

КОНЦЕПЦИЯ

ЗА РАЗВИТИЕ НА ВЪТРЕШНАТА МРЕЖА НА ПЛОВДИВСКИЯ УНИВЕРСИТЕТ

от Атанас Терзийски

За пълното разбиране на този документ и идеите в него се изискват по-задълбочени познания по компютри, мрежи и Интернет. Умишлено е пропуснато разясняването на техническите детайли с цел краткост и лекота на текста.

Въпреки всичко информацията тук е достъпно представена за по-голяма читателска аудитория.

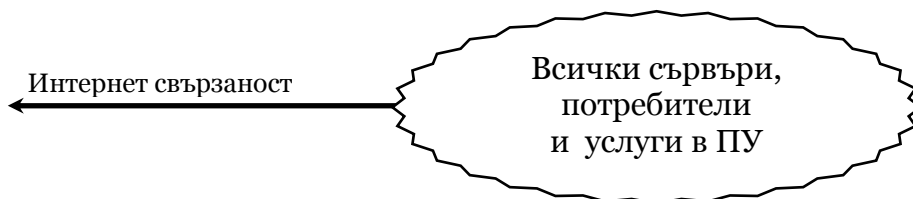
Версия 0.4

9 Април 2007

1. Реализации на вътрешната мрежа на Пловдивския университет през годините

(А) До ноември 2005

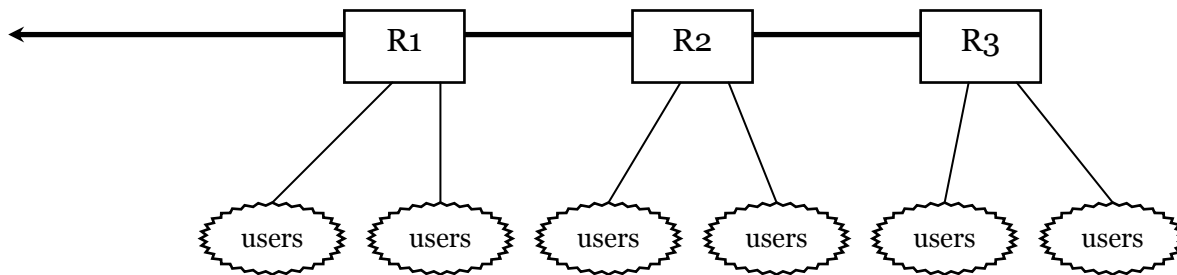
Обща LAN мрежа, управлявана от DHCP. Това е лесно, гъвкаво и същевременно евтино решение за неголеми мрежи. Схематично това изглежда така:



Недостатък на този подход, който се появи скоро, е сигурността на тази реализация. С развитието на мрежата и увеличаването на броя потребители нарастваха и пакостите в нея, било то умишлени, по невнимание или поради незнание. Тогава предложих да сменим тази реализация и да сегментираме мрежата.

(Б) След ноември 2005 и досега

С доклад до Зам.-Ректора от октомври 2005 мотивирах вече ялната нужда от сегментиране на локалната мрежа. Като най-надежден и същевременно не много скъп, напълно удовлетворяващ нуждите към момента вариант, предложих това да стане с разполагането на три софтуерни L3 маршрутизатора с по няколко интерфейса, които използвахме за разделяне на клиентите в университета. Тази топология, функционираща и до момента, може схематично да се покаже по следния начин:



Областите "users" са различните сегменти от потребители, маршрутизирани през съответния "Rx" маршрутизатор. С други думи вече имаме физическо разделение, като се предлага IP свързаност по Layer 3 (L3) до услугите, предоставяни в ПУ. Така евентуалните злоупотреби се локализируют и засягат само съответния сегмент, като проследяването и отстраняването на проблемите вече е доста по-лесно.

