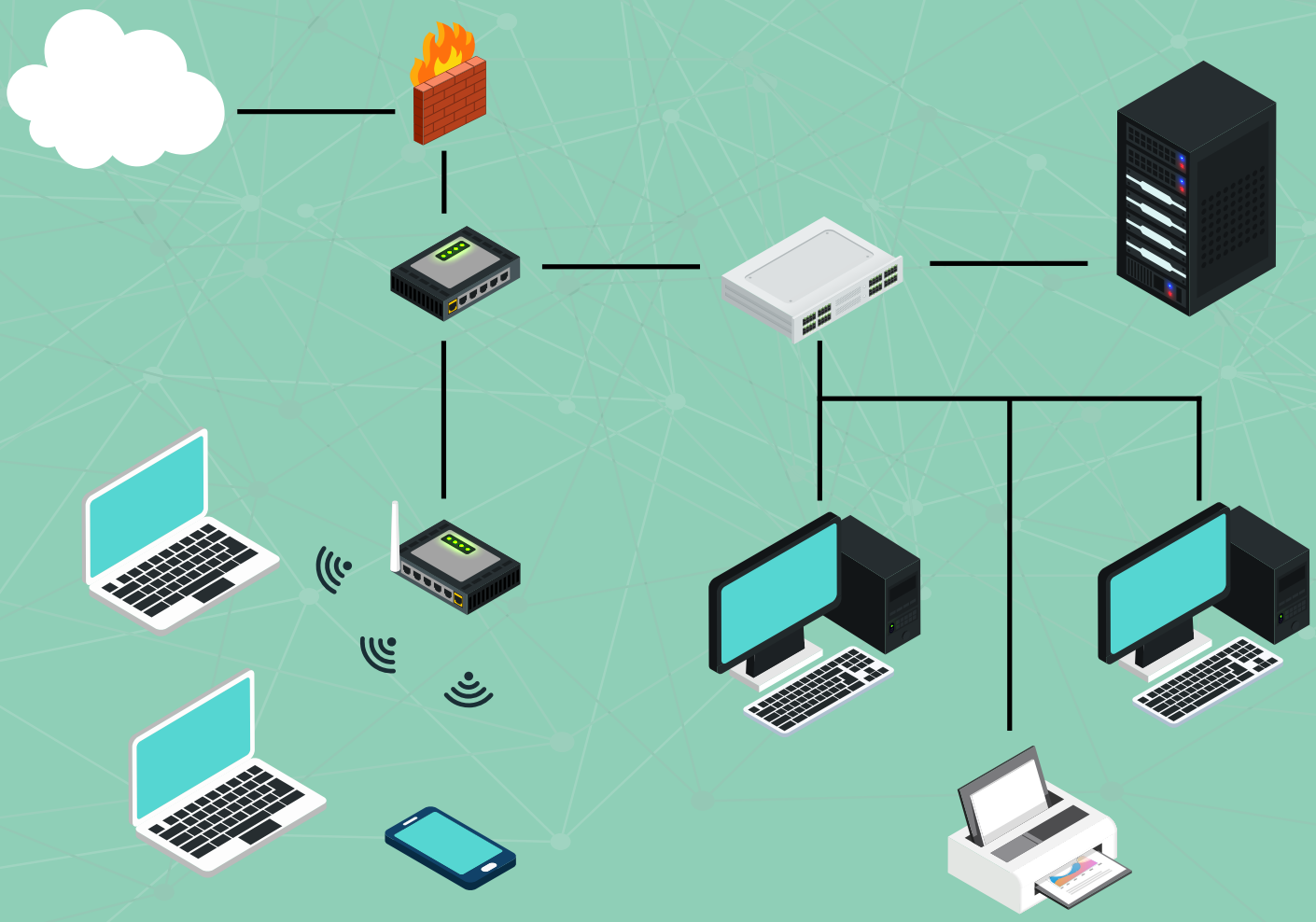
ក្រសួងអប់រំ យុវជនឆនិងកីឡា
Ministry of Education, Youth and Sport

ទំនាក់ទំនងទិន្នន័យ និងបណ្តាញកុំព្យូទ័រ



KOICA
Korea International Cooperation Agency

Korea National University of Education

បុព្វកថា

សង្គមកម្ពុជា បានបោះជំហានទៅរកការអភិវឌ្ឍផ្អែកលើសេដ្ឋកិច្ចឌីជីថល ស្របតាមការវិវត្តរបស់សកលក្នុងយុគសម័យឌីជីថល ដែលពោរពេញដោយព័ត៌មានសម្បូរបែប ការប្រកួតប្រជែងផ្នែកបច្ចេកវិទ្យាឌីជីថលយ៉ាងស្រួចស្រាល់ ព្រមទាំងមានឥទ្ធិពលលើជីវភាពរស់នៅ និងសង្គមការងារ។ ជាមួយគ្នានេះ បច្ចេកវិទ្យាព័ត៌មាន និងសារគមនាគមន៍(ICT) នឹងដើរតួនាទីយ៉ាងសំខាន់ ដើម្បីឆ្លើយតបនឹងការវិវត្តខាងលើ។

ផ្អែកលើមូលដ្ឋាននេះ ក្រសួងអប់រំ យុវជន និងកីឡា មានចក្ខុវិស័យអភិវឌ្ឍធនធានមនុស្សឱ្យមានចំណេះដឹង បំណិនពេញលេញ ជាពិសេសការពង្រឹងសមត្ថភាព ICT ក្នុងគោលដៅលើកកម្ពស់ការច្នៃប្រឌិតនវានុវត្តន៍ ការស្រាវជ្រាវ និងការដោះស្រាយបញ្ហាក្នុងជីវភាពប្រចាំថ្ងៃប្រកបដោយនិរន្តរភាព។ ការលើកកម្ពស់បំណិនសតវត្សរ៍ទី២១ ការអប់រំវិទ្យាសាស្ត្រ និងបច្ចេកវិទ្យា ការអប់រំឌីជីថល និងកំណែទម្រង់សាលាគរុកោសល្យជាអាទិភាពសំខាន់នៃវិស័យអប់រំ យុវជន និងកីឡា។

ក្រសួងអប់រំ យុវជន និងកីឡា បានសហការជាមួយភ្នាក់ងារសហប្រតិបត្តិការអន្តរជាតិកូរ៉េ (KOICA) អភិវឌ្ឍសៀវភៅសិក្សាចំនួន ៩ចំណងជើង សម្រាប់ការបណ្តុះបណ្តាលគរុសិស្ស គរុនិស្សិតមុខវិជ្ជា ICT នៅតាមគ្រឹះស្ថានបណ្តុះបណ្តាលគ្រូ រួមមាន (១) ការណែនាំអំពីកុំព្យូទ័រ (២) ទំនាក់ទំនងទិន្នន័យ និងបណ្តាញ កុំព្យូទ័រ (៣) ពហុមេឌៀអប់រំ (៤) ការសរសេរកម្មវិធីបញ្ញាសិប្បនិម្មិត (៥) មូលដ្ឋានទិន្នន័យ (៦) ភាសាសរសេរកូដកម្មវិធី Python (៧) ការអប់រំព័ត៌មានវិទ្យា (៨) មូលដ្ឋានគ្រឹះនៃអក្ខរកម្មឌីជីថល និង (៩) ការអប់រំ STEAM តាមរយៈ ICT។ ឯកសារបណ្តុះបណ្តាលទាំងនេះ នឹងរួមចំណែកដល់ការគាំទ្រ និងការអនុវត្តកំណែទម្រង់សាលាគរុកោសល្យ តាមរយៈការពង្រឹងចំណេះដឹង និងបំណិន ICT ដល់គ្រូឧទ្ទេស ដើម្បីបណ្តុះបណ្តាលដល់គរុសិស្ស គរុនិស្សិត ដែលនឹងត្រូវបង្រៀនសិស្សានុសិស្សបន្ត។

ក្រសួងអប់រំ យុវជន និងកីឡា សូមថ្លែងអំណរគុណយ៉ាងជ្រាលជ្រៅដល់អ្នកពាក់ព័ន្ធ ដែលបានចូលរួមចំណែកក្នុងការចងក្រង និងផលិតសៀវភៅសិក្សា សម្រាប់បណ្តុះបណ្តាលនៅតាមមជ្ឈមណ្ឌលគរុកោសល្យភូមិភាគ និងបណ្តាគ្រឹះស្ថានបណ្តុះបណ្តាលគ្រូផ្សេងៗទៀត ដើម្បីជាប្រយោជន៍ជូនដល់គ្រូឧទ្ទេស គរុសិស្ស គរុនិស្សិត អ្នកសិក្សា និងប្រជាជនកម្ពុជា។

ក្រសួងអប់រំ យុវជន និងកីឡាសង្ឃឹមថា សៀវភៅសិក្សានេះនឹងក្លាយជាធនធានសិក្សាដ៏មានសារៈសំខាន់ ដែលគាំទ្រដល់បរិវត្តកម្មសេដ្ឋកិច្ចឌីជីថល និងជួយដល់គ្រូឧទ្ទេស គរុសិស្ស គរុនិស្សិត និងអ្នកសិក្សាគ្រប់លំដាប់ថ្នាក់អភិវឌ្ឍសមត្ថភាព បំណិនបច្ចេកវិទ្យាចាំបាច់ ដើម្បីដោះស្រាយបញ្ហាក្នុងជីវភាពប្រចាំថ្ងៃ។

ថ្ងៃ ចន្ទ ៦ រោច ខែទុតិយាសាឍ ឆ្នាំថោះ បញ្ចស័ក ព.ស.២៥៦៧
រាជធានីភ្នំពេញ ថ្ងៃទី ០៧ ខែសីហា ឆ្នាំ២០២៣

រដ្ឋមន្ត្រីក្រសួងអប់រំ យុវជន និងកីឡា

បណ្ឌិតសភាចារ្យ ហង់ជួន ណារ៉ុន

គណៈកម្មាធិការគ្រប់គ្រងគម្រោង

ឯកឧត្តមបណ្ឌិតសភាចារ្យ **ណាត ប៊ុនរឿន**

ឯកឧត្តម **ពុត សាមិត្ត**

លោក **Rho Hyunjun**

លោក **Kim Junsu**

ទីប្រឹក្សាមហាវិទ្យាល័យ សាកលវិទ្យាល័យអប់រំជាតិកូរ៉ែ

បណ្ឌិត **Ki-Sang Song (PM)**
បណ្ឌិត **Taeyoung Kim**
បណ្ឌិត **Youngsik Kim**
បណ្ឌិត **Kwihoon Kim**
បណ្ឌិត **Hyun-Jong Choe**
បណ្ឌិត **Seung-Hyun Kim**
បណ្ឌិត **Sang-Mok Jung**
បណ្ឌិត **Kwan-Hee Yoo**
បណ្ឌិត **In-Seong Jeon (PMO)**

គណៈកម្មាធិការបច្ចេកទេសគម្រោង

ឯកឧត្តម **ពុត សាមិត្ត**
លោក **Kim Junsu**
បណ្ឌិត **Ki-Sang Song (PM)**
អ្នកស្រី **ម៉ែន ភុង្គីតា**
លោក **ង៉ោ ម៉េងឃុង**
លោក **ស៊ុន ប៊ុណ្ណា**
លោក **សុក ថា**
លោក **ព្រីង មរកត**
បណ្ឌិត **ឈូក ច័ន្ទឆាយា**
លោក **សេង ស៊ីម**
លោក **អឿ សុខម៉េង**
លោក **ង៊ួយ ភុទ្ធី**
លោក **ង៉ែត សូដា**

គណៈកម្មាធិការនិពន្ធ

បណ្ឌិត **ឈូក ច័ន្ទឆាយា**
លោក **សុភាព ភណ្ណតក្តី**
លោក **ឈុំ ណាង**
លោក **ហួត បញ្ញាឫទ្ធិ**
លោក **មៀច ឃុយ**
លោក **តែល តារុណា**
លោកស្រី **ប៉ុក ពិសី**
លោក **សំអាង ម៉េងហោង**
លោក **សាន តុន**
លោក **សុខ ថា**
លោក **សន រិទ្ធី**
លោក **តូយ កុម្ភៈ**
លោក **ង៉ី ពុទ្ធី**
លោក **អ៊ុក ប៊ូត្ថ**
លោក **អ៊ុក សម្ផស្ស**
លោក **ឡាយ សុខជា**
លោក **តិន ផល**

អារម្ភកថា

ការបង្រៀន ICT នៅអនុវិទ្យាល័យ ត្រូវមានចំណេះដឹងកុំព្យូទ័រជាមូលដ្ឋាន ហើយចំណេះដឹងកុំព្យូទ័រទាំងអស់ក្នុងសៀវភៅតែមួយបានទេ។ ទោះជាយ៉ាងណាក៏ដោយ នៅក្នុងសៀវភៅនេះ យើងបានព្យាយាមរៀបរាប់ពីមូលដ្ឋានគ្រឹះបណ្តាញ និងវិទ្យាសាស្ត្រកុំព្យូទ័រនៅក្នុងដំណាក់កាលដំបូង។ ក្នុងន័យនេះសៀវភៅនេះគ្របដណ្តប់លើបណ្តាញទំនាក់ទំនងប្រកបដោយប្រសិទ្ធភាព ដោយការណែនាំអំពីគំនិត និងបច្ចេកទេសវិទ្យាសាស្ត្រកុំព្យូទ័រ មុនពេលសិក្សាវិទ្យាសាស្ត្រកុំព្យូទ័រ។ សៀវភៅសិក្សានេះធ្វើតាមការចាត់ថ្នាក់នៃមុខវិជ្ជាដែលរីកចម្រើនទៅតាមលំដាប់លំដោយដែលនាំទៅដល់បទបង្ហាញគរុកោសល្យដែលមុខវិជ្ជានីមួយៗនាំទៅវាចាប់ផ្តើមជាមួយនឹងមូលដ្ឋានគ្រឹះនៃការអិនកូដព័ត៌មាន ការរក្សាទុកទិន្នន័យកុំព្យូទ័រ។

ផ្នែកទីមួយផ្តល់នូវទិដ្ឋភាពទូទៅនៃការទំនាក់ទំនងទិន្នន័យ និងបណ្តាញកុំព្យូទ័រ ហើយនៅក្នុងសៀវភៅនេះបានលើកឡើងអំពីខ្លឹមសារសំខាន់ដូចជា ជំពូកទី១ បានគ្របដណ្តប់គំនិតណែនាំដែលចាំបាច់សម្រាប់សៀវភៅដែលនៅសល់ និងការចាត់ថ្នាក់នៃបណ្តាញប្រព័ន្ធកុំព្យូទ័រ ជំពូកទី២ ពិភាក្សាអំពីប្រភេទនៃបណ្តាញ កុំព្យូទ័រ និងពិធីការបណ្តាញ ជំពូកទី៣ ពិភាក្សាអំពីការបញ្ជូន និងប្រព័ន្ធផ្សព្វផ្សាយ ជំពូកទី៤ ពិភាក្សាអំពី Data Link Layer ជំពូកទី៥ និងជំពូកទី៦ ត្រូវបានពិភាក្សាអំពីស្រទាប់បណ្តាញគំរូបណ្តាញ និងអាសយដ្ឋាន IP ជំពូកទី៧ Transport Layer និងការគ្រប់គ្រងការតភ្ជាប់ ICP ហើយជំពូកទី៨ សុវត្ថិភាពបណ្តាញ និងសុវត្ថិភាពគេហទំព័រ។

នៅលើជំពូកនីមួយៗ យើងមានផ្នែកដែលគ្របដណ្តប់លើប្រធានបទដែលចាប់អារម្មណ៍ជាពិសេសស្វែងយល់ពីបញ្ហាកាន់តែស៊ីជម្រៅ។ សេចក្តីផ្តើម បើកការពិភាក្សាជាមួយបញ្ហាតំណាង ដើម្បីផ្តល់ឱ្យអ្នកអាននូវទិដ្ឋភាពទូទៅនៃអ្វីដែលត្រូវរំពឹងពីជំពូក ចំណុចសំខាន់ៗបង្ហាញពីគោលគំនិតសំខាន់ៗដែលមាននៅក្នុងផ្នែកនីមួយៗ។ ជំពូកសង្ខេបប្រធានបទសំខាន់ៗដែលសិស្សគួរយល់ និងចងចាំ វាជួយពួកគេពង្រឹងគោលគំនិតសំខាន់ៗដែលពួកគេបានរៀននៅក្នុងជំពូក។ មិនតែប៉ុណ្ណោះ នៅចុងបញ្ចប់នៃជំពូកនីមួយៗ មានមេរៀនសង្ខេបខ្លឹមសារមេរៀន ដោយមានសំណួរ លំហាត់ និងកិច្ចការស្រាវជ្រាវក្នុងប្រភេទបញ្ហាសង្គម ដើម្បីផ្តល់ឱកាសដល់សិស្សានុសិស្សក្នុងការអនុវត្តជំនាញថ្មីៗដែលពួកគេបានរៀនដោយខ្លួនឯងផ្ទាល់។ ហើយក្នុងសៀវភៅនេះត្រូវបានរចនាឡើងសម្រាប់ការគិត និងការពិភាក្សា។ ភាគច្រើនអាចត្រូវបានប្រើដើម្បីចាប់ផ្តើមគម្រោងស្រាវជ្រាវ ដោយបញ្ចប់ដោយរបាយការណ៍សរសេរខ្លីៗ ឬផ្ទាល់មាត់។

មាតិកា

ជំពូកទី៧ ៖ Transport Layer

ជំពូកទី៨៖ សុវត្ថិភាពបណ្តាញ

ជំពូកទី ១

ការណែនាំអំពីការទំនាក់ទំនងទិន្នន័យ

ប្រព័ន្ធកុំព្យូទ័រដែលមានទំនាក់ទំនងគ្នាទៅវិញទៅមកនិងឧបករណ៍ផ្សេងៗដែលប្រើប្រាស់ជាមួយកុំព្យូទ័រ ដូចជាម៉ាស៊ីនបោះពុម្ពត្រូវបាន គេហៅថាបណ្តាញកុំព្យូទ័រការភ្ជាប់ ទំនាក់ទំនងគ្នារវាងកុំព្យូទ័រទាំងអស់នេះជួយសម្រួលដល់ការចែករំលែកព័ត៌មានក្នុងបណ្តាញកុំព្យូទ័រទាំងនោះ។ វិស្វកម្មបណ្តាញគឺជាកិច្ចការដ៏ស្មុគស្មាញមួយដែលពាក់ព័ន្ធនឹងកម្មវិធី កម្មវិធីបង្កប់ កម្រិតបន្ទះសៀគ្វីវិស្វកម្ម ផ្នែករឹង និងចរន្តអគ្គិសនី ដើម្បីសម្រួលដល់ការងារវិស្វកម្មបណ្តាញគំនិតនៃបណ្តាញទាំងមូលត្រូវបានបែងចែកទៅជាច្រើនកម្រិត។ អ៊ីនធឺណិតអនុញ្ញាតឱ្យយើងទំនាក់ទំនងជាមួយមនុស្សដែលអង្គុយនៅកន្លែងឆ្ងាយដាច់ស្រយាលពីយើងអាចទំនាក់ទំនងគ្នាបានហើយមានកម្មវិធី ផ្សេងៗដែលមាននៅលើបណ្តាញដែលប្រើអ៊ីនធឺណិតជាឧបករណ៍សម្រាប់ទំនាក់ទំនង។

ជំពូកទី១ នេះអ្នកនឹងរៀនអំពី៖

១.១ ការណែនាំទំនាក់ទំនងបណ្តាញ

នៅក្នុងភាពជាមនុស្សនៅលើផែនដីនេះ យើងអាចធ្វើការទំនាក់ទំនងគ្នាទៅវិញទៅមកតាមរយៈ ភាសាប៉ុន្តែមនុស្សយកអំណោយនេះទៅកម្រិតមួយទៀត ចំណាយពេលវេលា និងអត្ថិភាពរាងកាយរបស់មនុស្សមិនសំខាន់ទេក្នុងការប្រាស្រ័យទាក់ទងគ្នានាពេលបច្ចុប្បន្ននេះ ពីព្រោះពួកគេបង្កើតប្រព័ន្ធទំនាក់ទំនងតាមរយៈការដែលពួកគេអាចទំនាក់ទំនង ឬចែករំលែកទិន្នន័យដូចជា រូបភាព វីដេអូ អត្ថបទ ឯកសារជាដើម ជាមួយមនុស្សជាទីស្រលាញ់របស់ពួកគេគ្រប់ពេលវេលា គ្រប់ទីកន្លែង ការប្រាស្រ័យទាក់ទងគ្នា គឺជាដំណើរការមួយដែលកុំព្យូទ័រច្រើនជាងមួយផ្ទេរព័ត៌មាន និងការណែនាំទៅគ្នាទៅវិញទៅមក និងសម្រាប់ការចែករំលែកធនធានឬម្យ៉ាងទៀត ការទំនាក់ទំនងគឺជាដំណើរការ ឬសកម្មភាពដែលយើងអាចធ្វើ ឬទទួលទិន្នន័យ។ បណ្តាញកុំព្យូទ័រត្រូវបានកំណត់ថាជាបណ្តុំនៃកុំព្យូទ័រស្វ័យតដែលមានទំនាក់ទំនងគ្នាទៅវិញទៅមក ស្វ័យតមានន័យថាគ្មានកុំព្យូទ័រអាចចាប់ផ្តើម បញ្ឈប់ ឬគ្រប់គ្រងកុំព្យូទ័រផ្សេងទៀតបានទេ។

ទំនាក់ទំនងទិន្នន័យសំដៅលើការបញ្ជូនទិន្នន័យឌីជីថលនេះរវាងកុំព្យូទ័រពីរ ឬច្រើន ហើយបណ្តាញកុំព្យូទ័រជាច្រើនឬបណ្តាញទិន្នន័យគឺជាបណ្តាញទូរគមនាគមន៍ដែលអនុញ្ញាតឱ្យកុំព្យូទ័រផ្លាស់ប្តូរទិន្នន័យ។ ការតភ្ជាប់រូបវន្តរបស់ឧបករណ៍កុំព្យូទ័រតាមបណ្តាញត្រូវបានបង្កើតឡើងដោយការ ប្រើប្រាស់ ឬប្រព័ន្ធផ្សព្វផ្សាយឥតខ្សែ បណ្តាញកុំព្យូទ័រដែលល្បីជាងគេគឺជាអ៊ីនធឺណិត។ ហើយនៅក្នុងមេរៀននេះបង្រៀនអ្នកពីមូលដ្ឋានគ្រឹះនៃការទំនាក់ទំនងទិន្នន័យ និងបណ្តាញកុំព្យូទ័រហើយនឹងនាំឱ្យស្គាល់ពីកម្រិតខ្ពស់ផ្សេងៗទាក់ទងនឹងការទំនាក់ទំនងទិន្នន័យ និងបណ្តាញកុំព្យូទ័រ។

១.១.១ ការយល់ដឹងជាមូលដ្ឋានបណ្តាញ

បណ្តាញកុំព្យូទ័រគឺជាប្រព័ន្ធនៃកុំព្យូទ័រដែលមានទំនាក់ទំនងគ្នាទៅវិញទៅមក រវាងកុំព្យូទ័រ និងគ្រឿងកុំព្យូទ័រ កុំព្យូទ័រ និងម៉ាស៊ីនបោះពុម្ព ហើយនឹងឧបករណ៍ផ្សេងៗទៀត។ ការភ្ជាប់គ្នារវាងកុំព្យូទ័រនេះជួយសម្រួលដល់ការចែករំលែកព័ត៌មានក្នុងចំណោមកុំព្យូទ័រជាច្រើនក្នុងបណ្តាញតែមួយ កុំព្យូទ័រអាចភ្ជាប់ទំនាក់ទំនងគ្នាដោយមានខ្សែ ឬឥតខ្សែ។

១.១.២ ទិស្សកម្មបណ្តាញ

វិស្វកម្មបណ្តាញគឺជាការងារដ៏ស្មុគស្មាញដែលពាក់ព័ន្ធនឹងកម្មវិធី ផ្នែកទន់, កម្មវិធីបង្កប់ កម្រិតបន្ទះសៀគ្វីវិស្វកម្ម ផ្នែករឹង និងចរន្តអគ្គិសនី គំនិតនៃបណ្តាញត្រូវបានបែងចែកទៅជាស្រទាប់ជាច្រើនដើម្បីសម្រួលការងាររបស់វិស្វកម្មបណ្តាញស្រទាប់នីមួយៗត្រូវបានចូលរួមនៅក្នុងកិច្ចការពិសេសស្រទាប់ ផ្សេងទៀតទាំងអស់។ ប៉ុន្តែសរុបមកការងារបណ្តាញស្ទើរតែទាំងអស់គឺអាស្រ័យលើស្រទាប់ទាំងអស់នេះ។ ស្រទាប់ចែករំលែកទិន្នន័យគឺជាស្រទាប់មួយដ៏សំខាន់ពួកវាពឹងផ្អែកលើគ្នាទៅវិញទៅមកដើម្បីបញ្ចូល និងបញ្ជូនទិន្នន័យ។

១.១.៣ អ៊ីនធឺណិត

បណ្តាញនៃបណ្តាញត្រូវបានគេហៅថា ការងារអ៊ីនធឺណិត ឬជាធម្មតាអ៊ីនធឺណិត។ វាគឺជាបណ្តាញដ៏ធំបំផុតដែលមាននៅលើភពផែនដីនេះ។ អ៊ីនធឺណិតភ្ជាប់ WAN ទាំងអស់យ៉ាងធំធេង ហើយអាចទាក់ទងទៅបណ្តាញ LAN និង Home ។ អ៊ីនធឺណិតប្រើឈុតពិធីការ TCP/IP ហើយប្រើ IP ជាពិធីការអាសយដ្ឋានរបស់វាសព្វថ្ងៃនេះ អ៊ីនធឺណិតត្រូវបានអនុវត្តយ៉ាងទូលំទូលាយដោយប្រើ IPv4 ដោយសារតែកង្វះចន្លោះអាសយដ្ឋាន វាកំពុងផ្លាស់ប្តូរបន្តិចម្តងៗពី IPv4 ទៅ IPv6។

អ៊ីនធឺណិតអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ចែករំលែក និងចូលប្រើប្រាស់ព័ត៌មានដ៏ធំសម្បើមនៅទូទាំង ពិភពលោក។ វាប្រើ WWW, FTP, សេវាកម្មអ៊ីមែល អូឌីយ៉ូ និងវីដេអូស្ទ្រីម។ អ៊ីនធឺណិតប្រើឆ្អឹងខ្នងដែលមានល្បឿនលឿនបំផុតនៃខ្សែកាបអុបទិក។ ដើម្បីភ្ជាប់អន្តរទ្វីបផ្សេងៗ ជាសរសៃត្រូវបានដាក់នៅក្រោមបាតសមុទ្រ ដែលត្រូវបានគេស្គាល់ថាជាខ្សែទំនាក់ទំនងក្នុងនាវាមុជទឹក។

១.២ ទិដ្ឋភាពទូទៅនៃបណ្តាញ

បណ្តាញកុំព្យូទ័រគឺជាប្រព័ន្ធនៃកុំព្យូទ័រដែលមានទំនាក់ទំនងគ្នាទៅវិញទៅមក ហើយមានដូចជាគ្រឿងកុំព្យូទ័រដូចជាម៉ាស៊ីនបោះពុម្ពជាដើម។ ការភ្ជាប់ទំនាក់ទំនងគ្នារវាងកុំព្យូទ័រនេះជួយសម្រួលដល់ការចែករំលែកព័ត៌មានក្នុងចំណោមកុំព្យូទ័រទាំងនោះហើយកុំព្យូទ័រទាំងអស់អាចធ្វើការទំនាក់ទំនងគ្នាភ្ជាប់ដោយមេឌៀមានខ្សែ ឬឥតខ្សែ។

១.២.១ ចំណាត់ថ្នាក់បណ្តាញកុំព្យូទ័រ

បណ្តាញកុំព្យូទ័រត្រូវបានចាត់ថ្នាក់ដោយផ្អែកលើកត្តាផ្សេងៗរួមមាន៖

- វិសាលភាពភូមិសាស្ត្រ
- ការតភ្ជាប់អន្តរ
- ការគ្រប់គ្រង
- ស្ថាបត្យកម្ម

១.២.២ ទិសាលភាពភូមិសាស្ត្រ

តាមភូមិសាស្ត្រ បណ្តាញមួយអាចត្រូវបានគេមើលឃើញនៅក្នុងប្រភេទមួយដូចខាងក្រោម៖

- វាអាចលាតសន្ធឹងលើតុរបស់អ្នកក្នុងចំណោមឧបករណ៍ដែលប្រើប្លិ្លធូស ដែលមានទំហំមិនលើសពីពីរបីម៉ែត្រ
- វាអាចលាតសន្ធឹងពាសពេញអាគារទាំងមូល រួមទាំងឧបករណ៍កម្រិតមធ្យមដើម្បីភ្ជាប់ជាន់ទាំងអស់
- វាអាចលាតសន្ធឹងទូទាំងទីក្រុងទាំងមូល
- វាអាចលាតសន្ធឹងទូទាំងទីក្រុង ឬខេត្តជាច្រើន

- វាអាចជាបណ្តាញមួយដែលគ្របដណ្តប់ពិភពលោកទាំងមូល

១.២.៣ ការតភ្ជាប់អន្តរ

ធាតុផ្សំនៃបណ្តាញអាចតភ្ជាប់ខុសគ្នាតាមម៉ូដមួយចំនួនតាមរយៈការតភ្ជាប់ យើងមានន័យថាជាឡូជីខល រូបវន្ត ឬវិធីទាំងពីរ។

- រាល់ឧបករណ៍តែមួយអាចភ្ជាប់ទៅគ្រប់ឧបករណ៍ផ្សេងទៀតនៅលើបណ្តាញ បណ្តាញមួយអាចភ្ជាប់ជាមួយបណ្តាញជាច្រើនទៀត។
- ឧបករណ៍ទាំងអស់អាចភ្ជាប់ទៅឧបករណ៍ផ្ទុកតែមួយ ប៉ុន្តែត្រូវបានផ្តាច់តាមភូមិសាស្ត្រ បង្កើតរចនាសម្ព័ន្ធ Bus។
- ឧបករណ៍នីមួយៗត្រូវបានភ្ជាប់ទៅ (Peers)ឆ្វេង និងស្តាំរបស់វាតែប៉ុណ្ណោះបង្កើតប្រព័ន្ធលីនេអ៊ែរ។
- ឧបករណ៍ទាំងអស់ត្រូវបានភ្ជាប់ជាមួយឧបករណ៍តែមួយបង្កើតរចនាសម្ព័ន្ធ Star។
- ឧបករណ៍ទាំងអស់បានភ្ជាប់តាមអំពើចិត្តរបស់អ្នកប្រើប្រាស់ដើម្បីភ្ជាប់ទៅគ្នាទៅវិញទៅមកដែលបណ្តាលឱ្យមានរចនាសម្ព័ន្ធក្លាយទៅជារចនាសម្ព័ន្ធ Hybrid ។

១.២.៤ ការគ្រប់គ្រង

តាមទស្សនៈរបស់អ្នកគ្រប់គ្រងបណ្តាញអាចជាបណ្តាញឯកជនដែលជាកម្មសិទ្ធិរបស់ប្រព័ន្ធស្វ័យតតែមួយ។ វាមិនអាចចូលប្រើនៅខាងក្រៅដែនរូបវន្ត ឬឡូជីខលរបស់វាបានទេ។ បណ្តាញមួយអាចជាសាធារណៈ និងអាចចូលប្រើប្រាស់បានដោយមនុស្សទាំងអស់។

ក. ស្ថាបត្យកម្មបណ្តាញ

បណ្តាញកុំព្យូទ័រអាចត្រូវបានរើសអើងទៅជាប្រភេទផ្សេងៗដូចជា ម៉ាស៊ីនភ្ញៀវទៅម៉ាស៊ីនបម្រើ Peer-to-Peer ឬ បណ្តាញកូនកាត់ Hhybrid អាស្រ័យលើស្ថាបត្យកម្ម។

- អាចមានប្រព័ន្ធមួយ ឬច្រើនដើរតួជាម៉ាស៊ីនមេហើយមួយទៀតគឺ ម៉ាស៊ីនភ្ញៀវ ដែលស្នើសុំម៉ាស៊ីនបម្រើដើម្បីបម្រើសំណើម៉ាស៊ីនមេទទួលយក និងដំណើរការសំណើ
- ប្រព័ន្ធពីរអាចត្រូវបានតភ្ជាប់ពីចំណុចទៅចំណុច ឬក្នុងទម្រង់តែមួយដូច្នេះពួកគេទាំងពីរគឺនៅកម្រិតដូចគ្នា ហើយត្រូវបានគេហៅថាបណ្តាញ peer-to-peer ។
- បណ្តាញកូនកាត់(hybrid) អាចពាក់ព័ន្ធនឹងស្ថាបត្យកម្មនៃប្រភេទទាំងពីរខាងលើ។

ខ. កម្មវិធីបណ្តាញ

ប្រព័ន្ធកុំព្យូទ័រ និងគ្រឿងកុំព្យូទ័រត្រូវបានតភ្ជាប់ដើម្បីបង្កើតបណ្តាញទំនាក់ទំនងគ្នា បានផ្តល់អត្ថប្រយោជន៍ជាច្រើន៖

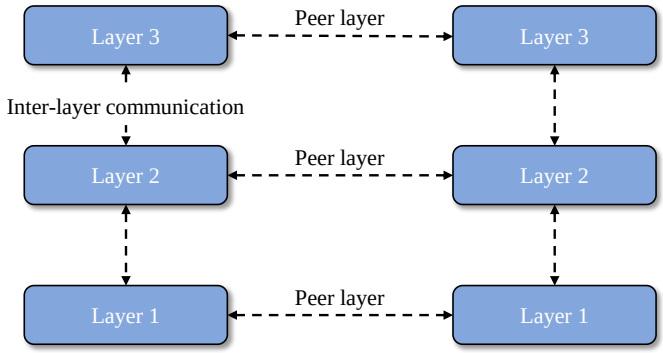
- ការចែករំលែកធនធាន ដូចជាម៉ាស៊ីនបោះពុម្ព និងឧបករណ៍ផ្ទុក
- ការផ្លាស់ប្តូរព័ត៌មានដោយប្រើអ៊ីមែល និង FTP
- ការចែករំលែកព័ត៌មានដោយប្រើគេហទំព័រ ឬអ៊ីនធឺណិត
- អន្តរកម្មជាមួយអ្នកប្រើប្រាស់ផ្សេងទៀតដោយប្រើគេហទំព័រថាមវន្ត
- IP ទូរស័ព្ទ
- សន្និសីទវីដេអូ
- ការគណនាប៉ារ៉ាឡែល
- ការផ្ញើសារភ្លាមៗ

១.៣ ការណែនាំអំពីគំរូបណ្តាញ

វិស្វកម្មបណ្តាញគឺជាកិច្ចការដ៏ស្មុគស្មាញដែលពាក់ព័ន្ធនឹង កម្មវិធីបង្កប់ កម្រិតបន្ទះសៀគ្វី វិស្វកម្ម ផ្នែករឹង និងចរន្តអគ្គិសនី ។ គំនិតនៃបណ្តាញត្រូវបានបែងចែកទៅជាស្រទាប់ជាច្រើនដើម្បី សម្រួលដល់វិស្វកម្មបណ្តាញស្រទាប់នីមួយៗត្រូវបានចូលរួមនៅក្នុងកិច្ចការពិសេស និងឯករាជ្យនៃ ស្រទាប់ផ្សេងទៀតទាំងអស់។ ប៉ុន្តែសរុបមក ការងារបណ្តាញស្ទើរតែទាំងអស់គឺអាស្រ័យលើស្រទាប់ ទាំងនេះហើយទាំងអស់ស្រទាប់ចែករំលែកទិន្នន័យរវាងពួកវា ពឹងផ្អែកលើគ្នាទៅវិញទៅមកដើម្បីដើម្បី បញ្ចូល និងបញ្ជូនទិន្នន័យ។

១.៣.១ កិច្ចការជាស្រទាប់

នៅក្នុងស្ថាបត្យកម្មស្រទាប់នៃ ម៉ូដែលបណ្តាញដំណើរការបណ្តាញទាំងមូលមួយត្រូវបានបែង ចែកទៅជាកិច្ចការតូចៗបន្ទាប់មកកិច្ចការតូចតាចនីមួយៗត្រូវបានផ្តល់ទៅឱ្យ ស្រទាប់ជាក់លាក់មួយ ដែលផ្តល់ដល់ដំណើរការសិក្សាតែប៉ុណ្ណោះ។ ស្រទាប់នីមួយៗធ្វើតែការងារជាក់លាក់ប៉ុណ្ណោះ នៅក្នុង ប្រព័ន្ធទំនាក់ទំនងជាស្រទាប់ហើយ ស្រទាប់មួយនៃម៉ាស៊ីនបានដោះស្រាយជាមួយនឹងកិច្ចការដែល បានធ្វើដោយផ្ទាល់ ឬក៏ត្រូវធ្វើដោយស្រទាប់មិត្តភ័ក្តិរបស់វានៅកម្រិតដូចគ្នានៅលើម៉ាស៊ីនពីចម្ងាការ សិក្សាត្រូវបានផ្តួចផ្តើមដោយស្រទាប់នៅកម្រិតទាបបំផុត ឬក៏កំពូលបំផុត។ ប្រសិនបើភារកិច្ចត្រូវបាន បង្កើតដោយស្រទាប់ខាងលើបំផុត វាត្រូវបានបញ្ជូនទៅស្រទាប់ខាងក្រោមសម្រាប់ដំណើរការបន្ថែម។



រូបភាព ១.១ កិច្ចការជាស្រទាប់

រាល់ស្រទាប់នីមួយៗរួមគ្នានូវរាល់នីតិវិធី ពិធីការ និងវិធីសាស្ត្រដែលវាទាមទារដើម្បីប្រតិបត្តិកិច្ចការជាផ្នែករបស់វា។ ស្រទាប់ទាំងអស់កំណត់អត្តសញ្ញាណសមភាគីរបស់ពួកគេដោយប្រើបឋមកថា និងកន្ទុយ។

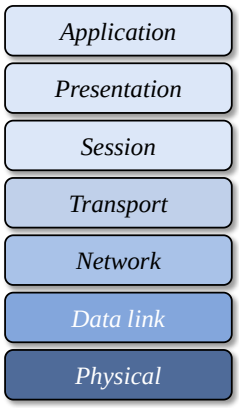
១.៣.២ OSI ម៉ូដែល

Open System Interconnect គឺជាស្តង់ដារបើកចំហសម្រាប់ប្រព័ន្ធទំនាក់ទំនងទាំងអស់គំរូ OSI ត្រូវបានបង្កើតឡើងដោយអង្គការស្តង់ដារអន្តរជាតិ (ISO)។

ម៉ូដែលនេះមានប្រាំពីរស្រទាប់៖

- **Application Layer ៖** ស្រទាប់នេះផ្តល់នូវចំណុចប្រទាក់ប្រឡាសម្រាប់អ្នកប្រើប្រាស់កម្មវិធីស្រទាប់នេះរួមបញ្ចូលពិធីការដែលមានអន្តរកម្មដោយផ្ទាល់ជាមួយអ្នកប្រើប្រាស់ផ្ទាល់តែម្តង
- **Presentation Layer ៖** ស្រទាប់នេះកំណត់ពីរបៀបដែលទិន្នន័យក្នុងទម្រង់ដើមរបស់ម៉ាស៊ីនពីចម្ងាយគួរត្រូវបានបង្ហាញជាទម្រង់ដើមរបស់ម៉ាស៊ីន។
- **Session Layer ៖** ស្រទាប់នេះរក្សាវគ្គរវាងម៉ាស៊ីនពីចម្ងាយ។ ឧទាហរណ៍នៅពេលដែលការផ្ទៀងផ្ទាត់អ្នកប្រើប្រាស់/ពាក្យសម្ងាត់ត្រូវបានធ្វើរួច ម៉ាស៊ីនពីចម្ងាយគាំទ្រ រក្សាទុកចំនុចនេះមួយរយៈ ហើយមិនស្នើសុំការផ្ទៀងផ្ទាត់ម្តងទៀតក្នុងរយៈពេលនោះ។
- **Transport Layer ៖** ស្រទាប់នេះទទួលខុសត្រូវចំពោះការចែកចាយពីចុងម្ខាងដល់ចុងម្ខាងរវាងម៉ាស៊ីនបម្រើ និងម៉ាស៊ីនភ្ញៀវ។
- **Network Layer ៖** ស្រទាប់នេះទទួលខុសត្រូវចំពោះការកំណត់អាសយដ្ឋាន និងកំណត់អាសយដ្ឋានម៉ាស៊ីនតែមួយនៅក្នុងបណ្តាញ។
- **Data Link Layer ៖** ស្រទាប់នេះទទួលខុសត្រូវចំពោះការអាន និងសរសេរទិន្នន័យពី និងលើបន្ទាត់កំហុសនៃតំណភ្ជាប់ត្រូវបានរកឃើញនៅស្រទាប់នេះ។

- **Physical Layer ៖** ស្រទាប់នេះកំណត់ផ្នែករឹង ខ្សែ និងខ្សែ ទិន្នផលថាមពលដែលបានប្រើប្រាស់។

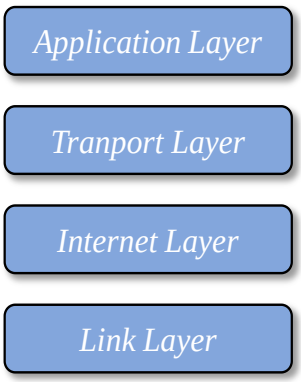


រូបភាព ១.២ OSI ស្រទាប់ម៉ូដែល

១.៣.៣ ម៉ូដែលអ៊ីនធឺណិត

អ៊ីនធឺណិត ដែលត្រូវបានគេស្គាល់ជាទូទៅប្រើប្រាស់ពិធីការ TCP/IP គឺជាសំណុំនៃពាក្យទំនាក់ទំនងដែលប្រើក្នុងអ៊ីនធឺណិត និងបណ្តាញកុំព្យូទ័រស្រដៀងគ្នាជាមូលដ្ឋានបច្ចុប្បន្ននៅក្នុងសារត្រួតពិនិត្យការបញ្ជូន (TCP) និងពិធីការអ៊ីនធឺណិត (IP) ក៏ដូចជាពិធីសារទិន្នន័យកម្មវិធី (UDP) ផងដែរ។ ក្នុងអំឡុងពេលនៃការអភិវឌ្ឍន៍ កំណែរបស់វាត្រូវបានគេស្គាល់ថាជាគំរូរបស់ក្រសួងការពារជាតិ (DoD) ដោយសារតែការអភិវឌ្ឍន៍នៃវិធីសាស្ត្របណ្តាញត្រូវបានផ្តល់មូលនិធិដោយក្រសួងការពារជាតិសហរដ្ឋអាមេរិកតាមរយៈ DARPA ហើយការអនុវត្តរបស់វាគឺជាពិធីការ stack។

អ៊ីនធឺណិតប្រើឈុតពិធីការ TCP/IP ដែលត្រូវបានគេស្គាល់ថាជាឈុតអ៊ីនធឺណិតនេះកំណត់នូវគំរូអ៊ីនធឺណិត ដែលមានស្ថាបត្យកម្មស្រទាប់ទីបួន។ គំរូអ៊ីនធឺណិតគឺជាគំរូទំនាក់ទំនងទូទៅ ប៉ុន្តែ គំរូអ៊ីនធឺណិត គឺជាអ្វីដែលអ៊ីនធឺណិតប្រើប្រាស់សម្រាប់ការទំនាក់ទំនងទាំងអស់របស់វា។ អ៊ីនធឺណិតគឺឯករាជ្យនៃស្ថាបត្យកម្មបណ្តាញមូលដ្ឋានរបស់វាហើយក៏ជាគំរូម៉ូដែលនេះមានស្រទាប់ដូចខាងក្រោម៖



រូបភាព ១.៣ គំរូអ៊ីនធឺណិត

- **Application Layer ៖** ស្រទាប់នេះបានកំណត់ពិធីការដែលអាចឱ្យអ្នកប្រើប្រាស់ធ្វើអន្តរកម្ម ជាមួយបណ្តាញ - ឧទាហរណ៍ FTP, HTTP ។
- **Transport Layer ៖** ស្រទាប់នេះបានកំណត់ពីរបៀបដែលទិន្នន័យធ្វើទំនាក់ទំនងរវាងម៉ាស៊ីន ពិធីការសំខាន់នៅស្រទាប់នេះគឺពិធីការការត្រួតពិនិត្យការបញ្ជូន (TCP) ។ ស្រទាប់នេះធានា ថាទិន្នន័យដែលបានបញ្ជូនរវាងម៉ាស៊ីនគឺស្ថិតនៅក្នុងលំដាប់ និងទទួលខុសត្រូវចំពោះការចែក ចាយពីដើមបដល់ចប់។
- **Internet Layer ៖** អ៊ីនធឺណិតពិធីការ (IP) ដំណើរការលើស្រទាប់នេះ ស្រទាប់នេះជួយ សម្រួលដល់អាសយដ្ឋានម៉ាស៊ីន និងការទទួលស្គាល់ ហើយស្រទាប់នេះជាស្រទាប់កំណត់ ការនាំផ្លូវរបស់បណ្តាញ។
- **Data Link Layer ៖** ស្រទាប់នេះផ្តល់នូវយន្តការសម្រាប់បញ្ជូន និងទទួលទិន្នន័យ មិនដូច សមភាគី OSI ម៉ូដែលទេ ស្រទាប់នេះគឺឯករាជ្យនៃបណ្តាញមូលដ្ឋាន។

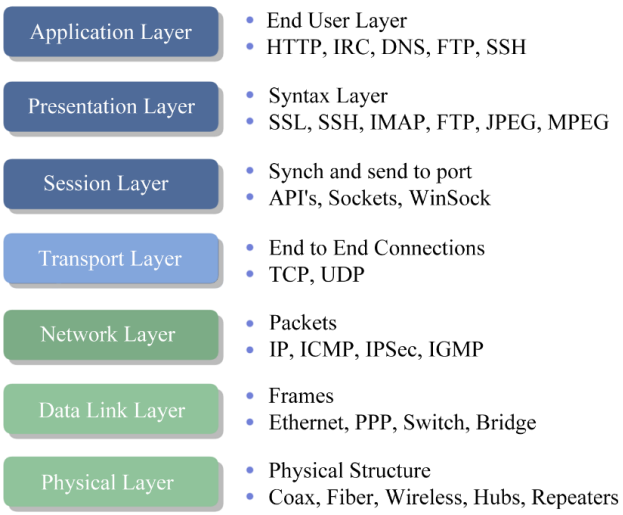
១.៣.៤ ស្រទាប់ OSI ៧

OSI ឬ គំរូការតភ្ជាប់ប្រព័ន្ធបើកទូលាយ ត្រូវបានបង្កើតឡើងដោយអង្គការស្តង់ដារអន្តរជាតិ (ISO)។ វាផ្តល់នូវក្របខ័ណ្ឌបណ្តាញជាស្រទាប់ ដែលបង្កើតគំនិតអំពីរបៀបដែលការទំនាក់ទំនងគួរតែ ត្រូវបានធ្វើរវាងប្រព័ន្ធខុសគ្នាវាមានប្រាំពីរស្រទាប់ដែលទាក់ទងគ្នាទៅវិញទៅមក។ ស្រទាប់ទាំង ប្រាំពីរនៃ OSI Model គឺជា Application Layer , Presentation Layer, Session Layer, Transport Layer, Network Layer, Data Link Layer, Physical Layer ស្រទាប់គាំទ្របណ្តាញគឺ តំណភ្ជាប់ទិន្នន័យ និងស្រទាប់បណ្តាញស្រទាប់គ្រប់គ្រងរាល់ការផ្ទេរទិន្នន័យពីឧបករណ៍មួយទៅ ឧបករណ៍មួយទៀត។ ស្រទាប់គាំទ្រអ្នកប្រើគឺជាផ្នែក។ បទបង្ហាញ និងស្រទាប់កម្មវិធី ស្រទាប់ទាំងនេះ អនុញ្ញាតឱ្យមានការប្រាស្រ័យទាក់ទងគ្នាក្នុងចំណោមកម្មវិធីដែលមិនទាក់ទងគ្នាក្នុងបរិយាកាសផ្សេ ងៗគ្នា។

Transport Layer ភ្ជាប់ក្រុមទាំងពីរត្រូវបានអង្គការស្តង់ដារអន្តរជាតិបង្កើតគំរូ OSI (Open Systems Interconnection)។ វាគឺជាក្របខ័ណ្ឌស្រទាប់សម្រាប់ការរចនាប្រព័ន្ធបណ្តាញដែលអនុញ្ញាតឱ្យមានទំនាក់ទំនងរវាងប្រព័ន្ធកុំព្យូទ័រទាំងអស់។ គោលបំណងចម្បងរបស់វាគឺផ្តល់គោលការណ៍ណែនាំរចនាសម្ព័ន្ធសម្រាប់ការផ្លាស់ប្តូរព័ត៌មានរវាងកុំព្យូទ័រ ស្ថានីយការងារ និងបណ្តាញ។

មុខងារសំខាន់នៃស្រទាប់នីមួយៗមានដូចខាងក្រោម ៖

- **Physical Layer ៖** មុខងាររបស់វាគឺដើម្បីបញ្ជូនប៊ីតនីមួយៗពីថ្នាំងមួយទៅថ្នាំងមួយទៀតលើឧបករណ៍ផ្ទុករូបវន្ត។
- **Data Link Layer ៖** វាទទួលខុសត្រូវចំពោះការផ្ទេរទិន្នន័យដែលអាចទុកចិត្តបាននៃស៊ុមទិន្នន័យពីថ្នាំងមួយទៅថ្នាំងមួយទៀតដែលតភ្ជាប់ដោយស្រទាប់រូបវន្ត។
- **Network Layer ៖** វាគ្រប់គ្រងការចែកចាយកញ្ចប់ទិន្នន័យបុគ្គលពីប្រភពទៅគោលដៅតាមរយៈអាសយដ្ឋាន និងការកំណត់ផ្លូវសមស្រប។
- **Transport Layer ៖** វាទទួលខុសត្រូវក្នុងការបញ្ជូនសារទាំងមូលពីម៉ាស៊ីនប្រភពទៅម៉ាស៊ីនគោលដៅ។
- **Session Layer ៖** វាបង្កើតវគ្គរវាងអ្នកប្រើប្រាស់ និងផ្តល់សេវាកម្មដូចជាការគ្រប់គ្រងប្រអប់ និងការធ្វើសមកាលកម្ម។
- **Presentation Layer ៖** វាត្រួតពិនិត្យវាក្យសម្ព័ន្ធ និងអត្ថន័យនៃព័ត៌មានដែលបានបញ្ជូនតាមរយៈការបកប្រែ ការបង្ហាប់ និងការអ៊ិនគ្រីប
- **Application Layer ៖** វាផ្តល់ឱ្យអ្នកប្រើប្រាស់នូវកម្រិតខ្ពស់ APIs (application programming interface)



រូបភាព ១.៤ OSI ៧ ម៉ូដែល

១.៤ ប្រវត្តិអ៊ីនធឺណិត

ប្រវត្តិសាស្ត្រនៃអ៊ីនធឺណិតមានប្រភពដើមនៅក្នុងទ្រឹស្តីព័ត៌មាន និងការខិតខំប្រឹងប្រែងក្នុងការសាងសង់ និងតភ្ជាប់បណ្តាញកុំព្យូទ័រដែលកើតឡើងពីការស្រាវជ្រាវ និងការអភិវឌ្ឍន៍នៅក្នុងសហរដ្ឋអាមេរិក និងពាក់ព័ន្ធនឹងកិច្ចសហប្រតិបត្តិការអន្តរជាតិ ជាពិសេសជាមួយអ្នកស្រាវជ្រាវនៅចក្រភពអង់គ្លេស និងប្រទេសបារាំង។ វិទ្យាសាស្ត្រកុំព្យូទ័រគឺជាវិន័យដែលកំពុងលេចចេញនៅចុងទសវត្សរ៍ឆ្នាំ ១៩៥០ ដែលបានចាប់ផ្តើមពិចារណាលើការចែករំលែកពេលវេលារវាងអ្នកប្រើប្រាស់កុំព្យូទ័រ ហើយក្រោយមកលទ្ធភាពនៃការសម្រេចបាននូវបណ្តាញយ៉ាងធំទូលាយ។ ដោយឯករាជ្យ លោក Paul Baran បានស្នើឱ្យបណ្តាញចែកចាយដោយផ្អែកលើទិន្នន័យនៅក្នុងប្លុកសារនៅដើមទសវត្សរ៍ឆ្នាំ ១៩៦០ ហើយលោក Donald Davies បានបង្កើតការប្តូរកញ្ចប់ព័ត៌មាននៅឆ្នាំ ១៩៦៥ នៅមន្ទីរពិសោធន៍រូបវិទ្យាជាតិ (NPL) ដោយស្នើបណ្តាញទិន្នន័យពាណិជ្ជកម្មជាតិនៅចក្រភពអង់គ្លេស។

ទីភ្នាក់ងារគម្រោងស្រាវជ្រាវកម្រិតខ្ពស់ (ARPA) នៃក្រសួងការពារជាតិសហរដ្ឋអាមេរិកបានផ្តល់កិច្ចសន្យាក្នុងឆ្នាំ ១៩៦៩ សម្រាប់ការបង្កើតគម្រោង ARPANET ដែលដឹកនាំដោយ Robert Taylor និងគ្រប់គ្រងដោយ Lawrence Roberts ។ ARPANET បានទទួលយកបច្ចេកវិទ្យា packet-switching ដែលស្នើឡើងដោយ Davies និង Baran ដែលគាំទ្រដោយការងារគណិតវិទ្យានៅដើមទសវត្សរ៍ឆ្នាំ ១៩៧0 ដោយ Leonard Kleinrock នៅ UCLA ។ បណ្តាញផ្លាស់ប្តូរកញ្ចប់ព័ត៌មានដំបូងជាច្រើនបានលេចចេញនៅក្នុងទសវត្សរ៍ឆ្នាំ ១៩៧0 ដែលបានស្រាវជ្រាវ និងផ្តល់បណ្តាញទិន្នន័យ។ គម្រោង ARPA ក្រុមការងារ អន្តរជាតិ និងគំនិតផ្តួចផ្តើមពាណិជ្ជកម្មបាននាំទៅដល់ការបង្កើតស្តង់ដារ និងពិធីការផ្សេងៗសម្រាប់ការងារអ៊ីនធឺណិត ដែលបណ្តាញដាច់ដោយឡែកជាច្រើនអាចត្រូវបានភ្ជាប់ជា បណ្តាញៗ។ លោក Bob Kahn នៅ ARPA និង Vint Cerf នៅសាកលវិទ្យាល័យ Stanford បានបោះពុម្ពផ្សាយការស្រាវជ្រាវក្នុងឆ្នាំ ១៩៧៤ ដែលបានវិវត្តទៅជាពិធីសារត្រួតពិនិត្យការបញ្ជូន (TCP) និងពិធីការអ៊ីនធឺណិត (IP) ដែលជាពិធីការទាំងពីរនៃឈុតពិធីការអ៊ីនធឺណិត។ ការចនារួមបញ្ចូលគំនិតពីគម្រោង CYCLADES របស់បារាំងដែលដឹកនាំដោយ Louis Pouzin ។ នៅដើមទសវត្សរ៍ឆ្នាំ ១៩៨0 មូលនិធិវិទ្យាសាស្ត្រជាតិ (NSF) បានផ្តល់មូលនិធិដល់មជ្ឈមណ្ឌលកុំព្យូទ័រទំនើបជាតិនៅសាកលវិទ្យាល័យជាច្រើននៅសហរដ្ឋអាមេរិក។ វាបានផ្តល់ការភ្ជាប់ទំនាក់ទំនងគ្នានៅក្នុងឆ្នាំ ១៩៨៦ ជាមួយនឹងគម្រោង NSFNET ដូច្នេះការបង្កើតបណ្តាញចូលទៅកាន់គេហទំព័រកុំព្យូទ័រទំនើបទាំងនេះសម្រាប់ការស្រាវជ្រាវ និងអង្គការសិក្សានៅសហរដ្ឋអាមេរិក។ ការតភ្ជាប់អន្តរជាតិទៅនឹង NSFNET ការលេចឡើងនៃស្ថាបត្យកម្មដូចជា Domain Name System និងការទទួលយក TCP/IP ជាអន្តរជាតិនៅលើបណ្តាញដែលមានស្រាប់បានសម្គាល់ការចាប់ផ្តើមនៃអ៊ីនធឺណិត។ ក្រុមហ៊ុនផ្តល់សេវាអ៊ីនធឺណិតពាណិជ្ជកម្ម (ISP) បានលេចឡើងនៅឆ្នាំ ១៩៨៩ នៅសហរដ្ឋអាមេរិក និងអូស្ត្រាលី។

ARPANET ត្រូវបានបញ្ឈប់នៅឆ្នាំ ១៩៩0 ។ ការតភ្ជាប់ឯកជនមានកម្រិតទៅផ្នែកខ្លះនៃអ៊ីនធឺណិតដោយអង្គភាពពាណិជ្ជកម្មជាផ្លូវការបានលេចឡើងនៅក្នុងទីក្រុងមួយចំនួនរបស់អាមេរិកនៅចុងឆ្នាំ ១៩៨៩ និង ១៩៩0។ ឆ្អឹងខ្នងអ៊ុបទិកនៃ NSFNET ត្រូវបានបញ្ឈប់នៅឆ្នាំ ១៩៩៥ ដោយដក

ចេញនូវការដាក់ជាកំហិតចុងក្រោយលើការប្រើប្រាស់អ៊ីនធឺណិតដើម្បីដឹកជញ្ជូនពាណិជ្ជកម្មជាចរាចរ ណ៍។ បានប្តូរទៅបណ្តាញអុបទិកដែលគ្រប់គ្រងដោយ Sprint, MCI និង AT&T ។ ជីតានៃអ៊ីនធឺណិត គឺជាបណ្តាញមួយដែលត្រូវបានបង្កើតឡើងដោយក្រសួងការពារជាតិសហរដ្ឋអាមេរិក (DOD) ។ ការងារសម្រាប់បង្កើតបណ្តាញបានចាប់ផ្តើមនៅដើមទសវត្សរ៍ឆ្នាំ ១៩៦០ ហើយ DOD បានឧបត្ថម្ភ ការងារស្រាវជ្រាវសំខាន់ៗ ដែលបណ្តាលឱ្យមានការបង្កើតពិធីការដំបូង ភាសា និងក្របខ័ណ្ឌសម្រាប់ ទំនាក់ទំនងបណ្តាញ។ វាមានថ្នាំងបួននៅសាកលវិទ្យាល័យកាលីហ្វ័រញ៉ានៅឡូសអេនជឺលេស (UCLA) វិទ្យាស្ថានស្រាវជ្រាវស្ទែនហ្វដ (SRI) សាកលវិទ្យាល័យកាលីហ្វ័រញ៉ានៅសាន់តាបាបាវ៉ា (UCSB) និងសាកលវិទ្យាល័យយូថាហ៍។ នៅថ្ងៃទី ២៩ ខែតុលា ឆ្នាំ ១៩៦៩ សារដំបូងត្រូវបានផ្លាស់ ប្តូររវាង UCLA និង SRI ។ អ៊ីមែលត្រូវបានបង្កើតឡើងដោយ Roy Tomlinson ក្នុងឆ្នាំ ១៩៧២ នៅ Bolt Beranek និង Newman, Inc. (BBN) បន្ទាប់ពី UCLA ត្រូវបានភ្ជាប់ទៅ BBN ។

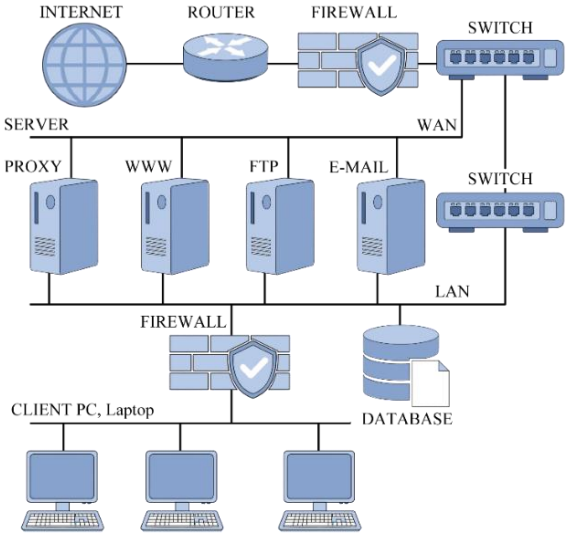
១.៤.១ អ៊ីនធឺណិត

អ៊ីនធឺណិត គឺជាប្រព័ន្ធសកលនៃបណ្តាញកុំព្យូទ័រដែលភ្ជាប់គ្នាទៅវិញទៅមក ដែលប្រើឈុត ពិធីការអ៊ីនធឺណិត (TCP/IP) ដើម្បីទំនាក់ទំនងរវាងបណ្តាញ និងឧបករណ៍។ វាគឺជាបណ្តាញដែលរួម មានបណ្តាញឯកជន សាធារណៈ ការសិក្សា អាជីវកម្ម និងបណ្តាញរដ្ឋាភិបាលនៃវិសាលភាពក្នុងមូល ដ្ឋានដល់សកលលោក ដែលភ្ជាប់ដោយអារេទូលំទូលាយនៃបច្ចេកវិទ្យា បណ្តាញអេឡិចត្រូនិច ឥត ខ្សែ និងអុបទិក។ អ៊ិនធឺណិតផ្តុំនូវធនធានព័ត៌មាន និងសេវាកម្មជាច្រើនដូចជា ឯកសារ និងកម្មវិធី ដែលមានតំណភ្ជាប់ខ្ពស់នៃវើលវ៉ាយវើប (WWW) សំបុត្រអេឡិចត្រូនិច ទូរស័ព្ទ និងការចែករំលែកឯក សារ។

ប្រភពដើមអ៊ិនធឺណិតមានតាំងពីការអភិវឌ្ឍន៍នៃការផ្លាស់ប្តូរកញ្ចប់ព័ត៌មាន និងការស្រាវជ្រាវ ដែលធ្វើឡើងដោយក្រសួងការពារជាតិសហរដ្ឋអាមេរិកក្នុងទសវត្សរ៍ឆ្នាំ ១៩៦០ ដើម្បីបើកការចែក រំលែកពេលវេលានៃកុំព្យូទ័រ។ បណ្តាញបុព្វបទចម្បង ARPANET ដំបូងឡើយបានបម្រើការជាឆ្អឹងខ្នង សម្រាប់ការតភ្ជាប់គ្នាទៅវិញទៅមកនៃបណ្តាញសិក្សាថ្នាក់តំបន់ និងបណ្តាញយោធានៅក្នុងទសវត្សរ៍ ឆ្នាំ ១៩៧០ ។ ការផ្តល់មូលនិធិនៃបណ្តាញមូលនិធិវិទ្យាសាស្ត្រជាតិជាឆ្អឹងខ្នងថ្មីនៅក្នុងទសវត្សរ៍ឆ្នាំ ១៩៨០ និងការផ្តល់មូលនិធិឯកជនសម្រាប់ការពង្រីកពាណិជ្ជកម្មផ្សេងទៀតបាននាំឱ្យមានការចូល រួមទូទាំងពិភពលោកក្នុងការអភិវឌ្ឍបច្ចេកវិទ្យាបណ្តាញថ្មី និងបណ្តាញរួមបញ្ចូលគ្នាជាច្រើន។ ការភ្ជាប់ បណ្តាញពាណិជ្ជកម្ម និង សហគ្រាសនៅដើមទសវត្សរ៍ឆ្នាំ ១៩៩០ បានសម្គាល់ការចាប់ផ្តើមនៃការ ផ្លាស់ប្តូរទៅកាន់ អ៊ីនធឺណិតទំនើប និងបង្កើតឱ្យមានការរីកចម្រើនជានិរន្តរភាព ដោយសារជំនាន់នៃ ស្ថាប័ន ផ្ទាល់ខ្លួន និងកុំព្យូទ័រចល័តត្រូវបានភ្ជាប់ទៅបណ្តាញ។ ទោះបីជាអ៊ិនធឺណិតត្រូវបានប្រើប្រាស់ យ៉ាងទូលំទូលាយដោយអ្នកសិក្សានៅក្នុងទសវត្សរ៍ឆ្នាំ ១៩៨០ ក៏ដោយ ពាណិជ្ជកម្មបានបញ្ចូលសេវា កម្ម និងបច្ចេកវិទ្យារបស់វាទៅក្នុងស្ទើរតែគ្រប់ទិដ្ឋភាពនៃជីវិតសម័យទំនើប។

ប្រព័ន្ធផ្សព្វផ្សាយទំនាក់ទំនងបែបប្រពៃណីភាគច្រើន រួមទាំងទូរស័ព្ទ វិទ្យុ ទូរទស្សន៍ សំបុត្រ ក្រដាស និងកាសែត ត្រូវបានផ្លាស់ប្តូរ កំណត់ឡើងវិញ ឬសូម្បីតែឆ្លងកាត់អ៊ីនធឺណិត ដោយ ផ្តល់

កំណើតដល់សេវាកម្មថ្មីៗដូចជា អ៊ីមែល ទូរស័ព្ទអ៊ីនធឺណិត ទូរទស្សន៍អ៊ីនធឺណិត តន្ត្រីអនឡាញ កាសែតឌីជីថល។ និងគេហទំព័រស្ត្រីមវីដេអូ កាសែត សៀវភៅ និងការបោះពុម្ពបោះពុម្ពផ្សេងទៀត កំពុងសម្របខ្លួនទៅនឹងបច្ចេកវិទ្យាគេហទំព័រ ឬត្រូវបានផ្លាស់ប្តូរទៅជាការសរសេរប្លុក មតិព័ត៌មានតាមអ៊ីនធឺណិត និងអ្នកប្រមូលព័ត៌មានតាមអ៊ីនធឺណិត។ អ៊ិនធឺណិតបានបើក និងពន្លឿនអន្តរកម្មផ្ទាល់ខ្លួនថ្មីតាមរយៈការផ្ញើសារភ្លាមៗ វេទិកា និងសេវាកម្មបណ្តាញ សង្គម ការដើរទិញទំនិញតាម អ៊ីនធឺណិត បានរីកចម្រើនយ៉ាងខ្លាំងសម្រាប់អ្នកលក់រាយធំៗ អាជីវកម្មខ្នាតតូច និងសហគ្រិន ដែលអនុញ្ញាតឱ្យក្រុមហ៊ុនពង្រីកវត្តមាន "ឥដ្ឋ និងបាយអ" របស់ពួកគេដើម្បីបម្រើទីផ្សារធំជាង ឬសូម្បីតែលក់ទំនិញ និងសេវាកម្មតាមអ៊ីនធឺណិតទាំងស្រុងអាជីវកម្មមួយទៅអាជីវកម្ម និងសេវាកម្មហិរញ្ញវត្ថុនៅលើអ៊ីនធឺណិតប៉ះពាល់ដល់ខ្សែ សង្វាក់ផ្គត់ផ្គង់នៅទូទាំងឧស្សាហកម្មទាំងមូល។



រូបភាព ១.៥ ការភ្ជាប់អ៊ីនធឺណិត

អ៊ិនធឺណិតមិនមានការគ្រប់គ្រងកណ្តាលនៅក្នុងការអនុវត្តបច្ចេកវិទ្យាឬគោលនយោបាយសម្រាប់ការចូលប្រើប្រាស់ និងការប្រើប្រាស់នោះទេ បណ្តាញធាតុផ្សំនីមួយៗកំណត់គោលការណ៍របស់វា។ និយមន័យលើសលប់នៃចន្លោះឈ្មោះសំខាន់ពីរនៅលើអ៊ីនធឺណិត អាសយដ្ឋានពិធីការអ៊ីនធឺណិត (អាសយដ្ឋាន IP) និងប្រព័ន្ធឈ្មោះដែន (DNS) ត្រូវបានដឹកនាំដោយអង្គការថៃទាំគឺ សាជីវកម្មអ៊ីនធឺណិតសម្រាប់ឈ្មោះ និងលេខដែលបានចាត់តាំង (ICANN) ។ ការគូសបញ្ជាក់ផ្នែកបច្ចេកទេសនិងស្តង់ដារនៃពិធីការស្នូល គឺជាសកម្មភាពមួយរបស់ក្រុមការងារវិស្វកម្មអ៊ីនធឺណិត (IETF) ដែលជាអង្គការមិនរកប្រាក់ចំណេញនៃអ្នកចូលរួមអន្តរជាតិដែលមានទំនាក់ទំនងធូររលុងដែលនរណាម្នាក់អាចភ្ជាប់ជា មួយដោយការរួមចំណែកជំនាញបច្ចេកទេស នៅខែវិច្ឆិកា ឆ្នាំ ២០០៦ អ៊ិនធឺណិតត្រូវបានបញ្ចូលក្នុងបញ្ជីអច្ឆរិយៈទាំងប្រាំពីរថ្មីរបស់សហរដ្ឋអាមេរិក។

ARPANET បានពង្រីកដើម្បីភ្ជាប់ DOD ជាមួយសាកលវិទ្យាល័យទាំងនោះនៃសហរដ្ឋអាមេរិកដែលកំពុងអនុវត្តការស្រាវជ្រាវដែលទាក់ទងនឹងការកំណត់វាគ្របដណ្តប់ភាគច្រើននៃសាកលវិទ្យាល័យធំៗនៅទូទាំងប្រទេស គំនិតបណ្តាញទទួលបានការជំរុញនៅពេលដែលសាកលវិទ្យាល័យ University College of London (UK) និង Royal Radar Network (Norway) បានតភ្ជាប់ទៅ ARPANET បង្កើតបានជាបណ្តាញបណ្តាញ។ ពាក្យ អ៊ីនធឺណិតត្រូវបានបង្កើតឡើងដោយ Vinton Cerf, Yogen Dalal និង Carl Sunshine នៃសាកលវិទ្យាល័យ Stanford ដើម្បីពិពណ៌នាអំពីបណ្តាញបណ្តាញនេះជាមួយគ្នាពួកគេក៏បានបង្កើតពិធីការដើម្បីសម្រួលដល់ការផ្លាស់ប្តូរព័ត៌មានតាមរយៈ អ៊ីនធឺណិត។ ពិធីសារត្រួតពិនិត្យការបញ្ជូន(TCP) នៅតែបង្កើតជាឆ្អឹងខ្នងនៃបណ្តាញ TELNET គឺជាការបន្សាំពាណិជ្ជកម្មដំបូងបង្អស់របស់ ARPANET ដែលបានណែនាំក្នុងឆ្នាំ ១៩៧៤ ជាមួយនេះគំនិតអ្នកផ្តល់សេវាអ៊ីនធឺណិត (ISP) ក៏ត្រូវបានណែនាំផងដែរ។ មុខងារចម្បងរបស់ ISP គឺផ្តល់ការភ្ជាប់អ៊ីនធឺណិតគ្មានការរំខានដល់អតិថិជនរបស់ខ្លួនក្នុងតម្លៃសមរម្យ។

១.៤.២ វើលវ៉ាយវ៉ែប

Tim Berners-Lee ជាអ្នកវិទ្យាសាស្ត្រជនជាតិអង់គ្លេសបានបង្កើត World Wide Web (WWW) ក្នុងឆ្នាំ ១៩៨៩ ពេលកំពុងធ្វើការនៅ CERN ។ គេហទំព័រត្រូវបានបង្កើតឡើងដំបូង និងបង្កើតឡើងដើម្បីបំពេញតម្រូវការសម្រាប់ការចែករំលែកព័ត៌មានដោយស្វ័យប្រវត្តិរវាងអ្នកវិទ្យាសាស្ត្រនៅតាមសាកលវិទ្យាល័យ និងវិទ្យាស្ថាននានាទូទាំងពិភពលោក។ WWW, Web, CERN50, Golden Jubilee Photos Tim Berners-Lee, រូបភាពនៅ CERN (រូបភាព: CERN) CERN មិនមែនជាមន្ទីរពិសោធន៍ដាច់ស្រយាលទេ ប៉ុន្តែជាចំណុចប្រសព្វសម្រាប់សហគមន៍ទូលំទូលាយដែលរួមបញ្ចូលអ្នកវិទ្យាសាស្ត្រជាង ១៧000នាក់មកពីជាង ១00 ប្រទេស។ ទោះបីជាជាធម្មតាពួកគេចំណាយពេលខ្លះនៅលើគេហទំព័រ CERN ក៏ដោយ អ្នកវិទ្យាសាស្ត្រជាធម្មតាធ្វើការនៅសាកលវិទ្យាល័យ និងមន្ទីរពិសោធន៍ជាតិនៅក្នុងប្រទេសកំណើតរបស់ពួកគេ។ ដូច្នេះ ឧបករណ៍ទំនាក់ទំនងដែលអាចទុកចិត្តបានគឺចាំបាច់ណាស់គំនិតជាមូលដ្ឋាននៃ WWW គឺដើម្បីបញ្ចូលគ្នានូវបច្ចេកវិទ្យាវិវត្តនៃកុំព្យូទ័រ បណ្តាញទិន្នន័យ និង hypertext ទៅជាប្រព័ន្ធព័ត៌មានសកលដ៏មានឥទ្ធិពល និងងាយស្រួលប្រើ។

ជាមួយនឹងការធ្វើពាណិជ្ជកម្មនៃអ៊ីនធឺណិត បណ្តាញកាន់តែច្រើនឡើងត្រូវបានបង្កើតឡើងនៅក្នុងផ្នែកផ្សេងៗនៃពិភពលោក បណ្តាញនីមួយៗបានប្រើពិធីការផ្សេងទៀតសម្រាប់ការទំនាក់ទំនងតាមបណ្តាញនេះបានរារាំងបណ្តាញផ្សេងៗពីការភ្ជាប់យ៉ាងរលូន។ នៅទសវត្សរ៍ឆ្នាំ ១៩៨0 លោក Tim Berners-Lee បានដឹកនាំក្រុមអ្នកវិទ្យាសាស្ត្រកុំព្យូទ័រនៅ CERN ប្រទេសស្វីស ដើម្បីបង្កើតបណ្តាញបណ្តាញជាច្រើនដែលហៅថា World Wide Web (WWW) ។ វើលវ៉ាយវ៉ែប គឺជាគេហទំព័រដ៏ស្មុគស្មាញនៃគេហទំព័រ និងទំព័រដែលតភ្ជាប់តាម រយៈអត្ថបទខ្ពស់ Hypertext គឺជាពាក្យ ឬក្រុមនៃពាក្យដែលភ្ជាប់ទៅកាន់ទំព័របណ្តាញផ្សេងទៀតនៃគេហទំព័រដូចគ្នា ឬផ្សេងគ្នានៅពេលចុច hypertext នោះទំព័របណ្តាញមួយទៀតនឹងបើក។ ការវិវត្តន៍ពី ARPANET ទៅ WWW គឺអាចធ្វើទៅបាន

ដោយសារតែសមិទ្ធិផលថ្មីៗជាច្រើនដោយអ្នកស្រាវជ្រាវ និងអ្នកវិទ្យាសាស្ត្រកុំព្យូទ័រទូទាំងពិភពលោក នេះគឺជាការវិវត្តន៍មួយចំនួន។

ឆ្នាំ	ចំណុចសំខាន់
១៩៥៧	ទីភ្នាក់ងារគម្រោងស្រាវជ្រាវកម្រិតខ្ពស់ បង្កើតឡើងដោយសហរដ្ឋអាមេរិក
១៩៦៩	ARPANET បានក្លាយជាមុខងារ
១៩៧០	ARPANET បានភ្ជាប់ទៅ BBNs
១៩៧២	Roy Tomlinson បង្កើតការផ្ញើសារតាមបណ្តាញ ឬអ៊ីមែល។ និមិត្តសញ្ញា @ មកមានន័យថា "នៅ"
១៩៧៣	APRANET បានភ្ជាប់ទៅ Royal Radar Network នៃប្រទេសន័រវេស
១៩៧៤	ពាក្យ អ៊ិនធឺណិត បង្កើត ការប្រើប្រាស់ពាណិជ្ជកម្មដំបូងរបស់ ARPANET, Telenet, ត្រូវបានអនុម័ត
១៩៨២	TCP/IP ត្រូវបានណែនាំជាពិធីការស្តង់ដារនៅលើ ARPANET
១៩៨៣	ប្រព័ន្ធឈ្មោះដែនត្រូវបានណែនាំ
១៩៨៦	មូលនិធិវិទ្យាសាស្ត្រជាតិនាំមកនូវការតភ្ជាប់ទៅកាន់មនុស្សកាន់តែច្រើនជាមួយនឹងកម្មវិធី NSFNET របស់ខ្លួន។
១៩៩០	ARPANET ត្រូវបានបញ្ឈប់ កម្មវិធីរុករកបណ្តាញដំបូង Nexus ត្រូវបានបង្កើតឡើង HTML ត្រូវបានបង្កើតឡើង
២០០២-២០០៤	គេហទំព័រ 2.0 បានកើតឡើង

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះ អ្នកបានរៀនដូចខាងក្រោម៖

គំរូយោង TCP/IP គឺជាឈុតបួនស្រទាប់នៃពិធីការទំនាក់ទំនងវាត្រូវបានបង្កើតឡើងដោយ DoD (នាយកដ្ឋានការពារជាតិ) ក្នុងទសវត្សរ៍ឆ្នាំ ១៩៦០។ វាត្រូវបានដាក់ឈ្មោះតាមពិធីការសំខាន់ពីរដែលប្រើក្នុងគំរូគឺ TCP និង IP ។ TCP តំណាងឱ្យពិធីសារត្រួតពិនិត្យការបញ្ជូន ហើយ IP តំណាងឱ្យពិធីការអ៊ីនធឺណិត។

ស្រទាប់ទាំងបួននៅក្នុងឈុតពិធីការ TCP/IP គឺ៖

- **Network Layer ៖** គឺជាស្រទាប់ទាបបំផុតដែលទាក់ទងនឹងការបញ្ជូនទិន្នន័យ TCP/IP មិនកំណត់យ៉ាងច្បាស់នូវពិធីការណាមួយនៅទីនេះទេប៉ុន្តែគាំទ្រពិធីការស្តង់ដារ។
- **Internet Layer ៖** វាកំណត់ពិធីការសម្រាប់ការបញ្ជូនទិន្នន័យឡូជីខលតាមបណ្តាញ។ ពិធីការចម្បងនៅក្នុងស្រទាប់នេះគឺ ពិធីការអ៊ីនធឺណិត (IP) ដែលត្រូវបានគាំទ្រដោយពិធីការ ICMP, IGMP, RARP និង ARP ។
- **Transport Layer ៖** វាទទួលខុសត្រូវចំពោះការចែកចាយទិន្នន័យពីចុងដល់ចុងដោយគ្មានកំហុស។ ពិធីសារត្រួតពិនិត្យការបញ្ជូន (TCP) និង ពិធីការ ដែលតាក្រាម អ្នកប្រើប្រាស់ (UDP) គឺជាពិធីការ។
- **Application Layer ៖** គឺជាស្រទាប់កំពូលបំផុត និងកំណត់ចំណុចប្រទាក់នៃកម្មវិធីម៉ាស៊ីនជាមួយសេវាកម្មស្រទាប់ដឹកជញ្ជូន។ ស្រទាប់នេះរួមបញ្ចូលពិធីការកម្រិតខ្ពស់ទាំងអស់ដូចជា Telnet, DNS, HTTP, FTP, SMTP ។ល។
- **ម៉ូដែល OSI** គឺជាគំរូទូទៅដែលផ្អែកលើមុខងាររបស់ស្រទាប់នីមួយៗ គំរូ TCP/IP គឺជាស្តង់ដារដែលតម្រង់ទិសពិធីការ។
- គំរូ OSI បែងចែកគោលគំនិតទាំងបី៖ សេវាកម្ម ចំណុចប្រទាក់ និងពិធីការ TCP/IP មិនមានភាពខុសគ្នាច្បាស់លាស់រវាងទាំងបីនេះទេ។
- នៅក្នុង OSI គំរូត្រូវបានបង្កើតឡើងដំបូង ហើយបន្ទាប់មកពិធីការនៅក្នុងស្រទាប់នីមួយៗត្រូវបានបង្កើតឡើង។ ពិធីការត្រូវបានបង្កើតឡើងនៅក្នុងឈុត TCP/IP ដំបូង ហើយបន្ទាប់មកគំរូត្រូវបានបង្កើត។

សំណួរ

១. តើ OSI Model ជាអ្វី?

២. តើអ្វីជា TCP/IP Model?

៣. តើអ៊ីនធឺណិតជាអ្វី?

៤. តើអ្វីជាភាពខុសគ្នារវាង OSI និង TCP/IP?

៥. ចូរពន្យល់ពីគុណសម្បត្តិ និងគុណវិបត្តិនៃ OSI Model ។

ការអនុវត្តន៍ទី១

ក. ការណែនាំអំពីការក្លែងធ្វើកញ្ចប់បណ្តាញ

ការអនុវត្តនេះពិតជាប្រើម៉ាស៊ីនក្លែងធ្វើបណ្តាញដើម្បីធ្វើការស្រមៃមើលការគ្រប់គ្រងនៃកញ្ចប់ព័ត៌មានបណ្តាញ និងការអនុវត្ត និងប្រតិបត្តិការរួមបញ្ចូលគ្នានៃឧបករណ៍ផ្សេងៗយើងប្រើក្នុងកម្មវិធី Packet Tracer ដែលជាកម្មវិធីក្លែងធ្វើបណ្តាញនិម្មិត។

ខ. គោលបំណងនៃការអនុវត្តនេះ

- ឱ្យយើងស្គាល់ Packet Tracer
- ឱ្យយើងចេះដំឡើងកម្មវិធី Packet Tracer
- ឱ្យយើងប្រើមុខងារសាមញ្ញមួយចំនួនរបស់ Packet Tracer

គ. តើអ្វីទៅជាកញ្ចប់តាមដាន ?

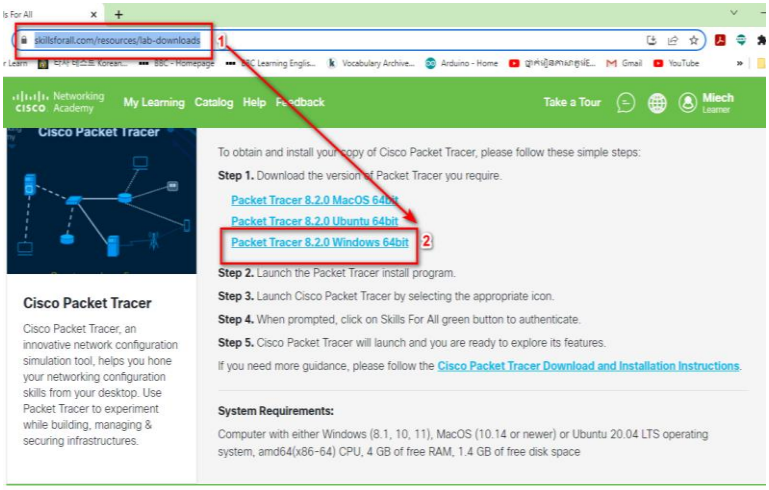
Packet Tracer គឺជាឧបករណ៍ក្លែងធ្វើរ៉ោតទ័ររបស់ក្រុមហ៊ុន Cisco ដែលអាចត្រូវបានប្រើសម្រាប់ការអប់រំការអនុវត្ត និងការស្រាវជ្រាវសម្រាប់ការក្លែងធ្វើបណ្តាញកុំព្យូទ័រ ដ៏សាមញ្ញ។ ឧបករណ៍នេះត្រូវបានបង្កើតឡើងដោយ Cisco Systems ហើយត្រូវបានចែកចាយ និងផ្តល់ជូនដោយឥតគិតថ្លៃដល់គ្រូបង្រៀន និងសិស្សដែលមាន ឬបានចូលរួមនៅក្នុង Cisco Networking Academy ។

គោលបំណងចម្បងនៃ Cisco Packet Tracer គឺដើម្បីជួយសិស្សឱ្យរៀនពីគោលការណ៍នៃការតភ្ជាប់បណ្តាញជាមួយនឹងបទពិសោធន៍ប្រើប្រាស់ដៃ និងអភិវឌ្ឍជំនាញជាក់លាក់នៃបច្ចេកវិទ្យា Cisco ដោយសារពិធីការគឺសម្រាប់តែកម្មវិធីប៉ុណ្ណោះ ឧបករណ៍នេះមិនអាចជំនួសរ៉ោតទ័រ ឬឧបករណ៍ប្តូរផ្នែករឹងបានទេ។ គួរឱ្យចាប់អារម្មណ៍ ឧបករណ៍នេះមិនត្រឹមតែរួមបញ្ចូលផលិតផល Cisco ប៉ុណ្ណោះទេ ប៉ុន្តែក៏មានឧបករណ៍បណ្តាញជាច្រើនទៀតផងដែរ។ ឧបករណ៍នេះត្រូវបានលើកទឹកចិត្តយ៉ាងទូលំទូលាយព្រោះវាជាផ្នែកមួយនៃកម្មវិធីសិក្សាដូចជា CCNA និង CCENT ដែលមហាវិទ្យាល័យប្រើប្រាស់ Packet Tracer ដើម្បីបង្ហាញពីគំនិតបច្ចេកទេស និងប្រព័ន្ធបណ្តាញ សិស្សបំពេញកិច្ចការដោយប្រើឧបករណ៍នេះ ធ្វើការដោយឯករាជ្យ ឬជាក្រុម។

១. របៀបដំឡើង Packet Tracer?

ចូលទៅកាន់គេហទំព័រដើមរបស់កម្មវិធី Packet Tracer បន្ទាប់មកអ្នកអាចទាញយក កម្មវិធីពី តំណលើងខាងក្រោមនេះ https://skillsforall.com/resources/lab-downloads ដោយចុច លើក្រាហ្វិច Packet Tracer ហើយជ្រើសរើសកញ្ចប់ OS ដែលសមស្របជាមួយ កុំព្យូទ័ររបស់អ្នក ហើយប្រសិនបើកាន់ទេច្បាស់ទៀតអអ្នកអាចចូលមើលវីដេអូដែលតាមរយៈតំណលើងខាងក្រោមនេះ https://youtu.be/6qGraARASu0 ។

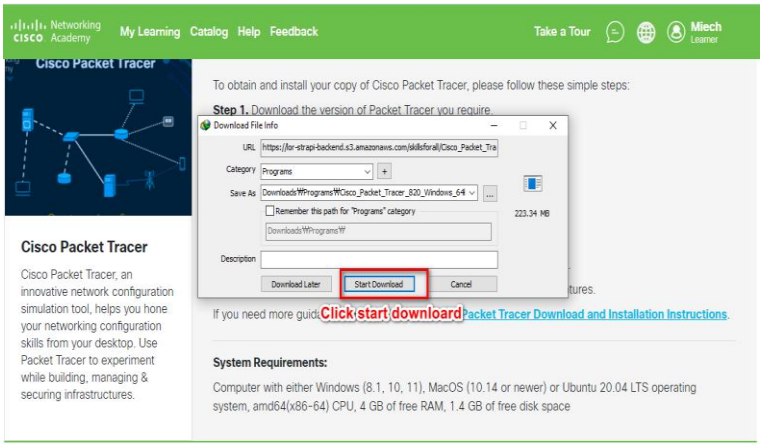
២. ការយទាញយកកម្មវិធី packet tracer 8.2.0



ក. បើកកម្មវិធីរុករកតាមអ៊ីនធឺណិត

ខ. ចូលទៅកាន់ https://skillsforall.com/resources/lab-download

គ. ចុចលើ Packet tracer 8.2.0 Windows

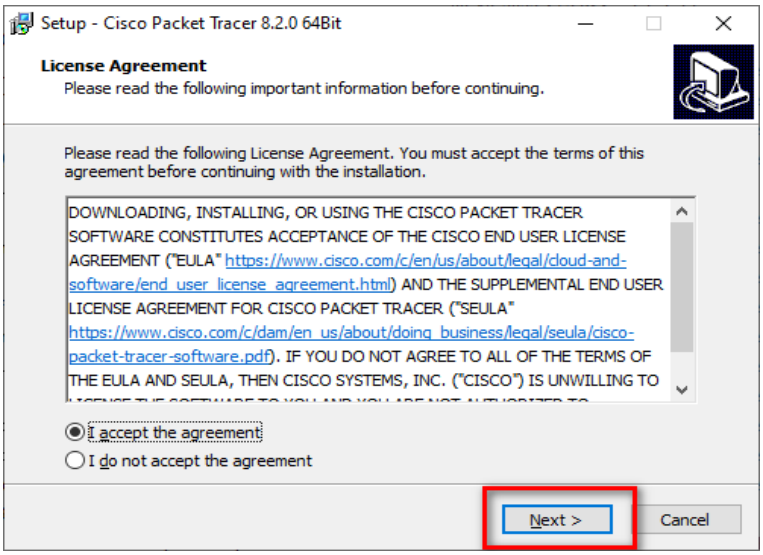


ឃ. ចុចពាក្យចាប់ផ្តើមទាញយក

ង. ស្វែងរកទីតាំងដើម្បីរក្សាទុកក្នុងកុំព្យូទ័ររបស់អ្នក

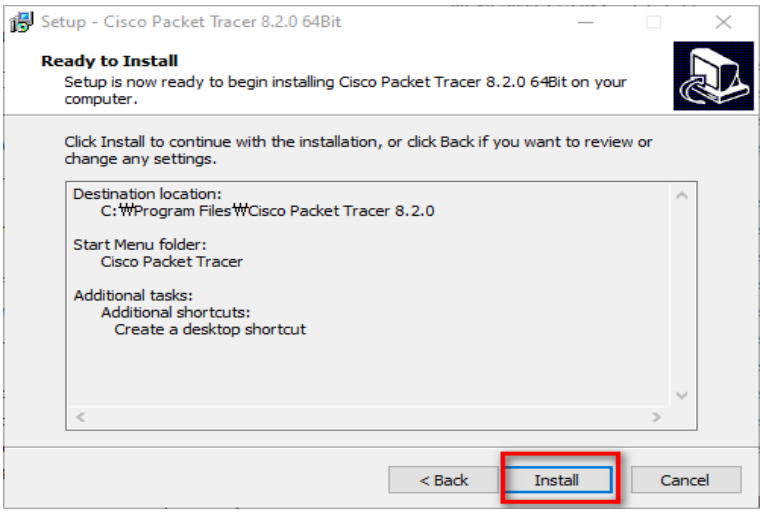
ឆ. ចុចរក្សាទុក

៣. ការដំឡើងកម្មវិធី Cisco Packet Tracer



ក.ធីកលើប្រអប់ ខ្ញុំទទួលយកកិច្ចព្រមព្រៀង

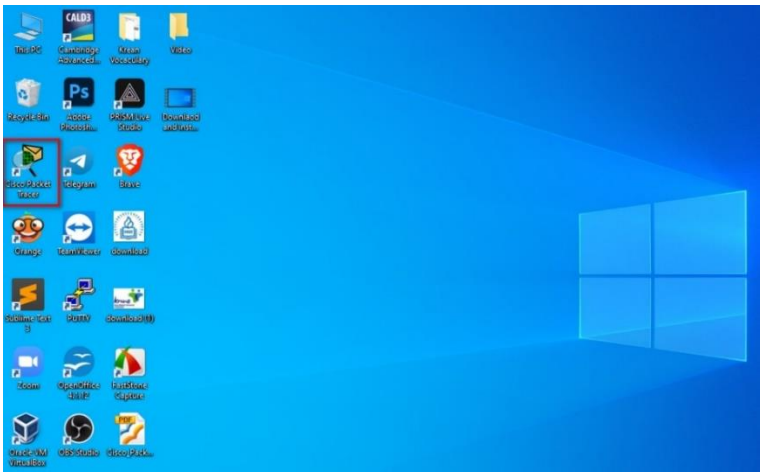
ខ. ចុចលើ បន្ទាប់→បន្ទាប់→បន្ទាប់→បន្ទាប់



គ. ចុចដំឡើង

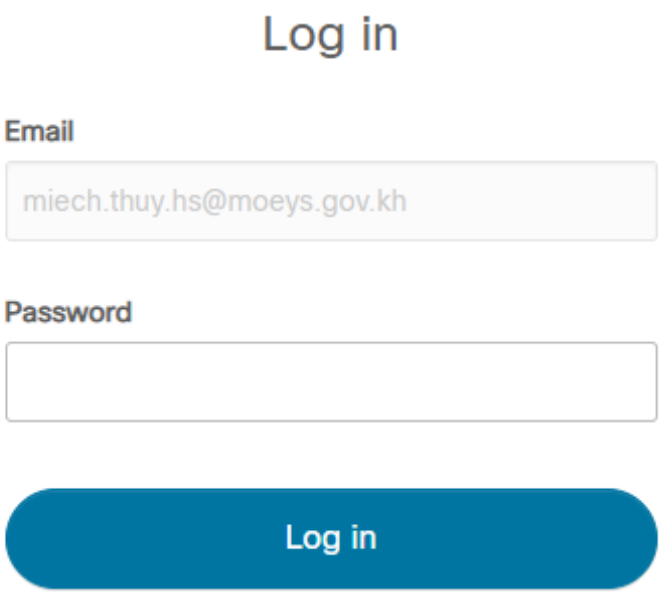
ឃ.ចុចពាក្យ បញ្ចប់

៤. ការបើកកម្មវិធីប្រើប្រាស់ Cisco Packet Tracer



ក. ចុចស្ទួនពីរដងលើរូបតំណាង Cisco Packet Tracer

ខ. ឬក៏ចុចប៊ូតុងចាប់ផ្តើមហើយស្វែងរក Cisco Packet Tracer



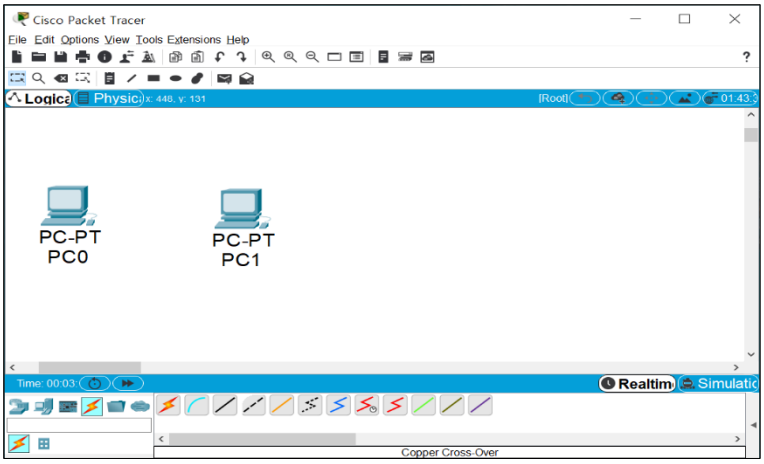
គ. ចូលគណនី Gmail និងពាក្យសម្ងាត់ដែលបានចុះឈ្មោះជាមួយកម្មវិធី

ឃ. អ្នកត្រូវតែចុះឈ្មោះនៅលើគេហទំព័រ Cisco មុនពេលចូល

ង. ពេលបំពេញរួចរាល់ចុច ចូលជាការស្រេច

៥. របៀបបង្កើតបណ្តាញដោយប្រើ Packet Tracer?

