



# Routers and Routing Protocol Hardening



CCNP ROUTE: Implementing IP Routing

# Čo nás čaká...

- Zabezpečenie manažment roviny smerovačov
  - SSH, ACL, syslog, snmp, ntp
- Zabezpečenie riadiacej roviny
  - Autentifikácia smerovacích protokolov
    - EIGRP a named EIGRP, OSPFv2/v3, BGP
- VRF-lite

# Smerovač

- Architektúra a činnosť smerovača môže byť rozdelená do troch rovín:
  - **Management plane**
    - Zaoberá sa riadením/manažovaním prevádzky smerovača
    - Spracováva toky manažmentov rozhraní
    - Zabezpečenie zahŕňa:
      - Použitie silných hesiel, autentifikáciu používateľov, pridelovanie CLI podľa rolí, implementácia SSH, logging, zabezpečenie NTP, zabezpečenie SNMP
  - **Control plane**
    - Má na starosti činnosti súvisiace s rozhodnutiami o smerovaní paketov => činnosť smerovacích protokolov
    - Zabezpečenie zahŕňa **autentifikáciu** smerovacích protokolov
  - **Data plane**
    - Forwarding plane – preposielanie paketov cez rozhrania smerovača
    - Zabezpečenie zvyčajne zahŕňa ACL



# Zabezpečenie roviny manažmentu / Securing management plane



# Zabezpečenie roviny manažmentu

- Zabezpečovanie zariadenia (device hardening) v rovine manažmentu zahŕňa
  - Aplikácia a nasledovanie bezpečnostných politík smerovačov
  - Zabezpečenie prístupu k manažmentu
  - Používanie SSH a obmedzenie prístupu k smerovaču cez ACL
  - Implementácia logovania (system logging)
  - Zabezpečenie SNMP
  - Zálohovanie konfigurácií
  - Používanie monitoringu siete
  - Zakázanie nepoužívaných služieb

# Securing the Management Plane

## Step 1.

- **Follow the written router security policy.**
  - The policy should specify who is allowed to log in to a router and how, who is allowed to configure and update the router, or who is allowed to perform logging and monitoring actions.
  - The policy should also specify the requirements for passwords that are used to access the router.

# Securing the Management Plane

## Step 2.

### ■ **Secure physical access.**

- Place the router and physical devices that connect to it in a secure locked room that is accessible only to authorized personnel.
- The room should also be free of electrostatic or magnetic interference, have fire suppression, and controls for temperature and humidity.
- Install an uninterruptible power supply (UPS) and keep spare components available.
- This reduces the possibility of a network outage from power loss.

# Securing the Management Plane

## Step 3.

### ■ Use strong encrypted passwords

- Use a complex password with a minimum of eight characters.
- Enforce a minimum length using the security password min-length global configuration command.
- Strong passwords should generally be maintained and controlled by a centralized authentication, authorization, and accounting (AAA) server.
- Some local passwords and secret information may be required, for local fallback in case AAA servers become unavailable, such as special-use usernames, secret keys, and other password information.
- Such local passwords should be properly encrypted to secure them from prying eyes.



# Securing the Management Plane

## Step 4.

- **Control the access to a router.**
  - Console and auxiliary ports: These ports are used to gain access when a physical connection to the router is available in the form of a terminal.
  - vty lines: Access to a router using SSH or Telnet is by far the most common administrative tool. For this reason, vty access should be protected using only SSH from authorized IP addresses identified in an ACL.

# Securing the Management Plane

## Step 5.

### ■ Secure management access

- Only authorized individuals should have access to infrastructure devices.
- For this reason, configure authentication, authorization, and accounting (AAA) to control who is permitted to access a network (authenticate), what they can do on that network (authorize), and audit what they did while accessing the network (accounting).
- Authentication can be performed locally or by using a AAA authentication server.

# Securing the Management Plane

## Step 6.

- **Use secure management protocols.**
  - Always use secure management protocols including SSH, HTTPS, and SNMPv3.
  - If unsecure management protocols such as Telnet, HTTP, or SNMP must be used, then protect the traffic using an IPsec virtual private network (VPN).
  - Also protect management access to the router by configuring ACLs that specify authorized hosts that can access the router.

# Securing the Management Plane

## Step 7.

### ■ Implement system logging

- System logging provides traffic telemetry, which helps detect unusual network activity and network device failures.
- Traffic telemetry is implemented by using various mechanisms such as syslog logging, SNMP traps, and NetFlow exports.
- Use the **service timestamps log datetime** global configuration command to include date and time in the log messages.
- When implementing network telemetry, it is important that the date and time is both accurate and synchronized across all network infrastructure devices.
- This is achieved using Network Time Protocol (NTP). Without time synchronization, it is very difficult to correlate different sources of telemetry.

# Securing the Management Plane

## Step 8.

- **Periodically back up configurations**

- A backed-up configuration allows a disrupted network to recover very quickly.
- This can be achieved by copying a configuration to an FTP (or TFTP) server at regular intervals or whenever a configuration change is made.

# Securing the Management Plane

## Step 9.

### ■ **Disable unneeded services**

- Routers support many services.
- Some of these services are enabled for historical reasons, but are no longer required today.
- Services that are not needed on the router can be used as back doors to gain access to it and should therefore be disabled.

# Politika zabezpečenia smerovača

Politika zabezpečenia smerovača by mala riešiť odpovede na otázky okolo:

- **Password encryption and complexity settings**
- **Authentication settings**
- **Management access settings**
- **Securing management access using SSH**
- **Unneeded services settings**
- **Ingress/egress filtering settings**
- **Routing protocol security settings**
- **Configuration maintenance**
- **Change management**
- **Router redundancy**
- **Monitoring and incident handling**
- **Security updates**

## Silné hesla

# Odporúčania pre používanie silných hesiel

- Používanie silných hesiel zahŕňa:
  - Use a password length of ten or more characters. A longer password is a better password.
  - Make passwords complex. Include a mix of uppercase and lowercase letters, numbers, symbols, and spaces.
  - Avoid passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, biographical information, such as birthdates, ID numbers, ancestor names, or other easily identifiable pieces of information.
  - Deliberately misspell a password (for example, Smith = Smyth = 5mYth or Security = 5ecur1ty).
  - Change passwords often. If a password is unknowingly compromised, the window of opportunity for the attacker to use the password is limited.
  - Do not write passwords down and leave them in obvious places, such as on the desk or monitor.



## Silné hesla

# Vynútenie konfigurácie silných hesiel

- Minimálna dĺžka

```
Router(config)# security passwords min-length ?  
<0-16> Minimum length of all user/enable passwords
```

- Obmedzenie počtu neúspešných prihlásení

```
Router(config)# security authentication failure ?  
rate Authentication failure threshold rate
```

Silné hesla

## Šifrovanie hesiel pre prístup k manažmentu

- Šifrovanie hesla pre prístup do privileged EXEC

```
Router(config)# enable secret PASSWORD
```

- IOS 15.0(1)S a novší používa SHA256 hash algoritmus
- Staršie verzie IOS používajú Message Digest 5 (MD5) hash algoritmus

## Zabezpečenie prístupu k zariadeniu

# Šifrovanie hesiel pre prístup k manažmentu

- Šifrovanie hesiel pre prístup na konzolu, vty a aux
  - Zdieľané heslo

```
Router(config)# line console 0 | vty 0 15 | aux
! Pozor, ulozene v konfigu ako plain text
Router(config-line)# login PASSWORD
! Zapni jeho šifrovanie
Router(config)# service password-encryption
```

- Použitie **lokálnej DB** mien a hesiel
  - Vytvorenie položky s heslom šifrovaným na úroveň 4 (SHA256),

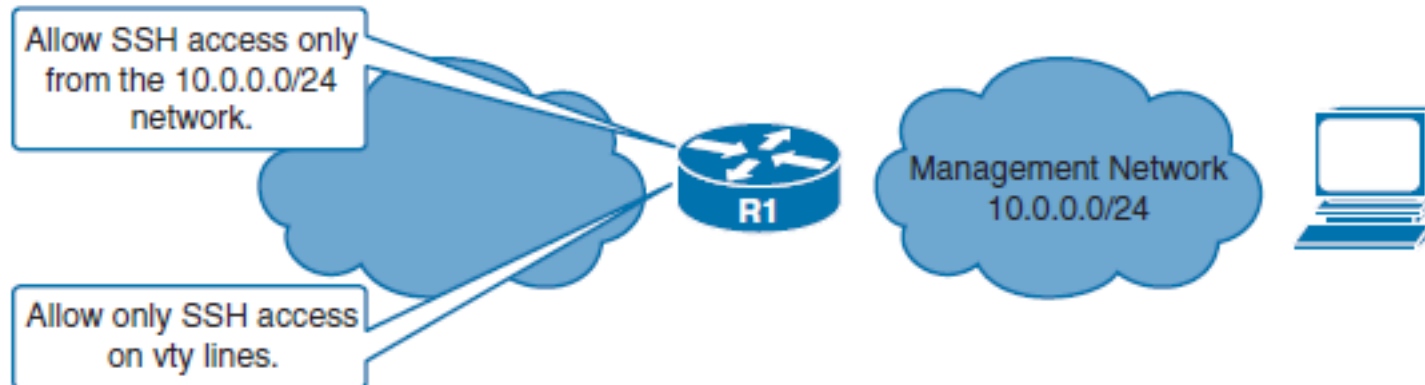
```
Router(config)# username NAME secret PASSWORD
```

- Nastav autentifikáciu konzoly a VTY voči lokal DB

```
Router(config)# line console 0 | vty 0 15 | aux
Router(config-line)# login local
```

Zabezpečenie prístupu k zariadeniu

# Uprednostni SSH pred telnet-om



```
Router(config)# hostname R1
R1(config)# ip domain-name cisco.com
R1(config)# username ADMIN privilege 15 secret class12345
```

```
R1(config)# crypto key generate rsa modulus 2048
The name for the keys will be: R1.cisco.com
% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 8 seconds)

R1(config)#
*Aug 13 17:22:58.625: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

## Zabezpečenie prístupu k zariadeniu

# Uprednostni SSH pred telnet-om

```
R1(config)# ip ssh version 2
```

```
R1(config)# ip access-list standard PERMIT-SSH  
R1(config-std-nacl)# remark ACL permitting SSH to hosts on the Management LAN  
R1(config-std-nacl)# permit 10.0.0.0 0.0.0.255  
R1(config-std-nacl)# deny any log  
R1(config-std-nacl)# exit
```

```
R1(config)# line vty 0 4  
R1(config-line)# login local  
R1(config-line)# transport input ssh  
R1(config-line)# access-class PERMIT-SSH in  
R1(config-line)# end  
R1#
```

## Zabezpečenie prístupu k zariadeniu/infraštruktúre

# Access control lists (ACL)

- ACL umožňuje
  - Riadiť prístup prevádzky do siete, k zariadeniu a logovanie
- Z hľadiska zabezpečene prístupu k zariadeniu
  - Potreba:
    - Zabrániť nevhodným používateľom zasielanie smerovacích informácií či menežmentového prístupu zariadeniu
    - Riadiť prístup k zariadeniu
    - Povolenie všetkých iných potrebných tokov cez zariadenie
    - Iné úlohy
      - Filtruj privátne IP
      - Filtruj fragmenty apod.

# Zabezpečenie prístupu k zariadeniu/infraštruktúre

## Router ACL

```
R1(config)# ip access-list extended ACL-INFRASTRUCTURE-IN
R1(config-ext-nacl)# remark Deny IP fragments
R1(config-ext-nacl)# deny tcp any any fragments
R1(config-ext-nacl)# deny udp any any fragments
R1(config-ext-nacl)# deny icmp any any fragments
R1(config-ext-nacl)# deny ip any any fragments
R1(config-ext-nacl)# remark permit required connections for management traffic
R1(config-ext-nacl)# permit tcp host 10.10.12.2 host 10.10.12.1 eq 179
R1(config-ext-nacl)# permit tcp host 10.10.12.2 eq 179 host 10.10.12.1
R1(config-ext-nacl)# permit tcp host 10.0.0.10 any eq 22
R1(config-ext-nacl)# remark Permit ICMP Echo from management station
R1(config-ext-nacl)# permit icmp host 10.0.0.10 any echo
R1(config-ext-nacl)# remark Deny all other IP traffic to any network device
R1(config-ext-nacl)# deny ip any 10.0.0.0 0.0.0.255
R1(config-ext-nacl)# remark permit transit traffic
R1(config-ext-nacl)# permit ip any any
R1(config-ext-nacl)# exit
R1(config)# interface ethernet 0/0
R1(config-if)# ip access-group ACL-INFRASTRUCTURE-IN in
R1(config-if)#^Z
R1#
*Aug 13 18:19:57.308: %SYS-5-CONFIG_I: Configured from console by console
```

# Unicast Reverse Path Forwarding

- RFC 2827
  - Odporúča ISP/SP filtrovať dáta používateľov vstupujúce do siete a dropnúť prevádzku pochádzajúcu z nelegitímnych zdrojových adries
    - Takých, ktoré sa nenachádzajú v sieti ISP
- Implementácia Unicast Reverse Path Forwarding (uRPF)
  - Spolupracuje s CEF (Cisco Express Forwarding)
  - Umožňuje smerovaču overiť, či zdrojová IP adresa v pakete je dosiahnuteľná cez jeho smerovaciu tabuľku
    - Ak nie je, paket je dropnutý
- Unicast Reverse Path Forwarding (uRPF) tak
  - Zabraňuje spoofing útokom
  - pomáha obmedzovať nevhodnú prevádzku v sieti
  - a v duchu odporúčania RFC 2827 pre vstupné filtrovanie v sieťach pomáha chrániť voči časti útokov typu denial-of-service (DoS)
    - Tým útokom, ktoré používajú Source IP address spoofing



# Módy Unicast Reverse Path Forwarding

- uRPF pracuje v dvoch módoch:

## Strict mód

- Paket musí byť prijatý na rozhraní, ktorým by smerovač smeroval paket v obrátenom smere späť
- Riziko
  - V prípade asymetrického smerovania môže byť dropnutý legitímny paket
  - Lebo vstúpil rozhraním, ktoré nebolo smerovač uvažované pri návrate
- Vhodné pri situáciách, kde je garantovaný zdroj (access LAN, pobočka)

```
Router(config-if) # ip verify unicast source reachable-via rx
```

## Loose mód

- Zdrojová adresa musí byť v smerovacej tabuľke
- Voľba **allow-default** umožňuje použiť na verifikáciu zdroja default route.
- Paket so zdrojovou adresou, ktorá má cestu nasmerovanú do **Null 0** bude dropnutý.
- Na ladenie je možné použiť ACL na špecifikáciu zdrojových adries a riadenie prijatia alebo dropnutia

```
Router(config-if) # ip verify unicast source reachable-via any
```

# Zapnutie uRPF

- Príkaz

```
Router(config-if)# ip verify unicast source reachable-via rx |  
any [allow-default] [allow-self-ping]
```

- Mód

