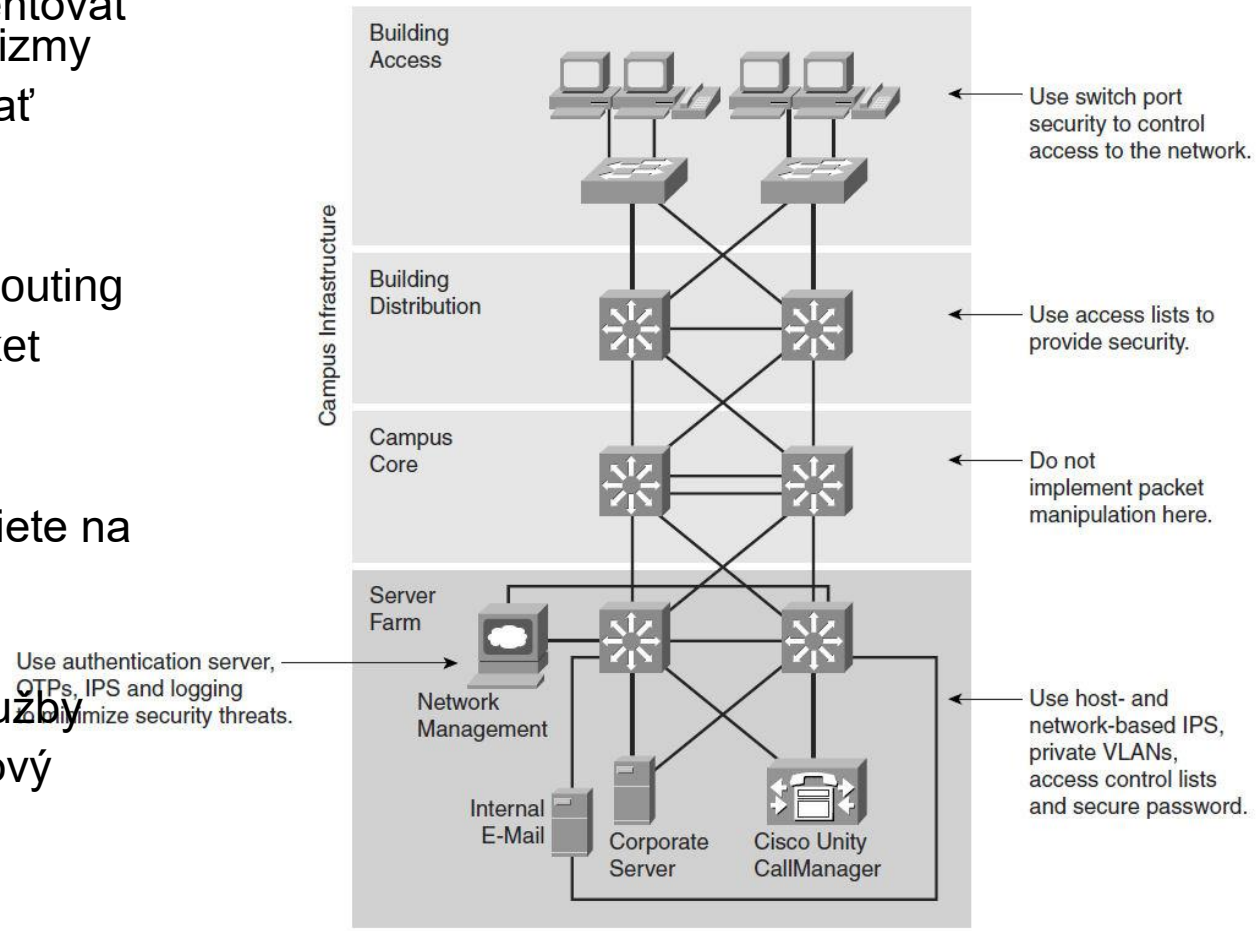
Zabezpečenie LAN infraštruktúry

- Bezpečnosť je väčšinou tlačená 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

