Contents

CAPITOLUL 6. DEVICE MONITORING AND MANAGEMENT

6.0 Introduction

6.0.1 - Scope

Infractorii cibernetici încearcă să exploateze fiecare vulnerabilitate posibilă. De exemplu, infractorii cibernetici ar putea:

- *Obține acces la routerul de bază și șterge fișierele de configurare IOS și Startup (cunoscute ca fișiere de bootset).*
- *Accesa un serviciu neutilizat care este încă operațional pe dispozitiv.*
- *Injecta informații false de rutare într-o rețea OSPF convergentă.*

Prima parte a cursului va oferi tehnici de atenuare împotriva unor astfel de atacuri.

A doua parte a acestui curs discută monitorizarea rețelei și instrumentele de monitorizare a rețelei, pentru a ne ajută să apărăm și să protejăm rețeaua.

6.0.2 – Obiective

Implementarea managementului securizat și monitorizarea dispozitivelor din rețea.

Topic Title	Topic Objective
Secure Cisco IOS Image and Configuration Files	Explicarea modului de cum sunt utilizate caracteristica de configurare rezistentă Cisco IOS și Secure Copy pentru a securiza imaginea Cisco IOS și fișierele de configurare.
Lock Down a Router Using AutoSecure	Utilizarea comenzilor corecte pentru AutoSecure pentru a activa securitatea pe routerele bazate pe IOS.
Routing Protocol Authentication	Utilizarea comenzilor corecte pentru a configura autentificarea protocolului de rutare.
Secure Management and Reporting	Compararea accesului de gestionare în bandă și în afara de bandă.
Network Security Using Syslog	Explicarea modului de configurare syslog pentru a înregistra evenimentele de sistem.
NTP Configuration	Configurare NTP pentru a activa marcarea temporală precisă între toate dispozitivele.
SNMP Configuration	Configurare SNMP pentru a monitoriza starea sistemului.

6.1 Secure Cisco IOS Image and Configuration Files

6.1.1 - Cisco IOS Resilient Configuration Feature

Caracteristica de configurare rezistentă Cisco IOS permite o recuperare mai rapidă dacă cineva reformatează memoria flash în mod rău intenționat sau neintenționat sau șterge fișierul de configurare de pornire din memoria nevolatilă cu acces aleatoriu (NVRAM). Caracteristica menține o copie de lucru sigură a fișierului imagine IOS al routerului și o copie a fișierului de configurare care rulează. Aceste fișiere securizate nu pot fi eliminate de către utilizator și sunt denumite in setul de pornire principal.

Iată câteva fapte despre configurația rezistentă Cisco IOS:

- *Fișierul de configurare din setul de pornire primar este o copie a configurației care rulează care se afla în router atunci când caracteristica a fost activată pentru prima dată.*
- *Caracteristica securizează cel mai mic set de fișiere de lucru pentru a păstra spațiul de stocare persistent.*
- *Nu este necesar spațiu suplimentar pentru a securiza fișierul imagine Cisco IOS principal. Caracteristica detectează automat imaginea sau nepotrivirea versiunii de configurare.*
- *Numai stocarea locală este utilizată pentru securizarea fișierelor, eliminând provocările de întreținere a scalabilității din stocarea mai multor imagini și configurații pe serverele TFTP.*
- *Funcția poate fi dezactivată numai printr-o sesiune de consolă.*

Notă: caracteristica este disponibilă numai pe routerele mai vechi care acceptă o interfață flash PCMCIA Advanced Technology Attachment (ATA). Routerele mai noi, cum ar fi ISR 4000, nu acceptă această caracteristică.

6.1.2 - Enable the IOS Image Resilience Feature

Comenzile pentru a securiza imaginea IOS și fișierul de configurare care rulează sunt prezentate în exemplu. Pentru a securiza imaginea IOS și a activa rezistența imaginii Cisco IOS, se utilizaeaza comanda secure boot-image global configuration mode. Când este activată pentru prima dată, imaginea Cisco IOS care rulează este securizată și este generată o intrare de jurnal. Caracteristica de rezistență a imaginii Cisco IOS poate fi dezactivată numai printr-o sesiune de consolă folosind forma no a comenzii. Această comandă funcționează corect numai

atunci când sistemul este configurat să ruleze o imagine de pe o unitate flash cu o interfață ATA. În plus, imaginea care rulează trebuie să fie încărcată din stocarea persistentă pentru a fi securizată ca principală. Imaginile care sunt încărcate dintr-o locație la distanță, cum ar fi un server TFTP, nu pot fi securizate.

Pentru a face un instantaneu al routerului care rulează configurația și a o arhiva în siguranță în stocarea persistentă, se utilizează comanda secure boot-config global configuration mode, așa cum se arată în figură. Pe consolă este afișat un mesaj de jurnal care anunță utilizatorul că reziliența de configurare este activată. Arhiva de configurare este ascunsă și nu poate fi vizualizată sau eliminată direct din promptul CLI. Se poate utiliza comanda secure boot-config în mod repetat pentru a actualiza arhiva de configurare la o versiune mai nouă după ce au fost emise noi comenzi de configurare.

Fișierele securizate nu apar în rezultatul unei comenzi dir care este emisă din CLI. Acest lucru se datorează faptului că sistemul de fișiere Cisco IOS împiedică listarea fișierelor securizate. Imaginea care rulează și arhivele de configurare care rulează nu sunt vizibile în ieșirea comenzii dir. Se utilizează comanda show secure bootset pentru a verifica existența arhivei, așa cum se arată în secventa de cod de mai jos.

```
  R1(config)# secure boot-image
  R1(config)#
  Sep 22 12:47:10.183: %IOS_RESILIENCE-5-IMAGE_RESIL_ACTIVE: Successfully
secured running image
  R1(config)#
  R1(config)# secure boot-config
  R1(config)#
  Sep 22 12:47:18.259: %IOS_RESILIENCE-5-CONFIG_RESIL_ACTIVE: Successfully
secured config archive [flash0:.runcfg-20200922-124717.ar]
  R1(config)#
  R1(config)# exit
  R1#
  Sep 22 12:47:22.783: %SYS-5-CONFIG_I: Configured from console by console
  R1# show secure bootset
  IOS resilience router id FTX1449AJBJ
  IOS image resilience version 15.4 activated at 12:47:09 UTC Tue Sep 22
2022
  Secure archive flash0:c2900-universalk9-mz.SPA.154-3.M.bin type is image
(elf) []
    file size is 103727964 bytes, run size is 103907016 bytes
    Runnable image, entry point 0x81000000, run from ram
  IOS configuration resilience version 15.4 activated at 12:47:18 UTC Tue
Sep 22 2022
  Secure archive flash0:.runcfg-20200922-124717.ar type is config
  configuration archive size 1683 bytes
  R1#
```

6.1.3 - The Primary Bootset Image

Restaurarea unui set de pornire primar dintr-o arhivă securizată după ce ruterul a fost modificat, așa cum se arată în următorii pași și exemplu:

Pasul 1. Reîncărcare router utilizând comanda reload. Dacă este necesar, se lanseaza secvența de pauză pentru a intra în modul monitor ROM (ROMmon).

Pasul 2. Din modul ROMmon, se introduce comanda dir pentru a lista conținutul dispozitivului care conține fișierul de bootset securizat.

Pasul 3. Se porneste routerul cu imaginea de pornire securizată folosind comanda de pornire urmată de locația memoriei flash (de exemplu, flash0), două puncte și numele fișierului găsit la ***Pasul*** 2.

Pasul 4. Se intra în modul de configurare globală și se restaureaza configurația securizată la un nume de fișier la alegere utilizând comanda ***secure boot-config restore*** urmată de locația memoriei flash (de exemplu, flash0), două puncte și un nume de fișier la alegere. În figură, este folosit numele de fișier rescue-cfg.

Pasul 5. Se iese din modul de configurare globală și se lanseaza comanda de copiere pentru a copia fișierul de configurare salvat în configurația care rulează.

```
Router# reload
<Issue Break sequence, if necessary>
rommon 1 > dir flash0:
program load complete, entry point: 0x80803000, size: 0x1b340
Directory of flash0:

4    103727964  -rw-     c2900-universalk9-mz.SPA.154-3.M.bin
   rommon 2 > boot flash0:c2900-universalk9-mz.SPA.154-3.M.bin <Router
reboots with specified image>
Router> enable
Router# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# secure boot-config restore flash0:rescue-cfg
ios resilience:configuration successfully restored as flash0:rescue-cfg
 Router(config)# end
Router# copy flash0:rescue-cfg running-config
Destination filename [running-config]?
%IOS image resilience is already active
%IOS configuration resilience is already active
2182 bytes copied in 0.248 secs (8798 bytes/sec)
R1#
```

6.1.4 - Configure Secure Copy

Caracteristica Cisco IOS Resilient oferă o metodă de securizare a imaginii IOS și a fișierelor de configurare local pe dispozitiv. Caracteristica Secure Copy Protocol (SCP) este

utilizată pentru a copia de la distanță aceste fișiere. SCP oferă o metodă sigură și autentificată pentru copierea configurației routerului sau a fișierelor imagine a routerului într-o locație de la distanță.

SCP se bazează pe:

- *SSH pentru a securiza comunicarea*
- *AAA pentru a furniza autentificare și autorizare*

Notă: Configurația AAA va fi tratată mai detaliat într-un capitol ulterior.

Se utilizează următorii pași pentru a configura un router pentru SCP pe server cu AAA local:

Pasul 1. Configurare SSH, dacă nu este deja configurat.

Pasul 2. Pentru autentificare locală, se configureaza cel puțin un utilizator de bază de date locală cu nivel de privilegii 15.

Pasul 3. Activare AAA cu comanda modului de configurare globală aaa new-model.

Pasul 4. Se utilizează comanda locală implicită aaa authentication login pentru a specifica că baza de date locală va fi utilizată pentru autentificare.

Pasul 5. Se utilizează comanda locală implicită aaa authorization exec pentru a configura autorizarea comenzii. În acest exemplu, toți utilizatorii locali vor avea acces la comenzile EXEC.

Pasul 6. Activarea funcționalitatatii serverului SCP cu comanda ***ip scp server enable***.

În exemplu, R1 este acum un server SCP și va folosi conexiuni SSH pentru a accepta transferuri de copii securizate de la utilizatori autentificați și autorizați. Transferurile pot proveni de la orice client SCP, indiferent dacă acel client este un alt router, comutator sau stație de lucru.

```
R1(config)# ip domain-name security.com
R1(config)# crypto key generate rsa general-keys modulus 2048
R1(config)#  username Bob privilege 15 algorithm-type scrypt secret
cisco12345
R1(config)# aaa new-model
R1(config)# aaa authentication login default local
R1(config)# aaa authorization exec default local
R1(config)# ip scp server enable
```

Dacă presupunem că vrem să copiem în siguranță configurația de rezervă a unui router numit R2 pe serverul SCP, care este R1, după cum se arată în rezultatul comenzii de mai jos, vom folosi comanda copy pe R2 și vom specifica mai întâi locația fișierului sursă

(flash0:R2backup.cfg) și apoi destinația (scp:). După ce se răspunde la seria de solicitări pentru a stabili o conexiune la serverul SCP de pe R1, fișierul va fi copiat.

```
R2# copy flash0:R2backup.cfg scp:
Address or name of remote host []? 10.1.1.1
Destination username [R2]? Bob
Destination filename [R2backup.cfg]?
Writing R2backup.cfg
Password: <cisco12345>
!
1381 bytes copied in 8.596 secs (161 bytes/sec)
R2#
```

Pe R1, se poate introduce comanda ***debug ip scp*** pentru a urmări trecerea transferului, așa cum se arată în exemplul următor. Cea mai frecventă problemă de autentificare este o combinație incorectă de nume de utilizator/parolă. Există, de asemenea, o eroare de autentificare dacă combinația nume de utilizator/parolă nu a fost configurată cu cuvântul cheie privilegiu 15 pe serverul SCP.

```
R1# debug ip scp
Incoming SCP debugging is on
R1#
*Feb 18 20:37:15.363: SCP: [22 -> 10.1.1.2:61656] send *Feb 18
20:37:15.367: SCP: [22 <- 10.1.1.2:61656] recv C0644 1381 R2backup.cfg *Feb
18 20:37:15.367: SCP: [22 -> 10.1.1.2:61656] send
```

6.1.5 - Recover a Router Password

Dacă un router este compromis sau trebuie recuperat dintr-o parolă configurată greșit, un administrator trebuie să utilizeze proceduri de recuperare a parolei, cum ar fi cele prezentate în pașii de mai jos. Din motive de securitate, recuperarea parolei necesită ca administratorul să aibă acces fizic la router printr-un cablu de consolă. În funcție de dispozitiv, procedura detaliată pentru recuperarea parolei variază.

Pasul 1. Conectare la portul de consolă.

Pasul 2. Utilizare comanda show version pentru a afișa setarea registrului de configurare și pentru a documenta valoarea (de exemplu, 0x2102).

Pasul 3. Pornire router.

Pasul 4. Emite secvența de pauză (de exemplu, CTRL-BREAK) pentru a intra în modul ROMMON.

Pasul 5. Schimbare registrul de configurare implicit cu comanda confreg 0x2142.

Pasul 6. Repornire router utilizând comanda de resetare în modul ROMMON.

Pasul 7. Apăsare Ctrl-C pentru a sări peste procedura de configurare inițială.

Pasul 8. Intrare în modul EXEC privilegiat.

Pasul 9. Copiere configurație de pornire în configurația de rulare utilizând comanda copy startup-config running-config.

Pasul 10. Verificare configurație.

Pasul 11. Schimbare parola secretă de activare.

Pasul 12. Activare toate interfețele folosind comanda no shutdown.

Pasul 13. Revenire la setarea registrului de configurare la setarea originală care a fost documentată în ***Pasul*** 2 cu comanda de configurare globală config-register. La următoarea repornire, routerul va folosi aceste setări și va încărca noul fișier de configurare de pornire care conține parola schimbată.

Pasul 14. Salvare modificări de configurare.

6.1.6 - Password Recovery

Dacă cineva a obținut acces fizic la un router, ar putea obține controlul asupra dispozitivului respectiv prin procedura de recuperare a parolei. Această procedură, dacă este efectuată corect, lasă intactă configurația routerului. Dacă atacatorul nu face modificări majore, acest tip de atac este greu de detectat. Un atacator poate folosi această metodă de atac pentru a descoperi configurația routerului și alte informații relevante despre rețea, cum ar fi fluxurile de trafic și restricțiile de control al accesului.

Un administrator poate atenua această potențială încălcare a securității utilizând comanda modului de configurare globală ***no service password-recovery***. Această comandă este o comandă Cisco IOS ascunsă și nu are argumente sau cuvinte cheie. Dacă un router este configurat cu comanda no service password-recovery, tot accesul la modul ROMmon este dezactivat.

