Sítě WAN a routery

1.1.1. Úvod do sítí WAN

WAN (Wide area network) sa používajú na preklenutie veľkých geografických oblastí ako štát, provincia alebo krajina.

Hlavné charakteristiky:

- prepájajú zariadenia na veľké geografické oblasti
- využívajú služby telekomunikačných spoločností
- používajú sériové pripojenia rôznych typov na dosiahnutie požadovanej šírky pásma cez rozsiahlejšiu
geografickú oblasť

Rozdiely medzi LAN a WAN:

- LAN prepájajú pracovné stanice, terminály, periféria a iné zariadenia v budove alebo malej geografickej
oblasti
- WAN vytvárajú prepojenie cez veľkú geografickú oblasť, pracujú na **fyzickej a dátovej** vrstve OSI

Zariadenia použité vo WAN:

- routre, poskytujú prepojenie sietí a WAN port
- switche vo WAN prepájajú dáta, hlas alebo video
- modemy obsahujú rozhranie pre hlasové služby
- komunikačné servery koncentrujú prichádzajúcu a odchádzajúcu užívateľskú komunikáciu

WAN štandardy definujú a spravujú:

- International Telecommunication Union-Telecommunication Standardization Sector (ITU-T)
- International Organization for Standardization (ISO)
- Internet Engineering Task Force (IETF)
- Electronic Industries Association (EIA)

1.1.2. Routery v sítích WAN

Rútre sú špecifickým tipom počítačov, obsahujú rovnaké základné komponenty ako štandartné PC ale vykonávajú špecifickú funkciu.

Rúre obsahujú: CPU, pamäť, systémovú zbernicu a rôzne vstupno – výstupné rozhrania

Funkcia: prepájajú siete, určujú najlepšiu cestu dát

Internetwork Operating System software (IOS) – operačný systém routra, slúži na spustenie konfiguračných súborov.

Konfiguračné súbory: obsahujú všetky informácie pre nastavenie a použitie, povolenie smerovania a smerovacie protokoly v smerovači

Hlavné vnútorné komponenty smerovača:

- random access memory (RAM)
- nonvolatile random-access memory (NVRAM)
- flash memory
- read-only memory (ROM)
- rozhrania

Funkcie RAM: prac. priestor pre OS, smerovacie tabuľky, bežiaca konfigurácia, vyrovnávacie pamäte

Funkcie NVRAM: štartujúca konfigurácia (vypnutím sa nestratí)

Funkcie FLASH: kompletný IOS, aktualizovateľný, aj viacero verzií súčasne

Funkcie ROM: diagnostické a zavádzacie (bootstrap) programy (ROM monitor), zvyčajne obsahuje aj

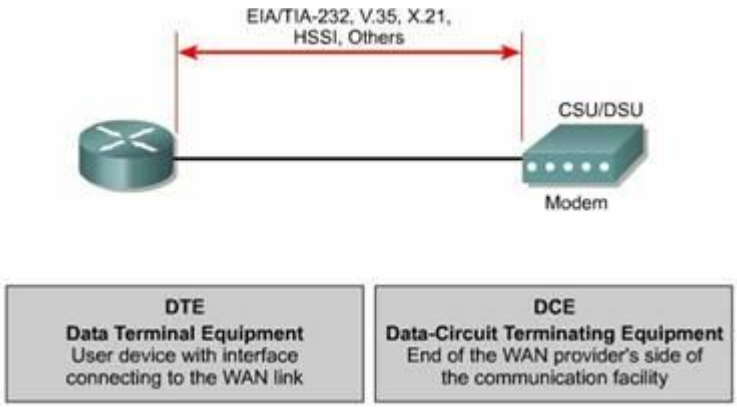
obmedzenú verziu IOS, nedá sa aktualizovať
Zbernice: system bus a CPU bus

1.1.3. Router v LAN a WAN

Router má WAN aj LAN rozhranie. Pracujú na 3 vrstve OSI modelu, vytvárajú rozhodnutia na základe sieťovej adresy. Funkciou routra je stavba smerovacích tabuliek, výmena sieťových informácií z ostatnými routrami, určovanie najlepšej cesty pri prepínaní rámca

1.1.4 Úloha routra vo WAN

Štandartné protokoly používané vo WAN na 1. a 2. vrstve sú iné ako v LAN na rovnakej vrstve. Fyzická vrstva popisuje prepojenie medzi data terminal equipment (DTE) a data circuit-terminating equipment (DCE). Spravidla DCE je poskytovateľ služby a DTE je zariadenie ktoré sa pripája.



Jednou z úloh routra vo WAN je smerovanie paketov na 3. vrstve, ale to je tiež aj v LAN. Keď router používa fyzickú a dátovú vrstvu a protokoly, ktoré sú spojené s WAN, pracuje ako WAN zariadenie. Primárnou úlohou routra je poskytovať prepojenie na a medzi rôznymi WAN fyzickými a dátovými štandardami.

WAN fyzické a dátové protokoly a štandardy:

- EIA/TIA-232
- EIA/TIA-449
- V.24
- V.35
- X.21
- G.703
- EIA-530
- ISDN
- T1, T3, E1, and E3
- xDSL
- SONET (OC-3, OC-12, OC-48, OC-192)

WAN dátové protokoly a štandardy:

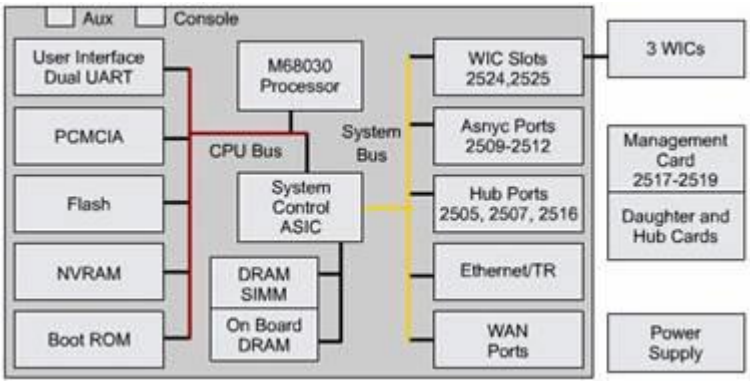
- High-level data link control (HDLC)
- Frame Relay
- Point-to-Point Protocol (PPP)
- Synchronous Data Link Control (SDLC)
- Serial Line Internet Protocol (SLIP)
- X.25
- ATM
- LAPB

- LAPD
- LAPF

DTE je schopné komunikovať len s DCE zariadení, DCE určuje hodiny, koncové zariadenie u poskytovateľa.

1.2.1. Vnútorné komponenty routra

Komponenty routra:



- CPU – The Central Processing Unit, vykonáva inštrukcie v operačnom systéme, je to mikroprocesor, väčšie routre môžu mať viac CPU
- RAM – Random-access memory, je používaná pre smerovacie tabuľky, rýchla prepínacia keš, smerovacia konfigurácia, vyrovnávacia pamäť pre IOS, pri výpadku napájania sa zmaže, rozširuje sa cez DIMMs.
- FLASH, pre uloženie CISCO IOS imidžu. Router normálne načítava IOS z FLASH. Imidž môže byť obnovený nahraním novšej verzie. Imidž môže byť komprimovaný alebo nekomprimovaný. Pridaním alebo nahradením flešky cez SIMMs alebo PCMCIA kartou sa dá rozšíriť veľkosť flešky.
- NVRAM – Nonvolatile random-access memory, používaná na uloženie spúšťacej konfigurácie, vypnutím sa nemaže.
- Zbernice, delíme na systémovú a CPU zbernicu. Systémová slúži na komunikáciu medzi CPU a rozhraniami, rozširujúcimi slotmi. CPU zbernica komunikuje z pamäťami.
- ROM – Read-only memory, je použitá pre trvalé uloženie spúšťacieho diagnostického kódu. Hlavná úloha je hardverová diagnostika počas spustenia routra a nahranie IOS z flešky do RAM. Niektoré routre majú obmedzenú verziu IOS, ktorá môže byť použitá ako alternatívny bútovací zdroj. ROM sa nedá zmazať.

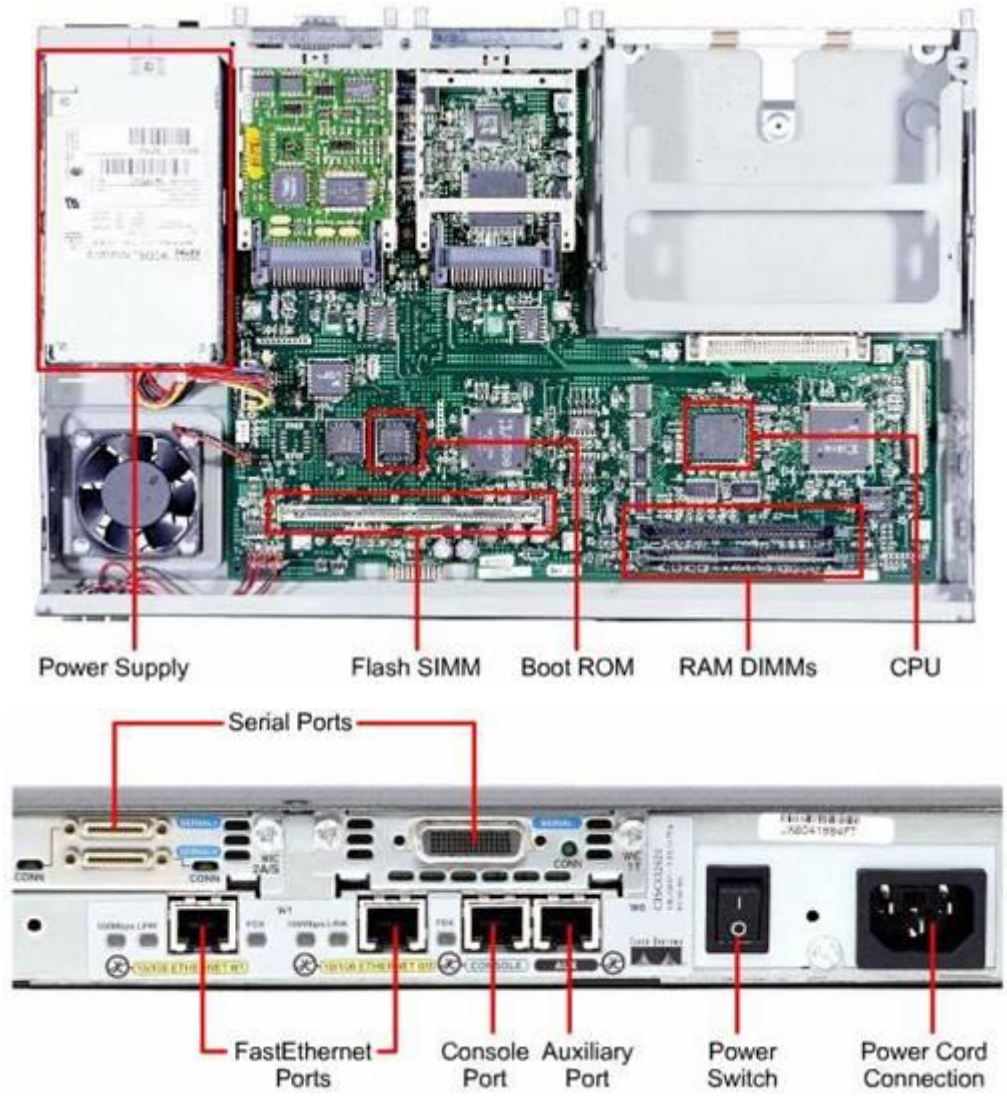
Upgrade sa robí výmenou čipu.

- rozhrania,

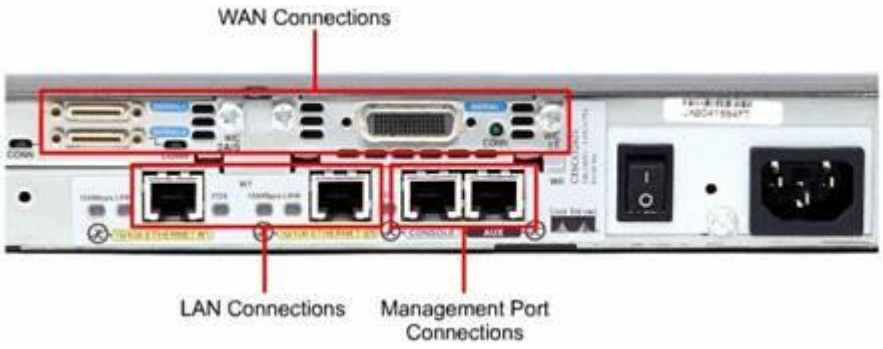
LAN, Ethernet alebo Token-Ring
WAN, sériové, ISDN, integrované CSU, LAN aj WAN rozhrania buď pevná konfigurácia alebo modulárne
Console/AUX, sériový, na inicializáciu routra, (AUX pre pripojenie modemu)

- napájací zdroj, napája všetky komponenty routra

1.2.2. Fyzická charakteristika routra



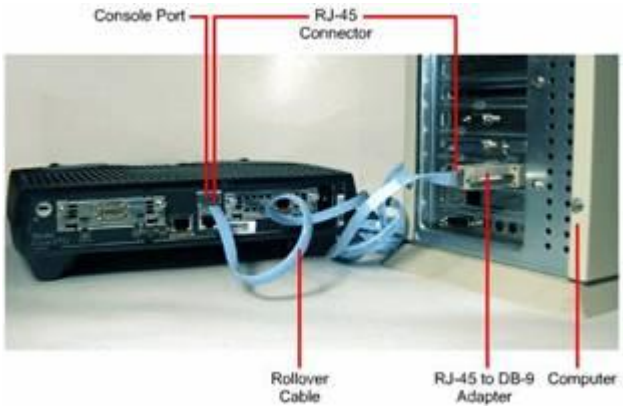
1.2.3. Vonkajšie konektory routra



Sú používané 3 typy konektorov:

- **LAN** rozhranie umožňuje routru pripojenie do LAN siete tipu Ethernet, Token Ring alebo ATM
- **WAN** umožňuje cez servisného provajdera pripojenie do vzdialenej siete alebo na internet, komunikácia je sériová
- **manažovatelné porty**, delíme ich na conzolové a auxilliary porty. Sú asynchrónne EIA 232.

1.2.4. Pripojenie smerovača ku konzole



Manažovatelné porty:

- konzolový port, doporučený pre inicializáciu, pripája sa na sériový port PC
- AUX, pre diaľkovú správu cez modem

Nie sú navrhnuté ako sieťové porty, jeden z nich je potrebný pre inicializačnú konfiguráciu routra. Po prvom zapnutí nie je router nakonfigurovaný, preto sa pripája cez RS232 ASCII terminál alebo počítačový terminál. Konzolový port môže byť tiež použitý pri riešení problémov, router vypisuje všetky úkony pri spúšťaní, prípadne pri zmene hesla ku správe.

1.2.5. Pripojenie konzolového rozhrania

Pripojenie je realizované cez konzolový port, rollover kábel zložená z konektora RJ45 a DB9.
Terminál musí podporovať VT100 emuláciu
Pripojenie na router:

1. Zkonfigurovanie terminálu:
   - Prideliť com port
   - 9600 baud
   - 8 dátových bitov
   - žiadna parita
   - 1 stop bit
   - žiadne riadenie toku
2. pripojiť konektor RJ45 rollover kábla do routra na konzolový port
3. pripojiť konektor DB9 adaptéra na rollover kábel
4. zapojiť DB9 adaptér do PC

1.2.6. Pripojenia LAN rozhrania

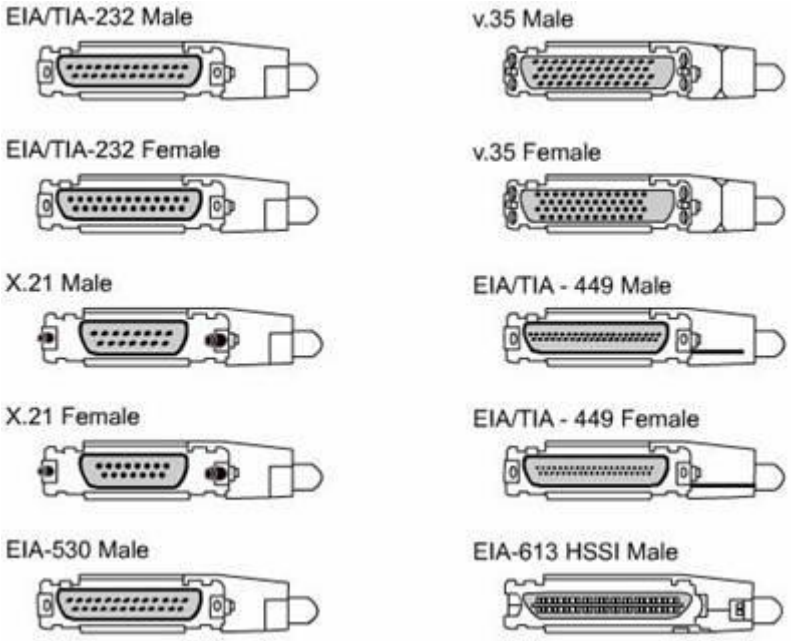
Router komunikuje z LAN cez HUB alebo SWITCH. Na pripojenie sa používa priami kábel. V niektorých tipoch Ethernetového prepojenie je router pripojený priamo na PC alebo na iný router, vtedy sa používa prekrížený kábel.

!!!Na pripojenie použi správny konektor!!!
Na lepšie rozpoznanie portov CISCO zaviedol farebné rozlíšenie:

Port or Connection	Port Type	Color	Connected To	Cable
Ethernet	RJ-45	yellow	Ethernet hub or Ethernet switch	Straight-through
T1/E1 WAN	RJ-48C/ CA81A	light green	T1 or E1 network	RJ-48 T1
Console	8 pin	light blue	Computer com port	Rollover
AUX	8 pin	black	Modem	Rollover
BRI S/T	RJ-48C/ CA81A	orange	NT1 device or private integrated network exchange (PINX)	RJ-48
BRI U WAN	RJ-49C/ CA11A	orange	ISDN network	RJ-49
Token	UTP, STP	purple	Token Ring device	RJ-45 Token Ring cable

1.2.7. Pripojenie WAN rozhrania

WAN pripojenie je realizované na veľké vzdialenosti cez rôzne typy technológií. Tieto WAN služby sú vždy
prenajaté od servisného poskytovateľa.
Pre každý tip WAN služby, customer premises equipment (CPE), často router, je data terminal equipment (DTE). Na poskytovateľa služieb sa pripájame cez DTE, často je top mode.
DCE sériové rozhrania:



Úvod do routerů

2.1.1. Účel Cisco IOS softvéru

Bez operačného systému nemá router žiadne schopnosti. Služby Cisco IOS:

1. základné smerovacie a prepínacie funkcie
2. spoľahlivý a bezpečný prístup na sieťové zdroje
3. sieťová škálovatelnosť

2.1.2. Užívateľské rozhranie routra

Cisco IOS používa command-line interface (CLI) ako tradičné konzolové prostredie. Prostredie je dostupné cez niekoľko metód:

- cez konzolu

Používa sa nízkorýchlostné sériové pripojenie priamo z PC na router. Druhou možnosťou je pripojenie cez AUX pomocou modemu

- cez Telnet

jedno z rozhraní musí byť zkonfigurované z IP adresou, a virtuálne pripojenie musí mať nakonfigurované meno/heslo

2.1.3. Módy užívateľského rozhrania routra

Každý mód je indikovaný iným promptom a umožňuje len príkazy pridelené tomuto módu. Command executive (EXEC) – IOS poskytuje command interpreter service, ten schvaľuje a vykonáva príkazy
Rozdelenie EXEC podľa bezpečnosti:

- užívateľský EXEC mód

umožňuje len základný počet monitorovacích príkazov, len prehliadanie, identifikácia: ">"

- privilegovaný EXEC mód, tiež známi ako povolený mód

umožňuje vykonávať všetky príkazy routra, je možné nastaviť heslo pre vstup do tohto módu, používa sa pre konfigurácia, identifikácia: "#" Enable – príkaz na prechod z užívateľského módu do privilegovaného, prejaví sa zmenou promptu Exit – ukončenie privilegovaného módu ? – výpis príkazov pre jednotlivé módy, alebo help k príkazu

2.1.4. Funkce Cisco IOS softwaru

Cisco pracuje na vývoji různych typoů IOSu, každý je určený len pre dané zariadenie, avšak zachováva základnú konfiguračnú štruktúru.
Názov IOS softvéru (súboru) sa skladá z 3 častí:

1. platforma na ktorej image beží
2. špeciálne funkcie, ktoré podporuje imidž
3. kde image beží, či je komprimovaný

Pri výbere nového IOS image je dôležitá kompatibilita s FLASH a RAM routra.
Show version – kontrola aktuálneho image a dostupnej pamäte RAM, zobrazí verziu, to čo pri štarte, či bútuje z
ROM alebo FLESH
príklad: … <output omitted>… cisco 1721 (68380) processor (revision C) with 3584K/512K bytes of memory.
c4500-i-mz_112-16.bin

1. platforma c4500
2. internetový i
3. komprimovaný mz
4. verzia 11.2(16)

Show flash – zistenie kapacity flash pamäte, verifikácia dostatku miesta pre nový IOS
príklad: ...15998976 bytes total (10889728 bytes free)
Cisco Software Advisor – interaktívny nástroj na výber špeciálnych IOS funkcií.

