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

NetAcad Newsletter 06

Ročník 2009

Medzinárodný úspech pedagógov NetAcad zo Slovenska

V dňoch 22. a 23. mája 2009 sa na Polytechnickej univerzite v Bukurešti uskutočnilo finále 2. ročníka medzinárodnej súťaže pedagógov (inštruktorov) škôl strednej a východnej Európy, zapojených do program Sieťových akadémií Cisco – súťaž **iCompetition 2009**.

Do súťaže sa zapojilo viac ako 200 pedagógov stredných a vysokých škôl, ktorí od marca 2009 absolvovali dištančne 3 kvalifikačné kola prostredníctvom portálu súťaže.

Do finále súťaže v Bukurešti sa kvalifikovalo 10 pedagógov (3 zo SR, 2 z Ukrajiny, 2 z Rumunska a po jednom z ČR, Bulharska a Turecka).

Finále súťaže skončilo veľkým úspechom práve pedagógov zo SR, ktorí boli v rámci súťaže najúspešnejší.

- **Celkovým víťazom súťaže sa stal Peter Palúch zo Žilinskej univerzity.**
- **Peter Feciľak z Technickej univerzity v Košiciach sa umiestnil na 5. mieste**
- **a Tomáš Kanocz, tiež z Technickej univerzity v Košiciach sa umiestnil na 8. mieste.**

Samotný priebeh dvojdňovej súťaže bolo možné sledovať prostredníctvom video IP streamingu, ktorého vysielanie zabezpečoval Videotím z Technickej univerzity v Košiciach (http://videoserver.cnl.tuke.sk). Viac informácií o priebehu súťaže je možné nájsť na www.icompetition.net.

Súťaž iCompetition 2009 ukázala, že úspechy, ktoré dosahujú študenti programu Sieťových akadémií zo Slovenska v medzinárodných súťažiach nie sú náhodne. Aj ich učitelia patria k medzinárodnej špičke.

František Jakab
koordinátor programu
Sieťových akadémií v SR

V tomto čísle nájdete:

Partneri programu Sieťových akadémií

Generálny partner

Mediálny partner

Partneri

KONTAKT:

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

Ing. Zuzana Fedáková
Šéfredaktor časopisu NetAcad Newsletter pre SR
netacad@netacad.sk, www.netacad.sk

Príhovor AAM

Vážená komunita,

šk. rok už máme takmer za sebou. Ešte využime posledné možnosti napraviť to, čo sme „pokazili“, prípadne nie celkom úspešne realizovali, aby sme do nového šk. roku išli s čistým štítom.

V uplynulom školskom roku došlo zase v rámci programu Sieťových akadémií **k niekoľkým významným zmenám.** Niektoré sa nám páčili viac, iné menej. Ukázalo sa, že zavedenie nových verzií vzdelávacích materiálov - Discovery a Exploration a podstatne významnejšie využívanie novej verzie Packet Tracer vo výučbovom procese bolo študentmi prijaté kladne. Zvlášť je vysoko hodnotené metodické využívanie simulačných vlastnosti PT a to, že študenti si majú možnosť nainštalovať a využívať aj na svojich osobných počítačoch. Je naozaj škoda, že dlho očakávané kurzy CCNA VoIP a CCNA WiFi nebudú zatiaľ do programu zavedené. Ako dočasnú náhradu, zvlášť pre inštruktorov programu, ponúkame účasť na Letnej škole NetAcad 2009, v rámci ktorej by sme radi ponúkli nielen možnosť absolvovať štandardné kurzy v skrátenom čase, ale aj práve v zozname kurzov chýbajúci a zo strany akadémií žiadaný kurz venovaný problematike VoIP.

Čo je však najdôležitejšie: Očakávame, že **Letná škola** už tradične vytvorí priestor nielen na vzdelávanie, ktoré je vedené špičkovými pedagógmi, ale aj na výmenu skúsenosti, vytváranie nových kontaktov, a priateľstiev.

Nechcem robiť záverečné hodnotenie minulého školského roku, pretože ešte máme pred sebou také významné aktivity ako sú **medzinárodné kolo súťaže NAG 2009**, ktoré tento rok bude opäť organizované na Slovensku, (*FIIT STU BA, 25.-26.6.2009*) za účasti súťažiacich z krajín strednej a východnej Európy. Verím, že aj tento rok nás budú naši študenti dobre reprezentovať a že sa zopakuje minuloročný úspešný „scenár“ zo súťaže v Brne.

Dovoľujem si ešte touto cestou vyzvať pedagógov programu k aktívnej účasti na významnej medzinárodnej konferencii, ktorá je venovaná využívaniu IKT vo vzdelávaní, **ICETA 2009** (www.iceta.sk) a na ktorej už tradične bude mať program samostatnú sekciu

No a samozrejme ešte ráz by som Vás chcel aj osobne pozvať na našu najvýznamnejšiu tohtoročnú aktivitu – **výročnú konferenciu programu NetAcad**, ktorá sa tento rok bude konať v Brne.

Toto číslo Newslettera je posledné v tomto školskom roku (v letných mesiacoch má Newsletter “prestávku”) a nové číslo bude vydané až v novom školskom roku - v septembri. Preto by som Vám chcel touto cestou popriať príjemné strávenie letných prázdnin, aby sme sa v novom šk. roku stretli plní síl a entuziazmu a aby nový školský rok bol pre nás ešte úspešnejší. Verím, že sa o svoje zážitky z leta s nami podelíte, a že septembrové číslo bude plné Vašich “sieťových aj nesieťových” zážitkov.

František Jakab

iCompetition: víťazstvo slovenských inštruktorov

Slovenskí pedagógovia boli vo finále súťaže iCompetition najúspešnejší

Inštruktori sieťových akadémií zo Slovenska dosiahli veľký medzinárodný úspech. Vo finále 2. ročníka súťaže pedagógov škôl zo strednej a východnej Európy zapojených do programu Sieťových akadémií Cisco, ktoré sa konalo na Polytechnickej univerzite v Bukurešti, obsadili prvé, piate a ôsme miesto. Slovensko sa tak stalo najúspešnejšou spomedzi 29 krajín strednej a východnej Európy.

