основного й дублюючого контролерів.

CoDeSys Professional Developer Edition розроблено для створення великих, нових, унікальних проектів. ICP містить систему управління версіями на базі Subversion (SVN), графічні редактори UML (діаграми класів, станів, діяльності), статичний аналізатор коду. Контроль версій потрібен в великих проектах, де працює багато розробників. У разі використання SVN зберігається вся історія виправлень з інформацією про те, хто, коли та що виправляв. Тому є можливість повернутися до будь-якої версії на будь-яку дату. UML-діаграма класів дає візуальне представлення залежностей функціональних блоків, методів та інтерфейсів, які можна редагувати графічно. Діаграми станів та активності дозволяють описувати стани та переходи складних процесів. Це дає змогу спростити взаємодію програмістів та технологів, прискорити побудову структури додатку та програмування.

Статичний аналізатор коду перевіряє код МЕК-програм на дотримання більш ніж 50 правил, виявляючи потенційно небезпечні місця та видалити їх до відлагодження та тестування проекту.

CoDeSys Application Composer – спрощена версія CoDeSys, орієнтована на повсякденні типові задачі. Головну роль тут відіграють час створення проекту, простота програмування, надійність програмного коду. У разі виконання робіт з автоматизації подібних об'єктів Application Composer дозволить суттєво підвищити продуктивність.

Вільна система аналізу трафіка WIRESHARK

Шапо В.Ф.

к.т.н., доцент, Одеська національна морська академія, stani@te.net.ua

Role of data transmission between different devices in modern world is analyzed. Complexity and variety of modern data transmission networks is shown. Necessary of data capturing and analyzing software using is proved. General possibilities and some teaching experience of free and open source WireShark software in preparation of maritime specialists are described.

У теперішній час неможливо уявити собі сучасний світ без комп'ютерних мереж. Вони стали найважливішим засобом передавання даних, бо, незважаючи на періодичні фінансово-економічні кризи, світова економіка в останні роки розвивається в цілому швидкими темпами. Виникли та продовжують виникати нові напрямки ведення бізнесу, а інші динамічно змінюються, прилаштовуючись до більш різноманітної та гнучкої роботи. Підприємства укрупнюються, стають транснаціональними, мають велику кількість офісів й створюють виробничі підрозділи в багатьох країнах. Підтримка існуючого бізнесу, освіти, культури, медицини та їхній розвиток стали неможливими без різномантіних мережевих технологій.

Персональні, локальні, кампусні, районні, міські, регіональні, глобальні, дротові та бездротові, домашні, офісні та промислові комп'ютерні мережі стали не тільки комп'ютерними, бо поєднують безліч різноманітних приладів. Продовжують з'являтися нові мережеві технології, а відомі удосконалюються, модернізуються, входять у нові галузі застосування. З'явилися та потроху поширюються новітні терміни "Інтернет речей", коли обмін даними у мережі можуть виконувати кавоварки, інтелектуальні телевізори (Smart TV), холодильники та інші пристрої, що мають свої IP-адреси та дають змогу своїм володарям налаштовувати деякі їхні характеристики.

Все більш поширеною стає також концепція BYOD (Bring Your Own Device, "принесіть свій власний пристрій"), що дає змогу користувачам під'єднуватися до корпоративних комп'ютерних мереж зі своїх пристроїв, працюючи на них і вдома, і на роботі. Це дає змогу працювати більш продуктивно, але збільшує навантаження на мережу та призводить по появи нових, більш складних задач з аналізу мережевого трафіку та управління ним. Новітній термін "інтелектуальний пил" (smart dust) дає змогу вести мову про інтегрування множини датчиків та обчислювальних приладів до одягу, безлічі пристроїв, предметів та навіть у організм людини для контролю її здоров'я.

Усі ці новітні технології також все ширше використовуються у промисловості для побудови автоматичних ліній, автоматизованих виробництв, автоматизації будь-яких процесів у житті людини.

У офісних та виробничих мережах з'явилося безліч новітніх видів програмного забезпечення (ПЗ), що працює в сучасних інформаційних системах (ІС) підприємств та організацій: ПЗ класів ERP (Enterprise Resources Planning, планування ресурсів підприємства), MRP (Manufacturing Resources Planning, планування ресурсів виробництва), CRM (Customer (Client) Relationships Management, управління взаємовідносинами із клієнтами), BI (Business Intelligence, бізнес-аналітика), ECM (Enterprise/Electronic Content Management, електронне управління документообігом підприємства), PMS (Project Management System, системи управління проектами), WMS (Warehouse Management System, системи управління складом) тощо. Усі ці системи виконують обмін даними у різноманітних комп'ютерних мережах.

За останні роки також суттєво зросла кількість шкідливого ПЗ, для боротьби з яким з'являється антивірусне ПЗ та мережеві екрани, що також обмінюються даними у мережі.