2.1.5. Prevádzka Cisco IOS softvéru

Módy Cisco IOS:

1. ROM monitor výpis spúšťacieho procesu, základné funkcie a diagnostika, identifikácia ">". Používa sa na obnovu pri systémovom zlyhaní a pri obnove hesla, do tohto módu je možné vstúpiť len cez konzolový port
2. Boot ROM je zavedená len obmedzená verzia IOS z ROM, je určený na výmenu Cisco IOS uloženej vo FLASH, identifikácia "(boot)>"
3. Cisco IOS normálna prevádzka routra, IOS je zavadený z FLASH, identifikácia "Router>"

Štartovací proces normálne nahráva do RAM jeden z týchto prostredí na základe nastavenie konfiguračného
registra.
Copy tftp flash – príkaz na obnovu IOS uloženom na TFTP do FLASH v routri.

2.2.1. Inicializačné spustenie CISCO routra

Po zapnutí routra sa spustí nahrávanie bootstrap, nasleduje operačný systém a konfiguračný súbor. Ak nevie
nájsť konfiguračný súbor, zavedie sa setup mód.
Primárne cieľom je spustiť smerovacie operácie. Na zavedenie tohto cieľu musí :

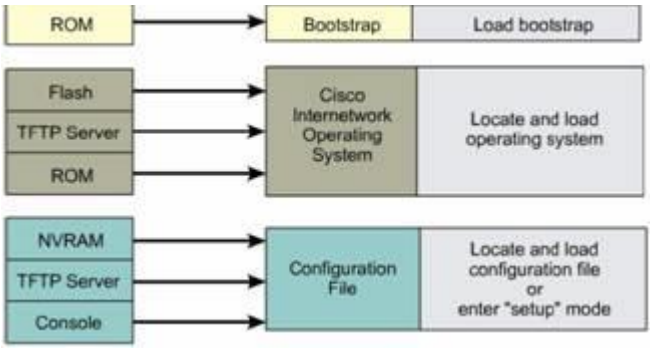
1. uistiť sa o funkčnosti hardwaru a otestovať ho
2. nájsť a spustiť Cisco IOS software

- nájsť a aplikovať konfiguračný súbor alebo sprístupniť setup mode

Po zapnutí routra sa vykonáva power-on self test (POST), diagnostika základných funkcií CPU, pamäte a sieťových portov. Po tomto teste sa prevádza software inicializácie. Po POST prebieha:

- spustí sa bootstrap, súbor inštrukcií testujúcich hardware a inicializácia IOS

1. IOS môže byť na viacerých miestach, rozhoduje sa na základe konfiguračného registru, môže biť vo FLASH alebo nahraný zo siete. V konfiguračnom súbore je udaná cesta a meno image.
2. nahranie image IOS, po funkčnom zavedení sa vypisujú pripravený hardware a software na konzole terminálu
3. konfiguračný súbor je nahraný z NVRAM do RAM, spúšťa sa smerovací proces
4. ak nebola nájdená konfigurácia v NVRAM IOS hľadá konfiguráciu na TFTF serveri. Ak nie je nájdená konfiguračný súbor, spustí sa setup dialóg.



V setup móde sa nás pýta, či nahrať default konfiguráciu. Ukončenie sprievodcu je možné cez **Ctrl+C**

2.2.2. Indikačné LED routra

LED indikujú aktivitu na príslušnom rozhraní. Ak zelená OK LED svieti, systém je zavedený správne

2.2.3. Skúmanie inicializačného bootup routra

Po 1. spustení nie je v NVRAN žiadna konfiguračný súbor, preto je zobrazené hlásenie "NVRAM invalid, possibly due to write erase", router musí biť skonfigurovaný a konfigurácia uložená do NVRAM konfiguračného
súboru.
Konfiguračný register je od výroby nastavený na 0x2102, konfiguračný súbor sa nahráva z FLASH pamäte.
Z výpisu na konzole je možné určiť:

1. bootstrap verziu a IOS verziu
2. model routra
3. procesor
4. hodnota celkovej pamäte
5. počet a typ rozhraní
6. veľkosť NVRAM a FLASH pamäte

2.2.4. Zavedenie HyperTerminal spojenia

Všetky Cisco routre obsahujú asynchrónny TIA/EIA-232 sériový konzolový port (RJ-45). Na vytvorenie spojenia sú potrebné káble a adaptér. Konzolový terminál je ASCII terminál alebo PC, na ktorom je spustený emulátor terminálu napr. HyperTerminal. Postup pripojenia:

1. pripojíme jeden koniec rollover kábla k routru, druhý pripojíme cez redukciu BD-9 alebo 25 k COM1 / 2.
2. skonfigurujeme terminál 9600baud, 8 data bits, bez parity, 1 stop bit, a bez kontroly toku

2.2.5. Prihlásenie do routra

Na konfiguráciu je potrebné mať prístup cez terminál alebo cez diaľkový prístup, pri vstupe sa užívateľ musí
prihlásiť.
Úrovne bezpečnosti:

- Užívateľský EXEC mód, nie je dovolená konfigurácia routra, lem prezeranie, príkazy sú podmožinou privilegovaného módu
- Privilegovaný EXEC mód, umožňuje zmeny s konfigurácii

Na sprístupnenie privilegovaného módu sa zadáva príkaz **Enable**, môže byť vyžadované heslo. Zmena promptu z > na #
enable password slabo **enable secret**: nastavenie hesla do privilegovaného módu **disable** alebo **exit** alebo **Ctrl+Z** návrat do užívateľského módu

2.2.6. Kláves help v routri CLI

? – výpis príkazov podľa módu, pri zobrazení "--More--" sú príkazy ešte aj na ďalšej obrazovke, medzerníkom
prejdeme o obrazovku ďalej, o riadok ďalej cez Enter.
Na prístup do privilegovaného módu je stačí zadať **ena**, čo je skratka **enable**.
Príklad využitia helpu na nastavení hodím:

1. predpokladáme, že nepoznáme správny príkaz, zadáme **?**, medzi príkazmi je **clock**
2. potrebujete zistiť syntax, zadáme **clock ?**
3. clock set 15:38:50 12 jan 2004 a potvrdíme Enster Šípkami hore dole sa vypisuje história, je nastavený na 20, dá sa meniť

2.2.7. Rozšírené editovacie príkazy

Klávesové skratky v rozšírenom editovacom móde:

terminal no editing – zakazuje rozšírený editovací mód, treba zadať v privilegovanom móde ($) – indikuje, že riadok bol posunutú doľava Ctrl-Z, príkaz na návrat z konfiguračného módu

Command	Description
Ctrl-A	Moves to the beginning of the command line
Esc-B	Moves back one word
Ctrl-B (or right arow)	Moves back one character
Ctrl-E	Moves to the end of the command line
Ctrl-F(or left arrow)	Moves forward one character
Esc-F	Moves forward one word

2.2.8 História príkazového riadku routra

Otázky spojené s históriou príkazového riadku:

1. nastavenie veľkosti buferu histórie
2. znovavyvolanie príkazu
3. zakázanie histórie príkazového riadku **terminal history size** alebo **the history size** nastavenie veľkosti histórie príkazov, maximum je 256

Command	Description
Ctrl-P or up arrow key	Recalls last (previous) command
Ctrl-N or down arrow key	Recalls most recent command
Router>**show history**	Shows command buffer
Router>**terminal history size number-of-lines**	Sets the command history buffer size*
Router>**terminal no editing**	Disables advanced editing features
Router>**terminal editing**	Re-enables advanced editing
<Tab>	Completes the entry

2.2.9. Odstraňovanie chýb v príkazovom riadku

Stávajú sa preklepom, užívateľské rozhranie indikuje chybu a označí ju (^). Príklad: Router#clock set 13:32:00 23 February 93
^ zle vložený vstup je označený strieškou. Chybu môžeme jednoducho odhaliť cez help, na mieste kde nastala chyba vložíme ? Príklad: Router#clock set 13:32:00 23 February ? <1993-2035> Year
Router#clock set 13:32:00 23 February

2.2.10. Príkaz show version

Zobrazí informácie o Cisco IOS software verzii bežiacej na routri. Obsahuje nasledujúce:

1. IOS verzia a popisné informácie
2. Bootstrap ROM verzia
3. Boot ROM verzia
4. Doba, ako dlho router beží
5. posledná metóda reštartu
6. image systémového súboru a jeho umiestnenie
7. platformu routra
8. nastavenie konfiguračného registra

Konfigurovanie routra

3.1.1. CLI príkazové módy

Všetky konfiguračné zmeny Cisco routra sa robia v globálnom konfiguračnom móde. Sprístupnenie GKM: cez skratku conf t alebo Router#**configure terminal** Router(config)# globálny konfiguračný mód GKM obsahuje ešte ďalšie módy:

1. interface more Router(config-if)#
2. line mode Router(config-line)#
3. router mode Router(config-router)#
4. subitinterface mode Router(config-subif)#
5. controller mode Router(config-controller)# sú aj ďalšie

Všetky zmeny, ktoré sa vykonávajú v jednotlivých módoch, sú aplikované len na rozhranie alebo proces, ktorý danému módu zodpovedá.
exit – návrat zo špecifického konfiguračného módu do globálneho konfiguračného módu **Ctrl+Z** – ukončenie konfiguračného módu a návrat do privilegovaného

3.1.2. Konfigurovanie mena routra

Zmena mena routra: Router(config)#**hostname** Tokyo Tokyo(config)#

3.1.3. Konfigurovanie hesiel routra

Obmedzujú prístup do routra, mali by byť vždy nastavené pre virtual terminal lines a conzole lines. Taktiež
slúžia na autentifikáciu do privilegovaného módu.
Heslo pre konzolu:
Router(config)#**line console** 0
Router(config-line)#login
Router(config-line)#**password** <password>
Heslo pre virtual terminal lines (VTY):
Router(config)#**line vty** 0
Router(config-line)#login
Router(config-line)#**password** <password>
Využitie hesla pre virtual terminal lines (VTY) pri službe telnet, pre tento prístup **musí byť** nastavené heslo.

Počet VTY je typicky 0-4
enable password a **enable secret –** nastavujú heslo do privilegovaného módu, doporučuje sa enable secret,
pretože je kryptované. Príklad:
Router(config)#enable password <password>
Router(config)#enable secret <password>
service password-encryption – zakryptuje všetky nekryptované heslá
show running-config alebo **show startup-config –** zobrazenie konfigurácie, zobrazuje aj heslá

3.1.4. Skúmanie príkazu show

show interfaces – zobrazí všetky štatistiky pre všetky rozhrania routra, ak nás zaujíma špecifické rozhranie,
stačí zadať: Router#show interfaces serial 0/1
show controllers serial – zobrazí špecifické informácie o rozhraní hardwaru
show clock – zobrazí čas nastavený v routri
show hosts – zobrazí kešovaný list hostiteľského mena a adresy
show users – zobrazí všetkých pripojených užívateľov k routru
show history – zobrazí históriu príkazov
show flash – zobrazí informáciu o flash pamäti a ktoré IOS súbory sú v nej uložené
show version – zobrazí informáciu o routri a IOS, ktorý beží v RAM
show ARP – zobrazí ARP tabuľku routra
show protocol – zobrazí globálne a rozhraňové informácie týkajúce sa všetkých konfigurovaných L3 protokolov
show startup-configuration – zobrazí uloženú konfiguráciu v NVRAM
show running-configuration – zobrazí konfiguráciu aktuálne bežiacu v RAM

3.1.5. Konfigurovanie sériového rozhrania

Môže byť konfigurované cez konzolu alebo cez virtual terminal line. Postup:

1. vstup do globálneho konfiguračného mód
2. vstup do módu rozhrania
3. uviesť adresu pre rozhranie a masku
4. nastaviť clock rate ak ide o DCE
5. zapnúť rozhranie

Každé pripojené sériové rozhranie musí mať IP adresu a masku siete. Príklad: Router(config)#interface serial 0/0 Router(config-if)#ip address <ip address> <netmask>
Sériové rozhranie vyžaduje hodinový signál na kontrolu časovania komunikácie. DCE zariadenie treba nastaviť na nastavenie poskytovania hodinového signálu.
clock rate – spúšťa časovač a definuje rýchlosť: 1200, 2400, 9600, 19200, 38400, 56000, 64000, 72000, 125000, 148000, 500000, 800000, 1000000, 1300000, 2000000, alebo 4000000. **no shutdown** – zapína rozhranie **shutdown** – vypína rozhranie príklad využitia príkazov pri rýchlosti 56000:
Router(config)#interface serial 0/0 Router(config-if)#clock rate 56000 Router(config-if)#no shutdown

3.1.6. Vykonávanie adds, presun a zmeny

Ak konfigurácia vyžaduje konfiguráciu, treba prejsť do potrebného módu, napríklad ak potrebujem zapnúť

nejaké rozhranie, spustím globálny konfiguračný mód, vstúpim do módu daného rozhrania a spustím ho cez
príkaz **no shutdown**.
show running-config – overenie aktuálnej konfigurácie, je čítaná z RAM
Postup, ak zmeny nerobia požadované:

1. Zrušenie/zmena konfiguračného príkazu v príslušnom konfiguračnom móde!!!–no príkaz(no ip address, no shutdown)
2. obnovenie konfigurácie z NVRAM
3. skopírovať konfiguráciu cez TFTP

- **erase startup-config** – odstráni spúšťaciu konfiguráciu z NVRAM, po reštarte prejsť do setup módu
  copy running-config startup-config – uloží bežiacu konfiguráciu do VNRAM

3.1.7. Konfigurovanie Ethernetového rozhrania

Je možné konfigurovať cez konzolu alebo cez virtual terminal line. Každé Ethernetové rozhranie musí mať IP a masku. Postup konfigurácie:

1. spustiť globálny konfiguračný mód
2. spustiť konfiguračné mód rozhrania
3. špecifikovať IP a masku
4. povoliť rozhranie Rozhranie je prednastavené ako vypnuté, spustíme ho cez **no shutdown,** vypneme cez **shutdown.**

3.2.1. Dôležité o konfiguračných štandardoch

Štandard je súbor noriem alebo procedúr, ktoré sú značne používané alebo oficiálne špecifikované, napomáhajú redukovať sieťovú zložitosť.

3.2.2. Popis rozhrania

Popis rozhrania pomáha sieťovým užívateľom zapamätať si špecifické informácie o rozhraní. Popis je mienený ako popis o rozhraní, nemá však žiadny efekt na funkcie.

```
Tokyo(config)#interface e 0

Tokyo(config-if)#description Engineering LAN, Bldg. 18
```

3.2.3. Konfigurovanie popisu

Postup:

1. spustím globálny konfiguračný mód: **configure terminal**
2. spustiť mód špecifického rozhrania, napr. Ethernet0: **interface ethernet 0**
3. vložím príkaz nasledovaný popisom, ktorý bude zobrazený: **command description** XYZ Network Building18
4. ukončím interface mód cez **Ctrl+Z**

5. uložím konfiguračné zmeny: **copy running-config startup-config**

3.2.4. Uvítacia správa pri prihlasovaní na smerovač

Správa sa zobrazí pri prihlásení. Je možné zadať ľubovolný text.

3.2.5. Konfigurovanie správy dňa (MOTD)

Zobrazuje sa na všetkých pripojených termináloch.

V GKM sa zadá: banner motd #<text> #

3.2.6. Preklad hostiteľských mien

V tomto procese sa asociujú symbolické mená z IP adresou.

```
Router(config)#ip host Auckland 172.16.32.1
Router(config)#ip host Beirut 192.168.53.1
Router(config)#ip host Capetown 192.168.89.1
Router(config)#ip host Denver 10.202.8.1
```

Pri smerovačoch je vhodné uviesť IP adresy všetkých rozhraní.

Host table – list hostiteľských mien a ich asociovaných IP adries, routre si ju udržiavajú v keši, čím sa zvyšuje rýchlosť prevodu mien na adresy. Príklad konfigurácie:

3.2.7. Konfigurovanie hostiteľskej tabuľky

Postup:

1. vstup do GKM v routri
2. zadám príkaz **ip host** meno routra a všetky IP adresy asociované z rozhraním routra
3. pokračovať v zadávaní, až sú všetky routre na sieti vložené
4. uložiť konfiguráciu do NVRAM V príkazoch telnet/ping/trace je možné použiť symbolické meno namiesto IP adresy

3.2.8. Konfigurovanie záloh a dokumentácie

Typické úlohy pri správe:

1. Porovnávanie bežiacich konfiguračných súborov
2. Ukladanie konfiguračných súborov na serveri
3. Aktualizácie programového vybavenia Môžu biť uložené na sieťový server, TFTP server alebo na disk uloženom na bezpečnom mieste

3.2.9. Kopírovanie, editovanie, vkladanie konfigurácie

1. Uloženie zálohy konfigurácie na TFTP

copy running-config tftp – uloženie aktuálnej konfigurácie na TFTP server, postup:

1. zadám príkaz **copy running-config tftp**
2. zadám IP adresu TFTP servera
3. zadám meno konfiguračného súboru
4. potvrdím voľbu yes

2. Obnovenie zo zálohy na TFTP

copy tftp running-config – príkaz na obnovu konfiguračného súboru zo zálohy, postup:

```
Router#copy running-config tftp
Remote host []? 131.108.2.155
Name of configuration file to write[tokyo-config]?tokyo.2
Write file tokyo.2 to 131.108.2.155? [confirm] y
Writing tokyo.2 !!!!!! [OK]
```

zadám príkaz **copy tftp running-config**

na PC si spustím TFTP, zadám cestu k image a spustím server, v termináli zadám IP PC, kde beží TFTP zadám meno konfiguračného súboru a potvrdím cez yes

```
Router#copy tftp running-config
Host or network configuration file [host]?
IP address of remote host [255.255.255.255]? 131.108.2.155
Name of configuration file [Router-config]? tokyo.2
Configure using tokyo.2 from 131.108.2.155? [confirm] y
Booting tokyo.2 from 131.108.2.155:!! [OK-874/16000 bytes]
tokyo#
```

Zisťovanie d'alších zariadení

4.1.1. Úvod do CDP

Cisco Discovery Protocol (CDP) – pracuje na 2 vrstve, prepája nižšie vrstvy protokolu s vyššími. Používa sa na získanie informácií o susedných zariadeniach bez ohľadu na konfigurovaný sieťový protokol, je možné získať typ pripojeného zariadenia, rozhranie, ktorým je pripojené a model zariadenia. Pracuje na všetkých zariadenia CISCO a len s Cisco zariadeniami.

Pri spustení zariadenia sa automaticky spúšťa aj CDP, každé zariadenie konfigurované pre CDP vysiela periodicky správu, obsahuje dobu platnosti.

4.1.2. Informácia získaná s CDP

Primárna funkcia CDP je získavanie informácií o všetkých priamo prepojených susedných CISCO zariadeniach. **show cdp neighbors :** zobrazí všetkých priamo pripojených susedov Pomocou tohto príkazu je možné zistiť:

1. Device ID (meno vzdialeného zariadenia)
2. Local Interface (cez ktoré naše lokálne rozhranie je dostupné)
3. Holdtime(kedy vyprší platnosť informácie–implicitne sú CDP pakety vysielané každých 60 s. a platnosť informácie je 180 s.)
4. Capability(smerovač, prepínač, …)
5. Platform(konkrétna platforma zariadenia)
6. Port ID (port na vzdialenom zariadení ,ktorý nám vyslal informáciu)

7. VTP Management Domain Name (CDPv2only)
8. Native VLAN (CDPv2only)
9. Full/Half-Duplex (CDPv2only)

4.1.3. Realizovanie, monitorovanie a údržba CDP

cdp run – globálne povolenie CDP na routri, býva defaultne povolené, doporučuje sa však zakázať kvôli bezpečnosti, GKM
cdp enable – povolenie CDP na určitom rozhraní, interface konfiguračí mód
clear cdp counters – vynuluje CDP počítadlá, užívateľský mód
show cdp – zobrazí interval medzi prenosom Z CDP zariadení, počet sekúnd CDP správy platnej na danom porte a verziu správy, privilegovaný mód
show cdp entry „meno zariadenia"- zobrazí informáciu o špecifickom susedovi, zobrazenie môže byť limitované protokolom alebo verziou správy, rozlišujú sa malé a veľké písmená v názve, ak je *, zobrazia sa všetky zariadenia, privilegovaný mód
show cdp interface „typ a číslo" – zobrazí informáciu o rozhraní, na ktorom je CDP povolené, privilegovaný mód
show cdp neighbors - zoznam susedov zistený cez CDP, privilegovaný mód
show cdp traffic - overenie, či som skutočne čosi poslal, užívateľský mód

4.1.4. Vytváranie sieťovej mapy okolia

Hoci sú CDP rámce malé, poskytujú detailné informácie o pripojených CISCO susedných zariadeniach. Pomocou týchto informácií môžeme vytvoriť mapu pripojených zariadení. Cez telnet je možné prihlásenie na tieto zariadenia a cez príkaz **show cdp neighbors** zobraziť susedné zariadenia.

