

АНАЛІЗ ПІДХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ЯКОСТІ ОБСЛУГОВУВАННЯ В ВІДОМЧІЙ ТЕЛЕКОМУНІКАЦІЙНІЙ МЕРЕЖІ ДПС УКРАЇНИ

У статті проведений аналіз підходів щодо забезпечення якості обслуговування сучасних телекомунікаційних мереж на основі класифікації пакетів (фреймів) на різних рівнях базової еталонної моделі взаємодії відкритих систем, розглянуто питання щодо використання списків управління доступом, як один із найефективніших методів забезпечення якості обслуговування та управління телекомунікаційною мережею. Встановлено, що загальноприйняті підходи щодо класифікації трафіку відповідно до рекомендацій Міжнародного союзу електрозв'язку та Європейського інституту телекомунікаційних стандартів не є прийнятними для відомчої телекомунікаційної мережі ДПС України, оскільки не в повному обсязі враховують значимість інформаційних потоків. Тому є необхідність розробки науково-методичного забезпечення щодо класифікацію трафіку в телекомунікаційній мережі ДПС України.

Ключові слова. телекомунікаційна мережа, якість обслуговування, трафік.

Вступ. Одним з основних аспектів, який повинен братися до уваги при аналізі телекомунікаційної мережі є забезпечення якості обслуговування. Якість обслуговування – це узагальнений (інтегральний) корисний ефект від обслуговування, який визначається ступенем задоволення користувача, як від послуг, які отримує так і від самої системи обслуговування [1].

Специфіка пакетних мереж полягає в тому, що на відміну від мереж з комутацією каналів, в одному і тому ж інформаційному потоці може передаватися різномірний трафік. При цьому кожен з типів трафіку характеризується низкою критичних і некритичних параметрів. Для передачі трафіку через пакетні мережі вводиться поняття класів обслуговування, що дозволяють оцінити якість надання послуги в пакетній мережі. Визначення якості обслуговування в даний момент є суб'єктивним і базується на методі експертних оцінок, тобто апіорі неможливо абсолютно гарантувати, що при проектуванні мережі будуть закладені мережні характеристики, що дозволяють однозначно забезпечити необхідну якість. З іншого боку, пакетні мережі мають розвинені механізми забезпечення якості обслуговування, використання яких дозволяє впливати на надання послуг зв'язку в процесі експлуатації в свою чергу існує ряд підходів, щодо класифікації трафіку в мережі.

Питання якості обслуговування, а саме теоретичними основами класифікації трафіку, висвітлювались в багатьох роботах. Вагомий внесок зроблений Міжнародним союзом електрозв'язку в рекомендаціях ITU-T Y.1541 [2, 3], Європейським інститутом телекомунікаційних стандартів в проекті TIPHONE [4] та провідного науковця в питаннях телекомунікаційних мереж Шриниваса Вегешна [5].

Постановка проблеми. Аналіз телекомунікаційної мережі ДПС України свідчить про те, що на даний час передача трафіку в телекомунікаційній мережі Державної прикордонної служби здійснюється без врахування типів інформаційних потоків, які транспортуються через мережу, і їх значення для підтримки основних задач покладених на телекомунікаційну систему Державної прикордонної служби України. Це приводить до того, що при перезавантаженні мережі погіршуються параметри передачі всіх потоків, незалежно від їх важливості. Одним з загальноприйнятим підходом є підхід щодо забезпечення якості обслуговування в телекомунікаційній мережі.

Використання функцій якості обслуговування дасть змогу забезпечити якісне обслуговування комутаційних вузлів та відповідність їх наступним умовам:

забезпечення раціонального налаштування параметрів комутаційних вузлів з метою оптимального використання інтенсивності вхідних потоків;

реалізація алгоритмів керування чергами інформаційних потоків шляхом використання механізмів обслуговування черг які б підтримували задані умови до якості обслуговування;

реалізація механізмів кондиціонування потоків пакетів з метою оптимального використання різнорідних потоків відповідно до профілів тарифіку;

оптимізація шляху проходження трафіку через мережу з метою максимізації завантаженості комутаційних вузлів та каналів передачі даних при заданих умовах до якості обслуговування потоків даних;

забезпечення підтримки існуючих і нових мультимедійних служб і додатків.

