



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

PIKS, prednáška 11: Dizajn, bezpečnosť a príkazy pre overenie funkčnosti malej siete

Introduction to Networks v7.0 – Chapter 11

Katedra informačných sietí

Fakulta riadenia a informatiky, UNIZA




CISCO

Networking
Academy



Obsah prednášky

- **Kapitola 11**
 - 11.1 Sieťový dizajn
 - 11.2 Sieťová bezpečnosť
 - 11.3 Príkazy pre overenie funkčnosti malej siete



Časť 11.1: Sieťový dizajn

Na konci by sme mali vedieť:

- Identifikovať zariadenia používané v sieťach menšieho rozsahu.
- Identifikovať protokoly používané v takýchto sieťach.
- Vysvetliť, prečo sú tieto siete základom pre siete väčšieho rozsahu.



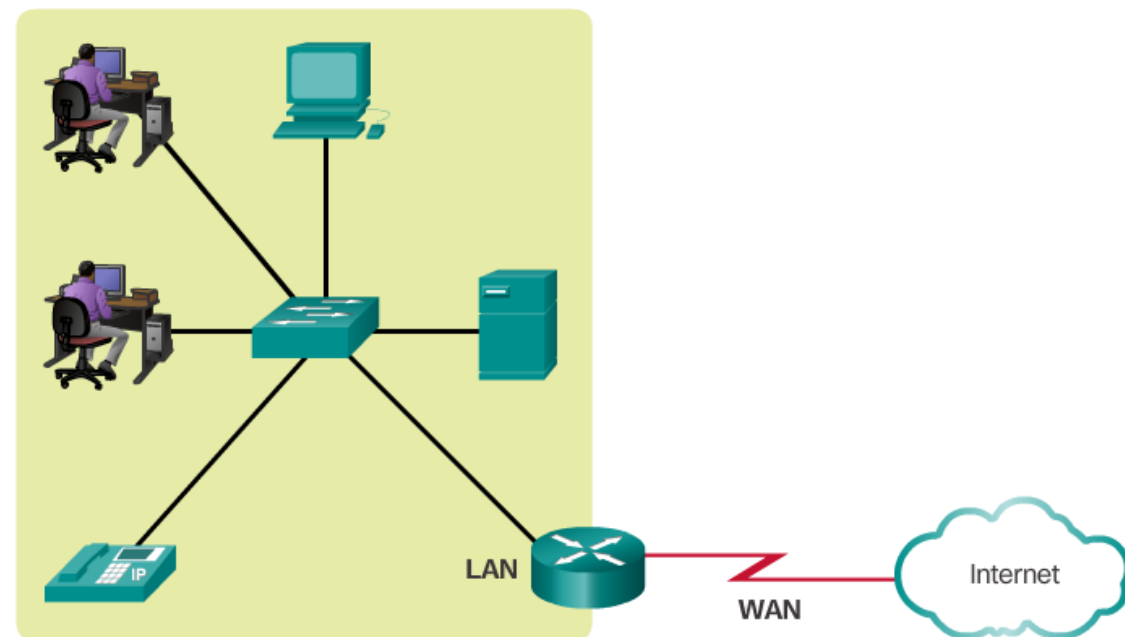
Téma 11.1.1: Zariadenia v sieťach menšieho rozsahu

Menšie sieťové topológie

- Pripojenie do Internetu je cez jednu WAN linku
- WAN môže byť kadečo: DSL, cable, Ethernet (na L1 tiež kadečo...)
- Manažovanie takejto siete zväčša znamená robiť správu a troubleshooting existujúcich zariadení.
 - Niekedy robí zamestnanec firmy na to vyhradený, alebo niekto mimo zazmluvnený

Typicky majú:

- Jednoduchý dizajn
- Menší počet zariadení
 - Zväčša 1 smerovač, niekoľko prepínačov a počítače používateľov



Treba zvážiť:

Výber vhodných zariadení pre malú sieť

Vlastnosti
a funkcie
závislé na OS:

- Bezpečnosť
- QoS
- VoIP
- L3 prepínanie
- NAT
- DHCP



Cost



Ports



Speed



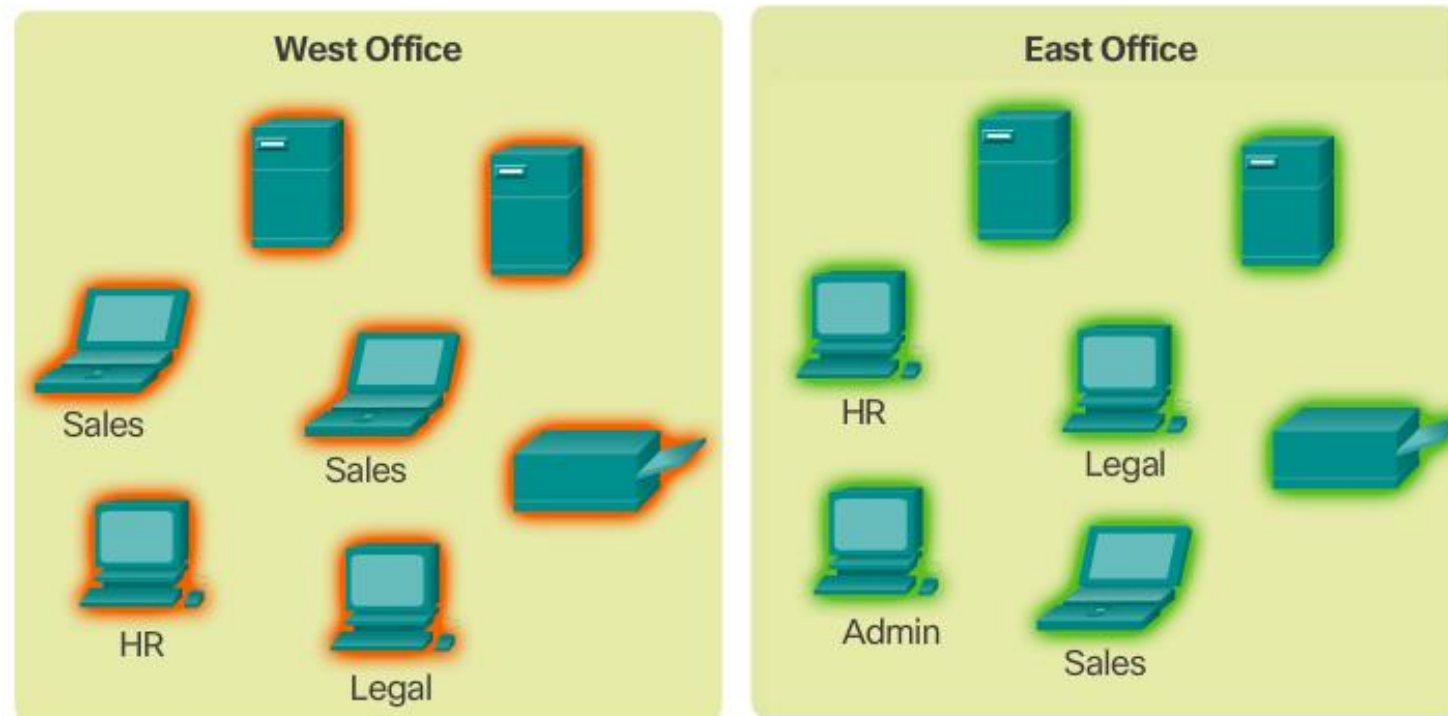
Expandable/Modular



Manageable

IP adresná schéma pre malú sieť

- Je kľúčovým komponentom sieťového dizajnu
- Musí byť naplánovaný, dokumentovaný a udržiavaný
- Dôležité pre troubleshooting a kontrolu prístupu k zdrojom v sieti
- Zvážiť kde dynamické a kde statické adresy.



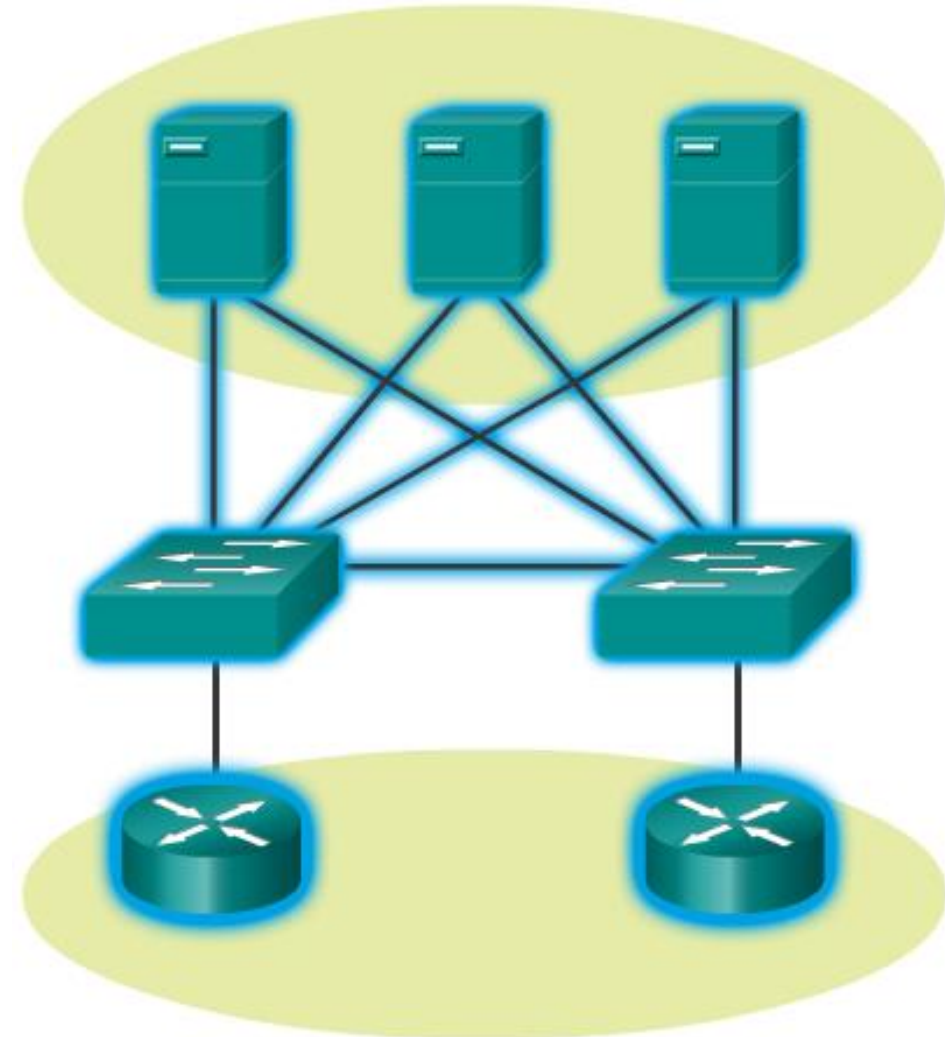
Redundancia v malej sieti

Čo ňou dosiahneme:

- Vyššiu spoľahlivosť – odstránime „single points of failure“
- Menšie náklady – za chyby sa platí, v sieti to platí dvojnásobne

Ako ju dosiahneme:

- Zduplikujeme sieťové zariadenia a/alebo linky
 - Replikácia serverov
 - Viac ciest do internetu