Do súťaže iCompetition 2009 sa zapojilo viac ako 200 pedagógov stredných a vysokých škôl, ktorí museli prejsť sitom troch kvalifikačných kôl prostredníctvom internetového portálu. **Do bukureštského finále sa prebojovalo desať najlepších** z nich. Okrem troch slovenských to boli po dvaja pedagógovia z Ukrajiny a Rumunska a po jednom z Česka, Bulharska a Turecka. Slovensko tak malo najúspešnejšie zastúpenie v počte finalistov.

Finále sa skončilo veľkým úspechom inštruktorov zo Slovenska. Víťazom súťaže sa stal Peter Palúch zo Žilinskej univerzity s celkovým skóre 94,65 bodu zo 100 možných. Peter Feciľak z Technickej univerzity v Košiciach sa umiestnil na 5. mieste a Tomáš Kanocz z rovnakej školy skončil na 8. mieste. „Súťaž iCompetition 2009 ukázala, že úspechy, ktoré dosahujú študenti programu Sieťových akadémií zo Slovenska v medzinárodných súťažiach, nie sú náhodné. Aj ich učitelia patria k medzinárodnej špičke,“ povedal koordinátor programu NetAcad František Jakab.

Online Round Winners			
#	**Name**	**Country**	**Total Score**
1	**Peter Paluch**	**Slovakia**	**94.65**
2	Romeo Lungu	Romania	90.56
3	Alexandr Oleynikov	Ukraine	87.16
4	Dmytro Andrushko	Ukraine	83.26
5	**Peter Fecilak**	**Slovakia**	**83.09**
6	Tomas Fidler	Czech Republic	79.19
7	Delian Genkov	Bulgaria	66.29
8	**Tomas Kanócz**	**Slovakia**	**61.67**
9	Anil Ergunsah	Turkey	54.62
10	Alexandru Ana	Romania	33.89

Záujemcovia mohli priebeh dvojdňovej súťaže sledovať prostredníctvom video IP streamingu, ktorého vysielanie zabezpečoval tím z Technickej univerzity v Košiciach.

„Súťaž bola zo strany organizátora skvele pripravená,” komentuje Peter Palúch. „Body bolo možné získavať v teoretických testoch, pri riešení praktických úloh a v príprave krátkej prezentácie na náhodne pridelenú tému. Bol som úprimne veľmi prekvapený, ako naši rumunskí kolegovia dokázali v hraniciach učiva CCNA semestrov postaviť neobvykle náročné a originálne súťažné zadania. Rozsiahle faktografické znalosti pri riešení zadaní boli dôležité, ale ešte dôležitejšia bola schopnosť kreatívne a najmä úplne netradične ich kombinovať a používať,” pokračuje. „Veľmi sa teším z toho, aký skvelý úspech mala naša slovenská 'expedícia' do Rumunska. Celý čas sme sa vynikajúco bavili a naše vydarené umiestnenia vo výslednom rebríčku sú odrazom toho, že na Slovensku má program Cisco Sieťových akadémií mimoriadne vysokú úroveň, a to aj v európskom meradle.

Ja osobne si však na súťaži iCompetition najviac vážim práve príležitosť stretnúť sa s novými ľuďmi na rovnakej vlnovej dĺžke a nadviazať nové priateľstvá. Veď o tom nakoniec všetky siete sú – o komunikácii a o kontakte.” uzatvára Peter Palúch.

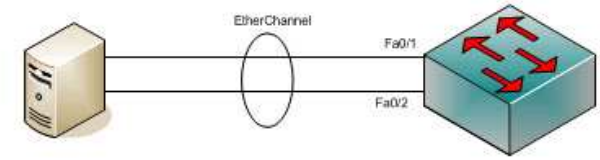
František Jakab
koordinátor programu
Sieťových akadémií v SR

Partneri NetAcad

T-Systems Slovakia: EtherChannel

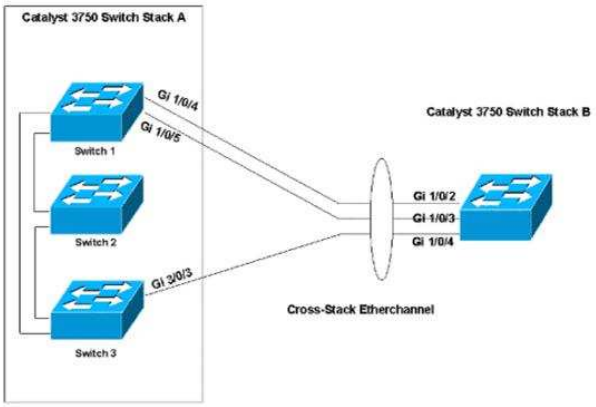
V minulých číslach sme vám predstavili tím NW&FW spoločnosti T-Systems Slovakia. Oboznámili sme vás s Load-Balancing technológiou, s ktorou tento tím pracuje. ***Dnes budeme pokračovať technológiou EtherChannel.***

Obr. 1.



Technológia **EtherChannel umožňuje spojiť viacero fyzických ethernetových liniek do jednej logickej**, čím je možné **efektívne znásobiť priepustnosť dát medzi prepínačmi, smerovačmi alebo servermi** až na 80Gb/s pri použití ôsmich 10Gb/s portov na každej strane. To okrem obrovskej rýchlosti zaručuje aj redundanciu v prípade zlyhania. Vďaka týmto výhodám je vhodné použiť EtherChannel na BACKBONE sieťach, ale možné to je na iných miestach v sieti. V minulosti platilo obmedzenie, že všetky použité porty museli byť na jednom zariadení, no Cisco Virtual Switching System tento problém odstraňuje. Je preto možné vytvárať Multichassis EtherChannel (MEC) a entity "virtuálnych prepínačov". Z toho vyplýva, že keď sa EtherChannel nakonfiguruje, všetky linky, ktoré sú jeho častou, zdieľajú tie isté MAC a IP adresy. To ho urobí z hľadiska aplikácií a užívateľov jednou logickou linkou a jej časti sú neviditeľné.

