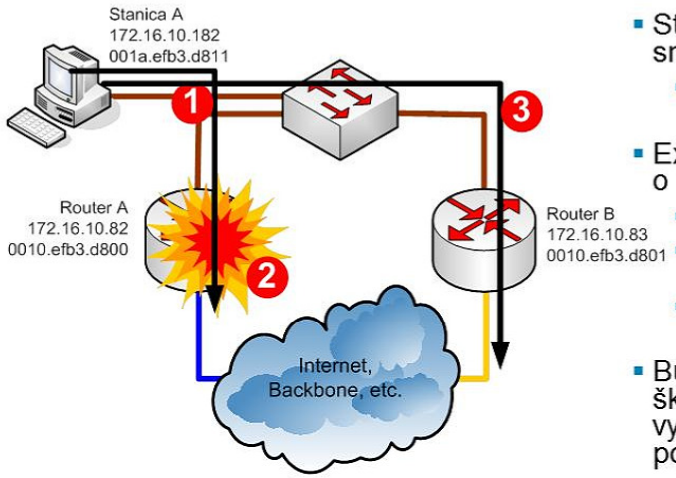
Stretnutie 5:

Niektoré protokoly pre redundanciu

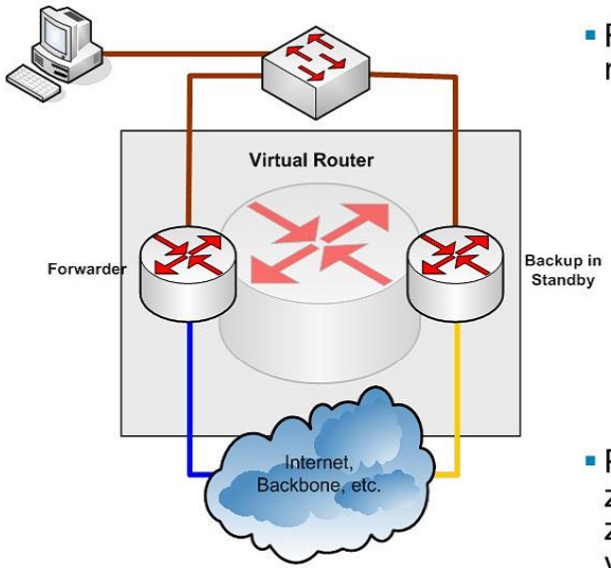
SWITCH Modul 5

L3 redundancia



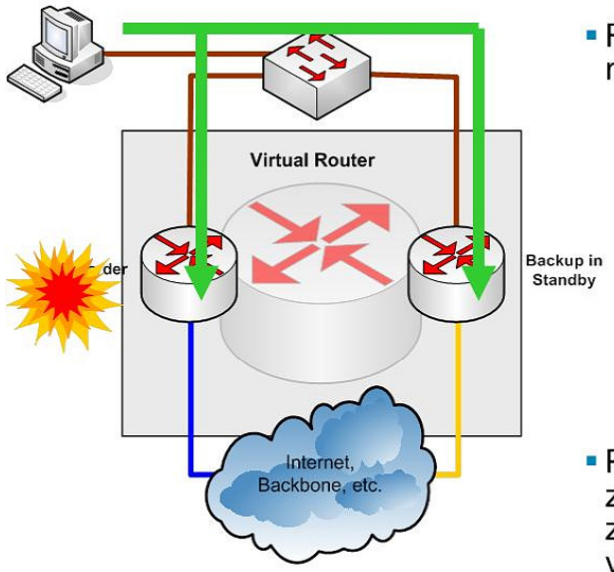
- Ak A padne, dynamické smerovanie začne využívať B
- Stanica však nepoužíva smerovací protokol
  - Obykle používa len jednu pridelenú IP brány
- Existujú viaceré pokusy o riešenie tohto problému
  - Proxy ARP
  - ICMP Router Discovery Protocol
  - Podpora smerovacieho protokolu v OS stanice
- Buď však nie sú tieto riešenia škálovateľné, alebo si vyžadujú osobitnú softvérovú podporu u klienta

Riešenie redundancie cez virtuálny router



- Routery môžu vytvárať ilúziu nového virtuálneho routera
  - Tento virtuálny router má svoju virtuálnu MAC a IP
  - Stanice budú používať túto vIP ako svoju bránu
  - Jeden z reálnych routerov bude nositeľom vMAC a vIP
  - Ak súčasný nositeľ virtuálnej identity prestane odpovedať, prevezme na seba vMAC a vIP ďalší router
- Pre stanice nebude táto zmena vôbec viditeľná, lebo z ich pohľadu sa vMAC ani vIP nezmenila

Riešenie redundancie cez virtuálny router



- Routery môžu vytvárať ilúziu nového virtuálneho routera
  - Tento virtuálny router má svoju virtuálnu MAC a IP
  - Stanice budú používať túto vIP ako svoju bránu
  - Jeden z reálnych routerov bude nositeľom vMAC a vIP
  - Ak súčasný nositeľ virtuálnej identity prestane odpovedať, prevezme na seba vMAC a vIP ďalší router
- Pre stanice nebude táto zmena vôbec viditeľná, lebo z ich pohľadu sa vMAC ani vIP nezmenila

Hot Standby Routing Protocol

Hot Standby Router Protocol (HSRP)

- HSRP je Cisco proprietárny protokol pre vytváranie virtuálnych routerov
  - Cisco Document ID: 10583, „Understanding and Troubleshooting HSRP Problems in Catalyst Switch Networks“
  - Cisco dokument: „Hot Standby Router Protocol Version 2“
- HSRP existuje v dvoch verziách:
  - HSRPv1 (RFC 2281)
    - Používa UDP/1985, pakety posiela na 224.0.0.2
    - Na jednom rozhraní dovoľuje vytvoriť maximálne 256 rôznych virtuálnych routerov
  - HSRPv2
    - Pakety posiela na 224.0.0.102, UDP/1985 je zachované
    - Na jednom rozhraní dovoľuje vytvoriť maximálne 4096 rôznych virtuálnych routerov
    - Podporuje časovače na úrovni milisekúnd
  - Predvolená verzia je 1

Pojmy v HSRP

- HSRP definuje tzv. standby group, ktorá obsahuje:
  - Active router
    - Nositeľ identity virtuálneho routera (vMAC, vIP)
    - Je zodpovedný za obsluhu paketov posielaných na identitu virtuálneho routera
    - V HSRP grupe je vždy iba jeden Active router
  - Standby router
    - Záložný router pre Active (podobne ako DR a BDR v OSPF)
    - Ak Active router prestane pracovať, Standby router preberie na seba vMAC a vIP
    - V HSRP grupe je vždy najviac jeden Standby router
  - Other routers
    - Ostatné routery v HSRP grupe, ktoré nie sú ani Active ani Standby. Monitorujú dostupnosť Active a Standby routerov. V prípade potreby vedia prejsť do roly Standby a následne Active.
  - Virtual router
    - Celá standby group

Činnosť HSRP – Active a Standby router

- Active router je nositeľom vMAC/vIP
  - Voľba prebieha na základe priority (0-255, predvolená hodnota je 100, vyššie číslo znamená vyššiu prioritu)
  - Ak sú priority rovnaké, vyhráva router s vyššou IP adresou
  - vIP adresa je daná konfiguráciou
  - vMAC adresa je odvodená od čísla HSRP grupy:
    - HSRPv1: 000.0c07.acxx, kde xx je číslo grupy v hexa tvare
    - HSRPv2: 0000.0C9F.Fxxx
- Standby router sa takisto volí na základe priority/vyššej IP
- Active a Standby posielajú Hello pakety
  - Informujú seba i všetky ostatné routery v grupe o svojej existencii
  - Ak Standby zistí, že Active router sa neozýva, prevezme na seba jeho funkcie a stane sa novým Active routerom
  - Ostatné routery v skupine neposielajú Hello, len monitorujú prítomnosť Active a Standby routera a v prípade potreby sa zúčastnia volieb na neobsadené pozície

HSRP stavy

- Init / Disabled
  - Router nie je schopný sa podieľať na činnosti grupy (napr. vypnuté rozhranie)
- Learn
  - Inicializácia HSRP, router sa snaží zistiť IP adresu virtuálneho routera a prítomnosť Active/Standby.
  - Router ešte nedostal Hello paket
- Listen (10 sec)
  - Router začal dostávať Hello správy
  - Monitoruje prítomnosť Active a Standby routera
- Speak (10 sec)
  - Router posiela a prijíma Hello správy
  - Podieľa sa na voľbe Standby alebo Active
- Standby
  - Pri neexistencii Standby sa obyčajný router označí za Standby
  - Pri existencii Active routera ostáva v Standby stave
  - Posiela Hello správy
  - Monitoruje prítomnosť Active routera
- Active
  - Pri neexistencii Active routra sa Standby router označí za Active
  - Posiela Hello správy
  - Privlastní si vMAC/vIP

HSRP časovače

Časovač	Popis
Active timer	Každý router v HSRP grupe monitoruje prítomnosť Active routera. Prijatím Hello paketu od Active routera sa nuluje časovač Active timer. Ak Active timer prekročí hodnotu Holdtime uvedenú v poslednom Hello pakete od Active routera, Standby router preberie funkciu Active.
Standby timer	Každý router v HSRP grupe okrem Active monitoruje prítomnosť Standby routera. Prijatím Hello paketu od Standby routera sa nuluje časovač Standby timer. Ak Standby timer prekročí hodnotu Holdtime uvedenú v poslednom Hello pakete od Active routera, musí sa spomedzi routerov zvoliť nový Standby.
Hello timer	Perióda posielania Hello paketov. Štandardne je 3s