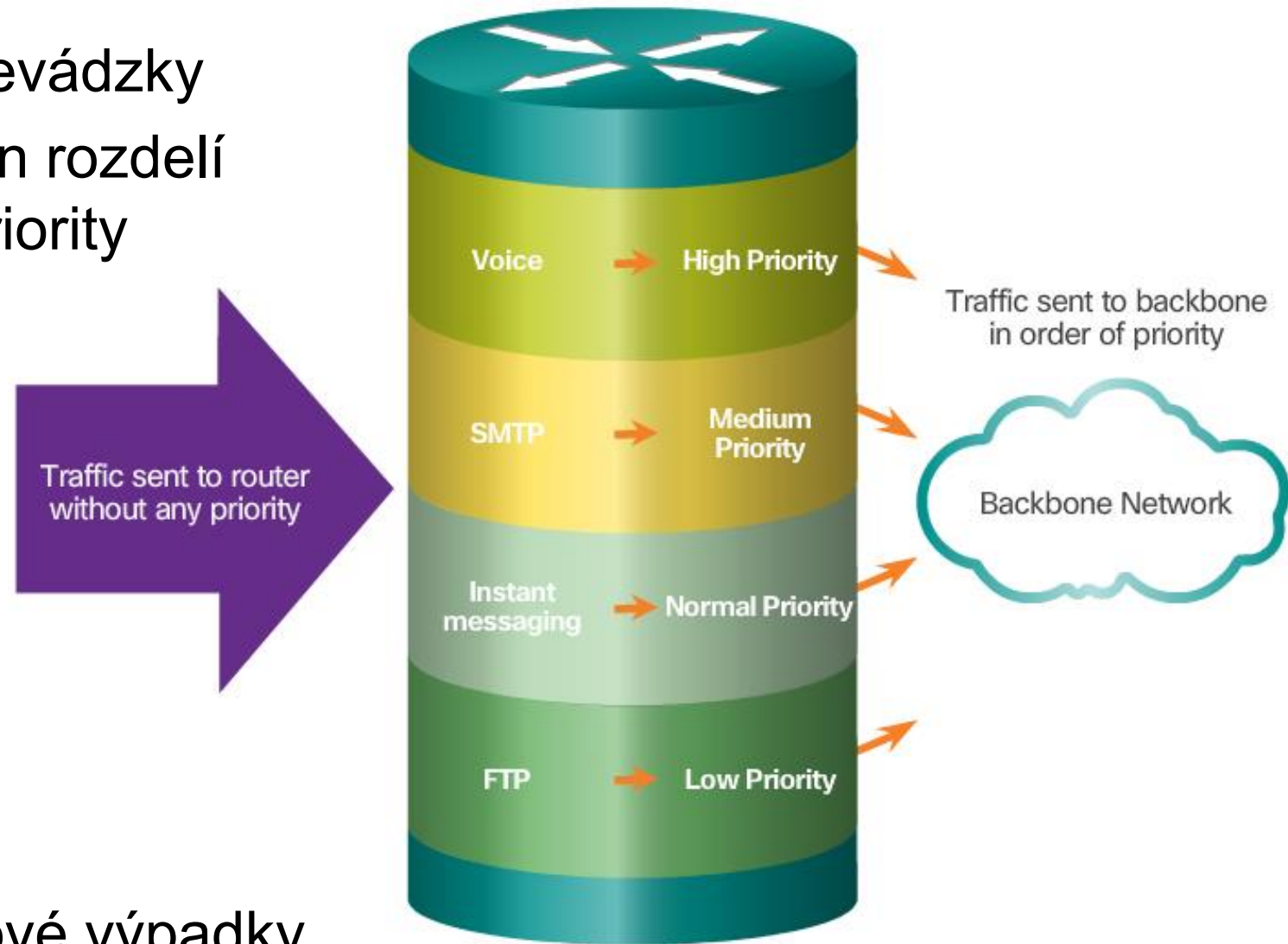


Manažovanie prevádzky (Traffic Management)

- Treba zväžiť typ prevádzky
- Dobrý sieťový dizajn rozdelí prevádzku podľa priority

Cieľom dobrého dizajnu siete je vždy:

- Zvýšiť produktivitu zamestnancov
- Minimalizovať sieťové výpadky





Téma 11.1.2: Malé sieťové aplikácie a protokoly

Známe aplikácie

Užitočnosť siete závisí od užitočnosti softvérových programov alebo procesov, ktoré zabezpečujú prístup do siete:

Sieťové aplikácie

- Pre komunikáciu cez sieť
- Napr. emailový klient, web prehliadač, ..

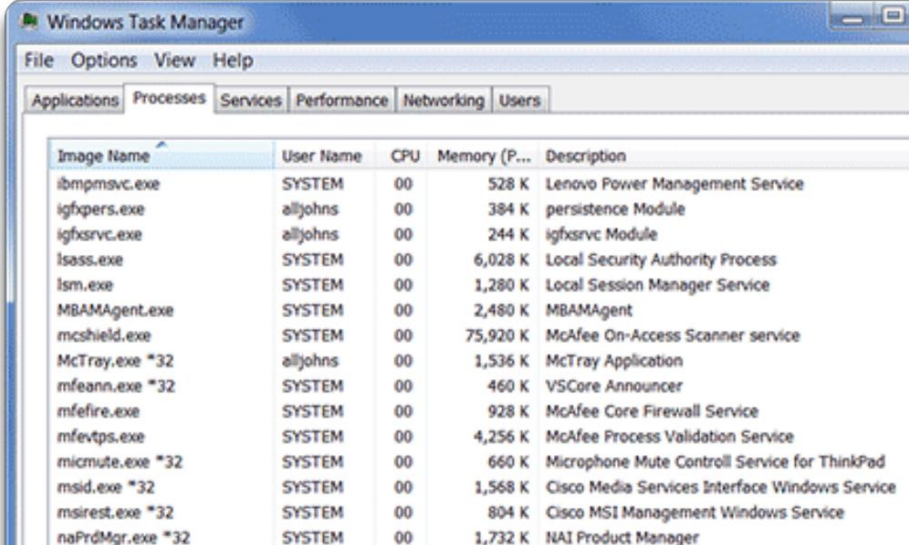


Image Name	User Name	CPU	Memory (P...	Description
ibmpmavc.exe	SYSTEM	00	528 K	Lenovo Power Management Service
igbpcers.exe	alljohns	00	384 K	persistence Module
igbpcsvc.exe	alljohns	00	244 K	igbpcsvc Module
lsass.exe	SYSTEM	00	6,028 K	Local Security Authority Process
lsm.exe	SYSTEM	00	1,280 K	Local Session Manager Service
MBAMAgent.exe	SYSTEM	00	2,480 K	MBAMAgent
mcsshield.exe	SYSTEM	00	75,920 K	McAfee On-Access Scanner service
McTray.exe *32	alljohns	00	1,536 K	McTray Application
mfeann.exe *32	SYSTEM	00	460 K	VSCore Announcer
mfire.exe	SYSTEM	00	928 K	McAfee Core Firewall Service
mfevtps.exe	SYSTEM	00	4,256 K	McAfee Process Validation Service
micmute.exe *32	SYSTEM	00	660 K	Microphone Mute Controll Service for ThinkPad
msid.exe *32	SYSTEM	00	1,568 K	Cisco Media Services Interface Windows Service
msirest.exe *32	SYSTEM	00	804 K	Cisco MSI Management Windows Service
naPrdMgr.exe *32	SYSTEM	00	1,732 K	NAI Product Manager

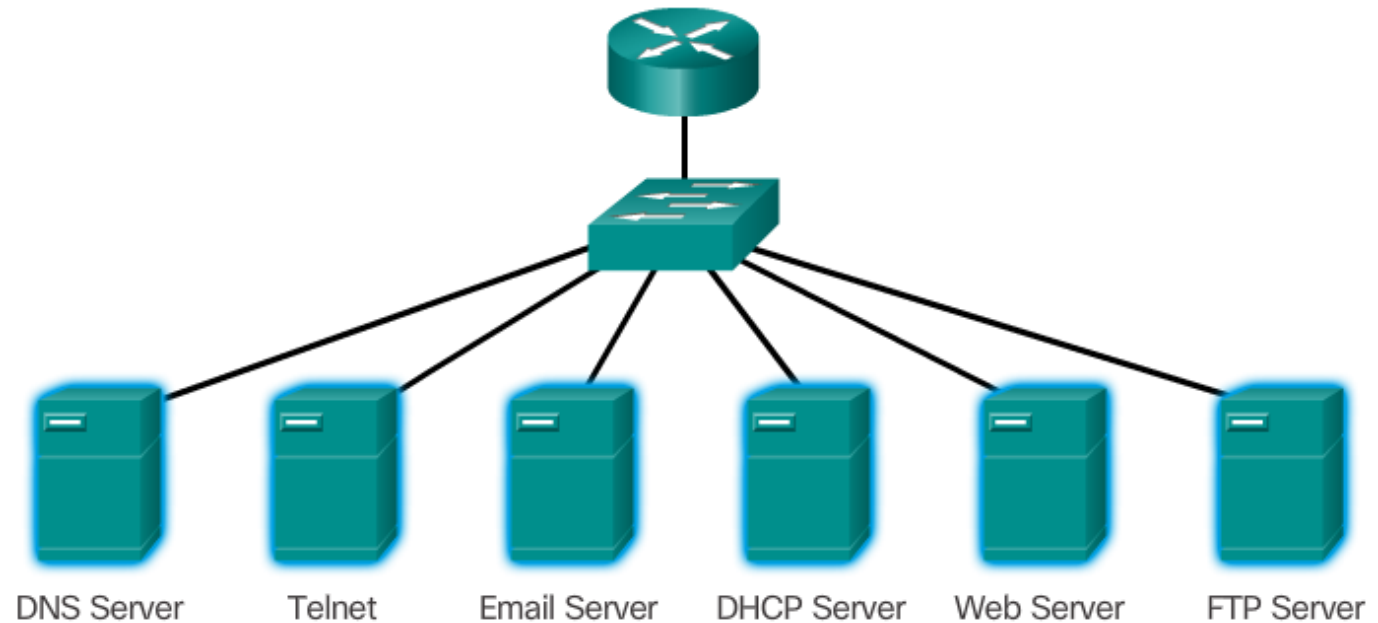
Aplikačné služby

- Program, ktorý je na rozhraní so sieťou a pripravuje dáta na prenos.
- Každá služba používa protokol(y), ktoré definujú štandardy a dátové formáty, ktoré treba použiť

Známe aplikačné protokoly

Každý z nich definuje:

- Procesy na oboch koncoch komunikačného spojenia
- Ako sa posielajú správy a aké sú možné/očakávané odpovede
- Typy správ
- Syntax správ
- Význam informačných polí
- Interakciu z nižšími vrstvami



Vhodná bezpečnostná politika: vždy keď sa dá, použiť zabezpečené verzie týchto protokolov (HTTPs, sFTP, SSH, ..)

Aplikácie typu real-time

Ich používanie má rastúci trend.

