ЎЗБЕКИСТОН РЕСПУБЛИКАСИ АХБОРОТ ТЕХНОЛОГИЯЛАРИ ВА КОММУНИКАЦИЯЛАРИНИ РИВОЖЛАНТИРИШ ВАЗИРЛИГИ

ТОШКЕНТ АХБОРОТ ТЕХНОЛОГИЯЛАРИ УНИВЕРСИТЕТИ

МУСТАҚИЛ ИШ

Мавзу: SNMP протоколлари

ТОШКЕНТ 2017

SNMP протоколлари

Режа

1. SNMP протоколи ривожланиш тарихи
2. SNMP бошқарув асослари
3. SNMP протоколи камчиликлари
4. NetFlow протоколи таҳлили

Таянч иборалар: *SNMP, High-Level Entity Management System, Simple Gateway Monitoring Protocol, Common Management Information Protocol, Internet Architecture Board, Structurefor Management Information, SNMP-менеджер, SNMP-агент, Protocol Data Unit.*

1. SNMP протоколи ривожланиш тарихи

SNMP протоколини яратишда уч йўнилиш бўйича ишланмалар ўз ҳиссасини қўшди:

1. High-Level Entity Management System (HEMS)

Юқори даражадаги бошқарув объектлари тизими. Бир қатор қизиқарли техник характеристикалар билан бошқарув тизимини белгилайди. Афсуски, HEMSдан фақат унинг ишлаб чиқилган жойларида фойдаланилди, ва бу, унинг фаолияти тўхтатилишига олиб келди.

2. Simple Gateway Monitoring Protocol (SGMP)

Оддий роутер ёрдамида бошқариш протоколи. Тадқиқот бир гурух тармоқ муҳандислари томонидан тез ўсаётган Internet билан боғлиқ масалар ечимини топиш учун бошланилган; уларнинг иши натижаси Internet роутерларини бошқариш учун мўлжалланган протокол ҳисобланади. SGMP Internetнинг кўплаб ҳудудий тармоқларида амалга оширилган.

3. TCP юзасидан CMIPoverTCP (CMOT). OSIга асосланган тармоқ бошқарувини, хусусан, TCPга асосланган бирлашган тармоқларни соддалаштириш учун Common Management Information Protocol (CMIP) (умумий бошқарув маълумот протоколи)ни қўллашни даъват қилади. Бу уч услубнинг (HEMS, SGMP и CMOT) устун ва камчиликлари 1987-йил иккинчи ярми давомида тез-тез ва қизғин муҳокама қилинди. 1988-йил бошига келиб, бугунги кунгача ўзаро таъсирнинг такрорланмас механизмларини сақлаб турадиган ўз тармоқ қурилмалари учун ўзининг мониторинг маҳсулотлари ва конфигурациясини яратган турли ишлаб чиқарувчилар бошқарув воситалари қандайдир умумий тўплами зарурлиги маълум бўлди.

Кўплаб кенгашлардан кейин IAB (Internet Architecture Board, Интернет протоколлари техник ишланмаси учун жавобгар гурух) 1988-йил апрелида даврга оид RFC 1052 IAB Recommendations for the Development of Internet Network Management Standardsни чоп этди: унда у тез орада Оддий Тармоқ Бошқаруви

элементларини (Simple Network Management) тузишга даъват қилди. Иккита ишчи гурух ташкил қилинди. Бир гурух Бошқарув Информацион базаси MIB (Management Information Base) элементларини ишлаб чиқиш билан шуғуллана бошлади. Кейинчалик, бу йўналиш бўйича ишлар Объектларни Бошқариш Структураси SMI (Structure for Management Information) тузилишига қўшилиб кетди.

Протокол бошқарувини ривожлантириш билан машғул бошқа гурух эса кейинчалик SNMP деб номланган SGMPнинг янги версиясини яратиш бошқарув муаммолари вақтинчалик ечими бўлади, деган қарорга келди. Узоқ вақт қўлланилиши учун, чуқур ва батафсил ишланмалардан кейин OSI (ёки CMOT, ёки CMIP) га асосланган технологиялардан бири қўлланилиши керак эди.

Ундан ташқари, барча бошқарув тизимларида бошқарув структураларини намойиш қилиш учун умумий тилга ўхшаш ASN 1 (Abstract Syntax Notation One, биринчи рақамли синтаксиса спецификацияси)ни қўллашга келишиб олинди. Бу спецификация ҳозирги кунда. MIB структураси ва элементларини тасвирлашда қўлланилади.