Obr. 2.



Táto technológia bola predstavená spoločnosťou Kalpana na začiatku 90-tych rokov minulého storočia a v roku 1994 ich odkúpila firma Cisco Systems. Popri tom vydal IEEE otvorený štandard EtherChannelu 802.3ad, ktorý je možné použiť na UTP aj na optických spojeniach.

Spoločnosť T-Systems Slovakia využíva túto technológiu v plnej miere pri prepojení dátových centier, kde sú potrebné veľké prenosové kapacity a spoľahlivosť pripojenia.

Tím NW&FW zodpovedá za správnu implementáciu požiadaviek zákazníkov, ako aj promptnú reakciu na potenciálne vzniknuté problémy. EtherChannel je však len jednou z mnohých technológií, s ktorými sa denne tím stretáva. V nasledujúcom čísle budeme pokračovať predstavením ďalšieho riešenia.

Martin Hanc
NW&FW Tím
T-Systems Slovakia s.r.o.

SPONZORSKÁ PODPORA na nákup zariadení potrebných pre výučbu NetAcad !!!

TERMÍN ZASIELANIA ŽIADOSTÍ O SPONZORSKÚ PODPORU JE 15. jún 2009

Vážená NetAcad komunita,

dovoľujem si Vám oznámiť, že aj v tomto roku sa nám vďaka dobrým výsledkom programu Sieťových akadémií v SR podarilo získať finančné prostriedky na podporu škôl zapojených do programu (podpora z MŠ SR a sponzorov programu).

Prostriedky sú účelovo určené na nákup zariadení potrebných pre výučbu programu NetAcad. O podporu sa môžu uchádzať všetky školy zapojené do programu prostredníctvom zaslania žiadosti na adresu:

František Jakab,
koordinátor programu NetAcad pre SR
Cisco Slovakia, spol. s.r.o.
Apollo Busines Center
Mlynske nivy 43
82109 Bratislava 2.

Žiadosť o finančnú podporu prosím zasielajte aj elektronicky na adresy szalay@elfa.sk a fjakab@cisco.com.

Zvlášť upozorňujeme, aby túto príležitosť využili predovšetkým nové školy a školy, ktoré potrebujú zabezpečiť inováciu skôr zakúpených výučbových zostáv.

Podmienky:

a. Škola má platnú podpísanú zmluvu o zriadení LCNA/RCNA
b. **Škola sa môže uchádzať o podporu až do výšky cca 70% z celkovej hodnoty kupovaných zariadení.**

Aktuálna cenová kalkulácia pre jednotlivé varianty LabKitov Vám bola poslaná mailom. K cene v prílohe je potrebné pripočítať DPH (19%) a je potrebné rátať aj s cca + 10% na dopravu a servisnú podporu.

V termíne do 25.6.2009 bude škola informovaná, či jej žiadosť bola podporená.

Prosím kontaktujte ma, ak potrebujete ďalšie informácie.

S pozdravom,

František Jakab
Koordinátor NetAcad pre SR
Cisco Slovakia
0905 715 816

LETNÁ ŠKOLA NetAcad 2009

Pozývame vás na program Letnej školy 2009, ktorá bude prebiehať v mesiacoch júl a august.

Cieľom Letnej školy programu Sieťových akadémií je zvyšovanie kvality prípravy inštruktorov (pedagógov stredných a vysokých škôl) ako aj študentov programu.

Ide o sériu veľmi intenzívnych, navzájom na seba nezávislých kurzov. Zámerom aktivity je umožniť akadémiám zapojeným v programe Sieťových akadémií vyškoliť si v čo najkratšom čase čo najviac inštruktorov a súčasne umožniť študentom intenzívnou formou získať nové vedomosti.

Tento rok bude Letná škola organizovaná na viacerých miestach a to na pôde:

- **Žilinskej univerzity**
- **SOŠ v Handlovej**
- **a Technickej univerzite v Košiciach**

(pre študentov stredných a vysokých škôl), pričom podujatie v Handlovej je určené študentom stredných škôl.