៥.១. ការបន្ថែមឧបករណ៍ PC



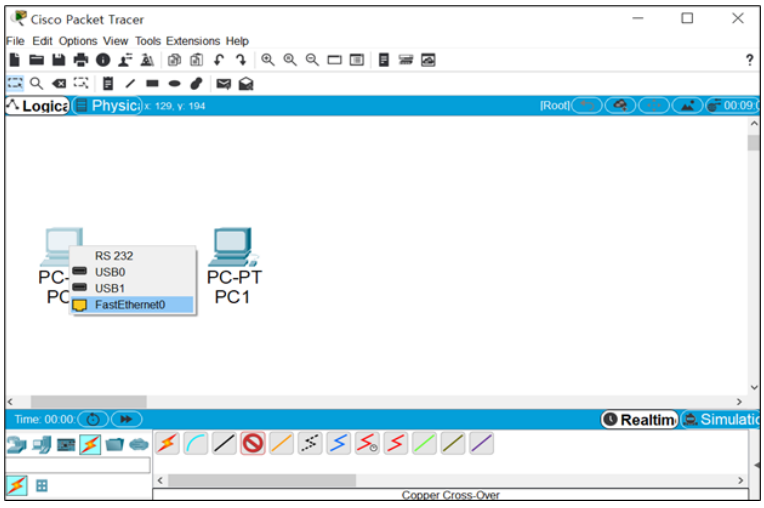
ក. ចុចលើ៖ [ឧបករណ៍បញ្ចប់ Device PC0]

ខ. ចុចលើ៖ [ឧបករណ៍បញ្ចប់ (Device PC1)]

គ. ចុចលើ 'PC' ហើយអូសទម្លាក់

ឃ. បន្ថែម 'PC' មួយទៀត

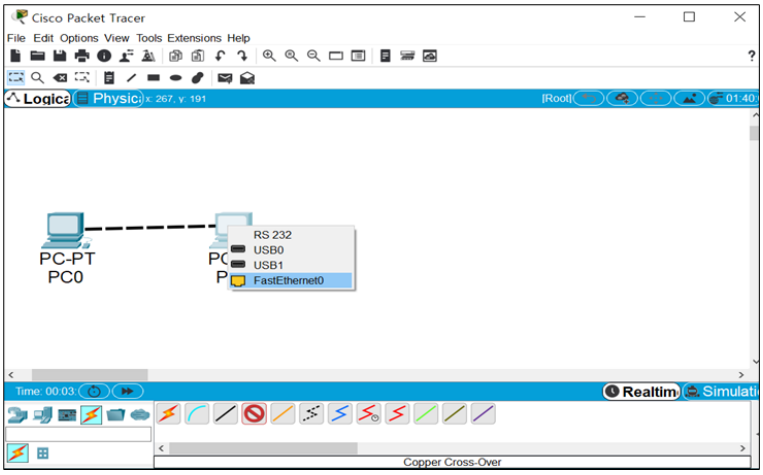
៥.២. ជ្រើសរើសខ្សែ ពីកុំព្យូទ័រមួយ ទៅកុំព្យូទ័រមួយទៀត



ក. ចុចកណ្តុរខាងឆ្វេងលើ៖ 'PC0'

ខ. ជ្រើសរើសខ្សែ(Cropper Cross-Over)

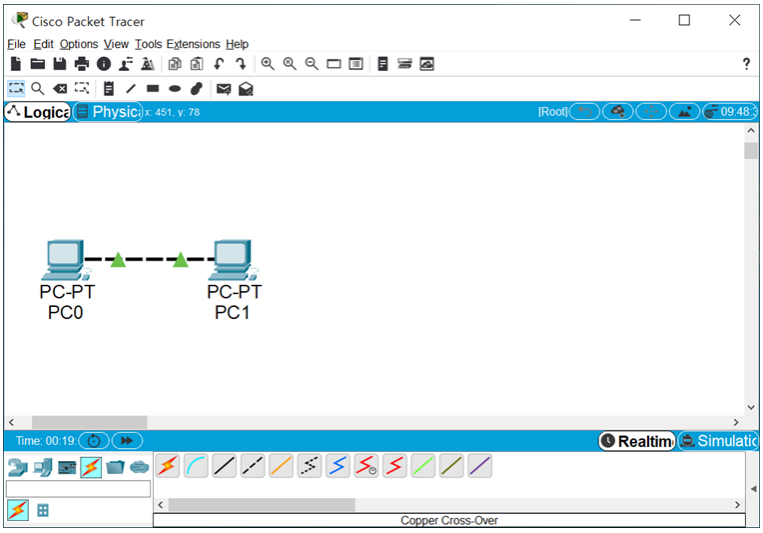
គ. ជ្រើសរើសយក [FastEthernet0]



ឃ.ចុចកណ្តុរខាងឆ្វេងលើ៖ 'PC1'

ង. ជ្រើសរើសយក [FastEthernet0]

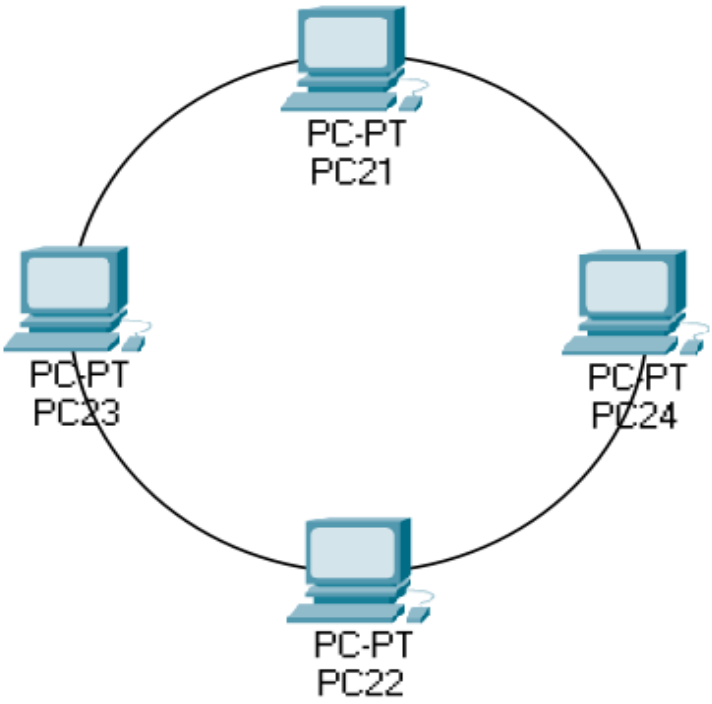
៦.លទ្ធផលបណ្តាញមូលដ្ឋានត្រូវបានបង្ហាញដូចខាងក្រោម



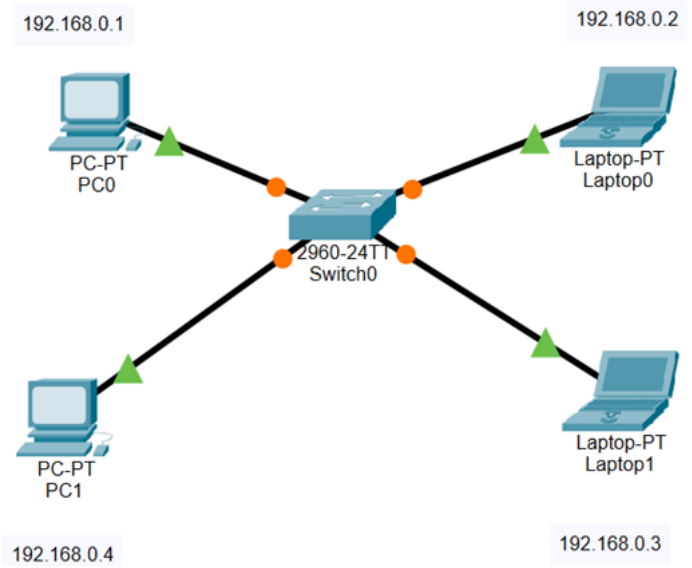
ឃ. កិច្ចការស្រាវជ្រាវ

ប្រើកម្មវិធី Packet Tracer ហើយសាកល្បងមុខងារតភ្ជាប់ដូចរូបខាងក្រោម

កិច្ចការទី១៖ បង្កើតរចនាសម្ព័ន្ធ Ring Topology សេរសេរពិព័រណ៌នាអំពីដំណាក់កាល និងជំហានសម្រាប់បង្កើតរចនាសម្ព័ន្ធ Ring Topology ដូចរូបខាងក្រោមនេះ។



កិច្ចការទី២៖ បង្កើតយរចនាសម្ព័ន្ធ Star Topology សរសេរពិព័រណ៌នាអំពី ដំណាក់កាល និងជំហានសម្រាប់បង្កើតរចនាសម្ព័ន្ធ Star Topology ដូចរូបខាងក្រោមនេះ។



ជំពូកទី២
ប្រភេទនៃបណ្តាញកុំព្យូទ័រ

បណ្តាញកុំព្យូទ័រគឺជាក្រុមនៃប្រព័ន្ធកុំព្យូទ័រដែលមានទំនាក់ទំនងគ្នាពីរ ឬច្រើនដែលប្រើពិធីការភ្ជាប់ស្តង់ដារ សម្រាប់ការចែករំលែកធនធាន និងឯកសារផ្សេងៗ អ្នកអាចបង្កើតការភ្ជាប់បណ្តាញកុំព្យូទ័រដោយប្រើខ្សែ ឬប្រព័ន្ធ ផ្សព្វផ្សាយឥតខ្សែហើយបណ្តាញនីមួយៗពាក់ព័ន្ធនឹង ផ្នែករឹង និងផ្នែកទន់ ដែលភ្ជាប់កុំព្យូទ័រ និងឧបករណ៍។

- LAN (បណ្តាញក្នុងតំបន់)
- PAN (បណ្តាញតំបន់ផ្ទាល់ខ្លួន)
- MAN (បណ្តាញតំបន់ទីក្រុង)
- WAN (បណ្តាញតំបន់ធំទូលាយ)

ជំពូកទី២ នេះអ្នកនឹងរៀនអំពី៖

២.១ ក្បួនតបណ្តាញ

២.២ ប្រភេទនៃបណ្តាញកុំព្យូទ័រ

២.៣ ពិធីការបណ្តាញ

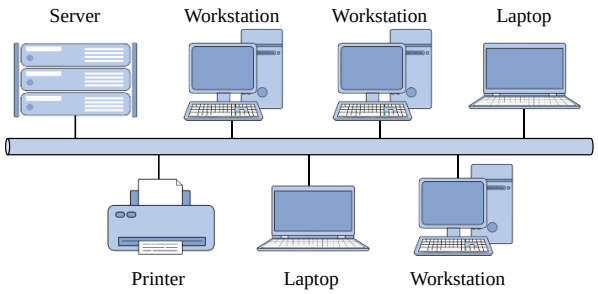
២.១ ក្បួនតបណ្តាញ

បន្ទាប់ពីការកំណត់បណ្តាញនៅក្នុងផ្នែកមុន និងពិភាក្សាអំពីរចនាសម្ព័ន្ធរូបវន្តរបស់ពួកគេយើងត្រូវពិភាក្សាអំពីប្រភេទនៃបណ្តាញដែលយើងជួបប្រទះសព្វថ្ងៃនេះ។ លក្ខណៈវិនិច្ឆ័យសម្រាប់ការបែងចែកប្រភេទនៃបណ្តាញមួយពីបណ្តាញមួយផ្សេងទៀតគឺស្មុគស្មាញហើយជួនកាលមានការភ័ន្តច្រឡំ។ យើងប្រើប្រាស់ទំហំ ការគ្របដណ្តប់ភូមិសាស្ត្រ និងតម្រូវការកម្មសិទ្ធិដើម្បីធ្វើឱ្យមានភាពខុសគ្នានេះ។ បន្ទាប់ពីពិភាក្សាអំពីបណ្តាញពីរប្រភេទគឺ LANs និង WANs យើងកំណត់ការប្តូរ ដែលភ្ជាប់បណ្តាញដើម្បីបង្កើតការងារអ៊ីនធឺណិត (បណ្តាញនៃបណ្តាញ) ។ របៀបដែលឧបករណ៍ត្រូវបានតភ្ជាប់គ្នាទៅវិញទៅមកក្នុងការបង្កើតបណ្តាញមួយត្រូវបានគេហៅថា **ក្បួនតបណ្តាញ** ។ កត្តាមួយចំនួនដែលប៉ះពាល់ដល់ជម្រើសនៃ ក្បួនតសម្រាប់បណ្តាញគឺ

- **ថ្លៃដើម៖** ថ្លៃដើមនៃការដំឡើងគឺជាកត្តាសំខាន់ក្នុងការចំណាយសរុបនៃការរៀបចំហេដ្ឋារចនាសម្ព័ន្ធដូច្នេះ ហើយយើងត្រូវសិក្សាពី ប្រវែងខ្សែ ចម្ងាយរវាងថ្នាំង ទីតាំងរបស់ម៉ាស៊ីនមេ ត្រូវតែគិតគូរនៅពេលរចនាបណ្តាញ។
- **ភាពបត់បែន៖** ក្បួនតនៃបណ្តាញគួរតែអាចបត់បែនបានគ្រប់គ្រាន់ដើម្បីអនុញ្ញាតឱ្យមានការកំណត់រចនាសម្ព័ន្ធឡើងវិញនៃការរៀបចំការិយាល័យ ការបន្ថែមថ្នាំងថ្មី និងការផ្លាស់ប្តូរទីតាំងនៃថ្នាំងដែលមានស្រាប់។
- **ភាពអាចជឿជាក់បាន៖** បណ្តាញគួរតែត្រូវបានរចនាឡើងតាមរបៀបដែលវាមានពេលវេលារងចាំអប្បបរមា ការបរាជ័យនៃថ្នាំងមួយ ឬផ្នែកខ្សែមួយមិនគួរធ្វើឱ្យបណ្តាញទាំងមូលគ្មានប្រយោជន៍ទេ។
- **លទ្ធភាពធ្វើមាត្រដ្ឋាន៖** ក្បួនតបណ្តាញគួរតែអាចធ្វើជាមាត្រដ្ឋានបាន ពោលគឺ វាអាចផ្ទុកឧបករណ៍ និងថ្នាំងថ្មីដោយគ្មានការធ្លាក់ចុះនៃការអនុវត្ត។
- **ភាពងាយស្រួលនៃការដំឡើង៖** បណ្តាញគួរតែមានភាពងាយស្រួលក្នុងការដំឡើងទាក់ទងនឹងតម្រូវការផ្នែករឹង កម្មវិធី និងបុគ្គលិកបច្ចេកទេស។
- **ភាពងាយស្រួលនៃការថែទាំ៖** ការដោះស្រាយបញ្ហា និងការថែទាំបណ្តាញគួរតែងាយស្រួល។

២.១.១ Bus Topology

បណ្តាញទិន្នន័យដែលមាន Bus Topology មានខ្សែបញ្ជូនលីនេអ៊ែរជាធម្មតាខ្សែកូស៊ីល (coaxial) ដែលឧបករណ៍បណ្តាញ និងស្ថានីយការងារជាច្រើនត្រូវបានភ្ជាប់តាមប្រវែងម៉ាស៊ីនមេគឺនៅចុងម្ខាងនៃឡានក្រុង។ នៅពេលដែលស្ថានីយការងារត្រូវតែផ្ញើទិន្នន័យ វាបញ្ជូនកញ្ចប់ព័ត៌មានដែលមានអាសយដ្ឋានទិសដៅនៅក្នុងបឋមកថារបស់វាតាម Bus Topology។



រូបភាព ២.១ Bus Topology

ទិន្នន័យធ្វើដំណើរក្នុងទិសដៅទាំងពីរតាមឡានក្រុងនៅពេលដែលស្ថានីយគោលដៅមើលឃើញទិន្នន័យ វាចម្លងវាទៅថាសមូលដ្ឋាន។

អត្ថប្រយោជន៍នៃ Bus Topology

ទាំងនេះគឺជាគុណសម្បត្តិនៃការប្រើប្រាស់ Bus Topology៖

- ងាយស្រួលក្នុងការតំឡើង និងថែទាំ
- វាអាចត្រូវបានពង្រីកយ៉ាងងាយស្រួល
- អាចទុកចិត្តបានខ្លាំងណាស់ ដោយសារខ្សែបញ្ជូនតែមួយ

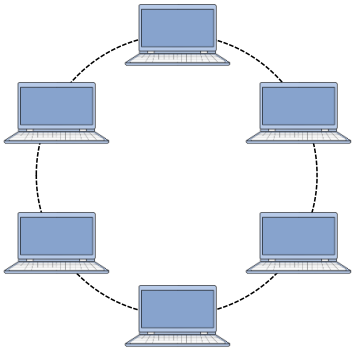
គុណវិបត្តិនៃ Bus Topology

ទាំងនេះគឺជាគុណវិបត្តិមួយចំនួននៃការប្រើប្រាស់ Bus Topology

- ការដោះស្រាយបញ្ហាមានភាពស្មុគស្មាញដោយសារមិនមានការគ្រប់គ្រងចំណុចគ្រប់គ្រងតែមួយ
- ថ្នាំងដែលមានកំហុសមួយអាចធ្វើអោយបណ្តាញទាំងមូលធ្លាក់ចុះ
- ទីតាំងមិនច្បាស់មិនអាចភ្ជាប់ជាមួយ Bus Topology បានទេ។

២.១.២ Ring Topology

ស្ថានីយនីមួយៗត្រូវបានភ្ជាប់ទៅថ្នាំងពីរយ៉ាងពិតប្រាកដនៅក្នុង Ring Topology ដែលផ្តល់ឱ្យបណ្តាញនូវរាងជារង្វង់ ទិន្នន័យធ្វើដំណើរក្នុងទិសដៅដែលបានកំណត់ជាមុនតែមួយប៉ុណ្ណោះ។



រូបភាព ២.២ Ring Topology

នៅពេលដែលស្ថានីយត្រូវបញ្ជូនទិន្នន័យ វាបញ្ជូនវាទៅថ្នាំងជិតខាង ដែលបញ្ជូនវាទៅឧបករណ៍បន្ទាប់។ មុនពេលបញ្ជូនបន្ត ទិន្នន័យអាចត្រូវបានពង្រីក។ វិធីនេះ ទិន្នន័យបញ្ជ្រាសបណ្តាញ និងទៅដល់ថ្នាំងទិសដៅ ដែលដកវាចេញពីបណ្តាញ។ ប្រសិនបើទិន្នន័យមកដល់អ្នកផ្ញើ វានឹងដកចេញ ហើយផ្ញើឡើងវិញនៅពេលក្រោយ។

អត្ថប្រយោជន៍នៃ Ring Topology

ទាំងនេះគឺជាគុណសម្បត្តិនៃការប្រើប្រាស់ Ring Topology៖

- ត្រូវការផ្នែកខ្សែតូចៗ ដើម្បីភ្ជាប់ថ្នាំងពីរ
- ល្អបំផុតសម្រាប់សរសៃអុបទិកដោយសារទិន្នន័យធ្វើដំណើរក្នុងទិសដៅតែមួយ
- ល្បឿនបញ្ជូនខ្ពស់គឺអាចធ្វើទៅបាន

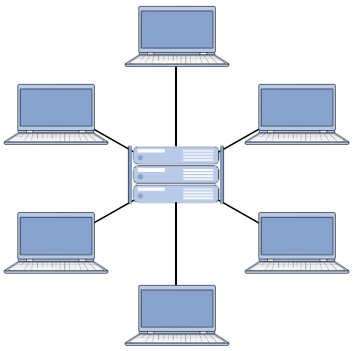
គុណវិបត្តិនៃ Ring Topology

ទាំងនេះគឺជាគុណវិបត្តិមួយចំនួននៃការប្រើប្រាស់ Ring Topology៖

- ការបរាជ័យនៃថ្នាំងតែមួយនាំឱ្យបណ្តាញទាំងមូលធ្លាក់ចុះ
- ការដោះស្រាយបញ្ហាមានភាពស្មុគស្មាញ ដោយសារថ្នាំងជាច្រើនអាចនឹងត្រូវត្រួតពិនិត្យ មុនពេលមានកំហុសត្រូវបានរកឃើញ
- ពិបាកក្នុងការដកថ្នាំងមួយ ឬច្រើនចេញ ខណៈពេលដែលរក្សាបណ្តាញដែលនៅសល់ឱ្យនៅដដែល។

២.១.៣ Star Topology

នៅក្នុង Star Topology ម៉ាស៊ីនមេត្រូវបានភ្ជាប់ទៅថ្នាំងនីមួយៗដោយឡែកពីគ្នា ម៉ាស៊ីនមេត្រូវបានគេហៅថាថ្នាំងកណ្តាលផងដែរ រាល់ការផ្លាស់ប្តូរទិន្នន័យរវាងថ្នាំងពីរត្រូវតែ ធ្វើឡើងតាមរយៈម៉ាស៊ីនមេវាគឺជាក្បួនដ៏ពេញនិយមបំផុតសម្រាប់បណ្តាញព័ត៌មាន និងបណ្តាញសំឡេងដោយសារថ្នាំងកណ្តាលអាចដំណើរការទិន្នន័យដែលទទួលបានពីថ្នាំងប្រភពបញ្ជូនវាទៅកាន់ថ្នាំងទិសដៅ។



រូបភាព ២.៣ Star Topology

អត្ថប្រយោជន៍នៃ Star Topology

ទាំងនេះគឺជាគុណសម្បត្តិនៃការប្រើប្រាស់ Star Topology៖

- ការបរាជ័យនៃថ្នាំងមួយមិនប៉ះពាល់ដល់បណ្តាញទេ
- ការដោះស្រាយបញ្ហាមានភាពងាយស្រួល ព្រោះថ្នាំងដែលមានកំហុសអាចត្រូវបានរកឃើញភ្លាមៗពីថ្នាំងកណ្តាល
- វិធីការចូលប្រើសាមញ្ញត្រូវបានទាមទារ ដោយសារថ្នាំងទំនាក់ទំនងមួយតែងតែជាថ្នាំងកណ្តាល

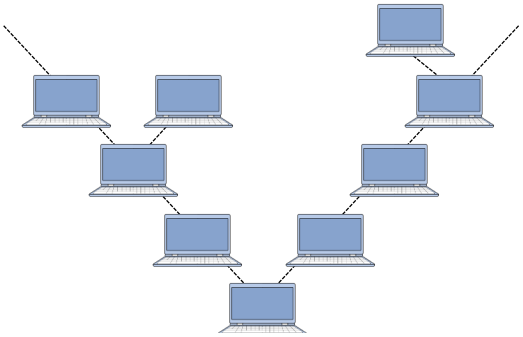
គុណវិបត្តិនៃ Star Topology

ទាំងនេះគឺជាគុណវិបត្តិនៃការប្រើប្រាស់ Star Topology៖

- ខ្សែវែងអាចត្រូវបានទាមទារដើម្បីភ្ជាប់ថ្នាំងនីមួយៗទៅម៉ាស៊ីនមេ
- ការបរាជ័យនៃថ្នាំងកណ្តាលធ្វើឱ្យបណ្តាញទាំងមូលធ្លាក់ចុះ

២.១.៣ Tree Topology

Tree Topology មានបណ្តាញផ្កាយមួយក្រុមដែលតភ្ជាប់ទៅខ្សែឆ្អឹងខ្នងរបស់ Bus លីនេអ៊ែរ ហើយវារួមបញ្ចូលលក្ខណៈពិសេសទាំង Star Topology និងBus Topology។ Tree Topologyត្រូវបានគេហៅថាហានុក្រមនៃក្បួនផងដែរ។



រូបភាព ២.៤ Tree Topology

អត្ថប្រយោជន៍នៃ Tree Topology

ទាំងនេះគឺជាគុណសម្បត្តិមួយចំនួននៃការប្រើប្រាស់ Tree Topology៖

- បណ្តាញដែលមានស្រាប់អាចពង្រីកបានយ៉ាងងាយស្រួល
- ខ្សែភ្លើងពីចំណុចមួយទៅចំណុចសម្រាប់ផ្នែកនីមួយៗ មានន័យថាការដំឡើង និងថែទាំកាន់តែងាយស្រួល
- សមល្អសម្រាប់បណ្តាញបណ្តោះអាសន្ន

គុណវិបត្តិនៃ Tree Topology

ទាំងនេះគឺជាគុណវិបត្តិមួយចំនួននៃការប្រើប្រាស់ Tree Topology៖

- តម្រូវឱ្យអ្នកជំនាញបច្ចេកទេសដើម្បីកំណត់រចនាសម្ព័ន្ធ និងរចនាសម្ព័ន្ធ Tree Topology ការបរាជ័យនៃខ្សែឆ្អឹងខ្នងធ្វើឱ្យបណ្តាញទាំងមូលធ្លាក់ចុះ
- បណ្តាញមិនមានសុវត្ថិភាព
- ការថែទាំពិបាកសម្រាប់បណ្តាញធំ

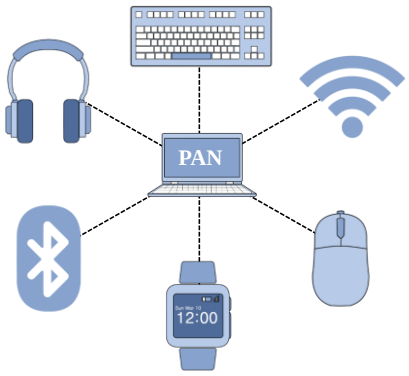
២.២ ប្រភេទនៃបណ្តាញកុំព្យូទ័រ

បណ្តាញអនុញ្ញាតឱ្យកុំព្យូទ័រតភ្ជាប់ និងទំនាក់ទំនងជាមួយកុំព្យូទ័រផ្សេងៗតាមរយៈឧបករណ៍ផ្ទុកណាមួយ។ LAN, MAN, និង WAN គឺជាបណ្តាញសំខាន់ៗចំនួនបីដែលត្រូវបានរចនាឡើងដើម្បីដំណើរការលើតំបន់ដែលគ្របដណ្តប់។ មានភាពស្រដៀងគ្នា និងភាពមិនដូចគ្នាមួយចំនួនរវាងភាពខុសប្លែកគ្នាដ៏សំខាន់មួយគឺតំបន់ភូមិសាស្ត្រដែលគ្របដណ្តប់ ពោលគឺ LAN គ្រប ដណ្តប់តំបន់តូចបំផុត MAN គ្របដណ្តប់តំបន់ធំជាង LAN ហើយ WAN រួមបញ្ចូលធំបំផុតទាំងអស់។ មានប្រភេទបណ្តាញកុំព្យូទ័រផ្សេងទៀតផងដែរ ដូចជា៖

- PAN (បណ្តាញតំបន់ផ្ទាល់ខ្លួន)
- SAN (បណ្តាញតំបន់ផ្ទុក)
- EPN (បណ្តាញឯកជនសហគ្រាស)
- VPN (បណ្តាញឯកជននិម្មិត)

២.២.១ បណ្តាញតំបន់ផ្ទាល់ខ្លួន (PAN)

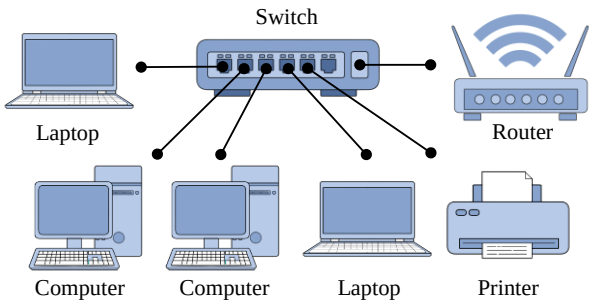
បណ្តាញតំបន់ផ្ទាល់ខ្លួន (PAN) គឺជាបណ្តាញកុំព្យូទ័រដែលភ្ជាប់កុំព្យូទ័រទៅកាន់ឧបករណ៍នៅក្នុងជួររបស់បណ្តាញ ។ ដោយសារ PAN ផ្តល់ជួរបណ្តាញក្នុងកម្រិតរបស់មនុស្ស ជាធម្មតាក្នុងចន្លោះ ១០ម៉ែត្រ (៣៣ហ្វីត) វាត្រូវបានគេហៅថាបណ្តាញតំបន់ផ្ទាល់ខ្លួន។ បណ្តាញតំបន់ផ្ទាល់ខ្លួនជាធម្មតាពាក់ព័ន្ធនឹងកុំព្យូទ័រ ទូរស័ព្ទ ថេប្លេត ម៉ាស៊ីនបោះពុម្ព PDA (ជំនួយការឌីជីថលផ្ទាល់ខ្លួន) និងឧបករណ៍កម្សាន្តផ្សេងទៀតដូចជាវាគ្មិន ម៉ាស៊ីនវីដេអូហ្គេមជាដើម។ Thomas Zimmerman និងអ្នកស្រាវជ្រាវផ្សេងទៀតនៅ Media Lab របស់ M.I.T. បានបង្កើតគំនិតដំបូង នៃ PAN វាមានសារៈប្រយោជន៍នៅក្នុងគេហដ្ឋាន ការិយាល័យ និងតំបន់បណ្តាញតូចៗ ដោយសារដំណើរការខ្ពស់របស់វាទាក់ទងនឹងភាពបត់បែន និងប្រសិទ្ធភាព។



រូបភាព ២.៥ បណ្តាញតំបន់ផ្ទាល់ខ្លួន (PAN)

២.២.២ បណ្តាញតំបន់មូលដ្ឋាន (LAN)

បណ្តាញ LAN ឬ បណ្តាញតំបន់មូលដ្ឋាន គឺជាបណ្តាញខ្សែដែលលាតសន្ធឹងលើផ្នែកតែមួយ ដូចជាការិយាល័យ អគារ ឬអង្គភាពផលិតកម្ម។ LAN ត្រូវបានបង្កើតឡើងនៅពេលដែលសមាជិកក្រុមត្រូវការចែករំលែកធនធានផ្នែកទន់ និងផ្នែករឹង ប៉ុន្តែមិនមែនជាមួយពិភពខាងក្រៅនោះទេ។ ធនធានកម្មវិធីធម្មតារួមមាន ឯកសារផ្លូវការ សៀវភៅណែនាំអ្នកប្រើប្រាស់ សៀវភៅណែនាំបុគ្គលិក ធនធានផ្នែករឹងដែលត្រូវបានចែករំលែកយ៉ាងងាយស្រួលនៅលើបណ្តាញមានដូចជា ម៉ាស៊ីនបោះពុម្ព ម៉ាស៊ីនទូសារ ម៉ូដឹម ទំហំអង្គចងចាំ ហើយវាកាត់បន្ថយថ្លៃដើមហេដ្ឋារចនាសម្ព័ន្ធសម្រាប់ស្ថាប័នយ៉ាងខ្លាំង។



រូបភាព ២.៦ បណ្តាញតំបន់មូលដ្ឋាន (LAN)

LAN អាចត្រូវបានតំឡើងដោយប្រើការភ្ជាប់តាមខ្សែ ឬឥតខ្សែ។ LAN ឥតខ្សែទាំងស្រុងត្រូវបានគេហៅថា Wireless LAN ឬ WLAN Local Area Network (LAN) LAN ឬ បណ្តាញតំបន់មូលដ្ឋានភ្ជាប់ឧបករណ៍បណ្តាញ ដូច្នេះកុំព្យូទ័រផ្ទាល់ខ្លួន និងស្ថានីយការងារអាចចែករំលែកទិន្នន័យ ឧបករណ៍ និងកម្មវិធី។ ក្រុមកុំព្យូទ័រ និងឧបករណ៍ត្រូវបានភ្ជាប់ដោយកុងតាក់ ដោយប្រើគ្រោងការណ៍អាសយដ្ឋានឯកជនដែលកំណត់ដោយពិធីការ TCP/IP ។ អាសយដ្ឋានផ្ទាល់ខ្លួនគឺមានតែមួយគត់សម្រាប់កុំព្យូទ័រផ្សេងទៀតនៅលើបណ្តាញមូលដ្ឋាន ហើយរ៉ោតទ័រត្រូវបានរកឃើញនៅព្រំដែននៃ LAN ដោយភ្ជាប់ពួកវាទៅ WAN កាន់តែទូលំទូលាយ។ ទិន្នន័យបញ្ជូនយ៉ាងលឿនព្រោះចំនួនកុំព្យូទ័រដែលភ្ជាប់មានកំណត់តាមនិយមន័យ ការតភ្ជាប់ត្រូវតែជាផ្នែករឹងដែលមានល្បឿនលឿន និងមានតម្លៃថោកសមរម្យ (Hubs អាដាប់ទ័របណ្តាញ និងខ្សែអ៊ីសឺរណិត)។ LANs គ្របដណ្តប់តំបន់ភូមិសាស្ត្រតូចជាង (ទំហំត្រូវបានកំណត់ត្រឹមពីរបីគីឡូម៉ែត្រ) និងជាកម្មសិទ្ធិឯកជន។មួយអាចប្រើសម្រាប់អគារការិយាល័យ ផ្ទះ មន្ទីរពេទ្យ សណ្ឋាគារ ធនាគារ សាលារៀន។ LAN ងាយស្រួលរចនា និងថែទាំឧបករណ៍ទំនាក់ទំនងដែលប្រើសម្រាប់ LAN មានខ្សែគូរមួល និងខ្សែឌូស៊ីល (coaxial) ។ វាគ្របដណ្តប់ចម្ងាយខ្លីដូច្នេះកំហុស និងសំលេងរំខានត្រូវបានបង្រួមអប្បបរមា។

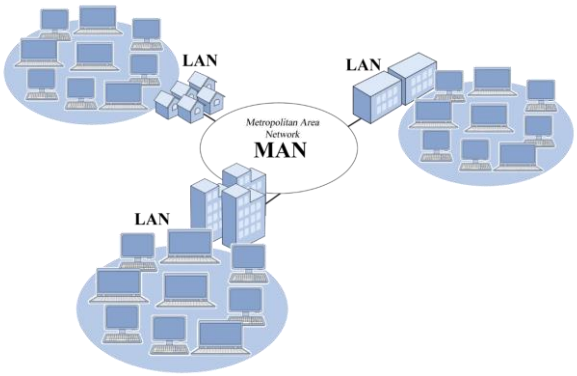
LANs ដំបូងមានអត្រាទិន្នន័យក្នុងចន្លោះពី ៤ ទៅ ១៦ Mbps សព្វថ្ងៃនេះ ល្បឿនជាធម្មតាគឺ ១០០ ឬ ១០០០ Mbps ការពន្យាពេលការផ្សព្វផ្សាយគឺខ្លីណាស់នៅក្នុងបណ្តាញមូលដ្ឋាន។ LAN តូចបំផុតអាចប្រើតែកុំព្យូទ័រពីរប៉ុណ្ណោះ ខណៈដែល LAN ធំជាងអាចផ្គុំកុំព្យូទ័ររាប់ពាន់។ LAN ជាធម្មតា

ពីងផ្នែកជាចម្បងលើការភ្ជាប់ខ្សែសម្រាប់បង្កើនល្បឿន និងសុវត្ថិភាព ប៉ុន្តែការតភ្ជាប់ឥតខ្សែក៏អាចជាផ្នែកមួយនៃ LAN ផងដែរ។ កំហុសរបស់ LAN គឺតែងតែជួបប្រទះ មានការកកស្ទះតិចជាងនៅក្នុងបណ្តាញនេះ។ ឧទាហរណ៍ សិស្សមួយក្រុមកំពុងលេង។

២.២.៣ បណ្តាញតំបន់ទីប្រជុំជន (MAN)

MAN គឺជាអក្សរកាត់សម្រាប់បណ្តាញតំបន់ទីប្រជុំជនវាគឺជាបណ្តាញដែលរីករាលដាលនៅលើទីក្រុង បរិវេណមហាវិទ្យាល័យ ឬតំបន់តូចមួយ។ MAN គឺសំខាន់ជាងបណ្តាញ LAN ហើយជាធម្មតារីករាលដាលជាងជាច្រើនគីឡូម៉ែត្រ។ គោលបំណងរបស់ MAN គឺដើម្បីចែករំលែកធនធានផ្នែករឹង និងផ្នែកទន់ ដោយកាត់បន្ថយការចំណាយលើហេដ្ឋារចនាសម្ព័ន្ធ។ MAN អាចត្រូវបានសាងសង់ដោយភ្ជាប់បណ្តាញ LAN ជាច្រើនរួមបញ្ចូលគ្នា។

ឧទាហរណ៍ទូទៅបំផុតនៃ MAN គឺបណ្តាញទូរទស្សន៍ខ្សែកាប។



រូបភាព ២.៧ បណ្តាញតំបន់ទីប្រជុំជន (MAN)

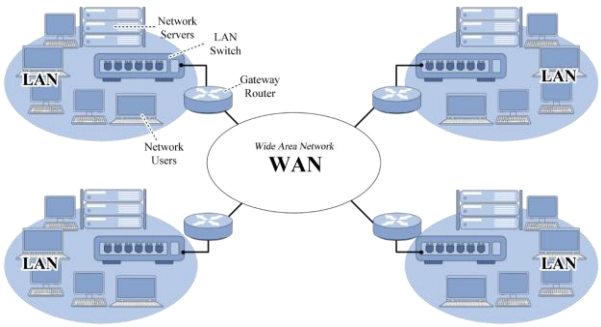
MAN ឬ បណ្តាញតំបន់ទីប្រជុំជន គ្របដណ្តប់តំបន់ធំជាង LAN និងតំបន់តូចជាង WAN វាភ្ជាប់កុំព្យូទ័រពីរ ឬច្រើនដែលនៅដាច់ពីគ្នា ប៉ុន្តែរស់នៅក្នុងទីក្រុងដូចគ្នា ឬផ្សេងគ្នា។ វាគ្របដណ្តប់តំបន់ភូមិសាស្ត្រដ៏ធំមួយ ហើយអាចបម្រើជា ISP (អ្នកផ្តល់សេវាអ៊ីនធឺណិត)។ MAN ត្រូវបានរចនាឡើងសម្រាប់អតិថិជនដែលត្រូវការការតភ្ជាប់ល្បឿនលឿន។ ល្បឿននៃ MAN នៅក្នុងលក្ខខណ្ឌមួយគិតជា Mbps វាពិបាកក្នុងការរចនា និងថែរក្សាបណ្តាញតំបន់ទីប្រជុំជន ។

កំហុសរបស់ MAN គឺតិចជាង ហើយមានការកកស្ទះកាន់តែច្រើននៅក្នុងបណ្តាញ វាមានតម្លៃថ្លៃ ហើយអាច ឬមិនអាចគ្រប់គ្រងដោយអង្គការតែមួយ អត្រាផ្ទេរទិន្នន័យ និងការពន្យារការផ្សព្វផ្សាយរបស់ MAN គឺមធ្យម។ ឧបករណ៍ដែលប្រើសម្រាប់ការបញ្ជូនទិន្នន័យតាមរយៈ MAN គឺ (Modem និង Wire/Cable ។ ឧទាហរណ៍នៃ MAN គឺជាផ្នែកនៃបណ្តាញក្រុមហ៊ុនទូរស័ព្ទដែលអាច ផ្តល់ខ្សែ DSL ល្បឿនលឿនដល់អតិថិជន ឬបណ្តាញទូរទស្សន៍ខ្សែកាបក្នុងទីក្រុងមួយ។

២.២.៤ បណ្តាញតំបន់ធំទូលាយ (WAN)

WAN ឬ បណ្តាញតំបន់ធំទូលាយ គឺជាបណ្តាញកុំព្យូទ័រដែលលាតសន្ធឹងលើតំបន់ភូមិសាស្ត្រដ៏ធំមួយ បើទោះបីជាវាអាចត្រូវបានបង្ខាំងនៅក្នុងព្រំដែននៃរដ្ឋ ឬប្រទេសក៏ដោយ។ WAN អាចជាការតភ្ជាប់នៃ LAN ដែលភ្ជាប់ទៅបណ្តាញ LAN ផ្សេងទៀតតាមរយៈខ្សែទូរស័ព្ទ និងរលកវិទ្យុ។ វាអាចត្រូវបានកំណត់ចំពោះសហគ្រាស (សាជីវកម្ម ឬអង្គការ) ឬអាចចូលដំណើរការបានសម្រាប់សាធារណៈបច្ចេកវិទ្យាមានល្បឿនលឿន និងមានតម្លៃថ្លៃគួរសម។

WAN មានពីរប្រភេទ៖ Switched WAN និង Point-to-Point WAN ។ WAN ពិបាកក្នុងការរចនា និងថែទាំ ស្រដៀងទៅនឹង MAN ដែរ ភាពកើតមានកំហុសរបស់ WAN គឺតិចជាង ហើយមានការកកស្ទះកាន់តែច្រើននៅក្នុងបណ្តាញ ឧបករណ៍ទំនាក់ទំនងដែលប្រើសម្រាប់ WAN គឺ PSTN ឬ Satellite Link ដោយសារតែការបញ្ជូនចម្ងាយឆ្ងាយ សំលេងរំខាន និងកំហុសគឺកាន់តែញឹកញាប់នៅក្នុង WAN ។



រូបភាព ២.៨ បណ្តាញតំបន់ធំទូលាយ (WAN)

៣.១ ពិធីការបណ្តាញ

ពិធីការបណ្តាញគឺជាសំណុំនៃច្បាប់ដែលគ្រប់គ្រងការផ្លាស់ប្តូរព័ត៌មានក្នុងមធ្យោបាយងាយស្រួល ជឿជាក់ និងសុវត្ថិភាព មុននឹងយើងពិភាក្សាអំពីពិធីការទូទៅបំផុតដែលប្រើដើម្បីបញ្ជូន និងទទួលទិន្នន័យតាមបណ្តាញយើងត្រូវយល់ពីរបៀបដែលបណ្តាញត្រូវបានរៀបចំឬរចនាយ៉ាងឡូជីខល គំរូ Open Systems Interface (OSI) ដែលស្នើឡើងដោយ ISO គឺជាគំរូដ៏ពេញនិយមបំផុតសម្រាប់បង្កើតទំនាក់ទំនងបើកចំហរវាងប្រព័ន្ធទាំងពីរ។ ប្រភេទនៃពិធីការអាចត្រូវបានចាត់ថ្នាក់យ៉ាងទូលំទូលាយជាបីប្រភេទធំៗ

- ការទំនាក់ទំនង
- ការគ្រប់គ្រង
- សុវត្ថិភាព

៣.១.១ ការធំឆាក់ធំឆន

ពិធីការទំនាក់ទំនងមានសារៈសំខាន់សម្រាប់ដំណើរការនៃបណ្តាញ ពួកវាមានសារៈសំខាន់ខ្លាំងណាស់ ដែលវាមិនអាចទៅរួចទេក្នុងការមានបណ្តាញកុំព្យូទ័រដោយគ្មានពួកវា។ ពិធីការទាំងនេះកំណត់ជាផ្លូវការនូវច្បាប់ និងទម្រង់ដែលទិន្នន័យត្រូវបានផ្ទេរ។ ពិធីការទាំងនេះគ្រប់គ្រងវាក្យសម្ព័ន្ធ អត្ថន័យ រកឃើញកំហុស ការធ្វើសមកាលកម្ម និងការផ្ទៀងផ្ទាត់។

ឧទាហរណ៍នៃពិធីសារទំនាក់ទំនង៖

- **HTTP៖** គឺជាពិធីការស្រទាប់ប្រាំពីរដែលត្រូវបានរចនាឡើងដើម្បីផ្ទេរអត្ថបទខ្ពស់រវាងប្រព័ន្ធពីរ ឬច្រើន។ HTTP ដំណើរការលើគំរូម៉ាស៊ីនភ្ញៀវ-ម៉ាស៊ីនមេ ហើយការចែករំលែកទិន្នន័យភាគច្រើននៅលើបណ្តាញគឺធ្វើឡើងដោយប្រើ HTTP ។
- **TCP៖** វាគឺជាការបង្ហាញការចែកចាយស្ទ្រីមដែលអាចទុកចិត្តបានដោយប្រើការទទួលស្គាល់តាមលំដាប់លំដោយ។ វាគឺជាពិធីការដែលផ្តោតលើការតភ្ជាប់ ពោលគឺវាបង្កើតការតភ្ជាប់រវាងកម្មវិធីមុនពេលផ្ទេទិន្នន័យណាមួយ វាត្រូវបានប្រើសម្រាប់ការទំនាក់ទំនងតាមបណ្តាញ។ ហើយវាមានកម្មវិធីជាច្រើនដូចជា អ៊ីមែល FTP ប្រព័ន្ធផ្សព្វផ្សាយស្ទ្រីមជាដើម។
- **UDP៖** គឺជាពិធីការគ្មានការតភ្ជាប់ដែលដាក់ចេញនូវសេវាកម្មសារជាមូលដ្ឋាន ប៉ុន្តែមិនអាចទុកចិត្តបាន វាបន្ថែមមុខងារគ្រប់គ្រងលំហូរ ភាពជឿជាក់ ឬកំហុសក្នុងការស្តារឡើងវិញ។ UDP មានមុខងារក្នុងករណីដែលមិនតម្រូវឱ្យមានភាពជឿជាក់ វាត្រូវបានប្រើនៅពេលដែលយើងចង់បានការបញ្ជូនលឿនជាងមុន សម្រាប់ការតភ្ជាប់ច្រើន និងការផ្សាយ។
- **BGP៖** វាគឺជាពិធីការនាំផ្លូវដែលគ្រប់គ្រងពីរបៀបដែលកញ្ចប់ព័ត៌មានឆ្លងកាត់រ៉ោតទ័រនៅក្នុងប្រព័ន្ធឯករាជ្យ បណ្តាញមួយ ឬច្រើនដំណើរការដោយអង្គការតែមួយ និងភ្ជាប់ទៅបណ្តាញផ្សេងៗ។ វាភ្ជាប់ចំនុចបញ្ចប់នៃ LAN ជាមួយ LANs និង ចុងបញ្ចប់នៃចំណុចផ្សេងទៀតនៅក្នុង LANs ផ្សេងគ្នាទៅគ្នាទៅវិញទៅមក។
- **ARP៖** គឺជាពិធីការដែលជួយកំណត់អាសយដ្ឋានឡូជីខលទៅកាន់អាសយដ្ឋានមូលដ្ឋានដែលត្រូវបានទទួលស្គាល់នៅក្នុងបណ្តាញមូលដ្ឋាន។ តារាងដែលគេស្គាល់ថាជាឃ្លាំងសម្ងាត់ ARP ត្រូវបានប្រើសម្រាប់ការគូសផែនទី និងរក្សាទំនាក់ទំនងរវាងអាសយដ្ឋានឡូជីខល និងរូបវន្តទាំងនេះ។
- **IP៖** គឺជាពិធីការដែលទិន្នន័យត្រូវបានបញ្ជូនពីម៉ាស៊ីនមួយទៅម៉ាស៊ីនមួយទៀតតាមរយៈអ៊ីនធឺណិតហើយវាត្រូវបានប្រើប្រាស់ ដើម្បីកំណត់អាសយដ្ឋាន និងបញ្ជូនកញ្ចប់ទិន្នន័យដូច្នេះពួកគេអាចទៅដល់គោលដៅរបស់ពួកគេ។
- **DHCP៖** នេះគឺជាពិធីការសម្រាប់ការគ្រប់គ្រងបណ្តាញ ហើយវាត្រូវបានប្រើប្រាស់ដើម្បីធ្វើឱ្យដំណើរការនៃការកំណត់ឧបករណ៍នៅលើបណ្តាញ IP ដោយស្វ័យប្រវត្តិ។ ម៉ាស៊ីនមេ DHCP

ផ្តល់អាសយដ្ឋាន IP ដោយស្វ័យប្រវត្តិ និងការផ្លាស់ប្តូរការកំណត់រចនាសម្ព័ន្ធផ្សេងៗទៅកាន់ឧបករណ៍នៅលើបណ្តាញ ដើម្បីទំនាក់ទំនងជាមួយបណ្តាញ IP ផ្សេងទៀត។ វាក៏អនុញ្ញាតឱ្យឧបករណ៍ប្រើប្រាស់សេវាកម្មផ្សេងៗដូចជា NTP, DNS ឬពិធីការណាមួយដែលមានមូលដ្ឋានលើ TCP ឬ UDP ។

៣.១.២ ការគ្រប់គ្រង

ពិធីការទាំងនេះពិពណ៌នាអំពីនីតិវិធី និងគោលការណ៍ដែលប្រើក្នុងការត្រួតពិនិត្យ ថែទាំ និងគ្រប់គ្រងបណ្តាញកុំព្យូទ័រ។ ពិធីការទាំងនេះក៏ជួយទំនាក់ទំនងតម្រូវការទាំងនេះនៅទូទាំងបណ្តាញ ដើម្បីធានាឱ្យមានទំនាក់ទំនងទៀងទាត់ ពិធីការគ្រប់គ្រងបណ្តាញក៏អាចដោះស្រាយបញ្ហាការតភ្ជាប់រវាងម៉ាស៊ីន និងម៉ាស៊ីនភ្ញៀវផងដែរ។

ឧទាហរណ៍នៃពិធីសារគ្រប់គ្រង៖

- **ICMP៖** គឺជាពិធីការស្រទាប់បីដែលប្រើដោយឧបករណ៍បណ្តាញដើម្បីបញ្ជូនព័ត៌មានប្រតិបត្តិការ និងសារកំហុស។ វារាយការណ៍ពីការកកស្ទះ កំហុសបណ្តាញ គោលបំណងវិនិច្ឆ័យ និងការអស់ពេល។
- **SNMP៖** ពិធីការស្រទាប់ប្រាំពីរត្រូវបានប្រើសម្រាប់ការគ្រប់គ្រងថ្នាំងនៅលើបណ្តាញ IP ។ មានសមាសភាគសំខាន់បីនៅក្នុងពិធីការ SNMP ពោលគឺភ្នាក់ងារ SNMP អ្នកគ្រប់គ្រង SNMP និងឧបករណ៍ដែលមើលរំលង។ ភ្នាក់ងារ SNMP មានចំណេះដឹងក្នុងតំបន់អំពីព័ត៌មានលម្អិតនៃការគ្រប់គ្រងវាបកប្រែព័ត៌មានលម្អិតទាំងនោះទៅជាទម្រង់ដែលត្រូវគ្នាជាមួយអ្នកគ្រប់គ្រង SNMP ។ អ្នកគ្រប់គ្រងបង្ហាញទិន្នន័យដែលទទួលបានពីភ្នាក់ងារ SNMP ដូច្នេះការជួយត្រួតពិនិត្យបញ្ហាបណ្តាញ និងដំណើរការ ក៏ដូចជាការដោះស្រាយបញ្ហាទាំងនោះ។
- **Gopher៖** វាគឺជាប្រភេទនៃពិធីការទាញយកឯកសារដែលផ្តល់នូវឯកសារដែលអាចទាញយកបានជាមួយនឹងការពិពណ៌នាមួយចំនួនសម្រាប់ការគ្រប់គ្រងងាយស្រួល ទាញយក និងស្វែងរកឯកសារ ឯកសារទាំងអស់ត្រូវបានរៀបចំនៅលើកុំព្យូទ័រពីចម្ងាយក្នុងលក្ខណៈតម្រៀបហើយវាគឺជាពិធីការចាស់មិនត្រូវបានគេប្រើច្រើនទេនាពេលបច្ចុប្បន្ន។
- **FTP៖** គឺជាពិធីការម៉ាស៊ីនភ្ញៀវ/ម៉ាស៊ីនមេ ដែលប្រើសម្រាប់ផ្លាស់ទីឯកសារទៅ ឬពីកុំព្យូទ័រម៉ាស៊ីន វាអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ទាញយកឯកសារ កម្មវិធី គេហទំព័រ និងអ្វីៗផ្សេងទៀតដែលមាននៅលើសេវាកម្មផ្សេងទៀត។
- **POP3៖** វាគឺជាពិធីការដែលកម្មវិធីអ៊ីមែលក្នុងស្រុកប្រើដើម្បីទទួលសារអ៊ីមែលពីម៉ាស៊ីនមេអ៊ីមែលពីចម្ងាយតាមរយៈការតភ្ជាប់ TCP/IP ។ ម៉ាស៊ីនមេអ៊ីមែលដែលបង្ហោះដោយ ISPs ក៏ប្រើពិធីការ POP3 ដើម្បីរក្សា និងទទួលអ៊ីមែលដែលមានបំណងសម្រាប់អ្នកប្រើប្រាស់របស់

ពួកគេ។ នៅទីបំផុត អ្នកប្រើប្រាស់ទាំងនេះនឹងប្រើកម្មវិធីកម្មវិធីអ៊ីមែល ដើម្បីមើលប្រអប់សំបុត្ររបស់ពួកគេនៅលើម៉ាស៊ីនមេពីចម្ងាយ និងដើម្បីទាញយកអ៊ីមែលរបស់ពួកគេបន្ទាប់ពីកម្មវិធី អ៊ីមែលទាញយកអ៊ីមែល ពួកវាជាទូទៅត្រូវបានលុបចេញពីម៉ាស៊ីនមេ ហើយវាគឺជាពិធីការដែលអនុញ្ញាតឱ្យអ្នកប្រើភ្ជាប់ទៅកម្មវិធីកុំព្យូទ័រពីចម្ងាយ និងដើម្បីប្រើវា

- **Telnet៖** ពោលគឺវាត្រូវបានរចនាឡើងសម្រាប់ការតភ្ជាប់ពីចម្ងាយ។ Telnet ភ្ជាប់ម៉ាស៊ីនមេ និងចំណុចបញ្ចប់ដើម្បីបើកវគ្គពីចម្ងាយ។

៣.៣.៣ សុវត្ថិភាព

ពិធីការទាំងនេះធានាសុវត្ថិភាពទិន្នន័យក្នុងការឆ្លងកាត់តាមបណ្តាញហើយពិធីការទាំងនេះក៏កំណត់ពីរបៀបដែលបណ្តាញធានាទិន្នន័យពីការប៉ុនប៉ងដោយគ្មានការអនុញ្ញាតក្នុងការស្រង់ចេញ ឬពិនិត្យមើលទិន្នន័យ។ ពិធីការទាំងនេះធានាថាគ្មានឧបករណ៍ អ្នកប្រើប្រាស់ ឬសេវាកម្មណាដែលគ្មានការអនុញ្ញាតអាចចូលប្រើទិន្នន័យបណ្តាញបានទេជាដំបូងពិធីការទាំងនេះពឹងផ្អែកលើការអ៊ិនគ្រីបដើម្បីធានាសុវត្ថិភាពទិន្នន័យ។

ឧទាហរណ៍នៃពិធីសារសុវត្ថិភាព៖

- **SSL៖** គឺជាពិធីការសុវត្ថិភាពបណ្តាញដែលត្រូវបានប្រើជាចម្បងដើម្បីការពារទិន្នន័យ និងធានាសុវត្ថិភាពការតភ្ជាប់អ៊ីនធឺណិត។ SSL អនុញ្ញាតឱ្យទំនាក់ទំនងរវាងម៉ាស៊ីនបម្រើទៅកាន់ម៉ាស៊ីនបម្រើ និងម៉ាស៊ីនភ្ញៀវទៅកាន់ម៉ាស៊ីនបម្រើ ទិន្នន័យទាំងអស់ដែលបានផ្ទេរតាមរយៈ SSL ត្រូវបានអ៊ិនគ្រីប ដូច្នេះអាចបញ្ឈប់បុគ្គលដែលគ្មានការអនុញ្ញាតពីការចូលប្រើប្រាស់វា។
- **HTTPS៖** គឺជាកំណែសុវត្ថិភាពរបស់ HTTP ហើយពិធីការនេះធានានូវការទំនាក់ទំនងប្រកបដោយសុវត្ថិភាពរវាងកុំព្យូទ័រពីរ ដែលមួយផ្ញើសំណើតាមរយៈកម្មវិធីរុករកតាមអ៊ីនធឺណិតហើយមួយទៀតទៅយកទិន្នន័យពីម៉ាស៊ីនមេគេហទំព័រ។
- **TSL៖** វាគឺជាពិធីការសុវត្ថិភាពដែលត្រូវបានរចនាឡើងសម្រាប់សុវត្ថិភាពទិន្នន័យ និងភាពឯកជនភាពនៅលើអ៊ីនធឺណិត។ មុខងាររបស់វាគឺការអ៊ិនគ្រីប ពិនិត្យមើលភាពត្រឹមត្រូវនៃទិន្នន័យ ពោលគឺថាតើវាត្រូវបានរំខានឬអត់ និងការផ្ទៀងផ្ទាត់ជាទូទៅវាត្រូវបានប្រើសម្រាប់ការទំនាក់ទំនងដែលបានអ៊ិគ្រីបវាងម៉ាស៊ីនមេ និងកម្មវិធីគេហទំព័រដូចជាកម្មវិធីរុករកតមអ៊ីនធឺណិតដែលកំពុងផ្ទុកគេហទំព័រ វាក៏អាចប្រើប្រាស់ដើម្បី អ៊ិនគ្រីបសារ អ៊ីមែល និង VoIP ដែរ។

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះ អ្នកបានសិក្សាអំពី៖

- **បណ្តាញតំបន់ផ្ទាល់ខ្លួន (PAN)** គឺជាបណ្តាញកុំព្យូទ័រដែលភ្ជាប់កុំព្យូទ័រ/ឧបករណ៍នៅក្នុងជួររបស់មនុស្ស ដោយសារ PAN ផ្តល់ជួរបណ្តាញក្នុងកម្រិតរបស់មនុស្ស ជាធម្មតាក្នុងចន្លោះ ១០ម៉ែត្រ (៣៣ ហ្វីត) វាត្រូវបានគេហៅថាបណ្តាញតំបន់ផ្ទាល់ខ្លួន។
- **បណ្តាញតំបន់មូលដ្ឋាន (LAN)** គឺជាបណ្តាញខ្សែដែលលាតសន្ធឹងលើផ្នែកតែមួយ ដូចជាការិយាល័យ អគារ ឬអង្គភាព ផលិតកម្ម។ LAN ត្រូវបានបង្កើតឡើងនៅពេលដែលសមាជិកក្រុមត្រូវការចែករំលែកធនធានផ្នែកទន់ និងផ្នែករឹង ប៉ុន្តែមិនមែនជាមួយពិភពខាងក្រៅនោះទេ។
- **បណ្តាញតំបន់ទីប្រជុំជន (MAN)** វាគឺជាបណ្តាញដែលរីករាលដាលនៅលើទីក្រុង បរិវេណមហាវិទ្យាល័យ ឬតំបន់តូចមួយ។ MAN គឺសំខាន់ជាងបណ្តាញ LAN ហើយជាធម្មតារីករាលដាលជាងជាច្រើនគីឡូម៉ែត្រ។
- **បណ្តាញតំបន់ធំទូលាយ (WAN)** គឺជាបណ្តាញកុំព្យូទ័រដែលលាតសន្ធឹងលើតំបន់ភូមិសាស្ត្រដ៏ធំមួយ បើទោះបីជាវាអាចត្រូវបានបង្ខាំងនៅក្នុងព្រំដែននៃរដ្ឋ ឬប្រទេសក៏ដោយ។ WAN អាចជាការតភ្ជាប់នៃបណ្តាញ LAN ដែលភ្ជាប់ទៅបណ្តាញ LAN ផ្សេងទៀតតាមរយៈខ្សែទូរស័ព្ទ និងរលកវិទ្យុ។ វាអាចត្រូវបានកំណត់ចំពោះសហគ្រាស (សាជីវកម្ម ឬអង្គការ) ឬអាចចូលដំណើរការបានសម្រាប់សាធារណជន។
- HTTP គឺជាពិធីការស្រទាប់ប្រាំពីរដែលត្រូវបានរចនាឡើងដើម្បីផ្ទេរអត្ថបទខ្ពស់រវាងប្រព័ន្ធពីរ ឬច្រើន។ HTTP ដំណើរការលើគំរូម៉ាស៊ីនភ្ញៀវ-ម៉ាស៊ីនមេ។ ការចែករំលែកទិន្នន័យភាគច្រើននៅលើបណ្តាញគឺធ្វើឡើងដោយប្រើ HTTP ។
- TCP៖ វាបង្ហាញការចែកចាយស្ទ្រីមដែលអាចទុកចិត្តបានដោយប្រើការទទួលស្គាល់តាមលំដាប់លំដោយហើយវាគឺជាពិធីការដែលផ្តោតលើការតភ្ជាប់ ពោលគឺវាបង្កើតការតភ្ជាប់រវាងកម្មវិធីមុនពេលផ្ទេរទិន្នន័យណាមួយហើយវាត្រូវបានប្រើសម្រាប់ការទំនាក់ទំនងតាមបណ្តាញ វាមានកម្មវិធីជាច្រើនដូចជា អ៊ីមែល FTP ប្រព័ន្ធផ្សព្វផ្សាយស្ទ្រីមជាដើម។
- HTTPS គឺជាកំណែសុវត្ថិភាពរបស់ HTTP ។ ពិធីការនេះធានានូវការទំនាក់ទំនងប្រកបដោយសុវត្ថិភាពរវាងកុំព្យូទ័រពីរ ដែលមួយផ្នើសំណើតាមរយៈកម្មវិធីរុករកតាមអ៊ីនធឺណិត ហើយមួយទៀតទៅយកទិន្នន័យពីម៉ាស៊ីនមេគេហទំព័រ។

សំណួរ

១. តើបណ្តាញតំបន់ផ្ទាល់ខ្លួន (PAN) ជាអ្វី?

២. តើបណ្តាញតំបន់មូលដ្ឋាន (LAN) ជាអ្វី?

៣. តើបណ្តាញតំបន់ទីប្រជុំជន (MAN) ជាអ្វី?

៤. តើបណ្តាញតំបន់ធំទូលាយ (WAN) ជាអ្វី?

៥. តើអ្វីជាភាពខុសគ្នារវាង LAN និង WAN?

៦. ចូរពិពណ៌នាអំពីក្បួនតបណ្តាញ។

ការអនុវត្តន៍ទី២

រ៉ោតទ័រនិង កុងតាក់មុខងារទូទៅនៅក្នុង Packet Tracer រ៉ោតទ័រ និងកុងតាក់ដែលផ្តល់ដោយ Packet Tracer ផ្តល់នូវចំណុចប្រទាក់ស្រដៀងគ្នា។ ដូច្នេះ ចូរយើងរៀនពីការរៀបចំ និងប្រតិបត្តិការ ឧបករណ៍មូលដ្ឋានក្នុងលំហាត់នេះ។

ក.គោលបំណងនៃការអនុវត្តន៍នេះ

- ដើម្បីធ្វើការកំណត់មូលដ្ឋានរបស់រ៉ោតទ័រ។
- ដើម្បីធ្វើការកំណត់មូលដ្ឋាននៃកុងតាក់។

ខ. ការកំណត់ 'ឈ្មោះម៉ាស៊ីន'

វាមានអត្ថប្រយោជន៍សម្រាប់ការគ្រប់គ្រងដើម្បីកំណត់ឈ្មោះឧបករណ៍នៅពេលដំឡើងវានៅលើបណ្តាញ និងកំណត់ប្រតិបត្តិការ ហើយបណ្តាញទូលំទូលាយធ្វើឱ្យវាកាន់តែងាយស្រួលសម្រាប់អ្នកគ្រប់គ្រងក្នុងការគ្រប់គ្រងឧបករណ៍ ប្រសិនបើឈ្មោះត្រូវបានកំណត់សម្រាប់វា។

ឧបករណ៍៖ ឈ្មោះចម្បងមានអក្សរ និងលេខ(ការកំណត់ឈ្មោះរ៉ោតទ័រ ការកំណត់ឈ្មោះប្តូរ)

```
Switch>enable
Switch #configure terminal
Switch(config)#hostname [name]
```

គ. ការកំណត់ IP Address, Subnet Mask លើរ៉ោតទ័រ

រ៉ោតទ័រ និងអាសយដ្ឋាន IP ត្រូវតែកំណត់នៅលើឧបករណ៍ ដើម្បីបញ្ជូនកញ្ចប់ទិន្នន័យ នៅពេលអ្នកភ្ជាប់ខ្សែរវាងឧបករណ៍ទៅ នឹងឧបករណ៍តាមដានកញ្ចប់ព័ត៌មាននឹងបែងចែកអាសយដ្ឋានដោយស្វ័យប្រវត្តិ ហើយដើម្បីបញ្ចូលដោយដៃសូមប្រើពាក្យបញ្ជា និងបញ្ចូលពាក្យបញ្ជាខាងក្រោម។

```
Router> enable
Router# configure terminal
Router(config)#interface fast Ethernet[N/N]
Router(config-if) #ip address [192.168.100.1 255.255.255.0]
Router(config)#no shutdown
```

ឃ. ការកំណត់សារបដា

សារបដា គឺជាពាក្យបញ្ជាដែលប្រើប្រាស់សម្រាប់បង្ហាញសារទៅកាន់អ្នកប្រើប្រាស់ដែលចូលប្រើរ៉ោតទ័រ ឬកុងតាក់។ ជាទូទៅការប្រុងប្រយ័ត្ន ឬការព្រមានអំពីការចូលប្រើរ៉ោតទ័រត្រូវបានបង្ហាញ។

```
Router>enable

Router# configure terminal

Router(config)#banner motd [message]
```

ង. ប្រវត្តិនៃការកំណត់(Key Log)

មុខងារប្រវត្តិចងចាំពាក្យបញ្ជាដែលបានប្រើថ្មីៗបំផុតដោយរ៉ោតទ័រ ពាក្យបញ្ជាចំនួនដប់ត្រូវបានរក្សាទុកជាលំដាប់បន្ទាប់ពីបញ្ចូលពាក្យបញ្ជា ចុចផ្នែកខាងលើនៃក្តារចុច ដើម្បីរំលឹកឡើងវិញនូវលំដាប់ដែលបានទន្ទេញ អ្នកអាចផ្លាស់ប្តូរចំនួននៃការចងចាំដោយប្រើពាក្យបញ្ជាជម្រើស។

```
Router>en

Router# Terminal history size [10]
```

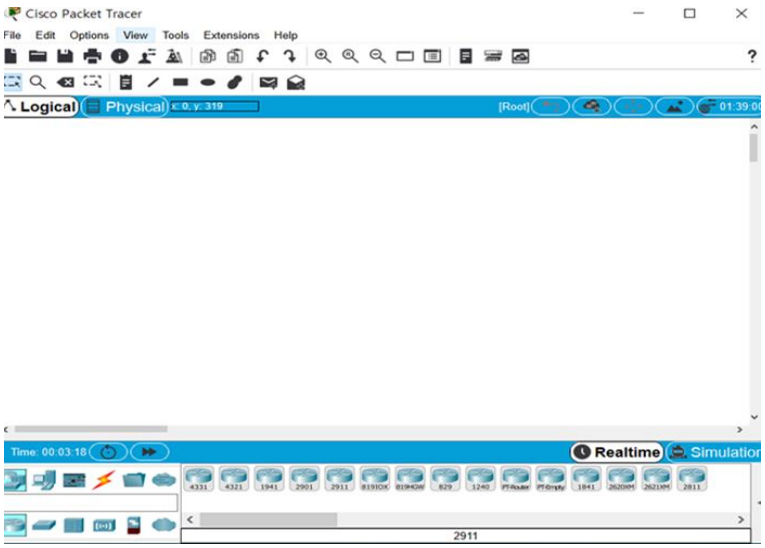
ច. ការកំណត់ពាក្យសម្ងាត់

ពាក្យបញ្ជាពាក្យសម្ងាត់កំណត់សុវត្ថិភាព ដូច្នេះមានតែអ្នកដែលមានសិទ្ធិអាចចូលប្រើឧបករណ៍បាន។

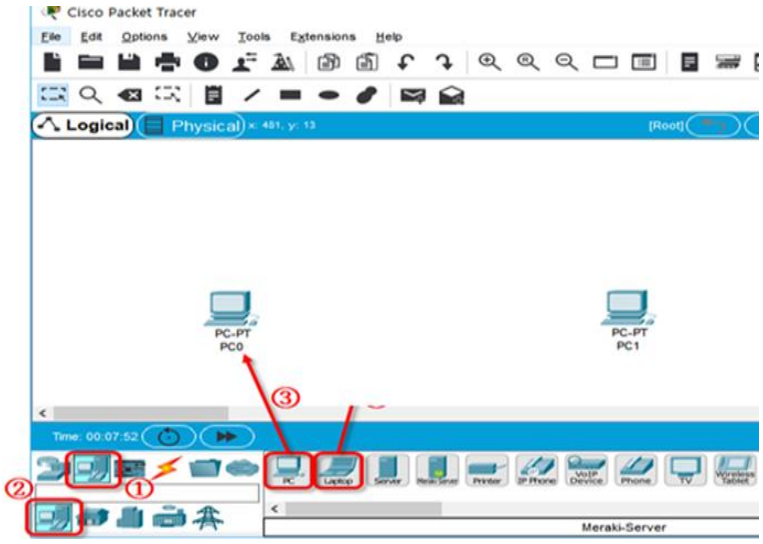
```
Router> enable

Router# configure terminal

Router(config)#enable password [password]
```

ឆ.ការអនុវត្តន៍

១. ប្រតិបត្តិការតាមដានកម្មវិធី



២ បន្ថែមកុំព្យូទ័រ.២

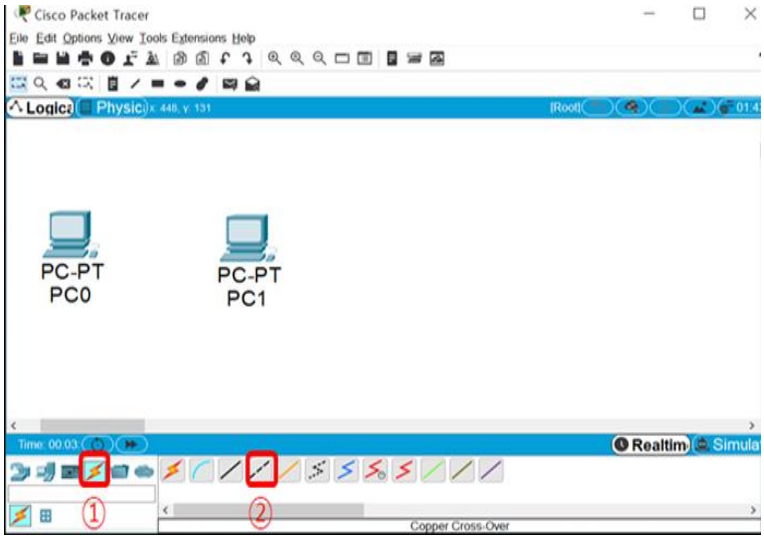


ក. ចុចលើ [ឧបករណ៍បញ្ចប់(End Devices)] → ជ្រើសរើស Desktop

ខ. ចុចលើ [ឧបករណ៍បញ្ចប់(End Devices)] → ជ្រើសរើស Laptop

គ. បន្ទាប់មក ចុចលើ 'PC' ឬLaptop ហើយអូសទម្លាក់លើផ្ទាំងកិច្ចការ

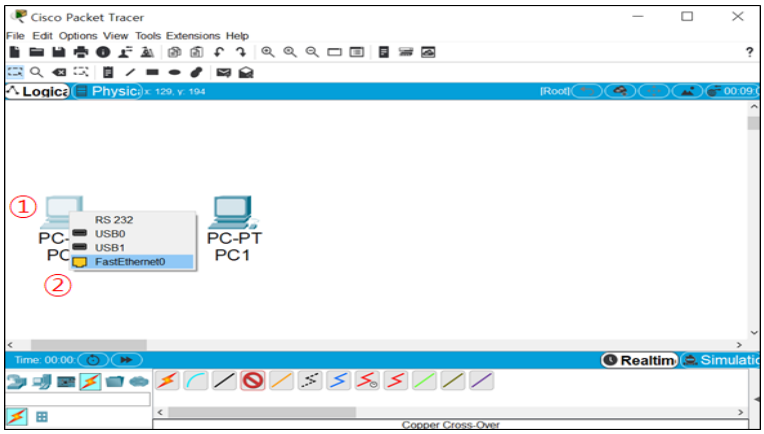
៣.ការភ្ជាប់ខ្សែរវាងកុំព្យូទ័រ ទៅកុំព្យូទ័រ



ក. ចុចលើ [ការតភ្ជាប់(Connection)] លើកុំព្យូទ័រ

ខ. ចុចលើប្រភេទខ្សែរ ដោយជ្រើសរើស [Copper Cross-over]

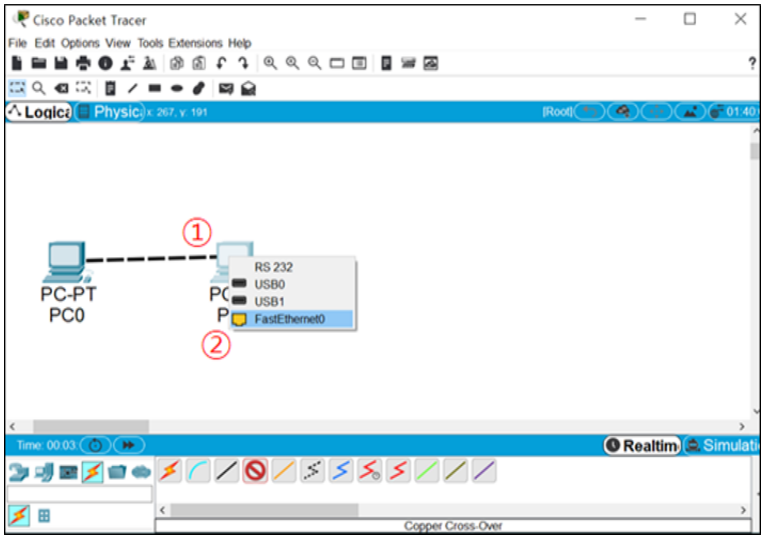
៤. ការភ្ជាប់ខ្សែ(Fast Ethernet) រវាងកុំព្យូទ័រ ទៅកុំព្យូទ័រ



ក. ចុចកណ្តុរខាងឆ្វេងលើ 'PC0'

ខ.ជ្រើសរើស [FastEthernet0]

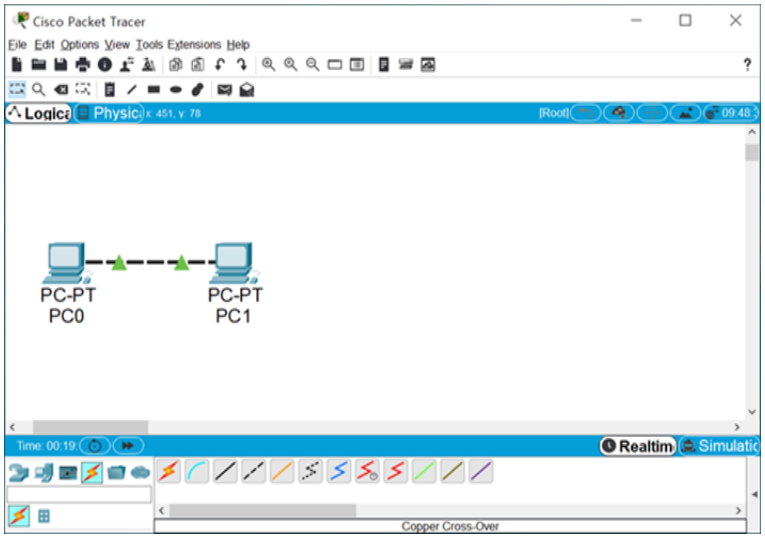
៥. ការភ្ជាប់ខ្សែ(Fast Ethernet) រវាងកុំព្យូទ័រទី១ ទៅកុំព្យូទ័រទី២



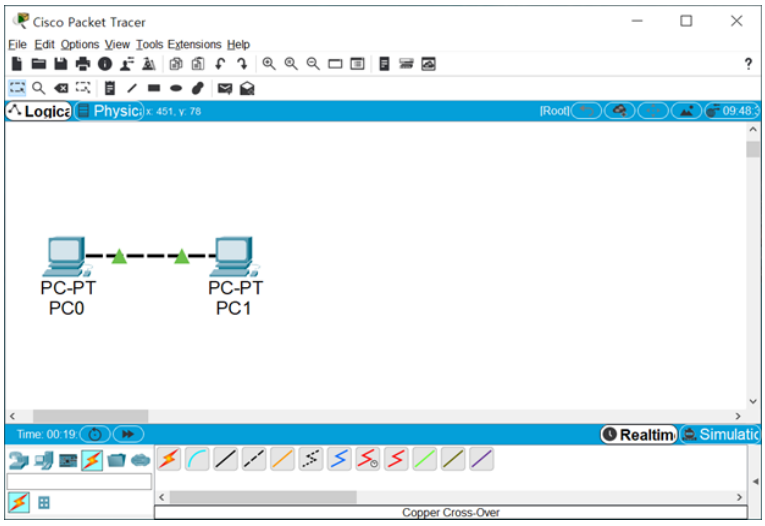
ក. ចុចកណ្តុរខាងឆ្វេងលើ 'PC1'

ខ.ជ្រើសរើស [FastEthernet0]

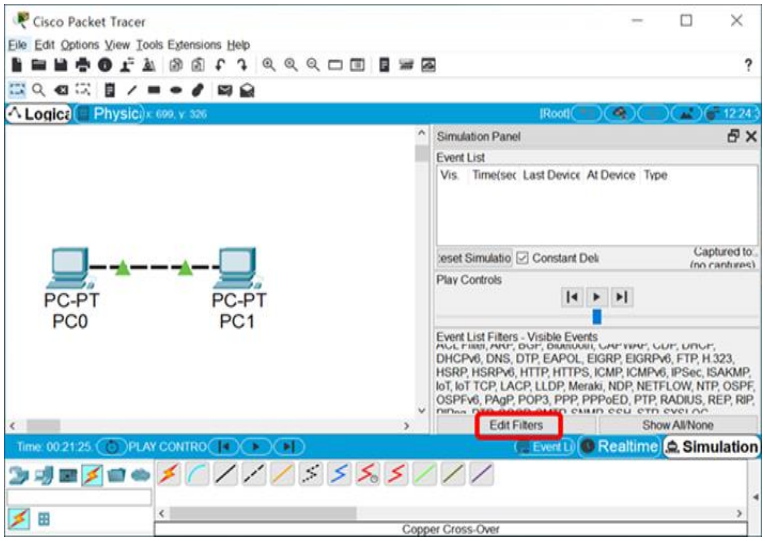
៦. ការបញ្ចប់បណ្តាញមូលដ្ឋាន



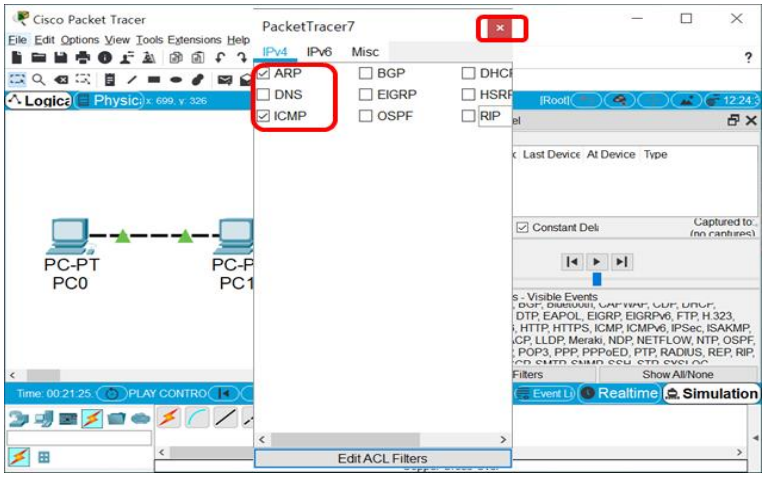
៧. ការផ្ញើ និងទទួលកញ្ចប់ព័ត៌មាននៅក្នុងឧបករណ៍តាមដានកញ្ចប់ព័ត៌មាន



ក. ចុចលើ 'ការក្លែងធ្វើ(Simulation)'

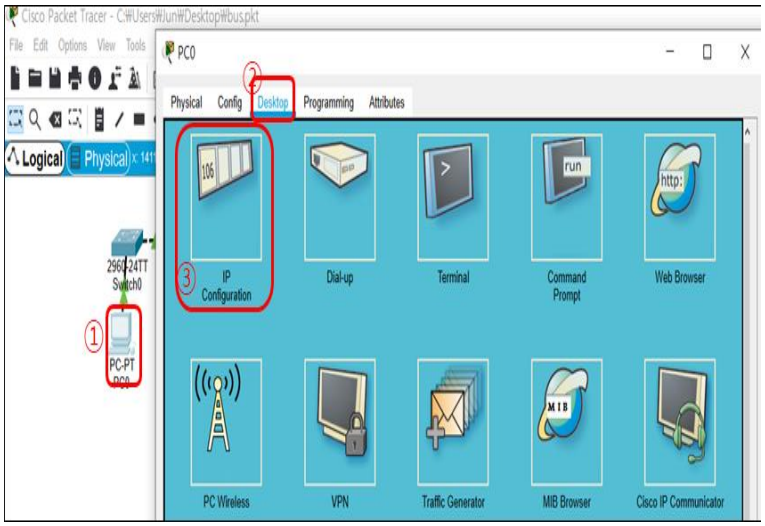


ខ. ចុចលើ 'កែសម្រួលតម្រង(Edit filter)'



គ. ពិនិត្យតែជម្រើសធីកពីរប៉ុណ្ណោះ៖ ARP, ICMP → ចុចបិទ

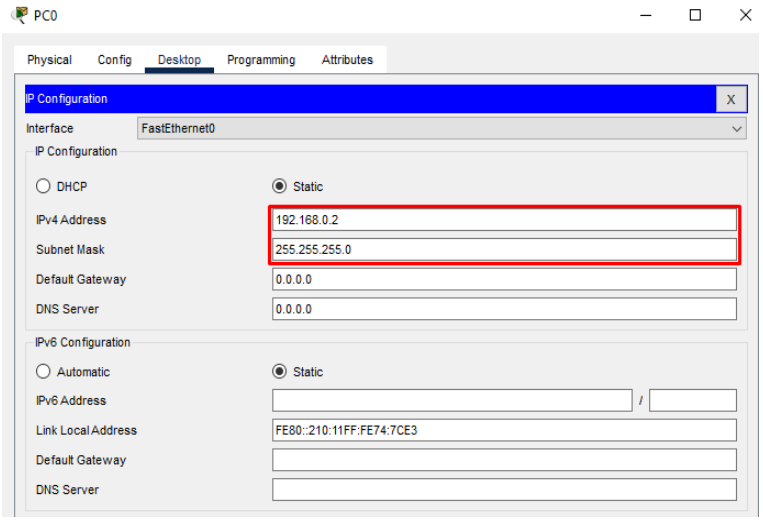
៨. ការកំណត់ IP នៅក្នុង Packet Tracer



ក. យកកណ្តុរចុចពីរដងលើ [PC0]

ខ. ចុចលើ [Desktop]

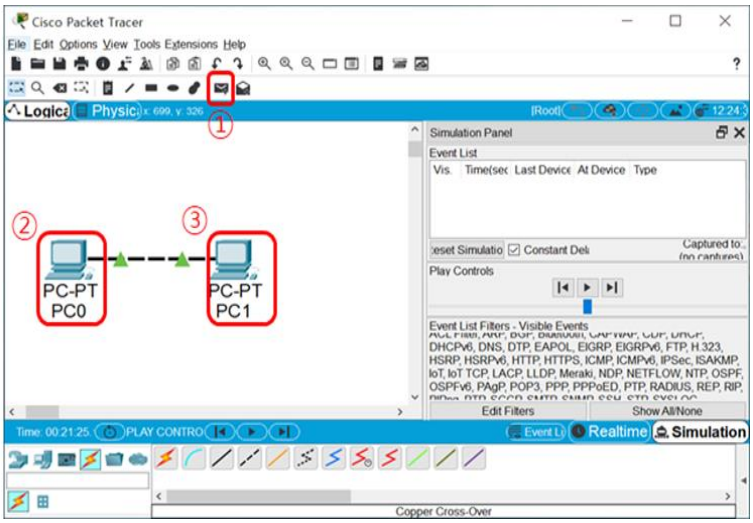
គ.ចុចលើ [IP Configuration]



ឃ. PC0: 192.168.0.2 / 255.255.255.0

ង. PC1: 192.168.0.3 / 255.255.255.0

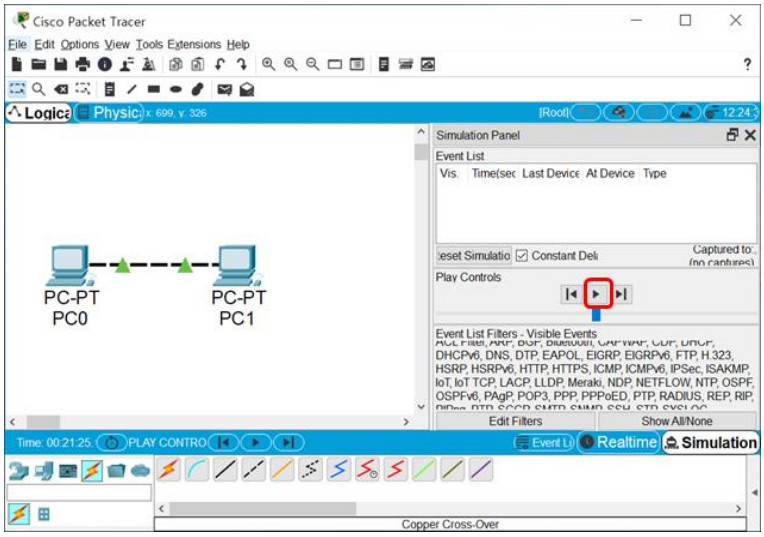
៩. ផ្ញើ PDUs ពីកម្មវិធីតាមដានកញ្ចប់ព័ត៌មាន



ក. ចុចលើ [Simple PDU]

ខ. ចុចលើ [PC0]

គ. ចុចលើ [PC1]



ឃ. ចុចលើប៊ូតុង : [▶] មើលកញ្ចប់ព័ត៌មាន

៩. សន្ទេបការអនុវត្តន៍

នៅក្នុងការអនុវត្តនេះ យើងបានពិនិត្យមើលមុខងារស្តង់ដារនៃរ៉ោតទ័រ និងកុងតាក់។ មុខងារ hostname គឺជាមុខងារមួយដើម្បីបញ្ជាក់ឈ្មោះរបស់ឧបករណ៍។ យើងបានព្យាយាមបញ្ចូល IP និងរចាំងបណ្តាញរងនៃរ៉ោតទ័រដោយដៃ។ នៅពេលអ្នកប្រើប្រាស់ចូលប្រើរ៉ោតទ័រ ឬកុងតាក់ សារបដាបង្ហាញសារជូនដំណឹងមុខងារប្រវត្តិផ្តល់នូវកំណត់ហេតុគន្លឹះ។

ឈ. កិច្ចការស្រាវជ្រាវ

ក. កិច្ចការទី១

១. ប្តូរឈ្មោះរ៉ោតទ័រទៅជា R1 ហើយកំណត់ IP ទៅ 192.168.0.1 / 255.255.25.0

២. ប្តូរឈ្មោះកុងតាក់ទៅ S1 ហើយកំណត់ IP ទៅ 192.168.1.1/ 255.255.255.0

ខ. កិច្ចការទី២

១. នៅពេលភ្ជាប់ទៅឧបករណ៍ “សូមស្វាគមន៍មកកាន់បណ្តាញ!” នឹងត្រូវបានបង្ហាញ

២. កំណត់ពាក្យសម្ងាត់ជា “mater!@” នៅលើឧបករណ៍។

ជំពូកទី ៣
ប្រភេទនៃការបញ្ជូនព័ត៌មាន និងប្រព័ន្ធផ្សព្វផ្សាយ

នៅក្នុងប្រព័ន្ធទំនាក់ទំនងសញ្ញាអាណាឡូកធ្វើដំណើរតាមប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូនដែលមានទំនោរធ្វើឱ្យគុណភាពនៃសញ្ញាអាណាឡូកកាន់តែយ៉ាប់យ៉ឺន។ ភាពមិនល្អឥតខ្ចោះនេះបណ្តាលឱ្យមានការថយចុះនៃសញ្ញានេះ មានន័យថាសញ្ញាដែលទទួលបានគឺខុសពីចលនាដែលបានធ្វើការបញ្ជូនទិន្នន័យគឺជាការផ្ទេរទិន្នន័យពីឧបករណ៍ឌីជីថលមួយទៅឧបករណ៍មួយទៀត។ ការផ្ទេរនេះកើតឡើងតាមរយៈស្ទ្រីមទិន្នន័យពីចំណុចមួយទៅចំណុច ឬបណ្តាញ។ បណ្តាញទាំងនេះពីមុនប្រហែលជាមានទម្រង់ជាខ្សែស្ពាន់ប៉ុន្តែឥឡូវនេះទំនងជាជាផ្នែកមួយនៃបណ្តាញឥតខ្សែ។

