UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale
2007-2013

Platformă de e-learning și curriculă e-content pentru învățământul superior tehnic

Proiectarea Rețelelor

35. Monitorizarea rețelei

Managementul reţelelor

Proiectarea Reţelelor

Cuprins

- Autentificare, Autorizare şi Accounting
- Descoperirea reţelei
  - CDP
  - NBAR
- Monitorizarea reţelei
  - SNMP
  - NETFLOW
  - SMOKEPING

Autentificare

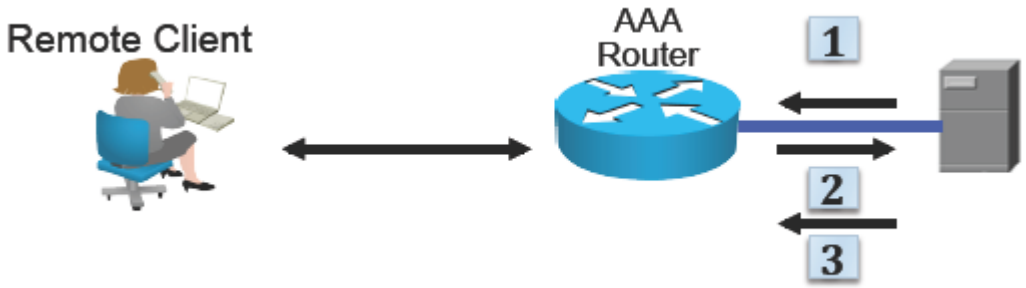
- Tipuri de autentificare
  - Password – only
  - Local – database
  - Server – database

TACACS+	RADIUS
Cisco server version	Open Standard
TCP	UDP
Urmăreşte arhitectura AAA	Combină autentificarea cu autorizarea

- Autentificarea se poate face pe bază de utilizator şi parolă sau folosind Kerberos 5

Autorizare

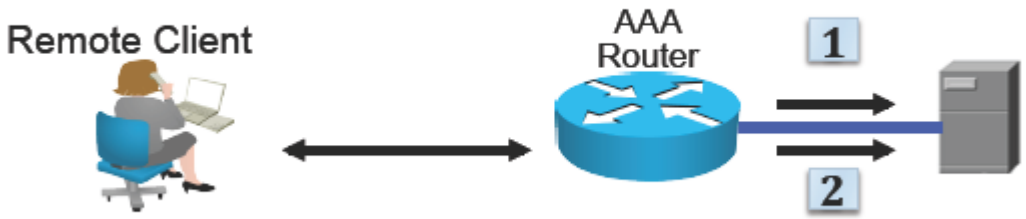
- Implementată de obicei folosind un server de AAA
- Utilizatorul primeşte un set de atribute ce descrie nivelul său de acces în reţea



  - Utilizatorul trimite o comandă către ruter
  - Ruterul întreabă serverul dacă utilizatorul are dreptul să execute această comandă
  - Serverul răspunde cu DA/NU

Accounting

- Implementare folosind un server de AAA
- Menţine evidenţa activităţilor individuale
- După autentificarea utilizatorului toate activităţile acestuia in reţea sunt salvate
- Foarte important pentru securitatea reţelei, dar şi pentru rapoarte despre activitatea utilizatorilor



Cisco Discovery Protocol

- protocol de nivel 2 proprietar Cisco
- folosit între două echipamente vecine pentru a anunţa informaţii referitoare la:
  - platformă
  - sistemul de operare
  - adresa IP
  - interfeţele direct conectate

```
R8# show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater

Device ID        Local Intrfce     Holdtme    Capability  Platform  Port ID
S1               Fas 0/0            163          S I      WS-C2960- Fas 0/4
R7               Ser 0/2/1          131        R S I      2801      Ser 0/2/1
```

NBAR

- Network Based Application Recognition
  - Recunoaşte un număr mare de protocoale şi poate fi extins prin folosirea de module (PDLM – Packet Description Language Modules)

- NBAR – protocol-discovery permite recunoaşterea protocoalelor pentru o anumită interfaţă

- Folosirea lui poate duce la o utilizare excesivă a procesorului şi a memoriei ruterului

NBAR

- configurarea pe interfaţă

```
Aegis#config t
     Aegis(config)#interface FastEthernet0/0
     Aegis(config-if)#ip nbar protocol-discovery
```

