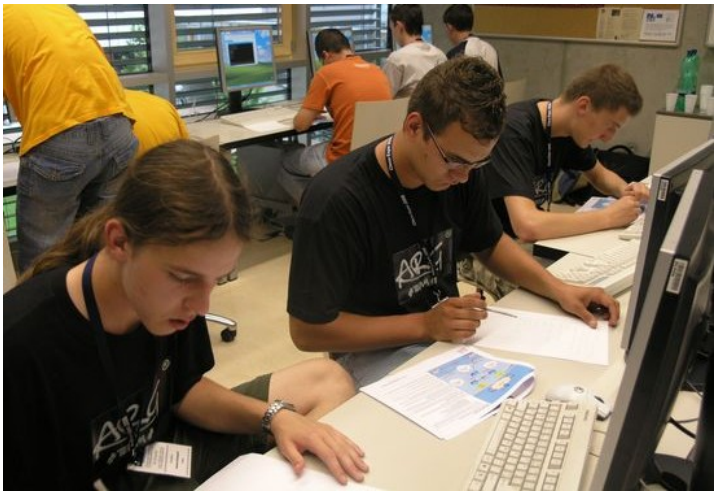
An official Newsletter of Cisco Networking Academy Program in the Slovak Republic

NetAcad Newsletter 07

Ročník 2008



Networking Academy Games 2008 (NAG 2008)—Slovenskí víťazi súťaže Cisco OLYMP 2008 zabodovali na medzinárodnej súťaži

Radi by sme sa pochválili úspechom slovenských študentov programu Sieťových akadémií. Reprezentanti Slovenska úspešne obhájili svoje vedomosti na medzinárodnom kole súťaže NETWORKING ACADEMY GAMES 2008 (NAG 2008).

Na Fakulte informatiky VUT Brno sa v dňoch 23. až 25. júna 2008 konalo medzinárodné kolo súťaže NAG 2008 – ide o súťaž budúcich profesionálov v oblasti informačných technológií so zameraním na počítačové siete (na Slovensku je to súťaž Cisco OLYMP).

následne v stredu bolo slávnostné vyhodnotenie súťaže. Všetky úlohy a zadania boli pripravené v anglickom jazyku.

Nad transparentnosťou a hodnotením celej súťaže dohliadala odborná porota, ktorá bola vymenovaná organizátorom súťaže, a ktorá pozostávala zo zástupcov/inštruktorov zo všetkých zúčastnených krajín.

Slovenska republika patri k európskej špičke v príprave budúcich sieťových profesionálov. Slovenskí študenti to potvrdili vyriešením neľahkých zadaní.

www.netacad-games.cz
NAG 2008

Na medzinárodnom kole sa zúčastnilo 50 stredoškolských a vysokoškolských študentov z 8 európskych štátov. Všetci Slovenskí študenti – desať členná skupina - dosiahli vynikajúce prvé miesta.

Počas súťaže NAG 2008 súťažiaci riešili praktické úlohy a on-line test. V pondelok 23. júna 2008 súťažili v teoretických vedomostiach, praktické zručnosti preukazovali 24. júna 2008 v laboratóriách FIT VUT Brno,

Výsledky súťaže nájdete na http://www.netacad-games.cz/results.php. Súťaž dáva študentom a ich pedagógom priestor na výmenu a zdieľanie cenných skúseností v oblasti sieťových technológií.

Radi by sme aj touto cestou zagratulovali k ich úspechom. Víťazov v jednotlivých kategóriách uvádzame nižšie. Viac informácií o súťaži, zadaniach, fotografie nájdete na stránke: **www.netacad-games.cz.**

Redakčná rada

V tomto čísle nájdete:

NetAcad

Vlado Michalec: víťaz NAG 2008 (str. 2)

Novinky

Víťazi NAG 2008 (str. 2)

PANDUIT štipendiá (str. 3)

Zadanie HS3 zo súťaže NAG (str. 4)

Zaujímavosti

Centralizované prepínanie: Catalyst 4500-E (časť 2) (str. 3)

Výročná konferencia: sprístupnené PPT prezentácie (str. 8)

Partneri programu Sieťových akadémií

Generálny partner: Slovenská sporiteľňa

Mediálny partner: PC REVUE

KONTAKT:

Ing. František Jakab, PhD.
Konzultant a koordinátor programu Sieťových akadémií pre SR
fjakab@cisco.com, www.netacad.sk

Ing. Zuzana Szabóová
Šéfredaktor časopisu NetAcad Newsletter pre SR
szaboova@elfa.sk, www.netacad.sk

Príhovor AAM

Vážená NetAcad komunita,

som nesmierne rád, že práve slovenskí študenti programu Sieťových akadémií zvíťazili na medzinárodnom kole súťaže NAG 2008 a obstáli tak v silnej medzinárodnej konkurencii. Je to dôkazom toho, že program je na Slovensku na vysokej úrovni a absolventi programu môžu byť vynikajúcimi zamestnancami.

Tiež by som touto cestou chcel poďakovať všetkým inštruktorom regionálnych akadémií, ktorí sa do prípravy súťaže NAG 2008 v Českej republike zapojili. Podelili sa o svoje minuloročné skúsenosti a napomohli vytvoriť skvelé podmienky pre súťaženie.

Rád by som Vás touto cestou pozval na medzinárodnú **konferenciu ICETA 2008**, ktorá sa uskutoční 11.-13. septembra 2008 v Starej Lesnej (viac na www.iceta.sk). V rámci programu konferencie bude mať program Sieťových akadémií svoju vlastnú sekciu a účasť zástupcov programu zo všetkých škôl je naozaj vítaná.

František Jakab
koordinátor programu
Sieťových akadémií v SR

Víťazi súťaže NAG 2008 sú z RCNA –FIIT Bratislava

V dňoch 23. - 25. júna sa v Brne za účasti 8 štátov (Slovenska, Česka, Maďarska, Nemecka, Talianska, Ukrajiny, Bulharska a Rumunska.) konal už 3. ročník medzinárodnej súťaž NAG 2008, ktorý bol pre Slovensko pokračovaním súťaže Cisco Olymp 2008. Súťaž prebiehala podobne ako u nás v troch kategóriách: UNI (súťaž jednotlivcov), HS3 (súťaž trojčlenných tímov) a PT (Packet Tracer, súťaž jednotlivcov).

S potešením môžeme konštatovať, že v tejto tvrdej konkurencii 8 štátov naši chlapci zo Slovenska obstáli najlepšie a vyhrali všetky 3 kategórie. Naša radosť a hrdosť je o to väčšia, že ide o odchovancov RCNA-FIIT Bratislava, konkrétne:

- **Vlado Michalec** (kategória UNI)
- **Marcel Duriš** (kategória PT).

Podrobnejšie informácie o priebehu, hodnotení a kategóriách nájdete na **www.netacad-games.cz**.

Obom srdečne gratulujeme a tento ich výnimočný úspech je aj úspechom celej bratislavskej RCNA-FIIT. Ďakujeme všetkým študentom našej sieťovej akadémie za šírenie dobrého mena našej RCNA-FIIT Bratislava aj za hranicami Slovenska.

Raketový štart nádejného študenta RCNA-FIIT Bratislava

Pre Cisco komunitu netreba nejako špeciálne predstavovať prvého študenta, ktorý ešte počas štúdia na Vysokej škole – FIIT Bratislava dosiahol najvyšší Cisco certifikát CCIE - routing & switching. Stále hovorím o našom Peťovi Mesjarovi, dnes už Ing. Peter Mesjar a jeho CCIE #17428.

