# 10. 1 Bazele Managementului Retelelor

Scopul capitolului il reprezinta faptul de a deveni familiarizat cu functiile de baza ale managementului retelelor. Acest capitol prezinta functiile uzuale ale arhitecturilor si protocoalelor de retea. De asemenea prezinta cele cinci arii conceptuale ale managementului asa cum sunt descrise de Standardul International de Organizare (ISO).

Managementul retelei reprezinta diferite lucruri pentru diferite persoane. In unele cazuri aceasta implica o solidaritate intre activitatea de monitorizare a retelei cu analizorul actual al protocolului. In general, managementul retelei este un service ce implica o varietate de obiecte, aplicatii si dispozitive pentru a ajuta managerii de retea in monitorizarea si intretinerea retelei.

In perioada anilor 1980 s-au observat dezvoltari spectaculoase in domeniul retelelor. Companiile au realizat beneficii legate de cost si productivitate legate de tehnologia retelelor si au inceput sa adauge retele si sa extinda retelele actuale aproape la fel de rapid cum produsele si tehnologiile retelei au fost introduse. Problemele asociate cu extinderea retelei afecteaza zi de zi atat operatia de management al retelei si strategia de planificare a retelei.

In jurul anilor 1980 lucrurile legate de echipamente pentru un management larg si retele heterogene a creat o criza pentru multe organizatii. O necesitate urgenta pentru managementul automat al retelei (incluzand ceea ce este tipic denumit planificarea capacitatii retelei) integrate in cele mai diverse medii.

**Arhitectura managementului retelei**

Majoritatea arhitecturilor managementului retelei folosesc aceeasi structura de baza si acelasi set de relatii. Finalul statiilor de lucru (dispozitive structurate) cum ar fi sistemele de calculatoare si alte dispozitive de retea, ruleaza software ce le permite acestora sa trimita avertizare atunci cand recunosc probleme. Desi primesc aceste avertizari entitatile managementului sunt programate sa reactioneze executand 1 cateva sau un grup de actiuni incluzand oprirea sistemului.

Entitatile sistemului pot de asemenea sa aleaga valorile variabilelor singure. Alegerea poate fi automata sau manuala, dar agentii din cadrul dispozitivelor de management raspund de toate alegerile. Agentii sunt module software ce la inceput compileaza informatiile despre dispozitivele de management in care se afla, apoi pastreaza aceste informatii intr-o baza de date.In final permite managementul entitatilor din sistemul de management al sistemului (NMSs) prin intermediul unui protocol. Binecunoscutele protocoale includ Simple Network Management Protocol (SNMP) si Common Management Information Protocol (CMIP).

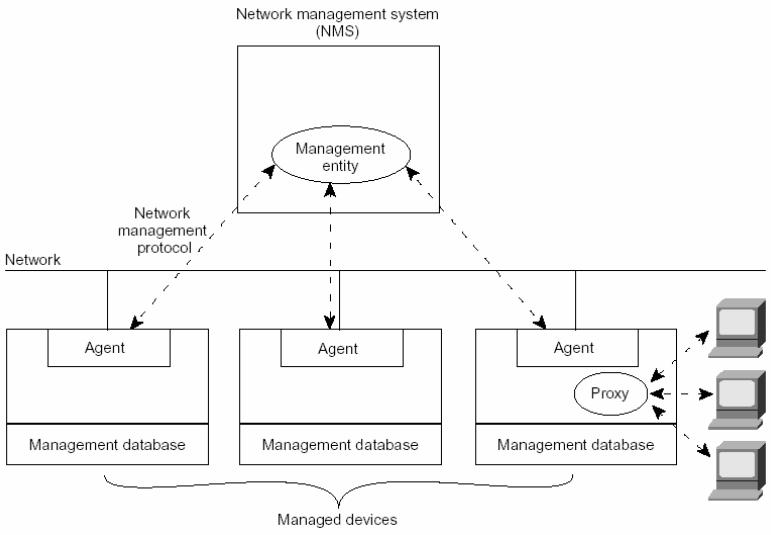



Figura alaturata prezinta arhitectura managementului retelei.

***Modelul ISO al managementului retelei***

ISO a contribuit foarte mult pentru standardizarea retelelor. Pentru a intelege principalele functii ale sistemului de management a retelei este important sa se inteleaga modelul de management a retelelor.