HSRP multicast správy a preempcia

- Správa Hello
  - Posiela Active a Standby
  - Obsahujú informácie o virtuálnej adrese grupy, priorite a stave odosielateľa
- Správa Coup
  - Použité, ak router chce prevziať úlohu Active routera
  - Najčastejšie pri tzv. preemption
- Správa Resign
  - Použité, keď sa Active router zrieka svojej funkcie
- Preemption je schopnosť iného routera prevziať na seba úlohu Active routera, aj keď Active stále žije, avšak jeho priorita je menšia než priorita na Standby
  - Štandardne je preempcia vypnutá, v takej situácii Standby preberie na seba úlohu Active len vtedy, keď Active úplne odíde

Virtuálna IP adresa HSRP grupy

- HSRP grupa vytvára jeden virtuálny router s virtuálnou IP
  - Pri konfigurácii HSRP bude mať každý člen HSRP grupy nastavenú tú istú vIP adresu, lebo v ktoromkoľvek momente môže začať plniť úlohu Active routera
- vIP adresa musí byť z priestoru IP adries rozhrania, na ktorom HSRP spúšťame
  - V HSRP však táto vIP nesmie byť rovnaká ako skutočná IP adresa niektorého člena HSRP grupy
  - Odporúčané použitie
    - vIP je najnižšia, reálne routery majú najvyššie IP v sieti
    - vIP je najvyššia, reálne routery majú najnižšie IP v sieti

Elementárna konfigurácia a overenie HSRP

```
! Vytvára HSRP grupu na rozhraní
! Všetky členské routery musia mať rovnaké vIP a číslo grupy
! Default group je 0
Router(config-if)# standby [ group-number ] ip vIP
```

```
! Zruší HSRP na rozhraní
Router(config-if)# no standby group-number
```

```
! Zobrazenie info o HSRP
Router# show run
Router# show standby [ brief ]
Router# show standby [ interface [ group-number ] ] [ brief ]
```

Optimalizácia HSRP – priorita a preempt

```
! Nastavenie priority – ovplyvnenie volieb Active a Standby routera
! Štandardná priorita je 100
! Ak je zhoda priorít, vyhráva najvyššia IP adresa
Router(config-if)# standby group-number priority priority-value
```

```
! Návrat priority na predvolenú hodnotu
Router(config-if)# no standby group-number priority
```

```
! Povolenie, aby tento router mohol prevziať na seba úlohu Active
! routera okamžite vždy vtedy, keď jeho priorita bude vyššia než
! priorita dovtedajšieho Active routera
! Tento príkaz vlastne dovoľuje posielať správu Coup
Router(config-if)# standby group-number preempt
```

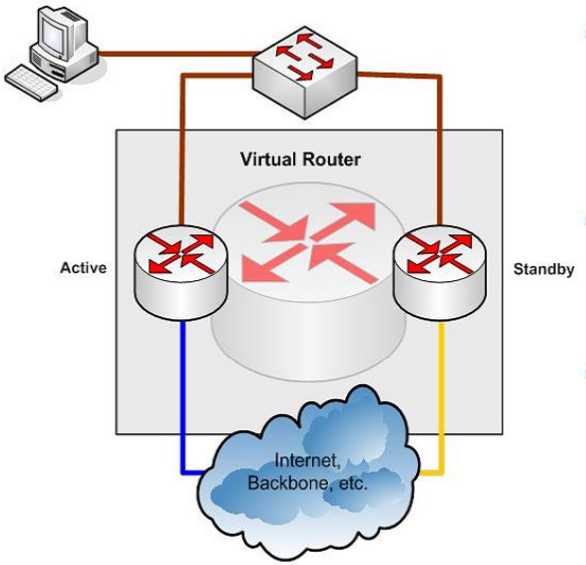
```
! Konfigurácia preempt, v ktorej tento router prevezme na seba úlohu
! Active až s istým oneskorením po tom, čo má právo byť novým Active
Router(config-if)# standby group-number preempt delay minimum SECONDS
```

```
! Konfigurácia preempt, v ktorej tento router po reštarte prevezme
! na seba úlohu Active až po istom oneskorení
Router(config-if)# standby group-number preempt delay reload SECONDS
```

Optimalizácia HSRP – časovače, verzia

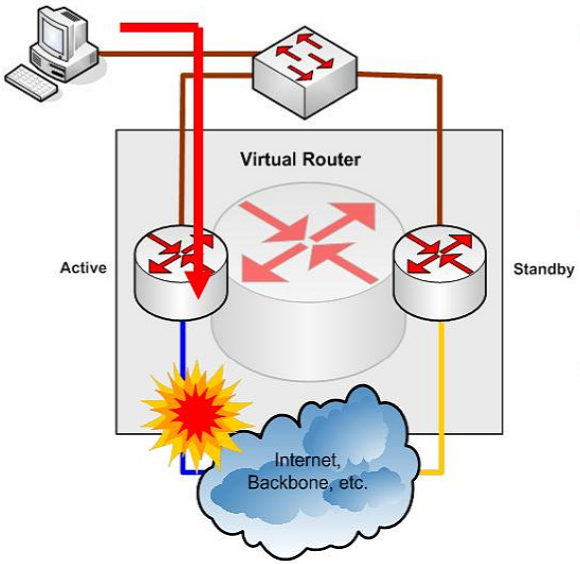
```
! Nastavenie časovačov, Hello štandardne 3s, Hold 10s
! Hold by mal byť aspoň 3x väčší ako Hello
! Rovnaké hodnoty by mali byť nastavené v celej HSRP grupe

Router(config-if)# standby group-number timers Hello Holddown

! Alebo v milisekundách (pre milisekundy sa odporúča HSRPv2,
! HSRPv1 nevie v Hello paketoch oznámiť milisekundové hodnoty)

Router(config-if)# standby group-number timers
                                  msec Hello msec Holddown

! Zmena verzie na 2 (musí byť na všetkých routeroch v grupe)
Router(config-if)# standby version 2
```

HSRP interface tracking



- Čo ak linka za aktívnym routrom spadla?
  - Na HSRP rozhraní je silne obmedzené používanie správ ICMP Redirect
- Potrebujeme možnosť, aby Active router opustil svoju rolu, ak kľúčové rozhranie prestane pracovať
- Riešením je tzv. interface alebo object tracking
  - Ak sledované rozhranie alebo iný objekt je vyhodnotený ako nefunkčný, zníži sa HSRP priorita routera o istú hodnotu

HSRP interface tracking



- Čo ak linka za aktívnym routrom spadla?
  - Na HSRP rozhraní je silne obmedzené používanie správ ICMP Redirect
- Potrebujeme možnosť, aby Active router opustil svoju rolu, ak kľúčové rozhranie prestane pracovať
- Riešením je tzv. interface alebo object tracking
  - Ak sledované rozhranie alebo iný objekt je vyhodnotený ako nefunkčný, zníži sa HSRP priorita routera o istú hodnotu

HSRP interface tracking – prvý spôsob

```
! Interface tracking
! Hodnota penalty vyjadruje, o koľko sa zníži naša HSRP priorita,
! ak je sledované rozhranie nefunkčné, štandardne 10
Router(config-if)# standby group-number track interface [ penalty ]
```

```
! Zrušenie interface tracking
Router(config-if)# no standby group-number track
```

Interface tracking (object tracking) – iný spôsob

```
Switch(config)# track object-number interface interface
                          { line-protocol | ip routing }
Switch(config-track)# exit

Switch(config)# interface ...
Switch(config-if)# standby group-number track object-number
                                  [ decrement penalty ]
```

```
DLS1(config)# track 100 interface Port-channel 1 line-protocol
DLS1(config-track)#exit
DLS1(config)# int vlan 20
DLS1(config-if)# standby 1 track 100 ?
  decrement  Priority decrement
  shutdown   Shutdown group
  <cr>

DLS1(config-if)# standby 1 track 100 decrement 60
```

HSRP autentifikácia

```
! Plain text autentifikácia
! Heslo ako clear text
Switch(config-if)# standby group-number authentication string
```

```
! MD5 autenfikácia
! Posiela sa MD5 hash z obsahu HSRP paketu a hesla
Switch(config-if)# standby group-number authentication md5
                                  key-string string
```

```
! MD5 autentifikácia s využitím key chain
Switch(config)# key chain chain-name
Switch(config-keychain)# key key-number
Switch(config-keychain-key)# key-string string

Switch(config)# interface ...
Switch(config-if)# standby group-number authentication md5
                                  key-chain chain-name
```

- Upozornenie: autentifikácia neprináša nijakú reálnu bezpečnosť
  - Dva HSRP routery s rôznymi heslami si navzájom ignorujú pakety a oba sa vyhlásia za Active, čo povedie ku konfliktu vIP/vMAC
  - vIP je možné (omylom či zámerne) nastaviť na akomkoľvek inom zariadení v sieti, čím takisto kompromitujeme činnosť HSRP grupy