No, ale v tomto článku by som vám rád predstavil ďalšieho nášho študenta a jeho cestu k certifikačným stupňom. Volá sa **Vlado Michalec** a v lete 2008 je v akademickom rebríčku už ako Bc. Vladimír Michalec.

Na našej fakulte FIIT STU Bratislava sa snažíme presadzovať myšlienku, že študent so zameraním počítačových systémov a sietí by ukončením Bc. štúdia mal zavŕšiť aj priemyselným CCNA certifikátom. Analogicky dosiahnutím titulu Ing. by mal zavŕšiť CCNP certifikátom. V prípade Vlada možno hovoriť o raketovom štarte... Zjednodušene povedané v druhom ročníku Bc. štúdia roku 2006 Vlado zavŕšil priemyselné CCNA. Potom nasledovalo CCNP. Ďalšie CCNP semestre Vlado už ako študent akadémie neabsolvoval, nakoľko sme ho angažovali ako ďalšieho Cisco-inštruktora našej RCNA-FIIT. Termíny skúšok k získaniu priemyselného certifikátu CCNP mal naozaj nahusto (behom pol roka absolvoval všetky štyri CCNP semestre). Vlado priemyselné CCNP zavŕšil 3. apríla 2008, kedy v lete toho istého roku získal akademický titul Bc.

Záverom možno už len konštatovať, že ak to takýmto tempom bude pokračovať, možno čoskoro budeme mať v našich radoch ďalšieho CCIE študenta.

Igor Grellneth
Inštruktor RCNA-FIIT Bratislava

Kategória HS3 – súťaž stredoškolských trojčlenných tímov

	Meno	Krajina	Škola	Spolu	Teoretický test	Praktický test
					max. 60 bodov	max. 138 bodov
					30 %	70 %
1.	Martin Bašti, Metod Rybár, Patrik Brigant	Slovensko	Spojená škola Handlová	77,34	37	116
2.	Tomas Herout, Michal Ciasnocha, Jan Hlavín	Česká republika	SSEAS, Ustí nad Labem-Stříbrníky	71,79	33	109
3.	Róbert Rakovics, Andrej Ondrejovič, Gabriel Kmeť	Slovensko	Spojená škola Handlová	70,79	31	109

Kategória PT – súťaž jednotlivcov

	Meno	Krajina	Škola	Spolu	Teoretický test	Praktický test
					max. 54 bodov	max. 126 bodov
					30 %	70 %
1.	Marcel Ďuriš	Slovensko	Spojená škola Handlová	88,33	47	112
2.	Tomas Herout	Česká republika	SSEAS, Ustí nad Labem-Stříbrníky	85,00	42	111
3.	Maroš Kukan	Slovensko	Spojená škola o.z. SPŠE S.A. Jedlíka, Nové Zámky	82,22	42	106

Kategória UNI – súťaž jednotlivcov

	Meno	Krajina	Škola	Spolu	Teoretický test	Praktický test
					max. 54 bodov	max. 100 bodov
					30 %	70 %
1.	Vladimír Michalec	Slovensko	Slovenská technická univerzita, FIIT, Bratislava	95,12	49	97
2.	Nikolay Nikolov	Bulharsko	Sofia University	89,83	42	95
3.	Andrej Krivulčík	Slovensko	Žilinská univerzita, Fakulta riadenia a informatiky, KIS	82,67	48	80

SERIÁL

Centralizované prepínanie v podobe novej rady Catalyst 4500-E (časť 2)

V minulom čísle sme sa pozreli na centralizovanú architektúru prepínača 4500-E z pohľadu komponentov. Dnes sa pozrieme, ako taká centralizovaná architektúra prepína pakety zo vstupných portov na výstupné. Taktiež sa pozrieme na novinky operačného systému IOS a CenterFlex technológie, ktoré prináša Catalyst 4500-E:

Prenos paketov zo vstupného portu na výstupný (Obr. 1.)

Základom centralizovaného prepínania v Catalyst 4500-E sú nasledujúce komponenty:

- IPP (Intelligent Packet Processor) – prepína pakety medzi vstupnými a výstupnými portami
- VFE (Very Fast Forwarding Engine) – vyhľadáva v TCAM pamäti informácie, čo treba s prijatým paketom vykonať
- Packet buffers – zdieľané pamäťové miesto pre uchovávanie všetkých prijatých paketov
- TCAM 4 (Ternary Content Addressable Memory, 4tá generácia) – pamäť hadvérovo uspôsobená pre extrémne rýchle vyhľadávanie a uchovávajúca informácie ako CEF štruktúry, QoS a bezpečnostné nastavenia

Prenos paketov môžeme v skratke popísať nasledujúcimi krokmi:

1. Paket je prijatý vstupným portom na jednej z line card. Cez backplane je paket poslaný na Supervisor 6-E, kde nad ním preberá kontrolu IPP.
2. IPP uloží celý paket do zdieľanej pamäte (packet buffer) a z prijatého paketu vytvorí PLD (packet lookup descriptor).
3. IPP posiela PLD do VFE. Na základe prijatej informácie VFE vyhľadá v TCAM 4 pamätiach informácie, ako napr. na aký výstupný port paket poslať, či vôbec paket poslať (napr. paket má byť zahodený v dôsledku PortSecurity, vstupným alebo výstupným policer-om, vstupným alebo výstupným ACL, atď.). V TCAM 4 pamätiach okrem iného nájdete aj CEF štruktúry. 4 generácia TCAM pamätí umožňuje dokonca až 4 paralelné vyhľadania. Práve pre jej výkon a schopnosť udržať informácie až o 256 tisíc IPv4 sieťach má byť neskôr implementovaná aj v najvýkonnejších Cisco CRS-1 smerovačoch.
4. Na základe vyhľadaných informácií z TCAM pamäte VFE vytvorí PTD (packet transmit descriptor). VFE posiela PTD naspäť na IPP.
5. IPP na základe informácií z PTD posiela (resp. neposiela, ak má byť paket zahodený) paket cez backplane na správny výstupný port.

Novinky operačného systému IOS

Operačný systém pre novú radu Catalsyt 4500-E je momentálne v dvoch verziách – 12.2(40)SG a 12.2(44)SG. **Prvý zo spomínaných ponúka** najmä:

- prepínanie IPv6 paketov priamo za asistencie hardvéru, čo znamená zvýšenie výkonu oproti predošlej rade Catalyst 4500 z 60Kpps na 125Mpps
- podpora TwinGig konvertera
- použitie MQC pre akúkoľvek QoS konfiguráciu
- podpora súborového systému FAT

Druhý zo spomínaných priniesol navyše najmä:

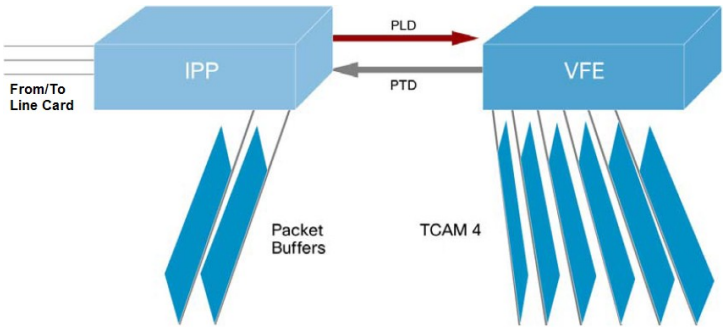
- podporu prémiového PoE s možnosťou dodať až 30W na port
- z pohľadu QoS môže byť každý port logicky rozdelený až na 8 výstupných radov (predchádzajúca rada mohla mať max. 4 výstupné rady na port)
- zníženie doby plánovaného výpadku prepínača za pomoci ISSU

Pri ISSU by som sa na chvíľočku zastavil. Na čo je to vlastne dobré? Skratka znamená In Service Software Upgrade, čo je vlastne možnosť aktualizovať softvér IOS počas prevádzky samotného zariadenia s minimálnym dopadom na prevádzku. Aby ste však mohli ISSU používať, potrebujete v jednom prepínači 2 supervisor moduly. Na ten v standby režime nahráte novú verziu IOS, zo stanby supervisor modulu spravíte aktívny (doba prepnutia je približne 150ms) a fungujete. Ak vám nový IOS vyhovuje, potvrdíte zmeny. Ak by ste však zistili, že nový IOS sa nespráva úplne podľa vašich predstáv, môžete zmenu vrátiť do pôvodného stavu. Dokonca implicitne na to máte 45 minút, po uplynutí ktorých sa systém automaticky vracia do pôvodného stavu.

