Междумрежови комуникации.Протоколи IP,ICMP,ARP.Междумрежовия протокол IP е неотделима част от фамилията TCP/IP.Макар че,в името му има думата Интернет,той се използва не само в тази мрежа.Истина е че всички машини в Интернет работят с IP или съвместими протоколи,но той може да се използва и в отделни мрежи нямащи нищо общо с Интернет.IP е много добро средство за комуникация между машини в произволна мрежа.Той обаче има и конкуренти в лицето на протокола IPX на мрежовата операционна система Novell NetWare,която се използва в неголеми локални мрежи.Главната задача на IP се заключава в това да обезпечи предаването на деитаграмите от компютър до компютър,а така също и разделянето им на фрагменти.Той дава формално описание на структурата на деитаграмите и реда за формиране на заглавната им част със служебна информация.IP отговаря за маршрутизацията на деитаграмите,т.е.определя пътя им като при възникване на неизправности в мрежата ги пренасочва.Важно е да се има в предвид,че IP не гарантира сигурно получаване.Това значи че деитаграма може да се забави,да не пристигне до получателя или да се повреди при разделянето и събирането на фрагментите.IP не управлява потока от данни и не осъществява контрол на трансфера - тази задача се решава на други нива.Контрол се осъществява само на заглавната част а не на целия пакет от данни.Маршрута по които се предават данните може да не е оптимален.Оптимизацията се осъществява локално тоест между съседни възли но няма никаква гаранция за оптимизация на маршрута като цяло.Част от протокола IP определя как да се обработват деитаграмите при достигането им до шлюзовете.В нея е зададен реда и условията за подаване на съобщение за грешка и реда за възстановяване след сбой.Максималния размер на IP пакета е 65 535 байта,което значително превъзхожда възможностите на повечето мрежи следователно се налага фрагментация.В IP тя се реализира автоматически в съответствие с определен набор от правила.Заглавната част на IP пакета съдържа информация в която е указан реда за събиране на съобщенията от машината получател.Когато деитаграма с първия фрагмент от голямо съобщение пристигне в компютъра за който е адресирана,в него се задейства програма на ниво междумрежови връзки наречена таймер на сбора.Ако в указаното време съобщението не бъде прието изцяло,всички постъпили деитаграми се унищожават Поради това разбиването на фрагменти намалява вероятността за получаване на цялото съобщение и повечето програми се опитват да изпращат съобщението като едно цяло ако това е възможно.Връзката по протокола IP се поддържа без предварителна заявка от подателя към получателя и за него е безразличен пътя по който ще мине информацията и даже началната и крайната точка от маршрута.IP работи с 32 разрядни адреси,като в новата версия 6 или т.нар.IPng е предвидена възможност за по-голяма разрядност на адреса.Протоколът,IP предава данните във вид на IP-дептаграми (пакети).Всяка IP-дейтаграма се състои от заглавна част и поле .Размерът на IP-дейтаграмата е променлив,като максималният й размер е ограничен на 64 KB.Нормалният размер на заглавната част (header) на IP-дейтаграмата е 20 байта Допълнително могат да бъдат включени полетата и Полето се използва обикновено при настройка на мрежата.То се състои от няколко подполета (до 8 типа).В тях може да се указва точният маршрут на преминаване на дейтаграмата,да се регистрират преминалите маршрутизатори,да се съдържат данни на системата за

