

Okruženje za implementaciju NMS alata

Sa stanovišta menadžmenta računarske 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.

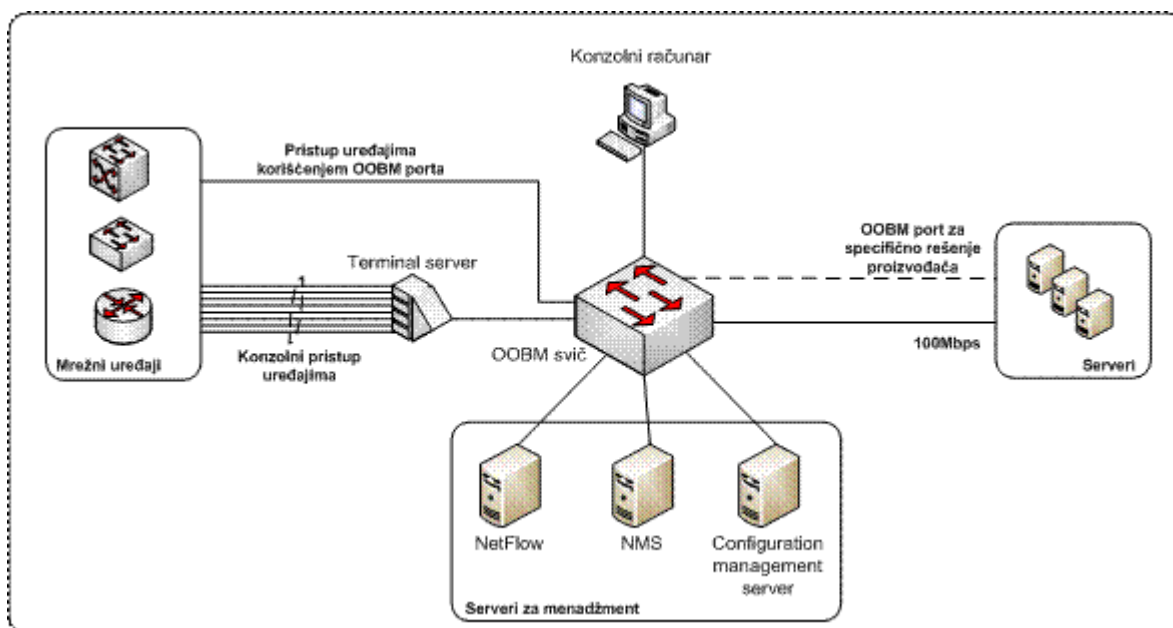
1. Out-of-band management

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 računarsku mrežu (mrežne ure?aje);
- linkove (kablove izme?u ure?aja nad kojima se vrši menadžment i samih OOBM mrežnih ure?aja);
- menadžment interfejsa na svim ure?ajima (fizi?ki odvojeni interfejsi od interfejsa koji se koriste za produkcionu saobra?aj);
- Konzolni račun(i) (računar 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 korišćenjem specijalizovanog interfejsa za ovu namenu (HP iLO, Dell DRAC);
- OOBM pristup korišćenjem jednog od mrežnih interfejsa

U konceptu korišćenja specijalizovanog interfejsa za OOBM, podrazumeva se korišćenje i specijalizovanog softvera svakog od proizvođača (da li Dell DRAC zahteva specijalizovani softver?). Uobičajeno je da pristupom ovim portovima mogu da se obavljaju menadžment funkcije poput telnet, ssh, RDP, VNC i drugih pristupa. ## dodatno izanalizirati

U slučaju korišćenja jednog od mrežnih interfejsa, podrazumeva se da taj interfejs ne sme biti istovremeno korišćen za drugu namenu (pored OOBM-a). Ovaj metod omogućava nivo pristupa uređajima identičan nivou pristupa korišćenjem In-band menadžmenta, sa tim da postavlja zahteve za dodatnim mrežnim interfejsom na serverima. ## Koje su preporuke po pitanju broja interfejsa?

