UOT 004.046

Şıxəliyev R.H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

KOMPYUTER ŞƏBƏKƏLƏRİNİN MONİTORİNQİ ÜSULLARI VƏ VASİTƏLƏRİ HAQQINDA

Məqalədə şəbəkə monitorinqi məsələlərinin və kompyuter şəbəkələrinin monitorinqinin həyata keçirilməsinin müxtəlif üsullarının və vasitələrinin analizi verilmişdir.
Açar sözləri: *şəbəkə monitorinqi, şəbəkə trafiki, şəbəkə avadanlıqları, şəbəkə indikatorları, passiv monitorinq, aktiv monitorinq.*

Giriş

Bu gün kompyuter şəbəkələri (KŞ) informasiya texnologiyalarının ən dinamik inkişaf edən sahələrindən biridir. KŞ-in funksional imkanları genişlənir, miqyası böyüyür və onlarda istifadə edilən şəbəkə xidmətlərinin, avadanlıqlarının sayı artır. Bununla yanaşı, informasiya mübadiləsi proseslərinin qloballaşması, multimedia tətbiqlərinin geniş istifadəsi, KŞ-in tətbiq sahələrinin genişlənməsi (məsələn, son zamanlar insanlar şəxsi və korporativ əlaqələrini, bank işlərini, ticarət işlərini və s. daha çox KŞ-in vasitəsi ilə həyata keçirirlər) bu şəbəkələr vasitəsi ilə ötürülən trafikin həcminin həddindən artıq böyüməsinə gətirib çıxarır.

Bütün bunlar KŞ-in idarə edilməsi, təhlükəsizliyinin təmin edilməsi və inkişafının proqnozlaşdırılması məsələlərini aktuallaşdırır və şəbəkə inzibatçılarının KŞ-in effektli idarə edilməsi üçün qəbul etdikləri qərarlara görə məsuliyyətini həddindən çox artırır. Əksər hallarda inzibatçılar KŞ-in idarə edilməsi ilə bağlı qərarları onun tam vəziyyəti haqqında informasiyanın qıtlığı və ya KŞ-də baş verən problemlərin analizi üçün vaxtın məhdudluğu şəraitində qəbul edirlər. Nəticədə, KŞ-in daim işlək vəziyyətinin təmin edilməsi və xidmət keyfiyyətinin lazımi səviyyədə saxlanılması çətinləşir. KŞ-in aparat və ya proqram təminatlarında baş verən nasazlıqlar, çox vacib şəbəkə xidmətlərinin işinin sürətinin aşağı düşməsi və hətta dayanması xoşagəlməz nəticələrə gətirib çıxara bilər. Məsələn, marşrutlayıcıların işində baş verən nasazlıqlar və onun işinin pozulması KŞ-in müxtəlif seqmentləri arasında əlaqənin pozulmasına gətirib çıxara bilər.

Bütün yuxarıda deyilənləri nəzərə alaraq qeyd etmək lazımdır ki, müasir KŞ-in vəziyyəti daim nəzarətdə saxlanılmalıdır və bunun üçün müntəzəm olaraq şəbəkə monitorinqi aparılmalıdır. Bu baxımdan, KŞ-də monitorinq sisteminin istifadəsi, onun normal fəaliyyətinin təmin edilməsi böyük əhəmiyyətə malikdir. Çünki KŞ-in normal fəaliyyətinin təmin edilməsi mürəkkəb və böyük maddi vəsait tələb edən məsələdir. Bu məsələnin həlli çoxlu sayda müxtəlif ixtisaslı informasiya texnologiyaları (İT) mütəxəssislərin cəlb edilməsi hesabına mümkündür. Həmin mütəxəssislər şəbəkə xidmətlərinin əlyetərliliyini təmin etməli, şəbəkənin işini optimallaşdırmalı, şəbəkə aparat və proqram təminatını tənzimləməli və yeniləşdirməli, şəbəkədə baş verən insidentləri aşkar edərək onları aradan qaldırmalıdır. Lakin bu hal həm iqtisadi, həm də fiziki cəhətdən əlverişli deyi, xüsusilə də böyük KŞ-də. Çoxlu sayda İT mütəxəssislərinin əvəzinə müxtəlif xüsusiləşdirilmiş proqram və aparat vasitələri, şəbəkə monitorinqi və idarəetmə sistemlərindən istifadə etmək olar.

Buna görə də hazırda KŞ-in monitorinqi üçün müxtəlif istehsalçılar tərəfindən yaradılmış şəbəkə monitorinqi sistemləri və üsullarından istifadə edilir. Mövcud şəbəkə monitorinqi sistemləri geniş funksional imkanlara malik olmasına baxmayaraq, KŞ-in idarə edilməsi prosesi mürəkkəb olaraq qalır və şəbəkə inzibatçısından lazımi səviyyədə bilik, təcrübə və əmək tələb edir.

Şəbəkə monitorinqinin məqsədi və məsələləri

Şəbəkə monitorinqi – xüsusi proqram vasitələrinin köməyi ilə KŞ-in fəaliyyətinə daimi nəzarət prosesidir. Şəbəkə monitorinqi sistemləri KŞ-də kompyuterlərin (hostların) və şəbəkə xidmətlərinin daimi fəaliyyətini və əlyetərliliyini təmin etməyə imkan verir. Bu sistemlər elektron poçt, mobil telefon və s. vasitəsi ilə şəbəkə izibatçısını şəbəkədə baş verən nasazlıqlar, dayanmalar, təhlükələr haqqında xəbərdar edir.

