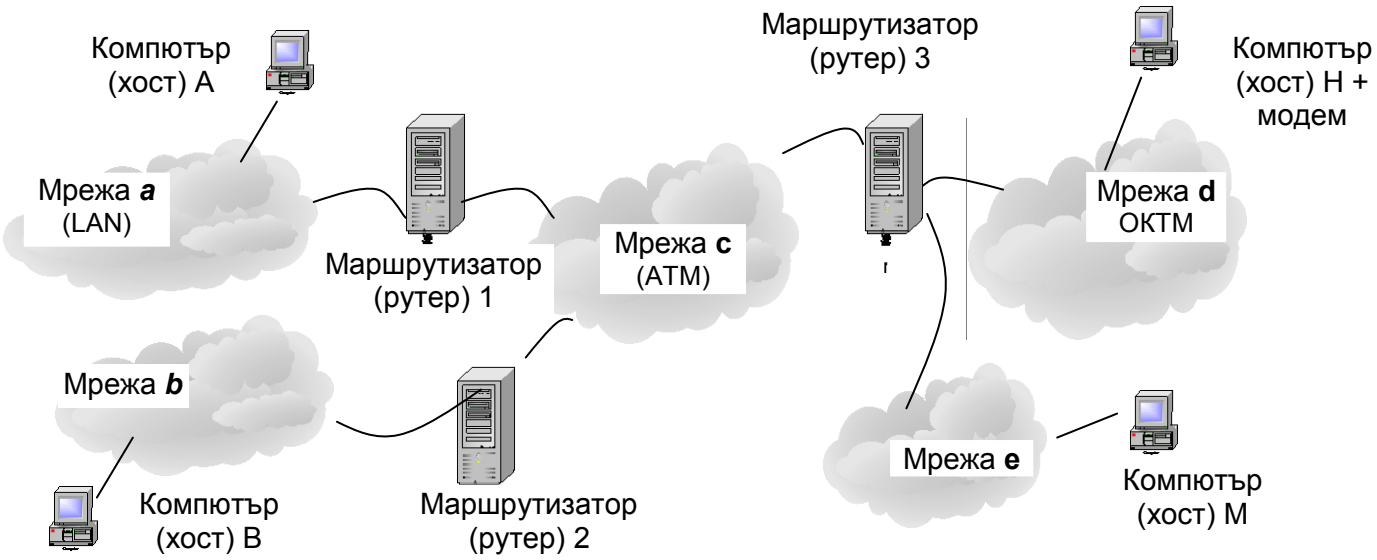
Тема 9. Интернет. Принципи на изграждане и функциониране. TCP/IP слоест модел. Сравнение с OSI модела за компютърни мрежи. Адресация в Интернет. Основни Интернет протоколи.

ИНТЕРНЕТ – принципи на изграждане и функциониране

Интернет е глобална компютърна мрежа. В нея са свързани много различни (локални LAN, WAN, ATM и др.) мрежи и компютри, които са равноправни от гледна точка на обмена на информация. Всяка мрежа, която е включена към Интернет, работи с набор от протоколи за комуникация, известни като Интернет протоколи. Никой няма монопол върху достъпа до мрежата, тя има отворена стандартна архитектура и продуктите, които я реализират, са широко разпространени и достъпни.



Крайните устройства са **клиенти и сървъри**, съответно изискващи и осигуряващи набор от услуги. **Клиентите** са компютри, наричани още хостове или абонати, чрез които потребителите комуникират с други крайни възли, а **сървърите** са централизирани доставчици на услуги, които предлагат услугите за клиентите, като например web- и mail-сървъри.

Междинните устройства (възли) са процесори, които предават трафика между отделните мрежови компоненти. Те се наричат рутери, комутатори и шлюзове. Връзката между два рутера се нарича **хоп**. Всеки хост има уникален идентификатор, наречен **IP (Internet Protocol) адрес** и може да извършва обмен с всеки друг хост.

Тази "хаотична" структура на Интернет предлага в повечето случаи за всеки обмен между два хоста да има повече от един път. При отказ или претоварване на междинен възел, обменът се насочва през другите възли, т.е. мрежата се адаптира. Набор от **Интернет протоколи** позволява на всяка двойка възли да обменят данни, като трябва само да знаят IP адреса или името на домейна на отсрещния възел.