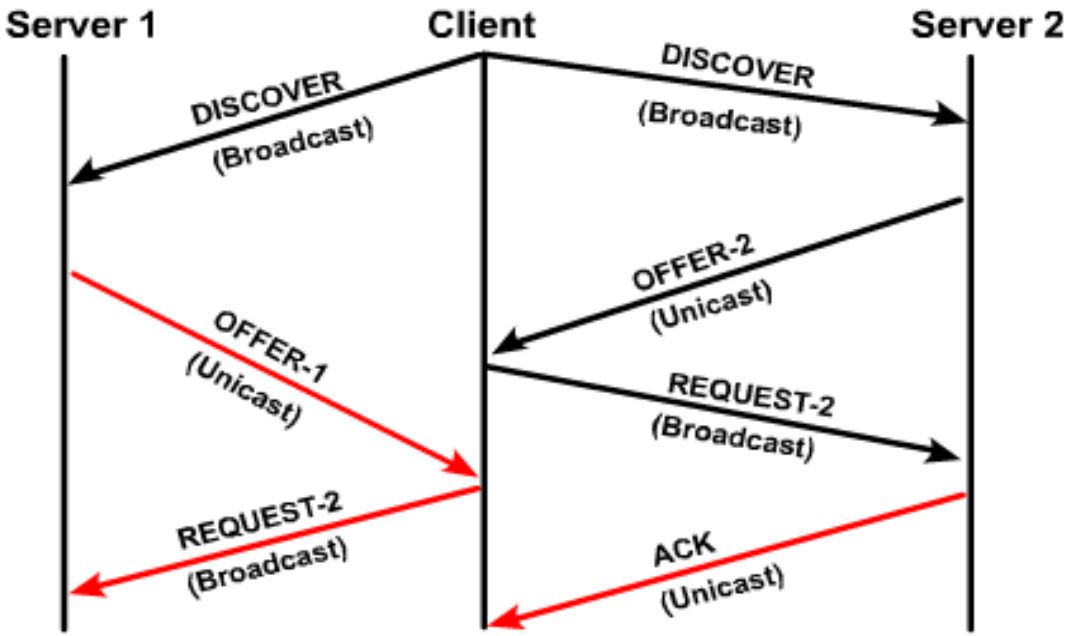
- Core
  - Nie je vhodné implementovať bezpečnostné mechanizmy
  - Musí rýchlo spracovávať pakety/rámce
- Distribution
  - Vykonáva inter VLAN routing
  - Vhodné aplikovať packet filtering.
- Access
  - Riadenie prístupu do siete na úrovni portu
- Server farm
  - Poskytuje aplikačné služby
  - Vhodné aplikovať sieťový manažment



Útoky na DHCP

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

DHCP činnosť

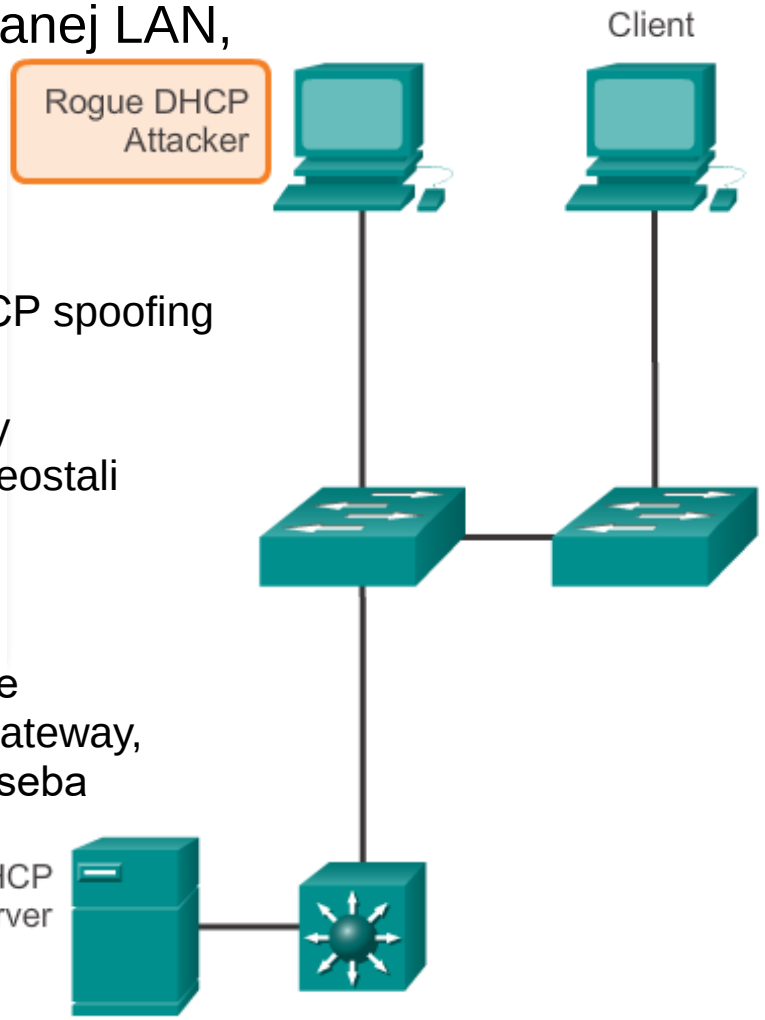


- DHCP client broadcasts DHCP DISCOVER packet on local subnet
- DHCP servers send OFFER packet with lease information
- DHCP client selects lease and broadcasts DHCP REQUEST packet
- Selected DHCP server sends DHCP ACK packet