1988-йил августда учта асосий ҳужжат пайдо бўлди:

1. RFC 1065: Structure and Identification of Management Information for TCP/IP-based internets.
2. RFC 1066: Management Information Base for Network Management of TCP/IP-based internets.
3. RFC 1067: A Simple Network Management Protocol.

Натижада бу ҳужжатлар қайта нашр қилинди ва SNMP кейинги авлодини белгилаш учун тўлдирилди: ўз навбатида қайта ишланган RFC 1155, 1156 и 1157. Охир оқибат, 1991-йил майида SNMP протоколи биринчи версиясини тузиш бўйича ишлар тугатилди ва бу қуйидаги ҳужжатлар тузилишида ўз аксини топди:

1. RFC 1155: (SIM) Structure and Identification of Management Information for TCP/IP-based internets (Май, 1990)

- глобал тармоқ кўринишида бошқарув ҳабарлари структурасини белгилайди.

Вақти вақти билан ўзгарадиган номларни аниқлаш синтаксисини белгилайди.

2. RFC 1212: (MIB) Concise MIB (Management Information Base) Definitions (Март, 1991)

- Вақти вақти билан ўзгарадиган номларни аниқлаш синтаксиси қисман RFC 1155ни тўлдиради.

3. RFC 1213: (MIB-II) Management Information Base for Network Management of TCP/IP-based internets: MIB-II (Март, 1991)

- TCP/IP тармоққа кирувчи статус ва статистика, конфигурация учун жавоб берадиган даврий ўзгарадиган тизимлар рўйхатини ўз ичига олади.

4. RFC 1157: (SNMP) A Simple Network Management Protocol (Май, 1990)

- даврий ўзгарадиган тизимлар белгиланишини қабул қилиш ва янгилаш

учун бошқарув станцияси ва бошқарув объекти алмашинадиган хабарларни белгилайди.

Конфигурациясида сезиларли ўзгаришлар бўлганда тизим томонидан юбориладиган trap (alarm) - хабарларни белгилайди.

Бугунги кунда SNMP турли тижорат, университет ва тадқиқот бирлашган тармоқларини бошқариш энг машҳур протоколи ҳисобланади. SNMP билан боғлиқ унинг стандартизацияси фаолияти етказиб берувчилар замонавий амалий бошқарув дастурлари ишга туширилиши билан бир йўсинда давом этади. SNMP нисбатан оддий протоколдир, бироқ, унинг характеристикалари тўплами гетероген тармоқлар бошқарувида юзага келадиган муаммоларни ечишда анча кучли ҳисобланади.

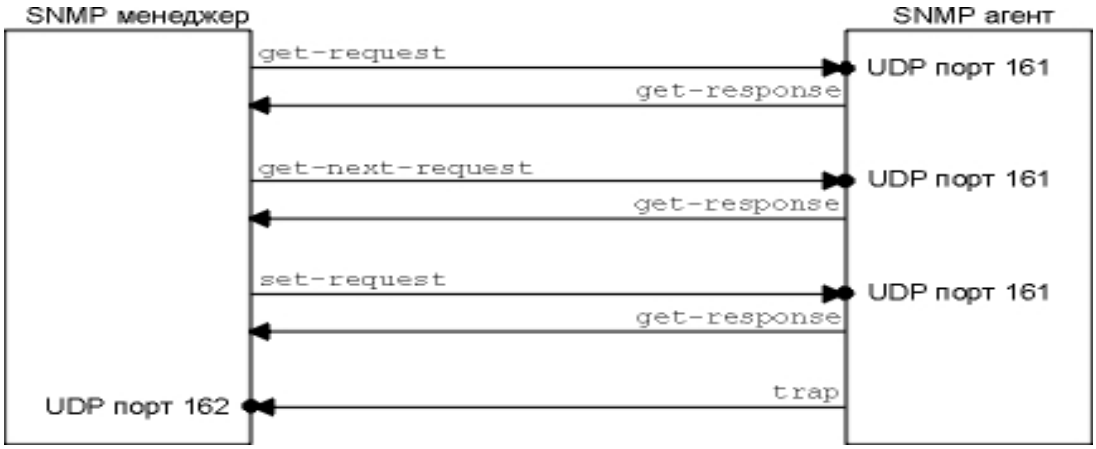
2. SNMP бошқарув асослари

SNMP бошқарув асослари мижоз ва провайдер ўртасида алмашинадиган беш турли хабарларларни белгилайди.