Când este introdusă comanda de recuperare a parolei fără servicii, se afișează un mesaj de avertizare și trebuie confirmat înainte ca caracteristica să fie activată, așa cum se arată în exemplu.

```
R1(config)# no service password-recovery
WARNING:
Executing this command will disable password recovery
mechanism.
Do not execute this command without another plan for
password recovery.
Are you sure you want to continue? [yes/no]: yes
R1(config)#
```

Când este configurată, comanda show running-config afișează o declarație de recuperare a parolei fără servicii, așa cum se arată in exemplul urmator.

```
R1# show running-config
Building configuration...
Current configuration : 836 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
no service password-recovery
```

După cum se arată mai jos, atunci când routerul este pornit, secvența inițială de pornire afișează un mesaj care spune că FUNCȚIONALITATEA DE RECUPERAREA PAROLEI ESTE DEZACTIVATĂ.

```
System Bootstrap, Version 12.4(13r)T, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2006 by cisco Systems, Inc.
PLD version 0x10
GIO ASIC version 0x127
c1841 platform with 131072 Kbytes of main memory
Main memory is configured to 64 bit mode with parity disabled

PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x8000f000, size:0xcb80
```

Pentru a recupera un dispozitiv după introducerea comenzii de recuperare a parolei fără servicii, se inițiaza secvența de pauză în cinci secunde după ce imaginea se decomprima în timpul pornirii. Se solicită confirmarea acțiunii tastei de pauză. După ce acțiunea este confirmată, configurația de pornire este complet ștearsă, procedura de recuperare a parolei este activată și routerul pornește cu configurația implicită din fabrică. Dacă nu se confirma acțiunea de întrerupere, routerul pornește în mod normal, cu comanda de recuperare a parolei fără servicii activată.

ATENȚIE: Dacă memoria flash a routerului nu conține o imagine Cisco IOS validă din cauza coruperii sau ștergerii, comanda ROMmon xmodem nu poate fi utilizată pentru a încărca o nouă imagine flash. Pentru a repara routerul, un administrator trebuie să obțină o nouă imagine Cisco IOS pe un SIMM flash sau pe un card PCMCIA. Cu toate acestea, dacă un administrator are acces la ROMmon, acesta poate restaura un fișier IOS în memoria flash folosind un server TFTP.

6.2 Lock Down a Router Using AutoSecure

6.2.1 - Discovery Protocols CDP and LLDP

Routerele Cisco sunt implementate inițial cu multe servicii care sunt activate implicit. Acest lucru se face pentru comoditate și pentru a simplifica procesul de configurare necesar pentru a pune dispozitivul în funcțiune. Cu toate acestea, unele dintre aceste servicii pot face dispozitivul vulnerabil la atac dacă securitatea nu este activată. Administratorii pot activa, de asemenea, servicii pe routerele Cisco care pot expune dispozitivul la riscuri semnificative. Ambele scenarii trebuie luate în considerare la securizarea rețelei.

Cisco Discovery Protocol (CDP) este un exemplu de serviciu care este activat implicit pe routerele Cisco. Protocolul Link Layer Discovery (LLDP) este un standard deschis care poate fi activat pe dispozitivele Cisco, precum și pe alte dispozitive de la furnizori care acceptă LLDP.

Configurarea și verificarea LLDP este similară cu CDP. În figură, R1 și S1 sunt ambele configurate cu LLDP, folosind comanda lldp run global configuration. Ambele dispozitive rulează CDP în mod implicit. Ieșirea pentru show cdp neighbors detail și show lldp neighbors detaliu va dezvălui adresa unui dispozitiv, platforma și detaliile sistemului de operare.

```
R1(config)# lldp run
R1(config)# end
R1# show cdp neighbors detail
-------------------------
Device ID: S1
Entry address(es):
  IP address: 192.168.1.254
Platform: cisco WS-C2960-24TT-L, Capabilities: Switch IGMP
Interface: GigabitEthernet0/1, Port ID (outgoing port): FastEthernet0/5
Holdtime : 164 sec
Version :
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
R1# show lldp neighbors detail
------------------------------------------------
Local Intf: Gi0/1
Chassis id: 0022.9121.0380
Port id: Fa0/5
Port Description: FastEthernet0/5
System Name: S1
System Description:
Cisco IOS Software, C2960 Software (C2960-LANBASEK9-M), Version
15.0(2)SE7,
RELEASE SOFTWARE (fc1)
<output omitted>
```

Din păcate, atacatorii nu trebuie să aibă dispozitive compatibile CDP sau LLDP pentru a aduna aceste informații sensibile. Software-ul ușor disponibil, cum ar fi Universal Network CDP & LLDP Evaluator (UNCLE), permite oricărui computer din rețea să capteze și să vizualizeze informațiile CDP și LLDP care sunt trimise pe o rețea LAN. În plus, CDP este vulnerabil la atacurile de falsificare CDP, deoarece CDP utilizează o adresă MAC binecunoscută de multicast. Aceasta este o formă de atac de denial of service care poate copleși tabelele CDP ale dispozitivului cu mesaje CDP false.

6.2.2 - Settings for Protocols and Services

Atacatorii aleg servicii și protocoale care fac rețeaua mai vulnerabilă la exploatarea rău intenționată.

Multe dintre aceste caracteristici ar trebui să fie dezactivate sau restricționate în funcție de nevoile de securitate ale unei organizații. Aceste caracteristici variază de la protocoale de descoperire a rețelei, cum ar fi CDP și LLDP, până la protocoale disponibile la nivel global, cum ar fi ICMP și alte instrumente de scanare.

Unele dintre setările implicite din software-ul Cisco IOS sunt acolo din motive istorice. Erau setări implicite logice în momentul în care software-ul a fost scris inițial. Alte setări implicite au sens pentru majoritatea sistemelor, dar pot crea expuneri de securitate dacă sunt utilizate în dispozitive care fac parte dintr-o apărare a perimetrului rețelei. Alte valori implicite sunt cerute de standarde, dar nu sunt întotdeauna de dorit din punct de vedere al securității.

Tabelul rezumă caracteristicile și setările implicite pentru protocoale și servicii.

Feature	**Default**
Cisco Discovery Protocol (CDP)	Enabled
Link Layer Discovery Protocol (LLDP)	Disabled
Configuration autoloading	Disabled
FTP server	Disabled
TFTP server	Disabled
Network Time Protocol (NTP) service	Disabled
Packet assembler/disassembler (PAD) service	Enabled
TCP and User Datagram Protocol (UDP) minor services	Enabled in versions 11.3 and later
Maintenance Operation Protocol (MOP) service	Enabled on most Ethernet interfaces
Simple Network Management Protocol (SNMP)	Enabled
HTTP or HTTPS configuration and monitoring	Setting is Cisco device dependent.
Domain Name System (DNS)	Enabled

Feature	Default
Internet Control Message Protocol (ICMP) redirects	Enabled
IP source routing	Enabled
Finger service	Enabled
ICMP unreachable notifications	Enabled
ICMP mask reply	Disabled
IP identification service	Enabled
TCP keepalives	Disabled
Gratuitous ARP (GARP)	Enabled
Proxy ARP	Enabled

Tabelul de mai jos prezintă setările de securitate recomandate pentru protocoale și servicii.

Există mai multe practici importante disponibile pentru a vă asigura că un dispozitiv este sigur:

- *Dezactivarea serviciilor și interfețelor inutile.*
- *Dezactivarea și restricționarea serviciilor de management configurate în mod obișnuit, cum ar fi SNMP.*
- *Dezactivarea sondelor și scanărilor, cum ar fi ICMP. Asigurarea securitatii accesului la terminal.*
- *Dezactivarea protocoalelor de rezoluție a adreselor (ARP) gratuite și proxy.*
- *Dezactivarea transmisiilor direcționate pe IP.*

Feature	Recommendation
Cisco Discovery Protocol (CDP)	Ar trebui să fie dezactivat la nivel global sau pe bază de interfață dacă nu este necesar.
Link Layer Discovery Protocol (LLDP)	Ar trebui să fie dezactivat la nivel global sau pe bază de interfață dacă nu este necesar.
Configuration autoloading	Ar trebui să rămână dezactivat atunci când nu este utilizat de router.
FTP server	Ar trebui să fie dezactivat atunci când nu este necesar.
TFTP server	Ar trebui să fie dezactivat atunci când nu este necesar.
Network Time Protocol (NTP) service	Ar trebui să fie dezactivat atunci când nu este necesar.
Packet assembler/disassembler (PAD) service	Ar trebui să fie dezactivat în mod explicit atunci când nu este utilizat.
TCP and User Datagram Protocol (UDP) minor services	Dezactivarea acestui serviciu în mod explicit.

Feature	Recommendation
Maintenance Operation Protocol (MOP) service	Ar trebui să fie dezactivat în mod explicit atunci când nu este utilizat.
Simple Network Management Protocol (SNMP)	Dezactivarea acestui serviciu atunci când nu este necesar.
HTTP or HTTPS configuration and monitoring	Dezactivarea serviciului dacă nu este necesar. Dacă acest serviciu este necesar, se restricționeaza accesul la serviciul HTTP sau HTTPS al routerului folosind liste de control al accesului (ACL).
Domain Name System (DNS)	Dezactivare când nu este necesar. Dacă este necesar serviciul de căutare DNS, se asigură că a fost setata adresa serverului DNS în mod explicit.
Internet Control Message Protocol (ICMP) redirects	Dezactivarea când nu este necesară.
IP source routing	Dezactivarea acestui serviciu atunci când nu este necesar.
Finger service	Dezactivarea acestui serviciu atunci când nu este necesar.
ICMP unreachable notifications	Dezactivarea interfețelor către rețele de neîncredere.
ICMP mask reply	Dezactivarea interfețelor către rețele de neîncredere.
IP identification service	Serviciul ar trebui să fie dezactivat în mod explicit.
TCP keepalives	Ar trebui să fie activat la nivel global pentru a gestiona conexiunile TCP și pentru a preveni anumite atacuri de tip denial of service (DoS). Serviciul este activat în versiunile software Cisco IOS înainte de Cisco IOS Release 12.0 și este dezactivat în Cisco IOS Release 12.0 și ulterioare. Dezactivarea acestui serviciu atunci când nu este necesar.
Gratuitous ARP (GARP)	Dezactivarea ARP-urilor gratuite pe fiecare interfață de router, cu excepția cazului în care acest serviciu este necesar.
Proxy ARP	Dezactivarea acestui serviciu pe fiecare interfață, cu excepția cazului în care routerul este utilizat ca punte LAN.

6.2.3 - Cisco AutoSecure

Lansat în versiunea IOS 12.3, Cisco AutoSecure este o caracteristică care este inițiată din CLI și execută un script. AutoSecure face mai întâi recomandări pentru remedierea vulnerabilităților de securitate și apoi modifică configurația de securitate a routerului, așa cum se arată în figură.

AutoSecure poate bloca funcțiile planului de management și serviciile și funcțiile planului de redirecționare ale unui router. Există mai multe servicii și funcții ale planului de management:

- *Securizare BOOTP, CDP, FTP, TFTP, PAD, UDP și TCP servere mici, MOP, ICMP (redirecționări, răspunsuri cu masca), rutare sursă IP, criptare Finger, parole, TCP keepalives, ARP gratuit, ARP proxy și difuzare direcționată*
- *Notificare legală folosind un banner*

- *Parolă sigură și funcții de conectare*
- *NTP securizat*
- *Acces SSH securizat*
- *Servicii de interceptare TCP*

Există trei servicii și funcții de redirecționare pe care le activează AutoSecure:

1. ***Cisco Express Forwarding (CEF)***
2. ***Filtrarea traficului cu ACL-uri***
3. ***Inspecție Cisco IOS firewall pentru protocoale comune***

AutoSecure este adesea folosit pe teren pentru a oferi o politică de securitate de bază pe un nou router. Caracteristicile pot fi apoi modificate pentru a sprijini politica de securitate a organizației.

```
R1# auto secure
  --- AutoSecure Configuration ---
 *** AutoSecure configuration enhances the security
 of the router but it will not make router
 absolutely secure from all security attacks ***
 All the configuration done as part of AutoSecure
will be shown here. For more details of why and
how this configuration is useful, and any possible
side effects, please refer to Cisco documentation of
AutoSecure.
 At any prompt you may enter '?' for help.
Use ctrl-c to abort this session at any prompt.
 Gathering information about the router for
AutoSecure
 Is this router connected to internet? [no]:yes
```

6.2.4 - Cisco AutoSecure Command Syntax

Utilizarea comenzii de securitate automată pentru a activa configurarea caracteristicii Cisco AutoSecure. Această configurație poate fi interactivă sau non-interactivă. Secventa de cod de mai jos arată sintaxa comenzii pentru comanda auto secure.

```
  Router# auto secure {no-interact | full} [forwarding | management] [ntp |
login | ssh | firewall | top-intercept]
```

Iată parametrii comenzii.

```
  R1# auto secure ?
    forwarding   Secure Forwarding Plane
    management   Secure Management Plane
    no-interact  Non-interactive session of AutoSecure
    <cr>
  R1#
```

Notă: Opțiunile pot varia în funcție de platformă.

În modul interactiv, routerul solicită opțiuni pentru a activa și dezactiva serviciile și alte funcții de securitate. Acesta este modul implicit, dar poate fi configurat și folosind comanda completă auto secure.

Modul non-interactiv este configurat cu comanda auto secure no-interact. Aceasta va executa automat caracteristica Cisco AutoSecure cu setările implicite recomandate de Cisco. Comanda auto secure poate fi introdusă și cu cuvinte cheie pentru a configura componente specifice, cum ar fi planul de management (cuvânt cheie de gestionare) și planul de redirecționare (cuvânt cheie de redirecționare).

Optional Parameters	Description
no-interact	Utilizatorului nu i se va solicita nicio configurație interactivă. Nu vor fi configurați parametrii de dialog interactiv, inclusiv numele de utilizator sau parolele.
full	Utilizatorului i se vor solicita toate întrebările interactive. Aceasta este setarea implicită.
forwarding	Doar planul de expediere va fi securizat.
management	Doar planul de management va fi securizat.
ntp	Specifică configurația caracteristicii NTP în CLI AutoSecure.
login	Specifică configurația caracteristicii de conectare în CLI AutoSecure.
ssh	Specifică configurația caracteristicii SSH în CLI AutoSecure.
firewall	Specifică configurația caracteristicii firewall în AutoSecure CLI.
tcp-intercept	Specifică configurația caracteristicii de interceptare TCP în CLI AutoSecure.

6.2.5 - Cisco AutoSecure Configuration Example

Când este inițiată comanda de securitate automată, un expert CLI îi conduce pe administratori prin configurarea dispozitivului. Este necesară introducerea utilizatorului.