Acest model contine 5 arii conceptuale asa cum urmeaza:
-managementul performantei
-managementul configuratiei
-managementul contabilizarii
-defectele managementului
-managementul securitatii

**Managementul performantei**: Scopul managementului performantei este acela de a masura si a face disponibile de lucru variate aspecte ale performantei retelei astfel incat performanta de lucru a internet-ului poate fi mentinuta la nivel acceptabil. Exemplu de variabile ale performantei care pot fi conditionate includ timpii de raspuns ai utilizatorului si utilizarea liniei.
Managementul performantei implica trei pasi importanti. Primul, perfectionarea informatiei este legata de variabilele de interes pentru administratorii de retea. In al doilea rand informatia este analizata pentru a determina nivelele normale.
Entitatile managementului continua monitorizarea performantei variabilelor. Cand performanta scade sub un anumit nivel , o avertizare este generata si trimisa sistemului de management a retelei.
Fiecare pas descris mai sus apartine procesului de setare a sistemului reactiv. Cand performantele devin inacceptabile pentru nivelul de performanta cerut utilizator , sistemul reactioneaza trimitand un mesaj. De asemenea performantele managementului permit metode proactive. Spre exemplu, simularea retelei poate fi utilizata planului de a largi reteaua. Aceasta va afecta performanta metrica. Simularea poate avertiza administratorii sa impiedice problemele astfel incat sa poata fi luate masuri de contracarare a acestora.

**Managementul configurarii :** Scopul managementului configurarii este acela de a monitoriza reteaua si informatiile legate de configurarea sistemului astfel incat efectele asupra variatelor elemente hard si soft ale retelei sa poata fi organizate. Managementul configuratiei subsistemelor pastreaza aceste informatii intr-o baza de date pentru un acces usor. Cand apare o problema aceasta baza de date poate fi cautata pentru a gasi un element ajutator pentru rezolvarea acestor probleme.

**Managementul contabilizarii**: Scopul managementului contabilizarii este acela de a masura parametrii de utilizare a retelei astfel incat utilizarea individuala sau de grup pot fi apropiate. Asa cum regularizarea minimizeaza problemele retelei (deoarece resursele retelei pot fi bazate pe capacitatile resurselor) si sa maximizeze accesul in retea in aceeasi masura pentru toti utilizatorii. Asa cum managementul performantei, primul pas apropiat in stabilirea managementului contabilizarii este acela de a masura utilizarea tuturor resurselor importante ale retelei. Desigur unele corectii vor fi aplicate pentru a realiza un acces optim. Din acest punct de vedere, sistemul de masurare a resurselor folosite poate oferi atat informatii despre costuri cat si despre utilizarea corecta si optimala a resurselor utilizator.

**Defectele managementulu**i: Scopul defectelor este acela de a detecta, informa utilizatorii si de a fixa automat problemele retelei, sa pastreze functionarea efectiva a retelei. Deoarece defectele pot cauza intarzieri sau degradari inacceptabile pentru retea, sistemul de detectie a defectelor managementului este probabil cel mai vast sistem din cadrul elementelor de management ISO ale retelei. Defectele managementului implica in primul rand determinarea simptomelor si izolarea problemei. Apoi problema este fixata si solutia este testata in toate subsistemele de baza (importante). In final, detectarea si rezolvarea problemei este inregistrata.

**Managementul securitatii**: Scopul managementului securitatii este acela de a controla accesul catre resursele retelei astfel incat reteaua sa nu poata fi absorbita (intentionat sau neintentionat) si informatii sensibile nu pot fi accesate de oricine fara a detine autorizatie. Spre exemplu, securitatea managementului subsistemului poate monitoriza utilizatorii logati la resursele retelei si poate refuza accesul acelora care nu introduc coduri de acces corecte.

Managementul securitatii subsistemului lucreaza impartind resursele retelei in zone autorizate si neautorizate. Pentru unii utilizatori accesul catre orice resursa a sistemului este interzisa in mare parte datorita faptului ca utilizatorii sunt de obicei companii din afara. Pentru alti utilizatori din interior nu se ofera acces la informatii originale din cadrul altui departament. Spre exemplu accesul la fisierele ce apartin Departamentului de Resurse Umane este interzis pentru majoritatea utilizatorilor ce nu fac parte din acest departament.