Ďalšie informácie o Letnej škole sú zverejnené na známej stránke www.netacad.sk

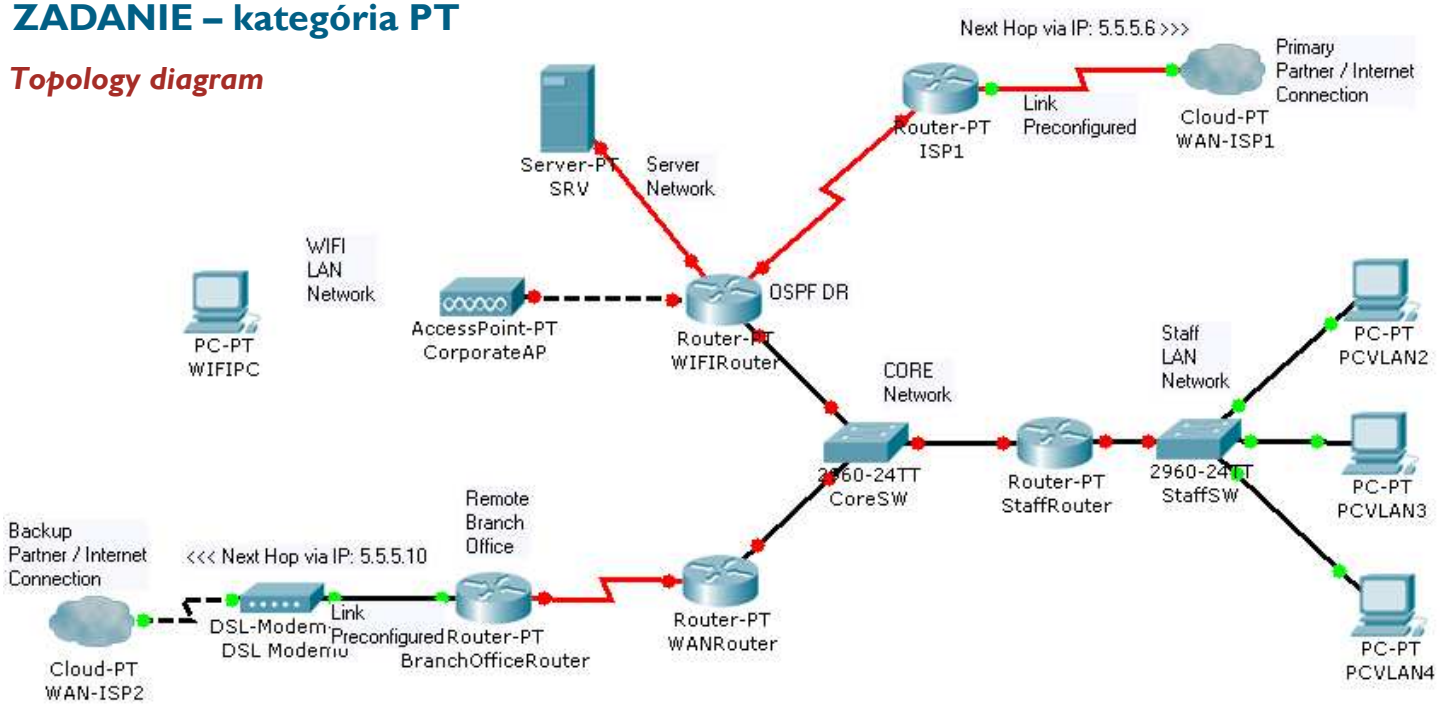
V prípade akýchkoľvek otázok kontaktujte administrátora Letnej školy: szalay@elfa.sk

Redakčná rada

Národné kolo súťaže študentov programu NetAcad Networking Academy Games (NAG 2009)

ZADANIE – kategória PT

Topology diagram



Instructions

You have **60 minutes** to configure all requirements.

Double-click on the "PT-NAG-2009.pkt" icon located on your desktop and wait until this file is open in Packet Tracer 5.1.

Follow the scenario to complete the configuration tasks. **During the configuration periodically save your file to prevent data loss in case of Packet Tracer crash**.

Do not make any changes to the logical topology. When configuring hostnames, passwords etc. follow the capitalization of letters exactly as it is in the assignment. If you have any questions, please, do not hesitate to ask. Try not to leave any task unconfigured. If you have only some parts of the task correct, you will receive partial credit.

After the task completion save the PT file under your surname on the desktop.

Scenario

The ICMP Inc. Company is building its new data network. The topology of the network is shown on the diagram above. A primary Internet and Partner company connection is through the ISP1 router. The ISP1 router redistributes the default route through a dynamic routing protocol. When the Internet and the Partner company connection through the ISP1 is broken, static backup routes will route packets through a BranchOfficeRouter and a DSL modem connection located in the Remote Branch Office network. Routers ISP1 and BranchOfficeRouter and the StaffSW switch are partially preconfigured. Your task is to enable reliable connection between the network segments, Internet and the Partner Connection .

Assignment – subnetting

Use the **VLSM** method to divide the address space of the 192.168.1.0/24 network to cover the needs of the topology shown on the diagram. Choose always the subnet mask with the fewest number of host bits required.

The WAN serial connection between routers WIFIRouter and ISP1 should use the 1st subnet.

1st subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

The WAN serial connection between routers WANRouter and BranchOfficeRouter should use the 2st subnet.

2nd subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

The 3rd subnet is to be used for the CORE Network.
3 routers will be used in this network.

3rd subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

The 4th subnet is to be used for the LAN WIFI Network.
10 computers will be used in this network.

4th subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

The 5th subnet is to be used for the LAN VLAN2 of the STAFF Network.
4 computers will be used in this network.

5th subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

Pokračovanie na str. 5

ZADANIE – kategória PT

Pokračovanie zo str. 4

The 6th subnet is to be used for the LAN VLAN3 of the STAFF Network. 5 computers will be used in this network.

6th subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

The 7th subnet is to be used for the LAN VLAN4 of the STAFF Network. 5 computers will be used in this network.

7th subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

The 8th subnet is to be used for the LAN VLAN5 of the STAFF Network. Use the same size of this subnet as the size of the 7th subnet.

8th subnet address: ___ . ___ . ___ . ___ Netmask: ___ . ___ . ___ . ___

NOTE: IP Subnet Zero is a valid subnet. Use it as the 1st subnet.

Assignment – configuration

Basic router configuration

Set the hostname of each router. The hostname has to be the same name as the Display Name of the device in Packet Tracer.

Each router has to require strong secured password "strawberry" to access the privileged executive mode. Password for console access has to be the same as the password for the privileged executive mode and it has to be secured by a weak encryption scheme.

Users connecting to the CLI of routers should be warned with the following message of the day text:

"Unauthorized access prohibited!"

On each router, disable following services:

- CDP (globally)
- DNS lookups (globally)

A Fast Ethernet interface of the router StaffRouter is connected to a trunk port on a switch StaffSW. On the StaffRouter create and configure subinterfaces with the same subinterface numbers as the VLAN numbers for VLAN2, VLAN3, VLAN4 and VLAN5 vlans of StaffSW.

Configure IP addresses on Fast Ethernet interfaces and subinterfaces of routers:

- The second usable IP addresses of the LAN subnets are to be used on Fast Ethernet interfaces and subinterfaces of routers connected to STAFF and WIFI networks.
- For the FastEthernet interface of the WIFIRouter connected to the server SVR use the IP address 10.0.0.1 with a default netmask.
- For the Fast Ethernet interface of the WIFIRouter connected to the CORE Network use the first usable IP address of the CORE Network subnet.
- For the Fast Ethernet interface of the StaffRouter connected to the CORE Network use the second usable IP address of the CORE Network subnet.
- For the Fast Ethernet interface of the WANRouter connected to the CORE Network use the third usable IP address of the CORE Network subnet.