Şəbəkə monitorinqi KŞ-in idarə edilməsi üçün lazım olan informasiyanın toplanması funksiyasını yerinə yetirir. Bu monitorinq şəbəkə və şəbəkə idarəetməsinə dair tətbiqi proqramlar üçün verilənlərin toplanması məqsədilə yaradılmışdır. KŞ optimal qurulsa da, serverlərdə və istifadəçi kompyuterlərində etibarlı proqram təminatı tətbiq edilsə də, onun vəziyyətinə avtomatik və fasiləsiz nəzarət etmək vacibdir.

Müasir KŞ-in miqyası böyük olduğu üçün bir neçə seqmentə bölünür və əksər şəbəkə avadanlıqları KŞ-in müxtəlif hissələrində (seqmetlərində) yerləşir. Adətən bu avadanlıqların birbaşa birləşmiş terminalları olmadığı üçün, tətbiqi idarəetmə proqramları onların vəziyyətinin monitorinqini apara bilmir. Bu səbəbdən də KŞ-in şəbəkə avadanlıqlarının vəziyyətinin yoxlanılması üçün xüsusi şəbəkə monitorinqi üsulları və vasitələri yaradılmışdır.

Şəbəkə monitorinqinin məqsədi KŞ-in idarə edilməsi üçün lazımi informasiyanın şəbəkənin müxtəlif hissələrindən toplanmasını və istifadəsini təmin etməkdir. Bu məqsədə uyğun olaraq monitorinq aşağıdakı istiqamətlərdə həyata keçirilir:

- şəbəkə məhsuldarlığının monitorinqi;
- şəbəkə səhvlərinin monitorinqi;
- şəbəkədən istifadənin monitorinqi.

Bu istiqamətlər KŞ-in idarə edilməsi üçün *OSI* (*Open Systems Interconnect*) tərəfindən təklif edilmiş beş funksional sahəyə aiddir. Digər iki sahə şəbəkə monitorinqinin məqsədi ilə bağlı deyildir – onlar şəbəkə konfiqurasiyasının və təhlükəsizliyin idarə edilməsi ilə əlaqədardır.

Şəbəkə məhsuldarlığının monitorinqi KŞ-in məhsuldarlığının qiymətləndirilməsini həyata keçirir. Bu istiqamət üzrə monitorinqlə bağlı, əsasən üç problem mövcuddur. Birincisi, şəbəkə məhsuldarlığının monitorinqi nəticəsində toplanılmış informasiya, adətən KŞ-in gələcək genişləndirilməsinin planlaşdırılması və şəbəkədən istifadənin cari problemlərinin müəyyən edilməsi üçün istifadə edilir. İkincisi, şəbəkə məhsuldarlığı monitorinqinin müddəti kifayət qədər böyük olmalıdır ki, şəbəkənin fəaliyyət modeli müəyyən edilsin. Üçüncüsü, optimal nəticə əldə etmək üçün qiymətləndirmə üsulunun seçilməsi mühüm əhəmiyyət daşıyır.

KŞ-də qiymətləndirilməsi vacib olan çoxlu sayda parametrlər vardır [1]. Lakin bu şəbəkə parametrlərinin siyahısının müəyyən edilməsi zamanı onların vacibliyi və iqtisadi səmərəliliyi nəzərə alınmalıdır. Qiymətləndirilən şəbəkə parametrləri onun xüsusiyyətlərini təsvir edir və Parametrlərin siyahısı şəbəkə indikatorları adlanır. (Şəbəkə indikatorlarının siyahısı Cədvəl 1-də göstərilmişdir.)

Şəbəkə səhvlərinin monitorinqi KŞ-də baş verən səhvlərin müəyyən edilməsi üçün həyata keçirilir. Şəbəkədə baş verən səhvlərin monitorinqi ilə bağlı, əsasən iki problem mövcuddur. Birincisi, şəbəkə səhvlərinin monitorinqi şəbəkənin müxtəlif səviyyələrində həyata keçirilir, çünki şəbəkənin müxtəlif səviyyələrində problem baş verə bilər. Buna görə də problemin baş verdiyi şəbəkə səviyyəsinin müəyyən olunması vacibdir. İkincisi, şəbəkə səhvlərinin monitorinqi uzun müddətə qəbul edilmiş normal şəbəkə xarakteristikalarının olmasını tələb edir. KŞ-də həmişə səhvlər olur, lakin səhvlərin olması həmişə problemin olması demək deyil. Bu səhvlərdən bəzilərinin həmişə baş verməsi gözlənilir. Məsələn, şəbəkənin əlaqə kanallarında olan küylər informasiyanın ötürülməsi zamanı səhvlərin meydana çıxmasına səbəb ola bilər. KŞ-də o zaman problem baş verir ki, səhvlərin sayı birdən-birə həddindən çox artır və onun normal fəaliyyəti pozulur. Buna görə də, KŞ-in normal fəaliyyəti haqqında qeydiyyatın aparılması vacibdir.