```
!strict  
Router(config)# interface GigabitEthernet 0/0  
Router(config-if)# ip verify unicast source reachable-via any  
!  
! loose  
Router(config)# interface GigabitEthernet 0/1  
Router(config-if)# ip verify unicast source reachable-via rx
```



# Zabezpečenie prístupu k manažmentu - Rozšírené AAA



aaa new-model

# Authentication, Authorization, Accounting

- AAA je súbor mechanizmov pre autentifikáciu, autorizáciu a účtovanie
  - Autentifikácia: Overenie identity (Kto je to?)
  - Autorizácia: Pridelenie práv (Čo môže robiť?)
  - Účtovanie (a reporting a auditing): Evidencia používania služieb (Koľko zaplatí? Koľko používal a čo?)
- Na Cisco zariadeniach sa AAA využíva na rôzne účely
  - Riadenie administratívneho prístupu (EXEC)
  - 802.1X na prepínačoch a access pointoch
  - WPA alebo WPA2 Enterprise
  - PPP, IPSec

# AAA

## ■ Autentifikácia

- Poskytuje metódy k:
  - Identifikácia používateľov
  - Riadenie prihlasovania
  - Messaging
  - Encryption

## ■ Autorizácia

- Poskytuje metódy k vzdialenému prístupu:
  - One-time authorization
  - Autorizácia pre každú službu per používateľa alebo skupinu
  - Používa RADIUS alebo TACACS+ security servers.

## ■ Účtovanie

- Poskytuje metódy potrebné k zbieraniu a zasielaniu informácií potrebných účtovaniu, reportovaniu a auditovaniu
- Používa
  - Identity používateľov
  - čas začiatku a konca
  - Vykonané príkazy
  - Prenesené pakety
  - Počet bajtov

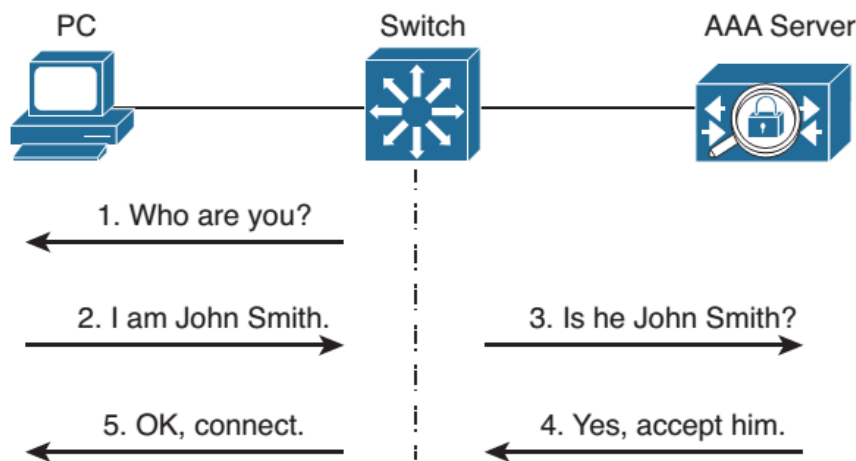
# Modely AAA

- Na Cisco zariadeniach je možné prepínať sa medzi dvomi modelmi AAA
- Starší model
  - Autentifikácia len voči lokálnej databáze
  - Autorizácia len voči lokálnej databáze
  - Minimálne (ak vôbec nejaké) možnosti pre účtovanie
- Novší model
  - Komplexná konfigurácia, ktorá umožňuje rôzne služby nasmerovať na AAA voči rôznym databázam
  - Ponúka.
    - Lepšiu flexibilitu a škálovateľnosť
    - Využitie viacerých systémov či riadenie ich záloh

# Nový model AAA

- Nový model AAA vychádza z týchto predpokladov
  - Na jednej strane máme isté druhy služieb, ktoré vedia pomocou istého mechanizmu riadiť prístup (dot1x, enable, login, ppp)
  - Na druhej strane máme rôzne databázy s evidenciou používateľov a ich práv (RADIUS, TACACS, lokálna databáza)
  - My chceme mať možnosť konkrétnej službe vysvetliť, v akej databáze má používateľa vyhľadať
- Napríklad:
  - Konzolové prihlásenia sa overia voči lokálnej databáze
  - SSH prihlásenia sa overia voči RADIUS serveru s IP 1.2.3.4
  - PPP prihlásenia sa overia voči RADIUS serveru s IP 5.6.7.8
  - Ethernet klienti sa overia voči RADIUS serveru s IP 9.8.7.6

# Možnosti autentifikácie a autorizácie



- Lokálna databáza

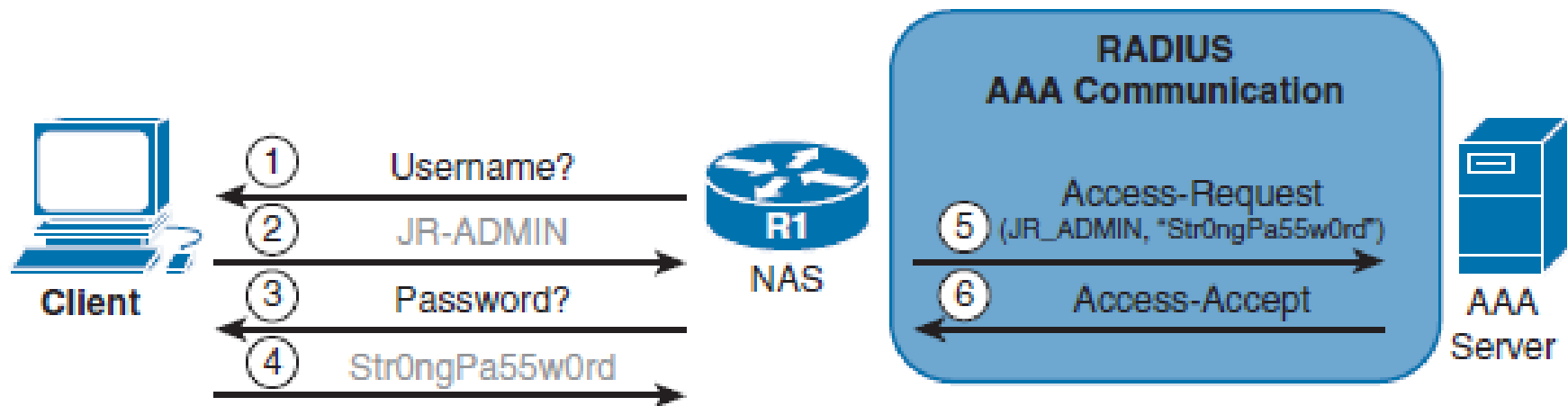
- Username NAME privilege LEVEL secret HESLO

- Sieťové servery

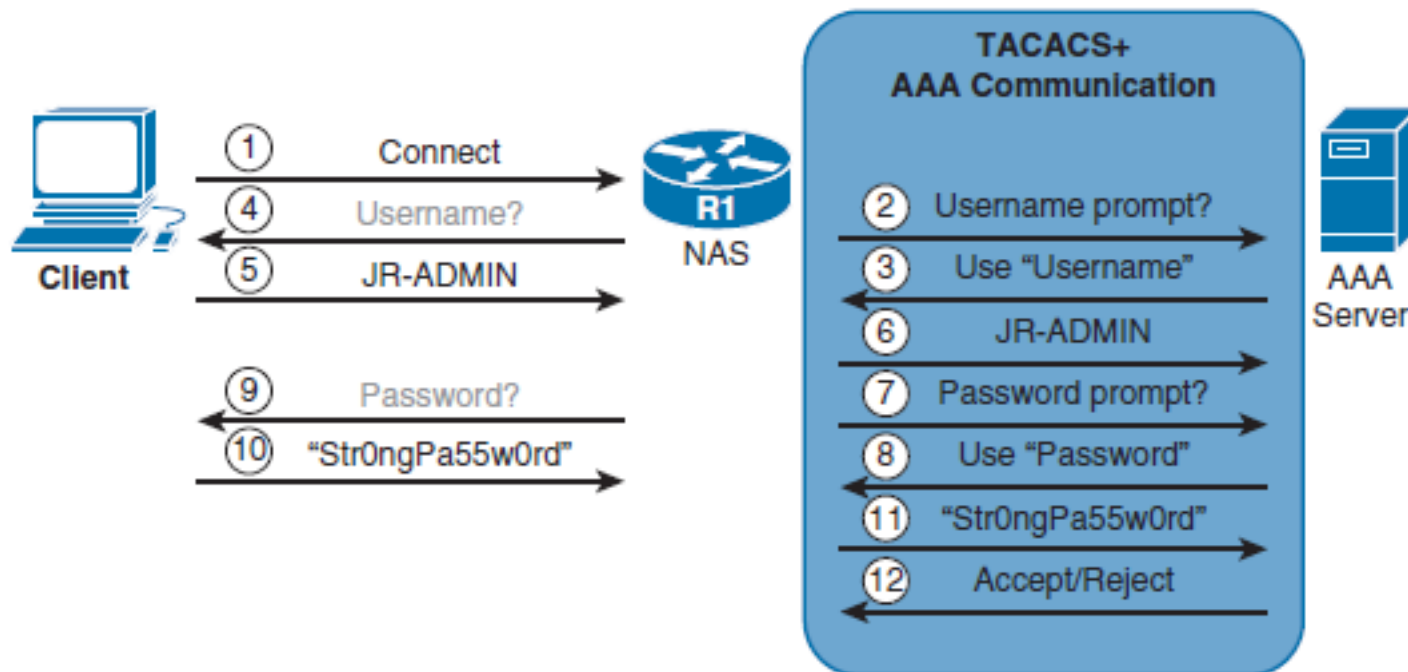
- TACACS/TACACS+ (Terminal Access Controller Access Control System+)
  - Cisco proprietárny, zabezpečené spojenie TCP port49
- Radius (Remote Authentication Dial-In User Service)
  - Otvorené riešenie, používa UDP porty 1812 a 1813
  - Šifrovaná je len časť správy s heslom



# RADIUS Message Exchange



# TACACS+ Message Exchange



# Konfigurácia AAA autentifikácie

## ■ 1) Definuj zdroje autentifikácie

```
!local DB
Router(config)# username username password password

! Radius
Router(config)# radius-server host {hostname | ip-address} [key
string]

! Tacacs
Router(config)# tacacs-server host {hostname | ip-address} [key
string]

! Mozme formovat grupu ako list zdrojov
Router(config)# aaa group server {radius | tacacs+} group-name
Router (config-sg)# server ip-address
```

## ■ 2) Aktivácia podpory nového AAA:

```
Router(config)# aaa new-model
```

# Konfigurácia AAA autentifikácie

- 3) Definuj zoznam autentifikačných metód (databáz), ktoré sa skúsia:

```
Router(config)# aaa authentication { ppp | dot1x | enable  
| login } {default | MENO_DB} db [db ...]
```

- DB
  - tacacs+: skús každý TACACS server v poradí ako si ich definoval
  - radius: skús každý Radius server v poradí ako si ich definoval
  - local: použi lokálne *Username*s.
  - line: line pass autentifikuje každého, kto ho použije, usernames nebude použité
- 4) Aplikuj metódy autentifikácie na con/vty/aux a over

```
Router(config-line)# login authentication {default |  
list-name}
```

# Príklad konfigurácie

- Využitie lokálnej databázy:

```
username MENO secret HESLO
!  
aaa new-model  
!  
aaa authentication login AE_L_LOCAL local  
!  
line vty 0 15  
  login authentication AE_L_LOCAL
```

- Využitie RADIUS servera a lokálnej databázy:

```
username MENO secret HESLO
!  
radius-server host 1.2.3.4 auth-port 1812 acct-port 1813 key HESLO  
!  
aaa new-model  
!  
aaa authentication login AE_L_RAD+L group radius local  
!  
line vty 0 15  
  login authentication AE_L_RAD+L
```

# Príklad konfigurácie RADIUS serverov

```
Router(config)# username admin password MySecretP@ssw0rd
Router(config)# aaa new-model
Router(config)# radius server RADIUS-1
Router(config-radius-server)# address ipv4 192.168.10.10
Router(config-radius-server)# key rad1-t@c@csk3y
Router(config-radius-server)# exit
Router(config)# radius server RADIUS-2
Router(config-radius-server)# address ipv4 192.168.10.11
Router(config-radius-server)# key rad2-t@c@csk3y
Router(config-radius-server)# exit
Router(config)# aaa group server radius RADIUS-GROUP
Router(config-sg)# server name RADIUS-1
Router(config-sg)# server name RADIUS-2
Router(config-sg)# exit
Router(config)# aaa authentication login default group RADIUS-
GROUP local
Router(config)# aaa authentication login TELNET-LOGIN group
RADIUS-GROUP local
Router(config)# line vty 0 15
Router(config-line)# login authentication TELNET-LOGIN
```

# Príklad konfigurácie TACACS serverov

- Využitie TACACS databázy:

```
Router(config)# aaa new-model
Router(config)# username lastresort password MySecretP@ssw0rd
Router(config)# tacacs-server host 192.168.10.10 key t@c@csk3y
Router(config)# tacacs-server host 192.168.10.11 key t@c@csk3y
Router(config)# aaa group server tacacs+ myauthservers
Router(config-sg)# server 192.168.10.10
Router(config-sg)# server 192.168.10.11
Router(config-sg)# exit
Router(config)# aaa authentication login myauth group
myauthservers local
Router(config)# line vty 0 15
Router(config-line)# login authentication myauth
```



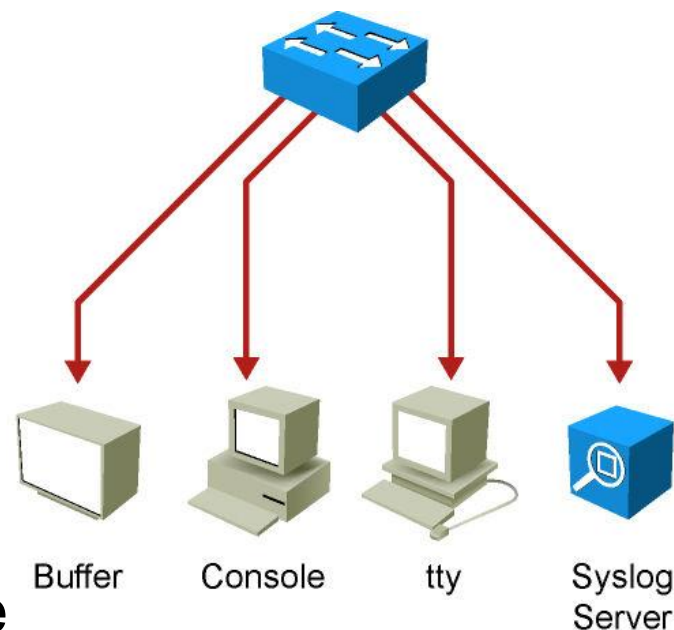
# Implementácia systémových logov - Syslog





# Syslog

- **System Message Logging**
- Umožňuje monitorovaným zariadeniam reportovať chyby a notifikačné správy
- Používa port UDP 514.
- Na cisco zariadeniach správa obsahuje úroveň závažnosti (severity) a zdroj (facility)
- Syslog je v súčasnosti univerzálne podporovaný na všetkých (solídnych) sieťových prvkoch
- Možnosť logovať na
  - Vty, konzolu, syslog server, buffer



# Syslog Severity Levels

- Čím nižšie číslo tým vyššia závažnosť (alarm)
  - Vyššie čísla zahŕňajú hlásky nižších levelov

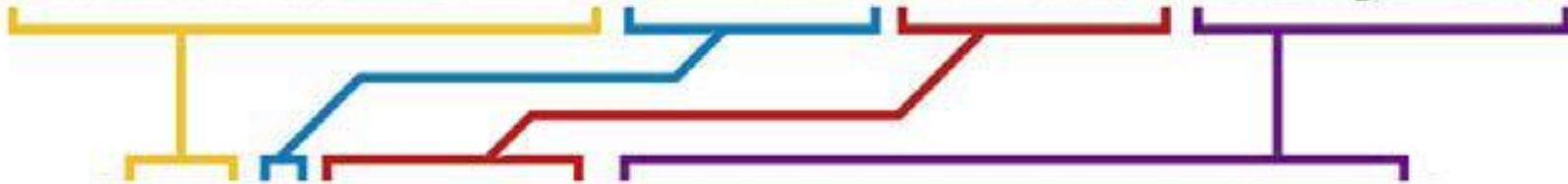
Syslog Severity	Severity Level
Emergency	Level 0, highest level
Alert	Level 1
Critical	Level 2
Error	Level 3
Warning	Level 4
Notice	Level 5
Informational	Level 6
Debugging	Level 7

# Syslog Facilities

- Identifikuje službu, ktorá poslala hlášku na syslog.
- Využívané na identifikáciu a kategorizáciu hlásení
- Cisco IOS má aktuálne viac ako 500 „facilities“
- Najznámejšie:
  - IP
  - OSPF
  - SYS operating system
  - IP Security (IPsec)
  - Route Switch Processor (RSP)
  - Interface (IF)

# Formát Syslog správ

`%FACILITY-SUBFACILITY-SEVERITY-MNEMONIC: Message-text`