Zraniteľnosti Ethernetových LAN sietí a známe typy útokov

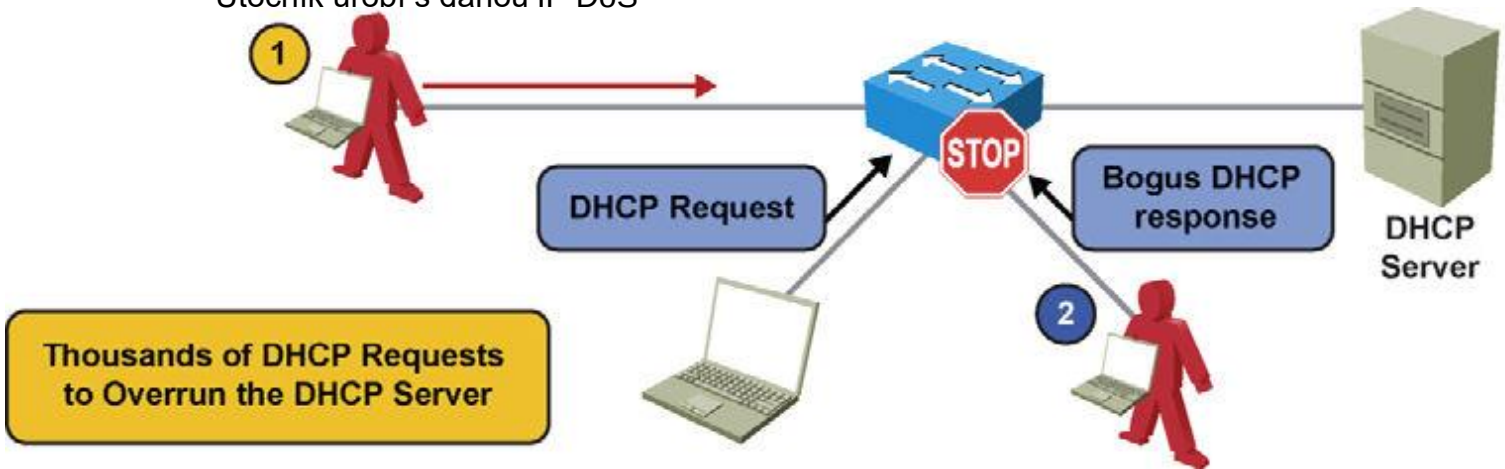
DHCP Spoofing a DHCP starvation

- Môže vykonať útočník fyzicky prítomný v danej LAN, alebo získal prístup z Internetu na niektorý PC v danej LAN
- DHCP starvation (vyhladovanie)
  - Často vykoná útočník ešte pred spustením DHCP spoofing útoku
  - Vygeneruje veľké množstvo žiadostí o IP adresy (posiela sa broadcastom), aby DHCP serveru neostali voľné IP adresy pre legitímnych používateľov
- DHCP spoofing (podvrhnutie)
  - Útočník spustí falošný DHCP server, a poskytuje IP adresné dáta (IP adresu, masku, IP default gateway, DNS, ...) legitímnym používateľom tak, že sám seba vyhlási za bránu.
  - Dáta od používateľov môže ďalej preposielať do cieľa, ktorého sú určené, čím ostáva pre používateľov neviditeľný.



