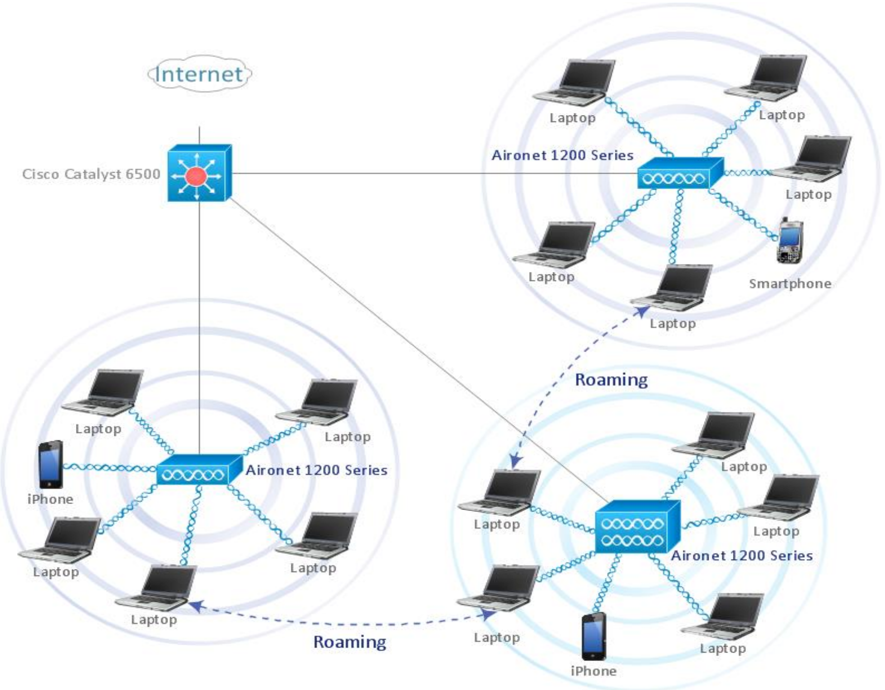
មូលដ្ឋានគ្រឹះនៃកុំព្យូទ័រណែតវើក
និង
ការគ្រប់គ្រង Windows Server

Windows Server 2012

រៀបរៀងដោយ
បណ្ឌិត អ៊ុក យាន
២០២២

គាំទ្រថវិកាលើការរៀបរៀង និពន្ធ និងកែលម្អដោយ
មូលនិធិស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍

មូលដ្ឋានគ្រឹះនៃកុំព្យូទ័រណែតវើក
និង
ការគ្រប់គ្រង Windows Server



រៀបរៀងដោយ
បណ្ឌិត អ៊ុក យាន
២០២២

គាំទ្រថវិកាលើការរៀបរៀង និពន្ធ និងកែលម្អដោយ
មូលនិធិស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍

សាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ
មហាវិទ្យាល័យវិទ្យាសាស្ត្រ
ដេប៉ាតឺម៉ង់ព័ត៌មានវិទ្យា

គណៈកម្មការនិពន្ធ

បណ្ឌិត អ៊ុក ឃាន

សាស្ត្រាចារ្យនៃសាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ

គណៈកម្មការត្រួតពិនិត្យ

លោក ជី គួង ប្រធានដេប៉ាតឺម៉ង់ព័ត៌មានវិទ្យា

លោក ប៉ុក លក្សមុនី អនុប្រធានដេប៉ាតឺម៉ង់ព័ត៌មានវិទ្យា

លោក ធូ រណ្ឌេ ប្រធានការិយាល័យស្រាវជ្រាវ

បុព្វកថា

ដំណើរអភិវឌ្ឍនៃព្រះរាជាណាចក្រកម្ពុជានៅក្នុងយុគសម័យទំនើបនេះ ជាមេរៀនដ៏ជោគជ័យបំផុតមួយដែលចាប់ឫសគល់ចេញពីការបញ្ចប់របបប្រល័យពូជសាសន៍ ការបញ្ចប់សង្គ្រាម ការផ្សះផ្សារជាតិ ការកសាងមូលដ្ឋានរឹងមាំនៃសន្តិភាពនិងស្ថេរភាព និងការអភិវឌ្ឍសេដ្ឋកិច្ច។ នៅក្រោយពេលដែលសន្តិភាពត្រូវបានកើតឡើងដោយបរិបូរណ៍នៅឆ្នាំ១៩៩៨ កម្ពុជាទទួលកំណើនសេដ្ឋកិច្ចខ្ពស់ គឺប្រមាណ៨% ក្នុងមួយឆ្នាំ។ លើសពីនេះទៀត អត្រានៃភាពក្រីក្រត្រូវបានកាត់បន្ថយពីប្រមាណ៥៣% នៅឆ្នាំ២០០៤ មកនៅទាបជាង១០% នៅឆ្នាំ២០១៩។ ដំណើរនៃការអភិវឌ្ឍជាតិជាសកម្មភាពដែលបន្តទៅមុខជាប់ជានិច្ច ហើយគោលនយោបាយថ្មីៗដែលមានលក្ខណៈអន្តរវិស័យគ្របដណ្តប់ ក៏កំពុងលេចរូបរាងឡើង ដើម្បីតម្រង់ទិសកម្ពុជាឆ្ពោះទៅកាន់ប្រទេសមានប្រាក់ចំណូលមធ្យមកម្រិតខ្ពស់នៅឆ្នាំ២០៣០ និងឈានឡើងជាប្រទេសមានប្រាក់ចំណូលខ្ពស់ នៅឆ្នាំ២០៥០។ ការប្រែប្រួលឆាប់រហ័សនៃនិម្មាបនកម្មពិភពលោកនិងតំបន់ រួមទាំងទំនាក់ទំនងភូមិសាស្ត្រនយោបាយបានផ្តល់កាលានុវត្តភាពសម្រាប់ការអភិវឌ្ឍឧស្សាហកម្មនៅកម្ពុជា ដែលត្រូវបានរាជរដ្ឋាភិបាលចាត់ទុកជាមូលដ្ឋានគ្រឹះនៃកំណើនសេដ្ឋកិច្ចកម្ពុជា។ រាជរដ្ឋាភិបាលកម្ពុជាបាន និងកំពុងបន្តពង្រឹង និងអភិវឌ្ឍវិស័យអប់រំឆ្ពោះទៅរកការស្រាវជ្រាវ និងនវានុវត្តន៍ ដើម្បីពង្រឹងសមត្ថភាពនិងជំនាញរបស់ធនធានមនុស្សនៅកម្ពុជា ឱ្យស្របទៅនឹងបរិបទថ្មីនៃការអភិវឌ្ឍ ជាពិសេសការពង្រឹងសហគ្រិនភាពក្នុងការរៀបចំម៉ូដែលធុរកិច្ចថ្មីៗ។ ដើម្បីចាប់យកកាលានុវត្តភាពពីបដិវត្តន៍ឧស្សាហកម្មទី៤ និងសេដ្ឋកិច្ចឌីជីថលដែលកំពុងផុសផុលឡើង ប្រព័ន្ធអេកូឡូហ្ស៊ីដែលបង្កលក្ខណៈអំណោយផលដល់ការបង្កើតថ្មី នវានុវត្តន៍ ការស្រាវជ្រាវ និងអភិវឌ្ឍន៍ ត្រូវតែមានការកែលម្អ។

បណ្តាប្រទេសនៅទ្វីបអាស៊ីកំពុងនាំមុខក្នុងការវិនិយោគលើការស្រាវជ្រាវនិងអភិវឌ្ឍ ដោយ មានភាគហ៊ុនប្រមាណ៤៤% នៃការវិនិយោគទាំងមូលរបស់ពិភពលោក។ ប្រទេសចិនកំពុងបន្តកសាងហេដ្ឋារចនាសម្ព័ន្ធនៃការវិនិយោគលើការស្រាវជ្រាវនិងអភិវឌ្ឍ ក៏ដូចជាសមត្ថភាពមនុស្ស។ ផ្ទុយទៅវិញ ប្រទេសនៅទ្វីបអាមេរិកខាងត្បូង និងអាហ្វ្រិក កំពុងស្ថិតនៅឆ្ងាយពីការវិនិយោគនេះ ហើយជាលទ្ធផល ប្រទេសទាំងនោះក៏ពុំមានកំណើនសេដ្ឋកិច្ចគួរឱ្យកត់សម្គាល់ដែរ។ ទុនវិនិយោគសរុបលើការស្រាវ ជ្រាវនិងអភិវឌ្ឍរបស់ប្រទេសនៅទ្វីបអាមេរិកខាងត្បូងនិងអាហ្វ្រិក មានប្រមាណ៥%នៃការវិនិយោគ ទាំងមូលរបស់ពិភពលោក ក្នុងពេលដែលតំបន់ទាំង២នេះមានប្រជាជនប្រមាណ២០%នៃប្រជាជនពិភពលោក។ ប្រទេសចំនួន៦ ដែលមានលំដាប់ខ្ពស់ជាងគេក្នុងការវិនិយោគលើការស្រាវជ្រាវនិងអភិវឌ្ឍ រួមមានសហរដ្ឋអាមេរិក ចិន ជប៉ុន អាល្លឺម៉ង់ ឥណ្ឌា និងកូរ៉េខាងត្បូង ដែលស្មើនឹងប្រមាណ ៧០%នៃទុនវិនិយោគសរុបរបស់ពិភពលោក។

តើចំណេះដឹង ផលិតផល និងសេវាកម្មថ្មីទាំងនេះកើតឡើងពីអ្វី? ហើយកើតឡើងដោយរបៀបណា? ព្រះរាជាណាចក្រកម្ពុជាកំពុងតែកសាងមូលដ្ឋានសម្រាប់ការត្រៀមខ្លួនទទួល និងប្រកួតប្រជែងក្នុងយុគសម័យបដិវត្តឧស្សាហកម្មទី៤ នៅក្នុងសេដ្ឋកិច្ចដែលផ្អែកលើពុទ្ធិ ហើយដែលប្រការនេះចាំបាច់តម្រូវឱ្យពលរដ្ឋកម្ពុជា

ត្រូវក្លាយខ្លួនជាពលរដ្ឋឌីជីថល ពលរដ្ឋសកល និងពលរដ្ឋដែលប្រកបដោយការទទួលខុសត្រូវ ដែលមានសមត្ថភាពក្នុងការផលិត ចែកចាយ និងប្រើប្រាស់ពុទ្ធិដើម្បីទទួលមនុញ្ញផល និងរួមចំណែកក្នុងកំណើន។ ធនាគារពិភពលោកបានធ្វើការកត់សម្គាល់តាំងពីឆ្នាំ២០០២នូវបម្លាស់ប្តូរនៃមូលដ្ឋានសេដ្ឋកិច្ច ពីសេដ្ឋកិច្ចដែលពឹងផ្អែកលើកម្លាំងពលកម្ម និងធនធានអតិកម្ម (Labour and Resource Based Economy) ទៅកាន់សេដ្ឋកិច្ចដោយយកពុទ្ធិ (Knowledge Based-Economy) ជាគន្លឹះនៃការអភិវឌ្ឍ។ អាស្រ័យហេតុនេះ នៅលើគន្លងដែលកម្ពុជាកំពុងធ្វើដំណើរឆ្ពោះទៅកាន់សេដ្ឋកិច្ចឌីជីថល សង្គមកម្ពុជាត្រូវតែមានសមត្ថភាពក្នុងការផលិត ជ្រើសរើស បន្សាំ បង្កើតមុខរបរ និងប្រើប្រាស់ពុទ្ធិ ដើម្បីរក្សានិរន្តរភាពនៃកំណើន និងកែលម្អជីវភាពរស់នៅ។ សមត្ថភាពទាំងនេះអាចកើតឡើងនៅពេលពលរដ្ឋកម្ពុជាមានឱកាសទទួលបានបទពិសោធពីការស្រាវជ្រាវ ការបណ្តុះគំនិតច្នៃប្រឌិត និងការស្វែងរកនវានុវត្តន៍។

កំណែទម្រង់វិស័យអប់រំ គឺជាការត្រួសត្រាយមាគ៌ាសម្រាប់ដំណើរឆ្ពោះទៅកាន់សង្គមប្រកបដោយពុទ្ធិ និងប្រជាពលរដ្ឋប្រកបដោយភាពរស់រវើក។ តាមរយៈមូលដ្ឋានអប់រំ សង្គមប្រកបដោយពុទ្ធិនឹងប្រមូលផ្តុំ បង្កើត និងចែករំលែក ទៅកាន់សមាជិកក្នុងសង្គមនូវសម្បទាអប់រំ ពិសេសគឺពុទ្ធិសម្បទា ក្នុងបុព្វហេតុនៃមនុស្សជាតិនិងឧត្តមប្រយោជន៍នៃប្រទេស។ សង្គមប្រកបដោយពុទ្ធិ គឺពុំគ្រាន់តែជាសង្គមដែលសម្បូរព័ត៌មានប៉ុណ្ណោះទេ តែជាសង្គមដែលប្រជាពលរដ្ឋអាចធ្វើបរិវត្តកម្មពីព័ត៌មានទៅជា មូលធនប្រកបដោយប្រសិទ្ធភាព។ ការរីកចម្រើនទៅមុខជាលំដាប់នៃបច្ចេកវិទ្យានិងតំណភ្ជាប់ បានពង្រីកព្រំដែននៃការចូលទៅកាន់ និងការទទួលបានព័ត៌មានជាសកល ហើយដែលក្នុងន័យនេះ ការអប់រំនឹងបន្តវិវត្តទៅមុខនិងមានការផ្លាស់ប្តូរ។ សង្គមមួយដែលមានអំណាន និងរបាប់ជាបុរេលក្ខខណ្ឌនៃជីវភាពប្រចាំថ្ងៃនៃប្រជាពលរដ្ឋ ពេលនោះបំណិននៃអំណាន និពន្ធ និងការគណនាលេខនព្វន្ត គឺជាចលករនៃការរៀនរបស់សិស្ស។ ជាតុដ៏ចម្បងមួយដែលស្ថិតនៅក្នុងការកសាងសង្គមដែលប្រកបដោយពុទ្ធិគឺសៀវភៅសិក្សា ហើយការរៀបរៀង និពន្ធ និងកែលម្អសៀវភៅសិក្សាជាប្រចាំគឺជានវានុវត្តន៍នៃវិស័យអប់រំដែលនាំទៅរកការសិក្សាពេញមួយជីវិត ការអភិវឌ្ឍសម្បទាអប់រំ និងការចែករំលែកចំណេះដឹង។ មូលដ្ឋានអប់រំ ជាពិសេស គឺគ្រឹះស្ថានឧត្តមសិក្សាត្រូវមានតួនាទីដែលប្រកបដោយការឆ្លើយតបចំពោះតម្រូវការខាងលើនេះ។ សាស្ត្រាចារ្យ អ្នកស្រាវជ្រាវ និងបុគ្គលិកអប់រំត្រូវបន្តសិក្សាជាប់ជានិច្ច តាមរយៈការរៀបរៀង និពន្ធ និងកែលម្អសៀវភៅសិក្សា ហើយដែលសៀវភៅសិក្សាទាំងនេះនឹងក្លាយជា ស្ពាននៃទំនាក់ទំនងរវាងនវានុវត្តន៍នៃបច្ចេកវិទ្យា និងការរៀននិងបង្រៀននៅក្នុងថ្នាក់រៀន។

សង្គម ដែលប្រកបពុទ្ធិ ក៏ជាសង្គមដែលបណ្តុះឱ្យមានរចនាសម្ព័ន្ធទន់នៃសេដ្ឋកិច្ចដែលពឹងផ្អែកលើពុទ្ធិដែរ។ ឧទាហរណ៍ជាក់ស្តែងនៃបែបផែននេះរួមមាន Silicon Valley នៃសហរដ្ឋអាមេរិក សួនឧស្សាហកម្មវិស្វកម្មអាកាសយានយន្តនិងយានយន្តនៅទីក្រុង Munich ប្រទេសអាល្លឺម៉ង់ តំបន់ជីវបច្ចេកវិទ្យានៅក្រុង Hyderabad ប្រទេសឥណ្ឌា តំបន់ផលិតគ្រឿងអេឡិចត្រូនិកនិងសារគមនាគមន៍ ឌីជីថលនៅទីក្រុង Seoul ប្រទេសកូរេខាងត្បូង ក៏ដូចជាសួនឧស្សាហកម្មថាមពល និងឥន្ទនគីមីសាស្ត្រនៃប្រទេសប្រេស៊ីល ហើយក៏នៅមានទីក្រុងនៃប្រទេស

ជាច្រើនទៀតនៅលើពិភពលោក។ លក្ខណៈសម្បត្តិនៃទីក្រុងទាំងនេះគឺការប្រើប្រាស់និន្នាការនៃការអភិវឌ្ឍដែលជំរុញ និងតម្រង់ទិសដោយចំណេះដឹង ហើយដែលចំណេះដឹងទាំងនោះកើតចេញជាដំបូងពីការវិនិយោគទៅលើគ្រឹះស្ថានឧត្តមសិក្សា ស្ថាប័នស្រាវជ្រាវ មជ្ឈមណ្ឌលឧត្តមភាពនៃជំនាញជាន់ខ្ពស់ ការប្រកួតប្រជែងដោយគុណាធិបតេយ្យ និង ជាពិសេស ការបណ្ដុះវប្បធម៌អំណាននិងនិពន្ធសៀវភៅ។ ល្បឿននៃការរីកចម្រើនផ្នែកពុទ្ធិ និងបច្ចេកវិទ្យាកំពុងមានសន្ទុះលឿនជាងអ្វីដែលសិស្ស និងនិស្សិតអាចទទួលបានពីគ្រូនៅគ្រឹះស្ថានសិក្សា ដែលធ្វើឱ្យគោលដៅនៃការអប់រំនៅពេលបច្ចុប្បន្ននេះ មានការប្រឈមខ្លាំងជាងពេលណាទាំងអស់។ ឧទាហរណ៍ ក្នុងមួយឆ្នាំ មានសៀវភៅជាង ២,២លានចំណងជើង ត្រូវបានសរសេរនិងបោះពុម្ព ដែលក្នុងនោះប្រទេសចិនមាន ៤៤០ពាន់ ចំណែកឯសហរដ្ឋអាមេរិកមាន ៣០៥ពាន់ និងប្រទេសរុស្ស៊ីមាន ១២០ពាន់ចំណងជើង។

ខណៈពេលដែលបច្ចេកវិទ្យាកំពុងរីកចម្រើនជារៀងរាល់ថ្ងៃ មធ្យោបាយសម្រាប់អំណានក៏មានច្រើនជម្រើសសម្រាប់សិស្ស-និស្សិត និងសាធារណៈជន រួមមានការអានសៀវភៅ ការអានលើឧបករណ៍ អេឡិចត្រូនិក ការអានដោយប្រើទូរសព្ទវៃឆ្លាត និងការអានលើកុំព្យូទ័រ ដែលសុទ្ធសឹងជាមធ្យោបាយសំខាន់ៗដែលនាំអ្នកអានទាំងឡាយឱ្យសម្រេចគោលបំណងអានរបស់ខ្លួន។ ម៉្យាងវិញទៀត អំណានដោយប្រើមធ្យោបាយបច្ចេកវិទ្យាទំនើប ចំណាយពេលតិច ងាយស្រួលអាន និងជួយដល់បរិស្ថានមួយកម្រិតទៀត។ នាពេលបច្ចុប្បន្ន សិស្ស-និស្សិត និងសាធារណៈជនកម្ពុជាដែលស្រឡាញ់អំណានកំពុងតែប្រើប្រាស់មធ្យោបាយអំណានទាំងនេះ។ បើយើងក្រឡេកមើលទៅប្រទេសជឿនលឿន ទោះបីជាបច្ចេកវិទ្យារីកចម្រើនខ្លាំងយ៉ាងណា អំណានតាមរយៈសៀវភៅនៅតែមានសន្ទុះដដែល។ ម៉្យាងវិញទៀត បច្ចេកវិទ្យាអានបែបទំនើបតាមរយៈឧបករណ៍ទំនើប អាស្រ័យលើលទ្ធភាពនៃធនធានអប់រំឌីជីថល និងមាតិកាឌីជីថលគ្រប់គ្រាន់ដែលបានផលិត និងបង្ហោះចែកចាយសម្រាប់អំណាន។

ក្នុងបរិបទកម្ពុជា ជាពិសេសក្នុងបរិការណ៍នៃការផ្ទុះរីករាលដាលនៃជំងឺកូវីដ-១៩ ក្រសួងអប់រំ យុវជន និងកីឡា បានជំរុញឱ្យមានបរិវត្តកម្មឌីជីថលនៅក្នុងអេកូស៊ីស្តែមនៃការអប់រំ ជាពិសេសការអប់រំតាមប្រព័ន្ធអេឡិចត្រូនិក និងការអប់រំពីចម្ងាយដើម្បីលើកកម្ពស់អំណានតាមរយៈការផលិតមាតិកាឌីជីថល ដែលមានភាពសម្បូរបែប ការកសាងសមត្ថភាពផ្នែកតំណភ្ជាប់និងវេទិកាឌីជីថល ការពង្រីកវិសាលភាពនៃមជ្ឈមណ្ឌលទិន្នន័យ និងការលើកកម្ពស់គុណភាពនៃការផលិតធនធានអប់រំឌីជីថល គួបផ្សំជាមួយការចែកសន្លឹកកិច្ចការឱ្យសិស្សយកទៅរៀននៅផ្ទះ និងការចុះទៅជួបជាមួយសិស្សជាបណ្ដុំនៅតាមសហគមន៍។ ក្នុងន័យលើកកម្ពស់អំណាន និងភាពសម្បូរបែបនៃធនធានសៀវភៅសិក្សា ឱ្យកាន់តែមានប្រសិទ្ធភាពនិងភាពសក្ដិសិទ្ធិ និងផ្ដល់ឱកាសអំណានកាន់តែច្រើនថែមទៀតដល់សិស្សានុសិស្ស និស្សិត និងសាធារណៈជន ក្រសួងអប់រំ យុវជន និងកីឡាលើកទឹកចិត្តនូវចំណុចមួយចំនួនដូចខាងក្រោម៖

1. សាស្ត្រាចារ្យ អ្នកស្រាវជ្រាវ និងបុគ្គលិកអប់រំ សូមបន្តនិងបង្កើនការបោះពុម្ពស្នាដៃបន្ថែមទៀត ដើម្បីធ្វើឱ្យធនធានសម្រាប់អំណានកាន់តែសម្បូរបែប ជាពិសេសធនធានអំណានជាខេមរភាសា

2. គ្រឹះស្ថានឧត្តមសិក្សា សូមផ្តល់លទ្ធភាពគ្រប់បែបយ៉ាង ដើម្បីឱ្យបុគ្គលិកអប់រំគ្រប់លំដាប់ថ្នាក់ និងនិស្សិតគ្រប់កម្រិតសិក្សាអាចចូលរួមអាន និងសិក្សាស្រាវជ្រាវតាមគ្រប់លទ្ធភាពជាមួយធនធានអំណាន ជាពិសេសការរៀបចំឱ្យមានពេលវេលាសម្រាប់សហសិក្សា និងអំណានក្នុងបណ្ណាល័យ
3. សាស្ត្រាចារ្យតាមមុខវិជ្ជា និងអ្នកស្រាវជ្រាវតាមជំនាញឬវិស័យ ត្រូវរៀបចំដំណើរការរៀន បង្រៀន និងស្រាវជ្រាវដែលមានដាក់បញ្ចូលកិច្ចការស្វ័យសិក្សា សហសិក្សា ឬការស្រាវជ្រាវបណ្ណាល័យដែលតម្រូវឱ្យនិស្សិត ត្រូវអាននិងស្រាវជ្រាវជាមួយធនធានអំណាន
4. គ្រឹះស្ថានឧត្តមសិក្សា និងមជ្ឈមណ្ឌលស្រាវជ្រាវ ត្រូវខិតខំឱ្យអស់លទ្ធភាពក្នុងការបង្កើតបណ្ណាល័យ មជ្ឈមណ្ឌលរក្សាឯកសារ ឬមជ្ឈមណ្ឌលអប់រំឌីជីថល ជាដើម ដើម្បីឱ្យបុគ្គលិកអប់រំគ្រប់លំដាប់ថ្នាក់ និងនិស្សិតគ្រប់កម្រិតសិក្សា អាចទទួលបាន និងស្វែងរកប្រភពសម្រាប់អំណាន កាន់តែសម្បូរបែប និងមានភាពបត់បែន ឆ្លើយតបតាមតម្រូវការអ្នកអាន
5. និស្សិតគ្រប់កម្រិតសិក្សា ត្រូវខិតខំនិងចំណាយពេលអាន និងចាត់ទុកវប្បធម៌ និងអកប្បកិរិយាអំណានជាផ្នែកមួយ នៃពេលវេលានិងភាពស៊ីវិល័យនៃជីវិតប្រចាំថ្ងៃ
6. បងប្អូនជនរួមជាតិ ដែលជាមាតាបិតា ឬអ្នកអាណាព្យាបាល សូមជួយជំរុញនិងបង្កលក្ខណៈកាន់តែច្រើនថែមទៀត ជាពិសេស ការលៃលកចំណាយនៅក្នុងគ្រួសារសម្រាប់ការទិញសម្ភារៈសិក្សា សៀវភៅអាន និងឧបករណ៍សម្រាប់អំណានដល់កូនៗ ដែលចាត់ទុកជាការវិនិយោគមួយដ៏សំខាន់សម្រាប់ បង្កើនចំណេះដឹង និងអនាគតរបស់ពួកគេ។

ដោយមានការគាំទ្រពីក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ នៅឆ្នាំ២០២០ ក្រសួងអប់រំ យុវជន និងកីឡា បានបង្កើតមូលនិធិស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍ ដែលហៅកាត់ថា “មូលនិធិ ស.គ.ន” និងហៅជាភាសាអង់គ្លេសថា The Research Creativity and Innovation Fund ដែលហៅកាត់ជាភាសាអង់គ្លេសថា “RCI Fund”។ គោលដៅចម្បងនៃមូលនិធិនេះ គឺរួមចំណែកលើកកម្ពស់វប្បធម៌នៃការស្រាវជ្រាវ បំផុសគំនិតច្នៃប្រឌិត និងជំរុញការធ្វើនវានុវត្ត ដើម្បីជាប្រយោជន៍ដល់វិស័យអប់រំ យុវជន និងកីឡា ដែលឆ្លើយតបទៅនឹងទីផ្សារពលកម្ម និងសាកលភាវូបនីយកម្ម។ មូលនិធិ ស.គ.ន បានសម្រេចកំណត់ប្រធានបទ ជាអាទិភាពសម្រាប់គាំទ្រដោយមូលនិធិចំនួន៣ រួមមាន ឌីជីថលនីយកម្មសម្រាប់បដិវត្តឧស្សាហកម្ម៤.០ (Digitalization for IR.4.0) ការស្រាវជ្រាវអនុវត្តលើវិស័យកសិកម្ម (Applied Agricultural Research) និងការស្រាវជ្រាវគរុកោសល្យសតវត្សទី២១ (21st Century Pedagogy Research)។

ដោយមានការធ្វើអាទិភាពូបនីយកម្មទៅលើទិសដៅនៃការប្រើប្រាស់ថវិកាមូលនិធិសម្រាប់ឆ្នាំ២០២០ ក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ និងក្រសួងអប់រំ យុវជន និងកីឡា បានផ្តល់ការគាំទ្រដល់ការ**រៀបរៀង និពន្ធ និងកែលម្អ សៀវភៅសិក្សា(Text book) ដែលនឹងត្រូវប្រើប្រាស់នៅកម្រិតឧត្តមសិក្សា**។ គោលបំណងនៃការរៀបរៀង និពន្ធ និងកែលម្អ សៀវភៅសិក្សានៅកម្រិតឧត្តមសិក្សា គឺដើម្បីបង្កើនបរិមាណ លើកកម្ពស់គុណភាព និងពង្រីក

សមធម៌នៃធនធានសិក្សាជាខេមរភាសា ជូនដល់និស្សិតដែលកំពុងបន្តការសិក្សា និងត្រៀមខ្លួនធ្វើការស្រាវជ្រាវនៅកម្រិតឧត្តមសិក្សា។ លើសពីនេះទៀត ការរៀបរៀង និពន្ធ និងកែលម្អសៀវភៅសិក្សានៅកម្រិតឧត្តមសិក្សាមានគោលដៅដូចខាងក្រោម ៖

- ឆ្លើយតបជាបន្ទាន់ចំពោះការខ្វះខាតធនធានសិក្សា ដែលជាតម្រូវការសិក្សារបស់និស្សិតនៅកម្រិតឧត្តមសិក្សា
- លើកកម្ពស់ទំនើបភាវូបនីយកម្ម និងឧត្តមានុវត្តន៍នៃការរៀននិងបង្រៀន និងការស្រាវជ្រាវនៅលើមុខវិជ្ជា កម្មវិធីសិក្សា ឬមុខជំនាញជាក់លាក់
- បង្កើនភាពស៊ីជម្រៅក្នុងការកសាងវិជ្ជាជីវៈនិងបទពិសោធន៍សម្រាប់ឋានៈសាស្ត្រាចារ្យ និងអ្នកស្រាវជ្រាវ
- រួមចំណែកដល់ការកសាងភាពជាសហគមន៍វិជ្ជាជីវៈ ការចែករំលែកបទពិសោធន៍ និងវប្បធម៌នៃការរៀបរៀង និពន្ធ និងកែលម្អសៀវភៅសិក្សានៅកម្រិតឧត្តមសិក្សា។

ក្រសួងអប់រំ យុវជន និងកីឡា បានវាយតម្លៃខ្ពស់ចំពោះការបោះជំហានប្រកបដោយមនសិការវិជ្ជាជីវៈនៃគ្រឹះស្ថានឧត្តមសិក្សា និងបុគ្គលិកអប់រំទាំងអស់ ក្នុងការរៀបចំ រៀបរៀង និពន្ធ និងកែលម្អសៀវភៅសិក្សា ដើម្បីបង្កើនបរិមាណ លើកកម្ពស់គុណភាព និងពង្រឹងសមធម៌នៃធនធានសិក្សាជាខេមរភាសា ជូននិស្សិតដែលកំពុងបន្តការសិក្សា និងត្រៀមខ្លួនធ្វើការស្រាវជ្រាវនៅកម្រិតឧត្តមសិក្សា។ សៀវភៅសិក្សាជាផ្នែកមួយនៃការទទួលស្គាល់គុណភាពអប់រំនៃគ្រឹះស្ថានឧត្តមសិក្សា និងជាធនធានសិក្សាដែលជាមូលដ្ឋានមួយដ៏សំខាន់ ក្នុងការគាំទ្រដល់ការបង្រៀន និងរៀន ហើយត្រូវមានបរិមាណគ្រប់គ្រាន់ ឆ្លើយតបទៅនឹងកម្មវិធីអប់រំ និងតម្រូវការសិក្សាស្រាវជ្រាវ។ ជាគោលការណ៍ គ្រឹះស្ថានឧត្តមសិក្សាទាំងអស់ ត្រូវមានសៀវភៅសិក្សាដែលប្រើជាគោលសម្រាប់មុខវិជ្ជានីមួយៗ។ ចំនួនសៀវភៅសិក្សាដែលគ្រប់គ្រាន់សម្រាប់ការស្រាវជ្រាវ និងការសិក្សារបស់និស្សិត ត្រូវមានយ៉ាងតិចមួយចំណងជើងក្នុងមួយមុខវិជ្ជា ហើយត្រូវតម្កល់យ៉ាងតិច២ច្បាប់ នៅក្នុងបណ្ណាល័យ ឬអាចរកបានតាមប្រព័ន្ធអេឡិចត្រូនិក។ ក្រសួងអប់រំ យុវជន និងកីឡា លើកទឹកចិត្តបន្ថែមទៀតជូនដល់គ្រឹះស្ថានឧត្តមសិក្សារដ្ឋ និងឯកជនដែលបានស្នើសុំថវិកាមូលនិធិរួច សូមចូលរួមបន្ថែមទៀតដើម្បីបង្កើនចំនួនចំណងជើងសៀវភៅ។ ចំណែកគ្រឹះស្ថានឧត្តមសិក្សារដ្ឋនិងឯកជនដែលពុំទាន់បានដាក់ពាក្យស្នើសុំ សូមចូលរួម ដើម្បីជាគុណប្រយោជន៍ដល់តម្រូវការដ៏ទទូច និងថ្លៃថ្លានៃនិស្សិតកម្ពុជាក្នុងការសិក្សា និងស្រាវជ្រាវនៅកម្រិតឧត្តមសិក្សា។

សេចក្ដីបញ្ជាក់

របស់មូលនិធិការស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍

សៀវភៅសិក្សានេះជាលទ្ធផលនៃការស្នើសុំអនុវត្តថវិកាមូលនិធិការស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍ ក្នុងគម្រោង**រៀបរៀង និពន្ធ និងកែលម្អសៀវភៅសិក្សា ដែលនឹងត្រូវប្រើប្រាស់នៅកម្រិតឧត្តមសិក្សា។** សៀវភៅសិក្សានេះ ត្រូវបានរៀបរៀង និពន្ធ ឬកែលម្អដោយមានការធានាអះអាងថាជាស្នាដៃរបស់អ្នកនិពន្ធផ្ទាល់ និងបានឆ្លងកាត់ត្រួតពិនិត្យ ផ្ដល់យោបល់ និងវាយតម្លៃដោយក្រុមប្រឹក្សាអប់រំ ក្រុមប្រឹក្សាស្រាវជ្រាវ ឬក្រុមប្រឹក្សាដែលមានតម្លៃស្មើនៃគ្រឹះស្ថានឧត្តមសិក្សា និងតាមរយៈកិច្ចសន្យាដែលបានធ្វើឡើង និងដែលបានតម្កល់ទុកនៅមូលនិធិការស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍។ រាល់ខ្លឹមសារ ការបកស្រាយ និងរូបភាព គឺជាជំហរនិងទស្សនៈផ្ទាល់របស់អ្នកនិពន្ធ ហើយ ពុំឆ្លុះបញ្ចាំង ឬជាតំណាងដល់មូលនិធិការស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍នៃក្រសួងអប់រំ យុវជន និងកីឡា ឡើយ។

អារម្ភកថា

សៀវភៅនេះត្រូវបានរៀបរៀងឡើងក្រោមការឧបត្ថម្ភគាំទ្ររបស់មូលនិធិស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍សម្រាប់ទុកជាសៀវភៅសិក្សាគោល ដើម្បីបម្រើឲ្យការរៀននិងបង្រៀនមុខវិជ្ជាកុំព្យូទ័រណែតវើកក្នុងដេប៉ាតឺម៉ង់ព័ត៌មានវិទ្យានៃមហាវិទ្យាល័យវិទ្យាសាស្ត្រនៅសាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ។ សៀវភៅនេះផ្ដល់ជូនអ្នកសិក្សាទាំងផ្នែកទ្រឹស្ដីនិងអនុវត្តន៍ ដែលខ្លឹមសារគោលក្នុងសៀវភៅនេះមានតាំងពីសញ្ញាណទូទៅនៃប្រព័ន្ធណែតវើកដំបូងរហូតដល់កម្រិតខ្ពស់ ដែលអាចសមល្មមឲ្យអ្នកសិក្សាផ្នែកព័ត៌មានវិទ្យាទាំងឡាយមានមូលដ្ឋានគ្រឹះរឹងមាំក្នុងការសិក្សាបន្ត ឬស្រាវជ្រាវបន្ថែម ឬក្នុងការប្រកបការងារផ្សេងៗក្នុងវិជ្ជាជីវៈរបស់ខ្លួន។ មិនតែប៉ុណ្ណោះ សៀវភៅនេះក៏អាចចាត់ទុកជាឯកសារពិគ្រោះសម្រាប់អ្នកចូលចិត្តដំឡើងប្រព័ន្ធណែតវើក និងការគ្រប់គ្រង Windows server ប្រកបដោយប្រសិទ្ធិភាពនិងសុវត្ថិភាពផងដែរ។

សេចក្តីថ្លែងអំណរគុណ

ខ្ញុំបាទ អ៊ុក ឃាន ជាសាស្ត្រាចារ្យដេប៉ាតឺម៉ង់ព័ត៌មានវិទ្យានៃមហាវិទ្យាល័យវិទ្យាសាស្ត្រនៃសាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ និងជាអ្នករៀបរៀងសៀវភៅសិក្សាដែលមានចំណងជើងថា "មូលដ្ឋានគ្រឹះនៃកុំព្យូទ័រណែតវើក និងការគ្រប់គ្រង Windows Server"។ ខ្ញុំបាទសូមសម្តែងនូវគារវកិច្ចដ៏ខ្ពង់ខ្ពស់និងសូមគោរពថ្លែងអំណរគុណ និងដឹងគុណយ៉ាងជ្រាលជ្រៅចំពោះ៖

- ក្រសួងសេដ្ឋកិច្ច និងហិរញ្ញវត្ថុ ដែលបានផ្តល់ថវិកាមកក្រសួងអប់រំ ដើម្បីបង្កើតជាមូលនិធិសម្រាប់គាំទ្រដល់ការសរសេរសៀវភៅសិក្សាសម្រាប់កម្រិតឧត្តមសិក្សារបស់ខ្ញុំបាទនេះ។

- ក្រសួងអប់រំ យុវជន និងកីឡា ដែលមាន ឯកឧត្តមបណ្ឌិតសភាចារ្យរដ្ឋមន្ត្រី ហង់ជួន ណារ៉ុន ជាប្រមុខ ដែលលោកបានដឹកនាំបង្កើតមូលនិធិស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍ឡើង ដើម្បីគាំទ្រទាំងស្រុងដល់ដំណើរការសរសេរសៀវភៅនេះ ដែលជាចំណែកមួយក្នុងបេសកកម្មកំណែទម្រង់វិស័យអប់រំឧត្តមសិក្សារបស់លោក។

- ឯកឧត្តមបណ្ឌិត សាន វឌ្ឍនា អនុរដ្ឋលេខាធិការក្រសួងអប់រំ យុវជន និងកីឡា ដែលក្នុងនាមលោកជាតំណាងមូលនិធិ លោកបានយកអស់កម្លាំងកាយចិត្ត ជួយចាត់ចែងនិងជ្រោមជ្រែងយ៉ាងពេញទំហឹង ព្រមទាំងផ្តល់ជាអនុសាសន៍ និងដំណោះស្រាយនានា ដើម្បីជំនះនូវរាល់ឧបសគ្គដែលកើតមានក្នុងដំណើរការសរសេរសៀវភៅនេះ។

- ឯកឧត្តមបណ្ឌិត ជេត ជាលី សាកលវិទ្យាធិការនៃសាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ ដែលបានយកអស់កម្លាំងកាយចិត្ត ព្រមទាំងពេលវេលាដ៏មមាញឹកនិងមានតម្លៃរបស់លោកក្នុងការជួយលើកទឹកចិត្ត ជួយខ្នះខ្នែងដោះស្រាយ និងផ្តល់អនុសាសន៍ដ៏ត្រឹមត្រូវ ក៏ដូចជាបង្កលក្ខណៈងាយស្រួលនានា ទាំងផ្នែករដ្ឋបាល និងទាំងផ្នែកបច្ចេកទេស ដើម្បីឲ្យដំណើរការរៀបរៀងសៀវភៅនេះបានប្រព្រឹត្តទៅដោយរលូនរហូតចប់ចុងចប់ដើម។

- លោក លួន ពេជ្របូរី និង អស់លោក-លោកស្រី ជាក្រុមការងារសម្របសម្រួលទាំងអស់របស់មូលនិធិស្រាវជ្រាវ គំនិតច្នៃប្រឌិត និងនវានុវត្តន៍ ដែលបានយកអស់កម្លាំងកាយចិត្ត ជួយឈឺឆ្អាលក្នុងការដោះស្រាយបញ្ហាប្រឈមនានាយ៉ាងសស្រាក់សស្រាំជាទីបំផុត ដោយមិនត្អូញត្អែរ និងមិនខ្លាចនឿយហត់ ដើម្បីឲ្យការសរសេរសៀវភៅនេះប្រព្រឹត្តទៅដោយរលូន។

- ឯកឧត្តមបណ្ឌិត ស្រ៊ីវ ថារិទ្ធ អ្នកសម្របសម្រួលសាលាក្រោយឧត្តម និង លោកបណ្ឌិត សុខ សិរី អនុប្រធានការិយាល័យស្រាវជ្រាវ ដែលតែងជួយឈឺឆ្អាល ជួយសម្របសម្រួល និងផ្តល់សេវាសម្រាប់ការប្រជុំបច្ចេកទេសនានាតាមអនឡាញតាំងពីដើមរៀងមក។

- អស់លោក-លោកស្រី ជាសមាជិក-សមាជិកាគណៈកម្មការអភិវឌ្ឍសៀវភៅសិក្សា ក៏ដូចជាគណៈកម្មការត្រួតពិនិត្យសៀវភៅសិក្សារបស់សាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ ដែលបានជួយផ្តល់ជាគុចូលដល់សៀវភៅនេះឲ្យកាន់តែមានគុណភាពប្រសើរថែមទៀត។

- ជាចុងក្រោយ និងជាពិសេស លោក ធូ រណ្ឌេ ប្រធានការិយាល័យស្រាវជ្រាវនៃសាកលវិទ្យាល័យភូមិន្ទភ្នំពេញ ដែលតែងជួយផ្តល់ជាគុចូលចំពោះរាល់ឯកសារការងារ ទាំងផ្នែករដ្ឋបាលនិងទាំងផ្នែកបច្ចេកទេស លោកថែមទាំងជួយសម្រួលរាល់បញ្ហាប្រឈមនានាយ៉ាងដឹតដល់បំផុត ដោយមិនប្រកាន់ពេលវេលា និងដោយចិត្តជ្រះថ្លា រហូតការសរសេរសៀវភៅនេះទទួលបានជោគជ័យជាស្ថាពរ។

មាតិកា

បុព្វកថា..i
សេចក្តីបញ្ជាក់ v
អារម្ភកថា vi
សេចក្តីថ្លែងអំណរគុណ...vii
ជំពូកទី១ 1
មូលដ្ឋានគ្រឹះរបស់ Network...1
១-១- តើ Network គឺជាអ្វី ? 1
១-២- ប្រភេទមូលដ្ឋានគ្រឹះនៃ Network...1
១-២-១- PAN (Personal Area Network)..1
១-២-២- Local Area Network 1
១-២-៣- Wide Area Network 1
១-៣- តើអ្វីទៅជា Protocol ? 3
១-៣-១- Ethernet 3
១-៣-២- Fast Ethernet 3
១-៣-៣- Gigabit Ethernet 3
១-៣-៤- LocalTalk.. 3
១-៣-៥- Token Ring 4
១-៣-៦- FDDI 4
១-៣-៧- ATM 6
១-៤- តើ Networking Hardware ជាអ្វី ? 7
១-៤-១- File Servers.. 8
១-៤-២- Workstations 10
១-៤-៣- Network Interface Cards 10
១-៤-៤- Ethernet Cards...10
១-៤-៥- Switch.. 11
១-៤-៦- Repeaters 12
១-៤-៧- Bridges..12
១-៤-៨- Router..13
១-៥- តើ Network Cabling ជាអ្វី ? 16
១-៥-១- Unshielded Twisted Pair (UTP) Cable..16
១-៦- Cisco 16xx/26xx/36xx Routers...21
១-៧- Cisco Catalyst Switches 21
១-៨- Wireless LANs 22

១-៨-១- ប្រភេទនៃ Access Point (AP 22
១-៨-២- ការរៀបចំដើម្បី Setup Wireless Network 24
១-៨-៣- វិធីរហ័សដែលឃើញ Wireless Network Profile នៅក្នុង Windows Vista 25
១-៨-៤- វិធីដ៏លឿនបំផុតគឺពិនិត្យមើល Wireless Card Driver Status ក្នុង Windows XP 26
១-៨-៥- វិធីឆាប់រហ័សដើម្បីពិនិត្យមើល Network ឬ Wireless Adapter Driver Status ក្នុង Windows Vista 28
១-៨-៦- របៀប Set Up Ad Hoc Wireless Network ក្នុង Windows Vista 30
១-៨-៧- Host កុំព្យូទ័រ Configuration 31
១-៨-៨- Client កុំព្យូទ័រ Configuration: 33
១-៨-៩- របៀបការពារ Vista ពីការភ្ជាប់ជាមួយ Ad Hoc Wireless Network 33
១-៨-១០- របៀបកំណត់ IP Address និងព័ត៌មានអំពី Network បន្ថែមទៀតក្នុង Windows XP 35
១-៨-១១- ការកំណត់ IP Address ដោយ Network Administrator 35
១-៨-១២- ការកំណត់ IP address តាមរយៈ DHCP server 36
១-៩- ការណែនាំពីរបៀបប្រើខ្សែ 37
១-១០- តើ Topology ជាអ្វី? 37
១-១១- ងាយស្រួលដំឡើង មើលថែទាំនិងដោះស្រាយបញ្ហានៅពេលជួបបញ្ហា 38
១-១២- ងាយស្រួលប្រើខ្សែ 38
១-១៣- វាបានផ្តល់ឱ្យនូវ Fault Tolerance និងទំនុកចិត្តខ្ពស់ 38
១-១៤- Linear Bus 38
១-១៥- Star 39
១-១៦- Star-Wired Ring 40
១-១៧- Tree 40
១-១៨- ច្បាប់ 5-4-3 41
១-១៩- តើ Network Operationg System ជាអ្វី? 42
១-១៩-១- Peer-to-Peer 42
១-១៩-២- Client/Server 43
ជំពូកទី២ 45
OSI Reference Model 45
២-១- ការរៀបចំ System តាមស្រទាប់ 45
២-២- ISO-OSI Model 45
២-៣- ការប្រាស្រ័យទាក់ទងរវាង Layer ដែលមានតួនាទីស្មើគ្នា 46
២-៤- Data Encapsulation 47
..... 50
២-៥- ការបង្កើតការតភ្ជាប់ 52
ជំពូកទី៣ 56
ការរំលឹកឡើងវិញអំពី LAN Technology និង 56

ការរៀបចំគម្រោងនៃការបង្កើតប្រព័ន្ធ Network 56
៣-១- Local Area Networks and Devices 56
៣-២- Physical Layer : Ethernet/802.3 57
៣-៣- Ethernet/802.3 Interface 58
៣-៤- Ethernet/802.3 Operation 59
៣-៥- Ethernet / 802.3 Broadcast 59
៣-៦- ភាពទុកចិត្តរបស់ Ethernet/802.3 60
៣-៧- ការស្វែងរក MAC address 61
៣-៨- គោលបំណងនៃការបង្កើត LAN 62
៣-៨-១- ការបង្កើត VLAN 64
៣-៨-១-២- ដំណើរការរបស់ VLAN 65
៣-៩- ការប្រមូលទិន្នន័យនិងការវិភាគលើតម្រូវការរបស់ប្រព័ន្ធ Network 65
៣-១០- វិភាគទៅលើតម្រូវការ 66
៣-១០-១- ការវិភាគទៅលើកត្តាដែលបណ្តាលឱ្យមានចរាចរណ៍ក្នុងប្រព័ន្ធ Network 67
៣-១០-២- ការវិភាគទៅលើតម្រូវការ -Applications ដែលបណ្តាលឱ្យមានចរាចរណ៍ធំ 67
៣-១១- បច្ចេកទេសនៃ Ethernet – ការចែក Network 68
៣-១២- Bandwidth Domain ប្រៀបធៀបជាមួយ Broadcast Domain 69
៣-១៣-៣- Extended Star Topology 71
៣-១៤- ការភ្ជាប់ពី Fast Ethernet-MDF ទៅ IDF 71
៣-១៤-១- ការប្រើប្រាស់ Switches ដើម្បីកាត់បន្ថយការកកស្ទះ (Congestion) 72
៣-១៤-២- Layer 2 Switch Collision Domains 73
៣-១៤-៣- Layer 2 Migration ដើម្បីឱ្យបាន Bandwidth ខ្ពស់ 74
៣-១៤-៤- Layer 3 Routing Implementation 75
៣-១៤-៥- ការប្រើប្រាស់ Router ដើម្បីឱ្យ Internetworks កាន់តែធំ 75
៣-១៤-៦- ការប្រើប្រាស់ Router ដើម្បីឱ្យរចនាសម្ព័ន្ធផ្នែកខាងក្នុងបានល្អប្រសើរ 76
៣-១៤-៧- ការ Design Network ដោយប្រើ Fiber Optic 77
៣-១៤-៧-២- ការកំណត់ទីតាំងនៃ Server 78
ជំពូកទី៤ 79
WAN (Wide Area Network) 79
៤-១- សេចក្តីផ្តើមចំពោះ WAN Technologies 79
៤-២- ការភ្ជាប់ពីចំណុចមួយទៅចំណុចមួយទៀត 79
៤-១-១- Circuit Switching 80
៤-១-២- Packet Switching 80
៤-២- WAN Dialup Services 82
៤-២-១- WAN Switch 82
៤-២-២- Access Server 83

៤-២-៣- Modem 83
៤-២-៤- CSU/DSU 83
៤-២-៥- ISDN Terminal Adapter 84
ជំពូកទី៥ 85
ប្រភេទនៃ IP addresses 85
៥-១- ថ្នាក់របស់ IP Addresses 85
៥-១-១- ប្រភេទនៃថ្នាក់ A 85
៥-១-២- ថ្នាក់ប្រភេទ B 86
៥-១-៣- ប្រភេទនៃថ្នាក់ C 86
៥-២- Classless Inter-Domain Routing 87
៥-២-១- CIDR blocks 87
៥-២-២- IPv4 private addresses 88
៥-៣- Subnets (ក្រុមតូចៗនៃ Networks) 88
ជំពូកទី៦ 91
IP Address 6 91
៦-១- ការពិពណ៌នាអំពី IPv 6.0 Packet Header 91
៦-២- ការពិពណ៌នាអំពី Address 91
៦-២-១- Broadcasting Methods 92
៦-២-១-១- Unicast 92
៦-២-១-២- Multicast 92
៦-២-១-៣- Any cast 93
៦-៣- IP Multicast Addresses 94
៦-៤- Internet Group Management Protocol (IGMP) 96
៦-៥- Multicast នៅក្នុងមជ្ឈដ្ឋាន layer 2 Switching 97
៦-៥-១- Cisco Group Management Protocol (CGMP) 97
៦-៦- Multicast Destination Trees 98
ជំពូកទី៧ 102
Routing Algorithm 102
៧-១- Distance Vector Algorthm 102
៧-១-១- ចំនួន Hop Count អតិបរមា 105
៧-១-២- Split Horizon 106
៧-១-៣- Route Poisoning 106
៧-១-៤- Hold-Down Timers 106
៧-២- សេចក្តីផ្តើមចំពោះ Link State 107
ជំពូកទី៨ 109
ការ Configure Peer to Peer Network 109

៨-១- ការ Configure Network ជា Peer-to-Peer Network 109
៨-១-១- ការដាក់ឈ្មោះឱ្យកុំព្យូទ័រ workgroup 109
៨-១-២- ការដាក់ឈ្មោះឱ្យកុំព្យូទ័រ 109
៨-២- របៀបចែលរំលែក local resources........ 110
៨-៣- របៀបចូលប្រើ resource ដែលបានចែកចាយ (network resource) 111
៨-៤- ការចែកចាយ Internet........ 111
៨-៤-១- ការចែកចាយ Internet ដោយប្រើ Windows XP........ 112
៨-៤-២- ការចែកចាយ Internet ជាមួយ Windows 7 118
ជំពូកទី៩ 121
ការចាប់ផ្តើមជាមួយ Windows Server 2008 121
៩-១- តម្រូវការ Hardware និង Software........ 121
៩-២- Installation and Configuration 122
៩-៣- Boot configuration Data 125
ជំពូកទី១០ 129
Server Core 129
១០-១- តួនាទី និងមុខងាររបស់ Server Core 129
១០-២- របៀបដំឡើង Server Core 129
១០-៣- Configure the Window Firewall........ 140
១០-៤- Installing and Configuring Server Roles 140
១០-៤-១- Installing and Configuring the DNS Server Role 140
១០-៤-២- ការដំឡើងនិងការ and Configuring លើ DHCP Server Role........ 141
១០-៤-៣- ការដំឡើងនិង Configure លើ File Server Role 142
១០-៤-៥- ការដំឡើង និង Configure ទៅលើ Printer Server Role 143
១០-៤-៦- ការដំឡើងនិង Configure ទៅលើ Streaming Media Services Role 143
១០-៤-៧- ការដំឡើងនិង Configure ទៅលើ Active Directory Services Role 144
១០-៤-៨- ការដំឡើង Optional Features........ 148
១០-៤-៩- ការគ្រប់គ្រង Server Core........ 149
ជំពូកទី១១ 151
ការគ្រប់គ្រងលើ Active Directory........ 151
១១-១- ដើមកំណើតនិងការវិវត្តន៍នៃ ACTIVE DIRECTORY 151
១១-២-១- តួនាទីរបស់ Active Directory........ 153
១០-២-២- លក្ខណៈពិសេសរបស់ Active Directory 153
១១-៣- បង្កើត Forward និង Reverse Lookup Zone DNS 160
១១-៤- Unattended Installation 174
១១-៥- Backup and Recovery 176
១១-៥-១- ការអនុវត្ត Authoritative 177

១១-៥-២- ការអនុវត្ត Non-Authoritative Restore of AD.....177
១១-៥-៣- ការអនុវត្ត Authoritative Restore នៃ AD.....178
១១-៥-៤- Global catalog (GC).....179
១១-៥-៤-១- ការគ្រប់គ្រង User Accounts.....179
១០-៥-៥- ការគ្រប់គ្រងគណនីក្រុម.....181
១០-៥-៥-១- ប្រភេទនៃក្រុម.....181
១១-៥-៥-២- ការណែនាំឱ្យស្គាល់ក្រុម.....181
ជំពូកទី១២.....184
Internet Information Service 7.0.....184
១២-១- លក្ខណៈពិសេសនៃ IIS 7.0.....184
១២-២- ការដំឡើង IIS 7.0.....184
១២-៣- កុងសូលសម្រាប់គ្រប់គ្រងលើ IIS.....185
១២-៤- ការគ្របគ្រង់ IIS ពីចម្ងាយ.....189
១២-៥- File សម្រាប់ Configure IIS 7.0.....191
១២-៦- ការចែកការគ្រប់គ្រង (delegate Administration).....192
១២-៧- ការកត់ត្រាទុកជាស្វ័យប្រវត្តចំពោះការស្នើសុំដែលបរាជ័យ.....195
ជំពូកទី១៣.....199
ការគ្រប់គ្រងលើ Resource និងការបង្ហាញពីសមត្ថភាពរបស់ Server.....199
១៣-១- អ្នកគ្រប់គ្រង់លើ WINDOWS SYSTEM RESOURCE.....200
១៣-២- ភាពទុកចិត្តនិងការបង្ហាញពីសមត្ថភាព.....222
ជំពូកទី១៤.....235
គោលការណ៍នៃ Network និងការប្រើប្រាស់សេវា.....235
១៤-១- សេចក្តីផ្តើម.....235
១៤-២- ការការពារការប្រើ Network.....235
១៤-២-១- សមាសភាពរបស់ NAP.....237
១៤-២-៣. ការអនុវត្តលើកិច្ចការ.....241
១៤-២-៤- ការដំឡើងនិងការ Configuring DHCP.....248
១៤-២-៥- ការធ្វើតេស្ត NAP Client.....256
ជំពូកទី១៥.....257
១៥-១- តួនាទីដ៏សំខាន់របស់ Terminal Services.....257
១៥-២- Single-sign-ON.....257
១៥-៣- Installing Terminal Services.....260
១៥-៤- Terminal Services Licensing.....262
១៥-៥- Terminal Services Gateway.....265
១៥-៥-១- TS Gateway Architecture.....265
១៥-៥-២- TS Gateway Certificates.....267

១៥-៥-៣- Configuring TS Gateway ដើម្បីប្រើ certificate....269
១៥-៥-៤- Configuring Connection Authorization Policies 270
១៥-៥-៣- Configuring Resource Authorization Policies.... 272
១៥-៥-៤- ការភ្ជាប់មក Terminal Server ដោយប្រើ Client តាមរយៈ TS Gateway 274
១៥-៦- Terminal Services Remote Programs....277
១៥-៧- Terminal Server Web Access 280
១៥-៨- ទីតាំងកំណត់កម្មវិធីនិងសមត្ថភាពសម្តែង 284
ជំពូកទី១៦ 286
Windows DNS, BitLocker Driver Encryption, and Itanium Support....286
១៦-១- Domain Name System 286
១៦-១-១- Background Zone Loading 287
១៦-១-២- IPv6 Support....288
១៦-១-៣- GlobalNames Zone 288
១៦-១-៣-១- Read-Only DNS Zone 288
១៦-២- Windows Link-Local Multicast Name Resolution....289
១៦-៣- Windows Bitlocker Drive Encryption.... 290
១៦-៣-១- BitLicker Architecture 291
១៦-៤- BitLocker Recovery....299
១៦-៤-១- ការបិទឬលុប BitLocker Drive Encryption.... 300
១៦-៥- WINDOWS SERVER 2008 ITANIUM SUPPORT 300
ជំពូកទី១៧.... 302
Routing និង Remote Access.... 302
១៧-១- Routing Services.... 302
១៧-២- Routing Basics 302
១៧-៣- Dynamic Routing.... 304
១៧-៣-១- Routing Information Protocol 304
១៧-៤- Routing Protocols.... 307
១៧-៥- Internet Group Management Protocol 316
១៧-៦- Network Address Translation 316
១៧-៧- Static Routes....319
១៧-៨- Remote Access....321
១៧-៨-១- Point–to-Point Protocol.... 322
១៧-៩- Virtual Private Network.... 323
១៧-២០- ការភ្ជាប់តាម SSTP 324
១៧-២១- DHCP Integration with RRAS 327
ជំពូកទី១៨ 333

Windows PowerShell 333
១៨-១- សេចក្តីផ្តើម 333
១៨-២- CMDLETS 338
១៨-៣- Windows PowerShell and .NET 338
១៨-២-១- Windows PowerShell, Scripting and Security 339
១៨-៣- ប្រភេទនៃអថេរ Windows PowerShell ដែលនិយមប្រើ 341
១៨-៤- ឃ្លាប្រយោគមានលក្ខខណ្ឌ 342
១៨-៥- Operator ក្នុង PowerShell 342
១៨-៦- Going Loopy 343
១៨-៧- PowerShell in Action 344
១៨-៨- សិក្សាអំពី Regisrty 345
១៨-៩- Working with Dates and Times 346
ជំពូកទី១៩ 351
Enterprise Public Key Infrastructure 351
១៩-១- PKI ប្រើប្រាស់ 351
១៩-២- Digital Signatures 352
១៩-៣- Digital Certificates 353
១៩-៤- Certification Authorities 353
១៩-៥- ប្រភេទនៃ CAs 353
១៩-៦- Cryptographic Service Providers 354
១៩-៧- Certification Authority Management Console 357
ជំពូកទី២០ 367
ការពារចរាចរណ៍របស់ Network ដោយប្រើ IPsec 367
២០-១- តើ IPsec ជាអ្វី? 367
២០-២- គោលការណ៍នៃ IPsec 367
២០-៣- របៀបដែល IPsec ត្រូវបានបង្កើតឡើង 368
២០-៤- ការប្រើ IPsec នៅក្នុង Tunnel Mode 369
២០-៥- ការកំណត់ឱ្យដោយប្រើ IPsec Policy ដែលបានកំណត់ទុកជាមុន 370
២០-៦- ការគ្រប់គ្រង IP filter Lists និង Filter Action 374
២០-៧- ការបង្កើតនិងការ Configure ច្បាប់សម្រាប់សុវត្ថិភាពនៃការភ្ជាប់ 375
២០-៧-១- ការប្រើ New connection Security Rule Wizard 375
២០-៧-២- Configure IPsec settings សម្រាប់ Connection security Rules 376
ឯកសារយោង 380

សៀវភៅ

មូលដ្ឋានគ្រឹះនៃប្រព័ន្ធណេតវើកនិងការគ្រប់គ្រងលើ Windows server

ជំពូកទី១

មូលដ្ឋានគ្រឹះរបស់ Network

១-១- តើ Network គឺជាអ្វី ?

Network រួមមានកុំព្យូទ័រពីរឬច្រើនត្រូវបានគេភ្ជាប់គ្នាក្នុងគោលបំនងចែកចាយការប្រើធនធានដូចជា Prin -ter,CD-ROMs និងផ្លាស់ប្តូរ files ឬអនុញ្ញាតឱ្យវាធ្វើការទំនាក់ទំនងតាមអេឡិចត្រូនិច។ កុំព្យូទ័រនៅលើបណ្តាញ Network ត្រូវបានភ្ជាប់គ្នាតាមរយៈខ្សែNetwork ប្រព័ន្ធទូរស័ព្ទ រលកវិទ្យុ ផ្កាយរណបឬពន្លឺ infrare។

១-២- ប្រភេទមូលដ្ឋានគ្រឹះនៃ Network

- Personal Area Network (PAN)
- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)

១-២-១- PAN (Personal Area Network)

វាគឺជាប្រភេទ Network ដែលទើបតែចេញឱ្យប្រើប្រាស់សម្រាប់អ្នកជំនួញដែលងាយស្រួលក្នុងការបញ្ជូនព័ត៌មានឬ File ពីមនុស្សម្នាក់មកមនុស្សម្នាក់ទៀតដូចជា BlueTooth, Infrared ឬ Wifi ជាដើម ។

១-២-២- Local Area Network

Local Area Network(LAN) វាគឺជាប្រភេទនៃ Network មួយដែលត្រូវបានបង្កើតឡើងសម្រាប់ប្រើប្រាស់នៅតាមតំបន់តូចៗដូចជា ប្រើប្រាស់សម្រាប់បន្ទប់ពិសោធន៍ សាលារៀននិងអាគារជាដើម។

ក្នុងការដំឡើង LAN មួយគេត្រូវការកុំព្យូទ័រមួយប្រើជា Fileserver។ វាមានតួនាទីសម្រាប់ផ្ទុកនូវរាល់ Software ទាំងអស់ឱ្យប្រព័ន្ធ Networkទាំងមូលប្រើនិងសម្រាប់គ្រប់គ្រងលើបណ្តាញ Network និងចែកចាយឱ្យ Clients ដែលស្ថិតនៅក្នុងប្រព័ន្ធ Network នោះប្រើប្រាស់។

កុំព្យូទ័រដែលភ្ជាប់មកកាន់ Fileserver ហៅថា Workstation។ Workstations គ្មានសមត្ថភាពដូច Fileserver នោះទេហើយគេអាច Install software មួយចំនួនលើវាបាន។ LAN ភាគច្រើនត្រូវបានគេភ្ជាប់វាដោយប្រើ NIC (Network Interface Card) ។

១-២-៣- Wide Area Network

Wide Area Network (WANs) គឺជាប្រព័ន្ធ Network មួយដែលត្រូវបានគេប្រើសម្រាប់ភ្ជាប់តាមតំបន់ដែលមានភូមិសាស្ត្រធំៗដូចជានៅរដ្ឋ Florida, United States ជាដើម។ គេអាចភ្ជាប់វាតាមខ្សែដែលឆ្លងកាត់មហាសមុទ្រឬតាមផ្កាយរណបជាដើម។

បើនិយាយអំពីការប្រើ WAN សាលារៀនជាច្រើននៅរដ្ឋ Florida អាចភ្ជាប់ជាមួយសាលារៀននៅទីក្រុងតូក្យូនៃប្រទេសជប៉ុនដោយចំណាយតិចបំផុត។

WAN មានលក្ខណៈសាំញ៉ាំពីព្រោះវាប្រើ Multiplexers ដើម្បីភ្ជាប់ Local និង MAN (Metropolitan Area Network) ទៅកាន់ពិភពលោកដូចជា Internet ។

គុណសម្បត្តិនៃការប្រើ Network នៅតាមសាលារៀន

- **Speed:**វាងាយស្រួលក្នុងការចែកចាយឯកសារ។ បើគ្មាន Network ទេ យើងត្រូវថតចម្លងដាក់ Floppy ឬ Flash ហើយធ្វើការចម្លងពីកុំព្យូទ័រមួយដាក់ក្នុង កុំព្យូទ័រមួយទៀត។
- **Cost:**ចំណេញក្នុងការទិញ Software សព្វថ្ងៃដែលមានអាជ្ញាបណ្ណ័។ ក្រៅពីការសន្សំសំចៃប្រាក់ វាអាចចែកចាយ Software មានល្អប្រសើរទៀត។
- **Security:** គ្រប់ Software ឬ Data ត្រូវបានរក្សាទុកនៅលើ Server ។ ដូច្នេះគេមិនអាចលួចចម្លងបាននោះទេ បើគ្មានសិទ្ធិ។ គ្រប់ទិន្នន័យទាំងអស់ត្រូវបានការពារដោយប្រព័ន្ធ Security របស់ Network ។
- **Centralized Software Management:** រាល់ Application Servers ទាំងអស់ត្រូវបានដំឡើងនៅលើ Server ។ ដូច្នេះយើងអាចគ្រប់គ្រង់បានទាំងអស់ក្នុងការចែកចាយឯសារឬផ្តល់សេវា។
- **Resource Sharing:** យើងអាចចែកចាយ resources ដែល Server មានទៅឱ្យគ្រប់ Clients ដែលគ្មាន Resourses ទាំងនោះដូចជា CD-ROM,Floppy,Flash និង printer Laser ដែលមានតម្លៃថ្លៃជាដើម។ ជាពិសេសទៅទៀតនោះវាមានកាត់បន្ថយក្នុងការទិញ Software ឬ hardware ដែលមានតម្លៃខ្ពស់។
- **Electronic Mail:**គឺមធ្យោបាយមួយដ៏ល្អប្រសើរបំផុតដែលមនុស្សបច្ចុប្បន្នប្រើប្រាស់សម្រាប់ផ្តល់ព័ត៌មានឱ្យគ្នាទៅវិញទៅមកបានយ៉ាងឆាប់រហ័សពាសពេញពិភពលោក។
- **Flexible Access:** ជួយសម្រួលដល់និស្សិតក្នុងការ Access យកនៅ Assignment ដែលបានដាក់នៅលើប្រព័ន្ធNetwork បានយ៉ាងឆាប់រហ័សហើយអាចធ្វើការរួមគ្នាពីផ្ទះរបស់គេបាន។
- **Workgroup Computing:** Workgroup software ដូចជា Microsoft BackOffice អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ធ្វើការលើ Document ឬគម្រោងព្រមគ្នា។

ឧទាហរណ៍

អ្នកសិក្សានៅក្នុងសាលានីមួយៗនៅគ្រប់ទីកន្លែងទាំងអស់អាចចូលរួមក្នុងការបញ្ចេញមតិទៅលើកម្មវិធីសិក្សាឬឯកសារផ្សេងដែលគេមិនពេញចិត្ត។

គុណវិបត្តិនៃការដំឡើងប្រព័ន្ធ Network នៅតាមសាលា

- **Expensive to Install:** យើងត្រូវចំណាយទុនច្រើនទៅលើការទិញសំភារៈដូចជា ខ្សែ Network ឧបករណ៍ Networks និងត្រូវការចំណាយទៅលើអ្នកបច្ចេកទេសក្នុងដំឡើងវា។
- **Requires Administrative Time:** អ្នកជំនាញត្រូវតែច្បាស់លាស់ក្នុងការមើលថែទាំវា និងគ្រប់គ្រង់លើវា។ ជាពិសេសជានានិរន្តភាពរបស់វា។
- **File Server May Fail:** ប្រព័ន្ធ Network ពឹងផ្អែកទាំងស្រុងទៅលើ Server ។ បើ Server ខូចនោះប្រព័ន្ធទាំងមូលត្រូវគាំងទាំងអស់។
- **Cable May Break:** បើខ្សែសំខាន់ត្រូវបានដាច់ នោះវាបានធ្វើឱ្យអាក់ខានក្នុងការបញ្ជូនទិន្ន័យឬអាចបាត់បង់ទិន្ន័យក្នុងកំឡុងពេលនៃការបញ្ជូន។

សំណួរត្រួតពិនិត្យ

១-តើ Network គេចែកចេញជាប៉ុន្មានប្រភេទសព្វថ្ងៃនេះ ?

២-តើ Network ផ្តល់នូវគុណសម្បត្តិនិងគុណវិបត្តិអ្វីខ្លះ ?

៣-តាមយោបល់របស់អ្នក តើអ្នកគិតថានៅប្រទេសយើងត្រូវភ្ជាប់ប្រព័ន្ធ Network នៅតាមសាលារៀនឬទេ?

១-៣- តើអ្វីទៅជា **Protocol?**

Protocol គឺជាសំនុំនៃក្បួនច្បាប់ដែលគេប្រើសម្រាប់គ្រប់គ្រងទៅលើទំនាក់ទំនងរវាងកុំព្យូទ័រពីរឬច្រើន នៅលើបណ្តាញណេតវើក។ ច្បាប់ទាំងនោះរួមមានការណែនាំដែលតម្រូវឱ្យប្រើប្រាស់នូវណេតវើកឱ្យបានត្រឹមត្រូវគឺ Access Method ដែលបានអនុញ្ញាតឱ្យរូបរាងនៃណេតវើក(Topology)និងល្បឿននៃការបញ្ជូនទិន្នន័យ។ Protocol ដែលគេនិយមប្រើភាគច្រើនបំផុតមានដូចជាៈ

- Ethernet
- LocalTalk
- Token Ring
- FDDI
- ATM

១-៣-១- Ethernet

Ethernet គឺជាប្រភេទនៃ Network មួយដែលមានការពេញនិយមប្រើប្រាស់ក្នុងប្រភេទនៃ Network មានទំហំធំ។ វាប្រើ Access Method មានឈ្មោះថា **CSMA/CD** ។ នេះគឺជាប្រភេទនៃ system មួយដែលគ្រប់ Devices ទាំងអស់ត្រូវស្តាប់ខ្សែ Network ជាមុនសិនទើបអាចធ្វើការបញ្ជូនទិន្នន័យបាន។ បើមានឧបករណ៍មួយកំពុងបញ្ជូននោះវាត្រូវរង់ចាំរហូតទាល់តែមានបញ្ជូនរួចឬទំនេរ។ បើមាន Stations ពីរធ្វើការបញ្ជូននៅពេលព្រមគ្នាតាមទិសដៅផ្ទុយគ្នានោះនិងមាន collision កើតឡើងជាពុំខាន។ បើមាន collision កើតឡើងនោះវានិងកាត់បន្ថយប្រសិទ្ធិភាពនៃការបញ្ជូន ទិន្នន័យ ។

១-៣-២- Fast Ethernet

គឺជាប្រភេទនៃ Ethernet ដែលបានមកពីការបន្ថែមល្បឿនឱ្យវាមានល្បឿនរហូតដល់១០០Mbps។ វាប្រើប្រាស់ខ្សែ cat5 ដែលមានល្បឿនលឿននិង concentrator ដែលមានល្បឿនលឿនដែរ។ សព្វថ្ងៃនេះត្រូវបានគេពេញនិយមប្រើប្រាស់វាណាស់នៅតាមសាលារៀន។

១-៣-៣- Gigabit Ethernet

មានការបង្កើតថ្មីៗនៅក្នុងស្តង់ដានៃ Ethernet គឺជា Protocol មួយដែលមានអត្រានៃការបញ្ជូនមានល្បឿន 1Gbps ។ Gigabit Ethernet ត្រូវបានគេប្រើសម្រាប់ Backbone network នៅពេលនេះ។ នៅពេលអនាគត់វាប្រហែលជាត្រូវបានគេប្រើសម្រាប់ Workstation និង Server ផងដែរ។ វាអាចជា Fiber Optic និង Copper ផងដែរ។ 1000 Base Tx cable ត្រូវបានប្រើសម្រាប់ Giggabit Ethernet ហើយវាបានក្លាយជាស្តង់ដាជាផ្លូវការនៅឆ្នាំ១៩៩០។

១-៣-៤- LocalTalk

LocalTalk គឺជា Network protocol មួយដែលត្រូវបានបង្កើតឡើងដោយក្រុមហ៊ុន Apple កុំព្យូទ័រ និង Macintosh។ Access Method ដែលប្រើដោយ LocalTalk មានឈ្មោះថា CSMA /CA(Carrier Sense Multiple Access with collision Avoidance)។ វាស្រដៀងទៅនិង CSMA/CD ដែរលើកលែងតែសញ្ញាល់របស់កុំព្យូទ័រគឺវាបានប្រាប់មុនឱ្យដឹងមុនពេលវាធ្វើការ។ localTalk និងខ្សែ UTP ត្រូវបានគេប្រើសម្រាប់ភ្ជាប់ពីកុំព្យូទ័រតាមរយៈ

Serial Port។ ចំពោះប្រព័ន្ធប្រតិបត្តិការនៃ Macintosh អនុញ្ញាតឱ្យបង្កើតការភ្ជាប់ជា Peer-to-Peer ដោយមិនចាំបាច់បន្ថែមនូវ Software នោះទេ។

ជាមួយការបន្ថែមនូវ ServerVersion នៃប្រភេទ Client/Server Soffware ដែលត្រូវបានបង្កើតឡើង ។ LocalTalk Protocol អនុញ្ញាតឱ្យរូបរាងនៃណេតវើកមានទម្រង់ជាLinear bus star ឬជា Tree ដោយប្រើ UTP ។ គុណសម្បត្តិរបស់វាគឺយឺត។ ល្បឿននៃការបញ្ជូនរបស់វាគឺត្រឹមតែ២៣០ Kbps ។

១-៣-៥- Token Ring

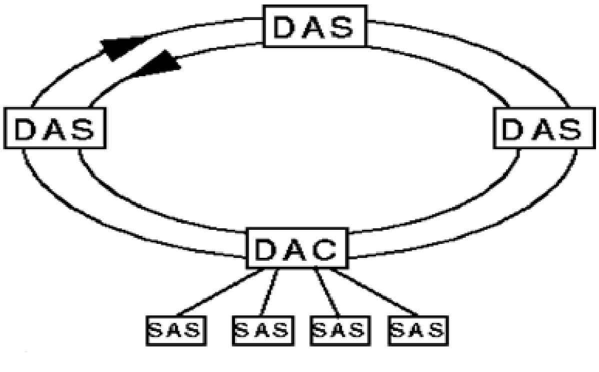
Token Ring protocol ត្រូវបានបង្កើតឡើងដោយក្រុមហ៊ុន IBM ក្នុងឆ្នាំ១៩៨០។ Access Method របស់វាគឺជា Token Passing។ នៅក្នុង Token passing គឺកុំព្យូទ័រទាំងអស់ត្រូវបានភ្ជាប់ជាមួយគ្នាជារង្វង់។ ដូច្នេះសញ្ញារបស់វាធ្វើដំណើរជុំវិញណេ Network ពីកុំព្យូទ័រមួយទៅកុំព្យូទ័រមួយទៀតក្នុងទម្រង់ជារង្វិលជុំ។ អេឡិចត្រូនិកតែមួយគត់បំលាស់ទីជុំវិញនៃ Ring ពីកុំព្យូទ័រមួយទៅកុំព្យូទ័រមួយទៀត។ ប្រសិនបើកុំព្យូទ័រមួយគ្មានព័ត៌មានត្រូវបញ្ជូននោះទេ វាបញ្ជូន Token ទៅឱ្យកុំព្យូទ័របន្ទាប់។ បើកុំព្យូទ័រមួយមានបំណងចង់ធ្វើការបញ្ជូននិងទទួលនូវ Token ទទេរមួយ វាភ្ជាប់ទិន្នន័យទៅកាន់ Token។ Token បំលាស់ទីជុំវិញ Ring រហូតមកដល់កុំព្យូទ័រដែលមានផ្ទុកទិន្នន័យ។ ចំណុចនេះទិន្នន័យត្រូវបានចាប់យកដោយកុំព្យូទ័រដែលជាអ្នកទទួល។ Token Ring Protocolត្រូវការ Star-Wired Ring ដោយប្រើ UTP ឬជា Fiber Optic ។ វាអាចធ្វើការបញ្ជូនដែលមានល្បឿន 4Mbps ឬ 16 Mpbs ។ ដោយសារតែមានការពេញនិយមប្រើ Ethernet ធ្វើឱ្យ Token Ring មានការធ្លាក់ចុះ។

១-៣-៦- FDDI

FDDI(Fiber Distributed Data Interface)គឺជា Network Protocol មួយដែលត្រូវបានបង្កើតឡើងសម្រាប់ភ្ជាប់ Local Area Network តាមធម្មតាដែលមានរយៈចម្ងាយឆ្ងាយ។ Access Method របស់វាគឺជាប្រើ Token Passing ។ FDDI ប្រើរូបរាងដែលមានខ្សែពីរ។ ការបញ្ជូនទិន្នន័យតាមធម្មតាប្រើខ្សែតែមួយក្នុងចំណោមខ្សែជាច្រើននោះ។ ប្រសិនបើមានការខូចខាតកើតមានឡើងចំពោះប្រព័ន្ធនោះព័ត៌មានត្រូវបានបញ្ជូនដោយប្រើខ្សែទី២ក្នុងការបង្កើតឡើងនូវ Ring ថ្មី។ គុណសម្បត្តិនៃ FDDI គឺវាមានល្បឿនលឿន។ វាប្រតិបត្តិការលើខ្សែ Optic មានល្បឿន 100Mpbs ។

Network Configuration

FDDI - Network Schematic



DAS : Dual Attach Station
DAC: Dual Attach Concentrator
SAS:Single Attach Station

FDDI - 2 Counter Rotating Rings

រូបភាព១-បង្ហាញពី Ring ដែលមានខ្សែពីរនិងឧបករណ៍ប្រើជាមួយវា

- Rings ទាំងពីររបស់ fibre ត្រូវបានដំឡើងគឺ - Primary and Secondary ring
- Token និង data flow តាមទិសដៅពីរផ្សេងគ្នាក្នុង Ring នីមួយៗ
- Ring ទី២ប្រហែលត្រូវបានប្រើប្រាស់ជាខ្សែបំរុង(Backup) នៅពេលដែល Ring ទី១ត្រូវបានខូច
- Stations នៅក្នុង FDDI Ring ត្រូវបានភ្ជាប់ទៅ Ring ទាំងពីរ

Fault tolerance

- Fibre break – Port ពីរជាប់គ្នាខូចវាត្រូវបានផ្តាច់ហើយ Stations ទាំងនោះត្រូវបានមិនដំណើរការ មានន័យថា Ring ក្លាយជា Ring តែមួយ។
- Station failure–Stations ពីរនៅជិតបំផុតត្រូវបានខូច មានន័យថា Ring ក្លាយជា Ring តែមួយ
- Multiple breaks - rings ត្រូវបានដាច់ជាកង់ៗ

របៀបនៃការភ្ជាប់

Workstations

- Device ដែលមាន port ពីរត្រូវបានភ្ជាប់ដោយផ្ទាល់ជាមួយ Ring ទាំងពីរដែលគេហៅថា DAS (Dual Attachment Station)។ គេកំរភ្ជាប់វាជាមួយ workstations ណាស់នៅលើ FDDI backbone
- SAS - Single Attachment Station -ត្រូវបានគេភ្ជាប់ជាមួយ primary ring

Concentrator

- DAC Dual Attachment Concentrator - SASs in a star
  - គេនិយមប្រើវា
    - Fault tolerant eg. powering down workstation
    - សម្រាប់ផ្តល់ជាគម្រោងល្អសម្រាប់ការដំឡើង network
    - ចំណាយតិចក្នុងការភ្ជាប់
    - មិនរំខានដល់ការភ្ជាប់
    - ងាយស្រួលដល់ការដោះស្រាយរាល់បញ្ហាដែលបានកើតឡើង
  - គេមិននិយមប្រើ
    - បើចំណុចមួយខូច វាធ្វើឱ្យ workstations ជាច្រើនខូចទាំងអស់
    - Concentrators អាចរៀបតាមលំដាប់ថ្នាក់បង្កើតបានជា Tree ។
    - SAC - Single Attachment Concentrator - សម្រាប់ភ្ជាប់មកកាន់ DAC type concentrator.
    - Dual homing - គឺជា DAS មួយត្រូវបានគេភ្ជាប់ជាមួយ concentrator ports ដែល port A គឺជា hot standby សម្រាប់ជាជំនួយឱ្យ B port ក្នុងករណីវាខូច

ប្រភេទនៃ Port

- មាន Port 4 ប្រភេទខុសគ្នាគឺ A, B, S, M
- DASs មាន 2 ports A និង B ដែលត្រូវបានភ្ជាប់ឆ្លាស់គ្នា មានន័យថា port A នៃ DAS គឺត្រូវបានភ្ជាប់ជាមួយ port B នៃ DAS មួយទៀត
- SASs មាន S port តែមួយគត់
- Concentrators មាន M ports ជាច្រើនដែលអាចភ្ជាប់ជាមួយ S ports នៃ SASs (ឬ A and B ports of DASs)

Port connections

- ការភ្ជាប់ខុសបច្ចេកទេស

M - M

- ពេញនិយមភ្ជាប់

A - B A - M B - M M - S

- ការភ្ជាប់ដែលបណ្ដាលឱ្យមានបញ្ហា (Vendor dependent)

A - A B - B S - A S - B S - S

ខ្សែ Fiber Optic

- Multimode fibre 62.5/125 micron (fibre/casing)
- អាចប្រើជាមួយ 50/125, 85/125 ...
- Single mode 8-12 micron
- 62.5/125 សម្រាប់ LED/photodiode technology ត្រូវបានប្រើប្រាស់សម្រាប់រកឱ្យឃើញពន្លឺនៅក្នុងខ្សែដែលត្រូវការ fibre ទំហំធំ
- 50/125 ប្រើប្រាស់ដោយក្រុមហ៊ុន PTTs ជាច្រើនក្នុងប្រទេសអឺរ៉ុប
- 8-12 micron cable ត្រូវបានប្រើប្រាស់ជាមួយ Laser

Cabling

- 4 fibres (2 transmit and 2 receive)
- Installation of spares recommended for replacement of faulty fibres

FDDI over Copper – CuDDI

- ប្រើ copper UTP (Unshielded Twisted Pair) ឬ STP (Shielded Twisted Pair) cables សម្រាប់ desktop FDDI
- មានប្រវែងអតិបរិមាន ១០០ម៉ែត្រ
- Standard: ANSI TP-PMD (Twisted Pair – Physical Medium Dependent)
- ខ្សែមានតម្លៃថោក ងាយស្រួលក្នុងការ installation និងងាយស្រួលក្នុងការភ្ជាប់
- Copper transceivers មានតម្លៃថោក តូចជាងនិងត្រូវការថាមពលតិច

១-៣-៧- ATM

ATM(Asynchronous Transfer Mode)គឺជា Network protocol មួយដែលបញ្ជូនទិន្នន័យនូវអត្រាល្បឿន 155 Mbps ឬខ្ពស់ជាងនេះ។ ATM ធ្វើការដោយបញ្ជូនទិន្នន័យទាំងអស់នៅក្នុងទម្រង់ជា Packets តូចៗនៃទំហំថេរពីព្រោះថា Protocol ផ្សេងទៀតបញ្ជូន Packets មានប្រវែងប្រែប្រួល។ ATM អាចប្រើជាមួយ Media មានដូចជា Video,CD-quality audio និង imaging។ ATM ធ្វើការជាមួយរាងជា STAR ដែលអាចធ្វើជាមួយ Fiber Optic និង UTP ផងដែរ។

ATP ភាគច្រើនត្រូវបានភ្ជាប់ជា LAN ពីរឬច្រើន។ វាត្រូវបានប្រើដោយ IPS(Internet Service Provider) ផងដែរដើម្បីដំណើរការដែលមានល្បឿនលឿនទៅកាន់ Internet សម្រាប់អតិថិជនរបស់គេ។
បច្ចេកវិទ្យា ATM កំពុងពេញនិយមដែលផ្ដល់ជាដំណោះស្រាយផ្សេងៗសម្រាប់ធ្វើឱ្យ LAN ល្បឿនលឿន។
តារាងសង្ខេបពី Protocol

Protocol	Cable	Speed	Topology
Ethernet	Twisted Pair, Coaxial, Fiber	10 Mbps	Linear Bus, Star, Tree
Fast Ethernet	Twisted Pair, Fiber	100 Mbps	Star
LocalTalk	Twisted Pair	.23 Mbps	Linear Bus or Star

Token Ring	Twisted Pair	4 Mbps - 16 Mbps	Star-Wired Ring
FDDI	Fiber	100 Mbps	Dual ring
ATM	Twisted Pair, Fiber	155-2488 Mbps	Linear Bus, Star, Tree

រូបភាព២-បង្ហាញពីតារាងសង្ខេបនៃ Network Protocols

សំណួរត្រួតពិនិត្យ

១-តើ protocol ជាអ្វី?

២-តើ Protocol ដែលអ្នកបានសិក្សាមានអ្វីខ្លះ?ចែកចេញជាប៉ុន្មានប្រភេទ?

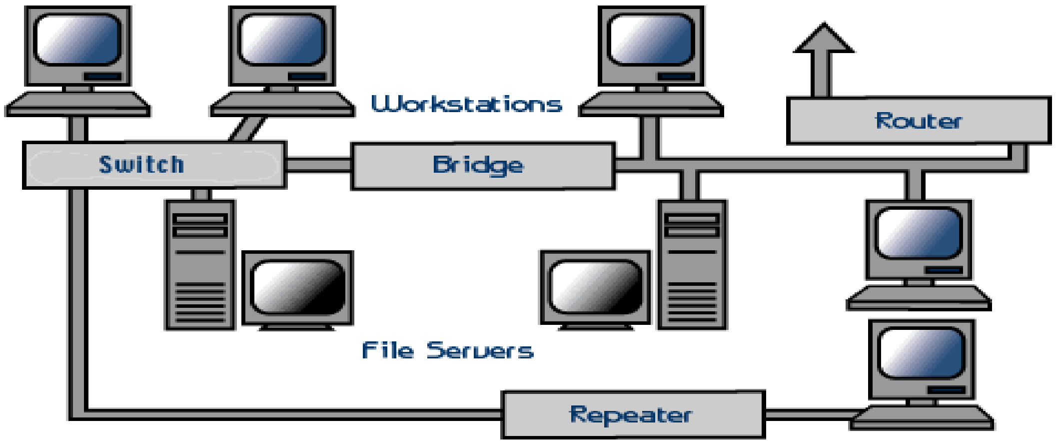
៣-តើ Protocol ណាដែលគេនិយមប្រើជាងគេ?ហេតុអ្វី?

៤-តើ FDDI ខុសពី Protocol ផ្សេងទៀតយ៉ាងដូចម្តេច?

៥-តើចំណុចពិសេសរបស់ FDDI ត្រង់ចំណុចណា?

១-៤- តើ Networking Hardware ជាអ្វី?

Networking hardware រួមមានកុំព្យូទ័រ peripherals,Interface cards និងឧបករណ៍ផ្សេងៗទៀតសម្រាប់ដំណើការទិន្នន័យនិងធ្វើការទំនាក់ទំនងនៅលើណេតវើក។ សូមពិនិត្យទៅលើរូបភាពខាងក្រោមស្តីអំពី network hardware ទាំងនោះ។



រូបភាព៣-បង្ហាញពីការដំឡើង Network ដោយប្រើ Networking devices

ផ្នែកនេះផ្តល់ព័ត៌មានអំពីសមាសភាពដូចខាងក្រោម:

- File Servers
- Workstation
- Network Interface Cards(NIC)
- Switches
- Repeater
- Bridges
- Router

១-៤-១- File Servers

Fileserver គឺជាផ្នែកមួយដ៏សំខាន់របស់ប្រព័ន្ធ Network។ វាគឺជាកុំព្យូទ័រមេមួយដែលមានទំហំ RAM ធំ មាន Hard disk ទំហំធំនិងមានភ្ជាប់មកជាមួយនូវ Network Card ដែលមានល្បឿនលឿន។ Network Operating System(NOS) ក៏ត្រូវបានគេដំឡើងរួចជាស្រេចនៅក្នុងកុំព្យូទ័រនោះផងដែរ។ ក្រៅពីនេះទៀតគេបានដំឡើងនូវ Software application និងទិន្នន័យមួយចំនួនទៀតត្រូវបានគេប្រើដើម្បីចែកចាយ។

Fileserver ត្រូវបានគេប្រើប្រាស់ដើម្បីគ្រប់គ្រងទៅលើប្រព័ន្ធណេតវើកដែលអាចឱ្យវាបញ្ជូននូវ Word processor ទៅឱ្យ Workstation មួយផ្សេងទៀតហើយរក្សាទុកនូវ Email message ជាមួយវាងដែរ ។ នេះគឺជាតម្រូវការនៃកុំព្យូទ័រមួយដែលអាចផ្ទុកព័ត៌មានជាច្រើនិអាចចែកចាយបានក្នុងល្បឿនយ៉ាងលឿន។ Fileserver យ៉ាងហោចណាស់ត្រូវមានលក្ខណៈដូចខាងក្រោមៈ

- 800 megahertz or microprocessor ឬលឿនជាងនេះ (Pentium 3 or 4, G4 or G5)
- Fast hard drive យ៉ាងតិចបំផុតផ្ទុកបាន 120 gigabytes
- RAID (Redundant Array of Inexpensive Disks) ដើម្បីការបារទិន្នន័យបន្ទាប់ពីមាន Disk ណាមួយខូច

SCSI Cabling

-Internal Devices

- 68 pin cable

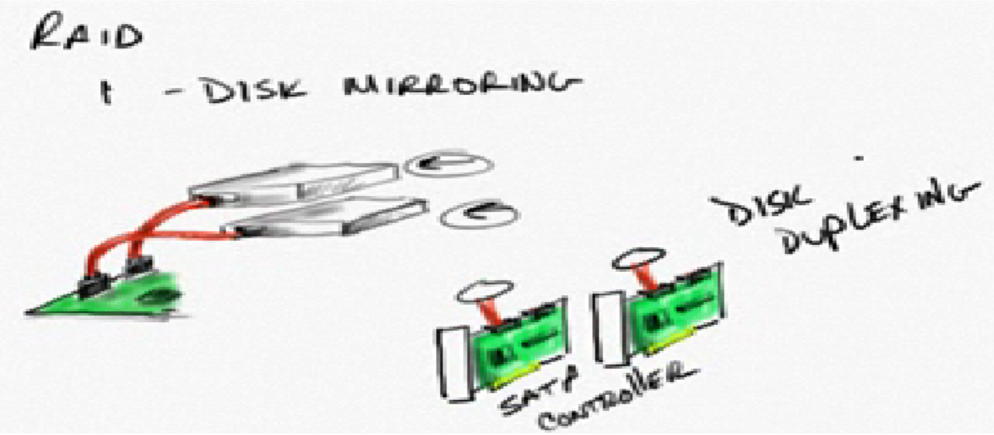
-External devices

- 50 pin or 68 pin

SCSI(Small កុំព្យូទ័រ Systems Interfaces

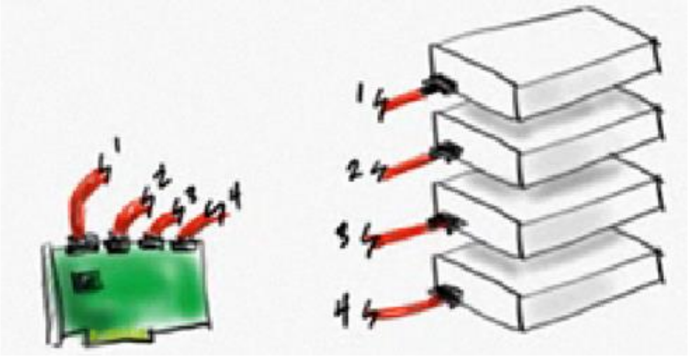
- 1970's

RAID-1:Mirroring



RAID-5:Disk Stripe Set with Parity

Disk Striping with Parity



RAID

- Seril ATA
- Parallel ATA

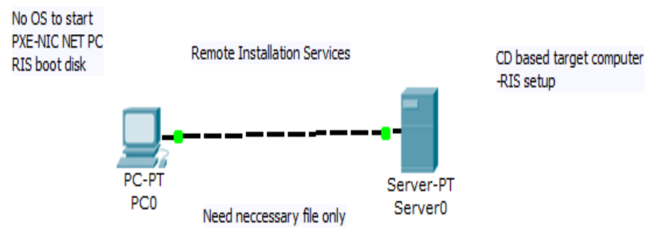
Hardware vs. Software

Configuration

Server អាចដើរតួនាទីជា RIS Server

RIs server ត្រូវការ DAD

- DNS-IP
- Active Directory ដើម្បីរក្សាទុក RIS Server
- DHCP-សម្រាប់ផ្តល់IP addresses ជាស្វ័យប្រវត្ត



- A tape backup-up unit (i.e. DATA, JAZ, Zip, ឬ CD-RW drive) គឺជាឧបករណ៍សម្រាប់រក្សាទុកទិន្នន័យនៅពេលធ្វើការ backup
- មាន expansion slot ជាច្រើន
- network interface card មានល្បឿនលឿន
- RAM យ៉ាងហោចណាស់ 512 MB

១-៤-២- Workstations

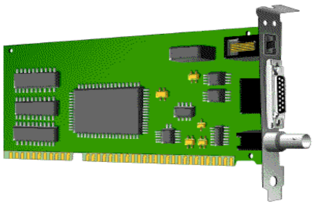
គ្រប់កុំព្យូទ័រទាំងអស់ដែលភ្ជាប់ទៅណែតវើកគេហៅថា Workstation។ Workstation គឺជាកុំព្យូទ័រមួយដែលត្រូវបានដំឡើងជាមួយ Network Interface card network software និងខ្សែសមរម្យ។ Workstation មិនចាំបាច់ត្រូវការនូវ Flopyy Disk drive នោះទេពីព្រោះថា Files អាចត្រូវបានរក្សាទុកនៅលើ Fileserver នោះ។ គ្រប់កុំព្យូទ័រទាំងអស់អាចប្រើជា Network station មួយបាន។

១-៤-៣- Network Interface Cards

Network interface card(NIC)សម្រាប់ផ្តល់ឱ្យនូវការភ្ជាប់រវាង Network និង Copmuter Workstation។ NICs ភាគច្រើនគឺជា Card ដែលស្ថិតនៅខាងក្នុងដែលដោតភ្ជាប់ទៅនិង expansion slot នៅខាងក្នុងនៃកុំព្យូទ័រ។ កុំព្យូទ័រមួយចំនួនគឺជា Macintosh ដែលប្រើប្រអប់ខាងក្រៅដែលអាចភ្ជាប់ជាមួយ Serial port ឬ SCSI port ។ កុំព្យូទ័រLaptopឥឡូវអាចទិញភ្ជាបមកជាមួយនូវNetwork card ឬជាមួយ network card អាចជា PCMCIA slot ។

Network Inferface Cards គឺជាកត្តាចម្បងជាងគេក្នុងការកំណត់ល្បឿននិងការបញ្ជូនទិន្នន័យក្នុងណេតវើក។ វាគឺជាគំនិតល្អដែលប្រើ Network cards ដែលមានល្បឿនលឿនសម្រាប់ Workstation ។

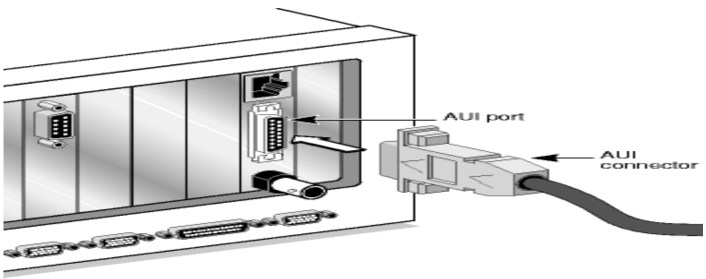
Network interface Card មានបីប្រភេទគឺ Ethernet cards, LocalTalk connectors និង Token Ring cards ។



១-៤-៤- Ethernet Cards

Ethernet cards ជាធម្មតាទិញមកជាប់ដោយឡែកពីកុំព្យូទ័រ ទោះបីជាកុំព្យូទ័រជាច្រើនដូចជា Macintosh មានភ្ជាប់ជាមួយ option សម្រាប់ភ្ជាប់ Enternet card ក៏ដោយ។ Ethernet card កន្លែងសម្រាប់ប្រើទាំងខ្សែជា Caxial និង UTP។

ប្រសិនជាវាត្រូវបានបង្កើតឡើងសម្រាប់ខ្សែCoaxial នោះវាជាប្រភេទ BNC។ ប្រសិនបើវាត្រូវបានបង្កើតឡើងសម្រាប់ UTP នោះវាជា RJ-45។ Ethernet card មួយចំនួនមានប្រភេទជា AUI ផងដែរ។



LocalTalk Connectors

LocalTalk គឺជាផលិតផលរបស់ក្រុមហ៊ុន Apple សម្រាប់កុំព្យូទ័រ Macintosh networking ។ វាប្រើប្រាស់ Adapter ពិសេសនិងខ្សែដែលភ្ជាប់ port printer នៃ Macintosh ។ គុណវិបត្តិនៃ LocalTalk គឺថាវាមានល្បឿនយឺតបើប្រៀបធៀបជាមួយ Ethernet ។ Ethernet ភាគច្រើនប្រតិបត្តិបាន 10Mbps។ ផ្ទុយមកវិញ LocalTalk ប្រតិបត្តិការបានត្រឹមតែ 230 Kbps ឬ .23 Mbps ។

Ethernet Cards ប្រៀបធៀបជាមួយ LocalTalk

Ethernet	LocalTalk
មានល្បឿនលឿនក្នុងការបញ្ជូនទិន្នន័យ(ពី១០ដល់ ១០០ Mbps)	មានល្បឿនយឺតក្នុងការបញ្ជូនទិន្នន័យ(.២៣ Mbps)
មានតម្លៃថ្លៃពីព្រោះទិញដាច់ដោយឡែកពីគ្នា	មានស្រាប់នៅក្នុង Macintosh
ត្រូវការ Slot	មិនត្រូវការ Slot
អាចប្រើបានជាមួយកុំព្យូទ័រភាគច្រើន	ប្រើបានតែជាមួយ Macintosh

រូបភាព៤-បង្ហាញពីការប្រៀបធៀប Ethernet និង LocalTalk network

Token Ring Cards

Token Ring network cards មានលក្ខណៈស្រដៀងទៅនិង Ethernet card ដែរ។ គេមើលឃើញភាពខុសគ្នាប្លែកមួយគឺប្រភេទនៃ Connector នៅខាងក្រោយនៃ Card ។ Token Ring Card ជាទូទៅមាន ៩ម្ជុល DIN ប្រភេទ Connector ដើម្បីភ្ជាប់ Card ទៅនឹងខ្សែ Network ។

១-៤-៥- Switch

Concentrator គឺជាឧបករណ៍មួយដែលផ្តល់ឱ្យនូវចំណុចតភ្ជាប់កណ្តាលសម្រាប់ខ្សែពី Workstation Server និង Pheripherals។ នៅក្នុងរូបរាងនៃ Star ខ្សែ UTP ត្រូវបានភ្ជាប់ពីគ្រប់ Workstation ទៅកាន់ Switch/Hub។ Switch ភាគច្រើនគឺជា Active ដែលវាមានកំលាំងសញ្ញាលដែលអាចបំលាស់ទីពីឧបករណ៍មួយទៅឧបករណ៍មួយទៀត។ Switch មិន Broadcast ដូច Hub នោះទេ។ វាចាំនូវ Address របស់កុំព្យូទ័រនិងបញ្ជូនព័ត៌មានទៅកាន់គោលដៅបានច្បាស់លាស់។

Swichs គឺ

- ប្រើ configured with 8, 12, ឬ 24 RJ-45 ports
- ប្រើនៅក្នុង star ឬ star-wired ring topology
- មាន software ពិសេសសម្រាប់គ្រប់គ្រងទៅលើ port
- ជាធម្មតាដំឡើងនៅក្នុងស្តង់ជាជាលោហៈធាតុដែលអាចផ្ទុកនូវ netmodems, bridge ឬ routers

១-៤-៦- Repeaters

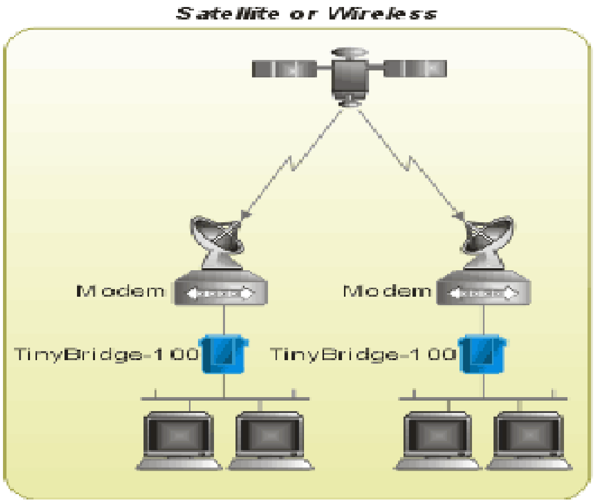
ដោយសារតែសញ្ញាលចុះខ្សោយនៅពេលដែលឆ្លងកាត់ខ្សែ ដូច្នេះគេត្រូវការធ្វើឱ្យសញ្ញាលនោះខ្លាំងឡើងវិញ គេប្រើឧបករណ៍មួយហៅថា Repeater ។ Repeater ធ្វើឱ្យសញ្ញាលដែលវាទទួលបានមានកម្លាំងខ្លាំងឡើងវិញ ហើយ Broadcast បន្តទៅមុខទៀត។ Repeater អាចជាឧបករណ៍មួយដាច់ដោយឡែកឬស្ថិតនៅក្នុង Concen - trator ។ វាត្រូវបានប្រើនៅពេលដែលប្រវែងនៃខ្សែសរុបរបស់ Network ទៅតាមស្តង់ដានៃប្រភេទខ្សែដែលត្រូវប្រើ។

ឧទាហរណ៍ល្អនៃការប្រើRepeater គួរតែប្រើនៅក្នុងLAN ដែលមានរូបរាងជា Star ជាមួយខ្សែUTP ។ ប្រវែងកំណត់នៃ UTP គឺ១០០ម៉ែត្រ។ ការដំឡើងសម្រាប់ Workstation នីមួយៗត្រូវបានភ្ជាប់ជាមួយ UTP ទៅកាន់ Port នៃ Active Concentrator ។ Concentrator បង្កើនកំលាំងសញ្ញាលទាំងអស់ដែលបានឆ្លងកាត់វាហើយ វាអនុញ្ញាតឱ្យការតភ្ជាប់នៃខ្សែអាចលើសពី១០០ម៉ែត្រ។

១-៤-៧- Bridges

TinyBridge-100

Miniature Remote Ethernet Bridge Extender



Bridges គឺជាឧបករណ៍ដែលអនុញ្ញាតឱ្យយើងអាចចែក Network ដ៏ធំមួយជាផ្នែកតូចៗជាច្រើនដែលគេហៅថា Segment ដើម្បីធ្វើឱ្យ Network ដំណើរការប្រសើរ។ បើយើងបន្ថែម Segment ថ្មីចំពោះគម្រោងនៃ Network ដែលមានស្រាប់ នោះយើងត្រូវប្រើ Bridges ដើម្បីភ្ជាប់ Network ទាំងពីរនោះ។ Bridges អាចបង្ហាញពីចរាចរណ៍ព័ត៌មានដែលស្ថិតនៅក្នុងផ្នែកទាំងសងខាងនៃ Nerworks។ ដូច្នោះវាអាចបញ្ជូន Packets ទៅចាំគោលដៅច្បាស់លាស់។ Bridge ភាគច្រើនបំផុតអាចដឹងពីប្រព័ន្ធ Network ហើយវាអាចស្គាល់ Address របស់កុំព្យូទ័រនីមួយៗដែលស្ថិតនៅទាំងសងខាងរបស់វាជាស្វ័យប្រវត្តិ។ Bridge ត្រួតពិនិត្យទៅលើសារនីមួយៗហើយនៅក្នុងករណីចាំបាចវា broadcast សារនោះទៅផ្នែកណាមួយនៃ Network។ Bridge គ្រប់គ្រងទភលើចរាចរណ៍របស់ Network ដើម្បីធ្វើឱ្យដំណើរការរបស់ Network ដែលស្ថិតនៅផ្នែកទាំងពីររបស់វាបានដំណើរការបានល្អប្រសើរ។ គេអាចប្រើប្រាស់វាដើម្បីភ្ជាប់ network ដែលមានខ្សែប្រភេទផ្សេងគ្នា ប្រភេទនៃរូបរាងផ្សេងគ្នា ប៉ុន្តែត្រូវបាន Software protocol ដូចគ្នា។

១-៤-៨- Router

គ្រប់ Cisco Routerមាន IOS(Internetworking Operating System)ដែលប្រើសម្រាប់គ្រប់គ្រង់លើវា ។
មូលដ្ឋានគ្រឹះនៃ Cisco Router មួយចំនួនមានដូចជា

1- Interface :គឺជា Ports ដែលអនុញ្ញាតឱ្យយើងអាចភ្ជាប់ជាមួយវាបាន ។
Interfaces ផ្នែកខាងក្រោយរបស់ Cisco Router

ISDN interfaces របស់ Cisco Router

Ethernet interfaces របស់ Cisco Router

2- Processor(CPU):បង្កើត Interrupt Request(IRQ) ជាមួយសមាភាពអេឡិចត្រូនិកក្នុង Router ដើម្បីធ្វើការប្រាស្រ័យទាក់ទងជាមួយគ្នា។ Cisco Router ប្រើ Motorola RISC processor ដែលជាទូទៅការប្រើប្រាស់របស់វាមិនលើសពី 20% ។

3- IOS: គឺជាប្រព័ន្ធប្រតិបត្តិការដ៏សំខាន់ដែល Router ប្រើសម្រាប់ដំណើរការ។ វាចាប់ផ្តើមដំណើរការនៅពេលដែល Router boot ឡើង។ ជាទូទៅវាមានទំហំពី 2MB ទៅ 5MB ។

4- Rxboot image:គឺជា bootloader ដែលជា Version របស់ IOS ហើយស្ថិតនៅក្នុង ROM របស់កុំព្យូទ័រ ។ បើគ្មាន Flash Card សម្រាប់ Load ពី IOS ទេ យើងអាច Configure វាឱ្យ load ចេញពី Rxboot Image ដែលផ្តល់លទ្ធភាពឱ្យយើងអាចមើលថែទាំ System និងធ្វើឱ្យ Interfaces ផ្សេងៗទៀតអាចដំណើរការឬមិនអាចដំណើរការបាន។

5- NVRAM (Non-volatile RAM):គឺជា Memory ពិសេសដែលវារក្សាទុក Configuration របស់វា។ នៅពេលយើង Configure វាហើយ Save វាត្រូវបានរក្សាទុកនៅទីនោះ (NV RAM)។

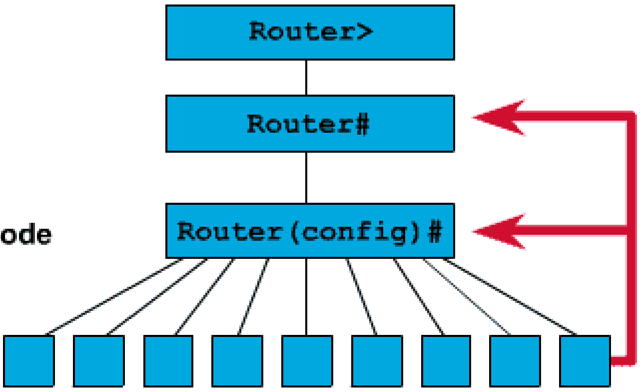
6- ROM (Read-Only Memory):គឺវារក្សាទុកនូវ Bootrap និង POST ។

7- Flash Memory:គឺជាEEPROM(Electronic Erasable Programmable Read Only Memory)

8- Configuration Register:សម្រាប់កំណត់ថាតើ Router ត្រូវ boot IOS image ពីFlash (tftp Server) ឬគ្រាន់តែ Load ចេញពី Rxboot image ។

Overview of Router Modes

- **User Exec mode**
- **Privileged Exec mode**
- **Global configuration mode**
- **Specific Configuration modes**



Configuration Mode	Prompt
Interface	Router(config-if)#
Subinterface	Router(config-subif)#
Controller	Router(config-controller)#
Map-list	Router(config-map-list)#
Map-class	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router	Router(config-ipx-router)#
Route-map	Router(config-route-map)#

ប្រភេទនៃ Cisco Routers មានដូចខាងក្រោម៖

Cisco 700 series

-Cisco 800 series

- Cisco 1600 series

Cisco 2600 series

Cisco 7200 Series

តួនាទីរបស់ Router

សម្រាប់បកប្រែព័ត៌មានពី Network មួយទៅកាន់ nerwork មួយផ្សេងទៀត វាហាក់បីដូចជា Bridge ដ៏វៃឆ្លាតមួយបំផុត។ Router អាចជ្រើសរើសផ្លូវបញ្ជូនដ៏ប្រសើរបំផុតដើម្បីបញ្ជូន Packets ដោយពឹងផ្អែកទៅលើ Address របស់អ្នកទទួលនិងអ្នកបញ្ជូនតាមផ្លូវណាដែលខ្លីជាងគេបំផុត។ ចំណែកឯ Bridge វិញស្គាល់ Address របស់កុំព្យូទ័រដែលស្ថិតនៅក្នុងផ្នែកនីមួយៗនៃ Network (MAC)។

Router ស្គាល់ Address របស់កុំព្យូទ័រ Bridge និង Address របស់ Router ផ្សេងៗទៀតរបស់ប្រព័ន្ធ Network។ Router មិនគ្រាន់តែដឹងពីប្រព័ន្ធ Network ទាំងមូលនោះទេ ប៉ុន្តែវាអាចដឹងពីផ្នែកណាមួយនៃ Network ដែលរវល់ជាងគេបំផុត។

បើសិនជា LAN នៅសាលាភ្ជាប់ទៅនឹង Intenrnet នោះគេត្រូវទិញ Router។ នៅក្នុងករណីនេះ Router ដើរតួនាទីជាអ្នកបកប្រែព័ត៌មានដែលស្ថិតនៅលើ LAN ជាមួយប្រព័ន្ធ Internet។ Router អាចជ្រើសរើសផ្លូវដែលល្អប្រសើរបំផុតដើម្បីបញ្ជូនទិន្នន័យតាមប្រព័ន្ធ Internet។ Router អាចធ្វើការបានដូចខាង ក្រោម:

- វាអាចដឹកនាំចារចរណ៍របស់សញ្ញាលដោយផ្ទាល់ហើយមានប្រសិទ្ធភាពខ្ពស់
- វាអាចបញ្ជូនសាររវាង Protocol ពីរផ្សេងគ្នា
- វាអាចបញ្ជូនសាររវាងរូបរាងជា bus star និង Star-wired ring
- វាអាចបញ្ជូនសារតាម Fiber Optic Coaxial និង UTP

១-៥- តើ Network Cabling ជាអ្វី?

Cable គឺជាខ្សែដែលផ្តល់ឱ្យព័ត៌មានផ្លាស់ប្តូរពីឧបករណ៍មួយទៅឧបករណ៍មួយទៀត។ ខ្សែមាន៤ប្រភេទដែលអាចប្រើជាមួយ LAN បាន។ ក្នុងករណីមួយចំនួន Network ប្រើខ្សែមួយប្រភេទហើយ network ប្រភេទផ្សេងទៀតប្រើខ្សែប្រភេទៀងទៀតដែរ។ ប្រភេទនៃខ្សែដែលត្រូវបានជ្រើសរើសសម្រាប់ Network ទាក់ទងជាមួយនឹងរូបរាងនៃ Network នឹងទំហំរបស់វា។

ការយល់ដឹងពីលក្ខណៈខុសគ្នានៃខ្សែនិងរបៀបដែលវាទាក់ទងទៅនឹងទិដ្ឋភាពផ្សេងៗនៃ Network មួយចាំបាច់សម្រាប់អភិវឌ្ឍជោគជ័យទៅលើ Network ទាំងមូល។ នៅផ្នែកខាងក្រោមនេះពិភាក្សាទៅលើប្រភេទនៃខ្សែដែលត្រូវប្រើក្នុង Network នឹងអ្វីៗដែលទាក់ទងជាមួយនឹងប្រធានបទ។

- Unshielded Twisted Pair (UTP) Cable
- Shield Twist Pair (STP) Cable
- Coaxial Cable
- Fiber Optic Cable
- Wireless LANs
- Cable Installation Guides

១-៥-១- Unshielded Twisted Pair (UTP) Cable

ខ្សែ Twisted Pair មានពីរប្រភេទគឺ **Shielded** និង **Unshiel**ded ។ **Unshielded Twisted Pair (UTP)** ត្រូវបានគេប្រើច្រើននឹងជាទូទៅវាត្រូវបានគេប្រើល្អបំផុតសម្រាប់ **Network** នៅតាមសាលារៀន។

ខ្សែ Cat7

គុណភាពនៃខ្សែ UTP អាចខុសគ្នាពីខ្សែសម្រាប់ប្រព័ន្ធទូរសព្ទ័ពីព្រោះវាមានល្បឿនលឿន។ ខ្សែនេះមាន៤គូរដែលស្ថិតនៅក្នុងសំបករបស់វា។ គូនីមួយៗត្រូវបានវិញបញ្ចូលគ្នាតាមស្តង់ដាដើម្បីជួយបំបាត់នៃការរំខានពីគូដែលជាប់គ្នានិងឧបករណ៍អេឡិចត្រូនិកផ្សេងៗទៀត។

EIA/TIA(Electronic Industry Association/Telecommunication Industry Association) បានបង្កើតស្តង់ដានៃ UTP និងតម្លៃ៧ប្រភេទនៃខ្សែ។

រូបភាព៥-បង្ហាញពីការសង្ខេបនៃ Categories of Unshielded Twisted Pair

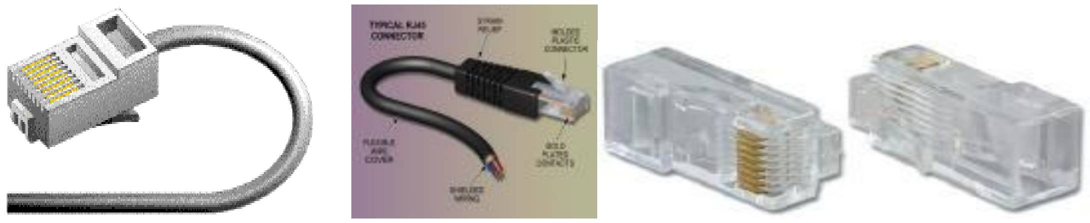
ប្រភេទ	ការប្រើប្រាស់
Category 1	Voice Only (Telephone Wire)
Category 2	Data to 4 Mbps (LocalTalk)
Category 3	Data to 10 Mbps (Ethernet)
Category 4	Data to 20 Mbps (16 Mbps Token Ring)
Category 5	Data to 100 Mbps (Fast Ethernet)
Category 6	Data to 1000Mbps(Gigabit Ethernet)
Category 7	Data to 100Gbps

ប្រសិនបើអ្នករៀបចំ 10 Mbps Ethernet network នឹងគិតដល់ការសន្សំក្នុងការទិញខ្សែ អ្នកគួរទិញខ្សែប្រភេទទី៣ជំនួសឱ្យប្រភេទទី៥វិញ។ ត្រូវចាំថាខ្សែប្រភេទទី៥ផ្តល់នូវលទ្ធភាពជាច្រើនដូចជា "នៅពេលដែលមានការកើនឡើងនៃចំនួនឧបករណ៍" ជាដើម។ ខ្សែប្រភេទទី៣នឹងទី៥ មានប្រវែង Segment វែងបំផុតគឺ១០០ម៉ែត្រ។

- 10BaseT សំដៅទៅលើទំហំនៃខ្សែ UTP(cat 3,4,5) សម្រាប់ទទួល Ethernet signal
- ប្រភេទទី៧គឺជាប្រភេទថ្មីសម្រាប់ Gigabit Ethernet ។

Unshielded Twisted pair Connector

ស្តង់ដានៃ Connector សម្រាប់ UTP គឺ RJ-5 ។ វាគឺជាក្បាលប្រភេទជាប្លាស្ទីកដែលមើលទៅដូចទៅនិងក្បាលសម្រាប់ភ្ជាប់នៃទូរសព្ទ័ដែរ។ Slot មួយអនុញ្ញាតឱ្យស៊ិកបាន RJ-45 តែមួយគត់។ RJ-5 តំណាងឱ្យ Registered Jack ។



រូបភាព៦-បង្ហាញពី RJ-45 connectors

Shielded Twisted Pair (STP) Cable

Cable	Length ft.	Max. Resolution
Cat5e Solid UTP	100	2048 x 1536 at 60Hz
	150	2048 x 1536 at 60Hz
	200	2048 x 1536 at 60Hz
Cat5e Stranded UTP/STP	100	2048 x 1536 at 60Hz
	200	1280 x 1024 at 60Hz
Cat6 Solid UTP	100	1920 x 1440 at 60Hz
	150	1600 x 1200 at 60Hz
550MHz Cat6 Solid UTP	100	2048 x 1536 at 60Hz
	150	1920 x 1200 at 60Hz
Cat6 Solid STP	100	2048 x 1536 at 60Hz
	150	1920 x 1200 at 60Hz
600MHz Cat7 Solid STP	150	2048 x 1536 at 60Hz
	200	2048 x 1536 at 60Hz
600MHz Cat7 Stranded STP	100	2048 x 1536 at 60Hz

គុណវិបត្តិនៃខ្សែ UTP គឺថាវាអាចងាយប៉ះពាល់ជាមួយប្រេកង់នៃវិទ្យុនិងចរន្តអគ្គសនី។ Shielded twisted pair (STP)មានលក្ខណៈសមរម្យសម្រាប់មជ្ឈដ្ឋានដែលមានការរំខាន។ Shielded twisted pair ត្រូវបានប្រើសម្រាប់ Token Ring topology។

RJ-45 colors

RJ-45 cable និង plug មាន 8 pin/conductors។ Pins ទាំងនោះត្រូវបានប្រើជាគូ។ វាមានសម្មតិកម្មអំពីរបៀបរៀបគូនៃ Pin ប៉ុន្តែ 100 baseT ត្រូវបានគេប្រើច្រើនជា EIA 568B ។ វាមានសម្មតិកម្មកូដបីពណ៌សម្រាប់អង្គជាតុចម្លងនីមួយៗជាមួយ RJ-45 cable ។

ក្នុងការតភ្ជាប់ខ្សែ UTP ជា Straigh Cable គេអាចភ្ជាប់តាមពីររបៀបគឺស្តង់ដា A និងស្តង់ដា B ។

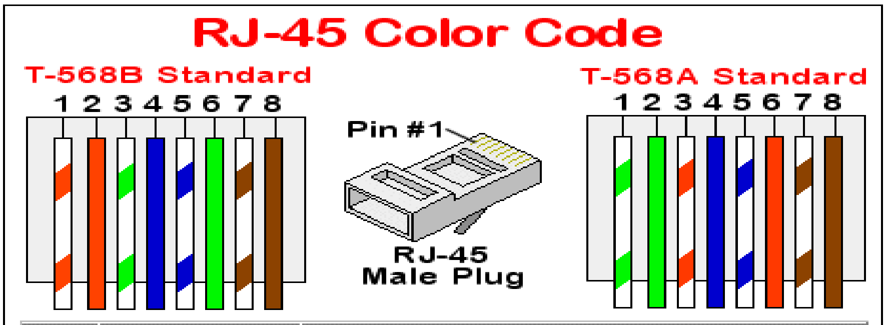
ស្តង់ដា EIA 568B

- Pin លេខ១គេដោតពណ៌សឆ្នូតទឹកក្រូចនឹង Pin លេខ២ គេដោតពណ៌ទឹកក្រូចដែលគេហៅថាគូទី២
- Pin លេខ៣ គេដោតពណ៌សឆ្នូតបៃតងនិង Pin លេខ៦ត្រូវបានគេដោតពណ៌បៃតងដែលគូរនេះគេហៅថាគូទី៣
- Pin លេខ៤ត្រូវបានគេដោតពណ៌ខៀវនឹង Pin លេខ៥ត្រូវបានគេដោតពណ៌ឆ្នូតខៀវដែលគេហៅថាគូទី១
- Pin លេខ៧ត្រូវបានគេដោតពណ៌ឆ្នូតត្នោតនឹង Pin លេខ៨ ត្រូវបានគេដោតពណ៌ត្នោតដែលគេហៅថាគូទី៤

```
  1 2 3 4 5 6 7 8        8 7 6 5 4 3 2 1
.-:-:-:-:-:-:-:-:-.    .-:-:-:-:-:-:-:-:-.
|                 |    |                 |
| female (such as |    |   male (cable)  |
|  ethernet card  |    |                 |
|     or hub)     |    |                 |
`------.   .------'    `------.   .------'
       |_ _|                  |_ _|
```

រូបភាព- Connector

- TIA/EIA 568 B (សមមូលនិង DTE)
  - Leg 1: ពណ៌សឆ្នូតទឹកក្រូច
  - Leg2: ទឹកក្រូច
  - Leg3: ពណ៌សឆ្នូតបៃតង
  - Leg 4: ពណ៌បៃតង
  - Leg5: ពណ៌សឆ្នូតខៀវ
  - Leg 6: ពណ៌ខៀវ
  - Leg 7: ពណ៌សឆ្នូតត្នោត
  - Leg 8: ពណ៌ត្នោត
- TIA/EIA 568 A (សមមូលនិង DCE)
  - Leg 1: ពណ៌សឆ្នូតបៃតង
  - Leg2: ពណ៌បៃតង
  - Leg3: ពណ៌សឆ្នូតទឹកក្រូច
  - Leg 4: ពណ៌ខៀវ
  - Leg5: ពណ៌សឆ្នូតខៀវ
  - Leg 6: ទឹកក្រូច
  - Leg 7: ពណ៌សឆ្នូតត្នោត
  - Leg 8: ពណ៌ត្នោត



Pin #	Ethernet 10BASE-T 100BASE-TX	EIA/TIA 568A	EIA/TIA 568B or AT&T 258A
1	Transmit +	White with green strip	White with orange stripe
2	Transmit -	Green with white stripe or solid green	Orange with white stripe or solid orange
3	Receive +	White with orange stripe	White with green stripe
4	N/A	Blue with white stripe or solid blue	Blue with white stripe or solid blue
5	N/A	White with blue stripe	White with blue stripe
6	Receive -	Orange with white stripe or solid orange	Green with white stripe or solid
7	N/A	White with brown strip or solid brown	White with brown strip or solid brown
8	N/A	Brown with white stripe or solid brown.	Brown with white stripe or solid brown.

ឧបករណ៍សម្រាប់តេស្តខ្សែ

ឧបករណ៍សម្រាប់តេស្តខ្សែ CAT 6

១-៦- Cisco 16xx/26xx/36xx Routers

Cisco Router មាន RI Console Port ហើយវាដំណើរការនូវ IOS(Internet Working Operating System) គ្រប់ប្រភេទទាំងអស់។ នៅក្នុងមេរៀននេះយើងនិងសិក្សាទៅលើស៊េរីនៃ 1600s និង 2600s តែប៉ុណ្ណោះ។ Station Card និង Router ស៊េរី 2600 មាន RJ-45 ប៉ុន្តែវាទាំងពីរមិនត្រូវបានប្រើប្រាស់ជាមួយគ្នានោះទេ។ ដូច្នោះ វាត្រូវតែមាន RJ-45 ទាំងសងខាងហើយយើងត្រូវតែដោតខ្សែនេះឱ្យបានត្រឹមត្រូវ។ តាមធម្មតាគេភ្ជាប់ Router ទៅនិង Patch Panel នឹង Stallion card ដោយប្រើខ្សែពិសេស។

Cisco RJ-45 Pin	Colour	Cisco Signal	Stallion RJ-45 Pin	Stallion Signal
1	White/Green	RTS	N/C	
2	Green	DTR	N/C	
3	White/Orange	TxD	5	RxD
4	Blue	Gnd	3	Gnd
5	White/Blue	Gnd	6	Gnd
6	Orange	RxD	4	TxD
7	White/Brown	DSR	N/C	
8	Brown	CTS	N/C	

រូបភាព-៧-Cisco RJ-45

១-៧- Cisco Catalyst Switches

ការចាប់គូ Pin នៅលើ Cisco Console Port របស់ Switch Catalyst ខុសគ្នាពីការចាប់គូ Pin នៅលើ Cisco 26xx ។ វិធីដែលគេចាបអារម្មណ៍គឺអាស្រ័យទៅលើ Operating software ។

Specification	Cable Type	Maximum length
10BaseT	Unshielded Twisted Pair	100 meters

10Base2	Thin Coaxial	185 meters
10Base5	Thick Coaxial	500 meters
10BaseF	Fiber Optic	2000 meters
100BaseT	Unshielded Twisted Pair	100 meters
100BaseTX	Unshielded Twisted Pair	220 meters

រូបភាព-៨-បង្ហាញពី Ethernet

សំណួរត្រួតពិនិត្យ

១-តើ Networking Hardware មានអ្វីខ្លះ?

២-ចូរបញ្ជាក់ពីតួនាទីនីមួយៗរបស់ Networking Hardware?

៣-តើ Switch និង router ខុសគ្នាដូចម្តេច?

៤-តើ Router មួយមានសមាសធាតុផ្សំអ្វីខ្លះ?

៥-តើ Router មានតួនាទីអ្វីខ្លះក្នុងប្រព័ន្ធ Network?

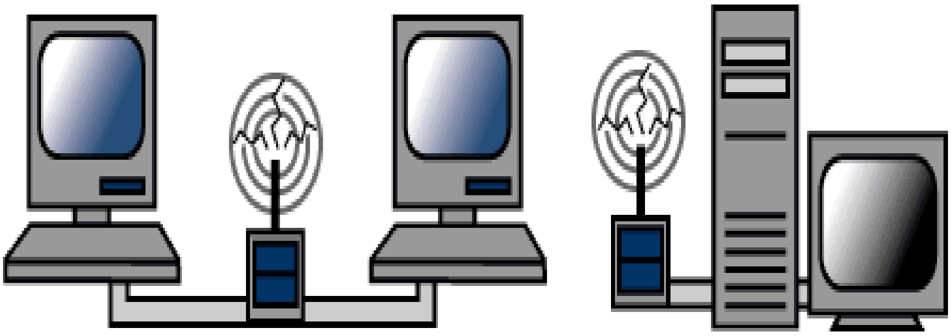
៦-តើខ្សែ UTP មានប៉ុន្មាន Category?ហើយ Category នីមួយៗខុសគ្នាដូចម្តេច?

៧-តើ Server (Hardware)មួយទាមទារឱ្យមានសមាសធាតុផ្សំអ្វីខ្លះ?

៨-តើ Pin ទាំង៨របស់ RJ-45 connector មានតួនាទីអ្វីខ្លះ?

១-៨- Wireless LANs

ដើម្បីភ្ជាប់ Wireless LANs បានគេត្រូវមានWireless Network CardនិងAccess Point (AP)។



១-៨-១- ប្រភេទនៃ Access Point (AP)

Wireless Router អាចដើរតួនាទីជា DHCP,NAT,Firewall ។

គ្រប់ Network ទាំងអស់មិនមែនតភ្ជាប់គ្នាដោយប្រើខ្សែទាំងអស់នោះទេ។ មាន Network ប្រភេទខ្លះត្រូវបានគេតភ្ជាប់ដោយមិនប្រើខ្សែដែលហៅថា Wireless LAN គឺប្រើរលកសញ្ញាលរបស់វិទ្យុដែលមានប្រេកង់កម្រិតខ្ពស់ដូចជាបាច់ពន្លឺ Infrared ឬកាំរស្មី Laser ដើម្បីបញ្ជូនរវាង Workstation និង Fileserver ដែលស្ថិតនៅលើ Wireless network ដោយប្រើនូវ Transceiver ឬជាអង់តែនដែលប្រើសម្រាប់បញ្ជូននិងទទួលទិន្នន័យ។

ព័ត៌មានត្រូវបានបញ្ជូនឆ្លងកាត់តាម Transceiver នៅពេលដែលគេតភ្ជាប់វាតាមលក្ខណៈជារូបរាងនៃ Network ដែលមានចម្ងាយឆ្ងាយ ។ ការប្រាស្រ័យទាក់ទងគ្មានខ្សែអាចប្រើប្រាស់ដូចជា ទូរសព្ទ័ ម៉ាយក្រូវ៉េវ ផ្កាយរណប។ Network គេប្រើសម្រាប់ Laptop កុំព្យូទ័រឬកុំព្យូទ័រពីចម្ងាយដែលភ្ជាប់ទៅនិង LAN ដែលគ្មានខ្សែដែលផ្តល់ឱ្យនូវគុណសម្បត្តិក្នុងការតភ្ជាប់ប្រព័ន្ធ network ដែលស្ថិតនៅក្នុងអាគារចាស់ៗដែលយើងមិនអាចអូសខ្សែបាន។ ការប្រាស្រ័យទាក់ទងតាម Infrare ដែលគេនិយមប្រើក្នុងសាលារៀនមានពីរប្រភេទគឺបាច់ពន្លឺខ្សែត្រង់(light sight)និងបាច់ពន្លឺបញ្ជូនទៅគ្រប់ទីកន្លែង(scattered broadcast light)។

បើសិនជានរណាម្នាក់ដើរកាត់បាច់ពន្លឺខ្សែត្រង់នោះក្នុងពេលវាកំពុងធ្វើការបញ្ជូនទិន្នន័យ នោះព័ត៌មានត្រូវបញ្ជូនឡើងវិញសាជាថ្មីដែលឧបសគ្គបែបនេះធ្វើឱ្យប្រព័ន្ធឥតខ្សែ(Wireless) ដើរយឺត។

ការប្រាស្រ័យទាក់ទងរបស់ Infrare ជារបាយគឺវាធ្វើឱ្យការបញ្ជូនទិន្នន័យតាមទម្រង់ជា Broadcast មានន័យថាសញ្ញាលត្រូវបានបញ្ជូនតាមទិសដៅជាច្រើនហើយអាចបត់បែនតាមជញ្ជាំងឬពិដានរហូតដល់ឧបករណ៍ Transceiver ។ ការប្រាស្រ័យទាក់ទងក្នុងប្រព័ន្ធ network ដែលប្រើ Laser គឺជាបាច់ពន្លឺនៃ infrared ដែលជាបន្ទាត់ខ្សែត្រង់។

Wireless LAN មានគុណវិបត្តិដូចខាងក្រោម:

- មានសុវត្ថិភាពទាប
- ងាយឆ្លងពីប្រភពពន្លឺនិងឧបករណ៍អេឡិចត្រូនិក
- មានល្បឿនយឺតជាង LAN ដែលប្រើខ្សែ

Wireless មាន Standard IEEE 802.11

- IEEE 802.11.b–2.4 GH_Z -11 Mbps មានចម្ងាយ 45m ពី access point
- IEEE 802.11.g-2.4GH_z-Hybrid/54Mbps
- IEEE 802.11.N:ចាប់ពី 54Mbps ឡើងទៅ
- IEEE 802.11.a:54Mbps

១-៨-២- ការរៀបចំដើម្បី Setup Wireless Network

Wireless Router ឬ Wireless Access Point

Wireless Router ឬ Wireless Access Point គឺជាឧបករណ៍ដ៏សំខាន់មួយនៅពេលដែលយើងត្រូវការ Setting Up ចំពោះ Wireless network:

- យើងប្រើ Wireless Router នៅពេលដែលយើងបង្កើត Network ជាលើកដំបូងនៅតាមផ្ទះឬការិយាល័យ ។ បើយើងមាន Ethernet network នៅតាមផ្ទះហើយ យើងគ្រាន់តែទិញនូវ Wireless Access Point និងគ្រាន់តែភ្ជាប់វាជាមួយ Network នោះជាការស្រេច។

Wireless Adapter for កុំព្យូទ័រ Users

- យើងត្រូវមាននូវឧបករណ៍ Wireless adater ដែលត្រូវបានដំឡើងរួចជាស្រេចហើយនៅលើកុំព្យូទ័ររបស់អ្នកក្នុងគោលបំណងចូលរួមក្នុងប្រព័ន្ធ Network ដែលគ្មានខ្សែ។

អ្នកប្រើប្រាស់កុំព្យូទ័រឬ Notebook ហើយអ្នកត្រូវការ Share នូវ Wireless adapter ជាមួយកុំព្យូទ័រផ្សេងនោះអ្នកត្រូវការប្រើនូវ USB wireless Adapter ។ អ្នកគ្រាន់តែដោត USB Wireless Adapter នៅលើកុំព្យូទ័រដែលអ្នកត្រូវការឱ្យមាន Wireless Acces ។

១-៨-៣- វិធីរំលោភដែលឃើញ Wireless Network Profile នៅក្នុង Windows Vista

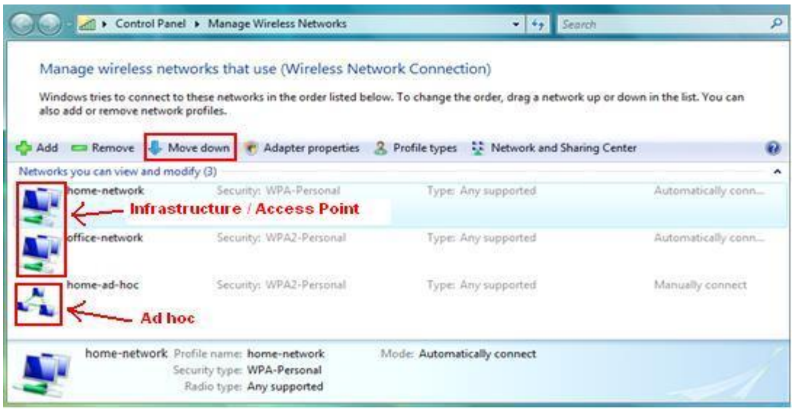
1) ចុចលើ **Start** ហើយចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ **Network** ហើយបន្ទាប់មកចុចលើ **Properties.**

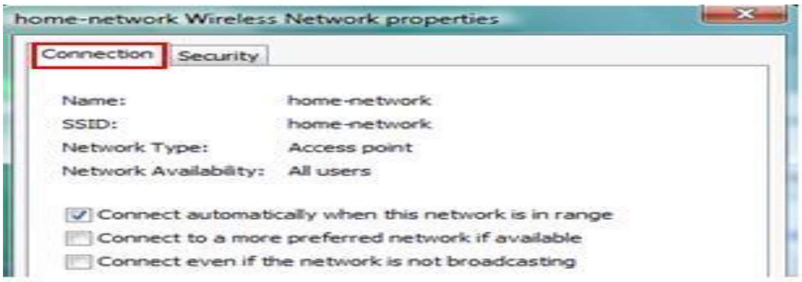
2) Network and Sharing Center window will appear, then click **Manage wireless networks** on the left panel.