Метою статті є аналіз підходів щодо забезпечення якості обслуговування в відомчій телекомунікаційній мережі ДПС України.

Виклад основного матеріалу. Якість обслуговування в маршрутизаторах на даний час досягається впровадження правил QoS (Quality of Service), для будь-якого правила потрібно насамперед визначити трафік, що має особливі вимоги, інструмент класифікації позначає пакет або фрейм певним значенням. Ці значення міток дозволяють розмежувати різні типи трафіку і застосувати до них різні правила обробки черг.

Класифікація пакетів (packet classification) являє собою засіб, що дозволяє віднести пакет до того чи іншого класу трафіку в залежності від значення одного або кількох полів пакета [5]. Функція розпізнання може бути як дуже простою, так і вельми складною і залежить від способу класифікації трафіку.

На даний час комутаційне обладнання різних рівнів може проводити класифікацію наступними шляхами:

1. Параметри другого рівня базової еталонної моделі взаємодії відкритих систем (Open Systems Interconnection Basic Reference Model, OSI):

біти класу послуг 802.1Q/p (CoS, Class of Service) - Ethernet фрейми можуть позначатися за допомогою біт в заголовку другого рівня з використанням 802.1p біту пріоритету в заголовку 802.1Q (рис. 1). Розмір поля 802.1p - 3 біти, таким чином тільки вісім класів сервісу (0-7) доступні для маркування Ethernet фреймів другого рівня;

PRI	CFI	VLAN ID
-----	-----	---------

PRI (Значення пріоритету) - 3 біти.

CFI (Canonical Format Indicator – індикатор канонічного формату) - 1 біт.

VLAN ID (ідентифікатор VLAN) - 12 біт.

Рис. 1. Фрагмент значення заголовку 802.1Q IP-пакету.

MPLS (Multiprotocol Label Switching) EXP - Біти MPLS EXP - це три біта в MPLS мітці (рис. 2), що містять індикатор QoS [6]. За замовчуванням, під час імпозиції (додавання) мітки в значення MPLS EXP записується значення поля IPP IP пакета. Розмір поля дозволяє використовувати до восьми QoS маркувань. Значення EXP біт використовуються для визначення PNH на вузлах MPLS мережі і можуть використовуватися для забезпечення прозорості перенесення значень IPP/DSCP в пакетах клієнта в разі застосування MPLS методів тунелювання Diffserv (MPLS DiffServ Tunneling Modes).

MPLS	CoS	S	TTL
------	-----	---	-----

CoS (клас обслуговування) - 3 біти.

S (ознака “дна” стека) - 1 біт.

TTL (“час життя”) - 8 біт.

Рис. 2. Формат MPLS-мітки

2. Параметри третього рівня (біти IP Precedence [IPP], кодові точки диференційованих послуг [DSCP Code-Points]):

байт типу сервісу IP-TypeofService (ToS). У зв'язку з тим, що в процесі проходження пакетів від джерела до призначення часто змінюється середу другого рівня, більш універсальний метод маркування полягає у використанні заголовка третього рівня. Другий байт заголовка IPv4 пакета - це байт TOS (рис. 3). Перші три біти байта TOS біти IPP (IP Precedence) дозволяють як і CoS біти 802.1p помітити пакет тільки вісьмома значеннями (0-7) [7];

P2	P1	P0	T3	T2	T1	T0	CU
----	----	----	----	----	----	----	----

IPP (IP-пріоритет) - 3 біти (P2-P0).

TOS (тип обслуговування) - 4 біти (T3-T0).

CU (не використовується) - 1 біт.

Рис. 3. Структура байта ToS

значення DSCP (Differentiated Services Code Point) можуть бути виражені в цифровій формі (рис. 4) або з використанням спеціальних ключових слів, які називаються поведінкою мережевих ділянок (PHB - Per-HopBehavior). Визначено три класи DSCP маркування: по можливості (besteffort - максимальних зусиль або DSCP 0), гарантована доставка (Гарантований Forwarding, AF) і термінова доставка (термінова доставка - EF) [8]. На додаток до цих трьох певних класів існують коди селектора класів (клас точок вибору коду), які сумісні з IPP (CS1-CS7 ідентичні значенням 1-7 IPP). Визначено чотири класи гарантованої доставки, вони починаються з AF і далі дві цифри. Перша цифра визначає AF клас і приймає значення від 1 до 4. Друга цифра визначає рівень ймовірності скидання пакета в межах кожного класу і приймає значення від 1 (мінімальна ймовірність скидання) до 3 (максимальна ймовірність скидання). Значення DSCP можуть бути виражені в десятковому форматі або з використанням ключових слів DSCP (EF - 46, AF31 – 26) [6].