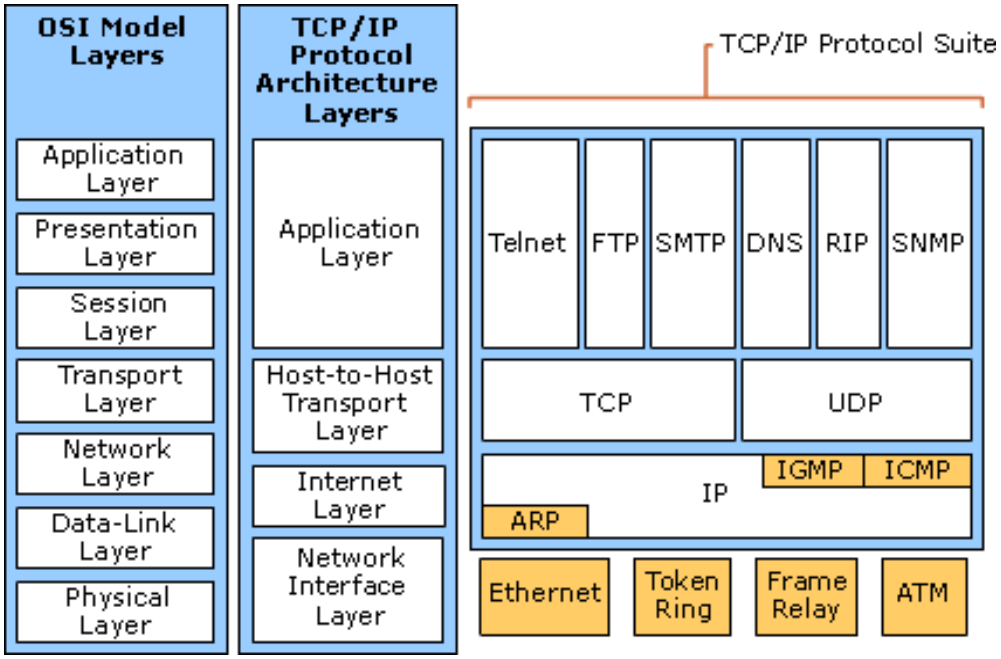
Достъп до Интернет мрежата

За достъп до Интернет се използват наличните ресурси на традиционнните мрежи. Достъпът може да бъде: некомутируем - чрез наети канали и високоскоростни модеми и комутируем - ADSL или HDSL абонатни линии, през местните (квартални) LAN, през мобилната мрежа със сравнително ниски, но постоянно нарастващи скорости и през кабелната телевизионна мрежа чрез висоокоскоростни модеми.

Интернет протоколи

Основните протоколи в Интернет са изградени и се контролират на йерархичен принцип. Тази фамилия протоколи се наричан **Internet Protocol Suite (IPS)** или по-популярна като **TCP/IP протоколен стек**.

Стандартната протоколна архитектура за обмен и пренос на данни TCP/IP (Transmission Control Protocol/Internet Protocol) представлява Интернет език за общуване. **IP е протокол с комутация на пакети**, **осигуряващ предаване на дейтаграми между възлите и маршрутизацията между мрежите**. IP е протокол за комуникации между мрежи и може да работи над множество протоколи от по-ниско ниво, включително Ethernet, ATM и протоколи за оптични мрежи (FDDI и др.).



TCP/IP моделът има само четири слоя: **слой за връзка**, **интернет слой**, **транспортен слой** и **слой за приложения**

Най-ниският слой е **слоя за връзка** и той е отговорен за мрежовия достъп. Той свързва възела и канала и определя правилата за това свързване. В резултат на това, по канала се изпраща сигнал. Този сигнал се образува от пакети, изградени от серии от битове, които съдържат информацията. Сигналът се предава през физически порт на канал, който може да е оптичен или меден кабел. Типичен представител на слоя за връзка е Ethernet протокола. Софтуерът за слоя за връзка е известен като драйвер за устройство и обикновено е вграден в мрежовата карта.