3) Manage Wireless Networks window និងបង្ហាញឡើងហើយអ្នកនិងឃើញ wireless network connection មាន។ ចុចពីរដងស្ទួនគ្នាលើ profile ហើយបន្ទាប់មកអ្នកអាចឃើញឬអាចប្តូរ setting របស់វា។

ចំណាំ:កុំព្យូទ័រ icon ពីរធំៗបង្ហាញថាវាគឺជា infrastructure ឬ access point network មានន័យថាអ្នកនិងភ្ជាប់ network តាមរយៈ access point ឬ wireless router។ រូបភាពកុំព្យូទ័រតូចៗចំនួន៣គឺជា ad hoc wireless network មានន័យថា កុំព្យូទ័រនិងភ្ជាប់គ្នាទៅវិញទៅមកដោយផ្ទាល់។

ចំណាំ:network profile ដែលស្ថិតនៅទីតាំងខ្ពស់ជាងនិងមានអាទិភាពជាង។ ឧទាហរណ៍ home-network និងត្រូវបានភ្ជាប់ជំនួសឱ្យ office-network បើ networks ទាំងពីរត្រូវបានភ្ជាប់គ្នាចំពោះអទិភាពជាងនៅលើ home-network profile។ អ្នកអាច **Move up/Move down** Icon ដើម្បីកំណត់អាទិភាព។



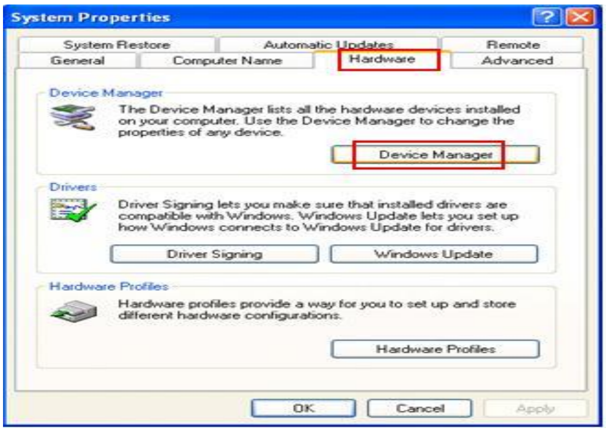


4) វិធីផ្សេងទៀតដែលអ្នកអាចប្តូរឬមើលពី connection profileលើ window(**Start-> Connect To**) ដោយចុចលើប៊ូតុងខាងស្តាំលើ wireless connection ហើយចុចលើ **Properties**។ ទោះបីជាយ៉ាងណាក៏ដោយអ្នកមិនអាចមើល profile នៅលើ wireless connection ថ្មីបាននោះទេ ។

១-៨-៤- វិធីដំឡើងចំផុតគឺពិនិត្យមើល Wireless Card Driver Status ក្នុង Windows XP

1) Go to **Start**, right click **My កុំព្យូទ័រ** and then click on **Properties.**

2) System Properties window និងបង្ហាញឡើង។ ចូលមក **Hardware** tab ហើយចុចលើ **Device Manager.**

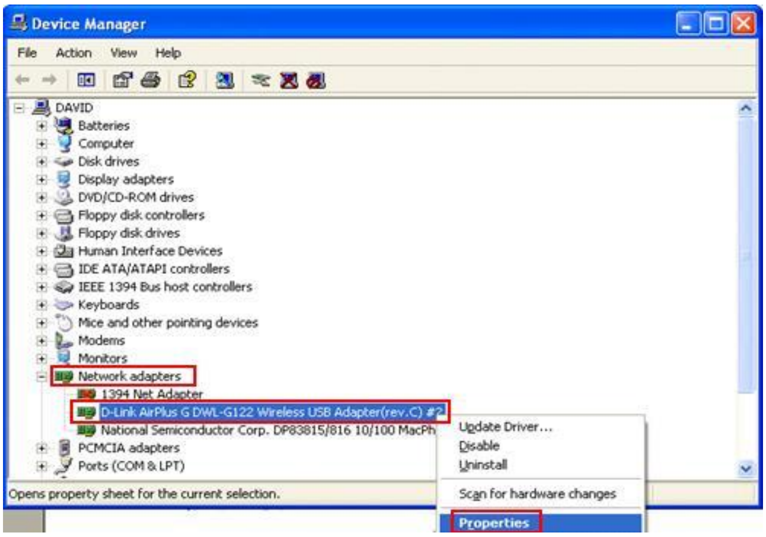


3) Device Manager window និងបង្ហាញឱ្យឃើញហើយអ្នកអាចពិនិត្យមើលពីលក្ខណៈរបស់ hardware drivers ទាំងអស់នៅទីនេះ។ ចុចទាញវាចុះក្រោមរកមើល **Networkadapters** ហើយបន្ទាប់មកចុចលើប៊ូតុងខាងស្តាំលើ wireless adapter ដែលអ្នកត្រូវការពិនិត្យមើលនិងចុចលើ **Properties**។

ឧទាហរណ៍

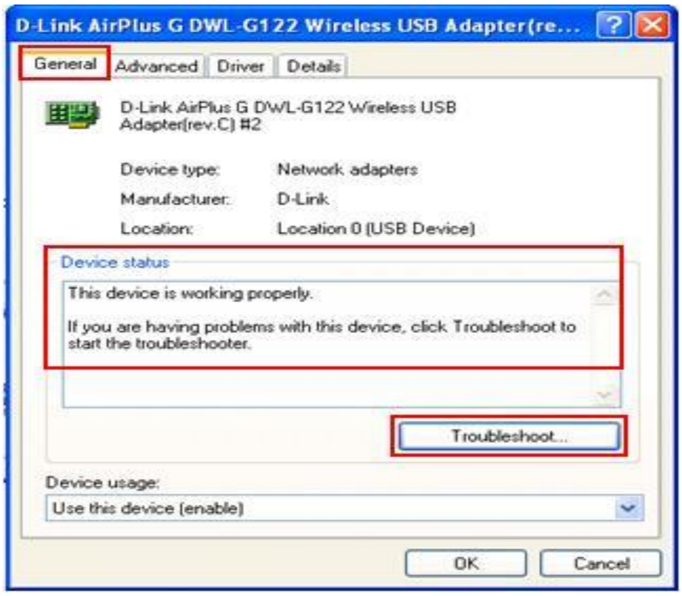
D-Link DWL-G122 USB wireless card's driver status.

ចំណាំ:បើអ្នកមិនអាចរកឃើញ wireless card នៅទីនេះទេ ចូរព្យាយាមមើលវាក្នុង **Other Devices** folder បើឃើញមានន័យថាអ្នកមិនបាន Install driver សម្រាប់ hardware នេះ ។

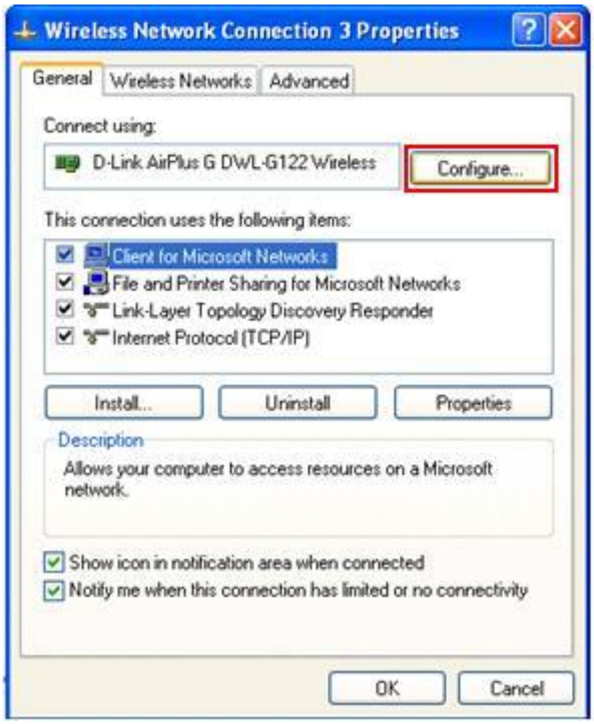


4) wireless card properties window និងបង្ហាញឡើងហើយអ្នកនិងឃើញលក្ខណៈនៃ Device បើ device មិនអាចដំណើរការបានល្អនោះទេ អ្នកអាចចុចលើ**Troubleshoot**...ដើម្បីដោះស្រាយបញ្ហាដែលបានកើតមានឡើងដែលមានការណែនាំភ្ជាប់មកជាមួយស្រាប់។

ចំណាំ:**Troubleshoot**... និងផ្តល់ដោយ Windows XP ប៉ុន្តែវាជាប្រភពនៃការសិក្សាបន្ថែមចំពោះ wireless card driver។ អ្នកអាចចចុចលើ **Advanced** tab ដើម្បីបង្កើត advanced hardware configuration,**Driver** tabដើម្បី update/roll back/uninstall driver។



ចំណាំ: គេមានវិធីផ្សេងទៀតដើម្បីមើល device status នោះដោយចុចលើ **Configure** button នៅក្នុង wireless **card** property ។



១-៨-៥- វិធីឆាប់រហ័សដើម្បីពិនិត្យមើល Network ឬ Wireless Adapter Driver Status ក្នុង Windows Vista

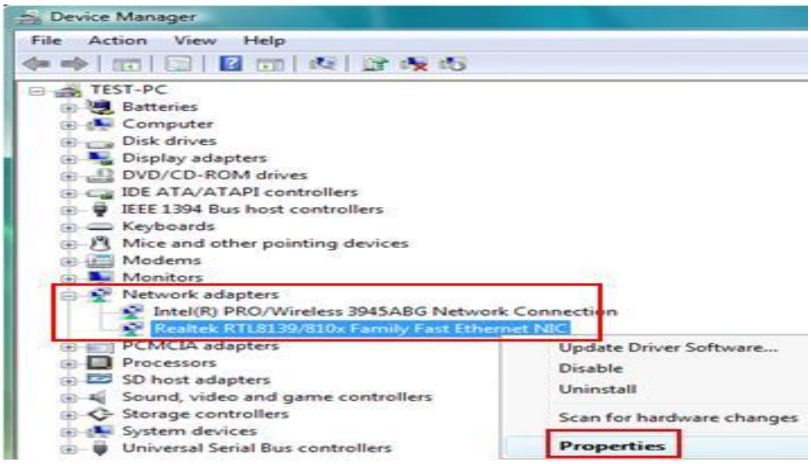
1) ចុចលើ **Start** ហើយបន្ទាប់មកចុចលើ **Control Panel.**

2) ចុចលើ **Hardware and Sound** ក្នុង Control Panel window.

ចំណាំ: បើ Control Panel ជា Classic View អ្នកគ្រាន់ចុចពីរដងលើ Device Manager.

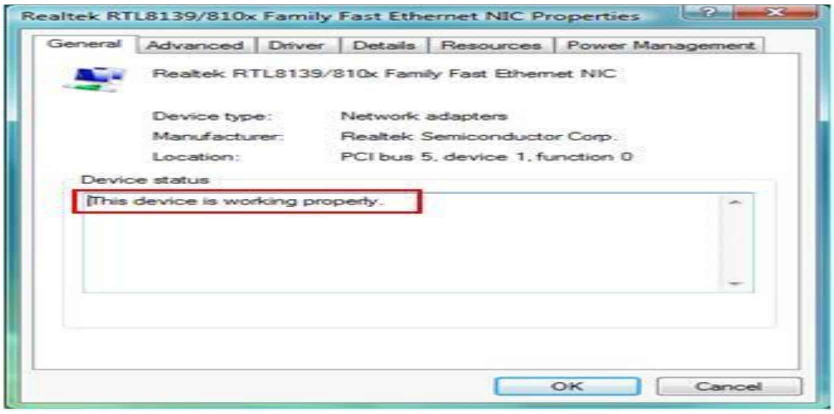
3) នៅក្នុង Hardware and Sound window ចុចលើ **Device Manager** ដើម្បីបើកវា

4）Device Manager និងបង្ហាញឡើងហើយបន្ទាប់មកពង្រីក **Network adapters** ហើយចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ network ឬ wireless adapter ដែលអ្នកត្រូវការត្រួតពិនិត្យហើយចុងក្រោយបង្អស់ចុចលើ **Properties** ។



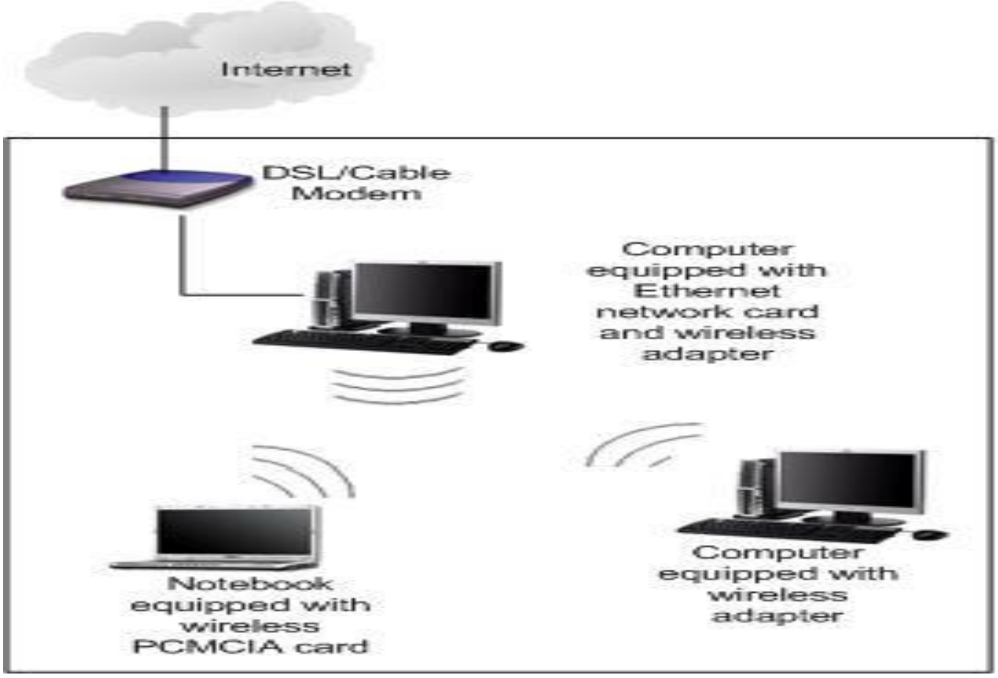
5）network ឬwireless adapter properties window និងបង្ហាញឱ្យឃើញថា driver កំពុងដំណើរការបានល្អបើវាបង្ហាញថា**This device is working properly**នៅក្រោម General tab អ្នកក៏អាច configure network adapter's driver parameters ស្ថិតក្នុង Advanced tab ។

ចំណាំ:បើ device របស់អ្នកមិនដំណើរការបានល្អនោះទេ ចុចលើ Driver tab ដើម្បីពិនិត្យមើលឱ្យបានក្បោះក្បាយ update driver, disable driver ឬ uninstall driver ។



១-៨-៦- របៀប Set Up Ad Hoc Wireless Network ក្នុង Windows Vista

តាមធម្មតាអ្នកមានប្រភេទ network ជាបណ្តោះអាសន្នដើម្បី share documents ក្នុងការប្រជុំ ការលេង game ជាច្រើននាក់ឬ share Internet connection ជាមួយមិត្តភក្តិ។ វាមានគុណវិបត្តិមួយរបស់ network នេះគឺ wireless អាចភ្ជាប់បានក្នុងរយៈចម្ងាយខ្លី។ ដើម្បីភ្ជាប់ឱ្យបានចម្ងាយវែង យើងត្រូវប្រើ wireless router ឬ access point ។



យើងមានកុំព្យូទ័របីហើយបំពាក់ដោយ wireless adapter ។ អ្នកអាច setup ad hoc wireless នៅលើកុំព្យូទ័រមួយហើយចាត់ទុកថាជា host កុំព្យូទ័រ។ នេះគឺជា IP និង netmask ដែលយើងនិងកំណត់ឱ្យ wireless adapter នីមួយៗ។ សូមចំណាំថា អ្នកមិនចាំបាច់ត្រូវការកំណត់ gateway IP និង DNS ទេពីព្រោះថាវាជា peer-to-peer network ។

Host computer:

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

Gateway:

DNS Servers:

Client computer A:

IP Address: 192.168.0.2

Subnet mask: 255.255.255.0

Gateway:

DNS Servers:

Client computer B:

IP Address: 192.168.0.3

Subnet mask: 255.255.255.0

Gateway:

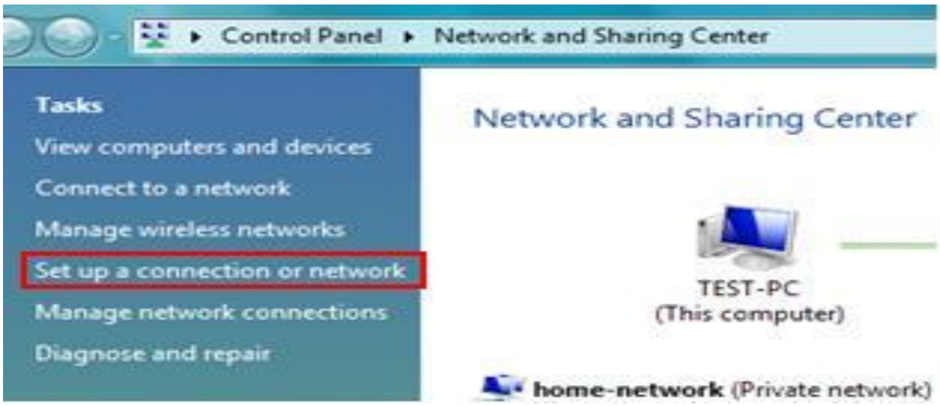
DNS Servers:

១-៨-៧- Host កុំព្យូទ័រ Configuration

នេះគឺជារបៀបនៃការ configure ad hoc wireless នៅលើ host កុំព្យូទ័រ។ ដូច្នេះកុំព្យូទ័រផ្សេងទៀតអាចភ្ជាប់ជាមួយវាតាម wireless ដោយផ្ទាល់ ។

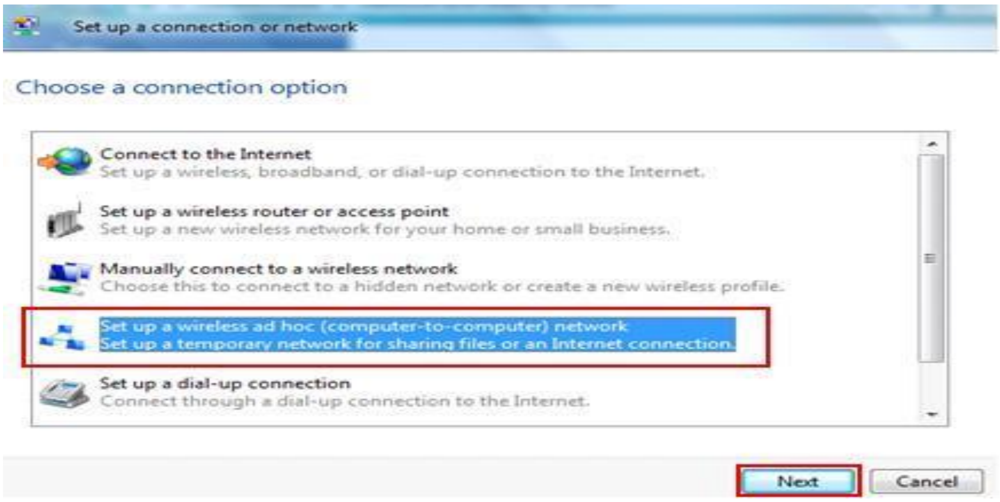
១- មក **Start** ហើយចុចដោយប្រើប៊ូតុងMouse ខាងស្តាំលើ **Network** ហើយបន្ទាប់មកចុចលើ **Properties.**

២- Network and Sharing Center window will appear, click on **Set up a connection or network. Note**: The other way to do it is by going to **Start -> Connect To -> click on Set up a connection or network.**

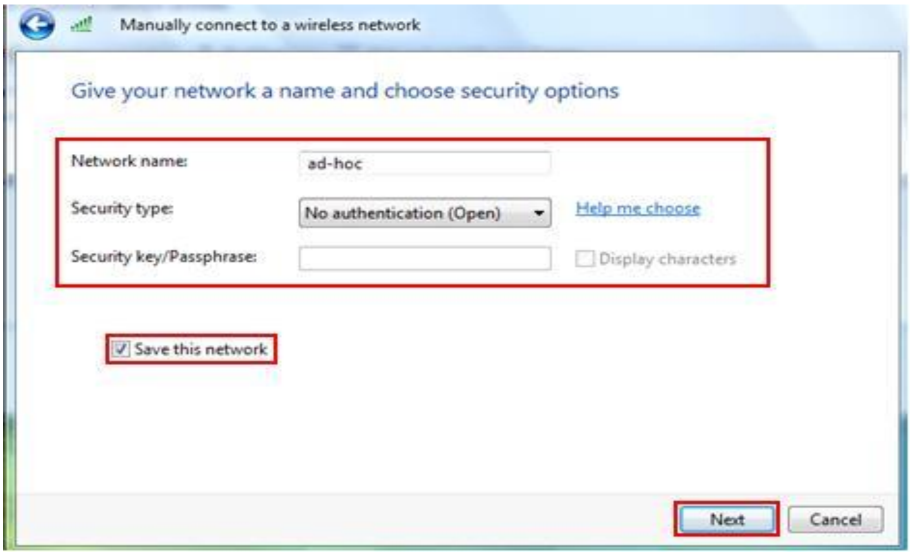


៣-Set up a connection or network window will appear, select **Set up a wireless ad hoc (កុំព្យូទ័រ-កុំព្យូទ័រ) network** option, then click **Next**

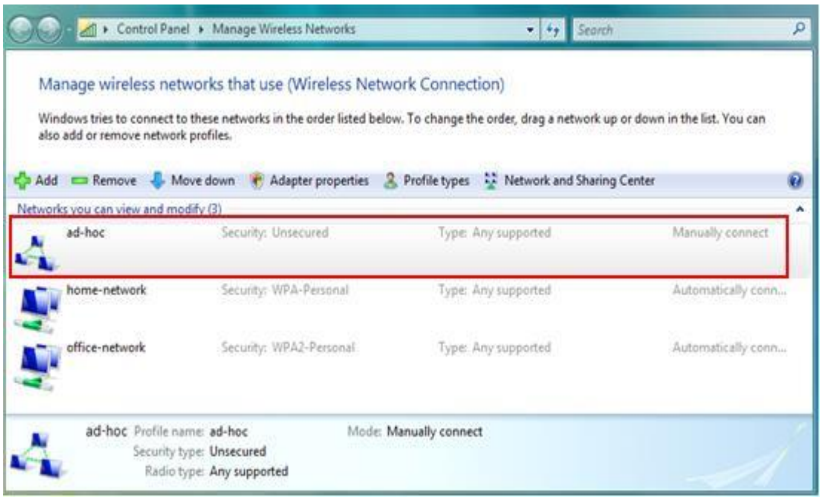
.



៤-បង្កើត wireless ad hoc network window មួយនិងបង្ហាញឡើងវានិងពន្យល់ឱ្យយើងដឹងពី ad hoc wireless network ។ ចុចលើ **Next** ក្រោយពីអានចប់ ។
៥-នៅលើផ្ទាំង wireless network configuration window អ្នកអាចវាយបញ្ចូលឈ្មោះរបស់ network name (SSID), security type (encryption) និង security keyអ្នកក៏អាចបង្កើត ad hoc connection ដោយមិនចាំបាច់ត្រូវការ authentication ក៏បានដែរហើយបន្ទាប់មកអាចបើក encryption (WEP,WPA2, etc) នៅពេលវាដំណើរការ។ សូមកុំភ្លេចបើក encryption ក្នុងករណីដែលគ្មានកុំព្យូទ័រនៅក្បែរនោះអាចភ្ជាប់ជាមួយ Network នេះ ។ ចុចលើ **Next** ម្តងទៀត ។
ចំណាំ: អ្នកអាចចុចលើ **Save network** ដើម្បី save វាជា wireless network profile ។ បើមិនបាន Save វាទេអ្នកនិងត្រូវបង្កើតវាម្តងទៀតនៅពេលអ្នកត្រូវការវា ។



៦- ផ្ទាំង window បន្ទាប់នឹងប្រាប់អ្នកអំពី ad hoc network ត្រូវបានរួចរាល់សម្រាប់ប្រើ ចុចលើ **Close** ដើម្បីបញ្ចប់ការ setup ។
៧-ត្រឡប់មក Network and Sharing Center ហើយចុចលើ **Manage Wireless networks**,អ្នកនិងឃើញ ad-hoc network ដែលទើបបង្កើតថ្មីនិងវាបានភ្ជាប់រួចជាស្រេច ។



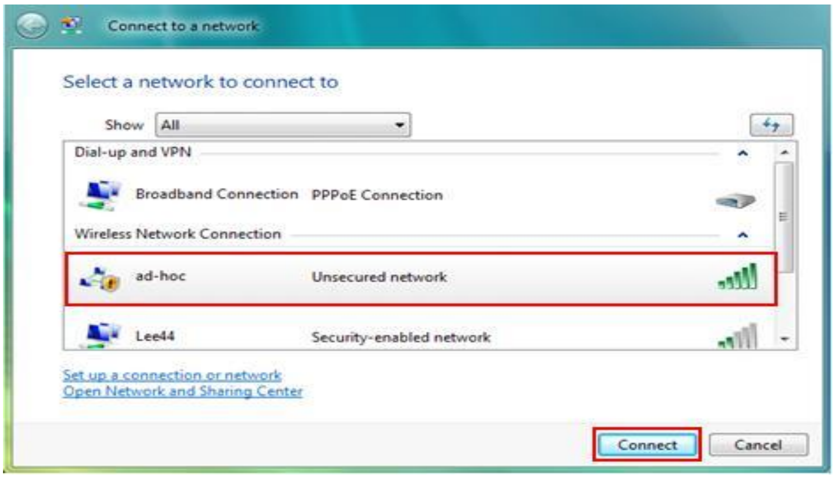
ចំណាំ:សូមចំណាំថា ad-hoc នេះគឺជា **Unsecured**ពីព្រោះវាគ្មាន encryption ត្រូវបានបើកនោះទេ។ ដូច្នេះកុំភ្លេចបើក encryption នៅពេលវាបានដំណើរការភ្លាម ។

១-៨-៨- Client កុំព្យូទ័រ Configuration:

បន្ទាប់មកអ្នកអាចប្រើ client កុំព្យូទ័រ ផ្សេងដើម្បីភ្ជាប់ជាមួយ ad hoc wireless network

1) ចុចលើ **Start** ហើយបន្ទាប់មកចុចលើ **Connect to.**

2) Connect to a network window និងបង្ហាញឡើង។ ផ្ទាំង window នេះនិងបង្ហាញពីការភ្ជាប់ដែលមានបំរុងទុកជាស្រេចគឺ dial-up, VPN និង wireless ប៉ុន្តែអ្វីដែលយើងចាប់អារម្មណ៍គឺ ad hoc wireless



ចំណាំ: វានិងសួរអ្នកបើអ្នកភ្ជាប់មកកាន់ wireless network ដែលគ្មានសុវត្ថិភាពហើយចុចលើ **Connect Anyway** ដើម្បីភ្ជាប់។

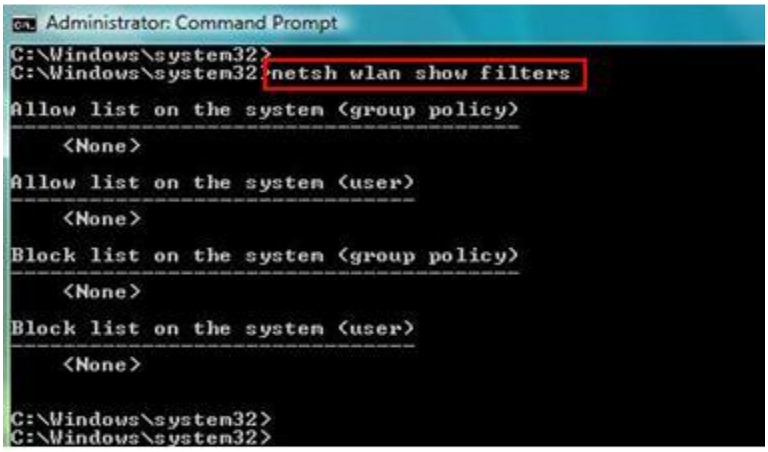
3) នៅពេលដែលបានភ្ជាប់ភ្លាម អ្នកនិងឃើញវាបង្ហាញ message ។ អ្នកអាចចុចលើ **Save this network** ហើយបន្ទាប់មកចុចលើ Close the window ។ បន្ទាប់មកអ្នកអាចធ្វើការ test ដោយប្រើបញ្ជា Ping ។

១-៨-៩- របៀបការពារ Vista ពីការភ្ជាប់ជាមួយ Ad Hoc Wireless Network

នេះគឺជាជំហានដ៏ខ្លីបំផុតសម្រាប់ប្រោះ ad hoc wireless network ពីការភ្ជាប់:

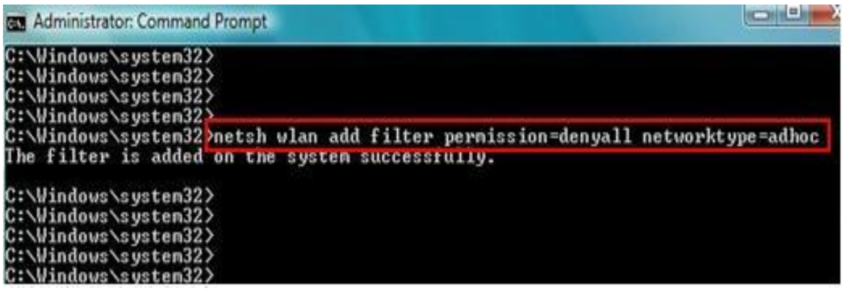
1) Go to **Start -> All Programs -> Accessories** -> then right click on **Command Prompt (cmd.exe)** and click **Run as administrator.**

2) Command prompt window will និងបើកបង្ហាញឡើងហើយបន្ទាប់មកវាយបញ្ជា **netsh wlan show filters** ហើយចុចលើ **Enter** button ដើម្បីបង្ហាញពី wireless filter setting ដែលមាននៅលើកុំព្យូទ័រនេះ។



3) អ្នកអាចវាយបញ្ជា **netsh wlan add filter permission=denyall networktype=adhoc** ដើម្បីបិទ Ad hoc network ពីការភ្ជាប់ ។

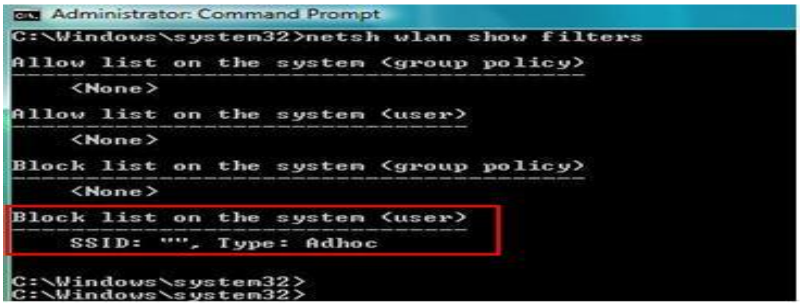
ចំណាំថាបើអ្នកឃើញ **Error: function WlanSetFilterList returns 5. The reques-ted operation requires elevation.** ក្រោយពីការប្រើបញ្ជាខាងលើ ។ អ្នកមិនអាចដំណើរការបញ្ជានេះបានទេពីព្រោះថាវាជាបញ្ជារបស់ administrator ។



4) បើអ្នកវាយបញ្ជា **netsh wlan show filters** ម្តងទៀតនោះអ្នកនិងឃើញវាដែលអ្នកបានកំណត់ឱ្យ។ អ្នកបានធ្វើវា កុំព្យូទ័រនឹងមិនភ្ជាប់ជាមួយ ad hoc wireless network ណាមួយនោះទេ

ចំណាំ:

អ្នកអាចវាយបញ្ជា **netsh wlan delete filter permission=denyall networktype=adhoc** ដើម្បីលុបការប្រោះនេះក្នុងករណីអ្នកប្រាកដជាត្រូវការភ្ជាប់ជាមួយ ad hoc wireless network



១-៨-១០- របៀបកំណត់ IP Address និងព័ត៌មានអំពី Network បន្ថែមទៀតក្នុង Windows XP

នេះគឺជាការណែនាំតាមជំហានៗនៃការកំណត់ IP address និងព័ត៌មានអំពី network បន្ថែមទៀត

2) Go to **Start** and click on **Control Panel.**

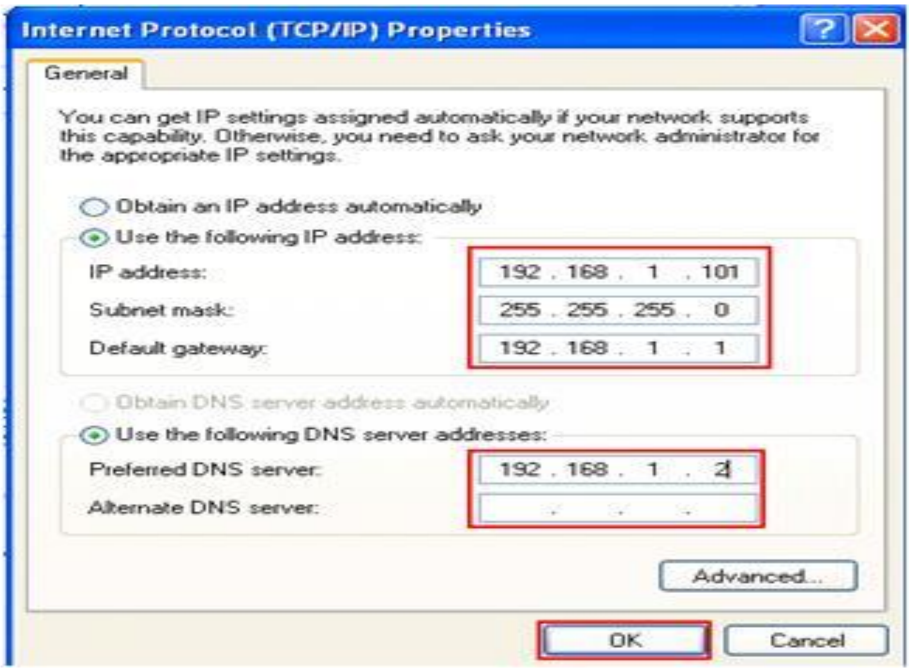
3) Control Panel window will appear. Double click on **Network Connections.**

4) Network Connections window will appear. Right click correct **Local Area Connection** by identifying correct network card and click **Properties.**

5) Select **Internet Protocol (TCP/IP).** Click on **Properties.**

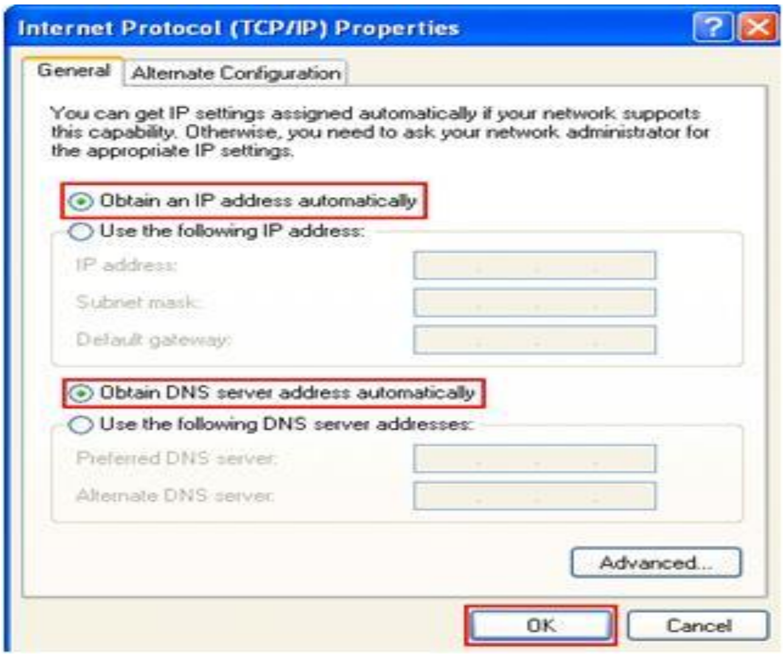
១-៨-១១- ការកំណត់ IP Address ដោយ Network Administrator

ចំណាំ: IP address របស់កុំព្យូទ័រត្រូវមានតែមួយគត់។ Default gateway គឺជា router មួយដែលអាច route traffic ឱ្យ network ផ្សេងទៀតឬ Internet។ DNS server គឺជា application server មួយដែលអាចបកប្រែ URL ឱ្យត្រូវជាមួយ IP address។ ឧទាហរណ៍ www.cert.org គឺជា URL ហើយវាត្រូវបានបំប្លែងឱ្យត្រូវជាមួយ 192.88.209.6 ដោយ DNS server ។



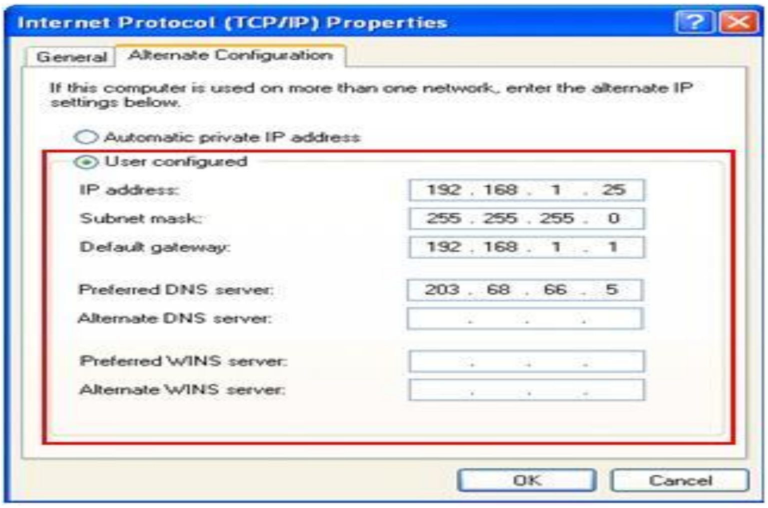
១-៨-១២- ការកំណត់ IP address តាមរយៈ DHCP server

បើអ្នកមាន DHCP server ដែលបាន setup នៅលើ router ឬអ្នកមាន DHCP server ក្នុង Home network កុំព្យូទ័ររបស់អ្នកអាចទទួលបាននូវ IP address ជាស្វ័យប្រវត្តដោយការជ្រើសរើសយក **Obtain an IP address automatically** និង **Obtain DNS server address automatically** ។



ចំណាំថាបើអ្នកមាន notebookមួយដែលកំពុងប្រើ static IP នៅឯផ្ទះហើយ IP ត្រូវបានកំណត់ឱ្យដោយ DHCP server នៅឯការិយាល័យ អ្នកអាចប្រើ **alternate configuration** ដើម្បីកំណត់ IP និងព័ត៌មានអំពី network សម្រាប់ network ពីរផ្សេងគ្នា ។

ដើម្បីទទួលបាន IP address ជាស្វ័យប្រវត្តគឺនៅលើ **General** tab ដូចយើងបានកំណត់ខាងដើម ។ ដូច្នេះ notebook និងត្រូវបានកំណត់ IP addresses ឱ្យជាស្វ័យប្រវត្តនៅឯការិយាល័យ។ ក្រោយពីនោះមកចុចលើ **Alternate Configuration** tab, ជ្រើសរើសយក **User configured** option និង key ក្នុង home network's static IP information ។



សំណួរត្រួតពិនិត្យ

១-ដូចម្ដេចហៅថា Wirelesss LAN ?

២-តើ Wireless LAN មានគុណសម្បត្តិនិងគុណវិបត្តិអ្វីខ្លះ ?

៣-ចូរបិទ Ad-hoc network

៤-ចូរបង្ហាញពីរបៀបបើក Ad-hoc network

៥-តើគេអាចសំគាល់ដឹងថា កុំព្យូទ័រ មាន Ad-hoc ឬ Acccess point Connection បានដោយសំគាល់លើអ្វី ?

៦-តើ Wireless Router មានតួនាទីជាអ្វីខ្លះ ?

៧-តើ Accesss Point មួយអាចភ្ជាប់បានចម្ងាយប៉ុន្មានម៉ែត្រ ?

១-៩- ការណែនាំពីរបៀបប្រើខ្សែ

ដើម្បីគូសខ្សែគេត្រូវអនុវត្តតាមវិធីសាស្ត្រដូចខាងក្រោមៈ

- គេត្រូវប្រើខ្សែឱ្យបានច្រើនជាងចំនួនខ្សែដែលអ្នកត្រូវការវាពិតប្រាកដ
- យើងត្រូវការធ្វើតេស្តទៅលើខ្សែដែលយើងបានតវារួចហើយ
- ត្រូវដាក់វាឱ្យឆ្ងាយពីអំពូលភ្លើងនឹងប្រភពនសញ្ញាលដែលជា Noise
- បើសិនជាក្នុងករណីដែលយើងត្រូវការអូសតាមជាន់នៃអាគារ
    - យើងត្រូវដាក់សំបកឱ្យវាដើម្បីការពារចំពោះ Noise signal
- យើងត្រូវដាកស្លាកសញ្ញាសម្គាល់ឱ្យវាហើយត្រូវចងវាជាដុំដើម្បីដាក់នៅទីតាំងជាមួយគ្នា

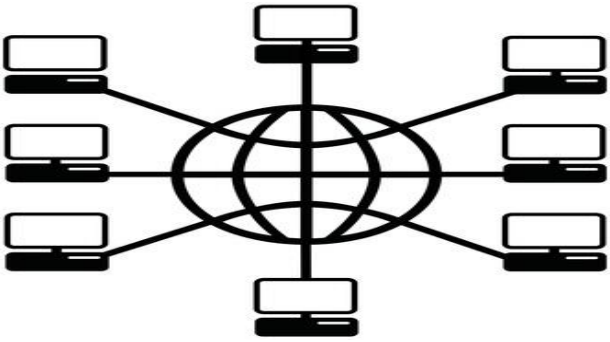
១-១០- តើ Topology ជាអ្វី ?

រូបសណ្ឋាននៃ network គឺសំដៅទៅលើការតខ្សែកុំព្យូទ័រនិង Pheriherals ផ្សេងៗទៀត។ រូបរាង (Topplogy)មិនអាចច្រឡំជាមួយ Logical topology ដែលជាវិធីសាស្ត្រនៃការបញ្ជូនព័ត៌មានរវាង Work - stations ។ Logical topology ត្រូវពិភក្សាជាមួយ Protocol ។

ប្រភេទនៃ Physical Topology សំខាន់ៗ

ផ្នែកចខាងក្រោមនេះពិភាក្សាទៅលើរូបរាងដែលត្រូវបានប្រើនៅក្នុង Network នឹងអ្វីៗផ្សេងៗទៀតដែលទាក់ទង

- Linear Bus
- Star
- Star-wired Ring



កុំព្យូទ័រ network មួយ (local area network ឬ wide area network) ដែលជាបន្សំនៃកុំព្យូទ័រ ខ្សែនិង peripherals ផ្សេងៗទៀតដែលមានគោលបំណងសម្រាប់ចែកចាយ ទិន្នន័យ និង/ឬ resource គ្រោងឆ្អឹងនៃ network មួយគេហៅថាជា topology របស់វា។ វាមាន physical topologies ជាច្រើនប្រភេទដែលប្រភេទនីមួយៗមានគុណសម្បត្តិនិងគុណវិបត្តិរបស់វា។

១-១១- ងាយស្រួលដំឡើង មើលថែទាំនិងដោះស្រាយបញ្ហានៅពេលជួបបញ្ហា

វាមានលក្ខណៈងាយស្រួលក្នុងការបន្ថែម workstationsនិង peripherals ក្នុង star-wired ring topology។ ពីព្រោះថាគ្រប់ nodes ទាំងអស់ត្រូវបានភ្ជាប់ជាមួយ central hub ដោយផ្ទាល់ហើយគ្មានការជ្រៀតជ្រៀកពីគ្នាទៅវិញទៅមកចំពោះការបន្ថែមឬការដក Node ណាមួយក្នុងប្រព័ន្ធ network។

១-១២- ងាយស្រួលប្រើខ្សែ

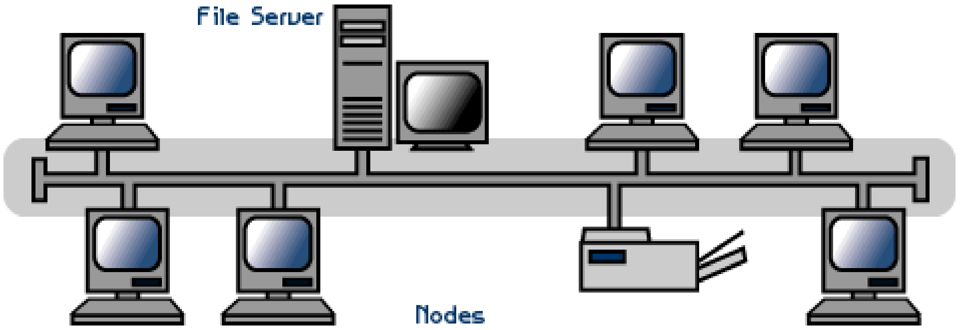
star-wired ring network មានសមត្ថភាពអាចភ្ជាប់ជាមួយខ្សែជាច្រើនប្រភេទ។ គេអាចប្រើខ្សែដូចជា fiber optic cabling, shielded twisted pair (STP) cables និង unshielded twisted pair (UTP)។ ប្រភេទនៃខ្សែដែលយកមកប្រើអាស្រ័យលើទំហំរបស់ network និងតម្រូវការចាំបាច់ ។

១-១៣- វាបានផ្តល់ឱ្យនូវ Fault Tolerance និងទំនុកចិត្តខ្ពស់

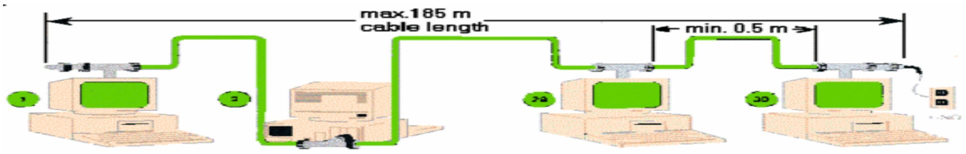
star-wired ring topology ផ្តល់ឱ្យនូវទិន្នន័យ fault tolerance ដ៏មានប្រសិទ្ធភាពខ្ពស់ជាង topology Broadcast data ត្រូវបានទទួលបកប្រែនិងបញ្ជូនបន្តឱ្យHub កណ្តាល។ access point នីមួយៗនៅលើ network គ្មានលក្ខណៈជា forwarding node (repeater) ដែលជាហេតុធ្វើឱ្យ មាន Error ក្នុងការបញ្ជូនទិន្នន័យ។ ក្រោយពីទិន្នន័យត្រូវបានទទួលនិងបកប្រែដោយ hub វាក៏បញ្ជូនបន្តឱ្យ Node បន្ទាប់នៅលើ network ហើយបន្ទាប់មកវាដំណើរការ។ បើ node មួយខូចឬខ្សែខូច hub និង forwards ទិន្នន័យឱ្យ Node បន្ទាប់ជាស្វ័យប្រវត្ត។ មានន័យថាវាបង្កើនទំនុកចិត្តឱ្យប្រព័ន្ធ Network ដើម្បីធានាថាការបញ្ជូនទិន្នន័យមិនត្រូវបានប៉ះពាល់ឡើយ ។

១-១៤- Linear Bus

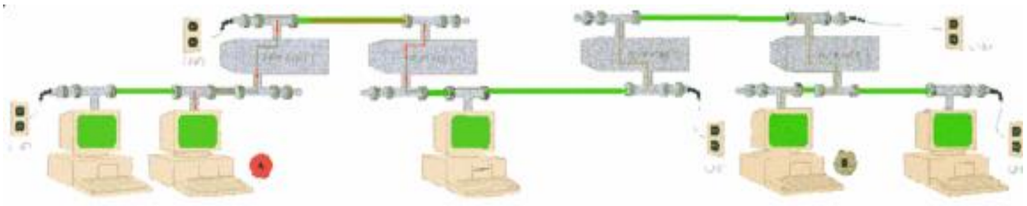
Linear bus topology រួមមានខ្សែមេមួយភ្ជាប់ជាមួយ terminator គ្រប់នៅចុងទាំងសងខាង។ គ្រប់ Node ទាំងអស់(Fileserver,Workstation និង Pheriperals)ត្រូវតែភ្ជាប់ទៅនឹង Linear cable។ Ethernet នឹង LocalTalk network ប្រើ Linear bus topology ។



ការភ្ជាប់ដោយប្រើ 10 base 2



ការភ្ជាប់ដោយប្រើ 10 base 5



គុណសម្បត្តិនៃ Linear Bus Topology

- ងាយស្រួលក្នុងភ្ជាប់កុំព្យូទ័រឬ Peripherals ទៅនឹង Linear Bus
    - ត្រូវការប្រវែងខ្សែតិចជាង Star topology

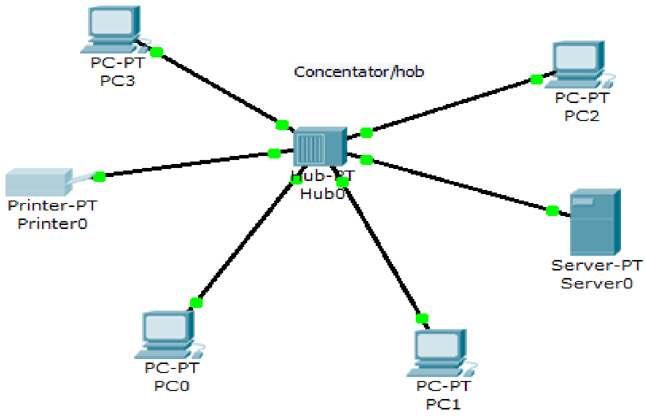
គុណវិបត្តិនៃ Linear Bus Topology

- ប្រព័ន្ធទាំងមូលខូច បើខ្សែរមេខូច
- Terminator ត្រូវការសម្រាប់សងខាងទាំងពីរនៃខ្សែរមេ
- ពិបាកេកបញ្ហាប្រសិនបើប្រព័ន្ធ Network ទាំងមូល
    - មិនមែនមានន័យថាវាត្រូវបានប្រើជាជំនណោះស្រាយនៅក្នុងអាគារដែលមានទំហំធំនោះទេ

១-១៥- Star

Star topology ត្រូវបានរៀបចំឡើងជាមួយគ្រប់ Nodes (Fileserver,Workstation និង peripherals) ដើម្បីភ្ជាប់ផ្ទាល់ទៅកាន់ Hub/Switch ឬ Concentator ដែលជាចំណុចកណ្តាល។

ទិន្នន័យនៅលើ Star network ត្រូវបានបញ្ជូនឆ្លងកាត់តាម Hub ឬ Concentrator មុនពេលបញ្ជូនបន្តទៅកាន់គោលដៅរបស់វា។ ការ Configure នេះជាទូទៅត្រូវបានប្រើជាមួយខ្សែ UTP ថ្វីបើវាអាចប្រើជាមួយ Caoxial ឬ Fiber optic ក៏ដោយ។



គុណសម្បត្តិនៃ Star Topology

- ងាយស្រួលក្នុងការដំឡើងនឹងតភ្ជាប់
    - គ្មានការបង្អាក់ចំពោះ Network បន្ទាប់ពីការភ្ជាប់ឬការដកយកឧបករណ៍ចេញនោះទេ
    - ងាយស្រួលក្នុងការស្វែងរកកំហុសនិងដោះស្រាយយកផ្នែកណាមួយចេញ

គុណវិបត្តិនៃ Star Topology

- ត្រូវការខ្សែច្រើនជាង Linear Bus topology
- ប្រសិនបើ Hub ឬ Concentrator ខូច នោះ Node ដែលបានភ្ជាប់គឺមិនអាចប្រើប្រាស់បាននោះទេ
- មានតម្លៃថ្លៃជា Linear Bus ពីព្រោះតម្លៃនៃ Concentrator ថ្លៃ

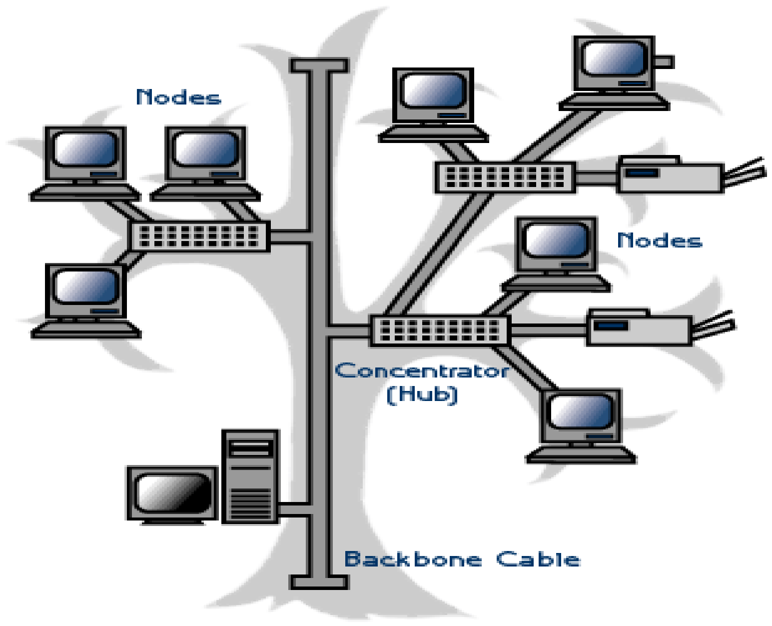
Protocols ត្រូវបានប្រើជាមួយ Star ឬ Ethernet ឬ localTalk។ Token ត្រូវបានគេប្រើជាមួយ Topology ដែលគេហៅថា Star-Wired Ring ។

១-១៦- Star-Wired Ring

Star-wired ring topology អាចលេចឡើងមានរាងដូចជា Star topology ដែរ។ MAU (Multistation Access Unit) នៃ Star-Wired Ring មានខ្សែដែលអនុញ្ញាតឱ្យព័ត៌មានឆ្លងកាត់ពីឧបករណ៍មួយទៅឧបករ ណ៍មួយទៀតនៅក្នុងរង្វង់។ Token Ring protocol ប្រើ Star-Wired Ring ។

១-១៧- Tree

Tree topology មានលក្ខណៈបញ្ចូលគ្នានៃ Linear Bus និង Star topology ។ វារួមមានក្រុមនៃ Star Workstation ភ្ជាប់ទៅនឹង Linear Bus backbone ។ Tree Topology អនុញ្ញាតឱ្យអាចពង្រីក Network ដែលមានស្រាប់និងអាចឱ្យគេ Configure ចំពោះ network ទៅតាមតម្រូវការរបស់គេ។



គុណសម្បត្តិនៃ Topology

- សម្រាប់ភ្ជាប់ពីចំណុចមួយទៅចំណុចមួយទៀតសម្រាប់ Segment នីមួយៗ

- មានការគាំទ្រដោយ Hardware នឹង Sofware ខ្លះ

គុណវិបត្តិនៃ Tree topology

- ប្រវែងនៃខ្សែនៃគ្រប់ Segment ត្រូវបានកំណត់ដោយប្រភេទនៃខ្សែដែលបានប្រើ
    - ប្រសិនបើខ្សែ Backbone ខូច នោះ Segment ទាំងមូលនិងខូចដែរ
    - ពិបាកក្នុងការ Configure និងតខ្សែជាង topology ផ្សេងៗទៀត

១-១៨- ច្បាប់ 5-4-3

គួរពិចារណាក្នុងការដំឡើងនៃ Tree topology ដោយប្រើ Ethernet Protocol គឺច្បាប់៥-៤-៣។ ទិដ្ឋភាពមួយនៃតម្រូវការ Ethernet protocol គឺសញ្ញាលបានបញ្ជូនចេញទៅក្រៅតាមខ្សែ network ទៅដល់គ្រប់ផ្នែកនៃ Nerwork ជាមួយរយៈពេលច្បាស់លាស។ គ្រប់ Concentrator ឬ Repeater ដែលសញ្ញាលឆ្លងកាត់ត្រូវបន្ថែមចំនួននៃពេលវេលាតូចមួយ។ នេះគឺជាគោលការណ៍កំណត់រវាង node ពីរនៅលើ Network ដែលមានប្រវែងត្រឹម៥កង់ដែលអាចភ្ជាប់បាន 4 repeaters/Concentrator ។ បន្ថែម៣កង់ទៀតអាចធ្វើឱ្យប្រើប្រាស់ភ្ជាប់ Workstation ដើមប្រសិនបើវាត្រូវបានប្រើជាមួយខ្សែ Coaxial ។

Segment ដើមគឺជា Segment មួយដែល node ពីរឬច្រើនភ្ជាប់ជាមួយវា។ Node ពីរដែលនៅឆ្ងាយនៅលើ network មាន 4 segments និង 3 repeater/concentrator រវាងពួកវា។

នេះគឺជាច្បាប់ដែលមិនអាចអនុវត្តបានចំពោះ network protocol ផ្សេងទៀតឬ Ethernet network ដែលគ្រប់ Fiber Optic ឬបន្សំនៃ Fiber backbone ជាមួយខ្សែ UTP ។ ប្រសិនបើបន្សំនៃមេ Fiber optic និងខ្សែ UTP ត្រូវប្រើច្បាប់ ៧-៦-៥។

គួរពិចារណានៅពេលជ្រើសរើសយក Topology

- Linear Bus network អាចមានតម្លៃថោក។ វិធីនៃការដំឡើង network មិនចាំបាច់ទិញ Concentrator នោះទេ
- ប្រវែងនៃខ្សែដែលត្រូវការសម្រាប់ network គឺប្រើប្រវែងខ្សែខ្លី
- ប្រភេទនៃខ្សែៈភាគច្រើនគេប្រើ UTP ដែលត្រូវបានគេប្រើជាមួយ Star

តារាងសង្ខេប

Physical Topology	Common Cable	Common Protocol
Linear Bus	Twisted Pair Coaxial Fiber	Ethernet LocalTalk
Star	Twisted Pair Fiber	Ethernet LocalTalk
Star-Wired Ring	Twisted Pair	Token Ring
Tree	Twisted Pair Coaxial Fiber	Ethernet

១-១៩- តើ Network Operationg System ជាអ្វី?

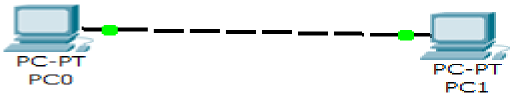
វាមិនដូចទៅនិងប្រព័ន្ធប្រតិបត្តិការដូចជា DOS និង Windows នោះទេដែលត្រូវបានដំឡើងដោយអ្នកប្រើប្រាស់តែម្នាក់គត់ដើម្បីគ្រប់គ្រងទៅលើកុំព្យូទ័រមួយ។ ប្រព័ន្ធប្រតិបត្តិការ network ធ្វើសកម្មភាពជា មួយកុំព្យូទ័រជាច្រើនដែលឆ្លងកាត់ប្រព័ន្ធ network ។ ប្រព័ន្ធប្រតិបត្តិការ network ដើរតួនាទីជាប្រធាននៃដំណើរការរបស់ network ឱ្យបានស្រួល។ ប្រភេទនៃប្រព័ន្ធប្រតិបត្តិការ network គឺៈ

- Peer-to-Peer
- Client/Server

១-១៩-១- Peer-to-Peer

Peer-to-Peer network operating system អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាចចែកចាយធនធាននិង files ដែលស្ថិតនៅលើកុំព្យូទ័រដើម្បីដំណើរការចំពោះធនធាន ដែលបានចែកចាយឱ្យបានឃើញនៅលើកុំព្យូ ទ័រផ្សេងៗទៀត។ ទោះបីជាយ៉ាងណាក៏ដោយវាគ្មាន Fileserver ឬប្រភពកណ្តាលដើម្បីគ្រប់គ្រង នៅក្នុង Peer-to-Peer network គឺគ្រប់កុំព្យូទ័រទាំងអស់ត្រូវបានចាត់ទុកស្មើៗគ្នា។ វាមានសិទ្ធស្មើគ្នាចំពោះការប្រើប្រាស់ធនធានដែលមានស្រាប់នៅលើ network។ Peer-to-Peer network ត្រូវបានគេបង្កើតឡើងប្រើប្រាស់ភាគច្រើននៃ LAN ដែលមានទំហំតូច Appeshare និង Windows សម្រាប់workgroup គឺជាឧទាហរណ៍នៃកម្មវិធីដែលអាចដើរតួនាទីជា peer-to-peer network operating system។

Peer-to-Peer Network



គុណសម្បត្តិនៃ Peer-to-Peer network

- ចំណាយទុនតិចដោយមិនចាំបាច់ទិញ Server
- Windows ដូចជា Windows XP, Windows 8, Windows 10 ត្រូវបាន Configure ជាស្រេចសម្រាប់ Peer-to-Peer network

គុណវិបត្តិនៃ Peer-to-Peer network

- គ្មានកន្លែងកណ្តាលសម្រាប់ Files និង applications
- គ្មានសុវត្ថិភាព

១-១៩-២- Client/Server

DELL

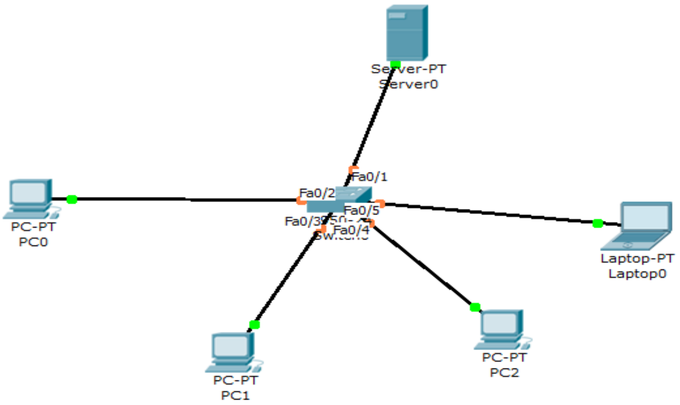
DELL

Blade Servers

Rack system

អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាចគ្រប់គ្រងទៅលើ applications ដែលស្ថិតនៅលើ Fileserver ។ ដូច្នេះ Fileserver គឺជាកុំព្យូទ័រដ៏សំខាន់មួយនៅក្នុងប្រព័ន្ធ network ពីព្រោះថាវាអនុញ្ញាតឱ្យយើងអាចប្រើប្រាស់បាននូវធនធាននិងផ្តល់នូវសុវត្ថិភាព។

Workstation ឬ client នីមួយៗអាចប្រើប្រាស់នូវធនធានទាំងអស់ដែលមាននៅលើ Fileserver ។ ប្រព័ន្ធប្រតិបត្តិការ network អនុញ្ញាតឱ្យយើងបញ្ចូលនូវសមាសធាតុទាំងអស់បញ្ចូលគ្នាហើយអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាចចែកចាយនូវធនធាននៅពេលព្រមគ្នាបាន។ Novell Netware នឹង Window 2000 server /2008/2012 /2016 គឺជាប្រព័ន្ធប្រតិបត្តិការនៃប្រព័ន្ធកូន-មេនៃប្រព័ន្ធ network ។



គុណសម្បត្តិនៃប្រព័ន្ធ network មេ-កូន

- Centralized: គ្រប់ធនធាននិងសុវត្ថិភាពនៃទិន្នន័យត្រូវបានគ្រប់គ្រងដោយម៉ាស៊ីនមេ។ មានន័យថាការប្រើប្រាស់នៃធនធានបានឬមិនបានអាស្រ័យទៅលើម៉ាស៊ីនមេជាអ្នកកំណត់ឱ្យ។
- Scalability: គ្រប់សមាសធាតុរបស់ network គេអាចជំនួសឬដោះដូរបានទៅតាមតម្រូវការនៃការកើនឡើង

- Flexibility: គេអាចបញ្ចូលបាននូវបច្ចេកវិទ្យាថ្មី
- Interoperability:គ្រប់សមាសធាតុទាំងអស់ត្រូវតែដំណើរការជាមួយគ្នាបាន
- Accessibility:គេអាចគ្រប់គ្រងទៅលើម៉ាស៊ីនមេតាម Platforms

គុណវិបត្តិនៃប្រព័ន្ធ network មេ-កូន

- ចំណាយទុនច្រើនដើម្បីទិញម៉ាស៊ីនមេ
- ការថែទាំៈចំពោះប្រព័ន្ធ network ធំត្រូវការបុគ្គលិកដែលមានជំនាញច្បាស់លាស់ដើម្បីធានាថា network មានប្រសិទ្ធភាពខ្ពស់។
- ភាពអាស្រ័យគ្នាៈបើម៉ាស៊ីនមេខូចឬមិនដំណើរការនោះប្រព័ន្ធ network ត្រូវបានគាំង

ឧទាហរណ៍នៃប្រព័ន្ធប្រតិបត្តិការ network មានដូចខាងក្រោមៈ

- AppleShare
- Microsoft Windows Server
- Novell Netware

សំណួរត្រួតពិនិត្យ

១-ចូរពន្យល់ច្បាប់ ៥-៤-៣ ?

២-ចូរពន្យល់ច្បាប់ ៧-៥-៦ ?

៣-តើ Peer to Peer network មានគុណសម្បត្តិនិងគុណវិបត្តិអ្វីខ្លះ ?

៤-តើ Client/Server network មានគុណសម្បត្តិនិងគុណវិបត្តិអ្វីខ្លះ ?

៥-តើ Network Operating System (NOS)មានអ្វីខ្លះ ?

ជំពូកទី២

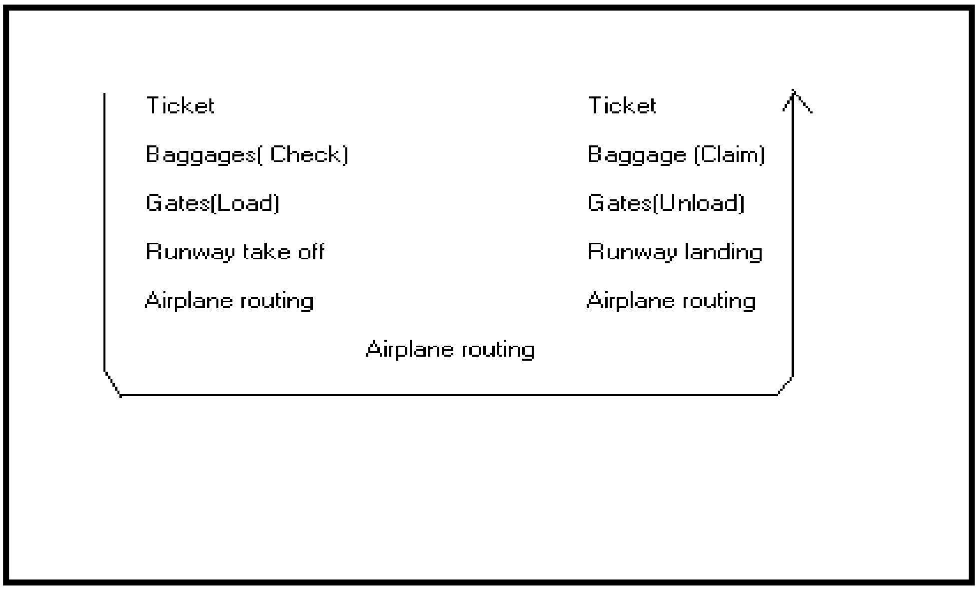
OSI Reference Model

២-១- ការរៀបចំ System តាមស្រទាប់

នៅពេលដែលយើងមានបំណងចង់បង្កើតនូវស្ថាបត្យកម្មនៃ Internet របស់យើងមួយគឺនៅពេលនោះយើងមានទំនាក់ទំនងជាមួយនឹងប្រព័ន្ធដែលមានលក្ខណៈសាំញ៉ាំគ្រប់ពេលវេលាទាំងអស់ក្នុងជីវិតប្រចាំថ្ងៃរបស់យើង។ ឧបមាថាប្រសិនបើនរណាម្នាក់ឱ្យអ្នកពិពណ៌នាពីអ្វីមួយ។

ឧទាហរណ៍

តើអ្នកអាចរកពិពណ៌នាអំពីរចនាសម្ព័ន្ធពីរបៀបណា ដើម្បីពិពណ៌នានៅក្នុងប្រព័ន្ធសាំញ៉ាំដែលមានដូចជាទីភ្នាក់ងារលក់សំបុត្រ អ្នកត្រួតពិនិត្យវ៉ាលី អ្នកត្រួតពិនិត្យច្រកចេញចូល អ្នកបើកបរយន្តហោះ ជើងយន្តហោះ អ្នកត្រួតពិនិត្យចរាចរណ៍ហើយនឹងប្រព័ន្ធពាសពេញពិភពលោកមួយសម្រាប់យន្តហោះហោះ ហើរ។មានវិធីមួយទៀតដើម្បីពិពណ៌នាអំពីប្រព័ន្ធនេះដែលអាចពិពណ៌នាពីសកម្មភាពទាំងអស់នេះតាមលំដាប់ដោយអ្នកយកសំបុត្រនៅពេលដែលអ្នកជិះនៅលើយន្តហោះ។ អ្នកអាចទិញសំបុត្រយន្តហោះរបស់អ្នក ត្រួតពិនិត្យលើឥវ៉ាន់របស់អ្នក ហើយទៅកន្លែងច្រកចេញចូលហើយបន្ទាប់មកនៅទីបំផុតយកសំបុត្រទៅដាក់នៅលើយន្តហោះ។ យន្តហោះក៏ចេញដំណើរទៅតាមគោលដៅរបស់វាដែលត្រូវទៅនោះ។ ក្រោយពេលដែលយន្តហោះបានមកដល់គោលដៅរបស់វាហើយនោះ អ្នកជិះក៏បានមកដល់ច្រកចេញចូលហើយបន្ទាប់មកទៀតត្រូវតែយកឥវ៉ាន់របស់ពួកគេ។



២-២- ISO-OSI Model

ស្រទាប់នីមួយៗនៃគំរូរបស់ OSI Reference មានតួនាទីច្បាស់លាស់។ ហើយតួនាទីនោះត្រូវបានកំណត់ ដោយ OSI ហើយក៏ត្រូវបានប្រើប្រាស់ដោយក្រុមហ៊ុនផលិតឧបករណ៍ network ។

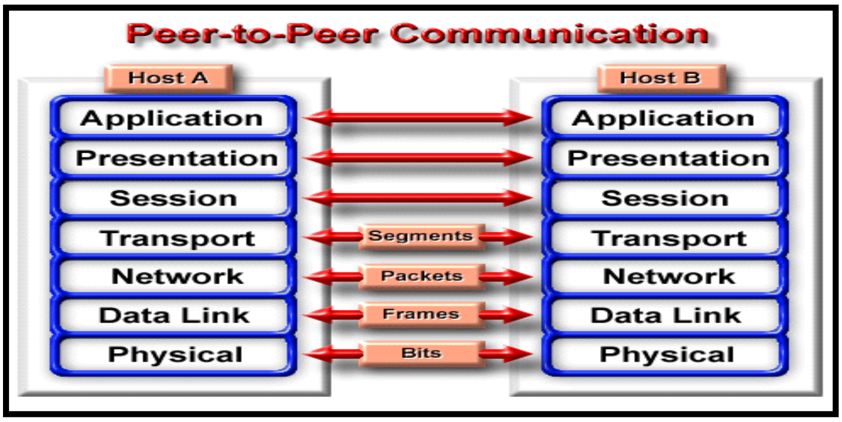
ស្រទាប់ទាំងនោះរួមមាន:

- Application layer គឺជាស្រទាប់មួយសម្រាប់ផ្តល់សេវា network ដល់អ្នកប្រើប្រាស់ application

ឧទាហរណ៍ Word Processor Application មួយត្រូវបានផ្ដល់នូវសេវាដោយប្រើ File Transfer Services នៅស្រទាប់នេះ។

- PresentationLayer:ស្រទាប់នេះបានផ្ដល់ឱ្យនូវការតំណាងឱ្យទិន្នន័យ ការរៀបចំទម្រង់ Code។ បើសិនទិន្នន័យដែលបានមកពី Network វាជានាថាអាចប្រើប្រាស់ដោយ Application ហើយគ្រប់ព័ត៌មានដែលបានបញ្ជូនដោយ Application អាចត្រូវបានបញ្ជូនតាមបណ្ដាញ network
- Session Layer: ស្រទាប់នេះមានតួនាទីជាអ្នកបង្កើតការភ្ជាប់ហើយរក្សាទុកនូវការភ្ជាប់និងគ្រប់គ្រងទៅលើ Session រវាង Application និង Appication
- Transport Layer:ការភ្ជាប់នេះមានតួនាទីចែកចាយនូវទិន្នន័យជាបំណែកតូចៗនិងប្រមូលផ្ដុំបំណែកទិន្នន័យនោះវិញដើម្បីទទួលបានជាចរន្តនៃទិន្នន័យ។ ការភ្ជាប់បែបនេះមាន Protocol មួយដែលមានឈ្មោះថា TC ដែលជា Conection Oriented Protocol ហើយត្រូវបានប្រើបប្រាស់ជា មួយ IP (Internet Protocol)
- Network Layer:ស្រទាប់នេះមានតួនាទីសម្រាប់កំណត់នូវផ្លូវបញ្ជូនដ៏ល្អបំផុតដើម្បីបញ្ជូននូវទិន្នន័យពីកន្លែងមួយទៅកន្លែងមួយទៀត។ នៅស្រទាប់នេះដែលមាន Protocol មួយដែលមានឈ្មោះថា IP (Internet Protocol)ដែលជា Connectionless
- Data Link Layer:Layer នេះរៀបចំទិន្នន័យទៅជា Frame ដើម្បីបញ្ជូនតាមខ្សែហើយវាមានតួនាទីទៅជាអ្នករកឱ្យឃើញពីកំហុសដែលកើតមានឡើង(error)ឱ្យដឹងពីប្រភេទនៃរូបរាងរបស់ Network និងការគ្រប់គ្រងនៃលំហូរព័ត៌មាន។ វាប្រើប្រាស់នូវ MAC address ។
- Physical Layer: ស្រទាប់នេះផ្ដល់នូវផ្នែកអេឡិចត្រិក មេកានិចនិងតួនាទី មានន័យថាវាមានតួនាទីសម្រាប់ភ្ជាប់រវាងប្រព័ន្ធនិងប្រព័ន្ធ។ នៅស្រទាប់នេះរួមមានដូចជាខ្សែ UTP នឹង Fiber Optic

២-៣- ការប្រាស្រ័យទាក់ទងខាង Layer ដែលមានតួនាទីស្មើគ្នា



Peer-to -Peer Communication

ស្រទាប់នីមួយៗដែលបានប្រើប្រាស់នូវ Layer Protocol របស់វាផ្ទាល់ដើម្បីភ្ជាប់ទំនាក់ទំនងជាមួយស្រទាប់ដែលមានតួនាទីស្មើគ្នារបស់វានៅក្នុងប្រព័ន្ធមួយផ្សេងទៀត។ Protocol របស់ស្រទាប់នីមួយៗបានធ្វើការបញ្ជូននូវព័ត៌មានរវាងគ្នាទៅវិញទៅមកដែលគេហៅថា Protocol Data Unit (PDUs) រវាងស្រទាប់ដែលមានតួនាទីស្មើគ្នា។ គេឱ្យស្រទាប់មួយអាចប្រើឈ្មោះពិតប្រាកដចំពោះ PDU របស់វា។

ឧទាហរណ៍

នៅក្នុង TCP/IP Transport Layer របស់ TCP ដែលមានទំនាក់ទំនងជាមួយតួនាទីរបស់ TCP ដែលមានតួនាទីស្មើគ្នាដោយប្រើប្រាស់ Segments ។

ការប្រាស្រ័យទាក់ទងរបស់ស្រទាប់ដែលមានតួនាទីស្មើគ្នាត្រូវបាមទទួលដោយប្រើស្រទាប់នីមួយៗហើយប្រើប្រាស់នូវសេវារបស់ស្រទាប់ដែលនៅខាងក្រោមវា។ ស្រទាប់នៅខាងក្រោមនស្រទាប់ដែលវាកំពុងស្ថិតនៅណាមួយផ្តល់ឱ្យនូវសេវារបស់វាទៅឱ្យស្រទាប់ដែលវាកំពុងស្ថិតនេះ។Layer Service ខាងក្រោមនីមួយៗទទួលយកព័ត៌មានពីស្រទាប់ខាងលើដែលជាផ្នែកមួយរបស់ Layer PDUs ខាងក្រោមហើយវាបានប្តូរជាមួយស្រទាប់ ដែលមានតួនាទីស្មើគ្នារបស់វា។ ដូច្នេះ TCP Segment បានក្លាយជាផ្នែកមួយនៃ Network Layer Packets(Data -gram) ប្តូររវាង IP ដែលមានតួនាទីស្មើគ្នា។ នៅពេលដែលវាបានបញ្ជូនត្រឡប់មកវិញនូវ IP Packets ត្រូវតែជាផ្នែកមួយរបស់ Data Link Frame ដែលបានប្តូរដោយផ្ទាល់រវាងឧបករណ៍ដែលបានភ្ជាប់គ្នា។ នៅទៅបំផុត Frame ទាំងអស់ត្រូវតែជា bits ទាំងអស់ដែលទិន្នន័យបានបញ្ជូនចុងក្រោយដោយ Physical Layer Protocol ដោយប្រើហាដវែរ។

២-៤- Data Encapsulation

ស្រទាប់នីមួយៗអាស្រ័យទៅលើតួនាទីរបស់សេវានៃគំរូ OSI reference ដែលស្ថិតនៅខាងក្រោមរបស់វា។ ដើម្បីផ្តល់នូវសេវានេះឱ្យបាន ស្រទាប់នៅក្រោមវាបានប្រើប្រាស់នូវ Encapsution ដើម្បីដាក់ PDU ចូលទៅក្នុងផ្នែក Data Field របស់វាដែលទទួលបានពីស្រទាប់ខាងលើហើយបន្ទាប់មកថែមនូវ Header និងនឹង Trailer ដើម្បីដំណើរការតាមតួនាទីរបស់វា។

ឧទាហរណ៍

Network Layer បានផ្តល់ឱ្យនូវសេវាមួយទៅឱ្យ Transport layer ហើយ Transport layer ក៏បានផ្តល់ឱ្យនូវទិន្នន័យនៅក្នុង Internetwork subsystem។ Network Layer មានតួនាទីសម្រាប់បញ្ជូននូវទិន្នន័យកាត់តាមប្រព័ន្ធ Internetwork។ វាបានបំពេញតួនាទីនេះដោយប្រើប្រាស់ encapsulation ទិន្នន័យដែលមានក្នុង packet។ Packet នេះរួមមាន Header ដែលមានព័ត៌មានដើម្បីបញ្ជូនដូចជា IP address របស់អ្នកបញ្ជូនឹងអ្នកទទួលហើយ data link layer ក៏បានផ្តល់ឱ្យនូវសេវាមួយទៅឱ្យ network layer វិញ។ វាបានធ្វើ encapsulate network layer នៅក្នុង frame។ frame Header មាននូវព័ត៌មានដែលត្រូវការចាំបាច់ដើម្បីបំពេញតួនាទីរបស់ data link។

ឧទាហរណ៍ frame header ដែលមាន Physical addresses។ នៅទីបំផុត Physical layer បានផ្តល់ឱ្យនូវសេវាមួយទៅឱ្យ datalink layer។ វាបានបញ្ជូនតាមខ្សែ។ ការ Encapsualion ចំពោះទិន្នន័យប្រព្រឹត្តទៅតាមដំណាក់កាលដូចតទៅះ

ជំហានទី១

នៅពេលដែលអ្នកប្រើប្រាស់ចាប់ផ្តើមបញ្ជូននូវសារ email មួយតួអក្សរនិងនិមិត្តសញ្ញាទាំងឡាយត្រូវបានបំប្លែងទៅជាទម្រង់មួយដែល Network អាចប្រើប្រាស់បានហៅថា Data ។

ជំហានទី២

នៅពេលដែលសារត្រូវបានរៀបចំសម្រាប់ធ្វើការបញ្ជូនឆ្លងកាត់តាមInternetwork នោះ Segment ត្រូវបានបញ្ជូនពីឧបករណ៍បញ្ជូននឹងទទួលទាំងសងខាង។

ជំហានទី៣

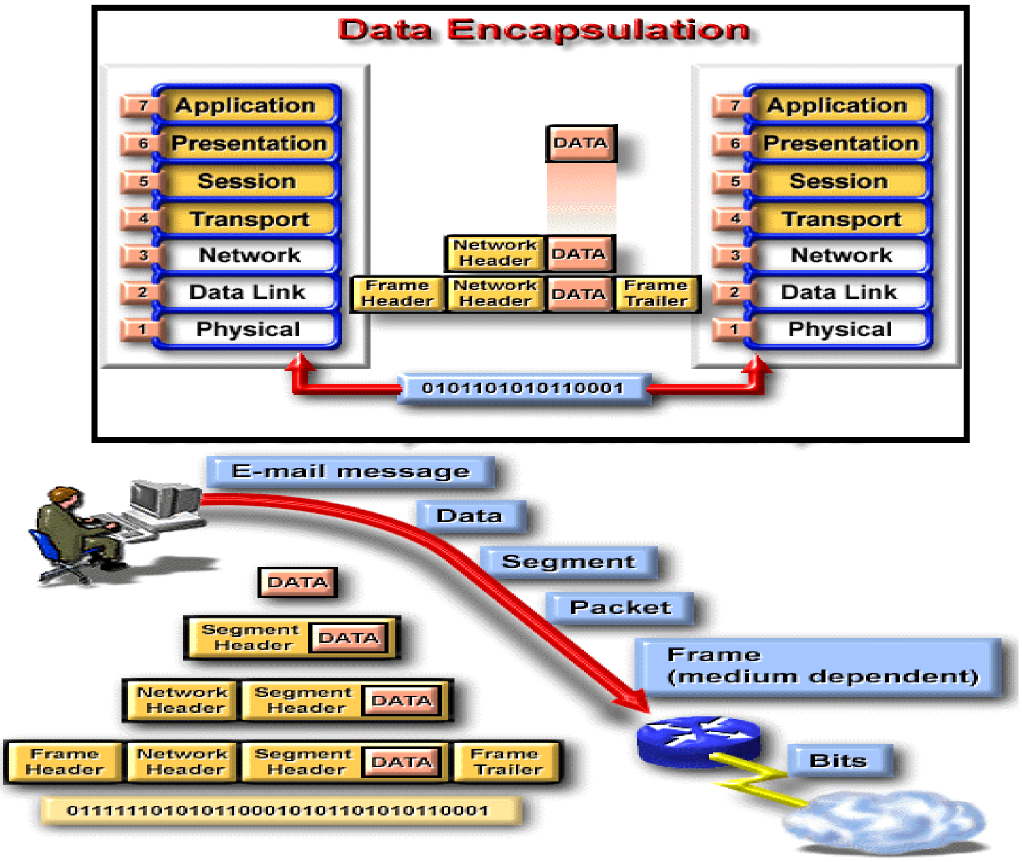
នៅជំហានបន្ទាប់ ទិន្នន័យត្រូវបានរៀបចំឡើងជា Packet ឬ Datagram ដែលភ្ជាប់មកជាមួយនូវ Network Header ដែលរួមមាន IP address របស់អ្នកបញ្ជូននិងអ្នកទទួល។ Network នេះអាចជួយដល់ឧបករណ៍របស់ Network ក្នុងការបញ្ជូនឆ្លងកាត់តាម Network នូវតាមផ្លូវដែលវាជ្រើសរើស។

ជំហានទី៤

ឧបករណ៍ Network នីមួយៗត្រូវតែរៀបចំ Packet ទៅជា Frame។ Frame អាចឱ្យយើងភ្ជាប់រវាងឧបករណ៍ដែលបានភ្ជាប់គ្នាដោយផ្ទាល់ទៅវិញទៅមកតាមខ្សែបណ្តាញ។ ឧបករណ៍នីមួយៗដែលស្ថិតនៅក្នុងផ្លូវបញ្ជូនដែលត្រូវបានកំណត់ជាស្រេចត្រូវការនូវ Frame នោះដើម្បីភ្ជាប់ទៅកាន់ឧបករណ៍ផ្សេងទៀត។

ជំហានទី៥

នៅក្នុងដំណាក់កាលចុងក្រោយនេះដែល Frame ត្រូវបានបំប្លែងទៅជា Bits សម្រាប់ធ្វើការបញ្ជូនឆ្លងកាត់តាមបណ្តាញដែលនិច្ចកាលគឺជាខ្សែ UTP។ នៅក្នុងការត្រឡប់មកវិញដើម្បីផ្តល់សេវាទៅឱ្យ Network Layer ។ វាជា Encapsulation Network Layer Packet នៅក្នុង frame ។ ព័ត៌មានរបស់ Frame ដើម្បីបំពេញតួនាទីឱ្យ Data Link ។



៥- Application Layer

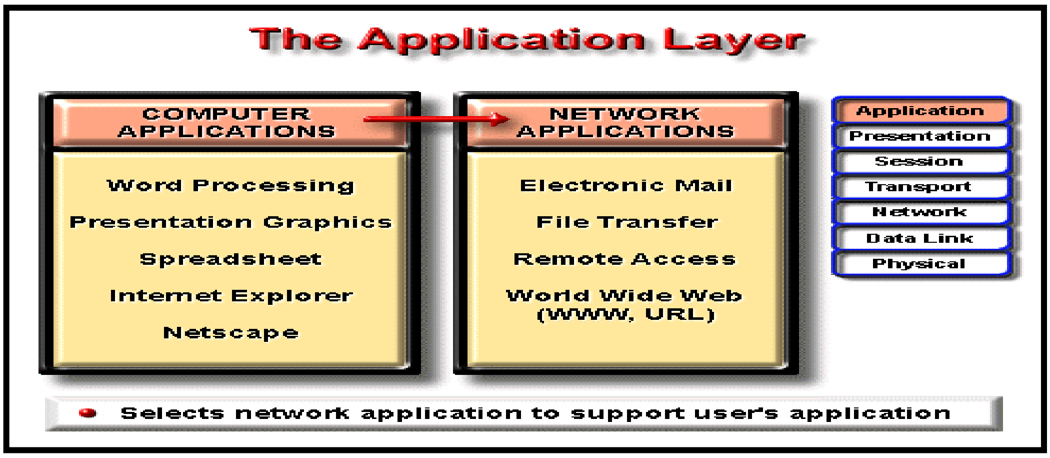
នៅក្នុងបរិបទនៃគំរូនៃ OSI reference និង Application Layer គឺស្រទាប់ទី៧របស់ OSI referece Model ហើយគាំទ្រ សមាសធាតុផ្សំរបស់ Application។ កុំព្យូទ័រ Application ត្រូវការត្រឹមព័ត៌មានដែលស្ថិតនៅលើកុំព្យូទ័ររបស់វា។ ទោះបីជាយ៉ាងណាក៏ដោយ Application មួយអាចមានសមាសធាតុការប្រាស្រ័យទាក់ទងមួយ ឬច្រើនពី Network Application។

ប្រភេទនៃ Network Application ដែលត្រូវបានគេបង្ហាញក្នុងជួរឈរតាមរយៈរូបភាព។ Word Processor អាចបញ្ចូលនូវសមាសធាតុនៃការផ្ទេរ File មួយដែលអនុញ្ញាតឱ្យមាននូវឯកសារដែលត្រូវបានបញ្ជូនជាទម្រង់ចរន្តនៅលើបណ្ដាញ Network ។

សមាសធាតុនៃការផ្ទេរនេះបញ្ជាក់នូវ Word Processor ដែលជា Application នៅក្នុងបរិបទនៃ OSI នឹងស្រទាប់ទី៧នៃគំរូ OSI Reference ។ Web browser ដូចជា Netscape Navigator នឹង Internet Explorer មានទាំងសមាសធាតុនៃការផ្ទេរ File ផងដែរ។

ឧទាហរណ៍

នៅពេលដែលយើងបើកចូលទៅក្នុង **Website** មួយនោះ **Webpages** ត្រូវតែបញ្ចូលទៅក្នុងកុំព្យូទ័ររបស់យើង។



៦- Presentation Layer

ស្រទាប់ទី៦នៃ OSI Reference Model គឺ Presentation Layer បានផ្ដល់ឱ្យនូវការរៀបចំកូដនិងការបំប្លែងកូដ។ ការរៀបចំកូដត្រូវបានគេប្រើដើម្បីធានាថា Application មានព័ត៌មានគ្រប់គ្រាន់ដើម្បីដំណើរការ។ ប្រសិនបើចាំបាច់ស្រទាប់នេះអាចបកប្រែរវាងការរៀបចំនៃទិន្នន័យ។ Presentation Layer មិនត្រឹមតែទាក់ទិនជា មួយការរៀបចំនៃទិន្នន័យនិងការតំណាងឱ្យទិន្នន័យប៉ុណ្ណោះនោះទេ។ វាត្រូវទាក់ទិនជាមួយផងដែរនៃ Data structure ដែលកម្មវិធីបានប្រើប្រាស់។ ដូច្នេះស្រទាប់ទី៦នេះបញ្ជូនទៅឱ្យស្រទាប់ទី៧ហើយទិន្នន័យត្រូវបានរៀបចំពេលដែលវាត្រូវបានបញ្ជូន។

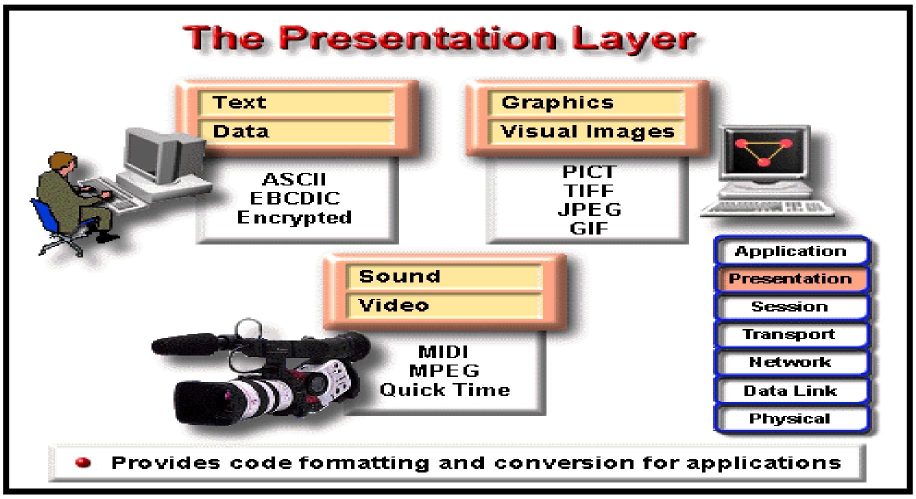
ដើម្បីដឹងពីដំណើរនេះ ឧបមាថាអ្នកមានប្រព័ន្ធចំនួនពីរធ្វើឱ្យដំណើរការ។ ប្រព័ន្ធមួយប្រើ EB-CDIC ហើយមួយទៀតប្រើ ASCII ដើម្បីបញ្ជូនទិន្នន័យ។ នៅពេលដែលប្រព័ន្ធពីរត្រូវការទំនាក់ទំនងគ្នានោះស្រទាប់ទី៦ត្រូវបានប្ដូរហើយបកប្រែរវាងការរៀបចំទិន្នន័យពីរផ្សេងគ្នា។ តួនាទីនៃស្រទាប់ទី៦គឺ Encrypt ទៅលើទិន្នន័យ។ Encryption ត្រូវបានគេប្រើប្រាស់នៅពេលដែលមានតម្រូវការដើម្បីការពារព័ត៌មានដែលបានបញ្ជូនពីឧបករណ៍ទទួលដែលគ្មានសិទ្ធិ។ ដើម្បីបំពេញការងារនេះបាន ដំណើរការនិង Codes ដែលមាននៅស្រទាបទី៦ត្រូវតែប្ដូរចំពោះទិន្នន័យនេះ។ កិច្ចការដដែលៗមាននៅក្នុង Presentation Layer នេះគឺបង្រួមអត្ថបទហើយប្ដូររូបភាពទៅជា bits។ ដូច្នេះត្រូវបានបញ្ជូនឆ្លងកាត់តាម Network មួយ។

ឧទាហរណ៍

PICT គឺជាការរៀបចំរូបភាពតាមទម្រង់ដើម្បីបញ្ជូននៃ Quickdraw Graphics រវាង macintosh ឬ power pc programs ត្រូវបានប្រើប្រាស់។ ការរៀបចំតំណាងមួយផ្សេងទៀតត្រូវបានគេប្រើប្រាស់គឺ image file formator TIFF។ TIFF ត្រូវបានគេប្រើសម្រាប់High-Resolution,Bit Mapped Images។

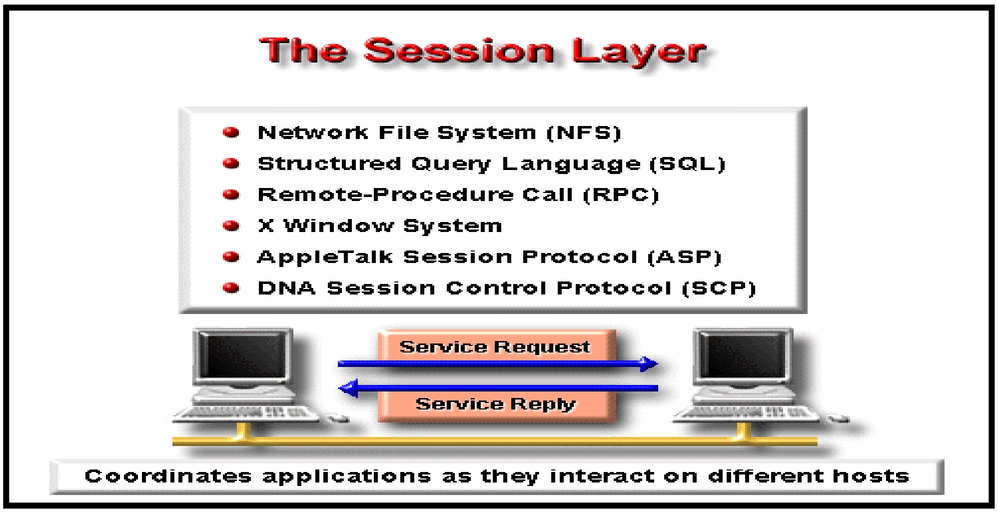
ស្តង់ដាស្រទាប់ទី៦ត្រូវបានគេប្រើសម្រាប់រូបភាពនៃក្រាហ្វដែលបានមកពី Joint Photographic Experts Group ដែលជាទូទៅគេហៅថា JPEG។ ប៉ុន្តែនៅស្តង់ដាស្រទាប់ទី៦ផ្សេងទៀតដែលត្រូវបង្ហាញនូវសំឡេងនិងវីដេរួមមានក្នុងស្តង់ដាទាំងអស់នេះគឺ Musical Instrument Digital Interface(MIDI)សម្រាប់ Digital Music នឹង

Motion Picture Experts Graphic នៃ Standard (MPEG) សម្រាប់ការបង្រួម(Compression)នឹង Coding Motion Video សម្រាប់ CDs,Digital Storageនឹង Bit Rates ឡើងដល់ទៅ 1.5Mbps និង Quick Time នឹង Standard មួយដោះស្រាយនូវ AudioនឹងVideo សម្រាប់ Macintosh និងPowerPC Programs ។



៧-The Session Layer

Session Layer គឺជាស្រទាប់ទី៥នៃគំរូ OSI Reference មានតួនាទីបង្កើត គ្រប់គ្រងនិងផ្តាច់ Session រវាង Aplication។ Session Layer រួមមាននូវសេវាដែលបានស្នើសុំនឹងសេវាឆ្លើយតបវិញដែលកើតមានឡើងនៅពេលដែល Application ធ្វើទំនាក់ទំនងរវាង Hosts ច្រើនផ្សេងគ្នា។



៨- Transport Layer

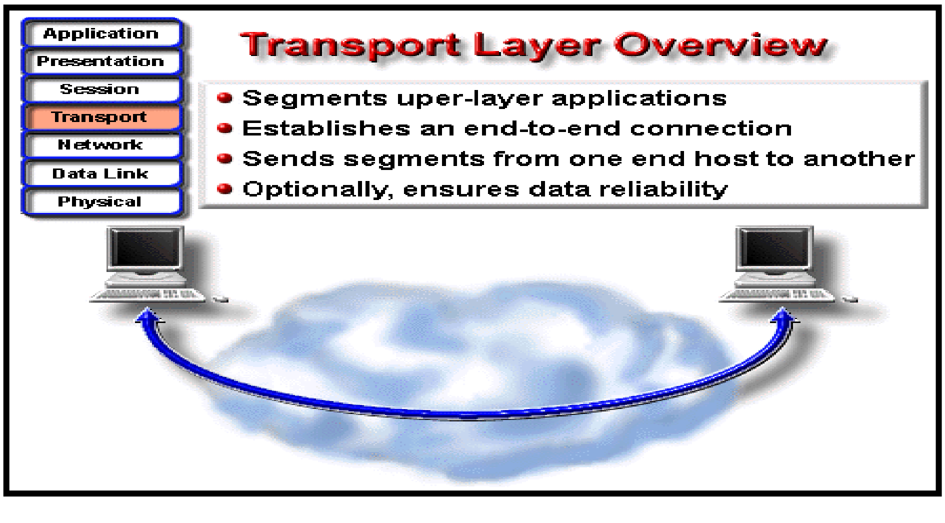
សេវាទាំងអសនេះមាននៅក្នុង Transort Layer ដែលជាស្រទាប់ទី៤នៃគំរូ OSI reference ដែលអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាចបំបែកផ្នាផ្នែកតូចៗនៅឯស្រទាប់ Application Layer ដែលជាស្រទាប់នៅខាងលើស្រទាប់ទី៤ជាមួយចរន្តនៃទិន្នន័យ។ សេវាទាំងអសនេះត្រូវបានប្រមូលផ្តុំឡើងវិញនូវ Segment នៅឯ Application Layer ខាងលើតែមួយគត់នៅពេលដែលវាត្រូវបានទទួលជាចុងក្រោយ។ ស្រទាប់ទី៤នៃចរន្តទិន្នន័យបានផ្តល់ឱ្យនូវសេវាដែលជារបស់ Transport ពី Host ទៅឱ្យគោលដៅ។ សេវាទាំងនោះមានដូចជា សេវារវាងឧបករណ៍បញ្ជូននិង

ឧបករណ៍ទទួលនៃស្រទាប់ទី៤ ចរន្តទិន្នន័យដែលជាការភ្ជាប់មួយរវាងចំណុចបញ្ចប់នៃបណ្តាញ Network។ នៅពេលដែល Transort Layer បានបញ្ជូននូវបំណែកនៃទិន្នន័យរបស់វា។ វាអាចធានាថាទិន្នន័យបានធ្វើដំណើរនៅលើបណ្តាញ Network ដោយសុវត្ថិភាពដែលត្រូវបានគេហៅថា Flow Control។ Flow Control អាចជៀសវាងនៅបញ្ហាមួយចំនួននៃ Host ដែលការភ្ជាប់មានការសន្ទុបត្រូវបានរក្សាទុកជាបណ្តោះអាសន្ននៅក្នុង Host ។

Overflows អាចធ្វើឱ្យមានបញ្ហាផ្សេងៗពីគ្នាពីព្រោះថា Overflow អាចធ្វើឱ្យទិន្នន័យបាត់បង់។ សេវានៃ Transport Layer ក៏អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ផងដែរដើម្បីស្នើសុំទិន្នន័យដែលត្រូវបានឱ្យរវាង Hosts និងគោលដៅ។ ដូច្នេះដើម្បីឱ្យមានទំនុកចិត្តចំពោះការបញ្ជូនទិន្នន័យទើបការភ្ជាប់ដែលទទួលខុសត្រូវ ត្រូវបានប្រើប្រាស់រវាងប្រព័ន្ធចុងបញ្ចប់។

Transport ដែលគួរឱ្យមានទំនុកចិត្តមានតួនាទីដូចខាងក្រោមៈ

- វាធានាថា Segment ដែលត្រូវបានចែករួចហើយនិងបានទៅដល់ឧបករណ៍បញ្ជូនវិញនូវចម្លើយបញ្ជាក់បន្ថែម
- វាបានផ្តល់សម្រាប់ការបញ្ជូនឡើងវិញនៃ Segment ដែលមិនមែនជាចម្លើយឆ្លើយតបវិញ
- វាបានដាក់នៅ Segment ត្រឡប់ទៅវិញតាមលំដាប់ត្រឹមត្រូវបន្តបន្ទាប់ៗគ្នានៅឯគោលដៅ
- វាជៀសវាង Congestion និង Control ។ ហើយអ្នកនិងជួបការពិភាក្សាកាន់តែច្បាស់លាស់ថែមទៀតនៃ Transort layer ដែលជាទំនុកចិត្តនៅក្នុងពេលក្រោយ

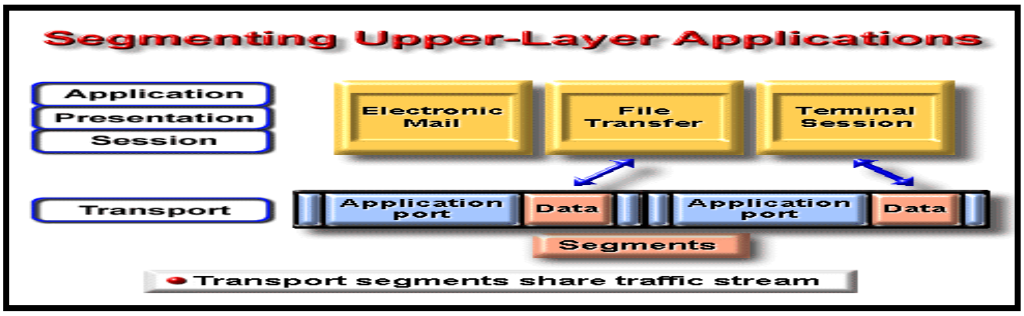


ការចែក Layer Application ខាងលើ

មានហេតុលមួយចំនួនចំពោះគំរូស្រទាបដែលមានច្រើនស្រទាប់ដូចជា OSI Reference Model ដែល Application ជាច្រើនត្រូវបានប្រើប្រាស់ Transport រួមគ្នា។ តួនាទីទាំងនេះត្រូវបានបំពេញនូវ Segment ដោយ Segment ។ នេះមានន័យថា Application អាចបញ្ជូននូវបំណែកនៃទិន្នន័យតាមគោលការណ៍មកមុនបំរើមុន។ ដូចនេះបំណែកនៃទិន្នន័យត្រូវបានផ្តល់ទៅឱ្យដល់គោលដៅដូចគ្នាឬគោលដៅជាច្រើនផ្សេងៗគ្នានៅលើបណ្តាញ Network ។

ដើម្បីដឹងពីដំណើរការនេះ ឧបមាថាអ្នកកំពុងតែបញ្ជូននូវសារអេឡិចត្រូនិកមួយហើយធ្វើការផ្ទេរ File មួយទៅឱ្យនរណាម្នាក់នៅលើបណ្តាញ Network។ នៅពេលដែលអ្នកផ្ញើនូវសារអេឡិចត្រូនិករបស់អ្នក Software នៅក្នុងឧបករណ៍បានដាក់ SMTP(e-mail) ចូលទៅក្នុងលេខ Port មុនពេលដែលវាត្រូវបានបញ្ជូនបន្ត។ វារួមមានលេខ Port មួយសម្រាប់កម្មវិធីដើមហើយនៅពេលដែល Application នីមួយៗបានបញ្ជូនបំណែកទិន្នន័យនោះវា

ប្រើប្រាស់លេខ Port ដែលបានកំណត់ពីមុនមកនោះ។ នៅពេលដែលឧបករណ៍ជាគោលដៅបានទទួលនូវចរន្តនៃបំណែកទិន្នន័យនោះ វាបានបំបែកនិងរៀបតាមលំដាប់នូវបំណែកនោះដើម្បីឱ្យ Transport Layer អាចបញ្ជូនទិន្នន័យទៅឱ្យ Application ដែលជាគោលដៅដែលត្រូវគ្នាបានយ៉ាងងាយ។

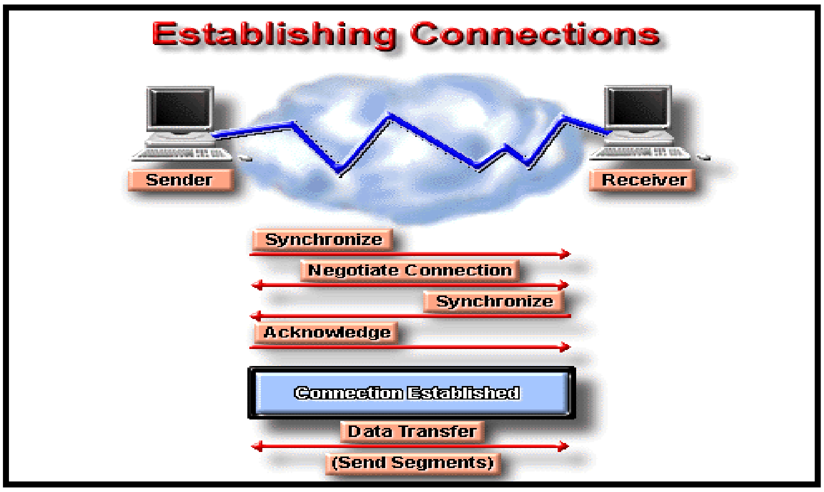


២-៥- ការបង្កើតការតភ្ជាប់

អ្នកប្រើប្រាស់ម្នាក់ៗនៃ Transport Layer ត្រូវបានបង្កើតឡើងនូវ Session ដែលទទួលខុសត្រូវដោយប្រព័ន្ធដែលមានតួនាទីស្មើគ្នារបស់វា។ ចំពោះការផ្ទេរទិន្នន័យដើម្បីបញ្ជូនបន្តទាំង Application ដែលកំពុងបញ្ជូននិងកំពុងទទួលបានផ្តល់ឱ្យនូវប្រព័ន្ធប្រតិបត្តិការដែលជាការតភ្ជាប់និងត្រូវបានចាប់ផ្តើម។ នៅក្នុងសញ្ញាណនេះម៉ាស៊ីនមួយបានបញ្ជូនហើយត្រូវទទួលបានដោយម៉ាស៊ីនមួយទៀត។

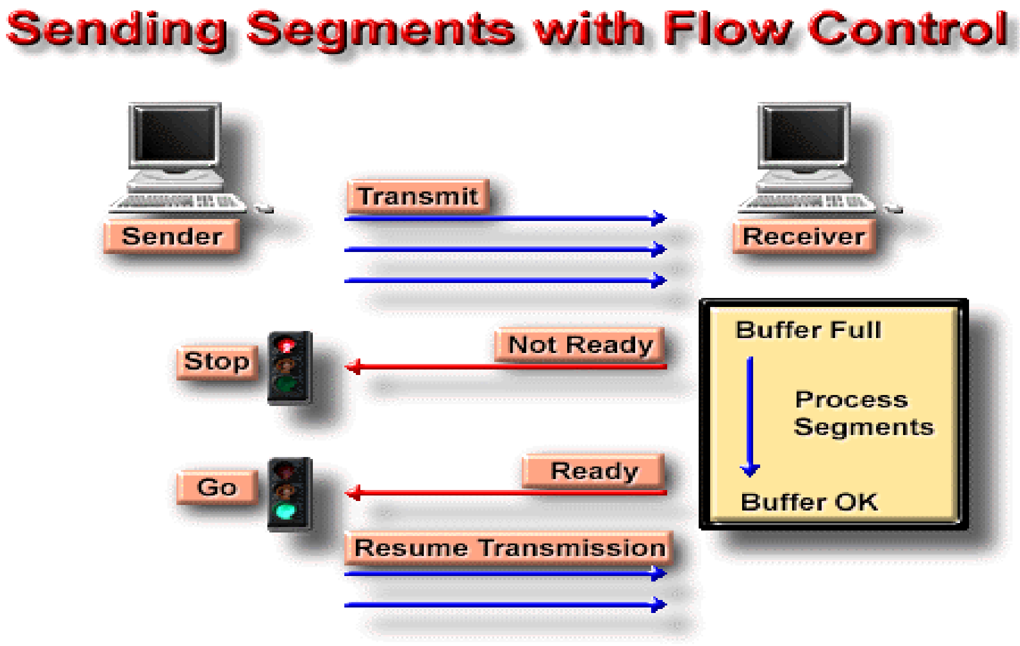
Protocol Software Modules នៅក្នុងប្រព័ន្ធប្រតិបត្តិការពីរបានធ្វើការទំនាក់ទំនងគ្នាដោយបញ្ជូននូវសារឆ្លងកាត់តាមបណ្តាញ networkដើម្បីបញ្ជាក់ថាការបញ្ជូនត្រូវបានទទួលបានដោជ័យរវាងឧបករណ៍បញ្ជូននិងឧបករណ៍ទទួល។ នៅក្រោយពេលដែលធ្វើឱ្យវាអាចស្គាល់គ្នាបាននោះ ការភ្ជាប់មួយក៏បានបង្កើតឡើងហើយការផ្ទេរទិន្នន័យក៏បានចាប់ផ្តើមធ្វើការបញ្ជូននៅក្នុងកំឡុងពេលដែលកំពុងតែបញ្ជូននោះម៉ាស៊ីនពីរបានបន្តទៅទៀតដើម្បីទំនាក់ទំនងគ្នាដែលមាន Protocol software ដើម្បីបញ្ជាក់ថាទិន្នន័យត្រូវបានទទួលដោយមិនបានបាត់បង់នោះទេនៅក្រោយពេលដែលបានបញ្ជូននោះ។

តាមរូបបង្ហាញនូវការភ្ជាប់រវាងប្រព័ន្ធកុំព្យូទ័របញ្ជូននិងកំពុងទទួល។ ជាដំបូងយើងត្រូវធ្វើឱ្យវាអាចស្គាល់គ្នាបានសិន។ ជំហានទី២និងទី៣បានផ្តល់មកវិញនូវចម្លើយឆ្លើយតបវិញ។ ការភ្ជាប់មានកម្រិតមួយថេរដែលមានទិសដៅផ្ទុយគ្នា។ នៅទីបញ្ចប់ Handshaking segmentគឺជាចម្លើយឆ្លើយតបមួយត្រូវបានប្រើប្រាស់ដើម្បីផ្តល់ព័ត៌មានទៅឱ្យដល់គោលដៅដើម្បីបញ្ជាក់ថាការភ្ជាប់ត្រូវបានបង្កើតឡើងហើយ។ ពេលភ្លាមនោះការភ្ជាប់ត្រូវបានបង្កើតឡើងហើយការផ្ទេរទិន្នន័យក៏ត្រូវបានចាប់ផ្តើមដំណើរការ។



ការបញ្ជូនទិន្នន័យជាមួយ Data Flow Control

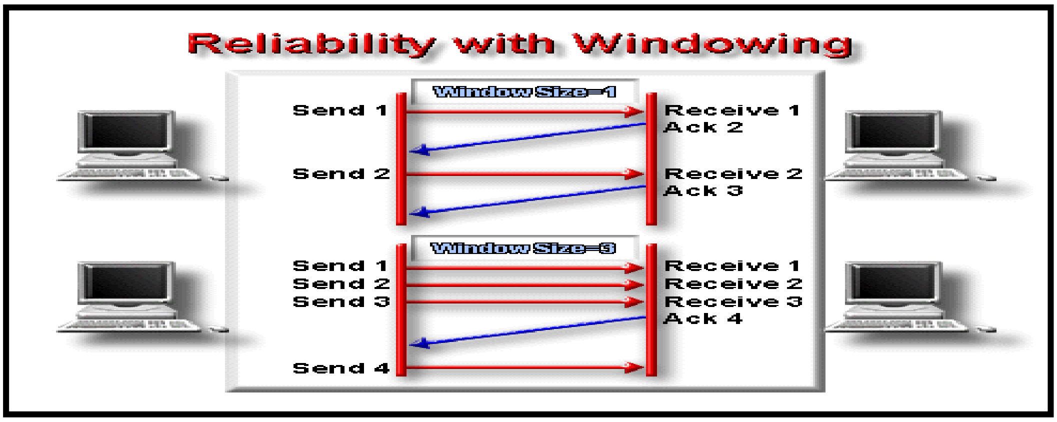
នៅពេលដែលការផ្ទេរទិន្នន័យត្រូវបានដំណើរការ នោះ Congestion អាចកើតមានឡើងដែលបណ្ដាលមកពីមូលហេតុពីរផ្សេងគ្នា។ ទី១គឺកុំព្យូទ័រមានល្បឿនលឿនជាការបញ្ជូនរបស់បណ្ដាញ។ ទី២ប្រសិនបើមានកុំព្យូទ័រច្រើនបានបញ្ជូននូវ datagram ទៅឱ្យគោលដៅតែមួយនៅពេលនោះឧបករណ៍ទទួលអាចកើតមានឡើងនូវ Congestion។ នៅពេលដែល datagram ត្រូវបានបញ្ជូនមកដល់លឿនពេកចំពោះ Host មួយឬ Gatway នៅពេលដែលកំពុងតែដំណើរការ វាត្រូវបានផ្ទុកជាបណ្ដោះអាសន្ននៅក្នុង Memory របស់កុំព្យូទ័រ។ ប្រសិនបើចរាចរណ៍នៅតែបន្តទៀតនោះ Host ឬ Gateway ត្រូវបានប្រើប្រាស់អស់នូវ Memory របស់វាហើយវាបានបោះបង់ចោលនូវ Datagram ដែលបានមកដល់នោះ។ ហើយធ្វើឱ្យទិន្នន័យបាត់បង់ហើយ Transport មានតួនាទីសម្រាប់បញ្ជូននូវពាក្យថា "មិនទាន់រួចរាល់" បានបង្ហាញទៅឱ្យឧបករណ៍បញ្ជូន។ សកម្មភាពវាដូចជាភ្លើងស្តុបអញ្ចឹងដែរ។ នៅពេលដែលវាទទួលបានសញ្ញាលនេះវាក៏បញ្ឈប់បញ្ជូនទិន្នន័យភ្លាម។ នៅពេលដែលឧបករណ៍ទទួលបអាចដោះស្រាយបញ្ហានេះបានហើយនោះឧបករណ៍ទទួលក៏បានបញ្ជូននូវពាក្យថា "រួចរាល់"ដែលជាសញ្ញាបង្ហាញថាអាចចេញដំណើរបន្តទៀតបាន។ នៅពេលដែលវាទទួល ឧបករណ៍បញ្ជូនក៏អាចបន្តបញ្ជូនបានសារជាថ្មីនូវ Segment ។



ភាពដែលអាចទុកចិត្តបានជាមួយWindowing

នៅក្នុងទ្រង់ទ្រាយដែលជាមូលដ្ឋានគ្រឹះរបស់ការបញ្ជូនទិន្នន័យដែលគួរឱ្យទុកចិត្តបាន Data Packets ត្រូវបានគេផ្ដល់ទៅឱ្យការទទួលនូវក្នុងលំដាប់លំដោយដូចគ្នានៅក្នុងពេលដែល Data Packet ត្រូវបានបញ្ជូន។ Protocol មិនទទួលបានជោគជ័យប្រសិនបើមាន Data Packet ណាមួយត្រូវបានបាត់បង់ ត្រូវបានបំផ្លាញ ត្រូវបានស្ទួន ឬទទួលបានមិនតាមលំដាប់ប្រសិនបើឧបករណ៍រងចាំទទួលនូវចម្លើយឆ្លើយតបវិញមួយក្រោយពីការបញ្ជូន Segment នីមួយៗនោះដែល Throughut មានកម្រិតទាប។ ដោយសារតែមានពេលវេលាគ្រប់គ្រាន់ក្រោយពីឧបករណ៍បញ្ជូនបានបញ្ចប់ការបញ្ជូន Data Packets នោះ មុនពេលដែលឧបករណ៍បញ្ជូនបានដំណើរការទទួលបាននូវចម្លើយតមវិញណាមួយក្នុងរយៈពេលនោះ ត្រូវតែបានប្រើសម្រាប់ការបញ្ជូនទិន្នន័យបន្ថែមទៀត។ Windowing គឺជាវិធីសាស្ត្រមួយដើម្បីត្រួតពិនិត្យបរិមាណនៃព័ត៌មានដែលបានបញ្ជូនរវាងឧបករណ៍នៃចុងបញ្ចប់ទាំងពីរ។ Protocol កំណត់ពីព័ត៌មាននៅក្នុង Packets ហើត TCP/IP កំណត់ពីព័ត៌មាននៅក្នុង Byte ។

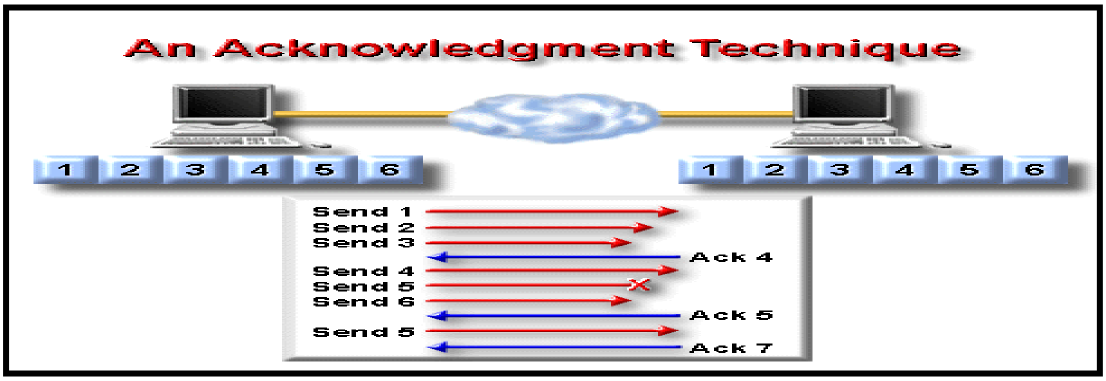
នៅក្នុងឧទាហរណ៍តាមរូប Windows មួយមានទំហំស្មើនឹង១ ត្រូវបានឧបករណ៍បញ្ជូនរង់ចាំនូវចម្លើយតបមកវិញមួយនៅគ្រប់ Data Packet នីមួយៗដែលបានបញ្ជូន។ ក្រោយមកដោយ Windows មួយមានទំហំស្មើនឹង៣វិញ ឧបករណ៍អាចបញ្ជូន Data packet 3 មុនពេលទទួលបាននូវចំឡើយតបវិញមួយ។ Windowing គឺជាការយល់ព្រមរវាងឧបករណ៍នៃចុងបញ្ចប់ទាំងពីរ។ នៅក្នុងឧទាហរណ៍តាមរូបខាងលើគឺឧបករណ៍បញ្ជូននឹងទទួលគឺជា Workstation ។



ការចែកចាយដែលទុកចិត្តបានធានាថាចរន្តនៃទិន្នន័យដែលត្រូវបានបញ្ជូនពីម៉ាស៊ីនកុំព្យូទ័រមួយត្រូវបានឆ្លងកាត់តាមរយៈ Data link មួយទៅកាន់ម៉ាស៊ីនកុំព្យូទ័រមួយផ្សេងទៀតដោយគ្មានស្ទួនឬបាត់បង់ព័ត៌ មានទេ។ ចម្លើយឆ្លើយតបមកវិញវិជ្ជមានមួយដែលមានការបញ្ជូនឡើងវិញគឺ ជាបច្ចេកទេសដែលធានានៃការទទួលនៃចរន្តនៃទិន្នន័យដែលជាទីទុកចិត្ត។ វាត្រូវការឧបករណ៍ទទួលមួយដើម្បីទំនាក់ទំនងគ្នាជាមួយនឹងប្រភពដើមហើយវាបញ្ជូនត្រឡប់វិញនូវចម្លើយឆ្លើយតបមកវិញនូវ Message មួយនៅពេលដែលវាទទួលនូវទិន្នន័យ។

ឧបករណ៍បញ្ជូនបានរក្សាទុកនូវការកត់ត្រានៃ Data Packet នីមួយៗដែលបានបញ្ជូនហើយរង់ចាំចំពោះចម្លើយឆ្លើយតបមកវិញមួយមុនពេលដែលមានការបញ្ជូននូវ Data Packet ក្រោយទៀត ឧបករណ៍បញ្ជូនក៏បានចាប់ផ្តើមកំណត់រយៈពេលមួយនៅពេលដែលវាបានបញ្ជូននូវ Segment មួយហើយវាបានបញ្ជូនឡើងវិញនូវ segment មួយប្រសិនបើអ្នកកំណត់ម៉ោងបានផុតកំណត់មុនពេល ដែលចម្លើយឆ្លើយតបមកវិញមួយបានមកដល់នោះ។ តាមរូបដែលបង្ហាញនៅក្នុងឧបករណ៍បញ្ជូនមួយដែលបានធ្វើការបញ្ជូននៅ Data Packet 1,2,3។

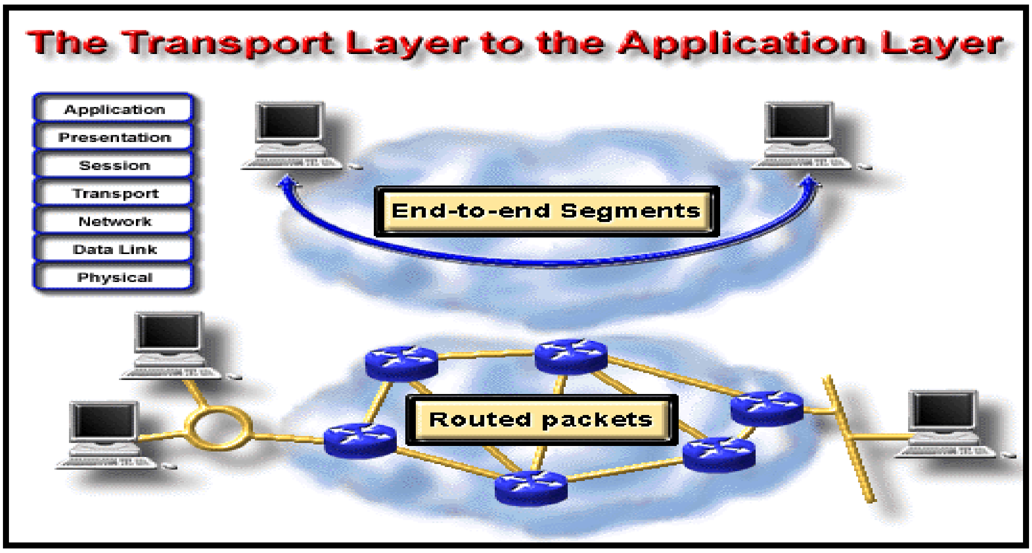
ឧបករណ៍ទទួលបាននូវប័ណ្ណនៃ Packets ដែលបានស្នើសុំចំពោះ Packet 4 ។ ឧបករណ៍បញ្ជូនបានទទួលនូវចម្លើយឆ្លើយតបមកវិញ វាបានបញ្ជូននូវ Packet 4,5,6 ។ ប្រសិនបើ Packet 5 មិនបានមកដល់គោលដៅទេ ឧបករណ៍ទទួលបានទទួលដោយស្នើសុំដើម្បីបញ្ជូនឡើងវិញនូវ Packets នោះ។



ឧបករណ៍បញ្ជូន វាបញ្ជូន Packet ទី៥ឡើងវិញហើយត្រូវតែឆ្លើយតបមកវិញដើម្បីបន្តជាមួយការបញ្ជូនរបស់ Packet ទី៧។

នៅក្នុងមេរៀននេះអ្នកបានសិក្សាខ្លះមកហើយពីស្រទាប់ខាងលើរបស់ Nerwork ដូចដែលកម្រិតខាងលើនីមួយៗក្នុងចំណោមកម្រិតខាងលើជាច្រើន ដំណើរការនូវតួនាទីរបស់វាដោយផ្ទាល់ហើយអាស្រ័យទៅលើសេវានៃស្រទាប់ខាងក្រោម។ គ្រប់ application នៃស្រទាប់ខាងលើទាំង៤ដូចជាស្រទាប់ទី ៧ ស្រទាប់ទី ៦ ស្រទាប់ទី ៥ ស្រទាប់ទី ៤ អាច encapsulate ទិន្នន័យនៅចុងទាំងសងខាងនៃឧបករណ៍ទាំងពីរ។

ឧបមាថា Transport Layer វាអាចប្រើប្រាស់ network ដូចជាពពកដើម្បីបញ្ជូននូវ Data packets ពីប្រភពបញ្ជូនទៅកន្លែងទទួល។ ប្រសិនបើយើងពិនិត្យមើលតួនាទីខាងក្នុងពពកយើងដឹងថាផ្លូវជាច្រើនដែលល្អបំផុតសម្រាប់ Route មួយដែលគេឱ្យ។ យើងអាចចាប់ផ្តើមមើលតួនាទីដែល Routers ដំណើរការនេះ។



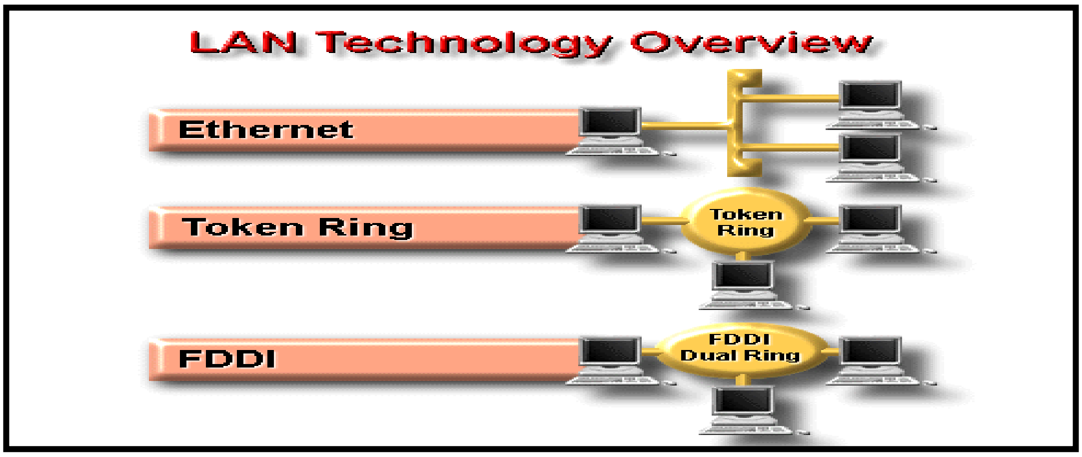
ជំពូកទី៣

ការរំលឹកឡើងវិញអំពី LAN Technology និង ការរៀបចំគម្រោងនៃការបង្កើតប្រព័ន្ធ Network

មុននិងអ្នកសិក្សាព័ត៌មានច្បាស់លាស់អំពីបច្ចេកវិទ្យានៃ LAN ដែលគេនិយមប្រើ។ មានបច្ចេកវិទ្យានៃ LAN ចំនួន៣ដែលត្រូវបង្ហាញក្នុងគឺៈ

- Ethernet:គឺជាបច្ចេកវិទ្យានៃ LAN ដែលសំខាន់ហើយវាដំណើរការនៅក្នុង LAN
- Token Ring:គឺជាបច្ចេកវិទ្យាដែលបានមកពីក្រុមហ៊ុន IBM ហើយឥឡូវនេះគេប្រើវាយ៉ាងច្រើននោះដែរ
- FDDI:គឺបានប្រើប្រាស់នូវ Token ផងដែរហើយសព្វថ្ងៃនេះគេពេញនិយមប្រើប្រាស់ជា LAN ដែលជំឡើងនៅតាមអាគារ។ យើងនិងសិក្សាពី Ethernet 802.3 ។

តាមរូបភាពបង្ហាញពីប្រភេទខ្សែដែលគេនិយមប្រើនៅក្នុង network សព្វថ្ងៃនេះគឺ Caxial Fiber optic និង UTP ។



៣-១- Local Area Networks and Devices

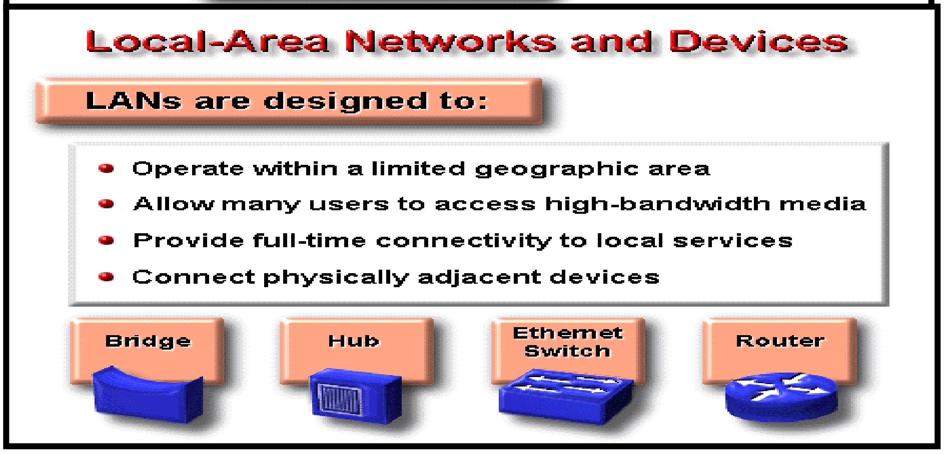
នេះគឺជាលក្ខណៈដ៏សំខាន់នៃ LAN:

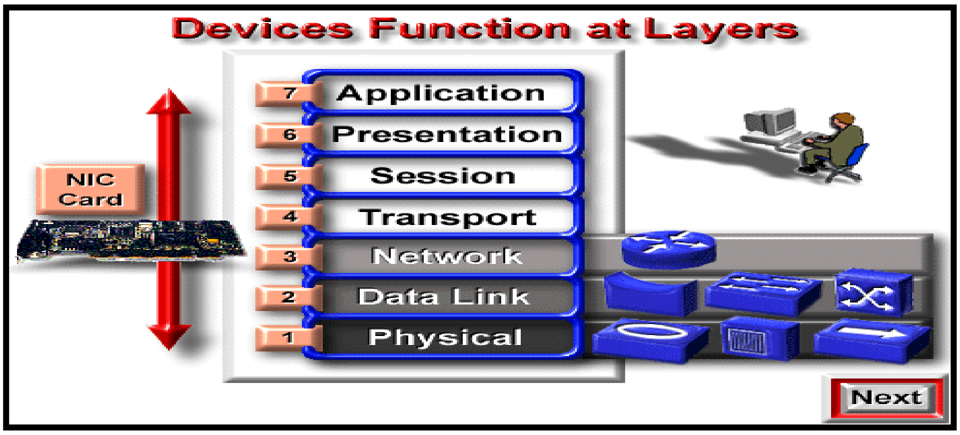
- ជាប្រភេទបណ្តាញ Network មួយដែលគេបានប្រើប្រាស់នៅក្នុងអាគារឬការិយាល័យនៃអាគារណាមួយ
- LAN បានអនុញ្ញាតឱ្យយើងអាចភ្ជាប់ឧបករណ៍ច្រើន(តាមធម្មតាជា PC)ដែលមានខ្សែមានល្បឿនលឿន។ បើតាមនិយមន័យនៃ LAN ត្រូវបានគេភ្ជាប់តាមរយៈ Physical layer ។

ឧបករណ៍របស់ LAN រួមមានដូចជាៈ

- Bridge: គឺត្រូវបានគេប្រើប្រាស់សម្រាប់ភ្ជាប់ទៅកាន់ LAN segment និងច្រោះចរាចរណ៍
- Hub: វាមានតួនាទីសម្រាប់តែភ្ជាប់ប៉ុណ្ណោះហើយអនុញ្ញាយឱ្យប្រើប្រាស់ខ្សែប្រភេទជា UTP
- Ethernet Switch: ត្រូវបានគេប្រើប្រាស់សម្រាប់បញ្ជូនទិន្នន័យដែលមានលក្ខណៈជា Full duplex ហើយអាចកំណត់នូវ bandwidth ទៅឱ្យ Segment ឬឧបករណ៍ណាមួយ

- Router:វាអាចផ្តល់ឱ្យនូវសេវាជាច្រើនរួមមាន Internetworking និងគ្រប់គ្រងទៅលើ broadcast



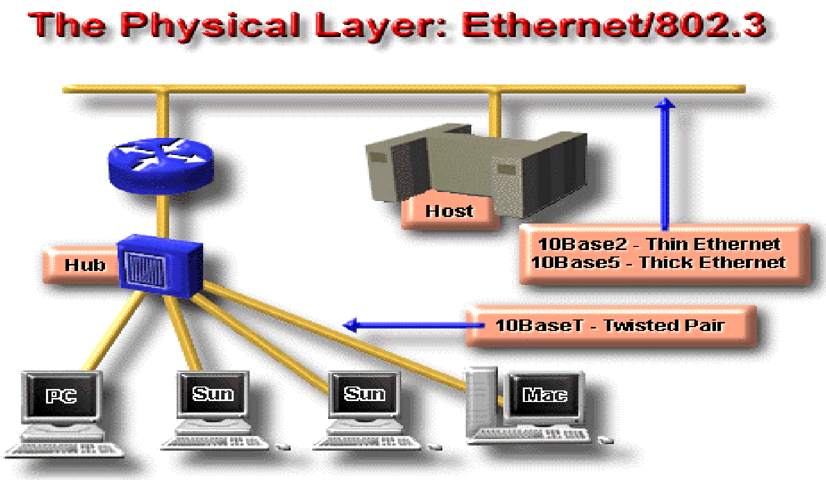


៣-២- Physical Layer : Ethernet/802.3

Ethernet និង IEEE 802.3 standards បានកំណត់ពីរូបរាងនៃ LAN ជា Bus ដែលប្រើប្រាស់នូវ Baseband signaling ដែលមានអត្រាល្បឿន 10 Mbps។ តាមរូបបង្ហាញនូវស្តង់ដាបីប្រភេទនៃ LAN គឺ:

- 10 Base 2:គឺជា Thin Ethernet អនុញ្ញាតឱ្យប្រើប្រាស់ត្រឹមតែមចម្ងាយ១៨៥ម៉ែត្រដែលជាខ្សែ Coaxial
- 10 Base 5:គឺជា Thick Ethernet អនុញ្ញាតឱ្យប្រើប្រាស់បានចម្ងាយរហូតដល់៥០០ម៉ែត្រដែលជា Coaxial
- 10 Base T:គឺជា Carrier Ethernet Frame វាមានតម្លៃមិនស៊ូវថ្លៃនោះទេ វាជាខ្សែ UTP ។ 10 base 5 និង10 base 2 ត្រូវបានផ្តល់នូវការប្រើសម្រាប់ក្នុង LAN segment ដូចគ្នា។ ឧបករណ៍ត្រូវបានគេភ្ជាប់ទៅនិង AUI(Attachment Unit Interface) តាមរយៈខ្សែទៅកាន់ Transceiver ដែលត្រូវបានភ្ជាប់ដោយផ្ទាល់ទៅកាន់ខ្សែ

Ethernet Coaxial ។ ដោយសារតែ 10 base T ត្រូវបានគេប្រើដើម្បីប្រើសម្រាប់តែឧបករណ៍តែមួយ។ ឧបករណ៍ជាច្រើនត្រូវបានគេភ្ជាប់ទៅនិង Ethernet LAN ដោយប្រើខ្សែ 10 base T ដែលត្រូវបានភ្ជាប់ទៅ Hub ឬ LAN switch មួយ។ នៅក្នុងការរៀបចំនេះ Hub ឬ LAN switch ដូចគ្នាទៅនិង Ethernet segment ដែរ។



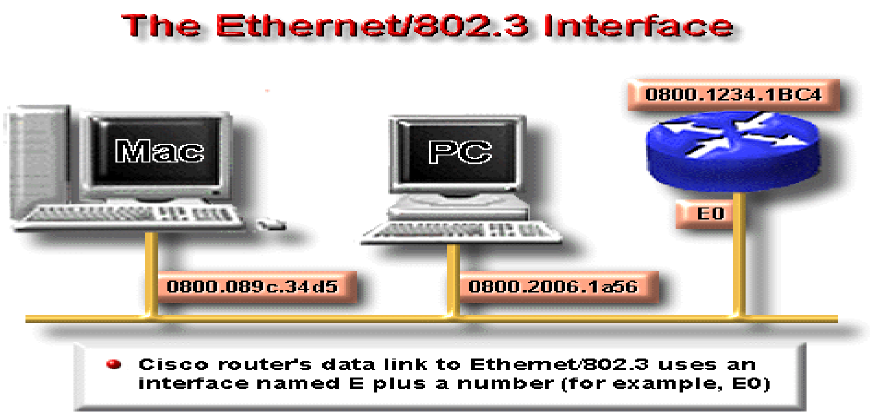
៣-៣- Ethernet/802.3 Interface

Ethernet និង 802.3 data link បានរៀបចំនូវទិន្នន័យសម្រាប់ការបញ្ជូនឆ្លងកាត់តាមខ្សែដែលត្រូវបានគេប្រើប្រាស់ដើម្បីភ្ជាប់ទៅឧបករណ៍ទាំងពីរ។