The first usable IP addresses of the WAN subnets are to be used on the DCE side of the serial connection.

The second usable IP addresses of the WAN subnets are to be used on the DTE side of the serial connection.

Cisco | Networking Academy®
Mind Wide Open™

Switch configuration

Configure VLAN 2, 3, 4 and 5 on switch StaffSW.

Configure a management network interface on the StaffSW.

For this purpose use the VLAN5 and the last usable IP address of VLAN5 subnet.

Configure a default gateway on the StaffSW so the switch will be available from remote networks.

On StaffSW, associate port F0/1 to VLAN 2, port F0/2 to VLAN 3 and port F0/3 to VLAN 4.

On StaffSW, make sure that the access ports used by PCs are able to transfer network traffic as soon as the PCs are connected to them.

On SwaffSW, configure port F0/24 into a mode, when all defined VLANs will be available on this port.

LAN connectivity

Configure each computer in the LAN Network to use a DHCP service to receive its IP configuration. Configure the corresponding DHCP services on the StaffRouter router.

Configure a SRV server with a static IP address: 10.0.0.2 with a default classfull netmask. Configure a default gateway on the SRV server.

Make sure that a computer WIFIPC will be associated and connected to a WIFI network provided by the CorporateAP access point.

WAN connectivity

On appropriate interfaces in the topology, configure the physical speed of serial links to be 250kbps.

Make sure that dynamic routing protocols (for future use) will use a proper transmission speed of serial interfaces in their calculations.

Routing

Configure a single area OSPF dynamic routing protocol on each router. As the OSPF process number use the number 1. As the OSPF area number use the number 0.

The number of "network" configuration commands should be as many as the number of active interfaces configured on a router.

Routers StaffRouter and WANRouter should never became OSPF Designated Routers on the CORE Network.

On the ISP1 router, configure redistribution of information about default route in the OSPF protocol.

A primary default route via ISP1 is redistributed in OSPF from the ISP1 router. Configure on each router *except the ISP1 router* one backup static default route that will route traffic through a modem connection to ISP2. These backup routes should be used in the routing table only, when the default route from the OSPF is not available anymore. For static routes use the next hop's IP address instead of the outgoing interface.

Security

The first VTY interface of the WIFIRouter should be accessible only from the 5.5.5.255 IP address. For this purpose create and assign a named access list called REMOTECLI.

Permit only telnet connections going to the Internet through the WANRouter, from networks in VLAN3 a VLAN4 in the LAN Network. All other communication going to the Internet through the WANRouter should be blocked. The ACL's name must be INET_TELNET. Computers in VLAN2 should be able to access the WANRouter.

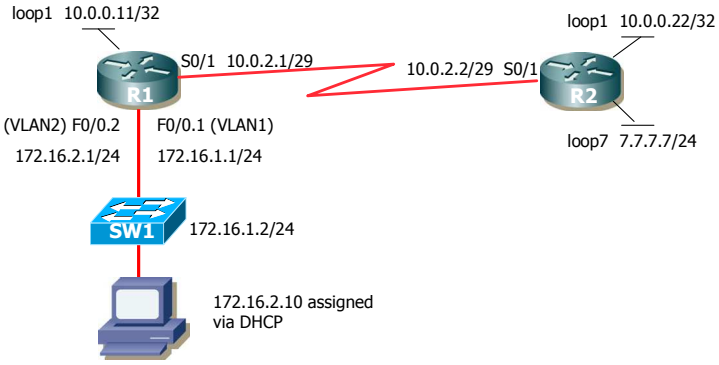
Verification

Copy the "pt3000-i6q4l2-mz.121-22.EA4.bin" file from the server SRV to the flash device of the "WIFIRouter" device.

Národné kolo súťaže študentov programu NetAcad Networking Academy Games (NAG 2009)

ZADANIE – kategória UNI

Topology diagram

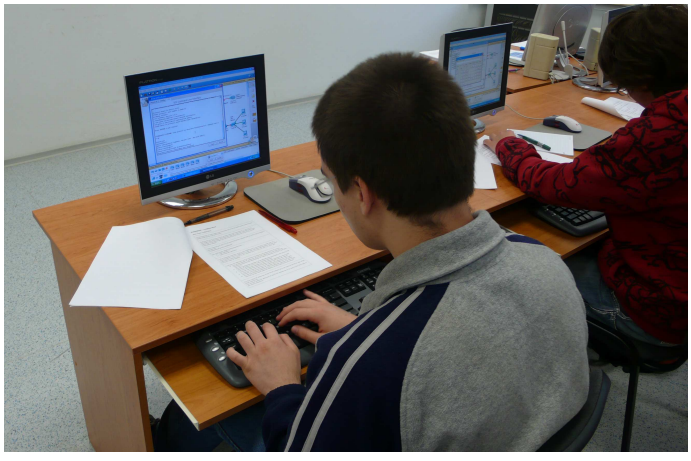


Instructions

You have 30 minutes to prepare and 60 minutes to configure all requirements. During preparation time, read tasks carefully and make notes. The topology is physically connected. If you have any questions or you think you may have physical layer problems, do not hesitate to ask. Try not to leave any tasks unconfigured. If you have at least some parts of the task correct, you will receive partial credit.

