Нов български университет

Общи архитектурни концепции използвани в IP маршрутизаторите

Доц. Д-р Емил Стоилов

Департамент по Информатика на НБУ

София, май 2013

Съдържание

1. Увод

Светът на компютърните мрежи се развива с неимоверно бързи темпове. В процес сме на повсеместното заместване на старите унаследени мрежи, използващи специално разработени технологии, такива като TDM, Frame Relay и ATM, с по-нови разработки, базирани на използването на Internet Protocol (IP). Този протокол позволява интегрирането на различни мрежови услуги в еднородна среда. Доставчиците на мрежови услуги не могат повече да си позволят да поддържат отделни мрежи, всяка от които е проектирана за определено приложение или услуга, например за телефонни разговори, пренасяне на корпоративни данни или Интернет трафик. Това е икономически неизгодно. Освен това самите клиенти вече изискват интегрирано обслужване. Те желаят да използват нови приложения, при които скоростта на доставка на услугата е от критично важно значение, т.е. появяват се нови изисквания към съвременните мрежови архитектури. Навсякъде по света водещите кабелните и безжични доставчици на услуги преминават към мрежи с IP ядро, за да се възползват от мащабираемостта и ефективното използване на честотната лента, които то предлага, както и от възможността за бърза експанзия на пазара на нови услуги.

Това изяснява изключителния интерес към използването на IP комутатори и маршрутизатори в съвременните мрежи. Повече информация за изискванията към ядрото на IP мрежите можете да намерите например в [1].

Две групи специалисти са заинтересовани от информацията за архитектурите, които се използват в този тип мрежови устройства, както и от функционалните възможности, които тези архитектури предоставят.

Към първата група спадат специалистите, които създават тези устройства. Това са инженерите по схемотехника, изграждащи хардуера и програмистите, които създават фирмуера. Те познават в детайли своето устройство, но нямат преки впечатления от неговата експлоатация, т.е. доколко техническите му характеристики и функции се използват в практиката, по какъв начин се използват и какви резултати се постигат.

Устройствата се експлоатират от втората група специалисти, а именно от мрежовите администратори. За администраторите всяко мрежово устройството е черна кутия с интерфейси, която трябва да изпълнява определени функции. Познавайки операционната система на устройството и разполагайки с определен брой нейни команди, администраторите го конфигурират и довеждат до работоспособност. С тази си задача те обикновено се справят добре. Когато обаче трябва да се проектира или експлоатира компютърна мрежа с повишени изисквания към нея, това не е достатъчно. Необходим е сравнителен анализ при избора на отделните устройства като при това не може да се разчита на маркетингова информация. По принцип администраторите не познават в детайли хардуера и фирмуера на отделните устройства - нямат необходимата научна подготовка за това. За да се направи такъв анализ обаче са необходими определени познания, поне на ниво архитектура. Малко повече информация за това как устройството е изградено и как физически функционира, може да помогне за постигането на значително по-добри резултати.

Целта на този технически доклад е да се систематизират различните архитектури използвани при изграждането на съвременните IP маршрутизатори и комутатори и да се

помогне на мрежовите администратори по-лесно да се ориентират при избора на мрежови устройства с определени качествени показатели.

2. Характерни особености на IP мрежите

По принцип във всяка мрежа наблюдаваме два вида пакети. Първият вид са пакетите с данни (data packets). Те съдържат потребителска информация и определят потребителския трафик. Вторият вид пакети са служебни пакети на самата мрежа (control and management packets). Те се генерират от мрежата и се използват за нейното изграждане и нормално функциониране. Една от силните страни на IP протокола е, че всички пакети преминават през една „обща тръба" (common pipe), или с други думи принадлежат към една група (in-band). Мрежовите специалисти знаят, че в по-старите технологии като TDM и ATM, каналът за данни (in-band), е отделен от канала за служебни съобщения (out-of-band). Това често предизвиква определено объркване за начина по който пакетите с данни в IP мрежата се разделят от служебните пакети и как се гарантира тяхната сигурност.

Въпреки, че при IP мрежите всички пакети от гледна точка на преминаването през мрежата са в една група (in-band), то от решаващо значение е да се направи разграничение между различните видове пакети, които се транспортират.

Разделяме пакетите на четири групи според тяхната функционалност и приемаме, че всяка група пакети преминава по своя собствена плоскост или равнина (plane). Тези отделни плоскости на трафика са:

- плоскост за предаване на данни (data plane), по която преминава потребителския трафик,
- плоскост за контрол на мрежата (control plane), по която преминава трафика от служебни съобщения с контролни функции,
- плоскост за управление на мрежата (management plane), по която преминава трафика от съобщения за управление и наблюдение на мрежата и
- плоскост за услуги (services plane).

Правилното класифициране на трафика, неговото разделяне и управление е от съществено значение за сигурността в IP мрежите.

При изграждането и експлоатацията на IP мрежова инфраструктура за интегрирани услуги, винаги трябва да се правят компромиси и да се търси определен баланс. Изпълнението на строгите административни изисквания към операторите на мрежи, заедно с предлагането на различни услуги, които често са с противоречиви изисквания за честотна лента (bandwidth), забавяне (delay), трептене (jitter) и брой загубени пакети е върхово предизвикателство. Старите мрежи бяха проектирани и изградени с конкретни експлоатационни характеристики и предлагаха една единствена услуга. При тях беше сравнително лесно да се постигне високо качество на приложението или услугата, тъй като параметрите бяха строго контролирани. Изискването през ядрото на мрежата да преминават различни по своята същност трафици (трафик генерират от Интернет, от поточното аудио и видео, от клетъчните телефони, голямото количество корпоративни данни и други) има значителни последици както за проектирането на мрежата, така и за нейната експлоатация. Смущения в обслужването на някой от тези трафици може потенциално да наруши всички останали услуги на мрежата. Това значително увеличава ролята на сигурността в такъв тип мрежи.

IP мрежите използват отворени стандарти, разработени от IETF. Достъпът до тези стандарти и протоколи е свободен за всеки. Те са независими от конкретния компютърен хардуер или операционната система. Тази отвореност насърчава към иновации и създаване на нови приложения и услуги. Те от своя страна обикновено предявяват по-строги изисквания към характеристиките на потока. Често е много трудно мрежата да е в крак с бързо променящите се изисквания.

В допълнение IP мрежите трябва да бъдат достатъчно устойчиви за да се справят с такива явления като неправилна употреба или злоупотреба, липси на конфигурации, неяснота в топологията и т.н. В съвременните IP мрежи е критично важно да се прави разлика между различните видове трафик, да се насочва той правилно към съответните плоскости и да се въведат механизми за контролиране на влиянието на отделния вид трафик върху цялата мрежа. За да се демонстрира как това става ще разгледаме две обособени категории мрежи: *корпоративна мрежа (enterprise network)* и *мрежа на доставчик на услуги (service provider network).* Описанието на тези два вида мрежи служи само за изясняване на концепцията за плоскостите на IP трафика.

2.1 Корпоративни мрежи

Корпоративните мрежи формират един широк клас от мрежи, който се отличава със своите архитектурни детайли и типични транспортни потоци. Фирмите често изграждат своите мрежи така, че в тях да бъдат постигнати четири основни цели:

- Да свързват вътрешните потребители с използваните от тях приложения.
- Да осигурят достъп на вътрешните потребители до отдалечени обекти на същата организация и до Интернет.
- Да осигурят достъп на външни потребители до публично рекламираните ресурси под контрола на организацията (например уеб сайт).
- Да свържат външни партньори (Extranet) към определени фирмени ресурси (които не са публични) и са под контрола на организацията.

Корпоративните мрежи могат да бъдат малки, средни или големи и несъмнено има различия между тях. Но те също така имат много общи характеристики, включително:

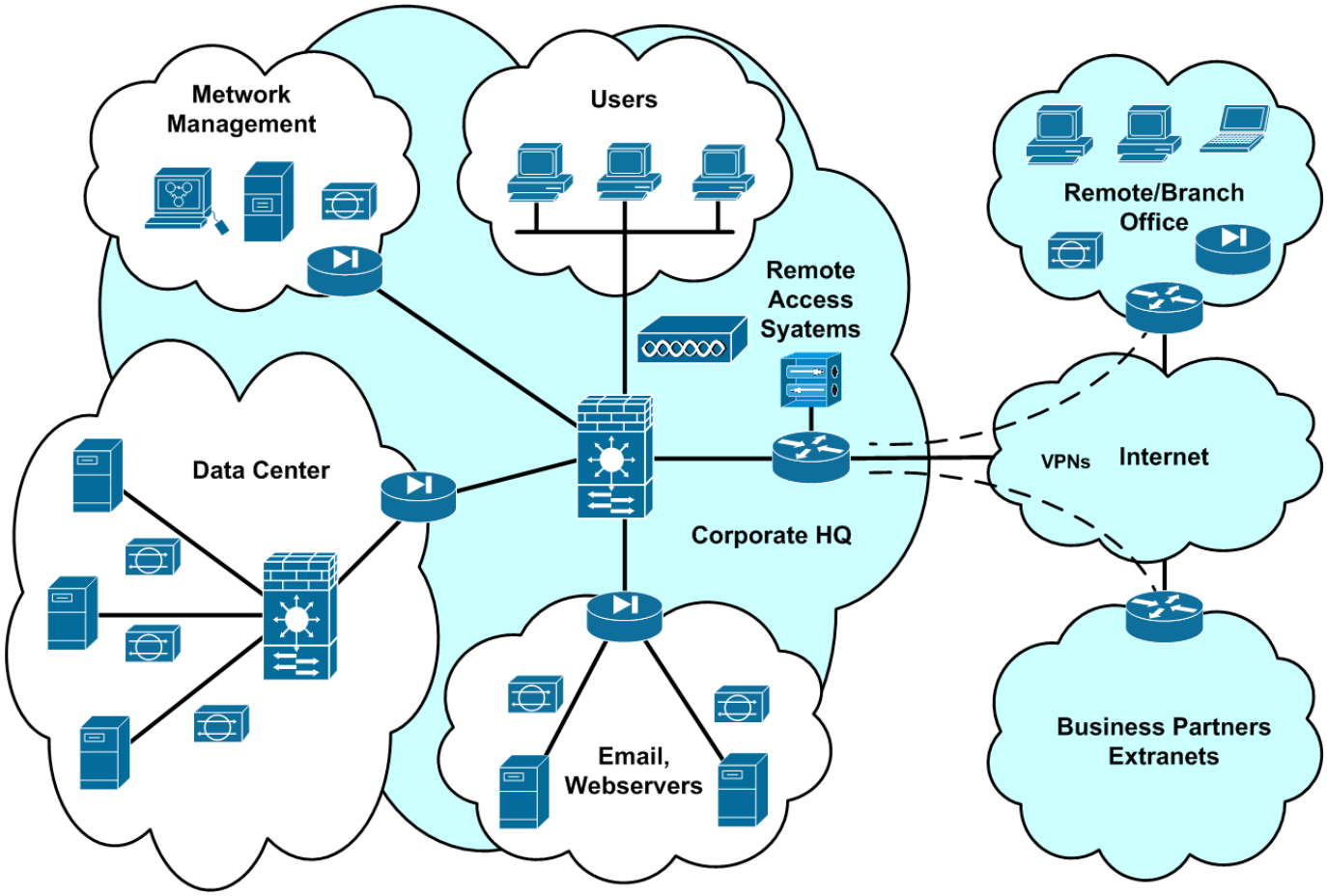
- Добре дефинирана архитектура. Обикновено се използва познатия йерархичен трислоен модел, състоящ се от слой на ядрото (core layer), слой за разпределение (distribution layer) и слой за достъп (access layer). Слоят на ядрото осигурява високоскоростен комутируем гръбнак (backbone) на мрежата, а също така и връзка към глобална мрежа, която от своя страна може да бъде Интернет, виртуална частна IP мрежа (VPN) или реална частна IP мрежа. Слоят за разпределение се намира между ядрото и слоя за достъп. Чрез моделиране на този слой се осигурява изпълнението на конкретната политика заложена при проектирането на мрежата. Свързването на потребителите и сървърите към мрежата става през слоя за достъп. В по-малките мрежи тези три слоя често са обединени.

- Точно дефинирана граница между фирмата и доставчика на услуги. Разграничението е както от гледна точка на собствеността, така и на капитала. Съвсем ясно е кой е собственик на устройствата в дадена мрежа, кой е отговорен за тези устройства и кой и кога има достъп до тези устройства и услуги.

- Напълно определен набор от IP съвместими протоколи, включително вътрешни протоколи за динамична маршрутизация (например OSPF), протоколи за наблюдение и управление на мрежата (SNMP, Syslog и т.н.), както и други IP протоколи необходими за различните клиент/сървър приложения използвани от фирмата.

- Трафикът преминаващ през граничната линия и в двете посоки е точно определен. Същото важи и за трафика вътре в корпоративната мрежа. На самата граница трафика може да бъде ограничаван въз основа на определени политики за сигурност. Вътрешните транспортни потоци остават изцяло в рамките на корпоративната мрежа. През корпоративната мрежа никога не трябва да преминава транзитен трафик, т.е. входящите пакети никога не трябва да имат местоназначения, които не са част от адресното пространство на корпоративната мрежа.

Общата архитектура на една корпоративна мрежа е представена на Фиг.1



Фиг.1 Обща архитектура на корпоративна мрежа.

2.2 Мрежи на доставчици на услуги

Мрежите на доставчици на услуги също формират един широк клас от мрежи, които се отличават по своите архитектурни детайли и типични транспортни потоци. Тези мрежи са изградени с цел печалба. Това означава, че мрежата е генератор на приходи (или улеснява генериране на приходи). Доставчиците изграждат своите мрежи така, че те да решават следните задачи:

- Да осигурят достатъчен капацитет за *транзитен* трафик на своите корпоративни клиенти до техните корпоративни мрежи, а също така и до всички сайтове огласени публично в адресното пространство (с други думи до Интернет).

- Да осигурят пропускателна способност и достъп на външни потребители до съдържанието на ресурси и услуги, които са под непосредственото управление на доставчика.

- Да осигурят достатъчен капацитет за ***вътрешен*** трафик на други интегрирани услуги на доставчика, с които той максимално се възползва от възможностите, които предлага ядрото на IP мрежата.

Най общо мрежите на доставчиците на услуги имат следните характеристики:

- Добре дефинирана архитектура, включваща маршрутизатори намиращи се в ядрото (core routers) и гранични маршрутизатори (edge routers). Обхватът на мрежата обикновено се разпростира в регионален, национален или дори глобален мащаб и се характеризира с „точки на присъствие" (points of presence – PoP), разположени в стратегически места. Мрежовата архитектура е изградена с хардуер. При нея имаме дублиране на връзки с цел осигуряване винаги на наличност и отказоустойчивост. Тя трябва да осигурява и висока пропускателна способност.

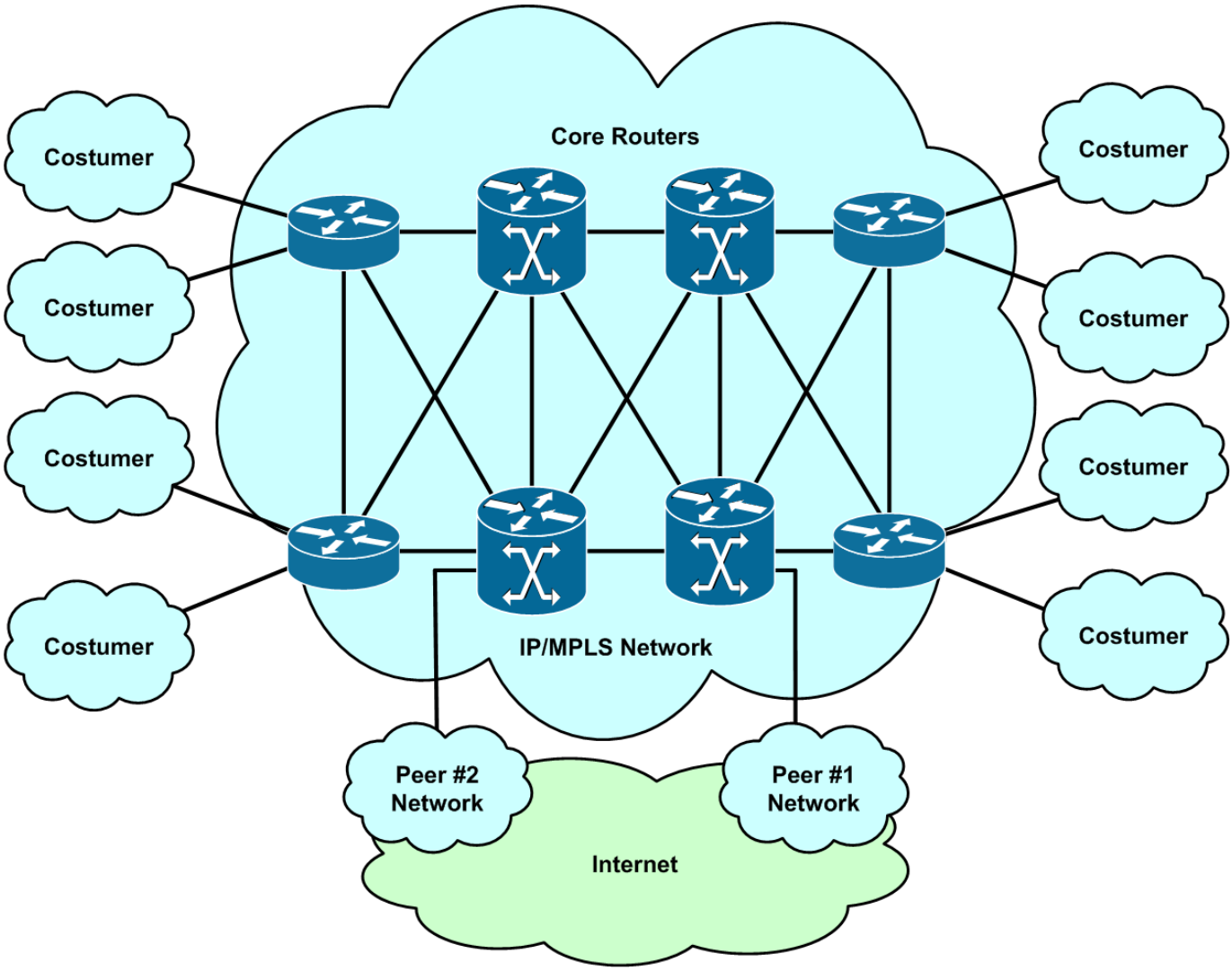
- Точно дефинирана граница между оборудването на доставчика на услуги и оборудването на клиента. В повечето случаи е напълно ясно кой е собственика на устройствата, кой отговаря за тях и кой е упълномощен за достъп до всички тези устройства и услуги. Въпреки, че това е вярно и за корпоративните мрежи, има все пак някои различия в това как доставчиците определят границите на техните мрежи. Всъщност при тях мрежите имат два вида граници. Първата е на мястото където мрежата на доставчика се среща с клиентската мрежа, а втората е там, където мрежите на отделните доставчици се свързват помежду си. Това придава допълнителна сложност при определянето на вида трафик, защото две независими мрежи, с различен по вид трафик са взаимосвързани. Това води до проблеми, особено със сигурността.

- Добре подбран набор от IP съвместими протоколи, включително вътрешни протоколи за динамична маршрутизация (Interior Gateway Protocols - IGP), както и многобройни сесии на BGP (Boarder Gateway Protocol). Избраният IGP е изцяло вътрешен за мрежата и никога не работи с клиентски IP адреси. BGP обикновено се използва между доставчика на услуги и корпоративните мрежи и работи с публично адресируемо IP адресно пространство. За изграждането на виртуални частни мрежи (VPN) между клиента и доставчика се използва IGP или BGP. Дефинирани

са и други IP протоколи като SNMP за наблюдение и управление на мрежата, протоколи за фактуриране и за специализирани вътрешни дейности.

Фигура 2 илюстрира една обща за доставчик на услуги архитектура.

Интересно е да се сравнят мрежите на доставчици на услуги с корпоративните мрежи, защото потокът на трафика в тях е много различен. В много отношения те могат да се разглеждат като противоположни една на друга. Първо, корпоративните мрежи почти винаги са със стриктно определена граница към Интернет и в тях нищо не е позволено да проникне, освен трафик като отговор на вътрешно генериран трафик или плътно контролиран външен трафик, но насочен към точно дефинирани публично обявени услуги. При доставчиците на услуги е точно обратното. Те изграждат своите мрежи така, че целият трафик да преминава през границата почти безпрепятствено. Границата е проектирана да бъде широко отворена – всичко преминава, освен ако нещо не е изрично забранено.