Managementul securitatii subsistemelor dezvolta cateva functii. Ele identifica resursele

sensibile ale retelei incluzand sisteme, fisiere si alte entitati si determina potrivirea intre resursele sensibile si utilizatorii corespunzatori. De asemenea ele monitorizeaza accesul catre resursele sensibile si realizeaza logarea adecvata a persoanelor catre resursele sensibile ale retei.

## 10.2 Simple network management protocol

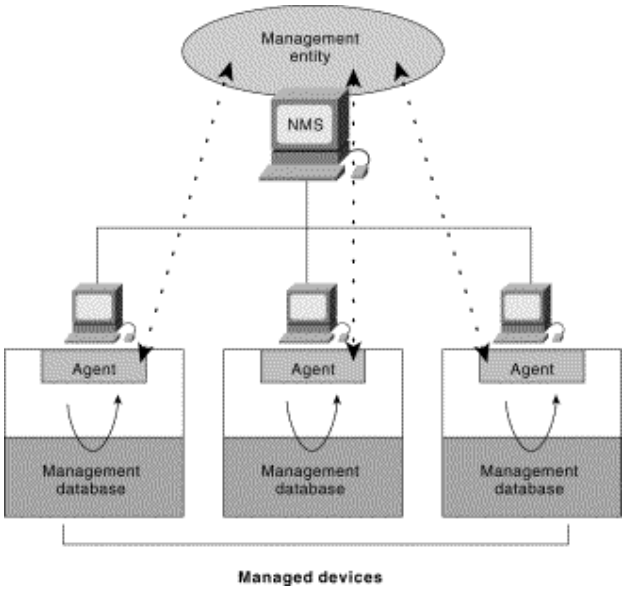
SNMP este un protocol care faciliteaza schimbul de informatii intre dispozitivele unei retele. Face parte din protocolul TCP/IP. SNMP permite administratorilor de retea sa administreze performantele retelelor, sa gaseasca sis a resolve problemele acestora, si sa planifice dezvoltarea lor.

Exista doua versiuni de SNMP: SNMP version 1 si SNMP version 2. Amandoua versiunile au un numar de trasatuir in comun , dar SNMP v2 ofera imbunatatiri, ca de exemplu operatii cu protocoale. Standardizarea unei alte versiuni de SNMP – SNMP v3 este in dezvoltare. SNMP v2 este incompatibil cu SNMP v1 in 2 domenii cheie:formate mesaj si operatii cu protocoale. Mesajele SNMP v2 folosesc headere diferite si protocol data unit ca cele din SNMP v1. SNMP v2 mai foloseste 2 protocoale de operatii care nu sunt specificate in SNMP v1.

Componentele de baza ale SNMP O retea administrate de protocolul SNMP consta in 3 componente: dispozitive administrate, agenti si sisteme de administrare a retelelor (NMSs).

Un dispozitiv administrat este un nod de retea care contine un agent SNMP care se afla pe o retea administrata. Dispozitivele administrate colecteaza si stocheaza informatia manageriala si fac disponibila aceasta informatie pentru NMSs, folosind SNMP. Dispozitivele administrate, uneori numite elemente de retea, pot fi routere si servere de acces switch-uri sau bridge-uri, hub-uri, computere gazda sau imprimante.

Un agent este un modul software administrator de retea care care se afla intr-un dispozitiv. Un agent are o cunostinta locala despre managementul informatiei si traduce acea informatie intr-o forma compatibila cu SNMP.




Un MIB (management information base) este o colectie de informatii organizate ierarhic. MIBs sunt accesate folosind un protocol de administrare cum este SNMP-ul. Sunt alcatuite din obiecte administrate si sunt identificate de identificatorii de obiecte.

Un obiect administrat, uneori numit obiect MIBeste unul din orice numar de caracteristici specifice ale unui dispozitiv. Obiectele sunt alcatuite din unul sau mai multe cazuri de obiecte, care sunt variabile esentiale.

Exista 2 tipuri de obiecte: scalare si tabelare. Obiectele scalare definesc un singur fel de obiect.Obiectele tabelare definesc mai multe feluri de obiecte inrudite care sunt grupate in tabele MIB.

Un nMs executa aplicatii care monitorizeaza si controleaza dispozitivele administrate. NMSs ofera majoritatea procesarii si resursele de memorie necesare pentru administrarea retelei. Uul sau mai multe NMSs trebuie sa existe in orice retea administrata.