4.1.5. Zakázanie CDP

no CDP run – v GKM, zakáže CDP pre všetky individuálne rozhrania
Vo verzii 10.3 a vyššie je CDP povolené, je možné posielať a prijímať CDP informácie.
no CDP enable command – na zakázanie CDP na určitom rozhraní, ak CDP bolo povolené, interface KM

4.1.6. Odstraňovanie porúch CDP

clear cdp table – zmaže informácie o susedoch z CDP tabuľky
clear cdp counters – vynulovanie počítadiel o prijatý / vyslaných CDP paketoch
show cdp traffic – zobrazí CDP počítadlá, obsahujú počet prijatých a odoslaných CDP paketov a kontrolný súčet
show debugging – zobrazí informáciu o tipoch ladenia, ktoré sú povolené
debug cdp adjacency – CDP susedné informácie
debug cdp events – CDP udalosti
debug cdp ip – CDP IP informácie
debug cdp packets – informácie súvisiace s paketom
cdp timer – špecifikuje, ako často Cisco IOS posiela CDP aktualizácie
cdp holdtime – určuje dobu platnosti poslaného paketu
show cdp – zobrazí globálne CDP informácie obsahujúce časovač a dobu platnosti

4.2.1. Telnet

Telnet je virtual terminal protocol, ktorý je súčasťou TCP/IP, pacuje na aplikačnej vrstve. **Umožňuje pripojenia na vzdialeného hosta**. Je IOS EXEC príkaz slúžiaci **na overenie aplikačnej vrstvy** medzi zdrojom a cieľom. Router umožňuje viacnásobné simultánne sedenie, max 5.

4.2.2. Zabezpečenie a overenie pripojenia Telnet

connect alebo **telnet** - nadviazanie spojenia medzi routrami, príklad: telnet paris, v privileg. e.m.
exit alebo **logout –** ukončenie spojenia, spojenie sa ukončí po **10** minútach nečinnosti
Je možné zadávať príkazy cez symbolické názvy, ale musí byť nakonfigurovaná tabuľka hostmane.
Ping adresa – overenie spojenia na sieťovej vrstve
Problémy: ak sa nedá pripojiť na vzdialený router cez telnet, treba overiť adresu, symbolické meno, alebo vty
nie je nakonfigurovaný.
Odstránenie problémov: skúsiť ping

4.2.3. Odpojenie a prerušenie Telnetového sedenia

Ukončenie sedenia : na prázdnom riadku stlačím **Enter, disconnect**
show sessions: zobrazí všetky momentálne bežiace telnet sedenia
Prerušenie sedenia: vrátim sa na svoj router: ctrl+shift+6, pustím a stlačím X
Návrat do sessions: na prázdnom riadku stlačím Enter, ak mám viac sessions zadám jej číslo, napr.: 2 a Enter

4.2.4. Zdokonalené telnet operácie

Môže byť niekoľko naraz spustených sedení.
session limit command – limit počtu sedení, routre rady 2500 majú max. počet sedení 5
Medzi sedeniami je možné prepínať, popis v predch. kapitole.

4.2.5. Alternatívne testy pripojenia

Veľa sieťových protokolov podporuje echo protokol, využívaný na testovanie smerovania paketov.
ping – pošle paket a čaká odpoveď od hosta, na overenie dosiahnutia alebo funkcionality hosta, vykonáva sa
privilegovanom móde, pacuje na L3 **traceroute** command – Zistenie konektivity na L3, využíva TTL IP paketov, vypíše, kadiaľ to lezie, testuje
každý krok počas cesty, vykonáva sa privilegovanom móde, prerušenie cez **Ctrl-Shift-6**

4.2.6. Riešenie problémov IP adresovania

Využívame 3 príkazy:

1. ping, využitý ICMP protokol na overenie hardwarového prepojenia a IP adries na sieťovej vrstve
2. telnet, overuje aplikačnú vrstvu medzi zdrojom a cieľom
3. traceroute, umožňuje lokalizáciu zlyhania v ceste zo zdroja do cieľa

Cisco IOS softver

Cisco router nevie pracovať bez IOS. Každý CISCO router má vopred danú boot-up sekvenciu pre nahrávanie IOS

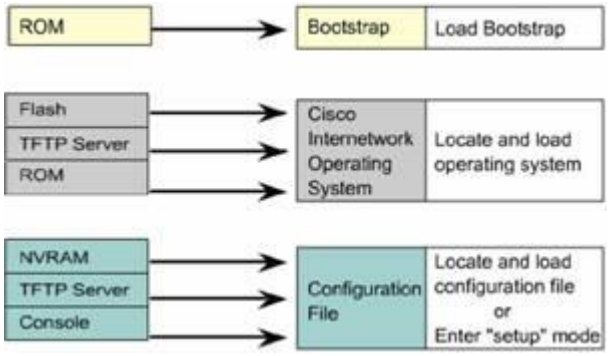
5.1.1. Postupnosť sekvencií pri zapnutí routra

Hlavnou úlohou routra je zabezpečiť smerovacie
operácie.

Pri spustení routra sa vykonávajú nasledovné operácie:

1. otestovanie hardwaru routra
2. nájdenie a nahranie Cisco IOS softwaru
3. nájdenie a aplikovanie konfiguračných pravidiel

5.1.2. Ako Cisco zariadenia hľadajú a nahrávajú IOS



Predvolený zdroj Cisco IOS je závislý na hardwarovej platforme, ale zvyčajne sa najskôr pozrie do boot system
commands uloženom v NVRAM.
Nastavenia konfiguračného registra umožňuje nasledovné alternatívy:

1. príkaz v boot system commands, určí postupnosť hľadania zdroja
2. pri neprítomnosti príkazu v boot system commands, využije sa IOS vo FLASH pamäti
3. ak je FLASH pamäť prázdna, router sa pokúsi použiť TFTP na nahranie imige zo siete. Router využije hodnoty z konfiguračného registra na určenie názvu súboru image uloženom na sieťovom serveri.

5.1.3. Využitie boot system príkazu

Sekvencia hľadania Cisco IOS:

1. Flash pamäť, výhoda zavedenia Cisco IOS z FLASH je, že nie je citlivá na zlyhanie siete, počas nahrávania image z TFTP príklad: v GKM, **boot system flash** meno_súboru
2. sieťový server, ak je image poškodený počas prenosu, systém nebude zavedený príklad: v GKM, **boot system tftp** meno_súboru ip adresa
3. ROM, ak FLASH je poškodená alebo zlyhalo zavedenie z TFTP, je to obmedzený verzia, býva taká stará, ako ROM, teda od kúpy alebo výmeny. príklad: v GKM, **boot system rom**

copy running-config startup-config – ukladá konfiguráciu z RAM do NVRAM

5.1.4. Konfiguračný register

Udáva v akom poradí hľadá systémové zavádzacie informácie.
config-register – v GKM, zmena konfiguračného registra, zadáva sa hexa číslo, je to 16 bitový register v NVRAM, dolné 4 bity hovoria o spôsobe bootovania
show version – v poslednom riadku je zobrazený aktuálny stav konfiguračného registra
Smernice pre zmenu konfiguračného registra:

Value	Description
0xnnn0	Use ROM monitor mode (manually boot using the b command)
0xnnn1	Automatically boot from ROM (default if router has no Flash)
0xnnn2 to 0xnnnF	Examine NVRAM for boot system commands (0xnnn2 is the default if the router has Flash)

1. vstup do ROM monitor módu, nastavím KR na **0xnnn0**, v ROM monitore zavediem IOS manuálne použitím príkazu **b**

2. na nakonfigurovanie na automatické bootovanie nastavím KR na **0xnnn1**
3. na nakonfigurovanie systému, aby nahliadol do boot system commands v NVRAM, zmením KR z 0xnnn2 na **0xnnnF**

Defautl býva využitie boot system commands v NVRAM

5.1.5. Problémy pri zlyhaní bootu IOS

Zlyhanie zavedenia IOS môže spôsobiť:

1. konfiguračný súbor chýba, alebo je nesprávny údaj v boot system
2. nesprávne nastavená hodnota konfiguračného registra
3. poškodený flash image
4. hardwarové zlyhanie

Pri bootovaní routra sa číta hodnota v boot system v konfiguračnom súbore, práve táto hodnota môže donútiť router nabootovať z iného image uloženého vo FLASH. **show running-config** – v hornej časti je možné vyčítať údaj z boot system **show version** - v dolnej časti aktuálny stav konfiguračného registra
Zobrazenie chybových správ pri poškodenom image:
open: read error...requested 0x4 bytes, got 0x0 trouble reading device magic number boot: cannot open "flash:"
boot: cannot determine first file name on device "flash:" Ak sa nezobrazí žiadna chybová správa a nezavedie sa IOS, ide pravdepodobne o hardwarovú chybu.

5.2.1. Prehliadanie Cisco IOS systému

Na prácu routrov a prepínačov je potrebný software, ten vyžaduje OS a konfiguráciu.
Cisco Internetwork Operating System (IOS) – obsahujú ho skoro všetky Cisco zariadenia, umožňuje hardwaru
prepínacie a smerovacie funkcie. Býva veľký niekoľko MB.
Konfiguračný súbor alebo konfig: určujú, či zariadenie bude svič alebo smerovač. Veľkosť niekoľko 100 bitov
Definované funkcie v konfigu:

1. IP adresa rozhrania
2. smerovací protokol
3. sieť Umiestnenie jednotlivých softwarových komponentov:
4. RAM, bežiaca konfigurácia
5. NVRAM, startup konfiguration
6. FLASH, IOS image, môže sa upgradovať, môže obsahovať viac IOS

Vo veľa architektúrach routrov je kopírovaný IOS z FLASH do RAM, konfiguračný súbor sa pri bootovaní tiež zavádza do RAM. Config:
running, uložený v RAM po nabootovaní startup, uložený v NVRAM

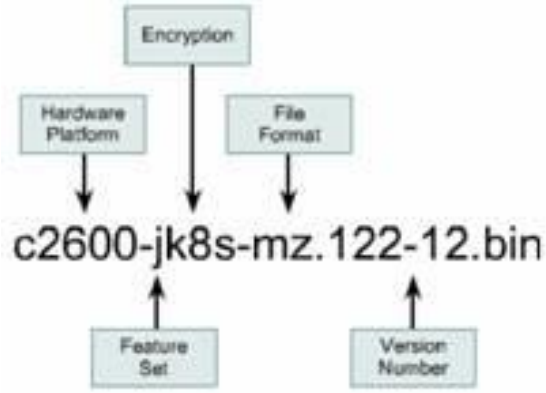
Prefix	Description
bootflash:	Bootflash memory
flash:	Flash memory. This prefix is available on all platforms. For platforms that do not have a device named flash, the prefix flash: is aliased to slot0:. Therefore, the prefix flash: can be used to refer to the main flash memory storage area on all platforms.
flh:	Flash load helper log files
ftp:	File Transfer Protocol (FTP) network server
nvram:	NVRAM
rcp:	Remote copy protocol (rcp) network server
Slot0:	First Personal Computer Memory Card International Association (PCMCIA) flash memory card
Slot1:	Second PCMCIA flash memory card
system:	Contains the system memory, including the running configuration
Tftp:	TFTP network server

IFS používajú URL konvenciu na špecifikovanie súboru na sieťovom zariadení a na sieti. Určujú umiestnenie konfiguračných súborov. Od verzie 12 existuje unifikované rozhranie Cisco IOS File System(IFS) pre všetky súborové systémy, ktoré smerovač podporuje:

5.2.2. Názvová konvencia súborov s Cisco IOS

c2600 - js - 1 . 121-3.bin

121-3 - typ verzie(12.13)
1 - súborový formát(nekomprimovaný)
js - (podnikový s rozšírenou kapacitou)
c2600 - hardwarová platforma (2600)
- na odlíšenie rôznych verzií



5.2.3. Správa konfiguračného súboru cez TFTP
Proces zálohy bežiacej konfigurácie na TFTP:

1. copy running-config tftp - zadám príkaz na skopírovanie bežiacej kon. na tftp v privilegovanom EM
2. zadám IP adresu tftp servera
3. pridelím meno alebo akceptujem preddefinované meno
4. potvrdím yes

proces obnovy konfigurácie z TFTP servera:

1. copy tftp running-config, kopíruje z tftp do bežiacej konfigurácie
2. zadám IP adresu TFTP servera, odkiaľ budem obnovovať súbor
3. zadám meno, alebo akceptujem predefinované
4. potvrdím meno konf. súboru a dresu servera

5.2.4. Správa konfiguračný súborov použitím copy a paste

Inou cestou zálohy je kopírovanie zachytenie príkazu show running-config. Je tom možné zrealizovať v terminálovej sesion kopírovaním textu a uložením do súboru. Postup zachytenia textu v hyperterminály:

1. v menu transfer vyberieme položku capture text
2. špecifikujeme meno súboru, kam sa daný text bude zachytávať
3. zachytávanie aktivujeme tlačidlom štart
4. zobrazenie konfigurácie zrealizujeme cez príkaz: show running-config
5. stlačíme medzerník pri zobrazení výzvy: more

- ukončenie zachytávania po ukončení výpisu konfigurácie zrealizujeme cez Transfer/Capture Text/Stop

Po ukončení zachytávanie je nutné odstrániť prebytočný text. Komentáre sa pridávajú za znak „!".
Text je možné editovať napríklad cez notepad. Odstránime nasledujúce riadky:

1. show running-config
2. Building configuration...
3. Current configuration:
4. - More -
5. Any lines that appear after the word "End"

Na konci každej sekcie rozhrania pridám príkaz no shutdown, len u zapnutých zariadení. Uložím súbor.
Obnova konfigurácie:
- Pred obnovou konfigurácie je potrebné zmazať starú a reštartovať router.
erase startup-config - zmazanie aktuálnej konfigurácie **reload** - reštartovanie routra

1. spustím GKM
2. V hyperterminály Transfer > Send Text File, vyberiem meno súboru s uloženou konfiguráciou
3. pozorujem, či nenastali chyby
4. opustím GKM
5. Uložím bežiacu konfiguráciu

5.2.5. Správa IOS image cez TFTP

Pred zmenou IOS je vhodné urobiť zálohu, napríklad na server s bežiacim TFTP. **copy flash tftp -** záloha IOS na TFTP server v privilegovanom EM.

Zmena IOS cez príkaz **copy tftp flash**

1. router vyžiada IP adresu servera, zadanie mena súboru
2. router môže zmazať FLASH, vypísaním erase flash a čaká na potvrdenie, väčšinou pri nedostatočne veľkej FLESH pre nový image
3. pri mazaní flash sa zobrazuje písmenko „e"
4. pri kopírovaní IOS image sa zobrazujú „!", po úspešnom prenose sa ešte nový IOS verifikuje.

5.2.6. Správa obrazu IOS použitím Xmodemu.

Ak je IOS poškodený, je ho možné obnoviť v **ROMmon mode**. Identifikácia: rommon 1 >
Prvým krokom je identifikovať, prečo nebol IOS zavedený z FLASH, môže byť poškodený alebo môže chýbať.

dir flash – preskúmanie obsahu hlash
Ak sa zdá, že image je OK, skúsime ho zaviesť
boot flash: command – nahratie IOS od pamäte, príklad: rommon 1>boot flash:c2600-is-mz.121-5
Ak sa IOS zavedie, je potrebné preskúmať, prečo sa router spustil v ROMmom móde. Postup overovania:

1. príkazom: **show version**, overím konfiguračný register
2. ak je KR ok, overím konfiguráciu pri spúšťaní cez príkaz: **show startup-config,** či router nie je boot system command navolený rommon mód.
3. ak router nenabootoval z image, je potrebné nahrať nový obraz IOS, je ho možné obnoviť cez TFTP alebo cez Xmodem

Postup nahrávanie cez Xmodem v ROMmon:
- potrebujeme súbor s IOS a terminálový program, napr. HyperTerminal, je možné použiť prednadstavenú
rýchlosť 9600 bps, prípadne zvýšiť na 115200 bps na zvýšenie rýchlosti
confreg – zmena konzolovej rýchlosti v ROMmod móde, router sa začne vypytovať, pri zobrazení otázky: "change console baud rate? y/n [n]:", zadám Y a na nasledujúcom riadku zvolí, požadovanú rýchlosť
xmodem -c image_file_name – v ROMmode obnova IOS software z PC. **c** – kontrola CRC
- teraz potrebujem v terminálovej emulácii spustiť Xmodem prenos. V Hyperterminály zadám: Transfer >
Send File, zadám správny súbor, vyberiem Xmodem ako protokol a spustím štart prenosu.
- po úspešnom prenose treba ešte nastaviť rýchlosť prenosu a nastaviť konfiguračný register na 0x2102
config-register 0x2102 – v privilegovanom EM, zmena konfiguračného registra

5.2.7. Prostredie premenných

Obnova IOS môže byť realizovaná aj cez TFTP, čo je rýchlejšie, ako cez Xmodem. Najskôr je nutné skonfigurovať router cez príkaz **set** a potom zadať príkaz **tftpdnld** na zrealizovanie prenosu. V ROMmon móde sú veľmi limitované funkcie, nie je žiadny konfiguračný súbor, nie sú pridelené žiadne IP a TFTP prenos funguje len na 1. LAN porte. Postup konfigurácie rozhrania: **!!!VŠETKO VEĽKÝM!!!**

```
rommon 10>set
IP_ADDRESS=10.0.0.1
IP_SUBNET_MASK=255.255.255.0
DEFAULT_GATEWAY=10.0.0.254
TFTP_SERVER=192.168.1.1
TFTP_FILE=GAD/original_2003_Jan_22/c2600-i-mz.121-5
```

tftpdnld – spustenie downloadu image.
Po úspešnom downloade treba router reštartnúť zadaním „**i**"

5.2.8. Verifikácia súborového systému

show version - vypíše odkiaľ a z ktorého súboru bol zavedený IOS – Celkovú kapacitu a voľné bajty vo flash – Obsah konfiguračného registra
showflash – vypíše celkovú kapacitu, voľné a obsadené bajty vo flash – súbory + ich veľkosti, ktoré sú uložené vo flash

Smerovanie a smerovacie protokoly

6.1.1. Úvod do smerovania

Smerovanie je proces, ktorý router používa na presun paketov do cieľovej siete, vytvára rozhodnutie na základe cieľovej IP adresy, z paketu určí jeho ďalší smer, ktorý ho dovedie do cieľa. Postupy učenia routra na určenie správneho smerovania:

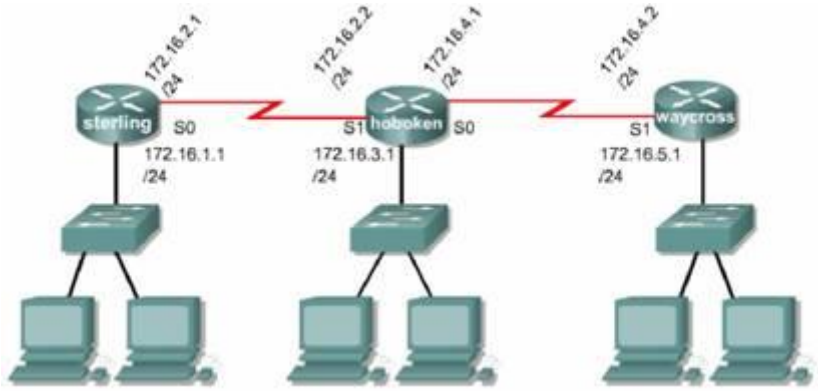
1. dynamické smerovanie, smerovacie informácie sa učí od iných routrov, pri veľkých sieťach
2. statické smerovanie, sieťový administrátori konfigurujú ručne informácie o smerovaní, malé siete

6.1.2. Statické smerovanie

Smerovacie operácie:

```
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s0
                   command  destination net  subnet mask   outgoing
                                                           interface
```

1. sieťový administrátori konfigurujú routre
2. router inštaluje smer smerovania v smerovacej tabuľke
3. pakety sú smerované použitím statických pravidiel **ip route** – v GKM, definuje statické smerovanie routra



Administrátor Hoboken potrebuje prístup k sieťam 172.16.1.0/24 a k 172.16.5.0/24. Siete, ktoré sú priamo pripojené **netreba** definovať. Môže to zrealizovať dvoma spôsobmi:
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 172.16.2.1
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 172.16.2.1

alebo
Hoboken(config)#ip route 172.16.1.0 255.255.255.0 s1
Hoboken(config)#ip route 172.16.5.0 255.255.255.0 s0

K tomuto príkazu je možné pridať ďalší parameter, **administratívna vzdialenosť** v rozsahu od 0-255, udáva mieru spoľahlivosti, čím menšie číslo, tým je spoľahlivosť vyššia. Default je 1. Vďaka tejto možnosti môžu byť v tabuľke dva rovnaké údaje, ale AV je iná, router dá prednosť záznamu s nižšou AV.