```
%SYS-5-CONFIG_I: Configured from console by  
cwr2000 on vty0 (192.168.64.25)
```

- Systémová správa začína so znakom percento (%)
- **Facility**
  - Dve alebo viac písmen identifikujúci hw zariadenie, protocol, alebo sw modul
- **Severity**
  - Kód od 0-7, ktorá indikuje úroveň závažnosti
- **Mnemonic**
  - Kód jednoznačne identifikujúci správu
- **Message-text**
  - Text popisujúci daný stav. Môže obsahovať detailnejší popis danej udalosti, zahŕňajúci portové číslo, terminal, meno používateľa apod

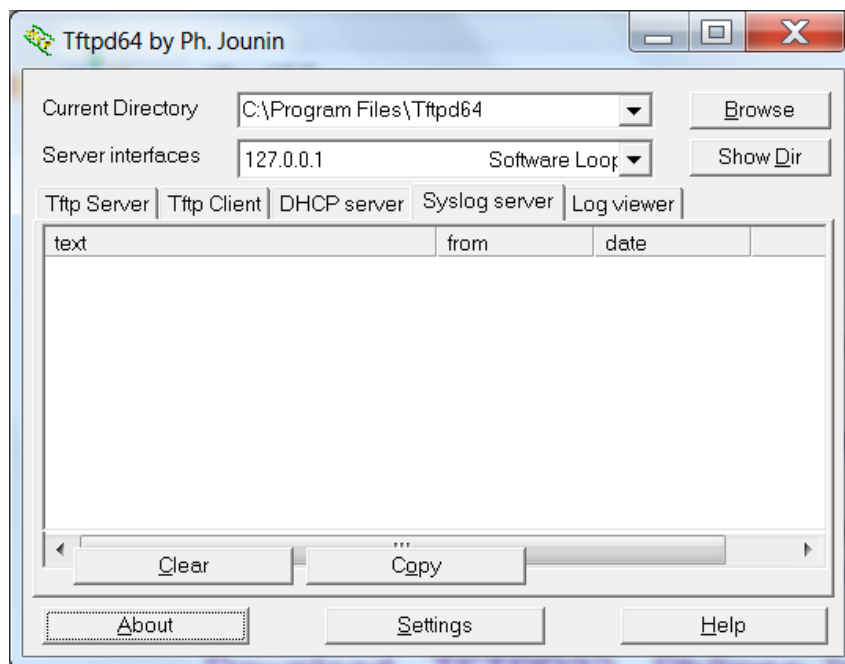
```
08:01:13: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
08:01:23: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(1) 1: Neighbor 10.1.1.1 (Vlan1) is up: new adjacency
08:02:31: %LINK-3-UPDOWN: Interface FastEthernet0/8, changed state to up
08:18:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to down
08:18:22: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/5, changed state to up
08:18:24: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down
08:18:24: %ILPOWER-5-IEEE_DISCONNECT: Interface Fa0/2: PD removed
08:18:26: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to down
08:19:49: %ILPOWER-7-DETECT: Interface Fa0/2: Power Device detected: Cisco PD
08:19:53: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
08:19:53: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up
```



# Voľne dostupné Syslog servery/windows

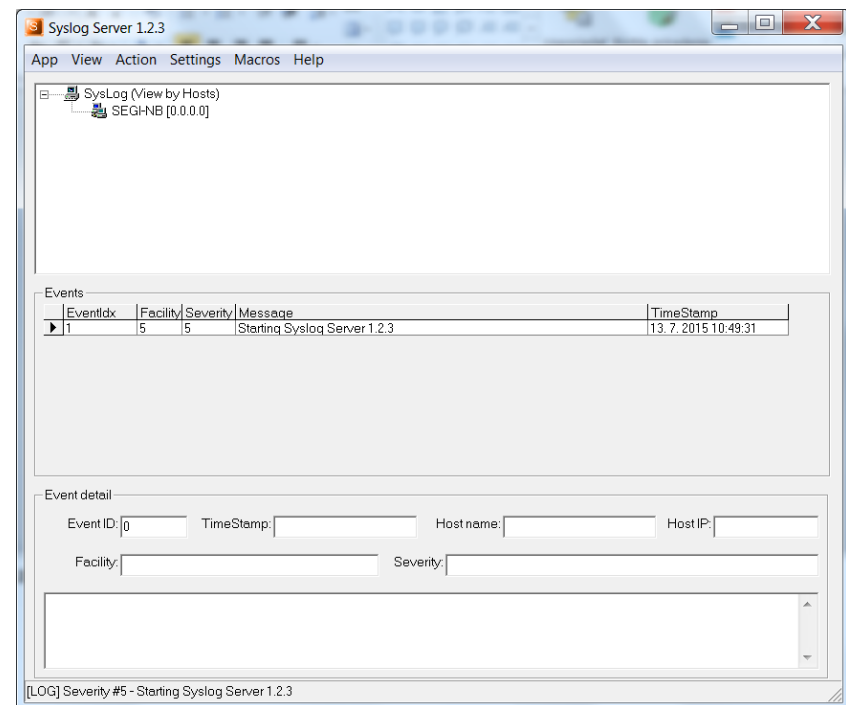
## Tftpd32 alebo Tftpd64

[tftpd32.jounin.net](http://tftpd32.jounin.net)



## Syslog Server

[sourceforge.net/projects/syslog-server](http://sourceforge.net/projects/syslog-server)



# Konfigurácia syslog (1)

- Konfigurácia syslog servera

```
! Nastav IP adresu syslog servera  
Switch(config)# logging IP_ADDR
```

- Nastavenie úrovne hlášok (severity level)

```
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 errors
```

# Konfigurácia syslog (2)

- Konfigurácia logovania do zásobníka (buffer)
  - Správy budú držané lokálne
  - Potrebné nastaviť level a veľkosť zásobníka

```
Switch(config)# logging buffered ?
<0-7>                Logging severity level
<4096-2147483647>    Logging buffer size
alerts               Immediate action needed                (severity=1)
critical             Critical conditions                    (severity=2)
debugging            Debugging messages                    (severity=7)
discriminator        Establish MD-Buffer association
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)
xml                  Enable logging in XML to XML logging buffer

Switch(config)# logging buffered errors

! Velkost bufra
Switch(config)# logging buffered 8192
```



# Overenie konfigurácie Syslog

- Príkaz
  - `show logging`
- Na filtráciu výpisov je vhodné používať pipe (|) s kľúčovým slovom
  - `include` or `begin`

```
Switch# show logging | include LINK-3
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/2, changed state to up
2d20h: %LINK-3-UPDOWN: Interface FastEthernet0/1, changed state to up
Switch# show logging | begin %DUAL
2d22h: %DUAL-5-NBRCHANGE: EIGRP-IPv4:(10) 10: Neighbor 10.1.253.13
(FastEthernet0/11) is down: interface down
2d22h: %LINK-3-UPDOWN: Interface FastEthernet0/11, changed state to down
2d22h: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/11,
changed state to down
```

# Čas (najmä správny) je dôležitý!!!!

! Pridaj casovu znacku pre debug spravy

```
Router(config)# service timestamps debug datetime msec localtime show-timezone
```

! Pridaj casovu znacku pre log spravy

```
Router(config)# service timestamps log datetime msec localtime show-timezone
```

debug	Indicates that the timestamp should be applied to debugging messages.
log	Indicates that the timestamp should be applied to system logging messages.
uptime	Time stamp with the time since the system was rebooted. The time stamp format for uptime is HHHH:MM:SS.
datetime	Time stamp with the date and time. The time stamp format for datetime is MMM DD HH:MM:SS.
msec	(Optional) Include milliseconds in the time stamp.
localtime	(Optional) Time stamp relative to the local time zone.
year	Include the year in the datetime format.
show-timezone	(Optional) Include the time zone name in the time stamp.

**Predpokladá sa správny lokálny čas (NTP?) !!!!!**

# Ďalšie čítanie

- Troubleshooting and Fault Management
  - <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/bsm/configuration/15-mt/bsm-15-mt-book/bsm-troubleshooting.html>

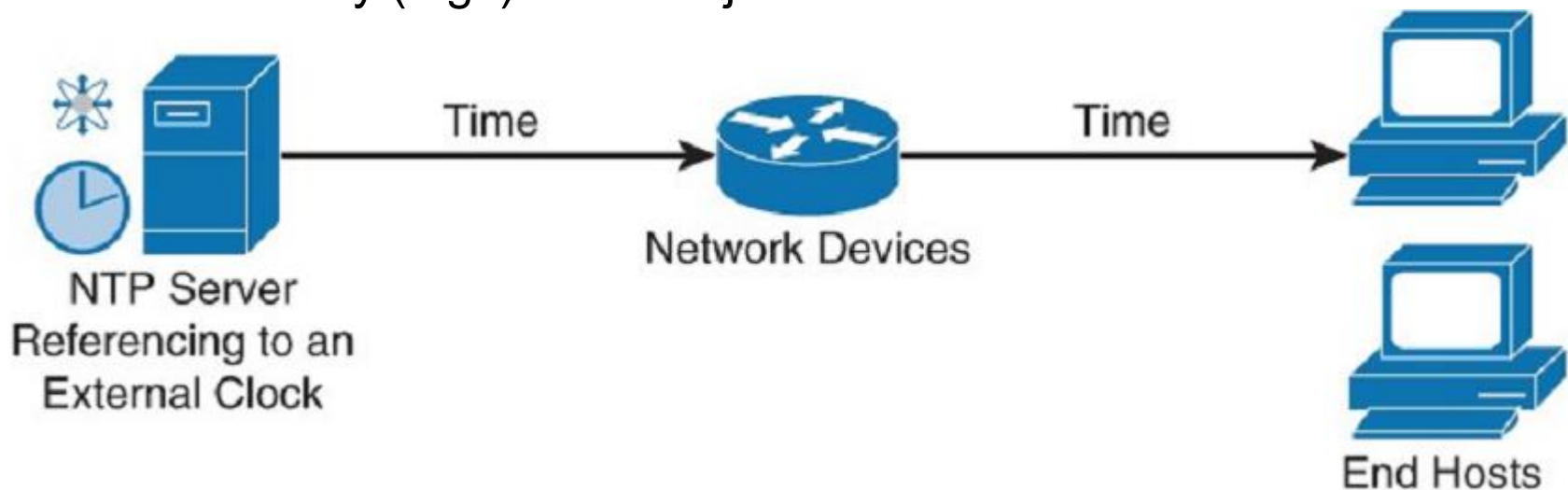


# Network Time Protocol



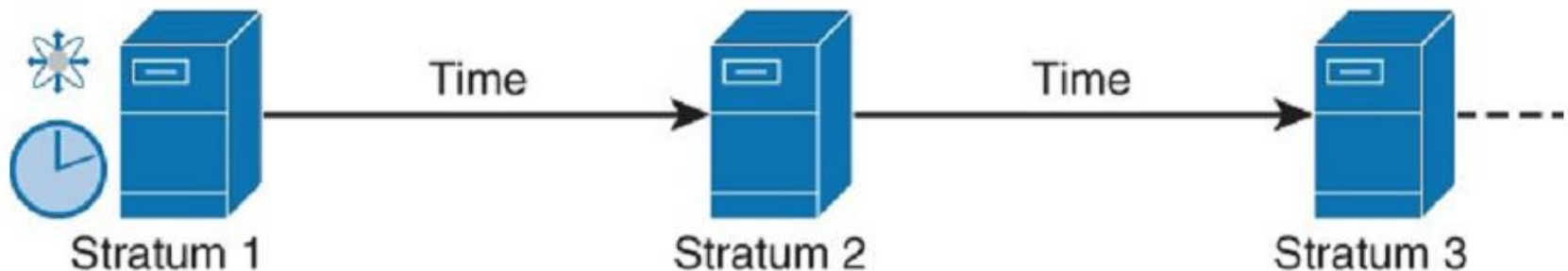
# Network Time Protocol

- NTP je otvorený protokol špecifikovaný v RFC 5905 pre časovú synchronizáciu sieťových uzlov
  - UDP zdrojový/cieľový port 123
- Používanie NTP je dôležité z mnohých dôvodov
  - Kľúčenky (key-chains) a časovo obmedzené platnosti kľúčov
  - Digitálne certifikáty a ich obmedzenia platnosti
  - Záznamy (logs) a ich vzájomná korelácia



# Network Time Protocol

- NTP zavádza pojem „stratum“ (počet hopov od hodín)
  - **Stratum 0**: zariadenie tvoriace časový normál (céziové hodiny, GPS prijímač, DCF-77 prijímač, atď.)
  - **Stratum 1**: NTP server, ktorý je priamo spojený s časovým normálom a používa ho ako svoj referenčný zdroj času
    - Je autoritatívnym serverom
  - **Stratum N**: NTP server, ktorý sa sieťovo synchronizuje od NTP servera v stratum N-1
- Maximálne číslo stratum je 15
- Ideál je synchronizovať sa o autoritatívneho servera, nie však vždy možné => preto je stratum hierarchia



# NTP

- Je klient / server protokol
- NTP zariadenie môže pracovať v nasledujúcich módoch
  - **Server:**
    - Poskytuje časové údaje klientom.
    - Volaný NTP master (ntp master command)
  - **Client:**
    - Synchronizuje svoj čas s NTP serverom/servermi (ntp server command).
  - **Peers:**
    - Peerovia si len vymieňajú časovú informáciu. Vzájomne sa synchronizujú.
    - Volaný symmetrický ntp mód (ntp peer command)
  - **Broadcast/multicast:**
    - „Push“ režim, kde server tlačí NTP údaje do siete. (ntp broadcast command)

# Príkazy pre konfiguráciu protokolu NTP

- Konfigurácia NTP **klienta** (smerovač, ktorý si voči serveru aktualizuje svoj čas):

```
Router(config)# ntp server IP [prefer]  
! Prefer urcuje preferovany ak je viac serverov
```

- Konfigurácia NTP **servera** (smerovač, ktorý poskytuje časové služby)

```
Router(config)# ntp master [1-15]  
! Štandardné stratum: 8
```

- Konfigurácia časovej zóny

```
Router(config)# clock timezone CET 1  
  
Router(config)# clock summer-time CEST recurring  
last Sun Mar 2:00 last Sun Oct 3:00  
  
!overenie  
Router# show clock detail
```



# Príklad konfigurácie a overenia NTP

- Konfigurácia NTP vrátane časovej zóny a vkladania časových pečiatok do debug a log záznamov

```
ntp server 158.193.48.7 prefer
ntp server 158.193.152.2
!
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime localtime show-timezone
!
clock timezone CET 1
clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00
```

```
Router# show ntp status
Clock is synchronized, stratum 12, reference is 158.193.48.7
nominal freq is 119.2092 Hz, actual freq is 119.2078 Hz, precision is 2**18
reference time is D2054E5B.686C9787 (01:31:39.407 CEST Mon Aug 29 2011)
clock offset is -0.0317 msec, root delay is 2.15 msec
root dispersion is 12.08 msec, peer dispersion is 0.23 msec
Router# show ntp associations
```

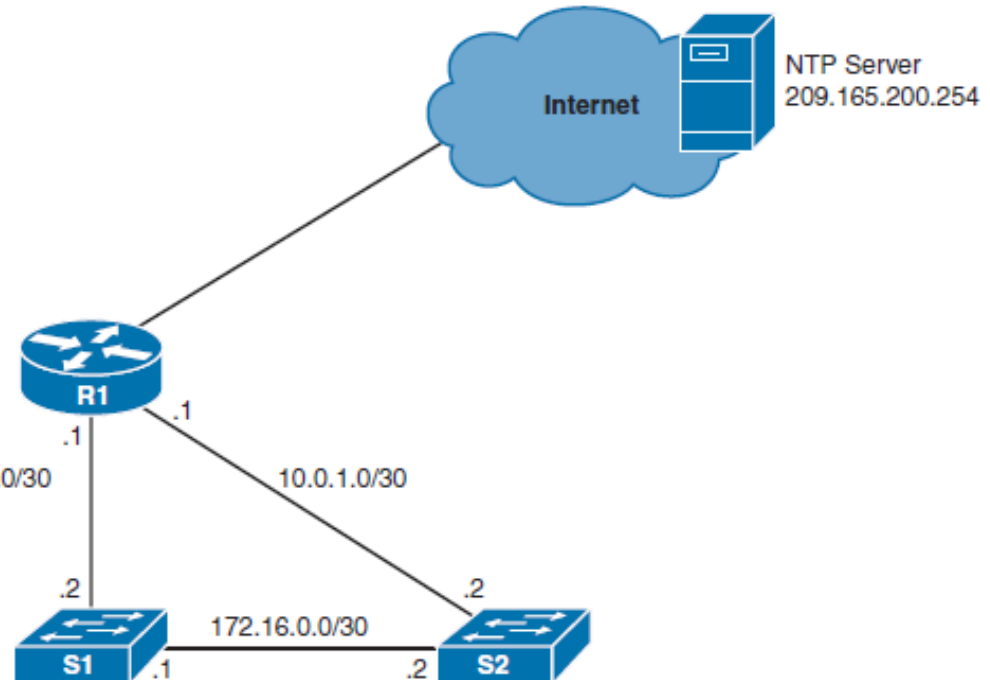
address	ref clock	st	when	poll	reach	delay	offset	disp
*~158.193.48.7	127.127.1.0	11	37	512	377	2.2	-0.03	0.2

\* master (syncd), # master (unsyncd), + selected, - candidate, ~ configured

# Konfigurácia NTP