Бир неча ўзгарувчан даврийликдан бирининг аҳамиятини олиш: get-request оператори. Шундан кейинги ёки бир нечта кўрсатилган ўзгарувчан даврийликни олиш. Бир нечта ўзгарувчан даврийликдан биттасини аҳамиятини белгилаш set-request оператори. Бир нечта ўзгарувчан даврийликдан биттасини аҳамиятини бериш: get-response оператори. Бу хабарни агент менеджерга get-request, get-next-request ва set-request операторларига жавоб тарзда юборади. Агент билан имадир содир бўлганда менеджергахабар бериш: trap оператори.

Биринчи учта хабар менеджердан агентга, қолган иккитаси агентдан менеджерга юборилади. 20.1-расмда барча беш операторлар кўрсатилган.

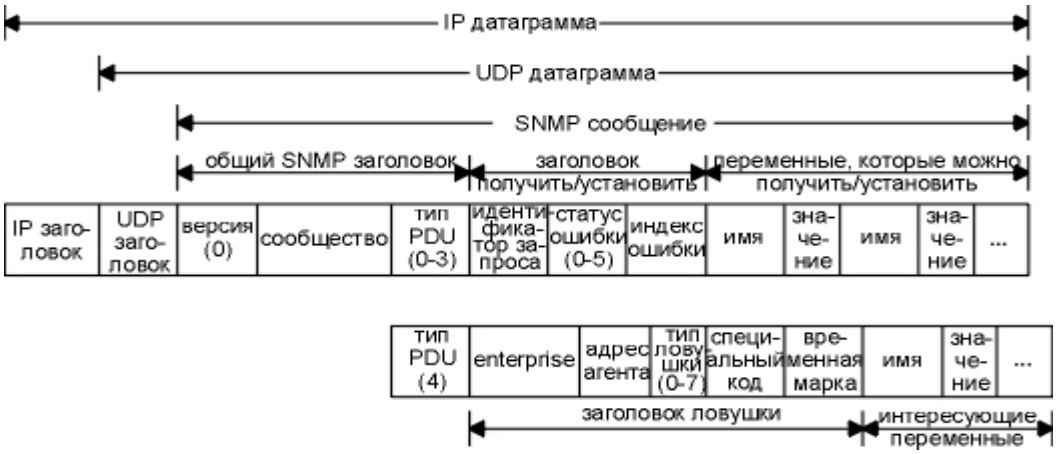
Бешта SNMPдан тўтрттаси оддий сўров-жавоб кетма-кетлигида юажарилгани сабаб(менеджер сўров юборади, агент жавоб қайтаради), SNMP лар UDPдан фойдаланишади. Бу англатадики, менеджер сўрови агентга болмаслиги, агент жавоби ҳам менеджерга етиб бормаслиги мумкин. Бундай ҳолатда, менеджер тайм-аутни ишлаб беради ва қайта жўнатади (20.1-расм).



Расм 20.1. SNMP бешта операторлари

Менеджер бу учта сўровни UDP порт 161га жўнатади. Агент UDP порт 162га тузоқлар (trap) юборади. Икки турли порт ишлатилганлиги сабаб, бир тизимбир вақтнинг ўзида ҳам агент, ҳам менеджер сифатида келиши мумкин.

20.2-расмда UDP датаграммага инкапсуляция қилинган SNMP беш хабарининг формати келтирилган.



Расм 20.2. SNMP бешта хабарининг кўриниши

Version майдонининг миқдори 0га тенг. Бу миқдор ҳақиқатда минус бир рақамига тенг.

20.1-жадвалда протоколнинг маълумотлар блоки тури учун белгиланиш ёки миқдор кўрсатилган (PDU type). (PDU – протокол маълумотлари блоки – Protocol Data Unit, одатда "пакет" деб номланади.)

Жадвал 20.1.