ឧទាហរណ៍

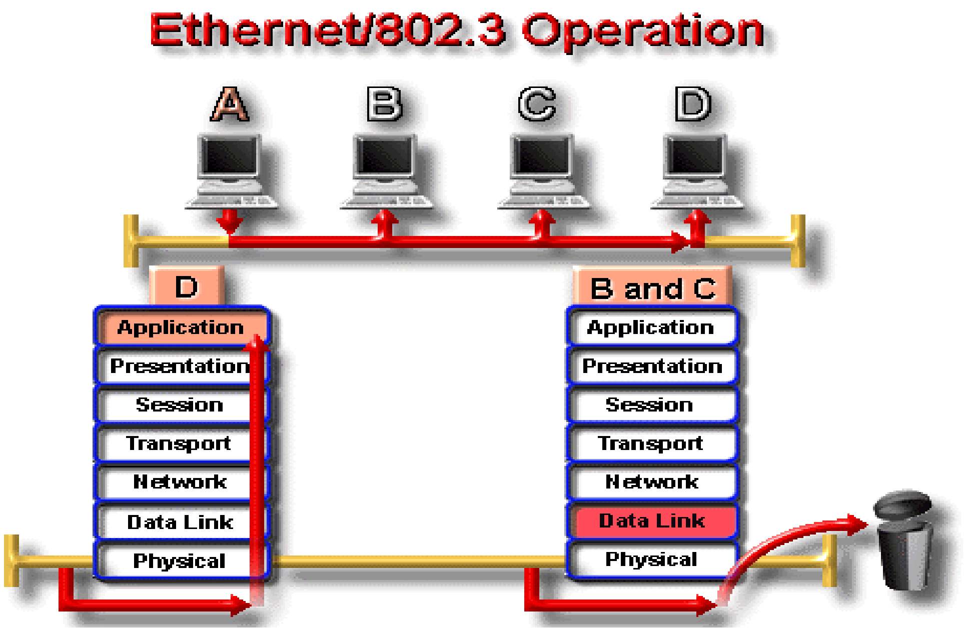
ដូចនៅក្នុងរូបភាពនេះបង្ហាញនូវឧបករណ៍ចំនួន៣ត្រូវបានគេតភ្ជាប់គ្នាទៅវិញទៅមកនៅលើ Ethernet LAN មួយ។

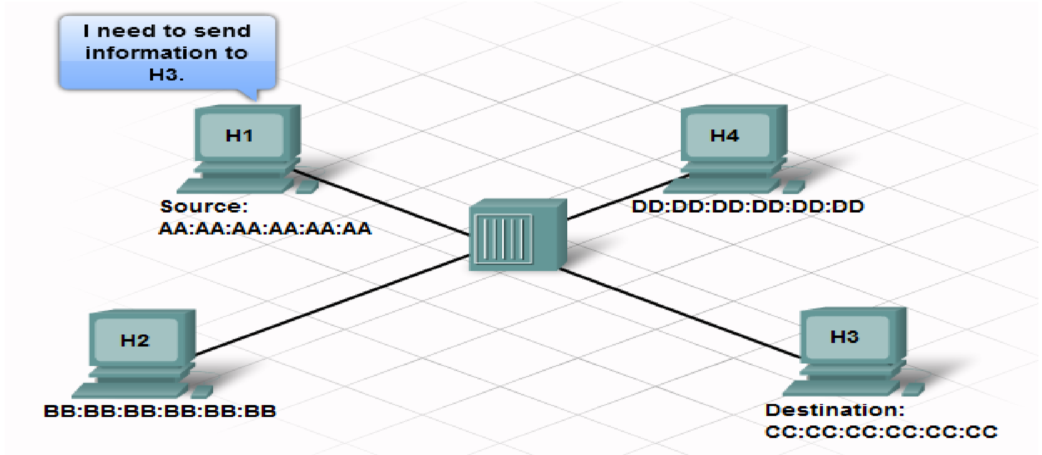
ម៉ាស៊ីនជាប្រភេទ Mancintosh នៅខាងឆ្វេងនឹង Intel-based pc ស្ថិតនៅកណ្តាលបានបង្ហាញនូវ MAC address បានប្រើដោយ Datalink Layer។ Router នៅខាងស្តាំប្រើប្រាស់នូវ MAC address ផងដែរសម្រាប់ LAN interface នីមួយៗរបស់វា។ ចំពោះ Ethernet /802.3 interface នៅក្នុង router ដែលយើងបានប្រើប្រាស់ជាមួយ Cisco IOS interface ដែលតាងដោយអក្សរកាត់គឺ E ប្រើសម្រាប់លេខ Interface(ឧទាហរណ៍ដូចបង្ហាញក្នុងរូប E 0)។



៣-៤- Ethernet/802.3 Operation

នៅក្នុង Carrier Sense Multile Access ដែលមាននូវ Collision Detection (CSMA/CD) network កើតឡើងហើយការបញ្ជូនរបស់ Node មួយត្រូវបានឆ្លងកាត់ Network ទាំងមូលហើយវាត្រូវបានទទួលនិងព្រមទាំងត្រូវបានត្រួតពិនិត្យតាមគ្រប់ Node នីមួយៗ។ នៅពេលដែលសញ្ញាលមួយបានមកដល់ចុងបញ្ចប់នៃ Segement ហើយនៅពេលនោះ Terminator បានស្រូបយកវាដើម្បីការពារវាមិនឱ្យវិលត្រឡប់មកវិញនៅលើ Segment ។ ដោយអនុញ្ញាតឱ្យមានការបញ្ជូនតែមួយគត់នៅលើ LAN មួយនៅពេលដែលគេបានផ្តល់ឱ្យ។



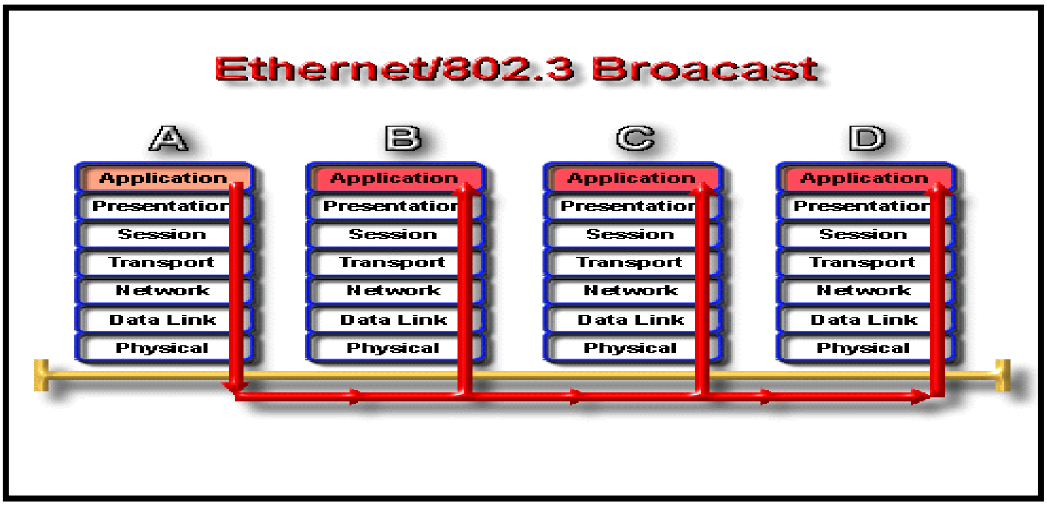


៣-៥- Ethernet / 802.3 Broadcast

Broadcasting គឺជា Tool មួយដែលមានឥទ្ធិពលបំផុតដែលវាធ្វើការបញ្ជូននូវ Frame មួយទៅឱ្យឧបករណ៍ជាច្រើននៅពេលតែមួយ។ Broadcast បានប្រើប្រាស់នូវអាស័យដ្ឋានរបស់គោលដៅស្ថិតនៅក្នុង Datalink ដែលមានទម្រង់ជា bits លេខ១ទាំងអស់(FFFFFFFFFFFFFFF គោល១៦)។ ដូចនៅក្នុងរូបបានបង្ហាញពីឧបករណ៍ A បានធ្វើការបញ្ជូននូវ Frame មួយដែលមាននូវអាស័យដ្ឋានរបស់គោលដៅរបស់ឧបករណ៍

ទាំងអស់ហើយនៅពេលនោះឧបករណ៍ B C នឹង D បានទទួលហើយបានផ្តល់ទៅឱ្យស្រទាប់ខាងលើសម្រាប់ដំណើរការបន្តទៀត។

Broadcast បានធ្វើឱ្យប៉ះពាល់យ៉ាងខ្លាំងដល់ដំណើរការរបស់ប្រព័ន្ធ network ព្រោះថាវាបានរំខានដល់ឧបករណ៍ដែលស្ថិតនៅលើប្រព័ន្ធ network នោះ។ ដូច្នេះ broadcast ត្រូវបានប្រើប្រាស់តែក្នុងករណីដែល MAC address របស់គោលដៅមិនត្រូវបានស្គាល់ឬនៅពេលដែលវាធ្វើការបញ្ជូននូវ frame មួយទៅឱ្យគ្រប់ឧបករណ៍ទាំងអស់។



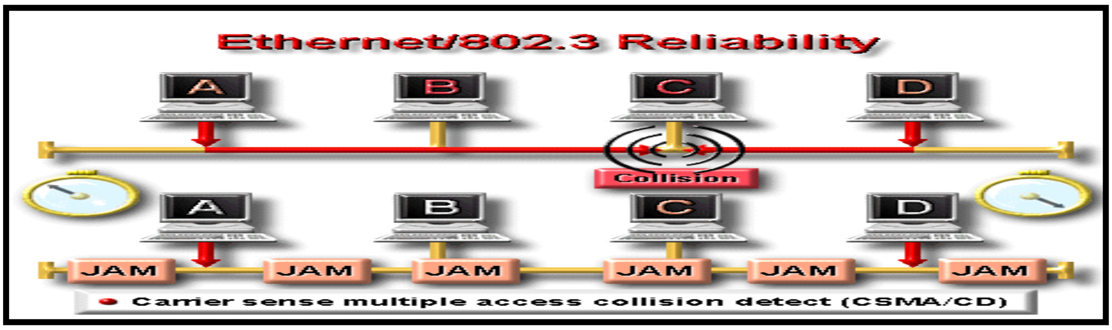
៣-៦- ភាពទុកចិត្តរបស់ Ethernet/802.3

CSMA / CD មានតួនាទីដូចខាងក្រោមៈ

នៅពេលដែលឧបករណ៍មួយមានបំណងចង់ធ្វើការបញ្ជូននោះវាបានត្រួតពិនិត្យបណ្តាញ network ជាមុនសិនដលម្បីកំណត់ថាតើឧបករណ៍មួយផ្សេងទៀតកំពុងធ្វើការបញ្ជូនដែរឬទេ។ បើបណ្តាញ network មិនត្រូវបានប្រាស់នោះទេ ឧបករណ៍ក៏បានចាប់ផ្តើមធ្វើការបញ្ជូន។ ខណៈដែលកំពុងតែធ្វើការបញ្ជូន ឧបករណ៍បានត្រួតពិនិត្យទៅលើបណ្តាញ network ដើម្បីធានាថាគ្មានឧបករណ៍ណាមួយផ្សេងទៀតកំពុងបញ្ជូននោះទេ។ ឧបករណ៍ពីរអាចចាប់ផ្តើមធ្វើការបញ្ជូននៅពេលតែមួយប្រសិនបើឧបករណ៍ទាំងពីរពិនិត្យឃើញថាបណ្តាញ Network នៅទំនេរ។

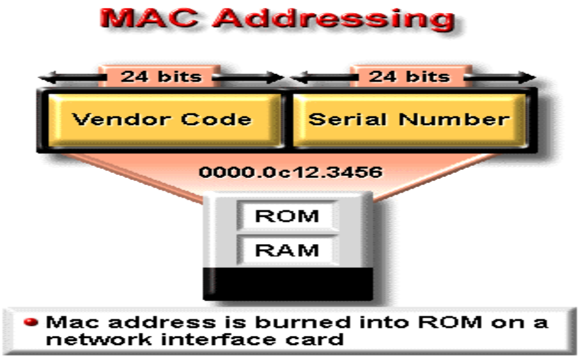
ប្រសិនបើឧបករណ៍ពីរបានធ្វើការបញ្ជូននៅពេលតែមួយនោះការប៉ះទង្គិចគ្នា បានកើតមានឡើងដូច ដែលបង្ហាញក្នុងរូបខាងក្រោម។ នៅពេលដែលវាធ្វើការបញ្ជូន node មួយបានទទួលនូវការប៉ះទង្គិច(collision) ហើយនៅពេលនោះ វាបានបញ្ជូននូវសញ្ញាលស្ទះ(Jam signal) មួយដែលបណ្តាលមកពីការប៉ះទង្គិចគ្នាដែលបានប្រើរយៈពេលយ៉ាងយូរសម្រាប់ឱ្យ nodes ផ្សេងៗទៀតដើម្បីទទួលយកវា។

គ្រប់ Nodes ទាំងអស់ដែលបានធ្វើការបញ្ជូន បន្ទាប់មកវាបានបញ្ឈប់ការបញ្ជូន Frame ជាបណ្តោះអាសន្នសិនមុនវាធ្វើការបន្តទៀតឡើងវិញ។ ប្រសិនបើការបញ្ជូនក្រោយទៀតបានផ្តល់លទ្ធផលជាការប៉ះទង្គិចនៅពេលនោះ node បានព្យាយាមធ្វើការបញ្ជូនសារជាថ្មីទៀតចំនួន១៥ដងមុនពេលដែលវាបោះបង់ចោល។ ម៉ោងបង្ហាញពីរយៈពេលនៃការត្រឡប់វិញផ្សេងៗគ្នា។ ប្រសិនបើរយៈពេលមានចំនួនពីរផ្សេងគ្នា នោះឧបករណ៍មួយនិងទទួលបានជោគជ័យនៅពេលបន្ទាប់មកទៀត។



MAC Addressing

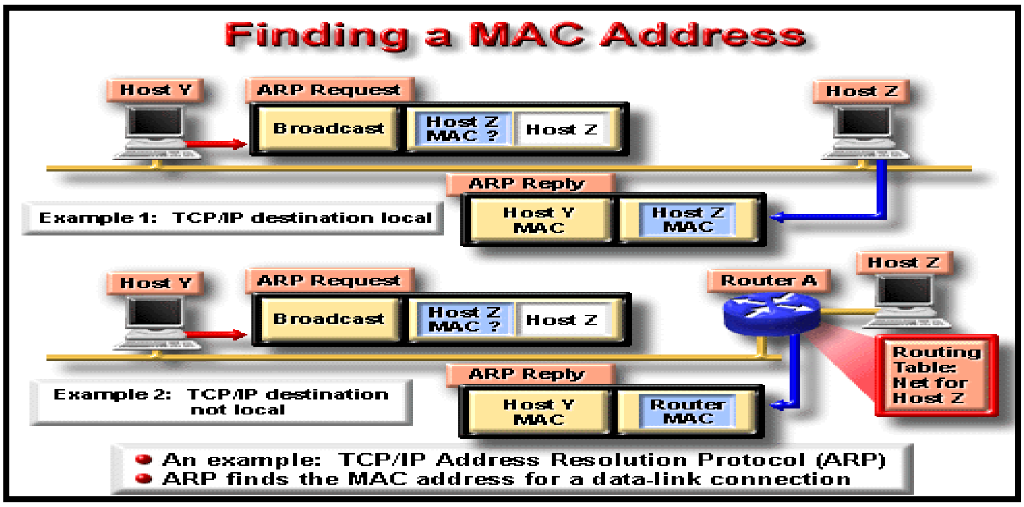
ចំពោះឧបករណ៍ជាច្រើនដើម្បីអាចប្រើប្រាស់នូវខ្សែរួមគ្នាបានហើយព្រមទាំងអាចស្គាល់គ្នាទៅវិញទៅមកបាន។ MAC sublayer បានកំណត់ឱ្យហាដវែរឬ Datalink address មួយដែលត្រូវបានគេហៅថា MAC address ។ MAC address មានតែមួយគត់សម្រាប់ LAN interface នីមួយៗ។ MAC address នៃ NIC ត្រូវបានគេបង្កើតឡើងស្ថិតនៅក្នុង ROM ។ នៅពេលដែល NIC បានផ្តល់ឱ្យនូវ Address នេះត្រូវបានចម្លងចូលទៅផ្ទុកក្នុង RAM ។



៣-៧- ការស្វែងរក MAC address

នៅមុននៅពេលដែលទិន្នន័យជា frame មួយត្រូវបានផ្លាស់ប្តូរជាមួយឧបករណ៍ដោយភ្ជាប់ផ្ទាល់ស្ថិតក្នុង LAN តែមួយ។ ឧបករណ៍បញ្ជូនមាននូវ MAC address មួយដែលវាបានប្រើជាអាស័យដ្ឋានគោលដៅ។ វិធីសាស្ត្រដើម្បីរកឱ្យឃើញនូវ MAC addressនៃឧបករណ៍មួយគឺប្រើប្រាស់នូវ ARP(Address Resolution Protocol)។ តាមរូបភាពបង្ហាញពីវិធីសាស្ត្រពីរនៃ TCP/IP ។ ARP ត្រូវបានប្រើសប្រាស់ដើម្បីរកឱ្យឃើញពី MAC address មួយ។ នៅក្នុងឧទាហរណ៍ទី១ Host Y នឹង Host Z គឺស្ថិតនៅក្នុង LAN តែមួយ។ Host Y បានបញ្ជូន broadcast នូវ APR ទៅឱ្យ LAN មួយដើម្បីរកឱ្យឃើញនូវ MAC address នៃ HostZ ។ ដោយសារតែ Host Y បានធ្វើការបញ្ជូនចេញនូវ broadcast មួយ នោះគ្រប់ឧបករណ៍ទាំងអស់រួមទាំង HostZ និងរកមើលនូវការស្នើសុំនោះ។

ទោះបីជាយ៉ាងណាក៏ដោយមានតែ Hostz តែមួយគត់ដែលបានឆ្លើយតបវិញដោយមានទាំង MAC address របស់វាផងដែរ។ Host Y បានទទួលនូវការឆ្លើយតបរបស់ Host Z ហើយបានរក្សាទុកនូវ MAC address នោះនៅក្នុង Memory ដែលត្រូវបានគេហៅកាត់ថា ARP cahe ។ នៅពេលក្រោយទៀត Host Y ត្រូវបានភ្ជាប់ដោយផ្ទាល់ជាមួយ Host Z ហើយវាបានធ្វើការហៅ MAC addres នៃ Host Z ដែលវាបានរក្សាទុកនោះមកវិញ។

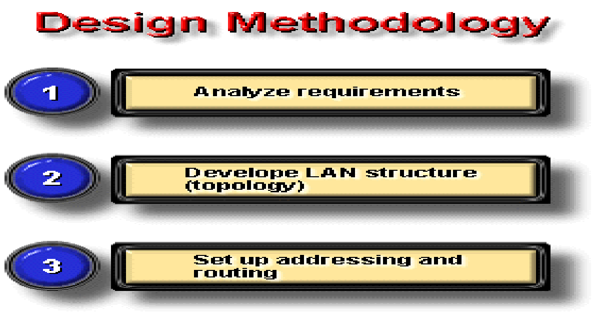


៣-៨- គោលបំណងនៃការបង្កើត LAN

ជំហានដំបូងក្នុងការបង្កើត LAN មួយគឺគេត្រូវកំនត់ពីគោលបំណងនៃការដំឡើងនោះដោយរៀបចំជាឯកសារ។ ឧទាហរណ៍

- សម្រាប់ចែកចាយនូវ Files និង printers
- សម្រាប់ចែកចាយនូវ Internet
- សម្រាប់បង្កើតជា intranet(Web server និង E-mail server) ដែលជាគោលបំណងទាំងនេះត្រូវបានបំពេញទៅតាមតម្រូវការរបស់អង្គភាពណាមួយឬក្រុមហ៊ុនណាមួយ ប៉ុន្តែតម្រូវការទូទៅសម្រាប់ការបង្កើត network មានដូចខាងក្រោម:
- Functionality: network ដែលបានបង្កើតឡើងរួចហើយត្រូវតែអាចប្រើប្រាស់បានហើយការប្រើប្រាស់នោះត្រូវតែបំពេញទៅតាមគោលបំណងរបស់អ្នកប្រើប្រាស់។
- Scalability: Network ដែលយើងបានបង្កើតឡើងរួចហើយត្រូវតែមានពង្រីកបាន។ វាមានន័យថាបើយើងចង់បន្ថែមនូវចំនួននៃឧបករណ៍ វាមិនអាចធ្វើឱ្យប៉ះពាល់ដល់ការបង្កើតឡើងនោះទេ
- Adatability:network ដែលយើងបានបង្កើតឡើងត្រូវតែគិតពីបច្ចេកវិទ្យាថ្មីដែលគេនិងប្រើប្រាស់នៅពេលខាងមុខ។ មានន័យថា network ដែលយើងបានបង្កើតឡើងនោះត្រូវតែអាចប្រើប្រាស់ជាមួយនឹងបច្ចេកវិទ្យាថ្មីបាន
- Manageability:យើងត្រូវតែបង្កើតវាយ៉ាងណាឱ្យមានលក្ខណៈងាយស្រួលក្នុងការគ្រប់គ្រងហើយធានាថាវាអាចដំណើរការបានយ៉ាងល្អ។ ដើម្បីឱ្យមានការគ្រប់គ្រងបានល្អគេត្រូវប្រើ Rack System សម្រាប់រក្សាទុកឧបករណ៍ Networking Devices និងម៉ាស៊ីន Server

មាន៣ជំហានបង្ហាញពីគំរូដែលគេនិយមប្រើក្នុងការដំឡើងប្រព័ន្ធ network

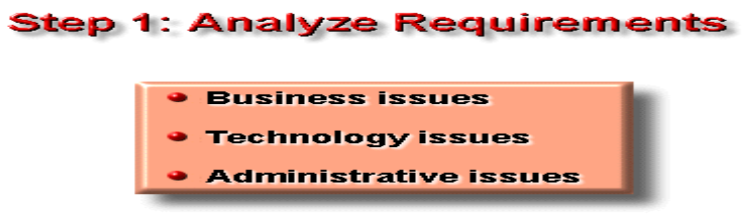


ជំហានទី១: វិភាគលើតម្រូវការ

នៅក្នុងវិធីសាស្ត្រនៃការបង្កើតនៃ network គេត្រូវធ្វើការវិភាគទៅលើតម្រូវការនៃ network និងអ្នកប្រើប្រាស់។ យើងត្រូវគិតទៅលើចំនួននៃអ្នកប្រើប្រាស់ដែលមានការប្រែប្រួល។

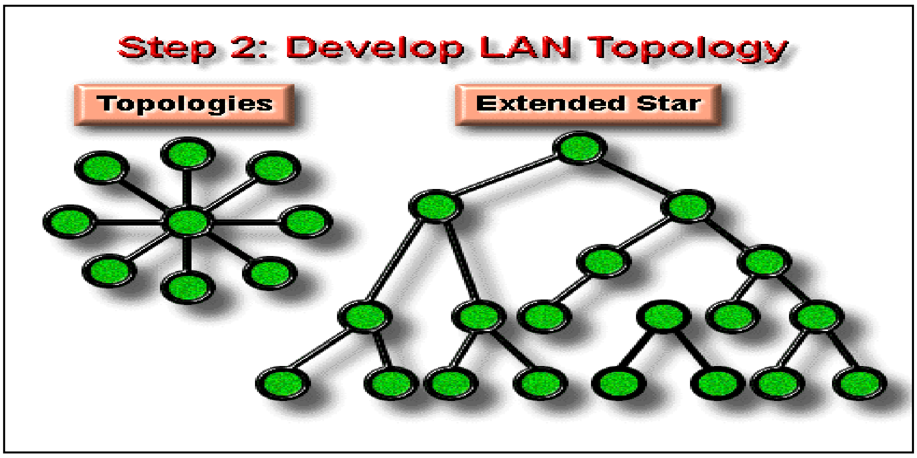
ឧទាហរណ៍

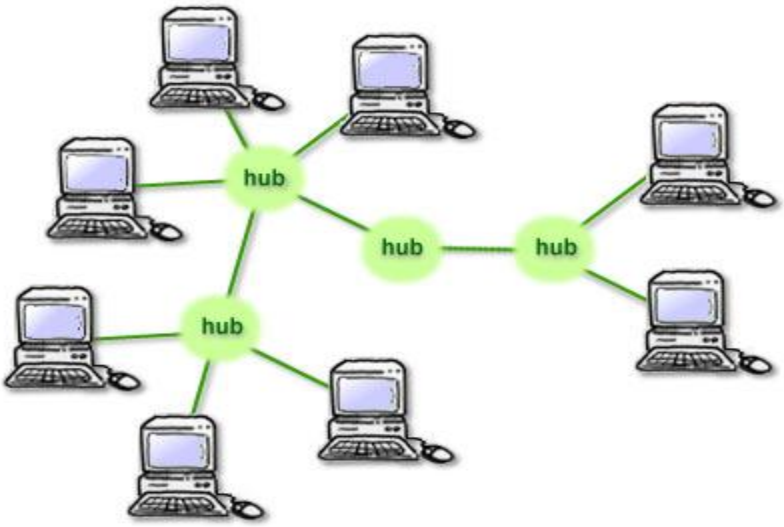
ប្រសិនបើប្រព័ន្ធ network មួយបានប្រើប្រាស់នូវ Applications ដើម្បីធ្វើការបញ្ជូននូវសំឡេងនិងវីដេអូតាមប្រព័ន្ធ network ។ ដូច្នេះវាទាមទារឱ្យមាន Bandwidth កម្រិតខ្ពស់។



ជំហានទី២:ការបង្កើតនៃរូបរាងរបស់ LAN

នៅពេលយើងបានដឹងថា Star ឬ Extended start បានប្រើប្រាស់នូវ Ethernet 802.3 CSMA/CD ។ រូបរាងនៃ network នេះកំពុងត្រូវបានប្រើប្រាស់យ៉ាងទូលំទូលាយសព្វថ្ងៃនេះ។

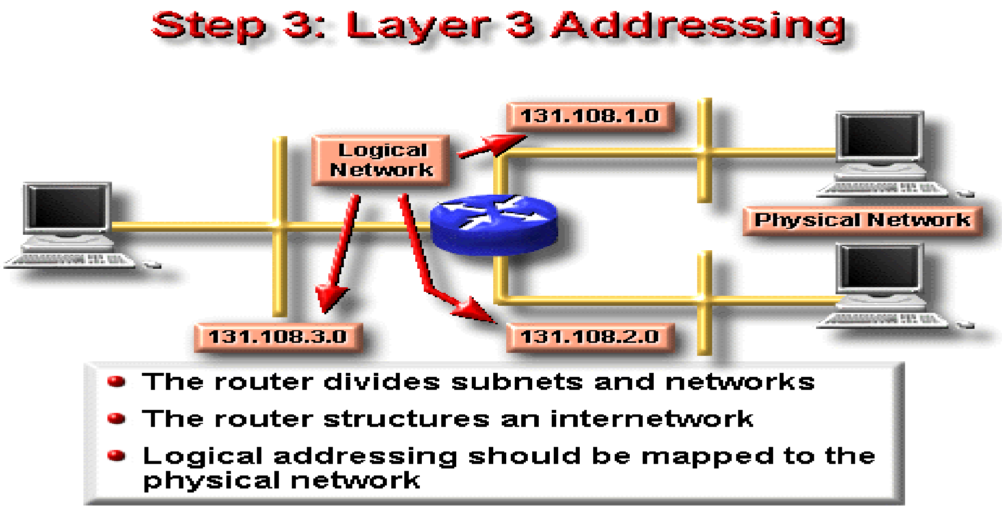




ជំហានទី៣:ការកំណត់ Address នៃ Layer 3

Router អាចឱ្យយើងប្រើប្រាស់នូវបណ្ដាញ network បានកាន់តែទូលំទូលាយពីព្រោះថាវាដើរតួនាទីជា Firewall ដើម្បីទប់ស្កាត់ការ boroadcast ។ ជំហានចុងក្រោយក្នុងការបង្កើត LAN គេត្រូវកំណត់ឱ្យបានច្បាស់លាស់នូវ IP addresses ជាមួយ network នេះ។ គេប្រើ Router ដូចខាងក្រោម:

- ដើម្បីចែក network ជា subnet នឹង network
- សម្រាប់បង្កើតរចនាសម្ព័ន្ធនៃ Internetwork ឬ internetworking
- សម្រាប់ភ្ជាប់ network ពីរឬច្រើន។ ចំពោះរូបរាងនៃ network មួយត្រូវការនូវ network ដែលជា logical network



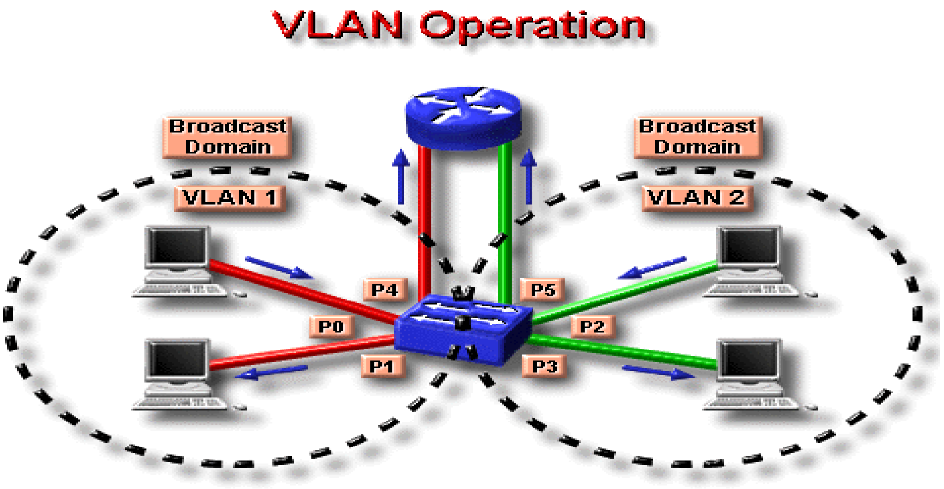
៣-៨-១- ការបង្កើត VLAN

ដោយការប្រើប្រាស់នៃ VLAN(Virtual LAN) នោះធ្វើឱ្យចរាចរណ៍នៃ broadcast ត្រូវតែមានដែលកំណត់នៅក្នុង VLAN មួយហើយវាបង្កើតបានជាដែនកំណត់នៃ broadcast ឱ្យកាន់តែតូច។ VLAN ត្រូវបានប្រើប្រាស់ដើម្បីផ្ដល់ឱ្យនូវសុវត្ថិភាពដោយបង្កើតបាននូវក្រុមនៃ VLAN ទៅតាមតួនាទីរបស់វា។

ទំហំនៃដែនកំណត់នៃ broadcast មានទំហំកាន់តែតូចហើយការប្រើប្រាស់នៃ Router ដើម្បីទប់ស្កាត់នូវ Broadcast នេះ។ ប្រសិនបើ VLAN1 បង់បញ្ជូនទៅឱ្យ VLAN2 ដូច្នេះការប្រើប្រាស់វាមានសុវត្ថិភាព។

៣-៨-១-២- ដំណើរការរបស់ VLAN

នៅក្នុងឧទាហរណ៍នេះ Port ដែលទាក់ទងត្រូវបានគេប្រើសម្រាប់អនុវត្តនូវការកំណត់របស់ VLAN ។ Port P0 P1 នឹង PC4 ត្រូវបានគេប្រើប្រាស់ដើម្បីផ្តល់ទៅឱ្យ VLAN1។ VLAN 2 មាន Port P2 P3និង P5។



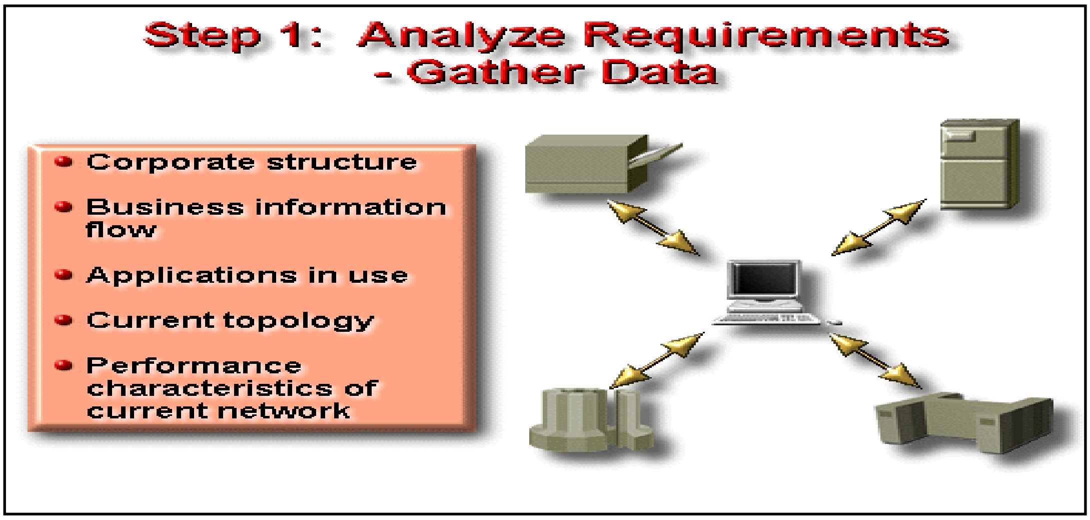
៣-៩- ការប្រមូលទិន្នន័យនិងការវិភាគលើតម្រូវការរបស់ប្រព័ន្ធ Network

ជំហានដំបូងគឺការប្រមូលព័ត៌មានដែលមានការទាក់ទងទៅ នឹងរចនាសម្ព័ន្ធនៃសាជីវកម្ម ។ នៅដំណាក់កាលចុងក្រោយនៃការបង្កើតត្រូវតែឆ្លើយតបទៅតាមតម្រូវការរបស់រចនាសម្ព័ន្ធនៃសាជីវកម្ម។ ដើម្បីប្រមូលនូវទិន្នន័យដែលយើងត្រូវអនុវត្តដូចខាងក្រោមនេះ។

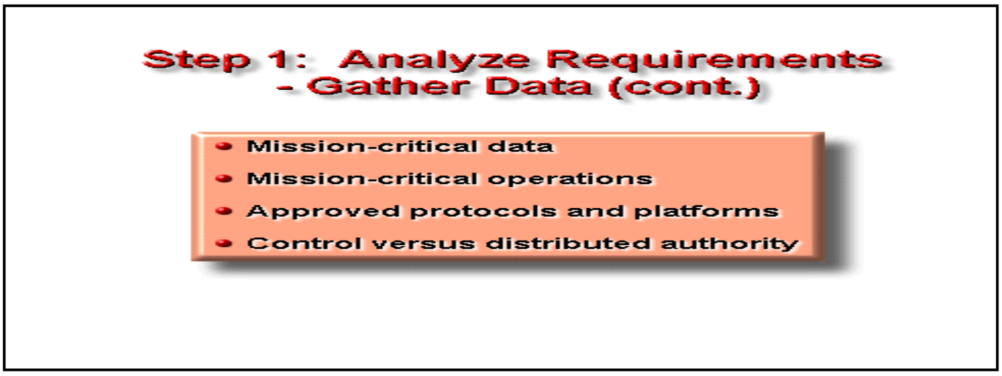
យើងត្រូវពិភាក្សាជាមួយអ្នកប្រើប្រាស់ឱ្យបានច្រើនដងដែលនៅក្នុងនោះ យើងត្រូវរកឱ្យឃើញនូវទីតាំងនៃភូមិសាស្ត្រ Applications ដែលគេកំពុងតែប្រើប្រាស់នៅក្នុងគម្រោងដែលមាននៅថ្ងៃខាងមុខ។

ក្រោយពេលដែលយើងបានប្រមូលព័ត៌មានបានរួចរាល់ហើយ ដែលទាក់ទងជាមួយនិងរចនាសម្ព័ន្ធនៃសាជីវកម្ម បន្ទាប់មកយើងត្រូវដឹងពីប្រភពលំហូរព័ត៌មាននៅក្នុងក្រុមហ៊ុន។ យើងត្រូវដឹងពីប្រភពព័ត៌មានដែលបានចែកចាយនឹងអ្នកដែលប្រើប្រាស់ទិន្នន័យនោះ។ យើងត្រូវតែស្វែងយល់ឱ្យបានច្បាស់លាស់ថាតើអ្នកប្រើប្រាស់ណាមួយអាចជួយយើងក្នុងការបង្កើត internetwork។ យើងត្រូវតែដឹងពីប្រភពនៃព័ត៌មានដែលបានពីខាងក្រៅ។

ឧទាហរណ៍ការប្រើប្រាស់នូវទិន្នន័យបានមកពី Internet ជាដើម។ យើងត្រូវស្វែងយល់ឱ្យបានស៊ីជម្រៅពីដំណើរការរបស់ប្រព័ន្ធ network ណាមួយដែលមានស្រាប់។ បើសិនជាយើងមានពេលគ្រប់គ្រាន់ យើងត្រូវវិភាគទៅលើដំណើរការរបស់ប្រព័ន្ធ internetwork ដែលមានស្រាប់។ ផ្នែកដ៏សំខាន់បំផុតក្នុងការបង្កើត internetwork គឺត្រូវតែស្វែងយល់ឱ្យបានច្បាស់លាស់ពីតម្រូវការរបស់អតិថិជន។



យើងត្រូវតែធ្វើយ៉ាងណាឱ្យដឹងថាអ្នកណាក្នុងក្រុមហ៊ុនមានសិទ្ធគ្រប់គ្រងទៅលើ Address ការដាក់ឈ្មោះ ការជ្រើសរើសយករូបរាង ការ Configure លើប្រព័ន្ធជាដើម។ នៅក្នុងក្រុមហ៊ុនខ្លះមានផ្នែកការគ្រប់គ្រងព័ត៌មានវិទ្យា(MIS)ដែលគ្រប់គ្រងទៅលើផ្នែកទាំងអស់នោះ។ មានក្រុមហ៊ុនខ្លះទៀតគេបានធ្វើការចែកនូវMISទៅជាផ្នែកតូចៗជាច្រើនទៀតហើយគេបានផ្តល់ឱ្យនូវសិទ្ធគ្រប់គ្រងទៅតាមផ្នែកនីមួយៗ។



៣-១០- វិភាគទៅលើតម្រូវការ

ដើម្បីវិភាគទៅលើតម្រូវការរបស់ប្រព័ន្ធ internetwork នោះយើងត្រូវតែវិភាគទៅលើការធ្វើជំនួញរបស់អតិថិជននឹងគោលដៅបច្ចេកទេសជាច្រើនទៀត។

- តើ Applications ថ្មីជាច្រើនដែលបាននិងត្រូវបានគេប្រើយ៉ាដូចម្តេច?
- តើប្រព័ន្ធ network ថ្មីជាច្រើននិងត្រូវបានគេចូលប្រើយ៉ាងដូចម្តេច?
- តើដូចម្តេចហៅថាលក្ខខណ្ឌទទួលបានជោគជ័យ?
- តើអ្នកអាចដឹងតាមវិធីណាថាបង្កើតថ្មីទទួលបានជោគជ័យ?

យើងត្រូវវិភាគទៅលើអ្វីត្រូវតែមានជាស្រេចដែលនៅក្នុងនោះមានដូចជា:

-Throughput

- រយៈពេលនៃការឆ្លើយតប

- ការចូលប្រើធនធាន

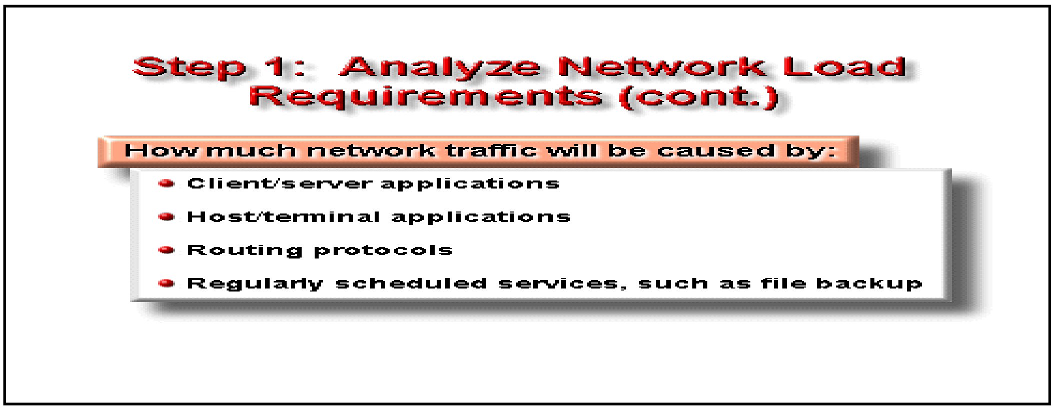
គ្រប់អតិថិជនទាំងអស់បានឱ្យនិមយន័យនៃតម្រូវការផ្សេងៗគ្នា។ តម្រូវការជាស្រេចត្រូវបានបង្កើតឡើងដោយបន្ថែមនូវធន ធានជាច្រើនទៀត។ ធនធានមានតម្លៃកាន់តែថ្លៃ នោះប្រព័ន្ធ Internetwork បានធ្វើឱ្យការបង្កើតឡើងដើម្បីផ្តល់ឱ្យនូវតម្រូវការ ជាស្រេចកាន់តែប្រសើរឡើងហើយចំពោះតម្លៃវិញមិនជាថ្លៃនោះទេ។

៣-១០-១- ការវិភាគទៅលើកត្តាដែលបណ្តាលឱ្យមានចរាចរណ៍ក្នុងប្រព័ន្ធ Network

នៅពេលដែលយើងចាប់ផ្តើមវិភាគទៅលើតម្រូវការផ្នែកបច្ចេកទេសរបស់អតិថិជន យើងត្រូវដឹងអំពីប្រភេទ នៃ applications និងប្រភេទនៃ Protocol ដែលបណ្តាលឱ្យមាននូវចរាចរណ៍នៅក្នុងប្រព័ន្ធ network
ឧទាហរណ៍

នៅពេលដែលយើងបានភ្ជាប់នូវ Node មួយទៅក្នុងប្រព័ន្ធ network គឺនៅពេលនោះទំហំរបស់ចរាចរណ៍ កាន់តែមានទំហំធំជាងមុន។ ដើម្បីបានដឹងពីចរាចរណ៍របស់ប្រព័ន្ធ network យើងត្រូវដឹងថានៅពេលណាដែល ប្រព័ន្ធ network រវល់ជាងគេនិងត្រូវកំណត់នូវសេវាដែលដំណើរការតាមការកំណត់ទុកដូចជា backup file server ជាដើម។

គោលការណ៍ៈមុនពេលយើងចាប់ផ្តើមបង្កើតប្រព័ន្ធ Internetwork ហើយព្រមទាំងការប្រើប្រាស់នូវហាដវែ្វ យើង ត្រូវតែយល់ឱ្យបានច្បាស់អំពីចរាចរណ៍របស់ប្រព័ន្ធ network ។



៣-១០-២- ការវិភាគទៅលើតម្រូវការ -Applications ដែលបណ្តាលឱ្យមានចរាចរណ៍ធំ

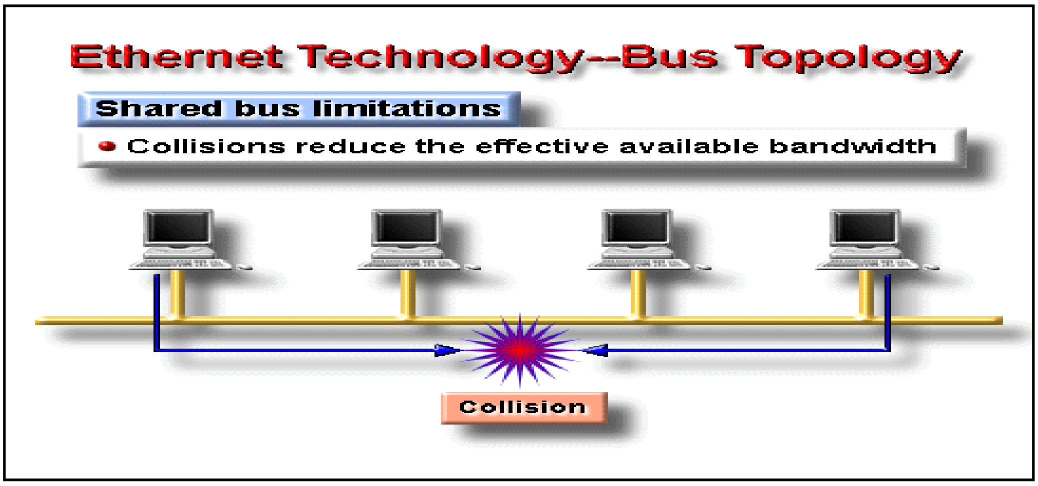
Network applications បានបង្កើតឱ្យមានចរាចរណ៍កាន់តែធំ។ នេះគឺជាតារាងមួយនៃ Aplications ដែលបណ្តាលឱ្យមាននូវការកកស្ទះ(Congestion) ដូចខាងក្រោមៈ

- ការចូលប្រើ Internet

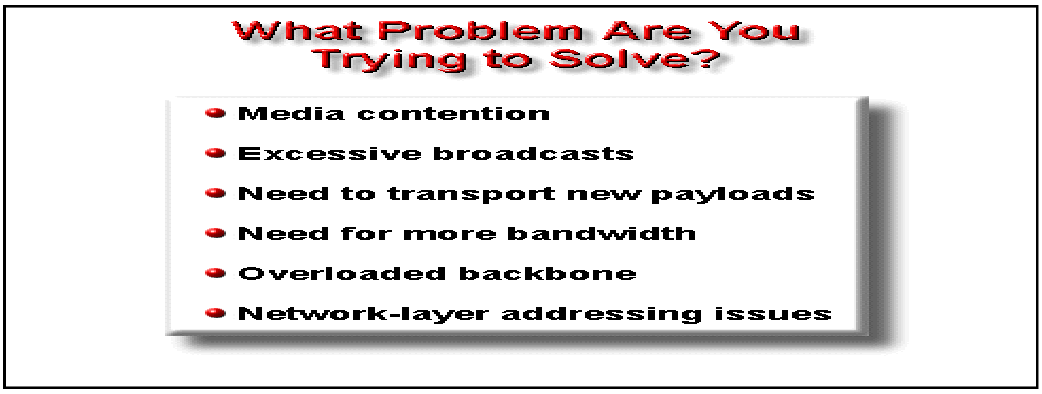
- កុំព្យូទ័រដែលប្រើ Software ពីចម្ងាយ
- ការបញ្ជូននូវរូបភាពវីដេអូ
- ការប្រើប្រាស់នូវប្រព័ន្ធ Database កណ្តាល
- file serverសម្រាប់ដេប៉ាតឺម៉ង់

គោលការណ៍នៃការដំឡើង:យើងត្រូវដឹងពី Application ដែលបណ្តាលឱ្យមានបញ្ហាចំពោះចរាចរណ៍របស់ Network

៣-១១- បច្ចេកទេសនៃ Ethernet – ការចែក Network



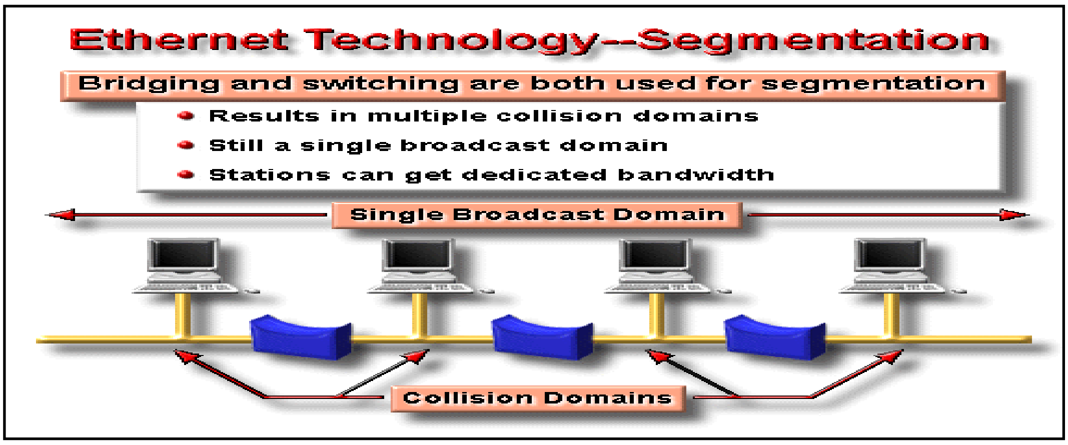
តើមានបញ្ហាអ្វីខ្លះដែលកើតឡើងក្នុងប្រព័ន្ធ Network ?



Segmentation គឺជាដំណើរការនៃការចែកដែនកំណត់នៃ Collision មួយទៅជា Collision domain ពីរឬច្រើន។

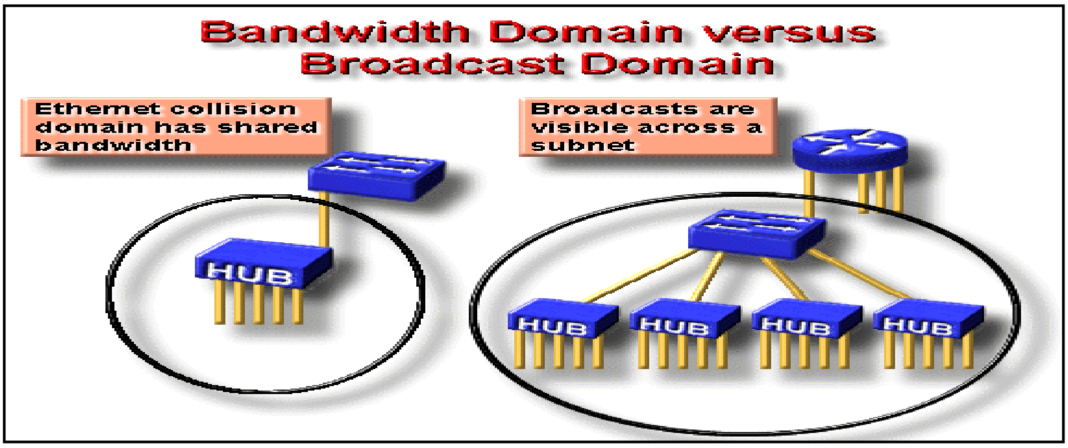
- Layer 2 bridging ត្រូវបានគេប្រើប្រាស់សម្រាប់ចែកនូវរូបរាងនៃ BUS ហើយព្រមទាំងបានបំបែកនូវ Collision domain ជាច្រើននិងបានផ្តល់លទ្ធផលឱ្យឧបករណ៍នីមួយៗមាននូវ Bandwith គ្រប់គ្រាន់សម្រាប់ប្រើប្រាស់បាន

☞ ចំណាំ: នៅក្នុងរូបរាងជា BUS ទាំងមូលមាននូវដែលកំណត់នៃ Broadcast តែមួយគត់ពីព្រោះថា ទោះបីជាយើងប្រើប្រាស់នូវ Bridge នឹង Switch ក៏ដោយ។



៣-១២- Bandwidth Domain ប្រៀបធៀបជាមួយ Broadcast Domain

ដែនកំណត់នៃ Bandwith មួយត្រូវបានគេភ្ជាប់ទៅនិង Port មួនៃ Bridge មួយឬ Switch មួយ។ នៅក្នុងករណីវាជា Ethernet Switch មួយនោះដែលកំណត់នៃ Bandwidth មួយត្រូវបានគេហៅថា Collision domain ផងដែរ។ ដែនកំណត់នៃ Broadcast មួយត្រូវតែភ្ជាប់ជាមួយ Port មួយនៃ Router មួយ។ គ្រប់ឧបករណ៍ទាំងអស់នៅក្នុងដែនកំណត់នៃ Bandwidth មួយបានប្រើប្រាស់រួមគ្នានៅក្នុងធនធានរបស់ LAN bandwidth តែមួយ។ គ្រប់ចរាចរណ៍ទាំងអស់បានមកពី Host ណាមួយនៅក្នុងដែនកំណត់នៃ Bandwidth វាជាការមើលឃើញទៅគ្រប់ Hosts ផ្សេងៗទៀត។ នៅក្នុងករណីនៃដែនកំណត់របស់ Ethernet Collision មួយនោះឧបករណ៍ចំនួនពីរអាចធ្វើការបញ្ជូននៅពេលតែមួយដែលបណ្តាលឱ្យមាន Collision កើតមានឡើង។ គ្រប់ broadcast ទាំងអស់បានមកពី Host ណាមួយនៅក្នុង broadcast domain តែមួយវាជាការមើលឃើញទៅគ្រប់ Hosts ផ្សេងៗទៀតនៅក្នុងដែនកំណត់នៃ Broadcast តែមួយ។ Broadcasts ត្រូវតែមើលឃើញចំពោះគ្រប់ Hosts ទាំងអស់នៅក្នុងដែនកំណត់នៃ broadcast តាមលំដាប់លំដោយដើម្បីបង្កើតបានជាសកម្មភាពនៃការភ្ជាប់។



៣-១៣- គោលការណ៍នៃការដំឡើងប្រព័ន្ធ Network

៣-១៣-១- ការបង្កើតខ្សែ LAN Topology

ក្រោយពីយើងបានប្រមូលនូវព័ត៌មានដែលទាក់ទងទៅនឹងប្រព័ន្ធ Network បានរួចរាល់ហើយ នោះយើងត្រូវជ្រើសរើសប្រភេទនៃរូបរាងឬគំរូនៃ LAN មួយដែលត្រូវបានបង្កើតឡើងនោះ។ ផ្នែកដ៏សំខាន់នៃការបង្កើតនៃរូបរាងនេះត្រូវបានបំបែកទៅជា៣ប្រភេទនៃ OSI Model ។

- Layer 1- Physical Layer

គោលបំណងនៃការបង្កើតៈការបង្កើតនូវ Layer នេះនៃ OSI Model ដែលមានល្បឿនលឿននិងការបង្កើតនូវសមត្ថភាពដែលអាចប្រើប្រាស់បាន។

- Layer 2- Data Link Layer

នៅក្នុង Layer នេះឧបករណ៍ដូចជា Bridge ឬ LAN Switch ត្រូវបានគេប្រើសម្រាប់ការភ្ជាប់ LAN segment តាមរយៈនៃខ្សែ។ ឧបករណ៍ដែលដំណើរការនៅក្នុង Layer នេះមានតួនាទីសម្រាប់កំណត់នូវទំហំនៃ Collision និងដែនកំណត់នៃ Broadcast ។

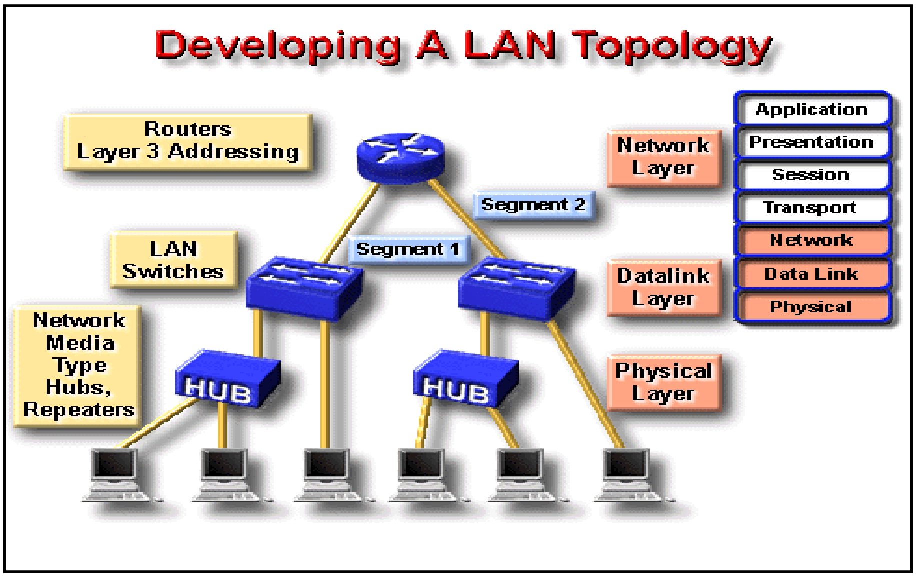
គោលបំណងនៃការបង្កើតៈ សម្រាប់បង្កើតនូវចំណុចកណ្តាលមួយដែលមាននៅក្នុងនោះរួមមាន MDFឬ IDF ដែល Host ត្រូវបានបង្កើតជាក្រុមតាមរយៈនៃ Physical Layer ដើម្បីបានទម្រង់ជា Physical LAN segment មួយ។ ការដំឡើងនូវឧបករណ៍នៃ LAN Switch ដែលបានប្រើប្រាស់នូវផ្នែកតូចៗដើម្បីកាត់បន្ថយទំហំនៃដែនកំណត់របស់ Collision ដែលកើតមានឡើង។ ការបង្កើតឱ្យមាននូវចំណុចមួយនៅ Layer 2 នៃរូបរាងនេះដែលអ្នកប្រើប្រាស់ត្រូវបង្កើតឡើងជាក្រុមទៅជា VLAN(Virtual LAN) ហើយមាននូវដែលកំណត់នៃ Broadcast តែមួយគត់។

- Layer 3- Network Layer

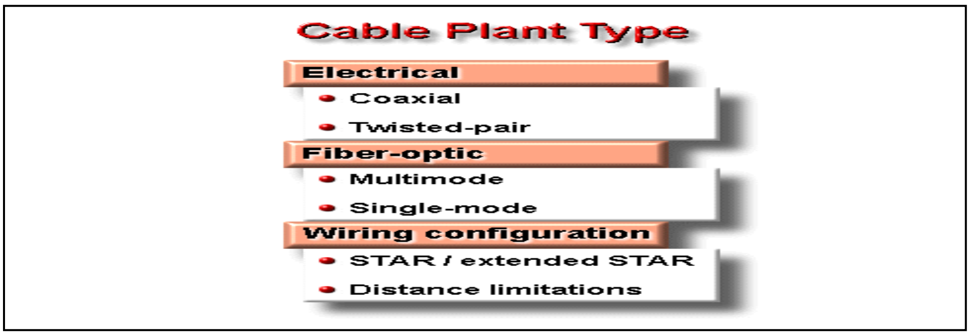
នៅក្នុង Layer នេះឧបករណ៍ដូចជា Router ត្រូវបានប្រើប្រាស់ដើម្បីបង្កើតបានជា LAN segment មួយហើយអនុញ្ញាតឱ្យមានការភ្ជាប់រវាង Segment នៅ Layer 3 ដូចជា IP address ជាដើម។

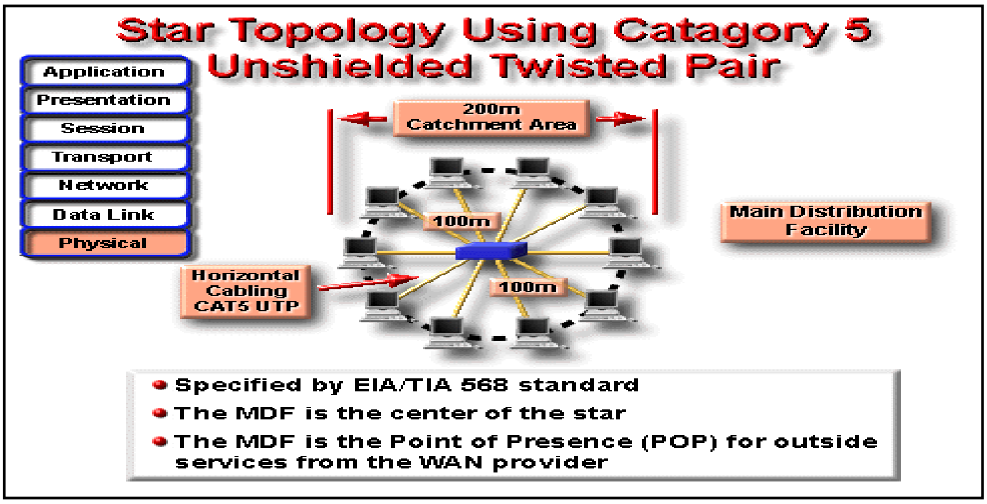
គោលបំណងនៃការបង្កើតៈ បង្កើតនូវផ្លូវមួយរវាង LAN segment ដែលបានច្រោះនូវ Data packet ។

- ចែក ARP Protocol Broadcast ដាច់ស្រឡះពីគ្នា
- ចែកឱ្យដាច់ស្រឡះពីគ្នានូវ Collision រវាង Segments.
- ច្រោះសេវានៅ layer TI 4 រវាង Segments



ប្រភេទនៃខ្សែរបស់ Network





៣-១៣-៣- Extended Star Topology

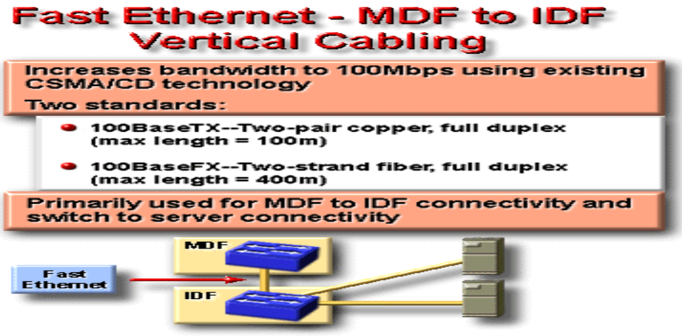
នៅក្នុងប្រព័ន្ធ Network មួយដែលកាន់តែធំជាធម្មតាវាត្រូវការនូវបន្ទប់សម្រាប់រក្សាទុកខ្សែច្រើនជាងមួយ ប្រសិនជាមានចំនួន Hosts កាន់តែច្រើនឡើងដែលត្រូវការភ្ជាប់ជា Network ប៉ុន្តែការភ្ជាប់ទៅខាងក្រៅមានចម្ងាយត្រឹមតែ១០០ម៉ែត្រប៉ុណ្ណោះចំពោះ CAT5 UTP Ethernet ។

ដោយត្រូវការបន្ថែមនូវបន្ទប់ខ្សែ(Wiring Closet)នោះតំបន់សម្រាប់ភ្ជាប់ជាច្រើនត្រូវបានបង្កើតឡើង។ បន្ទប់ខ្សែទី២ត្រូវបានផ្តល់នូវ IDF(Intermedate Distrubution Facilities)។ ស្តង់ដា EIA/TIA 568 បានបង្កើតឡើងនោះមាន IDFs ត្រូវបានភ្ជាប់ទៅ MDF ដោយប្រើប្រាស់នូវVC(Vertical Cabling)។ VC នេះគឺជាប្រភេទនៃ Fiber Optics ពីព្រោះថាដោយសារតែ Fiber Optic អាចប្រើប្រាស់បានចម្ងាយកាន់តែឆ្ងាយ។ នៅក្នុង MDFs និង IDFs ផ្នែកដ៏សំខាន់ផ្សេងៗគ្នាមានការប្រើប្រាស់ Patch Panel មួយផ្សេងទៀតដែលជា VCC(Vertical Cross Connect)។ VCC នេះត្រូវបានប្រើប្រាស់ដើម្បីភ្ជាប់ IDFs ជាច្រើនទៅ MDF កណ្តាល។ ប្រវែងនៃ VC គឺជាប្រភេទនៃខ្សែដែលមានប្រវែងវែងជាង១០០ម៉ែត្រចំពោះ CAT 5 UTP ចំពោះ Fiber Optic វិញត្រូវបានប្រើប្រាស់ជាធម្មតា។

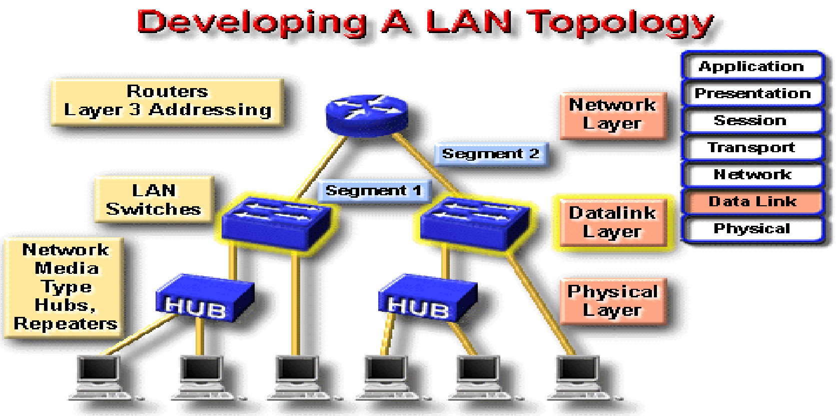
៣-១៤- ការភ្ជាប់ពី Fast Ethernet-MDF ទៅ IDF

Fast Ether គឺជា Ethernet ដែលត្រូវបានបង្កើតឡើងដែលមានល្បឿនរហូតដល់ 100 Mbps ។ ប្រភេទនេះបានប្រើប្រាស់នូវស្តង់ដា Ethernet ដែលមានរាងជា BUS ដែលមាន Broadcast ដែលយើងប្រើនូវ 10 base T ។

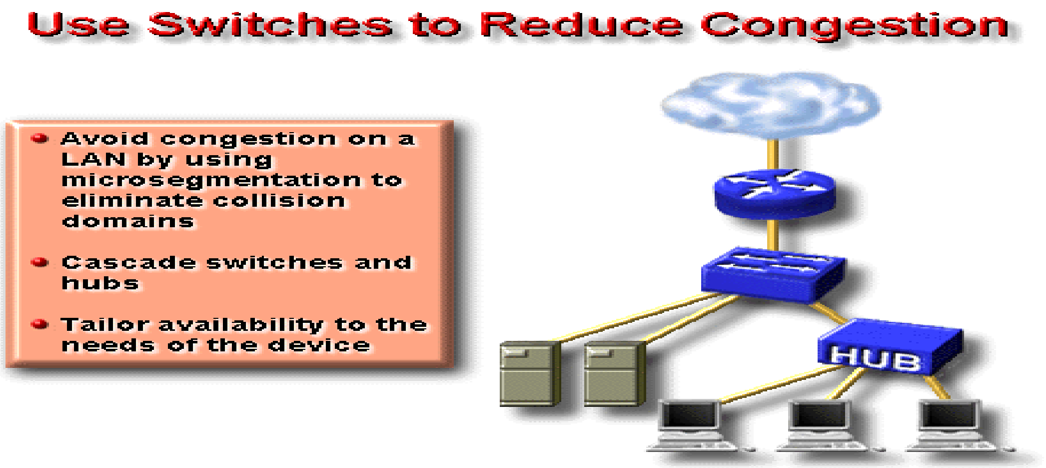
CSMA/CD Method គឺជា Media Access Control (MAC) មួយ។ ស្តង់ដា Fast Ethernet មាន៤ផ្សេងៗគ្នាដូចជា Copper-Pair Wire (100Base TX) នឹង Fiber (100Base FX) ហើយគ្មាន Fast Ethernet ដែលប្រើខ្សែ Coaxial នោះទេ។



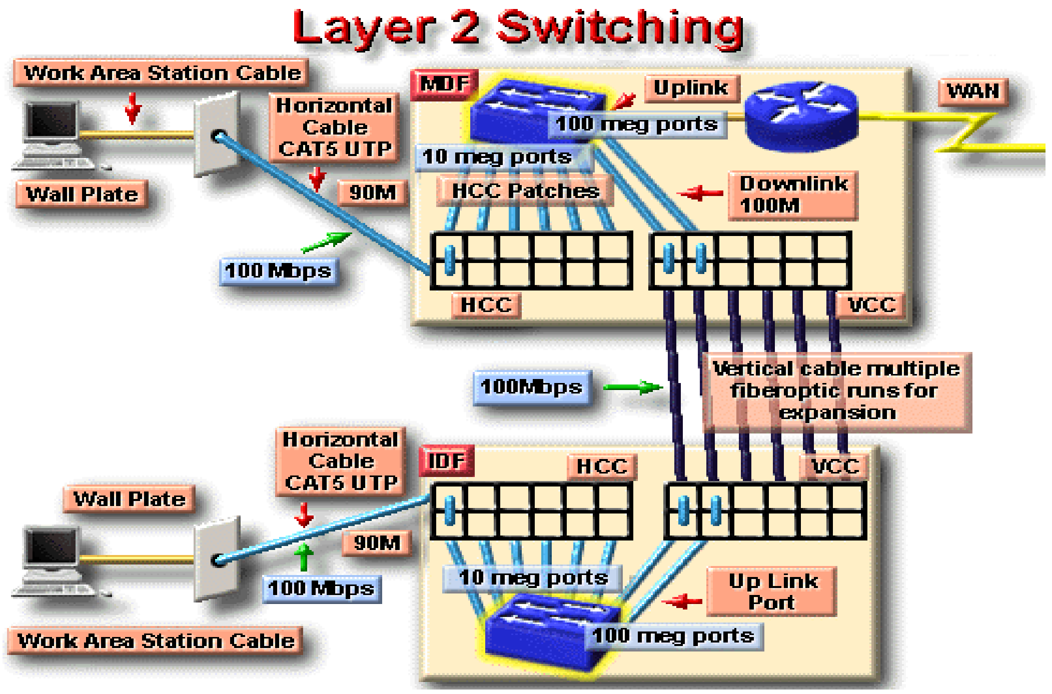
LAN Swith ដែលមានពីរស្រទាប់នៃ OSI Model



៣-១៤-១- ការប្រើប្រាស់ Switches ដើម្បីកាត់បន្ថយការកកស្ទះ (Congestion)

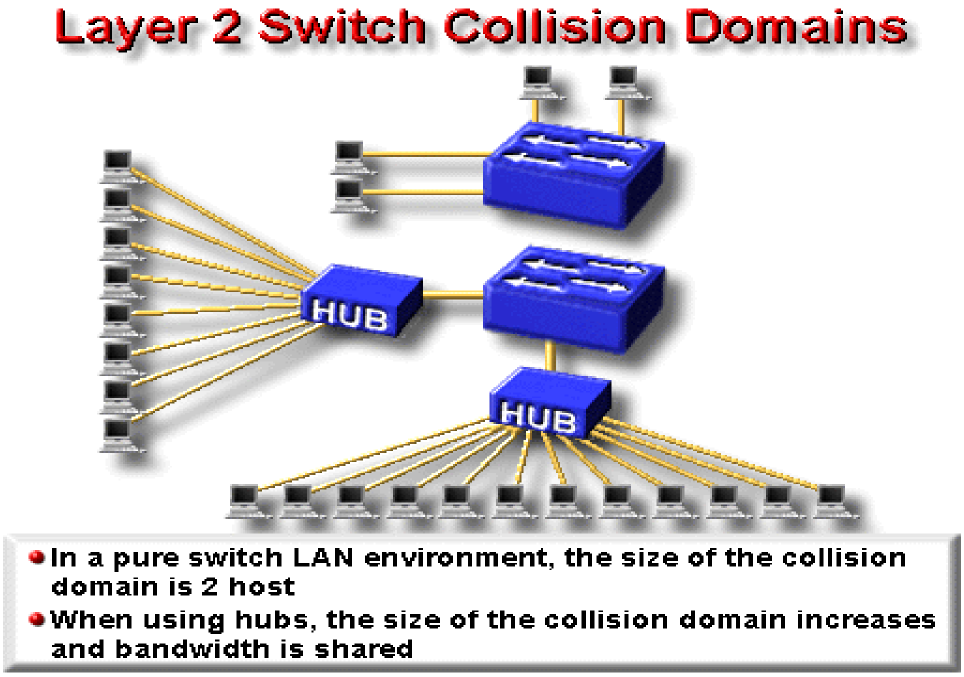


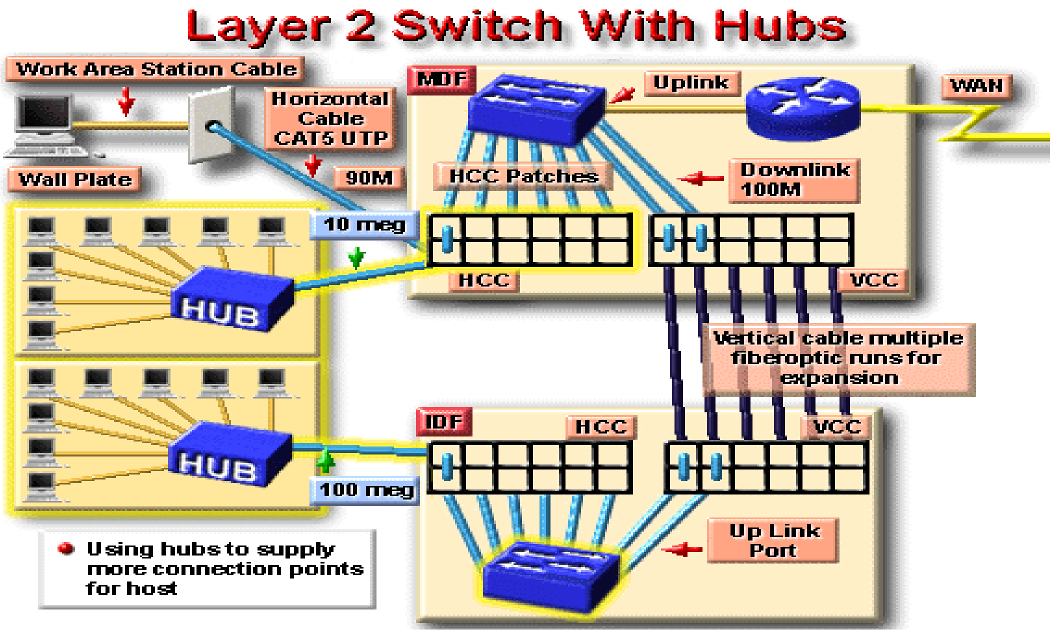
Microsegmentation មានន័យថាការប្រើប្រាស់នូវ Bridge និង Switch ដើម្បីឱ្យដំណើរការរបស់ Workgroup ឬ Backbone network បានល្អប្រសើ។ បើ Switch ត្រូវបានប្រើប្រាស់ជាមួយ Hub នោះដើម្បីឱ្យដំណើរការរបស់ប្រព័ន្ធ Network បានល្អប្រសើរសម្រាប់អ្នកប្រើប្រាស់ចាំបាច់នឹង Server ។



៣-១៤-២- Layer 2 Switch Collision Domains

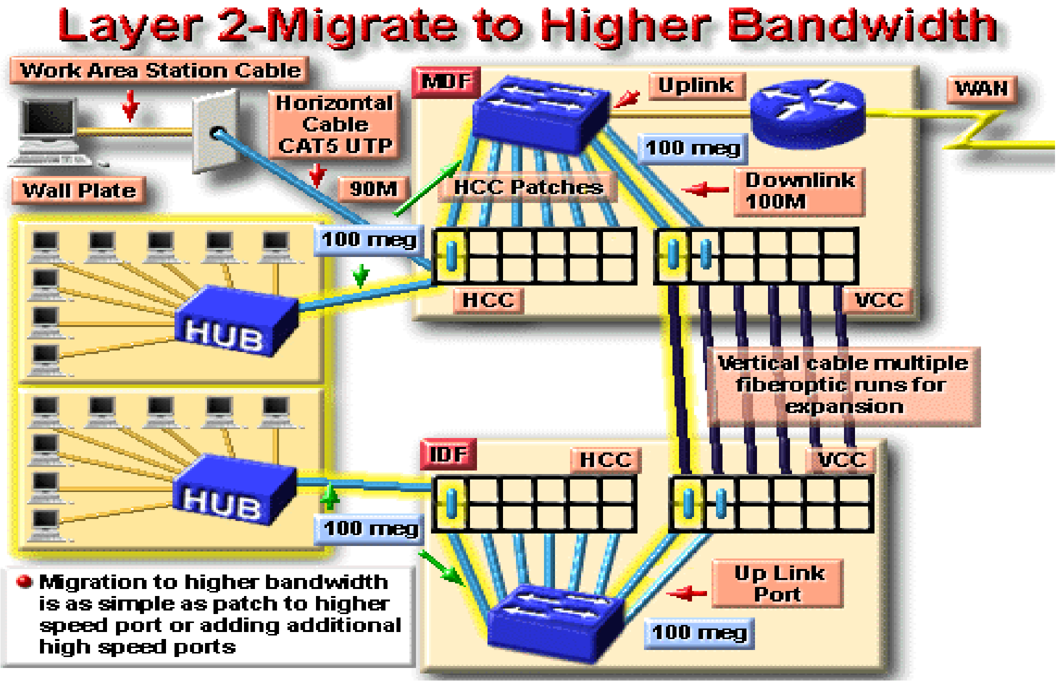
ដើម្បីកំណត់ពីទំហំនៃដែលកំណត់របស់ Collision មួយយើងត្រូវដឹងពីចំនួន Hosts ដែលត្រូវភ្ជាប់ទៅ Port តែមួយរបស់ Switch ។ ការកំណត់នេះវាមានការទាក់ទងជាមួយនឹង Bandwidth ដែលបម្រុងទុកសម្រាប់ Host នីមួយៗ។ នៅក្នុងស្ថានភាពបែបនេះមាន Host តែមួយគត់ដែលបានភ្ជាប់ទៅ LAN switch port ។ យើងត្រូវតែ កំណត់នូវទំហំនៃដែលកំណត់របស់ Collision ចំនួនពីរ(Source Host នឹង Destination Host)។ ដោយសារតែទំហំនៃដែនកំណត់របស់ Collision កាន់តែតូចនោះវាគ្មាន Collision កើតឡើងនោះទេនៅពេលដែល Host ពីរបានកំពុងតែបញ្ជូនឱ្យគ្នាទៅវិញទៅមក។





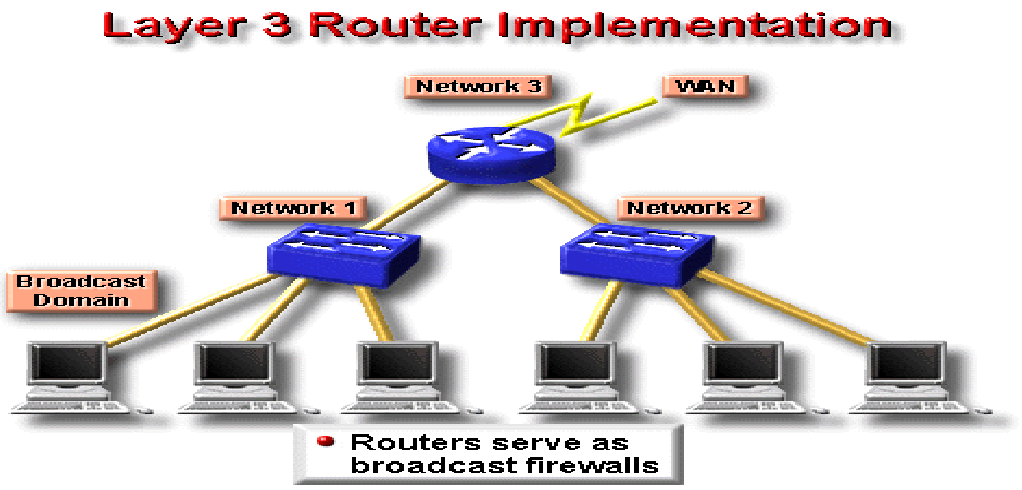
៣-១៤-៣- Layer 2 Migration ដើម្បីឱ្យបាន Bandwidth ខ្ពស់

Migration គឺជាការបញ្ចូលគ្នានៃការប្រើប្រាស់ដើម្បីឱ្យការប្រើប្រាស់បានល្អប្រសើរ។ យើងត្រូវការភ្ជាប់ Host មួយទៅ Port មួយរបស់ Switch ។ នៅពេលដែលប្រព័ន្ធ Network មួយកាន់តែធំនោះតម្រូវការនៃ Bandwidth ក៏កាន់តែធំដែរ។ VCC ត្រូវបានគេប្រើប្រាស់ដើម្បីភ្ជាប់ MDF ជាមួយ IDF ។ ដូច្នេះគេត្រូវការនូវ bandwidth សម្រាប់ Port នោះចំនួន 100Mbps ហើយនៅពេលដែលយើងបានប្រើប្រាស់នូវ Switch ដែលមានពីរស្រទាប់នោះវាបានផ្តល់ឱ្យយើងនូវ Bandwidth គ្រប់គ្រាប់សម្រាប់ Migration ។ នៅក្នុងខ្សែ HC(Horizontal Cabling)bandwidth បានកើនឡើងហើយការផ្លាស់ប្តូរពី HCC ទៅជា Port មួយនៃ Switch ដែលមានល្បឿន 100 Mbps។ ការកំណត់នូវទំហំនៃ layer 2 LAN switch វាមានសារៈសំខាន់ណាស់ដើម្បីឱ្យមាន bandwidth ដល់ 100 Mbps port សម្រាប់ Migration ដែលត្រូវការ bandwidth កាន់តែធំ។



៣-១៤-៤- Layer 3 Routing Implementation

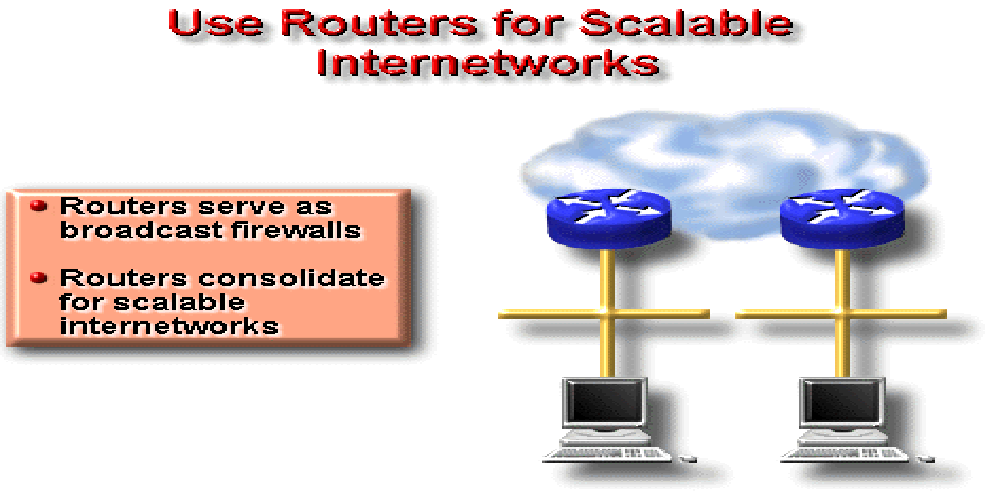
ការប្រើប្រាស់ឧបករណ៍ដែលមាន៣ស្រទាប់ដូចជា Router បានអនុញ្ញាតឱ្យមានការបំបែកជាផ្នែកនៃ LAN នៅក្នុងប្រព័ន្ធ network រួមមានទាំងផ្នែករូបរាងនិងផ្នែកខាងក្នុង។ Routers ត្រូវបានប្រើប្រាស់សម្រាប់ភ្ជាប់ទៅជាមួយ WAN(Wide Area Network) ដូចជា Internet ជាដើម។



៣-១៤-៥- ការប្រើប្រាស់ Router ដើម្បីឱ្យ Internetworks កាន់តែធំ

បច្ចេកវិទ្យា Routing បានប្រោះនូវការ Broadcast នៃ Data Link នឹង Multicast ។ ដោយសារតែមានការបន្ថែមនូវ Port របស់ Router ដែលមានការបន្ថែមនូវ Subnet ឬ Network Address នោះប្រព័ន្ធ Internetwork ត្រូវបានចែកចេញជាផ្នែកៗទៅតាមតម្រូវការ។ Network Protocol AddressingនឹងRouting បានផ្តល់នូវការបង្កើតប្រព័ន្ធមួយដែលអាចពង្រីកបាន។ នៅពេលធ្វើការសម្រេចចិត្តថាតើត្រូវប្រើប្រាស់នូវ RouterឬSwitch នោះយើងត្រូវដឹងតើមានអ្វីកើតមានឡើងនៅពេលដែលយើងកំពុងតែព្យាយាមដោះស្រាយបញ្ហានោះ ?

បើសិនជាបញ្ហារបស់អ្នកជាបញ្ហានៃ Protocol វិញនោះ ទាក់ទងទៅនឹងបញ្ហាកកស្ទះ។ Router ត្រូវបានប្រើប្រាស់សម្រាប់ដោះស្រាយនូវរាល់បញ្ហាដែលមានបរិមាណនៃចំនួន Broadcast ច្រើនហើយនិង Protocol ដែលមិនអាចពង្រីកបាន បញ្ហាផ្នែកសុវត្ថិភាព បញ្ហាផ្នែកការកំណត់ IP address ។ ទោះបីជាយ៉ាងណាក៏ដោយ Router មានតម្លៃថ្លៃហើយមានលំបាកក្នុងការ Configure ជាង Switches ។

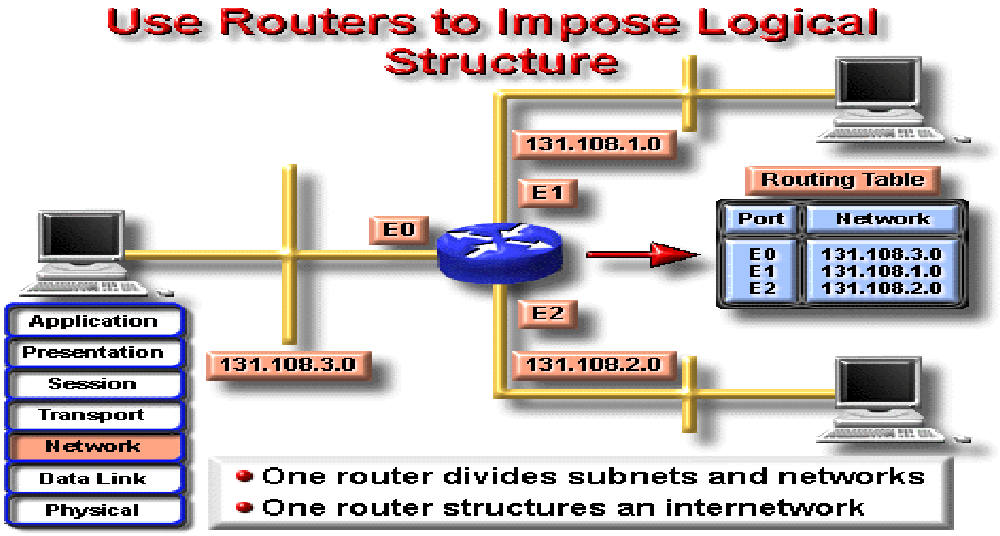


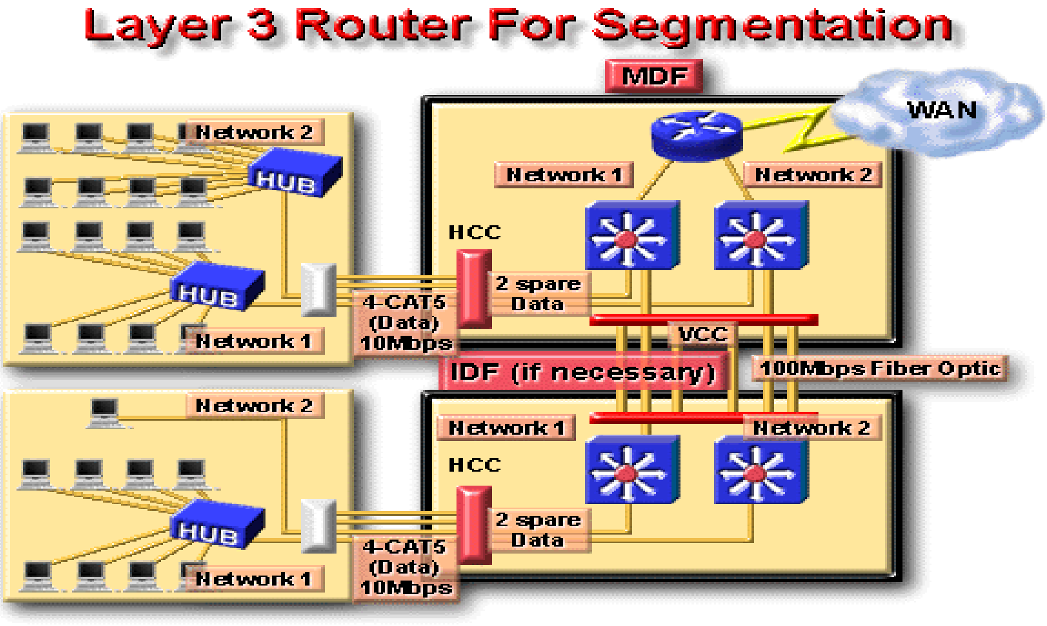
៣-១៤-៦- ការប្រើប្រាស់ Router ដើម្បីឱ្យរចនាសម្ព័ន្ធផ្នែកខាងក្នុងបានល្អប្រសើរ

Router ត្រូវបានប្រើប្រាស់ដើម្បីធ្វើឱ្យមានលទ្ធភាពក្នុងការពង្រីកឱ្យកាន់តែធំបានល្អពីព្រោះវាត្រូវបានប្រើ Firewall សម្រាប់ការពារកុំឱ្យមាននូវ Broadcast ។ លើសពីនេះទៅទៀត Router បានធ្វើឱ្យមាននូវសមត្ថភាពនៃការពង្រីកបានកាន់តែប្រសើរដោយសារតែ Layer 3 ។

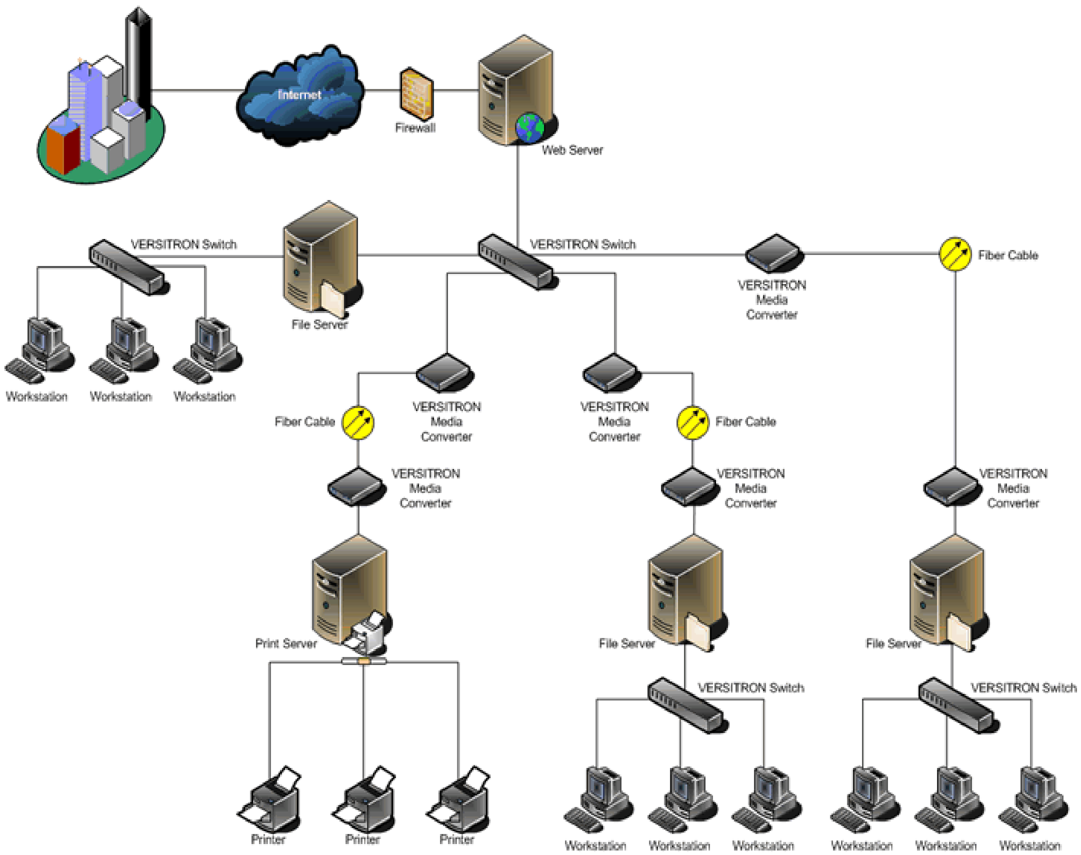
ឧទាហរណ៍ IP subnet បានបន្ថែមនូវរចនាសម្ព័ន្ធទៅឱ្យ Addresses ។ ដោយសារតែ Bridge និង Switches មិនបានស្គាល់នូវAddress បាននោះទេ។ ដូច្នេះវាបានបញ្ជូនចេញទៅគ្រប់Portទាំងអស់។

ជាមួយនិង Routers Hosts បានប្រើនូវ Protocol ដែលបាននូវ Network Layer អាចដោះស្រាយបញ្ហាក្នុងការរក Address នៃ Host ផ្សេងៗទៀតដោយមិនបញ្ជូនទៅឱ្យជា Broadcast នោះទេ។ បើសិនជាអាស័យដ្ឋានរបស់គោលដៅជា IP address វិញនោះការបញ្ជូន Host អាច Encasulate ចំពោះ Packet នៅក្នុង Data Link header មួយនិងបានបញ្ជូន Unicast Frame ដោយផ្ទាល់ទៅឱ្យឧបករណ៍មួយ។





៣-១៤-៧- ការ Design Network ដោយប្រើ Fiber Optic

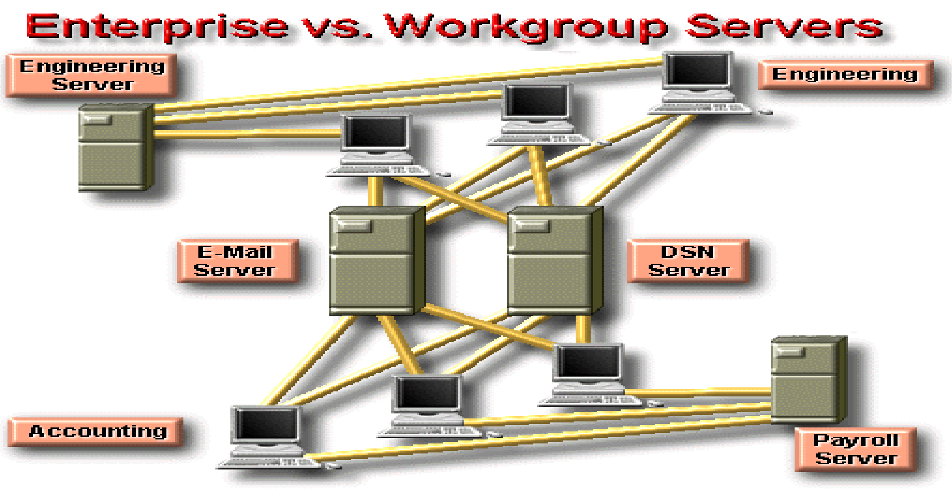


File Servers and Traffic Patterns

៣-១៤-៧-១- Enterprise ប្រៀបធៀបជាមួយ Workgroup Servers

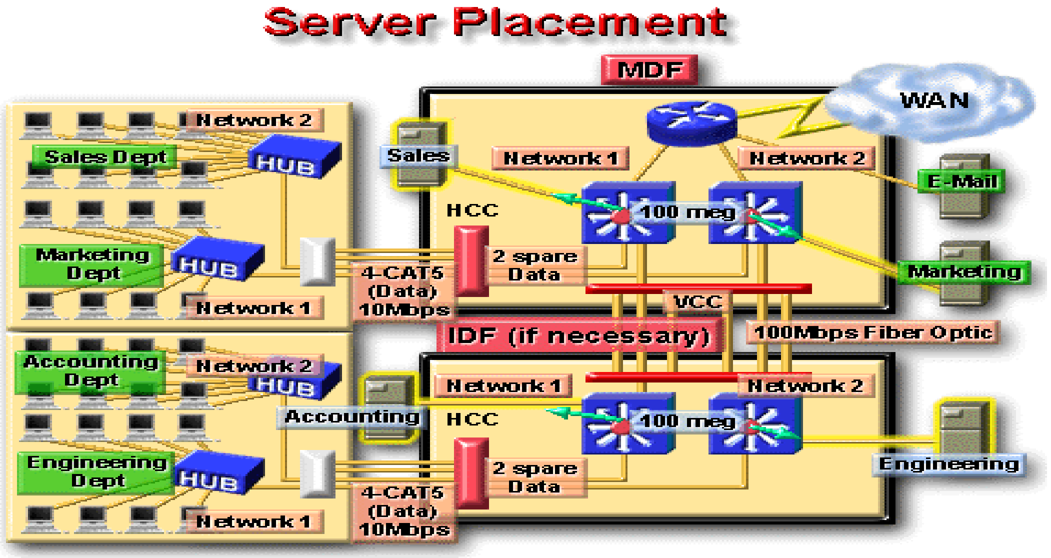
ដើម្បីធ្វើការដំឡើងប្រព័ន្ធ Network មួយឱ្យទទួលបានជោគជ័យនោះ យើងត្រូវតែយល់ឱ្យបានច្បាស់ពីចរាចរណ៍ទិន្នន័យនៃប្រព័ន្ធ Network។ Application server ត្រូវបានចែកចេញជាពីរប្រភេទគឺ Enterprise Server នឹង Workgroup server។ Enterprise Server ប្រើប្រាស់សម្រាប់អ្នកប្រើប្រាស់ទាំងអស់នៅក្នុងប្រព័ន្ធ Network ទាំងមូលដូចជា E-mail server ឬ DNS server ។ ចំណែកឯ Workgroup server វិញត្រូវបានប្រើប្រាស់សម្រាប់ក្រុមនៃអ្នកប្រើប្រាស់ផ្នែកណាមួយនៃ Nerwork ។

អ្នកប្រើប្រាស់ទាំងអស់នៅក្នុងប្រព័ន្ធ Network ត្រូវការចូលប្រើចំពោះ Enterprise Server វាត្រូវតែភ្ជាប់ទៅនិង MDF។ ចរាចរណ៍ចំពោះប្រភេទនៃសេវានេះមានតែមួយគត់ដែលត្រូវតែបញ្ជូនទៅកាន់ MDF ហើយវាមិនត្រូវបានបញ្ជូនឆ្លងកាត់ Network ផ្សេងៗទៀតនោះទេ។ Workgroup server ត្រូវមានទីតាំងនៅក្នុង IDF ដើម្បីឱ្យអ្នកប្រើប្រាស់ទាំងអស់អាចចូលប្រើនូវ Application ទាំងនោះបាន។ ដោយការធ្វើការបែបនេះ ចរាចរណ៍ចំពោះ Servers ទាំងអស់នេះត្រូវតែមានមួយគត់ត្រូវបានបញ្ជូនទៅកាន់ Network ទៅកាន់ IDF នឹងមិនធ្វើឱ្យមានការប៉ះពាល់ដល់អ្នកប្រើប្រាស់ផ្សេងៗទៀតនៅក្នុងប្រព័ន្ធផ្នែកនៃ Segment ទេ។



៣-១៤-៧-២- ការកំណត់ទីតាំងនៃ Server

ប្រសិនបើ Server ត្រូវបានផ្តល់ឱ្យនូវ network ហើយវាអាស្រ័យទៅតាមតួនាទីរបស់វា។ Network Layer 2 និង ៣ត្រូវបានបង្កើតឡើងដើម្បីផ្តល់ឱ្យតាមតម្រូវ។ នៅក្នុង MDFs និង IDFs គឺ Layer 2 LAN Switch ត្រូវតែមានល្បឿនខ្ពស់គឺ 100Mbps port ដែលត្រូវប្រើសម្រាប់ Server ទាំងអស់នោះ។



សំណួរត្រួតពិនិត្យ

១-តើ MDF ជាអ្វី?

២-តើ IDF គឺជាអ្វី?

៣-តើ Server ចែកចេញជាប៉ុន្មានប្រភេទ?អ្វីខ្លះ?

៤-Broadcast domain និងBandwidth domain គឺជាអ្វី?

៥-តើ Congestion គឺជាអ្វី? ហើយដើម្បីកាត់បន្ថយ Congestion តើគេត្រូវធ្វើដូចម្តេច?

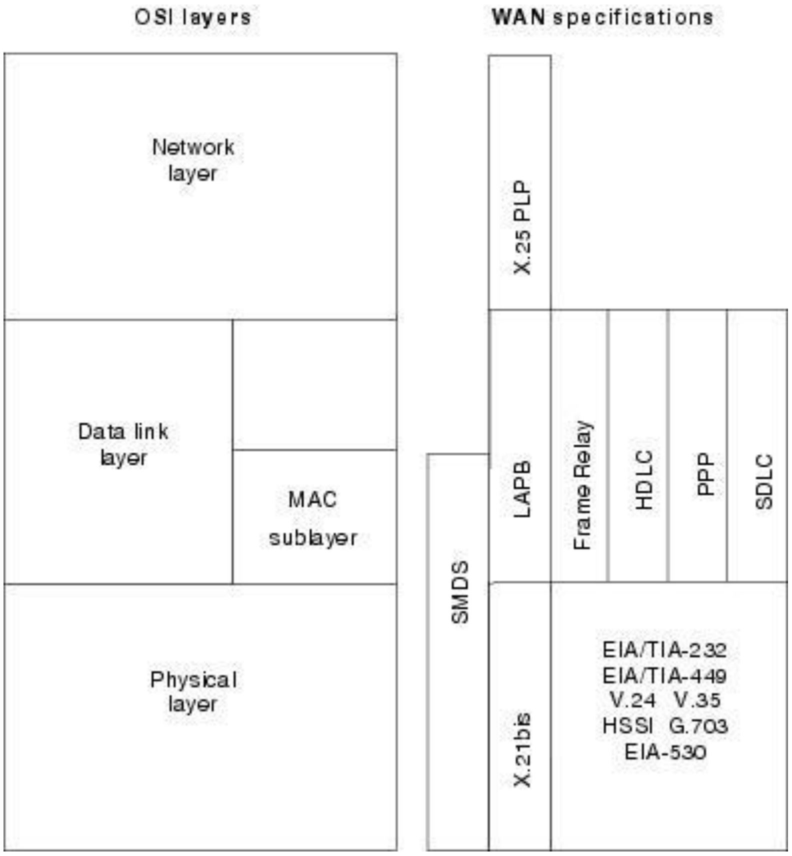
ជំពូកទី៤

WAN (Wide Area Network)

៤-១- សេចក្តីផ្តើមចំពោះ WAN Technologies

តើ WAN ជាអ្វី ?

WAN គឺជាប្រព័ន្ធបញ្ជូន Data តាមប្រព័ន្ធ Network ដែលគ្រប់ដណ្តប់លើតំបន់ដែលមានភូមិសាស្ត្រធំពាសពេញពិភពលោកតាមរយៈបណ្តាញរបស់ក្រុមហ៊ុនទូរស័ព្ទ។ WAN technologies ជាទូទៅមានតួនាទីប្រព្រឹត្តទៅនៅស្រទាប់ទីពារបស់ OSI reference model គឺ physical layer, data link layer, និង network layer ។ រូបភាពខាងក្រោមបង្ហាញពីទំនាក់ទំនងរវាង WAN technologies ដែលគេនិយមប្រើនិង OSI model ។



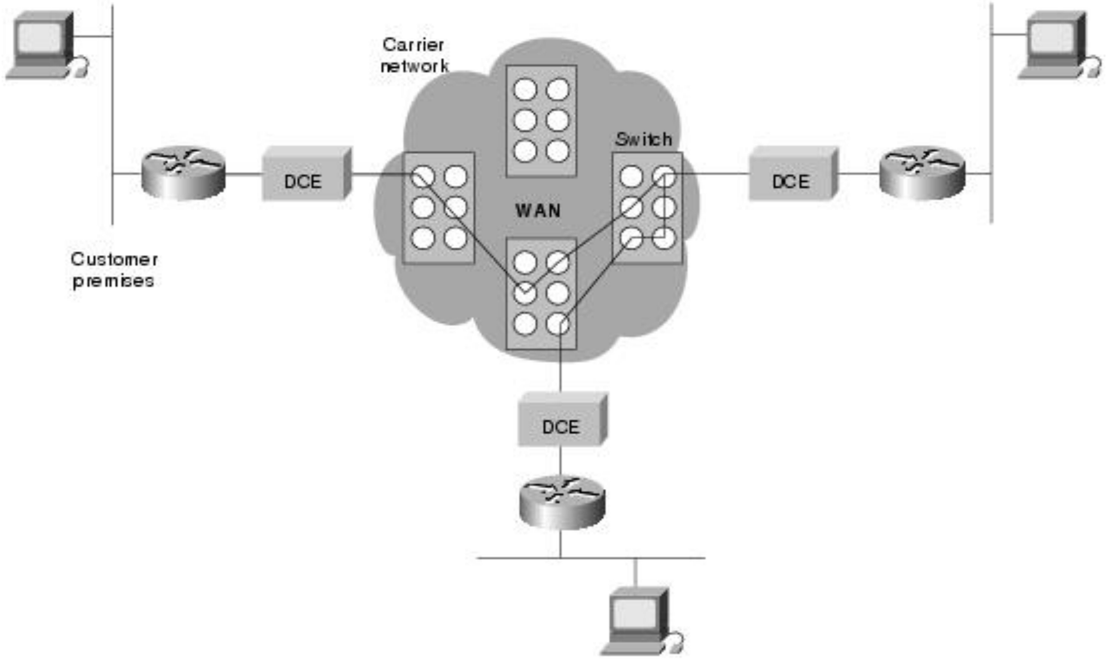
៤-២- ការភ្ជាប់ពីចំណុចមួយទៅចំណុចមួយទៀត

point-to-point link ផ្តល់ឱ្យផ្លូវបញ្ជូនដែលបានបង្កើតឡើងជាមុនតែមួយគត់ពី customer premises តាមរយៈ carrier network តែមួយគត់ដូចជាក្រុមហ៊ុនទូរស័ព្ទដែលភ្ជាប់ចំពោះ remote network មួយ។ បណ្តាញរបស់ Point-to-point ជាទូទៅត្រូវបានជួលពី carrier ហើយគេហៅថា leased lines។ ចំពោះបណ្តាញ point-to-point carrier បានជ្រើសរើសយកគូរនៃខ្សែនិង hardware ភ្ជាប់មកខ្សែទូរស័ព្ទរបស់អ្នកតែប៉ុណ្ណោះ។ សៀគ្វី

ទាំងនេះមានតម្លៃពឹងផ្អែកលើទំហំ bandwidth ដែលត្រូវការនិងចម្ងាយរវាងចំណុចពីរដែលបានភ្ជាប់គ្នា។ ការភ្ជាប់ពីចំណុចមួយមក ចំណុចមួយទៀតមានតម្លៃថ្លៃជាង shared services ដូចជា Frame Relay។ រូបភាពខាងក្រោមបង្ហាញពីការភ្ជាប់រវាងពីចំណុចមួយមកចំណុចមួយទៀតតាមរយៈWANមួយ ។

៤-១-១- Circuit Switching

Switched circuits អនុញ្ញាតឱ្យការភ្ជាប់ data ដែលអាចចាប់ផ្តើមនៅពេលដែលត្រូវការនិងផ្តាច់ការភ្ជាប់នៅពេលដែលការភ្ជាប់ត្រូវបានបញ្ចប់។ ការងារនេះវាមានលក្ខណៈដូចទៅនិងខ្សែទូរស័ព្ទដែលប្រើសម្រាប់ការប្រាស្រ័យទាក់ទងជាសំឡេង។ Integrated Services Digital Network(ISDN)គឺជាឧទាហរណ៍មួយដ៏ល្អប្រសើរចំពោះ circuit switching។ នៅពេល router មួយមាន data សម្រាប់តំបន់ឆ្ងាយ switched circuit ក៏ត្រូវបានចាប់ផ្តើមជាមួយចំនួននៃ circuit របស់ remote network.។ ក្នុងករណីរបស់ ISDN circuits device ជាទូទៅបានហៅមកកាន់របស់លេខទូរស័ព្ទរបស់ remote ISDN circuit ។ នៅពេល Networks ពីរត្រូវបានភ្ជាប់ហើយត្រូវបាន authenticated វាអាចធ្វើការបញ្ជូន data បាន។ នៅពេលការបញ្ជូន data ត្រូវបានបញ្ចប់ ការហៅទូរស័ព្ទក៏បានផ្តាច់ទៅវិញ។ រូបភាពខាងក្រោមបង្ហាញពីឧទាហរណ៍របស់ប្រភេទនៃសៀគ្វីនេះ។



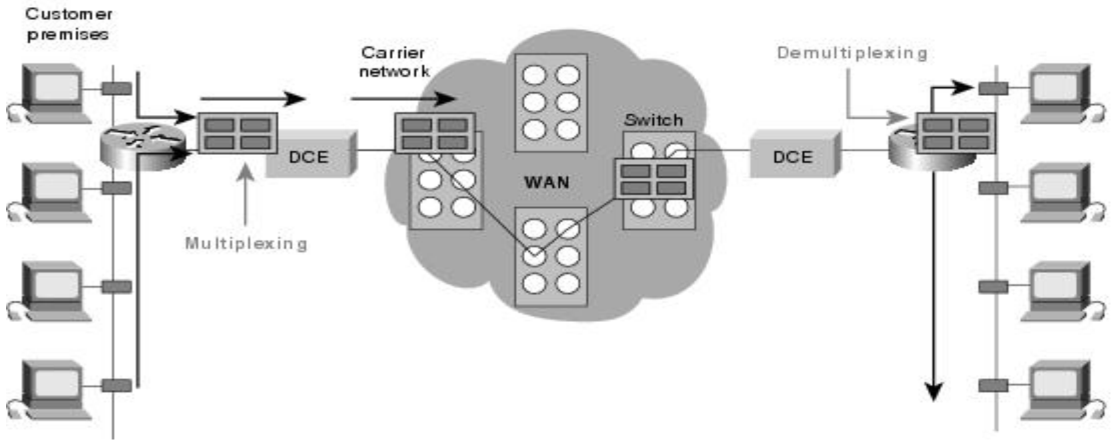
៤-១-២- Packet Switching

Packet switching គឺជា WAN technology មួយដែលអ្នកប្រើប្រាស់បានប្រើ carrier resources រួមគ្នាពីព្រោះថាវាអនុញ្ញាតឱ្យ carrier អាចបង្កើនប្រសិទ្ធភាពនៃការប្រើប្រាស់នៅហេដ្ឋារចនាសម្ព័ន្ធរបស់វា តម្លៃចំពោះ

customer ដែលជាទូទៅត្រូវមានលក្ខណៈល្អប្រសើរជាងការភ្ជាប់ពីចំណុចមួយមកចំណុចមួយទៀត។ ក្នុងការបង្កើត packet switching មួយ networks បានភ្ជាប់ជាមួយ carrier របស់ network ហើយអតិថិជនភាគច្រើនបានចែលរំលែកនៅ Network របស់។ បន្ទាប់មក carrier អាចបង្កើត virtual circuits រវាងខាងផ្នែករបស់អតិថិជនដោយ packets របស់ data ត្រូវបានទទួលពី Virtual Circuit មួយតាមរយៈ network មួយផ្សេងទៀត។ ផ្នែកនៃ Network របស់ carrier ដែលត្រូវបានចែករំលែកសំដៅទៅលើសញ្ញាពពក។ ឧទាហរណ៍របស់ packet switching networks រួមមាន Asynchronous Transfer Mode (ATM),Frame Relay, Switched Multimegabit Data Services (SMDS),និង X.25។ រូបភាពខាងក្រោមបង្ហាញពីឧទាហរណ៍របស់ packet-switched circuit ។

virtual connections រវាង customer sites គេហៅថាជា virtual circuit ។

រូបភាពនេះបង្ហាញពី Packet Switching ធ្វើការបញ្ជូន Packets ឆ្លងកាត់តាម Carrier Network



WAN Virtual Circuits

virtual circuit គឺជា software សៀគ្វីដែលបានបង្កើតក្នុង shared network មួយរវាង network devices ចំនួនពីរ។ virtual circuits មានដូចជា: switched virtual circuits (SVCs) និង permanent virtual circuits (PVCs)។

SVCs គឺជា virtual circuits ដែលត្រូវបានបង្កើតឡើងជាស្វ័យប្រវត្តតាមតម្រូវការហើយបានផ្តាច់ទៅវិញនៅពេលការភ្ជាប់ត្រូវបានបញ្ចប់។ ការប្រាស្រ័យទាក់ទងតាម SVC មួយរួមមានបីដំណាក់កាលគឺការបង្កើតសៀគ្វី ការបញ្ជូន data និងការផ្តាច់សៀគ្វី។ ជំហាននៃការបង្កើតការភ្ជាប់រួមមានបង្កើត virtual circuit រវាងប្រភពដើមនិង devices ដែលជាគោលដៅ។ ការផ្ទេ Data ទាក់ ទងជាមួយការបញ្ជូន data រវាង devices តាម virtual circuit ហើយការផ្តាច់សៀគ្វីទាក់ទងជា មួយការហែក virtual circuit ផ្តាច់រវាងប្រភព devices ដែលជាគោលដៅ។ SVCs ត្រូវបានប្រើក្នុងស្ថានភាពដែលការបញ្ជូន Data រវាង devices ដែលមាន data ប្រែប្រួលធំពីព្រោះថា SVCs បានបង្កើនទំហំbandwidth ដែលបានប្រើដោយសារតែការបង្កើតសៀគ្វីនិងដំណាក់កាលនៃការផ្តាច់ ប៉ុន្តែវាបានកាត់បន្ថយតម្លៃដែលទាក់ទងជាមួយ virtual circuit ដែលមានលក្ខណៈថេរ ។

PVC គឺជា virtual circuit ដែលត្រូវបានបង្កើតឡើងជាអចិន្ត្រៃយ៍ដែលរួមមានការផ្ទេdata។ PVCs ត្រូវបានប្រើក្នុងស្ថានភាពដែលការផ្ទេរ data រវាង devices មានការថេរ។ PVCs បានកាត់បន្ថយទំហំ bandwidth ដែលប្រើជាមួយការបង្កើតនិងការផ្តាច់នៃ virtual circuits ប៉ុន្តែវាបានកាត់បន្ថយតម្លៃដោយសារតែ virtual circuit មិនប្រែប្រួល។ PVCs ត្រូវបាន configure ជាទូទៅដោយ service provider នៅពេលគេបានកុម្ម៉ង់ service ។

៤-២- WAN Dialup Services

Dialup services គឺជាវិធីសាស្ត្រដែលមានប្រសិទ្ធភាពសម្រាប់ការភ្ជាប់តាម WANs។ ការអនុវត្តនៃ dialup ដែលពេញនិយមមានពីរគឺ dial-on-demand routing (DDR) និង dial backup ។

DDRគឺជាបច្ចេកទេសមួយដែល router មួយអាចចាប់ផ្តើមការហៅនៅលើ switched circuit នៅពេលវាត្រូវការបញ្ជូន data ក្នុងការបង្កើត DDR setup មួយដែល router ត្រូវបាន configureដើម្បីចាប់ផ្តើមដំណើរការហៅនៅពេលដែលជួបជាមួយលក្ខខ័ណ្ឌវិនិច្ឆ័យដូចជាប្រភេទនៃ network traffic ពិសេសដែលត្រូវការសម្រាប់បញ្ជូន។ នៅពេលបានភ្ជាប់ traffic ត្រូវបានឆ្លងកាត់តាមបណ្តាញ។ ការ configure ចំពោះ router បានកំណត់រយៈពេលសំរាកដែលបានប្រាប់ Router ឱ្យបោះចោលការភ្ជាប់នៅពេលសៀគ្វីត្រូវបានផ្អាកក្នុងរយៈពេលមួយ ។

Dial backup គឺជាវិធីសាស្ត្រមួយទៀតនៃការ Configure DDR។ ទោះបីជាយ៉ាងណាក៏ដោយក្នុង dial backup switched circuit ត្រូវបានប្រើប្រាស់ដើម្បីផ្តល់នៅ backup service សម្រាប់ប្រភេទនៃសៀគ្វីមួយទៀតដូចជា Point-to-point ឬ Packet Switching។ Routerត្រូវបាន Configure ដូច្នេះនៅពេលវាដឹងថាវាខូចនៅលើសៀគ្វីទី១បណ្តាញ Dial backupក៏បានចាប់ផ្តើម។ បន្ទាប់មកបណ្តាញ Dial backup ក៏បានភ្ជាប់សម្រាប់ WAN រហូតទាល់តែសៀគ្វីទី១ត្រូវបានជួសជុលឡើងវិញ។ នៅពេលមានបញ្ហានេះកើតឡើងការភ្ជាប់សម្រាប់ Dial backup ក៏ត្រូវបានផ្តាច់ទៅវិញ ។

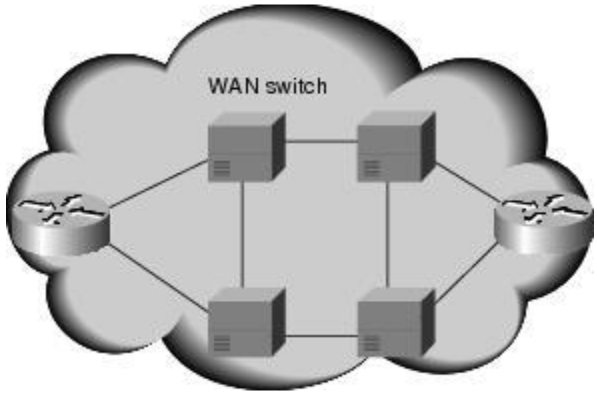
WAN Devices

WANs ប្រើប្រភេទនៃDevicesផ្សេងៗគ្នាដែលបានកំណត់សម្រាប់ WAN ។ WAN switches , Access Servers,Modems,CSU/DSUs និង ISDN terminal Adapters ត្រូវបានលើកយកមកសិក្សាក្នុងផ្នែកខាងក្រោម។ Devices ប្រភេទផ្សេងៗទៀតដែលយកមកប្រើមានដូចជា Routers ATM Switches និង Multiplexers ។

៤-២-១- WAN Switch

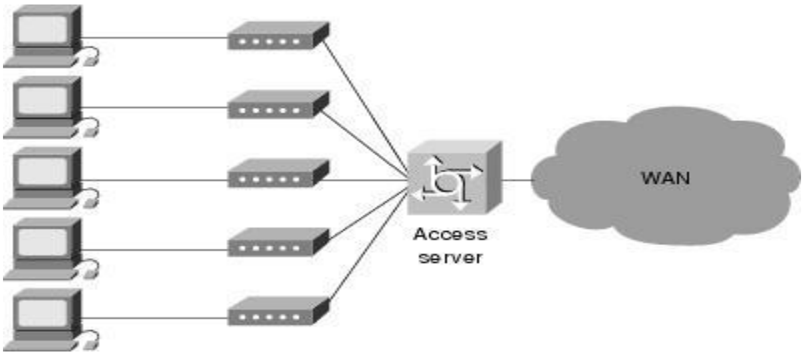
WAN switchគឺជា internetworking devices ដែលមានច្រើន ports។ Devices ទាំងនេះមានដូចជា Frame Relay,X.25 និង SMD ហើយដំណើរការនៅស្រទាប់ទី២នៃ OSI reference Model។ រូបភាពខាងក្រោមបង្ហាញពី Routersពីរដែលស្ថិតនៅឆ្ងាយនៃ WAN ដែលត្រូវបានភ្ជាប់ជាមួយ Switches ។

Routers ពីរស្ថិតនៅឆ្ងាយផ្នែកទាំងសងខាងរបស់ WANដែលភ្ជាប់គ្នាដោយ WAN Switches



៤-២-២- Access Server

access server ដើរតួនាទីជាចំណុចកណ្តាលសម្រាប់ Dial-in និង dial-out។ រូបភាពខាងក្រោមបង្ហាញពី Access Server មួយកំពុងប្រើការភ្ជាប់តាម Dial-out ជាមួយ WAN មួយ ។

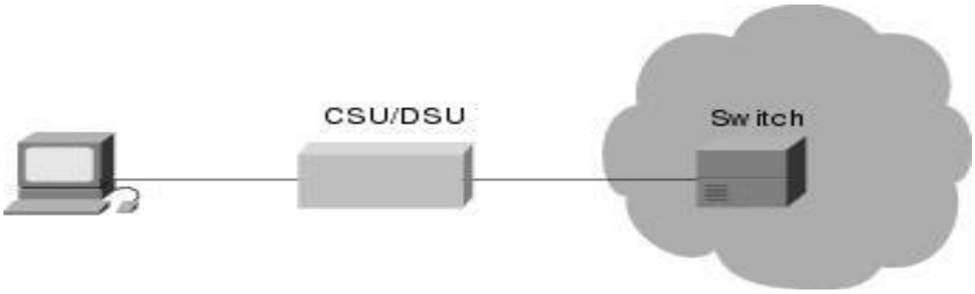


៤-២-៣- Modem

modem គឺជាឧបករណ៍សម្រាប់បកប្រែ digital និង Analog Signal ដែលធ្វើឱ្យ Data អាចបញ្ជូនតាមបណ្តាញទូរស័ព្ទ។ នៅខាងប្រភពដើម Digital Signal ត្រូវបានបំប្លែងជាទម្រង់មួយសម្រាប់បញ្ជូនតាមប្រព័ន្ធ Analog ។ នៅឯឧបករណ៍ទទួលវិញanalog signal ត្រូវបានបំប្លែងជា Digital Signal វិញ។ នៅឯគោលដៅ analog Signal ត្រូវបានត្រឡប់មកជាDigitalវិញ ។ រូបភាពខាងក្រោមបង្ហាញពីការភ្ជាប់ពី Modem ជាមួយ Modem តាមរយៈ WAN ។

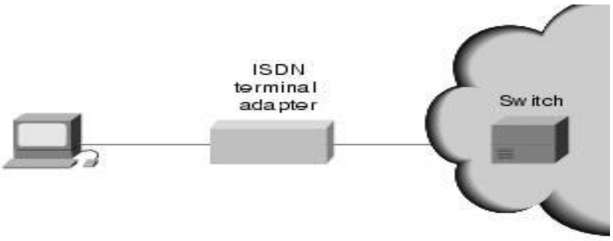
៤-២-៤- CSU/DSU

channel service unit/digital service unit (CSU/DSU) គឺជា digital interface device ដែលបានប្រើសម្រាប់ភ្ជាប់ Router ជាមួយ Digital Circuit ដូចជាT1 ។ CSD/DSU ក៏ផ្តល់ឱ្យនៅ Signal សម្រាប់ការប្រាស្រ័យទាក់ទងជាមួយឧបករណ៍ទាំងនេះ។ រូបភាពខាងក្រោមបង្ហាញពីការកំណត់ទីតាំងរបស់ CSU/ DSU ក្នុងការប្រើ WAN ។



៤-២-៥- ISDN Terminal Adapter

ISDN terminal adapter គឺជាឧបករណ៍ដែលប្រើសម្រាប់ភ្ជាប់ជាមួយ ISDN Basic Rate Interface (BRI) ជាមួយ interface ផ្សេងទៀតដូចជា EIA/TIA-232 លើ Router មួយ។ Terminal Adapter គឺជា ISDN modem ពីព្រោះថាវាមិនបំប្លែង Analog មកជា Digital Signal នោះទេ។ រូបភាពខាងក្រោមបង្ហាញពីការកំណត់ទីតាំងរបស់ Terminal Adapter ក្នុង ISDN ។



សំណួររំលឹកឡើងវិញ

Q—តើប្រភេទនៃ WAN circuits មានអ្វីខ្លះ?

A—Point-to-point, packet-switched, and circuit-switched.

Q—តើ DDR គឺជាអ្វីហើយវាខុសគ្នាពី dial backupត្រង់ណាខ្លះ?

A—DDR គឺជា dial-on-demand routing ។ DDR សម្រាប់ភ្ជាប់ជាមួយ remote site នៅពេលដែលចរាចរណ៍ Network ត្រូវការបញ្ជូន។ Dial backup ប្រើប្រភេទនៃ Service ដូចគ្នា ប៉ុន្តែចំពោះ backup វិញត្រូវបានប្រើជំនួស primary circuit ។ នៅពេលដែល primary circuit ខូច dial backup line ត្រូវបានចាប់ផ្តើមរហូតទាល់តែ primary circuit ត្រូវបានជួសជុលឡើងវិញ។

Q—តើ CSU/DSU ត្រូវបានប្រើប្រាស់សម្រាប់ធ្វើអ្វី?

A—A CSU/DSU សម្រាប់ផ្តល់ interfaces ឱ្យ router ដែលមាន digital line ដូចជា T1 ។

Q—តើ modem និង ISDN terminal adapter ខុសគ្នាត្រង់ចំណុចណាខ្លះ?

A—A modem បំប្លែង digital signals ឱ្យមកជា analog ដើម្បីធ្វើការបញ្ជូនតាមប្រព័ន្ធទូរស័ព្ទ។ ចំណែកឯ ISDN circuits វិញគឺជា digital ។ ដូច្នេះមិនត្រូវការបំប្លែងនោះទេ។

ជំពូកទី៥

ប្រភេទនៃ IP addresses

៥-១- ថ្នាក់របស់ IP Addresses

IP addresses ដែលយើងកំពុងប្រើប្រាស់សព្វថ្ងៃមាន ៥ ថ្នាក់គឺ

- Class A :1.0.0.0->126.255.255.255 និង Subnetmask :255.0.0.0

IP address ចាប់ផ្តើមជាមួយលេខ 0 និង១២៧ ត្រូវបានបំរុងទុកសម្រាប់ System ប្រើប្រាស់ ។ ឧទាហរណ៍ 127.0.0.1 ត្រូវបានប្រើប្រាស់សម្រាប់កុំព្យូទ័រនីមួយៗដូចជា localhos។ នៅក្នុង IP address មួយត្រូវបានចែកចេញជាពីរផ្នែកសំខាន់ៗគឺ

- **HostID(Hostid)** ដែលសម្រាប់សំគាល់ឱ្យ host ឬ កុំព្យូទ័រនីមួយៗ
- **NetworkID(Netid)** ត្រូវបានប្រើសម្រាប់សំគាល់ឱ្យ Network សម្រាប់ឱ្យក្រុមនៃ Hosts

៥-១-១- ប្រភេទនៃថ្នាក់ A

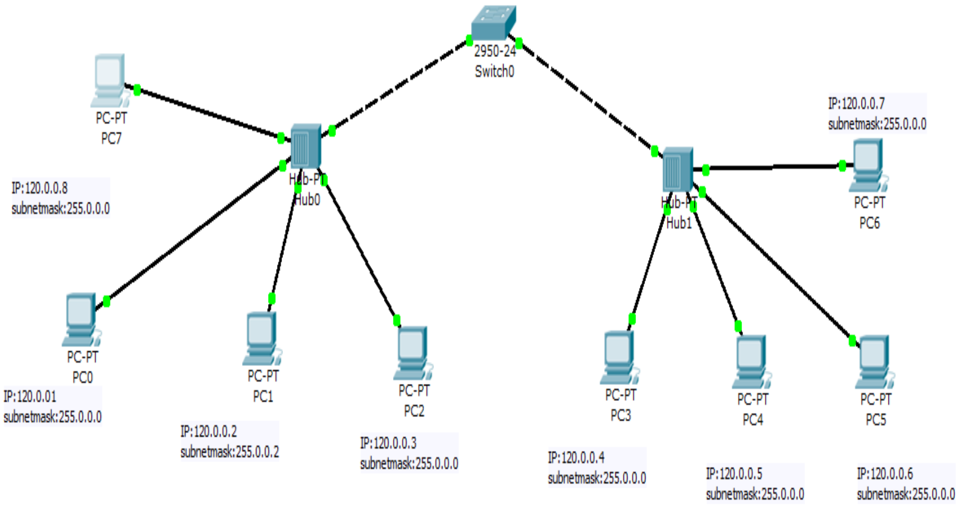
នៅក្នុងថ្នាក់ A Octetដំបូងតំណាងឱ្យ NetIDហើយ៣ octets ចុងក្រោយតំណាងឱ្យ HostID ។

00000001.0.0.0-->01111110.255.255.255

Octet ចាប់ផ្តើមជាមួយ bit 00000001 និងបញ្ចប់ជាមួយ bit 01111110។ ដូច្នេះថ្នាក់ A IP address មាន bit ទី១ជាលេខសូន្យ(0)។ យើងអាចគណនាចំនួន Network ក្នុងថ្នាក់ A តាមរូបមន្ត $២^{៧}$=១២៨-២=១២៦Network ។ ចំនួន៣ Octets ចុងក្រោយស្មើនិង២៤ bits តំណាងឱ្យ HostID ។ ដូច្នេះចំនួន Hosts ក្នុង network នីមួយៗមានចំនួនស្មើនិង $២^{២៤}$ -២=១៦៧៧៧២១៤ hosts ។

ចំណាំៈគ្រប់ Hosts ទាំងអស់អាចប្រាស្រ័យទាក់ទងគ្នាបានជាមួយគ្នាទៅវិញទៅមកបើវាមាន Network ដូចគ្នា ។ មានន័យថា វាមាន NetID ដូចគ្នា ។

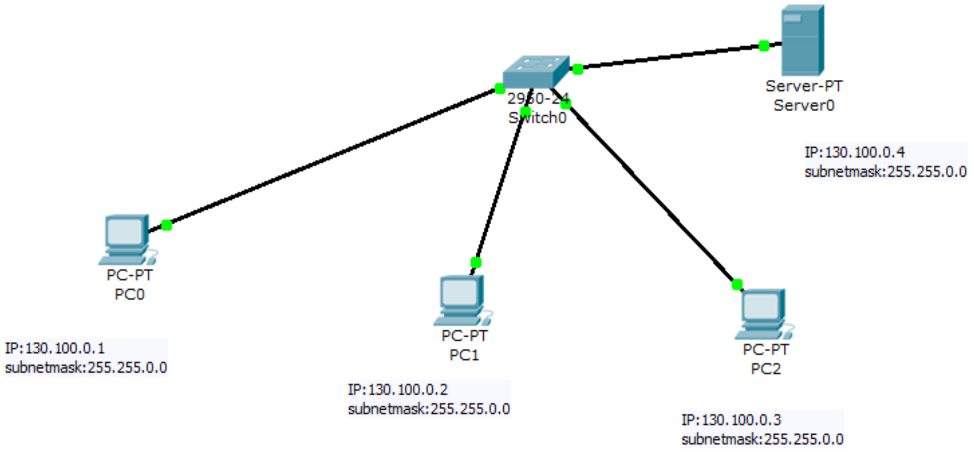
ឧទាហរណ៍



៥-១-២- ថ្នាក់ប្រភេទ B

នៅក្នុងថ្នាក់ប្រភេទ B ចាប់ផ្តើមជាមួយលេខ **128**.0.0.0→**191**.255.255.255ហើយមានSubnetmask :**255.255**.0.0 ។ នៅក្នុងថ្នាក់ប្រភេទ B ពីរ Octets ដំបូងត្រូវបានប្រើប្រាស់សម្រាប់សំគាល់ឱ្យ Network ហើយពីរ octets ចុងក្រោយត្រូវបានប្រើប្រាស់សំគាល់ឱ្យ HostID។ នៅក្នុងថ្នាក់ប្រភេទ B Octet ទី១ចាប់ផ្តើមជាមួយលេខ **10**000000.0.0.0→**10**111111.255.255.255 ។ ដូចអ្នកបានដឹងរួចមកហើយ ២ bits ដំបូងនៃ octet ទី១មានតម្លៃ១0ជានិច្ច ។ ដូច្នេះចំនួន Network ក្នុងថ្នាក់ប្រភេទ B ស្មើទៅនិង 2^{14}=16384 networks ហើយ network នីមួយៗមាន Hosts ចំនួនស្មើ 2^{16}-2=65534 hosts ។

ឧទាហរណ៍

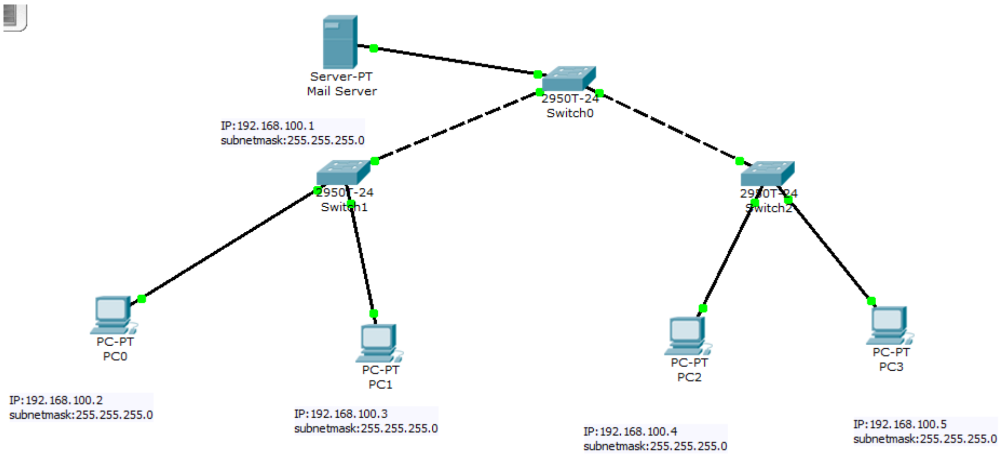


៥-១-៣- ប្រភេទនៃថ្នាក់ C

នៅក្នុងថ្នាក់ C ចាប់ផ្តើមជាមួយលេខ **192**.0.0.0-> **223**.255.255.255 និងមានSubnetmask : **255. 255.255**.0 ដែលបី Octets ដំបូងជា NetworkID និង Octet ចុងក្រោយគឺជា HostID ។ 3 bits ដំបូងនៃ Octet ទី១គឺជា bits លេខ 11 0 ជានិច្ច ។ **110**00000.0.0.0->**110**11111.255.255.255.

ដូច្នេះយើងអាចគណនាចំនួន Network ក្នុងថ្នាក់ C ស្មើនិង 2^{21}=2097152 networks ហើយចំនួនhosts ក្នុង Network នីមួយៗស្មើនិង 2^{8}-2=254 hosts។

ឧទាហរណ៍



៥-២- Classless Inter-Domain Routing

Classless Inter-Domain Routing (CIDR)គឺជាមេកានិចដែលបានបង្ហាញពីការកើនឡើងរបស់ Routing Tables យ៉ាងឃើតៗនៅលើ Router ក្នុងប្រព័ន្ធ Internet។ ដូច្នេះដើម្បីជួយដល់ការការពារនៃការសល់របស់ IP addresses គេត្រូវចែកវាជា Subnets នៃថ្នាក់ A B និង C វាអនុញ្ញាតឱ្យកំណត់ក្នុងសញ្ញាណ CIDR ។

៥-២-១- CIDR blocks

CIDR គឺជា Bitwise ដែលបានកំណត់នៅនិយាមមួយសម្រាប់ការបកប្រែរបស់ IP addresses។ វាបានបានបង្កឱ្យមានលក្ខណៈងាយស្រួលដល់ការ route ដោយអនុញ្ញាតឱ្យបណ្តុំនៃ IP address ត្រូវបានដាក់ក្នុងក្រុមតែមួយក្នុង Routing Tables។ ក្រុមទាំងនេះគេហៅថា CIDR block ដែលមានលេខលំដាប់ bits តំណាងឱ្យ IP addresses របស់វា។ IPv4 CIDR block ត្រូវ បានគេស្គាល់វាដោយការប្រើ Syntax ប្រហាក់ប្រហែលគ្នាចំពោះ IPv4 addresses។ Address ជាលេខគោលដប់៤ខ្ទង់ដំបូងនិងសញ្ញា(/) បន្ទាប់មកលេខចាប់ពី០ដល់៣២គឺ **A.B.C.D/N**។ ផ្នែកគោលដប់ត្រូវបានបកប្រែជាលេខគោលពីដែលមានប្រវែង 32 bits ហើយត្រូវបានចែកជា 4 octets ។ លេខខាងក្រោយ slash មានប្រវែងថេរ ចំនួននៃ bits ដែលដូចគ្នាត្រូវបានរាប់ពីឆ្វេងមកស្តាំនៃ IP addresses ។

CIDR ត្រូវបានប្រើផងដែរជាមួយ IPv6 address ដែលប្រវែងចាប់ពី០ដល់១២៨ ។ Syntax ដូចគ្នាត្រូវបានប្រើជាមួយ IPv6 ដែលភ្ជាប់មកជាមួយSlash(/) និងចំនួន bits ដែល bitsក្នុងprefix mask ។

Subnet masks

Subnetmaskគឺជា bitmaskដែលសម្រាប់បកប្រែប្រវែង Prefixក្នុងទម្រង់ដូចទៅនិងIPv4 address ដែរ

CIDR notation

Classless Inter-Domain Routing Address បានកំណត់ជា CIDR ដែលចាប់ផ្តើមជាមួយ Internet Protocol address ដែលភ្ជាប់មកជាមួយ Slash(/) និងលេខប្រព័ន្ធគោលដប់កំណត់ពីប្រវែងគិតជា bits នៃ Subnetmask ឬ routing Prefix ។

ឧទាហរណ៍ចំពោះ IPv4 និង IPv6 addresses

- 192.168.100.1/**24** តំណាងឱ្យ IPv4 address និង routing prefix ដែលទាក់ទងគ្នា(192.168.100.0) ឬសមមូលទៅនិង Subnetmask:255.255.255.0 ។
- 192.168.0.0/**22** តំណាងឱ្យ 1024 IPv4 addresses ដែលមានលេខចាប់ពី 192.168.0.0 រហូតដល់ 192.168.3.255 ។
- 2001:DB8::/48 តំណាងឱ្យ IPv6 addresses ដែលមានលេខចាប់ពី 2001:DB8:0:0:0:0:0:0 រហូតដល់ 2001:DB8:0:FFFF:FFFF:FFFF:FFFF:FFFF
- ::1/128 តំណាងឱ្យ IPv6 loopback address.