- verificarea protocoalelor ce rulează

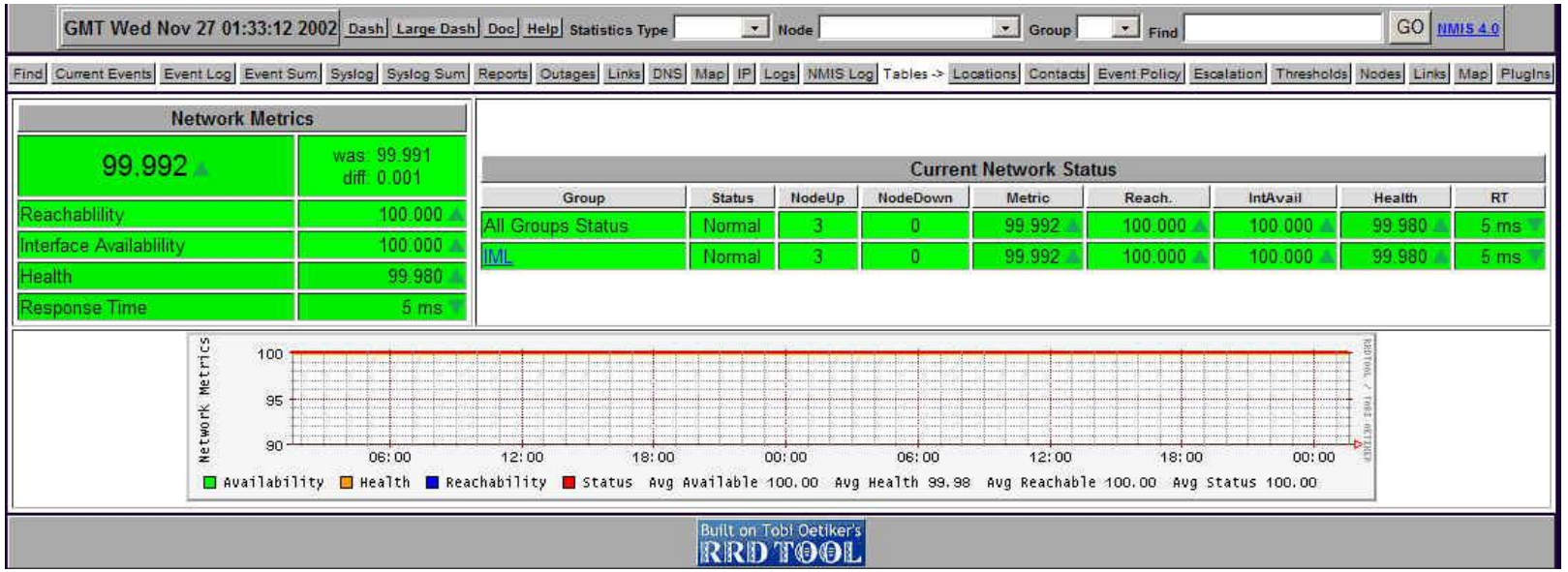
```
     Aegis#sh ip nbar protocol-discovery
     FastEthernet0/0    Input                  Output
     Protocol         Packet Count           Packet Count
                      Byte Count             Byte Count
                           5min Bit Rate (bps)      5min Bit Rate (bps)
                      5min Max Bit Rate (bps)  5min Max Bit Rate (bps)
      ------------------------ ------------------------ ------------
          ftp                617                      606
                             792480                   34749
                             34000                    1000
                             34000                    1000
          ospf               78                       78
                             7356                     7376
                             0                        0
                             0                        0
          Total              3898                     4113
               3045939                488008
                         59000                  1000
                      78000                  16000
```

SNMP

- Simple Network Management Protocol
- Protocol de Nivel Aplicaţie folosit pentru schimbarea de informaţii într-o reţea
- Componentele unei reţele ce foloseşte SNMP
  - Dispozitivul de monitorizat
  - Un software denumit agent instalat pe acest dispozitiv
  - O aplicaţie de monitorizare ce primeşte informaţii de la aceste dispozitive
- Prin SNMP se pot primi informaţii de la echipamente, existând şi posibilitatea de trimitere de comenzi

NMIS

- Network Management Information System
- Oferă informaţii despre disponibilitatea şi încărcarea echipamentelor din reţea
- Foloseşte SNMP pentru colectarea datelor

