ВИША ЕЛЕКТРОТЕХНИЧКА ШКОЛА

Михаило Стефановић

КОНЦЕПЦИЈА И РЕАЛИЗАЦИЈА МЕЂУСОБНО ПОВЕЗАНИХ ЛОКАЛНИХ РАЧУНАРСКИХ МРЕЖА

- дипломски рад –

Београд, 2003.

Кандидат: **Стефановић Михаило**

Бр. индекса: **350/98**

Смер: **Нове рачунарске технологије**

Тема: **КОНЦЕПЦИЈА И РЕАЛИЗАЦИЈА МЕЂУСОБНО ПОВЕЗАНИХ ЛОКАЛНИХ РАЧУНАРСКИХ МРЕЖА**

Основни задаци:

1. Међусобно повезивање рачунарских мрежа

2. Уређаји за међусобно повезивање мрежа

3. Мултимедијални приказ

Хардвер: **Софтвер:** **Теорија:**

Београд, 1.7.2003.

Ментор:

_____

Мр Верица Васиљевић, проф. ВЕТШ

ИЗВОД

У дипломском раду описане су основне концепције и начини реализације међусобног повезивања локалних рачунарских мрежа – међуумрежавање или Internetworking, као и основне технологије које се у ту сврху користе: брицинг (премошћавање, bridging), рутирање (routing) и свичинг (комутирање, switching). Дат је преглед основних технологија која се данас користе у LAN и WAN мрежама, као и неке будуће перспективе развоја.

ABSTRACT

This work describes basic concepts and implemantation of Local Area Networks (LAN) of internetworking, and technologies used, such as Bridging, Routing, and Switching. Basic overview of technologies used today in LANs and WANs is given, as well as future development perspectives.

САДРЖАЈ

УВОД

Циљ овог рада је да објасни основне међусобног повезивања локалних мрежа – **међуумрежавање** или **Internetworking**, као и основне технологије које се у ту сврху користе: **брицинг** (премошћавање, **bridging**), **рутирање** (**routing**) и **свичинг** (комутирање, **switching**).

Рачунарска мрежа се може дефинисати као скуп два или више међусобно повезаних рачунара. Када се они налазе на релативно малом међусобном растојању, обично у оквиру једног предузећа или организације, такву мрежу називамо **локална рачунарска мрежа (Local Area Network – LAN**). Повезивањем локалних мрежа на нивоу једног града настају **градске мреже** (**Metropolitan Area Networks – MAN**), док се мреже које обухватају веће области, од неколико километара па све до неколико хиљада километара, називају **регионалне мреже (Wide Area Networks – WAN).**

Заједничко за већину локалних мрежа данас је да су у највећем броју базиране на Етернет (Ethernet) стандардима. Етернет је настао касних 70-их година у сарадњи фирми Xerox, Intel и DEC, и у међувремену је потпуно потиснуо остале стандарде коришћене у локалним рачунарским мрежама, као што су Токен Ринг (Token Ring) или Arc Net. Обухваћен је IEEE 802.3 серијом стандарда, а базира се на CSMA/CD (Carrier Sense Multiple Access with Collision Detection) приступу, који обезбеђује да више станица на мрежи деле исти физички медијум. Од почетних 1 мегабит у секунди (Мб/с), брзина приступа је порасла и до више од неколико десетина гигабита у секунди. Међутим, све то, као и рапидан раст броја умрежених рачунара, као и тежња да се они међусобно повезују у све шире регионалне везе, довело је и до развоја бројних технологија које имају за циљ да омогуће превазилажење свих ових проблема.

ДИЗАЈН МЕЂУУМРЕЖАВАЊА

ПОСЛОВНА МОТИВАЦИЈА И ИЗАЗОВИ МЕЂУУМРЕЖАВАЊА

Локалне рачунарске мреже (ЛАН) имају природну тенденцију раста све док дељени медијум мрежне архитектуре (Ethernet, Token Ring, FDDI, итд.) не постане преоптерећен, а перформансе мреже почну да опадају. Ово је један од два главна разлога за проучавање решења за међуумрежавање. Друга ситуација настаје када је потребно да се између независно оформљених локални мрежа почне вршити размена информација. Оба разлога се заправо своде на пословне одлуке. Слабе перформансе због преоптерећеног дељеног медијума локалне мреже доводе до пада продуктивности радника, што се може проширити и на пад задовољства клијената, продаје, удела на тржишту и слично.

Могућност да се доносиоцима одлука пруже праве информације на правом месту и у право време, без обзира на локацију тих информација, је заправо кључна мотивација за међуумрежавање. Главни изазов или највећа препрека за постизање транспарентног приступа информацијама су бројне некомпатибилности између хардверских и софтверских технологија различитих произвођача које се користе у међусобно повезаним мрежама. Операционе карактеристике локалних мрежа се дефинишу протоколима, које када су организоване у слојевити модел као што је то OSI модел, називамо протокол стек *(protocol stack)*. Протокол стек локалне мреже је заправо опис

њених особености. Другим речима, ако желимо да постигнемо транспарентну интероперабилност локалних мрежа, сваки мрежни протокол стек морамо упарити или конвертовати у одговарајући протокол који ће моћи да комуницира са протоколом мреже са којом се повезујемо. Транспарентно повезивање више локалних мрежа се остварује само транспарентним повезивањем одговарајућих протокола.

ОПШТЕ СТРАТЕГИЈЕ ДИЗАЈНА МЕЂУУМРЕЖАВАЊА

За побољшање перформанси на преоптерећеним локалним мрежама, може се применити неколико доказаних стратегија дизајна:

Сегментација мреже је обично први корак. Што је мање радних станица у сегменту, мање надметања за заједнички дељени проток. Сегментација унапређује перформансе и код CSMA/CD (Carrier Sense Multiple Access with Collision Detection – Ethernet) и код Token Ring технологија. Одређена врста међумрежног уређаја, као што је бриџ или рутер, је неопходна за повезивање сегмената мреже.

Екстремни случај сегментације, када сваки сегмент мреже садржи само једну радну станицу, називамо **микросегментација**. Микросегментирана мрежа захтева употребу мрежних свичева који су компатибилни са мрежним картицама (NIC) инсталираним на радним станицама. И етернет и токен ринг свичеви су широко доступни.

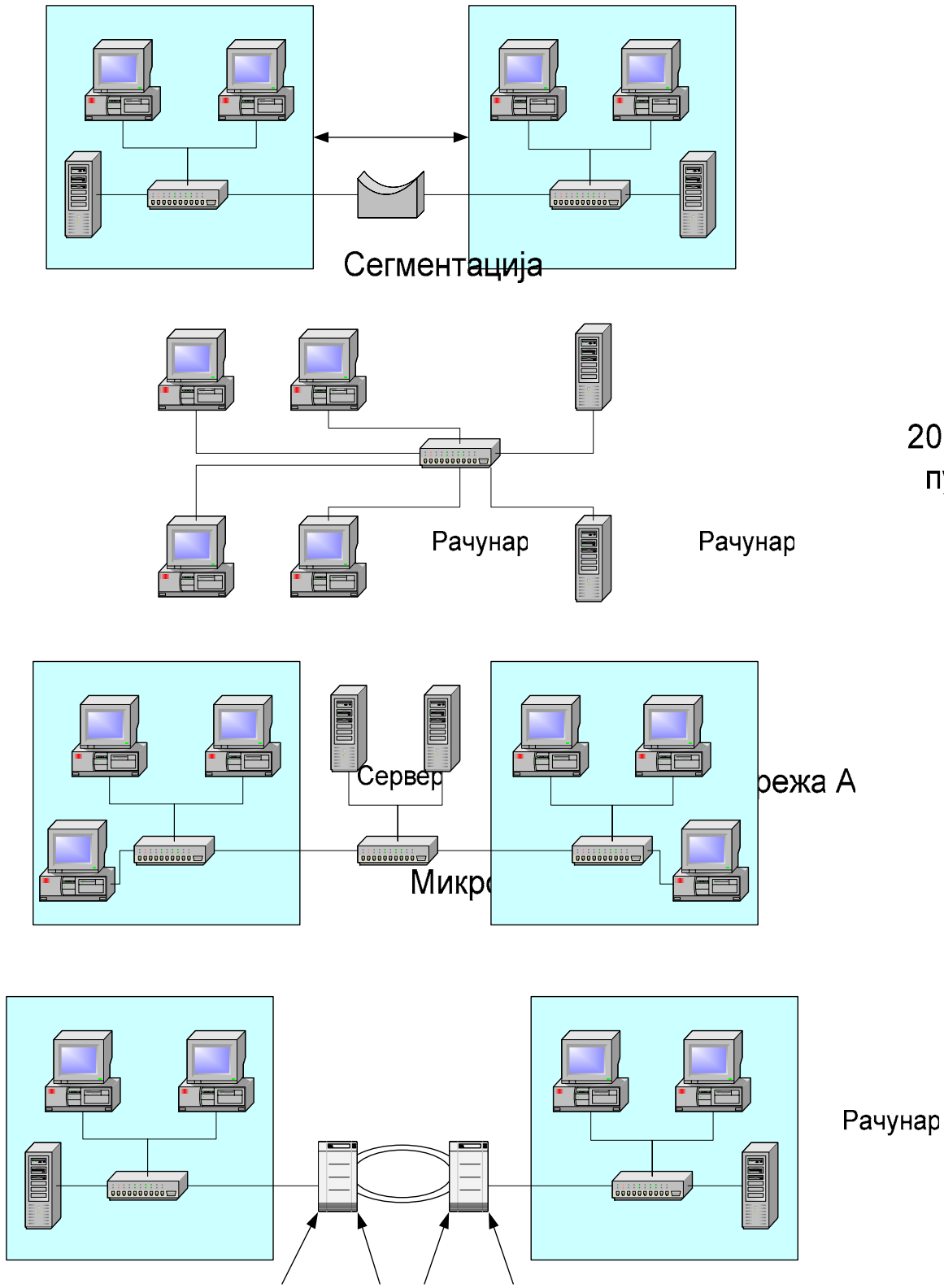
Уместо да свака радна станица чини посебан сегмент мреже, некада је потребно издвојити само посебне, високо захтевне уређаје као што су сервери. Оваква стратегија сегментирања назива се **изолација сервера** (Server Isolation). Изолујући сервере у посебне мрежне сегменте, осигуравамо њихов сигуран приступ дељеним мрежним ресурсима.

Хијерархијско умрежавање изолује локални мрежни саобраћај на локалној мрежној архитектури (као што је етернет или токен ринг), док за пренос међумрежног саобраћаја користи архитектуре великих брзина као што су FDDI, Fast Ethernet или ATM. Сервери се најчешће повезују на **кичму мреже** (backbone network), док јој радне станице могу приступати само по потреби и то преко рутера. ***Слика 1.*** илуструје ове опште стратегије дизајна међуумрежавања.

Бриџинг, рутинг и свичинг су три основна процеса међуумрежавања који омогућују сегментирање мреже и одвајање мрежних ресурса. У сва три ова процеса се заправо обрађују мрежне адресе, и доносе одлуке да ли ће саобраћај бити прослеђиван на основу адреса из дата-линк и мрежног слоја. Ови процеси се међусобно разликују по начину коришћења адреса, софистицираности, предностима и ограничењима.

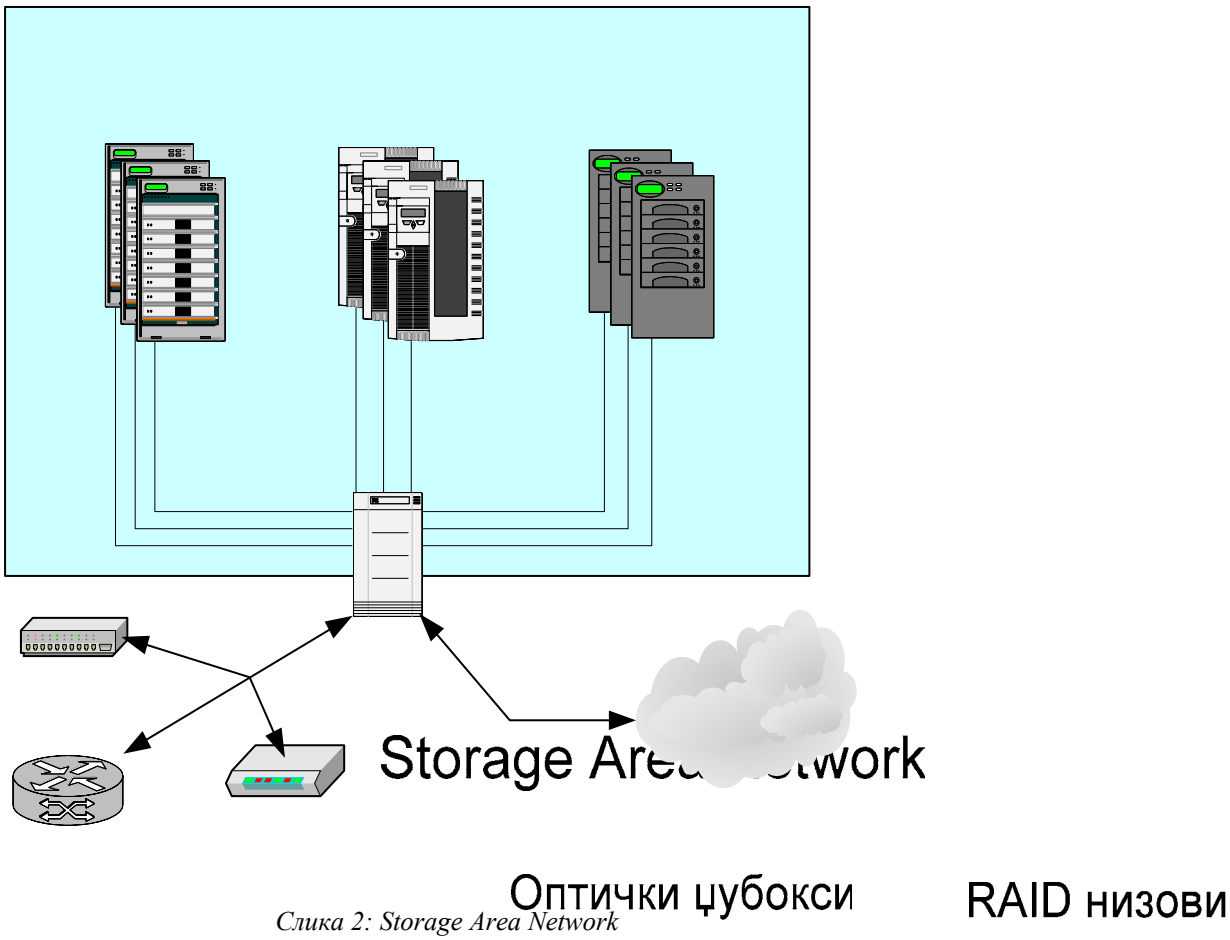
MAN – Metropolitan Area Networks Представља мрежу која обухвата територију једног града. Често постоји потреба да се више локалних мрежа које припадају једном предузећу или организацији, а које су расуте на територији једног града међусобно повежу. У том случају се користе MAN – Metropolitan Area Networks. Најчешће услуге повезивања у MAN обезбеђује телекомуникациона компанија, мада у неким случајевима и сама предузећа могу одржавати сопствене MAN. За изградњу оваквих мрежа се најчешће користе фибер-оптички каблови и SONET као основни транспортни механизам. Кључна одлука са којом се сусрећу пројектанти MAN мрежа је *који ће се транспортни протоколи користити на мрежи?* Међу изборима за MAN транспортни протокол најчешћи су гигабит Етернет, ATM, Packet Over SONET, и Cisco динамички пакетни транспорт. Wavelength Division мултиплексирање омогућава да се више

транспортних протокола истовремено преноси на више различитих таласних дужина преко истог оптичког влакна.