SNMP хабарлари PDU хили

PDU type	Исм
0	get-request
1	get-next-request
2	set-request
3	get-response
4	Trap

Ҳамжамият (community) - бу парол очиқ ҳолда сақланадиган рамзлар қаторидир. Парол менеджер ва агент ўртасидаги мумоқотда қўлланилади. Одатий белгиланиш – 6 рамзли public қатори.

get, get-next ва set операторларида менеджер агент томонидан get-response хабарида қайтариладиган сўров идентификаторини (request ID) биз бу турдаги

ўзгарувчан даврийликни бошқа UDP киритмаларида кўрганмиз. Бу мижозга (берилган вазиятда менеджер) сервердан кеган жавобларни ўзи жўнатган сўровлар билан солинтириш имконини беради. Бу майдон, шунингдек, бир ёки бир неча агентларга сўров юбориш, кейин эса олинган жавобларни ўз жойи бўйича қўйиш имконини беради. Хато статуси (errorstatus) бу агентларга қайтариб бериладиган ва хатони кўрсатадиган бутун сондир. 20.2-жадвалда хатолар тасвири, номлари ва миқдорлари келтирилган.

Жадвал 20.2.

SNMP хатоси статуси мазмуни

Хато статуси	**номи**	**Тасвир**
0	No Error	Ҳаммаси жоўида
1	Too Big	Мижоз жавобни бир SNMP хабарига жойлаштира олмайди
2	No SuchName	оператор аҳамиятсиз ўзгарувчан даврийликни кўрсатади
3	Bad Value	Ўрнатиш операцияларида нотўри белгилашга йўл қўйилган ёки хато қилинган
4	readOnly	менеджер “фақат ўқиш учун” деб белгиланган ўзгарувчан даврийликни ўзгартиришга ҳаракат қилди
5	Gen Error	Аниқланмаган хато

Хато юзага чиққанда, хатолар индекси қайси ўзгарувчан даврийликда хато содир бўлганини кўрсатадиган тўлиқ ишдан олинишдир. Бу миқдор агент томонидан фақат noSuchName (бундай исм йўқ), badValue (нотўғри миқдор) и readOnly (фақат ўқиш учун)хатолари учун ўрнатилади

Ўзгарувчан даврийлик номлари рўйхати get, get-next ва set сўровларида келтирилади. Миқдорлар бўлими get ва get-next операторларида инкор қилинади. trap (PDU type 4га тенг) оператори учун хабарлар SNMP ўзгартирилади.

3. SNMP протоколи камчиликлари

SNMP протоколи кўплаб бошқарув тизимларида асос вазифасини бажаради, бироқ бир қанча принципиал камчиликларга эга бўлиб, улар қуйида саналган.

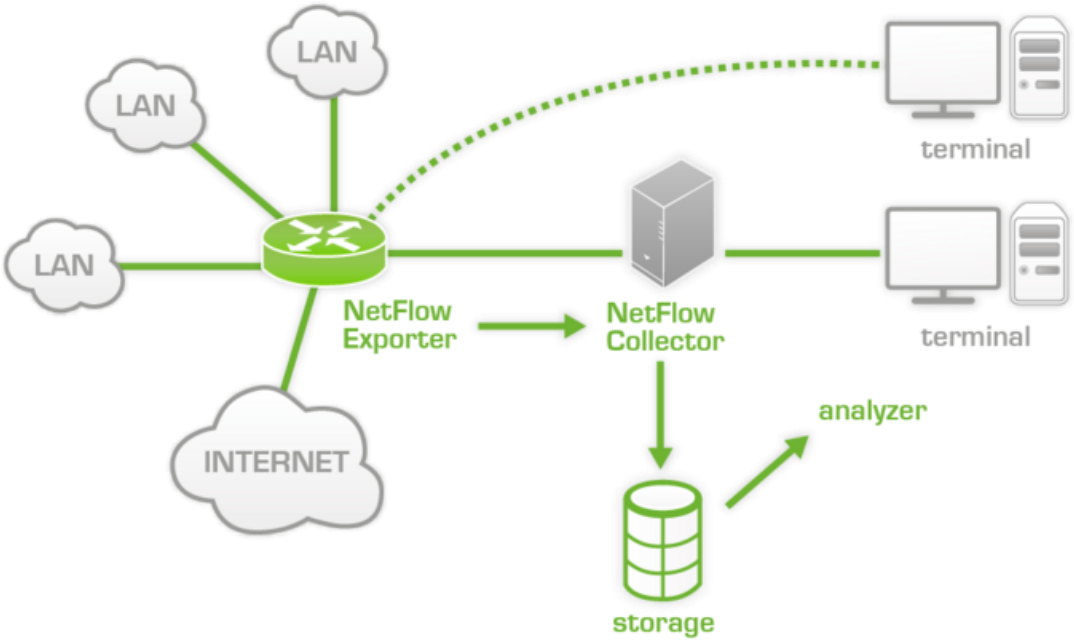
Агентлар ва менеджерлар ўзаро аутентификацияси воситаси йўқлиги. аутентификация воситасларига киритилиши мумкин бўлган ягона восита хабарларда «ҳамжамият қаторлари» - «community string» нинг қўлланилишидир. Бу қатор тармоқ бўйлаб очиқ шаклда юборилади ва агентлар ва