### 10.2.2 Comenzi de baza SNMP

Dispozitivele administrate sunt monitorizate si controlate folosind 4 comenzi de baza SNMP: read (citeste), write (scrie), trap (captura eveniment), si traversal operations (operatii transversale).

Comanda read este folosita de un NMS pentru a monitoriza dispozitivele. NMS-ul

examineaza diferite care sunt mentinute de dispozitivele administrate.

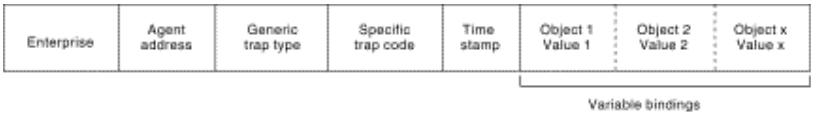
Comanda write este folosita de NMS pentru a controla dispozitivele. NMS-ul schimba valorile variabilelor stocate in dispozitive.

Comanda trap este folosita de dispozitive pentru a raporta asincron evenimentele NMS-ului. Cand anumite tipuri de evenimente se intampla un dispozitiv trimte un trap NMS-ului.

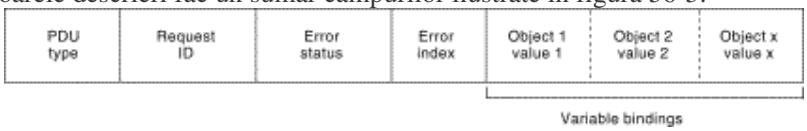
Operatiile transversale sunt folosite de NMS pentru a determina care variabila este suportate de un dispozitiv si pentru a aduna informatii in tabele de variabile, ca de exemplu o routing table.

### 10.2.3 Unitatea de protocol SNMP v1

SNMP v1 PDU contin o comanda specifica si operanzi care indica instanta obiectului implicat in tranzactie. Campurile SNMP v1 PDU sunt variabile in lungime. Figura urmatore ilustreaza campurile SNMP v1




Urmatoarele descrieri fac un sumar campurilor ilustrate in figura 56-5:

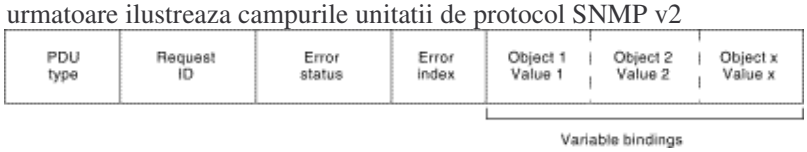



-PDU type specifica tipul de PDU transmis
-Request Id asociaza cererile SNMP cu raspunsuri
-Error status indica unul dintre numerele de erori si tipul acestora.
-Error index asociaza o eroare cu o anumita instanta de obiect.
-Variable bindings foloseste ca camp de date al SNMP v1 PDU

### 10.2.4. Unitatea de protocol SNMP v2

SNMP v2 specifica 2 tipuri de formate PDU in funcite de operatia cu protocoale SNMP. Campurile SNMP v2 PDU sunt variabile in lungime

Figura urmatoare ilustreaza campurile unitatii de protocol SNMP v2




-Pdu type identifica tipul de pdu transmis
-Request id asociaza cererile SNMP cu raspunsuri
-Error status asociaza numarul unei erori cu tipul erorilor.
-error index asociaza o eroare cu o instanta de obiect anume.
-Variable bindings foloseste ca camp de date pt SNMP v2 PDU.

## 11.1. Securitatea retelelor de calculatoare

Protejarea informațiilor proprietare este de o importanta cruciala. Ignorarea nevoii de securitate duce inevitabil la pierderi materiale. Un angajat nemulțumit sau dornic de un câştig necuvenit va încerca (si aproape sigur va reuşi) sa-si însuşească informații ce nu ar trebui sa îi parvină (liste de clienți, studii de piața, strategii, surse software proprietare, înregistrări contabile, etc.), ceea ce se va reflecta direct în pierderi severe pentru companie.

La fel de uşor atacul poate surveni si din exterior. Orice entitate (concurent, investitor, etc.) poate contracta un atac asupra rețelei informatice a companiei pentru scopuri ce variază în funcție de interesele contractorului (scăderea valorii companiei-victima pentru a o achiziționa apoi la un preț mai mic, însuşirea de proiecte secrete, surse de programe confidențiale, analiza contabilității, furtul de tehnologie, etc.