ចំពោះ IPv4 network គេអាចសរសេរវាក្នុងទម្រង់ជា

- 192.168.0.0/**24** អាចសរសេរកាត់ជា 192.168.0.0/**255.255.255.0**
- 192.168.0.0/**22** អាចសរសេរកាត់ជា 192.168.0.0/**255.255.252.0**

ចំនួននៃ Addresses របស់ subnet មួយត្រូវបានកំណត់ដោយ Mask ឬ Prefix ដែលអាចគណនាដោយរូបមន្ត $2^{(\text{address size-mask})}$ ។ ឧទាហរណ៍ Mask ស្មើ២៩ នោះយើងបាន $2^{(32-29)}=2^3=8$Address ចំពោះ IPv4

networks។ ទោះបីជាយ៉ាងណាក៏ដោយ ពីព្រោះថាមានយ៉ាងហោចណាស់មាន IP address មួយក្នុងចំណោម IP address ទាំងនេះត្រូវបានប្រើប្រាស់សម្រាប់ Gateway ចំពោះ Subnet ផ្សេងៗទៀតហើយដោយសារតែ Address ខ្លះត្រូវបានបំរុងទុកជា Broadcast Address ដូច្នេះចំនួននៃ Address ដែលអាចប្រើបានសម្រាប់ Hosts ត្រូវបានថយចុះ ។

៥-២-២- IPv4 private addresses

ក្នុងការបង្កើតប្រព័ន្ធ Network ពីមុន នៅពេលដែលមានការភ្ជាប់ប្រព័ន្ធ Network មានលក្ខណៈពាសពេញពិភពលោកជាមួយ Hosts ក្នុងប្រព័ន្ធ Internet IP Address ដែលបានប្រើត្រូវតែមានតែមួយគត់សម្រាប់កំណត់ឱ្យ Device នីមួយៗ ។

កុំព្យូទ័រs ដែលមិនភ្ជាប់ជាមួយ Internet ដូចជាម៉ាស៊ីនតាមរោងចក្រអាចទាក់ទងតែជាមួយគ្នាទៅវិញទៅមកតាម TCP/IP ប៉ុណ្ណោះ ។ មានជួរនៃ IP address Version 4 ចំនួន 3 ដែលត្រូវបានប្រើជា Private IP address ដែលបានបំរុងក្នុង RFC 1918 ។ Addresses ទាំងនេះមិនអាច Route បានលើប្រព័ន្ធ Internet នោះទេ។ ដូច្នេះការប្រើប្រាស់របស់វាមិនត្រូវបានចុះក្នុងបញ្ជីនោះទេ ។

សព្វថ្ងៃនេះ គេត្រូវការប្រភេទនៃ IP address នេះសម្រាប់ភ្ជាប់ជាមួយ Internet តាមរយៈ NAT ។

Q. តើ Private IP address គឺជាអ្វី ?

A. Internet Assigned Numbers Authority (IANA) បានបំរុង IP address បីផ្នែក សម្រាប់ Private IP address :

10.0.0.0 - 10.255.255.255

172.16.0.0 - 172.31.255.255

192.168.0.0 - 192.168.255.255

IP address ស្ថិតក្នុងជួរនៃ IP address ចាប់ពី 169.254.0.0 ដល់ 169.254.255.255 ត្រូវបានបំរុងទុកសម្រាប់ **Automatic Private IP Addressing** ។ IP address ទាំងនេះមិនត្រូវបានប្រើប្រាស់ក្នុងប្រព័ន្ធInternet នោះទេ។

ជាទូទៅ IP address លេខ 192.168.0.1, 192.168.0.2, ។ល។និង Subnetmask លេខ 255. 255.255.0 នៅពេលកំណត់ជា Static IP address ឱ្យ កុំព្យូទ័រs លើប្រព័ន្ធ LANs ។ បើ DHCP Server មួយស្ថិតនៅលើ LAN មួយ ជួរនៃ IP address ត្រូវបានកំណត់ដោយទទួលជាស្វ័យប្រវត្តត្រូវតែកំណត់យ៉ាងណាកុំឱ្យមានដូចជាមួយ Static IP addresses ។

៥-៣- Subnets (ក្រុមតូចៗនៃ Networks)

ដូចដែលអ្នកបានសិក្សារួចមកហើយអំពីថ្នាក់របស់ Network គឺថ្នាក់ A B និង C networks ដែលថ្នាក់នីមួយៗមានចំនួនកុំព្យូទ័រជាច្រើនដែលជាហេតុបណ្តាលឱ្យមានទំហំចរាចរណ៍នៃ Dataកាន់តែច្រើនឡើងនៅពេលដែល Hosts ទាំងនោះបាន Broadcast នៅលើប្រព័ន្ធ Network ។ ដើម្បីធ្វើឱ្យមានទំហំចរាចរណ៍នៃ Data ឱ្យកាន់តែតូចៗយើងត្រូវតែចែក Network នោះឱ្យជាក្រុមតូចៗជាច្រើនដែលក្រុមនីមួយៗនោះគេហៅថា Subnet ។

របៀបបង្កើត Subnet

ដើម្បីចែក Network ធំមួយជា Subnets តូចៗជាច្រើននោះ យើងប្រើវិធីសាស្ត្រដែលគេហៅថា "**Borrowing the bits from the hostID to the NetworkID**" ។

ឧទាហរណ៍

ក្នុងថ្នាក់ C Network មានចំនួន Hosts សរុបចំនួន ២៥៤ ។ នៅពេលដែល Host ណាមួយបាន Boradcast នោះគ្រប់ Hosts ទាំងអស់និងទទួលបាននូវ Broadcast messages ។ មានន័យថាវាបានបង្កើតនូវទំហំចរាចរណ៍នៃ Network ដែលមានទំហំធំ។

Default subnetmask នៃ class c is 255.255.255.**0** (11111111. 11111111.11111111. **00000000**).

នៅក្នុង subnetmask bit លេខមួយទាំងអស់(1s) គឺជា bit តំណាងឱ្យ network ID ហើយ bit លេខសូន្យទាំងអស់(0s)គឺតំណាងឱ្យ HostID ។

បើអ្នកចង់ឱ្យ hostID ក្លាយជា networkID យើងត្រូវប្តូរវាពីសូន្យមកជាលេខមួយដូចខាងក្រោម

11111111.11111111. 11111111.**00000000**(255.255.255.0)

11111111.11111111. 11111111.**1**0000000(255.255.255.128)

11111111.11111111. 11111111.**11**000000(255.255.255.192)

11111111.11111111. 11111111.**111**00000(255.255.255.224)

11111111.11111111. 11111111.**1111**0000(255.255.255.240)

11111111.11111111. 11111111.**11111**000(255.255.255.248)

11111111.11111111. 11111111.**111111**00(255.255.255.252)

ឧទាហរណ៍

IP address : 192.168.100.200

Subnetmask :255.255.255.240

IP Address និង subnetmask នេះគឺជា IP address នៃ subnet មួយដែលមាន network address: 192.168.100.192/28 ។

ដើម្បីគណនាចំនួននៃ Subnet និងចំនួន Hosts ក្នុងមួយ Subnet គេអនុវត្តតាមរូបមន្តដូចខាងក្រោម

- ចំនួន Subnet ស្មើនិង ២ ស្វ័យគុណ bits ដែលបានខ្ចីហើយចំនួន Host ក្នុងមួយ Subnet ស្មើនិង ២ ស្វ័យគុណ bits ដែលនៅសល់ដកពីរចេញ។

ឧទាហរណ៍

យើងមានhe subnetmask : 255.255.255.240 ដូច្នេះ ចំនួន bits ដែលបានខ្ចីគឺ ៤ ។ ដូច្នេះចំនួន Subnetស្មើនិង ២^{៤} ស្មើនិង១៦ហើយចំនួន Hosts ក្នុងមួយ Subnet ស្មើនិង២^{៤} -២ស្មើនិង១៤ ។

ដើម្បីរក Network Address យើងត្រូវធ្វើវិធី AND operation រវាង IP address និង Subnetmask

ឧទាហរណ៍

192.168.100.200

AND

255.255.255.240

លទ្ធផលទទួលបានពី AND operation គឺ 192.168.100.192 ដែលជា Network Address ។

The logic operation

1 AND 1=1

1 AND 0=0

0 AND 1=0

0 AND 0 =0

ដើម្បីធ្វើប្រមាណវិធី AND បានយើងត្រូវបំប្លែងវាជាលេខប្រព័ន្ធគោលពីរជាមុនសិន។

របៀបបំប្លែងពីប្រព័ន្ធគោលពីរមកជាប្រព័ន្ធគោលដប់

$(xxxxxxxx)_2 = x * 2^7 + x * 2^6 + x * 2^5 + x * 2^4 + x * 2^3 + x * 2^2 + x * 2^1 + x * 2^0$

បើមេគុណណាមានតម្លៃស្មើសូន្យ លេខណាក៏ដោយគុណជាមួយសូន្យនិងស្មើសូន្យជានិច្ច។

ដូច្នេះយើងត្រូវគិតតែលេខណាដែលមានមេគុណខុសពីសូន្យតែប៉ុណ្ណោះ

96=64+32

$64=2^6$

$32=2^5$

ដូច្នេះយើងបាន $96=0*2^7 + 1 *2^6 + 1 * 2^5 + 0 * 2^4 + 0 * 2^3 + 0 * 2^2 + 0 * 2^1 + 0 * 2^0$ =0 1 1 0 0 0 0 0

តារាងសង្ខេបឡើងវិញពី bits Class A,B,C និង D

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits don't change)	Network (N) and Host (H) parts of an address	Default subnet mask (decimal and binary)	Numbers of possible networks and hosts per network
A	1 - 127	00000000 - 01111111	N.H.H.H	255.0.0.0 11111111.00000000.00000000.00000000	126 nets (2^7-2) 16,777,214 hosts per net (2^24-2)
B	128 - 191	10000000 - 10111111	N.N.H.H	255.255.0.0 11111111.11111111.00000000.00000000	16,382 nets (2^14-2) 65,534 hosts per net (2^16-2)
C	192 - 223	11000000 - 11011111	N.N.N.H	255.255.255.0 11111111.11111111.11111111.00000000	2,097,150 nets (2^21-2) 254 hosts per net (2^8-2)
D	224 - 239	11100000 - 11101111	Not for commercial use as a host		
E	240 - 255	11110000 - 11111111	Not for commercial use as a host		

ជំពូកទី៦

IP Address 6

IPv40 គឺជា Protocol មួយដែលគេពេញនិយមប្រើប្រាស់សព្វថ្ងៃនេះ។ IPv4.0 ត្រូវបានបង្កើតឡើងនៅក្នុងទសវត្ស១៩៧0s។ ចំពោះ IPv6.0 វិញត្រូវបានបង្កើតឡើងប្រើប្រាស់ដោយសារតែមានការខ្វះខាតនៃ IP address ពីព្រោះមានឧបករណ៍ជាច្រើនត្រូវបានប្រើប្រាស់ IPv4.0 អស់។

IPv6.0 ត្រូវបានវិស្វករនឹងអ្នកបង្កើត Software ប្រើប្រាស់ដើមទសវត្ត១៩៩0s ។ IP address ត្រូវបានពង្រីកពី 32 bits មកជា 128 bits address ។

- IPV6 addresses មានប្រវែងស្មើនិង 128 bits ដែលមានទម្រង់ជា: x:x:x:x:x:x:x ដែលលេខប្រព័ន្ធគោល១៦មានតម្លៃលេខពី(0000-FFFF) ។
- នៅក្នុងករណីខ្លះ IPV6 addresses មានសុទ្ធតែលេខសូន្យទាំងអស់ដូចជា

0000:0000:0000:0000:0000:0000:0000:1 ត្រូវបានគេសរសេរជា 0:0:0:0:0:0:0:1។ វាបានបង្ហាញពីក្រុមនៃ bit លេខសូន្យដោយប្រើនិមិត្តសញ្ញា"::"។ ដូច្នេះគេអាចសរសេរដោយអក្សរកាត់ជា"::1"។ ដោយប្រើសញ្ញា "::" IPV6 អាចកំណត់ពីចំនួនតម្លៃនៃលេខដែលបានបាត់គឺជាលេខសូន្យទាំងអស់ ។ ទោះបីជាយ៉ាងណាក៏ដោយបើសញ្ញា "::" ត្រូវបានប្រើច្រើនជាងមួយដង វាមិនអាចប្រាប់ឱ្យដឹងពីចំនួន bit នៃលេខសូន្យដែលបានបាត់នោះទេ។

៦-១- ការពិពណ៌នាអំពី IPv 6.0 Packet Header

Header មានប្រវែង 40 bits ហើយការរៀបចំមាន Version , Class, Flow Label, Payload, Length, Next Header, Hop Limit, Source address, Destination Address, Data នឹង Payload fields

Hexadecimal "Hex"

0 1 2 3 4 5 6 7 8 9 A B C D E F

A = 10

B = 11

C = 12

D = 13

E = 14

F = 15

លេខ0ដល់៩ក្នុងប្រព័ន្ធគោល១0ស្មើនឹង0ដល់៩ក្នុងប្រព័ន្ធគោល១៦

៦-២- ការពិពណ៌នាអំពី Address

ចូរពិនិត្យទៅលើឧទាហរណ៍របស់ IPv6 address ។ Address ត្រូវបានរៀបចំតាម៨ផ្នែកដែលចែកដាច់ពីគ្នាដោយសញ្ញា ":" ។ ផ្នែកនីមួយៗមានប្រវែង 16 bits ។ ដូច្នេះ IPv6.0 មានប្រវែងស្មើនឹង 128 bits (16 bits x 8)។

Address មានទម្រង់ជា:

n:n:n:n:n:n:n:n ដែល n ស្មើ៤ខ្ទង់ជាគោល១៦

ឧ 1080:0:0:0:8:800:200C:417A ជា Unicast

FF01:0:0:0:0:0:0:101 ជា multicast address

៦-២-១- Broadcasting Methods

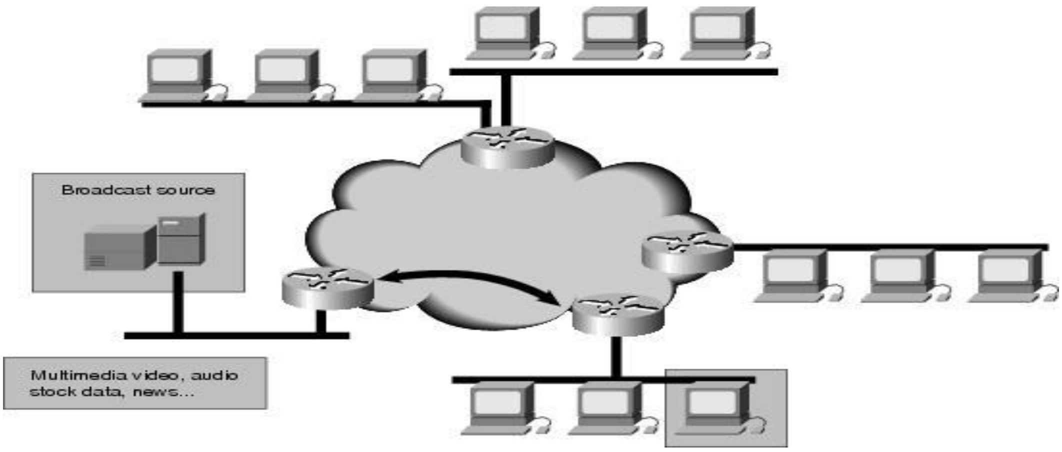
នៅក្នុង IPv6.0 មានវិធីនៃការ Broadcast ថ្មីដូចជា:

- Unicast
- Multicast
- Anycast

៦-២-១-១- Unicast

Unicast គឺជាការប្រាស្រ័យទាក់ទងរវាង Host តែមួយគត់ជាមួយឧបករណ៍ទទួលតែមួយគត់។ Packet ត្រូវបានបញ្ជូននូវ Unicast address ហើយត្រូវបានទទួលតែចំពោះ Interface ដែលមាន Address កំណត់ក្នុងនោះប៉ុណ្ណោះ។

	Long format	Shortcut format
Unicast	1070:200:0:0:0:900:300C:618A	1070:200::900:300C:618A



រូបភាព-១-Unicast បញ្ជូន Packets ទៅឱ្យ Interface ច្បាស់លាស់

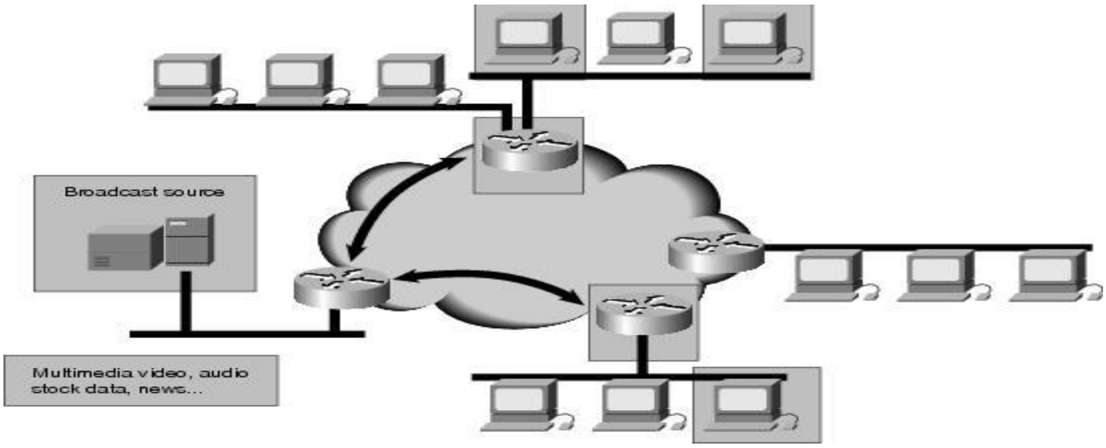
៦-២-១-២- Multicast

Multicast គឺជាការប្រាស្រ័យទាក់ទងរវាង Host តែមួយគត់ជាមួយឧបករណ៍ទទួលជាច្រើន។ Packets ត្រូវបានបញ្ជូនទៅឱ្យគ្រប់ Interface ទាំងអស់ដែលបានកំណត់ដោយ Address មាននៅក្នុងនោះ។

	Long format	shortcut
Multicast	FF01:0:0:0:0:0:0:100	FF01::100

- FF01::1 សម្រាប់ nodes ទាំងអស់ដែលស្ថិតនៅក្នុង node-local scope
- FF02::1 សម្រាប់ nodes នៅលើ local link
- FF01::2 សម្រាប់ routers នៅក្នុង node-local scope.

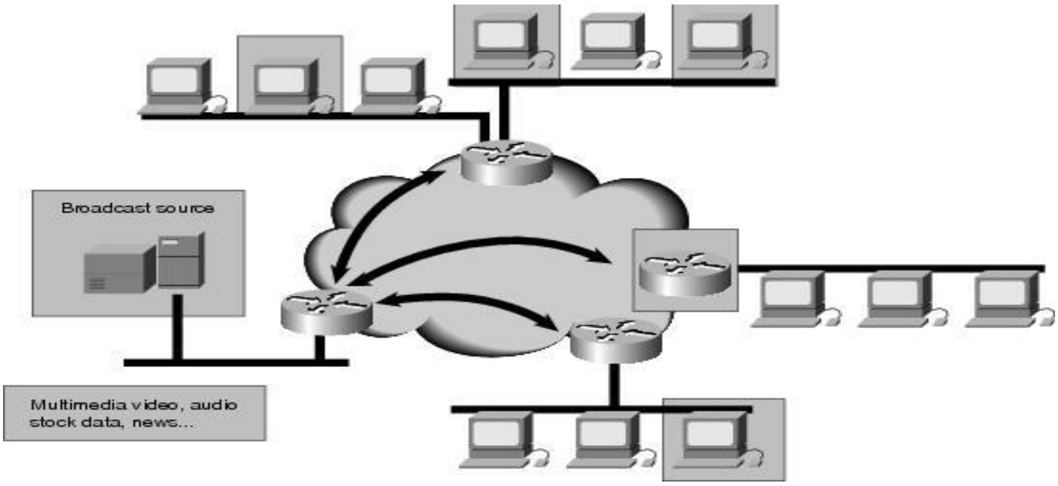
- FF02:: 2 សម្រាប់ routers នៅលើ link-local scope.
- FF05::2 សម្រាប់ routers នៅក្នុង site



រូបភាព-២ Multicast បញ្ជូន Packets ទៅឱ្យ Subnet នឹងឧបករណ៍ដែលបានកំណត់ទុក ដើម្បីសម្រាប់ Multicast Packets

៦-២-១-៣- Any cast

Packets ដែលបានបញ្ជូនចំពោះ anycast address ឬបណ្តុំនៃ Addresses ត្រូវបានទទួលដោយ Interface ដែលស្ថិតនៅជិតបំផុតដែលបានកំណត់ដោយ Address នោះ។ Anycast គឺជាការប្រាស្រ័យទាក់ទងរវាងឧបករណ៍បញ្ជូនតែមួយជាមួយបណ្តុំនៃ Address ។



រូបភាព-៣- Anycast បញ្ជូន Packets ទៅឱ្យបណ្តុំនៃ Interface ហើយអាចមានឧបករណ៍ចុងបញ្ចប់និង Routers

៦-៣- IP Multicast Addresses

Multicast addresses កំណត់ច្បាស់លាស់ពីក្រុមនៃ IP host ដែលបានចូលរួមក្នុងក្រុមហើយចង់ទទួលចរាចរណ៍ដែលបានបញ្ជូនឱ្យចំពោះក្រុមនេះ។

IP class D address

IANA(Internet Assigned Number Authority)គ្រប់គ្រងក្នុងការកំណត់ IP multicast address ។ គេបានកំណត់ Class D address ប្រើជា IP multicast ។ ដូច្នេះ IP multicast group addresses ចាប់ផ្តើមពី 224.0.0.0 → 239.255.255.255 ។

Reserved Link Local Addresses

IANA បានបំរុង Address ចាប់ពី 224.0.0.0 ដល់ 224.0.0.255 សម្រាប់ network protocol នៅលើ LAN segement ណាមួយ។ Packets ប្រើជាមួយ Addresse ទាំងនេះគឺ Router មិនអាចបញ្ជូនបន្តនោះបានទេវាស្ថិតនៅក្នុងផ្នែក LAN មួយ។ វាត្រូវបញ្ជូនជាមួយTTL(Time-to-Live)នៃ1s។ Network protocolsប្រើ addresses ទាំងនេះសម្រាប់រក Router ជាស្វ័យប្រវត្តហើយសម្រាប់ទំនាក់ទំនងជាមួយ Routing ព័ត៌មានដែលបានកំណត់។ ឧទាហរណ៍ OSPF ប្រើ 224.0.0.5 នឹង224.0.0.6 ដើម្បីផ្លាស់ប្តូរព័ត៌មានអំពី លក្ខណៈរបស់ Link ។ តាមតារាងខាងក្រោមបង្ហាញពី Address ដែលគេស្គាល់:

Table Link Local Addresses	
Address	ការប្រើប្រាស់
224.0.0.1	គ្រប់ប្រព័ន្ធទាំងអស់នៅលើ subnet នេះ
224.0.0.2	គ្រប់ routers ទាំងអស់នៅលើ subnet នេះ
224.0.0.5	OSPF routers
224.0.0.6	OSPF designated routers
224.0.0.12	DHCP server/relay agent

Global Scoped Address

Address ចាប់ផ្តើមពី 224.0.1.0ដល់ 238.255.255.255 ដែលគេហៅថា globally scoped address។ គេប្រើប្រាស់វាសម្រាប់បញ្ជូនទិន្នន័យតាមអង្គការនិងឆ្លងកាត់តាមប្រព័ន្ធអ៊ិនធឺណែត។ Address ត្រូវបានបំរុងទុកសម្រាប់ប្រើប្រាស់ដោយ multicast application តាមរយៈ IANA។ ឧទាហរណ៍ 224. 0.1.1 ត្រូវបានប្រើប្រាស់សម្រាប់ Network Time Protocol (NTP)។

Limited Scoped Address

Addresses ចាប់ផ្តើមពី 239.0.0.0 រហូតដល់ 239.255.255.255 បានកំណត់ address សម្រាប់ scope address Address ទាំងនេះត្រូវបានកំណត់ដោយ RFC 2365 ដោយប្រើសម្រាប់ local group ឬអង្គការ។

Global Addressing

RFC 2770 បានស្នើ address 233.0.0.0/8 សម្រាប់បំរុងទុកឱ្យអង្គការដែលបានបំរុង AS number។ AS number របស់ domain ត្រូវបានភ្ជាប់ជាមួយ Octet ទី២នឹងទី៣នៃ233.0.0.0/8។ ឧទាហរណ៍ As 62010 ត្រូវ

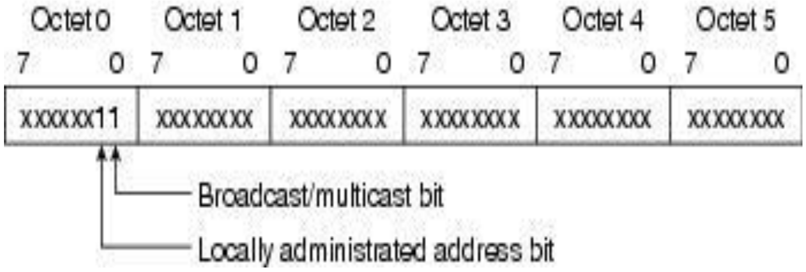
បានសរសេរជាគោល១៦គឺF23A។ យើងញែកវាជាពីរគឺ F2 នឹង 3A នោះយើងទទួលបាន 242 នឹង58 ជាគោល ១០។ វាបានផ្តល់ឱ្យយើងនូវ Subnet មួយនៃ 233.242.58.0 ដែលត្រូវបានបំរុងទុកសម្រាប់ As 62010 ។

Layer 2 Multicast Addresses

តាមធម្មតា NICs ដែលស្ថិតនៅលើផ្នែកមួយនៃ LAN មួយនិងទទួលតែ Packets ដែលមានកំណត់គោលដៅសម្រាប់ MAC ឬ Broadcast MAC address ។ Address ខ្លះត្រូវបានប្រើប្រាស់ជា Multicast ដែលធ្វើឱ្យ Hosts អាចទទួលបាននូវPackets ហើយគេអាចបែងចែកនូវភាពខុសគ្នានៃ Multicast group ។

តែសំណាងល្អដែលការកំណត់ IEEE LAN បានបង្កើតឡើងជាបណ្តោះអាសន្នសម្រាប់ធ្វើការបញ្ជូននៃ Broadcast ឬ Multicast packets។

នៅក្នុងស្តង់ដា 802.3 standard bit 0 នៃ octet ទី១ ត្រូវបានប្រើដើម្បីបង្ហាញពី broadcast/ Multicast bit ក្នុង Ethernet frame។



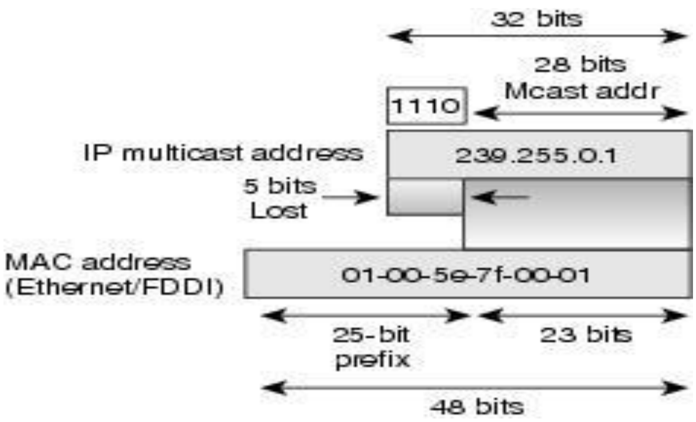
រូបភាព-៣- IEEE 802.3 MAC Address Format

bit នេះបង្ហាញជា Frame ដែលត្រូវបានកំណត់ជាគោលដៅចំពោះក្រុមណាមួយនៃ Hosts ឬគ្រប់ Hosts ទាំងអស់នៅលើ Network ។ ចំពោះ broadcast address គឺ 0xFFFF.FFFF.FFFF។

Ethernet MAC Address Mapping

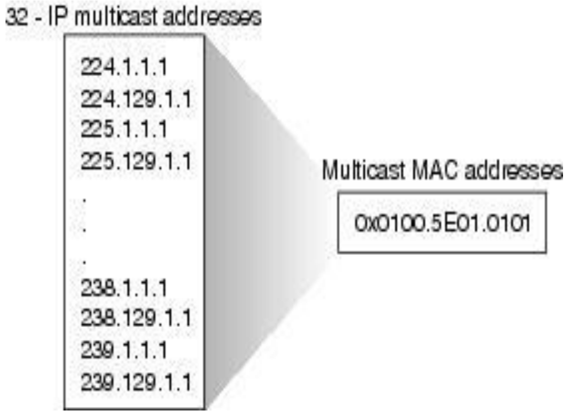
IANA មានបណ្តុំនៃ Ethernet MAC address ផ្ទាល់ដែលចាប់ផ្តើមជាមួយ 01:00:5E(គោល16)។ ពាក់កណ្តាលនៃបណ្តុំនេះត្រូវបានកំណត់ប្រើជា Multicast address។ នេះបង្កើតបាននូវ Ethernet MAC address ចាប់ពី 0100.5e00.0000 រហូតដល់ 0100.5e7f.ffff ។

ការកំណត់បែបនេះអនុញ្ញាតឱ្យ 32 bits ក្នុង Ethernet Address ដើម្បីបំពេញចំពោះ IP multicast group address ។



រូបភាព-៤: ការកំណត់ឱ្យត្រូវនៃ IP Multicast ជាមួយ Ethernet/FDDI MAC Address

ដោយសារតែ 5 bits ខាងលើនៃ IP multicast address ត្រូវបានបោះចោលក្នុងការកំណត់នេះ ដូច្នេះ address មិនមែនតែមួយប៉ុណ្ណោះ។ តាមពិត 32 multicast group IDs ខុសៗគ្នាដែលត្រូវគ្នាជាមួយ Ethernet address។



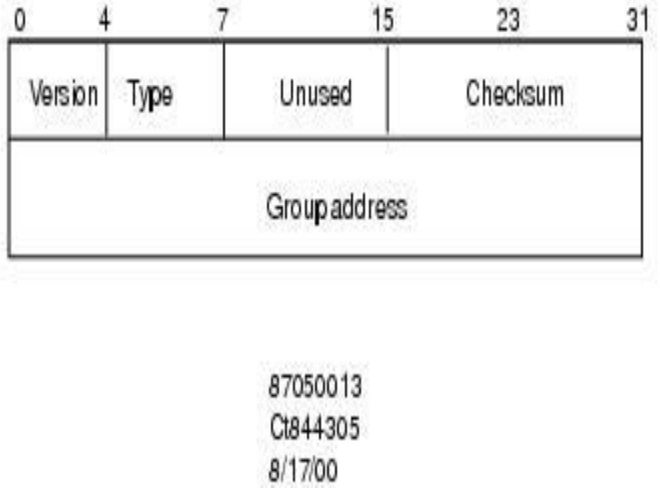
រូបភាព-៥- MAC Address Ambiguities

៦-៤- Internet Group Management Protocol (IGMP)

IGMP ត្រូវបានគេប្រើដើម្បីចុះបញ្ជី Host នីមួយៗជាស្វ័យប្រវត្តក្នុង Multicast group នៅលើ LAN ណាមួយ។ Host អាចសម្គាល់ភាពជាសមាជិកបានដោយបញ្ជូល IGMP message ទៅឱ្យ local multicast router។ ក្រោម IGMP routerស្គាល់ចំពោះ IGMP message ហើយក្នុងរយៈពេលច្បាស់លាស់វាបញ្ជូនចេញនូវការសាកសួរដើម្បីរកឱ្យឃើញក្រុមណាមួយដែលសកម្មឬមិនសកម្មនៅលើSubnet

IGMP Version 1

RFC 1112 កំណត់ច្បាស់លាស់សម្រាប់ IGMPV 1។



រូបភាព-៦- IGMP Version 1 Packet Format

IGMP Version 2

RFC 2236 កំណត់ច្បាស់លាស់សម្រាប់ IGMPV2។

0 – 7	7 – 15	15 – 23	23 – 31
Type	Maximum response time	Checksum	
Group address			

រូបភាព-៧- IGMPv2 Message Format

IGMP V2 ធ្វើការដូច IGMPv1 ដែរ។ ភាពខុសគ្នាជាចម្បងគឺមាន Leave Group Messag មួយ។

ឥឡូវនេះ Hosts អាចធ្វើការទាក់ទងជាមួយ local multicast router ដែលការយកចិត្តទុកដាក់គឺចាកចេញពីក្រុម។ បន្ទាប់មក Router បញ្ជូនចេញនូវការសាកសួរហើយកំណត់ថាតើមាន Host នៅសល់ដែលពេញចិត្តទទួលចរាចរណ៍។ បើគ្មានការឆ្លើយតបទេRouterកំណត់រយៈពេលហួសកំណត់ឈប់បញ្ជូនបន្ត។ ការធ្វើបែបនេះកាត់បន្ថយយ៉ាងច្រើននូវ Leave latency បើប្រៀបធៀបជាមួយ IGMPv1 ។ ចរាចរណ៍ដែលមិនត្រូវការនឹងមិនចាំបាច់ត្រូវបានបញ្ឈប់យ៉ាងឆាប់រហ័ស។

៦-៥- Multicast នៅក្នុងមជ្ឈដ្ឋាន layer 2 Switching

លក្ខណៈតាមលំនាំដើមសម្រាប់ Layer 2 Switch គឺត្រូវបញ្ជូនបន្តនូវចរាចរណ៍ Multicast ទាំងអស់ទៅគ្រប់ Ports ដែលជារបស់ LAN គោលដៅនៅលើ Switch ។ នេះជាលក្ខណៈរបស់ Switch ដែលបានកំណត់ចរាចរណ៍ចំពោះ Port ដែលត្រូវការទទួលទិន្នន័យ។

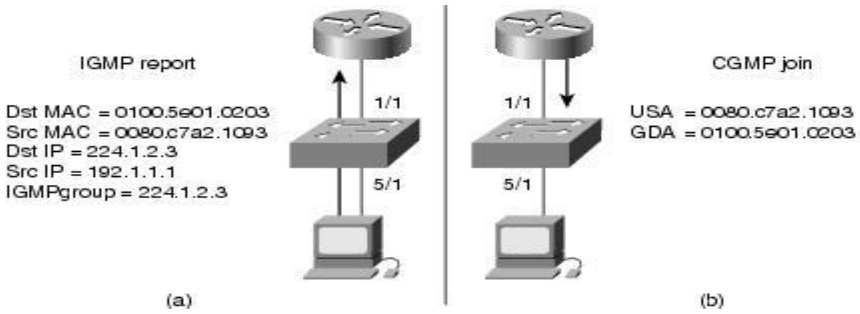
វិធីសាស្ត្រពីរដែលប្រើជាមួយ Multicast ក្នុង Layer 2 Switchingគឺ Cisco Group Management Protocol(CGMP) នឹង IGMP ។

៦-៥-១- Cisco Group Management Protocol (CGMP)

CGMP គឺជា Protocol របស់ Cisco ដែលអនុញ្ញាតឱ្យ Catalyst Switch កំណត់ព័ត៌មាន IGMP នៅលើ Cisoc Router ដើម្បីធ្វើឱ្យ Layer 2 សម្រេចបញ្ជូនបន្ត។ CGMP ត្រូវ Configure នៅលើ multicast routers នឹងលើ Layer 2 swicthes។ ជាលទ្ធផលជាមួយចរាចរណ៍ CGMP IP multicast ត្រូវទទួលតែចំពោះ Catalyst Switch Port ដែលប្រើសម្រាប់ចរាចរណ៍។ Ports ផ្សេងៗទៀតគ្មានចរាចរណ៍និងមិនទទួលវា។ មូលដ្ឋានគ្រឹះនៃ CGM បង្ហាញក្នុងរូបភាពខាងក្រោម។ នៅពេលដែល Host មួយចូលរួមក្នុង multicast group(Port A) វា multicast នូវ IGMP membership message ឱ្យគ្រប់គោលដៅក្រុម (224.1.2.3) ក្នុងឧទាហរណ៍។ របាយការណ៍ IGMP ត្រូវបានបញ្ជូនឆ្លងកាត់ Switch ទៅកាន់ Router ដើម្បីឱ្យ IGMP ដំណើរការ។ Router (ត្រូវតែមាន CGMP បើកនៅលើ interface នេះ) ទទួលរបាយការណ៍ IGMP ហើយដំណើរការវាតាមធម្មតា ប៉ុន្តែវាបង្កើត CGMP មួយដើម្បីចូលរួមសារនិងបញ្ជូនវាទៅឱ្យ switch។

Switch ទទួល CGMP នេះចូលក្នុងសារហើយបន្ទាប់មកបន្ថែម Port ឱ្យ CAM(content addressable memory) table សម្រាប់ multicast group។ ជាលទ្ធផលចរាចរណ៍ត្រូវបានដឹកនាំដោយផ្ទាល់ទៅឱ្យ multicast group នេះនិងត្រូវបញ្ជូនបន្តចេញតាម Port ចំពោះ Host នោះ។ Port របស់ Router ក៏ត្រូវបានបន្ថែមផងដែរចំពោះ multicast group។ Multicast routers ត្រូវបានបន្ថែមផងដែរចំពោះ multicast group។ Multicast routers ត្រូវតែស្តាប់ចំពោះចរាចរណ៍ Multicast ទាំងអស់ចំពោះ Group នីមួយៗពីព្រោះIGMPគ្រប់គ្រងសារដែល

ត្រូវបានបញ្ចូលជាលក្ខណៈចរាចរណ៍ multicast ផងដែរ។ ជាមួយ CGMP Switch ត្រូវតែស្តាប់ចំពោះCGMP ដែលចូលរួមនឹងCGMP ដែលចាកចេញសារពី Router ។ ផ្នែកនៅសល់របស់ចរាចរណ៍ multicast ត្រូវបានបញ្ជូនបន្តដោយប្រើ CAM table របស់វាដូចគ្នានឹងវិធីសាស្ត្រដែល Switch ត្រូវបានបង្កើតឡើង។



រូបភាព-៨- Basic CGMP Operation

IGMP Snooping

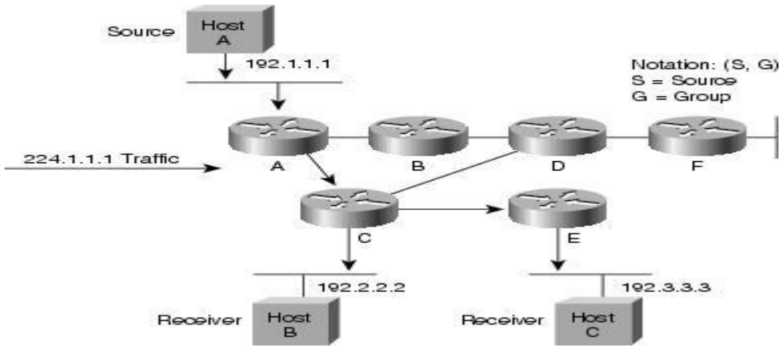
IGMP Snooping ទាមទារឱ្យ LAN Switch ត្រួតពិនិត្យនូវព័ត៌មានរបស់ Layer 2 នៅក្នុង IGMP packets ដែលត្រូវបានបញ្ជូនរវាង Host នឹង Router ។ នៅពេលដែល Switch ដឹងពីរបាយការនៃ IGMP host ពី Host មួយសម្រាប់ multicast group, switch បន្ថែម Port របស់ Host ទៅនឹង multicast table។ នៅពេលដែល Switch បានដឹងពី IGMP ចាកចេញពី Host មួយវាក៏លុប Port របស់ Host ពីតារាង។

៦-៦- Multicast Destination Trees

Router ដែលមានសមត្ថភាពបង្កើត Tree ជាគោលដៅដែលគ្រប់គ្រងផ្លូវបញ្ជូនដែលចារចរណ៍ IP multicast ឆ្លងកាត់តាម Network ដើម្បីទទួលយកចរាចរណ៍ឱ្យគ្រប់ឧបករណ៍ទទួល។ មាន Multicast destination trees ប្រភេទគឺ Source trees និង Share trees។

Source Trees

ជាទម្រង់ងាយរបស់ multicast destination tree គឺ Source tree ដែល Root របស់វាគឺជាប្រភពនៃ multicast tree ហើយសាខារបស់វាបង្កើតបានជា spanning tree តាមរយៈ Network មកកាន់ឧបករណ៍ទទួល។ ដោយសារតែ Tree នេះប្រើ Shortest Path តាមរយៈNetwork ដែលគេហៅវាថា Shortest Path Tree(SPT) ។



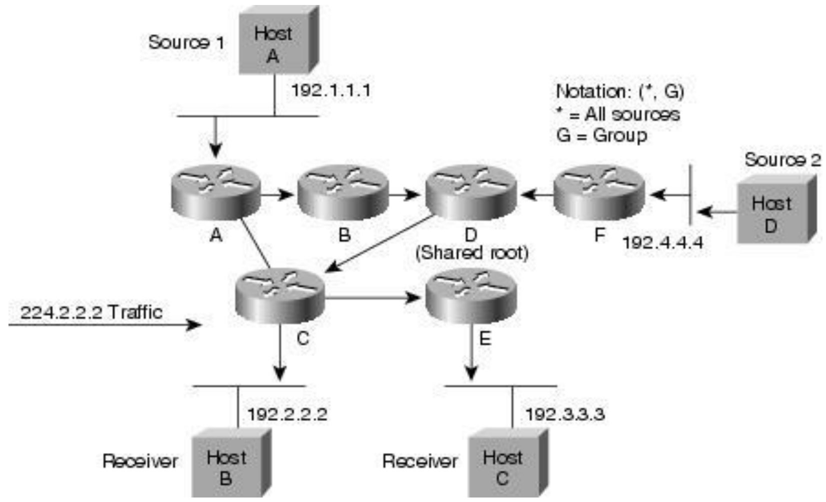
រូបភាព-៩- Host A Shortest Path Tree

(S,G) គេអាចថា " S comma G" ដែល S ជា IP address របស់ប្រភពដើមហើយ G ជា multicast group address។ ការប្រើសញ្ញាសម្គាល់នេះ SPT ក្នុងឧទាហរណ៍គឺ (192.1.1.1, 224.1.1.1) ។

សញ្ញាសម្គាល់(S,G) មានន័យថា SPT មានស្រាប់សម្រាប់ប្រភពដើមនីមួយៗដែលកំពុងបញ្ជូនឱ្យក្រុមនីមួយៗដែលត្រឹមត្រូវ។ ឧទាហរណ៍បើ Host B កំពុងបញ្ជូនចរាចរណ៍ឱ្យ Group 224.1.1.1 ហើយ Host A នឹង C គឺជាឧបករណ៍ទទួលនោះ (S,G) SPT មានសញ្ញាសម្គាល់(192.2.2.2, 224.1.1.1)។

Shared Trees

មិនដូចជា Source Tree ទេដែលមាន Root នៅឯប្រភពដើម Share tree ប្រើ root តែមួយគត់ដែលបានដាក់ត្រង់ចំណុចណាមួយក្នុង network ។ Shared root នេះគេហៅថា rendezrous point (RP)។ រូបខាងក្រោមបង្ហាញពី Shared Tree សម្រាប់ Group 224.2.2.2 ជាមួយ Root ដែលស្ថិតនៅឯ Router D។ នៅពេលយើងជ្រើសរើសយក Shared tree នោះ Source ត្រូវតែបញ្ជូនចរាចរណ៍របស់ពួកគេឱ្យ root ហើយបន្ទាប់មកចរាចរណ៍ត្រូវបញ្ជូនតាម Shared tree ទៅឱ្យឧបករណ៍ទទួលនីមួយៗ។



រូបភាព-១០-Shared Distribution Tree

នៅក្នុងឧទាហរណ៍នេះចរាចរណ៍ Multicast ពីប្រភពដើម Host A និង D ធ្វើដំណើរមក root (Router D) ហើយបន្ទាប់មកចុះមក Shared tree មកកាន់ឧបករណ៍ទទួលពីរគឺ Host B នឹង C។ ដោយសារតែប្រភពដើមទាំងអស់ស្ថិតនៅក្នុង multicast group ប្រើ Shared tree រួមគ្នា (*,G) អានថា "Star comma G" តំណាងឱ្យ tree។ ក្នុងករណីនេះ * មានន័យថាគ្រប់ប្រភពដើមទាំងអស់និង G តំណាងឱ្យ multicast group។ ដូច្នោះ Shared tree បង្ហាញក្នុងរូបខាងលើ(4.8)ត្រូវសរសេរជា(*, 224.2.2.2)។ ទាំង SPT នឹង Shared tree ជា loop-free។ Messages មាន replicate តែចំពោះ tree ដែលមានសាខា។

សំណួររំលឹកឡើងវិញ

Q—តើ Standard នៃ IP address ដែលកំពុងប្រើបច្ចុប្បន្នជា version ប៉ុន្មាន ?

A—IPv4.

Q—តើមានហេតុផលអ្វីខ្លះដែលគេបង្កើត IPv6 Addres ឡើង ?

A—ហេតុផលជាចម្បងនៃការបង្កើត IPv6 ឡើងគឺ IPv4 ដែលកំពុងប្រើនិងត្រូវបានប្រើអស់។ ដូច្នេះ IPv6 គឺជាដំណោះស្រាយ ប៉ុន្តែវានៅមិនទាន់ក្លាយជា Standard នៅឡើយនោះទេ។

Q—តើវាបានពង្រីកប៉ុន្មាន bits *?*

A—វាបានពង្រីកពី 32 bits មក 128 bits address

Q—តើការពង្រីកនោះវាផ្តល់បានផលប្រយោជន៍អ្វីខ្លះ *?*

A—វាបានផ្តល់ឱ្យនូវ unicast និង broadcasting method ថ្មី។ ចំពោះ Address ដែលបានពង្រីកថ្មីនេះបានប្រើសញ្ញា":" ជំនួសឱ្យ ".''។

Q—តើ broadcast method ថ្មីមាននៅក្នុង IPv6 អ្វីខ្លះ *?*

A—Unicast, multicast, and anycast.

Q—តើអ្វីទៅជា *unicast?*

A— Unicast គឺជាការប្រាស្រ័យទាក់ទងរវាងឧបករណ៍បញ្ជូនតែមួយនិងឧបករណ៍ទទួលតែមួយ

Q—តើអ្វីទៅជា *multicast?*

A—Multicast គឺជាការប្រាស្រ័យទាក់ទងរវាង Host តែមួយគត់និងឧបករណ៍ទទួលជាច្រើន

Q—តើ anycast គឺជាអ្វី *?*

A—Anycastគឺជាការប្រាស្រ័យទាក់ទងរវាងឧបករណ៍បញ្ជូនតែមួយនិងបណ្តុំនៃ IP adder sses

Q—តើ Range នៃ IP multicat addresses មានអ្វីខ្លះ *?*

A—224.0.0.0 to 239.255.255.255.

Q—តើ IGMP មានគោលបំណងអ្វីខ្លះ *?*

A—IGMP ត្រូវបានប្រើប្រាស់រវាង Host ជាច្រើននិង local multicast router របស់វាដើម្បីចូលរួមក្នុងក្រុមនិងចាកចេញពី multicast groups.

Q—តើអ្វីខ្លះជាគុណសម្បត្តិនៃ *IGMPv2* មកលើ *IGMPv1?*

A—IGMPv2 មាន leave group message ដែលកាត់បន្ថយនូវ latency នៃចរាចរណ៍ដែលមិនត្រូវការនៅលើ LAN.

Q—តើអ្វីខ្លះជាគុណវិបត្តិនៃ *IGMP snooping* មកលើ *CGMP* ចំពោះ *low-end Layer 2 switch?*

A—IGMP snooping ទាមទារឱ្យ switch ត្រួតពិនិត្យនៅគ្រប់ multicast packet សម្រាប់ IGMP control message ។ ចំពោះ switch វិញ វាមានផលប៉ះពាល់យ៉ាងខ្លាំងចំពោះសមត្ថភាព

Q—តើអ្វីជាគុណសម្បត្តិនៃ *shortest path (or source) trees* បើប្រៀបធៀបទៅនិង *shared trees?*

A—Source trees ជានាផ្លូវបញ្ជូនស្រេចចិត្តរវាងឧបករណ៍បញ្ជូននិងឧបករណ៍ទទួលនីមួយៗមានន័យថាវាបានកាត់បន្ថយនូវ network latency.

Q—តើអ្វីជាគុណសម្បត្តិនៃការប្រើ *shared trees?*

A—Shared trees ទាមទារនូវលក្ខណៈរបស់វាតិចបំផុតដែលស្ថិតនៅក្នុង routers មានន័យថាត្រូវការ Memory តិច

Q—តើព័ត៌មានអ្វីខ្លះដែល *router* ប្រើដើម្បីធ្វើ *RPF check?*

A—The unicast routing table.

Q—ហេតុអ្វីបានជាprotocol-independent multicast ត្រូវបានគេហៅថាជា "independent"?

A—PIM ធ្វើការជាមួយ IP unicast routing protocol—RIP, EIGRP, OSPF, BGP or static routes.

Q—តើអ្វីជាគុណសម្បត្តិនៃ *MBGP ?*

A—Providers can have noncongruent unicast and multicast routing topologies.

Q—*How do RPs learn about sources from other RPs with MSDP*?

A—RPs are configured to be MSDP peers with other RPs. Each RP forwards source active (SA) messages to each other.

Q—*What is the purpose of the anycast RP ?*

A—Load balancing and fault tolerance

ជំពូកទី៧

Routing Algorithm

៧-១- Distance Vector Algorthm

សេចក្តីផ្តើម

Distance Vector routing protocols ប្រើ broadcasts(255.255.255.255 ឬ FF:FF:FF: FF) របស់ routing table ទាំងមូលរបស់វារៀងរាល់៣០វិនាទី។ នៅគ្រប់ interfaces របស់វាក្នុងគោលបំណងប្រាស្រ័យទាក់ទងជាមួយ Router ជិតខាងរបស់វា។ នៅពេលដែល routing tables កាន់តែធំ broadcasts ក៏មានកាន់តែច្រើនដែរ។ វិធីសាស្រ្តនេះកំណត់ទំហំរបស់ network លើ Distance Vector ដែលត្រូវប្រើប្រាស់ ។

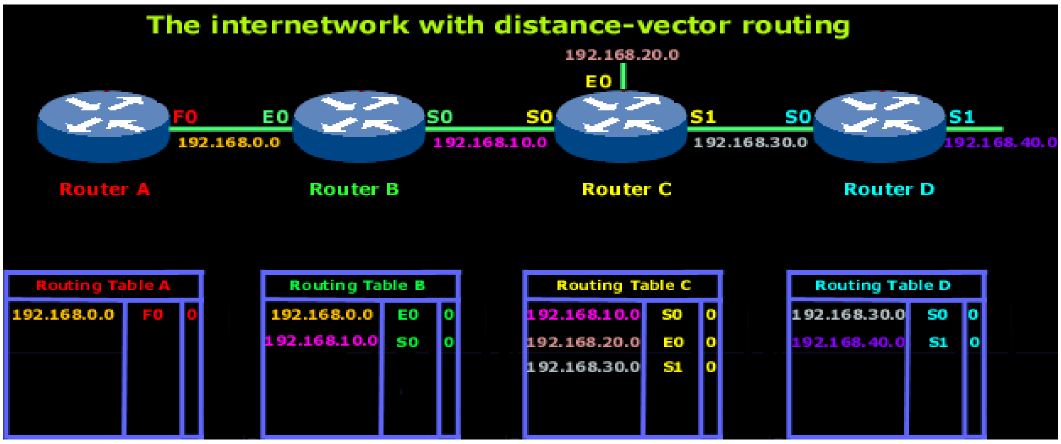
Routing Information Protocol (RIP) និង Interior Gateway Routing Protocol (IGRP) គឺជា Distance Vector routing protocols ពីរដែលគេនិយមប្រើបំផុត។ អ្នកអាចស្វែងរក link ចំពោះព័ត៌មានបន្ថែមអំពី protocols ទាំងនេះ ។

Distance Vector protocols បានមើល networks សំដៅលើ routers ដែលស្ថិតនៅជាប់ៗគ្នានិង hop counts ដែលកើតឡើងហើយត្រូវបានប្រើជា metric។ "hop" count (ចំនួនអតិបរិមាគឺ១៥សម្រាប់ RIP និង ១៦ គឺជា unreachable និង 255 សម្រាប់ IGMP) និងកើនម្តងមួយៗរៀងរាល់ពេលដែល Packet ឆ្លងកាត់ router ។

ដូច្នេះ router ធ្វើការសម្រេចចិត្តអំពីផ្លូវដែល packet មួយនិងធ្វើដំណើរដោយពឹងផ្អែកលើចំនួន hops ដែលវាគិតដើម្បីមកដល់គោលដៅហើយបើផ្លូវពីរផ្សេងគ្នាទៅដល់គោលដៅតែមួយវានិងបញ្ជូនតាមផ្លូវដែលខ្លីជាងគេបំផុតដោយមិនគិតពីល្បឿន ។ នេះគេហៅថា pin hole congestion ។

ខាងក្រោមនេះគឺជា routing table របស់ router មួយដែលប្រើ Distance Vector routing

protocols:

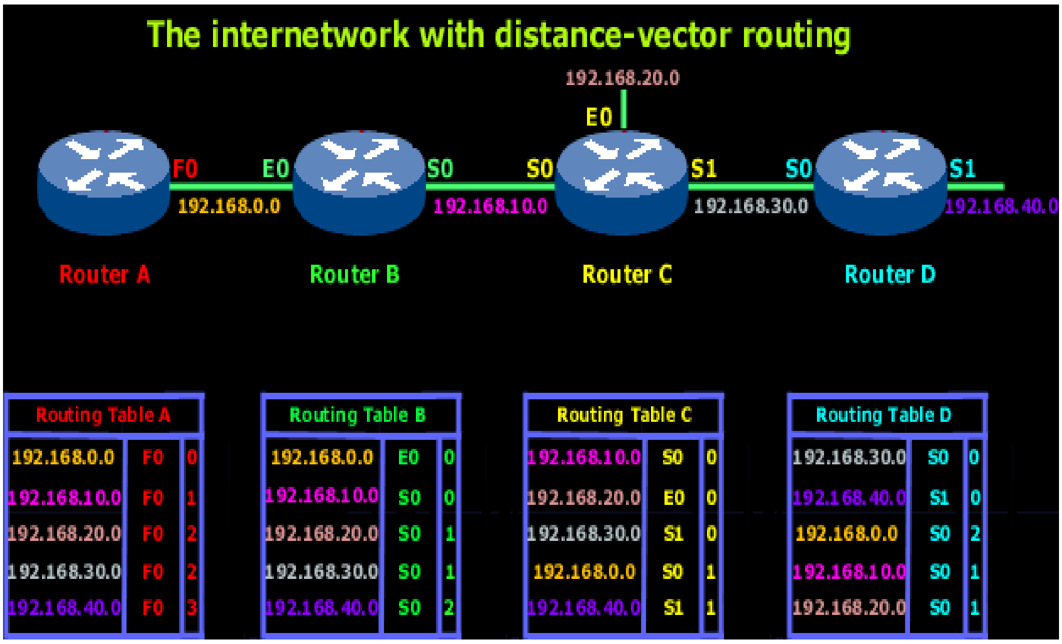


ក្នុងរូបភាពខាងលើ អ្នកឃើញ routers ចំនួន៤ ដែលនីមួយៗភ្ជាប់ជាមួយ Router ជិតខាងរបស់វាតាមប្រភេទនៃ WAN link មួយចំនួនដូចជា ISDN ។

នៅពេលបើកភ្លើងរបស់ router វានិងស្គាល់ភ្លាមអំពី networks ដែលវាអាចភ្ជាប់ជាមួយតាម interface ។ ក្នុងករណីនេះ **Router B** ស្គាល់ interface E0 បានភ្ជាប់ជាមួយ 192.168.0.0 network ហើយ S0 interface ត្រូវបានភ្ជាប់ជាមួយ 192.168.10.0network ។

សូមពិនិត្យម្តងទៀតនៅឯ routing table ចំពោះ Router B ចំនួនដែលអ្នកបានឃើញនៅខាងស្តាំនៃ interfaces គឺជា "hop counts" ដែលជា metric ដែល distance vector protocols ប្រើសម្រាប់រក្សាពីរបៀបរកផ្លូវបញ្ជូនចំពោះ network ពិសេសណាមួយ។ ដោយហេតុថា networks ចំនួនពីរត្រូវបានភ្ជាប់ដោយផ្ទាល់ជាមួយ interface របស់ router វានិងមានតម្លៃសូន្យក្នុង table entry របស់ router ។ ច្បាប់ដូចគ្នានេះអនុវត្តចំពោះគ្រប់ router ក្នុងឧទាហរណ៍ ។

យើងត្រូវចាំថា យើងគ្រាន់តែបើកភ្លើងរបស់ Router ដូច្នេះ network ត្រូវបាន converge មានន័យថាគ្មាន data ត្រូវបញ្ជូន។ នៅពេលខ្ញុំនិយាយថា"គ្មាន data"មានន័យថា data ពី កុំព្យូទ័រ ណាមួយឬ server អាចនៅលើ networks ណាមួយ។ ក្នុងពេល "convergence" នេះ មានតែ data មួយប្រភេទត្រូវបានឆ្លងកាត់រវាង routers ដែលអនុញ្ញាតឱ្យវាផ្សព្វផ្សាយ routing tables របស់វានិងក្រោយមក routers និងបញ្ជូន data គ្រប់ប្រភេទទាំងអស់រវាងគ្នាវា។ ហេតុដូច្នោះហើយមានជារយៈពេល convergence គឺជាគុណវិបត្តដ៏ធំមួយ។ បញ្ហាមួយរបស់វាជាមួយ RIP គឺថាវាមាន convergence timeយឺត ។



ចូរពន្យល់ពីអ្វីដែលយើងបានឃើញ។

ក្នុងរូបភាពខាងលើ network ត្រូវបានគេនិយាយថាមាន "converged" គ្រប់ routers ទាំងអស់នៅលើ network បានផ្សព្វផ្សាយ routing table របស់វាហើយត្រូវដឹងពី networks ដែលវាបានទាក់ទង ដោយ network ត្រូវបាន converge កុំព្យូទ័រក្នុង networks ខាងលើអាចទាក់ទងគ្នាបានជាមួយគ្នា។

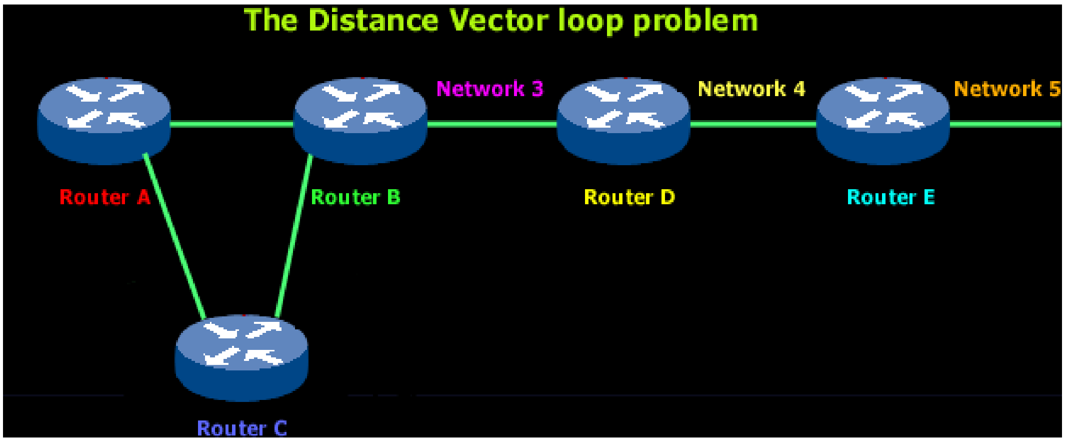
ម្តងទៀតសូមពិនិត្យមើល routing tables មួយដែលអ្នកនិងចំណាំថា network address ដែលមាន interface នៅខាងស្តាំហើយបន្ទាប់មកទៀតគឺថាវាជា hop count ចំពោះ network។ ត្រូវចាំថា RIP និងមានតែ 15 hops ប៉ុណ្ណោះ បើលើសពីនោះ packet ត្រូវបានបោះចោល។

router នីមួយៗនិង broadcast routing table ទាំងមូលរបស់វាគ្រប់៣០វិនាទីម្តង។

Routing ដែលពឹងផ្អែកលើ Distance Vector អាចបណ្តាលឱ្យមានបញ្ហាច្រើននៅពេល links ភ្ជាប់និងផ្តាច់ដែលជាហេតុបណ្តាលឱ្យមាន loop មិនកំណត់ហើយអាចជា de-synchronise network

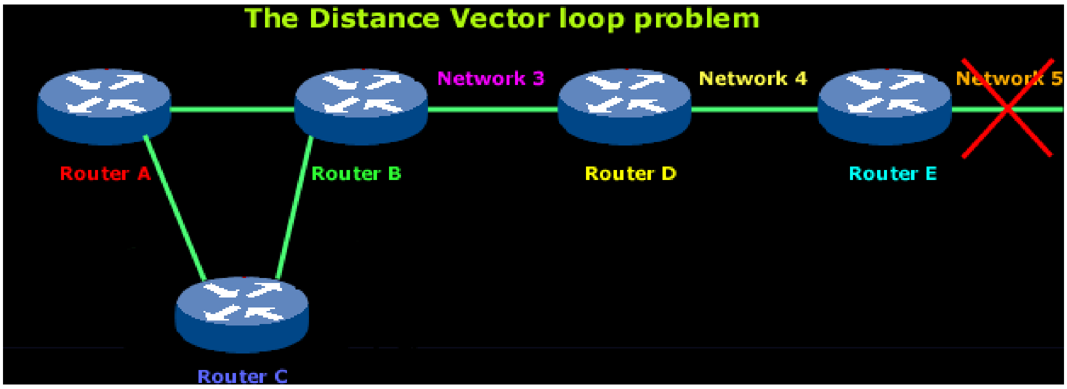
Routing loops អាចកើតឡើងនៅពេលគ្រប់ router មិនត្រូវបាន updated នៅពេលតែមួយ ។

សូមពិនិត្យមើលបញ្ហាមុនពេលយើងពិនិត្យមើលពីដំណោះស្រាយ:

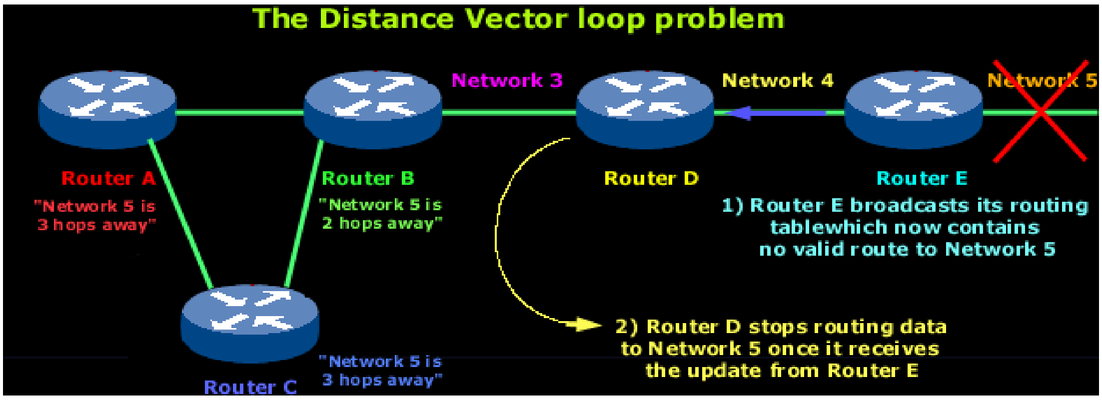


សូមពន្យល់

ក្នុងរូបភាពខាងលើអ្នកអាចឃើញ Router ៥ ដែល routers A និង B ត្រូវបានភ្ជាប់ជាមួយ Router C ហើយវាទាំងភ្ជាប់ជាមួយគ្នាតាម routers D និង E ចំពោះ Network 5 ។

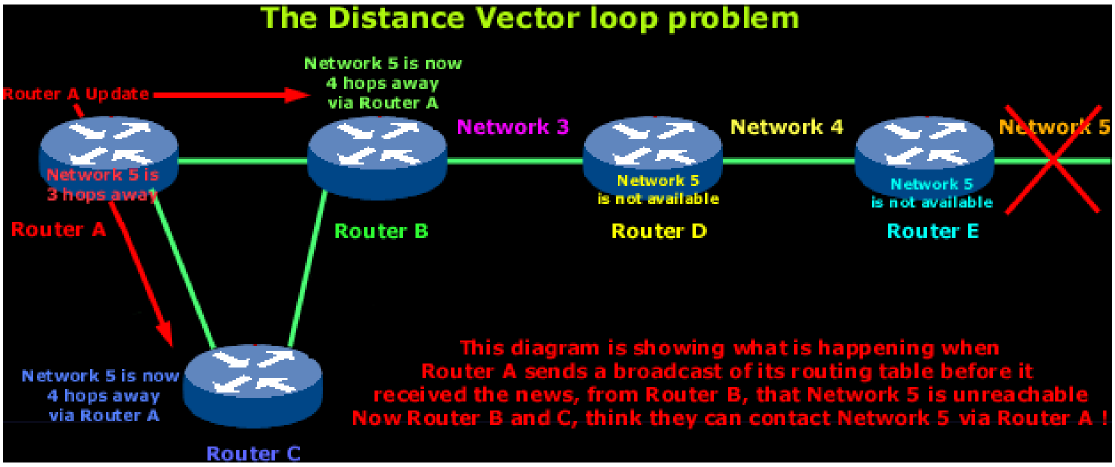


ដូចរូបភាពខាងលើ Network 5 បរាជ័យ ។



គ្រប់ routers ទាំងអស់ស្គាល់អំពី Network 5 ពី Router E ។ ឧទាហរណ៍ Router A ក្នុង tables របស់វាមានផ្លូវមកកាន់ Network 5 តាមរយៈ routers B,D និង E ។

នៅពេល Network 5 បរាជ័យ Router E បានស្គាល់វាអំពីវាពីព្រោះវាបានភ្ជាប់ជាវាដោយផ្ទាល់ហើយប្រាប់ Router D អំពីវានៅលើ update លើក្រោយរបស់វា(នៅពេលវា broadcast routing table របស់វា)។ នេះនិងផ្តល់លទ្ធផលក្នុង Router D បញ្ឈប់ routing data ចំពោះ Network 5 តាមរយៈ Router E ។ ប៉ុន្តែដូចអ្នកបានឃើញក្នុងរូបភាពខាងលើ routers A B និង C មិនបានដឹងអំពី Network 5 នោះទេ ដូច្នេះវានៅតែបញ្ជូន update information។ Router D និងបញ្ជូន update របស់វានិងធ្វើឱ្យ Router B បញ្ឈប់ routing ចំពោះ Network 5 ប៉ុន្តែ routers A និង C មិនត្រូវបាន updated ។ ចំពោះវា វានិងបង្ហាញ Network 5 មានតាមរយៈ Router B ជាមួយ metric នៃ 3 ។



ឥឡូវនេះ Router A បញ្ជូន broadcast របស់វាជាទៀងទាត់នៅ routing table របស់វាដែលរួមមានភាពដែលអាចភ្ជាប់បានសម្រាប់ Network 5។ Routers C និង B ទទួលព័ត៌មានថ្មីថា Network 5 អាចភ្ជាប់ជាមួយវាពីRouter A ដូច្នេះវាបញ្ជូនព័ត៌មានថា network 5 មានត្រៀមជាស្រេច ។

ចាប់ពីពេលនេះទៅ packet ណាមួយមានគោលដៅជា Network 5 និងទៅ Router A ហើយបន្ទាប់មក Router B និងបានត្រឡប់មក Router A (ត្រូវចាំថា Router B ទទួលព័ត៌មានថ្មីថា Network 5 បានត្រៀមរួចរាល់តាម Router A) ។

ដូច្នេះវាគឺជាការទទួលបាន bit ញើរញៃហើយអ្នកទទួលបាន loop ដ៏អស្ចារ្យមួយដែល data បានឆ្លងកាត់ពី router មួយទៅ Router មួយទៀត ។ វាហាក់ដូចជាការលេងពីងប៉ុងដែរ ។
ដើម្បីដោះស្រាយបញ្ហាគេប្រើបច្ចេកទេសដូចខាងក្រោម:

៧-១-១- ចំនួន Hop Count អតិបរមា

routing loop ដែលយើងទើបពិនិត្យត្រូវបានគេហៅថាជា "counting to infinity" ហើយដែលបណ្តាលដោយព័ត៌មានខុសដែលកំពុងប្រាស្រ័យទាក់ទងរវាង routers និង routers។ បើគ្មានអ្វីទប់ស្កាត់ប្រកែទៃ loop នេះទេ hop count និងរក្សាការកើនឡើងគ្រប់ពេលដែល Packet ឆ្លងកាត់ router មួយ។ វិធីមួយនៃការដោះស្រាយបញ្ហានេះគឺកំណត់ចំនួន hop count អតិបរមា។ Distance Vector(RIP) អនុញ្ញាតឱ្យ hop count មានតម្លៃរហូតដល់ 15 ដូច្នេះបើលើសពី១៥(១៦)គឺជា Network ដែលមិនអាចភ្ជាប់បាន ។ ដូច្នេះបើមាន loop មួយកើតឡើង

វានិងធ្វើដំណើរជុំវិញ network រហូតទាល់តែ packet មានតម្លៃនៃ hop count ស្មើ 15 ហើយ next router និងបោះ packet ចោល ។

៧-១-២- Split Horizon

ការធ្វើការលើគោលការណ៍ដែលវាគ្មានសារៈសំខាន់នោះគឺការបញ្ជូនព័ត៌មានអំពី router មួយត្រឡប់ឱ្យគោលដៅ packet ដើមវិញ។ ដូច្នេះបើខ្ញុំប្រាប់អ្នកអំពីរឿងកំប្លែងមួយ វាមិនអាចនិយាយថា អ្នកប្រាប់ខ្ញុំវិញអំពីរឿងកំប្លែងនោះម្តងទៀតទេ ។

នៅក្នុងឧទាហរណ៍របស់យើង មាន Router A មួយត្រូវបានគេការពារវាពីការបញ្ជូនព័ត៌មានត្រូវបាន update ដែលវាបានទទួលពី Router B ត្រឡប់មក Router B វិញនោះបានទេ។

៧-១-៣- Route Poisoning

គឺជាដំណោះស្រាយមួយទៀតចំពោះ split horizon ។ នៅពេលដែល router មួយទទួលព័ត៌មានអំពី route មួយពី network ពិសេសណាមួយ router ក៏ផ្សព្វផ្សាយអំពី route ត្រឡប់ឱ្យ network នោះជាមួយ metric ស្មើ 16 ដែលចង្អុលបង្ហាញថាគោលដៅ Network មិនអាចភ្ជាប់បាន ។

ក្នុងឧទាហរណ៍របស់យើងគឺមានន័យថានៅពេល Network 5 ខូច Router E ក៏ចាប់ផ្តើម router ដែលកំពុងបំពុលដោយការបញ្ចូលនៅ table entry មួយសម្រាប់ Network 5 ជាតម្លៃ 16 មានន័យថាមិនអាចភ្ជាប់បាន (unreachable)។ ក្នុងវិធីនេះ Router D មិនទទួលការ updates ខុសអំពី route ចំពោះ Network 5។ នៅពេល Router D ទទួល router មួយដែលកំពុងបំពុលពីRouter E វាបញ្ជូន update មួយហៅថា poison reverse ត្រឡប់មក Router E ។ នេះធ្វើឱ្យគ្រប់ផ្លូវបញ្ជូនទាំងអស់នៅលើ segment បានទទួលព័ត៌មានដែលបានបំពុល ។

ផ្លូវបញ្ជូនដែលបានបំពុលបានប្រើជាមួយ hold-downs និងបង្កើនល្បឿននៅរយៈពេល conver -gence ពីព្រោះrouters ដែលនៅជិតៗវាគ្មានរងចាំរហូតដល់ ៣០វិនាទីមុនពេលផ្សព្វ ផ្សាយផ្លូវបញ្ជូនដែលបានបំពុល ។

៧-១-៤- Hold-Down Timers

Routers រក្សាទុក entry មួយដែលនិយាយអំពី network បានខូចដែលកំពុងអនុញ្ញាតឱ្យ routers ផ្សេងៗទៀតគណនាអំពី topology ដែលបានប្តូរ។ តាមវិធីនេះការអនុញ្ញាតពេលវេលាចំពោះ router ដែលខូចត្រឡប់មកដើមវិញឬ network ដែលមានស្ថេរ ភាពមុនពេលវាប្តូរចំពោះផ្លូវបញ្ជូនបន្ទាប់ ។

នៅពេល router មួយទទួលការ update ពីអ្នកជិតខាងវាបង្ហាញថា accessible network ពីមុនមិនដំណើរការហើយមិនអាច access បាន។ hold-down timer និងដំណើរការ។ បើ update ថ្មីមួយទទួលពី neighbor មួយមាន metric មួយល្អប្រសើរជាង network entry ដើមរបស់វា hold-down ត្រូវបានលុបចោលហើយ data ត្រូវបានបញ្ជូន។ ប៉ុន្តែ update មួយត្រូវបានទទួលពី neighbor router មួយមុនពេល hold-down timer ត្រូវបានផុតកំណត់និងមាន metric តិចជាង route ពីមុន។ ដូច្នេះ update មិនត្រូវបានអើពើហើយ hold-down timer នៅតែមាន។ វាអនុញ្ញាតឱ្យមានពេលវេលាច្រើនសម្រាប់ network ចំពោះ converge ។

Hold-down timers ប្រើ triggered updates ដែលធ្វើឡើងវិញចំពោះ hold-down timer គឺជាការប្រកាសឱ្យដឹងពី Router របស់អ្នកជិតខាងដែលបានប្តូរក្នុង network។ មិនដូចទៅនិង update messages ពី routers ជិតខាង triggered updates បង្កើត routing table ថ្មីដែលត្រូវបានបញ្ជូនភ្លាមឱ្យ neighbor routers ពីព្រោះវាបានដឹងថាមានការផ្លាស់ប្តូរក្នុង network ។

មាន instances បីកើតឡើងនៅពេល triggered updates និងធ្វើឡើងវិញចំពោះ hold-down timer:

1) hold-down timer ត្រូវបានផុតកំណត់

2) router បានទទួល processing task ជាផ្នែកៗចំពោះចំនួនរបស់ links ក្នុង internetwork

3) update មួយផ្សេងទៀតត្រូវបានទទួលចង្អុលបង្ហាញថា network ត្រូវបានផ្លាស់ប្តូរ

នៅក្នុងឧទាហរណ៍របស់យើង update ណាមួយទទួលបានដោយ Router B ពី Router A និងមិនទទួលលុះត្រាតែ hold-down timer ត្រូវបានផុតកំណត់។ នេះប្រាកដថា Router B និងមិនទទួលការ update ខុសពី routers ណាមួយដែលមិនបានស្គាល់ថា Network 5 មិនអាចភ្ជាប់បាន។ បន្ទាប់មក Router B និងបញ្ជូន update មួយហើយបានកែ tables របស់ routers ផ្សេងទៀត ។

៧-២- សេចក្តីផ្តើមចំពោះ Link State

Link State protocols មិនដូចទៅនិងDistance Vectorដែល broadcasts របស់វាប្រើ multicast ។

Multicast គឺជា "broadcast" មួយចំពោះក្រុមនៃ hosts ក្នុងករណី Router នេះ បើយើងមាន Routers ចំនួន១០ដែល Router ចំនួន៤គឺជាផ្នែកមួយនៃ "mutilcast group" មួយនោះនៅពេលយើងបញ្ជូនចេញ multicast packet មួយឱ្យក្រុមនេះគឺមានតែ Routers ចំនួន៤ប៉ុណ្ណោះដែលទទួល updates រីឯផ្នែកនៅសល់វានិងមិនអើពើចំពោះdata។ multicast address គឺមានលេខជា 224.0.0.5 & 224.0.0.6 ដែល address នេះកំណត់ដោយ IGRP (Interior Gateway Routing Protocol) ។

Link State routing protocols មិនបានមើលពី routers ដែលនៅជាប់ៗគ្នានិង hop counts នោះទេ ប៉ុន្តែវាបង្កើតនៅការពិនិត្យមើលnetwork ទាំងមូលដែលពិពណ៌នាអំពីផ្លូវបញ្ជូនដែលអាចបញ្ជូនបានជាមួយតម្លៃរបស់វា។ ការប្រើ SPF (Shortest Path First) al gorithm router បង្កើតជា "topological database" ដែលជាទម្រង់នៃរចនារបស់ network routers ដែលវាបានដឹងពីខ្លួនវា។ បន្ទាប់មកវាដាក់ខ្លួនវានៅផ្នែកខាងលើបំផុតនៃទម្រង់រៀបតាមលំដាប់ ។

នៅពេល router មួយប្រើ Link State protocol មួយដូចជា OSPF (Open Shortest Path First) ដែលស្គាល់អំពីការប្តូរលើ network វានិង multicast ការផ្លាស់ប្តូរនេះ ដូចនេះវា flood ឱ្យ network ជាមួយព័ត៌មាននេះ។ ព័ត៌មានដែលroutersត្រូវការសម្រាប់បង្កើត databases របស់វាត្រូវបានផ្តល់ក្នុងទម្រង់របស់ Link State advertisement packets (LSAP)។ Routers មិនផ្សព្វផ្សាយនៅ routing tables ទាំងមូលនោះទេ ផ្ទុយទៅវិញ router នីមួយៗផ្សព្វផ្សាយតែព័ត៌មានរបស់វាប៉ុណ្ណោះដោយគិតពី routers ដែលស្ថិតនៅជាប់គ្នា ។

Link State protocols ប្រៀបធៀបជាមួយ Distance Vector protocols មានដូចខាងក្រោម:

- ត្រូវការទំហំ Memory ធំ
- ការគណនា Shortest path ត្រូវការ CPU circles ជាច្រើន
- បើ Network មានស្ថេរភាពហើយមានការប្រើប្រាស់ bandwidth តិចនោះវាមានប្រតិកម្មរហ័សចំពោះការផ្លាស់ប្តូរ topology
- ការផ្សព្វផ្សាយមិនអាចប្រោះបានទេ ។ គ្រប់ Items ទាំងអស់នៅក្នុង database ត្រូវតែបញ្ជូនឱ្យ Router នៅជិតខាង

- គ្រប់Router នៅជិតខាងត្រូវតែមានទំនុកចិត្ត
- Authentication mechanisms ត្រូវបានប្រើប្រាស់ដើម្បីជៀសវាងភាពជាប់គ្នាដែលមិនត្រូវការ
- គ្មាន split horizon កើតឡើង

ទោះបីជា Link State protocols ដំណើរការបានល្អយ៉ាងណាក៏ដោយបញ្ហានៅតែកើតមានឡើង។ តាមធម្មតាបញ្ហាអាចកើតឡើងបណ្តាលមកពីមានការផ្លាស់ប្តូរក្នុង network topology (ដូចជាមានខ្សែដាច់ជាដើម) ហើយគ្រប់ Routers មិនទទួលបានការ Update ភ្លាមនោះទេពីព្រោះវាស្ថិតនៅលើកម្រិតល្បឿនខុសគ្នា ដូច្នេះ Router ដែលភ្ជាប់តាមបណ្តាញដែលមានល្បឿនលឿននិងទទួលបានការ Update លឿនជាង

បច្ចេកទេសផ្សេងៗត្រូវបានបង្កើតឡើងដើម្បីដោះស្រាយបញ្ហាមានដូចជា

1) កាត់បន្ថយការ update ជាញឹកញាប់
2) Target link-state updates ប្រើ multicast
3) ប្រើ link-state area hierarchy សម្រាប់ topology
4) ផ្លាស់ប្តូរព័ត៌មានសង្ខេបពីផ្លូវបញ្ជូននៅឯ area borders
5) ប្រើប្រាស់ Time-stamps Update numbering & counters
6) គ្រប់គ្រង់ partitions ដោយប្រើ area hierarchy

ជំពូកទី៨

ការ Configure Peer to Peer Network

៨-១- ការ Configure Network ជា Peer-to-Peer Network

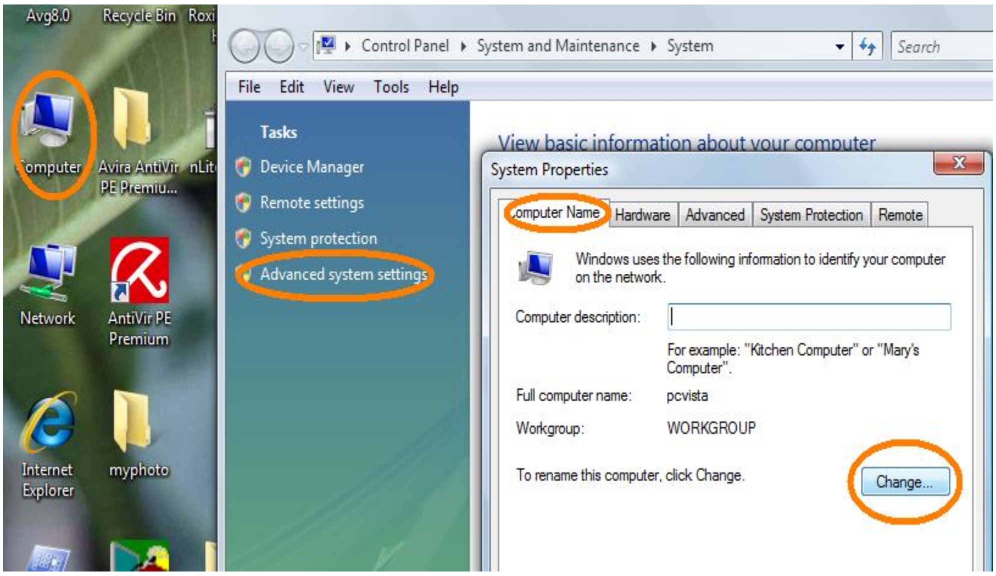
នៅក្នុង Peer-to-Peer Nerwork ឬ Workgroup កុំព្យូទ័រត្រូវតែភ្ជាប់គ្នាដោយគ្មាន Server ហើយគេប្រើវាសម្រាប់តែចែកចាយនូវធនធានផ្ទាល់ខ្លួនតែប៉ុណ្ណោះ។

៨-១-១- ការដាក់ឈ្មោះឱ្យកុំព្យូទ័រ workgroup

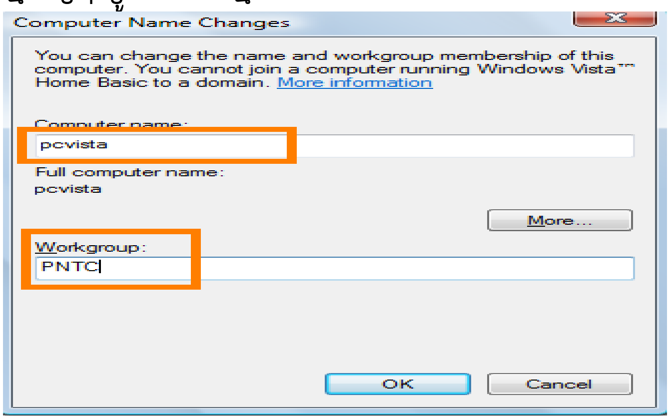
នៅក្នុង Network មួយគឺគ្រប់កុំព្យូទ័រទាំងអស់មិនអាចមានឈ្មោះដូចគ្នាបានហើយឈ្មោះរបស់កុំព្យូទ័រនីមួយៗមានអាចដូចទៅនឹងឈ្មោះរបស់ Workgroup។ គ្រប់កុំព្យូទ័រទាំងអស់ដែលស្ថិតនៅក្នុង Workgroup តែមួយអាចទាញយកធនធានរបស់ network នៅពេលតែមួយបាន។

៨-១-២- ការដាក់ឈ្មោះឱ្យកុំព្យូទ័រ

a. Right-click on the កុំព្យូទ័រ => properties=>Advanced system settings=>change.



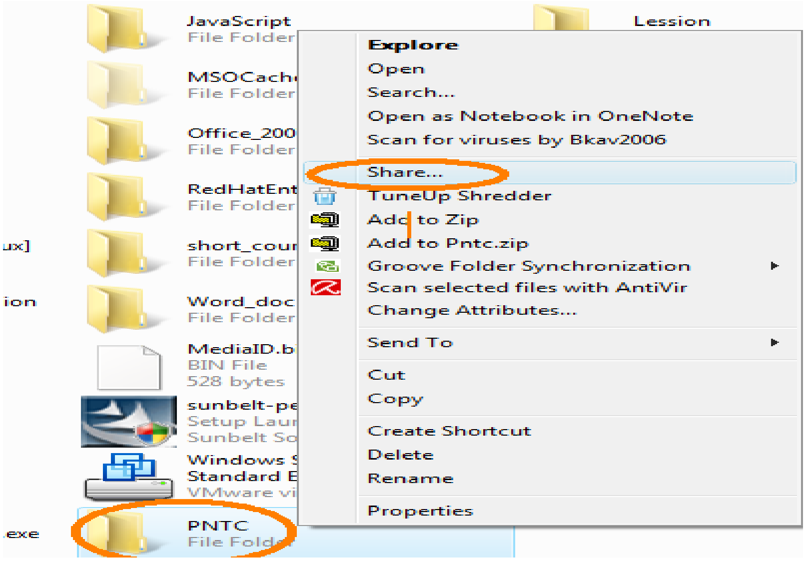
b. ដាក់ឈ្មោះឱ្យកុំព្យូទ័រ និងឈ្មោះរបស់ workgroup

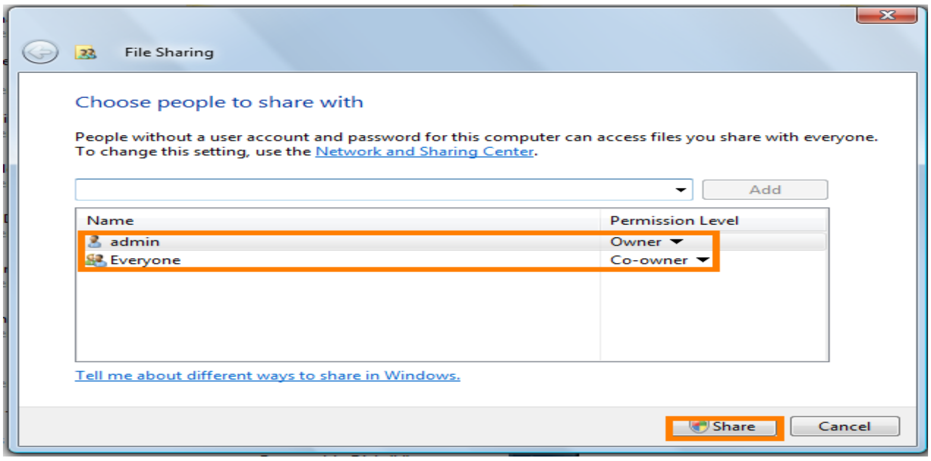


c. Ok ។ System របស់អ្នកនិងចាប់ផ្តើមសារជាថ្មីដើម្បីឱ្យមានប្រសិទ្ធិភាពចំពោះអ្វីដែលយើងបានផ្លាស់ប្តូរ

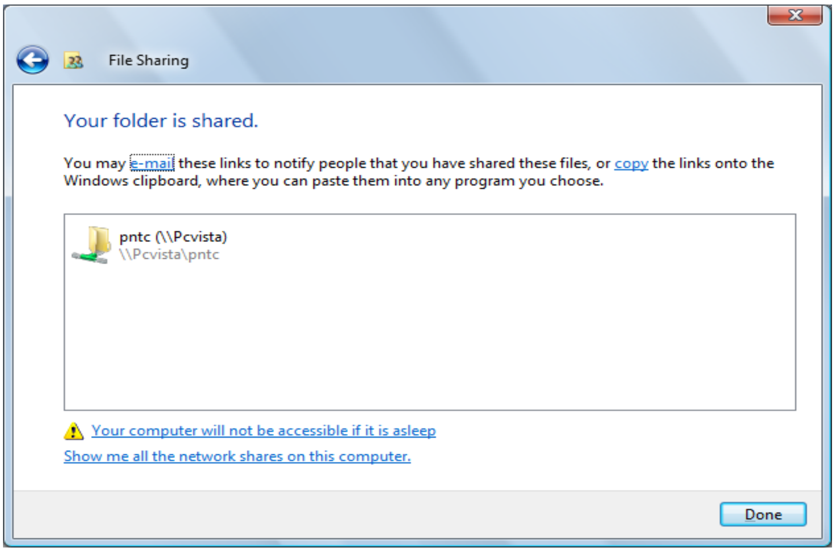
៨-២- របៀបចែលរំលែក local resources

1- Right-click លើ folder ឬ drive ដែលត្រូវចែកចាយ





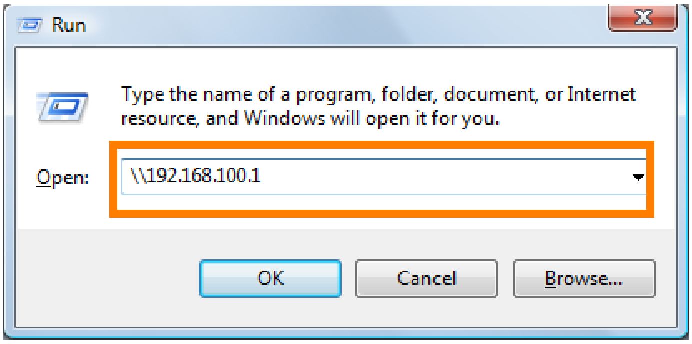
2- click on Share



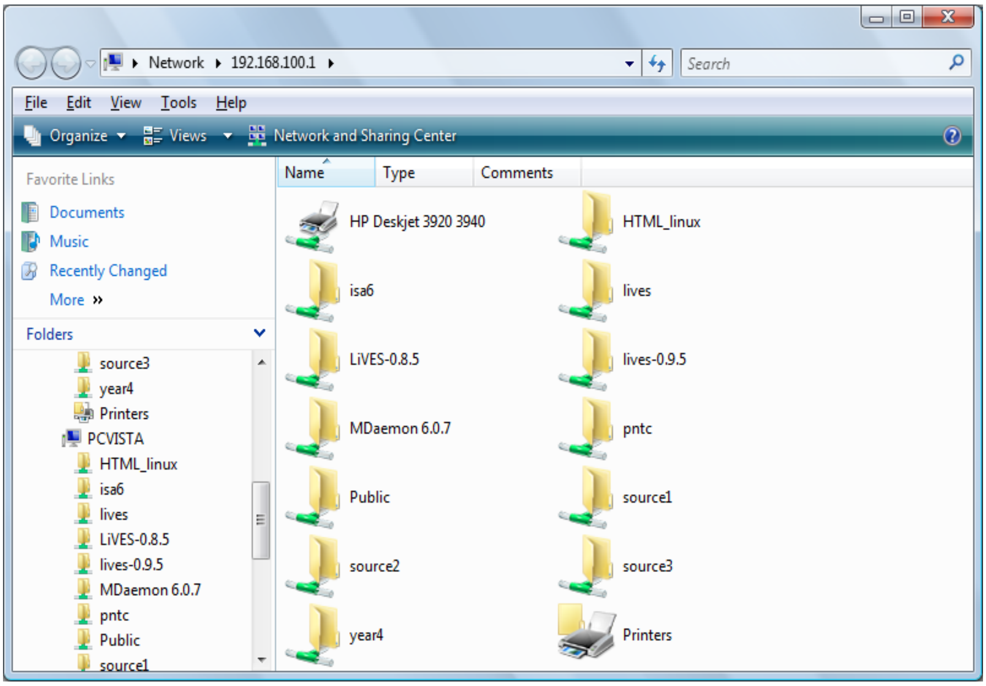
3- done

៨-៣- របៀបចូលប្រើ resource ដែលបានចែកចាយ (network resource)

1- Go to start=>run and type



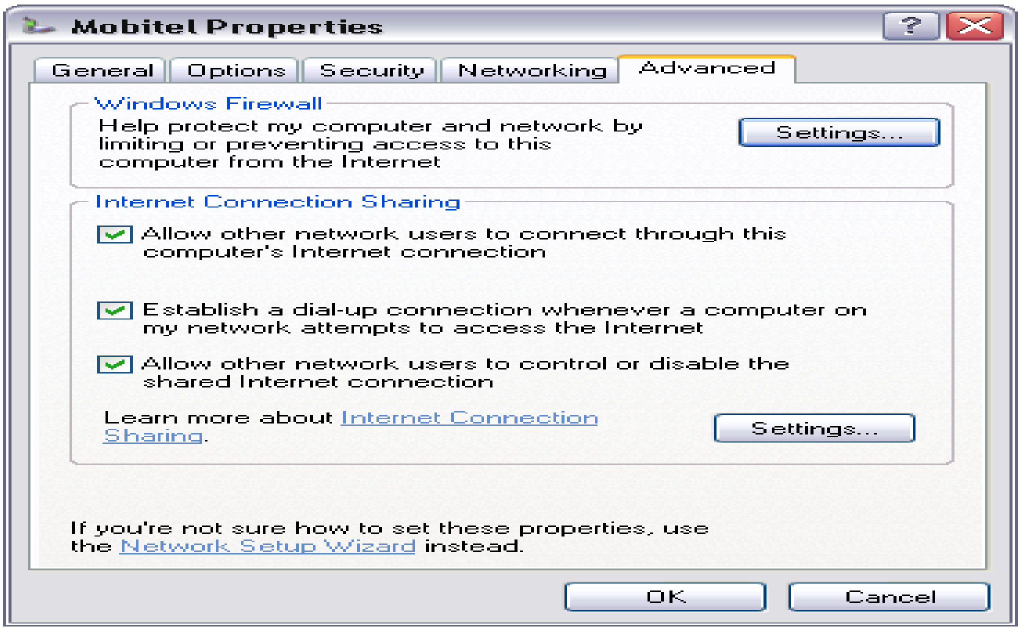
2- Ok



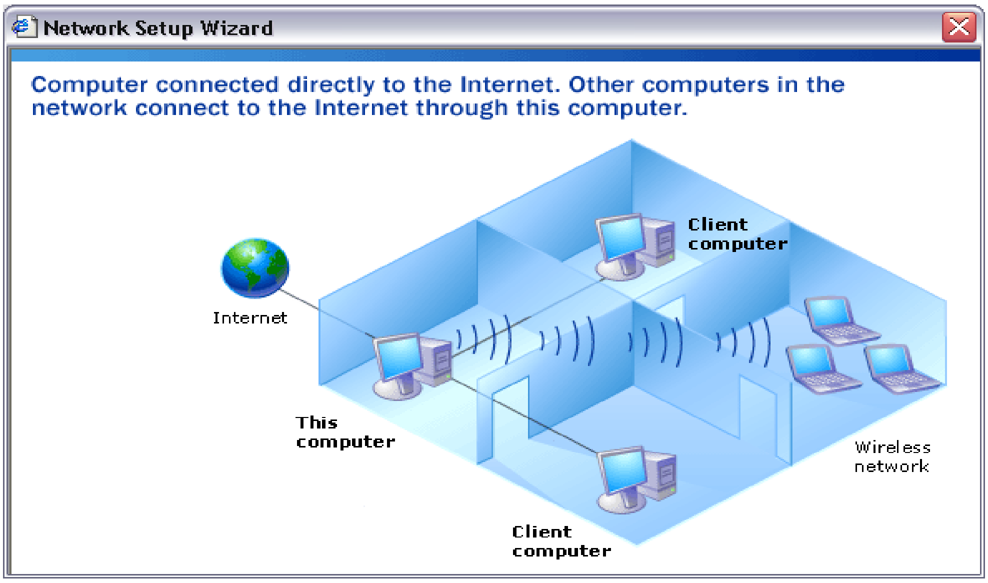
៨-៤- ការចែកចាយ Internet

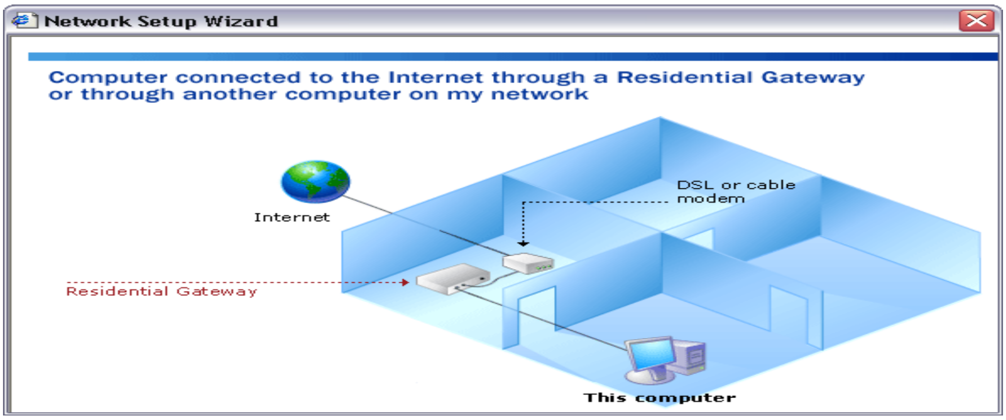
វាមាន Tool តែមួយគត់ដែលគេប្រើសម្រាប់ចែកចាយ Internet នៅក្នុង Windows 2000 professional /XPគឺ ICS (Internet Connection Sharing)។ ICS ត្រូវបានគេប្រើជា DHCP server តូចមួយសម្រាប់ចែកចាយ IP address ក្នុងការចែកចាយ Internet ។ វាអាចកំណត់ IP address បានចំនួន២៥៤ Hosts ដែលមាន network address គឺ 192.168.0.0 និង default subnetmask: 255.255.255.0។

៨-៤-១- ការចែកចាយ Internet ដោយប្រើ Windows XP



ប្លង់នៃការបង្កើតសម្រាប់ចែកចាយ Internet





k- តម្រូវការសម្រាប់ភ្ជាប់ Internet

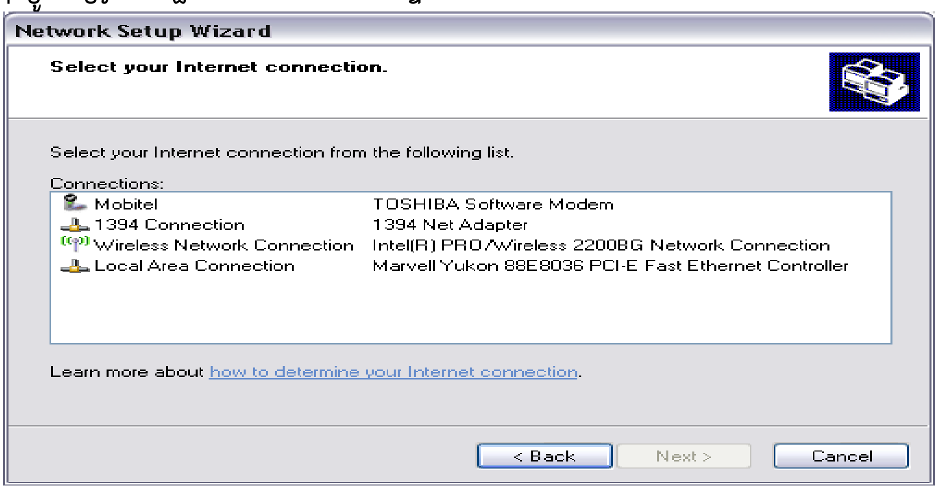
ត្រូវចុះឈ្មោះ Account ជាមួយក្រុមហ៊ុន ISP (Internet Service Provider) ដូចជា:

- Mobitel
- Camshin
- Camnet
- Online
- DSL modem and telephone line service
- Iphone

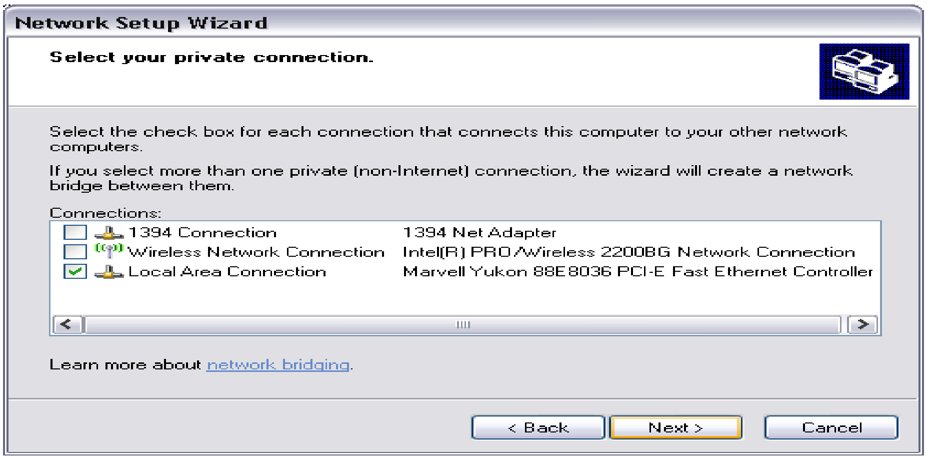
ត្រូវមាន Switch ឬ hub ដើម្បីភ្ជាប់មកកាន់ LAN network

ខ-បង្កើតការតភ្ជាប់

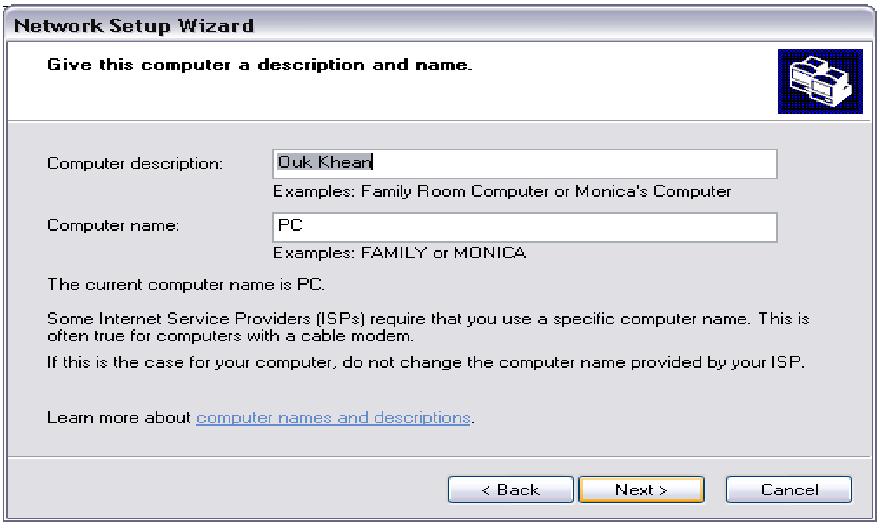
- កុំព្យូទ័រ ត្រូវបានភ្ជាប់ Internet ដោយផ្ទាល់



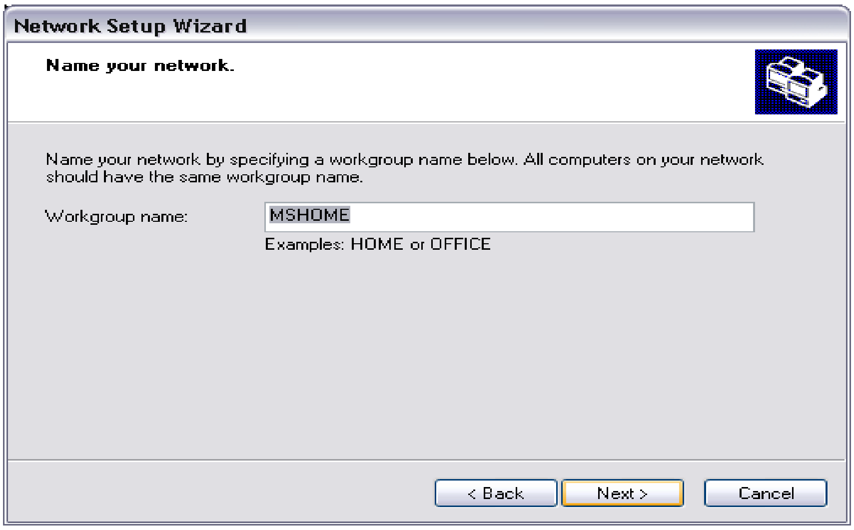
- ជ្រើសរើសយក Network Interface card



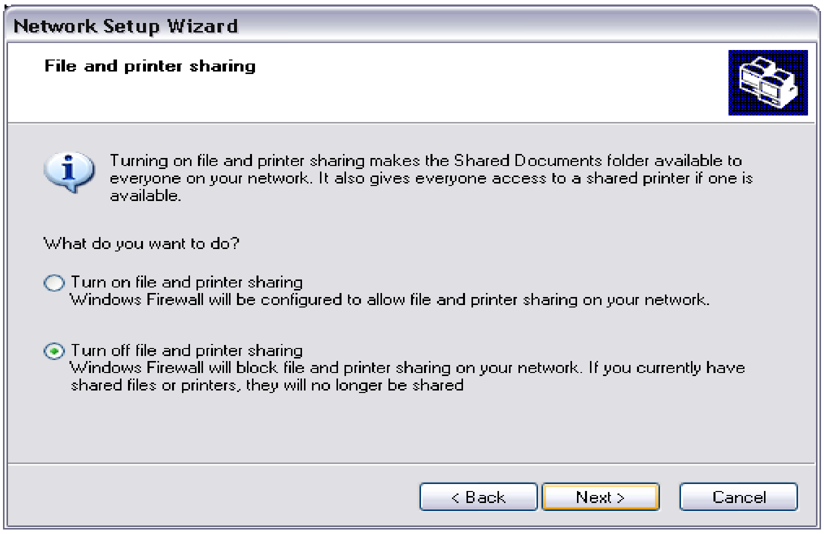
- ត្រូវបំពេញឈ្មោះនិងការពិពណ៌នា



- ត្រូវបំពេញឈ្មោះរបស់ Workgroup

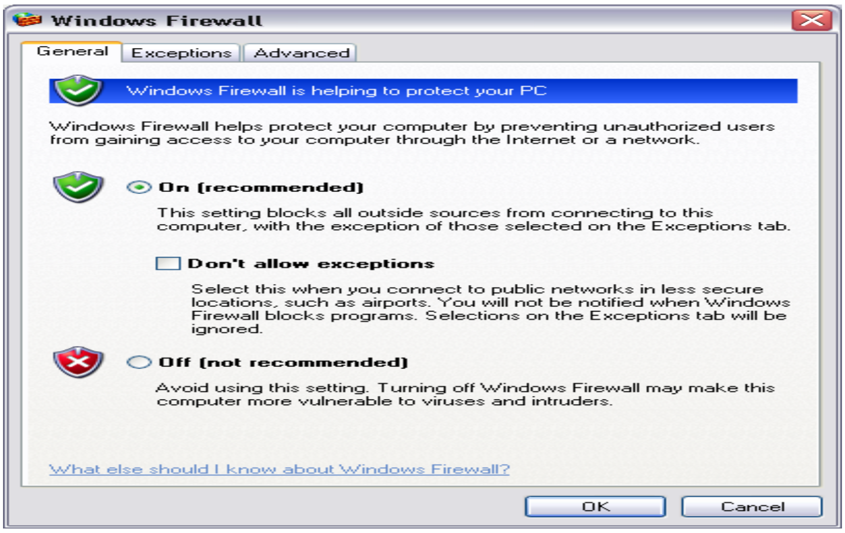


- យើងត្រូវជ្រើសរើសយក file and printer Sharing ឬបិទ file and printer Sharing

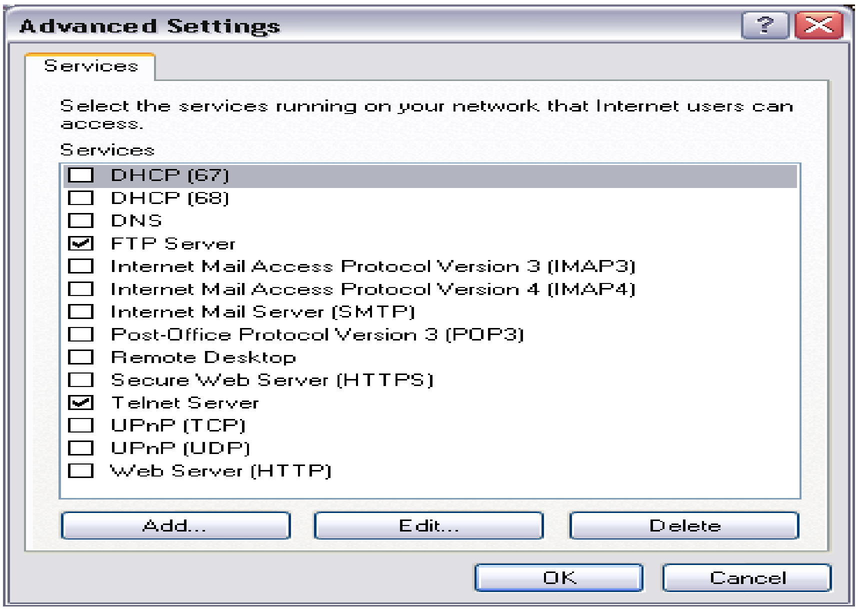


- តើយើងត្រូវ Setup Network តាមវិធីសាស្ត្រមួយណា ?

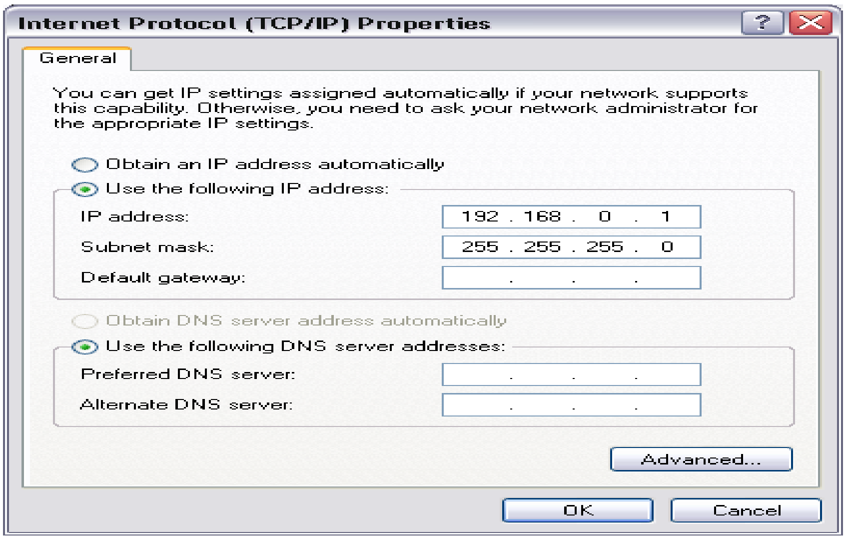
- តើយើងត្រូវបើកឬបិទ Firewall



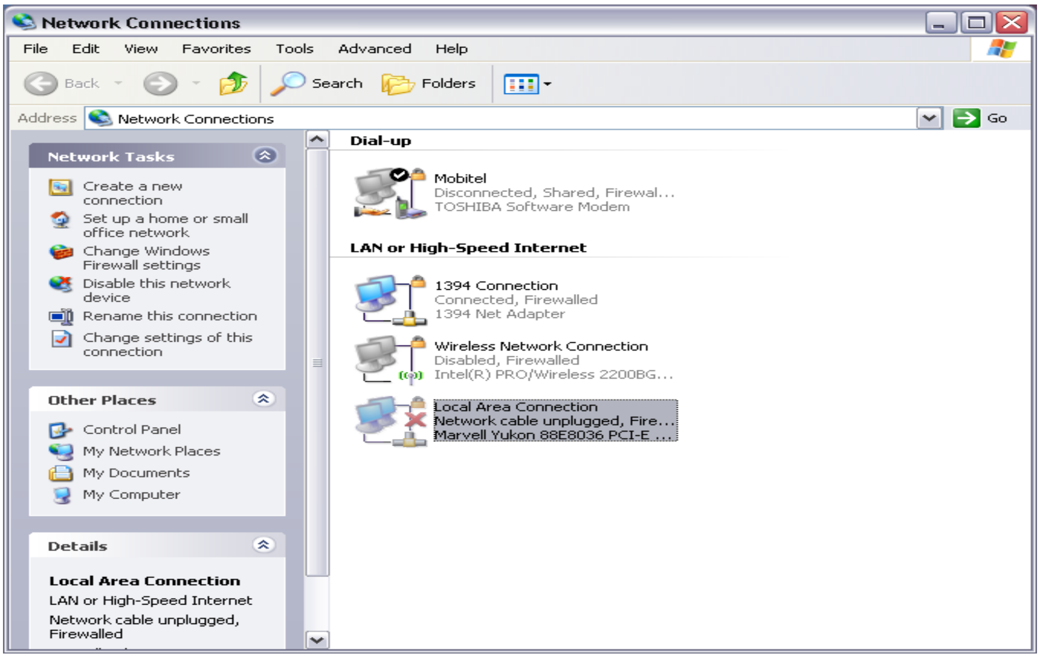
- តើសេវាណាខ្លះដែលយើងត្រូវអនុញ្ញាតឱ្យ Internet Users ប្រើប្រាស់បាន ?



- ក្រោយពីយើង Enable ICS រួចវាកំណត់ IP address ឱ្យកុំព្យូទ័រដែលភ្ជាប់ Internet ជាស្វ័យប្រវត្ត

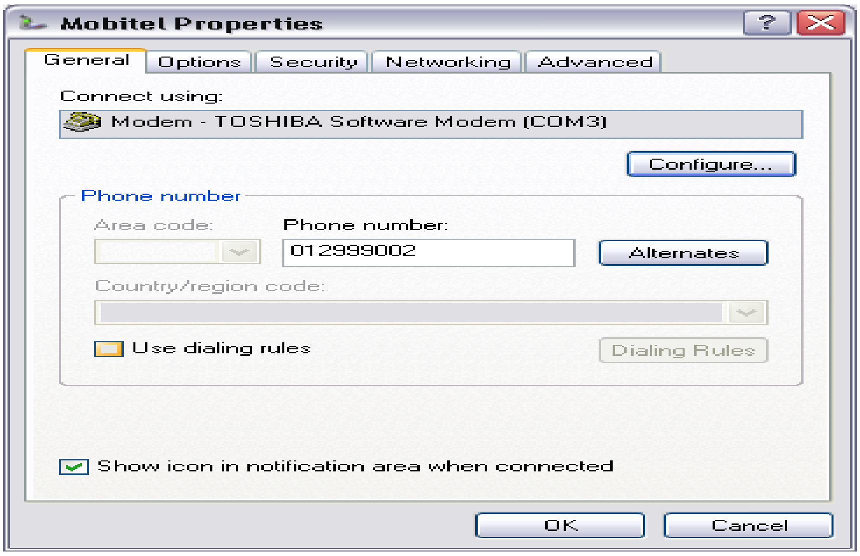


- នេះវាបង្ហាញអំពី Dial-up connection ដែលយើងបានបង្កើត

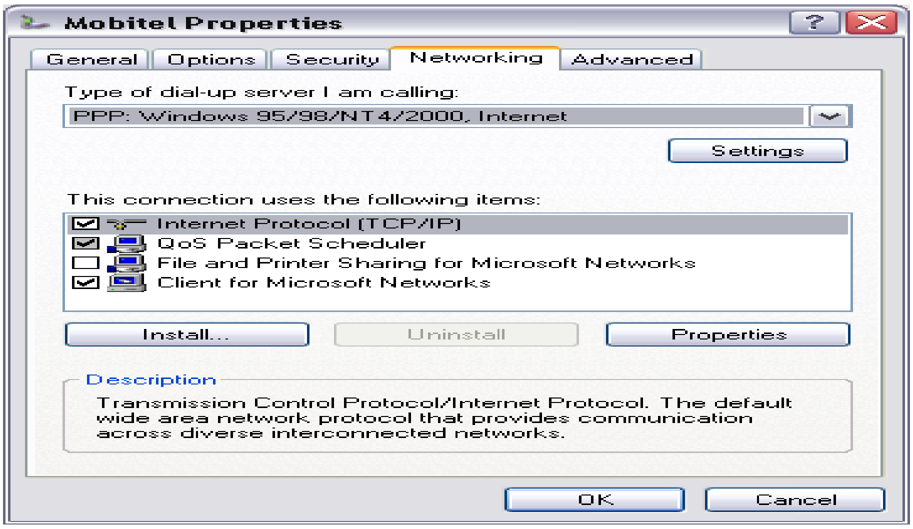


Properties of dial-up connection

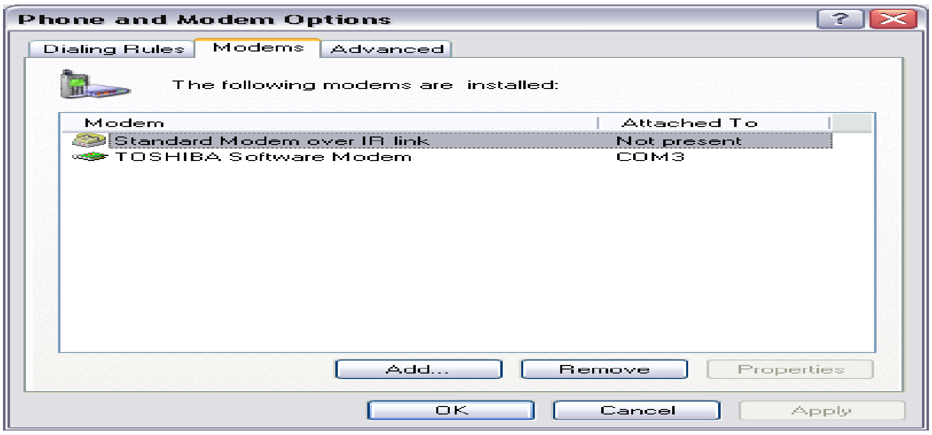
លេខទូរស័ព្ទដែលគេប្រើសម្រាប់ Dial-UP



- មើល Prototcol សម្រាប់ WAN (Dial-up)

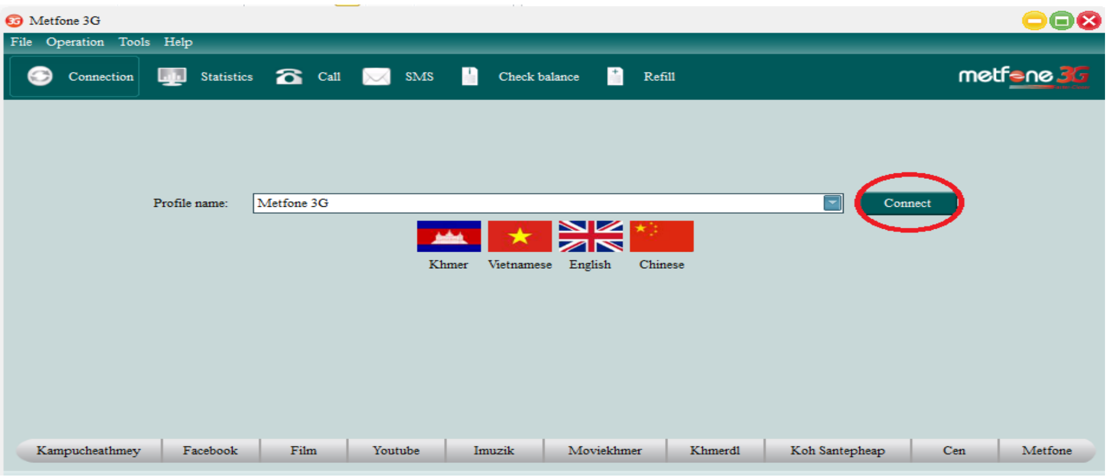


- មើល Hardware របស់ Modem



៨-៤-២- ការចែកចាយ Internet ជាមួយ Windows 7

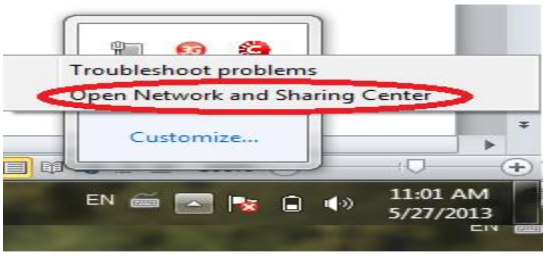
ដោយសព្វថ្ងៃមានបច្ចេកវិទ្យាទំនើបគឺគេប្រើប្រព័ន្ធទូរសព្ទ 2G ឬ 3G។ ដូច្នេះបើអ្នកមាន Wireless modem អ្នកគ្រាន់តែដោតវាចូលក្នុងប្រព័ន្ធកុំព្យូទ័រហើយក្រោយពីវាបានរកឃើញ Modem រួចហើយអ្នកគ្រាន់តែចុចលើ connect ដើម្បីភ្ជាប់វា។



រូបភាព១-ការភ្ជាប់ Internet ដោយប្រើ Wireless modem

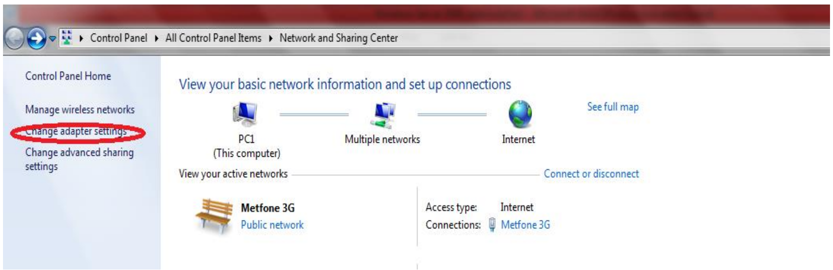
ដោយចុចលើ Icon នៃ Network ផ្នែកខាងក្រោមខាងស្តាំនៃ status bar របស់ Windows ហើយ

១-ជ្រើសរើសយក Open Network and Sharing Center



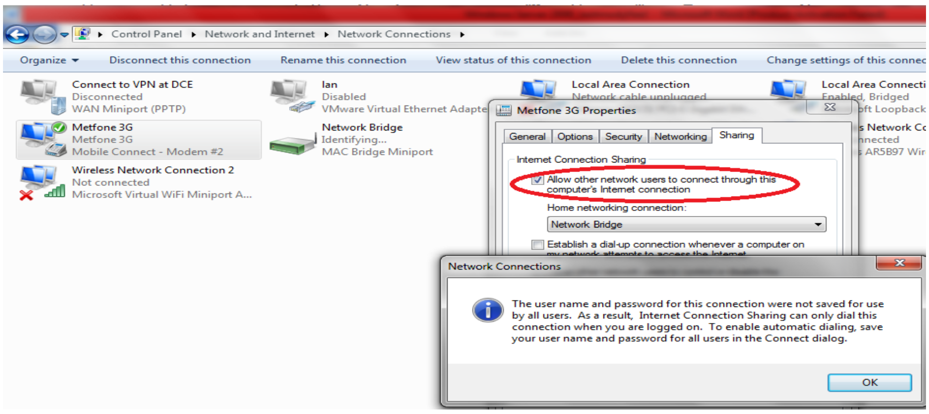
រូបភាព២-Network Icon សម្រាប់ចូលទៅ Share Internet

២-ចុចលើ Change adapter settings



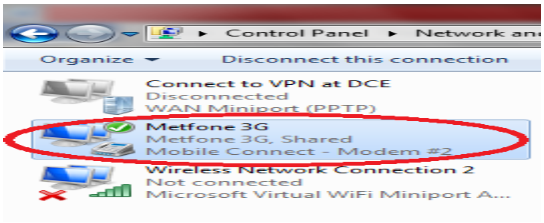
រូបភាព៣-ការបង្ហាញពី Adapter setting ក្នុង Control Panel

៣-ចុចលើ Metfone 3G ដោយប្រើ button Mouse ខាងស្តាំ=>Properties



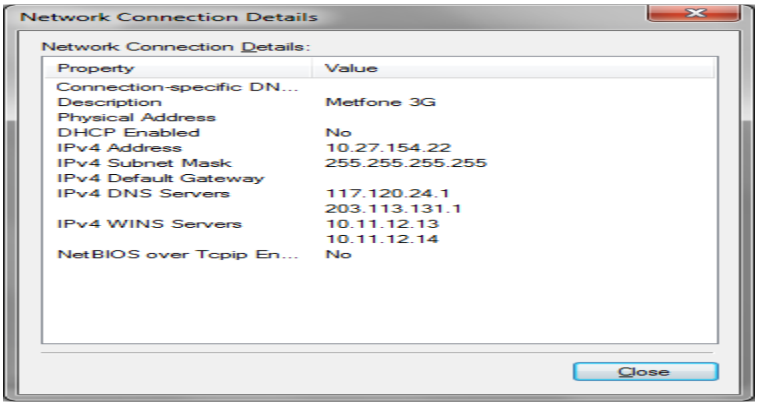
រូបភាពទី៤-ការជ្រើសរើសយក Internet Connection Sharing

៤-ចុចលើ OK



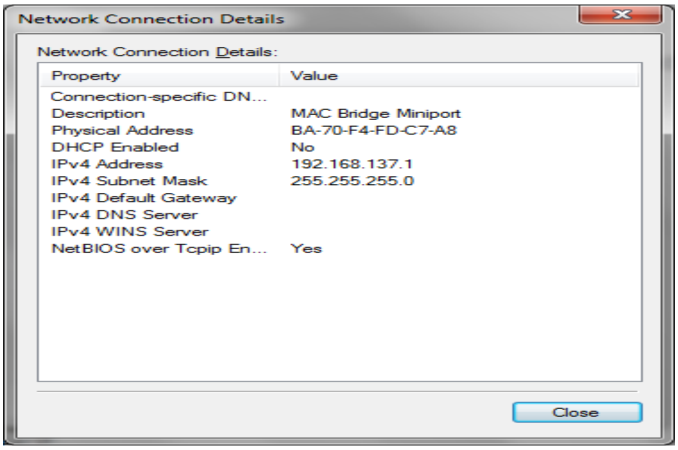
រូបភាពទី៥-Metfone បាន Share Internet ដោយប្រើ ICS

៥-ចុចលើ Metfone =>Status ដើម្បីមើលការ Assign IP address ពី ISP



រូបភាពទី៦-លក្ខណៈរបស់ Metfone ដែលកំណត់ដោយ ISP

៦-ចុចលើ Network Bridge =>Status ដើម្បីមើលការ Assign IP address ពី ICS



រូបភាពទី៨-លក្ខណៈរបស់ Network Bridge ដោយកំណត់ដោយ ICS ក្នុង Windows 7

សំណួរត្រួតពិនិត្យ

១- តើ ICS គេប្រើសម្រាប់ធ្វើអ្វី?

២- តើ ICS មានក្នុង Windows OS ណាខ្លះ?

៣- ចំពោះ Windows xp តើវាប្រើ IP address មានលេខអ្វី?

៤- ចំពោះ Windows 7 តើវាប្រើ IP address មានលេខអ្វី?