Фиг.2 Обща архитектура на мрежа на доставчик на услуги.

Второ, корпоративните мрежи са проектирани така, че трафикът да се затваря или напълно вътре в мрежата или да стига най-много до ядрото на вътрешната мрежа. За да

се контролира трафика в корпоративната мрежа почти винаги се използват устройства, които следят състоянието на сесиите (stateful devices), като например защитни стени следящи потоците от външни пакети. При мрежите на доставчици на услуги отново е точно обратното. При тях външният клиентски трафик не трябва никога да е насочен към техните вътрешни устройства или мрежови елементи. Вместо това трафикът се очаква да премине транзитно през мрежата. Ето защо, поради големия по обем трафик и множеството входни и изходни точки на мрежата на доставчика, следящи трафика устройства като защитни стени и системи за защита от проникване се използват много рядко по отношение на транзитния трафик. Задачата на доставчика на услуги е да предаде пакетите към крайната им дестинация възможно най-бързо.

Защо архитектурата на мрежата е толкова важна? Главно поради начина по който мрежата се изгражда – от определяне на топологията, през схемата за адресиране до избора на мрежовите устройства. Архитектурата в значителна степен определя как трафика да бъде класифициран и как да бъде защитен.

3. Характерни особености на IP трафика

IP е мрежов протокол без установяване на връзка (connectionless), който капсулира данните в собствени самостоятелни маршрутизируеми единици известни като пакети. Всеки пакет има заглавна част (header), която съдържа определена информация (включително адресите на източника и местоназначението), и която информация се използва от маршрутизаторите при вземане на решението за препредаване на пакета. Знаем вече, че IP предава всички пакети в една група (in-band). Пакетите съдържащи данни и управляващите пакети се приемат от един общ интерфейс в маршрутизатора и се обработват от него, но очевидно тези пакети имат различно предназначение. Казано съвсем опростено, маршрутизаторът обработва всеки един пакет, като взема под внимание адреса на неговото местоназначение. От гледна точка на маршрутизатора, ако пакетът е насочен към адрес намиращ се в самия маршрутизатор, то това най-вероятно е контролен или управляващ пакет. Ако местоназначението на пакета е някъде другаде в мрежата, то той се третира като пакет с данни и се препраща. Разбира се това е много опростен поглед. За пълното разбиране на това как IP трафика се разпределя в различните плоскости очевидно е необходимо по-задълбочено изследване на операциите които се извършват в мрежата и маршрутизатора.

Както е показано на Фиг.3, един маршрутизатор обикновено участва в по-голяма мрежова среда, може би дори и в Интернет. Ето защо всеки маршрутизатор, сам за себе си, може да разбира или да не разбира контекста на всеки един пакет, който обработва (с други думи, към коя плоскост на IP трафика този пакет принадлежи). От гледна точка на маршрутизатора в момента когато обработва даден пакет е важен *вида на IP трафика*, който той разпознава. Концепцията за различни *плоскости на IP трафика (IP traffic planes)* е логическа, не физическа. Концепцията за *вида на IP трафика (IP traffic type)* е реална, и тя ще бъде разгледана в този раздел.

Разбирането на това как маршрутизаторите обработват различните видове пакети е от изключителна важност. Защо маршрутизаторите обработват някои пакети различно от другите? Какви са последиците за сигурността в резултат от разликите? По-долу ще разгледаме подробно трите основни вида пакети, а именно *транзитните пакети (transit packets), входящите пакети за маршрутизатора (receive packets)* и *пакетите-изключения (exception packets).*

3.1 Транзитни пакети

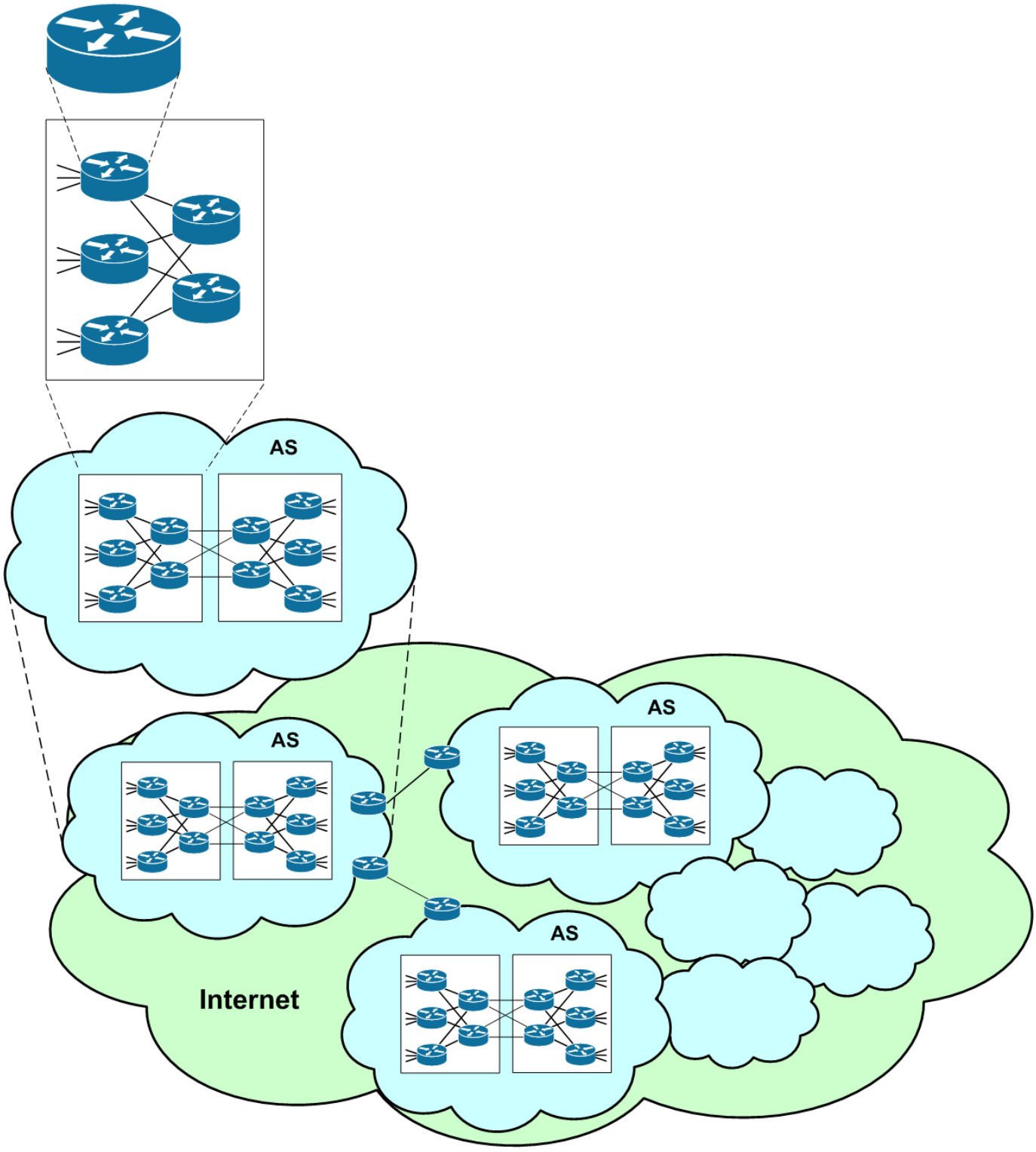
IP мрежите се изграждат, за да се препредават по тях пакетите между крайните хостове. Това, което маршрутизаторът прави, е да приеме пакета по единия интерфейс, да погледне полето за адреса на местоназначението в заглавната част на пакета, да намери съответствие за този адрес в маршрутната таблица (изградена впрочем от плоскостта за контрол на мрежата!) и да изпрати пакета по друг подходящ интерфейс към следващия маршрутизатор, който се намира с един скок по-близо да крайното местоназначение.

При транзитните пакети тяхното крайно местоназначение се намира някъде на разстояние от маршрутизатора. Това означава, че IP адреса на местоназначението не се намира в *конкретния маршрутизатор*, който обработва пакетите, а по-скоро е някъде другаде в мрежата. Той може да бъде в директно свързана към маршрутизатора подмрежа (LAN), или много по-далеко, като пътят до него минава през множество маршрутизатори. От съществено значение е, че пакетът не е предназначен за този маршрутизатор; той само ще премине през него. Следователно когато маршрутизаторът види транзитен пакет, той взема решение да го предаде по някой от своите интерфейси. За бързата обработка на пакетите маршрутизаторите обикновено използват специализиран хардуер и алгоритми, които ще бъдат разгледани по-късно.

Трябва да се отбележи, че не се обявява явно или неявно към коя плоскост на IP трафика транзитните пакети принадлежат. От гледна точка на маршрутизатора те могат да принадлежат към всяка една IP плоскост. Да разгледаме като пример сесия за управление по Secure Shell (SSH) между администратор намиращ се в центъра за управление на мрежата и маршрутизатор в ядрото на тази мрежа. Пакетите от тази сесия минават през много маршрутизатори по пътя към крайния маршрутизатор. За всички тези маршрутизатори те са транзитни пакети. Когато обаче пакетите достигнат до крайния маршрутизатор, за него те вече не са транзитни пакети. Те са или *входящи пакети за маршрутизатора (receive packets)* или *входящи близки пакети за маршрутизатора (receive-adjacency packets)* (виж следващия раздел). От логическа гледна точка обаче, тези пакети през цялото време са от *плоскостта за управление на мрежата (management plane)*.

3.2 Входящи пакети за маршрутизатора

IP пакетите, които се получават в маршрутизатора, и са насочени към IP адрес, който е собственост на този маршрутизатор, т.е. крайното местоназначение е самия маршрутизатор, се наричат *входящи пакети за маршрутизатора* или *входящи близки пакети за маршрутизатора*. Термините *входящи пакети за маршрутизатора (receive packets)* или *входящи близки пакети за маршрутизатора (receive-adjacency packets)* произлизат от номенклатурата, която се използва при създаване на таблицата за съседство, съгласно механизма за бързо препредаване на пакети носещ наименованието Cisco Express Forwarding (CEF). Когато CEF изгражда своята таблица за съседство и изброява в нея IP адресите на своите интерфейси (логически и физически), тези интерфейси са описани като входящи, т.е. по тях се получават (receive) пакети. Друг термин, използван в някои документи, е пакети „за нас” (“for-us”).



Фиг. 3 Място на маршрутизаторите в Интернет

Когато маршрутизаторът анализира такъв пакет, адресът на местоназначението винаги е на нещо, което се намира вътре в дадения маршрутизатор. Това може да бъде или физически интерфейс, или логически интерфейс, като например *вътрешен затварящ интерфейс (loopback interface)* или *интерфейс на тунел (tunnel interface)*. Тези пакети могат да бъдат получени от директно свързана LAN или да са преминали вече през множество маршрутизатори. При всички случаи реакцията на маршрутизатора при

обработката на такъв пакет е коренно различна от тази при транзитните пакети. При входящите пакети за маршрутизатора не може да се използва специализирания хардуер за бързо препредаване. Маршрутизаторът трябва да обработи пакета сам, като за целта използва собствените ресурси на локалния микропроцесор. Следователно такива пакети се изваждат от високоскоростния хардуерен път и се насочват за обработка към CPU.

Може да останете с впечатление, че всички входящи пакети за маршрутизатора съдържат контролна информация. Това не винаги е така. Както и при транзитните пакети, съществуват много различни пакети, които потенциално попадат в тази категория. Те обикновено съдържат информация от плоскостите за контрол, управление и услуги. Най-важното е да се разбере, че този вид пакети се обработват по различен начин от транзитните пакети. Обикновено това означава, че в маршрутизатора се използва различен хардуер и/или софтуер и че почти винаги скоростта на обработка е много по-малка, отколкото при транзитните пакети. Една от основните причини за разделянето на IP трафика в отделни плоскости и тяхното анализиране е тази, че различния начин на обработка на входящите пакети за маршрутизатора и транзитните пакети, влияе в голяма степен върху производителността на маршрутизатора и има последици за сигурността на мрежата.

3.3 IP пакети-изключения и не-IP пакети

В предходните раздели бяха разгледани два различни вида пакети - транзитни и входящи пакети за маршрутизатора. Транзитните пакети се препредават от маршрутизаторите, които за това обикновено използват някакъв механизъм за високоскоростно пренасочване. Входящите пакети за маршрутизатора трябва да бъдат обработвани от самия маршрутизатор локално. Интересното е, че тези два вида трафик не обхващат всички случаи в IP мрежите. При маршрутизаторите се наблюдават още два вида пакети, известни като IP пакети-изключения и не-IP пакети.

IP пакетите-изключения могат да бъдат както транзитни, така и входящи за маршрутизатора. Те имат някои особени характеристики, което налага тяхната специфична обработка. Не-IP пакетите са точно това, което показва наименованието им – те не са част от IP протокола. Обикновено такива пакети се използват от маршрутизаторите за изграждане и поддръжка на мрежата. IP пакетите-изключения и не-IP пакетите трябва да бъдат разглеждани като самостоятелна група, защото те се обработват различно от транзитните и входящите пакети за маршрутизатора. Тези пакети са важни, защото всеки от тях има потенциал да оказва влияние върху функционирането на мрежата. С тях се предават служебни данни и те помагат за изграждането на маршрутните таблици и за управлението на маршрутизаторите.

3.3.1 IP пакети-изключения

Сега ще представим един пример за IP пакет-изключение. Да предположим, че в маршрутизатора пристига транзитен пакет, който трябва да бъде препратен по-нататък по веригата. В полето TTL (Time-to-Live) в заглавната част на пакета обаче има записана стойност 1. Преди изпращането на пакета тази стойност трябва да бъде намалена с 1, така че получаваме 0. IP протоколът изисква пакетите с TTL = 0 да бъдат отстранени. Допълнително трябва да бъде генерирано съобщение за грешка в протокола ICMP и това съобщение да бъде изпратено на източника на изхвърления транзитен пакет за да бъде той информиран за това. Съобщението за грешка на ICMP е от вида „времето е

превишено при транзитно предаване” (“time exceeded in transit”), т.е. ICMP тип 11 код 0. Възниква извънредна ситуация, която изисква маршрутизаторът да изразходва допълнителни ресурси за нейното овладяване.

Друг пример: Пристигащият IP пакет съдържа опции в заглавната си част, изисква фрагментация или е пакет от групово предаване (multicast packet) със специално предназначение. Съществуват и други изключения, като при това те са различни за различните платформи използвани в маршрутизаторите.

3.3.2 Не-IP пакети

Другата разновидност са не-IP пакетите. Най-общо има две групи не-IP пакети, които се налага маршрутизаторите да обработват. Към първата група принадлежат пакети от слой 2 (Layer 2), които се генерират от самите маршрутизатори с цел изграждането и поддържането на мрежата. Като примери тук можем да посочим:

- *Пакети за поддържане на връзките в слой 2 (Layer 2 keepalives).* Различните протоколи, като Cisco HDLC, Frame Relay, ATM и други протоколи от слой 2 обикновено изпращат периодични съобщения за поддържане на връзките между различните устройства, както и на състоянията на техните интерфейси.

- *Link Control Protocol (LCP):* LCP е неразделна част от протокола PPP и Multilink PPP и осигурява автоматично конфигуриране на интерфейси, като се грижи за големината на рамките, избягването на символи, избора на автентикация и т.н. LCP открива затворени контури (looped-back links) и непълна конфигурация, а също така прекратява връзки.

- *Cisco Discovery Protocol (CDP):* CDP е патентован от Cisco протокол, който предава информация за състоянието на интерфейсите на съседни маршрутизатори, като използва групово предаване (multicast).

В горните примери се използват съобщения от слой 2, които се третират от маршрутизаторите като изключения и се обработват от техния процесор. Това всъщност са местни пакети, т.е. пакети от точка до точка. Те се различават от пакетите от слой 2, които преминават през тунел (например на AToM, VPLS и L2TP).

Втората група включва всички пакети от слой 3, които са не-IP пакети, но маршрутизаторите са така конфигурирани, че такива пакети да преминават през тях на конкурентна база, едновременно с IP пакетите. Като примери за такива протоколи, генериращи не-IP пакети от слой 3, можем да изредим следните:

- *Intermediate System - to - Intermediate System (IS-IS):* Това е маршрутизиращ вътрешен протокол, който често се използва в мрежите на големите доставчици на услуги (вместо OSPF) за определяне на следващите възли на BGP. IS-IS работи също като IP в слой 3, но е отделен протокол. Първоначално беше разработен от ISO като маршрутизиращ протокол за CNLP (Connectionless Network Protocol), но по-късно беше разширен да поддържа IP маршрутизиране.

- *Address Resolution Protocol (ARP):* Този протокол за преобразуване на адреси се използва за намиране на физическия (MAC) адрес по зададен IP адрес на мрежа или хост.

- *Multiprotocol Label Switching (MPLS):* Това е механизъм за предаване на данни, който емулира някои от свойствата на мрежите с комутиране на вериги (виж например [1]). Често MPLS се разглежда като протокол, който работи по средата между слой 2 и слой 3.

Други примери за протоколи от слой 3, които генерират не-IP пакети са протоколите *Internetwork Packet Exchange (IPX)* на Novell и *Apple Talk* на Apple.

Както видяхме, маршрутизаторите обработват четири различни вида пакети: транзитни пакети, входящи пакети за маршрутизатора, IP пакети-изключения и не-IP пакети. Основната причина тези четири вида трафик да бъдат тук описани отделно е, че маршрутизаторите обработват пакетите им по различен начин. Производителите на маршрутизатори, като Cisco например, създават хардуер и софтуер, които да се справят с всякакъв вид трафик, осигурявайки максимална производителност при зададена структура на разходите. В същото време мрежовите архитекти и администратори трябва да са наясно с взаимодействието на тези четири вида трафик и да разбират последиците, които те могат да имат върху маршрутизатора и неговата производителност и достъпност. Например някои атаки от типа на отказ на услуга (DoS) използват целенасочено манипулиране на IP пакетите-изключения. Маршрутизаторите и мрежовата инфраструктура трябва да бъдат проектирани и изградени така, че ефективно да преминава „нормалния" трафик, и в същото време останалия трафик да се обработва така, че да се смекчават последствията от атаките и те да не оказват отрицателно въздействие.

4. Плоскости на IP трафика

Плоскостите на IP трафика представляват логически категории, които се използват за разделяне на трафика въз основа на функцията, която той изпълнява в мрежата. Този подход се използва главно поради две причини. Първо, той създава стабилна основа, върху която може да се изгражда политиката за сигурност на мрежата и второ, той е много полезен в процеса на превръщане на тази политика за сигурност в реални мрежови функции за контрол, които могат да бъдат приложени върху различни мрежови елементи.

В зависимост от това къде маршрутизаторът се намира в мрежата, той има различно виждане за вида на пакета, който в момента обработва (например транзитен или входящ за маршрутизатора). Видът на пакета обаче не дава автоматично никаква индикация за функциите, които той изпълнява. Такава информация ни предоставя концепцията за различните плоскости на IP трафика. Към пакетите от всяка плоскост на трафика се предявяват определени изисквания, независимо от това къде те се намират в мрежата. Както вече знаете, определени са четири плоскости на IP трафика: плоскост за предаване на данни, плоскост за контрол на мрежата, плоскост за управление на мрежата и плоскост за услуги. Всяка от тях има своите отличителни характеристики, както и свои собствени изисквания за сигурност. Следва тяхното по-подробното описание.