Основни и вече осезаеми недостатъци на тази реализация са следните:

- (1) Нарушена L2 свързаност в локалната мрежа. В резултат на това е невъзможно L2 разделянето на трафика или създаване на виртуални подмрежи (VLANs) с достъп до университетските услуги, примерно Интернет телефония, безжичен Интернет, предефинирани на групи по интереси, примерно счетоводство, библиотека, факултети и т.н.

- (2) Маршрутизаторите R1, R2 и R3 често се оказват неадекватни (като физически параметри или ограничения на ОС) да поддържат по-сложни IP филтри, приложени за голям трафик, предлагане на услуги като IPv6 свързаност, IPv4 multicast, IPsec и т.н.
- (3) Децентрализираната поддръжка и администрацията на R1, R2 и R3 се усложнява особено с недостига на човешкия ресурс, с който в момента разполага университетът.

Тези три основни пункта налагат промяна на топологията на университетската мрежа, като възможностите за това се дискутират в следващата точка.

2. Възможни реализации оттук насетне

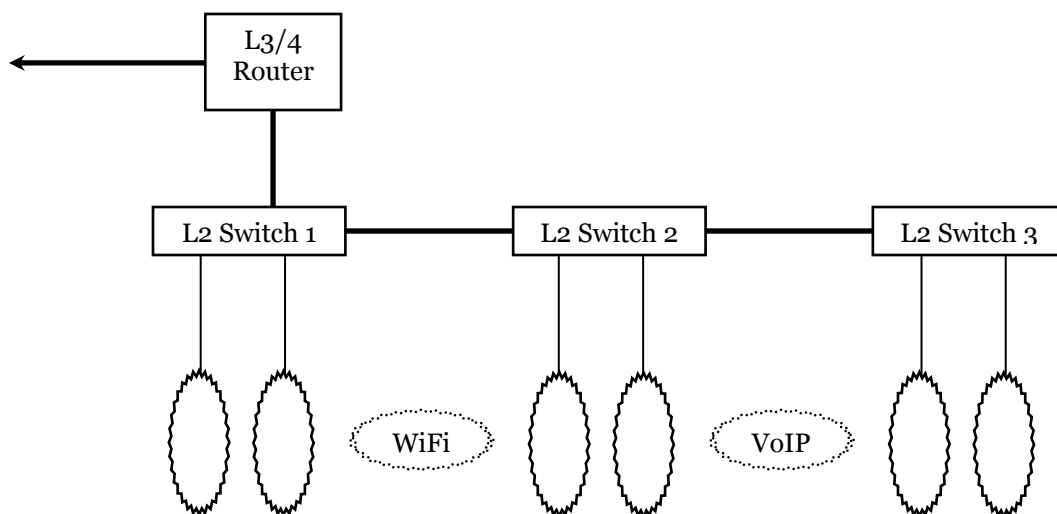
Тук ще бъдат разгледани и коментирани от техническа и финансова гледна точка два основни типа реализации на локална мрежа. Оптималната (според мен) реализация за Пловдивския университет от гледна точка на цена, възможности и нужди е смесената топология.

(А) Йерархична (по L2/3/4)

Като основно и безспорно предимство на йерархичната мрежа, реализирана с децентрализирано разположени Layer 2/3/4 маршрутизатори, е високата им рутираща ефективност. Такава топология е подходяща и дори задължителна за по-големи мрежи като например MAN или национални мрежи, в които има значителен вътрешен трафик между хостовете. Изграждането на йерархична мрежа в рамките на организация като Пловдивския университет е неоправдано, безсмислено засега и значително скъпо (от порядъка на шестцифрена сума).

(Б) Смесена

С доклад от 10.11.2006 мотивирах нуждата от закупуване на три L2 комутатора, които да използваме за сегментиране на локалната мрежа с различни VLAN мрежи, като заменим с тях досегашните L3 софтуерни R1, R2 и R3 маршрутизатори. Това схематично би могло да се представи по следния начин:



Както става ясно, запазва се подобие с досегашната сегментирана мрежа, като в случая се прави разделяне на Layer 2, а Layer 3 свързаност се получава

централизирано от L3/4 маршрутизатор. В този случай отпадат трите ограничения, дискутирани по-горе като налични за сегашната реализация. Зоните WiFi и VoIP са отделни хардуерни устройства в мрежата, които виртуално също се обединяват в отделен L2 сегмент или VLAN.