Debug HSRP

```
DLS1# debug standby ?
  errors    HSRP errors
  events    HSRP events
  packets   HSRP packets
  terse     Display limited range of HSRP information
  <cr>
```

```
DLS1# debug standby terse
HSRP:
  HSRP Errors debugging is on
  HSRP Events debugging is on
    (protocol, neighbor, redundancy, track, ha, arp)
  HSRP Packets debugging is on
    (Coup, Resign)
```

debug standby – ukážka voľby Active

```
DLS1# debug standby
HSRP debugging is on
DLS1#

*Mar 8 20:34:10.221: SB11: Vl11 Init: a/HSRP enabled
*Mar 8 20:34:10.221: SB11: Vl11 Init -> Listen
*Mar 8 20:34:20.221: SB11: Vl11 Listen: c/Active timer expired (unknown)
*Mar 8 20:34:20.221: SB11: Vl11 Listen -> Speak
*Mar 8 20:34:20.221: SB11: Vl11 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:23.101: SB11: Vl11 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:25.961: SB11: Vl11 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:28.905: SB11: Vl11 Hello out 172.16.11.111 Speak pri 100 ip 172.16.11.115
*Mar 8 20:34:30.221: SB11: Vl11 Speak: d/Standby timer expired (unknown)
*Mar 8 20:34:30.221: SB11: Vl11 Standby router is local
*Mar 8 20:34:30.221: SB11: Vl11 Speak -> Standby
*Mar 8 20:34:30.221: SB11: Vl11 Hello out 172.16.11.111 Standby pri 100 ip 172.16.11.115
*Mar 8 20:34:30.221: SB11: Vl11 Standby: c/Active timer expired (unknown)
*Mar 8 20:34:30.221: SB11: Vl11 Active router is local
*Mar 8 20:34:30.221: SB11: Vl11 Standby router is unknown, was local
*Mar 8 20:34:30.221: SB11: Vl11 Standby -> Active
*Mar 8 20:34:30.221: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Standby -> Active
*Mar 8 20:34:30.221: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
```

debug standby – ukážka voľby Active pri preempt

```
DLS1# debug standby
*Mar 1 00:16:41.295: %SYS-5-CONFIG_I: Configured from console by console
*Mar 1 00:16:43.095: %LINK-3-UPDOWN: Interface Vlan11, changed state to up
*Mar 1 00:16:43.099: SB: Vl11 Interface up
*Mar 1 00:16:43.099: SB11: Vl11 Init: a/HSRP enabled
*Mar 1 00:16:43.099: SB11: Vl11 Init -> Listen
*Mar 1 00:16:43.295: SB11: Vl11 Hello in 172.16.11.112 Active pri 50 ip 172.16.11.115
*Mar 1 00:16:43.295: SB11: Vl11 Active router is 172.16.11.112
*Mar 1 00:16:43.295: SB11: Vl11 Listen: h/Hello rcvd from lower pri Active router (50/172.16.11.112)
*Mar 1 00:16:43.295: SB11: Vl11 Active router is local, was 172.16.11.112
*Mar 1 00:16:43.295: SB11: Vl11 Coup out 172.16.11.111 Listen pri 100 ip 172.16.11.115
 Mar 1 00:16:43.295
*Mar 1 00:16:43.299: %STANDBY-6-STATECHANGE: Vlan11 Group 11 state Listen -> Active
*Mar 1 00:16:43.299: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:43.303: SB11: Vl11 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:44.095: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan11, changed state to up
*Mar 1 00:16:46.187: SB11: Vl11 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:46.207: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:49.095: SB11: Vl11 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:49.195: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:52.079: SB11: Vl11 Hello in 172.16.11.112 Speak pri 50 ip 172.16.11.115
*Mar 1 00:16:52.147: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:53.303: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:16:53.303: SB11: Vl11 Standby router is 172.16.11.112
*Mar 1 00:16:55.083: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:56.231: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:16:58.023: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:16:59.223: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:17:00.983: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.115
*Mar 1 00:17:02.211: SB11: Vl11 Hello in 172.16.11.112 Standby pri 50 ip 172.16.11.115
*Mar 1 00:17:03.847: SB11: Vl11 Hello out 172.16.11.111 Active pri 100 ip 172.16.11.11
```

debug standby events

```
*Mar  3 05:38:28.502: HSRP: Vl10 Interface UP
*Mar  3 05:38:28.502: HSRP: Vl10 Starting minimum interface delay (1 secs)
*Mar  3 05:38:29.458: HSRP: Vl10 Grp 1 Active router is 172.16.10.102
*Mar  3 05:38:29.458: HSRP: Vl10 Nbr 172.16.10.102 is no longer passive
*Mar  3 05:38:29.458: HSRP: Vl10 Nbr 172.16.10.102 active for group 1
*Mar  3 05:38:29.500: HSRP: Vl10 Interface min delay expired
*Mar  3 05:38:29.500: HSRP: Vl10 Grp 1 Init: a/HSRP enabled
*Mar  3 05:38:29.500: HSRP: Vl10 Grp 1 Init -> Listen
*Mar  3 05:38:29.500: HSRP: Vl10 Grp 1 Redundancy "hsrp-Vl10-1" state Init -> Backup
*Mar  3 05:38:29.500: HSRP: Vl10 IP Redundancy "hsrp-Vl10-1" update, Init -> Backup
*Mar  3 05:38:30.507: %LINK-3-UPDOWN: Interface Vlan10, changed state to up
*Mar  3 05:38:30.515: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up
*Mar  3 05:38:32.260: HSRP: Vl10 Grp 1 Listen: h/Hello rcvd from lower pri Active router
(100/172.16.10.102)
*Mar  3 05:38:32.260: HSRP: Vl10 Grp 1 Active router is local, was 172.16.10.102
*Mar  3 05:38:32.260: HSRP: Vl10 Nbr 172.16.10.102 no longer active for group 1 (Listen)
*Mar  3 05:38:32.260: HSRP: Vl10 Nbr 172.16.10.102 Was active or standby - start passive holddown
*Mar  3 05:38:32.260: HSRP: Vl10 Grp 1 Listen -> Active
*Mar  3 05:38:32.260: %HSRP-5-STATECHANGE: Vlan10 Grp 1 state Listen -> Active
*Mar  3 05:38:32.260: HSRP: Vl10 Grp 1 Redundancy "hsrp-Vl10-1" state Backup -> Active
*Mar  3 05:38:32.260: HSRP: Vl10 Added 172.16.10.1 to ARP (0000.0c07.ac01)
*Mar  3 05:38:32.268: HSRP: Vl10 Grp 1 Activating MAC 0000.0c07.ac01
*Mar  3 05:38:32.268: HSRP: Vl10 Grp 1 Adding 0000.0c07.ac01 to MAC address filter
*Mar  3 05:38:32.268: HSRP: Vl10 IP Redundancy "hsrp-Vl10-1" update, Backup -> Active
*Mar  3 05:38:35.254: HSRP: Vl10 IP Redundancy "hsrp-Vl10-1" update, Active -> Active
*Mar  3 05:38:42.913: HSRP: Vl10 Grp 1 Standby router is 172.16.10.102
*Mar  3 05:38:42.913: HSRP: Vl10 Nbr 172.16.10.102 is no longer passive
*Mar  3 05:38:42.913: HSRP: Vl10 Nbr 172.16.10.102 standby for group 1
```

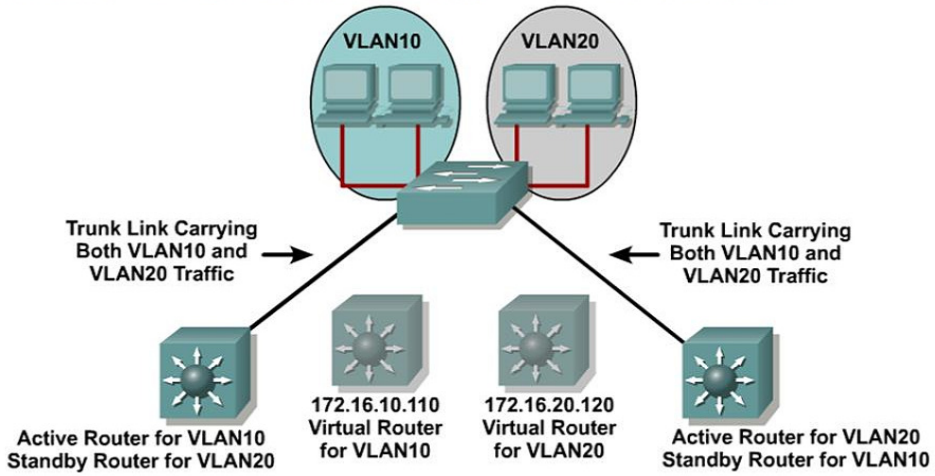
Diagnostika HSRP autentifikácie

```
Switch# debug standby errors
*Mar  3 05:40:49.606: HSRP: Vl1 Grp 1 Auth failed for Hello pkt
from 10.1.1.102, Text auth failed
*Mar  3 05:40:52.131: HSRP: Vl1 Grp 1 Auth failed for Hello pkt
from 10.1.1.102, Text auth failed
*Mar  3 05:40:54.715: HSRP: Vl1 Grp 1 Auth failed for Hello pkt
from 10.1.1.102, Text auth failed
```

Konfigurácia a overenie HSRP

- Koncová stanica by sa nemala dozvedieť fyzickú MAC alebo IP adresu aktívneho routera
  - Ak funkciu Active preberie iný router, znalosť fyzickej MAC adresy znemožní koncovej stanici začať transparentne používať nový Active router
  - Podobný problém môže spôsobiť znalosť reálnej IP adresy
- Aktivácia HSRP na rozhraní modifikuje správanie sa protokolov ICMP a ARP
  - Na aktívnom routeri Proxy ARP odpovedá pomocou vMAC, na ostatných routeroch v HSRP grupe je Proxy ARP vypnutý
  - Obsluha ICMP protokolu je podstatne zložitejšia, odporúčam detaily zistiť z „Cisco IOS IP Application Services Configuration Guide“ pre IOS 15.0M a novší

HSRP load balancing – tzv. MHSRP



To load balance routers and links:

- Per VLAN, configure the HSRP active router and the spanning tree root to be the same multilayer switch.