Для вчасного та ефективного вирішення проблем, що виникають у комп'ютерних мережах, сучасному розробнику та експлуатаційнику ІС потрібно бути знайомим з ПЗ аналізу мережевого трафіку. Тому для вчасного підготування кваліфікованих кадрів в галузі суднових ІС та управління електрообладнанням в Одеській національній морській академії у дисципліні "Суднові комп'ютерні мережі" на 4-му курсі спеціальності "Електричні системи і комплекси транспортних засобів" та 3-му курсі у дисципліні

“Суднові комп'ютери та комп'ютерні мережі” спеціальності “Експлуатація суднового електрообладнання і засобів автоматики” факультету електромеханіки і радіоелектроніки з'явився розділ, присвячений саме аналізу мережевого трафіку.

Для вивчення цього матеріалу було обрано утиліту Wireshark. Це безкоштовне ПЗ для захвату й аналізу мережевого трафіку (т. зв. сніфер, від англ. to sniff – нюхати). Wireshark працює з більшістю відомих мережевих протоколів (підтримується 1378 протоколів та типів пакетів), має зрозумілий графічний інтерфейс. На початок марту 2015 р. остання стабільна версія 1.12.4. Система працює в ОС Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Mac OS X, Windows й може бути безкоштовно завантажена з сайту wireshark.org.

Аналізатори трафіку потрібні для проведення дослідження мережевих програмних додатків й протоколів та пошуку проблем в роботі мережі зі з'ясуванням причини цих проблем. Щоб ефективно використовувати аналізатори трафіку, необхідні хоча б загальні знання мережевих технологій та розуміння роботи мереж і мережевих протоколів.

Wireshark містить два види фільтрів – захоплення та відображення. Фільтри захоплення використовуються для фільтрації на етапі захоплення трафіку, але при цьому можна безповоротно втратити частину потрібного трафіку. Фільтри відображення фільтрують тільки вже захоплений трафік. Взагалі фільтр – вираз, що складається зі стандартних значень, які можна поєднувати логічними функціями «і», «або», «ні» (and, or, not відповідно). Фільтрувати можна протоколи, адреса, специфічні поля в протоколах.

Wireshark має кілька вбудованих функцій для роботи з технологією VoIP, підтримує багато голосових протоколів: SIP, SDP, RTSP, H.323, RTCP, SRTP та інші, дає змогу захоплювати голосовий трафік та зберігати дані для подальшого прослуховування, знаходити проблеми в мережах Voice over IP.

Під час передавання голосових даних дуже часто використовують протокол RTP (англ. Real-time Transport Protocol, транспортний протокол реального часу), який працює на транспортному рівні моделі OSI та використовується у разі передачі трафіку реального часу. Сумісно з протоколом RTP звичайно використовують наступні протоколи.

1. Для з'ясування якості обслуговування (QOS, Quality Of Service), зворотнього зв'язку та синхронізації між медіа-потоками використовується протокол контролю RTCP (Real-Time Transport Control Protocol, протокол управління передаванням в реальному часі). Смгу пропускання RTCP мала в порівнянні з RT і звичайно складає біля 5 %.

2. Управляючий сигнальний протокол SIP (Session Initiation Protocol, протокол встановлення сеансу зв'язку, працює на прикладному рівні моделі OSI), H.323, MGCP (Media Gateway Control Protocol, протокол управління медіашлюзами), H.248. Сигнальні протоколи управляють відкриттям, модифікацією й закриттям RTP-сесій між приладами та програмними додатками реального часу.

3. Управляючий протокол опису медіа SDP (Session Description Protocol, протокол описання сеансу зв'язку).

Існує також хмарна версія програми WireShark, – ресурс CloudShark.org.

Тут програма Wireshark реалізована у виді онлайн-сервісу (cloud service, хмарне рішення). Зрозуміло, що з його допомогою неможливо захоплювати мережевий трафік, але можна виконувати аналіз дампу трафіка. Завантаживши PCAP-файл на вказаний ресурс для аналізу, можна отримати послідовність пакетів, в якій дані розбиті на зрозумілі поля залежно від протоколу. В цілому даний ресурс відрізняється від Wireshark зменшеною кількістю можливостей, але доступний з будь-якого веб-переглядача.

Бібліотека Pcap (Packet Capture) дає змогу створювати програми аналізу мережевих даних, що надходять на мережеву карту комп'ютера. Її використовують різноманітні програми моніторингу й тестування мережі. Бібліотека призначена для роботи сумісно з мовами C/C++, а для роботи з бібліотекою мовами Java і .NET використовують додаткові оболонки. Для Unix-подібних систем це бібліотека libpcap, а для Microsoft Windows – WinPcap. Програмне забезпечення мережевого моніторингу може використовувати libpcap або WinPcap, щоб захопити пакети, що передаються по мережі, а в новіших версіях, – для передачі пакетів у мережу. Libpcap і WinPcap також підтримують збереження захоплених пакетів в файл та зчитування файлів, що містять збережені пакети. Програми, що написані на базі libpcap или WinPcap, можуть захоплювати мережевий трафік, аналізувати його. Файл захопленого трафіку зберігається в форматі, зрозумілому для програмних додатків, що використовують Pcap.