Като единствен недостатък на предложената схема може да се изтъкне известна неоптималност при маршрутизиране на вътрешния трафик, тъй като комуникацията на клиентите от различни сегменти ще се извършва само през централния L3/4 маршрутизатор. Известно е обаче, че статистиките за натоварване на мрежата през последните години не показват наличие на сериозен вътрешен трафик.

3. Какво е нужно оттук нататък

За изпълнението на предложената топология е необходимо да се създаде гигабитов L3/4 маршрутизатор, който да доставя L3 свързаност на отделните VLAN мрежи, сегментирани на L2 чрез трите комутатора. Има два варианта за това:

- (1) Хардуерен маршрутизатор: професионално и скъпо решение, може би от порядъка на десетки хиляди евро. Неоправдана инвестиция.
- (2) Софтуерен маршрутизатор за около 2000 евро. Това ще е надежден многопортов сървър, който ще обслужва VLAN сегментите по L3 и L4.

До момента на закупуване на по-мощен софтуерен L3/4 маршрутизатор различните сегменти ще се обслужват на 10 Mbps само по L3 (без въвеждане на IP филтри). Това ограничение се налага само и единствено поради недостатъчния хардуерен ресурс на досегашния маршрутизатор или PC.

4. Свързаност

Свързаността между трите L2 комутатора, показани на последната схема, е реализирана в момента с меден UTP кабел от нисък клас. За поддържане на гигабитова свързаност на по-дълги разстояния (над 70-80 метра) в момента ползваме множество некачествени концентратори и комутатори, които често не работят коректно, имат много аварии и блокирания и това води до сериозна нестабилност и прекъсване на мрежата.

Смятам за задължително, особено при централизирана L3 локална мрежа, свързаността на основния носещ гръбнак (backbone) да бъде оптична на 1 Gbps.

5. Човешки ресурси

Развитието и поддръжката на вътрешната мрежа е пряко свързано с човешките ресурси, които университета отделя за това. Нека разгледаме основните аспекти поотделно, свързани с развитието и поддръжката на мрежата.

(А) Развитие

Тук основно се включват (А1) запознаване с нови технологии, хардуер, софтуер и услуги, (А2) тестване и (А3) внедряване, което включва и достъпно описание на предлаганите услуги.

(Б) Поддръжка

Поддръжката включва както (Б1) хардуерна, така и софтуерна или на предлаганите услуги, (Б2) гореща линия или работа с потребители, (Б3) сигурност във всичките и аспекти или Computer Security Incident Response Team, (Б4) външна и вътрешна свързаност и т.н.

Към момента ресурса от локални администратори покрива малка част от споменатите по-горе аспекти само на софтуерната и отчасти хардуерната поддръжка на потребителските станции. Занемаряването на аспектите (А) и (Б) води до ограничения или дори забрани, които рано или късно се забелязват от крайния потребител или като цяло качеството на Интернет услугите намалява.

Проблема “Липса на IT човешки ресурси” в Пловдивския университет е осезаем. Би могло да се работи по политика за използване на студентския ресурс под формата примерно на дипломни работи или като цяло по политика за запазване на интелектуалния ресурс в университета.

6. Заключение

В заключение мога да обобщя, че предлагането на нови мрежови услуги в университета изисква по-голям капацитет и по-висока надеждност на мрежата, както и общо казано човешки ресурси за развитие и поддръжка. Следващите важни стъпки за това са (1) закупуване на дискутирания по-горе L3/4 маршрутизатор и (2) оптична свързаност на основния гръбнак на мрежата. Въпроса за човешките ресурси остава засега отворен в тази концепция.