Príklad konfigurácie HSRP

Load Balance

```
Lavy(config)#interface FastEthernet0/0
Lavy(config)#no shut
Lavy(config)#interface FastEthernet0/0.1
Lavy(config-if)#encapsulation dot1Q 1 native
Lavy(config-if)#ip address 192.168.1.101
255.255.255.0
Lavy(config-if)#standby 1 priority 150
Lavy(config-if)#standby 1 ip 192.168.1.1
Lavy(config-if)#standby 1 preempt
Lavy(config-if)#standby 1 track fa 0/1 60
Lavy(config-if)#interface FastEthernet0/0.2
Lavy(config-if)#encapsulation dot1Q 2
Lavy(config-if)#ip address 192.168.2.101
255.255.255.0
Lavy(config-if)#standby 2 ip 192.168.2.1
Lavy(config-if)#standby 2 preeempt


Lavy(config-if)#interface FastEthernet0/1
Lavy(config-if)#ip address 10.0.0.1 255.0.0.0
Lavy(config-if)#exit
Lavy(config)#router rip
Lavy(config-router)#network 10.0.0.0
Lavy(config-router)#network 192.168.1.0
Lavy(config-router)#network 192.168.2.0
```

```
Pravy(config)#interface FastEthernet0/0
Pravy(config)#no shut
Pravy(config)#interface FastEthernet0/0.1
Pravy(config-if)#encapsulation dot1Q 1 native
Pravy(config-if)#ip address 192.168.1.102
255.255.255.0
Pravy(config-if)#standby 1 ip 192.168.1.1
Pravy(config-if)#standby 1 preempt


Pravy(config-if)#interface FastEthernet0/0.2
Pravy(config-if)#encapsulation dot1Q 2
Pravy(config-if)#ip address 192.168.2.102
255.255.255.0
Pravy(config-if)#standby 2 ip 192.168.2.1
Pravy(config-if)#standby 2 priority 150
Pravy(config-if)#standby 2 preempt
Pravy(config-if)#standby 2 track fa 0/1 60
Pravy(config-if)#interface FastEthernet0/1
Pravy(config-if)#ip address 10.0.0.2 255.0.0.0
Pravy(config-if)#exit
Pravy(config)#router rip
Pravy(config-router)#network 10.0.0.0
Pravy(config-router)#network 192.168.1.0
Pravy(config-router)#network 192.168.2.0
```

Overenie konfigurácie – sh standby brief

```
Lavy#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Fa0/0.1     1    150  P Active   local           192.168.1.102   192.168.1.1
Fa0/0.2     2    100  P Standby  192.168.2.102   local           192.168.2.1
```

```
Pravy#sh standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp  Prio P State    Active          Standby         Virtual IP
Fa0/0.1     1    100  P Standby  192.168.1.100   local           192.168.1.1
Fa0/0.2     2    150  P Active   local           192.168.2.100   192.168.2.1
```

Overenie konfigurácie – sh standby

```
Lavy#sh standby
FastEthernet0/0.1 - Group 1
  State is Active
    11 state changes, last state change 00:05:16
  Virtual IP address is 192.168.1.1
  Active virtual MAC address is 0000.0c07.ac01
    Local virtual MAC address is 0000.0c07.ac01 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.784 secs
  Preemption enabled
  Active router is local
  Standby router is 192.168.1.102, priority 100 (expires in 9.788 sec)
  Priority 150 (configured 150)
  IP redundancy name is "hsrp-Fa0/0.1-1" (default)
FastEthernet0/0.2 - Group 2
  State is Standby
    7 state changes, last state change 01:41:07
  Virtual IP address is 192.168.2.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 2.988 secs
  Preemption enabled
  Active router is 192.168.2.102, priority 150 (expires in 7.796 sec)
  Standby router is local
  Priority 100 (default 100)
  IP redundancy name is "hsrp-Fa0/0.2-2" (default)
```

Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol

- Otvorená alternatíva k proprietárnemu HSRP
  - IETF RFC 3768 – Verzia 2
  - IETF RFC 5798 – Verzia 3 (IPv4 + IPv6)
- Princíp činnosti je podobný HSRP
  - Množina navzájom zálohujúcich sa routerov sa nazýva VRRP Group a predstavuje virtuálny router s vlastnou vMAC a vIP
  - Nositeľ vMAC/vIP sa volá Master (ekvivalent Active)
    - Vo VRRP môže vIP byť zhodná s IP adresou niektorého člena grupy
    - Tento člen sa nazýva IP Address Owner a vždy vyhrá voľby na Master (bude ohlasovať prioritu 255), dokonca bez ohľadu na preempt
    - Ak sa používa len virtuálna IP, voľba prebieha na základe priority a vyššej IP adresy (konfigurovateľná priorita je od 1 do 254)
    - vMAC adresa virtual routra je 0000.5e00.01xx, kde xx je hexa číslo grupy
  - Všetky ostatné routery vo VRRP grupe sa nazývajú Backup
  - VRRP nemá koncept Standby routera

VRRP činnosť

Step	Description	Notes
1	Router A is currently the master, so it is sending advertisements by default every 1 second.	Router A is the only device sending advertisements.
2	Router A fails.	Advertisements stop.
3	Router B and Router C stop receiving advertisements and wait for their respective master down interval to expire before transitioning to the master state.	By default, the master down interval is 3 seconds plus the skew time.
4	Because the skew time is inversely proportional to priority, the master down interval of Router B is less than that of Router C. Router B has a master down interval of approximately 3.2 seconds. Router C has a master down interval of approximately 3.6 seconds.	The skew time for Router B equals. (256 – 200) / 256, which is approximately equal to 0.2 seconds. The skew time for Router C equals. (256 – 100) / 256, which is approximately equal to 0.6 seconds.
5	Router B transitions to the master state after 3.2 seconds and starts sending advertisements.	
6	Router C receives the advertisement from the new master, so it resets its master down interval and remains in the backup state.	

- Master router posiela tzv. advertisements
  - IP 224.0.0.18, protokol 112, interval 1s
- Ak sa Master zrieka svojej úlohy
  - Pošle advertisement s prioritou 0 (ako Resign)
  - Backup s najvyššou prioritou preberie úlohu Master po čase skew time
- Ak Master odíde náhle, použijeme časovače
  - Advertisement interval: 1s
  - Master down interval:
    - Čas, po uplynutí ktorého považujeme Master router za nefunkčný
    - 3x Advertisement Interval + skew time
  - Skew time
    - (256 - priority) / 256 s
- Preempt je vo VRRP štandardne zapnutý

Konfigurácia VRRP

```
! Switch A
SwitchA(config)# interface vlan10
SwitchA(config-if)# ip address 10.1.10.5 255.255.255.0

! Textový popis (nepovinný)
SwitchA(config-if)# vrrp 10 description POPIS GRUPY

! Virtual IP pre grupu 10
SwitchA(config-if)# vrrp 10 ip 10.1.10.1

! Priorita pre router a pre grupu 10 (štandardná priorita je 100)
SwitchA(config-if)# vrrp 10 priority 150

! Preempt
SwitchA(config-if)# vrrp 10 preempt delay minimum 380

! Advertisement timer
SwitchA(config-if)# vrrp 10 timer advertise 4

! Časovače všetkých routerov v grupe musia byť identické,
! inak si navzájom nebudú akceptovať Advertisement správy
! a každý z nich sa vyhlási za Master router
```

Overenie a diagnostika VRRP

```
Switch# show vrrp
Switch# show vrrp all
Switch# show vrrp GROUP_NUM
```

```
Switch# debug vrrp all
Switch# debug vrrp error
Switch# debug vrrp events
Switch# debug vrrp packets
Switch# debug vrrp state
```

Interface tracking (object tracking)

```
! Monitorovanie stavu rozhrania
track 1 interface Serial0/1 line-protocol
!
interface Ethernet1/0
 ip address 10.0.0.2 255.0.0.0
 vrrp 1 ip 10.0.0.3
 vrrp 1 priority 120
 vrrp 1 track 1 decrement 25
```

VRRP autentifikácia

- Autentifikácia vo všetkých troch formách (plaintext, MD5 heslo, MD5 kľúčenka) sa konfiguruje vo VRRP analogicky ako v HSRP
  - Autentifikácia je vo VRRP rovnako nezmyselná ako v HSRP
- RFC 3768 cielene podporu autentifikácie z VRRP vypustilo s peknou analýzou, prečo je zbytočná
  - Cisco zatiaľ stále autentifikáciu podporuje

Diagnostika VRRP autentifikácie

```
Switch# show vrrp


Ethernet0/1 - Group 1
State is Master
Virtual IP address is 10.21.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 1.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority is 100
  Authentication MD5, key-string
Master Router is 10.21.0.1 (local), priority is 100
Master Advertisement interval is 1.000 sec
Master Down interval is 3.609 sec
```

Diagnostika VRRP autentifikácie

```
Router1#: debug vrrp authentication


VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1


VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: B861CBF1B9026130DD34AED849BEC8A1
VRRP: HshR: C5E193C6D84533FDC750F85FCFB051E1
VRRP: Grp 1 Adv from 172.24.1.2 has failed MD5 auth


Router2#: debug vrrp authentication


VRRP: Sent: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1


VRRP: Rcvd: 21016401FE050000AC1801FE0000000000000000
VRRP: HshC: C5E193C6D84533FDC750F85FCFB051E1
VRRP: HshR: B861CBF1B9026130DD34AED849BEC8A1
VRRP: Grp 1 Adv from 172.24.1.1 has failed MD5 auth
```

Gateway Load Balancing Protocol

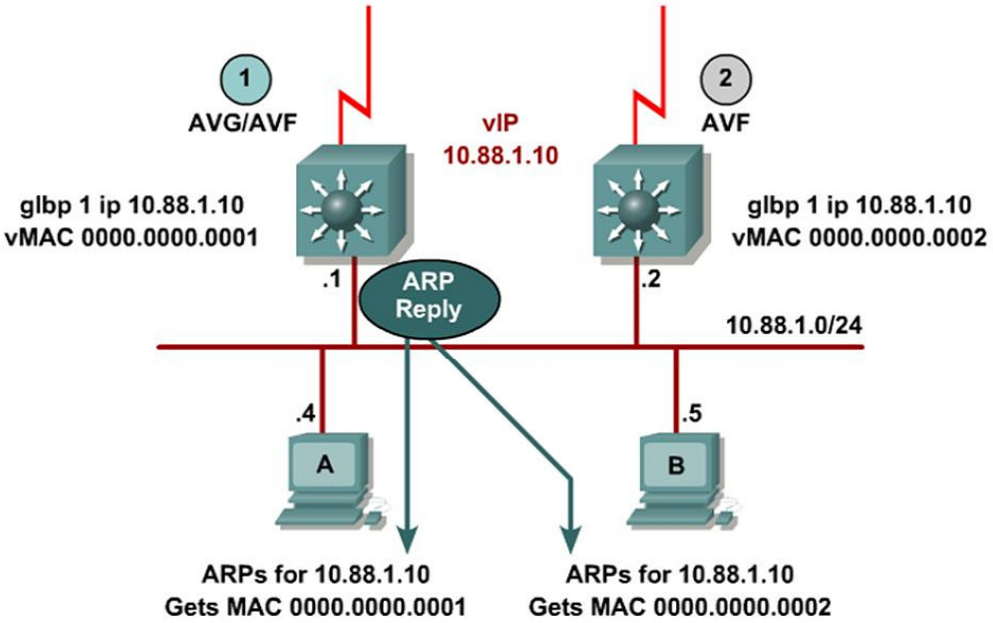
Gateway Load Balancing Protocol

- Cieľom GLBP (U.S. Patent 7881208) je vylepšenie HSRP s cieľom využiť pôvodne neaktívne routery
  - Routery Standby a Other v HSRP bežia a sú plnohodnotné, avšak keďže nie sú nositeľmi vMAC/vIP, stanice ich nevyužívajú
  - Dajú sa robiť rôzne triky, ako nad jednou IP sieťou vytvoriť niekoľko HSRP/VRRP grúp a klientov medzi tieto grupy rozdeliť
  - Tieto triky sú však v konečnom dôsledku statické a pomerne neobratné
- GLPB vychádza z HSRP a jeho ideou je využiť súbežne viacerých členov GLBP grupy pre poskytovanie smerovacích služieb
- Na to GLBP používa
  - Jednu vIP pre grupu
  - Viaceré, najviac 4, vMAC na grupu