Интернет слоят се намира над слоя за връзка. Той е отговорен за адресирането на данни и за прехвърлянето на информацията. Протоколите определят начина на предаване на пакетите в мрежата, по какъв начин информацията се маршрутизира от начален към краен възел. Информацията се представя в сегменти и пакети. Един пакет се състои от набор от битове и байтове. Основният протокол от мрежовия слой се нарича Интернет протокол (**Internet Protocol**- IP). Друг протокол, използван на това ниво е отговорен за предаването на едно съобщение до множество получатели, като се намалява необходимата честотна лента за изпращане на информацията. Този протокол се използва за аудио и видео предавания в Интернет и се нарича **Intemet Group Management Protocol** (**IGMP**).

IP протоколът дефинира базова единица за пренасяне на данни (**IP дейтаграма**) с определен формат. Програмното осигуряване на IP слоя изпълнява функцията маршрутизиране чрез поддържане на специални таблици на базата на дефинирани адреси. Чрез протокола за разрешаване на адреса (**Address Resolution Protocol - ARP**) се преобразува адреса на мрежовия слой в адрес на физическия и обратно.

Следващото ниво е **транспортния слой**, който е отговорен за доставката на данните до определен възел. Той показва как и дали може да се гарантира пълното и точно получаване на информацията, представена във формата на съобщения и сегменти. Съобщенията се състоят от група пакети. Транспортният слой разделя по-големите съобщения на сегменти, които се предават. При този слой имат значение два протокола - **Transmission Control Protocol** (**TCP**) и **User Datagram Protocol** (**UDP**). TCP протоколът е основен и осигурява надеждно предаване. UDP е по-несигурен и не предлага гарантирана услуга, а работи по принципа на най-доброто усилие (**the best effort**).

TCP обезпечава гарантирана доставка на голямо количество информация чрез изграждане на логическа връзка и поддържа различни приложения като: прехвърляне на файлове FTP; отдалечен достъп - TELNET и др. В приемната страна идентифицира пакетите от едно съобщение, подрежда ги в правилна последователност и разрешава повторно изпращане на загубените пакети. TCP намалява скоростта на пренасяне, когато мрежата е претоварена.

UDP се използва при пренасяне на малко количество информация през големи интервали от време. При него качеството на обслужване се осигурява от приложния слой. UDP поддържа следните приложения: конфигуриране, управление на алармите и извличане на данни чрез **прост протокол за управление на мрежата - SNMP**; използва се от услуги, работещи в реално време (аудио и видео).

Слоят за приложенията гарантира доставката на данни от едно приложение до друго, като приложението, от което се предават данните е

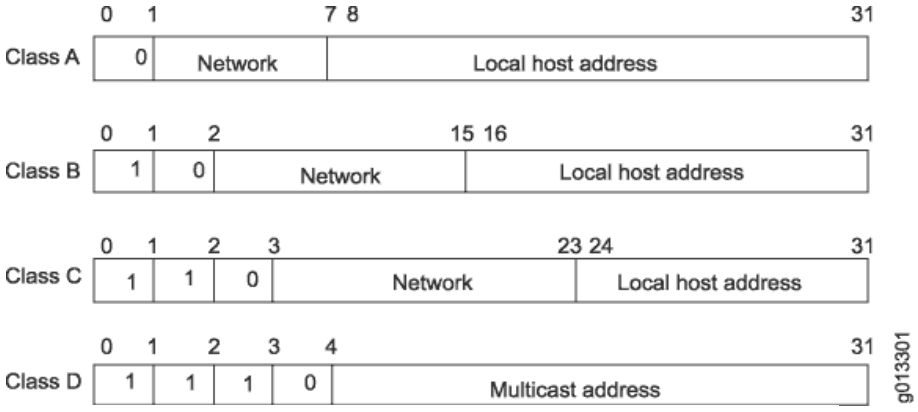
разположено на същия или друг възел в мрежата. При предаването на информация този слой използва съобщения. Протоколите на това ниво са: **Hypertext Transfer Protocol** (**HTTP**), който гарантира предаването на HTML документ, **SimpleMail Transfer Protocol** (**SMTP**), който предава пощи от един възел към друг и **File Transfer Protocol** (**FTP**), който предава файлове между възлите. И трите протокола (SMTP, FTP и HTTP) работят върху TCP.

Въпреки че тази структура може да изглежда сложна, тя действително опростява изпълнението на набора от протоколи. Чрез сегментиране на информацията в съобщения, пакети, байтове, битове и сигнали, в зависимост от слоя, е по-лесно да се разработи софтуер, който да включва необходимите протоколи. Всеки слой може да се разработи отделно, без познания за останалите слоеве, при което софтуерът се опростява и е по-устойчив. Освен това така е по-лесно да се интегрира софтуер от различни разпространители в едно решение, дори и ако различните продукти работят на различни нива.