ជំពូកទី៣នេះ អ្នកនឹងរៀនអំពី៖

៣.១ ការបញ្ជូនទិន្នន័យ

ស្រទាប់រាងកាយនៅក្នុងគំរូOSI ដើរតួនាទីនៃការធ្វើអន្តរកម្មជាមួយផ្នែករឹងជាក់ស្តែងនិងយន្តការផ្តល់សញ្ញា។ ស្រទាប់រូបវន្តគឺជាស្រទាប់តែមួយគត់នៃគំរូបណ្តាញ OSI ដែលទាក់ទងនឹងការតភ្ជាប់រូបវន្តនៃស្ថានីយពីរស្រទាប់នេះកំណត់ឧបករណ៍ផ្នែករឹង ខ្សែ ខ្សែភ្លើង ប្រេកង់ ជីពចរដែលប្រើដើម្បីតំណាងឱ្យសញ្ញាប្រើប្រាស់គឺ ប្រព័ន្ធគោលពីរ។ ស្រទាប់រូបវន្តផ្តល់សេវាកម្មរបស់វាដល់ស្រទាប់ភ្ជាប់ទិន្នន័យ Data Link Layer ប្រគល់ស៊ុមទៅស្រទាប់រូបវន្តហើយស្រទាប់រាងកាយបំលែងពួកវាទៅ ជាជីពចរអគ្គិសនី ដែលតំណាងឱ្យទិន្នន័យគោលពីរ។ បន្ទាប់មកទិន្នន័យគោលពីរត្រូវបានបញ្ជូនតាមប្រព័ន្ធផ្សព្វផ្សាយដែលមានខ្សែឬឥតខ្សែ។

៣.១.១ សញ្ញា

នៅពេលដែលទិន្នន័យត្រូវបានបញ្ជូនតាមឧបករណ៍ផ្ទុករូបវន្ត នោះដំបូងត្រូវតែបំប្លែងទៅជាសញ្ញាអេឡិចត្រូម៉ាញ៉េទិច។ ទិន្នន័យអាចជាអាណាឡូក ដូចជាសំឡេងមនុស្ស ឬឌីជីថល ដូចជាឯកសារនៅលើថាស ទាំងទិន្នន័យអាណាឡូក និងឌីជីថលអាចត្រូវបានតំណាងជាសញ្ញាឌីជីថល ឬអាណាឡូក។

- **សញ្ញាឌីជីថល៖** សញ្ញាឌីជីថលមានលក្ខណៈដាច់ដោយឡែកពីគ្នា និងតំណាងឱ្យលំដាប់នៃវ៉ុលជីពចរសញ្ញាឌីជីថលត្រូវបានប្រើនៅក្នុងសៀគ្វីនៃប្រព័ន្ធកុំព្យូទ័រ។
- **សញ្ញាអាណាឡូក៖** សញ្ញាអាណាឡូកស្ថិតនៅក្នុងទម្រង់រលកបន្តក្នុងធម្មជាតិ និងតំណាងដោយរលកអេឡិចត្រូម៉ាញ៉េទិចថេរ។

៣.១.២ គាពអនុថយនៃការបញ្ជូន

នៅពេលដែលសញ្ញាធ្វើដំណើរឆ្លងកាត់ឧបករណ៍ផ្ទុកហើយសញ្ញាញមានទំនោរទៅកាន់តែលំបាកអាចបណ្តាលមកពីហេតុផលជាច្រើនដូចដែលបានផ្តល់ឱ្យ៖

- **ភាពរំជើបរំជួល៖** សញ្ញាត្រូវតែខ្លាំងគ្រប់គ្រាន់សម្រាប់អ្នកទទួលដើម្បីបកស្រាយទិន្នន័យបានត្រឹមត្រូវ។ នៅពេលដែលសញ្ញាឆ្លងកាត់ឧបករណ៍ផ្ទុក វាមានទំនោរទៅខ្សោយនៅពេលដែលវាគ្របដណ្តប់ចម្ងាយវាបាត់បង់កម្លាំង។
- **ការបែកខ្ញែក៖** នៅពេលដែលសញ្ញាធ្វើដំណើរតាមប្រព័ន្ធផ្សព្វផ្សាយ វារីករាលដាល និងត្រួតលើគ្នា បរិមាណនៃការបែកខ្ញែកអាស្រ័យលើប្រេកង់ដែលបានប្រើ។
- **ការបង្ខូចទ្រង់ទ្រាយការពន្យារពេល៖** សញ្ញាត្រូវបានបញ្ជូនតាមប្រព័ន្ធផ្សព្វផ្សាយជាមួយនឹងល្បឿននិងប្រេកង់ដែលបានកំណត់ជាមុន។ ប្រសិនបើល្បឿន និងប្រេកង់សញ្ញាមិនត្រូវគ្នាវាមានលទ្ធភាពដែលសញ្ញាទៅដល់គោលដៅនៅក្នុងប្រព័ន្ធផ្សព្វផ្សាយឌីជីថលវាមានសារសំខាន់ខ្លាំងណាស់ដែលប៊ីតខ្លះមកដល់មុនជាងការផ្ញើពីមុន។

- **សំឡេងរំខាន៖** ការរំខានដោយចៃដន្យ ឬការប្រែប្រួលនៃសញ្ញាអាណាឡូក ឬឌីជីថលត្រូវបានគេនិយាយថាជា សំឡេងរំខាន នៅក្នុងសញ្ញាដែលអាចបង្ខូចទ្រង់ទ្រាយព័ត៌មានពិតដែលកំពុងអនុវត្ត។ សំឡេងរំខានអាចត្រូវបានកំណត់លក្ខណៈនៅក្នុងថ្នាក់មួយដូចខាងក្រោម៖
    - **សំឡេងរំខានកម្តៅ៖** កំដៅធ្វើឱ្យរំញ័រឧបករណ៍អេឡិចត្រូនិករបស់ឧបករណ៍ផ្ទុកដែលអាចបង្ហាញសំឡេងរំខាននៅក្នុងប្រព័ន្ធផ្សព្វផ្សាយ រហូតដល់កម្រិតជាក់លាក់មួយសំឡេងកម្តៅគឺមិនអាចជៀសបានឡើយ។
    - **អន្តរម៉ូឌុល៖** នៅពេលដែលប្រែកង់ជាច្រើនចែករំលែកឧបករណ៍ផ្ទុកមួយ ការជ្រៀតជ្រែកហើយអាចបណ្តាលឱ្យមានសម្លេងរំខាននៅក្នុងឧបករណ៍ផ្ទុក។ សម្លេងរំខានអន្តរម៉ូឌុលកើតឡើងប្រសិនបើប្រែកង់ពីរផ្សេងគ្នាចែករំលែកឧបករណ៍ផ្ទុកមួយហើយមួយមានកម្លាំងលើស សមាសធាតុដំណើរការត្រឹមត្រូវហើយប្រែកង់លទ្ធផលអាចត្រូវបានចែកចាយខុសពីការរំពឹងទុក។
    - **ការនិយាយឆ្លង៖**សំឡេងរំខាននេះកើតឡើងនៅពេលដែលសញ្ញាបរទេសចូលក្នុងប្រព័ន្ធផ្សព្វផ្សាយ។នេះគឺដោយសារតែសញ្ញានៅក្នុងឧបករណ៍ផ្ទុកមួយប៉ះពាល់ដល់សញ្ញានៃឧបករណ៍ផ្ទុកទីពីរ។
    - **កម្លាំងរុញច្រាន៖**សំឡេងរំខាននេះត្រូវបានណែនាំដោយសារតែការរំខានមិនទៀងទាត់ដូចជារន្ទះ អគ្គិសនីសៀគ្វីខ្លី ឬសមាសធាតុខុស។ ទិន្នន័យឌីជីថលត្រូវបានរងផលប៉ះពាល់ជាចម្បងដោយប្រភេទនៃសំឡេងរំខាននេះ។

៣.១.៣ ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូន

ប្រព័ន្ធផ្សព្វផ្សាយដែលព័ត៌មានរវាងប្រព័ន្ធកុំព្យូទ័រពីរត្រូវបានបញ្ជូនហៅថាមេឌៀបញ្ជូន។ ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូនមានពីរទម្រង់៖

- **ប្រព័ន្ធផ្សព្វផ្សាយណែនាំ៖** ខ្សែភ្លើង ខ្សែទំនាក់ទំនងទាំងអស់គឺជាប្រព័ន្ធផ្សព្វផ្សាយណែនាំដូចជា UTP ខ្សែ coaxial និងខ្សែកាបអុបទិក។ នៅក្នុងប្រព័ន្ធផ្សព្វផ្សាយនេះ អ្នកផ្ញើ និងអ្នកទទួលត្រូវបានភ្ជាប់ដោយផ្ទាល់ហើយព័ត៌មានត្រូវបានបញ្ជូនតាមរយៈវា។
- **ប្រព័ន្ធផ្សព្វផ្សាយដែលមិនមានការណែនាំ៖**ចន្លោះឥតខ្សែ ឬខ្យល់បើកចំហត្រូវបានគេនិយាយថាជាប្រព័ន្ធផ្សព្វផ្សាយដែលមិនមានការណែនាំពីព្រោះមិនមានការតភ្ជាប់រវាងអ្នកផ្ញើ និងអ្នកទទួល។ ព័ត៌មានត្រូវបានផ្សព្វផ្សាយនៅលើបណ្តាញប្រព័ន្ធហើយនរណាម្នាក់ រួមទាំងអ្នកទទួលពិតប្រាកដអាចប្រមូលព័ត៌មានបាន។

សមត្ថភាពប៉ុស្តិ៍

ល្បឿននៃការបញ្ជូនព័ត៌មានត្រូវបានគេនិយាយថាជាសមត្ថភាពឆានែលយើងរាប់វាជាអត្រាទិន្នន័យនៅក្នុងពិភពឌីជីថលវាអាស្រ័យលើកត្តាជាច្រើនដូចជា៖

- **កម្រិតបញ្ជូន៖** ការកំណត់រូបវន្តនៃមេឌៀមូលដ្ឋាន។
- **អត្រាកំហុស៖** ការទទួលព័ត៌មានមិនត្រឹមត្រូវ ដោយសារសំឡេងរំខាន។
- **ការអ៊ីនកូដ៖** ចំនួនកម្រិតដែលប្រើសម្រាប់ផ្តល់សញ្ញា។

ម៉ាល់ធីភ្លិចស៊ីង (Multiplexing)

ម៉ាល់ធីភ្លិចស៊ីង(Multiplexing) គឺជាបច្ចេកទេសមួយដើម្បីលាយនិងបញ្ជូនទិន្នន័យជាច្រើនលើឧបករណ៍ផ្ទុកមួយ។ បច្ចេកទេសនេះទាមទារផ្នែករឹងប្រព័ន្ធដែលហៅថាម៉ាល់ធីភ្លិចហ្ស៊ីរ(MUX) សម្រាប់ម៉ាល់ធីភ្លិចស៊ីងស្ទ្រីម និងបញ្ជូនវានៅលើ មេឌៀ មួយ និង ឌីម៉ាល់ធីភ្លិចហ្ស៊ីរ(DMUX) ដែលយកព័ត៌មានពី មេឌៀហើយចែកចាយវាទៅទិសដៅផ្សេងៗគ្នា។

កុងតាក់

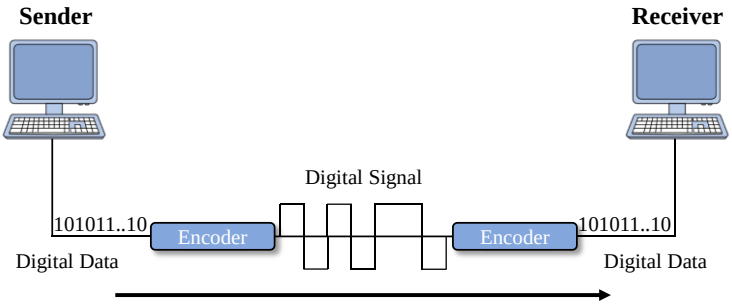
កុងតាក់គឺជាយន្តការមួយដែលទិន្នន័យព័ត៌មានត្រូវបានបញ្ជូនពីប្រភពឆ្ពោះទៅកាន់គោលដៅ ដែលមិនត្រូវបានភ្ជាប់ដោយផ្ទាល់។ បណ្តាញមានឧបករណ៍តភ្ជាប់គ្នាដែលទទួលទិន្នន័យពីប្រភពដែលបានភ្ជាប់ដោយផ្ទាល់រក្សាទុកវា វិភាគវា ហើយបន្ទាប់មកបញ្ជូនវាទៅឧបករណ៍ភ្ជាប់ទំនាក់ទំនងបន្ទាប់ដែលនៅជិតបំផុតទៅនឹងគោលដៅ។

៣.២ ការបញ្ជូនឌីជីថល

ទិន្នន័យឬព័ត៌មានអាចត្រូវបានរក្សាទុកតាមពីរយ៉ាងគឺអាណាឡូកនិងឌីជីថលសម្រាប់កុំព្យូទ័រប្រើទិន្នន័យវាត្រូវតែស្ថិតក្នុងទម្រង់ឌីជីថលដាច់ពីគ្នាស្រដៀងនឹងទិន្នន័យដែរសញ្ញាក៏អាចស្ថិតនៅក្នុងទ្រង់ទ្រាយអាណាឡូក និងឌីជីថលផងដែរដើម្បីបញ្ជូនទិន្នន័យឌីជីថលដំបូងវាត្រូវតែប្តូរទៅជាទម្រង់ឌីជីថល។

៣.២.១ ការបំលែងពីឌីជីថល ទៅឌីជីថល

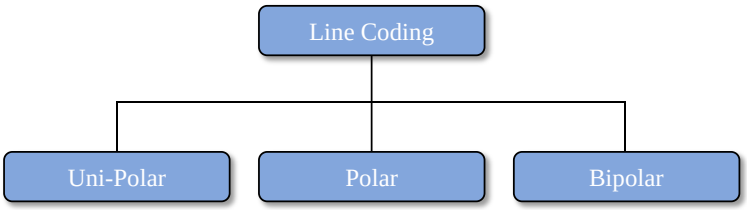
ផ្នែកនេះពន្យល់ពីរបៀបបំប្លែងទិន្នន័យឌីជីថលទៅជាសញ្ញាឌីជីថលវាអាចត្រូវបានធ្វើតាមពីរវិធី គឺការសរសេរកូដបន្ទាត់ និងការសរសេរកូដប្លុក សម្រាប់ទំនាក់ទំនងទាំងអស់ ការសរសេរកូដតាមបន្ទាត់គឺចាំបាច់ ចំណែកការសរសេរកូដប្លុកគឺស្រេចចិត្ត។



រូបភាពទី ៣.១ ឌីជីថលទៅឌីជីថល

ឡាញ្ជកូដឌីជ

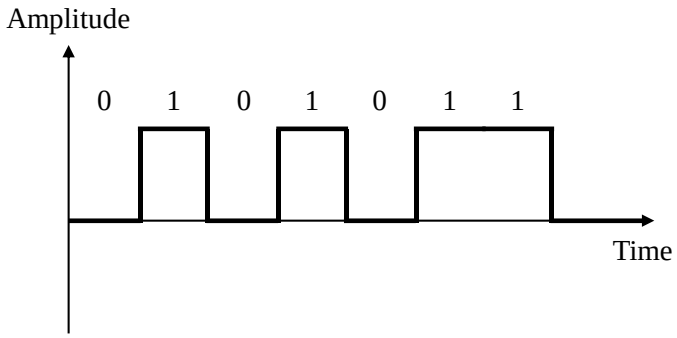
ដំណើរការនៃការបំប្លែងទិន្នន័យឌីជីថល ទៅជាសញ្ញាឌីជីថលត្រូវបានគេនិយាយថា ឡាញ្ជកូដឌីជ ទិន្នន័យឌីជីថលត្រូវបានរកឃើញជាទម្រង់ប្រព័ន្ធគោលពីរ វាត្រូវបានតំណាង (រក្សាទុក) ខាងក្នុងជាស៊េរីនៃ ១s និង 0s។ សញ្ញាឌីជីថលត្រូវបានតំណាងដោយសញ្ញាមិនប្រុងប្រយ័ត្ន ដែលតំណាងឱ្យទិន្នន័យឌីជីថល គ្រោងការណ៍សរសេរកូដបន្ទាត់មានបីប្រភេទ៖



រូបភាពទី ៣.២ ប្រភេទឡាញ្ជកូដឌីជ

ក. ការអ៊ិនកូដ Uni-polar

គ្រោងការណ៍ការអ៊ិនកូដ Unipolar ប្រើកម្រិតវ៉ុលតែមួយដើម្បីតំណាងឱ្យទិន្នន័យ។ ក្នុងករណីនេះ ដើម្បីតំណាងឱ្យប្រព័ន្ធគោលពីរ ១ តង់ស្យុងខ្ពស់ត្រូវបានបញ្ជូន ហើយដើម្បីតំណាងឱ្យ 0 មិនមានវ៉ុលត្រូវបានបញ្ជូនទេ។ វាត្រូវបានគេហៅផងដែរថា unipolar-non-return-to-zero ពីព្រោះមិនមានលក្ខខណ្ឌនៅសល់ ពោលគឺវាតំណាងឱ្យ ១ ឬ 0។



រូបភាព ៣.៣ ការអ៊ិនកូដ Uni-polar

ខ. ការអ៊ិនកូដរាងប៉ូល (Polar)

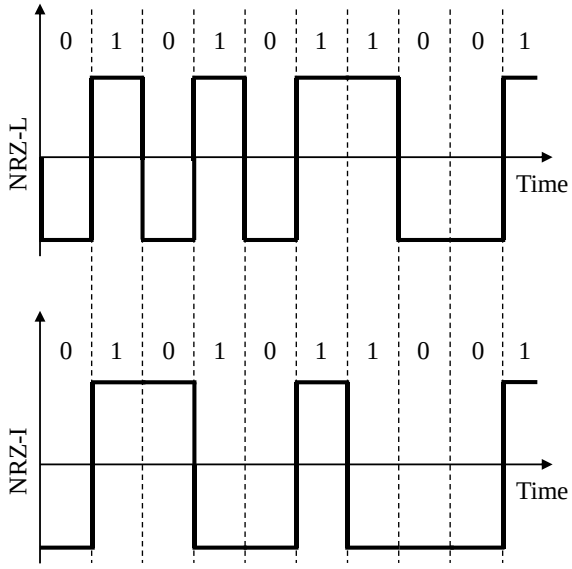
គ្រោងការណ៍ការអ៊ិនកូដរាងប៉ូលប្រើកម្រិតវ៉ុលច្រើនដើម្បីតំណាងឱ្យតម្លៃគោលពីរ ហើយកូដប៉ូឡាគឺជាកូដកែកំហុសប្តូកលីនេអ៊ែរ។ ការបង្កើតកូដគឺផ្អែកលើការភ្ជាប់គ្នាឡើងវិញ ច្រើននៃកូដខឺណែលខ្លីដោយបំប្លែងឆានែលរូបវន្តទៅជាបណ្តាញខាងក្រៅនិម្មិត។ នៅពេលដែលចំនួននៃការផ្សាយឡើងវិញកាន់តែធំបណ្តាញនិម្មិតមានទំនោរមានភាពជឿជាក់ខ្ពស់ ឬភាពជឿជាក់ទាប (និយាយម្យ៉ាងទៀត ពួកវាប្រែជារាងប៉ូល ឬកាន់តែតូច) ។ ប៊ីតទិន្នន័យត្រូវបានបែងចែកទៅជាបណ្តាញដែលអាចទុកចិត្តបំផុតសម្រាប់វានោះគឺជាលេខកូដដំបូងដែលមានការស្តាបនាយ៉ាងច្បាស់លាស់ដើម្បីសម្រេចបាននូវសមត្ថភាពឆានែល សម្រាប់ស៊ីមេទ្រីការបញ្ជូលប្រព័ន្ធគោលពីរ, ដាច់ពីគ្នា, ឆានែលគ្មានការចងចាំ (B-DMC) ជាមួយនឹងការពឹងផ្អែកពហុនាមលើគម្លាតទៅនឹងសមត្ថភាព។

ហើយការអ៊ិនកូដរាងប៉ូលមានបីប្រភេទគឺ៖

- Polar None ត្រឡប់ទៅសូន្យ (Polar NRZ)
- NRZ មានបំរែបំរួលពីរ (NRZ-L និង NRZ-I)
- ត្រឡប់ទៅសូន្យ (RZ)

Polar None ត្រឡប់ទៅសូន្យ (Polar NRZ)

វាប្រើកម្រិតវ៉ុលពីរផ្សេងគ្នាដើម្បីតំណាងឱ្យតម្លៃគោលពីរជាទូទៅវ៉ុលវិជ្ជមានតំណាងឱ្យ១ ហើយតម្លៃអវិជ្ជមានតំណាងឱ្យ 0 វាក៏ជា NRZ ផង។



រូបភាពទី ៣.៨ Polar None *ត្រឡប់ទៅសូន្យ (ប៉ូល* NRZ)

NRZ **មានបំរែបំរួលពីរ** (NRZ-L **និង** NRZ-I)

- NRZ-L ផ្លាស់ប្តូរកម្រិតវ៉ុល នៅពេលដែលប៊ីតផ្សេងគ្នាត្រូវបានជួបប្រទះ
- NRZ-I ផ្លាស់ប្តូរវ៉ុលនៅពេលដែលទីតាំងមួយស្ថិតនៅ។

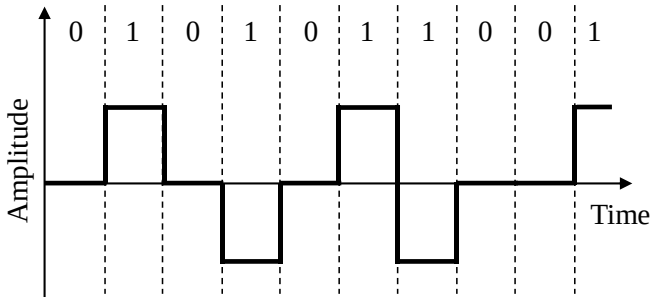
ត្រឡប់ទៅសូន្យ (RZ)

បញ្ហាជាមួយ NRZ គឺថាអ្នកទទួលមិនអាចសន្និដ្ឋានបាននៅពេលបញ្ចប់បន្តិច ហើយនៅពេលដែលប៊ីតបន្ទាប់ត្រូវបានចាប់ផ្តើម នៅពេលដែលនាឡិការបស់អ្នកផ្ញើ និងអ្នកទទួលមិនត្រូវបានធ្វើសមកាលកម្ម។ RZ ប្រើកម្រិតវ៉ុលបី វ៉ុលវិជ្ជមានតំណាងឱ្យ ១ វ៉ុលអវិជ្ជមានតំណាងឱ្យ ០និងវ៉ុលសូន្យសម្រាប់គ្មាន។ សញ្ញាផ្លាស់ប្តូរកំឡុងពេលប៊ីត មិនមែនរវាងប៊ីតទេ។

- **Manchester៖** គ្រោងការណ៍ការអ៊ិនកូដនេះគឺជាការរួមបញ្ចូលគ្នានៃ RZ និង NRZ-L ។ ពេលវេលាប៊ីតត្រូវបានបែងចែកជាពីរផ្នែកហើយវាឆ្លងកាត់ពាក់កណ្តាលនៃប៊ីត និងផ្លាស់ប្តូរដំណាក់កាលនៅពេលដែលប៊ីតផ្សេងគ្នាត្រូវបានជួបប្រទះ។
- **ឌីផេរ៉ង់ស្យែល Manchester៖** គ្រោងការណ៍ការអ៊ិនកូដនេះគឺជាការរួមបញ្ចូលគ្នានៃ RZ និង NRZ-I ។ វាក៏ឆ្លងកាត់នៅពាក់កណ្តាលប៊ីត ប៉ុន្តែផ្លាស់ប្តូរដំណាក់កាលតែនៅពេលដែលជួប ១ ប៉ុណ្ណោះ។

គ. ការអ៊ិនកូដ Bipolar

ការអ៊ិនកូដ bipolar ប្រើកម្រិតវ៉ុលបី វិជ្ជមាន អវិជ្ជមាន និងសូន្យ វ៉ុលសូន្យតំណាងឱ្យប្រព័ន្ធគោលពីរ ០ ហើយប៊ីត ១ ត្រូវបានតំណាងដោយការផ្លាស់ប្តូរវ៉ុលវិជ្ជមាន និងអវិជ្ជមាន។



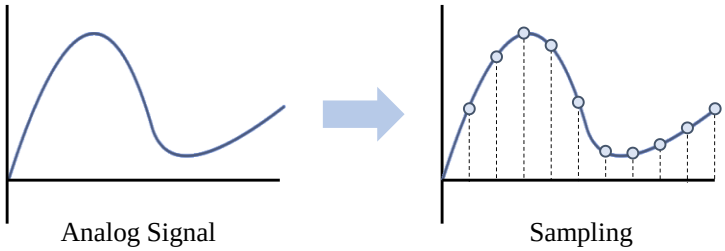
រូបភាពទី ៣.៥ ការអ៊ិនកូដ Bipolar

៣.២.២ ការបំប្លែងអាណាឡូកទៅឌីជីថល

មីក្រូហ្វូនបង្កើតសំឡេងអាណាឡូក ហើយកាមេរ៉ាបង្កើតវីដេអូអាណាឡូក ដែលត្រូវបានចាត់ទុកជាទិន្នន័យអាណាឡូក។ ដើម្បីបញ្ជូនទិន្នន័យអាណាឡូកនេះតាមសញ្ញាឌីជីថល យើងត្រូវការការបំប្លែងអាណាឡូកទៅឌីជីថល។ទិន្នន័យអាណាឡូកគឺជាការបន្តនៃទិន្នន័យនៅក្នុងទម្រង់រលកចំណែកទិន្នន័យឌីជីថលគឺជាច់ដោយឡែក យើងប្រើ Pulse Code Modulation (PCM) ដើម្បីបំប្លែងរលកអាណាឡូកទៅជាទិន្នន័យឌីជីថល។ PCM គឺជាវិធីសាស្ត្រមួយដែលគេប្រើជាទូទៅបំផុតដើម្បីបំប្លែងទិន្នន័យអាណាឡូកទៅជាទម្រង់ឌីជីថលហើយវារួមបញ្ចូលបីជំហាន៖

- គំរូ
- បរិមាណ
- ការអ៊ិនកូដ

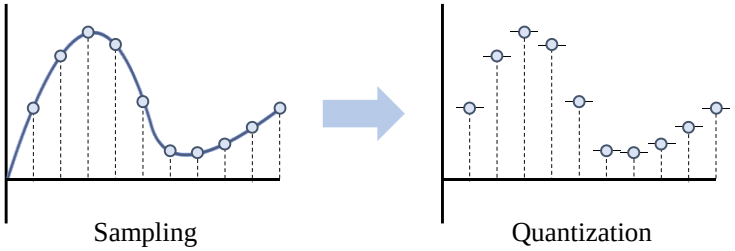
ក. គំរូ



រូបភាពទី ៣.៦ គំរូ

សញ្ញាអាណាឡូកត្រូវបានយកគំរូតាមរាល់ចន្លោះ T កត្តាសំខាន់បំផុតក្នុងការជ្រើសរើសគឺ អត្រាដែលសញ្ញាអាណាឡូកត្រូវបានយកគំរូតាម។ យោងតាមទ្រឹស្តីបទ NY Quist អត្រាគំរូត្រូវតែមានយ៉ាងហោចណាស់ពីរដងនៃប្រេកង់ខ្ពស់បំផុតរបស់សញ្ញា។

ខ. បរិមាណ

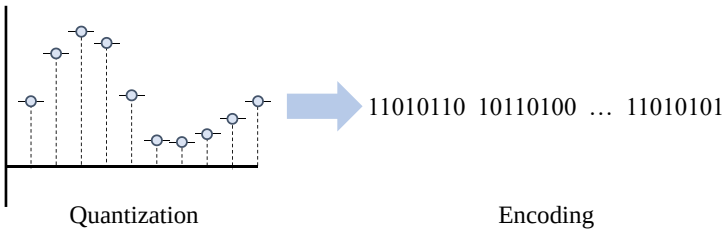


រូបភាពទី ៣.៧ បរិមាណ

គំរូផ្តល់លទ្ធផលជាទម្រង់ដាច់ពីគ្នានៃសញ្ញាអាណាឡូក បន្តរាល់លំនាំដាច់ពីគ្នាបង្ហាញ ពីទំហំនៃសញ្ញាអាណាឡូកនៅក្នុងឧទាហរណ៍នោះ។ បរិមាណត្រូវបានធ្វើរវាងតម្លៃអតិបរមា និងអប្បបរមា។ បរិមាណគឺជាតម្លៃប្រហាក់ប្រហែលនៃតម្លៃអាណាឡូកភ្លាមៗ។

គ. ការអ៊ិនកូដ

នៅក្នុងការអ៊ិនកូដតម្លៃប្រហាក់ប្រហែលនីមួយៗត្រូវបានបំប្លែងទៅជាទម្រង់គោលពីរ



រូបភាពទី ៣.៨ ការអ៊ិនកូដ

៣.២.៣ វិធីបែបនៃការបញ្ជូន

របៀបបញ្ជូនមានន័យថាផ្នែរទិន្នន័យរវាងឧបករណ៍ពីរ វាត្រូវបានគេស្គាល់ផងដែរថាជារបៀបទំនាក់ទំនងខ្សែបញ្ជូន និងបណ្តាញត្រូវបានរចនាឡើងដើម្បីអនុញ្ញាតឱ្យទំនាក់ទំនងកើតឡើងរវាងឧបករណ៍នីមួយៗដែលមានទំនាក់ទំនងគ្នាទៅវិញទៅមក។ ហើយវាត្រូវបានកំណត់ជាពីរបៀបដែលទិន្នន័យត្រូវបានបញ្ជូនរវាងកុំព្យូទ័រពីរ។ ទិន្នន័យគោលពីរក្នុងទម្រង់ ១ និង ០ អាចត្រូវបានធ្វើជាទម្រង់ប៉ារ៉ាឡែល និងសៀរៀល។

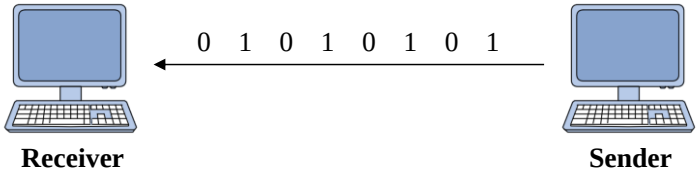
ក. ការបញ្ជូនប៉ារ៉ាឡែល

រូបភាពទី ៣.៩ ការបញ្ជូនប៉ារ៉ាឡែល

ប៊ីតគោលពីរត្រូវបានរៀបចំជាក្រុមនៃប្រវែងថេរទាំងអ្នកផ្ញើ និងអ្នកទទួលត្រូវបានភ្ជាប់ស្របគ្នាជាមួយនឹងចំនួនបន្ទាត់ទិន្នន័យស្មើគ្នា។ កុំព្យូទ័រទាំងពីរបែងចែករវាងខ្សែទិន្នន័យលំដាប់ខ្ពស់ និងលំដាប់ទាប អ្នកផ្ញើផ្ញើប៊ីតទាំងអស់ក្នុងពេលតែមួយនៅលើបន្ទាត់ទាំងអស់ដោយសារតែបន្ទាត់ទិន្នន័យស្មើនឹងចំនួនប៊ីតក្នុងក្រុម ឬស៊ុមទិន្នន័យ ក្រុមទាំងមូលនៃប៊ីត (ស៊ុមទិន្នន័យ) ត្រូវបានផ្ញើក្នុងមួយពេល អត្ថប្រយោជន៍នៃការបញ្ជូនប៉ារ៉ាឡែលគឺល្បឿនលឿន ហើយគុណវិបត្តិគឺតម្លៃនៃខ្សែភ្លើងព្រោះវាស្មើនឹងចំនួនប៊ីតដែលបញ្ជូនស្របគ្នា។

ខ. ការបញ្ជូនសៀរៀល

នៅក្នុងការបញ្ជូនសៀរៀល ប៊ីតត្រូវបានបញ្ជូនពីមួយទៅមួយក្នុងលក្ខណៈជាជួរព័ត៌មានសៀរៀលត្រូវការតែបណ្តាញទំនាក់ទំនងមួយប៉ុណ្ណោះ។ ផ្នែករឹងដែលត្រូវការដើម្បីបំប្លែងទិន្នន័យរវាងទម្រង់ប៉ារ៉ាឡែលខាងក្នុង និងទម្រង់សៀរៀលអាចត្រង់ ឬស្មុគស្មាញអាស្រ័យលើប្រភេទនៃយន្តការទំនាក់ទំនងសៀរៀល។ ក្នុងករណីសាមញ្ញបំផុតបន្ទះឈីបតែមួយឧបករណ៍ទទួល និងបញ្ជូនអសមកាលសកល (UART) ដំណើរការការបំប្លែងបន្ទះឈីបដែលទាក់ទង, សមកាលកម្មសកល អ្នកទទួលអសមកាល, និងឧបករណ៍បញ្ជូន (USART) គ្រប់គ្រងការបំប្លែងសម្រាប់បណ្តាញដែលធ្វើសមកាលកម្ម។



រូបភាពទី ៣.១០ ការបញ្ជូនសៀរៀល

ខ.១.ការបញ្ជូនសៀរៀលអសមកាល

វាត្រូវបានគេដាក់ឈ្មោះដូច្នេះដោយសារតែមិនមានសារៈសំខាន់លើពេលវេលាប៊ីតទិន្នន័យមានលំនាំជាក់លាក់ដែលជួយអ្នកទទួលទទួលស្គាល់ការចាប់ផ្តើម និងចុងបញ្ចប់នៃប៊ីតទិន្នន័យ។ ឧទាហរណ៍ 0 ត្រូវបានបញ្ជូលបុព្វបទលើរាល់បៃទិន្នន័យ ហើយ 1s ឬច្រើនត្រូវបានបន្ថែមនៅចុងបញ្ចប់ ហើយស៊ុមទិន្នន័យបន្តពីរ (បៃ) អាចមានគម្លាតរវាងពួកវា។

ខ.២. ការបញ្ជូនសៀរៀលសមកាលកម្ម

ការកំណត់ពេលវេលាក្នុងការបញ្ជូនសមកាលកម្មមានសារសំខាន់ ដោយសារចាំបាច់ត្រូវមានយន្តការមួយដែលត្រូវអនុវត្តតាម ដើម្បីសម្គាល់ការចាប់ផ្តើម និងចុងបញ្ចប់នៃប៊ីតទិន្នន័យ។ មិនមានលំនាំ ឬវិធីបុព្វបទ/បច្ច័យទេ ប៊ីតទិន្នន័យត្រូវបានផ្ញើក្នុងរបៀបផ្ទុកដោយមិនរក្សាគម្លាតរវាងបៃ (៨ ប៊ីត)។ ប៊ីតទិន្នន័យដែលផ្ទុកតែមួយអាចមានបៃជាច្រើនដូច្នេះហើយពេលវេលាមានសារសំខាន់ខ្លាំងណាស់លើអ្នកទទួលក្នុងការទទួលស្គាល់ និងបំបែកប៊ីតទៅជាបៃ។ អត្ថប្រយោជន៍នៃការបញ្ជូនសមកាលកម្មគឺជាល្បឿនខ្ពស់ ហើយវាមិនមានលើសពីការបន្ថែមបឋមកថា និងបាតកថាប៊ីតដូចនៅក្នុងការបញ្ជូនអសមកាលនោះទេ។

៣.៣ ការបញ្ជូនអាណាឡូក

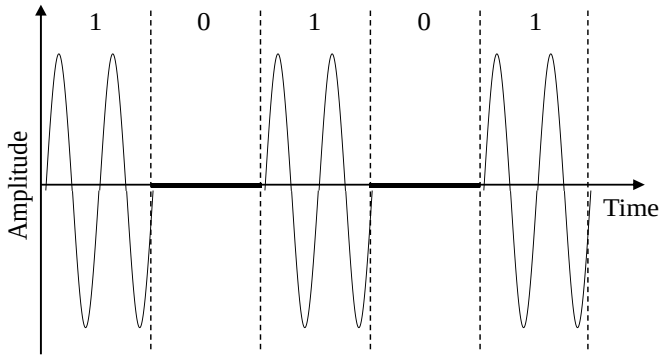
វាត្រូវការបំប្លែងទៅជាសញ្ញាអាណាឡូក ដើម្បីបញ្ជូនទិន្នន័យឌីជីថលតាមប្រព័ន្ធផ្សព្វផ្សាយអាណាឡូក ហើយវាអាចមានពីរករណីយោងទៅតាមការធ្វើទ្រង់ទ្រាយទិន្នន័យ។

- **Band pass៖** តម្រងត្រូវបានប្រើដើម្បីត្រង និងឆ្លងកាត់ប្រេកង់ដែលចាប់អារម្មណ៍ band pass គឺជាក្រុមប្រេកង់ដែលអាចផ្តល់ឱ្យតម្រង។
- **Low-pass៖** គឺជាតម្រងដែលបញ្ជូនសញ្ញាប្រេកង់ទាបហើយ បំប្លែងឌីជីថល ទៅអាណាឡូក នៅពេលដែលទិន្នន័យឌីជីថលត្រូវបានបំប្លែងទៅជាសញ្ញាអាណាឡូក band pass ។ វាត្រូវបានគេហៅថាការបំប្លែងពីអាណាឡូក ទៅអាណាឡូក នៅពេលដែលសញ្ញាអាណាឡូកឆ្លងទាបត្រូវបានបំប្លែងទៅជាសញ្ញាអាណាឡូក band pass ។

៣.៣.១ ការបំប្លែងឌីជីថលទៅអាណាឡូក

នៅពេលដែលទិន្នន័យពីកុំព្យូទ័រមួយត្រូវបានបញ្ជូនទៅមួយផ្សេងទៀតតាមរយៈក្រុមហ៊ុនបញ្ជូន អាណាឡូកមួយចំនួនវាត្រូវបានបំប្លែងជាសញ្ញាអាណាឡូកជាមុនសិន។ សញ្ញាអាណាឡូកត្រូវបានកែប្រែដើម្បីឆ្លុះបញ្ចាំងពីទិន្នន័យឌីជីថល សញ្ញាអាណាឡូកត្រូវបានកំណត់លក្ខណៈដោយទំហំប្រេកង់ និងដំណាក់កាលរបស់វា។ ការបំប្លែងពីឌីជីថលទៅអាណាឡូកមានបីប្រភេទ៖

❖ អំព្លីទីត

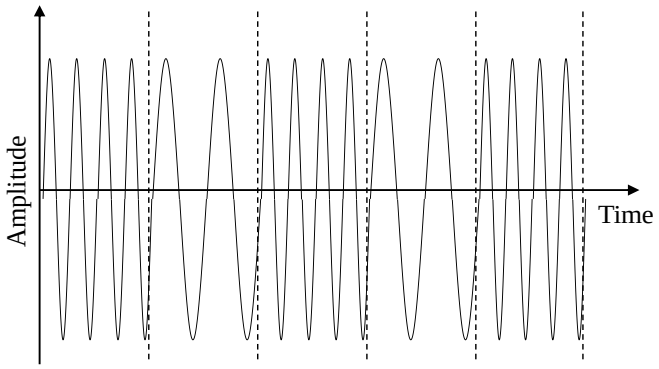


រូបភាពទី ៣.១១ អំព្លីទីត

នៅក្នុងបច្ចេកទេសបំប្លែងនេះទំហំនៃសញ្ញាបញ្ជូន នៃអាណាឡូកត្រូវបានកែប្រែដើម្បីឆ្លុះបញ្ចាំងពីទិន្នន័យគោលពីរ។ នៅពេលដែលទិន្នន័យគោលពីរតំណាងឱ្យខ្ទង់ទី ១ អំព្លីទីតត្រូវបានធ្វើឡើងបើមិនដូច្នេះទេ វាត្រូវបានកំណត់ទៅ ០ ហើយទាំងប្រេកង់ និងដំណាក់កាលនៅតែដដែលដូចនៅក្នុងសញ្ញាក្រុមហ៊ុនបញ្ជូនដើម។

❖ ប្រេកង់

នៅក្នុងបច្ចេកទេសបំប្លែងនេះ ប្រេកង់នៃសញ្ញាក្រុមហ៊ុនបញ្ជូនអាណាឡូកត្រូវបានកែប្រែដើម្បីឆ្លុះបញ្ចាំងទិន្នន័យគោលពីរ។

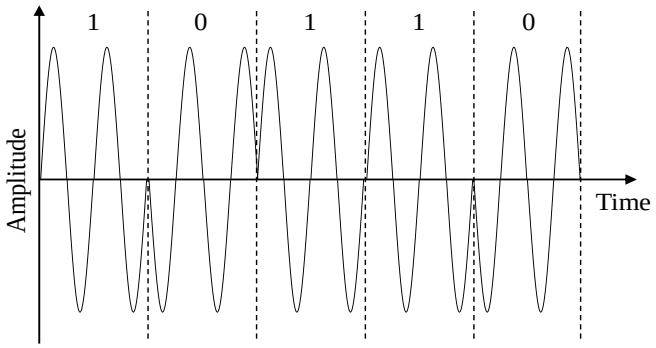


រូបភាពទី ៣.១២ ប្រេកង់

❖ តំណាក់កាល

នៅក្នុងគ្រោងការណ៍ការបំលែងនេះដំណាក់កាលនៃសញ្ញាក្រុមហ៊ុនដឹកជញ្ជូនដើមត្រូវបានផ្លាស់ប្តូរដើម្បីឆ្លុះបញ្ចាំងពីទិន្នន័យគោលពីរ។ ដំណាក់កាលនៃសញ្ញាត្រូវបានផ្លាស់ប្តូរនៅពេលដែល

និមិត្តសញ្ញាគោលពីរថ្មីត្រូវបានជួបប្រទះ ហើយ ទំហំ និងភាពញឹកញាប់នៃសញ្ញាក្រុមហ៊ុនដឹកជញ្ជូនដើមត្រូវបានរក្សាទុកនៅដដែល។



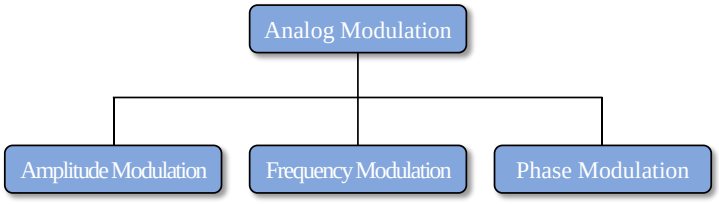
រូបភាពទី ៣.១៣ តំណាក់កាល

❖ ដំណាក់កាល quadrature

QPSK ផ្លាស់ប្តូរដំណាក់កាលដើម្បីឆ្លុះបញ្ចាំងពីលេខគោលពីរក្នុងពេលតែមួយនេះត្រូវបានធ្វើនៅក្នុងដំណាក់កាលពីរផ្សេងគ្នា។ ចរន្តសំខាន់នៃទិន្នន័យគោលពីរត្រូវបានបែងចែកស្មើៗគ្នាទៅជាអនុស្ទ្រីមពីរហើយព័ត៌មានសៀរៀលត្រូវបានបំប្លែងទៅជាប៉ារ៉ាឡែលនៅក្នុងស្ទ្រីមរងទាំងពីរ ហើយបន្ទាប់មកស្ទ្រីមនីមួយៗត្រូវបានបំប្លែងទៅជាសញ្ញាឌីជីថលដោយប្រើបច្ចេកទេស NRZ ក្រោយមកទៀតសញ្ញាឌីជីថលទាំងពីរត្រូវបានបញ្ចូលគ្នា។

៣.៣.២ ការបំលែងអាណាឡូកទៅអាណាឡូក

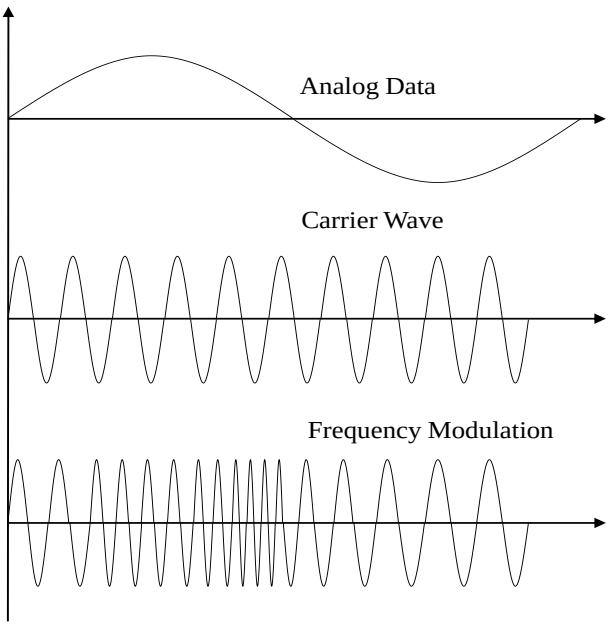
សញ្ញាអាណាឡូកត្រូវបានកែប្រែដើម្បីតំណាងឱ្យទិន្នន័យអាណាឡូកការបំលែងនេះត្រូវបានគេស្គាល់ផងដែរថាជាម៉ូឌុលអាណាឡូក។ ម៉ូឌុលអាណាឡូកត្រូវបានទាមទារនៅពេលដែល band pass ត្រូវបានប្រើ ការបំប្លែងអាណាឡូកទៅអាណាឡូកអាចធ្វើបានតាមបីវិធី៖



រូបភាព ៣.១៤ ប្រភេទនៃម៉ូឌុលអាណាឡូក

❖ ម៉ូឌុលអំប្លីទីត

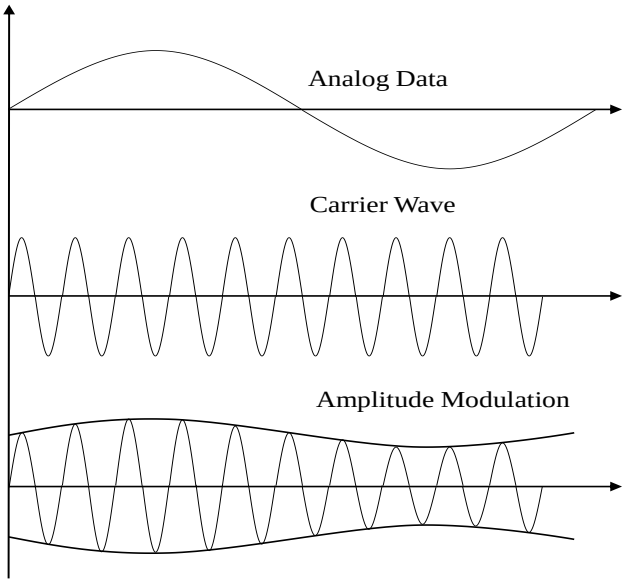
នៅក្នុងម៉ូឌុលនេះ ទំហំនៃសញ្ញាក្រុមហ៊ុនដឹកជញ្ជូនត្រូវបានកែប្រែដើម្បីឆ្លុះបញ្ចាំងពីទិន្នន័យអាណាឡូក ម៉ូឌុលអំប្លីទីតត្រូវបានអនុវត្តដោយប្រើមេគុណ។ ទំហំនៃសញ្ញាម៉ូឌុល បានគុណនឹងទំហំនៃប្រេកង់ក្រុមហ៊ុនបញ្ជូន ដែលបន្ទាប់មកឆ្លុះបញ្ចាំងពីទិន្នន័យអាណាឡូក ប្រេកង់ និងដំណាក់កាលនៃសញ្ញាក្រុមហ៊ុនបញ្ជូននៅតែមិនផ្លាស់ប្តូរ។



រូបភាព ៣.១៥ ម៉ូឌុលអំប្លីទីត

❖ ម៉ូឌុលប្រេកង់

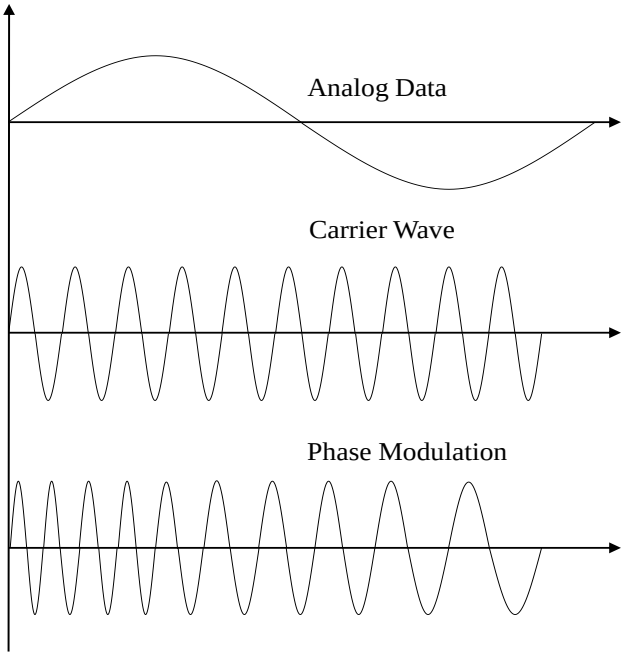
នៅក្នុងបច្ចេកទេសម៉ូឌុលនេះ ប្រេកង់សញ្ញាក្រុមហ៊ុនបញ្ជូនត្រូវបានកែប្រែដើម្បីឆ្លុះបញ្ចាំងពីការផ្លាស់ប្តូរកម្រិតវ៉ុលនៃសញ្ញាម៉ូឌុល (ទិន្នន័យអាណាឡូក)។ ទំហំ និងដំណាក់កាលនៃសញ្ញាក្រុមហ៊ុនដឹកជញ្ជូនមិនត្រូវបានផ្លាស់ប្តូរទេ។



រូបភាព ៣.១៦ ម៉ូឌុលប្រែកង់

❖ ម៉ូឌុលដំណាក់កាល

នៅក្នុងបច្ចេកទេសម៉ូឌុល ដំណាក់កាលនៃសញ្ញាក្រុមហ៊ុនដឹកជញ្ជូនត្រូវបានកែប្រែដើម្បីឆ្លុះបញ្ចាំងពីការផ្លាស់ប្តូរវ៉ុល (អំពីទីត) នៃសញ្ញាទិន្នន័យអាណាឡូក។



រូបភាព ៣.១៧ ម៉ូឌុលដំណាក់កាល

ម៉ូឌុលដំណាក់កាលគឺស្រដៀងគ្នាទៅនឹងម៉ូឌុលប្រេកង់ ប៉ុន្តែនៅក្នុងម៉ូឌុលដំណាក់កាល ភាពញឹកញាប់នៃសញ្ញាក្រុមហ៊ុនបញ្ជូនមិនត្រូវបានកើនឡើងទេ។ ភាពញឹកញាប់នៃពាក្យសម្ងាត់របស់ក្រុមហ៊ុនដឹកជញ្ជូនត្រូវបានផ្លាស់ប្តូរ (ធ្វើឱ្យក្រាស់ និងតូច) ដើម្បីឆ្លុះបញ្ចាំងពីការផ្លាស់ប្តូរវ៉ុលនៅក្នុងអំព្លីទីតសញ្ញាម៉ូឌុល។

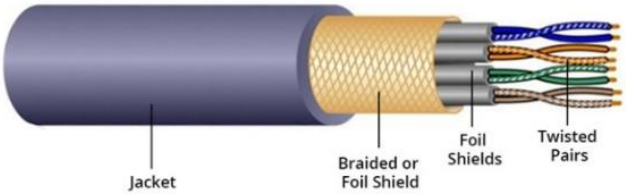
៣.៤ ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូន

ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូន គឺជាប្រព័ន្ធផ្សព្វផ្សាយរូបវន្ត ដែលបណ្តាញកុំព្យូទ័រទំនាក់ទំនង។

- ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូនគឺជាបណ្តាញទំនាក់ទំនងដែលបញ្ជូនព័ត៌មានពីអ្នកផ្ញើទៅអ្នកទទួល ហើយទិន្នន័យត្រូវបានបញ្ជូនតាមរយៈសញ្ញាអេឡិចត្រូម៉ាញ៉េទិច។
- មុខងារចម្បងរបស់ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូនគឺដើម្បីបញ្ជូនព័ត៌មានក្នុងទម្រង់ជាប៊ីតតាមរយៈបណ្តាញមូលដ្ឋាន (បណ្តាញតំបន់)។
- វាគឺជាផ្លូវរូបវន្តរវាងអ្នកបញ្ជូន និងអ្នកទទួលក្នុងការទំនាក់ទំនងទិន្នន័យ។
- នៅក្នុងបណ្តាញដែលមានមូលដ្ឋានលើទង់ដែង ប៊ីតមានទម្រង់ជាសញ្ញាអគ្គិសនី។
- នៅក្នុងបណ្តាញដែលមានជាសរសៃ ប៊ីតគឺស្ថិតនៅក្នុងទម្រង់នៃជីពចរពន្លឺ។
- នៅក្នុងដំណាក់កាល OSI ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូនគាំទ្រស្រទាប់ទី១ ដូច្នេះវាត្រូវបានចាត់ទុកថាជាធាតុផ្សំនៃស្រទាប់ទី១ ។
- សញ្ញាអគ្គិសនីអាចត្រូវបានបញ្ជូនតាមរយៈខ្សែស្ពាន់ ខ្សែកាបអុបទិក បរិយាកាស ទឹក និងសុញ្ញាកាស។
- លក្ខណៈពិសេសនៃឧបករណ៍ផ្ទុក និងសញ្ញាកំណត់លក្ខណៈ និងគុណភាពនៃការបញ្ជូនទិន្នន័យ។
- មេឌៀបញ្ជូនមានពីរប្រភេទ៖ ប្រព័ន្ធផ្សព្វផ្សាយមានខ្សែ និងប្រព័ន្ធផ្សព្វផ្សាយឥតខ្សែ នៅក្នុងប្រព័ន្ធផ្សព្វផ្សាយតាមខ្សែ លក្ខណៈមធ្យមគឺសំខាន់ជាង ចំណែកលក្ខណៈសញ្ញាមានសារៈសំខាន់ជាងនៅក្នុងប្រព័ន្ធផ្សព្វផ្សាយឥតខ្សែ។
- មេឌៀបញ្ជូនផ្សេងគ្នាមានលក្ខណៈសម្បត្តិផ្សេងទៀតដូចជា កម្រិតបញ្ជូន ការពន្យារពេល ការចំណាយ និងភាពងាយស្រួលនៃការដំឡើង និងការថែទាំ។
- ប្រព័ន្ធផ្សព្វផ្សាយបញ្ជូនមាននៅក្នុងស្រទាប់ទាបបំផុតនៃគំរូយោង OSI

៣.៤.១ ខ្សែ Twisted Pair

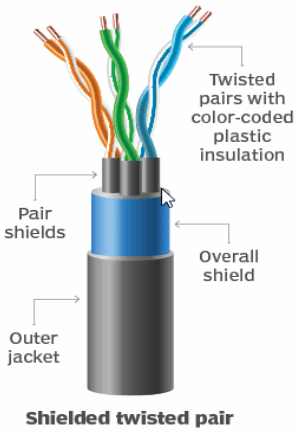
ខ្សែគូរមួលមានខ្សែស្ពាន់ដែលស្រោបដោយប្លាស្ទិកពីរដែលបត់ចូលគ្នាដើម្បីបង្កើតជាមេខ្សែតែមួយ។ មានតែខ្សែមួយប៉ុណ្ណោះដែលផ្ទុកសញ្ញាពិតប្រាកដចេញពីខ្សែទាំងពីរនេះ ហើយមួយទៀតត្រូវបានប្រើសម្រាប់ការយោងដី ការបង្វិលរវាងខ្សែភ្លើងជួយកាត់បន្ថយសំឡេងរំខាន (ការរំខាន អេឡិចត្រូម៉ាញ៉េទិច) និងការនិយាយឆ្លង ហើយខ្សែ twisted pair មានពីរប្រភេទគឺ៖



រូបភាព ៣.១៨ ខ្សែ Twisted Pair

ក. Shielded Twisted Pair (STP)

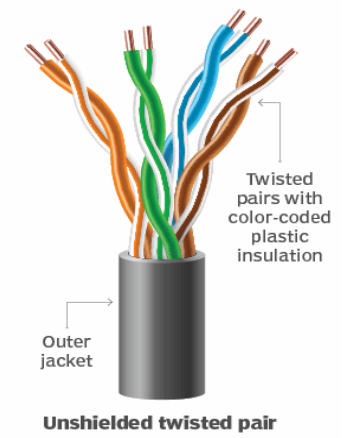
Shielded twisted pair (STP) គឺជាខ្សែទូរសព្ទស្ពាន់តែមួយគត់ និងបណ្តាញក្នុងតំបន់ (LAN) ដែលប្រើក្នុងការដំឡើងអាជីវកម្មមួយចំនួន វាបន្ថែមគម្របខាងក្រៅ ឬការពារមុខងារទាំងនោះជាដីទៅនឹងខ្សែភ្លើងគូរមួលស្តង់ដារ។ twisted pair គឺជាខ្សែស្ពាន់ស្តង់ដារដែលភ្ជាប់បណ្តាញកុំព្យូទ័រជាច្រើនទៅកាន់ក្រុមហ៊ុនទូរសព្ទ ដើម្បីកាត់បន្ថយការនិយាយឆ្លងគ្នា ឬការបញ្ចូលអេឡិចត្រូម៉ាញ៉េទិចរវាងខ្សែភ្លើង ខ្សែស្ពាន់ដែលមានអ៊ីសូឡង់ពីរត្រូវបានបង្វិលជុំវិញគ្នាទៅវិញទៅមក។ សញ្ញានីមួយៗនៅលើគូរមួលត្រូវការខ្សែទាំងពីរ មិនដូចគូរមួលដែលមិនមានការការពារ (UTP) ទេគូរមួលដែលមានប្រឡោះក៏រុំព័ទ្ធខ្សែទាំងនេះនៅក្នុងខែល ហើយធ្វើមូលដ្ឋានីយកម្មពួកវាដើម្បីកាត់បន្ថយការជ្រៀតជ្រែកអេឡិចត្រូម៉ាញ៉េទិច និងប្រែកង់វិទ្យុបន្ថែមទៀត។ ខ្សែ STP មានតម្លៃថ្លៃជាង និងពិបាកដំឡើងជាងខ្សែ UTP ។



រូបភាព ៣.១៩ ខ្សែ Shielded Twisted Pair (STP)

២. Unshielded Twisted Pair (UTP)

ខ្សែ Unshielded twisted pair (UTP) ត្រូវបានគេប្រើយ៉ាងទូលំទូលាយនៅក្នុងឧស្សាហកម្មកុំព្យូទ័រ និងទូរគមនាគមន៍ ដូចជាខ្សែ Ethernet និងខ្សែទូរសព្ទ។ នៅក្នុងខ្សែ UTP, conductors ដែលបង្កើតជាសៀគ្វីតែមួយត្រូវបានបង្វិលជុំវិញគ្នាទៅវិញទៅមកដើម្បីលុបចោលការជ្រៀតជ្រែកអេឡិចត្រូម៉ាញ៉េទិច (EMI) ពីប្រភពខាងក្រៅ។ Unshielded មានន័យថាមិនមានការការពារបន្ថែមដូចជាសំណាញ់ឬសន្លឹកអាលុយមីញ៉ូម (ដែលបន្ថែមជាដុំ) ត្រូវបានប្រើ។ ខ្សែ UTP ជារឿយៗជាក្រុមនៃគូរមួយដែលត្រូវបានដាក់ជាក្រុមជាមួយនឹងអ៊ីសូឡង់ដែលមានកូដពណ៌ ដែលចំនួននេះអាស្រ័យលើគោលបំណង។



រូបភាព ៣.២០ ខ្សែ Unshielded Twisted Pair (UTP)

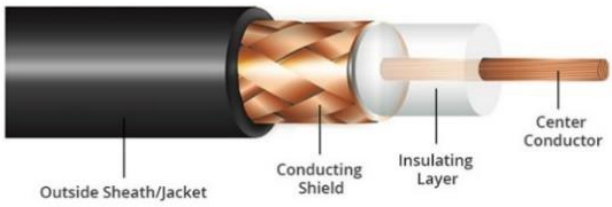
តើអ្វីជាភាពខុសគ្នារវាង STP, FTP និង S/FTP និង UTP? សូមក្រឡេកមើលភាពខុសប្លែកគ្នារវាងខ្សែគូរមួលដែលការពារ និងជម្រើសគូរមួលមួយចំនួន៖

STP CATEGORY	PURPOSE	BANDWIDTH	DATA TRANSFER RATE
Cat1	Voice only	N/A	N/A
Cat2	Data	4 MHz	4 Mbps
Cat3	Data	16 MHz	10 Mbps
Cat4	Data	20 MHz	16 Mbps
Cat5	Data	100 MHz	100 Mbps
Cat5e	Data	100 MHz	1 Gbps
Cat6	Data	250 MHz	Up to 10 Gbps
Cat6a	Data	500 MHz	Up to 10 Gbps
Cat7	Data	600 MHz	Up to 10 Gbps
Cat7a	Data	1 GHz(1000 MHz)	Between 40 and 100 Gbps
Cat8	Data	2 GHz(2000 MHz)	Between 25 and 40 Gbps

- **STP** ខ្សែក្រវាត់គូរមួលដែលមានស្រទាប់ការពារដើរតួនាទីជាខែលការពារដោយគ្របដណ្តប់ខ្សែចំនួនបួនគូនៃខ្សែដែលផ្ទុកសញ្ញាដើម្បីកាត់បន្ថយការជ្រៀតជ្រែកអេឡិចត្រូម៉ាញ៉េទិច។ មានខ្សែ STP ជាច្រើនដូចជាខ្សែ foil twisted pair (FTP) និង shielded foil twisted pair (S/FTP) ។
- **FTP** វាក៏មានខ្សែ STP ដែលប្រើស្រទាប់ការពារ foil ស្រាលជាងមុនផងដែរទោះជាយ៉ាងណាក៏ដោយ សូមចំណាំថាកាំពត់ និងភាពតានតឹងទាញត្រូវតែត្រួតពិនិត្យកំលុងពេលដំឡើង ដើម្បីការពារខ្សែការពារទាំងនេះពីការរហែក។
- **S/FTP** ដើម្បីជៀសវាងលទ្ធភាពនៃការរហែក ប្រព័ន្ធខ្សែ STP ប្រើប្រឡោះក្រាស់ដើម្បីធ្វើឱ្យខ្សែកាន់តែរឹងមាំ។ សំខាន់ ខ្សែភ្លើងរបស់ខ្សែត្រូវបានរមួល និងការពារ ដើម្បីផ្តល់នូវការការពារដ៏ល្អបំផុតប្រឆាំងនឹងការនិយាយឆ្លង និងការជ្រៀតជ្រែកអេឡិចត្រូម៉ាញេទិក។
- **UTP** ប្រភេទខ្សែភ្លើងធម្មតាជាងដែលបានដំឡើងនៅក្នុងផ្ទះគឺ គូរមួលដែលមិនមានការការពារមិនដូច STP, FTP, និង S/FTP ខ្សែ UTP មិនមានរបាំងការពាររាងកាយដើម្បីទប់ស្កាត់ការជ្រៀតជ្រែកឡើយ។ ផ្ទុយទៅវិញ UTP ពឹងផ្អែកលើតម្រងប្រព័ន្ធផ្សព្វផ្សាយ និងតម្លៃដែលជាសំណង់ពី “តុល្យភាពទៅគ្មានតុល្យភាព” ជាយន្តការតុល្យភាព និងតម្រង។

៣.៤.២ ខ្សែ Coaxial

ខ្សែ coaxial មានខ្សែពីរនៃទង់ដែង ខ្សែស្នូលស្ថិតនៅចំកណ្តាល ហើយធ្វើពីចំហាយរឹង។ ស្នូលត្រូវបានរុំព័ទ្ធដោយស្រទាប់អ៊ីសូឡង់ ខ្សែទីពីរត្រូវបានរុំជុំវិញស្រោម ហើយនៅក្នុងវេនត្រូវបានរុំដោយស្រទាប់អ៊ីសូឡង់ ហើយទាំងអស់នេះត្រូវបានគ្របដណ្តប់ដោយគម្របផ្លាស្ទិច។



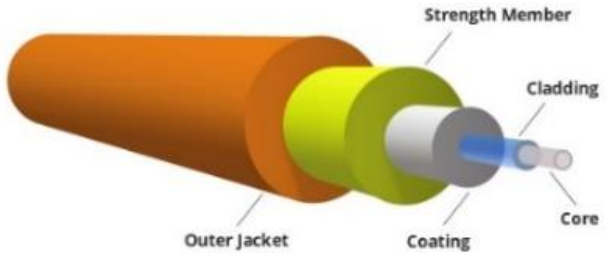
រូបភាព ៣.២១ ខ្សែ Coaxial Cable

ដោយសារតែរចនាសម្ព័ន្ធរបស់វា ខ្សែ coaxial មានសមត្ថភាពផ្ទុកសញ្ញាប្រេកង់ខ្ពស់ជាងខ្សែ twisted pair ការរចនារុំផ្តល់ឱ្យវានូវខែលដ៏ល្អប្រឆាំងនឹងសំឡេងរំខាន និងការនិយាយឆ្លងគ្នា។ ខ្សែ coaxial ផ្តល់អត្រាបញ្ជូនខ្ពស់រហូតដល់ 450 Mbps ។ ខ្សែកាប coaxial មានបីប្រភេទគឺ RG-59 (Cable TV), RG-58 (Thin Ethernet) និង RG-11 (Thick Ethernet)។ RG តំណាងឱ្យវិទ្យុរដ្ឋាភិ

បាល ខ្សែត្រូវបានភ្ជាប់ដោយប្រើឧបករណ៍ភ្ជាប់ BNC និង BNC-T ។ ឧបករណ៍បញ្ចប់ BNC ត្រូវបានប្រើដើម្បីបញ្ចប់ខ្សែភ្លើងនៅចុងឆ្ងាយ។

៣.៤.៣ ខ្សែកាបអុបទិក

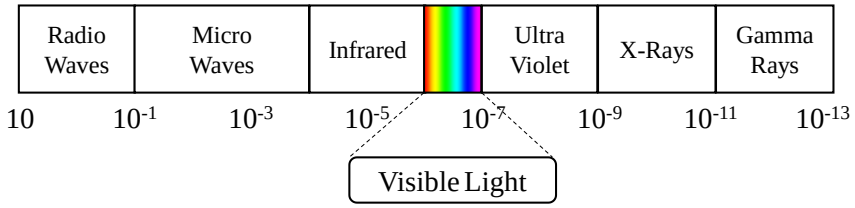
ខ្សែកាបអុបទិកធ្វើការលើលក្ខណៈសម្បត្តិនៃពន្លឺនៅពេលដែលកាំរស្មីពន្លឺប៉ះមុំសំខាន់ វានឹងឆ្លុះនៅមុំ ៩០ ដឺក្រេ។ ទ្រព្យសម្បត្តិនេះត្រូវបានប្រើប្រាស់ក្នុងខ្សែកាបអុបទិក ស្នូលនៃខ្សែកាបអុបទិកត្រូវបានផលិតពីកញ្ចក់ឬប្លាស្ទិកដែលមានគុណភាពខ្ពស់។ ពីចុងម្ខាងរបស់វា ពន្លឺត្រូវបានបញ្ចេញ វាធ្វើដំណើរឆ្លងកាត់វា ហើយនៅចុងម្ខាងទៀត ឧបករណ៍ចាប់ពន្លឺ រកឃើញស្ទ្រីមពណ៌មាស ហើយបំប្លែងវាទៅជាទិន្នន័យអគ្គិសនី។ខ្សែកាបអុបទិកផ្តល់នូវរបៀបខ្ពស់បំផុតនៃល្បឿន។ វាមកជាពីររបៀប មួយគឺ single-mode fiber ហើយទីពីរគឺ multimode fiber។ ជាសរសៃបៀបតែមួយអាចផ្ទុកកាំរស្មីតែមួយ ចំណែកពហុម៉ូដអាចផ្ទុកពន្លឺបានច្រើន។ខ្សែកាបអុបទិកក៏មកក្នុងសមត្ថភាព unidirectional និង bidirectional ។ ដើម្បីភ្ជាប់ និងចូលប្រើខ្សែកាបអុបទិក ប្រភេទឧបករណ៍ភ្ជាប់ជាក់លាក់ត្រូវបានប្រើប្រាស់នានែលអតិថិជន (SC), គន្លឹះត្រង់ (ST) ឬ MT-RJ ។



រូបភាព ៣.២២ ខ្សែកាបអុបទិក

៣.៥ ការបញ្ជូនឥតខ្សែ

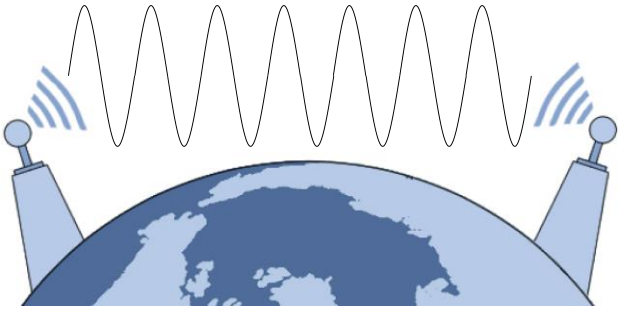
ការបញ្ជូនឥតខ្សែ គឺជាទម្រង់នៃប្រព័ន្ធផ្សព្វផ្សាយដែលមិនមានការណែនាំអំពី ការប្រាស្រ័យទាក់ទងឥតខ្សែពាក់ព័ន្ធនឹងការមិនភ្ជាប់ទំនាក់ទំនងរវាងឧបករណ៍ពីរឬច្រើនដែលទំនាក់ទំនងឥតខ្សែ។ សញ្ញាឥតខ្សែត្រូវបានរីករាលដាលនៅលើអាកាស ហើយត្រូវបានទទួល និងបកស្រាយដោយអង់តែនសមស្រប។ នៅពេលដែលអង់តែនត្រូវបានភ្ជាប់ទៅសៀគ្វីអគ្គិសនីរបស់កុំព្យូទ័រ ឬឧបករណ៍ឥតខ្សែ វាបំលែងទិន្នន័យឌីជីថលទៅជាសញ្ញាឥតខ្សែ វារីករាលដាលពាសពេញក្នុងជួរប្រេកង់របស់វា អ្នកទទួលនៅផ្នែកម្ខាងទៀតទទួលសញ្ញាទាំងនេះ ហើយបំប្លែងពួកវាត្រឡប់ទៅជាទិន្នន័យឌីជីថលវិញ ផ្នែកតូចមួយនៃវិសាលគមអេឡិចត្រូម៉ាញ៉េទិចអាចត្រូវបានប្រើសម្រាប់ការបញ្ជូនឥតខ្សែ។



រូបភាពទី ២.២៣ ការបញ្ជូនឥតខ្សែ

៣.៥.១ ការបញ្ជូនវិទ្យុ

ប្រេកង់វិទ្យុមានភាពងាយស្រួលក្នុងការបង្កើត ហើយដោយសារតែរលកធំរបស់វា វាអាចជ្រាបចូលតាមជញ្ជាំង និងរចនាសម្ព័ន្ធនានា។ រលកវិទ្យុអាចមានប្រវែងរលកចាប់ពី ១ ម.ម ទៅ ១០០.០០០ គីឡូម៉ែត្រ និងមានប្រេកង់ចាប់ពី ៣ ហឺត (ប្រេកង់ទាបខ្លាំង) ដល់ ៣០០ GHz (ប្រេកង់ខ្ពស់ខ្លាំង)។ ប្រេកង់វិទ្យុត្រូវបានបែងចែកជាជ្រាំមួយក្រុម រលកវិទ្យុនៅប្រេកង់ទាបអាចធ្វើដំណើរតាមជញ្ជាំង ចំណែកឯ RF ខ្ពស់អាចធ្វើដំណើរក្នុងបន្ទាត់ត្រង់ និងត្រឡប់មកវិញ។ ថាមពលនៃរលកប្រេកង់ទាបថយចុះយ៉ាងខ្លាំង នៅពេលដែលវាគ្របដណ្តប់ចម្ងាយឆ្ងាយ រលកវិទ្យុដែលមានប្រេកង់ខ្ពស់មានថាមពលកាន់តែច្រើន ប្រេកង់ទាបដូចជា VLF, LF, និង MF bands អាចធ្វើដំណើរលើដីរហូតដល់ ១០០០ គីឡូម៉ែត្រពីលើផ្ទៃផែនដី។ រលកវិទ្យុនៃប្រេកង់ខ្ពស់ងាយនឹងត្រូវបានស្រូបដោយភ្លៀង និងឧបសគ្គផ្សេងទៀត ពួកគេប្រើ Ionosphere នៃបរិយាកាសផែនដី។ រលកវិទ្យុដែលមានប្រេកង់ខ្ពស់ដូចជា HF និង VHF ត្រូវបានរីករាលដាលឡើងលើ នៅពេលដែលពួកគេទៅដល់ Ionosphere ពួកវានឹងត្រឡប់មកផែនដីវិញ។



រូបភាពទី ៣.២៤ វិទ្យុបញ្ជូនផែនដី

៣.៥.២ ការបញ្ជូនមីក្រូវ៉ែវ

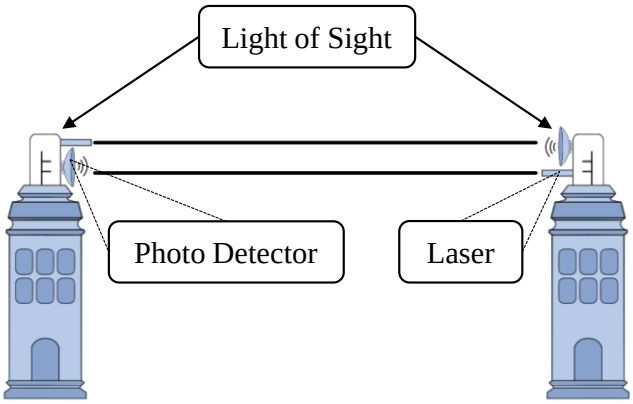
រលកអេឡិចត្រូម៉ាញ៉េទិចលើសពី ១00 MHz មានទំនោរធ្វើដំណើរក្នុងបន្ទាត់ត្រង់មួយ ហើយសញ្ញានៅលើពួកវាអាចត្រូវបានបញ្ជូនដោយការបញ្ជូនរលកទាំងនោះទៅកាន់ស្ថានីយជាក់លាក់មួយ។ ដោយសារតែមីក្រូវ៉ែវធ្វើដំណើរក្នុងបន្ទាត់ត្រង់ ទាំងអ្នកផ្ញើ និងអ្នកទទួលត្រូវតែតម្រឹមយ៉ាងតឹងរ៉ឹងនៅក្នុងបន្ទាត់នៃការមើលឃើញ។ មីក្រូវ៉ែវអាចមានប្រវែងរលកចាប់ពី ១ មីលីម៉ែត្រ ទៅ ១ ម៉ែត្រ និងប្រេកង់ចាប់ពី ៣00 MHz ដល់ ៣00 GHz ។

រូបភាពទី ៣.២៥ ការបញ្ជូនមីក្រូវ៉ែវ

អង់តែនមីក្រូវ៉ែវប្រមូលផ្តុំរលកបង្កើតជាធ្នឹមរបស់ពួកគេ ដូចដែលបានបង្ហាញក្នុងរូបភាពខាងលើ អង់តែនជាច្រើនអាចត្រូវបានតម្រឹមដើម្បីទៅដល់ឆ្ងាយ។ មីក្រូវ៉ែវមានប្រេកង់ខ្ពស់ជាង និងមិនជ្រាបចូលទៅក្នុងឧបសគ្គដូចជញ្ជាំង ការបញ្ជូនមីក្រូវ៉ែវអាស្រ័យយ៉ាងខ្លាំងទៅលើលក្ខខណ្ឌអាកាសធាតុ និងប្រេកង់ដែលវាត្រូវបានប្រើប្រាស់។

៣.៥.៣ ការបញ្ជូនពន្លឺ

វិសាលគមអេឡិចត្រូម៉ាញ៉េទិចខ្ពស់បំផុតដែលអាចត្រូវបានប្រើសម្រាប់ការបញ្ជូនទិន្នន័យគឺ ពន្លឺ ឬសញ្ញាអុបទិកនេះត្រូវបានសម្រេចដោយប្រើឡាស៊ែរ។ ដោយសារតែភាពញឹកញាប់នៃពន្លឺដែលបានប្រើវាមានទំនោរធ្វើដំណើរយ៉ាងតឹងរ៉ឹងក្នុងបន្ទាត់ត្រង់ ដូច្នេះ អ្នកផ្ញើ និងអ្នកទទួលត្រូវតែស្ថិតនៅក្នុងបន្ទាត់នៃការមើលឃើញ ពីព្រោះការបញ្ជូនឡាស៊ែរមានទិសដៅតែមួយ។ នៅចុងទាំងពីរនៃការទំនាក់ទំនង ឡាស៊ែរ និងឧបករណ៍ចាប់រូបភាពចាំបាច់ត្រូវដំឡើង។ ធ្នឹមឡាស៊ែរជាទូទៅមានទទឹង ១មីលីម៉ែត្រ ដូច្នេះវាគឺជាការងារនៃភាពជាក់លាក់មួយដើម្បីតម្រឹមអ្នកទទួលពីរឆ្ងាយ ដែលនីមួយៗចង្អុលទៅប្រភពនៃឡាស៊ែរ។ ហើយអង់តែនមីក្រូវ៉ែវប្រមូលផ្តុំរលកបង្កើតជាធ្នឹមរបស់ពួកគេ ដូចដែលបានបង្ហាញក្នុងរូបភាពខាងលើ អង់តែនជាច្រើនអាចត្រូវបានតម្រឹមដើម្បីទៅដល់ឆ្ងាយ។ មីក្រូវ៉ែវមានប្រេកង់ខ្ពស់ជាងនិងមិនជ្រាបចូលទៅក្នុងឧបសគ្គដូចជញ្ជាំងការបញ្ជូនមីក្រូវ៉ែវអាស្រ័យយ៉ាងខ្លាំងទៅលើលក្ខខណ្ឌអាកាសធាតុ និងប្រេកង់ដែលវាត្រូវបានប្រើប្រាស់។



រូបភាពទី ៣.២៦ ការបញ្ជូនពន្លឺ

ឡាសែរដំណើរការជា Tx (ឧបករណ៍បញ្ជូន) ហើយឧបករណ៍ចាប់រូបភាពដំណើរការជា Rx (អ្នកទទួល) ។ ឡាសែរមិនអាចជ្រាបចូលទៅក្នុងឧបសគ្គដូចជាជញ្ជាំង ភ្លៀង ឬអ័ព្ទក្រាស់ លើសពីនេះទៀតកាំរស្មីឡាសែរត្រូវបានបង្ខូចទ្រង់ទ្រាយដោយខ្យល់ សីតុណ្ហភាពបរិយាកាស ឬការប្រែប្រួលនៃសីតុណ្ហភាពនៅក្នុងផ្លូវ។ ឡាសែរមានសុវត្ថិភាពសម្រាប់ការបញ្ជូនទិន្នន័យ ដោយសារវាពិបាកក្នុងការប៉ះឡាសែរធំទូលាយមួយមម ដោយមិនរំខានដល់បណ្តាញទំនាក់ទំនង។

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះ អ្នកបានសិក្សាអំពី៖

- **ខ្សែ Shielded twisted pair (STP)** គឺជាខ្សែទូរសព្ទស្ពាន់តែមួយគត់និងបណ្តាញក្នុងតំបន់ (LAN) ដែលប្រើក្នុងការដំឡើងអាជីវកម្មមួយចំនួនវាបន្ថែមគម្របខាងក្រៅ ឬការពារមុខងារទាំងនោះជាដីទៅនឹងខ្សែភ្លើងគូរមួលស្តង់ដារ។
- **ខ្សែ Unshielded twisted pair (UTP)** ត្រូវបានគេប្រើយ៉ាងទូលំទូលាយនៅក្នុងឧស្សាហកម្មកុំព្យូទ័រនិងទូរគមនាគមន៍ ដូចជាខ្សែ Ethernet និងខ្សែទូរសព្ទ។
- **ខ្សែ coaxial** មានខ្សែពីរនៃទង់ដែង ខ្សែស្នូលស្ថិតនៅចំកណ្តាល ហើយធ្វើពីចំហាយរឹង។ ស្នូលត្រូវបានរុំព័ទ្ធដោយស្រទាប់អ៊ីសូឡង់ ខ្សែទីពីរត្រូវបានរុំជុំវិញស្រោម ហើយនៅក្នុងវេនត្រូវបានរុំដោយស្រទាប់អ៊ីសូឡង់ ហើយទាំងអស់នេះត្រូវបានគ្របដណ្តប់ដោយគម្របផ្លាស្ទិច។
- **ខ្សែកាបអុបទិក**ធ្វើការលើលក្ខណៈសម្បត្តិនៃពន្លឺនៅពេលដែលកាំរស្មីពន្លឺប៉ះមុំសំខាន់ វានឹងឆ្លុះនៅមុំ ៩០ ដឺក្រេ។ទ្រព្យសម្បត្តិនេះត្រូវបានប្រើប្រាស់ក្នុងខ្សែកាបអុបទិក ស្នូលនៃខ្សែកាបអុបទិកត្រូវបានផលិតពីកញ្ចក់ឬប្លាស្ទិកដែលមានគុណភាពខ្ពស់។
- **សញ្ញាឌីជីថល សញ្ញាឌីជីថល៖** ទាំងនេះគឺដាច់ពីគ្នានៅក្នុងធម្មជាតិ និងតំណាងឱ្យលំដាប់នៃវ៉ុលជីពចរ សញ្ញាឌីជីថលត្រូវបានប្រើនៅក្នុងសៀគ្វីនៃប្រព័ន្ធកុំព្យូទ័រ។
- **សញ្ញាអាណាឡូក សញ្ញាអាណាឡូក៖** ទាំងនេះស្ថិតក្នុងទម្រង់រលកបន្តក្នុងធម្មជាតិ ហើយត្រូវបានតំណាងដោយរលកអេឡិចត្រូម៉ាញ៉េទិចថេរ។
- **ការបំប្លែងពី ឌីជីថល ទៅឌីជីថល៖** ផ្នែកនេះពន្យល់ពីរបៀបបំប្លែងទិន្នន័យឌីជីថលទៅជាសញ្ញាឌីជីថលវាអាចត្រូវបានធ្វើតាមពីរវិធី គឺការសរសេរកូដបន្ទាត់ និងការសរសេរកូដប្លុក សម្រាប់ទំនាក់ទំនងទាំងអស់ ការសរសេរកូដតាមបន្ទាត់គឺចាំបាច់ ចំណែកការសរសេរកូដប្លុកគឺស្រេចចិត្ត។
- **អាណាឡូកការបំប្លែង អាណាឡូក ទៅឌីជីថល៖** ទិន្នន័យគឺជាទិន្នន័យបន្តបន្ទាប់គ្នាក្នុងទម្រង់រលក ចំណែកទិន្នន័យឌីជីថលគឺដាច់ដោយឡែក។ យើងប្រើ Pulse Code Modulation (PCM) ដើម្បីបំប្លែងរលកអាណាឡូកទៅជាទិន្នន័យឌីជីថល។
- **ការបំប្លែងពី ឌីជីថលទៅ អាណាឡូក៖** សញ្ញាអាណាឡូកដែលកំណត់លក្ខណៈដោយទំហំ ប្រេកង់ និងដំណាក់កាលរបស់វា។

សំណួរ

១. តើការបញ្ជូនទិន្នន័យគឺជាអ្វី?

២. ចូរពន្យល់ពីសញ្ញាឌីជីថលទៅជាសញ្ញាអាណាឡូក។

៣. តើអ្វីជាភាពខុសគ្នារវាងការបញ្ជូនទិន្នន័យ និងការបញ្ជូនអាណាឡូក?

៤. តើអ្វីជាភាពខុសគ្នារវាង Polar Non-Return to Zero (Polar NRZ) និង Return to Zero (RZ)?