DS5	DS4	DS3	DS2	DS1	DS0	CU	CU
-----	-----	-----	-----	-----	-----	----	----

DSCP (Код диференційованих послуг) - 6 біт (DS5-DS0).

CU (не використовується) – 2 біти.

Рис. 4. Структура байта DS

елемент списку доступу (Access Control Entries - ACE) перевіряється відповідність трафіку на основі адреси та інформації порту третього рівня. ACE-записи групуються в списки управління доступом (Access Control Lists - ACL), або QoS-стратегії, що застосовуються до певних портів комутуючих пристроїв. Списки управління доступом представляють собою набір директив, які визначають: як організований вхід на інтерфейси; як проходить передача інформації через комутаційний пристрій; як організований вихідний інтерфейс комутаційного пристрою.

Списки управління доступ складаються з двох компонентів:

перевірка відповідності характеристик пакету, дозволяє визначити чи пакет відповідає інструкції списків доступу. Відповідність як правило визначається тим чи входить в списки доступу в діапазон IP-адрес (MAC-адрес) пакет, який поступив на вхідний (вихідний) порт;

дії над правилом полягають в тому, що пакет який відноситься до певного правила (групи правил) повинний оброблятися відповідними інструкціями.

Отже списки управління доступом можуть бути створені для кожного протоколу, для якого буде відбуватись фільтрація даних, та для кожного інтерфейсу окремо. По своїй суті списки управління доступом можуть створюватись один для фільтрації вхідного потоку даних інший для вихідного потоку даних.

Суть підходу до забезпечення якості обслуговування на основі використання списків управління доступу полягає в тому, що для кожного протоколу, дані якого необхідно

фільтрувати, і для кожного інтерфейсу необхідно створити список керування доступом. У деяких протоколах створюється один список для фільтрації вхідних пакетів інформаційних потоків інший - для вихідних.

Після того як пакет буде перевірений на відповідність заданій умові за допомогою директиви списку доступу, йому може бути дозволено або заборонено використання інтерфейсу, сам список управління доступом підключається до інтерфейсу за допомогою так званої групи доступу. Маршрутизатори та комутатори перевіряють пакети інформаційних потоків і заголовки верхніх рівнів для списків доступу, як показано на рис. 5.