Z ostatných vlastností IOS podporuje všetko, čo od prepínača potrebujete – prepínanie IPv4 a IPv6 paketov na druhej ako aj tretej vrstve, STP (PVST/PVST+, 802.1w, 802.1s), bezpečnosť na druhej a tretej vrstve (port security, DHCP snooping, IP source guard, uRPF, 802.1x, NAC), smerovacie protokoly ako RIP, OSPF a BGP a v neposlednej rade multicast (IGMP, MLD, PIM).

Na supervisor module je možnosť USB portu. Tento port však nemôžete použiť na štartovanie prepínača. Dôvodom je, že port je plnohodnotne inicializovaný až keď aj prepínač je plnohodnotne naštartovaný (takže žiadny Rommon mód). USB port preto môžete používať ako záložné médium pre IOS alebo konfiguračné súbory. Avšak je tu k dispozícii samostatný (tzv. out-of-band) 10/100Mbps RJ45 port pre naštartovanie prepínača zo siete v prípade, že naštartovanie z Flash pamäte zlyhá.

OBR. 1.



Ochrana investícií v podobe CenterFlex technológie

Veľmi peknou vlastnosťou novej CenterFlex technológie je spätná kompatibilita s predchádzajúcou generáciou Catalyst 4500 prepínačov. Do Catalyst 4500-E preto bez problémov vložíte line card moduly ako aj napäťové zdroje z predchádzajúcej generácie. Dokonca nový supervisor modul viete vložiť aj do chassis predchádzajúcej generácie Catalyst 4500 – ak máte staršiu generáciu Catalyst 4500 a potrebujete napr. zvýšiť veľkosť smerovacej tabuľky alebo IPv6 prepínanie za asistencie hardvéru, stačí vymeniť supervisor modul a nie celý prepínač.

Týmto by sme ukončili našu krátku púť novinkami v oblasti prepínačov. V jednom z budúcich čísiel sa ale pozrieme aj na novinky v oblasti smerovačov, ktoré priniesla nová rada Cisco ASR1000 (napr. 40 jadrový Cisco QuantumFlow procesor, čomu sa už povie výkon :).

Peter Mesjar
CCIE #17428
Inštruktor RCNA, FIIT STU Bratislava
(pmesjar@centrum.sk)

PANDUIT—štipendiá pre študentov

Vážená NetAcad komunita,

Radi by sme Vás informovali o možnosti získania štipendia pre Vašich študentov. Spoločnosť PANDUIT sa rozhodla poskytnúť štipendiá v rámci celého sveta vo výške $40,000. Cisco Learning Institute (CLI) bude napomáhať v administrácii tohto procesu.

V rámci tejto iniciatívy bude môcť každý študent CCNA získať **štipendium vo výške až $1000** – termín na podanie žiadosti o štipendium je do **15-teho augusta 2008**.

Ak mate záujem zapojiť sa do tejto iniciatívy, kliknite na: Cisco Learning Institute Scholarship Site (https://scholarship.ciscolearning.org/) a získajte viac informácií.

František Jakab
Koordinátor programu
Sieťových akadémií

2008 Panduit Excellence Scholarship Program

Panduit, a global manufacturer of wiring and communication applications and the sponsor of the Networking Academy Panduit Network Infrastructure Essentials (PNIE) course, has partnered with Cisco Learning Institute to provide scholarships through the Panduit Excellence Scholarship Program. This scholarship program was established to support the educational needs of post-secondary Networking Academy students in the Asia Pacific, Canada, Europe, Latin America, Middle East, and U.S. regions who are enrolled in CCNA Discovery and CCNA Exploration courses for the 2008-2009 academic year. A US$1000 scholarship will be awarded to 40 recipients to partially fund their tuition at their respective institution.

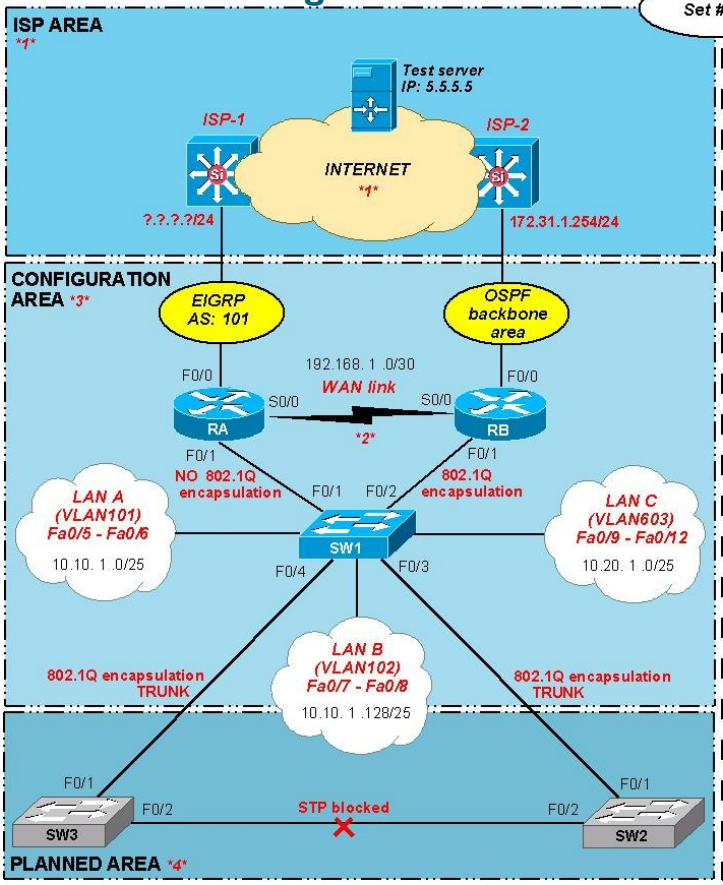
Applications will be accepted from August 1, 2008 through August 15, 2008 and all submissions must be in English. Recipients will be selected by a team of representatives from Cisco Academy Training Centers, Panduit, Cisco, and Cisco Learning Institute, and will be notified by September 1, 2008. Recipients will be chosen based on their academic achievements, community involvement, and commitment to the networking technology field.

Cisco Learning Institute encourages all CCNA students who are interested in pursuing professional careers in the networking field to apply. To submit an application online, visit the Cisco Learning Institute Scholarship Site.