Адресация в Интернет

Адресите в Интернет протокола версия 4 (**IPv4**) представляват 32-битови двоични числа, които е прието да се записват като четири десетични числа, разделени от точки. Всяка от тези четири части на адреса се нарича байт или **октет**, защото представлява осем битово двоично число.

IP адресите са разделени логически на две части, въпреки че са записани като четири байта. Първата част се нарича мрежов идентификатор (адрес на мрежата), а втората - идентификатор на крайния възел. Адресите в Интернет са разделени на пет класа, означени с латинските букви от A до E. Всеки клас определя различна дължина на полетата на адреса на мрежата и съответно и различна дължина на адреса на крайния възел.



Клас	Десетична стойност на първия байт
клас A	от 1 до 126 включително
клас B	от 128 до 191 включително
клас C	от 192 до 223 включително
клас D	от 224 до 239 включително
клас E	от 240 до 254 включително

Стандартните мрежови маски за петте класа са дадени в таблицата:

Клас	Мрежова маска
клас A	255.0.0.0
клас B	255.255.0.0
клас C	255.255.255.0
клас D	липсва
клас E	липсва

Подмрежи: Разделянето на адресното пространство на подмрежи дава възможност за по-ефективното му използване, улеснява управлението и контрола на мрежовия трафик. За реализация на подмрежите маршрутизаторите се нуждаят от подмрежова маска (Subnet Mask – SM). Тя представлява 32 битово двойно число, което се състои от последователност от единици следвана от последователност от нули, като най-често се записва еквивалента в десетичен вид.

Пример: IP адрес 192.168.1.0 с мрежова маска 255.255.255.0 може да се запише така 192.168.1.0/24.

Много често се налага използване на маски с променлива дължина VLSM (Variable Length Subnet Mask), които са различни от стандартните с цел по-гъвкаво управление на адресното пространство и администриране на хостовете в подмрежа

Изчисляване на брой мрежи, префикси и маски:

Общо адреси	брой битове	префикс	мрежова маска
Y= 2^x	**x**	**/ 32-x**	**256 - Y**
8= 2^3	3	32 -3=29 /29	256 – 2^3 =248 255.255.255.248
64= 2^6	6	32 -6=26 /26	256 – 2^6 =192 255.255.255.192

Пример: Изчислете мрежовата маска, ако броят на хостовете в една мрежа са 50 и се използва клас C мрежа (192.168.1):

Решение: За 50 хоста (адреси) са ни необходими 2^x-2>=50 на брой битове, за да могат да се назначат уникални адреси, т.е. **x=6 (host bits), за мрежовата маска остават 32-6 = 26 bits (8+8+8+(8-6)=26)**
Получената мрежова маска е 11111111.11111111.11111111.11000000 или в десетичен формат **255.255.255.192**, 2^6=64.
Вариантите за подмрежи са четири: 00, 01, 10 и 11, като във всяка от тях може да има по 64 адреса (за мрежа, хостове и броудкаст).

Съществува калкулатор за изчисляване на подмрежата маска:

Всеки възел в Интернет има уникален IP адрес. Поради факта, че IP адресите се запомнят трудно, вместо тях се използват **имена на домейни**. За

повечето хора е по-лесно да се запомни името на домейна **www.tu-sofia.bg**. вместо отговарящия на него IP адрес - **81.161.240.14**.

Всяко име на домейн отговаря на един или повече IP адреса и всеки IP адрес отговаря на едно или повече имена на домейн. В случай, че има повече от един IP адрес за едно име на домейн, това означава, че на едно и също място има няколко сървъра, които споделят входящите заявки и ако няколко имена на домейни отговарят на един IP адрес, тогава няколко клиента споделят един голям web сървър при доставчика на Интернет услуги.