Domeniul securității informatice este unul dintre cele mai dinamice domenii ale informaticii. Noi metode de atac apar zilnic, si zilnic se proiectează metode de contracarare a lor.

## 11.2. Planificarea securitatii retelei

Intr-o retea de calculatoare, trebuie sa existe garantia ca datele secrete sunt protejate, astfel incat doar utilizatorii autorizati sa aiba acces la ele.

Vulnerabilitatea retelelor de calculatoare se manifesta in doua moduri:

-Modificarea sau distrugerea informatiei

-Posibilitatea folosirii neautorizate a informatiilor

Asigurarea "securitatii datelor" stocate in cadrul unei retele de calculatoare, presupune proceduri de manipulare a datelor care sa nu poata duce la distribuirea accidentala a lor/sau masuri de duplicare a datelor importante, pentru a putea fi refacute in caz de nevoie.

A avea o retea de calculatoare cu acces sigur la date, presupune o procedura de autentificare a utilizatorilor si/sau de autorizare diferentiata pentru anumite resurse.

Orice retea trebuie asigurata impotriva unor daune intentionate sau accidentale. Exista patru amenintari majore la securitatea unei retele de calculatoare:

1. Accesul neautorizat
2. Alterarea electronica a datelor
3. Furtul de date
4. Daunele intentionate sau accidentale

Cade in sarcina administratorului de retea sa asigure o retea sigura, fiabila si pregetita sa faca fata pericolelor de mai sus.

Vom considera ca o retea de calculatoare este sigura daca toate operatiile sale sunt intotdeauna executate conform unor reguli strict definite, ceea ce are ca efect o protectie completa a entitatilor, resurselor si operatiilor. Lista de amenintari constituie baza definirii cerintelor de securitate. Odata acestea fiind cunoscute, trebuie elaborate regulile conform carora sa se controleze ansamblul operatiilor retelei.

Aceste reguli operationale se numesc"servicii de securitate", iar implementarea serviciilor se face prin protocoale de securitate.

### Utilizarea retelelor de calculatoare

Pentru ca activitatea utilizatorilor unei retele să fie eficient organizată si să se poată asigura securitatea retelei, fiecărui utilizator îi va fi asociat un cont, care va fi caracterizat printr-o sumă de drepturi de acces la resursele fizice si logice ale retelei (fisiere, directoare, programe, drive-uri de retea, imprimante de retea), corespunzător necesităților si cunostintelor utilizatorilor. Stabilirea riguroasă a drepturilor de acces este foarte importantă pentru asigurarea securității retelei; softul de retea va asigura respectarea drepturilor acordate. Uzual, aceste drepturi sunt stabilite pe grupuri de utilizatori cu obiective si necesități similare. Un grup este o multime de utilizatori care au aceleasi drepturi de acces la o anumită resursă a retelei (de exemplu, se pot defini grupuri pentru studenti,

cadre didactice etc.).

Crearea domeniilor de lucru, a grupurilor de utilizatori si a conturilor cu drepturile aferente, precum si actualizarea acetora este realizată de administratorul de retea, persoana cu pregătire de specialitate care se ocupă de (instalarea,) configurarea, si administrarea functionării eficiente si în conditii de securitate a retelei. Securitatea retelei poate fi identificată cu controlul pe care administratorul de retea îl detine asupra resurselor retelei, precum si asupra drepturilor de acces la aceste resurse.

Fiecare cont de retea va avea un nume de identificare - numele contului - si o parolă atasată, cu rol în asigurarea protectia datelor utilizatorului. Parola, formată din orice caractere tipăribile, are o lungime dependentă de sistemul de operare de retea (cel putin 5-8 caractere). Utilizatorii îsi pot schimba oricând, în cursul unei sesiuni de lucru, parola proprie folosind facilitătile oferite de sistemului de operare (de exemplu, optiunile ferestrei de securitate deschise cu Ctrl-Alt-Del într-o sesiune Windows NT sau comanda setpass în Novell Netware).

Conectarea la o retea este procesul prin care serverul care gestionează reteaua este informat că un utilizator va începe folosirea resurselor retelei. Procedura de conectare este dependentă de sistemul de operare de retea (de exemplu, fereastra de logare deschisă cu combinatia de taste Ctrl-Alt Del în Windows NT, unde se completează numele contului, parola si domeniul pe care se face logarea sau comanda login în Novell Netware).

