## *5. Plan de reţea*

Un cloud hibrid combină modelele de servicii şi de implementare. Dacă se foloseşte un cloud privat, atât furnizorul de servicii cât şi beneficiarul acestora se află în cadrul aceleiaşi reţele. Dacă se foloseşte un cloud public, furnizorul de servicii şi beneficiarul acestora se află în reţele separate. În cazul unui cloud hibrid, furnizorul de servicii trebuie să se extindă în cadrul reţelei beneficiarului, iar beneficiarul trebuie să se extindă în cadrul reţelei furnizorului, ceea ce are ca rezultat faptul că atât furnizorul de servicii cât şi beneficiarul acestora trebuie să-şi expună o parte a reţelei unul către celălalt, ceea ce presupune realizarea unei arhitecturi de reţea mult mai flexibilă, asigurând fezabilitatea unor servicii de reţea independente de locaţie. Abstractizarea resurselor reprezintă o oportunitate pentru provizionarea automată.

Un factor important în respectarea acordului de furnizare a serviciilor îl reprezintă lărgimea de bandă. Lărgimea de bandă trebuie să ia în considerare cantitatea de date anticipată a fi transferată prin reţea, care poate fi dificil de calculat şi care poate deveni foarte costisitoare dacă este supraevaluată. Pentru a rezolva această problemă, oportunitatea e dată de soluţii scalabile pentru lărgimea de bandă care să permită o utilizare mult mai eficientă a resurselor de reţea, fără a afecta securitatea sau flexibilitatea arhitecturală.

O altă problemă de conectivitate o reprezintă latenţa. Atunci când utilizatorii, aplicaţiile şi datele sunt distribuite pe zone de mari dimensiuni se poate ca fiabilitatea şi performanţele aplicaţiilor să fie puternic afectate, deoarece utilizatorii aşteaptă rezultatele într-un timp foarte scurt. Pentru a evalua performanţa, trebuie analizate atât infrastructura cloud-ului, cât şi partea de reţea, ambele jucând un rol extrem de important în acest sens. Din acest motiv, trebuie să se aleagă locaţia potrivită pentru infrastructura de cloud, astfel încât aceasta să fie cât mai apropiată de utilizatori.

În sfârşit, dar nu în ultimul rând trebuie luate în considerare sistemele de protecţie ale reţelei. Acestea trebuie să fie unele adecvate pentru sistemele de tip cloud computing, deoarece nu trebuie să necesite modificări în cadrul componentelor hardware sau software în cazul apariţiei unei ameninţări. Deoarece astfel de soluţii sunt gestionate în mod centralizat, detectarea pericolelor se face împreună cu toţi cei care participă atât la furnizarea serviciului cât şi la utilizarea acestuia, ceea ce permite o creştere a ratei de detecţie.

În cadrul acestui rezultat a fost prezentată o vedere de ansamblu asupra arhitecturii reţelei de comunicare ce va trebui folosită în proiectul NOAH, obţinându-se arhitectura conceptuală corespunzătoare soluției alese.

În vederea folosirii sistemului de cloud de la Institutul de Cercetare al Universității Transilvania din Brașov, a fost proiectată rețelistica completă ce a fost prezentată ca rezultat al Activităţii I.3. A fost prezentat întregul sistem de componente ce fac posibilă funcționarea completă, consistentă și sigură a sistemului proiectat, propus anterior.