Cədvəl 1

Şəbəkə indikatorlarının siyahısı

Şəbəkə indikatorları	**Təsviri**
Əlaqə kanallarının əlyetərliliyi	İstifadəçilərin şəbəkəyə qoşulması və şəbəkə əlaqələrinin əlyetərliliyinin faktiki müddəti
Qovşaqların əlyetərliliyi	İstifadəçilərin şəbəkə qovşaqlarından səhvsiz istifadəsinin faktiki müddəti
Təcridetmə əmsalı	Şəbəkəyə daxil ola biməyən istifadəçilərin say;
Cavab müddəti	Siqnalın göndərilməsi və cavabın alınması müddəti

Şəbəkədən istifadənin monitorinqi istifadəçilərin şəbəkədən necə istifadə etdiklərini müəyyən etməyə imkan verir. Həmin monitorinq KŞ istifadəçilərinin hansı şəbəkə avadanlıqlarını və necə istifadə etməsi ilə bağlı qeydiyyat aparır. Bu informasiya istifadəçilərin şəbəkədən istifadə profilini müəyyən etməyə və gələcəkdə baş verəcək hərəkətlərini proqnozlaşdırmağa imkan verir.

Şəbəkə monitorinqi sahəsinə aid digər bir vacib məsələ şəbəkə trafikinin ölçülməsidir. Şəbəkə trafikinin ölçülməsi – KŞ-in müxtəlif tipli trafikinin ölçülməsi və toplanmasıdır. Bu, əsasən KŞ-in buraxılış zolağının idarə olunması üçün vacibdir.

Şəbəkə monitorinqi aşağıdakı şəbəkə komponentlərinin vəziyyətini və fəaliyyətini analiz etməyə imkan verir:

- şəbəkə avadanlıqları;
- şəbəkə əlaqələri;
- şəbəkə trafiki;
- şəbəkə xidmətləri;
- şəbəkə istifadəçilərinin fəaliyyəti (şəbəkə resursundan istifadənin uçotu)
- və s.

Qeyd etmək lazımdır ki, əvvəlcədən planlaşdırılmadıqda, KŞ-in (xüsusilə də böyük KŞ-in) monitorinqi çox mürəkkəb məsələyə çevrilir. Buna görə də KŞ-də monitorinqin aparılması üçün şəbəkə avadanlıqları, tətbiqi proqramlar, resurslar və xidmətlər əvvəlcədən müəyyən edilməlidir.

Əlbəttə, KŞ-in monitorinqinin ən yaxşı strategiyası bütün şəbəkə avadanlıqlarının, tətbiqi proqramların, resursların və xidmətlərin monitorinq edilməsi olardı. Lakin bu halda monitorinq prosesinin özü çox böyük xidməti trafik generasiya edə bilər və böyük sistem resurslarından istifadə edər və nəticədə KŞ-in işinin pozulmasına gətirib çıxarar.

Buna görə də, adətən KŞ-in ancaq əsas və ya kritik avadanlıqlarının, məsələn, serverlərin, marşrutlayıcıların, kommutatorların, habların və şəbəkələrarası ekranların monitorinqi həyata keçirilir. Bundan başqa, digər avadanlıqların, məsələn, işçi stansiyaların, terminalların və s. monitorinqi həyata keçirilə bilər. Həmçinin qarşıya qoyulmuş məsələlərdən asılı olaraq, KŞ-in monitorinqi üçün üsulların və vasitələrin seçilməsi də çox vacibdir.

Adətən şəbəkə monitorinqi aşağıdakı məsələləri həll etməyə imkan verir:

- KŞ-in vəziyyətinə nəzarət;
- Verilən buraxılış zolağının optimal istifadəsi;
- Anomal aktivliyin və hücumların aşkarlanması;
- Qeyri-qanuni xidmətlərin və serverlərin aşkarlanması;
- İstifadəçilərin aktivliyinin analizi;
- Şəbəkə protokollarının analizi;
- Şəbəkə avadanlıqlarının parametrlərinin optimallaşdırılması;
- KŞ-dəki nasazlıqların aşkarlanması;
- KŞ-in işinin təşkil edilməsi üzrə qərarların qəbul edilməsi üçün verilənlərin əldə edilməsi və s.

Şəbəkə monitorinqi məsələlərini optimal və effektli şəkildə reallaşdırmaq üçün müəyyən modelin olması vacibdir. Bunun üçün Beynəlxalq Telekommunukasiya İttifaqı (BTİ) şəbəkə idarəetməsi və monitorinqinə dair proqram təminatlarının əsas funksiyalarının reallaşdırılmasına dair şəbəkə idarəetmə modeli təklif etmişdir. Bu idarəetmə modeli BTİ-nin *X 700* sənəddə öz əksini tapan tövsiyələrinin tərkib hissəsidir və *ISO/OSI (Open Systems Interconnection)* modelinə əsaslanır. Bu model beş əsas sahəni əhatə edir: iş qabiliyyətinin idarə olunması, konfiqurasiyanın idarə olunması, şəbəkə resurslarının uçotu, nasazlıqların idarə olunması və təhlükəsizliyin idarə olunması.