Deconectarea de la o retea este procesul prin care serverul este anuntat că utilizatorul respectiv încheie utilizarea resurselor retelei. După deconectarea de la retea se pot folosi doar resursele locale ale calculatorului (hard-disk-ul local si programele aflate pe acesta, pe dischete sau CD-uri).

Într-o retea locală se pot partaja, adică folosi în comun de către mai multi utilizatori (termenul englez pentru partajare este "share"), resurse fizice sau logice, folosind instrumente specifice oferite de sistemul de operare (de exemplu, sub Windows NT, optiunea Share din meniul contextual al obiectului dorit). Resursele partajate vor putea fi folosite de către utilizatori în functie de drepturile de acces pe care le au asupra acestor resurse.

Resursele fizice partajate într-o retea locală sunt discurile si imprimantele de retea.

## 11.3 Aspecte de securitate în retele de calculatoare

Importanta aspectelor de securitate în retelele de calculatoare a crescut odată cu extinderea prelucrărilor electronice de date si a transmiterii acestora prin intermediul retelelor. În cazul operării asupra unor informatii confidentiale, este important ca avantajele de partajare si comunicare aduse de retelele de calculatoare să fie sustinute de facilităti de securitate substantiale. Acest aspect este esential în conditiile în care retelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea de operatiuni bancare, cumpărături sau plata unor taxe.

Problemele de asigurare a securitătii retelelor pot fi grupate în următoarele domenii interdependente:

- *confidentialiatea* se referă la asigurarea accesului la informatie doar pentru utilizatorii autorizati si împiedicarea accesului pentru persoanele neautorizate;
- *integritatea* se referă la asigurarea consistentei informatiilor (în cazul transmiterii unui mesaj prin retea, integritatea se referă la protectia împotriva unor tentative de falsificare a mesajului);
- *autentificarea* asigură determinarea identitătii persoanei cu care se comunică (aspect foarte important în cazul schimbului de informatii confidentiale sau al unor mesaje în care identitatea transmitătorului este esentială);
- *ne-repudierea* se referă la asumarea responsabilitătii unor mesaje sau comenzi, la autenticitatea lor. Acest aspect este foarte important în cazul contractelor realizate între firme prin intermediul mesajelor electronice: de exemplu, un contract / comandă cu o valoare foarte mare nu trebuie să poată fi ulterior repudiat(ă) de una din părti (s-ar putea sustine, în mod fraudulos, că întelegerea initială se referea la o sumă mult mai mică).

Implementarea unor mecanisme de securitate în retelele de calculatoare de arie largă, în particular - Internet-ul, priveste rezolvarea următoarele aspecte:

1. bombardarea cu mesaje - asa numitul spam - trimiterea de mesaje nedorite, de obicei cu un continut comercial. Acest fenomen este neplăcut în cazul unui număr mare de mesaje publicitare nedorite si poate avea efecte mai grave în cazul invadării intentionate cu mesaje ("flood"), uzual cu un continut nesemnificativ.
2. rularea unui cod (program) dăunător, adesea de tip virus - acesta poate fi un program Java sau ActiveX, respectiv un script JavaScript, VBScript etc. ;
3. infectarea cu virusi specifici anumitor aplicatii - se previne prin instalarea unor programe antivirus care detectează virusii, devirusează fisierele infectate si pot bloca accesul la fisierele care nu pot fi "dezinfectate". În acest sens, este importantă devirusarea fisierelor transferate de pe retea sau atasate mesajelor de mail, mai ales dacă contin cod sursă sau executabil, înainte de a le deschide / executa.
4. accesarea prin retea a calculatorului unui anumit utilizator si "atacul" asupra acestuia. La nivelul protocoalelor de retea, protejarea accesului la un calculator sau la o retea de calculatoare se realizează prin mecanisme de tip firewall, prin comenzi specifice; acestea pot fi utilizate si în sens invers, pentru a bloca accesul unui calculator sau a unei retele de calculatoare la anumite facilităti din Internet.
5. interceptarea datelor în tranzit si eventual modificarea acestora - snooping. Datele se consideră interceptate atunci când altcineva decât destinatarul lor le primeste. În Internet, datele se transmit dintr-un router în altul fără a fi (uzual) protejate. Routerele pot fi programate pentru a intercepta, eventual chiar modifica datele în tranzit. Realizarea unei astfel de operatii este destul de dificilă, necesitând cunostinte speciale de programare în retele si Internet, dar există numeroase programe (de tip „hacker") care pot fi utilizate în aceste scopuri, ceea ce duce la cresterea riscului de interceptare a datelor. Transmisia protejată a datelor trebuie să garanteze faptul că doar destinatarul primeste si citeste datele trimise si că acestea nu au fost modificate pe parcurs (datele primite sunt identice cu cele trimise). Modificarea datelor s-ar putea realiza în mod intentionat, de către o persoană care atentează la securitatea retelei sau printr-o transmisie defectuoasă.
6. expedierea de mesaje cu o identitate falsă, expeditorul impersonând pe altcineva (pretinde că mesajul a fost trimis de la o altă adresă de postă electronică): spoofing. Această problemă se revolvă prin implementarea unor mecanisme de autentificare a expeditorului.