P1. Este introdusă comanda de securitate automată. Routerul afișează mesajul de bun venit al asistentului de configurare AutoSecure, așa cum se arată.

```
R1# auto secure
--- AutoSecure Configuration ---
 *** AutoSecure configuration enhances the security of the router, but it
will not make it
absolutely resistant to all security attacks ***
 AutoSecure will modify the configuration of your device. All configuration
changes will be
shown. For a detailed explanation of how the configuration changes enhance
security and any
possible side effects, please refer to Cisco.com for Autosecure
documentation.
At any prompt you may enter '?' for help.
```

```
Use ctrl-c to abort this session at any prompt.
 Gathering information about the router for AutoSecure
 <continued>
```

P2. Expertul adună informații despre interfețele exterioare, așa cum se arată mai jos.

```
Gathering information about the router for AutoSecure
 Is this router connected to internet? [no]: yes
Enter the number of interfaces facing the internet [1]:
 Interface                  IP-Address      OK? Method  Status
Protocol
FastEthernet0/0       192.168.10.1    YES manual up                    up
FastEthernet0/1       192.168.11.1    YES manual up                    up
FastEthernet0/1/0     unassigned      YES unset  up                    down
FastEthernet0/1/1     unassigned      YES unset  up                    down
FastEthernet0/1/2     unassigned      YES unset  up                    down
FastEthernet0/1/3     nassigned       YES unset  up                    down
Serial0/0/0           192.168.2.101   YES manual up                    up
Serial0/0/1           unassigned      YES manual administratively down down
Vlan1                 unassigned      YES manual up                    down
Enter the interface name that is facing the internet: Serial 0/0/0
Invalid interface name
Enter the interface name that is facing the internet: Serial0/0/0
 <continued>
```

P3. AutoSecure securizează planul de management prin dezactivarea serviciilor inutile, după cum se arată in urmatoarea secventa.

```
Securing Management plane services...

Disabling service finger
Disabling service pad
Disabling udp & tcp small servers
Enabling service password encryption
Enabling service tcp-keepalives-in
Enabling service tcp-keepalives-out
Disabling the cdp protocol

Disabling the bootp server
Disabling the http server
Disabling the finger service
Disabling source routing
Disabling gratuitous arp
 <continued>
```

P4. AutoSecure solicită un banner, așa cum se arată.

```
Here is a sample Security Banner to be shown at every access to device.
Modify it
to suit your enterprise requirements.
 Authorized Access only
  This system is the property of So-&-So-Enterprise.
  UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
  You must have explicit permission to access this
  device. All activities performed on this device
  are logged. Any violations of access policy will result
  in disciplinary action.
 Enter the security banner {Put the banner between k and k, where k is any
character}:
#*********     AUTHORIZED ACCESS ONLY ***********
     UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.
```

```
   You must have explicit permission to access this
   device. Any violations of access policy will result
   in disciplinary action.  #
<continued>
```

P5. AutoSecure solicită parole și activează funcțiile de parolă și de conectare, după cum se arată.

```
Enable secret is either not configured or is the same as enable password
Enter the new enable secret: cisco123
Confirm the enable secret : cisco123
Enter the new enable password: cisco1
% Password too short - must be at least 6 characters. Password
configuration failed
Enter the new enable password: cisco321
Confirm the enable password: cisco321
Configuring AAA local authentication
Configuring Console, Aux and VTY lines for local authentication, exec-
timeout,
and transport
Securing device against Login Attacks
Configure the following parameters
 Blocking Period when Login Attack detected: 120
Maximum Login failures with the device: 2
Maximum time period for crossing the failed login attempts: 60
 Configure SSH server? [yes]: y
 <continued>
```

P6. Interfețele sunt securizate, așa cum se arată.

```
Configuring interface specific AutoSecure services
Disabling the following ip services on all interfaces:
  no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
Disabling mop on Ethernet interfaces
 <continued>
```

P7. Planul de expediere este securizat, așa cum se arată.

```
Securing Forwarding plane services...
 Enabling CEF (This might impact the memory requirements for your platform)
Enabling unicast rpf on all interfaces connected to internet
 Configure CBAC Firewall feature? [yes/no]: yes
```

Când expertul este complet, o configurație care rulează afișează toate setările și modificările de configurare.

Notă: AutoSecure ar trebui să fie utilizat atunci când un router este configurat inițial. Nu este recomandat pe routerele de producție.

6.3 Routing Protocol Authentication

6.3.1 Dynamic Routing Protocols

Protocoalele de rutare dinamică sunt folosite de routere pentru a partaja automat informații despre accesibilitatea și starea rețelelor de la distanță. Protocoalele de rutare dinamică efectuează mai multe activități, inclusiv descoperirea rețelei și menținerea tabelelor de rutare.

Avantajele importante ale protocoalelor de rutare dinamică sunt capacitatea de a selecta cea mai bună cale și capacitatea de a descoperi automat o nouă cale ca fiind cea mai bună atunci când există o schimbare în topologie.

Descoperirea rețelei este capacitatea unui protocol de rutare de a partaja informații despre rețelele despre care știe de la alte routere care folosesc, de asemenea, același protocol de rutare. În loc să depindă de rutele statice configurate manual către rețelele de la distanță pe fiecare router, un protocol de rutare dinamică permite ruterelor să învețe automat despre aceste rețele de la alte routere. Aceste rețele și cea mai bună cale către fiecare, sunt adăugate la tabelul de rutare al routerului și identificate ca o rețea învățată printr-un protocol specific de rutare dinamică.

Figura prezintă routerele R1 și R2 care utilizează un protocol comun de rutare pentru a partaja informații de rețea.

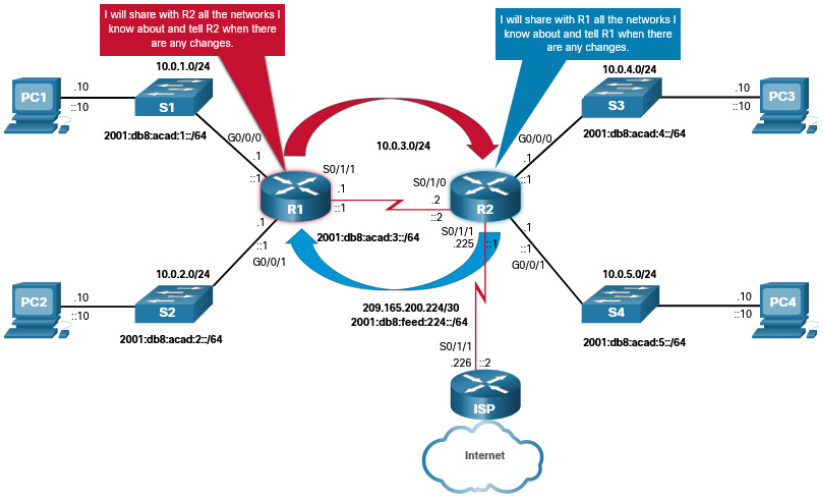


Fig. 6.1. Folosirea unui protocol obisnuit pentru rutare.

6.3.2 - Routing Protocol Spoofing

Sistemele de rutare pot fi atacate prin întreruperea ruterelor de rețea peer-to-peer sau prin falsificarea informațiilor transportate în cadrul protocoalelor de rutare. Informațiile de rutare falsificate pot fi utilizate în general pentru a determina sistemele să dezinformeze (mint) unele pe altele, să provoace un atac DoS sau să determine traficul să urmeze o cale pe care nu ar urma-o în mod normal. Există mai multe consecințe ale falsificării informațiilor de rutare:

- *Redirecționarea traficului pentru a crea bucle de rutare*
- *Redirecționarea traficului astfel încât să poată fi monitorizat pe o legătură nesigură*
- *Redirecționarea traficului pentru a-l renunța*

Presupunem că un atacator s-a putut conecta direct la legătura dintre R1 și R2. Atacatorul trimite R1 informații false de rutare care indică faptul că R2 este destinația preferată către rețeaua 192.168.10.0/24. Deși R1 are deja o intrare în tabelul de rutare în rețeaua 192.168.10.0/24, noua rută are o metrică mai mică și, prin urmare, este intrarea preferată în tabelul de rutare.

În consecință, atunci când PC3 trimite un pachet către PC1 (192.168.10.10/24), R3 redirecționează pachetul către R2 care, la rândul său, îl transmite către R1. R1 nu transmite pachetul către gazda PC1. În schimb, direcționează pachetul către R2, deoarece cea mai bună cale aparentă către 192.168.10.0 /24 este prin R2. Când R2 primește pachetul, caută în tabelul său de rutare și găsește o rută legitimă către rețeaua 192.168.10.0/24 prin R1 și redirecționează pachetul înapoi către R1, creând bucla. Bucla a fost cauzată de dezinformarea injectată în R1.

Pentru mai multe informații despre amenințările generice la adresa protocoalelor de rutare, a se verifica RFC 4593. Reducerea atacurilor asupra protocoalelor de rutare se face configurând autentificarea OSPF.

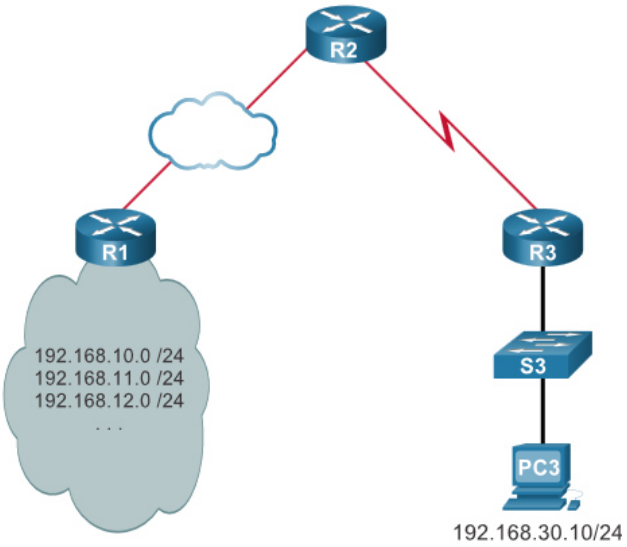


Fig. 6.2. Atacatorii pot manipula actualizările de rutare neautentificate.

6.3.3 - OSPF MD5 Routing Protocol Authentication

OSPF acceptă autentificarea protocolului de rutare folosind MD5. Autentificarea MD5 poate fi activată global pentru toate interfețele sau pe bază de interfață.

Activațre autentificare OSPF MD5 la nivel global:

ip ospf message-digest-key key md5 password interface configuration command.

area area-id autentificare mesaj-digest comanda de configurare a routerului.

Această metodă forțează autentificarea pe toate interfețele activate OSPF. Dacă o interfață nu este configurată cu comanda ip ospf message-digest-key, nu va putea forma adiacente cu alți vecini OSPF.

Activare autentificare MD5 pe bază de interfață:

ip ospf message-digest-key key md5 password interface configuration command.

Comanda de configurare a interfeței de autentificare ip ospf mesaj-digest.

Setarea interfeței înlocuiește setarea globală. Parolele de autentificare MD5 nu trebuie să fie aceleași în întreaga zonă. Cu toate acestea, trebuie să fie aceleași între vecini.

În această figură, R1 și R2 sunt configurate cu OSPF și rutarea funcționează corect. Cu toate acestea, mesajele OSPF nu sunt autentificate sau criptate.

Figura prezintă două routere conectate printr-o conexiune serială. Fiecare router este, de asemenea, conectat la o rețea gigabit Ethernet.

Fig. 6.3. OSPF configurat fără autentificare.

```
R1# show run | begin router ospf
router ospf 1
 passive-interface GigabitEthernet0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
<output omitted>
!--------------------------------
R2# show run | begin router ospf
router ospf 1
 passive-interface GigabitEthernet0/1
 network 10.1.1.0 0.0.0.3 area 0
 network 192.168.2.0 0.0.0.255 area 0
!
<output omitted>
```

În figura de mai jos, R1 și R2 sunt configurate cu autentificare OSPF MD5. Autentificarea este configurată pe bază de interfață, deoarece ambele routere folosesc o singură interfață pentru a forma adiacențele OSPF. Observați că atunci când R1 este configurat, adiacența OSPF se pierde cu R2 până când R2 este configurat cu autentificarea MD5 corespunzătoare.

Fig. 6.4. OSPF configurat cu autentificare MD5.

```
R1# conf t
R1(config)# interface s0/0/0
R1(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R1(config-if)# ip ospf authentication message-digest
R1(config-if)#
000209: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
000210: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on
Serial0/0/0 from LOADING to FULL, Loading Done
---------------------------
R2# conf t
000137: Feb 20 13:59:35.091 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1
on
Serial0/0/0 from FULL to DOWN, Neighbor Down: Dead timer expired
R2(config)# interface s0/0/0
R2(config-if)# ip ospf message-digest-key 1 md5 cisco12345
R2(config-if)# ip ospf authentication message-digest
R2(config-if)#
000138: Feb 20 14:01:09.975 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1
on
Serial0/0/0 from LOADING to FULL, Loading Done
R2(config-if)#
```

6.3.4 - OSPF SHA Routing Protocol Authentication

MD5 este acum considerat vulnerabil la atacuri și ar trebui utilizat numai atunci când nu este disponibilă o autentificare mai puternică. Cisco IOS versiunea 15.4(1)T a adăugat suport pentru autentificare OSPF SHA, așa cum este detaliat în RFC 5709. Prin urmare, administratorul ar trebui să folosească autentificarea SHA atâta timp cât toate sistemele de operare ale routerului acceptă autentificarea OSPF SHA.

Autentificarea OSPF SHA include doi pași majori. Sintaxa pentru comenzi este prezentată în figură:

Pasul 1. Specificarea unui lanț de chei de autentificare în modul de configurare globală:

Configurare nume de lanț de chei cu comanda lanț de chei.

Atribuirea lanțului de chei un număr și o parolă cu comenzile de cheie și șir de chei.

Specificare autentificare SHA cu comanda algoritmului criptografic.

(Opțional) Specificare când va expira această cheie cu comanda send-lifetime.

Sintaxa acestor comenzi este următoarea:

```
Router(config)#                key                chain                name
 Router(config-keychain)#                    key                    key-id
 Router(config-keychain-key)#                key-string             string
 Router(config-keychain-key)# cryptographic-algorithm {hmac-sha-1 | hmac-
sha-256      |      hmac-sha-384      |      hmac-sha-512      |      md5}
 Router(config-keychain-key)# send-lifetime start-time {infinite | end-time
| duration seconds}
```

Pasul 2. Folosim următoarea sintaxă pentru a atribui cheia de autentificare interfețelor dorite cu comanda ***ip ospf authentication key-chain***.

```
Router(config)#                interface                type                number
Router(config-if)# ip ospf authentication key-chain name
```

În exemplul care urmează, figura 6.5, R1 și R2 sunt configurate cu autentificare OSPF SHA folosind o cheie numită SHA256 și șirul de chei ospfSHA256. Se observa că atunci când R1 este configurat, adiacența OSPF se pierde cu R2 până când R2 este configurat cu autentificarea SHA potrivită.

Figura prezintă două routere conectate printr-o conexiune serială. Fiecare router este, de asemenea, conectat la o rețea gigabit Ethernet.

Fig. 6.5. OSPF configurat cu autentificare SHA.

```
R1(config)# key chain SHA256
R1(config-keychain)# key 1
R1(config-keychain-key)# key-string ospfSHA256
R1(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R1(config-keychain-key)# exit
R1(config-keychain)# exit
R1(config)# interface s0/0/0
R1(config-if)# ip ospf authentication key-chain SHA256
R1(config-if)#
000218: Feb 20 15:06:07.607 UTC: %OSPF-5-ADJCHG: Process 1, Nbr 10.1.1.2 on
Serial0/0/0
from FULL to DOWN, Neighbor Down: Dead timer expired
R1(config-if)#
-------------------------------------
R2(config)# key chain SHA256
R2(config-keychain)# key 1
R2(config-keychain-key)# key-string ospfSHA256
R2(config-keychain-key)# cryptographic-algorithm hmac-sha-256
R2(config-keychain-key)# exit
R2(config-keychain)# exit
R2(config)# interface s0/0/0
R2(config-if)# ip ospf authentication key-chain SHA256
R2(config-if)#
000142: Feb 20 15:07:22.631: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on
Serial0/0/0
from LOADING to FULL, Loading Done
R2(config-if)#
```

6.4 Secure Management and Reporting

6.4.1 - Types of Management Access

Într-o rețea mică, gestionarea și monitorizarea unui număr mic de dispozitive de rețea este o operațiune simplă. Cu toate acestea, într-o întreprindere mare cu sute de dispozitive, monitorizarea, gestionarea și procesarea mesajelor de jurnal poate fi o provocare. Din punct de vedere al raportării, majoritatea dispozitivelor de rețea pot trimite date de jurnal care pot fi de neprețuit atunci când depanează problemele de rețea sau amenințările de securitate. Aceste date pot fi vizualizate în timp real, la cerere și în rapoarte programate.