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

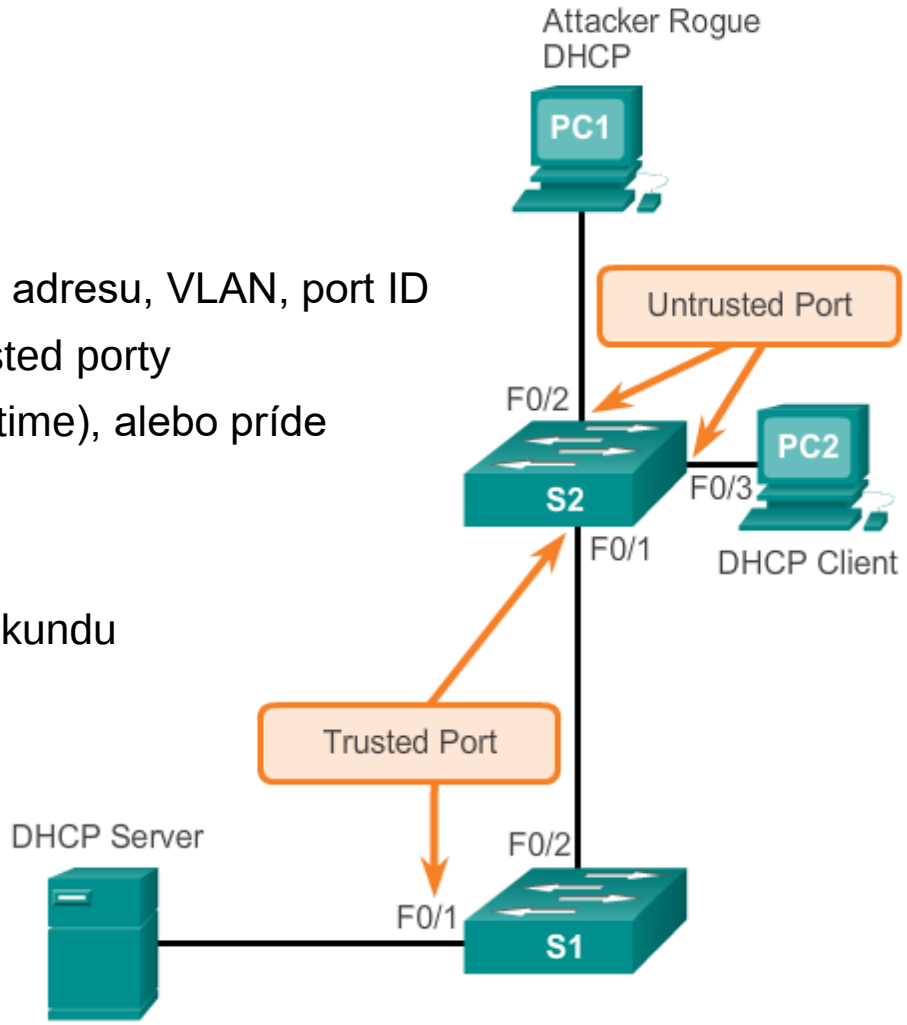


Ochrana pred DHCP Spoofing

DHCP Snooping

- Zadefinujem, z ktorých portov môžu prísť odpovede na DHCP žiadosti = trusted
- Ostatné = untrusted
- DHCP snooping binding table
  - Prepínač zaznamenáva MAC adresu, IP adresu, VLAN, port ID
  - z prichádzajúcich DHCP správ na untrusted porty
  - Záznam zmaže, keď vyprší čas (leased time), alebo príde správa DHCPRELEASE (uvoľňujem IP)
- limit rate
  - obmedzím počet DHCP requestov za sekundu

```
S1(config)# ip dhcp snooping
S1(config)# ip dhcp snooping vlan 10,20
S1(config)# interface fastethernet 0/1
S1(config-if)# ip dhcp snooping trust
S1(config)# interface fastethernet 0/2
S1(config-if)# ip dhcp limit rate 5
```