Слика 1: опште стратегије дизајна међуумрежавања

SAN – Storage Area Networks. Логичан наставак претходно поменуте технике изолације сервера је САН. САН мреже покушавају да одвоје складиштење података од апликационих сервера, тако што се уређаји за складиштење као што су низови дискова или библиотеке трака директно повезују на компанијску мрежу редундантним везама великог капацитета. Иако постоје бројне алтернативе, за повезивање сан најчешће се користи Fiber Channel (пренос фибер-оптичким кабловима, брзине до 1 гигабит у секунди на раздаљини до 10 км). Мада САН мреже имају велики потенцијал за коришћење у мрежним решењима великих предузећа, остају проблеми интеграције и интероперабилности. Fiber Channel уређаји различитих произвођача су често некомпатибилни међу собом или са SCSI интерфејсима на различитим уређајима за складиштење података. Такође, ни сви клијентски или серверски оперативни системи често не могу да приступе директно САН уређајима. На ***слици 2.*** је дат општи приказ САН мреже и одговарајућих протокола.



Слика 2: Storage Area Network

БРИЏИНГ

Брицинг (Bridging, премошћавање) је често прва стратегија која се примењује у међуумрежавању или сегментирању локалних мрежа, пре свега због једноставности имплементације и ефективних резултата. Подела једне преоптерећене мреже у два мрежна сегмента повезана брицом мора се извести уз мало претходног планирања да би се минимизовао саобраћај између сегмената и тако избегло да бриџ постане уско грло мреже. Да би се одлучило у ком сегменту треба да се нађу који сервери и радне станице, често се користи правило 80/20. Правило каже да 80% саобраћаја треба да

остане у локалном сегменту, а да максимално 20% може да се прослеђује другом сегменту преко брица.

Адресирање

Премошћавање (бриџинг) је процес нивоа везе, при чему се одлуке о усмеравању мрежног слоја доносе на основу MAC адреса или адреса нивоа везе. Бриџеви су пасивни или транспарентни уређаји, који примају сваки фрејм пренет на датој локалној мрежи. Каже се да су **транспарентни** због своје особине да обрађују само адресу у нивоу везе, док се подаци у горњим нивоима протокола транспарентно преносе. Уместо да прослеђују сав саобраћај између мрежа или сегмената мреже, бриџеви читају **одредишну адресу** (MAC адресу одредишног мрежног адаптера, тј. мрежне картице) сваког пакета података на локалној мрежи, и на основу ње одлучују да ли је пакет намењен одредишту у локалу или на другој страни брица, пропуштајући само пакете са не-локалним одредишним адресама.

Протоколи нивоа везе као што је Етернет садрже **изворишну адресу**, као и одредишну адресу у оквиру предефинисаног етернет оквира (фрејма). Бриџ проверава изворишну адресу сваког фрејма који прими и ту адресу додаје у **табелу познатих локалних чворова**. На тај начин, бриџ «учи» о свим новим радним станицама које се појаве на локалној мрежи, без потребе да се ручно конфигурише. Неки бриџеви шаљу захтеве свим локално повезаним радним станицама, и на основу добијених одговора конструишу табелу локалних чворова.

Након што бриџ прочита одредишну адресу, она се упоређује са садржајем табеле познатих локалних чворова да би се одлучило да ли пакет треба проследити или је намењен само локалној мрежи. Пошто се само пакети са одредишном адресом која није у локалној табели чворова прослеђују преко брица, они се понекад називају **проследи-ако-није-локално** (forward-if-not-local) уређаји. На ***слици 3.*** је приказано на који начин бриџ користи адресе из слоја везе.

Оквир слоја везе

Заглавље оквира		**Поље података оквира**	**Реп оквира**
Изворна адреса	**Одредишна адреса**	Протоколи виших слојева укључујући адресе слоја мреже	
MAC адреса изворне радне станице	MAC адреса одредишне радне станице		
Ове адресе бриџеви користе да би одредили да ли пакет треба проследити преко брица			
Бриџеви НЕ мењају адресе у слоју везе			

Слика 3: како бриџеви користе адресе из слоја везе

Предности

Због своје могућности да уче, бриџеве су релативно једноставни за инсталирање и конфигурисање, омогућујући брзо и исплативо решење за презагушене мрежне сегменте. Поред логичке сегментације локалног мрежног саобраћаја, бриџеви су у могућности да продуже растојања између мрежних сегмената тако што понављају,

временски усклађују и регенеришу примљене сигнале пре него што прослеђивања. Такође омогућавају превођење између различитих мрежних архитектура (са токен ринга на етернет) или са различитих врста физичких медија (нпр. УТП на оптику).

Бриџеви се најчешће користе за сегментирање саобраћаја између локалних мрежа, или између локалне мреже и кичме мреже велике брзине.

Ограничења

Највеће ограничење бриџева је истовремено једна од највећих предности. Пошто бриџеви уче и не захтевају текуће конфигурисање, они знају само да прослеђују све пакете који нису намењени локалним одредиштима. У случају када је између одредишног чвора и локалне мреже налази више локалних мрежа и бриџева, свим радним станицама на свим мрежама између извора и одредишта биће прослеђен пакет намењен удаљеном одредишту. Прослеђивање порука свим радним станицама на успутним мрежама назива се **пропагација**. У случају да је оквир погрешно адресиран или послат на непостојећу адресу, може се десити да пакети почну бесконачно да се умножавају и шире, доводећи до стања које се назива емисиона олуја (*broadcast storm*). Бриџеви најчешће не могу да се користе у мрежама које садрже редундантне везе јер више активних веза између мрежа може да доведе до појаве емисионих олуја.

РУТИРАЊЕ

Иако се код оба процеса врши испитивање и условно прослеђивање пакета података, рутирање и премошћавање се значајно разликују у неколико кључних функционалних области:

Док бриџ чита одредишну адресу сваког пакета који се појави на мрежи, рутери проверавају само оне пакете који су им експлицитно послати.

Уместо да само преусмеравају пакете података између мрежа као бриџеви, рутери су много опрезнији и кориснији.

Уместо да само проследи пакет података, рутер прво проверава постојање одредишне адресе, као и последње информације о мрежним путањама преко којих пакет може стићи до одредишта. Затим, на основу последњих података о мрежном саобраћају рутер бира најбољу путању и њом прослеђује пакет до одредишта

Адресирање

Док бриџеви одлуку о прослеђивању пакета доносе на основу адресе MAC слоја садржане у заглављу оквира слоја везе, рутери одлуку о прослеђивању доносе на основу садржаја адресе мрежног слоја садржане у пољу података слоја нивоа везе. Сам рутер има одредишну адресу нивоа везе, и способан је да прима, обрађује и прослеђује пакете података са било које локације до сваке мреже на коју је директно или индиректно повезан.

Како пакети података стижу до рутера? Одредишна адреса Етернет или Токен ринг пакета мора бити MAC адреса рутера који ће обавити даље прослеђивање. Тако, рутер се адресира преко одредишног поља адресе у нивоу везе. Рутер затим одбацује «омотницу» MAC подслоја која садржи његову адресу и чита садржај поља података у Етернет или токен ринг оквиру. Адресирање у дата линк слоју се обично назива адресирање од тачке до тачке (point-to-point addressing).

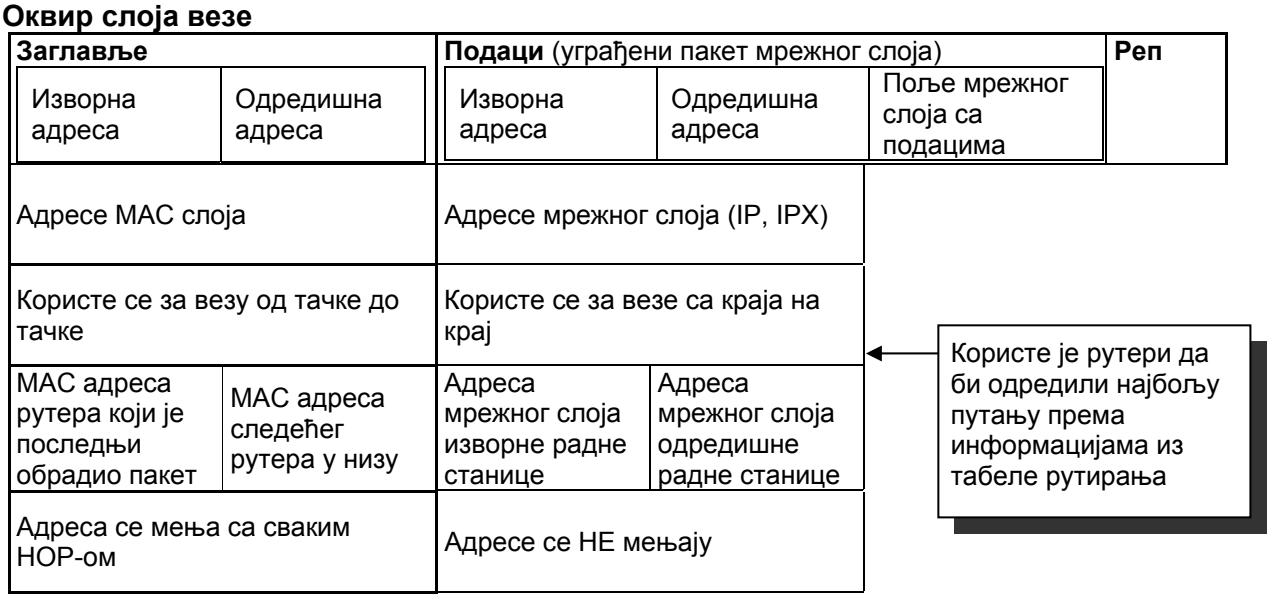
Као и у случају протокола дата линк слоја, и протоколи мрежног слоја одређују тачну структуру оквира података који рутер разуме. Оно што изгледа као само податак и што међумрежни уређаји као што је бриџ игноришу, код рутера се «распакује» и детаљно испитује да би се даље обрађивало.

Након што прочита одредишну адресу у мрежном слоју, а што је заправо адреса одредишне радне станице којој је пакет намењен, рутер консултује своју **табелу рутирања** да би одредио најбољу путању којом треба проследити пакет. Табеле рутирања садрже бар нека од следећих поља на основу којих одређују "најбољу путању":

- Мрежни број одредишне мреже. Ово поље служи као кључ који се користи за проналажење одговарајућег записа са детаљнијим информацијама о најбољој путањи до те мреже.
- MAC адресу следећег рутера на путу до одредишне мреже.
- Порт рутера са кога реадресиран оквир дата-линк слоја треба да буде послат
- Број скокова (Hops) или успутних рутера до одредишне мреже
- Старост записа, да би се избегло да се одлуке о рутирању доносе на основу застарелих информација.

Пошто пронађе најбољу путању, рутер има способност да препакује пакет података у зависности од најбоље путање која је изабрана. Иако адресе мрежног слоја остају непромењене, рутер прави нови оквир слоја везе. Као одредишна адреса слоја везе уписује се MAC адреса следећег рутера на путањи која је као најбоља изабрана до коначног одредишта, а као изворишна адреса слоја везе поставља се MAC адреса рутера који врши прослеђивање. Адресирање у мрежном слоју обично се назива адресирање са краја на крај (end-to-end addressing).

За разлику од бриџева, који само омогућавају приступ спољним мрежама, рутери прослеђују пакете података тачно одређеним циљним рутерима. Међутим, пре него што упути пакет на међу-мрежу, рутер потврђује да постоји одредишна адреса којој је пакет намењен. Само онда када је рутер задовољан са доступношћу одредишне адресе, као и са квалитетом путање до ње, пакет ће бити прослеђен. Ова активност на страни рутера назива се "forward-if-proven-remote" логика. ***Слика 4.*** илуструје коришћење адреса мрежног и слоја везе од стране рутера.



Слика 4:Како рутери користе адресе из мрежног слоја и слоја везе

Предности

У поређењу са брицингом, рутирање даје могућности да се ефикасније искористи слободан опсег на великим мрежама које садрже редундантне путање. Ефективно коришћење редундантних путања у мрежи дозвољава рутерима да направе прерасподелу оптерећења (load balancing) укупног мрежног саобраћаја дуж две или више веза између две дате локације. Избор "најбољег пута" од стране рутера може бити одређен различитим факторима, као што су број скокова (hops), трошкови преноса или тренутно загушење линија. Рутери могу да динамички одржавају табеле рутирања и тако ускладе перформансе у зависности од променљивих мрежних услова. Захваљујући forward-if-proven-remote логици, рутери су способни да сачувају мрежу од погрешно адресираног саобраћаја кроз филтрирање адреса мрежног слоја. На тај начин, рутери се понашају као заштитна баријера (firewall) између повезаних мрежа. Мреже базиране на рутерима много су скалабилније од мрежа заснованих на брицевима. Рутери су у могућности да прослеђују много софистицираније и потпуније управљачке информације системима за мрежно управљање преко SNMP (Simple Network Management Protocol).

Када се повезују две локалне мреже на великој међусобној удаљености преко WAN веза, рутери се употребљавају више него брицеви као интерфејс према WAN вези. Због способности рутера да прецизније идентификује протоколе виших слојева, непотребни или нежељени саобраћај се не шаље преко WAN веза које су релативно споре и прилично скупе.

Можда најважнија предност рутера је њихова способност да обрађују више протокола мрежног слоја истовремено. Одговарајуће подешен рутер може да обрађује истовремено IP, IPX и AppleTalk пакете и да притом сваки протокол упућује на одговарајућу одредишну мрежу. Поред тога, неки рутери могу да раде и са нерутабилним протоколима као што су NetBIOS, LAT или SNA/SDLC који немају никакву адресну схему мрежног слоја. У тим случајевима, оквири дата-линк слоја се или бришу или се протоколи виших слојева енкапсулирају у пакете мрежног слоја као што је ИП.

Да сумирамо, рутери пружају следеће услуге међуумрежавања:

- Служе као заштитне баријере (Firewalls) између повезаних локалних мрежа;
- Спречавају пролаз емисионих (broadcast) пакета на међумреже;
- На основу протокола мрежног слоја врше одабир и приоритетизују обраду пакета;
- Пружају сигурност филтрирањем пакета по адресама слоја везе или мрежног слоја;
- Омогућавају транспарентно повезивање између локалних мрежа.

Ограничења

Због софистицираног процесирања које омогућавају, рутери су знатно сложенији за конфигурисање и управљање од бриџева. Како број рутера у мрежи расте, тако се и пропорционално повећава ниво комплексности управљања мрежом. Ако рутери треба да обрађују више протокола мрежног слоја, сваки од њих мора имати одговарајући протокол стек инсталиран и правилно конфигурисан.

Софистицираност обрађивања података код рутера такође утиче и на софистицираност и више трошкове технологије код рутера у поређењу са технологијом бриџева.

СВИЧИНГ

Свичинг (Switching, LAN Switching, комутација) је по функцији врло сличан бриџингу. Кључна разлика је што се свичинг обавља хардверски, у ASIC (Application-Specific Integrated Circuit) колима, и самим тим је изузетно бржи у поређењу са бриџингом. Основна сврха употреба свича је повећање доступног пропусног опсега на локалној мрежи са дељеним медијумом, спровођењем процеса микросегментације локалне мреже. Пошто свич креира конекције од тачке до тачке за сваки пакет који прими, мреже са дељеним медијумом *(Shared Media LAN)* постају мреже са комутираним медијумом *(Switched Media LAN)*.

Адресирање

Свичеви користе адресе на сличан начин као бриџеви. Свичеви читају одредишну MAC адресу долазећег оквира дата линк слоја и брзо праве комутирану везу према сегменту мреже који садржи одредишну радну станицу. Портови свича на сегментима мреже који садрже више радних станица умеју да разликују саобраћај између локалних радио станица и саобраћај који треба да буде пребачен на други порт ЛАН свича.