Je úlohou admina siete zabezpečiť na to infraštruktúru

- S ohľadom na súčasnosť aj plány
- V predmete Počítačové siete 3
- **VoIP**
 - Protokol, ktorý definuje ako preniesť hlas cez IP
 - Skype, Cisco WebEx, ..
- **IP telefónia**
 - Potrebná infraštruktúra pre VoIP:
 - IP telefóny
 - IP PBX (server pre riadenie a signalizáciu hovorov)
- **Transportné protokoly (L4) pre real-time aplikácie**
 - RTP (Real-Time Transport Protocol)
 - RTCP (Real-Time Control Protocol)
- Nasadenie **QoS** mechanizmov
 - V predmete Optimalizácia konvergovaných sietí





Téma 11.1.3: Škálovateľnosť na siete väčšieho rozsahu

Trend rozširovania malej siete

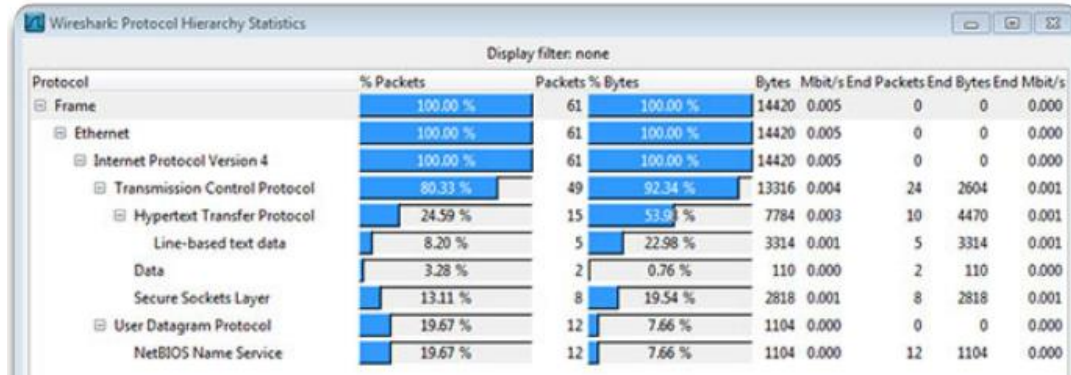
S rastom firmy musí **rásť** aj jej sieť.
Aby admin vedel robiť **inteligentné** rozhodnutia, je potreba:

- Dokumentácia siete
 - Fyzická a logická topológia
- Zoznam zariadení, ktoré používajú alebo tvoria sieť
- Finančný rozpočet
- Analýza prevádzky
 - Protokoly, aplikácie, služby a ich požiadavky treba zdokumentovať
 - Nástroje, ktorými vieme robiť analýzu, sa učia v predmete Počítačové siete 2



Analýza protokolov

- Napr. cez Wireshark

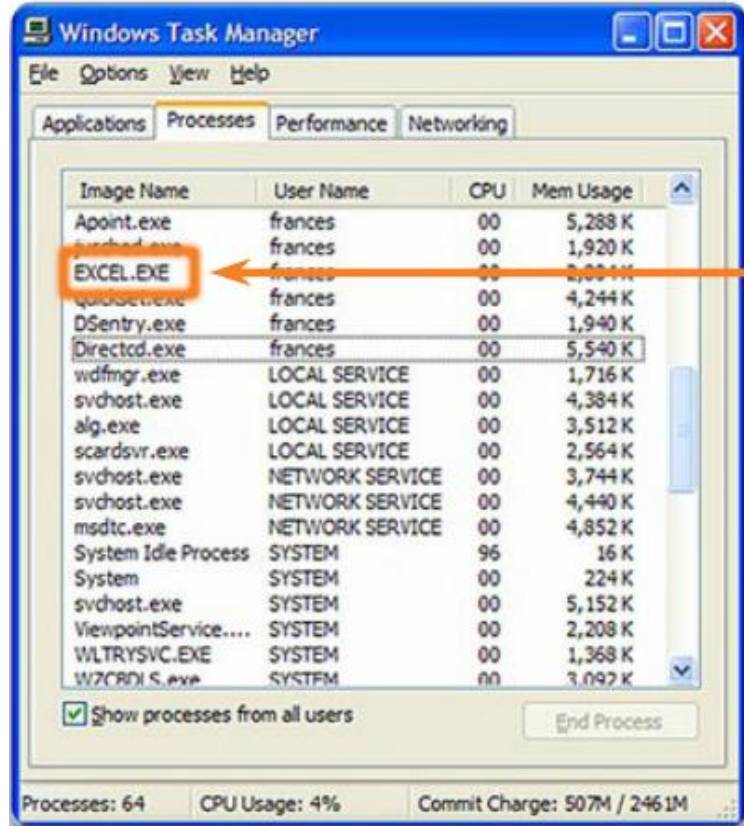


- Kedy odchytať prevádzku?
 - Počas špičky (peak)
- Kde odchytať prevádzku?
 - V rôznych častiach siete
- Načo analyzovať prevádzku?
 - Efektívnejšie manažovať prevádzku v sieti
 - Redukovať nepotrebné toky prevádzky
 - Zvýšiť výkonnosť siete, napríklad presunutím servera inam

Na čo používajú sieť zamestnanci danej firmy

IT snapshots

- Admin siete by mal byť informovaný ako a či sa ich použitie mení.
- Vie na to využiť tzv. IT “snapshots”



Processes are individual software programs running concurrently.

Processes can be:

- 1 Applications
- 2 Services
- 3 System operations
- 4 One program may be running several times, each in its own process

Na čo používajú sieť zamestnanci danej firmy

IT snapshots

- Info, ktoré možno získať z daných snapshotov:

- OS a verzia OS
- Nesieťové aplikácie
- Sieťové aplikácie
- Vyťaženie CPU
- Využitie diskov
- Vyťaženie RAM

- Treba zdokumentovať, sledovať vývoj v čase a pretaviť to do požiadaviek na protokoly (ak treba nejaké zmeny)
- Výrazné zmeny vo využiteľnosti zdrojov môžu vyvolať potrebu prispôbiť pridelovanie sieťových zdrojov.

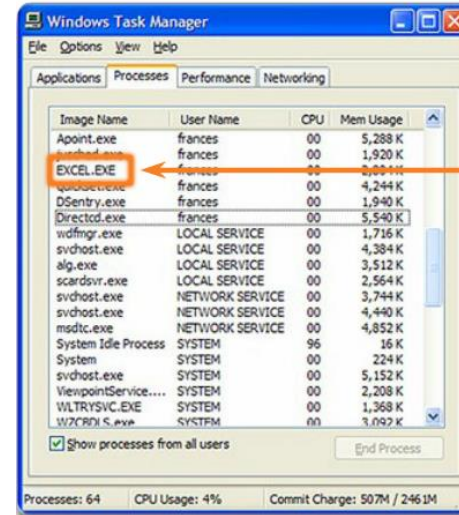


Image Name	User Name	CPU	Mem Usage
Apoinst.exe	frances	00	5,288 K
cmd.exe	frances	00	1,920 K
EXCEL.EXE	frances	00	2,004 K
svchost.exe	frances	00	4,244 K
DSEntry.exe	frances	00	1,940 K
Directcd.exe	frances	00	5,540 K
wdfmgr.exe	LOCAL SERVICE	00	1,716 K
svchost.exe	LOCAL SERVICE	00	4,384 K
alg.exe	LOCAL SERVICE	00	3,512 K
scardsvr.exe	LOCAL SERVICE	00	2,564 K
svchost.exe	NETWORK SERVICE	00	3,744 K
svchost.exe	NETWORK SERVICE	00	4,440 K
msdtc.exe	NETWORK SERVICE	00	4,852 K
System Idle Process	SYSTEM	96	16 K
System	SYSTEM	00	224 K
svchost.exe	SYSTEM	00	5,152 K
ViewpointService...	SYSTEM	00	2,208 K
WLTRYSVC.EXE	SYSTEM	00	1,368 K
WZCRUI S.exe	SYSTEM	00	3,092 K

Processes are individual software programs running concurrently.

Processes can be:

1 Applications

2 Services

3 System operations

4 One program may be running several times, each in its own process



Časť 11.2: Siet'ová bezpečnosť

Na konci by sme mali vedieť:

Vysvetliť prečo je dôležité zisťovať mieru bezpečnosti siet'ových zariadení.

Identifikovať bezpečnostné hrozby (security vulnerabilities).

Identifikovať všeobecné techniky pre minimalizovanie týchto hrozieb.

Konfigurovať siet'ové zariadenia tak, aby boli odolnejšie voči týmto hrozbám.

Aplikovať príkazy na zálohovanie a obnovenie konfiguračných súborov pre IOS.



Téma 11.2.1: Bezpečnostné hrozby a zraniteľnosti (Security Threats and Vulnerabilities)

Typy bezpečnostných hrozieb

- Digitálny prienik zväčša spôsobí nemalé škody
 - Strata časová a/alebo finančná
 - Kvôli poškodeniu alebo krádeži dôležitých informácií, alebo aktív
- Narušitelia (hackeri) využívajú bezpečnostné diery softvérov alebo útoky na hardvér, a môžu sa zamerať na:

- Využiť/predať info
- Firemné utajené dáta/výskum

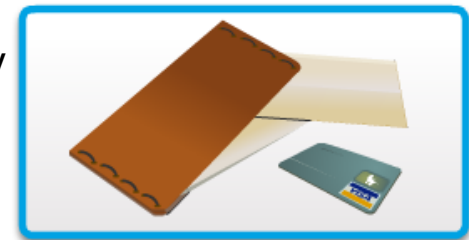


Information Theft

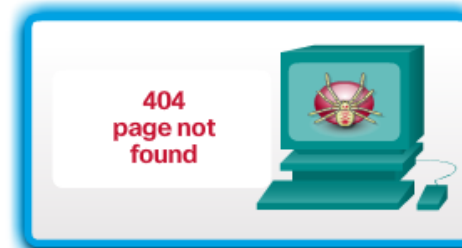


Data Loss and Manipulation

- Krádež údajov - kreditka – nákupy cez Internet
- V USA sa takto strácajú milióny dolárov



Identity Theft



Disruption of Service

- Zničiť/zmeniť dáta
- Vírus sformátuje HDD/ hacker zmení výsledky volieb
- DoS útoky na servery, sieťové zariadenia, linky
- Legitímnym používateľom sa odoprie prístup k sieťovej službe

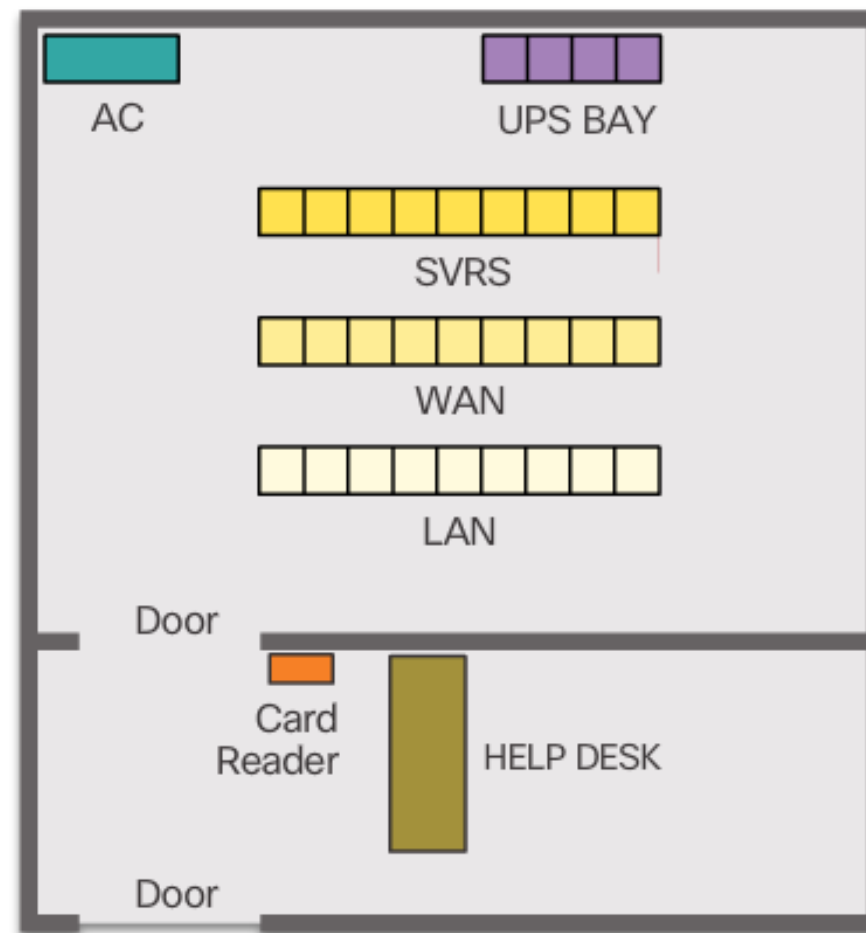
Fyzická bezpečnosť

Aj tú treba **plánovať** !