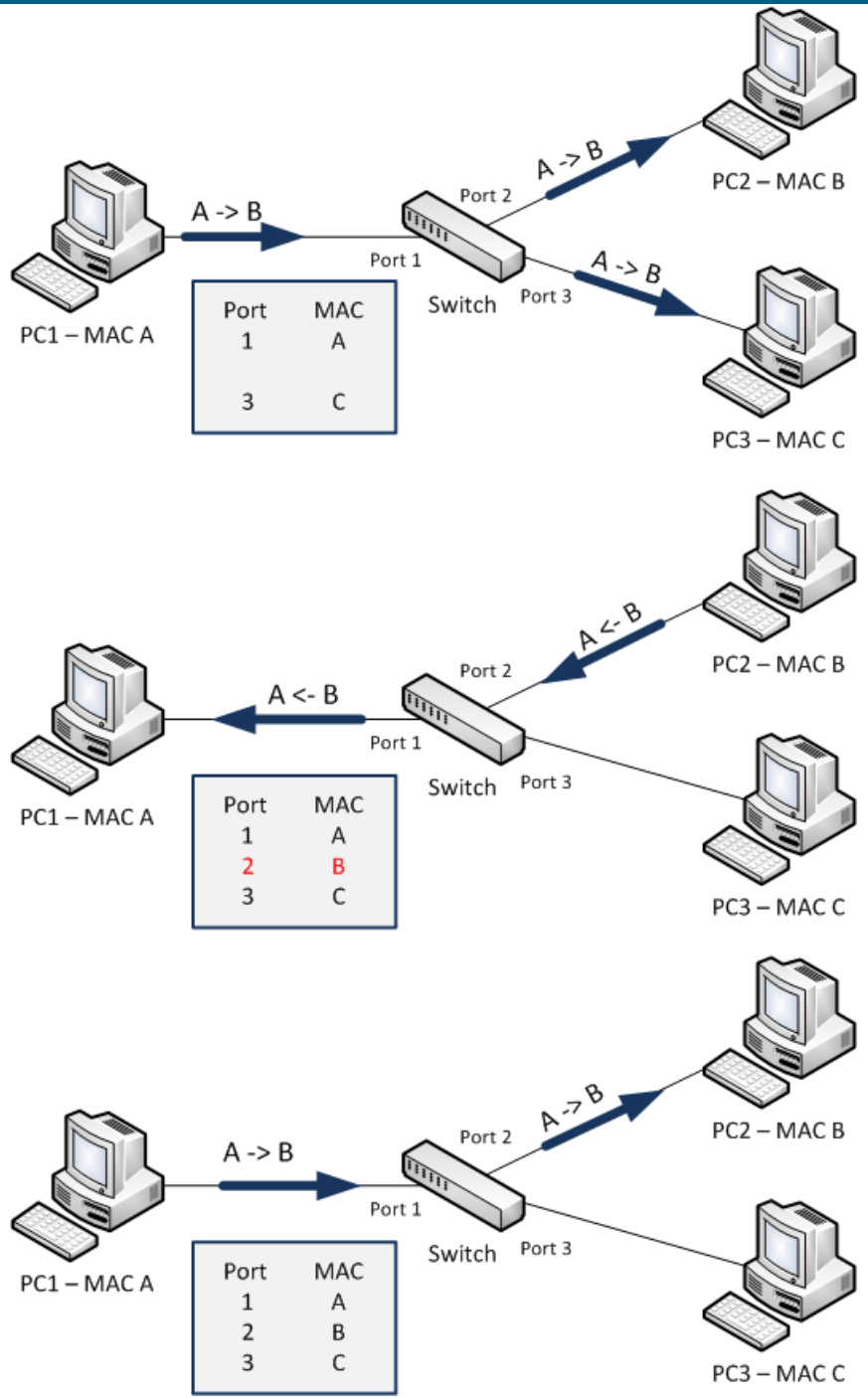
Útoky na MAC/CAM

Útoky na CAM

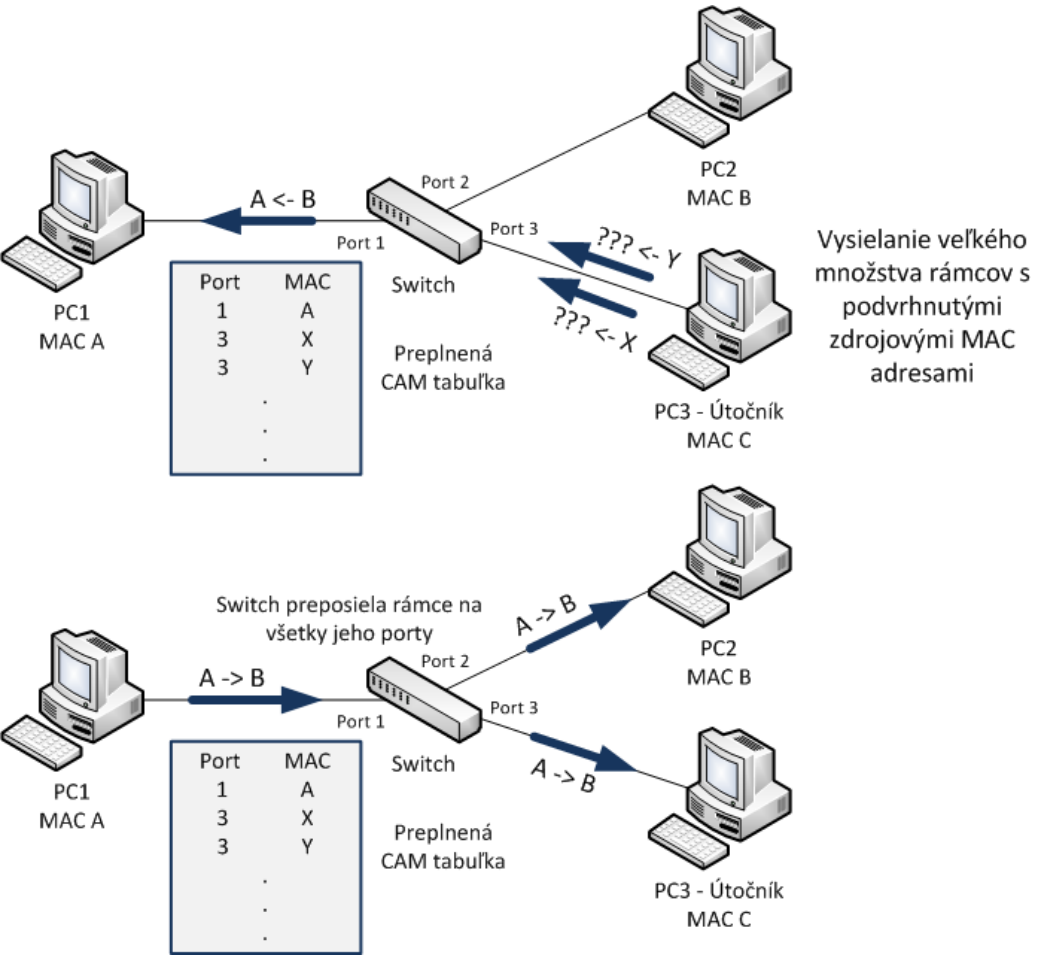
Vytvorené v rámci projektu KEGA 011STU - 4/2017.

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

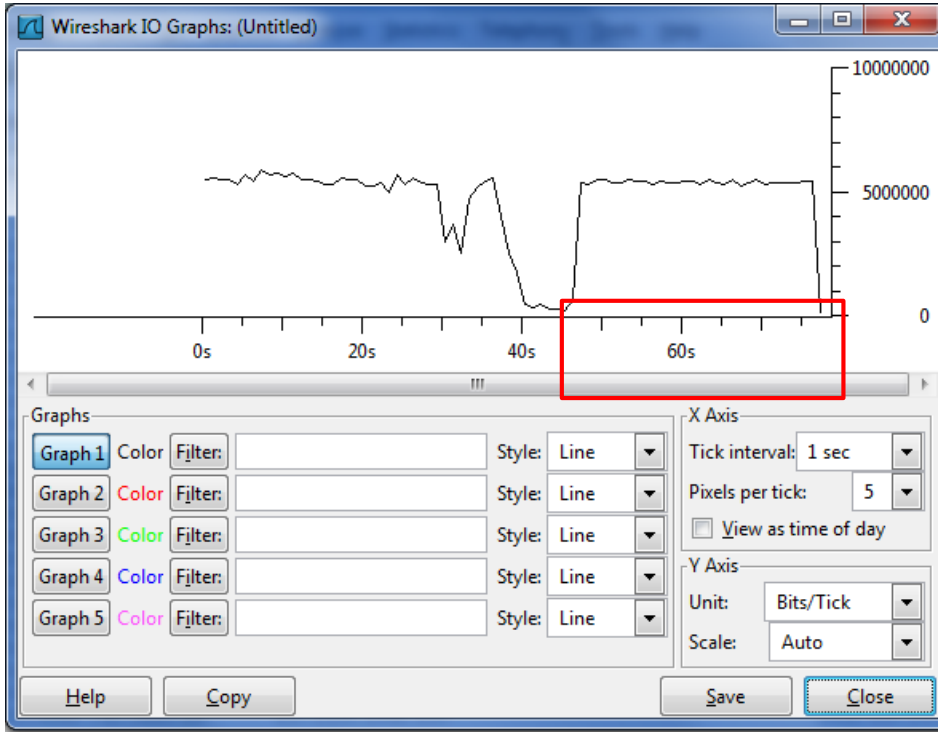
Realizácia - macof

- 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 – plnenie tabuľky položkami