៥. ចូរពន្យល់ពីប្រព័ន្ធផ្សព្វផ្សាយដែលអ្នកបានដឹង។

៦. ចូរពន្យល់អំពីការបញ្ជូនឥតខ្សែ។

ការអនុវត្តន៍ទី៣

ការបង្កើតខ្សែ LAN ដើមឡើយប្រើជាខ្សែទូរស័ព្ទ ឬខ្សែបណ្តាញវា គឺជាខ្សែដែលប្រើក្នុងសម័យទំនើបដើម្បីបង្កើតបណ្តាញក្នុងតំបន់។ វាអាចត្រូវបានផលិតយ៉ាងងាយស្រួលដោយប្រើតែ RJ-45 ពីរ ខ្សែ និងឧបករណ៍ភ្ជាប់ កុងកាត់ ហៅថា ឧបករណ៍ LAN ។

ក.គោលបំណងនៃការអនុវត្តនេះ

- ដើម្បីស្វែងយល់អំពីគោលការណ៍នៃខ្សែ LAN
- ដើម្បីដឹងពីភាពខុសគ្នារវាងខ្សែ LAN
- ដើម្បីធ្វើខ្សែបណ្តាញ LAN

ខ. តើអ្វីទៅជាខ្សែ RJ45

ខ្សែ RJ45 ភ្ជាប់ ALL HMI និងស្ថានីយវិស្វករ តាមរយៈកុងតាក់ដើម្បីទំនាក់ទំនងគ្នាទៅវិញទៅមក វាត្រូវបានប្រើដើម្បីទាញយកការកែប្រែណាមួយ ហើយត្រូវបានធ្វើឡើងជាក្រាហ្វិកនៅក្នុងស្ថានីយវិស្វកម្ម ខ្សែ RJ45 ក៏ត្រូវបានប្រើសម្រាប់បង្ហាញម៉ាស៊ីនបោះពុម្ពជាមួយកុំព្យូទ័រផងដែរ។

១. ខ្សែអ៊ីសឺរណិត – ប្រភេទ 5e ឬ CAT5e ឬ CAT6

២.RJ-45 ឧបករណ៍ Crimping

៣.RJ45 Crimp អាច Connectors

ក.ឧបករណ៍សម្រាប់ធ្វើការកឹបខ្សែបណ្តាញ

ខ.សូមមើលវីដេអូអំពីរបៀបបង្កើតខ្សែ RJ45

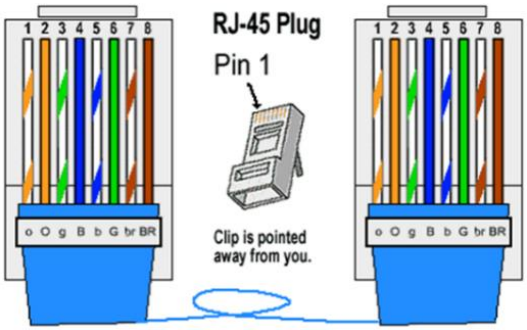
https://youtu.be/WvP0D0jiyLg

គ. របៀបធ្វើខ្សែ RJ45

សេចក្តីណែនាំ៖ មានខ្សែចំនួនបួនគូនៅក្នុងខ្សែអ៊ីសឺរណិត ហើយឧបករណ៍ភ្ជាប់អ៊ីសឺរណិត (8P8C) មានរន្ធដោតចំនួនប្រាំបី។ ម្ជុលនីមួយៗត្រូវបានកំណត់អត្តសញ្ញាណដោយលេខ ដោយចាប់ផ្តើមពីឆ្វេងទៅស្តាំ ដោយឃ្លីបបែរមុខអ្នក។

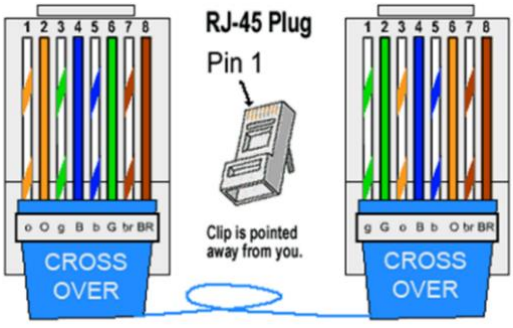
គ១. ការតឹបខ្សែស្រប

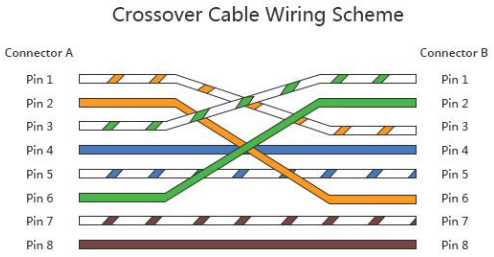
ខ្សែអ៊ីសឺរណិតគឺជាខ្សែស្តង់ដារដែលប្រើសម្រាប់គោលបំណងស្ទើរតែទាំងអស់ ហើយជារឿយៗត្រូវបានគេហៅថា “ខ្សែបំណះ”។ វាត្រូវបានផ្គាតយ៉ាងខ្លាំងឱ្យអ្នកស្ទួនលំដាប់ពណ៌នៅខាងឆ្វេង។ចំណាំពីរបៀបដែលគូពណ៌បែតងមិននៅម្ខាងដូចគូផ្សេងទៀតទាំងអស់ ការកំណត់រចនាសម្ព័ន្ធនេះអនុញ្ញាតឱ្យដំណើរការខ្សែបានយូរ។ ចំពោះការប្រើប្រាស់ការកិច្ចខ្សែស្របគឺប្រើប្រាស់សម្រាប់ឧបករណ៍ផ្សេងគ្នា។



គ២. ការតឹបខ្សែខ្វែង

គោលបំណងនៃខ្សែ Crossover Ethernet គឺដើម្បីភ្ជាប់កុំព្យូទ័រមួយដោយផ្ទាល់ទៅកុំព្យូទ័រផ្សេងទៀត (ឬឧបករណ៍) ដោយមិនចាំបាច់ឆ្លងកាត់រ៉ោតទ័រ កុងតាក់ ឬមជ្ឈមណ្ឌល។ ចំពោះការប្រើប្រាស់ការកិច្ចខ្សែស្របគឺប្រើប្រាស់សម្រាប់ឧបករណ៍ដូចគ្នា។





ឃ.សង្ខេប

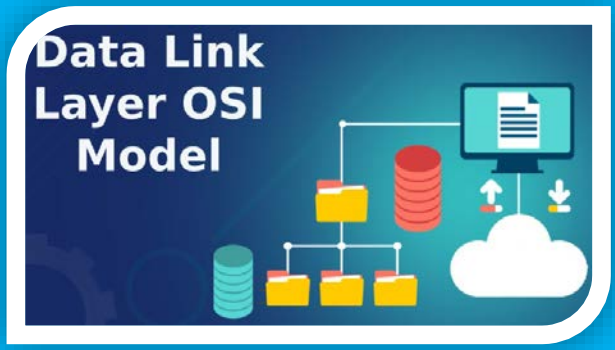
នៅក្នុងការអនុវត្តនេះខ្សែភ្ជាប់ដោយផ្ទាល់ត្រូវបានប្រើរវាងឧបករណ៍នៅក្នុងស្រទាប់ដូចគ្នានៅក្នុងស្រទាប់ OSI 7 (កាត LAN - កាត LAN) ។ ខ្សែឆ្លងកាត់ត្រូវបានប្រើរវាងឧបករណ៍នៅក្នុងស្រទាប់ដូចគ្នានៅក្នុងស្រទាប់ OSI ៧។

ង.កិច្ចការស្រាវជ្រាវ

១. ចូរប្រើប្រាស់ខ្សែ RJ45 កិបខ្សែជាប្រភេទស្រប។

២. ចូរប្រើប្រាស់ខ្សែ RJ45 កិបខ្សែជាប្រភេទខ្វែង។

៣. ការអនុវត្តអនុវត្តខ្សែបណ្តាញជាមួយ RJ45 ភ្ជាប់ជាមួួយឧបករណ៍ផ្សេងៗ។



ជំពូកទី៤

Data Link Layer

Data Link Layer គឺជាស្រទាប់ទីពីរនៃ OSI ម៉ូដែលស្រទាប់ ស្រទាប់នេះគឺជាស្រទាប់មួយក្នុងចំណោមស្រទាប់ច្រើនដែលស្មុគស្មាញបំផុត ហើយវាមានមុខងារស្មុគស្មាញ និងបំណុល។ Data Link Layer លាក់ព័ត៌មានលម្អិតនៃផ្នែករឹងមូលដ្ឋាន ហើយតំណាងឱ្យស្រទាប់ខាងលើជាឧបករណ៍ផ្ទុកសម្រាប់ទំនាក់ទំនង Data Link Layer មានការព្រួយបារម្ភជាមួយ នឹងការចែកចាយស៊ុមក្នុងស្រុករវាងថ្នាំងនៅលើកម្រិតបណ្តាញដូចគ្នា ស៊ុមតំណភ្ជាប់ទិន្នន័យ ដូចដែលឯកតាទិន្នន័យពិធីការទាំងនេះត្រូវបានហៅមិនត្រូវឆ្លងកាត់ព្រំដែននៃបណ្តាញក្នុងតំបន់នោះទេ ការកំណត់ផ្លូវអន្តរបណ្តាញ និងអាសយដ្ឋានសកលគឺជាមុខងារស្រទាប់ខ្ពស់ដែលអនុញ្ញាតឱ្យពិធីការភ្ជាប់ទិន្នន័យផ្តោតលើការចែកចាយ អាសយដ្ឋាន អាជ្ញាកណ្តាលប្រព័ន្ធផ្សព្វផ្សាយ។ វិធីនេះ ស្រទាប់តំណភ្ជាប់ទិន្នន័យ គឺស្រដៀងទៅនឹងប៉ូលីសចរាចរណ៍សង្កាត់។ ពិធីការភ្ជាប់ទិន្នន័យបញ្ជាក់ពីរបៀបដែលឧបករណ៍រកឃើញ និងសង្គ្រោះពីការប៉ះទង្គិចបែបនេះ ហើយអាចផ្តល់នូវយន្តការដើម្បីកាត់បន្ថយ ឬការពារពួកគេ។

ជំពូកទី៤ នេះ អ្នកនឹងរៀនអំពី៖

៤.១ ការណែនាំអំពី Data Link Layer

Data Link Layer ដំណើរការរវាងម៉ាស៊ីនពីរដែលត្រូវបានភ្ជាប់ដោយផ្ទាល់ ការភ្ជាប់ដោយផ្ទាល់នេះអាចជាចំណុចមួយទៅចំណុច ឬការចាក់ផ្សាយ។ ប្រព័ន្ធនៅលើបណ្តាញផ្សាយត្រូវបានគេនិយាយថាស្ថិតនៅលើតំណរដូចគ្នា។ ការងារនៃ Data Link Layer មាននិន្នាការកាន់តែស្មុគស្មាញនៅពេលដោះស្រាយជាមួយម៉ាស៊ីនច្រើននៅលើដែនតែមួយ Data Link Layer ទទួលខុសត្រូវក្នុងការបំប្លែងចរន្តទិន្នន័យទៅជាសញ្ញាបន្តិចម្តងៗ ហើយបញ្ជូនវាទៅផ្នែករឹងមូលដ្ឋាន នៅចុងបញ្ចប់នៃការទទួល Data Link Layer នឹងយកទិន្នន័យពីផ្នែករឹងនៅក្នុងសញ្ញាអគ្គិសនី ប្រមូលផ្តុំពួកវាជាទម្រង់ស៊ុមដែលអាចស្គាល់បាន ហើយប្រគល់វាទៅស្រទាប់ខាងលើ។ Data Link Layer មានស្រទាប់រងពីរ៖

- **ការត្រួតពិនិត្យតំណរភ្ជាប់ឡូជីខល៖** វាទាក់ទងនឹងពិធីការ ការគ្រប់គ្រងលំហូរ និងការគ្រប់គ្រងកំហុស
- **ការគ្រប់គ្រងការចូលប្រើប្រព័ន្ធផ្សព្វផ្សាយ៖** វាទាក់ទងនឹងការគ្រប់គ្រងជាក់ស្តែងនៃមេឌៀ

មុខងារនៃData Link Layer ធ្វើកិច្ចការជាច្រើនជំនួសឱ្យស្រទាប់ខាងលើហើយស្រទាប់ទាំងនេះមានដូចជា៖

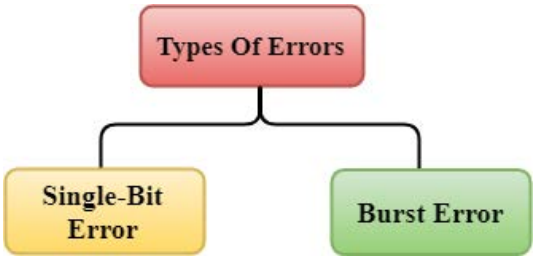
- **ការដាក់ស៊ុម៖** Data Link Layer យកកញ្ចប់ព័ត៌មានពីស្រទាប់បណ្តាញ ហើយបញ្ចូលពួកវាទៅក្នុងស៊ុមបន្ទាប់មកវាបញ្ជូនស៊ុមនីមួយៗទៅផ្នែករឹង។ នៅចុងបញ្ចប់របស់អ្នកទទួល Data Link Layer ចាប់យកសញ្ញាពីផ្នែករឹងហើយផ្តុំពួកវាទៅជាស៊ុម។
- **ការកំណត់អាសយដ្ឋាន៖** Data Link Layer ផ្តល់នូវយន្តការកំណត់អាសយដ្ឋានផ្នែករឹងរបស់ស្រទាប់ទី២ អាសយដ្ឋានផ្នែករឹងត្រូវបានសន្មត់ថាមានតែមួយគត់នៅលើតំណរ វាត្រូវបានអ៊ិនកូដទៅក្នុងផ្នែករឹងនៅពេលផលិត។
- **ការធ្វើសមកាលកម្ម៖** នៅពេលដែលស៊ុមទិន្នន័យត្រូវបានផ្ញើនៅលើតំណរ ម៉ាស៊ីនទាំងពីរត្រូវតែធ្វើសមកាលកម្មសម្រាប់ការផ្ទេរ។
- **ការគ្រប់គ្រងកំហុស៖** ពេលខ្លះសញ្ញាអាចជួបប្រទះបញ្ហាក្នុងការផ្លាស់ប្តូរ ហើយប៊ីតត្រូវបាន ត្រឡប់ កំហុសទាំងនេះត្រូវបានរកឃើញ និងព្យាយាមសង្គ្រោះទិន្នន័យពិតៗ វាក៏ផ្តល់នូវយន្តការរាយការណ៍កំហុសដល់អ្នកផ្ញើផងដែរ។
- **ការគ្រប់គ្រងលំហូរ៖** ស្ថានីយនៅលើតំណរដូចគ្នាអាចមានល្បឿន ឬសមត្ថភាពខុសៗគ្នាData Link Layer ធានានូវការគ្រប់គ្រងលំហូរដែលអាចឱ្យម៉ាស៊ីនទាំងពីរផ្លាស់ប្តូរទិន្នន័យក្នុងអត្រាដូចគ្នា។
- **ការចូលប្រើច្រើន៖** នៅពេលដែលម៉ាស៊ីននៅលើតំណរភ្ជាប់ដែលបានចែករំលែកព្យាយាមផ្ទេរទិន្នន័យ វាមានប្រូបាបខ្ពស់នៃការប៉ះទង្គិច។ Data Link Layer ផ្តល់នូវយន្តការដូចជា CSMA/CD ដើម្បីបំពាក់សមត្ថភាពនៃការចូលប្រើប្រព័ន្ធផ្សព្វផ្សាយដែលបានចែករំលែកក្នុងចំណោមប្រព័ន្ធជាច្រើន។

៤.២ ការរកឃើញកំហុសនិងការកែតម្រូវ

មានហេតុផលជាច្រើនដូចជា សំឡេងរំខាន ការនិយាយឆ្លងគ្នាជាដើម ដែលអាចបណ្តាលឱ្យទិន្នន័យខូចកំលុងពេលបញ្ជូន ស្រទាប់ខាងលើដំណើរការលើទិដ្ឋភាពទូទៅមួយចំនួននៃស្ថាបត្យកម្មបណ្តាញ ហើយមិនបានដឹងពីដំណើរការទិន្នន័យផ្នែករឹងពិតប្រាកដនោះទេ។ ដូច្នេះស្រទាប់ខាងលើរំពឹងថានឹងមានការបញ្ជូនដោយគ្មានកំហុសរវាងប្រព័ន្ធ កម្មវិធីភាគច្រើននឹងមិនដំណើរការដូចការរំពឹងទុកទេ ប្រសិនបើពួកគេបានទទួលទិន្នន័យខុស។ កម្មវិធីដូចជាសំឡេង និងវីដេអូប្រហែលជាមិនប៉ះពាល់នោះទេ ហើយដោយមានកំហុសមួយចំនួន ពួកវាអាចនៅតែដំណើរការបានល្អ។ Data Link Layer ប្រើយន្តការត្រួតពិនិត្យកំហុសមួយចំនួន ដើម្បីធានាថាស៊ុម (ស្ទ្រីមទិន្នន័យ) ត្រូវបានបញ្ជូនជាមួយនឹងកម្រិតជាក់លាក់នៃភាពត្រឹមត្រូវ។ ប៉ុន្តែដើម្បីយល់ពីរបៀបដែលកំហុសត្រូវបានគ្រប់គ្រង វាចាំបាច់ណាស់ក្នុងការដឹងថាកំហុសអ្វីអាចនឹងកើតឡើង។

៤.២.១ ប្រភេទនៃកំហុស

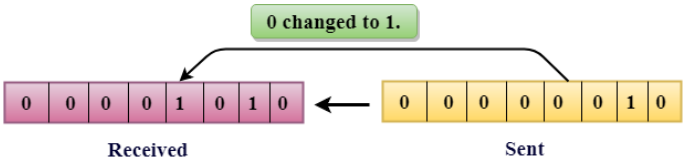
កំហុសអាចមានពីរប្រភេទ



រូបភាព ៤.១ ប្រភេទនៃកំហុស

ក. កំហុសមួយប៊ីត

ឯកតាទិន្នន័យដែលបានផ្តល់ឱ្យតែមួយប៊ីតប៉ុណ្ណោះត្រូវបានផ្លាស់ប្តូរពី ១ ទៅ ០ ឬពី ០ ទៅ ១



រូបភាព ៤.២ កំហុសមួយប៊ីត

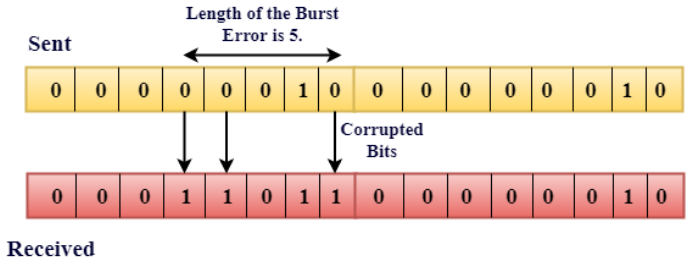
- **កំហុសមួយប៊ីត៖** មិនលេចឡើងទំនងជានៅក្នុងការបញ្ជូនទិន្នន័យសៀរៀលទេ។ ឧទាហរណ៍ អ្នកផ្ញើបញ្ជូនទិន្នន័យក្នុងល្បឿន ១០ Mbps ដែលមានន័យថាប៊ីតមាន

រយៈពេលត្រឹមតែ១ ហើយដើម្បីឱ្យមានកំហុសមួយប៊ីតកើតឡើង សំឡេងត្រូវតែលើសពី ១។

- **កំហុសមួយប៊ីត**៖ កើតឡើងជាចម្បងនៅក្នុងការបញ្ជូនទិន្នន័យស្របគ្នា។ ឧទាហរណ៍ ប្រសិនបើខ្សែភ្លើងចំនួនប្រាំបីត្រូវបានប្រើដើម្បីផ្ទេប្រាំបីប៊ីតនៃបៃមួយ ប្រសិនបើខ្សែភ្លើងមួយមានសំឡេងរំខាន នោះប៊ីតតែមួយនឹងខូចក្នុងមួយបៃប។

ខ.កំហុសប៊ូស

កំហុសប៊ូស ត្រូវបានគេស្គាល់ថាជាប៊ីតពីរ ឬច្រើនដែលត្រូវបានផ្លាស់ប្តូរពី ០ ទៅ ១ ឬពី ១ ទៅ ០ ។ កំហុសប៊ូស ត្រូវបានកំណត់ពីប៊ីតដែលខូចដំបូងទៅប៊ីតដែលខូចចុងក្រោយ។

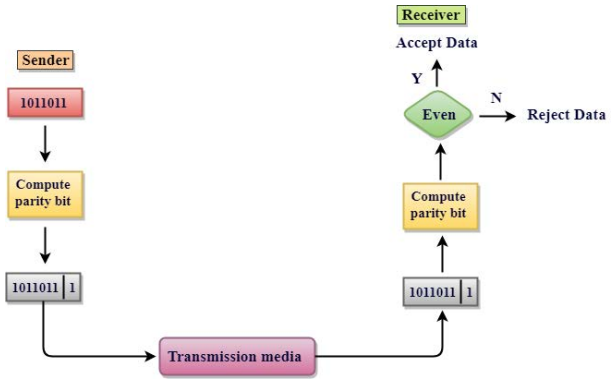


រូបភាព ៤.៣ កំហុសប៊ូស

៤.២.២ ការរកឃើញកំហុស

ការត្រួតពិនិត្យភាពស្មើគ្នា និងការត្រួតពិនិត្យស៊ីក្លីក (CRC) បានរកឃើញកំហុសនៅក្នុងស៊ុមដែលបានទទួល។ ក្នុងករណីទាំងពីរនេះ ប៊ីតបន្ថែមមួយចំនួនត្រូវបានផ្ញើ រួមជាមួយនឹងទិន្នន័យដាក់ស្តែងដើម្បីបញ្ជាក់ថាប៊ីតដែលទទួលបាននៅចុងម្ខាងទៀតគឺដូចគ្នានឹងពួកគេត្រូវបានផ្ញើ ប៊ីតត្រូវបានគេចាត់ទុកថាខូច ប្រសិនបើការពិនិត្យប្រឆាំងនៅខាងចុងអ្នកទទួលបរាជ័យ។

ការត្រួតពិនិត្យភាពស្មើគ្នាតែមួយ



រូបភាព ៤.៤ ការត្រួតពិនិត្យភាពស្មើគ្នាតែមួយ

- ការត្រួតពិនិត្យភាពស្មើគ្នាតែមួយគឺជាយន្តការដ៏សាមញ្ញមួយ និងមានតម្លៃថោកសម្រាប់ការរកឃើញកំហុស។
- នៅក្នុងបច្ចេកទេសនេះ ប៊ីតដែលលែងត្រូវការតទៅទៀតត្រូវបានគេស្គាល់ថាជាប៊ីត ភាពស្មើគ្នាដែលត្រូវបានបន្ថែមនៅចុងបញ្ចប់នៃឯកតាទិន្នន័យ ដូច្នេះចំនួន ១s ក្លាយជាគូ។ ដូច្នេះចំនួនសរុបនៃប៊ីតដែលបានបញ្ជូននឹងមាន ៩ ប៊ីត។
- ប្រសិនបើចំនួនប៊ីត ១s គឺសេស នោះ ភាពស្មើគ្នា ១ប៊ីត ត្រូវបានបន្ថែម ហើយប្រសិនបើចំនួន ១s bits គឺស្មើ នោះ ភាពស្មើគ្នា ០ប៊ីតត្រូវបានបន្ថែមនៅចុងបញ្ចប់នៃឯកតាទិន្នន័យ។
- នៅចុងបញ្ចប់នៃការទទួល ប៊ីត ភាពស្មើគ្នាត្រូវបានគណនាពីប៊ីតទិន្នន័យដែលទទួលបាន ហើយប្រៀបធៀបជាមួយនឹងប៊ីតដែលបានទទួល។
- បច្ចេកទេសនេះបង្កើតចំនួនសរុបនៃ ១វិនាទី ដូច្នេះវាត្រូវបានគេស្គាល់ថាជាការត្រួតពិនិត្យគូរ

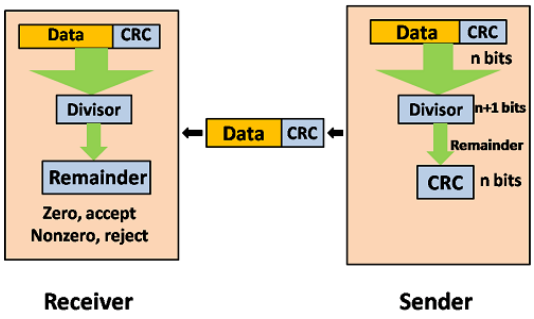
ការត្រួតពិនិត្យការបង្ក្រាបសីក្លីត (CRC)

CRC គឺជាវិធីសាស្ត្រផ្សេងគ្នាក្នុងការរកឃើញប្រសិនបើស៊ុមដែលទទួលបានមានទិន្នន័យត្រឹមត្រូវ បច្ចេកទេសនេះពាក់ព័ន្ធនឹងការបែងចែកប្រព័ន្ធគោលពីរនៃប៊ីតទិន្នន័យដែលត្រូវបានផ្ញើ។ ការបែងចែកត្រូវបានបង្កើតដោយប្រើពហុនាមអ្នកផ្ញើធ្វើប្រតិបត្តិការបែងចែកលើប៊ីតដែលបានបញ្ជូន ហើយគណនាសេស។ មុនពេលផ្ញើប៊ីតពិតប្រាកដ អ្នកផ្ញើបន្ថែមនៅសល់នៅចុងបញ្ចប់នៃប៊ីតសំខាន់ៗប៊ីតទិន្នន័យពិតបូកនឹងអ្វីដែលនៅសល់ត្រូវបានគេហៅថាពាក្យកូដ។ អ្នកផ្ញើបញ្ជូនទិន្នន័យប៊ីតជាកូដកូដ។

CRC គឺជាបច្ចេកទេសកំហុសដដែលៗដែលប្រើដើម្បីកំណត់កំហុស ខាងក្រោមនេះជាជំហានដែលត្រូវបានប្រើក្នុង CRC សម្រាប់ការរកឃើញកំហុស៖

- **នៅក្នុងបច្ចេកទេស CRC** ៖ខ្សែអក្សរនៃ n 0s ត្រូវបានបន្ថែមទៅឯកតាទិន្នន័យ ហើយចំនួន n នេះគឺតិចជាងចំនួនប៊ីតនៅក្នុងចំនួនដែលបានកំណត់ទុកជាមុន ដែលត្រូវបានគេស្គាល់ថាជាផ្នែកដែល n+1 ប៊ីត។
- **ទីពីរ៖** ទិន្នន័យដែលបានពង្រីកថ្មីត្រូវបានបែងចែកដោយអ្នកចែកដោយប្រើដំណើរការដែលគេស្គាល់ថាជាការបែងចែកប្រព័ន្ធគោលពីរ។ នៅសល់ដែលបានបង្កើតពីផ្នែកនេះត្រូវបានគេស្គាល់ថាជា CRC ដែលនៅសល់។
- **ទីបី៖** CRC ដែលនៅសល់ជំនួស 0s បន្ថែមនៅចុងបញ្ចប់នៃទិន្នន័យដើម ឯកតាដែលបានបង្កើតថ្មីនេះត្រូវបានបញ្ជូនទៅអ្នកទទួល។ អ្នកទទួលទទួលបានទិន្នន័យ បន្ទាប់មក CRC ដែលនៅសល់។
- **អ្នកទទួល**៖ នឹងចាត់ទុកអង្គភាពទាំងមូលនេះជាឯកតាតែមួយដែលបែងចែកដោយផ្នែកដូចគ្នាដែលប្រើដើម្បីស្វែងរក CRC ដែលនៅសល់។

ប្រសិនបើលទ្ធផលនៃការបែងចែកនេះគឺសូន្យ ដែលមានន័យថាវាមិនមានកំហុសទេ ទិន្នន័យត្រូវបានទទួលយក។ ប្រសិនបើលទ្ធផលនៃការបែងចែកនេះមិនមែនសូន្យទេ វាមានន័យថាទិន្នន័យមានកំហុស។ ដូច្នេះទិន្នន័យត្រូវបានលុបចោល។



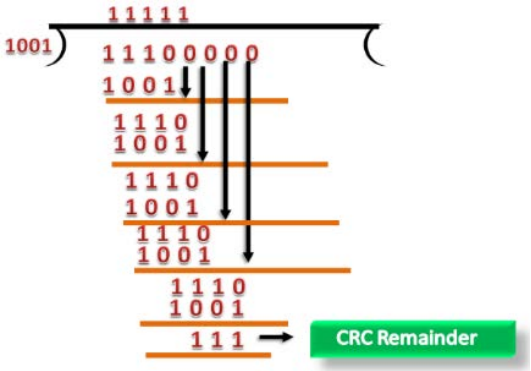
រូបភាព ៤.៥ ការត្រួតពិនិត្យការបង្ក្រាបស៊ីក្លីក (CRC)

អ្នកបង្កើត CRC

ឧបមាថាទិន្នន័យដើមគឺ 11100 ហើយផ្នែកគឺ 1001 ។

- CRC ប្រើផ្នែក ចែកយកសំណល់នឹង ២ ។ ទីមួយ លេខសូន្យបីត្រូវបានបន្ថែមនៅចុងបញ្ចប់នៃទិន្នន័យ ដោយសារប្រវែងនៃផ្នែកចែកគឺ ៤ ហើយយើងដឹងថាប្រវែងនៃខ្សែអក្សរ 0s ដែលត្រូវបន្ថែមគឺតែងតែមួយតិចជាងប្រវែងនៃផ្នែកចែក។

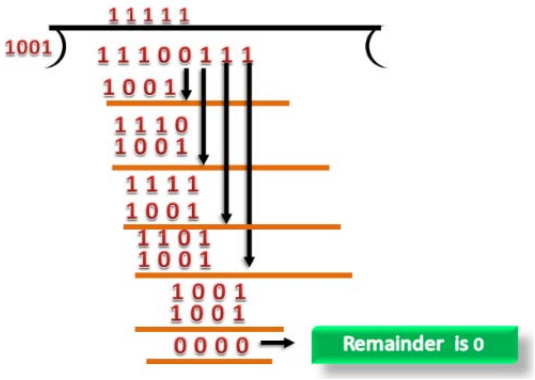
- ឥឡូវនេះ ខ្សែនេះក្លាយជា 11100000 ហើយខ្សែលទ្ធផលត្រូវបានបែងចែកដោយ 1001 ។
- នៅសល់ដែលបង្កើតចេញពីផ្នែកគោលពីរត្រូវបានគេស្គាល់ថាជា CRC ដែលនៅសល់ តម្លៃដែលបានបង្កើតនៃ CRC ដែលនៅសល់គឺ 111 ។
- សេសសល់ CRC ជំនួសខ្សែអក្សរបន្ថែមនៃ 0s នៅចុងបញ្ចប់នៃឯកតាទិន្នន័យ ហើយខ្សែអក្សរចុងក្រោយគឺ 11100111 ដែលផ្ញើឆ្លងកាត់បណ្តាញ។



រូបភាព ៤.៦ អ្នកបង្កើត CRC

អ្នកត្រួតពិនិត្យ CRC

- មុខងាររបស់ អ្នកត្រួតពិនិត្យ CRC គឺស្រដៀងទៅនឹង អ្នកបង្កើត CRC ។
- នៅពេលដែលខ្សែអក្សរ 11100111 ត្រូវបានទទួលនៅចុងទទួល អ្នកត្រួតពិនិត្យអនុវត្តការបែងចែកយកសំណល់នឹង ២។
- ខ្សែអក្សរមួយត្រូវបានបែងចែកដោយផ្នែកដូចគ្នា ពោលគឺ 1001។
- ក្នុងករណីនេះ អ្នកត្រួតពិនិត្យ CRC បង្កើតចំនួនសូន្យដែលនៅសល់ ដូច្នេះទិន្នន័យត្រូវបានទទួលយក។



រូបភាព ៤.៦ អ្នកត្រួតពិនិត្យ CRC

៤.២.៣ ការកែតម្រូវកំហុស

នៅក្នុងពិភពឌីជីថល ការកែកំហុសអាចធ្វើឡើងតាមពីរវិធី៖

- **ការកែកំហុសថយក្រោយ៖** នៅពេលដែលអ្នកទទួលរកឃើញ កំហុសនៅក្នុងទិន្នន័យដែលទទួលបាន វាស្នើសុំត្រឡប់ទៅអ្នកផ្ញើវិញ ដើម្បីបញ្ជូនឯកតាទិន្នន័យឡើងវិញ។
- **ការកែកំហុសបញ្ជូនបន្ត៖** នៅពេលដែលអ្នកទទួលរកឃើញកំហុសមួយចំនួននៅក្នុងទិន្នន័យដែលទទួលបាន វាដំណើរការកូដកែកំហុស ដែលជួយឱ្យវាងើបឡើងវិញដោយស្វ័យប្រវត្តិ និងកែកំហុសមួយចំនួន។

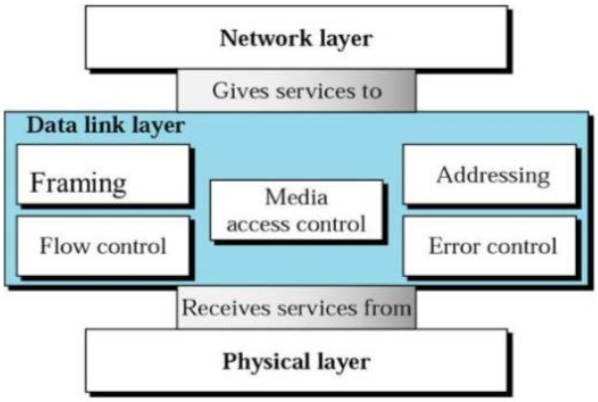
ទីមួយការកែកំហុសថយក្រោយ គឺសាមញ្ញ ហើយអាចប្រើយ៉ាងមានប្រសិទ្ធភាព ដែលការបញ្ជូនសារឡើងវិញមិនថ្លៃ។ ឧទាហរណ៍នៅក្នុងខ្សែកាបអុបទិក ប៉ុន្តែនៅក្នុងករណីនៃការបញ្ជូនឥតខ្សែ ការបញ្ជូនឡើងវិញអាចចំណាយច្រើនពេក។ ក្នុងករណីចុងក្រោយ ការកែកំហុសឆ្លងទៅមុខត្រូវបានប្រើដើម្បីកែកំហុសក្នុងស៊ុមទិន្នន័យ អ្នកទទួលត្រូវតែដឹងច្បាស់ថាប៊ីតណាមួយនៅក្នុងស៊ុមខូច។ ដើម្បីកំណត់ទីតាំងប៊ីតដែលមានកំហុស ប៊ីតមិនច្របូកច្របល់ត្រូវបានប្រើជាប៊ីតស្មើសម្រាប់ការរកឃើញកំហុស។ ឧទាហរណ៍ ប្រសិនបើយើងយកពាក្យ ASCII (ទិន្នន័យ ៧ ប៊ីត) យើងអាចត្រូវការព័ត៌មានប្រាំបីប្រភេទ៖ ប្រាំពីរប៊ីតដំបូងដើម្បីប្រាប់យើងថាប៊ីតមួយណាជាកំហុស និងមួយប៊ីតទៀតដើម្បីដឹងថាគ្មានកំហុស។ សម្រាប់ m ទិន្នន័យ ប៊ីតr លែងត្រូវការតទៅទៀត bits ត្រូវបានប្រើ។ r ប៊ីតអាចផ្តល់ព័ត៌មាន 2r បញ្ចូលគ្នានៅក្នុងពាក្យកូដ m + r ប៊ីតមានលទ្ធភាពដែល r ប៊ីតខ្លួនឯងអាចនឹងខូច។ ដូច្នេះចំនួន r ប៊ីតដែលបានប្រើត្រូវតែជូនដំណឹង (ប្រាប់អ្នកណាឬអ្វី?) អំពីទីតាំង m + r ប៊ីតបូកនឹងព័ត៌មានគ្មានកំហុស ពោលគឺ m + r + 1 ។

$$2^r >= m+r+1$$

រូបភាព ៤.៨ ការកែកំហុសរូបមន្ត

៤.៣ ពិធីការគ្រប់គ្រងតំណរភ្ជាប់ទិន្នន័យ

ការគ្រប់គ្រងតំណរភ្ជាប់ទិន្នន័យ (DLC) គឺជាមុខងារនៃ Data Link Layer នៅក្នុងគំរូ បើកការភ្ជាប់អន្តរប្រព័ន្ធ (OSI) ។ Data Link Layer ត្រូវតែផ្តល់ទិន្នន័យដែលអាចទុកចិត្តបានរវាង Physical layer និងបណ្តាញ លើសពីនេះ ចាំបាច់ត្រូវកំណត់ស៊ុម បញ្ចូល ECC (កំហុសក្នុងការកែកូដ) រវាងការរកឃើញកំហុស និងស៊ុម ហើយគ្រប់គ្រងលំហូរ។)



រូបភាព ៤.៩ ពិធីការគ្រប់គ្រងតំណរភ្ជាប់ទិន្នន័យ

ការគ្រប់គ្រងតំណរភ្ជាប់ទិន្នន័យមានគោលបំណងសម្រាប់ការទំនាក់ទំនងទិន្នន័យប្រកបដោយប្រសិទ្ធភាពរវាងការទទួល និងការបញ្ជូន។

- **ការធ្វើសមកាលកម្មស៊ុម៖** ទិន្នន័យត្រូវបានធ្វើក្នុងប្លុកដែលហៅថាស៊ុម។ អ្នកត្រូវដឹងពីការចាប់ផ្តើម និងចុងបញ្ចប់នៃស៊ុម។
- **ការគ្រប់គ្រងលំហូរ៖** ស៊ុមត្រូវតែផ្ញើទៅតាមអ្វីដែលអ្នកទទួលអាចទទួលយកបាន។
- **ការគ្រប់គ្រងកំហុស៖** កំហុសប៊ីតនៅក្នុងប្រព័ន្ធបញ្ជូនត្រូវតែត្រូវបានកែតម្រូវ។
- **អាសយដ្ឋាន៖** ដូចជា LAN (បណ្តាញក្នុងតំបន់) ចំណុចពីរដែលចូលរួមក្នុងការទំនាក់ទំនងត្រូវតែបញ្ជាក់នៅលើតំណរដូចគ្នា។
- **ការគ្រប់គ្រង និងទិន្នន័យនៅលើតំណរដូចគ្នា៖** ព័ត៌មានត្រួតពិនិត្យ និងទិន្នន័យមិនត្រូវបានរក្សាទុកដោយឡែកទេ ប៉ុន្តែត្រូវបានដំណើរការក្នុងការតភ្ជាប់ដូចគ្នា។ អ្នកទទួលត្រូវតែអាចបែងចែករវាងព័ត៌មានគ្រប់គ្រង និងទិន្នន័យ។
- **ការគ្រប់គ្រងតំណរភ្ជាប់៖** ការគ្រប់គ្រងតំណរគឺត្រូវបានទាមទារសម្រាប់ការផ្លាស់ប្តូរទិន្នន័យជាបន្តបន្ទាប់រវាងចំណុច។

៤.៣.១ ការត្រួតពិនិត្យលំហូរ

ការគ្រប់គ្រងលំហូរគឺជាបច្ចេកវិទ្យាដែលកែតម្រូវអត្រាទិន្នន័យមិនឱ្យលើសពីអត្រាដែលអ្នកទទួលអាចទទួលយកបានបើគ្មានការគ្រប់គ្រងលំហូរទេវានឹងហៀរចេញខណៈពេលដែលសតិបញ្ជាបណ្តោះ អាសន្នរបស់អ្នកទទួលកំពុងដំណើរការ។

ការគ្រប់គ្រងលំហូរមានពីរប្រភេទ។

- **ឈប់ និង រង់ចាំ៖** ផ្ទៃតែស៊ុមមួយក្នុងពេលតែមួយ។
- **បង្ហូចរអិល៖** ផ្ទៃស៊ុមជាច្រើនក្នុងពេលតែមួយ។

ក. ការត្រួតពិនិត្យលំហូរឈប់និងរង់ចាំ

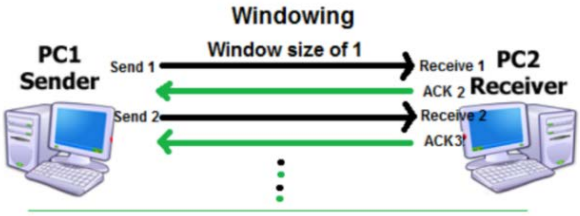
ការគ្រប់គ្រងលំហូរឈប់ និងរង់ចាំ គឺជាទម្រង់សាមញ្ញបំផុតរបស់វា សារត្រូវបានបំបែកជាស៊ុមជាច្រើន។ អ្នកផ្ទៃផ្ទើស៊ុមមួយក្នុងពេលតែមួយ ហើយរង់ចាំឱ្យអ្នកទទួលដំណើរការទិន្នន័យ និងផ្ទើសារ ACK ។ ការបញ្ជូនកាន់តែយូរ ឱកាសនៃកំហុសកាន់តែខ្ពស់ ប្រសិនបើស៊ុមមួយ ឬ ACK ត្រូវបានបាត់បង់ អ្នកផ្ទៃត្រូវតែបញ្ជូនឡើងវិញ។ ប្រតិបត្តិការនេះត្រូវបានគេហៅថា ARQ (ការស្នើសុំឡើងវិញដោយស្វ័យប្រវត្តិ)។

១. វាត្រូវតែរង់ចាំសារ ACK នៅពេលដែលរាល់ស៊ុមត្រូវបានបញ្ជូន ប្រសិនបើរយៈពេលនៃការបញ្ជូនមានរយៈពេលយូរនោះវាគ្មានប្រសិទ្ធភាពខ្លាំងទេ។

២. នៅពេលដែលការបញ្ជូនមានរយៈពេលយូរវាមិនមានប្រសិទ្ធភាព ការបញ្ជូនកាន់តែយូរ ហើយឱកាសនៃកំហុសកាន់តែខ្ពស់។ ប្រសិនបើការបញ្ជូនមានរយៈពេលខ្លី កំហុសអាចត្រូវបានចាប់បានទាន់ពេល។

ខ. ការត្រួតពិនិត្យលំហូរ

វិធីសាស្ត្រនេះបញ្ជូនទិន្នន័យរហូតដល់អ្នកទទួលពេញការបញ្ជូនគួរតែបញ្ឈប់រហូតទាល់តែអ្នកទទួលជូនដំណឹងដល់ការគ្រប់គ្រងលំហូរបង្ហូចរអិលមានប្រសិទ្ធភាពនៅពេលដែលទំហំផ្ទុកមានកំណត់។ នៅពេលដែលអ្នកទទួលមានចន្លោះអង្គចងចាំបណ្តោះអាសន្នដើម្បីទទួល n ស៊ុម អ្នកផ្ទៃអាចផ្ទៃដោយមិនបានទទួលសារ ACK រហូតដល់អ្នកទទួលដាក់ n ស៊ុម ទៅក្នុង អង្គចងចាំបណ្តោះអាសន្ន ស៊ុមបញ្ជូនបន្តត្រូវបានដាក់លេខដើម្បីធ្វើតាមស៊ុម ACK ។



រូបភាព ៤.១០ ការគ្រប់គ្រងលំហូរ

៤.៣.២ បច្ចេកទេសត្រួតពិនិត្យកំហុស

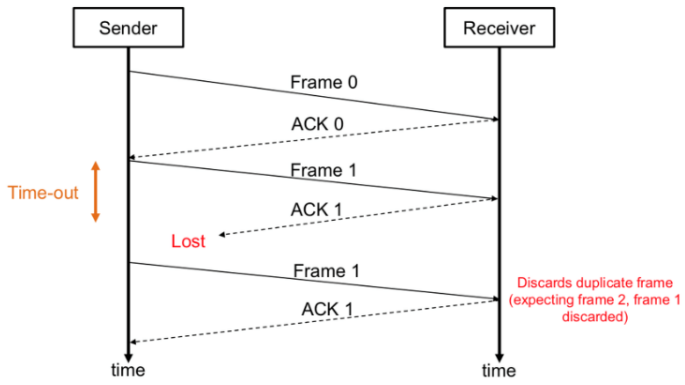
នៅពេលដែលស៊ុមទិន្នន័យត្រូវបានបញ្ជូន វាមានប្រូបាប៊ីលីតេដែលថាស៊ុមទិន្នន័យអាចនឹងបាត់បង់ក្នុងពេលបញ្ជូនឬវាត្រូវបានទទួលខូច។ក្នុងករណីទាំងពីរអ្នកទទួលមិនទទួលបានស៊ុមទិន្នន័យត្រឹមត្រូវទេ ហើយអ្នកផ្ញើមិនដឹងអ្វីទាំងអស់អំពីការបាត់បង់ណាមួយឡើយ។ ក្នុងករណីបែបនេះ ទាំងអ្នកផ្ញើនិងអ្នកទទួលត្រូវបានបំពាក់ដោយពិធីការមួយចំនួនដែលជួយពួកគេឱ្យរកឃើញកំហុសឆ្លងកាត់ដូចជាការបាត់បង់ស៊ុមទិន្នន័យជាដើម ដូច្នេះទាំងអ្នកផ្ញើបញ្ជូនស៊ុមទិន្នន័យឡើងវិញ ឬអ្នកទទួលអាចស្នើសុំឱ្យបញ្ជូនស៊ុមទិន្នន័យពីមុនឡើងវិញ។ តម្រូវការសម្រាប់យន្តការត្រួតពិនិត្យកំហុស៖

- **ការរកឃើញកំហុស៖** អ្នកផ្ញើ និងអ្នកទទួល មិនថាទាំងពីរ ឬណាមួយឡើយ ត្រូវតែបញ្ជាក់អំពីកំហុសមួយចំនួននៅក្នុងការដឹកជញ្ជូន។
- **ACK វិជ្ជមាន៖** នៅពេលដែលអ្នកទទួលបានទទួលស៊ុមត្រឹមត្រូវ វាគួរតែទទួលស្គាល់វា។
- **ACK** អវិជ្ជមាន៖ នៅពេលដែលអ្នកទទួលទទួលបានស៊ុមដែលខូច ឬស៊ុមស្ងួន វាបញ្ជូន NACK ត្រឡប់ទៅអ្នកផ្ញើវិញ ហើយអ្នកផ្ញើត្រូវតែបញ្ជូនស៊ុមត្រឹមត្រូវឡើងវិញ។
- **ការបញ្ជូនឡើងវិញ៖** អ្នកផ្ញើរក្សានាឡិកា និងកំណត់រយៈពេលអស់ពេល។ ឧបមាថាការទទួលស្គាល់ស៊ុមទិន្នន័យដែលបានបញ្ជូនពីមុនមិនមកដល់មុនពេលអស់ពេល។ ក្នុងករណីនោះ អ្នកផ្ញើបញ្ជូនស៊ុមឡើងវិញ ដោយគិតថាស៊ុម ឬការទទួលស្គាល់របស់វាត្រូវបានបាត់បង់ក្នុងពេលឆ្លងកាត់។

មានបច្ចេកទេសបីប្រភេទដែលData Link Layer អាចដាក់ពង្រាយដើម្បីគ្រប់គ្រងកំហុសដោយការស្នើសុំម្តងទៀតដោយស្វ័យប្រវត្តិ (ARQ)៖

ក. បញ្ឈប់និងរង់ចាំ ARQ

ការគ្រប់គ្រងកំហុសនេះ គឺត្រូវផ្អែកលើបច្ចេកទេសគ្រប់គ្រងលំហូរឈប់ និងរង់ចាំ។ ប្រភពត្រូវតែផ្ញើស៊ុមមួយហើយបន្ទាប់មករង់ចាំ ACK ស៊ុមដូចគ្នាត្រូវបានផ្ញើម្តងទៀត ប្រសិនបើគ្មានសារ ACK ត្រូវបានទទួលក្នុងអំឡុងពេលអស់ពេល។



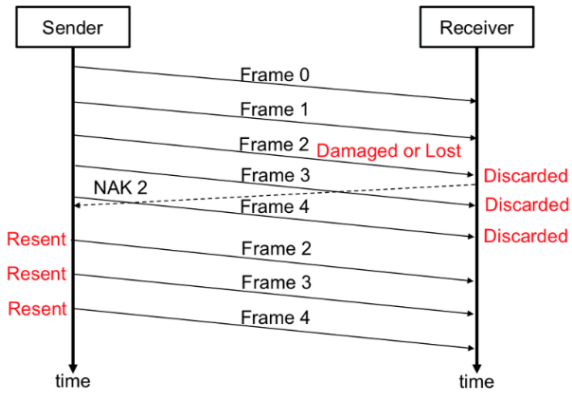
រូបភាព ៤.១១ បញ្ឈប់និងរង់ចាំ ARQ

ការផ្លាស់ប្តូរខាងក្រោមអាចកើតឡើងនៅក្នុងការបញ្ឈប់ និងរង់ចាំ ARQ ៖

- អ្នកផ្ញើរក្សាការរាប់ម៉ោង។
- នៅពេលដែលស៊ុមមួយត្រូវបានផ្ញើ អ្នកផ្ញើចាប់ផ្តើមរាប់ម៉ោងអស់។
- ប្រសិនបើការទទួលស្គាល់ស៊ុមមកទាន់ពេល អ្នកផ្ញើបញ្ជូនស៊ុមបន្ទាប់ក្នុងជួរ។
- ប្រសិនបើការទទួលស្គាល់មិនមកទាន់ពេល អ្នកផ្ញើសន្មត់ថា ស៊ុម ឬការទទួលស្គាល់របស់វាត្រូវបានបាត់បង់ក្នុងពេលឆ្លងកាត់ អ្នកផ្ញើបញ្ជូនស៊ុមឡើងវិញ ហើយចាប់ផ្តើមការរាប់ពេលវេលា។

ខ. ត្រឡប់ទៅវិញ N ARQ

បញ្ឈប់ហើយរង់ចាំយន្តការ N ARQ ត្រូវការប្រើប្រាស់ធនធានឱ្យអស់ពីសមត្ថភាពពេលទទួលបានការទទួលស្គាល់ អ្នកផ្ញើអង្គុយនៅទំនេរមិនធ្វើអ្វីឡើយ។ នៅក្នុងវិធីត្រឡប់ទៅវិញ N ARQទាំងអ្នកផ្ញើ និងអ្នកទទួលរក្សាបង្ហួច។

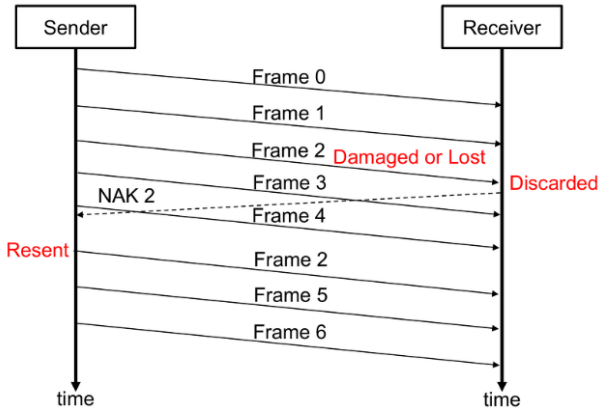


រូបភាព ៤.១២ ត្រឡប់ទៅវិញ N ARQ

ទំហំបញ្ជូនអនុញ្ញាតឱ្យអ្នកផ្ញើផ្ញើស៊ុមច្រើនដោយមិនទទួលបានការទទួលស្គាល់ពីស៊ុមមុន ទទួលអនុញ្ញាតឱ្យអ្នកទទួលទទួលស៊ុមជាច្រើន និងទទួលស្គាល់ពួកគេ។ អ្នកទទួលតាមដានលេខលំដាប់នៃស៊ុមចូលនៅពេលអ្នកផ្ញើផ្ញើស៊ុមទាំងអស់ វាពិនិត្យមើលថាតើលេខលំដាប់ណាដែលវាបានទទួលការទទួលស្គាល់ជាវិជ្ជមាន។ អ្នកផ្ញើផ្ញើសំណុំបន្ទាប់នៃស៊ុម ប្រសិនបើស៊ុមទាំងអស់ត្រូវបានទទួលស្គាល់ជាវិជ្ជមាន ប្រសិនបើអ្នកផ្ញើរកឃើញថាវាបានទទួល NACK ឬមិនបានទទួល ACK ណាមួយសម្រាប់ស៊ុមជាក់លាក់មួយ វាបញ្ជូនស៊ុមទាំងអស់ឡើងវិញបន្ទាប់ពីនោះវាមិនទទួលយក ACK វិជ្ជមានណាមួយឡើយ។

គ. ជ្រើសរើសបដិសេធ ARQ

វិធីសាស្ត្របញ្ជូនគឺដូចគ្នានឹងទម្រង់ត្រឡប់ទៅវិញ N ARQដែរ ភាពខុសគ្នានោះគឺថាប្រសិនបើអ្នកទទួលបដិសេធស៊ុមតែមួយ វាបញ្ជូនតែស៊ុមនោះឡើងវិញ។ អ្នកទទួលត្រូវតែអង្គចងចាំបណ្តោះអាសន្ននូវស៊ុមដែលមិនមានការបញ្ជាទិញ។ដូច្នេះត្រូវការអង្គចងចាំបណ្តោះអាសន្នធំល្មមដើម្បីរក្សាទុកស៊ុមក្នុងលំដាប់មុនរហូតដល់ពួកវាត្រូវបានបញ្ជូនសាជាថ្មី។



រូបភាព ៤.១៣ ជ្រើសរើសបដិសេធ ARQ

នៅក្នុង ជ្រើសរើសធ្វើម្តងទៀត ARQ ខណៈពេលដែលរក្សាការតាមដានលេខលំដាប់ អ្នកទទួលផ្ទុកស៊ុមក្នុងសតិ ហើយផ្ញើ NACK សម្រាប់តែស៊ុមដែលបាត់ ឬខូចប៉ុណ្ណោះ។ អ្នកផ្ញើក្នុងករណីនេះផ្ញើតែកញ្ចប់ព័ត៌មានដែល NACK ត្រូវបានទទួល។

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះអ្នកបានសិក្សាអំពី៖

- **ការរៀបចំ Data Link Layer** ៖ យកកញ្ចប់ព័ត៌មានពីស្រទាប់បណ្តាញ ហើយបញ្ចូលពួកវាទៅក្នុងស៊ុម បន្ទាប់មក វាបញ្ជូនស៊ុមនីមួយៗទៅលើផ្នែករឹង។ នៅចុងបញ្ចប់របស់អ្នកទទួល ស្រទាប់តំណទិន្នន័យចាប់យកសញ្ញាពីផ្នែករឹង ហើយផ្គុំពួកវាទៅជាស៊ុម។
- **ការដោះស្រាយ Data Link Layer** ៖ ផ្តល់នូវយន្តការកំណត់អាសយដ្ឋានផ្នែករឹងរបស់ស្រទាប់ទី២។ អាសយដ្ឋានផ្នែករឹងត្រូវបានសន្មត់ថាមានតែមួយគត់នៅលើតំណ វាត្រូវបានអ៊ិនកូដទៅក្នុងផ្នែករឹងនៅពេលផលិត។
- **ការធ្វើសមកាលកម្ម**៖ នៅពេលដែលស៊ុមទិន្នន័យត្រូវបានផ្ទេរនៅលើតំណ ម៉ាស៊ីនទាំងពីរត្រូវតែធ្វើសមកាលកម្មដើម្បីផ្ទេរទៅកន្លែង។
- **ការគ្រប់គ្រងកំហុសពេលខ្លះ**៖ សញ្ញាអាចជួបប្រទះបញ្ហាក្នុងការផ្លាស់ប្តូរ ហើយប៊ីតត្រូវបានត្រឡប់។ កំហុសទាំងនេះត្រូវបានរកឃើញ ហើយការព្យាយាមត្រូវបានធ្វើឡើងដើម្បីសង្គ្រោះទិន្នន័យពិតប្រាកដប៊ីតវាក៏ផ្តល់នូវយន្តការរាយការណ៍កំហុសដល់អ្នកផ្ញើផងដែរ។
- **ស្ថានីយ៍ត្រួតពិនិត្យ**៖ លំហូរនៅលើតំណដូចគ្នាអាចមានល្បឿន ឬសមត្ថភាពខុសៗគ្នា។ Data Link Layer ធានានូវការគ្រប់គ្រងលំហូរ ដែលអនុញ្ញាតឱ្យម៉ាស៊ីនទាំងពីរផ្លាស់ប្តូរទិន្នន័យក្នុងពេលដំណាលគ្នា។
- **ការចូលប្រើច្រើន**៖ នៅពេលដែលម៉ាស៊ីននៅលើតំណភ្ជាប់ដែលបានចែករំលែកព្យាយាមផ្ទេរទិន្នន័យ វាមានប្រូបាបខ្ពស់នៃការប៉ះទង្គិច។ Data Link Layer ផ្តល់នូវយន្តការដូចជា CSMA/CD ដើម្បីធ្វើការអនុញ្ញាតឱ្យចូលប្រើប្រព័ន្ធផ្សព្វផ្សាយដែលបានចែករំលែកក្នុងចំណោមប្រព័ន្ធជាច្រើន។
- **ការកែកំហុសចុយក្រោយ**៖ នៅពេលដែលអ្នកទទួលរកឃើញកំហុសនៅក្នុងទិន្នន័យដែលទទួលបាន វាស្នើសុំត្រឡប់ទៅអ្នកផ្ញើវិញ ដើម្បីបញ្ជូនឯកតាទិន្នន័យឡើងវិញ។
- **ការកែកំហុសបញ្ជូនបន្ត**៖ នៅពេលអ្នកទទួលរកឃើញកំហុសមួយចំនួននៅក្នុងទិន្នន័យដែលទទួលបាន វាដំណើរការកូដកែកំហុស ដែលជួយឱ្យវាងើបឡើងវិញដោយស្វ័យប្រវត្តិ និងកែកំហុសមួយចំនួន។

សំណួរ

១. តើអ្វីជាមុខងារនៃ Data Link Layer?

២. តើអ្វីជាភាពខុសគ្នារវាងការកែកំហុសចុយក្រោយ និងការកែកំហុសឆ្គងទៅមុខ?

៣. ចូរពន្យល់ពីការគ្រប់គ្រងកំហុស។

៤. តើការពិនិត្យ ការពិនិត្យភាពស្មើគ្នានិងការត្រួតពិនិត្យការបង្ក្រាបស៊ីក្លីគ (CRC) ខុសគ្នាដូចម្តេច?

5. តើការគ្រប់គ្រងលំហូរគឺជាអ្វី?

ការអនុវត្តន៍ទី៤

សមាសធាតុនៃបណ្តាញ នៅពេលអ្នកចង់ប្រើបណ្តាញនៅលើកុំព្យូទ័ររបស់អ្នក មានចំណុចមួយចំនួនដែលអ្នកត្រូវកំណត់រចនាសម្ព័ន្ធ៖ អាសយដ្ឋាន IP បណ្តាញរង និងច្រកផ្លូវ។

- **អាសយដ្ឋាន IP៖** សំដៅលើអាសយដ្ឋានលេខតែមួយគត់នៅលើអ៊ីនធឺណិត។
- **ច្រកផ្លូវ៖** គឺជាផ្លូវសម្រាប់ការតភ្ជាប់អ៊ីនធឺណិតខាងក្រៅ។
- **បណ្តាញរង៖** បណ្តាញដាច់ដោយឡែក។

ក. គោលបំណងនៃការអនុវត្តនេះ

- ដើម្បីពន្យល់ពីសមាសធាតុបណ្តាញ។
- ដើម្បីពន្យល់ពីភាពខុសគ្នារវាង IP, Gateway, និង Subnet ។
- ដើម្បីក្លែងធ្វើការកំណត់ IP តាមរយៈ Packet Tracer ។

ក១.តើអាសយដ្ឋាន IP គឺជាអ្វី?

អក្សរកាត់នៃពិធីការអ៊ីនធឺណិត សំដៅលើពិធីការទំនាក់ទំនងសម្រាប់ការទទួល និងបញ្ជូនព័ត៌មានជាក់លាក់នៅក្នុងបណ្តាញតាមរយៈអ៊ីនធឺណិត។ ក្នុងករណីកុំព្យូទ័រ ប្រព័ន្ធប្រតិបត្តិការដែលប្រើគឺខុសគ្នា ហើយក្នុងករណីកម្មវិធី ភាសាដែលបានអនុវត្តគឺខុសគ្នា ដូច្នេះពិធីការទំនាក់ទំនងទូទៅ (ពិធីការ) គឺត្រូវបានទាមទារដើម្បីឱ្យពួកវាអាចទំនាក់ទំនងតាមបណ្តាញ។ នៅទសវត្សរ៍ឆ្នាំ ១៩៦០ នៅពេលដែលទំនាក់ទំនងកុំព្យូទ័រស្ថិតជាដំបូង ក្រុមហ៊ុនផលិតឧបករណ៍ផ្សេងៗគ្នាបានប្រើប្រាស់ពិធីការផ្សេងៗគ្នាក្នុងការទំនាក់ទំនងរវាងឧបករណ៍របស់ក្រុមហ៊ុនផ្សេងៗគ្នាគឺពិបាក ឬមិនអាចទៅរួច។ សម្រាប់ហេតុផលនេះ គណៈកម្មាធិការអាយអេសអូ សម្រាប់ស្តង់ដារអន្តរជាតិនៃពិធីការពាក់ព័ន្ធត្រូវបានបង្កើតឡើង ហើយម៉ូដែល OSI ៧ស្រទាប់ ត្រូវបានប្រកាសនៅឆ្នាំ ១៩៧៧។

ក២. តើបណ្តាញរង គឺជាអ្វី?

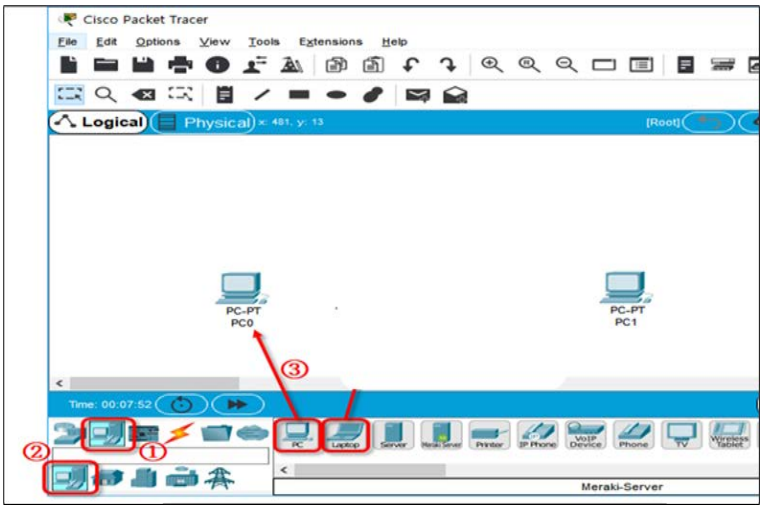
អាសយដ្ឋាន IPv4 បានក្លាយជាការពិតហើយ NIC (មជ្ឈមណ្ឌលព័ត៌មានបណ្តាញ) របស់ប្រទេសនីមួយៗបានខិតខំប្រឹងប្រែងដើម្បីបែងចែកតែក្រុម IP សាធារណៈឱ្យបានច្រើនតាមដែលម៉ាស៊ីនត្រូវការទៅកាន់តំបន់បណ្តាញមូលដ្ឋានដែល ផ្សាយដោយរ៉ោតទ័រនីមួយៗដើម្បីបន្ថយល្បឿនរបស់វាឱ្យបានច្រើន។ តាមដែលអាចធ្វើបានដើម្បីឆ្លើយតបទៅនឹងតម្រូវការរបស់អង្គការ NIC ទាំងនេះ IETF បានកំណត់ស្តង់ដារមធ្យោបាយមួយដើម្បីសម្គាល់យ៉ាងច្បាស់នូវក្រុម IP របស់ម៉ាស៊ីនដែលតភ្ជាប់ពីក្នុងបណ្តាញមូលដ្ឋានពីបណ្តាញខាងក្រៅ ហើយនេះគឺជារបាំងបណ្តាញរង។

ក៣. តើអ្វីជាច្រកផ្លូវ?

ច្រកផ្លូជាឧបករណ៍ដែលត្រូវគ្នានឹងស្រទាប់ដឹកជញ្ជូនក្នុងចំណោម OSI ៧ស្រទាប់ វាគឺជាឧបករណ៍ដែលភ្ជាប់ពិធីការផ្សេងដូច្នេះការទំនាក់ទំនងតាមបណ្តាញអាចធ្វើទៅបាន។
ឧទាហរណ៍៖ តំណាងគឺជាច្រករវាងឧបករណ៍ទំនាក់ទំនងចល័ត និងអ៊ីនធឺណិតដោយសារតែមានច្រកចេញចូលទើបយើងអាចចូលប្រើប្រាស់ អ៊ីនធឺណិតបានដូចជាកុំព្យូទ័រដែលមានទូរសព្ទស្មាតហ្វូន។

ខ. ការកំណត់ IP នៅក្នុង Packet Tracer

១.បន្ថែមកុំព្យូទ័រ

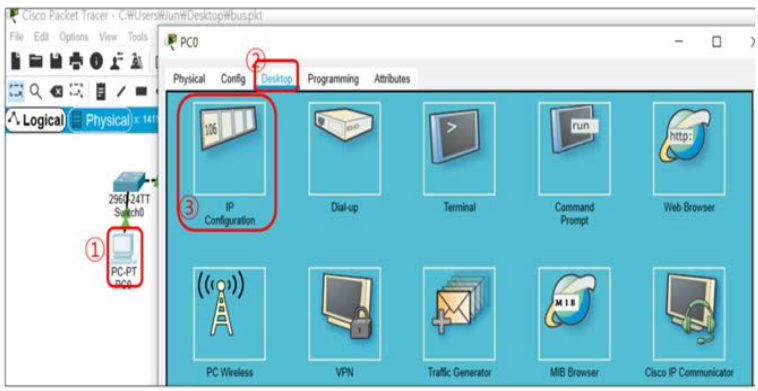


ក. ចុចលើ [ឧបករណ៍បញ្ចប់(End Devices)] → ជ្រើសរើស Desktop

ខ. ចុចលើ [ឧបករណ៍បញ្ចប់(End Devices)] → ជ្រើសរើស Laptop

គ. បន្ទាប់មក ចុចលើ 'PC' ឬLaptop ហើយអូសទម្លាក់លើផ្ទាំងកិច្ចការ

២. ការកំណត់ IP នៅក្នុង Packet Tracer

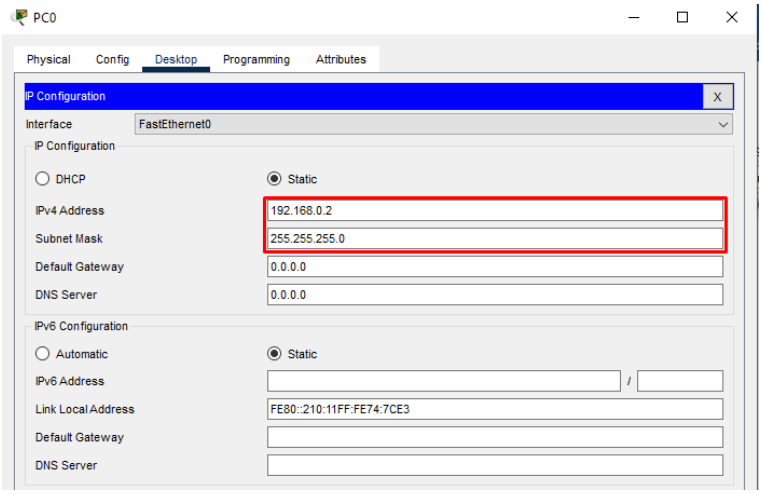


ក. យកកណ្តុរចុចពីរដងលើ [PC0]

ខ. ចុចលើ [Desktop]

គ.ចុចលើ [IP Configuration]

៣. ការកំនត់ IP លើកុំព្យូទ័រ



ក. IP Address: 192.168.0.2

ខ. Subnet Mask: 255.255.255.0

គ.សង្ខេបការអនុវត្តន៍

បណ្តាញប្រព័ន្ធមានសមាសភាគសំខាន់បីយ៉ាងគឺ អាស័យដ្ឋាន (IP Address) ច្រកផ្លូវ (Gateway)និង បណ្តាញរង (Subnet mask)។

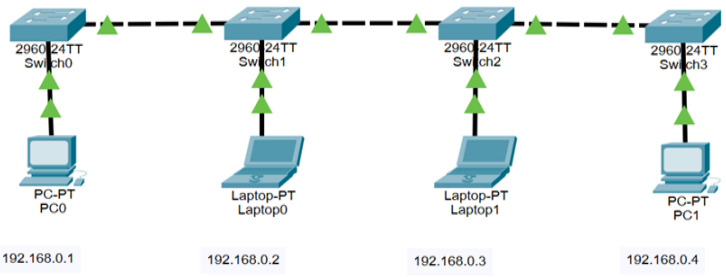
- អាសយដ្ឋាន IP សំដៅលើអាសយដ្ឋានលេខតែមួយគត់នៅលើអ៊ីនធឺណិត។
- ច្រកផ្លូវគឺជាផ្លូវសម្រាប់ការតភ្ជាប់អ៊ីនធឺណិតខាងក្រៅ។
- បណ្តាញរង បណ្តាញដាច់ដោយឡែក។

ឃ.កិច្ចការស្រាវជ្រាវ

កិច្ចការ១៖ ចូរបង្កើតរចនាសម្ព័ន្ធ **Bus Topology** ហើយបញ្ចូល **IP** ទៅកាន់ឧបករណ៍ នីមួយៗ ដើម្បីកំណត់រចនាសម្ព័ន្ធបណ្តាញ ហើយធ្វើឱ្យបណ្តាញទំនាក់ទំនងគ្នាបាន។

ក. ដាក់កុងតាក់ចំនួន៤ ហើយភ្ជាប់គ្នាដូចរូប

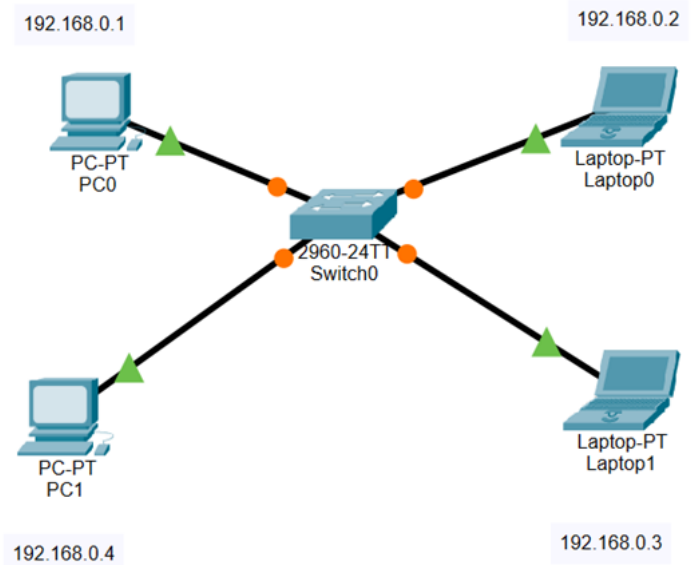
ខ. ភ្ជាប់កុំព្យូទ័រដាក់ **IP Address** ដូចរូបខាងក្រោម បន្ទាប់ធ្វើការតេស្តគឺង **IP**

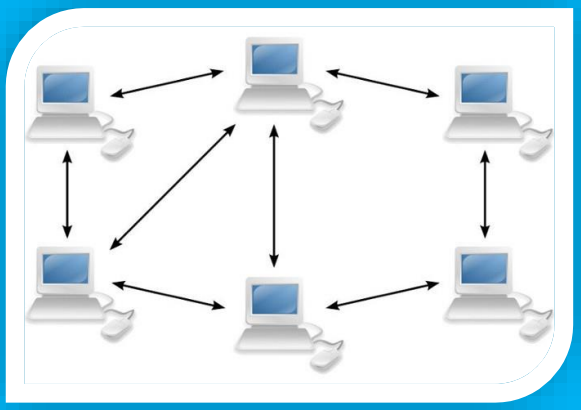


កិច្ចការ២៖ ចូរបង្កើតរចនាសម្ព័ន្ធ **Ring Topology** ហើយបញ្ចូល IP ទៅកាន់ឧបករណ៍នីមួយៗដើម្បីកំណត់រចនាសម្ព័ន្ធបណ្តាញ ហើយធ្វើឱ្យបណ្តាញទំនាក់ទំនងគ្នាបាន។

ក. ដាក់កុងតាក់ចំនួន១ ហើយភ្ជាប់គ្នាដូចរូប

ខ. ភ្ជាប់កុំព្យូទ័រដាក់ **IP Address** ដូចរូបខាងក្រោម បន្ទាប់ធ្វើការតេស្តភីង **IP**





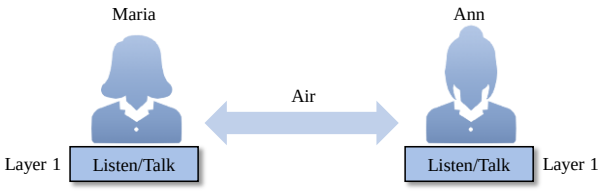
ជំពូកទី៥
ម៉ូដែលបណ្តាញ

ដើម្បីធ្វើឱ្យទំនាក់ទំនងទទួលបានជោគជ័យរវាងឧបករណ៍ ច្បាប់ និងនីតិវិធីមួយចំនួនគួរតែត្រូវបានយល់ព្រមនៅពេលបញ្ចប់ការផ្ទេ និងទទួលនៃប្រព័ន្ធ។ ច្បាប់ និងគោលការណ៍ណែនាំបែបនេះត្រូវបានគេហៅថាពិធីការ ប្រភេទផ្សេងគ្នានៃពិធីការត្រូវបានប្រើសម្រាប់ប្រភេទផ្សេងគ្នានៃការទំនាក់ទំនង។ វិស្វកម្មបណ្តាញពាក់ព័ន្ធនឹងកម្មវិធី កម្មវិធីបង្កប់ វិស្វកម្មកម្រិតបន្ទះឈីប ផ្នែករឹង និងជីពចរអគ្គិសនី គំនិតនៃបណ្តាញត្រូវបានបែងចែកទៅជាស្រទាប់ជាច្រើន ដើម្បីសម្រួលដល់វិស្វកម្មបណ្តាញ។ ស្រទាប់នីមួយៗត្រូវបានចូលរួមនៅក្នុងកិច្ចការពិសេស និងឯករាជ្យនៃស្រទាប់ផ្សេងទៀតទាំងអស់ ប៉ុន្តែសរុបមក ការងារបណ្តាញស្ទើរតែទាំងអស់គឺអាស្រ័យលើស្រទាប់ទាំងនេះទាំងអស់ ស្រទាប់ចែករំលែកទិន្នន័យហើយពួកវាពឹងផ្អែកលើគ្នាទៅវិញទៅមកដើម្បីទទួលបញ្ចូល និងបញ្ជូនលទ្ធផល។

ជំពូកទី៥ នេះ អ្នកនឹងរៀនអំពី៖

៥.១ ស្រទាប់ពិធីការ និងបណ្តាញ

នៅក្នុងការទំនាក់ទំនងទិន្នន័យ និងបណ្តាញ ពិធីការមួយកំណត់ច្បាប់ដែលទាំងអ្នកផ្ញើ និងអ្នកទទួល និងឧបករណ៍កម្រិតមធ្យមទាំងអស់ត្រូវតែអនុវត្តតាម ដើម្បីទំនាក់ទំនងប្រកបដោយប្រសិទ្ធភាព នៅពេលដែលទំនាក់ទំនងមានលក្ខណៈសាមញ្ញ យើងប្រហែលជាត្រូវការតែពិធីការត្រង់ប៉ុណ្ណោះ។ ប៉ុន្តែនៅពេលដែលទំនាក់ទំនងមានភាពស្មុគស្មាញ យើងប្រហែលជាត្រូវបែងចែកកិច្ចការរវាងស្រទាប់ផ្សេងៗគ្នា យើងត្រូវការ ពិធីការ នៅស្រទាប់នីមួយៗ ឬ ស្រទាប់ពិធីការ នៅក្នុងសេណារីយ៉ូទីមួយ ការទំនាក់ទំនងគឺសាមញ្ញណាស់ ដែលវាអាចកើតឡើងក្នុងស្រទាប់តែមួយប៉ុណ្ណោះ។ សន្មត់ថា Maria និង Ann គឺជាអ្នកជិតខាងដែលមានគំនិតទូទៅច្រើនការប្រាស្រ័យទាក់ទងគ្នារវាង Maria និង Ann ធ្វើឡើងក្នុងស្រទាប់តែមួយ ទល់មុខគ្នាជាភាសាតែមួយ។



រូបភាព ៥.១ ស្រទាប់ពិធីការ និងបណ្តាញ

សូម្បីតែនៅក្នុងសេណារីយ៉ូសាមញ្ញនេះ យើងអាចមើលឃើញថាច្បាប់ត្រូវតែអនុវត្តតាម។

- **ទីមួយ៖** Maria និង Ann ដឹងថាពួកគេគួរតែធ្វើការទំនាក់ទំនងគ្នាទៅវិញទៅមកនៅពេលពួកគេជួបគ្នាជាលើកដំបូង
- **ទីពីរ៖** ពួកគេដឹងថាពួកគេគួរតែកំណត់វាក្យសព្ទរបស់ពួកគេដល់កម្រិតនៃទំនាក់ទំនងរបស់ពួកគេ។
- **ទីបី៖** ភាគីនីមួយៗដឹងថានាងគួរតែបដិសេធ មិននិយាយនៅពេលដែលភាគីម្ខាងទៀតកំពុងនិយាយអ្វីមួយ។
- **ទីបួន៖** ភាគីនីមួយៗដឹងថាការសន្ទនាគួរតែជាប្រអប់ អ្នកទាំងពីរគួរតែមានឱកាសនិយាយអំពីបញ្ហា។
- **ទីប្រាំ៖** ពួកគេប្រើប្រាស់ពាក្យស្និទ្ធស្នាលខ្លះមុខពេលចាកចេញ។

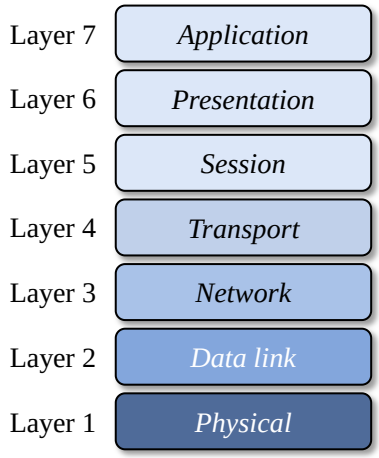
យើងអាចមើលឃើញថាពិធីការដែលប្រើដោយ Maria និង Ann ខុសពីការប្រាស្រ័យទាក់ទងរវាងសាស្ត្រាចារ្យ និងសិស្សនៅក្នុងសាលបង្រៀនមួយ។ ការទំនាក់ទំនងនៅក្នុងករណីទីពីរគឺភាគច្រើន monolog សាស្ត្រាចារ្យនិយាយភាគច្រើន លុះត្រាតែសិស្សមានសំណួរ ស្ថានភាពដែលពិធីការកំណត់ថានាងគួរលើកដៃឡើង ហើយរង់ចាំការអនុញ្ញាតនិយាយ ក្នុងករណីនេះ ការ

ទំនាក់ទំនងជាធម្មតាមានលក្ខណៈផ្លូវការ និងមានកម្រិតចំពោះមុខវិជ្ជាដែលបានបង្រៀន។

៥.២ ម៉ូដែល Network Layer OSI ៧

នៅពេលនិយាយអំពីអ៊ីនធឺណិត ទោះបីជាមនុស្សគ្រប់គ្នានិយាយអំពីឈុតពិធីការ TCP/IP ក៏ដោយ ឈុតនេះមិនមែនជាឈុតតែមួយនៃពិធីការដែលបានកំណត់នោះទេ។ ត្រូវបានបង្កើតឡើងក្នុង ១៩៤៧ អង្គការអន្តរជាតិសម្រាប់ស្តង់ដារនីយកម្ម (ISO) គឺជាស្ថាប័នអន្តរជាតិមួយដែលទទួលស្គាល់កិច្ចព្រមព្រៀងទូទាំងពិភពលោកស្តីពីស្តង់ដារអន្តរជាតិហើយស្ទើរតែ ៣/៤ នៃបណ្តាប្រទេសនៅលើពិភពលោកត្រូវបានតំណាងនៅក្នុង ISO ។ ស្តង់ដារ ISO ដែលគ្របដណ្តប់គ្រប់ទិដ្ឋភាពទាំងអស់នៃទំនាក់ទំនងបណ្តាញគឺជាគំរូ OSI វាត្រូវបានណែនាំជាលើកដំបូងនៅចុងទសវត្សរ៍ឆ្នាំ ១៩៧០ ។

ប្រព័ន្ធបើកទូលាយគឺជាសំណុំនៃពិធីការដែលអនុញ្ញាតឱ្យប្រព័ន្ធទាំងពីរទំនាក់ទំនងដោយមិនគិតពីស្ថាបត្យកម្មមូលដ្ឋានរបស់វា គំរូ OSI មានគោលបំណងបង្ហាញពីរបៀបជួយសម្រួលទំនាក់ទំនងរវាងប្រព័ន្ធផ្សេងៗគ្នា ដោយមិនចាំបាច់មានការផ្លាស់ប្តូរផ្នែករឹង និងផ្នែកទន់ ជាមូលដ្ឋាន។ គំរូ OSI មិនមែនជាពិធីការទេ ប៉ុន្តែជាគំរូសម្រាប់ការយល់ដឹង និងរចនាស្ថាបត្យកម្មបណ្តាញដែលអាចបត់បែនបាន រឹងមាំ និងអាចធ្វើអន្តរកម្មបាន គំរូ OSI មានបំណងជាមូលដ្ឋានសម្រាប់បង្កើតពិធីការនៅក្នុងជង់ OSI



រូបភាព ៥.២ ម៉ូដែលNetwork Layer OSI ៧

- **Physical Layer ៖** គឺជាស្រទាប់ទាបបំផុតនៅក្នុងគំរូ OSI វាទំនួលខុសត្រូវចម្បងរបស់វារួមមានការផ្សព្វផ្សាយពិតប្រាកដនៃប៊ីតទិន្នន័យដែលមិនមានរចនាសម្ព័ន្ធ (0's និង 1's) នៅទូទាំងបណ្តាញ ពី Physical Layer នៃឧបករណ៍បញ្ជូនទៅកាន់ Physical Layer នៃឧបករណ៍ទទួល។ Physical Layer មានព័ត៌មានជាទម្រង់ប៊ីត វាបញ្ជូនប៊ីតនីមួយៗពីថ្នាំងមួយទៅថ្នាំងបន្ទាប់ប្រព័ន្ធ

ផ្សព្វផ្សាយបញ្ជូនដែលកំណត់ដោយស្រទាប់រូបវន្តរួមមាន ខ្សែលោហៈធាតុ ខ្សែកាបអុបទិក និងរលកវិទ្យុឥតខ្សែ។

- Physical Layer **រួមបញ្ចូល**
    - **ការធ្វើសមកាលកម្មប៊ីត៖** Physical Layerផ្តល់នូវការធ្វើសមកាលកម្មប៊ីតនៃប៊ីតដោយផ្តល់នាឡិកា។ នាឡិកានេះគ្រប់គ្រងអ្នកផ្ញើ និងអ្នកទទួល ដោយផ្តល់នូវការធ្វើសមកាលកម្មនៅកម្រិតប៊ីត។
    - **ការគ្រប់គ្រងអត្រាប៊ីត៖** Physical Layer កំណត់អត្រាបញ្ជូនចំនួនប៊ីតដែលបានផ្ញើក្នុងមួយវិនាទី។
    - **បណ្តាញ Physical Layer ៖**បញ្ជាក់ពីរបៀបដែលឧបករណ៍ផ្សេងគ្នាត្រូវបានរៀបចំ នៅក្នុងបណ្តាញ (Bus, Ring, Star, និងTree Topology)។
    - **របៀបបញ្ជូន៖** Physical Layerពិនិត្យមើលថាតើការបញ្ជូនគឺសាមញ្ញ ពាក់កណ្តាលពីរ ឬពេញពីរជាន់ វាកំណត់ពីរបៀបដែលទិន្នន័យហូររវាងឧបករណ៍ដែលបានតភ្ជាប់ទាំងពីរ។
- Data Link Layer ៖ គឺជាស្រទាប់ទីពីរនៃគំរូ OSI Data Link Layer ផ្តល់នូវការប្រាស្រ័យទាក់ទងដោយគ្មានកំហុសឆ្លងកាត់តំណភ្ជាប់ជាក់ស្តែងដែលភ្ជាប់ថ្នាំងចម្បង និងបន្ទាប់បន្សំនៅក្នុងបណ្តាញមួយវាផ្តល់នូវការបញ្ជូនទៅកាន់ការបញ្ជូនបន្ត។ វាខ្ចប់ទិន្នន័យពីស្រទាប់រូបវន្តទៅជាក្រុមដែលហៅថាប្លុក Data Link Layer ផ្តល់នូវស៊ុមចុងក្រោយនៃសញ្ញាព័ត៌មាន និងឧបករណ៍ធ្វើសមកាលកម្មសម្រាប់លំហូរទិន្នន័យតាមលំដាប់រវាងថ្នាំង។
    - **ស៊ុម៖** បំបែកសារចូលទៅក្នុងស៊ុមហើយផ្ញើស៊ុមទៅជាសារ។
    - **ការដោះស្រាយកំហុស៖** ប្រើសម្រាប់ បាតជើង(soles) ស៊ុមខូច បាត់បង់ និងស្ទួន។
    - **ការគ្រប់គ្រងលំហូរ៖** វារក្សាឧបករណ៍បញ្ជូនលឿនពីការលើសច្រើនហួសកម្រិតធ្វើឱ្យអ្នកទទួលយឺត។
    - **ការគ្រប់គ្រងការចូលដំណើរការ៖** នៅក្នុងការគ្រប់គ្រងការចូលប្រើ ប្រសិនបើម៉ាស៊ីនជាច្រើនប្រើឧបករណ៍ផ្ទុកនៅពេលដែលឧបករណ៍ជាច្រើនចែករំលែកបណ្តាញទំនាក់ទំនងតែមួយ ស្រទាប់រង MAC នៃData Link Layerជួយកំណត់ថាតើឧបករណ៍មួយណាមានការគ្រប់គ្រងលើបទនៅពេលណាមួយ។
- Network Layer ៖ ផ្តល់សេចក្តីលម្អិតដែលអនុញ្ញាតឱ្យទិន្នន័យត្រូវបានបញ្ជូនរវាងឧបករណ៍នៅក្នុងបរិស្ថានដោយប្រើបណ្តាញច្រើន បណ្តាញរង ឬទាំងពីរ។ សមាសធាតុបណ្តាញដែលដំណើរការនៅ Network Layer រួមមានរ៉ោតទ័រ និងកម្មវិធីរបស់ពួកគេ វាកំណត់ការកំណត់រចនាសម្ព័ន្ធបណ្តាញណាដែលសមស្របបំផុតសម្រាប់មុខងារដែលផ្តល់ដោយការគ្រប់គ្រងបណ្តាញនិងអាសយដ្ឋាន និងទិន្នន័យផ្លូវក្នុងបណ្តាញដោយបង្កើត ថែទាំ និងបញ្ចប់ឧបករណ៍ភ្ជាប់រវាងពួកវា ផ្តល់ឱ្យស្រទាប់ខាងលើនៃឋានានុក្រមដោយឯករាជ្យពីការបញ្ជូនទិន្នន័យ និងបច្ចេកវិជ្ជាប្តូរ ដែលប្រើដើម្បីភ្ជាប់ប្រព័ន្ធ។ វាក៏ផ្តល់នូវអាសយដ្ឋានបណ្តាញប្រភព និងទិសដៅ ព័ត៌មានបណ្តាញរង

និងអាសយដ្ឋានថ្នាំងប្រភព និងទិសដៅផងដែរ នៅក្នុងនេះបណ្តាញត្រូវបានបែងចែកទៅជាបណ្តាញរង បំបែកដោយ រ៉ោតទ័រ។

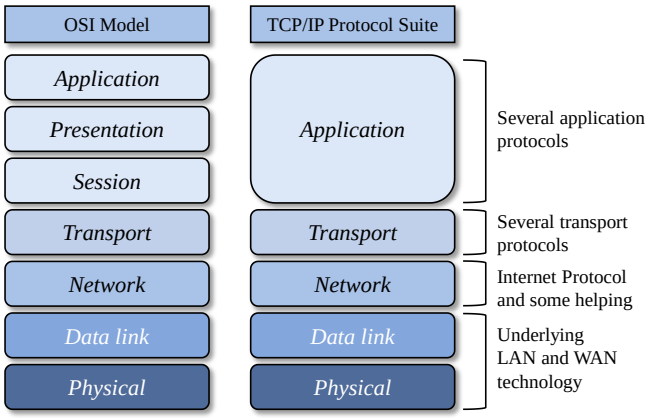
- **Transport Layer** គឺជា Transport Layer គ្រប់គ្រង និងធានានូវភាពត្រឹមត្រូវពីចុងដល់ចុងនៃសារទិន្នន័យដែលត្រូវបានផ្សព្វផ្សាយតាមរយៈបណ្តាញរវាងឧបករណ៍ពីរ ដោយផ្តល់នូវការផ្ទេរទិន្នន័យប្រកបដោយតម្លាភាព និងគួរឱ្យទុកចិត្តរវាងចំណុចបញ្ចប់នៃបណ្តាញ។ ទំនួលខុសត្រូវនៃ Transport Layer ៖
    - **ការបែងចែក និងការប្រមូលផ្តុំឡើងវិញ៖** សារមួយត្រូវបានបែងចែកទៅជាបំណែកតូចៗ ហើយប្រមូលផ្តុំសារឡើងវិញឱ្យបានត្រឹមត្រូវនៅពេលមកដល់គោលដៅ។
    - **ភាពជឿជាក់៖** វាធានាថាកញ្ចប់មកដល់គោលដៅរបស់ពួកគេ ប្រមូលផ្តុំសារដែលមិនមានការបញ្ជាទិញឡើងវិញ។
    - **ការសម្រេចចិត្តសេវាកម្ម៖** វាត្រូវបានប្រើដើម្បីពិនិត្យមើលប្រភេទសេវាកម្មណាដែលផ្តល់នូវកំហុសដោយគ្មានកំហុសពីចំណុចមួយទៅចំណុច ទិន្នន័យក្រាម ជាដើម។
    - **ការគូសផែនទី ៖** វាកំណត់ថាសារណាមួយជាកម្មសិទ្ធិរបស់ការតភ្ជាប់។
    - **ការដាក់ឈ្មោះ៖** វាត្រូវតែត្រូវបានបកប្រែទៅជាអាសយដ្ឋានខាងក្នុងនិងផ្លូវផ្ទៃថ្នាំង XYZ
    - **ការគ្រប់គ្រងលំហូរ ៖** វារក្សាឧបករណ៍បញ្ជូនលឿន។
    - **ការគ្រប់គ្រងកំហុស៖** បញ្ជូនផ្នែកដែលខូចឡើងវិញ។
- **Session Layer** ៖ បង្កើតបណ្តាញទំនាក់ទំនងរវាងឧបករណ៍ វាទទួលខុសត្រូវចំពោះការបើកសម័យ ដោយធានាថាពួកគេនៅតែបើកចំហ និងមានមុខងារខណៈពេលដែលទិន្នន័យកំពុងត្រូវបានផ្ទេរ និងបិទសម័យ នៅពេលទំនាក់ទំនងបញ្ចប់។ Session Layer ក៏អាចកំណត់ចំណុចត្រួតពិនិត្យនៅក្នុងកំឡុងពេលផ្ទេរទិន្នន័យផងដែរ ប្រសិនបើវគ្គមួយត្រូវបានរំខាន ឧបករណ៍អាចបន្តការផ្ទេរទិន្នន័យពីចំណុចត្រួតពិនិត្យចុងក្រោយ។ Session Layer គឺទទួលខុសត្រូវចំពោះភាពអាចរកបាននៃបណ្តាញសម្រាប់ការផ្ទុកទិន្នន័យ និងសមត្ថភាពដំណើរការវាផ្តល់នូវធាតុតភ្ជាប់ឡូជីខលនៅApplication Layer។ ទំនួលខុសត្រូវនៃ Session Layer ៖
    - ដំណើរការចូល និងបិទបណ្តាញ
    - ការធ្វើឱ្យធ្លាត់ម្នុកប្រើប្រាស់
    - កំណត់ប្រភេទនៃប្រអប់ដែលអាចប្រើបាន សាមញ្ញ ពាក់កណ្តាលពីរ និងពេញពីរជាន់
    - ការធ្វើសមកាលកម្មនៃលំហូរទិន្នន័យសម្រាប់គោលបំណងសង្គ្រោះ
    - ការបង្កើតឯកតាប្រអប់ និងអង្គភាពសកម្មភាព
- **Presentation Layer** ៖ រៀបចំទិន្នន័យសម្រាប់ស្រទាប់ខាងលើ ឬកម្មវិធីរបស់វាហើយវាកំណត់ពីរបៀបដែលឧបករណ៍ពីរគួរអ៊ិនកូដ អ៊ិនគ្រីប និងបំណែនទិន្នន័យ។
    - Presentation Layer ទទួលបានទិន្នន័យដែលបានបញ្ជូនដោយApplication Layer ហើយរៀបចំវាសម្រាប់ការបញ្ជូនតាម Session Layer

- វាបញ្ជាក់ពីរបៀបដែលកម្មវិធីអ្នកប្រើប្រាស់ចុងក្រោយគួរធ្វើទ្រង់ទ្រាយទិន្នន័យ
- ស្រទាប់នេះផ្តល់នូវការបកប្រែរវាងតំណាងមូលដ្ឋាននៃទិន្នន័យ និងតំណាងនៃទិន្នន័យដែលនឹងត្រូវបានប្រើសម្រាប់ការផ្ទេររវាងអ្នកប្រើប្រាស់ចុងក្រោយលទ្ធផលនៃការអ៊ិនគ្រីបការបង្ហាប់ ទិន្នន័យ និងស្តានីយនិម្មិត គឺជាឧទាហរណ៍នៃសេវាកម្មបកប្រែ។

- **Application Layer ៖** គឺជាស្រទាប់កំពូលបំផុតនៅក្នុងគំរូ OSI ហើយដើរតួជាអ្នកគ្រប់គ្រងទូទៅនៃបណ្តាញដោយផ្តល់នូវការចូលទៅកាន់បរិស្ថាន OSI ។ ស្រទាប់នេះផ្តល់សេវាព័ត៌មានចែកចាយ និងគ្រប់គ្រងលំដាប់នៃសកម្មភាពនៅក្នុងកម្មវិធីមួយ និងលំដាប់នៃព្រឹត្តិការណ៍រវាងកម្មវិធីកុំព្យូទ័រ និងអ្នកប្រើប្រាស់កម្មវិធី វាទាក់ទងដោយផ្ទាល់ជាមួយកម្មវិធីកម្មវិធីរបស់អ្នកប្រើ។ Application Layer ប្រើប្រាស់ HTTP, FTP, POP, SMTP និង DNS protocols ដែលអនុញ្ញាតឱ្យកម្មវិធីផ្ញើ និងទទួលព័ត៌មាន និងបង្ហាញទិន្នន័យដ៏មានអត្ថន័យដល់អ្នកប្រើប្រាស់។

៥.៣ ពិធីការ TCP/IP

TCP/IP គឺជាឈុតបួនស្រទាប់នៃពិធីការទំនាក់ទំនង វាត្រូវបានបង្កើតឡើងដោយ DoD (នាយកដ្ឋានការពារជាតិ) ក្នុងទសវត្សរ៍ឆ្នាំ ១៩៦០ ត្រូវបានដាក់ឈ្មោះតាមពិធីការសំខាន់ពីរដែលប្រើក្នុងគំរូគឺ TCP និង IP ។ TCP តំណាងឱ្យពិធីសារត្រួតពិនិត្យការបញ្ជូន ហើយ IP តំណាងឱ្យពិធីការអ៊ីនធឺណិត។ ឥឡូវនេះយើងដឹងអំពីការបញ្ឈប់ពិធីការ និងការទំនាក់ទំនងឡូជីខលរវាងស្រទាប់នៅក្នុងសេណារីយ៉ូទីពីររបស់យើង យើងអាចណែនាំ TCP/IP (ពិធីការការត្រួតពិនិត្យការបញ្ជូន/ពិធីការអ៊ីនធឺណិត)។ TCP/IP គឺជាឈុតពិធីការ (សំណុំនៃពិធីការដែលរៀបចំក្នុងស្រទាប់ផ្សេងៗគ្នា) ដែលប្រើនៅលើអ៊ីនធឺណិតសព្វថ្ងៃនេះ។ វាគឺជាពិធីការតាមឋានានុក្រមដែលរួមមានម៉ូឌុលអន្តរកម្ម ដែលនីមួយៗផ្តល់មុខងារជាក់លាក់។ ពាក្យឋានានុក្រមមានន័យថាពិធីការកម្រិតខាងលើនីមួយៗត្រូវបានគាំទ្រដោយសេវាកម្មដែលផ្តល់ដោយពិធីការកម្រិតមួយ ឬកម្រិតទាប។ ឈុតពិធីការ TCP/IP ដើមត្រូវបានកំណត់ថាជាស្រទាប់ផ្នែកទន់ចំនួនបួនដែលបង្កើតឡើងនៅលើផ្នែករឹង។ ទោះជាយ៉ាងណាក៏ដោយសព្វថ្ងៃនេះ TCP/IP ត្រូវបានគេចាត់ទុកថាជាគំរូប្រាំស្រទាប់នៅពេលយើងប្រៀបធៀបម៉ូដែលទាំងពីរ យើងឃើញថាស្រទាប់ពីរ Session Layer និង Presentation Layer ត្រូវបានបាត់ពីឈុតពិធីការ TCP/IP ។ ស្រទាប់ទាំងពីរនេះមិនត្រូវបានបន្ថែមទៅឈុតពិធីការ TCP/IP ទេ បន្ទាប់ពីការបោះពុម្ពផ្សាយគំរូ OSI Application Layer នៅក្នុងឈុតជាធម្មតាត្រូវបានចាត់ទុកថាជាការរួមបញ្ចូលគ្នានៃស្រទាប់បីនៅក្នុងគំរូ OSI។



រូបភាព ៥.៣ ពិធីការ TCP/IP

ហេតុផលពីរត្រូវបានលើកឡើងសម្រាប់ការសម្រេចចិត្តនេះ។

- ទីមួយ៖ TCP/IP មានពិធីការ Session Layer ច្រើនជាងមួយ មុខងារមួយចំនួននៃ Session Layer មាននៅក្នុងពិធីការ Session Layer មួយចំនួន។
- ទីពីរ៖ Application Layer មិនមែនមានតែផ្នែកមួយនៃកម្មវិធីនោះទេ កម្មវិធីជាច្រើនអាចត្រូវបានបង្កើតឡើងនៅស្រទាប់នេះ។ ប្រសិនបើមុខងារមួយចំនួនដែលបានរៀបរាប់នៅក្នុងវគ្គ និងស្រទាប់បទបង្ហាញគឺត្រូវការសម្រាប់កម្មវិធីជាក់លាក់មួយ ពួកគេអាចបញ្ចូលទៅក្នុងការបង្កើតកម្មវិធីនោះ។