```
R1(config)# ntp server 209.165.200.254
R1(config)# clock timezone EST -5
R1(config)# clock summer-time EST recurring
R1(config)#
```

```
S1(config)# ntp server 10.0.0.1
S1(config)# clock timezone EDT -5
S1(config)# clock summer-time EDT recurring
S1(config)# ntp peer 172.16.0.2
S1(config)#
```



```
S2(config)# ntp server 10.0.1.1
S2(config)# clock timezone EST -5
S2(config)# clock summer-time EST recurring
S2(config)# ntp peer 172.16.0.1
S2(config)#
```

# Zabezpečenie NTP – autentifikácia a ACL

```
Router(config)# ntp authentication-key KEY-NUMBER md5 KEY-STRING
```

```
Router(config)# ntp authenticate
```

```
Router(config)# ntp trusted-key KEY-NUMBER
```

*! Cislo validneho kluca*

```
Router(config)# ntp server IP-ADDRESS key KEY-NUMBER
```

- zabezpečenie, kto sa môže synchronizovať

```
Router(config)# access-list ACL-NUM permit IP-ADDRESS MASK
```

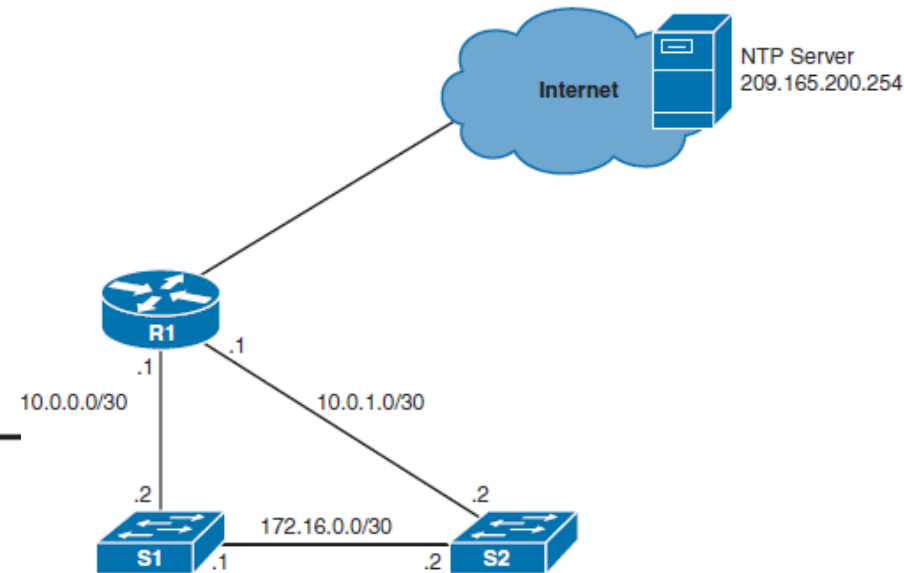
```
Router(config)# ntp access-group {serve-only | serve | peer | query-only} acl-num
```

- Na ntp mastroch
- serve-only Allows only time requests
- serve: Allows time requests and NTP control queries, but does not allow the router to synchronize to the remote device.
- peer: Allows time requests and NTP control queries and allows the router to synchronize to the remote device.
- query-only: Allows only NTP control queries.

# NTP autentifikácia

```
R1(config)# ntp authentication-key md5 NTP-pa55w0rd
R1(config)# ntp authenticate
R1(config)# ntp trusted-key 1
R1(config)#
R1(config)# access 10 permit 10.0.0.0 0.0.255.255
R1(config)# ntp access-group serve-only 10
R1(config)#
```

```
S1(config)# ntp authentication-key md5 NTP-pa55w0rd
S1(config)# ntp authenticate
S1(config)# ntp trusted-key 1
S1(config)# ntp server 10.0.0.1 key 1
S1(config)#
```



# NTP verzie

- V súčasnosti sa používajú verzie 3 a 4
  - V4 je rozšírenie verzie 3
- Verzia 4 ponúka vlastnosti ako:
  - Podpora IPv4 aj IPv6 so spätnou podporu voči NTPv3 (tá nepodporuje IPv6)
  - Používa na posielanie a príjem správ IPv6 multicast namiesto bcastu v IPv4
  - Zvyšuje bezpečnosť použitím PKI a X509 certifikátov
  - Zlepšila časovú synchronizáciu a výkonnosť
  - Podporuje IPv6 named ACL (v3 len číslované IPv4 ACL)

# Simplified Network Time Protocol (SNTP)

- Ak chceme aby dané zariadenie sa len synchronizovalo
  - NTP klient
- SNTP ponúka obmedzenú sadu funkcií NTP
- Konfigurácia ako NTP len zameniť slovíčko za **sntp**



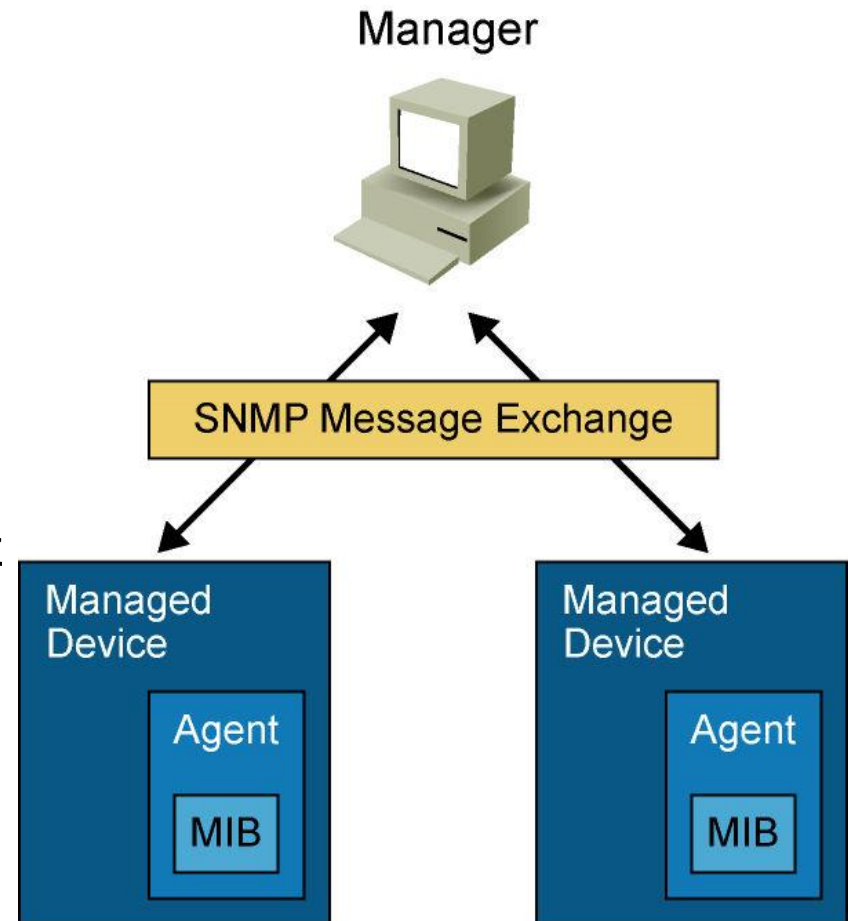
# Simple Network Management Protocol



SNMP

# Simple Network Management Protocol

- Je de facto jediný štandard pre manažment v IP sieťach
- SNMP má tri komponenty:
  - Network Management Application (SNMP Manager)
  - SNMP Agents
    - Pracuje vo vnútri riadeného zariadenia
  - MIB Database
    - Databáza objektov, ktoré popisujú informáciu v definovanom formáte (SMI)
- SNMP definuje ako budú riadiace správy manažmentu vymieňané cez sieť medzi SNMP aplikáciou a SNMP agentom
  - Pull model
    - Manažér sa opýta agenta
  - Push model
    - Agent sám pošle info manažérovi
- Existujú viaceré verzie SNMP protokolu





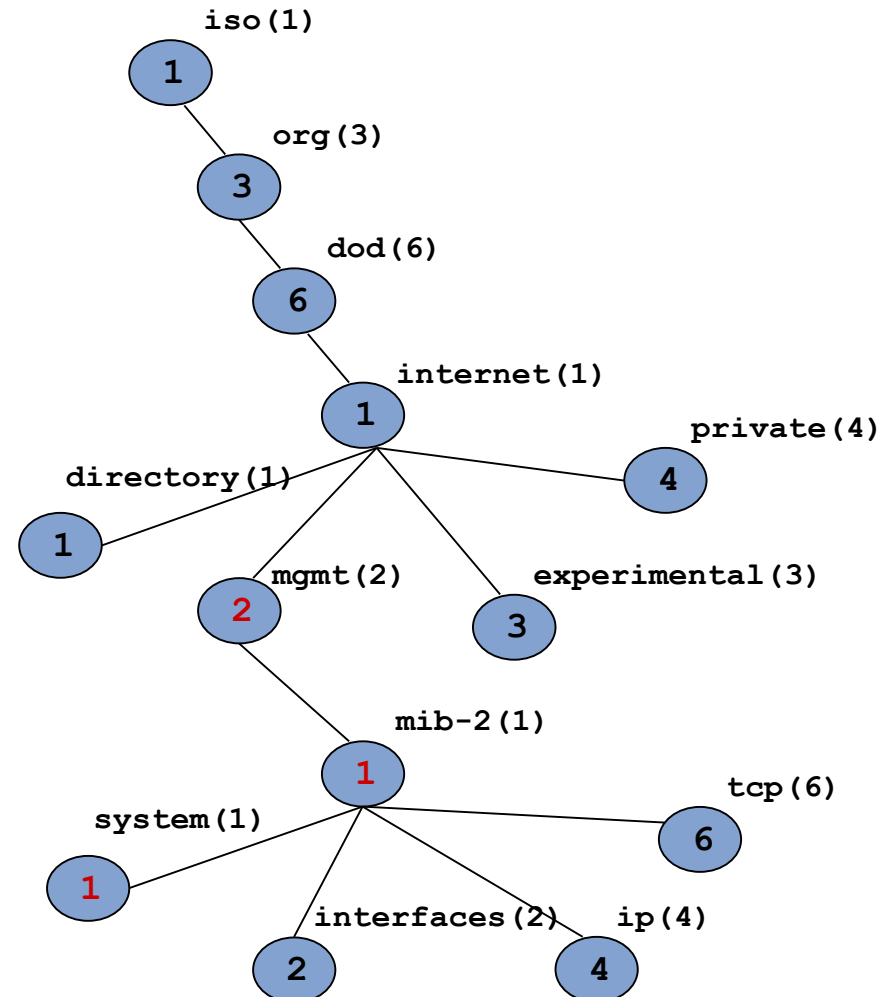
# MIB – Management Information Base

- 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

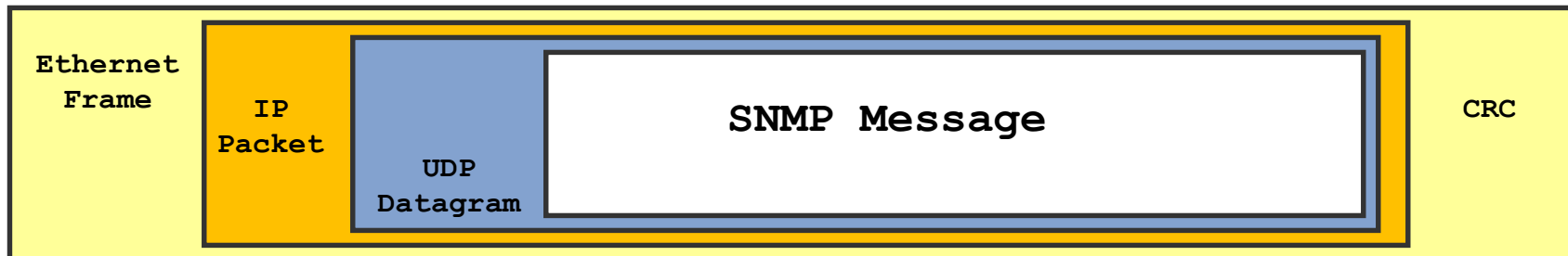
- Príklad: **.1.3.6.1.2.1.1**

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



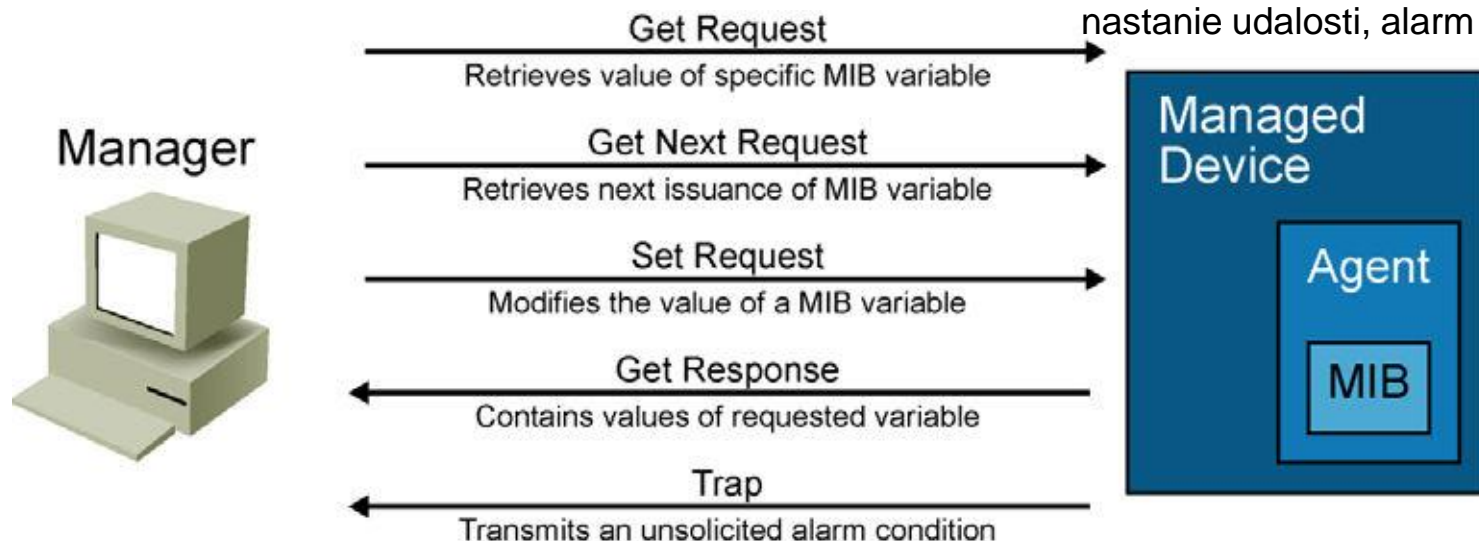
# Porty a UDP

- SNMP ako transportný mechanizmus používa User Datagram Protocol (UDP) s portami
  - 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 danej MIB premennej agenta
  - **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 Get Request a Get Next request
  - **Trap**
    - Zasielanie nevyžiadanej správy z agenta na manažéra. Zvyčajne nastanie udalosti, alarm a pod.



# 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 SNMP
  - SNMPv2C používa administratívny framework definovaný v SNMPv1, ktorý používa read/write komunitné reťazce (heslá) za účelom riadenia prístupu
- 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 nastáti udalosti
    - Prijem je potvrdzovaný

# SNMP Security

- SNMPv1 a v2 Community Strings (like passwords)
  - **READ-ONLY**
    - Overenie zasielaných Get & GetNext na SNMP agenta
    - Ak agent používa rovnaké reťaze odpovie na request
  - **READ-WRITE**
    - Overenie Get, GetNext, a Set.
    - Ak daný MIB objekt má ACCESS hodnotu typu read-write, Set správou môžeme zmeniť hodnotu premennej MIB objektu
  - **TRAP**
    - Spájanie entít do komunitných skupín

# SNMP Verzia 3

- RFCs 3410 až 3415
- Pridáva metodiku na zabezpečenie prenosu kritických dát medzi manažovanými zariadeniami
- SNMPv3 prináša tri úrovne zabezpečenia
  - **noAuthNoPriv:**
    - Autentifikácia nie je vyžadovaná, šifrovanie nie je poskytované
  - **authNoPriv**
    - Využíva autentifikáciu postavenú nad Hash-based Message Authentication Code with Message Digest 5 (HMAC-MD5) alebo Hash-based Message Authentication Code with Secure Hash Algorithm (HMAC-SHA).
    - Šifrovanie nie poskytované
  - **authPriv**
    - K autentifikácii sa pridáva šifrovanie cez Cipher Block Chaining-Data Encryption Standard (CBC-DES)
- Úroveň zabezpečenia definuje ku ktorému SNMP objektu môže používateľ pristupovať, pre čítanie, zápis alebo nastavenie notifikácie

# Porovnanie zabezpečenia SNMP verzií

SNMP Version	Security Level	Authentication	Encryption
SNMPv1	noAuthNoPriv	Community string	No
SNMPv2	noAuthNoPriv	Community string	No
SNMPv3	noAuthNoPriv	Username	No
	authNoPriv	MD5 or SHA-1	No
	authPriv	MD5 or SHA-1	DES, 3DES, or AES

# Odporúčania pre používanie SNMP

- Komunitné reťazce v SNMPv1 a SNMPv2 sú prenášané ako čistý text
  - Používaj dlhé reťazce
- Komunitné reťazce by sa mali meniť v pravidelných intervaloch podľa požiadaviek sieťovej politiky
  - Napr. pri zmene admina 😊
- Ak cez SNMP len monitorujeme zariadenia, treba používať len Read Only komunitu
- Na riadenie prístupu zo SNMP manažérov používaj ACL.
- Nasadenie SNMPv3 je vysoko odporúčané kvôli autentifikácii a šifrovaniu



# Základná konfigurácia SNMPv2c

- Nastavenie systémových informácií