ជំពូកទី៩

ការចាប់ផ្ដើមជាមួយ Windows Server 2008

នៅពេលដែល Microsoft បានចេញដាក់ឱ្យប្រើប្រាស់ Windows server 2008។ ក្រុមហ៊ុនបានចំណាយពេលវេលាដើម្បីប្រមូលព័ត៌មានពីអ្នកប្រើប្រាស់ហើយបានបញ្ចូលព័ត៌មានទាំងនោះទៅក្នុងលក្ខណៈពិសេសរបស់ Windows Server 2008 ។

៩-១- តម្រូវការ Hardware និង Software

ដើម្បីដំឡើងWindows Server 2008 ត្រូវការតម្រូវការដូចខាងក្រោម៖
ដើម្បីឱ្យការដំឡើងWindows server 2008 ឱ្យបានល្អ យើងត្រូវបំពេញទៅតាមតម្រូវការអប្បបរមារបស់ Server និងតម្រូវការ Hardware ។

Proccessor	Minimum:1GHz Recommended:2GHz Optimal:3GHz or Faster *Intel Itanium 2 proccessors required for Windows Server 2008 for Itanium-based system.
Memory	Minimum: 512MB RAM Recommended: 1GB RAM Optimal: 2GB RAM (Full installation) or 1GB RAM (Server Core installation) or more Maximum (32-bit): 4GB (Standard) or 64GB (Enterprise and Datacenter) Maximum (64-bit): 32GB (Standard) or 2TB (Enterprise, Datacenter, and Itanium-based systems)
Disk Space	Minimum: 8GB Recommended: 40GB (Full installation) or 10GB (Server Core installation) Optimal: 80GB (Full installation) or 40GB (Server Core installation) or more
Drive	DVD-ROM drive
Display	SVGA (800 × 600) or higher resolution Keyboard Microsoft mouse or compatible pointing device

៩-២- Installation and Configuration

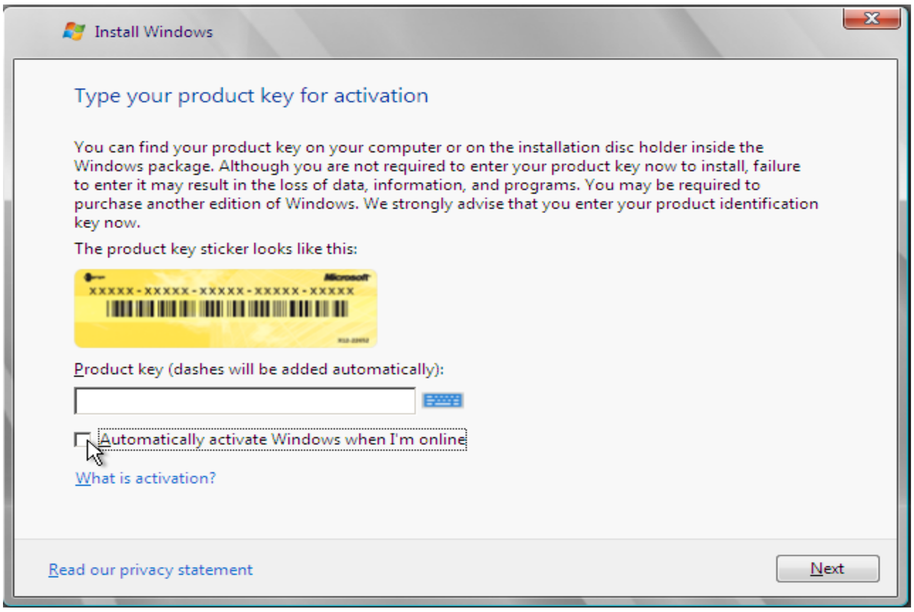
គេអាចដំឡើង Windows server 2008 តាមពីររបៀបគឺ Full Installation server និង Server Core ។ Server Core គឺជាការដំឡើងServer ដែលគ្មាន GUI និង Service ដែលមិនត្រូវការចាំបាច់។

លំហាត់អនុវត្ត: សកម្មភាពនៃការដំឡើងWindows Server 2008

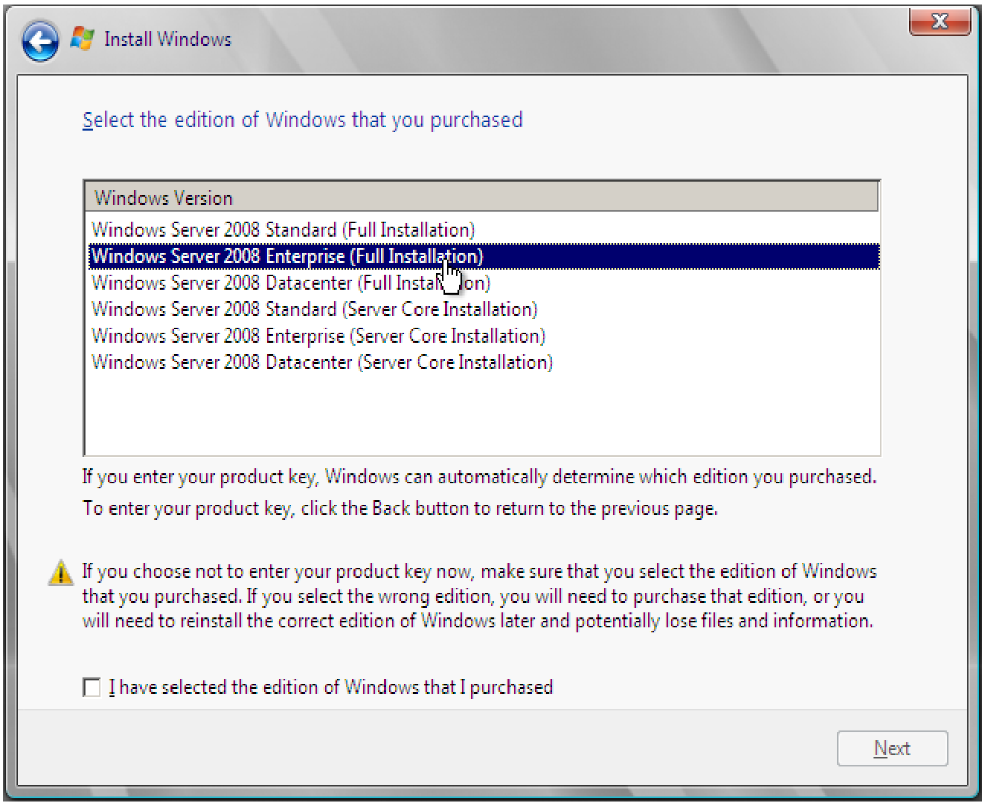
១-Boot កុំព្យូទ័រ ដោយប្រើ Windows Server 2008 Installation media ។ ជ្រើសរើសយកភាសាសម្រាប់ Install ម៉ោងនិងរូបិយបណ្ណ័ គម្រោង Keybaord ហើយបន្ទាប់មកចុចលើ Next

២-ចុចលើ Install Now ដើម្បីចាប់ផ្តើមដំណើរការ Install ។ ដូចបានបង្ហាញក្នុងរូបភាព១-២ អ្នកអាច Access system recovery tools ដោយចុចលើ Repair Your កុំព្យូទ័រ option នៅខាងក្រោមនៃអេក្រង់

៣-វាយបញ្ចូល Key សម្រាប់ Install។ បើអ្នកមិនចង់ឱ្យវា Activate Windows ភ្លាមនោះទេ នោះអ្នកមិនចាំបាច់ចុចលើប្រអប់ Automatocally Activate Windows ។



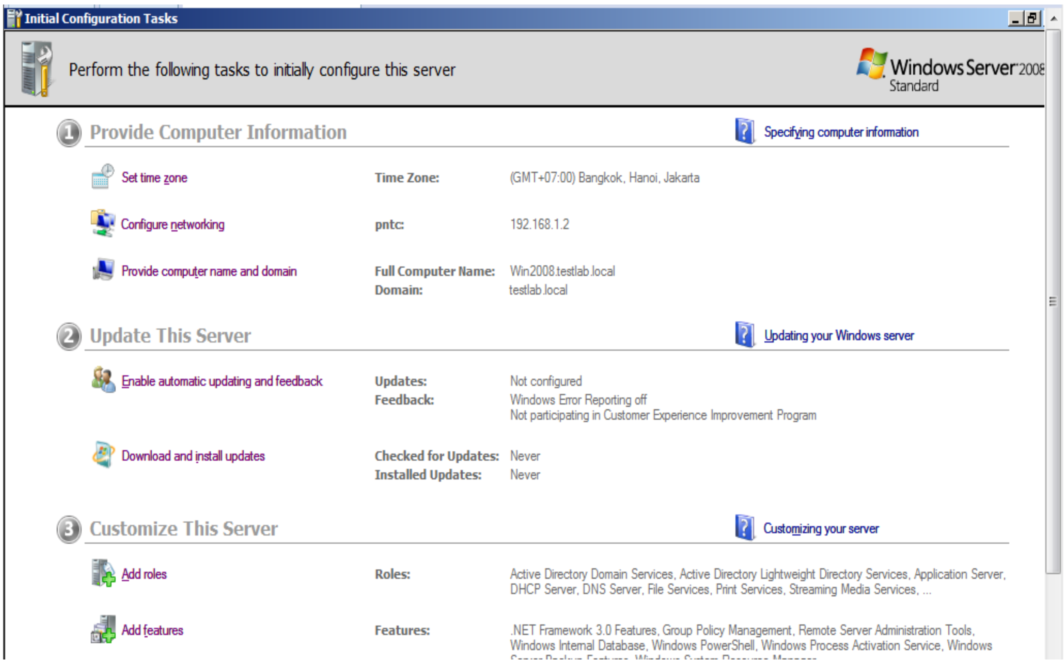
៤-តើអ្នកត្រូវជ្រើសរើសយក Windows Server 2008 Enterprise (Full Installation) ឬ Windows Server 2008 (Core Installation)។ បើអ្នកជ្រើសរើសយក Windows Server 2008 Enterprise (Full Installation) វានិងបង្ហាញដូចខាងក្រោម



៥-បន្ទាប់មកអនុវត្តតាមការណែនាំរបស់អេក្រង់

ការងារដែលត្រូវធ្វើក្រោយពីការដំឡើងនិងចាប់ផ្តើមជាមួយ Initial Configuration Tasks

ក្រោយពីបាន Install រួចហើយ វានិងបង្ហាញឱ្យយើងឃើញនូវ Initial Configuration Task ដូចក្នុងរូបភាព ១-១។



Task	ការពិពណ៌នា
Set the Administrator Password	អនុញ្ញាតឱ្យអ្នកអាចប្តូរ Password សម្រាប់ Administrator Account និងប្តូរ Account
Set Time Zone	កំណត់ Time zone ឱ្យ Server
Configure Networking	បើក Network Control Panel Applet ដូច្នេះអ្នកអាច Configure network interfacesបាន។
Provide កុំព្យូទ័រ Name and Domain	អនុញ្ញាតឱ្យអ្នកប្តូរឈ្មោះរបស់កុំព្យូទ័រនិងចូលរួមក្នុង Domain
Updating and Feedback	Windows Update,Windows Error Reporting and the Customer Experience Improvement Program (CEIP)។
Download and Install Updates	អនុញ្ញាតឱ្យអ្នកអាច Download និង Install Updates។
Add Roles	អនុញ្ញាតឱ្យអ្នកបន្ថែមតួនាទីឱ្យ Server ដូចជា DHCP, DNS, IIS ។ល។
Add Features	Interface ថ្មីនេះជំនួសឱ្យ Add/Remove Windows Components ពី Add/Remove Programs Control Panel applet ដែលមាននៅក្នុង Version ចាស់នៃ Windows
Enable Remote Desktop	អនុញ្ញាតឱ្យអ្នកអាច Configure remote desktop
Configure Windows Firewall	សម្រាប់បើកឬបិទ Firewall

៩-៣- Boot configuration Data

គ្រប់ Windows Server ទាំងអស់ពឹងផ្អែកលើ Windows NT ដែលប្រើ NT Loader (NTLDR) និង boot.ini ដើម្បីគ្រប់គ្រង់លើដំណើរការ boot និងគ្រប់គ្រង់លើ multi-boot ជាមួយ Windows ។ ដំណើរការ boot ទាំងអស់ត្រូវបានបង្កើតឡើងវិញដោយបង្កើត Boot Configuration Data(BCD) ។ BCD ត្រូវបានប្រើជំនួសឱ្យ NTLDR ទាំងស្រុង។ វាមានបានរក្សា boot process ក្នុង BCDEdit.exe ដោយជំនួសឱ្យ boot.ini ហើយប្រើ Windows Management Interface (WMI) ។

BCD Store

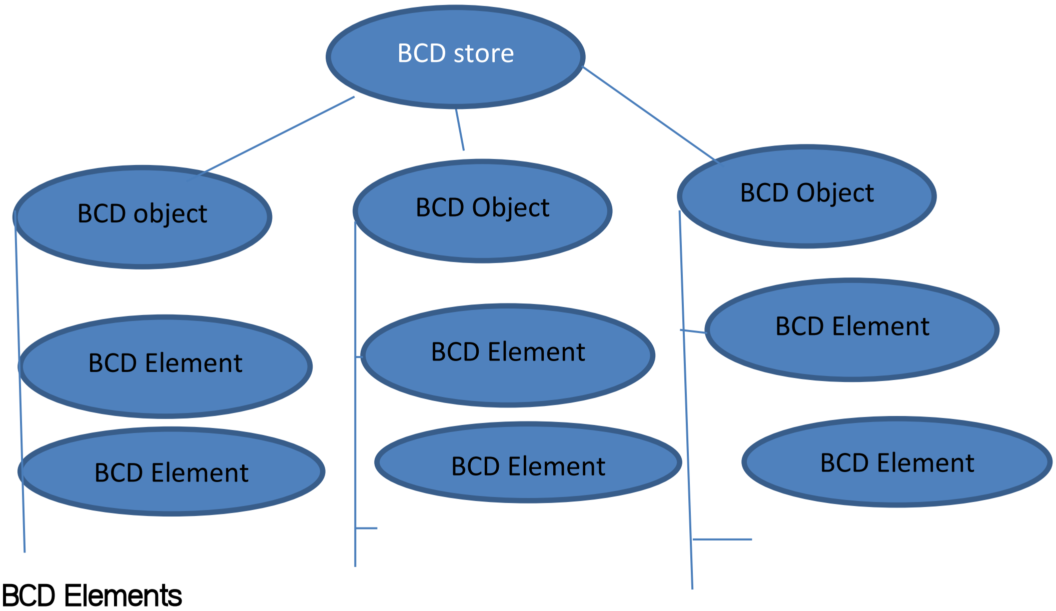
BCD store គឺជា Physical binary file ដែលបានរក្សាទុកនៅ Active Partition ឬEFI system partition (ESP) ។ វារក្សាទុករាល់ព័ត៌មានទាំងអស់ដែលពិពណ៌នាអំពី boot up សម្រាប់ Windows ។

សមាសធាតុផ្សំ	ការពិព៌ណនា
BCD Store	គឺជាកម្រិតខ្ពស់បំផុតនៃការរៀបចំតាមលំដាប់ថ្នាក់។ វាគឺជា root នៃសមាសធាតុក្នុង Windows ។
BCD Object	វាគឺជា Container សម្រាប់គ្រប់សមាសធាតុរបស់ BCD ។
BCD Element	វាគឺជា properties និង parameters របស់ BCD object ។

System នីមួយៗមាន BCD Store ច្រើនជាងមួយ។ ទោះបីជាយ៉ាងណាក៏ដោយវាមានតែមួយគត់ដែលអាច Active បាន។

ចំពោះ BIOS-based systems File នេះស្ថិតនៅក្នុង \BOOT folder របស់ Active Partition ចំណែកឯ EFI-based systems វិញ វាស្ថិតនៅក្នុង \Windows\boot\EFI folder ។

ការរៀបសមាសធាតុនៃ BCD តាមលំដាប់ថ្នាក់



BCD Elements

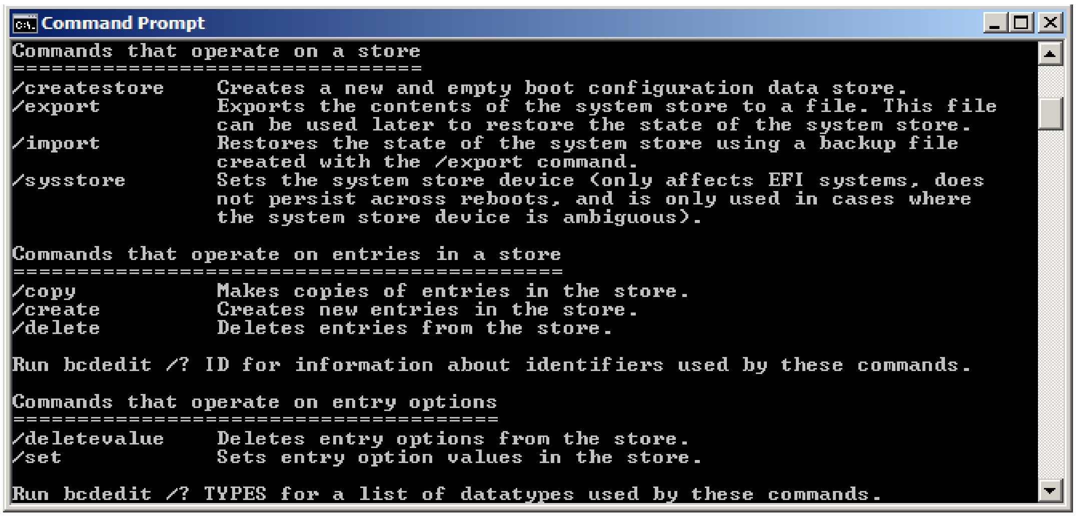
មិនដូចគ្នាទៅនិង boot.ini ចាស់នោះទេ BCD elements មានប្រភេទ Data ដែលទាក់ទងទៅនិងតម្លៃនៃ Data ។ ឧទាហរណ៍ Element អាចជា String , Object , Integer ឬ Boolean ។

BCD Modification Methods

យើងអាចអនុវត្ត BCD តាមបួនរបៀបគឺ

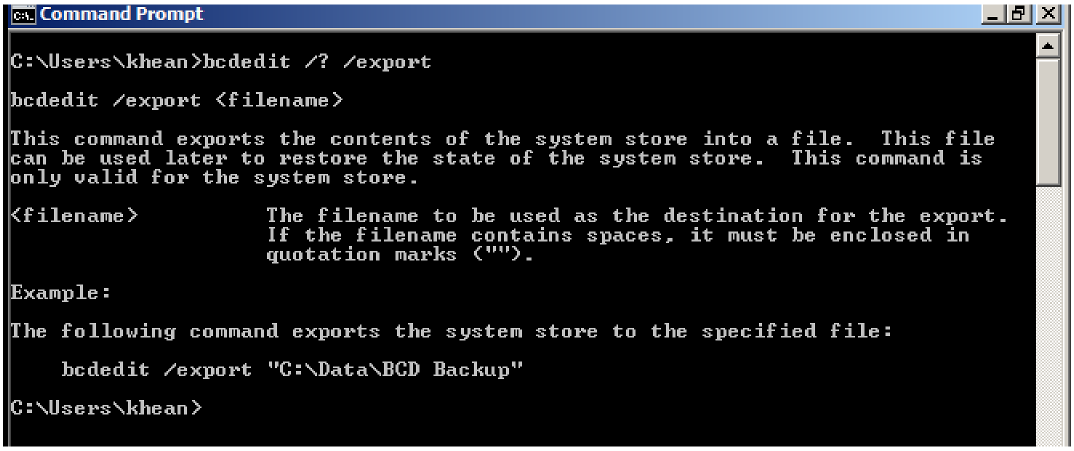
ការប្រើ BCDEdit

បើសិនជាអ្នកចង់ដឹងពីរបៀបប្រើប្រាស់វាឱ្យបានច្បាស់លាស់ ត្រូវប្រើបញ្ជាដូចខាងក្រោម:



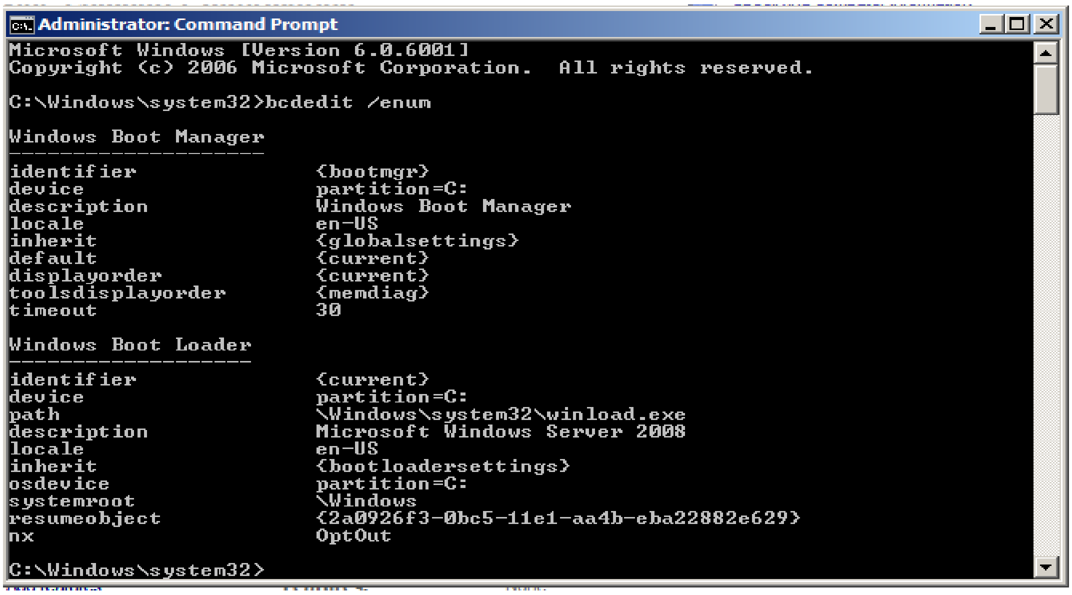
```
Command Prompt
Commands that operate on a store
================================
/createstore     Creates a new and empty boot configuration data store.
/export          Exports the contents of the system store to a file. This file
                 can be used later to restore the state of the system store.
/import          Restores the state of the system store using a backup file
                 created with the /export command.
/sysstore        Sets the system store device (only affects EFI systems, does
                 not persist across reboots, and is only used in cases where
                 the system store device is ambiguous).

Commands that operate on entries in a store
===========================================
/copy            Makes copies of entries in the store.
/create          Creates new entries in the store.
/delete          Deletes entries from the store.

Run bcdedit /? ID for information about identifiers used by these commands.

Commands that operate on entry options
======================================
/deletevalue     Deletes entry options from the store.
/set             Sets entry option values in the store.

Run bcdedit /? TYPES for a list of datatypes used by these commands.
```

បើអ្នកចង់រៀនអំពី export switch ត្រូវប្រើបញ្ជាដូចខាងក្រោម



```
Command Prompt

C:\Users\khean>bcdedit /? /export

bcdedit /export <filename>

This command exports the contents of the system store into a file.  This file
can be used later to restore the state of the system store.  This command is
only valid for the system store.

<filename>          The filename to be used as the destination for the export.
                    If the filename contains spaces, it must be enclosed in
                    quotation marks ("").

Example:

The following command exports the system store to the specified file:

    bcdedit /export "C:\Data\BCD Backup"

C:\Users\khean>
```

ដើម្បីទាញយក Current Configuration ត្រូវប្រើ

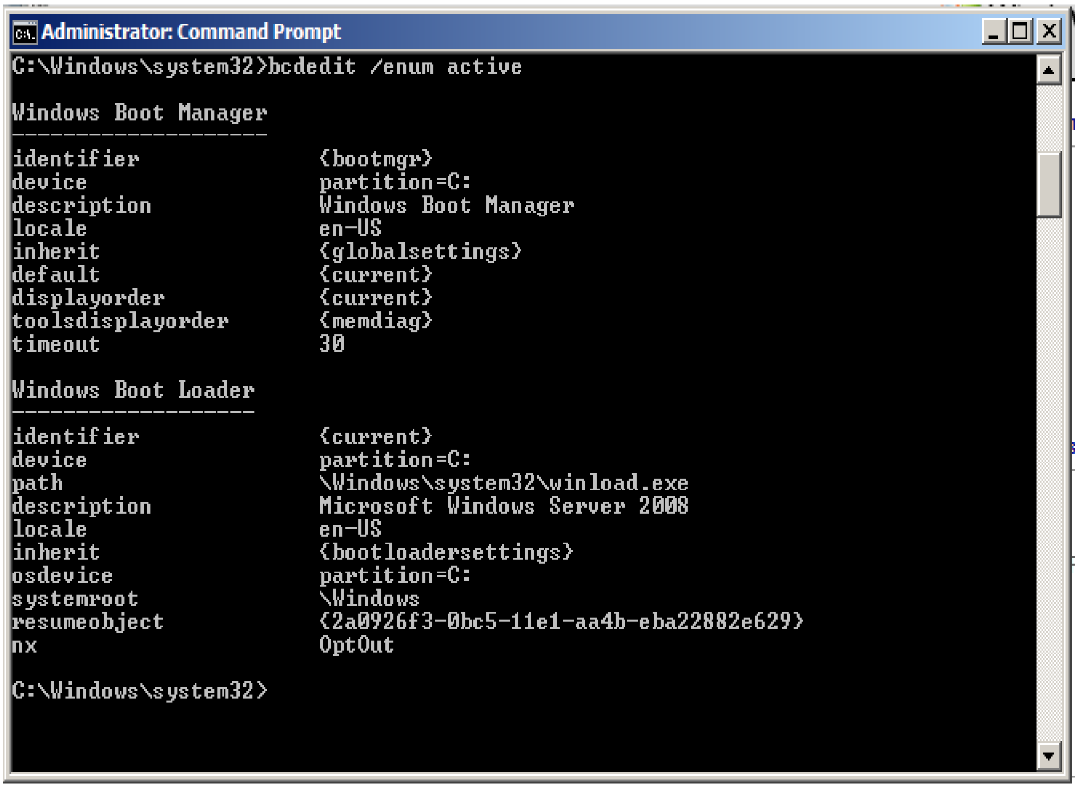


```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>bcdedit /enum

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
default                 {current}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Microsoft Windows Server 2008
locale                  en-US
inherit                 {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject            {2a0926f3-0bc5-11e1-aa4b-eba22882e629}
nx                      OptOut

C:\Windows\system32>
```

គេអាចអនុវត្តតាម៤របៀបដូចខាងក្រោម

Method	ការពិពណ៌នា
System Control Panel applet	អនុញ្ញាតឱ្យអ្នកអាចកំណត់ Default OS កំណត់ពេលវេលាឱ្យបង្ហាញតារាងនៃ OS និងពេលវេលាដើម្បី Recover .
MSConfig.exe	ជា GUI ដែលអនុញ្ញាតឱ្យគ្រប់គ្រង់លើ Startup options ។
BCDEdit.exe	គឺជា Command-line tool ដែលមានឥទ្ធិពលបំផុតសម្រាប់អនុវត្តលើ BCD
WMI	សម្រាប់ប្រើជាមួយ Script ហើយត្រូវការច្រើនជាង BCDEdit.exe

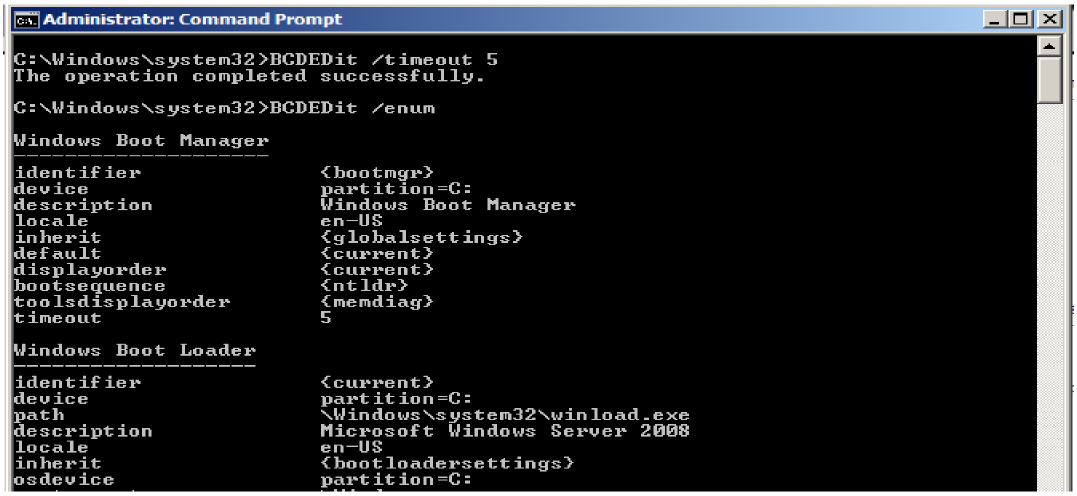
ការប្រើ BCDEdit.exe /enum ACTIVE



```
Administrator: Command Prompt
C:\Windows\system32>bcdedit /enum active

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
default                 {current}
displayorder            {current}
toolsdisplayorder       {memdiag}
timeout                 30

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Microsoft Windows Server 2008
locale                  en-US
inherit                 {bootloadersettings}
osdevice                partition=C:
systemroot              \Windows
resumeobject            {2a0926f3-0bc5-11e1-aa4b-eba22882e629}
nx                      OptOut

C:\Windows\system32>
```

ការកែ Boot sequence

ការកំណត់ Boot Manager Timeout ជាមួយបញ្ជា BCDEdit /timeout 5



```
Administrator: Command Prompt

C:\Windows\system32>BCDEDit /timeout 5
The operation completed successfully.

C:\Windows\system32>BCDEDit /enum

Windows Boot Manager
--------------------
identifier              {bootmgr}
device                  partition=C:
description             Windows Boot Manager
locale                  en-US
inherit                 {globalsettings}
default                 {current}
displayorder            {current}
bootsequence            {ntldr}
toolsdisplayorder       {memdiag}
timeout                 5

Windows Boot Loader
-------------------
identifier              {current}
device                  partition=C:
path                    \Windows\system32\winload.exe
description             Microsoft Windows Server 2008
locale                  en-US
inherit                 {bootloadersettings}
osdevice                partition=C:
```

ការ Backup និង ស្តារ BCD

នេះគឺជាការ Backup BCD ។ តាមធម្មតា វាបង្កើត files ចំនួនពីរដាច់ដោយឡែកពីគ្នាក្រោយពេលវាដំណើរការរួច។ មួយគឺជា File សម្រាប់ការ Backup data ហើយមួយទៀតគឺ Backup log file ។

```
Administrator: Command Prompt
09/19/2006  04:43 AM                24 autoexec.bat
09/19/2006  04:43 AM                10 config.sys
01/19/2008  04:40 PM    <DIR>          PerfLogs
11/10/2011  10:07 AM    <DIR>          Program Files
11/10/2011  10:05 AM    <DIR>          Users
11/10/2011  10:26 AM    <DIR>          Windows
               2 File(s)             34 bytes
               4 Dir(s)  35,748,761,600 bytes free

C:\>mkdir c:\backup

C:\>dir
 Volume in drive C has no label.
 Volume Serial Number is B4F0-321B

 Directory of C:\

09/19/2006  04:43 AM                24 autoexec.bat
11/10/2011  02:54 PM    <DIR>          backup
09/19/2006  04:43 AM                10 config.sys
01/19/2008  04:40 PM    <DIR>          PerfLogs
11/10/2011  10:07 AM    <DIR>          Program Files
11/10/2011  10:05 AM    <DIR>          Users
11/10/2011  10:26 AM    <DIR>          Windows
               2 File(s)             34 bytes
               5 Dir(s)  35,748,761,600 bytes free

C:\>bcdedit /export "C:\backup\BCD-backup"
The operation completed successfully.

C:\>_
```

ការស្តារ BCD ជាមួយបញ្ជា bcdedit /import "c:\backup\BCD-backup"

```
C:\>bcdedit /import "C:\backup\BCD-backup"
The operation completed successfully.

C:\>
```

ចំណាំ: បើអ្នកស្តារ data មិនបានត្រឹមត្រូវ System របស់អ្នកនឹងក្លាយជា nonbootable ក្រោយពី reboot System ឡើងវិញ

សំណួរត្រួតពិនិត្យ

១-តើ File សម្រាប់ឱ្យ Windows Server 2008 អាចដំណើរការបានមានអ្វីខ្លះ ?

២-តើ BCD configuration file ត្រូវបានគេប្រើសម្រាប់ធ្វើអ្វី ?

៣-ចូរកែ Default Timeout របស់ Windows Server 2008 មកត្រឹម ៥វិនាទី

៤-តើគេកំណត់ Timeout របស់ Windows server 2008 ឱ្យស្មើសូន្យក្នុងករណីណា ?

ជំពូកទី១០

Server Core

១០-១- តួនាទី និងមុខងាររបស់ Server Core

Server Core អាចឱ្យយើងដំឡើងនូវ Tools មួយចំនួនទៀតដូចជាៈ

- Active Directory Domain Services (AD DS)
- Active Directory Lightweight Directory Services (AD LDS)
- File Server
- DHCP Server
- DNS Server
- Printer Server
- Streaming Media Services

តើនឹងមានអ្វីកើតឡើងចំពោះ **Server Core នៅពេល Power Supply Down ?**

ក្នុងការដែលដំឡើង Server Core គឺទទួលបាននូវគុណប្រយោជន៍ជាច្រើន។ វាកាត់បន្ថយនូវចំនួន Services ដែលត្រូវការផ្តល់ទៅឱ្យ Operating System ដូច្នេះវាកាត់បន្ថយនូវការគ្រប់គ្រងចំពោះ តម្រូវការតំហែទាំ Server ទាំងនេះ។ ការដំឡើង **Server Core** គឺមិនបានផ្តល់ឱ្យនូវ User Interface សម្រាប់ដំណើរការប្រតិបត្តិការសម្រាប់ដោះស្រាយបញ្ហានោះទេ អ្វីដែលមាននោះគឺ Command-Line។ មធ្យោបាយតែមួយគត់ក្នុងការគ្រប់គ្រងទៅលើ **Server Core** នោះគឺ Command-Line និង Scripts មួយចំនួន ឬក៏ត Microsoft Management Console (MMC) snap-ins ឬតាមរយៈ tool ដទៃទៀតដែលដែលជួយផ្តល់ការផ្គត់ផ្គង់ដល់ remote administration និង Terminal Services។

១០-២- របៀបដំឡើង Server Core

មុនពេលដំឡើង Windows Server 2008 Enterprise (Server Core) អ្នកត្រូវតែពិនិត្យមើល hard ware ដែលអ្នកមានហើយតម្រូវការអប្បបរមារបស់ប្រព័ន្ធ System សម្រាប់ Server Core រួមមាន hardware សំខាន់ៗដូចខាងក្រោមៈ

CD/DVD Windows Server 2008 Installation Media

and a valid product key

- Standard
- Enterprise
- Data Center

Disk Space :

- **1GB** of disk space for the actual Server Core installation and
- **2GB** of disk space for regular server operations.

RAM :

- Maximum : 4GHz
- Recommend : 256 MB

CPU : (Pentium-Compatible processor)

- Maximum : 1GHz
- Recommend : 133 MHz
- Optional : 3 GHz or Fast

DVD-ROM Drive : *not required for network installation*.

Display :

- Resolution : 640 x 480
- Recommend : 1024 x 768

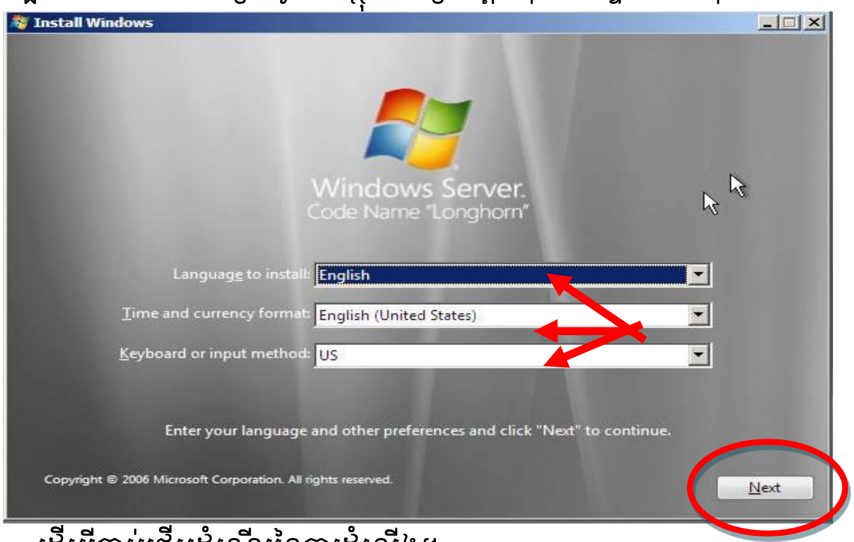
- **បញ្ជាក់:**
  - មិនអាចធ្វើការ upgrade ពី Windows Server 2008 ទៅ Server Core នឹងមិនអាចដំឡើងពី Server Core ទៅ Windows Server 2008
  - Server Core ត្រូវតែដំឡើងដាច់ដោយឡែកពីវា
  - គួរមាន Internet access ដើម្បី activate ក្រោយពីការដំឡើងរួចរាល់
  - **Roles** គឺមានតួនាទីបន្ថែមនូវ Services ដែលធ្វើឱ្យ Windows Server 2008 មានតួនាទីកាន់តែច្រើនឡើងដែលតួនាទីទាំងនោះមានដូចជា DHCP Server និង DNS Server ជាដើម
  - **Features** : គឺត្រូវបានគេប្រើប្រាស់ធ្វើឱ្យតួនាទី (Roles) ទាំងនោះអាចដំណើរការបាន។

➔ សកម្មភាពក្នុងការដំឡើងរបស់ **Server Core**

ក្នុងការដំឡើង Server Core ក៏មិនមានអ្វីខុសគ្នាទៅនឹងការដំឡើងWindows Server 2008 Enterprise (Full Installation) នោះដែរ លើកលែងតែនៅជំហានចុងក្រោយ Installing Process គឺ មានការឃើតបន្តិចនៃការ Configuration Tasks Screen តែប៉ុណ្ណោះ ហើយអ្នកនឹងទទួលបាននូវ Command prompt មួយដែល Command prompt នេះសម្រាប់អ្នកប្រើប្រាស់នូវរាល់ការផ្លាស់ប្តូរនៃ Configuration ណាមួយ។ ករណីយើងបាន

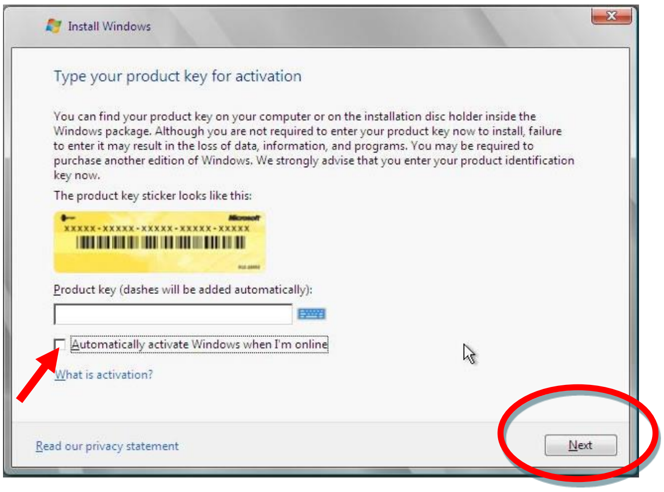
បិទ Command prompt នោះដោយចៃដន្យ ហើយយើងចង់បើកវិញ នោះយើងត្រូវចុចនូវបង្គំ key (Ctr+Alt+Del)-> Start Task Manager->File->New Task->cmd->ok។

១. ជាដំបូងចាប់ផ្តើមដំណើរការកុំព្យូទ័ររបស់អ្នកនិង boot ដោយប្រើ Window Server 2008 ដើម្បីធ្វើការដំឡើង។ ជ្រើសយកនូវការដំឡើងភាសា,ម៉ោង, ទម្រង់រូបិយវត្ថុនិងទម្រង់ក្តារចុច។ បន្ទាប់មក ចុច Next។

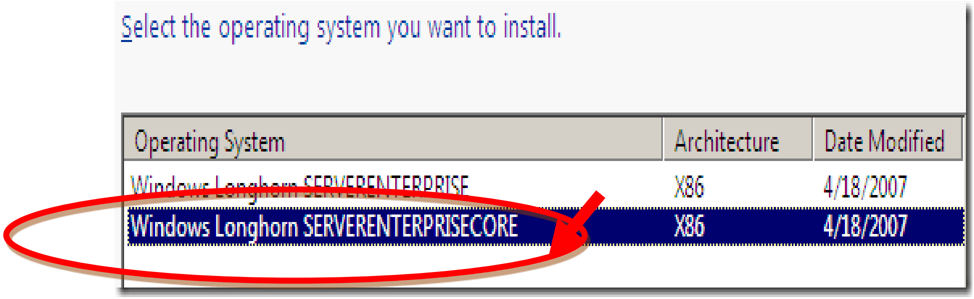


២. ចុច Install Now ដើម្បីចាប់ផ្តើមដំណើរនៃការដំឡើង។

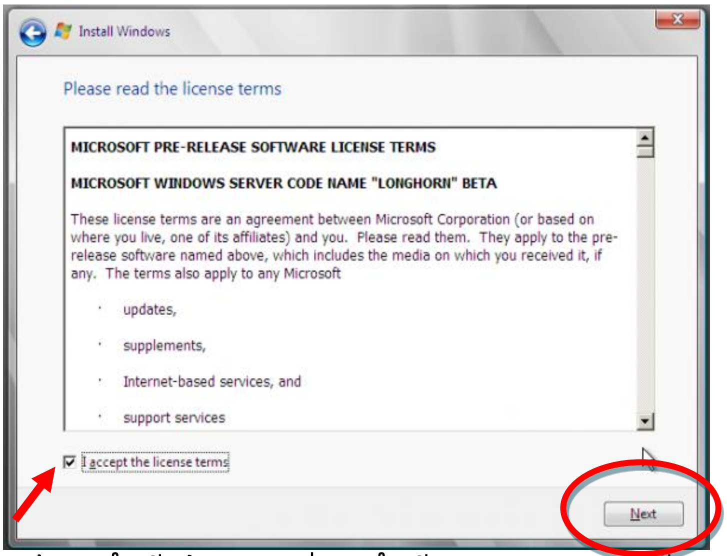
៣. វាយបញ្ចូលលេខកូដផលិតផលរបស់អ្នក រួចចុច Next។ ប្រសិនជាអ្នកមិនចង់ Windows របស់អ្នក activate នៅពេលដែលកុំព្យូទ័ររបស់អ្នក online អ្នកអាចដោះគូសប្រអប់ Auto matically Activate Windows When I'm Online។



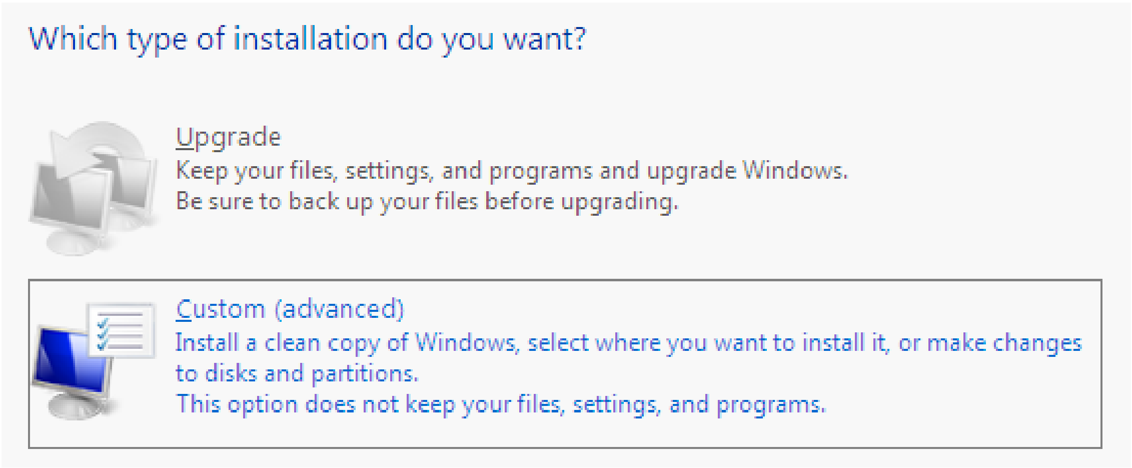
៤. អ្នកអាចជ្រើសរើសការដំឡើង Windows Server 2008 Enterprise (Full Installation) រឺក៏ Windows Server 2008 Enterprise (Server Core Installation)។ ជ្រើសរើសយក Windows Server 2008 Enterprise (Server Core Installation) ដើម្បីដំឡើង Server Core (ដូចរូបខាងក្រោម) បន្ទាប់មកចុច Next ។



៥. ប្រសិនជាអ្នកយល់ស្របទៅលើការឯកភាពសិទ្ធិនៃការប្រើប្រាស់គូសនៅក្នុងប្រអប់ I Accept the License Terms (ជាតម្រូវការក្នុងការប្រើប្រាស់ Windows) បន្ទាប់មកចុច Next ។

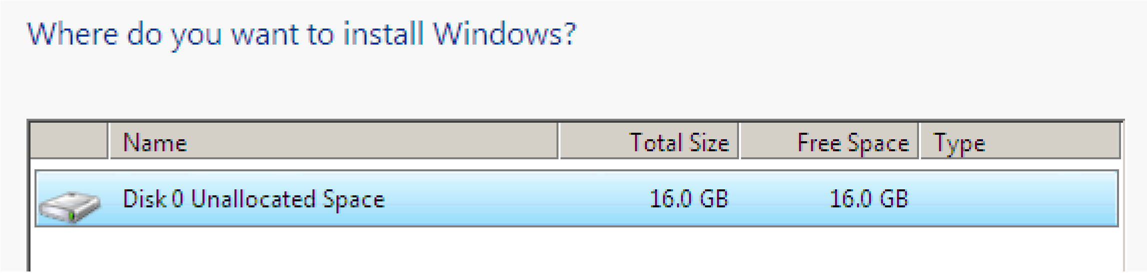


៦. ជ្រើសរើសយកប្រភេទនៃការដំឡើងដែលអ្នកចង់យកដំណើរការ។ នៅក្នុងករណីនេះអ្នកអាចជ្រើសរើសយកដំណើរការដំឡើងដោយសុវត្ថិភាពនិងអ្នកអាចជ្រើសរើសយកCustom (Advanced)

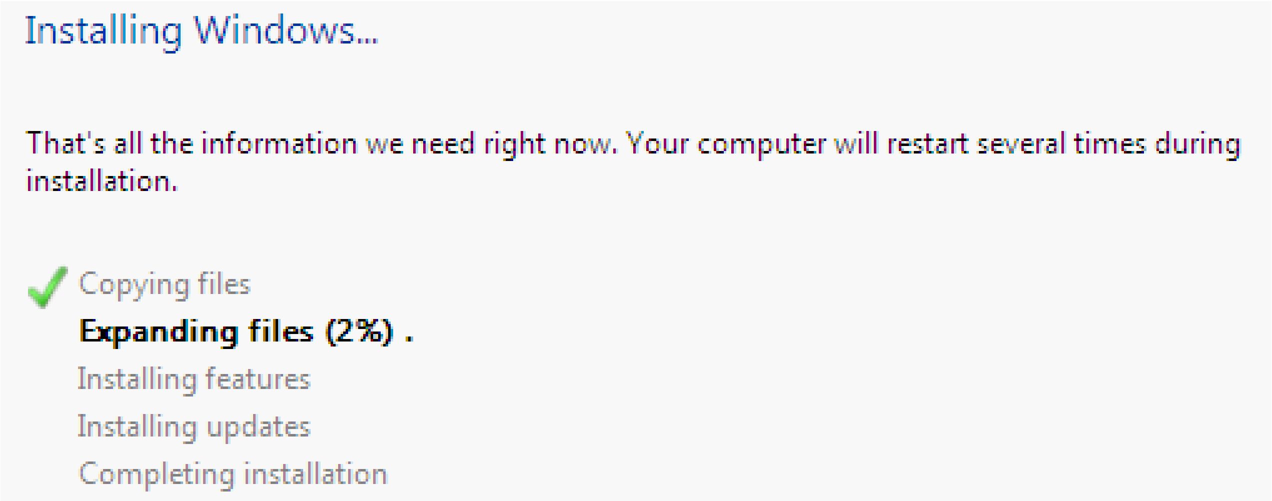


៧. ប្រសិនជា Hard Disk របស់អ្នកត្រូវបានរកឃើញដោយស្វ័យប្រវត្តនោះអ្នកអាចបង្កើតនិងរៀបចំបង្កើត partitions តាមតម្រូវការក្នុងពេលដំឡើងនេះ។ តែប្រសិនបើ Hard Disk របស់អ្នកមិនត្រូវបានរកឃើញ នោះមានន័យថា device driver សម្រាប់ controller របស់អ្នកមិនត្រូវបានបង្កើតចូលក្នុងWindows នៅឡើយនោះទេ។ ក្នុង

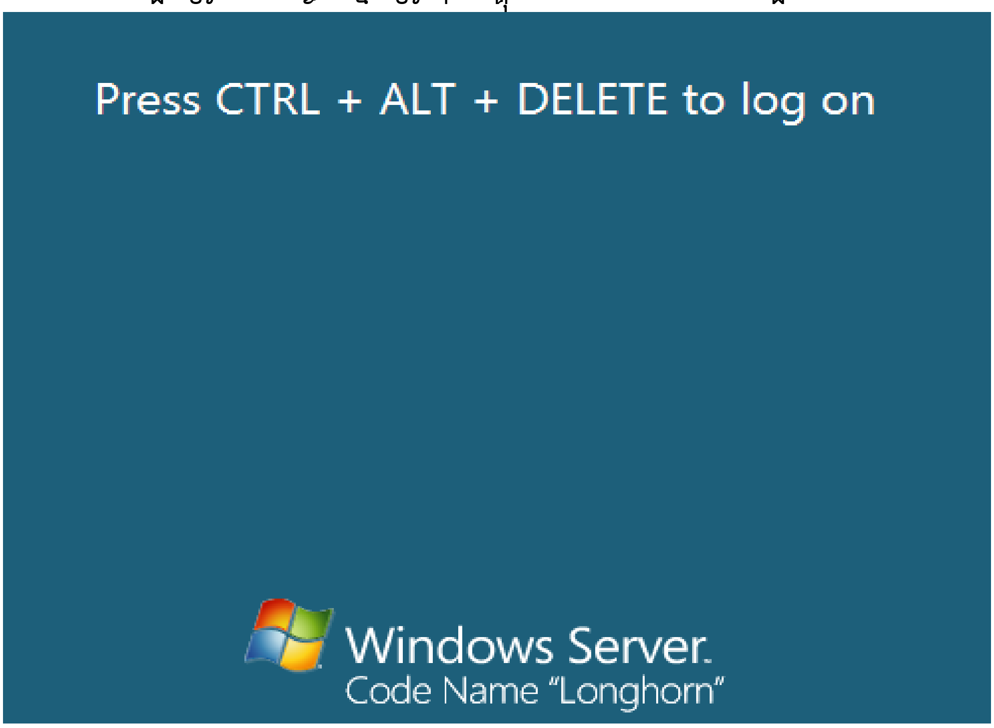
ករណីនេះអ្នកអាចចុច Load Driver ដើម្បី load វា។ ចុច Next បន្ទាប់ពីបានបង្កើត partition ដែលអ្នកនឹងត្រូវធ្វើការដំឡើង។



៨. នៅពេលនេះ Windows Server 2008 ផ្តល់នូវព័ត៌មានសំខាន់ៗទាំងអស់ដែលត្រូវការក្នុងការដំណើរការនៃការដំឡើង។វានឹងចាប់ផ្តើមដំណើរការនៃការដំឡើងនិងបង្ហាញនៅដំណាក់កាលនៃការដំឡើង។

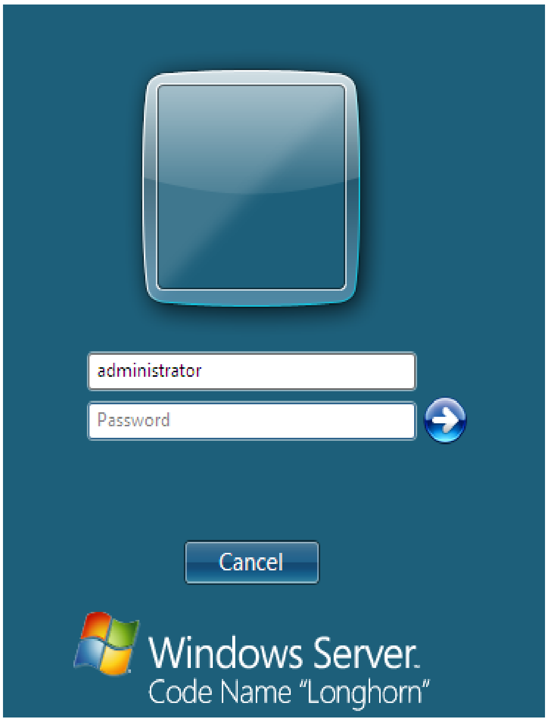


៩. នៅពេលដែលការដំឡើងត្រូវបានបញ្ចប់ អ្នកត្រូវចុចបង្គុំ CTRL+ALT+DEL ដើម្បី Log in



១០. ចុច Other User button (ដែលបង្ហាញក្នុងរូបខាងក្រោម) ចាប់ផ្តើម Login។ វាយបញ្ចូល Adminis -trator ជា Username ទុក Password ឱ្យទទេ រួចចុច arrow button ដើម្បី login រឺក៏ចុច ENTER។

១១. នៅពេលដែល **login** នៅលើកដំបូង អ្នកនឹងត្រូវការប្តូរ password ឱ្យវា។ ទុក New Password field ឱ្យនៅទទេ និងវាយបញ្ចូល password ថ្មីនៅក្នុង New Password និងConfirm Password field។ ចុច OK នៅពេលធ្វើការប្តូរ password របស់អ្នកបានសម្រេច។

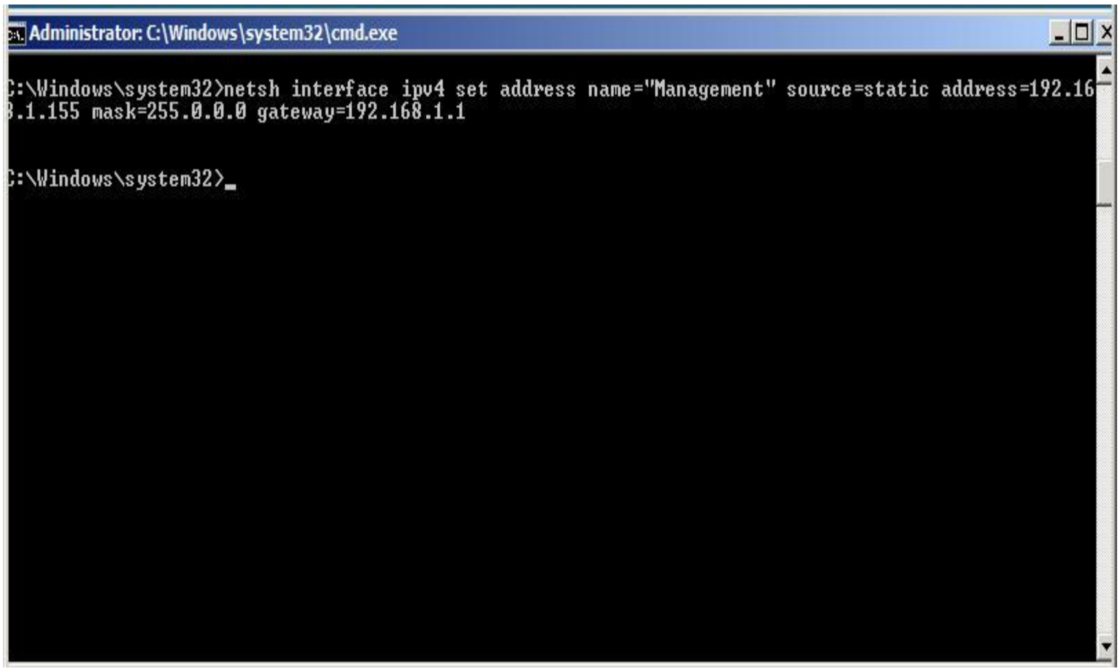


ក្រោយពីចុច **Other User** រួចនោះគឺចាប់ផ្តើមធ្វើការ **Log in** សូមវាយ ឈ្មោះគណនេយ្យ(**User Account**)ថា: **Admin istrator**

បញ្ជាក់: ក្នុងប្រអប់ **Password** វាយបំពេញឲ្យហើយក៏បាន ឬ ចាំពេលក្រោយក៏បានរួចចុចសញ្ញាព្រួញ ឬ ចុច**Key Enter**។

ការ **Log in** លើកបន្ទាប់ៗទៀតក្រោយពីអ្នកបានប្តូរ **Password** ជាថ្មីនោះ។

១២. ពេលអ្នក login រួចអ្នកនឹងទទួលបានតែ command prompt តែប៉ុណ្ណោះ។(ដូចរូបខាងក្រោម)



នៅចំនុចនេះអ្នកអាចគ្រប់គ្រង Sever ដោយប្រើតែ command prompt ប៉ុណ្ណោះ។ Remote administration ត្រូវបិទដោយ default។ ជំហានបន្ទាប់ដែលអ្នកត្រូវធ្វើគឺរៀបចំការ Configuration tasks ដោយសុទ្ធតែប្រើប្រាស់ command prompt ទាំងអស់។

៤-កិច្ចការដែលត្រូវធ្វើបន្ទាប់ពីការ Install បានបញ្ចប់

ដោយសារតែ Server Core សម្រាប់ Windows Server 2008 គ្មាន Interface (Graphic Tool) ក្នុងការរៀបចំ Server នោះទេ អ្នកត្រូវតែប្រើប្រាស់ command prompt ដូចបានបញ្ជាក់រួចខាងលើ។ ដើម្បីរៀបចំ Server អ្នកត្រូវធ្វើតាម ៦ ដំណាក់កាលដូចខាងក្រោម ៖

១. កំណត់ Administrator password

២. កំណត់ IP address ទៅឱ្យ Network card

៣. Activate the Server

៤. ប្តូរឈ្មោះរបស់ Server និងការភ្ជាប់ទៅកាន់ Domain

៥. កំណត់ Automatic Update

៦. បើក Remote administration

៧. កំណត់ Windows Firewall

១- កំណត់ Administrator password

ក្នុងការផ្លាស់ប្តូរ administrator password អ្នកអាចចុច **CTRL+ALT+DEL** និងជ្រើសរើស យក **Change a Password** រឺក៏ប្រើ command prompt ដូចខាងក្រោម៖

Net user Administrator *P@ssword*

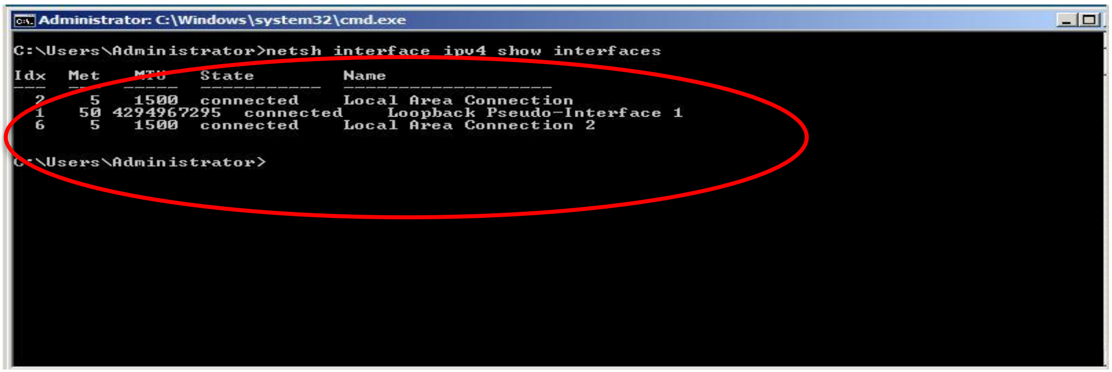
ផ្លាស់ប្តូរ *P@ssword* ទៅតាម password ដែលអ្នកចង់បាន។

២-Configure Network Interface (ការកំណត់ IP adress ទៅឱ្យ Network card)

Server Core ថ្មីដែលអ្នកទើបតែដំឡើងប្រើ DHCP ដើម្បីទទួលយកIP address។ បើសិនជា Server របស់អ្នកប្រើ Static IP address អ្នកត្រូវផ្តល់ IP address ដោយប្រើ *Netsh* command។ ដើម្បីធ្វើការកំណត់ IP address អ្នកត្រូវស្គាល់អំពីព័ត៌មានរបស់ Network card ដែលមាននៅក្នុង Server របស់អ្នកដោយប្រើ command ដូចខាងក្រោមនេះ ៖

Netsh interface ipv4 show interfaces

ប្រសិនជាអ្នកប្រើ IPv6 នោះអ្នកគ្រាន់តែប្តូរcommandពី ipv4 ទៅជា ipv6។ បន្ទាប់មកcommand ត្រូវបានបង្ហាញចេញនៅតារាងមួយ(ដូចមានក្នុងរូបខាងក្រោម)



ដែលនៅក្នុងក្បាលនៃតារាងមួយ ឈ្មោះ Idx ផ្តល់តម្លៃពិសេសឱ្យ Network interface និមួយៗដែលមាន។ រីឯការកំណត់ឱ្យ Network card ដែលមានលេខ Idx សម្រាប់ Local Area Connection ដែលមាន IP address 192.168.100.75 ជាមួយនិង Subnet mask 255.255.255.0 និង gateway 192.168.100.1 ដោយប្រើcommand ដូចខាងក្រោម ៖

Netsh interface ipv4 set address name=2 source=static address=192.168.100.75 mask=255.255.255.0 gateway=192.168.100.1

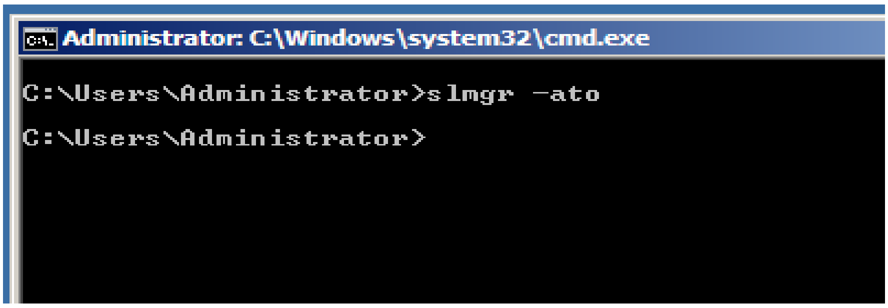
ចំពោះការកំណត់ DNS Server សម្រាប់ server ដែលមាន IP address 192.168.100.40 ដោយប្រើcommand ដូចខាងក្រោម ៖

Netsh interface ipv4 add dnsserver name=2 address=192.168.100.40

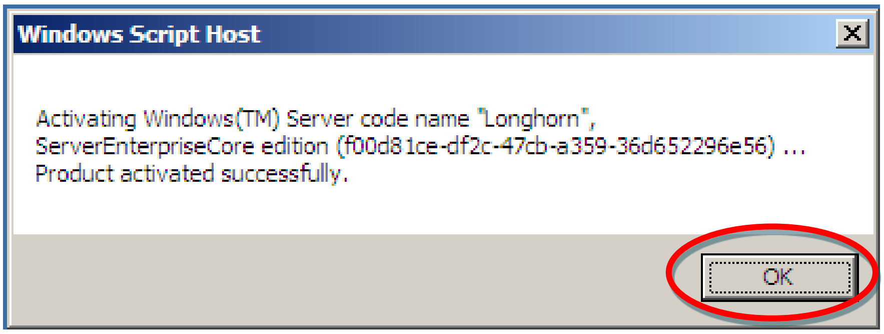
គ-Activating Your Server

Window Server 2008 ដែលអ្នកបានដំឡើងរួច គឺមានសុពលភាពត្រឹមតែរយៈពេល ១៤ ថ្ងៃប៉ុណ្ណោះ ដូច្នេះអ្នកត្រូវធ្វើឱ្យ Window Server 2008 របស់អ្នកអាចដំណើរការនិងមានសុពលភាពយូរអង្វែងដូចជាការប្រើប្រាស់ Window Software License Management Tool ដូចជាកម្មវិធី slmgr.vbs ដែលស្ថិតនៅក្នុង %WINDIR%\ system32 directory ជាដើម។ យើងដឹងហើយថា Server Core គ្មាន Graphical method ណា ដែលអាចប្រើសម្រាប់ activate Server នៅក្នុង Windows Server 2008 នោះឡើយ មានន័យថាអ្នកត្រូវប្រើប្រាស់នូវ Command:

Slmgr.vbs –ato



We even receive a confirmation pop-up:



លើសពីនេះទៅទៀត Command មួយនេះ(slmgr.vbs)អាចឱ្យអ្នកយកទៅប្រើប្រាស់ក្នុងការ activate នូវ Windows Server 2008 ថ្មីមួយទៀតពី Windows Server 2008 ដូចគ្នា (Remote ពី Windows Server 2008 Server)ដែលមានស្រាប់។ ឧទាហរណ៍ អ្នកចង់activate នូវ Windows Server 2008ថ្មី មួយហៅថា Utopia ដែលនៅ administrator password មានpassword123 ឱ្យពេញលក្ខណៈដូចគ្នាដែរ នោះអ្នក ត្រូវប្រើ Command ដូចខាងក្រោម:

Slmgr.vbs Utopia Administrator password123 -ato

Netsh Up Close and Personal

Netsh គឺ Ultimate command–line shell មួយសម្រាប់គ្រប់គ្រងនិងកំណត់នូវរាល់ Componenets Network របស់ Windows Server 2008 ។ Command គឺអាចប្រើបានក្នុង Windows version មុន ប៉ុន្តែឥឡូវ

Critical tool ច្រើនប្រើក្នុង Windows Server 2008 សម្រាប់ប្រើប្រាស់ក្នុងការ Query និងគ្រប់គ្រងពីគ្រប់ Network interface ,Windows Firewall និង DHCP server parameter បញ្ចូលទាំងការកំណត់ scope និងការដក IP address ចេញដើម្បីកំណត់ routing និង remote access policies។ Server Core វាបង្កើតសម្រាប់Windows administrator ដោយខានពុំបានដើម្បីស្វែងយល់ពីរបៀបប្រើឧបករណ៍ជាលទ្ធផលសម្រេចបាន។ ទោះបីជា Core network service ដែល Server Core អាចផ្តល់ក្នុងការគ្រប់គ្រង remote ដោយប្រើ MMC snap-in , key tasksក៏ដោយមិនអាចសម្រេចដោយគ្មាន Netsh នោះដែរ ជាពិសេសការ Configure network interfaces ដូចជាការកំណត់ static address រឺ DNS server ដើម្បីប្រើប្រាស់។

៤-ប្តូរឈ្មោះ Server និងកំណត់វាជាសមាជិករបស់ Domain

ដើម្បីប្តូរឈ្មោះកុំព្យូទ័រមុនពេលដែលធ្វើការចូលរួមទៅកាន់ Domain នោះគឺចាំបាច់ត្រូវប្រើ Windows Management Interface (WMI)។ ដូច្នេះការសរសេរ Script នឹងប្រតិបត្តិ (Execute)គឺត្រូវប្រើ command " WMI command-line "(WMIC) នេះ។ Command-line tool មួយនេះគឺត្រូវបានគេបង្កើតឡើងយ៉ាងពិសេសដើម្បី run WMI command សម្រាប់ដោះស្រាយការប្តូរឈ្មោះដោយពុំមានភាពស្មុគស្មាញ។ ឧទាហរណ៍ដើម្បីប្តូរឈ្មោះរបស់ server មួយ WINSRV1 ត្រូវវាយ command ដូចខាងក្រោមនេះ៖

wmic កុំព្យូទ័រsystem where name="%កុំព្យូទ័រname%" rename name="WINSRV1"

Command នេះបង្ហាញលទ្ធផល Return Value=0 ដើម្បីបង្ហាញថារួចរាល់ដោគជយ័ក្នុងការប្តូរឈ្មោះដូចបង្ហាញក្នុងរូបភាព២-៥។

បញ្ជាក់:

សម្រាប់ការប្តូរឈ្មោះកុំព្យូទ័រម្តងៗគឺចាំវាបាច់ត្រូវ ចាប់ផ្តើមម៉ាស៊ីនសាជាថ្មីវិញ ដើម្បីមានប្រសិទ្ធភាព។

បន្ទាប់ពីអ្នក ប្តូរឈ្មោះកុំព្យូទ័ររួចរាល់ហើយ អ្នកអាចភ្ជាប់វាទៅកាន់ domain ដោយប្រើ netdom join command ដែល command នេះចែកជា៣ផ្នែកគឺ:ឈ្មោះរបស់ Domain username នៃ account (ឈ្មោះប្រើប្រាស់) ដែលត្រឹមត្រូវសម្រាប់ join កុំព្យូទ័រ domain និង password(លេខសំងាត់)សម្រាប់ User account។ ឧទាហរណ៍: អ្នកចង់ Add Server មួយទៅកាន់ domain មួយឈ្មោះថា TESTLAB ដែលប្រើ account មួយហៅថា **SysAdmin** និងមាន លេខសំងាត់ P@assword អ្នកអាចដំណើរការតាម command ដូចខាងក្រោមនេះ

Netdom join %កុំព្យូទ័រname% /domain:TESTLAB /userD:SysAdmin/passwordD:P@ssword

បើសិនអ្នកមិនចង់វាយPassword ពេលនេះទេ ព្រោះមនុស្សជុំវិញអ្នកអាច View console អ្នកក៏អាចជំនួស /password: P@ssword ដោយ passwordd: នោះវានឹងលោត prompt password ជំនួសវិញ។ អ្នកត្រូវ restart កុំព្យូទ័រ បន្ទាប់ពីវាបាន join ទៅ domain រួចរាល់។

៥-Configure Automatic Update

អ្នកដឹងថា Microsoft យ៉ាងហោចណាស់បានផ្តល់វិធីងាយស្រួលដើម្បីចាប់ផ្តើមនិង configure Automatic Updates ប៉ុន្តែគ្មាន Windows explorer រឺក៏ Internet Explorer ដើម្បីទទួលបាននូវការ Update នោះទេ។ វាពិតជាលំបាក! អ្នកត្រូវការ Windows script file ហៅថា **scregdit.wsf** ដែលមានទីតាំងក្នុង **%WINDIR%\System32 directory** ប៉ុន្តែ Server coreគ្មាន **GUI** នោះទេ។ ប្រសិនបើគ្មាន GUI អ្នកប្រាកដជាមិនអាច control update ដើម្បី installបាននោះឡើយ។ ជាការពិត Workaround ទាំងអស់នេះគឺ Configure automatic update ដោយប្រើគោលការណ៍និងដំណោះស្រាយ **patch-management** ដូចជា Windows Server Update Service ដើម្បីត្រួតពិនិត្យជាក់លាក់ថា patch server មួយណាដែលអ្នកនឹងទទួល។ ដើម្បីឱ្យ Automatic update ដំណើរការបាន អ្នកអាច run តាម commandមួយនេះ :

Cscript Scregedit.wsf /AU 4

ដើម្បីបិទ Automatic update អ្នកអាច run តាម command:

Cscript Scregedit.wsf /AU 1

Note: Graphical warning message វាតែងតែបង្ហាញឡើងនៅពេលអ្នក run scregedit.wsf command ដើម្បីបញ្ជាក់ថាអ្នកបើក command prompt នេះប៉ុណ្ណោះ។ តែក៏អាចផ្លាស់ប្តូរ current directory ទៅ %WINDIR%\System32 និង run តាម command ដោយប្រើ Cscript ។

ឧទាហរណ៍ **cscript.exe scregedit.wsf /AU 4.**

៦ Enable remote Administration

អ្នកក៏អាចដំឡើង Console បានងាយស្រួលដើម្បីគ្រប់គ្រងកុំព្យូទ័រចំនួនច្រើនឬម៉ាស៊ីនទោល។ ក្នុងចំណុចនេះនឹងប្រាប់ពី Command-Line មួយក្នុងការប្រើនូវ Console មួយដែលអាចប្រើគ្រប់គ្រងពីចម្ងាយ(Remote)ទៅកុំព្យូទ័រផ្សេងទៀត។ Console មួយនេះរួមមានសេវា(Snap-in)ជាច្រើនដែលគ្រប់ គ្រងសេវាប្រព័ន្ធ System និង Event-Viewer snap-in ដែលអនុញ្ញាតឱ្យចូលទៅ event log។ Console នោះគឺ MMC snap-in ដែលវាជាបណ្តុំនៃ Tools ផ្សេងៗទៀតជាច្រើនងាយស្រួលក្នុងការគ្រប់គ្រង។ ការប្រើ MMC គឺជាអនុភាពបន្ថែមលើអ្នកគ្រប់គ្រងប្រព័ន្ធ System។ MMC ធ្វើការជាកញ្ចប់នៃប្រព័ន្ធ System tool មានលទ្ធភាពអ្នកគ្រប់គ្រង System ដើម្បីបង្កើតឯកទេសកម្មលើ tool ដែលអាចប្រើកិច្ចការគ្រប់គ្រងដើម្បី User ឬ Groupដែលមានរក្សាទុកក្នុងMMC (.msc) file មានទាំង Custom tool អាចផ្ញើរដោយ e-mail ចែកចាយតាម network folder ឬផ្ញើលើ web។ ជាមួយការបង្កើត System Policy វាអាចផ្តល់ឱ្យទៅ user, group ឬកុំព្យូទ័រ។

អ្នកអាចគ្រប់គ្រងការដំឡើងServer Core របស់អ្នកដោយប្រើ កុំព្យូទ័រ Management **MMC snap-in** (Microsoft Management Console) ប៉ុន្តែដោយការចូលប្រើតាម terminal service ក្នុង Remote administration mode។ ម្យ៉ាងទៀត ការដែលចូលប្រើតាម Terminal Service នៅក្នុង remote Administration mode គឺត្រូវបាន Disable ដោយ Default តែបើអ្នកត្រូវការបើកវាដើម្បីចង់ដឹងពីសមត្ថភាពរបស់វានោះត្រូវចូលទៅ Screge-dit.wsf Script និងRun ដោយវាយថា :

Secregedit.wsf/ARO

វាជាការពិតណាស់នេះគឺជាការបង្កើតឡើងដែលផ្ទុយពីវិធីសាស្រ្ត។ សូន្យមានន័យថាអ្នកចង់ enable Terminal Service in remote Administration mode និង**1** មានន័យថា អ្នកចង់ **Disable** វា។ បើសិនជាអ្នកចង់គ្រប់គ្រងទៅលើ Windows Server 2008 ពី Window Versionចាស់នោះអ្នកចាំបាច់ត្រូវជ្រើសប្រភេទជា "Legacy" ដើម្បីប្រាកដក្នុងការភ្ជាប់ឱ្យមានកម្រិត Security កាន់តែខ្ពស់សម្រាប់ Terminal Server in Window Server 2008។ ដើម្បីអនុញ្ញាតឱ្យ Terminal Server អាចភ្ជាប់ទៅ Window Version អ្នកត្រូវ Run តាម Command ដូចខាងក្រោម៖

Secregedt.wsf/cs 0

បើសិនជាអ្នកកំណត់ cs ទៅ ១ វិញ គឺអាចភ្ជាប់ Terminal Service ដើម្បីប្រើ CredSSP បាន ករណីនេះគឺវា Support តែជាមួយ Window Server 2008 និង Window Vista ប៉ុណ្ណោះ។

Tip : អំឡុងពេលដែល Windows Firewall enable ទៅលើ interface រឺក៏គ្រប់ profile ដោយ មិនបានបង្ហាញនោះវានិង enable Terminal Service in administration mode ដោយមិនចាំ បាច់បញ្ជាទៅលើ Server ក្នុងការប្រើ Remote Desktop protocol (RDP) ទេ ក្នុងការបើក Terminal Service port ទៅលើ Server គឺអាចបញ្ចូលច្បាប់ Firewall ដើម្បីត្រលប់ TCP connection ទៅ port 3389 តាមរយៈ netsh:

Netsh advfirewall firewall add rule name="Ts Admin" protocol=TCP dir=in local port=3389 action=allow

១០-៣- Configure the Window Firewall

Window Firewall គឺជា host-base, bidirectional network traffic filter មានន័យថា វាប្រើប្រាស់សម្រាប់ការការពារប្រព័ន្ធ Network ពីពពួក Hacker, Spyware និង Virus ជាដើម។ Window Firewall នៅក្នុង Windows Server 2008 វាមិនដូចទៅ Window Firewall នៃ Windows XP SP2 ធម្មតានោះទេ តែវាមានលក្ខណៈពិសេសៗជាច្រើនក្នុងការគ្រប់គ្រងដូចជា Inbound នឹង outbound traffic។ Window Firewall នេះដែរក៏អាចការពារប្រព័ន្ធ Network នៅពេលដែលភ្ជាប់ជាមួយ internet Network ដោយមានការពឹងផ្អែកទៅលើ Server នៅក្នុង Network ដោយការ define polices ផ្សេងៗជាដើម។ ឧទាហរណ៍៖ អ្នកអាចធ្វើការ configure polices ដូចជាអនុញ្ញាតឱ្យ file and print sharing បាននៅក្នុង domain network ហើយក៏អាចបិទវាបើសិនជាករណីស្ថិតក្នុង public network។ ការ configure ទៅលើ Firewall និងដំណើរការជាមួយនិង Netsh លើ Command Window Firewall ជាមួយនឹងSecurity MMC ទៅ Command Window Server 2008 យ៉ាងណាក៏ដោយមុននឹងអ្នកអាចគ្រប់គ្រងលើ Server Core installation's firewall ដោយប្រើ MMC Snap អ្នកត្រូវ Enable និងបញ្ជារលើការគ្រប់គ្រងជាមុន។ដើម្បីអនុវត្តន៍វាត្រូវវាយ Command

Netsh advfirewall set current settings remotemanagement enable

អ្នកអាចចូលទៅក្នុង Window Server 2008 ដទៃទៀតដើម្បីធ្វើការ Install និង add Window Firewall ជាមួយនិង Advance Security MMC snap-in និងចង្អុលវាទៅកាន់ Server ដែលអ្នកចង់គ្រប់ គ្រង។ ប៉ុន្តែបើសិនជាមានតែ Window Server 2008 តែមួយដែលដំណើរការលើ Network របស់អ្នក ដូច្នេះអ្នកចាំបាច់ត្រូវ Configure ទៅលើ Firewall ដោយប្រើ Netsh៕

ដើម្បីបង្ហាញView គ្រប់ Profile Firewall ទាំងអស់នៅក្នុង system ដែលអ្នកអាច Run តាម Command ខាងក្រោម៖

Netsh advfirewall show allprofiles

នៅក្នុងការ output អ្នកនឹងឃើញ Property ទូទៅនៃកម្មសិទ្ធរបស់អ្នកជា Public និង Private ដូចជា State បើសិនជាអ្នកចង់ enable ចំពោះ Profile ឧទាហរណ៍កម្មសិទ្ធ Profile អ្នកអាច Run តាម Command ដូចខាងក្រោម៖

ដើម្បីបង្ហាញបិទ ឬ បើក Firewall Run តាម Command ខាងក្រោម៖

Netsh advfirewall set domainprofile state on

១០-៤- Installing and Configuring Server Roles

អ្នកអាចប្រតិបត្តិទៅតាមមូលដ្ឋានក្នុងការ install Server Core ក៏ដូចជាការ Install Server 2008 ដែរ ។

១០-៤-១- Installing and Configuring the DNS Server Role

DNS (Domain Name System) គឺជាស្តង់ដា Internet Services ដែលបានរៀបចំជាក្រុមនៃកុំព្យូទ័រទៅក្នុងដែនកំណត់ domain។ វាជាឈ្មោះសេវាសម្រាប់ដោះស្រាយឈ្មោះកុំព្យូទ័រទៅ Internet Protocol (IP) address។ ការប្រើប្រាស់ DNS ដូចជាឈ្មោះ host.omega. microsoft.com។ DNS ធ្វើប្រតិបត្តិការលើ

Transmission Control Protocol/ Internet Protocol (TCP/IP) ហើយអាចប្រើជា Window Internet Name Services(WINS)និងDynamic Host Configuration Protocol (DHCP) ហើយនិង Active directory ។ ដើម្បី Install DNS Server Role អ្នកត្រូវ Run តាម Command ដូចខាងក្រោម:

Start /w ocsetup DNS-Server-Core-Role

វាត្រូវការ ៣ រឺ ៤ នាទីក្នុងការ Install ប៉ុន្តែវាមិនបង្ហាញនៅលើ dialog box ទេ ។ យើងត្រូវចងចាំថាការ Install គឺអាចប្រើបានតែនៅលើ DNS តែប៉ុណ្ណោះ។ អ្នកអាច Configure DNS Server ដោយប្រើ DNS snap-in ពីកុំព្យូទ័រផ្សេងគ្នា រឺ ក៏វាយនូវ *dnscmd* នៅលើ Command Prompt ។ ដើម្បីបង្ហាញនូវការកំណត់ទូទៅ និងព័ត៌មាននៃការ Install/DNS Server របស់អ្នក អ្នកអាច run តាម Command:

Dnscmd /info

ជំហានដំបូងបន្ទាប់ពី Install DNS Server អ្នកត្រូវ **Configure DNS Zone**។ ឧទាហរណ៍ :

ដើម្បី **add zone as a Primary Zone** អ្នកអាច run តាម Command:

Dnscmd /zoneadd "testlab.local" /Primary /file "testlab.local.dns"

ដើម្បី **Assing IP adress** វាយ Command:

Dnscmd /recordadd testlab.local testpc A 192.168.100.71 /f

ដើម្បីបង្ហាញតារាងទាំងអស់ដែលមាននូវនៃប្រភេទ record ចូរវាយ Command:

Dnscmd /recordadd /?

បើសិនជាអ្នកចង់មើលឃើញគ្រប់ record ទាំងអស់និង zone ពិសេសអ្នកអាចប្រើ **Zoneprint switch**។ ឧទាហរណ៍:

ដើម្បីបង្ហាញនូវរាល់ **List** ទាំងអស់ ដែលចូលមកក្នុង testlab.local zoneរបស់អ្នក ត្រូវវាយ Command:

Dnscmd /zoneprint testlab.local

បើចង់លុបនូវ record អ្នកអាច run តាម dnscmd ជាមួយនឹង recordadd ត្រូវវាយCommand:

Dnscmd /recordadd testlab.local testpc A 192.168.100.71 /f

* មានវិធីតែមួយគត់ក្នុងការប្តូរ DNS server របស់អ្នកក្នុង Zone ប៉ុន្តែវាក៏អាចពិនិត្យទៅលើserverផ្សេងទៀតបានផងដែរ។ បើសិនជាអ្នកសម្រេចថា server core ពិតជាផ្តល់ចម្ងាយឆ្ងាយជាងDNS Service អ្នកអាច **uninstall** វាដោយវាយ Command ដូចខាងក្រោម:

Start /w ocsetup DNS-Server-Core-Role /uninstall

១០-៤-២- ការដំឡើងនិងការ and Configuring លើ DHCP Server Role

អ្នកអាចប្រើ **Dynamic Host Configuration Protocol(DHCP)** ដើម្បីងាយស្រួលក្នុងការគ្រប់គ្រង Active Directory និង សេវា domain ហើយ DHCP ក៏មាននាទីក្នុងការ Assign information ទៅឱ្យ DHCP Client ដោយស្វ័យប្រវត្ត។នៅពេលដែល DHCP Server ផ្តល់ IP Address ទៅឱ្យ DHCP Clientនោះ DHCP Client គ្មាន IP Address ទេ មានន័យថា Client មាន IP Address នោះគ្រាន់តែប្រើបណ្តោះអាសន្នប៉ុណ្ណោះ។

DHCP គឺជាមជ្ឈមណ្ឌលសម្រាប់ឱ្យអ្នកត្រួតពិនិត្យ IP address។ ប្រសិនបើ Network បានប្រើ DHCP Server លោកអ្នកអាចផ្តល់ Dynamic IP Address ទៅឱ្យ network interface card (NICs)ទាំងអស់ដែលនៅលើកុំព្យូទ័រ។ ម្យ៉ាងទៀត DHCP ត្រូវបានដំឡើងនៅលើ DHCP Serverដើម្បីផ្គត់ផ្គង់ព័ត៌មានមូលដ្ឋានចាំបាច់សម្រាប់ប្រព័ន្ធ TCP/IP ដែលរួមមានដូចជា: IP address, Subnet mask និង Default gateway និងផ្សេងៗទៀត

ដូចជា Primary និង Secondary Windows Internet Name Services (WINS) Server និងសំខាន់គឺឈ្មោះ DNS domain។ អ្នកគ្រប់គ្រងប្រព័ន្ធ Network ងាយស្រួលក្នុងការគ្រប់គ្រងប្រព័ន្ធ Network ទាំងមូលដោយមិនចាំបាច់បញ្ចូល IP ដោយប្រើដៃ នៅពេលមាននរណាម្នាក់ភ្ជាប់ជាមួយប្រព័ន្ធដោយដោតភ្ជាប់ម៉ាស៊ីន Server ដែលប្រើ Windows Server 2008 ដែលមានជំនឿងប្រើ DHCP បានបញ្ជូន IP ដោយស្វ័យប្រវត្តមកឱ្យ Client ដែលកំពុងភ្ជាប់ នោះអ្នកអាចចូលបានក្នុងប្រព័ន្ធ Network តំបន់នោះ។

ការដំឡើងDHCPគឺស្តង់ដារ TCP/IP ត្រូវបានបង្កើតឱ្យមានភាពងាយស្រួលក្នុងពេលគ្រប់គ្រងលើប្រព័ន្ធ Network ទាំងមូល។ ការដំឡើងដើម្បីគ្រប់គ្រង address ដែលបានបង្កើតឡើងដោយប្រើកុំព្យូទ័រ Server ដែលជាមជ្ឈមណ្ឌលនៃការគ្រប់គ្រង IP address ជាច្រើននិងការទំនាក់ទំនងក្នុងការបង្កើត ដែលមាននៅលើប្រព័ន្ធ Network របស់អ្នកដែលប្រើ នៅលើ Window Server 2008 ហើយបានផ្តត់ផ្គង់សេវា DHCP វាមានលទ្ធភាពធ្វើឱ្យ Server ដែលមានសណ្ឋាន DHCP Server និងដំឡើងDHCP ។ វាអាចផ្តត់ផ្គង់ឱ្យ Client នៅលើ Network របស់លោកអ្នក។

មុននឹងអ្នកអាចប្រើវាជាមួយ Window Server Core អ្នកចាំបាច់ត្រូវការ Install ដោយប្រើ command ដូចខាងក្រោម:

Start /w ocsetup DHCPServerCore

ក្នុងការ Install អ្នកនឹងមាន option ដើម្បីconfigure DHCP របស់អ្នកដោយប្រើ **netsh** ឬក៏ DHCP MMC snap-in ពី Remote Server។ បើសិនជា DHCP Server ដំណើរការនៅក្នុង Active Directory domain វាត្រូវតែអនុញ្ញាតឱ្យ Active Directory មានមុខងារអាចដោះស្រាយ IP address អ្នកអាចផ្តល់សិទ្ធទៅឱ្យ **DHCP Server** ក្នុងdomain ដោយប្រើ**DHCP MMS** snap-in ប៉ុន្តែវាក៏អាចប្រើ netsh ផងដែរ។

ឧទាហរណ៍:

ឧបមាថា Server Core របស់អ្នកឈ្មោះ **WINDHCP1** មួយ ដែលមាន IP address 172.16.0.5 ហើយអ្នកមានបំណងចង់ផ្តល់សិទ្ធិវាទៅក្នុង domain របស់អ្នក សូម log on ទៅកាន់ **WINDHCP1** ឱ្យបានជាក់លាក់ជាមួយនឹង domain ត្រឹមត្រូវទៅកាន់ DHCP Servers បន្ទាប់មក run វាតាម command ខាង ក្រោម:

Netsh dhcp add server WINDHCP1 172.16.0.5

ប៉ុន្តែបើសិនជាអ្នកមិនចង់ផ្តល់សិទ្ធិឱ្យទៅ Server នោះត្រូវ run command ខាងក្រោម:

Netsh dhcp delete server WINDHCP1 172.16.0.5

បើសិនជាអ្នកសម្រេចថា Server Core មិនអាចប្រើបានវែងជាងការផ្តល់នៃ DHCP Service វាអាចuninstall ដូចជា:

Start /w ocsetup DHCPServerCore /uninstall

១០-៤-៣- ការដំឡើងនិង Configure លើ File Server Role

ជា Default តួនាទីរបស់ **File Server** គឺត្រូវបានដំឡើងនៅក្នុង Window Server 2008 Server Core រួចជាស្រេចទៅហើយ តែបើសិនជាអ្នកចង់ប្រើប្រាស់បន្ថែមនូវតួនាទីផ្សេងៗមួយចំនួនទៀតដូចបានរាយខាងក្រោមនេះ:

- File Replication
- Distributed File System (DFS)
- Distributed File System Replication

➢ Network File System (NFS)

ក្នុងការដំឡើងបន្ថែមនូវតួនាទីខាងលើ គឺអ្នកនឹងប្រើប្រាស់ **ocsetup** Command ដូចគ្នាទៅនិងការដំឡើង DNS និង DHCP នោះដែរវាមិនមានអ្វីខុសប្លែកគ្នានោះទេ។

តារាងខាងក្រោមនេះ ជា Command មួយចំនួនសម្រាប់ការដំឡើងបន្ថែមនូវតួនាទីរបស់ **File Server :**

តួនាទី	Installation Command
File Replication	start /w ocsetup FRS-Infrastructure
Distribute File System	start /w ocsetup DFSN-Server
Distribute File System Replication	start /w ocsetup DFSR-Infrastructure-ServerEdition
Network File System	start /w ocsetup ServerForNFS-Base start /w ocsetup ClientForNFS-Base

១០-៤-៥- ការដំឡើង និង Configure នៅលើ Printer Server Role

អ្នកគ្រប់គ្រងត្រូវធ្វើការជាមួយបញ្ហាពីរចម្បងដូចជាអ្នកប្រើប្រាស់ User ឆ្លងកាត់តាមប្រព័ន្ធ Network មួយអាចអនុញ្ញាតចូលឧបករណ៍ print ដែលភ្ជាប់ជាមួយ Windows Server 2008 ពេលនោះអ្នកត្រូវបង្កើត **Printer Server** មួយ ហើយអ្នកត្រូវប្រើ Printer Server ដើម្បីចែកចាយ print លើប្រព័ន្ធ Network ។ ក្នុងចំណុចនេះនឹងប្រាប់ពីការដំឡើងម៉ាស៊ីន Printer Server លើ Windows Server 2008 ដែលអនុញ្ញាត្តឱ្យអ្នកដំឡើងនិងគ្រប់គ្រងម៉ាស៊ីន print លើប្រព័ន្ធ Network។ ដើម្បីដំឡើង Print Servers សូមប្រើប្រាស់នូវ command មួយនេះ :

Start /w ocsetup Printing-ServerCore-Role

ឧបមាអ្នកចង់ដំឡើងនូវ Line Printer Daemon (LPD) Services មួយដូច្នេះអ្នកត្រូវ run command-line ដូចខាងក្រោម:

Start /w ocsetup Printing-LPDPrintService

១០-៤-៦- ការដំឡើងនិង Configure នៅលើ Streaming Media Services Role

Streaming Media Services គឺជា Service មួយសម្រាប់បង្កើតជា Image file ដែល Image file នោះសម្រាប់យកទៅប្រើប្រាស់ក្នុងការ Back up ឬ Restore។ ដើម្បីដំឡើងនូវ Streaming Media Services ត្រូវអនុវត្តន៍តាមជំហានដូចខាងក្រោម:

១-ទាញយក (Download) Streaming Media Services installer KB934518 ពីគេហទំព័ររបស់ Microsoft ′s support ដែលមាន អាស័យដ្ឋានគេហទំព័រ (http://support.microsoft.com/kb/934518) ហើយ Copy វាទៅដាក់ក្នុង Server Core អ្នក នៅពេលអ្នកធ្វើការដំឡើងServer Core ។

* **បញ្ជាក់:**

អ្នកត្រូវធ្វើរបៀបនេះខុសគ្នាទៅតាម Server ចាប់តាំងពី Server Core មិនទាន់ Browser មកម្លេះ

២-ដំណើរការ (run) MSI file ដែលបាន Download នោះ

៣-ដំឡើង Service នេះដោយ run command-line ដូចខាងក្រោម:

Start /w ocsetup MediaServer

- អ្នកនឹងត្រូវការគ្រប់គ្រងការដំឡើងតួនាទីថ្មីៗដែលត្រូវមានការអនុញ្ញាតពី Server រឺ Works-tation ដោយប្រើ Streaming Media Services MMC snap-in។

១០-៤-៧- ការដំឡើងនិង Configure នៅលើ Active Directory Services Role

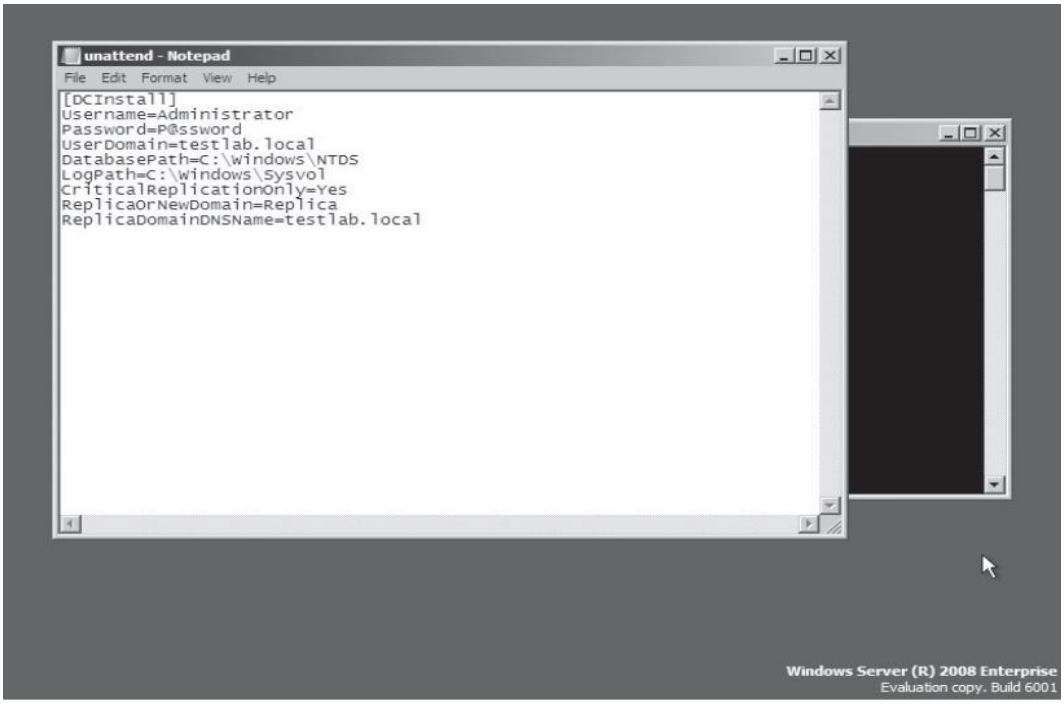
ការគ្រប់គ្រង Active Directory គឺជាចំណុចបំភ្លឺរួមដែលអ្នកត្រូវធ្វើជាមួយសេវា Active Directory ដូចជា បង្កើត Account កុំព្យូទ័រឬចូលរួមទៅកាន់ domain និងគ្រប់គ្រងទៅលើ Object ដូចជា User group printer file and resource ដែលមាននៅក្នុង Windows ។ នៅក្នុងចំណុចនេះ អ្នកនឹងស្វែងយល់ពីការប្រើប្រាស់ Command-line ជាច្រើនដែលអ្នកគ្រប់គ្រង Active Directory មានលក្ខណ:ពិសេសសម្រាប់គ្រប់គ្រងកុំព្យូទ័រ domain controller Organization Unit ជាដើម។

Active Directory Domain Service (AD DS)គឺជាDirectory Service មួយនិង data ដែលរៀបចំតាមលំដាប់ថ្នាក់សម្រាប់រក្សាទុកនូវព័ត៌មានអំពី Objects ដែលស្ថិតនៅលើប្រព័ន្ធ Network ហើយធ្វើឱ្យ Network Administrator ងាយស្រួលក្នុងការគគ្រប់គ្រងនិងស្វែងរក Objects ទាំងនោះ ។

គ្រប់ role ដទៃទៀតដែលបានរួមបញ្ចូលនៅក្នុងការដំឡើងServer Coreគឺ Active Directory មានភាពស្មុកស្មាញជាងគេ។ វាមិនមានភាពសមមូលទៅនឹង **ocsetup command** សម្រាប់ដំឡើង Active Directory នោះទេ តែវាជំនួសដោយបានពឹងពាក់ការប្រើប្រាស់ **dcpromo.exe** ទៅវិញ ព្រោះថាការដំឡើងServer Core នោះគឺពុំមាន GUI display នោះទេ។ ដូច្នេះទើបបង្ខំឱ្យយើងដំឡើងនូវ **Active Directory** ទៅតាម unattended setup។

dcpromo /unattend:c:\unattend.txt

ដោយសន្មត់ថា **c:\unattend.txt** គឺជាលទ្ធផលនៃ file dcpromo.exe វាអាចមានទីតាំងខុសពីនេះ។ ទាំងនេះមិនមានភាពស្មុគស្មាញនោះទេ ប៉ុន្តែអ្វីដែលសំខាន់នោះថាតើត្រូវ Format file unattend.txt សម្រាប់ dcpromo.exe យ៉ាងដូចម្តេច? **dcpromo.exe** បានបង្កើត(built)នៅក្នុង Window Sever 2008 ក៏មិនខុសពីបានបង្កើត(built)នៅក្នុង Window Sever 2003 គ្រាន់តែជំនាន់ថ្មីនេះsupport នូវ Feat លក្ខណ:ពិសេសជាច្រើន។ ដូចនេះអ្នកអាចប្រើ unattend.txt file ក្នុង Windows Sever 2003 លើ Windows Sever 2008។ (*មើលក្នុងរូបភាពខាងក្រោម unattend.txt file*)។ unattend.txt file support នូវ option ច្រើនជាងដូចដែលបានឃើញនៅ ឧទាហរណ៍ file ក្នុងរូបភាព។ អ្នកត្រូវប្រាកដច្បាស់ចំពោះ option ទាំងនោះនូវអ្វីដែលអ្នកត្រូវការវា។ នៅក្នុងរូបភាពនៃឧទាហរណ៍របស់ខ្ញុំ គឺខ្ញុំប្រើសម្រាប់ join ការដំឡើងServer Core របស់ខ្ញុំទៅកាន់ Windows Server 2008 Domain ដែលមានស្រាប់ឈ្មោះថា: testlab.local ។



អ្វីៗទាំងអស់នៅក្នុង Version(កំណែប្រែថ្មី)នៃ Graphical របស់ dcpormo តាមរយៈការដំឡើងunttended នៅក្នុងតារាងនៃប៉ារ៉ាម៉ែត្រខាងក្រោមនេះ អ្នកអាចប្រើវាក្នុង unttended.txt file សម្រាប់ធ្វើការ configure domain controller។

AdministratorPassword	<password>	សម្រាប់លុបDC វានឹងកំណត់ default administrator pass word ។ បើមិនបានកំណត់នោះទេ វានឹងប្រើ Password ទទេរ។
AllowDomainControllerReInstall	Yes | No | NoAndNo PromptEither	បើមាន DC មួយទៀតដែលមានឈ្មោះរួចហើយ វាគ្រប់គ្រងលើដំឡើងបន្ត។ វានឹង overwrite លើ DS data សម្រាប់ DC ដែលមានស្រាប់។
ApplicationPartitionsToRepLicate	<partitions>	សម្រាប់កំណត់ application partition ដែលត្រូវ Replicated ។ បើកំណត់ជា * វិញ នោះគ្រប់ partitions ទាំងអស់និងត្រូវ replicated ។
AutoConfigDNS	Yes | No	If yes, configures DNS for a new domain if DNS dynamic update protocol is not enabled.
ChildName	<child_domain _name>	The portion of the domain name that refers to the child domain. Applies only when installing a child domain.
ConfirmGC	Yes | No	សម្រាប់កំណត់ច្បាស់លាស់ឱ្យដឹងថា DC នេះជា global catalog ។ default គឺ yes.

CriticalReplicationOnly	Yes | No	បើ yes កំណត់ការចាប់ផ្តើមនៃ replication ចំពោះផ្នែកសំខាន់ដែលត្រូវការដើម្បីដំណើរការ។ ចំពោះផ្នែកមិនសំខាន់ដូចជា application partitions ដែលត្រូវ replication នៅពេលក្រោយ។ ដោយសារតែ replication មានរយៈពេលយូរ ការប្រើ Option នេះជានាថា AD installationឆាប់រហ័សពីព្រោះថា dcpromo មិនត្រូវការរង់ចាំសម្រាប់ replication ទាំងមូលនោះទេ។
Database Path	<path_to_database_file>	ទីតាំងសម្រាប់រក្សាទុក domain database %SYSTEMROOT% \NTDS.
DemoteFSMO	Yes | No	នៅពេលកំណត់វាជា yes វាបង្ខំឱ្យដកតួនាទីនៃ DC ទោះបីវាជា Flexible Single Master Opera tions role ដែលគេបានរកឃើញវានៅលើ DC.
DisableCancelForDnsInstall	Yes | No	បង្ហាញឱ្យដឹងថា Cancel button ត្រូវបានបិទក្នុងកំឡុងពេលនៃការដំឡើង DNS ។ ដោយសារតែ Server Core មិនបង្ហាញជា GUI នោះទេ វាបានបង្ហាញជា prompts ជំនួសវិញដែលអនុញ្ញាតឱ្យអ្នកចុចបង្កំ ctrl-c ដើម្បីផ្អាកលការដំឡើង។
DNSDelegation	Yes | No	បញ្ជាក់ឱ្យដឹងថា DNS delegation សម្រាប់ domain ត្រូវបានបង្កើតក្នុង parent zone ។
DNSDelegationUserName	<username>	គឺជា username ដែលត្រូវបានប្រើសម្រាប់បង្កើត DNS delegation.
DNSDelegationPassword	<password>	បញ្ជាក់ឱ្យដឹងថាត្រូវកំណត់ DNS Server addresses ជាស្វ័យប្រវត្ត
DomainNetBiosName	<domain_netbios_name>	កណត់ឈ្មោះរបស់ NETBIOS ចំពោះ domain។ ប្រើ Option នេះសម្រាប់ Domain ថ្មី
DomainLevel	0 | 2 | 3	គឺជាកម្រិតនៃ Domain នៅពេលដែលផ្តល់តួនាទី Domain ថ្មី
ForestLevel	0 | 2 | 3	គឺជាកម្រិតនៃ Forest នៅពេលដែលបង្កើនតួនាទី Domain ថ្មីក្នុង forest ថ្មីមួយ។
IgnoreIsLastDNSServerForZone	Yes | No	បញ្ជាក់ឱ្យដឹងថាការកាត់បន្ថយតួនាទីបន្តនៅពេលវាជា DNS Server ចុងក្រោយសម្រាប់ AD Integrated zones មួយឬច្រើនដែលវាជាអ្នកបង្ហោះ
IgnoreIsLastDcInDomainMismatch	Yes | No	បង្ខំឱ្យ dcpromo គោរពប៉ារ៉ាម៉ែត្រ IsLastDCInDomain ទោះបីជាវារកឃើញថា DC នេះមិនមែនជា DC ចុងក្រោយក្នុង Domain

IsLastDCInDomain	Yes | No	នៅពេលវាដកតួនាទីពី DC នេះ បញ្ជាក់ឱ្យដឹងថាវាជា DC ចុងក្រោយក្នុង Domain។
LogPath	<path_to_logfile>	គឺជាទីតាំងសម្រាប់រក្សាទុក domain log files ។ Defaults to %SYSTEM ROOT %\NTDS.
NewDomain	Tree | Child | <Forest>	បើវាជា Domain ថ្មីមួយត្រូវបញ្ជាក់ពីប្រភេទរបស់វា
OnDemandAllowed	<security_group> | None	Name of the Branch Replicated security group that contains the កុំព្យូទ័រ and user accounts to be replicated to a read-only DC.
OnDemandDenied	<security_group> | None	Name of the Branch Non rep -licated security group. Contains the list of កុំព្យូទ័រ and user accounts that are not to be replicated to a read-only DC.
ParentDomainDNSName	<dns_name_of_domain>	When installing a child domain, specifies the DNS name of its parent.
Password	<password>	The password of the username used for promoting this server.
RebootOnCompletion	Yes | No	Restart upon completion regard less of success.
RebootOnSuccess	Yes | No	Restart upon successful comple tion.
RemoveApplicationPartitiOns	Yes | No	Specifies whether to remove the application partitions. Applicable only when demoting a DC.
ReplicaDomainDNSName	<dns_name_of_domain>	DNS domain name of the domain to replicate from.
ReplicaOrNewDomain	<Replica> | ReadOnlyReplica | Domain	Specifies whether this is the first DC in a new domain or a replica directory service DC.
ReplicationSourceDC	<dns_name_of_DC>	The DNS name of the DC to replicate from.
ReplicationSourcePath	<replication_source_path>	Specifies the location of the source files when creating a new DC using the Installation from Media option.
SafeModeAdminPassword	<password>	The password used to start the

		កុំព្យូទ័រ in safe mode and directory service restore mode. The default is blank for new domains, so you should set this password when creating a new domain.
SiteName	<site_name>	Name of the existing site to place this new DC. The default is Default-First- Site-Name.
SysKey	<none> | system key	Specifies whether the user needs to supply a system key.
SysVolPath	<path_to_database_file>	Path to SYSVOL database. The default is %SYSTEM ROOT% \ sysvol.
UserDomain	<domain_name>	Domain name for the username used to promote this DC.
UserName	<username>	Username used for promoting this DC.

១០-៤-៨- ការដំឡើង Optional Features

នៅពេលដែលអ្នកដំឡើង Server Core ហើយធ្វើការ configure ចំពោះ roles ទាំងនោះរួចមកអ្នកក៏អាចដំឡើងបន្ថែមនូវលក្ខណៈពិសេសមួយចំនួនទៀតផងដែរ។ ខាងក្រោមនេះគឺជាលក្ខណៈពិសេសដែលអាចប្រើសម្រាប់ជាប្រយោជន៍ក្នុងការដំឡើងServer Core នោះ៖

- Backup
- Bitlocker Drive Encryption
- Microsoft Failover Clustering (not available in Windows Server Standard Edition)
- Multipath IO
- Network Load Balancing
- Removable Storage Management
- Simple Network Management Protocol (SNMP)
- Subsystem for UNIX-based applications
- Telnet Client
- Windows Internet Name Service (WINS)

បញ្ជាក់៖ ចំពោះលក្ខណៈពិសេសទាំងនេះគឺមិនបានបកស្រាយក្នុងកិច្ចការនេះទាំងអស់បានទេ តែមានជាតារាងសម្រាប់ប្រើប្រាស់នូវ Command-line ។

ចំណាំៈចំពោះលក្ខណៈពិសេសមួយចំនួនត្រូវការនូវតម្រូវការទៅតាម Hardware របស់វាដូចជាៈ Bitlocker Drive Encryption, Microsoft Failover Clustering, Multipath IO, Network Load Balancing និង Removable Storage Management។ គ្រប់លក្ខណៈពិសេសដែលបានដំឡើងគឺសុទ្ធតែប្រើ ocsetup

command ទាំងអស់។ តារាងខាងក្រោមនេះជាតារាងនៃ Command-lineដែលត្រូវការប្រើសម្រាប់ដំឡើងនៃលក្ខណៈពិសេសទាំងនេះ

Backup	**start /w ocsetup WindowsServerBackup**
Bitlocker Drive Encryption	**start /w ocsetup BitLocker**
Microsoft Failover Clustering	**start /w ocsetup FailoverCluster-Core**
Multipath IO	**start /w ocsetup MultipathIo**
Network Load Balancing	**start /w ocsetup NetworkLoadBalancing HeadlessServer**
Removable Storage Management	**start /w ocsetup Microsoft-Windows-RemovableStorageManagementCore**
Simple Network Management Protocol	**start /w ocsetup SNMP-SC**
Subsystem for UNIX-based applications	**start /w ocsetup SUACore**
Telnet Client	**start /w ocsetup TelnetClient**
Windows Internet Name Service	**start /w ocsetup WINS-SC**

ចំណាំៈចំពោះ **command** ទាំងនេះគឺមានលក្ខណៈផ្ទុយមកវិញ(Install និង Uninstall) មានន័យថា មួយចំនួនបើយើងអាច Installក៏អាច Uninstall បានដែរ គ្រាន់តែបន្ថែមពាក្យ **a/uninstall** នៅខាងចុង។

១០-៤-៩- ការគ្រប់គ្រង Server Core

User interface របស់ Sever Core មានដែនកំណត់ ដូច្នេះមានការលំបាកក្នុងការគ្រប់គ្រង Sever Core ក្នុង Instance Local ឬ Event Remote អំពី Terminal Services ។ ដូចដែលបានដឹងហើយថាការប្រើប្រាស់សុទ្ធតែប្រើ command-line ទាំងអស់ជាក់ស្តែងការគ្រប់គ្រង remote ដោយប្រើ MMC snap-in ក្នុង Local-workstation ឬពី Windows Server ដ៏ទៃទៀតលើកលែងតែTask Manager actual graphical application Server Core Notepad Edit text file។ ម៉្យាងទៀតអ្នកដំឡើងWindows Installer (MSI)-based package ផងដែរ ប៉ុន្តែ GUI (Graphic User Interface) មិនបានបង្ហាញនោះទេ ដូច្នេះអ្នកត្រូវធ្វើការបញ្ជាក់នូវលក្ខណៈពិសេសទៅគ្រប់ Parameter ដែលជាតម្រូវការក្នុងការដំឡើងរួចបញ្ជាក់ច្បាស់លាស់ពីការផ្លាស់ប្តូរ **/qb** ។

ឧទាហរណ៍ៈ

អ្នកមាន toolkits សម្រាប់ Windows Server 2008 ចំនួនបី package នៅក្នុង MSI ដែលហៅថា mgmtpack ស្ថិតក្នុង Drive **C:** នោះត្រូវ run command ដូចខាងក្រោមៈ

Msiexec /I c:\mgmtpack.msi /qb

➢ ដើម្បីបើកនូវ Control Panel ពីរនៅក្នុង Server Core សម្រាប់ផ្លាស់ប្តូរតំបន់ពេលវេលានិងកែសម្រួល International Applets។ ក្នុងតំបន់ពេលវេលាផ្តល់ឱ្យអ្នកនូវកាលបរិច្ឆេទ ម៉ោង។ នោះត្រូវ run command ដូចខាងក្រោមៈ

Control timedate.cpl

➢ ដើម្បីកែប្រែនូវទ្រង់ទ្រាយ International Applets ក្នុងនោះមានរូបបិយប័ណ្ណ តំបន់ ក្តារចុច ភាសា។ នោះត្រូវ run command ដូចខាងក្រោមៈ

Control intl.cpl

➢ អាចគ្រប់គ្រងក្នុងការដំឡើង Server Core ដោយការប្រើប្រាស់នូវ Windows Remote Shell ការប្រើប្រាស់ Windows Remote Shell គឺ run ដោយ command prompt remotely ដែលប្រហាក់ប្រហែលទៅនឹង UNIX ឬ Linux System។ វាមិនត្រូវបាន Enable ដោយ default នោះទេ ដូច្នេះជំហានដំបូងសម្រាប់ Enable ចំពោះ Windows Remote Shell នៅក្នុង Server ប្រើ command :

WinRM quickconfig

➢ អ្នកអាចភ្ជាប់ដោយប្រើ remote shell ពីកុំព្យូទ័រដទៃទៀតពីការ run **Winrs** command។

ឧទាហរណ៍

ដើម្បីភ្ជាប់ទៅកាន់ Server Core instance មួយដែលមានឈ្មោះ WINSRV-CORE ហើយបើកនូវ command prompt នោះត្រូវ run command ដូចខាងក្រោម:

Winrs -r:WINSRVCORE cmd

➢ **Winrs** ក៏ support ការបន្ថែមនូវភាពជាក់លាក់ដូចជា username និង password នៅពេលដែលធ្វើការតភ្ជាប់ទៅកាន់ remote server ហើយកែប្រែ environment variable ពេលដែលshell start។ tool នេះមានប្រយោជន៍ បើសិនជាអ្នកចង់ run command-line-based tool remotely ដោយមិនមានការ log in ជាមុនដើម្បីប្រើប្រាស់ Terminal Services។

ផ្នែកមួយនៃតួនាទីដែលមានភាពលំបាកក្នុង Server Core នោះគឺការគ្រប់គ្រងលើ hardware។ បើសិនជាអ្នកភ្ជាប់ Plug និង Play device ទៅកាន់ Server Core នោះ Driver វានឹង load ដោយស្វ័យប្រវត្ត តែទោះជាយ៉ាងណាក៏ដោយវាមិនមែនងាយស្រួលដើម្បីឱ្យវាស្គាល់ device នោះនិងត្រូវការ load នូវ driver បីទៀត។ អ្នកត្រូវចាត់ចែងឱ្យបានច្បាស់លាស់ ៖

ជាដំបូងអ្នកត្រូវ Copy driver files ទាំងនោះទៅដាក់ក្នុង Server។ បន្ទាប់មកអ្នកអាច load driver ដោយការប្រើ INF File ដែលបានមកពីការប្រើ driver **drvload** command ឧទាហរណ៍

អ្នកបាន Copy driver ទៅកាន់ C:\TEMP\NEWDRIVERS ហើយ INF file សម្រាប់ driver ហៅថា **oemsetup.inf** នោះត្រូវ run command ដូចខាងក្រោម:

C: >cd temp\newdrivers

Drvload oemsetup.inf

➢ ដើម្បីស្វែងរក(query)នូវ driver ដែលបានដំឡើងទាំងនោះនៅក្នុង Server អ្នកត្រូវប្រើ **SC** command (* មិនត្រូវមាន space នៅចន្លោះរវាងសញ្ញា = និងពាក្យ **driver** នោះទេ)។

Sc query type= driver

➢ SC command គឺជាផ្នែក history របស់ Windows Resource Kit ប៉ុន្តែវាជា Build-in command ហើយមិនត្រឹមតែអាចប្រើក្នុងការស្វែងរក device driver ប៉ុណ្ណោះទេ តែវាជា Service ផងដែរ។Command មួយនេះក៏អាចប្រើក្នុងការ Startup នៃ device ហើយ services មួយចំនួនដែលបាន disable ដោយស្វ័យប្រវត្តនិង event device ដែលបានលុបហើយនិងចំណោម service ដទៃទៀត។ ដើម្បីដឹងឱ្យច្បាស់ពី **SC** command ទាំងនេះនោះត្រូវ run command ដូចខាងក្រោម:

SC /?

ជំពូកទី១១

ការគ្រប់គ្រងលើ Active Directory

១១-១- ដើមកំណើតនិងការវិវត្តន៍នៃ ACTIVE DIRECTORY

នៅពេលដែល Microsoft ជួបប្រទះនូវវិបត្តិនៃការចូលទៅកាន់ទីផ្សារនៃសហគ្រាសផលិតផលកុំព្យូទ័រដែលមានលក្ខណៈ Backend នៅក្នុងពាក់កណ្តាលទសវត្ស១៩៩0s នៃក្រុមហ៊ុននេះត្រូវការផលិត ផលមួយដែលការរក្សាទុកទិន្នន័យមានលក្ខណៈកណ្តាលសម្រាប់អ្នកប្រើប្រាស់តាមគេហដ្ឋាន សហគមន៍និងកុំព្យូទ័រ account information សម្រាប់ Windows NT។

វាពិតជាមានភាពងាយស្រួលសម្រាប់គ្រប់គ្រងនិងមានការថ្លឹងថ្លែងបានល្អច្បាស់លាស់។ ចាប់ពីពេលមានគំនិតបែបនេះមកWindows NT domain model ដែលជា NetBios drivenដ៏សំបើម នេះតែមានតួនាទីធម្មតាហើយជា centralized authentication store។ ដូច្នោះ សហគ្រាសភាគច្រើនបានដាក់ចេញនូវផលិតផលនេះ ហើយពួកគេបានដឹងថាWindows NT model។ ទោះបីជាអាចថ្លឹងថ្លែងបានល្អដូចនៅលើ ក្រដាស់ក៏ដោយក៏វាបានក្លាយជាសុបិនដ៏អាក្រក់មួយដើម្បីកាន់កាប់ក្នុងជីវិតពិត។ គេអាចថ្លឹងថ្លែងបាននូវតម្រូវឱ្យមានភាពបត់បែនបាននេះគឺជាមូលហេតុនៃកង្វះខាត់នៃភាពអាចបត់បែនបានរបស់ NT domain ដែលជាលទ្ធផលនៃការបត់បែនជាបន្តបន្ទាប់របស់វាដែលមានកង្វះខាត់។

ក្នុង Windows NT domain មួយអ្នកប្រើប្រាស់ឬក្រុមនៃអ្នកប្រើប្រាស់និងកុំព្យូទ័រជាច្រើនត្រូវបានរក្សាទុកទាំងអស់មានលក្ខណៈដូចជាទម្រង់នៃផ្ទះល្វែងគ្មានវិធីណាផ្សេងដើម្បីបែងចែកតាមលំដាប់លំដោយឱ្យសមហេតុផលទៅតាមរចនាសម្ព័ន្ធគ្រប់គ្រងដទៃទៀតបានល្អជាងការរចនាសម្ព័ន្ធរបស់ក្រុម NT ឬក្នុងករណីខ្លះដែលមាន domain ច្រើន។ ការជំនួសអ្នកគ្រប់គ្រងទៅលើកុំព្យូទ័រ Users, groups គឺពិបាកក្នុងការសម្រេចចិត្ត។ ក្រុមហ៊ុនធំៗជាច្រើនមានការលំបាកក្នុងការកាន់កាប់ទៅលើចំនួនដ៏ច្រើនក្រុមនៃ NT របស់ពួកគេ។ ជាការពិតក្រុមហ៊ុនធំៗជាច្រើនពិបាកត្រួតត្រាទៅលើ Domain ច្រើនដោយសាតែមូលហេតុនយោបាយច្រើនជាងមូលហេតុបច្ចេកទេស(ឧទាហរណ៍ៈផ្នែកមួយនៃការគ្រប់គ្រងមិនទុកចិត្តឬមិនអនុញ្ញាតឱ្យផ្នែកដទៃទៀតធ្វើការចាត់ចែងទៅលើផ្នែកគណនីរបស់អ្នកប្រើប្រាស់បានទេ)។ បើទោះបីជាយើងខំប្រឹងប្រែនិយាយច្រើនដោយយកនូវគំនិតខ្លីៗស្តីអំពី Windows NT ក៏ដោយយើងនឹងឆ្ពោះទៅក្នុង Windows 2000 និង Active Directory ឱ្យបានលឿនក្នុងរយៈពេលដ៏ខ្លីដើម្បីអភិវឌ្ឍន៍ ។

នៅពេលដែលអ្នកបង្កើត Microsoft បានត្រលប់ទៅប្រើការគូលើក្តារវិញសម្រាប់ Windows 2000 ពួកគេបានដឹងថា NT domain model គឺមិនអាចជួយបំពេញតម្រូវការដើម្បីក្លាយជា Enterprice Directory Service ឡើយ។ អ្វីដែលនឹងកើតឡើងពីការអនុវត្តន៍នៃការអភិវឌ្ឍន៍ Active Directory ដែលកំណត់នូវចំនុចខ្សោយដែលមានក្នុង NT domain model ។ វាបានបង្កឱ្យភាពអាចពង្រីកបាន, ភាពងាយស្រួលនិងលក្ខណៈឋានានុក្រមដល់អ្នកគ្រប់គ្រង។ ភាគច្រើននៃពួកយើង ដែលមានភាពងាយស្រួលពីការប្រើប្រាស់ជា មួយនិង NT domain concept Active Directory បានអភិវឌ្ឍខ្លួនទៅមុខកាន់តែប្រសើរ។ ពិតណាស់ភាពអាចបត់បែនបាននិងការបង្កើននូវភាពអាចទុកចិត្តបានវាបានធ្វើឱ្យ Active Directory ជាជម្រើសដ៏ល្អបំផុតសសម្រាប់អ្នកប្រើប្រាស់។ Active Directory តម្រូវឱ្យ Windows Administrator ធ្វើការផ្លាស់ប្តូរទាំងស្រុងចំពោះការមិនយកចិត្តទុក ដាក់របស់ពួកគេទៅរបស់ថ្មីនេះ។ ជាងនេះទៅទៀតគ្រាន់តែចាប់ផ្តើមគិតទៅលើ domain ធម្មតានិងក្រុមដែលយើងគួររៀបចំផងដែរនូវការប្រើប្រាស់ domain *organizational unit (OUs)*។

ក្រុមនៃអង្គការមួយចំនួនយល់ព្រមសម្រាប់ការបែងចែកដ៏សមហេតុផលដើម្បីបង្កើតឱ្យមានភាពសមស្រប ទៅតាមរចនាសម្ព័ន្ធនៃការគ្រប់គ្រងរបស់អ្នកនិងដែនកំណត់របស់ Admin បានយ៉ាងជាក់លាក់។ ការបន្ថែមក្នុង គម្រោងឋានានុក្រមនេះគឺថាអ្នកអាចផ្លាស់ប្ដូរអ្នកគ្រប់គ្រងបានយ៉ាងល្អិតល្អន់ ដូច្នេះមិនមែនអ្នកគ្រប់គ្នាសុទ្ធតែអាច ជា domain administrator ដែលអាចធ្វើការគ្រប់គ្រងនៅក្នុងទម្រង់ផ្សេងៗនៃ directory បានឡើយ។ ជា ឧទាហរណ៍យើងអាចឱ្យបុគ្គលិកនៃផ្នែកធនធានមនុស្សចូលទៅកាន់គណនីព័ត៌មានរបស់អ្នកប្រើប្រាស់។ ដូច្នោះ ពួកគេអាច Update និងផ្លាស់ប្ដូរព័ត៌មានអ្នកប្រើប្រាស់ដូចជាអាសយដ្ឋាននិងព័ត៌មានផ្ទាល់ខ្លួនដោយយើងមិនបាន ផ្ដល់សិទ្ធិឱ្យពួកគេក្នុងការកែប្រែពត៌មានរបស់អ្នកក្នុង Window Group Member បែបនេះឡើយ ។

Active Directoryគឺជា Domain Name System (DNS), service ឯករាជ្យមិនដូចជា NT domain model នោះទេដែលភាគច្រើនជា NetBIOS driven។ ឋានានុក្រមនៃរចនាសម្ព័ន្ធរបស់ DNS ត្រូវបានផ្សព្វផ្សាយ ដោយប្រើប្រាស់ TCP/IPជាprimary network protocol នៅក្នុងការគ្រប់គ្រងជាច្រើនបានធ្វើ Active Directory ក្លាយជាជម្រើសដ៏ល្អបំផុតសម្រាប់ការគ្រប់គ្រងទៅលើ name resolution និង service location។ Active Directory មិនអាចកើតមានឡើងដោយគ្មានមុខងាររបស់ DNS service បានទេ។ ទោះបីជា Microsoft មិនបាន ផ្ដល់អនុសាសន៍ក្នុងការប្រើប្រាស់ DNS service របស់ខ្លួនវាផ្ទាល់ក៏ដោយ។ ក៏អ្នកមិនអាចទាញយកផលប្រយោជន៍ ពីការរួមផ្សំគ្នានៃលក្ខណៈពិសេសរបស់ DNS service ដែល Microsoft បានផ្ដល់ឱ្យបានទេ។ អ្នកអាចប្រើប្រាស់នូវ ជម្រើសផ្សេងទៀតដែលបានផ្ដល់ការគាំទ្រដល់ SRV records (ទោះបីជាយ៉ាងណាក៏ដោយយើងមិនអាចទទួល យកផលប្រយោជន៍នូវលក្ខណៈទាំងស្រុងដែ Microsoft's DNS Service បានផ្ដល់ឱ្យឡើយ)។ ជាមួយ Active Directory អ្នកក៏មិនត្រូវបានកំណត់នូវសិទ្ធិក្នុងការបង្កើតទំនាក់ទំនងទុកចិត្តរវាង domain និង domain នោះដែរ។ អ្នកដំឡើងនូវ domain trees ទាំងមូលហើយ domain និងត្រូវបានរួមបញ្ចូលគ្នាដើម្បីបង្កើតបានជា forests។ វា មានសារៈប្រយោជន៍នៅពេលដាក់បញ្ចូលទំនាក់ទំនងរវាងការគ្រប់គ្រងដែលមានលក្ខណៈដាច់ដោយឡែកពីគ្នាដូច ជារវាងដៃគូពាណិជ្ជកម្ម រឺកំឡុងពេលនៃការចូលរួមនិងការទទួលបានមកវិញ។

តាំងពីមានសកម្មភាពនេះ Active Directory បានទទួលនូវការផ្លាស់ប្ដូរយ៉ាងធំធេងនិងការរិះគន់ច្រើនពី សំណាក់អ្នកប្រើប្រាស់ចំពោះ Microsoft ដែលទទួលបានពីសហគមន៍អ្នកប្រើប្រាស់ Active Directory និងសេនារី យោនៃពិភពពិត។ ជាឧទាហរណ៍ Windows Server 2003 បានបន្ថែមនូវមុខងារថ្មីៗជាច្រើនដែលមានសារៈ សំខាន់សម្រាប់ Windows 2000 Active Director។ លើសពីនេះទៀតពួកគេបានបន្ថែមនូវមុខងារដែលសម ស្របសម្រាប់ការប្ដូរឈ្មោះថ្មីឱ្យ domain controllers ពួកគេបានបន្ថែមការប្រើ backup media, rename នូវ domainsទាំងមូលនិងកាត់បន្ថយនូវ network traffic ដោយ គ្រាន់តែធ្វើការផ្លាស់ប្ដូរការ replicate ទៅលើក្រុម ប៉ុណ្ណោះ ជាជាងផ្លាស់ប្ដូរទៅលើក្រុមទាំងមូលឱ្យសមាជិកក្រុមទាំងស្រុងដែលអ្នកប្រើប្រាស់អាចធ្វើការបន្ថែមនិង លុបចេញពីតារាងបាន។ Windows Server 2008 បានទៅឆ្ងាយមួយជំហានទៀតយើងនឹងសិក្សាបន្ថែមនូវលក្ខ ណៈទាំងអស់របស់វានូវក្នុងជំពូកនេះដូចដែលយើងបានដឹងហើយពីរបៀបដែល Windows Server 2008 នឹងត្រូវ ចូលរួមទៅក្នុងការរៀបចំរបស់យើង។

១១-២- ACTIVE DIRECTORY PRIMER

ឥឡូវនេះយើងនឹងសិក្សាសង្ខេបៗនូវប្រវត្តិរបស់ Active Directory យើងចង់ឱ្យអ្នកទាំងអស់គ្នាចំណាយ ពេលបន្តិចបន្តួច ដើម្បីសិក្សានូវគំនិតខ្លះៗដែលយើងទាំងអស់គ្នាបានសិក្សានៅលើទំព័រដែលស្ដីអំពី Windows Server 2008 ឱ្យកាន់តែច្បាស់ទៅលើ Active Directory។ ផ្នែកនេះបានឆ្លើយទៅនឹងសំនួរខាងក្រោមៈ

- What is Active Directory?

- How isActive Directory organized ?
- What role does Active Directory play in all this ?
- Whatare Domain function levels ?