Când se face înregistrarea și gestionarea informațiilor, fluxul de informații dintre gazdele de gestionare și dispozitivele gestionate poate lua două căi:

În bandă - informațiile circulă printr-o rețea de producție a întreprinderii, pe internet sau ambele, folosind canale de date obișnuite.

Out-of-band (OOB) - Fluxuri de informații într-o rețea de management dedicată pe care nu există trafic de producție.

De exemplu, rețeaua din figură are două segmente de rețea separate de un router Cisco IOS care oferă servicii firewall pentru a proteja rețeaua de management. Conexiunea la rețeaua de producție permite gazdelor de management să acceseze internetul și oferă un trafic limitat de gestionare în bandă. Gestionarea în bandă are loc numai atunci când gestionarea OOB nu este posibilă sau disponibilă. Dacă este necesară gestionarea în bandă, atunci acel trafic ar trebui trimis în siguranță folosind un tunel criptat privat sau un tunel VPN.

Figura ilustrează managementul în bandă.

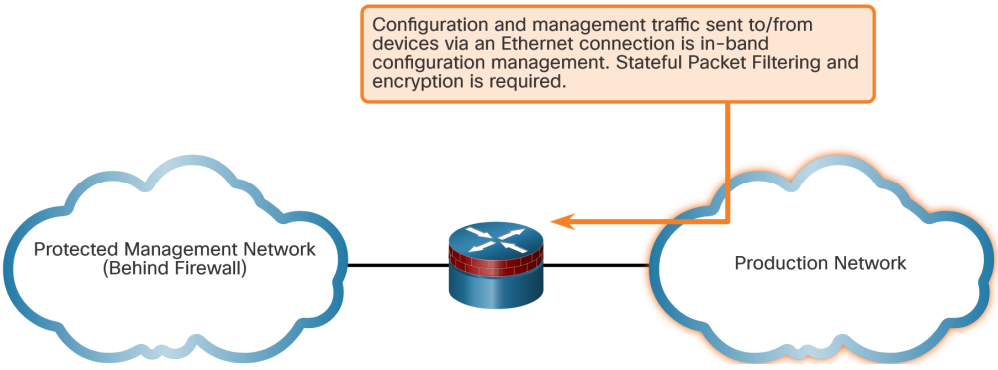


Fig. 6.6. Management în bandă.

Rețea de producție/Rețea de management protejată. (În spatele paravanului de protecție) Configurarea și gestionarea traficului trimis către/de la dispozitive printr-o conexiune Ethernet este gestionarea configurației în bandă. Este necesară filtrarea și criptarea pachetelor cu stare.

Figura de mai jos prezintă mai multe detalii pentru rețeaua de management protejată. Aici sunt plasate gazdele de management și serverele terminale. Când sunt plasate în rețeaua de administrare, serverele terminale oferă conexiuni directe OOB de consolă prin rețeaua de management la orice dispozitiv de rețea care necesită administrare în rețeaua de producție. Majoritatea dispozitivelor ar trebui să fie conectate la acest segment de gestionare și să fie configurate utilizând managementul OOB.

Deoarece rețeaua de management are acces administrativ la aproape fiecare zonă a rețelei, poate fi o țintă foarte atractivă pentru hackeri. Modulul de management de pe firewall încorporează mai multe tehnologii menite să atenueze astfel de riscuri. Amenințarea principală este un hacker care încearcă să obțină acces la rețeaua de management. Acest lucru poate fi realizat printr-o gazdă gestionată compromisă pe care trebuie să o acceseze un dispozitiv de management. Pentru a atenua amenințarea unui dispozitiv compromis, ar trebui implementat un control puternic al accesului la firewall și la orice alt dispozitiv. Dispozitivele de gestionare ar trebui să fie configurate într-un mod care să împiedice comunicarea directă cu alte gazde de pe aceeași subrețea de gestionare, utilizând segmente LAN sau VLAN-uri separate.

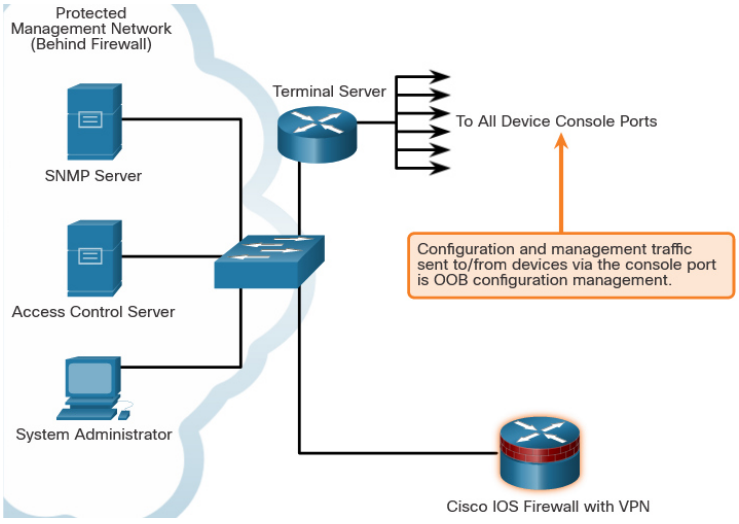


Fig. 6.7. Management OOB.

(În spatele paravanului de protecție)Server terminal Cisco IOS Firewall cu VPN la toate porturile consolei. Dispozitivele Configurarea și gestionarea traficului trimis către/de la dispozitive prin portul de consolă este gestionarea configurației OOB.

6.4.2 - Out-of-Band and In-Band Access

Ca regulă generală, din motive de securitate, managementul OOB este adecvat pentru rețelele mari ale întreprinderilor. Cu toate acestea, nu este întotdeauna de dorit. Decizia de a utiliza managementul OOB depinde de tipul de aplicații de management care rulează și de protocoalele monitorizate. De exemplu, luam în considerare o situație în care două switch-uri de bază sunt gestionate și monitorizate folosind o rețea OOB. Dacă o legătură critică între aceste două switch-uri de bază eșuează în rețeaua de producție, este posibil ca aplicația care monitorizează acele dispozitive să nu determine niciodată că legătura a eșuat și să nu alerteze niciodată administratorul. Acest lucru se datorează faptului că rețeaua OOB face ca toate dispozitivele să pară atașate la o singură rețea de management OOB. Rețeaua de management OOB rămâne neafectată de legătura întreruptă. Cu aplicații de management ca acestea, este de preferat să rulați aplicația de management în bandă într-un mod sigur.

Ghidurile de management OOB sunt:

- *Oferire de cel mai înalt nivel de securitate.*
- *Reducerea riscului de a trece protocoale de management nesigure prin rețeaua de producție.*

Administrarea în bandă este recomandată în rețelele mai mici ca mijloc de a realiza o implementare de securitate mai rentabilă. În astfel de arhitecturi, traficul de management circulă în bandă în toate cazurile. Se face cât mai sigur posibil folosind protocoale de management securizate, de exemplu folosind SSH în loc de Telnet. O altă opțiune este crearea de tuneluri securizate, folosind protocoale precum IPsec, pentru gestionarea traficului. Dacă accesul de management nu este necesar în orice moment, găurile temporare pot fi plasate într-un firewall în timp ce funcțiile de management sunt efectuate. Această tehnică trebuie utilizată cu prudență și toate găurile trebuie închise imediat când funcțiile de management sunt finalizate.

Orientările de gestionare în bandă sunt:

- *Aplicat numai dispozitivelor care trebuie gestionate sau monitorizate.*
- *Folosit IPsec, SSH sau SSL atunci când este posibil.*
- *Decidere dacă canalul de management trebuie să fie deschis în orice moment.*

În cele din urmă, dacă sunt utilizate instrumente de management de la distanță cu management în bandă, trebuie avut grijă de vulnerabilitățile de securitate subiacente ale

instrumentului de management în sine. De exemplu, managerii SNMP sunt adesea folosiți pentru a ușura sarcinile de depanare și configurare într-o rețea. Cu toate acestea, SNMP trebuie tratat cu cea mai mare atenție, deoarece protocolul de bază are propriul set de vulnerabilități de securitate.

6.5 Network Security Using Syslog

6.5.1 - Introduction to Syslog

La fel ca o lumină Check Engine de pe tabloul de bord al mașinii, componentele din rețea pot spune dacă este ceva în neregulă. Protocolul syslog a fost conceput pentru a asigura faptul că se pot primi și înțelege aceste mesaje. Atunci când anumite evenimente au loc într-o rețea, dispozitivele de rețea au mecanisme de încredere pentru a notifica administratorul cu mesaje detaliate de sistem. Aceste mesaje pot fi fie necritice, fie semnificative. Administratorii de rețea au o varietate de opțiuni pentru stocarea, interpretarea și afișarea acestor mesaje. Ei pot fi, de asemenea, alertați cu privire la acele mesaje care ar putea avea cel mai mare impact asupra infrastructurii rețelei.

Cea mai comună metodă de accesare a mesajelor de sistem este utilizarea unui protocol numit syslog.

Syslog este un termen folosit pentru a descrie un standard. De asemenea, este folosit pentru a descrie protocolul dezvoltat pentru acel standard. Protocolul syslog a fost dezvoltat pentru sistemele UNIX în anii 1980, dar a fost documentat pentru prima dată ca RFC 3164 de către IETF în 2001.

Multe dispozitive de rețea acceptă syslog, inclusiv routere, comutatoare, servere de aplicații, firewall-uri și alte dispozitive de rețea. Protocolul syslog permite dispozitivelor de rețea să-și trimită mesajele de sistem prin rețea către serverele syslog.

Mai exact, syslog folosește portul UDP 514 pentru a trimite mesaje de notificare de evenimente prin rețelele IP către colectorii de mesaje de evenimente. De exemplu, figura afișează un router (R1) și un comutator (S1) care trimit mesaje de sistem către un server syslog.

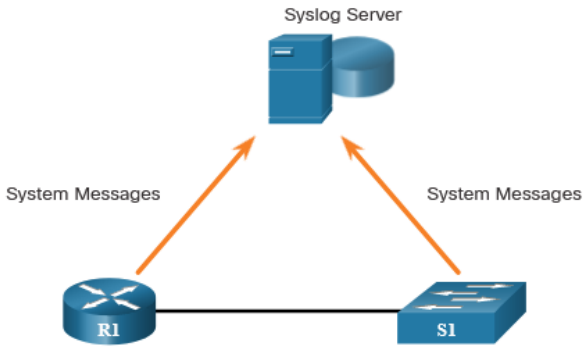


Fig. 6.8. Monitorizare cu SysLog.

Există mai multe pachete software de server syslog pentru Windows și UNIX disponibile. Multe dintre ele sunt freeware.

Serviciul de logare syslog oferă trei funcții principale, după cum urmează:

1. *Capacitatea de a aduna informații de înregistrare pentru monitorizare și depanare.*
2. *Capacitatea de a selecta tipul de informații de înregistrare care sunt capturate.*
3. *Capacitatea de a specifica destinațiile mesajelor syslog capturate.*

6.5.2 - Syslog Operation

Pe dispozitivele de rețea Cisco, protocolul syslog începe prin a trimite mesaje de sistem și informatii de depanare la un proces local de înregistrare în jurnal care este intern dispozitivului. Modul în care procesul de înregistrare gestionează aceste mesaje și ieșiri se bazează pe configurațiile dispozitivului. De exemplu, mesajele syslog pot fi trimise prin rețea către un server syslog extern. Mesajele de pe serverul syslog pot fi apoi filtrate fără a fi nevoie să accesați dispozitivul real. Mesajele de jurnal și ieșirile stocate pe serverul extern pot fi extrase în diferite rapoarte pentru o citire mai ușoară.

Alternativ, mesajele syslog pot fi trimise într-un buffer intern. Mesajele trimise în bufferul intern sunt vizibile numai prin CLI-ul dispozitivului.

În cele din urmă, administratorul de rețea poate specifica ca numai anumite tipuri de mesaje de sistem să fie trimise către diferite destinații. De exemplu, dispozitivul poate fi configurat să redirecționeze toate mesajele de sistem către un server Syslog extern. Cu toate acestea, mesajele la nivel de depanare sunt redirecționate către bufferul intern și sunt accesibile numai de către administrator din CLI.

După cum se arată în figură, destinațiile populare pentru mesajele syslog includ:

- *Buffer de înregistrare (RAM în interiorul unui router sau comutator)*
- *Linia de consolă*

- *Linie terminală*
- *Server Syslog*

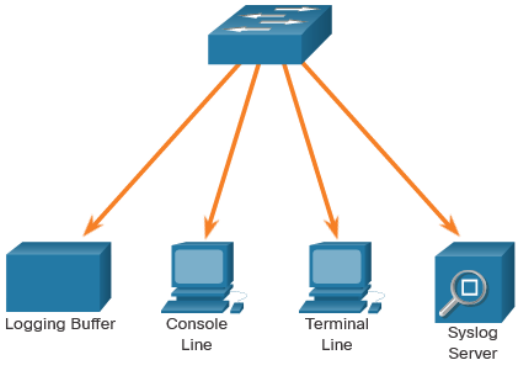


Fig. 6.9. Stocare mesajelor de tip syslog.

Este posibil să fie monitorizate de la distanță mesajele de sistem prin vizualizarea jurnalelor pe un server syslog sau prin accesarea dispozitivului prin Telnet, SSH sau prin portul de consolă.

6.5.3 - Syslog Message Format

Dispozitivele Cisco produc mesaje syslog ca rezultat al evenimentelor din rețea. Fiecare mesaj syslog conține un nivel de severitate și o facilitate.

Cu cât nivelurile numerice sunt mai mici cu atat sunt alarmele syslog mai critice. Nivelul de severitate al mesajelor poate fi setat pentru a controla unde este afișat fiecare tip de mesaj (adică pe consolă sau pe celelalte destinații). Lista completă a nivelurilor syslog este prezentată în tabel.

Severity Name	**Severity Number**	**Description**
Emergency	Level 0	System Unusable
Alert	Level 1	Immediate Action Needed
Critical	Level 2	Critical Condition
Error	Level 3	Error Condition
Warning	Level 4	Warning Condition
Notification	Level 5	Normal, but Significant Condition
Informational	Level 6	Informational Message
Debugging	Level 7	Debugging Message

Fiecare nivel de syslog are propriul său sens:

Nivelul de urgență 0 - ***Nivelul de avertizare 4***: Aceste mesaje sunt mesaje de eroare despre defecțiuni software sau hardware; aceste tipuri de mesaje înseamnă că funcționalitatea dispozitivului este afectată. Severitatea problemei determină nivelul real de syslog aplicat.

Nivelul de notificare 5: Acest nivel de notificări este pentru evenimente normale, dar semnificative. De exemplu, tranzițiile în sus sau în jos ale interfeței și mesajele de repornire a sistemului sunt afișate la nivelul notificărilor.

Nivelul informativ 6: Acesta este un mesaj informativ normal care nu afectează funcționalitatea dispozitivului. De exemplu, atunci când un dispozitiv Cisco pornește, este posibil să vedeți următorul mesaj informativ: %LICENSE-6-EULA_ACCEPT_ALL: Dreptul de utilizare a acordului de licență pentru utilizatorul final este acceptat.