Basic router configuration

Each router is to be named and have enable secret: Cisco
Configure WAN link between R1 and R2 routers. Enable PPP protocol and set up 256kbps speed to link.
Make sure that dynamic routing protocols (for future use) will use a proper transmission speed of serial interfaces in their calculations of metric.
Set IP addresses to loopback interfaces and WAN link according to the diagram to both routers. Verify connectivity on WAN link by ping.
Each router should allow telnet access on all VTY lines. Configure VTY line password as cisco01. On VTY lines enable synchronization of CLI (prevent of rewriting of commands in CLI by router's messages).
Users connecting to the CLI of both routers should be warned with the following text: "Unauthorized access prohibited!"
On each router disable following services: • CDP (globally) • DNS lookups (globally)



Routing

Enable OSPF on both routers. Enable routing for 10.0.0.0/8 and 172.16.1.0/24 networks. Use area ID 0 and OSPF process number 1. Verify correct routing by ping to loopback 1 IP address of the opposite router.
On router R2 configure static route toward R1 for subnet 10.0.51.0/24.
On router R1 configure static route toward R2 for subnet 7.7.7.0/24. Verify correct routing by ping IP address 7.7.7.7 from router R1.

LAN

Configure VLAN 2 on switch SW1, set up port F0/1 (PC connected) to access mode and associate it to VLAN 2
Enable trunk on port F0/24 on switch SW1 without negotiation.
On router R1 configure subinterfaces F0/0.1 and F0/0.2. Associate appropriate VLANs and IP address to subinterfaces according to the diagram.
Configure IP address on switch SW1 and default gateway. Verify connectivity from switch by ping to IP address 10.0.0.22.

End host (PC) connectivity configuration

Configure DHCP server on R1 for host connected to SW1 F0/1 interface. R1 should always assign following parameters to the host: • IP address: 172.16.2.10 • Default gateway: 172.16.2.1 • DNS server: 7.7.7.7 • Domain name: olymp.sk • Lease time: 2 hours 35 minutes Do not use static DHCP configuration (do not bind MAC address to IP address in your configuration). Configure this task with the minimum commands necessary.
172.16.2.0/24 network should not be listed in routing table of R2. When R2 receives any packet from network 172.16.2.10/24, it must be seen with source IP address of network 10.0.51.0/24.

Security

Host connected to R1 may ping only to loopback7 on router R2 and telnet only to loopback 1 on router R1. Other communication for this host must be denied. Apply this ACL: • inbound to F0/0 interface of R2 • using name OLYMP Configure this ACL with minimum number of lines necessary. All other communication must be unrestricted.
Passwords must not be saved into configuration file as clear text.
Configure Syslog logging on R1. Syslog server runs on host 172.16.2.10.

Notice: Be sure to save your configuration to the NVRAM frequently. For evaluation purposes, the running-config from each device will be downloaded and evaluated; however, if the running-config will not be accessible for whatever reason, the startup-config will be taken instead and evaluated by the jury.

Cisco Slovakia

Naučte svoju sieť základom sebaobrany

Počet odhalených zraniteľných miest v informačno-komunikačných technológiách medziročne vzrástol o 11,5 percenta. Kriminálne prostredie neustále objavuje nové spôsoby zneužívania ľudí, sietí aj internetu.

Podľa bezpečnostnej správy Cisco Annual Security Report počet útokov z legitímnych domén sa temer zdvojnásobil, sú čoraz viac cielené, kombinované a viacsmerové. Množstvo škodlivého softvéru šíreného cez prílohy elektronickej pošty sa síce počas posledných dvoch rokov znížil o polovicu, na druhej strane však až trojnásobne stúpol počet zraniteľných miest v oblasti virtualizačných technológií. Kým v minulosti bývali útoky na informačné systémy zväčša prípadmi kybervandalizmu a slúžili na zviditeľnenie sa hackerov, súčasné útoky sú dielom cieľavedomého "biznisu", často riadeného organizovaným zločinom.

Všadeprítomná hrozba

Súčasné bezpečnostné hrozby sú rozšírenejšie a nebezpečnejšie ako v minulosti. Nesústreďujú sa už len na jednotlivé PC, ale na celé podnikové a regionálne siete a dokonca aj na globálnu infraštruktúru. Známy vírus Slammer sa dokázal rozšíriť po celom svete za 11 minút a v čase svojho najväčšieho rozšírenia infikoval každú sekundu 55 miliónov nových počítačov.

Situácia sa oproti časom, keď sa vírusy šírili takmer výlučne cez diskety, podstatne zmenila. Všadeprítomný prístup k webovým aplikáciám na jednej strane umožňuje používateľom pracovať odkiaľkoľvek a kedykoľvek, čo je síce fajn, ale na druhej strane sú i siete vystavené hrozbám odkiaľkoľvek a kedykoľvek. Tradičné sieťové bariéry, ktoré oddeľujú dôveryhodné časti infraštruktúry od tých ostatných, postupne miznú. Tým, že sa aplikácie sprístupňujú aj vzdialeným počítačom a systémom, sa sieťový perimeter stáva menej konkrétny a zložitejší na ochranu.

Bezpečnostné hrozby sa týkajú veľkých i malých. Zatiaľ čo prvá skupina organizácií využíva špecializované bezpečnostné tímy, malé a stredné podniky si takýto "luxus" spravidla nemôžu dovoliť. Sofistikovanejším druhom škodlivých kódov však musia čeliť všetci, bez ohľadu na to, či sú malí alebo veľkí. Organizácie môžu riziko strát svojich dát znížiť vyladením prístupu a aplikovaním záplat na známe zraniteľné miesta. Mali by však urobiť viac.

Sebaobranná sieť

Pre menšie organizácie je dôležité, aby mali bezpečnú a adaptabilnú sieť, ktorá si nevyžaduje podporu vlastných bezpečnostných špecialistov. Jednou z možností, ako zabezpečiť firemnú infraštruktúru bez špecializovaného útvaru, je koncept sebaobrannej siete. Takáto sieť, ktorá dokáže sama seba chrániť, má v sebe integrované tri základné vrstvy - bezpečnosť aplikácií, ochranu pred škodlivými kódmi, ako aj komplexnú kontrolu siete. Vďaka tomu je schopná predpokladať hrozby, prispôsobovať sa im a reagovať na ne skôr, ako sa vyskytnú, resp. hneď ako začnú pôsobiť.