បើយើងបានដឹងនូវចម្លើយនៃសំនួរទាំងអស់នេះ ហើយយើងអាចរំលងមួយផ្នែកនេះដោយធ្វើការសិក្សាបន្តទៅលើ Windows Server 2008 ប៉ុន្តែអ្នកអាចអានផ្នែកនេះនៅពេលក្រោយ។ ដើម្បីអាចធ្វើការដោះស្រាយបញ្ហាសម្រាប់ការគ្រប់គ្រង់លើ Active directory បានយើងត្រូវស្វែងយល់អំពីៈ

-ការបង្កើតDomain (Tree, forest, Trust)

-ការបង្កើតOU Object

-ការបង្កើតការJoin domain

-ការបង្កើតGroup និងUser

-ការដំឡើងDNS ជាដើម។

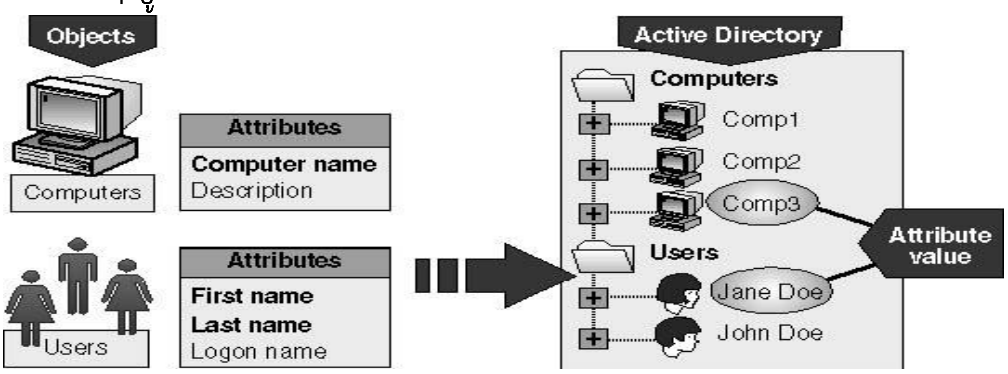
១១-២-១- តួនាទីរបស់ Active Directory

- ប្រើប្រាស់នូវ Container(Folder)ដែលតំណាងឱ្យដេប៉ាតឺម៉ង់ណាមួយរៀបចំព័ត៌មានតាមទម្រង់ជា Tree ដើម្បីបង្កើត Tree សម្រាប់ Object
- ផ្តល់នូវភាពងាយស្រួលចំពោះ Administrator សម្រាប់ការគ្រប់គ្រង់លើ Object ជាច្រើនស្ថិតក្នុងកម្រិតមួយ
- Object ទាំងអស់ត្រូវបានកំណត់ Attribute សម្រាប់ពិពណ៌នាអំពី Object
- ផ្ទេរសិទ្ធិរបស់ Administrator និង Task ចំពោះUser ម្នាក់ៗនិងGroup ដើម្បីប្រើប្រាស់ Resource

១០-២-២- លក្ខណៈពិសេសរបស់ Active Directory

- ផ្តល់នូវ Open Application programming interface (OAPI)
- Domain ជាច្រើនបង្កើតបានជាDomain Tree
- Root Domain ក្លាយជា Parent របស់Child Domain
- បានAdd Internet និងIntranet Environment។

Active Directory បានប្រើប្រាស់នូវ Object តំណាងឱ្យ Network Resource ដូចជាៈDomain, forest , OU , User, Group, កុំព្យូទ័រ, Device, share folder ,printer ,site ,subnet។



Active Directory ត្រូវបានរៀបតាមរចនាសម្ព័ន្ធ២យ៉ាងគឺ Physical Structure និង Logical Structure។

- Logical Structure

Logical Structure គឺរាល់ Object ដែលស្ថិតក្នុង Active Directory ដែលជា node ស្ថិតនៅលើ Tree មួយ ហើយ Logical Structure បានបង្ហាញអំពី Domain, Organization Units (OU), Domain tree និង Domain Forest ។

- **Domain Tree**

Tree ជាបណ្តុំនៃDomain មួយរឺច្រើនដែលកើតឡើពី Role តែមួយមានន័យថាចែកចាយ ឈ្មោះ Namespace តែមួយ ដោយមានការចូលរួមពី Parent domain (Root Doman) និង Child domain (Sub domain , Secondary domain or Nested domain)។

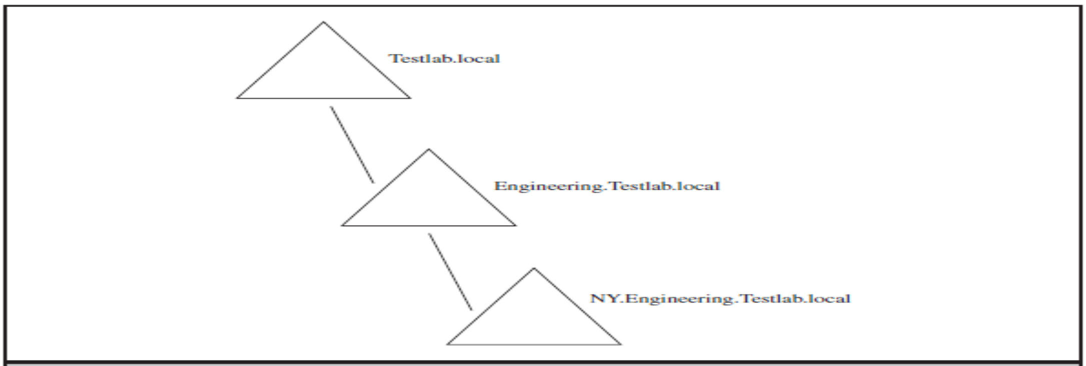


Figure 4-1. A domain tree

រូបភាព 4-1 បង្ហាញនូវ Domain Tree មួយ

Testlab.local គឺជាRoot Domain ហើយចំពោះ Engineering.Testlab.local និង NY. Engineering.Testlab.local គឺជា Child Domain។

- **Domain Forest**

Forestគឺជាការភ្ជាប់រវាង Domain tree ផ្សំជាមួយគ្នាចាប់ពី២ឡើងទៅមានន័យថាចែកចាយព័ត៌មាន Directory Information រួម។ ហើយរាល់ Domain ទាំងអស់ស្ថិតក្នុង Forest ចូលរួមជា Common Schema និង Global Catalog។ Domain ដែលស្ថិតក្នុង Forest វាមិនពឹងផ្អែកលើគេឡើយ។

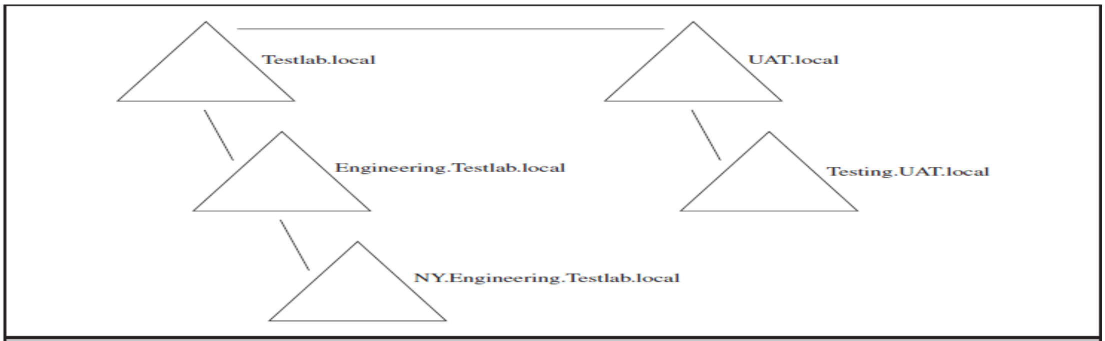


Figure 4-2. An Active Directory forest

រូបភាព៤-២បង្ហាយថាមានDomain ចំនួនពីរ

Testlab.local និង UAT.local ដែលស្ថិតនៅក្នុង Domain ខុសគ្នាហើយ Domain មាន Child Domain របស់វាទាំងពីរអាចចែកចាយ Resource ជាមួយគ្នាទៅវិញទៅមក។

- **Trusts**

Trust គឺជាការភ្ជាប់ទំនាក់ទំនង់រវាង Domain ដែល link ចូលគ្នាជាមួយ Tree មួយ រឺច្រើនដើម្បីបង្កើតជា Forest មួយ។ ដោយDefault នៅក្នុង Domain Tree វាមានទំនាក់ទំនង់រវាង Domain ទាំងអស់ជាស្វ័យប្រវត្តពេលដែលមានChild Domain ត្រូវបានបង្កើតគេហៅថា two way transitive trust ដែលជាទំនាក់ទំនង់តាមទិសដៅពីរមានលក្ខណ:ឆ្លង។

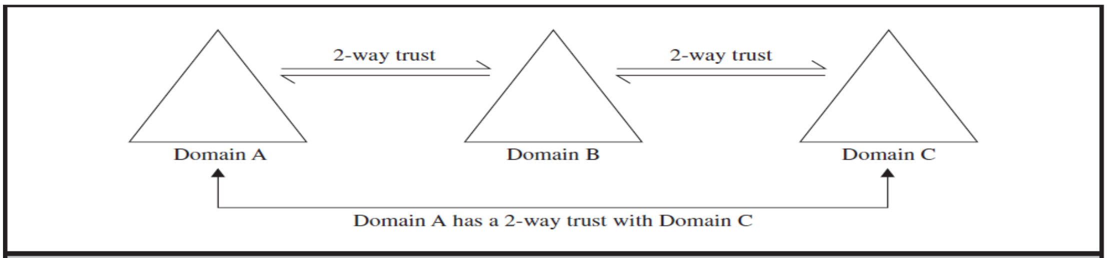


Figure 4-3. A two-way transitive trust

រូបភាព៤-៣ បង្ហាញពីទំនាក់ទំនងពីរដែលមានលក្ខណ:ឆ្លងជាមួយ Domain A និង Domain C

គេបានបង្កើតទំនាក់ទំនងរវាង Domain និង Domain ក្នុងគោលបំណងដើម្បីឱ្យUser ដែលនៅក្នុង Domain ទាំងអស់អាចប្រើប្រាស់នូវ Resource ពីគ្នាទៅវិញទៅមក។

- **Organization Units (OU)**

- OUគឺជា Container មួយដែលត្រូវបានប្រើប្រាស់សម្រាប់ការចែកនូវរាល់ Object ទាំង ឡាយនៅក្នុង AD ទៅជាផ្នែកតូចៗ ដើម្បីផ្តល់នូវភាពងាយស្រួលឱ្យ Administrator ក្នុងការគ្រប់គ្រង់លើ Object ទាំងនោះ។

- OU អាចផ្ទុកទៅដោយ User Account, Group, កុំព្យូទ័រ, Printers និងOU ដែលកើតចេញពី Domain តែមួយ។

- OU មានតែមួយគត់រាល់ពេលដែល Domain Controller របស់ OU ត្រូវបានបង្កើតជាស្វ័យប្រវត្តដោយនៅពេលដែលAD សម្រាប់ Domain ថ្មីមួយត្រូវបានបង្កើតឡើង។

- អាចផ្ទេរសិទ្ធិដែលបាបកំណត់ឱ្យ OUនិង Object ក្នុង Containers
- ងាយស្រួលកំណត់គោលការណ៍សម្រាប់ Application។

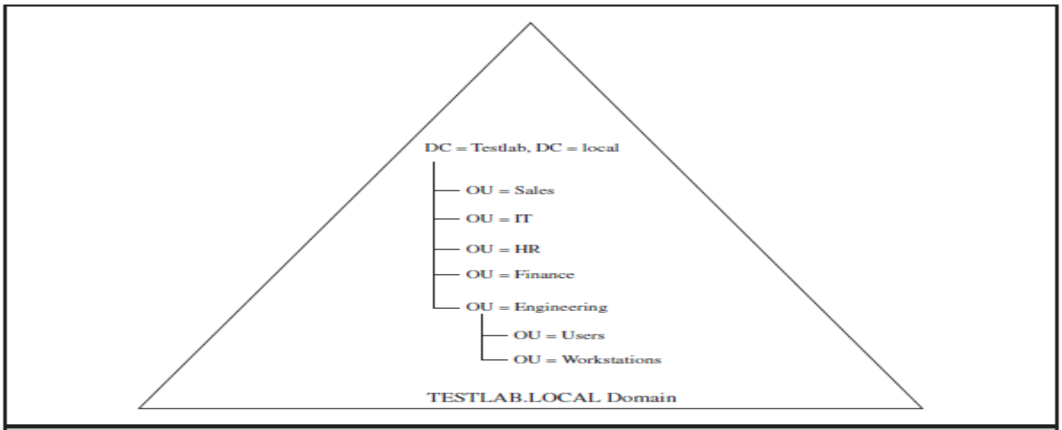


Figure 4-4. A domain split up into OUs

រូបភាព៤-៤ បង្ហាញថា Domain Testlab.local ត្រូវបានចែកDomain មួយទៅជាច្រើនផ្នែកដូចជា Sales,IT,HR,Finance,និងEngineering ដែលនៅក្នុងនោះមាន User និង Workstation

ដូចនេះគេប្រើប្រាស់សម្រាប់ Group Policy និង Delegate Security។ Group Policy បានកំណត់ឱ្យ OU ណាមួយប្រើបានតែ Application មួយនោះប៉ុណ្ណោះ។ រីឯ Delegate Security ផ្តល់នូវការបែងចែកតួនាទីឱ្យ OU ណាមួយអាចធ្វើកិច្ចការបានដូចជាការផ្លាស់ប្តូរ Password ជាដើម។

- **Physical Structure**

Physical Structure មានន័យថារាល់ AD ត្រូវបានរក្សាទុកក្នុង Domain Controllerនីមួយៗដែលជាសំនុំនៃ Binary file តំណាងឱ្យ Database មួយ ហើយ Physical Structure បានបង្ហាញពី Sites, Subnet

Sites:ត្រូវបានប្រើប្រាស់សម្រាប់ដំឡើងDirectory Access និងការឆ្លើយតប។

Subnet:ក្រុមនៃប្រពន្ធ័Network Group ជាមួយនឹងលក្ខណៈពិសេស IP address និងNetwork Mask

- **Active Directory Sites**

នៅពេលដែលយើងមានគម្រោងប្រើប្រាស់ AD យើងត្រូវតែគិតអំពីចំនួនដែលត្រូវការអំពីរចនាសម្ព័ន្ធនៃចំនួន Domain controller និងទីតាំងសម្រាប់ Server និងចំនួននៃការបែកចែក OU ដែលត្រូវបង្កើត។

- **Application Data Partitions**

Active Directory processes ដោយស្វ័យប្រវត្តតាមលទ្ធភាពនៃការចម្លងទិន្នន័យជាលក្ខណៈ Enterprise logical ។ យើងអាចបង្កើតនូវ application data ជាផ្នែកៗនៅក្នុងActive Directory របស់យើងដើម្បីរក្សាទុកនូវទិន្នន័យសម្រាប់application របស់យើង។ នេះអាស្រ័យទៅលើអ្នកបង្កើតនិងអ្នកប្រើប្រាស់ appli-cation ដែលធ្វើការរក្សា data ក្នុង Active Directory និងកំលាំងអនុភាពដែលភ្ជាប់មកជាមួយនូវសមត្ថភាពដែលជាការឆ្លើយតប។

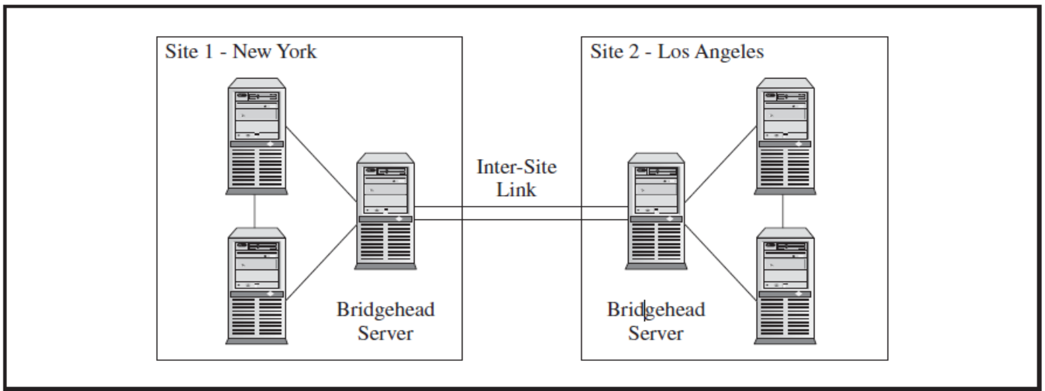


Figure 4-5. A simple multisite domain

- **Flexible Single Master Operation Rules (FSMO)**

Server នីមួយៗដែលមាននៅក្នុង Active Directory domain អាចជា Domain Controller រឺ member server។

- Domain Controller គឺ Domain មួយដែលជា AD ហើយរក្សាទុកនូវព័ត៌មាននៃការ Copy របស់ AD ដូចជាការបិទ account វានឹងធ្វើការ Update ភ្លាមៗហើយទទួលខុសត្រូវចំពោះ Authentication (ការផ្ទៀងផ្ទាត់User និង Password) របស់ User និងកុំព្យូទ័រ ។ រីឯ Member Server វិញវាចូលរួមក្នុង Domain ហើយអាចដើរតួនាទីផ្តល់នូវ Service មួយចំនួនដូចជា File Server ជាដើម។

- **FSMO role**

- **Schema Master:**ត្រូវបានប្រើប្រាស់ដើម្បីរក្សាទុកនិងគ្រប់គ្រងអ្វីដែលបានផ្លាស់ប្តូរក្នុង AD ហើយ Domain controller ដំបូងគឺជា Schema Master។
- **Domain Naming Master:**ត្រូវបានប្រើប្រាស់គ្រប់គ្រង់លើ Domain ដែលបាន Create, Add, Delete ចេញពីForest ទាំងមូល។
- **Relative ID (RID) Master:**ត្រូវបានប្រើប្រាស់ធានាថាគ្រប់ Security principles ដែលត្រូវបានប្រើប្រាស់ដោយAD តែមួយ។
- **Primary Domain controller (PDC) Emulator:** ត្រូវបានប្រើប្រាស់ដើម្បីធ្វើឱ្យ Time នៅក្នុង Domain ដូចគ្នានិងសម្រាប់គ្រប់គ្រង់លើ Account logon និង password synchronization។
- **Infrastructure Master:** ត្រូវបានប្រើប្រាស់ដើម្បីគ្រប់គ្រង់លើ Group Member។ ហើយធានាថា Object ស្ថិតក្នុង Domain ផ្សេងៗត្រូវបានUpdate។

➢ ការប្រើប្រាស់Active Directory and DNS

នៅក្នុង AD ប្រើប្រាស់ DNS ដែលជាស្តង់ដារ Internet Service ដើម្បីកំណត់ពី Domain Controller ព្រមទាំងកំណត់ពី FSMO role ដូចជា Global Catalog server និងPDC emulator។ DNS គឺជាវិធីសាស្ត្រនៃការបកប្រែពី Domain name ទៅ IP address និងពី IP address មកកាន់ Domain វិញ។ DNS អាចប្រើប្រាស់ Domain name មួយដែលជំនួសឱ្យការប្រើប្រាស់ IP address នៅលើAD ព្រមទាំងជួយការពារ Dynamic Update ដើម្បីឱ្យកុំព្យូទ័ររបស់អ្នកអាចចុះបញ្ជីនូវ IP address ដោយស្វ័យប្រវត្តជាមួយ DNS Server ដោយមិនចាំបាច់ចាត់ចែងពី Administrator។

➢ កម្រិតតួនាទីនៃ Domain and Forest

AD នៅក្នុងWindow Sever 2008 អាចដំណើរការក្នុងកម្រិតមួយក្នុងចំណោម Domain Functional ទាំង៥ ហើយលក្ខណៈពិសេសទាំងអស់នេះសម្រាប់បង្កើនកម្រិតតួនាទីរបស់ AD បន្ថែម។

- **Domain Levels**
  - Window 2000 mixed
  - Window 2000 Native
  - Window Server 2003 Interim
  - Window Server 2003
  - Window Server 2008
- **Forest Levels**
  - Window 2000
  - Window Server 2003
  - Window Server 2003 Interim
  - Window Server 2008

➢ Install Option for Active Directory Domain Server

នៅពេលដែល Install AD នៅលើ Window server 2008 យើងអាចជ្រើសរើស Option មួយចំនួនដែលអាស្រ័យលើតម្រូវការរបស់ប្រព័ន្ធ network ដូចខាងក្រោម៖

➤ New window server 2008 domain in a new window server 2008 forest (ជាការ Install នូវ Domain controller ថ្មីដំបូងគេបង្អស់នៅលើWindow server 2008)

- New window server 2008 domain in an existing window server 2000/2003 forest
- (ជាការ Installនូវ domain controller ថ្មីមួយទៀតដោ Upgrade ពី window server 2000 /2003 forest ដែលមានរួចជាស្រេច)
- New window server 2008 domain controller in an existing windows 2000/2003 domain (ជាការ Installនូវ Child domain ដែលមានParent domain រួចជាស្រេច ដោយ Upgrade ពី window server 2000 /2003 forest)
- New window server 2008 domain controller in an existing window 2000/ 20003 /20008 domain form restored backup media (ជាការ Install Additional domain controller មួយទៀតសម្រាប់ការធ្វើ Backup ទៅកាន់ Primary domain controller)

- **Active Directory Requirements**

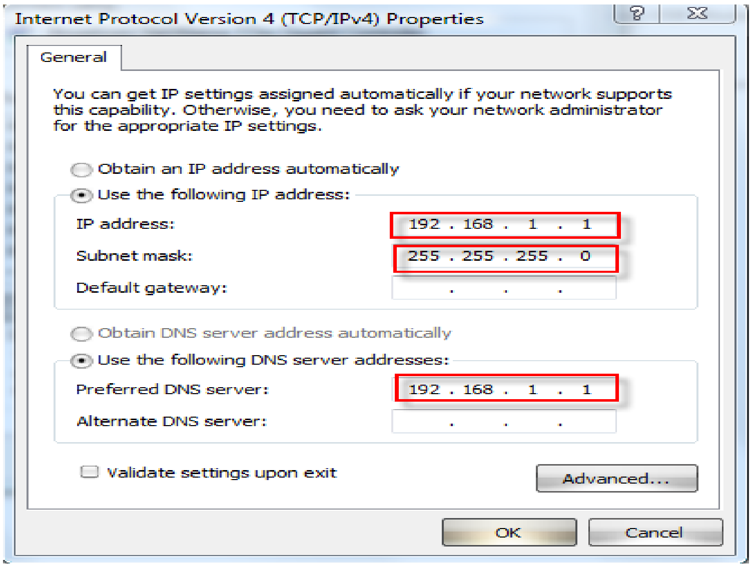
ដើម្បីអាចធ្វើការ Install AD បាន ជាដំបូងយើងត្រូវត្រួតពិនិត្យលើតម្រូវការនៃការ Install AD។ AD គឺជា Service មួយដែលសំខាន់បំផុតសម្រាប់ការគ្រប់គ្រង់លើប្រព័ន្ធ Network ដូច្នេះហើយប្រសិនបើមិនបានបំពេញតាមតម្រូវការនោះយើងមិនអាច Install Active Directory Service នេះបានឡើយ។

ដូចមុនពេលធ្វើការ Install Windows Server 2008 Active Directory យើងត្រូវការល័ក្ខខណ្ឌដូចជា៖

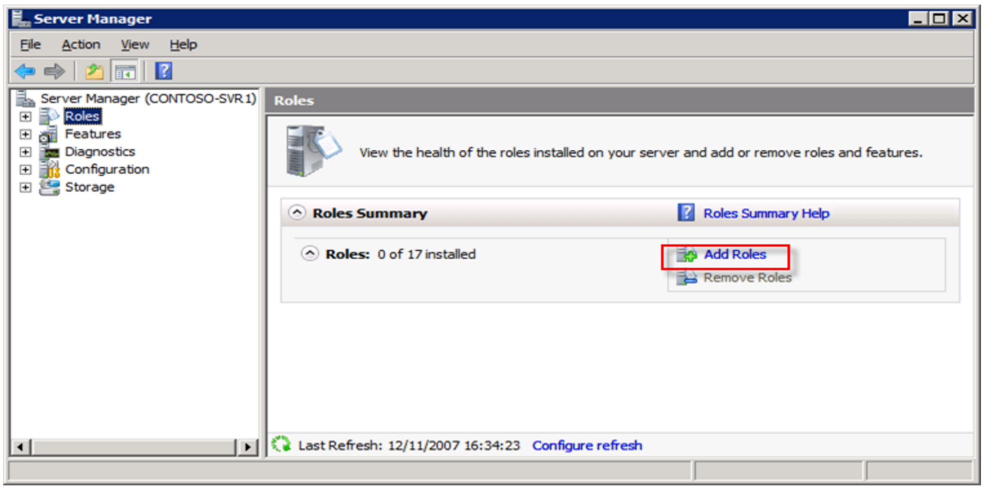
- ត្រូវធានាថាម៉ាស៊ីនServer កំពុងដំណើរការជាមួយ Windows Server 2008 operating System
- ត្រូវធានាថាTCP/IP និង DNS Server address ត្រូវបាន configure រួចរាល់។ បើនេះជាលើកដំបូងនៃ domain controller និង DNS Server ការដំឡើងនូវដំណើរការនឹងបានដំណើរការដោយស្វ័យប្រវត្តនិង Update primary DNS ទៅកាន់ DNS របស់យើង។
- Run Command Adprep /Forestprep សម្រាប់ការ Update (ប្រសិនបើបាន Add Server នេះទៅក្នុង Window 2000 រឺក៏ Windows Server 2008 forest យើងត្រូវតែធ្វើការ Update schema ជាលើកដំបូង)។
- Run Command Adprep /Domainprep /Gpprep សម្រាប់ការ Update (ប្រសិនបើបាន Add Server នេះទៅក្នុង Window 2000 រឺក៏ Window Server 2003 Domain)។
- Run Command Adprep /Rodcprep សម្រាប់ការដំឡើងForest (ប្រសិនបើInstall read only domain controller(RODC))។
- ត្រូវការ Install DNS(ប្រសិនបើមិនទាន់បាន Install នោះអាច Install ជាមួយ Active Directory)
- ត្រូវតែមាន Partition ជា ប្រភេទ NTFS សម្រាប់ការរក្សាទុកនៅក្នុង Sysvol folder ។

ជាដំបូងចំពោះការ Install AD domain service ថ្មីមួយត្រូវការ Install DNS ជាមុនសិនដើម្បី DNS និង AD ត្រូវបាន configured យ៉ាងសមរម្យ។ ហើយត្រូវធានាថាបាន IP address ដែលបានកំណត់ឱ្យសម្រាប់ Server ជា Static។ DNS និង AD domain controller ត្រូវតែមាននូវ Static address ដើម្បីធានាថា client អាចកំណត់ពី Server ដោយជឿជាក់។

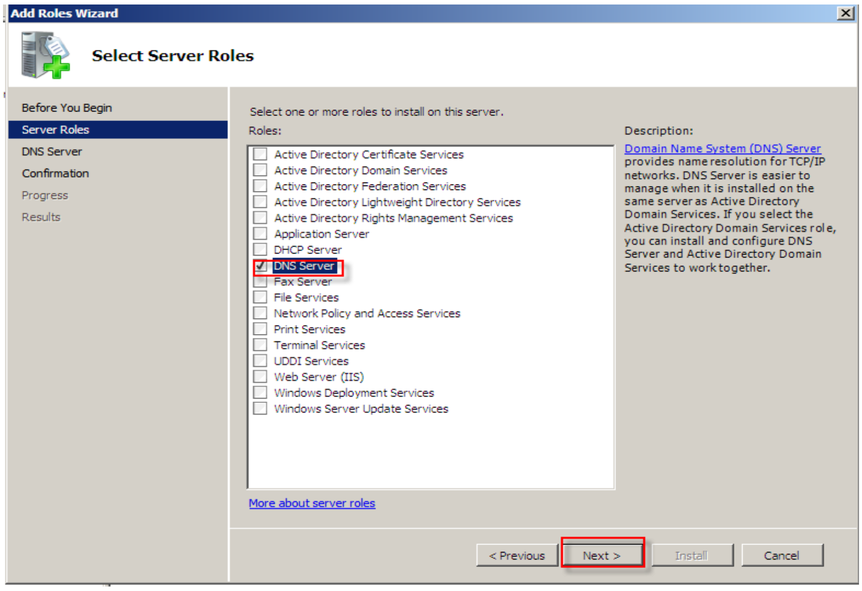
Install DNS ចូលទៅកាន់ TCP/IPv4 → ចុច **Properties→** កំណត់ **IP address**



1. ចុច Start → ចុចAdministrative tools → ចុច Server Manager
2. ចុច Roles
3. ចុច Add Roles

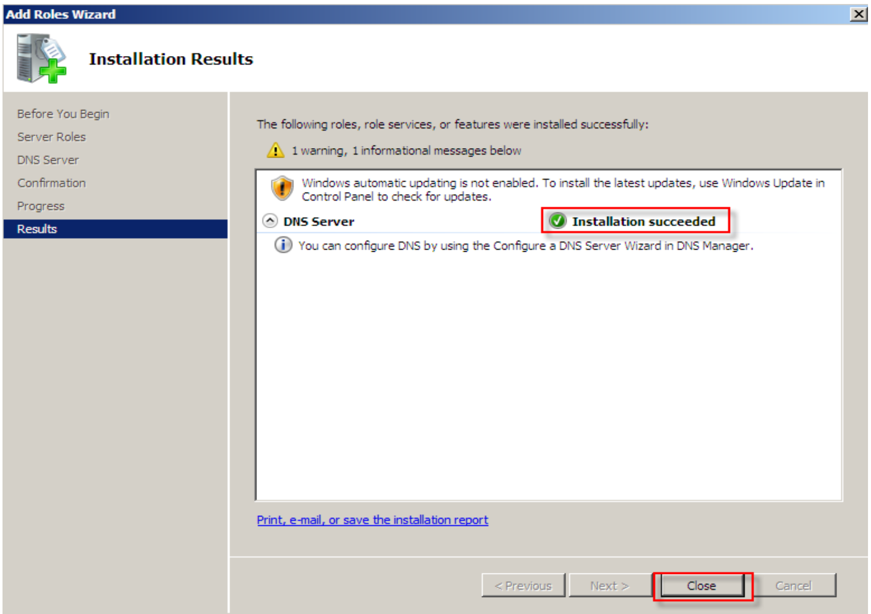


4. លើSelect Server Roles page →check DNS Server → ចុច Next



5. នៅលើ Confirm installation selection → ចុច Install

6. ចុច Finish



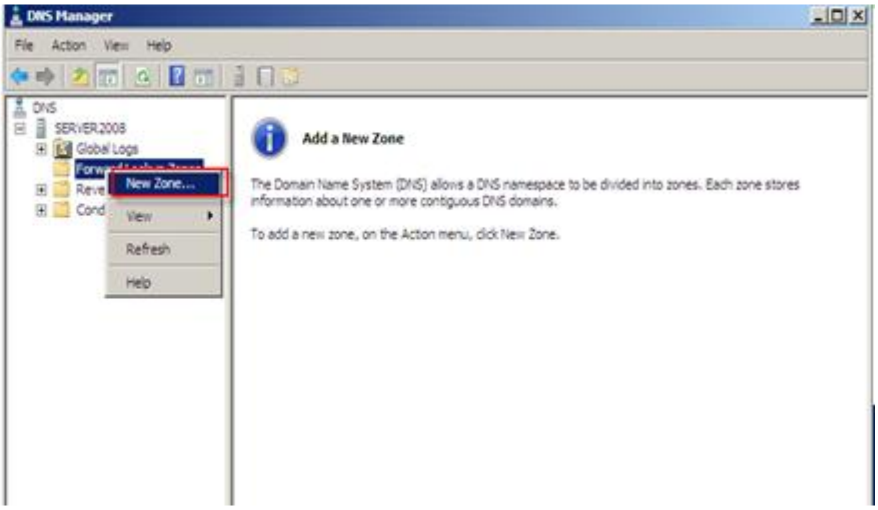
7- ចុចលើ Close

១១-៣- បង្កើត Forward និង Reverse Lookup Zone DNS

Note ប្រសិនបើយើងធ្វើ forward and reverse lookup zone មិនអាចដំណើរការនោះ យើងក៏មិនអាចធ្វើ AD ដំណើរការបានដែរ។

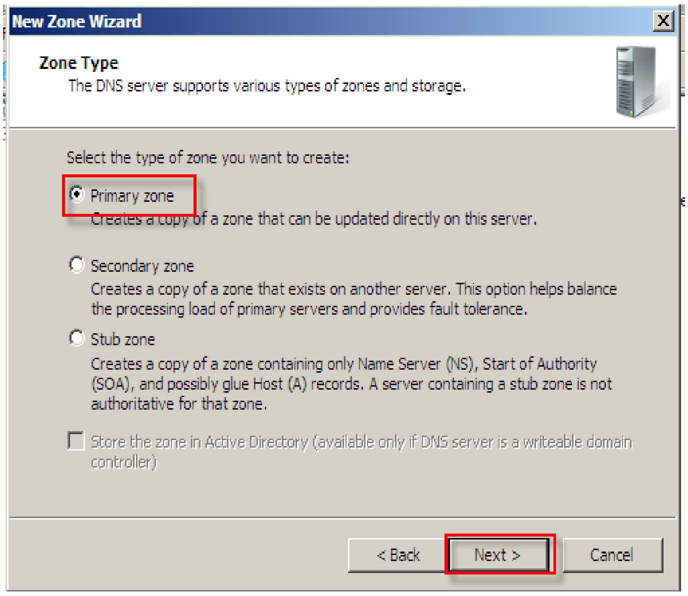
• បង្កើត Forward Lookup zone

1. ចុចmouse ស្តាំលើ Forward lookup zone→**New Zone**

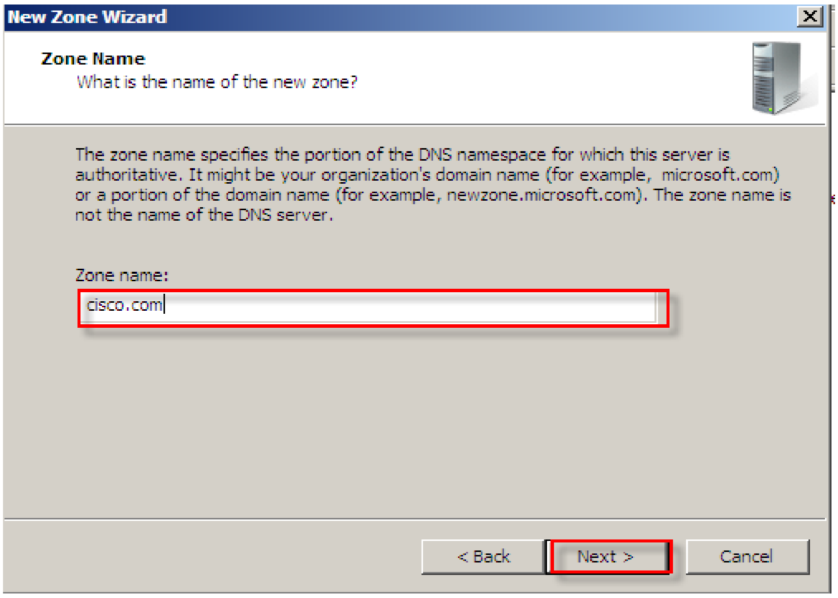


2. ចុចលើ Next

3. នៅលើ Zone Type choose Primary Zone→ ចុច Next



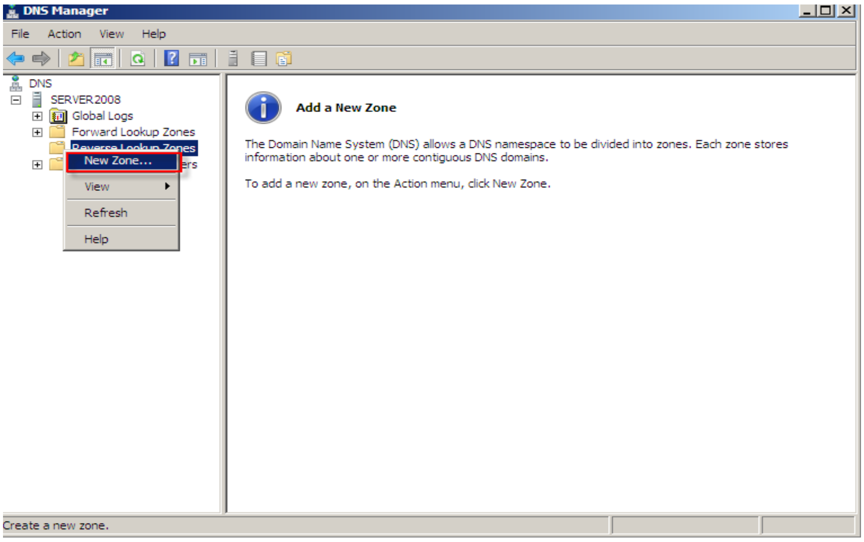
4. នៅលើ Zone Name → វាយឈ្មោះរបស់ zone → ចុច next



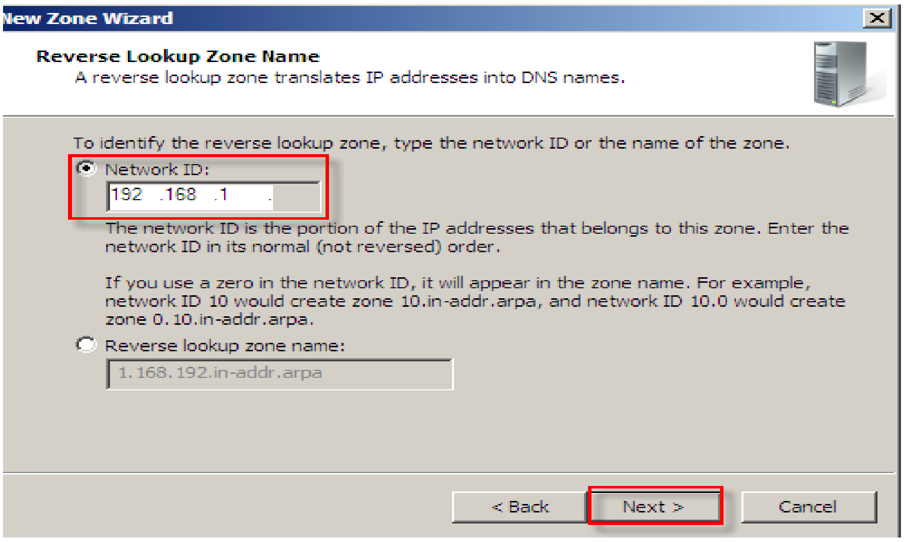
5. នៅលើ zone File → ចុច Create a new file with this file name→ ចុចលើNext
6. នៅលើ Dynamic update → ចុច Next
7. ចុច Finish

បង្កើត Reversed Lookup Zone

1. ចុចmouse ស្តាំ លើ revered lookup zone →New zone



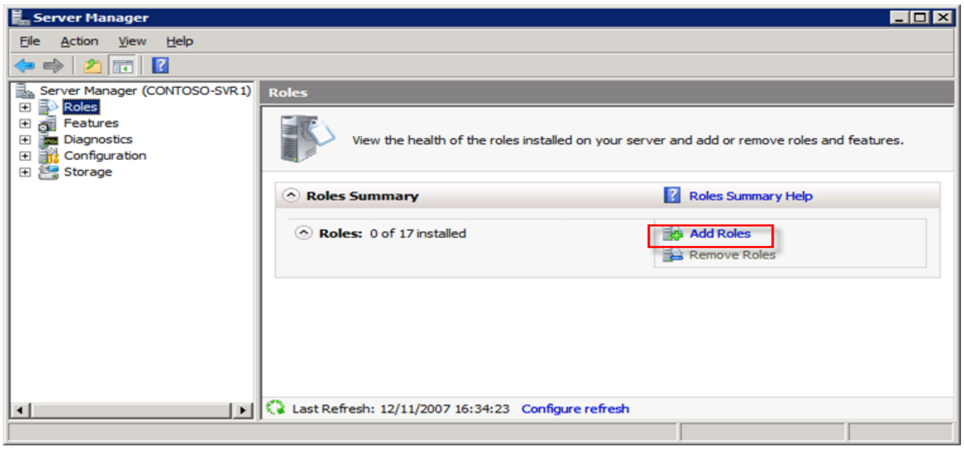
2. ចុច Next
3. នៅលើ Zone type → ចុច Primary zone → ចុច Next
4. នៅលើ Reverse lookup zone name→ ចុច ipv4Reverse lookup zone→ ចុច Next
5. នៅលើ Reverser lookup zone name →Set network ID → ចុច Next



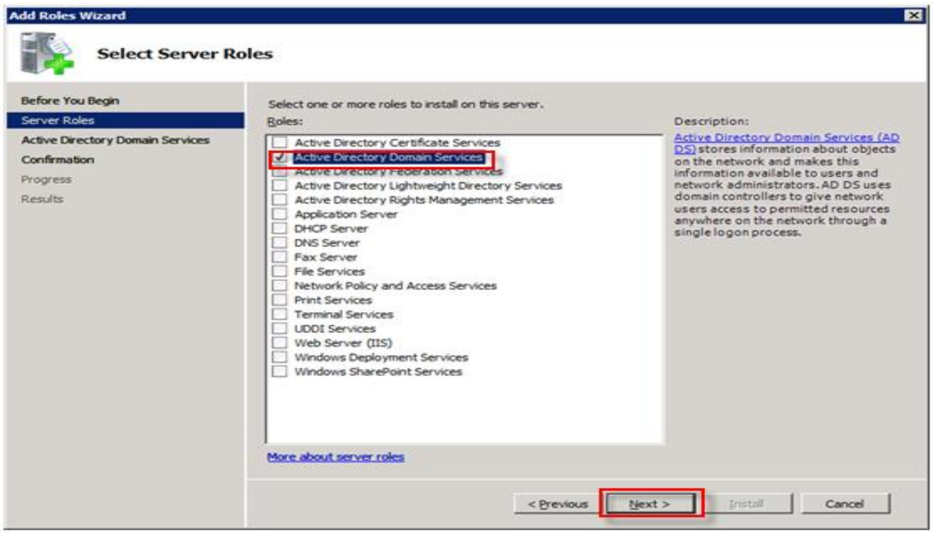
6. នៅលើ zone file→ ចុច Create a new file with this file name → ចុច Next
7. នៅលើ Dynamic update → ចុច Do not allow dynamic update → ចុច Next
8. ចុច Finish

Install AD DS as a new Primary domain Controller

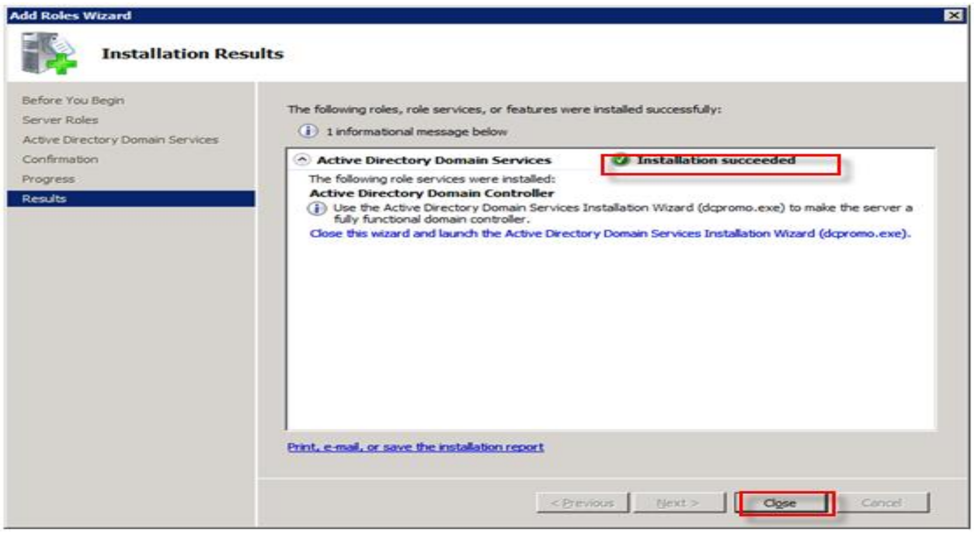
1. ចុច **Start** → ចុច **Administrative tools** → ចុច **Server Manager**
2. ចុច **Roles**
3. ចុច **Add Roles**



4. នៅលើ the **Before You Begin** page → ចុច **next**
5. នៅលើ the Select Server Roles page →ចុច Active **Directory Domain Services** → ចុច **Next**

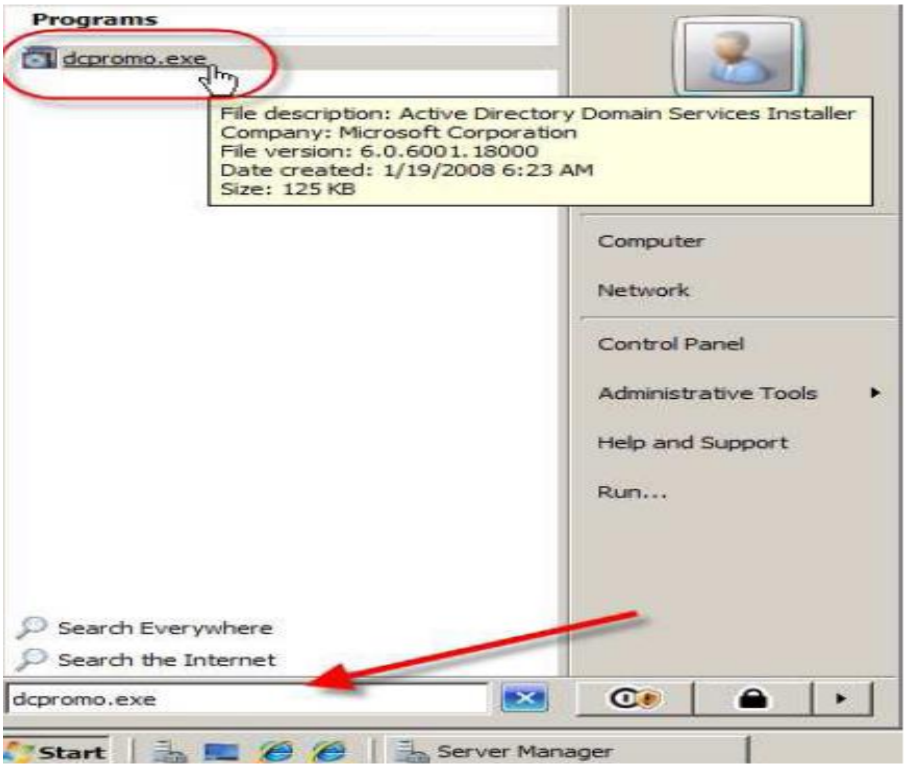


6. នៅលើ the **Active Directory Domain Services** → ចុច **Next**
7. នៅលើ the **Confirm Installation Selections** → ចុច **Install**
8. បន្ទាប់ AD DS installation បានបញ្ចប់ លើ the **Installation Results** page→ ចុច **close**



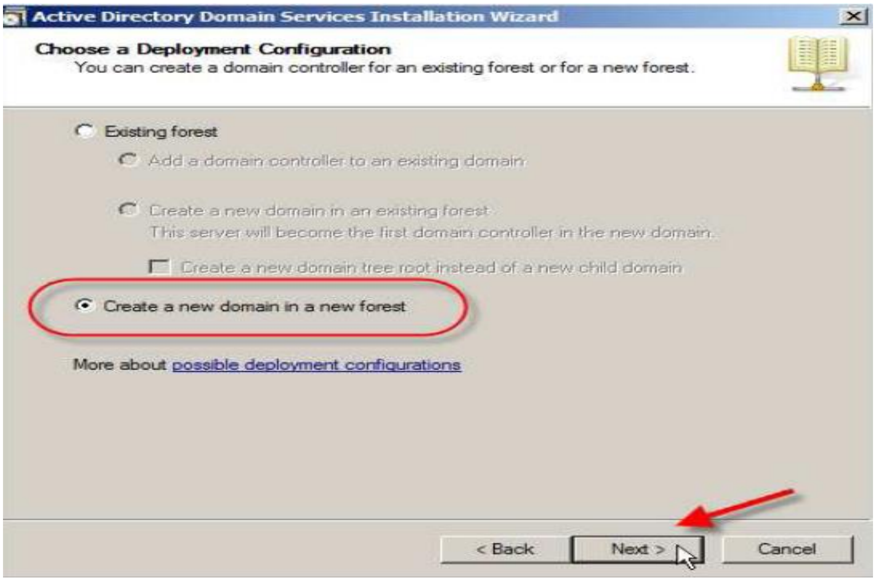
9. Run →**dcpromo.exe** (ដើម្បីPromote ក្លាយជាdomain controller)

ឬ→Server manager →ជ្រើស Active directory domain →run Active directory domain server installation

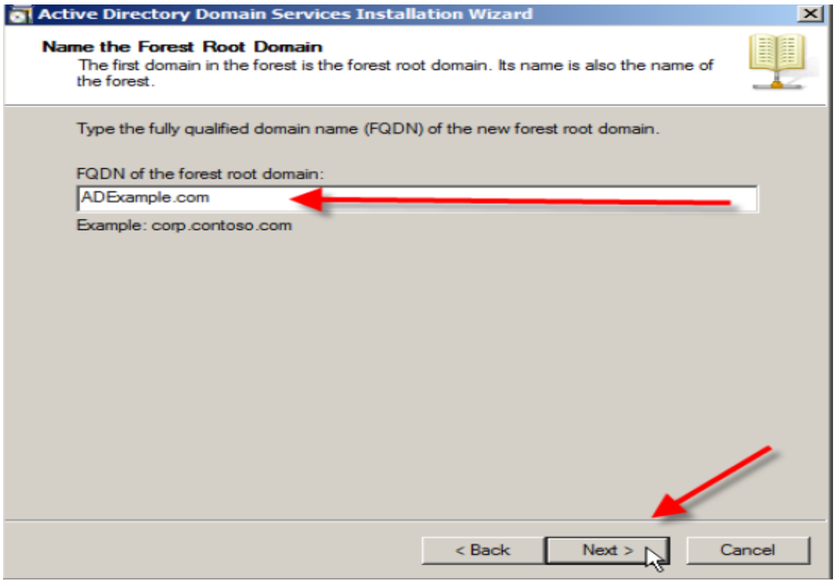


10. លើ the **Welcome to the Active Directory Domain Services Installation Wizard** page→ ចុច **next**

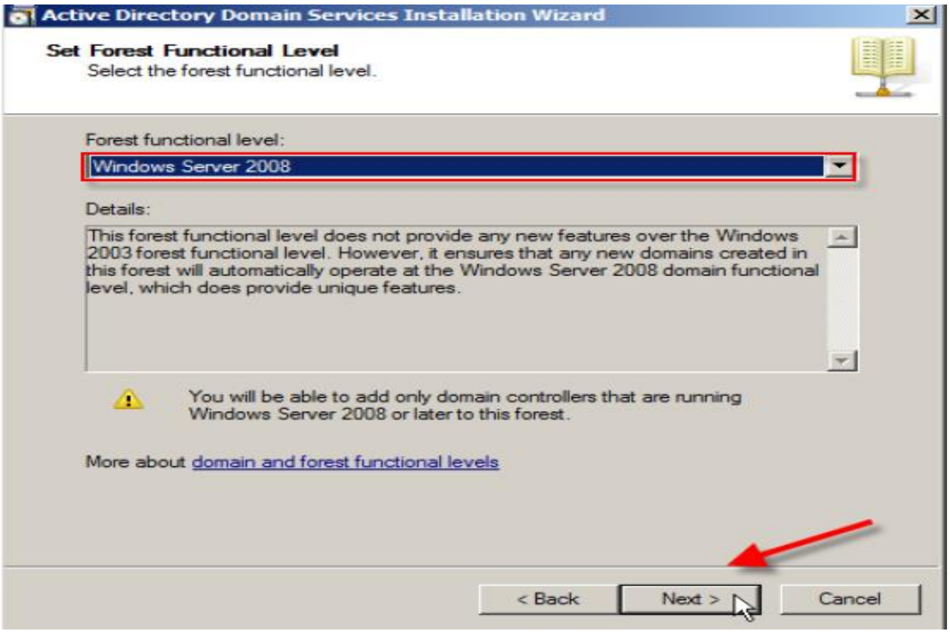
11. នៅលើ **Choose a Deployment Configuration** page→ ចុច **create a new domain in a new forest** (បង្កើតDomain controller ថ្មីដំបូងគេបង្អស់) → ចុច **next** (ប្រសិនបើជ្រើសរើសយកពាក្យ Existing forest មានន័យថាយក Server ជាBack up ទៅកាន់Primary domain)



11. នៅលើ the **Name the Forest Root Domain** page →វាយ the full DNS name (ADExample.com) for the new domain→ ចុច **next.**



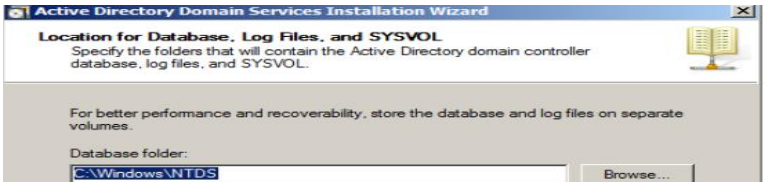
12. នៅលើ Set Forest Functional Level (ដើម្បីបង្កើនកម្រិតតួនាទីរបស់AD) page→select Windows Server 2008→ ចុច next.



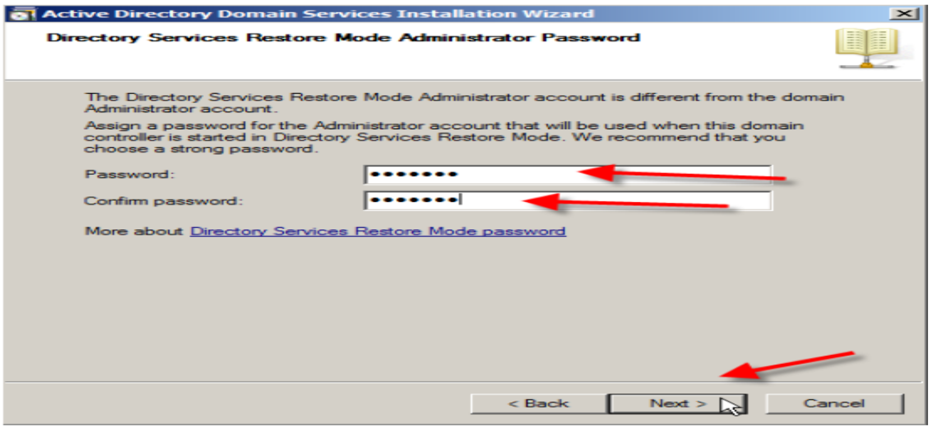
13. នៅលើ Additional Domain Controller Options page→ត្រូវប្រាកដថាDNSត្រូវបាន install រួចហើយ→ ចុច next

14. ចុច yes

15. ចុច install



16. នៅលើ **Directory Services Restore Mode Administrator Password (ជាPassword សម្រាប់ការ Restore នូវ Directory)** → វាយpasswordដើម្បីlog ទៅកាន់ serverនៅក្នុងDirectory Services Restore Mode →confirm the password→ ចុច **Next**



17. ចុច next ដើម្បីinstall

18. បន្ទាប់ពីការរង់ចាំinstall បានបញ្ចប់ →ចុច **restart** ដើម្បីបញ្ចប់

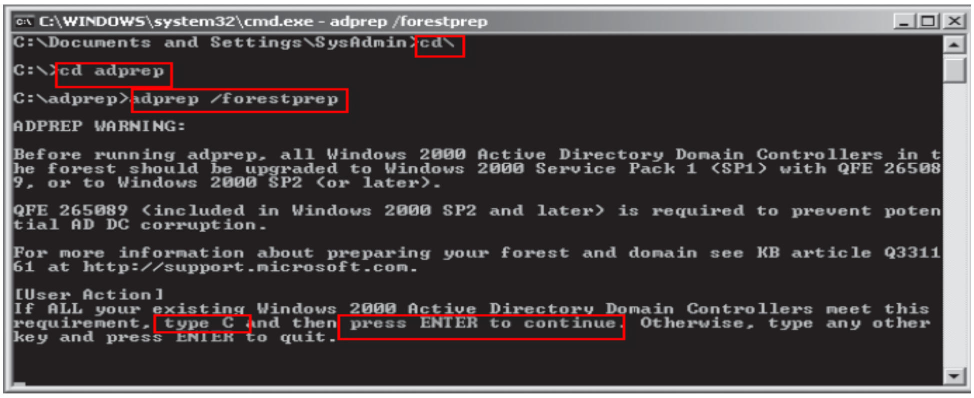
- Install Domain in an existing window 2000/2003 forest

វាគឺជាការ Install នូវ domain controller ថ្មីមួយនៅលើ window server 2008 ទៀតដែលជា forest មានន័យថា upgrade ពីwindow 2000/2003 forest ដែលមានរួចជាស្រាច ។

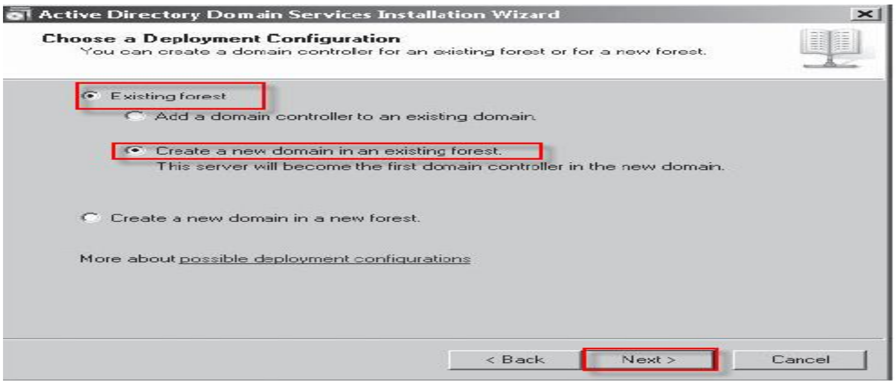
ដើម្បីអាច Install បានជាដំបូងយើងត្រូវតែមានWindow server 2003 forest មួយ ហើយត្រូវតែមាន username និង password ដែលជា Member មួយ នៃ Enterprise administrator, Schema Administrator និង domain administrator ក្នុងគោលបំណង់ដើម្បីបញ្ចូល window server 2008 ទៅចូលរួមក្នុង domain របស់ window server 2003 forest ។

1. Log ទៅកាន់ server ដែលមានWindow 2003 forest ដែលដើរតួនាទីជាSchema Master
2. Copy the\Sources\adprep folder ពីwindow server 2008 →**Local Driver on Schema Master**
3. ចូលទៅកាន់ **command prompt** ផ្លាស់ប្តូរទៅកាន់ **directory** នៅកន្លែងដែលបាន **Copy** ដាក់ក្នុង **adprep folder** → **run** →**adprep /forestprep**
4. Adprep នឹងបង្ហាញពី warning ដែលwindow 2000 AD domain controller ត្រូវបាន

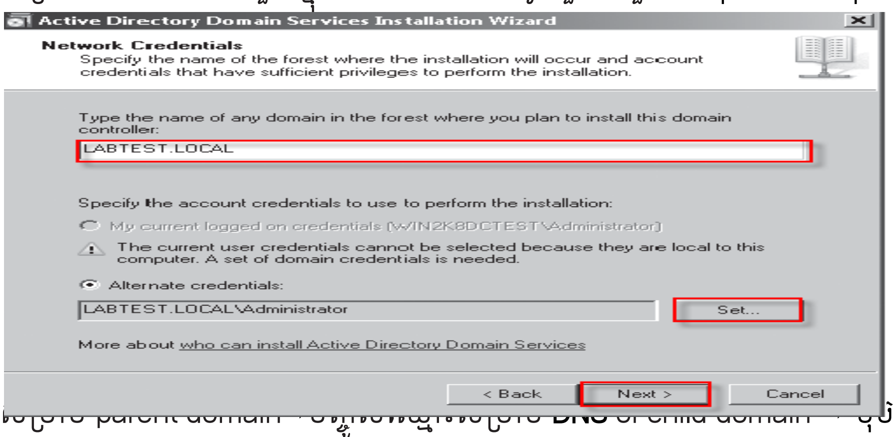
   Upgrade →ចុច **c** →ចុច **enter**



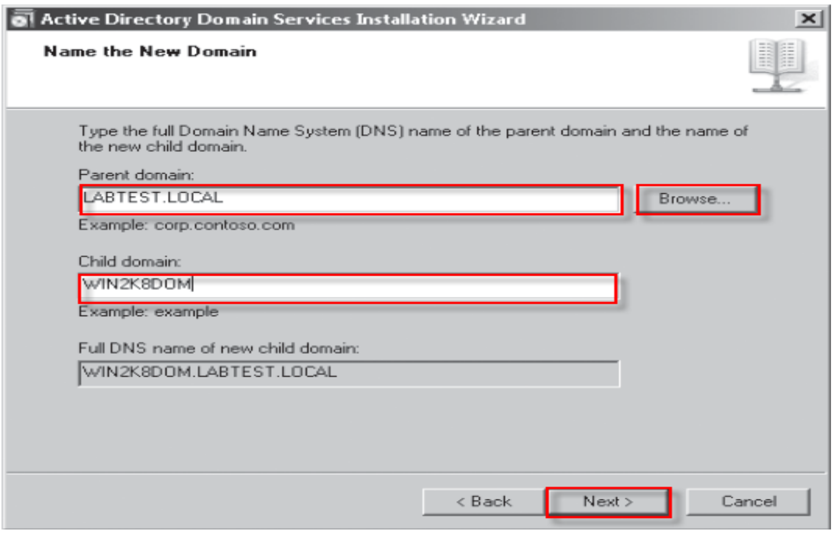
5. Log ទៅកាន់window server 2008
6. ក្នុង server manager → ចុច add roles to start
7. នៅលើ Select Server Roles page →ជ្រើសរើស Active Directory Domain Services→ ចុច next
8. ផ្ទៀងផ្ទាត់លើការ install→ ចុច Next
9. ចុច Install
10. ចុច Close
11. ក្នុង Server Manager→ expand the Roles node →ជ្រើសរើសActive Directory Domain Services
12. ចុច the Run the Active Directory Domain Services installation
13. នៅលើ Welcome screen → ចុច next
14. នៅលើ the Choose a Deployment Configuration screen→ជ្រើសរើស Existing Forest → Create a New Domain in an Existing Forest → ចុចNext



15. បញ្ចូលឈ្មោះសម្រាប់ domain ណាមួយក្នុងforest ដែលចង់ចូលរួមជាមួយ→ ចុច Set → ចុច Next

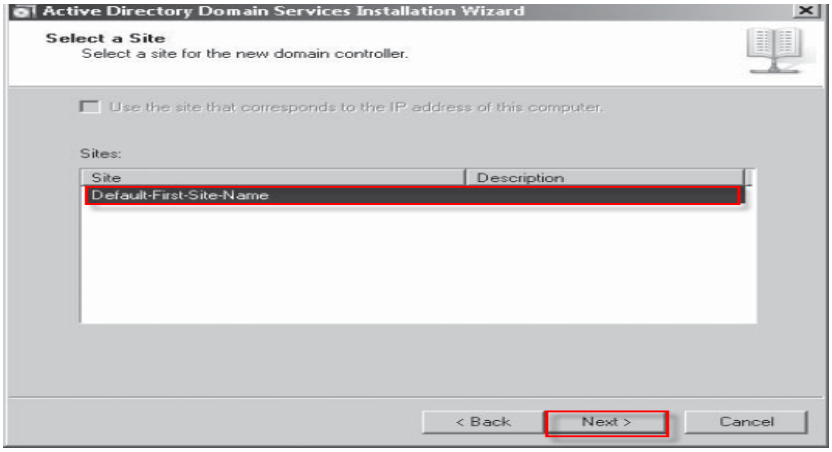


16. បញ្ចូលឈ្មោះ ... Next



17. ជ្រើសរើសយក domain functional level **window server 2008**→ ចុច next

18. ជ្រើសរើសយកActive Directory site ដែលវានឹងក្លាយជាdomain controller ដោយសារយើងមានតែ Site មួយ ដូច្នេះSelect លើ Default-first-site-nam



19. នៅក្នុង additional option screen យើងអាច ជ្រើសរើសយក domain controller ឱ្យវាក្លាយជា global catalog→ ចុច next

20. ចុច Next
21. Enter restore mode password (ដែលជា password ត្រូវតែខុសពី domain administrator)
22. ចុច Next
23. Restart ដើម្បីបញ្ចប់ទាំងស្រុង

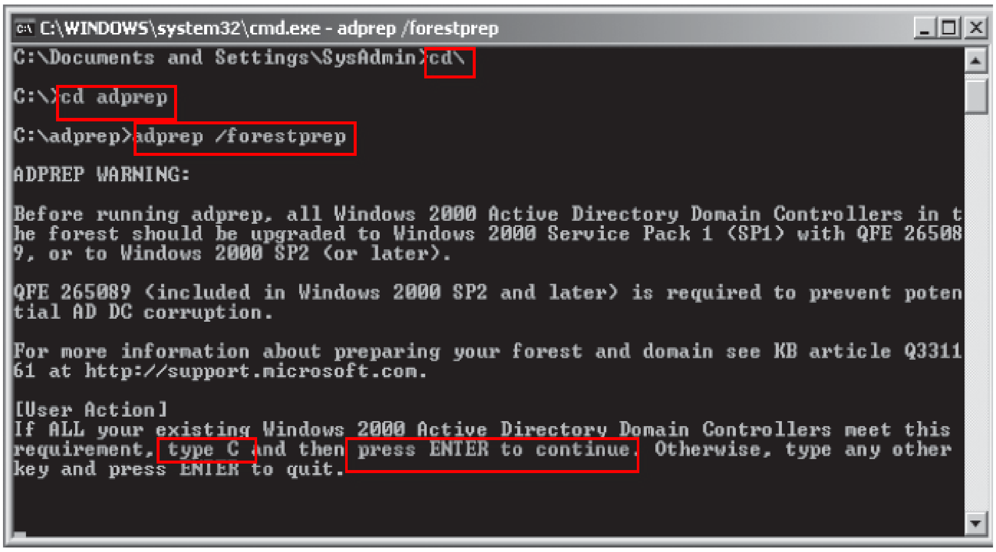
➢ Install Domain controller in an existing window 2000/2003 domain

នេះជាការ Install នូវ domain controller មួយ នៅលើ window server 2008 ដែលupgrade ពី window 2000/2003 ដែលមាន domain រួចជាស្រេចហើយវាក៏មានភាពស្រដៀងចំពោះការ Add new window server 2008 domain ទៅលើ window 2000/2003 forest ដែលមានហើយដែរ ។

1. Log ទៅកាន់ server ដែលមាន Window 2003 forest ដែលដើរតួនាទីជាSchema Master

Copy the\Sources\adprep folder ពីwindow server 2008 →Local Driver on Schema Master

2. ចូលទៅកាន់command prompt ផ្លាស់ប្ដូរទៅកាន់ directory នៅកន្លែងដែលបាន Copy ដាក់ក្នុង adprep folder → run →adprep /forestprep
3. Adprep នឹងបង្ហាញពី warning ដែល window 2000 AD domain controller ត្រូវបាន Upgrade →ចុច c →ចុច enter



4. Log ទៅកាន់ window server 2003 domain ដែលដើរតួនាទីជា Infrastructure master
5. ចូលទៅកាន់command prompt→ផ្លាស់ប្ដូរ director y ដែលបាន copied→run→adprep/ domainprep
6. Log ទៅកាន់ window server 2008
7. នៅក្នុង server manager → ចុច add roles to start
8. ចុច next
9. នៅលើ selects Server Roles screen→ ជ្រើសរើសយក Active Directory Domain Services→ចុច next
10. ចុច Next
11. ផ្ទៀងផ្ទាត់ installation options→ ចុច Install
12. ចុច Close នៅពេលបញ្ចប់ដំណើរការដំឡើង
13. ពង្រីក Roles node នៅក្នុង Server Manager ជ្រើសរើស Active Directory Domain Services
14. ចុច → Run Active Directory Domain Services Installation
15. នៅលើ welcome screen →ចុច Next
16. នៅលើ Deployment Configuration screen→ ជ្រើសរើស Existing Forest → Add a Domain Controller to an Existing Domain→ ចុច next
17. បញ្ចូលឈ្មោះDNS សម្រាប់ parent domain→បញ្ចូលឈ្មោះ DNS of child domain →ចុច next
18. នៅលើ select domain screen →ចុច yes
19. នៅលើ select site screen → ចុច next

20. នៅលើ additional option screen យើងអាចជ្រើសរើសdomain controller ឱ្យវាក្លាយជា global catalog→ ចុច next

21. ចុច Next

22.បញ្ចូល password សម្រាប់ Restore mode (ដែលជា password ត្រូវតែខុសពី domain administrator)

23. ចុច Next

24. Restart

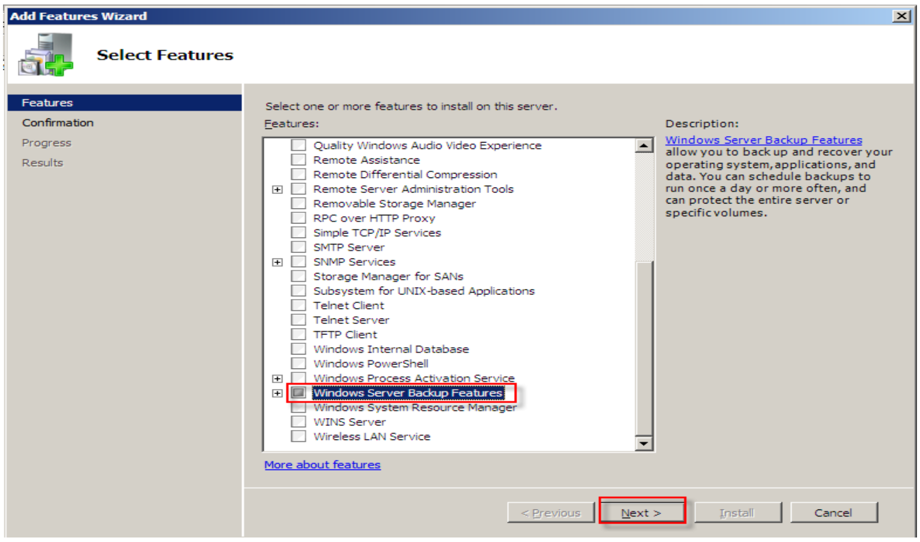
➢ Install active directory form restored backup

Window 2003 និង Window server 2008 បានបង្ហាញពីសមត្ថភាពមួយនៃការស្តារឡើងវិញនូវ active directory ពីការ Backup media ដើម្បីកាត់បន្ថយលើ Replication នៃចរាចរណ៍ដែលបានកំណត់ដើម្បីដំឡើង setup domain controller ថ្មីមួយ។ ដើម្បីអាច Install នៅលើ window server 2008 លុះត្រាតែ យើងមាន Primary domain controller មួយ មានន័យថាយក server មួយធ្វើជា Primary domain controller និងយក Server មួយទៀតដែលធ្វើជា Member(Additional domain controller) ដែលជាការ Backup នូវរាល់ object ទាំងឡាយដើម្បីជៀសវាងពីការខូចដោយករណីណាមួយ។ ដោយហេតុថា additional domain controller ប្រសិនបើ DC ខូច នោះ additional domain controller វានឹងដំណើរការដោយស្វ័យប្រវត្ត។

ដើម្បីកំណត់ពី Option ខាងក្រោមត្រូវតែមាន៖

- domain controller option (writable versus read-only)
- ប្រព័ន្ធប្រតិបត្តិការរួមមាន service pack level
- Platform(x86, x64,or IA64)

Note ជាដំបូងadd **window server backup feature** នៅលើServerទាំងពីរ



1. Log ទៅកាន់SERVER1
2. Run Server Manager→expand the Storage node→ ជ្រើស Windows Server Backup
3. ចុចmouseស្តាំលើ Windows Server Backup → ជ្រើស Backup Once

4. ចុច next on the Backup Options screen.

5. ជ្រើស Custom from the Items menu→ ចុច next

6. ជ្រើស volume containing the ntds.dit files and ចុច next

7. នៅលើ Specify Location Type screen→ ជ្រើសរើសRemote Shared Folder → ចុច Next

8. វាយ in the UNC path to the share on SERVER2 → ជ្រើស Inherit from the Access Control options→ ចុច next

9. Review the summary page→ ចុច Backup

10. Logទៅកាន់ SERVER2

11. បើក command prompt

12. Run →wbadmin get versions -BackupTarget:\\SERVER2\e$\backup

13. ចំណាំពី Version Identifier for example, 12/10/2007-01:30

14. បង្កើត a folder ដែលអ្នកចង់ស្តារឡើងវិញ ឧទាហរណ៍ដូចជា E:\restore

15. Restore the system state data by run→Wbadmin start recovery -backupTarget: \\SERVER2\e$\backup-version:12/10/2007-01:30 -items:ADExtended -itemtype:app -recoveryTarget:"E:\restore"

16. ចុច y to save

17. ក្នុង Server Manager → ចុច Add Roles to launch

18. ចុច Next

19. នៅលើ the Select Server Roles page → ជ្រើសរើស Active Directory Domain Services → ចុច next

20. ចុច Next

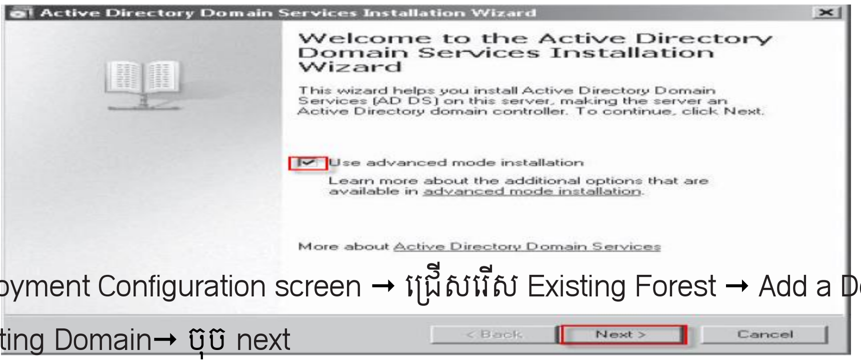
21. ផ្ទៀងផ្ទាត់ installation options → ចុច Install

22. ចុច Close

23. Expand the Roles node in Server Manager → ជ្រើសរើសយកActive Directory Domain Services

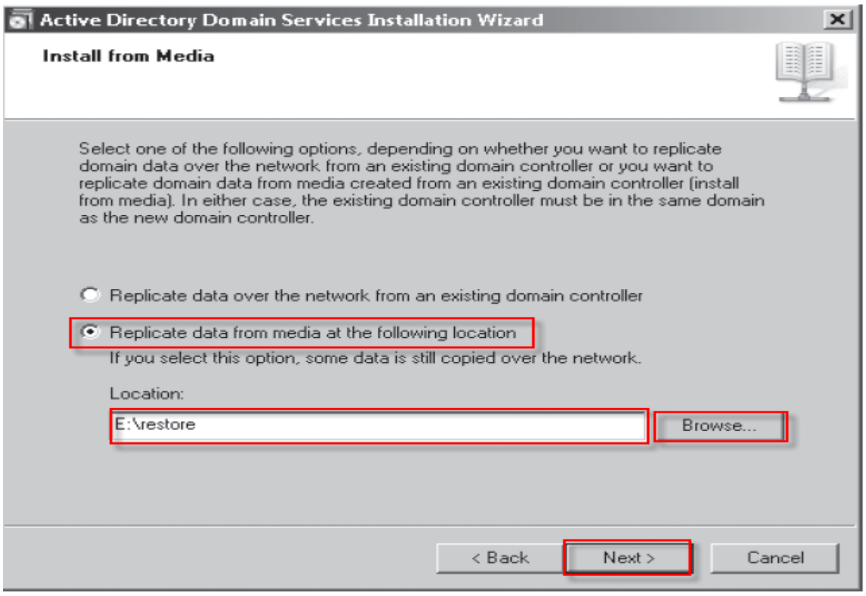
24. ចុច Run the Active Directory Domain Services Installation

25. នៅលើ Active Directory Domain Services Installation → check the Use Advanced Mode Installation→ ចុច Next



26. ក្នុង Deployment Configuration screen → ជ្រើសរើស Existing Forest → Add a Domain Controller to an Existing Domain→ ចុច next

27. បញ្ចូលឈ្មោះសម្រាប់ domain in the forest → ចុច Set to add a domain in the parent domain, → ចុច next
28. នៅលើ the Select Domain screen→ ជ្រើសរើស belonging domain→ ចុច next
29. នៅលើ the Select Site screen → ជ្រើសរើស site belonging domain→ ចុច Next
30. នៅលើ the Additional Options screen→ ចុច Next
31. នៅលើ Install from Media screen→ ជ្រើស Replicate Data from media នៅ ទីកន្លែងខាងក្រោមដែលជា folderដែលចង់ restored the Backup from SERVER1→ ចុច Next

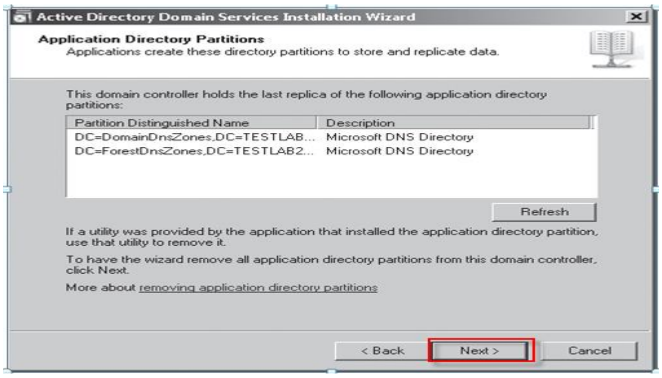


32. ជ្រើសរើស Any Writable Domain Controller from the Source Domain Controller list→ ចុច next
33. ជាទីតាំងដែលមានលក្ខណៈជា Default សម្រាប់ Database, Log Files, and SYSVOL screen→ ចុច next
34. បញ្ចូលRestore Mode Password→ ចុច Next.
35. Review the Summary → ចុច next
36. Restart the computer when prompted

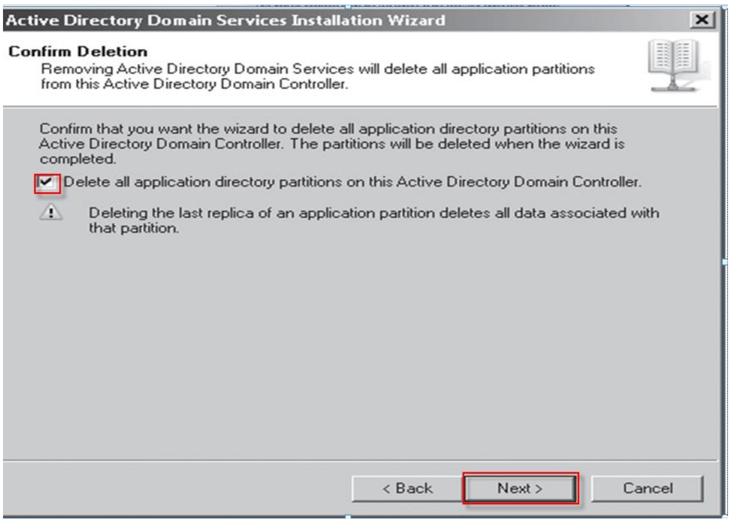
- Removing Active Directory Domain Service from the Last Domain Controller in a Domain and a Forest

1. Run dcpromo
2. បន្ទាប់មកនឹងលេចផ្ទាំង Welcome សូមចុច Next ចង់ឱ្យបង្ហាញបញ្ជីរាយឈ្មោះរបស់ Server សូមចុច Ok វិញ
3. នៅផ្ទាំងបន្តសូមចុចយកត្រង់ពាក្យថា Delete the Domain Because this Server Is the Last Domain Controller បន្ទាប់មកចុច Next

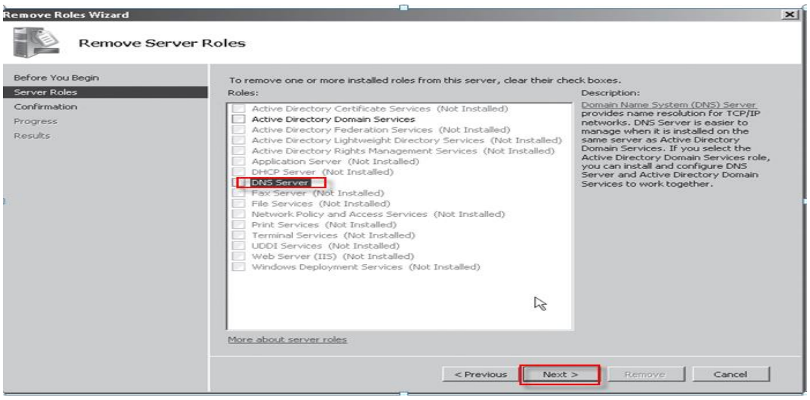
4. បន្ទាប់មកចុច Next ដើម្បីធ្វើការលប់ Partition ទាំងអស់



5. សូម Check ប្រអប់ដើម្បី Confirm រួចចុច Next ដើម្បីបន្តដូចរូបខាងក្រោម:



6. បន្ទាប់មកបញ្ចូល Password domain របស់ administrator account→ click Next
7. ចុច Next ដើម្បីធ្វើការលុប
8. Restart Server ពេលលុបត្រូវបានបញ្ចប់
9. បន្ទាប់ពី Restart ហើយ សូមចូលទៅក្នុងServer Manager ដើម្បីធ្វើការRun Remove Roles Wizard តាមរយៈការចុចRemove Role link in Server Manager តាមរយៈការប្រើ Initial Configuration Wizard
10. ពិនិត្យមើលកិច្ចការឡើងវិញ ហើយចុច Next ដើម្បីបន្ត
11. ដោះប្រអប់ Active Directory Domain Services ហើយចុច Next



១១-៤- Unattended Installation

ការ Install AD DS តាមរយៈការប្រើ Active Directory Domain Services Installation Wizard មានការងាយស្រួលជាងការ Install តាម Role ដែលមានក្នុងWindows Server 2008។ ក្នុងករណីខ្លះ បើអ្នកចង់ Install AD DS តាមរយៈការប្រើ Unattended Installation វិញ។ យើងអាចតាម method នេះ ប្រសិនបើជាការ Install multiple domain controllers ដើម្បីឱ្យច្បាស់ថា domain controllers ទាំងអស់នេះមានរួចហើយ។ ដើម្បី Install និង Configured AD SD តាមរយៈការប្រើUnattended Installation អ្នកនឹងត្រូវការបង្កើត Answer File មួយឈ្មោះថា dcpromo.exe ។បើសិនជាអ្នកមិនចង់ប្រើ answer file នេះទេ អ្នកអាចអនុវត្តវាបាននៅក្នុង Command line។

កំណត់សំគាល់ :

Unattended option បានជំនួសជំហានខ្លះក្នុងការ Install AD SD តែទៅលើអ្វីដែលបាន Select ក្នុង Active Directory Domain Service Installation Wizard ប៉ុណ្ណោះ។

- Unattended Installation of a New Domain Controller to an Existing Windows Server 2008 Domain

1. បើកម្មវិធី Notepad
2. សរសេរពាក្យ [DCINSTALL] រួចចុច Enter ដើម្បីចុះបន្ទាត់
3. រួចសរសេរពាក្យទៅតាមលំដាប់ឱ្យដូចខាងក្រោម៖

UserName=Administrator

UserDomain=LABTEST.LOCAL

Password=P@ssword

ReplicaOrNewDomain=replica

ReplicaDomainDNSName=LABTEST.LOCAL

DNSOnNetwork=yes

SafeModeAdminPassword=P@ssword

RebootOnCompletion=yes

កំណត់សំគាល់ : សូមចងចាំថាចំណុចខាងលើនេះអ្នកត្រូវតែប្តូរនូវ Username, Passwords, និងឈ្មោះ domain គឺធ្វើយ៉ាងណាឱ្យដូចទៅ Network Configuration។

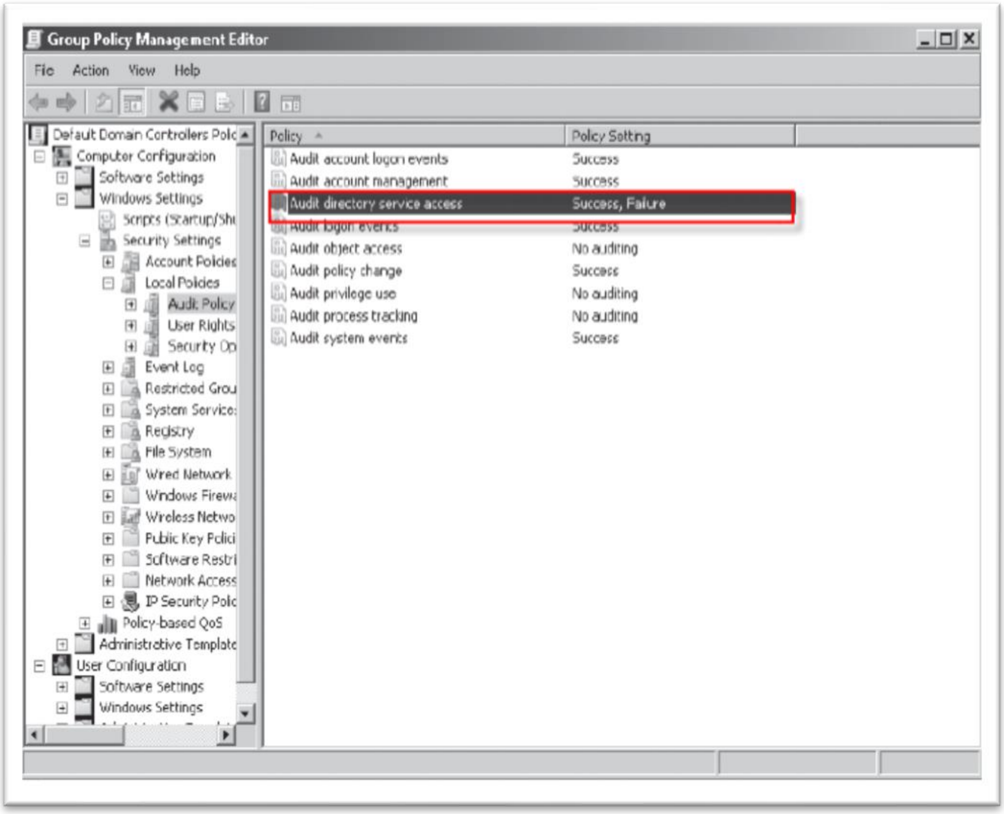
4. សូម save file មួយនេះ→ C:\Unattend.txt

5. បើក Command Prompt → Run dcpromo / unattend:c:\unattend.txt

- Auditing Active Directory Domain Services

វិធីសាស្ត្រនេះអនុញ្ញាតឱ្យអ្នកអាចត្រួតពិនិត្យនូវការចូលប្រើប្រាស់និងការផ្លាសប្តូរផ្សេងៗនៅក្នុង Active Directory ។ Auditing តែងតែមាននៅលើគ្រប់ Windows Server ទាំងអស់ ប៉ុន្តែជាមួយ Windows Server 2008 វិញត្រូវបញ្ចូលវាបន្ថែម ។ ប៉ុន្តែផ្ទុយមកវិញការធ្វើ Auditing ច្រើនអាចជួយកាត់បន្ថយនូវដំណើរការមិនប្រក្រតីរបស់ AD កាត់បន្ថយការកើនឡើងនៃទំហំរក្សាទុកទិន្នន័យបានទៀតផង។យើងក៏អាចបង្កើត Event log "clutter" ដែលជាតម្រូវការយ៉ាងសំខាន់ក្នុងការ Filter ។

Auditing នេះមានកាលណាអ្នកចូលទៅផ្លាស់ប្តូរនៅក្នុង Domain Controller Policy នៅពេលដែលអ្នកចូលទៅកែប្រែ Audit Policy អ្នកគួរចាំឱ្យច្បាស់ ទោះបីជាវាទទួលជោគជ័យរឺ បរាជ័យក៏ដោយ រឺ អ្នកមិនត្រូវ Audit អ្វីទាំងអស់។ ដូចដែលបានបង្ហាញក្នុងរូបខាងក្រោមនេះក្រុមយើងបាន Enabled Success និង Failure Auditing នៃ Directory Service Access សម្រាប់ Windows Server 2008 domain។



- Windows Server 2008 បែកចេញជាបួនផ្នែកតូចៗដែលជាប់ទាក់ទងក្នុងការ Audit Directory Service Access Policy:

1. Directory Service Access
2. Directory Service Changes
3. Directory Service Replication
4. Detailed Directory Service Replication

ដើម្បីត្រួតពិនិត្យលើគោលការណ៍ដែលកំពុងប្រើសម្រាប់ directory service change ណាមួយយើងអាចប្រើប្រាស់តាមរយៈCommand lineដូចខាងក្រោម៖

Auditpol /get /subcategory: "Directory service change"

ដើម្បីបិទ Event logs ដែលមិនដំណើរការសម្រាប់ Directory Service change subcategory យើងអាចប្រើប្រាស់តាមរយៈCommand line ដូចខាងក្រោម៖

Auditpol/get/subcategory:"Directory service change"/failure: disable

- **Read-only domain controller**

Read-only domain controller គឺជាលក្ខណៈពិសេសថ្មីមួយដែលទើបតែបង្កើតឡើងនៅក្នុងwindow server 2008។ រីឯ Additional backup domain controller (BDC) បានផ្តល់ឱ្យនូវLoad balancing service និង redundancy (ដំណើរការបានទាំងពីរ)ចំពោះ domain controller ប៉ុន្តែ(BCD) នេះអនុញ្ញាតឱ្យតែ Read-only copy នៃ domain controller តែប៉ុណ្ណោះ។ read-only domain controller វាមានសារៈសំខាន់ប្រសិនបើយើងចង់ផ្តល់នូវActive directory authentication service ក្នុងផ្នែកណាដែលវាមិនបានផ្តល់នូវ security គ្រប់គ្រាន់សម្រាប់ writable copy នៃ active directory database។ BDC ក៏បានបន្ថែមចំពោះការកំណត់មួយដែលមិនអាចឱ្យដើរតួនាទីជា Global Catalog server ឡើយ ប៉ុន្តែវាអនុញ្ញាតឱ្យស្គាល់ជាមួយ Universal group ផងដែរ។

RODC active directory database អាចរក្សាទុកនូវរាល់ Object ទាំងឡាយណាដែលដូចគ្នានឹង attribute ដែល domain controller ជាទូទៅណាមួយអាចរក្សាទុក ប៉ុន្តែវាមិនអាចរក្សាទុកនូវ account password បានឡើយ។ RODC ក៏អនុញ្ញាតឱ្យយើងផ្ទេរសិទ្ធិចំពោះUser account ដែលមានសិទ្ធិជា administrator ណាមួយនៅលើ RODC Server របស់យើងផងដែរ។

១១-៥- Backup and Recovery

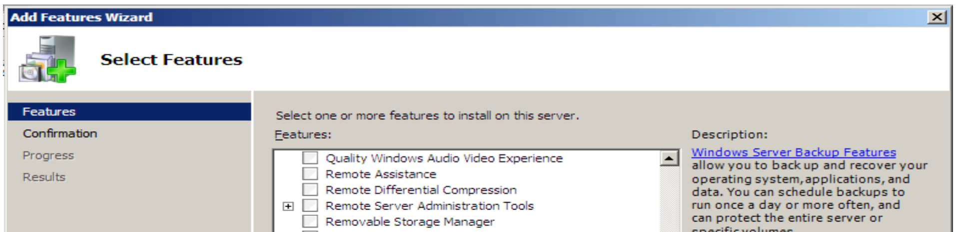
សមាសធាតុសម្រាប់ការ Backup និង recovery AD គឺជាជំនាញមួយដ៏សំខាន់ដែលមិនអាចខ្វះបានចំពោះ administrator។

+System state នៅក្នុង window server 2008 មានសមាសធាតុដូចខាងក្រោម:

- Registry
- COM +class registration database
- Boot file and system file
- Certificate service database
- AD domain service
- Cluster service information
- Microsoft IIS metactiratory
- System file protected by window file protection (WEP)

កំណត់សំគាល់:

ដើម្បីប្រើប្រាស់ Backup នឹង recovery នៃ AD យើងត្រូវ install window server 2008 backup មុនចំពោះការ backup AD database វិញ យើងត្រូវការ backup យ៉ាងហោចណាស់ឱ្យបានមួយដងក្នុងមួយថ្ងៃអាស្រ័យលើការផ្លាស់ប្តូរ AD ក្នុងdatabase។ មុនពេលដែលអ្នកធ្វើការ backup និង Recovery នៃ AD បាន យើងត្រូវ Install Windows Server Backup ជាមុនសិនដូចរូបខាងក្រោម៖



អ្នកអាចធ្វើការ Backup ទាំងអស់ក្នុងកុំព្យូទ័រតែមួយ ឬ backup យកតែ partition ណាដែលសំខាន់ៗ។ Partition ដែលសំខាន់ៗរួមមានសមាសធាតុដូចខាងក្រោម:

- OS files (the entire % windir % Director)
- Registry
- Ntds.dit database files and associated log file
- Sysvol folder

១១-៥-១- ការអនុវត្ត Authoritative

ដោយយកចិត្តទុកចំពោះការស្តារ AD បញ្ហាដែលជួបជាញឹកញាប់គឺនរណាដែលបានលុប object ដោយអចេតនា ឬ តាមគម្រោងដែលបានគ្រោងទុក។

ដើម្បី Recovery object ដែលបានលុបនោះយើងត្រូវស្តារវាមកវិញបានតាម Authoritative ហើយបន្ទាប់មកយើងត្រូវធ្វើការចំណាំលើ object ដែលយើងបានមកវិញ។

១១-៥-២- ការអនុវត្ត Non-Authoritative Restore of AD

Non-authoritative វាគឺជាការ Restore នៃ Object នៅក្នុង AD ដែលមិនអាចធ្វើការកំណត់លើ Object ច្បាស់លាស់សម្រាប់ការសង្គ្រោះឡើងវិញ។

1. Log ទៅកាន់ server មួយណាដែលអ្នកចង់ restore→ open a command prompt
2. Run នូវCommandខាងក្រោមដើម្បីចាប់ផ្តើម server in Directory Services Restore ចុច Switch User នៅលើ logon screen.

   Mode (DSRM)ដើម្បីចូលទៅកាន់Safe mode

   bcdedit /set safeboot dsrepair

   shutdown -t 0 –r
3. ចុចនៅលើOther User
4. វាយពាក្យAdministrator ជា username និង DSRM password→ log in
5. បើក command prompt
6. Enter Diskpart → ចុច enter

7. Enter list vol → ចុច enter
8. កត់ចំណាំលើឈ្មោះនៃ drive ដែលបាន assigned ទៅកាន់ volumn នៅកន្លែងដែលបានបង្កើត
9. Enter exit → ចុច enter
10. Run command ខាងក្រោម (ដាក់ E: ជាឈ្មោះនៃdriver របស់អ្នក):

    Wbadmin get versions -backuptarget:E:
11. ចំណាំនូវversion identifier សម្រាប់ការbackup វាមានទម្រង់ **MM/DD/YYYY-HH:MM—for example, 09/26/2007-22:30.**
12. បញ្ចូលcommand ដើម្បីចាប់ផ្តើម restore

    Wbadmin start sysstaterecovery -version: 09/26/2007-22:30 -backuptarget:E:
13. ចុច y → ចុច enter ដើម្បីចាប់ផ្តើម
14. បន្ទាប់ពីការស្តារបានបញ្ចប់ run នូវ command ខាងក្រោមដើម្បីចាកចេញពី safe mode វិញ

    Bcdedit /deletevalue safeboot

    shutdown -t 0 –r

១១-៥-៣- ការអនុវត្ត Authoritative Restore នៃ AD

ចំពោះការ Restore Authoritative Restore of AD ជាគឺ restore ចំពោះ Object ដែលស្ថិតនៅក្នុង AD ហើយអាចធ្វើការកំណត់ទៅលើ Object ណាមួយច្បាស់លាស់ដើម្បី Restore ដូចជានៅពេល ដែលយើងបានច្រលំលុប Object ណាមួយដោយអចេតនា។

Ex : CN=TESTUSER,CN=USER,DC=TESTDOM2,DC=LOCAL

1. អនុវត្ត Non-authoritative restore of Active Directory ប៉ុន្តែមិនចាំបាច់ restart Server ទៅកាន់ normal mode
2. ជ្រើសរើសStart →Run → command prompt →វាយ **ntdsutil** →ចុច enter.
3. វាយ **activate instance NTDS** ចុច enter
4. វាយ **authoritative restore** ចុច enter.
5. វាយ **restore object "CN=TestUser,CN=Users,DC=TESTDOM2,DC=LOCAL"** →ចុច enter
6. ចុច Yes ដើម្បី confirm
7. ចំណាំនៅកន្លែដែលtext file និង LDIF files ដំណើរការដែលបានផ្ទុក
8. វាយ **quit**→ចុច enter
9. បន្ទាប់ពីការស្តារឡើងវិញបានបញ្ចប់→run ខាងក្រោមដើម្បីចាកចេញពី Safe mode

    Bcdedit /deletevalue safeboot

    shutdown -t 0 –r
10. Log ទៅកាន់server
11. បើក command prompt → run command ខាងក្រោមដោយត្រូវប្រាកដថាគ្មាន Error កើតឡើង

    Repadmin /syncall SERVER3.TESTDOM2.LOCAL /e d /A /P /q
12. Recover any backlinks ចំពោះ Objectដែលអ្នកទើបតែស្តារឡើងវិញដោយប្រើប្រាស់ LDIF fileដែលត្រូវបានបង្កើតដោយ authoritative restore→ Run command ខាងក្រោម

Ldifde -i -k -f c:\restored_object.ldf

13. ប្រសិនបើមានតែ domainនៅក្នុង tree នោះបន្តNext Step
14. ប្រសិនបើអ្នកកំពុងតែស្តារឡើងវិញនូវ Object នៅក្នុងforest ដែលមាន domain ច្រើនជាងមួយ នោះចាំបាច់ត្រូវ Create LDIF file សម្រាប់ object ដែលបានទាញយកមកវិញដោយការ boot ពី domain controller នៅក្នុង domain ដែលនៅក្នុង Tree នីមួយៗ ហើយចូលទៅកាន់ DSRM → **run**

Ntdsutil

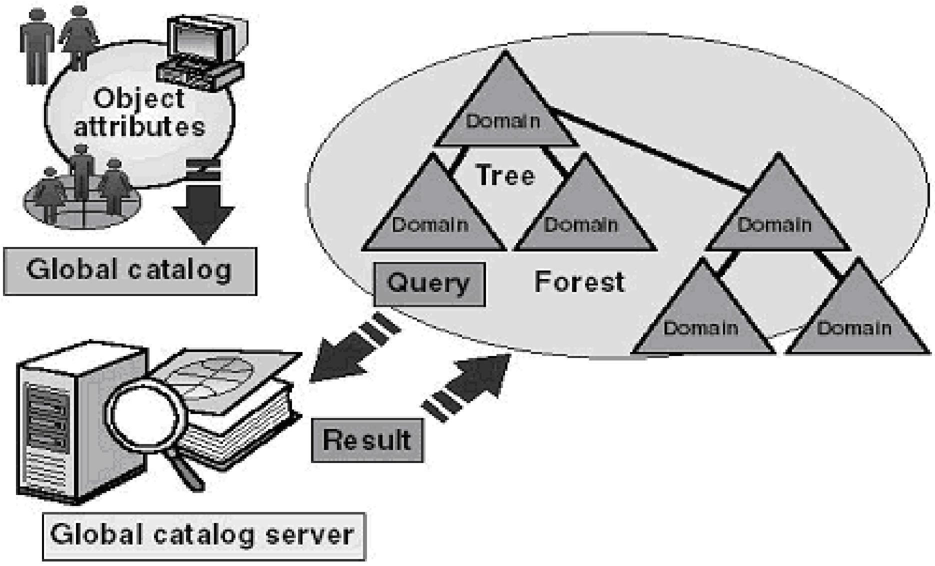
Ntdsutil: authoritative restore

Ntdsutil authoritative restore : create ldif from c:\Restored object.txt

15. ចំណាំពីទីតាំងថ្មីដែលបានបង្កើត LDIF file →ចាកចេញពី ntdsutil និង restart domain controller ទៅកាន់ normal mode
16. Log onទៅកាន់ domain controller → run command ដូចគ្នាប្រើជំហាន១២យើងត្រូវអនុវត្តននូវជំហានទី១៤ដល់១៦នៅលើ domain controller មួយសម្រាប់ domain tree នីមួយៗ។

១១-៥-៤- Global catalog (GC)

- ផ្តល់ឱ្យនូវសេវាដើម្បីងាយស្រួលរក Objects ក្នុង AD
- GC មាន replica ដោយផ្នែករបស់ Object នីមួយៗក្នុង AD
- Domain Controller ទី១ត្រូវបានបង្កើតឡើងជា Global catalog server ជាស្វ័យប្រវត្ត
- Global catalog server គឺជា Server ដែលប្រមូលផ្តុំព័ត៌មាននៅលើវាតែមួយគត់



១១-៥-៤-១- ការគ្រប់គ្រង User Accounts

ជាទូទៅគ្រប់បុគ្គលិកនៅក្នុងក្រុមហ៊ុនត្រូវការនូវ User Account ម្នាក់មួយដើម្បីប្រើប្រាស់នូវធនធានរបស់ Network ។ គួររម្លឹកថា Domain User Account ស្ថិតនៅលើ Domain Controller ហើយអាច Logon ពីគ្រប់ Clients ហើយអាចប្រើប្រាស់នូវធនធាននៅក្នុង Domain ទាំងមូលបាន។

ការណែនាំអំពី User Account

- User Account អាចផ្ដល់ឱ្យ Users នូវលទ្ធភាព
    - អាច Logon ទៅកាន់ Domain ដើម្បីទទួលបានសិទ្ធិក្នុងការប្រើប្រាស់ធនធានរបស់ Network
    - User ម្នាក់ត្រូវបានផ្ដល់ឱ្យនូវ User Account តែមួយគត់
- Local User Account គឺជា Account ដែលត្រូវបានបង្កើតឡើងនៅលើ Windows 7/Windows 8/Windows 10
- វាអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាច Logon និងប្រើប្រាស់ចំពោះធនធានដែលមានចំពោះតែកុំព្យូទ័រខ្លួនវាប៉ុណ្ណោះ
- វាមិនអាចប្រើប្រាស់ធនធាននៅក្នុង Domain បាននោះទេ

Domain User Account ជា Account ដែលត្រូវបានបង្កើតឡើងនៅលើ Domain Controller (DC)

- វាអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាច Logon ទៅកាន់ Domain និងអាចប្រើប្រាស់ចំពោះធនធាននៅក្នុងប្រព័ន្ធ Network ទាំងមូល

Built-in User Accounts ជា User Accounts ដែលមានស្រាប់

a. Administrator: Full privileges.
b. Guest: only gain access the resources.

ការបង្កើត User Account ថ្មី

ដើម្បីបង្កើត User Account ថ្មីមួយយើងត្រូវគិតទៅលើលក្ខខ័ណ្ឌ

- ត្រូវដាក់ឈ្មោះ
- ត្រូវដាក់លេខសម្ងាត់
- ត្រូវកំណត់ Account Option ដូចជា logon hours, account expiration

ការដាក់ឈ្មោះ

- User Logonname ត្រូវបានតែមួយគត់
- មានប្រវែង២០តួអក្សរជាអតិបរិមាន(អក្សរធំឬអក្សរតូច)
- អក្សរមិនអាចប្រើប្រាស់បាន " / \ [] : ; = , + * ? <>
- User logon name មិនប្រកាន់អក្សរធំឬអក្សរតូច
- លេខសម្ងាត់ត្រូវការជាចាំបាច់
    - ដើម្បីការពារអ្នកដែលគ្មានសិទ្ធិក្នុងការលួចប្រើប្រាស់
    - ត្រូវប្រើលេខសម្ងាត់ដែលគេពិបាកទាយត្រូវ
    - លេខសម្ងាត់អាចមានប្រវែងរហូតដល់១២៨តួអក្សរ
    - គេអាចប្រើបន្សំនៃអក្សរធំ អក្សរតូចនិងនិមិត្តសញ្ញា

Account options

- Logon Hours សម្រាប់កំណត់ពេលវេលាអាច Loggon បានឬមិនបាន
- ការកំណត់ Logon hours ដើម្បីកំណត់ម៉ោងដែលអាចប្រើប្រាស់ Network បាន
    - ការពារការលួចប្រើប្រាស់ព័ត៌មានដែលស្ថិតនៅលើកុំព្យូទ័រ

Account expiration

- សម្រាប់កំណត់ឱ្យ User មិនអាចប្រើប្រាស់បាននៅពេលដែលផុតកំណត់

- ការលុប User Account
- នៅពេលដែល User ឈប់ធ្វើការនៅក្នុមហ៊ុន

Resetting Passwords and Unlocking User Accounts

- មិនអាច Logon បាន(ភ្លេចលេខសម្ងាត់)
- Unlock កុំព្យូទ័រ
- ការព្យាយាម Logon ដោយវាយលេខសម្ងាត់ខុសច្រើនដង
- ក្នុងការអនុវត្ត អ្នកគួរតែកំណត់ User Account សម្រាប់បុគ្គលបណ្តែតឱ្យផុតកំណត់ពេលចប់កិច្ចសន្យា

១០-៥-៥- ការគ្រប់គ្រងគណនីក្រុម

១០-៥-៥-១- ប្រភេទនៃក្រុម

1- Security Groups.

2- Distributed groups.

3- Group Scopes

1. Domain local.
2. Global
3. Universal

១១-៥-៥-២- ការណែនាំឱ្យស្គាល់ក្រុម

Group គឺជាការប្រមូលផ្តុំនៃ user accounts ។ Groups គេប្រើសម្រាប់សម្រួលក្នុងការគ្រប់គ្រង។

1-Permissions ជាសិទ្ធីសម្រាប់ដាក់លើ Files និង Directories

2-User rights ជាសិទ្ធិសម្រាប់ដាក់ឱ្យ Users ប្រើប្រាស់ចំពោះ System Users អាចជាសមាជិករបស់ group ជាច្រើន។

- Security group
- windows 2000 operating system ប្រើតែ security group ប៉ុណ្ណោះ ។
- អ្នកអាចប្រើវាសម្រាប់កំណត់ permissions ដើម្បីទទួលសិទ្ធិប្រើប្រាស់ resources
- កម្មវិធីត្រូវបានគេប្រើសម្រាប់ស្វែងរកក្នុង AD ដែលអាចប្រើ security groups សម្រាប់ផ្ញើ e-mail messages ទៅឱ្យក្រុមនៃ users នៅពេលតែមួយ ។
- security group មានសមត្ថភាពគ្រប់គ្រង distribution group.
- Distribution Groups
  - Applications ប្រើ distribution groups សម្រាប់តួនាទីដែលមិនទាក់ទង security ឧទាហរណ៍ sending e-mail messagesទៅ users មួយក្រុមនៅពេលតែមួយ
  - អ្នកមិនអាចប្រើ distribution group សម្រាប់កំណត់ permissions ។
- Group Scopes
  - អនុញ្ញាតឱ្យ users អាចកំណត់ permissions ។
  - អាចកំណត់ទីតាំងក្នុង network ដែលអ្នកអាចប្រើប្រាស់ group ។

- Domain Local Groups
    - គេប្រើភាគច្រើនបំផុតសម្រាប់កំណត់ permissions ចំពោះresources.
    - domain local group មានលក្ខណៈដូចខាងក្រោមៈ
        - បើកចំហចំពោះសមាជិក
        - អាចចូលប្រើ resources ក្នុង domainមួយ
- Global Groups
    - ដើម្បីរៀបចំ users ដែលមានតម្រូវការប្រើប្រាស់ network access ដូចគ្នា
    - global group មានលក្ខណៈដូចខាងក្រោមៈ
    - កំណត់ភាពជាសមាជិក
    - ប្រើប្រាស់ resources បានក្នុង domain ណាមួយ
- Universal Groups
    - គេប្រើភាគច្រើនបំផុតសម្រាប់កំណត់ permissions ចំពោះដែលទាក់ទងក្នុង domains ជាច្រើន ។
    - universal group មានលក្ខណៈដូចខាងក្រោមៈ
        - បើកចំហចំពោះសមាជិក-សមាជិកអាចមកពី domain ណាមួយ
        - អាចប្រើប្រាស់ resources ក្នុង domain ណាមួយ
        - គេអាចប្រើវាតែក្នុង Native mode ប៉ុណ្ណោះ ។
- Built-in groups ដែលមានស្រាប់
    - Windows 2000 មាន built-in groups ចំនួន៤គឺ:
        - Global
        - Domain local
        - Local
        - System
- Built-in global Groups
    - Domain Users-មានសិទ្ធិត្រឹមតែប្រើប្រាស់ Resources
    - DomainAdmins-មានសិទ្ធិប្រើប្រាស់នូវការងារគ្រប់គ្រងលើកុំព្យូទ័រណាមួយក្នុង domain
    - Domain Guests-guest account ជាសមាជិករបស់វា
    - Enterprise Admins-មានសិទ្ធិគ្រប់គ្រងលើ administrative tasks សម្រាប់ប្រព័ន្ធ Network ទាំងមូល។ តាមធម្មតា administrators គឺជាសមាជិករបស់ enterprise Admins ។
- Built-in local groups
    - Domain users-គ្រប់ users ទាំងអស់ជាសមាជិករបស់វា
    - Domain Admins-administrator គឺជាសមាជិករបស់វា
    - Domain guests-guest account គឺជាសមាជិករបស់វា
    - Enterprise Admins-administrator គឺជាសមាជិករបស់វា
- Built-in Local Groups
    - Users-មានសិទ្ធិត្រឹមតែប្រើប្រាស់ resources ដែលអនុញ្ញាតឱ្យប្រើប្រាស់ក្នុង domain

- Administrators-មានសិទ្ធិប្រើប្រាស់នូវ administrative tasks ទាំងអស់ក្នុង domain
- Guests-មានសិទ្ធិត្រឹមតែប្រើប្រាស់ resources ដែលអនុញ្ញាតឱ្យប្រើប្រាស់ប៉ុណ្ណោះ
- Backup Operators-អាច backup និង restore
- Power Users- អាចបង្កើតអាចកែប្រែនិងអាចចែកចាយនូវ resources.
- Replicator-អាច configure file replication service

- Built-in system
  - Everyone-គ្រប់ users អាចប្រើប្រាស់ចំពោះ resources ជា default
  - Authenticated Users-យើងប្រើ authenticated group ជំនួសឱ្យ Everyone group ដើម្បីការពារជនអានាមិកប្រើប្រាស់ចំពោះ resource
  - Creator Owner-Administrators គឺជាម្ចាស់របស់ resources
  - Network-រួមទាំង user ណាម្នាក់ដែលបានភ្ជាប់ពីកុំព្យូទ័រណាមួយនៅលើ network ដើម្បីចែកចាយ resource
  - Interactive-ទទួលសិទ្ធិប្រើប្រាស់ resources នៅលើកុំព្យូទ័រដែលត្រូវបានភ្ជាប់ ។ ពួកគេ logon ហើយទទួលការ access ចំពោះ resources ដោយ "interacting" ជាមួយកុំព្យូទ័រ
  - Anonymous Logon រួមទាំង user account ដែល Windows 2000 មិន authenticate
  - Dial-up-រួមទាំង user ដែលកំពុង dial-up connection

ជំពូកទី១២

Internet Information Service 7.0

Internet Information Services (IIS) security បានទទួលសមត្ថភាពល្អជាយូរឆ្នាំមកហើយដោយសារតែ IIS 6.0 ទទួលបានសមត្ថភាពពី IIS 4.0 ។ នៅពេលដំឡើង IIS កំណែមុន អ្វីៗក៏ដោយស្ទើរតែទទួលបានទាំងអស់តាមលំនាំដើម។

IIS 7.0 ទទួលបានលក្ខណៈពេញលេញនៃ Windows server 2008 គឺ "អ្វីដែលមិនបានដំឡើងគឺមិនត្រូវការនូវ Patch នោះទេ"។

១២-១- លក្ខណៈពិសេសនៃ IIS 7.0

IIS 7.0 ត្រូវបានបង្កើតឡើងហើយមានលក្ខណៈពិសេសដូចខាងក្រោម:

- ផ្តល់សមត្ថភាពឱ្យផ្ទេរសិទ្ធិនៃការគ្រប់គ្រង
- ផ្តល់ឱ្យនូវសមត្ថភាពបត់បែននៃការពង្រីកសមត្ថភាពដែលអនុញ្ញាតឱ្យកែប្រែដោយបង្កើតឱ្យមានសុវត្ថិភាព
- ត្រូវបានបញ្ចូលនូវ Applications និងប្រព័ន្ធត្រួតពិនិត្យសុខភាព
- បង្កើនសមត្ថភាពនៃការស្វែងរកកំហុស (Diagnostic) និងការដោះស្រាយបញ្ហា (Trouble shooting)
- ផ្តល់នូវ Tools សម្រាប់គំនិតផ្តួចផ្តើមនៃការគ្រប់គ្រង
- ផ្តល់នូវ Application ពិតប្រាកដ Xcopy deployment

១២-២- ការដំឡើង IIS 7.0

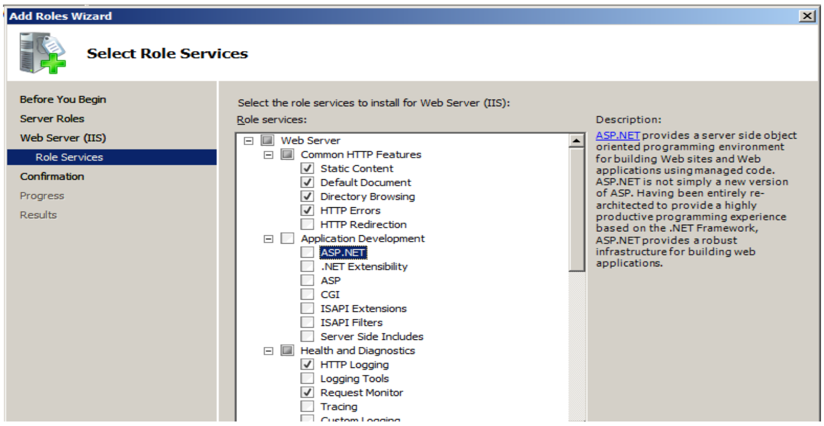
១-បើក Server Manager

២-ចុចលើ Add Roles Link នៅក្រោម Roles Summary

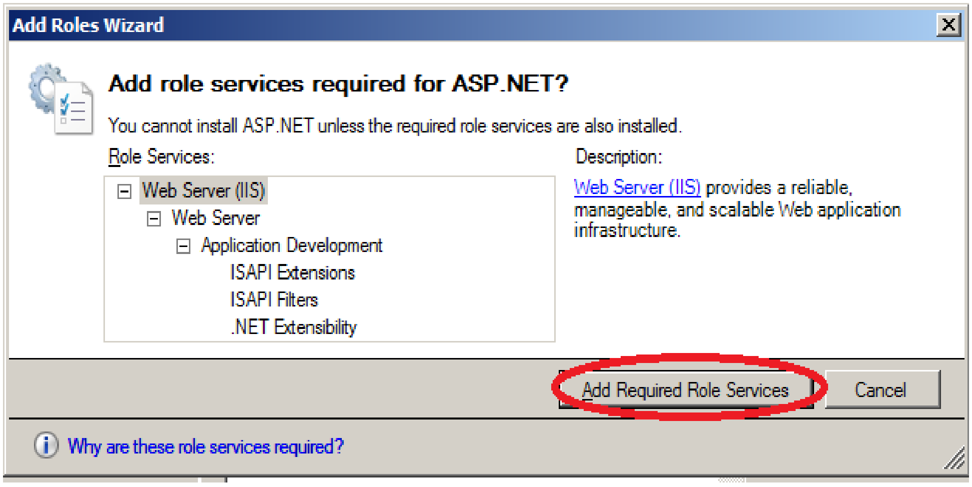
៣-ចុចលើ Next ដើម្បីបន្ត

៤-ជ្រើសរើសយក Web Server (IIS)

៥-ចុចលើ Add requirement Feature ហើយបន្ទាប់មកចុចលើ Next



រូបភាព ១២-១-សមាសធាតុរបស់ IIS 7.0

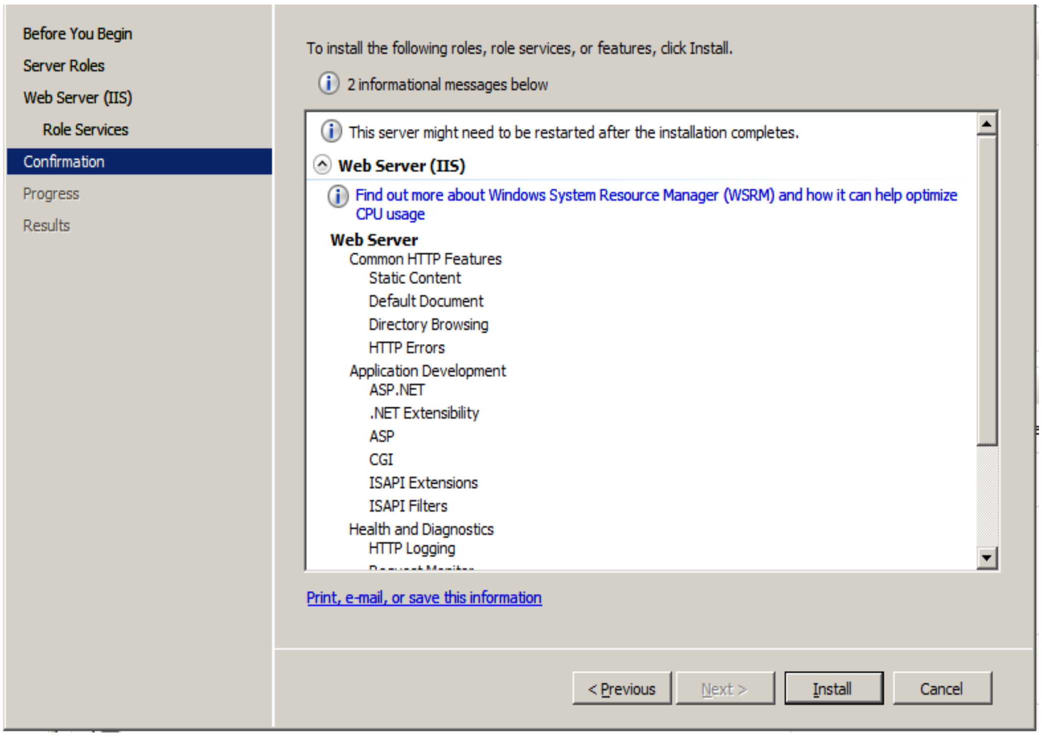


រូបភាព ១២-២-ការដំឡើង ASP.NET

៦-ចុចលើ Next

៧-ជ្រើសរើសយកសមាសធាតុនៃ IIS ដូចជា ASP.NET, ASP,CGI, FTP ជាដើម

៨-ពិនិត្យមើលពីជម្រើសឡើងវិញហើយចុចលើ Install



រូបភាព ១២-៣-ការដំឡើង IIS 7.0

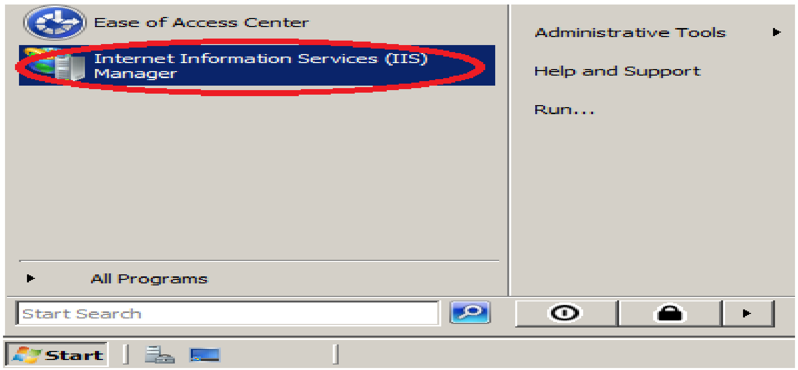
៩-ចុចលើ Close ដើម្បីបញ្ចប់ការដំឡើង

១២-៣- ក្ងួងស្ទួលសម្រាប់គ្រប់គ្រងលើ IIS

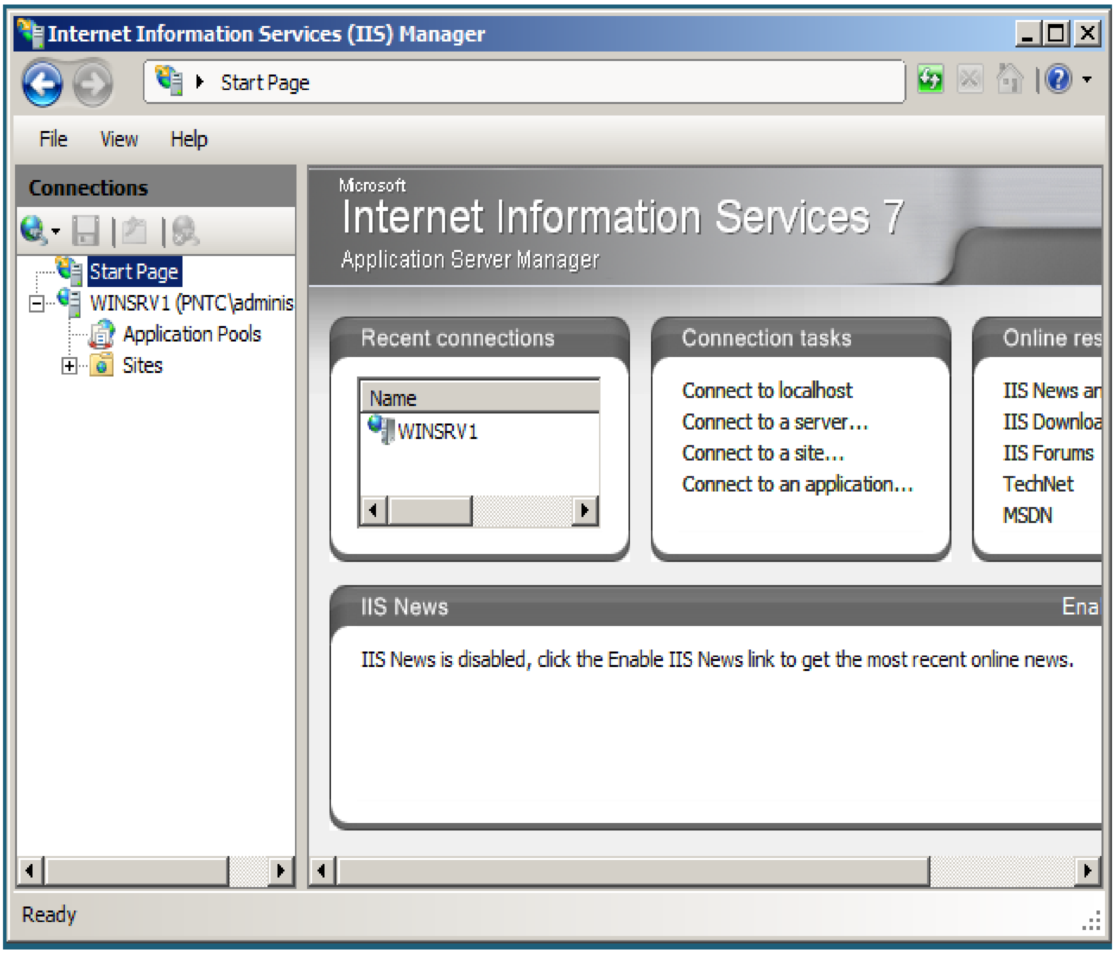
ចំណុចមួយដ៏សំខាន់ដែលមានការផ្លាស់ប្តូរចំពោះ IIS គឺការគ្រប់គ្រងដោយប្រើ Interface របស់វាគឺ IIS Manager ។

អ្នកអាចមើលពីការ Configure Server បានដោយអនុវត្តតាមជំហានដូចខាងក្រោម

Start=>Internet Information Services (IIS) Manager



រូបភាពទី១២-៤- IIS manager



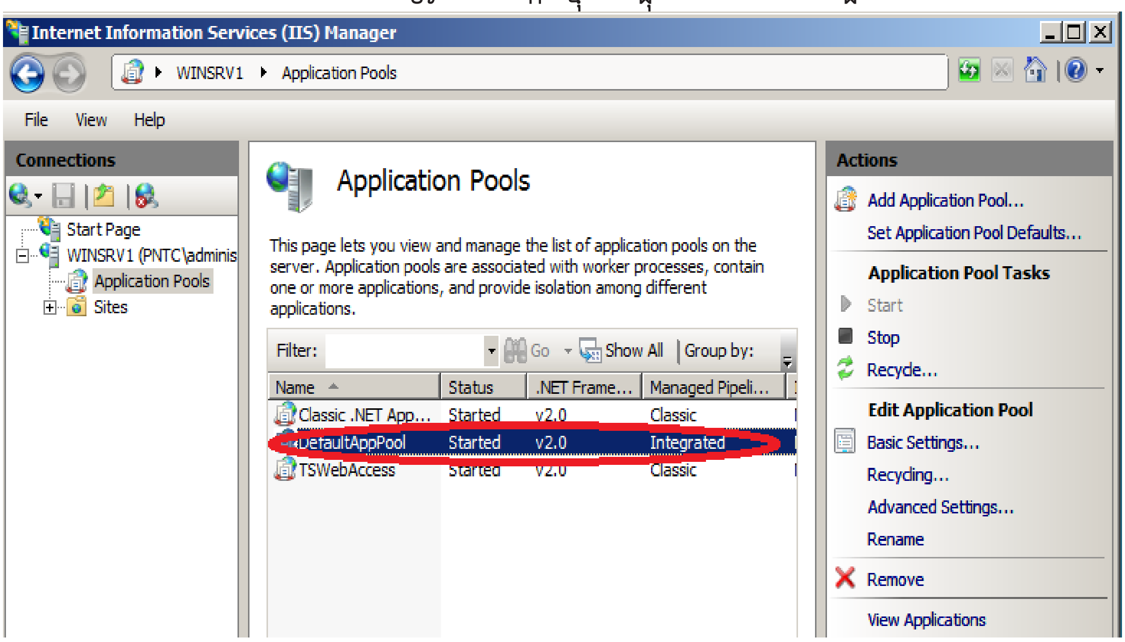
រូបភាពទី១២-៥-IIS manager start page

បើអ្នកមានបំណងពង្រីក Server នៅក្នុងផ្ទាំងនៃការភ្ជាប់ អ្នកនិងឃើញ containers ពីរគឺ:

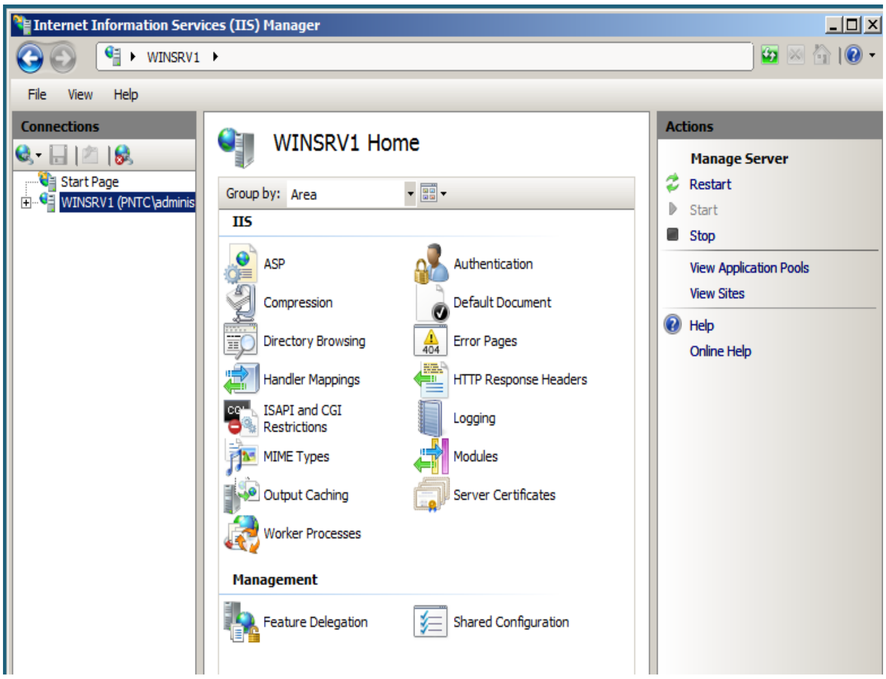
- Applicatopn Pools
- Web sites

គេប្រើ Application Pools ដើម្បីដាក់ Applications ជាក្រុម ជាពិសេសគឺដាក់ Applications ផ្សេងៗគ្នាទៅតាមក្រុមរបស់វា។ ពីព្រោះថា applications នីមួយៗមានទំនាក់ទំនងគ្នាជាមួយ Worker Thread ផ្ទាល់ខ្លួនរបស់វា អ្នកមិនបាច់បារម្ភណ៍ពីកំហុសកើតមានឡើងនៅក្នុង application នីមួយៗដែលនិងធ្វើឱ្យមានការប៉ះពាល់ដល់ Application ផ្សេងនោះទេនៅពេលវាស្ថិតនៅក្នុង application pool ផ្សេងគ្នា។

តាមលំនាំដើម DefaultAppPool ត្រូវបានបង្កើតក្នុងកំឡុងពេលនៃការដំឡើង។



រូបភាពទី ១២-៦-Default AppPool

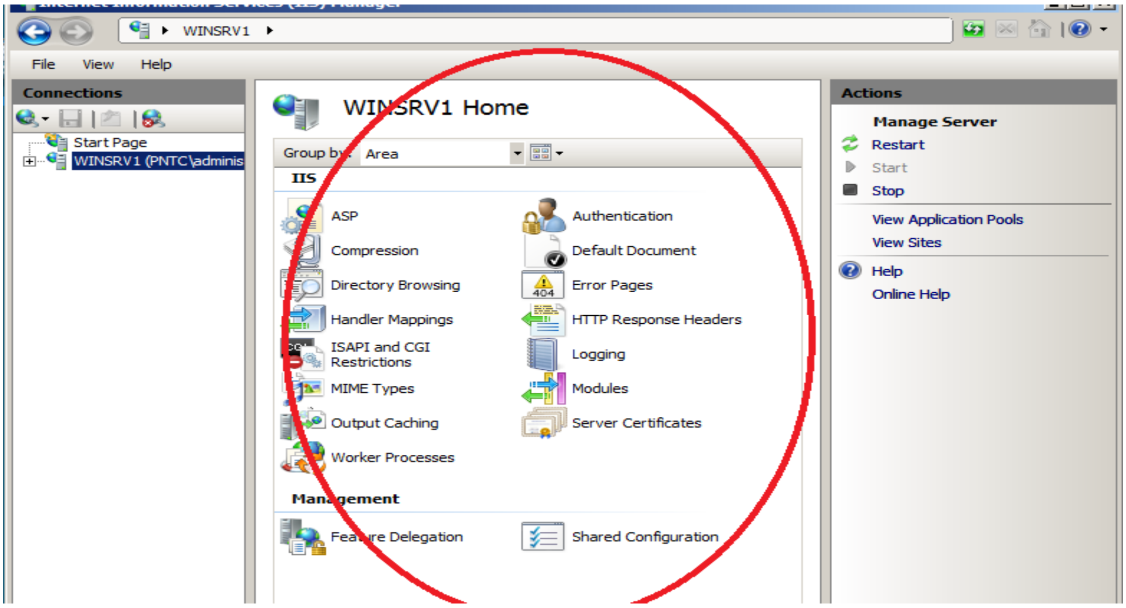


រូបភាពទី ១២-៧- IIS Server Home Page

តាមលំនាំដើម IIS ត្រូវបានដំឡើងហើយមានការគាំទ្រតែ Static Webpages ប៉ុណ្ណោះ(HTML)។

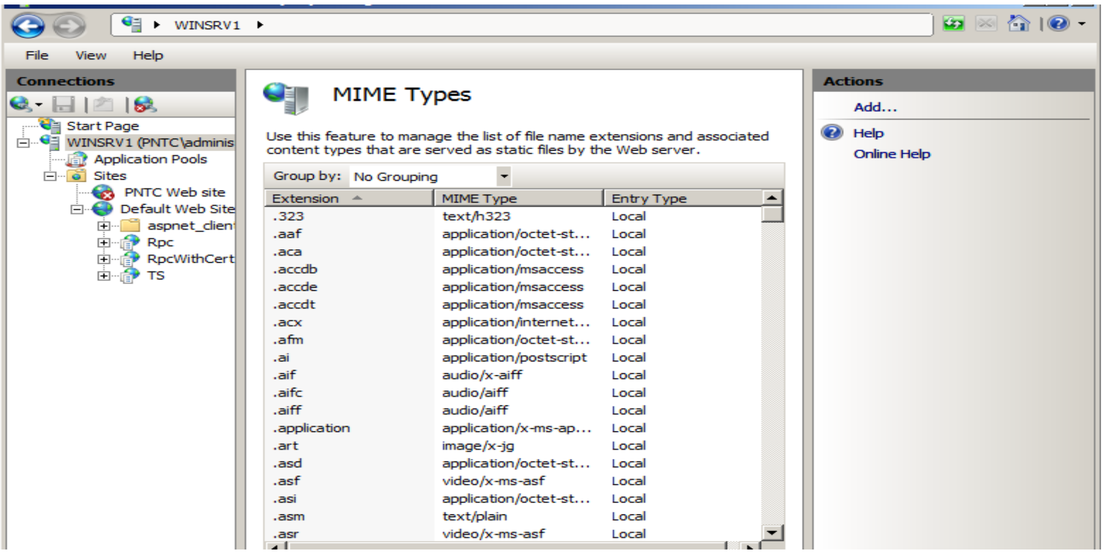
បើអ្នកមានបំណងចង់ឱ្យវាមានការគាំទ្រចំពោះ Dynamic contents ដូចជា ASP.NET,CGI អ្នកត្រូវដំឡើងវាបន្ថែមទៀត។

Default Web site មានទីតាំងស្ថិតនៅត្រង់ចំណុច c:\Inetpub\wwwroot ។ Home panel នៅចំកណ្តាលត្រូវបានគេប្រើសម្រាប់បង្ហាញពីលក្ខណៈពិសេសឬអត្ថន័យនៃ Object ដែលបានជ្រើសរើស



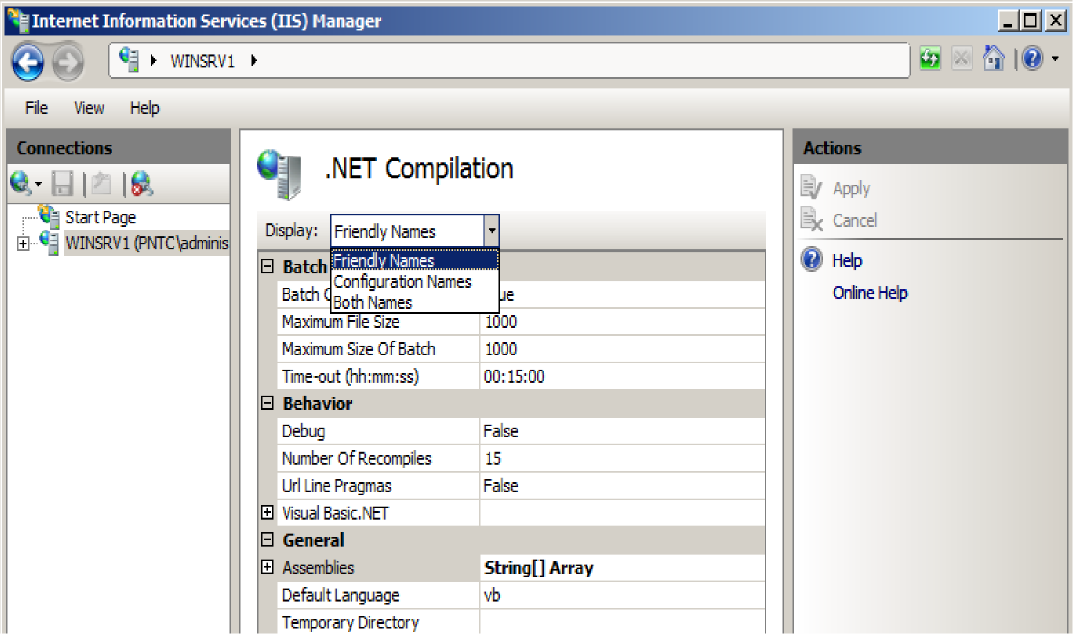
រូបភាពទី ១២-៨-Home Pane

List page គឺជាតារាងគម្រោងត្រូវបានប្រើសម្រាប់បង្ហាញពីតារាងនៃវត្ថុដែលត្រូវការ។ ឧទាហរណ៍ បើអ្នកចុចលើ MIME Types ពីរដង តារាងនៃ MIME Types ទាំងអស់ដែលបានកំណត់ពី Web site ត្រូវបានបង្ហាញដូចក្នុងរូបភាព ១២-៩។



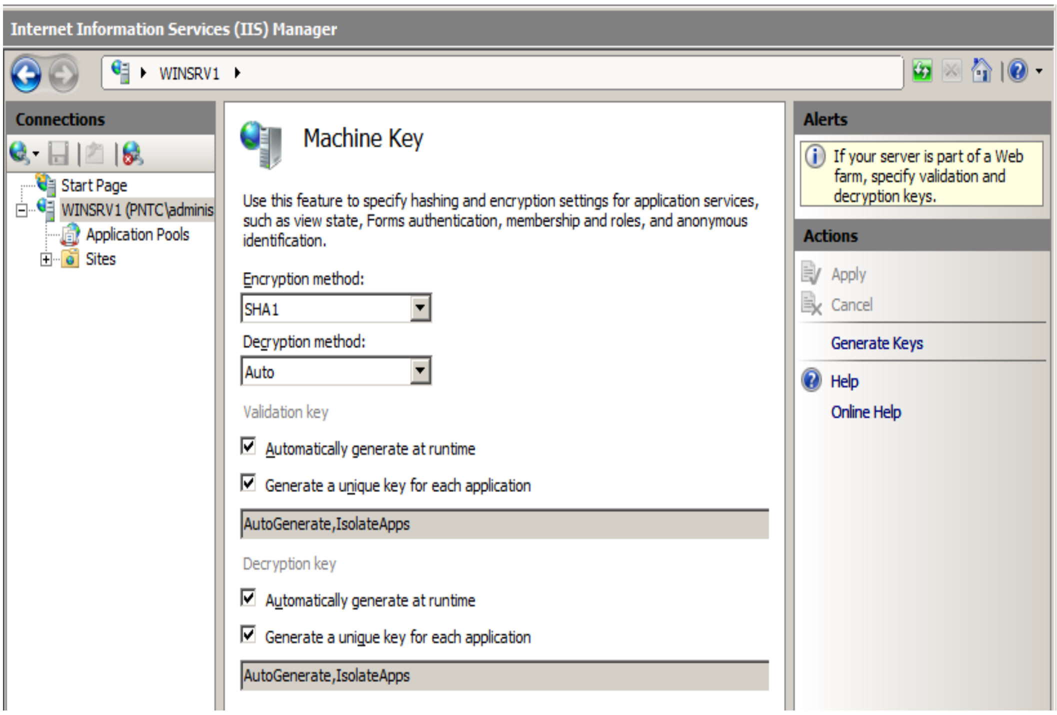
រូបភាព ១២-៩-List page

Property Grid ត្រូវបានប្រើបង្ហាញពី Properties ផ្សេងៗត្រូវបាន Configure ។ Property ក៏បង្ហាញផងដែរពី Friendly Name និង Configuration Name ក៏ដូចជាតម្លៃរបស់វា។



រូបភាព ១២-១០-Property Grid page

Dialog pages មានលក្ខណៈដូចទៅនិង dialog box ហើយមានសមាសធាតុដូចជា Drop-down menu, Checkboxes និង Dialog boxes ផ្សេងៗទៀត។



រូបភាពទី១២-១១-Dialog page

១២-៤- ការគ្រប់គ្រង IIS ពីចម្ងាយ

តាមលំនាំដើម ការគ្រប់គ្រងលើ IIS ពីចម្ងាយត្រូវបានបិទ។ ដើម្បីប្រើវាបានអ្នកត្រូវដំឡើងវាជាមុនសិនគឺ Web Management Service WMSVC ដែលត្រូវបាន Startup ដោយអ្នកគ្រប់គ្រង។

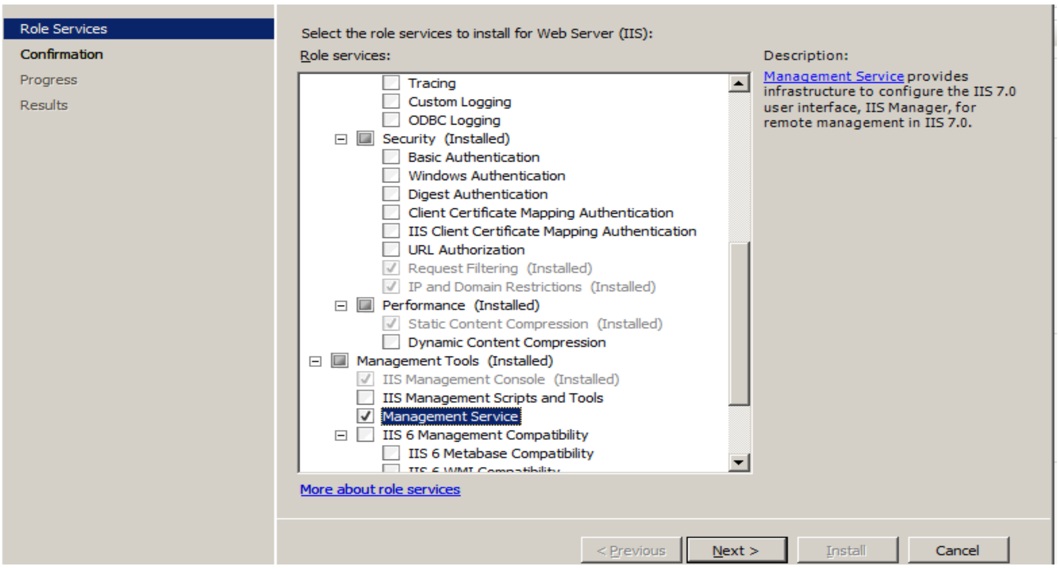
ការដំឡើងនិងបើក IIS Remote Management

១-បើក Server manager

២-នៅក្នុង Roles summary ចុចលើ Web server (IIS)

៣-នៅលើ Web server (IIS) ចុចលើ Add Role serfice

៤-Tick លើប្រអប់ Management Service Checkbox ដូចក្នុងរូបភាព១២-១២



រូបភាពទី១២-១២- Management Service

៥-ចុចលើ Install

៦-ចុចលើ Close

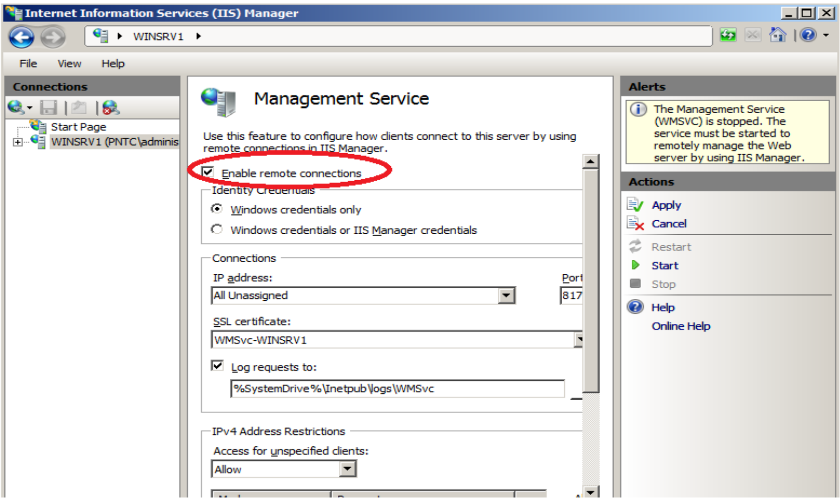
៧-បិទ Server Manager

៨-បើក IIS Manager

៩-ចុចលើឈ្មោះរបស់ Server

១០-ចុចពីរដងស្ទួនលើ Management Service

១១-ចុចលើ Enable Remote Connections checkbox

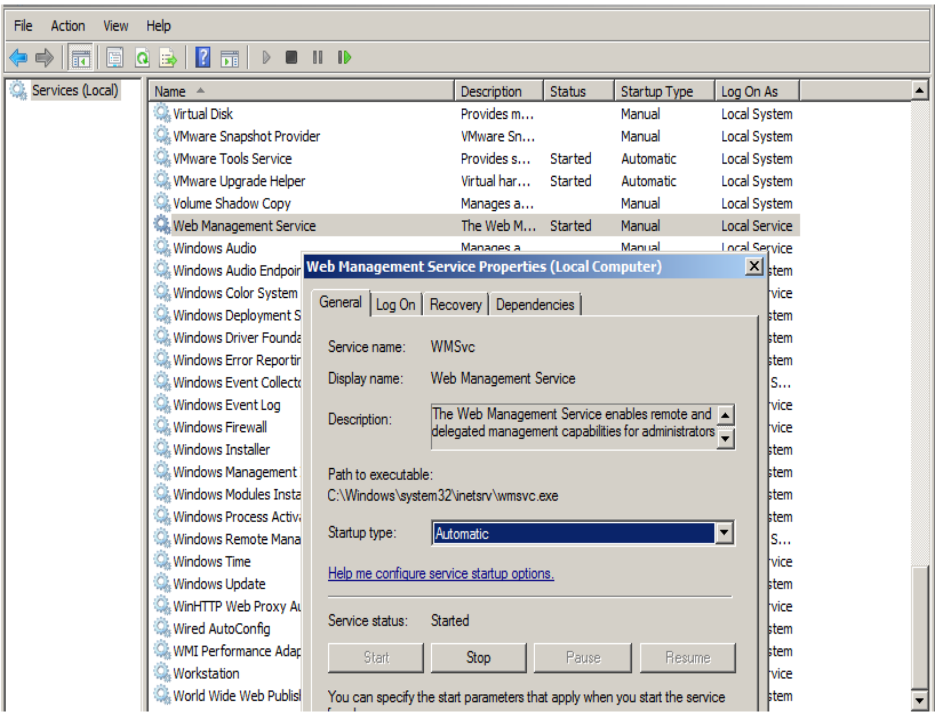


រូបភាពទី១២-១៣-ការបើក IIS remote Management

១២-ចុចលើ Start នៅក្នុង Actions pane ដើម្បី Start Management Service

១៣-Start=>Administrative Tools=>Service

១៤-ចុចពីរដងស្ទួនលើ Web Management Service ហើយបន្ទាប់មកប្តូរពី Manual មកជា Automatic startup ។ ចុចលើ Ok ដើម្បី Save វា។



រូបភាព១២-១៤-ការប្តូរពី Manual មកជា Automatic Startup

១២-៥- File សម្រាប់ Configure IIS 7.0

ចំណុចដ៏សំខាន់មួយបានផ្លាស់ប្តូរក្នុង IIS 7.0គឺវាបានប្រើ File ជំនួសឱ្យ IIS metabase សម្រាប់គ្រប់គ្រងការ Configure Server ។ តាមការពិត ASP.NET និង IIS configuration settings ត្រូវបានបញ្ចូលជា file តែមួយ។ Configuration ត្រូវបានចែកចេញជា ៤ផ្នែកគឺ:

- Machine.config:ការកំណត់នេះនិងមានឥទ្ធិពលទៅលើ Server ទាំងមូលហើយទទួលបានពី .NET និង IIS configuration File ។
- ApplicationHost.config:ការកំណត់នេះបានកំណត់គោលដៅចំពោះ IIS ហើយទទួលបានអ្វីដែលបានកំណត់ពី Machine.config។ File នេះមានទីតាំងស្ថិតនៅទីតាំង%systemroot%\system32\inetsrv
- Web.config(root-level):ការកំណត់ទាំងនេះត្រូវបានចែកចាយដោយ ASP.NET applications នៅលើ Server ហើយវាទទួលបន្តពី Machine.config និង Application.config ។ File នេះត្រូវរក្សាទុកនៅទីតាំង %systemroot%\Microsoft.NET\Framework\versionNumber\CONFIG.
- **Web.config(application-level):**ការកំណត់នេះត្រូវបានប្រើសម្រាប់គ្រប់គ្រងទៅលើ Configuration Settings សម្រាប់ ASP.NET applications ។ វាទទួលបានបន្តពី files ទាំងបី។ File មានទីតាំងស្ថិតនៅដូច File ASP.NET applications ដែរ។

១២-៦- ការចែកការគ្រប់គ្រង (delegate Administration)

នៅពេលយើងនិយាយពី IIS វាមានការគ្រប់គ្រងមួយដ៏អស្ចារ្យគឺអនុញ្ញាតឱ្យយើងអាចផ្លាស់ប្តូរការ Config -ure តាម application នីមួយៗដែលអ្នកបានបង្ហោះនៅលើ server របស់អ្នក។ វាគឺជាភាពអស្ចារ្យមួយដែលអនុញ្ញាតឱ្យអ្នកសរសេរកម្មវិធីអាចកែប្រែទៅតាមតម្រូវការរបស់គេ ហើយយើងនៅតែអាចគ្រប់គ្រងទៅលើស្ថិរភាពនៃ Server ។ ចំពោះ IIS7.0 អ្នកអាចចាក់សោរឬដោះសោរចំពោះផ្នែកផ្សេងៗនៃ Globla Configuration ដូច្នេះវាអាចកំណត់ទៅលើ web.config ។

ការផ្ទេរតួនាទីនៃលក្ខណៈពិសេសដោយប្រើ IIS Manager

វិធីដ៏ងាយមួយនៃការ Configure delegation គឺធ្វើតាមក្រាហ្វិកនៃ IIS Manager។ អ្នកអាច Configure delegation នៅឯកម្រិត Server ដែលការផ្ទេរតួនាទីនេះមានឥទ្ធិពលទៅលើ sites ទាំងអស់នៅលើ Server ឬក៏អ្នកអាចបង្កើត site delegation ចំពោះ Web site ណាមួយពិតប្រាកដបាន។