4.1 Плоскост за предаване на данни (data plane)

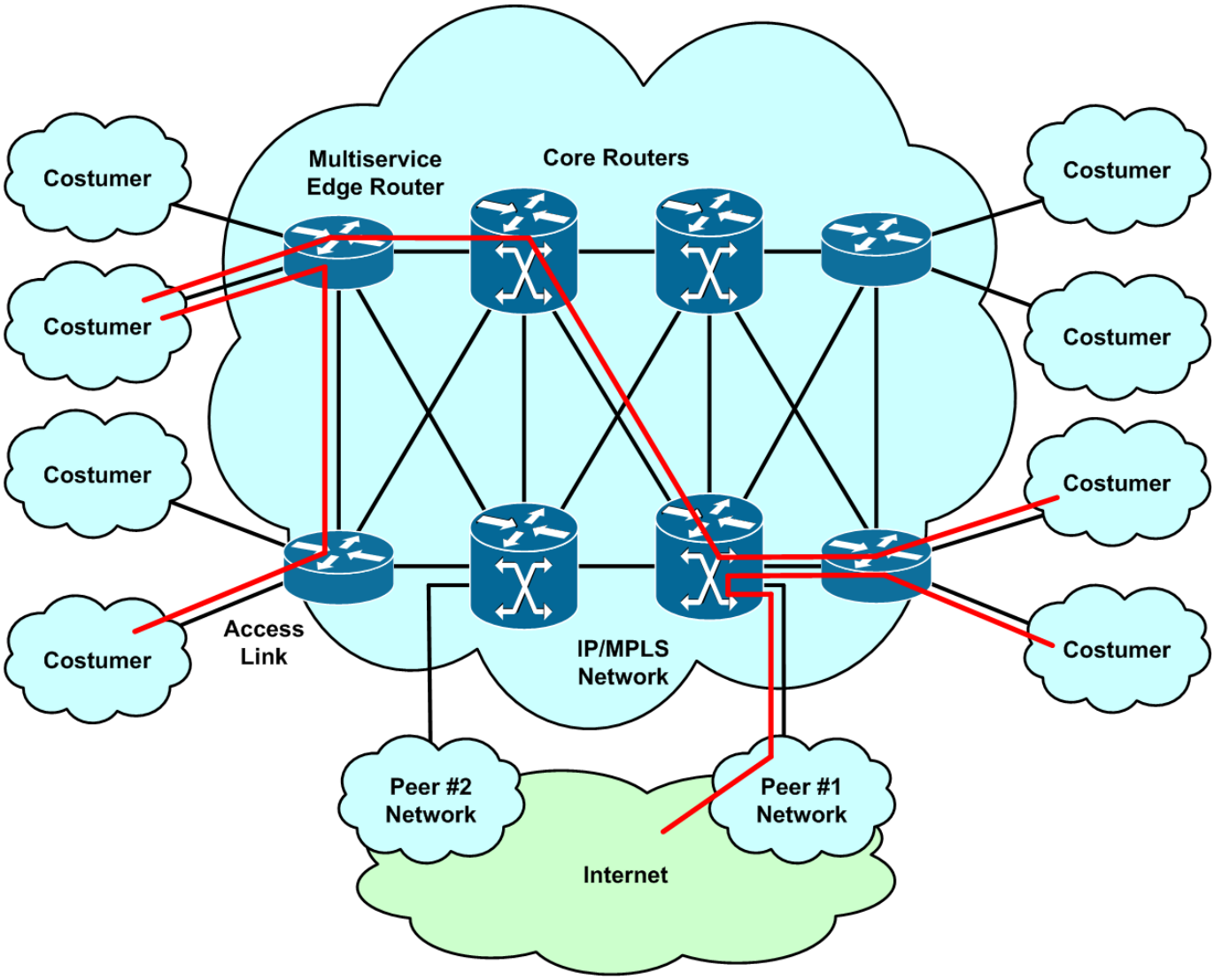
Плоскостта за предаване на данни е логическа единица, която обхваща целия „клиентски" приложен трафик. Тук под „клиентски" трафик разбираме трафик генериран от хостове, клиенти, сървъри и приложения, който използва мрежата само за транспорт. Следователно IP адресите на получателя в пакетите на този трафик никога не принадлежат на мрежови устройства (като маршрутизатори и комутатори). По-скоро те трябва да бъдат доставени на друг тип устройства поддържани от мрежата, например компютри и сървъри. Основната задача на маршрутизатора за пакетите от плоскостта за предаване на данни е да предаде тези пакети надолу по веригата възможно най-бързо. Фиг.4 илюстрира основната концепция на плоскостта за предаване на данни.

Мрежите се изграждат и експлоатират за да преминава по тях трафика от плоскостта за предаване на данни. Без плоскост за предаване на данни няма нужда от мрежа. Първото и най-важно е, тя да бъде налична (available). Както ще видим след малко, плоскостта за предаване на данни зависи от плоскостта за контрол на мрежата и в известна степен от плоскостта за управление на мрежата, т.е. съществуват определени взаимозависимости между отделните плоскости. В допълнение, може да има изискване за „конфиденциалност", което да бъде изпълнено чрез разделяне на данните (както е например във Frame Relay или MPLS VPN) или криптиране. Транзитните пакети по принцип се намират в плоскостта за предаване на данни. При нормални условия транзитният трафик представлява голям процент от целия трафик в тази плоскост.. Точно заради това маршрутизаторите често използват специализиран хардуер и алгоритми за да извършат пренасочването възможно най-бързо. Това не означава, че всички транзитни пакети принадлежат към плоскостта за предаване на данни, нито че плоскостта за предаване на данни се състои само от транзитни пакети. Има изключения, и при тях маршрутизаторите са принудени да извършват допълнителна работа, за да препредадат такива пакети. Следователно в плоскостта за предаване на данни могат да пътуват и някои транзитни пакети-изключения, и тогава се включват допълнителни ресурси на маршрутизатора, за да бъдат тези пакети препратени. Два примера ще помогнат за изясняването на този момент:

Първи пример: В интерфейса на маршрутизатора пристига пакет и маршрутизаторът решава, че това е транзитен пакет, който трябва да бъде доставен на хост намиращ се в директно свързан сегмент на локална мрежа Ethernet. Маршрутизаторът обаче няма запис в своята ARP таблица за IP адреса на получателя. В този случай той трябва да се обърне към плоскостта за контрол на мрежата и използвайки протокола ARP, да открие MAC адреса на получателя. След като този MAC адрес е записан вече в ARP таблицата, пакетът, както и всички следващи пакети към този IP адрес, ще се предават директно, без допълнителни „изключения".

Втори пример: В интерфейса на маршрутизатора пристига пакет, който има максимална единица за предаване (MTU) от 1500 байта. Маршрутизаторът решава, че този транзитен пакет трябва да бъде изпратен в интерфейс с MTU = 1200 байта. Това изисква маршрутизаторът да фрагментира пакета. Трябва да се провери дали това е допустимо, т.е. да се провери стойността на бита DF (Do not fragment) в заглавната част на IP пакета. Ако DF = 0, пакетът трябва да се раздели на два пакета и след това те да се изпратят. Ако DF = 1, маршрутизаторът трябва да отхвърли пакета и да генерира съобщение за грешка на ICMP тип 3, код 4 (Необходима е фрагментация, но тя е забранена) и да изпрати това

съобщение на източника на получения пакет. И в двата случая маршрутизаторът трябва да използва допълнителни ресурси, за да отработи ситуацията.



Фиг.4 Плоскост за предаване на данни

Както можете да се убедите дори само от тези два примера, законният, позволен трафик в плоскостта за предаване на данни може да влияе на производителността на маршрутизатора и мрежата чрез предизвикване на изключителни условия, които маршрутизаторът трябва да изпълни. Повечето книги за сигурност описват методи за защита на трафика в плоскостта за предаване на данни от различни атаки. Съществува обаче и необходимост да се защитава и самия маршрутизатор от този трафик при възникване на изключителни условия. Ефективната политика за сигурност в плоскостта за предаване на данни трябва да преследва и двете цели.

4.2 Плоскост за контрол на мрежата (control plane)

Плоскостта за контрол на мрежата е логическа единица, която е свързана с маршрутизиращите процеси и функции, и се използва за създаване и поддържане на необходимата интелигентност за състоянието на мрежата и интерфейсите на

маршрутизаторите. Тази плоскост включва мрежови протоколи за маршрутизация, за сигнализация, за състоянието на връзките, които протоколи се използват за комуникация между различните мрежови устройства, както и други протоколи, които се използват за изграждане на мрежови услуги. Следователно плоскостта за контрол на мрежата е отговорна за динамичното изграждане на мрежата и осигурява механизми с които маршрутизаторите научават топологията и оперативното състояние на мрежата. Без плоскостта за контрол на мрежата всички останали плоскости не могат да функционират. Фиг.5 илюстрира основните концепции на плоскостта за контрол на мрежата.

Плоскостта за контрол на мрежата винаги включва входящи пакети за маршрутизатора. Тези пакети се генерират и консумират от различни контролиращи процеси, които са стартирани в маршрутизатора. Това могат да бъдат пакети от слой 3 на различните маршрутизиращи протоколи като OSPF и BGP, или на други протоколи свързани с поддържането на таблиците за пренасочване, като например Protocol Independent Multicast (PIM), Label Distribution Protocol (LDP) и Hot Standby Routing Protocol (HSRP).

Плоскостта за контрол на мрежата също включва транзитни пакети. Например има пакети на eBGP (multihop packets), които преминават през няколко вътрешни маршрутизатора на мрежата на доставчика и за тези маршрутизатори те имат транзитен характер. Тези пакети не са предназначени за процесите в междинните маршрутизатори, но несъмнено са част от плоскостта за контрол на мрежата.

Като други примери можем да посочим виртуалните връзки при OSPF и протоколът за резервиране на ресурси Resource Reservation Protocol (RSVP). Протоколът ICMP е част от плоскостта за контрол на мрежата, който обикновено генерира съобщения в отговор на грешки при доставката на IP пакетите или за диагностични цели. Плоскостта за контрол на мрежата също включва някои не-IP пакети от слой 3 като тези на маршрутизиращия протокол IS-IS и пакети от слой 2 на CDP, ATM, PPP и LCP.

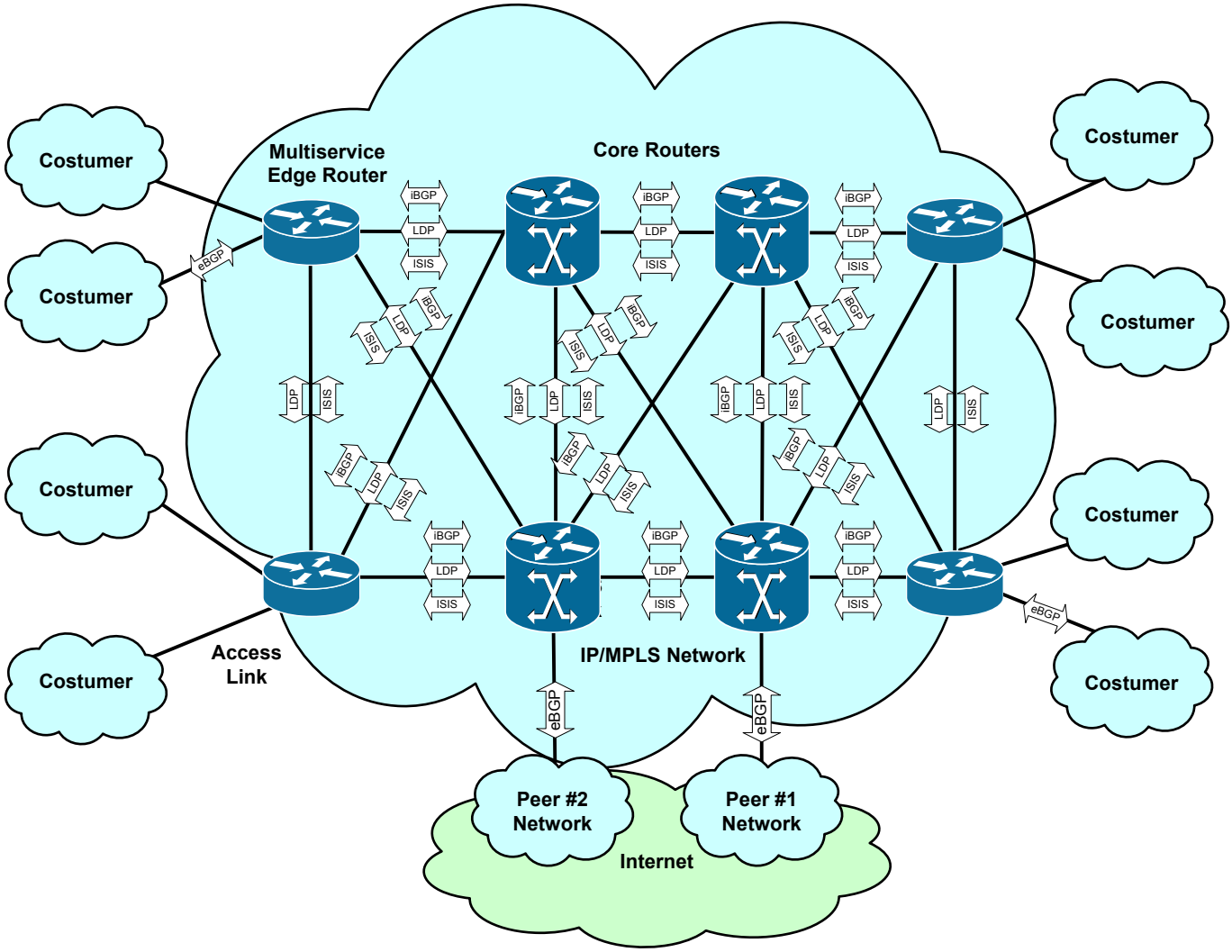
Плоскостта за контрол на мрежата обикновено се свързва с пакетите генерирани от мрежовите устройства и предназначени за самите тях. Крайните потребители нямат пряк достъп до тази плоскост. Единственото изключение тук е ping на ICMP, което приложение позволява на крайните потребители да използват плоскостта за контрол на мрежата, за да получат информация за достижимост на мрежа.

Защитата на плоскостта за контрол на мрежата е от критично важно значение както за маршрутизаторите, така и за мрежовите операции. Ако тази плоскост е компрометирана, нищо вече не може да гарантира състоянието на мрежата. Нарушенията в нея влияят неблагоприятно на всички останали плоскости. Различните мрежови устройства са различно застрашени в зависимост от това, къде те се намират в мрежата. Например граничните маршрутизатори в мрежата на доставчика на услуги са по-застрашени, тъй като те са директно свързани с мрежите на различните неконтролируеми клиенти. При граничните маршрутизатори на корпоративните мрежи също имаме повишен риск.

4.3 Плоскост за управление на мрежата (management plane)

Плоскостта за управление на мрежата е логическа единица, която описва трафика използван за достъп до мрежовите устройства и за тяхното управление. Тя осигурява всички функции необходими за наблюдението на мрежата и нейната поддръжка. Пакетите на тази плоскост се предават заедно с пакети на другите плоскости, т.е. in-band. Много от

доставчиците на услуги и големи корпорации изграждат обаче и свои собствени отделни мрежи за управление (out-of-band) с цел да има достъп до мрежовите устройства дори тогава, когато главният път in-band е прекъснат. Основните концепции на плоскостта за управление са илюстрирани на Фиг.6.



Фиг.5 Пример на плоскост за контрол на мрежата

Плоскостта за управление винаги включва входящи пакети за маршрутизатора. Тези пакети се генерират и консумират от различни процеси за управление стартирани в маршрутизатора, като например SSH, FTP, TFTP, SNMP, Syslog, TACACS+ и RADIUS, DNS, ROMMON и други, които персоналът на центъра за наблюдение на мрежата и приложенията използват.

Плоскостта за управление на мрежата също включва транзитни пакети. В зависимост от това къде персоналът и сървърите за управление се намират, всички пакети на изброените по-горе протоколи се явяват като транзитни за междинните маршрутизатори и входящи пакети за крайните маршрутизатори. Трафикът за управление обикновено е напълно вътрешен за мрежата и се появява само в някои определени интерфейси на маршрутизаторите.

Плоскостта за управление на мрежите много рядко включва IP пакети-изключения. Тя обаче може да включва не-IP пакети-изключения. Като пример тук може да се посочи протоколът CDP, който работи в каналното ниво и позволява маршрутизаторите и комутаторите динамично да се откриват един друг.

Защитата на плоскостта за управление на мрежата е също толкова критично важна за маршрутизаторите и мрежовите операции, както и защитата на плоскостта за контрол. Една компрометирана плоскост за управление на мрежата неизбежно води до неоторизиран достъп и позволява хакерите да продължат атаките си към останалите плоскости на IP трафика, като добавят маршрути, променят транспортните потоци или просто филтрират транзитните пакети. Нападателите многократно са демонстрирали способността си да компрометират маршрутизаторите, когато в мрежата се използват слаби защитни механизми (например некриптирани пароли в Telnet).

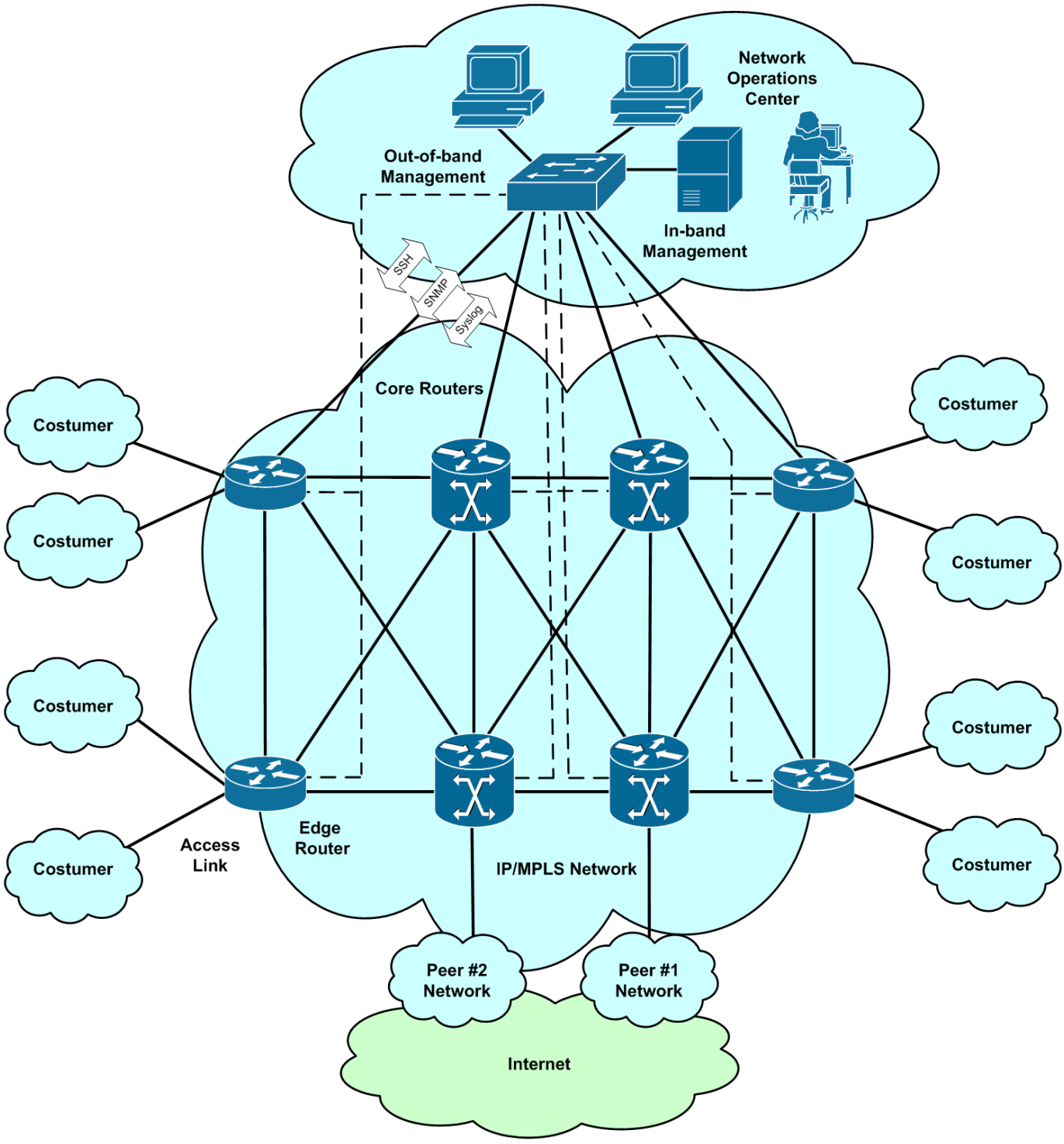
4.4 Плоскост за услуги (services plane)

Конвергенцията на мрежите води до появата на множество услуги с различни характеристики, които използват общото ядро на IP мрежата. Всички тези услуги могат да бъдат разглеждани в рамките на една плоскост за услуги (services plane), така че към тях да се прилага едно последователно отношение в цялата мрежа. Плоскостта за услуги е логическа единица, която включва клиентския трафик от мрежово базираните услуги като VPN тунелиране (MPLS, IPSec и Secure Socket Layer – SSL), от интерфейса между частните и публичните мрежи (Network Address Translation – NAT), от защитните стени (Firewalls), от системите за откриване на проникванията (Intrusion Detection Systems – IDS), от системите изискващи определено качество на услугата QoS (пренос на глас и видео), както и от много други. Основните концепции на плоскостта за услуги са илюстрирани на Фиг.7.