Medzinárodné kolo súťaže Networking Academy Games 2008 (NAG 2008 = Cisco Olymp) organizovaná na VUT Brno, Česká Republika

ZADANIE – kategória HS3

Set # 1



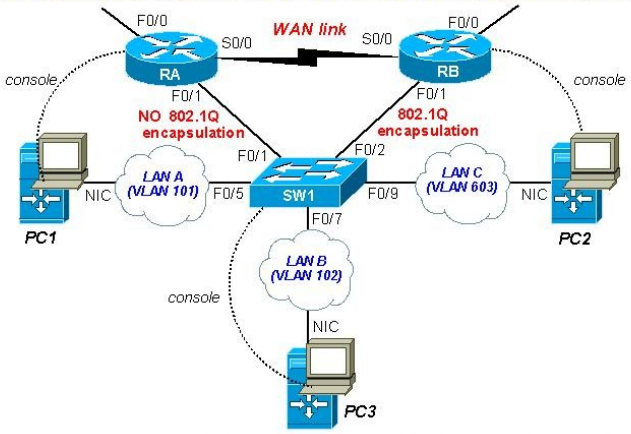
Refer to the exhibit. Network topology is physically connected and logically separated into three parts:
- ISP area, CONFIGURATION area, PLANNED area.

Notes:

1 - *ISP area represents connectivity to Internet via two internet service providers: ISP-1 and ISP-2. Internet network cloud is emulated, for testing purposes you can try to reach internet Test server at IP address 5.5.5.5*

2 - *Serial 0/0 interface may differ on modular/non modular platforms. It can be for example Serial 0/0/0 or Serial 0/1/0 in some cases. You can check the notation with "show interfaces" command*

3 - *Configuration area is part of the final network that has to be configured by student. For this purpose Computers PC1, PC2 and PC3 have their serial ports connected to console ports of routers and switch. Also network cards of computers PC1, PC2 and PC3 are connected to LAN A, LAN B and LAN C as follows:*



PC1 - console connected to router RA, ethernet NIC connected to FastEthernet 0/5 of switch SW1 (LAN A)
PC2 - console connected to router RB, ethernet NIC connected to FastEthernet 0/9 of switch SW1 (LAN C)
PC3 - console connected to switch SW1, ethernet NIC connected to FastEthernet 0/7 of switch SW1 (LAN B)

4 - *Planned area is only virtual - a reference point to the final network and refers to the planned expansion of the access layer of network in the future. Catalyst 2950 switches SW2 and SW3 are pre-configured. Concerning the tasks, you need to refer to their configuration to prepare SW1 switch for the future expansion and for connection of the switches SW2 and SW3.*

You have 60 minutes to complete the tasks. Do not hasitate to ask, if you will think that there are some physical layer issues in network topology.

Good luck!

CONFIGURATION TASKS

Physical and logical structure checking/troubleshooting

The topology is physically connected, all routers have startup configuration erased and are reloaded.

Routers inside of ISP area are configured with dynamic routing protocols as shown in the exhibit. Router ISP-1 is using EIGRP with autonomous system number 102 and ISP-2 router is using OSPF in backbone area 0. Both ISP routers are distributing default-route via dynamic routing protocol.

SW2 and SW3 switches are configured with the following commands:

```
Switch(config)# interface range FastEthernet 0/1 - 12
Switch(config-if-range)# switchport mode trunk
Switch(config-if-range)# switchport trunk native vlan 1
Switch(config)# spanning-tree vlan 1-4096 priority 4096
Switch(config)# vtp mode client
Switch(config)# vtp domain SWCXOSY001
```

5p Router RA has bootup problems and after restart it stays in ROMMON mode. Solve this bootup problem. In the case you are not able to solve this problem, ask responsible person for help. In that case you will receive 0 points per this task.

Interface Configuration (RA,RB,SW1)

6p Configure all interfaces to become operational using the address space as shown in the exhibit. Configure router RA interfaces with the lowest usable IP address in each network and also configure the highest usable IP address on interfaces at RB router for each directly connected network.

5p ISP-1 and ISP-2 inside of ISP area are completely configured with IP addressess and are running data-link layer protocol for neighbor discovery. Using information provided by this protocol, configure the FastEthernet 0/0 interface of the RA router with the lowest possible appropriate IP address.

Basic router and switch configuration (RA,RB,SW1)

5p Configure router RA so that password "strawberry" will be used when entering the privileged level. Make sure that privileged mode password is stored in running-config as MD5 encrypted.

7p Configure router RA to accept incoming telnet connections. Configure RA router so it will require password "cisco" for user-exec level for connections using the telnet service. Also, the same password should be used when connecting via console port of the router. Make sure that passwords to user-exec level are not encrypted in running-config.

4p Protect router RB so that password "secure" will be used when entering the user-exec level via console port. Make sure that password to user-exec level will be encrypted in configuration file.

5p Configure router RB to display welcome information after entering the password to user-exec level. Make sure that no other banners will be displayed.

5p Configure routers so that when the command "telnet RA" will be used at the RB router, it will automatically open the telnet session to the RA router.

5p Configure both routers so that the router RB will not be seen via CDP protocol at the RA router. Make sure that ISP-1 and ISP-2 will be able to discover RA and RB router via CDP.

CONFIGURATION TASKS

Switching configuration (SW1)

6p Create three aditional VLANs on SW1 switch with VLAN-IDs 101, 102 and 603. Assign the names LANA, LANB, LANC to VLANs 101, 102, 603, respectively.

8p Assign access ports to VLANs as shown in the exhibit. Assign ports Fa0/5 - Fa0/6 to VLAN101, Fa0/7 - 0/8 to VLAN102 and Fa0/9 - Fa0/12 to VLAN 603. Make sure that no other ports of the switch will be asigned to VLANs 102 and 603.

2p Make sure that 802.1q tagging will not be used on the line between SW1 switch and RA router. Note: Routing for LAN A should be done at RA router.

3p Configure SW1 switch to tag the frames using the 802.1q encapsulation when sending frames from VLAN102 or VLAN603 via FastEthernet 0/2 interface of SW1 switch.

6p Secure all access ports that belong to VLAN102 so there will be only two MAC addresses allowed. Make sure that when switch SW1 learns MAC address of client connected to its ethernet interface, it will store the MAC address in running-config even after the computer disconnects.

2p If any computer connected to SW1 switch violates the security policy in VLAN102, all the frames received from computer at violated port should be dropped and security violation counter should be incremented but the port should not be disabled.

5p Concerning to the initial configurations of SW2 and SW3 switches, configure the spanning tree protocol at SW1 switch so that the link between SW2 and SW3 will be blocked.

Routing configuration (RA,RB)

12p InterVLAN routing between VLANs 102 and 603 should be done at RB router. Make sure that when you trace the communication from LAN A to LAN B or LAN C, it will be routed over the WAN link between the RA and the RB router.

15p Configure both routers RA and RB so the link connected to F0/0 interfaces will be used as primary for routing packets to the internet. (LAN A reaches internet via ISP-1, LAN B and C via ISP-2, primarily). Static routing is not allowed to solve this task.

15p In the event of primary link failure, secondary link via neighboring router should be used (routed over the WAN link between RA and RB). It is not allowed to use dynamic routing protocol on WAN link with default administrative distance higher than 2.

6p Make sure, that no OSPF or EIGRP updates will be sent to Local Area Networks A, B and C.

Network filtering rules (RA,RB)

5p Configure router RB so that the CLI of routers reachable via telnet session will be allowed only from within VLAN 101. For this purpose, it is not allowed to use filtering on interface.

Note: The following ACL (next task) should not be applied at FastEthernet0/0 interface or Serial0/0 interface of the RB router.

6p Make sure that computers in LAN B and C will not be able to reach SMTP servers at internet except of server at IP address 209.208.207.206. Also make sure that computers in LANs B, C will not be able to reach internet services at destination TCP ports in range from 4001 to 4096. All other communication should be allowed.