Nivelul de depanare 7: Acest nivel indică faptul că mesajele sunt generate din emiterea diferitelor comenzi de depanare.

6.5.4 - Syslog Facilities

Pe lângă specificarea severității, mesajele syslog conțin și informații despre facilitate. Facilități Syslog sunt identificatori de serviciu care identifică și clasifică datele despre starea sistemului pentru raportarea mesajelor de eroare și evenimente. Opțiunile de înregistrare disponibile sunt specifice dispozitivului de rețea. De exemplu, switch-urile din seria Cisco 2960 care rulează Cisco IOS Release 15.0(2) și routerele Cisco 1941 care rulează Cisco IOS Release 15.2(4) acceptă 24 de opțiuni de facilitate care sunt clasificate în 12 tipuri de unități.

Unele coduri comune pentru mesajele Syslog raportate pe routerele Cisco IOS includ:

- ***IF*** - *Identifică faptul că mesajul syslog a fost generat de o interfață.*
- ***IP*** - *Identifică faptul că mesajul syslog a fost generat de IP.*
- ***OSPF*** - *Identifică faptul că mesajul syslog a fost generat de protocolul de rutare OSPF.*
- ***SYS*** - *Identifică faptul că mesajul syslog a fost generat de sistemul de operare al dispozitivului.*
- ***IPSEC*** - *Identifică faptul că mesajul syslog a fost generat de protocolul de criptare IP Security.*

În mod implicit, formatul mesajelor syslog din software-ul Cisco IOS este următorul:

```
%facility-severity-MNEMONIC: description
```

De exemplu, eșantionul de ieșire pe un comutator Cisco pentru o stare de schimbare a conexiunii EtherChannel în sus este:

```
%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
```

Aici facilitatea este LINK și nivelul de severitate este 3, cu un MNEMONIC de UPDOWN.

Cele mai frecvente mesaje sunt mesajele link up și down și mesajele pe care un dispozitiv le produce atunci când iese din modul de configurare. Dacă înregistrarea ACL este configurată, dispozitivul generează mesaje syslog atunci când pachetele corespund unei condiții de parametru.

6.5.5 - Configure Syslog Timestamps

În mod implicit, mesajele de jurnal nu sunt marcate de timp. În exemplu, interfața R1 GigabitEthernet 0/0/0 este oprită. Mesajul înregistrat în consolă nu identifică când a fost schimbată starea interfeței. Mesajele de jurnal ar trebui să fie marcate de timp, astfel încât atunci când sunt trimise către o altă destinație, cum ar fi un server Syslog, să existe o înregistrare a momentului în care mesajul a fost generat.

Se utilizaeaza comanda ***service timestamps log datetime*** pentru a forța evenimentele înregistrate să afișeze data și ora. După cum se arată în rezultatul comenzii, atunci când interfața R1 GigabitEthernet 0/0/0 este reactivată, mesajele de jurnal conțin acum data și ora.

```
R1# configure terminal
R1(config)# interface g0/0/0
R1(config-if)# shutdown
%LINK-5-CHANGED: Interface GigabitEthernet0/0/0, changed state to
administratively down
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0/0,
changed state to down
R1(config-if)# exit
R1(config)# service timestamps log datetime
R1(config)# interface g0/0/0
R1(config-if)# no shutdown
*Mar 1 11:52:42: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed
state to down
*Mar 1 11:52:45: %LINK-3-UPDOWN: Interface GigabitEthernet0/0/0, changed
state to up
*Mar 1 11:52:46: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0/0,
changed state to up
R1(config-if)#
```

Notă: Când folosim cuvântul cheie datetime, ceasul de pe dispozitivul de rețea trebuie setat, fie manual, fie prin NTP.

1. **Refer to the syslog output.** What security level generated the message?

- ◯ Error
- ◯ Informational
- ◯ Warning
- ◯ Debugging

2. **Refer to the syslog output.** What is the mnemonic for this syslog message?

- ◯ `IFMGR`
- ◯ `Unable to open nvram`
- ◯ `NO_IFINDEX_FILE`
- ◯ `ifIndex-table`

3. **Refer to the syslog output.** What is the syslog reporting facility?

- ◯ `IFMGR`
- ◯ `NO_IFINDEX_FILE`
- ◯ `IFMGR-7`
- ◯ `ifIndex-table`

6.5.7 - Syslog Systems

Implementările Syslog conțin întotdeauna două tipuri de sisteme:

- ***Servere Syslog*** *- Cunoscute și ca gazde de jurnal, aceste sisteme acceptă și procesează mesajele de jurnal de la clienții syslog.*
- ***Clienți Syslog*** *- Routere sau alte tipuri de echipamente care generează și transmit mesaje de jurnal către serverele Syslog.*

Topologia din figură identifică serverul syslog la adresa IP 10.2.2.6. Restul serverelor și dispozitivelor din topologie pot fi configurate drept clienți syslog, care trimit mesaje syslog către serverul syslog.

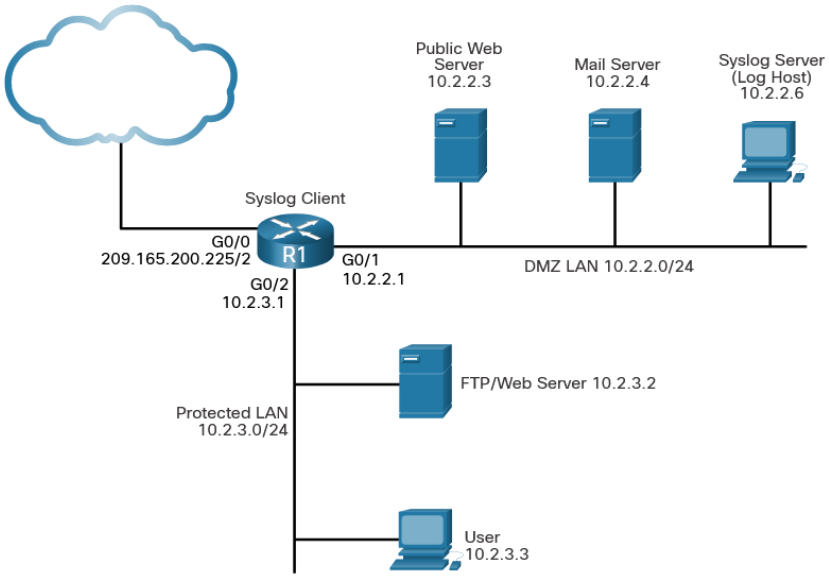


Fig. 6.10. Topologie de referință Syslog.

6.5.8 - Syslog Configuration

Pasul 1. Identificarea serverului syslog de destinație folosind comanda logging host.

Parameter	Description
hostname	Specifică numele gazdei pe care dorim să o folosim ca server syslog.
ip-address	Specifică adresa IP a gazdei pe care dorim să o folosim ca server syslog.

```
Router(config)# logging host [hostname | ip-address]
```

Pasul 2. (Opțional) Setarea nivelului de severitate a jurnalului (capcană) utilizând comanda logging trap.

Notă: Un ISR este implicit la Nivelul 7 (depanare).

```
Router(config)# logging trap level
```

Pasul 3. (Opțional) Setarea interfeței sursă utilizând comanda logging source-interface. Această comandă specifică că pachetele syslog conțin adresa IPv4 sau IPv6 a unei anumite interfețe (de exemplu, o interfață loopback), indiferent de interfața pe care o folosește pachetul pentru a ieși din router.

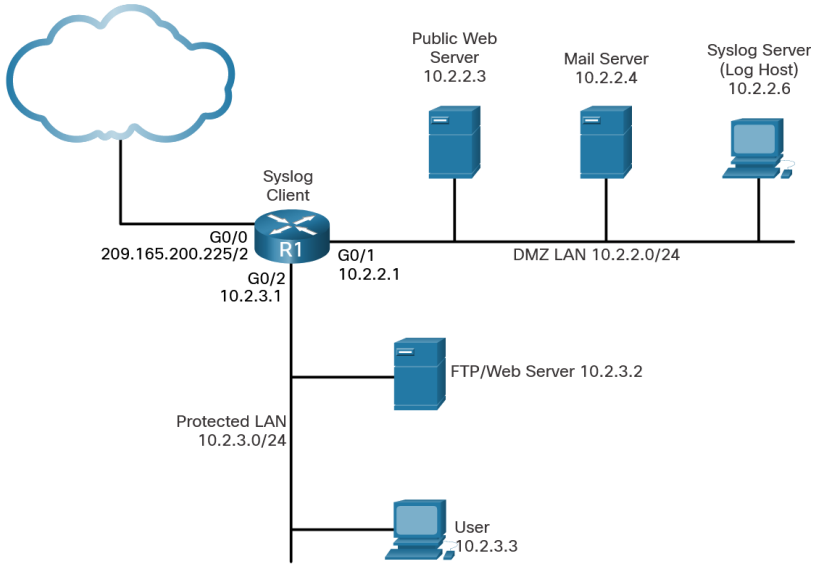
Parameter	Description
interface-type	Specifică tipul de interfață.
interface-number	Specifică numărul interfeței (de exemplu, 0/1).

```
Router(config)# logging source-interface interface-type interface-number
```

Pasul 4. (Opțional) Activarea înregistrării la toate destinațiile activate cu comanda de conectare.

Notă: Înregistrarea Syslog este activată în mod implicit.

```
Router(config)# logging on
```



6.11. Figura prezintă topologia de referință syslog.

```
R1(config)# logging 10.2.2.6
R1(config)#
*Sep  25  12:57:14.120:  %SYS-6-LOGGINGHOST_STARTSTOP:  Logging  to  host
10.2.2.6 port 514 started - CLI initiated
R1(config)#
R1(config)# logging trap informational
R1(config)# logging source-interface lo0
R1(config)# logging on
R1(config)# exit
R1#
*Sep 25 12:58:29.591: %SYS-5-CONFIG_I: Configured from console by console
R1#
R1# show logging
Syslog  logging:  enabled  (0  messages  dropped,  2  messages  rate-limited,  0
flushes, 0 overruns, xml disabled, filtering disabled)

<Output omitted>

    Trap logging: level informational, 83 message lines logged
        Logging to 10.2.2.6  (udp port 514, audit disabled,
              link up),
              7 message lines logged,
              0 message lines rate-limited,
              0 message lines dropped-by-MD,
              xml disabled, sequence number disabled
              filtering disabled
        Logging Source-Interface:       VRF Name:
        Loopback0

<Output omitted>
```

6.6 NTP Configuration

6.6.1 - Time and Calendar Services

Înainte de a intra cu adevărat în gestionarea rețelei, singurul lucru care va ajuta să menținem pe drumul cel bun este să asiguram faptul că toate componentele sunt setate la aceeași oră și dată.

Ceasul software de pe un router sau comutator pornește când sistemul pornește. Este sursa primară de timp pentru sistem. Este important să fie sincronizara ora pe toate dispozitivele din rețea, deoarece toate aspectele legate de gestionarea, securizarea, depanarea și planificarea rețelelor necesită o marcare temporală precisă. Când ora nu este sincronizată între dispozitive, va fi imposibil să se determine ordinea evenimentelor și cauza unui eveniment.

Setările de dată și oră de pe un router sau comutator pot fi configurate manual, așa cum se arată în exemplu.

```
R1# clock set 16:01:00 sept 25 2022
*Sep 25 16:01:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated
from 13:09:49 UTC Fri Sep 25 2022 to 16:01:00 UTC Fri Sep 25 2022,
configured from console by console.
Sep 25 16:01:00.001: %PKI-6-AUTHORITATIVE_CLOCK: The system clock has been
set.
R1#
```

Deși setarea manuală a orei este ușoară, nu este practică în majoritatea rețelelor. Pe măsură ce o rețea crește, devine dificil, dacă nu imposibil, să se asigure faptul că toate dispozitivele de infrastructură funcționează cu timp sincronizat. Chiar și într-un mediu de rețea mai mic, metoda manuală nu este ideală.

“Dacă un router repornește, cum va obține o dată și un marcaj de timp exact ?”

O soluție mai bună și mai scalabilă este implementarea Network Time Protocol (NTP), care este documentată în RFC 1305. NTP permite dispozitivelor de rețea (adică clienții NTP) să-și sincronizeze setările de timp cu o sursă de timp autorizată NTP, cum ar fi un server NTP. Sursa de timp NTP poate fi un dispozitiv (de exemplu, un router) din rețea care este selectat ca ceas principal privat sau poate fi un server NTP disponibil public pe internet.

Sursa NTP și clienții deschid portul UDP 123 pentru a trimite și a primi marcaje temporale.

6.6.2 - NTP Operation

Rețelele NTP utilizează un sistem ierarhic de surse de timp. Fiecare nivel din acest sistem ierarhic este numit strat. Nivelul stratului este definit ca numărul de numărări de hamei din sursa autorizată.

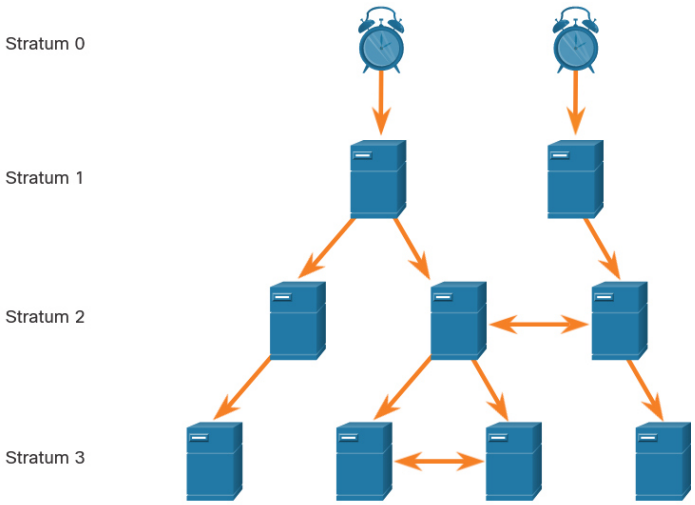


Fig 6.12. Figura afișează un exemplu de rețea NTP.

Rețeaua de eșantionare este formată din patru niveluri de strat care își dobândesc timpii după cum urmează:

Serverul stratului 1 își obține timpul de la sursa de timp stratului 0.

Serverul stratului 2 își primește timpul de la serverul stratului 1.

Serverul Stratum 3 își primește timpul de la serverul Stratum 2.

Stratul 0 - Aceasta identifică un dispozitiv care oferă cea mai autorizată sursă de timp. Dispozitivele Stratum 0, inclusiv ceasurile atomice și GPS, sunt cele mai precise surse de timp autorizate.

Mai exact, dispozitivele NTP din nivelul 0 sunt dispozitive de cronometrare de înaltă precizie care nu fac parte din rețea, presupuse a fi precise și cu o întârziere mică sau deloc asociată acestora. În figură, acestea sunt reprezentate de pictograma ceasului.

Stratul 1 - Dispozitivele NTP din nivelul 1 sunt dispozitive de rețea care sunt conectate direct la sursele de timp autorizate. Acestea funcționează ca standard de timp de rețea primar pentru dispozitivele din nivelul 2.

Stratul 2 și Inferior - Serverele NTP nivelul 2 sunt conectate într-o rețea la un dispozitiv nivelul 1. Dispozitivele Stratum 2 sunt clienți NTP și își sincronizează timpul utilizând

pachetele NTP de la un server Stratum 1, cum ar fi un router. La rândul lor, pot fi servere NTP pentru dispozitivele din nivelul 3.