- Uzamykateľná serverovňa
- Kontrolovať prístup cez čipové karty
- Použiť bezpečnostné kamery

Triedy fyzických hrozieb:

- **Hardvérové**
 - Servre, smerovače, prepínače, káble, PC, ..
- **Prostredím**
 - Teplota, vlhkosť
- **Elektrické**
 - Výkyvy napätia, šum, výpadok prúdu
- **Údržbou**
 - Slabá/zlá kabeláž, chabo označená



Secure computer room floor plan

Typy zraniteľností

Cieľ útoku:

- Zväčša sú cieľom útoku koncové zariadenia (servery, PC)

Spôsob ako:

- Využiť pri útoku možno akúkoľvek z **3 kategórií zraniteľností**:
 - **Technologické**
 - Zraniteľnosť protokolov, OSs, sieťových zariadení
 - **Konfiguračné**
 - Zraniteľnosť zlou/nesprávnou konfiguráciou, použitím preddefinovaných hodnôt, ľahko uhádnuteľných hesiel
 - **Z bezpečnostnej politiky**
 - Slabá b.p., inštalácia SW a HW nie je v súlade s b.p., alebo nie je žiadny plán obnovenia (disaster/recovery plan)

Typy zraniteľnosti - technologické

- Slabiny TCP/IP protokolu
 - HTTP, FTP, ICMP sú
- Slabiny operačných systémov

Network security weaknesses:

TCP/IP protocol weakness

- Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Internet Control Message Protocol (ICMP) are inherently insecure.
- Simple Network Management Protocol (SNMP) and Simple Mail Transfer Protocol (SMTP) are related to the inherently insecure structure upon which TCP was designed.

Operating system weakness

- Each operating system has security problems that must be addressed.
- UNIX, Linux, Mac OS, Mac OS X, Windows Server 2012, Windows 7, Windows 8
- They are documented in the Computer Emergency Response Team (CERT) archives at <http://www.cert.org>.

Network equipment weakness

Various types of network equipment, such as routers, firewalls, and switches have security weaknesses that must be recognized and protected against. Their weaknesses include password protection, lack of authentication, routing protocols, and firewall holes.

Typy zranitel'nosti - konfiguračne

Configuration Weakness	How the weakness is exploited
Unsecured user accounts	User account information may be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result of poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in Web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes.

Typy zraniteľnosti - bezpečnostné

Policy Weakness	How the weakness is exploited
Lack of written security policy	An unwritten policy cannot be consistently applied or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of authentication continuity	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist.
Software and hardware installation and changes do not follow policy	Unauthorized changes to the network topology or installation of unapproved applications create security holes.
Disaster recovery plan is nonexistent	The lack of a disaster recovery plan allows chaos, panic, and confusion to occur when someone attacks the enterprise.



Téma 11.2.2: Siet'ové útoky

Malware

- zlomyseľný softvér alebo kód, ktorý obyčajne poškodí, zničí, alebo zablokuje používanie kontroly alebo odcudzí informáciu z počítačového systému



- Vírusy
 - Šíri sa kopírovaním, zväčša je časťou iného programu, užívateľ tento program musí spustiť, dovtedy je vírus nečinný, nevie sa replikovať, potom sa šíri cez mail, sieť, disky, USB kľuče, ...
- Červy
 - nepotrebujú hostiteľský program, vedia existovať samostatne, aj sa replikovať
- Trójske kone
 - tvári sa ako legitímny SW, ale nie je...
- Logické bomby, rootkity, bootkity, metódy tajných vstupov, špionážny softvér a reklamný softvér

Prieskumné metódy

(Reconnaissance Attacks)

- Pre odhalenie systémov a služieb
- Nie sú samy o sebe útokom, len vyzvedaním sa
- Cieľom je získať dostatok informácií o cieľovom systéme ešte pred samotným útokom – hľadajú sa zraniteľnosti
- Bežné nástroje sú postavené na otvorených a verejných internetových službách alebo protokoloch:
 - DNS
 - Whois.
 - Port-scanners
 - Packet sniffers



Internet queries



Ping sweeps

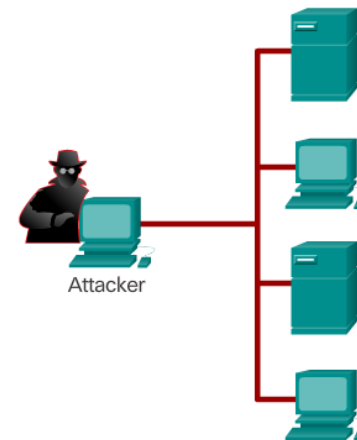


Port scans



Packet sniffers

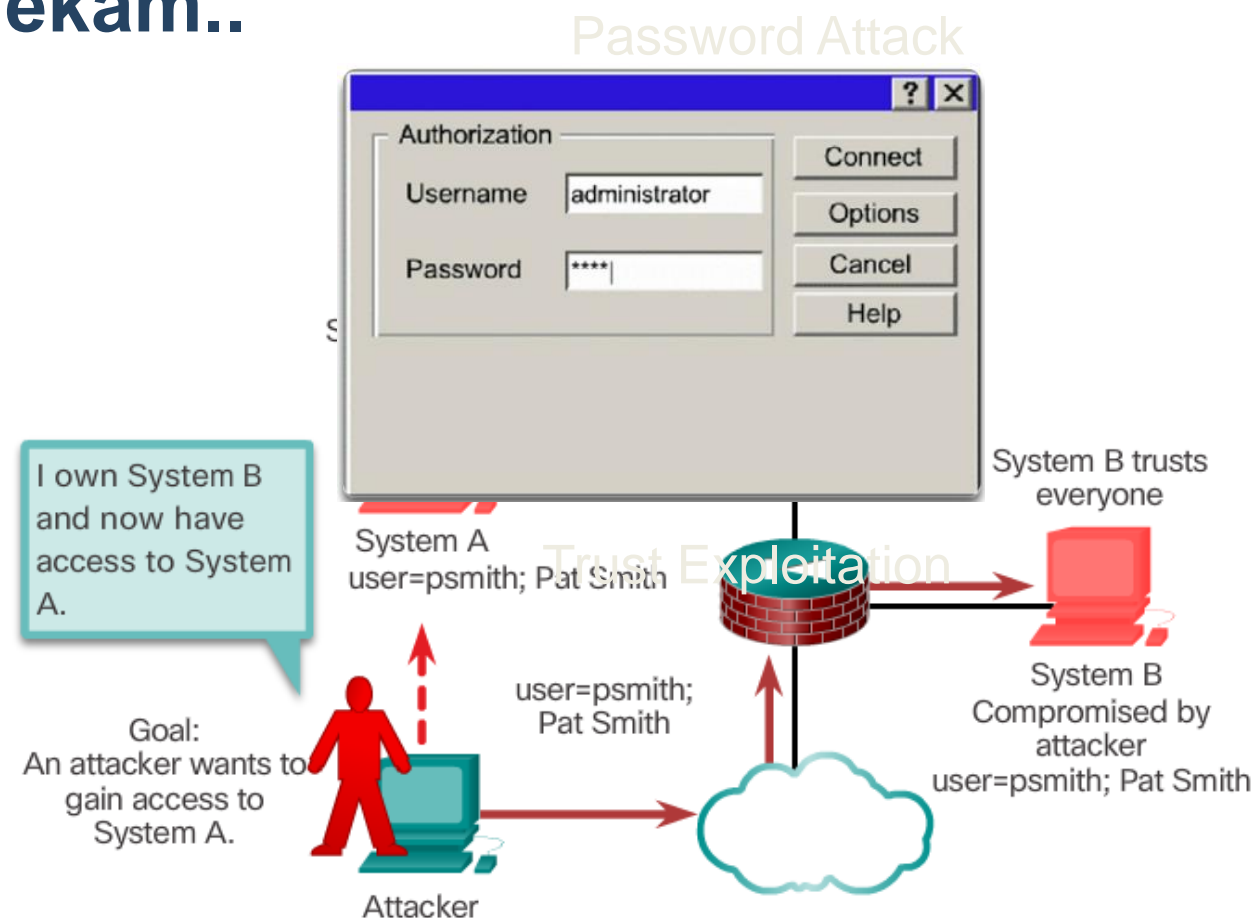
Netacad: animácia 11.2.2.2



Útoky na získanie prístupu niekam..

(Access Attacks)

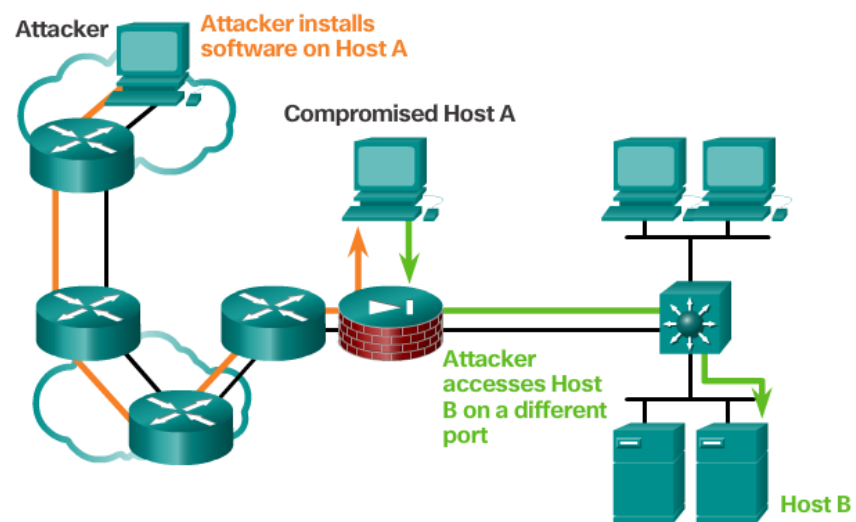
- Útok voči známym zraniteľnostiam a službám.
- Cieľom je získať prístup k tajným informáciám.
- Možno klasifikovať do 4 kategórií:
 - Útoky na odhalenie hesla (Password Attacks)
 - Zneužitie dôvery (Trust Exploitation)
 - Presmerovanie portov (Port Redirection)
 - Tzv. „Man-in-the-Middle“ útoky



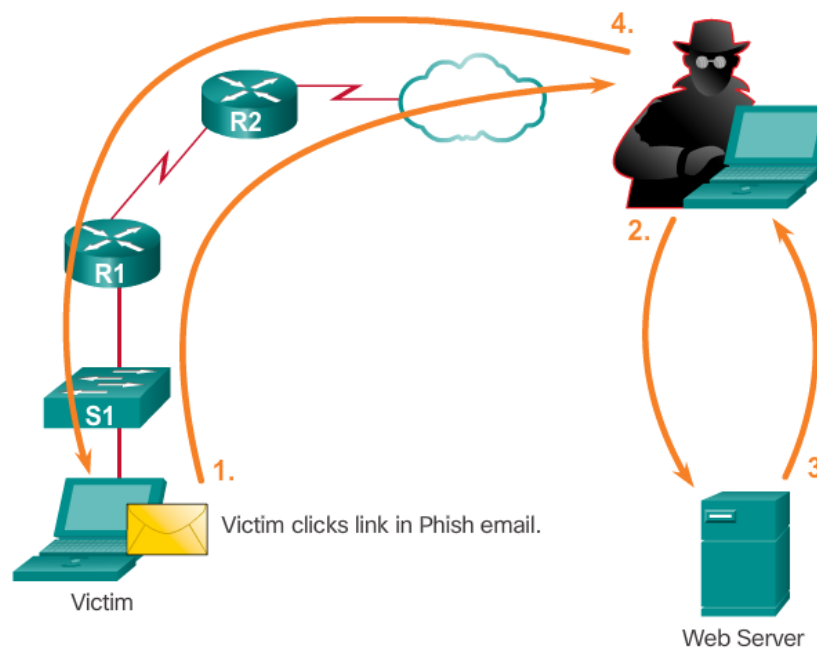
Útoky na získanie prístupu niekam..