Riešenie kategórie HS3: (pokračovanie na str. 6)

Physical and logical structure checking/troubleshooting

Smerovač RA sa nachádzal po reštartovaní v ROMMON móde, čo bolo signalizované príkazovým interpréterom s výpisom *rommon 1>*

Problém štartu smerovača spočíval v nesprávne nastavenej hodnote konfiguračného registra (0x2100). Štart smerovača bolo možné zabezpečiť zmenou konfiguračného registra na 0x2102.

```
rommon 1> confreg 0x2102
rommon 2> reset
```

Po úspešnom naštartovaní smerovača sa smerovač na konzole preukáže hlásením „*Would you like to enter initial router configuration?* [yes/no]“ čím indikuje, že nemá žiadnu konfiguráciu.

Interface Configuration (RA,RB,SW1)

V rámci zadania je dané, že pre zaadresovanie rozhraní je potrebné na smerovači RA použiť najnižšie použiteľné logické adresy a na smerovači RB najvyššie použiteľné logické adresy. Z nastavenej logickej adresy rozhrania ISP-2 je možné dedukovať adresný priestor použitý na prepoj RB<->ISP-2.

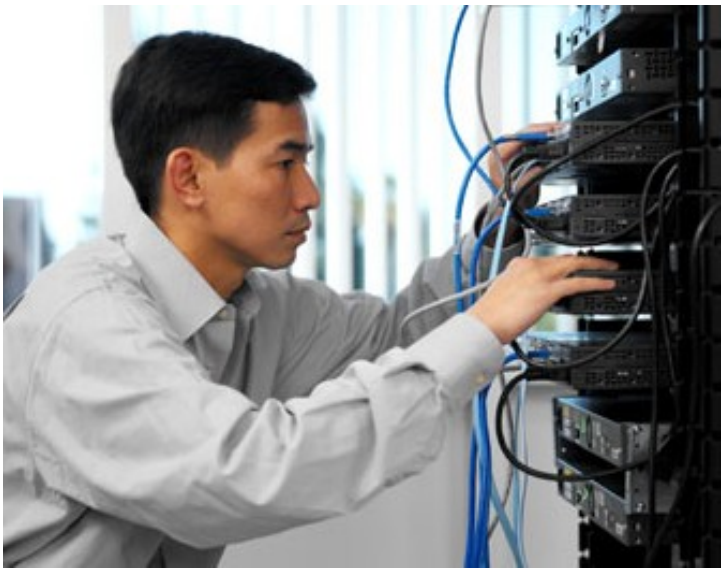
ISP-1 a ISP-2 v oblasti ISP sú nakonfigurované a teda aj ich rozhrania sú zaadresované s príslušnými logickými adresami. V rámci zadania nie je uvedené aký adresný priestor je použitý voči ISP-1 zo smerovača RA. V zadaní je naznačené, že ISP-1 využíva protokol druhej vrstvy, ktorý umožňuje detekciu susedných zariadení a ich nastavení. Využitím CDP protokolu je možné získať nastavenia logickej adresy na rozhraní susedného zariadenia.

Prostredníctvom príkazu: *RA# show cdp neighbor detail*

je možné zistiť, že ISP-1 má na svojom rozhraní, ktorým sa pripája k smerovaču RA nastavenú logickú adresu 172.30.1.254. Na základe uvedených a získaných informácií je možné definovať adresné priestory nasledovne. Prepoj ISP-1 a RA využíva adresný priestor 172.30.1.0/24 (zistené prostredníctvom CDP) a ISP-2 voči smerovaču RB využíva adresný priestor 172.31.1.0/24 (dané v zadaní). Logické adresy rozhraní smerovačov ISP-1 a ISP-2 majú nastavené logické adresy 172.30.1.254 a 172.31.1.254, ktoré sú nepoužiteľné pre susedné zariadenia (RA,RB) keďže sú už použité.

Zo zadania vyplýva, že smerovač RA musí na svojom rozhraní FastEthernet0/0 na základe zadaného pravidla vyžitia najnižších logických adries vyžiť logickú adresu 172.30.1.1 a smerovač RB na základe zadaného pravidla využitia najvyšších logických adries IP adresu 172.31.1.253. Sériová WAN linka medzi smerovačmi RA a RB má definovaný adresný priestor 192.168.1.0/30 z ktorého na základe pravidiel o najvyšších a najnižších logických adresách je možné dedukovať logickú adresu 192.168.1.1 pre smerovač RA a logickú adresu 192.168.1.2 pre smerovač RB.

Z kontextu zadania a naznačených zapúzdrení prostredníctvom 802.1q voči prepínaču SW1 je evidentné, že smerovač RA smeruje prevádzku pre sieť LAN A bez využitia zapúzdrenia 802.1q. Smerovač RB smeruje prevádzku pre siete LAN B a C s využitím 802.1q (tzv. routing-on-the-stick). Z uvedených kritérií pre výber logických adries, ktoré majú byť na smerovači nastavené je možné určiť logickú adresu brány (F0/1) pre jednotlivé siete. V sieti LAN A ide o logickú adresu 10.10.1.1, v sieti LAN B o logickú adresu 10.10.1.254 a v sieti LAN C o logickú adresu 10.20.1.126. Pre nastavenie sub-rozhraní na smerovači RB pre LAN B a C je potrebné identifikovať VLAN ID, ktorými budú rámce pri preposielaní do lokálnej siete značené. V zadaní je priamo naznačené, že sieť LAN B využíva VLAN ID - 102 a sieť LAN C – VLAN ID 603. Smerovač RA nevyžíva značenie rámcov prostredníctvom 802.1q a preto nie je potrebné vytvárať sub-rozhrania a logickú adresu je možné nastaviť priamo na rozhraní FastEthernet0/1 smerovača RA.



```
RA(config)# interface FastEthernet 0/0
RA(config-if)# ip address 172.30.1.1 255.255.255.0
RA(config-if)# no shutdown
RA(config)# interface FastEthernet 0/1
RA(config-if)# ip address 10.10.1.1 255.255.255.128
RA(config-if)# no shutdown
RA(config)# interface Serial 0/0
RA(config-if)# ip address 192.168.1.1 255.255.255.252
RA(config-if)# no shutdown

RB(config)# interface FastEthernet 0/0
RB(config-if)# ip address 172.31.1.253 255.255.255.0
RB(config-if)# no shutdown
RB(config)# interface FastEthernet 0/1
RB(config-if)# no shutdown
RB(config)# interface FastEthernet0/1.102
RB(config-subif)# encapsulation dot1q 102
RB(config-subif)# ip address 10.10.1.254 255.255.255.128
RB(config)# interface FastEthernet0/1.603
RB(config-subif)# encapsulation dot1q 603
RB(config-subif)# ip address 10.20.1.126 255.255.255.128
RB(config)# interface Serial 0/0
RB(config-if)# ip address 192.168.1.2 255.255.255.252
RB(config-if)# no shutdown
```

Poznámka: Na sériovej linke medzi smerovačmi RA a RB nebolo definované, ktorá strana sériovej linky je DCE a ktorá DTE. Na základe výstupu z príkazu *RA# show controllers Serial 0/0* je možné identifikovať, či je na strane sériového rozhrania smerovača RA rozhranie typu DCE alebo DTE. Na základe zistenej informácie je potrebné na strane DCE aplikovať nastavenie rýchlosti príkazom *clock rate* na sériovom rozhraní na ľubovoľnú rýchlosť, keďže rýchlosť linky nebola v zadaní stanovená.