6.1.4. Konfigurácia prednastaveného smerovania

Default route je použitá na smerovanie paketov, ktorý sa nezhoduje ani z jedným smerom v smerovacej tabuľke. Umožňuje udržiavať menšie smerovacie tabuľky (internet), lebo nie všetky smery v sieti musia byť v nich explicitne uvedené

ip route 0.0.0.0 0.0.0.0 nasledujúci smerovač alebo rozhranie k nemu : v GKM, smerovanie všetkých paketov, ktoré nie sú v smerovacej tabuľke cez špecifikované rozhranie alebo IP adresa nasledujúceho smerovača.

Postup konfigurácie:

1. spustiť GKM
2. zadať príkaz **ip route 0.0.0.0 0.0.0.0**, kde 0.0.0.0 0.0.0.0 sú cieľové IP a maska siete, cieľová brána je meno rozhrania alebo IP adresa nasledujúceho routra
3. odchod z GKM
4. uloženie aktuálnej konfigurácie: copy running-config startup-config

6.1.5. Overovanie konfigurácie statického smerovania

Po zadaní smerovanie treba overiť, že smerovanie je v smerovacej tabuľke a preveriť, či pracuje podľa očakávaní.

show running-config: overenie, že statické smerovanie bolo zadané správne **show ip route**: príkaz na overenie, že statické smerovanie je v smerovacej tabuľke Postup overovania:

1. show **running-config**, zadám v privilegovanom móde, vypíše aktívnu konfiguráciu
2. overím, že statické smerovanie bolo správne vložené, pri chybnom, v GKM odstránim chybný riadok a vložím správny, ku koncu sa zobrazí riadok: ip route IP maska rozhranie
3. zadám príkaz: **show ip route**
4. overím, že smerovanie, ktoré bolo vložené, je v smerovacej tabuľke

6.1.6. Odstraňovanie problémov pri konfigurácii statického smerovania

Pri zadaní **ping** na špecifickú sieť, dojde ku chybe prenosu. Na vyriešenie problému zadám **traceroute** na tú istú adresu, zobrazí sa mi, kde je problém

6.2.1. Úvod do smerovacích protokolov

Smerovacie protokoly sú odlišné od smerovaných protokolov.

Smerovací protokol slúži na dorozumievanie medzi routrami, týmto spôsobom si udržiavajú aktuálnu smerovaciu tabuľku.

Príklady smerovacích protokolov:

1. Routing Information Protocol (RIP)
2. Interior Gateway Routing Protocol (IGRP)
3. Enhanced Interior Gateway Routing Protocol (EIGRP)
4. Open Shortest Path First (OSPF)

Smerované protokoly sú využívané na priamu užívateľskú komunikáciu. Sieťovou adresou poskytujú postačujúcu informáciu, aby paket mohol byť forwardovaný z jedného hosta na druhý na základe adresovej schémy. Príkladom smerovaného protokolu sú:

1. Internet Protocol (IP)
2. Internetwork Packet Exchange (IPX)

6.2.2. Autonómne systémy

AS je kolekcia sietí pod spoločnou administráciou, zdieľajú rovnakú smerovaciu stratégiu. Vonkajší svet vníma daný AS ako jedinú entitu American Registry of Internet Numbers(ARIN), poskytovateľ pripojenia alebo administrátor prideľuje 16-bitové identifikačné číslo AS (využíva napr. protokol IGRP), ktoré ho jednoznačne odlišuje od iných AS v globálnej sieti.

6.2.3. Účel smerovacích protokolov a autonómnych systémov

Cieľom smerovacích protokolov je stavba a udržiavanie smerovacích tabuliek. Tabuľky obsahujú naučené siete a asociované porty s týmito sieťami. Routre využívajú smerovací protokol na manažovanie informácií prijatých z ostatných routrov, informácie z vlastnej konfigurácie. Smerovacie algoritmy sú základom dynamického smerovania. Pri každej zmene na sieti vzniknutej vplyvom rekonfigurácie, zlyhania, výpadku je potrebné udržiavať tabuľky v správnom stave, keď majú všetky routre aktuálny stav siete, je sieť konvergovaná.

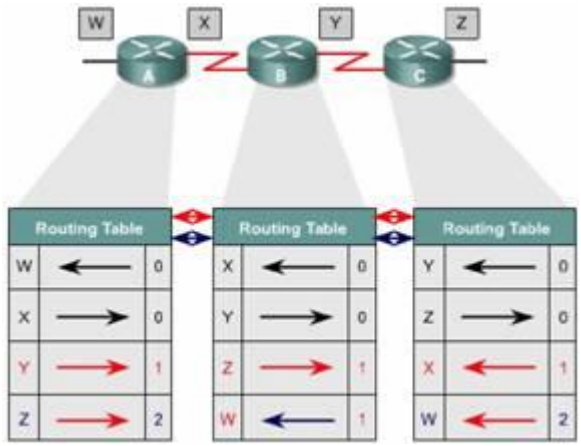
6.2.4. Identifikácia skupín smerovacích protokolov

Delenie smerovacích algoritmov:

1. distance vector, vektor vzdialeností
2. link-state, stav spoja

6.2.5. Popis distance vector smerovacieho protokolu

Distančný vektorový algoritmu prechádza periodicky kópie smerovacích tabuliek z routra na router. Je založený na smerovacom algoritme, tiež sa mu hovorí **Bellman-Ford** algoritmus. Každý router prijíma tabuľky od všetkých priamo pripojených susedov.



Príklad: routre sú zapojené do kruhu v poradí: R1<->R2<->R3<->R1:

Router R2 príme informáciu z R1, pridá distančné vektorové číslo (ako počet preskokov), ktoré zväčší distančný vektor. R2 predá túto novú smerovaciu tabuľku jeho susedom, teda R3. Takýto proces nastáva pri všetkých priamo pripojených routroch. Každý router, ktorý využíva distančné vektorové smerovanie, začína identifikáciu jeho susedov. Priamo pripojená sieť má distančný vektor **0**. Router preskúma najlepšiu cestu do cieľovej siete, založenej na informácii prijatej od každého suseda. Router A sa o inej sieti učí z informácie prijatej od routra B. Každá sieťová jednotka má v smerovacej tabuľke informáciu o vzdialenosti. Zmeny v smerovacej tabuľke nastanú pri zmene topológie. Každá smerovacia tabuľka obsahuje metriku a logickú adresu na prvý router v ceste do každej

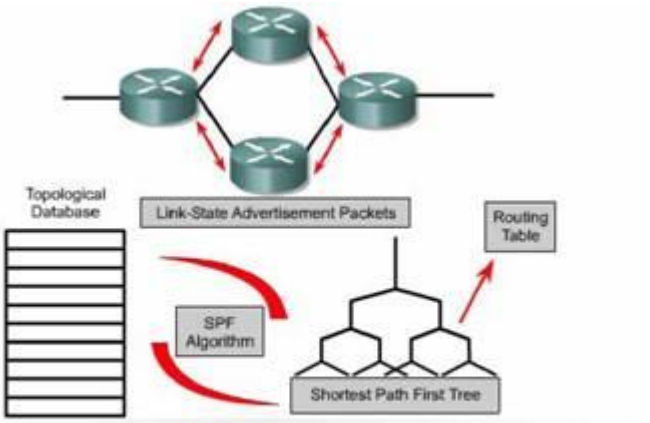
siete v tabuľke. Ak od suseda nedostane v danom čase aktualizáciu, smery od neho získané zo smer. tabuľky odstránené.

6.2.6. Popis protokolu Link-state

Druhý základný smerovací algoritmus, je tiež známi ako Dijkstras algoritmus alebo ako SPF (shortest path first) algoritmus. (algoritmus najkratšej cesty). Udržiava si komplexnú databázu topologických informácií. Tento algoritmus je schopný určiť vzdialenosť routrov a vie, ako sú prepojené.
Link-state smerovanie používa:

1. **Link-state advertisements (LSAs)** – link-state správa je malý paket poslaný medzi routre
2. **Topologická databáza** – kolekcia informácií zložená z LSAs
3. **SPF algoritmus** - shortest path first (SPF), výpočet založený na databáze založenej na SPF strome
4. **Smerovacie tabuľky** – list známych ciest a rozhraní

Sieťový prieskumný protokol pre linkové statické smerovanie sú vymieňané medzi routrami, štartujú s priamo pripojenými sieťami, pre ktoré majú priame informácie. SPF algoritmus vypočítava sieťovú dosiahnuteľnosť, router vytvára túto logickú topológiu ako strom, kde on je root, pozostávajúcich zo všetkých možných častí do každej podsiete. Router v smerovacej tabuľke zobrazí najlepšiu cestu a rozhranie do cieľovej siete. Router pri zistení zmeny topológie posiela informáciu ostatným routrom. Na zaistenie konvergencie router udržuje cestu k susedným routrom, meno routra, stav rozhrania a ohodnotenie linky k susedom. Medzi **nevýhody** patrí zaťaženie procesora, pamäťové požiadavky, spotreba šírky pásma. Periodické aktualizácie sa vysielajú menej frekventovane ako u DV, LSA pakety sa navyše vysielajú vždy při zmene topológie siete.



Routers send LSAs to their neighbors. The LSAs are used to build a topological database. The SPF algorithm is used to calculate the shortest path first tree in which the root is the individual router and then a routing table is created.

6.3.1. Určenie cesty

Funkcie pre určovanie cesty paketu z jednej linky na druhú:

1. funkcia určovania cesty, prebieha na sieťovej vrstve, na určenie najlepšej cesty sa používa smerovacia tabuľka
2. funkcia prepínania, interné funkcie, využívajú sa na zabezpečenie prechodu paketu z jedného rozhrania na druhé na rovnakom routri

Na určenie cesty router využíva sieťovú časť IP adresy.

6.3.2. Smerovacia konfigurácia

Povolenie IP smerovacieho protokolu zahŕňa nastavenie globálny a smerovacích parametrov. Globálne zahŕňajú smerovacie protokoly ako RIP, IGRP, EIGRP alebo OSPF. Hlavnou otázkou konfiguračnom smerovacom móde je indikovať IP číslo siete. Dynamické smerovanie využíva broadcast a multicast na komunikáciu s ostatnými routrami. Smerovacia metrika umožňuje routrom nájsť najlepšiu cestu v sieti alebo podsieti.

router príkaz: štart smerovacieho procesu
network príkaz: určenie rozhraní pre posielanie a prijímanie smerovacích updatov
príklad:
GAD(config)#router rip
GAD(config-router)#network 172.16.0.0

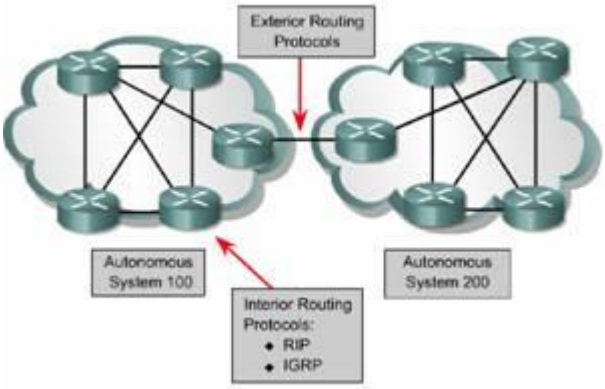
6.3.3. Smerovacie protokoly

Smerovacie protokoly:

1. RIP (Routing Information Protokol): vnútorný smerovací protokol založený na distančnom vektore, na určenie cesty využíva počet hopů, maximálny počet hopov 15, potom je paket zahodený, smerovacie updaty sú vysielané cez broadcast každých 30 sekúnd
2. IGRP (Interior Gateway Routing Protocol), vyvinutý CISCOM: vnútorný smerovací protokol, distančný vektorový smerovací protokol na vytváranie metriky využíva šírku pásma, oneskorenie, záťaž, spoľahlivosť smerovacie updaty sú vysielané cez broadcast každých 90 sekúnd
3. OSPF (Open Shortest Path First): vnútorný smerovací protokol, smerovací protokol založený na stave linky na výpočet používa SPF algoritmus updaty sú poslané po topologickej zmene
4. EIGRP (Enhanced IGRP): vnútorný smerovací protokol, distance vector routing Cisco protokol, rozšírený distančný vektorový protokol dokáže vyvažovať záťaž u viacerých liniek (load balancing). Používa algoritmus DUAL na nájdenie optimálnej cesty smerovacie updaty sú vysielané cez broadcast každých 90 sekúnd, prípadne pri zmene topologie
5. BGP (Border Gateway Protocol): distančný vektorový vonkajší smerovací protokol využíva sa medzi ISP, je využívaný na smerovanie internetovej dopravy medzi autonómnymi systémami

6.2.4. Autonómny systém a IGP verzus EGP

Vnútorné smerovacie protokoly sú navrhnuté pre samostatné organizácie, kritériom je nájdenie najlepšej cesty. Vonkajší smerovací protokol je navrhnutý pre použitie medzi dvoma rozličnými sieťami, ktoré sú pod správou dvoch rozličných organizácií, využíva sa medzi poskytovateľmi internetu.



Kroky pred spustením vonkajšieho smerovacieho protokolu:

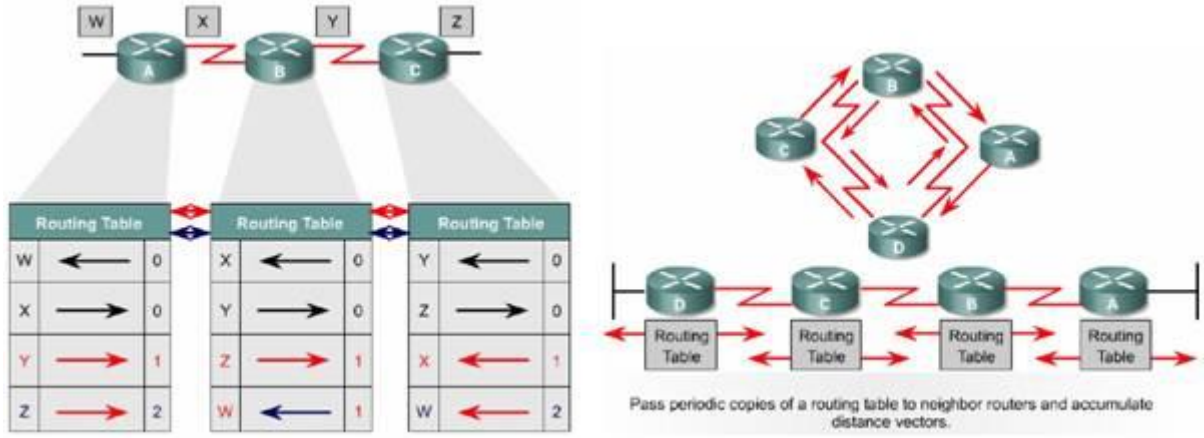
1. zoznam susedných routrov, z ktorým si vymieňa smerovacie informácie
2. zoznam priamo dosiahnuteľných sietí

- číslo autonómneho systému pre lokálny router

Vonkajší smerovací protokol musí izolovať autonómny systém. Autonómny systém má 16 bitové identifikačné číslo, ktoré je jedinečné.

6.3.6. Distance vektor

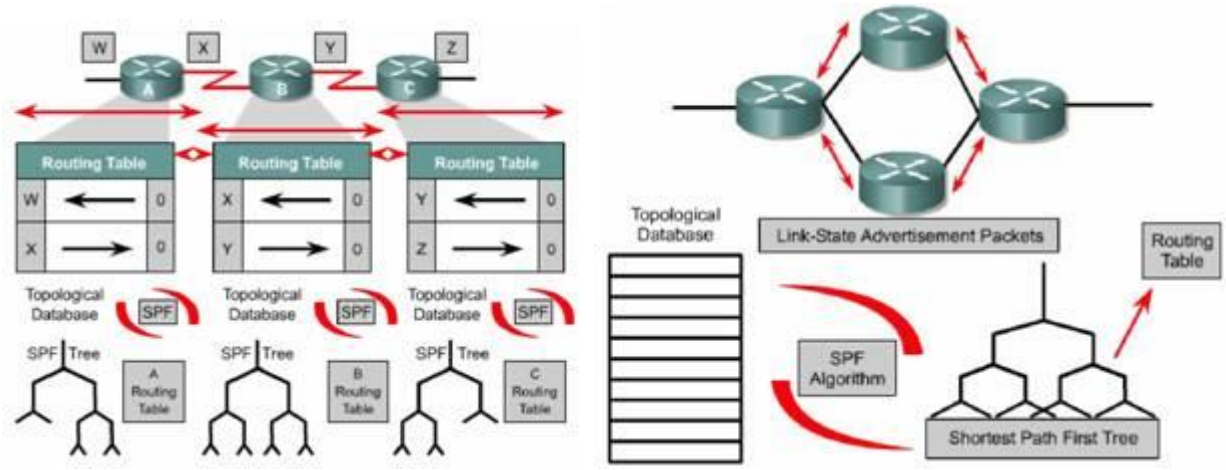
Distančný vektorový algoritmus (tiež známi ako Bellman-Ford algoritmus) vykonáva smerovanie na základe informácií poskytnutými susednými routrami. Spotrebúva menšie systémové zdroje, ale má pomalšiu konvergenciu, nie je vhodný pre veľké systémy. Vzdialenosť určuje z počtu hopov. Tento systém vyžaduje, že každý router informuje susedov o svojej smerovacej tabuľke. Medzi všeobecné smerovacie protokoly zahŕňame RIP a IGRP.



6.3.6. Link-state

Algoritmus stavu linky (tiež známi ako algoritmus kratšej cesty) posiela smerovacie informácie na všetky routre v sieti, ktoré tvoria mapu danej siete. Každý router posiela pakety svojim susedom. Paket obsahuje popis sietí alebo siete na ktoré je router pripojený. Router si zhromažďuje tieto informácie kvôli výpočtu kratšej cesty. Pri vygenerovaní smerovacej tabuľky zobrazí najlepšiu cestu. Po skonvergovaní siete už vysiela len zmeny. Konvergujú rýchlejšie ako distance smerovací protokol, ale využíva viac systémových prostriedkov. Pri zmene na sieti je vyslaný link-state advertisement (LSA) (inzerát), všetky routre si zmenia stav ve smerovacích tabuľkách. Táto metóda je jednoduchšia, spoľahlivejšia a menej náročná na šírku pásma ako distance-vector.

Príkladom je IS-IS a OSPF.



Distančné vektorové smerovacie protokoly

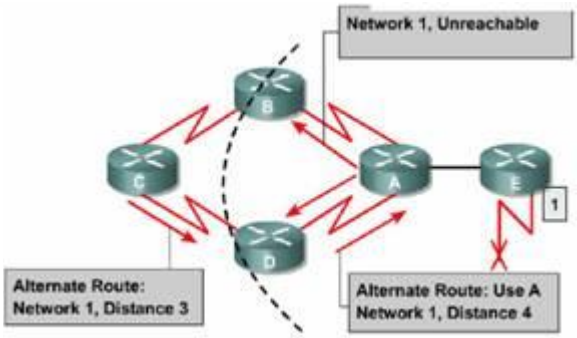
7.1.1. Vzdialenostné vektorové smerovacie aktualizácie

Aktualizácie môžu byť periodické alebo pri zmene topológie siete. Dôležité je, že smerovací protokol bude efektívne aktualizovať smerovacie tabuľky. Aktualizácie prechádzajú z routra na router. Router posiela celú svoju smerovaciu tabuľku všetkým svojim susedom. Smerovacia tabuľka obsahuje:

1. informácie o úplne ceste
2. metriku
3. logickú adresu na 1. router v ceste do každej siete obsiahnutej v tabuľke

7.1.2. Slučky v Distance Vector smerovaní

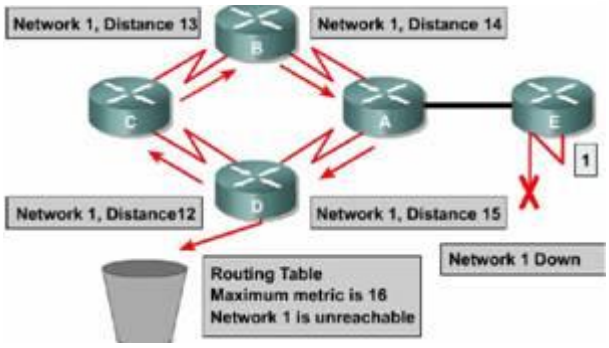
Nastávajú v neskonvergovanej sieti.