Свичеви најбоље раде када саобраћај остаје у оквиру ЛАН сегмента везаног на дати свич. Другим речима, да би се редуковало коришћење скупих ВАН линкова или да би се филтрирао саобраћај који се пропушта на кичму мрежу велике брзине, рутер мора да испита протоколе 3. слоја. У неким случајевима, функционалност рутера је уграђена у ЛАН свичеве. Основни ЛАН свичеви су уређаји 2. слоја уз које се или морају користити екстерни рутери 3. нивоа, или морају имати уграђену могућност рутирања 3. слоја.

На сличан начин као што бриџеви обрађују "нелокални" саобраћај, када свич прими оквир нивоа везе намењен дестинацији ван локане мреже, он једноставно прави

комутирану везу ка свич порту на који је повезан рутер, или према виртуалном рутеру унутар свича преко кога се врши функција рутирања у свичу.

Предности

Употребом ЛАН свичева се постиже драстично повећање пропусног опсега у поређењу са мрежама са дељеним медијумом, ако се довољно пажње посвети организовању радних станица и сервера у мрежне сегменте на логичан начин.

Виртуалне мреже су омогућене могућностима свича да веома брзо постигне да се било које две радне станице или сервера појаве као да су физички повезане на исти сегмент мреже. Виртуелне мреже користе предност могућности свича логички дефинишући оне радне станице и рачунаре који припадају истим виртуелним мрежама без обзира на физичку локацију тих радних станица или сервера. Свака радна станица или сервер може припадати једној или више локалних мрежа.

Ограничења

Ограничења ЛАН свичева су у многоме резултат њиховог порекла од бриџева. Свичеви не могу да врше софистицирана филтрирања или сигурности на основу протокола нивоа мреже, пошто свичеви нису у стању да читају протоколе нивоа мреже. Свичеви не могу да разликују вишеструке путање и одреде оптималну путању. Управљачке информације које се нуде системима мрежног управљања великих предузећа су минималне у поређењу са оним које дају рутери.

И можда најважније, пошто свичована ЛАН веза траје само делић секунде, праћење и управљање саобраћајем знатно је већи изазов него што је то случај код рутера. Традиционални анализатори мрежа конструисани за коришћење на мрежама дељеног медијума нису од користи на свичованим мрежама

ТЕХНОЛОГИЈА МЕЂУУМРЕЖАВАЊА

ТЕХНОЛОГИЈА МЕЂУУМРЕЖАВАЊА И OSI МОДЕЛ

Технологије међуумрежавања могу се категоризовати према нивоу OSI модела који одговара протоколима које је дати међумрежни уређај у стању да обради. На тај начин, следећи међумрежни уређаји могу се категорисати по следећим OSI нивоима:

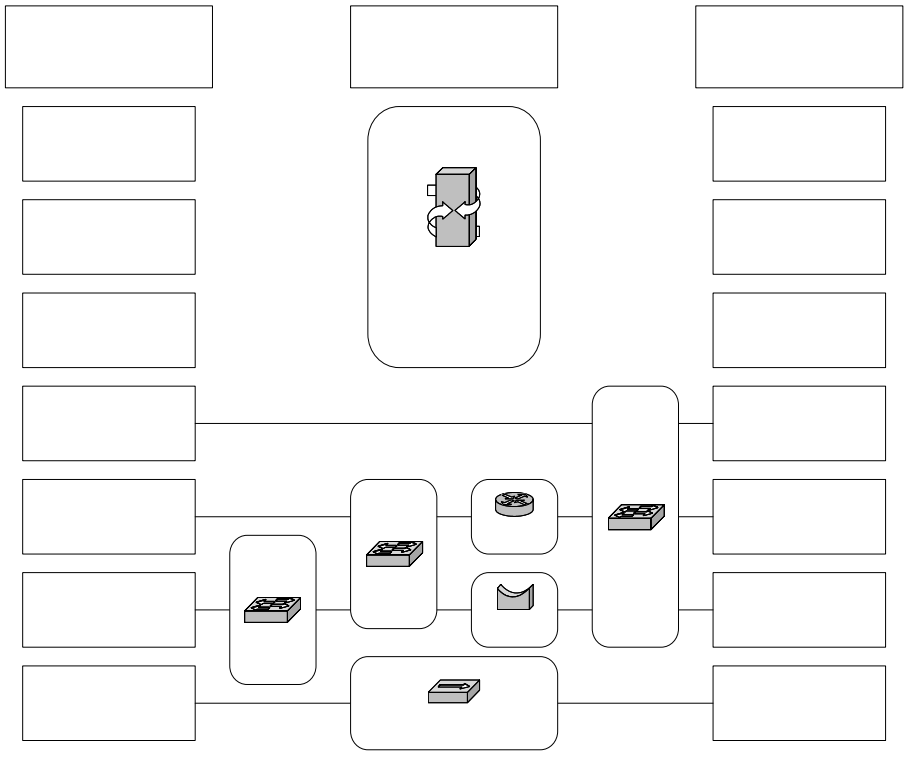
Рипитери:	1. ниво OSI	физички ниво
Бриџеви:	2. ниво OSI	ниво везе
Рутери:	3. ниво OSI	мрежни ниво
Свичеви 2. нивоа:	2. ниво OSI	ниво везе
Свичеви 3. нивоа:	2. и 3. ниво OSI	ниво везе, мрежни ниво
Свичеви 4. нивоа:	2, 3. и 4. ниво OSI	ниво везе, мрежни и транспортни ниво

Сваку од ових категорија међумрежних уређаја детаљније ћемо обрадити у наредним излагањима.

Неке карактеристике су заједничке за све међумрежне уређаје везано за протоколе OSI нивоа који им одговарају:

- Сваки поменути мрежни уређај може да преводи или конвертује протоколе везане за OSI ниво нижи или једнак OSI нивоу међумрежног уређаја.
- Ни један поменути мрежни уређај не може да обрађује протоколе везане за OSI нивое који су виши од OSI нивоа датог међумрежног уређаја.

Однос између OSI модела и међумрежних уређаја илустрован је на ***слици 5.***



Слика 5: Однос између OSI модела и међумрежних уређаја

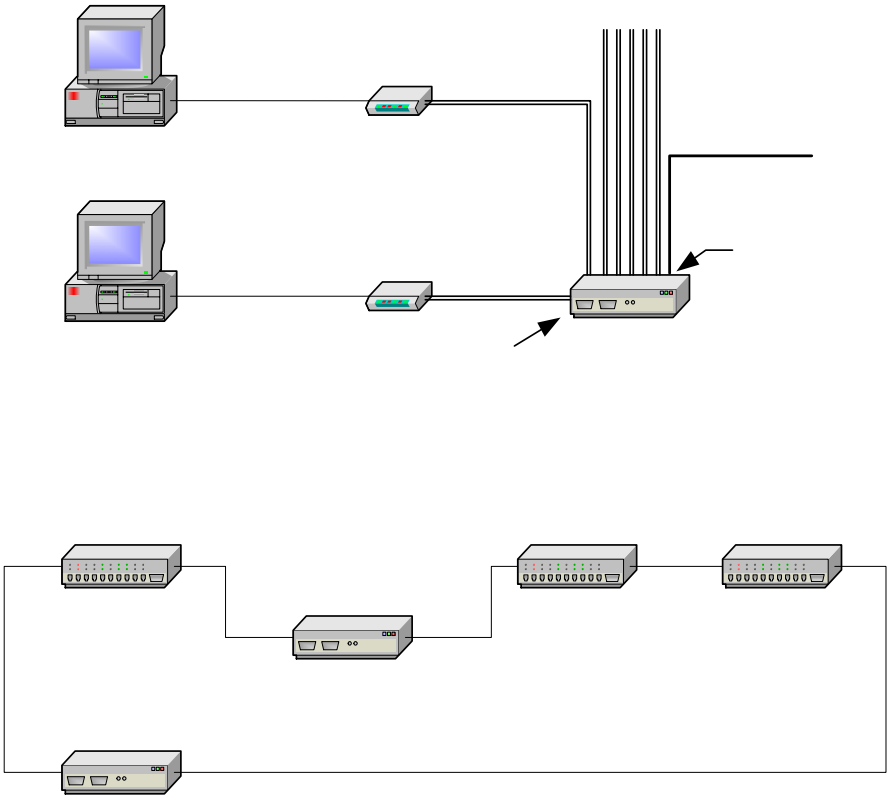
РИПИТЕРИ

Функционалност

Сав мрежни саобраћај на локалној мрежи се обавља сигналима дигиталног облика са дискретним напонима дискретног трајања, који путују преко неке од врста физичког медијума. Једини изузетак су бежичне мреже код којих се сигнали преносе кроз ваздух у аналогном облику. Када се ово има у виду, посао рипитера је једноставан:

- Понавља дигитални сигнал тако што регенерише и временски усклађује долазни сигнал;
- Прослеђује све сигнале између повезаних сегмената;
- Не чита одредишне адресе пакета података;
- Омогућава повезивање и превођење између различитих врста медијума;
- Повећава ефективни домет мреже понављањем сигнала између сегмената.

Рипитер је недискриминишући мрежни уређај. Он не прави разлику између пакета података. Сваки сигнал који долази са једне стране рипитера се понавља и шаље на другу страну. Рипитери су доступни и за Етернет и за Токен ринг мрежне архитектуре, и за читав низ медијума који се на њима користе. Рипитер је уређај физичког нивоа који се бави сигналним протоколима физичког нивоа везаним за напонске нивое и тајминг сигнала.

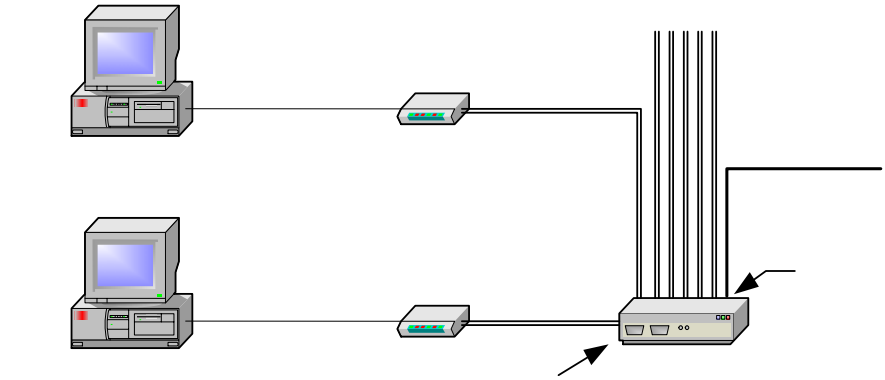


Слика 6: Инсталација рипитера

Основни разлози за употребу рипитера су следећи:

- Повећавање укупне дужине мрежног медијума понављањем сигнала између више мрежних сегмената. У Токен ринг мрежама, неколико MAU (Multistation Access Unit) се могу међусобно повезати рипитерима повећавајући на тај начин величину мреже;
- Изоловање кључних мрежних ресурса на различите мрежне сегменте да би се осигурала већа поузданост;
- Превођење између различитих врста медијума које подржава дата мрежна архитектура.

Слика 6. илуструје типичну примену рипитера.



Слика 6: Инсталација рипитера

Анализа технологије

Табела 7. скицира нека питања анализе технологије која треба узети у обзир пре куповине Етернет или Токен ринг рипитера.

UTP 10BaseT

Fiber-o
trancie

Мрежна архитектура	Питање за анализу технологије	Важност/импликације
Етернет	Подршка за физичке медије или интерфејсе	• 10BaseT: UTP, RJ-45 • 10Base2: Thin Coax, BNC • 10Base5: Thick Coax, AUI • 10BaseFL: фибер-оптички кабл, CT или CMA конектори
	Репетитори за велика растојања	• раде преко једне телефонске парице • повећавају домет ЛАН до 412м • морају се користити у пару • фибер-оптичке везе омогућавају домет до 2км
	Локални репетитори	• Користе се за сегментирање и продужавање домета локалних мрежа
	Модуларни репетитори	• Модули који се могу мењати "у лету" омогућавају флексибилно коришћење различитих типова медија и интерфејса
	Репетитори за радне групе	• Користе се за конверзију медија • Могуће је комбиновати све врсте медија
	Аутоматско партиционисање	• Важна особина која спречава да квар на једном сегменту утиче на друге сегменте • Поновна успостава везе након отклањања квара често је могућа
	Број сегмената по репетитору	• Репетитори подржавају различит број сегмената • Креће се обично од 2 до 8
	Ланчано повезивање	• Неки репетитори могу се ланчано (каскадно) повезати
	Ранг цена	• 250$–2500$
Токен Ринг	Брзина преноса	• брзина Токен Ринга је 4 или 16 Mbps • неки репетитори могу да конвертују између брзина • репетитор мора бити направљен за одређену брзину
	Дужина MAU прстена према lobe растојању	• Токен ринг репетитори продужавају укупну дужину прстена, која се мери или растојањем између MAU, или растојањем од MAU до радне станице (Lobe length),
	Фиберoптички репетитори	• Повећавају максималну дужину прстена до 2700 м
	Подршка за физичке медије или интерфејсе	• Type 1 каблирање: STP, type 1 конектори • Type 3 каблирање: UTP, RJ-45 конектори
	Ранг цена	• 815$–2300$

Табела 7: Анализа технологије рипитера

БРИЏЕВИ

Функционалност

Када је корисницима једне мреже потребан повремен приступ подацима на другој мрежи, потребан је међумрежни уређај софистицираније и дискриминантније од обичног репетитора. Компаративном анализом репетитора и брида, може се закључити да је брић дискриминантнији.

Овакво читање, обрада и дискриминација које обавља брић указује на већи ниво софистицираности коју омогућава уграђени софтвер, али указује и на већу цену (репетитори: $250–$2500; брићеви: $2000–$6000). Брићеви постоје у многим варијантама које су одређене карактеристикама мрежа које треба да премосте. Физички, брићеви могу бити у облику мрежних картица које се прикључују на слот за проширење персоналних рачунара, заједно са одговарајућим софтвером, или у облику самосталних уређаја.

Перформансе брићева генерално се одређују према два критеријума:

- **Брзина филтрирања**: мери се бројем пакета у секунди или оквира у секунди. Процес у коме брић чита одредишну адресу Етернет или Токен ринг пакета и одлучује да ли пакет треба проследити између мрежа, назива се филтрирање. Брзине филтрирања брићева крећу се између 7.000 и 60.000 пакета у секунди.
- **Брзина прослеђивања**: такође се меру бројем пакета или оквира у секунди. Када у процесу филтрирања одлучи да ли ће пакет имати приступ међумрежи или не, врши се операција прослеђивања (forwarding) пакета на међумрежни медијум. Брзине прослеђивања крећу се од 700, па све до 30,000 пакета у секунди за локалне брићеве велике брзине засноване на RISC технологији.

Иако смо о функционалности брида већ говорили у поглављу о међумрежном дизајну, два питања специфична за брићинг треба детаљније објаснити:

- поступање са редундантним путањама и емисионим олујама
- брићинг изворне руте (Source Route Bridging).

Spanning Tree алгоритам Spanning Tree алгоритам (STA) је стандардизован под ознаком IEEE 802.1 у циљу контролисања редундантних путања у брићованим мрежама и спречавања појаве емисионих олуја. Када се више брићева инсталира у комплексним међумрежним аранжманима, може доћи до појаве више активних петљи у мрежној архитектури. Spanning Tree алгоритам (IEEE 802.1), који је обично софтверски имплементиран у брићевима који га подржавају, може да открије вишеструке путање и онемогући све осим једне. Осим тога, ако дође до прекида главне везе између две мреже, STA може да укључи претходно искључену редундантну путању и на тај начин очува међумрежне везе. STA брићеви врше овакво управљање путањама тако што међусобно комуницирају преко **configuration bridge protocol units.** Укупан ефекат STA брићева је да омогућавају све позитивне аспекте редундантних путања у мрежама елиминишући при том све негативне аспекте.

