



3.1 Funcția pe care echipamentul trebuie să le îndeplinească în rețeaua RNTD-SNR este de Switch de acces layer 2,3,4;

3.2. Arhitectura echipamentului și sistemul de operare trebuie să respecte:

- a) Arhitectura complet non-blocking pentru matricea de switching;
- b) Switch-ul trebuie să fie modular și să asigure minim următoarele interfețe:
  - b.1) 2 interfețe 10GE de WAN
  - b.2) 48 de interfețe 1GE de acces, lucrând simultan în full-rate;
- c) Capacitatea de switching minim de 120 Gbps

3.3 Echipamentul trebuie să suporte fără restricții de orice natură proprietatea și caracteristici Layer 2:

- a) Layer 2 hardware forwarding la minimum 100 mpps
- b) Layer 2 switch ports and VLAN trunks
- c) IEEE 802.1Q VLAN encapsulation
- d) Inter-Switch Link (ISL) VLAN encapsulation
- e) Dynamic Trunking Protocol (DTP)
- f) VLAN Trunking Protocol (VTP) și VTP domains
- g) 4096 VLAN
- h) PVST și PVST+
- i) Spanning Tree PortFast și PortFast Guard
- j) Spanning Tree UplinkFast și BackboneFast
- k) IEEE 802.1s
- l) IEEE 802.1w
- m) IEEE 802.3ad
- n) IGMPv1, v2, and v3 snooping
- o) Link Aggregation Control Protocol (LACP)
- p) IEEE 802.1 QinQ în hardware
- q) Multilayer jumbo frames (pană la 9216 bytes)
- r) Layer 2 protocol tunneling
- s) Class-of-service (CoS) mutation
- t) E-OAM 802.3ah și CFM: 802.1ag

3.4 Echipamentul trebuie să suporte fără restricții de orice natură proprietăți și caracteristici Layer 3:

- a) Frame-uri Jumbo pe toate porturile (up to 9216 bytes)
- b) Protocole de routing: OSPF, RIP, and RIP2
- c) BGP4 și Multicast Border Gateway Protocol (MBGP)
- d) Hot Standby Router Protocol (HSRP)
- e) IS-IS routing protocol
- f) IGMPv1, v2, and v3
- g) IP Multicast routing protocols: PIM, SSM, and Distance Vector Multicast Routing Protocol (DVMRP)
- h) IPv6
- i) OSPF fast convergence



*Ley*

*Stefan*



j) Protecție OSPF și ISIS

3.5 Echipamentul trebuie să suporte mecanisme QoS:

- a) QoS configurabil per port și VLAN
- b) Prioritizarea cozilor
- c) IP DSCP (differentiated services code point)
- d) Clasificare și marcare în funcție de IP ToS sau DSCP

3.6 Echipamentul ofertat trebuie să respecte următoarele condiții referitoare la redundanta și fiabilitatea sistemului:

- a) Toate componentele critice: Power supply și Fan-uri trebuie să fie redundante și funcționabile în configurație hot-stand-by;
- b) Graceful restart;
- c) Module de uplink OIR(Online Insertion and Removal).

3.7 Echipamentul/architectura rețelei ofertat trebuie să suporte capabilități referitoare la securitate:

- a) Acces pe mai multe nivele de competență în funcție de ID și parola;
- b) TACACS+ și RADIUS
- c) ACL-uri pentru toate porturile
- d) IEEE 802.1x autentificarea userului, private VLAN assignment

3.8 OFERTANTUL trebuie să ofere informațiile detaliate referitoare la următorii parametrii de performanță a echipamentului, în configurația oferită:

- a) Rata de forward pentru pachete IPv4 sau Ipv6 pe fiecare linie
- b) Numărul maxim de adrese MAC pentru aplicații UNICAST și MULTICAST
- c) Numărul de intrări în tabela de routare
- d) Numărul de VLAN-uri active
- e) Capacitatea maximă de banda agregată.