GLBP – Základné bloky

- GLBP grupa má dva druhy členov: Active Virtual Gateway (AVG) a Active Virtual Forwarder (AVF)
- Active virtual gateway (AVG)
  - Zvolený ako router s najvyššou prioritou, prípadne najvyššou IP
  - Na jednu GLBP grupu pripadá práve jeden AVG
  - Úlohou AVG je prideliť ďalším členom GLBP grupy rôzne vMAC adresy k tej istej vIP a odpovedať klientom na ARP žiadosti na vIP
    - Dispečer grupy: keď príde žiadosť o preklad vIP na vMAC, AVG vráti klientovi niektorú z vMAC, ktorú pridelil
- Active virtual forwarder (AVF)
  - Maximálne 4 na grupu (ak je routerov viac, sú v tichom režime Backup AVF)
  - AVF sú zodpovední za im pridelenú vMAC/vIP
  - AVG je zároveň AVF
  - Každý AVG/AVF posiela Hello messages každé 3 sekundy na adresu 224.0.0.102, UDP/3222
- Všetky routery v GLBP grupe sa navzájom zálohujú (AVG aj AVF)

GLBP činnosť



GLBP mechanizmy rozkladania záťaže

- GLBP podporuje 3 mechanizmy rozkladania záťaže:
  - Vážený round-robin (Weighted load-balancing algorithm)
    - Objem prevádzky pripadajúci na AVF je úmerný váhe, ktorú tento AVF ohlasuje
  - Per-host (Host-dependent load-balancing algorithm)
    - Konkrétna koncová stanica používa vždy ten istý AVF
  - Round-robin load-balancing algorithm (predvolený)
    - Na ARP otázky klientov AVG odpovedá cyklickým striedaním pridelených vMAC

Konfigurácia GLBP

```
! Bežná IP adresa rozhrania
Switch(config-if)# ip address ip-address mask [secondary]

! vIP adresa
Switch(config-if)# glbp group-number ip [ip-address [secondary]]

! Priorita
Switch(config-if)# glbp group-number priority level

! Preempcia pre AVG (štandardne vypnutá)
Switch(config-if)# glbp group-number preempt [delay min seconds]

! Preempcia pre AVF (štandardne zapnutá)
Switch(config-if)# glbp group-number forwarder preempt
                                    [delay min seconds]

! Časovače
Switch(config-if)# glbp group-number timers [msec] hellotime
                                    [msec] holdtime

! Typ load-balance
Switch(config-if)# glbp group-number load-balancing
              { host-dependent | round-robin | weighted }
```

GLBP Objekt tracking a weighting

- Rieši situáciu, kedy sa má AVF vzdať svojej úlohy

```
Switch(config)# track object-number interface interface
                                    {line-protocol | ip routing}
Switch(config-track)# exit
Switch(config)# interface type number
Switch(config-if)# glbp group weighting maximum [lower lower] [upper upper]
Switch(config-if)# glbp group weighting track object-number [decrement
value]
Switch(config-if)# glbp group forwarder preempt [delay minimum seconds]
Switch(config-if)# end
```

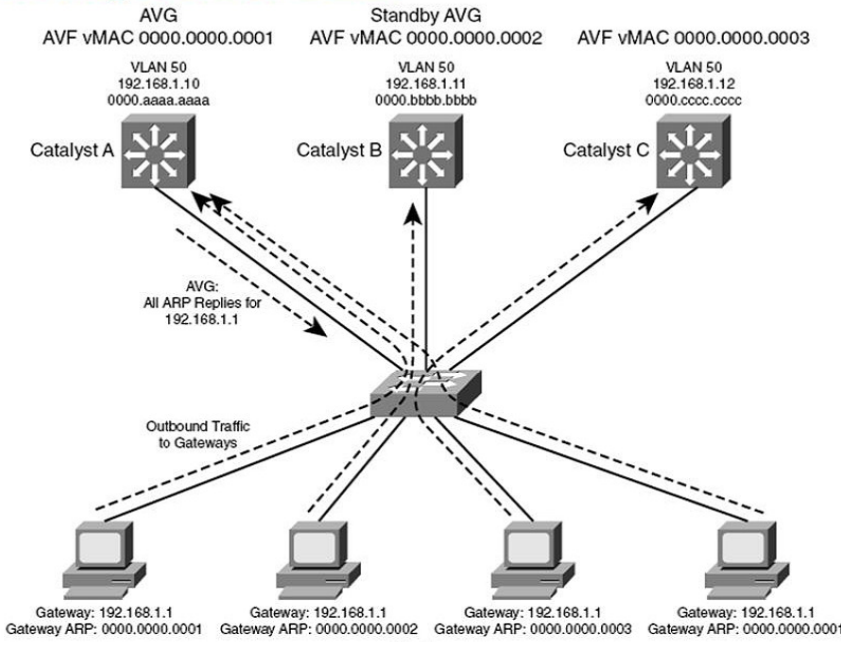
```
Switch# configure terminal
Switch(config)# track 2 interface Port-channel 1 line-protocol
Switch(config-track)# exit
Switch(config)# interface vlan 10
Switch(config-if)# glbp 10 weighting 110 lower 95 upper 105
Switch(config-if)# glbp 10 weighting track 2 decrement 20
Switch(config-if)# glbp 10 forwarder preempt delay minimum 60
Switch(config-if)# end
```

Overenie a diagnostika GLBP

```
Switch# show glbp
Switch# show glbp brief
Switch# show glbp GROUP_NUM
```

```
Switch# debug glbp error
Switch# debug glbp events
Switch# debug glbp packets
Switch# debug glbp terse
```

Konfigurácia GLBP



Konfigurácia – príklad

```
CatalystA(config)# interface vlan 50
CatalystA(config-if)# ip address 192.168.1.10 255.255.255.0
CatalystA(config-if)# glbp 1 priority 200
CatalystA(config-if)# glbp 1 preempt
CatalystA(config-if)# glbp 1 ip 192.168.1.1
-----------------------------------------------------------
CatalystB(config)# interface vlan 50
CatalystB(config-if)# ip address 192.168.1.11 255.255.255.0
CatalystB(config-if)# glbp 1 priority 150
CatalystB(config-if)# glbp 1 preempt
CatalystB(config-if)# glbp 1 ip 192.168.1.1
-----------------------------------------------------------
CatalystC(config)# interface vlan 50
CatalystC(config-if)# ip address 192.168.1.12 255.255.255.0
CatalystC(config-if)# glbp 1 priority 100
CatalystC(config-if)# glbp 1 ip 192.168.1.1
```

Overenie – príklad

```
CatalystA# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl50        1    -   200 Active   192.168.1.1     local           192.168.1.11
Vl50        1    1   7   Active   0007.b400.0101  local           -
Vl50        1    2   7   Listen   0007.b400.0102  192.168.1.11    -
Vl50        1    3   7   Listen   0007.b400.0103  192.168.1.13    -
CatalystB# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl50        1    -   150 Standby  192.168.1.1     192.168.1.10    local
Vl50        1    1   7   Listen   0007.b400.0101  192.168.1.10    -
Vl50        1    2   7   Active   0007.b400.0102  local           -
Vl50        1    3   7   Listen   0007.b400.0103  192.168.1.13    -
CatalystB#
CatalystC# show glbp brief
Interface   Grp  Fwd Pri State    Address         Active router   Standby router
Vl50        1    -   100 Listen   192.168.1.1     192.168.1.10    192.168.1.11
Vl50        1    1   7   Listen   0007.b400.0101  192.168.1.10    -
Vl50        1    2   7   Listen   0007.b400.0102  192.168.1.11    -
Vl50        1    3   7   Active   0007.b400.0103  local           -
CatalystC#
```

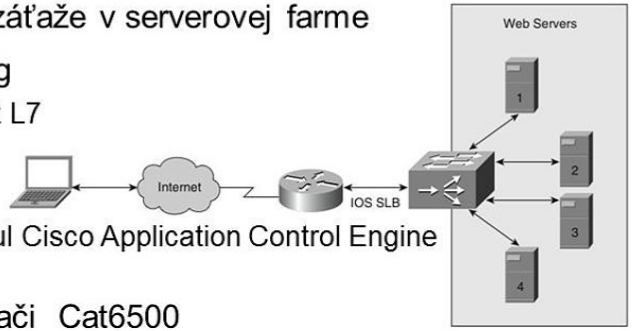
Výpis `show glbp` na CatalystA

```
CatalystA# show glbp
Vlan50 - Group 1
State is Active
7 state changes, last state change 03:28:05
Virtual IP address is 192.168.1.1
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.672 secs
Redirect time 600 sec, forwarder time-out 14400 sec
Preemption enabled, min delay 0 sec
Active is local
Standby is 192.168.1.11, priority 150 (expires in 9.632 sec)
Priority 200 (configured)
Weighting 100 (default 100), thresholds: lower 1, upper 100
Load balancing: round-robin
There are 3 forwarders (1 active)
Forwarder 1
State is Active
3 state changes, last state change 03:27:37
MAC address is 0007.b400.0101 (default)
…
…
```