Pentru asigurarea securitătii retelei este importantă implementarea unor mecanisme specifice pornind de la nivelul fizic (protectia fizică a liniilor de transmisie ), continuând cu proceduri de blocare a accesului la nivelul retelei (firewall), până la aplicarea unor tehnici de codificare a datelor (criptare), metodă specifică pentru protectia comunicării între procesele de tip aplicatie care rulează pe diverse calculatoare din retea.

Împiedicarea interceptării fizice este în general costisitoare si dificilă; ea se poate realiza mai facil pentru anumite tipuri de medii (de exemplu, detectarea interceptărilor pe fibre optice este mai simplă decât pentru cablurile cu fire de cupru). De aceea, se preferă implementarea unor mecanisme de asigurare a securitătii la nivel logic, prin tehnici de codificare / criptare a datelor transmise care urmăresc transformarea mesajelor astfel încât să fie întelese numai de destinatar; aceste tehnici devin mijlocul principal de protectie a retelelor.

## 11. 2 Metode de autentificare a utilizatorilor

In comunicatiile moderne, nevoia stabilirii veridicitatii unui document sau a unui corespondent este mare. Autentificarea este parte integranta din strategia generala de securitate a unei firme.

Informatia de autentificare poate fi necesara cand utilizatorii se conecteaza la un sistem, si sunt identificati in general printr-o informatie care le este cunoscuta: o parola, o cheie, sau o cartela. Pe baza acestor informatii ii sunt accesibile utilizatorului anumite servicii de retea. Se poate preveni astfel accesul neautorizat al unor persoane la sistemele din retea.

Autentificarea poate fi folosita si pentru a se asigura originalitatea sursei mesajului intr-un mod asemanator semnaturii de pe o scrisoare.

Modurile prin care se poate realiza autentificarea sunt mutiple:

1. parole
2. autentificare prin cheie criptografica

3. coduri cu mesaj de autentificare
4. prin folosirea de servere de autentificare (trusted third parties)
5. jetoanele de securitate(security tokens)
6. date biometrice

**Parolele**: atunci cand ne aflam in situatia de a restrictiona accesul la anumite fisiere din retea, utilizatorii trebuie sa fie identificati in mod unic. Aceasta se poate realiza prin folosirea unei parole pentru autentificare. Este cel mai usor de implementat si simplu de administrat. Totusi, parolele pot fi descoperite de potentiali atacatori fie prin gasirea lor in locuri usor accesibile, prin observarea introducerii acestora, sau prin atacuri prin incercare "cu dictionarul". In general structura unei parole nu trebuie sa fie usor de descoperit, insa trebuie sa fie usor de retinut, de aceea ar trebui ca utilizatorii sa fie cei care o compun.

Bresele de securitate inerente acestui sistem sunt

- parolele introduse la momentul instalarii sistemului ("Default passwords")
- parole active ale persoanelor care nu mai acceseaza sistemul
- risc relativ mare la atacuri "cu dictionarul"
- decriptarea fisierelor care contin liste de parole
- intercepterea parolelor prin monitorizare trafic

Masuri de securitate care se pot lua:

- Lungime parola suficient de mare pentru a nu fi usor gasita
- Expirarea parolelor (de ex. la 30 de zile)
- Numar limitat de incercari de login (de obicei 3)
- Mentinere fisier log pentru accesarile de conectare
- Monitorizare interactiva a autentificarii

**Autentificarea criptografica**: cu ajutorul unui agoritm, un text simplu este transformat intr-o secventa cifrata care nu are o anumita seminficatie. Doar utilizatorii autorizati au metodele de a decfisfa datele la forma initiala.