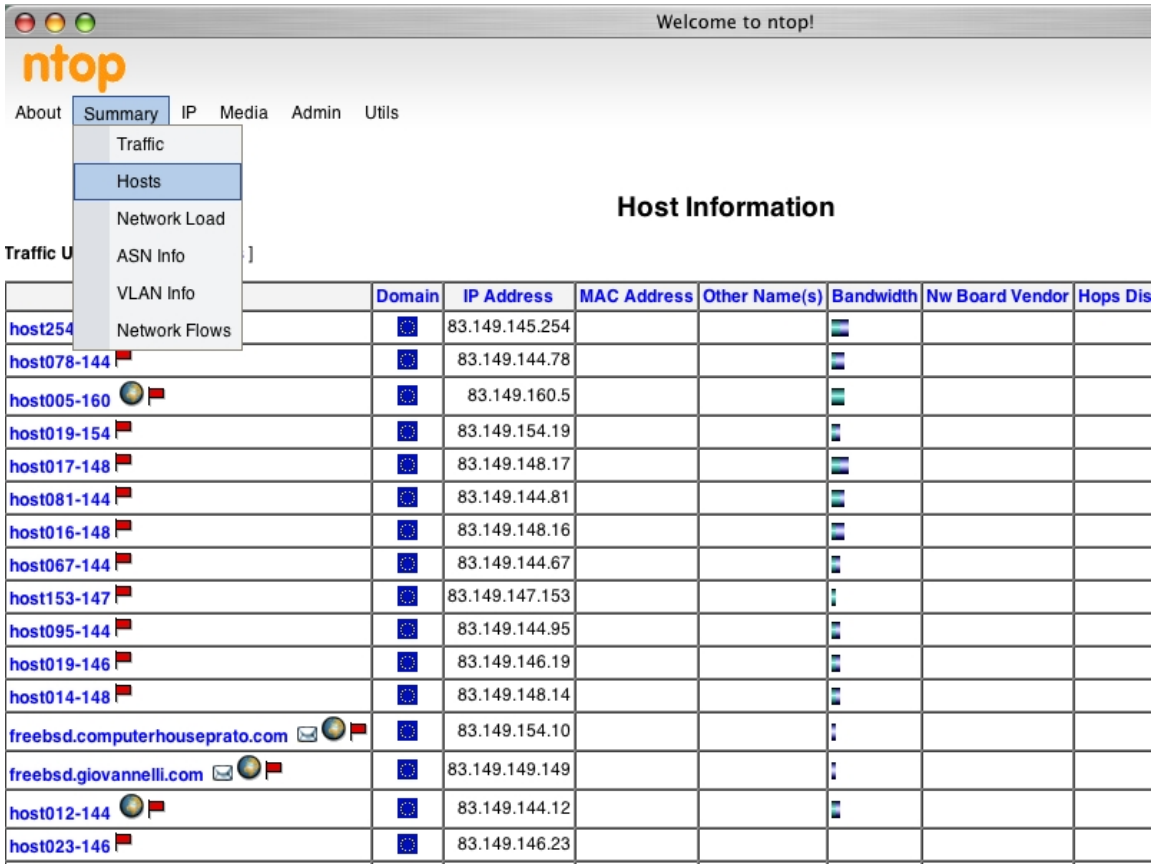


Netflow

- Protocol implementat de Cisco pentru colectarea informaţiilor despre trafic
- Arhitectura se bazează pe colectarea datelor de către un sistem separat, folosirea ruterului poate duce la suprasolicitarea acestuia
- Foloseşte mesaje sumarizate pentru transmiterea de informaţii referitoare la un anumit tip de trafic
- IPFIX este dezvoltat de IETF pentru îmbunătăţirea şi standardizarea protocolului

Ntop

- Este o unealtă de monitorizare a traficului prin protocolul Netflow/IPFIX
- Poate identifica
  - tipurile de trafic
  - dispozitivele
  - lăţimea de bandă



Smokeping

- Folosit pentru monitorizarea latenţei în reţea
- Trimite pachete de ping către staţiile configurate, implicit 20 de pachete la fiecare 300 de secunde
- Pe baza răspunsurilor primite poate genera grafice cu disponibilitatea echipamentelor sau a reţelei