Nivelurile stratului NTP se bazează pe o scară de la 0 (nivelul cel mai înalt al stratului) la 15 (nivelul cel mai scăzut al stratului). De exemplu, un server NTP la un nivel de strat cu număr redus este mai aproape de sursa de timp autorizată decât un server la un nivel de strat cu număr mare.

Numărul maxim de hop de strat este 15 (adică 0 – 15). Reținem că unui client NTP care nu este sincronizat cu un server i se atribuie un nivel de strat 16.

Serverele NTP din același nivel de strat pot fi configurate ca peer pentru a oferi surse de timp redundante pentru clienți sau pentru a se sincroniza reciproc.

6.6.3 - Configure and Verify NTP

Figura arată topologia utilizată pentru a demonstra configurarea și verificarea NTP.

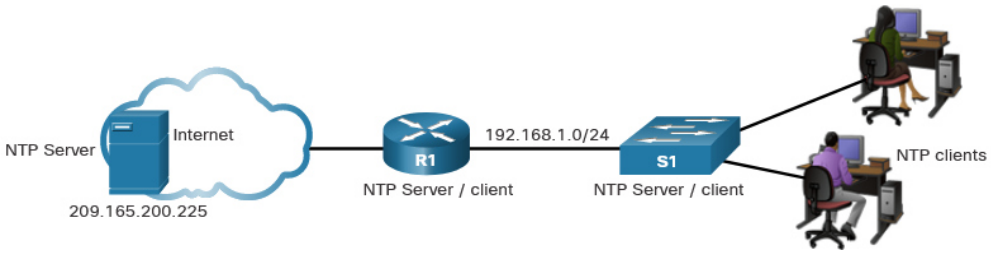


Fig. 6.13. Topologie NTP.

Înainte ca NTP să se configureze în rețea, comanda show clock afișează ora curentă pe ceasul software, așa cum se arată în exemplu. Cu opțiunea de detaliu, observăm că sursa de timp este configurația utilizatorului. Asta înseamnă că ora a fost configurată manual cu comanda ceasului.

```
R1# show clock detail
20:55:10.207 UTC Fri Nov 15 2019
Time source is user configuration
```

În topologia data, serverul de internet NTP este sursa de timp autorizată. Cu toate acestea, un dispozitiv de rețea locală ar putea fi selectat ca sursă de timp autorizată NTP folosind comanda de configurare globală ntp master [stratum].

În topologie, R1 este un client NTP al serverului NTP. Se utilieaza comanda ntp server ip-address global config pentru a configura 209.165.200.225 ca server NTP pentru R1.

Pentru a verifica că sursa de timp este setată la NTP, se utilizeaza comanda show clock detail. Observam că acum sursa de timp este NTP.

```
R1(config)# ntp server 209.165.200.225
```

```
R1(config)# end
R1# show clock detail
21:01:34.563 UTC Fri Nov 15 2019
Time source is NTP
```

În exemplul următor, comenzile show ntp associations și show ntp status sunt folosite pentru a verifica dacă R1 este sincronizat cu serverul NTP la 209.165.200.225. Observați că R1 este sincronizat cu un server NTP nivelul 1 la 209.165.200.225, care este sincronizat cu un ceas GPS. Comanda show ntp status afișează că R1 este acum un dispozitiv din nivelul 2 care este sincronizat cu serverul NTP la 209.165.220.225. Notă: St evidențiat reprezintă strat.

```
R1# show ntp associations
  address           ref clock        st    when    poll reach   delay   offset
disp
*~209.165.200.225 .GPS.             1      61      64    377   0.481    7.480
4.261
 *  sys.peer,  #  selected,  +  candidate,  -  outlyer,  x  falseticker,  ~
configured

R1# show ntp status
Clock is synchronized, stratum 2, reference is 209.165.200.225
nominal freq is 250.0000 Hz, actual freq is 249.9995 Hz, precision is 2**19
ntp uptime is 589900 (1/100 of seconds), resolution is 4016
reference time is DA088DD3.C4E659D3 (13:21:23.769 PST Fri Nov 15 2019)
clock offset is 7.0883 msec, root delay is 99.77 msec
root dispersion is 13.43 msec, peer dispersion is 2.48 msec
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000001803
s/s
system poll interval is 64, last update was 169 sec ago.
```

Apoi, ceasul de pe S1 este configurat să se sincronizeze cu R1 cu comanda server ntp și apoi configurația este verificată cu comanda show ntp associations, așa cum este afișat.

```
S1(config)# ntp server 192.168.1.1
S1(config)# end
S1# show ntp associations
  address           ref clock        st    when    poll reach   delay   offset
disp
*~192.168.1.1      209.165.200.225   2      12      64    377   1.066   13.616
3.840
 *  sys.peer,  #  selected,  +  candidate,  -  outlyer,  x  falseticker,  ~
configured
```

Ieșirea din comanda show ntp associations verifică dacă ceasul de pe S1 este acum sincronizat cu R1 la 192.168.1.1 prin NTP. R1 este un dispozitiv din nivelul 2 și un server NTP la S1. Acum S1 este un dispozitiv din nivelul 3 care poate oferi serviciu NTP altor dispozitive din rețea, cum ar fi dispozitivele finale.

```
S1# show ntp status
Clock is synchronized, stratum 3, reference is 192.168.1.1
nominal freq is 119.2092 Hz, actual freq is 119.2088 Hz, precision is 2**17
reference time is DA08904B.3269C655 (13:31:55.196 PST Tue Nov 15 2019)
clock offset is 18.7764 msec, root delay is 102.42 msec
root dispersion is 38.03 msec, peer dispersion is 3.74 msec
```

```
loopfilter state is 'CTRL' (Normal Controlled Loop), drift is 0.000003925
s/s
system poll interval is 128, last update was 178 sec ago.
```

6.7 SNMP Configuration

6.7.1 - Introduction to SNMP

SNMP a fost dezvoltat pentru a permite administratorilor să gestioneze noduri precum servere, stații de lucru, routere, comutatoare și dispozitive de securitate, într-o rețea IP. Acesta permite administratorilor de rețea să monitorizeze și să gestioneze performanța rețelei, să găsească și să rezolve problemele de rețea și să planifice creșterea rețelei.

SNMP definește modul în care informațiile de management sunt schimbate între aplicațiile de gestionare a rețelei și agenții de management. Este un protocol de nivel de aplicație care oferă un format de mesaj pentru comunicarea între manageri și agenți. Sistemul SNMP este format din trei elemente:

- ***Manager SNMP***
- ***Agenți SNMP (nod gestionat)***
- ***Baza de informații de management (MIB)***

Pentru a configura SNMP pe un dispozitiv de rețea, este mai întâi necesar să se defineasca relația dintre manager și agent.

Managerul SNMP face parte dintr-un sistem de management al rețelei (NMS). Managerul SNMP rulează software-ul de management SNMP.

După cum se arată în figură, managerul SNMP poate colecta informații de la un agent SNMP utilizând acțiunea „obține”. Poate modifica configurațiile unui agent utilizând acțiunea „set”. În plus, agenții SNMP pot transmite informații direct către un manager de rețea folosind „capcane”.

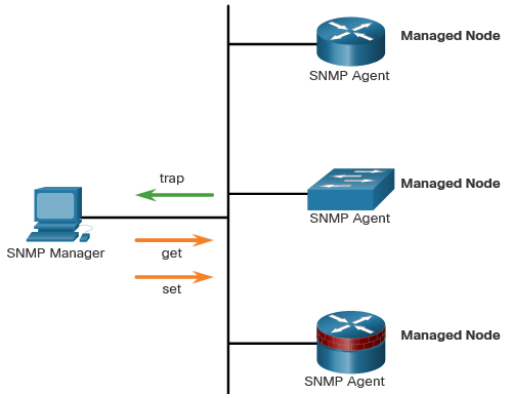


Fig. 6.14. Structura unei topologii cu implementare SNMP.

Agentul SNMP și MIB rezidă pe dispozitivele client SNMP. Dispozitivele de rețea care trebuie gestionate, cum ar fi comutatoarele, routerele, serverele, firewall-urile și stațiile de lucru, sunt echipate cu un modul software agent SNMP. MIB stochează date și statistici operaționale despre dispozitiv.

Managerul SNMP trimite o solicitare de obținere către agentul SNMP pentru a accesa datele stocate în MIB-ul local. Mai exact, managerul SNMP interogează agenții și interogează MIB-ul pentru agenți SNMP pe portul UDP 161. Agenții SNMP trimit orice capcane SNMP managerului SNMP pe portul UDP 162.

6.7.2 - SNMP Operation

Agenții SNMP care se află pe dispozitivele gestionate colectează și stochează informații despre dispozitiv și funcționarea acestuia. Aceste informații sunt stocate de agent local în MIB. Managerul SNMP utilizează apoi agentul SNMP pentru a accesa informațiile din MIB.

Există două solicitări principale de manager SNMP:

1. ***obțineți cerere*** *- Folosit de NMS pentru a solicita date dispozitivului.*
2. ***set request*** *- Folosit de NMS pentru a modifica variabilele de configurare în dispozitivul agent. O solicitare setată poate iniția, de asemenea, acțiuni în cadrul unui dispozitiv. De exemplu, o solicitare de setare poate determina repornirea unui router, trimiterea unui fișier de configurare sau primirea unui fișier de configurare.*

Managerul SNMP utilizează acțiunile get și set pentru a efectua operațiunile descrise în tabel.

Operation	Description
`get-request`	Preia o valoare dintr-o anumită variabilă.
`get-next-request`	Preia o valoare dintr-o variabilă dintr-un tabel; managerul SNMP nu trebuie să cunoască numele exact al variabilei. Se efectuează o căutare secvenţială pentru a găsi variabila necesară dintr-un tabel.
`get-bulk-request`	Preia blocuri mari de date, cum ar fi mai multe rânduri dintr-un tabel, care altfel ar necesita transmiterea multor blocuri mici de date. (Funcționează numai cu SNMPv2 sau o versiune ulterioară.)
`get-response`	Răspunsuri la o solicitare get, get-next-request și set-request trimise de un NMS.
`set-request`	Stochează o valoare într-o anumită variabilă.

Agentul SNMP răspunde solicitărilor managerului SNMP după cum urmează:

- ***Obține o variabilă MIB*** *- Agentul SNMP îndeplinește această funcție ca răspuns la un GetRequest-PDU de la managerul de rețea. Agentul preia valoarea variabilei MIB solicitate și răspunde managerului de rețea cu acea valoare.*
- ***Setaeaza o variabilă MIB*** *- Agentul SNMP îndeplinește această funcție ca răspuns la o SetRequest-PDU de la managerul de rețea. Agentul SNMP modifică valoarea variabilei MIB la valoarea specificată de managerul de rețea. Un răspuns de agent SNMP la o solicitare setată include noile setări în dispozitiv.*

Figura ilustrează utilizarea unui SNMP GetRequest pentru a determina dacă interfața G0/0/0 este up/up.

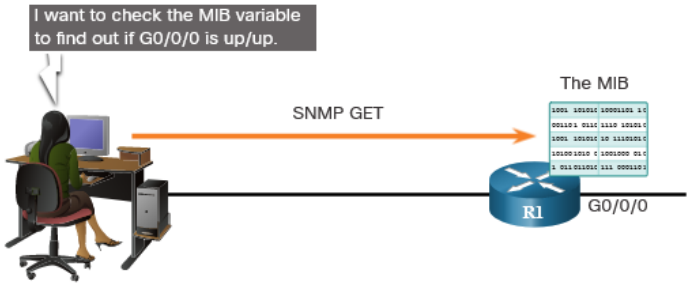


Fig. 6.15. SNMP Get.

6.7.3 - Management Information Base (MIB)

MIB organizează variabilele ierarhic. Variabilele MIB permit software-ului de management să monitorizeze și să controleze dispozitivul de rețea. În mod formal, MIB-ul definește fiecare variabilă ca un ID de obiect (OID). OID-urile identifică în mod unic obiectele gestionate în ierarhia MIB. MIB organizează OID-urile pe baza standardelor RFC într-o ierarhie de OID-uri, de obicei prezentată ca un arbore.

Arborele MIB pentru orice dispozitiv dat include unele ramuri cu variabile comune multor dispozitive de rețea și unele ramuri cu variabile specifice dispozitivului sau furnizorului respectiv.

RFC-urile definesc unele variabile publice comune. Majoritatea dispozitivelor implementează aceste variabile MIB. În plus, furnizorii de echipamente de rețea, cum ar fi Cisco, își pot defini propriile ramuri private ale arborelui pentru a găzdui noile variabile specifice dispozitivelor lor.

Figura prezintă porțiuni din structura MIB definită de Cisco. Observați modul în care OID-ul poate fi descris în cuvinte sau numere pentru a ajuta la localizarea unei anumite variabile în

arbore. OID-urile aparținând Cisco, sunt numerotate astfel: .iso (1).org (3).dod (6).internet (1).private (4).întreprinderi (1).cisco (9). Prin urmare, OID este 1.3.6.1.4.1.9.

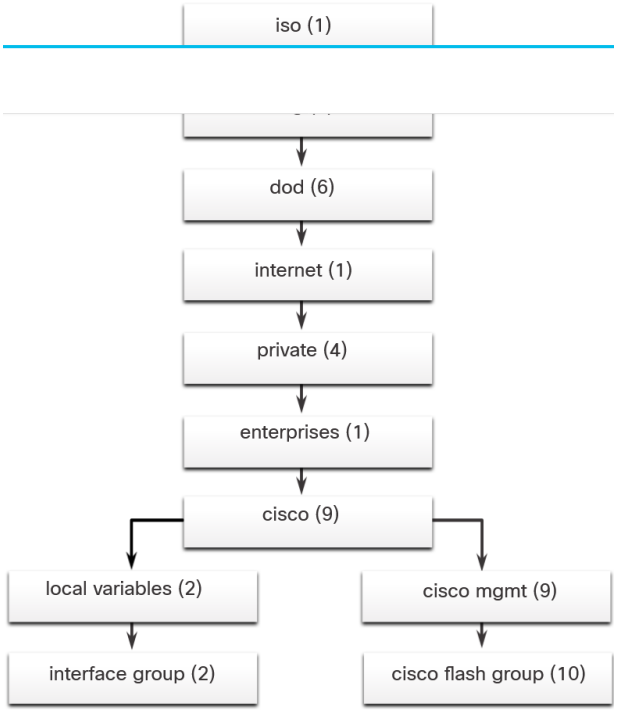


Fig. 6.16. Portiuni din MIB.

6.7.4 - SNMP Versions

Există mai multe versiuni de SNMP:

1. ***SNMPv1*** - Acesta este protocolul simplu de gestionare a rețelei, un standard complet de internet, care este definit în RFC 1157.
2. ***SNMPv2c*** - Acesta este definit în RFC-urile 1901 până la 1908. Utilizează un cadru administrativ bazat pe șiruri comunitare.
3. ***SNMPv3*** - Acesta este un protocol interoperabil bazat pe standarde definit inițial în RFC-urile 2273 până la 2275. Acesta oferă acces securizat la dispozitive prin autentificarea și criptarea pachetelor prin rețea. Include aceste caracteristici de securitate: integritatea mesajului pentru a se asigura că un pachet nu a fost manipulat în tranzit, autentificare pentru a determina dacă mesajul provine dintr-o sursă validă și criptare pentru a preveni citirea conținutului unui mesaj de către o sursă neautorizată.