İş qabiliyyətinin idarə olunması KŞ-in cari və gözlənilən iş qabiliyyətlərini nəzərdə tutur. KŞ-in iş qabiliyyətinin montorinqi üçün *CAIDA Metrics Working Group* və *IETF's IP Performance Metrics* ölçmə üzrə işçi qrupları tərəfindən müəyyən indikatorlar təklif edilmişdir [4].

CAIDA Metrics Working Group tərəfindən təklif edilən indikatorlar (metrikalar) aşağıdakılardır:

- latentlik;
- paketin itirilməsi;
- buraxma qabiliyyəti;
- əlaqənin istifadəsi;
- əlyetərlilik.

Konfiqurasiyanın idarə olunmasının məqsədi KŞ-in həm aparat, həm də proqram təminatının konfiqurasiyasının izlənməsidir. Buraya hər bir şəbəkə avadanlığının hansı versiya proqram təminatı ilə idarə edilməsi və həmçinin hər bir avadanlığın proqram təminatının konfiqurasiyası daxildir.

Şəbəkə resurslarının uçotu şəbəkə aktivlərinə nəzarəti və keyfiyyətin idarə edilməsi kimi iki geniş sahəni əhatə edir. Şəbəkə aktivlərinə nəzarət, şəbəkədəki kompyuterləri və onların kimə məxsus olmasını, həmçinin kimin istifadə etməsini və harada yerləşməsini müəyyən edir.

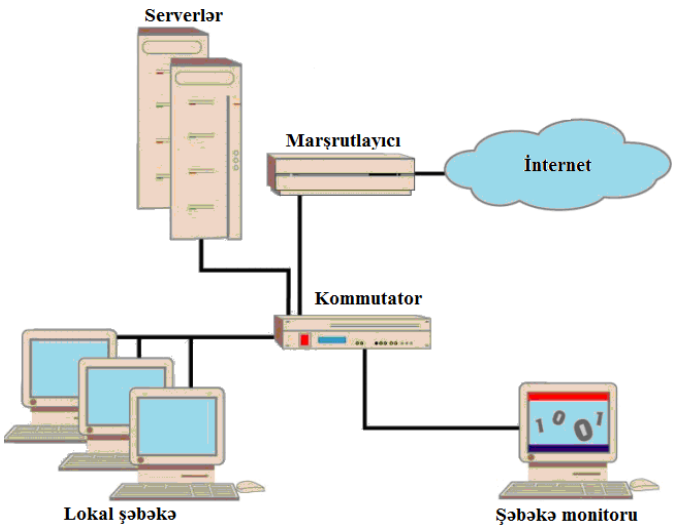
Nasazlıqların idarə olunmasının məqsədi KŞ-də problemlərin və səhvlərin aşkarlanmasıdır. Bu cür səhvlər qeyd olunmalıdır və uyğun həyacan siqnalı verilməlidir. Bu sahə problemin identifikasiyasına, səhvlərin səbəbinin müəyyən edilməsinə və lazımi tədbirlərin görülməsinin təmin edilməsinə cavabdehdir.

Təhlükəsizliyin idarə olunması özündə təhlükəsizlik siyasəti ilə müəyyən edilmiş, orijinallığın təyin edilməsi və girişin idarə olunması aspektlərini birləşdirir.

Şəbəkə monitorinqi məsələləri proqram və aparat vasitələrinin, şəbəkə analizatorlarının, kommunikasiya avadanlıqlarına yerləşdirilmiş monitorinq vasitələrinin, həmçinin şəbəkə idarəetmə sisteminin agentlərinin köməyi ilə həyata keçirilir. Monitorinqin nəticələrinin analizi məsələsinin həlli üçün isə insanın daha aktiv iştirakı və çoxlu sayda şəbəkə mütəxəssislərinin praktiki təcrübəsini özündə cəmləşdirən mürəkkəb ekspert sistemlərindən istifadə etmək tələb olunur.

Adətən KŞ-in monitorinqi bir neçə sxem üzrə həyata keçirilir [5]. KŞ haqqında ətraflı məlumat əldə etmək üçün xüsusi monitorinq serverinin bütün nəzarət olunan şəbəkə obyektlərinə girişi olmalıdır. Həmçinin KŞ ilə İnternet arasındakı əlaqənin monitorinqi üçün monitorinq serveri marşrutlayıcıdan keçən trafikə nəzarət etməlidir.

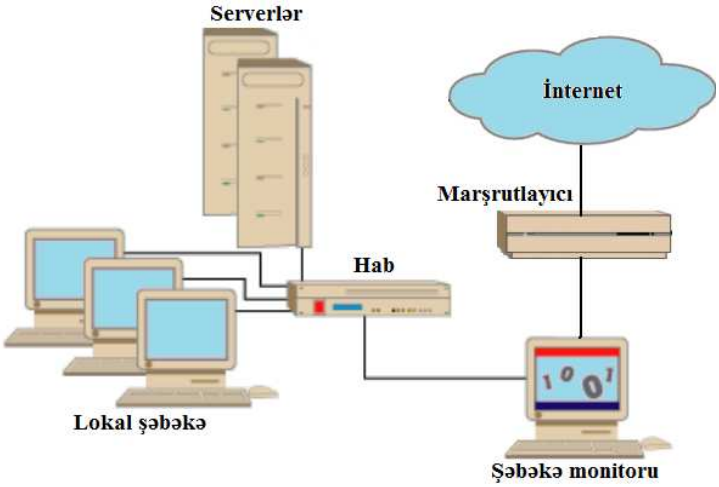
KŞ-in monitorinqi üçün, adətən monitorinq serveri kommutatorun monitorinq portuna qoşulur (Şəkil 1).