Before Macof

```
Access01#show mac-address-table count

NM Slot: 1
--------------

Dynamic Address Count:                  2
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              3
Total MAC addresses:                    5
Maximum MAC addresses:                  8192
```

After Macof

```
Access01#show mac-address-table count

NM Slot: 1
--------------

Dynamic Address Count:                  8187
Secure Address (User-defined) Count:    0
Static Address (User-defined) Count:    0
System Self Address Count:              2
Total MAC addresses:                    8189
Maximum MAC addresses:                  8192
```

- 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

```
switch1#show mac address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0011.5ccc.5c00    STATIC      CPU
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0100.0cdd.dddd    STATIC      CPU
   1    0009.5b44.9d2c    DYNAMIC     Fa0/1
   1    000f.66e3.352b    DYNAMIC     Fa0/1
   1    0012.8015.c940    DYNAMIC     Fa0/24
   1    0012.8015.c941    DYNAMIC     Fa0/24
   1    001a.adb3.bef7    DYNAMIC     Fa0/1
   1    0025.2266.d104    DYNAMIC     Fa0/1
   1    0026.b865.313e    DYNAMIC     Fa0/1
   1    64a7.6973.8e4d    DYNAMIC     Fa0/1
   1    6c71.d976.fce7    DYNAMIC     Fa0/1
   1    74f6.12d4.1e1c    DYNAMIC     Fa0/1
   1    a477.3344.98b6    DYNAMIC     Fa0/1
```

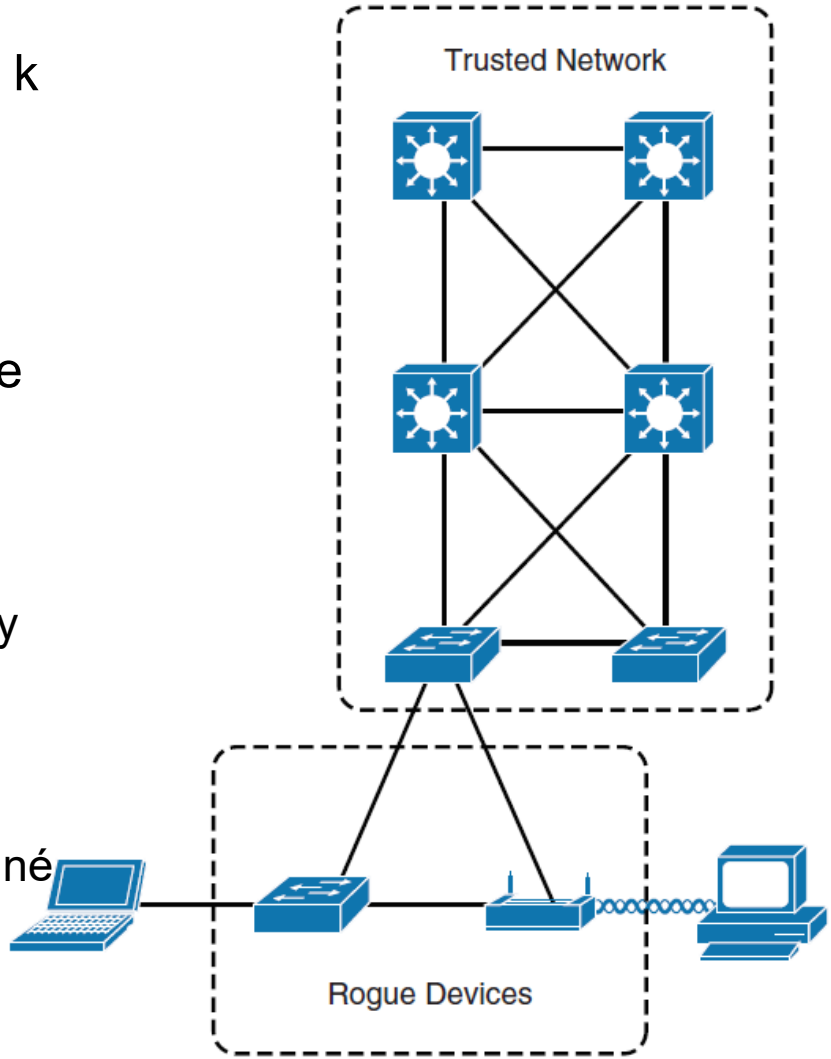
Potieranie útokov na CAM a kontrola prístupu do prepínanej siete

Port Security

Vytvorené v rámci projektu KEGA 011STU - 4/2017.