IOS Server Load Balancing

Server Load Balancing

- SLB poskytuje rozklad záťaže v serverovej farme
- SLB vykonáva balancing
  - Podľa informácii z L4 až L7
  - Sofvérovo
  - Hardvérovo
    - Je vyžadovaný modul Cisco Application Control Engine (ACE)
- Dostupné len na prepínači Cat6500
- Výhody
  - Znížená záťaž na individuálne servery
  - Zvýšená bezpečnosť, lebo reálna IP adresa serverov nemusí byť viditeľná
  - Zníženie času nedostupnosti pri nasadení viac serverov



Pracovné režimy Cisco IOS SLB

- **Dispatched mode**
  - Každý server vo farme má svoju reálnu adresu a naviac virtuálnu adresu celej farmy – konfigurovaná na Loopbacku alebo ako sekundárna IP
  - Presmerovanie sa deje vložením paketu idúceho na virtuálnu IP do rámca adresovaného MAC adrese konkrétneho reálneho servera
  - V tomto režime musia byť servery spolu so SLB v spoločnej sieti
- **Directed mode**
  - Každý server vo farme má iba svoju reálnu adresu
  - Virtuálna adresa celej farmy je serverom neznáma
  - SLB realizuje NAT tak, že prepisuje cieľovú virtuálnu IP na adresu konkrétneho reálneho servera

Konfigurácia serverovej farmy v dátovom centre s reálnymi servermi

- Krok 1. Definuje serverovú farmu:

```
Switch(config)# ip slb serverfarm SERVERFARM-NAME
```

- Krok 2. Pridá reálny server do serverovej farmy:

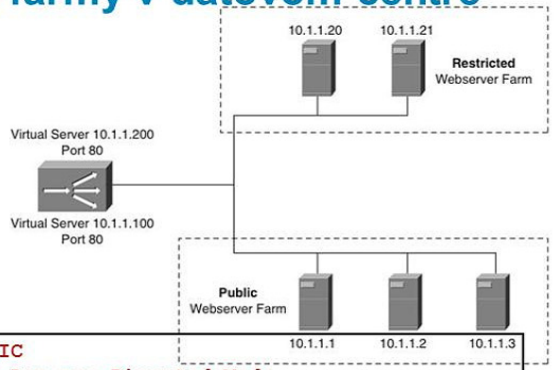
```
Switch(config-slb-sfarm)# real A.B.C.D
```

- Krok 3. Povolí používanie reálneho servera vo farme:

```
Switch(config-slb-real)# inservice
```

Konfigurácia serverovej farmy v dátovom centre s reálnymi servermi (2)

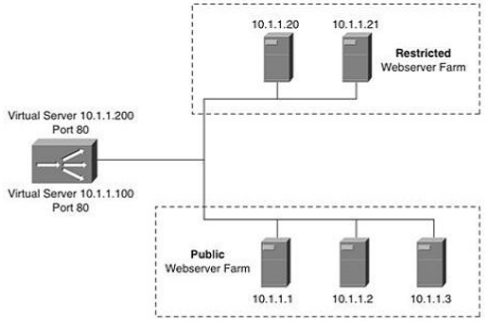
- Dve farmy v dátovom centre, PUBLIC a RESTRICTED
- PUBLIC: tri reálne servery: 10.1.1.1, 10.1.1.2 a 10.1.1.3
- RESTRICTED: dva reálne servery: 10.1.1.20 a 10.1.1.21




```
Switch(config)# ip slb serverfarm PUBLIC
Switch(config-slb-sfarm)# nat server ! Len pre Directed Mode
Switch(config-slb-sfarm)# real 10.1.1.1
Switch(config-slb-real)# inservice
Switch(config-slb-real)# real 10.1.1.2
Switch(config-slb-real)# inservice
Switch(config-slb-real)# real 10.1.1.3
Switch(config-slb-real)# inservice
!
Switch(config)# ip slb serverfarm RESTRICTED
Switch(config-slb-sfarm)# nat server ! Len pre Directed Mode
Switch(config-slb-sfarm)# real 10.1.1.20
Switch(config-slb-real)# inservice
Switch(config-slb-real)# real 10.1.1.21
Switch(config-slb-real)# inservice
```

Diagnostika SLB

- Zobrazenie stavu a konfigurácie serverových fariem
  - Asociované reálne servery
  - Stav reálnych serverov
  - Systém rozkladania záťaže
  - Počet obsluhovaných spojení




```
Switch# show ip slb real
real            farm name       weight  state          cons
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
10.1.1.1        PUBLIC          8       OPERATIONAL    0
10.1.1.2        PUBLIC          8       OPERATIONAL    0
10.1.1.3        PUBLIC          8       OPERATIONAL    0
10.1.1.20       RESTRICTED      8       OPERATIONAL    0
10.1.1.21       RESTRICTED      8       OPERATIONAL    0

Switch# show ip slb serverfarm
server farm     predictor       nat     reals   bind id
- - - - - - - - - - - - - - - - - - - - - - - - - - - -
PUBLIC          ROUNDROBIN      none    3       0
RESTRICTED      ROUNDROBIN      none    2       0
```

Konfigurácia serverovej farmy v dátovom centre s virtuálnymi servermi (1)

- **Krok1.** Definuje virtuálny server:

  `Switch(config)# ip slb vserver vserver-name`

- **Krok 2.** Nastaví IP adresu virtuálneho servera:

  `Switch(config-slb-vserver)# virtual ip-address [network-mask] {tcp | udp} [port-number | wsp | wsp-wtp | wsp-wtls | wsp-wtp-wtls] [service service-name]`

- **Krok 3.** Asociuje serverovú farmu k virtuálnemu serveru:

  `Switch(config-slb-vserver)# serverfarm primary-serverfarm-name [backup backup-serverfarm-name [sticky]]`

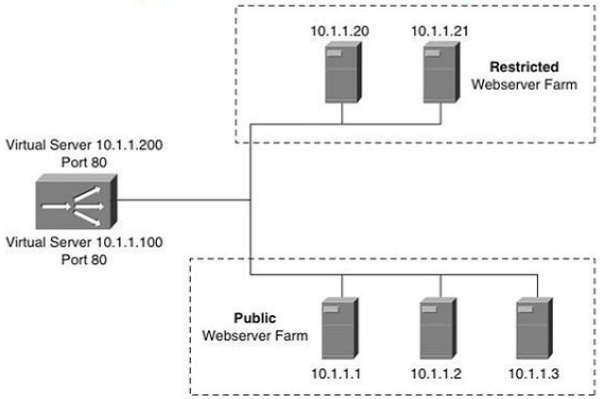
- **Krok 4.** Povolí virtuálny server

  `Switch(config-slb-vserver)# inservice`

- **Krok 5.** Špecifikuje klientov, ktorí majú prístup na virtuálny server:

  `Switch(config-slb-vserver)# client ip-address network-mask`

Konfigurácia serverovej farmy v dátovom centre s virtuálnymi servermi (2)




```
Switch(config)# ip slb vserver PUBLIC_HTTP
Switch(config-slb-vserver)# virtual 10.1.1.100 tcp www
Switch(config-slb-vserver)# serverfarm PUBLIC
Switch(config-slb-vserver)# inservice
Switch(config)# ip slb vserver RESTRICTED_HTTP
Switch(config-slb-vserver)# virtual 10.1.1.200 tcp www
Switch(config-slb-vserver)# client 10.4.4.0 255.255.255.0
Switch(config-slb-vserver)# serverfarm RESTRICTED
Switch(config-slb-vserver)# inservice
```

Overenie

```
! Verifikacia konfiguracie
Switch# show ip slb vserver
slb vserver      prot    virtual          state           cons
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
PUBLIC_HTTP      TCP     10.1.1.100:80    OPERATIONAL     0
RESTRICTED_HTTP  TCP     10.1.1.200:80    OPERATIONAL     0


! Stav spojenia
Switch# show ip slb connections
vserver          prot    client          real            state           nat
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
RESTRICTED_HTTP  TCP     10.4.4.0:80     10.1.1.20       CLOSING         none
```

Overenie

- Zobrazenie detailných info o stave omedzeného prístupu klienta restricted

```
show ip slb connections client
```

- Zobrazenie štatistík

```
show ip slb stats
```

```
Switch# show ip slb connections client 10.4.4.0 detail
VSTEST_UDP, client = 10.4.4.0:80
state = CLOSING, real = 10.1.1.20, nat = none
v_ip = 10.1.1.200:80, TCP, service = NONE
client_syns = 0, sticky = FALSE, flows attached = 0

Switch# show ip slb stats
Pkts via normal switching: 0
Pkts via special switching: 6
Connections Created: 1
Connections Established: 1
Connections Destroyed: 0
Connections Reassigned: 0
Zombie Count: 0
Connections Reused: 0
```

IP Service Level Agreements

IP Service Level Agreements

- Cisco IOS IP Service Level Agreements (SLAs) slúžia na aktívny monitoring činnosti siete
- Cisco IOS IP SLAs testy prenášajú sieťou simulované dáta a merajú parametre ich prenosu
  - Je možné stanoviť, aké hodnoty meraných parametrov musia byť splnené, aby bol test považovaný za úspešný
- IP SLA testy je možné realizovať medzi
  - Dvojicou Cisco zariadení
  - Cisco zariadením a bežným IP uzlom (testy budú obmedzené na verifikáciu IP aplikácií a služieb)