```
configure terminal
snmp-server contact text
snmp-server location text
snmp-server chassis-id number
```

- Nastavenie SNMP komunít

```
snmp-server community string [view view-name] [ro | rw] [ipv6 nacl]
[access-list-number]
```

- Nastavenie cieľa pre zasielanie správ SNMP Trap

```
snmp-server host host-id [traps | informs]
[version {1 | 2c | 3 [auth | noauth | priv]}] community-string [udp-port port-
number] [notification-type]
```

- Aktivácia konkrétnych SNMP Trap správ

# Overenie

- Show access-list
- Show snmp chassis
- Show snmp community
- Show snmp host

# Základná konfigurácia SNMPv2c a jednoduchého zabezpečenia

```
Switch(config)# access-list 1 permit 10.1.1.0 0.0.0.255
Switch(config)# snmp-server chassis-id Cisco 3560 SN
FTX222222
Switch(config)# snmp-server community cisco RO 1
Switch(config)# snmp-server community xyz123 RW 1

! trapy
Switch(config)# snmp-server host 10.1.1.50 xyz123
Switch(config)# snmp-server enable traps ?
auth-framework      Enable SNMP CISCO-AUTH-FRAMEWORK-MIB traps
bgp                  Enable BGP traps
bridge               Enable SNMP STP Bridge MIB traps
bulkstat             Enable Data-Collection-MIB Collection
notifications
call-home             Enable SNMP CISCO-CALLHOME-MIB traps
...
Switch(config)# snmp-server trap-source vlan99
```

# SNMP Views

- 1.3.6.1.2.1.4.21 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipRouteTable-21).
- 1.3.6.1.2.1.4.22 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipNetToMediaTable-22).
- 1.3.6.1.2.1.4.35 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(ip-4).(ipNetToPhysicalTable-35).
- 1.3.6.1.2.1.3 is (iso-1).(org-3).(dod-6).(internet-1).(mgmt-2).(mib2-1).(atTable-3)

```
DLS1(config)#snmp-server view NMS-LIMIT iso included
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.35 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.3 excluded
```

```
DLS1# show snmp view
NMS-LIMIT iso - included nonvolatile active
NMS-LIMIT at - excluded nonvolatile active
NMS-LIMIT snmpUsmMIB - excluded nonvolatile active
NMS-LIMIT ip.21 - excluded nonvolatile active
NMS-LIMIT ip.22 - excluded nonvolatile active
NMS-LIMIT ip.35 - excluded nonvolatile active
vldefault iso - included permanent active
vldefault internet - included permanent active
```

# Konfigurácia SNMPv3

- **Step 1.** Configure an ACL to limit who has access SNMP access to the device.
- **Step 2.** Configure an SNMPv3 view using the `snmp-server view view-name` global configuration command.
- **Step 3.** Configure an SNMPv3 group using the `snmp-server group group-name` global configuration command.
- **Step 4.** Configure an SNMPv3 user using the `snmp-server user username groupname` global configuration command.
- **Step 5.** Configure an SNMPv3 trap receiver using the `snmp-server host` global configuration command.
- **Step 6.** Configure interface index persistence using the `snmp-server ifindex persist` global configuration command.

# SNMP Groups (SNMPv3)

- Spája Views s grupami (používatelia a prístupy)

```
! ACL
DLS1(config)# ip access-list standard NMS-SERVERS
DLS1(config-std-nacl)# permit 172.16.99.0 0.0.0.255

! pouzivatelialia
DLS1(config)# snmp-server user student ccnp-switch3 v3 auth sha
cisco123 priv aes 128 cisco123
ALS1(config)# snmp-server user student ccnp-switch2 v2c

! View
DLS1(config)#snmp-server view NMS-LIMIT iso included
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.21 excluded
DLS1(config)#snmp-server view NMS-LIMIT 1.3.6.1.2.1.4.22 excluded
...

!SNMP groups
DLS1(config)# snmp-server group ccnp-switch3 v3 priv read NMS-LIMIT
access NMS-SERVERS
!
ALS1(config)# snmp-server group ccnp-switch2 v2c read NMS-LIMIT
access NMS-SERVERS
```

# Sample SNMPv3 Configuration

```
R1(config)# ip access-list standard SNMPv3-ACL
R1(config-std-nacl)# remark ACL limits SNMP access to management network
R1(config-std-nacl)# permit 10.1.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)#
R1(config)# snmp-server view OPS sysUpTime included
R1(config)# snmp-server view OPS ifOperStatus included
R1(config)# snmp-server view OPS ifAdminStatus included
R1(config)# snmp-server view OPS ifDescr included
R1(config)#
R1(config)# snmp-server group MY-GROUP v3 priv read OPS write OPS access SNMPv3-ACL
R1(config)# snmp-server user ADMIN MY-GROUP v3 auth sha SNMP-Secret1 priv aes 256
SNMP-Secret2
*Nov  3 21:12:10.863: Configuring snmpv3 USM user, persisting snmpEngineBoots.
Please Wait...
R1(config)#
R1(config)# snmp-server enable traps
NHRP MIB is not enabled: Trap generation suppressed
However, configuration changes effective
R1(config)#
R1(config)# snmp-server host 10.1.1.254 traps version 3 priv ADMIN cpu
R1(config)#
R1(config)# snmp-server ifindex persist
R1(config)#
```

# Overenie

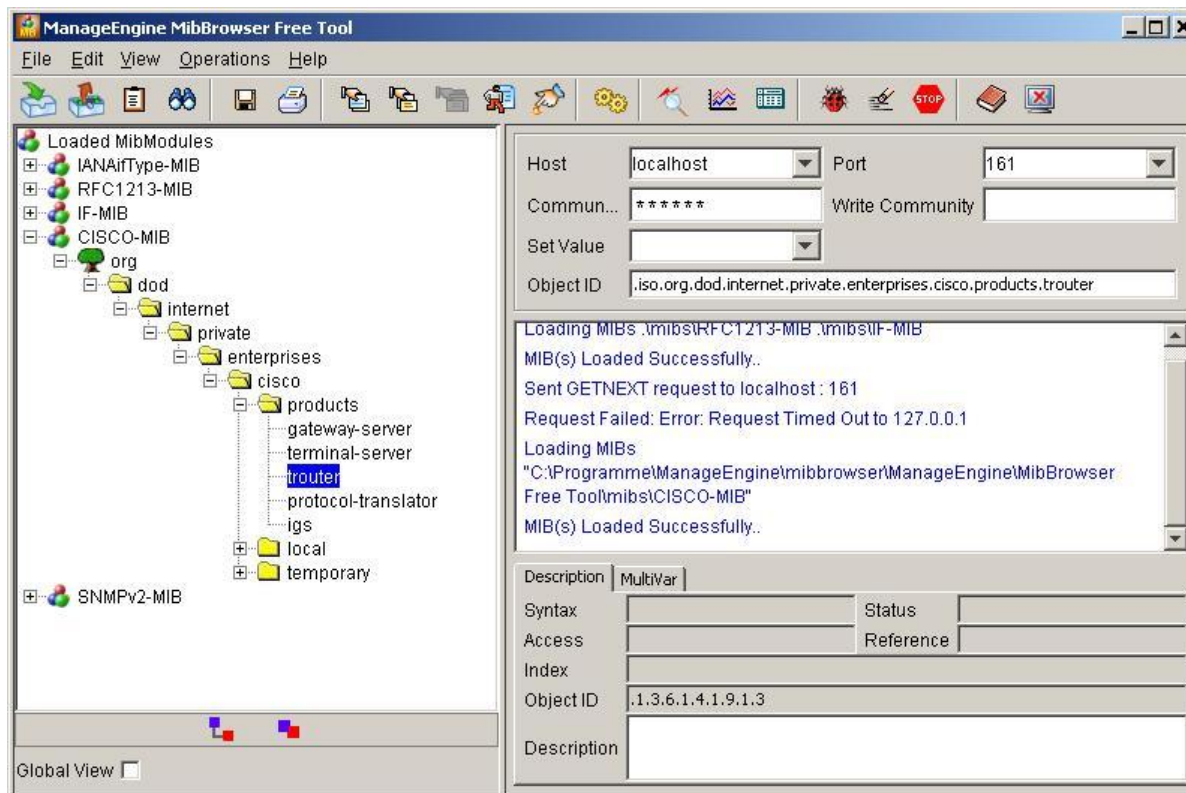
```
DLS1# show snmp
Chassis: FDT11111111
2932 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    20 Encoding errors
    1421 Number of requested variables
    0 Number of altered variables
...
```

```
DLS1# show snmp view
cac_view pimMIB - included read-only active
cac_view msdpMIB - included read-only active
cac_view ip - included read-only active
cac_view ospf - included read-only active
cac_view bgp - included read-only active
cac_view dot1dBridge - included read-only active
cac_view ipMRRouteStdMIB - included read-only active
cac_view igmpStdMIB - included read-only active
...
```



# Voľne šíriteľné SNMP MIB broser-y (walkers)

- Free SNMP MIB Browser Tools
  - <http://www.manageengine.com/products/mibbrowser-free-tool/>
- SnmpB
  - <http://sourceforge.net/projects/snmpb/>



# How to Configure SNMP Support

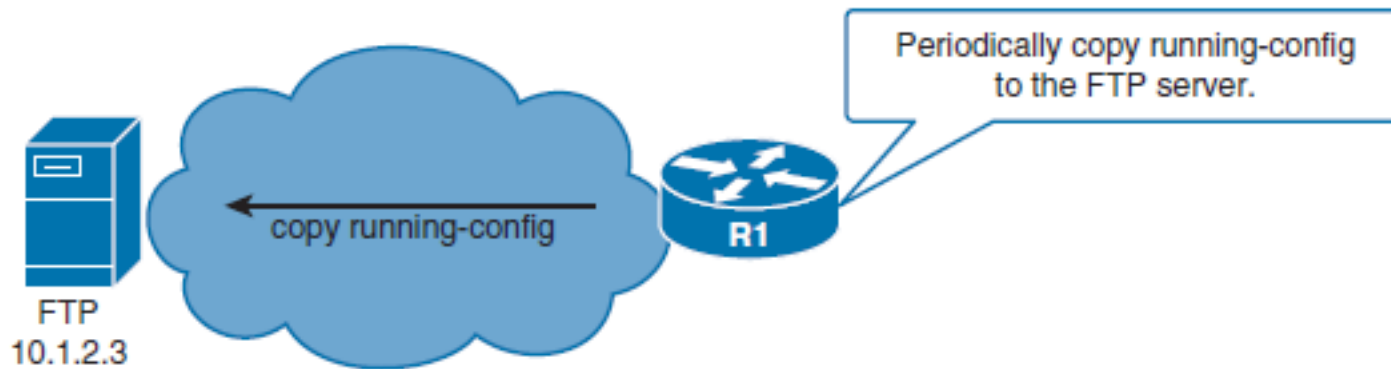
- [Configuring System Information](#)
- [Configuring SNMP Versions 1 and 2](#)
- [Configuring SNMP Version 3](#)
- [Configuring a Router as an SNMP Manager](#)
- [Enabling the SNMP Agent Shutdown Mechanism](#)
- [Defining the Maximum SNMP Agent Packet Size](#)
- [Limiting the Number of TFTP Servers Used via SNMP](#)
- [Disabling the SNMP Agent](#)
- [Configuring SNMP Notifications](#)
- [Configuring Interface Index Display and Interface Indexes and Long Name Support](#)
- [Configuring SNMP Support for VPNs](#)
- [Configuring Interface Index Persistence](#)
- [Configuring MIB Persistence](#)
- [Configuring Event MIB Using SNMP](#)
- [Configuring Event MIB Using the CLI](#)
- [Configuring Expression MIB Using SNMP](#)
- [Configuring Expression MIB Using the CLI](#)



# Riešenie zálohovania



# Konfigurácia zálohovania



- Na automatické zálohovanie sa používa príkaz **archive**
  - Jeho súčasťou je povinný parameter **path**, ktorý špecifikuje URL kam sa bude zálohovať
    - Môžeme zálohovať lokálne (flash) alebo vzdialene cez sieť (ftp, scp ...)
  - Súčasťou **path** môžu byť dve premenné
    - **\$h** bude nahradený menom zariadenia.
    - **\$t** bude nahradený dňom a časom vykonania archívu.

# Konfigurácia archivácie

## ■ Manuálna

```
R1(config)# archive
R1(config-archive)# path ftp://admin:cisco123@10.1.2.3/$h.cfg
R1(config-archive)# ^Z
R1#
```

```
R1# archive config
Writing R1.cfg-Sep-20-13-05-09.868-0
R1#
```

## ■ Automatická

```
R1(config)# archive
R1(config-archive)# write-memory
R1(config-archive)# time-period 10080
R1(config-archive)# end
R1#
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
Writing R1.cfg-Sep-20-13-15-09.496-1
R1#
```

# Overenie archivácie

```
R1# show archive
The maximum archive configurations allowed is 10.
The next archive will be named ftp://admin:cisco123@10.1.2.3/R1-5
Archive #   Name
0
1           ftp://admin:cisco123@10.1.2.3/R1-1
2           ftp://admin:cisco123@10.1.2.3/R1-2
3           ftp://admin:cisco123@10.1.2.3/R1-3
4           ftp://admin:cisco123@10.1.2.3/R1-4
```

# Nasadenie SCP služby

- The Secure Copy (SCP) feature provides a secure and authenticated method for copying router configuration or router image files.

## Enabling SCP on a Router

- **Step 1.** Use the `username name [ privilege level ] { secret password }` command for local authentication or configure TACACS+ or RADIUS.
- **Step 2.** Enable SSH. Configure a domain name using the `ip domain-name` and generating the crypto keys using the `crypto key generate rsa general key` global configuration commands.
- **Step 3.** AAA with the `aaa new-model` global configuration mode command.
- **Step 4.** Use the `aaa authentication login { default | list-name } method1 [ method2 ... ]` command to define a named list of authentication methods.
- **Step 5.** Use the `aaa authorization { network | exec | commands level } { default | listname } method1... [ method4 ]` command to configure command authorization.
- **Step 6.** Enable SCP server-side functionality with the `ip scp server enable` command.

# Príklad SCP konfigurácie