Fast Spanning Tree Време које је spanning tree алгоритму потребно да поново омогући линкове и реконфигурише Етернет мрежу назива се време опоравка (recovery time). Fast Spanning Tree, званично познат као IEEE 802.1w, је унапређење STA које покушава да смањи време опоравка са 30 до 60 секунди на мање од 10 секунди. Смањење времена опоравка је неопходно да би се избегао губитак података и истек

времена сесије на великим свичованим Етернет мрежама. Док FST протокол, познат и као рапидна реконфигурација, не буде завршен, различити произвођачи као што су 3Com, Cisco и Foundry направили су своја решења за проблем реконфигурације. На жалост, ова решења су међусобно некомпатибилна.

Source Route Bridging Бриџинг изворне руте не треба мешати са рутирањем, јер обраду рутинг информација које одређују изабрану путању до одредишне адресе врше изворни уређаји, најчешће умрежени рачунари, а не сами бриџеви. Рачунар шаље специјални **истраживачки пакет** (explorer packet) који одређује најбољу путању до жељеног одредишта. Истраживачки пакети се стално шире кроз бриџеве са изворним рутирањем све док не стигну до одредишне станице. Дуж пута до одредишне станице, сваки бриџ са изворним рутирањем додаје своју адресу у поље информација о рутирању (Routing Information Field – RIF) истраживачког пакета. Одредишна станица шаље комплетирано RIF поље назад изворној станици. Све следеће поруке са подацима садрже предложену путању до одредишта уписану у заглавље токен ринг оквира. Пошто одреди најбољу путању до жељеног одредишта, изворни рачунар шаље поруке са подацима заједно са инструкцијама о путањи до локалног бриџа који их даље усмерава према примљеним инструкцијама.

Поруке са подацима стижу до бриџа са изворним рутирањем заједно са детаљним планом којим путем треба да стигну до одредишта. Једно веома важно правило бриџинга са изворним рутирањем које се примењује у великим мрежама познато је као ограничење 7 скокова (7 hop limit). Због ограниченог простора у RIF пољу, само 7 међуодредишта може бити укључено у путањи до одредишта. Као последица тога, у великим међумрежама често се употребљавају рутери са већим капацитетом табела рутирања.

Да би се избегло загушење мрежа истраживачким пакетима који траже одредиште, бриџеви са изворним рутирањем често примењују неку врсту складиштења адреса (Address Caching) или RIF поља, тако да се претходно одређене путање чувају и поново употребљавају.

Анализа технологије

Бриџеви се могу разврстати на више различитих начина. Можда најважнији критеријум је мрежна архитектура мрежа које се бриџевима повезују. Прво и основно, да ли су две мреже које се повезују Етернет или Токен ринг? Бриџеви који повезују мреже сличног облика везе називају се **транспарентни бриџеви.** Транспарентни бриџеви одликују се следећим карактеристикама:

- промискуитетно слушање, што значи да бриџ прима све пакте података емитоване на мрежама на које је повезан;
- сачувај-и-проследи премошћавање, што значи да се све поруке које нису намењене локалним станицама прослеђују преко бриџа чим је одредишна мрежа доступна;
- учење се постиже испитивањем свих изворних MAC адреса примљених оквира нивоа везе да би бриџ знао које радне станице припадају којој локалној мрежи повезаној на њега;
- IEEE 802.1 алгоритам разгранатог дрвета примењује се да би се управљало путањама између мрежа.

Посебна врста бриџева који садрже конвертере формата служи да међусобно повезивање Етернет и Токен ринг мрежа. Ови бриџеви се називају и **мултипротокол бриџеви** или **преводећи (translating) бриџеви**.

Трећа врста бриџева, слична преводећим бриџевима се користи за повезивање између Етернет и FDDI мрежа. За разлику од преводећих бриџева који морају да обраде и препишу оквир нивоа везе, ови **енкапсулирајући бриџеви** узимају цео Етернет оквир нивоа везе и пакују га у омотницу која одговара протоколима FDDI нивоа везе.

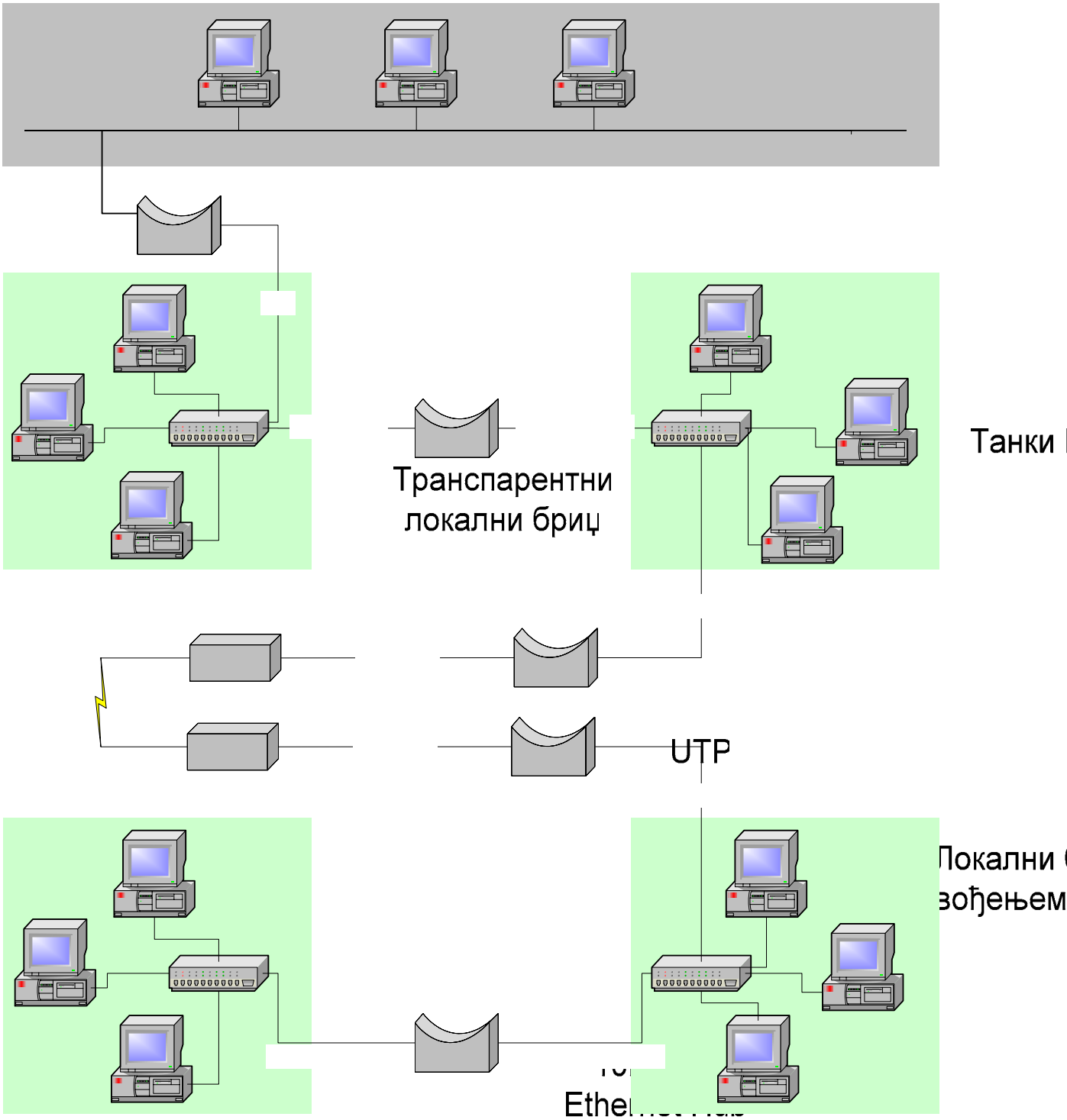
Бриџеви са изворним рутирањем су специјално дизајнирани за Токен ринг мреже које имају могућност изворног рутирања. Немају све токен ринг мреже изворно рутирање, али се оно среће само код токен ринг мрежа. Бриџеви који подржавају везе између токен ринг мрежа са изворним рутирањем, или транспарентних мрежа, називају се транспарентни бриџеви са изворним рутирањем (Source Routing Transparent /STR/ Bridges). Ови бриџеви су у стању да одреде да ли оквире података треба транспарентно проследити или изворно рутирати тако што читају флегове подешене у заглављу оквира нивоа везе.

Слика 8. илуструје типичну инсталацију бриџева, а ***табела 9.*** идентификује нека питања анализе технологије која треба размотрити пре куповине бриџинг технологије.

Бежични бриџеви

Када треба повезати две локалне мреже једне фирме које се налазе на растојању до неколико километара, често се користе WAN везе брзине 56Kbps или веће. Код оваквог решења, поред фиксних трошкова набавке бриџева и остале комуникационе опреме јављају се и месечни трошкови веза у износу од неколико стотина долара. Све популарнија алтернатива оваквом повезивању мрежа које су међусобно удаљене до 5 километара је бежично повезивање (wireless bridging). Бежични бриџеви користе радио пренос spread spectrum технологијом, и тренутно су ограничени само на Етернет повезивање.

Као и већина етернет бриџева, и већина бежичних бриџева подржава spanning tree алгоритам, филтрирање по MAC адресама, заштиту од емисионих олуја, SNMP управљање, енкрипцију и различите Етернет физичке медијуме. И ови бриџеви се морају употребљавати у паровима. Цене се тренутно крећу између $2700 и $14000 долара, при чему највећи број спада у категорију од $4000 до $5000. По овим ценама бежични бриџеви су упоредиви са класичним бриџевима за WAN повезивање, али имају ту предност да уз њих нема додатних месечних трошкова.



Слика 8: Инсталација бриџева

Питање за анализу технологије	**Важност/импликације**
Мрежне архитектуре које треба повезати	• Најчешћи су бриџеви за Етернет и токен ринг • Бриџеви за FDDI, 100BaseT и 100BaseVG су мање уобичајени • Од мрежне архитектуре зависи брзина мреже и подржани медији
Транспарентни бриџеви	• Користе се за повезивање етернет са етернет мрежама, или токен ринг са токен ринг мрежама (без изворног рутирања) • Морају подржавати промискуитетно слушање, сачувај-и-проследи премошћавање, учење, и STA
Преводећи бриџеви	• Најчешће се преводи између етернета и токен ринга • Могу постати озбиљно уско грло некомпатибилности између формата оквира, брзина преноса и дужина оквира
Бриџеви са изворним рутирањем	• Користе се за повезивање две или више токен ринг мрежа са изворним рутирањем • Изворне руте се одређују емитовањем истраживачких пакета • Истраживачки пакети негативно утичу на перформансе мреже • Путање су ограничене на 7 скокова (успутних бриџева)
Транспарентни бриџеви са изворним рутирањем	• Интелигентни бриџеви који могу да разликују између транспарентног и саобраћаја са изворним рутирањем и да сваки премосте на одговарајући начин
Тестирање перформанси бриџева	• Могу се мерити према следећим критеријумима: o Проток: максимални непрекидан пренос без грешака или изгубљених пакета o Степен губитка пакета: проценат изгубљених пакета при максималној теоријској брзини преноса o Латенција: време потребно за обраду једног пакета; односно, кашњење по пакету које бриџ доноси
Локални бриџеви	• Повезују две или више мрежа директно путем мрежних медија • Садрже два или више мрежних интерфејса • Користе се за превођење између различитих медијума
Вишепортни бриџеви	• Садрже више од два мрежна интерфејса • Када бриџ научи на ком је порту одредишна станица, оквире слоја везе прослеђује директно том порту • Ако не зна на ком је порту станица, емитоваће оквир свим портовима осим оног са кога је пакет дошао
Удаљени бриџеви	• Садрже мрежне интерфејсе, као и серијске портове за повезивање WAN на путем модема или CSU/DSU-ова • Већина има једну мрежну картицу и један серијски интерфејс (RS-232 или V.35) • Компатибилан бриџ мора се користити на другом крају везе • Компресија података је веома битна јер је често брзина WAN мања од брзине LAN. Могућ је степен компресије и до 3:1 • SNMP управљачке информације су важне јер омогућавају праћење и управљање бриџевима преко компанијског система за управљање мрежом • Да би се омогућило конфигурисање удаљених бриџева, они морају подржавати Telnet логовање.
WAN сервиси за удаљене бриџеве	• Међу доступним сервисима су 56K DDS, ISDN, T-1 (1.544 Mbps)
Модули који се могу мењати "у лету"	• Неки бриџеви подржавају модуле који се могу мењати у току рада, омогућавајући флексибилност конфигурисања мрежних интерфејса без прекида рада мреже
RISC процесори	• Перформансе директно зависе од брзине процесора у бриџу • RISC процесори дају супериорне резултате
Ранг цена	• 2000$–6000$

Табела 9: Анализа технологије бриџева

РУТЕРИ

Функционалност

Од свих напредних могућности које рутери нуде, можда је најважнија њихова способност да разликују више протокола мрежног слоја. На пример, ако знамо да више протокола може бити уграђено у "омотнице" Етернет нивоа везе, рутер се може програмирати тако да "отвара" омотнице и прослеђује сав NetWare (IPX) саобраћај на једну мрежу, а сав TCP/IP или AppleTalk (AFP) саобраћај на неку другу. У неким случајевима, одређени протоколи могу захтевати приоритетну обраду, због ограниченог времена трајања сесије или временске осетљивости уграђених података.

Рутери су направљени тако да читају специфичне мрежне протоколе и максимизују брзину филтрирања и прослеђивања. Ако рутер треба да рутира само једну врсту мрежног протокола, онда он тачно зна где треба да тражи одредишну адресу и може знатно брже да обрађује пакете. Међутим, када знамо да различити протоколи мрежног слоја имају различиту структуру пакета са одредишним адресама различите дужине и позиције, неки софистицираније рутери познати као **мултипротокол рутери** имају способност да разумеју, обраде и проследе пакете података различитих протокола.

У случају оквира етернет нивоа везе, мултипротокол рутер зна који је протокол мрежног слоја уграђен у поље информација оквира нивоа везе на основу садржаја поља типа (TYPE) у Етернет оквиру.

Ово су неки од најчешћих мрежних протокола и њима одговарајући мрежни оперативни системи или протоколи виших слојева:

- IPX Novel NetWare
- IP TCP/IP
- VIP Banyan Vines
- AFP AppleTalk
- XNS 3Com
- OSI OpenSystems

Остали протоколи које неки рутери могу да обрађују су заправо протоколи нивоа везе који немају адресне схеме мрежног нивоа. Ови протоколи се називају **нерутабилни.** Нерутабилни протоколи се ипак могу обрађивати тако што се рутер понаша као бриџ, или тако што се протоколи виших нивоа нерутабилних оквира нивоа везе енкапсулирају у рутабилне мрежне протоколе као што је IP. Једно време су се специјализовани уређаји који су могли да се понашају као бриџеви или рутери називали **брутери**. Данас, међутим, већина напредних рутера има могућност бриџинга. Ово су неки од нерутабилних протокола и њихова мрежна окружења:

- LAT Digital DECNet
- SNA/SDLC IBM SNA
- NetBIOS мреже под (MS)DOS-ом
- NetBEUI LAN Manager

Протоколи рутирања

Рутери различитих произвођача морају имати начин да међусобно комуницирају и размењују табеле рутирања које описују тренутне услове мрежног саобраћаја. Протоколи рутирања који се користе међу рутерима унутар једне корпорацијске мреже обично се називају **Interior Gateway протоколи**. Сваки мрежни оперативни систем садржи одговарајући рутинг протокол као део свог протокол стека. ***Табела 10.*** илуструје најчешће интерне гејтвеј рутинг протоколе и њима одговарајуће скупове протокола или мрежна окружења.