безопасност,времеви отметки и т.н.Полето се използва за изравняване на размера на заглавната част до цяло число 32-битови думи.Тъй като маршрутът на IP-дейтаграмите може да преминава през различни подмрежи,една от функциите на протокола IP е фрагментирането на деитаграмите на по-малки пакети (фрагменти) със създаване на съответните служебни полетал.В IPv6 се използват следните типов е адреси: индивидуален адрес тип,,unicast2) групов адрес тип „cluster" 3) групов адрес тип „multicast На всеки Internet - доставчик се назначава уникален идентификатор,с който се маркират всички поддържани от него мрежи.След това доставчикът сам назначава уникални идентификатори на своите абонати,а абонатът сам дава идентификатори на своите подмрежи и техните хостове. 2.Протокол ICMP.Протоколът ICMP е предназначен за предаване на различни управляващи съобщения или съобщения за грешки.Маршрутизацията на съобщения от подателя към получателя е свързана с много проблеми.Може да изтече времето на живот на деитаграма,могат да се повредят части от фрагментите,шлюза може да насочи деитаграма не там където трябва и т.н.т.Необходимо е не само да се обработят грешките при предаването,но и да се съобщи за тях на подателя.Последната задача се поема от ICMP (- междумрежов протокол за управление на съобщения).Протокола ICMP е система от правила за уведомяване при грешки.Той е неразривно свързан с протокола IP и е задължително да бъде включен във всяка негова реализация.ICMP предлага логически строен формат на съобщения и сигнали за грешки,пригодени за различни версии на IP и различни операционни системи.ICMP е добре да се възприема като средство за междумрежово взаимодействие за подаване на съобщения от дадено ниво към същото ниво на друга машина.Или казано по-кратко ICMP е система за свръзка за IP.ICMP дейтаграма е с IP заглавие и се обработва в мрежата така както и IP деитаграм,а в машината получател се интерпретира на ниво междумрежово взаимодействие(IP).Съгласно ICMP съобщението за грешка се предава почти винаги на машината подател.Това се обяснява с факта,че заглавието съдържа само IP адресите на подателя и получателя а последния не знае как да поправи грешката.При получаване на съобщение подателя определя типа на грешката и избира ред за повторно предаване на дейтаграма.Реда за пакетиране на ICMP съобщение е такъв както и при другите IP съобщения: най-напред се поставя IP заглавна част а след това от полчения деитаграм се формира кадър на слоя за достъп до мрежата.Този процес е показан на следната фигура:Въпреки всичко ICMP заглавието се различава от IP заглавието и зависи от типа на съобщението.Всяка ICMP заглавна част започва със следните 3 полета: тип на съобщението,код на съобщението и контролна сума ICMP е протокол на мрежовия слой,разположен над протокола IP Контролната сума обхваща целия ICMP-пакет и се използва за откриване на грешки,възникнали в него при предаването му през интермрежата.Използва се същият механизъм на контролно сумиране както при протокола IP.Полето съдържа различна допълнителна информация,съпровождаща изпратеното съобщение и подпомагаща неговата обработка.С цел избягване на излишно натоварване на мрежата не се изпращат съобщения за грешки,възникнали от други ICMP-пакети,или от broadcast - и multicast - пакети,или от фрагменти на една и съща дейтаграма (само в отговор на първия фрагмент се връща съобщение за грешка).3.Протокол ARP.IP - адресът на дадения хост се назначава от мрежовия администратор и не е свързан пряко с неговия локален адрес.Локалния адрес се използва само в границите на локалната (или глобалната) мрежа при обмен на кадри между хостовете и IP - маршрутизаторите на

тази мрежа.Когато даден IP - маршрутизатор получи IP - дейтаграма за хост,участващ в една от мрежите,непосредствено свързани към портовете му,то той е длъжен да капсулира дейтаграмата в кадър,съответстващ на дадената мрежа,да укаже в него локалния адрес на хоста-получател и да му изпрати този кадър.Ако локалния адрес на хоста-получател е неизвестен за IP -маршрутизатора,то маршрутизаторът трябва най-напред да намери този локален адрес по съдържащия се в пристигналата дейтаграма IP - адрес на хоста-получател.Същата задача възниква,когато дадения хост иска да изпрати IP - дейтаграма към друга мрежа чрез IP - маршрутизатор,чийто локален адрес му е неизвестен.За тази цел се използва протоколът ARP,описан в документа RFC 826.ARP работи по различен начин в зависимост от това,какъв протокол на каналния слой се използва в дадената мрежа.В локалните мрежи (LAN) протоколът ARP използва общодостъпен кадър ("до всички") за намиране на хоста (или маршрутизатора) с дадения IP адрес.Всички хостове на LAN получават тази ARP-заявка и сравняват указания в нея IP-адрес с техния собствен IP-адрес.Ако някой от хостовете установи съответствие,то той формира ARP -пакет - отговор (в който своя IP - адрес и локалния си (MAC) адрес),вмъква го в кадъра на каналния протокол и го предава към хоста - инициатор,чийто локален адрес е указан в ARP - заявката.Хостът - инициатор запомня в кеша си установения (чрез ARP) локален адрес на другия хост (или маршрутизатор) за да го използва при бъдещи комуникации с него.ARP - заявките и ARP - пакет - заявка,запълва в него всички полета с изключение на търсения локален адрес.Това поле се попълва от хоста,опознал своя IP - адрес.В глобалните мрежи (WAN) тази задача се решава най-често,като администраторът ръчно създава ARP - таблици на съответствие между IP -адреси и например,X.25 - адреси.В последно време обаче се използва автоматизация на този процес.Протоколът RARP пък решава обратната задача,т.е.намеране на IP - адрес по известен локален адрес.РАРП се използва,например при стартиране на бездискови работни станции,които в началния момент не знаят своя IP -адрес,а знаят само MAC - адреса на своя мрежов адаптер.Не трябва да се мисли,че всяка мрежова машина съдържа списък на физическите адреси на всички други машини и устройства.Това би било много ресурсоемко и администрирането на мрежата би се затруднило изключително много като се има в предвид постоянното и разширяване.От тук възниква и проблема за определяне на физическия адрес на машината получател.Ако тя се намира в друга мрежа то трябва да се намери и път за достъп до нея.За тази цел се използва протокола ARP (протокол за преобразуване на адреси).Той преобразува IP адресите в физически адреси,като освобождава приложните програми от необходимостта да работят с.

k c f .0pt'>q Осъществяване на всякакъв вид плащания чрез порталите на регионалните и държани органи на властта;

q Създаване на регионални портали обединяващи услугите на държавни и недържавни организации.

Трансформация на правителството

q Създаване на електронна структура за държавно управление на база единни стандарти;

q Създаване на правителствен портал, като обща точка за достъп до всички услуги, предоставяни на гражданите и бизнеса.