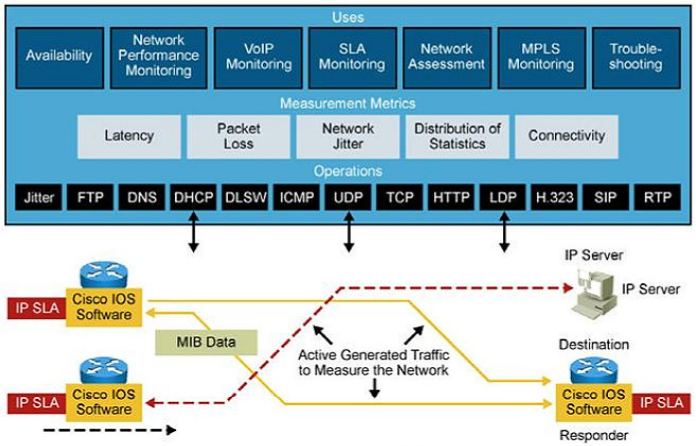
Cisco IOS IP SLAs

- Medzi merané parametre patria:
  - Dostupnosť sieťovej služby
  - Čas odpovede (response time)
  - Jednosmerné oneskorenie (One-way latency)
  - Jitter (kolísanie oneskorenia)
  - Stratovosť paketov
  - Hodnotenie kvality hlasu
  - Aplikačný výkon

Zdroje, respondenti a operácie v IP SLA

- IP SLA zdroj (source) posiela testovaciu prevádzku na stanovený cieľ
  - Všetky testy sú konfigurované na SLA zdroji
  - SLA zdroj využíva samostatný riadiaci protokol pre komunikáciu s respondentom ešte pred začiatkom testu (dohodnutie TCP/UDP portov, typ testu, získanie výsledkov atď.). Správy tohto protokolu môžu byť autentifikované pomocou MD5.
  - Najmä pre časové charakteristiky je nutné, aby zdroj a respondent boli časovo synchronizovaní (NTP)
- IP SLA respondent (responder), ktorý je súčasťou IOSu, je komponent na cieli testovacej prevádzky, ktorý slúži na koordináciu prebiehajúceho testu s IP SLA zdrojom
- IP SLA operácia (operation) je meranie, ktorého súčasťou je protokol, frekvencia a prahové hodnoty parametrov

IP SLA operácie



- IP SLA voči zariadeniu, na ktorom nebeží SLA respondent (web server alebo IP stanica)
  - Obvykle sú to testy bežného aplikačného protokolu alebo ping
- IP SLA voči zariadeniu, na ktorom beží SLA respondent (napr. Cisco router)
  - Je možné realizovať dodatočné testy, prípadne získavať presnejšie výsledky

Konfigurácia IP SLAs

- Definovať aspoň jednu SLA operáciu (test, tzv. probe)
- Definovať aspoň jeden tzv. tracking object, ktorý bude reprezentovať úspech alebo neúspech SLA operácie
- Definovať akciu asociovanú s tracking object-om

- Pozor:
  - Počnúc verziou IOSu 12.4(4)T, 12.2(33)SB a 12.2(33)SXI sa príkaz **`ip sla monitor`** nahrádza príkazom **`ip sla`**

Vytvorenie IP SLA operácie

- Vytvorenie IP SLA operácie

```
Router(config)#
ip sla operation-number ! alebo: ip sla monitor operation-number
```

- Parameter *`operation-number`* je ID operácie (ľubovoľné)

```
R1(config)# ip sla 1 ! Alebo: ip sla monitor 1
R1(config-ip-sla)# ?
IP SLAs entry configuration commands:
  dhcp          DHCP Operation
  dns           DNS Query Operation
  exit          Exit Operation Configuration
  icmp-echo     ICMP Echo Operation ! alebo: type echo protocol ipIcmpEcho
  icmp-jitter   ICMP Jitter Operation
  ! Skrátené kvôli stručnosti
R1(config-ip-sla)#
```

Defining an IP SLAs ICMP Echo Operation

- Definovanie ping operácie voči non-responder cieľu

```
Router(config-ip-sla)#
icmp-echo {destination-ip-address | destination-hostname} [source-
  ip {ip-address | hostname} | source-interface interface-name]
```

Parameter	Popis
destination-ip-address | *destination-hostname*	Cieľová IPv4/IPv6 adresa
source-ip *{ip-address | hostname}*	(Nepovinné) Stanovuje zdrojovú IPv4/IPv6 adresu
source-interface *interface-name*	(Nepovinné) Stanovuje rozhranie, z ktorého sa požičia zdrojová IPv4/IPv6 adresa

Pozor:

- Počnúc verziou IOSu 12.4(4)T, 12.2(33)SB a 12.2(33)SXI sa príkaz **type echo protocol ipIcmpEcho** nahrádza príkazom **icmp-echo**

icmp-echo – nastavenie detailov

```
R1(config-ip-sla)# icmp-echo 209.165.201.30
R1(config-ip-sla-echo)# ?

IP SLAs echo Configuration Commands:
  default             Set a command to its defaults
  exit                Exit operation configuration
  frequency           Frequency of an operation
  history             History and Distribution Data
  no                  Negate a command or set its defaults
  owner               Owner of Entry
  request-data-size   Request data size
  tag                 User defined tag
  threshold           Operation threshold in milliseconds
  timeout             Timeout of an operation
  tos                 Type Of Service
  verify-data         Verify data
  vrf                 Configure IP SLAs for a VPN Routing/Forwarding in-stance

R1(config-ip-sla-echo)#
```

- Existuje množstvo parametrov, avšak pre nás sú teraz podstatné len parametre **frequency** a **timeout**

icmp-echo – nastavenie detailov

```
Router(config-ip-sla-echo)#
frequency seconds
```

- Stanovuje, ako často sa operácia bude opakovať
  - Parameter *seconds* udáva počet sekúnd medzi dvomi behmi tejto operácie. Štandardná hodnota je 60 sekúnd.

```
Router(config-ip-sla-echo)#
timeout milliseconds
```

- Stanovuje čas, do ktorého SLA operácia očakáva odpoveď na odoslanú žiadosť

Naplánovanie SLA operácie

- IP SLA operáciu je potrebné naplánovať

```
Router(config)#
ip sla schedule operation-number [life {forever | seconds}]
  [start-time {hh:mm[:ss] [month day | day month] | pending |
  now | after hh:mm:ss}] [ageout seconds] [recurring]]
```

Pozor:

- Počnúc verziou IOSu 12.4(4)T, 12.2(33)SB a 12.2(33)SXI sa príkaz **ip sla monitor schedule** nahrádza príkazom **ip sla schedule**

Vytvorenie tracking object-u

- Vytvoriť tracking object, ktorý bude vyhodnocovať výsledok IP SLA operácie

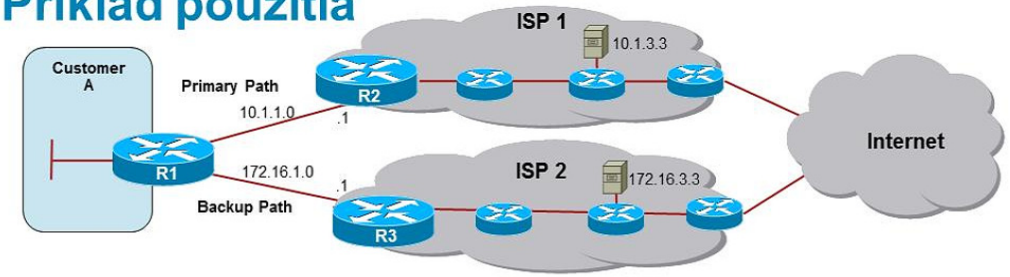
```
Router(config)#
track object-number ip sla operation-number {state |
 reachability}
```

Parameter	Popis
object-number	Číslo tracking object-u od 1 do 500 (ľubovoľné)
operation-number	Číslo SLA operácie, ktorej stav bude tento tracking object uchovávať.
state	Uchováva návratový kód (OK, OverThreshold, ...)
reachability	Uchováva všeobecnú úspešnosť

Pozor:

- Počnúc verziou IOSu 12.4(20)T, 12.2(33)SXI1 a 12.2(33)SRE je príkaz `track rtr` nahradený príkazom `track ip sla`

Príklad použitia

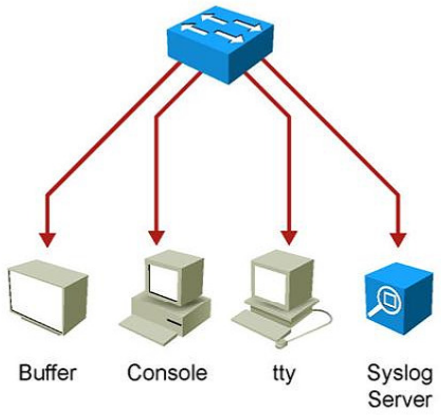



```
R1(config)# ip sla 11
R1(config-ip-sla)# icmp-echo 10.1.3.3
R1(config-ip-sla-echo)# frequency 10
R1(config-ip-sla-echo)# exit ! 2x
R1(config)# ip sla 22
R1(config-ip-sla)# icmp-echo 172.16.3.3
R1(config-ip-sla-echo)# frequency 10
R1(config-ip-sla-echo)# exit ! 2x
R1(config)# track 1 ip sla 11 reachability
R1(config-track)# delay down 10 up 1
R1(config-track)# exit
R1(config)# track 2 ip sla 22 reachability
R1(config-track)# delay down 10 up 1
R1(config-track)# exit
R1(config)# ip sla schedule 11 life forever start-time now
R1(config)# ip sla schedule 22 life forever start-time now
R1(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.1 2 track 1
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.1.1 3 track 2
```

Dohľad nad sieťou Syslog, SNMP

Služba Syslog

- Syslog je sieťový protokol využívajúci UDP/514 a prenáša textové správy (hlavička je binárna)
  - Pôvodne Unix služba pre centralizované zbieranie systémových záznamov
- Každá správa má vyznačenú závažnosť (severity) a pôvod (facility)
- Syslog je v súčasnosti univerzálne podporovaný na všetkých (solídnych) sieťových prvkoch