Рутинг протокол		Мрежно окружење
RIP/RIP2	(routing information protocol)	XNS, NetWare, TCP/IP
OSFP	(open shortest path first)	TCP/IP
NLSP	(NetWare link state protocol)	NetWare 4.1
IS-IS	(Intermediate system to intermediate system)	DECnet, OSI
IGRP	(interior gateway protocol)	Cisco
EIGRP	(enhanced interior gateway protocol)	Cisco
RTMP	(routing table maintenance protocol)	AppleTalk
RTP	(router table protocol)	Vines

Табела 10: Протоколи за комуникацију међу рутерима

RIP (Routing Information Protocol) је дуго времена био најпопуларнији стандард рутер протокола. Данас га је увелико заменио **OSFP, Open Shortest Path First**. OSFP нуди неколико значајних предности у односу на RIP, укључујући способност да ради у много већим међумрежама, а да измене у рутинг табелама имају много мањи утицај на мрежни саобраћај.

Главна разлика између рутинг протокола је у начину или алгоритму којим рутери прикупљају ажурне информације о рутирању. На пример, RIP користи алгоритам **вектора раздаљине** (distance vector), који мери само број скокова (максимално 16) до удаљеног рутера, док OSFP користи много напреднији алгоритам **стања везе** (link state), који врши избор између алтернативних путања не само на основу броја скокова, већ и кашњења, капацитета, протока и поузданости кола која повезују рутере. И што је можда још важније, захтева OSFP много мањи проток за одржавање ажурних табела рутирања.

Рутирање вектором раздаљине захтева да сваки рутер одржава табелу са бројем скокова, који се понекад назива и трошак линка (link cost), између себе и сваког другог доступног рутера. Ове раздаљине се израчунавају коришћењем садржаја табела рутирања суседних рутера, и додавањем раздаљине од себе до рутера од кога је преузета табела са информацијама. Табеле рутирања морају у свако доба бити ажурне да би приказале сваку промену на мрежи. Кључни проблем са вектором раздаљине је што сви рутери не дознају да је дошло до промене на мрежи због кашњења до кога долази јер сваки рутер мора да прерачуна сопствене табеле рутирања пре него што их проследи суседним рутерима. Ово кашњење се назива спора конвергенција.

Протоколи стања везе као што је OSPF (TCP/IP) и NLSP (Netware) су у могућности да превазиђу спору конвергенцију и понуде још нека унапређења перформанси. Једна од важних разлика између ове две врсте протокола је што протоколи вектора раздаљине могу да користе само информације од рутера са којима су непосредно повезани, док протоколи рутирања стања везе користе мрежне информације примљене од свих рутера на датој међумрежи.

Рутинг протоколи стања везе могу да имају комплетнији и ажурнији поглед на целу међумрежу него рутинг протоколи вектора раздаљине придржавајући се следећих основних процедура:

- Рутери стања везе користе специјализоване датаграме познате као **пакети стања везе** (link state packets – LSP) за одређивање назива и раздаљине до суседних рутера и повезаних мрежа;
- Све информације које се о мрежи науче шаљу се свим познатим рутерима, а не само суседним, коришћењем LSP;
- Сваки рутер је одговоран за компајлирање информација садржаних у свим најскорије примљеним LSP пакетима и тако прављење ажурног погледа на стање целе међумреже. Из овог пуног погледа рутинг протокол стања везе је у могућности да одреди најбољу путању до одредишне мреже, као и алтернативне путање са различитим трошковима;
- Ново примљени LSP-ови се одмах прослеђују даље, за разлику од протокола вектора раздаљине код којих се прво мора прерачунати сопствена табела рутирања пре него што се ажуриране информације проследе суседним рутерима. Моментално прослеђивање LSP-ова омогућава бржу конвергенцију у случају прекида везе или додавања нових чворова.

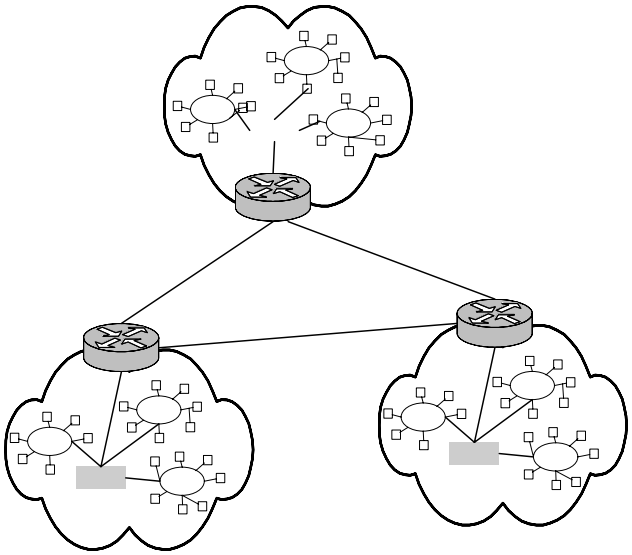
	Вектор раздаљине (Distance Vector)	**Стање везе (Link State)**
Примери	RIPv1, RIPv2, IGRP, EIGRP	OSPF, NLSP, ISIS
Ажурирање	Цела табела рутирања се размењује са суседима сваких 30-90 секунди	Ажуриране путање се шаљу само по потреби
Процесирање	Када прими табелу од суседа, сваки рутер прерачунава све раздаљине	Пакети стања везе се одмах обрађују. Информације садржане у њима користе се за ажурирање погледа на мрежу
Коришћење опсега	Веће	Мање
Коришћење CPU и RAM	Мање	Веће
Метрика	RIP: Број скокова IGRP: Опсег, кашњење, оптерећење, поузданост, МТУ	Трошак, алгоритам најкраћег пута
Предности	• мали захтеви за меморијом и процесорском снагом • једноставнији за имплементацију	• без размене табела рутирања • без лимита броја скокова • опсег везе и кашњење се узимају у обзир • брза конвергенција • подршка за VLSM и CIDR • хијерерхијски поглед на мрежу боље скалира у великим међумрежама
Мане	• не узимају у обзир пропусни опсег када доносе одлуку о рутирању • спора конвергенција • лимит броја скокова 15 • размена целих табела рутирања је неефикасна • не подржавају подмрежне маске променљивих дужина и безкласно рутирање (RIPv1) • Нема хијерархије мреже, слабо скалирање у великим мрежама	• Већа процесорска и меморијска захтевност • Компликованије за имплементацију

Табела 11: Разлика између протокола вектора раздаљине и стања везе

Екстерни гејтвеј протоколи

Док се интерни гејтвеј протоколи користе код рутера унутар дате корпорацијске мреже, **екстерни гејтвеј протоколи (ЕГП)** су неопходни на рутерима који припадају различитим корпорацијским мрежама или **аутономним системима (АС)**. Аутономни систем се прилично слободно дефинише као мрежа под контролом једног ентитета чија су интерна правила рутирања или интерни гејтвеј протоколи (ИГП) независни од оних на другим аутономним системима.

Најчешће коришћен екстерни гејтвеј протокол тренутно је **BGP4 (Border Gateway Protocol Version 4)**. BGP4 је екстерни гејтвеј протокол који врши рутирање између више аутономних система или домена и размену рутинг информација и информација о доступности са другим BGP системима. За спољни свет, сваки АС је јединствен ентитет. Сваки аутономни систем користи своје ИГП независно од осталих АС. Једноставно речено, свака мрежа може да комуницира са сваком другом мрежом на Интернету, због тога што све једно којим језиком интерно говоре, све мреже међусобно говоре истим језиком (BGP). Стриктно говорећи, BGP је **протокол вектора путање** (path vector protocol). То значи да BGP рутери међусобно размењују информације о путањи, представљене скупом АС бројева, којим указују на путање између аутономних система. Правила рутирања у BGP се могу врло прецизно поставити изменом BGP атрибута и подешавањем филтрирања рута. На ***слици 12.*** је једноставан дијаграм који илуструје овај процес.



Слика 12: Аутономни системи и екстерни гејтвеј протоколи

BGP се ослања на TCP за испоруку информација о векторима путања и самим тим се сматра за поуздан протокол. BGP ради по концепту суседних аутономних система. Када се открије суседни аутономни систем, keep-alive поруке се непрестано размењују да би се осигурала видљивост оглашених путања. На тај начин, BGP рутери знају када дође до квара суседног рутера и када информације о вези постану неважеће. Сваки BGP рутер у аутономном систему се конфигурише да оглашава скупне мреже унутар тог АС, и да дефинише са којим ће се рутерима на суседним аутономним системима размењивати информације о векторима путања. Различита тежина се може доделити појединим путањама тако да се једна путања учини атрактивнијом од друге.

У случају аутономних система, статичко рутирање може бити пожељније од динамичког. Пошто се информације о рутирању не деле преко линкова који повезују

различите аутономне системе, знатно се смањује опасност да један лоше подешен рутер из другог аутономног система негативно утиче на рутере датог АС.

OSPF области

Ако је се као ИГП у датој мрежи користи OSPF, онда се уводи додатни ниво у мрежној хијерархији познат као **OSPF област (OSPF Area).** Све OSPF мреже морају имати бар једну конфигурисану област, познату као област 0 или кичмена област (backbone area). У зависности од величине мреже, да би се тополошка база података одржала у прихватљивим оквирима и да би се смањила количина OSPF информација које се преносе између рутера, могу се дефинисати додатне области. Све области међусобно комуницирају кроз нулту област.

Приватно адресирање и превођење мрежних адреса

Као што је претходно поменуто, рутери доносе одлуке о прослеђивању на основу информација садржаних у табелама рутирања. Те информације су организоване према бројевима подмрежа (subnets) које представљају скуп ИП адреса организованих у логичке групе. Пошто све више и више организација и појединаца желе да буду повезани у корпорацијске мреже или Интернет, потребе за ИП адресама су експоненцијално расле. Недостатак ИП адреса је резултат експлозивног раста интернета, као и неефикасног коришћења постојећих адреса условљеног класним (classfull) адресирањем. Један од начина превазилажења проблема недостатка ИП адреса је коришћење **приватног адресирања.**

Када се једна организација повезује на Интернет, њена ИП адреса мора бити глобално јединствена. У највећем броју случајева, ову доделу глобално јединствених адреса врши провајдер интернет услуга (ISP) организације.

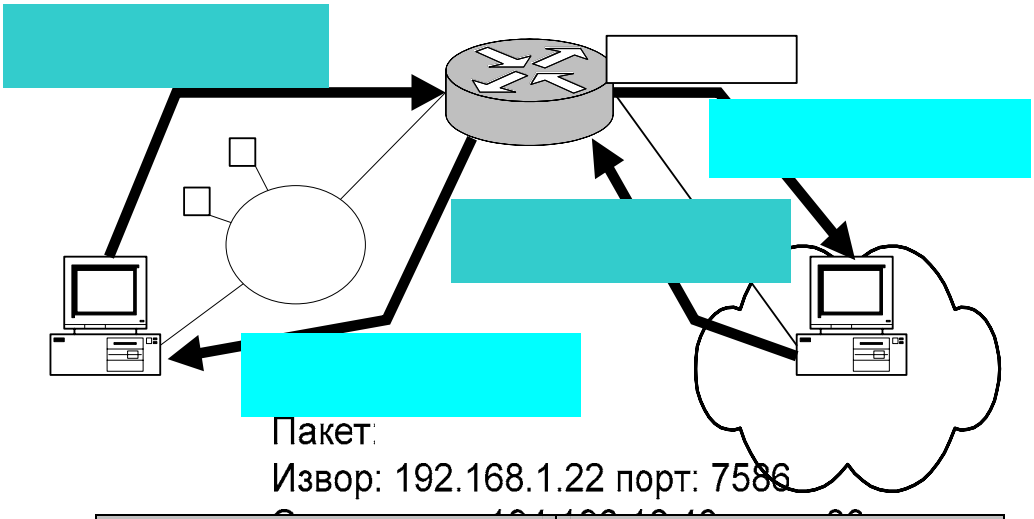
Међутим, за саобраћај који остаје унутар организације не морају се користити глобално јединствене адресе, већ је довољно да адресе буду јединствене у оквиру приватне мреже организације. У ту сврху, Internet Assigned Numbers Authority (IANA) је издвојила следећа три опсега приватних ИП адреса:

10.0.0.0–10.255.255.255	(еквивалент једне А класе мрежних адреса)
172.16.0.0–172.31.255.255	(еквивалент 16 узастопних Б класа адреса)
192.168.0.0–192.168.255.255	(еквивалент 256 узастопних Ц класа адреса)

Саобраћај на преко ових мрежних адреса мора остати унутар приватне мреже организације. Пошто је свима омогућено коришћење ових адреса, оне нису глобално јединствене, па се не могу користити на Интернету.

Рачунари на мрежи која користи приватне ИП адресе ипак могу да шаљу и примају садржај са Интернета користећи **превођење мрежних адреса (Network Address Translation – NAT)**. Превођење мрежних адреса врши рутер или самостални софтвер инсталиран на серверу са више мрежних картица (Multihomed Server). Овај термин се користи да означи сервер који има једну мрежну картицу која има адресу која припада приватном ИП адресном простору, и другу мрежну картицу којој је додељена глобално јединствена ИП адреса. Један од програма који врши ту функцију под Linux системима назива се IP Masquerade, док за Windows NT постоји верзија под називом WinRoute. Додатна предност NAT-а је да приватна мрежа организације није видљива са

Интернета. ***Слика 13.*** илуструје како коришћење мрежног превођења омогућава организацији коришћење приватног адресирања задржавајући при томе користи глобалног Интернет повезивања.



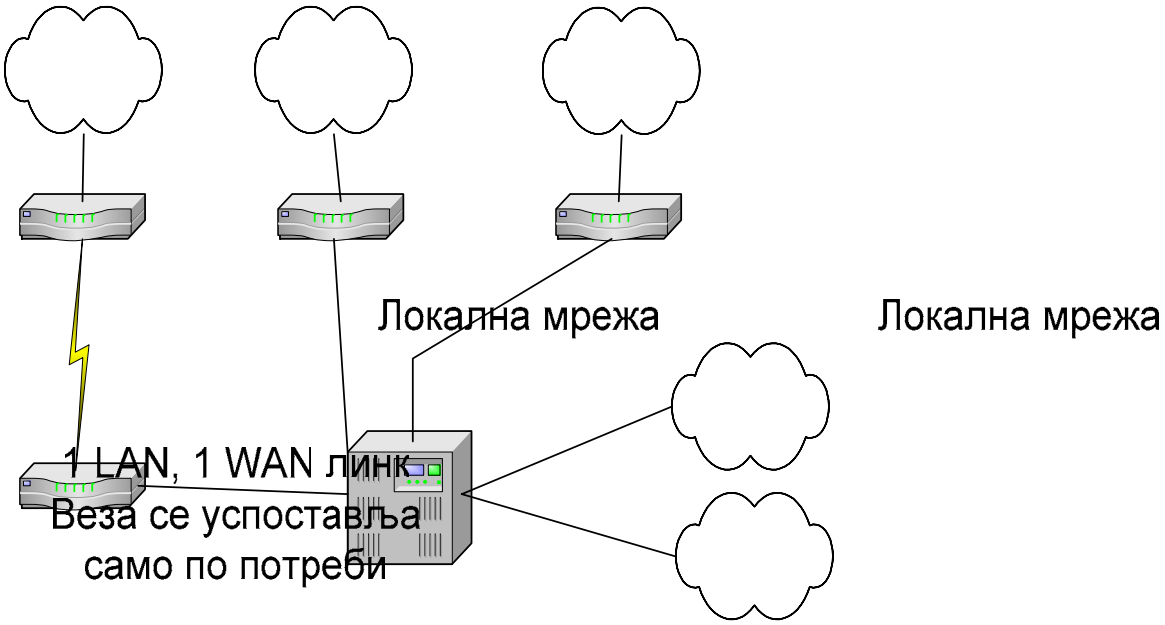
Приватна ИП адреса извора	Приватни порт додељен извору
192.168.1.22	61001
192.168.1.23	61002
192.168.1.24	61003
192.168.1.25	61004
итд..	итд.