Отдавна са известни много недостатъци на IPv4, между които:

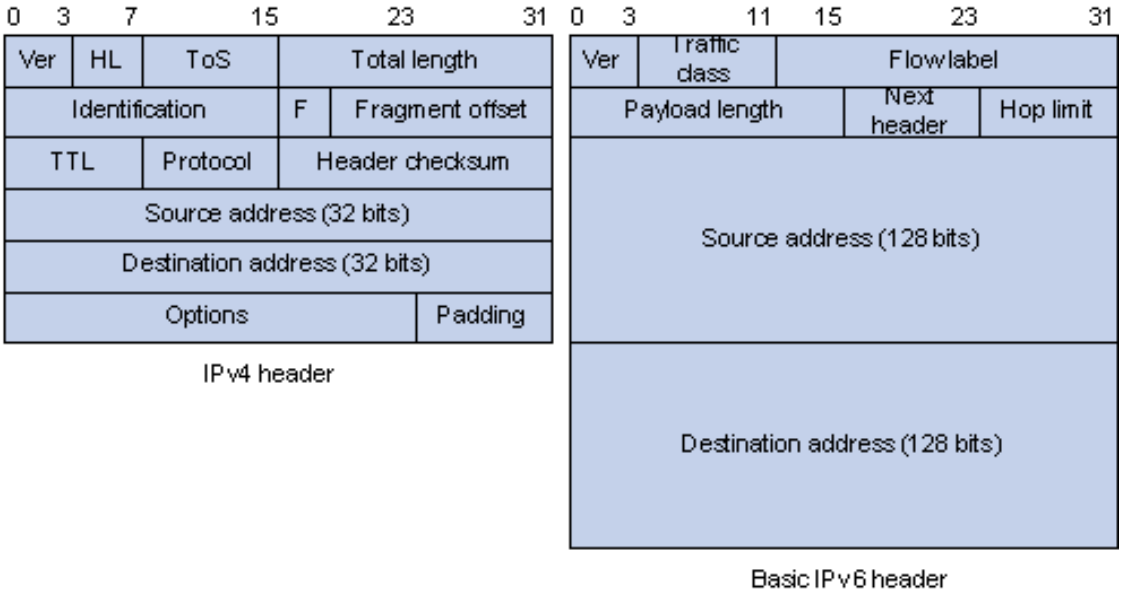
- малко адресно пространство,
- слаба защита срещу посегателство
- тромаво третиране на изохронния трафик (реч).

Новата версия на Интернет протокола IPv6 е специфицирана от IETF още преди повече от 10 години. Сега тя тепърва навлиза в практиката. Въвеждането на IPv6 се сблъсква с две различни групи проблеми. Първата е свързана с IPv6 комуникацията между два и повече IPv6 острова, изолирани в IPv4 морето. Втората е свързана с комуникацията между света на IPv4 и новия свят на IPv6.

Адресите в IPv6 са 128 битови, като те се разделят на 16 битови полета и всяко 16 битово поле се преобразува в 4 цифрено шестнадесетично число и се разделят с двуеточие.

пример: 21DA:00D3:0000:2F3B:02AA:00FF:FE28:9C5A

Структура на IPv4 и IPv6 дейтаграма в Интернет



IPv4 структура:

Ver (version) указва версията на протокола, към който принадлежи пакета. **HL (Internet header length)** указва дължината на заглавната част в 32-

битови думи. **ToS (Type of service)** показва какво обслужване очаква пакета. **Total length** показва общата дължина на дейтаграмата (заглавна част + данни). Максималната дължина е 65535 байта. **Identification** съдържа номер на пакета. Всички фрагменти на един и същ пакет имат еднакъв номер и по този начин получателя разбира кой фрагмент към коя дейтаграма принадлежи. **F** е група от флагове, които управляват фрагментирането на дейтаграмата. **Fragment offset** указва къде се намира фрагмента в оригиналната дейтаграма. **TTL** (Time to live) е брояч, който отброява времето на живот на пакета в секунди (хопове). Максималната му стойност е 255. Това поле се намалява с единица на всеки hop. При нулиране пакета се премахва и в обратна посока се изпраща предупредителен пакет. **Protocol** указва протокола на транспортно ниво: TCP или UDP. **Header checksum** е контролна сума само на заглавната част. Тя трябва да се преизчислява на всеки hop, тъй като поне едно поле се променя - TTL. Полетата **Source Address** и **Destination Address** съдържат съответно адрес на източника и адрес на получателя.