(Access Attacks)

Port Redirection



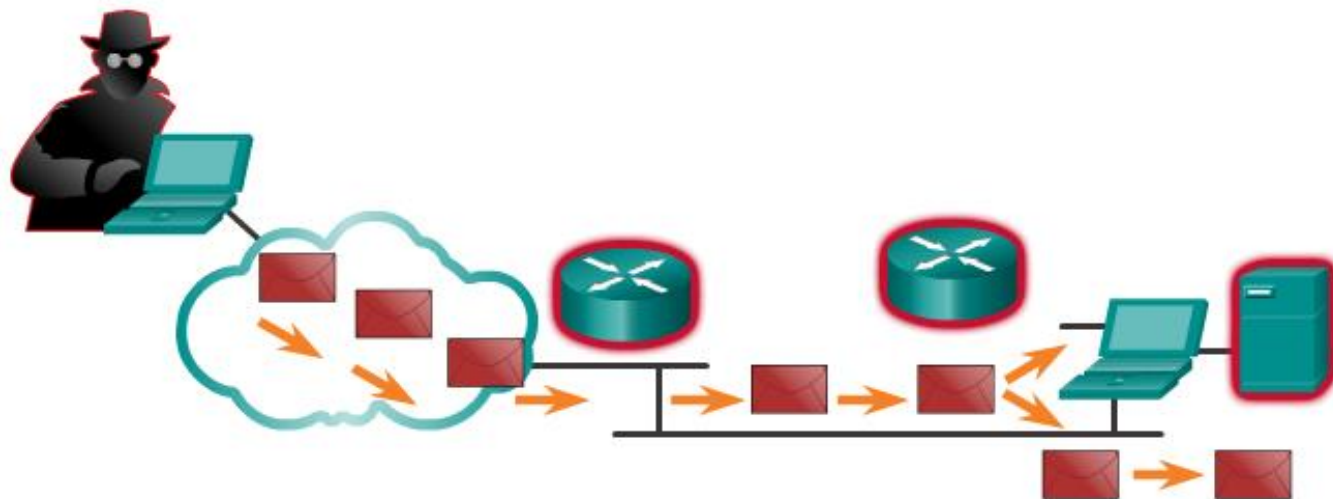
Man-in-the-Middle



Útoky na odopretie prístupu k službe

(DoS = Denial of Service Attacks)

- Ťažké úplne eliminovať
- Sú triviálne svojou podstatou, na vykonanie stačí malé úsilie
- Jednoduché ale stále nebezpečné
- Autorizovaným používateľom sa odoprie prístup k službe tým, že útočník vyčerpá všetky zdroje daného systému – zahlťe systém inými požiadavkami.
- Prevencia: mať najnovšie bezpečnostné aktualizácie



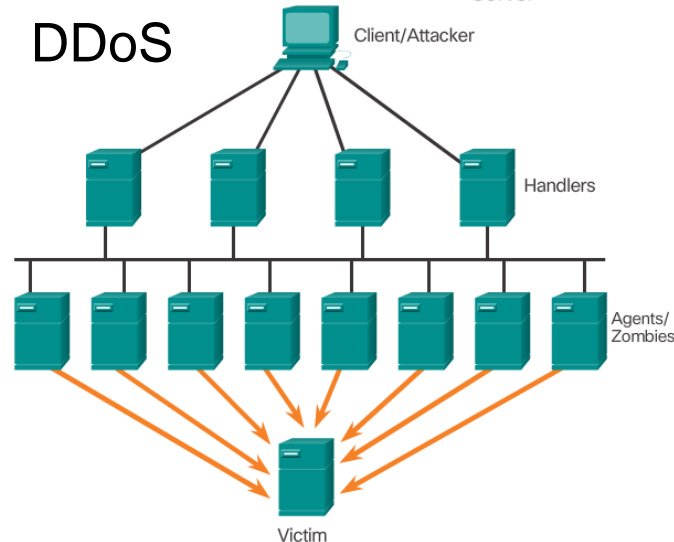
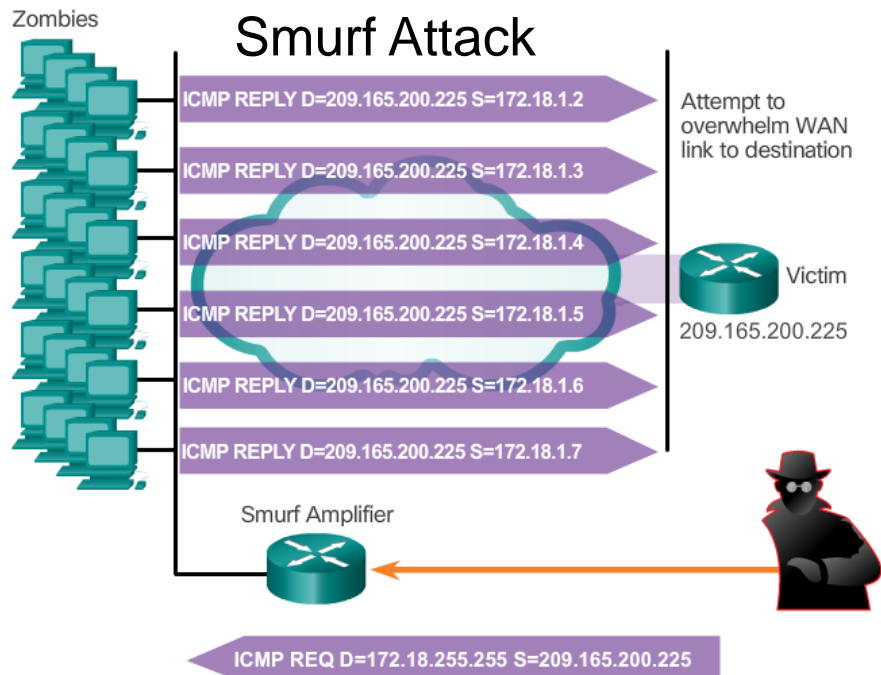
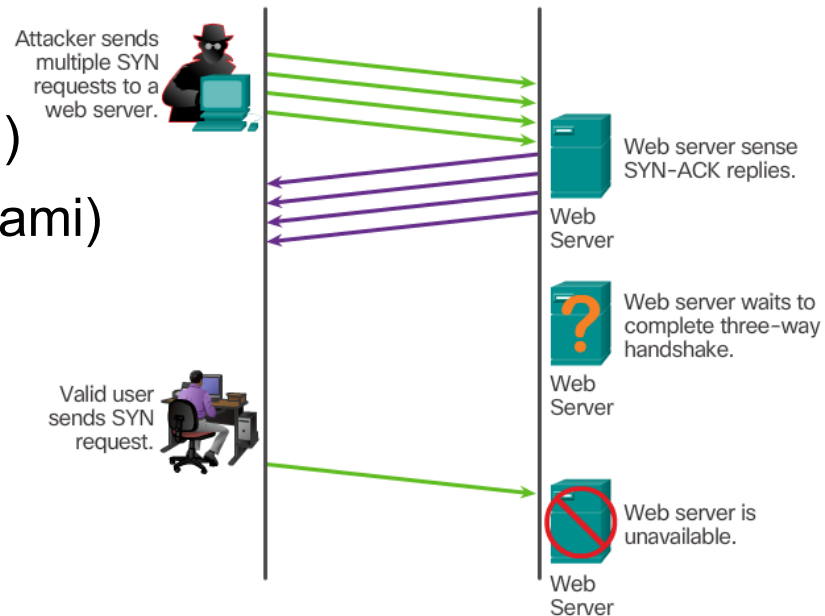
Útoky na odopretie prístupu k službe

(Denial of Service Attacks)

Známe DoS útoky:

- Ping of Death (smrťiaci/veľký PING)
- SYN Flood (záplava SYN segmentami)
- DDoS (distribúovaný DoS útok)
- Smurf Attack (útok paketmi PING)

SYN Flood



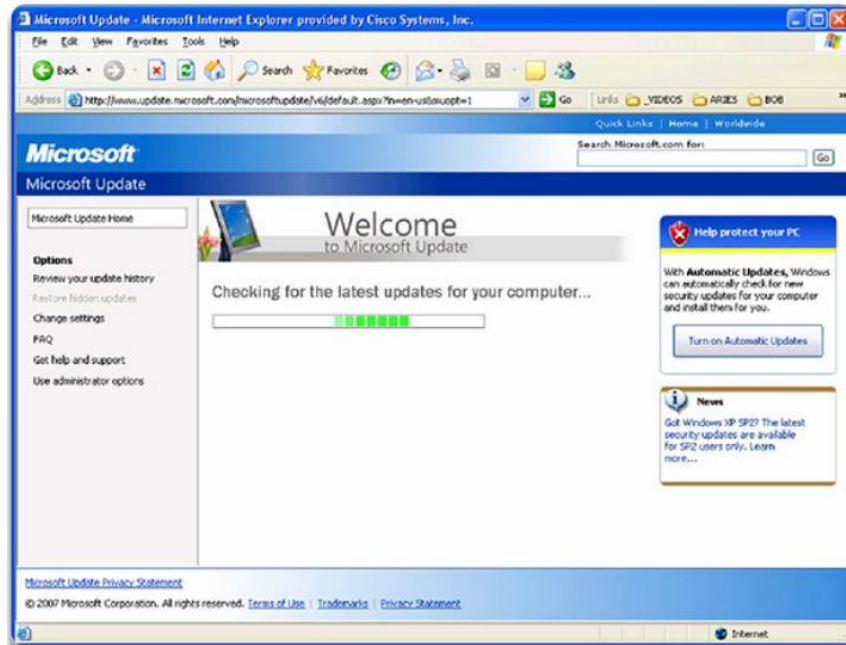


Téma 11.2.3: Ako zmierniť sieťové útoky

Zálohovať, inovovať, aktualizovať, inštalovať záplaty (Backup, Upgrade, Update, Patch)

Držať krok s vývojom, a tak zmierniť dopad útoku:

- Proti vírusom: najaktuálnejšie verzie antivírusového SW
- Proti červom: Aplikovať záplaty pre všetky známe slabiny
 - Vhodné je použiť centrálny patch server (pre všetky servery a systémy)..
..odkiaľ sa záplaty stiahnu a nainštalujú automaticky



Autentifikácia, autorizácia, účtovanie

(Authentication, Authorization, Accounting)

- Umožňujú riadenie prístupu k sieťovým zariadeniam:
 - Kto má právo** pristupovať k daným zdrojom (authenticate)
 - Čo môžu** počas prístupu robiť/vykonávať (authorize)
 - Ako dlho a čo** na danom zdroji **vykonávali**, aby bola možnosť ich za to vyúčtovať (accounting)
- Dôležitý prvok pre zmiernenie sieťových útokov

Authentication
Who are you?



Accounting
What did you spend it on?

Account Number: 1234-567-890 | Statement Closing Date: 01-31-01 | Current Amount Due: \$278.50

JOE EMPLOYEE
456 SKYVIEW DRIVE
HOMETOWN, USA 99900-1234

MAIL PAYMENT TO:
THE BANK
132 VINE STREET
ANYTOWN, USA 67500-0010

872919345 00172255000000003

Detach here
Do not staple or fold.

Authorization
How much can you spend?

Statement Closing Date: 01-31-01

Payment Due Date: 03-01-01

Closing Date: 01-31-01

Credit Limit: \$1,500.00

New Balance: \$278.50

Credit Available: \$1221.50

Minimum Payment Due: \$20.00

Account Summary

Previous Balance:	+74.24	Transaction Fees:	+3.00
Purchases:	+250.50	Annual Fees:	+25.00
Cash Advances:	+0	Current Amount Due:	+250.50
Payments:	-74.25	Amount Past Due:	+0
Finance Charge:	+0	Amount Over Credit Line:	+0
Late Charge:	+0	NEW BALANCE:	\$278.50

Reference Number	Sold	Posted	Activity Since Last Statement	Amount
43210987	01-03	01-13	Payment, Thank You	-\$74.25
01234567	01-12	01-13	Wings 'N' Things Anytown, USA	\$25.25
78901234	01-14	01-17	Record Release Anytown, USA	\$40.00
45678901	01-14	01-17	Sports Stadium Anytown, USA	\$75.25
3210987	01-22	01-23	Tie Tack Anytown, USA	\$20.75
78943210	01-29	01-30	Electronic World Anytown, USA	\$89.25
2345678		01-30	Transaction Fees	\$3.00
34567890		01-01	Annual Fee	\$25.00

PAGE 1 OF 1

Bezpečnostné rozhranie = Firewall

- kombinácia softvéru a hardvéru, ktorá filtruje alebo blokuje prevádzku z verejnej siete
- udržiava časti neverejnej siete nedostupné a neviditeľné pre verejnú sieť
- zabraňuje neautorizovanému a nepovolenému prístupu
- zariadenie na filtrovanie dát, ktoré sa inštaluje medzi server alebo dátové komunikačné zariadenie a verejnú sieť (internet) trvalo dohliada na postupnosti dát, ktoré indikujú neautorizované použitie alebo nežiaducu komunikáciu so serverom
- líšia sa počtom vyrovnávacích pamätí a filtrovacou schopnosťou



Bezpečnostné rozhranie = Firewall

- Ako admin viem nadefinovať čo pustím a čomu prístup zakážem:
 - Packet filtering
 - Bude v predmete PS1
 - Application filtering
 - URL filtering
 - Stateful packet inspection (SPI)



Cisco Security Appliances



Server-Based Firewall



Linksys Wireless Router with Integrated Firewall



Personal Firewall

Bezpečnosť koncových zariadení

Laptops, desktops, servers, smartphones, tablets, ...