Слика 13: Превођење мрежних адреса (NAT)

Као што се на слици може видети, све радне станице на мрежи деле исту ИП адресу (195.75.16.65) на глобалном Интернету тако што NAT софтвер одржава табелу конекција и мапира сваку приватну радну станицу на јединствени TCP порт. У случају WinRoute софтвера, ови портови су из опсега 61000–61600, да не би долазило до мешања са често коришћеним портовима.

Анализа технологије

Најзначајнији фактор разлике између рутера је директно везан за локацију на којој ће се рутер налазити и везане захтеве рутирања. Као резултат тога, **рутери за централне локације** *(central site routers)*, познати и као *enterprise* или *backbone* рутери се примењују у великим корпорацијским седиштима, док се **гранични** *(boundary, branch office)* рутери примењују на удаљеним локацијама које имају мање захтеве за рутирањем и мање расположивог техничког особља. За пословнице чија количина међумрежног саобраћаја не оправдава стални проток саобраћаја и више трошкове изнајмљених линија, користе се **dial-up** рутери (најчешће ISDN). **Слика 14.** илуструје инсталацију различитих типова рутера.



Слика 14: Инсталација рутера

Гранични рутери У случају граничних рутера, све рутинг информације чувају се у рутеру централне локације. Ово омогућава граничним рутерима да буду мање захтевни по питањима техничке конфигурације и да буду јефтинији од рутера за централне локације. Гранични рутери често имају само два мрежна интерфејса, један за ЛАН и један за WAN везу. Логика код граничних рутера је прилично једноставна. Сви локално генерисани пакети који имају одредиште на локалној мрежи се игноришу, док се пакети којима одредиште није локално прослеђују преко WAN везе до рутера на централној локацији на даљу обраду.

Очигледно ограничење такве топологије је да нема директне комуникације између граничних рутера, и да због тога мора постојати редундантност код рутера на централној локацији јер се цела међумрежна комуникација на њих ослања. Такође, гранични рутери једног произвођача морају бити упарени са одговарајућим централним рутерима истог произвођача јер тренутно не постоје стандарди за међусобну комуникацију у оваквим конфигурацијама. ***Табела 15.*** илуструје нека питања анализе технологије која треба размотрити код граничних рутера.

Питање за анализу технологије	**Важност/импликације**
Рад са нерутабилним саобраћајем	• Морају радити са нерутабилним протоколима као што су SNA/SDLC и NetBIOS • Морају подржавати временска ограничења као што је ограничење временског одзива код SDLC
Подршка за даљинско конфигурисање	• Морају имати подршку за даљинско конфигурисање • Морају имати могућност ажурирања софтвера са централне локације
SNMP компатабилност	• Морају подржавати SNMP управљачке информације за интеграцију са системима компанијског управљања мрежом
Подржани WAN сервиси	• Могу бити следећи: 56K DDS, T-1, Frame Relay
Подршка за Frame Relay	• Ако се користи Frame Relay као WAN услуга, може ли уређај подржати контролне механизме који спречавају губитак пакета?
Резервни WAN сервиси	• Могу ли се користити комутирани WAN сервиси као резерва у случају пада главне линије? • Примери: ISDN, асинхрони dial-up, PPP

Питање за анализу технологије	Важност/импликације
Подржани WAN протоколи	• Примери: HDLC, X.25 Frame Relay, PPP
Подржане LAN архитектуре	• Примери: Ethernet, Token Ring, остале
Рутирани LAN протоколи	• пример: IP, IPX, DECnet, AppleTalk, Vines, XNS, OSI
Филтрирани LAN протоколи	• Неки мрежни протоколи су веома "брбљиви" и беспотребно троше скупи WAN линк • Гранични протоколи треба да филтрирају ове протоколе и одстране их са WAN линка: SAP, RIP, NetBIOS емисије, истраживачке пакете изворног рутирања

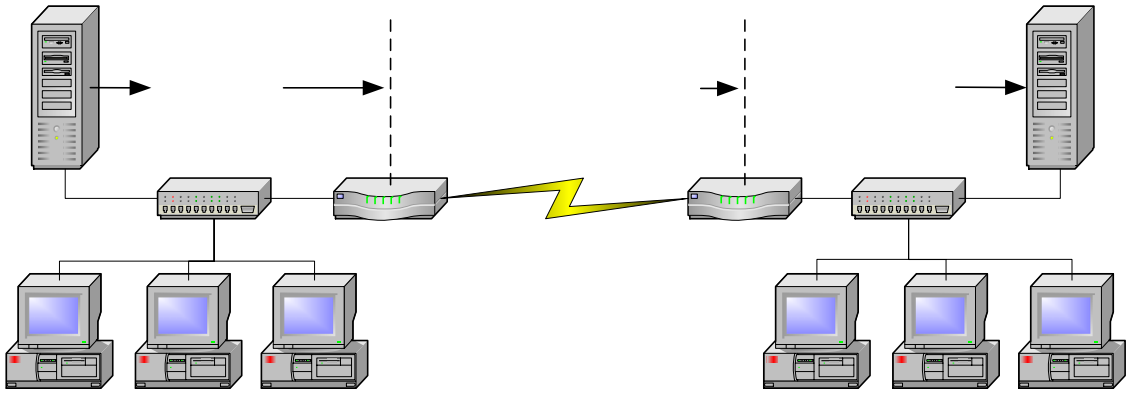
Табела 15: Анализа технологије граничних рутера

Dial-up рутери Ако количина међумрежног саобраћаја не оправдава трошкове изнајмљених линија, рутери за везе са бирањем бројева (dial-up) могу бити одговарајући избор међумрежне опреме. Ово је нарочито тачно ако је на оба краја везе расположива дигитална веза по позиву позната као ISDN (Integrated Services Digital Network). ISDN BRI (basic rate interface) омогућава до 128 Кб/с протока по потребни, док ISDN PRI (primary rate interface) омогућава до 1.536 Мб/с корисног дигиталног протока по потреби. Тренутно не постоје стандарди међуоперабилности између ISDN рутера, па се због тога они увек морају куповати у пару од истог произвођача.

Поред свих осталих техничких карактеристика које су важне за граничне рутере, можда најважнија особина рутера за везе са бирањем бројева је тзв. **Spoofing.** То је метод филтрирања "брбљивих" или нежељених протокола са WAN везе при чему се осигурава да удаљени програми који захтевају сталну комуникацију преко ових филтрираних протокола те податке ипак добију емулацијом ових протокола на локалном рутеру. Међу протоколима који се највише морају филтрирати су:

- RIP (Routing Information Protocol): NetWare, TCP/IP
- SAP (Service Advertising Protocol): NetWare
- Watchdog, познат као keep-alive поруке: NetWare
- Serialization (проверава дупле серијске бројеве): NetWare

Разлог зашто је филтрирање толико важно је што ови протоколи лако могу успоставе везу или да је држе отвореном, што може довести до непотребно великих трошкова. **Spoofing** као комбинација филтрирања и емулације приказан је на ***слици 16.***



Слика 16: Spoofing код dial-up рутера

Повремено, ажуриране информације као што су статус сесије или доступност сервиса морају се разменити између рутера за везе по позиву, да не би дошло до грешака у рутирању или нерегуларног прекида сесија. Начин на који се врши размена ових информација може значајно утицати на ефикасност рутера за везе по позиву и висину трошкова за коришћење комуникационих веза. Важно је запамтити да ови рутери међусобно комуницирају само преко веза по позиву и би било веома неекономично успостављати или одржавати везу при сваком ажурирању ових информација.

Различити рутери користе различите механизме ажурирања. Три основна метода ажурирања су:

- **Временско ажурирање** (timed updates), обавља се у предефинисаним временским интервалима
- **Окинуто ажурирање** (triggered updates) се обавља кад год се деси одређен програмирани догађај, као што је измена у доступности сервиса, и
- **Успутно ажурирање** (piggyback updates), које се врши само када је веза већ успостављена за размену података корисника.

Остала питања анализе технологије ISDN рутера приказана су у ***табели 17.***

Питање за анализу технологије	Важност/импликације
Категоризација	• ЛАН модеми: мање од 24 корисника, локална мрежа, BRI ISDN по позиву, дељена IP адреса • Рутери за филијале: подршка за глас, више од 24 корисника, подржавају рутинг табеле, заштитне баријере и виртуелне приватне мреже
Аутоматска SPID детекција	• SPID (Service Provider Identifier Number) се мора подесити на рутеру. Неки рутери сами препознају и подешавају SPID
Прикривање гласа	• Поједини провајдери наплаћују више за пренос гласа преко ISDN-а. Ово се може избећи ако рутер подржава прикривање гласа у виду података на Б каналу
Превођење мрежних адреса	• Омогућава да се једна ИП адреса дели између више радних станица на интерној мрежи
Опсег по потреби	• Међу протоколима који би требало да буду подржани су MLPPP (Multilink PPP) и BACP (Bandwidth Allocation Control Protocol)
Транспортни протоколи	• Сви подржавају IP, неки и IPX и/или AppleTalk
Рутинг протоколи	• Већина ISDN рутера подржава само RIP, евентуално RIP2
Сигурност	• Неки имају уграђене могућности заштитне баријере (Firewall)
Компресија	• Због ограниченог пропусног опсега ISDN -а, важно је до максимума га искористити компресијом података. Рутери се разликују по броју подржаних алгоритама компресије
Број портова	• ISDN рутери се разликују по броју интегрисаних етернет и гласовних аналогних портова

Табела 17: Анализа технологије ISDN рутера

Еволуција рутирања

Иако нико засигурно не може рећи шта доноси будућност у међумрежном дизајну и технологијама, већина се слаже да ће се у догледној будућности све више користити комбинација свичинга и рутирања. Иако је свичинг одличан за обезбеђивање великог протока у локалном мрежи, то је ипак технологија 2. слоја која не може да понуди

могућности напредног филтрирања, сигурности и међумрежне сегментације које су везане за технологије рутирања 3. слоја.

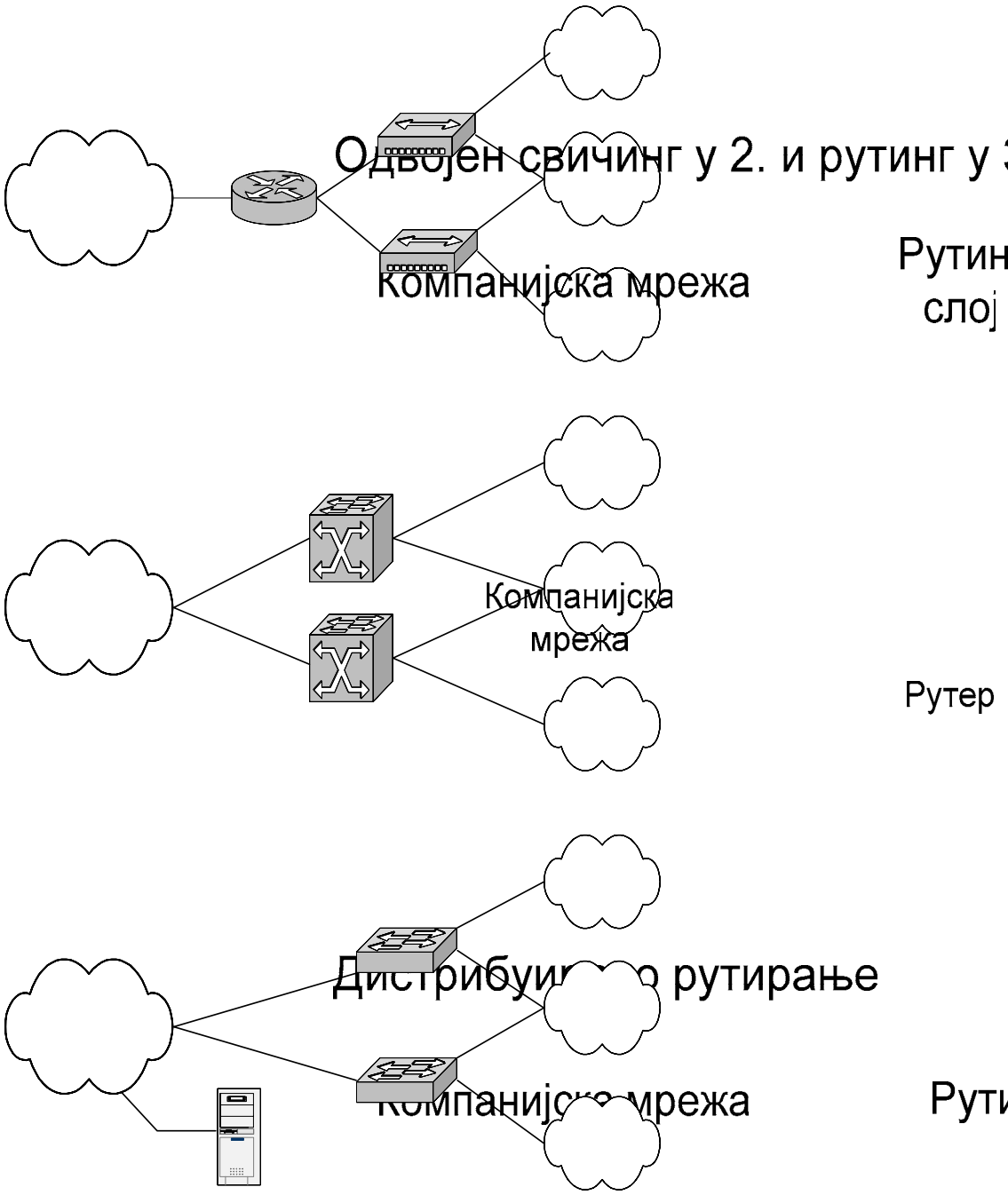
Ово су три могућа сценарија еволуције међумрежног дизајна:

- **Одвојени свичинг у 2. и рутирање у 3. слоју**, при чему одвојени свичеви 2. слоја и рутери 3. слоја сарађују тако што свако обавља свој део посла, и на тај начин доприносе максималној ефикасности испоруке међумрежног саобраћаја;
- **Дистрибуирано рутирање**, где су функционалности свичева 2. слоја и рутера 3. слоја комбиноване у једном уређају који се обично назива **вишеслојни** (multilayer) или **свич 3. нивоа** (layer 3 switch).
- **Сервери рута** ће обезбеђивати централизовану базу рутинг информација, док ће **ивични** (edge) **свичеви** унутар локалних мрежа бити програмирани са минимумом информација о рутирању. Ивични свичеви ће консултовати дистрибуиране сервере рута кад год дођу у ситуацију да немају одговарајуће информације које су им потребне за рутирање. У овом сценарију, информације о рутирању и процесни overhead се држи на минимуму у локалним свичевима, који су пре свега одговорни за пружање максималног локалног протока.

На различите начине, сваки од ових сценарија у будућности примењује међумрежни дизајн описан популарном изреком: "Свичуј кад год можеш, рутирај кад мораш". Ова три сценарија међумрежног дизајна илустрована су на ***слици 18.***

Терабитни рутери Још један аспект еволуције рутера се значајно повећање процесне моћи рутера. Такви рутери се називају различитим именима, као што су **терабит рутери**, **wire-rate** или **wire-speed** рутери. Такви рутери могу да обаве преко 40 милиона упита рута у секунди и имају укупан проток који се креће између 10 и 160 гигабита у секунди. Максималан теоријски капацитет таквих уређаја износи и до 184 терабита у секунди. Међутим, да би се дошло до стварног максималног корисног капацитета, треба помножити максималан број портова на једном уређају са максималном брзином порта. Ови рутери могу да подрже различите мрежне интерфејсе као што су гигабит Етернет, ATM, и SONET (OC-48). Међу произвођачима терабит рутера су Argon, Avici, Charlotte's Web, Cisco, Juniper, Lucent, NetCore, Nexabit, Nortel, Packet, Pluris и други.