1.2 OOBM mrežnih uređaja

U zavisnosti od proizvođača mrežnih uređaja, za OOBM se mogu koristiti sledeći interfejsi:

- Konzolni port
- Specijalizovan OOBM port
- AUX port

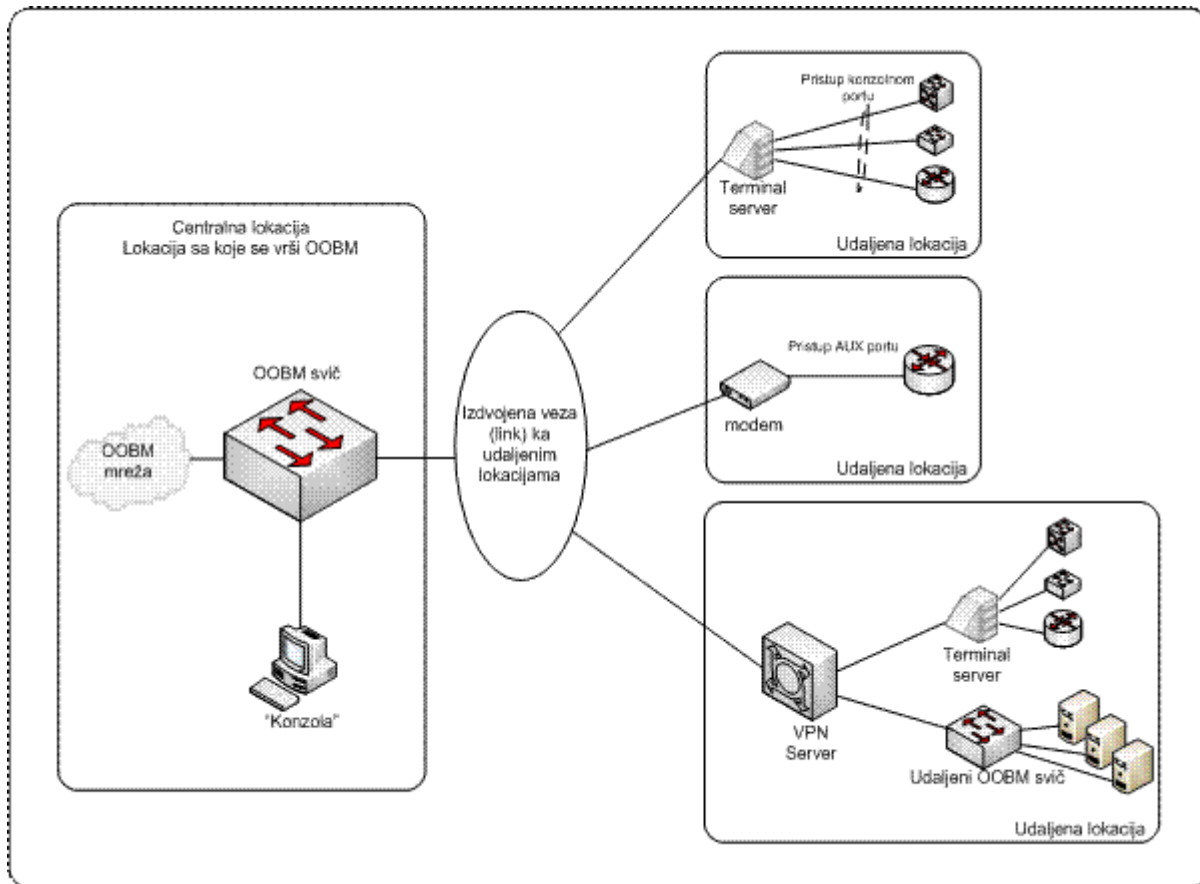
Konzolni port je za razliku od specijalizovanog OOBM porta i AUX porta, zastupljen kod mrežnih uređaja najvećeg broja proizvođača, zbog čega se ovaj način pristupa preporučuje ukoliko se teži uniformnom rešenju. Ovo rešenje podrazumeva i korišćenje terminal servera za pristup samom portu. Uređaji koji imaju OOBM port omogućavaju pristup po IP adresi (layer 3). AUX port omogućava korišćenje modemske veze (dial-in) za direktan pristup uređajima. ## ovde treba još objasnjenja

1.3 OOBM uređaja na udaljenim lokacijama

Kako „po definiciji“ OOBM podrazumeva korišćenje nezavisnih linkova i uređaja, u situacijama kada je potrebno vršiti OOBM uređaja na udaljenim lokacijama potrebno je:

- Na lokaciji sa koje se vrši OOBM, obezbediti uređaje za zasebnu vezu ka udaljenim lokacijama (npr. modemi za dial-up pristup);
- Zasebne (nezavisne od produkcionog saobraćaja) WAN linkove ka svim udaljenim lokacijama;
- Uređaje na udaljenim lokacijama koji imaju OOBM vezu ka portovima uređaja (navedenim u poglavlju 2). Ovi uređaji 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 uređaja u OOBM mrežu.