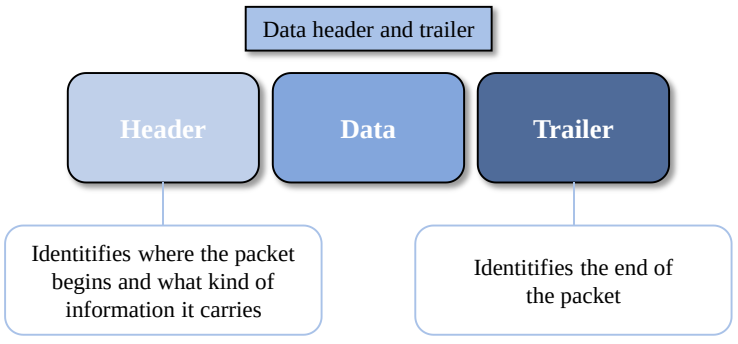
- **Physical Layer និង Data Link Layer៖** ស្រទាប់ទាបបំផុតទាក់ទងនឹងការបញ្ជូនទិន្នន័យ TCP/IP មិនកំណត់យ៉ាងច្បាស់នូវពិធីការណាមួយនៅទីនេះទេ ប៉ុន្តែគាំទ្រពិធីការស្តង់ដារ
- **Network Layer ៖** វាកំណត់ពិធីការសម្រាប់ការបញ្ជូនទិន្នន័យឡើងខ្លួនតាមបណ្តាញ ពិធីការចម្បងនៅក្នុងស្រទាប់នេះគឺ ពិធីការអ៊ីនធឺណិត (IP) ដែលត្រូវបានគាំទ្រដោយពិធីការ ICMP, IGMP, RARP និង ARP ។
- **Session Layer ៖** វាទទួលខុសត្រូវចំពោះការចែកចាយទិន្នន័យពីចុងដល់ចុងដោយគ្មានកំហុស ពិធីសារត្រួតពិនិត្យការបញ្ជូន (TCP) និង ពិធីការ Datagram អ្នកប្រើប្រាស់ (UDP) គឺជាពិធីការ។
- **Application Layer ៖** នេះគឺជាស្រទាប់កំពូលបំផុត និងកំណត់ចំណុចប្រទាក់នៃកម្មវិធីម៉ាស៊ីនជាមួយសេវាកម្ម Transport Layer ស្រទាប់នេះរួមបញ្ចូលពិធីការកម្រិតខ្ពស់ទាំងអស់ដូចជា Telnet, DNS, HTTP, FTP, SMTP ។

៥.៤ Encapsulations និង Decapsulations

Encapsulation គឺជាការបន្ថែមព័ត៌មានទៅកញ្ចប់ព័ត៌មាននៅពេលវាធ្វើដំណើរទៅកាន់គោលដៅរបស់វា។ Decapsulation បញ្ច្រាសដំណើរការដោយយកព័ត៌មានចេញ ដើម្បីឱ្យឧបករណ៍គោលដៅអាចអានទិន្នន័យដើមបាន នៅក្នុងដំណើរការ encapsulation កុំព្យូទ័រប្រភពបញ្ជូនកញ្ចប់ព័ត៌មានពី ស្រទាប់ទី៧ Application Layer, ស្រទាប់ទី១ Physical Layer ការវេចខ្ចប់ទិន្នន័យចាប់ផ្តើមនៅពេលដែលកញ្ចប់ព័ត៌មានឈានដល់ស្រទាប់ទី៤ ដែលជា Session Layer។ បន្ទាប់ពីនោះ ស្រទាប់ដែលនៅសេសសល់បន្ថែមព័ត៌មានដែលត្រូវគ្នាទៅកញ្ចប់ព័ត៌មាន ដែលអនុញ្ញាតឱ្យវាធ្វើដំណើរតាមប្រព័ន្ធ។ Decapsulation ផ្លាស់ទីក្នុងលក្ខណៈបញ្ច្រាសពីស្រទាប់ទី១ ទៅស្រទាប់ទី៧ នៅក្នុងគំរូ OSI នៅពេលដែលកញ្ចប់ព័ត៌មានធ្វើដំណើរទៅកាន់កុំព្យូទ័រទទួល។

៥.៤.១ Encapsulations

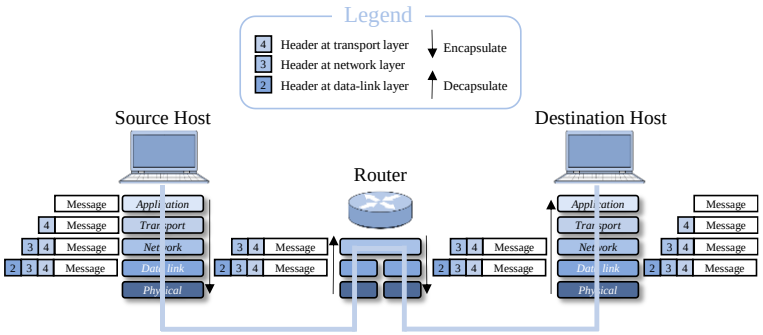
Encapsulation សម្គាល់កន្លែងដែលកញ្ចប់ព័ត៌មាន ឬឯកតាទិន្នន័យចាប់ផ្តើម និងបញ្ចប់។ ផ្នែកចាប់ផ្តើមនៃកញ្ចប់ព័ត៌មានត្រូវបានគេហៅថា បឋមកថា ហើយចុងបញ្ចប់ត្រូវបានគេហៅថា ឈុតខ្លី។ ទិន្នន័យរវាងបឋមកថា និងឈុតខ្លី។ ជួនកាលត្រូវបានគេហៅថាជាបន្ទុក។ បឋមកថានៃកញ្ចប់ព័ត៌មានផ្ទុកព័ត៌មាននៅក្នុងបៃពីរបីដំបូងរបស់វា ដើម្បីសម្គាល់កន្លែងដែលកញ្ចប់ព័ត៌មានចាប់ផ្តើម និងដើម្បីកំណត់ប្រភេទព័ត៌មានដែលវាមានស្រទាប់ផ្សេងៗគ្នានៅក្នុងប្រព័ន្ធកុំព្យូទ័ររួមចំណែកដល់បឋមកថាកញ្ចប់ព័ត៌មាន នៅពេលដែលកញ្ចប់ព័ត៌មានធ្វើដំណើរពីប្រភពរបស់វាទៅកាន់គោលដៅមួយ។ ព័ត៌មានបឋមកថាប្រែប្រួលអាស្រ័យលើពិធីការណាមួយដែលត្រូវប្រើ ដោយសារពិធីការនីមួយៗមានទម្រង់ដែលបានកំណត់។ ឈុតខ្លីៗនៃកញ្ចប់ព័ត៌មានបង្ហាញទៅកាន់ឧបករណ៍ទទួលថាវាបានឈានដល់ចុងបញ្ចប់នៃកញ្ចប់ព័ត៌មានជារឿយៗវាមានតម្លៃពិនិត្យកំហុសដែលឧបករណ៍ទទួលអាចប្រើដើម្បីបញ្ជាក់ថាវាបានទទួលកញ្ចប់ព័ត៌មានទាំងមូល។



រូបភាព ៥.៤ ទម្រង់កញ្ចប់ TCP/IP ពិធីការ

៥.៤.២ Decapsulation

Decapsulation ដកព័ត៌មានបឋមកថា និងឈុតខ្លីៗចេញពីកញ្ចប់ព័ត៌មាន នៅពេលវាផ្លាស់ទីទៅគោលដៅរបស់វា។ ឧបករណ៍គោលដៅទទួលទិន្នន័យក្នុងទម្រង់ដើមរបស់វាគោលគំនិតសំខាន់មួយក្នុងការរៀបចំពិធីការនៅលើអ៊ីនធឺណិតគឺ encapsulation និងdec-capsulations។



រូបភាព ៥.៥ Encapsulation

❖ Encapsulation នៅម៉ាស៊ីនប្រភព

ទិន្នន័យដែលត្រូវផ្លាស់ប្តូរនៅ Application Layer គឺសំដៅលើសារ។ សារជាធម្មតាមិនមានបឋមកថា ឬឈុតខ្លីៗទេ ប៉ុន្តែប្រសិនបើវាកើតឡើង យើងសំដៅលើសារទាំងមូលសារត្រូវបានបញ្ជូនទៅ Session Layer។

- **Session Layer** ៖ យកសារជាបន្ទុក បន្ទុកដែល Session Layer គួរយកចិត្តទុកដាក់។ វាបន្ថែមបឋមកថានៃ Session Layer ទៅការដឹកជញ្ជូន ដែលផ្ទុកនូវអត្តសញ្ញាណនៃកម្មវិធីកម្មវិធីប្រភព និងទិសដៅដែលចង់ទំនាក់ទំនង បូករួមទាំងព័ត៌មានបន្ថែមមួយចំនួនទៀតដែលត្រូវការសម្រាប់ការបញ្ជូនសារពីចុងដល់ចុង ដូចជាព័ត៌មានដែលត្រូវការសម្រាប់ លំហូរ ការគ្រប់គ្រងកំហុស ឬការគ្រប់គ្រងការកកស្ទះ។ លទ្ធផលគឺកញ្ចប់ដឹកជញ្ជូនដែលហៅថាផ្នែក (ក្នុង TCP) និង user datagram (ក្នុង UDP) ។ Session Layer បន្ទាប់មកបញ្ជូនកញ្ចប់ទៅ Network Layer។
- **Network Layer** ៖ យកកញ្ចប់ដឹកជញ្ជូនស្រទាប់ជាទិន្នន័យ ឬបន្ទុក ហើយបន្ថែមបឋមកថារបស់វាទៅនឹងបន្ទុក។ បឋមកថាមានអាសយដ្ឋានរបស់ម៉ាស៊ីនប្រភព និងទិសដៅ និងព័ត៌មានបន្ថែមមួយចំនួនទៀតដែលប្រើសម្រាប់ការត្រួតពិនិត្យកំហុសនៃបឋមកថា ព័ត៌មានការបែងចែក និងអ្វីៗផ្សេងទៀត។ លទ្ធផលគឺកញ្ចប់បណ្តាញស្រទាប់ដែលគេ

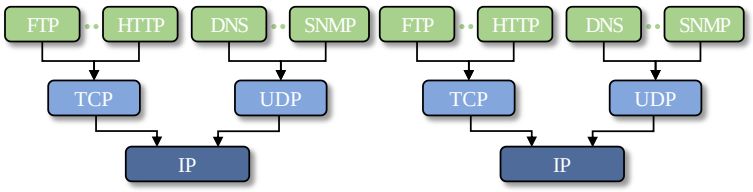
ហៅថា datagram បន្ទាប់មក Network Layer បញ្ជូនកញ្ចប់ព័ត៌មានទៅ Data Link Layer

- **Data Link Layer ៖** យកកញ្ចប់ព័ត៌មាន Network Layer ជាទិន្នន័យ ឬបន្ទុក ហើយបន្ថែមបឋមកថារបស់វា ដែលមានអាសយដ្ឋានស្រទាប់តំណរបស់ម៉ាស៊ីន ឬហៅបបន្ទាប់ (រ៉ោតទ័រ)។ លទ្ធផលគឺកញ្ចប់ Data Link Layer ដែលត្រូវបានគេហៅថាស៊ុមហើយស៊ុមត្រូវបានបញ្ជូនទៅ Physical Layer សម្រាប់ការបញ្ជូន។

❖ Decapsulation នៅឯម៉ាស៊ីនគោលដៅ

ស្រទាប់នីមួយៗគ្រាន់តែជាកញ្ចប់ decapsulation ដែលទទួលបានយកបន្ទុកហើយបញ្ជូនបន្ទុកទៅស្រទាប់ពិធីការខ្ពស់ជាងនេះ រហូតទាល់តែសារទៅដល់ Application Layer។ វាចាំបាច់ក្នុងការនិយាយថា decapsulation នៅក្នុងម៉ាស៊ីនពាក់ព័ន្ធនឹងការត្រួតពិនិត្យកំហុស។

៥.៤.៣ ពហុគុណ និងការបំប្លែងពហុផ្លាក



a. Multiplexing at source b. Demultiplexing at destination

រូបភាព ៥.៦ ពហុគុណ និងការបំប្លែងពហុផ្លាក

- **ពហុគុណ៖** ក្នុងករណីនេះមានន័យថា ពិធីការនៅស្រទាប់មួយអាចជាកញ្ចប់ encapsulate ពីស្រទាប់ពិធីការខ្ពស់បន្ទាប់ជាច្រើនម្តងមួយៗការបំប្លែងពហុផ្លាកមានន័យថាពិធីការមួយអាច decapsulate និងបញ្ជូនកញ្ចប់មួយទៅ ពិធីការស្រទាប់បន្ទាប់កម្រិតខ្ពស់ជាច្រើន (មួយក្នុងពេលតែមួយ)។
- **នៅក្នុងពហុគុណ៖** Transport Layer ទិន្នន័យត្រូវបានប្រមូលពីដំណើរការកម្មវិធីផ្សេងៗ។ ផ្នែកទាំងនេះមានលេខច្រកប្រភព លេខច្រកគោលដៅ ឯកសារបឋមកថា និងទិន្នន័យ។
- **ផ្នែកទាំងនេះ៖** ត្រូវបានបញ្ជូនទៅ Network Layer ដែលបន្ថែមអាសយដ្ឋាន IP ប្រភព និងទិសដៅដើម្បីទទួលបានទិន្នន័យក្រាប។

- **ការបំប្លែងពហុផ្លាក**៖ គឺជាការបញ្ជូនផ្នែកដែលទទួលបាន នៅផ្នែកអ្នកទទួលទៅកាន់ដំណើរការ Application Layer ត្រឹមត្រូវ។

ម៉ាស៊ីនគោលដៅទទួលបាន IP Datagrams នីមួយៗមានអាសយដ្ឋាន IP ប្រភព និងអាសយដ្ឋាន IP គោលដៅ។

- Datagrams នីមួយៗផ្ទុកផ្នែក Session Layer មួយ។
- ផ្នែកនីមួយៗមានលេខច្រកប្រភព និងទិសដៅ។
- ម៉ាស៊ីនគោលដៅប្រើអាសយដ្ឋាន IP និងលេខច្រកដើម្បីដឹកនាំផ្នែកទៅរន្ធដែលសមស្រប។

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះអ្នកបានសិក្សាអំពី៖

- **Physical Layer និង Data Link Layer ៖** ស្រទាប់ទាបបំផុតទាក់ទងនឹងការបញ្ជូនទិន្នន័យ។ TCP/IP មិនកំណត់យ៉ាងច្បាស់នូវពិធីការណាមួយនៅទីនេះទេ ប៉ុន្តែគាំទ្រពិធីការស្តង់ដារទាំងអស់។
- **Network Layer ៖** វាកំណត់ពិធីការសម្រាប់ការបញ្ជូនទិន្នន័យឡូជីខលតាមបណ្តាញ ពិធីការចម្បងនៅក្នុងស្រទាប់នេះគឺ ពិធីការអ៊ីនធឺណិត (IP) ហើយវាត្រូវបានគាំទ្រដោយពិធីការ ICMP, IGMP, RARP និង ARP ។
- **Transport Layer ៖** វាទទួលខុសត្រូវចំពោះការចែកចាយទិន្នន័យពីចុងដល់ចុងដោយគ្មានកំហុស។ ពិធីសារត្រួតពិនិត្យការបញ្ជូន (TCP) និង ពិធីការ Datagram អ្នកប្រើប្រាស់ (UDP) គឺជាពិធីការ។
- **Application Layer ៖** នេះគឺជាស្រទាប់កំពូលបំផុត និងកំណត់ចំណុចប្រទាក់នៃកម្មវិធីម៉ាស៊ីនជាមួយសេវាកម្ម Transport Layer ស្រទាប់នេះរួមបញ្ចូលពិធីការកម្រិតខ្ពស់ទាំងអស់ដូចជា Telnet, DNS, HTTP, FTP, SMTP ។
- **Encapsulation ៖** សម្គាល់កន្លែងដែលកញ្ចប់ព័ត៌មាន ឬឯកតាទិន្នន័យចាប់ផ្តើម និងបញ្ចប់ ផ្នែកចាប់ផ្តើមនៃកញ្ចប់ព័ត៌មានត្រូវបានគេហៅថា បឋមកថា ហើយចុងបញ្ចប់ត្រូវបានគេហៅថា ឈុតខ្លីទិន្នន័យរវាងបឋមកថា និងឈុតខ្លីៗ ជួនកាលត្រូវបានគេហៅថាជាបន្ទុក។
- **Decapsulation៖** ដកព័ត៌មានបឋមកថា និងឈុតខ្លីៗចេញពីកញ្ចប់ព័ត៌មាន នៅពេលវាផ្លាស់ទីទៅគោលដៅរបស់វា។ ឧបករណ៍គោលដៅទទួលទិន្នន័យក្នុងទម្រង់ដើមរបស់វា។
- **ពហុគុណ៖** Transport Layer ទិន្នន័យត្រូវបានប្រមូលពីដំណើរការកម្មវិធីផ្សេងៗ។ ផ្នែកទាំងនេះមានលេខច្រកប្រភព លេខច្រកគោលដៅ ឯកសារបឋមកថា និងទិន្នន័យ។
- **ការបំប្លែងពហុផ្លាក៖** បញ្ជូនផ្នែកដែលទទួលបាននៅផ្នែកអ្នកទទួលទៅដំណើរការស្រទាប់កម្មវិធីត្រឹមត្រូវ។

សំណួរ

១.តើ OSI ម៉ូដែលជាអ្វី?

២. តើពិធីការ TCP/IP ជាអ្វី?

៣. តើអ្វីជាភាពខុសគ្នារវាងពិធីការ OSI និង TCP/IP?

៤. តើអ្វីជា Encapsulation?

៥.តើអ្វីជា Decapsulation?

៦. តើអ្វីជាភាពខុសគ្នារវាង Encapsulations និង Decapsulations?

ការអនុវត្តន៍ទី៥

ឧបករណ៍បណ្តាញទំនាក់ទំនងបញ្ជូនទិន្នន័យដោយបញ្ជាក់ផ្លូវខ្លីបំផុត។ ចំនួននៃកញ្ចប់ព័ត៌មានដែលអាចដំណើរការបានគឺមានទំហំធំ ហើយល្បឿនបញ្ជូនត្រូវបានធ្វើឱ្យប្រសើរឡើងជាងមជ្ឈមណ្ឌលសម្រាប់ទំនាក់ទំនងតូចដែលជាឧបករណ៍ទំនាក់ទំនងដែលភ្ជាប់អង្គភាពបណ្តាញ។

ក. គោលបំណងនៃការអនុវត្តនេះ

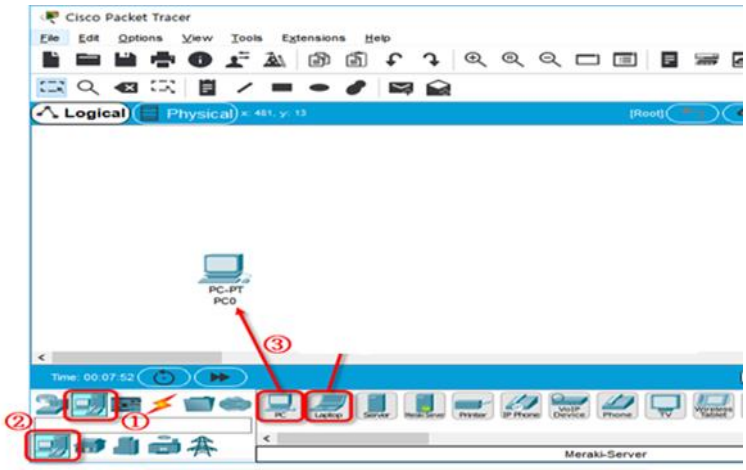
- ដើម្បីយល់ពីមុខងារ Switch។
- ដើម្បីធ្វើការកំណត់មូលដ្ឋាននៃSwitch។
- ដើម្បីធ្វើការកំណត់មូលដ្ឋាននៃ VLAN ។

ខ. តើ Switch នៅក្នុងបណ្តាញគឺជាអ្វី?

Switch គឺជាឧបករណ៍ទំនាក់ទំនងដែលភ្ជាប់ឯកតាបណ្តាញជាមួយនឹងកញ្ចប់ព័ត៌មានជាច្រើនដែលអាចដំណើរការបាន និងមានល្បឿនបញ្ជូនប្រសើរឡើងជាងមជ្ឈមណ្ឌលសម្រាប់ទំនាក់ទំនងខ្នាតតូច។ ជារឿយៗវាត្រូវបានគេហៅថា switching and a bridging hub, MAC bridge, switching hub, និង port switching hub ។ គោលបំណងនៃ Switch គឺស្រដៀងទៅនឹងមជ្ឈមណ្ឌលប៉ុន្តែ Switch ផ្តល់នូវល្បឿនបណ្តាញដែលប្រសើរឡើងយ៉ាងខ្លាំងនេះអាចទៅរួចព្រោះទិន្នន័យដែលបានផ្ញើ និងទទួលដោយកុំព្យូទ័រនីមួយៗត្រូវបានផ្ញើទៅតែកុំព្យូទ័រដែលត្រូវការទិន្នន័យប៉ុណ្ណោះ មិនមែនទៅកាន់កុំព្យូទ័រផ្សេងទៀតទាំងអស់ដូចជា hub នោះទេ។ ដូច្នេះ វាមិនងាយក្លាយជាឧបសគ្គដូចជាមជ្ឈមណ្ឌលនោះទេ ដោយសារ Switch ភាគច្រើនគាំទ្រការទំនាក់ទំនងវាផ្តល់នូវល្បឿនប្រសើរឡើងច្រើននៅពេលការបញ្ជូន និងការទទួលកើតឡើងក្នុងពេលដំណាលគ្នា។

គ. ការកំណត់ IP នៅក្នុង Packet Tracer

១.បន្ថែមកុំព្យូទ័រ

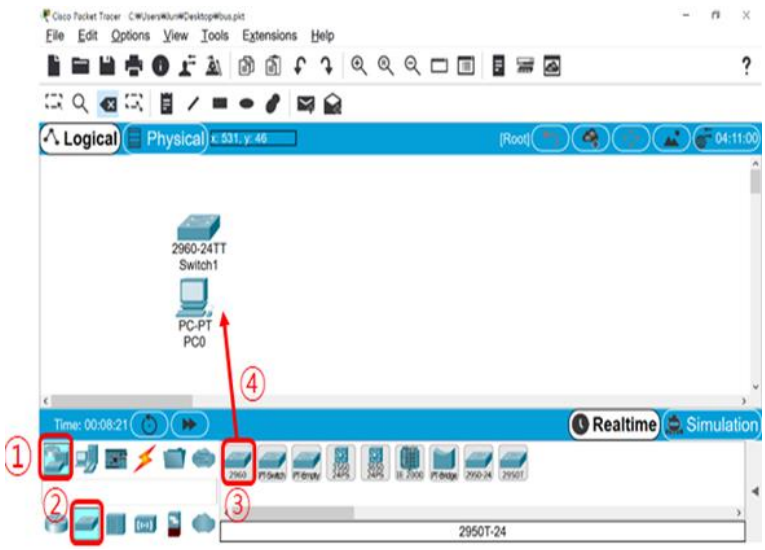


ក. ចុចលើ [ឧបករណ៍បញ្ចប់(End Devices)] → ជ្រើសរើស Desktop

ខ. ចុចលើ [ឧបករណ៍បញ្ចប់(End Devices)] → ជ្រើសរើស Laptop

គ បន្ទាប់មក .ចុចលើ 'PC' ឬLaptop ហើយអូសទម្លាក់លើផ្ទាំងកិច្ចការ

២.បន្ថែមSwitch

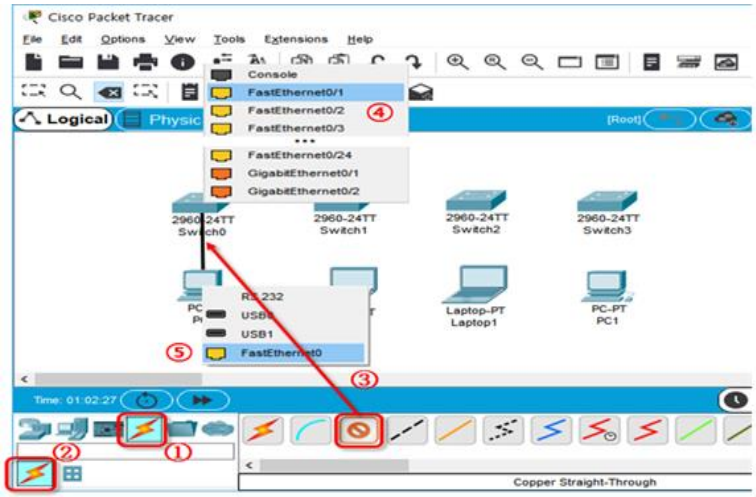


ក.ចុចលើ)ឧបករណ៍បញ្ចប់](Network Devices)

ខ. ជ្រើសរើសយក Switches(Model 2960)

គ. បន្ទាប់មក ចុចលើ ‘2960’ Switch ហើយអូសទម្លាក់លើផ្ទាំងកិច្ចការ

៣.បន្ថែមSwitch

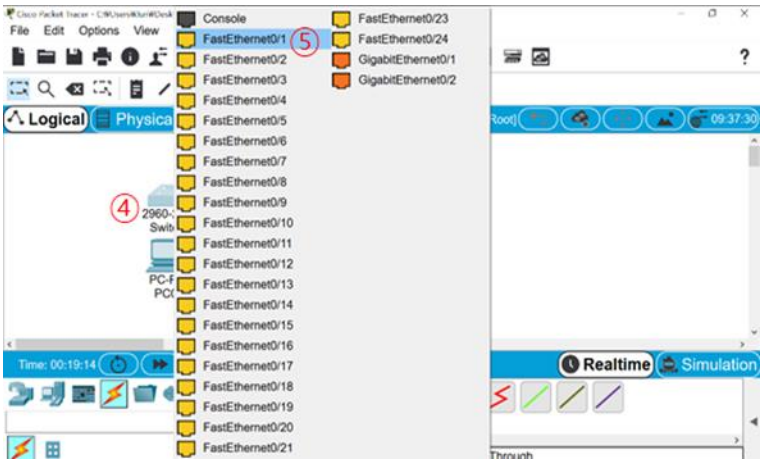


ក.ចុចលើ)ឧបករណ៍បញ្ជាប់]Connections)[

ខ. ជ្រើសរើសយក Copper Straight-Through

គ.ជ្រើសរើស ផតអ៊ីសូណេតដើម្បីភ្ជាប់Switch មួយទៅSwitchមួយ

៤. ភ្ជាប់បន្ថែមពី Switch មួយទៅ Switch មួយ



ក.ចុកលើឧបករណ៍កញ្ចាប់ (Network Device)

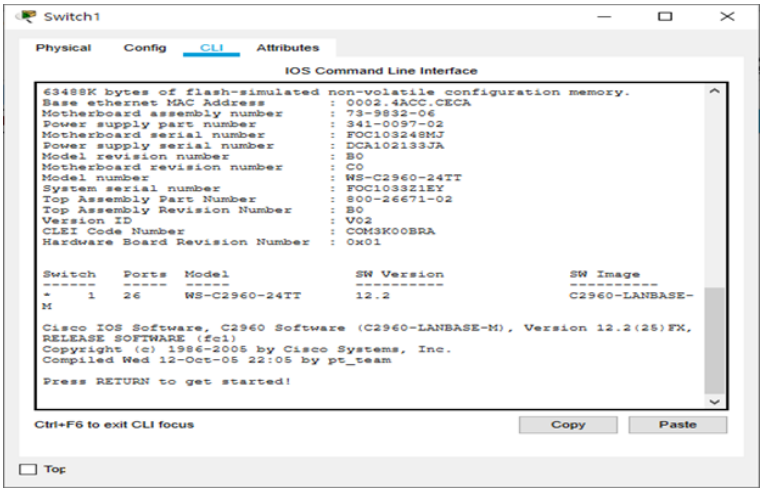
ខ.ជ្រើសរើស ផតអ៊ីសូណេត [FastEthernet0/1] ដើម្បីភ្ជាប់Switch

ឃ. តើ VLAN ជាអ្វី?

VLAN គឺជា Switch ដែលបែងចែកដោយឡូជីខល មិនមែនជាការបែងចែកឧបករណ៍រូបវន្តទេ។ VLANs ត្រូវបានបង្កើតឡើងដើម្បីការពារឧបករណ៍ដែលភ្ជាប់ទៅ Switch ពីការទទួល ឬបញ្ជូនព័ត៌មានដែលមិនចាំបាច់ ដើម្បីបង្កើនសុវត្ថិភាព និងការទំនាក់ទំនងនៃឧបករណ៍ដែលបានភ្ជាប់។ បណ្តាញស្រទាប់ទី២ តែមួយអាចត្រូវបានបែងចែកដើម្បីបង្កើតដែនផ្សព្វផ្សាយផ្សេងៗគ្នាជាច្រើននៅក្នុងបណ្តាញកុំព្យូទ័រ ដូច្នេះកញ្ចប់ព័ត៌មានអាចធ្វើដំណើរបានតែរវាងរ៉ោតទ័រមួយ ឬច្រើនប៉ុណ្ណោះ ដែនបែបនេះត្រូវបានគេហៅថា LAN និម្មិត ហើយត្រូវបានបញ្ជាក់ផងដែរថាជាបណ្តាញតំបន់មូលដ្ឋាននិម្មិត LAN និម្មិត ឬសាមញ្ញ VLAN ។

ង. ការកំណត់រចនាសម្ព័ន្ធ VLAN

១.ការកំណត់ Switch VLAN



ក.ចុចលើ Switch

ខ. ចុចលើពាក្យ CLI

ង១.បង្កើតលេខជាគូទៅ VLAN

```
Switch>en
Switch#conf t
Switch(config)#vlan[number]
Switch(config-vlan)#name [name]
Switch(config-vlan)#exit
```

១២.កំណត់លេខច្រកទៅជាកម្មសិទ្ធិរបស់ VLAN ហើយប្តូរការកំណត់

```
Switch(config)#interfacefa[n]/[n]
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access [number]
Switch(config-if)#exit
```

ឧទាហរណ៍) ការកំណត់រចនាសម្ព័ន្ធ VLAN

```
Switch>en
Switch#conf t
Switch(config)#vlan 10
Switch(config-vlan)#name VLAN-10
Switch(config-vlan)#exit
Switch(config)#vlan 20
Switch(config-vlan)#name VLAN-20
Switch(config-vlan)#exit
Switch(config)#vlan 30
Switch(config-vlan)#name VLAN-30
Switch(config-vlan)#exit
Switch(config)#interface fa0/2
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 10
Switch(config-if)#exit
Switch(config)#interface fa0/3
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 20
Switch(config-if)#exit
Switch(config)#interface fa0/4
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 30
Switch(config-if)#exit
```

ច. សេចក្តីអនុវត្តន៍

Switch គឺជាឧបករណ៍ផ្នែករឹងបណ្តាញដែលអនុញ្ញាតឱ្យទំនាក់ទំនងរវាងឧបករណ៍នៅក្នុងបណ្តាញ ដូចជាបណ្តាញផ្ទះក្នុងស្រុក។ ក្នុងនាមជាគំនិតពង្រីកនៃមជ្ឈមណ្ឌលមួយ មជ្ឈមណ្ឌលមួយផ្សាយកញ្ចប់ព័ត៌មានដែលបានបញ្ជូនពីឧបករណ៍មួយ ទៅឧបករណ៍ទាំងអស់ដែលភ្ជាប់ទៅមជ្ឈមណ្ឌល។ ផ្ទុយទៅវិញ Switch បញ្ជូនកញ្ចប់តែទៅកាន់ច្រកដែលនាំទៅដល់ឧបករណ៍ដែលបានកំណត់ថាជាអាសយដ្ឋានគោលដៅរបស់កញ្ចប់ព័ត៌មានប៉ុណ្ណោះ។ VLAN គឺជាបណ្តាញប្តូរដែលបែងចែកដោយតក្កវិជ្ជាជាមួយ។ វាមានសមត្ថភាពក្នុងការរៀបចំក្រុមការងារនៅក្នុងអង្គភាព VLAN ត្រូវបានកំណត់នៅលើ Switch មួយ ហើយការទំនាក់ទំនងអាចធ្វើទៅបានតែរវាងតំបន់ដែលមាន VLANs កំណត់។

ឃ.កិច្ចការស្រាវជ្រាវ

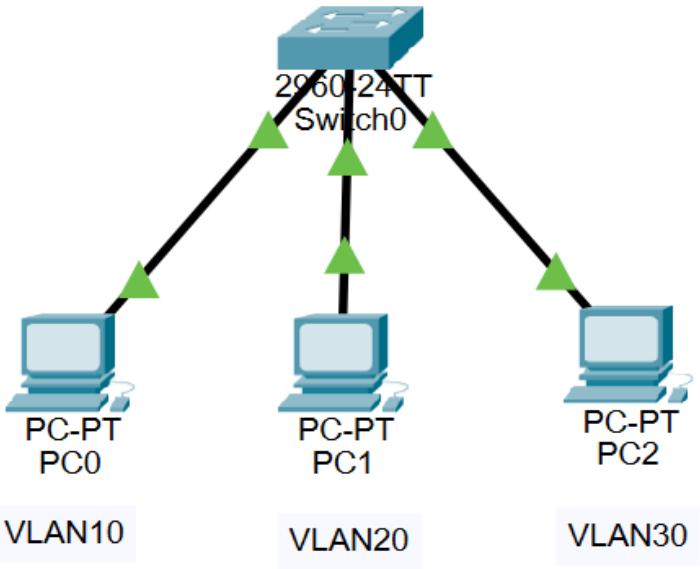
កិច្ចការទី១៖ កំណត់រចនាសម្ព័ន្ធបណ្តាញដូចខាងក្រោម ហើយដំឡើង VLANs នៅលើ Switch ៖

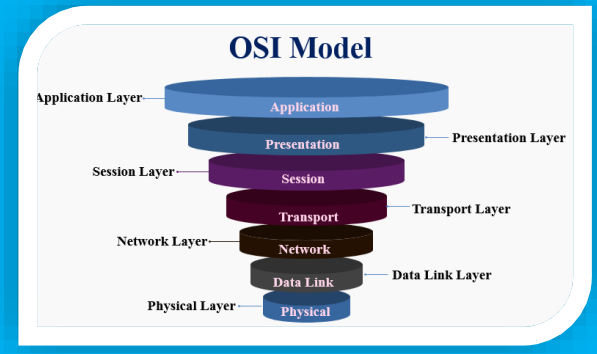
ក. ធ្វើការបង្កើតរចនាសម្ព័ន្ធដូចរូបខាងក្រោម

ខ. ដាក់ឈ្មោះ VLAN10, VLAN20, VLAN30 ដោយធ្វើការ Configuration

Port Fast Ethernet

- Fa0/1 សម្រាប់ VLAN10,
- Fa0/2 សម្រាប់ VLAN20,
- Fa0/3 សម្រាប់ VLAN30,





ជំពូកទី៦

Network Layer

ស្រទាប់បណ្តាញក៏អាចបែងចែកកញ្ចប់ព័ត៌មានធំ ៗ ទៅជាបំណែកតូច។ ប្រសិនបើកញ្ចប់ព័ត៌មានខ្ពស់ជាងស្រទាប់ភ្ជាប់ទិន្នន័យទូលំទូលាយបំផុតបណ្តាញប្រមូលផ្តុំបំណែកចូលទៅក្នុងកញ្ចប់ព័ត៌មាននៅចុងបញ្ចប់នៃការទទួលដូចជា រ៉ោតទ័រ និង ច្រកផ្លូវ ដើរតួក្នុងស្រទាប់បណ្តាញ។

- ស្រទាប់បណ្តាញគឺជាស្រទាប់ទីបីនៃគំរូ OSI ។
- វាគ្រប់គ្រងសំណើរសេវាកម្មពី Transport Layer និងបញ្ជូនបន្តសំណើរសេវាកម្មទៅ Data Link Layer
- ស្រទាប់បណ្តាញបកប្រែអាសយដ្ឋានឡូជីខលទៅជាអាសយដ្ឋានជាក់ស្តែង។
- វាកំណត់ផ្លូវពីប្រភពទៅកាន់គោលដៅ គ្រប់គ្រងបញ្ហាចរាចរណ៍ដូចជាការប្តូរ និងការកំណត់ផ្លូវ និងគ្រប់គ្រងការកកស្ទះនៃកញ្ចប់ទិន្នន័យ។
- តួនាទីសំខាន់នៃស្រទាប់បណ្តាញគឺដើម្បីផ្លាស់ទីកញ្ចប់ព័ត៌មានពីម៉ាស៊ីនប្រភពទៅកាន់ម៉ាស៊ីនទទួល។

ជំពូកទី៦ នេះ អ្នកនឹងរៀនអំពី៖

៦.១ ការណែនាំអំពី Network Layer

ស្រទាប់ទី៣ នៅក្នុងគំរូ OSI ត្រូវបានគេហៅថា Network Layer ហើយ Network Layer គឺគ្រប់គ្រងម៉ាស៊ីន និងអាសយដ្ឋានបណ្តាញ បណ្តាញរង និងជម្រើសដំណើរការអ៊ីនធឺណិត។ Network Layer ទទួលខុសត្រូវចំពោះការបញ្ជូនកញ្ចប់ព័ត៌មានពីប្រភពទៅកាន់ទិសដៅក្នុង ឬក្រៅបណ្តាញរង ហើយបណ្តាញរងពីរផ្សេងគ្នាអាចមានគ្រោងការណ៍អាសយដ្ឋានផ្សេងៗគ្នា ឬប្រភេទអាសយដ្ឋានដែលមិនត្រូវគ្នា។ វាដូចគ្នាជាមួយនឹងពិធីការ៖ បណ្តាញរងពីរផ្សេងគ្នាអាចដំណើរការលើពិធីការមិនឆបគ្នា Network Layer ទទួលខុសត្រូវក្នុងការបញ្ជូនកញ្ចប់ព័ត៌មានពីប្រភពទៅគោលដៅ និងគូសផែនទីគម្រោងអាសយដ្ឋាន និងពិធីការផ្សេងៗ។

៦.១.១ មុខងាររបស់ស្រទាប់ទី៣

ឧបករណ៍ដែលដំណើរការលើ Network Layer ផ្តោតជាសំខាន់លើការនាំផ្លូវ ការកំណត់ផ្លូវ អាចរួមបញ្ចូលកិច្ចការផ្សេងៗដែលមានគោលបំណងសម្រេចបាននូវគោលដៅតែមួយ។

ទាំងនេះអាចជាមុខងារសំខាន់របស់ស្រទាប់ទី៣៖

- អាសយដ្ឋានឧបករណ៍ និងបណ្តាញ
- បង្កើតតារាងនាំផ្លូវ ឬផ្លូវធ្វើដោយដៃ
- តម្រង់ជួរទិន្នន័យចូល និងចេញ ហើយបន្ទាប់មកបញ្ជូនបន្តពួកវាតាមកម្រិតគុណភាពនៃសេវាកម្មដែលបានកំណត់សម្រាប់កញ្ចប់ព័ត៌មានទាំងនោះ
- ដំណើរការអ៊ីនធឺណិតរវាងបណ្តាញរងពីរផ្សេងគ្នា
- ការបញ្ជូនកញ្ចប់ព័ត៌មានទៅកាន់គោលដៅរបស់ពួកគេជាមួយនឹងការខិតខំប្រឹងប្រែងដ៏ល្អបំផុត
- ផ្តល់នូវយន្តការតម្រង់ទិស និងការតភ្ជាប់តិច

៦.១.២ លក្ខណៈពិសេសនៃ Network Layer

ជាមួយនឹងមុខងារស្តង់ដាររបស់វាស្រទាប់ទី៣ អាចផ្តល់នូវមុខងារជាច្រើនដូចជា៖

- គុណភាពនៃការគ្រប់គ្រងសេវាកម្ម
- ការផ្ទុកតុល្យភាព និងការគ្រប់គ្រងតំណ
- សន្តិសុខសុវត្ថិភាពបណ្តាញ
- ទំនាក់ទំនងអន្តរកម្មនៃពិធីការ និងបណ្តាញរងផ្សេងគ្នាជាមួយគ្រោងការណ៍ផ្សេងគ្នា
- ការរចនាបណ្តាញឡូជីខលផ្សេងៗគ្នាលើការរចនាបណ្តាញរូបវន្ត
- VPN និងផ្លូវរូងក្រោមដីអាចត្រូវបានប្រើដើម្បីផ្តល់នូវការភ្ជាប់ជាក់លាក់ពីចុងដល់ចប់

៦.២ Network Layer នៅក្នុងគំរូ OSI

គំរូ Open Systems Interconnect (OSI) គឺជាក្របខ័ណ្ឌគោលគំនិតដែលពិពណ៌នាអំពីប្រព័ន្ធបណ្តាញ ឬទូរគមនាគមន៍ជាប្រាំពីរស្រទាប់ ដែលស្រទាប់នីមួយៗមានមុខងាររបស់វា។ ស្រទាប់ជួយឱ្យអ្នកជំនាញបណ្តាញមើលឃើញនូវអ្វីដែលកំពុងកើតឡើងនៅក្នុងបណ្តាញរបស់ពួកគេ ហើយអាចជួយអ្នកគ្រប់គ្រងបណ្តាញបង្រួមបញ្ហា (វាជាបញ្ហា Hardware ឬជាអ្វីមួយជាមួយកម្មវិធី?) ក៏ដូចជាអ្នក សរសេរកម្មវិធីកុំព្យូទ័រ (នៅពេលបង្កើតកម្មវិធី ដែលស្រទាប់ផ្សេងទៀតធ្វើ ត្រូវការធ្វើការជាមួយ) អ្នកលក់បច្ចេកវិទ្យាដែលលក់ផលិតផលថ្មីជាញឹកញាប់នឹងសំដៅទៅលើគំរូ OSI ដើម្បីជួយអតិថិជនឱ្យយល់ពីស្រទាប់ណាមួយដែលផលិតផលរបស់ពួកគេដំណើរការជាមួយ ឬថាតើវាដំណើរការឆ្លងកាត់។

៦.២.១ តើ OSI Model ជាអ្វី?

OSI Model គឺជាគំរូឡូជីខល និងគំនិតដែលកំណត់ការទំនាក់ទំនងបណ្តាញដែលប្រើដោយប្រព័ន្ធបើកចំហសម្រាប់ធ្វើទំនាក់ទំនងអន្តរកម្ម និងការប្រាស្រ័យទាក់ទងជាមួយប្រព័ន្ធផ្សេងទៀត។ Open System Interconnection (OSI Model) ក៏តំណាងឱ្យបណ្តាញឡូជីខល និងពិពណ៌នាយ៉ាងមានប្រសិទ្ធភាពអំពីការផ្ទេរកញ្ចប់ព័ត៌មានកុំព្យូទ័រដោយប្រើស្រទាប់ពិធីការផ្សេងៗ។

Layer	Name	Protocols
Layer 7	Application	SMTP, HTTP, FTP, POP3, SNMP
Layer 6	Presentation	MPEG, ASCH, SSL, TLS
Layer 5	Session	NetBIOS, SAP
Layer 4	Transport	TCP, UDP
Layer 3	Network	IPV5, IPV6, ICMP, IPSEC, ARP, MPLS.
Layer 2	Data Link	RAPA, PPP, Frame Relay, ATM, Fiber Cable, etc.
Layer 1	Physical	RS232, 100BaseTX, ISDN, 11.

រូបភាព ៦.១ Network Layer នៅក្នុងគំរូ OSI

៦.២.២ ប្រវត្តិនៃ OSI Model

- នៅចុងទស្សវត្សរ៍ឆ្នាំ ១៩៧0 ISO បានធ្វើកម្មវិធីមួយដើម្បីអភិវឌ្ឍស្តង់ដារទូទៅ និងវិធីសាស្ត្រនៃបណ្តាញ។

- នៅឆ្នាំ ១៩៧៣ ប្រព័ន្ធផ្លាស់ប្តូរកញ្ចប់ពិសោធន៍នៅចក្រភពអង់គ្លេសបានកំណត់តម្រូវការសម្រាប់កំណត់ពិធីការកម្រិតខ្ពស់។
- នៅឆ្នាំ ១៩៨៣ OSI Model ត្រូវបានបម្រុងទុកដំបូងដើម្បីជាការបញ្ជាក់លម្អិតនៃចំណុចប្រទាក់និម្មិត។
- នៅឆ្នាំ ១៩៨៤ ស្ថាបត្យកម្ម OSI ត្រូវបានអនុម័តជាផ្លូវការដោយ ISO ជាស្តង់ដារអន្តរជាតិ។

ក.គុណសម្បត្តិនៃ OSI Model

នេះគឺជាអត្ថប្រយោជន៍ និងគុណសម្បត្តិសំខាន់ៗនៃការប្រើប្រាស់ OSI Model៖

- វាជួយអ្នកក្នុងការធ្វើស្តង់ដារហ៊ាតទ័រ កុងតាក់ បន្ទះមេ និងផ្នែករឹងផ្សេងទៀត។
- កាត់បន្ថយភាពស្មុគស្មាញ និងធ្វើឱ្យចំណុចប្រទាក់ស្តង់ដារ
- សម្រួលវិស្វកម្មម៉ូឌុល
- អនុញ្ញាតឱ្យអ្នកធានាបាននូវបច្ចេកវិទ្យាអន្តរប្រតិបត្តិការ
- វាជួយអ្នកឱ្យពន្លឿនការវិវត្ត
- ពិធីការអាចត្រូវបានជំនួសដោយពិធីការថ្មីនៅពេលដែលបច្ចេកវិជ្ជាផ្លាស់ប្តូរ
- ផ្តល់ការគាំទ្រសម្រាប់សេវាកម្មតម្រង់ទិសការតភ្ជាប់ ក៏ដូចជាសេវាកម្មគ្មានការតភ្ជាប់
- វាជាគំរូស្តង់ដារក្នុងបណ្តាញកុំព្យូទ័រ
- គាំទ្រការតភ្ជាប់គ្មានការតភ្ជាប់ និងសេវាកម្មតម្រង់ទិស
- ផ្តល់ភាពបត់បែនក្នុងការសម្របខ្លួនទៅនឹងប្រភេទផ្សេងៗនៃពិធីការ

ខ.គុណវិបត្តិនៃ OSI Model

នេះគឺជាគុណវិបត្តិមួយចំនួននៃការប្រើប្រាស់ OSI Model៖

- ការបំពេញពិធីការគឺជាកិច្ចការដ៏ធុញទ្រាន់
- អ្នកអាចប្រើវាជាគំរូយោងប៉ុណ្ណោះ។
- មិនកំណត់ពិធីការជាក់លាក់ណាមួយឡើយ។
- នៅក្នុងគំរូ Network Layer OSI សេវាកម្មមួយចំនួនត្រូវបានចម្លងគ្នាក្នុងស្រទាប់ជាច្រើន ដូចជាស្រទាប់ដឹកជញ្ជូន និងតំណទិន្នន័យជាដើម។

៦.៣ សេវា Network Layer

Network Layer គឺជាស្រទាប់ទីបីនៅក្នុងគំរូ OSI នៃបណ្តាញកុំព្យូទ័រហើយមុខងារចម្បងរបស់វាគឺផ្ទេរកញ្ចប់បណ្តាញពីប្រភពទៅទិសដៅ។ វាពាក់ព័ន្ធទាំងម៉ាស៊ីនប្រភព និងម៉ាស៊ីនគោលដៅនៅពេលចាប់ផ្តើម វាទទួលយកកញ្ចប់ព័ត៌មានពីស្រទាប់ដឹកជញ្ជូន បញ្ចូលវាក្នុង datagram ហើយបន្ទាប់មកបញ្ជូនកញ្ចប់ព័ត៌មានទៅ Data Link Layer ដូច្នេះវាអាចត្រូវបានផ្ញើទៅអ្នកទទួល នៅគោលដៅ ទិន្នន័យក្រាមត្រូវបានរុំព័ទ្ធ ហើយកញ្ចប់ព័ត៌មានត្រូវបានស្រង់ចេញ និងបញ្ជូនទៅ Transport Layerដែលត្រូវគ្នា។

លក្ខណៈពិសេសរបស់សេវា Network Layer មានដូចជា៖

- ទំនួលខុសត្រូវចម្បងនៃ Network Layer គឺដើម្បីយកកញ្ចប់ទិន្នន័យពីប្រភពទៅគោលដៅដោយមិនផ្លាស់ប្តូរ ឬប្រើប្រាស់ពួកវា។
- ប្រសិនបើកញ្ចប់ធំពេកសម្រាប់ការចែកចាយ ពួកវាត្រូវបានបែងចែក ពោលគឺ បំបែកទៅជាកញ្ចប់តូចៗ។
- វាធ្វើការសម្រេចផ្លូវដែលត្រូវយកដោយកញ្ចប់ព័ត៌មានដើម្បីធ្វើដំណើរពីប្រភពទៅគោលដៅក្នុងចំណោមវិធីជាច្រើនដែលមាននៅក្នុងបណ្តាញ (ហៅផងដែរថាការនាំផ្លូវ)។
- អាសយដ្ឋានប្រភព និងទិសដៅត្រូវបានបន្ថែមទៅកញ្ចប់ទិន្នន័យដែលនៅខាងក្នុង Network Layer។

៦.៣.១ ការវេចខ្ចប់

ដំណើរការនៃការវេចខ្ចប់ទិន្នន័យដែលទទួលបានពីស្រទាប់ខាងលើនៃបណ្តាញ (ហៅផងដែរថា payload) នៅក្នុងកញ្ចប់ Network Layer នៅប្រភព និង Eencapsulating payload ពី Packet Network Layer នៅគោលដៅត្រូវបានគេហៅថា Ppacketizing ។ ម៉ាស៊ីនប្រភពបន្ថែមបឋមកថាដែលមានអាសយដ្ឋានប្រភព និងទិសដៅ និងព័ត៌មានពាក់ព័ន្ធមួយចំនួនទៀតដែលតម្រូវដោយពិធីការ Network Layerទៅបន្ទុកដែលទទួលបានពីពិធីការស្រទាប់ខាងលើ ហើយបញ្ជូនកញ្ចប់ព័ត៌មានទៅស្រទាប់តំណទិន្នន័យ។ ម៉ាស៊ីនគោលដៅទទួលបានកញ្ចប់ព័ត៌មានNetwork Layerពីស្រទាប់តំណទិន្នន័យរបស់វា បំបែកកញ្ចប់ព័ត៌មាន និងបញ្ជូនបន្ទុកទៅពិធីការស្រទាប់ខាងលើដែលត្រូវគ្នារ៉ោតទ័រនៅក្នុងផ្លូវមិនត្រូវបានអនុញ្ញាតឱ្យផ្លាស់ប្តូរទាំងប្រភព ឬអាសយដ្ឋានគោលដៅនោះទេ។ រ៉ោតទ័រដែលនៅតាមផ្លូវមិនត្រូវបានអនុញ្ញាតឱ្យបំបែកកញ្ចប់ព័ត៌មានដែលពួកគេទទួលបានទេ លុះត្រាតែពួកគេចាំបាច់ត្រូវបែងចែក។

៦.៣.២ ការដាំផ្លូវ និងការបញ្ជូនបន្ត

ទាំងនេះគឺជាសេវាកម្មពីរផ្សេងទៀតដែលផ្តល់ដោយ Network Layer ហើយនៅក្នុងបណ្តាញមួយមានផ្លូវជាច្រើនអាចរកបានពីប្រភពទៅគោលដៅ។ Network Layer បញ្ជាក់ពីយុទ្ធសាស្ត្រមួយ

ចំនួនដើម្បីស្វែងរកផ្លូវដែលល្អបំផុតដំណើរការនេះត្រូវបានគេហៅថា នាំផ្លូវ។ ពិធីការនាំផ្លូវជាច្រើនត្រូវបានប្រើក្នុងដំណើរការនេះ ហើយពួកវាគួរតែត្រូវបានដំណើរការដើម្បីជួយរ៉ោតទ័រសម្របសម្រួលគ្នាទៅវិញទៅមក និងជួយបង្កើតទំនាក់ទំនងទូទាំងបណ្តាញ។ ការបញ្ជូនបន្តគឺជាសកម្មភាពដែលអនុវត្តដោយរ៉ោតទ័រនីមួយៗ នៅពេលដែលកញ្ចប់ព័ត៌មានមកដល់ចំណុចប្រទាក់ណាមួយរបស់វា នៅពេលដែលរ៉ោតទ័រទទួលបានកញ្ចប់ព័ត៌មានពីបណ្តាញភ្ជាប់ណាមួយរបស់វា វាចាំបាច់ត្រូវបញ្ជូនកញ្ចប់ព័ត៌មានទៅបណ្តាញផ្សេងទៀត (ការបញ្ជូនបន្ត unicast) ឬបណ្តាញភ្ជាប់មួយចំនួន ។

សេវាកម្មមួយចំនួនផ្សេងទៀតដែលត្រូវបានរំពឹងទុកពី Network Layer គឺ៖

- **ការគ្រប់គ្រងកំហុស៖** ទោះបីជាវាអាចត្រូវបានអនុវត្តនៅក្នុង Network Layer ក៏ដោយ ជាធម្មតាវាមិនត្រូវបានគេពេញចិត្តទេ ពីព្រោះកញ្ចប់ទិន្នន័យនៅក្នុង Network Layer អាចត្រូវបានបំបែកនៅក្នុងរ៉ោតទ័រនីមួយៗ ដែលធ្វើឱ្យការត្រួតពិនិត្យកំហុសក្នុង Network Layer មិនមានប្រសិទ្ធភាព។
- **ការគ្រប់គ្រងលំហូរ៖** វាគឺជាគ្រប់គ្រងបរិមាណទិន្នន័យដែលប្រភពអាចផ្ញើដោយមិនផ្ទុកលើសទម្ងន់របស់អ្នកទទួលប្រសិនបើប្រភពផលិតទិន្នន័យលឿនជាងអ្នកទទួលអាចប្រើប្រាស់បាន អ្នកទទួលនឹងផ្ទុកទិន្នន័យលើសទម្ងន់។ ដើម្បីគ្រប់គ្រងលំហូរទិន្នន័យ អ្នកទទួលគួរតែផ្ញើមតិត្រឡប់ទៅកាន់អ្នកផ្ញើ ដើម្បីប្រាប់អ្នកក្រោយនាវាផ្ទុកទិន្នន័យលើសទម្ងន់មានការខ្វះខាតការគ្រប់គ្រងលំហូរនៅក្នុងការរចនា Network Layer។ វាមិនផ្តល់ការគ្រប់គ្រងលំហូរដោយផ្ទាល់ទេ។ datagrams ត្រូវបានផ្ញើដោយអ្នកផ្ញើ នៅពេលដែលពួកគេរួចរាល់ ដោយមិនយកចិត្តទុកដាក់លើការត្រៀមខ្លួនរបស់អ្នកទទួលឡើយ។
- **ការគ្រប់គ្រងការកកស្ទះ៖** ការកកស្ទះកើតឡើងនៅពេលដែលចំនួន datagram ដែលផ្ញើដោយប្រភពគឺលើសពីសមត្ថភាពរបស់បណ្តាញ ឬរ៉ោតទ័រ។ នេះគឺជាបញ្ហាមួយផ្សេងទៀតនៅក្នុងពិធីការ Network Layer ប្រសិនបើការកកស្ទះនៅតែបន្ត ពេលខ្លះស្ថានភាពអាចនឹងមកដល់កន្លែងដែលប្រព័ន្ធដួលរលំ ហើយមិនមានទិន្នន័យទិន្នន័យត្រូវបានបញ្ជូនទោះបីជាការគ្រប់គ្រងការកកស្ទះត្រូវបានអនុវត្តដោយប្រយោលនៅក្នុង Network Layer ក៏ដោយ ក៏នៅតែមានការខ្វះខាតនៃការគ្រប់គ្រងការកកស្ទះ។

ក. អត្ថប្រយោជន៍នៃសេវាកម្ម Network Layer ៖

- សេវារៀបចំកញ្ចប់ព័ត៌មានក្នុង Network Layer ផ្តល់ភាពងាយស្រួលនៃការដឹកជញ្ជូនកញ្ចប់ទិន្នន័យ។
- ការវេចខ្ចប់ក៏លុបបំបាត់ចំណុចបរាជ័យតែមួយនៅក្នុងប្រព័ន្ធទំនាក់ទំនងទិន្នន័យផងដែរ។
- រ៉ោតទ័រនៅក្នុង Network Layer កាត់បន្ថយចរាចរណ៍បណ្តាញដោយបង្កើតការប៉ះទង្គិចនិងដែនផ្សាយ។

- ដោយមានជំនួយពីការបញ្ជូនបន្ត កញ្ចប់ទិន្នន័យត្រូវបានផ្ទេរពីកន្លែងមួយទៅកន្លែងមួយទៀតនៅក្នុងបណ្តាញ។

ខ. គុណវិបត្តិ នៃសេវាកម្ម Network Layer ៖

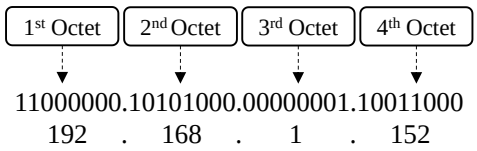
- មានការខ្វះខាតការគ្រប់គ្រងលំហូរនៅក្នុងការរចនា Network Layer។
- ជួនកាលការកកស្ទះកើតឡើងដោយសារតែទិន្នន័យបណ្តាញច្រើនពេកលើសពីសមត្ថភាពរបស់បណ្តាញ ឬរ៉ោតទ័រ ដោយសារតែបញ្ហានេះ រ៉ោតទ័រមួយចំនួនអាចទម្លាក់ទិន្នន័យទិន្នន័យមួយចំនួនហើយព័ត៌មានសំខាន់ៗមួយចំនួនអាចនឹងបាត់បង់។
- ទោះបីជាការគ្រប់គ្រងកំហុសដោយប្រយោលមានវត្តមាននៅក្នុង Network Layer ក៏ដោយ ក៏ចាំបាច់ត្រូវមានយន្តការត្រួតពិនិត្យកំហុសដែលត្រឹមត្រូវបន្ថែមទៀតដោយសារវត្តមាននៃកញ្ចប់ទិន្នន័យដែលបែកខ្ញែកការគ្រប់គ្រងកំហុសក្លាយជាការលំបាកក្នុងការអនុវត្ត។

៦.៤ អាសយដ្ឋាន IP

អាសយដ្ឋាន IP អាចត្រូវបានសរសេរជាសញ្ញាណបី៖ គោលពីរ ចំណុច-ទសភាគ និងគោលដប់ប្រាំមួយ។ ពីសញ្ញាណទាំងនេះ កុំព្យូទ័រស្គាល់តែសញ្ញាគោលពីរប៉ុណ្ណោះ សញ្ញាគោលពីរគឺស្មុគស្មាញក្នុងការសរសេរ និងយល់ ដើម្បីធ្វើឱ្យអាសយដ្ឋាន IP ងាយស្រួលប្រើ អាសយដ្ឋាន IP ក៏ត្រូវបានសរសេរជាសញ្ញាចុច-ទសភាគ និងគោលដប់ប្រាំមួយផងដែរ។ ប្រសិនបើអាសយដ្ឋាន IP ត្រូវបានសរសេរជាសញ្ញាខ្ទង់-ទសភាគ ឬគោលដប់ប្រាំមួយ កុំព្យូទ័រនឹងបំប្លែងពួកវាទៅជាសញ្ញាគោលពីរដោយស្វ័យប្រវត្តិ មុនពេលដំណើរការពួកវា។ អាសយដ្ឋាន IP មានពីរកំណែ IPv4 និង IPv6 រយៈពេលនៃអាសយដ្ឋាន IP គឺខុសគ្នានៅក្នុងកំណែទាំងពីរ។ កំណែទាំងពីរនេះក៏ប្រើទម្រង់ផ្សេងទៀត ដើម្បីបែងចែករវាងអាសយដ្ឋានបណ្តាញ និងម៉ាស៊ីន។ ចូរយើងយល់ពីអាសយដ្ឋាន IP នៅក្នុងកំណែទាំងពីរ។

៦.៤.១ អាសយដ្ឋាន IPv4

ហានានុក្រមនៃពិធីការរបស់អ៊ីនធឺណិតមានClass អាសយដ្ឋាន IP ជាច្រើនដែលត្រូវប្រើប្រាស់ប្រកបដោយប្រសិទ្ធភាពក្នុងស្ថានភាពផ្សេងៗទៅតាមតម្រូវការរបស់ម៉ាស៊ីនក្នុងមួយបណ្តាញជាទូទៅ ប្រព័ន្ធអាសយដ្ឋាន IPv4 ត្រូវបានបែងចែកជា ៥Class នៃអាសយដ្ឋាន IP ។ Class ទាំងប្រាំត្រូវបានកំណត់អត្តសញ្ញាណដោយ octet ដំបូងនៃអាសយដ្ឋាន IP សាធីវកម្មអ៊ីនធឺណែតសម្រាប់ឈ្មោះ និងលេខដែលបានចាត់តាំង ទទួលខុសត្រូវក្នុងការកំណត់អាសយដ្ឋាន IP ។ octet ទីមួយដែលសំដៅទីនេះគឺឆ្ងាយបំផុតទៅខាងឆ្វេង octets ត្រូវបានដាក់លេខដូចខាងក្រោម៖



រូបភាព ៦.២ អាសយដ្ឋាន IPv4

នៅពេលគណនាអាសយដ្ឋាន IP របស់ម៉ាស៊ីន អាសយដ្ឋាន IP ត្រូវបានចយចុះ២ ព្រោះវាមិនអាចកំណត់ទៅម៉ាស៊ីនបានទេពោលគឺ IP ទីមួយនៃបណ្តាញគឺជាលេខបណ្តាញហើយ IP ចុងក្រោយត្រូវបានបម្រុងទុកសម្រាប់ការផ្សាយ IP ។

Number of Networks	=2^network_bits
Number of Host/networks	=2^host_bits - 2

រូបភាព ៦.៣ ការស្វែងរកបណ្តាញ និងម៉ាស៊ីន

ក. អាស័យដ្ឋាន Class A

ប៊ីតដំបូងនៃ octet ទីមួយតែងតែកំណត់ទៅ 0 (សូន្យ)។ ដូច្នេះ octet ដំបូងមានចាប់ពី ១ ដល់ ១២៧ ។

- អាសយដ្ឋាន Class A រួមបញ្ចូលតែ IP ដែលចាប់ផ្តើមពី 1. x.x.x ដល់ 126. x.x.x តែប៉ុណ្ណោះ។ ជួរ IP គឺ 127. x.x.x ត្រូវបានបម្រុងទុកសម្រាប់អាសយដ្ឋាន IP រង្វិលជុំ។
- Subnet Mask លំនាំដើមសម្រាប់អាសយដ្ឋាន IP Class A គឺ 255.0.0.0 ដែលមានន័យថាអាសយដ្ឋាន Class A អាចមានបណ្តាញ 126 (2^7-2) និង 16777214 ម៉ាស៊ីន (2^{24}-2) ។
- ទម្រង់អាសយដ្ឋាន IP Class A គឺដូច្នេះ៖

  0NNNNNNN.HHHHHHHH. HHHHHHHH.HHHHHHHH

00000001 - 01111111

1 - 127

រូបភាព ៦.៤ អាសយដ្ឋាន IP Class A

ខ. អាសយដ្ឋាន Class B

IP ដែលជាកម្មសិទ្ធិរបស់ Class B មានពីរប៊ីតដំបូងក្នុង octet ដំបូងកំណត់ទៅ 10

- អាសយដ្ឋាន IP Class B មានចាប់ពី 128.0.x.x ដល់ 191.255.x.x ។ Subnet Mask លំនាំដើមសម្រាប់ Class B គឺ 255.255.x.x ។
- Class B មានអាសយដ្ឋានបណ្តាញ 16384 (2^{14}) និងអាសយដ្ឋានម៉ាស៊ីន 65534 (2^{16}-2)
- ទម្រង់អាសយដ្ឋាន IP Class B គឺ៖

  10NNNNNN.NNNNNNNN. HHHHHHHH.HHHHHHHH

10000001 - 10111111
128 - 191

រូបភាព ៦.៥ អាសយដ្ឋាន IP Class B

គ. អាសយដ្ឋាន Class C

octet ដំបូងនៃអាសយដ្ឋាន IP Class C មាន 3 ប៊ីតដំបូងរបស់វាត្រូវបានកំណត់ទៅ 110 នោះគឺ

- អាសយដ្ឋាន IP Class C មានចាប់ពី 192.0.0.x ដល់ 223.255.255.x ។ Subnet Mask លំនាំដើមសម្រាប់ Class C គឺ 255.255.255.x ។
- Class C ផ្តល់អាសយដ្ឋានបណ្តាញ 2097152 (2^{21}) និងអាសយដ្ឋានម៉ាស៊ីន 254 (2^{8}-2) ។
- ទម្រង់អាសយដ្ឋាន IP Class C គឺ៖

  110NNNNN.NNNNNNNN. NNNNNNNN.HHHHHHHH

11000001 - 11011111
192 - 223

រូបភាព ៦.៦ អាសយដ្ឋាន IP Class C

ឃ. អាសយដ្ឋានClass D

បួនប៊ីតដំបូងនៃ octet ដំបូងនៅក្នុងអាសយដ្ឋាន IP Class D ត្រូវបានកំណត់ទៅ 1110 ដោយ ផ្តល់ជូរនៃ៖

- Class D មានអាសយដ្ឋាន IP ពី 224.0.0.0 ដល់ 239.255.255.255 ។
- Class D ត្រូវបានបម្រុងទុកសម្រាប់ Multicasting នៅក្នុង multicasting ទិន្នន័យមិនមានកំណត់សម្រាប់ host ជាក់លាក់ណាមួយទេ ដូច្នេះមិនចាំបាច់ទាញយក host address ចេញពី IP address ហើយ Class D មិនមាន Subnet Mask ណាមួយទេ។

11100001 - 11101111
224 - 239

រូបភាព ៦.៧ អាសយដ្ឋាន IP ក្នុងបៃទី១ នៃClass D

ង. អាសយដ្ឋានClass E

Class IP នេះត្រូវបានបម្រុងទុកសម្រាប់គោលបំណងពិសោធន៍សម្រាប់តែការសិក្សាប៉ុណ្ណោះ។

• អាសយដ្ឋាន IP នៅក្នុង Class នេះមានចាប់ពី 240.0.0.0 ដល់ 255.255.255.254 ដូច Class D Class នេះមិនត្រូវបានបំពាក់ដោយ Subnet Mask ណាមួយទេ។

៦.៤.២ បណ្តាញគ្មានថ់រេង IPv4

Class IP នីមួយៗត្រូវបានបំពាក់ដោយ Subnet Mask លំនាំដើមរបស់វា ដែលកំណត់ Class IP ឱ្យមានចំនួនបណ្តាញបុព្វបទ និងចំនួនបុព្វបទនៃម៉ាស៊ីនក្នុងមួយបណ្តាញអាសយដ្ឋាន IP Class មិនផ្តល់ភាពបត់បែនក្នុងការមានម៉ាស៊ីនតិចជាងមុនក្នុងមួយបណ្តាញ ឬបណ្តាញច្រើនក្នុងមួយ IP Class ។ CIDR ឬ Classless Inter-Domain Routing ផ្តល់នូវភាពបត់បែននៃការខ្ចីប៊ីតនៃផ្នែកម៉ាស៊ីននៃអាសយដ្ឋាន IP និងប្រើប្រាស់ពួកវាជាបណ្តាញនៅក្នុងបណ្តាញដែលហៅថាបណ្តាញរង។ បណ្តាញរងអាចប្រើអាសយដ្ឋាន IP Class A តែមួយដើម្បីឱ្យមានបណ្តាញរងតូចជាង ដោយផ្តល់នូវសមត្ថភាពគ្រប់គ្រងបណ្តាញកាន់តែប្រសើរ។

ក. បណ្តាញរង Class A

នៅក្នុងClass A មានតែ octet ដំបូងប៉ុណ្ណោះដែលត្រូវបានប្រើជាឧបករណ៍កំណត់អត្តសញ្ញាណបណ្តាញ ហើយចំនួន octet ដែលនៅសល់ចំនួនបីត្រូវបានផ្តល់ទៅឱ្យ Hosts (ឧ. 16777214 hosts ក្នុងមួយបណ្តាញ) ។ ដើម្បីបង្កើតបណ្តាញរងបន្ថែមទៀតនៅក្នុងClass A ប៊ីតពីផ្នែកម៉ាស៊ីនត្រូវបានខ្ចី ហើយ Subnet Mask ត្រូវបានផ្លាស់ប្តូរទៅតាមនោះ។ ឧទាហរណ៍ ប្រសិនបើ MSB មួយ (Bit Significant Bit) ត្រូវបានខ្ចីពី host bits នៃ octet ទីពីរ ហើយបន្ថែមទៅ network address នោះវាបង្កើត subnets ពីរ (2^1=2) ជាមួយនឹង (2^{23}-2) hosts 8388606 per subnet។ Subnet Maskត្រូវបានផ្លាស់ប្តូរស្របតាមការឆ្លុះបញ្ចាំងពីបណ្តាញរង។ ដែលបានផ្តល់ឱ្យខាងក្រោមគឺជាបញ្ជីនៃបន្សំដែលអាចធ្វើបានទាំងអស់នៃបណ្តាញរង Class A ៖

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
8	255.0.0.0	0	1	16777214
9	255.128.0.0	1	2	8388606
10	255.192.0.0	2	4	4194302
11	255.224.0.0	3	8	2097150
12	255.240.0.0	4	16	1048574
13	255.248.0.0	5	32	524286
14	255.252.0.0	6	64	262142
15	255.254.0.0	7	128	131070
16	255.255.0.0	8	256	65534
17	255.255.128.0	9	512	32766
18	255.255.192.0	10	1024	16382
19	255.255.224.0	11	2048	8190
20	255.255.240.0	12	4096	4094
21	255.255.248.0	13	8192	2046
22	255.255.252.0	14	16384	1022
23	255.255.254.0	15	32768	510
24	255.255.255.0	16	65536	254
25	255.255.255.128	17	131072	126
26	255.255.255.192	18	262144	62
27	255.255.255.224	19	524288	30
28	255.255.225.240	20	1048576	14
29	255.255.225.248	21	2097152	6
30	255.255.255.252	22	4194304	2

រូបភាព ៦.៨ បណ្តាញរង Class A

ក្នុងករណីនៃបណ្តាញរង វាល់អាសយដ្ឋាន IP ដំបូង និងចុងក្រោយរបស់បណ្តាញរង ត្រូវបានប្រើសម្រាប់លេខបណ្តាញរង និងអាសយដ្ឋាន IP ផ្សព្វផ្សាយបណ្តាញរងរៀងៗខ្លួន។ ដោយសារតែអាសយដ្ឋាន IP ទាំងពីរនេះមិនអាចត្រូវបានកំណត់ទៅម៉ាស៊ីនទេ បណ្តាញរងមិនអាចត្រូវបានអនុវត្តដោយប្រើច្រើនជាង 30 ប៊ីតជាបណ្តាញប៊ីត ដែលផ្តល់ម៉ាស៊ីនតិចជាងពីរក្នុងមួយបណ្តាញរង។

ខ. បណ្តាញរង Class B

តាមលំនាំដើមដោយប្រើបណ្តាញ Class 14 bits ត្រូវបានប្រើជា network bits ដែលផ្តល់ (2^{14}) 16384 networks និង (2^{16}-2) 65534 hosts។ អាសយដ្ឋាន IP Class B អាចត្រូវបានដាក់បញ្ចូលតាមវិធីដូចគ្នានឹងអាសយដ្ឋានClass A ដោយខ្ចីបីតពីបីតម៉ាស៊ីន។ ខាងក្រោមនេះត្រូវបានផ្តល់ឱ្យនូវការរួមបញ្ចូលគ្នាដែលអាចធ្វើបានទាំងអស់នៃបណ្តាញរងClass B៖

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
16	255.255.0.0	0	0	65534
17	255.255.128.0	1	2	32766
18	255.255.192.0	2	4	16382
19	255.255.224.0	3	8	8190
20	255.255.240.0	4	16	4094
21	255.255.248.0	5	32	2046
22	255.255.252.0	6	64	1022
23	255.255.254.0	7	128	510
24	255.255.255.0	8	256	254
25	255.255.255.128	9	512	126
26	255.255.255.192	10	1024	62
27	255.255.255.224	11	2048	30
28	255.255.225.240	12	4096	14
29	255.255.225.248	13	8192	6
30	255.255.255.252	14	16384	2

រូបភាព ៦.៩ បណ្តាញរង Class B

គ. បណ្តាញរង Class C

អាសយដ្ឋាន IP Class C ជាធម្មតាត្រូវបានកំណត់ទៅបណ្តាញទំហំតូចព្រោះវាអាចមានម៉ាស៊ីនតែ 254 ក្នុងបណ្តាញមួយ ខាងក្រោមនេះគឺជាបញ្ជីនៃបន្សំដែលអាចធ្វើបានទាំងអស់ Class C

Network Bits	Subnet Mask	Bits Borrowed	Subnets	Hosts/Subnet
24	255.255.255.0	0	0	254
25	255.255.255.128	1	2	126
26	255.255.255.192	2	4	62
27	255.255.255.224	3	8	30
28	255.255.225.240	4	16	14
29	255.255.225.248	5	32	6
30	255.255.255.252	6	64	2

រូបភាព ៦.១០ បណ្តាញរង Class C

៦.៤.៣ IPv4 – VLSM

❖ សេចក្តីណែនាំនៃ Subnet Mask ប្រែប្រួលអថេរ (VLSM)

VLSM តំណាងឱ្យ Subnet Mask ប្រែប្រួលអថេរ ដែលការរចនាបណ្តាញរងប្រើរបាំងច្រើនជាងមួយនៅក្នុងបណ្តាញតែមួយ ដែលមានន័យថារបាំងច្រើនជាងមួយត្រូវបានប្រើសម្រាប់បណ្តាញរងផ្សេងៗគ្នានៃ Class A, B, C ឬបណ្តាញមួយ។ វាត្រូវបានប្រើដើម្បីបង្កើន លទ្ធភាពប្រើប្រាស់នៃបណ្តាញរងហើយដោយសារពួកវាអាចមានទំហំអថេរវាក៏ត្រូវបានកំណត់ថាជាដំណើរការនៃការបង្កើតបណ្តាញរង។

❖ នីតិវិធីសម្រាប់ការអនុវត្ត VLSM

នៅក្នុង VLSM បណ្តាញរងប្រើទំហំប្លុកដោយផ្អែកលើតម្រូវការដូច្នេះការដាក់បណ្តាញរងត្រូវបានទាមទារច្រើនដង ឧបមាថាមានអ្នកគ្រប់គ្រងដែលមាននាយកដ្ឋានចំនួនបួនដើម្បីគ្រប់គ្រង។ ទាំងនេះគឺជាផ្នែកលក់ និងទិញដែលមានកុំព្យូទ័រចំនួន 120 គ្រឿង នាយកដ្ឋានអភិវឌ្ឍន៍ដែលមានកុំព្យូទ័រចំនួន 50 គ្រឿង នាយកដ្ឋានគណនេយ្យដែលមានកុំព្យូទ័រចំនួន 26 គ្រឿង និងផ្នែកគ្រប់គ្រងដែលមានកុំព្យូទ័រចំនួន 5 គ្រឿង។ អ្នកផ្តល់សេវាអ៊ីនធឺណិតអាចប្រឈមមុខនឹងស្ថានភាពដែលពួកគេត្រូវបែងចែកបណ្តាញរង IP ដែលមានទំហំខុសៗគ្នាតាមតម្រូវការរបស់អតិថិជន។ អតិថិជនម្នាក់អាចសួរបណ្តាញរង Class C នៃអាសយដ្ឋាន IP ចំនួន 3 ហើយម្នាក់ទៀតអាចស្នើសុំ IP ចំនួន 10 ។ សម្រាប់ ISP វាមិនអាចធ្វើទៅបានក្នុងការបែងចែកអាសយដ្ឋាន IP ទៅជាបណ្តាញរងដែលមានទំហំថេរនោះទេ ផ្ទុយទៅវិញ គាត់ប្រហែលជាចង់ដាក់បណ្តាញរងក្នុងវិធីមួយដែលនាំឱ្យមានការខ្ជះខ្ជាយអប្បបរមានៃអាសយដ្ឋាន IP ។ ឧទាហរណ៍ អ្នកគ្រប់គ្រងមានបណ្តាញ 192.168.1.0/24 ។ បច្ចុយ /24 (បញ្ចេញសំឡេងជា ``សញ្ញា 24``) ប្រាប់ពីចំនួនប៊ីតដែលប្រើសម្រាប់អាសយដ្ឋានបណ្តាញ។ ក្នុងឧទាហរណ៍នេះ អ្នកគ្រប់គ្រងមាននាយកដ្ឋានបីផ្សេងគ្នាជាមួយនឹងចំនួនម៉ាស៊ីនផ្សេងទៀត ផ្នែកលក់មានកុំព្យូទ័រ 100 គ្រឿង។ នាយកដ្ឋានទិញមានកុំព្យូទ័រចំនួន 50 គណនីមានកុំព្យូទ័រចំនួន 25 គ្រឿង និងផ្នែកគ្រប់គ្រងមានកុំព្យូទ័រចំនួន 5 គ្រឿង។ នៅក្នុង CIDR បណ្តាញរងមានទំហំថេរ។ ដោយប្រើវិធីសាស្ត្រដូចគ្នា អ្នកគ្រប់គ្រងអាចបំពេញតម្រូវការមួយចំនួននៃបណ្តាញប៉ុណ្ណោះ។

នីតិវិធីខាងក្រោមបង្ហាញពីរបៀបដែល VLSM អាចបែងចែកអាសយដ្ឋាន IP តាមនាយកដ្ឋានដូចដែលបានរៀបរាប់ក្នុងឧទាហរណ៍។

ជំហានទី១

Subnet Mask	Slash Notation	Hosts/Subnet
255.255.255.0	/24	254
255.255.255.128	/25	126
255.255.255.192	/26	62
255.255.255.224	/27	30
255.255.225.240	/28	14
255.255.225.248	/29	6
255.255.255.252	/30	2

រូបភាព ៦.១១ អាសយដ្ឋាន IP VLSM

ជំហានទី២

តម្រៀបតម្រូវការរបស់ IP តាមលំដាប់ចុះ (ខ្ពស់បំផុតទៅទាបបំផុត)។

- លក់ ១០០
- អភិវឌ្ឍន៍ 50
- គណនេយ្យ ២៥
- ការគ្រប់គ្រង ៥

ជំហានទី៣

បែងចែកជួរខ្ពស់បំផុតនៃ IPs ទៅនឹងតម្រូវការខ្ពស់បំផុត ដូច្នេះសូមកំណត់ 192.168.1.0 /25 (255.255.255.128) ទៅផ្នែកលក់។ បណ្តាញរង IP នេះដែលមានលេខបណ្តាញ 192.168.1.0 មានអាសយដ្ឋាន IP ម៉ាស៊ីនត្រឹមត្រូវចំនួន 126 ដែលបំពេញតម្រូវការរបស់ផ្នែកលក់។ Subnet Mask ដែលប្រើសម្រាប់ subnet នេះមាន 10000000 ជា octet ចុងក្រោយ។

ជំហានទី៤

បែងចែកនៃជួរខ្ពស់បំផុតខាងក្រោមសូមចាត់ចែងទៅតាមអស័យដ្ឋាន 192.168.1.128 /26 (255.255.255.192) ទៅផ្នែកអភិវឌ្ឍន៍ ។ បណ្តាញរង IP នេះដែលមានលេខបណ្តាញ 192.168.1.128 មានអាសយដ្ឋាន IP របស់ម៉ាស៊ីនត្រឹមត្រូវចំនួន 62 ដែលអាចត្រូវបានកំណត់យ៉ាងងាយស្រួលទៅកាន់កុំព្យូទ័រទាំងអស់នៃផ្នែកទិញ។ Subnet Maskដែលបានប្រើមាន 11000000 ក្នុង octet ចុងក្រោយ។

ជំហានទី៥

បែងចែកជួរខ្ពស់បំផុតបន្ទាប់ ពោលគឺ គណោន្យ។ តម្រូវការ 25 IPs អាចត្រូវបានបំពេញដោយ 192.168.1.192 /27 (255.255.255.224) IP បណ្តាញរងដែលមាន IP ម៉ាស៊ីនត្រឹមត្រូវ 30 ។ លេខបណ្តាញនៃនាយកដ្ឋានគណោន្យនឹងមាន 192.168.1.192 ។ octet ចុងក្រោយនៃ Subnet Maskគឺ 11100000។

ជំហានទី៦

បែងចែកជួរខ្ពស់បំផុតបន្ទាប់ទៅការគ្រប់គ្រង នាយកដ្ឋានគ្រប់គ្រងមានតែកុំព្យូទ័រប្រាំគ្រឿងប៉ុណ្ណោះ។ បណ្តាញរង 192.168.1.224 /29 ជាមួយ Mask 255.255.255.248 មានអាសយដ្ឋាន IP ម៉ាស៊ីនត្រឹមត្រូវចំនួនប្រាំមួយ។ ដូច្នេះ នេះអាចត្រូវបានចាត់ឱ្យទៅ Class គ្រប់គ្រង octet ចុងក្រោយនៃ Subnet Mask នឹងមាន 11111000។

ដោយប្រើ VLSM អ្នកគ្រប់គ្រងអាចបញ្ចូលបណ្តាញរង IP ដូច្នេះចំនួនអាសយដ្ឋាន IP តិចបំផុតត្រូវបានខ្ជះខ្ជាយ។ សូម្បីតែបន្ទាប់ពីការចាត់តាំង IPs ទៅគ្រប់នាយកដ្ឋានក៏ដោយ អ្នកគ្រប់គ្រងក្នុងឧទាហរណ៍នេះ នៅតែត្រូវការអាសយដ្ឋាន IP ឱ្យបានច្រើន ដែលនឹងមិនអាចទៅរួចទេប្រសិនបើគាត់បានប្រើ CIDR ។

៦.៤.៤ CIDR និងរបៀបដែលវាដំណើរការ

Classless Inter-Domain Routing (CIDR) គឺជាក្រុមនៃអាសយដ្ឋាន IP ដែលត្រូវបានបម្រុងទុកសម្រាប់អតិថិជននៅពេលដែលពួកគេទាមទារចំនួនអាសយដ្ឋាន IP ថែរ។ នៅក្នុង CIDR មិនមានការខ្ជះខ្ជាយនៃអាសយដ្ឋាន IP បើប្រៀបធៀបទៅនឹងអាសយដ្ឋានពេញClassទេ ពីព្រោះមានតែចំនួនអាសយដ្ឋាន IP ដែលអតិថិជនទាមទារប៉ុណ្ណោះដែលត្រូវបានបែងចែកទៅឱ្យអតិថិជន។ ក្រុមនៃអាសយដ្ឋាន IP ត្រូវបានគេហៅថា Block in Classless Inter-Domain (CIDR) ។ CIDR ធ្វើតាមសញ្ញាសម្គាល់ CIDR ឬសញ្ញាកាត់។ តំណាងនៃសញ្ញាណ CIDR គឺ x.y.z.w /n, x.y.z.w គឺជាអាសយដ្ឋាន IP ហើយ n ត្រូវបានគេហៅថារបាំង ឬចំនួនប៊ីតដែលប្រើក្នុងលេខសម្គាល់បណ្តាញ។

❖ លក្ខណៈសម្បត្តិរបស់ CIDR Block

លក្ខណៈសម្បត្តិនៃប្លុក CIDR មានដូចខាងក្រោម៖

- អាសយដ្ឋាន IP នៅក្នុងប្លុកគឺបន្ត។
- អាសយដ្ឋានទីមួយរបស់ប្លុកគួរត្រូវបានបែងចែកដោយចំនួនអាសយដ្ឋាននៃភាពជាដៃគូ
- ទំហំនៃប្លុកគួរតែគុណនឹង 2 ។

❖ ការប្រើប្រាស់ CIDR

- Subnet Mask ប្រវែងអថេរ គឺជាមូលដ្ឋានគ្រឹះនៃ CIDR (VLSM)។ ឥឡូវនេះ វាអាចបញ្ជាក់បុព្វបទនៃរយៈពេលណាមួយដែលធ្វើឱ្យវាមានឥទ្ធិពលខ្លាំងជាងវិធីសាស្ត្រមុន។
- ការប្រមូលលេខចំនួនពីរបង្កើតជាអាសយដ្ឋាន IP CIDR ។ អាសយដ្ឋានបណ្តាញត្រូវបានគេសរសេរជាបុព្វបទ ស្រដៀងនឹងអាសយដ្ឋាន IP (ឧ. 192.255.255.255) ។
- សមាសភាគទីពីរគឺបច្ច័យ ដែលមានន័យថាចំនួនប៊ីតនៅក្នុងអាសយដ្ឋានទាំងមូល (ឧ./12)។ អាសយដ្ឋាន IP របស់ CIDR នឹងមើលទៅដូចនេះ នៅពេលដាក់បញ្ចូលគ្នា

  192.255.255.255/12

- ជាផ្នែកមួយនៃអាសយដ្ឋាន IP បុព្វបទបណ្តាញត្រូវបានកំណត់ផងដែរ។ ការផ្លាស់ប្តូរទាំងនេះគឺផ្អែកលើចំនួនប៊ីតដែលត្រូវការ។ ឧទាហរណ៍ខាងលើ អាសយដ្ឋាន 12 ប៊ីតដំបូងគឺសម្រាប់បណ្តាញខណៈ 20 ប៊ីតចុងក្រោយគឺសម្រាប់អាសយដ្ឋានម៉ាស៊ីន។

❖ សញ្ញាណ CIDR

- ដោយប្រើ CIDR យើងអាចកំណត់អាសយដ្ឋាន IP ទៅម៉ាស៊ីនដោយមិនប្រើ Class អាសយដ្ឋាន ID ស្តង់ដារដូចជា Class A, B, និង C។
- នៅក្នុង CIDR យើងប្រាប់ចំនួនប៊ីតដែលត្រូវបានប្រើសម្រាប់លេខសម្គាល់បណ្តាញ។ ប៊ីតលេខសម្គាល់បណ្តាញត្រូវបានផ្តល់ជូនបន្ទាប់ពីនិមិត្តសញ្ញា '/' ។ ដូចជា /10 មានន័យថា 10ប៊ីត ត្រូវបានប្រើសម្រាប់ផ្នែក ID បណ្តាញ ហើយនៅសល់ 32-10=22 ប៊ីតត្រូវបានប្រើសម្រាប់ផ្នែកលេខសម្គាល់ម៉ាស៊ីន។
- អត្ថប្រយោជន៍នៃការប្រើប្រាស់សញ្ញាសម្គាល់ CIDR គឺថាវាកាត់បន្ថយចំនួនធាតុនៅក្នុងតារាងនាំផ្លូវ និងគ្រប់គ្រងចន្លោះអាសយដ្ឋាន IP ។

❖ គុណវិបត្តិ CIDR

គុណវិបត្តិនៃការប្រើប្រាស់ CIDR Notation មានដូចខាងក្រោម៖

- ការប្រើប្រាស់ CIDR វាស្មុគស្មាញក្នុងការកំណត់ផ្លូវ។ ដោយប្រើអាសយដ្ឋាន Class ពេញលេញយើងមានតារាងដាច់ដោយឡែកសម្រាប់ Class A-C ។
- ដូច្នេះយើងចូលទៅកាន់តារាងទាំងនេះដោយផ្ទាល់ដោយមើលបុព្វបទអាសយដ្ឋាន IP ។ ប៉ុន្តែដោយប្រើ CIDR យើងមិនមានតារាងទាំងនេះដាច់ដោយឡែកទេ។ ធាតុទាំងអស់ត្រូវបានដាក់ក្នុងតារាងតែមួយ។ ដូច្នេះការស្វែងរកផ្លូវគឺពិបាកណាស់។

៦.៤.៥ IPv4 - អាសយដ្ឋានដែលបានបម្រុងទុក

ចន្លោះអាសយដ្ឋាន IPv4 ដែលបានបម្រុងទុកមួយចំនួនមិនអាចប្រើនៅលើអ៊ីនធឺណិតបានទេ អាសយដ្ឋានទាំងនេះបម្រើគោលបំណងជាក់លាក់មួយ ហើយមិនអាចបញ្ជូនចេញក្រៅបណ្តាញតំបន់មូលដ្ឋានបានទេ។

❖ អាសយដ្ឋាន IP ឯកជន

រាល់ Class IP (A, B & C) មានអាសយដ្ឋានមួយចំនួនដែលត្រូវបានបម្រុងទុកជាអាសយដ្ឋាន IP ឯកជន។ IP ទាំងនេះអាចត្រូវបានប្រើនៅក្នុងបណ្តាញ បរិវេណសាលា ឬក្រុមហ៊ុន ហើយមាន លក្ខណៈឯកជន អាសយដ្ឋានទាំងនេះមិនអាចបញ្ជូនតាមអ៊ីនធឺណិតបានទេ ដូច្នេះរ៉ោតទ័រទម្លាក់កញ្ចប់ព័ត៌មានដែលមានអាសយដ្ឋានផ្ទាល់ខ្លួនទាំងនេះ។

Class A IP Range		Subnet Mask
10.0.0.0	-10.255.255.255	255.0.0.0
172.16.0.0	-172.31.255.255	255.240.0.0
192.168.0.0	-192.168.255.255	255.255.0.0

រូបភាព ៦.១២ អាសយដ្ឋាន IP ឯកជន Class A

ដើម្បីទំនាក់ទំនងជាមួយពិភពខាងក្រៅ អាសយដ្ឋាន IP ទាំងនេះត្រូវតែត្រូវបានបកប្រែទៅជាអាសយដ្ឋាន IP សាធារណៈមួយចំនួនដោយប្រើដំណើរការ NAT ឬម៉ាស៊ីនមេប្រូកស៊ីបណ្តាញអាចត្រូវបានប្រើ។ គោលបំណងតែមួយគត់នៃការបង្កើតជួរដាច់ដោយឡែកនៃអាសយដ្ឋានឯកជនគឺដើម្បីគ្រប់គ្រងការចាត់តាំងនៃក្រុមអាសយដ្ឋាន IPv4 ដែលបានកំណត់រួចហើយ។ ការប្រើប្រាស់ជួរអាសយដ្ឋានឯកជននៅក្នុង LAN បានកាត់បន្ថយតម្រូវការសម្រាប់អាសយដ្ឋាន IPv4 ជាសកល។ វាក៏បានជួយពន្យាពេលអស់អាសយដ្ឋាន IPv4 ផងដែរ។ Class IP ខណៈពេលដែលប្រើជួរអាសយដ្ឋានឯកជនអាចត្រូវបានជ្រើសរើសតាមទំហំ និងតម្រូវការរបស់ស្ថាប័ន។ អង្គការធំជាងអាចជ្រើសរើស Class A ជួរអាសយដ្ឋាន IP ឯកជន ចំណែកអង្គការតូចៗអាចជ្រើសរើស Class C ។ អាសយដ្ឋាន IP ទាំងនេះអាចត្រូវបានដាក់បន្ថែម និងដាក់ឱ្យនាយកដ្ឋានក្នុងស្ថាប័នមួយ។

❖ Loopback អាសយដ្ឋាន IP

ជួរអាសយដ្ឋាន IP 127.0.0.0 - 127.255.255.255 ត្រូវបានបម្រុងទុកសម្រាប់ loopback ពោលគឺអាសយដ្ឋានដោយខ្លួនឯងរបស់ម៉ាស៊ីន ដែលត្រូវបានគេស្គាល់ថាជាអាសយដ្ឋានម៉ាស៊ីនមូលដ្ឋាន។ អាសយដ្ឋាន IP រង្វិលជុំនេះត្រូវបានគ្រប់គ្រងទាំងស្រុងដោយ និងនៅក្នុងប្រព័ន្ធប្រតិបត្តិការ។

អាសយដ្ឋាន Loopback បើកដំណើរការម៉ាស៊ីនមេ និងម៉ាស៊ីនភ្ញៀវនៅលើប្រព័ន្ធតែមួយដើម្បីទំនាក់ទំនងគ្នាទៅវិញទៅមក។ នៅពេលដែលដំណើរការបង្កើតកញ្ចប់ព័ត៌មានដែលមានអាសយដ្ឋានទិសដៅជាអាសយដ្ឋានរង្វិលជុំវិញប្រព័ន្ធប្រតិបត្តិការនឹងវិលត្រលប់មកខ្លួនវាវិញដោយគ្មានការជ្រៀតជ្រែកពី NIC ។ ទិន្នន័យដែលបានផ្ញើនៅលើ loopback ត្រូវបានបញ្ជូនបន្តដោយប្រព័ន្ធប្រតិបត្តិការទៅកាន់ចំណុចប្រទាក់បណ្តាញនិម្មិតនៅក្នុងប្រព័ន្ធប្រតិបត្តិការ។ ហើយអាសយដ្ឋាននេះត្រូវបានប្រើជាចម្បងសម្រាប់គោលបំណងសាកល្បង ដូចជាស្ថាបត្យកម្មម៉ាស៊ីនភ្ញៀវ-ម៉ាស៊ីនមេ នៅលើម៉ាស៊ីនតែមួយ។ ជាងនេះទៅទៀត ប្រសិនបើម៉ាស៊ីនអាច ping 127.0.0.1 ដោយជោគជ័យ ឬ IP ណាមួយពីជួររង្វិលជុំវិញ វាមានន័យថា កម្មវិធី TCP/IP នៅលើម៉ាស៊ីនត្រូវបានផ្ទុក និងដំណើរការដោយជោគជ័យ។

❖ តំណភ្ជាប់ អាស័យដ្ឋានមូលដ្ឋាន

ប្រសិនបើម៉ាស៊ីនមិនអាចទទួលបានអាសយដ្ឋាន IP ពីម៉ាស៊ីនមេ DHCP ហើយមិនត្រូវបានផ្តល់អាសយដ្ឋាន IP ដោយដៃទេនោះ ម៉ាស៊ីននេះអាចកំណត់ដោយខ្លួនវានូវអាសយដ្ឋាន IP ពីជួរនៃអាសយដ្ឋានតំណដែលបានបម្រុងទុក។ តំណភ្ជាប់ អាស័យដ្ឋានមូលដ្ឋាន ក្នុងតំបន់មានចាប់ពី 169.254.0.0 - 169.254.255.255 ។ សន្ទតផ្នែកបណ្តាញដែលប្រព័ន្ធទាំងអស់ត្រូវបានកំណត់រចនាសម្ព័ន្ធដើម្បីទទួលបានអាសយដ្ឋាន IP ពីម៉ាស៊ីនមេ DHCP ដែលភ្ជាប់ទៅផ្នែកបណ្តាញដូចគ្នា។ ប្រសិនបើម៉ាស៊ីនមេ DHCP មិនអាចប្រើបានទេ គ្មានម៉ាស៊ីននៅលើផ្នែកនឹងអាចទំនាក់ទំនងជាមួយអ្នកដទៃបានទេ។ វីនដូ (98 ឬក្រោយ) និង Mac OS (8.0 ឬខ្ពស់ជាងនេះ) គាំទ្រមុខងារកំណត់រចនាសម្ព័ន្ធដោយខ្លួនឯងនៃអាសយដ្ឋាន IP មូលដ្ឋាននៃតំណ។ អវត្តមាននៃម៉ាស៊ីនមេ DHCP រាល់ម៉ាស៊ីនមេជ្រើសរើសដោយចៃដន្យនូវអាសយដ្ឋាន IP ពីជួរដែលបានរៀបរាប់ខាងលើ ហើយបន្ទាប់មកពិនិត្យមើលដើម្បីបញ្ជាក់ដោយប្រើ ARP ប្រសិនបើម៉ាស៊ីនផ្សេងទៀតមិនបានកំណត់រចនាសម្ព័ន្ធដោយខ្លួនវាជាមួយអាសយដ្ឋាន IP ដូចគ្នា។ នៅពេលដែលម៉ាស៊ីនទាំងអស់ប្រើតំណភ្ជាប់-អាសយដ្ឋានមូលដ្ឋាននៃជួរដូចគ្នា ពួកគេអាចទំនាក់ទំនងគ្នាទៅវិញទៅមក។ អាសយដ្ឋាន IP ទាំងនេះមិនអាចជួយប្រព័ន្ធទំនាក់ទំនងបានទេ នៅពេលដែលពួកវាមិនមែនជាកម្មសិទ្ធិរបស់ផ្នែករូបវន្ត ឬឡូជីខលដូចគ្នា IP ទាំងនេះក៏មិនអាចដំណើរការបានដែរ។

❖ ច្បាប់សម្រាប់ការចាត់តាំងលេខសម្គាល់ម៉ាស៊ីន៖

លេខសម្គាល់ម៉ាស៊ីនត្រូវបានប្រើដើម្បីកំណត់អត្តសញ្ញាណម៉ាស៊ីននៅក្នុងបណ្តាញ លេខសម្គាល់ ម៉ាស៊ីនត្រូវបានចាត់តាំងដោយផ្អែកលើច្បាប់ខាងក្រោម៖

- នៅក្នុងបណ្តាញណាមួយលេខសម្គាល់ម៉ាស៊ីនត្រូវតែមានតែមួយគត់សម្រាប់បណ្តាញនោះ។
- លេខសម្គាល់ម៉ាស៊ីនដែលប៊ីតទាំងអស់ត្រូវបានកំណត់ទៅ 0 មិនអាចកំណត់បានទេព្រោះលេខសម្គាល់ម៉ាស៊ីននេះតំណាងឱ្យលេខសម្គាល់បណ្តាញនៃអាសយដ្ឋាន IP ។

- លេខសម្គាល់ម៉ាស៊ីនដែលប៊ីតទាំងអស់ត្រូវបានកំណត់ទៅជា 1 មិនអាចកំណត់បានទេព្រោះលេខសម្គាល់ម៉ាស៊ីននេះត្រូវបានបម្រុងទុកជាអាសយដ្ឋានផ្សាយដើម្បីផ្ញើកញ្ចប់ព័ត៌មានទៅម៉ាស៊ីនទាំងអស់នៅលើបណ្តាញជាក់លាក់នោះ។

❖ ច្បាប់សម្រាប់កំណត់លេខសម្គាល់បណ្តាញ៖

ម៉ាស៊ីនដែលមានទីតាំងនៅលើបណ្តាញរូបវន្តដូចគ្នាត្រូវបានកំណត់អត្តសញ្ញាណដោយលេខសម្គាល់បណ្តាញ ដោយសារម៉ាស៊ីនទាំងអស់នៅលើបណ្តាញរូបវន្តដូចគ្នាត្រូវបានផ្តល់លេខសម្គាល់បណ្តាញដូចគ្នា។ លេខសម្គាល់បណ្តាញត្រូវបានចាត់តាំងដោយផ្អែកលើច្បាប់ខាងក្រោម៖

- លេខសម្គាល់បណ្តាញមិនអាចចាប់ផ្តើមជាមួយ 127 បានទេ ព្រោះ 127 ជាកម្មសិទ្ធិរបស់អាស័យដ្ឋាន Class A ហើយត្រូវបានបម្រុងទុកសម្រាប់មុខងារខាងក្នុងរង្វិលជុំ។
- រាល់ប៊ីតនៃលេខសម្គាល់បណ្តាញដែលបានកំណត់ទៅ 1 ត្រូវបានបម្រុងទុកសម្រាប់ប្រើជាអាសយដ្ឋានផ្សាយ IP ហើយដូច្នេះមិនអាចប្រើបានទេ។
- រាល់ប៊ីតនៃលេខសម្គាល់បណ្តាញដែលបានកំណត់ទៅ 0 ត្រូវបានប្រើដើម្បីសម្គាល់ម៉ាស៊ីនជាក់លាក់មួយនៅលើបណ្តាញមូលដ្ឋាន ហើយមិនត្រូវបានបញ្ជូនបន្តទេ ដូច្នេះហើយមិនត្រូវបានប្រើទេ។

❖ សេចក្តីសង្ខេបនៃអាសយដ្ឋាន Class៖

CLASS	LEADING BITS	NET ID BITS	HOST ID BITS	NO, OF NETWORKS	ADDRESS PER NETWORK	START ADDRESS	END ADDRESS
CLASS A	0	8	24	2^7(128)	2^{24}(16,777,216)	0.0.0.0	127.255.255.255
CLASS B	10	16	16	2^{14}(16,384)	2^{16}(65,536)	128.0.0.0	191.255.255.255
CLASS C	110	24	8	2^{21}(2,097,152)	2^8(256)	192.0.0.0	223.255.255.255
CLASS D	1110	NOTE DEFINDED	NOTE DEFINDED	NOTE DEFINDED	NOTE DEFINDED	224.0.0.0	239.255.255.255
CLASS E	1111	NOTE DEFINDED	NOTE DEFINDED	NOTE DEFINDED	NOTE DEFINDED	240.0.0.0	255.255.255.255

រូបភាព ៦.១៣ សង្ខេបនៃ Class អាសយដ្ឋាន IP

៦.៤.៦ អាសយដ្ឋាន IP ជំនាន់ 6 (IPV6)

ពិធីការអ៊ីនធឺណិតជំនាន់ 6 (IPv6) គឺជាពិធីការអាសយដ្ឋានថ្មីដែលត្រូវបានរចនាឡើងដើម្បីរួមបញ្ចូលតម្រូវការដែលអាចមាននៃអ៊ីនធឺណិតនាពេលអនាគតដែលគេស្គាល់ថាជាកំណែអ៊ីនធឺណិតជំនាន់ទី២ ។ ពិធីការនេះដូចជំនាន់មុន IPv4 ដំណើរការលើNetwork Layer (ស្រទាប់ទី៣) រួមជាមួយនឹងការផ្តល់ជូននូវទំហំអាស័យដ្ឋានឡូជីខលដ៏ច្រើនសន្ធឹកសន្ធាប់ ពិធីសារនេះមានលក្ខណៈពិសេសជាច្រើនដែលដោះស្រាយបញ្ហាកង្វះ IPv4 ។

❖ ហេតុអ្វីបានជាកំណែ IP ថ្មី?