3.9 Electroalimentare

- a) Echipamentele instalate în PoP-urile SNR se vor alimenta de la tensiunea -48 Vdc;
- b) Echipamentele trebuie să aibă 2 intrări distincte pentru sursele de alimentare.
- c) Se va specifica consumul maxim al echipamentului în configurația oferită/ și pentru fiecare card/modul în parte;
- d) Se va specifica căldura dissipată pentru echipamentul în configurația oferită/ și pentru fiecare card/modul în parte
- e) Cablurile furnizate pentru alimentarea echipamentelor trebuie să aibă secțiunea corespunzătoare pentru a asigura în limite normale consumul maxim al acestora, ținând cont de consumul maxim al echipamentului complet echipat. Conductorii vor avea izolația în culori distincte.



### 3.10 Condiții de mediu

- a) Echipamentul oferit trebuie să fie capabil să funcționeze fără întreruperi, menținându-și caracteristicile tehnice în următoarele condiții ambientale: temperatură minima/maxima 0°C / 35°C, umiditate cel puțin de 70%.
- b) Echipamentul trebuie să fie capabil să-si asigure recircularea aerului în interiorul șasiului;
- c) Zgomotul produs de echipament trebuie să fie de minim 72dBA;
- d) Echipamentul trebuie să fie compatibil cu standardele și cerințele EMC UE și FCC.

### II.2.4 PLATFORMA DE MANAGEMENT CENTRALIZAT – NMS IP

#### 4.1 Cerințe funcționale

- a) NMS IP trebuie să asigure management distant în timp real pentru toate echipamentele de date care fac parte din soluția oferită;
- b) Operare și administrare la distanță fără restricții;
- c) NMS scalabil pentru o eventuală extensie a numărului de echipamente ce vor fi administrate și monitorizate;
- d) FURNIZORUL va include în oferta de NMS IP platforma hardware pe care va rula soft-ul de management;
- e) Platforma hardware NMS IP va fi dimensionată din punct de vedere al resurselor astfel încât să poată manager-ia toate elementele rețelei și un plus de 50% de elemente de rețea fără alte costuri suplimentare.
- f) NMS trebuie să ruleze pe o platformă hardware cu sursa de alimentare redundantă și posibilitatea de harddisk mirroring pentru baza de date pe o alta platformă hardware;
- g) NMS trebuie să fie capabil să utilizeze mai multe rute pentru management de la serverul NMS central către elementele de rețea monitorizate;
- h) NMS trebuie să ofere Graphic Interface User în Windows style (Menus, Pointer, Icons);
- i) Evenimente ca: boot-are, restartare NMS nu trebuie să afecteze funcționarea normală a rețelei de date IP
- j) să monitorizeze și echipamentele existente în rețea în acest moment.
- k) Sa emuleze o reprezentare virtuală a echipamentelor monitorizate, astfel incat acestea să nu fie interogate excesiv
- l) NMS IP oferit va fi capabil să îndeplinească funcțiile de:

- I.1) Configuration management
- I.2) Topology management
- I.3) Fault și Maintenance management
- I.4) Performance management
- I.5) Security management
- I.6) Modul de Help/Asistenta
- I.7) Log Management

m) Caracteristici pentru funcția Performance Management



m.1) NMS trebuie să genereze rapoarte cu parametrii de performanță ai elementelor de rețea în timp real sau pe o perioadă predefinită pentru fiecare interfață de 1xGb/10xGb;

m.2) Parametrii de performanță ai elementelor de rețea după care se fac analizele trebuie să fie selectabili;

n) Caracteristici pentru funcția Log Management

n.1) NMS trebuie să genereze log-uri cu alarme, performante în format electronic și printabile.

o) Caracteristici pentru funcția Topology Management

o.1) Trebuie să furnizeze harta cu topologia logică a rețelei, cu indicarea sub forma de icoane a nodurilor de rețea și a interconexiunilor între nodurile de rețea și cu alte elemente de rețea.

