Дәріс №6: Пакеттер фильтрациясы. Фильтрация ережелері және критерийлері.

1) Пакеттер фильтрациясы

Жергілікті желілерде ақпарат бөлек үлестермен беріледі. Олар әр түрлі әдебиетте пакеттер (packets), кадрлар (frames) немесе сегменттер деп аталады. Пакеттік жіберулерді таңдау бірнеше маңызды қасиеттерге байланысты таңдалады.

Егер де желі арқылы мәліметтер жіберуші мен қабылдаушы арасында пакеттерді бөлмей үздіксіз жіберсе, онда желіні екеуі ғана қолдана алар еді. Басқа тұтынушыларға мәліметтер беріліп болғанша дейін тосуға тура келуші еді. Сонымен қатар үлкен масивті мәліметтерді жіберу кезінде жүйеде қателер мен кедергілер, істен шығу ықтималдылығы жоғары. Мысалға жергілікті желіде қателердің болу ықтималдығы 10^{-8}пакет ұзындығына 10 Кбит 10^{-4} ықтималдылықпен бұзылуы мүмкін, ал 10 Мбит ұзындықтағы массив 10^{-1} ықтималдылықпен. Бірнеше килобайт пакетке қарағанда бірнеше мегабайт массивтен қатені анықтау қиынырақ. Егер де қате табылған жағдайда барық массивті қайта жіберуге тура келеді. Массивті қайта жібергенде де қате шығу ықтималдығы үлкен, сондықтан килобайтпен шектелетін пакеттер тиімдірек.

Барлық тұтынушылардың құқықтарын теңестіру негізінде, желіде әрекеттесетін уақыт көлемін бірдей болу үшін пакеттер колданылады. Пакет ұзындығын шектеулі (көлемі бірнеше килобайт) түрде тасымалдау.

Үлкен пакеттер кішкентай пакеттерге карағанда артықшылықтары бар, мысалы, байт бойынша (8 бит) немесе (16 бит немесе 32 бит) мәліметті жіберу. Әрбір пакет өзінің мәліметтерінен басқа қызыметші мәліметтерді қоса жібереді. Көбінесе адрестік мәліметтер, кімнен кімге пакеттің берілетінін анықтайды. Егер тасымалданатын мәліметтердің қатынасы өте кішкентай болса, онда қызыметші мәліметтер көлемі үлкен болады, соған байланысты желідегі мәліметтердің жіберілу интегралды жылдамдығына әсер етеді.

Пакеттің құрылымы мен көлемі әр желіде сол желі технологиясының стандарттарымен белгіленген (мысалы, Ethernet, FDDI, Token Ring…) және осы ортадағы мәліметтерді жіберу желінің аппараттық мүмкіндігіне байланысты. Сонымен қатар бұл айнымалылар қолданылатын протоколға да байланысты.

Пакеттің құрылымы бойынша жалпы құрылу принциптері бар, олар жергілікті желідегі мәліметтермен алмасудың өзіндік ерекшеліктерін анықтайды.

Пакет негізгі жолдар мен бөліктерден тұрады (1-сурет).

1-сурет – Пакеттің құрылымы

– Биттердің ең басты әрекеті немесе преамбула – пакетті қабылдау және өңдеу үшін желілік адаптердің немесе басқа желілік құралдардың аппаратурасын алдын ала жөнге келтіруді қамтамасыз етеді. Бұл өріс толығымен жоқ болуы мүмкін немесе бір ғана бастапқы битке жүктелуі мүмкін.

– Қабылдаушы абоненттің желілік адресі (идентификатор), яғни желідегі әр қабылдаушы абонентке берілген жеке немесе топтық нөмір – қабылдағышқа өзіне жеке, өзі кіретін топқа, немесе біруақытта барлық желідегі абоненттерге адрестелген пакетті айыруға мүмкіндік береді.