រហូតមកដល់ពេលនេះ IPv4 បានបង្ហាញឱ្យឃើញដោយខ្លួនវាថាជាពិធីការអាសយដ្ឋានដែលអាចដំណើរការបានដ៏រឹងមាំ ហើយបានបម្រើយើងអស់ជាច្រើនទសវត្សរ៍លើយន្តការបញ្ជូនកិច្ចខិតខំប្រឹងប្រែងដ៏ល្អបំផុតរបស់វា។ វាត្រូវបានរចនានៅដើមទសវត្សរ៍ទី 80 ហើយមិនទទួលបានការផ្លាស់ប្តូរគួរឱ្យកត់សម្គាល់ណាមួយបន្ទាប់ពីនោះ នៅពេលចាប់កំណើត អ៊ីនធឺណែតត្រូវបានកំណត់ត្រឹមតែសាកលវិទ្យាល័យមួយចំនួនប៉ុណ្ណោះសម្រាប់ការស្រាវជ្រាវរបស់ពួកគេ។ IPv4 មានប្រវែង 32 ប៊ីត ហើយផ្តល់ជូនប្រហែល 4,294,967,296 (2^{32}) អាសយដ្ឋាន។ ទំហំអាសយដ្ឋាននេះត្រូវបានចាត់ទុកថាច្រើនជាងគ្រប់គ្រាន់នៅពេលនោះដែលបានផ្តល់ឱ្យខាងក្រោមគឺជាចំណុចសំខាន់ៗដែលបានដើរតួនាទីយ៉ាងសំខាន់នៅក្នុងកំណើតនៃ IPv6៖

- អ៊ិនធឺណិតមានការកើនឡើងជាលំដាប់ ហើយទំហំអាសយដ្ឋានដែលអនុញ្ញាតដោយ IPv4 កំពុងតែជិតពេញ មានតម្រូវការដើម្បីឱ្យមានពិធីការដែលអាចបំពេញតម្រូវការនៃអាសយដ្ឋានអ៊ីនធឺណិតនាពេលអនាគតដែលរំពឹងថានឹងកើនឡើងដោយមិននឹកស្មានដល់។
- IPv4 ដោយខ្លួនឯងមិនផ្តល់មុខងារសុវត្ថិភាពណាមួយទេ។ ទិន្នន័យត្រូវតែត្រូវបានអ៊ិនគ្រីបជាមួយនឹងកម្មវិធីសុវត្ថិភាពមួយចំនួនផ្សេងទៀត មុនពេលត្រូវបានផ្ទើរនៅលើអ៊ីនធឺណិត។
- ការកំណត់អាទិភាពទិន្នន័យនៅក្នុង IPv4 មិនទាន់សម័យទេ ទោះបីជា IPv4 មានប៊ីតមួយចំនួនដែលត្រូវបានបម្រុងទុកសម្រាប់ប្រភេទសេវាកម្ម ឬគុណភាពនៃសេវាកម្មក៏ដោយ ពួកគេមិនផ្តល់មុខងារច្រើនទេ។
- អតិថិជនដែលបើក IPv4 អាចត្រូវបានកំណត់រចនាសម្ព័ន្ធដោយដៃ ឬត្រូវការយន្តការកំណត់រចនាសម្ព័ន្ធអាសយដ្ឋាន។ វាមិនមានយន្តការក្នុងការកំណត់ឧបករណ៍ដែលមានអាសយដ្ឋាន IP តែមួយគត់ជាសកលទេ។

❖ ប្រវត្តិសង្ខេប

បន្ទាប់ពីការអភិវឌ្ឍន៍របស់ IPv4 នៅដើមទសវត្សរ៍ទី 80 បណ្តុំអាសយដ្ឋាន IPv4 ដែលមានស្រាប់បានចាប់ផ្តើមធ្លាក់ចុះយ៉ាងឆាប់រហ័ស ដោយសារតម្រូវការសម្រាប់អាសយដ្ឋានកើនឡើងជា

លំដាប់ជាមួយនឹងអ៊ីនធឺណិត។ ដោយទទួលយកការដឹងជាមុនអំពីស្ថានភាពដែលអាចកើតឡើង IETF ក្នុងឆ្នាំ 1994 បានផ្តួចផ្តើមបង្កើតពិធីការអាសយដ្ឋានដើម្បីជំនួស IPv4 ។ វឌ្ឍនភាពនៃ IPv6 អាចត្រូវបានតាមដានដោយប្រើ RFC ដែលបានបោះពុម្ពផ្សាយ៖

- 1998 - RFC 2460 ៖ ពិធីសារមូលដ្ឋាន
- 2003 - RFC 2553 ៖ Basic Socket API
- 2003 - RFC 3315 ៖ DHCPv6
- 2004 - RFC 3775 ៖ Mobile IPv6
- 2004 - RFC 3697 ៖ លក្ខណៈបច្ចេកទេសនៃស្លាកលំហូរ
- 2006 - RFC 4291 ៖ អាសយដ្ឋានស្ថាបត្យកម្ម (ការកែប្រែ)
- 2006 - RFC 4294 ៖ តម្រូវការថ្នាំង

នៅថ្ងៃទី 06 ខែមិថុនា ឆ្នាំ 2012 ក្រុមហ៊ុនអ៊ីនធឺណិតយក្សមួយចំនួនបានជ្រើសរើសដាក់ Servers របស់ពួកគេនៅលើ IPv6 ។ បច្ចុប្បន្នពួកគេកំពុងប្រើយន្តការ Dual Stack ដើម្បីអនុវត្ត IPv6 ស្របជាមួយ IPv4 ។

❖ IPv6 - **អាសយដ្ឋាន និងការធ្វើទ្រង់ទ្រាយ**

មុននឹងណែនាំទម្រង់អាសយដ្ឋាន IPv6 យើងនឹងពិនិត្យមើលប្រព័ន្ធលេខគោលដប់ប្រាំមួយ។ លេខគោលដប់ប្រាំមួយគឺជាប្រព័ន្ធលេខទីតាំងដែលមានកាំ (គោល) នៃ 16។ ដើម្បីតំណាងឱ្យតម្លៃក្នុងទម្រង់ដែលអាចអានបាន ប្រព័ន្ធនេះប្រើនិមិត្តសញ្ញា 0-9 ដើម្បីតំណាងឱ្យតម្លៃពីសូន្យដល់ប្រាំបួន និង A-F ដើម្បីតំណាងឱ្យតម្លៃពីដប់ដល់ដប់ប្រាំ។ រាល់ខ្ទង់នៅក្នុងលេខគោលដប់ប្រាំមួយអាចតំណាងឱ្យតម្លៃពី 0 ដល់ 15 ។

DECIMAL	BINARY	HEXDECIMAL
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

រូបភាព ៦.១៨ លេខប្រព័ន្ធមូលដ្ឋាន

❖ សញ្ញាណ CIDR

ដូចដែលយើងនឹងឃើញក្នុងពេលឆាប់ៗនេះ IPv6 ប្រើអាសយដ្ឋានឋានានុក្រម សម្រាប់ហេតុផលនេះ IPv6 អនុញ្ញាតឱ្យមានសញ្ញាកាត់ ឬ CIDR ។ ជាឧទាហរណ៍ ខាងក្រោមនេះបង្ហាញពីរបៀបដែលយើងអាចកំណត់បុព្វបទនៃ 60 ប៊ីតដោយប្រើ CIDR ក្រោយមកយើងនឹងបង្ហាញពីរបៀបដែលអាសយដ្ឋាន IPv6 ត្រូវបានបែងចែកទៅជាបុព្វបទ និងបច្ច័យមួយ។ 22.1.2 លំហអាសយដ្ឋាន

- ចន្លោះអាសយដ្ឋាន IPv6 មាន 2^{128}
- អាសយដ្ឋាននេះគឺ 2^{96}

ចំនួនអាសយដ្ឋាន IPv4 ប្រាកដជាគ្មានការលុបអាសយដ្ឋានដូចដែលបានបង្ហាញទំហំនៃចន្លោះគឺ

340, 282, 366, 920, 938, 463, 374, 607, 431, 768, 211, 456។

❖ កំណត់សម្គាល់ចម្រុះ

ពេលខ្លះយើងឃើញតំណាងចម្រុះនៃអាសយដ្ឋាន IPv6 គោលដប់ប្រាំមួយ និងសញ្ញាចំនុចទសភាគ នេះគឺសមរម្យក្នុងអំឡុងពេលអន្តរកាលដែល IPv4 អាសយដ្ឋានត្រូវបានបង្កប់នៅក្នុងអាសយដ្ឋាន IPv6 (ជា 32 ប៊ីតខាងស្តាំបំផុត) ។ យើងអាចប្រើសញ្ញាណគោលដប់ប្រាំមួយសម្រាប់ផ្នែកខាងឆ្វេងបំផុតទាំងប្រាំមួយ និងសញ្ញាណចំនុចខ្ទង់បួនបៃជំនួសឱ្យផ្នែកពីរខាងស្តាំបំផុត។ ទោះយ៉ាងណាក៏ដោយ វាកើតឡើងនៅពេលដែលផ្នែកខាងឆ្វេងបំផុតទាំងអស់ ឬភាគច្រើននៃអាសយដ្ឋាន IPv6 គឺ 0s ។ ឧទាហរណ៍ អាសយដ្ឋាន (::130.24.24.18) គឺជាអាសយដ្ឋានស្របច្បាប់នៅក្នុង IPv6 ដែលការបង្កាប់សូន្យបង្ហាញថា 96 ប៊ីតខាងឆ្វេងបំផុតនៃអាសយដ្ឋានគឺសូន្យ។

❖ រចនាសម្ព័ន្ធអាសយដ្ឋាន

អាសយដ្ឋាន IPv6 ត្រូវបានធ្វើឡើងពី 128 ប៊ីត បែងចែកជាប្រាំបីប្លុក 16 ប៊ីត។ បន្ទាប់មកប្លុកនីមួយៗត្រូវបានបំប្លែងទៅជាលេខគោលដប់ប្រាំបួនខ្ទង់ដែលបំបែកដោយនិមិត្តសញ្ញាពោះវៀនធំ។

ជាឧទាហរណ៍ ការផ្តល់ជូនខាងក្រោមគឺជាអាសយដ្ឋាន IPv6 128 ប៊ីតដែលតំណាងក្នុងទម្រង់គោលពីរ ហើយបែងចែកជាប្រាំបីប្លុក 16 ប៊ីត៖

0010000000000001 0000000000000000 0011001000111000 1101111111100001
0000000001100011 0000000000000000 0000000000000000 1111111011111011

បន្ទាប់មកប្លុកនីមួយៗត្រូវបានបំប្លែងទៅជាលេខគោលដប់ប្រាំមួយ ហើយបំបែកដោយនិមិត្តសញ្ញា ':'៖

- 2001:0000:3238: DFE1:0063:0000:0000: FEFB

ទោះបីជាបន្ទាប់ពីបំប្លែងទៅជាទម្រង់គោលដប់ប្រាំមួយក៏ដោយ អាសយដ្ឋាន IPv6 នៅតែមានរយៈពេលយូរ។ IPv6 ផ្តល់នូវច្បាប់មួយចំនួនដើម្បីកាត់បន្ថយអាសយដ្ឋាន។

ច្បាប់មានដូចខាងក្រោម៖

- **ច្បាប់ទី១ ៖** បោះបង់សូន្យនាំមុខ៖ នៅក្នុងប្លុកទី 5, 0063 លេខ 0 នាំមុខពីរអាចត្រូវបានលុបចោល ដូចជា ៖ 2001:0000:3238: DFE1:63:0000:0000: FEFB
- **ច្បាប់ទី២ ៖** ប្រសិនបើប្លុកពីរ ឬច្រើនមានលេខសូន្យជាប់គ្នា សូមលុបវាចោលទាំងអស់ ហើយជំនួសពួកវាដោយសញ្ញា(::) 2001: 0000: 3238: DFE1: 63:FEFB

❖ តំណភ្ជាប់-អាសយដ្ឋានមូលដ្ឋាន

អាសយដ្ឋាន IPv6 ដែលត្រូបានកំណត់រចនាសម្ព័ន្ធដោយស្វ័យប្រវត្តិត្រូវបានគេស្គាល់ថាជាអាសយដ្ឋាន តំណភ្ជាប់-ក្នុងតំបន់ អាសយដ្ឋាននេះតែងតែចាប់ផ្តើមដោយ FE80។ 16 ប៊ីតដំបូងនៃអាសយដ្ឋានតំណ - មូលដ្ឋានតែងតែត្រូវបានកំណត់ទៅ 1111 1110 1000 0000 (FE80) 48 ប៊ីតបន្ទាប់ត្រូវបានកំណត់ទៅ 0 ។

1111 1110 1000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000	Interface ID

តំណភ្ជាប់-អាសយដ្ឋានក្នុងតំបន់ត្រូវបានប្រើសម្រាប់ការទំនាក់ទំនងក្នុងចំណោមម៉ាស៊ីន IPv6 នៅលើតំណភ្ជាប់ (ផ្នែកផ្សាយ) ប៉ុណ្ណោះ។ អាស័យដ្ឋានទាំងនេះមិនអាចដំណើរការបានទេ ដូច្នេះ រ៉ោតទ័រមិនដែលបញ្ជូនអាសយដ្ឋានទាំងនេះនៅខាងក្រៅតំណទេ។

៦.៥ ការកំណត់បណ្តាញ រ៉ោតទ័រ

នៅពេលដែលឧបករណ៍មានផ្លូវច្រើនដើម្បីទៅដល់គោលដៅមួយ វាតែងតែជ្រើសរើសផ្លូវមួយដោយវាចូលចិត្តជាងផ្លូវផ្សេងទៀត ដំណើរការជ្រើសរើសនេះត្រូវបានគេហៅថា នាំផ្លូវ។ ឧបករណ៍បណ្តាញពិសេសដែលកំណត់ផ្លូវត្រូវបានគេហៅថា រ៉ោតទ័រ ដែលអាចត្រូវបានធ្វើដោយប្រើដំណើរការកម្មវិធី។ រ៉ោតទ័រដែលមានមូលដ្ឋានលើកម្មវិធីមានមុខងារកំណត់ និងវិសាលភាពមានកំណត់។រ៉ោតទ័រត្រូវបានកំណត់ជាអចិន្ត្រៃយ៍ជាមួយនឹងផ្លូវលំនាំដើមមួយចំនួន។ ផ្លូវលំនាំដើមប្រាប់រ៉ោតទ័រកន្លែងដែលត្រូវបញ្ជូនបន្តកញ្ចប់ព័ត៌មាន ប្រសិនបើរកមិនឃើញផ្លូវសម្រាប់គោលដៅជាក់លាក់ណាមួយទេ ក្នុងករណីមានផ្លូវច្រើនដើម្បីទៅដល់គោលដៅដូចគ្នា។

រ៉ោតទ័រអាចធ្វើការសម្រេចចិត្តដោយផ្អែកលើព័ត៌មានខាងក្រោម៖

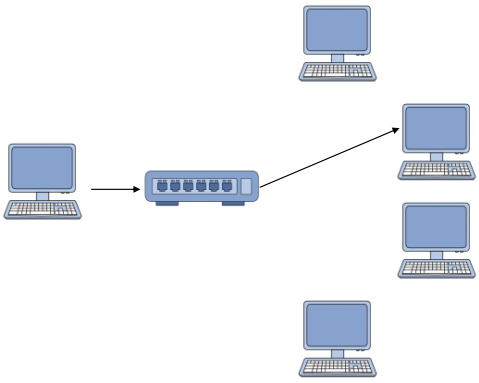
- Hop Count
- កម្រិតបញ្ជូន

- ម៉ែត្រ
- ប្រវែងបុព្វបទ
- ពន្យាពេល

ផ្លូវអាចត្រូវបានកំណត់រចនាសម្ព័ន្ធបិតិវន្ត ឬឌីណាមិកផ្លូវមួយអាចត្រូវបានកំណត់រចនាសម្ព័ន្ធឱ្យពេញចិត្តជាងផ្លូវផ្សេងទៀត។

ក. ការកំណត់ផ្លូវ Unicast

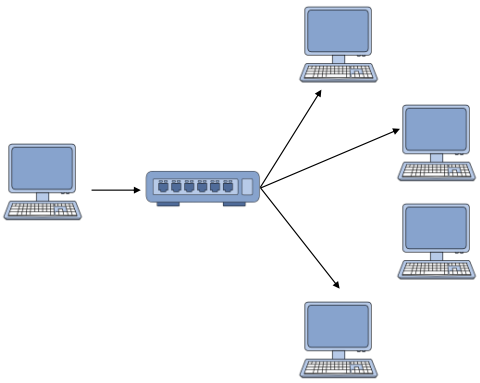
អ៊ីនធឺណែត និងអ៊ីនធឺណែតភាគច្រើន ដែលគេស្គាល់ថាជាទិន្នន័យ unicast ឬចរាចរ unicast ត្រូវបានផ្ញើជាមួយគោលដៅជាក់លាក់មួយ។ ការបញ្ជូនទិន្នន័យ unicast នៅលើអ៊ីនធឺណិតត្រូវបានគេហៅថាការកំណត់ផ្លូវ unicast ។ វាជាទម្រង់ផ្លូវសាមញ្ញបំផុតព្រោះទិសដៅត្រូវបានគេស្គាល់រួចហើយ ដូច្នេះ រ៉ោតទ័រត្រូវរកមើលតារាងនាំផ្លូវ ហើយបញ្ជូនកញ្ចប់ព័ត៌មានទៅ ហបបន្ទាប់។



រូបភាព ៦.១៥ ការកំណត់ផ្លូវ Unicast

ខ. ការកំណត់ផ្លូវ Multicast

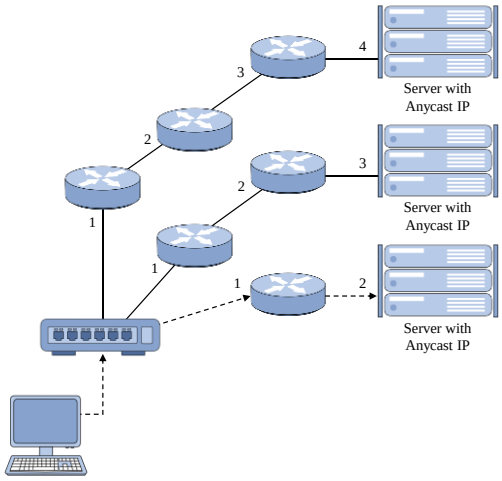
ការកំណត់ផ្លូវ Multicast គឺជាករណីពិសេសនៃការបញ្ជូនបន្តដែលមានភាពខុសគ្នា និងបញ្ហាប្រឈមសំខាន់ៗ នៅក្នុងការបញ្ជូនបន្ត កញ្ចប់ព័ត៌មានត្រូវបានផ្ញើទៅកាន់ថ្នាំងទាំងអស់ ទោះបីជាពួកគេមិនចង់ក៏ដោយ។ ប៉ុន្តែនៅក្នុង ការកំណត់ផ្លូវ Multicast ទិន្នន័យត្រូវបានផ្ញើទៅតែ nodes ដែលចង់ទទួល packets ប៉ុណ្ណោះ។ រ៉ោតទ័រត្រូវតែដឹងថាមានថ្នាំងដែលចង់ទទួលបានកញ្ចប់ព័ត៌មានច្រើន (ឬស្ទើម)។ មានតែពេលនោះទេដែលវាគួរទៅមុខ។ ការកំណត់ផ្លូវ Multicast ដំណើរការលើពិធីការមែកធាងដើម្បីជៀសវាងការរង្វិលការកំណត់ផ្លូវ Multicast ក៏ប្រើបច្ចេកទេសបញ្ជូនបន្តផ្លូវបញ្ច្រាស ដើម្បីស្វែងរក និងបោះបង់ការស្ទួន និងរង្វិលជុំ។



រូបភាព ៦.១៦ ការកំណត់ផ្លូវ Multicast

គ. ការកំណត់ផ្លូវ Anycast

ការបញ្ជូនបន្តរបស់កញ្ចប់ព័ត៌មាន Anycast គឺជាយន្តការមួយដែលម៉ាស៊ីនច្រើនអាចមានអាសយដ្ឋានឡូជីខលដូចគ្នា។នៅពេលដែលកញ្ចប់ព័ត៌មានដែលកំណត់សម្រាប់អាសយដ្ឋានឡូជីខលនេះត្រូវបានទទួល វាត្រូវបានផ្ញើទៅម៉ាស៊ីនដែលនៅជិតបំផុតនៅក្នុងក្បួនបណ្តាញនាំផ្លូវ។



រូបភាព ៦.១៧ ការកំណត់ផ្លូវ Anycast

ការកំណត់ផ្លូវ Anycast ត្រូវបានធ្វើដោយជំនួយពីម៉ាស៊ីនមេ DNS នៅពេលណាដែលកញ្ចប់ព័ត៌មាន Anycast ត្រូវបានទទួល វាសួរ DNS កន្លែងដែលវាគួរតែត្រូវបានផ្ញើ។ DNS ផ្តល់អាសយដ្ឋាន IP និង IP ដែលនៅជិតបំផុតដែលបានកំណត់នៅលើវា។

៦.៥.១ ពិធីការនាំផ្លូវ Unicast

វាសំដៅទៅលើពិធីការដែលស្វែងរកផ្លូវទំនាក់ទំនងជាមួយនឹងប្រវែងដ៏ល្អប្រសើរបំផុតនៅលើរ៉ោតទ័រទំនាក់ទំនង Unicast ធ្វើបច្ចុប្បន្នភាពផ្លូវទំនាក់ទំនងដ៏ល្អប្រសើរ ដោយជូនដំណឹងគ្នាទៅវិញទៅមកអំពីការផ្លាស់ប្តូរនៅក្នុងអ៊ីនធឺណិតដោយប្រើពិធីការនាំផ្លូវ។ មានពិធីការនាំផ្លូវពីរប្រភេទដែលអាចរកបានដើម្បីបញ្ជូនកញ្ចប់ព័ត៌មាន unicast៖

❖ ពិធីការបញ្ជូនវិចម័រចម្ងាយ

វិចទ័រចម្ងាយ គឺជាពិធីការកំណត់ផ្លូវសាមញ្ញដែលធ្វើការសម្រេចចិត្តលើចំនួននៃការលោតរវាងប្រភពនិងទិសដៅ។ ផ្លូវដែលមានចំនួនម៉ាស៊ីនតូចជាងត្រូវបានចាត់ទុកថាជាផ្លូវល្អបំផុតរាល់រ៉ោតទ័រទាំងអស់ផ្សព្វផ្សាយនូវការកំណត់ផ្លូវល្អបំផុតរបស់ខ្លួនទៅកាន់រ៉ោតទ័រផ្សេងទៀត។ ទីបំផុតរ៉ោតទ័រទាំងអស់បង្កើតក្បួនបណ្តាញរបស់ពួកគេដោយផ្អែកលើការផ្សាយពាណិជ្ជកម្មនៃរ៉ោតទ័រ។

❖ ស្តាប់ពិធីការកំណត់ផ្លូវរដ្ឋ

ភ្ជាប់ពិធីការកំណត់ផ្លូវរដ្ឋគឺជាពិធីការដែលមានភាពស្មុគស្មាញជាង វិចទ័រចម្ងាយបន្តិច។ វាពិចារណាស្ថានភាពនៃតំណភ្ជាប់នៃរ៉ោតទ័រទាំងអស់នៅក្នុងបណ្តាញមួយ។ បច្ចេកទេសនេះជួយផ្លូវបង្កើតក្រាហ្វធម្មតានៃបណ្តាញទាំងមូល។ បន្ទាប់មក រ៉ោតទ័រទាំងអស់គណនាផ្លូវល្អបំផុតរបស់ពួកគេសម្រាប់គោលបំណងកំណត់ផ្លូវ។ ឧទាហរណ៍ បើកផ្លូវខ្លីបំផុតដំបូង (OSPF) និងប្រព័ន្ធកម្រិតមធ្យមទៅប្រព័ន្ធកម្រិតមធ្យម (ISIS)។

៦.៥.២ ពិធីការនាំផ្លូវ Multicast

ពិធីការនាំផ្លូវ Unicast ប្រើក្រាហ្វខណៈពេលដែលពិធីការបញ្ជូនផ្លូវច្រើនប្រើដើមឈើ ពោលគឺកាត់ដើមឈើ ដើម្បីជៀសវាងរង្វិលជុំ។ មែកធាងដ៏ប្រសើរបំផុតត្រូវបានគេហៅថា ដើមឈើដែលមានផ្លូវខ្លីបំផុត។

- DVMRP ៖ ពិធីការនាំផ្លូវវិចទ័រពីចម្ងាយ
- MOSPF ៖ Multicast បើកផ្លូវខ្លីបំផុតដំបូង
    - PIM ៖ ពិធីសារឯករាជ្យ ពិធីការ Multicast ត្រូវបានគេប្រើជាទូទៅឥឡូវនេះ។
    - PIM Dense៖ ទម្រង់នេះប្រើដើមឈើផ្អែកលើប្រភពវាត្រូវបានប្រើក្នុងបរិយាកាសក្រាស់ដូចជា LAN ។

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះអ្នកបានសិក្សាអំពី៖

- នៅចុងទស្សវត្សរ៍ឆ្នាំ 1970 ISO បានធ្វើកម្មវិធីមួយដើម្បីអភិវឌ្ឍស្តង់ដារទូទៅ និងវិធីសាស្ត្រនៃបណ្តាញ។
- នៅឆ្នាំ 1973 ប្រព័ន្ធផ្លាស់ប្តូរកញ្ចប់ពិសោធន៍នៅចក្រភពអង់គ្លេសបានកំណត់តម្រូវការសម្រាប់កំណត់ពិធីការកម្រិតខ្ពស់
- នៅឆ្នាំ 1983 គំរូ OSI ត្រូវបានបម្រុងទុកដំបូងដើម្បីជាការបញ្ជាក់លម្អិតនៃចំណុចប្រទាក់និម្មិត។
- នៅក្នុងឆ្នាំ 1984 ស្ថាបត្យកម្ម OSI ត្រូវបានអនុម័តជាផ្លូវការដោយ ISO ជាស្តង់ដារអន្តរជាតិ។
- ការងារអ៊ីនធឺណិត៖ នេះគឺជាការទទួលខុសត្រូវចម្បងរបស់ស្រទាប់បណ្តាញ។ វាផ្តល់នូវការតភ្ជាប់ឡូជីខលរវាងបណ្តាញជាច្រើនប្រភេទ។
- **អាសយដ្ឋាន៖** អាសយដ្ឋានមានសារៈសំខាន់ណាស់ក្នុងការស្គាល់ឧបករណ៍នីមួយៗនៅលើអ៊ីនធឺណិតជាពិសេស។
- **ការនាំផ្លូវ៖** មានឫសដែលអាចធ្វើបានជាច្រើនពីប្រភពមួយទៅទិសដៅមួយ ហើយមួយគឺត្រូវជ្រើសរើស។ ក្បួនដោះស្រាយការនាំផ្លូវត្រូវបានបង្កើតឡើងដើម្បីស្វែងរកផ្លូវដែលមានប្រសិទ្ធភាពបំផុតរវាងប្រភពសារ និងមជ្ឈមណ្ឌលគោលដៅ។
- **ការវេចខ្ចប់៖** វាបែងចែកកញ្ចប់ព័ត៌មានដែលលេចធ្លោជាងទៅជាកញ្ចប់តូច ប្រសិនបើវាលើសពីទិន្នន័យទូលំទូលាយបំផុតពីស្រទាប់តំណទិន្នន័យ។ នេះត្រូវបានគេស្គាល់ថាជាការវេចខ្ចប់។
- **ការប្តូរទិន្នន័យ៖** នីតិវិធីនៃការផ្លាស់ប្តូរកញ្ចប់ព័ត៌មាន (ប្តូរទិន្នន័យ) ពីប្រភពទៅមជ្ឈមណ្ឌលគោលដៅ ត្រូវបានគេស្គាល់ថាជាការប្តូរទិន្នន័យ។
- **ការគ្រប់គ្រងការកកស្ទះ៖** ការកកស្ទះនៅក្នុងបណ្តាញអាចលេចឡើងនៅពេលដែលកញ្ចប់បណ្តាញ (ផ្ទុកលើសទម្ងន់)។ កញ្ចប់ព័ត៌មានជាច្រើនត្រូវបានបញ្ជូនទៅបណ្តាញដែលខ្ពស់ជាងសមត្ថភាពរបស់វា។
- នៅក្នុងបណ្តាញណាមួយ លេខសម្គាល់ម៉ាស៊ីនត្រូវតែមានតែមួយគត់សម្រាប់បណ្តាញ
- លេខសម្គាល់ម៉ាស៊ីនដែលប៊ីតទាំងអស់ត្រូវបានកំណត់ទៅ 0 មិនអាចកំណត់បានទេ ព្រោះលេខសម្គាល់ម៉ាស៊ីននេះតំណាងឱ្យលេខសម្គាល់បណ្តាញនៃអាសយដ្ឋាន IP ។

សំណួរ

១. តើសេវាបណ្តាញគឺជាអ្វី?

២. តើ OSI ម៉ូដែលជាអ្វី?

៣. ចូរពន្យល់ពីគុណសម្បត្តិ និងគុណវិបត្តិនៃ OSI ម៉ូដែល ។

៤. តើការបញ្ជូនតបណ្តាញមានប៉ុន្មានប្រភេទ?ហើយមានអ្វីខ្លះ?

៥. តើអាសយដ្ឋាន IP មានប៉ុន្មាន Class ? ហើយមានអ្វីខ្លះ?

៦. តើអ្វីជាភាពខុសគ្នារវាង IPv4 និង IPv6?

ការអនុវត្តន៍ទី៦

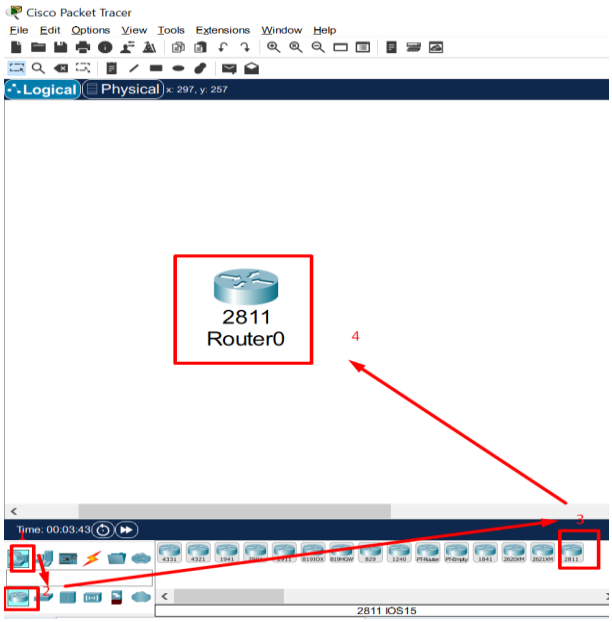
ការកំណត់រ៉ោតទ័រនៅក្នុងកញ្ចប់តាមដានឧបករណ៍បណ្តាញបានបញ្ជូនកញ្ចប់ទិន្នន័យរវាងបណ្តាញកុំព្យូទ័រទីតាំងនៃកញ្ចប់ព័ត៌មានត្រូវបានស្រង់ចេញ ផ្លូវល្អបំផុតទៅកាន់ទីតាំងនោះត្រូវបានបញ្ជាក់ ហើយកញ្ចប់ទិន្នន័យត្រូវបានបញ្ជូនបន្តតាមផ្លូវនេះទៅកាន់ឧបករណ៍បន្ទាប់។ នៅពេលនេះ ផ្លូវល្អបំផុតជាទូទៅគឺជាផ្លូវដែលអនុញ្ញាតឱ្យមានទំនាក់ទំនងលឿនបំផុត ដូច្នេះជាទូទៅវាអាចជាចម្ងាយខ្លីបំផុត។ ទោះបីជាវាអាចឆ្លងកាត់ផ្លូវល្បឿនលឿនក៏ដោយ និយាយឱ្យសាមញ្ញវាគឺជាឧបករណ៍ដែលដើរតួជាអ្នកបញ្ជូនតរវាងបណ្តាញផ្សេងៗគ្នា។

ក. គោលបំណងនៃការអនុវត្តនេះ

- គោលបំណង៖ រ៉ោតទ័រភ្ជាប់បណ្តាញផ្សេងៗ។
- ស្រទាប់៖រ៉ោតទ័រដំណើរការទៅស្រទាប់រាងកាយស្រទាប់ភ្ជាប់ទិន្នន័យ និង *Network Layer*។
- ការងារ៖ រ៉ោតទ័រកំណត់ផ្លូវល្អបំផុតសម្រាប់កញ្ចប់ព័ត៌មានដែលកុំព្យូទ័រគោលដៅ (ទទួល)
- កំណត់៖ ការកំណត់ផ្លូវបិតិវន្ត និងការកំណត់ថាមវន្ត

ខ. កំណត់រចនាសម្ព័ន្ធ រ៉ោតទ័រ បណ្តាញនៅក្នុង Packet Tracer

១. ការបញ្ចូលរ៉ោតទ័រ

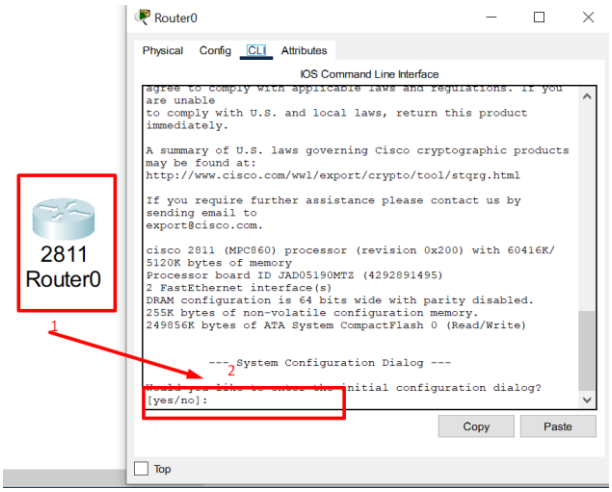


ក.ចុចលើ] ឧបករណ៍បញ្ចប់)Network Devices)[

ខ. ជ្រើសរើសយក Routers (Model 2811)

គ. បន្ទាប់មក ចុចលើ ‘2811’ Router ហើយអូសទម្លាក់លើផ្ទាំងកិច្ចការ

២. ចូលទៅកាន់រ៉ោតទ័រ CLI

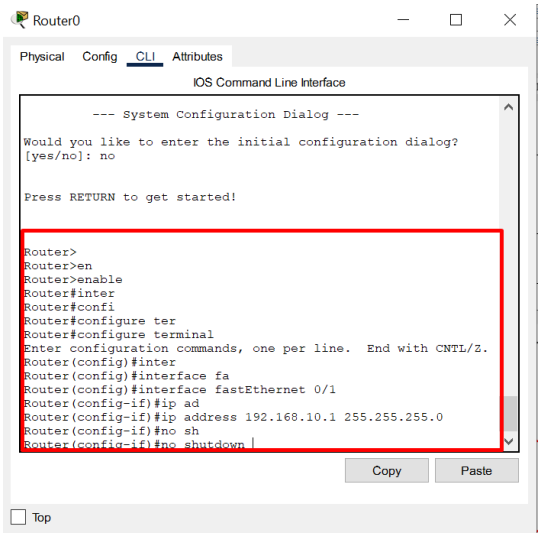


ក.ចុចលើ Routers (Model 2811

ខ. ជ្រើសរើសយក CLI

គ. បន្ទាប់មកសរសេរពាក្យ “no” → enter

ឧទាហរណ៍៖ ការកំណត់ IP លើ រ៉ោតទ័រ

ការប្រើប្រាស់ CLI	បង្ហាញកិច្ចការបង្ហាញ
Router>enable Router# configure terminal Router(config)#interface fastEthernet 0/1 Router(config-if)#ip address 192.168.10.1 255.255.255.0 Router(config-if)#no shutdown	

គ. សន្ទេបការអនុវត្តន៍

រ៉ោតទ័រទាញយកផ្លូវសម្រាប់កញ្ចប់ព័ត៌មានដែលត្រូវឆ្លងកាត់រវាងបណ្តាញដាច់ដោយឡែកពីគ្នាដោយឡូជីខល ឬរាងកាយដើម្បីស្វែងរកផ្លូវដែលល្អបំផុត ហើយបញ្ជូនកញ្ចប់ព័ត៌មានទៅបណ្តាញផ្សេងទៀត។

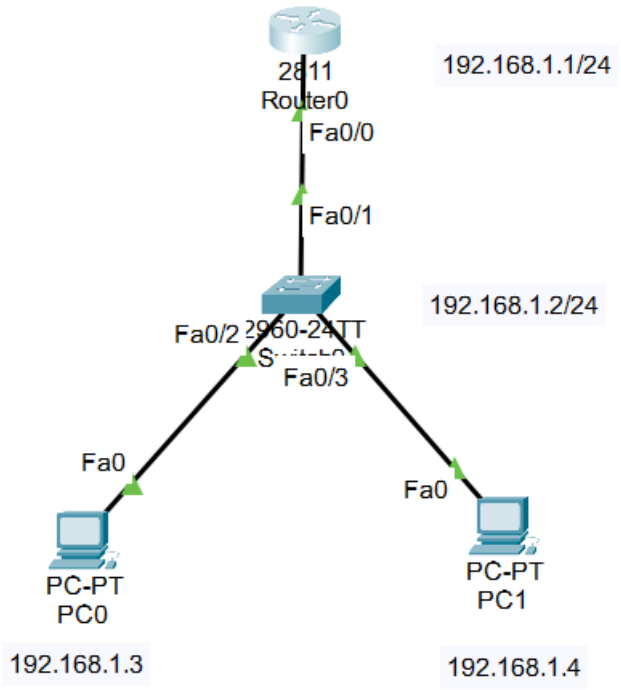
ឃ.កិច្ចការស្រាវជ្រាវ

កិច្ចការ៖ កំណត់រចនាសម្ព័ន្ធរ៉ោតទ័របណ្តាញខាងក្រោម.

ក. កំណត់ IP Address Router : 192.168.1.1 ហើយ Subnet Mask : 255.255.255.0

ខ. កំណត់ IP Switch : 192.168.1.2 ហើយ Subnet Mask : 255.255.255.0

គ. កំណត់ IP របស់របស់កុំព្យូទ័រដូចរូបខាងក្រោម ហើយអាចទំនាក់ទំនងគ្នាបាន។



ជំពូកទី ៧

Transport Layer

Transport Layer ផ្តល់នូវការតភ្ជាប់ពីគ្នាទៅវិញទៅមក និងពីចម្ងាយរវាងដំណើរការពីរនៅលើម៉ាស៊ីនពីចម្ងាយ Transport Layer យកទិន្នន័យពីស្រទាប់ខាងលើ ហើយបន្ទាប់មកបំបែកវាទៅជាផ្នែកដែលមានទំហំតូចជាង លេខបៃនីមួយៗ ហើយប្រគល់វាទៅស្រទាប់ខាងក្រោម Network Layer សម្រាប់ចែកចាយ។ នៅក្នុងបណ្តាញកុំព្យូទ័រ ស្រទាប់ដឹកជញ្ជូនគឺជាការបែងចែកគំនិតនៃវិធីសាស្ត្រនៅក្នុងស្ថាបត្យកម្មស្រទាប់នៃពិធីការនៅក្នុងបណ្តាញនៅក្នុងឈុតពិធីការអ៊ីនធឺណិត និងគំរូ OSI ។ ពិធីការនៃស្រទាប់នេះផ្តល់សេវាទំនាក់ទំនងពីចុងដល់ចុងសម្រាប់កម្មវិធីវាផ្តល់សេវាកម្មដូចជាការទំនាក់ទំនងតម្រង់ទិសការតភ្ជាប់ ភាពជឿជាក់ ការគ្រប់គ្រងលំហូរ និងការពហុគុណ។

ជំពូកទី៧ នេះអ្នកនឹងរៀនអំពី៖

៧.១ ការណែនាំអំពី Transport Layer

Transport Layer ផ្តល់នូវសេវាកម្មទំនាក់ទំនងដែលភ្ជាប់អ្នកផ្ញើ និងអ្នកទទួលនៅក្នុងសមាសធាតុបណ្តាញហានានុក្រម និងពិធីការក្នុងដំណើរការកុំព្យូទ័រ និងការទំនាក់ទំនងអេឡិចត្រូនិច។ Transport Layer ផ្តល់នូវសេវាកម្មងាយស្រួលដូចជាការគាំទ្រស្ត្រីមទិន្នន័យដែលតម្រង់ទិសការតភ្ជាប់ ភាពជឿជាក់ ការគ្រប់គ្រងលំហូរ និងការពហុគុណ។ Transport Layer រួមមានគំរូយោង TCP/IP មូលដ្ឋាននៃអ៊ីនធឺណិត និង Open Systems Interconnection (OSI) ដែលជាគំរូបណ្តាញទូទៅ ម៉ូដែលទាំងពីរនេះកំណត់ Transport Layer ខុសគ្នាបន្តិចបន្តួច ពិពណ៌នាជាចម្បងអំពីគំរូ TCP/IP ពិធីសារដឹកជញ្ជូនដែលល្បីជាងគេគឺពិធីការត្រួតពិនិត្យការបញ្ជូន (TCP) ដែលប្រើគ្រោងការណ៍ដឹកជញ្ជូនដែលផ្តោតលើការតភ្ជាប់ពិធីការកម្មវិធីទិន្នន័យអ្នកប្រើប្រាស់(UDP) ក៏ត្រូវបានគេប្រើប្រាស់សម្រាប់ការដឹកជញ្ជូនត្រង់ជាងមុនផងដែរ។ ស្រទាប់បន្ទាប់នៅក្នុង OSI ម៉ូដែលត្រូវបានគេហៅថា Transport Layer ម៉ូឌុល និងនីតិវិធីទាំងអស់អំពីទិន្នន័យ ឬការដឹកជញ្ជូនទិន្នន័យត្រូវបានចាត់ថ្នាក់ទៅក្នុងស្រទាប់នេះដូចស្រទាប់ផ្សេងទៀតទាំងអស់។

ស្រទាប់នេះទាក់ទងជាមួយ Transport Layer ដូចគ្នានៃម៉ាស៊ីនពីចម្ងាយ៖

- Transport Layer គឺជាស្រទាប់ទី៤ ពីខាងលើ។
- តួនាទីចម្បងនៃ Transport Layer គឺផ្តល់សេវាទំនាក់ទំនងដោយផ្ទាល់ទៅដំណើរការកម្មវិធីដែលកំពុងដំណើរការលើម៉ាស៊ីនផ្សេងៗគ្នា។
- Transport Layer ផ្តល់នូវទំនាក់ទំនងឡូជីខលរវាងដំណើរការកម្មវិធីដែលកំពុងដំណើរការលើម៉ាស៊ីនផ្សេងៗគ្នា។
- ទោះបីជាដំណើរការកម្មវិធីនៅលើម៉ាស៊ីនផ្សេងគ្នាមិនត្រូវបានភ្ជាប់ជារូបវន្តក៏ដោយ ដំណើរការកម្មវិធីប្រើទំនាក់ទំនងឡូជីខលដែលផ្តល់ដោយ Transport Layer ដើម្បីផ្ញើសារទៅគ្នាទៅវិញទៅមក។
- ពិធីការ Transport Layer ត្រូវបានអនុវត្តនៅក្នុងប្រព័ន្ធចុងក្រោយ ប៉ុន្តែមិនមែននៅក្នុងរ៉ោតទ័របណ្តាញទេ។
- បណ្តាញកុំព្យូទ័រផ្តល់ពិធីការច្រើនជាងមួយទៅកម្មវិធីបណ្តាញ។ ឧទាហរណ៍ TCP និង UDP គឺជាពិធីការ Transport Layer ពីរដែលផ្តល់សំណុំសេវាកម្មផ្សេងគ្នាដល់ Network Layer
- ពិធីការ Transport Layer ទាំងអស់ផ្តល់នូវសេវា multiplexing/demultiplexing។ វាផ្តល់ជូននូវសេវាកម្មផ្សេងទៀតដូចជាការធ្វើទិន្នន័យដែលអាចទុកចិត្តបាន កម្រិតបញ្ជូន និងការធានាការពន្យារពេល។
- កម្មវិធីនីមួយៗនៅក្នុងស្រទាប់កម្មវិធីអាចផ្ញើសារដោយប្រើ TCP ឬ UDP ។

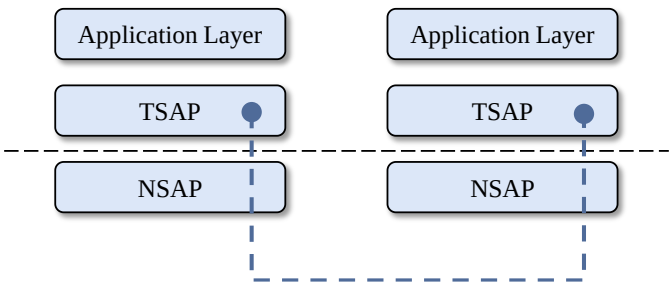
- កម្មវិធីទំនាក់ទំនងដោយប្រើពិធីការទាំងពីរនេះ TCP និង UDP នឹងទាក់ទងជាមួយពិធីការអ៊ីនធឺណិតនៅក្នុងស្រទាប់អ៊ីនធឺណិត។
- កម្មវិធីអាចអាន និងសរសេរទៅកាន់ Transport Layer។ ដូច្នេះការប្រាស្រ័យទាក់ទងគ្នាគឺជាដំណើរការពីរផ្លូវ។

៧.១.១ តួនាទី និងមុខងារ

- ស្រទាប់នេះគឺជាស្រទាប់ទីមួយដែលបំបែកទិន្នន័យព័ត៌មានដែលផ្តល់ដោយស្រទាប់កម្មវិធីទៅជាឯកតាតូចៗហៅថា Segments វារាប់រាល់បៃក្នុងផ្នែក និងរក្សាគណនេយ្យរបស់វា។
- ស្រទាប់នេះធានាថាទិន្នន័យត្រូវតែទទួលបានក្នុងលំដាប់ដូចគ្នាដែលវាត្រូវបានផ្ញើ។
- ស្រទាប់នេះផ្តល់នូវការបញ្ជូនទិន្នន័យពីចុងដល់ចុងរវាងម៉ាស៊ីនដែលអាចឬមិនមែនជារបស់បណ្តាញរងដូចគ្នា។
- ដំណើរការម៉ាស៊ីនមេទាំងអស់ដែលមានបំណងទំនាក់ទំនងតាមបណ្តាញត្រូវបានបំពាក់ដោយចំណុចចូលដំណើរការសេវាដឹកជញ្ជូនល្បី (TSAP) ដែលត្រូវបានគេស្គាល់ថាជាលេខច្រក។

៧.១.២ ការប្រាស្រ័យទាក់ទងពីចុងដល់ចប់

ដំណើរការនៅលើម៉ាស៊ីនមួយកំណត់ម៉ាស៊ីនដូចគ្នារបស់វានៅលើបណ្តាញពីចម្ងាយដោយប្រើ TSAPs ដែលត្រូវបានគេស្គាល់ផងដែរថាជាលេខច្រក។ TSAPs ត្រូវបានកំណត់យ៉ាងល្អ ហើយដំណើរការដែលព្យាយាមទំនាក់ទំនងជាមួយមិត្តភ័ក្តិរបស់ខ្លួនដឹងពីរឿងនេះជាមុន។



រូបភាព ៧.១ ការប្រាស្រ័យទាក់ទងពីចុងដល់ចប់

ឧទាហរណ៍ នៅពេលដែលម៉ាស៊ីនភ្ញៀវ DHCP ចង់ទំនាក់ទំនងជាមួយម៉ាស៊ីនមេ DHCP ពីចម្ងាយ វាតែងតែស្នើសុំលេខច្រក 67 ។ នៅពេលដែលម៉ាស៊ីនភ្ញៀវ DNS ចង់និយាយជាមួយម៉ាស៊ីនមេពីចម្ងាយ វាតែងតែស្នើសុំលេខច្រក 53 (UDP) ។

ពិធីការ Transport Layer សំខាន់ពីរគឺ៖

- **ពិធីការត្រួតពិនិត្យការបញ្ជូន៖** វាផ្តល់នូវទំនាក់ទំនងដែលអាចទុកចិត្តបានរវាងម៉ាស៊ីនពីរ។
- **ពិធីការកម្មវិធីទិន្នន័យអ្នកប្រើប្រាស់៖** វាផ្តល់នូវការទំនាក់ទំនងដែលមិនអាចជឿទុកចិត្តបានរវាងម៉ាស៊ីនទាំងពីរ។

៧.២ ពិធីការត្រួតពិនិត្យការបញ្ជូន

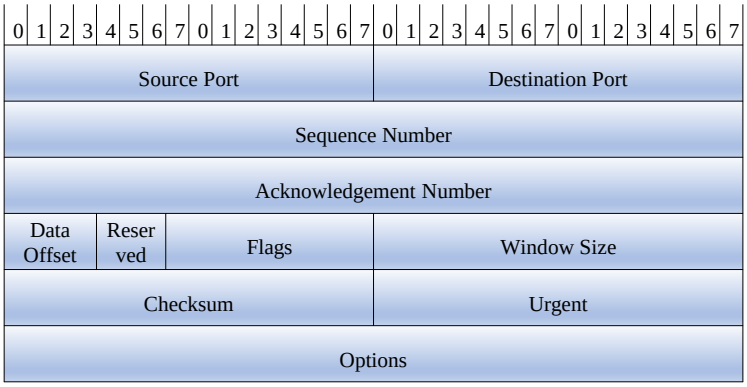
ពិធីសារត្រួតពិនិត្យការបញ្ជូន(TCP) គឺជាពិធីការដ៏សំខាន់បំផុតមួយនៃពិធីការអ៊ីនធឺណិត វាគឺជាពិធីការដែលត្រូវបានប្រើប្រាស់យ៉ាងទូលំទូលាយបំផុតសម្រាប់ការបញ្ជូនទិន្នន័យនៅក្នុងបណ្តាញទំនាក់ទំនងដូចជាអ៊ីនធឺណិត។

❖ លក្ខណៈពិសេស

- TCP គឺជាពិធីការដែលអាចទុកចិត្តបាននោះគឺអ្នកទទួលតែងតែផ្ញើការទទួលស្គាល់ជាវិជ្ជមាន ឬអវិជ្ជមានអំពីកញ្ចប់ទិន្នន័យទៅកាន់អ្នកផ្ញើ ដើម្បីឱ្យអ្នកផ្ញើមានតម្រុយច្បាស់លាស់អំពីថាតើកញ្ចប់ទិន្នន័យបានទៅដល់គោលដៅឬក៏ត្រូវបញ្ជូនឡើងវិញ។
- TCP ធានាថាទិន្នន័យទៅដល់គោលដៅដែលបានគ្រោងទុកក្នុងលំដាប់ដូចគ្នាដែលវាត្រូវបានផ្ញើ។
- TCP គឺផ្តោតលើការតភ្ជាប់ TCP តម្រូវឱ្យបង្កើតការតភ្ជាប់រវាងចំណុចដាច់ស្រយាលពីរ មុនពេលបញ្ជូនទិន្នន័យពិតប្រាកដ។
- TCP ផ្តល់នូវយន្តការត្រួតពិនិត្យកំហុស និងការស្តារឡើងវិញ។
- TCP ផ្តល់ការទំនាក់ទំនងពីចុងដល់ចុង។
- TCP ផ្តល់ការត្រួតពិនិត្យលំហូរ និងគុណភាពនៃសេវាកម្ម។
- TCP ដំណើរការក្នុងរបៀបម៉ាស៊ីនភ្ញៀវពីចំណុចទៅចំណុច។
- TCP ផ្តល់នូវម៉ាស៊ីនមេ duplex ពេញលេញ ពោលគឺ វាអាចបំពេញតួនាទីទាំងអ្នកទទួល និងអ្នកផ្ញើ។

❖ បឋមកថា

ប្រវែងនៃបឋមកថា TCP គឺយ៉ាងហោចណាស់ 20 បៃវែង និងអតិបរមា 60 បៃ។



រូបភាព ៧.២ ប្រវែងនៃបឋមកថា TCP

- **ច្រកប្រភព (16 ប៊ីត)៖** វាកំណត់ច្រកប្រភពនៃដំណើរការកម្មវិធីនៅលើឧបករណ៍បញ្ជូន។
- **ច្រកគោលដៅ (16 ប៊ីត)៖** វាកំណត់ច្រកគោលដៅនៃដំណើរការកម្មវិធីនៅលើឧបករណ៍ដែលទទួលវា។
- **លេខលំដាប់ (32-ប៊ីត)៖** ចំនួនលំដាប់នៃបៃទិន្នន័យនៃផ្នែកក្នុងវគ្គមួយ។
- **លេខការទទួលស្គាល់ (32 ប៊ីត)៖** នៅពេលដែលទង់ ACK ត្រូវបានកំណត់ លេខនេះមានលេខលំដាប់ខាងក្រោមនៃបៃទិន្នន័យដែលរំពឹងទុក ហើយដំណើរការជាការទទួលស្គាល់នៃទិន្នន័យពីមុនដែលទទួលបាន។
- **ទិន្នន័យអុហ្វសិត (4 ប៊ីត)៖** វាលនេះបង្កប់ន័យទំហំនៃបឋមកថា TCP (ពាក្យ 32 ប៊ីត) និងអុហ្វសិតទិន្នន័យនៅក្នុងកញ្ចប់ព័ត៌មានបច្ចុប្បន្ននៅក្នុងផ្នែក TCP ទាំងមូល។
- **បម្រុងទុក (3 ប៊ីត)៖** បម្រុងទុកសម្រាប់ការប្រើប្រាស់នាពេលអនាគត ហើយទាំងអស់ត្រូវបានកំណត់ទៅសូន្យតាមលំនាំដើម។

❖ ធង់ជាតិ

- NS៖ ដំណើរការផ្តល់សញ្ញាការជូនដំណឹងការកកស្ទះច្បាស់លាស់ប្រើណាន់ផលបូកប៊ីត។
- CWR៖ នៅពេលដែលម៉ាស៊ីនទទួលបានកញ្ចប់ព័ត៌មានដែលមានសំណុំ ECE ប៊ីត វាកំណត់ការកកស្ទះវិនដូបានកាត់បន្ថយដើម្បីទទួលស្គាល់ថា ECE បានទទួល។
- ECE៖ វាមានអត្ថន័យពីរ៖

- ប្រសិនបើប៊ីត SYN ច្បាស់ដល់ 0 នោះ ECE មានន័យថា កញ្ចប់ព័ត៌មាន IP មានសំណុំប៊ីត CE (បទពិសោធន៍កកស្ទះ) របស់វា។
- ប្រសិនបើប៊ីត SYN ត្រូវបានកំណត់ទៅ 1 ECE មានន័យថាឧបករណ៍នេះមានសមត្ថភាព ECT ។

- URG៖ បង្ហាញថាវាលទ្រនិចបន្ទាន់មានទិន្នន័យសំខាន់ៗ ហើយគួរតែត្រូវបានដំណើរការ។
- ACK៖ វាបង្ហាញថាវាលទទួលស្គាល់មានសារៈសំខាន់ ប្រសិនបើ ACK ត្រូវបានជម្រះដល់ 0 វាបង្ហាញថាកញ្ចប់ព័ត៌មានមិនមានការទទួលស្គាល់ទេ។
- PSH៖ នៅពេលកំណត់ វាគឺជាសំណើទៅកាន់ស្ថានីយ៍ទទួលដើម្បី PUSH ទិន្នន័យ (ភ្លាមៗ នៅពេលដែលវាមកដល់) ទៅកាន់កម្មវិធីទទួលដោយមិនបាច់ផ្ទុកវា។
- RST ៖ កំណត់ទង់ឡើងវិញមានលក្ខណៈពិសេសដូចខាងក្រោម៖
  - វាត្រូវបានប្រើដើម្បីបដិសេធការភ្ជាប់ចូល។
  - វាត្រូវបានប្រើដើម្បីបដិសេធផ្នែកមួយ។
  - វាត្រូវបានប្រើដើម្បីចាប់ផ្តើមការតភ្ជាប់ឡើងវិញ។
- SYN៖ ទង់នេះត្រូវបានប្រើដើម្បីរៀបចំការតភ្ជាប់រវាងម៉ាស៊ីន។
- FIN៖ ទង់នេះត្រូវបានប្រើដើម្បីបញ្ចេញការតភ្ជាប់ ហើយមិនមានទិន្នន័យណាមួយត្រូវបានផ្លាស់ប្តូរទៀតទេបន្ទាប់ពីនោះ។ ដោយសារកញ្ចប់ព័ត៌មានដែលមានទង់ SYN និង FIN មានលេខលំដាប់ ពួកគេត្រូវបានដំណើរការតាមលំដាប់លំដោយត្រឹមត្រូវ។
- ទំហំវីនដូ៖ វាលនេះត្រូវបានប្រើសម្រាប់ការគ្រប់គ្រងលំហូររវាងស្ថានីយពីរ និងបង្ហាញពីបរិមាណនៃសតិបណ្តោះអាសន្ន (គិតជាបៃ) ដែលអ្នកទទួលបានបែងចែកសម្រាប់ផ្នែកមួយ ពោលគឺចំនួនទិន្នន័យដែលអ្នកទទួលរំពឹង។
- Checksum៖ វាលនេះមាន checksum នៃបឋមកថា ទិន្នន័យ និងបឋមកថា Pseudo ។
- Urgent Pointer៖ វាចង្អុលទៅបៃទិន្នន័យបន្ទាន់ ប្រសិនបើទង់ URG ត្រូវបានកំណត់ទៅ 1 ។
- ជម្រើស៖ វាជួយសម្រួលជម្រើសបន្ថែមដែលមិនត្រូវបានគ្របដណ្តប់ដោយបឋមកថាធម្មតា។ វាលជម្រើសតែងតែត្រូវបានពិពណ៌នាជាពាក្យ 32 ប៊ីត ប្រសិនបើវាលនេះផ្ទុកទិន្នន័យតិចជាង 32 ប៊ីត នោះ ទ្រនាប់ត្រូវបានប្រើដើម្បីគ្របដណ្តប់ប៊ីតដែលនៅសល់ដើម្បីឈានដល់ព្រំដែន 32 ប៊ីត។

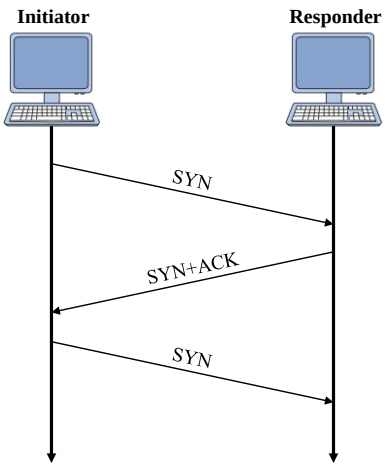
❖ អាសយដ្ឋានច្រក

ការទំនាក់ទំនង TCP រវាងម៉ាស៊ីនពីចម្ងាយពីរប្រើលេខច្រក (TSAPs)លេខច្រកអាចមានចាប់ពី 0 ដល់ 65535 ដែលបែងចែកជា៖

- ច្រកប្រព័ន្ធ (0 - 1023)
- ច្រកអ្នកប្រើប្រាស់ (1024 - 49151)
- ច្រកឯកជន/ចាមវ៉ន្ត (49152 - 65535)

៧.៣ ការគ្រប់គ្រងការតភ្ជាប់

ការទំនាក់ទំនង TCP ដំណើរការក្នុងគំរូម៉ាស៊ីនមេ/អតិថិជន ម៉ាស៊ីនភ្ញៀវចាប់ផ្តើមការតភ្ជាប់ ហើយម៉ាស៊ីនមេទទួលយក ឬបដិសេធវា ការចាប់ដៃបីផ្លូវត្រូវបានប្រើសម្រាប់ការគ្រប់គ្រងការតភ្ជាប់។



រូបភាព ៧.៣ ការគ្រប់គ្រងការតភ្ជាប់

៧.៣.១ ការបង្កើត

ម៉ាស៊ីនភ្ញៀវផ្ញើចផ្តើមការតភ្ជាប់ ហើយផ្ញើផ្នែកជាមួយលេខលំដាប់។ ម៉ាស៊ីនមេទទួលស្គាល់វាជាមួយនឹងលេខលំដាប់របស់វា និង ACK នៃផ្នែករបស់អតិថិជន ដែលលើសពីលេខលំដាប់ របស់អតិថិជនបន្ទាប់ពីទទួលបាន ACK នៃផ្នែករបស់វា អតិថិជនទទួលស្គាល់ការឆ្លើយតបរបស់ម៉ាស៊ីនមេ។

❖ ចេញផ្សាយ

ទាំងម៉ាស៊ីនមេ និងម៉ាស៊ីនភ្ញៀវអាចផ្ញើផ្នែក TCP ដែលមានទង់ FIN កំណត់ទៅ ១ នៅពេលដែលចុងបញ្ចប់ទទួលឆ្លើយតបដោយការទទួលស្គាល់ FIN ទិសដៅនៃការទំនាក់ទំនង TCP នោះត្រូវបានបិទ ហើយការតភ្ជាប់ត្រូវបានបញ្ចេញ។

❖ ការគ្រប់គ្រងកម្រិតបញ្ជូន

TCP ប្រើគំនិតនៃទំហំបង្ហួចដើម្បីបំពេញតម្រូវការសម្រាប់ការគ្រប់គ្រងកម្រិតបញ្ជូនទំហំបង្ហួចប្រាប់អ្នកផ្ញើនៅចុងដាច់ស្រយាលពីចំនួនផ្នែកបៃទិន្នន័យដែលអ្នកទទួលនៅចុងនេះអាចទទួលបាន។ TCP ប្រើដំណាក់កាលចាប់ផ្តើមយឺតដោយប្រើទំហំបង្ហួចមួយ និងបង្កើនទំហំបង្ហួចដោយអិចស្ប៉ូណង់ស្យែលបន្ទាប់ពីការទំនាក់ទំនងជោគជ័យនីមួយៗ។

ឧទាហរណ៍៖ អតិថិជនប្រើបង្ហួចទំហំពីរហើយផ្ញើទិន្នន័យ ២បៃ នៅពេលដែលការទទួលស្គាល់នៃផ្នែកនេះត្រូវបានទទួល ទំហំបង្ហួចត្រូវបានកើនឡើងទ្វេដងដល់ ៤ ហើយផ្នែកដែលបានបញ្ជូនបន្ទាប់ដែលផ្ញើនឹងមានប្រវែងទិន្នន័យ ៤បៃ។ នៅពេលដែលការទទួលស្គាល់ផ្នែកទិន្នន័យ ៤បៃត្រូវបានទទួល អតិថិជនកំណត់ទំហំនៃបង្ហួចទៅ ៨ ហើយដូច្នេះនៅលើ។

❖ ការគ្រប់គ្រងកំហុស និងការគ្រប់គ្រងលំហូរ

TCP ប្រើលេខច្រកដើម្បីដឹងថាដំណើរការកម្មវិធីអ្វីដើម្បីប្រគល់ផ្នែកទិន្នន័យ វាក៏ប្រើលេខលំដាប់ដើម្បីធ្វើសមកាលកម្មខ្លួនវាជាមួយម៉ាស៊ីនពីចម្ងាយផងដែរ។ ផ្នែកទិន្នន័យទាំងអស់ត្រូវបានផ្ញើ និងទទួលជាមួយនឹងលេខលំដាប់ អ្នកផ្ញើដឹងថាផ្នែកទិន្នន័យចុងក្រោយមួយណាត្រូវបានទទួលដោយអ្នកទទួល នៅពេលដែលវាទទួលបាន ACK ។ អ្នកទទួលដឹងអំពីផ្នែកចុងក្រោយដែលផ្ញើដោយអ្នកផ្ញើដោយយោងទៅលេខលំដាប់នៃកញ្ចប់ព័ត៌មានដែលទទួលបានថ្មីៗនេះ ប្រសិនបើលេខលំដាប់នៃផ្នែកដែលទទួលបានថ្មីៗនេះមិនត្រូវគ្នានឹងលេខលំដាប់ដែលអ្នកទទួលកំពុងរំពឹងទុកនោះទេវាក៏ត្រូវបានគេបោះបង់ចោល ហើយ NACK ត្រូវបានបញ្ជូនមកវិញ។ ប្រសិនបើសមាសធាតុពីរមកដល់ជាមួយលេខលំដាប់ដូចគ្នា តម្លៃពេលវេលា TCP ត្រូវបានប្រៀបធៀបដើម្បីធ្វើការសម្រេចចិត្ត។

❖ Multiplexing

បច្ចេកទេសនៃការរួមបញ្ចូលគ្នារវាងស្ទ្រីមទិន្នន័យពីរ ឬច្រើននៅក្នុងសម័យមួយត្រូវបានគេហៅថា Multiplexing ។ នៅពេលដែលម៉ាស៊ីនភ្ញៀវ TCP ចាប់ផ្តើមការតភ្ជាប់ជាមួយ ម៉ាស៊ីនបម្រើ វាតែងតែសំដៅទៅលើលេខច្រកដែលបានកំណត់យ៉ាងល្អដែលបង្ហាញពីដំណើរការកម្មវិធី ម៉ាស៊ីនភ្ញៀវប្រើលេខច្រកដែលបានបង្កើតដោយចៃដន្យពីក្រុមលេខច្រកឯកជន។ ដោយប្រើ TCP Multiplexing អតិថិជនអាចទំនាក់ទំនងជាមួយដំណើរការកម្មវិធីជាច្រើនក្នុងវគ្គតែមួយ។

ឧទាហរណ៍៖ ប្រសិនបើអតិថិជនស្នើសុំទំព័របណ្តាញដែលមានទិន្នន័យប្រភេទផ្សេងៗដូចជា (HTTP, SMTP, FTP) លើសអាចត្រូវបានជៀសវាង។

៧.៣.២ ការត្រួតពិនិត្យការកកស្ទះ

នៅពេលដែលទិន្នន័យមួយចំនួនធំត្រូវបានបញ្ចូលទៅក្នុងប្រព័ន្ធដែលមិនអាចគ្រប់គ្រងវាបានការកកស្ទះកើតឡើង។ TCP គ្រប់គ្រងការកកស្ទះដោយប្រើយន្តការ បង្អួច TCP កំណត់ទំហំបង្អួចប្រាប់ចុងម្ខាងទៀតថាតើផ្នែកទិន្នន័យត្រូវផ្ញើប៉ុន្មាន។ TCP អាចប្រើក្បួនដោះស្រាយបីសម្រាប់ការគ្រប់គ្រងការកកស្ទះ៖

- ការកើនឡើងបន្ថែម ការថយចុះពហុគុណ
- ចាប់ផ្តើមយឺត
- អស់ពេលប្រតិកម្ម

ក. ការគ្រប់គ្រងកម្មវិធីកំណត់ពេលវេលា

TCP ប្រើប្រភេទកម្មវិធីកំណត់ម៉ោងផ្សេងៗគ្នា ដើម្បីគ្រប់គ្រង និងគ្រប់គ្រងកិច្ចការផ្សេងៗ៖

❖ រក្សាពេលវេលាកំណត់ពេលវេលា

- កម្មវិធីកំណត់ម៉ោងនេះគឺជាចំណុចមួយត្រូវបានប្រើដើម្បីពិនិត្យមើលភាពត្រឹមត្រូវ និងសុពលភាពនៃការតភ្ជាប់។
- នៅពេលដែលពេលវេលារក្សាជីវិតផុតកំណត់ ម្ចាស់ផ្ទះផ្ញើការស៊ើបអង្កេតដើម្បីពិនិត្យមើលថាតើមានការតភ្ជាប់ឬអត់។

❖ កម្មវិធីកំណត់ពេលវេលាបញ្ជូនបន្ត

- កម្មវិធីកំណត់ម៉ោងនេះរក្សាផ្នែកនៃទិន្នន័យដែលបានផ្ញើ។
- ផ្នែកទិន្នន័យត្រូវបានផ្ញើម្តងទៀតប្រសិនបើការទទួលស្គាល់ទិន្នន័យដែលបានបញ្ជូនមិនទទួលបានក្នុងរយៈពេលបញ្ជូនឡើងវិញ។

❖ កម្មវិធីកំណត់ពេលវេលាបន្ត

- ម៉ាស៊ីនទាំងពីរអាចផ្អាកផ្នែកនៃ TCP ដោយផ្ញើទំហំបង្អួច0។
- ដើម្បីបន្តវេន ម្ចាស់ផ្ទះត្រូវតែផ្ញើទំហំបង្អួចជាមួយនឹងតម្លៃសំខាន់មួយចំនួនទៀត។
- ប្រសិនបើផ្នែកនេះមិនដែលទៅដល់ចុងម្ខាងទៀត នោះចុងទាំងពីរអាចនឹងរង់ចាំគ្នាទៅវិញទៅមកដោយគ្មានកំណត់។
- នៅពេលដែលកម្មវិធីកំណត់ពេលវេលាបន្តផុតកំណត់ ម្ចាស់ផ្ទះនឹងផ្ញើទំហំបង្អួចរបស់វាឡើងវិញដើម្បីឱ្យភាគីម្ខាងទៀតដឹង។

- កម្មវិធីកំណត់ពេលវេលាបន្តជួយជៀសវាងការជាប់គាំងក្នុងការទំនាក់ទំនង។

❖ **ពេលខេណ រង់ចាំ**

- បន្ទាប់ពីបានចេញផ្សាយការតភ្ជាប់ ម្ចាស់ផ្ទះទាំងពីររង់ចាំពេលវេលាកំណត់-រង់ចាំ ដើម្បីបញ្ចប់ការតភ្ជាប់ទាំងស្រុង។
- នេះពេលវេលាដែលបានធានាថាចុងម្ខាងទៀតបានទទួលការទទួលស្គាល់នៃសំណើបញ្ចប់ការតភ្ជាប់របស់វា។
- ការអស់ពេលអាចមានរយៈពេលអតិបរមា ២៤0 វិនាទី (៤នាទី)។

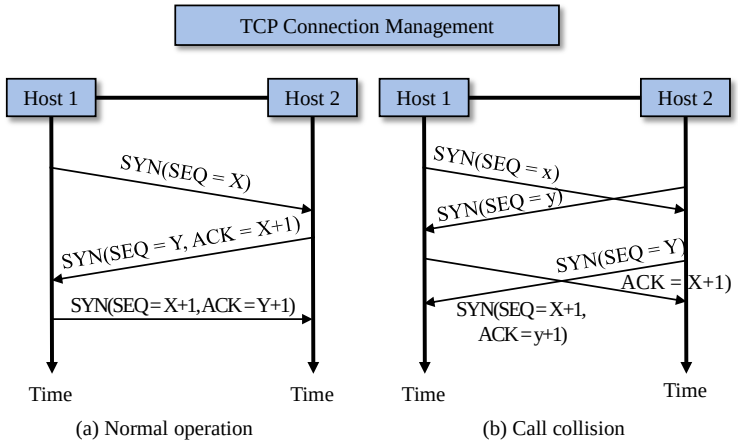
ខ. ការខើបឡើងវិញនៃការគាំង

TCP គឺជាពិធីការដែលអាចទុកចិត្តបានវាផ្តល់លេខលំដាប់សម្រាប់បៃនីមួយៗដែលបានផ្ទៀនៅក្នុងផ្នែក។ វាផ្តល់នូវយន្តការមតិត្រឡប់ ពោលគឺនៅពេលដែលម៉ាស៊ីនទទួលបានកញ្ចប់ព័ត៌មាន វាត្រូវបានចងភ្ជាប់ទៅនឹង ACK ដែលកញ្ចប់ព័ត៌មានដែលមានលេខលំដាប់ដូចខាងក្រោមរំពឹងទុក ប្រសិនបើវាមិនមែនជាផ្នែកចុងក្រោយ។ នៅពេលដែលម៉ាស៊ីនមេ TCP គាំងទំនាក់ទំនងពាក់កណ្តាលផ្លូវ ហើយចាប់ផ្តើមដំណើរការរបស់វាឡើងវិញ វាផ្ទៀការផ្សាយ TPDU ទៅម៉ាស៊ីនទាំងអស់របស់វាបន្ទាប់មកម៉ាស៊ីនអាចផ្ទៀផ្នែកទិន្នន័យចុងក្រោយ ដែលមិនធ្លាប់មានការទទួលស្គាល់។

៧.៤ ការគ្រប់គ្រងការតភ្ជាប់ TCP

ការតភ្ជាប់ត្រូវបានបង្កើតឡើងនៅក្នុង TCP ដោយប្រើការចាប់ដៃបីផ្លូវដែលបានពិភាក្សាពីមុន ដើម្បីបង្កើតការតភ្ជាប់ភាគីម្ខាងនិយាយថាម៉ាស៊ីនមេ ស្តាប់នៅដោយអសកម្មសម្រាប់តំណចូល ដោយអនុវត្តការស្តាប់ និងទទួលយកបុព្វកាល ទាំងកំណត់ផ្នែកផ្សេងទៀតជាក់លាក់ ឬគ្មាននរណាម្នាក់ជាពិសេស។ ភាគីម្ខាងទៀតអនុវត្តការតភ្ជាប់បឋមដែលបញ្ជាក់ច្រក I/O ដែលវាចង់ចូលរួមទំហំផ្នែក TCP អតិបរមាដែលមាន។ ជម្រើសផ្សេងទៀតមានដូចជា ទិន្នន័យឯកជនមួយចំនួន ភ្ជាប់បុព្វកាលបញ្ជូនផ្នែក TCP ដោយបើក SYN bit ហើយបិទ ACK ហើយរង់ចាំការឆ្លើយតប។

លំដាប់នៃផ្នែក TCP ដែលបានផ្ទៀនៅក្នុងករណីធម្មតាដូចបានបង្ហាញក្នុងរូបភាពខាងក្រោម ៖



រូបភាព ៧.៤ ការគ្រប់គ្រងការតភ្ជាប់ TCP

នៅពេលដែលផ្នែកដែលផ្ញើដោយម៉ាស៊ីន១ ទៅដល់គោលដៅពោលគឺ ម៉ាស៊ីន ២ មុនពេលទៅដល់នោះម៉ាស៊ីនមេ ទទួលពិនិត្យដើម្បីមើលថា តើមានដំណើរការដែលបានធ្វើស្តាប់នៅលើច្រកដែល បានផ្តល់ឱ្យក្នុងវាលច្រកទិសដៅ។ ប្រសិនបើមិនមានទេ វាផ្ញើការឆ្លើយតបជាមួយ RST ប៊ីត ដើម្បីបដិសេធការភ្ជាប់បើមិនដូច្នោះទេ វាគ្រប់គ្រងផ្នែក TCP ទៅដំណើរការចុះបញ្ជី ដែលអាចទទួលយក ឬបដិសេធ ការតភ្ជាប់។

ការប៉ះទង្គិចគ្នា

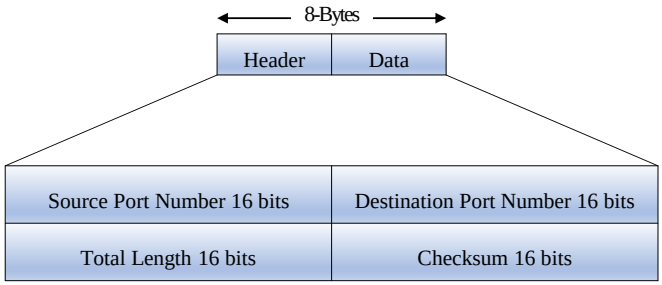
ប្រសិនបើម៉ាស៊ីនពីរព្យាយាមបង្កើតការតភ្ជាប់ក្នុងពេលដំណាលគ្នារវាងរន្ធទាំងពីរដូចគ្នា នោះលំដាប់នៃព្រឹត្តិការណ៍ត្រូវបានបង្ហាញក្នុងរូបភាពក្រោមកាលៈទេសៈបែបនេះ។ ការតភ្ជាប់តែមួយគត់ត្រូវបានបង្កើតឡើង វាមិនអាចជ្រើសរើសតំណទាំងពីរបានទេ ដោយសារចំណុចបញ្ចប់របស់ពួកគេកំណត់ទំនាក់ទំនង។ ឧបមាថាការរៀបចំដំបូងមានលទ្ធផលក្នុងសេចក្តីយោងដែលបានកំណត់ដោយ (x, y) ហើយការតភ្ជាប់ទីពីរក៏ត្រូវបានបញ្ចេញដែរ ក្នុងករណីនោះមានតែការបញ្ចូលកន្ទុយប៉ុណ្ណោះដែលនឹងត្រូវបានធ្វើឡើង ពោលគឺសម្រាប់ (x, y) សម្រាប់លេខលំដាប់ដំបូង គ្រោងការណ៍ផ្នែកលើនាឡិកាត្រូវបានប្រើ ដោយជីពចរមកក្រោយរៀងរាល់ ៤មីក្រូវិនាទី។ ដើម្បីធានាសុវត្ថិភាពបន្ថែមនៅពេលម៉ាស៊ីនគាំង វាអាចនឹងមិនដំណើរការឡើងវិញក្នុងរយៈពេលមួយវិនាទី ដែលជាអាយុកាលអតិបរមានៃកញ្ចប់ព័ត៌មាន នេះគឺដើម្បីប្រាកដថាមិនមានកញ្ចប់ព័ត៌មានពីការតភ្ជាប់ពីមុនត្រូវកំពុងដើរជុំវិញ។

៧.៥ ពិធីការកម្មវិធីធនន័យអ្នកប្រើប្រាស់

ពិធីការទិន្នន័យកម្មវិធីអ្នកប្រើប្រាស់ (UDP) គឺជាពិធីការ Transport Layer វាគឺជាពិធីការដែលគ្មានការតភ្ជាប់ និងមិនអាចទុកចិត្តបាន ដែលគ្មានការគ្រប់គ្រងលំហូរ និងកំហុស។ UDP ប្រើលេខច្រកដើម្បីគុណទិន្នន័យពីស្រទាប់កម្មវិធី UDP គឺជាពិធីការដ៏សាមញ្ញមួយ វាមានតម្លៃតិចជាងមុន។ ឧបមាថាដំណើរការមួយចង់ផ្ញើសារតូចមួយ បន្ទាប់មក UDP នឹងត្រូវការអន្តរកម្មតិចតួចបំផុតរវាងអ្នកផ្ញើ និងអ្នកទទួល បើប្រៀបធៀបទៅនឹងពិធីការត្រួតពិនិត្យការបញ្ជូន (TCP)។

៧.៥.១ អ្នកប្រើប្រាស់ UDP ទម្រង់ទិន្នន័យ

អ្នកប្រើប្រាស់កញ្ចប់ UDP datagram មានទំហំថេរនៃ 8 បៃ។



រូបភាព ៧.៥ អ្នកប្រើប្រាស់ UDP ទម្រង់ទិន្នន័យ

❖ បឋមកថា UDP

វាជាបឋមកថាថេរ ៨ បៃ នៃ ៨បៃដំបូងនៃ datagram មានព័ត៌មានបឋមកថាចាំបាច់ ហើយនៅសល់មានទិន្នន័យវាលលេខច្រក UDP នីមួយៗមាន ១៦ប៊ីត ឬ ២បៃវែង។ លេខច្រកជួយបែងចែកសំណើរបស់អ្នកប្រើប្រាស់ ឬដំណើរការផ្សេងៗ។

- លេខច្រកប្រភព៖ លេខច្រកប្រភពត្រូវបានប្រើដោយដំណើរការដែលដំណើរការលើម៉ាស៊ីនប្រភព លេខច្រកនេះមានប្រវែង ១៦ប៊ីត ឬ ២ បៃ។
- លេខច្រកគោលដៅ៖ លេខច្រកទិសដៅនេះមានប្រវែង ១៦ប៊ីត ហើយត្រូវបានប្រើប្រាស់ដោយដំណើរការដែលកំពុងដំណើរការនៅលើម៉ាស៊ីនគោលដៅ។
- ប្រវែងគឺជាវាល ១៦ ប៊ីត ដែលកំណត់ប្រវែងសរុបនៃទិន្នន័យអ្នកប្រើប្រាស់ បឋមកថា និងទិន្នន័យ។
- Checksum ៖ វាល Checksum ត្រូវបានប្រើដើម្បីរកឃើញកំហុសលើ Datagram ដែលបានប្រើទាំងមូល។

❖ កម្មវិធី UDP

- UDP ត្រូវបានប្រើសម្រាប់ការទំនាក់ទំនងការស្នើសុំ ឆ្លើយតបដោយត្រង់ៗនៃទិន្នន័យដែលមានចំនួនតិចតួច ដោយលុបបំបាត់កង្វល់ទាក់ទងនឹងការគ្រប់គ្រងកំហុស ឬលំហូរនៃកញ្ចប់ព័ត៌មាន។
- វាស័ក្តិសមសម្រាប់ multicasting ព្រោះ UDP ដំណើរការល្អជាមួយការប្តូរកញ្ចប់ព័ត៌មាន។
- វាជាពិធីការធ្វើបច្ចុប្បន្នភាពផ្លូវមួយដូចជាពិធីការព័ត៌មានផ្លូវការ។
- UDP គឺជាកម្មវិធីតាមពេលវេលាជាក់ស្តែង ដែលព័ត៌មានចាំបាច់ត្រូវបញ្ជូនយ៉ាងលឿនរហ័ស និងរលូន។

៧.៥.២ លក្ខណៈពិសេសនៃ UDP

ពិធីការទិន្នន័យអ្នកប្រើប្រាស់ (UDP) គឺជាពិធីការទំនាក់ទំនង Transport Layer ត្រង់បំផុតដែលមាននៅក្នុងឈុតពិធីការ TCP/IP ។ វាពាក់ព័ន្ធនឹងចំនួនអប្បបរមានៃយន្តការទំនាក់ទំនង UDP ត្រូវបានគេនិយាយថាជាពិធីការដឹកជញ្ជូនដែលមិនអាចទុកចិត្តបាន ប៉ុន្តែវាប្រើសេវា IP ដែលផ្តល់នូវយន្តការចែកចាយដែលប្រឹងប្រែងបំផុត។ នៅក្នុង UDP អ្នកទទួលមិនបង្កើតការទទួលស្គាល់នៃកញ្ចប់ព័ត៌មានដែលបានទទួលទេ ហើយអ្នកផ្ញើមិនរង់ចាំការបង្ហាញណាមួយនៃកញ្ចប់ព័ត៌មានដែលបានផ្ញើនោះទេ ការខ្វះខាតនេះធ្វើឱ្យពិធីការនេះមិនគួរឱ្យទុកចិត្ត ក៏ដូចជាងាយស្រួលក្នុងការដំណើរការ។

❖ តម្រូវការរបស់ UDP

តើហេតុអ្វីបានជាយើងត្រូវការពិធីការ UDP ដែលមិនគួរឱ្យទុកចិត្តដើម្បីដឹកជញ្ជូនទិន្នន័យ? យើងដាក់ពង្រាយ UDP ដែលកញ្ចប់ព័ត៌មានទទួលស្គាល់ចែករំលែកកម្រិតបញ្ជូនដ៏សំខាន់ រួមជាមួយនឹងទិន្នន័យជាក់ស្តែង។ ឧទាហរណ៍ កញ្ចប់ព័ត៌មានរាប់ពាន់ត្រូវបានបញ្ជូនបន្តទៅកាន់អ្នកប្រើប្រាស់របស់ពួកគេក្នុងការផ្សាយវីដេអូ។ ការទទួលស្គាល់កញ្ចប់ព័ត៌មានទាំងអស់គឺមានបញ្ហា ហើយអាចមានការខ្ជះខ្ជាយកម្រិតបញ្ជូនដ៏ធំ យន្តការចែកចាយដ៏ល្អបំផុតនៃពិធីការ IP មូលដ្ឋានធានានូវកិច្ចខិតខំប្រឹងប្រែងដ៏ល្អបំផុតក្នុងការចែកចាយកញ្ចប់ព័ត៌មានរបស់វា។ ទោះយ៉ាងណាក៏ដោយ បើទោះបីជាកញ្ចប់ព័ត៌មានមួយចំនួននៅក្នុងការផ្សាយវីដេអូត្រូវបានបាត់បង់ក៏ដោយ ផលប៉ះពាល់គឺមិនមានគ្រោះថ្នាក់ទេ ហើយអាចត្រូវបានមិនអើពើយ៉ាងងាយស្រួល ការបាត់បង់កញ្ចប់ព័ត៌មានមួយចំនួននៅក្នុងវីដេអូ និងសំឡេង ពេលខ្លះមិនមានការកត់សម្គាល់ទេ។

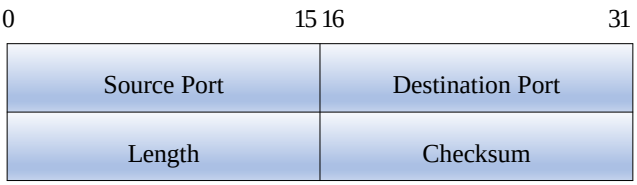
❖ លក្ខណៈពិសេស

- UDP ត្រូវបានប្រើប្រាស់នៅពេលដែលការទទួលស្គាល់ទិន្នន័យមិនមានសារៈសំខាន់ណាមួយឡើយ។
- UDP គឺជាពិធីការសមរម្យសម្រាប់ទិន្នន័យដែលហូរក្នុងទិសដៅមួយ។
- UDP គឺសាមញ្ញ និងសមរម្យសម្រាប់ការទំនាក់ទំនងតាមសំណួរ។
- UDP មិនផ្តោតលើការតភ្ជាប់ទេ។

- UDP មិនផ្តល់យន្តការគ្រប់គ្រងការកកស្ទះទេ។
- UDP មិនធានាការចែកចាយទិន្នន័យដែលបានស្នើសុំ។

❖ **បឋមកថា** UDP

បឋមកថា UDP គឺសាមញ្ញដូចមុខងាររបស់វា៖



រូបភាព ៧.៦ មុខងារបឋមកថា UDP

បឋមកថា UDP មានប៉ារ៉ាម៉ែត្រសំខាន់ៗចំនួនបួន៖

- **ច្រកប្រភព៖** ព័ត៌មាន ១៦ប៊ីតនេះ ត្រូវបានប្រើដើម្បីកំណត់អត្តសញ្ញាណច្រកប្រភពនៃកញ្ចប់ព័ត៌មាន។
- **ច្រកគោលដៅ៖** ព័ត៌មាន ១៦ ប៊ីតនេះត្រូវបានប្រើដើម្បីកំណត់អត្តសញ្ញាណសេវាកម្រិតកម្មវិធីនៅលើម៉ាស៊ីនគោលដៅ។
- **ប្រវែង៖** វាលប្រវែងបញ្ជាក់ប្រវែងទាំងមូលនៃកញ្ចប់ព័ត៌មាន UDP រួមទាំងបឋមកថា។ វាជាវាល ១៦ ប៊ីតដែលមានតម្លៃអប្បបរមា ៨ ប៊ីត ពោលគឺទំហំនៃបឋមកថា UDP ខ្លួនឯង។
- **Checksum៖** វាលនេះរក្សាទុកតម្លៃ checksum ដែលបង្កើតដោយអ្នកផ្ញើមុនពេលផ្ញើ IPv4 មានវាលនេះជាជម្រើស ដូច្នេះនៅពេលដែលវាល checksum មិនមានតម្លៃណាមួយទេ វាត្រូវបានបង្កើត 0 ហើយប៊ីតទាំងអស់របស់វាត្រូវបានកំណត់ទៅសូន្យ។

❖ **កម្មវិធី** UDP

នេះគឺជាកម្មវិធីមួយចំនួនដែល UDP ត្រូវបានប្រើដើម្បីបញ្ជូនទិន្នន័យ៖

- សេវាឈ្មោះដែន
- ពិធីការគ្រប់គ្រងបណ្តាញសាមញ្ញ
- ពិធីការផ្ទេរឯកសារមិនសំខាន់
- ពិធីសារព័ត៌មានផ្លូវ

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះអ្នកបានសិក្សាអំពី៖

- Transport Layer គឺជាស្រទាប់ទីមួយដែលបំបែកទិន្នន័យព័ត៌មានដែលផ្តល់ដោយស្រទាប់កម្មវិធីទៅជាឯកតាតូចៗហៅថាចម្រៀករាល់បែក្នុងផ្នែក និងរក្សាគណនេយ្យរបស់វា។
- Transport Layer ធានាថាទិន្នន័យត្រូវតែទទួលបានក្នុងលំដាប់ដូចគ្នាដែលវាត្រូវបានផ្ញើ
- Transport Layer នេះផ្តល់នូវការបញ្ជូនទិន្នន័យពីចុងដល់ចុងរវាងម៉ាស៊ីនដែលអាចឬមិនមែនជារបស់បណ្តាញរងដូចគ្នា។
- ដំណើរការម៉ាស៊ីនមេទាំងអស់ដែលមានបំណងប្រាស្រ័យទាក់ទងគ្នាតាមបណ្តាញត្រូវបានបំពាក់ដោយចំណុចចូលដំណើរការសេវាដឹកជញ្ជូនល្បី (TSAP) ដែលត្រូវបានគេស្គាល់ថាជាលេខច្រក។
- ពិធីសារត្រួតពិនិត្យការបញ្ជូន (TCP) គឺជាពិធីការដ៏សំខាន់បំផុតមួយនៃឈុតពិធីការអ៊ីនធឺណិត។ វាគឺជាពិធីការដែលត្រូវបានប្រើប្រាស់យ៉ាងទូលំទូលាយបំផុតសម្រាប់ការបញ្ជូនទិន្នន័យនៅក្នុងបណ្តាញទំនាក់ទំនងដូចជាអ៊ីនធឺណិត។
- ការតភ្ជាប់ត្រូវបានបង្កើតឡើងនៅក្នុង TCP ដោយប្រើការចាប់ដៃបីផ្លូវ ដូចដែលបានពិភាក្សាមុននេះ ដើម្បីបង្កើតការតភ្ជាប់។ ភាគីម្ខាងនិយាយថាម៉ាស៊ីនមេ ស្តាប់នៅដោយអសកម្មសម្រាប់តំណចូល ដោយអនុវត្តការស្តាប់ និងទទួលយកបុព្វកាល ទាំងកំណត់ផ្នែកផ្សេងទៀតជាក់លាក់ ឬគ្មាននរណាម្នាក់ជាពិសេស។
- ពិធីសារទិន្នន័យអ្នកប្រើប្រាស់ (UDP) គឺជាពិធីការទំនាក់ទំនង Transport Layer ត្រង់បំផុតដែលមាននៅក្នុងឈុតពិធីការ TCP/IP ។ វាពាក់ព័ន្ធនឹងចំនួនអប្បបរមានៃយន្តការទំនាក់ទំនង UDP ត្រូវបានគេនិយាយថាជាពិធីការដឹកជញ្ជូនដែលមិនអាចទុកចិត្តបាន ប៉ុន្តែវាប្រើសេវា IP ដែលផ្តល់នូវយន្តការចែកចាយដែលប្រឹងប្រែងបំផុត។
- ការទទួលស្គាល់កញ្ចប់ព័ត៌មានទាំងអស់គឺមានបញ្ហា ហើយអាចមានការខ្ជះខ្ជាយកម្រិតបញ្ជូនយ៉ាងច្រើន យន្តការចែកចាយដ៏ល្អបំផុតនៃពិធីការ IP មូលដ្ឋានធានានូវកិច្ចខិតខំប្រឹងប្រែងដ៏ល្អបំផុតក្នុងការចែកចាយកញ្ចប់ព័ត៌មានរបស់វា។ ទោះយ៉ាងណាក៏ដោយ បើទោះបីជាកញ្ចប់ព័ត៌មានមួយចំនួននៅក្នុងការផ្សាយវីដេអូត្រូវបានបាត់បង់ក៏ដោយ ផលប៉ះពាល់គឺមិនមានគ្រោះថ្នាក់ទេ ហើយអាចត្រូវបានមិនអើពើយ៉ាងងាយស្រួល។

សំណួរ

១. តើពិធីការ TCP ជាអ្វីនៅក្នុងបណ្តាញកុំព្យូទ័រ?