Riadenie prístupu k prepínanej sieti

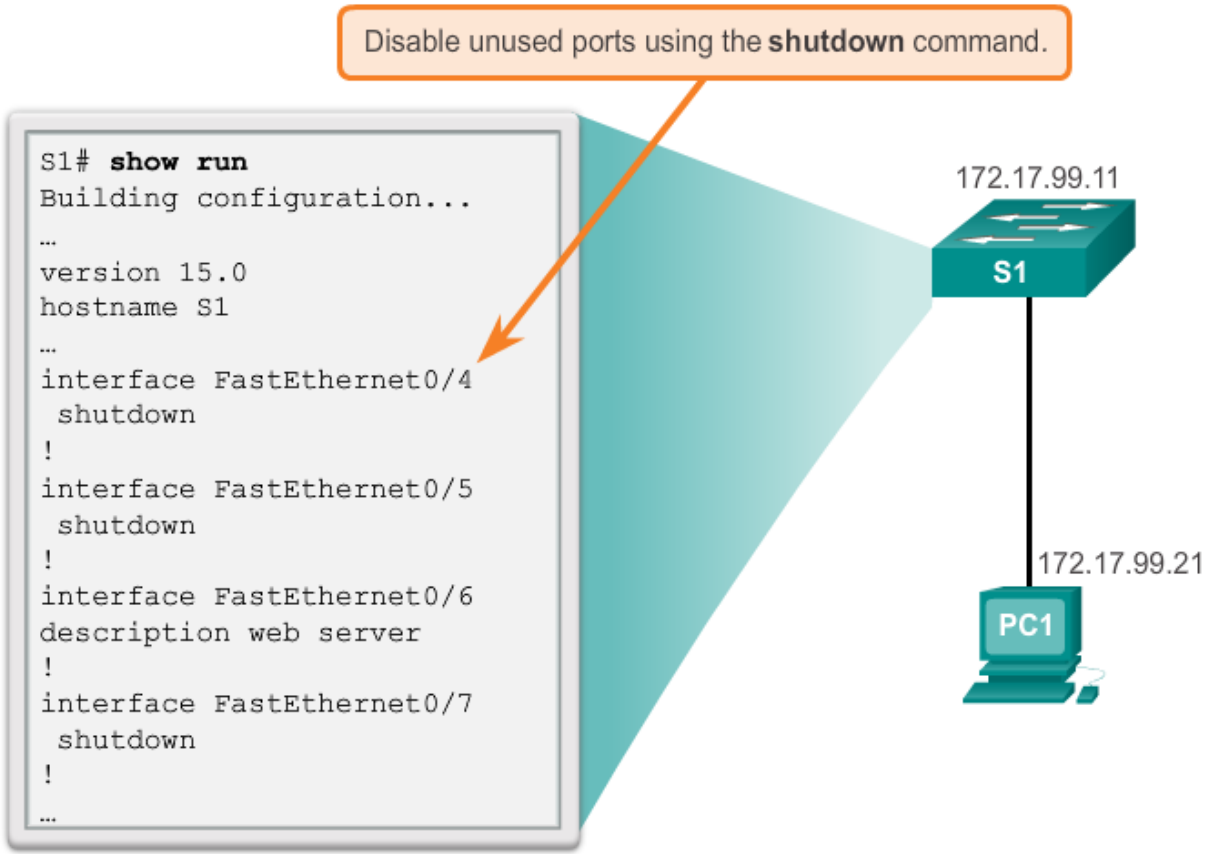
- Častým (a neželaným) javom je nekontrolované pripájanie zariadení k prepínanej sieti
  - Nové notebooky, PC, prístupové body, routery, PDA, ...
- Úlohou prepínačov v prístupovej vrstve je aj ochrana prístupu do siete
- Prepínače Cisco ponúkajú niekoľko mechanizmov na riadenie prístupu k prepínanému portu
  - (Okrem, toho, že nepoužívané porty by mali byt shutdown, next slajd)
  - Port Security
  - Autentifikácia 802.1X
  - Network Admission Control (posledné dva nie sú predmetom tohto kurzu)



Zabezpečenie portov na prepínači

Zabezpečenie nepoužívaných portov

- Nepoužívané porty vypnúť – jednoduché a efektívne
- Pozn. Neskôr bude v kurze spomínaná black hole or suspend/parking vlan



Port security

Funkcie port security

- Funkcia Port Security umožňuje na porte
  - Obmedziť počet zariadení, ktoré môžu byť pripojené k jednému rozhraniu prepínača
    - Definovaním maxima MAC adries vyskytujúcich sa na porte
  - Definovať zoznam bezpečných MAC adries staníc, ktoré smú byť pripojené k danému rozhraniu prepínača
    - Uviesť kto je bezpečný
    - Alebo nechať rozhodnúť prepínač
  - Definovať, čo sa stane, ak dôjde k porušeniu niektorého z týchto bezpečnostných pravidiel
    - Tzv. violation
    - Stanica, ktorej MAC nie je v zozname bude „*nejako*“ obmedzená

Port Security

Ktoré a koľko adries je bezpečných?