1. Pred zlyhaním siete 1 bola sieť konvergovaná. Predpokladajme, že router C ide na sieť 1 cez router B a vzdialenosť routra C na sieť 1 je 3.
2. Pri zlyhaní siete 1 router E pošle aktualizáciu na router A. Router A zastaví smerovanie na sieť 1, ale routre B, C a D pokračujú, pretože nemajú informáciu o zlyhaní. Keď router A pošle aktualizáciu, routre B a D zastavia smerovanie na sieť 1. Zatiaľ router C nevie o zlyhaní siete 1 cez router B
3. Router C pošle periodickú aktualizáciu routru D, vďaka pomalej konvergencii indikuje cestu do siete 1 cez router B. Router D zmení svoju tabuľku a pošle ju routru A, čím mu dá nesprávnu informáciu, A to pošle E a B. Všetky pakety smerované do siete 1 tak budú cykliť medzi A,B,C,D.

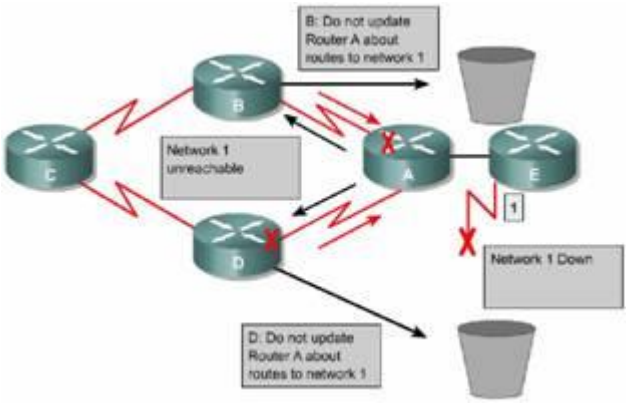
7.1.3. Definovanie maximálne počtu skokov

Nesprávne aktualizácie o sieti 1 budú pokračovať, až kým iný proces nezastaví cyklus. Na ochranu proti nekonečným slučkám bol zavedený maximálny počet prechodov cez 1 router. Počet hopov sa zväčšuje pri prechode cez každý iný router, pri maxime bude paket zahodený, sieť 1 je považovaná za nedosiahnuteľnú. Toto je samoopravný mechanizmus.



7.2.4. Eliminovanie smerovacích slučiek cez pravidlo split horizont

Jednou z možností smerovacích cyklov je keď nesprávna informácia bola poslaná na router popiera s správnu informáciu, ktorú router originálne distribuoval.

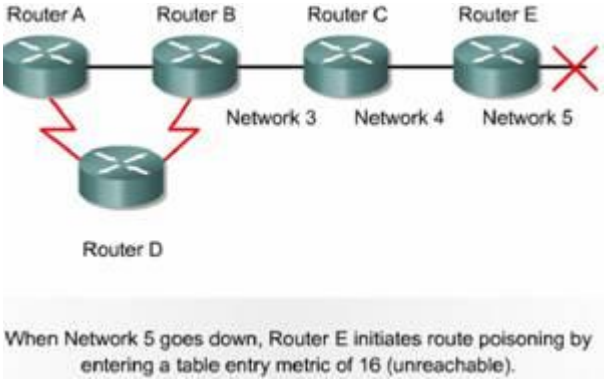


Popis problému:

1. Router A poslal na B a D, že sieť 1 je dole. Ale router C preniesol aktualizáciu na B, že sieť 1 je dostupná cez D pri 4 hopoch.
2. Router B vyvodil, že je ešte jedna cesta do siete 1, i keď z horšou metrikou. B poslal aktualizáciu A o novej ceste k sieti 1.
3. A sa rozhodlo, že do siete 1 sa dostane cez B a C, C určil, že môže poslať cez D. Všetky paketu budú putovať medzi routrami.
4. Riešenie je použitie **Split-horizont**. Ak smerovacie informácie o sieti 1 prichádzajú z routra A, B a D nemôžu poslať informáciu o sieti 1 späť na A.

7.1.5. Smerovanie poisoning (spätné/otrávené)

Je používané pre rôzne distančné smerovacie protokoly, ne prekonanie veľkých smerovacích slučiek, keď sieť alebo podsieť je nedostupná. Počet hopov sa nastaví sa nastaví o 1 viac ako je maximum. Zabráni sa tým prijatiu nekorektných smerovacích informácií o danej sieti (routing loop) z iných zdrojov. Zabraňuje nekompletným updatom.

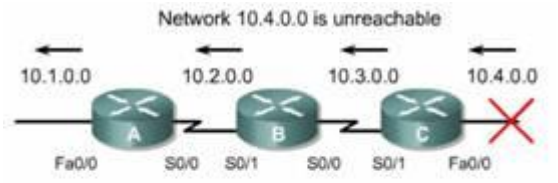


When Network 5 goes down, Router E initiates route poisoning by entering a table entry metric of 16 (unreachable).

Pri výpadku siete 5, router E inicializuje route poisoning, do tabuľky zapíše metriku 16 alebo nedosiahnuteľný. Router C nie je potom citlivý na nesprávny údaj v tabuľke. Keď router C prijme router poisoning z E, pošle na E spätnú aktualizáciu nazvanú **poisoning reverse**, toto spravia všetky routre. Pre urýchlenie konvergencie sa nečaká na čas pravidelnej aktualizácie, ale aktualizácia sa vyšle okamžite, keď smerovač zistí zmenu.

7.1.6. Zabránenie smerovacím slučkám so spúšťacími aktualizáciami

Spúšťacie aktualizácie sú vykonávané hneď po zmene v smerovacej tabuľke. Router, ktorý detekuje topologické zmeny okamžite pošle aktualizačnú správu susedom a tí ďalším susedom, táto vlna sa okamžite rozšíri. Keď smerovanie zlyhá, router čaká na exspiráciu aktualizačného časovača.
Spúšťací update routra C oznámi, že sieť 10.4.0.0 je nedostupná, po prijatí tejto informácie, router B oznám cez rozhranie S0/1, že sieť 10.4.0.0. je nedostupná. Router A pošle aktualizáciu na rozhranie Fa0/0.



With the triggered update approach, routers send messages as soon as they notice a change in their routing table.

7.1.7. Zabránenie smerovacím slučkám použitím holddown (potlačenie) časovača

Pri prijatí správy o nedostupnosti siete, router označí smerovanie ako nedostupné a nastaví holddown časovač. Ak počas tohto času príde aktualizácia od toho istého suseda o dostupnosti siete, je smerovanie povolené a časovač odstránený. Ak príchode aktualizácia od iného suseda s lepšou metrikou, je sieť

označená ako dostupná a časovač je odstránený. Ak počas HD je prijatá aktualizácia o iného suseda s horšou metrikou, aktualizácia je ignorovaná.

7.2.1. RIP smerovací protokol

je distančný vektorový smerovací protokol, pre výber cesty je použitá metrika z počtu hopov, ak je počet hopov väčší ako 15, je paket zahodený, aktualizácie sú cez broadcast každých 30 sekúnd. RIP je vo verzii 1 a 2. RIP v 2 obsahuje: schopnosť viesť rozšírenú paketovú informáciu, využíva autentifikačný mechanizmus na zabezpečenie tabuľky aktualizácií, podporuje sieťové masky.

Na zabránenie nekonečných slučiek používa počet hopov ceste, maximálny počet je 15, po prekročení tohto čísla je cieľová sieť označená ako nedostupná.

7.2.2. Konfigurácia RIP

router rip, spustenie smerovacieho protokolu RIP.
network, povie routru, na ktorom rozhraní beží RIP, definujú sa len pre priamo pripojené siete. Smerovací proces potom spojí špecifické rozhranie so sieťovou adresou a začne prijímať a vysielať RIP aktualizácie na toto rozhranie. Keď router prijme smerovacie pakety, ktoré obsahujú nové záznamy, pridá ich do svojej smerovacej tabuľky. Hodnota prijatej metriky pre cestu je zväčšená o 1, na základe tejto hodnoty sa dá určiť počet hopov. RIP routre udržiavajú vo svojich smerovacích tabuľkách len najlepšie cesty, ale môžu ich obsahovať aj viac.
ip rip triggered command, RIP posiela aktualizácie pri zmene na sieti. Je ho možná nastaviť len pre sériové rozhraní na routri. Po zmene smerovacej tabuľky, hneď začne prenášať zmeny smerovacie zmeny na iné routre.

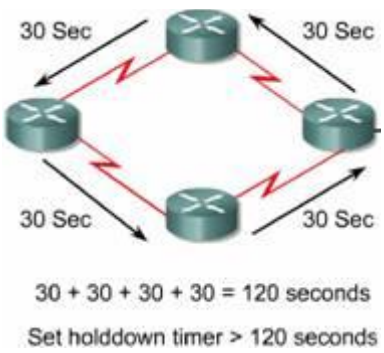
7.2.3. Použitie príkazu IP classless

Supernetroute = smer, ktorý pokrýva jednou položkou viacero smerov do podsietí; napr., ak máme podsiete 10.1.33.0/24, 10.1.34.0/24, 10.1.36.0/24, supernet môže byť napr. 10.1.0.0/16, ale aj 10.1.32.0/21 (prvých 21 bitov je u všetkých adries rovnakých)
ip classless, umožní smerovanie paketov do viacerých sietí, je dostupný od Cisco IOS Software Release 11.3 a neskorších, zadáva sa v GKM, zakázanie je robené cez **no** pred príkazom IP classless nemá žiadny vplyv na vybudovanú smerovaciu tabuľku.

7.2.4. Všeobecné konfiguračné otázky pri RIP

Routre založené na RIP sa musia spoliehať na informácie o sieti z iných routrov. Keďže je založený na vektorovom smerovacom protokole, jeho konvergencia je pomalá. Na redukovanie smerovacích slučiek a čítanie do nekonečna boli zavedené nasledujúce technológie:

1. maximálny počet hopov 15, pri prekročení je označené ako nedosiahnuteľné, zabraňuje nekonečným smerovacím slučkám
2. split-horizon, neposiela informáciu o smerovaní späť na smer odkiaľ prišla. V niektorých cieľových konfiguráciách je nutné zakázať túto funkciu **no ip split-horizon**, zakázanie split-horizon, zadáva sa pre špecifické rozhranie
3. Poison reverse



4. Holddown counters, pomáha predísť čítaniu do nekonečna, ale zväčšuje čas konvergencie. Pri RIP je default 120s. Ideálne nastavenie by malo byť väčšie, než najdlhší aktualizačný čas na sieti.

timers basic, zmena časovača, v konfigurácii smerovanie (router rip)
- Triggered updates (Okamžité aktualizácie)

update-timer –zmena aktualizačného intervalu, prednadstavený je na 30s, v konfigurácii smerovanie (router rip)
passive-interface command, zabráni posielaniu aktualizácií cez určité rozhranie
neighbor ip adress, definujem susedný router, kam budú zasielané informácie, manuálne zadanie vysielania aktualizácií, využíva sa pri sieťach, kde nie je možné vysielať broadcast, napr. v sieťach Frame Relay
version command, na definovanie posielania aktualizačných paketov, default je v1 aj v2
ip rip receive version command, definuje, aké protokolu bude spracovávať

Command	Purpose
GAD(config-if)**#ip rip receive version 1**	Configures an interface to receive RIP Version 1 packets
GAD(config-if)**#ip rip receive version 2**	Configures an interface to receive RIP Version 2 packets
GAD(config-if)**#ip rip receive version 1 2**	Configures an interface to receive RIP Version 1 or 2 packets

Použití pro vysílání:

GAD(config-if)#ip rip send version 1 - konfiguruje interface k odesílání paketů RIP Ver. 1

GAD(config-if)#ip rip send version 2 - konfiguruje interface k odesílání paketů RIP Ver. 2

GAD(confiq-if)#ip rip send version 1 2 - konfiguruje interface k odesílání paketů RIP Ver. 1 nebo 2

7.2.5. Overovanie konfigurácie RIP

Na overovanie RIP je možné použiť niekoľko príkazov. **show ip protocols**, zobrazí smerovacie protokoly Body na overenie funkčnosti:

1. či je RIP nakonfigurovaný
2. či sú na správnych rozhrania prijímané a vysielané RIP aktualizácie
3. aké siete oznamuje

show ip route, overenie, či sú v smerovacej tabuľke záznamy získané cez RIP, v smerovacej tabuľke je RIP označené písmenom **R**.

7.2.6. Otázky pri riešení problémov pri RIP

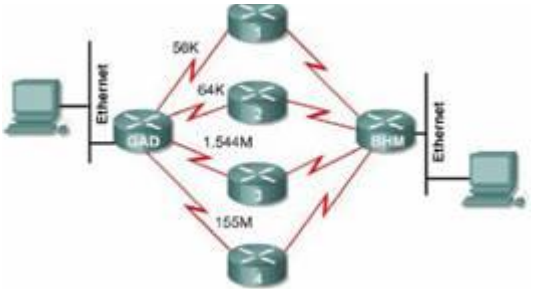
debug ip rip, zobrazuje RIP smerovacie aktualizácie, ako sú posielané a prijímané. Problémy môžu biť odhalené napríklad zo zlej metriky, ak je väčšia ako 15, ide o nedosiahnuteľnú sieť. Všetko debugovanie sa vypne príkazom **undebug all**.

7.2.7. Zabránenie smerovacej aktualizácie cez rozhranie

passive interface command, zabráni routru posielať smerovacie aktualizácie cez dané rozhranie routra. Router už nevysiela informácie, ale naďalej prijíma a používa aktualizácie z hostov. Zadáva sa v konfigurácii RIP.

7.2.8. Vyváženie záťaže z RIP

Umožňuje routrom využiť výhody viacnásobnej dobrej cesty k danému cieľu. Je ich možno nadefinovať staticky (administrátorom, tento spôsob má najvyššiu metriku) alebo dynamicky cez RIP. Ak existuje do cieľovej siete viacero smerov s rovnakou metrikou, cyklicky sa využívajú všetky smery. Defaultne RIP môže takto obhospodarovať až 4 smery, dá sa nastaviť až max. 6 smerov. Pri všetkých musí byť rovnaká metrika, rovnaký počet hopov. Nevie rozlíšiť medzi šírkou pásma. Výpis smerovania je možné zobraziť cez **show ip route**, * označuje aktívne smerovanie, ktoré je použité pre nové vysielanie.

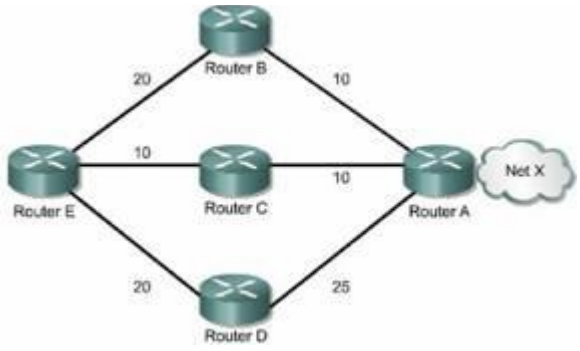


7.2.9. Vyrovnávanie záťaže cez viacnásobné cesty

Vyrovnávanie záťaže umožňuje routrom prenášať pakety do cieľa cez viac než jednu cestu. Pri učení routra je do smerovacej tabuľky poznačená cesta s nižšou administratívnou vzdialenosťou (AV). Ak má router cesty z rovnakou AV, použije vyrovnávanie záťaže, cyklicky sa využívajú všetky smery. Pri **RIP** môže použiť maximálne **6** ciest, default je 4, pri **IGRP** sú to **4** cesty. Pri **BGP** je to len **1** cesta! Router(config-router)#**maximum-paths** [number], definuje maximálny počet ciest.

Administrative Distance Route Source	Default Distance
Connected interface	0
Static route	1
Enhanced IGRP summary route	5
External BGP	20
Internal Enhanced IGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP external route	170
Internal BGP	200
Unknown	255

Proces rozhodovania routra:
E to B to A za metrika 30
E to C to A za metrika 20
E to D to A za metrika 45
Router si vyberie cestu E-C-A, má lepšiu metriky.
RIP – všetky smery s vyrovnávaním záťaže musia mať rovnaký hop count
IGRP – až 6 liniek s rôznou metrikou, vyrovnávanie záťaže sa riadi podľa bandwidth



IOS poskytuje dve metódy vyrovnávania záťaže:

– **Per destination (defaultné nastavenie**) –keď je zapnuté fast switching, pre jednu cieľovú IP adresu hosta sa používa stále rovnaký smer, pre dvoch rôznych hostov na rovnakej cieľovej sieti sa používajú rôzne smery

– **Per packet** – aj pre jednu cieľovú IP adresu hosta sa používa vyrovnávanie záťaže cez viacero smerov. Treba vypnúť na všetkých dotyčných rozhraniach fast switching: R(config-if)#**no ip route-cache .** Zistiť, či je fast switching zapnuté, možno príkazom: R#**show ip interface**

7.2.10. Integrovanie statického smerovania z RIP

Užívateľ nadefinuje cestu, kadiaľ bude prebiehať smerovanie. Je dôležité, ak Cisco IOS sa nevie naučiť smerovanie na jednotlivé ciele. Ak je paket smerovaný do siete, ktorá nie je uvedená v smerovacej tabuľke, je presmerovaný ne default route, môže ju získať od iného routra cez RIP, prípadne sa nestaví manuálne.

no ip route, v GKM zakážem statické smerovanie.

Smerovanie je potom nahradené dynamickým smerovaním, kde sa vyberá podľa administratívnej vzdialenosti (AD).

redistribute static, príkaz, ktorý zahrnie aj statické smerovanie do vysielania aktualizačných paketov, zadáva sa v router rip

7.3.1. Vlastnosti smerovacieho protokolu IGRP

Interior Gateway Protocol (IGP) je proprietálny CISCO distančný vektorový protokol. Matematicky porovnáva vzdialenosti, meranie je známe ako distančný vektor. V pravidelných intervaloch musia ich susedom posielať ich smerovacie tabuľky (každých 90s). Pri prijímaní paketu:

1. identifikujú nové ciele
2. učia sa o zlyhaní Kľúčové charakteristiky:
3. škálovatelný vo veľkých sieťach
4. flexibilita potrebná pre rozdielnu šírku pásma a oneskorenie Ako defautl metriku používa šírku pásma a oneskorenie. Metrika môže byť počítaná:
5. Najnižšieho bandwidth na celej ceste
6. Kumulovaného oneskorenia (delay) po celej ceste
7. Spoľahlivosti linky smerom k cieľovej sieti
8. Zaťaženosti linky smerom k cieľovej sieti
9. MTU celej cesty (min. MTU na celej ceste) Defaultne sa používa len **bandwidth a delay**.

7.3.2. Metrika IGRP

show ip protocols, zobrazí parametre, filtre a sieťové informácie týkajúce sa smerovacích protokolov použitých na routri. IGRP definuje hodnoty K1-K5 metriky a poskytuje informácie založené na max. počte hopov.

K1 predstavuje šírku pásma

K3 predstavuje oneskorenie

Predvolené hodnoty K1 a K3 sú 1, pokiaľ K2,4,5 sú rovné 0.

Tento spôsob metriky je **presnejší** ako pri počte hopov u RIP. Cesta z menšou metrikou je lepšia.

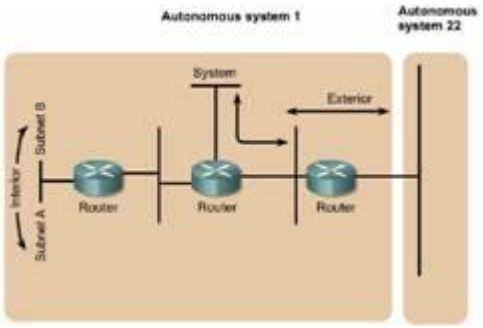
Metrika pri IGRP:

1. šírka pásma, lepšia cesta má nižšie číslo
2. oneskorenie, súčet oneskorení počas cesty
3. spoľahlivosť, spoľahlivosti linky smerom k cieľovej sieti
4. záťaž, záťaž ku na linke ku cieľu založená na bps
5. The Maximum Transmission Unit na celej ceste **show ip route**, v hranatých zátvorkách je zobrazená metrika

7.3.3. Smery IGRP

IGRP inzeruje 3 druhy trás:

- vnútorná
- systémová
- vonkajšia



Vnútorná - medzi podsieťami siete pripojenými k rozhraniu smerovača
Systémová – smerovania na siete v autonómnom systéme. Neobsahujú informáciu o podsieti, systém ich vytvorí na základe priamo pripojených sietí a z ďalších IGRP zariadení.
Vonkajšia – smerovanie mimo autonómneho systému cez gateway. Používajú sa, keď neexistuje lepší smer a cieľová sieť
nie je priamo pripojená sieť.