Şəkil 1. Monitorinq serverinin kommutatorun montorinq portuna qoşulması sxemi

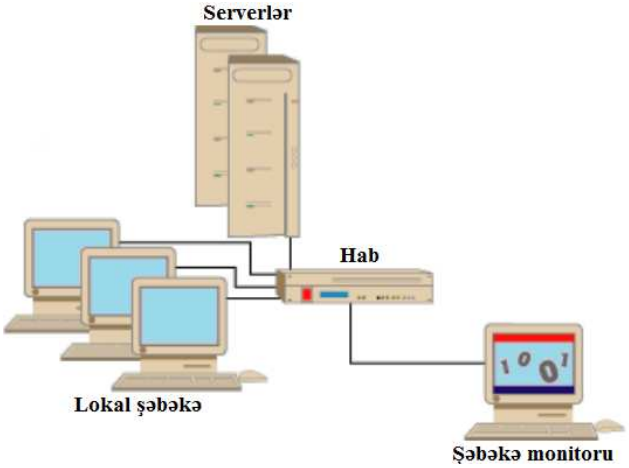
Əgər KŞ-də bir neçə kommutator istifadə edilərsə, onda monitorinq serveri onların hər birinin monitorinq portuna qoşulmalıdır. Bu zaman əlaqə ya fiziki kabel, ya da virtual kanal vasitəsi ilə həyata keçirilə bilər.

Kommutatorların monitorinq portu əlyetərli olmadığı halda, monitorinq serveri KŞ-in İnternetlə birləşmə nöqtəsində yerləşdirilə bilər və bu halda monitorinq serveri KŞ ilə İnternet arasında baş verən bütün trafikə nəzarət edir (Şəkil 2).



Şəkil 2. Monitorinq serverinin KŞ ilə İnternet arasında yerləşdirilməsi sxemi

Lakin bu halda xüsusi monitorinq serverində yaranan problemlər şəbəkə üçün dayanma təhlükəsi yarada bilər. Həmçinin xüsusi monitorinq serverinin imkanları şəbəkənin ötürmə qabiliyyətinə olan tələblərə cavab vermədikdə "butulka boğazı" problemi meydana çıxa bilər. Bu problemin ən yaxşı həlli xüsusi monitorinq serverini daxili şəbəkə ilə birləşdirən sadə habdan istifadə edilməsidir. (Şəkil 3).



Şəkil 3. Monitorinq serverinin haba qoşulması sxemi

Bu halda isə habın sıradan çıxması şəbəkə üçün dayanma təhlükəsi yaradır. Lakin hablar marşrutlayıcılara nisbətən daha etibarlıdır və onlar sıradan çıxdıqda işlək hablara dəyişdirilməsi daha asan və sadədir.

Şəbəkə monitorinqi üsulları

KŞ-in monitorinqi zamanı monitorinq verilənlərinin əldə edilməsi, əsasən iki üsulla - aktiv və passiv monitorinq üsulu [6, 7, 8] ilə həyata keçirilir və onların müqayisəsi Cədvəl 2-də verilmişdir.

Aktiv şəbəkə monitorinqi – şəbəkəyə əlavə test paketlərinin daxil edilməsi nəticəsində toplanmış verilənlərin analizinə əsaslanır. Əsasən, *ping* (şəbəkələrə qoşulmanın yoxlanılması üçün nəzərdə tutulan kompyuter proqramı), *traceroute* (şəbəkələrdə məlumatların izlənilməsi marşrutlarının müəyyən edilməsi üçün nəzərdə tutulan xidməti kompyuter proqramı), *pathchar* (şəbəkələrdə buraxılış imkanlarını, gecikmələri müəyyən etməyə və s. imkan verən kompyuter proqramı), ICMP (**Internet Control Message Protocol** - Şəbəkələrarası Məlumat İdarəetmə Protokolu) vasitələrinin köməyi ilə həyata keçirilir.

Cədvəl 2

Şəbəkə monitorinqi üsullarının müqayisəsi

	Aktiv monitorinq	**Passiv monitorinq**
Forması	Çoxnöqtəli	Bir və ya çoxnöqtəli
Verilənlərin həcmi	Kiçikdir	Böyükdür
Yerinə yetirilməsi	Əlavə trafik	Proqram, proqram-aparat təminatı
Məqsədi	Ləngimə, paketlərin itməsi, iş qabiliyyəti	Səmərəlilik, trafikin parametrləri, meyllər və aşkarlama
CPU tələblər	Orta aşağı	Yüksək

Aktiv monitorinq sistemləri aşağıdakı metrikaları ölçür:

- əlyetərlilik;
- latentlik;
- paketin itirilməsi;
- buraxılış qabiliyyəti;
- əlaqənin istifadəsi;
- və s.