- Zabepečiť koncové zariadenia je veľká **výzva**
- Zamestnancov treba školiť – ako bezpečne využívať sieť
- Bezpečnostné postupy zväčša zahŕňajú
 - **antivírusový softvér**
 - softvér na **prevenciu vniknutia**
- Komplexnejšie riešenia sú závislé na systémoch pre riadenie kontroly do siete

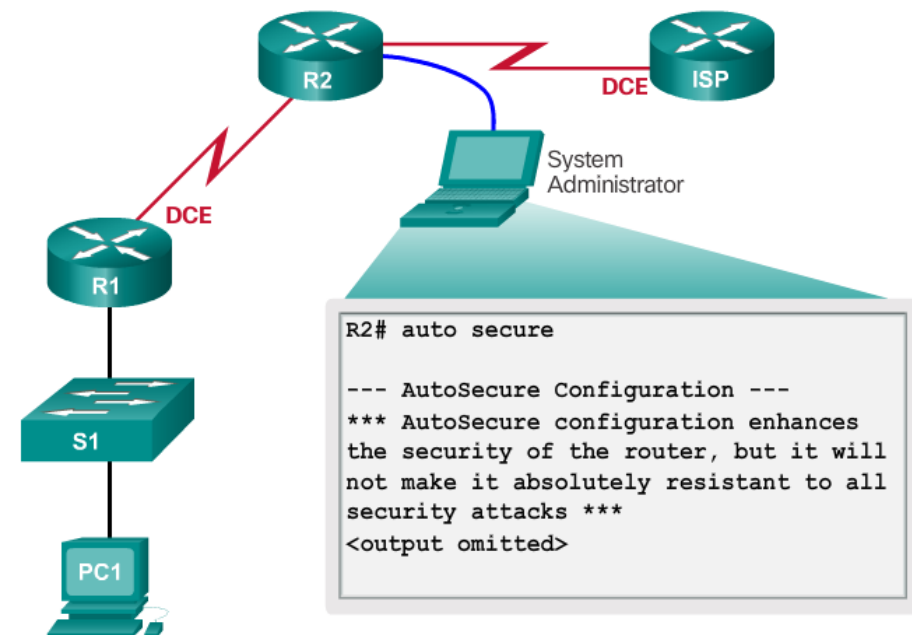




Téma 11.2.4: Bezpečnosť medzi'ahľých sieťových zariadení

Celkový pohľad na bezpečnosť zariadení

- **Defaultné** nastavenia sú nebezpečné, lebo sú známe
- Cisco smerovače majú funkciu **AutoSecure**
- Okrem toho je však potrebné minimálne:
 - Zmeniť defaultné nastavenia pre prihlasovacie mená a heslá
 - Obmedziť prístup k systémovým zdrojom len pre autorizovaných používateľov.
 - Vypnúť nepotrebné služby.
 - Aktualizovať všetok používaný softvér a nainštalovať bezpečnostné záplaty
- Toto všetko spraviť ešte pred samotným nasadením zariadenia do reálnej prevádzky



Heslá

- Používať silné heslá:
 - Minimálne **8 znakov**, ideálne 10 a viac
 - Kombinácia malých, veľkých písmen, číslíc, symbolov a medzier
 - B54n74d85m
 - 12^f s7@1w4
 - Nepoužívať slová zo slovníka akéhokoľvek jazyka, mená svojich známych, zvierat, alebo inak ľahko identifikovateľné časti informácií
 - Možno použiť slová obsahujúce pravopisné alebo iné chyby
 - Smyth = 5mYth
 - Security = 5ecur1ty
 - Často obmieňať
- Cisco smerovače podporujú použitie frázy zloženej s viacerých slov oddelených medzerou, tzv. **passphrase**
 - Napr.: 5mYth'5 5ecurYti Ys the be5t!
 - (Smith's security is the best!)

Základné bezpečnostné pravidlá pre heslá

- Silné heslá sú len vtedy použiteľné a silné keď ostatnú **tajné** (nepísať na nástenku ani na papier do zásuvky)
- Použiť príkaz na **zašifrovanie** všetkých hesiel na Cisco zariadení (súčasných alebo tých čo pribudnú do konfigurácie v budúcnosti):

```
service password-encryption
```

- Použiť príkaz, ktorým stanovíme **min. dĺžku** zadávaných hesiel:

```
security passwords min-length počet_znakov
```

- Blokovať počet za sebou idúcich **neúspešných** pokusov o prihlásenie, pre minimalizovanie útokov hrubou silou (brute-force attacks) pre uhádnutie hesla:

```
login block-for 120 attempts 3 within 60
```

- Zablokuje možnosť prihlásenie na 120 sekúnd, ak používateľ 3x po sebe netrafí heslo v intervale 60 sekúnd
- Použiť príkaz pre automatické odhlásenie používateľa pri neaktivite:

```
exec timeout čas_v_minútach
```

Základné bezpečnostné pravidlá pre heslá

```
Router(config)#service password-encryption
Router(config)#security password min-length 8
Router(config)#login block-for 120 attempts 3 within 60
Router(config)#line vty 0 4
Router(config-vty)#exec-timeout 10
Router(config-vty)#end
Router#show running-config
-more-
!
line vty 0 4
  password 7 03095A0F034F38435B49150A1819
  exec-timeout 10
  login
```

Konfigurácia a povolenie SSH

- že Telnet nie je bezpečný sme sa presvedčili na 11. cvičení
- Preto sa vysoko odporúča používať pre vzdialenú správu zariadenia prihlasovanie cez **SSH**.
- Postup konfigurácie Cisco zariadenia, aby podporovalo SSH:
 1. Zabepečiť, aby smerovač mal jedinečný hostname a IP doménu.
ip domain-name uniza.sk
 2. Vygenerovať kľuče pre SSH.
crypto key generate rsa general-keys modulus 1024
 3. Vytvoriť lokálne prihlasovacie meno (username)
username Bob **secret** cisco
 4. Povoľiť SSH pre tie relácie, kde ho potrebujeme (napr. pre vty)
line vty 0 15
login local
transport input ssh
- Následne sa bude dať na smerovač (alebo prepínač) pripájať vzdialene už len cez SSH.

Konfigurácia a povolenie SSH



```
R1# conf t
R1(config)# ip domain-name span.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.span.com
% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
R1(config)#
*Dec 13 16:19:12.079: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# username Bob secret cisco
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exit
```

- Step 1: Configure the IP domain name.
- Step 2: Generate one-way secret keys.
- Step 3: Verify or create a local database entry.
- Step 4: Enable VTY inbound SSH sessions.



Téma 11.2.5: Záloha a obnovenie konfiguračných súborov

Systemy súborov smerovača s Cisco IOS

(Cisco IOS Router File Systems)

- Umožňujú operácie read (r) aj write (w).
- Zobrazím ich príkazom **show file systems**, a následne obsah ľubovoľného z nich zobrazím príkazom **dir ...**
- Pre nás v tomto predmete sú zaujímavé súborové systémy:
 - **TFTP**
 - **FLASH**
 - Zväčša najväčší súborový systém
 - Zväčša obsahuje obraz operačného systému Cisco IOS (image)
 - **NVRAM**
 - Zväčša obsahuje konfiguračné súbory (startup-config)
 - Zväčša kapacitne malý

```
Router#show file systems
File Systems:

      Size (b)      Free (b)      Type  Flags  Prefixes
      -          -          -     -     -
      -          -          opaque rw  archive:
      -          -          opaque rw  system:
      -          -          opaque rw  tmpsys:
      -          -          opaque rw  null:
      -          -          network rw  tftp:
* 256487424      183234560      disk  rw  flash0: flash:#
      -          -          disk  rw  flash1:
      262136      254779        nvram  rw  nvram:
      -          -          opaque wo  syslog:
      -          -          opaque rw  xmodem:
      -          -          opaque rw  ymodem:
      -          -          network rw  rcp:
      -          -          network rw  http:
      -          -          network rw  ftp:
      -          -          network rw  scp:
      -          -          opaque ro  tar:
      -          -          network rw  https:
      -          -          opaque ro  cns:
```

File Systems

```
Router#dir
Directory of flash0:/

 1 -rw-   2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
 19xx.cfg
 2 -rw-  3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-   1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-  122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw- 1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
 ios-3.1.1.45-k9.pkg
 6 -rw-  415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
 1.1.4.176.pkg
 7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00  cl900-
 universalk9-
 mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

Flash

show file systems

Systemy súborov smerovača s Cisco IOS

(Cisco IOS Router File Systems)

```
Router#show file systems
File Systems:

      Size (b)      Free (b)      Type  Flags  Prefixes
      -           -           opaque  rw    archive:
      -           -           opaque  rw    system:
      -           -           opaque  rw    tmpsys:
      -           -           opaque  rw    null:
      -           -           network rw    tftp:
* 256487424 183234560      disk   rw    flash0: flash:#
      -           -           disk   rw    flash1:
      262136    254779      nvram   rw    nvram:
      -           -           opaque  wo    syslog:
      -           -           opaque  rw    xmodem:
      -           -           opaque  rw    ymodem:
      -           -           network rw    rcp:
      -           -           network rw    http:
      -           -           network rw    ftp:
      -           -           network rw    scp:
      -           -           opaque  ro    tar:
      -           -           network rw    https:
      -           -           opaque  ro    cns:
```

Flash

Systemy súborov smerovača s Cisco IOS

(Cisco IOS Router File Systems)

```
Router#dir
Directory of flash0:/

 1 -rw-      2903 Sep 7 2012 06:58:26 +00:00  cpconfig-
    19xx.cfg
 2 -rw-  3000320 Sep 7 2012 06:58:40 +00:00  cpexpress.tar
 3 -rw-      1038 Sep 7 2012 06:58:52 +00:00  home.shtml
 4 -rw-   122880 Sep 7 2012 06:59:02 +00:00  home.tar
 5 -rw-  1697952 Sep 7 2012 06:59:20 +00:00  securedesktop-
    ios-3.1.1.45-k9.pkg
 6 -rw-   415956 Sep 7 2012 06:59:34 +00:00  sslclient-win-
    1.1.4.176.pkg
 7 -rw- 67998028 Sep 26 2012 17:32:14 +00:00  c1900-
    universalk9-
    mz.SPA.152-4.M1.bin

256487424 bytes total (183234560 bytes free)
```

Systemy súborov prepínača s Cisco IOS

(Cisco IOS Switch File Systems)

- Podobne ako na smerovači
- Súborový systém Flash podporuje:
 - konfiguračné súbory
 - kopírovať a archivovať obrazy Cisco IOSu (upload/download)
- Príkazy rovnaké ako na smerovači:
 - **show file systems**
 - **dir...**

Cisco 2960 Switch