7.3.4. Stabilita IGRP

IGRP má počet znakov, ktoré sú navrhnuté na zlepšenie stability:

1. Holddowns
2. Split horizons
3. Poison reverse updates

Holddowns – pri výpadku routra, to susedný zistí z nedostatku aktualizácií
Split horizons – aktualizačná správa sa neposiela na miesto, odkiaľ prišla. Zabraňujú smerovacím slučkám Poison reverse updates – zabraňujú smerovacím slučkám medzi priľahlými routrami. Sú posielané, ak metrika je vyššia ako 1,1. IGRP udržiava časovače:

- aktualizačný časovač, určuje, ako často budú posielané aktualizačné správy. Default je 90s

1. invalid (neplatný) časovač, definuje, ako dlho čaká pri nedostatku aktualizácií, kým smer označí ako neplatný. Default je 270s
2. holddown časovač špecifikuje, po akom čase bude daný smer ignorovaný. Default je 280s
3. flush časovač určuje, po akom čase bude vymazaný zo smerovacej tabuľky

7.3.5. Konfigurácia IGRP

RouterA(config)#**router igrp** as-number, spustenie IGRP RouterA(config)#**no router igrp** as-number, zakázanie IGRP Autonómny systém - číslo autonómneho systému IGRP procesu **network ip**, zadávam zoznam priamo pripojených sietí

7.3.6. Prechod od RIP na IGRP

Po vytvorení IGRP v roku 1980, Cisco ako prvý skúmal smerovanie medzi vonkajšími sieťami. Určuje cestu na základe šírky pásma a oneskorenia. Konverguje rýchlejšie ako RIP, čím sa zabraňuje smerovacím slučkám. Oproti RIP nie je závislý na počte hopov, preto ho je možné použiť aj vo väčších sieťach. Postup prechodu z RIP na IGRP:

1. overiť, či existujúci smerovací protokol je skonvergovaný, show ip route
2. nakonfigurovať IGRP na routroch, v GKM: router IGRP a číslo
3. show ip protocols
4. show ip route, smery získané cez IGRP –„I", defaultná administratívna vzdialenosť IGRP je 100 (uprednostní v smerovacích tabuľkách IGRP pred RIP-om)

7.3.8. Riešenie problémov spojených z IGRP

Problémy sú spojené s nekonečnými sieťami, alebo s nesprávnym autonómnu číslo. Príkazy na riešenie problémov:

1. show ip protocols
2. show ip route
3. debug ip igrp events
4. debug ip igrp transactions
5. ping
6. traceroute

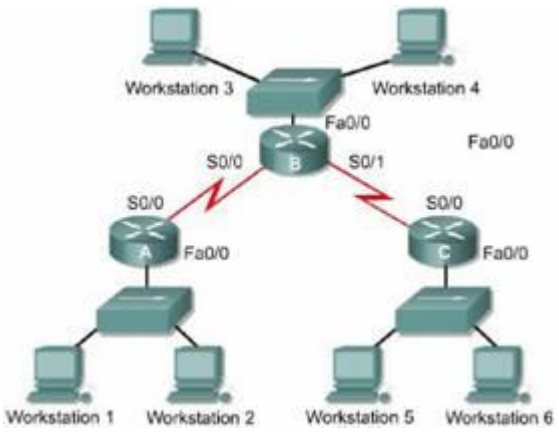
TCP IP chyby a kontrolné správy

8.1.1. Internet Control Message Protocol (ICMP)

IP je nespoľahlivá metóda pre doručovanie dát, nemá zabudovaný mechanizmu o zlyhaní prenosu. ICMP protokol je súčasťou TCP/IP, pracuje na 3. vrstve OSI modelu, slúži ako protokol pre hlásenie (odstraňovanie) chýb v rodine protokolov TCP/IP.

8.1.2. Ohlasovanie chýb a oprava chýb

ICMP je protokol slúžiaci na ohlasovanie chýb v IP protokole. Pri vyskytnutí chyby hlási tento stav na zdroj, kde bola vyvolaná. Ak pracovná stanica 1 pošle datagram na stanicu 6 a na routri C dojde k výpadku Fa0/0, router C využije ICMP protokol na poslanie správy stanici 1 o nemožnosti ho doručiť. ICMP neopravuje chyby, len ich hlási.
Pri doručení správy routru C, vie zdrojovú a cieľovú IP adresu, ale nepozná, kadiaľ šiel, preto pošle správu o zlyhaní len zdrojovému zariadeniu.



8.1.3. ICMP dodaná správa

ICMP správy sú doručované IP protokolom ako ostatné dáta.

Frame Header	Datagram Header	ICMP Header	ICMP Data
Frame Header	Datagram Header	Datagram Data Area	
Frame Header	Frame Data Area		

Výnimka: Ak vznikne pri doručovaní ICMP správy chyba, negeneruje sa nová ICMP správa upozorňujúca na chybu (aby sa nezahlcovala sieť)

8.1.4. Nedosiahnuteľná sieť

Sieťová komunikácia závisí na niektorých základných podmienkach. Najskôr zariadenia pred vysielaním a prijímaním musia mať správne nakonfigurovaný TCP/IP protokol. Musia byť pridelené ip adresy, masky siete a default gateway, ak paket opúšťa lokálnu sieť. Ďalej sú to zariadenia medzi zdrojom a cieľom. Routre obsluhujú tieto funkcie, pričom musia mať správne nastavené protokoly a rozhrania. Ak routre nemajú potrebné informácie na prenos, prípadne sú poškodené alebo rozhranie majú vypnuté je cieľová sieť nedosiahnuteľná.

An ICMP destination unreachable message is sent if:
- Host or port unreachable
- Network unreachable

8.1.5. Použitie príkazu ping na otestovanie dosiahnutelnosti cieľa.

ICMP protokol môže byť použitý na overenie dosiahnutelnosti cieľa. ICMP vyšle echo požiadavku na cieľové
zariadenie, ak zariadenie prijme požiadavku, formuluje echo odpoveď a pošle ju späť.
ping ip adresa – posiela echo požiadavku na cieľovú IP, v tomto prípade sa používajú 4 echo požiadavky.

8.1.6. Detekovanie neúmerne dlhej cesty.

Cyklenie paketov alebo príliš komplexná sieť. V oboch prípadoch paket presiahne maximálny počet hopov. Každý IP datagram nesie v hlavičke položku TTL (time-to-live). Každý prechod smerovačom znižuje TTL o 1. Keď TTL dosiahne 0, datagram je zničený a jeho odosielateľovi sa pošle správa ICMP Time exceeded. Účelom je zabrániť zahlteniu siete cyklujúcimi paketmi.

8.1.7. Správy Echo

ICMP Message Types	
0	Echo Reply
3	Destination Unreachable
4	Source Quench
5	Redirect/ Change Request
8	Echo Request
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp Request
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply

0	8	16	31
Type (0 or 8)	Code (0)	Checksum	
Identifier		Sequence Number	
Optional Data			
...			

ICMP správy majú špecifický formát. Každá správa más svoju charakteristiku, ale všetky ICMP správy začínajú s troma rovnakými poľami:

- typ, typ ICMP správy
- kód, ďalšie špecifické informácie o type
- kontrolný súčet, na overenie integrity dát

8.1.8. Správa cieľ nedosiahnuteľný

0 = net unreachable
1 = host unreachable
2 = protocol unreachable
3 = port unreachable
4 = fragmentation needed and DF set
5 = source route failed
6 = destination network unknown
7 = destination host unknown
8 = source host isolated
9 = communication with destination network administratively prohibited
10 = communication with destination host administratively prohibited
11 = network unreachable for type device
12 = host unreachable for type of service

0	8	16
Type (3)	Code (0-12)	Checksum
Unused (must be zero)		
Internet Header + First 64 Bits of Datagram		
	...	

Datagram sa vždy nemusí dostať do svojho cieľa, môže nastať hardwarové zlyhanie, nesprávna konfigurácia protokolu, vypnuté rozhranie, nesprávne smerovanie. V tejto situácii sa pošle odosielateľovi správa o nedosiahnuteľnosti cieľa. Hodnota 3 v type poľa indikuje, že ide o správu typu cieľ nedosiahnuteľný. 0 v kóde hovorí o príčine, sieť bola nedosiahnuteľná.

8.1.9. Rôzne ohlasovanie chýb

0	8	16
Type (12)	Code (0-2)	Checksum
Pointer		Unused (must be zero)
Internet Header + First 64 Bits of Datagram		

Ak zariadenie nie je schopné poslať správu ďalej, pošle sa zdroju IP datagram s parametrom 12, v hlavičke je aj kód, ak je rovný 0, potom položka Pointer obsahuje číslo oktetu datagramu, ktorý spôsobil chybu.

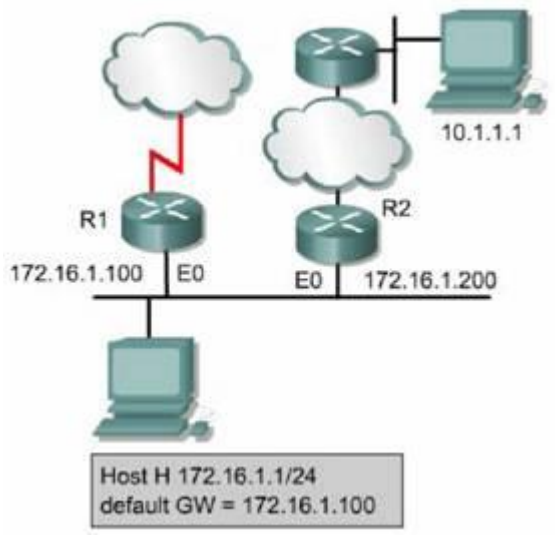
8.2.1. Úvod do kontrolný správ

Internet Control Message Protocol (ICMP) je integrovaná časť TCP/IP protokolu. IP nemá zabudovanú podporu o hlásení chýb, ako aj poskytovanie informácií alebo kontrolných správ na hosta. O toto sa stará ICMP. ICMP kontrolné správy sú zapuzdrené v IP datagramoch. Na rozdiel od chybových správ nie sú generované ako výsledok straty paketu alebo chybovej situácie. Informujú hostov napr. o zahltení siete, o existencii „bližšej" brány do vzdialených sietí.

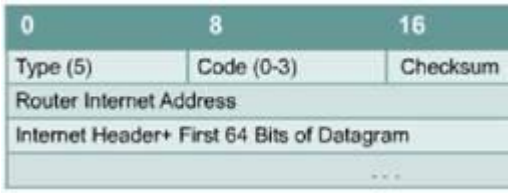
8.2.2. ICMP presmerovanie/zmena požiadavky

ICMP redirect/change request je všeobecnou ICMP kontrolnou správou. Tento typ správy môže byť inicializovaný len gateway, zvyčajne ide o router. Pokiaľ chcú hosti komunikovať z inou sieťou, musia mať nastavenú východziu bránu, ktorá je adresou portu routra pripojeného do rovnakej siete ako hosti. Ak chce host komunikovať s inou sieťou, router ho informuje cez redirect/change request o najlepšej ceste do danej siete.

H vyšle paket určený pre 10.1.1.1 (sieť 10.0.0.0/8) na default GW (172.16.1.100)
R1 cez svoje ST zistí, že paket má ďalej forwardovať na 172.16.1.200 cez rovnaké rozhranie(E0) ako paket obdržal R1 paket forwarduje na 172.16.1.200, súčasne zašle H správu ICMP Redirect/Change požadujúcu, aby H pakety pre 10.0.0.0/8 forwardoval na 172.16.1.200 ICMP Redirect/Change Request zasiela smerovač na zdrojovú IP adresu datagramu, ak:



1. Vstupné aj výstupné rozhranie datagramu na smerovači je rovnaké
2. Adresa siete/podsiete u zdrojovej IP adresy je rovnaká ako adresa siete/podsiete nasledujúceho smerovača na ceste
3. Datagram nie je source routed
4. Smer v ICMP Redirect nie je ďalší ICMP Redirect alebo default route



Smerovač je skonfigurovaný na zasielanie redirectov defaultne zapnuté, možno vypnúť na rozhraní príkazom R(config-if)#**no ip redirects**)

Code value	**Required Action**
0	Redirected datagrams for the network.
1	Redirected datagrams for the host.

2 Redirected datagrams for the type of services and networks.
3 Redirected datagrams for the type of services and host.

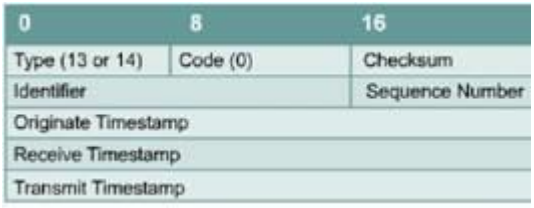
Pri ICMP redirect/change request je použitý typ 5, kód 0-3. Interná adresa poľa obsahuje defaultnú bránu pre príslušnú sieť.

8.2.3. Synchronizácia času a odhad času prenosu

Hosti na rôznych sieťach, ktorí sa pokúšajú spojiť použitím programov, ktoré vyžadujú časovú synchronizáciu, môžu sa niekedy stretnúť s problémami. ICMP správy typu timestamp slúžia na zmiernenie tohto problému. Host pošle ICMP požiadavku o aktuálny čas vzdialeného hosta, ten mu odpovie cez ICMP timestamp odpoveď.

Pole v ICMP timestamp message:

1. 13: požiadavka, obsahuje aktuálny čas
2. 14: odpoveď, obsahuje čas vzdialeného hosta
   Kódové pole je **0**, lebo nie sú dostupné žiadne prídavné parametre.



Prijatý a poslaný čas sú počítané v počte milisekúnd času trvania od polnoci univerzálneho času.
Všetky ICMP timestamp správy obsahujú originálneho a prijatého času, na základe nich vie určiť dobu trvania prenosu. Tento spôsob odhadu však je dosť nepresný, na výpočet času sa používa Network Time Protocol (NTP).

8.2.4. Informačné správy požiadavky a odpovede

Pôvodne určené k tomu, aby host mohol zistiť svoju adresu siete. V súčasnosti sú už menej používané, sú zastaralé, namiesto nich sa používa DHCP resp. BOOTP protokol. Sú dva typy správ, 15 je požiadavka a 16 je odpoveď.

8.2.5. Požiadavka na sieťovú masku

Administrátori delia siete do podsietí. Aby bol host schopný komunikovať v danej podsieti, musí poznať sieťovú masku. Ak ju nevie, pošle požiadavku typu address mask na router. Ak vie adresu routra, pošle ju priamo na router, inak je poslaná na broadcast. Pri obdržaní požiadavky routrom, router odpovie správou typu address mask.
Príklad:
Host má IP adresu 172.16.5.2 a chce vedieť masku, pošle požiadavku na 255.255.255.255, z týmito parametrami: ICMP = 1 Type: Address Mask Request = AM1 Code: 0 Mask: 255.255.255.0
Požiadavku spracuje router z IP adresou 172.16.5.1 a pošle odpoveď z týmito parametrami:
Destination address: 172.16.5.2, Protocol: ICMP = 1, Type: Address Mask Reply = AM2, Code: 0, Mask: 255.255.255.0
Rozdelenie typov v ICMP správe:

1. 17, je pridelená požiadavke
2. 18, je pridelená pre odpoveď

6.2.6. Prieskumné správy routra

Slúži na zistenie default gateway od všetkých routrov. Tento proces začína hosť poslaním požiadavky na všetky routre, použitím multicastovej adresy 224.0.0.2. Môže byť použitý broadcast, ak by náhodou router nemal nakonfigurovaný multicast. Po prijatí žiadosti routrom, odpovie na žiadosť.

0	8	16
Type (9)	Code (0)	Checksum
Number of Addresses	Address Entry Size	Lifetime
Router Address 1		
Preferences Level 1		
Router Address 2		
Preferences Level 2		

6.27. Router solicitation message

Hosť generuje ICMP router solicitation message v dôsledku neznalosti východzej brány. Lokálny router mu ju zodpovie.

0	8	16	31
Type (10)	Code (0)	Checksum	
Reserved			

IP Fields	
Source Address	An IP address belonging to the interface from which this message is sent, or 0.
Destination Address	The Configured solicitation address
Time- to - live	1If the destination address is an IP multicast address; at least 1 otherwise

ICMP Fields	
Type	10
Code	0
Checksum	The 16-bit one's complement of the one's complement sum of the ICMP message, starting with the ICMP type. For computing the checksum, the checksum field is set to 0.
Reserved	

8.2.8. Preťaženie a kontrola prúdových správ

Ak sa viaceré počítače pokúšajú naraz o prístup na jeden počítač, môže dôjsť k zahlteniu dopravy. Podobne tento problém môže nastať pri prechode z rýchlej LAN na pomalšiu WAN. Dôjde k strate paketov. ICMP source-quench sú použité na redukovanie hodnoty dátových strát. Vysiela sa zdroju paketov s cieľom požiadať ho, aby dáta vysielal pomalšie. Cisco smerovače defaultne nevysielajú, pretože tieto správy tiež prispievajú k zahlteniu siete. Efektívne využitie je v malých úradoch a domácnostiach. Dobrým príkladom je domáca sieť, kde napr. 4 PC chcú pristupovať 56k na internet.

Odstraňovanie problémov so routrami

9.1.1. Príkaz show ip route

Primárnou funkciou routrov je určiť najlepšiu cestu do cieľa, sú zaznamenané v smerovacej tabuľke s DRAM. **show ip route** command, zobrazí obsah smerovacej tabuľky, tabuľka obsahuje záznamy o všetkých známych sieťach a o spôsobe, akým bol záznam vytvorený. Príklady využitia:

```
C   192.168.4.0/24 is directly connected, Ethernet0
    10.0.0.0/16 is subnetted, 3 subnets
C   10.3.0.0 is directly connected, Serial0
C   10.4.0.0 is directly connected, Serial1
C   10.5.0.0 is directly connected, Ethernet1
```

1. show ip route connected
2. show ip route network
3. show ip route rip
4. show ip route igrp
5. show ip route static

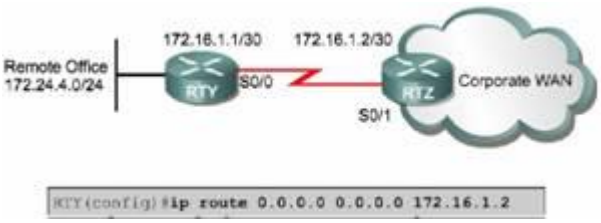
Keď router prijme paket určený pre 192.168.4.46, pozrie sa do smerovacej tabuľky na prefix 192.168.4.0/24, na základe tohto záznamu presunie paket na rozhranie E0. Smerovanie:

1. **statické**, administrátor manuálne definuje smerovanie na jednu alebo viac cieľových sietí
   výhody: Nízke nároky na záťaž procesora, na bandwidth liniek. Vyššia bezpečnosť voči útokom, precízna kontrola výberu cesty administrátorom nevýhody: Prácna konfigurácia, neadaptabilnosť na zmeny stavu liniek:
2. **dynamické**, routre podľa definovaných pravidiel pre smerovacie protokoly si vymieňajú smerovacie informácie a určujú najlepšiu cestu

výhody: Adaptabilnosť na zmeny topológie siete, nízke nároky na administráciu nevýhody: Vyššia záťaž pre procesor, pamäť, bandwidth liniek

9.1.2. Určenie východzej brány

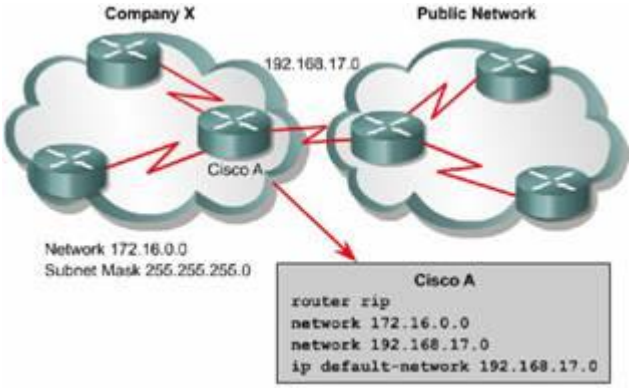
Používa sa, keď sa router nie je schopný spojiť so sieťou pre chýbajúci záznam v smerovacej tabuľke. Router použije default route ako poslednú možnosť pred vrátením paketu. Je ju možné nastaviť staticky cez administrátora, alebo naučiť dynamicky cez smerovací protokol. Administrátor musí aspoň na 1smerovači staticky nakonfigurovať default route:



Po zadaní príkazu **ip default-network 192.168.17.0** definovaného pre triedu C, budú všetky pakety, pre ktoré nie je záznam v smerovacej tabuľke presmerované na 192.168.17.0.