Se folosesc in mod uzual doi algoritmi in autentificare:

- simetric (folosesc aceeasi cheie la criptare si la decriptare)
- asimetric (folosesc chei diferite pentru fiecare functie). Semnaturile digitale folosesc algoritmi asimetrici.

Pentru sisteme cu chei simetrice este necesar ca toate partile autorizate sa detina cheia, deci, pe langa taria algoritmului de secretizare, o mare influenta asupra securitatii o are modul de generare, transmitere si stocare al cheii. In mod curent se folosesc algoritmi cu chei de criptare mai mari de 64 biti. Autentificarea se poate face prin criptarea intregului text sau doar a unei sume de control.

Pentru sisteme cu chei asimetrice functiile de criptare/decriptare sunt diferite, dar matematic asemanatoare pentru ca aici cheile sunt diferite. Se dezvolta deci chei perechi, una pentru criptare, cealalta pentru decriptare. Acestea se pot deduce foarte greu una din cealalta daca s-ar incerca acest lucru de persoane neautorizate (timpul de calcul este foarte mare). Modul de lucru permite publicarea uneia dintre chei: "cheie publica" in timp ce a doua cheie este tinuta secreta. Autentificarea se realizeaza prin codarea unei sume de control folosind cheia secreta. Orice persoana poate decripta si verifica, folosind cheia publica, faptul ca autorul criptarii este cel care are cheia secreta.

Deoarece folosesc chei foare lungi (de ex. 1024 biti) acesti algoritmi sunt mai lenti decat cei cu chei simetrice.

**Codurile cu mesaj de autentificare**: se folosesc atunci cand exista un risc de modificare intentionata sau neintentionata. Acestea sunt o parte esentiala din procesul de semnatura digitala. Astfel, se genereaza o suma de control dependenta de continutul mesajului, care este atasata la sfarsit. La receptie se verifica daca din mesaj se obtine suma de control. Algoritmul trebuie sa fie eficient, pentru a nu produce atasamente foarte mari la mesajul initial si suficient de puternic pentru a nu permite deducerea mesajului initial din valoarea sa. In aceasta categorie se incadreaza codurile CRC-16 si CRC-32. Ele nu cripteaza mesajul foarte puternic, insa orice modificare in continutul mesajului se reflecta in modificarea CRC (cyclic redundancy checks). Alti algoritmi din aceasta categorie: MD2

si MD5 folositi in standardul internet pentru mail cu grad mare de securitate (Privacy Enhanced Mail). ANSI X9.9 e propus de American National Standards Institute pentru autentificarea mesajelor pentru institutiile financiare, folosind algoritm pe 32, 48 sau 64 de biti. In final Secure Hash Algorithm (SHA) e standardul in SUA pentru semnaturi digitale folosind valori algoritm pe 160 biti.

**Folosirea de servere de autentificare**: este metoda preferata atunci cand exista nevoia de autentificare de mesaje sau de utilizatori in sisteme distribuite. Aceste servere pot sa asigure diferite servicii de autentificare pentru utilizatori. Un exemplu de asemenea sistem este Kerberos authentication server (KAS) si Ticket-Granting Server (TGS). Odata ce utilizatorul este autentificat, KAS elibereaza un "bilet" care este valabil pe toata durata cat acesta este logat. Spre deosebire de aceasta metoda, TGS elibereaza asemenea "bilete" care expira dupa o anumita durata de timp.

**Jetoanele de securitate(security tokens)**: aceste dispozitive sunt conectate la dispozitive electronice si asigura autentificarea persoanei. Aceste dispozitive variaza, de la cele pasive, pana la cele active, portabile, care comunica direct cu sistemul care cere autentificarea (hand-held authentication devices: HHAD).
Procedeul este urmatorul:

a) utilizatorul initialzea procedura prin introducerea unei parole in sistem;
b) sistemul genereaza un numar de 6-8 cifre
c) utilizatorul introduce numarul dat de sistem in dispozitivul HHAD
d) numarul rezultat din HHAD este introdul la promptul sistemului
e) utilizatorul a fost autentificat

Alte dispozitive din aceasta categorie sunt smart-card-urile care incorporeaza microchipuri cu memorii flash, sau dongle-urile care se ataseaza la porturile calculatoarelor pentru a activa software-ul