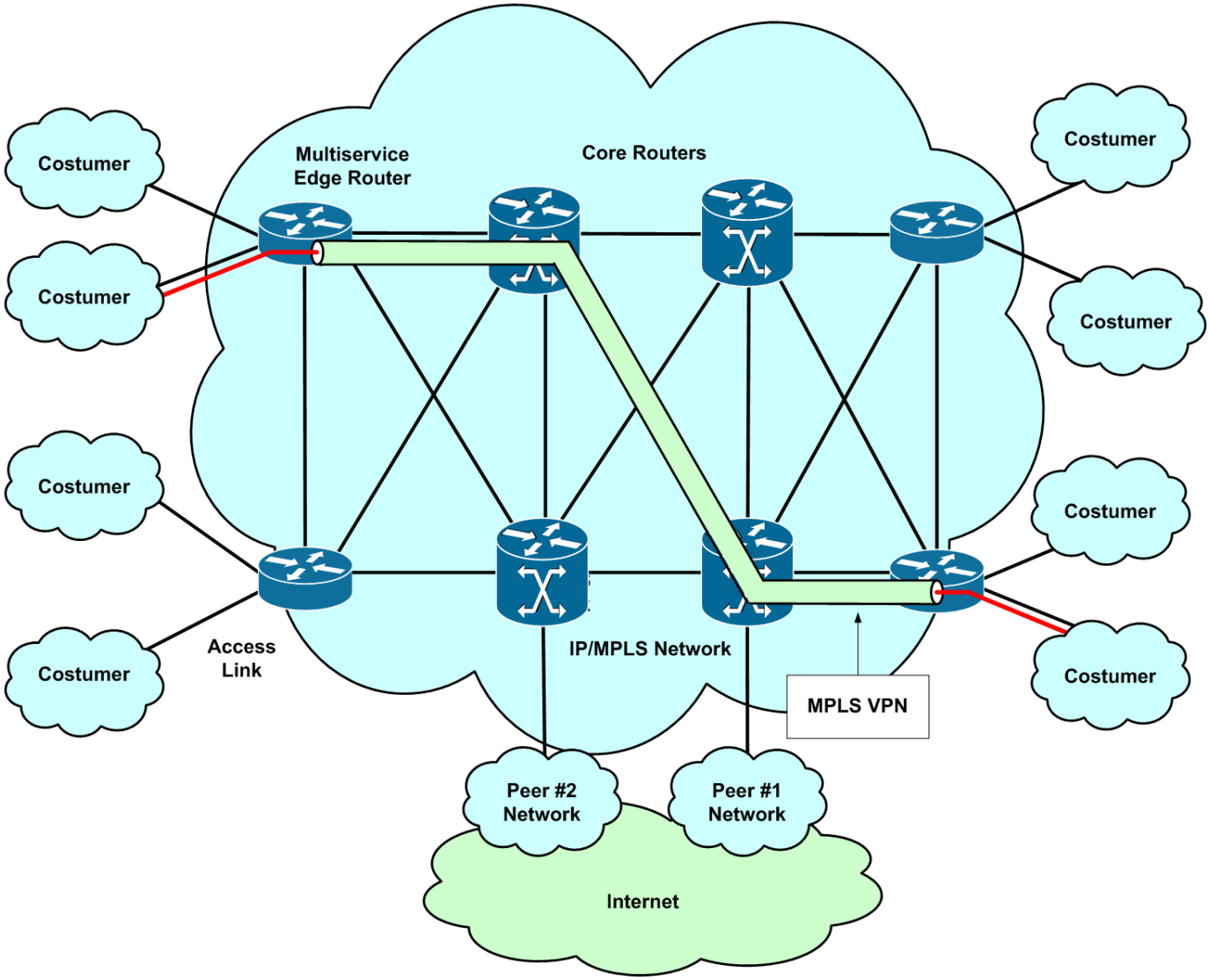
Плоскостта за услуги по същества съдържа „клиентски" трафик, т.е. както и плоскостта за предаване на данни, но с една голяма разлика. Към трафика в тази плоскост трябва да се прилагат специални мрежови функции и трябва да бъде обработван по един и същи начин от край до край в мрежата. За пакетите от плоскостта за предаване на данни обикновено се прилага само вградената поддръжка за IP доставка. Наличието на различни видове услуги предполага създаването и налагането и на различни политики за сигурност.

Както вече беше казано, трафикът в плоскостта за услуги се обработва различно от трафика в плоскостта за предаване на данни. Следните примери илюстрират това.

- *Криптирани тунели използващи SSL или IPSec.* При този тип частни виртуални мрежи (VPN) обикновено се прибягва до вътрешно пренасочване на пакетите към специален криптографски хардуер. За това се грижат допълнителен процесор и специализирани превключващи схеми. Служебното капсулиране в тунелите често сменя характера на трафика. В самия тунел трафикът е транзитен, но за последния маршрутизатор на изхода от тунела той се променя във входящ, защото там трябва да бъде преобразуван отново (декапсулиран).



Фиг. 6 Пример на плоскост за управление



Фиг.7 Пример на плоскост за услуги

- *Разделна маршрутизация при MPLS VPN*. Маршрутизаторите с MPLS VPN услуги трябва да поддържат за всеки един клиент отделни виртуални маршрутни и пренасочващи таблици. Този процес се нарича Virtual Routing and Forwarding (VRF) [1]. Това изисква допълнителна памет и допълнителна информация в пакетите (overhead), което пък от своя страна може да наложи впоследствие тяхното фрагментиране.

- *Мрежова защита с използване на защитни стени, системи за предпазване от проникване (Intrusion Protection Systems – IPS) и други подобни системи [2].* Прилагането на услуги за мрежова защита често влияе върху характеристиките на трафика. Защитните стени и IPS обикновено изискват потоци със симетричен трафик, т.е пакетите на изходящия трафик да следват същия път, както пакетите на входящия трафик. Симетричните транспортни потоци не са присъщи на IP и трябва изкуствено да се налагат.

- *Мрежови споразумения за ниво на обслужване (Service-level Agreements – SLA) с използване на QoS.* QoS осигурява виртуален клас от обслужващи мрежи (Class of Service – CoS) като се използва една физическа мрежа. Прилагането на политиките на QoS влияе върху другия, не-QoS трафик, чрез промяна в механизмите за препредаване на пакети, като се налагат допълнителни ограничения. Например MPLS VPN мрежите (RFC 4364) добавят към протокола BGP механизми за разделна маршрутизация и протоколи LDP и RSVP за изчисления на пътищата за пренасочване. IPSec VPN добавя механизма IKE (Internet Key Exchange) към плоскостта за контрол с цел генерирането на ключове и изграждането и поддържането на тунели. Предявяват се допълнителни изисквания и към плоскостта за управление на мрежата. Управлението на един тунел на IPSec VPN изисква взаимодействие с всеки един маршрутизатор участващ в предоставянето на услугата.

Гарантирането на сигурността в плоскостта за услуги е от решаващо значение за стабилна и надеждна доставка на трафик в тези специализирани транспортни потоци. В някои случаи това може да се реализира лесно. Капсулирането на генерирания от потребителя IP трафик с обща заглавна част на пакетите за дадена услуга позволява опростен подход за сигурност. Трябва само да се погледне за типа на услугата, а да не се гледа в индивидуалния потребителски трафик използващ тази услуга (както е например в плоскостта на предаване на данни). В някои случаи такова капсулиране може да даде допълнителна защита на ядрото на мрежата, защото сравнително „ненадеждния" потребителски трафик може да бъде изолиран в обвивката на услугата и да няма допир с мрежовата инфраструктура. Например MPLS VPN маршрутизиращите функции са разделени на маршрутизиращи функции за отделен потребител и маршрутизиращи функции на мрежовата инфраструктура. Зависимостите между плоскостите за услуги, контрол и управление създават допълнителна сложност и трябва да се анализират много внимателно.

5. Различни концепции за обработка на пакетите в IP маршрутизаторите

Маршрутизаторите са създадени за колкото е възможно по-ефективно пренасочване на пакетите от плоскостта за предаване на данни и от плоскостта за контрол на мрежата. Същите тези маршрутизатори трябва да изграждат и поддържат мрежата като се използват плоскостите за контрол и управление. Концепцията за разделянето на трафика на различни плоскости е „логическа". Тя позволява да се разработят и въведат специфични изисквания за сигурност. Както беше показано на Фиг.3, концепциите за сигурност на трафика могат да се разглеждат в зависимост от това къде даденият маршрутизатор се намира в мрежата. Къде се генерира трафикът и накъде е насочен? Къде са границите на мрежата и какъв трафик може да преминава през тези граници? Кои IP адреси трябва да бъдат включени за рекламиране в различните протоколи за маршрутизация? Тези и много други въпроси ще се обсъждат в този раздел.

Маршрутизаторите разпределят реалните, действителни пакети в мрежата. Те са автономни устройства и действията им са съобразени само с техния хардуер, софтуер и конфигурация. Разбирането на това как маршрутизаторът насочва всеки един тип пакети към различните интерфейси и ресурсите, които се използват за обработката на тези пакети, е от ключово значение за сигурността на IP трафика.

Въпреки че ще се фокусираме главно върху маршрутизаторите на Cisco, разгледаните тук понятия съвсем не се отнасят само до тази платформа. Всяко мрежово устройство което „докосва” даден пакет има своя хардуерна и софтуерна архитектура, която е изградена за да обработва пакета, да определи какво точно трябва да се направи с него и каква политика да се приложи към него. Терминът „политика” в този контекст означава най-общо всяко действие прилагано към пакета, например пренасочване, отхвърляне, промяна на неговите размери, размножаване, капсулиране и т.н.

Основната задача на маршрутизатора е да предаде пакета от интерфейс в една мрежа към интерфейс в друга мрежа. Всеки мрежов интерфейс представлява или пряко свързан сегмент в който се намират хостове и сървъри, или връзка към друго маршрутизиращо устройство по пътя към крайната дестинация на пакета. Най-общо процесът на вземане на решение в слой 3 на един IP маршрутизатор включва следните стъпки (в скоби е подадена и терминологията на английски за да има съвпадение с Фиг.8):

1. Пакетът постъпва във входния интерфейс (IP packet received)

2. Изчислява се контролната сума и се сравнява със същата такава в заглавната IP част на пакета с цел валидиране на целостта му (Header checksum valid?). Ако контролните суми не съвпадат, пакетът се отхвърля (Drop Packet).

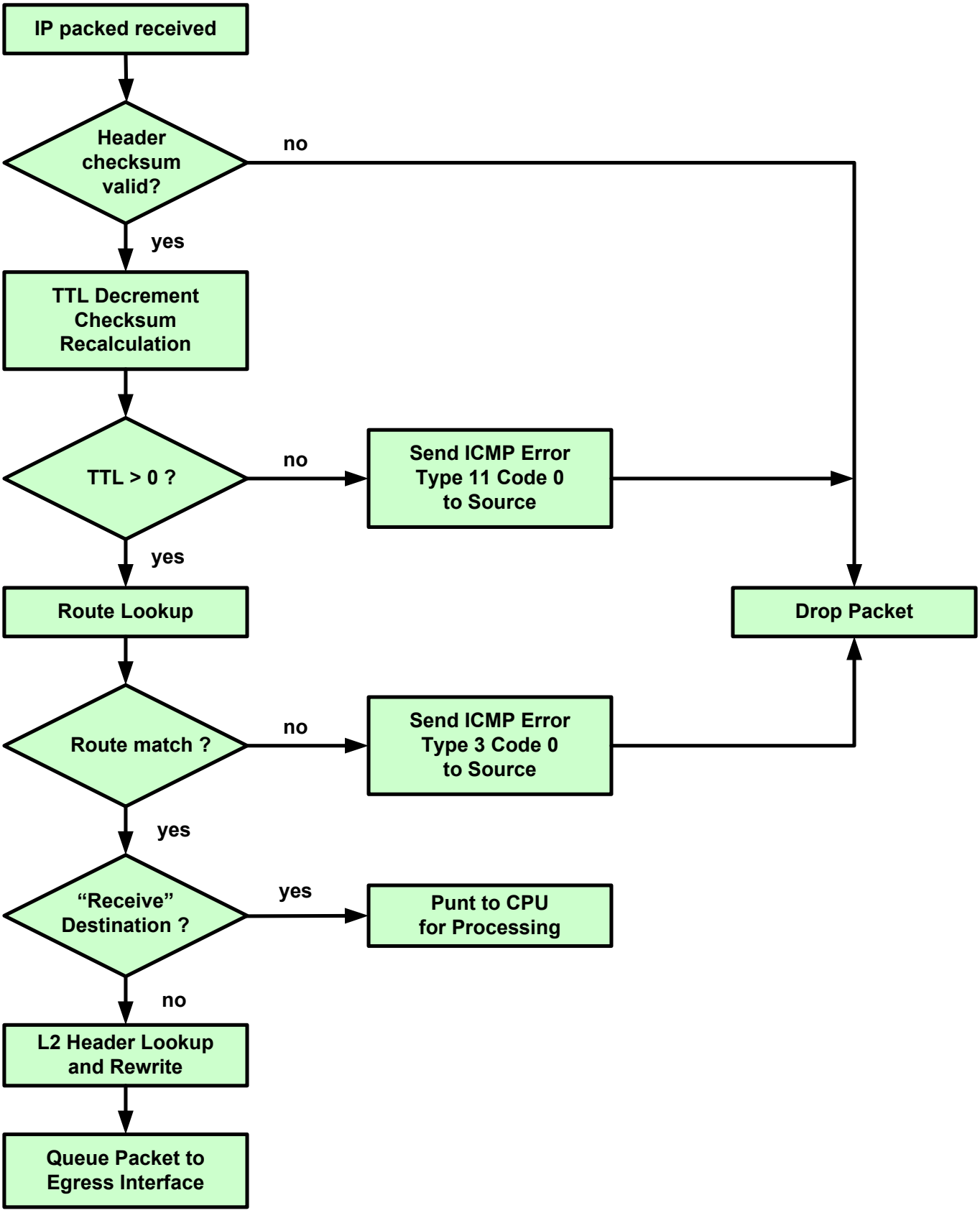
3. Полето TTL (Time-to-Live) в IP заглавната част се намалява с единица и контролната сума се изчислява отново (защото данните в тази заглавна част вече са променени) (TTL Decrement Checksum Recalculation).

4. Новата стойност на TTL се проверява, за да се гарантира, че тя е по-голяма от 0. Ако не е, пакета се отхвърля, генерира се съобщение тип 11 (time exceeded) на ICMP, и това съобщение се изпраща към източника на пакета (Send ICMP Error Type 11 Code 0 to Source).

5. При валидност на TTL полето се проверява IP адреса на получателя (Route Lookup). Местоназначението може да бъде някъде извън маршрутизатора (транзитен пакет) или в самия маршрутизатор (входящ пакет за маршрутизатора). Ако няма съвпадение (адресът на получателя не съществува в маршрутната таблица) (Route match ?), пакета се отхвърля и се генерира съобщение на ICMP за недостижимост на местоназначението тип 3 (Send ICMP Error Type 3 Code 0 to Source).

6. Ако имаме съвпадение, то се извършва подходящо капсулиране от слой 2 на информацията (L2 Header Lookup and Rewrite) и пакетът се изпраща (транзитно) към подходящия интерфейс (Queue Packet to Egress Interface). Когато пакетът е входящ за самия маршрутизатор, той се пренасочва към процесора на маршрутизатора за обработка (Punt to CPU for Processing).

Този процес е илюстриран на Фиг. 8



Фиг. 8 Пример за обработка на IP пакети в маршрутизатора

Разбира се, истинският процес на обработка на пакетите е значително по-сложен от този показан на Фиг.8. Върху него влияят такива параметри като наличната памет, входно-изходния хардуер, различните видове IP пакети, конфигурираните политики, както и много други фактори. Обикновено по-голямата част от пакетите са в плоскостите за предаване на данни и за услуги. Трафикът в плоскостите за контрол и управление на мрежата е само малка част от целия трафик. Има и изключения, когато пакетите от плоскостта за предаване на данни изискват допълнителни ресурси от плоскостта за контрол или когато пакетите не могат да бъдат обработвани по нормалния механизъм за препредаване на пакети.

По принцип маршрутизаторите обработват транзитните пакети, входящите за маршрутизатора пакети и пакетите-изключения по различен начин. Има специализирани маршрутизатори, които са оптимизирани да обработват транзитни пакети и те се справят с тази задача много бързо и ефикасно. От особено значение обаче е как един маршрутизатор обработва входящите за него пакети и пакетите-изключения. Начинът на тази обработка влияе както върху производителността, така и върху уязвимостта на маршрутизатора и неговата устойчивост на атаки.

Повечето маршрутизатори на Cisco използват програмното осигуряване Cisco IOS за комутирането на пакетите. Когато се появи първата разработка на IOS, съществуваше само един механизъм за комутиране. Този метод, известен като *процесорно комутиране (Process Switching)*, е много прост и не-особено ефективен. С нарастването на скоростта на мрежата и изискванията за висока производителност, бяха направени някои подобрения в Cisco IOS, като се въведоха усъвършенствани методи за комутиране. Бяха разработени и вградени в маршрутизаторите специализирани хардуерни компоненти. Днес разполагаме с маршрутизатори на Cisco, които препредават пакетите със скорост от хиляди пакети в секунда (Kpps) до стотици милиони пакети в секунда (Mpps). Такива високи скорости се постигат с използването на хардуерни устройства, изградени главно със специализирани приложни интегрални схеми (Application-Specific Integrated Circuits – ASIC). Други параметри, като скоростите на входно-изходните памети и производителността на вътрешните магистрали също имат голямо значение за скоростта на комутиране. Предизвикателство е да се постигне максимална производителност при ограничен набор от ASIC, процесори, входно-изходни магистрали, памети и разбира се, цена.

По принцип Cisco IOS ни предлага днес три метода за комутиране:

- *Процесорно комутиране (Process Switching):* Пакетите се обработват (и понякога изпращат) директно от CPU на маршрутизатора.

- *Бързо комутиране (Fast Switching):* Пакетите се предават с прекъсвания на CPU и използване на кеш-записи създадени при процесорно комутиране.

- *Експресно пренасочване на Cisco (Cisco Express Forwarding):* Пакетите се изпращат като се използва предварително изчислена и много добре оптимизирана версия на маршрутната таблица.

По-долу ще разгледаме всеки един от тези три метода по-подробно. Целта не е да се опишат всички възможни механизми и методи за оптимизация използвани в тях. Такава информация читателят може да намери например в [3], [4], [5], [6]. Целта е да се проучи

как тези три метода за комутиране обработват пакетите в различните плоскости на IP трафика, да видим какво влияние това оказва върху производителността на маршрутизатора, а от там и върху стабилността на мрежата и нейната сигурност.

5.1 Процесорно комутиране (Process Switching)

Основният и най-стар метод за комутиране е процесорното комутиране. Той е и най-бавен. При него обработката на съобщенията и вземането на решенията се извършват от маршрутизиращия процесор. Терминът маршрутизиращ процесор (route processor) се употребява за описание на модул, който съдържа CPU, системен софтуер, и различни компоненти памет, които се използват от маршрутизатора за да предаде пакета. При този метод всяка една заявка за обслужване на пакет се нарежда в опашка и се отработва от софтуера на маршрутизиращия процесор. Фиг.9 илюстрира отделните стъпки, описани по-долу и участващи в процеса на комутиране:

1. Процесът на комутация започва в момента, когато хардуерът на мрежовия интерфейс (наричан често интерфейсен процесор – Interface Processor) получи пакета и го прехвърли във входно/изходната памет (организирана като входяща опашка – Input Queue). След това хардуерът на мрежовия интерфейс прекъсва CPU за да го предупреди, че във входящата опашка има пакет очакващ обслужване. IOS актуализира своите входящи броячи на пакети.

2. Софтуерът на IOS проверява информацията в заглавната част на пакета (типа капсулиране, заглавната част на мрежовия слой и т.н.), определя че това е IP пакет, след което го нарежда във входна опашка на пакети за комутиране, където той очаква софтуерен процес (процедура) да го обработи.