Stratégiu sebaobrannej siete Cisco pôvodne budovalo na sieťovom základe, čiže na integrácii technológií pre firewally, virtuálne privátne siete a proaktívne zabezpečovacie systémy pred napadnutím. Nové bezpečnostné hrozby viedli k zdokonaleniu tohto konceptu. V súčasnosti je architektúra sebaobrannej siete postavená na ochranných mechanizmoch nielen pre siete, ale i pre koncové zariadenia vrátane aplikačnej bezpečnosti, zabezpečenia obsahu, správy identít, vynucovania bezpečnostných politík a monitorovania bezpečnosti. Ak napríklad Cisco Security Agent zachytí podozrivú aktivitu na PC, informuje o tom Cisco Security Monitoring, Analysis and Response System. Ten následne začne spolupracovať s riešením Cisco IPS na podrobnej analýze sieťovej prevádzky generovanej týmto počítačom a potlačení potenciálneho útoku. Cisco Security Manager umožňuje definovať presné firemné bezpečnostné politiky prostredníctvom centralizovaného rozhrania.

Za sieťovým perimetrom

Základnými stavebnými kameňmi sebaobrannej siete je modulárny bezpečnostný systém ASA 5500 Series, Cisco Integrated Services Routers a Cisco Catalyst 6500 Series, ktoré vnášajú do sieťovej infraštruktúry robustný súbor bezpečnostných služieb. ASA 5500 Series je výkonný modulárny systém, ktorý poskytuje funkcie aplikačného firewallu a zabezpečené prenosy cez virtuálne privátne siete.

Nové spôsoby komunikácie a spolupráce, ako sú webové aplikácie alebo instant messaging, na jednej strane zjednodušujú prácu, ale súčasne sú aj lákavým cieľom pre hackerov. Ďalším rizikom je narastajúce množstvo nevyžiadanej pošty. Do tejto kategórie možno zaradiť takmer 200 miliárd e-mailov denne, čiže okolo 90 percent celosvetovej elektronickej pošty. Preto je nevyhnutné starať sa o bezpečnostnú ochranu aj za sieťovým perimetrom. Cisco vyvinulo rad prvotriednych technológií, ktoré to umožňujú. Patria medzi ne spomínaný systém ASA 5500 Series pre ochranu obsahu, Cisco IOS pre filtrovanie obsahu a bezpečnosť hlasovej komunikácie a najnovšie aj popredné webové a e-mailové bezpečnostné riešenia od spoločnosti IronPort, ktorá patrí pod spoločnosť Cisco .

Skôr identifikovať hrozby

Bezpečnostný systém Cisco ASA 5500 Series využíva i distribučná farmaceutická spoločnosť Unipharma, dvojka na slovenskom trhu s liečivami. Pomocou distribučných áut zabezpečuje permanentné zásobovanie lekární, nemocníc a zdravotníckych zariadení po celom Slovensku. Unipharma zamestnáva približne 500 pracovníkov.

"Na komunikáciu s klientmi aj medzi sebou navzájom využívame prakticky všetky dostupné komunikačné kanály, od telefonovania až po elektronické obchodovanie," tvrdí IT manažér spoločnosti Roman Karak. Pri predaji liekov sa uplatňujú prísne legislatívne pravidlá, ktoré musia dodržiavať všetci účastníci biznisu. Je to jednak správna distribučná prax, ale aj určité zákonné obmedzenia. Pri elektronickom obchodovaní lekárnik na základe svojich skladových zásob zašle objednávku na lieky, ktoré potrebuje dodať. Po posúdení predpísaných pravidiel, ako je povolenie obchodovať s liekmi ako takými, doplnkovými zdravotníckymi materiálmi, omamnými či psychotropnými látkami, Unipharma objednávku zrealizuje.

"V duchu legislatívnych noriem sme povinní zabezpečiť zdravotnú starostlivosť, čo v našom prípade znamená, že musíme dodať objednaný liek v určitom predpísanom čase. Z tohto hľadiska je pre firmu funkčnosť informačného systému a sieťovej infraštruktúry životne dôležitá, nehovoriac o samotnom komerčnom rozmere dostupnosti týchto systémov. Výpadok čo i len na niekoľko minút by pre Unipharmu znamenal pomerne vysoký negatívny dopad, hlavne vo vzťahu so zákazníkom.

Po implementácii Cisco ASA 5500 Series spoločnosť dokáže skôr identifikovať a prispôsobiť sa potenciálnym bezpečnostným hrozbám, ako aj negatívnym dopadom, ktoré by mohli mať na distribúciu liečiv. Pokiaľ ide o oblasť bezpečnosti a dostupnosti služieb, ďalšie investície Unipharma plánuje zamerať najmä do skvalitnenia informačných technológií a komunikačnej infraštruktúry, aby dosiahla minimálne 99-percentnú úroveň prevádzky bez výpadkov.

Cisco

Cisco ASA 5500

Produktový rad Cisco ASA 5500 (Adaptive Security Appliance) zahŕňa portfólio špičkových vysokovýkonných multifunkčných bezpečnostných zariadení, ktorý získal mnohé ocenenia. Implementuje konvergentné riešenia ako sú firewall, či riešenie pre vytváranie virtuálnych privátnych sietí (VPN), čím chráni vašu sieť pred vonkajšími útokmi a inými bezpečnostnými rizikami.

Cisco ASA 5505 je výkonný, modulárny bezpečnostný produkt so širokým využitím. Poskytuje funkcie aplikačného firewallu a zabezpečené VPN prenosy. Produkty Cisco ASA 5500 umožňujú štandardizovať bezpečnostné funkcie na jednej platforme pod jednotnou správou, čím je možné zjednodušiť správu siete a dosiahnuť nižšie prevádzkové náklady resp. nižšie náklady na náhradné komponenty.