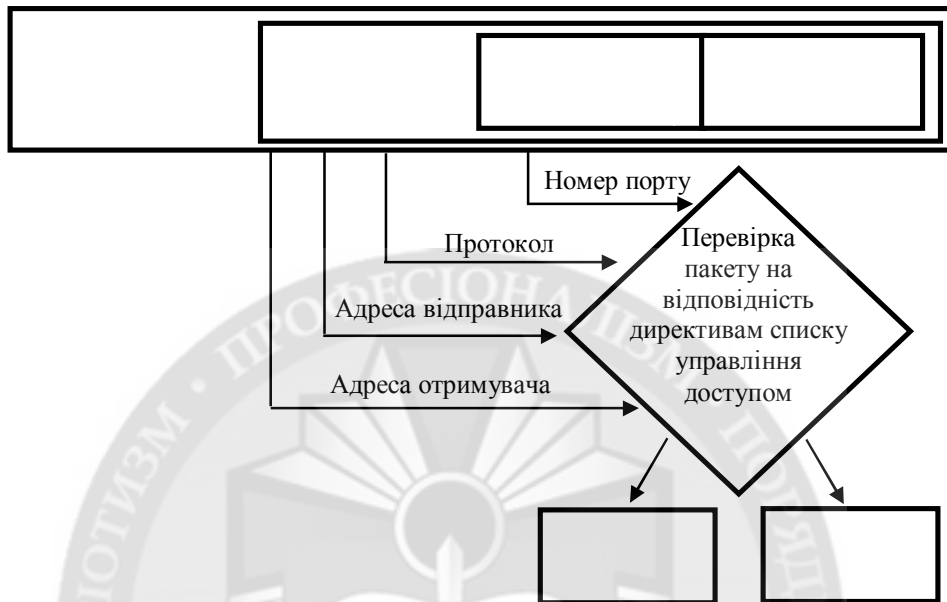


Рис. 5. Перевірка пакетів и заголовків верхніх рівнів

На даний час широкого розповсюдження отримали два основних типи списків доступу, а саме стандартний та розширений список доступу, проте існують і інші, а саме: динамічні; рефлексивні; обмежені за часом; іменовані IP-списки; списки, що використовують тимчасові діапазони; контекстно-орієнтовані та проксі-аутентифіковані. Найбільш прийнятними з огляду врахування основних показників розмежування трафіку є розширені списки доступу. На рисунку 6 відображено частину IP-пакету, по яким може бути проведена перевірка на співставлення з критеріями за допомогою розширеного списку доступу, тобто розширені ACL (тільки для зареєстрованих клієнтів) керують трафіком, порівнюючи адреси джерела і призначення IP-пакетів з адресами, заданими в списку.

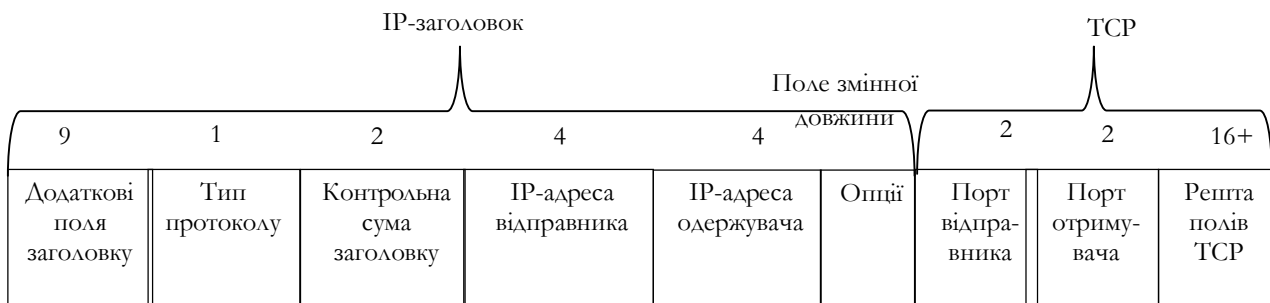


Рис. 6. Частина IP-пакету, по яким може бути проведена перевірка на співставлення з критеріями за допомогою розширеного списку доступу

Слід зазначити, що характерною особливістю списків управління доступом є можливість використання бітів інвертованої маски (wildcardmask). Інвертована маска являє

собою 32-бітову величину, яка розділена на чотири октети, кожна з яких складається з восьми бітів [9]. Дана маска дає змогу використовувати для вказівки одного або декількох IP-адрес (діапазону IP-адрес), які будуть перевірятися на відповідність умовам списку контролю доступу. Інвертована маска, як і маска підмережі, тісно пов'язана з IP-адресою і використовує нулі й одиниці, для того щоб вказати, як слід трактувати відповідні біти IP-адреси.

Незважаючи на те що інвертована маска списків управління доступом і маска підмережі представляють собою 32-бітові величини функції, як вони виконують значно відрізняються. Нулі й одиниці в масці підмережі визначають мережу, підмережа і номер вузла. Біти інвертованою маски вказують, чи буде перевірятися відповідний біт. Отже, нулі й одиниці в інвертованою масці вказують списку управління доступом на необхідність перевіряти чи не перевіряти відповідні біти в IP-адресі.

Виходячи з можливостей списків управління доступом та порядком інформаційного обміну між ІТС та підсистемами в телекомунікаційній системі Держприкордонслужби України та з метою забезпечення якості обслуговування необхідними параметрами є: визначення напрямку правила (вхідний/вихідний), IP-адреса відправника (діапазон IP-адрес), IP-адреса отримувача (діапазон IP-адрес), протокол передачі, порт відправника, порт отримувача, тип сервісу.