1. ip default-network, smerovanie využitím dynamických smerovacích protokolov

2. ip route 0.0.0.0 0.0.0.0



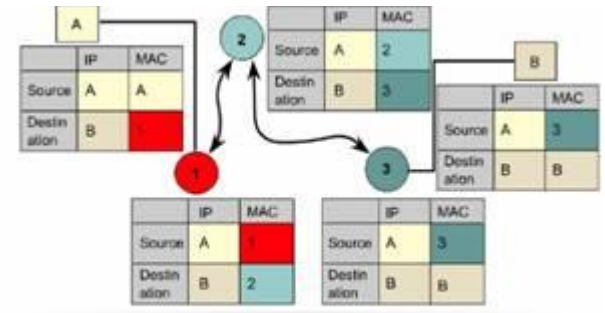
Príkaz **ip route to 0.0.0.0/0** je inou možnosťou zápisu pre default route. Príklad: Router(config)#ip route 0.0.0.0 0.0.0.0 [next-hop-ip-address | exit-interface] Po zadaní príkazu: **show ip route** sa zobrazí smerovanie. Príklad: Gateway of last resort is 172.16.1.2 to network 0.0.0.0

9.1.3. Určovanie cesty zdroja a cieľa

Pri doprave paketu prechádzajúceho cez sieť v tvare mraku, určovanie cesty nastáva na sieťovej vrstve. Určovanie cesty umožňuje routrom vyhodnotiť dostupnú cestu k cieľu a zabezpečiť spracovanie paketu. Na doručenie zo zdrojovej do cieľovej siete využíva sieťová vrstva smerovacie tabuľky

9.1.4. Určovanie L2 a L3 adries

Pri prechode paketu zo zdroja do cieľa sa používajú obidve vrstvy a adresy. Pri putovaní paketu cez sieť sa skúma smerovacia tabuľka k nasledujúcemu hopu. Paket sa presunie na nasledujúci hop použitím MAC adresy. IP adresa zdroja a cieľa sa v hlavičke nemení. Adresy 3. vrstvy sú používané na smerovanie paketov zo zdrojovej do cieľovej siete. IP adresy zdroja a cieľa sa nemenia, ale MAC adresy sa menia pri každom hope alebo routri. Adresy dátovej (2vrstva) vrstvy sú dôležité pre presun paketu medzi sieťami, pretože doručenie medzi sieťami je založené na adrese 2. vrstvy a nie 3. Keď je najbližšia cesta na základe ST identifikovaný (L3), smerovač prepne paket z jedného rozhrania na druhé (L2), zodpovedajúce vybratému smeru do cieľovej siete



At each interface, as the packet moves across the network, the routing table is examined and the router determines the next hop. The packet is then forwarded using the MAC address of the next hop. The IP source and destination headers do not change, at any time.

9.1.5. Určovanie administratívnej vzdialenosti

Router môže zisťovať smerovania použitím dynamických smerovacích protokolov alebo môže byť konfigurovaný manuálne administrátorom. Po zistení stavu siete,

Protocols	Default Administrative Distances
Connected	0
Static	1
EIGRP summary route	5
eBGP	20
EIGRP (Internal)	90
IGRP	100
OSPF	110
IS	115
RIP	120
EIGRP (External)	170
iBGP (external)	200

router musí vybrať najlepšiu cestu do danej siete. Pri rozhodovaní používa **administratívnu vzdialenosť.**

9.1.6. Určovanie smerovacej metriky

Administratívna vzdialenosť: vyjadruje mieru zdroja dôveryhodnosti informácie, čím menšie, tým lepšie. Každý smerovací protokol má inú AV. V prípade viacerých zdrojov sa do ST umiestni smer s najmenšou administratívnou vzdialenosťou do cieľovej siete.
Smerovacie protokoly využívajú metriku na určenie najlepšej cestu do cieľa. Každý smerovací algoritmus ohodnocuje jednotlivé smery hodnotou metriky; čím menšia hodnota metriky, tým „lepšia" cesta. Rôzne protokoly využívajú pri výpočte rôzny počet faktorov, čím viac, tým je metrika presnejšia. Napr. RIP používa len počet hopov. Faktory pri tvorbe metriky:

1. Statické – kapacita linky, oneskorenie, hopcount, nemenia svoje hodnoty
2. Dynamické –spoľahlivosť(1-255), záťaž (1-255), v reálnom čase sú premenlivé Príklad výpočtu metriky pre IGRP:

Metrika = K1 *Bandwidth + (K2 *Bandwidth)/256-load) + K3 *Delay Pričom defaultne K1, K3 = 1, K2, K4, K5 = 0 Výsledkom je Metric = Bandwidth + Delay

9.1.7. Určenie nasledujúceho smerovača (nexthop)

Smerovacie tabuľky sú vypĺňané smerovacím algoritmom. Cieľový/nasledujúci skok povie routru, že cieľová adresa môže byť dosiahnutá poslaním paketu na daný router, tento router predstavuje nasledujúci skok k finálnemu cieľu. Pri príjme router spracuje cieľovú adresu a pokúsi sa ho spojiť s adresou nasledujúceho skoku.
Jeden z riadkov príkazu: **show ip route**

9.1.8. Určovanie poslednej smerovacej aktualizácie

Príkazy pre nájdenie poslednej smerovacej aktualizácie:

1. show ip route
2. show ip route network
3. show ip protocols

4. show ip rip database

9.1.9. Zistenie viacerých smerov do rovnakej cieľovej siete

Niektoré smerovacie protokoly umožňujú viacnásobné smerovanie do rovnakého cieľa. Tým sa dosahuje väčšej priepustnosti a spoľahlivosti.
Časť príkazu **show ip route**, kde sú uvedené 2 cestu k jednej sieti:

```
I  192.168.20.0/24 [100/8486] via 192.168.0.2,
00:00:22, FastEthernet0/0
          [100/10476] via 192.168.10.2, 00:00:22,
```

9.2.1. Úvod do testovania sietí

Po jednotlivých vrstvách OSI modelu prebieha testovanie od fyzickej vrstvy končiac na aplikačnej. Teda najskôr
skontrolujeme kábel :-)
Najčastejšie problémy sú spôsobené chybami v adresovacích schémach
Testovacie príkazy:

1. telnet, testuje všetkých 7 vrstiev OSI modelu
2. ping, testuje prvé 3 vrstvy OSI modelu

9.2.2. Využitie štruktúrovaného výstupu na riešenie problémov

Pri riešení problémov je dôležité viesť dokumentáciu. Postupnosť krokov:

1. zozbierať všetky dostupné informácie a analyzovať symptómy zlyhania
2. lokalizovať problém vo vnútri jednoduchého sieťového segmentu, v samostatnom module alebo jednotke, alebo na samostatnom užívateľovi
3. lokalizovať problém na špecifickom hardware alebo software vnútri jednotky, module, alebo užívateľskom sieťovom prístupe
4. lokalizovať a opraviť špecifický problém
5. overiť, že problém bol odstránený

9.2.3. Testovanie vrstiev OSI

Začína sa na 1. vrstve a končí na 7, ak je to nevyhnutné.
01. Chyba na 1. vrstve (fyzická)

1. prelomený kábel
2. rozpojený kábel
3. kábel pripojený na zlý port
4. zle pripojený kábel
5. nesprávny typ kábla (priamy namiesto krížového apod.)
6. problémy stransceiverom
7. problémy s DCE, DTE káblom

8. vypnuté zariadenie (pozn. autora: častý problém :-))

02. Chyba na 2. vrstve (linková)

1. nesprávne nakonfigurované sériové, ethernetové rozhranie
2. nesprávne nakonfigurovaný typ zapuzdrenia (default pre sériové rozhrania je HDLC)
3. chýbajúce alebo nesprávne nastavené časovanie na sériovom rozhraní
4. problém so sieťovou kartou (NIC)

03. Chyba na 3. vrstve (sieťová)

1. nenastavený smerovací protokol
2. zapnutý nesprávny smerovací protokol

- nesprávna IP alebo maska siete

ping – otestuje spojenie na vrstvách 1-3. **telnet** - otestuje spojenie na vrstvách 4-7

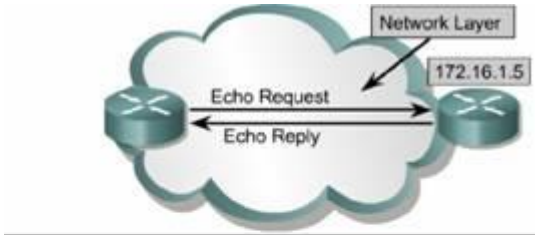
9.2.4. Riešenie problémov na 1. vrstve využitím indikátorov

Indikačné svetielka sú užitočným nástrojom pri riešení problémov, sú tiež nazývané linkové svetlá, napr. pri NIC
indikujú, či je správne pripojenie, či switche a huby majú pripojené káble na porty. Niektoré zariadenia majú
osobitné svetielka pre vysielanie (TX) a pre príjem (RX).
Častou príčinou nefunkčnosti siete je použitie nesprávneho kábla:
- crossover: medzi priame pripojenie medzi swithom a hubom, prípadne medzi 2 hostami (2xPC, 2xrouter)

Overenie, či kábel z jedného rozhrania je pripojený na správny konektor na druhom zariadení. Treba preveriť, či
je dobre **dotlačený** kábel. Ak spojenie nie je funkčné, môže sa vyskúšať zameniť kábel za už overený.
Pri vysielačoch/prijímačoch overiť či je použitý správny typ, či je správne pripojený a nakonfigurovaný.
Vždy overiť, že zariadenie je **zapnuté**.

9.2.5. Riešenie problémov na 3. vrstve použitím ping

ping – využíva sa na testovanie sieťovej konektivity prostredníctvom echo protokolu, Internet Control Message Protocol (ICMP), je dostupný v privilegovanom a užívateľskom móde. Pošle sa paket na cieľový host a čaká sa na odpoveď.




```
Router>ping 172.16.1.5
Type escape sequence to abort.
Sending 5, 100 byte ICMP Echos to 172.16.1.5,
timeout is 2 seconds:
!!!!!
Success rate is 100 percent,
round-trip min/avg/max = 1/3/4 ms
Router>
```

Na 172.16.1.5. je poslaný ping. Ten odpovie cez ECHO. Ak sú zobrazené „**!**" echo prebehlo v poriadku. Pri zobrazení „**.**" bol priveľký time out, prípadne cieľ je nedosiahnuteľný. V dolnej časti je zobrazený min., priemerný a maximálne čas odpovede.

Rozšírený ping – v privilegovanom režime bez udania
cieľovej adresy, umožňuje širšie možnosti nastavení

9.2.6. Riešenie problémov na 7. vrstve použitím Telnet

Telnet – je virtuálny terminálový protokol, je súčasťou TCP/IP. Slúži na overenie aplikačnej vrstvy medzi zdrojom a cieľom. Normálne sa využíva na diaľkové pripojenie na zariadenie, zbieranie informácií a spúšťanie
programov. Úspešné pripojenie cez telnet indikuje, že nižšie vrstvy pracujú správne.
Ak sa chce administrátor pripojiť na router, ale telnet zlyhá, admin. použije ping, ak dostane odpoveď, je pravdepodobné, že je problém s prístupom, prípadne je zle zadané meno alebo IP adresa.
Možné príčiny pri zlyhaní konektivity:

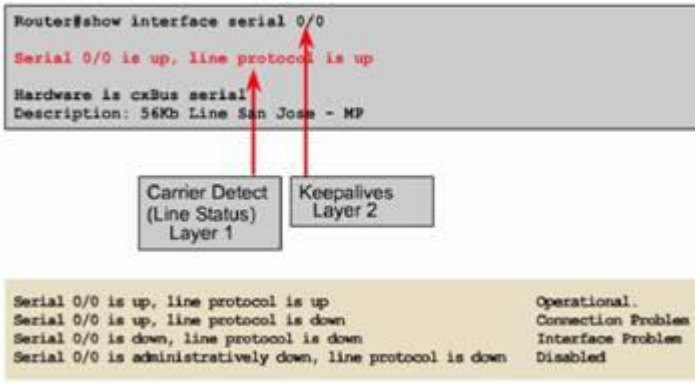
1. nefunkčné reverzné DNS (časté pri používaní DHCP)
2. nie je možné medzi klientom a serverom dohodnúť požadované parametre (na smerovačoch Cisco možno zistiť cez **debug telnet**)
3. Služba telnet bola na cieľovom serveri vypnutá alebo presunutá na iný port ako 23

9.3.1. Riešenie problémov na 1. vrstve použitím show interfaces

show interfaces command, slúži na kontrolu stavu a štatistiku na rozhraní. Pri zadaní parametrov si môžeme dať zobraziť stav konkrétneho rozhrania, napr. Serial 0/0 show interfaces serial 0/0.

Rozdelenie výpisu:

1. fyzický (hardwarová) časť, obsahuje káble, konektory a rozhrania odrážajúce stav fyz. pripojenia medzi zariadeniami, využitá vrstva 1., určuje či zariadenie prijíma Carrier Detect (CD) signál
2. softwarová časť, sem zahŕňame správy o trvanlivosti, kontrolných informáciách a užívateľských informáciách medzi susednými zariadeniami, využitá vrstva 2.



L1 problémy u sériových rozhraní možno zistiť na základe stavu počítadiel:

1. Veľký počet **Carrier transitions** (straty CD signálu z druhej strany): Časté prerušenia na linke (k ISP), vadný prepínač, DSU, HW smerovača
2. Veľký počet **Input errors**: Vadná linka, kábel, telefónne zariadenie, konektor, CSU, DSU, HW smerovača
3. Veľký počet **Interface resets** (keď nepríde po dlhú dobu keepalive): Vadná linka, HW problém na CSU, DSU, prepínači

Počítadlá možno vynulovať príkazom – R#clear counters command (rozhranie)

9.3.2. Riešenie problémov na 2. vrstve použitím show interfaces

Príkaz show interfaces je dôležitý nástroj na riešenie problémov na 1. a 2. vrstve. Prvý parameter príkazu sa odkazuje na fyzickú vrstvu. Druhý parameter kontroluje, či procesy využívajú rozhranie, zisťuje, či je prijaté keepalives.
Keepalives je správa poslaná jedným zariadením druhému, že virtuálne spojenie medzi nimi je stále aktívne. Ak táto informácia chýba 3 nasledujúce keepalive, je rozhranie označené ako down, keď line je down, potom aj protokol je down. Tento stav nastáva pri hardwarových problémoch a keď je rozhranie administratívne dole. Ak rozhranie je up a protokol je down, je problém na 2. vrstve. Možné príčiny:

1. Nevymieňajú sa keepalive správy
2. Nie je nastavený clockrate
3. Nie je na obidvoch stranách linky nastavený rovnaký typ zapúzdrenia
4. Problémy s autentifikáciou

9.3.3. Riešenie problémov použitím príkazu show cdp

Cisco Discovery Protocol (CDP) inzeruje svojim priamo pripojených susedov o MAC, IP adrese a odchádzajúcom rozhraní.
show cdp neighbors – zobrazí informácie o priamo pripojených susedoch
show cdp neighbors detail – zobrazí detaily špecifického zariadenia, aktívne rozhrania, port ID a verziu Cisco IOS bežiacom na vzdialenom zariadení Z bezpečnostných dôvodov by mal byť CDP povolený len na rozhrania medzi Cisco zariadeniami a nie na užívateľských portoch

9.3.4. Riešenie problémov použitím príkazu traceroute

traceroute - Umožňuje vystopovať cestu datagramu do cieľového hosta, pacuje na 3. vrstve, generuje zoznam hopov, cez ktoré úspešne prešiel. Pri zobrazení * paket zlyhal.
round trip time (RTT) – je to čas potrebný na poslanie paketu a získanie odpovede. ICMP zlyhanie nemusí indikovať problém, pretože niektoré správy môžu byť filtrované.
Zdroj vysiela postupne po 3udp datagramy s neplatným číslom portu. TTL hodnota je najprv 1 potom 2, 3 atď. Ak TTL bolo 1, na ďalšom smerovači bude 0 a tento vyšle zdroju ICMP Time Exceeded správu; z nej sa zistí, cez ktorý prvý smerovač datagram prešiel.
Podobne pre TTL 2, 3, ... Keď datagram dorazí do cieľového hosta, tento namiesto Time Exceeded odpovie správou ICMP Port Unreachable.

9.3.5. Problémy so smerovaním

Základné príkazy:

1. show ip protocols, informácie o smerovacích protokolov
2. show ip route, obsah smerovacej tabuľky, obsahuje všetky známe siete a podsiete, spôsob akým boli tieto informácie naučené. Využíva sa na overenie, či je zadané smerovanie do príslušnej siete. Ak sa hľadaná cieľová sieť nenachádza v ST, pravdepodobne je problém so smerovacím protokolom

show ip protocols, slúži na zistenie informácie o všetkých bežiacich smerovacích protokoloch na smerovači, timery, filtre, sumarizácia a redistribúcia smerov atď.

9.3.6. Riešenie problémov použitím príkazu show controllers serial

show controllers serial command, slúži na určenie typu kábla, z toho je možné určiť, či je kábel pripojený, či kábel nie je zlý

9.3.7. Úvod do debugovania

debug – je používaný na zobrazenie dynamických dát a udalostí. Tieto správy môžu byť dopravou na zariadení, chybové správy a inými užitočnými informáciami. Náročné na čas procesora, môže narušiť normálnu činnosť smerovača. Používať len pri odstraňovaní problémov, nie na monitorovanie prevádzky!!! Výpis správ je prednadstavený na konzolu. Pri existujúcom telnetovom pripojení môžu byť správy presmerované cez príkaz **terminal monitor** command. Pri telnete je pravidlo, že na výpis všetkých správ neposiela na port, kde
je telnet sedenie, došlo by k zahlteniu linky.
timestamps debug command – pridá časové značky ku debug správam
no debug all command alebo **undebug all**, zrušenie diagnostického výstupu, ak chcem zakázať len výpis nejakej udalosti, zadám **no**, napr.: **no debug ip rip**
show debugging, zobrazenie, čo všetko je aktuálne debagované.

Transportná vrstva TCPIP

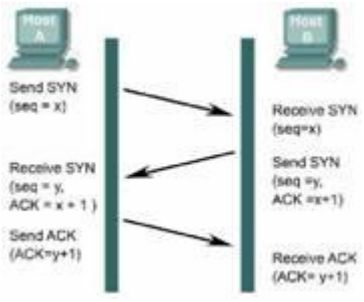
10.1.1. TCP operácie

IP adresovanie umožňuje smerovanie paketov medzi sieťami, ale negarantuje ich doručenie. Transportná vrstva – je zodpovedná za spoľahlivý prenos a reguluje dátový tok medzi zdrojom a cieľom. Na zabezpečenie tohto cieľa sa využíva posuvné okno a sekvencia čísel so synchronizačným procesom ktorý zaisťuje, že hosť je pripravený a ochotný komunikovať.

10.1.2. Synchronizácia alebo 3-cestné nadviazanie spojenia

TCP je spojito orientovaný protokol. Pri dátovom prenose sa najskôr medzi dvoma hostami uskutoční synchronizácia na zabezpečenie virtuálnej komunikácie. Synchronizácia zabezpečí, že obe strany sú pripravené na prenos a umožnia zariadeniam určiť inicializačné sekvenčné čísla. Tomuto procesu sa hovorí 3-cestné nadviazanie spojenia.