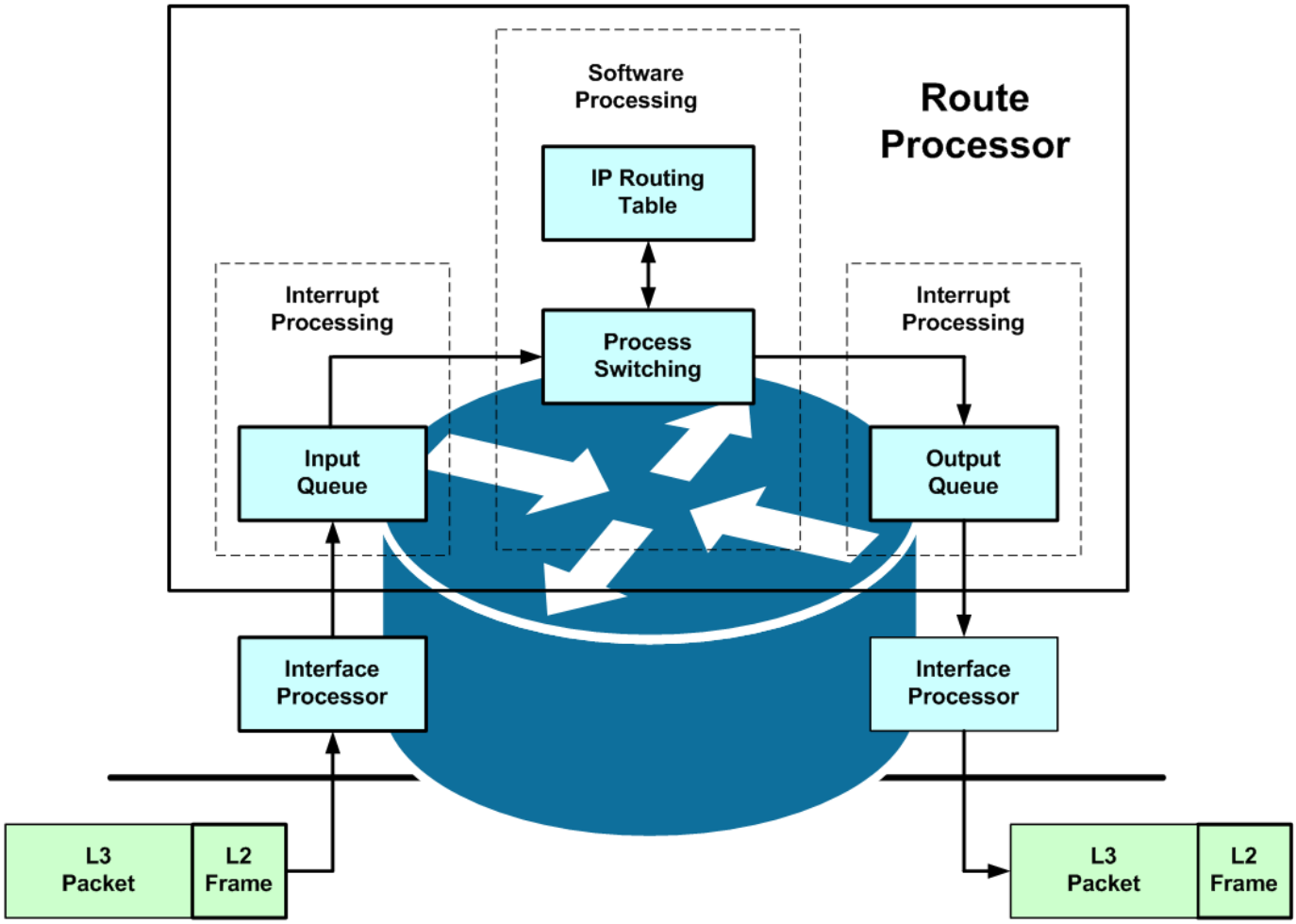
3. Процесорът претърсва IP маршрутната таблица (IP Routing Table). Когато намери съвпадение на маршрут, той извлича от нея IP адреса на следващия маршрутизатор, неговия MAC адрес от ARP-кеш таблицата и създава нова заглавна част на пакета, след което го нарежда в изходящата опашката (Output Queue) на другия мрежов интерфейс.

4. Хардуерът на изходящия мрежов интерфейс изважда пакета от опашката и го предава по мрежата. След това прекъсва CPU за да го уведоми, че пакетът е предаден. IOS актуализира своите изходящи броячи на пакети и освобождава мястото в опашката.

Вече сте забелязали, че този метод на комутиране има съществени недостатъци по отношение на производителността. Първо, всеки пакет се обработва по определена предварително процедура. Всички следващи пакети принадлежащи на един и същи поток ще се обработват по тази процедура, т.е. по един и същи начин. В тази схема няма механизми, които да разпознават, че следващите пакети са от същия поток и че измененията засягащи L2 и L3 параметрите вече са били изчислявани и прилагани.

Второ, понеже процесорното комутиране изисква проверка в маршрутната таблица за всеки пакет, то когато размерът на таблицата нарасне, значително нараства и времето за нейното претърсване (а от там и общото време за комутиране). Рекурсивните маршрути допълнително увеличават времето за претърсване на маршрутната таблица.

От гледна точка на плоскостта за предаване на данни е ясно, че процесорното комутиране изпълнява идентични функции за всеки пакет в тази плоскост, независимо от вида на пакета, защото всеки пакет трябва да се обработва от процесора. В зависимост от вида на пакета обаче, след като IOS провери заглавната част на пакета, тя определя кой софтуерен процес да поеме пакета за обработка. Понякога се изисква допълнителна обработка за определени пакети и това влияе на производителността на маршрутизатора.



Фиг.9 Схема на процесорно комутиране

Плоскост за предаване на данни: Транзитните пакети от тази плоскост се обработват от маршрутизиращия процесор, точно както е показано на Фиг.9. Тъй като CPU има ограничена тактова честота, то времето за анализ на пакетите, изчисляване на маршрутите и всички други функции, които трябва да се извършват, също е ограничено. Производителността на предаването зависи от натоварването на CPU и може да варира. Съществува горна граница на скоростта на обработка на пакетите, т.е. максимален брой пакети за секунда (packets per second – pps), независимо от скоростите на входящите и изходящи интерфейси. Необходима е също и допълнителна обработка на пакетите-изключения. Например при TTL=0 пакетът трябва да се отстрани и да се генерира ICMP съобщение за грешка, което да се изпрати обратно до първоизточника. Пакетите, които използват IP опции също изискват допълнителна обработка на заглавната част. Когато броят на пакетите-изключения нарасне значително спрямо броя на нормалните транзитни пакети, това оказва влияние върху производителността. Следователно контролирането

на въздействието на пакетите-изключения може да бъде от решаващо значение за защита на ресурсите на маршрутизатора.

Плоскост за контрол на мрежата: Транзитните пакети от плоскостта за контрол се обработват абсолютно по същия начин както транзитните пакети от плоскостта за предаване на данни. Пристигащите пакети за маршрутизатора и не-IP пакетите-изключения (например пакетите от слой 2 за поддържане на връзката, пакетите на IS-IS и други) следват същия процес както показания на Фиг.9. Въпреки това, когато се установи, че те са пакети от този вид, за тяхната обработка се използват други контролни процедури и се консумират други, допълнителни ресурси. Например честите актуализации на маршрутизиращите протоколи (което се получава при нестабилни интерфейси) водят до рекламирания на маршрути и преизчисления на пътища и в резултат до голямо временно натоварване на процесора. Това натоварване от своя страна може да доведе до загуба на пакети от плоскостта за предаване на данни, ако маршрутизаторът не е в състояние да обслужва заявките от опашките. Правилното проектиране на мрежата може да намали нестабилността при маршрутизацията. За този тип платформи с процесорно комутиране е критично важно да се предотврати влиянието на подменени (spoofed) и злонамерени (malicious) пакети, които да използват ресурсите на маршрутизатора и да нарушават стабилността на цялата мрежа.

Плоскост за управление на мрежата: Транзитните пакети от плоскостта за управление се обработват абсолютно по същия начин както транзитните пакети от плоскостта за предаване на данни. Пристигащите управляващи пакети за маршрутизатора следват същия процес както показания на Фиг.9. Въпреки това, когато се установи че това са пакети от този вид, те се предават за обработка на отделни подходящи процедури за управление на мрежата. Трафикът за управление на мрежата обикновено не съдържа IP пакети-изключения, но може да съдържа не-IP пакети (например CDP пакети). По принцип трафикът в плоскостта за управление на мрежата оказва незначително влияние върху производителността на централния процесор. Възможно е при някои управляващи действия, като често запитване при SNMP или при стартиране на операции за проследяване (debug) за откриване на грешки, да се получи висока степен на използване на процесора. Прилагането обаче на внимателно дефинирани приемливи политики би следвало да възпрепятства неумишлени въздействия върху CPU. Въпреки това, тъй като трафикът на плоскостта за управление се обработва директно от CPU, възможността за злоупотреба изисква неотменно прилагането на политики за сигурност в тази плоскост.

Плоскост за услуги: Пакетите от тази плоскост следват процеса показан на Фиг.9. Тези пакети обаче по принцип изискват специална обработка от страна на маршрутизатора. Примери за това са действията по капсулиране (например при GRE, IPSec или MPLS VPN) или извършване на някои специални операции (QoS) или функции на политики за маршрутизиране. Това изисква обработката на тези пакети да се извършва от различни софтуерни елементи в CPU с използването на допълнителни ресурси. По принцип пакетите в тази плоскост влияят значително върху натоварването на процесора. Ето защо основната ни загриженост тук е как да защитим интегритета на плоскостта за услуги от влиянието на подправени и злонамерени пакети върху процесора.

Въпреки че при процесорното комутиране имаме минимални възможности за оптимизация и се консумират значителни процесорни ресурси, този метод има предимството да е платформено независим и това го прави общодостъпен. Срещаме го при всички Cisco

IOS-базирани продукти. Все пак при него, от гледна точка на изпълнението, има още много какво да се желае.

Както се вижда на Фиг.9, при комутирането на всеки пакет ползваме три вида ключова информация:

- Адресът на получателя трябва да присъства в маршрутната таблица.
- Ако съществува маршрут, трябва да се знае интерфейса и IP адреса на следващия маршрутизатор.
- Трябва да е известен физическия адрес на следващия маршрутизатор.

Тази информация се определя за всеки пакет, дори ако предишния пакет е изисквал точно същата информация. В IP мрежите потокът към дадено местоназначение обикновено съдържа множество пакети. Какво би станало, ако резултатите от една заявка (комбинацията от IP адреса на получателя, интерфейса, IP и физическия адрес на следващия маршрутизатор) временно се запазят в една по-малка таблица? Можем ли така да постигнем съществено намаление на времето за обработка за по-голямата част от постъпващите пакети? Това е идеята, която стои зад бързото комутиране на пакетите в IOS.

5.2 Бързо комутиране (Fast Switching)

Бързото комутиране е софтуерно подобрение на процеса на комутиране, което ускорява обработката на пакетите като използва пътека за пренасочване (forwarding path). При него се използва кеш памет, в която се съхранява информация за потока от пакети. При всеки пакет първо се проверява тази памет, вместо да се използва тромавата процедура за претърсване на цялата маршрутна таблица. На Фиг.10 са показани описаните по-долу стъпки на алгоритъма за бързо комутиране:

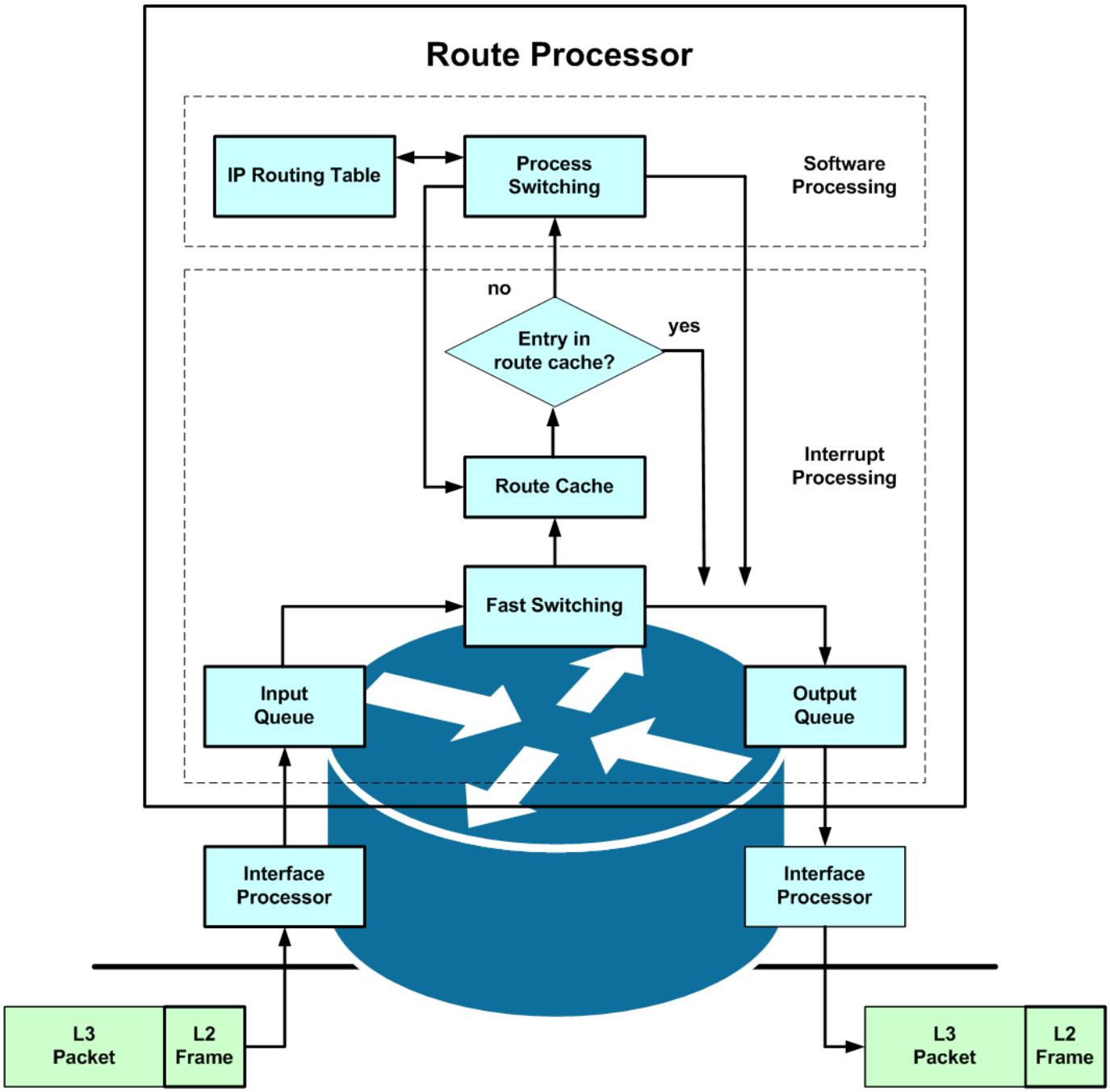
1. Бързото комутиране започва точно както процесорното комутиране. Първо интерфейсният процесор получава пакета и го прехвърля във входно-изходната памет, след което прекъсва CPU за да го предупреди, че има пакет очакващ обслужване. IOS актуализира своите входящи броячи на пакети.

2. Процедурата на IOS, активирана от прекъсването, проверява информацията в заглавната част на пакета (типа капсулиране, заглавната част на мрежовия слой и т.н.) и определя че това е IP пакет. Вместо да нареди пакета във входната опашка за обработка от CPU, процедурата прави справка в кеш-паметта за наличие на запис за IP адреса на получателя. Ако такъв запис съществува, информацията за изходящия интерфейс и физическия адрес на следващия маршрутизатор се извлича от него и се изгражда нова заглавна част на рамката в слой 2. Следва сигнализиране на интерфейсния процесор, че пакетът е готов за изпращане.

3. Отново както при процесорното комутиране, изходящият интерфейсен процесор изважда пакета от опашката и го предава по мрежата.

Забележете, че ако IP адреса на получателя не се намира в кеш паметта, маршрутизаторът следва процедурите на метода за процесорно комутиране, описани в

предходния раздел. Единствената разлика е, че когато е активирано бързото комутиране, след завършването на обработката на пакета се прави нов запис в маршрутния кеш за бъдеща употреба. Това означава, че всеки първи пакет от един нов поток винаги изисква процесорно комутиране. Следващите пакети са бързо комутирани. По този начин бързото комутиране разделя скъпите CPU-базирани маршрутизиращи процедури от относително простите, работещи на прекъсване, процедури за пренасочване на пакети. Записите в маршрутния кеш се създават и изтриват динамично. Нов запис се създава, когато първият пакет към дадено местоназначение е процесорно комутиран, и командата *ip route-cache* е въведена за изходящия интерфейс. Записът се изтрива, когато не е бил използван за известно време (по таймаут) или при липса на място в кеш паметта.



Фиг.10 Схема на бързо комутиране

Освен описаната функция за препредаване на IP пакети, в бързото комутиране се поддържат и много други функции, например инфраструктурни списъци за достъп (Infrastructure Access Control Lists – IACL), политики за маршрутизация, IP групово маршрутизиране (IP multicast routing) и др. Не всички функции се поддържат от бързото комутиране. Понякога се налага то просто да бъде забранено. При такава забрана маршрутизаторът преминава към процесорно комутиране. Това се налага например когато искате да проследите определени пакети (packet-level tracing). Бързото комутиране също е независимо от използваната платформа и се използва в почти-всички маршрутизатори на Cisco. В IOS то е активирано по подразбиране. Можете да проверите дали бързото комутиране е разрешено и какви записи се намират в момента в кеш паметта.

Ясно е, че бързото комутиране е създадено за ускоряване на обработката на пакети от данни. То работи много добре във високоскоростни мрежи, при които голяма част от пакетите са именно такива. Не всички функции и пакети обаче могат да бъдат бързо комутирани. В такъв случай се преминава към процесорно комутиране, което влияе нелагоприятно на производителността на маршрутизатора. Класифицирането на трафика и защитата на ресурсите на маршрутизатора става на моменти критично, особено с увеличаването на скоростта на мрежата. Когато трафикът е в нормални граници, маршрутизаторът работи добре. Ако обаче трафикът промени своя характер, например при злонамерени атаки, и това налага процесорно комутиране, маршрутизаторът ще почувства недостиг на ресурси.

Плоскост за предаване на данни: Пакетите ще бъдат бързо комутирани, когато са транзитни и в маршрутния кеш съществува вече запис. При липса на запис е необходима процесорна обработка за определяне на следващия скок и детайлите в заглавната част на рамката от слой 2. Процесорна обработка е необходима и при IP пакетите-изключения и IP пакетите съдържащи опции. Когато съотношението между IP пакетите-изключения и нормалните транзитни пакети нарасне, ресурсите на маршрутизатора могат да се изчерпят и това да окаже влияние върху стабилността на мрежата.

Плоскост за контрол на мрежата: Транзитните пакети от плоскостта за контрол се обработват при бързо комутиране абсолютно по същия начин както транзитните пакети от плоскостта за предаване на данни. Пристигащите пакети за маршрутизатора и не-IP пакетите-изключения (например пакетите от слой 2 за поддържане на връзката, пакетите на IS-IS и други) следват същия процес на бързо комутиране, както показания на Фиг.10. След като се идентифицират като такъв вид пакети, те се насочват към CPU и се обработват с други процедури и изразходват различни други ресурси. Създава се допълнително натоварване на процесора с всичките произтичащи от това последици (загуба на пакети и мрежова нестабилност).

Плоскост за управление на мрежата: Транзитните пакети от плоскостта за управление се комутират бързо абсолютно по същия начин както транзитните пакети с данни. Пристигащите управляващи пакети за маршрутизатора и не-IP пакетите следват същия процес на бързо комутиране, както тези от плоскостта за контрол. След като тези пакети се идентифицират като такива, те се насочват към CPU и се обработват от различни процедури за управление. Забележките направени за влиянието на различните видове управляващи пакети върху производителността при описанието на метода за процесорно комутиране важат напълно и при бързото комутиране.