Basic router and switch configuration (RA,RB,SW1)

V zadaní je uvedené, že smerovač RA musí vyžiadať heslo pre prístup do privilegovaného režimu „strawberry“ pričom heslo musí byť uložené v šifre MD5. Z uvedeného je evidentné, že jediná možnosť kedy je heslo uložené v podobe MD5 je využitím príkazu *enable secret*. Riešením je teda sekvencia príkazov:

```
RA# configure terminal
RA(config)# enable secret strawberry
```

Smerovač RA musí pri vstupe do používateľského režimu prostredníctvom konzoly alebo virtuálneho terminálu (telnet) vyžadovať heslo “cisco”. Vzhľadom na to, že heslo nesmie byť šifrované v konfigurácii, nie je možné použiť službu šifrovanie – *service password-encryption*. Príkaz login je implicitný na virtuálnych termináloch, preto je potrebné ho zadať iba na konzole.

```
RA(config)# line console 0
RA(config-line)# password cisco
RA(config-line)# login
RA(config)# line vty 0 4
RA(config-line)# password cisco
```

Na smerovači RB je potrebné zabezpečiť, aby sa vyžadovalo heslo „secure“ pri prístupe do používateľského režimu prostredníctvom konzoly, avšak heslo musí byť v konfigurácii šifrované. Toto je možné zabezpečiť prostredníctvom služby *service password-encryption*. Riešením úlohy je nasledovná sekvencia príkazov:

```
RB(config)# service password-encryption
RB(config)# line console 0
RB(config-line)# password secure
RB(config-line)# login
```

Na smerovači RB je ďalej potrebné zabezpečiť, aby sa uvítacia hláška (banner) vypísala až po zadaní hesla do používateľského režimu. Žiadne iné uvítacie hlášky neboli povolené. Riešením úlohy je nasledovná sekvencia príkazov:

```
RB(config)#  banner exec # Welcome.... #
```

Riešenie kategórie HS3: (pokračovanie na str. 7)

Na smerovači RB bolo potrebné zabezpečiť, aby sa po spustení príkazu „telnet RA“ automaticky otvorilo telnetové spojenie na smerovač RA. Toto bolo možné docieliť lokálnou tabuľkou logických adries prislúchajúcich k menám smerovačov (host table).

```
RB(config)# ip host RA 192.168.1.1
```

Posledná úloha tejto sekcie naznačuje potrebu manipulácie nastavení CDP protokolu tak, aby bolo možné protokol CDP využívať na linke voči ISP avšak nie voči susednému smerovaču na sériovej linke. Riešením je ponechať CDP zapnuté globálne, avšak vypnúť ho na rozhraní Serial 0/0.

```
RA(config)# interface Serial 0/0
RA(config-if)# no cdp enable
```

Switching configuration (SW1)

Na prepínači SW1 bolo potrebné vytvoriť 3 VLAN siete s pridelenými menami – LANA, LANB a LANC a príslušnými VLAN ID 101,102 a 603.

```
SW1(config)# vlan 101
SW1(config-vlan)# name LANA
SW1(config)# vlan 102
SW1(config-vlan)# name LANB
SW1(config)# vlan 603
SW1(config-vlan)# name LANC
```

Porty prepínača boli v zadaní priradené k jednotlivým VLAN sieťam, čo bolo možné vykonať nasledovnou sekvenciou príkazov. Zároveň je potrebné si uvedomiť, že na porte FastEthernet0/1 voči smerovaču RA nie je použité zapúzdrenie 802.1q a teda sa jedná o obyčajný “access” port. Naproti tomu, rozhranie FastEthernet0/2 zapúzdrenie 802.1q využíva a vzhľadom na to je potrebné toto rozhranie konfigurovať ako TRUNK port. Rovnako porty FastEthernet 0/3 a 0/4, ktoré sú plánované pre pripojenie ďalších prepínačov je potrebné konfigurovať ako TRUNK porty so zapúzdrením 802.1q.

```
SW1(config)# interface range FastEthernet 0/5 – 6
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# switchport access vlan 101
SW1(config)# interface range FastEthernet 0/7 – 8
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# switchport access vlan 102
SW1(config)# interface range FastEthernet 0/9 – 12
SW1(config-if-range)# switchport mode access
SW1(config-if-range)# switchport access vlan 603

SW1(config)# interface FastEthernet 0/1
SW1(config-if)# switchport mode access
SW1(config-if)# switchport access vlan 101

SW1(config)# interface range FastEthernet 0/2 – 4
SW1(config-if-range)# switchport mode trunk
```

Všetky porty prislúchajúce do VLAN 102 bolo potrebné zabezpečiť (port-security) tak, aby umožňovali zaznamenanie maximálne dvoch fyzických adries na každom porte (maximum mac-address 2), pričom bolo potrebné zabezpečiť, aby sa naučené fyzické adresy uložili do konfigurácie prepínača a aby boli dostupné v konfigurácii aj v prípade odpojenia zariadenia z fyzického rozhrania prepínača (sticky). Zároveň je potrebné zvoliť typ akcie pri porušení bezpečnostnej politiky tak, aby boli rámce zahadzované, avšak aby bolo možné sledovač zvyšovanie hodnoty počítadla porušení bezpečnostnej politky (restrict).

```
SW1(config)# interface range FastEthernet 0/7 – 8
SW1(config-if-range)# switchport port-security
SW1(config-if-range)# switchport port-security maximum 2
SW1(config-if-range)# switchport port-security mac-address sticky
SW1(config-if-range)# switchport port-security violation restrict
```

Vzhľadom na plánované pripojenie prepínačov SW2 a SW3 a s ohľadom na ich konfiguráciu je potrebné zabezpečiť, aby bola linka medzi prepínačmi SW2 a SW3 po pripojení do topológie blokovaná. Je potrebné si uvedomiť, že štandardná (default) priorita spanning-tree protokolu je 32768, ktorá bola na prepínačoch SW2 a SW3 zmenená (zadané – priorita 4096). Po pripojení takto nakonfigurovaných prepínačov bude mať prepínač SW1 štandardne prioritu 32768, SW2 a SW3 4096 a teda ako Root bridge v spanning-tree protokole sa zvolí jeden z prepínačov SW2 alebo SW3. Ako dôsledok tohoto stavu, bude mať root bridge všetky porty „designated” a nebudú blokované. Keďže v topológii vznikne slučka a linka medzi root-bridge prepínačom a susedmi nemôže byť blokovaná, jediné linky ktoré môžu byť blokované tvoria prepoj SW1 a SW2 alebo SW1 a SW3. Keďže požadovaný stav je, aby bola linka medzi SW1 a SW2 blokovaná, je potrebné zabezpečiť, aby sa SW1 stal root-bridge prepínačom a mal svoje porty voči prepínačom SW2 a SW3 designated. Toto je možné zabezpečiť tak, že sa na prepínači SW1 nastaví priorita STP pre VLAN siete, ktorých sa to týka.

```
SW1(config)# spanning-tree vlan 1,101,102,603 priority 0
```

Routing configuration (RA,RB)

Smerovanie medzi sieťami LAN B a LAN C sa automaticky realizuje na smerovači RB nakoľko je tento smerovač nakonfigurovaný pre tzv. routing-on-the stick a zároveň je jediným smerovačom, ktorý spracováva rámce značené pre VLAN siete s ID 102 a 603. Podobne, v dôsledku konfigurácie portu FastEthernet0/1 prepínača SW1 ako prístupového portu bez značenia rámcov je možné komunikáciu z VLAN 101 smerovať cez FastEthernet0/1 rozhranie smerovača RA.