```
Switch# show file systems
File Systems:
```

	Size (b)	Free (b)	Type	Flags	Prefixes
*	32514048	20887552	flash	rw	flash:
	-	-	opaque	rw	vb:
	-	-	opaque	ro	bs:
	-	-	opaque	rw	system:
	-	-	opaque	rw	tmsys:
	65536	48897	nvrám	rw	nvrám:
	-	-	opaque	ro	xmodem:
	-	-	opaque	ro	ymodem:
	-	-	opaque	rw	null:
	-	-	opaque	ro	tar:
	-	-	network	rw	tftp:
	-	-	network	rw	rcp:
	-	-	network	rw	http:
	-	-	network	rw	ftp:
	-	-	network	rw	scp:
	-	-	network	rw	https:
	-	-	opaque	ro	cns:

Zálohovanie a obnovenie konfigurácie

Zálohovanie konfigurácie

- Konfiguračné súbory možno uložiť/zálohovať do textového súboru
1. Zobrazit' si výpis:
`show running-config`
alebo `show startup-config`
 2. Skopírovať výpis (ctrl+c)
 3. Vložit' do textového súboru (ctrl+v), vhodne pomenovať
 4. Skontrolovať obsah
 5. Ak ukladáme running-config, a chceme neskôr použiť pre nenakonfigurované zariadenie, čo treba pridať pre každé rozhranie?

no shutdown

Obnovenie konfigurácie

- Konfiguráciu možno nahrat' naspät' na zariadenie
1. Nastaviť sa do globálneho konfiguračného módu
 2. Skopírovať obsah uloženého konfiguračného súboru (ctrl+c) a vložit' do príkazového riadku na zariadení (ctrl+v)
 3. Všetko sa vykoná v IOSe ako príkazy a pridá sa do aktuálneho súboru `running-config`

(no shutdown totiž nie je v running-config explicitne viditeľné)

Zálohovanie a obnovenie konfigurácie z TFTP servera

Zálohovanie konfigurácie

1. `copy running-config tftp`
2. Zadať IP adresu TFTP servera
3. Zadať názov konfiguračného súboru
4. enter

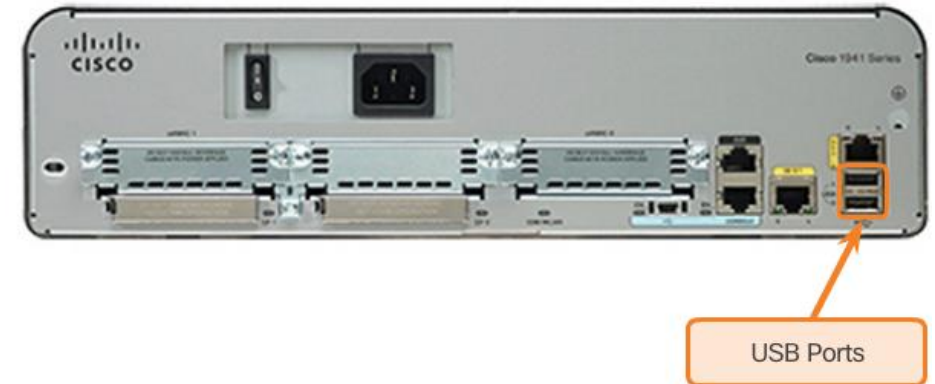
Obnovenie konfigurácie

1. `copy tftp running-config`
2. Zadať IP adresu TFTP servera
3. Enter – potvrdíme názov súboru v [...]
alebo zadáme názov ak chceme niečo špecifické

Používanie portov USB na smerovači Cisco

Cisco 1941 USB Port

- Niektoré modely smerovačov Cisco podporujú USB flash disky.
- Funkcia USB flash poskytuje možnosti ďalšieho ukladania a ďalšie boot zariadenie.
- Môže obsahovať obrázky, konfigurácie a ďalšie súbory.
- USB flash pamäť môže obsahovať:
 - Cisco IOS.
 - Viaceré konfigurácie smerovača.
- Na zobrazenie obsahu USB flash disku sa používa príkaz **dir**, ako je znázornené na obrázku.



```
Router# dir usbflash0:  
Directory of usbflash0:/  
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00  
c3825-entservicesk9-mz.123-14.T  
63158272 bytes total (33033216 bytes free)
```

Zálohovanie a obnovenie pomocou USB

Záložné konfigurácie pomocou USB Flash Drive

- Zobrazenie príkazom **show file systems**
- Pomocou príkazu **copy run usbflash0:/** skopírujete konfiguračný súbor na jednotku USB flash.
- IOS vyzve na zadanie názvu súboru.
- Pomocou príkazu **dir** zobrazíte súbor na jednotke USB.

```
R1# show file systems
File Systems:

      Size(b)      Free(b)      Type  Flags  Prefixes
      -          -          -     -     -
      -          -          opaque rw    archive:
      -          -          opaque rw    system:
      -          -          opaque rw    tmpsys:
      -          -          opaque rw    null:
      -          -          network rw    tftp:
* 256487424      184819712      disk  rw    flash0: flash:#
      -          -          disk  rw    flash1:
      262136      249270          nvram rw    nvram:
      -          -          opaque wo    syslog:
      -          -          opaque rw    xmodem:
      -          -          opaque rw    ymodem:
      -          -          network rw    rcp:
      -          -          network rw    http:
      -          -          network rw    ftp:
      -          -          network rw    scp:
      -          -          opaque ro    tar:
      -          -          network rw    https:
      -          -          opaque ro    cns:
4050042880      3774152704      usbflash rw    usbflash0:
```

Shows the USB port and name: "usbflash0:"

Obnovenie konfigurácie pomocou jednotky USB Flash

- Za predpokladu, že názov súboru je **R1-Config**, použite príkaz **copy usbflash0:/R1-Config running-config** na obnovenie bežiackej konfigurácie.



Časť 11.3: Príkazy pre overenie funkčnosti malej siete



Téma 11.3.1: Príkaz PING

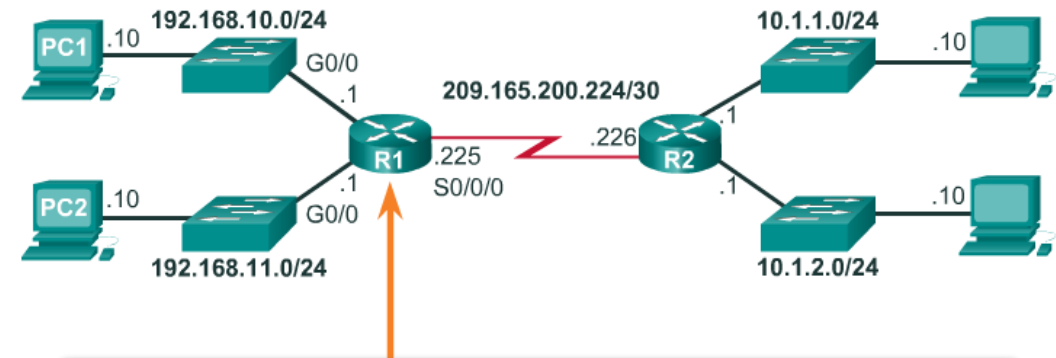
PING

- Použitie **pingu** je efektívny spôsob ako otestovať konektivitu.
- Zabezpečuje ho protokol Internet Control Message Protocol (ICMP) pre overenie konektivity na 3 vrstve.
- **Pingom** vieme zistiť problém v spojení.
- Ping zobrazuje jednu z niekoľkých indikácií pre každú ICMP echo správu, ktorá bola odoslaná. Najbežnejšie indikácie sú:
 - **!** - Označuje príjem odpovede na odpoveď ICMP echo.
 - **.** - Označuje čas, ktorý uplynul pri čakaní na odpoveď ICMP echo.
 - **U** - Označuje, že bola prijatá správa ICMP o nedostupnosti.

PING

IOS ping indikátory

- "." indikuje, že nastal problém s konektivitou na ceste do cieľa. Možné príčiny:
 - Smerovač na ceste do cieľa nepozná cestu.
 - Ping bol administratívne zablokovaný.
 - Pingu vypršala platnosť z dôvodu prebiehajúcej žiadosti ARP.
- "U" indikuje, že smerovač na ceste do cieľa odpovedal správou ICMP unreachable message. Smerovač nepozná cestu do cieľa alebo je žiadosť administratívne zablokovaná.



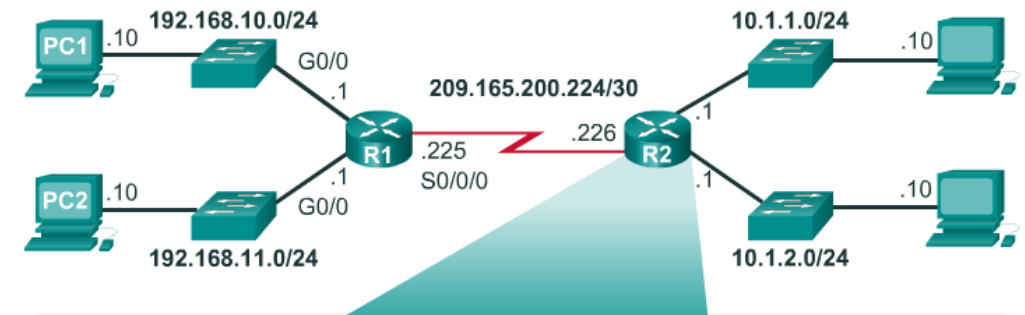
```
R1# ping 209.165.200.226

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout
is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max =
3/3/4 ms

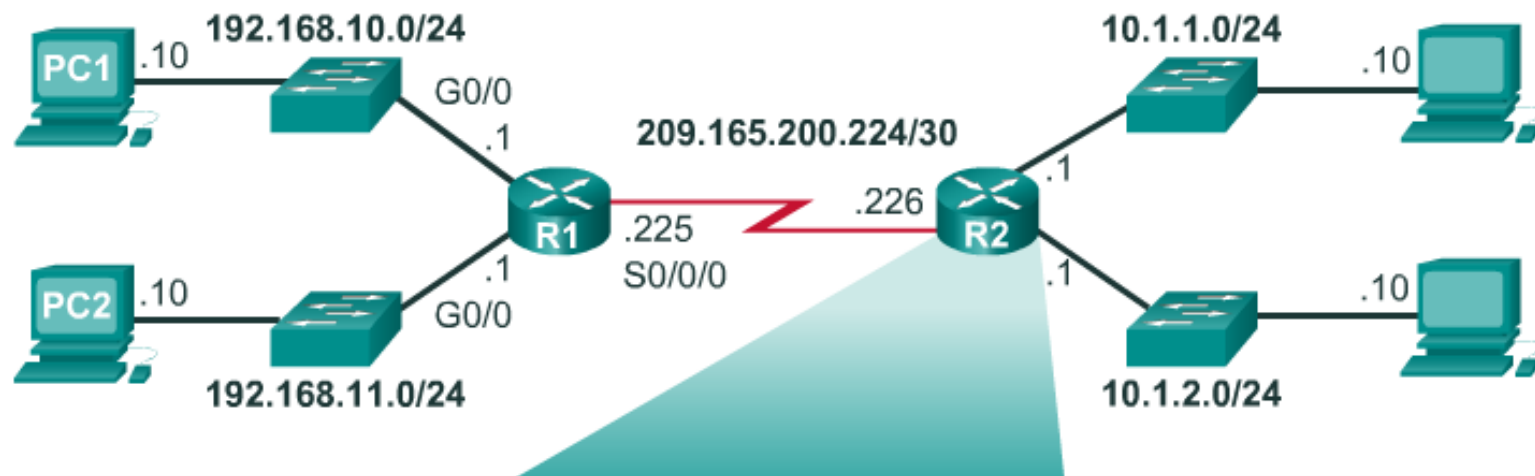
R1#
```

Rozšířený ping

- Cisco IOS ponúka rozšírený ping.
- Používa sa zadaním príkazom **ping** bez cieľovej IP adresy v EXEC móde.
- IOS nás vyzve zadať ďalšie voliteľné parametre.