- 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 (dynamic learning)**: dynamicky získaná adresa z CAM
    - Nachádza sa len v CAM tabuľke
    - Po odpojení portu alebo reštarte prepínača sa stráca
  - **Sticky secure MAC (sticky learning)**: hybrid medzi statickou a dynamickou adresou
    - Získava sa dynamicky, no prepínač automaticky vygeneruje záznam do bežiacej konfigurácie
    - Nachádza sa v konfigurácii aj v CAM tabuľke
    - Po reštarte prepínača sa opätovne načíta z uloženej konfigurácie
- Zároveň je na porte 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)

Port Security

Reakcia na porušenie - Violation Modes

- 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

Violation Mode	Forwards Traffic	Sends Syslog Message	Displays Error Message	Increases Violation Counter	Shuts Down Port
Protect	No	No	No	No	No
Restrict	No	Yes	No	Yes	No
Shutdown	No	No	No	Yes	Yes

Port Security
Konfigurácia

- Port Security sa konfiguruje individuálne na prepínaných portoch
- Odporúčaný 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, default je dynamic learning
  - 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  CurrentAddr  SecurityViolation  Security Action
                 (Count)       (Count)          (Count)
---------------------------------------------------------------------------
      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
```

Zabezpečenie portov na prepínači

Porty v stave „Error Disabled“

- Vtedy keď je na porte nastavená akcia pri narušení na shutdown a narušenie nastane
- Port je vtedy v skutočnosti shutdown-utý
- Prepínač túto zmenu oznámi cez konzolové správy:

```
Sep 20 06:44:54.966: %PM-4-ERR_DISABLE: psecure-violation
error detected on Fa0/18, putting Fa0/18 in err-disable state
Sep 20 06:44:54.966: %PORT_SECURITY-2-PSECURE_VIOLATION:
Security violation occurred, caused by MAC address
000c.292b.4c75 on port FastEthernet0/18.
Sep 20 06:44:55.973: %LINEPROTO-5-PPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to down
Sep 20 06:44:56.971: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to down
```

Zabezpečenie portov na prepínači

Porty v stave „Error Disabled“

- Možno overiť príkazom `show interface`

```
S1# show interface fa0/18 status
Port Name   Status        Vlan   Duplex   Speed    Type
Fa0/18      err-disabled  1      auto     auto     10/100BaseTX

S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-shutdown
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 0
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 000c.292b.4c75:1
Security Violation Count   : 1
```

Zabezpečenie portov na prepínači

Porty v stave „Error Disabled“

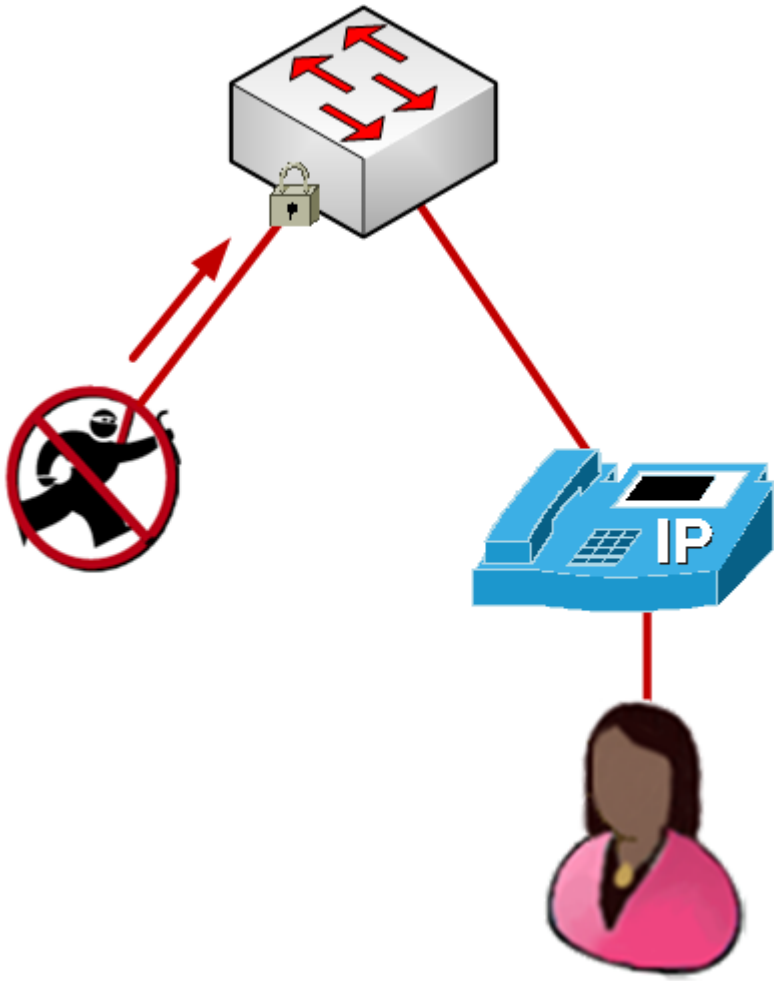
Ako znova sfunkčniť port?

`shutdown + no shutdown`

```
S1(config)# interface FastEthernet 0/18
S1(config-if)# shutdown
Sep 20 06:57:28.532: %LINK-5-CHANGED: Interface
FastEthernet0/18, changed state to administratively down
S1(config-if)# no shutdown
Sep 20 06:57:48.186: %LINK-3-UPDOWN: Interface
FastEthernet0/18, changed state to up
Sep 20 06:57:49.193: %LINEPROTO-5-UPDOWN: Line protocol on
Interface
FastEthernet0/18, changed state to up
```

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 politík)
- Cieľom nie je riadiť prístup ale ochrániť službu a prepínač



MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť!

Ohodnoť našu CNA na google:

- https://goo.gl/maps/BAnFvQKYCBpffcEX7


Cisco | Networking Academy®
Mind Wide Open™