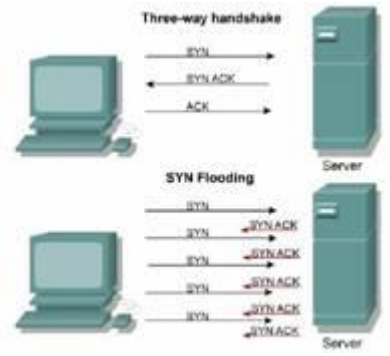
Postup nadviazania 3-cestného spojenia:



1. Prvý host inicializuje spojenie zaslaním paketu s nastaveným SYN bitom a svojím začiatočným poradovým číslom (Sequence Number) x
2. Druhý host si zaznamená poradové číslo x, odpovie potvrdzovacím číslom (Acknowledge Number) x+ 1 a súčasne oznámi svoje vlastné poradové číslo y
3. Prvý host si zaznamená poradové číslo druhého hosta a odpovie paketom s potvrdzovacím číslom y+ 1

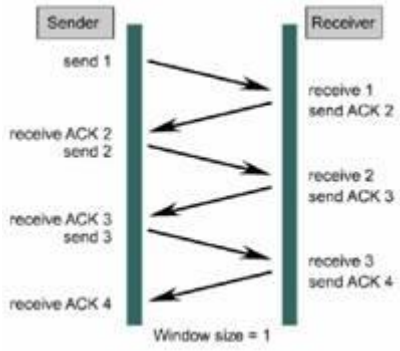
10.1.3. Útok Denial of service (DOS)

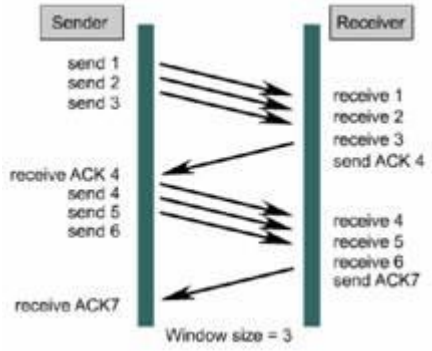
DOS útok je navrhnutý na odoprení služby legitímnemu užívateľovi pokúšajúceho sa o nadviazanie spojenia. Hacker predstieranou IP adresou (spoofing) sa snaží veľkým množstvom žiadostí o spojenie zahltiť Server a vyčerpať jeho systémové prostriedky (spojenia márne čakajú na 3. časť potvrdenia spojenia, keďže zdrojová IP bola falošná, kým neuplynie timeout)
Obrana: skrátiť timeout pre spojenie, zväčšiť veľkosť connection queue, špeciálny SW pre zachytávanie týchto útokov



10.1.4. Používanie okien a veľkosť okien

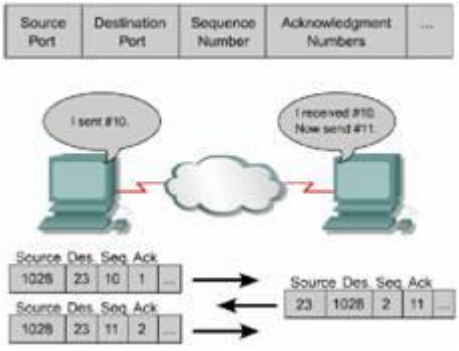
Na prenos dát je potrebná ich rozdeliť na menšie segmenty, to zabezpečuje TCP.
Windowing – je to proces prúdovej kontroly, servisný poskytovateľ reguluje, aké množstvo dát môže byť poslané počas periódy prenášania. Určuje množstvo dát, ktoré môžu byť poslané pred potvrdením z cieľa. Po poslaní dát určených veľkosťou okna, hosť musí prijať potvrdenie, pred posielaním ďalších dát. Napr. ak WS je 1 po každom segmente musí nasledovať potvrdenie. TCP používa techniku sliding window, čo umožňuje komunikujúcim zariadeniam dynamicky nastavovať a meniť veľkosť okna podľa aktuálnej situácie na sieti





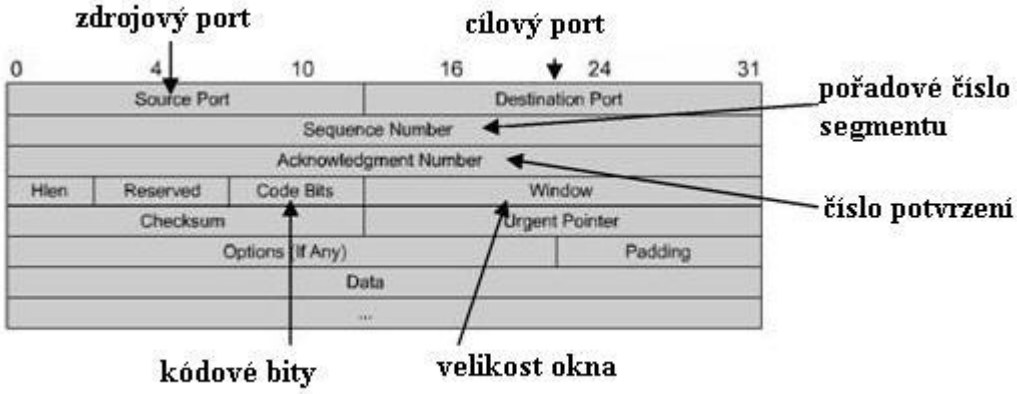
10.1.5. Poradové čísla (Sequencing numbers)

TCP delí dáta na segmenty, tie sú označené poradovými číslami a odoslané, keďže pri prenose nie je zaručené, že budú prijaté v rovnakom poradí. Pri prijatí TCP aplikuje poradové čísla a poskladá späť dáta. Umožňujú identifikovať, či nejaký dátový segment v cieľovom zariadení nechýba, ak áno, bude opakovane vyslaný.



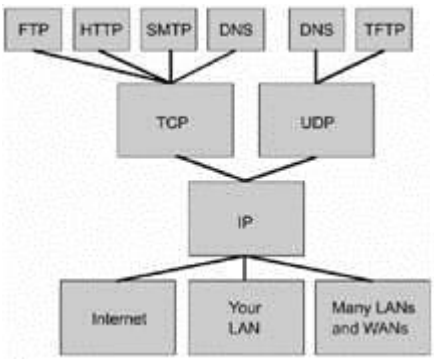
10.1.6. Pozitívne potvrdzovanie a retransmisia

Potvrdenie je všeobecným krokom synchronizačného procesu obsahujúceho pohyblivé okná a dátové sekvencie. Po poli so sekvenčným číslom nasleduje pole potvrdenia.



Príznaky (SYN, ACK, FIN,...) Veľkosť okna TCP využíva pozitívny ACK a opakovaný prenos na kontrolu dátového prúdu a overenie dátového doručenia. Je využívaný veľa protokolmi na overenie spoľahlivosti. Zdroj pošle paket, spustí časovač a čaká na potvrdenie pred poslaním ďalšieho. Ak timer pre segment vyprší bez potvrdenia, segment sa vyšle ešte raz, súčasne sa zníži rýchlosť vysielania dát. Bez potvrdenia zdroj môže vyslať maximálne veľkosť okna bajtov. TCP užívateľ očakáva potvrdenie v ktorom sa číslo potvrdenia odkazuje na nasledujúci paket.

10.1.7. UDP protokol



UDP je nespojito orientovaný protokol, pracuje na 4. vrstve, negarantuje doručenie paketu. Využitie protokolu pre aplikácie: TCP musí byť použitý, keď aplikácie potrebujú garantovať, že paket príde celý, súvislý a neduplicitný.
UDP je vhodný pre aplikácie, kde sa vyžaduje rýchlosť na úkor spoľahlivosti, neprebieha potvrdzovanie, úlohu detekcie chýb preberá

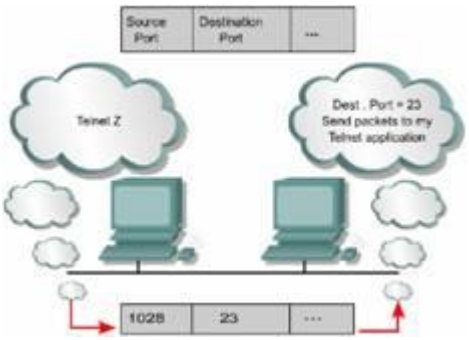
# of Bits	16	16	16	16	16
	Source Port	Destination Port	Length	Check Sum	Data...

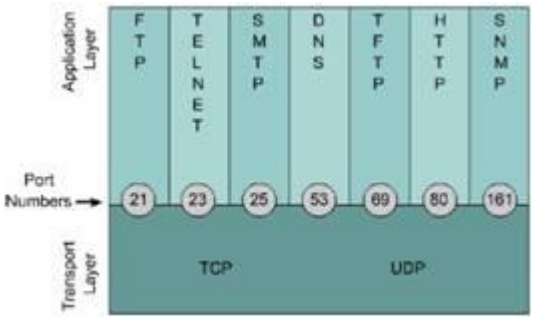
aplikačná vrstva. Hlavička UDP,

neobsahuje potvrdenia ani veľkosť okien. Pri DNS požiadavke od hosta, bude mať cieľový port 53, dĺžka identifikuje počet oktetov v UDP segmente. Je možné nastaviť aj kontrolný súčet na zabezpečenie, že dáta neboli zmenené počas
prenosu. Pri prenose cez sieť je UDP zapuzdrený vnútri IP paketu. Cieľový port špecifikuje aplikáciu, z ktorej sa posielajú dáta.

10.2.1. Viacnásobný rozhovor medzi hostami

Pri prenose sa používajú čísla portov, ktoré umožňujú zistiť, pre akú aplikáciu je paket určený. Napr. FTP má č. portu 21.





Pridelený rozsah čísel portů:

1. pod 255 pre verejné aplikácie
2. 255 -1023 pridelené firmám na manažovanie aplikácií
3. od 1023 sú nepridelený
4. 0 -1023 – well-known porty Príklad komunikácie:

Klient sa pripája na službu telnet (cieľový port 23), pričom číslo jeho zdrojového portu je nepodstatné (1028), je vždy väčšie ako 1023. Server v tomto dialógu používa cieľový port 1028 (s ktorým klient nadviazal spojenie) a zdrojový 23.

10.2.3. Porty pre klientov

Klient musí mať pridelený port, aby sa mohol pripojiť na službu na serveri. Cieľový port je z oblasti well-known portov. Zdrojový port je dynamicky pridelený v oblasti nad 1023. Príklad:
Chcem sa pripojiť na web, zdrojový port je 1045 a cieľový 80, 80 zodpovedá portu http na ktorom beží webový server.

10.2.4. Číslovanie portov a dobre známe čísla portov

V hlavičke TCP a UDB sú 2 bajty vyhradené na čísla portov, tie môžu byť v rozsahu 0 – 65535. Delenie portov:

1. 0 – 1023 dobre známe portu, napr.: FTP, Telnet, DNS
2. 1024 – 49151 registrované porty
3. 49152 – 65535 dynamické alebo privátne

10.2.5. Príklad viacnásobného sesion medzi hostami

Zdrojový a cieľový port sú skombinované zo sieťovou adresou. Hosť môže v rovnakom čase surfovať na internete, port 80, a zároveň mať spustené telnet na porte 23. IP adresa a MAC adresa budú rovnaké, ale každá
aplikácia a služba bude mať vlastný port .
Príkaz **netstat –n** (Windows) zobrazí stav jednotlivých relácií
Na smerovači príkaz R#**show tcp**

10.2.6. Porovnanie MAC adries, IP adries a čísiel portov

Všetky 3 predstavujú adresy. MAC adresa –Linková vrstva IP adresa –Sieťová vrstva Číslo portu – Transportná vrstva

Prístupové zoznamy

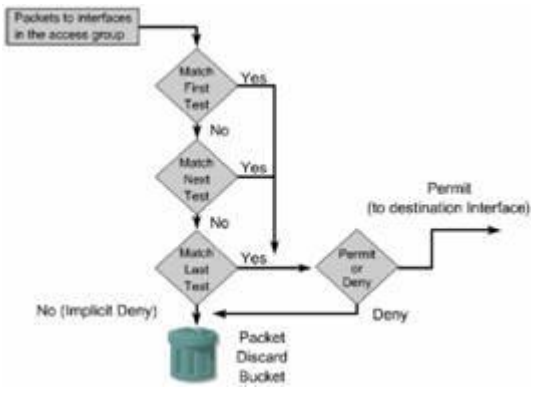
11.1.1. Čo sú prístupové listy (ACL)

ACL je zoznam pravidiel, ktoré sú aplikované na dopravu cez rozhranie routra. Hovoria routru, ktoré typy paketov povolí alebo blokuje. Umožňujú správu dopravy a zabezpečujú prístup na a zo siete.
Môžu byť vytvorené pre všetky smerované protokoly ako IP alebo IPX.
Router testuje každý paket, podľa podmienok v ACL, tie môžu byť založené na zdrojovej alebo cieľovej adrese,
protokole alebo na čísle portu.
Pre jeden smer, rozhranie a protokol môže byť definovaný 1 ACL. Ak mám 2 rozhrania a 3 protokoly, budem
potrebovať 12 ACL, 3 pre každý protokol, 2 pre vstup a výstup, 2 pre porty.
Primárne dôvody vytvárania ACL:

1. limitovať sieťovú dopravu, zvýšiť sieťový výkon. Ak niekto sťahuje video, obmedzením tejto činnosti sa zvýši sieťový výkon
2. kontrola prúdového toku.
3. poskytnúť základnú úroveň bezpečnosti pre sieťový prístup.
4. rozhodujú, aký typ trafiku bude prepustený a aký zablokovaný
5. umožňujú administrátorovi riadiť, do ktorých častí siete / alebo k akým službám (http, telnet,...) budú mať klienti prístup

Ak nie je definovaný ACL na rozhraní, do siete prejdú všetky pakety.

11.1.2. Ako pracuje ACL



ACL je skupina pravidiel, ktoré definujú či pakety sú akceptované alebo zamietnuté na prichádzajúcom alebo odchádzajúcom rozhraní. Tieto rozhodnutia sú spracované podľa podmienok v ACL, kým sa nenájde zhoda o povolenej a alebo zakázanej akcii, ďalej sa už ACL nekontroluje. Záleží na poradí v akom boli jednotlivé príkazy vložené, CISCO IOS testuje zhora dole. Ak pri pakete nenastane zhoda ani pri jednom príkaze ACL, paket je implicitne odstránený, pretože na konci ACL je príkaz "deny any", ten nie je zobrazený .
Ak je nutné vložiť nové pravidlo do ACL, je ho nutné zmazať a opätovne vytvoriť s novým pravidlami. Je vhodné mať ALC pripravený v textovom editore a tento potom vložiť do konfigurácie routra.

11.1.3. Vytváranie ACL

ACL sa vytvára v GKM. Sú rôzne typy ACL, delia sa podľa čísla, pre každý ACL je pridelené len jedno číslo.

Protocol	Range
IP	1-99
Extended IP	100-199
AppleTalk	600-699
IPX	800-899
Extended IPX	900-999
IPX Service Advertising Protocol	1000-1099

access-list – slúži na vloženie pravidla Pri vytváraní ACL sa najskôr nadefinujú pravidlá a potom sa ACL pridelí rozhraniu.
access-group – pridelenie ACL jednému alebo viac rozhraniam, ktoré môžu kontrolovať prichádzajúcu alebo odchádzajúcu dopravu. Zadáva sa v konfiguračnom móde rozhrania.
no access-list číslo – zmazanie ACL
Pravidlá pre vytvorenie ACL:
01. Krok – vytvorenie ACL:
R(config)#access-list <číslo ACL> {permit / deny} <testovacie podmienky>
<číslo ACL> -určuje typ ACL
permit resp. deny–určuje, či príkaz povolí alebo zakáže paket vyhovujúci <testovacím podmienkam>
Zrušenie ACL:
R(config)#no access-list <číslo ACL>
!!! Pri akejkoľvek zmene ACL je potrebné zrušiť celý ACL a **vytvoriť ho odznova !!!**
02. Krok – aplikácia ACL na konkrétne rozhranie smerovača
R(config-if)# <protokol> access-group<číslo ACL> {in |out}
<protokol> - ip, ipx, ...
<číslo ACL> - číslo ACL, ktorý sa má aplikovať na rozhranie
in resp. out – či je ACL aplikovaný na prichádzajúce (in) alebo odchádzajúce pakety (out); implicitne je out

11.1.4. Funkcia masky s náhradnými znakmi (wildcard masks)

MASKA

- 32-bitové číslo rozdelené do 4 oktetov, párované s danou IP adresou. Čísla 0 a 1 definujú, ako spracovať príslušný IP adresový bit. Je prirovnávaný ku žolíku z kariet.
- sú navrhnuté na filtrovanie individuálnej skupiny IP adries pre prístup alebo blokovania prístupu k zdroju
založenom na IP adrese.

1. – musí nastať zhoda so zodpovedajúcim bitom IP adresy
2. – nemusí nastať zhoda so zodpovedajúcim bitom IP adresy

Príklady na WM: IP: 172.20.0.0 WM: 0.0.0.255

10101100.00010100.00000000.00000000 00000000.00000000.00000000.11111111

Dvojici 172.20.0.0 0.0.0.255 vyhovujú všetky IP adresy tvaru 172.20.0.X
binárně 10101100.00010100.00000000.xxxxxxxx

Dvojicu 0.0.0.0 255.255.255.255 možno nahradiť slovom **any** (vyhovuje ľubovolná IP)

Dvojicu A.B.C.D 0.0.0.0 možno nahradiť **host** A.B.C.D (vyhovuje len jedna IP adresa A.B.C.D)

11.1.5. Overovanie ACL

show ip interface - zobrazí informáciu, či je na rozhraní aplikovaný ACL
show access-lists - zobrazí príkazy všetkých ACL na smerovači
show running-config - zobrazí ACL aj ich aplikáciu na príslušné rozhrania

11.2.1. Štandartný ACL

- kontroluje zdrojovú IP adresu paketu
Porovnaním s ACP je paket blokovaný alebo prepustený pre všetky protokoly, založené na sieti, podsieti alebo adrese hosta. Príklad:
ak paket prichádza na Ea0/0, sú kontrolované zdrojové adresy a protokol. Ak sú povolený, budú smerované na výstupné rozhranie. Ak sú blokované, budú zahodené už na prichádzajúcom rozhraní. Umiestňujú sa čo najbližšie k cieľu paketov, ktorý je potrebné chrániť. Router(config)#**access-list** access-list-number {deny | permit} source [source-wildcard] [log] log – ak nastane u paketu prvá zhoda, vypíše na konzolu; ďalej vypisuje štatistiky v 5 min. intervaloch access-list-number - používajú sa s číslami ACL 1-99. Dôležité: príkazy je potrebné radiť od špecifickejších k všeobecnejším!!! Na konci každého ACL je deny all

11.2.2. Rozšírené ACL

Používané častejšie než štandartné, poskytujú väčší rozsah kontroly. Kontrolujú zdrojovú a cieľovú adresu,
protokol a číslo portu.
Umiestňujú sa čo najbližšie k zdroju paketov, ktoré je potrebné filtrovať, používajú sa s číslami ACL 100-199.
Syntax:
R(config)#**access-list**<číslo ACL>{deny / permit}<protokol> <zdroj. IP adresa>[<WM zdroj. IP adresy><cieľ.
IP adresa> <WM cieľ. IP adresy> <operátor> <operand>][established]
<protokol> -ip, tcp, udp, icmp, igrp, ...
<operátor> <operand> -lt(<) ,gt(>), eq(=) ,neq(=.) číslo portu – testuje u paketu číslo portu
established – v prípade tcp protokolu umožňuje prechod paketu v prípade už nadviazaného spojenia (napr. keď je
nastavený ACK bit)

```
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq telnet
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp
access-list 114 permit tcp 172.16.6.0 0.0.0.255 any eq ftp-data
```

Povolí zo siete 172.16.6.0/24 prístup len na služby telnet(port 23) a ftp(porty21, 20) s ľubovoľnou cieľovou ip adresou (any) a všetky ostatné IP pakety implicitne zakáže
ip access-group command links, pripája existujúci ACL na špecifické rozhranie
Príklad: Router(config-if)#ip access-group access-list-number {in | out}

11.2.3. Pomenované ACL

Sú od verzie CISCO IOS 1.12, umožňujú štandartným alebo rozšíreným ACL prideliť meno namiesto čísla.
Výhody pomenovaných ACL:

1. intuitívna identifikácia oproti číselnému pomenovaniu
2. odstránenie limitu 798 pri jednoduchom a 799 pri rozšírenom ACL
3. umožňujú zmenu konfigurácie bez zmazania aktuálnej, ale nový záznam sa vkladá až na koniec.
   Pri tvorbe pomenovaných ACL je vhodné použiť textový editor.

ip access-list command, vytvorenie ACL
Príklad:

```
Rt1(config)#ip access-list extended server-access
Rt1(config-ext-nacl)#permit TCP any host 131.108.101.99 eq
smtp
Rt1(config-ext-nacl)#permit UDP any host 131.108.101.99 eq
domain
Rt1(config-ext-nacl)#deny ip any any log
Rt1(config-ext-nacl)#^Z
Applying the named list:
Rt1(config)#interface fastethernet 0/0
Rt1(config-if)#ip access-group server-access out
Rt1(config-if)#^Z
```

Na hosta 131.108.101.99 povolí smtp (tcp port 25) a DNS (udp port 53), ostatné IP pakety zakáže; ACL aplikuje na trafik odchádzajúci cez rozhranie fastethernet0/0

11.2.4. Umiestnenie ACL

ALC sú využívané na kontrolovanie dopravy na sieti a na eliminovanie nežiadúcej dopravy na sieti.
Správnym umiestnením ACL sieť pracuje efektívnejšie.

11.2.5. Firewall

Slúži na ochranu internej siete proti votrelcom z vonkajšieho sveta. Typicky sieťový firewall pozostáva z niekoľkých rôznych zariadení, ktoré pracujú spoločne na zabránení nežiadúceho prístupu.
ACL môžu byť použité vo firewalloch, ktoré sú často umiestnené medzi vonkajšou a vnútornou sieťou, ako napr.
internet.
Firewally na okrajoch sieti výrazne prispievajú k zvýšeniu bezpečnosti.

11.2.6. Obmedzenie prístupu na virtuálne terminály

Štandartné alebo rozšírené ACL nie sú určené na filtrovanie telnetu. Je možné nastaviť ACL pre VTY, čím sa zvýši sieťová bezpečnosť.

access-group command, aplikovanie ACL na VTY

```
Creating the standard list:

Rtl(config)#access-list 2 permit 172.16.1.0 0.0.0.255
Rtl(config)#access-list 2 permit 172.16.2.0 0.0.0.255
Rtl(config)#access-list 2 deny any

Applying the access list:

Rtl(config)#line vty 0 4
Rtl(config)#login
Rtl(config)#password secret
Rtl(config)#access-class 2 in
```

Podmienky pri konfigurovaní ACL pre VTY:

1. môžu byť použité len číslované ACL
2. pre všetky VTY sa používajú rovnaké obmedzenia
3. môžeme definovať počet prihlásení

V tomto príklade sa cez telnet možno na smerovač prihlásiť len zo sietí 172.16.1.0/24 a 172.16.2.0/24