Slika 2.

2. Not-so-OOBM

U okruženjima u kojima nije moguće implementirati OOBM u potpunosti preporuka je da se koriste raspoložive tehnike i koncepti a koji uključuju:

Za pristup uređajima radi nadziranja (telnet, ssh, RDP...)

- Korišćenje logičke segmentacije mreže (VLAN-ovi), pri čemu bi se koristio zaseban VLAN za nadziranje;
- Korišćenje NAT-a za pristup uređajima do kojih nije moguće pristupiti direktno iz OOBM ili kroz izdvojeni VLAN.

Pristup nadziranja servera uređajima radi nadgledanja, prenosa konfiguracija i sl.

- Korišćenje dodatnog mrežnog interfejsa za pristup uređajima u VLAN-u za nadziranje;
- Korišćenje dodatnog mrežnog interfejsa za pristup uređajima do kojih nije moguće pristupiti 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 nadziranje uređaja, VLAN A za nadziranje servera kroz naše uređaje. ##VLAN na serverima?!!!!?

3. Implementacija NMS-a

Pri implementaciji NMS-a potrebno je razmotriti komunikaciju između NMS server i uređaja koji nad kojim se vrše "funkcije menadžmenta". Razlikujemo slučajeve 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 uređajima koja se obavlja kroz OOBM podrazumeva bezbednu komunikaciju između interfejsa NMS servera koji se nalazi u OOBM-u i interfejsa uređaja koji su takođe u OOBM-u. Sa aspekta servera, ovo podrazumeva komunikaciju NMS - interfejs servera namenjen isključivo za menadžment.

Sa aspekta mrežnih uređaja, potrebno je obezbediti Layer 3 vezu što dovodi do toga da je:

- kod rutera potrebno obezbediti dodatni xEthernet interfejs (teško za otkrivati)
- kod L2/L3 sviđeva je potrebno da se određeni xEthernet port postavi u VLAN namenjen za menadžment i isti poveže u OOBM mrežu.

3.2 Not-so-OOBM okruženje

Komunikacija između NMS-a sa uređajima koji su van OOBM-a, možemo svrstati u dve grupe:

- Uređaji koji nemaju interfejs u OOBM-u, ali imaju interfejs koji se nalazi u menadžment VLAN-u
- Uređaji koji nemaju interfejs u OOBM-u ni u menadžment VLAN-u, već se do pristupa uređajima mora komunicirati rutiranjem (Layer 3)

Menadžment VLAN

U slučajevima Layer 2 WAN mreže, kada postoji menadžment VLAN, potrebno je obezbediti komunikaciju NMS-a sa uređajima u tom VLAN-u. Ovo se može obaviti na dva načina:

- Dodatni interfejsi 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 fizička interfejsa.
- Korišćenjem interfejsa NMS-a koji se nalazi u OOBM delu mreže i funkcijom statičkog NAT-a (zbog potreba komunikacije od uređaja ka NMS-u, na primer SNMP trap).

Layer 3 baziran menadžment

Ovo se odnosi na mrežne uređaje i može se svrstati u grupu „specijalnih slučajeva“, obzirom da se ne očekuje da se mrežna topologija pravi tako da se uređaja mora doći kroz layer 3, odnosno rutiranjem. Ovakav scenario se javlja u situacijama kada je potrebno da se vrši menadžment nad uređajem koji se nalazi „iza“ uređaja druge institucije (nad kojim nemamo ingerencije).

Ovde opet imamo dva scenarija:

- NMS komunicira sa uređajem preko statičkog NAT-a (interfejsom koji se nalazi u OOBM-u)
- NMS komunicira sa uređajem 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**