Passiv şəbəkə monitorinqi aktiv şəbəkə trafikindən toplanmış verilənlərin (loq-faylların) analizinə əsaslanır. Əsasən, *polling* (qurğuların hazırlıq səviyyəsinin sorğu edilməsi), *event reporting* (hadisələr haqqında hesabat), *sniffing* (şəbəkə trafikinin passiv dinlənilməsi), *SNMP* (*Simple Network Management Protocol* – Sadə Şəbəkə İdarəetmə Protokolu), *RMON (Remote Network Monitoring*, Kompyuter Şəbəkələrinin Monitorinq Protokolu), *NetFlow* (Şəbəkə trafikinin qeydiyyatı üçün nəzərdə tutulan şəbəkə protokolu) vasitələrinin köməyi ilə həyata keçirilir [9, 10, 11].

Aktiv monitorinqdən fərqli olaraq passiv şəbəkə monitorinqi zamanı KŞ-ə test paketləri əlavə olunmur və buna görə də KŞ-in trafikinə heç bir dəyişiklik edilmir. Həmçinin aktiv monitorinqdən fərqli olaraq passiv monitorinq KŞ-in bir nöqtəsindən (məsələn, marşrutlayıcıdan, kommutatordan və ya habdan) həyata keçirilir və nəzarət olunan nöqtədən keçən trafikdən verilənləri toplayır.

Passiv şəbəkə monitorinqi istənilən *sniffer* proqramı vasitəsi ilə həyata keçirilə bilər. Passiv şəbəkə monitorinqi əsasında toplanmış verilənlər daha sonra analiz olunur. Bu zaman ortaya çıxan əsas problemlərdən biri böyük həcmdə verilənlərin emalı ilə bağlıdır. Buna görə də hər iki monitorinq üsulundan kombinə edilmiş şəkildə istifadə olunması daha effektlidir.

Passiv şəbəkə monitorinqi sistemi, əsasən üç hissədən ibarət olur: monitorinq nöqtəsi, verilənlərin toplanması və analizi nöqtələri. Əgər şəbəkənin monitorinqi üçün bir kompyuterdən istifadə edilirsə, onda bu hissələr həmin kompyuterdə yerləşə bilər. Bəzən passiv şəbəkə monitorinq sistemi daha geniş olur və beş hissəyə bölünür. Bunlara trafikin (paketlərin) toplanmasını, onun (onların) ilkin emalını, statistik göstəricilərin müəyyən edilməsini, statistik göstəricilərin toplanmasını və emalını aid etmək olar.

Şəbəkə monitorinqi zamanı trafikin toplanması və analizi prosesi aşağıdakı mərhələlərdən ibarət olur:

- Şəbəkə paketləri nəzarət nöqtəsində əldə edilir (adətən, serverdə, marşrutlayıcıda və yaxud şəbəkənin istənilən nöqtəsində yerləşən kompyuter vasitəsi ilə əldə edilir);
- Paketlər seçilir və süzülür (məsələn, protokollara, şəbəkə xidmətlərinə, portlara və s. görə). Seçim mərhələsi həmişə tətbiq edilir və yaxud hər ikisi bir neçə dəfə tətbiq edilə bilər;
- Paketlər klassifikasiya edilir və axın yazıları kimi təsvir edilir;
- Axın yazıları seçilir və süzülür. Seçim mərhələsi həmişə tətbiq edilir və yaxud hər ikisi bir neçə dəfə tətbiq edilə bilər;
- Axın yazıları tətbiqi proqramlarda emal edilir (hücumların analizi, DoS-un monitorinqi, vizuallaşdırma (FlowScan), toplama (TCPdump), əks etdirmə və s.).

Şəbəkə monitorinqi üçün istifadə edilən ən geniş yayılmış protokollardan biri *PING* (*Packet Internet Groper*) protokoludur. *PİNG* İnternet paketlərinin göndəricisi olaraq, KŞ-dəki verilmiş hosta (kompyuterə) test paketlərini göndərir və cavab paketlərini alır.

PİNG 1983-cü ildə Unix platforması üçün yaradılmışdır və sonra isə digər platformalara keçirilmişdir, nəticədə KŞ-in monitorinqinin standart vasitəsinə çevrilmişdir [12]. Əsas məqsəd KŞ-in avadanlıqları ilə əlaqənin olub-olmamasının yoxlanılmasıdır. Bu zaman paketlərin göndərilməsinə və şəbəkə avadanlıqları tərəfindən test paketlərinin təsdiqlənməsinə sərf edilən vaxt müəyyən edilir. Bunun nəticəsində onların hazırlığı və əlyetərliliyi təyin olunur. Bu yoxlama əsasında şəbəkənin latentlik və əlyetərlilik xüsusiyyətlərini asanlıqla yoxlamaq mümkündür.

Şəbəkə monitorinqi vasitələri

Hazırda şəbəkə inzibatçılarına geniş seçim imkanı verən çoxlu sayda müxtəlif şəbəkə monitorinqi vasitələri mövcuddur [13]. Bununla belə, monitorinq vasitələrinin müxtəliflliyi seçim prosesini çox çətinləşdirir. Şəbəkə inzibatçılarının KŞ-in fəaliyyətinin sabitliyini və əlyetərliliyini təmin etmək üçün, effektli şəbəkə monitorinqi və analizi vasitələrinə ehtiyac

duyurlar. Mövcud şəbəkə monitorinqi vasitələrində SNMP protokolu, WMI (Windows Management Instrumentation), sniffer və Netflow şəbəkə monitorinqi və analizi üsullarından istifadə edilir.