ИП свичинг и квалитет услуге (Quality of Service) Још један могући сценарио комбиновања свичинга и рутирања је познат као **ИП свичинг.** Имплементацијом ИП рутинг софтвера директно у ATM свичинг хардверу, ИП свичинг комбинује могућности свичинга и рутинга у једном уређају који прави разлику који је саобраћај потребно свичовати а који рутирати. За текући (streaming) саобраћај као што је пренос фајлова или мултимедијалне сесије, успостављају се ATM свичована виртуелна кола, која дозвољавају да саобраћај тече без типичне пакет-по-пакет обраде која се везује за рутирање. За connectionless датаграме и краће преносе, примењује се софтвер за ИП рутирање. Протоколе који одређују који саобраћај треба да буде свичован, а који рутиран су предложиле бар три компаније, и треба да буду размотрени од стране организације IETF (Internet Engineering Task Force). Први предложени протоколи су *Flow Management Protocol* фирме IPsilon Networks, *Tag Distribution Protocol* фирме Cisco и *Aggregate Route-Based Switching* предложен од стране IBM. IPsilon је једна од првих фирми која је представила ИП свичинг, а касније ју је купила Nokia. Cisco таг свичинг протокол постао је познат под именом **MPLS (Multiprotocol Label Switching**) када га је IETF узео у разматрање.



Слика 18: Сценарији еволуције рутера

.

Иако је MPLS изворно био намењен за коришћење у свичованим међумрежним окружењима, домен његове примене проширен је тако да укључује и Интернет. MPLS пружа следеће функционалности:

- Користи ознаке (labels) за прављење пречица између специфичних кола за брзо рутирање без потребе за типичним пакет-по-пакет упитима табеле рутирања
- Ознаке се такође користе за захтеве квалитета услуге (QOS) или виртуелне приватне мреже преко Интернета

- Дефинисан је за коришћење преко Frame Relay, ATM и PPP (point-to-point protocol) WAN веза, као и IEEE 802.3 локалних мрежа
- Подржава експлицитно рутирање, које дозвољава да одређена врста саобраћаја, видео на пример, буде експлицитно додељена одређеном колу.

Међутим, ова последња функционалност може успорити прихватање MPLS. Cisco и Juniper Networks фаворизују коришћење RSVP (Resource Reservation Protocol) за имплементирање експлицитног рутирања, док су други произвођачи као што су Nortel и Ericsson за коришћење LDP (Label Distribution Protocol).

Као потпуна алтернатива MPLS јавља се **Diff-Serv (Differentiated Services**) који припрема још једна IETF радна група. Diff-Serv пружа следеће функционалности:

- Користи битове врсте услуга (Type of Service, ToS) који већ постоје у заглављима ИП пакета за обезбеђивање различитих нивоа услуга различитим апликацијама
- Подржава договоре о нивоу услуга (service level agreements) између корисника и провајдера услуга.

Ако користимо OSI модел за разликовање MPLS и Diff-Serv, треба имати у виду да је MPLS решење другог, а Diff-Serv решење трећег слоја. Из тог разлога, ова два стандарда нису у међусобној конкуренцију, иако их неки тако доживљавају. MPLS, услуга 2. слоја радиће са или без Diff-Serv у 3. слоју. Заправо, најбоље решење може бити да оба протокола заједно раде, при чему би MPLS укључивао свичинг ознаке за доделу кола након испитивања ToS битова у ИП заглављу 3. слоја.

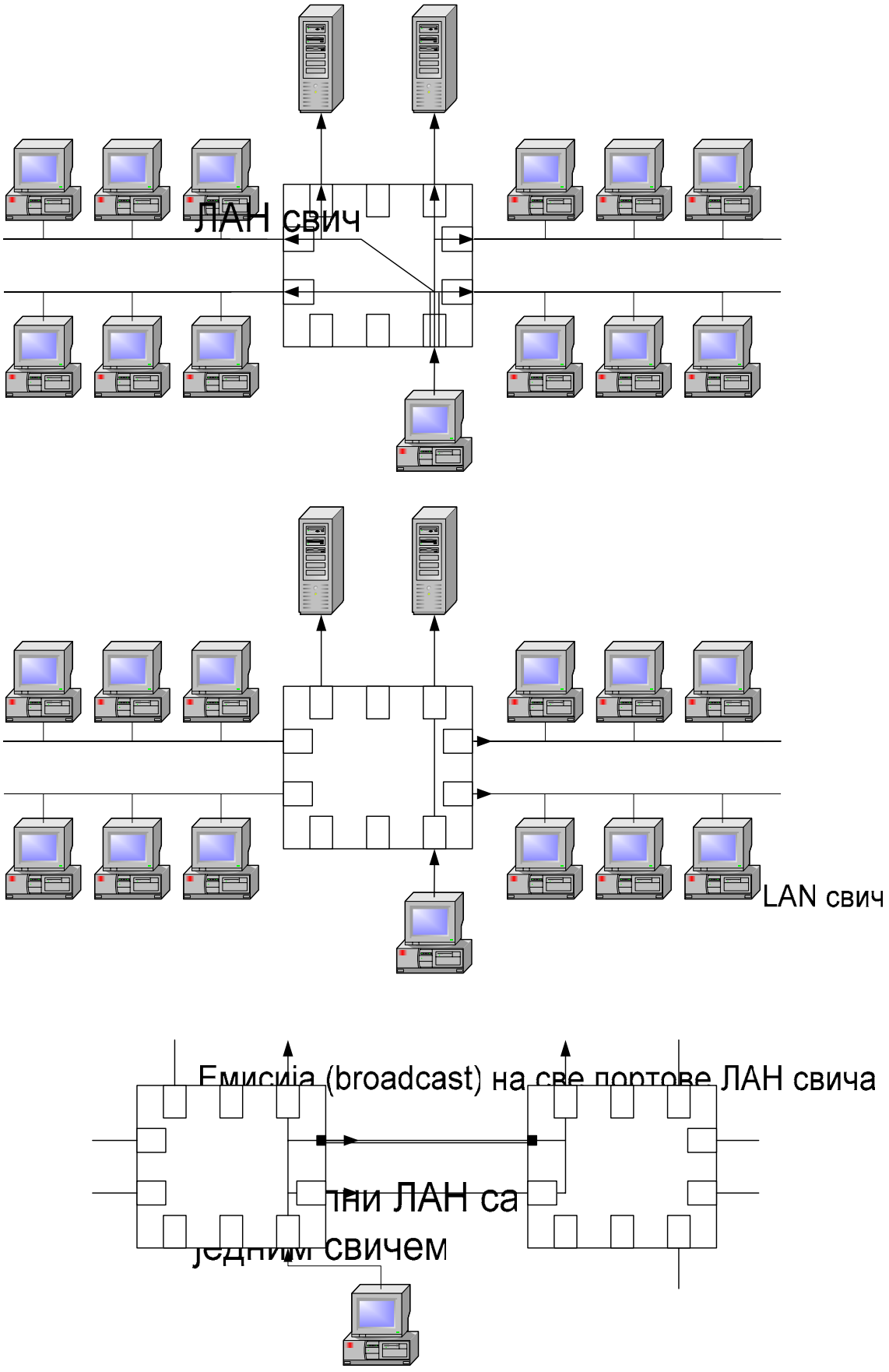
СВИЧЕВИ И ВИРТУЕЛНЕ ЛОКАЛНЕ МРЕЖЕ (VLAN)

Основна функционалност

Логички мрежни дизајн познат као виртуелне локалне мреже (Virtual LANs) зависи од физичког уређаја, ЛАН свича, за своју функционалност. Иако су први ЛАН свичеви испоручивали велики пропусни опсег локалним радним станицама и сегментима, они нису имали могућност партиционисања свича у више одвојених емисионих зона и сегментирања корисника у одговарајуће одвојене радне групе.

Виртуелне локалне мреже се софтверски дефинишу преко конфигурационог софтвера садржаног у мрежном свичу. Коришћење виртуелних мрежа дозвољава да се чланови радних група једноставно и брзо додељују једној или више група по потреби. Самим тим, свакој радној групи се додељује одређени део капацитета свича. Свичеви који подржавају виртуелне локалне мреже користе функционалност бриџинга у 2. OSI слоју за логичко сегментирање саобраћаја унутар свича у различите виртуелне мреже.

Свака порука намењена локалној радној станици коју свич прими прослеђује се одредишној станици преко индивидуалне свичоване конекције. Кључна разлика између свичева који подржавају виртуелне мреже и оних који их не подржавају је у третману broadcast и multicast порука. У виртуелним мрежама, оне су ограничене само на чланове те виртуелне мреже, уместо да се прослеђују свим повезаним уређајима. Овим се спречава ширење података на целу мрежу и смањује мрежни саобраћај. Да поједноставимо, виртуелне локалне мреже су ништа друго до логички дефинисане broadcast/multicast групе унутар свичева 2. слоја, јер се саобраћај од-тачке-до-тачке обавља преко посвећених свичованих конекција.



Слика 19: LAN свичеви и виртуелне локалне мреже

Ограничења

Кључно ограничење виртуелних мрежа је да када су чланови исте виртуелне мреже повезани на различите мрежне свичеве, информације о конфигурацији морају се делити између свичева. Тренутно не постоје стандарди за пренос или дељење информација о виртуелним мрежама између различитих мрежних свичева. Због тога се могу користити само специфични протоколи појединих произвођача за комуникацију између свичева тог истог произвођача у виртуелној мрежи са више свичева.

Управљање и праћење виртуелних локалних мрежа знатно је компликованије него код класичних мрежа пре свега због зависности виртуелне мреже од мрежних свичева за физичко повезивање. Пошто се свичоване везе успостављају, користе и прекидају у току од неколико микросекунди, тешко је ако не и немогуће пратити ове везе у реалном времену уобичајеним средствима. Једно од решења је познато као дупликација саобраћаја где се саобраћај између два свичована порта дуплицира на трећи порт на који се прикључује стандардни анализатор локалних мрежа.

Пренос између мрежних свичева 2. слоја

Међу алтернативним методама које произвођачи свичева користе за дељење информација о виртуелним локалним мрежама између свичева 2. слоја издвајају се следеће:

- **Сигналне поруке (Signaling Message)**: када се нова радна станица појави на мрежи, свичеви један другог обавештавају о њеној MAC адреси и броју виртуелне мреже. Да би информације свих свичева биле синхронизоване, свичеви периодично емитују своје табеле виртуелних мрежа осталим свичевима. На већим свичованим мрежама, ова емитовања могу да доведу до значајног пораста мрежног саобраћаја.
- **Обележавање оквира (Frame Tagging)**: сваком оквиру слоја података који путује између два свича додаје се "привезак" са бројем виртуелне мреже изворне станице. На тај начин, пријемни свич одмах зна којој радној станици виртуелне мреже треба да се проследи примљени оквир. Једна од тешкоћа са обележавањем оквира што се додавањем битова може премашити дозвољена дужина оквира у протоколу слоја мреже, па се морају користити додатни методи за превазилажење овог ограничења.
- **Временско мултиплексирање**: Свакој виртуелној мрежи додељује се одређени део опсега доступног свичу. Додељени опсег може да користи само виртуелна мрежа којој је опсег додељен. На тај начин, свака виртуелна мрежа има виртуелни приватни backplane и не долази до мешања саобраћаја различитих приватних мрежа. Међутим, додељен а неискоришћен опсег не може се делити између осталих виртуелних мрежа.

Једна од могућности за стандардизацију комуникације између свичева за подршку виртуелним мрежама које обухватају више свичева је коришћење **IEEE 802.10** стандарда. Изворно замишљен као стандард за сигурну размену података на локалним мрежама који би омогућио радним станицама да подешавају енкрипцију и аутентикације, овај стандард је интересантан за произвођаче VLAN свичева због додатка 32-битног заглавља постојећим оквирима MAC подслоја. Уместо да чува само сигурносне податке, ово додатно 32-битно заглавље може да носи идентификаторе

виртуелних мрежа. Да би се превазишла ограничења максималне дужине оквира слоја везе, IEEE 802.10 такође укључује спецификације за сегментирање и поновно састављање сваког оквира уколико он због додатног 32-битног заглавља премашује максималну дозвољену дужину.

Пренос између виртуелних мрежа

Виртуелне мреже се граде коришћењем ЛАН свичева који су уређаји 2. OSI слоја и у стању су само да праве разлику између адреса MAC слоја. Као резултат тога, свичеви су у могућности само да користе "проследи-ако-није-локално" међумрежну логику преузету од бриџева. За селективан пренос саобраћаја између виртуелних мрежа, потребна је функционалност рутера. Она се може обезбедити коришћењем екстерних рутера, или уградњом специјализованог рутинг софтвера у ЛАН свичеве. ЛАН свичеви са могућностима рутирања називају се називају се свичеви 3. слоја (layer 3 switches). Пошто саобраћан је може да тече између виртуелних мрежа без рутирања, , захваљујући могућностима филтрирања успутних рутера овакав дизајн виртуелних мрежа може да понуди и могућност постављања заштитних баријера (firewall-a) .

Класификација виртуелних мрежа

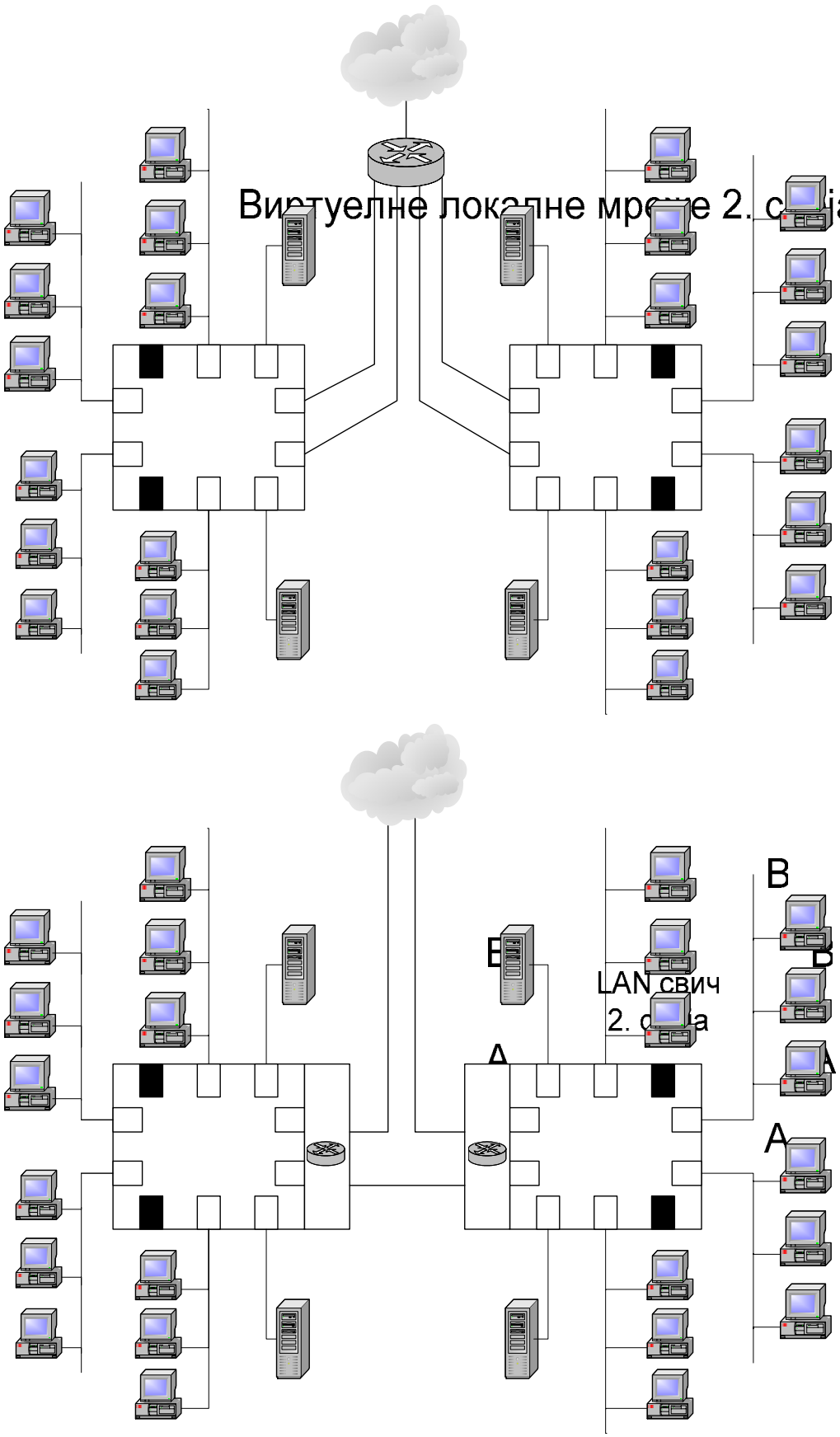
Виртуелне мреже се обично класификују према највишем слоју OSI протокола коме по функционалности одговарају.