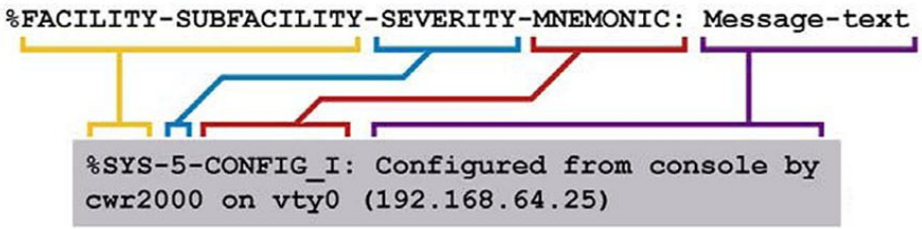


Úrovne závažnosti správ Syslog

Čím nižšie číslo v Cisco značení, tým väčšia závažnosť

Závažnosť v terminológii Syslog	Závažnosť v Cisco označení
Emergency	Level 0, najvyššia úroveň závažnosti
Alert	Level 1
Critical	Level 2
Error	Level 3
Warning	Level 4
Notice	Level 5
Informational	Level 6
Debugging	Level 7

Formát Syslog správy v Cisco IOS



- Systémové správy začínajú znakom %
- **Facility:** Aspoň dve písmená vyjadrujúce pôvod správy (hardvérový komponent, protokol, modul operačného systému atď.)
- **Severity**: Číslo od 0 do 7 vyjadrujúce závažnosť správy
- **Mnemonic:** Pomocný symbolický textový popis
- **Message-text:** Samotný obsah správy

Konfigurácia Syslog v Cisco IOS

```
! Konfigurácia Syslog klienta (zariadenie bude posielať Syslog správy
! na definovaný server)
Switch(config)# logging host 192.0.2.1
Switch(config)# logging trap ?
<0-7>          Logging severity level
alerts         Immediate action needed                (severity=1)
critical       Critical conditions                    (severity=2)
debugging      Debugging messages                     (severity=7)
emergencies    System is unusable                     (severity=0)
errors         Error conditions                       (severity=3)
informational  Informational messages                 (severity=6)
notifications  Normal but significant conditions      (severity=5)
warnings       Warning conditions                     (severity=4)
Switch(config)# logging trap informational
```

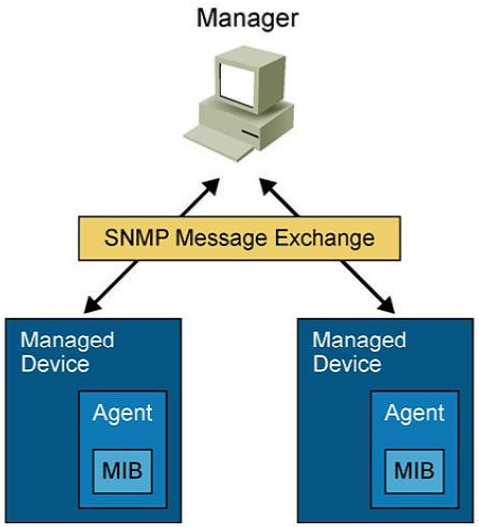
```
! Konfigurácia zaznamenávania správ do buffera v pamäti
! Parametre: veľkosť buffera v bajtoch, závažnosť správy
Switch(config)# logging buffered 10000 6
```

Zobrazenie nastavení loggingu

```
Switch# show logging
Syslog logging: enabled (11 messages dropped, 0 messages rate-limited,
                0 flushes, 0 overruns, xml disabled, filtering disabled)
    Console logging: level debugging, 174 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging: level informational, 3 messages logged, xml disabled,
                    filtering disabled
    Logging Exception size (4096 bytes)
    Count and timestamp logging messages: disabled

No active filter modules.

    Trap logging: level informational, 43 message lines logged
        Logging to 192.0.2.1(global) (udp port 514, audit disabled,  link
up), 2 message lines logged, xml disabled,
             filtering disabled

Log Buffer (10000 bytes):

*Mar  1 01:40:47.395: %SYS-5-CONFIG_I: Configured from console by console
```

Simple Network Management Protocol

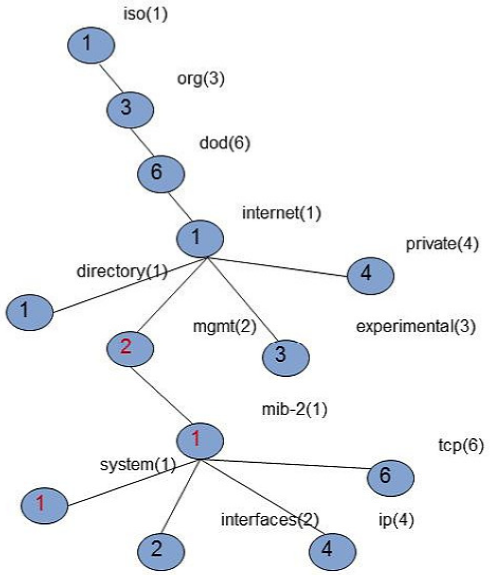
- Je de facto jediný štandard pre manažment v IP sieťach
- SNMP má tri komponenty:
  - Network Management Application
  - Agenti – súčasť spravovaného zariadenia, ktorá implementuje podporu SNMP
  - MIB databáza – jednotlivé objekty spravovaného zariadenia
- SNMP pracuje v dvoch režimoch
  - Pull model – manažér získava údaje pravidelným dopytovaním
  - Push model – agent sám posiela informácie manažérovi



MIB – Management Information Base

- Objekty na agentovi majú svoje identifikátory OID (Object IDentifier)
  - OID sú usporiadané v stromovej štruktúre
  - Vrcholy majú číselný i slovný názov
  - Konkrétny objekt je adresovaný cestou od koreňa stromu
- Príklad: .1.3.6.1.2.1.1

iso(1) org(3) dod(6) internet(1)
mgmt(2)
mib-2 (1)
system (1)

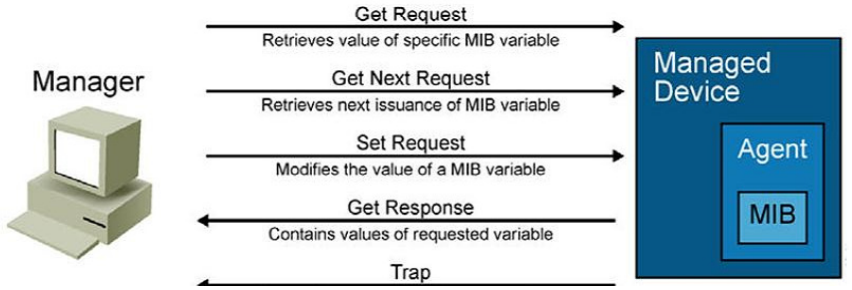


Porty a UDP

- SNMP ako transportný mechanizmus používa User Datagram Protocol (UDP) s portmi
  - UDP Port 161 - SNMP Messages
  - UDP Port 162 - SNMP Trap Messages

SNMP Verzia 1 (SNMPv1)

- Definovaná v RFC 1157
- Definuje päť základných správ
  - Get Request (Get)
    - Požaduje načítanie hodnoty objektu podľa OID
  - Get Next Request (GetNext)
    - Použitá po počiatočnom „Get Request“ na získanie ďalšej položky z MIB
  - Set Request (Set)
    - Použitá na nastavenie MIB premennej na agentovi
  - Get Response (Response)
    - Použitá agentom na odoslanie odpovede na GetRequest a GetNextRequest
  - Trap
    - Zasielanie nevyžiadanej správy z agenta na manažéra



SNMP Verzia 2 (SNMPv2)

- Definovaná v RFC 1441
  - Problém s akceptáciou v IETF z dôvodu bezpečnosti a administratívy
  - Má len experimentálne implementácie
- Community-based SNMPv2 (SNMPv2c)
  - RFC 1901
  - Najbežnejšia implementácia SNMPv2
  - SNMPv2c stále používa pre autentifikáciu prístupu iba názvy komunít
- SNMPv2 pridáva dva nové druhy správ:
  - Get Bulk Request:
    - Umožňuje preniesť väčšie množstvo dát
    - Zvyšuje výkonnosť obmedzením opakujúcich sa správ Request/Reply
  - Inform Request:
    - Umožňuje informovať manažéra o výskyte udalosti
    - Príjem je potvrdzovaný

SNMP Verzia 3

- Definované v RFC 3410 až 3415
- Hlavné vylepšenie je v aspekte autentifikácie a šifrovania prenášaných dát
- SNMPv3 má tri úrovne zabezečenia
  - **noAuthNoPriv**
    - Bez autentifikácie a šifrovania
  - **authNoPriv**
    - Autentifikácia pomocou HMAC-MD5 alebo HMAC-SHA. Šifrovanie nie poskytované
  - **authPriv**
    - Autentifikácia pomocou HMAC-MD5 alebo HMAC-SHA, šifrovanie pomocou DES, 3DES alebo AES.
- Cisco zariadenia v SNMPv3 podporujú User-based Security Model (autentifikácia menom a heslom)

Odporúčania pre používanie SNMP

- Komunitné reťazce v SNMPv1 a SNMPv2 sú prenášané ako plaintext
  - Komunitné reťazce by sa mali meniť v pravidelných intervaloch podľa požiadaviek sieťovej politiky
  - Ak cez SNMP len monitorujeme zariadenia, treba používať iba Read-Only komunitu
  - Na riadenie prístupu zo SNMP manažérov používať ACL
- Nasadenie SNMPv3 je vysoko odporúčané kvôli autentifikácii a šifrovaniu

Konfigurácia SNMP

- Vytvorenie ACL pre limitovaný prístup k SNMP agentovi
- Nastavenie SNMP komunít
- Nastavenie cieľa pre zasielanie správ SNMP Trap
- Aktivácia konkrétnych SNMP Trap správ

```
Switch(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Switch(config)# snmp-server community cisco RO 1
Switch(config)# snmp-server community xyz123 RW 1
Switch(config)# snmp-server host 10.1.1.50 xyz123
Switch(config)# snmp-server enable traps ?
```


CISCO