KŞ-in lazımi və effektiv monitorinqi üçün əvvəlcə monitorinq vasitəsi seçilməlidir. Mövcud monitorinq vasitələrini funksiyalarından asılı olaraq müxtəlif siniflərə bölmək olar:

- Seçim əsasında yoxlama aparan monitorinq vasitələri - KŞ-də nasazlıqların tapılması və aradan qaldırılması üçün nəzərdə tutulmuşdur.

Bu vasitələr interaktiv rejimdə işləyir və qısa müddətə işə salınır (misal olaraq, ping proqramını göstərmək olar). Ping seçilmiş hostlarla əlaqəni yoxlamaq üçün ona test trafiki göndərir.

- Şəbəkədəki hər bir paketi yoxlayan və bütün birləşmələr haqqındakı məlumatı toplayan (məsələn, məlumat göndərənin və alanın İP-ünvanları, protokollar haqqında informasiyanı və hətta tətbiq səviyyəsinin məlumatlarını da toplayır) protokol analizatorları.
- Meylləri aşkarlayan monitorinq vasitələri - uzun müddət fon rejimində monitorinq aparır və nəticəni, adətən qrafik şəklində ifadə edir.

Real zamanda monitorinq aparan vasitələr meylləri aşkarlayan vasitələrə oxşar şəkildə monitorinq aparır və problem aşkarlayan kimi, dərhal şəbəkə inzibatçısına xəbər verir.

- Loq-analiz vasitələri - müxtəlif proqramların loq-fayllarını analiz edir və problem aşkar etdikdə şəbəkə inzibatçısına xəbər verir.
- Müdaxilələrin aşkarlanması vasitələri - şəbəkə trafikini analiz edir və anomal hadisələr, hücum cəhdləri aşkarladıqda müvafiq əməliyyatı həyata keçirir (adətən, girişi qadağan edir və ya inzibatçını məlumatlandırır).
- Etalon testləşdirmə vasitələri - şəbəkə xidmətlərinin və ya şəbəkə birləşmələrinin məhsuldarlığını qiymərləndirməyə imkan verir.
- Kabel sisteminin diaqnostikası və sertifikatlaşdırılması avadanlıqları.

Şərti olaraq bu avadanlıqları dörd əsas qrupa bölmək olar: şəbəkə monitoru, kabel sistemlərinin sertifikatlaşdırılması cihazları, kabel skanerləri və testerləri (multimetrlər)-şəbəkə monitorları (həmçinin şəbəkə analizatorları adlandırılır) müxtəlif kateqoriyalı kabellərin test edilməsi üçün nəzərdə tutulmuşdur.

Şəbəkə monitorlarını və protokol analizatorlarını fərqləndirmək vacibdir. Belə ki, şəbəkə monitorları trafikin ancaq statik göstəriciləri haqqında məlumatı toplayır. Bu göstəricilərə şəbəkə trafikinin ümumi orta intensivliyi, müəyyən növ səhvlərə malik paketlərin orta intensivliyi və s. aiddir.

Kabel sistemlərinin sertifikatlaşdırılması qurğularının təyinatı birbaşa adından məlum olur. Sertifikatlaşdırma kabel sistemlərinə dair beynəlxalq standartın tələblərinə uyğun aparılır. Kabel skanerləri kabel sistemlərinin diaqnostikası üçün istifadə edilir. Testerlər isə kabellərdə baş verən fiziki qırılmaların yoxlanması üçün nəzərdə tutulmuşdur.

- Ekspert sistemləri - şəbəkədə baş verən anomal halların aşkarlanması və şəbəkənin işçi vəziyyətinə gətirilməsinin mümkün üsulları haqqında mütəxəssis biliklərini özündə cəmləyir.

Ekspert sistemləri çox zaman müxtəlif şəbəkə monitorunda analiz vasitələrinin altsistemi şəklində realizə edilir. Ekspert sistemlərinin sadə variantı kontekst-asılı help-sistemdir. Daha mürəkkəb ekspert sistemi "biliklər bazası" adlanır və süni intellekt elementlərinə malikdir. Belə sistemlərə misal olaraq *Cabletron* şirkətinin *Spectrum* idarəetmə sisteminə qoşulmuş ekspert sistemini göstərmək olar [14].

Cədvəl 3-də bəzi şəbəkə monitorinqi vasitələrinin verilənlərin əldə edilməsi və analizi üsullarına, analiz sahəsinə (*ISO/OSI* modeli), arxitekturuna və istifadəçi interfeysinə görə müqayisəsi verilmişdir.