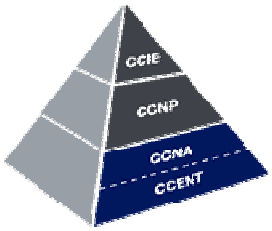
Kľúčové vlastnosti Cisco ASA 5505:

- *Kombinuje firewall a VPN*
- *Chráni sieť pred útokmi z vonkajšieho prostredia, ochrana pred DoS útokmi*
- *Zabezpečuje aplikácie a blokuje nevhodnú komunikáciu.*
- *VPN služby a VPN termináciu pre prepájanie sietí*
- *IPSec SSL VPN služby pre bezpečný vzdialený prístup mobilných užívateľov*
- *Hĺbková plnostavová inšpekcia a ochrana desiatok protokolov*
- *Centralizovaná správa pri nasadení viacerých systémov*
- *Podpora translácie adries NAT*

Cisco

FREE CCENT Certification Training

Dear Colleague



Are you CCENT certified? Do you know the CCENT certification exam? Can you truly prepare your students for an exam unless you take it yourself?

Cisco Networking Academy would like to invite CCNA Discovery & Exploration instructors to attend a FREE exam certification training webinars starting in June 2009.

The webinars will be hosted by the Technical Advocacy team live on WebEx. You will receive full training that will prepare you to pass your CCENT certification exam. And the exam fee waiver programme currently open to all Networking Academy instructors means that you can take your certification exam totally FREE of charge.

There has never been a better opportunity for you to become certified.

- *Up to 6 FREE EXAM VOUCHERS per instructor*
- *FREE training with your Networking Academy Technical Advocacy Managers*
- *A full training schedule kicking off in June*
- *In the very unlikely event that you do not pass your exam first time, you can attend more training and try again*

There will be four sessions covering all you need to know in order to become CCENT certified. It is recommended that you attend all fours sessions to gain full benefit of this training.

The schedule kicks off on June 9th, followed by sessions on the 11th, 16th, and 17th in English.

To register for these sessions please follow these instructions:

Topic: CCENT Instructor Training - Session 1 (English)
Host: Jaskaran Kalsi
Date: Tuesday 9th June, 2009
Time: 13:00 GMT Daylight Time (GMT +01:00, London)
Event Number: 202 718 118
To register for this training session:
- Go to https://cisco.webex.com/cisco/onstage/g.php?d=202718118&t=a and register.
- Once registered, you will receive a confirmation email with instructions for joining the session.

Topic: CCENT Instructor Training - Session 2 (English)
Host: Jaskaran Kalsi
Date: Thursday 11th June, 2009
Time: 13:00 GMT Daylight Time (GMT +01:00, London)
Event Number: 201 186 557
To register for this training session
- Go to https://cisco.webex.com/cisco/onstage/g.php?d=201186557&t=a and register.
- Once registered, you will receive a confirmation email with instructions for joining the session.

Topic: CCENT Instructor Training - Session 3 (English)
Host: Jaskaran Kalsi
Date: Tuesday 16th June, 2009
Time: 13:00 GMT Daylight Time (GMT +01:00, London)
Event Number: 204 823 012
To register for this training session
- Go to https://cisco.webex.com/cisco/onstage/g.php?d=204823012&t=a and register.
- Once registered, you will receive a confirmation email with instructions for joining the session.

Topic: CCENT Instructor Training - Session 4 (English)
Host: Jaskaran Kalsi
Date: Wednesday 17th June, 2009
Time: 13:00 GMT Daylight Time (GMT +01:00, London)
Event Number: 202 909 812
To register for this training session
- Go to https://cisco.webex.com/cisco/onstage/g.php?d=202909812&t=a and register.
- Once registered, you will receive a confirmation email with instructions for joining the session.

For assistance: You can contact
- **Jaskaran Kalsi at: jkalsi@cisco.com; +44 7825 774337**

We hope you will make the time to attend June's training webinars and take this opportunity to become CCENT qualified.

Best wishes
Cisco Networking Academy team

8. ročník výročnej konferencie programu Sieťových akadémií

Dovoľujeme si Vás pozvať na 8. ročník výročnej konferencie vzdelávacích inštitúcií zapojených do programu Sieťových akadémií v Českej a Slovenskej republike.

- Dátum: 18. - 20. júna 2009
- Miesto konania konferencie: FIT VUT Brno, Božetěchova ulica č. 1., Brno
- Ubytovanie a spoločenský večer: SŠ informatiky a spojů, Čichnova 23, Brno

Samotná konferencia bude prebiehať v priestoroch FIT VUT Brno, kde bude zaistené občerstvenie ako aj obedy. Registrácia účastníkov bude po oba dni otvorená od 8:00 hod pred vstupom do konferenčnej sály.

Ubytovanie vrátane raňajok je rezervované v rámci ubytovania v internátoch SŠ informatiky a spojů (http://www.sosinformatikybrno.cz). V každej izbe sú dve samostatné bunky (dvoj-troj posteľové) a spoločné sociálne zariadenie. Nezabudnite pri registrácii uviesť svojho spolubývajúceho. Ubytovanie si hradí každý účastník sám na mieste a to v hotovosti (cena 450 Kč / osoba / noc vrátane raňajok).

Z miesta ubytovania bude zaistená kyvadlová doprava na miesto konferencie.

Pre účastníkov, ktorí dorazia večer 18. 6. 2009 pred zahájením konferencie, bude organizovaná večera na mieste ubytovania od 18:00 do 19:30 hod. Od 20:00 hod plánujeme pre záujemcov bowlingový turnaj.

Pre účastníkov so Slovenska bude zabezpečený autobus s klasickou trasou KE-PP-ZA-BA-Brno.

Registrujte sa už dnes na http://www.cisco.com/web/offer/emea/3726/index.html registrácia bude otvorená do 31.5.2009! Tešíme sa na Vašu účasť.

Organizačný tím
NetAcad konferencie 2009

VTIPY ☺

Aké mená dá dvojčatám IT-čkár? :D