Всі вказані параметри є наявними та мають жорстку прив'язку: по IP-адресам до наказів Адміністрації ДПС України, щодо IP-адресації; по портам до технічних завдань на розроблення ІТС або по комп'ютерним додаткам, тип сервісу до рекомендацій ІТУ-Т Y.1541 [2, 3] та європейським інститутом телекомунікаційних стандартів в проекті TIPHONE [4].

Проте підхід щодо призначення пріоритетів інформаційним потокам відповідно до загальноприйнятих рекомендацій спрямований перш за все для інтернет мережі та не враховує інформаційні процеси які циркулюють в телекомунікаційній мережі та пов'язані з оперативно-службовою діяльністю органів та підрозділів охорони кордону. Тому загальноприйняті підходи щодо пріоритезації трафіку не є прийнятними.

Тому постає істотне питання щодо розробки науково-методичного апарату по забезпеченню якості обслуговування мережевої складової інтегрованої інформаційно-телекомунікаційної системи на основі списків управління доступом з встановленням відповідного пріоритету трафіку (класифікацію пакетів).

Висновки. Проведений у роботі аналіз показав що найбільш доцільно використовувати механізм кондиціонування потоків пакетів з метою оптимального використання різнорідних потоків відповідно до профілів трафіку, а саме використання розширених списків управління доступом з вказанням в полі опція пріоритету (значення DSCP). Проте стандартні підходи по пріоритезації не є прийнятними з огляду на те що телекомунікаційна система ДПС України є телекомунікаційна система спеціального призначення і потребує врахування особливостей оперативно-службової діяльності ДПС України. Тому метою подальшого дослідження є розробка науково-методичного апарату по забезпеченню якості обслуговування мережевої складової інтегрованої інформаційно-телекомунікаційної системи з урахуванням особливостей оперативно-службових діяльності ДПСУ.

ЛІТЕРАТУРА:

1. Глоба Л.С., Скуліш М.А., Дяденко О.М. Посібник для студентів технічних спеціальностей/ Рек. МОН України, НТУУ "КПІ", Інститут телекомунікацій, кафедра інформаційно-телекомунікаційних мереж, К.: Норіта-плюс, 2007. – 348 с.
2. Ash G., Morton A. RFC 5976 - Y.1541-QOSM – Model for Networks Using Y.1541 QoS Classes draft-ietf-nsis-y1541-qosm-10. – 2010. Режим доступу: <http://www.rfc-editor.org/rfc/rfc5976.txt>. Дата доступу: 04.02.2016.
3. Postel J. RFC 791 – Internet Protocol / J. Postel // RfcEditor [Electronic resource]. – 1981. Режим доступу: <http://www.ietf.org/rfc/rfc791.txt>. Дата доступу: 04.02.2016.
4. ETSI TR 102 805-1- End-to-end QoS management at the Network Interfaces, Part 1: User's E2E QoS - Analysis of the NGN interfaces (user case) // [Electronic resource]. – 2009. Режим доступу:

https://www.etsi.org/deliver/etsi_tr/102800_102899/10280501/01.01.01_60/tr_10280501v010101p.pdf.

Дата доступу: 04.02.2016.

5. Шринивас Вегешна Качество обслуживания в сетях IP. - М.: Вильямс, 2003. - 368 с.

6. Mario Marchese. QoS over heterogeneous networks. - New York: John Wiley & Sons, 2007 - 330 p.

7. Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide. Режим доступу: http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfmcli2.html. Дата доступу: 04.02.2016.

8. Nichols K. RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers // RfcEditor [Electronic resource]. - 1998. Режим доступу: <http://www.ietf.org/rfc/rfc2474.txt>. Дата доступу: 04.02.2016.

9. Программа сетевой академии Cisco CCNA 1 и 2. Вспомогательное руководство, 3-изд., с испр.: Пер. с англ. - М.: Издательский дом "Вильямс", 2005. - 1168 с.

REFERENCES:

1. Globa L.S., Skulish M.A., Djadenko O.M. Posibnyk dlja studentiv tehnicnyh special'nostej/ Rek. MON Ukraïny, NTUU "KPI", Instytut telekomunikacij, kafedra informacijno-telekomunikacijnyh mrezh, K.: Norita-pljus, 2007. - 348 s.