២. តើអ្វីទៅជាពិធីសារត្រួតពិនិត្យការបញ្ជូន(TCP) នៅក្នុងបណ្តាញកុំព្យូទ័រ?

៣. ចូរពន្យល់ពីគំរូសេវាកម្ម TCP នៅក្នុងបណ្តាញកុំព្យូទ័រ។

៤. តើការចេញផ្សាយការតភ្ជាប់ TCP គឺជាអ្វី?

៥. តើអ្វីទៅជាពិធីការ Datagram អ្នកប្រើប្រាស់(UDP)?

៦. តើ UDP មានលក្ខណៈពិសេសអ្វីខ្លះ?

ការអនុវត្តន៍ទី៧

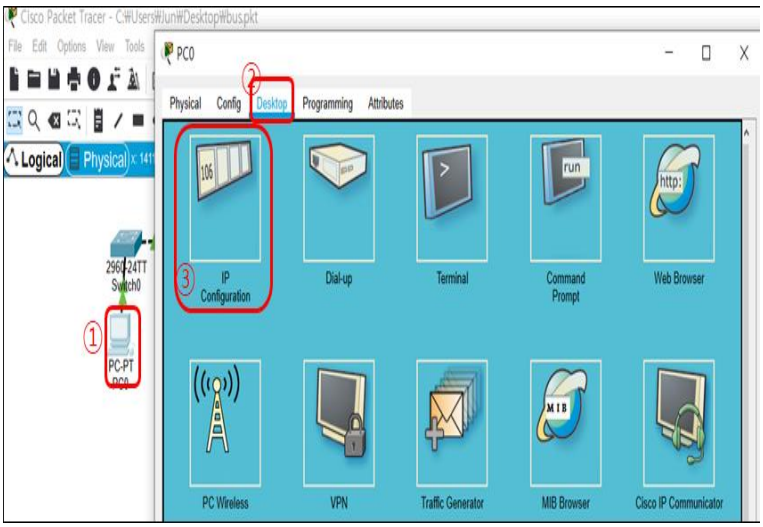
បណ្តាញមួយទទួលបានអត្ថន័យរបស់វាដោយការភ្ជាប់ទៅបណ្តាញមួយផ្សេងទៀតនៅក្នុងជំពូកនេះគោលការណ៍នៃប្រតិបត្តិការបណ្តាញត្រូវបានអនុវត្តតាមរយៈការភ្ជាប់រវាងរ៉ោតទ័រក្នុងការអនុវត្តបណ្តាញ។

ក. គោលបំណងនៃការអនុវត្តនេះ

- ដើម្បីភ្ជាប់រ៉ោតទ័រ១ ទៅកាន់រ៉ោតទ័រមួយទៀត
- ដើម្បីយល់ពីគោលការណ៍នៃផ្លូវក្នុងដំណើរការបណ្តាញ

ខ. ការតភ្ជាប់ជាមួយបណ្តាញច្រើននៅក្នុង Packet Tracer

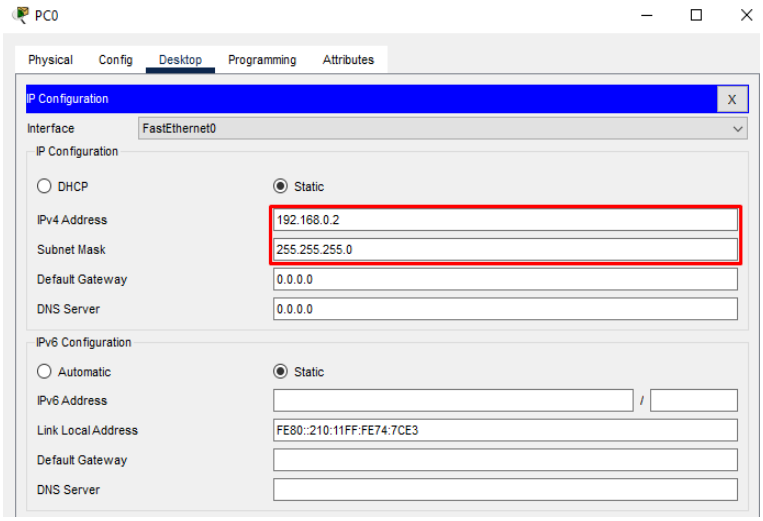
១. ការកំណត់ IP ទៅកុំព្យូទ័រនីមួយៗ



ក. យកកណ្តុរចុចពីរដងលើ [PC0]

ខ. ចុចលើ [Desktop]

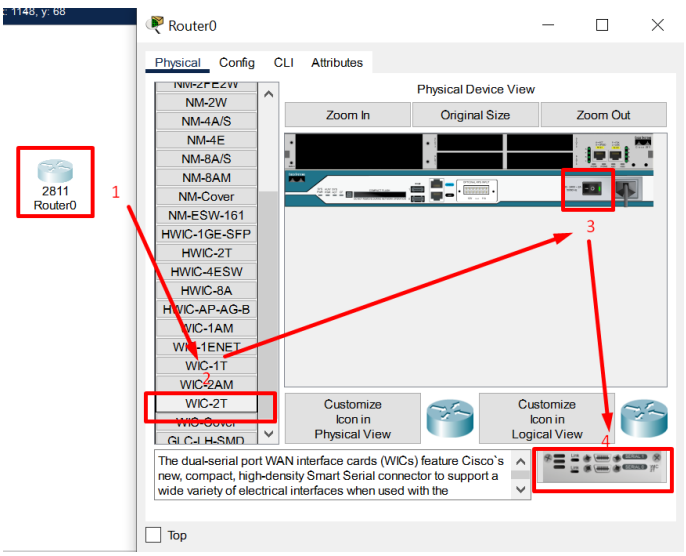
គ.ចុចលើ [IP Configuration]



ឃ. PC0: 192.168.0.2 / 255.255.255.0

ង. PC1: 192.168.0.3 / 255.255.255.0

២. ការបន្ថែមឧបករណ៍ Serial នៅក្នុងរ៉ោតទ័រ

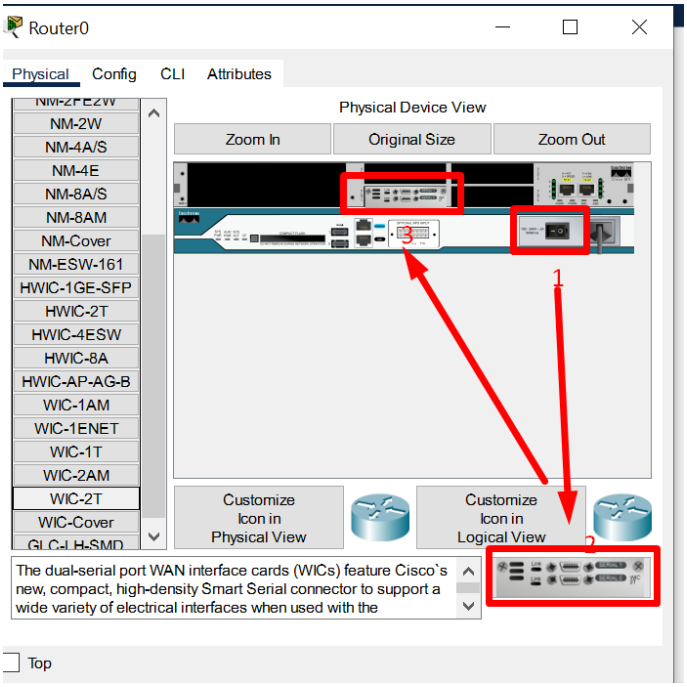


ក.ចុចស្តួន លើរ៉ោតទ័រ] ឧបករណ៍បញ្ចប់)Connections)[

ខ. ជ្រើសរើសយក WIC-2T

គ.ជ្រើសរើសបិទកុងតាក់ចរន្តអគ្គិសនី

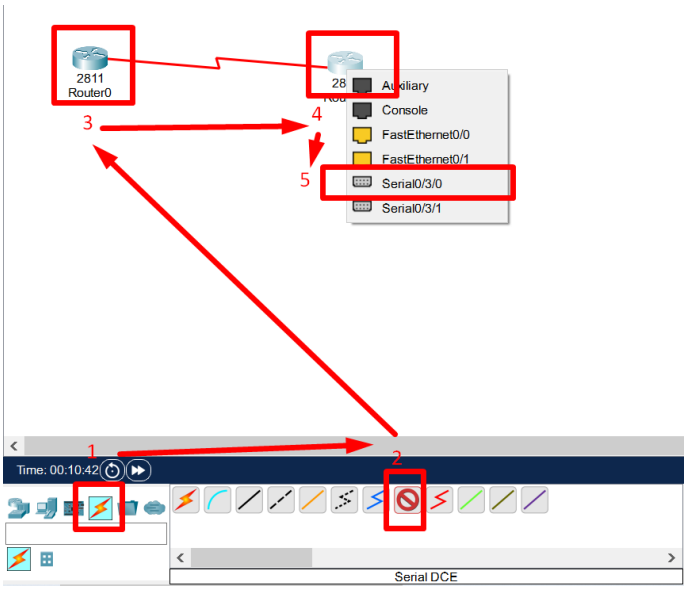
៣. ការបន្ថែមឧបករណ៍ Serial នៅក្នុងរ៉ោតទ័រកន្លែងទទេ



ក.ជ្រើសរើសឧបករណ៍ Dual-Serial

ខ. បន្ទាប់ទាញទម្លាក់ចូលក្នុងផ្ទៃទទេដូចរូប

៤.ការភ្ជាប់រ៉ោតទ័រ១ ទៅរ៉ោតទ័រ១ទៀតដោយខ្សែ Serial



ក. ចុចលើ [ការតភ្ជាប់(Connection)]

ខ. ចុចលើប្រភេទខ្សែ ដោយជ្រើសរើស [Serial DCE]

គ. រ៉ោតទ័រទី១ជ្រើសរើស Serial 0/3/0 រ៉ោតទ័រទី២ជ្រើសរើស Serial 0/3/0

គ. ការប្រើប្រាស់ CLI ក្នុងបណ្តាញប្រព័ន្ធ Packet Tracer រ៉ោតទ័រ0 និងរ៉ោតទ័រ1

❖ ការកំណត់រ៉ោតទ័រ0

១. ការកំណត់ក្នុងរ៉ោតទ័រ0 ក្នុង IP Address ក្នុង FastEhernet Port

```
Router>en
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip add 192.168.10.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

២. ការកំណត់ IP Address ក្នុងរ៉ោតទ័រ0 លើ Port Serial

```
Router>en
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface se0/3/0
Router(config-if)#ip add 10.10.10.1 255.255.255.252
Router(config-if)#no sh
Router(config-if)#exit
```

៣. ការកំណត់មុខងារផ្លូវរបស់រ៉ោតទ័រ 0

```
Router>en
Router#config terminal
Router(config)#ip route 192.168.20.0 255.255.255.0 10.10.10.2
Router(config)#no sh
```

❖ ការកំណត់រ៉ោតទ័រ១

៤. ការកំណត់ IP Address ក្នុងរ៉ោតទ័រ១ លើ Port Fast Ethernet

```
Router>en
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface fa0/0
Router(config-if)#ip add 192.168.20.1 255.255.255.0
Router(config-if)#no sh
Router(config-if)#exit
```

៥. ការកំណត់ក្នុងរ៉ោតទ័រ១ ក្នុង IP Address ក្នុង Serial Port

```
Router>en
Router#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface se0/3/0
Router(config-if)#ip add 10.10.10.2 255.255.255.252
Router(config-if)#no sh
Router(config-if)#exit
```

៦. ការកំណត់មុខងារផ្លូវរបស់រ៉ោតទ័រ ១

```
Router>en
Router#config terminal
Router(config)#ip route 192.168.10.0 255.255.255.0 10.10.10.1
Router(config)#no sh
```

ឃ. សន្ទេបការអនុវត្តន៍

នៅក្នុងការអនុវត្តនេះយើងបានអនុវត្តការភ្ជាប់បណ្តាញច្រើនឧបករណ៍ *Serial* សម្រាប់ការផ្ញើនិងទទួលកញ្ចប់ព័ត៌មានរវាងរ៉ោតទ័រត្រូវបានដំឡើងដើម្បីភ្ជាប់រវាងរ៉ោតទ័រ។ បន្ទាប់មក បញ្ចូលអាសយដ្ឋាន *IP* តែមួយគត់សម្រាប់ឧបករណ៍នីមួយៗ និងអ៊ីសឺរណិត យើងកំពុងបញ្ជូនរ៉ោតទ័រដើម្បីទាក់ទងជាមួយអាសយដ្ឋាន *IP* ដែលត្រូវគ្នា។

ង.កិច្ចការស្រាវជ្រាវ

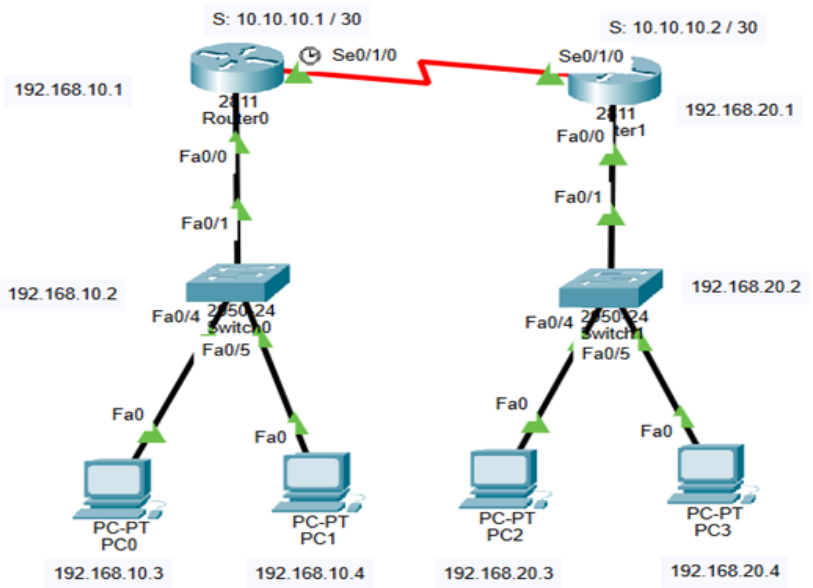
កិច្ចការទី១. កំណត់រចនាសម្ព័ន្ធបណ្តាញ

ក.កំណត់ IP Address សម្រាប់កុំព្យូទ័រនីមួយៗនៅក្នុងបណ្តាញដូចរូប

ខ.កំណត់ IP Address ក្នុងឧបករណ៍ Switch

គ. កំណត់ IP Address, IP serial និង IP Route នៅក្នុងរ៉ោតទ័រ

ឃ. ធ្វើការតេស្ត Ping ពី PC0 ទៅកាន់ PC3 នៅក្នុងបណ្តាញ

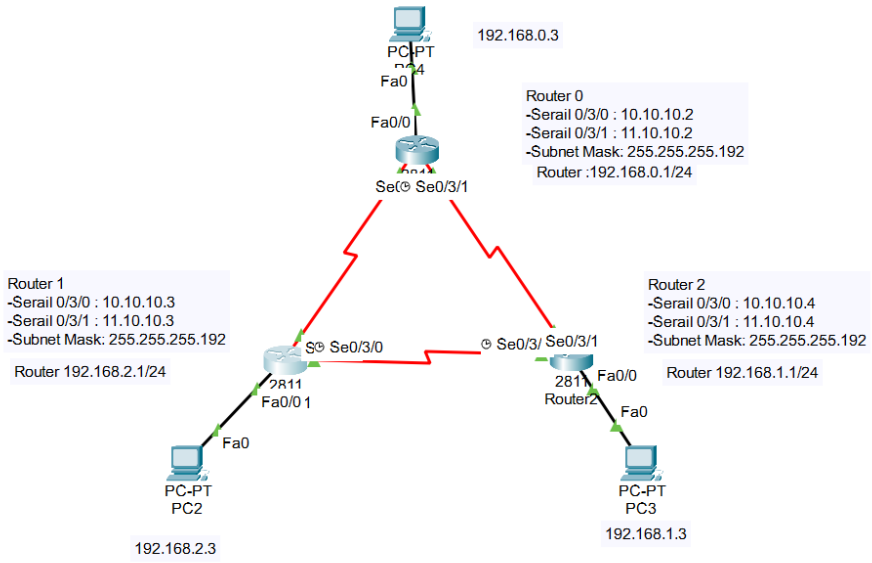


កិច្ចការទី២. កំណត់រចនាសម្ព័ន្ធបណ្តាញ

ក.កំណត់ IP Address សម្រាប់កុំព្យូទ័រនីមួយៗនៅក្នុងបណ្តាញដូចរូប

ខ. កំណត់ IP Address, IP serial និង IP Route នៅក្នុងរ៉ោតទ័រ

គ. ធ្វើការតេស្ត Ping ពី PC0 ទៅកាន់ PC3 នៅក្នុងបណ្តាញ



ជំពូកទី៨
សុវត្ថិភាពបណ្តាញ

សុវត្ថិភាពបណ្តាញគឺជាបណ្តុំនៃបច្ចេកវិទ្យា ដែលការពារលទ្ធភាពអ្នកប្រើប្រាស់ និងភាពសុចរិតភាពនៃហេដ្ឋារចនាសម្ព័ន្ធរបស់ក្រុមហ៊ុនដោយការពារការជ្រៀតចូល ឬការរីកសាយនៅក្នុងបណ្តាញនៃការគំរាមកំហែងដ៏ធំទូលាយមួយ។ ស្ថាបត្យកម្មសុវត្ថិភាពបណ្តាញរួមមានឧបករណ៍ដែលការពារបណ្តាញ និងកម្មវិធីដែលដំណើរការលើវាយុទ្ធសាស្ត្រសុវត្ថិភាពបណ្តាញដ៏មានប្រសិទ្ធភាពប្រើប្រាស់ខ្សែការពារជាច្រើនដែលអាចធ្វើមាត្រដ្ឋាននិងស្ម័យប្រវត្តិ។ ស្រទាប់ការពារនីមួយៗអនុវត្តនូវសំណុំនៃគោលការណ៍សុវត្ថិភាពដែលកំណត់ដោយអ្នកគ្រប់គ្រង។

ជំពូកទី៨ នេះអ្នកនឹងរៀនអំពី៖

- ៨.១ ការណែនាំអំពីសន្តិសុខតាមអ៊ីនធឺណិត
- ៨.២ សុវត្ថិភាពបណ្តាញ
- ៨.៣ សុវត្ថិភាពប្រព័ន្ធ
- ៨.៤ សុវត្ថិភាពគេហទំព័រ

៨.១ ការណែនាំអំពីសន្តិសុខតាមអ៊ីនធឺណិត

ការណែនាំអំពីសុវត្ថិភាពតាមអ៊ីនធឺណិតត្រូវបានរចនាឡើងដើម្បីជួយអ្នកសិក្សាអភិវឌ្ឍការយល់ដឹងកាន់តែស៊ីជម្រៅអំពីបច្ចេកវិទ្យា និងវិធីសាស្ត្រការពារប្រព័ន្ធនាពេលបច្ចុប្បន្ន។ លទ្ធផលសិក្សាគឺសាមញ្ញ យើងសង្ឃឹមថាអ្នកសិក្សានឹងបង្កើតនូវចំណង់ចំណូលចិត្តពេញមួយជីវិត និងការកោតសរសើរចំពោះសុវត្ថិភាពអ៊ីនធឺណិត ដែលយើងជឿជាក់ថានឹងជួយដល់ការខិតខំប្រឹងប្រែងនាពេលអនាគតរបស់ពួកគេ។ អ្នកអភិវឌ្ឍ អ្នកគ្រប់គ្រង វិស្វករ និងសូម្បីតែប្រជាពលរដ្ឋឯកជននឹងទទួលបានអត្ថប្រយោជន៍ពីបទពិសោធសិក្សានេះការសម្ភាសន៍តាមបំណងពិសេសជាមួយដៃគូឧស្សាហកម្ម ត្រូវបានរួមបញ្ចូលដើម្បីជួយភ្ជាប់គំនិតសុវត្ថិភាពតាមអ៊ីនធឺណិតទៅនឹងបទពិសោធអាជីវកម្មក្នុងជីវិតពិត សុវត្ថិភាពតាមអ៊ីនធឺណិតកំណត់បច្ចេកវិទ្យា នីតិវិធី និងការអនុវត្តដែលត្រូវបានបង្កើតឡើងដើម្បីការពារបណ្តាញ ឧបករណ៍ កម្មវិធី និងទិន្នន័យពីការវាយប្រហារតាមអ៊ីនធឺណិត សន្តិសុខតាមអ៊ីនធឺណិតអាចត្រូវបានកំណត់ថាជាសុវត្ថិភាពបច្ចេកវិទ្យាព័ត៌មាន (IT) ។

សុវត្ថិភាពតាមអ៊ីនធឺណិត គឺអំពីការការពារឧបករណ៍ និងបណ្តាញរបស់អ្នកពីការចូលប្រើ ឬការផ្លាស់ប្តូរដោយគ្មានការអនុញ្ញាត។ អ៊ីនធឺណិតជាប្រភពទិន្នន័យដ៏សំខាន់ និងជាបណ្តាញដែលមនុស្សធ្វើអាជីវកម្ម។ សន្តិសុខតាមអ៊ីនធឺណិតមានគោលបំណងការពារកុំព្យូទ័រ បណ្តាញ និងកម្មវិធីកុំព្យូទ័រពីការវាយប្រហារតាមអ៊ីនធឺណិតបែបនេះ ការវាយប្រហារតាមឌីជីថលភាគច្រើនមានគោលបំណងវាយតម្លៃ កែប្រែ ឬលុបទិន្នន័យដែលសំខាន់ៗ ទាញយកប្រាក់ពីជនរងគ្រោះ ឬជ្រៀតជ្រែកក្នុងប្រតិបត្តិការអាជីវកម្មធម្មតា។

៨.១.១ ប្រភេទនៃសុវត្ថិភាពតាមអ៊ីនធឺណិត

អ្នកជំនាញផ្នែកសន្តិសុខតាមអ៊ីនធឺណិតបន្តការពារប្រព័ន្ធកុំព្យូទ័រប្រឆាំងនឹងប្រភេទផ្សេងៗនៃការគំរាមកំហែងតាមអ៊ីនធឺណិត ការវាយប្រហារតាមអ៊ីនធឺណិតបានវាយប្រហារលើអាជីវកម្ម និងប្រព័ន្ធឯកជនជារៀងរាល់ថ្ងៃ ហើយការវាយប្រហារផ្សេងៗបានកើនឡើងយ៉ាងឆាប់រហ័ស។ យោងតាមអតីតនាយកប្រតិបត្តិ Cisco លោក John Chambers បាននិយាយថាមានក្រុមហ៊ុនពីរប្រភេទដែលក្រុមហ៊ុនដែលត្រូវបាន hacked និងអ្នកដែលមិនទាន់ដឹងថាពួកគេត្រូវបានគេលួចចូល ។ ហេតុផលសម្រាប់ការវាយប្រហារតាមអ៊ីនធឺណិតមានច្រើន ការវាយប្រហារតាមអ៊ីនធឺណិតអាចប្រើប្រព័ន្ធក្រៅបណ្តាញ ហើយទាមទារការទូទាត់ដើម្បីស្តារមុខងាររបស់វា។

មេរោគ Ransomware វាយប្រហារដែលតម្រូវឱ្យមានការបង់ប្រាក់ដើម្បីស្តារសេវាឥឡូវនេះគឺមានលក្ខណៈទំនើបជាងពេលណាៗទាំងអស់។ សាជីវកម្មងាយរងគ្រោះនឹងការវាយប្រហារតាមអ៊ីនធឺណិតប៉ុន្តែបុគ្គលម្នាក់ៗក៏ជាគោលដៅផងដែរ ជាញឹកញាប់ដោយសារតែពួកគេរក្សាទុកព័ត៌មានផ្ទាល់ខ្លួននៅលើទូរសព្ទដៃរបស់ពួកគេ និងប្រើប្រាស់បណ្តាញសាធារណៈដែលមិនមានសុវត្ថិភាព។

❖ សុវត្ថិភាពព័ត៌មាន

គោលបំណងសំខាន់នៃសុវត្ថិភាពព័ត៌មានគឺដើម្បីការពារទិន្នន័យឯកជនរបស់អ្នកប្រើប្រាស់ពីការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត និងការក្លែងបន្លំអត្តសញ្ញាណ។ វាគ្របដណ្តប់លើព័ត៌មានសំខាន់ និងផ្នែករឹងដែលគ្រប់គ្រង រក្សាទុក និងបញ្ជូនព័ត៌មាននោះ។ ឧទាហរណ៍នៃសុវត្ថិភាពព័ត៌មានមាន ការធ្វើឲ្យផ្ទាត់អ្នកប្រើប្រាស់ និងការសរសេរកូដសម្ងាត់។

❖ សុវត្ថិភាពកម្មវិធី

គោលដៅសុវត្ថិភាពកម្មវិធីគឺដើម្បីការពារកម្មវិធីកម្មវិធីពីភាពងាយរងគ្រោះដោយសារការរចនាកម្មវិធី ការអភិវឌ្ឍ ការដំឡើង និងធ្វើបច្ចុប្បន្នភាព ឬផ្តល់ការថែទាំចំពោះកំហុសនៃនីតិវិធី។

❖ មេរោគ

មេរោគត្រូវបានកំណត់ថាជាកម្មវិធីព្យាបាទដែលពាក់ព័ន្ធនឹង spyware, ransomware និងមេរោគ។ ជាទូទៅ វាបំពានបណ្តាញតាមរយៈភាពងាយរងគ្រោះ ដូចជាការចុចលើការភ្ជាប់អ៊ីមែលគួរឱ្យសង្ស័យ ឬដំឡើងកម្មវិធីដែលមានហានិភ័យពេលដែលនៅក្នុងបណ្តាញមួយ មេរោគអាចទទួលបានទិន្នន័យរសើប បង្កើតកម្មវិធីដែលបង្កគ្រោះថ្នាក់បន្ថែមទៀតនៅក្នុងក្របខ័ណ្ឌ ហើយថែមទាំងរារាំងការចូលប្រើធាតុបណ្តាញអាជីវកម្មសំខាន់ៗផងដែរ។

❖ សុវត្ថិភាពបណ្តាញ

គោលបំណងសំខាន់នៃសុវត្ថិភាពបណ្តាញគឺដើម្បីការពារការប្រើប្រាស់ សុចរិតភាព និងសុវត្ថិភាពនៃបណ្តាញ ធាតុដែលពាក់ព័ន្ធ និងទិន្នន័យដែលបានបញ្ជូនតាមបណ្តាញ នៅពេលដែលបណ្តាញមួយត្រូវបានសម្រេច ការគំរាមកំហែងដែលអាចកើតមានត្រូវបានរារាំងមិនឱ្យណែនាំ ឬពង្រីក។ ឧទាហរណ៍នៃសុវត្ថិភាពបណ្តាញមានកម្មវិធីកម្ចាត់មេរោគ និងកម្ចាត់មេរោគ ជញ្ជាំងភ្លើងដែលរារាំងការចូលប្រើបណ្តាញដែលគ្មានការអនុញ្ញាត និង VPNs (បណ្តាញឯកជននិម្មិត) ដែលប្រើសម្រាប់ការចូលប្រើពីចម្ងាយដែលមានសុវត្ថិភាព។

❖ ការលួចអត្តសញ្ញាណ

នេះគឺជាប្រភេទនៃការគំរាមកំហែងសន្តិសុខតាមអ៊ីនធឺណិតដែលពាក់ព័ន្ធនឹងការលួចទិន្នន័យរបស់ជនរងគ្រោះពីគេហទំព័រប្រព័ន្ធផ្សព្វផ្សាយសង្គម រួមទាំង Facebook, Instagram ជាដើម ហើយប្រើប្រាស់ទិន្នន័យនោះដើម្បីបង្កើតរូបភាពរបស់ជនរងគ្រោះ ប្រសិនបើព័ត៌មានរសើបគ្រប់គ្រាន់ត្រូវបានប្រមូលផ្តុំ ឧក្រិដ្ឋជនតាមអ៊ីនធឺណិតអាចក្លែងបន្លំអ្នកតាមមធ្យោបាយណាមួយ។

❖ ការខាយប្រហារពាក្យសម្ងាត់

នេះគឺជាប្រភេទនៃការគំរាមកំហែងសន្តិសុខតាមអ៊ីនធឺណិតដែលពាក់ព័ន្ធនឹងការប៉ុនប៉ងលួចចូលរបស់អ្នកប្រើដើម្បីបំបែកពាក្យសម្ងាត់របស់អ្នកប្រើ ដោយមានការគាំទ្រពីឧបករណ៍លួចចូល ពួក Hacker អាចណែនាំពាក្យសម្ងាត់ជាច្រើនក្នុងមួយវិនាទី ដើម្បីបំបែកអត្តសញ្ញាណគណនីរបស់ជនរងគ្រោះ និងទទួលបានសិទ្ធិចូលប្រើប្រាស់។ ពួក Hacker ក៏អាចអនុវត្តការវាយប្រហារពាក្យសម្ងាត់នៅលើអេក្រង់ចូលកុំព្យូទ័រ ដើម្បីជំរុញការចូលប្រើកុំព្យូទ័ររបស់ជនរងគ្រោះ និងទិន្នន័យរបស់វា។

❖ ការគំរាមកំហែងផ្នែកសុវត្ថិភាព និងមេរោគ

បច្ចេកទេសនៃការការពារកុំព្យូទ័រ ម៉ាស៊ីនមេ ឧបករណ៍ចល័ត ប្រព័ន្ធអេឡិចត្រូនិក បណ្តាញ និងទិន្នន័យប្រឆាំងនឹងការឈ្លានពានអរិភាពត្រូវបានគេស្គាល់ថាជាសន្តិសុខតាមអ៊ីនធឺណិត។ វាត្រូវបានគេស្គាល់ផងដែរថាជាសន្តិសុខព័ត៌មានអេឡិចត្រូនិក ឬសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន អ្នកវាយប្រហារតាមអ៊ីនធឺណិតអាចប្រើប្រាស់ទិន្នន័យរសើបដើម្បីលួចព័ត៌មាន ឬចូលប្រើគណនីធនាគាររបស់បុគ្គល ឬក្រុមហ៊ុន ក្នុងចំណោមសកម្មភាពដែលអាចបំផ្លិចបំផ្លាញផ្សេងទៀត ដែលជាមូលហេតុដែលអ្នកឯកទេសសន្តិសុខអ៊ីនធឺណិតមានសារសំខាន់សម្រាប់ការការពារទិន្នន័យឯកជនឱ្យមានសុវត្ថិភាព។

៨.១.២ ប្រភេទនៃការព្រួយបារម្ភក្នុងសន្តិសុខអ៊ីនធឺណិត

អ្នកជំនាញផ្នែកសន្តិសុខអ៊ីនធឺណិតគួរតែយល់អំពីប្រភេទនៃហានិភ័យសុវត្ថិភាពអ៊ីនធឺណិតខាងក្រោមឱ្យបានល្អ។

❖ មេរោគ

កម្មវិធី Malevolent រួមមាន spyware, ransomware, មេរោគ និងពពួក Worm មេរោគត្រូវបានធ្វើឱ្យសកម្ម ហើយកម្មវិធីដែលមានគ្រោះថ្នាក់ត្រូវបានដាក់ឱ្យប្រើប្រាស់ នៅពេលដែលអ្នកប្រើប្រាស់ចុចលើតំណ ឬឯកសារភ្ជាប់ដែលមានមេរោគ។ នៅពេលដែលមេរោគត្រូវបានចូលទៅកាន់ប្រព័ន្ធសុវត្ថិភាព Cisco វាអាចបណ្តាលឱ្យ៖

- សមាសធាតុបណ្តាញសំខាន់ៗដើម្បីឱ្យមានការចូលប្រើមានកំណត់ (ransomware)។
- បង្កើនចំនួនកម្មវិធីដែលអាចបង្កគ្រោះថ្នាក់ដែលបានដំឡើង។
- ការបញ្ជូនទិន្នន័យពីថាសរឹងដើម្បីទទួលបានព័ត៌មានដោយមិនត្រូវបានរកឃើញ (Spyware)
- សមាសភាគបុគ្គលទៅជាមានកំហុស ធ្វើឱ្យប្រព័ន្ធមិនអាចប្រើបាន។

❖ The Emoted

Emoted គឺជា "Trojan បែបធនាគារដ៏ឆ្លាតវៃ ដែលដំណើរការជាចម្បងជាអ្នកទាញយក ឬទម្លាក់ Trojan ធនាគារផ្សេងទៀត" នេះបើយោងតាមទីភ្នាក់ងារសន្តិសុខអ៊ីនធឺណិត និងហេដ្ឋារចនាសម្ព័ន្ធ (CISA) មេរោគដែលថ្លៃបំផុត និងគ្រោះថ្នាក់បំផុតមួយគឺ ``Emoted`` ។

❖ ការរំខានផ្នែកសេវាកម្ម

ការវាយប្រហារដោយការរំខានផ្នែកសេវាកម្ម (DoS) បានវាយប្រហារកុំព្យូទ័រ ឬបណ្តាញ ដែលធ្វើឱ្យវាមិនអាចឆ្លើយតបទៅនឹងការសាកសួរ ការវាយប្រហារដែលចែកចាយ DoS (DDoS) សម្រេចបានលទ្ធផលដូចគ្នា លើកលែងតែវាធ្វើវានៅលើបណ្តាញកុំព្យូទ័រ ចោរតាមអ៊ីនធឺណិតជាធម្មតាប្រើការវាយប្រហារដូចជាទឹកជំនន់ដើម្បីរំខានពិធីការ "handshake" និងអនុវត្ត DoS ។ មធ្យោបាយបន្ថែមអាចនឹងត្រូវបានប្រើប្រាស់ ហើយចោរតាមអ៊ីនធឺណិតមួយចំនួនឆ្លៀតយកអត្ថប្រយោជន៍ពីពេលទំនេរដើម្បីបើកការវាយប្រហារបន្ថែមទៀត។ botnet ដែលជាប្រភេទ DDoS ដែលឧបករណ៍រាប់លានត្រូវបានឆ្លងមេរោគ និងគ្រប់គ្រងដោយពួក Hacker គឺជាក្រុមហ៊ុនកម្មវិធីសុវត្ថិភាពព័ត៌មានវិទ្យា។ Botnets ដែលជួនកាលគេហៅថាប្រព័ន្ធ zombie គឺជាបណ្តាញកុំព្យូទ័រដែលត្រូវបានរចនាឡើងដើម្បីវាយប្រហារ និងគ្របដណ្តប់លើកុំព្យូទ័រតែមួយ។

❖ មេននៅក្នុងការវាយប្រហារកណ្តាល

ការវាយប្រហារដោយមេននៅកណ្តាល (MITM) កើតឡើងនៅពេលដែលពួក Hacker បញ្ចូលខ្លួនពួកគេទៅក្នុងប្រតិបត្តិការភាគីពីរ។ Cisco អះអាងថា បន្ទាប់ពីបញ្ឈប់ការបញ្ជូន ពួកគេអាចត្រង និងប្រមូលទិន្នន័យបានការវាយប្រហាររបស់ MITM កើតឡើងជាញឹកញាប់នៅពេលដែលអ្នកទស្សនាប្រើបណ្តាញ Wi-Fi សាធារណៈដែលមិនមានសុវត្ថិភាព បន្ទាប់ពីបង្កើតរបាំងរវាងអ្នកចូលមើល និងបណ្តាញ អ្នកវាយប្រហារប្រើប្រាស់មេរោគ ដើម្បីដំឡើងកម្មវិធី និងលួចទិន្នន័យ។

❖ SQL Injection

SQL Injection គឺជាការវាយប្រហារតាមអ៊ីនធឺណិតដែលកើតឡើងនៅពេលដែលកូដព្យាបាទត្រូវបានបញ្ចូលទៅក្នុងម៉ាស៊ីនមេ SQL នៅពេលដែលម៉ាស៊ីនមេឆ្លងមេរោគ វាលេចធ្លាយព័ត៌មានការវាយបញ្ចូលកូដព្យាបាទទៅក្នុងវាលស្វែងរកនៅលើគេហទំព័រដែលងាយរងគ្រោះ។

❖ ការវាយប្រហារលើពាក្យសម្ងាត់

អ្នកវាយប្រហារតាមអ៊ីនធឺណែតអាចចូលប្រើព័ត៌មានយ៉ាងទូលំទូលាយជាមួយនឹងពាក្យសម្ងាត់ត្រឹមត្រូវ ទិន្នន័យខាងក្នុងពិពណ៌នាអំពីវិស្វកម្មសង្គមថាជា "អ្នកវាយប្រហារតាមប្រព័ន្ធ អ៊ីនធឺ-ណេត ដោយប្រើយុទ្ធសាស្ត្រដែលពឹងផ្អែកជាចម្បងលើទំនាក់ទំនងរបស់មនុស្ស ហើយជារឿយៗទាក់

ទាញបុគ្គលឱ្យបំពានស្តង់ដារសុវត្ថិភាពសាមញ្ញ”។ ការវាយប្រហារដោយពាក្យសម្ងាត់ក៏អាចរួមបញ្ចូលការចូលប្រើមូលដ្ឋានទិន្នន័យ ឬទាយពាក្យសម្ងាត់ផងដែរ។

❖ The CIA Trinity នៃសន្តិសុខតាមអ៊ីនធឺណិត

The CIA Trinity នៃសន្តិសុខតាមអ៊ីនធឺណិតមានផ្នែកបីនៃការព្រួយបារម្ភនៅក្នុងសន្តិសុខអ៊ីនធឺណិត នេះត្រូវបានគេស្គាល់ថាជាThe CIA Trinityដែលតំណាងឱ្យការសម្ងាត់ទិន្នន័យ សុចរិតភាព និងភាពមាន។ អ្នកបច្ចេកវិទ្យាព័ត៌មានតែងតែចាត់ទុកការរក្សាការសម្ងាត់ទិន្នន័យជារឿងសំខាន់បំផុត នាយកដ្ឋាន IT តែងតែដោះស្រាយជាមួយព័ត៌មានដែលអាចកំណត់អត្តសញ្ញាណផ្ទាល់ខ្លួន (PII) ភាពចាំបាច់នៃការសម្ងាត់ត្រូវបានគ្របដណ្តប់ដោយភាពសុចរិត និងលទ្ធភាពនៃទិន្នន័យនៅក្នុងកម្មវិធី pumping ដ៏ឆ្លាតវៃ។ លទ្ធភាពទទួលបានព័ត៌មានទៅ និងមកពីកម្មវិធីអាចជាកត្តាសំខាន់បំផុតទាក់ទងនឹងសុវត្ថិភាព ភាពឆ្លាតវៃរបស់កម្មវិធីអាចនឹងបាត់បង់ ប្រសិនបើទិន្នន័យមិនអាចប្រើបាន ដោយសារការវាយប្រហារ ដូចជាការបដិសេធសេវាកម្មជាដើម។ ភាពត្រឹមត្រូវនៃទិន្នន័យក៏សំខាន់ផងដែរ ទិន្នន័យនឹងត្រូវបានគេសម្របសម្រួលប្រសិនបើមានការផ្លាស់ប្តូរនៅក្នុងការធ្វើដំណើរ ឬពេលសម្រាកជាលទ្ធផល ការវិភាគទិន្នន័យណាមួយ ទោះជាធ្វើឡើងក្នុងពេលជាក់ស្តែង ឬក្រោយក៏ដោយ នឹងត្រូវសង្ស័យ និងអាចមានគ្រោះថ្នាក់។

៨.១.៣ តើ មេរោគ គឺជាអ្វី?

មេរោគ គឺជាពាក្យកាត់មកពី ``កម្មវិធីដែលមានគំនិតអាក្រក់`` សំដៅទៅលើកម្មវិធីដែលបានបង្កើតឡើងដោយឧក្រិដ្ឋជនអ៊ិនធឺរណែត (ជាញឹកញាប់ហៅថា ``ពួក Hacker``) ដើម្បីលួចទិន្នន័យ និងបំផ្លាញកុំព្យូទ័រនិងប្រព័ន្ធកុំព្យូទ័រ។ ឧទាហរណ៍ នៃមេរោគទូទៅរួមមានវីរុសដង្កូវវីរុស Trojan, Spyware, Adware, និង Ransomware ការវាយប្រហាររបស់មេរោគថ្មីៗនេះមានទិន្នន័យដែលបានចៀសផុតក្នុងបរិមាណដ៏ច្រើន។

❖ តើខ្ញុំការពារបណ្តាញរបស់ខ្ញុំប្រឆាំងនឹង មេរោគ យ៉ាងដូចម្តេច?

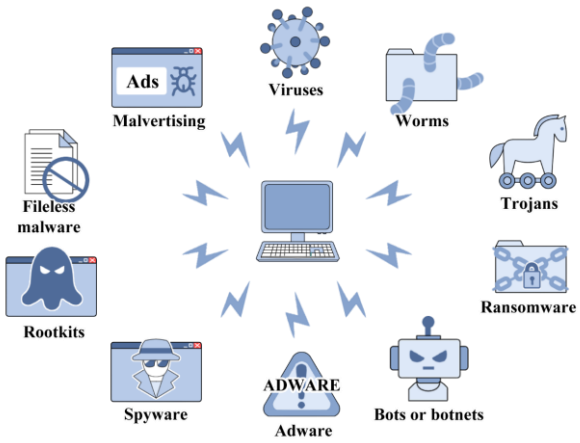
ជាធម្មតាអាជីវកម្មផ្តោតលើឧបករណ៍បង្ការ ឬការពារ បញ្ឈប់ការរំលោភបំពានតាមរយៈការធានាបរិវេណក្រុមហ៊ុនបានសន្មតថាពួកគេមានសុវត្ថិភាព។ មេរោគកម្រិតខ្ពស់មួយចំនួននឹងធ្វើឱ្យផ្លូវរបស់អ្នកចូលក្នុងបណ្តាញរបស់អ្នកនៅទីបំផុតជាលទ្ធផលវាចាំបាច់ណាស់ក្នុងការដាក់ពង្រាយបច្ចេកវិទ្យាដែលបន្តឃ្លាំមើលនិងរកឃើញមេរោគដែលបានគេចចេញពីការការពារដំរី។ ការការពារមេរោគកម្រិតខ្ពស់គ្រប់គ្រាន់ទាមទារឱ្យមានស្រទាប់ការពារជំពូកជាច្រើនរួមជាមួយភាពមើលឃើញនៃបណ្តាញខ្ពស់និងភាពវៃឆ្លាត។

❖ តើខ្ញុំអាចរកឃើញនិងឆ្លើយតបចំពោះមេរោគយ៉ាងដូចម្តេច?

មេរោគនឹងជ្រាបចូលទៅក្នុងបណ្តាញរបស់អ្នកដោយចៀសមិនផុត អ្នកត្រូវតែមានការពារដែលផ្តល់នូវភាពមើលឃើញគួរឱ្យកត់សម្គាល់និងការរកឃើញរំលោភបំពាន។ ដើម្បីលុបបំបែកអ្នកត្រូវតែអាចកំណត់អត្តសញ្ញាណអ្នកសំដែងព្យាបាទបានយ៉ាងឆាប់រហ័ស នេះទាមទារការស្តែនបណ្តាញថេរ។ នៅពេលដែលការគំរាមកំហែងបានកើតឡើងអ្នកត្រូវតែដកចេញពីបណ្តាញរបស់អ្នក កម្មវិធីកំចាត់មេរោគសព្វថ្ងៃមិនគ្រប់គ្រាន់ទេក្នុងការការពារប្រឆាំងនឹងការគំរាមកំហែងតាមអ៊ីនធឺណិតកម្រិតខ្ពស់រៀនពីរបៀបធ្វើបច្ចុប្បន្នភាពយុទ្ធសាស្ត្រប្រឆាំងមេរោគរបស់អ្នក។

❖ មេរោគ ៧ប្រភេទដែលតែងតែជួបជាញឹកញាប់

ប្រភេទទូទៅបំផុតនៃមេរោគទូទៅរួមមាន Worm, Trojans, Ransomware, រូបយន្តឬ Botnets, Adware, spyware, rootkwits, ឯកសារ, កោសិកា, និងការផ្សាយពាណិជ្ជកម្មហើយខណៈពេលដែលគោលដៅចុងក្រោយនៃការវាយប្រហាររបស់អ្នកវាយប្រហារច្រើនតែដូចគ្នា ដើម្បីទទួលបានព័ត៌មានផ្ទាល់ខ្លួនឬធ្វើឱ្យខូចខុបករណ៍ដែលជាធម្មតាសម្រាប់ការកើនឡើងហិរញ្ញវត្ថុ វិធីសាស្ត្រចែកចាយអាចខុសគ្នាអ្នកខ្លះក៏អាចពាក់ព័ន្ធនឹងការរួមបញ្ចូលគ្នារវាងប្រភេទគូបប្រភេទទាំងនេះដែរប្រភេទ។



រូបភាព ៨.១ ប្រភេទ មេរោគ

១. ទីរុស(Viruses)

វីរុសគឺជាកម្មវិធីដែលមានគំនិតអាក្រក់ដែលភ្ជាប់ទៅនឹងឯកសារឬឯកសារដែលគាំទ្រម៉ាក្រូដើម្បីប្រតិបត្តិកូដរបស់វាហើយរាលដាលចេញពីម៉ាស៊ីនទៅម៉ាស៊ីន។ នៅពេលដែលបានទាញយក, មេរោគនឹងដេកលក់រហូតដល់ឯកសារត្រូវបានបើកនិងប្រើ។ វីរុសត្រូវបានរចនា

ឡើងដើម្បីរំខានដល់សមត្ថភាពរបស់ប្រព័ន្ធក្នុងការធ្វើប្រតិបត្តិការជាលទ្ធផលវីរុសអាចបណ្តាលឱ្យមានបញ្ហាប្រតិបត្តិការសំខាន់ៗនិងការបាត់បង់ទិន្នន័យ។

២. ដង្កូវ(Worm)

ពពួក Worm គឺជាកម្មវិធីដែលមានគំនិតអាក្រក់ដែលចម្លងយ៉ាងឆាប់រហ័សនិងរាលដាលដល់ឧបករណ៍ណាមួយនៅក្នុងបណ្តាញមិនដូចមេរោគទេដង្កូវមិនត្រូវការកម្មវិធីម៉ាស៊ីនដើម្បីផ្សព្វផ្សាយទេ។ ដង្កូវឆ្លងឧបករណ៍មួយតាមរយៈឯកសារដែលបានទាញយកឬការភ្ជាប់បណ្តាញមុនពេលវាកាន់តែច្រើននិងបែកខ្ញែកគ្នា។ ដូចជាមេរោគ, ពពួក Worm អាចរំខានដល់ប្រតិបត្តិការរបស់ឧបករណ៍យ៉ាងធ្ងន់ធ្ងរហើយបណ្តាលឱ្យបាត់បង់ទិន្នន័យ។

៣. មេរោគ Trojan

វីរុស Trojan ត្រូវបានក្លែងបន្លំកម្មវិធីសូហ្វវែរដែលមានប្រយោជន៍ប៉ុន្តែនៅពេលដែលអ្នកប្រើប្រាស់ទាញយកវាមេរោគ Trojan អាចចូលប្រើទិន្នន័យរសើបហើយបន្ទាប់មកកែប្រែប្តូរឬលុបវាចោល។ មេរោគនេះអាចមានគ្រោះថ្នាក់ខ្លាំងណាស់ទៅលើការសម្តែងរបស់ឧបករណ៍មិនដូចមេរោគនិងពពួក Worm ទៀងទាត់មេរោគ Troupan មិនត្រូវបានរចនាឡើងដើម្បីចម្លងដោយខ្លួនឯងទេ។

៤. spyware

spyware គឺជាកម្មវិធីដែលមានគំនិតអាក្រក់ដែលដំណើរការដោយសម្ងាត់នៅលើកុំព្យូទ័រហើយរាយការណ៍ទៅអ្នកប្រើប្រាស់ពីចម្ងាយជាជាងការរំខានដល់ប្រតិបត្តិការរបស់ឧបករណ៍, spyware កំណត់គោលដៅព័ត៌មានរសើបនិងអាចផ្តល់ការចូលប្រើពីចម្ងាយ។ spyware ជារឿយៗត្រូវបានគេប្រើដើម្បីលួចព័ត៌មានហិរញ្ញវត្ថុឬផ្ទាល់ខ្លួនប្រភេទជាក់លាក់នៃ spyware គឺជា KeyLogger ដែលកត់ត្រាការចុចគ្រាប់ចុចរបស់អ្នកដើម្បីបង្ហាញពាក្យសម្ងាត់និងព័ត៌មានសម្ងាត់។

៥. Adware

Adware គឺជាកម្មវិធីដែលមានគំនិតអាក្រក់ដែលត្រូវបានប្រើដើម្បីប្រមូលទិន្នន័យនៅលើការប្រើប្រាស់កុំព្យូទ័ររបស់អ្នកនិងផ្តល់ការផ្សាយពាណិជ្ជកម្មសមស្របខណៈពេលដែល Adware មិនត្រឹមតែបង្កគ្រោះថ្នាក់ក្នុងករណីខ្លះ Adware អាចបង្កបញ្ហាសម្រាប់ប្រព័ន្ធរបស់អ្នក។ Adware អាចប្តូរទិសកម្មវិធីរុករករបស់អ្នកទៅគេហទំព័រដែលមិនមានសុវត្ថិភាពហើយវាថែមទាំងមានសេះ Trojan និង spyware ផងដែរលើសពីនេះទៀតកម្រិតសំខាន់នៃ Adware អាចធ្វើឱ្យប្រព័ន្ធរបស់អ្នកយឺតគួរឱ្យកត់សម្គាល់ដោយសារតែមិនមាន adware ទាំងអស់គឺមានគំនិតអាក្រក់វាចាំបាច់ក្នុងការការពារដែលតែងតែស្កេនកម្មវិធីទាំងនេះជាប្រចាំ។

៦. Ransomware

Ransomware គឺជាកម្មវិធីដែលមានគំនិតអាក្រក់ក្នុងការដែលទទួលបានការចូលប្រើព័ត៌មានរសើបនៅក្នុងប្រព័ន្ធអ៊ិនគ្រីបនៅក្នុងប្រព័ន្ធដែលបានអ៊ិនគ្រីបព័ត៌មានដូច្នេះអ្នកប្រើមិនអាចចូលប្រើវាបានទេហើយបន្ទាប់មកទាមទារការទូទាត់ប្រាក់ហិរញ្ញវត្ថុសម្រាប់ទិន្នន័យដែលត្រូវចេញផ្សាយ។ Ransomware គឺជារឿងជាទូទៅនៃការបោកប្រាស់ដោយចុចលើតំណភ្លែងបន្លំអ្នកប្រើទាញយក Ransomware អ្នកវាយប្រហារដំណើរការដើម្បីអ៊ិនគ្រីបព័ត៌មានជាក់លាក់ដែលអាចត្រូវបានបើកដោយកូនសោរគណិតវិទ្យាដែលពួកគេបានដឹងនៅពេលដែលអ្នកវាយប្រហារទទួលបានការទូទាត់ទិន្នន័យត្រូវបានដោះសោ។

៧. មេរោគគ្មានឯកសារ

មេរោគគ្មានឯកសារគឺជាប្រភេទនៃមេរោគដែលមានអង្គចងចាំ ដូចពាក្យបានបង្ហាញថាមេរោគដំណើរការពីការចងចាំរបស់កុំព្យូទ័ររបស់ជនរងគ្រោះមិនមែនមកពីឯកសារនៅលើផ្នែករឹងនោះទេ។ ដោយសារតែមិនមានឯកសារដែលត្រូវស្កេនវាពិបាកក្នុងការរកឃើញជាងមេរោគបែបបុរាណវាក៏ធ្វើឱ្យកោសល្យវិច័យកាន់តែពិបាកដែរព្រោះមេរោគបាត់នៅពេលកុំព្យូទ័ររបស់ជនរងគ្រោះត្រូវបានចាប់ផ្តើមឡើងវិញ។

៨.២ សុវត្ថិភាពបណ្តាញ

ក្នុងសម័យទំនើបនេះ អង្គការពឹងផ្អែកលើបណ្តាញកុំព្យូទ័រ ដើម្បីចែករំលែកព័ត៌មានប្រកបដោយប្រសិទ្ធភាព និងផលិតភាពទូទាំងអង្គភាព។ បណ្តាញកុំព្យូទ័ររបស់អង្គការឥឡូវនេះក្លាយជាធំ និងគ្រប់ទីកន្លែងដោយសន្មតថាបុគ្គលិកម្នាក់ៗមានស្ថានីយការងារដែលខិតខំប្រឹងប្រែង ក្រុមហ៊ុនធំមួយនឹងមានស្ថានីយការងារពីរបីពាន់ និងម៉ាស៊ីនមេជាច្រើននៅលើបណ្តាញ។

ទំនងជាស្ថានីយការងារទាំងនេះប្រហែលជាត្រូវការគ្រប់គ្រងកណ្តាលច្រើនជាងមុន ហើយត្រូវការការពារបរិវេណ។ ពួកគេអាចមានប្រព័ន្ធប្រតិបត្តិការផ្សេងៗ ផ្នែករឹង កម្មវិធី និងពិធីការ ជាមួយនឹងកម្រិតផ្សេងគ្នានៃការយល់ដឹងតាមអ៊ីនធឺណិតក្នុងចំណោមអ្នកប្រើប្រាស់។ ស្រមៃថាស្ថានីយការងារាប់ពាន់ទាំងនេះនៅលើបណ្តាញរបស់ក្រុមហ៊ុនត្រូវបានភ្ជាប់ដោយផ្ទាល់ទៅអ៊ីនធឺណិត។ បណ្តាញដែលគ្មានសុវត្ថិភាពនេះក្លាយជាគោលដៅសម្រាប់ការវាយប្រហារដែលផ្ទុកព័ត៌មានដ៏មានតម្លៃ និងបង្ហាញភាពងាយរងគ្រោះ។ នៅក្នុងជំពូកនេះ យើងពិពណ៌នាអំពីភាពងាយរងគ្រោះសំខាន់ៗនៃបណ្តាញ និងសារសំខាន់នៃសុវត្ថិភាពបណ្តាញនៅក្នុងជំពូកបន្តបន្ទាប់ យើងនឹងពិភាក្សាអំពីវិធីដើម្បីសម្រេចបានដូចគ្នា។

❖ បណ្តាញរាងកាយ

បណ្តាញគឺជាឧបករណ៍កុំព្យូទ័រពីរ ឬច្រើនដែលតភ្ជាប់ដើម្បីចែករំលែកធនធានប្រកបដោយប្រសិទ្ធភាពលើសពីនេះ ការរួមបញ្ចូលបណ្តាញពីរ ឬច្រើនត្រូវបានគេហៅថា ការងារអ៊ីនធឺណិត។

ដូច្នេះ អ៊ីនធឺណិតគឺគ្រាន់តែជាការងារអ៊ីនធឺណិតប៉ុណ្ណោះ ដែលជាបណ្តុំនៃបណ្តាញភ្ជាប់គ្នាទៅវិញទៅមកសម្រាប់ការបង្កើតបណ្តាញផ្ទៃក្នុងរបស់ខ្លួន អង្គការមួយមានជម្រើសផ្សេងៗវាអាចប្រើបណ្តាញខ្សែ ឬបណ្តាញឥតខ្សែ ដើម្បីភ្ជាប់ស្ថានីយការងារទាំងអស់ សព្វថ្ងៃនេះ អង្គការនានាកំពុងប្រើប្រាស់ជាចម្បងនូវការរួមបញ្ចូលគ្នានៃបណ្តាញខ្សែ និងឥតខ្សែ។

❖ បណ្តាញខ្សែ និងឥតខ្សែ

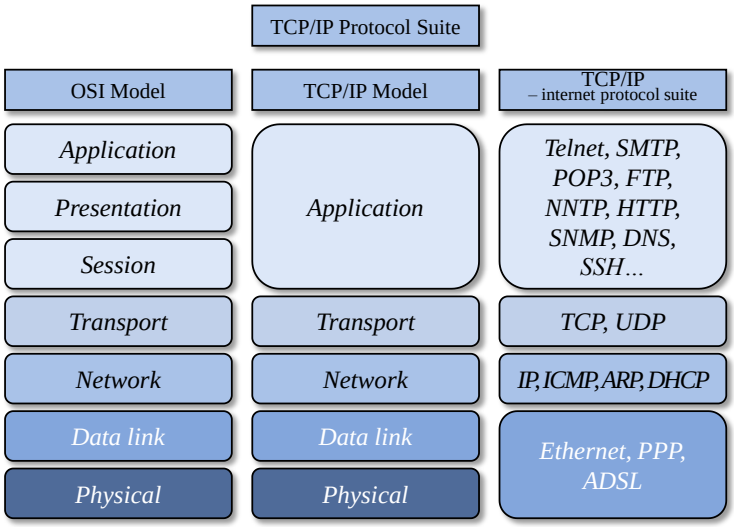
នៅក្នុងបណ្តាញខ្សែ ឧបករណ៍ត្រូវបានភ្ជាប់ដោយប្រើខ្សែជាធម្មតា បណ្តាញខ្សែគឺផ្អែកលើពិធីការអ៊ីសឺរណិត ដែលឧបករណ៍ត្រូវបានភ្ជាប់ដោយប្រើខ្សែ Unshielded Twisted Pair (UTP) ទៅកាន់ Switch ផ្សេងគ្នា Switch ទាំងនេះត្រូវបានភ្ជាប់បន្ថែមទៅរ៉ោតទ័របណ្តាញសម្រាប់ការចូលប្រើប្រាស់អ៊ីនធឺណិត។

❖ ពិធីការបណ្តាញ

ពិធីការបណ្តាញគឺជាសំណុំនៃច្បាប់ដែលគ្រប់គ្រងទំនាក់ទំនងរវាងឧបករណ៍ដែលភ្ជាប់ទៅបណ្តាញមួយពួកវារួមបញ្ចូលយន្តការសម្រាប់ការតភ្ជាប់ និងច្បាប់ធ្វើទ្រង់ទ្រាយសម្រាប់ការវេចខ្ចប់ទិន្នន័យសម្រាប់សារដែលបានផ្ញើ និងទទួល។ ពិធីការបណ្តាញកុំព្យូទ័រជាច្រើនត្រូវបានបង្កើតឡើងដែលនីមួយៗត្រូវបានរចនាឡើងសម្រាប់គោលបំណងជាក់លាក់ពិធីការពេញនិយម និងប្រើប្រាស់យ៉ាងទូលំទូលាយគឺ TCP/IP ជាមួយនឹងពិធីការកម្រិតខ្ពស់ជាង និងកម្រិតទាប។

❖ ពិធីការ TCP/IP

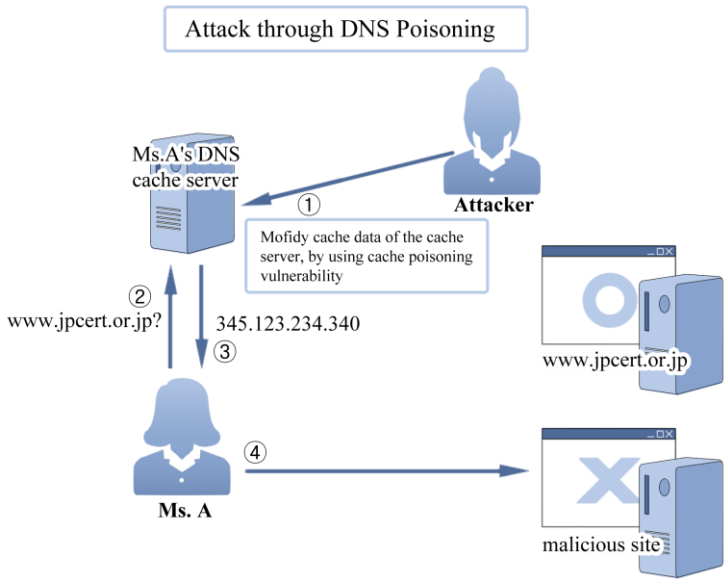
ពិធីសារត្រួតពិនិត្យការបញ្ជូន (TCP) និង ពិធីការអ៊ីនធឺណិតណ (IP) គឺជាពិធីការបណ្តាញ កុំព្យូទ័រពីរផ្សេងគ្នាដែលប្រើជាចម្បងជាមួយគ្នា។ ដោយសារតែប្រជាប្រិយភាព និងការទទួលយកយ៉ាងទូលំទូលាយ ពួកគេត្រូវបានបង្កើតឡើងនៅក្នុងប្រព័ន្ធប្រតិបត្តិការទាំងអស់នៃឧបករណ៍បណ្តាញ។ IP ត្រូវគ្នាទៅនឹងស្រទាប់បណ្តាញស្រទាប់ទី៣ចំណែក TCP ត្រូវនឹងស្រទាប់ដឹកជញ្ជូន ស្រទាប់ទី៤ នៅក្នុង OSI ។ TCP/IP អនុវត្តចំពោះការទំនាក់ទំនងបណ្តាញដែលការដឹកជញ្ជូន TCP ផ្តល់ទិន្នន័យឆ្លងកាត់បណ្តាញ IP ។ ពិធីការ TCP/IP ត្រូវបានគេប្រើជាទូទៅជាមួយពិធីការដូចជា HTTP, FTP និង SSH នៅស្រទាប់កម្មវិធី និងអ៊ីសឺរណិតនៅតំណទិន្នន័យ/ស្រទាប់រាងកាយ។



រូបភាព ៨.២ ឈុតពិធីការ TCP/IP

❖ ពិធីការ DNS

ប្រព័ន្ធឈ្មោះដែន (DNS) ដោះស្រាយឈ្មោះដែនម៉ាស៊ីនទៅអាសយដ្ឋាន IP អ្នកប្រើប្រាស់បណ្តាញពឹងផ្អែកលើមុខងារ DNS ជាចម្បង ខណៈពេលកំពុងរុករកអ៊ីនធឺណិត ដោយវាយបញ្ចូល URL នៅក្នុងកម្មវិធីរុករកតាមអ៊ីនធឺណិត។



រូបភាព ៨.៣ ការវាយប្រហារតាមរយៈ DNS

នៅក្នុងការវាយប្រហារលើ DNS អ្នកវាយប្រហារមានបំណងកែប្រែកំណត់ត្រា DNS ស្របច្បាប់ ដើម្បីដោះស្រាយវាទៅអាសយដ្ឋាន IP ដែលមិនត្រឹមត្រូវ។ វាអាចដឹកនាំចរាចរទាំងអស់សម្រាប់ IP នោះទៅកាន់កុំព្យូទ័រខុស អ្នកវាយប្រហារអាចទាញយកភាពងាយរងគ្រោះនៃពិធីការ DNS ឬ សម្របសម្រួលម៉ាស៊ីនមេដើម្បីធ្វើការវាយប្រហារ។ ការវាយប្រហារឃ្លាំងសម្ងាត់ DNS គឺជាការវាយប្រហារដោយប្រើភាពងាយរងគ្រោះដែលរកឃើញនៅក្នុងពិធីការ DNS ។ អ្នកវាយប្រហារអាចបំពុលឃ្លាំងសម្ងាត់ដោយបង្កើតការឆ្លើយតបទៅនឹងសំណួរ DNS ដែលកើតឡើងដដែលៗដែលផ្ញើដោយអ្នកដោះស្រាយទៅកាន់ម៉ាស៊ីនមេដែលមានការអនុញ្ញាត។ នៅពេលដែលការផ្គត់ផ្គង់ឧបករណ៍ដោះស្រាយ DNS ត្រូវបានបំពុល ម្ចាស់ផ្ទះនឹងត្រូវបានបញ្ជូនទៅគេហទំព័រដែលមានគំនិតអាក្រក់ ហើយអាចសម្របសម្រួលព័ត៌មានសម្ងាត់ដោយការទំនាក់ទំនងជាមួយគេហទំព័រនេះ។

❖ គោលដៅនៃសុវត្ថិភាពបណ្តាញ

ដូចដែលបានពិភាក្សានៅក្នុងផ្នែកមុននេះ មានភាពងាយរងគ្រោះមួយចំនួនធំនៅក្នុងបណ្តាញ ដូច្នេះក្នុងអំឡុងពេលបញ្ជូនទិន្នន័យគឺងាយរងគ្រោះខ្លាំងចំពោះការវាយប្រហារ។ អ្នកវាយប្រហារអាចកំណត់គោលដៅបណ្តាញទំនាក់ទំនង ទទួលបានទិន្នន័យ និងអានដូចគ្នា ឬបញ្ចូលសារមិនពិតឡើងវិញ ដើម្បីសម្រេចបាននូវគោលបំណងដ៏អាក្រក់របស់គេ សុវត្ថិភាពបណ្តាញមិនត្រឹមតែមានការព្រួយបារម្ភជាមួយនឹងកុំព្យូទ័រនៅចុងខ្សែសង្វាក់ទំនាក់ទំនងនីមួយៗប៉ុណ្ណោះទេវាមានគោលបំណងធានាថាបណ្តាញទាំងមូលមានសុវត្ថិភាព។ សុវត្ថិភាពបណ្តាញការពារលទ្ធភាពប្រើប្រាស់ ភាពជឿជាក់ សុចរិតភាព និងសុវត្ថិភាពនៃបណ្តាញ និងទិន្នន័យ។ សុវត្ថិភាពបណ្តាញប្រកបដោយប្រសិទ្ធភាពកម្ចាត់ការគំរាមកំហែងផ្សេងៗពីការចូល ឬរីករាលដាលនៅលើបណ្តាញ គោលដៅចម្បងនៃសុវត្ថិភាពបណ្តាញគឺភាពសម្ងាត់ សុចរិតភាព និងលទ្ធភាពមាន សសរស្តម្ភទាំងបីនៃសន្តិសុខបណ្តាញនេះត្រូវបានតំណាងជាញឹកញាប់ថាជាត្រីកោណ CIA ។

- **ការសម្ងាត់៖** មុខងារនៃភាពឯកជនគឺដើម្បីការពារទិន្នន័យអាជីវកម្មដ៏មានតម្លៃពីបុគ្គលដែលគ្មានការអនុញ្ញាត ផ្នែកសម្ងាត់នៃសុវត្ថិភាពបណ្តាញធានាថាទិន្នន័យមានសម្រាប់តែបុគ្គលដែលមានគោលបំណង និងមានការអនុញ្ញាតប៉ុណ្ណោះ។
- **សុចរិតភាព៖** គោលដៅនេះមានន័យថារក្សា និងធានានូវភាពត្រឹមត្រូវ និងភាពស៊ីសង្វាក់គ្នានៃទិន្នន័យ មុខងារនៃសុចរិតភាពគឺដើម្បីធ្វើឱ្យប្រាកដថាទិន្នន័យអាចជឿទុកចិត្តបាន និងមិនត្រូវបានផ្លាស់ប្តូរដោយអ្នកដែលគ្មានការអនុញ្ញាត។
- **ភាពអាចរកបាន៖** មុខងារនៃភាពអាចរកបាននៅក្នុង សុវត្ថិភាពបណ្តាញគឺដើម្បីធានាថាទិន្នន័យ ធនធានបណ្តាញ/សេវាកម្មមានជាបន្តបន្ទាប់សម្រាប់អ្នកប្រើប្រាស់ស្របច្បាប់នៅពេលណាដែលពួកគេត្រូវការវា។

❖ ការសម្រេចបានគោលដៅសុវត្ថិភាពបណ្តាញ

ការធានាសុវត្ថិភាពបណ្តាញអាចហាក់ដូចជាសាមញ្ញណាស់គោលដៅដែលត្រូវសម្រេចគឺត្រង់ ប៉ុន្តែតាមការពិត យន្តការដែលប្រើដើម្បីសម្រេចបាននូវគោលដៅទាំងនេះគឺមានភាពស្មុគ្រស្មាញខ្លាំង ហើយការយល់អំពីវាពាក់ព័ន្ធនឹងការវែកញែកសមហេតុផល សហភាពទូរគមនាគមន៍អន្តរជាតិ (ITU) នៅក្នុងអនុសាសន៍របស់ខ្លួនលើស្តាបត្យកម្មសុវត្ថិភាព X.800 បានកំណត់យន្តការជាក់លាក់ដើម្បីនាំយកស្តង់ដារនៃវិធីសាស្ត្រដើម្បីសម្រេចបាននូវសុវត្ថិភាពបណ្តាញ។

យន្តការទាំងនេះមួយចំនួនគឺ៖

- **ការអ៊ិនគ្រីប៖** យន្តការនេះផ្តល់សេវាកម្មរក្សាការសម្ងាត់ទិន្នន័យដោយបំប្លែងទិន្នន័យទៅជាទម្រង់ដែលមិនអាចអានបានសម្រាប់អ្នកដែលគ្មានការអនុញ្ញាត យន្តការនេះប្រើក្បួនដោះស្រាយការអ៊ិនគ្រីប ឱគ្រីបជាមួយសោសម្ងាត់។
- **ហត្ថលេខាឌីជីថល៖** យន្តការនេះគឺសមមូលអេឡិចត្រូនិចនៃហត្ថលេខាធម្មតានៅក្នុងទិន្នន័យអេឡិចត្រូនិច វាផ្តល់នូវភាពត្រឹមត្រូវនៃទិន្នន័យ។
- **ការគ្រប់គ្រងការចូលប្រើ៖** យន្តការនេះត្រូវបានប្រើដើម្បីផ្តល់សេវាកម្មត្រួតពិនិត្យការចូលប្រើយន្តការទាំងនេះអាចប្រើប្រាស់ក្នុងការកំណត់អត្តសញ្ញាណ និងការផ្សៀងផ្ទាត់អង្គភាពដើម្បីកំណត់ និងអនុវត្តសិទ្ធិចូលប្រើប្រាស់របស់អង្គភាព។

❖ យន្តការសុវត្ថិភាពនៅស្រទាប់បណ្តាញ

យន្តការសុវត្ថិភាពជាច្រើនត្រូវបានបង្កើតឡើង ដូច្នេះពួកគេអាចបង្កើតបាននៅស្រទាប់ជាក់លាក់នៃគំរូស្រទាប់បណ្តាញ OSI ។

- **សុវត្ថិភាពនៅ Application Layer ៖** វិធានការសុវត្ថិភាពដែលប្រើនៅស្រទាប់នេះគឺជាកម្មវិធីជាក់លាក់ប្រភេទផ្សេងគ្នានៃកម្មវិធីនឹងត្រូវការវិធានការសុវត្ថិភាពដាច់ដោយឡែកដើម្បីធានាសុវត្ថិភាពស្រទាប់កម្មវិធី កម្មវិធីចាំបាច់ត្រូវកែប្រែ។
- **ពិធីការកម្មវិធី៖** ដែលមានសំឡេងជាកូដសម្ងាត់គឺពិបាកខ្លាំងណាស់ ហើយការអនុវត្តវាឱ្យបានត្រឹមត្រូវគឺកាន់តែពិបាកដូច្នេះ យន្តការសុវត្ថិភាពស្រទាប់កម្មវិធីសម្រាប់ការពារការទំនាក់ទំនងបណ្តាញត្រូវបានគេពេញចិត្តថាគ្រាន់តែជាដំណោះស្រាយផ្អែកលើស្តង់ដារដែលបានប្រើប្រាស់អស់មួយរយៈ។ ឧទាហរណ៍នៃពិធីការសុវត្ថិភាពស្រទាប់កម្មវិធីគឺ សុវត្ថិភាពផ្នែកបន្ថែមអ៊ីមែលច្រើន Secure Multipurpose Internet Mail Extension (S/MIME) ដែលប្រើជាទូទៅដើម្បីអ៊ិនគ្រីបសារអ៊ីមែល។ DNSSEC គឺជាពិធីការមួយផ្សេងទៀតនៅស្រទាប់នេះដែលប្រើដើម្បីផ្លាស់ប្តូរសារសំណួរ DNS ដោយសុវត្ថិភាព។

- **សុវត្ថិភាពនៅ Transport Layer៖** វិធានការសុវត្ថិភាពនៅស្រទាប់នេះអាចត្រូវបានប្រើដើម្បីការពារទិន្នន័យក្នុងវគ្គទំនាក់ទំនងតែមួយរវាងម៉ាស៊ីនពីរ។ ការប្រើប្រាស់ទូទៅបំផុតសម្រាប់ពិធីការសុវត្ថិភាពស្រទាប់ដឹកជញ្ជូនគឺមើលចរាចរណ៍វគ្គ HTTP និង FTP ។ Transport Layer Security (TLS) និង Secure Socket Layer (SSL) គឺជាពិធីការទូទៅបំផុតដែលប្រើសម្រាប់គោលបំណងនេះ។
- **សុវត្ថិភាពនៅ Network Layer៖** វិធានការសុវត្ថិភាពនៅស្រទាប់នេះអាចត្រូវបានអនុវត្តទៅគ្រប់កម្មវិធីទាំងអស់មិនមែនជាកម្មវិធីជាក់លាក់ទេការទំនាក់ទំនងបណ្តាញទាំងអស់រវាងម៉ាស៊ីន ឬបណ្តាញអាចត្រូវបានការពារនៅស្រទាប់នេះដោយមិនចាំបាច់កែប្រែកម្មវិធីណាមួយឡើយ។ នៅក្នុងបរិយាកាសមួយចំនួន ពិធីការសុវត្ថិភាពស្រទាប់បណ្តាញ ដូចជា Internet Protocol Security (IPsec) ផ្តល់នូវដំណោះស្រាយល្អប្រសើរជាងការគ្រប់គ្រងលើការដឹកជញ្ជូន ឬស្រទាប់កម្មវិធី ដោយសារមានការលំបាកក្នុងការបន្ថែមការគ្រប់គ្រងទៅលើកម្មវិធីនីមួយៗ។

៨.៣ សុវត្ថិភាពប្រព័ន្ធ

សុវត្ថិភាពនៃប្រព័ន្ធកុំព្យូទ័រ គឺជាកិច្ចការសំខាន់វាដំណើរការធានានូវភាពសម្ងាត់ និងសុចរិតភាពនៃ OS។ សុវត្ថិភាពគឺជាការងារដ៏សំខាន់ និងសំខាន់បំផុតមួយដើម្បីរក្សារាល់ការគំរាមកំហែងការងារព្យាបាទ ការវាយប្រហារ ឬកម្មវិធីនានាឱ្យនៅឆ្ងាយពីប្រព័ន្ធសូហ្វវែររបស់កុំព្យូទ័រ ប្រព័ន្ធមួយមានសុវត្ថិភាព ប្រសិនបើធនធានរបស់វាត្រូវបានប្រើប្រាស់ និងចូលប្រើតាមបំណងក្នុងគ្រប់កាលៈទេសៈទាំងអស់ទោះយ៉ាងណាក៏ដោយ គ្មានប្រព័ន្ធណាអាចធានាសុវត្ថិភាពទាំងស្រុងពីការគំរាមកំហែងផ្សេងៗ និងការចូលប្រើដោយគ្មានការអនុញ្ញាត។ សុវត្ថិភាពនៃប្រព័ន្ធអាចត្រូវបានគំរាមកំហែងតាមរយៈការរំលោភបំពានពីរ៖

- **ការគំរាមកំហែង៖** ជាកម្មវិធីដែលអាចបង្កការខូចខាតធ្ងន់ធ្ងរដល់ប្រព័ន្ធ។
- **ការវាយប្រហារ៖** ការប៉ុនប៉ងបំបែកសន្តិសុខសុវត្ថិភាព និងប្រើប្រាស់ទ្រព្យសម្បត្តិដោយគ្មានការអនុញ្ញាត។

ការបំពានផ្នែកសុវត្ថិភាពដែលប៉ះពាល់ដល់ប្រព័ន្ធអាចត្រូវបានចាត់ថ្នាក់ថាជាការគំរាមកំហែងដោយចេតនា ការគំរាមកំហែងព្យាបាទ ដូចដែលឈ្មោះបានបង្ហាញ គឺជាកូដកុំព្យូទ័រដែលមានគ្រោះថ្នាក់ ឬស្ត្រីបគេហទំព័រដែលត្រូវបានរចនាឡើងដើម្បីបង្កើតភាពងាយរងគ្រោះរបស់ប្រព័ន្ធដែលនាំទៅដល់ទ្វារខាងក្រោយ និងការរំលោភលើសុវត្ថិភាព ម្យ៉ាងវិញទៀត ការគំរាមកំហែងដោយចៃដន្យ គឺងាយស្រួលជាងក្នុងការការពារ។ ឧទាហរណ៍៖ ការបដិសេធសេវាកម្ម DDoS វាយប្រហារ។ សុវត្ថិភាពអាចត្រូវបានសម្របសម្រួលតាមរយៈការបំពានណាមួយដែលបានរៀបរាប់៖

- **ការរំលោភលើការសម្ងាត់៖** ការបំពានប្រភេទនេះពាក់ព័ន្ធនឹងការអានទិន្នន័យដែលគ្មានការអនុញ្ញាត។

- **ការបំពានលើសុចរិតភាព៖** ការបំពាននេះពាក់ព័ន្ធ នឹងការកែប្រែទិន្នន័យគ្រប់ប្រភេទដែលគ្មានការអនុញ្ញាត។
- **ការរំលោភលើភាពអាចរកបាន៖** វាពាក់ព័ន្ធនឹងការបំផ្លាញទិន្នន័យដោយគ្មានការអនុញ្ញាត។
- **ការលួចសេវា៖** វាពាក់ព័ន្ធនឹងការប្រើប្រាស់ធនធានដែលគ្មានការអនុញ្ញាត។
- **ការបដិសេធសេវាកម្ម៖** វាពាក់ព័ន្ធនឹងការការពារការប្រើប្រាស់ប្រព័ន្ធស្របច្បាប់ ដូចដែលបានរៀបរាប់ពីមុន ការវាយប្រហារបែបនេះអាចកើតឡើងដោយចៃដន្យនៅក្នុងធម្មជាតិ។

៨.៣.១ គោលដៅប្រព័ន្ធសុវត្ថិភាព

ចាប់ពីពេលនេះតទៅ ដោយផ្អែកលើការបំពានខាងលើ គោលដៅសុវត្ថិភាពខាងក្រោមមានគោលបំណង៖

- **ភាពសុចរិត៖** វត្ថុនៅក្នុងប្រព័ន្ធមិនត្រូវចូលប្រើដោយអ្នកប្រើប្រាស់ដែលគ្មានការអនុញ្ញាតណាមួយឡើយ ហើយអ្នកប្រើប្រាស់ណាដែលមិនមានសិទ្ធិគ្រប់គ្រាន់ មិនគួរត្រូវបានអនុញ្ញាតឱ្យកែប្រែឯកសារ និងធនធានសំខាន់ៗរបស់ប្រព័ន្ធឡើយ។
- **ការសម្ងាត់៖** វាគឺជាវត្ថុនៃប្រព័ន្ធត្រូវតែអាចចូលប្រើបានតែចំពោះអ្នកប្រើប្រាស់ដែលមានការអនុញ្ញាតមួយចំនួនប៉ុណ្ណោះមិនមែនគ្រប់គ្នាគួរតែអាចមើលឯកសារប្រព័ន្ធបានទេ។
- **ភាពអាចរកបាន៖** ធនធានប្រព័ន្ធទាំងអស់ត្រូវតែអាចចូលប្រើបានសម្រាប់អ្នកប្រើប្រាស់ដែលមានការអនុញ្ញាតទាំងអស់ ពោលគឺមានតែអ្នកប្រើប្រាស់/ដំណើរការមួយប៉ុណ្ណោះមិនគួរមានសិទ្ធិក្នុងការទាញយកធនធានប្រព័ន្ធទាំងអស់នោះទេ ប្រសិនបើស្ថានភាពបែបនេះកើតឡើង ការបដិសេធសេវាកម្មអាចកើតឡើងនៅក្នុងស្ថានភាពបែបនេះ មេរោគអាចទាញយកធនធានសម្រាប់ខ្លួនវា ហើយដូច្នេះរារាំងដំណើរការស្របច្បាប់ពីការចូលប្រើធនធានប្រព័ន្ធ។

៨.៣.២ ការគំរាមកំហែងកម្មវិធី

Hacker បានសរសេរកម្មវិធីមួយដើម្បីលួចយកសុវត្ថិភាព ឬផ្លាស់ប្តូរឥរិយាបថរបស់ដំណើរការធម្មតាម្យ៉ាងវិញទៀតប្រសិនបើកម្មវិធីអ្នកប្រើប្រាស់ត្រូវបានផ្លាស់ប្តូរ និងត្រូវបានបង្កើតឡើងបន្ថែមទៀតដើម្បីបំពេញកិច្ចការព្យាបាទដែលមិនចង់បាននោះ វាត្រូវបានគេស្គាល់ថាជាកម្មវិធីគំរាមកំហែង។ ការគំរាមកំហែងទាំងនេះពាក់ព័ន្ធនឹងការបំពានលើសេវាប្រព័ន្ធពួកគេខិតខំបង្កើតស្ថានភាពដែលធនធានប្រព័ន្ធប្រតិបត្តិការ និងឯកសារអ្នកប្រើប្រាស់ត្រូវបានប្រើប្រាស់ខុសហើយ ត្រូវបានគេប្រើជាឧបករណ៍ផ្ទុកដើម្បីចាប់ផ្តើមការគំរាមកំហែងកម្មវិធីផងដែរ។

ប្រភេទនៃការគំរាមកំហែងកម្មវិធីមានដូចជា៖

១. ទីរុស (Viruses)

ការគំរាមកំហែងដ៏អាក្រក់ដែលគេស្គាល់យ៉ាងទូលំទូលាយបំផុតវាគឺជាខ្សែស្រឡាយដែលចម្លងដោយខ្លួនឯង និងព្យាបាទដែលភ្ជាប់ខ្លួនវាទៅនឹងឯកសារប្រព័ន្ធ ហើយបន្ទាប់មកចម្លងខ្លួនវាយ៉ាងឆាប់រហ័ស កែប្រែ និងបំផ្លាញឯកសារសំខាន់ៗ និងនាំទៅដល់ការបំបែកប្រព័ន្ធ។ លើសពីនេះ ប្រភេទនៃមេរោគកុំព្យូទ័រអាចត្រូវបានពិពណ៌នាដោយសង្ខេបដូចខាងក្រោម៖

- **ឯកសារ/ប៉ារ៉ាស៊ីត៖** បញ្ចូលខ្លួនវាទៅក្នុងឯកសារ
- **ចាប់ផ្តើម / អង្គចងចាំ៖** ប៉ះពាល់ដល់ផ្នែកចាប់ផ្តើម
- **ម៉ាក្រូ៖** សរសេរជាភាសាកម្រិតខ្ពស់ដូចជា VB ហើយប៉ះពាល់ដល់ឯកសារ MS Office
- **កូដប្រភព៖** ស្វែងរក និងកែប្រែកូដប្រភព
- **ប៉ូលីម័រហ្វីក៖** ការផ្លាស់ប្តូរក្នុងការចម្លងរាល់ពេល
- **បានអ៊ិនគ្រីប៖** មេរោគដែលបានអ៊ិនគ្រីប និង ឌិគ្រីបកូដ
- **ការបំបាំងកាយ៖** ជៀសវាងការរកឃើញដោយការកែប្រែផ្នែកនៃប្រព័ន្ធដែលអាចត្រូវបានប្រើដើម្បីស្វែងរកវា ដូចជាការហៅប្រព័ន្ធអាន
- **ផ្លូវរូងក្រោមដី៖** ដំឡើងដោយខ្លួនវាផ្ទាល់នៅក្នុងទម្លាប់នៃសេវាកម្មរំខាន និងកម្មវិធីបញ្ជាឧបករណ៍
- **ពហុភាគី៖** ឆ្លងផ្នែកជាច្រើននៃប្រព័ន្ធ

២. Trojan Horse

ផ្នែកកូដដែលប្រើប្រាស់បរិស្ថានរបស់វាខុសត្រូវបានគេហៅថា Trojan Horse ពួកវាហាក់ដូចជាកម្មវិធីគ្របដណ្តប់ដ៏គួរឱ្យទាក់ទាញ និងគ្មានការបង្កគ្រោះថ្នាក់ ប៉ុន្តែជាកម្មវិធីលាក់កំបាំងដែលបង្កគ្រោះថ្នាក់ដែលអាចប្រើជាអ្នកផ្ទុកមេរោគ។ នៅក្នុងកំណែមួយនៃ Trojan អ្នកប្រើប្រាស់ត្រូវបានបញ្ឆោតក្នុងការបញ្ចូលព័ត៌មានលម្អិតនៃការចូលសម្ងាត់នៅលើកម្មវិធីមួយព័ត៌មានលម្អិតទាំងនោះត្រូវបានលួចដោយកម្មវិធីត្រាប់តាមការចូលហើយអាចត្រូវបានប្រើបន្ថែមទៀតសម្រាប់ការបំពានព័ត៌មានការគំរាមកំហែង ឬផលវិបាកធ្ងន់ធ្ងរ និងធ្ងន់ធ្ងរមួយនៃសេះ Trojan គឺថាវានឹងធ្វើការខូចខាតបានត្រឹមត្រូវនៅពេលដំឡើង ឬដំណើរការលើប្រព័ន្ធកុំព្យូទ័រ ទោះយ៉ាងណាក៏ដោយ នៅក្រឡេកមើលដំបូង វាហាក់ដូចជាកម្មវិធីមានប្រយោជន៍ ហើយក្រោយមកវាប្រែចេញដោយចេតនាអាក្រក់។ ភាពខុសគ្នាមួយទៀតគឺ Spyware ហើយ Spyware អមជាមួយកម្មវិធីដែលអ្នកប្រើប្រាស់បានជ្រើសរើសដើម្បីដំឡើងនិងទាញយកការផ្សាយពាណិជ្ជកម្មដើម្បីបង្ហាញនៅលើប្រព័ន្ធរបស់អ្នកប្រើប្រាស់ បង្កើតបង្អួចកម្មវិធីរុករកលេចឡើងនៅពេលអ្នកប្រើប្រាស់ចូលទៅកាន់គេហទំព័រជាក់លាក់ វាចាប់យកព័ត៌មានសំខាន់ៗ វាបញ្ជូនវាទៅម៉ាស៊ីនមេពីចម្ងាយ។

៣.Trap Door

អ្នករចនាកម្មវិធី ឬប្រព័ន្ធអាចទុករន្ធនៅក្នុងកម្មវិធីដែលមានតែគាត់ប៉ុណ្ណោះដែលអាចប្រើបានទ្វារអន្ទាក់ដំណើរការលើគោលការណ៍ស្រដៀងគ្នា។ ទ្វារអន្ទាក់គឺពិបាកណាស់ក្នុងការរកឃើញ និងវិភាគ អ្នកត្រូវឆ្លងកាត់កូដប្រភពនៃសមាសធាតុប្រព័ន្ធទាំងអស់ ម្យ៉ាងវិញទៀត ប្រសិនបើយើង

ប្រហែលជាត្រូវកំណត់ទ្វារអន្ទាក់ វានឹងមានដូចខាងក្រោម៖ ទ្វារអន្ទាក់គឺជាប្រភេទនៃចំណុចចូលសម្ងាត់ទៅក្នុងកម្មវិធីដែលកំពុងដំណើរការ ឬបិតវិន្ត ដែលអនុញ្ញាតឱ្យនរណាម្នាក់ចូលប្រើប្រព័ន្ធណាមួយដោយមិនចាំបាច់ឆ្លងកាត់ការចូលប្រើសុវត្ថិភាពធម្មតានីតិវិធី។

៤. Logic Bomb

កម្មវិធីដែលផ្តួចផ្តើមការវាយប្រហារផ្នែកសន្តិសុខតែនៅក្រោមស្ថានភាពជាក់លាក់មួយ ដើម្បីឱ្យច្បាស់លាស់ Logic Bomb គឺជាកម្មវិធីព្យាបាទបំផុត ដែលបញ្ចូលក្នុងប្រព័ន្ធកុំព្យូទ័រដោយចេតនាវាត្រូវបានកេះ ឬដំណើរការនៅពេលដែលលក្ខខណ្ឌជាក់លាក់ត្រូវបានបំពេញដើម្បីឱ្យវាដំណើរការយ៉ាងរលូន។

៥. Worm:

ដង្កូវកុំព្យូទ័រ គឺជាមេរោគមួយប្រភេទដែលចម្លងខ្លួនវា និងឆ្លងទៅកុំព្យូទ័រផ្សេងទៀត ខណៈពេលដែលវានៅតែសកម្មនៅលើប្រព័ន្ធដែលរងផលប៉ះពាល់។ ដង្កូវកុំព្យូទ័រកើតឡើងម្តងទៀតដើម្បីឆ្លងម៉ាស៊ីនដែលមិនបានឆ្លងជាញឹកញាប់វាសម្រេចបានដោយការទាញយកអត្ថប្រយោជន៍ពីសមាសធាតុនៃប្រព័ន្ធប្រតិបត្តិការដែលមានដោយស្វ័យប្រវត្តិ និងមិនមាននរណាកត់សម្គាល់ដោយអ្នកប្រើប្រាស់ ដង្កូវត្រូវបានគេមើលរំលងជាញឹកញាប់រហូតដល់ការចម្លងដោយមិនអាចគ្រប់គ្រងបានរបស់វាបំផ្លាញធនធានរបស់ប្រព័ន្ធ ការយឺតយ៉ាវ ឬបញ្ឈប់សកម្មភាពផ្សេងទៀត។

៨.៣.៣ ប្រភេទនៃការគំរាមកំហែងប្រព័ន្ធ

ក្រៅពីការគំរាមកំហែងកម្មវិធី ការគំរាមកំហែងរបស់ប្រព័ន្ធផ្សេងៗក៏កំពុងតែបង្កគ្រោះថ្នាក់ដល់សុវត្ថិភាពប្រព័ន្ធ។ កម្មវិធីឆ្លងមេរោគដែលរីករាលដាលតាមបណ្តាញ មិនដូចមេរោគទេ ពួកវាកំណត់គោលដៅជាចម្បង LANs។ កុំព្យូទ័រដែលរងផលប៉ះពាល់ដោយពពួក Worm វាយប្រហារប្រព័ន្ធគោលដៅ ហើយសរសេរកម្មវិធីតូចមួយ ``hook`` នៅលើវា ទំពក់នេះត្រូវបានប្រើបន្ថែមទៀតដើម្បីចម្លងដង្កូវទៅកុំព្យូទ័រគោលដៅ។ ដំណើរការនេះកើតឡើងដដែលៗ ហើយមិនយូរប៉ុន្មាន ប្រព័ន្ធទាំងអស់នៃ LAN ត្រូវបានរងផលប៉ះពាល់ វាប្រើយន្តការពងដើម្បីចម្លងខ្លួនឯង ដង្កូវបង្កើតច្បាប់ចម្លងដោយខ្លួនឯង ដោយប្រើធនធានប្រព័ន្ធភាគច្រើន និងបិទដំណើរការផ្សេងទៀតទាំងអស់។ មុខងារជាមូលដ្ឋាននៃពពួក Worm អាចត្រូវបានតំណាងដូចខាងក្រោម៖

- **ការស្កេនតាមច្រក**

ការស្កេនតាមច្រកគឺជាមធ្យោបាយដែលពួក Hacker កំណត់អត្តសញ្ញាណភាពងាយរងគ្រោះនៃប្រព័ន្ធដើម្បីវាយប្រហារហើយដំណើរការស្វ័យប្រវត្តិដែលពាក់ព័ន្ធនឹងការបង្កើតការតភ្ជាប់ TCP/IP ទៅកាន់ច្រកជាក់លាក់មួយ។ ដើម្បីការពារអត្តសញ្ញាណរបស់អ្នកវាយប្រហារ ការវាយប្រហារស្កេនច្រកត្រូវបានចាប់ផ្តើមពីប្រព័ន្ធ Zombie ដែលជាប្រព័ន្ធឯករាជ្យពីមុនដែលបម្រើម្ចាស់របស់ពួកគេផងដែរ ខណៈពេលដែលត្រូវបានប្រើប្រាស់សម្រាប់គោលបំណងដ៏ល្បីបែបនេះ។

❖ ការបដិសេធសេវាកម្ម

ការវាយប្រហារបែបនេះមិនមានគោលបំណងប្រមូលព័ត៌មាន ឬបំផ្លាញឯកសារប្រព័ន្ធទេ ផ្ទុយទៅវិញ ពួកវាត្រូវបានប្រើដើម្បីរំខានដល់ការប្រើប្រាស់ប្រព័ន្ធ ឬឧបករណ៍ស្របច្បាប់។

ការវាយប្រហារទាំងនេះជាទូទៅផ្អែកលើបណ្តាញហើយការវាយប្រហារគេចែកចេញជាពីរប្រភេទ៖

- ការវាយប្រហារនៅក្នុងប្រភេទទីមួយនេះអាចប្រើប្រាស់ធនធានប្រព័ន្ធជាច្រើនដែលមិនមានការងារជាក់ស្តែងអាចត្រូវបានអនុវត្ត។ ឧទាហរណ៍ ការទាញយកឯកសារពីគេហទំព័រដែលបន្តប្រើប្រាស់គ្រប់ពេលវេលាដែលមាន។
- ការវាយប្រហារក្នុងប្រភេទទីពីរពាក់ព័ន្ធនឹងការរំខានបណ្តាញនៃកន្លែង ការវាយប្រហារទាំងនេះបណ្តាលមកពីការបំពានគោលការណ៍ TCP/IP ជាមូលដ្ឋានមួយចំនួន។ មុខងារជាមូលដ្ឋាននៃ TCP/IP ។

៨.៤ សុវត្ថិភាពគេហទំព័រ

សុវត្ថិភាពគឺសំខាន់ចំពោះសេវាកម្មគេហទំព័រ ទោះយ៉ាងណាក៏ដោយ ទាំង XML-RPC ឬ SOAP ជាក់លាក់មិនធ្វើឱ្យមានតម្រូវការសុវត្ថិភាព ឬការផ្ទៀងផ្ទាត់ច្បាស់លាស់ណាមួយឡើយ។

មានបញ្ហាសុវត្ថិភាពជាក់លាក់ចំនួនបីជាមួយសេវាកម្មគេហទំព័រ៖

- ការសម្ងាត់
- ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ
- សុវត្ថិភាពបណ្តាញ

❖ ការសម្ងាត់

ប្រសិនបើអតិថិជនផ្ញើសំណើ XML ទៅម៉ាស៊ីនមេ តើយើងអាចធានាថាទំនាក់ទំនងនៅតែរក្សាការសម្ងាត់ដោយរបៀបណា?

- XML-RPC និង SOAP ដំណើរការជាចម្បងនៅលើ HTTP ។
- HTTP មានការគាំទ្រសម្រាប់ Secure Sockets Layer (SSL)។
- ការទំនាក់ទំនងអាចត្រូវបានអ៊ិនគ្រីបតាមរយៈ SSL ។
- SSL គឺជាបច្ចេកវិទ្យាដែលបង្ហាញឱ្យឃើញ និងត្រូវបានប្រើប្រាស់យ៉ាងទូលំទូលាយ។

សេវាបណ្តាញតែមួយអាចមានខ្សែសង្វាក់នៃកម្មវិធី។ ឧទាហរណ៍ សេវាធំមួយអាចភ្ជាប់សេវាកម្មនៃកម្មវិធីបីផ្សេងទៀត ក្នុងករណីនេះ SSL មិនគ្រប់គ្រាន់ទេ សារត្រូវតែត្រូវបានអ៊ិនគ្រីបនៅថ្នាំងនីមួយៗតាមបណ្តោយផ្លូវសេវាកម្ម ហើយថ្នាំងនីមួយៗតំណាងឱ្យតំណាខ្សោយដែលមានសក្តានុពលនៅក្នុងខ្សែសង្វាក់។ បច្ចុប្បន្ននេះ មិនមានដំណោះស្រាយដែលយល់ព្រមចំពោះបញ្ហានេះទេ ប៉ុន្តែ

ដំណោះស្រាយដ៏ជោគជ័យមួយគឺស្តង់ដារការអ៊ិនគ្រីប W3C XML ។ ស្តង់ដារនេះផ្តល់នូវក្របខ័ណ្ឌ សម្រាប់ការអ៊ិនគ្រីប និងឌិគ្រីបឯកសារ XML ទាំងមូល ឬគ្រាន់តែជាផ្នែកនៃឯកសារ XML ប៉ុណ្ណោះ។ អ្នកអាចពិនិត្យមើលវានៅ www.w3.org/Encryption ។

❖ ការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវ

អតិថិជនភ្ជាប់ទៅសេវាកម្មបណ្តាញតើយើងកំណត់អត្តសញ្ញាណអ្នកប្រើប្រាស់ដោយរបៀបណា? តើអ្នកប្រើត្រូវបានអនុញ្ញាតឱ្យប្រើសេវាកម្មឬទេ? ជម្រើសខាងក្រោមអាចត្រូវបានពិចារណា ប៉ុន្តែការយល់ស្របច្បាស់លាស់លើគ្រោងការណ៍ការផ្ទៀងផ្ទាត់ដ៏រឹងមាំចាំបាច់ត្រូវបង្កើតឡើង។

- HTTP រួមបញ្ចូលការគាំទ្រដែលភ្ជាប់មកជាមួយសម្រាប់ការផ្ទៀងផ្ទាត់មូលដ្ឋាន និង Digest ហើយដូច្នេះសេវាកម្មអាចត្រូវបានការពារតាមរបៀបដូចគ្នាដែលឯកសារ HTML ត្រូវបានការពារនាពេលបច្ចុប្បន្ន។
- SOAP Digital Signature (SOAP-DSIG) ប្រើប្រាស់ការគ្រីបសោសាធារណៈដើម្បីធ្វើការចុះហត្ថលេខា លើសារ SOAP ជាឌីជីថល។ វាអនុញ្ញាតឱ្យម៉ាស៊ីនភ្ញៀវ ឬម៉ាស៊ីនមេ ធ្វើសុពលភាពអត្តសញ្ញាណរបស់ភាគីម្ខាងទៀត។ ពិនិត្យវានៅ www.w3.org/TR/SOAP-design ។
- អង្គការសម្រាប់ភាពជឿនលឿននៃស្តង់ដារព័ត៌មានដែលមានរចនាសម្ព័ន្ធ (OASIS) កំពុងធ្វើការលើភាសាសម្គាល់ការអះអាងសុវត្ថិភាព (SAML)។

❖ សុវត្ថិភាពបណ្តាញ

សុវត្ថិភាពបណ្តាញគឺសំដៅលើវិធានការដែលធ្វើឡើងដោយសហគ្រាស ឬស្ថាប័នណាមួយ ដើម្បីការពារបណ្តាញកុំព្យូទ័រ និងទិន្នន័យរបស់ខ្លួន ដោយប្រើប្រាស់ទាំងប្រព័ន្ធ ផ្នែករឹង និង ផ្នែកទន់។ នេះមានគោលបំណងធានាការសម្ងាត់ និងលទ្ធភាពប្រើប្រាស់ទិន្នន័យ និងបណ្តាញ គ្រប់ក្រុមហ៊ុន ឬស្ថាប័នដែលគ្រប់គ្រងទិន្នន័យយ៉ាងច្រើន មានកម្រិតនៃដំណោះស្រាយប្រឆាំងនឹងការគំរាមកំហែងតាមអ៊ីនធឺណិតជាច្រើន សន្តិសុខបណ្តាញបានក្លាយជាប្រធានបទសំខាន់នៃសន្តិសុខតាមអ៊ីនធឺណិតជាមួយនឹងអង្គការជាច្រើនដែលអញ្ជើញកម្មវិធីពីអ្នកដែលមានជំនាញនៅក្នុងផ្នែកនេះ។

ដំណោះស្រាយសុវត្ថិភាពបណ្តាញការពារភាពងាយរងគ្រោះផ្សេងៗនៃប្រព័ន្ធកុំព្យូទ័រដូចជា៖

- អ្នកប្រើប្រាស់
- ទីតាំង
- ទិន្នន័យ
- ឧបករណ៍
- កម្មវិធី

មេរៀនសង្ខេប

នៅក្នុងមេរៀននេះអ្នកបានសិក្សាអំពី៖

- គោលបំណងសំខាន់នៃសុវត្ថិភាពព័ត៌មានគឺដើម្បីការពារទិន្នន័យឯកជនរបស់អ្នកប្រើប្រាស់ពីការចូលប្រើប្រាស់ដោយគ្មានការអនុញ្ញាត ការក្លែងបន្លំអត្តសញ្ញាណ។ វាការពារភាពឯកជននៃព័ត៌មាន និងផ្នែករឹងដែលគ្រប់គ្រង រក្សាទុក និងបញ្ជូនព័ត៌មាននោះ។
- Malware ខ្លីសម្រាប់ "កម្មវិធីព្យាបាទ" សំដៅលើកម្មវិធីដែលរំខានណាមួយដែលត្រូវបានបង្កើតឡើងដោយឧក្រិដ្ឋជនតាមអ៊ីនធឺណិត (ជាញឹកញាប់ហៅថា "ពួក Hacker") ដើម្បីលួចទិន្នន័យ និងធ្វើឱ្យខូចខាត ឬបំផ្លាញកុំព្យូទ័រ និងប្រព័ន្ធកុំព្យូទ័រ។
- បច្ចេកទេសការពារកុំព្យូទ័រ ម៉ាស៊ីនមេ ឧបករណ៍ចល័ត ប្រព័ន្ធអេឡិចត្រូនិក បណ្តាញ និងទិន្នន័យប្រឆាំងនឹងការឈ្លានពានអរិភាព ត្រូវបានគេស្គាល់ថាជាសន្តិសុខតាមអ៊ីនធឺណិត។ វាត្រូវបានគេស្គាល់ផងដែរថាជាសន្តិសុខព័ត៌មានអេឡិចត្រូនិក ឬសន្តិសុខបច្ចេកវិទ្យាព័ត៌មាន។
- ប្រព័ន្ធឈ្មោះដែន (DNS) ត្រូវបានប្រើដើម្បីដោះស្រាយឈ្មោះដែនម៉ាស៊ីនទៅអាសយដ្ឋាន IP អ្នកប្រើប្រាស់បណ្តាញពឹងផ្អែកលើមុខងារ DNS ជាចម្បងក្នុងអំឡុងពេលរុករកអ៊ីនធឺណិតដោយវាយបញ្ចូល URL នៅក្នុងកម្មវិធីរុករកតាមអ៊ីនធឺណិត។
- Transmission Control Protocol (TCP) និង Internet Protocol (IP) គឺជាពិធីការបណ្តាញកុំព្យូទ័រពីរផ្សេងគ្នាដែលភាគច្រើនប្រើជាមួយគ្នា។ ដោយសារតែប្រជាប្រិយភាព និងការទទួលយកយ៉ាងទូលំទូលាយ ពួកគេត្រូវបានបង្កើតឡើងនៅក្នុងប្រព័ន្ធប្រតិបត្តិការទាំងអស់នៃឧបករណ៍បណ្តាញ។
- ការគំរាមកំហែងទាំងនេះពាក់ព័ន្ធនឹងការបំពានលើសេវាប្រព័ន្ធពួកគេខិតខំបង្កើតស្ថានភាពដែលធនធានប្រព័ន្ធប្រតិបត្តិការ និងឯកសារអ្នកប្រើប្រាស់ត្រូវបានប្រើប្រាស់ខុស។
- សុវត្ថិភាពមានសារៈសំខាន់ចំពោះសេវាកម្មគេហទំព័រ។ ទោះយ៉ាងណាក៏ដោយ ទាំង XML-RPC ឬ SOAP ជាក់លាក់មិនធ្វើឱ្យមានតម្រូវការសុវត្ថិភាព ឬការផ្ទៀងផ្ទាត់ច្បាស់លាស់ណាមួយឡើយ។
- សេវាបណ្តាញតែមួយអាចមានខ្សែសង្វាក់នៃកម្មវិធី។ ឧទាហរណ៍ សេវាធំមួយអាចភ្ជាប់សេវាកម្មនៃកម្មវិធីបីផ្សេងទៀត ក្នុងករណីនេះ SSL មិនគ្រប់គ្រាន់ទេ។ សារត្រូវតែត្រូវបានអ៊ិនគ្រីបនៅថ្នាំងនីមួយៗតាមបណ្តោយផ្លូវសេវាកម្ម ហើយថ្នាំងនីមួយៗតំណាងឱ្យតំណខ្សោយដែលមានសក្តានុពលនៅក្នុងខ្សែសង្វាក់បច្ចុប្បន្ននេះ មិនមានដំណោះស្រាយដែលយល់ព្រមចំពោះបញ្ហានេះទេ ប៉ុន្តែដំណោះស្រាយដ៏ជោគជ័យមួយគឺស្តង់ដារការអ៊ិនគ្រីប W3C XML ។

សំណួរ

១. តើការគំរាមកំហែង និងការវាយប្រហារបណ្តាញសុវត្ថិភាពមានអ្វីខ្លះ?

២. តើអ្វីជាការគំរាមកំហែងផ្នែកសន្តិសុខ?

៣. តើមេរោគជាអ្វី?

៤. ចូរពន្យល់ពីមេរោគដែលអ្នកស្គាល់។

៥. តើសុវត្ថិភាពបណ្តាញគឺជាអ្វី?

ការអនុវត្តន៍ទី៨

ក. តើការគ្រប់គ្រងបណ្តាញគឺជាអ្វី?

ការគ្រប់គ្រងបណ្តាញគឺគ្រប់គ្រង និងដំណើរការបណ្តាញទិន្នន័យដោយប្រើប្រព័ន្ធគ្រប់គ្រងបណ្តាញ។ ប្រព័ន្ធគ្រប់គ្រងបណ្តាញបច្ចុប្បន្នប្រើប្រាស់កម្មវិធី និងផ្នែករឹងដើម្បីប្រមូល និងវិភាគទិន្នន័យឥតឈប់ឈរ និងជំរុញការផ្លាស់ប្តូរការកំណត់រចនាសម្ព័ន្ធសម្រាប់ការបង្កើនប្រសិទ្ធភាព ភាពជឿជាក់ និងសុវត្ថិភាពវាពាក់ព័ន្ធនឹងការកំណត់រចនាសម្ព័ន្ធការត្រួតពិនិត្យ និងអាចកំណត់រចនាសម្ព័ន្ធឡើងវិញនូវសមាសធាតុនៅក្នុងបណ្តាញ ដើម្បីផ្តល់នូវដំណើរការល្អបំផុត ពេលវេលារង់ចាំអប្បបរមា ការការពារត្រឹមត្រូវ គណនេយ្យភាព និងភាពបត់បែន។

ខ.សុវត្ថិភាពបណ្តាញ

សុវត្ថិភាពបណ្តាញគឺជាឧបករណ៍ ឬវិធានការចាំបាច់ដែលសំដៅលើសុវត្ថិភាពក្នុងហេដ្ឋារចនាសម្ព័ន្ធបណ្តាញ នៅពេលដែលអ្នកប្រើប្រាស់ដែលគ្មានការអនុញ្ញាតព្យាយាមចូលប្រើបណ្តាញ សុវត្ថិភាពបណ្តាញមានគោលបំណងទប់ស្កាត់ការចូលប្រើដែលមិនមានការអនុញ្ញាត ឬការពារឥរិយាបថបណ្តាញមិនប្រក្រតីជាមុន។

គ. គោលបំណងនៃការអនុវត្តនេះ

ការកំណត់ Port Security នៅលើSwitch Port Security មានន័យថាកំណត់ចំនួនអាសយដ្ឋាន MAC ដែលបានអានពី switch ឬអនុញ្ញាតឱ្យចូលប្រើតែអាសយដ្ឋាន MAC ជាក់លាក់ប៉ុណ្ណោះ។ ការការពារបណ្តាញគឺអាចធ្វើទៅបានដោយការទប់ស្កាត់អាសយដ្ឋាន MAC ដែលគ្មានការអនុញ្ញាតនៅពេលពួកគេចូលប្រើ។

គ១. ការកំណត់ចំនួននៃការចូលប្រើ