– Жіберуші абоненттің желілік адресі (идентификатор), яғни желідегі әр жіберуші абонентке берілген жеке нөмір – қабылдаушы абонентті пакеттің қайдан келгені туралы ақпараттандырады. Жіберушінің адресін пакетке қосу бірі қабылдағышқа әр түрлі қабылдғыштардан алма кезек пакеттер келіп отырған кезде қажет болады.

– Қызметші ақпарат – пакеттің типі, оның нөмірі, өлшемі, форматы, оны жеткізу маршруты, қабылдағыштың онымен не істеу керегі жайлы және т.б. ақпараттармен қамтылған.

– Деректер (деректер өрісі) – бұл ақпаратты жіберу үшін пакет қолданылатын ақпарат. Деректер өрісінің пакеттің барлық қалған өрістерінен айырмашылығы пакеттің толық ұзындығын анықтайтын айнымалы ұзындығының болуында. Деректер өрісі жоқ арнайы басқару пакеттері де бар. Оларды желілік команда сияқты қарастыруға болады. Деректер өрісі бар пакеттер ақпараттық пакеттер деп аталады. Басқарушы пакеттер байланыс сеансының басталуы мен аяқталуының қызметін, ақпараттық пакеттің қабылдауын, ақпараттық пакеттің сұранысын растауды және т.б. жүзеге асыра алады.

– Пакеттің бақылау сомасы – бұл белгілі бір ережелерге сәйкес тапсырушы құратын және барлық пакеттер туралы ықшамдалған түрдегі ақпаратты иемденген сандық код. Қабылданған пакетпен тапсырушы жасаған есептеулерді қайталай отырып, қабылдағыш олардың нәтижелерін бақылау сомасымен салыстырады және пакетті жіберудің дұрыстығы немесе қателігі жайлы қорытынды жасайды. Егер пакеттен қателік табылса, онда қабылдағыш оның

қайтадан жіберілуін сұрайды. Әдетте циклды бақылау сомасы (CRC) қолданылады.

– Тоқтамды әдіс қабылдаушы абоненттің аппаратурасын пакеттің аяқталғаны туралы ақпараттандыру үшін қызмет етеді, қабылдағыш аппаратының қабылдау жағдайынан шығуын қамтамасыз етеді. Егер пакеттің жіберілуінің аяқталу моментін анықтауға мүмкіндік беретін өздігінен синхрондалатын кодты қолданса бұл өрістің болмауы мүмкін.

Алдында ескертілгендей, "пакет" (packet) терминінен басқа әдебиеттерде "кадр" (frame) термині жиі кездеседі. Кейде бұл терминдер бірдей мағынада болады. Бірақ кейде кадр мен пакет әр түрлі ұғым ретінде түсіндіріледі. Және де бұл әр түрліліктің анықтамалары бірегей емес.

Кейбір әдебиеттерде кадр пакетке кірістірілген деп айтылған. Мұндай жағдайда преамбула мен тоқтамды әдістен басқа аталан пакеттер өрісі кадрға жатады.

Басқа әдебиеттерде, керісінше, пакет кадрға кірістірілген делінген. Сонда пакет деп кадрда болатын ақпаратты айтуға болады, ол желі бойынша жіберіледі және қызмет өрістерімен жабдықталған.

Желі бойынша ақпаратпен алмасу сеансы процесінде алмасу протоколы деп аталатын белгіленген ережелер бойынша жіберуші және қабылдаушы абоненттер арасында ақпараттық және басқарушы пакеттермен алмасу жүзеге асады. Бұл желі бойынша алмасудың кез келген қарқындылығында ақпаратты сенімді жіберуді қамтамасыз етуге көмектеседі.

Қарапайым протоколдың мысалы суретте бейнеленген (2-сурет).