Плоскост за услуги: Пакетите от тази плоскост следват процеса показан на Фиг.10. Тези пакети обаче по принцип изискват специална обработка от страна на маршрутизатора. Примери за това са действията по капсулиране (например при GRE, IPSec или MPLS VPN) или извършване на някои специални операции (QoS) или функции на политики за маршрутизиране. Някои от тези операции могат да се обработват с бързо комутиране, а някои не могат. Например системата за маршрутизиране policy routing се обработва с бързо комутиране, докато при GRE капсулирането не е така. Когато не е възможно бързото комутиране се преминава към процесорно комутиране. В този случай пакетите от тази плоскост могат да окажат значително влияние върху натоварването на процесора.

Разрастването на Интернет постави изискването маршрутизаторите в ядрото на мрежата да поддържат значителни по размер маршрутни таблици и високи скорости на предаване. Въпреки че бързото комутиране е едно значително усъвършенстване на технологията за препредаване на пакети, то все още има много недостатъци.

- Записите в кеш паметта се създават по заявка. Първият пакет от всеки нов поток трябва да бъде процесорно комутиран, за да се създаде нов запис. Това не е добре мащабируемо, когато през мрежата преминава значителен трафик, за който нямаме записи в маршрутния кеш. Например такъв е случаят когато научаваме за маршрути от BGP, понеже там се определя само адреса на следващия маршрутизатор, но не и интерфейса и се налага рекурсивно претърсване на маршрутната таблица.

- Записите в кеш паметта използват IP адреса на получателя, което също не е мащабируемо, тъй като основните маршрутизатори съдържат голям брой IP адреси. Размерът на паметта, в която се съхранява маршрутния кеш е ограничен и не можем да поддържаме големи таблици. Нарастването на таблицата също води до увеличение на времето за нейното претърсване, т.е. до спад на производителността.

- Бързото комутиране не поддържа разпределение на натоварването и използване на паралелни маршрути. Ако искаме да използваме такава технология трябва да деактивираме бързото комутиране и да използваме процесорно комутиране. При високите скорости използването на един процесор да върши всичко не е особено удачно.

Като решение на тези и други проблеми беше разработен един нов метод за комутиране наречен експресно пренасочване на Cisco (Cisco Express Forwarding - CEF). Той не решава само проблемите с производителността на бързото комутиране, но също така и разглежда въпроса за създаване на нова генерация „разпределени" платформи за препредаване на пакети.

5.3 Експресно пренасочване на Cisco (Cisco Express Forwarding)

При експресното пренасочване на Cisco (CEF), както и при бързото комутиране, се използва запис в кеш паметта. При бързото комутиране преминаването на първия пакет служеше за създаване на такъв запис. При CEF този механизъм е премахнат. Таблицата, която използва CEF, наречена таблица с информация за пренасочване, се изгражда предварително директно от маршрутната таблица. Използва се още една таблица,

наречена таблица за съседство, която също се изгражда предварително, като за целта се използва кеша на протокола ARP. Много е важно да се подчертае, че тези две CEF структури са предварително изградени, преди да са комутирани каквито и да са пакети. След като таблиците един път са създадени, CPU на маршрутизиращия процесор вече не е пряко ангажиран в препращането на пакети (въпреки че трябва да извършва някои допълнителни функции, например управление на паметта и др.). Предварително изградените структури на CEF значително подобряват производителността, особено на маршрутизатори с големи маршрутни таблици. По долу ще разгледаме двете основни поддържани от CEF структури, а именно:

- таблица с информация за пренасочване (Forwarding Information Base – FIB)
- таблица за съседство (Adjacency table).

5.3.1 Таблица с информация за пренасочване (FIB)

Таблицата с информация за пренасочване (по-нататък ще използваме английското съкращение FIB) е специално конструирана версия на маршрутната таблица, която се съхранява в една дървовидна структура от данни. FIB е оптимизирана за последователно високоскоростно претърсване. Тя зависи от архитектурата на маршрутизатора и от използваната в него операционна система. Търсенето на адреса на местоназначението става на байтова основа, т.е. за IP v4 са необходими максимум четири претърсвания за откриване на маршрут до всяка конкретна дестинация.

FIB съдържа всички пътища намиращи се в основната маршрутна таблица. Двете таблици във всеки момент са напълно синхронизирани. При появата на изменения в маршрутите или топологията на мрежата, IP маршрутната таблица се актуализира, и настъпилите промени се отразяват във FIB. Поради това еднозначно съответствие, FIB съдържа всички познати маршрути и не е необходимо да се поддържа маршрутен кеш, както при бързото комутиране. Във FIB са създадени специални записи “receive” за входящите пакети за маршрутизатора, т.е. за пакетите насочени към IP адреси, собственост на самия маршрутизатор. Те включват адреси присвоени на физически интерфейси, затварящи (loopback) интерфейси, тунелни интерфейси, запазени групови адреси от областта 224.0.0.0/8, както и някои бродкастни адреси. Входящите пакети за маршрутизатора се обработват от CEF както всички останали пакети, като просто се записват в опашките за локална доставка.

Във всеки входен запис на FIB има една или повече връзки към записите в таблицата за съседство, като това дава възможност за поддържане на няколко пътища за доставка с цел балансиране на натоварването.

Конкретния вид на таблицата с информация за пренасочване можете да видите, като използвате например командата **show ip cef** [7]**.**

5.3.2 Таблица за съседство (Adjacency table)

Таблицата за съседство съдържа информацията необходима за капсулиране на пакетите, които трябва да бъдат изпратени към мрежово устройство от следващия скок. CEF разглежда мрежовите устройства от следващия скок като съседи, ако маршрутизаторът е пряко свързан с тях чрез обща IP подмрежа. Всеки входен запис в таблицата за съседство

съдържа предварително изчислени заглавни части на рамките, които се използват при препращането на пакета. При наличие на повече от един маршрут, записът съдържа повече заглавни части, като това позволява да се реализира механизъм за балансиране на натоварването. Таблицата за съседство се попълва когато се открие нов съсед. Тогава се използва ARP протокола и се извършват необходимите промени.

В допълнение към информацията за интерфейса от следващия скок, в таблицата има и информация необходима за обработка на пакетите при извънредни ситуации, например когато се изискват операции, които не се поддържат от CEF (като IP настройки) или насочване на пакета към интерфейс, който ще го отстрани (като Null0 интерфейс).

Конкретния вид на таблицата за съседство можете да видите, като използвате командата **show adjacency** [7]**.**

5.3.3 Действие на CEF

Експресното пренасочване на Сиско (CEF) се активира, като в режим на глобално конфигуриране използваме командата **ip cef**. С това се разрешава използването на CEF по подразбиране във всички интерфейси на маршрутизатора, които го поддържат. CEF може да бъде активиран и деактивиран и на ниво интерфейси. За да използваме CEF, той трябва да бъде активиран на входния интерфейс, тъй като там се вземат решенията за препращане. За това в режим на конфигуриране на интерфейс се използва командата **ip route-cache cef** за активиране на CEF и **no** версията на същата команда за деактивиране на CEF.

Всеки път, когато получим пакет в интерфейс с активиран CEF, пакетът се препраща по начин илюстриран на Фиг.11 и описан по-долу:

1. Процесът при този метод започва точно по същия начин, както при останалите методи за комутиране. Първо хардуерният интерфейсен процесор получава пакета и го прехвърля във входно-изходната памет, след което прекъсва CPU за да го предупреди, че има пакет очакващ обслужване. IOS актуализира своите входящи броячи на пакети.

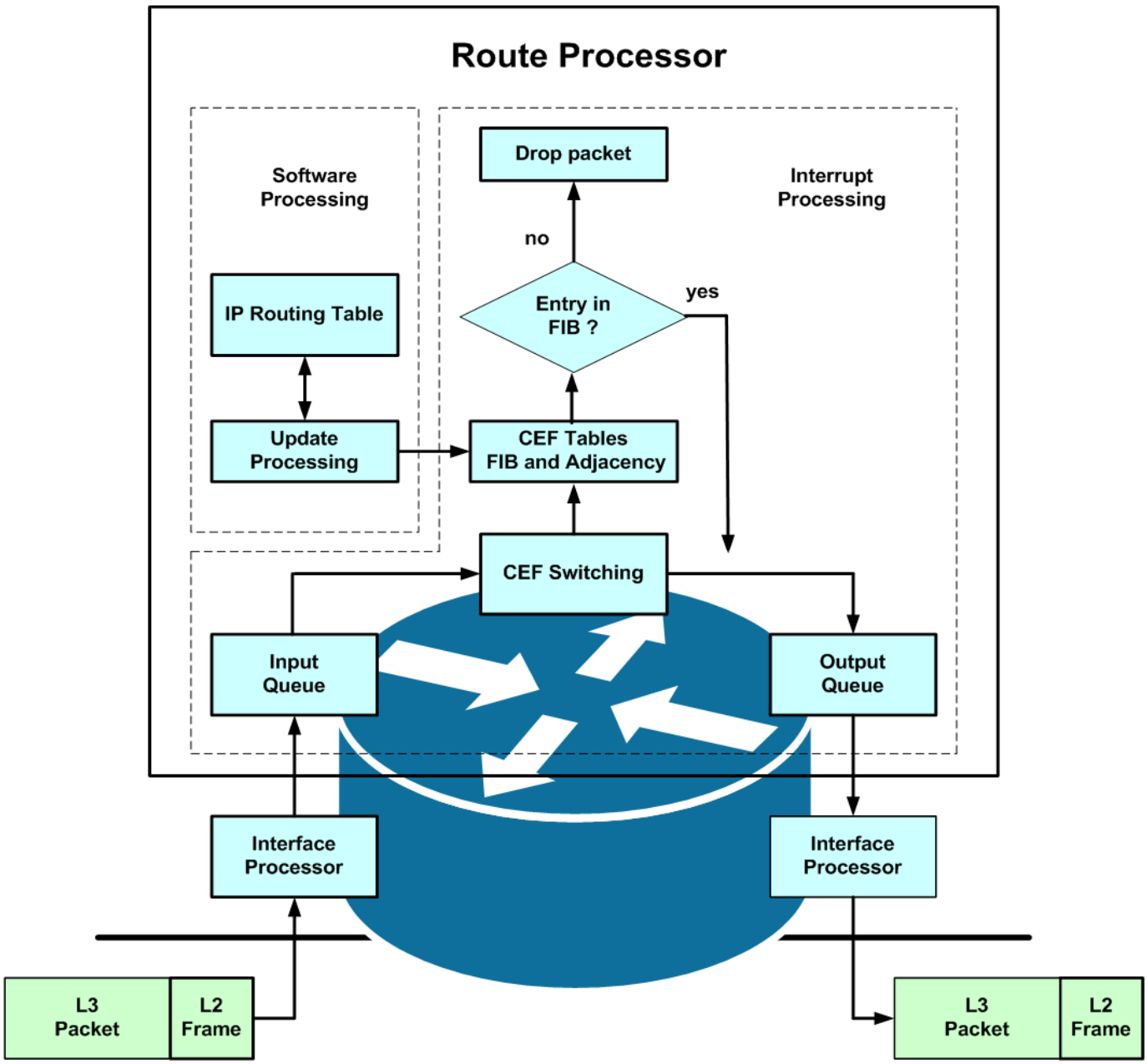
2. Процедурата на IOS, активирана от прекъсването, проверява информацията в заглавната част на пакета (типа капсулиране, заглавната част на мрежовия слой и т.н.) и определя че това е IP пакет. Вместо да нареди пакета във входната опашка за обработка от CPU, процедурата проверява за входен запис във FIB съвпадащ с IP адреса на получателя. Ако такъв запис съществува, процедурата извлича информацията за заглавната част на L2 рамката от таблицата за съседство, след което подготвя пакета за изпращане. Следва сигнализиране на процесора на изходящия интерфейс, че пакетът може да бъде изпратен.

3. Изходящият интерфейсен процесор изважда пакета от опашката и го предава по мрежата.

4. Ако адресът на получателя не е намерен във FIB, CEF просто изхвърля пакета, с което принуждава CPU да генерира съобщение на ICMP тип 3 (destination unreachable). Това е най-голямото предимство на CEF - не се изразходва

процесорно време за обработка на пакети, насочени към дестинации до които няма връзка.

От гледна точка на IP трафика, CEF не само помага за ускоряване на предаването на пакетите от плоскостта за данни, но също така и изпълнява някои допълнителни операции за много други видове пакети. Именно това е необходимо за изграждането на високоскоростни мрежи. Във всяка една мрежа съществуват множество пакети от различни типове. Те всички трябва да бъдат обработени, но не всички е възможно да бъдат обработени от CEF. В този случай се задействат алтернативни обработващи функции, което се отразява в значителна степен на производителността. Критично за мрежите се оказва разделянето на трафика в различните плоскости и защитата на ресурсите на маршрутизатора. Ще разгледаме отново всяка плоскост на трафика, но от гладна точка на CEF.



Фиг. 11 Схема на експресно пренасочване на Cisco

Плоскост за предаване на данни: CEF беше разработен за да се ускори доставката на пакетите от транзитния трафик в плоскостта за данни. Тези пакети са CEF пренасочвани, когато за тях съществуват входни точки във FIB, и са отстранявани в противния случай. Отстраняването на пакетите с неизвестни за маршрутизатора дестинации дава на CEF огромно предимство пред другите методи за комутиране, тъй като CPU не се включва за тяхната обработка, а те просто се отхвърлят. При това обаче се генерират ICMP пакети за грешки. В повечето маршрутизатори ICMP пакетите се създават и обработват от CPU. Следователно, дори при CEF, при наличието на голямо количество ICMP съобщения за грешки, наблюдаваме значително намаление на производителността на CPU. Генерирането на ICMP съобщения за недостижимост може да бъде ограничено при намаление на производителността на CPU или дори забранено. Предпазването от подправени и злонамерени пакети да попаднат в плоскостта за данни и да злоупотребят с нея също може да помогне за защитата на маршрутизатора и неговите ресурси. Както и при другите методи на комутиране се налага допълнителна обработка на пакетите-изключения. Например при TTL = 0 пакетите се отхвърлят и се връщат ICMP съобщения за грешка. IP пакетите с опции също изискват допълнителна обработка. CEF използва за такива пакети специални образци в таблицата за съседство, което означава, че CPU може да не участва в процеса на тяхната същностна обработка. В някои случаи обаче може да се изисква обработката на такива пакети от CPU след CEF. Когато съотношението на пакети-изключения към нормалните транзитни пакети стане голямо може да настъпи липса на ресурси в маршрутизатора, което влияе на стабилността на мрежата.

Плоскост за контрол на мрежата: Пакетите от плоскостта за контрол на мрежата с транзитни дестинации са пренасочвани от CEF абсолютно по същия начин както транзитните пакети от плоскостта за данни. Пристигащите пакети за маршрутизатора и не-IP пакетите-изключения (например пакетите от слой 2 за поддържане на връзката, пакетите на IS-IS и други) се насочват по специален начин за обработка към CPU. За пълната обработка на такива пакети се използват допълнителни ресурси. Следователно, независимо от използвания метод за комутиране, този тип пакети се обработват от CPU, което води до неговото високо натоварване. Това от своя страна влияе на синхронизацията на CEF таблиците (например когато трябва да бъдат изчислени промените в маршрутната таблица) и в краен резултат води до отхвърлен трафик. Тук критично се явява предотвратяването на подправени и злонамерени пакети да влияят на плоскостта за контрол на мрежата като консумират ресурсите на маршрутизатора и нарушават стабилността на цялата мрежа.

Плоскост за управление на мрежата: Пакетите от плоскостта за управление на мрежата с транзитни дестинации са пренасочвани от CEF абсолютно по същия начин както транзитните пакети от плоскостта за данни. Пристигащите управляващи пакети за маршрутизатора се насочват по специален начин за обработка към CPU. За пълната обработка на такива пакети се използват допълнителни ресурси. Трафикът в плоскостта за управление на мрежата по принцип не трябва да включва IP пакети-изключения, но може да включва не-IP (Layer 2) пакети-изключения (обикновено под формата на CDP пакети). При нормални условия трафикът в плоскостта за управление на мрежата оказва минимално влияние върху производителността на CPU. Възможно е при някои управляващи действия, като често запитване при SNMP или при стартиране на операции за проследяване (debug) за откриване на грешки, да се получи висока степен на използване на процесора. Това от своя страна ще окаже влияе на синхронизацията на

CEF таблиците и в краен резултат ще се прояви като отхвърлен трафик. Тъй като трафикът в плоскостта за управление на мрежата се обработва директно от CPU, възможността за злоупотреба се оказва критична и трябва да се приложат специални механизми за управление на сигурността.

Плоскост за услуги: Пакетите от плоскостта за услуги обикновено изискват специална обработка от страна на маршрутизатора. Като примери тук можем да изтъкнем действията по капсулирането (при GRE, IPSec или MPLS VPN) или извършване на някои специални операции (QoS) или функции на политики за маршрутизиране. Някои от тези операции могат да се обработват от CEF, други не могат. Ако една функция или вид капсулиране не се поддържа от CEF, пакетът се предава на следващото комутиращо ниво (за повечето маршрутизатори това ще бъде бързото комутиране), което ще се опита да комутира пакета като използва своя кеш. Ако не може да бъде комутиран на ниво прекъсване, пакетът се поставя в опашката за директна обработка от CPU. CEF няма да успее да комутира пакета, само ако се изискват неподдържани от него функции. Тогава това ще окаже голямо влияние върху натоварването на процесора. Защитата на плоскостта на услугите се концентрира около предотвратяването на въздействието на подправени и злонамерени пакети върху CPU.

6. Общи архитектурни концепции за изграждане на IP маршрутизатори

Сега, след като разгледахме основните методи за комутиране поддържани от IOS и беше описано въздействието на трафика в различните плоскости върху тяхното функциониране и производителност, е редно да представим различните хардуерни архитектури използвани в маршрутизаторите на Cisco. Някои маршрутизатори на Cisco не поддържат всички описани досега методи за комутиране. Освен това хардуерните варианти водят до различни нива на производителност за всяка от плоскостите на IP трафика. Следователно много важно е да се разберат конкретните възможности на производителността на всеки маршрутизатор включен в мрежата. В този раздел специално ще наблегнем върху начина по който злонамерения трафик може да влияе на хардуерната архитектура на маршрутизатора.

Изискванията за по-голяма производителност и поддържането на интегрирани услуги доведоха до съществени промени в хардуера на маршрутизаторите. Повечето маршрутизатори на Cisco използват само един активен процесор за маршрутизиране (route processor) дори когато повече от един са инсталирани. По този начин обработката се извършва в едно централно място. При някои маршрутизатори е вграден специализиран ASIC хардуер с цел ускоряване на комутирането. При други пък се използват разпределени хардуерни архитектури за постигане на максимална висока скорост на пренасочване.

Следващите раздели съдържат общ преглед на основните хардуерни архитектури, използвани в маршрутизаторите на Cisco. В тях са включени достатъчно подробности, за да се разбере добре как различните плоскости на IP трафика влияят на тяхната производителност. Повече подробности за архитектурите можете да намерите например в [4], [5], [6], [8].

6.1 Централизирани CPU-базирани архитектури

Архитектурата използвана в първоначалните оригинални маршрутизатори на Cisco, както и в няколко поколения маршрутизатори от корпоративния клас, е с централизиран, CPU-базиран дизайн. Маршрутизаторите от тази категория, които все още се намират в експлоатация, включват моделите от серии 800, 1600, 1700, 2500, 2600, 3600 и 3700. Маршрутизаторите от неостаряващата серия 7200, както и по-новите маршрутизатори от серии 1800, 2800 и 3800, както и маршрутизаторите с интегрерани услуги (ISR), също използват централизирана CPU-базирана архитектура.

Централизираните CPU-базирани архитектури разчитат един процесор да изпълнява всички функции изисквани от маршрутизатора. Това включва функции като:

- Поддържане на всички мрежови функции, такива като протоколи за маршрутизиране, кеш памети, състояния на връзките, интерфейси, глобални броячи, генериране на ICMP съобщения за грешки, както и други функции за контрол на мрежата.

- Поддържане на всички функции по обработката и пренасочването на пакетите. Тук се включват и други услуги като списъци за достъп, NAT, QoS и други, които се използват в процеса на комутиране.