менеджерларнинг ҳамжамиятларга бўлиниши асиси бўлиб хизмат қилади, шу сабаб агент фақат community string майдонида агент омборида сақланадиган қатор каби бир хил рамзий қаторни кўрсатадиган менеджерлар билан ўзаро таъсирлашади. Бу, албатта, аутентификация усули эмас, балки агентлар ва менеджерлар тузилиши усулидир. SNMP v.2 версияси бу камчиликни бартараф қилиши керак, лекин стандарт тадқиқотчилари ўртасидаги келишмовчиликлар сабаб янги аутентификацияси воситалари бу версияда пайдо бўлган бўлсада, шартли бўлмаган деб белгиланди.

Ишончсиз UDP протоколи орқали ишлаш (хусусан, SNMP агентлари реализациялари шундай ишлайди) агентлардан менеджерларга авария юборилган хабарлар йўқолишига, шу билан сифатсиз бошқарувга олиб келиши мумкин. Қурилманинг ўрнатилган тармоқларида мавжуд кўп сонли ўрнатилган SNMP агентлари билан бирлаштирилган бир бирини олиб келувчи йўқотишлар бирлашмасини ўрнатиш орқали ишончли транспорт протоколига ўтиш йўли билан тўғирлаш. Бошқарув платформаларини ишлаб чиқувчилар бу камчиликларни енгиб ўтишга ҳаракат қидалилар. Масалан, TMN ва ISO стандартларига мувофиқ равишда кўп даражали бошқарув системларини ишлаб чиқиш учун платформа ҳисобланадиган HP OV Telecom DM TMN платформасида агентлар ва менеджерлар ўртасида SNMP хабарлари йўқолганда уларни мустақил равишда қайта юборишни ташкил қилувчи ишончли хабар алмашинувини таъмиловчи янги SNMP реализацияси ишлайди

4. NetFlow протоколи таҳлили

NetFlow - Cisco томонидан тармоқда трафик мониторинги учун ишлаб чиқилган очиқ истиқболли протоколдир. Netflow ҳар бир TCP/IP транзакция ҳақида ёзиб олиб тармоқ трафигини таҳлил қилиш имконини беради.



Расм 20.3. NetFlow архитектураси тузилиши

Тизимнинг архитектураси сенсор, коллектор ва анализаторга асосланади:

- Сенсор ўзи орқали ўтган трафик бўйича статистика йиғади. Сенсорларни “узел нуқталари” да, масалан, тармоқ сегментлари маршрутизаторлари чегарасида қўйиш самаралидир.

- Коллектор сенсорлардан маълумотларни йиғади. Қабул қилинган файлларни у кейинчалик ишлов бериш учун файлга ташлайди. Турли коллекторлар маълумотларни турли форматларда сақлайди.

- Анализатор, ёки қайта ишлаш тизими бу файлларни ҳисоблайди ва ҳисоботларни одамларга қулай шаклда генерировка қилади. Бу тизим коллектор тақдим қилган маълумотлар билан киришиши керак. Замонавий тизимларда коллектор ва анализатор бир ситемага бирлаштирилган.

Одатда коллектор ва анализатор серверда ишловчи битта дастур комплекси қисмлари ҳисобланади. ПО коллектор/анализатор турлари жуда кўп - пулли ва бепул, Windows ва Unix-тизимлари га асосланган.

Таъкидлаш жоизки, коллектор ва унинг орқасида жойлашган анализатор тизимнинг пассив элементлари ҳисобланади. Моҳиятан, сервер кўтарилган бўлса, мониторингга ва серверга тушадиган қурилмаларни қўлда қўшишимиз шарт эмас. Сенсор ҳисоботларни юборади, коллектор уларни қабул қилади, анализатор рўйхатдан ўтказади. Агар сенсор ўчирилган бўлса, у жорий онлайн-статистикадан йўқолиб қолади.