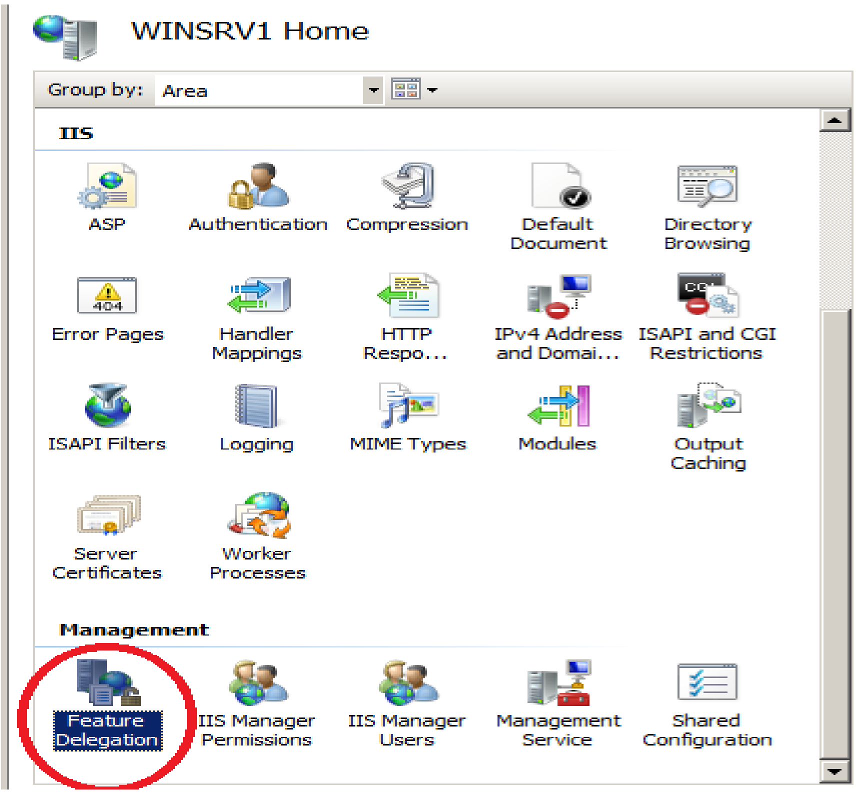
ដើម្បី Configure site delegation យើងអនុវត្តតាមជំហានដូចខាងក្រោម:

១-បើក IIS Manager

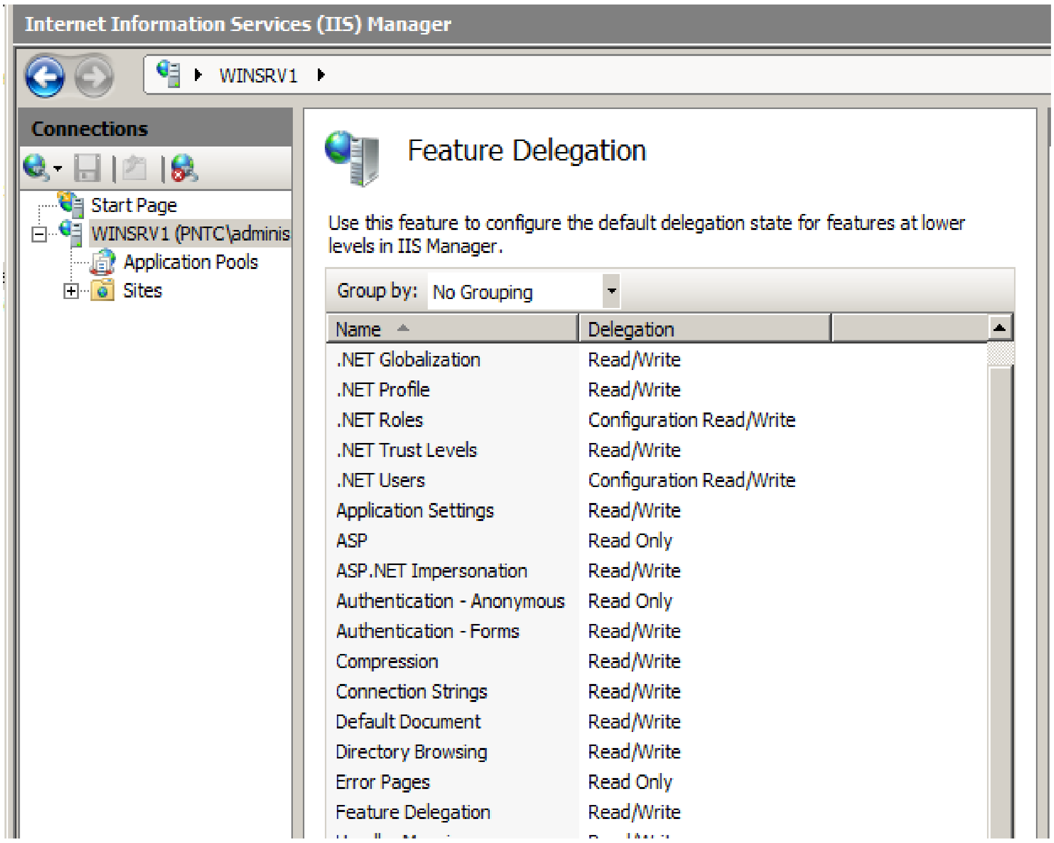
២-ចុចលើ IIS Server

៣-ចុចពីរដងលើ Feature Delegation នៅក្នុង Home pane

៤-ដើម្បីប្តូរ Delegation ចុចពីរដងលើលក្ខណៈពិសេសដែលអ្នកចង់ប្តូរវាហើយបន្ទាប់មកចុចលើ delega -tion state ដែលអ្នកពេញចិត្តនៅក្នុង Action pane ។



រូបភាព១២-១៥-បង្ហាញពី Feature Delegation



រូបភាព១២-១៦-បង្ហាញពី Feature Delegation List

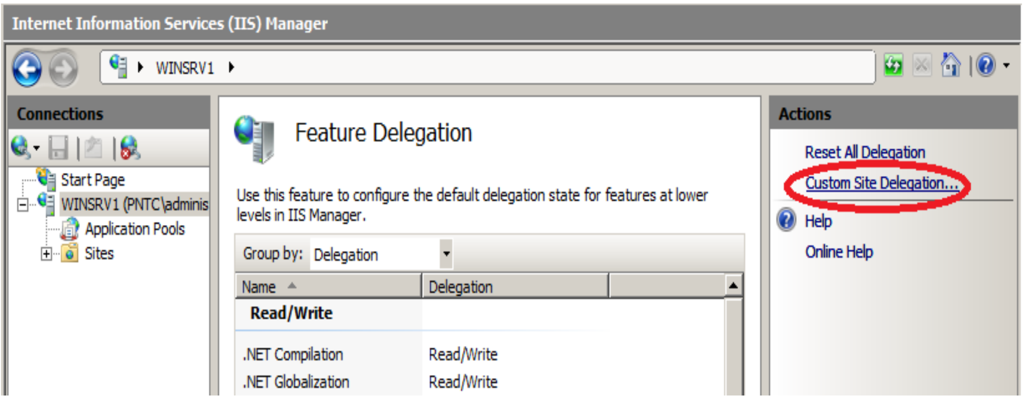
បើអ្នកត្រូវការបង្កើតច្បាប់សម្រាប់ Delegation ចំពោះ Site ណាមួយពិតប្រាកដ អ្នកត្រូវអនុវត្តតាមជំហានខាងក្រោម:

១-បើក IIS Manager

២-ចុចលើ IIS Server នៅក្នុង Connection Pane

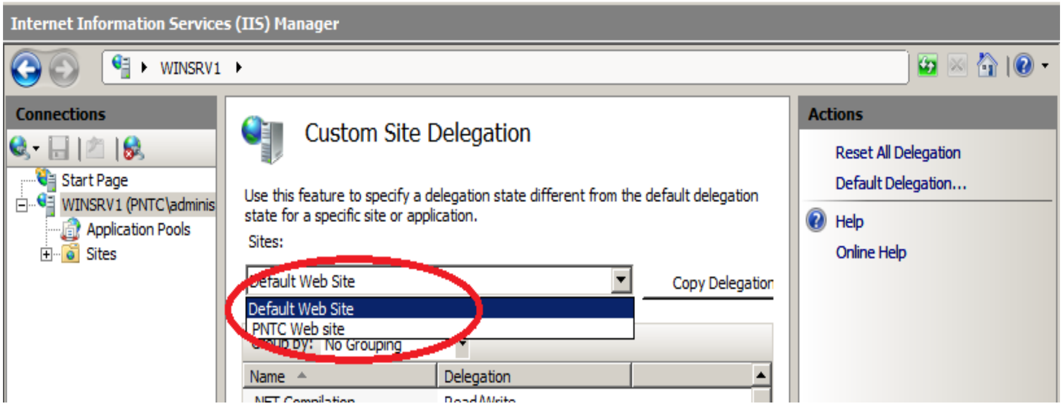
៣-ចុចពីរដងស្ទួនលើ Feature Delegation នៅក្នុង Home Pane របស់ Server

៤-ចុចលើ Custom Web Site Delegation នៅក្នុង Action Pane



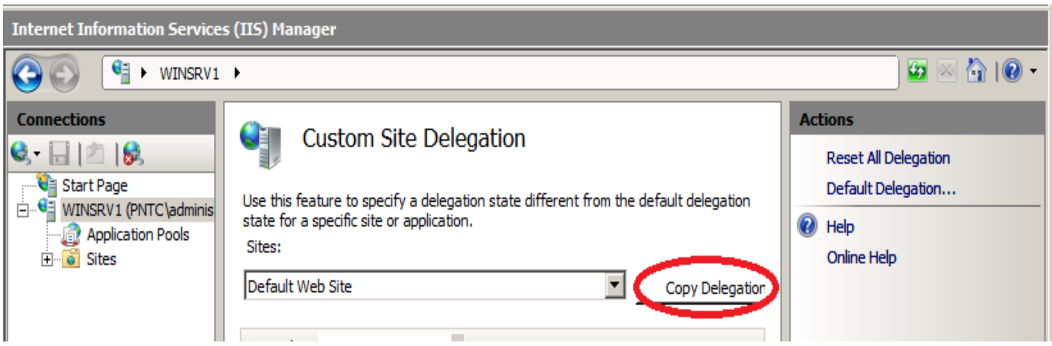
រូបភាព១២-១៧-បង្ហាញពី custom Site Delegation

៥-នៅក្នុងតារាងបង្ហាញពី Site អ្នកត្រូវជ្រើសរើសយក Site ដែលអ្នកចង់ Configure



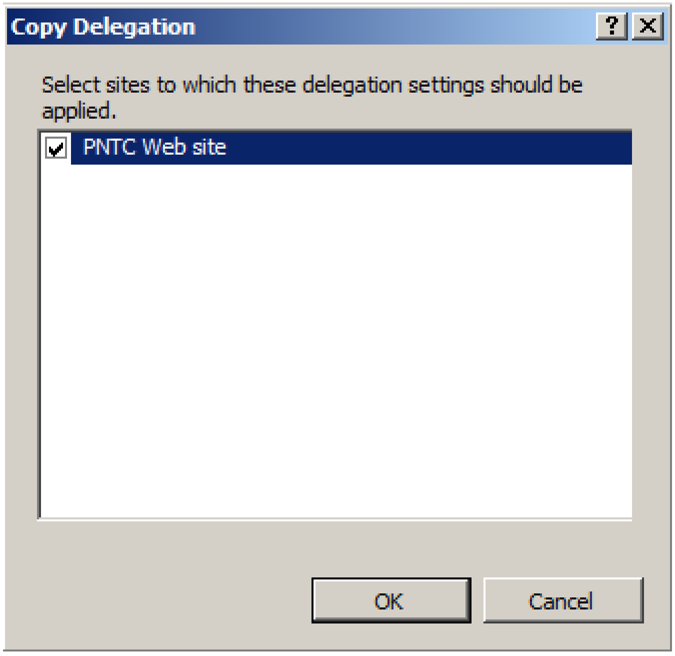
រូបភាព១២-១៨-បង្ហាញពី Web site ដែលអ្នកចង់ Delegate

៦-ជាមួយគ្នានេះដែរ អ្នកអាចធ្វើការផ្លាស់ប្តូរចំពោះ Web sites ជាច្រើនបានដោយអ្នកគ្រាន់តែចុចលើ Copy Delegation ហើយជ្រើសរើសយក Additional Site



រូបភាព១២-១៩-បង្ហាញពី Copy Delegation

៧-Configure នូវ Feature Delegation State ដោយជ្រើសរើសយក Site ដែលអ្នកចង់ Delegate



រូបភាព១២-១៩-បង្ហាញពី delegate ចំពោះ Web site ច្រើន

១២-៧- ការកត់ត្រាទុកជាស្វ័យប្រវត្តចំពោះការស្នើសុំដែលបរាជ័យ

បញ្ហាដែលយើងត្រូវយកចិត្តទុកដាក់ជាមួយ Application គឺការដោះស្រាយបញ្ហានូវពេលវាមានកំហុស (error)កើតឡើង។ ពេលខ្លះវាជាការពិបាកដែលយើងមិនអាចរកឬសគល់នៃបញ្ហាដែលបណ្តាលឱ្យមានកំហុសកើតឡើងដូចជា Application មិនអាចប្រើបានឬបាត់បង់សមត្ថភាពនៃការសម្តែង។ អ្វីដែលយើងត្រូវធ្វើគឺត្រូវធ្វើការកត់ត្រារាល់អ្វីបានកើតឡើងនៅលើ Server ។

ដើម្បីកត់ត្រាវា អ្នកត្រូវអនុវត្តតាមជំហានដូចខាងក្រោម:

១-Tracing ត្រូវតែដំឡើងនៅក្នុង IIS

២-ផ្ទៀងផ្ទាត់ឱ្យដឹងថា FailedRequestTracingModule ត្រូវបានកំណត់នៅក្នុង IIS Manager

៣-បើក Failed Request Tracing

៤-Configure Failure

Setting Up ការកត់ត្រាការស្នើសុំបរាជ័យដោយស្វ័យប្រវត្ត

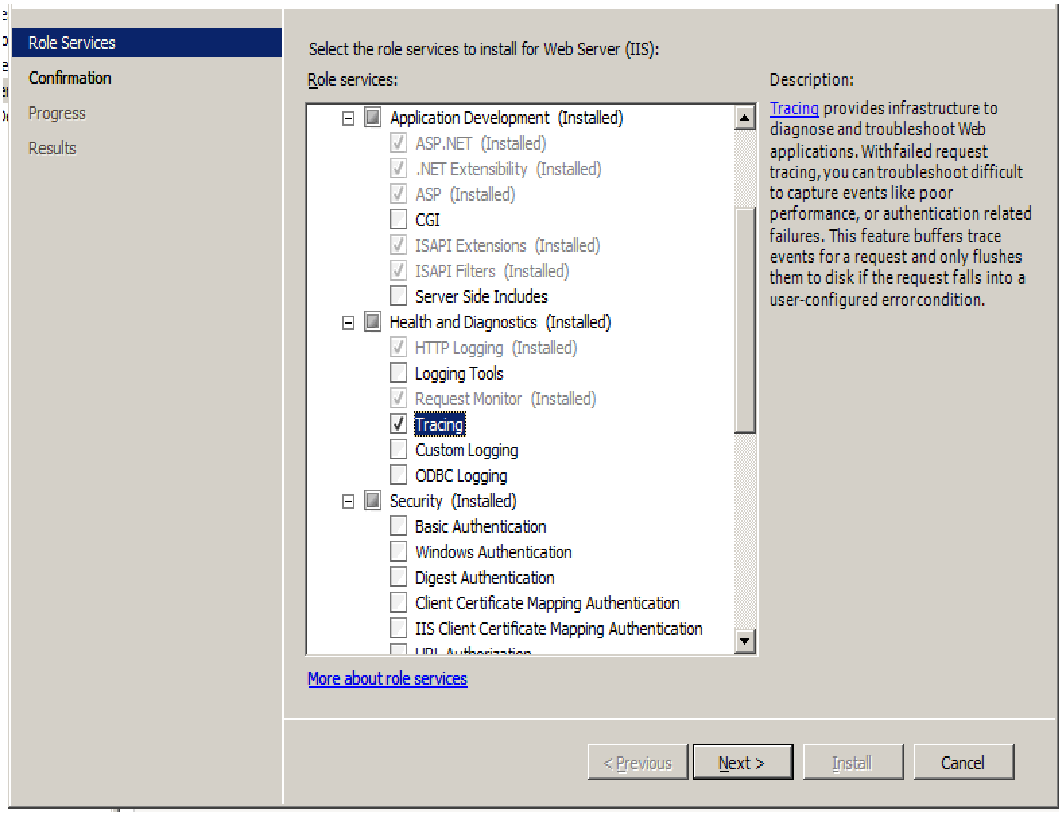
នៅពេលនេះអ្នកនិងដំឡើង IIS Tracing ហើយបន្ទាប់មកអ្នកអាចបើកវាឱ្យដំណើរការហើយនិងបង្កើតនិយមន័យឱ្យការបរាជ័យដែល Server និងប្រើដើម្បីសម្រេចចិត្តបង្កើតការកត់ត្រាចំពោះលក្ខខណ្ឌត្រឹមត្រូវណាមួយ:

១-បើក server Manager

២-ចុចលើ Web server (IIS) នៅក្នុង Roles Summary

៣-ចុចលើ Add Role Service

៤-Tick លើ Tracing ពីតារាងនៃ Role Service ហើយចុចលើ Install

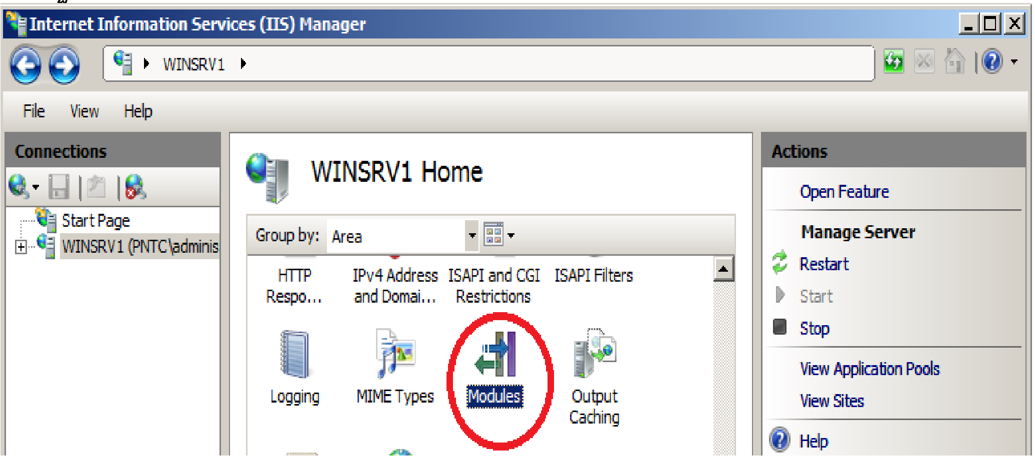


រូបភាព១២-២០-ការជ្រើសរើសយក Tracing ក្នុង Web server

៥-បើក IIS Manager

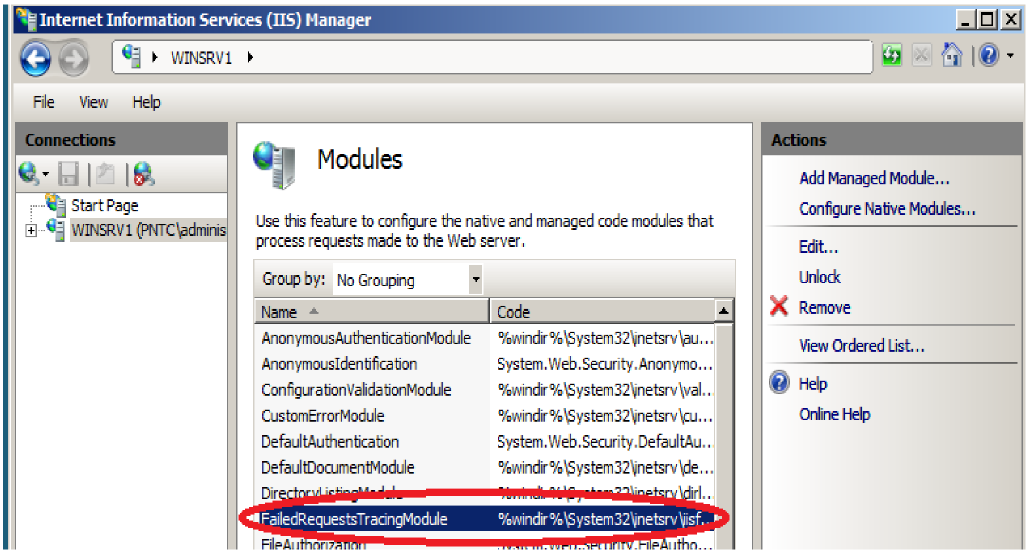
៦-ជ្រើសរើសយក Server នៅក្នុង Connections pane

៧-ចុចពីរដងស្ទួនលើ Modules ពី Feature List



រូបភាព១២-២១-ការជ្រើសរើសយក Modules

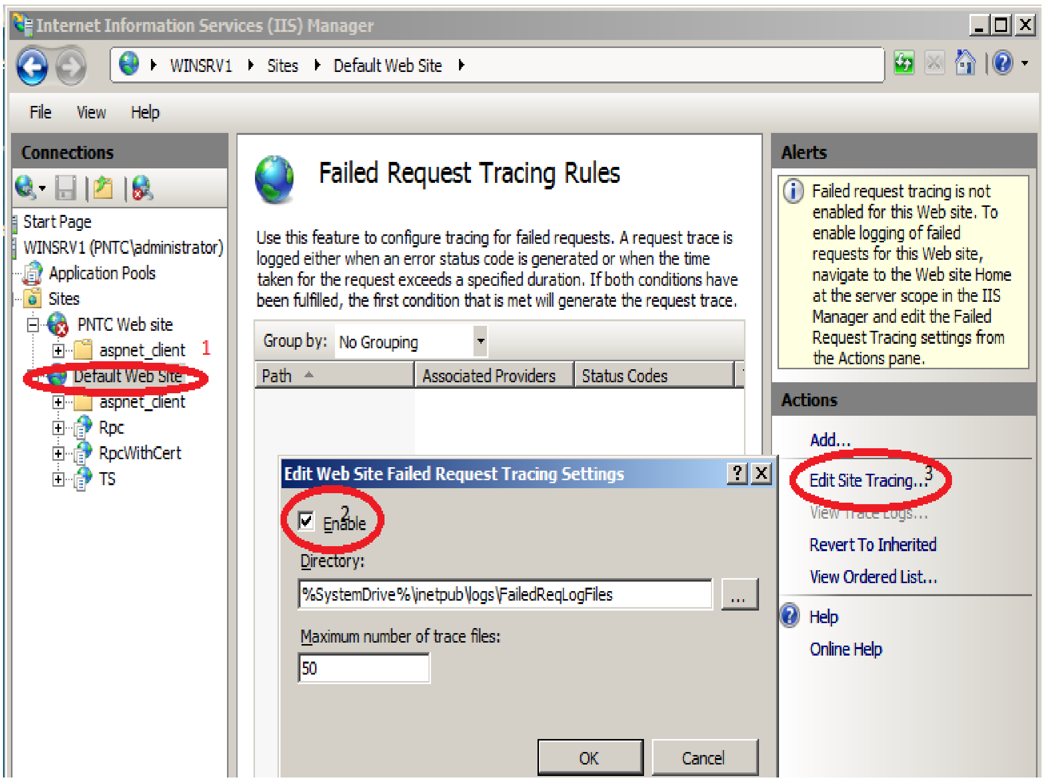
៨-នៅក្នុង Web sites folder ខាងក្រោម Server នៅក្នុង Connection pane ជ្រើសរើសយក Web site ដែលអ្នកចង់បើក Failed request tracing ។



រូបភាព១២-២២-បង្ហាញពី FailedRequestsTracingModule ក្នុង Modules

៩-នៅក្នុង Action Pane ចុចលើ Failed Request Tracing

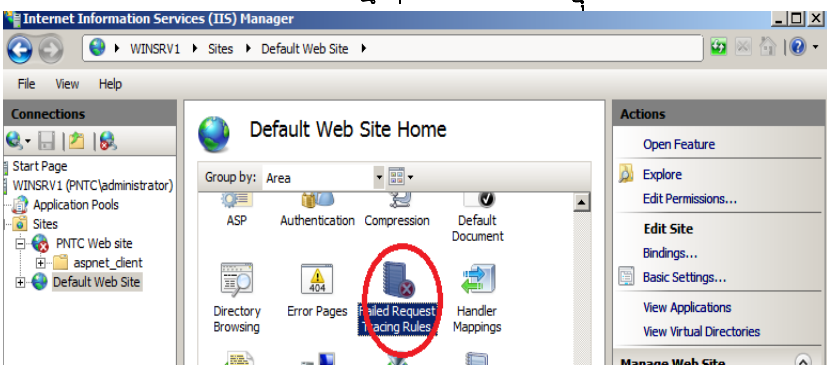
១០-នៅក្នុង Edit Web Site Failed Request Tracing Setting dialog box Tick លើប្រអប់ Enable checkbox



រូបភាព១២-២៣-បង្ហាញពី Edit site Tracing….និង Enable Web site Failed Request Tracing

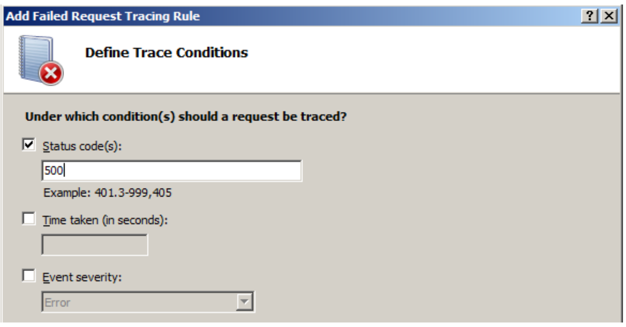
១១-នៅក្នុង Web site Home pane, ចុចពីរដងលើ Failed Request Tracing Rules

១២-ដើម្បីបង្កើត Failed Request Tracing Rule ថ្មី ចុចលើ Add នៅក្នុង Action pane

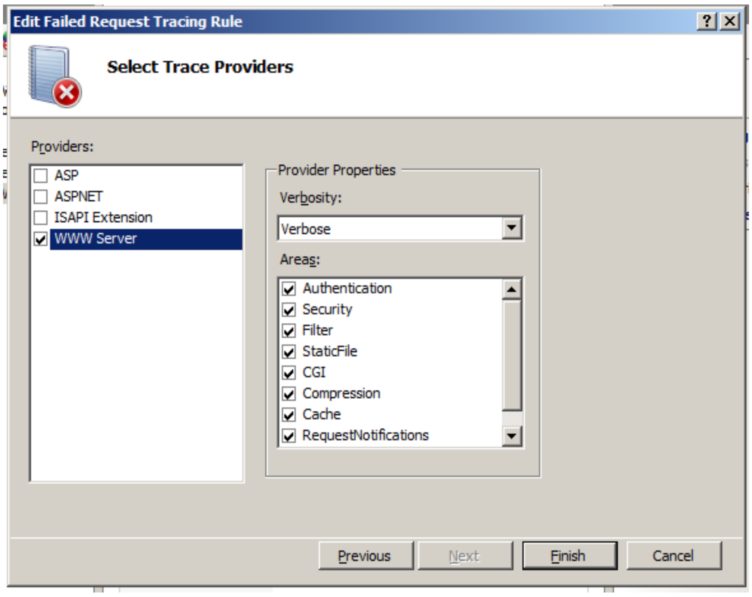


រូបភាព១២-២៤-ការជ្រើសរើសយក Failed Request Tracing Rule

១៣-កំណត់អ្វីដែលអ្នកចង់បានឱ្យវាកត់ត្រា



រូបភាព១២-២៤-កំណត់ Code ដែលចង់បង្ហាញ



រូបភាព១២-២៥-កត់ត្រារាល់ Event ដែលទាក់ទងជាមួយ WWW server

ជំពូកទី១៣

ការគ្រប់គ្រងលើ Resource និងការបង្ហាញពីសមត្ថភាពរបស់ Server

ខ្លឹមសារនៃមេរៀននេះផ្តោតទៅលើផ្នែកពីរសំខាន់ៗគឺ៖

- ការគ្រប់គ្រងលើ Windows System Resource
- ភាពមានទំនុកចិត្តនិងការបង្ហាញពីសមត្ថភាព

ផ្នែកទីមួយគឺផ្តោតទៅលើសញ្ញាណនៃការគ្រប់គ្រងទង្វើរសកម្មភាពរបស់ server ដូចជាការកំណត់ដំណើរការដែលមានលក្ខណៈវិនិច្ឆ័យត្រូវគ្នាគោលការណ៍លៃទុក Resources ប្រតិទិន Accounting លក្ខខណ្ឌនិងការពិនិត្យមើល Resources ជាដើម ។

ផ្នែកទីពីរគឺនិយាយពីការប្រមូល data/metrics នៃទង្វើរសកម្មភាពរបស់ server ដើម្បីធ្វើការតាមដានទង្វើរសកម្មភាពរបស់ server ដែលបាននិយាយពី tools មួយចំនួនគឺ Data Collector Set, ការបង្ហាញឱ្យឃើញពីទំនុកចិត្តនិងរបាយការណ៍។

ផលប្រយោជន៍នៃ Server គឺចែកចាយនូវទម្រង់ខ្លះនៃសេវាដែលជាមជ្ឈមណ្ឌលកណ្តាលសម្រាប់អ្នកប្រើប្រាស់។ Server ចែកចាយ Resources ដែលមានតម្លៃជាដើម។ ពួកវាគឺជាបំណែកសំខាន់នៃហេដ្ឋារចនាសម្ព័ន្ធនៅក្នុងការរៀបចំប្រើប្រាស់ពួកវា។ ទោះបីជាពួកវាមើលមិនឃើញហើយនិងមានសម្តែងនូវភាពស្ងប់ស្ងាត់ក្នុងការដំណើរការសេវា ពួកវាក៏ដោយអ្នកអាចវាយតម្លៃលក្ខណៈសំខាន់ៗយ៉ាងងាយដោយគ្រាន់តែត្រួតពិនិត្យមើលប្រតិកម្មរបស់អ្នកប្រើប្រាស់នៅពេលដែលមានមួយឬច្រើន Server ក្លាយជា Server មិនបានការនិងឆ្លើយតបយឺត Window Admin -istrators វាជាភារកិច្ចរបស់ពួកយើងមិនមែនជាការរ៉ាប់រងដែល Server ធ្វើយ៉ាងប្រាកដនោះទេប៉ុន្តែវាបន្ថែមនូវប្រតិបត្តិនៃសភាពខាងក្រៅរបស់ System របស់យើង លើសពីនេះវាតាមដាននូវសមត្ថភាពនិងការព្យាករណ៍នៃការកើតឡើងអ្វីផ្សេងៗទៀត។ មធ្យោបាយតែមួយគត់ដើម្បីបំពេញនូវគោលបំណងបានជោគជ័យនោះគឺសម្តែងនូវភាពដែលអាចទុកចិត្តបាននិងការត្រួតពិនិត្យមើលសកម្មភាពនៅលើ Server យ៉ាងពិតដល់ប្រាកដមួយ។ នេះគឺជាលក្ខណៈពិសេសប្រាកដសម្រាប់ Application Server ដែលកើនឡើងនៅក្នុងការប្រើប្រាស់លើសម៉ោង។

ឯកត្តាបង្ហាញពីសមត្ថភាពត្រូវស្វែងមើលពេលវេលាសមស្របដូច្នេះនៅពេលដែលទង្វើរសកម្ម ភាពកើតមាននូវបញ្ហា, អ្នកអាចរៀបចំបានយ៉ាងលឿននិងងាយស្រួល Performance Profile ជាមួយរបាយការណ៍ Profile នៅពេលមុនៗដើម្បីកំណត់នូវអ្វីដែលកើតឡើងខុសពីធម្មតា។ Monitor របស់ System Performance របស់អ្នកគឺជាវត្ថុមួយប៉ុន្តែការគ្រប់គ្រង Performance នោះជារឿងមួយផ្សេងទៀត។ Window Server 2008 បានបញ្ចូលនូវ Window System Resource Manager (WSRM),ណាមួយដែលមានការចាប់ផ្តើមនៅក្នុង Window Server 2003 Enterprise ហើយនិង Datacenter Edition។ Toolsទាំងនេះអាចប្រើដើម្បីកែសំរួលនូវPerformance របស់Serverរបស់អ្នកដោយអនុញ្ញាតឱ្យអ្នកកំណត់នូវការចែក CPU ហើយនិងធនធាន Memory ទុក។ Window Server 2008 រួមបញ្ចូលនូវទំនុកចិត្តហើយនិងការបង្ហាញពីសមត្ថភាពណាមួយដែលធ្វើឱ្យប្រសើរឡើងនូវជំនាន់នៃការបង្ហាញពីសមត្ថភាពដែលមិនអាចធ្វើបាននៅWindowជំនាន់មុនៗ។

ប្រសិនបើអ្នកធ្វើការជាមួយនឹងភាពមានទំនុកចិត្តហើយនិង tools ដែលប្រមូលផ្តុំពីការបង្ហាញសមត្ថភាពអ្នកនឹងរកឃើញថាវាគឺពិបាកប្រមូលផ្តុំអ្វីដែលជាទិន្នន័យជាច្រើន។ ជួនកាលទិន្នន័យដែលអ្នកប្រមូលបានគឺមិនដូចនូវអ្វីដែលចង់បាន។

ឧទាហរណ៍

ប្រសិនបើអ្នកធ្វើការនៅក្នុងមជ្ឈដ្ឋានដែលធ្លាប់ធ្វើជាច្រើន និងការកើនឡើងឆាប់រហ័សនោះអ្នកប្រហែលជានឹងមិនចំណាយពេលច្រើនដើម្បីទៅធ្វើតាមការអនុវត្តរបស់អ្នកទៀតទេ។ ដូច្នេះក្នុងរយៈមួយហើយនិងនៅពេលដែលអ្នកបញ្ចប់នូវការប្រមូលឯកត្តាវាស់សមត្ថភាព អ្នកប្រហែលជាគិតថា Servers របស់អ្នកធ្វើហួសសមត្ថភាពដូចជាអ្នកអញ្ចឹងដែរ។ បំនែកតូចៗជាច្រើនត្រូវបានរៀបចំប្រើការប្រមូលផ្តុំ metrics ,tools ទាំងនោះយកចេញនៅពេល Administrator កំពុងធ្វើឱ្យមានបញ្ហាកាន់តែធ្ងន់ធ្ងរដូចជានៅពេលដែល application server សម្តែងនូវភាពមិនចុះសំរុង។

ផ្នែកដ៏សំខាន់បំផុតនោះប្រសិនបើអ្នកប្រមូលផ្តុំ ហើយនិងមាននិន្នាការលើទិន្នន័យរបស់អ្នកជាមុនអ្នកអាចរកដំណោះស្រាយវិជ្ជមានដ៏ល្អមុនពេលពួកវាក្លាយជាបញ្ហា។ នៅក្នុងសភាពនេះគឺភាពមានទំនុកចិត្តហើយនិងឯកត្តាវាស់សមត្ថភាព។ ការប្រមូលព័ត៌មានគឺមូលដ្ឋាននៃការគ្រប់គ្រង System ជាមុន។ ប្រសិនបើអ្នកត្រូវបានទទួលការគ្រប់គ្រង Server បានតិចតួចបំផុតនោះអ្នកប្រហែលពេញចិត្តនូវអ្វីដែលទិន្នន័យបង្ហាញឱ្យអ្នកឃើញនោះទេ យ៉ាងហោចណាស់អ្នកមានព័ត៌មានអ្នកត្រូវការបង្កើតការសម្រេចចិត្តដ៏ល្អអំពីកន្លែងផ្ទុកព័ត៌មាននោះ ដើម្បីកំណត់នូវការយកចិត្តទុកដាក់របស់អ្នក។ ជាព័ត៌មានដែលជះឥទ្ធិពលលើកការគ្រប់គ្រងនូវអ្វីដែលអ្នកត្រូវការចំណាយប្រាក់លើតម្រូវការនិងធនធានផ្សេងៗ។ អ្នកអាចបន្ថែមនូវគម្រោងការជាមួយនឹងបង្ហាញទិន្នន័យតាមបៀបប្រកបដោយសមត្ថភាព ។

Server គឺការបង្រួញនិងបញ្ហាដែលអាចកើតមានឡើងប្រសិនបើបញ្ហានេះមិនត្រូវបានដោះស្រាយ។ សរុបមកវាមានសារៈសំខាន់ណាស់ដែលពួកយើងមានឯកត្តាវាស់សមត្ថភាពដ៏ល្អដើម្បីដឹកនាំទិន្នន័យនៅក្នុង Server ណាមួយហើយ Server ទាំងប៉ុន្មានអាចជា Hostនៅលើ host node តែមួយគត់។

១៣-១- អ្នកគ្រប់គ្រងលើ WINDOWS SYSTEM RESOURCE

Windows System Resource Manager គឺជាផ្នែកមួយនៃ Windows Server 2003 Enterprise ហើយនិង Datacenter editions ហើយស្ថិតនៅលើ CD ដាច់ដោយឡែក។ នៅក្នុងWindows Server 2008 Enterprise ,WSRM គឺជាផ្នែកមួយនៃ Windows Server 2008 Enterprise និង Datacenter editions ភាពខុសគ្នាសំខាន់ៗរវាងជំនាន់ចាស់និងថ្មី WSRMអាចដំឡើងដោយផ្ទាល់លើServer Manager interface ដើម្បី run វាពីឌីសដាច់ដោយឡែក។ WSRM ដូចជាប្រភេទ "គោលការណ៍ Resources" ក្នុងចំណោម Process ផ្សេងៗគ្នានៅក្នុង System របស់អ្នក។ វាអនុញ្ញាតឱ្យអ្នកគ្រប់គ្រងកំណត់ការបញ្ជាលើ Process នីមួយៗដូចជាថាតើ CPU និង Memory ប៉ុន្មានដើម្បីប្រើប្រាស់លើ Process នីមួយៗហើយបន្ទាប់មកធ្វើតាមការបញ្ជានោះដូច្នេះ application មួយឬ process អាចប្រើប្រាស់បានតែទៅតាមការកំណត់បរិមាណរបស់ resources ថាតើវាគ្រប់គ្រាន់ឬអត់។ការដាក់បញ្ជាអាចបណ្តាលឱ្យ Process ដាក់លាក់មួយណាដើម្បីដំណើរការទៅតាមកាបញ្ជាទៅលើវាប៉ុន្តែយ៉ាងហោចវានិងមិនអនុញ្ញាត Process សន្ធប់ទៅលើ Server និងធ្វើឱ្យមានបញ្ហាជាមួយ Process ដទៃទៀតដែរ។

WSRM ផ្សំដោយឬមានឥទ្ធិពលលើគ្នាទៅវិញទៅមកជាមួយនឹងសមាសធាតុដែលផ្សេងៗគ្នាចំនួន៩រាប់បញ្ចូលទាំង Management interface មួយ information stores,schedulers និង manager។ តារាងខាងក្រោមបង្ហាញនូវសមាសធាតុនិងពិពណ៌នានៃសមាសធាតុនីមួយៗ

សមាសធាតុ	**ពិពណ៌នា**
WSRM console	Graphical interface ប្រាប់សម្រាប់គ្រប់គ្រងនិង Monitor WSRM ។
Distributed Component Object	Remote APIs ប្រើសម្រាប់ទាក់ទងរវាង Client និង WSRM Service ។
Model (DCOM) interface	
WSRM service	Service ចម្បងដែលដំណើរការលើការងារលើការគ្រប់គ្រង resource ។ ការងាររបស់វាគឺតាមដាន process និងរៀបចំសម្រាប់ការពារឱ្យសមស្របទៅតាមច្បាប់ប្រសិនបើមួយហួសនិងការលៃទុក resource វានិងធ្វើលុះត្រាតែ process គោរពតាមការកំណត់បែងចែកនៃResource
Accounting database	ផ្ទុកពត៌មានអំពីការគ្រប់គ្រង Process នៅលើគ្រឹះ Per-Process មួយ ។
Policy store	ផ្ទុកច្បាប់ទាំងអស់និង Resource និង resource ត្រូវនិងលក្ខខណ្ឌវិនិច្ឆ័យដែលបានកំណត់ក្នុងWSRM ។
WSRM settings	ផ្ទុកនូវ Current Management Settings ។
Calendar	ផ្ទុកព្រឹត្តិការណ៍ដែលទាក់ទងនឹងប្រតិទិនទាំងអស់ ។
Memory Manager	គ្រប់គ្រងលើការកំណត់ Memory ដើម្បីគ្រប់គ្រងលើProcess ។
Kernel Scheduler	មូលដ្ឋានគ្រឹះProcessនៅលើច្បាប់WSRM ។

Processes ដែលអាចគ្រប់គ្រងបានប្រៀបធៀបជាមួយ Processes ដែលមិនអាចគ្រប់គ្រងបាន

ប្រភេទនៃ WSRM គឺគ្រប់ដំណើការទាំងអស់មួយណាក៏បានដែលអាចគ្រប់គ្រងបាននិងមិនអាចគ្រប់គ្រងបាន។

Processes ដែលអាចគ្រប់គ្រងបានគឺជាគ្រប់ដំណើការទាំងអស់លើកលែងការត្រួតពិនិត្យដោយ WSRM។ ទាំងនេះគឺរួមបញ្ចូលទាំង process ទាំងឡាយណាមិនត្រូវគ្នាជាមួយនិងការវិនិច្ឆ័យសម្រាប់ប្រោះ Processes ឬមិនរាប់បញ្ចូលដំណើការ។ ការព្យាយាមកំណត់ប្រព័ន្ធដំណើការនៃការប្រើប្រាស់ WSRM ដែលជាលទ្ធផលធ្វើឱ្យប៉ះពាល់ទៅលើ Server របស់អ្នក។ ពីព្រោះតែចំនុចនេះ WSRM បានបញ្ចូលនូវការលើកលែងនៃបណ្ដុំដែលសម្រេចដោយ System។ បញ្ជីទាំងនេះមិនអាចកែប្រែបាន ហើយចំនួននៃដំណើការត្រូវបានកំណត់ដោយ Microsoft ដ៏សំខាន់ក្នុការដំណើការភាពជាចម្បងនៃ operating system ហើយ file ទាំងនេះមិនត្រូវបានគេកាត់បន្ថយឡើយ។ Processes ទាំងនេះមានដូចខាងក្រោម៖

- Csrss.exe
- Dumprep.exe

- Lsass.exe
- Msdtc.exe
- Services.exe
- Smss.exe
- Spoolsv.exe
- Taskmgr.exe
- Winlogon.exe
- Wmiprvse.exe

WSRM Service

ផ្នែកសំខាន់នៃ WSRM គឺជា WSRM Service។ ក្នុងនាមជាកំលាំងចលករនៃ WSRM វាកំណត់ចំនួន Processរបស់ Server របស់អ្នកនឹងប្រៀបធៀបវាទៅនិងគោលការណ៍នៃច្បាប់ដែលត្រូវគ្នាដែលមានស្រាប់។ វាក៏មានទទួលខុសត្រូវលើការត្រួតពិនិត្យការប្រើប្រាស់នៃ Resource របស់ CPU និង RAM ដូច្នេះវាអាចគ្រប់គ្រងលើ Process ដែលហួសនិងកម្រិតនៃផលប៉ះពាល់។ នៅពេលណាដែល process ថ្មីមួយត្រូវបានរកឃើញ WSRM Service នឹងប្រៀបធៀប process នោះនឹងតារាងនៃ process ដែលរាប់បញ្ចូលឬមិនរាប់បញ្ចូលដោយប្រើ algorithm ត្រូវនិងអាទិភាពដែលដើរតាមលក្ខខណ្ឌវិនិច្ឆ័យអាទិភាពដែលអ្នកបានកំណត់ច្បាប់ក្នុង policy របស់អ្នក។ បើមិនត្រូវគ្នាទេ process នោះ ត្រូវបានដាក់ចូលដោយស្វ័យប្រវត្តទៅក្នុង default group ហើយនិងត្រូវបានត្រួតពិនិត្យដោយ Default group។ Default group ត្រូវបានគេបែងចែក Resource ដោយមិនបានប្រាប់ដោយគោលការណ៍នៃការគ្រប់គ្រង់ដោយការបែងចែកនោះស្មើគ្នាក្នុងចំណោម Default group process ទាំងអស់។ បើ WSRM service រកឃើញ process ដែលត្រូវគ្នានឹងច្បាប់ក្នុងតារាង process process ថ្មីនោះត្រូវបានចាត់ទុកចូលក្នុងក្រុមជាមួយនឹង process ផ្សេងទៀតដែលត្រូវគ្នានឹងលក្ខណៈវិនិច្ឆ័យដូចគ្នានោះ។ ហើយក៏ត្រូវបានដាក់ក្រោមច្បាប់នៃ utilization ដែលត្រូវបានកំណត់នៅក្នុងគោលការណ៍នោះ។ តារាងនៃ process ដែលកំពុងដំណើរការនោះក៏ត្រូវបានត្រួតពិនិត្យម្តងទៀត បើសិនមានការប្រែប្រួលណាបានកើតឡើងទៅលើដំណើរការដែលត្រូវនិងលក្ខខណ្ឌវិនិច្ឆ័យឬក៏ទៅលើគោលការណ៍លែទុកដែលសកម្មឡើង។ នៅពេលណាដែល process មួយដែលហួសទៅនឹងការលៃ resource ទុកជាគោលដៅ វាក៏ត្រូវបានដាក់នៅក្រោម algorithm គ្រប់ គ្រងលើអាទិភាព Process ស្វ័យប្រវត្តដែលផ្លាស់នូវ resource រវាង process នឹង process និងផ្អែកទៅលើ process អទិភាពដែលកំណត់រួចជាស្រេចម្តងទៀត

<u>លំហាត់អនុវត្តន៍</u> «ការដំឡើង WSRM»

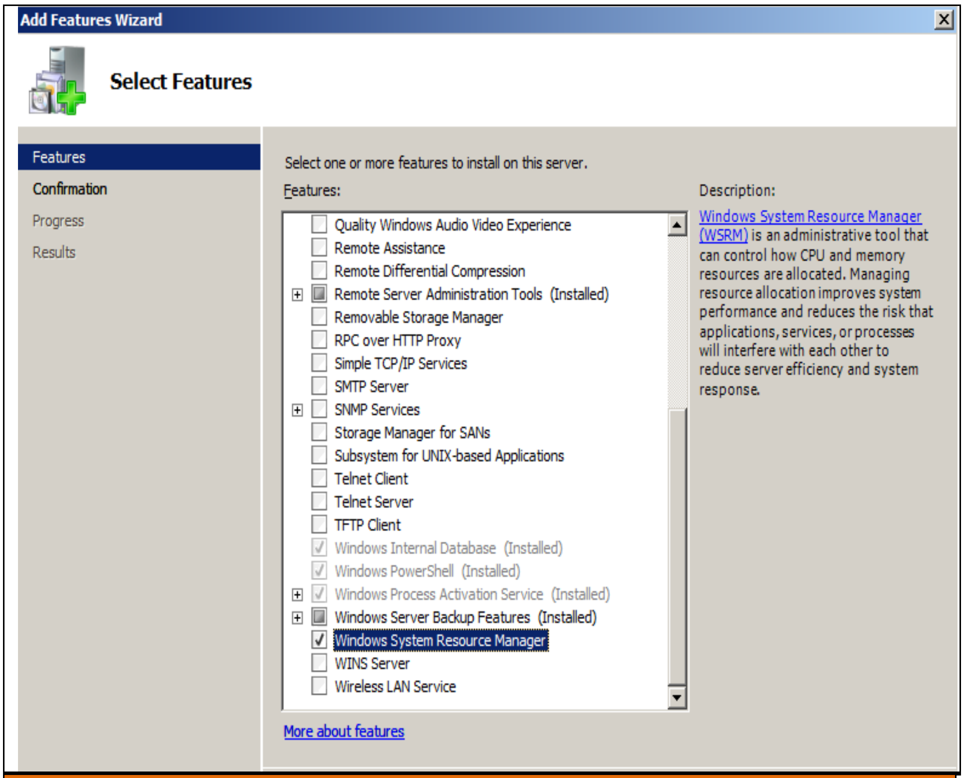
WSRM មិនមែនជា Service role ទេ។ ផ្ទុយទៅវិញ វាគឺជា លក្ខណៈពិសេសដែលអត់មានក៏បាន ដែលអាចត្រូវបានដំឡើងទៅលើ Machince Server ដែលមាន OS ជា Server 2008។ ដើម្បីដំឡើង WSRM ចូលធ្វើតាមជំហានខាងក្រោម៖

<u>ជំហាននៃការអនុវត្តៈ</u>

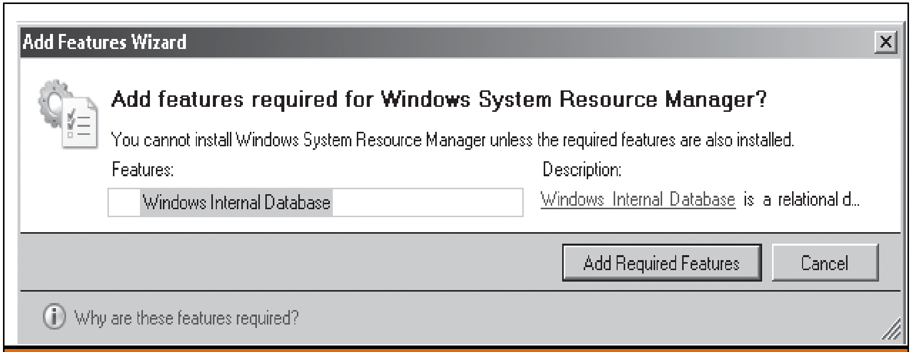
១. បើកឱ្យដំណើរការ Server manager

២. ចុច Linkនៃ Add feature ដើម្បីបើកនូវផ្ទាំង Add feature wizard

៣. ចូល Windows System Resource manager (ដូចរូបភាព៧-១)។ ចូរចុចលើ Add Required feature (ដូចរូបភាព៧-១) ប្រសិនបើវាទាមទារឱ្យដំឡើង Windows Internal Database ដែលវាតម្រូវឱ្យ WSRM ដំណើរការ។ ចុច Next ។



រូប ៧-១. ការរើសយកនូវ Windows System Resource manager



រូប ៧-២. ការបន្ថែមនូវ Windows Internal Database

៤. Confirm the Installation Options បន្ទាប់មកចុច Install ។

៥. ចុច Close នៅពេល installation រួចរាល់ ។

៦. Reboot server រឺ start Window system Resource Manager service ប្រសិនបើវាមិនទាន់បានចាប់ផ្តើម។ WSRM console អាចប្រើបានក៏ដោយសារការជ្រើសយក start រួចយក Administrative Tools បន្ទាប់មកយក Windows System Resource Manager ។

WSRM Management Interface

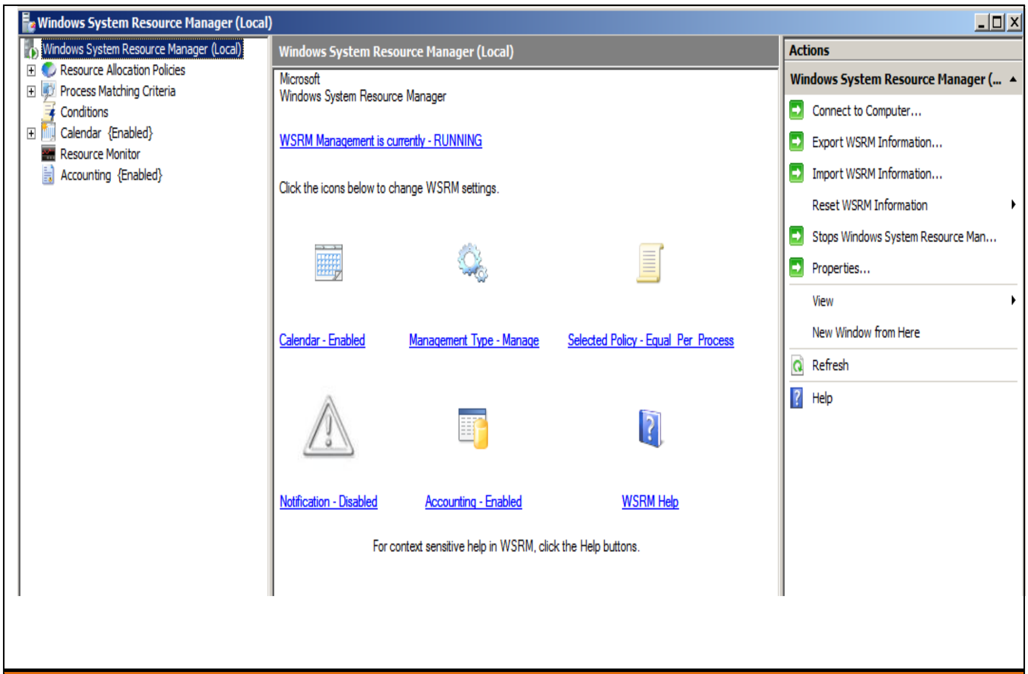
Windows Server 2008 សុទ្ធតែជា interfaces ដែលបានកំណត់គោលដៅការងារ ដូច្នេះវាមិនធ្វើឱ្យភ្ញាក់ផ្អើលទេ នៅពេលយើងបើក WSRM management interface ។ យើងនឹងឃើញ interface មានបីផ្នែកតូចៗស្រដៀងទៅនឹង IIS 7.0 management interface ដូចរូបភាព៧-៣ ត្រូវបានបង្ហាញ។ pane ខាងឆ្វេងគឺជា Navigation pane ធ្លាប់បានប្រើសម្រាប់ access ទៅកាន់សមាសធាតុផ្សេងៗនៃ WSRM ។ ម្យ៉ាងវិញទៀត pane ដែលនៅកណ្តាលត្រូវបានស្គាល់ថាជា Home pane គឺជា primary interface ដែលជាកន្លែងសម្រាប់ configuration information ត្រូវបានបង្ហាញនិងអាចធ្វើការគ្រប់គ្រងបាន។ pane ខាងស្តាំគឺជា context-sensitive Action Pane ។

នៅពេលយើងភ្ជាប់ទៅកាន់ WSRM-enable server ជាលើកដំបូង យើងនឹងឃើញតារាងសង្ខេបមួយដែលបង្ហាញនូវលក្ខណៈ WSRM ដែលកំពុងដំណើរការឬបញ្ឈប់ក៏ដូចជា links ភ្ជាមជាមួយសមាសធាតុ ផ្សេងៗដែលបង្កើតបានជា WSRM ។

ឧទាហរណ៍:

វានឹងបង្ហាញថាតើ Calender, Notification ឬ Account component មួយណាដែលអាចធ្វើបាននិងវាផ្តល់ links ដើម្បីធ្វើការប្តូរគ្រប់ settingទាំងនោះ។

នៅក្នុងជំពូកនេះ រួមផ្សំនូវចំណាក់ថ្នាក់នៃ configuration សំខាន់ៗនីមួយៗក្នុង WSRM ដូចជា: គោលការណ៍កំណត់ Resource លក្ខខណ្ឌនៃប្ល័យលើ Process លក្ខខណ្ឌ ប្រតិទិន Resource Monitor និង Accounting ។ បើសិនយើងមិនទាន់ពិនិត្យមើលវាទេ WSRM ក៏មិនអាចត្រូវបានសម្រាប់កំណត់លើគោលការណ៍កំណត់ resource វាក៏អាចប្រើជា monitor resource utilization ដែរ ។



រូប ៧-៣. WSRM management interface

Resource Monitor នៅក្នុង navigation pane អ្នកនឹងឃើញinterfaceដែលអ្នកធ្លាប់បានឃើញ ក្នុង home pane។ ជាការពិតណាស់ Resource Monitor ផ្នែកភាគច្រើនគ្មានអ្វីដែលថ្មីជាង versionដែលរួមបញ្ចូលគ្នានៃ

Performance Monitor ចាស់ដែលប្រើនៅក្នុង version ពីមុនៗនៃWindows ដែលរួមជាមួយការបន្ថែមផ្នែកខ្លះៗទៀតបញ្ចូលគ្នា។

Process ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យ

Process ដែលត្រូវនិងលក្ខខណ្ឌវិនិច្ឆ័យគឺមានសារៈសំខាន់ណាស់ ព្រោះវាធ្វើការកំណត់ន័យឱ្យគោលការណ៍ជំច្បាស់លាស់មួយដែលនឹងត្រូវដាក់បញ្ចូលទៅកាន់ Process។ Process ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យមានចំនួនពីរដែលបញ្ជាក់អត្ថន័យជាស្វ័យប្រវត្តដោយប្រព័ន្ធគឺ Residual និង IISApool ។ Residual ភ្ជាប់ជាមួយនឹងគ្រប់ process ទាំងអស់ ហើយក៏អាចត្រូវបានប្រើវា ប្រសិនបើអ្នកចង់ឱ្យគោលការណ៍របស់អ្នកដាក់បញ្ចូលទៅគ្រប់ process running system របស់អ្នក។ IISAppPool ភ្ជាប់ជាមួយនិង IIS application pool worker processes ។ វាពិតជាមានប្រយោជន៍ណាស់ បើសិនជាមាន IIS ត្រូវបាន install ហើយបើអ្នកចង់បង្កើតនូវ Policy ទាំងឡាយដែល resource IIS worker processes មាន។ លក្ខខណ្ឌវិនិច្ឆ័យអាចផ្អែកលើផ្លូវទៅ file, command line រឺលើ users និង groups ហើយអ្នកអាចគ្រប់គ្រងនូវអ្វីដែលដាក់បញ្ចូល រឺ មិនដាក់បញ្ចូល។

ឧទាហរណ៍:

អ្នកអាចបង្កើតគោលការណ៍មួយដើម្បីដាក់ឱ្យដំណើរការទៅគ្រប់ account ដែលមាននៅក្នុងក្រុម User Local ប៉ុន្តែមិនត្រូវបានដាក់បញ្ចូលទៅក្នុង Local Administrator account នោះទេ។

Process ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យគឺមិនអាចប្រើខ្លួនវាដោយផ្ទាល់ទេ។ អ្នកអាចគិតថា ពួកវាដូចជា process filters ដែរ។ អ្នកអាចបង្កើតពួកវាប៉ុន្មានក៏បានតាមតែអ្នកចង់បង្កើត ប៉ុន្តែពួកវាមិនអាចធ្វើដំណើរការបានអ្វីទាំងអស់រហូតទាល់តែអ្នកបានកំណត់ពួកវាឱ្យស្របទៅកាន់គោលការណ៍។

សម្រាប់ Processes ដែលបានផ្ទៀងផ្ទាត់រកដោយប្រើប្រាស់ files រឺ command lines ដែលបានដាក់បញ្ចូល នោះជាដំបូង WSRM ព្យាយាមភ្ជាប់ដោយផ្អែកលើឈ្មោះ process ។ បើសិនមានការឆ្លោះឆ្លោយវានឹងប្រៀបធៀបរវាងផ្លូវដែលបានកំណត់ច្បាស់លាស់នឹង filena-mes។ ជាចុងក្រោយ វានឹងប្រៀបធៀបជាមួយនឹង file ដែលមាន Process ពេញលេញ។ ប្រសិនបើមានការភ្ជាប់នោះ ត្រូវបានរកឃើញនៅក្នុង files ដែលបានដាក់បញ្ចូលនោះ WSRM នឹងធ្វើការត្រួតពិនិត្យមើល files listដែលបានដកចេញនោះ។ វាមានសារៈសំខាន់ណាស់គឺតាំងពី process អាចត្រូវបានភ្ជាប់ដោយសារតែ wildcard filter ប៉ុន្តែក៏អាចត្រូវបានដកចេញយ៉ាងជាក់លាក់ដោយ administrator ។ បន្ទាប់មកទៀត រវាង file ដែលដកចេញនោះ វានឹងគោរពទៅតាមអ្វីដែលដូចទៅនឹង matching procedure entries ទូទៅសម្រាប់ដាក់បញ្ចូល files entries ។

ចំពោះ process ដែលបានផ្ទៀងផ្ទាត់រកដោយ Users និង groups WSRM នឹងប្រៀបធៀប account ដែលធ្លាប់បានបង្កើត process រវាងតារាងនៃ users និង groups។ នេះគឺជាលើកដំបូងហើយ ក្នុងការប្រើប្រាស់ User account ដែលត្រូវគ្នាតែមួយគត់ដែលទទួលជោគជ័យ។ ប្រសិនបើវាមិនជោគជ័យទេ WRSM នឹងប្រៀបធៀប User account ជាមួយ ភាពជាសមាជិករបស់គ្រប់ក្រុមដែលបានបញ្ជាក់ច្បាស់ ។ បើការភ្ជាប់នេះត្រូវបានរកឃើញនោះការប្រៀបធៀបរវាង user ដែលបានដកចេញនិងតារាងនៃក្រុមគឺត្រូវបានចាត់ចែងបន្តទៅកាន់ប្រោះគ្រប់ process ដែលមិនបានដាក់ចូលដោយផ្អែកលើច្បាប់ទាំងអស់នោះ។

គ្រប់ការវិនិច្ឆ័យនៃការប្រោះដែលដាក់បញ្ចូលទាំង file និងការវិនិច្ឆ័យដែលត្រូវនិងបញ្ជា និង user និង groups ដែលត្រូវនិងការវិនិច្ឆ័យយើងត្រូវវាយតម្លៃទាំងពីរនេះដោយត្រួត ពិនិត្យឱ្យបានសព្វគ្រប់ដើម្បីដាក់បញ្ចូល។

ឧទាហរណ៍

បើសិនអ្នកបង្កើត process ដែលត្រូវនិងលក្ខខណ្ឌវិនិច្ឆ័យដើម្បីស្វែងរក process MyService.exe ហើយក៏កំណត់ជា user ជា BUILIN\Administrator។ មានតែ MyService.exe processesទេ បានធ្វើឡើងដោយសារ BUILTIN\Administratorដែលនឹងត្រូវបានដាក់បញ្ចូល។ ប្រសិនបើគ្រប់ user ដទៃទៀតចាប់ផ្តើមធ្វើ MyService.exe គឺវាមិនត្រូវបានដាក់បញ្ចូលហើយវានឹងត្រូវផ្លាស់ប្តូរទីកន្លែងនៅក្នុងdefault group ។

> **ចំណាំ៖** ឈ្មោះរបស់លក្ខខណ្ឌវិនិច្ឆ័យមិនអាចចាប់ផ្តើមដោយសញ្ញា(-) និងដកឃ្លា រឺក៏សញ្ញាដទៃទៀតដូចជា: \ / ? * | : < > , ; ... ។

លំហាត់អនុវត្ត៖ «ការបង្កើត Process ដែលត្រូវនិងលក្ខខណ្ឌវិនិច្ឆ័យ»

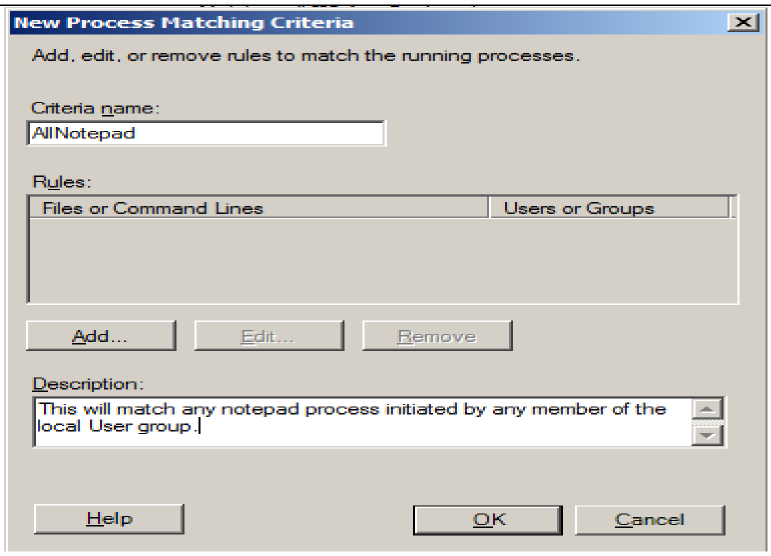
ក្នុងកិច្ចការនេះយើងនឹងបង្កើត Process ដែលត្រូវនឹងការវិនិច្ឆ័យមួយដើម្បីភ្ជាប់ជាមួយ Notepad. exe នៅពេលប្រតិបត្តិដោយ account មួយដែលជាកម្មសិទ្ធិរបស់ local users group។

ជំហានអនុវត្ត៖

១. បើក Window system resource manager (Start | Administrative Tools | Windows system resource manager)

២. អ្នកត្រូវរើសយក Server to administrator the local ក៏បាន រឺ remote node ក៏បាន។ រើសយក This កុំព្យូទ័រ បន្ទាប់មកទៀតចុច Connect។

៣. ចុចMouse ខាងស្តាំលើProcess ដែលត្រូវនឹងការវិនិច្ឆ័យនៅក្នុងnavigation pane ហើយជ្រើសយក Process ដែលត្រូវនឹងការវិនិច្ឆ័យថ្មីពី pop-up menu



រូប ៧-៤. New Process Matching Criteria

៤. នៅក្នុង Description field ត្រូវវាយពាក្យ AllNotepad ធ្វើជាឈ្មោះរបស់ លក្ខខណ្ឌវិនិច្ឆ័យហើយវាយពាក្យ This will match any notepad process initiated by any member of the local Users group។ (Figure 7-4)

៥. ចុចប៊ូតុងAdd ដើម្បីបន្ថែម ruleថ្មី។

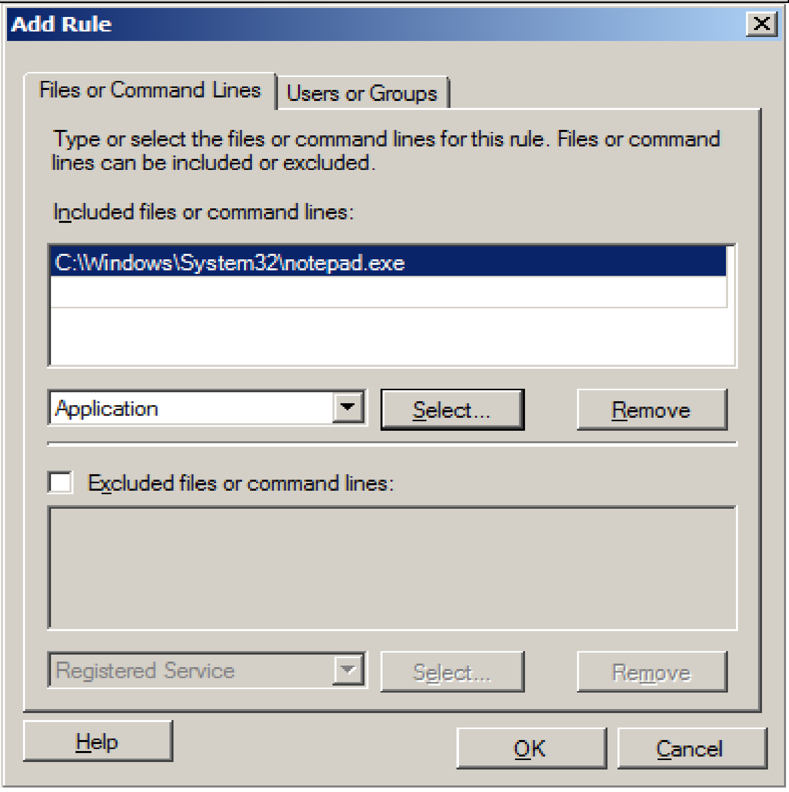
៦. នៅក្នុងIncluded file Or Command Line section ជ្រើសយកApplication ពី drop-down menuរួចចុចប៊ូតុងSelect។

៧. ចូលទៅកាន់C:\Windows\System32 ហើយជ្រើសយកnotepad.exe រួចចុច Open ។ វានឹងបន្ថែមC:\Windows\System32\notepad.exe ចូលទៅ list of included files របស់អ្នកដូចក្នុងរូប 7-5។

៨. ចុចUsers or Groups tab

៩. ចុចប៊ូតុងAdd ដែលនៅជាប់ប្រអប់ Included Users and Groups

១០. វាយពាក្យUsers នៅក្នុង Select Users or Groups dialog box ហើយចុច OK វានឹងបន្ថែម BUILTIN\Users ចូលទៅ list of Included Users And Gruops ដូចក្នុងរូបភាព ៧-៦។



រូប ៧-៥. ការដាក់ notepad.exe ទៅកាន់ list នៃ included files

១១. ចុចOK លើប្រអប់Add Rule ដើម្បីរក្សាទុកការផ្លាស់ប្តូរ។

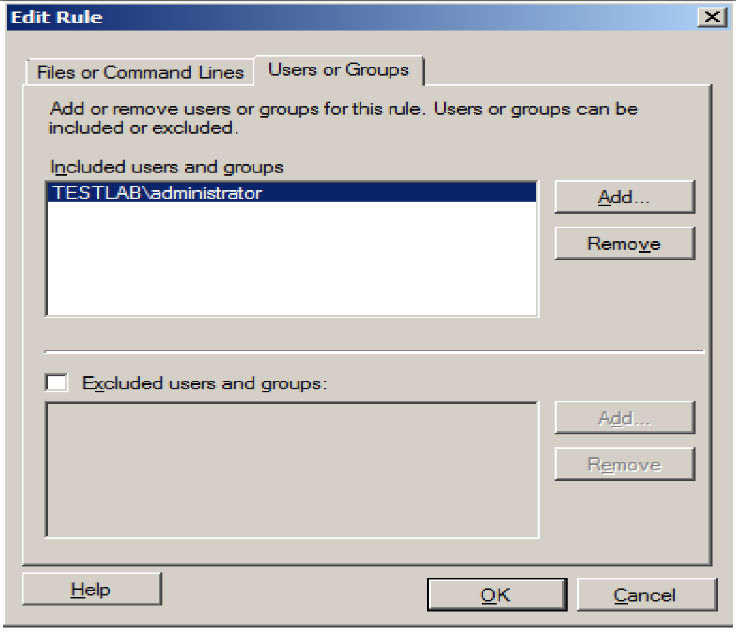
១២. ចុចOK នៅលើប្រអប់ New Process Matching Criteriaដើម្បីរក្សាទុក Criterion (រូប 7-7)

គោលការណ៍លៃ Resource

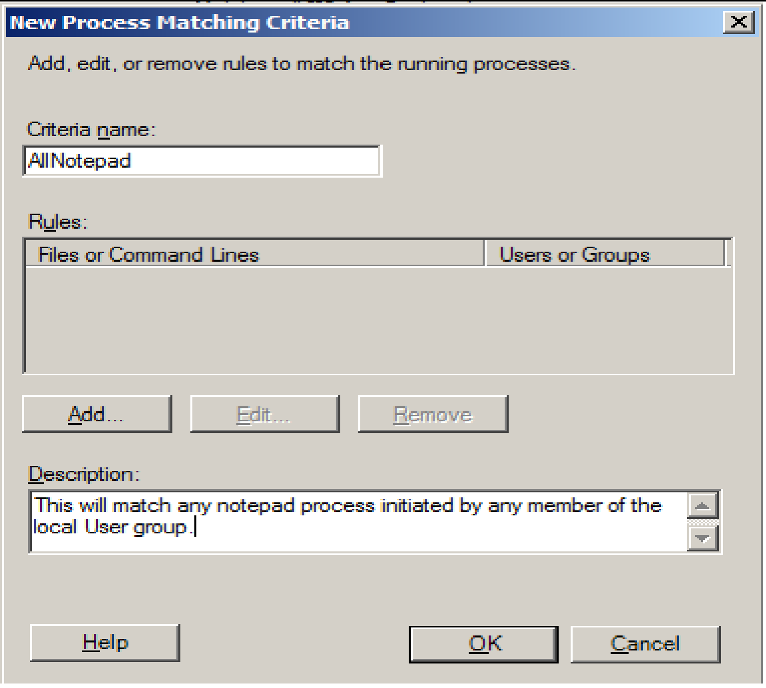
ពេលអ្នកបានបង្កើត process ដែលត្រូវនិងការវិនិច្ឆ័យរបស់អ្នករួចហើយអ្នកក៏អាចបង្កើតគោលការណ៍លៃ resource ដែរ។ គោលការណ៍ទាំងនេះបញ្ជាឱ្យ processesទទួលនូវការចែកចាយនៃ Resource តាមរបៀបណា។ គ្រប់គោលការណ៍ផ្ទុកនូវតារាងនៃ process ដែលត្រូវនឹងការវិនិច្ឆ័យមួយរឺច្រើនដែលម្យ៉ាងទៀតមានសំណុំនៃ resource constraints ដូចជាការលៃ CPU និង memory limits។ គោលការណ៍លៃ Resource ទាំង៤នេះបានបញ្ជាក់ន័យចេញតាមរយៈប្រអប់។ ដោយ default Equal-Per-Process policy ជាផ្នែកមួយដែលធ្វើឱ្យគ្រប់បំណែងចែកនៃពេល CPU ស្មើៗគ្នាក្នុងការដំណើរការ។ មានតែគោលការណ៍លៃ resource មួយគត់ដែលអាចដំណើរការគ្រប់ពេលវេលាទាំងអស់ដែលបានដាក់។ គោលការណ៍ដែលមានសកម្មភាពនេះគឺហៅថាគោលការណ៍ដែលកំពុង

គ្រប់គ្រង នៅក្នុងគោលការណ៍ WSRM console នេះបង្ហាញអ្វីៗយ៉ាងច្បាស់លាស់ដោយ String{Manage} ដែលលេចឡើងនៅជាប់នឹង policy name។ ខាងក្រោមនេះសុទ្ធតែជាគោលការណ៍នៃ resource:

- Equal-Per-Process: គ្រប់ process ដែលដំណើរការសុទ្ធតែទទួលការប្រើប្រាស់ស្មើគ្នានៃ CPU cycles(defualt) របស់វា។
- Equal-Per-User: គ្រប់ processes របស់ Users ទទួលនូវការចែកស្មើគ្នានៃ CPU cycles។
- Equal-Per-IISAppPool: គ្រប់IIS application pool's worker process ទទួលបាននូវការចែកស្មើគ្នានៃ CPU cycles។
- Equal-Per-Session: គ្រប់ User-session's processes ទាំងអស់ទទួល ការចែកស្មើគ្នានៃ CPU cycles (សំដៅទៅ លើ Terminal Sessions)។



រូប ៧-៦. ដាក់ TESTLAB\Administrator ចូលក្នុង list នៃ included users and group



រូប ៧-៧. Process ដែលត្រូវនឹងការវិនិច្ឆ័យថ្មីដែលទើបនឹងបញ្ចប់ហើយ

អ្នកអាចគ្រប់គ្រងលើគោលការណ៍នៃ Resources ពីរប្រភេទគឺតាមការប្រើប្រាស់នូវ WSRM: CPU និង Memory។ ក្បួនទូទៅនៃការបង្កើតនូវគោលការណ៍គឺថាអ្នកត្រូវផ្តល់តម្លៃឱ្យ process ដែលត្រូវនិងការវិនិច្ឆ័យនឹងប្រាប់ដល់គោលការណ៍ថា proccesses ណាដែលវាអនុវត្តហើយនឹងកំណត់ពីមួយភាគរយនៃ resources ទាំងឡាយរបស់អ្នកដែលអាចជា CPU ឬ Memory ដែលកំណត់លើ processes ទាំងនោះ។ គោលការណ៍នីមួយៗអាចមាន Resourcesទាក់ទងជាច្រើនដែលត្រូវនឹងការវិនិច្ឆ័យនិងរាល់លក្ខខណ្ឌវិនិច្ឆ័យអាចមានសំណុំផ្ទាល់ខ្លួនរបស់វានៃប៉ារ៉ាម៉ែត្រនៃការកំណត់ resource ។ អ្នកក៏អាចធ្វើការកំណត់ដល់ទៅ ៩៩ ភាគរយនៃ CPU ទៅកាន់រាល់ Process ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យ ប៉ុន្តែចំនួនសរុបគឺមិនអាចលើសពី ១០០ភាគរយឡើយ ។ មួយភាគរយអប្បរមាដែលនៅសល់គឺត្រូវរក្សាទុកប្រើនោះពេលក្រោយសម្រាប់ការប្រើប្រាស់ដោយ processes ដែលបានដាក់ក្នុង default group ។

> *ចំណាំ៖* WSRM នឹងមិនអនុវត្តនូវច្បាប់នៃការកំណត់ CPU រហូតដល់ resources ចាប់ ផ្តើមប្រើប្រាស់អស់។ រហូតមកដល់ពេលនេះ រាល់ processes អាចទទួលបាន CPU ច្រើនប៉ុន្មានដូចដែលវាចង់បាន ។ ជាឧទាហរណ៍ ប្រសិនបើ Server របស់អ្នកកំពុងដំណើរការត្រឹមតែ 50 ភាគរយនៃការប្រើ CPU ដែលគ្មាននៃ policies នៃការកំណត់ CPU នឹងមានឥទ្ធិពលឡើយ ទោះបីជាអ្នកកំណត់បញ្ជាក់ត្រឹមតែ process មួយដែលគួរតែមាន 20 ភាគរយនៃ resources របស់ CPU ។ ពេលដែល Server ចាប់ផ្តើមខិតទៅជិត utilization អតិបរមា, Processes ត្រូវបានកំហិតដោយផ្អែកលើ policies អ្វីក៏ដោយដែលអ្នកបានកំណត់ហើយ ។

ចំនួននៃពេល processing ដែលរាល់ process នីមួយៗក្នុង groups ដែលត្រូវនឹងវាដោយជាក់លាក់ណាមួយដែលត្រូវកំណត់ដោយច្បាប់នៃការគ្រប់គ្រងដែលអ្នកបានជ្រើសរើស ។

- Standard គឺការកំណត់ដោយ Default ។ មិនមែនជា WSRM ទេ តែជាប្រព័ន្ធដំណើរការនោះទេ ដែលមានទំនួលខុសត្រូវលើការចែកចាយនូវ ពេលវេលា processing របស់ CPU ទៅ processes នីមួយៗ ។
- Equal per process WRSM នឹងធ្វើឱ្យរាល់ Processes ដែលស្ថិតនៅក្នុង group នោះត្រូវបានប្រើប្រាស់នូវចំនួនដូចគ្នានៃវង្វិលជុំនៃ CPU។ ទោះបីជាយ៉ាងណាក៏ដោយរាល់ Processes ដែលស្ថិតក្នុង group ជាក់លាក់នោះ នឹងត្រូវកំហិតទៅតាមភាគរយទូទៅទាំងអស់ដែលអ្នកកំណត់ក្នុងគោលការណ៍របស់អ្នក។ ឧទាហរណ៍ បើអ្នកកំណត់នូវ២៥ភាគរយនៃពេល processing របស់ CPU សម្រាប់ process ដែលត្រូវលក្ខខណ្ឌវិនិច្ឆ័យជាក់លាក់ណាមួយនោះរាល់ processes ទាំងអស់ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យនោះដែលត្រូវតែកំណត់ឱ្យចែកគ្នាស្មើនូវ២៥ភាគរយនៃ CPU។ ក្នុងន័យផ្សេងទៀត បើអ្នកមាន process ចំនួនប្រាំដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យនោះ នោះរាល់ process នឹងទទួលបានតែ ៥ ភាគរយនៃ cycles របស់ CPU ប៉ុណ្ណោះ ។
- Equal per user វាប្រហាក់ប្រហែលនឹង Equal per process លើកលែងតែវាបានចាត់ជាក្រុមនូវ processes តាមអ្នកប្រើប្រាស់ដែលចាប់ផ្តើមដំណើរការវា។ នេះគឺមានសារៈសំខាន់ណាស់ក្នុង terminal server environment ។

សម្រាប់ប្រព័ន្ធ multiprocessor វានឹងអាចរឹតតែស្មុគស្មាញឡើង ។ ភាគរយនោះគឺឆ្លុះបញ្ចាំងនូវភាគរយដែលជៀបទៅនឹងដែនកំហិត CPU bandwidth ទូទៅទាំងអស់។ ឧទាហរណ៍ ប្រសិនបើអ្នកមាន processors ចំនួនបួនហើយអ្នកកំណត់ 25 ភាគរយដើម្បីបែងចែករវាង process ដែលអាចគ្រប់គ្រងបានដែល 25 ភាគរយនៃ bandwidth របស់ CPU សរុប បន្ទាប់មកអ្នកនឹងកំណត់នូវមធ្យមជាក់លាក់ជំនួសឱ្យការមាន 100 ភាគរយនៃ CPU

មួយសម្រាប់ process របស់អ្នកហើយអ្នកនឹងមានត្រឹមតែ 50 ភាគរយនៃ CPU មួយ(25 ភាគរយនៃ CPUs ពីរស្មើនិង 50 ភាគរយនៃ CPU មួយ)។ អ្វីទាំងអស់នេះមានន័យថារាល់ចុងថ្ងៃនីមួយៗថាអ្នកអាចកំណត់ចំនួននៃ processes ដែលមិនអាចគ្រប់គ្រងបានទៅដល់ចំនួនអប្បរមាមួយដើម្បីធ្វើឱ្យការគ្រប់គ្រងលើ resource របស់ WRSM ឱ្យមានប្រសិទ្ធិភាព ក្រៅពីតារាងដែលមាន processes មិនរាប់បញ្ចូលដែល system បានកំណត់ទុកនោះ អ្នកគួរតែចៀសវាងនូវ process ដែលរាប់ចេញនោះតាមដែលអាចធ្វើទៅបាន។ ចំនួននៃ memory ដែលអ្នកបានកំណត់ទៅកាន់លក្ខខណ្ឌវិនិច្ឆ័យរបស់អ្នកនីមួយៗគឺកំណត់ត្រឹមតែចំនួននៃ memory ដែលអ្នកមានលើប្រព័ន្ធរបស់អ្នក ។ អ្នកអាចបង្កើតការកំណត់នោះជា soft ឬក៏ជា hard ដែល soft limit គឺបានអភិវឌ្ឍឡើងក្នុងទម្រង់នៃ entry នៃ event log ដែលត្រូវបានបង្កើតឡើងនៅពេលដែល process ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យ នោះបានទៅហួស memory អតិបរមាដែលវាបានកំណត់ទុកឱ្យ។ Hard limit បញ្ឈប់រាល់ applications ទាំងស្រុងតែម្តងនៅពេលដែលវាប្រើហួសចំនួន memory ដែលបានកំណត់ឱ្យ។ នេះមានសារៈប្រយោជន៍ណាស់ក្នុងការដំណើរការ processes ដែលប្រើប្រាស់អស់ទាំងស្រុងនៃ resources របស់ server។ ឧទាហរណ៍ អ្នកអាចប្រើវាទៅកាន់ process នៃ IIS worker ។ តាមវិធីនេះ ប្រសិនជា Web application ដែលបានសរសេរឡើងដោយមានលក្ខណៈខ្វះខាតស្រាប់តែភ្លាមៗនោះចង់ប្រើប្រាស់អស់នូវ memory ទាំងអស់របស់អ្នក នោះ WSRM នឹងបញ្ឈប់វាដោយស្វ័យប្រវត្តសម្រាប់អ្នកដោយទុកឱ្យ processes ដទៃទៀតឱ្យនៅតែដំណើរការដដែល។ ដោយមិនដូចគ្នានឹងការកំណត់នូវ CPU resource ទេ ការកំណត់ដែននៃ memory ដែលអ្នកបញ្ជាក់នឹងត្រូវបានអនុវត្តទៅកាន់ process នីមួយៗដែលស្ថិតក្នុងក្រុមហើយមិនត្រូវបានចែកចាយទៅវាងគ្នាវានោះទេ។ ឧទាហរណ៍ បើអ្នកកំណត់ឱ្យជាក់លាក់នូវដែនកំណត់អតិបរិមានៃ 20 MB ទៅដល់ process ដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យជាក់លាក់ណាមួយនោះprocessនីមួយៗដែលត្រូវនឹងលក្ខខណ្ឌវិនិច្ឆ័យនោះនឹងទទួលបាន 20MB ។

Limits អាចកំណត់លើសំនុំការងារឬក៏ memory ។ សំនុំនៃ Memoryដែលកំពុងធ្វើការ គឺសំដៅទៅលើចំនួន memory ដែលត្រូវបានប្រើប្រាស់ដោយ Process ក្នុងខណៈពេលកំពុងដំណើរការ។ នៅពេលដែលការប្រើប្រាស់បានឈានទៅដល់កម្រិតផ្នែកខាងលើសម្រាប់សំនុំនៃ Memory ដែលកំពុងធ្វើការនោះ memory manager ក៏ចាប់ផ្តើមធ្វើការជំនួសចេញនូវ memory pages នោះ។ ការធ្វើបែបនេះអាចកាត់បន្ថយប្រសិទ្ធភាពដំណើរការរបស់ application ប៉ុន្តែវានឹងមិនបង្កើតឱ្យមាន errors កើតឡើងពីការខ្វះ Memory ឡើយ។ ចំណែកឯ Committed Memory វិញគឺប្រើសម្រាប់ការឃ្លាំមើលពី processes ដែលដំណើរការខុសរឿងឬក៏ memory ដែលបានលេចឡើង។ ដោយកំណត់នូវលក្ខណៈកម្រិតចាប់ផ្តើមនៃដំណើរការ processes ដ៏សមរម្យមួយ អ្នកអាចបង្ខំឱ្យ processes នោះឈប់ដំណើរការនៅពេលដែលវាដើរដល់កម្រិតមួយឬក៏បង្កើតជា log entry មួយទុកក្នុង Event Log សម្រាប់ការរកមើលនូវបញ្ហានៅពេលក្រោយទៀត។ ជាក់ស្តែងWRSM មិនទាក់ទិននឹងការកំណត់ទីតាំងរបស់ memory ទេ។ វាគឺជាការងាររបស់ memory manager ។ ការងាររបស់ WRSM គឺជាការត្រួតពិនិត្យមើលនូវ Utilization(ការធ្វើឱ្យកាន់តែមានប្រសិទ្ធភាពក្នុងដំណើរការ)និងប្រសិនបើវាដំណើរការហួស utilization នោះ វានឹងប្រាប់ memory manager ដូច្នេះវាអាចធ្វើកំណត់កែប្រែ ឬក៏អាចសូម្បីនឹងច្រានចោល memory បន្ថែមទៀតពីការធ្វើការកំណត់ទីតាំងទៅកាន់ process នោះ ។

អ្នកក៏អាចកំណត់ឱ្យកាន់តែជាក់លាក់នូវ Advanced options បន្ថែមទៀតក៏បានដែរ។ នៅលើប្រព័ន្ធ multiprocessor អ្នកអាចកំណត់ឱ្យជាក់លាក់ថាតើ processor មួយឬច្រើនណាដែលអាចកំណត់ឱ្យប្រើបានលើ process នីមួយៗនោះ។ អ្នកអាចកំណត់ suballocate ឱ្យ resources របស់ processor ក៏បាន ឬអត់ក៏បានដែរ។ ជាឧទាហរណ៍ ប្រសិនបើអ្នកមាន processors ចំនួន៤នៅលើ Server របស់អ្នក អ្នកអាចធ្វើការ កំណត់ទីតាំងការងារចំនួនពីរ processors សម្រាប់ process ជាក់លាក់ណាមួយដែលវាគោរពតាមលក្ខខណ្ឌ នោះរួចហើយអ្នក

ក៏អាចធ្វើការកំណត់ប្រើការលែលកបន្តបន្ទាប់ដើម្បីកំណត់បញ្ជាក់ឱ្យច្បាស់ទៀតថាតើ processors ទាំងពីរនោះនឹងចែកគ្នារវាង processes នោះ។ ការធ្វើបែបនេះ នឹងបង្កើតនូវទំនាក់ទំនង parent/child រវាងការធ្វើការលែទុក និងការលែទុកបន្តទៀតរបស់វា។ អ្នកក៏មិនត្រូវបានកម្រិតទៅកាន់តែកម្រិតទំនាក់ទំនង parent/child នោះទេ។ ការធ្វើ allocation នេះចាប់ផ្តើមនៅកម្រិតទាបបំផុត ហើយ resources ដែលដែលបានត្រៀមទុកនៅកម្រិតនោះនឹងត្រូវបានធ្វើឱ្យអាចប្រើប្រាស់បានផងដែរទៅដល់ parent របស់វារហូតដល់ resources ដែលអាចប្រើប្រាស់ដែលនៅសល់ត្រូវបានធ្វើឱ្យអាចប្រើប្រាស់បានទៅដល់ default group នោះ នេះវាសំដៅទៅលើគោលការណ៍នៃការរៀបតាមលំដាប់នៃអទិភាព។

លំហាត់អនុវត្តៈ «ការបង្កើតគោលការណ៍លែ CPU »

ក្នុងឧទាហរណ៍សាមញ្ញនេះ យើងនឹងប្រើប្រាស់ process AllNotepad ដែលត្រូវនិង criterion ដែលដាក់កម្រិតទៅដល់រាល់ processes របស់ notepad.exe ឱ្យប្រើត្រឹមតែ ១០ ភាគរយនៃ CPU និងដល់ទៅ 10MB នៃ memory ក្នុងខណៈពេលដាក់លាក់មួយ ។

<u>ជំហាននៃការអនុវត្តៈ</u>

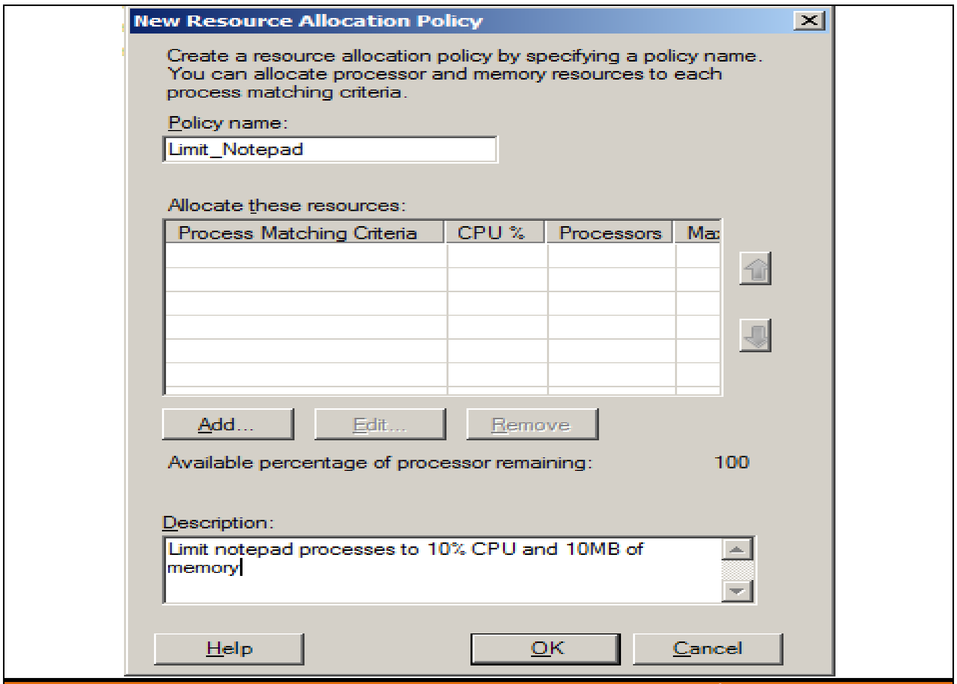
១. បើក Windows System Resource Management និងធ្វើការភ្ជាប់ទៅ server របស់អ្នក ។

២. ចូរចុច mouse ខាងស្តាំទៅលើ Resource Allocation Policies នៅឯ navigation pane ហើយជ្រើសរើសយក New Resource Allocation Policies ពី pop-up menu ។

៣. វាយបញ្ចូលពាក្យ Limit_Notepad ចូលក្នុង field Policy Name និង Limit notepad Proccesses to 10% and 10MB of memory នៅក្នុង field Description ដូចបានបង្ហាញក្នុងរូប ៧-៨ ។

> **ចំណាំៈ** ឈ្មោះរបស់ policy គឺដូចជាឈ្មោះរបស់ criteria ដែលដោយមិនអាចចាប់ផ្តើមដោយ សញ្ញាទ្រ ឡើយឬក៏មិនអាចមានដកឃ្លានិងគ្មាននូវតួអក្សរដូចជា \ / ? * | : < > " , ; ឡើយ ។

៤. ចុចលើ ប៊ូតុង Add ។



រូប ៧-៨. Resources Allocation Policy ថ្មី

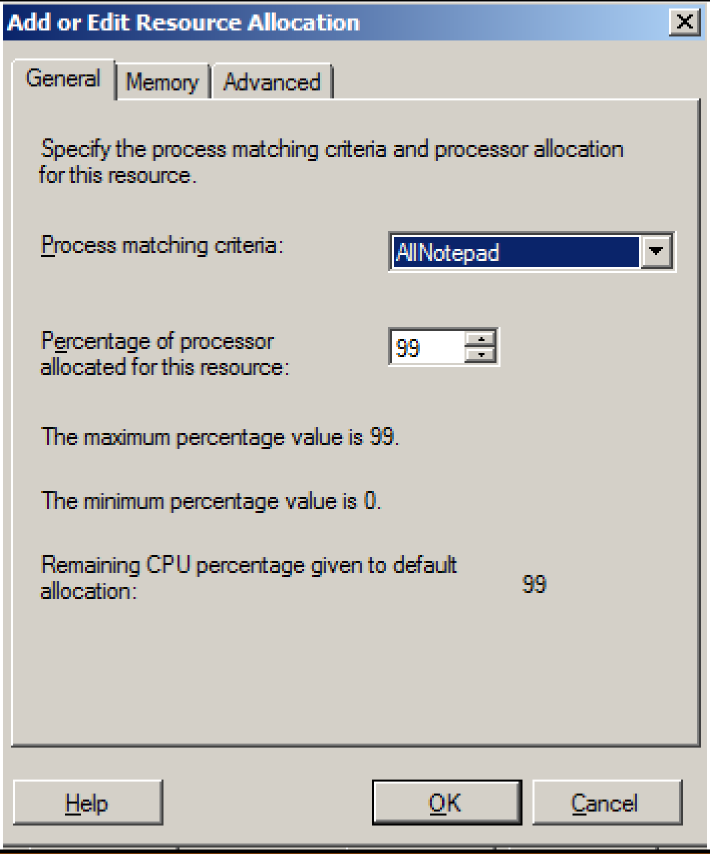
៥. ចូររើសយក AllNotepad ពី Process Matching Criteria dropdown menu ហើយនឹងបញ្ចូលតម្លៃ ១0 សម្រាប់ Percentage of Processor Allocated for This Resource ដូចក្នុងរូប ៧-៩។

៦. ចុចលើ tab Memory ហើយរើសយក Use Maximum Committed Memory for Each Process ក្នុងប្រអប់គូស tick ។

៧. វាយចូលលេខ ១០ ក្នុងប្រអប់ Maximum Committed Memory Limit Per Process ។

៨. ប្រសិនបើ memory នោះទៅហួសកំណត់ដែលគេរំពឹងទុកនោះវានឹងបង្កើត Event Log Message ពី dropdown list (ដូចរូប ៧-១០) ។ រួចចុច OK ដើម្បីធ្វើការរក្សាទុកការកំណត់ allocation ។

៩. អ្នកបានបង្កើតនូវresource allocation policyដោយជោគជ័យដូចបង្ហាញក្នុងរូប៧-១១ ។ រួចចុច OK ដើម្បីរក្សាទុក policy ថ្មីនេះ ។



រូប ៧-៩. ការដាក់កំណត់ process matching criteria និងភាគរយនៃ CPU

ប្រតិទិន

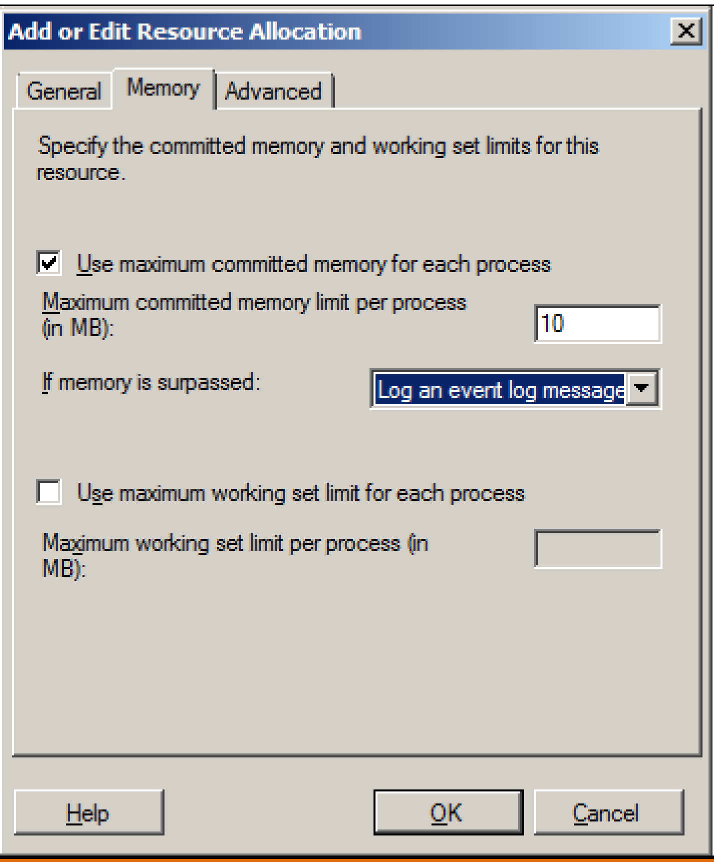
ប្រតិទិនគឺជា WRSM sheduling module។ វាអនុញ្ញាតឱ្យកំណត់ច្បាស់លាស់នៅពេលមានគោលការណ៍ច្បាស់លាស់នៃការលៃ resource អាចដំណើរការបាន។ ប្រតិទិនត្រូវបានគេបង្កើតឡើងរបស់ព្រឹត្តិ ការណ៍ប្រតិទិន ហើយនិង schedules។ schedules គឺខណៈពេលនៅក្នុង 24 ម៉ោង នៅពេលគោលការណ៍មានសកម្មភាព។ សម្រាប់ឧទាហរណ៍:អ្នកត្រូវការកំណត់គោលការណ៍ច្បាស់លាស់មួយឱ្យក្លាយជាសកម្មអំឡុងពេលធ្វើការហើយ

ភាពខុសប្លែកមួយមានសកម្មភាពពេលម៉ោងឈប់ធ្វើការ។ ប្រតិទិនកំណត់ច្បាស់លាស់ពីពេលវេលានៃការចាប់ផ្ដើមកាលបរិច្ឆេទហើយដូចនឹងការបញ្ចប់ពេលវេលានៃកាលបរិច្ឆេទ ហើយកន្លែងពេលវេលាដ៏ទៀងទាត់មួយ policy នឹងក្លាយទៅជាសកម្ម។ ពួកវាក៏អាចត្រូវបានគេប្រើផងដែរនៅក្នុងឈ្នាប់ជាមួយ schedule ដើម្បីដាក់ត្រៀមកាលបរិច្ឆេទមួយ នៅពេល schedule មួយនឹងយក។ល។

ឧទាហរណ៍:

អ្នកអាចត្រូវការម៉ោងធ្វើជំនួញនិងពេលវេលាសំរាកដែលកើតឡើងខែមករា។ ប្រភេទនៃប្រតិទិនព្រឹត្តិការណ៍គឺមានដូចខាងក្រោម៖

- **One Time:** បង្កើតព្រឹត្តិការណ៍ one-timeមួយ នៅពេល policyមួយមានសកម្មភាព។ នេះជាការស្នើសុំពេលនៃការចាប់ផ្ដើមនៃកាលបរិច្ឆេទនិងពេលវេលានៃការបញ្ចប់នៃកាលបរិច្ឆេទ។
- **Recurring Event:** ដូចជា recurring meeting មួយ នៅក្នុងOutlooks អ្នកអាចប្រើវានេះដើម្បីschedule recurring ប្រតិទិនព្រឹត្តិការណ៍សម្រាប់ policies របស់អ្នក។
- **Schedule:** ប្រើសម្រាប់ធ្វើឱ្យសកម្មឡើងគោលការណ៍លៃ resource ផ្សេងគ្នានូវការរត់ឆ្លងកាត់អំឡុងពេលនៃ 24 ម៉ោង។



រូប ៧-១០. ការកំណត់លក្ខណៈលើកម្រិតប្រើប្រាស់អង្គចងចាំ

លំហាត់អនុវត្ត៖ «ការបង្កើតនូវព្រឹត្តិការណ៍មួយនៃប្រតិទិន»

បន្តពីលំហាត់មុនរបស់យើង យើងនឹងបង្កើតនូវព្រឹត្តិការណ៍មួយនៃប្រតិទិនដែលដំណើរការម្ដងចប់ ដើម្បីបង្កើតនូវគោលការណ៍បំណែងចែកនូវធនធាននៃ Limit_Notepad របស់យើង ដែលវានឹងនៅសកម្មក្នុងរយៈពេលពីរអាទិត្យដែលយើងបានកំណត់ថាពី ថ្ងៃ ១៥ ខែ កក្កដា ២០០៧ នៅម៉ោង ៦:០០ ព្រឹក ដល់ថ្ងៃ ទី៣០ ខែ កក្កដា ២០០៧ នៅម៉ោង ៦:០០ ល្ងាច ។

ជំហានអនុវត្ត

១. បើកកម្មវិធី Windows System Resource Manager

២. ត្រូវប្រាកដថា មុខងារ Calendar ត្រូវបានដាក់ឱ្យដំណើរការ (enabled) (គឺវាដាក់ថា *Calendar {Enabled}* នៅផ្នែកជ្រើសមុខងាររបស់ WSRM)

៣. នៅឯផ្នែកជ្រើសមុខងារនោះដែរ ចូលចុចលើចំណុចពង្រីករបស់(+) Calendar

៤. ចូរចុច Mouse ខាងស្តាំលើមុខងារ Calendar Events ហើយជ្រើសយក New One Time Event

៥. ចូរបញ្ចូលព័ត៌មាន ឬក៏ជ្រើសយកព័ត៌មានដូចបានបង្ហាញក្នុងរូបភាព ៧-១២៖

Event Name: **NotepadSchedule**

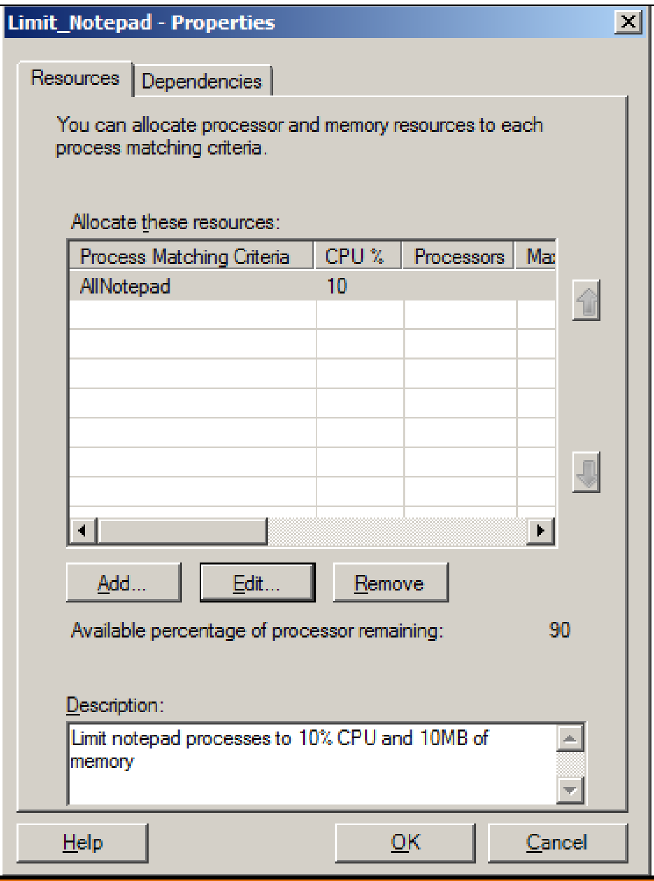
Description: **Enable Limit_Notepad**

Policy Name: **Limit_Notepad**

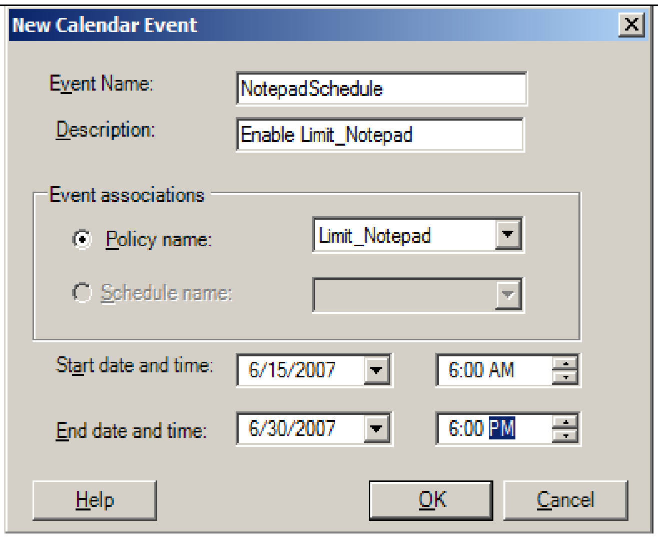
Start date and time: **6/15/2007 6:00AM**

End date and time: **6/30/2007 6:00PM**

៦. រួចចុចលើ OK ដើម្បីធ្វើការរក្សាទុកនូវព្រឹត្តិការណ៍ថ្មីនៃប្រតិទិននោះ ។



រូប ៧-១១. បំពេញនូវគោលការណ៍បែងចែកធនធានថ្មី (resource allocation policy)



រូប ៧-១២. ការបង្កើតនូវព្រឹត្តិការណ៍ថ្មីរបស់ប្រតិទិន (calendar event)

លំហាត់អនុវត្តៈ «ការបង្កើតនូវគម្រោងពេលវេលាមួយ (Schedule)»

នៅក្នុងលំហាត់នេះ យើងនឹងកំណត់កាលវិភាគពេលឱ្យគោលការណ៍ Limit_Notepad នោះដើម្បីឱ្យវាអាចមានសកម្មភាពពីម៉ោង ០៥:០០ ព្រឹកដល់ ០៩:០០ ល្ងាច និងពីម៉ោង ០៦:០០ ល្ងាចដល់ម៉ោង ១០:០០ ល្ងាច ។

<u>ជំហានអនុវត្ត</u>

១. ចូរបើកនូវកម្មវិធី Windows System Resources Manager

២. ចូរចុចលើចំណុចពង្រីករបស់ Calendar

៣. ចុច Mouse ខាងស្តាំលើមុខងារ Schedule រួចរើសយក New Schedule

៤. ចូរវាយឃ្លា **Notepad_Schedule** នៅក្នុងប្រអប់បំពេញ Schedule Name និងវាយឃ្លា **My custom notepad schedule** ចូរក្នុងប្រអប់បំពេញ Description ។

៥. ចូរចុច Mouse ពីរដងនៅឯណាក៏បានក្នុងផ្ទៃតំបន់គម្រោងពេលវេលាពណ៌ទឹកក្រូច ។

៦. នៅក្នុងផ្ទាំប្រអប់ Add Schedule Item ចូររើសយក Limit_Notepad ដែលស្ថិតនៅក្នុងប្រអប់ជ្រើសរើសPolicy ហើយរើសយក 5:00 AMនិង 9:00 AM ជាម៉ោងចាប់ផ្តើមនឹងបញ្ចប់រៀងគ្នាហ្នឹង រួចចុច OK (រូប៧-១៣) ។

៧. ចូរចុច Mouse ពីរដងនៅឯណាក៏បានក្នុងផ្ទៃតំបន់គម្រោងពេលវេលាពណ៌ទឹកក្រូច នឹងធ្វើដូចជំហានណែនាំដដែលដូចក្នុងជំហានទី ៦ លើកលែងតែប្តូរពេលយក 6:00 PM និង 10:00 PM ជាម៉ោងចាប់ផ្តើមនឹងបញ្ចប់រៀងគ្នា ។

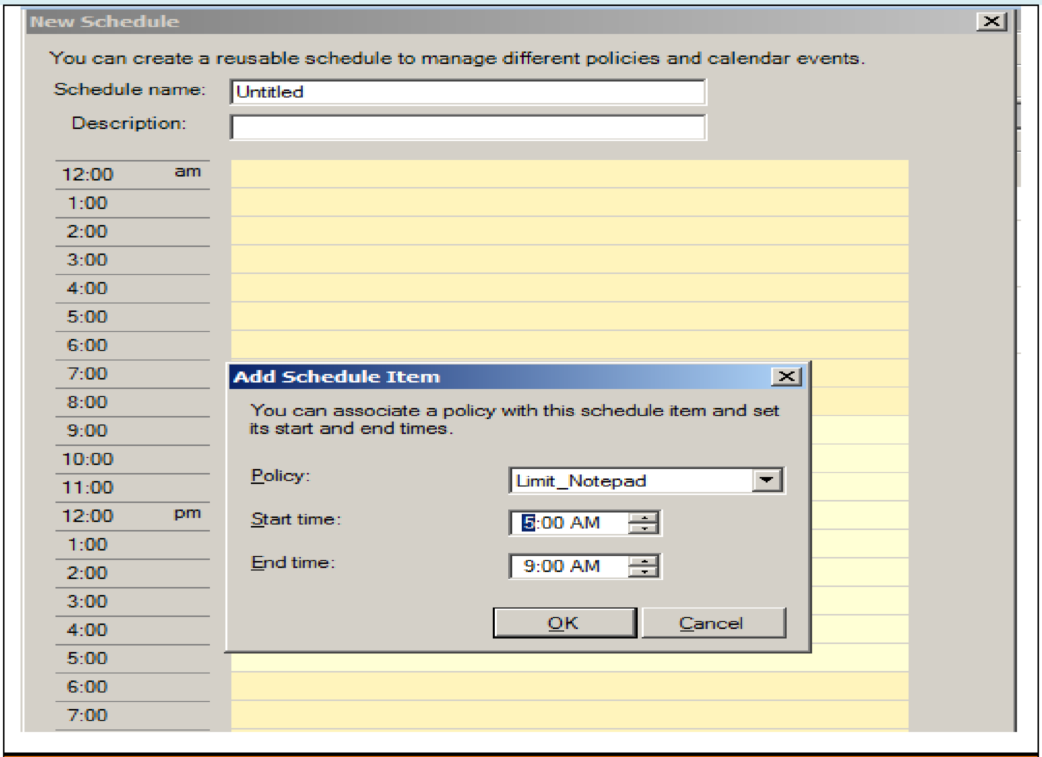
៨. ឥឡូវគម្រោងកាលថ្មីរបស់អ្នក គឺមានទម្រង់ដូចក្នុងរូបភាព ៧-១៤ ។ ហើយចុច OK ដើម្បីរក្សានូវគម្រោងពេលថ្មីនោះទុក ។

Accounting

សមាសធាតុនៃ Accounting នៃ WSRM នេះត្រូវបានប្រើប្រាស់ជាមូលដ្ឋានទិន្នន័យកណ្តាលដែលផ្តល់ការផ្ទុកលើព័ត៌មានរបស់ទិន្នន័យគណនីដើម្បីអាចធ្វើការបង្ហាញនូវជួរព័ត៌មានដែលទាក់ទងនឹងអាបក្បកិរិយារបស់ processes ដែលបានគ្រប់គ្រង។

មុខងារ Accounting នេះត្រូវបានបិទដោយស្វ័យប្រវត្តពេលអ្នកប្រើប្រាស់មិនបានកំណត់ដោយ WSRM។ ដើម្បីបើកវាវិញ ចូរចុច Mouse ខាងស្តាំលើឈ្មោះ Accounting នៅឯ navigation pane នោះ ហើយរើសយក Enable ។ ដោយកុំព្យូទ័រកំណត់ជាស្រេចគឺថាមូលដ្ឋានទិន្នន័យ Accounting ត្រូវបានរក្សាទុកដោយផ្ទាល់លើ WSRM server ។ អ្នកក៏អាចកំណត់វាឱ្យទៅ WSRM server ផ្សេងទៀតដែរ បើអ្នកចង់ធ្វើឱ្យទិន្នន័យនៃ accounting អាចត្រូវបាន access ពីទីណាក៏បានឬក៏អ្នកអាចបង្កើតនូវ instance របស់ SQL Server ដើម្បីផ្ទុករាល់ទិន្នន័យ account របស់អ្នក ។ ការរៀបចំ account លើ WSRM ក្នុងកុំព្យូទ័រនេះផ្ទាល់មានលក្ខណៈលឿនជាងគេ ប៉ុន្តែបើអ្នកមាន WSRM servers ជាច្រើនដែលបានបើកឱ្យដំណើរការហើយនោះ អ្នកប្រហែលជានឹងគិតថានឹងយកទិន្នន័យ account ទៅផ្ទុកមួយក្នុងចំណោមជម្រើសទាំងពីរខាងលើ។ដើម្បីផ្លាស់ប្តូរទីតាំងមូលដ្ឋានទិន្នន័យរបស់អ្នក ចូរចុចលើឈ្មោះ Accounting នៅឯ navigation pane ហើយនៅក្នុងប៉ាន់ Action ចូរចុចលើ Set DB Server ។ ការយកជម្រើសនេះ នឹងបើកនូវផ្ទាំង Set Accounting Database (រូបភាព ៧-១៥) ដែលអ្នកអាចកំណត់ទីតាំង database មួយជម្រើសទៀត ។

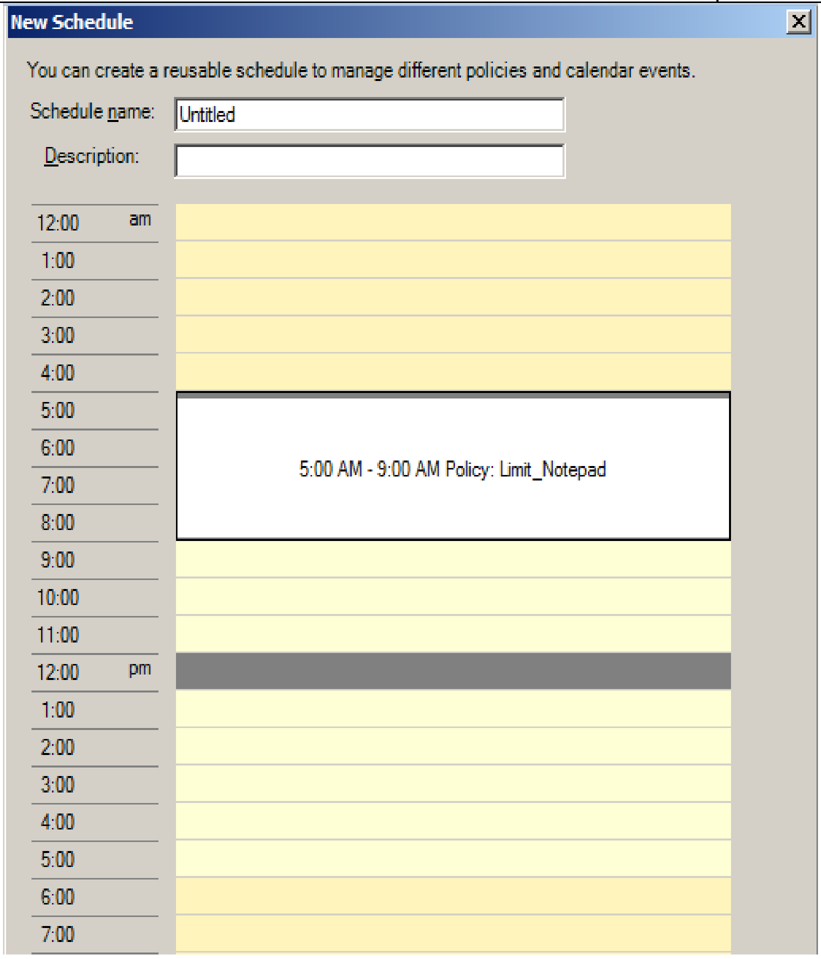
> **ចំណាំះ** មុខងារ Accounting អាចត្រូវបានថែមយ៉ាងសំខាន់ទៅកាន់ផ្នែកធនធានដែលប្រើដោយ WSRM និងប៉ះពាល់យ៉ាងខ្លាំងលើដំណើរការនៃ server របស់អ្នក។ អ្នកគឺគ្រាន់តែពិចារណាបើកនូវមុខងារនេះនៅពេលដែលកំពុងរកបញ្ហាដែលកើតមានឬក៏ដំណើរការសាកល្បងនូវគោលការណ៍របស់អ្នក ។



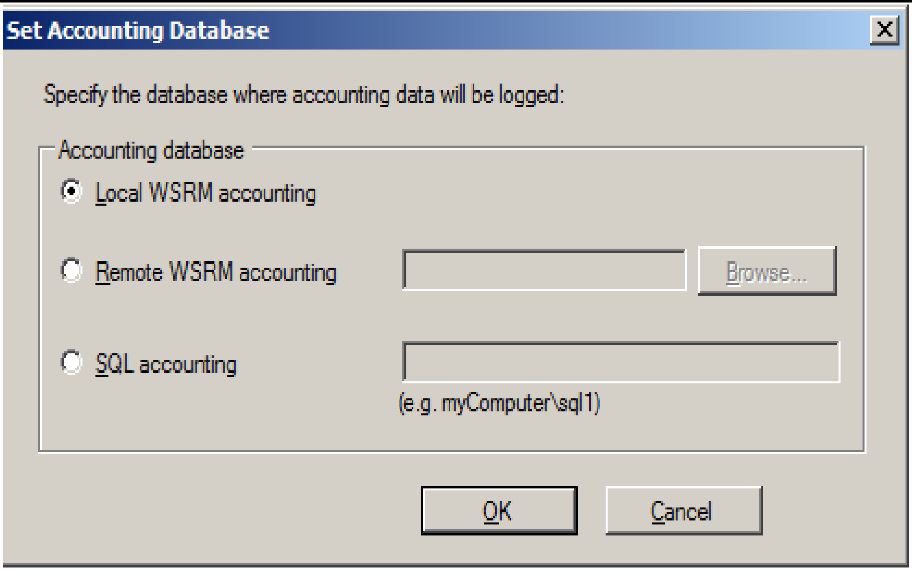
រូប៧-១៣. ដាក់ថែមនូវវត្ថុនៃគម្រោងពេល

រៀងរាល់ ១០ នាទី ព័ត៌មាន accounting គឺត្រូវបាន update និងអាចមើលវាបានតែនៅក្នុង console របស់ WSRM នៅឯទំព័រ Accounting ប៉ុណ្ណោះ។ ការបង្ហាញដែលកំណត់ជាស្រេចដោយកុំព្យូទ័រនេះគឺជាការបញ្ជូនទិន្នន័យដោយមិនបាច់ដំណើរការយ៉ាងសាមញ្ញបំផុតនៃរាល់ទិន្នន័យ ដែលបានស្រង់មកហើយវាស្រដៀងនិងអ្វីដែលអ្នកបានឃើញពីរបាយការណ៍សង្ខេប (log) ពីព្រឹត្តិការណ៍ដែលកំណត់ដោយកុំព្យូទ័រផ្ទាល់។ ដើម្បីធ្វើឱ្យមានភាពប្រសើរឡើងនៃការបង្ហាញអ្នកអាចកំណត់ប្តូរនូវលទ្ធផល ដោយដាក់នូវលក្ខខណ្ឌជ្រើសរើសលើទិន្នន័យផ្សេងៗ។ លើសពីនេះទៅទៀត ការបង្ហាញដែលបានកំណត់លក្ខខណ្ឌទាំងនោះអាចរក្សាទុកបាននិងបើកមកមើលវិញ។ ដូច្នេះប្រសិនបើអ្នកមានលក្ខខណ្ឌជ្រើសរើសសំញុំអ្នក

នឹងចង់ប្រើប្រាស់វាជាប្រចាំ អ្វីដែលអ្នកត្រូវការធ្វើទាំងអស់គឺកំណត់ថាលក្ខខណ្ឌប្រោះជ្រើសរើសនោះម្តងរួចចុចលើ ប៊ូតុង Save View នៅឯផ្ទាំង Configure Accounting View Filter ដូចបង្ហាញក្នុងរូបភាព ៧-១៦ ។



រូប៧-១៤. ទម្រង់គោលការណ៍គម្រោងពេលវេលាពេលលេញ

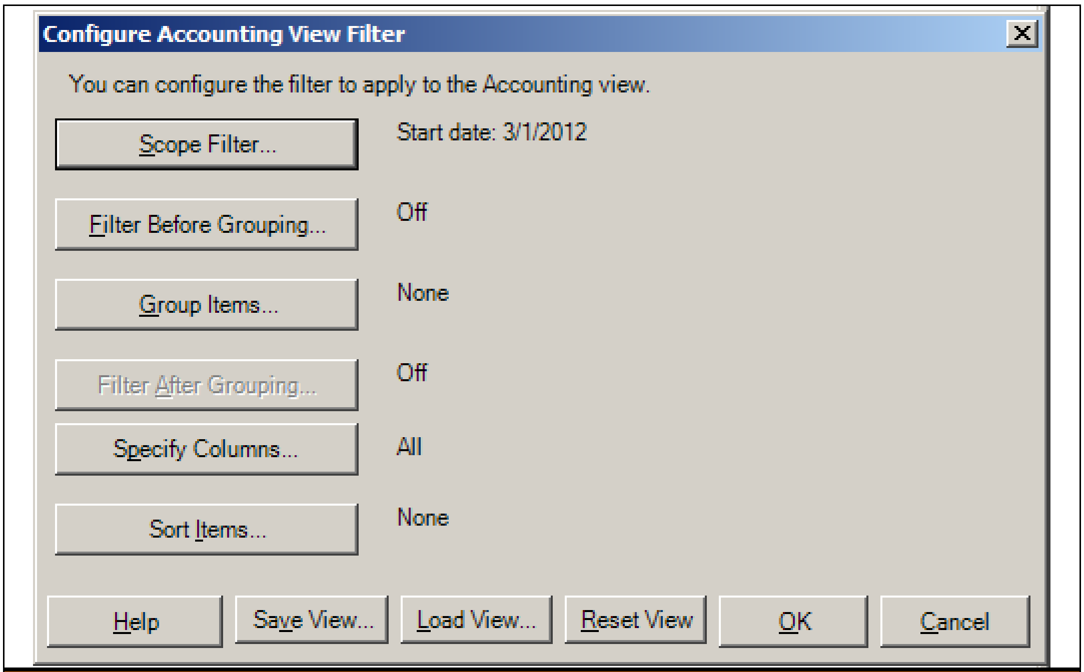


រូប៧-១៥. Set Account Database Dialog Box

តាមជម្រើសខាងក្រោមគឺអាចប្រើសម្រាប់លក្ខខណ្ឌជ្រើសរើសក្នុងការបង្ហាញ:

- Scope Filter:កំណត់លក្ខខណ្ឌជាក់លាក់សម្រាប់ដែននៃទិន្នន័យដែលអ្នកចង់បង្ហាញ

- Filter Before grouping:បង្កើតនូវលក្ខខណ្ឌជ្រើសរើសជាក់លាក់មួយសម្រាប់ Acc -ounting Items មុនពេល items ទាំងនោះត្រូវបានបញ្ចូលជាក្រុម។
- Group Item:អនុញ្ញាតឱ្យអ្នកបញ្ចូលជាក្រុមនូវលទ្ធផលដោយ Process Name, Domain, User, Policy Name, Process Matching Criteria, Program Path, និង command line។



រូប៧-១៦. ការរក្សាទុកការបង្ហាញក្នុង Configure Account View Filter Dialog Box

- Filter After Grouping: ការប្រើប្រាស់ជម្រើសនេះ គឺការបន្ថែមលក្ខខណ្ឌជ្រើសរើស អាចត្រូវបានកំណត់ទៅលើitems ទាំងនោះបន្ទាប់ពីitems ទាំងនោះត្រូវបានបញ្ចូលជាក្រុមសម្រាប់ បើសិនក្រុមនៃ items ត្រូវបានកំណត់ច្បាស់លាស់ ។
- Specify Columns: ជាមួយពត៌មានមួយចំនួនធំ ដែលបានស្រង់ទុកសម្រាប់គ្រប់items នៅក្នុងទិន្នន័យ accounting ទាំងនោះមានដូចជា៖ process name, ចំនួន thread, CPU Time,និង ទិន្នន័យជាច្រើនទៀត។ ចំនុចនេះអនុញ្ញាតឱ្យអ្នកកំណត់ភាពជាក់លាក់ច្បាស់លាស់មួយចំពោះជួរឈរដែលអ្នកចាប់អារម្មណ៍នៅក្នុងការបង្ហាញ។
- Sort Item: ការប្រើប្រាស់ជម្រើសនេះ គឺដើម្បីតំរៀបទិន្នន័យ។

លំហាត់អនុវត្ត៖ «Archiving Accounting Information»

បើអ្នកទុកឱ្យ accounting ដំណើការបានសម្រាប់រយៈពេលមួយ ដោយថាហេតុអ្នកនិងឃើញបញ្ជីនៃ processor ដែលត្រូវបានកត់ត្រាទុកដោយ សមាសធាតុរបស់ Accounting។ បើអ្នកចង់ វេចខ្ចប់ទិន្នន័យ និងត្រូវបានធ្វើការបង្ហាញពេលក្រោយ។ អនុវត្តតាមជំហានខាងក្រោមនេះ៖

ជំហាននៃការអនុវត្ត៖

១. បើក Windows System Resource Manager

២. ម៉ៅស្តាំលើ Accounting និង ជ្រើសរើស Archive រឺ Delete information

៣. កំណត់ឱ្យច្បាស់នូវពេលវេលា ចាប់ផ្តើម និង បញ្ចប់សម្រាប់ទិន្នន័យដែលអ្នកចាប់អារម្មណ៍

៤. គូស ✓ លើប្រអប់ Archive Data
៥. ចូលទៅជ្រើសរើស Location ដែលជាកន្លែងវេចខ្ចប់នឹងត្រូវផ្ទុក
៦. ជ្រើសនូវ File Format ដែលអ្នកចង់ Archive ដើម្បីធ្វើការរក្សាទុក
៧. រូបភាព Archive រឺ Delete Accounting Information គួរតែមើលទៅដូចរូបភាព ៧-១៧។ ចុចលើ Ok ដើម្បីធ្វើការរក្សាទុកនូវ Archive ។

Condition

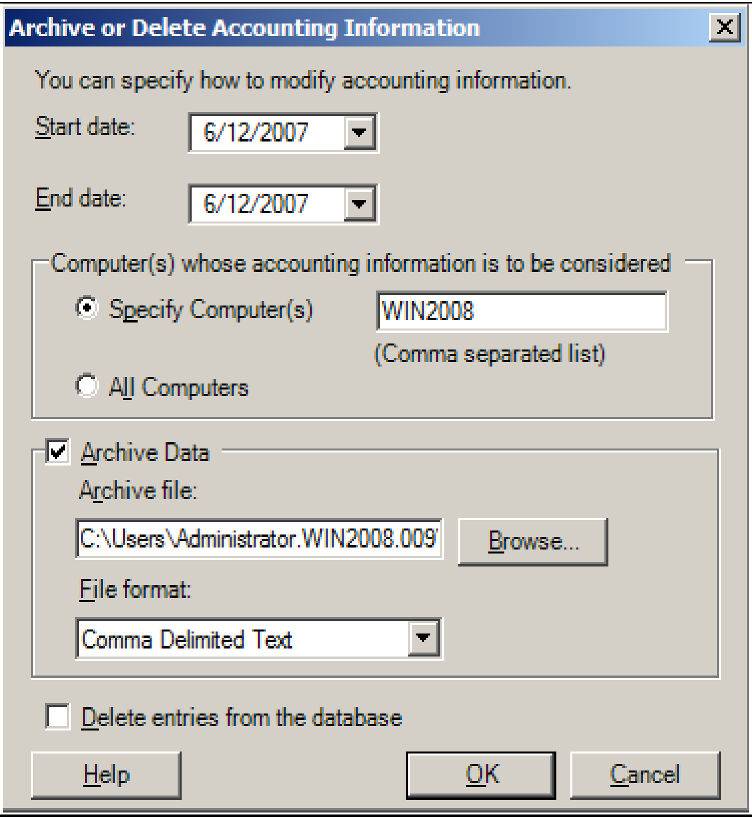
conditions node ដែលនៅក្នុង navigation pane ផ្ទុកនូវលក្ខខណ្ឌជាច្រើនកំណត់ទុកជាស្រេចដែលត្រូវបានប្រើប្រាស់សម្រាប់ធ្វើជាគន្លឹះសម្រាប់ផ្លាស់ប្តូរនៅក្នុងគោលការណ៍មួយ។

ឧទាហរណ៍:

នៅពេល processorថ្មីមួយគឺបានរកឃើញ រឺបើលេខថ្មីមួយនៃ processor នោះខ្ពស់ជាងចំនួនជាក់លាក់ណាមួយ អ្នកអាចប្រាប់ទៅកាន់ WSRM ដើម្បីធ្វើការផ្លាស់ប្តូរគោលការណ៍ផ្សេងមួយទៀត។

ឧទាហរណ៍:

អ្នកប្រហែលស្វែងរកឃើញនូវការប្រើប្រាស់ទាំងនេះ បើសិនជាអ្នកចង់ឱ្យគោលការណ៍នេះត្រូវបានផ្លាស់ប្តូរនៅពេល node គឺជាផ្នែកមួយនៃ Microsoft Cluster Service ឱ្យមិនអាចដំណើការបាន។ អ្នកអាចមានគោលការមួយក្នុងការផ្លាស់ប្តូរនូវអទិភាព នៃ processor របស់អ្នកជាស្វ័យប្រវត្តនៅពេល cluster node មួយត្រូវបានធ្លាក់ចុះភ្លាមៗ ហើយបន្ទាប់មកទៀតវានឹងត្រលប់មកវិញនូវគោលការធម្មតាជាស្វ័យប្រវត្តនៅពេលដែល node ត្រលប់មក online វិញ ។



រូប៧-១៧. Archiving accounting information

Resource Monitor

Resource Monitor គឺត្រូវបានបកស្រាយជាសង្ខេបនៅទីនេះ ពីព្រោះថាអ្នកបានធ្វើការជាមួយ Perfor mance Monitor នៅក្នុង Windows versions មុន ដូចដែលអ្នកបានដឹងពីរបៀបប្រើប្រាស់វារួចមកហើយ។ នៅពេលដែលអ្នកចុចលើ Resource Monitor node នៅក្នុងWSRM navigation pane អ្នកនឹងឃើញនូវរូបភាពប្រហាក់ប្រហែលនិង graph interface (figure 7-18)។ អាប់ស៊ីសតំណាងឱ្យកំឡុងរយៈពេលណាមួយ ហើយអរដោនេតំណាងឱ្យតម្លៃដែលអាចត្រូវបានកែតម្រូវពីគ្រប់ធនធានទិន្នន័យនីមួយៗ។ វាអាចត្រូវបានប្រើប្រាស់សម្រាប់គ្រប់គ្រងលើការត្រួតពិនិត្យទូទៅនៅលើធនធាន server របស់អ្នក ប៉ុន្តែអ្នកនិងឃើញពេលក្រោយទៀតនូវភាពទុកចិត្តនិងការបង្ហាញពីសមត្ថភាពគឺបានបន្ថែមនូវ version នៃ Resource Monitor។

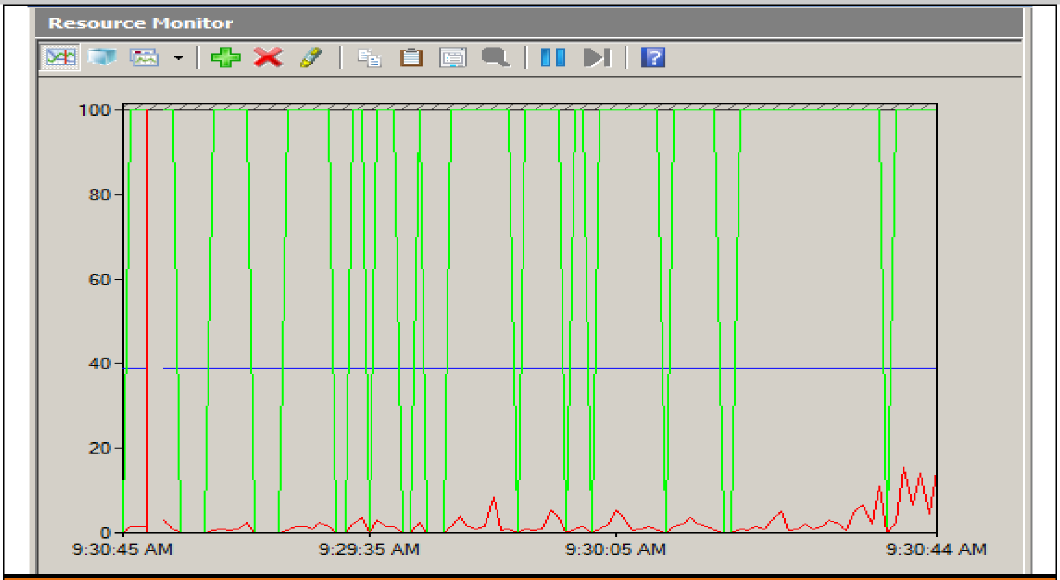
លំហាត់អនុវត្តះ «ការប្រើប្រាស់ Resource Monitor ដើម្បីតាមដានការប្រើ CPU and Memory»

នៅក្នុងលំហាត់នេះ ពួកយើងនិងconfigure Resource Monitor ដើម្បីតាមដាន total CPU utilization និង ស្ថិតិនៃ Memory Usage មួយចំនួន។

<u>ជំហាននៃការអនុវត្តះ</u>

១. បើក Windows System Resource Manager

២. ចុច Resource Monitor



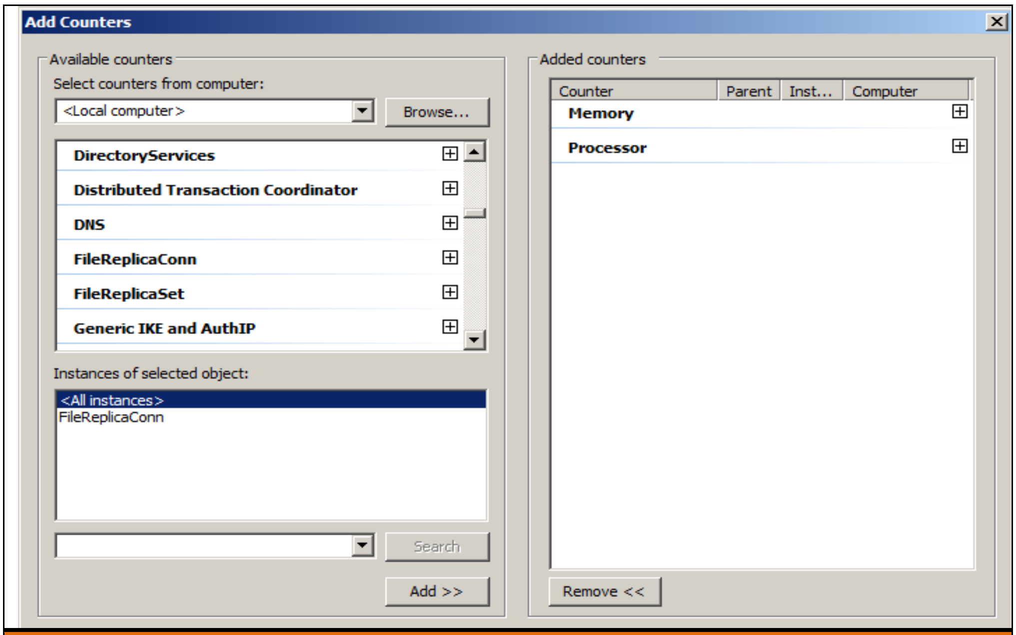
រូប៧-១៨. Resource Monitor

៣. លុបចោលនូវcounterទាំងឡាយដែលបានបង្ហាញដោយចុចលើ counter នីមួយៗ បន្ទាប់មកចុចលើសញ្ញាXពណ៌ក្រហមរហូតដល់ក្រាហ្វិចទទេ

៤. ចុចលើសញ្ញ(+)ពណ៌បៃតងនៅផ្នែកខាងលើនៃទំព័ររបស់Resource Monitor

៥. នៅផ្នែកខាងក្រោមនៃបញ្ជី Available Counter ចុចលើសញ្ញា(+)ជិតទៅនិងProcessor ហើយបន្ទាប់មកទៀតជ្រើសរើស% Processor Time