```
R1(config)# username ADMIN privilege 15 secret SCP-Secret
R1(config)# ip domain-name scp.cisco.com
R1(config)# crypto key generate rsa general-keys modulus 1024
The name for the keys will be: R1.scp.cisco.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 2 seconds)

R1(config)#
*Nov  3 22:25:28.135: %SSH-5-ENABLED: SSH 1.99 has been enabled
R1(config)# aaa new-model
R1(config)# aaa authentication login default group radius local-case
R1(config)# aaa authorization exec default group radius local
R1(config)# ip scp server enable
```



# Zakázanie nepoužívaných služieb

Service	Description of Service	Commands Used to Disable Service
DNS Name Resolution	If no DNS server is specifically mentioned in the router configuration, all the name queries are sent to the broadcast address of 255.255.255.255 by default.	Router(config)# <b>no ip domain-lookup</b>
CDP	The CDP is a proprietary protocol that Cisco devices use to identify their directly connected neighbors. CDP, like any other unnecessary local service, is considered potentially harmful to security.	Router(config)# <b>no cdp run</b> Router(config-if)# <b>no cdp enable</b>
NTP	If NTP is not used in the network, it should be disabled. You can disable the processing of NTP packets on a specific interface.	Router(config-if)# <b>ntp disable</b>

BOOTP Server	BOOTP uses UDP to formulate a network request to allow a device to obtain and configure its own IP information, such as IP address and subnet mask. However, the BOOTP protocol is seldom used, and it gives a hacker an opportunity to steal an IOS image.	Router(config)# <b>no ip bootp server</b>
DHCP	DHCP is essentially an extension of BOOTP.	Router(config)# <b>no ip dhcp-server</b>
Proxy ARP	Proxy ARP replies are sent to an ARP request destined for another device. When an intermediate Cisco device knows the MAC address of the destination device, it can act as a proxy. When an ARP request is destined for another Layer 3 network, a proxy ARP device extends a LAN perimeter by enabling transparent access between multiple LAN segments. This presents a security problem. An attacker can issue multiple ARP requests and use up the proxy ARP device's resources when it tries to respond to these requests in a DoS attack. Proxy ARP is enabled on Cisco router interfaces.	Router(config-if)# <b>no ip proxy-arp</b>
IP Source Routing	An option is found in the header of every IP packet. The Cisco IOS Software examines the option and acts accordingly. Sometimes an option indicates source routing. This means that the packet is specifying its own route. This feature poses a known security risk, such as a hacker taking control of a packet's route and directing it through the network. So, if source routing is not necessary in your network, you should disable it on all routers.	Router(config)# <b>no ip source-route</b>
IP Redirects	ICMP messages that are automatically sent by Cisco routers in response to various actions can give away a lot of information, such as routes, paths, and network conditions, to an unauthorized individual.	Router(config-if)# <b>no ip redirects</b>
HTTP Service	The Cisco IOS Software includes a web browser user interface from which you can issue Cisco IOS commands. You should disable HTTP server if it is not used.	Router(config)# <b>no ip http server</b>

# Podmienený debugging

- Obmedziť rozsah debug výstupov môžeme:
  - Použitím ACL
  - Aktivovaním podmieneného debugovania (conditional debugging)
- Napr.
  - `debug ip packet [ access-list ]`
    - Zobrazí všetky IP pakety prechádzajúce, generované či odosialané cez rozhrania smerovača
    - ACL obmedzí listing len na tie, ktoré budú mať permit
- Podmienené debugovanie
  - Nazývané aj ako podmienene spúšťané debugovanie (conditionally triggered debugging)
  - Sa používa
    - Obmedzenie aktivít per interface
      - Debuging pre všetky iné rozhrania okrem špecifikovaného bude vypnutý
    - Zapnutie debugovanie pre podmienené udalosti
      - Debug je zobrazený pre všetky rozhrania ale len pre špecifické udalosti

# Príklad podmieneného debugovania

- Debugovanie NAT a IP paketov prlen pre fa0/0 rozhranie.

```
R1# debug condition interface fa0/0
Condition 1 set
R1# debug ip packet detail
IP packet debugging is on (detailed)
R1#
R1# debug ip nat detailed
IP NAT detailed debugging is on
R1#
```



# Zabezpečenie radiacej roviny



**Control plane - Routing Protocol Authentication Option**

# Routing Protocol Authentication Options

- The purpose of routing protocol authentication
- Increasing the security of routing protocol authentication with time-based key chains
- Authentication options with different routing protocols

# The Purpose of Routing Protocol Authentication

- The falsification of routing information is a more subtle class of attack that targets the information carried within the routing protocol.
- The consequences of falsifying routing information are as follows:
  - Redirect traffic to create routing loops
  - Redirect traffic to monitor on an insecure line
  - Redirect traffic to discard it
- Two types of neighbor authentication can be used:
  - Plain-text authentication
  - Hashing authentication

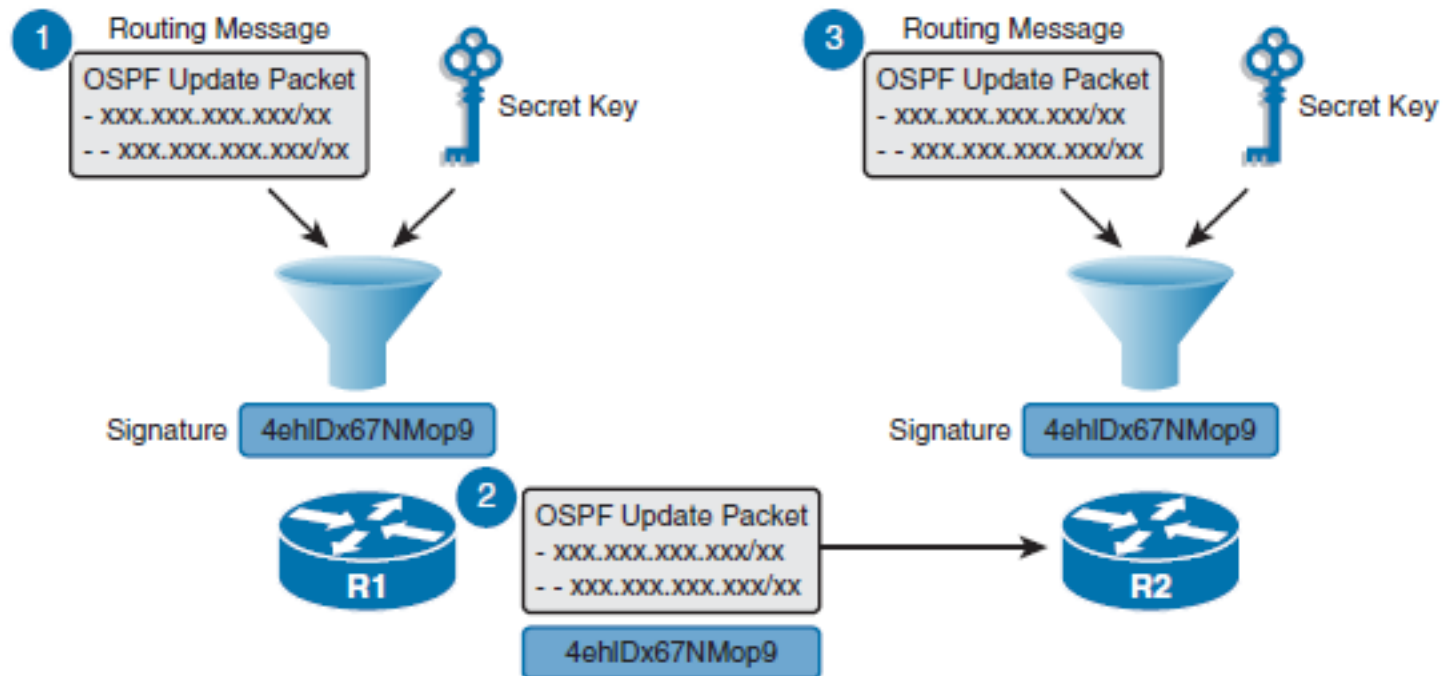
# Plain-Text Authentication



```
R1(config)# interface ethernet 0/1
R1(config-if)# ip ospf authentication
R1(config-if)# ip ospf authentication-key PLAINTEXT
% OSPF: Warning: The password/key will be truncated to 8 characters
R1(config-if)# ip ospf authentication-key PLAINTEX
R1(config-if)#
*Sep 21 11:45:53.670: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Ethernet0/1 from
FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
```

```
R2(config)# interface ethernet 0/0
R2(config-if)# ip ospf authentication
R2(config-if)# ip ospf authentication-key PLAINTEX
R2(config-if)#
*Sep 21 11:46:38.709: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Ethernet0/0 from
LOADING to FULL, Loading Done
R2(config-if)# exit
```

# Hashing Authentication





# Hashing Authentication

- The process can be explained in three steps:
- **Step 1.** When R1 sends a routing update to R2, it uses a hashing algorithm such as MD5 or SHA. The hashing algorithm is essentially a complex mathematical formula that uses the data in the OSPF update and a predefined secret key to generate a unique hash value (signature). The resulting signature can be derived only by using the OSPF update and the secret key that is only known to the sender and receiver.
- **Step 2.** The resulting signature is appended to the routing update and sent to R2.
- **Step 3.** When R2 receives the routing update and uses the same hashing algorithm as R1 to calculate a hash value. Specifically, it uses the data from the received OSPF update and its predefined secret key.

# Time-Based Key Chains

- Key Chain Specifics:
  - **Key ID:** Configured using the `key key-id key chain` configuration mode command. Key IDs can range from 1 to 255.
  - **Key string (password):** Configured using the `key-string password key chain` key configuration mode command.
  - **Key lifetimes:** (Optional) Configured using the `send-lifetime` and `accept-lifetime` key chain key configuration mode commands.

# Sample EIGRP Key Chain Configuration

```
R1(config)# key chain R1-Chain
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string firstkey
R1(config-keychain-key)# accept-lifetime 4:00:00 Jan 1 2015 Jan 31 2015
R1(config-keychain-key)# send-lifetime 4:00:00 Jan 1 2015 4:00:00 Jan 31 2015
R1(config-keychain-key)# exit
R1(config-keychain)# key 2
R1(config-keychain-key)# key-string secondkey
R1(config-keychain-key)# accept-lifetime 4:00:00 Jan 25 2015 Feb 28 2015
R1(config-keychain-key)# send-lifetime 4:00:00 Jan 25 2015 Feb 28 2015
R1(config-keychain-key)# end
R1#
```

# Authentication Options with Different Routing Protocols

<b>Routing Protocol</b>	<b>Plain Text Authentication</b>	<b>MD5 Hashing Authentication</b>	<b>SHA Hashing Authentication</b>	<b>Key Chain Support</b>
RIPv2	Yes	Yes	No	Yes
EIGRP	No	Yes	Yes, using named EIGRP	Yes
OSPFv2	Yes	Yes	Yes, using key chains	Yes
OSPFv3	No	Yes	Yes	No
BGP	No	Yes	No	No

# Autentifikácia v EIGRP



# Autentifikácia v EIGRP

- EIGRP pre IPv4 aj IPv6 podporuje len MD5 autentifikáciu na susedskej báze
  - Obsah EIGRP paketov nie je šifrovaný
  - Heslo sa neprenáša
    - Prenáša sa MD5 hash (message digest) počítaný z čísla kľúča (key ID) a hesla (key)
    - Odosielajúci pridať hash, prijímajúci počíta vlastnú a porovnáva s prijatou
- Spôsob konfigurácie je analogický ako v RIPv2, kľúče aj ich čísla musia byť zhodné
  1. Vytvorenie kľúčenky
    - Voliteľne parametre
  2. Aktivácia konkrétnej formy autentifikácie na rozhraní
  3. Aktivácia konkrétnej kľúčenky na rozhraní
- Je možné mať viaceré kľúče v kľúčenke
  - Platnosť môže byť voliteľne definovaná
  - Odosielajúci smerovač použije na počítanie hash prvý platný kľúč (od najnižšieho ID)
  - Prijímajúci smerovač skúša všetky kľúče v kľúčenke kým nie je zhoda

# Autentifikácia v EIGRP

- Vytvorenie kľúčenky

```
Router(config)# key chain MENO
Router(config-keychain)# key ČÍSLO
Router(config-keychain-key)# key-string HESLO
Router(config-keychain)# key INE_ČÍSLO
Router(config-keychain-key)# key-string INE_HESLO
```

- Aktivácia konkrétnej formy autentifikácie na rozhraní

```
Router(config-if)# ip authentication mode eigrp AS md5
```

- Aktivácia konkrétnej kľúčenky na rozhraní

```
Router(config-if)# ip authentication key-chain eigrp AS
MENO
```

# Časová platnosť klúčov

Router(config-keychain-key) #

```
accept-lifetime start-time {infinite | end-time | duration  
seconds}
```

- Voliteľný príkaz
  - definuje, odkedy dokedy akceptujeme pakety podpísané týmto klúčom

Router(config-keychain-key) #

```
send-lifetime start-time {infinite | end-time | duration  
seconds}
```

- Voliteľný príkaz
  - definuje, odkedy dokedy my používame pre odosielanie paketov daný klúč na podpisovanie

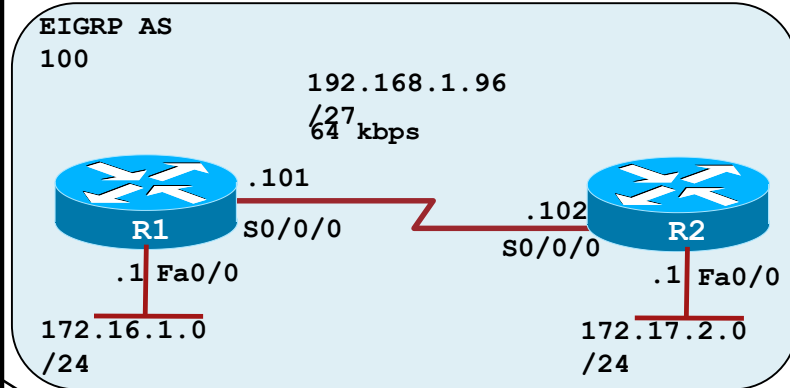


# Konfigurácia EIGRP MD5 autentifikácie s migráciou kľúčov

```

R1# show running-config
!
<output omitted>
!
key chain R1chain
key 1
  key-string FIRST-KEY
  accept-lifetime 04:00:00 Jan 1 2009 infinite
  send-lifetime 04:00:00 Jan 1 2009 04:00:00 Jan 31 2009
key 2
  key-string SECOND-KEY
  accept-lifetime 04:00:00 Jan 25 2009 infinite
  send-lifetime 04:00:00 Jan 25 2009 infinite
!
<output omitted>
!
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
!
interface Serial0/0/0
  bandwidth 64
  ip address 192.168.1.101 255.255.255.224
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 R1chain
!
router eigrp 100
  network 172.16.1.0 0.0.0.255
  network 192.168.1.0
  auto-summary

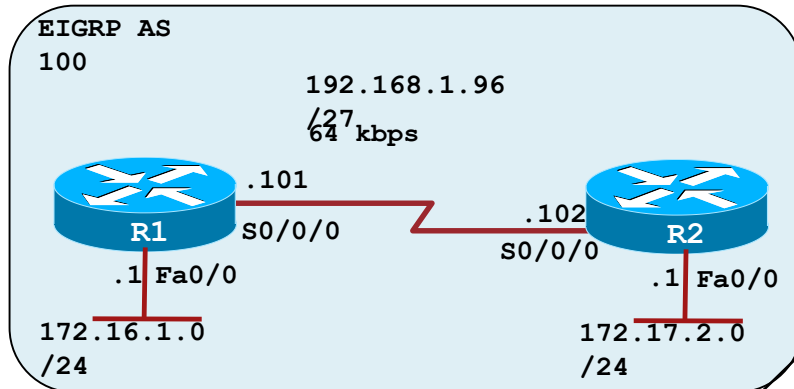
```



- R1 použije na odoslanie kľúč jedna od 1.1.2009 do 31.1.2009
- R1 akceptuje príjem kľúča jedna od 1.1.2009 do nekonečna

- R1 môže od 25.1.2009 používať na príjem aj odoslanie kľúč dva

# Konfigurácia EIGRP MD5 autentifikácie s migráciou kľúčov



- R2 bude používať na príjem aj odoslanie kľúč jedna od 1.1.2009 do nekonečna

- od 25.1.2009 môže R2 používať na príjem aj kľúč dva
- na odoslanie až keď kľúč jedna bude vymazaný alebo skončí životnosť