2. Ash G., Morton A. RFC 5976 - Y.1541-QOSM - Model for Networks Using Y.1541 QoS Classes draft-ietf-nsis-y1541-qosm-10. - 2010. Rezhym dostupu: <http://www.rfc-editor.org/rfc/rfc5976.txt>. Data dostupu: 04.02.2016.

3. Postel J. RFC 791 - Internet Protocol // J. Postel // Rfc Editor [Electronic resource]. - 1981. Rezhym dostupu <http://www.ietf.org/rfc/rfc791.txt>. Data dostupu: 04.02.2016.

4. ETSI TR 102 805-1- End-to-end QoS management at the Network Interfaces, Part 1: User's E2E QoS - Analysis of the NGN interfaces (user case) - // [Electronic resource]. - 2009. Rezhym dostupu: https://www.etsi.org/deliver/etsi_tr/102800_102899/10280501/01.01.01_60/tr_10280501v010101p.pdf. Data dostupu: 04.02.2016.

5. Shrinivas Vegeshna Kachestvo ob sluzhivanija v setjah IP. - M.: Vil'jams, 2003. - 368 s.

6. Mario Marchese. QoS over heterogeneous networks. - New York: John Wiley & Sons, 2007 - 330 p.

7. Cisco IOS Release 12.0 Quality of Service Solutions Configuration Guide. Rezhym dostupu: http://www.cisco.com/c/en/us/td/docs/ios/12_2/qos/configuration/guide/fqos_c/qcfmcli2.html. Data dostupu: 04.02.2016.

8. Nichols K. RFC 2474 - Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers // RfcEditor [Electronic resource]. - 1998. Rezhym dostupu: <http://www.ietf.org/rfc/rfc2474.txt>. Data dostupu: 04.02.2016.

9. Programma setevoj akademii Cisco CCNA 1 i 2. Vspomogatel'noe rukovodstvo, 3-izd., s ispr.: Per: s angl. - M.: Izdatel'skij dom "Vil'jams", 2005. - 1168 s.

Рецензент: д.т.н., проф. Катеринчук І.С., доцент кафедри зв'язку автоматизації та захисту інформації, Національна академія ДПС України

к.т.н. Хоптинский Р.П.

АНАЛИЗ ПОДХОДОВ ПО ОБЕСПЕЧЕНИЮ КАЧЕСТВА ОБСЛУЖИВАНИЯ В ВЕДОМСТВЕННОЙ ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ДПС УКРАИНЫ.

В статье проведен анализ подходов по обеспечению качества обслуживания современных телекоммуникационных сетей на основе классификации пакетов (фреймов) на различных уровнях базовой эталонной модели взаимодействия открытых систем, рассмотрены вопросы использования списков управления доступом, как один из наиболее эффективных методов обеспечения качества обслуживания и управления телекоммуникационной сетью. Установлено, что общепринятые подходы к классификации трафика в соответствии с рекомендациями Международного союза электросвязи и Европейского института телекоммуникационных стандартов не приемлемы для ведомственной телекоммуникационной сети ГПС Украины, поскольку не в полном объеме учитывают значимость информационных потоков. Поэтому есть необходимость разработки научно-методического обеспечения по классификации трафика в телекоммуникационной сети ГПС Украины.

Ключевые слова. телекоммуникационная сеть, качество обслуживания, трафик

ANALYSIS APPROACHES TO QUALITY SERVICE IN TELECOMMUNICATIONS NETWORKS STATE BORDER GUARD SERVICE OF UKRAINE.

The article analyzes approaches to ensure quality of service modern telecommunications networks based on the classification of packets (frames) at various levels of open systems interconnection basic reference model, the issues regarding the use of access control lists as one of the most effective methods to ensure quality of service and management of telecommunications network. Found that conventional approaches to classification of traffic according to the recommendations of the International Telecommunication Union and the European Telecommunications Standards Institute is not suitable for departmental telecommunications network Border Guard Service of Ukraine because they do not fully take into account the importance of information flow. Therefore, there is need to develop scientific and methodological support for the classification of traffic in telecommunications networks Border Guard Service of Ukraine.

Keywords. telecommunication network, quality of service, traffic.

