Okruženje za implementaciju NMS alata

Sa stanovišta menadžmenta ra?unarske mreže postoje potrebe za definisanjem preporuka za arhitekturu odnosno topologiju same mreže, kao i na?ina implementacije NMS (Network Management System) u realnim okruženjima. Pod pojmom menadžment mreže ovde podrazumevamo protokole koji se koriste za pristup ure?ajima radi konfigurisanja, održavanja, nadgledanja i sl, me?u kojima su najkoriš?eniji telnet, ssh, remote desktop protocol (RDP), SNMP.

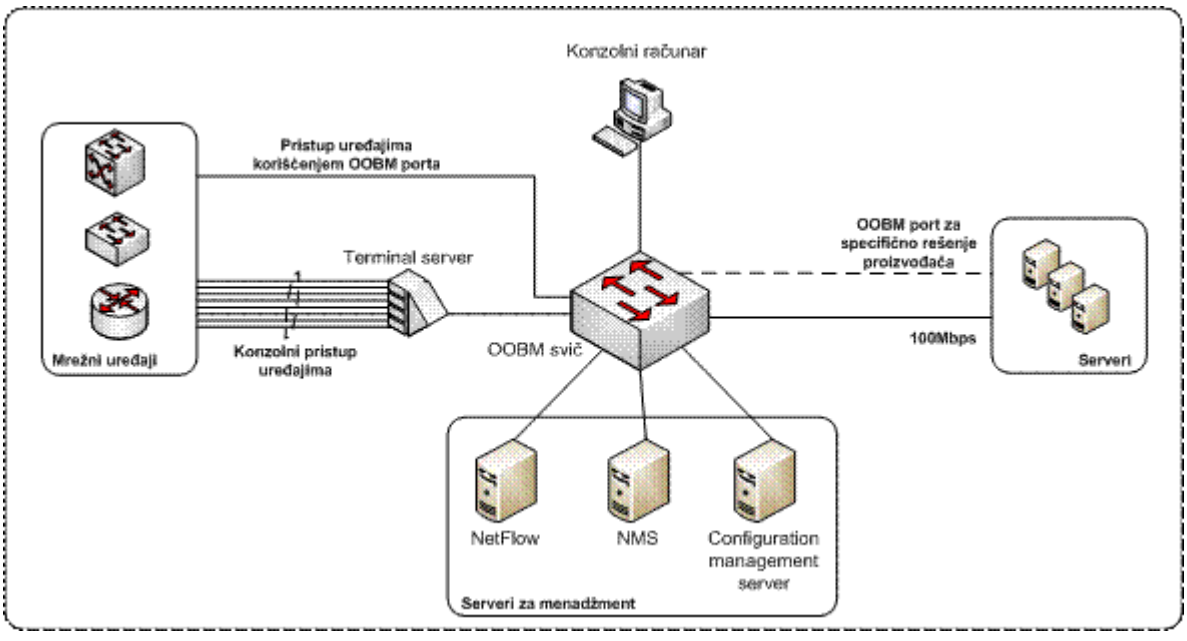
Preporuke treba da prikažu „idealna“ okruženja (za slu?aj da takvih mogu?nosti ima), i što je bitnije, da ukažu na realna okruženja i razli?ite topologije samih mreža, kao i mogu?nosti implementacije NMS-a u takvim okruženjima.

1. Out-of-band management

Out-of-band menadžment (OOBM) predstavlja koncept razdvajanja menadžmenta ure?aja (servera, mrežnih ure?aja, ups-eva itd.) od produkcionog saobra?aja (data traffic). Cilj ovog koncepta jeste bezbedan pristup ure?ajima u svrhu njihovog nadgledanja i održavanja.
Opšte definicije OOBM nalažu postojanje kompletno izdvojene fizi?ke infrastrukture, što uklju?uje:

• izdvojenu ra?unarsku mrežu (mrežne ure?aje);
• linkove (kablove izme?u ure?aja nad kojima se vrši menadžment i samih OOBM mrežnih ure?aja);
• menadžment interfejse na svim ure?ajima (fizi?ki odvojeni interfejsi od interfejsa koji se koriste za produkcioni saobra?aj);
• Konzolni ra?unar(i) (ra?unar koji se nalazi u OOBM-u i koji se koristi za pristup ure?ajima kroz sam OOBM)

Na slici 1, prikazana je opšta topologija OOBM-a. U „centru“ topologije se nalaze mrežni ure?aji na koje su povezani svi ure?aji nad kojima se predvi?a OOBM. OOBM pristup ure?ajima se može obavljati na razli?ite na?ine opisane u poglavljima 1.1 i 1.2.



\

1.1 OOBM servera

Za OOBM pristup serverima mogu se koristiti dva koncepta:

• OOBM pristup koriš?enjem specijalizovanog intefejsa za ovu namenu (HP iLO, Dell DRAC);
• OOBM pristup koriš?enjem jednog od mrežnih interfejsa

U konceptu koriš?enja specijalizovanog interfejsa za OOBM, podrazumeva se koriš?enje i specijalizovanog softvera svakog od proizvo?a?a (da li Dell DRAC zahteva specijalizovani softver?). Uobi?ajeno je da pristupom ovim portovima mogu da se obavljaju menadžment funkcije poput telnet, ssh, RDP, VNC i drugih pristupa. ## dodatno izanalizirati

U slu?aju koriš?enja jednog od mrežnih interfejsa, podrazumeva se da taj interfejs ne sme biti istovremeno koriš?en za drugu namenu (pored OOBM-a). Ovaj metod omogu?ava nivo pristupa ure?ajima identi?an nivou pristupa koriš?enjem In-band menadžmenta, sa tim da postavlja zahteve za dodatnim mrežnim intefejsom na serverima. ##Koje su preporuke po pitanju broja intefejsa?

1.2 OOBM mrežnih ure?aja

U zavisnosti od proizvo?a?a mrežnih ure?aja, za OOBM se mogu koristiti slede?i interfejsi:

• Konzolni port
• Specijalizovan OOBM port
• AUX port

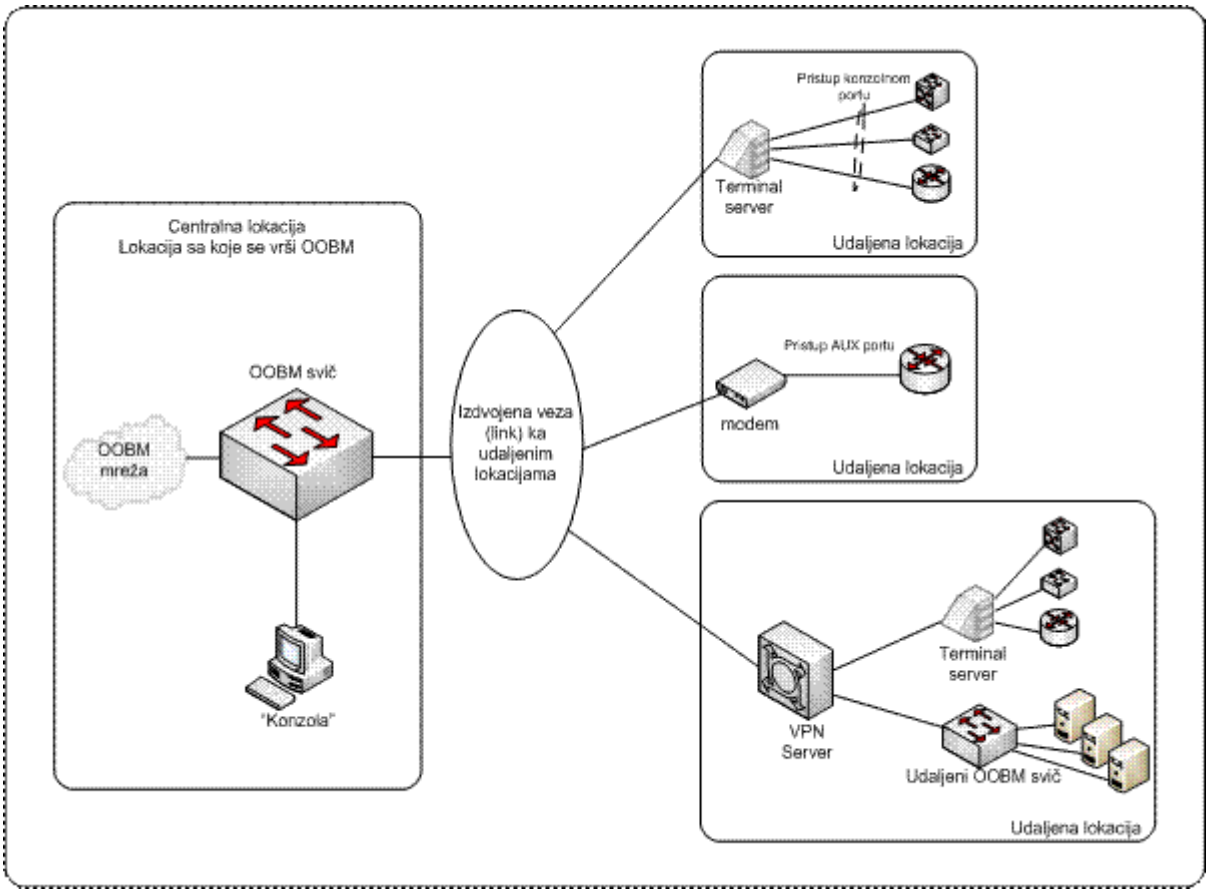
Konzolni port je za razliku od specijalizovanog OOBM porta i AUX porta, zastupljen kod mrežnih ure?aja najve?eg broja proizvo?a?a, zbog ?ega se ovaj na?in pristupa preporu?uje ukoliko se teži uniformnom rešenju. Ovo rešenje podrazumeva i koriš?enje terminal servera za pristup samom portu. Ure?aji koji imaju OOBM port omogu?avaju pristup po IP adresi (layer 3).
AUX port omogu?ava koriš?enje modemske veze (dial-in) za direktan pristup ure?ajima.
##ovde treba jos objasnjenja

1.3 OOBM ure?aja na udaljenim lokacijama

Kako „po definiciji“ OOBM podrazumeva koriš?enje nezavisnih linkova i ure?aja, u situacijama kada je potrebno vršiti OOBM ure?aja na udaljenim lokacijama potrebno je:

• Na lokaciji sa koje se vrši OOBM, obezbediti ure?aje za zasebnu vezu ka udaljenim lokacijama (npr. modemi za dial-up pristup);
• Zasebne (nezavisne od produkcionog saobra?aja) WAN linkove ka svim udaljenim lokacijama;
• Ure?aje na udaljenim lokacijama koji imaju OOBM vezu ka portovima ure?aja (navedenim u poglavlju 2). Ovi ure?aji su modemi (pristup AUX portu), terminal serveri (pristup konzolnom portu), vpn serveri (OOBM port za IP pristup) i sl.

Na slici 2, prikazani dati su primeri povezivanja udaljenih ure?aja u OOBM mrežu.



Slika 2.

2. Not-so-OOBM

U okruženjima u kojima nije mogu?e implementirati OOBM u potpunosti preporuka je da se koriste raspoložive tehnike i koncepti a koji uklju?uju:

Za pristup ure?ajima radi menadžmenta (telnet, ssh, RDP…)

• Koriš?enje logi?ke segmentacije mreže (VLAN-ovi), pri ?emu bi se koristio zaseban VLAN za menadžment;
• Koriš?enje NAT-a za pristup ure?ajima do kojih nije mogu?e pri?i direktno iz OOBM ili kroz izdvojeni VLAN.