Toate versiunile folosesc manageri SNMP, agenți și MIB-uri. Software-ul Cisco IOS acceptă cele trei versiuni de mai sus. Versiunea 1 este o soluție moștenită și nu este des întâlnită astăzi în rețele.

Atât SNMPv1, cât și SNMPv2c folosesc o formă de securitate bazată pe comunitate. Comunitatea de manageri care poate accesa MIB-ul agentului este definită de un șir de comunitate.

Spre deosebire de SNMPv1, SNMPv2c include un mecanism de recuperare în bloc și raportare mai detaliată a mesajelor de eroare către stațiile de management. Mecanismul de recuperare în vrac recuperează tabele și cantități mari de informații, reducând la minimum numărul de călătorii dus-întors necesare. Gestionarea îmbunătățită a erorilor SNMPv2c include coduri de eroare extinse care disting diferitele tipuri de condiții de eroare. Aceste condiții sunt raportate printr-un singur cod de eroare în SNMPv1. Codurile de returnare de eroare din SNMPv2c includ tipul de eroare.

Notă: SNMPv1 și SNMPv2c oferă caracteristici de securitate minime. Mai exact, SNMPv1 și SNMPv2c nu pot nici autentifica sursa unui mesaj de management și nici nu pot furniza criptare. SNMPv3 este descris cel mai în prezent în RFC-urile 3410 până la 3415. Acesta adaugă metode pentru a asigura transmiterea securizată a datelor critice între dispozitivele gestionate.

SNMPv3 oferă atât modele de securitate, cât și niveluri de securitate. Un model de securitate este o strategie de autentificare configurată pentru un utilizator și pentru grupul în care locuiește utilizatorul. Un nivel de securitate este nivelul permis de securitate într-un model de securitate. O combinație a nivelului de securitate și a modelului de securitate determină ce mecanism de securitate este utilizat la manipularea unui pachet SNMP.

Există modele de securitate disponibile pentru SNMPv1, SNMPv2c și SNMPv3. Tabelul identifică caracteristicile diferitelor combinații de modele și niveluri de securitate.

SNMPv1	
Level	noAuthNoPriv
Authentication	Community string
Encryption	No
Result	Uses a community string match for authentication.
SNMPv2c	
Level	noAuthNoPriv
Authentication	Community string
Encryption	No
Result	Uses a community string match for authentication.

SNMPv3 noAuthNoPriv	
Level	noAuthNoPriv
Authentication	Username
Encryption	No
Result	Uses a username match for authentication (an improvement over SNMPv2c).
SNMPv3 authNoPriv	
Level	authNoPriv
Authentication	Message Digest 5 (MD5) or Secure Hash Algorithm (SHA)
Encryption	No
Result	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms.
SNMPv3 authPriv	
Level	authPriv (requires the cryptographic software image)
Authentication	MD5 or SHA
Encryption	Data Encryption Standard (DES) or Advanced Encryption Standard (AES)
Result	Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Allows specifying the User-based Security Model (USM) with these encryption algorithms: • DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard • 3DES 168-bit encryption • AES 128-bit, 192-bit, or 256-bit encryption

Un administrator de rețea trebuie să configureze agentul SNMP pentru a utiliza versiunea SNMP acceptată de stația de management. Deoarece un agent poate comunica cu mai mulți manageri SNMP, este posibil să se configureze software-ul să accepte comunicații utilizând SNMPv1, SNMPv2c sau SNMPv3.

6.7.5 - SNMP Vulnerabilities

În orice topologie de rețea, cel puțin un nod manager ar trebui să ruleze software-ul de gestionare SNMP. Dispozitivele de rețea care pot fi gestionate, cum ar fi comutatoarele, routerele, serverele și stațiile de lucru, sunt echipate cu modulul software agent SNMP. Acești agenți sunt responsabili pentru furnizarea accesului managerului SNMP la un MIB local, care stochează date despre funcționarea dispozitivului.

SNMP este vulnerabil la atac tocmai pentru că agenții SNMP pot fi interogați cu solicitări de obținere și pot accepta modificări de configurare cu solicitări setate, așa cum se arată în figură. De exemplu, o solicitare de setare poate determina repornirea unui router, trimiterea unui fișier de configurare sau primirea unui fișier de configurare. Un agent SNMP poate fi, de asemenea, configurat pentru a trimite capcane sau notificări. În SNMPv1 și SNMPv2c, aceste solicitări și notificări nu sunt autentificate sau criptate.

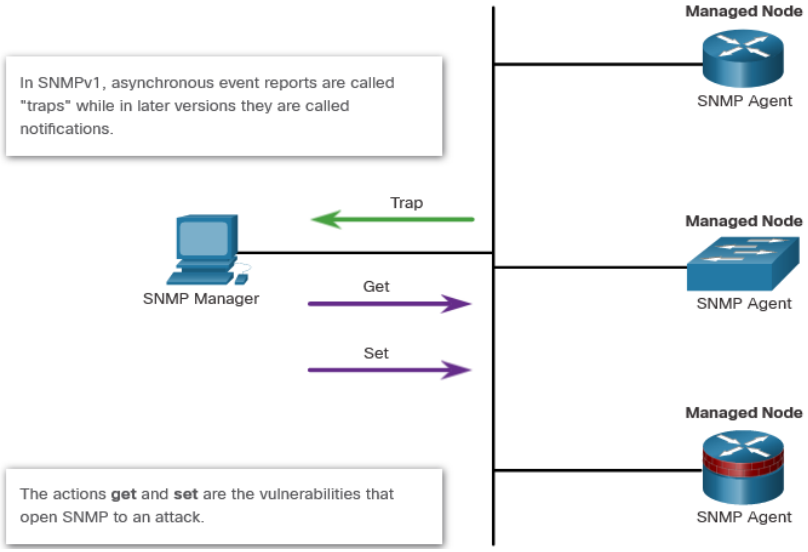


Fig. 6.17. Operatii SNMP.

6.7.6 - SNMPv3

SNMPv3 autentifică și criptează pachetele prin rețea pentru a oferi acces securizat la dispozitive. Acest lucru a abordat vulnerabilitățile versiunilor anterioare de SNMP.

SNMPv3 oferă trei caracteristici de securitate:

- ***Integritatea mesajului și autentificarea*** *- Se asigură că un pachet nu a fost manipulat în tranzit și că provine dintr-o sursă validă.*
- ***Criptare*** *- amestecă conținutul unui pachet pentru a preveni ca acesta să fie văzut de o sursă neautorizată.*
- ***Controlul accesului*** *- Restricționează fiecare principal la anumite acțiuni pe anumite porțiuni de date.*

6.7.7 - SNMPv3 Security Configuration

SNMPv3 poate fi securizat cu doar câteva comenzi, așa cum se arată în pașii următori.

Pasul 1. Configurara unui ACL care va permite accesul managerilor SNMP autorizați.

```
Router(config)# ip access-list acl-name
Router(config-std-nacl)# permit source_net
```

Pasul 2. Configurarea unei vizualizări SNMP cu comanda snmp-server view pentru a identifica OID-urile MIB pe care managerul SNMP le va putea citi. Configurarea unei vizualizări este necesară pentru a limita mesajele SNMP la acces numai în citire.

```
Router(config)# snmp-server view view-name oid-tree
```

SNMPv3 poate fi securizat cu doar câteva comenzi, așa cum se arată în figură.

Pasul 3. Configurarea caracteristicilor grupului SNMP cu comanda snmp-server group:

- *Configurarea unui nume pentru grup.*
- *Setare versiune SNMP la 3 cu cuvântul cheie v3.*
- *Solicitare autentificare și criptare cu cuvântul cheie priv.*
- *Asociere vizualizare la grup și acordare acces numai pentru citire cu comanda de citire.*
- *Specificare ACL configurat la **Pasul** 1.*

```
Router(config)# snmp-server group group-name v3 priv read view-name
access [acl-number | acl-name]
```

Pasul 4. Configurarea caracteristicilor utilizatorului grupului SNMP cu comanda utilizator snmp-server:

- *Configurare nume de utilizator și asocierea utilizatorului cu numele grupului configurat la **Pasul** 3.*
- *Setare versiunea SNMP la 3 cu cuvântul cheie v3.*
- *Setare tip de autentificare la md5 sau sha și configurare parolă de autentificare. SHA este preferat și ar trebui să fie acceptat de software-ul de management SNMP.*
- *Solicitare criptare cu cuvântul cheie priv și configurare parolă de criptare.*

```
Router(config)# snmp-server user username group-name v3 auth {md5 | sha}
auth-password priv {des | 3des | aes {128 | 192 | 256}} priv-password
```

6.7.8 - SNMPv3 Security Configuration Example

Figura prezintă un exemplu de configurare pentru securizarea SNMPv3.

Pasul 1. Un ACL standard este numit PERMIT-ADMIN și este configurat să permită numai rețeaua 192.168.1.0/24. Toate gazdele atașate la această rețea vor avea voie să acceseze agentul SNMP care rulează pe R1.

Pasul 2. O vizualizare SNMP se numește SNMP-RO și este configurată pentru a include întregul arbore iso din MIB. Într-o rețea de producție, administratorul de rețea ar configura

probabil această vizualizare pentru a include numai OID-urile MIB care erau necesare pentru monitorizarea și gestionarea rețelei.

Pasul 3. Un grup SNMP este configurat cu numele ADMIN. SNMP este setat la versiunea 3, fiind necesare autentificare și criptare. Grupului i se permite acces numai în citire la vizualizare (SNMP-RO). Accesul pentru grup este limitat de ACL PERMIS-ADMIN.

Pasul 4. Un utilizator SNMP, BOB, este configurat ca membru al grupului ADMIN. SNMP este setat la versiunea 3. Autentificarea este setată să utilizeze SHA și este configurată o parolă de autentificare. Deși R1 acceptă criptare până la AES 256, software-ul de management SNMP acceptă doar AES 128. Deci, criptarea este setată la AES 128 și este configurată o parolă de criptare.

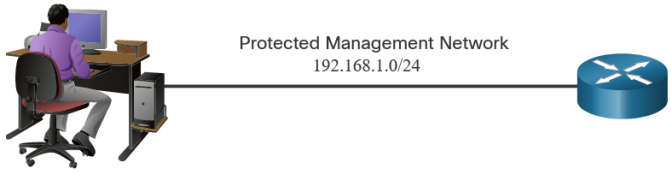


Fig. 6.18. Securizare SNMPv3.

```
R1(config)# ip access-list standard PERMIT-ADMIN
R1(config-std-nacl)# permit 192.168.1.0 0.0.0.255
R1(config-std-nacl)# exit
R1(config)# snmp-server view SNMP-RO iso included
R1(config)#  snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-
ADMIN
R1(config)# snmp-server user BOB ADMIN v3 auth sha cisco12345 priv aes 128
cisco54321
R1(config)# end
R1#
```

6.7.9 - SNMPv3 Verification

Verificarea celei mai mari parti a configurației de securitate SNMPv3 prin vizualizarea configurației care rulează, așa cum se arată în figură. Se observa că aceasta configurație a utilizatorului snmp-server este ascunsă. Se utilieaza comanda show snmp user pentru a vizualiza informațiile despre utilizator.

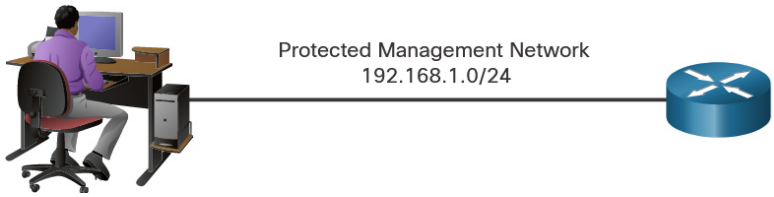


Fig. 6.19. Verificare Securitate SNMPv3.

```
R1# show run | include snmp
snmp-server group ADMIN v3 priv read SNMP-RO access PERMIT-ADMIN
snmp-server view SNMP-RO iso included
R1# show snmp user
User name: BOB
Engine ID: 80000009030030F70DA30DA0
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: ADMIN
```

Verificarea faptului că managerul SNMP poate trimite solicitări de obținere către R1 utilizând un instrument de gestionare SNMP, cum ar fi browserul MIB SNMP gratuit al ManageEngine. Configurare instrument cu detaliile utilizatorului, așa cum se arată în figură. Când un utilizator este configurat, se utilizeaza caracteristicile instrumentului de gestionare SNMP pentru a testa dacă utilizatorul configurat poate accesa agentul SNMP.

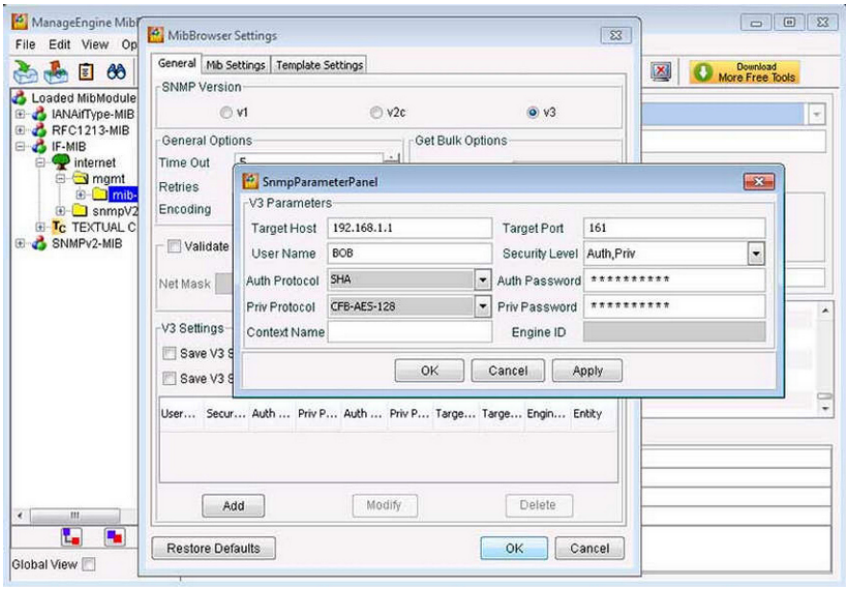


Fig. 6.20. Configurare SNMP Manager Access la SNMP Agent.

În figura de mai jos, administratorul de rețea a introdus OID-ul pentru tabelul de adrese IP. Solicitarea get a returnat toate informațiile de adresare pentru R1. Administratorul de rețea s-a autentificat cu acreditările corespunzătoare.