o.2) Rapoarte configurate pe web

o.3) Export rapoarte și în urmatoarele formate: pdf, excel, rtf (sau word)

o.4) Distribuția rapoartelor (nu doar a alertelor) pe email

o.5) Integrare cu AD / LDAP pentru modulele Client și Web Unitel

o.6) Integrare cu Mind pentru preluarea automata a facturilor detaliate din sistemul de billing intern Radiocom

o.7) Să suporte și caracterele specifice limbii române (diacritice) în toate modulele suitei

o.8) Mantenanță soluție pentru anul 2009

o.9) Suport tehnic telefonic și pe email cu timp de răspuns 8x5 / 4 ore de la semnalarea incidentului

o.10) Acces la versiunile noi ale sistemului pentru anul iulie 2009 / iulie 2010

o.11) Verificare contracte cu facturi (se verifică valorile din analiza cu cele din monitorizare pe apelurile din analiza).

o.12). Impartirea abonamentelor globale (trafic de date și voce) pe structura organizațională a firmei

o.13) Rapoarte integrate cu costuri pentru voce și date pentru elementele organizaționale comune

## 4.2 Securitatea platformei de management

4.2.1 Platforma de management trebuie să ofere un sistem de securitate virtualizată care să permită crearea a mai multor sisteme de securitate virtuală pe un singur echipament, pentru a reduce costurile și a consolida infrastructura hardware.

4.2.2 Sistemul trebuie să ofere servicii integrate de Firewall, VPN, URL filtering și Intrusion Prevention către multiple rețele.

4.2.3 Toate sistemele virtuale trebuie să fie gestionabile de o platformă centralizată de management.

### 4.2.4 Specificații minime:





4.2.4.1 Numar de sisteme virtuale : minim 10

4.2.4.2 Numar de sisteme virtuale suportate maxim pe un sistem: minim 150

4.2.5 Performanta:

4.2.5.1 Firewall throughput: min 27 Gbps

4.2.5.2 VPN throughput: min. 7 Gbps

4.2.5.3 Sesiuni concurente: 1.8 milioane

4.2.6 Interfete:

4.2.6.1 Built-in: 28 GbE cupru

4.2.6.2 Optional: LOM, 2x2x4 1 GbE Fiber, sau 2x2x4 1GbE Copper, sau 2x2x2 10 GbE

4.2.7. Dimensiuni: max. 4u

4.2.8. Sursa de alimentare: Duala, hot-swappable

4.2.9 Consum: max. 500W

4.2.10 Firewall:

4.2.10.1 Suport Protocole/Aplicatii: min. 200 de aplicatii si protocole

4.2.10.2 Protectie VoIP: SIP, H.323, MGCP, si SIP cu suport NAT

4.2.10.3 Control Instant Messaging: MSN, Yahoo, ICQ, Skype (inclusiv peste HTTP si SSL)

4.2.10.4 Blocare aplicatii Peer-to-peer: Kazaa, GNUTella, BitTorrent, eMule, IRC (inclusive peste HTTP)

4.2.11 NAT: Static/hide NAT suport cu reguli manuale si automate

4.2.12 Filtrare URL:

4.2.13 Acces Internet securizat: activate per system virtual

4.2.14 Monitorizare: activare optionala

4.2.15 Lista White/Black: Control acces catre site-uri specifice definite de utilizatori

4.2.16 Suport de criptare: AES 128-256 bit, 3DES 56-168 bit

4.2.17 Metode de autentificare: Password, RADIUS, TACACS, X.509, SecurID

4.2.18 Autoritate de certificare: X.509 integrata

4.2.19 Suport topologie: star si mesh

4.2.20 Acces la distanta bazat pe SSL

4.2.21 Scanarea endpoint pentru complianta/malware inainte de admiterea in retea

4.3 Prevenirea Intruziunilor:

4.3.1 Protectie la nivel layer de retea: trebuie sa blocheze atacuri de tip DoS, Scanarea porturilor, sau de tip IP/ICMP/TCP

4.3.2 Protectie la nivel layer de aplicatie: trebuie sa blocheze atacuri de tip DNS cache poisoning, FTP bounce

4.3.3 Metode de detectare: bazate pe semnaturi sau anomalii de prorocol

4.4 Networking:

4.4.1 Virtualizare: virtualizare completa pentru toate componentele de retea, cum ar fi routere si switch-uri virtuale