Zadanie uvádza, že je potrebné zabezpečiť, aby komunikácia medzi sieťami LAN A a sieťami LAN B a C bola smerovaná po sériovej linke medzi smerovačmi RA a RB. Túto úlohu je možné zabezpečiť statickým smerovaním.

```
RA(config)# ip route 10.10.1.128 255.255.255.128 serial 0/0
RA(config)# ip route 10.20.1.0 255.255.255.128 serial 0/0
RB(config)# ip route 10.10.1.0 255.255.255.128 serial 0/0
```

Pre komunikáciu voči ISP je potrebné nakonfigurovať smerovacie protokoly EIGRP (AS 101) a OSPF v oblasti 0, pričom je potrebné oznámiť lokálne siete. Sériová WAN linka medzi smerovačmi RA a RB nesme využívať dynamický smerovací protokol. Podobne, smerovacie informácie nie je potrebné posielať do lokálnych sietí. Je potrebné si uvedomiť, že smerovač RB využíva routing-on-the stick a aplikácia príkazu *passive-interface FastEthernet0/1* sa vzťahuje iba na rámce, ktoré sú neznačené (native vlan) avšak nie na rámce označené a spracovávané v rámci sub-rozhraní. Vzhľadom na to, že je adresný priestor triedy A rozdelený na viacero podsietí a fyzicky oddelený WAN linkou vzniká tzv. „discontigous networks“ problém, ktorý je možné riešiť vypnutím automatickej sumarizácie v konfigurácii EIGRP protokolu. Základná konfigurácia dynamického smerovania s obmedzením vysielania informácií smerovacích protokolov do lokálnych sietí je vykonateľná nasledovnou sekvenciou príkazov:

```
RA(config)# router eigrp 101
RA(config-router)# no auto-summary
RA(config-router)# network 172.30.1.0 0.0.0.255
RA(config-router)# network 10.10.1.0 0.0.0.127
RA(config-router)# passive-interface FastEthernet 0/1

RB(config)# router ospf 1
RB(config-router)# network 172.31.1.0 0.0.0.255 area 0
RB(config-router)# network 10.10.1.128 0.0.0.127 area 0
RB(config-router)# network 10.20.1.0 0.0.0.127 area 0
RB(config-router)# passive-interface FastEthernet0/1.102
RB(config-router)# passive-interface FastEthernet0/1.603
```

Základnou konfiguráciou dynamických smerovacích protokolov smerovače RA a RB automaticky získali predvolenú bránu (default route) smerom k ISP, ktorý je bližšie. Keďže je v zadaní definované, že komunikácia má byť primárne smerovaná prostredníctvom smerovača ISP, ktorý je k okrajovému smerovaču RA a RB bližšie, základná konfigurácia zabezpečí túto funkcionalitu propagáciou predvolenej brány.

Riešenie kategórie HS3:

V prípade výpadku primárnej linky je potrebné zabezpečiť, aby sa smerovanie do siete internetu odklonilo a zabezpečilo prostredníctvom susedného zariadenia (tj. v prípade výpadku linky voči ISP-1 je prevádzka odklonená prostredníctvom smerovača RB, následne ISP-2 do siete internetu a naopak, v prípade výpadku linky k ISP-2 je prevádzka z LAN B a C odklonená na smerovač RA a následne prostredníctvom ISP-1 smerovaná do siete internetu).

Odklonenie smerovania je možné docielit' prostredníctvom staticky definovanej predvolenej brány (default route), avšak je potrebné konfiguráciu upraviť tak, aby sa staticky definovaná brána (prostredníctvom susedného zariadenia) aplikovala až v prípade výpadku primárnej trasy. Je potrebné si uvedomit', že predvolená brána (default route) je propagovaná v rámci dynamického smerovacieho protokolu zo strany ISP-1 a ISP-2. V prípade výpadku linky voči ISP sa stane zároveň dynamický smerovací protokol voči ISP nefunkčným a ako dôsledok bude dynamicky naučená predvolená brána vyradená zo smerovacej tabuľky. V staticky definovanej predvolenej bráne je potrebné definovat' administrative distance, ktorý by bol menej výhodný ako predvolená brána naučená dynamicky. V prípade výpadku dynamického smerovania síce bude využitá predvolená brána s „horším" administrative distance ako primárnej linky, avšak v takejto situácii pôjde o jediný možný smer.

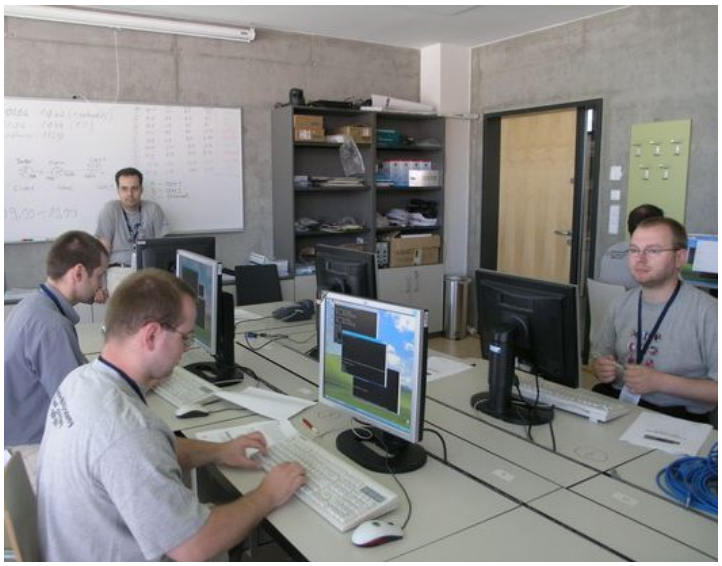
Je potrebné si taktiež uvedomit', že predvolená brána je oznámená zo strany ISP -1 s administrative distance 170 a teda pre záložnú trasu je potrebné použiť' administrative distance 171 a viac. V prípade protokolu OSPF je predvolená brána oznámená s administrative distance 110 a teda pre záložnú trasu je potrebné použiť' administrative distance 111 a vyššie.

```
RA(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0 171
RB(config)# ip route 0.0.0.0 0.0.0.0 serial 0/0 111
```

Odklonenie prevádzky na susedné zariadenie však ešte nerieši „fault-tolerant" smerovanie úplne. Je potrebné si uvedomit', že pre zasmerovanie požiadaviek do siete internetu z klienta je potrebné mat' vytvorenú obojsmernú cestu a teda byt' schopný dáta zasmerovat' aj späť' ku klientovi. V prípade odklonenia prevádzky voči susednému zariadeniu staticky sa dáta zasmerujú prostredníctvom ISP až do siete internetu, avšak pri generovaní odpovede klientovi smerovač ISP nemá informáciu získanú dynamicky, kadiaľ' sú príslušné zdrojové siete dosiahnuteľné. V prípade výpadku linky RA<->ISP-1 je teda komunikácia odklonená na smerovač RB, následne na ISP-2 a smerovaná do siete internetu. V smerovacej tabuľke ISP-2 však neexistuje informácia o spätnej ceste k sieti LAN A, nakoľko táto sieť' nemohla byt' oznámená zo smerovača RB prostredníctvom príkazu *network* (nepôjde o priamo pripojenú sieť', ktorú je možné takto oznámiť'). Riešením tohto problému je redistribúcia statických smerov do dynamického smerovacieho protokolu, nakoľko dostupnosť' susedných sietí je v dôsledku požiadavky priameho smerovania po WAN linke riešená statickým smerom (static route).

```
RA(config)# router eigrp 101
RA(config-router)# redistribute static

RB(config)# router ospf 1
RB(config-router)# redistribute static
```



Network filtering rules (RA,RB)

Telnetové spojenia na smerovač RB je potrebné zabezpečiť' tak, aby bolo možné pristupovať' k virtuálnemu terminálu výhradne iba z vnútra siete VLAN 101 s adresným priestorom 10.10.1.0/25. Za týmto účelom nie je povolené aplikovať' filter sieťovej prevádzky na rozhraní.