```
R2# ping
Protocol [ip]:
Target IP address: 192.168.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:
```



```

R2# ping
Protocol [ip]:
Target IP address: 192.168.10.1
Repeat count [5]:
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface: 10.1.1.1
Type of service [0]:
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.10.1, timeout is 2 seconds:

```

Pravidelné sieťové záznamy

- Je veľmi dôležitý nástroj pre monitorovanie a zisťovanie problémov.
- Počas určitého časového intervalu sa vytvoria záznamy o výkone siete.
- Slúžia pre porovnanie výkonnosti siete podľa času.

FEB 8, 2013 08:14:43

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 10.66.254.159:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

MAR 17, 2013 14:41:06

```
C:\>ping 10.66.254.159
```

```
Pinging 10.66.254.159 with 32 bytes of data:
```

```
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128  
Reply from 10.66.234.159: bytes=32 time<6ms TTL=128
```

```
Ping statistics for 10.66.254.159:  
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),  
Approximate round trip times in milli-seconds:  
Minimum = 6ms, Maximum = 6ms, Average = 6ms
```



Téma 11.3.2: Príkazy traceroute a tracert

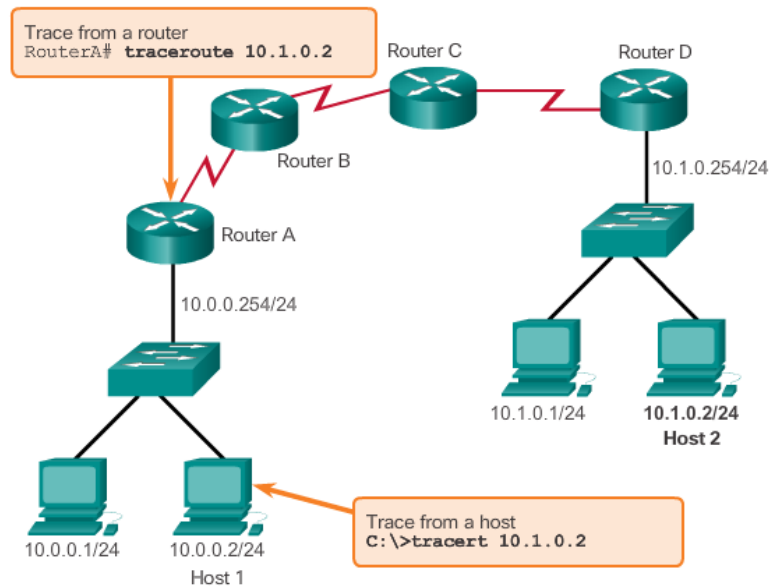
Príkaz tracert

- Zobrazí zoznam zariadení, cez ktoré vedie cesta do cieľa.
- Syntax príkazu je závislá od OS.
- Vo Windows sa používa príkaz **tracert**
- V Cisco IOS a UNIX OS sa používa **tracert**.

Tracing the Route from Host 1 to Host 2

Testing the Path to a Remote Host

```
C:\> tracert 10.1.0.2
Tracing route to 10.1.0.2 over a maximum of 30 hops
 1  2 ms  2 ms  2 ms  10.0.0.254
 2  * * * Request timed out.
 3  * * * Request timed out.
 4  ^C
C:\>
```





Téma 11.3.3: Príkazy show

Časté príkazy show

- Sú vhodné nástroje pre zisťovanie informácií a riešenie problémov.
- Zobrazia konfiguračné súbory, stav rozhraní a procesov.
- Najčastejšie používané príkazy **show**:
 - **show running-config**
 - **show interfaces / show ip interface ... / show ip interface brief**
 - **show arp**
 - **show ip route**
 - **show protocols**
 - **show version**

```
R1# show running-config
<Output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
description LAN 192.168.1.0 default gateway
ip address 192.168.1.1 255.255.255.0
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
shutdown
duplex auto
speed auto
!
interface Serial0/0/0
description WAN link to R2
ip address 192.168.2.1 255.255.255.0
encapsulation ppp
clock rate 64000
no fair-queue
!
interface Serial0/0/1
no ip address
shutdown
!
interface Vlan1
no ip address
!
router rip
version 2
network 192.168.1.0
network 192.168.2.0
!
banner motd ^CUnauthorized Access Prohibited^C
!
ip http server
!
```

```
R1# show running-config
<Output omitted>
Building configuration...
Current configuration : 1063 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname R1
enable secret 5 $1$i6w9$dvdpmVM6zV10E6tSyLdkR5/
no ip domain lookup
!
interface FastEthernet0/0
  description LAN 192.168.1.0 default gateway
  ip address 192.168.1.1 255.255.255.0
  duplex auto
  speed auto
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
```

```
!  
interface Serial0/0/0  
  description WAN link to R2  
  ip address 192.168.2.1 255.255.255.0  
  encapsulation ppp  
  clock rate 64000  
  no fair-queue  
!  
interface Serial0/0/1  
  no ip address  
  shutdown  
!  
interface Vlan1  
  no ip address  
!  
router rip  
  version 2  
  network 192.168.1.0  
  network 192.168.2.0  
!  
banner motd ^CUnauthorized Access Prohibited^C  
!  
ip http server  
!  
line con 0
```



Téma 11.3.4: Host a IOS příkazy

Príkaz ipconfig

- Príkaz **ipconfig** je možné použiť na zobrazenie IP informácií o počítači so systémom Windows.
- Príkaz **ipconfig /all** zobrazí detailnejšie IP informácie vrátane MAC adresy.
- Príkaz **ipconfig /displaydns** zobrazí všetky uložené DNS záznamy na OS Windows.

ipconfig




```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix . . . :
    IP Address. . . . . : 192.168.1.2
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.1.254
```

Legend

-  IP address for this host computer
-  Local network subnet mask
-  Default gateway address for this host computer

ipconfig /all

```
C:\>ipconfig /all

Ethernet adapter Network Connection:

    Connection-specific DNS Suffix: example.com
    Description . . . . . : Intel(R)
    PRO/Wireless 3945ABG Network Connection
    Physical Address. . . . . : 00-18-DE-C7-F3-FB
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 10.2.3.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 10.2.3.254
    DHCP Server . . . . . : 10.2.3.69
    DNS Servers . . . . . : 192.168.226.120
    Lease Obtained. . . . . : Thursday, May 03,
                             2007 3:47:51 PM
    Lease Expires . . . . . : Friday, May 04,
                             2007 6:57:11 AM

C:\>
```

Príkaz ipconfig

ipconfig /displaydns

```
C:\> ipconfig /displaydns

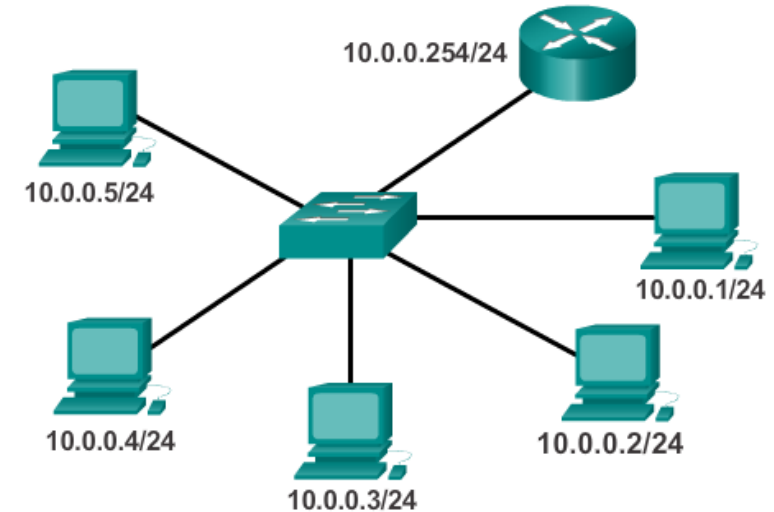
Windows IP Configuration

    cisco-tags.cisco.com
-----
Record Name . . . . . : cisco-tags.cisco.com
Record Type . . . . . : 1
Time To Live . . . . . : 44024
Data Length . . . . . : 4
Section . . . . . : Answer
A (Host) Record . . . : 72.163.10.10
```

<output omitted>

Príkaz arp

- Zobrazí informácie o zariadeniach v ARP cache hosta
- Zahŕňa aj IPv4 adresu, fyzickú adresu a typ adresovania (statické/dynamické) pre každé zariadenie.
- Vymazanie príkazom **arp -d**



```
c:\>arp -a
Internet Address Physical Address Type
10.0.0.2          00-08-a3-b6-ce-04 dynamic
10.0.0.3          00-0d-56-09-fb-d1 dynamic
10.0.0.4          00-12-3f-d4-6d-1b dynamic
10.0.0.254       00-10-7b-e7-fa-ef dynamic
```

IP- MAC Address Pair



Príkaz show cdp neighbors

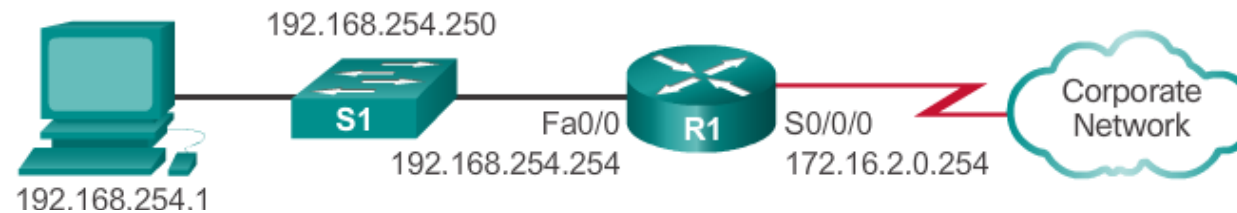
- **CDP je Cisco proprietárny protokol, ktorý funguje na linkovej vrstve**
- Dve a viac Cisco zariadení sa môžu o sebe dozvedieť aj keď konektivita na 3 vrstve neexistuje
- V základnom nastavaní je CDP **aktivované**
- **CDP vymieňa hardvérové a softvérové informácie s priamo pripojenými susedmi**
- CDP poskytuje:
 - Identifikátory zariadení
 - Zoznam adries
 - Identifikátor portov
 - Zoznam schopností
 - platformu

Príkaz show cdp neighbors

- Príkaz **show cdp neighbors**
 - **Zobrazí IP adresu susedných smerovačov**
 - Zobrazí IP adresu aj keď nie je možné spraviť na ňu ping (ping je administratívne zablokovaný)
- Príkaz **show cdp neighbors detail**
 - Detailné informácie od susedných smerovačov
 - Tento príkaz zobrazí, či niektorý z CDP susedov má chybu v konfigurácii IP adresy
 - Ak je CDP protokol aktívny vzniká bezpečnostné riziko
- Pre globálne **vypnutie CDP** sa používa príkaz **no cdp run**.
 - Pre vypnutie CDP na rozhraní sa používa príkaz **no cdp run**.

Príkaz show ip interface brief

- Príkaz **show ip interface brief** zobrazí skrátené informácie o rozhraniach na smerovači a ich stav.



```
R1# show ip interface brief
Interface      IP-Address      OK?  Method  Status      Protocol
FastEthernet0/0  192.168.254.254  YES  NVRAM   up           up
FastEthernet0/1  unassigned      YES  unset   down         down
Serial0/0/0      172.16.0.254    YES  NVRAM   up           up
Serial0/0/1      unassigned      YES  unset   administratively down
                                         down
```

```
S1# show ip interface brief
Interface      IP-Address      OK?  Method  Status      Protocol
Vlan1          192.168.254.250  YES  manual  up           up
FastEthernet0/1  unassigned      YES  unset   down         up
FastEthernet0/2  unassigned      YES  unset   up           up
FastEthernet0/3  unassigned      YES  unset   up           up
```



UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics



MINISTERSTVO
ŠKOLSTVA, VEDY,
VÝSKUMU A ŠPORTU
SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť
Priestor pre Vaše otázky

*Doma treba prečítať kapitulu 11
a spraviť si kvíz 11 z portálu Netacad*



Networking
Academy