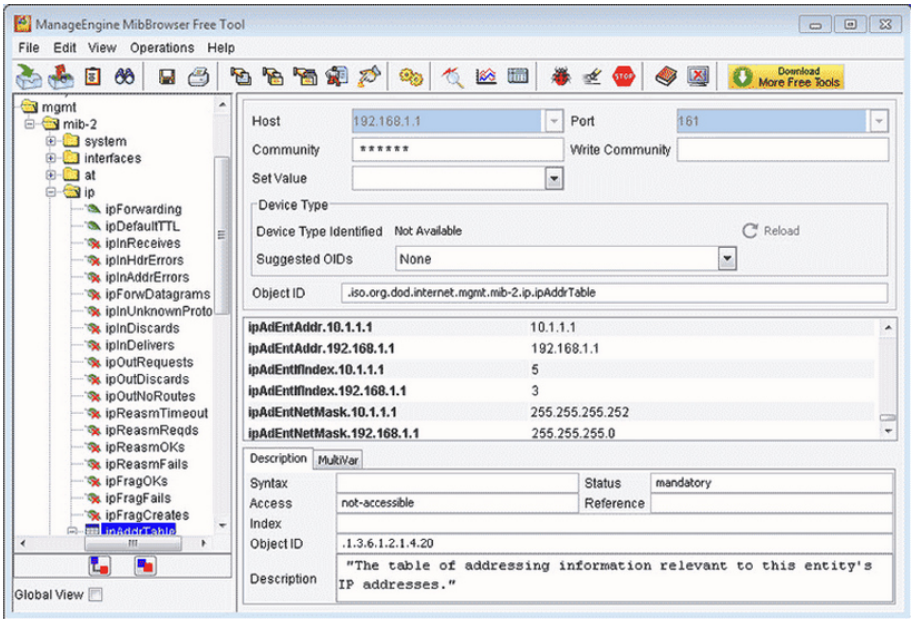


Fig. 6.21. Configurare SNMP Manager Get Request.

Figura este o captură de ecran cu adăugarea unui agent S. N. M. P. la software-ul gratuit al sistemului de management al rețelei Manage Engine S. N. M. P. M. I. B. Browser.

Verificare dacă datele au fost criptate rulând un analizor de protocol, cum ar fi Wireshark, și capturare pachete SNMP.

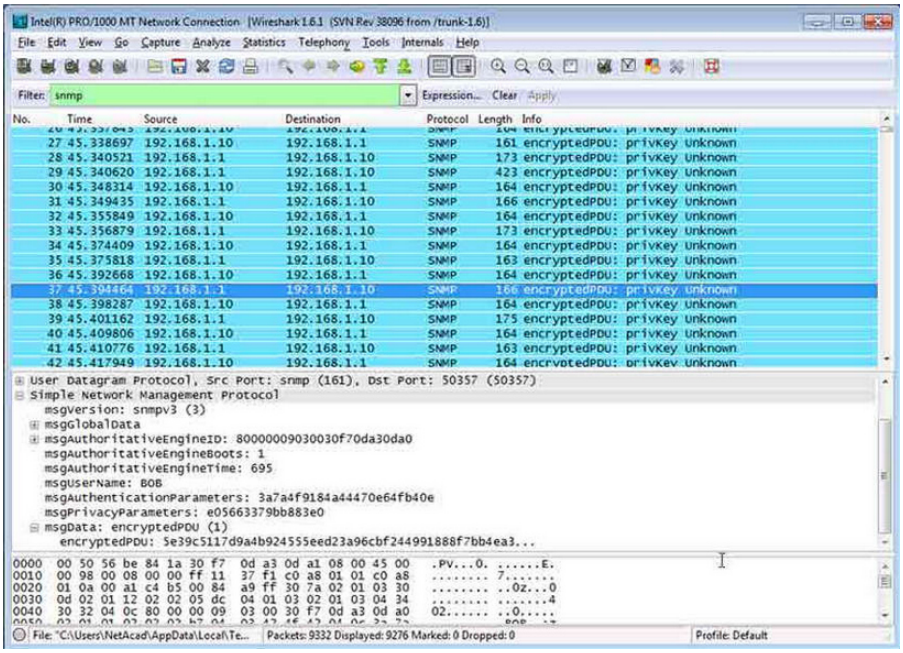


Fig. 6.22. Pachete capturate cu Wireshark criptate cu SNMPv3.

6.8 SUMMARY

Securizează fișierele de imagine și de configurare Cisco IOS - Caracteristica de configurare rezistentă Cisco IOS permite o recuperare mai rapidă dacă cineva reformatează memoria flash în mod rău intenționat sau neintenționat sau șterge fișierul de configurare de pornire din memoria nevolatilă cu acces aleatoriu (NVRAM). Caracteristica menține o copie de lucru sigură a fișierului imagine IOS al routerului și o copie a fișierului de configurare care rulează. Aceste fișiere securizate nu pot fi eliminate de către utilizator și sunt denumite setul de pornire principal. Funcția este disponibilă numai pe routerele mai vechi care acceptă o interfață flash PCMCIA Advanced Technology Attachment (ATA). Routerele mai noi, cum ar fi ISR 4000, nu acceptă această caracteristică. Pentru a securiza imaginea IOS și a activa rezistența imaginii Cisco IOS, utilizați comanda secure boot-image global configuration mode. Când este activată pentru prima dată, imaginea Cisco IOS care rulează este securizată și este generată o intrare de jurnal. Pentru a face o imagine a ruterului care rulează configurația și a o arhiva în siguranță în stocarea persistentă, utilizați comanda secure boot-config global configuration mode. Routerul poate fi configurat să pornească imaginea securizată din modul ROMmon. Fișierul de configurare poate fi copiat din locația securizată cu comanda secure boot-config restore. Caracteristica Secure Copy Protocol (SCP) oferă o metodă sigură și autentificată pentru copierea configurației routerului sau a fișierelor de imagine a routerului într-o locație la distanță. SCP se bazează pe SSH pentru comunicarea sigură și pe AAA pentru autentificare și autorizare. Dacă un router a fost compromis și parolele au fost modificate în valori necunoscute, există o procedură de recuperare a parolei pentru pornirea routerului fără configurarea acestuia, astfel încât parolele să poată fi modificate la valori cunoscute. Această procedură poate diferi între diferitele modele de dispozitiv. Este necesar accesul fizic la router și modul ROMmon. Este posibil să dezactivați accesul la procedura de recuperare a parolei cu comanda fără serviciu de recuperare a parolei.

Blocare unui router utilizând AutoSecure - Routerele Cisco sunt implementate inițial cu multe servicii care sunt activate implicit. Cu toate acestea, unele dintre aceste servicii, cum ar fi Cisco Discovery Protocol (CDP) și Link Layer Discovery Protocol (LLDP), pot face rețeaua vulnerabilă la atac. Ambele protocoale pot permite atacatorilor să învețe informații detaliate despre un router. Sunt furnizate instrucțiuni pentru modul în care fiecare serviciu de pe router ar trebui să fie configurat pentru securitate maximă. Caracteristica Cisco AutoSecure execută

un script care face recomandări pentru remedierea vulnerabilităților de securitate și apoi modifică configurația de securitate a routerului. AutoSecure permite trei servicii de redirecționare, Cisco Express Forwarding (CEF), filtrarea traficului cu ACL-uri și inspecția firewall Cisco IOS. AutoSecure este adesea folosit pe teren pentru a oferi o politică de securitate de bază pe un nou router. Caracteristicile pot fi apoi modificate pentru a sprijini politica de securitate a organizației. Când este introdusă comanda de securitate automată, dispozitivul va afișa mesajul de bun venit AutoSecure. AutoSecure va aduna apoi informații despre configurația curentă a dispozitivului și va intra într-un dialog de configurare. Apoi, va dezactiva și activa serviciile și va face alte modificări de configurare a dispozitivului. Când expertul este complet, configurația care rulează afișează toate setările și modificările de configurare. AutoSecure ar trebui să fie utilizat atunci când un router este configurat inițial. Nu este recomandat pe routerele de producție.

Autentificarea protocolului de rutare - Protocoalele de rutare dinamică sunt folosite de routere pentru a partaja automat informații despre accesibilitatea și starea rețelelor de la distanță. Protocoalele de rutare dinamică efectuează mai multe activități, inclusiv descoperirea rețelei și menținerea tabelelor de rutare. Avantajele importante ale protocoalelor de rutare dinamică sunt capacitatea de a selecta cea mai bună cale și capacitatea de a descoperi automat cea mai bună cale nouă atunci când există o schimbare în topologie. Descoperirea rețelei este capacitatea unui protocol de rutare de a partaja în mod dinamic informații despre rețelele pe care le cunoaște cu alte routere care utilizează același protocol de rutare. Sistemele de rutare pot fi atacate prin întreruperea ruterelor de rețea peer sau prin falsificarea sau falsificarea informațiilor transportate în cadrul protocoalelor de rutare. Acest lucru poate fi folosit pentru a determina sistemele să se dezinforma (mint) unul pe celălalt, să provoace un atac DoS sau să determine traficul să urmeze o cale pe care în mod normal nu ar urma-o. Actualizările protocolului de rutare pot fi configurate pentru a utiliza autentificarea MD5 sau SHA. Acest lucru vă ajută să vă asigurați că actualizările protocolului de rutare provin din surse de încredere. Autentificarea MD5 este disponibilă pentru protocolul de rutare OSPF, totuși SHA este preferat pentru o mai mare securitate.

Management și raportare sigure - Majoritatea dispozitivelor de rețea pot aduna și transmite informații de jurnal care pot fi foarte valoroase pentru diagnosticarea problemelor de rețea și detectarea incidentelor de securitate. Într-o rețea mică, gestionarea și monitorizarea

unui număr mic de dispozitive de rețea este o operațiune simplă. Cu toate acestea, într-o întreprindere mare cu sute de dispozitive, monitorizarea, gestionarea și procesarea mesajelor de jurnal poate fi o provocare. Fluxul de informații între gazdele care colectează fișierele jurnal și dispozitivele de rețea gestionate poate lua două căi. Căile de informații în bandă folosesc rețeaua de producție, internetul sau ambele. Traficul de gestionare este trimis în aceeași rețea ca și traficul utilizatorilor. Căile de gestionare în afara benzii (OOB) utilizează rețele de gestionare dedicate care nu transmit trafic de utilizatori. Ca regulă generală, din motive de securitate, managementul OOB este adecvat pentru rețelele mari ale întreprinderilor. Cu toate acestea, nu este întotdeauna de dorit. Depinde de aplicațiile și protocoalele de management care sunt monitorizate. Administrarea în bandă este recomandată în rețelele mai mici ca mijloc de a realiza o implementare de securitate mai rentabilă. Ghidurile de securitate pentru managementul OOB trebuie să ofere cel mai înalt nivel de securitate și să atenueze riscul de a trece protocoale de management nesigure prin rețeaua de producție. Pentru gestionarea în bandă, liniile directoare se aplică numai dispozitivelor care trebuie gestionate sau monitorizate, utilizați IPSec, SSH sau SSL atunci când este posibil și decideți dacă canalul de gestionare trebuie să fie disponibil în orice moment. Dacă utilizați instrumente de management de la distanță cu management în bandă, aveți grijă de vulnerabilitățile de securitate subiacente ale instrumentului de management în sine.

Securitatea rețelei folosind Syslog - Cea mai comună metodă de accesare a mesajelor de sistem este utilizarea unui protocol numit syslog. Multe dispozitive de rețea acceptă standardul syslog. Protocolul syslog permite dispozitivelor de rețea să-și trimită mesajele de sistem prin rețea către serverele syslog. Serviciul de înregistrare syslog oferă posibilitatea de a aduna informații de înregistrare, de a selecta tipul de informații care sunt înregistrate și de a specifica dispozitivele de destinație care vor primi și stoca mesaje syslog. Pe dispozitivele de rețea Cisco, protocolul syslog poate trimite mesaje de sistem și poate depana ieșirea comenzii către un proces de înregistrare locală care este intern dispozitivului sau poate trimite mesaje către un buffer intern. Mesajele trimise în bufferul intern pot fi vizualizate numai prin CLI-ul dispozitivului. Un dispozitiv poate fi configurat să trimită mesaje syslog către un buffer de înregistrare, linie consolă, o linie terminală sau un server syslog extern. Mesajele Syslog conțin un nivel de severitate care poate varia de la Nivelul 0 la Nivelul 7. Cu cât numărul nivelului este mai mic, cu atât severitatea este mai mare. De exemplu, mesajele de la Nivelul 0

până la Nivelul 4 sunt despre defecțiuni software sau hardware. Mesajele de nivel 5 indică funcționarea normală, dar sunt semnificative. Nivelul 6 se referă la evenimente normale de funcționare, iar Nivelul 7 este pentru depanarea mesajelor. În plus, mesajele syslog includ un cod de facilitate syslog. Unele facilități indică sistemul, componenta sau protocolul care a raportat mesajul. Comanda service timestamps log datetime configurează dispozitivul să utilizeze marcajele de timp ale sistemului pentru toate mesajele. Marcajele de timp pot proveni de la ceasul dispozitivului local sau pot fi sincronizate între dispozitivele care utilizează Network Time Protocol (NTP) pentru ora sistemului. Implementările Syslog constau din servere syslog, cunoscute ca gazde de jurnal, care primesc și stochează mesaje syslog din întreaga rețea și clienți syslog care generează și transmit mesaje syslog către serverele syslog. Un dispozitiv Cisco este configurat să utilizeze syslog prin specificarea gazdei de înregistrare cu comanda de înregistrare, setând opțional nivelul de severitate al mesajelor care urmează să fie înregistrate cu comanda logging trap, setând opțional interfața.

Protocolul simplu de gestionare a rețelei (SNMP) a fost dezvoltat pentru a permite administratorilor să gestioneze noduri precum servere, stații de lucru, routere, comutatoare și dispozitive de securitate, într-o rețea IP. SNMP definește modul în care informațiile de management sunt schimbate între aplicațiile de gestionare a rețelei și agenții de management. Este un protocol de nivel de aplicație care oferă un format de mesaj pentru comunicarea între manageri și agenți. Sistemul SNMP necesită trei elemente și constă dintr-un manager SNMP, un agent SNMP și baza de informații de management (MIB). Managerul SNMP face parte dintr-un sistem de management al rețelei (NMS) care rulează software de management SNMP. Agenții SNMP se află pe dispozitivele de rețea și permit colectarea și partajarea datelor din rețea. MIB stochează variabile standardizate care conțin date de rețea. Managerul de rețea poate trimite o solicitare de obținere pentru a prelua informații de la MIB-ul local al unui agent sau poate trimite o solicitare setată pentru a schimba valoarea unei variabile din MIB. MIB organizează variabilele ierarhic. Variabilele MIB permit software-ului de management să monitorizeze și să controleze dispozitivul de rețea. RFC-urile definesc unele variabile publice comune pe care le suportă majoritatea dispozitivelor. În plus, furnizorii de echipamente de rețea, cum ar fi Cisco, își pot defini propriile ramuri private ale arborelui pentru a găzdui noile variabile specifice dispozitivelor lor. Există trei versiuni de SNMP. SNMPv1 este învechit și este menționat doar, dar SNMPv2c și SNMPv3 sunt relevante pentru acest curs. SNMPv2c ar

trebui utilizat cel puțin cu SNMPv3 recomandat. SNMPv1 și SNMPv2c oferă caracteristici minime de securitate. Mai exact, SNMPv1 și SNMPv2c nu pot nici autentifica sursa unui mesaj de management și nici nu pot furniza criptare. SNMPv3 adaugă metode pentru a asigura transmiterea securizată a datelor critice între dispozitivele gestionate. SNMPv3 oferă atât modele de securitate, cât și niveluri de securitate. Un model de securitate este o strategie de autentificare configurată pentru un utilizator și pentru grupul în care locuiește utilizatorul. Un nivel de securitate este nivelul permis de securitate într-un model de securitate. O combinație a nivelului de securitate și a modelului de securitate determină ce mecanism de securitate este utilizat la manipularea unui pachet SNMP. SNMPv3 autentifică și criptează pachetele prin rețea pentru a oferi acces securizat la dispozitive. Acest lucru a abordat vulnerabilitățile versiunilor anterioare de SNMP.