Pristup menadžment servera ure?ajima radi nadgledanja, prenosa konfiguracija i sl.
• Koriš?enje dodatnog mrežnog interfejsa za pristup ure?ajima u VLAN-u za menadžment;
• Koriš?enje dodatnog mrežnog interfejsa za pristup ure?ajima do kojih nije mogu?e pri?i direktno kroz OOBM ili izdvojeni VLAN. Ovaj interfejs može imati javnu IP adresu (ovo može biti i interfejs koji služi za web pristup).

##VLAN1 za menadzment uredjaja, VLAN A za menadzment servera kroz nase uredjaje. ##VLAN na serverima?!?!!?

3. Implementacija NMS-a

Pri implementaciji NMS-a potrebno je razmotriti komunikaciju izme?u NMS server i ure?aja koji nad kojim se vrše “funkcije menadžmenta”. Razlikujemo slu?ajeve u kojima se komunikacija obavlja kroz OOBM i kada komunikacija mora da se obavlja i van okvira izdvojene mreže za menadžment.

3.1 OOBM okruženje

Komunikacija NMS-a sa ure?ajima koja se obavlja kroz OOBM podrazumeva bezbednu komunikaciju izme?u interfejsa NMS servera koji se nalazi u OOBM-u i interfejsa ure?aja koji su tako?e u OOBM-u. Sa aspekta servera, ovo podrazumeva komunikaciju NMS – interfejs servera namenjen isklju?ivo za menadžment.
Sa aspekta mrežnih ure?aja, potrebno je obezbediti Layer 3 vezu što dovodi do toga da je:
• kod rutera potrebno obezbediti dodatni xEthernet interfejs (teško za o?ekivati)
• kod L2/L3 svi?eva je potrebno da se odre?eni xEthernet port postavi u VLAN namenjen za menadžment i isti poveže u OOBM mrežu.

3.2 Not-so-OOBM okruženje

Komunikacija izme?u NMS-a sa ure?ajima koji su van OOBM-a, možemo svrstati u dve grupe:
• Ure?aji koji nemaju interfejs u OOBM-u, ali imaju intefejs koji se nalazi u menadžement VLAN-u
• Ure?aji koji nemaju interfejs u OOBM-u ni u menadžment VLAN-u, ve? se do pristupa ure?ajima mora komunicirati rutiranjem (Layer 3)

Menadžment VLAN

U slu?ajevima Layer 2 WAN mreže, kada postoji menadžment VLAN, potrebno je obezbediti komunikaciju NMS-a sa ure?ajima u tom VLAN-u. Ovo se može obaviti na dva na?ina:
• Dodatni intefejsi NMS servera koji su direktno povezani u menadžment VLAN (i imaju IP adresu iz tog VLAN-a). Ovo rešenje zahteva da NMS server ima najmanje 3 fizi?ka interfejsa.
• Koriš?enjem intefejsa NMS-a koji se nalazi o OOBM delu mreže i funkcijom stati?kog NAT-a (zbog potreba komunikacije od ure?aja ka NMS-u, na primer SNMP trap).

Layer 3 baziran menadžment

Ovo se odnosi na mrežne ure?aje i može se svrstati u grupu „specijalnih slu?ajeva“, obzirom da se ne o?ekuje da se mrežna topologija pravi tako da se ure?aja mora do?i kroz layer 3, odnosno rutiranjem. Ovakav scenario se javlja u situacijama kada je potrebno da se vrši menadžment nad ure?ajem koji se nalazi „iza“ ure?aja druge institucije (nad kojim nemamo ingerencije).
Ovde opet imamo dva scenarija:
• NMS komunicira sa ure?ajem preko stati?kog NAT-a (interfejsom koji se nalazi u OOBM-u)
• NMS komunicira sa ure?ajem preko interfejsa koji je ujedno interfejs za web pristup samom NMS-u.

4. Mendžment sa udaljenih lokacija

From:
http://www.bpd.amres.ac.rs/ - **AMRES wiki**

Permanent link:
http://www.bpd.amres.ac.rs/doku.php?id=glava_1

Last update: **2009/09/30 22:03**