Cədvəl 3

Bəzi şəbəkə monitorinqi vasitələrinin müqayisəsi

Vasitələr	**Verilənlərin əldə edilməsi üsulu**	**Verilənlərin analizi üsulu**	**Analiz sahəsi (ISO/OSI modeli)**	**Paylanmış arxitektura**	**İstifadəçi iterfeysi**
Tcpdump	libpcap	real zamanda	7-ci səviyyə	yox	Text
Ntop	libpcap	seriya	7-ci səviyyə	yox	Web
Ethereal	libpcap	real zamanda, seriya	7-ci səviyyə	yox	X-Windows
MRTG	snmp agent	seriya	2-ci səviyyə	hə	Web
WebTraf Mon	libpcap	real zamanda, seriya	7-ci səviyyə	yox	Web

Şəbəkə monitorinqinin qarşısına qoyulan məsələdən asılı olaraq bu və ya digər vasitədən istifadə edilir. Misal üçün, şəbəkə inzibatcıları şəbəkələrarası ekranları testləşdirmək və ya trafiki tədqiq etməklə problemləri müəyyən etmək üçün *TCPDump* vasitəsindən istifadə edə bilərlər [15]. Trafik axınlarının xarakteristikalarını müəyyən etmək üçün isə *Netflow*, *Sflow* və *SNMP* vasitələrindən istifadə etmək məqsədəuyğundur [16]. Lakin elə bir vahid şəbəkə monitorinqi vasitəsi yoxdur ki, bütün məsələləri həll etsin. Adətən şəbəkə inzibatçıları spesifik məsələləri həll edən müxtəlif monitorinq vasitələrindən kompleks şəklində istifadə edirlər.

Nəticə

KŞ-in tətbiq sahələri və əhatə dairəsi getdikcə genişlənməkdədir. Bununla yanaşı KŞ-də baş verən fasilələrdən dəyən ziyanın həcmi də artır. Nəticədə KŞ inzibatçılarının şəbəkədə baş verən hadisələrdən xəbərdar olması və onların idarə edilməsi üçün əsaslandırılmış qərarların qəbul edilməsi məsələsi çox aktuallaşır. Lakin bu gün KŞ-in miqyasının böyüməsi və daha yüksək sürətli olması, çoxlu sayda müxtəlif şəbəkə xidmətlərinin, protokollarının və tətbiqi proqramların istifadəsi onların idarə edilməsi məsələsini çətinləşdirir. Buna görə də KŞ-in vəziyyəti daimi nəzarətdə olmalıdır və bu isə şəbəkə monitorinqi aparmadan mümkün deyil. KŞ-in vacib şəbəkə xidmətlərinin, aparat və proqram təminatlarının fəaliyyətinə daimi nəzarəti və şəbəkənin effektiv idarə edilməsini təmin etmək üçün müxtəlif şəbəkə monitorinqi üsullarından və vasitələrindən istifadə edilməsi məqsədəuyğundur.

Ədəbiyyat

1. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей. Изд. «Лори», 2002, 350 с.
2. Breitbart Y., Feodor F. Dragan, Gobjuka H.: Effective Network Monitoring. Proceedings of the International Conference On Computer Communications and Networks (ICCCN 2004), October 11-13, 2004, Chicago, IL, USA, pp. 394-399.
3. Breitbart Y., Chan C. Y., Garofalakis M., Rastogi R., and Silberschatz A., Efficiently Monitoring Bandwidth and Latency in IP Networks, In Proceedings of IEEE INFOCOM, (2000).
4. http://www.caida.org
5. Breitbart Y., Dragan F., Gobjuka H., Effective Monitor Placement in Internet Networks, Journal of Networks, Vol 4, No 7 (2009), 657-666, Sep 2009

6. Lindh T. A new approach to performance monitoring in IP networks - combining active and passive methods. Proc. of Passive and Active Measurements (PAM 2002), 2002.
7. "Active Network Performance Measurement and Estimation" Nov. 14, 2006 http://www.imse.cnm.es/fedemp/abet/index.html
8. Curtis J. "Passive Measurement", Jan 17, 2000. http:// www.wand.cs.waikato.ac.nz/old/wand/publications/jamie_420/final/node9.html
9. RFC 1157 - Simple Network Management Protocol (SNMP) (http://ip-doc.com/rfc/rfc1157)
10. Waldbusser S. Remote network monitoring management information base. RFC2819/STD0059, May 2000, http://www.rfc-editor.org/
11. Cisco Corporation. Netflow services and applications, 2000, http://www.cisco.com/
12. http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html#ping
13. Network monitoring tools. http://www.slac.stanford.edu/xorg/nmtf/nmtf-tools.html, 2007.
14. Cabletron Systems, Spectrum for Open Systems, http://www.cabletron.com/ spectrum/
15. http://www.tcpdump.org/tcpdump_man.html
16. http://www.sflow.org/sFlowOverview.pdf

УДК 004.046

Шыхалиев Рамиз Г.
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

О способах и средствах мониторинга компьютерных сетей

В статье дан анализ задач сетевого мониторинга и различных методов и средств реализации мониторинга компьютерных сетей.

Ключевые слова: *сетевой мониторинг, сетевой трафик, сетевое оборудование, сетевые индикаторы, активный мониторинг, пассивный мониторинг.*

Ramiz H. Shikhaliyev
Institute Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

On methods and means of computer network monitoring

The article analyzes the network monitoring goals and various methods and realization means of monitoring of computer networks.

Keywords: *network monitoring, network traffic, network facility, network indicators, active monitoring, passive monitoring.*