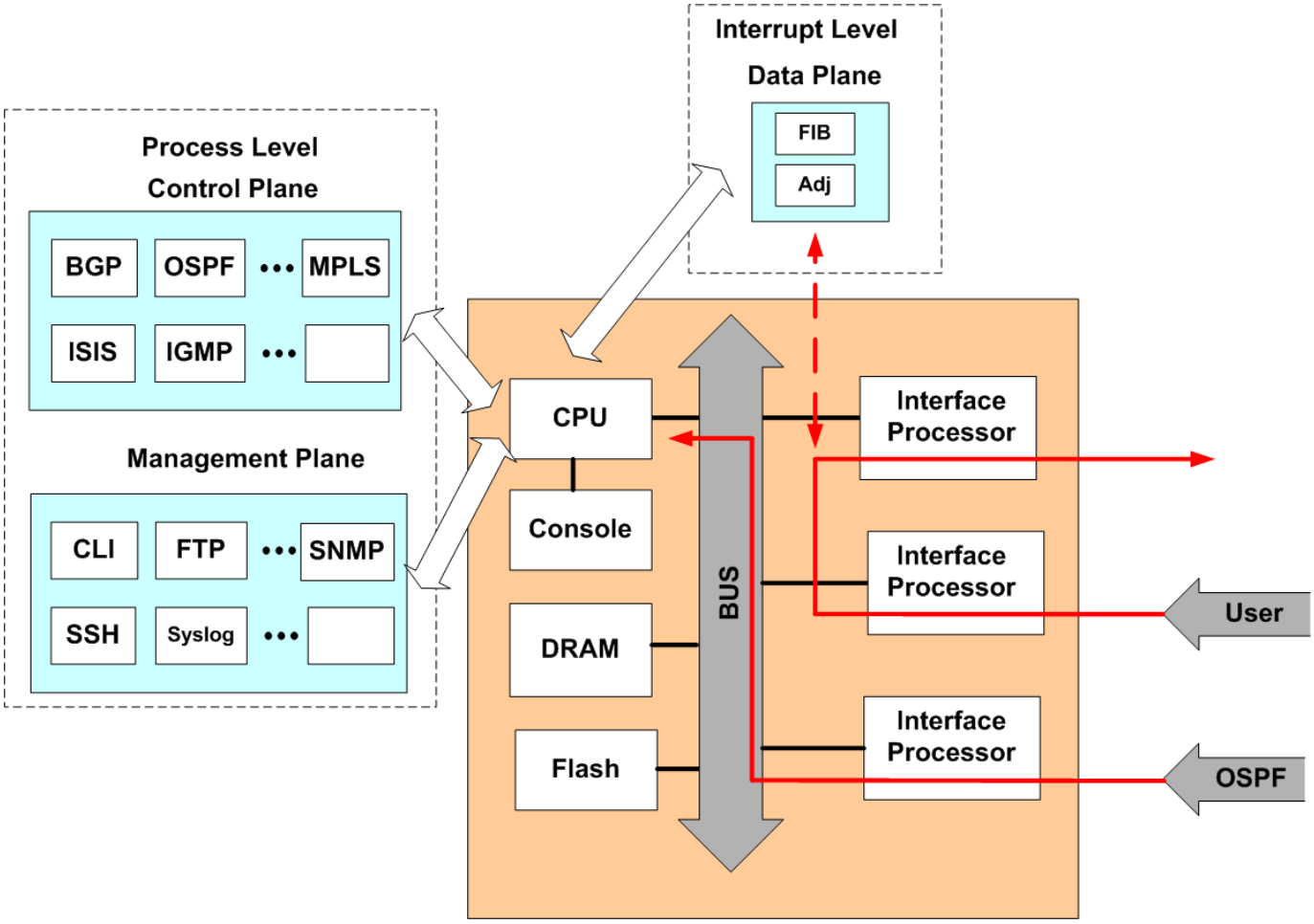
- Поддържане на всички функции свързани с конфигурирането на маршрутизатора, включително конфигуриране от командния ред, SNMP, Syslog, както и други функции свързани с управлението на устройството.

Всички тези (и други) функции се извършват от Cisco IOS софтуера. Cisco IOS е монолитна операционна система, всички софтуерни модули са статично компилирани и свързани в момента на създаването и, като тя използва едно адресно пространство. В модела по който тя функционера, грешка в една функция могат да предизвикат смущения в други функции.

Една типична централизирана CPU-базирана архитектура е показана на Фиг.12. Използването на съвременни магистрални (bus) решения, големи и бързи модули памет, най-нови процесори, както и специализирани интегрални схеми, води до повишение на общата производителност на маршрутизатора. Но дори и при използването на всички нововъведения, централизираните CPU-базирани устройства ще бъдат ограничени в производителността поради тяхната архитектура.

Както е показано на Фиг.12, централният процесор изпълнява функциите по поддръжката на маршрутизатора (CLI, управляващи функции и т.н.). Той се грижи за функционирането на маршрутизиращите протоколи, както и за изчисляването и попълването на FIB и таблицата за съседство. FIB и таблицата за съседство се намират в адресното пространство на процесора. Всички пакети преминаващи транзитно през маршрутизатора (влизащи и излизащи през различните интерфейси) се обработват от процедурата за прекъсване на CPU ако CEF може да пренасочи пакета. Пакетите които не могат да бъдат пренасочени от CEF (по бързия начин) се прехвърлят за директна обработка от CPU (бавен начин). Към тази група пакети спадат всички входящи IP пакети за маршрутизатора, които при нормални условия са пакети от плоскостите за контрол и управление на мрежата, всички IP пакети-изключения, както и не-IP пакетите.

Маршрутизаторите от тази категория са подходящи за повечето малки и средни предприятия, които се характеризират с ниска пропускателна способност, но с големи изисквания за интегрирано обслужване. Тези маршрутизатори представляват чудесен компромис между приемлива производителност, множество предлагани услуги и ниска цена. Тяхната липса на капацитет за високоскоростно предаване означава, че е необходимо да се проучат други типове архитектури.



Фиг.12 Централизирана CPU-базирана архитектура на маршрутизатор

6.2 Централизирани ASIC-базирани архитектури

С нарастването на изискванията към мрежите, CPU-базираните архитектури все по-малко са в състояние самостоятелно да гарантират приемливо ниво на производителност. За да се преодолее този недостатък, в модерните централизирани CPU-базирани платформи започнаха да се вграждат специализирани приложни интегрални схеми (ASIC) за да се разтовари CPU от някои негови задължения и да се подобри цялостната производителност на устройството. Към тази категория устройства спадат семействата на въздесъщите комутатори Catalyst 6500, маршрутизаторите Cisco 7600, Cisco 7300 и RPM-XF PXF базираните маршрутизатори, както и семейството на Cisco 10000 Edge Service Router (ESR). Тези устройства ще срещнете на границата на мрежите на Интернет доставчиците на услуги, в средните и големи предприятия, както и в центровете с данни, където съществуват множество потоци и има изисквания за високоскоростно комутиране.

Използването на централизирана архитектура има смисъл само като компромис между цената, сложността и производителността. Разбира се много от функциите, описани в предходния раздел, продължават да се изпълняват от един главен процесор. Вграждането на ASIC в архитектурата позволява изпълнението на много сложни операции, като например претърсване на списъците за контрол на достъпа (ACL), QoS, политики за маршрутизация и др., като в същото време се запазва много висока скорост на комутиране. Като типична централизирана ASIC-базирана архитектура на Фиг.13 е показана обобщената схема на граничния маршрутизатор Cisco 10000 ESR. Там операциите по пренасочването на пакетите се извършват в модула Performance Routing Engine (PRE).

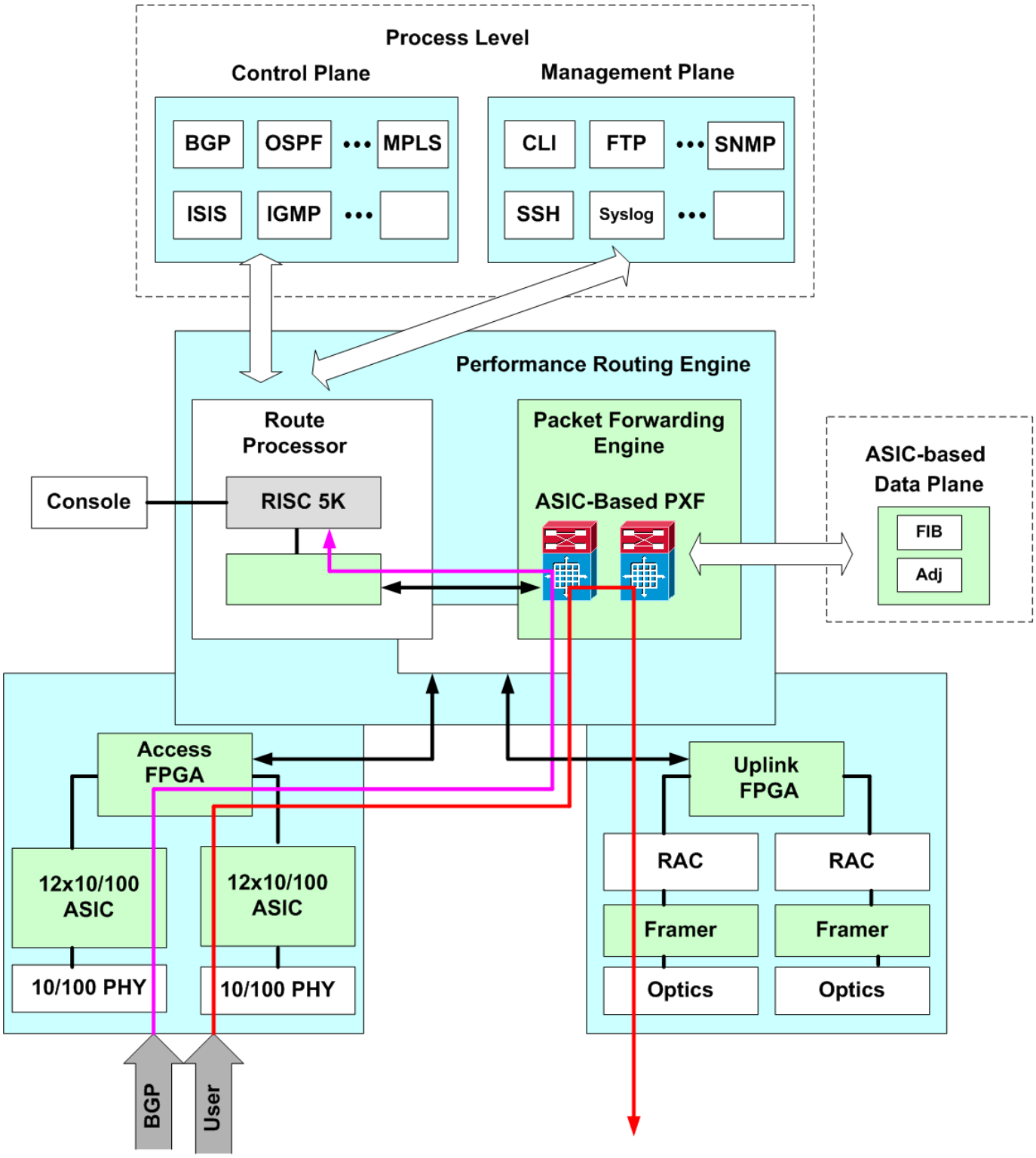
В този модул има CPU, който се грижи за поддръжката на маршрутизатора (CLI, ICMP, управляващи функции и др.), за функционирането на маршрутизиращите протоколи, както и за изчисленията и поддръжката на FIB и таблицата за съседство. Един път изградени, тези две таблици стават достъпни за ASIC структура наречена Parallel Express Forwarding (PXF).

Всички пакети преминаващи транзитно през маршрутизатора (с други думи които влизат и излизат през различните интерфейсни модули), се обработват от PXF. CPU не се занимава с пренасочването на тези пакети. Ако са конфигурирани допълнителни услуги, като ACL, QoS, политики за маршрутизиране и т.н., те също се конфигурират в PXF и се отработват от тази структура. За пълнота ще изясним и двете останали съкращения използвани във Фиг.13. FPGA (Field-Programmable Gate Array) означава цифрова интегрална схема съдържаща програмируема цифрова логика, докато с RAC (Ring Access Controller) е означена интегралната схема грижеща се за достъпа до оптичния кабел.

Някои пакети и функции не могат да се обработват в рамките на ASIC структурата. Тези пакети се прехвърлят за пълна обработка към CPU. Пакетите попадащи в тази група включват входящите пакети за маршрутизатора, което по същество означава всички пакети в плоскостите за контрол и управление, както и всички пакети-изключения.

ASIC са проектирани да изпълняват високоскоростни операции за точно определен набор от пакети. Например буферите, паметта и операциите са проектирани за обработка на IP пакети с 20 байтови заглавни части. Пакетите, които включват IP опции и заглавната им част надхвърля 20 байта, не могат да се обработват в ASIC. Тези пакети се предават за бавна обработка от CPU. Тъй като ASIC пренасочва пакетите без участието на CPU, голяма част от транзитния трафик не влияе на общата производителност на маршрутизатора. Когато обаче броят на пакетите-изключения нарасне, неговата производителност намалява.

Централизираната ASIC-базирана архитектура предлага отличен компромис между производителност, използването на интегрирани услуги и цена. Маршрутизаторите от тази категория са изключително подходящи за местата които бяха споменати. Те не трябва да се използват обаче в случаите, когато изключително високата пропускателна способност е задължителна. Централизираният характер на всяка платформа ограничава скоростта на пренасочване на пакетите до възможностите на един модул за пренасочване. За по-високи скорости трябва да се използват други архитектури и по-специално разпределени архитектури.



Фиг.13 Централизирана ASIC-базирана архитектура на маршрутизатор

6.3 Разпределени CPU-базирани архитектури

Към маршрутизаторите използвани в големите мрежи се предявяват изисквания не само за голяма скорост на комутиране на пакетите, но и за висока плътност на портовете им. Тази висока плътност намалява общите разходи за хардуер, както и оперативните разходи, тъй като значително по-малко устройства трябва да бъдат управлявани.

Увеличението на изискванията води до непрекъснато усъвършенстване на архитектурите, използвани в маршрутизаторите. Два подхода могат да бъдат приложени за увеличение на скоростта на комутиране. Първият, който вече разгледахме, е да се запази централизирания начин на обработка, но да се използват нови, по-производителни процесори и да се добавят хардуерно-базирани (ASIC) схеми за комутиране. Този тип архитектури в определен момент се натъкват на ограничения и по двата параметъра – максималната скорост на комутация и високата плътност на портовете.

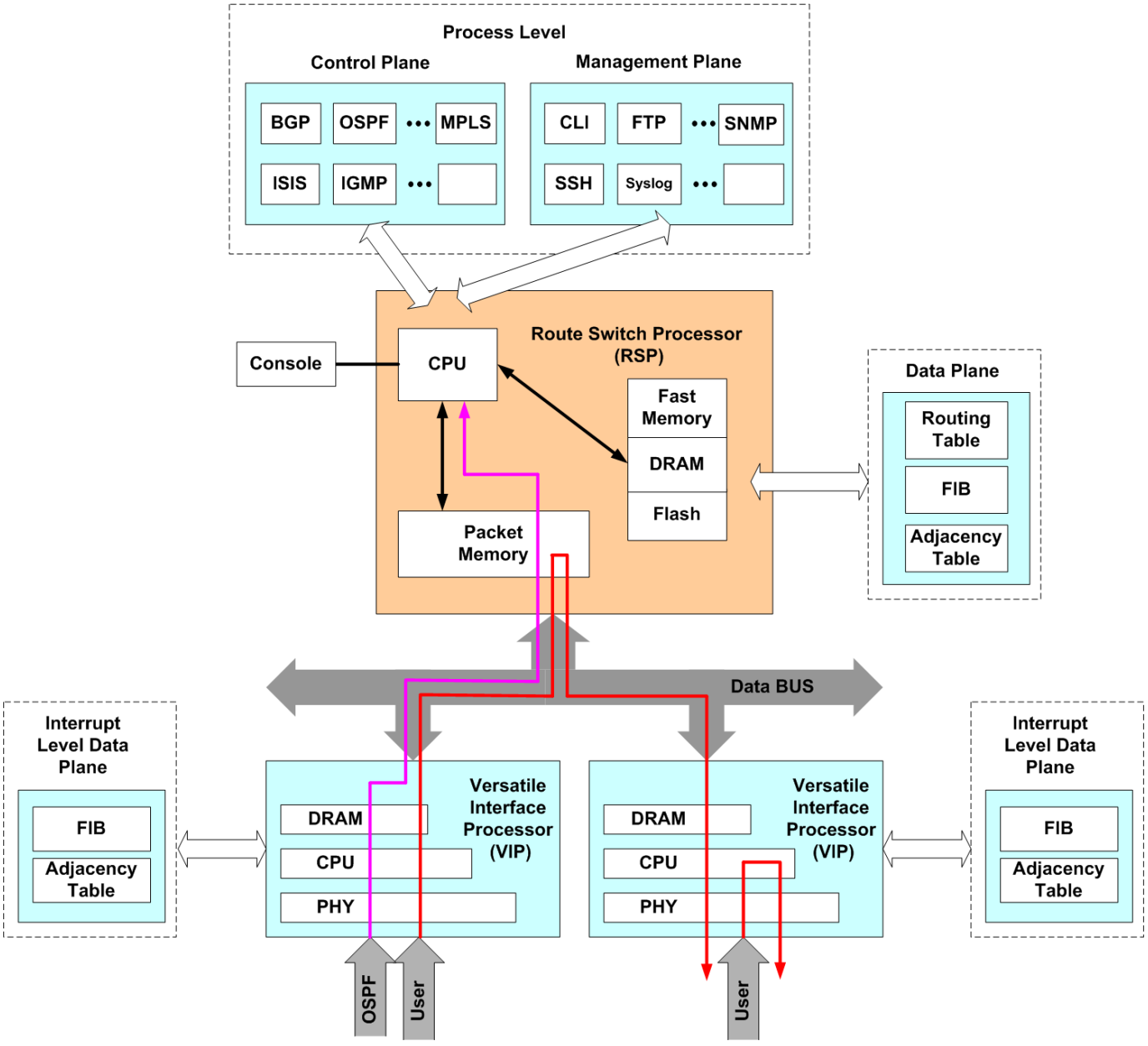
При другия подход маршрутизаторът се разделя на отделни линейни модули (line cards), всеки от които поддържа определен брой мрежови интерфейси. Наричат се линейни, защото комуникационните линии се присъединяват към тях. Обработката и функциите по комутирането се прехвърлят (разпределят) на тези модули. Видяхме вече, че CEF изчислява FIB и таблицата за съседство, след което предава тези таблици на ASIC структурата PXF. Тук се вижда, как CEF е идеално подходящ за разпределена архитектура, където всеки модул има необходимата интелигентност да пренасочва пакетите постъпващи на входните му интерфейси. В този случай се стараем комутирането да става колкото е възможно по-близко до точката, в която пакетът постъпва в маршрутизатора. Другият компонент, който ни трябва, за да имаме завършена разпределена архитектура, е високоскоростна магистрала (bus) или комутираща матрица (switching fabric), която да свърже отделните модули в един цял логически домейн, какъвто е маршрутизаторът. Модулите с функции за препредаване наричаме пренасочващи модули (forwarding engines). При по-ранните разпределени архитектури се използват CPU-базирани пренасочващи модули. Производствената гама на тези ранни CPU-базирани устройства включва маршрутизаторите от серия Cisco 7500 и първите образци от серия Cisco 12000 Gigabit Switch Router (GSR). С цел да се илюстрират основните елементи на една разпределена CPU-базирана архитектура, на Фиг. 14 е показан маршрутизатор от серия Cisco 7500.

Както е показано на Фиг.14, маршрутизаторът Cisco 7500 включва централен процесор, наречен тук Route Switch Processor (RSP), който се грижи за поддръжката на маршрутизатора (CLI, ICMP, управляващи функции и др.), за функционирането на маршрутизиращите протоколи, за обработката на интерфейсните съобщения от типа keepalives и т.н. По този начин всички пакети от плоскостите за контрол и управление се обработват от RSP. Cisco 7500 включва и няколко модула наречени универсални интерфейсни процесори (Versatile Interface Processors – VIP) с порт адаптери (Port Adapters – PA). Използването на PA не само осигурява висока плътност на портовете, но добавя и определена гъвкавост на интерфейсите с тяхната модулност. Разпределеното комутиране се извършва от VIP. Тези модули имат собствени процесори, памети и буфери. Във всеки от тях работи отделен, специализиран образ (image) на IOS. Високоскоростна магистрала се използва за предаване на пакетите между VIP и RSP. Когато PA приеме пакет, той го копира в общата памет на VIP и след това изпраща прекъсване на процесора на VIP. Процесорът на VIP изпълнява CEF претърсване, след което променя заглавната част на пакета. Ако изходният порт се намира във същия модул VIP, пакетът се пренасочва директно. Ако изходният порт е в друг VIP модул, пакетът трябва да се предаде на него. За това действие не е необходимо RSP да обработва пакета, но все пак се губи време, защото RSP се използва като арбитър на магистралата.