2-сурет – Пакеттерді тасымалдау реттілігі

Алмасу сеансы тапсырушының деректерді қабылдауға қабылдағыштың дайындығы туралы сұраныстан басталады. Ол үшін басқарушы пакет «Сұраныс» қолданылады. Егер қабылдағыш дайын болмаса, ол арнайы басқарушы пакет арқылы сеанстан бас тартады. Егер қабылдағыш дайын болған жағдайда, ол

жауап ретінде «Дайындық» басқарушы пакетін жібереді. Содан кейін деректерді жіберу басталады. Сонымен қатар әр қабылданған ақпараттық пакетке қабылдағыш «Растау» басқарушы пакетімен жауап қатады. Деректер пакеті қателіктермен жіберілген жағдайда, оған жауап ретінде қабылдағыш қайта жіберуді сұрайды. Сеанс тапсырушы байланыстың үзілуі жайлы хабарлайтын «Соңы» басқарушы пакетімен аяқталады.

Желі бойынша нақты алмасу кезінде көпдеңгейлі протоколдар қолданылады, олардың әрқайсысы өзінің пакет құрылымын болжамдайды (адрестеуді, басқарушы ақпаратты, деректер форматын және т.б.).

Пакеттің оптималды ұзындығын есептеу әдісі

Желі бойынша жіберілетін хабарламалар үшін пакеттің ұзындығы тұрақты болып таңдалады. Оны ақылмен таңдау желінің жіберу қабілеттілігін жоғарылатуға және ондағы жүктеуді азайтуға мүмкіндік береді. Пакет ұзындығы өте аз бола алмайды, өйткені пакеттің қызмет бөлігінің (атауы) белгіленген ұзындығында, бір пакетте жіберілетін хабарлама ақпаратының бөлшегі төмендейді. Сонымен қатар, ЭЕМ-ң хабарламаларды жинақтауға (бөлшектеуге) және пакеттерді бейнелеушілерді және олардың атауларын сақтауға қажет жады көлеміне бөлетін уақыттық шығындары көбейеді. Пакеттің үлкен ұзындығында және байланыс каналында деректерді жіберудің берілген анықтығында пакетті жіберудің қателікке ұшырауы, пакетті қайта жіберу жиілігінің болу ықтималдығы жоғарылайды, ол өз кезегінде желінің тиімділігін төмендетеді.

Әр желі үшін пакеттің оптималды ұзындығы (немесе пакеттердің ұзындықтарының оптималды диапазоны) беріледі, онда желі бойынша ақпарат алмасудың орташа жылдамдығы максималды болады. Бұл ұзындық өзгертілмейін өлшем емес, ол бөгеулер деңгейіне, алмасуды басқару әдісіне, желі абоненттеріні санына, жіберілетін ақпараттың сипаттамасына және басқа факторларға байланысты.

$$\omega^* = \begin{cases} 1{,}2\,\omega_2, \text{ егер } w \geq w_2 \\ \dfrac{\omega_2 + \omega_3}{2}, \text{ егер } w < w_2 \end{cases} \qquad (1)$$

мұнда ω_2 – жадыны үнемдеу және хабарламаларды жинақтау (бөлшектеу) бойынша процессордың жүйелік шығындарын минималдау жағынан қарағандағы пакеттің рационалды ұзындығы;

ω_3 – байланыс каналының берілген анықтылығы кезінде деректерді жіберудің максималды жылдамдығын қамтамасыз ететін пакеттің рационалды ұзындығы.

Пакеттің оптималды ұзындығының алынған мәні ω^* жақын мәнге 2^m жуықталады, мұндағы m – бүтін сан.

ЭЕМ желісінде жіберілген хабарлама ұзындығы l (бит) тең болатын математикалық үмітпен экспоненциалды заң бойынша үлестірілген деп қарастырса, онда жадыны үнемдеу жағынан қарағанда, пакетке бөлінген буфердің рационалды ұзындығын, сәйкесінше пакеттің рационалды ұзындығын келесі түрде алады:

$$\omega_1 = C + \sqrt{4Cl}, \qquad (2)$$

мұнда C – пакет атауының ұзындығы, (бит).