Riešením je vytvorenie filtra sieťovej prevádzky (ACL), ktorý povoľuje prístup zo siete VLAN 101 a všetky ostatné zdroje zakazuje. Keďže je potrebné rozhodovať' sa iba na základe zdrojovej adresy, na riešenie tejto úlohy postačuje štandardný ACL, či už číslovaný alebo pomenovaný) a jeho nasledovná aplikácia na virtuálny terminál.

```
RB(config)# access-list 1 permit 10.10.1.0 0.0.0.127
RB(config)# line vty 0 4
RB(config-line)# access-class 1 in
```

Je potrebné zabezpečiť', aby z lokálnych sietí LAN B a C bol dosažiteľný výhradne iba SMTP server 209.208.207.206 (tcp/25). Prevádzka na TCP portoch v rozsahu 4001 až 40096 nesmie byt' povolená, avšak štandardná politika je „čo nie je zakázané, je povolené". Vzhľadom na obmedzenie zadania je evidentné, že takýto filter sieťovej prevádzky nie je možné aplikovať' na rozhrania FastEthernet 0/1 a Serial0/0. Z toho vyplýva, že prevádzku je potrebné filtrovať' na vstupe zo sietí LAN B a C na sub-rozhraniach smerovača RB.

Je potrebné si uvedomit', že aplikácia filtra sieťovej prevádzky na fyzickom rozhraní smerovača FastEthernet0/1 nefiltruje zároveň prevádzku aj na jeho sub-rozhraniach. Filter sieťovej prevádzky aplikovaný na fyzickom rozhraní FastEthernet0/1 sa aplikuje len pre neznačenú komunikáciu (native vlan). Keďže je potrebné prevádzku filtrovať' z lokálnych sietí LAN B a C, filter sieťovej prevádzky je potrebné aplikovať' na sub-rozhraniach FastEthernet0/1.102 a FastEthernet0/1.603 smerovača RB.

Z pohľadu návrhu filtra sieťovej prevádzky nie je nutné striktne rozlišovať' zdrojovú sieť' a klasifikovať' ju ako LAN B a LAN C, nakoľko všetka komunikácia ktorá sa bude definovaným ACL filtrovať' bude pochádzať' z lokálnej siete LAN B alebo C. Vzhľadom na potrebu filtrovania na základe protokolu a portu je nutnosťou použitie rozšíreného ACL (či už číslovaného alebo pomenovaného).

```
RB(config)# ip access-list extended FILTER
RB(config-ext-nacl)# permit tcp any host 209.208.207.206 eq 25
RB(config-ext-nacl)# deny tcp any any eq 25
RB(config-ext-nacl)# deny tcp any any range 4001 4096
RB(config-ext-nacl)# permit ip any any

RB(config)# interface FastEthernet0/1.102
RB(config-subif)# ip access-group FILTER in
RB(config)# interface FastEthernet0/1.603
RB(config-subif)# ip access-group FILTER in
```

Peter Feciľak,
Inštruktor RCNA, TU v Košiciach
člen organizačného tímu NAG 2008,
(fecilak-cnl@cnl.tuke.sk)

NetAcad Newsletter 07/08

MULTICAST INSTRUCTOR NEWS

Vážená NetAcad komunita,
radi by sme Vám predstavili novinku v komunikácii medzi inštruktormi programu Sieťových akadémií.

Zástupcovia Cisco Networking Academy programu budú v štvrťročných intervaloch pripravovať pre Vás Newsletter pod názvom - **MULTICAST INSTRUCTOR NEWS**, ktorý bude zameraný na BEST PRACTICE od inštruktorov, analýzu nových curricúl, pomoc od kolegov/ inštruktorov, nové technológie budúcnosti, diskusie, kvízy a pod.

Ak budete mať chuť zapojiť sa, Vaša iniciatíva je vítaná – pôjde predsa o Newsletter inštruktorov pre inštruktorov.

Newsletter bude pripravovaný v Angličtine, a zaujímavé príspevky Vám budeme predstavovať aj v našom mesačníku NetAcad Newsletter. Pevne veríme, že si ho obľúbite a napomôže Vám lepšie sa pripraviť na hodiny programu Sieťových akadémií.

Najbližšie číslo bude obsahovať tieto témy:

- A feature on WHO WRITES CCNA and an invitation for instructors and academies to give feedback
- Best Practice in TEACHING CCNA from two of our top instructors
- Cisco's green agenda and policies explained and a featurette on recycling routers
- Curriculum quiz
- COMPETITION sponsored by Cisco Press.

Please, look for the newsletter which will be **emailed directly to you the week beginning July 21st.**

František Jakab
koordinátor programu
Sieťových akadémií pre SR
fjakab@cisco.com

Výročná konferencia programu NetAcad—sprístupnené PPT prezentácie

Chceli by sme Vás informovať o zmenách na stránke www.netacad.sk.

7. ročník výročnej konferencie programu Sieťových akadémií je úspešne za nami. Konferencia patrí k najvýznamnejším odborným podujatiam zameraným na sieťové technológie a vzdelávanie sieťových profesionálov, preto sme sa rozhodli sprístupniť celej NetAcad komunite program konferencie **- program aj s videami a PPT prezentáciami** nájdete na našich stránkach.

Dúfame, že prednášky domácich a zahraničných expertov budú pre Vás prínosom a pomôžu Vám pri implementácii program na Vašich školách. Naša vďaka patrí aj všetkým partnerom, ktorí konferenciu podporili a bez ktorých by program na Slovensku nemohol mať takú skvelú úroveň.

Zuzana Szaboova
Organizátor výročnej konferencie
programu Sieťových akadémií
szaboova@elfa.sk

PARTNERI VYROCNEJ KONVERENCIE

OZNAM: NOVÝ ŠKOLSKÝ ROK

Vážená NetAcad komunita,

radi by sme Vás upozornili na zmeny v programe Sieťových akadémií. Ako isto už viete v novom školskom roku **budú musieť všetky akadémie prejsť na výučbu novej verzie curricúl (4.1)** – škola má možnosť si vybrať výučbu verzie **DISCOVERY** alebo **EXPLORATION**.

- Posledná možnosť pre vytvorenie študentskej triedy vo verzii 3.1 – kurz CCNA 1 – bola 31. marca 2008.
- Posledná možnosť pre vytvorenie študentskej triedy vo verzii 3.1 – kurz CCNA 2-4 – bude 31. január 2009

Viac informácii o termínoch nájdete v **NetAcad newsletteri – 05/08**.

Tiež by sme Vás chceli upozorniť, že **akadémie, ktoré neotvoria v priebehu pol roka** (v novom školskom roku) **aspoň jednu triedu** (v novej verzii, s min. 5 študentmi v triede) **budú navrhnuté na zrušenie**.

Chceme Vás touto cestou poprosiť, aby ste do nového školského roka zabezpečili prechod Vašej akadémie na nove curricula.

V prípade otázok kontaktujte: fjakab@cisco.com.

František Jakab
Koordinátor programu Sieťových akadémií
fjakab@cisco.com

VTIPY ☺

Náhrobný kameň programátora:
Príčina smrti: Run Time Error at 18:30:04
Príčina narodenia General Protection Fault at 16:20:35