VIP модулите поддържат много сложни операции, като списъци за контрол на достъпа ACL, QoS, политики за маршрутизиране, криптиране, компресии, опашки, IP групово

предаване (multicasting), тунелиране, фрагментация и други. Някои от тези операции се поддържат от CEF, други изискват други методи за комутиране.

По принцип RSP не е пряко свързан с изпращането на пакети. Въпреки това има изключения, както и при другите архитектури. Разбира се трафикът в плоскостите за контрол, управление и услуги се препраща към RSP за директна обработка. Други изключения са обработката на пакети със специфични функции, например с IP опции, TTL = 0 и т.н. Твърде много неподходящи пакети изпратени към RSP може за застраши състоянието на цялата платформа.



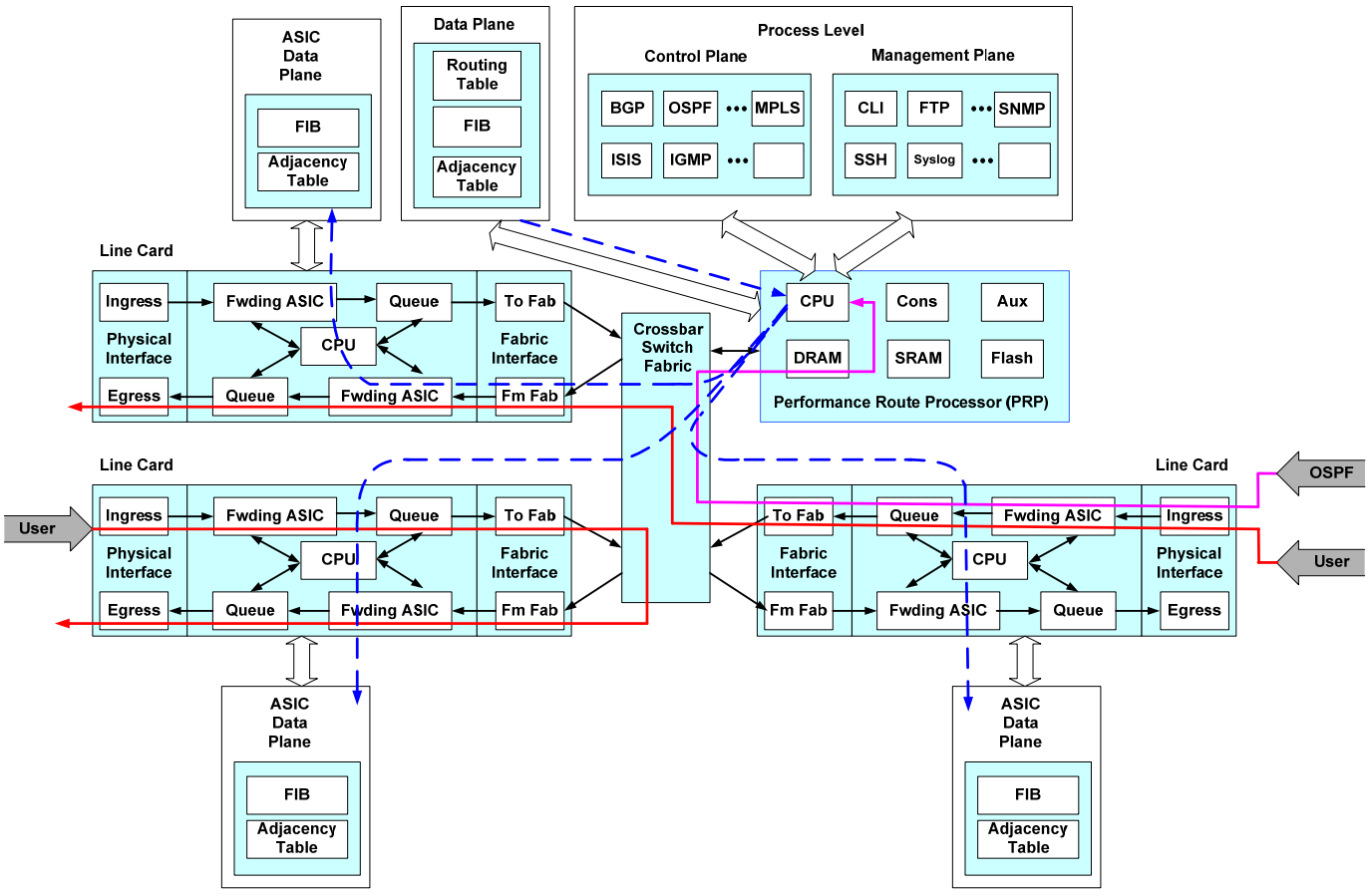
Фиг.14 Разпределена CPU-базирана архитектура на маршрутизатор

Първите маршрутизатори използвани във високоскоростните ядра на мрежите бяха с разпределена CPU-базирана архитектура. Някои от тези маршрутизатори все още се използват и днес. Като логическо продължение на този CPU-базиран дизайн се явяват

устройствата с разпределена ASIC-базирана архитектура, която ще разгледаме в следващия раздел.

6.4 Разпределени ASIC-базирани архитектури

Съвременните маршрутизатори, които са предназначени за работа във високоскоростните мрежи, имат напълно разпределени функции по комутирането. Стремежът е тези функции да се извършват със скорост равна на скоростта на приемане на пакетите в мрежовите интерфейси. Както при централизираните архитектури, вграждането на ASIC предоставя възможност за разтоварване на CPU от функциите по комутирането. В централизираната ASIC-базирана архитектура, ограниченията са наложени от използването на един ASIC модул за препращане. За увеличение на общия капацитет, концепцията за ASIC е разширена за разпределена среда. В разпределените ASIC-базирани архитектури всеки линеен модул (Line Card) има своя ASIC схема за комутиране, която работи независимо от всички останали модули в режим на реално време. Модулът се нарича линеен, защото към него се свързват комуникационните линии. Първите маршрутизатори, които използваха напълно разпределена ASIC-базирана архитектура са от серията Cisco 12000. След това тази архитектура беше приложена и в Cisco 7600. Най-новото допълнение към устройствата на Cisco с напълно разпределена ASIC-базирана архитектура е Carrier Routing System (CRS-1). За да илюстрираме действието на една разпределена ASIC-базирана архитектура, на Фиг.15 е показана опростената схема на маршрутизатор Cisco 12000.



Фиг.15 разпределена ASIC-базирана архитектура на маршрутизатор

В маршрутизаторите Cisco 12000 има един главен маршрутизиращ процесор наречен Performance Route Processor (PRP). Могат да се използват и резервни PRP, но само един е активен и действа като основен. Модулът PRP е от решаващо значение за функционирането на маршрутизатора. Той изпълнява протоколите за маршрутизация, изчислява FIB и таблицата за съседство, извършва промените в CEF таблиците, които се съхраняват локално във всеки модул. Той се грижи и за поддръжката на маршрутизатора, т.е. изпълнява такива функции като системна диагностика, управление на конзолата, наблюдение и диагностика на останалите модули и т.н.

Комутиращата матрица (Crossbar Switch Fabric) на Cisco 12000 осигурява синхронизация и връзка между модулите с гигабитова скорост. През нея е основният път за пакетите между линейните модули, както и между тях и PRP. Използването на модули ни гарантира високата плътност на интерфейсите на маршрутизатора.

Комутиращите функции са поверени на линейните модули. За целите на пренасочването те използват заредени в тях създадени то PRP копия на FIB и таблицата за съседство. Всеки линеен модул извършва независимо претърсване на локалната FIB за да открие адреса на получателя за всеки един получен пакет. Тук се определя изходящия линеен модул, на който пакета трябва да бъде предаден. След това пакетът се изпраща на този модул през комутиращата матрица. Линейните модули имат три отделни секции:

- Секция за физически интерфейс (Physical Layer Interface Module -PLIM): Тази секция терминира физическите връзки. Тя осигурява ATM, Packet-over-SONET (POS), Fast Ethernet, и Gigabit Ethernet интерфейси.

- Секция за комутиране в слой 3 (Layer 3 Switching Engine): В тази секция се намира комутиращия хардуер. Там се извършват претърсванията на таблиците, презаписването на заглавните части, буферирането, контролиране на претоварването и други поддържащи функции.

- Секция за интерфейс към комутиращата матрица (Fabric Interface): В тази секция пакетите са подготвят за транспортиране през комутиращата матрица към изходящия линеен модул. Тук се обработват заявките на комутиращата матрица, опашките към и от нея, размножаването на пакетите при групово предаване и се извършват много други функции.

Линейните модули се класифицират съгласно типа на вградената в тях секция за комутиране (engine type). Първите линейни модули, известни като Engine 0 и Engine 1 са CPU-базирани. В следващото поколение, Engine 2, са включени някои от по-старите ASIC схеми за да се разтовари процесора им от функциите по комутиране. В по-новите високоскоростни версии Engine 4 и Engine 4+ имаме пълна ASIC подкрепа. Съвременните линейни модули са от фамилиите Engine 3 и Engine 5. Тези модули използват последното поколение специално проектирани ASIC, в които са включени високоскоростни памети, известни като Ternary Content Addressable Memory (TCAM), които позволяват всички функции като ACL, QoS, политики за маршрутизация и други, да бъдат извършвани едновременно с високоскоростното комутиране на пакета. Тези ASIC са програмируеми. На Фиг.15 са показани линейни модули от типа Engine 3.

При версиите GSR (Gigabit Switch Router) линейните модули са отговорни за вземането на всички решения по комутирането на пакетите. Понеже FIB е предварително определена и

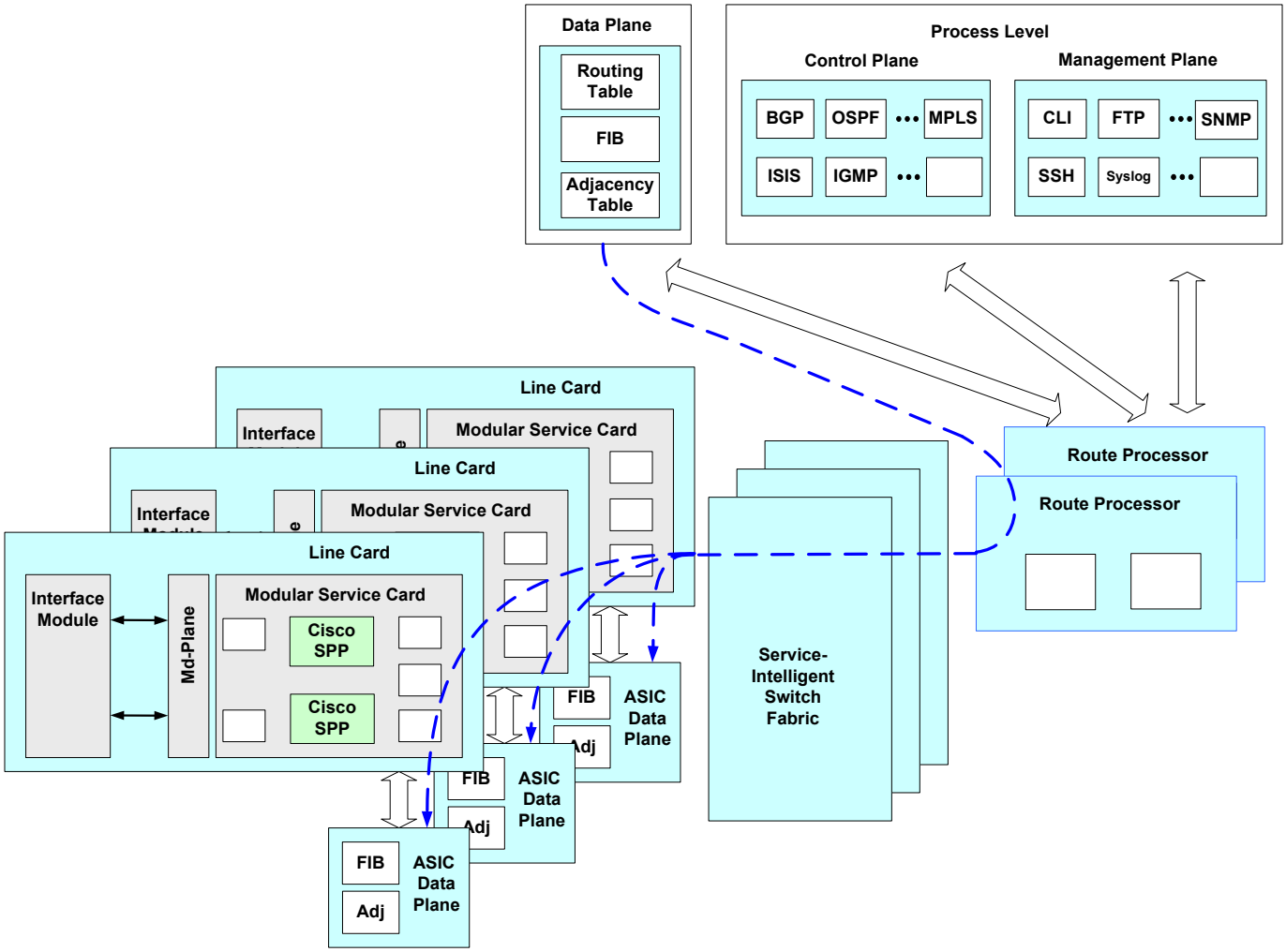
заредена, всеки един линеен модул има пълната информация необходима за пренасочването на пакета. Ако адреса на получателя не се намира във FIB, то пакетът просто се отстранява. Разпределеният CEF (dCEF) е единственият метод за комутиране, който тук е на разположение. Процесорното и бързото комутиране не са налични като резервни за неизвестни дестинации (няма такива). Има разбира се входящи пакети за маршрутизатора и пакети-изключения, но те се изпращат на PRP за обработка. Това са главно пакети от контролната и управляващата плоскост. Другите пакети-изключения, такива за които TTL изтича, ICMP заявки, IP опции и т.н., се обработват по различен начин. Някои от тези пакети е възможно да бъдат обработени от CPU на линейния модул. Технически, макар че засега ASIC не поддържат това, те могат да бъдат обработвани напълно локално. Например съобщенията за ICMP недостижимост се изпращат директно от линейния модул. Други пакети-изключения се обработват само от PRP. Когато броят на пакетите, които се предават за обработка или към CPU на линейния модул или към PRP, нарасне прекалено, платформата изпитва затруднения.

Прегледът на архитектурите няма да бъде пълен, ако не разгледаме архитектурата на маршрутизатор CRS-1. При тази архитектура виждаме както еволюционни, така и революционни промени в технологията. Четири ключови елемента определят тези архитектурни достижения: 40-Gbps линейни модули, усъвършенствани маршрутизиращи процесори (Route Processors), интелигентни комутиращи матрици (Service-Intelligent Switch Fabrics) и Cisco IOS XR операционна система. Някои от тези елементи са показани на Фиг.16 и описани по-долу.

Първият ключов елемент, показан на Фиг.16 е дизайна на новите 40-Gbps линейни модули. Всеки линеен модул е разделен от свързваща схема наречена Mid-plane на две части: Интерфейсен модул (Interface Module – IM) и платка за модулни услуги (Modular Services Card - MSC). Интерфейсният модул осигурява физическата връзка към мрежата, включително всички функции от Layer 1 и Layer 2 (POS и Gigabit Ethernet). Функциите от Layer 3 се извършват в MSC. Това е високопроизводителен комутиращ модул, снабден с две ASIC схеми, наречени силиконови пакетни процесори (Silicon Packet Processors – SPP). Едната от тези 40-Gbps ASIC схеми обработва входящите пакети, а другата – изходящите. В документацията на Cisco и при някои команди на маршрутизатора можете да срещнете тези схеми и под наименованието Packet Switching Engine (PSE). Всеки линеен модул в CRS-1 поддържа отделен екземпляр на FIB и таблицата за съседство, като с това се постига максимална мащабируемост и производителност.

Вторият ключов елемент е използването на маршрутизиращи процесори (Route Processors – RP). За разлика от предишните маршрутизатори, където само един такъв процесор може да бъде активен в даден момент (дори когато имаме няколко вградени като резервни), маршрутизаторът CRS-1 може да използва няколко активни RP, които да изпълняват функциите по обработката на пакетите в плоскостта за контрол, пакетите за управление и другите поддържащи функции. Едновременната работа на много RP осигурява възможност за разделяне на услугите, сегментиране на плоскостта за контрол и реализация на опростени пътища.

Третият ключов елемент е използването на интелигентни комутиращи матрици, които осигуряват комуникацията между отделните линейни модули. Накратко, комутиращата матрица е проектирана с отделни приоритетни опашки за пакетите в плоскостта за контрол и за пакетите за единично (unicast) и групово (multicast) предаване.



Фиг.16 Архитектура на маршрутизатор CRS-1

Четвъртият ключов елемент е използването на нова Cisco IOS XR операционна система. Традиционната IOS, използвана от Cisco, е модулна, многозадачна операционна система, в която процесите се изпълняват в обща, споделена памет, и чиито възможности и функции се дефинират в момента на нейното създаване. Тази операционна система лежи в основата на всички маршрутизатори на Cisco през последните 20 години. Тя се оказа устойчива на огромните подобрения направени през годините както в хардуера, така и в софтуерните технологии. При IOS се използва архитектура на едностепенно комутиране, където решенията по пренасочването се вземат във входящите интерфейси и линейните модули.

Новата IOS XR операционна система използва защита на паметта на отделните процеси. Изградена е от сменяеми в реално време модули в ядрото. Проектирана е да използва предимствата на многопроцесорната архитектура, каквато имаме в маршрутизатора CRS-1. Позволява максимално използване на системните ресурси и тяхното управление, като в същото време има превъзходна производителност за пакетите от плоскостта за контрол. Процесите съответстващи на протоколите за маршрутизация и сигнализация могат да се изпълняват в един RP или да бъдат разпределени между много модули RP. В допълнение, IOS XR предлага двустепенна архитектура на комутиране, в която решенията се взимат както във входящите, така и в изходящите линейни модули. Тя

осигурява огромна производителност и предимството на добра мащабируемост. При нея във FIB на входящия линеен модул има само връзка между Интернет адреса на получателя и съответния изходящ линеен модул. Физическият адрес на изходящия интерфейс не е необходим в този момент. Той се определя от изходящия линеен модул.

Да отбележим, че маршрутизаторът Cisco 12000 GRS също може да използва IOS XR операционната система при инсталирани подходящи маршрутни процесори и линейни модули.

Наборът от CLI команди за двете операционни системи (IOS и IOS XR) е различен. Наборът от функции, които са на разположение в IOS XR, е значително по-голям и в него са включени много механизми за сигурност. Поради тази причина директното конвертиране и сравняването на конфигурациите на устройства използващи различни Cisco операционни системи е почти невъзможно.

7. Литература

[1] Стоилов Емил, Технология за многопротоколно етикетно комутиране (MPLS), Technical Report, Научен електронен архив на НБУ, 2012, http://eprints.nbu.bg/1254/

[2] Стоилов Емил, Управление на мрежовата сигурност. Системи за откриване на нарушители, Technical Report, Научен електронен архив на НБУ, 2011, http://eprints.nbu.bg/677/

[3] Bollapragada, V., C. Murphy, and R. White, Inside Cisco IOS Software Architecture. Cisco Press, 2000. ISBN: 1-57870-181-3.

[4] Cisco 12000 Series Internet Router Architecture: Packet Switching, Cisco Tech Note. (Doc. ID: 47320.), http://www.cisco.com/en/US/partner/products/hw/routers/ps167/ products_tech_note09186a0080 note09186a00801e1dc1.shtml

[5] Parallel Express Forwarding on the Cisco 10000 Series, Cisco white paper. http://www.cisco.com/en/US/partner/products/hw/routers/ps133/ products_white_paper09186a008008902a.shtml.

[6] Switching Path Section in “Performance Tuning Basics.” Cisco Tech Note. (Doc. ID: 12809.) http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/ products_tech_note09186a00800a7306.shtml.

[7] http://www.cisco.com/en/US/docs/ios/ipswitch/command/reference/isw_s1.html#wp1115453

[8] Cisco Catalyst 6500 Supervisor Engine 32 Architecture, Cisco white paper. http://www.cisco.com/en/US/products/hw/switches/ps708/ products_white_paper0900aecd803e508c.shtml.