Пакеттің ұзындығы қысқарған жағдайда жоғарылайтын хабарламаларды жинақтауға (бөлшектеуге) ЭЕМ процессорларының жүйелік шығындарын есепке ала отырып, сонымен қатар жіберілетін хабарламалардың ұзындықтарының ұзаруына бір жақтылықты есептей отырып пакеттің рационалды ұзындығын пайдалылығына қарай мына формула арқылы анықтау:

$$\omega_2 = K_1\left(C + \sqrt{4Cl}\right), \qquad (3)$$

мұнда K_1 = 1,3 - 1,5.

ω мәні болғанда, деректерді жіберудің тиімді жылдамдығы $S_э$ максималды, және пакеттің ω_3 ұзындығына сәйкес келеді. Байланыс каналы бойынша пакетті жіберудің тиімді жылдамдығы:

$$S_Э = \frac{\omega - C}{\left(t_n + \frac{\omega}{S_H}\right)\left(1 + \frac{P_m}{1 - P_m}\right)}, \qquad (4)$$

мұнда ω - пакет ұзындығы, (бит);
C – пакет атауының ұзындығы, (бит);
t_n – деректерді жіберу бағытының өзгеру уақыты, (с);
S_H – канал бойынша деректерді жіберудің номиналды жылдамдығы, (бит/с);
p_m – пакеттегі қателіктер ықтималдығы,

$$p_m = 1 - \left(1 - p_B\right)^{\omega}$$

p_B – жіберудің бір биті бұрмалануының ықтималдығы.

2) Фильтрация ережелері және критерийлері

OSI моделінің деңгейінде функционалдау:

- Пакет сүзгіші *(screening* – экрандалатын маршрутизатор*);*
- Сеанстық деңгей шлюзі (экрандалатын көлік);
- Қолданбалы шлюз *(aplication gateway);*
- Эксперттік деңгей шлюзі *(stateful inspection firewall).*

Қолданылатын технология бойынша:

- Протокол жағдайын қадағалау *(stateful inspection);*
- Орадағы модульдер *(proxy).*

Орындалуы бойынша:

- Программа – аппараттық;
- Программалық.

Қосылу схемасы бойынша:

- Желіні қорғаудың ортақ схемасы;
- Қорғалатын жабық және қорғалмайтын ашық желі сегменттерінің схемасы;
- Бөлек жабық қорғау мен ашық желі сегментінің схемасы.

Фильтрдің әрқайсысы бөлек сүзгілерді мына жолдармен интерпретациялау үшін арналған:

1. интерпретацияланатын критерий ережелеріне сәйкес ақпаратты анализдеу, мысалы қабылдаушы адресі бойынша және ақпарат арналған жіберушіге немесе түсініктеме түріне.

2. интерпретацияланатын ереженің біреуі негізінде келесі шешімдерді қабылдау:

- берілгендерді тастап кетпеу;
- алушы атынан берілгендерді өңдеу және жіберушіге қорытындыны жіберу;
- анализді жалғастыру үшін берілгендерді келесі сүзгіге жіберу;
- келесі фильтрлардан берілгендерді өткізіп жіберу.

Сүзгілеудің ережесін жалғастырушы функциясына жататын қосымша іс - әрекеттерде бере алады, мысалға берілгендерді өңдеу, оқиғаларды тіркеу және т.б. Соған байланысты сүзгілеу ережесі орындалуына байланысты шарттарды анықтайды:

- алдағы берілгендердің жіберілуін шектеу немесе шешу;
- қосымша қорғаныс функцияларының орындалуы;

Ақпараттық ағымның талдауының критерийлері ретінде келесі шамалар қолданыла алады:

- желілік адрестерден, индикаторлардан, интерфейс адресінен, порттар номерінен және де басқа мәні бар берілгендерден тұратын хабарламалар пакетінің қосымша өрістері;
- мысалы компьютерлік вирустың бар жоғына тексеретін хабарлама пакеттерінің құрамы;
- ақпараттық ағымның сыртқы мінездемелері, мысалы уақытша, жиілік мінездемелер, берілгендердің көлемі және т.б.

Қолданылып отырған анализ критерийлері сүзгілеу жүзеге асырып жатқан OSI моделінің деңгейіне байланысты болады.