```
Switch>en
Switch#config terminal
Switch(config)#interface fa0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security maximum 2
```

```
Switch(config-if)#switchport port-security violation shutdown
```

ក២.បញ្ជាក់អាសយដ្ឋាន MAC ដែលអាចចូលប្រើបាន

ប្រសិនបើអាសយដ្ឋាន MAC ច្រើនជាង 2 អាចចូលប្រើបានច្រើនបំផុតនៅលើច្រក fa0/0 នោះសូមព្យាយាមយកច្រកនោះចុះ។

```
Switch>en
Switch#config terminal
Switch(config)#interface fa0/0
Switch(config-if)#switchport mode access
Switch(config-if)#switchport port-security
Switch(config-if)#switchport port-security mac-address stricky
Switch(config-if)#switchport port-security mac-address XXXX.XXXX.XXX[mac address]
Switch(config-if)#switchport port-security violation shutdown
```

ឃ. តើសន្តិសុខបណ្តាញគឺជាអ្វី?

សុវត្ថិភាពបណ្តាញគឺជាពាក្យទូលំទូលាយដែលគ្របដណ្តប់លើបច្ចេកវិទ្យា ឧបករណ៍ និងដំណើរការជាច្រើននៅក្នុងនិយមន័យដ៏ត្រង់បំផុត វាគឺជាសំណុំនៃច្បាប់ និងការកំណត់រចនាឡើងដើម្បីការពារភាពសុចរិត ការសម្ងាត់ និងភាពងាយស្រួលនៃបណ្តាញកុំព្យូទ័រ និងទិន្នន័យដោយប្រើទាំងផ្នែកទន់ និងបច្ចេកវិទ្យាផ្នែករឹង។ គ្រប់ស្ថាប័នទាំងអស់ ដោយមិនគិតពីទំហំ ឧស្សាហកម្ម ឬហេដ្ឋារចនាសម្ព័ន្ធ ទាមទារកម្រិតនៃដំណោះស្រាយសុវត្ថិភាពបណ្តាញ ដើម្បីការពារវាពីទិដ្ឋភាពដែលកំពុងរីកចម្រើននៃការគំរាមកំហែងតាមអ៊ីនធឺណិតនៅលើពិភពលោកនាពេលបច្ចុប្បន្ននេះ។

- **ការកំណត់ពាក្យសម្ងាត់នៅលើរ៉ោតទ័រ**

```
Router>en
Router#conf t
Router(config)#enable password [password]
Router(config)#exit
```

-ឧទាហរណ៍នៃការកំណត់ពាក្យសម្ងាត់រ៉ោតទ័រ

```
Router>en
Router#conf t
Router(config)#enable password hello!@#
Router(config)#exit
Router#exit
```

-ត្រូវប្រាកដថាពាក្យសម្ងាត់របស់អ្នកត្រូវបានកំណត់ត្រឹមត្រូវ។

```
Router>en
password:
Router#
```

❖ រៀបចំបញ្ជីចូលប្រើដើម្បីលើរ៉ោតទ័ររបស់អ្នក

បញ្ជីការចូលប្រើគឺជាពាក្យបញ្ជាដែលគ្រប់គ្រងកញ្ចប់ព័ត៌មានចូលប្រើរ៉ោតទ័រ អ្នកអាចកំណត់វាដើម្បីអនុញ្ញាត ឬរារាំងការចូលប្រើកញ្ចប់ព័ត៌មានជាក់លាក់។

១.វិធីសាស្ត្រដំឡើងបញ្ជីការចូលប្រើស្តង់ដារ

```
Router>en
Router(config)#access-list [Number] [Permit] ı [Deny] [IP]
```

ឧទាហរណ៍៖ ការកំណត់ការអនុញ្ញាត 192.168. 0.1

```
Router>en
Router(config)#access-list 10 permit 192.168.0.1 0.0.0.255
```

ឧទាហរណ៍៖ ការបដិសេធ 192.168. 0.1

```
Router>en
Router(config)#access-list 10 deny 192.168.0.1 0.0.0.255
```

ឧទាហរណ៍៖ ការកំណត់ការអនុញ្ញាតទាំងអស់

```
Router>en
Router(config)#access-list 99 permits any
```

ឧទាហរណ៍៖ ការកំណត់ការអនុញ្ញាតទាំងអស់

```
Router>en
Router(config)#access-list 1 deny 255.255.255.255
```

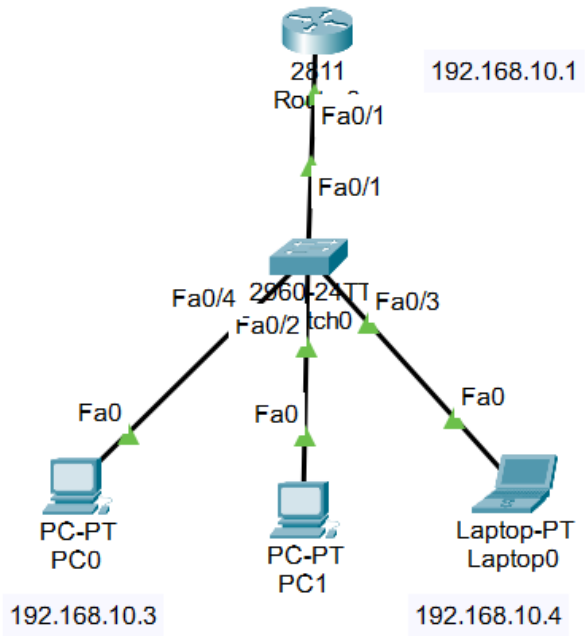
៦.កិច្ចការស្រាវជ្រាវ

កិច្ចការទី១ .កំណត់រចនាសម្ព័ន្ធបណ្តាញ

ក. កំណត់ Port Security ទៅលើ FastEthernet 0/3 ដើម្បីប្រាស់បានតែជាមួយកុំព្យូទ័រយួដៃ១ តែប៉ុនណ្ណោះ

ខ.កំណត់ពាក្យសំងាត់លើរ៉ោតទ័រដោយដាក់៖ P@ssw0rd

គ. កំណត់ IP នៅលើកុំព្យូទ័រ Switch និងរ៉ោតទ័រក្នុង LAN តែមួយ



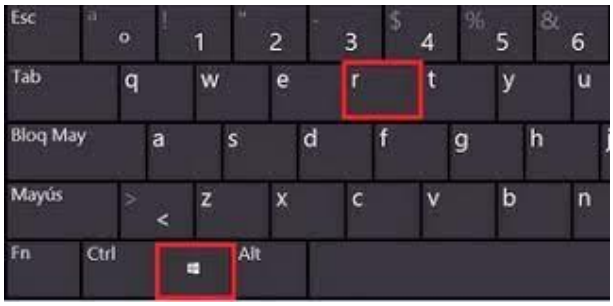
ការអនុវត្តន៍ទី៩

ក. ពាក្យបញ្ជាបណ្តាញនៅក្នុង Windows

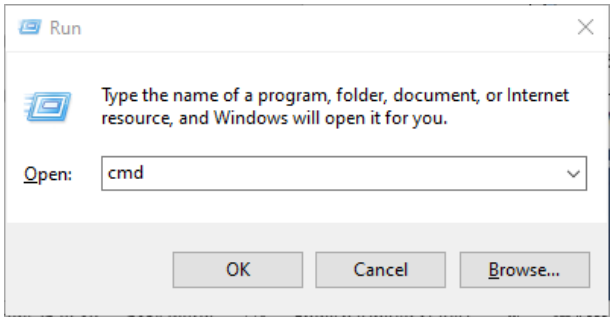
វីនដូគឺជាប្រព័ន្ធប្រតិបត្តិការកុំព្យូទ័រដែលយើងប្រើប្រាស់ប្រចាំថ្ងៃមានពាក្យបញ្ជាផ្ទៀងផ្ទាត់បណ្តាញផ្សេងៗនៅក្នុងវីនដូចនេះផងដែរប្រើពាក្យបញ្ជាខាងក្រោមដើម្បីទទួលបានទិដ្ឋភាពទូទៅនៃកញ្ចប់ព័ត៌មាន និងការកំណត់រចនាសម្ព័ន្ធបណ្តាញនៅក្នុងវីនដូ។

Open Windows Command Shell

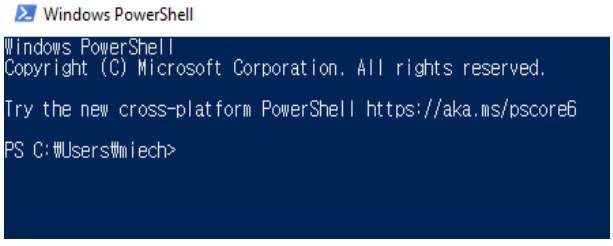
- Windows Key +R



- Type commnad “cmd”

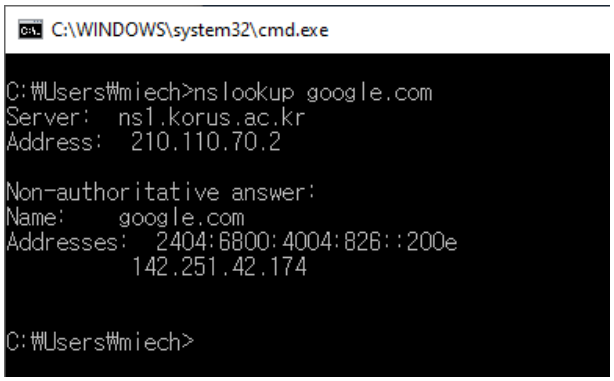


- Open the window command



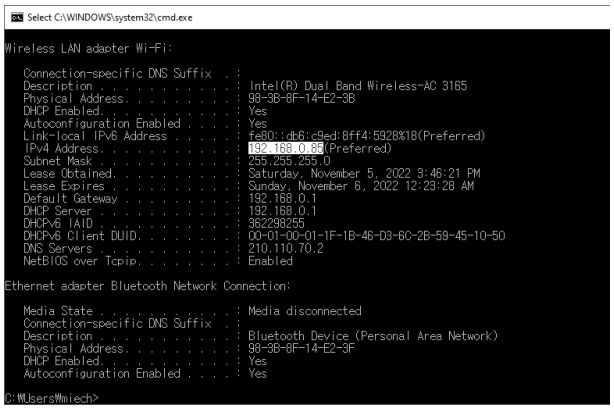
ស្គាល់អាសយដ្ឋាន IP នៃគេហទំព័រ៖

- nslookup google.com



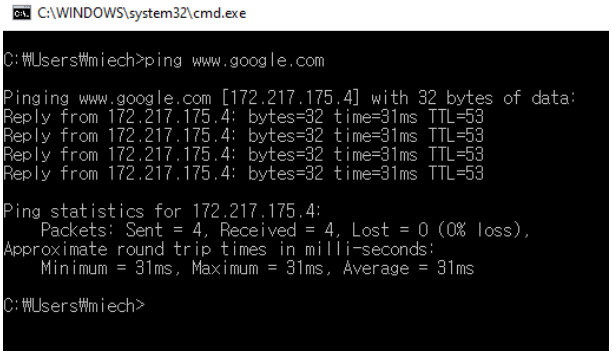
ពិនិត្យអាសយដ្ឋាន IP នៃកុំព្យូទ័រ

- ipconfig
- ipconfig /all



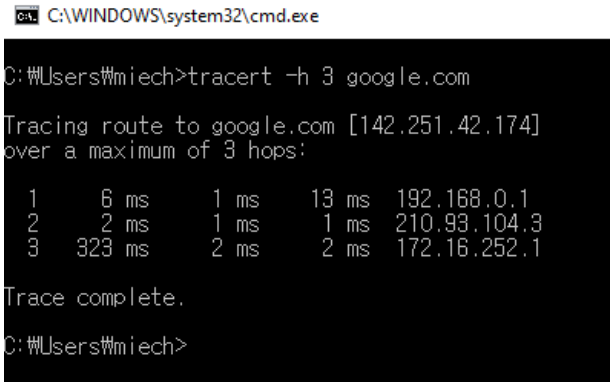
ពិនិត្យពេលវេលាឆ្លើយតប ping ជាមួយ IP គោលដៅ

- ping www.google.com



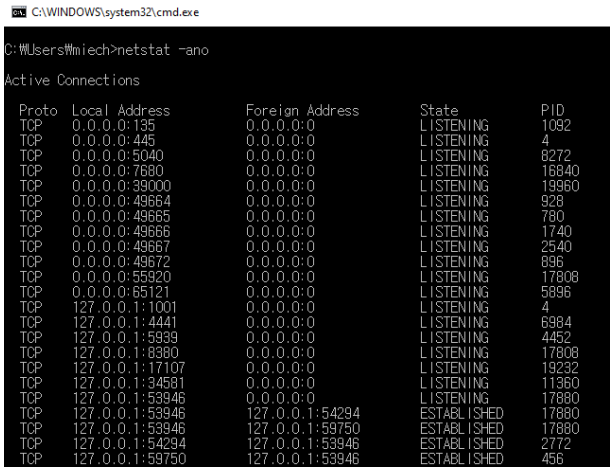
តាមដានរ៉ោតទ័រដែលចូលទៅកាន់គេហទំព័រ

- "tracert [ ]" / "tracert -h 3 [ ]"



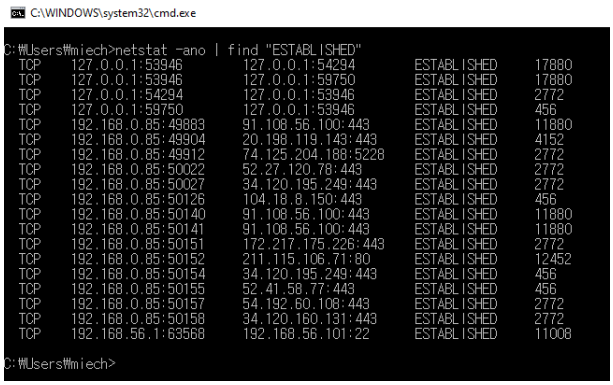
ពិនិត្យ IP ដែលភ្ជាប់ទៅកុំព្យូទ័រ

- netstat -ano



ពិនិត្យស្ថានភាពស្តាប់នៅលើកុំព្យូទ័រ

- "netstat -ano | find "ESTABLISHED"



១.កិច្ចការស្រាវជ្រាវ

កិច្ចការទី១. ចូរប្លូនៗសាកល្បងប្រើប្រាស់ command នៅក្នុងវីនដូរ ដូចខាងក្រោម៖

ក. nslookup google.com

ខ. ipconfig /all

គ. ping www.google.com

ឃ. tracert -h 3 google.com

ង. Netstat -ano

ការអនុវត្តន៍ទី១០

ក. សេចក្តីណែនាំអំពីប្រព័ន្ធប្រតិបត្តិការ Unix

នៅក្នុងការអនុវត្តនេះ អ្នកនឹងរៀនពាក្យបញ្ជាជាមូលដ្ឋានដើម្បីប្រើយូនីកដោយប្រើបរិយាកាសប្រតិបត្តិការលើនុចនៅពេលអ្នកធ្វើការជាអ្នកគ្រប់គ្រងប្រព័ន្ធនៅក្នុងស្ថាប័នរបស់អ្នក អ្នកប្រហែលជាត្រូវស្គាល់ Unix ឱ្យស៊ីជម្រៅ ព្រោះវាទាមទារចំណេះដឹងជ្រៅជ្រះនៃការគ្រប់គ្រងបណ្តាញ ការរៀបចំម៉ាស៊ីនមេ ការគ្រប់គ្រងជាដើម។

❖ តើUnix គឺជាអ្វី?

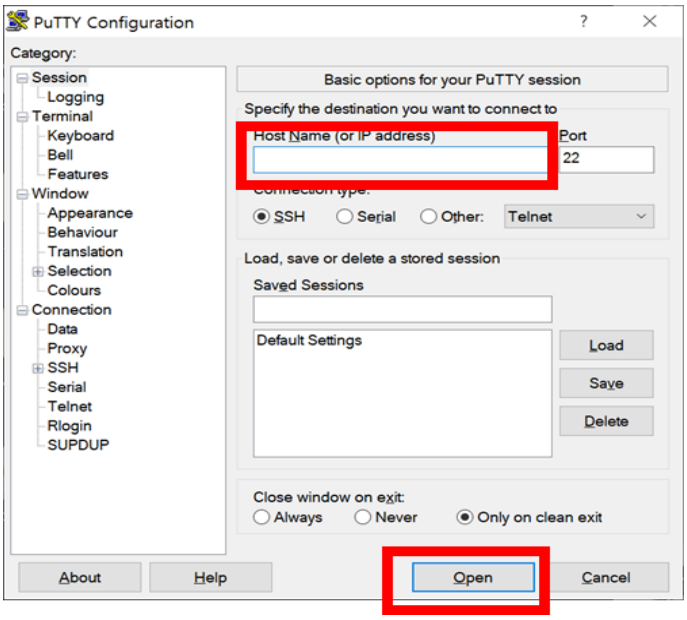
Unix គឺជាប្រព័ន្ធប្រតិបត្តិការសម្រាប់គោលបំណងទូទៅ អ្នកប្រើប្រាស់ច្រើន អន្តរកម្ម ប្រព័ន្ធចែករំលែកពេលវេលា ដែលពេញនិយមនៅក្នុងស្ថាប័នអប់រំ និងស្រាវជ្រាវ។ Unix ត្រូវបានរចនា ឡើងតាំងពីដើមដំបូងមកដើម្បីអាចចល័តបានរវាងប្រព័ន្ធផ្សេងៗនិងដើម្បីគាំទ្រកិច្ចការច្រើននិងអ្នកប្រើច្រើន។ ប្រព័ន្ធ Unix មានគោលគំនិតដូចខាងក្រោម៖

- ចាត់ចែងឯកសារអត្ថបទធម្មតា
- អ្នកបកប្រែបន្ទាត់ពាក្យបញ្ជា
- ប្រព័ន្ធឯកសារតាមឋានានុក្រម
- ការទំនាក់ទំនងរវាងឧបករណ៍
- ប្រភេទដំណើរការមួយចំនួនជាឯកសារ។

❖ ពាក្យបញ្ជាមូលដ្ឋានលើ Unix

ពាក្យបញ្ជាខាងក្រោមដំណើរការលើ OS ដែលមានមូលដ្ឋានលើ Unix ដោយសារតែនេះ កុំព្យូទ័រដែលមានយូនីកឬលើនុចបានដំឡើងចូលប្រើពីចម្ងាយគួរតែត្រូវបានរៀបចំ។ ព័ត៌មានខាងក្រោមគឺត្រូវភ្ជាប់ទៅម៉ាស៊ីនមេ លើនុចពីចម្ងាយដោយប្រើកម្មវិធី Putty ។

១.ការភ្ជាប់ទៅកាន់ម៉ាស៊ីនបម្រើរបស់ Unix



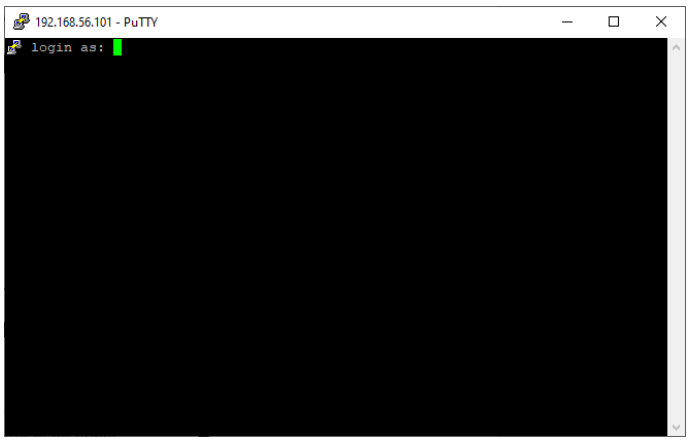
ក.ការភ្ជាប់ទៅម៉ាស៊ីនមេ Unix ពីចម្ងាយដោយប្រើ Putty

ខ.បើកកម្មវិធី Putty

គ. បញ្ចូល IP របស់ Unix server ដើម្បីភ្ជាប់ទៅ Hostname

ឃ.ចុចបើក ដើម្បីភ្ជាប់ទៅម៉ាស៊ីនមេ

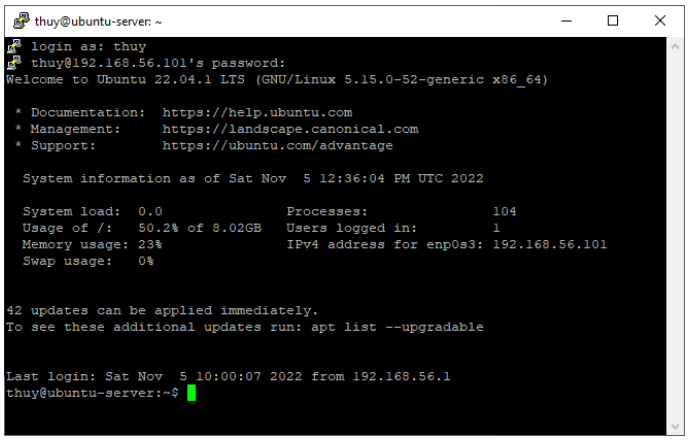
២.ការចូលទៅកាន់ ម៉ាស៊ីនបម្រើ



ក.បញ្ចូលឈ្មោះ គណនីដែលបានបង្កើត

ខ.ធ្វើការចូលទៅកាន់ម៉ាស៊ីនបម្រើ

៣. ដំបូង អ្នកត្រូវតែមាន គណនី និងពាក្យសម្ងាត់ ដើម្បីភ្ជាប់ទៅម៉ាស៊ីនមេ Unix



ក.ពេលបញ្ចូលគណនីហើយ បន្ទាប់មកបញ្ចូលពាក្យសង្ងាត់

ខ.ធ្វើការចូលទៅកាន់ម៉ាស៊ីនបម្រើ

ខ.ការប្រើប្រាស់ពាក្យបញ្ជាសំខាន់ៗ

ពាក្យបញ្ជា	អត្ថន័យ និងខ្លឹមសារ
ifconfig	ពិនិត្យអាសយដ្ឋានរបស់ម៉ាស៊ីន
pwd	ទីតាំងដែល User
cd (path)	ចូលទៅកាន់ (path)
ls	មើលឯកសារទាំងអស់នៅក្នុងថតមួយ
mkdir (directory name)	បង្កើតថតឯកសារ
rmdir (file name)	លុបថតឯកសារ
chmod (authority) (file name)	ផ្លាស់ប្តូរការអនុញ្ញាតឯកសារ

១. Syntax: mkdir (name of folder)

ជាមួយពាក្យបញ្ជា mkdir សម្រាប់បង្កើតថតឯកសារ។ ពាក្យបញ្ជាខាងក្រោមបង្កើតថតដូចឧទាហរណ៍ខាងក្រោម ៖

```
$ mkdir example
```

```
$ mkdir -p example/one/two
```

២. Syntax: List (ls)

ពាក្យបញ្ជា ls ដើម្បីបង្ហាញឯកសារ និងលក្ខណៈសម្បត្តិទាំងអស់របស់ពួកគេនៅក្នុងថតមួយ។ ពាក្យបញ្ជា ls មានជម្រើសជាច្រើន រួមទាំង -l ដើម្បីមើលបញ្ជីវែងនៃឯកសារ និងបង្ហាញម្ចាស់ឯកសារ និងការអនុញ្ញាត។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ ls
```

```
$ ls -l
```

៣. Syntax: Change Directory (cd)

ពាក្យបញ្ជា cd ប្រើប្រាស់សម្រាប់ការផ្លាស់ប្តូរថត។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ cd Documents
```

៤.Syntax : Remove a File (rm)

ពាក្យបញ្ជា rm គឺប្រើប្រាស់សម្រាប់ធ្វើការលុប file ចេញ។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ rm example.txt
```

៥. Syntax: Copy a File (cp)

ពាក្យបញ្ជា cp គឺប្រើប្រាស់សម្រាប់ធ្វើការចម្លងឯកសារ ហើយអាចធ្វើការទៅកាន់ទីតាំងដែលត្រូវការ។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ cp file1.txt newfile1.txt
```

៦. Syntax: Move File (mv)

ពាក្យបញ្ជា mv ប្រើប្រាស់សម្រាប់ធ្វើការផ្លាស់ទីឯកសារ។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ mv file1.txt file_001.txt
```

៧.Syntax: Create an Empty File (touch)

ពាក្យបញ្ជា touch ប្រើប្រាស់សម្រាប់ធ្វើការបង្កើត File ។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ touch one.txt
$ touch two.txt
$ touch three.md
```

៨. Syntax: Change Permissions (chmod)

ពាក្យបញ្ជា chmod ប្រើប្រាស់សម្រាប់ការផ្លាស់ប្តូរការអនុញ្ញាតរបស់ឯកសារ។ មួយនៃការប្រើប្រាស់ទូទៅបំផុតនៃ chmod គឺធ្វើឱ្យឯកសារអាចប្រតិបត្តិបាន។

ឧទាហរណ៍ខាងក្រោម ៖

```
$ chmod +x myfile
```

ឧទាហរណ៍នេះគឺជារបៀបដែលអ្នកផ្តល់សិទ្ធិឱ្យឯកសារដើម្បីប្រតិបត្តិជាពាក្យបញ្ជាវាមានប្រយោជន៍ជាពិសេសសម្រាប់ស្គ្រីប។ សាកល្បងលំហាត់សាមញ្ញនេះ៖

```
$ echo 'echo Hello $USER' > hello.sh
$ chmod +x hello.sh
$ ./hello.sh
Hello, Don
```

៩. Syntax: Shut Down (poweroff)

ពាក្យបញ្ជា poweroff ប្រើប្រាស់សម្រាប់ការម៉ាស៊ីនបម្រើដូចខាងក្រោម៖

ឧទាហរណ៍ខាងក្រោម ៖

```
$ sudo shutdown -h 60

Or immediately:

$ sudo shutdown -h now
```

90.Syntax: chmod -R o-r *.page

ពាក្យបញ្ជា chmod គឺផ្តល់ការអនុញ្ញាតដែលអ្នកចង់ផ្តល់ឱ្យទៅម្ចាស់ ក្រុម និងអ្នកដទៃជាលេខបីខ្ទង់។

- ខ្ទង់ខាងឆ្វេងបំផុតតំណាងឱ្យការអនុញ្ញាតសម្រាប់ម្ចាស់
- ខ្ទង់កណ្តាលតំណាងឱ្យការអនុញ្ញាតសម្រាប់សមាជិកក្រុម
- ខ្ទង់ខាងស្តាំបំផុតតំណាងឱ្យការអនុញ្ញាតសម្រាប់អ្នកដទៃ

លេខដែលអ្នកអាចប្រើបាន និងទទួកស្គាល់ការអនុញ្ញាតមានដូចខាងក្រោម៖

- 0: (000) No permission.
- 1: (001) Execute permission.
- 2: (010) Write permission.
- 3: (011) Write and execute permissions.
- 4: (100) Read permission.
- 5: (101) Read and execute permissions.
- 6: (110) Read and write permissions.
- 7: (111) Read, write, and execute permissions.

ឧទាហរណ៍ខាងក្រោម ៖

$chmod 575 test_education.txt

គ.កិច្ចការស្រាវជ្រាវ

ក. ប្រើពាក្យបញ្ជា PWD ដើម្បីពិនិត្យមើលទីតាំងថតបច្ចុប្បន្ន និងចាប់យកអេក្រង់។

ខ. ដោយប្រើពាក្យបញ្ជា cd ផ្លាស់ទីទៅថតផ្សេងទៀតហើយចាប់យកអេក្រង់ដែលត្រូវគ្នា។

គ. ពិនិត្យឯកសារនៅក្នុងថតបច្ចុប្បន្នដោយប្រើពាក្យបញ្ជា ls –al ។

ឃ. បង្កើតថតថ្មីមួយជាមួយ mkdir ដាក់ឈ្មោះ Document_RTTC, Document_test។

ង. លុបថតដែលបង្កើតដោយ rmdir ដោយធ្វើការលុបចោលនៅថត Document_test។

ច. កែប្រែការអនុញ្ញាតនៃឯកសារមួយជាមួយ chmod ។

- chmod 555 test.txt៖ ប្តូរសិទ្ធិរបស់ឯកសារទៅ r-x r-x r-x ។
- chmod 777 test.txt៖ ប្តូរការអនុញ្ញាតឯកសារទៅជា rwx rwx rwx។

ការអនុវត្តន៍ទី១១

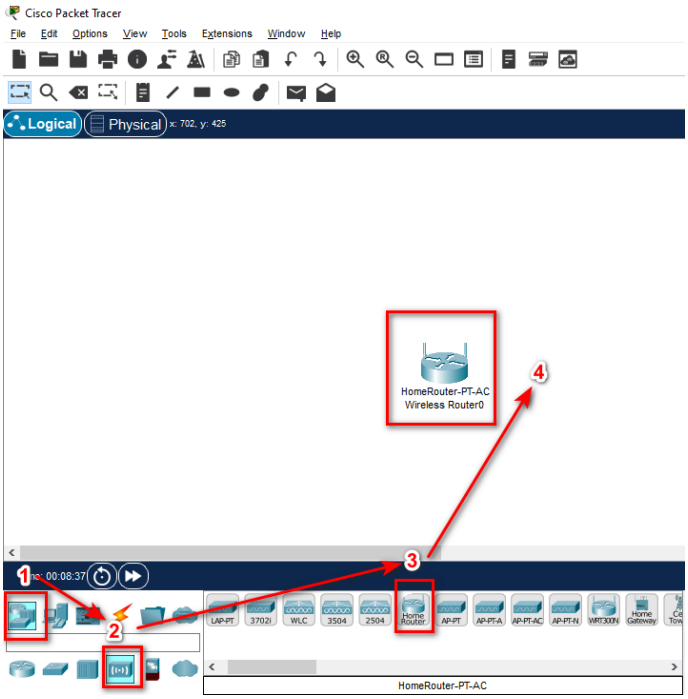
បណ្តាញឥតខ្សែ គឺជាបណ្តាញកុំព្យូទ័រដែលប្រើការតភ្ជាប់ទិន្នន័យឥតខ្សែរវាងថ្នាំងបណ្តាញ ហើយវាសម្រាប់បណ្តាញទំនាក់ទំនងដែលប្រើឥតខ្សែជំនួសឱ្យខ្សែដើម្បីបញ្ជូនសញ្ញា។

ក. គោលបំណងនៃការអនុវត្តនេះ

- ដើម្បីយល់ពីឧបករណ៍បណ្តាញឥតខ្សែនោះ
- ដើម្បីប្រើទៅកាន់រ៉ោតទ័រឥតខ្សែ
- ដើម្បីកំណត់រចនាសម្ព័ន្ធរ៉ោតទ័រឥតខ្សែនៅក្នុង Packet Tracer

ខ. របៀបកំណត់រចនាសម្ព័ន្ធបណ្តាញឥតខ្សែ និងស្ថានភ្ញៀនលើ Packet Tracer

១.ការបន្ថែមរ៉ោតទ័រ Home PT-AC



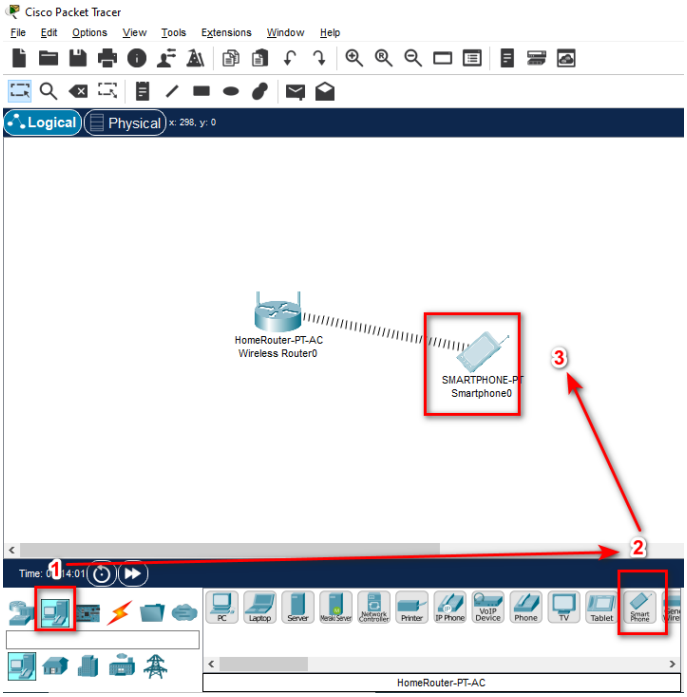
ក.ចុចឧបករណ៍បណ្តាញ(Network Device)

ខ. ចុចលើឧបករណ៍ឥតខ្សែ

គ. ជ្រើសរើស Home Router PT-AC

ឃ. ទាញ Home Router Task PT-AC ទៅកាន់ថ្នាំងកិច្ចការ

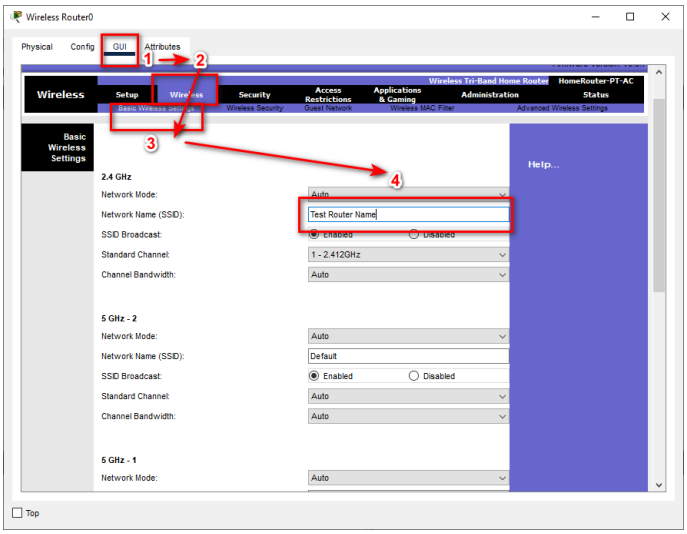
២. បន្ថែមឧបករណ៍ Smart Phone ទៅកាន់ការតភ្ជាប់រ៉ោតទ័រ PT-AC



ក.ចុចលើ ឧបករណ៍(End Device)

ខ. ជ្រើសរើសស្មាតហ្វូន ហើយទម្លាក់ចូលផ្ទាំងកិច្ចការ

៣. កំណត់រចនាសម្ព័ន្ធឈ្មោះ SSID នៅលើ Router PT-AC

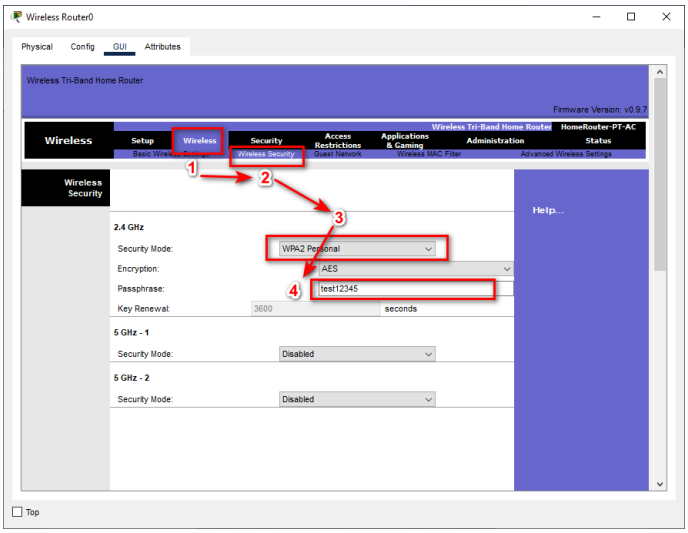


ក. ចុចលើ GUI → Wireless

ខ. ជ្រើសរើស Basic Wireless Setting

គ. នៅត្រង់ In Network Work (SSID): (Test Name Router)

៤. ការដាក់ពាក្យសម្ងាត់ នៅក្នុង Router Device



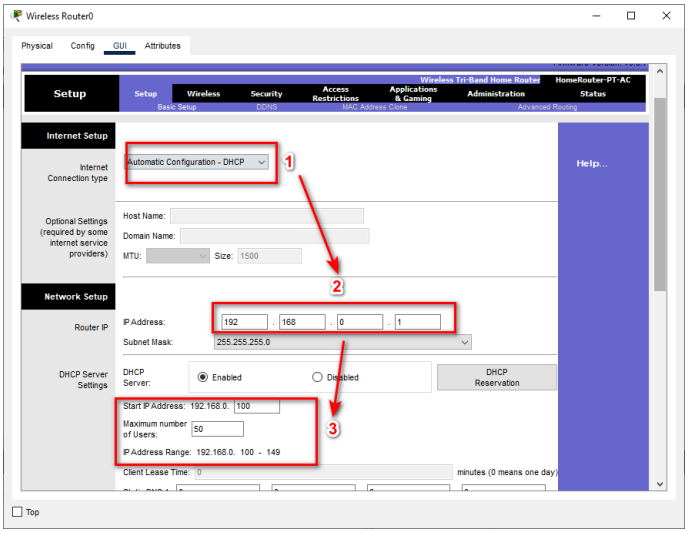
ក. ចុចទៅលើ Click Wireless

ខ. ជ្រើសរើស Click Wireless Security

គ. ជ្រើសរើស WPA2 Personal

ឧ. នៅត្រង់ Passphrase : rttc@edu

៥. កំណត់ការកំណត់រចនាសម្ព័ន្ធដោយស្វ័យប្រវត្តិ DHCP



ក. ចុចទៅលើ Setup

ខ. ជ្រើសរើស Automatic Configuration DHCP

គ. កំណត់ IP Address (192.168.0.1)

ឃ. ត្រង់ Start IP Address (192.168.0.100)

គ.សន្ទេបការអនុវត្តន៍

នៅក្នុងការអនុវត្តដែលយើងបានបង្ហាញខាលើនេះ និយាយពីរបៀបក្នុងការប្រើប្រាស់រ៉ោតទ័រ ដើម្បីធ្វើការបែងចែក IP ទៅកាន់អ្នកប្រើប្រាស់ដោយធ្វើការបោះ IP ដោយស្វ័យប្រវត្តិទៅកាន់ឧបករណ៍ទទួលដូចជាកុំព្យូទ័រ ទូរស័ព្ទស្មាតហ្វូន និងឧបករណ៍ផ្សេងៗទៀតដែលបានធ្វើការស្នើសុំដើម្បីប្រើប្រាស់ក្នុងបណ្តាញ ដោយធ្វើការឆ្លងកាត់រ៉ោតទ័រតែមួួយ។

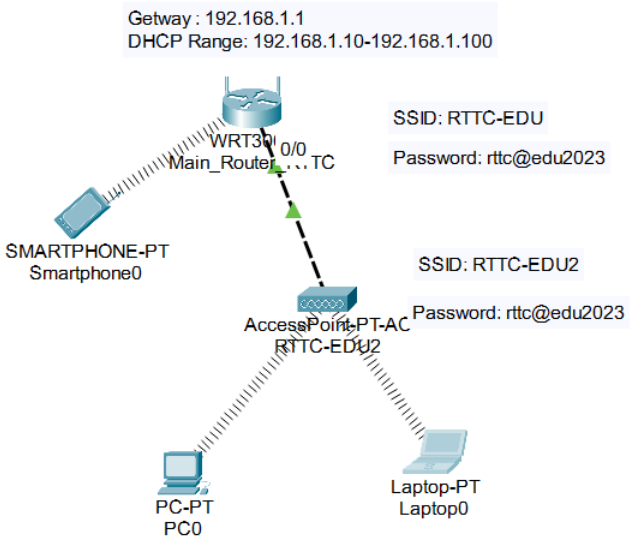
ឃ.កិច្ចការស្រាវជ្រាវ

កិច្ចការ១. ដំឡើងបណ្តាញឥតខ្សែពីរដូចរូបខាងក្រោម៖

ក. បង្កើត Main រ៉ោតទ័រដោយដាក់ Getway: 192.168.1.1

ខ. ដាក់ឈ្មោះ WiFi(SSID) : RTTC-EDU ហើយ Access Point(SSID): RTTC-EDU2 និងធ្វើការប្រើប្រាស់ពាក្យសម្ងាត់ WEP2(Password): rttc@edu2023

គ. យកទូរស័ព្ទស្មានហ្វូន កុំព្យូទ័រលើតុ និងកុំព្យូទ័រយូដៃភ្ជាប់ទៅរ៉ោតទ័រ និង Access Point ដូចរូបខាងក្រោម៖



ការអនុវត្តន៍ទី១២

ក. តើការអ៊ិនគ្រីប (Encryption) គឺជាអ្វី ?

ការអ៊ិនគ្រីបគឺជាវិធីនៃការច្របូកច្របល់ទិន្នន័យ ដូច្នេះមានតែភាគីដែលមានការអនុញ្ញាត ប៉ុណ្ណោះដែលអាចយល់ព័ត៌មានបាន។ នៅក្នុងពាក្យបច្ចេកទេស វាបំប្លែងអត្ថបទធម្មតាដែលអាចអាន បានរបស់មនុស្សទៅជាអត្ថបទដែលមិនអាចយល់បាន ដែលគេស្គាល់ផងដែរថាជា ciphertext នៅ ក្នុងពាក្យសាមញ្ញជាការអ៊ិនគ្រីបយកទិន្នន័យដែលអាចអានបាន ហើយផ្លាស់ប្តូរវាឱ្យលេចឡើងដោយ ចៃដន្យ ការអ៊ិនគ្រីបតម្រូវឱ្យប្រើសោគ្រីប សំណុំនៃតម្លៃគណិតវិទ្យាដែលទាំងអ្នកផ្ញើ និងអ្នកទទួលសារ ដែលបានអ៊ិនគ្រីបយល់ព្រម។

ខ. គោលបំណងនៃការអនុវត្តនេះ

ក. ដើម្បីស្វែងយល់អំពីប្រព័ន្ធឌីជីថល

ខ. ដើម្បីយល់ពីការអ៊ិនគ្រីប DES (Data Encryption Standard) ។

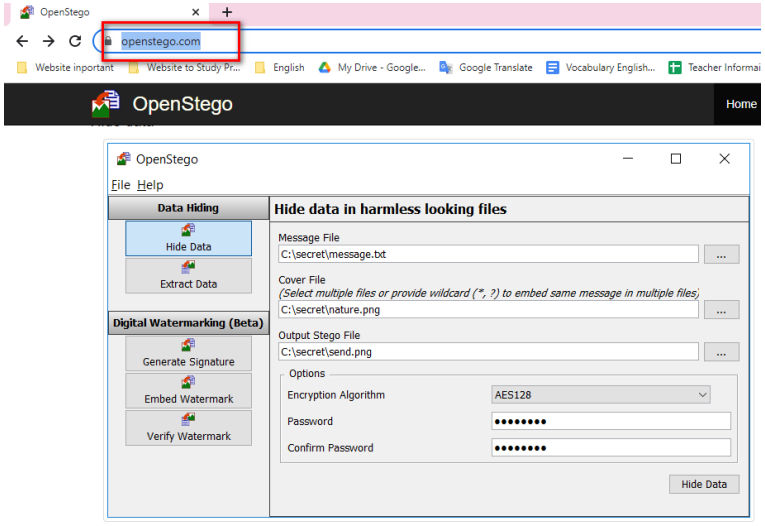
គ. ដើម្បីយល់ពីការអ៊ិនគ្រីប RCA (Rivest-Shamir-Addleman) ។

គ. តើអ្វីទៅជា Digital Steganography ?

Steganography គឺជាបច្ចេកទេសគ្រីបដ៏ស៊ីជម្រៅដែលលាក់ព័ត៌មានសម្ងាត់ដែលអ្នកចង់ បង្ហាញនៅក្នុងឯកសារ សារ រូបភាព ឬវីដេអូនៅក្នុងឯកសារ សារ រូបភាព ឬវីដេអូផ្សេងទៀត។ អត្ថប្រយោជន៍គឺថាវាលាក់ឯកសារនៅក្នុងឯកសារ ហើយប្រសិនបើអ្នកមិនដឹងវិធីសាស្ត្រលាក់វាពិបាក សម្រាប់ភាគីទីបីក្នុងការកត់សម្គាល់។ នៅក្នុងករណីនៃការអ៊ិនគ្រីប ភាគីទីបីក៏អាចរកឃើញថាទិន្នន័យ ត្រូវបានអ៊ិនគ្រីប ហើយព្យាយាមឌិគ្រីបវា ទោះយ៉ាងណាក៏ដោយក្នុងករណី steganography វាមាន សុវត្ថិភាពជាងព្រោះវាពិបាកក្នុងការដឹងថាវាត្រូវបានអ៊ិនគ្រីបឬអត់។

ក១. ការអនុវត្ត Steganography ឌីជីថល

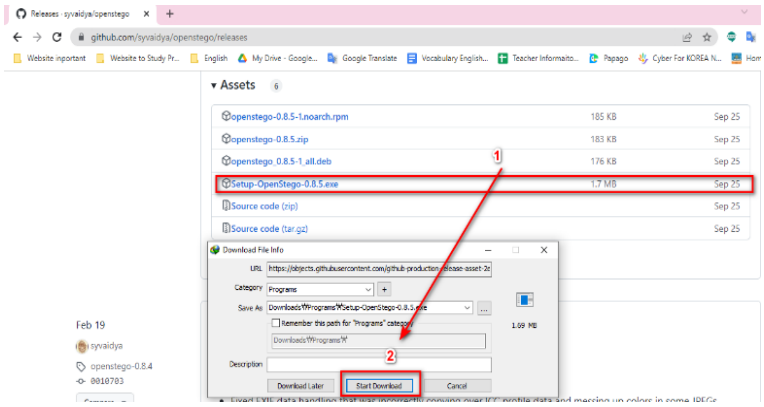
១. បើកកម្មវិធីរុករកដូចជា Chrome, Mozilla Firefox ,...



ក. វាយពាក្យ *openstego.com* ឬក៏ស្កេន QR code

ខ.ចុចពាក្យ Enter ឬក៏ធ្វើការ Search

២. ការទាញយកកម្មវិធី OpenStego

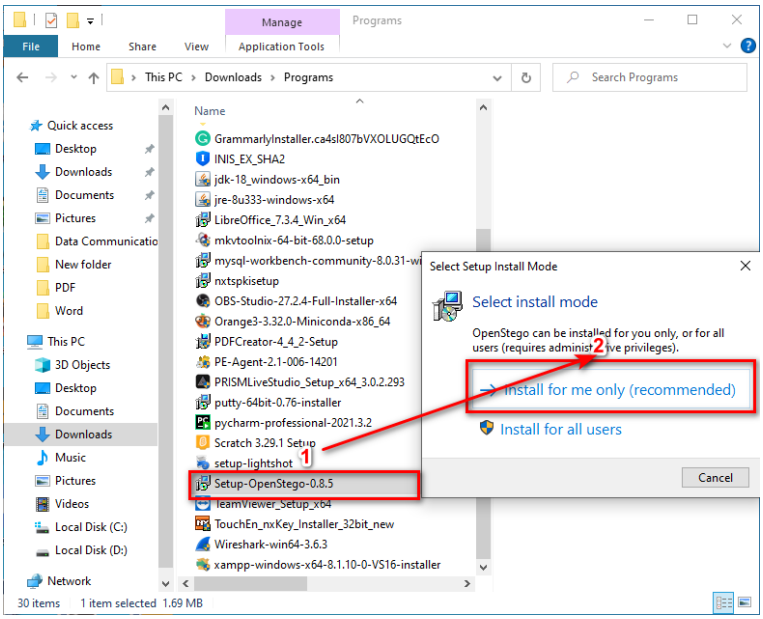


ក. ធ្វើការស្វែងរកពាក្យ Setup-OpenStego-0.8.5.exe បន្ទាប់ចុចលើវា

ខ.ជ្រើសរើសទីតាំងដែលត្រូវទុក

គ. វានឹងចេញដូចរូបខាងលើ បន្ទាប់ចុចចាប់ផ្តើមទាញយក

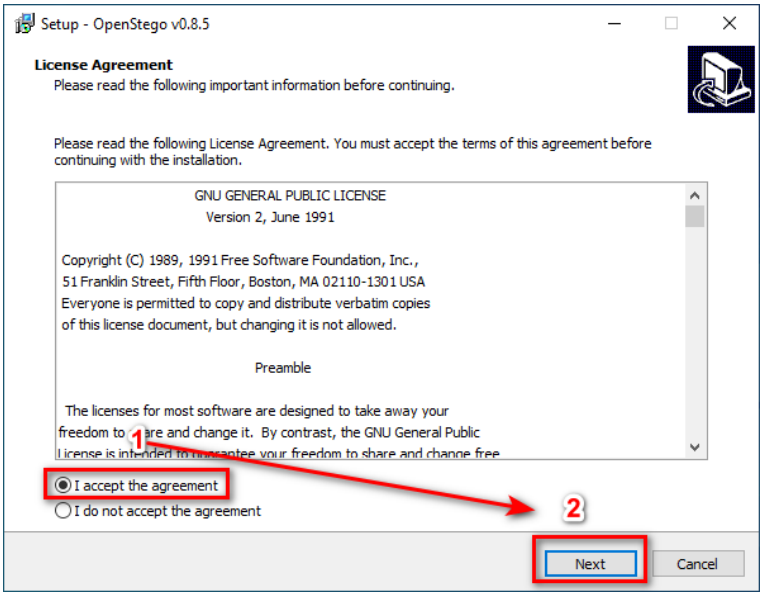
៣. ការតម្លើងកម្មវិធី OpenStego-0.8.5



ក. ជ្រើសរើសកម្មវិធីដែលបានដោនឡូតឈ្មោះ Setup-OpenStego-0.8.5

ខ. ចុចពីរដងលើ Setup-OpenStego-0.8.5

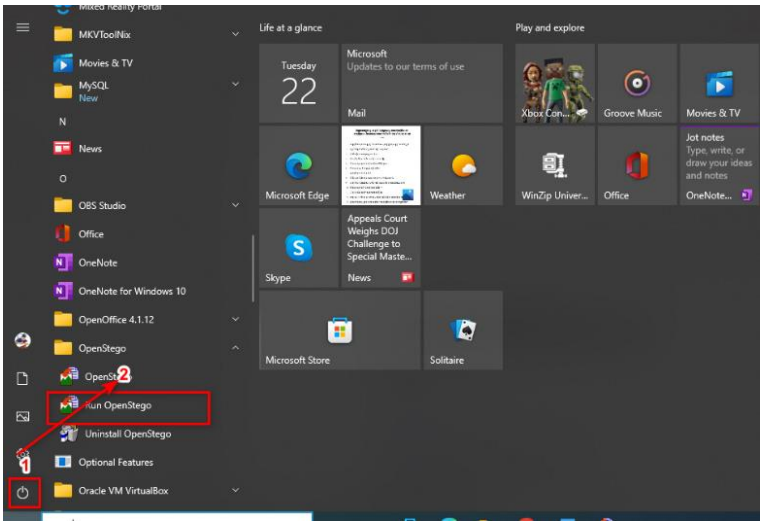
៤. ដំណើរការនៃការតម្លើងកម្មវិធី



ក. ជ្រើសរើស ខ្ញុំទទួលយកកិច្ចព្រមព្រៀង

ខ. បន្ទាប់→ បញ្ចប់→បញ្ចប់

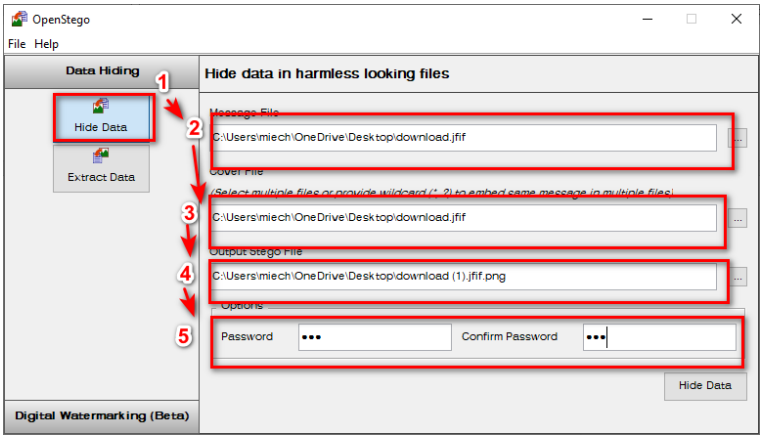
៥. ការចាប់ផ្តើមបើកកម្មវិធីដើម្បីធ្វើការប្រើប្រាស់



ក. ចុចប៊ូតុងចាប់ផ្តើម

ខ. ជ្រើសរើសកម្មវិធី Run OpenStego

៦. រៀបចំឯកសារអត្ថបទដែលអត្ថបទបន្ថែម ដើម្បីធ្វើការអ៊ីនគ្រិប និងលាក់ឯកសារ



ក. ជ្រើសរើសឯកសារអត្ថបទដែលបានរៀបចំសម្រាប់ 'ឯកសារសារ'

ខ. ជ្រើសរើសឯកសាររូបថតដែលបានរៀបចំសម្រាប់ 'ឯកសារគម្រប'

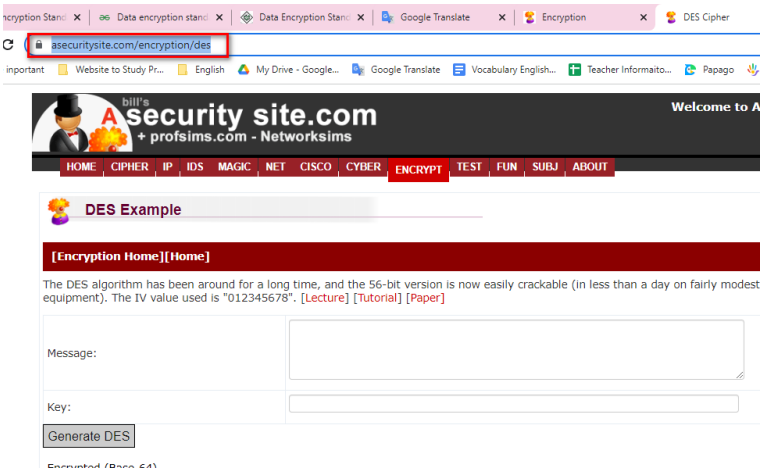
គ. សម្រាប់លទ្ធផល សូមជ្រើសរើសឈ្មោះឯកសារដែលត្រូវជា 'លទ្ធផល'

ឃ. ចុចលើ Hidden Data ដើម្បីធ្វើការលាក់

ក២.តើ DES (ស្តង់ដារអ៊ិនគ្រីបទិន្នន័យ) គឺជាអ្វី?

ស្តង់ដារការអ៊ិនគ្រីបទិន្នន័យ (DES) ត្រូវបានគេរកឃើញថា ងាយរងការវាយប្រហារខ្លាំងដូច្នេះហើយ ប្រជាប្រិយភាពរបស់ DES គឺធ្លាក់ចុះបន្តិច។ DES គឺជា block cipher ដែលអ៊ិនគ្រីបទិន្នន័យក្នុងប្លុក 64 ប៊ីតនីមួយៗ។ មានន័យថា 64 ប៊ីតនៃអត្ថបទធម្មតាទៅជាការបញ្ចូលទៅ DES បង្កើត 64 ប៊ីតនៃអក្សរសម្ងាត់។ ក្បួនដោះស្រាយ និងសោដូចគ្នាត្រូវបានប្រើសម្រាប់ការអ៊ិនគ្រីប និងការឌិគ្រីប ដោយមានភាពខុសគ្នាតិចតួច ប្រវែងគន្លឹះគឺ 56 ប៊ីត។

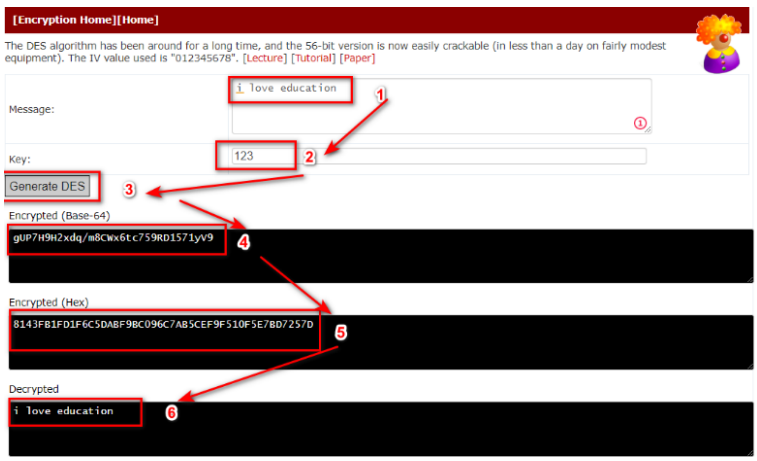
១. បើកកម្មវិធីរុករកដូចជា Chrome, Mozilla Firefox ,...



ក. វាយពាក្យ https://asecuritysite.com/encryption/des ឬក៏ស្កេន QR code

ខ.ចុចពាក្យ Enter ឬក៏ធ្វើការ Search

២. បង្កើតអត្ថបទសម្រាប់ធ្វើការ អ៊ិនគ្រីប



ក. បញ្ចូលពាក្យដែលអ្នកត្រូវការ (I love education)

ខ. បញ្ចូលពាក្យសម្ងាត់ដែលអ្នកត្រូវការ (123)→ចុចលើ បង្កើត ESD

គ. លទ្ធផលបង្ហាញពីការអ៊ិនគ្រីប (Base-64)

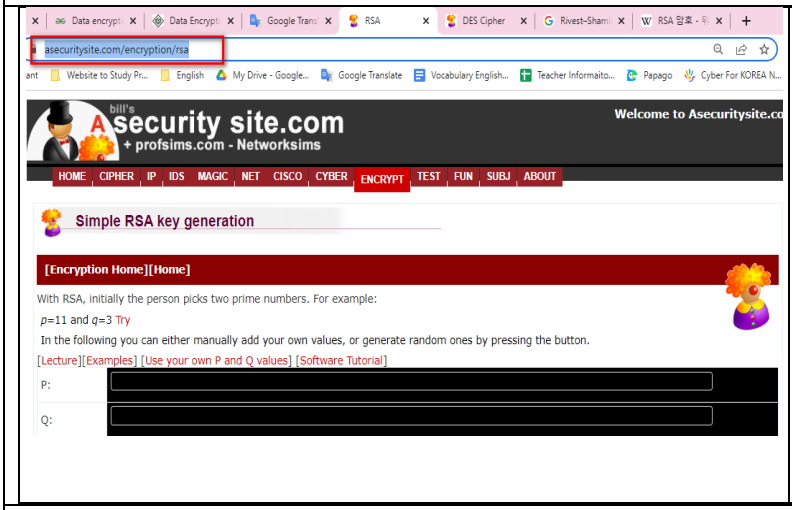
ឃ. តើ RSA (Rivest-Shamir-Adleman) គឺជាអ្វី ?

RSA (Rivest–Shamir–Adleman) គឺជាប្រព័ន្ធគ្រីបតូកូដសាធារណៈដែលត្រូវបានប្រើប្រាស់យ៉ាងទូលំទូលាយសម្រាប់ការបញ្ជូនទិន្នន័យប្រកបដោយសុវត្ថិភាព។ វាក៏ជាវត្ថុចំណាស់ជាងគេមួយដែរ អក្សរកាត់ "RSA" មកពីនាមត្រកូលរបស់ Ron Rivest, Adi Shamir និង Leonard Adleman ដែលបានពិពណ៌នាជាសាធារណៈនូវក្បួនដោះស្រាយក្នុងឆ្នាំ 1977 ។ ប្រព័ន្ធសមមូលមួយត្រូវបានបង្កើតឡើងជាសម្ងាត់ក្នុងឆ្នាំ 1973 នៅ GCHQ (ទីភ្នាក់ងារស៊ើបការណ៍សម្ងាត់របស់ចក្រភពអង់គ្លេស) ដោយគណិតវិទូអង់គ្លេស Clifford។

នៅក្នុងប្រព័ន្ធគ្រីបសាធារណៈ សោអ៊ិនគ្រីបគឺមានលក្ខណៈសាធារណៈ និងខុសប្លែកពីសារឱគ្រីប ដែលត្រូវបានរក្សាទុកជាសម្ងាត់ (ឯកជន)។ អ្នកប្រើប្រាស់ RSA បង្កើត និងបោះផ្សាយសោសាធារណៈដោយផ្អែកលើលេខសំខាន់ពីរ និងតម្លៃបន្ថែម លេខសំខាន់ៗត្រូវបានរក្សាទុកជាសម្ងាត់។ នរណាម្នាក់អាចអ៊ិនគ្រីបសារតាមរយៈសោសាធារណៈ ប៉ុន្តែពួកវាអាចត្រូវបានឱកូដដោយអ្នកដែលស្គាល់លេខសំខាន់ៗប៉ុណ្ណោះ។

ឃ១. RSA (Rivest-Shamir-Addleman) ការអនុវត្ត

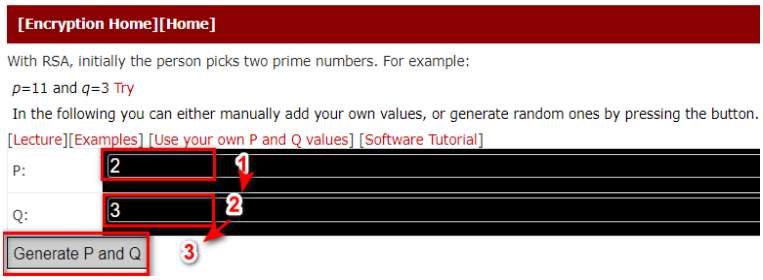
១. បើកកម្មវិធីរុករកដូចជា Chrome, Mozilla Firefox ,...



ក. វាយពាក្យ https://asecuritysite.com/encryption/rsa ឬក៏ស្កេន QR code

ខ.ចុចពាក្យ Enter ឬក៏ធ្វើការ Search

២. បញ្ចូល RSA

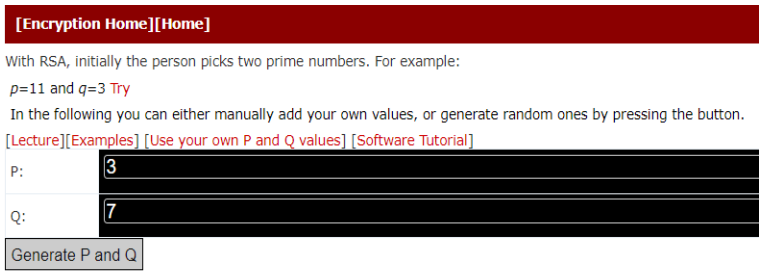


ក. បញ្ចូលតម្លៃ P ដែលអ្នកត្រូវការ (2)

ខ. តម្លៃបញ្ចូល Q ដែលអ្នកត្រូវការ (3)

គ. ចុចលើពាក្យ Generate P and Q

៣. លទ្ធផលបង្ហាញថា Next តម្លៃ n ត្រូវបានគណនា។ n = p x q



ឯសទ្ធេបការអនុវត្តន៍ .

- Digital Steganography វាគឺជាបច្ចេកវិទ្យាអ៊ីនគ្រីបយ៉ាងស៊ីជម្រៅ ដែលលាក់ព័ត៌មានសម្ងាត់ដែលអ្នកចង់បញ្ជូនចេញពីឯកសារ សារ រូបភាព ឬវីដេអូនៅក្នុងឯកសារ សារ រូបភាព ឬវីដេអូផ្សេង
- DES (ស្តង់ដារការអ៊ិនគ្រីបទិន្នន័យ)៖ នៅឆ្នាំ 1971 ក្រុមហ៊ុន IBM បានបង្កើតក្បួនដោះស្រាយការគ្រីបមួយហៅថា 'Lucifer' ដែលត្រូវបានកែលម្អ និងកំណត់ថាជាស្តង់ដារជាតិដោយ NIST ។
- RSA (Rivest–Shamir–Adleman)៖ ប្រព័ន្ធគ្រីបគ្រីបសាធារណៈដែលប្រើយ៉ាងទូលំទូលាយសម្រាប់ការបញ្ជូនទិន្នន័យប្រកបដោយសុវត្ថិភាព វាក៏ជាវត្ថុចំណាស់ជាងគេមួយដែរ។ អក្សរកាត់ "RSA" មកពីនាមត្រកូលរបស់ Ron Rivest, Adi Shamir និង Leonard Adleman ដែលបានពិពណ៌នាជាសាធារណៈនូវក្បួនដោះស្រាយក្នុងឆ្នាំ 1977 ។

ច. កិច្ចការស្រាវជ្រាវ

កិច្ចការ៖ ការគ្រប់គ្រងឌីជីថល និងការ អ៊ិនគ្រីប និងឌិសគ្រីប

ក. ពិពណ៌នាអំពីក្បួនដោះស្រាយអ៊ិនគ្រីប Steganography និងតម្លៃលទ្ធផល។

ខ.ចូរពិពណ៌នាអំពីក្បួនដោះស្រាយ ការអ៊ិនគ្រីប DES និងតម្លៃលទ្ធផល។

គ. ចូរពិពណ៌នាអំពីក្បួនដោះស្រាយ ការអ៊ិនគ្រីប RSA និងតម្លៃលទ្ធផល។

សៀវភៅនេះត្រូវបានរៀបរៀង ដោយមានកិច្ចសហការពី
ក្រសួងអប់រំ យុវជន និងកីឡា (MoEYS) ក្រោមគម្រោង
កសាងសមត្ថភាពបច្ចេកវិទ្យាព័ត៌មានសម្រាប់ការអប់រំនៅ
មធ្យមសិក្សាបឋមភូមិនៅកម្ពុជា ដែលគាំទ្រដោយ KOICA ។

KOICA
Korea International
Cooperation Agency

Korea National University
of Education