```

R2# show running-config
!
<output omitted>
!
key chain R2chain
  key 1
    key-string FIRST-KEY
    accept-lifetime 04:00:00 Jan 1 2009 infinite
    send-lifetime 04:00:00 Jan 1 2009 infinite
  key 2
    key-string SECOND-KEY
    accept-lifetime 04:00:00 Jan 25 2009 infinite
    send-lifetime 04:00:00 Jan 25 2009 infinite
!
<output omitted>
!
interface FastEthernet0/0
  ip address 172.17.2.2 255.255.255.0
!
interface Serial0/0/0
  bandwidth 64
  ip address 192.168.1.102 255.255.255.224
  ip authentication mode eigrp 100 md5
  ip authentication key-chain eigrp 100 R2chain
!
router eigrp 100
  network 172.17.2.0 0.0.0.255
  network 192.168.1.0
  auto-summary
  
```

# Overenie MD5 Authentication

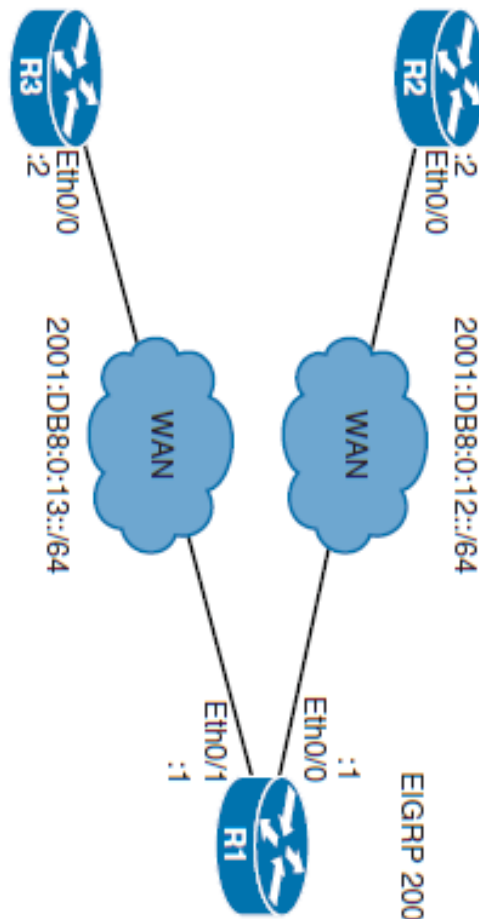
```
R1# show key chain
Key-chain R1chain:
  key 1 -- text "FIRST-KEY"
    accept lifetime (04:00:00 Jan 1 2009) - (always valid) [valid now]
    send lifetime (04:00:00 Jan 1 2009) - (04:00:00 Jan 31 2009)
  key 2 -- text "SECOND-KEY"
    accept lifetime (04:00:00 Jan 25 2009) - (always valid) [valid now]
    send lifetime (04:00:00 Jan 25 2009) - (always valid) [valid now]
```

# Diagnostika zlého hesla v EIGRP

```
R2# show ip eigrp neighbors
IP-EIGRP neighbors for process 100
R2#
```

```
R2# debug eigrp packets
EIGRP Packets debugging is on
  (UPDATE, REQUEST, QUERY, REPLY, HELLO, IPXSAP, PROBE, ACK, STUB, SIAQUERY, SIAREPLY)
*Jan 21 16:50:18.749: EIGRP: pkt key id = 2, authentication mismatch
*Jan 21 16:50:18.749: EIGRP: Serial0/0/0: ignored packet from 192.168.1.101, opcode = 5 (invalid
authentication)
*Jan 21 16:50:18.749: EIGRP: Dropping peer, invalid authentication
*Jan 21 16:50:18.749: EIGRP: Sending HELLO on Serial0/0/0
*Jan 21 16:50:18.749:   AS 100, Flags 0x0, Seq 0/0 idbQ 0/0 iidbQ un/rely 0/0
*Jan 21 16:50:18.753: %DUAL-5-NBRCHANGE: IP-EIGRP(0) 100: Neighbor 192.168.1.101
  (Serial0/0/0) is down: Auth failure
R2#
```

# Konfigurácia IPv6 EIGRP autentifikácie



```
R1(config)# key chain R1-IPv6-Chain
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string secret-1
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface ethernet 0/0
R1(config-if)# ipv6 authentication mode eigrp 200 md5
Sep 20 23:06:57.444: %DUAL-5-NBRCHANGE: EIGRP-IPv6 200: Neighbor
FE80::A8BB:CCFF:FE00:7400 (Ethernet0/0) is down: authentication mode changed
R1(config-if)# ipv6 authentication key-chain eigrp 200 R1-IPv6-Chain
R1(config-if)# end
R1#
```

```
R2(config)# key chain R2-IPv6-Chain
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string secret-1
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)# interface ethernet 0/0
R2(config-if)# ipv6 authentication mode eigrp 200 md5
R2(config-if)# ipv6 authentication key-chain eigrp 200 R2-IPv6-Chain
R2(config-if)# exit
R2(config)# exit
*Sep 20 23:13:09.602: %DUAL-5-NBRCHANGE: EIGRP-IPv6 200: Neighbor
FE80::A8BB:CCFF:FE00:5F00 (Ethernet0/0) is up: new adjacency
R2#
```

# Konfigurácia Named EIGRP autentifikácie

```
R1(config)# key chain NAMED-R1-Chain
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string secret-1
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# router eigrp ROUTE
R1(config-router)# address-family ipv4 autonomous-system 110
R1(config-router-af)# network 10.10.0.0 0.0.255.255
R1(config-router-af)# af-interface ethernet 0/0
R1(config-router-af-interface)# authentication key-chain NAMED-R1-Chain
R1(config-router-af-interface)# authentication mode hmac-sha-256 secret-2
R1(config-router-af-interface)# end
R1#
```



# Autentifikácia v OSPF

OSPFv2/OSPFv3



# Autentifikácia v OSPF

- V default stave OSPF nepoužíva autentifikáciu
- OSPFv2 podporuje
  - **Plain-text autentifikácia**
    - Najmenej bezpečná, jednoduchá autentifikácia heslom
    - Neodporúča sa pre produkčné prostredie
  - **MD5 autentifikácia**
    - Jednoduchá a zabezpečená autentifikácia
    - Odporúča sa používať ak nie je dostupná SHA autentifikácia.
  - **SHA autentifikácia**
    - Nazývaná aj ako **kryptografická autentifikácia**
    - Dostupná v IOS 15.4(1)T.
    - Momentálne najlepšia forma zabezpečenia, používa key chains



# Konfigurácia tzv. Simple Password Authentication (plaintext)

Router(config-if) #

```
ip ospf authentication-key password
```

- Na rozhraní nastaví heslo pre plaintext

Router(config-router) #

```
area area-id authentication
```

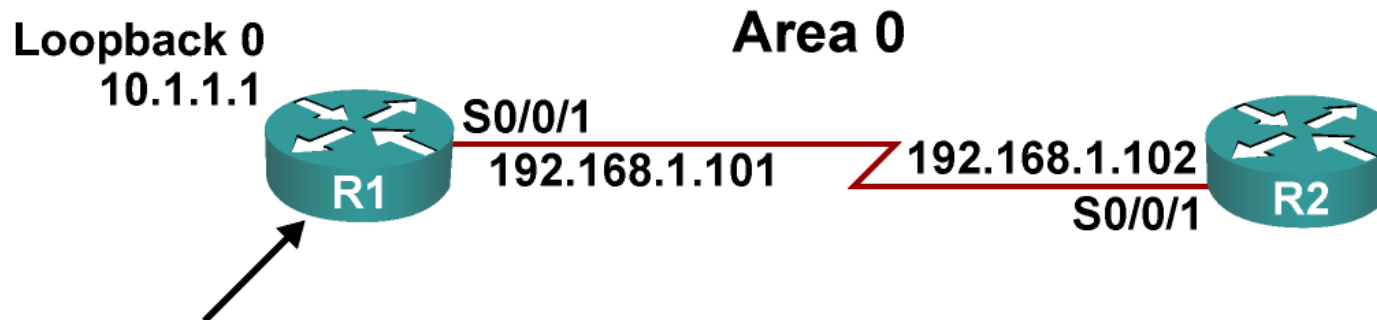
- Definuje druh autentifikácie pre oblasť (v tomto prípade plaintext)

Router(config-if) #

```
ip ospf authentication [null]
```

- Prepíše druh autentifikácie na konkrétnom rozhraní
  - bez argumentu aktivuje plaintext,
  - argument `null` deaktivuje autentifikáciu

# Príklad konfigurácie plaintext autentifikácie



```
<output omitted>
interface Loopback0
  ip address 10.1.1.1 255.255.255.0

<output omitted>
interface Serial0/0/1
  ip address 192.168.1.101 255.255.255.224
  ip ospf authentication
  ip ospf authentication-key plainpas

<output omitted>
router ospf 10
  log-adjacency-changes
  network 10.1.1.1 0.0.0.0 area 0
  network 192.168.1.0 0.0.0.255 area 0
```

314P\_076

# Diagnostika problémov pri Simple Password

- Simple authentication on R1, no authentication on R2:

```
R1# debug ip ospf adj
...
...
*Feb 17 18:51:31.242: OSPF: Rcv pkt from 192.168.1.102,
Serial0/0/1 : Mismatch Authentication type. Input packet specified
type 0, we use type 1

R2#
*Feb 17 18:50:43.046: OSPF: Rcv pkt from 192.168.1.101,
Serial0/0/1 : Mismatch Authentication type. Input packet specified
type 1, we use type 0
```

- Type 0 = Null
- Type 1 = Simple password
- Type 2 = MD5 password

# Konfigurácia MD5 autentifikácie

Router(config-if) #

```
ip ospf message-digest-key key-id md5 key
```

- Vytvorí kľúč so zadaným ID a heslom
  - Kľúče susedov sa musia zhodovať v ID i hesle
  - Ak je na rozhraní kľúčov viac, pre odosielanie sa používa naposledy pridaný (alebo všetky, ak sú na segmente routery s rôznymi kľúčmi), pre prijatie sa akceptuje ktorýkoľvek

Router(config-router) #

```
area area-id authentication message-digest
```

- Definuje druh autentifikácie pre oblasť (v tomto prípade MD5)

Router(config-if) #

```
ip ospf authentication {message-digest | null}
```

- Prepíše druh autentifikácie na konkrétnom rozhraní
  - argument `message-digest` aktivuje MD5
  - argument `null` deaktivuje autentifikáciu

# Príklad konfigurácie MD5 autentifikácie - rozhranie

```
R1(config)# interface ethernet 0/2
R1(config-if)# ip ospf authentication message-digest
R1(config-if)# ip ospf message-digest-key 1 md5 secret-1
R1(config-if)#
*Sep 21 14:56:55.750: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Ethernet0/2
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
```

```
R3(config)# interface ethernet 0/0
R3(config-if)# ip ospf authentication message-digest
R3(config-if)# ip ospf message-digest-key 1 md5 secret-1
R3(config-if)#
*Sep 21 14:57:41.473: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Ethernet0/0
from LOADING to FULL, Loading Done
R3(config-if)#
```

# Príklad konfigurácie MD5 autentifikácie - Area

```
R1(config)# interface ethernet 0/0
R1(config-if)# ip ospf message-digest-key 1 md5 secret-2
R1(config-if)# exit
R1(config)#
R1(config)# router ospf 1
R1(config-router)# area 0 authentication message-digest
R1(config-router)#
*Sep 21 15:22:27.614: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Ethernet0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-router)#
```

```
R4(config)# interface ethernet 0/0
R4(config-if)# ip ospf message-digest-key 1 md5 secret-2
R4(config-if)# exit
R4(config)# router ospf 1
R4(config-router)# area 0 authentication message-digest
R4(config-router)#
*Sep 21 15:23:12.394: %OSPF-5-ADJCHG: Process 1, Nbr 1.1.1.1 on Ethernet0/0 from
LOADING to FULL, Loading Done
R4(config-router)#
```

# OSPFv2 – kryptografická autentifikácia

- Konfiguruje sa v dvoch krokoch
  - Krok 1.
    - Vytvor kľúčenku

```
key-chain KEY-NAME  
    key KEY-ID  
        key-string HESLO  
        cryptographic-algorithm ALGORITMUS
```

- Krok 2.
  - Prirad' kľúčenku k rozhraniu

```
Ip ospf authentication key-chain KEY-NAME
```

# Konfigurácia OSPFv2 kryptografickej autentifikácie - príklad

```
R1(config)# key chain SHA-CHAIN
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string secret-1
R1(config-keychain-key)# cryptographic-algorithm ?
    hmac-sha-1      HMAC-SHA-1 authentication algorithm
    hmac-sha-256    HMAC-SHA-256 authentication algorithm
    hmac-sha-384    HMAC-SHA-384 authentication algorithm
    hmac-sha-512    HMAC-SHA-512 authentication algorithm
    md5             MD5 authentication algorithm

R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config-if)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA-CHAIN
R1(config-if)#
*Sep 21 16:53:03.227: %OSPF-5-ADJCHG: Process 1, Nbr 2.2.2.2 on Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
```



# Autentifikácia v OSPFv3

- OSPFv3 predpokladá využitie natívnej podpory IPSec v IPv6
  - Preto v OSPFv3 paketoch chýbajú polia pre autentifikáciu
  - Od IPSec požaduje buď IPv6 Authentication Header (AH) alebo IPv6 Encapsulating Security Payload (ESP).
- Nasadenie OSPFv3 autentifikácie vyžaduje
  - Najprv definovanie security policy
    - Obsahuje kombináciu kľúča a tzv. security parameter index (SPI)
    - SPI je identifikačný tag pridávaný do IPSec hlavičky.
- Autentifikácia môže byť konfigurovaná opäť buď na:
  - Per rozhranie
  - Per oblasť

# Príklad konfigurácie OSPFv3 autentifikácie - rozhranie

```
R1(config)# interface Ethernet0/1
R1(config-if)# ipv6 ospf authentication ipsec spi 300 sha1
1234567890123456789012345678901234567890
R1(config-if)#
*Sep 21 19:56:02.195: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R1(config-if)#
*Sep 21 19:56:35.245: %OSPFv3-5-ADJCHG: Process 1, IPv6, Nbr 2.2.2.2 on
Ethernet0/1 from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
```

```
R2(config)# interface Ethernet 0/0
R2(config-if)# ipv6 ospf authentication ipsec spi 300 sha1 1234567890123456789012345
678901234567890
R2(config-if)#
*Sep 21 19:58:51.543: %CRYPTO-6-ISA_KMP_ON_OFF: ISAKMP is ON
R2(config-if)#
*Sep 21 19:58:55.179: %OSPFv3-5-ADJCHG: Process 1, IPv6, Nbr 1.1.1.1
on Ethernet0/0 from LOADING to FULL, Loading Done
R2(config-if)#
```

# Príklad konfigurácie OSPFv3 autentifikácie - oblasť

```
R1(config)# router ospfv3 1
R1(config-router)# area 0 authentication ipsec spi 500 sha1 123456789012345678901234
5678901234567890
R1(config-router)#
*Sep 21 20:02:24.415: %OSPFv3-5-ADJCHG: Process 1, IPv6, Nbr 4.4.4.4 on
Ethernet0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-router)#
```