IPv6 структура:

Ver– идентификатор за версията на протокола. **Traffic Class** се използва за определяне на QoS (Quality of Service). Чрез това поле се задава различен клас или приоритет на трафика (в комбинация с други полета, като поле за адрес на източника/приемника). **Flow Label** определя потока, което е група от свързани пакети. **Payload Length** – в това поле се задава дължината на пакета, включително и онази част, която е след заглавната част (extension header). Стойността на полето се дава в байтове, така че максималната дължина на пакета е 64 KB. **Next Header** показва на кой протокол е следващата заглавна част. Чрез това поле се определя вида на следващата информация – дали ще е extension header или протокол от горно ниво (TCP, UDP и т.н.). **Hop Limit** – ограничение за времето на живот на пакета. **Source Address** – IP ареса на източника на пакета. **Destination Address** – IP адреса на получателя

Една от услугуте, които са доста актуални в последните години е изграждането на **виртуални частни мрежи (Virtual Private Network).** VPN е услуга, която предлага сигурност, надеждна връзка през споделената обществена мрежова инфраструктура (Интернет). VPN поддържа същата сигурност и управленска политика, както при една частна мрежа. Те предлагат един от най-евтините методи за изграждане на point-to-point връзка между отдалечени потребители и мрежата на дадено предприятие. Видове VPN:

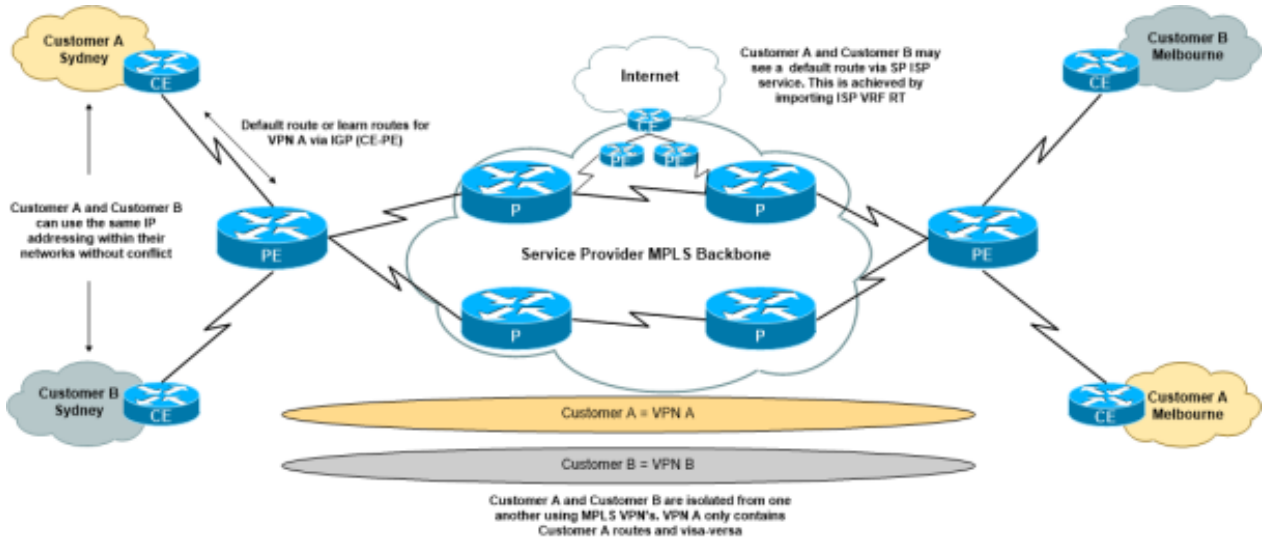
• **access VPN** - предлага отдалечен достъп на мобилен служител и малък офис/домашен офис до отделите на Intranet или Extranet през споделена

инфраструктура. Тази тип може да използва аналогови, dialup, ISDN, DSL и мобилни IP технологии за сигурен достъп от мобилните служители.

•**Intranet VPN** - свързва регионални или отдалечени офиси до отделите на вътрешната мрежа през споделената инфраструктура, използвайки предвидена за това връзка. Intranet VPN се различават от Extranet VPN по това, че те дават достъп само на служителите на предприятието.

•**Extranet VPN** - свързва бизнес партньори с отделите на мрежата през споделената инфраструктура, ползвайки предвидена за това връзка. За разлика от Intranet VPN, Extranet VPN разрешава достъп на потребители, намиращи се извън предприятието.

Layer 3 MPLS VPN



Layer 2 MPLS VPN