Виртуелне мреже 2. слоја граде се коришћењем ЛАН свичева који се понашају као микросегментирајући бриџеви. Заправо, може се рећи да **свич 2. слоја** није ништа друго до вишеулазни бриџ.ЛАН свич који подржава виртуелне мреже 2. слоја прави разлику само на основу MAC адресе повезаних радних станица. Он не може да прави разлику између протокола трећег, мрежног слоја. На сваки улаз свича може се повезати једна или више радних станица.

Виртуелне мреже 3. слоја се граде коришћењем свичева који могу да обрађују и мрежне адресе 3. слоја. Такви уређаји се називају **рутирајући свичеви** или **свичеви 3. слоја.** Пошто могу да врше филтрирање на основу адреса и протокола мрежног слоја, у могућности су да подрже више виртуелних мрежа које користе различите протоколе слоја мреже.

Другим речима, једна виртуелна мрежа може да подржава само TCP/IP, док друга подржава само IPX/SPX. Пошто свичеви 3. слоја разумеју адресне схеме 3. слоја, у могућности су да користе подмрежне бројеве уграђене у адресе 3. слоја за организовање виртуелних мрежа. Пошто се ови подмрежни бројеви претходно додељују станицама, неки свичеви су у стању да пошаљу упит свим повезаним станицама и да на основу ових подмрежних бројева аутоматски конфигуришу или повежу станице у одговарајуће локалне мреже. Радне станице које користе нерутабилне протоколе као што су LAT, NetBEUI или NetBIOS такође се могу одвојити у посебне виртуелне мреже.

Слика 20. илуструје разлике у архитектури између виртуелних мрежа 2. и 3. слоја, а ***табела 21.*** показује функционалне разлике.



Слика 20: Поређење архитектуре свичева 2. и 3. слоја

Карактеристике виртуелне мреже	Функционалност 2. слоја виртуелне мреже	Функционалност 3. слоја виртуелне мреже
Конфигурација	Једноставнија	Тежа
Трошкови	Јефтиније, али захтева додатни рутер	Скупље, али има уграђене могућности рутирања
Перформансе	Брже јер обрађују само адресе 2. слоја	До 30% спорије јер морају да обрађују протоколе 3. слоја
Нерутабилни протоколи	Нису проблем јер су уређаји 2. слоја	Могу се одвојити у посебан сегмент или нису подржани
Рутабилни протоколи	Не праве разлику између протокола 3. нивоа	Могу да разликују између протокола 3. нивоа и праве одвојене ВЛАН-ове на основу њих; разликују се по броју подржаних протокола
Виртуелне ЛАН са више свичева	Користе нестандардну комуникацију између свичева, што повећава загушење мреже	Користе подмрежне бројеве и адресама мрежног слоја за виртуелне мреже без потребе за нестандардним протоколима
Опште емисије	Емитују свим сегментима који припадају одређеној виртуелној мрежи	Емитују само одговарајућим подмрежама на виртуелној локалној мрежи
Филтрирање	Филтрирање по адресама или протоколима мрежног слоја није могуће	Филтрирање могуће по адресама или протоколима мрежног слоја у циљу сегментирања и веће сигурности
Могућност рутирања	Обезбеђује их спољни рутер	Омогућене уграђеним рутинг софтвером који омогућава управљање саобраћајем и изолацију протокола. Неки свичеви подржавају RIP и OSPF

Табела 21: Функционално поређење виртуелних локалних мрежа 2. и 3. слоја

Реалности виртуелних мрежа – у основи

Виртуелне локалне мреже су у почетку сматране за коначно решење за повећање управљивости локалним мрежама и контролу саобраћаја. Спроводећи концепт "рутирај једном, свичуј много", VLAN технологије су обећавале пораст перформанси уз смањење потреба за управљањем.

У почетку базираним на референтном OSI моделу технологија свичинга 2. слоја, виртуелним мрежама били су потребни одвојени уређаји – рутери 3. слоја за усмеравање саобраћаја између виртуелних мрежа. Да би се ослободили ове зависности, рутерима 2. слоја су додате могућности рутирања.

ЛАН свичеви који имају могућност рутирања, познати и као свичеви 3. слоја или рутинг свичеви, врше уобичајен процес рутирања првог пакета у серији, додају одредишну адресу 2. слоја (MAC) у табелу адреса, и свичују остале пакете у 2. слоју. Поред тога што група свичева може да опслужи сав саобраћај унутар виртуелних локалних мрежа, свичеви 3. слоја врше рутирање између сегмената локалне мреже много брже него класични рутери.

Како је технологија свичинга 3. слоја напредовала, тако су јој додаване могућности анализе тока саобраћаја на основу врсте тока (дефинисаног бројем порта). Тако настали свичеви 4. слоја обезбеђују могућност рангирања саобраћаја по приоритетима на основу врсте саобраћаја, повећавају сигурност филтрирањем и сакупљају статистике саобраћаја на нивоу апликација по сваком појединачном порту.

Иако су обећања о повећаној контроли саобраћаја у потпуности испуњена, побољшање управљивости није било толико успешно. Када пакет треба испоручити VLAN чвору који је на другом физичком свичу, тада се морају имплементирати начини утврђивања локалне мреже којој се пакет треба испоручити.

Једно од највећих питања у имплементацији виртуелних локалних мрежа је кашњење стандарда за управљање таквом идентификацијом пакета. У недостатку јасних стандарда, различити произвођачи имплементирали су различита индивидуална решења. Са тренутно постојећим технологијама, произвођачи нису вољни да своја појединачна решења замене новијим стандардним решењима као што је 802.10 обележавање пакета. Као резултат, VLAN решења су обично ограничена на коришћење решења истог произвођача. Управљивост се знатно разликује од произвођача до произвођача, па се тако не може дати дефинитиван одговор о управљивости виртуелних локалних мрежа.

Поред тога, неколико значајних технолошких иновација се десило од појаве VLAN технологија. Промене како у нормалним мрежним окружењима, тако и у технологијама рутирања утицале су на исплативост виртуелних локалних мрежа.

Један од главних разлога за имплементирање виртуелних локалних мрежа традиционално је била контрола мрежног емисионог (broadcast) саобраћаја. Емисиони саобраћај је често садржао висок ниво оптерећујућег саобраћаја због ARP, RIP и SAP емисија. Повремено би код мрежних чворова долазило до грешке и они би изнова понављали ове емисије, трошећи тако значајан део опсега. Контрола ових емисионих активности била је важна јер је мрежни опсег био веома ограничен. Поред проблема са капацитетом мреже, сваки емисиони пакет би проузроковао да га анализира протокол стек сваког повезаног чвора на мрежи, генеришући тако прекиде и трошећи циклусе централног процесора.

Истраживања, међутим, указују да контрола емисија више није тако велики проблем као што је некада био. Новији мрежни софтвер има оптимизованију ARP функционалност, RIP се убрзано мења ефикаснијим протоколима рутирања, а IPX и његове SAP емисије све више се мењају ИП-ом. Поред смањења учесталости мрежних емисија, дошло је и до повећања доступног мрежног опсега, па је сада проценат емисионих активности готово безначајан. Потреба за управљањем мрежним емисијама додатно се смањена јер су повећана процесна моћ и стандардизација bus-master мрежних адаптера утицала на смањење трошења процесорске снаге на емисионе пакете који су за већину мрежа бескорисни.

На основу свих ових информација, може се закључити да су мреже базиране само на технологији свичинга 2. слоја постале исплатива опција. Без оптерећења с таквим бригама о контроли емисија, такве мреже су значајно лакше за одржавање и управљање него групе виртуелних мрежа. Све док је капацитет кичме мреже свичева 2. нивоа довољан да покрије целокупне потребе за мрежним саобраћајем, ова врста решења омогућава да се мрежни чвор једноставно прикључи на било који слободан порт свича.

Технологије рутирања су такође значајно напредовале. Новији рутери који имплементирају функције рутирања у хардверским, специјално дизајнираним ASICS колима имају знатно смањену латенцију која се обично повезује са рутерима. Ови нови рутери "брзине жице" нуде перформансе рутирања сличне свичевима 3. нивоа, задржавајући познату, лаку за управљање и одржавање парадигму. Ови нови производи такође укључују многе особине свичева 4. слоја за приоритетизацију пакета, сигурност и скупљање података о току пакета на нивоу апликација.

Мада су технологије рутирања брзином жице релативно нове на тржишту, компаније као што су Rapid-City Communications, Foundry Networks и Cisco (са технологијом преузетом од фирме Systems Granite Systems) су развиле или развијају производе коришћењем овог приступа. Ти производи нуде гигабитну брзину рутирања у локалној мрежи по цени која је релативно слична цени свичева 3. слоја. Коришћење таквих рутера "брзине жице" даје нови живот традиционалној парадигми рутиране мреже.

Иако виртуелне локалне мреже и даље нуде изванредну контолу емисионог саобраћаја и пристојне (иако не стандардне) могућности управљања, промене у осталим ЛАН технологијама значајно су утицале на питања виртуелних локалних мрежа. Више није неопходно имплементирати VLAN решења да би се добиле многе од предности које иначе доносе VLAN технологије.

Традиционалне свичоване мреже сада нуде сличне перформансе као и виртуелне локалне мреже, уз много мање потребног времена за послове администрације и без проблема по питањима стандарда. Једна од потенцијалних брига у тако великим свичованим мрежама је алокација мрежних адреса. За IPX базиране мреже ово није проблем јер поље адресе мрежног слоја није фиксирано. Међутим, у ИП базираним мрежама значајан редизајн мрежног адресирања може бити неопходан при имплементацији оваквих решења.

Појава рутера "брзине жице" такође задире у тржишни сегмент који су држала VLAN решења. За организацију која је тренутно направљена на локалним мрежама са дељеним медијима или свичингом, међусобно повезаним рутерима, ово решење има додатну предност јер се може задржати постојећи дизајн мреже и проверене технике анализе и отклањања кварова, уз значајно побољшање перформанси мреже. Међутим, ова решења су још увек релативно нова на тржишту и због тога се не могу правити релевантна поређења перформанси.

Коначна одлука о томе коју је технологију најбоље користити са аспеката управљивости и контроле мрежног саобраћаја зависи пре свега од постојећег дизајна мреже и жељених особина. За мреже базиране на IPX-у, виртуелне локалне мреже или велике свичоване мреже су једино исплативо решење, јер тржиште за IPX рутере брзине жице вероватно никада неће бити довољно велико да би оправдало њихов развој. За она решења која захтевају прикупљање детаљних информација о току података, VLAN решења 3/4. слоја имају најзрелија решења прикупљања информација од свих описаних технологија.

СВИЧЕВИ 3. И 4. СЛОЈА

Док свичеви 3. слоја обрађују ИП адресе мрежног (трећег) слоја и веома брзо граде везе од-тачке-до-тачке на основу информација из табеле рутирања, свичеви 4. слоја обрађују бројеве TCP портова и могу да дистрибуирају вишеструке захтеве за дате сервисе различитим физичким серверима, обезбеђујући на тај начин расподелу оптерећења (load balancing).

Свич 3. слоја није ништа друго него функционалност рутера упакована у ASIC (Application Specific Integrated Circuit) чипове. Уграђујући функционалност рутера у силицијум могу се остварити значајне уштеде при преласку са решења базираних на софтверском рутирању. Свичеви 3. слоја такође олакшавају мрежним администраторима премештања, додавања или промене у виртуелним мрежама 3.

нивоа, јер администратори не морају да знају на које су физичке портове корисници повезани.

Свич 4. слоја користи виртуелне ИП адресе за расподелу (балансирање) саобраћаја између више сервера на основу информација о сесијама и статуса. Овај процес се понекад назива расподела оптерећења према сервисима. Свичеви 4. слоја су најкориснији када више сервера нуди исте апликације и постоји потреба да се изврши расподела оптерећења међу њима. Свич 4. слоја је способан да одреди која се сесија захтева и да упути захтев најдоступнијем серверу замењујући при том адресу виртуелног сервера адресом стварног сервера коме се захтев прослеђује. Међутим, због превођења мрежних адреса (NAT – Network Address Translation) коришћење вишеструких сервера у позадини је потпуно транспарентно за кориснике и њихове апликације.Свичеви 4. слоја понекад се називају преусмеривачи апликација (Application Redirector). У неким случајевима свичеви испитују и саобраћај изнад 4. слоја и на основу тога доносе одлуке о свичовању. На пример, HTTP протокол (веб саобраћај) може бити идентификован у 4. слоју, на порту 80. Међутим, свичеви 4. слоја могу да расподељују оптерећење или врше преусмеравање и на основу стварног садржаја сесије, омогућавајући тако да се различите врсте веб садржаја чувају на различитим физичким серверима, иако им се свима приступа преко на изглед исте адресе сервера.

Свичеви 4. слоја такође се могу користити за филтрирање нежељених протокола 4. слоја као што је IPX SAP (Service advertising Protocol) или за омогућавање приоритетизације. На основу тога да ли је пакет намењен локалној или регионалној мрежи, свич ће доделити приоритет преко 802.1p ознаке приоритета (у 2. слоју) или подесити приоритет у IP ToS (Type of Service) пољу ИП заглавља (3. слој).

Други пак свичеви 4. слоја користе TCP и UDP бројеве портова за управљање пропусним опсегом или обликовање саобраћаја. На пример, PacketShaper фирме Packeteer врши класификацију саобраћаја према бројевима портова и додељује гарантовани и максимални опсег заједно са степеном приоритета свакој од различитих класа саобраћаја. Циљ коришћења ових уређаја је постизање несметаног и контролисаног протока саобраћаја.

ЛИТЕРАТУРА:

1. Applied Data Communications, A Business-Oriented Approach, 3rd Edition; James E. Goldman, Philip T. Rawles; John Wiley & Sons, 2001.
2. Основе умрежавања (Networking Essentials), превод другог издања; Microsoft Press/CET, 1997.
3. Building Cisco Remote Access Networks, Mark Edwards, Ron Fuller, Andy McCullough, Syngress, 2000.
4. Техничка документација са веб сајтова произвођача:
   - Cisco (www.cisco.com)
   - Allied Telesyn (www.alliedtelesyn.com)
   - Lucent (www.lucent.com)
5. comp.dcom.lans.ethernet Frequently Asked Questions (http://www.networkuptime.com/faqs/ethernet/)
6. Информације са сајта Телекома Србија (www.telekom.yu