NetFlow трафик коллектори тўғрисидаги маълумотларни юбориш учун UDP ва SCTPдан фойдаланади. Одатда, коллектор 2055, 9555 ёки 9995 (ёки сиз коллектор ва сенсор қурилмасида кўрсатадиган) портларини тинглайди. Сенсор қуйидаги параметрлар билан характерланадиган трафикдан ўтаётган

оқимларни ажратади:

1. Манба манзили;
2. Топшириқ манзили;
3. UDP ва TCP манзил порт;
4. UDP ва TCP учун порт топшириғи;
5. ICMP учун хабар коди ва тури;
6. IP протокол рақами;
4. Тармоқ интерфейс (ifindex SNMP параметр);
5. IP Type of Service.

NetFlow - CiscoSystems компанияси томонидан ишлаб чиқилган тармоқ трафигини ҳисоблаш учун мўлжалланган тармоқ протоколидир. Асосланган саноат стандарти ҳисобланади ва нафақат Cisco қурилмаси томонидан, балки бошқа кўплаб қурилмалар томонидан қўллаб қувватланади (хусусан, Juniper, MikroTik ва Enterasys). Шунингдек, . UNIX га ўхшагаи тизимлар учун мустақил реализациялар ҳам мавжуд. Протокотнинг бир неча версиялари мавжуд бўлиб, 2011-йилда 5 ва 9 версиялари кенг тарқалди. 9 версия асосида, шунингдек IPFIX (InternetProtocolFlowInformationeXport IP оқимлари тўғрисида экспорт информацияси).

Оқим деб - бир йўналишда ўтадиган пакетлар тўпламига айтилади. Сенсор оқим тугаганини аниқлаганда, (пакет параметрлари ўзгаргани ёки TCP - сессия ишдан чиқиши билан) у маълумотни коллекторга юборади. Қурилмаларга боғлиқ тарзда, у, шунингдек, коллекторга ҳалиям давом этаётган оқимлар ҳақидаги маълумотни вақти-вақти билан юбориши мумкин. Бу жуда муҳимдир – сенсор ққурилмасида биз қайси параметрлар бўйича юборилган маълумот ҳисоботларда бирлаштирилишини қарор қиламиз.

Протокол рақами версияи;

1. Ёзиб олиш рақами;
2. Кирувчи ва чиқувчи тармоқ интерфейси;
3. Оқим бошланиши ва тугаши вақти;
4. Оқимда байт ва пакетлар миқдори;
5. Манба ва топшириқ манзили;
6. Манба ва топшириқ манзили;
7. IP протоколи рақами;
8. Type of Service миқдори;
9. TCP-боғланишлар учун — флага боғланиши давомидаги барча кузатувлар;
10. Шлюза манзили;
11. Манба ва топшириқ манзили.

Агар сенсор сифатида тармоқ қурилмаси келса, NetFlow ресурсларини тежаш мақсадида асосий статистика йиғишни исталган интерфейслар учун қўшилади.

Процессор ресурсларини тежаш мақсадида, шунингдек «sampledNetFlow»

қўлланилади. Бундай вазиятда сенсор ҳамма эмас, балки ҳар бир n-пакетни таҳлил қилади, бунда n административ ёки тасодифий тарзда белгиланган бўлиши мумки. sampledNetFlow қўлланилганда олинган миқдорлар аниқ эмас, баҳоловчи бўлади.

Назорат саволлари

1. SNMP протоколи ривожланиш тарихи.
2. SNMP бошқарув асослари.
3. SNMP протоколи камчиликлари.
4. NetFlow протоколи таҳлили.
5. Юқори даражадаги бошқарув объектлари тизими.
6. Оддий роутер ёрдамида бошқариш протоколи.
7. Умумий бошқарув маълумот протоколи

Адабиётлар ва интернет ресурслар

1. Computer networking : a top-down approach / James F. Kurose, Keith W. Ross.—6th ed. 2013. by Pearson Education, Inc., publishing as Addison-Wesley.
2. TCP/IP protocol suite / Behrouz A. Forouzan.—4th ed. Published by McGraw-Hill, a business unit of The McGraw-Hill Companies, Inc., 1221 Avenue of the Americas, New York, NY 10020. Copyright © 2010
3. Java Network Programming, Fourth Edition by Elliotte Rusty Harold. 2014. Published by O'Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol.
4. The Definitive Guide to Linux Network Programming Copyright © 2004 by Keir Davis, John W. Turner, Nathan Yocom. 2011.
5. Keir Davis. TCP/IP Network Programming Design Patterns in C++. Vic Hargrave. 2013.