```
R4(config)# router ospfv3 1
R4(config-router)# area 0 authentication ipsec spi 500 sha1 123456789012345678901234
5678901234567890
R4(config-router)#
*Sep 21 20:02:29.367: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
R4(config-router)#
*Sep 21 20:02:31.186: %OSPFv3-5-ADJCHG: Process 1, IPv6, Nbr 1.1.1.1
on Ethernet0/0 from LOADING to FULL, Loading Done
R4(config-router)#
```



# Autentifikácia v BGP

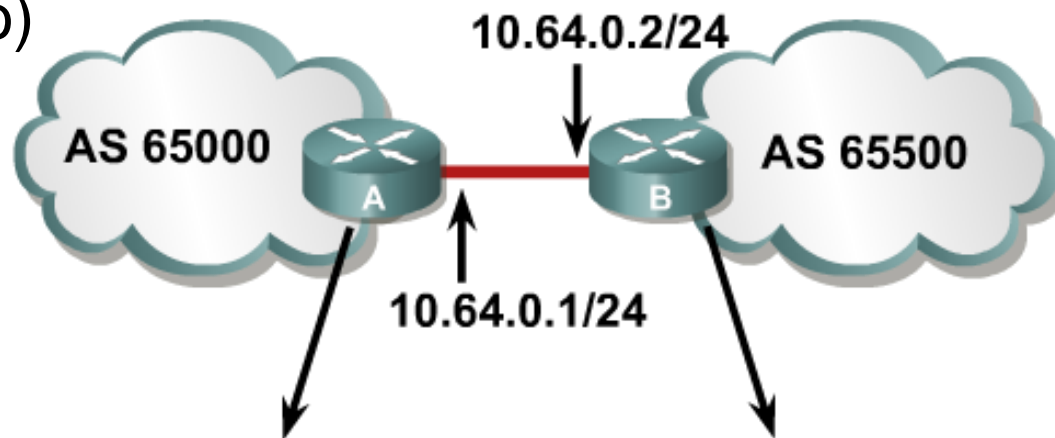


# Autentifikácia v BGP

Router (config-router) #

```
neighbor {ip-address | peer-group-name} password string
```

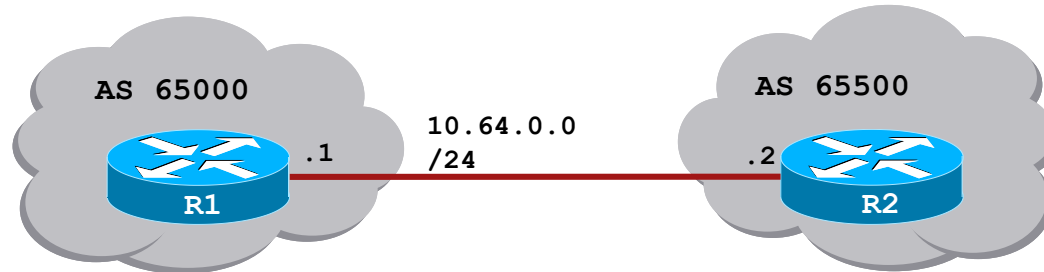
- BGP používa MD5 autentifikáciu
  - Hash sa počíta z hesla (key) a správy
- Pre každého suseda sa môže definovať nezávislý kľúč (heslo)



```
router bgp 65500
neighbor 10.64.0.2 remote-as 65500
neighbor 10.64.0.2 password v6lne0qkel33&
```

```
router bgp 65500
neighbor 10.64.0.1 remote-as 65000
neighbor 10.64.0.1 password v6lne0qkel33&
```

# Príklad konfigurácie MD5 autentifikácie



```
R1(config)# router bgp 65000
R1(config-router)# neighbor 10.64.0.2 remote-as 65500
R1(config-router)# neighbor 10.64.0.2 password BGP-Pa55w0rd
R1(config-router)#
```

```
R2(config)# router bgp 65500
R2(config-router)# neighbor 10.64.0.1 remote-as 65000
R2(config-router)# neighbor 10.64.0.1 password BGP-Pa55w0rd
R2(config-router)#
```

## Diagnostika:

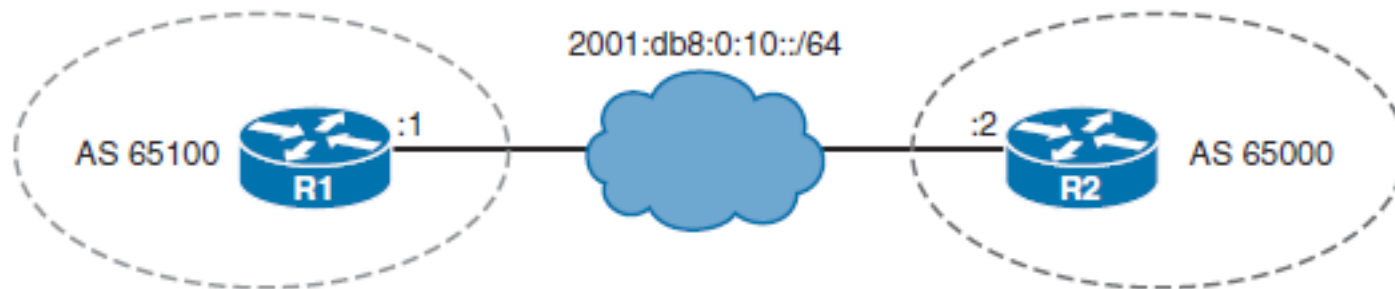
Ak jeden smerovač má heslo pre suseda a druhý nemá:

```
%TCP-6-BADAUTH: No MD5 digest from 10.1.0.2(179) to 10.1.0.1(20236)
```

Ak oba smerovače majú heslá, ale nesprávne:

```
%TCP-6-BADAUTH: Invalid MD5 digest from 10.1.0.1(12293) to
10.1.0.2(179)
```

# Príklad konfigurácie MD5 autentifikácie - BGP IPv6



```
R1(config)# router bgp 65100
R1(config-router)# neighbor 2001:db8:0:10::2 remote-as 65000
R1(config-router)# neighbor 2001:db8:0:10::2 password secret-2
R1(config-router)#
```

```
R2(config)# router bgp 65000
R2(config-router)# neighbor 2001:db8:0:10::1 remote-as 65100
R2(config-router)# neighbor 2001:db8:0:10::1 password secret-2
R2(config-router)#
```

VRF-Lite





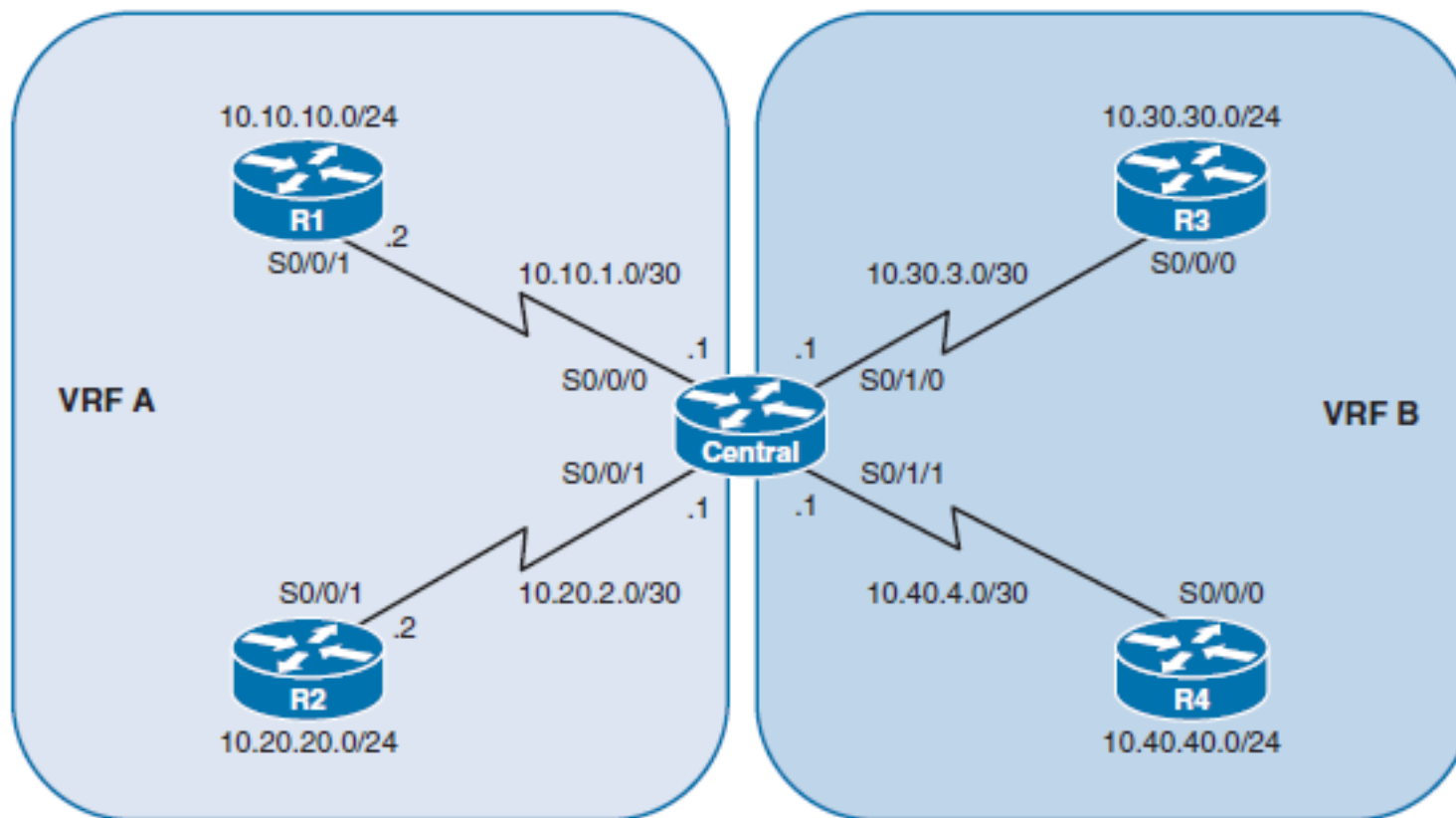
# VRF-Lite

- Virtual Routing and Forwarding (VRF)
  - je technológia, ktorá umožňuje zariadeniu mať viaceré separované smerovacie tabuľky pracujúce simultánne
    - Niečo ako VLAN na L2
  - VRF inštancia je niečo ako logický smerovač, ktorý sa skladá:
    - Smerovacej tabuľky
    - Z forwarding tabuľky
    - Sady rozhraní, ktoré využívajú danú FW tabuľku
    - Sady pravidiel a smerovacích protokolov, ktoré určujú čo bude do FW tabuľky vložené
- VRF zvyšuje
  - Sieťovú funkcionality tým, že umožňuje udržiavať separované cesty bez toho aby bolo treba mať viaceré zariadenia
  - Sieťovú bezpečnosť oddelením sieťových tokov
- Service providers (SPs) využívajú VRF na tvorbu oddelených virtuálnych privátnych sietí (VPNs) zákazníkov s oddelenými smerovacími tabuľkami
  - Preto občas sa VRF volá ako *VPN routing and forwarding* .

# VRF a VRF-Lite

- Cisco odlišuje
  - VRF
  - VRF-Lite
- **VRF** typicky je asociované a využíva sa v SP prostredí spolu s MPLS (Multiprotocol Label Switching)
  - MPLS oddeľuje toky zákazníkov vo VPN
  - VRF udržiava separovane smerovacie informácie zákazníkov
    - Predpoklad, že môžu používať napr. Rovnaké privátne rozsahy
- **VRF-Lite** je nasadenie VRF bez MPLS
  - Oddeľujeme len smerovacie informácie
  - Umožňuje SP udržiavať dve a viac separovaných VPN (napr. s prekrývaným adresovaním)
  - Na odlíšenie ktoré smerovacie info do ktorej VRF sa používa vstupné rozhranie
    - Je jedno či fyzické alebo logické
    - Avšak môže patriť len do jednej VRF

# Konfigurácia VRF



# Konfigurácia VRF

```
Central(config)# ip vrf VRF-A
Central(config-vrf)# exit
Central(config)# ip vrf VRF-B
Central(config-vrf)# exit
Central(config)# interface Serial0/0/0
Central(config-if)# ip vrf forwarding VRF-A
Central(config-if)# ip address 10.10.1.1 255.255.255.252
Central(config-if)# clock rate 2000000
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
Central(config-if)# interface Serial0/0/1
Central(config-if)# ip vrf forwarding VRF-A
Central(config-if)# ip address 10.20.2.1 255.255.255.252
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
Central(config-if)# interface Serial0/1/0
Central(config-if)# ip vrf forwarding VRF-B
Central(config-if)# ip address 10.30.3.1 255.255.255.252
Central(config-if)# clock rate 2000000
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
Central(config-if)# interface Serial0/1/1
Central(config-if)# ip vrf forwarding VRF-B
Central(config-if)# ip address 10.40.4.1 255.255.255.252
Central(config-if)# no shut
Central(config-if)# exit
Central(config)#
```

# Overenie smerovacej tabuľky pri použití VRF

```
Central# show ip route | begin Gateway
Gateway of last resort is not set

Central#
Central# show ip route vrf VRF-A | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.1.0/30 is directly connected, Serial0/0/0
L       10.10.1.1/32 is directly connected, Serial0/0/0
C       10.20.2.0/30 is directly connected, Serial0/0/1
L       10.20.2.1/32 is directly connected, Serial0/0/1
Central#
Central# show ip route vrf VRF-B | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.30.3.0/30 is directly connected, Serial0/1/0
L       10.30.3.1/32 is directly connected, Serial0/1/0
C       10.40.4.0/30 is directly connected, Serial0/1/1
L       10.40.4.1/32 is directly connected, Serial0/1/1
Central#
```

# Named EIGRP s použitím VRF-A

```
Central(config)# router eigrp 1
Central(config-router)# address-family ipv4 vrf VRF-A
Central(config-router-af)# network 10.10.1.0 0.0.0.3
Central(config-router-af)# network 10.20.2.0 0.0.0.3
Central(config-router-af)# autonomous-system 1
Central(config-router-af)# no auto-summary
Central(config-router-af)#
*Aug  5 04:45:35.879: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.20.2.2
(Serial0/0/1) is up: new adjacency
*Aug  5 04:45:35.883: %DUAL-5-NBRCHANGE: EIGRP-IPv4 1: Neighbor 10.10.1.2
(Serial0/0/0) is up: new adjacency
Central(config-router-af)# ^Z
Central#
```

# Overenie smerovacej tabuľky pre VRF-A

```
Central# show ip route vrf VRF-A | begin Gateway
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C       10.10.1.0/30 is directly connected, Serial0/0/0
L       10.10.1.1/32 is directly connected, Serial0/0/0
D       10.10.10.0/24 [90/2297856] via 10.10.1.2, 00:00:06, Serial0/0/0
C       10.20.2.0/30 is directly connected, Serial0/0/1
L       10.20.2.1/32 is directly connected, Serial0/0/1
D       10.20.20.0/24 [90/2297856] via 10.20.2.2, 00:05:41, Serial0/0/1

Central# show ip eigrp neighbors
EIGRP-IPv4 Neighbors for AS(1)
% No usable Router-ID found

Central#
Central# show ip eigrp vrf VRF-A neighbors
EIGRP-IPv4 Neighbors for AS(1) VRF(VRF-A)
```

H	Address	Interface	Hold (sec)	Uptime	SRTT (ms)	RTO	Q Cnt	Seq Num
1	10.20.2.2	Se0/0/1	13	00:43:42	3	100	0	4
0	10.10.1.2	Se0/0/0	11	00:47:54	1	100	0	5

```
Central#
```

# Povolenie OSPF pre VRF-B

```
Central(config)# router ospf 1 vrf VRF-B
Central(config-router)# router-id 5.5.5.5
Central(config-router)# network 10.30.3.0 0.0.0.3 area 0
Central(config-router)# network 10.40.4.0 0.0.0.3 area 0
Central(config-router)#
*Aug  5 04:47:22.327: %OSPF-5-ADJCHG: Process 1, Nbr 3.3.3.3 on Serial0/1/0 from
LOADING to FULL, Loading Done
*Aug  5 04:47:22.467: %OSPF-5-ADJCHG: Process 1, Nbr 4.4.4.4 on Serial0/1/1 from
LOADING to FULL, Loading Done
Central(config-router)# ^Z
Central#
```



# Overenie smerovacej tabuľky pre VRF-B

```
Central# show ip route vrf VRF-B | begin Gateway
Gateway of last resort is not set

    10.0.0.0/8 is variably subnetted, 6 subnets, 3 masks
C       10.30.3.0/30 is directly connected, Serial0/1/0
L       10.30.3.1/32 is directly connected, Serial0/1/0
O       10.30.30.0/24 [110/65] via 10.30.3.2, 00:05:07, Serial0/1/0
C       10.40.4.0/30 is directly connected, Serial0/1/1
L       10.40.4.1/32 is directly connected, Serial0/1/1
O       10.40.40.0/24 [110/65] via 10.40.4.2, 00:07:30, Serial0/1/1
Central#
```