៦. ជ្រើសរើស Total ពី Instance of Selected Object list box, បន្ទាប់មកចុចលើប៊ូតុង Add



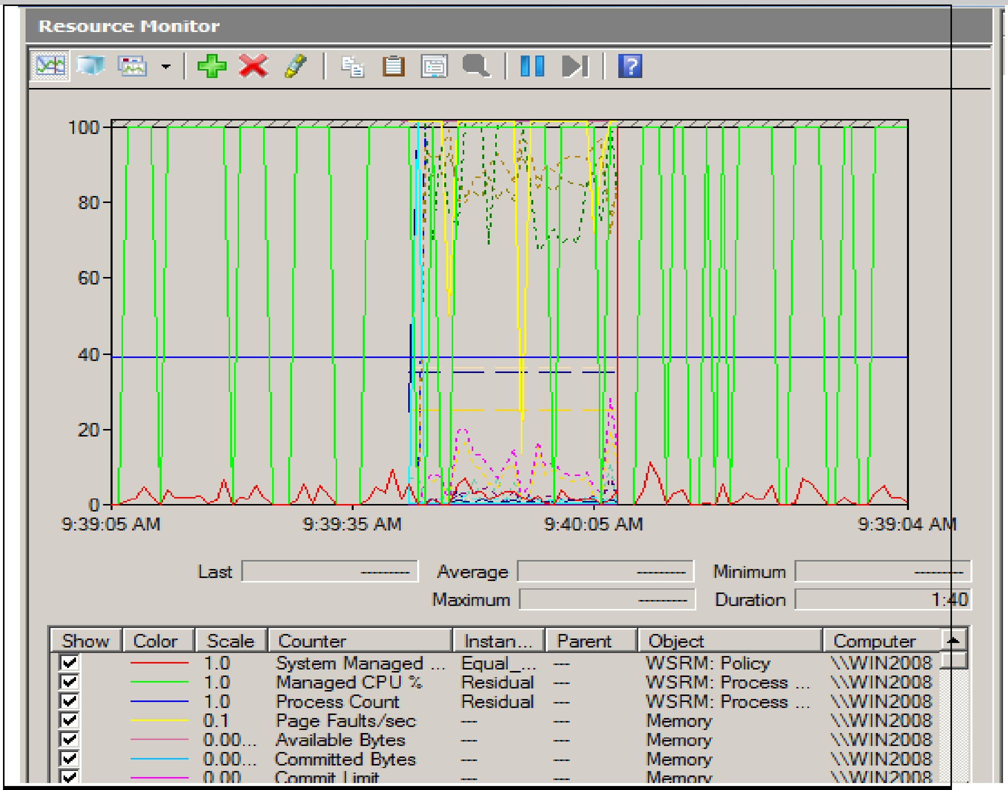
រូប៧-១៩. Add Counter Dialog Box

៧. អូសឡើងលើនូវបញ្ជី Available Counter ហើយចុចលើសញ្ញា(+)ដែលនៅជាប់នឹងMemory។ បន្ទាប់មកជ្រើសរើសAvailable Mbytes ហើយចុចលើប៊ូតុងAdd

៨. ខាងក្រោមដូចនឹង Memory Counter ជ្រើសរើស Page/sec បន្ទាប់មកចុចលើប៊ូតុង Add

៩. ប្រអប់ Add counter របស់អ្នក ឥឡូវវាគួរតែមើលទៅដូចរូបភាព៧-១៩។ ចុចប៊ូតុងOk

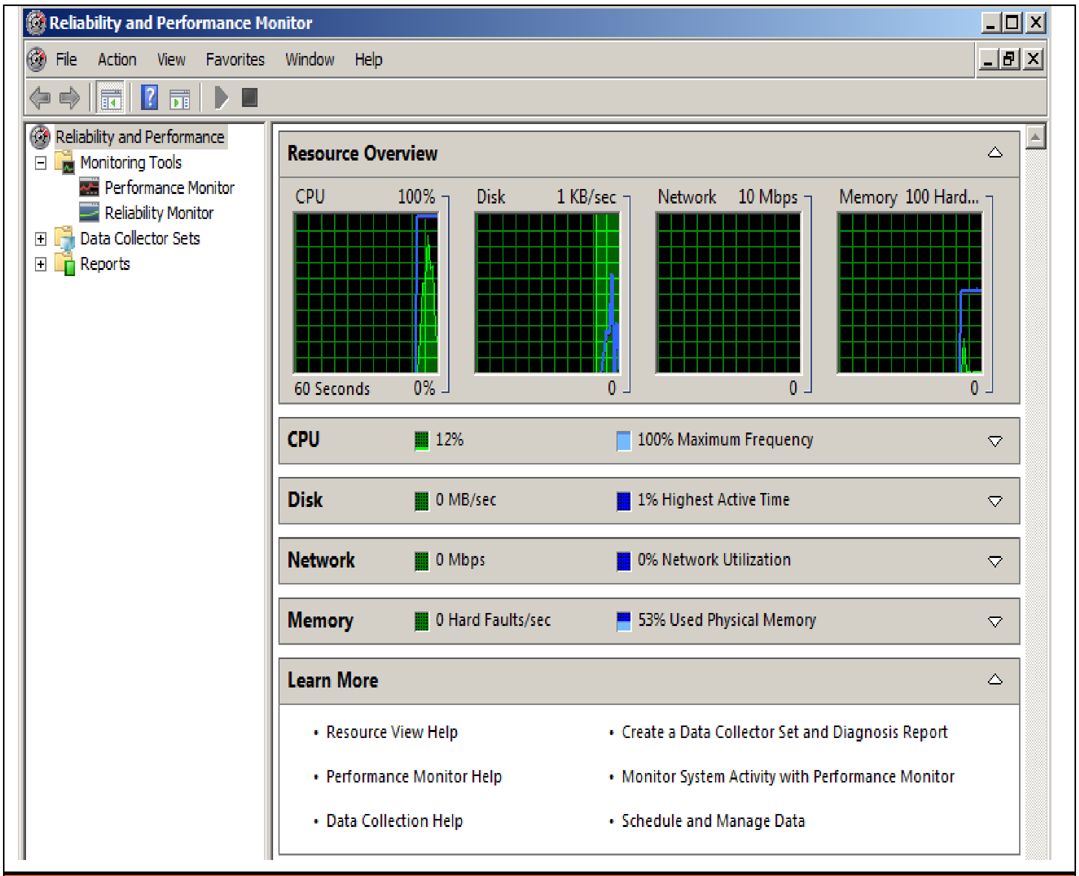
១០. Resource Monitor នឹងបង្ហាញក្រាហ្វិចមួយនៃទិន្នន័យរបស់អ្នកគ្រប់ពេលជាមួយរយៈពេល១វិនាទីម្តង (រូបភាព៧-២០) ។



រូប ៧-២០. Resource Monitor ដាក់ចំណុចនៃ data លើអ័ក្ស

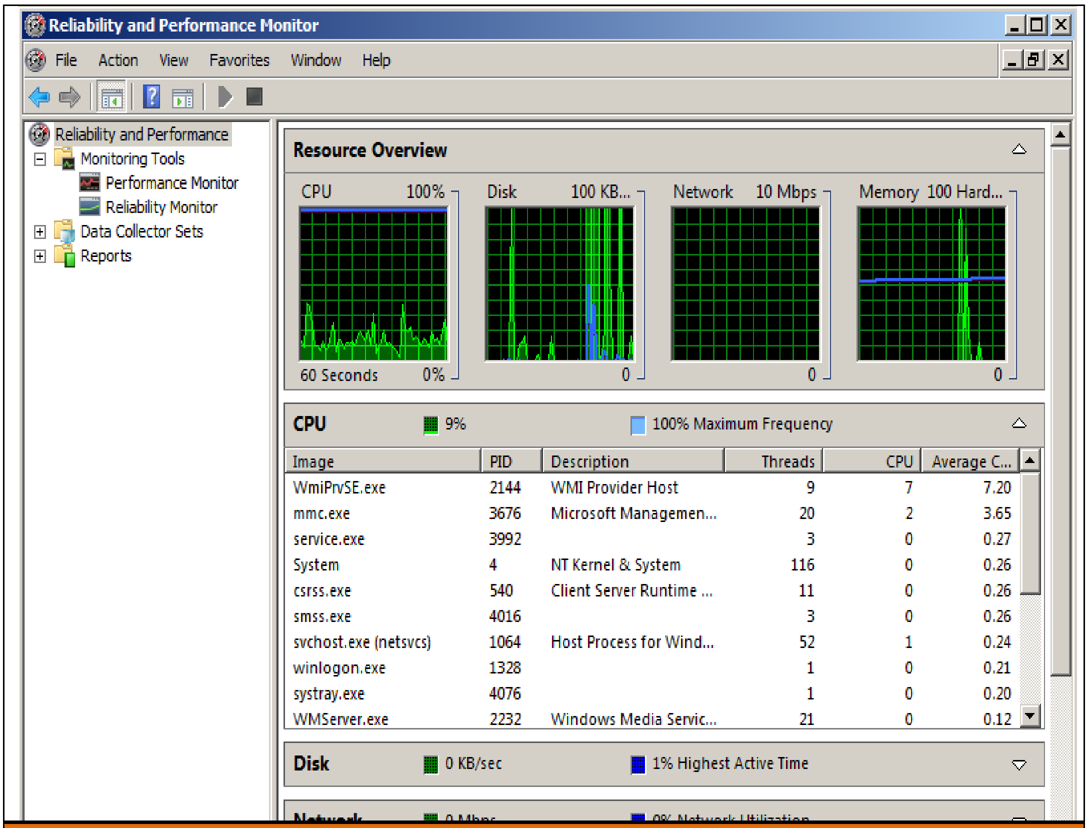
១៣-២- ភាពទុកចិត្តនិងការបង្ហាញពីសមត្ថភាព

ហេតុមកដល់ពេលនេះ យើងបានចំណាយពេលមួយចំនួនក្នុងការស្វែងយល់ពីរបៀបនៃការត្រួតពិនិត្យនូវ Sever resources របស់យើងដោយប្រើប្រាស់នូវ WSRM។ អ្វីដែលសំខាន់នោះគឺសមត្ថភាពនៃការអង្កេតនូវដំណើរការរបស់ Server ដែលដំណើរការក្នុងពីរគោលបំណងគឺសម្រាប់ប្រមូលផ្តុំនូវរង្វាស់នៃដំណើរការសម្រាប់ Baseline data set រឺក៏សម្រាប់ troubleshooting ហើយសម្រាប់សមត្ថភាពគម្រោង។ ដូចដែលអ្នកបានដឹងថា Resource Monitor អាចបង្ហាញបាននូវ Basic performance monitoringមួយចំនួនដែលអ្នកចង់បាននៅលើ Server។ ភាពមានទំនុកចិត្តនិងការបង្ហាញពីសមត្ថភាព គឺជាការរីកដុះដាលជាមូលដ្ឋានមួយនៃ Performance Monitor ដែលអាចប្រើប្រាស់បាននៅលើ Windows version មុនៗ។ Tool នេះនៅតែអនុញ្ញាតឱ្យអ្នកប្រមូលនូវរង្វាស់នៃដំណើរការ, ប៉ុន្តែវាក៏មាននូវសមត្ថភាពក្នុងការតាមដាននូវស្ថិតិនៃស្ថេរភាពនិងភាពដែលអាចទុកចិត្តបាននៃ Server។ នៅពេលដែលអ្នកចាប់ផ្តើមដំណើរការនូវភាពទុកចិត្តនិងការបង្ហាញពីសមត្ថភាព(Start→ Administrative Tools → Reliability and Performance Monitor) អ្នកនឹងបានឃើញនូវ Resource Overview, ដែលជាការបង្ហាញដោយសង្ខេបនូវរង្វាស់នៃដំណើរការសំខាន់ៗនៃ Server របស់អ្នក។ វាបង្ហាញនៅក្នុងពេលវេលាពិតនូវការប្រើប្រាស់ CPU, Memory ព្រមទាំង Disk, សកម្មភាព Network ហើយនិងបម្រើបម្រាស់។ អ្នកអាចទទួលបាននូវព័ត៌មានជាក់លាក់ជាងនេះដោយអ្នកចុចពីរដងលើទៅលើសញ្ញាព្រួញចុះក្រោមនៃប្រភេទនីមួយៗនៅខាងក្រោមក្រាហ្វ។ ឧទាហរណ៍ដើម្បីដឹងថាតើ Processes អ្វីខ្លះដែលធ្វើឱ្យ CPU cycles កើនឡើងនោះ អ្នកត្រូវចុចពីរដងផ្ទួននៅលើ CPU នោះ អ្នកនឹងបានឃើញនូវតារាងនៃProcess ដែលវាស្រដៀងទៅនឹងអ្វីដែលអ្នកបានឃើញនៅក្នុងTask Manager ។



រូប៧-២១. Resource Overview

ដូចជាមួយនឹង Performance Monitor, Resource Monitor នៅក្នុង WSRM អនុញ្ញាតឱ្យអ្នក បន្ថែមនូវ Performance Countersនិងតាមដាននូវដំណើរការរបស់ Performance Counters នោះ ដូចដែលអ្នកបានធ្វើជាធម្មតា លើកលែងតែនៅក្នុង Reliability និង Performance Monitor។ Counters ដែលបានជ្រើសរើសយកក៏អាចត្រូវបានប្រើដើម្បីបង្កើតនូវ Data Collector sets (នឹងសិក្សានៅក្នុងជំពូកផ្សេងទៀត)។ Reliability និង Performance Monitor ត្រូវបានពឹងផ្អែកទៅលើស្ថិតិនៃភាពបិតថេរ។ Reliability and Performance Monitor តាមដាននូវការផ្លាស់ប្តូរនៃ Server របស់អ្នកនិងតាមដាននូវ Error ដែលមិនបានព្រៀងទុកដែលត្រូវបានបកប្រែទៅជា Stability index ដែលអ្នកអាចប្រើដើម្បីវាស់នូវភាពដែលអាចទុកចិត្តបាននៃប្រពន្ធ័ Server របស់អ្នកទាំងមូល។ សរុបសេចក្តីមក បើសិនជា Server របស់អ្នកមានភាពទៀងទាត់ និងរឹតតែមានភាពជឿជាក់ទៅលើ Server ទៅទៀត។



រូប៧-២២. CPU detail view

ជារឿយៗ Local administrators បាន Access ទៅដំណើរការនូវការងារផ្សេងៗនៃតួនាទីប្រមូលព័ត៌មានអំពីសមត្ថភាព ទោះជាយ៉ាងនេះក្តី ក្រុមដែលមានស្រាប់ចំនួន២ដែលបានបន្ថែមត្រូវបានប្រើប្រាស់ដើម្បីអនុញ្ញាតឱ្យអ្នកមិនមែនជា administrators access ទៅដំណើរ ការទិន្នន័យ។ Group នៃ Performance log users គួរតែផ្ទុកនូវ user account ដែលអាចកំណត់ពេលវេលា logging ពី performance counter ដែលដាក់ឱ្យអាចតាមដាន providers និងប្រមូលនូវការកត់ត្រាព្រឹត្តិការណ៍ទាំងលក្ខណៈ local និង remotely។ សមាជិករបស់ក្រុមនៃ Performance Monitors users អាចបង្ហាញនូវ performance counters ជាលក្ខណៈ local និង remote។ Group នេះមានសារៈសំខាន់ណាស់ បើអ្នកចង់អនុញ្ញាតឱ្យអ្នកគ្រប់គ្រងដោយមិនមែនគ្រប់គ្រងដូចជា application

developers ឱ្យមើលនូវ data ពី performance របស់ server ពីចម្ងាយដោយមិនឱ្យសិទ្ធិពេញលេញជា administrators ក្នុងការ access ឡើយ។

គន្លឹះ:

បើអ្នកដំណើរការ Reliability and Performance Monitor ជាលក្ខណៈ local លើserver ដែលអ្នកចង់ត្រួតពិនិត្យ អ្នកត្រូវការផ្តល់នូវព័ត៌មានសម្រាប់ resources នៃprocessing និង memory បន្ថែមទៀត ដែលត្រូវបានប្រើដោយ tool ដែលនៅពេលមើលទៅកាន់ dataទាំងអស់។ ក្នុងករណីច្រើនទៀត វាអាចទំនងជាងក្នុងការកត់ត្រានូវperformance metrics ពីចម្ងាយពី server ឬ workstation ផ្សេង ដូច្នេះហើយវាកាត់បន្ថយនូវលទ្ធភាពនៃការកែច្នៃ data ដែលបានប្រមូលផ្តុំដល់កម្រិតអប្បបរមា។ Caveat គឺថាប្រសិនបើអ្នកតាមដាននូវ performance របស់network អ្នកក៏ត្រូវតែយកពត៌មានពីរាល់ចរាចរណ៍បន្ថែមដែលត្រូវបានបង្កើតដោយដំណើរការវាពីចម្ងាយ ។ ដូចនេះហើយក្នុងករណីនៃការតាមដានការធ្វើ utilization លើ network វាក៏ទំនងដែរ បើកត់ត្រាព័ត៌មាន log ដែលធ្វើជាលក្ខណៈ local លើ server នោះជំនួសវិញ។

Data Collector Sets

Data collector set គឺជាធាតុមួយដែលប្រើប្រាស់សម្រាប់ប្រមូលទិន្នន័យពីការប្រព្រឹត្តដំណើរការរបស់ Server របស់អ្នក។

ឧទាហរណ៍

data collector របស់ proce ssor ប្រមូលព័ត៌មានពី processor ដូចជាការធ្វើ utilization របស់វា ។ Data collectors មួយឬច្រើនអាចយកមកដាក់ជាក្រុមតែមួយដើម្បីផ្តុំបានជាទម្រង់ data collector set។ Data collector sets អាចប្រើប្រាស់សម្រាប់កំណត់នូវក្រុមនៃគោលរបស់ data ដែលអ្នកចាប់អារម្មណ៍ក្នុងការប្រមូលទិន្នន័យ។ អ្នកអាចដំណើរការនូវពេលការងារប្រមូលទិន្នន័យនេះដោយភ្លាមៗតាមគោលបំណងឬបញ្ហាឬក៏ធ្វើតាមការកំណត់ schedule រួចហើយធ្វើការបង្ហាញ Data នោះជាទម្រង់របាយការណ៍តាមរយៈ console របស់ Reliability and Performance Monitor។ នេះវាធ្វើឱ្យមានភាពងាយស្រួលក្នុងការប្រមូលទិន្នន័យពីដំណើរការ។

ឧទាហរណ៍៖ អ្នកអាចបង្កើតនូវ data collector set ដើម្បីទទួលបាននូវចំនួន metrics នៃបទដ្ឋានរបស់ដំណើរការមួយចំនួនដូចជា CPUនិងការប្រើប្រាស់ memory ក៏ដូចជាសេវា Terminal មួយចំនួនដែលទាក់ទងនឹងការរាប់ចំនួនទៅលើ Session ដែលមានសកម្មភាពនិងគ្មានសកម្មភាព។ បន្ទាប់មកអ្នកក៏អាចធ្វើការកំណត់ថ្ងៃឱ្យ data collector set នោះដំណើរការពីម៉ោង 6:00 P.Mដល់ 6:00 A.Mដូច្នេះអ្នកអាចធ្វើការតាមដាននូវដំណើរការនិងការប្រើប្រាស់នៃ terminal serverក្នុងកំឡុងពេលដែលគ្មានដំណើរការអាជីវកម្ម។ នេះជាឧទាហរណ៍ដែលសាមញ្ញបំផុតប៉ុន្តែខ្ញុំប្រាកដថាអ្នកនឹងយល់ជាមិនខាន ។

Data collector set អាចបង្កើតឡើងតាមមធ្យោបាយមួយក្នុងចំណោមមធ្យោបាយបីគឺតាម Performance Monitor, template និងកំណត់ដោយខ្លួនឯងផ្ទាល់។ ការបង្កើត Data collector set ដោយប្រើ Performance Monitor ជាប់ទាក់ទងទៅនឹងការដាក់បន្ថែមនូវរាល់ counter objects ទៅកាន់ Performance Monitor ហើយប្រើប្រាស់តារាងនៃ counter នោះមកបង្កើតជា data collector sets។ Windows ផ្តល់នូវឈុតគំរូដែលអាចចាប់យកមកប្រើមួយចំនួនធំដែលអ្នកអាចយកវាមកប្រើជាចំណុចចាប់ផ្តើមក្នុងការបង្កើតនូវ data collec

-tor sets អ្នកក៏អាចបង្កើតនូវឈុតគំរូដោយខ្លួនឯងផ្ទាល់ពី data collector sets ដែលមានស្រាប់ផងដែរដែលអាចត្រូវបានយកនាំចូលនិងប្រើប្រាស់ជាឈុតគំរូសម្រាប់បង្កើតនូវ data collector sets ថ្មីមួយ។ អ្នកក៏អាចបង្កើត data collector sets ដែលកំណត់ដោយខ្លួនឯងផងដែរគឺកំណត់និងទាញយកទិន្នន័យ សូម្បីតែតាមដានទិន្នន័យនិងព័ត៌មានរបស់ system configuration ដែលបានពី counters នៃដំណើរការ ។ Data collector sets ក៏អាចប្រើប្រាស់សម្រាប់ពិនិត្យមើលការប្រព្រឹត្តរបស់ប្រព័ន្ធនិងបង្កើតឡើងនូវការបង្ហាញឱ្យដឹងពីនូវដែលទៅដល់កម្រិតមួយជាក់លាក់ ។

លំហាត់អនុវត្តៈ «ការបង្កើត Data Collector Set ពី Performance Monitor»

ក្នុងឧទាហរណ៍នេះ យើងនឹងធ្វើការបង្កើតនូវ data collector set ដោយត្រួតពិនិត្យមើលលើ performance metrics គោលៗពី server របស់យើងដែលយើងហៅវាថា Baseline Performance Metric

<u>ជំហាននៃការអនុវត្តៈ</u>

១. ជ្រើសរើសយក Start ->Administrative Tools -> Reliability and Performance Monitor

២. ចុចពង្រីកលើចំណុច Monitoring Tools ដែលមាននៅក្នុង navigation pane ផ្ទាំងជ្រើសរើសមុខងារ

៣. ចុចរើសយក Performance Monitor

៤. ដោយកំណត់ជាស្រេច, % Processor Time របស់អ្នកគឺត្រូវបានដាក់បន្ថែមដោយស្វ័យប្រវត្ត និងរួចរាល់ក្នុងការត្រួតពិនិត្យមើលប្រព័ន្ធរបស់អ្នក ។

៥. ចុចលើសញ្ញា (+) ពណ៌បៃតងខាងលើក្រាហ្វដើម្បីបន្ថែម counters ។

៦. ក្នុងតារាងនៃ Available Counters ចូរបន្ថែមនូវ counters ដូចខាងក្រោម ដោយការចុចពង្រីកលើ Category ដែលសមស្របហើយរើសយក counter ។ រួចចុច Add នៅពេលអ្នករួចរាល់ ។

Memory: % **Committed Bytes In Use**

Memory: **Page Faults/sec**

Network Interface: **Bytes Received/sec**

Network Interface: **Bytes Sent/sec**

Server: **Logon/sec**

Server: **Server Sessions**

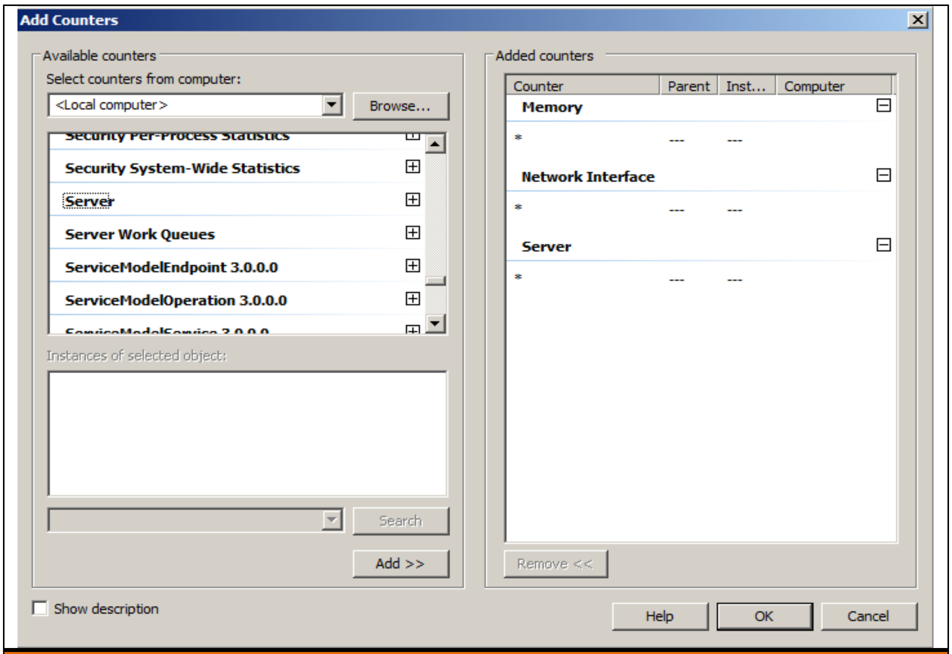
ផ្ទាំង Add Counters គួរតែមើលទៅដូចក្នុងរូប ៧-២៣

៧. ចុចលើ Ok ដើម្បីធ្វើការបន្ថែមនូវ counters ចូលក្នុង Performance Monitor ។

៨. ចុច Mouseស្តាំលើPerformance Monitor ហើយរើសយក New | Data Collector Set ។

៩. វាយ Baseline Performance Metrics ចូលដែលដាក់ឈ្មោះឱ្យ Data Collector Set ហើយចុច Next ។

១០. ទិន្នន័យដែលបានប្រមូលពី data collector ជាទូទៅត្រូវបានរក្សាទុកក្នុង %system drive%\perflogs\<*Name of Data Collector Sets*> ។ ដាក់វាទំនេរដូចឱ្យវាយកទីតាំងដែលវាកំណត់ជាស្រេច ឬក៏ចុចរើសយកទីតាំងដែលអ្នកចង់ឱ្យទិន្នន័យនោះរក្សាទុក រួចចុច Next ។



រូប ៧-២៣. បន្ថែម Counters

១១. ចូរជ្រើសយក Save and Close នៅក្នុងផ្ទាំង dialog នៃ Create New Data Collector Set និងរួច ហើយចុចលើ Finish (រូបភាព ៧-២៤) ។

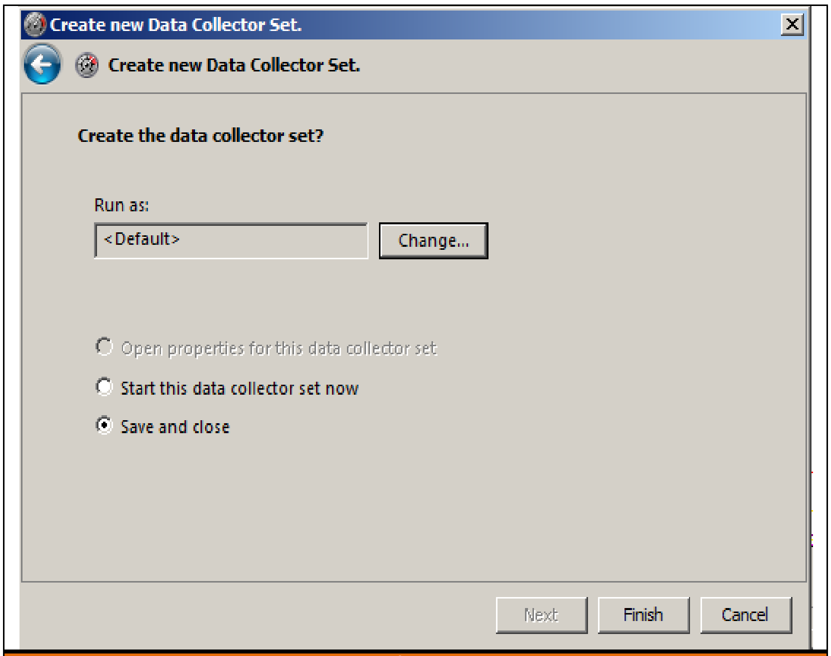
១២. ធ្វើការផ្ទៀងផ្ទាត់ data collector set ដែលត្រូវបានបង្កើតដោយការចុចពង្រីកលើ node នៃ Data Collector Sets ហើយជ្រើសយក User Defined ។ ហើយត្រូវប្រាកដថា data collector set នៃ Baseline Performance Metric វាបានលេចឡើង ។

១៣. ចុច mouse ខាងស្ដាំលើ Baseline Performance Metric Data Collector Set នៅឯ Navigation Pane រួចជ្រើសយក Properties ។

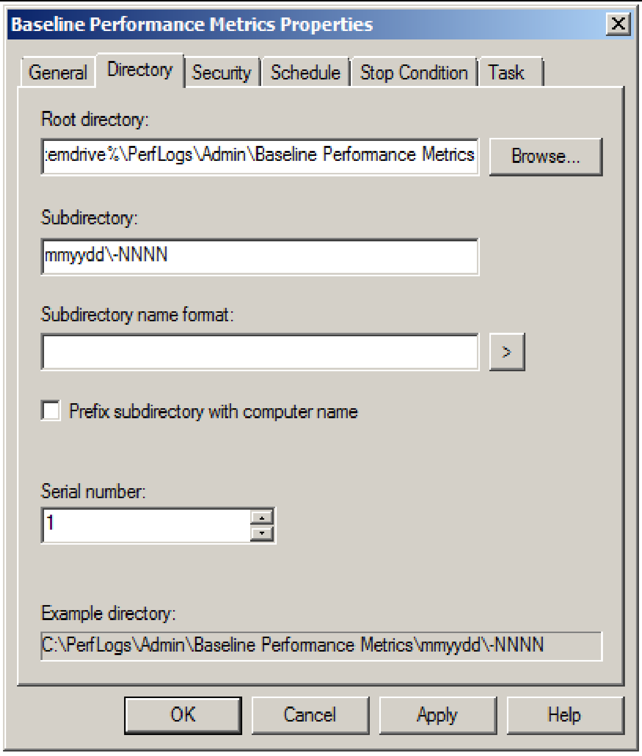
១៤. ចុចលើ tab នៃ Directory ។

១៥. នៅឯ format របស់ subdirectory name ចូរវាយ mmyydd\-NNNN ។ នេះនឹងបង្កើត subdirectory ដោយលក្ខណៈ dynamic រាល់ពេលដែល data collector set នេះត្រូវបានប្រតិបត្តិ ជាមួយនឹង format នៃកាលបរិច្ឆេទបច្ចុប្បន្ន ដោយមានសញ្ញា(-)មួយ និងលេខ serial number (មើលរូបភាព ៧-២៥)

១៦. ចុច Ok ដើម្បីរក្សាទុក និងបិទ ។



រូប ៧-២៤. ការបង្កើត data collector set



រូប ៧-២៥. ការកំណត់ឱ្យច្បាស់នៃ subdirectory name

លំហាត់អនុវត្តៈ «ការកំណត់ពេលឱ្យ Data Collector Set ឱ្យដំណើរការរាល់ថ្ងៃ»

ប្រសិនបើអ្នកចង់ប្រមូលទិន្នន័យលើ performance metrics ជាប្រចាំដោយមិនបាច់កំណត់ដោយខ្លួនឯងនូវ data collection ឱ្យដំណើរការ, អ្នកអាចកំណត់ពេលវេលាឱ្យ data collector set នោះដំណើរការនៅថ្ងៃខែ និងពេលជាក់លាក់ណាមួយ។ ក្នុងលំហាត់នេះ យើងនឹងធ្វើការកំណត់ពេលឱ្យ data collector set នៃ Baseline Performance Metric ដែលយើងបានបង្កើតក្នុងលំហាត់មុខៗឱ្យដំណើរការពីថ្ងៃច័ន្ទដល់ថ្ងៃសុក្រពីម៉ោង ៩ ព្រឹក ដល់ម៉ោង ៦ ល្ងាច ។

ជំហាននៃការអនុវត្តៈ

១. បើក Reliability and Performance Monitor ។

២. ចុចពង្រីកលើផ្នែក Data Collector Sets និង User Defined ។

៣. ចុច mouse ស្តាំលើ Baseline Performance Metric និងជ្រើសរើសយក Properties

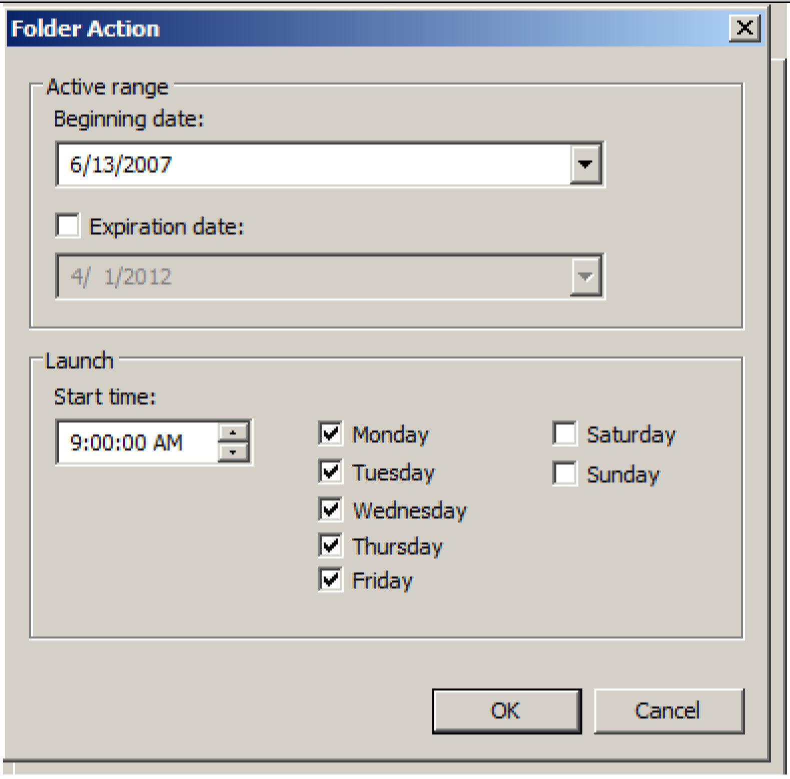
៤. ចុចលើ Schedule Tab ។

៥. ចុចលើប៊ូតុង Add ។

៦. កំណត់ Start Launch Time ទៅ 9:00:00 AM និងដោះធីកលើ Saturday និង Sunday រួចចុច OK (រូប ៧-២៦) ។

៧. ចុចលើ Stop Condition Tab ។

៨. ដាក់ធីកត្រង់ Overall Duration និងចុចបញ្ចូល 9 Hours សម្រាប់រយៈពេល (ពី 9:00:00 A.M. ទៅ 6:00:00 P.M.) ។ រួចចុច ok (ដូចរូប ៧-២៧) ។



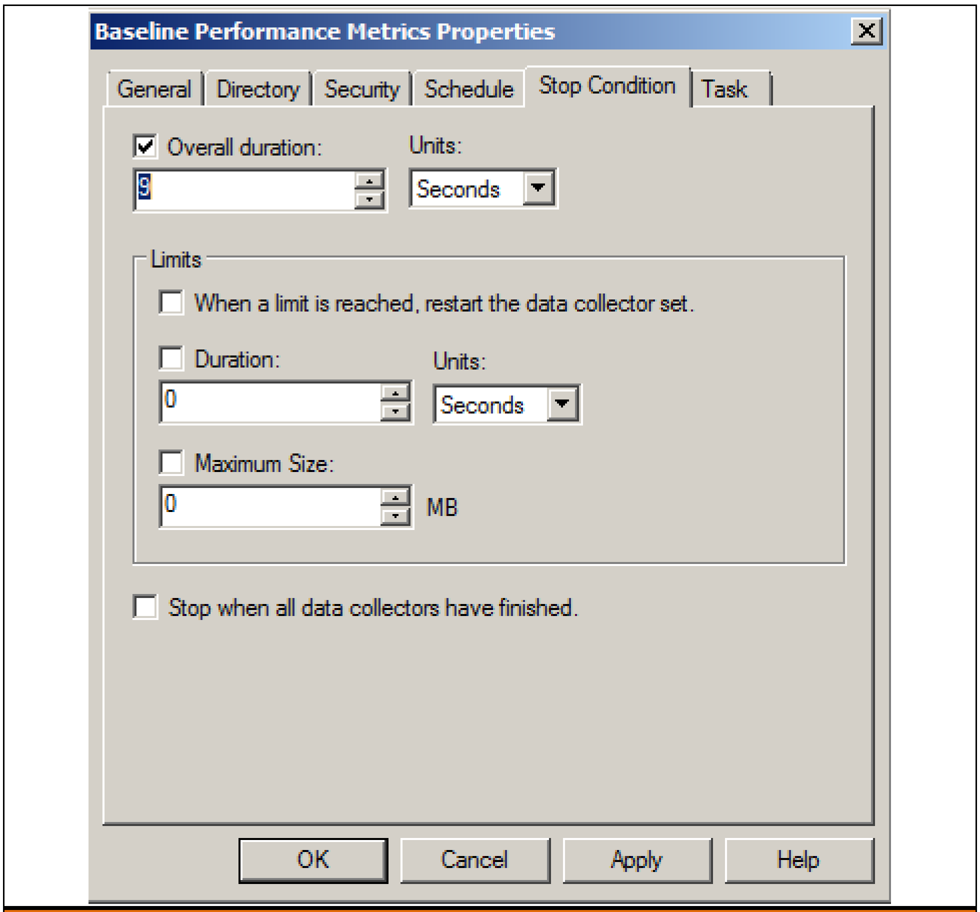
រូប៧-២៦. ការជ្រើសរើស Launch Schedule

ការបង្ហាញឱ្យឃើញពីទំនុកចិត្ត

ការបង្ហាញឱ្យឃើញពីទំនុកចិត្តគឺវិធីដ៏ល្អមួយក្នុងការទទួលបានន័យទូទៅ ថាតើ Server របស់អ្នកកំពុងតែដំណើរការក្នុងការវាយតម្លៃមួយដែលបានស្ថិតក្នុងស្ថានភាពល្អប្រសើរនិងនឹងនរ។ រាល់ថ្ងៃប្រព័ន្ធគឺត្រូវបានយកទៅប្រៀបធៀបនឹងរបាយការណ៍ទាំងឡាយណាដែលគេបានដឹងថាប្រព័ន្ធមានស្ថេរភាព។ វារាប់នូវចំនួនរបស់ softwa - re ដែលបានបញ្ចូលនិងបានលុបចេញក្នុងកំឡុងពេល ២៤ ម៉ោងមុនមកដល់ឥឡូវ។ វាស្វែងរកមើលនូវការបរាជ័យ

ទាំងឡាយដែលអាចបានកើតឡើងពី application,hardware, Windows និងផ្នែកផ្សេងៗទៀត។ ដោយការប្រើប្រាស់នូវ Algorithm ព័ត៌មាននេះនឹងបន្ទាប់មកត្រូវបានបកប្រែជា index ដែលបង្ហាញពីស្ថេរភាពរបស់ប្រព័ន្ធ ដែលមានចាប់ពីលេខ ១ ដល់ ១០ ដែលលេខ ១០ សំគាល់លើភាពមានស្ថេរភាពជាងគេ។ លេខ index នេះគឺត្រូវបានបង្ហាញនៅលើ System Stability Chart ដូច្នេះអ្នកអាចកំណត់នូវភាពដែលអាចទុកចិត្តលើ server របស់អ្នក តាមពេលវេលាមួយ ។

ប្រសិនបើមានការប្រែប្រួលឬក៏បរាជ័យថ្មីៗបានកើតមានបណ្តាលឱ្យមានលេខ index ទាបជាងនោះ អ្នកនឹងអាចស្វែងរកបាននូវព័ត៌មានបន្ថែមទៀតដោយចុចពង្រីកលើផ្នែក category ដែលទាក់ទងនោះក្នុងរបាយការណ៍ដែលបង្ហាញពីស្ថេរភាពរបស់ System ដែលស្ថិតនៅក្រោមប្លង់ក្រាហ្វិកនោះ។ ប្រភេទនីមួយៗទាំងនេះមានផ្ទុកនូវព័ត៌មានសំខាន់ៗដែលអ្នកអាចប្រើសម្រាប់ធ្វើការ troubleshoot លើ server របស់អ្នក។ ជាឧទាហរណ៍ ប្រសិនបើមានការបរាជ័យរបស់ Windows វានឹងបង្ហាញប្រភេទនៃការបរាជ័យ(boot failure ឬ OS Crash), OS version, service pack, និងព័ត៌មានលំអិតពីការបរាជ័យដែលរួមមាន codes ដែលបញ្ជាក់ពីការឈប់ដំណើរការ និងហេតុផលនិងក៏អាចមាននូវកាលបរិច្ឆេទនិងពេលវេលាថាការបរាជ័យនោះបានកើតឡើងនៅពេលណាផងដែរ

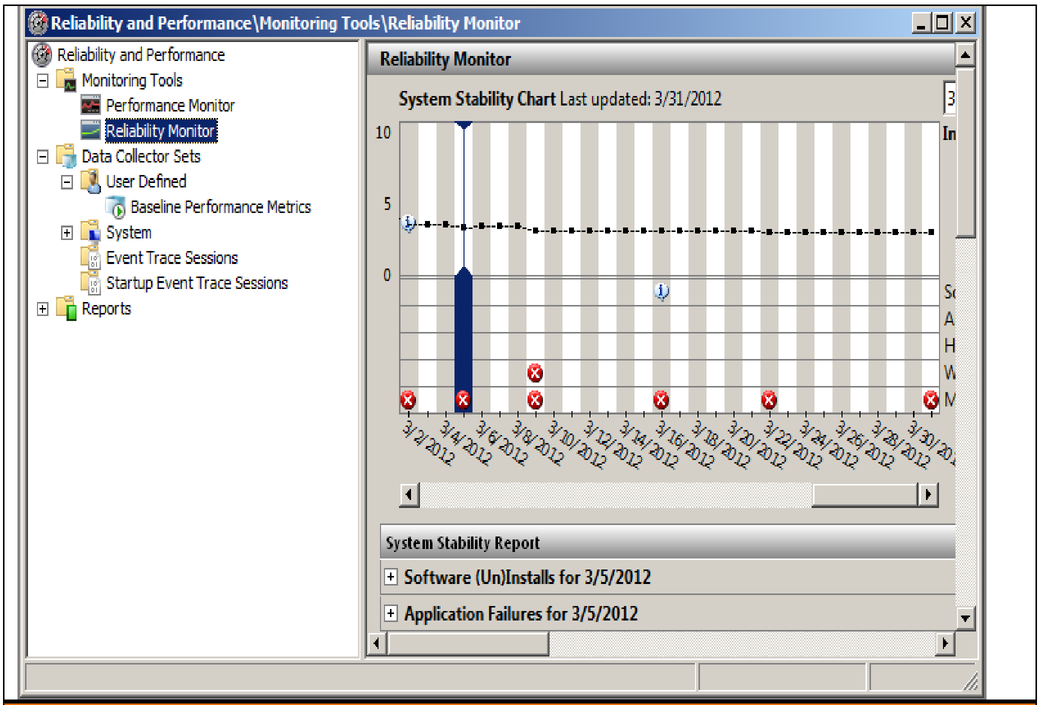


រូប ៧-២៧. ការកំណត់ឱ្យច្បាស់នូវលក្ខខណ្ឌសម្រាប់បញ្ឈប់

អ្នកគួរតែកត់ចំណាំនូវផ្នែកខាងក្រោមនេះដែលនិយាយអំពី Reliability Monitor ដែលរួមមានថាតើវាកើតឡើងយ៉ាងម៉េចជាមួយនឹង លេខ index នៃស្ថេរភាពដូចជា៖

- ការបរាជ័យដែលកើតឡើងថ្មីៗនេះវាមានភាពធ្ងន់ធ្ងរជាងភាពបរាជ័យពីមុន ។
- ប្រព័ន្ធនោះបានមិនរាប់បញ្ចូលនូវថ្ងៃណាដែល server បិទ ឬក៏ស្ថិតក្នុងសភាពដេកលក់ជាស្វ័យប្រវត្ត

- គំនូសអុចៗត្រូវបានប្រើក្នុងប្លង់ក្រាហ្វិកនៅពេលណាដែលទិន្នន័យមានមិនគ្រប់គ្រាន់សម្រាប់ការគណនារក index នៃភាពនឹងនរដែលគួរឱ្យជឿជាក់មួយ។ នេះប្រហែលជាមកពីភាពនឹងនរនោះបានប្រែប្រួលថេរក្នុងតម្លៃឬក៏serverទើបនឹងបានដំឡើង
- រាល់ការប្រែប្រួលសំខាន់ៗក្នុង systemត្រូវបានកត់ត្រាលើក្រាហ្វដើម្បីបញ្ជាក់ពី ការកែប្រែនូវម៉ោងរបស់ប្រព័ន្ធ ។ វានឹងបង្ហាញពីពេលវេលាចាស់ ពេលវេលាថ្មីនិងថ្ងៃដែលការកែប្រែនោះបានធ្វើឡើង (ដោយផ្អែកលើពេលវេលាថ្មី) ។
-



រូប៧-២៨. Reliability Monitor System Stability Chart

របាយការណ៍

របាយការណ៍គឺជាហេតុផលមួយដ៏សំខាន់ដែលជាហេតុដែលអ្នកចង់ប្រើប្រាស់ data collectors set នៅពេលដែលប្រមូលនូវរង្វាស់ស្ថិតិនៃដំណើរការអំពី Server របស់អ្នក។ នៅពេលដែលសំណុំប្រមូលទិន្នន័យកំពុងតែដំណើរការ វារក្សាទុករាល់បញ្ជីនៃទិន្នន័យនោះទុកទៅក្នុង log file នៅក្នុងថតឯកសារដែលអ្នកបានកំណត់។ នៅពេលបញ្ឈប់ការប្រមូលទិន្នន័យនោះ ទិន្នន័យដែលបានមកពីការប្រមូលនេះត្រូវបានដាក់ថាអាចយកទៅប្រើប្រាស់បានចំពោះអ្នក នៅក្នុងទម្រង់ជារបាយការណ៍។ របាយការ ណ៍បង្ហាញនូវរបាយការណ៍សង្ខេបនៃដំណើរការឬក៏ផ្ទាំងនៃ Performance Monitor ជាមួយនឹងទិន្នន័យពី file ទិន្នន័យជាជាងពីផ្ញើរទិន្នន័យដែលបានក្នុងពេលដំណើរការតែម្តង។

ឧទាហរណ៍

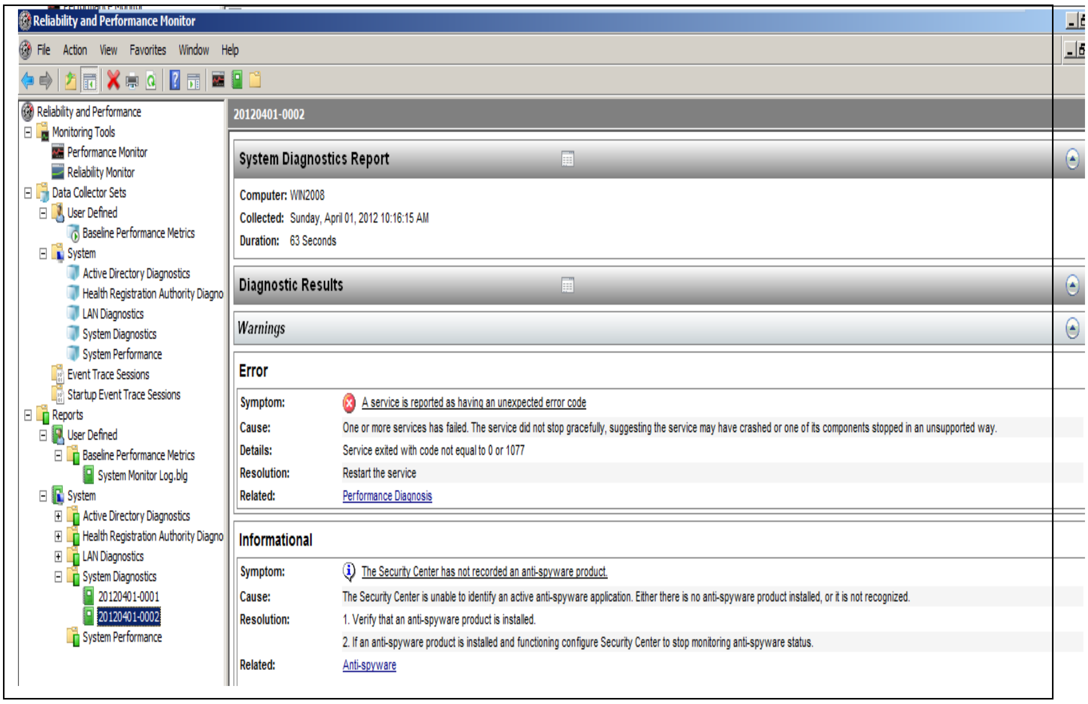
ប្រសិនបើសំណុំប្រមូលទិន្នន័យនៃ System Performanceដែលដំណើរការក្នុងរយៈពេល ១២ ម៉ោង នោះលទ្ធផលនឹងបញ្ចេញនូវរបាយការណ៍ Performance Monitor ដែលនឹងបង្ហាញនូវក្រាភិចនៃរាល់បញ្ជីនៃទិន្នន័យដែលបានប្រមូលសម្រាប់សំណុំឯកសារនេះក្នុងពេល១២ ម៉ោងពេញនេះ។ អ្នកអាចឃើញនូវទំនោរទិសដៅនៃ

Server របស់អ្នកនិងប្រើប្រាស់វាដើម្បីតាមដានការឡើងចុះក្នុងប្រព័ន្ធរបស់អ្នកដែលអាចចង្អុលបង្ហាញឱ្យឃើញពីបញ្ហានៃសមត្ថភាពឬការដំណើរការ។ ឧទាហរណ៍ ប្រសិនបើអ្នកកំណត់ចំណាំនៅចន្លោះម៉ោង 12:00P.M.និង 1:00P.M ការឡើងចុះដ៏ច្រើនសំបើមបានកើតឡើងក្នុងដំណើរដែលធ្វើឱ្យ processor មានប្រសិទ្ធភាពអ្នកប្រហែលជាចង់ស៊ើបរកថាតើមានកិច្ចការដែលបានគ្រោងទុកនោះកំពុងដំណើរការឬអត់នៅពេលដែលវាអាចធ្វើឱ្យកើតមានការឡើងចុះនោះ ។

របាយការណ៍អាចចូលមកប្រើតាមផ្នែក Reliability and Performance Monitor។ ចុចពង្រីកចំណុចត្រង់របាយការណ៍ដើម្បីរើសយកផ្នែកមកប្រើហើយពេលនោះ អ្នកនឹងឃើញចែកចេញជាពីរចំណាត់ថ្នាក់គឺ User Defined(កំណត់ជាស្រេចតាមអ្នកប្រើប្រាស់)និង System(ការកំណត់ជាស្រេចតាមប្រព័ន្ធ)។ របាយកាណ៍ពីដំណើរការដែលកំណត់ដោយ System មានផ្ទុករបាយការណ៍ទាំងឡាយណាដែលផលិតចេញដោយសំណុំប្រមូលទិន្នន័យដែលកំណត់បានពីប្រព័ន្ធ។ សំណុំប្រមូលទិន្នន័យដែលកំណត់បានពីប្រព័ន្ធនោះត្រូវបានគេកំណត់លក្ខណៈជាស្រេច ដូច្នេះហើយថត directory ដែលសម្រាប់ដាក់លទ្ធផលនោះមានលក្ខណៈបត់បែនតាមការប្រែប្រួលតាម ថ្ងៃ ខែ ឆ្នាំ និងលេខលំដាប់នៅរាល់ពេលដែលសំណុំប្រមូលទិន្នន័យបានប្រតិបត្តិ។ រាល់ពេលដែលអ្នកធ្វើការហៅមកប្រើប្រាស់នូវសំណុំប្រមូលទិន្នន័យមួយក្នុងចំណោមពួកវាទាំងអស់របាយការណ៍ថ្មីមួយនឹងត្រូវបង្កើតដែលដាក់ជាមួយថ្ងៃខែឆ្នាំនិងលេខលំដាប់ដូចដែលបានប្រើលើថតផ្ទុកវានោះដែរ, ដូចបានបង្ហាញក្នុងរូបភាព ៧-២៩ ។

តាមការកំណត់ជាស្រេចរបស់វា នៅពេលដែលអ្នកធ្វើការបើកមើលនូវរបាយការ ណ៍ដែលកំណត់តាមអ្នកប្រើប្រាស់ អ្នកនឹងឃើញតែផ្នែកបង្ហាញនៃផ្នែកការត្រួតពិនិត្យលើដំណើរការនៃទិន្នន័យដែលបានកត់ត្រាទុករបស់អ្នកតែប៉ុណ្ណោះ។ អ្វីដែលអ្នកប្រហែលជាចង់បាននោះគឺជារបាយការណ៍ជាក់ច្បាស់មួយដែលសង្ខេបនូវទិន្នន័យដែលបានប្រមូលមកទៅជាអ្វីដែលអាចបង្ហាញបានមកក្នុងការគ្រប់គ្រង។

អ្វីដែលខ្ញុំបានផ្តល់ឱ្យក្នុងឧទាហរណ៍ សម្រាប់បង្កើតសំណុំនៃភ្នាក់ងារប្រមូលទិន្នន័យដែលកំណត់តាមអ្នកប្រើប្រាស់គឺ ថាបើអ្នកចង់ឱ្យអាចបង្កើតចេញនូវរបាយការណ៍មានលក្ខណៈប្រណិតដូចដែលអ្នកបានឃើញក្នុងរូប ៧-២៩សម្រាប់សំណុំទាំងឡាយនៃភ្នាក់ងារប្រមូលទិន្នន័យ ដែលកំណត់តាមប្រព័ន្ធអ្នកនឹងត្រូវផ្លាស់ប្តូរនូវលក្ខណៈខ្លះៗនៃសំណុំភ្នាក់ងារប្រមូលទិន្នន័យរបស់អ្នកដើម្បីឱ្យវាអាចធ្វើការគ្រប់គ្រងលើទិន្នន័យនិងការផលិតរបាយការណ៍ ។



រូប៧-២៩. ទម្រង់គោលការណ៍គម្រោងពេលវេលាពេញលេញ

លំហាត់អនុវត្តៈ ការកំណត់ទ្រង់ទ្រាយលក្ខណៈនៃសំណុំប្រមូលទិន្នន័យ (Data Collector Set) ឱ្យវាផលិតនូវរបាយការណ៍ ។

នៅក្នុងលំហាត់នេះ យើងនឹងធ្វើការកំណត់ទ្រង់ទ្រាយនៃសំណុំប្រមូលទិន្ន័យ Baseline Performance Metrics ដែលយើងបានបង្កើតនៅក្នុងឧទាហរណ៍មុនៗដើម្បីអនុញ្ញាតឱ្យវា ផលិតចេញនូវផ្ទៃបង្ហាញរបស់របាយការណ៍។

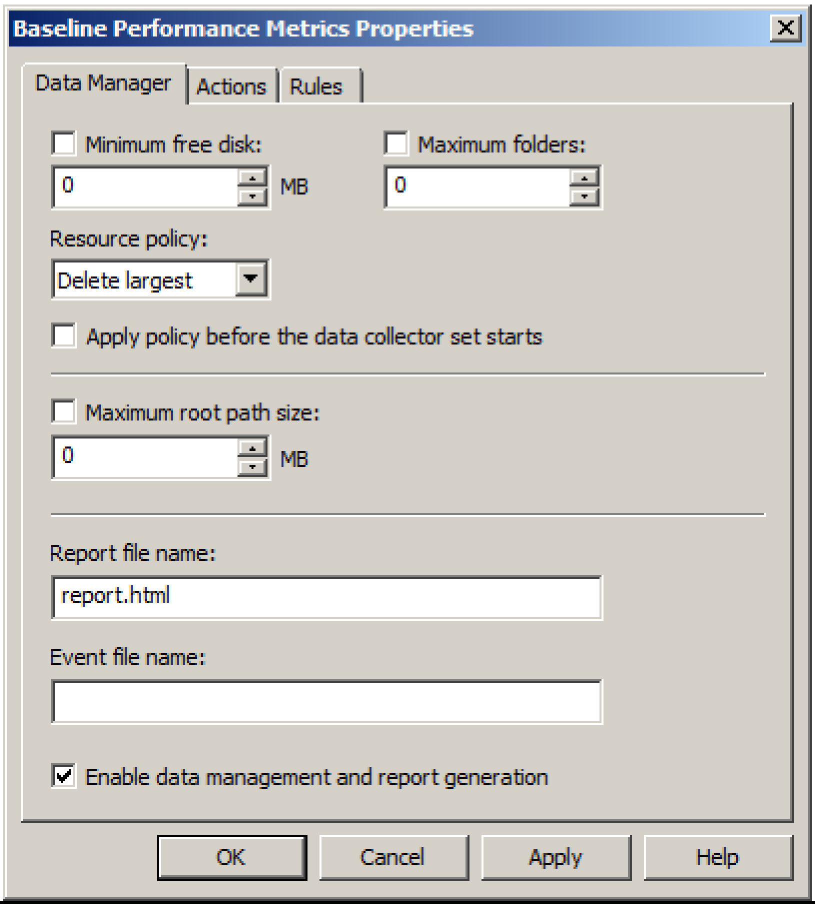
<u>ជំហានអនុវត្តៈ</u>

១. ចូរបើកមុខងារ Reliability and Performance Monitor ។

២. ចុចចំណុចពង្រីកលើ Data Collector Sets រួចយកពាក្យ User Defined ។

៣. ចុច Mouse ខាងស្តាំទៅលើ Baseline Performance Metrics រួចរើសយក Data Manager

៤. នៅឯផ្ទាំង Data Manager ចូរចុចគ្រីសជ្រើសរើស Enable Data Manage ment and Report Generation ក្នុងប្រអប់ជ្រើសរើស រួចចុច OK (រូប៧-៣០)



រូប៧-៣០. ការដាក់ឱ្យមុខងារការគ្រប់គ្រងទិន្នន័យ និងការផលិតរបាយការណ៍ដំណើរការបាន

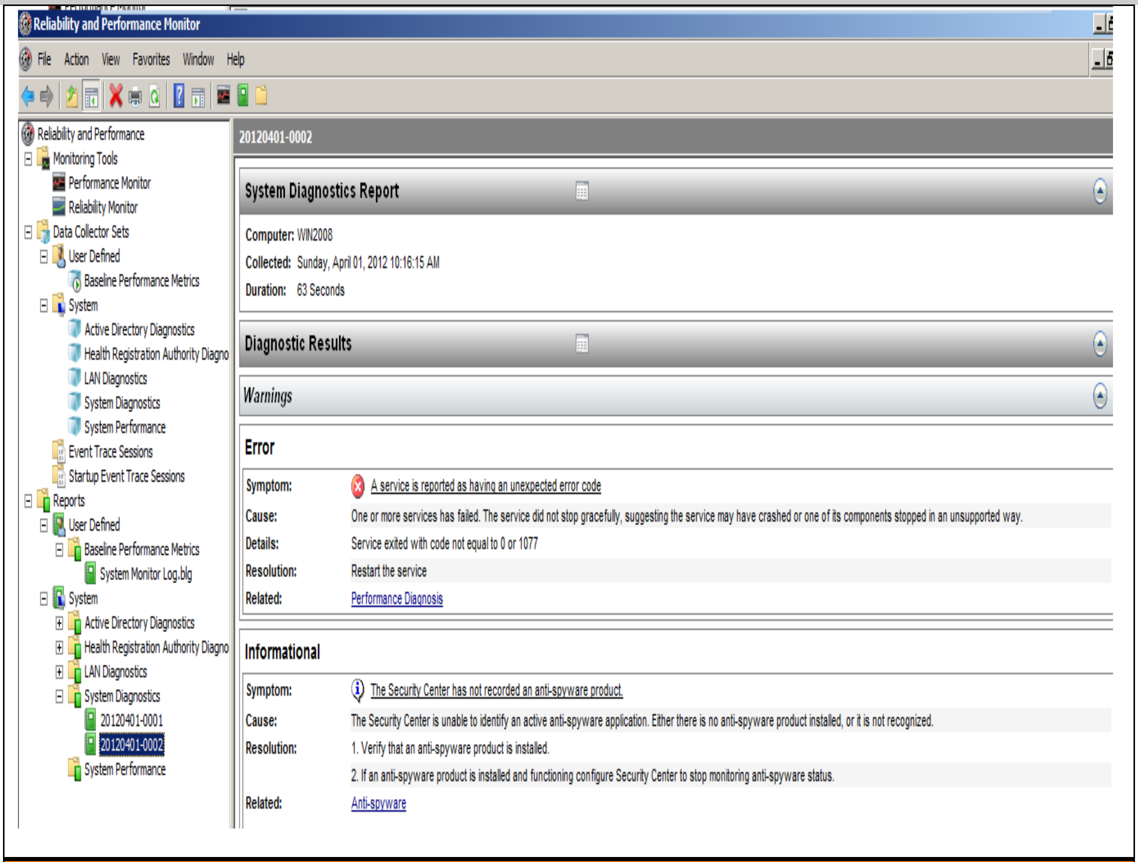
៥. ដើម្បីប្រើសាកល្បងនូវមុខងារធ្វើរបាយការណ៍នោះ ចូរចុច Mouse ខាងស្តាំលើ Baseline Performance Metrics រួចចុចយក Run Start ។

៦. ចូររង់ចាំប្រហែលជាប៉ុន្មាននាទីឬក៏ប៉ុន្មាននាទី ដូច្នេះវាមានពេលសម្រាប់ប្រមូលទិន្នន័យខ្លះ រួចហើយចុចMouse ស្តាំលើ Baseline Performance Metrics ម្តងទៀត រួចចុចយក Stop។

៧. ចុចលើចំណុចពង្រីករបស់ Reports រួចចុចយក User Defined ។

៨. ចុចលើចំណុចពង្រីករបស់ Baseline Performance Metrics រួចចុចយករបាយការណ៍ដែលទើបនឹងបង្កើតថ្មីនោះ ។ របាយការណ៍នោះគួរតែមើលទៅប្រហែលនឹងក្នុងរូប ៧-៣១។

៩. ដើម្បីផ្លាស់ទៅការបង្ហាញរបស់ Performance Monitor ចូរចុចរើសយករបាយការណ៍មួយដែលមានឈ្មោះថា System Monitor Log.blg ។



រូប៧-៣១. ការបើកមើលនូវរបាយការណ៍របស់ data collector set ដែលកំណត់ឡើងដោយ User

សង្ខេបមេរៀនក្នុងជំពូក៖

ការត្រួតពិនិត្យមើលការដំណើរការរបស់ Server របស់អ្នកឱ្យមានប្រសិទ្ធិភាពរួចធ្វើឱ្យវាដំណើរការបានល្អដោយបានធ្វើឱ្យអ្នកអាចបង្កើនសមត្ថភាពរបស់វាដល់ចំណុចអតិបរមានោះគឺពិតជាអ្វីដែលកិច្ចការគ្រប់គ្រងធនធានរបស់ Server និងការត្រួតពិនិត្យលើដំណើរការរបស់ Server ចង់និយាយ។ អ្នកត្រូវការចាំបាច់ប្រមូលនូវជាតុទិន្នន័យឱ្យគ្រប់គ្រាន់អំពីដំណើរការរបស់ Server កំឡុងវគ្គនៃប្រតិបត្តិការដែលបង្ហាញចេញនូវលក្ខណៈ

ដំណើរការអាចឱ្យយើងដឹងបាននូវការប្រែប្រួលតាមពេលក្នុងសមត្ថភាពនិងដំណើរការរបស់វា។ ទិន្នន័យនេះអាចត្រូវបានប្រើប្រាស់ដើម្បីកំណត់ឱ្យផ្លាស់ប្តូរនៃការទទួលនូវ Servers ប៉ុន្មានបន្ថែមទៀត ឬក៏ធ្វើឱ្យប្រសើរឡើងនៃ Server ទាំងឡាយណាដែលមានហើយ។វាក៏អាចជួយឱ្យអ្នកសម្គាល់ដឹងនូវផ្នែកសំខាន់ដែលធ្វើឱ្យដំណើរការមានភាពរាំងស្ទះក្នុងប្រព័ន្ធហើយវាក៏អាចឱ្យអ្នកធ្វើការរុករកនូវបញ្ហារបស់ Server និងបញ្ហារបស់កម្មវិធី (application)ផ្សេងៗយ៉ាងមានប្រសិទ្ធភាព ។

ចូរទាញយកឱ្យបាននូវគុណប្រយោជន៍នៃសមត្ថភាពថ្មីមួយទៀតលើការត្រួតពិនិត្យលើថាមពលរបស់ Server របស់អ្នកតាមរយៈការប្រើប្រាស់នូវសូចនាករជំនឹងនរមួយ ។ ទោះបីជាសូចនាករជំនឹងនរនោះ អាចមានភាពលំអៀងបន្តិចលើ Server ដែលទើបនឹងដំឡើងថ្មីៗ ដោយសារតែមានការផ្លាស់ប្តូរជាច្រើនសន្ទឹកដែលអាចកើតមានក្នុងកំឡុងពេលដំឡើងវាដំបូងឆ្លងអស់ប៉ុន្មានពេលទៅមុខទៅសូចនាករដែលមានភាពនឹងនរនោះនឹងក្លាយទៅជាចង្អុលបង្ហាញយ៉ាងច្បាស់ក្រឡែកនៃអ្វីដែល Servers ត្រូវការការយកចិត្តទុកដាក់ជាងអ្វីផ្សេងៗទៀត។ វាក៏អាចក្លាយជាឧបករណ៍ក្នុងការរុករកបញ្ហាយ៉ាងអស្ចារ្យដែលអាចចង្អុលប្រាប់យ៉ាងរហ័សនូវការដំឡើងឬលុបនូវកម្មវិធីកុំព្យូទ័រ(applications)ដែលបានប្រព្រឹត្តទៅនៅពេលថ្មីៗនោះផងដែរហើយកំហុសឆ្គងផ្សេងៗដែលបង្កើតឡើងដោយប្រព័ន្ធប្រតិបត្តិ(OS),កម្មវិធីឬ ក៏ផ្នែករឹងនៃកុំព្យូទ័រមកលើប្រព័ន្ធរបស់អ្នក ។

ទិន្នន័យដែលបានប្រមូលមកពីការត្រួតពិនិត្យដំណើរការ គួរតែអាចប្រើប្រាស់ដើម្បីជាជំនួយក្នុងការធ្វើការសម្រេចចិត្តជុំវិញការគ្រប់គ្រងលើធនធានរបស់ Server។ Wind ows System Resource Manager ជាឧបករណ៍ដ៏អស្ចារ្យមួយដែលអាចឱ្យអ្នកកំណត់ អទិភាពនៃ processes ផ្សេងៗដែលដំណើរការដោយ Server ដើម្បីបញ្ជាក់ឱ្យប្រាកដថា server កំពុងតែប្រតិបត្តិក្នុងកម្រិតមួយដ៏ប្រសើរបំផុត នៅរាល់ពេល និងថាបើភាពមិនចុះសម្រុងគ្នាលើការប្រើប្រាស់ធនធានបានកើតឡើង នោះកម្មវិធីណាដែលអ្នកបានកំណត់អទិភាពឱ្យមានសិទ្ធិទទួលយកធនធានទាំងនោះតែម្តង។ ជាពិសេសនេះពិតជាមានសារៈប្រយោជន៍សម្រាប់គ្រប់គ្រងលើ terminal servers និង IIS servers ដែល processes ដែលមានចំនួនដ៏ច្រើនលើសលុបអាចនឹងដំណើរការក្នុងពេលតែមួយហើយសុទ្ធតែប្រជែងទាមទារយកធនធានមកប្រើប្រាស់។ WSRM អនុញ្ញាតឱ្យអ្នកអាចដាក់កម្រិតថាតើ processes ទាំងឡាយនោះអាចទទួលយកនូវធនធាននិងសម្របសម្រួលវាឱ្យសមទៅនឹងតម្រូវការអាជីវកម្មនិងតម្រូវការបច្ចេកទេសរបស់អ្នក ។

ជំពូកទី១៤

គោលការណ៍នៃ Network និងការប្រើប្រាស់សេវា

១៤-១- សេចក្តីផ្តើម

ក្នុងពិភពលោកយើងនេះការរស់នៅត្រូវការមានទំនាក់ទំនងជាមួយគ្នាដើម្បីប្រតិបត្តិការងារអ្វីមួយ។ កុំព្យូទ័រក៏ដូច្នោះដែរ ដើម្បីប្រតិបត្តិការក្នុងកិច្ចការធំមួយគឺត្រូវការកុំព្យូទ័រដទៃមកសម្រួលការងារគ្នា។ ពួកគេប្រើការតភ្ជាប់ Network ប៉ុន្តែក្នុងការតភ្ជាប់ Network ពួកយើងអាចជួបប្រទះបញ្ហាជាច្រើនព្រោះយើងអាចមាន Users ច្រើនមកភ្ជាប់នឹង Network របស់យើង ។ ក្នុងចំណុចនេះហើយទើប យើងត្រូវធ្វើការសិក្សាទៅលើ **Network Policy and Access Services** ដើម្បីការពារ Network យើងពីបញ្ហានានា ។

អ្វីទៅជា Network Policy and Access Services ?

នៅពេលដែលពួកយើងនិយាយពីការការពារ Network របស់យើង ជាធម្មតាយើងតែងតែគិតអំពីការការពារតាមរយៈ Hardware និង Software ដូចជាការប្រើ firewalls និង anti-virus។ នៅក្នុងប្រព័ន្ធដ៏ធំមួយ ការគំរាមដ៏ធំជាងគេរបស់ពួកយើងគឺមកពី hosts ដែលគួរឱ្យទុកចិត្តដូចជាប្រព័ន្ធដែលយើងមានប្រព័ន្ធដែលយើងគ្រប់គ្រង និងប្រព័ន្ធដែលពួកយើងទទួលខុសត្រូវ។ វាហាក់ដូចជាចម្លែកតែវាជាការពិត។ ទោះបីជាអង្គការជាច្រើន បានធ្វើការដ៏ល្អជាមួយនឹងការការពារប្រព័ន្ធរបស់ពួកគេតាមរយៈ firewalls និង tunneling remote access តាមការប្រើ VPN រឺ remote terminal-based system ដូចជា Terminal Services និង Citrix ក៏ដោយក៏ពួកគេអាចគ្រប់បន្តិចបន្តួចប៉ុណ្ណោះទៅលើអ្វីដែលកើតក្នុង Network ។

ភាគច្រើនគេប្រើគម្រោងសម្រាប់ការដោះស្រាយបញ្ហា Network តែតើយើងអាចដោះស្រាយយ៉ាងណានៅពេលដែលអ្នកប្រើប្រាស់យក Laptop ទៅផ្ទះរួចយកមកភ្ជាប់ Network វិញនៅថ្ងៃបន្ទាប់? រយៈពេលដែលគេយក Laptop ទៅផ្ទះគឺជាឱកាសមួយដែល អាចឱ្យកុំព្យូទ័រទទួលរងនូវបញ្ហា ។

តើវាមើលទៅមិនសមស្របទេគ្រប់ពេលដែលអ្នកប្រើប្រាស់យកកុំព្យូទ័រមកភ្ជាប់ Network វាគួរតែត្រូវបានពិនិត្យមុនពេលទទួលការអញ្ញាតិក្នុងការភ្ជាប់ប្រព័ន្ធ? ទាំងអស់នេះទាក់ទងទៅនឹង Network Access Protection(NAP)។ NAP ជាកន្លែងដែលឧបករណ៍មិនទុកចិត្តត្រូវបានរក្សាទុកក្នុងកន្លែងដែលត្រូវត្រួតពិនិត្យជាមុនរហូតដល់ពេលធ្វើការត្រួតពិនិត្យសុខភាព។ បើវាជាប់ វានឹងអាចភ្ជាប់ទៅកាន់ប្រព័ន្ធ Network ដែលមានទំនុកចិត្ត។ ប្រសិនបើមានបញ្ហាវានឹងត្រូវបានផ្តល់ឱកាសដើម្បីទទួលការដោះស្រាយដោយស្វ័យប្រវត្តឬក៏ដោយ User ណាមួយរួចនឹងធ្វើការត្រួតពិនិត្យម្តងទៀត ។

១៤-២- ការការពារការប្រើ Network

NAP ជាអ្វី?ដំបូងខ្ញុំនឹងប្រាប់ថាវាមិនមែនជាអ្វី។ វានឹងមិនការពារអ្នកពី Users ដែលអាចបង្កបញ្ហាទេ។ NAP ជាដំណោះស្រាយដែលអនុញ្ញាតឱ្យ Administrator host ដែលអាចមានបញ្ហាមកភ្ជាប់ Network នៅពេលដែលជាប់ការត្រួតពិនិត្យមួយចំនួន។ ប្រព័ន្ធដែលមិនជាប់ការពិនិត្យនឹងត្រូវបានទុកក្នុងលក្ខខណ្ឌកម្រិតណាមួយដែលអនុញ្ញាតឱ្យវាធ្វើការទាក់ទងទៅនឹង hosts ជាក់លាក់ដែលអាចឱ្យវាចូលទៅ Healthy State ។ ជាធម្មតារួម

មាន antivirus និង patch-management Servers, ប៉ុន្តែវាអាចជា Server ណាមួយដែលអ្នកត្រូវការឱ្យមានដើម្បីឱ្យប្រព័ន្ធរបស់អ្នកមានភាពត្រឹមត្រូវ។ នៅពេលដែលភាពខុសប្រក្រតីនៃ Health ត្រូវបានដោះស្រាយ នោះប្រព័ន្ធដែលទទួលការកែប្រែអាចចូលរួមក្នុងប្រព័ន្ធដែលគួរឱ្យទុកចិត្តរបស់អ្នក ។

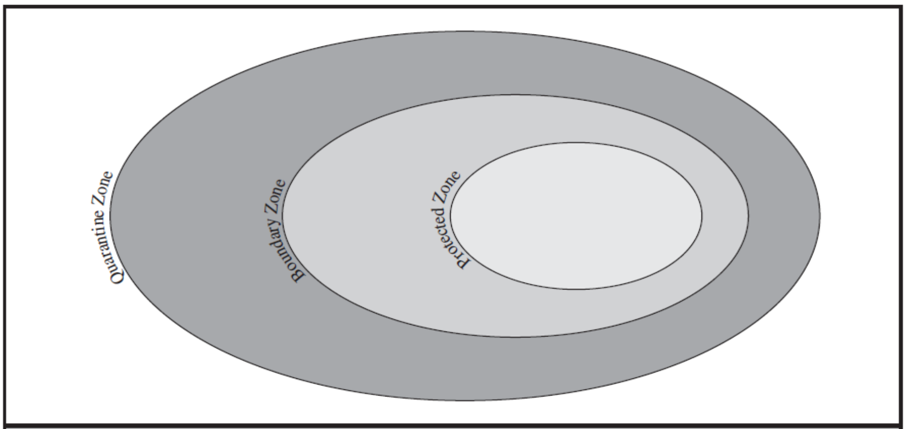


Figure 8-1. NAP logical network zones using IPSec

រូបភាព៨-១បង្ហាញពីឧទាហរណ៍នៃរបៀបដែល NAP ត្រូវបានប្រើដើម្បីចែក Network តាមការប្រើ Policy ជាជាង Topology ។ ក្នុងឧទាហរណ៍នេះគេប្រើ IPSec។ Hosts ថ្មីណាក៏ដោយគឺត្រូវរក្សាក្នុង Quarantine Zone ។ បើ hosts ទាំងនោះចង់ចូលទៅក្នុង Protected Zone នោះនឹងត្រូវឆ្លងកាត់ការធ្វើការត្រួតសុខភាពមួយចំនួន។ បើធ្លាក់នូវការធ្វើត្រួតពិនិត្យសុខភាពណាមួយវាត្រូវទាក់ទងនឹង remediation servers ដែលស្ថិតនៅក្នុង boundary zone ដើម្បីធ្វើការតម្រូវ។ នៅពេលកែតម្រូវហើយ វាអាចចូលក្នុង protected zone ហើយអាចទាក់ទងនឹង hosts ក្នុង zone នោះបាន ។ Hosts មួយអាចទាក់ទងនឹង hosts ដទៃក្នុង zone តែមួយ រឺ zone នៅក្បែរគ្នា។ Hosts នៅក្នុង boundary zone អាចនិយាយជាមួយគ្រប់ system ក្នុងខណៈដែល hosts នៅក្នុង quarantine zone មិនអាចនិយាយជាមួយ hosts នៅក្នុង protected zone និងច្រាសមកវិញ។

NAP ត្រូវបានសាងសង់ដោយច្បាប់៤គឺ policy validation (health check),network restriction, remediation (getting healthy) និង ongoing compliance ។ ongoing compliance មានន័យថាដើម្បីបន្តនៅក្នុងតំបន់ការពារប្រព័ន្ធនោះត្រូវតែមានសុខភាពល្អ ។ បើមានការផ្លាស់ប្តូរដែលនាំឱ្យប្រព័ន្ធមិនគោរពតាមគោលការណ៍ NAP ប្រព័ន្ធនឹងត្រូវបានផ្ទេរទៅ quarantine zone និងមិនអាចទាក់ទងនឹង hosts នៅក្នុងតំបន់ការពាររហូតដល់បញ្ហាត្រូវបានដោះស្រាយ ។

ឧទាហរណ៍

បើតាមគោលការណ៍និយាយថា Window Firewall ត្រូវតែបើកគ្រប់ពេល។ នៅពេលភ្ជាប់ទៅ Network ដោយ Window Firewall របស់ប្រព័ន្ធបើកនោះប្រព័ន្ធទទួលបានការត្រួតពិនិត្យសុខភាពហើយត្រូវបានចូលក្នុងតំបន់ការពារ។ ក្នុងពេលនៅក្នុងតំបន់ការពារ បើប្រព័ន្ធនោះបានបិទ Window Firewall ប្រព័ន្ធនោះនឹងត្រូវកាត់ផ្តាច់ពីតំបន់ការពារនៅពេលវាត្រូវបានវាយតម្លៃបន្ទាប់រហូតដល់វាបើក Window Firewall រឺក៏ remediation server បើកWindow Firewall ឱ្យវាវិញ។ នេះជាបញ្ហាដ៏សំខាន់ យើងអាចបង្កើត remediation server ដើម្បីយក host ឱ្យធ្វើតាមដោយស្វ័យប្រវត្ត។ យើងក៏អាចឱ្យ users ផ្លាស់ប្តូរដោយខ្លួនឯងផងដែរដោយយើងផ្តល់ជាដំណោះ

ស្រាយដល់ users ។ យើងគួរតែមានប្រព័ន្ធទាំងពីរនេះ ព្រោះបើការកែតម្រូវដោយស្វ័យប្រវត្ត ការបរាជ័យនោះ users អាចប្រើការកែតម្រូវដោយខ្លួនឯង ។

១៤-២-១- សមាសភាពរបស់ NAP

NAP ជាប្រព័ន្ធដ៏ធំមួយ។ ដោយគ្មានគ្រប់ផ្នែកដែលទាមទារ វានិងគ្មានឥទ្ធិពលទេ។ អ្វីដែលជាបញ្ហាក្នុងការប្រើប្រាស់ NAP គឺតម្លៃ។ ដើម្បីប្រើ NAP យើងត្រូវ Upgrade ចំណុចខ្លះដូចជា Upgrade switches បើវាមិនអាចប្រើជាមួយ 802.1 Xauthentication។ NAP មាន Components មួយចំនួនដូចជា:

- IPSec enforcement
- 802.1X enforcement
- VPN enforcement
- Dynamic Host Configuration Protocol (DHCP) enforcement
- Network Policy Server (NPS)/ Radius
- NAP Agent
- System Health Agent (SHA)
- NAP administrative server
- System Health Validator (SHV)
- Health policy
- Accounts database
- Health Registration Authority (HRA)
- Remediation server

បញ្ជីនេះវែង ប៉ុន្តែបើគិតពីអ្វីដែលអ្នកព្យាយាមទទួលបានដើម្បីការពារ Network ផ្នែកនីមួយៗមានតួនាទីយ៉ាងសំខាន់ដើម្បីឱ្យ NAP ដំណើរការបាន ។

1. IPsec enforcement

   IPsec enforcement ដំណើរការដោយប្រើវិញ្ញាបនប័ត្រ X-509 ដើម្បីគ្រប់គ្រងការ access network។ គ្រប់ host ពុំមានវិញ្ញាបនប័ត្រសុខភាពដែលមានសុពលភាពគឺមិនអនុញ្ញាតឱ្យធ្វើទំនាក់ទំនងជាមួយ host ដែលមានវិញ្ញាបនប័ត្រ។

   ដោយប្រើ IPsec enforcement ,hostដែលមានលទ្ធភាពត្រូវបានស្នើឡើងឱ្យមានវិញ្ញាបន ប័ត្រពីHealth Registration Authority(HRA)។ HRA មានតួនាទីត្រួតពិនិត្យការគោរពតាមរបស់ host ជាមួយនិងការយល់ព្រមរបស់ NAP។ HRA រក្សាវិញ្ញាបនប័ត្រសុខភាពពីអ្នកជំនាញការដែលអនុញ្ញាតឱ្យប្រើដើម្បីធ្វើទំនាក់ទំនងទៅវិញទៅមកដោយ IPsec-enabled host ជាមួយនិងវិញ្ញាបនប័ត្រដែលមានសុពលភាព។ ប្រសិនបើបរាជ័យ clientគឺមិនផ្តល់នូវវិញ្ញាបនប័ត្រសុខភាព ប៉ុន្តែជំនួសមកវិញវានឹងផ្តល់នូវការណែនាំពីរបៀបបង្ការខ្លួនឯង។ host បានផ្តល់នូវលទ្ធភាពដែលមានដែនកំណត់ឱ្យ network អាស្រ័យដោយ server ។ ការបង្ការគឺកើតមានឡើងនូវពេល host ធ្វើការត្រួតពិនិត្យឡើងវិញសម្រាប់ការយល់ព្រម និងការបញ្ចេញនូវវិញ្ញាបនប័ត្រសុខភាពដែលមានសុពលភាព ប្រសិនបើជាប់លើសពីនេះវាត្រូវតែស្ថិត

ក្រោមដំណើរការនៃការបង្ការម្តងទៀត។ នេះគឺជាវិធីសាស្ត្ររបស់ NAP enforcement ដែលរឹតត្បិតការ Access network។

2. 802.1x enforcement
   - នេះគឺជាចំនុចមួយដែលគេនិយាយទៅលើការជ្រើសរើសប្រភេទការភ្ជាប់ហើយមានពីរប្រភេទ ដែលអាចប្រើប្រាស់បានគឺ៖
     i. IEEE 802.11 ចំពោះ Wireless network access
     ii. IEEE 802.3 ចំពោះ Ethernet network access

   នៅក្នុងវិធីសាស្ត្រ Network layer-base enforcementសម្រាប់ NAP, hosts តម្រូវឱ្យ Access គឺកើតមានឡើងនៅក្នុងការបំបែកតាមរយៈ IP filter រឺ Virtual LAN (VLAN) ការបែងចែកនិងរហូតដល់វា បញ្ជូនឱ្យមានការកំណត់នូវការត្រួតពិនិត្យសុខភាពដោយ NPS។ 802.1X-compliant client ភ្ជាប់ទៅកាន់ ហើយចាប់ផ្តើម Authentication ជាមួយ 802.1X-compliant access point, ដូចជា Ethernet ,Switch រឺWireless Access point។ NPS server បានស្នើឱ្យ Client ប្រើ SOH ប្រសិនបើAuthentication ជោគជ័យ។ បន្ទាប់មកវានិងវាយតម្លៃថា SOH យល់ព្រមឬក៏អត់អាស្រ័យទៅនឹងគោលការ Networkដែលកំពុងប្រើ ប្រសិនបើវាយល់ព្រម, 802.1X Client ទទួលបាននូវការAccess ដើម្បីការការពារ Network ជាទូទៅ វាមានដែនកំណត់ក្នុងការបញ្ជូនTraffic ដើម្បី Remediation Server ហើយពិនិត្យដែនកំណត់នៃការ Access រហូតដល់វាបញ្ចប់ការអនុវត្តជាមួយHealth Policy ។

3. VPN enforcement

   VPN enforcement គឺជាផ្លូវដ៏ល្អសម្រាប់ការពង្រីករបស់គោលការណ៍ NAP របស់អ្នកដើម្បីការពារខ្លួនអ្នកពីអ្នកប្រើប្រាស់ដែលត្រូវការប្រើវាពីចម្ងាយតាមរយៈ VPN។ NAP-aware VPN enforce - ment agent អាចត្រួតពិនិត្យការយល់ព្រមសុខភាពនិងការផ្តល់រឺបដិសេធ Access VPN អាស្រ័យទៅលើគោលការ NAP។ ចាប់តាំងពី inbound VPN បានបង្កើតចំនួនដ៏ច្រើនបំផុតនៃ Host ដែលភ្ជាប់ទៅកាន់Network របស់អ្នកដែលអ្នកមិនបានគ្រប់គ្រងដោយផ្ទាល់។ វាមានសារៈសំខាន់បំផុតដោយអនុវត្តទៅលើគ្រប់ទម្រង់នៃ VPN enforcement។ វាជាផ្នែកមួយនៃយុទ្ធសាស្ត្ររបស់ NAP ទាំងមូល។ ការ Remote System គឺវាមានភាពមិនល្អទាំងស្រុងនូវក្នុង Network របស់អ្នកដែលគេងាយស្រួលចូលបាន(Hack)។ VPN client ភ្ជាប់ទៅកាន់ Server NPN របស់អ្នកនិងបញ្ជាក់ពីការការពារ Protected Extensible Authentication Protocol(PEAP)ហើយ MS-CHAPv2។ ការបញ្ជាក់របស់ Client ត្រូវតែផ្តល់ដោយ Statement of Health ដែលធ្វើការវាយតម្លៃដោយ NPS.VPN Client និងទទួលការភ្ជាប់ដោយពុំមានការកំណត់ទៅលើការភ្ជាប់ដែលអាស្រ័យថាតើវាធ្វើតាមទៅនឹងគោលការសុខភាពរឺទេ។

4. Dynamic Host Configuration Protocol (DHCP) enforcement

   ប្រសិនបើអ្នកមិនចង់ឱ្យមានការស្មុគស្មាញជាមួយនឹងប្រព័ន្ធ Network របស់អ្នកដូច្នេះអ្នកគួរតែប្រើប្រាស់ DHCP enforcement។ ហើយវាប្រើប្រាស់ IP address រឺ ការកំណត់ IP ដើម្បីកំណត់ថា Network នេះមានការកំណត់ចំនួនដែល Client អាចចូលទៅទាញយកប្រភពទិន្នន័យរបស់អ្នកបានពី Server ប៉ុន្តែបើមិនអាចឆ្លងកាត់ការត្រួតពិនិត្យរបស់លក្ខណៈវិនិច្ឆ័យសុខភាព។ នេះមិនមែនជាដំណោះស្រាយដ៏ល្អនោះទេ ពីព្រោះDHCP enforcement វាធ្វើការកសាងនូវ IP routing Table សម្រាប់ Network របស់អ្នក។ ប៉ុន្តែវិធីនេះប្រើសម្រាប់ការពារចំពោះអ្នកដែលបានដឹងពីព័ត៌មានរបស់ Network ហើយធ្វើការ

ផ្តល់ IP ឱ្យខ្លួនឯងដើម្បីធ្វើការទាក់ទងទៅនឹង Network។ ជាងនេះទៅទៀតដើម្បីឱ្យ Network នេះមានលក្ខណៈឱ្យកាន់តែប្រសើរឡើងគឺត្រូវធ្វើការបន្ថែមសមត្ថភាពឧបករណ៍និងការអនុវត្ត IPsec ដែលមិនធ្វើឱ្យសហគ្រាសមានការខ្វះខាត(ចំនុចដែលខ្វះខាតនូវក្នុងNetwork) នេះជាហេតុផលមួយក្នុងចំណោមបញ្ហាផ្សេងទៀត។

5. Network Policy Server (NPS) / Radius

NPS គឺជាការផ្លាស់ប្តូររបស់ Internet Authentication Service (IAS)ដែលវាជាផ្នែកមួយរបស់ Microsoft's ប្រើប្រាស់ជាមួយ RADIUS(Remote Authentication Dial-In User Service)ហើយវាមានលក្ខណៈសក្តិសមប្រើប្រាស់ជាមួយតួនាទីរបស់ Windows server 2008។ ហេតុនេះហើយបានជា NPS មានអទិភាពនិងមានលក្ខណៈត្រឹមត្រូវច្បាស់លាស់ ដែលប្រើប្រាស់នៅក្នុង NPS server និងត្រូវបានគេចាប់ថ្នាក់ថាជា Health Certification និង connection to 802.1x and VPN device ។

6. NAP Agent

NAP Agentគឺជា Client មួយប្រភេទដែលប្រើប្រាស់សម្រាប់ប្រមូលព័ត៌មានពីSystem Health Agent ទាំងអស់ហើយធ្វើការបញ្ជូនព័ត៌មាននេះទៅកាន់ NAP Enforcement Client

7. System Health Agent (SHA)

ចំពោះ Windows Server 2008 និង Windows Vista គឺធ្វើឡើង Build-in system ហើយទីភ្នាក់ងារត្រួតពិនិត្យសុខភាព ធ្វើការអនុញ្ញាតនិងប្រើប្រាស់ព័ត៌មានដើម្បីធ្វើការវាយតម្លៃដូចជា Firewall និង anti-virus។ នេះគឺជាដៃគូរសហការដ៏ធំរបស់Microsoft ដែលធ្វើការអភិវឌ្ឍដើម្បីចេញនូវទីភ្នាក់ងារត្រួតពិនិត្យសុខភាព។ អ្នកក៏អាចប្រើប្រាស់ SHA សម្រាប់ System ដែលវាផ្តល់នូវប្រព័ន្ធត្រួតពិនិត្យសុខភាព។ ឧទាហរណ៍ អ្នកឱ្យបុគ្គលិករបស់អ្នកទៅធ្វើការសហការជាមួយ SHA ដើម្បីធ្វើការបង្កើតនូវ applica tion ច្បាសលាស់ដែលសម្រាប់ដំឡើងឱ្យ System ដែលគិតពីសុខភាព។ SHA នេះមានលក្ខណៈប្រសើរជាង NAP agent សម្រាប់ធ្វើការពិចារណាទៅលើសុខភាពនិងធ្វើការប្រាស្រ័យទាក់ទងដើម្បីធ្វើការយកព័ត៌មានត្រឡប់មកវិញ(NPS) ដែលអាចធ្វើឱ្យមានការចំណេញនិងពេញលេញក្នុងការ Access ចំពោះ network របស់អ្នក។

8. NAP administration Server

NAP administration server គឺជាការទទួលខុសត្រូវចំពោះការទាញយកទន្និន័យទាំងអស់ពី System Health Validator (SHV) ហើយកំណត់ថាតើ Client នោះនៅកន្លែងណាដែលអាចឱ្យ server បង្ការការពារបាននេះជាហេតុធ្វើឱ្យ System ធ្វើការការពារការ Access បានយ៉ាងល្អដោយសារ NAP adminis -tration Server។

9. System Health Validator (SHV)

SHV គឺជាផ្នែកមួយនៃ Server ដែលធ្វើការកំណត់ពីសុខភាពរបស់ Client ចំពោះការប្រមូល Data ពី Client ទៅ SHAs ហើយវាធ្វើការទំនាក់ទំនងទៅ Client ដោយប្រើប្រាស់ Statement of Health response (SoHR)។ នេះគឺជាសុពលភាពនៅក្នុង NPS Server និងធ្វើការប្រៀបធៀបពីការស្នើសុំរបស់ Client ដែលបានប្រើប្រាស់នៅក្នុងServer។

10. Health Policy

នេះជាគោលនយោបាយមួយដែលប្រើដើម្បីកំណត់ឱ្យបានច្បាស់លាស់ចំពោះតម្រូវការការពារដែលប្រើសម្រាប់ការ Access មកកាន់ Network ។ គោលនយោបាយនេះគឺធ្វើការសាកសួរឱ្យ Windows firewall បើកហើយ

ទោះជា Network មិនមានកម្មវិធីកំចាត់មេរោគចុងក្រោយក៏ដោយ។ នៅមាន Policy ជាច្រើនទៀតដែលអាចការពារបាននូវ System ,វាមានមួយប្រភេទទៀតគឺ Enforcement Client ។ ឧទាហរណ៍ អ្នកអាចធ្វើការវិនិច្ឆ័យបានក្នុងការប្រើប្រាស់ 802.1X ដើម្បី Access ប្រឆាំងVPN access ។

11. Accounts database

Database គឺជាកន្លែងសំខាន់មួយដែលធ្វើការប្រមូលទុកនូវ Account ទាំងអស់ដែលមានសិទ្ធិស្របច្បាប់ដែលបានកំណត់។ ចំពោះបំណងនិងគំនិតរបស់ Active Directory ដែលបានបំពេញមុខងារក្នុង Windows server 2008។

12. Health Registration Authority (HRA)

តួនាទីរបស់ HRA គឺជាអ្នកដែលនៅចន្លោះកណ្តាលរវាងកុំព្យូទ័រដែលមានសុខភាពនិង CA ដើម្បីទទួលបានវិញ្ញាបនប័ត្រសុខភាពដើម្បីបង្ហាញឱ្យដឹងថា client បានឆ្លងកាត់ការត្រួតពិនិត្យសុខភាព។ ការត្រួតពិនិត្យនេះគឺធ្វើឡើងដោយប្រើប្រាស់ Windows server 2008 និង Web service (IIS)។

13. Remediation Server

នៅពេលដែល Client មិនបានធ្វើការបំពេញចំពោះ Health Policy,ដូច្នេះវាធ្វើការបង្ការមិនឱ្យ Access។ Client ត្រូវតែមានការអនុញ្ញាតពី Remediation Servers កំណត់ពីប្រភេទបន្ទាប់មក ផ្តល់សញ្ញាទៅឱ្យ Server ចំពោះ Client ណាដែលមិនបានប្រតិបត្តិតាម។ Remediation Servers គឺវាស្ថិតនៅចន្លោះរវាង quarantine និង protected zones

ចំពោះទំហំនៃ Server ដែលមានសិទ្ធិឱ្យ Client Access យក Data យកទៅប្រើប្រាស់

- NAP Health Policy Server
- NAP Administration Server
- System Health validators (SHV)
- NAP Enforcement Server (NAP ES)
- NAP Enforcement Point
- Health Requirement Server
- Remediation of Health response

ចំពោះ ទំហំនៃអ្នកប្រើប្រាស់ (Client)ដែលអាច Access ទៅយក Data

- System Health Agent (SHE)
- NAP Agent
- NAP Enforcement Client
- Statement of Health (SoH)

តើ Server និង Client មានទំនាក់ទំនងយ៉ាងដូចម្តេចដើម្បីយក Data ទៅវិញទៅមកបាន ?
តម្រូវការនៃការទំនាក់ទំនងមានដូចខាងក្រោម ៖

- Communication Flow
    - Requirements
    - Preparation
    - Installing the Network Policy Server
    - Configuration the Network Policy and Server

- Installing and Configuration DHCP

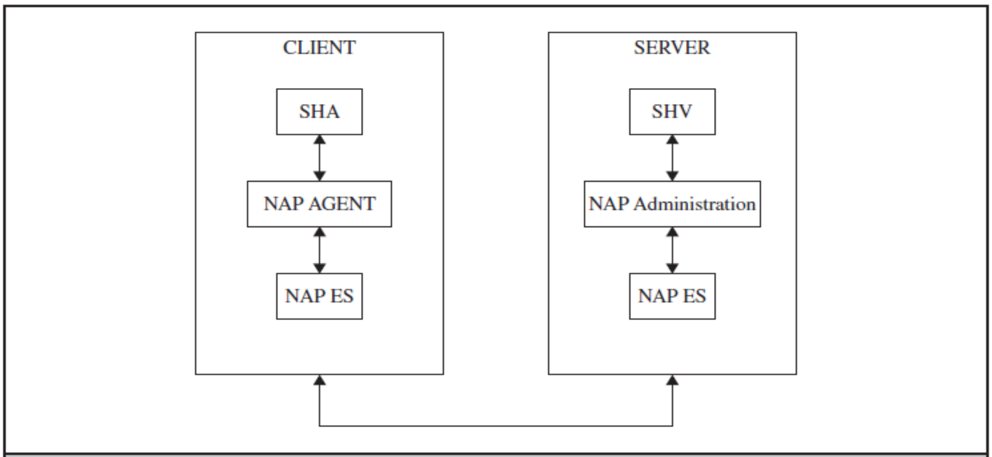


Figure 8-3. Statement of Health communication path

រូបភាព៨-៣បង្ហាញនូវសមាសភាពទំនាក់ទំនងជាមួយនឹងសមាសភាពមួយផ្សេងទៀតសម្រាប់គោលបំណងនៃការវាយតម្លៃ health ។

SHA ផ្តល់ SoH ទៅឱ្យភ្នាក់ងារ NAP។ ភ្នាក់ងារ NAP បានបញ្ជូនទៅភ្នាក់ងារ NAP EC, ដែល Nap EC នឹងបញ្ជូនទៅ NAP ES ហើយ NAP ES បញ្ជូនទៅ NAP Admini-strator ហើយបញ្ជូនទៅ SHV។ លទ្ធផល SoHR គឺត្រូវបានបញ្ជូនមកវិញតាមបណ្តោយខ្សែ SHA លើ client ដទៃទៀតដើម្បីយល់ព្រម connection ឬក៏ផ្តល់ដំបូន្មានសម្រាប់ធ្វើយ៉ាងណាដើម្បីកែកំហុសដោយខ្លួនវា។ EC និង ES ជាសមាសភាពបញ្ហាលើបណ្តាញដំណើរការជាមូលដ្ឋានលើលទ្ធផលនៃការឆ្លើយតប។

១៤-២-៣. ការអនុវត្តលើកិច្ចការ

❖ ឧទាហរណ៍ដែលការលើកយកការប្រើប្រាស់ NAP ដោយប្រើ DHCP Enforcement

NAP គឺជាវិធានការស្មុគស្មាញមួយដែលតម្រូវឱ្យមានជំនាញក្នុងកាន់វិន័យជាច្រើន ។ អ្នកនឹងចំណាំថាជំពូកនេះមានលំហាត់ខ្លះដែលបានកែប្រែមានសារៈសំខាន់ជាងជំពូកមុនៗ។ នេះគឺងាយស្រួលពីព្រោះការបង្កើត NAP environment មានន័យថាអ្នកបានបង្កើត configuration settings ដែលហួលពីដែនកំណត់នៃសៀវភៅនេះ(យ៉ាងណាក៏ដោយ)មួយក្នុងចំណោម NAP enforcement methods ដែលយើងអាចប្រើដើម្បីបង្ហាញ NAP concept ដោយសារវាងាយស្រួលប្រែប្រួលពេលគឺ NAP ប្រើ DHCP enforcement។ ព្រោះតែលំហាត់ជាច្រើនយើងបានរៀបចំ NAP architecture ធម្មតា ដោយប្រើ DHCP enforcement ដើម្បីគ្រប់គ្រងលើ network access NAP-enabled client. សម្រាប់ NAP-enable client ។

នៅក្នុងការលើកឧទាហរណ៍នេះយើងត្រូវការតម្រូវការដូចជា (Requirements)៖

ប្រភេទនៃ system ដែលតូចបំផុតដែលអ្នកត្រូវការសម្រាប់ឧទាហរណ៍នេះគឺ

▼Domain controller

- Windows Server 2008 server acting as network policy server
- DCHP Server (either on the domain controller or NPS server)
- DNS Server (required for Active Directory anyway)

▲Client កុំព្យូទ័រ running Windows Vista

Preparation

ចំពោះការអនុវត្តន៍នេះយើងជ្រើសរើសយក Windows Server 2008 សម្រាប់យកមកធ្វើជា Server និង Workstation ដែលកំពុងដំណើរការជាមួយ Windows Vista សម្រាប់ធ្វើជា Client ។ ប្រើប្រាស់ Domain ត្រូវដាក់ឈ្មោះថា **TESTLAB.LOCAL**និងមាន workstation កំពុងដំណើរការ Windows Vista ៕

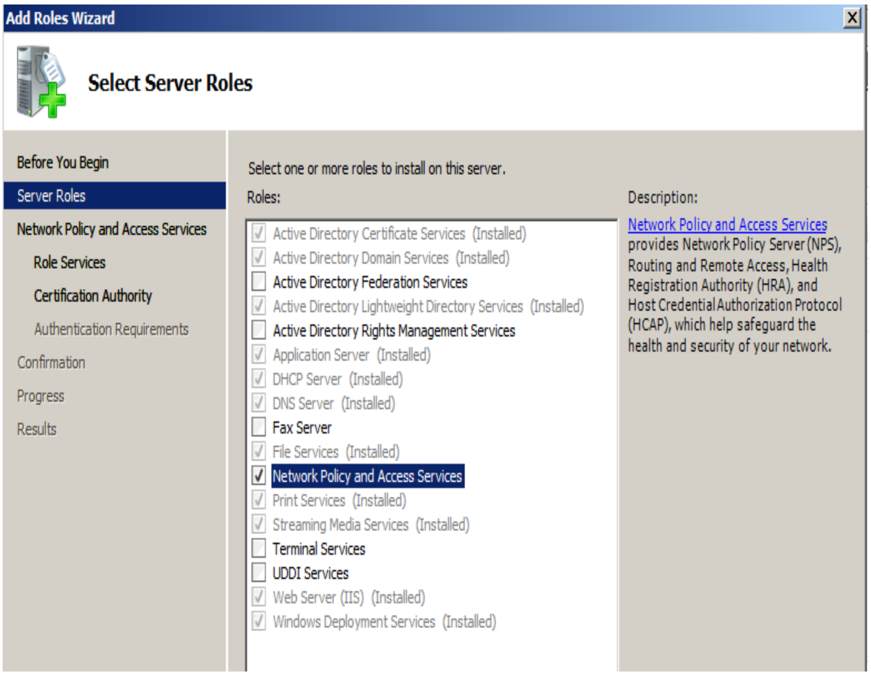
ចំពោះតម្រូវការប្រព័ន្ធនេះរួមមាន(**System Setup Requirements**) ៖

- WIN2K8DC
  - Windows Server 2008
  - Domain Controller, Primary DNS Server
  - IP Address: 192.168.100.25
- WIN2K8NPS
  - Windows Server 2008
  - DHCP Server, Network Policy Server
  - IP Address: 192.168.100.26
- VISTAWKS
  - Windows Vista Ultimate workstation
  - IP Address: DHCP

ជំហានទី១ ការដំឡើង Network policy Server

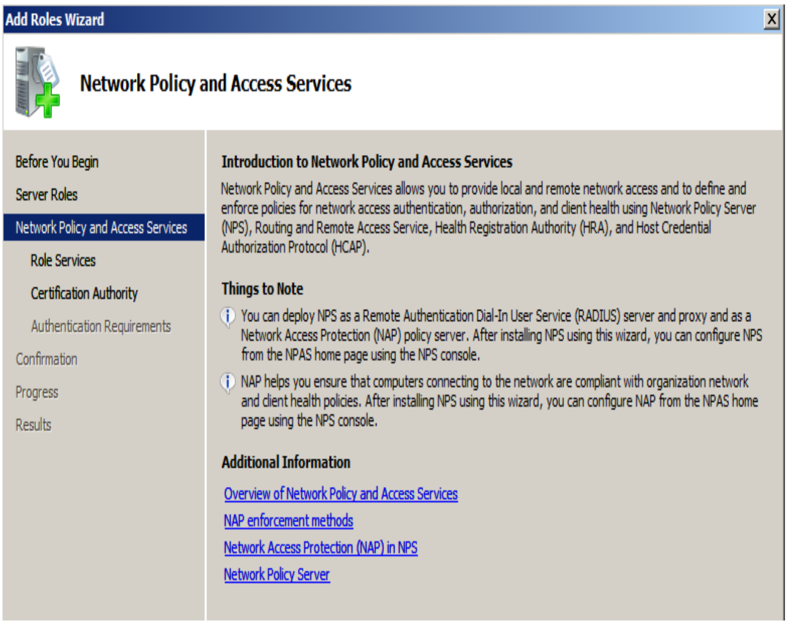
ខ្ញុំសន្មត់ថាអ្នកបាន Setup Active Directory និងបានដំណើរការរួចរាល់ហើយនូវ Server នោះអ្នកប្រើដូច Network Policy Server

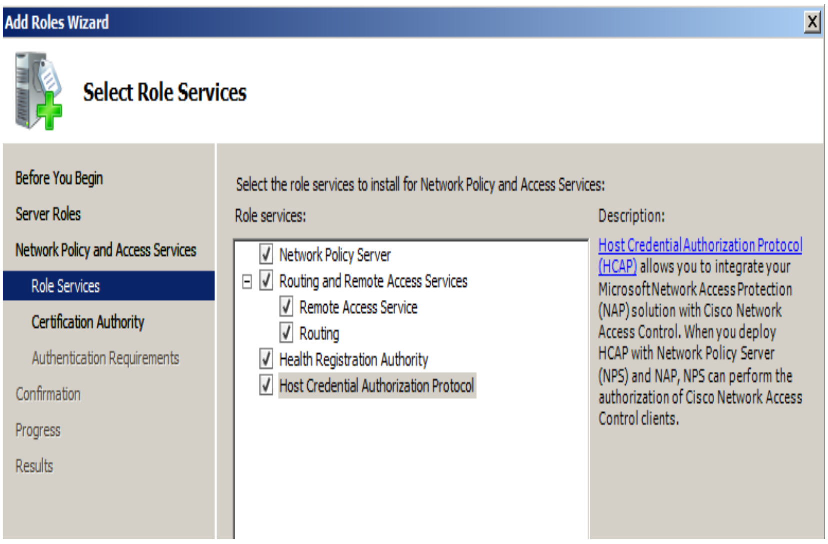
1. Log On ទៅលើ Server ដែលអ្នកចង់ Install NPS
2. បើក Server manager
3. ចុច Add Roles ហើយ Link ដើម្បីបើកនូវ Add Roles Wizard
4. ចុចលើ Next មុនពេលអ្នកចាប់ផ្តើមចូលក្នុងផ្ទាំងអេក្រង់
5. ត្រួតពិនិត្យមើល Network Policy និង Access Services ហើយគូសគ្រីសក្នុងប្រអប់ហើយជ្រើសរើស Server Roles លើអេក្រង់ហើយបន្ទាប់មកចុច Next
6. ក្នុងការបង្ហាញទៅនិង Network Access Service នៅលើអេក្រង់ចុច Next
7. នៅក្នុងកាជ្រើសរើស Role Services នៅលើអេក្រង់ ពិនិត្យមើល Network Policy Server នៅក្នុង checkbox បន្ទាប់មកចុចNext
8. Confirm ការ Install ហើយបន្ទាប់មកចុច Next
9. ចុច Close នៅពេលការ Install បានបញ្ចប់



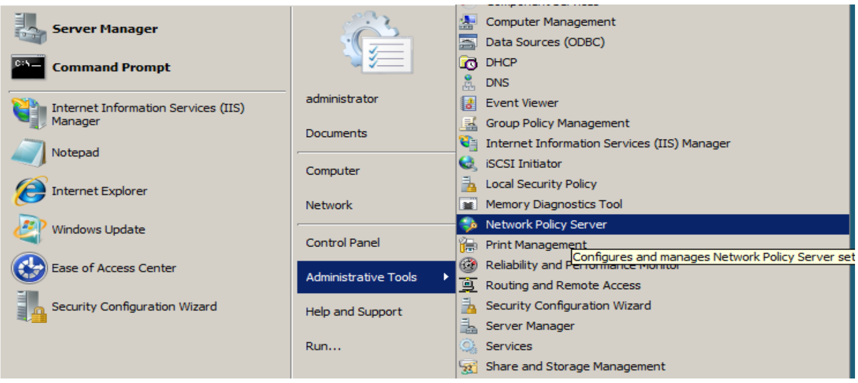
ជំហានទី២ Configure the Network Policy Server

ការ Configure Network Policy Server បន្ទាប់ពីដំឡើង NPS រួចរាល់ហើយអ្នកនិងត្រូវការ Configure NPS ដើម្បី Window System Health Validator អ្នកនិង Configure Validator ដើម្បីឱ្យវាប្រាកដថាប្រពន្ធ័មានសុវត្ថិភាព។

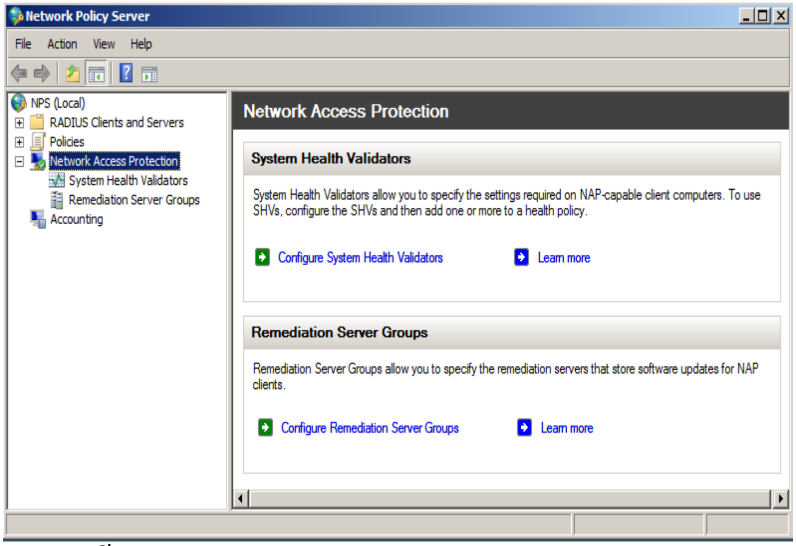




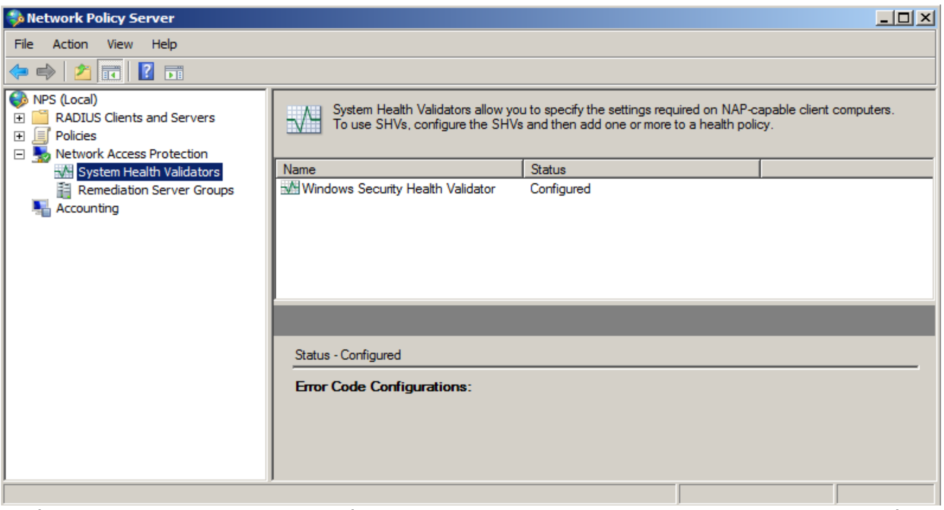
1. ជ្រើសរើសStart → Administrative Tools → Network Policy Server ដើម្បីបើក Network Policy Server management Console



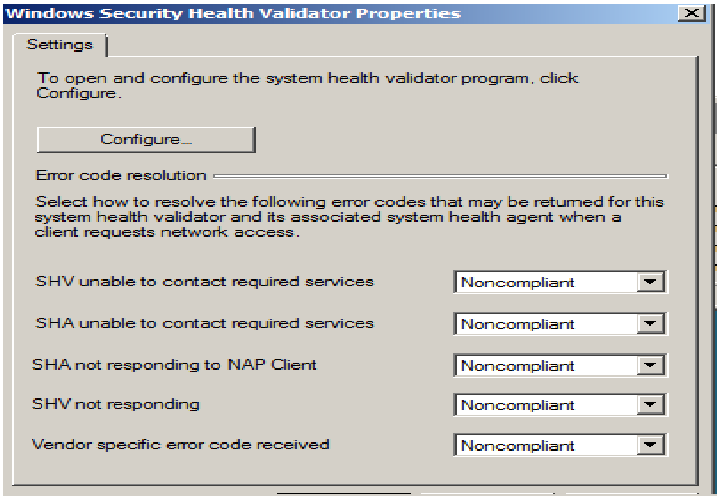
2. ពង្រីក Network Access Protection node



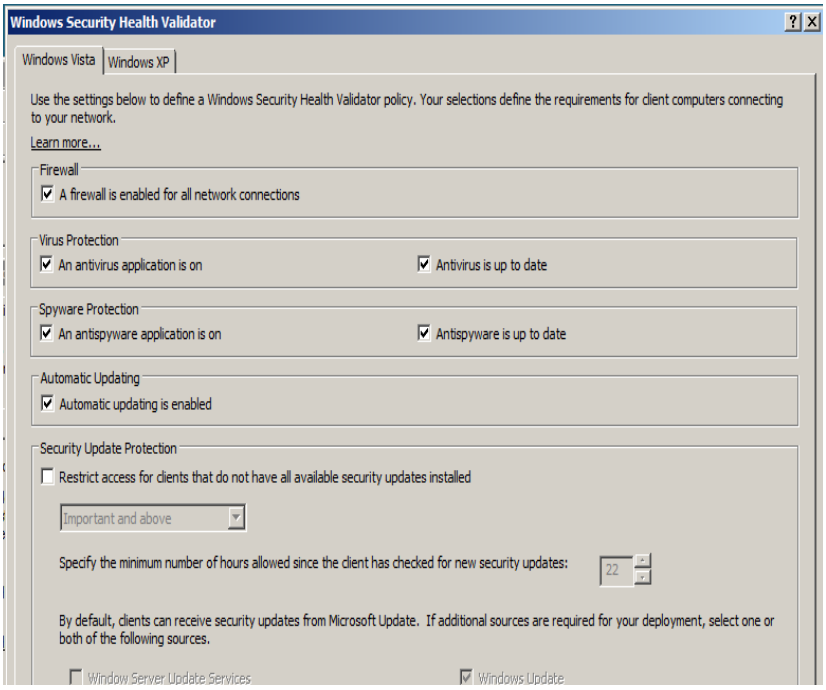
រូបភាព៨-៦ជ្រើសរើស System Health Validator ដូចបានបង្ហាញក្នុងរូបភាព៨-៦



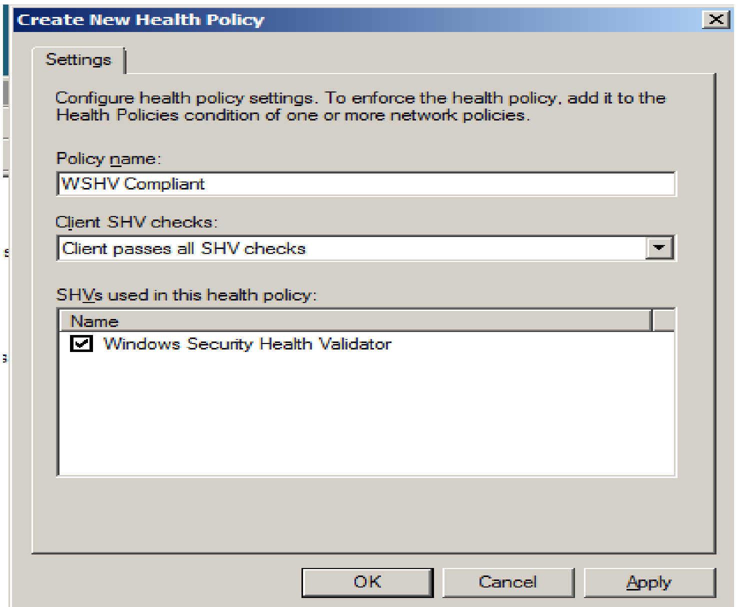
3. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Window Security Health Validator ហើយជ្រើសរើស Properties ដើម្បីបើកទំព័រProperties



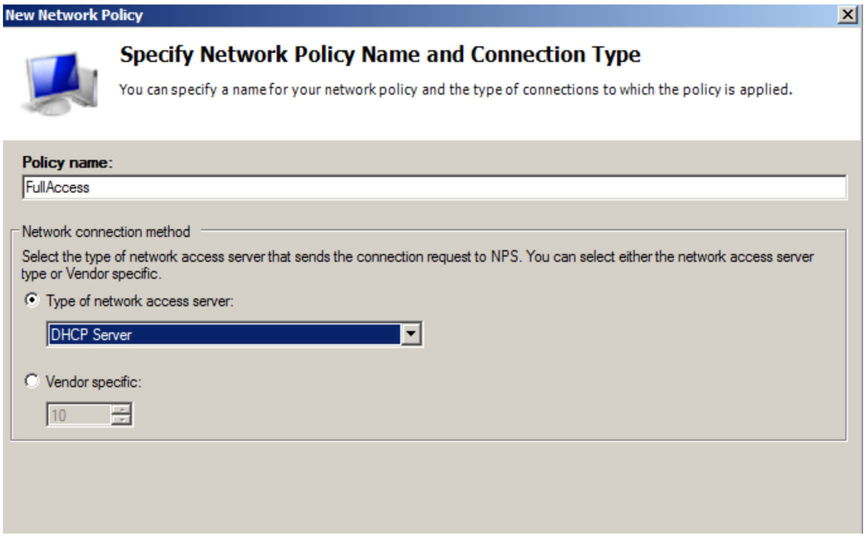
4. ចុចលើ Configure button បើសិន Configure button មិនមានសកម្មភាពការសាកល្បងរបស់អ្នកអាចតម្រូវឱ្យបើក Network Policy Server សាឡើងវិញដើម្បីចាប់ផ្តើមបង្កើត Button Variable



5. នៅក្នុង Window Vista សង្កេតឃើញថាពុំទាន់បានត្រួតពិនិត្យគ្រប់ checkbox ទាំងអស់លើកលែងតែ checkbox របស់ Firewall ហើយបន្ទាប់មកចុច OK
6. ចុច OK នៅលើទំព័ររបស់ Properties ដើម្បីរក្សាទុកពេលយើងផ្លាស់ប្តូរ
7. បន្ថែមនូវ Policies node
8. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Health Policies ហើយជ្រើសរើស New
9. ចូល WSHV Compliant នៅក្នុងកន្លែងឈ្មោះ Policy ,ជ្រើសរើសយក Client Pass All SHV ពិនិត្យនៅក្នុងClient SHV check កំណត់ក្នុងបញ្ជីហើយពិនិត្យ Window Security Validator ដូចបានបង្ហាញក្នុង Configure ៨-៩ , បន្ទាប់មកចុចOk
10. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Health Policies ហើយជ្រើសរើសយក New

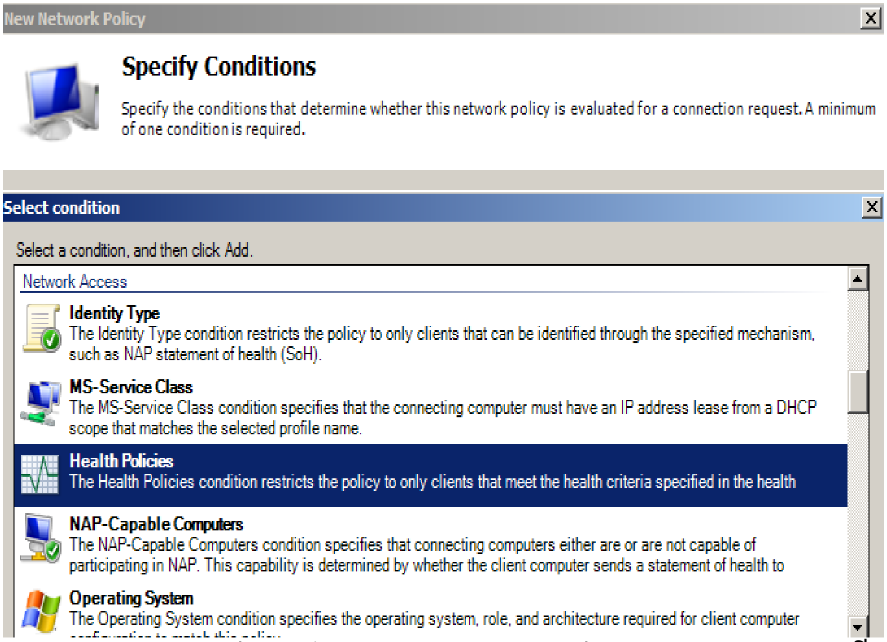


11. ចូលក្នុង WSHV Noncompliant នៅក្នុង Policy Nameជ្រើសរើសយក Client Fail One រឺ More WSHV checkនៅក្នុង Client SHV check កំណត់ចូលក្នុងតារាងហើយ ពិនិត្យមើល Window Security Health Validator បន្ទាប់មកចុច OK
12. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Network Policies ហើយជ្រើសរើសយក New
13. ចូលក្នុង Full Access នៅក្នុង Policy Name ហើយជ្រើសរើស DHCP Server ដូចបានវាយបញ្ចូល Network Access Server បន្ទាប់មកចុច Next

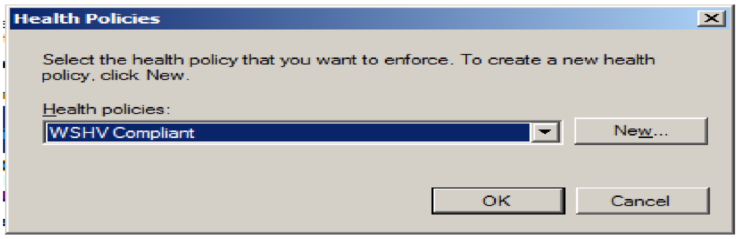


14. នៅលើអេក្រង់ Specify Conditionsចុចលើ Add button

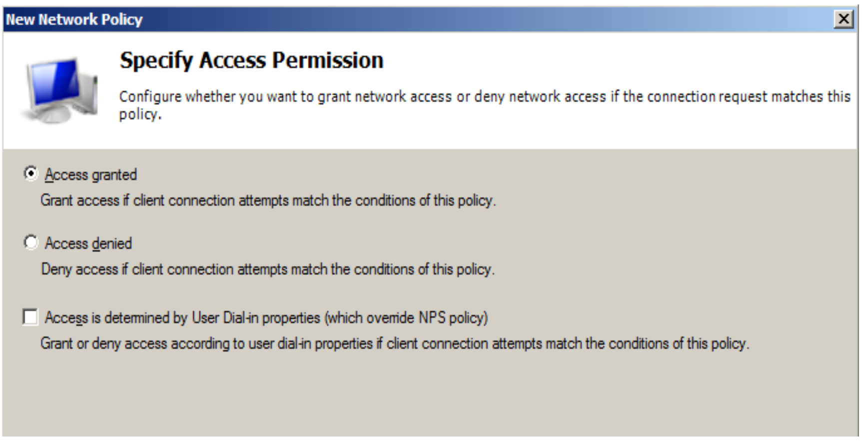
15. នៅក្នុងការជ្រើសរើស Condition ទាញចុះមកក្រោមក្នុង Network Access Protection Section ជ្រើសរើសHealth Policies ហើយចុច Add



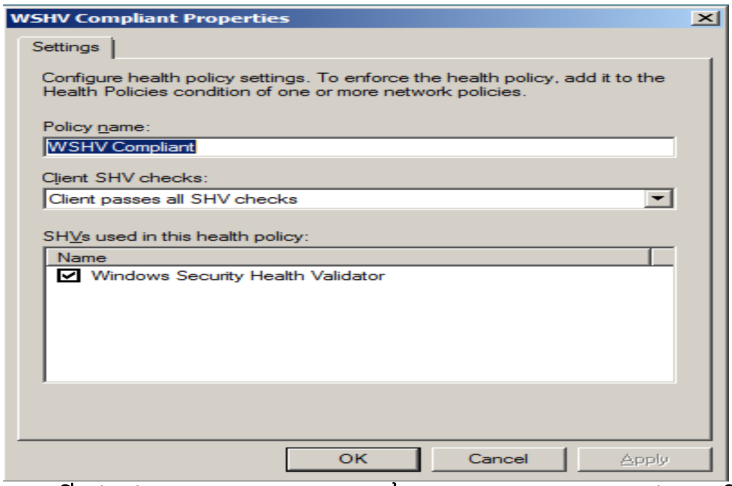
16. ជ្រើសរើស WSHV Compliant ពីតារាងនៃ Health Policies ហើយចុច OK ,ចុច Next ដើម្បីបន្តទៅមុខទៀត



ជ្រើសរើស Granted ពី Specify Access Permission លើអេក្រង់ហើយបន្ទាប់មកចុច Next



17. នៅលើ Configure Authentication Method លើអេក្រង់,ត្រួតពិនិត្យ Allow Client ដើម្បី connect ដោយគ្មាន Negotiating an Authentication Method ហើយនិងមិនពិនិត្យគ្រប់ Checkboxes ផ្សេងទៀតដូចបានបង្ហាញក្នុង Configure 8-14 បន្ទាប់មកចុច Next, ចុច No



នៅពេលអ្នកមានចម្ងល់ដើម្បីរំលឹកដល់ការជួយបន្ថែមទៀតនូវរាល់ការព្រមានអំពីការជ្រើសរើសមិនត្រឹមត្រូវ

18. ចុច Next នៅលើ Configure Constraints កំណត់ទុក
19. នៅលើអេក្រង់របស់Configure Setting ជ្រើសរើសNAP Enforcement ពី Setting នៅលើអេក្រង់ផ្នែកខាងឆ្វេង

១៤-២-៤- ការដំឡើងនិងការ Configuring DHCP

យើងមានបច្ចេកទេសនៃការ Install និង Configure DHCP ផ្សេងៗគ្នាតាមរយៈ Windows Server 2008 សម្រាប់ឧទាហរណ៍ខាងក្រោមនេះ យើងអនុវត្តនៅលើ NPS Server យើងត្រូវការចូលទៅកាន់ NAP-enable ហើយប្រើ DHCP Options ដើម្បីការពារ Clients ផ្តល់ Access ទៅឱ្យ Network នៅក្នុង NAP Policies។

១.Log on NPS server របស់យើងដែលមាន Account មាន Domain Admin Privileges។

២. បើក Server Manager

៣. ចុចលើ Add Roles ដើម្បីបើក Add Roles Wizard

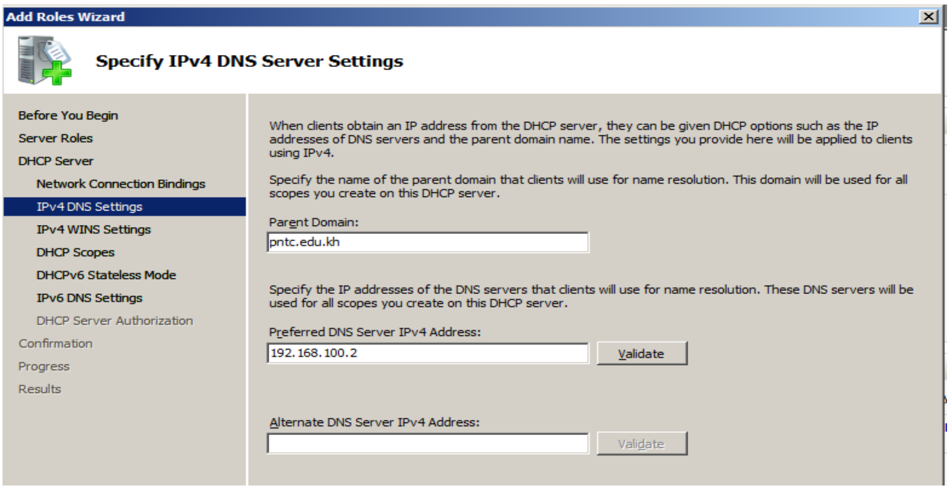
៤. ចុច Next មុននឹងឃើញ Begin Page

៥. ជ្រើសរើស DHCP Server នៅក្នុង Select Server Roles screen បន្ទាប់មកចុច Next

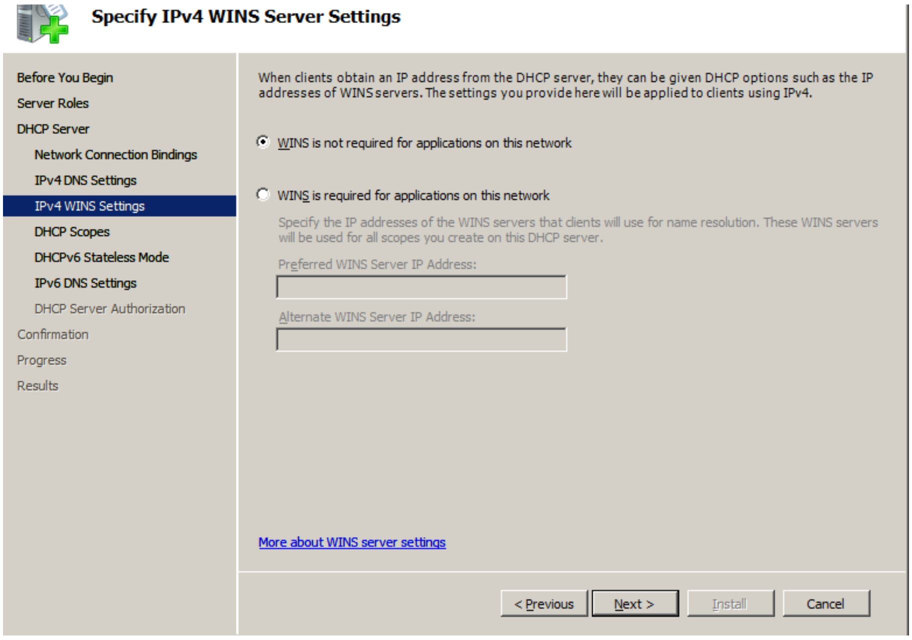
៦. ចុច Next ដើម្បីបើកទំព័រណែនាំអំពីការប្រើប្រាស់ DHCP

៧. ជ្រើសរើស Network Connection ណាមួយដែលយើងភ្ជាប់ DHCP Server ហើយចុច Next

៨. Enter the Preferred (ហើយ Optionally the alternative) DNS Server IP address បន្ទាប់មកចុច Next

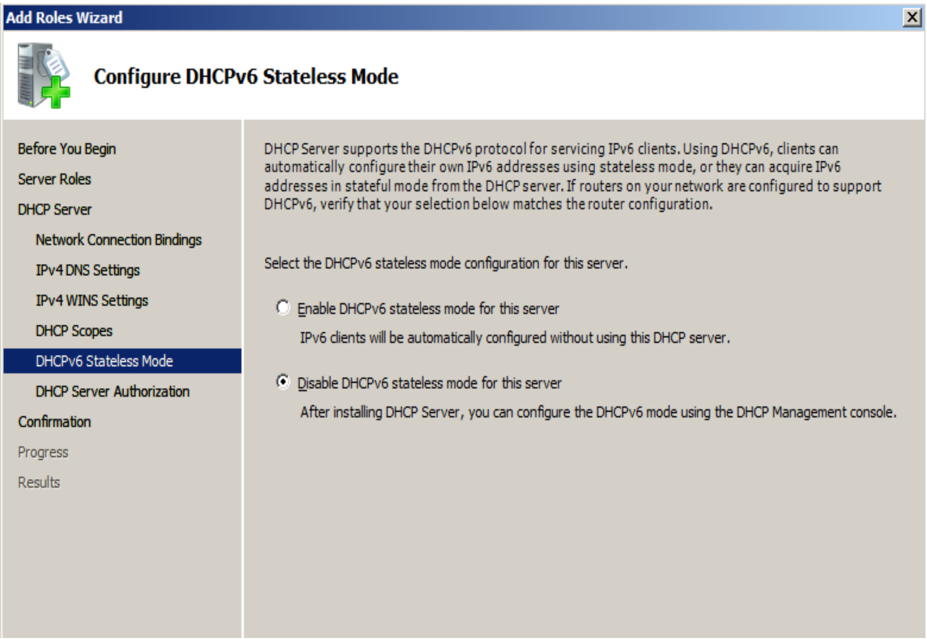


៩. ជ្រើសរើស WINS Is Not Required This Network បន្ទាប់មកចុច Next



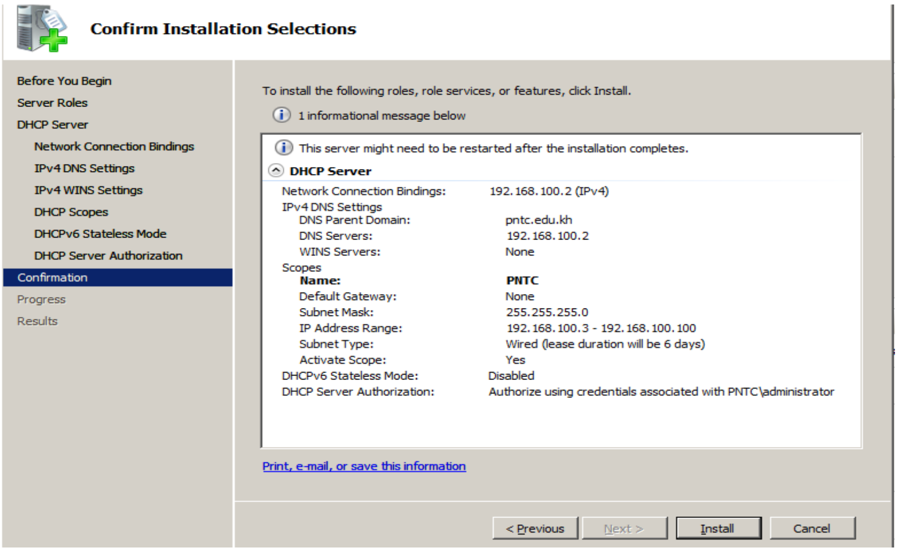
១០.ក្នុង DHCP Scope Screen ចុច Next បន្ទាប់មកចុច Next ម្តងទៀត។ យើងនឹង Configure Scopes ពេលក្រោយ។

១១. ជ្រើសរើស No, Do Not Configure This Server សម្រាប់ DHCPv6 Stateless Operation Now បន្ទាប់មកចុច Next



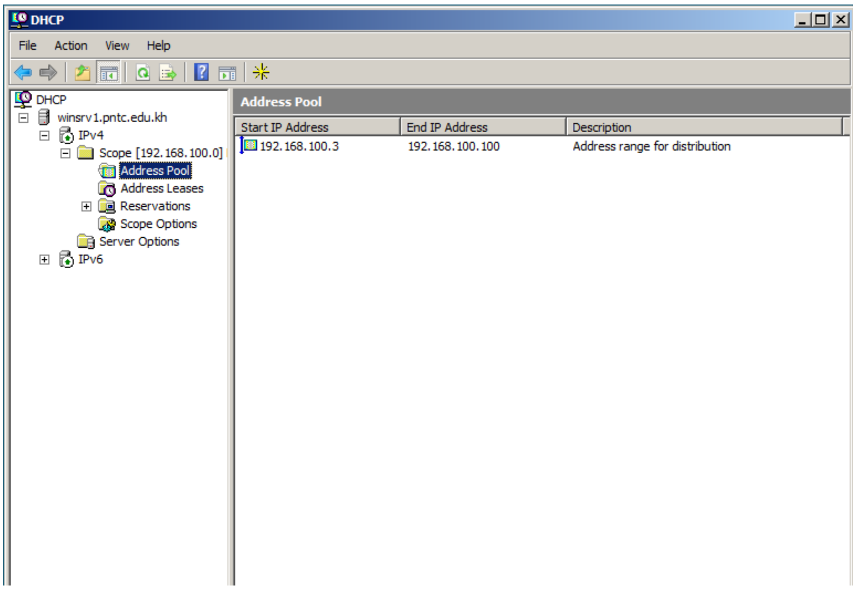
១២. លើ DHCP Server Authorization Screen ជ្រើសរើស Use Current Credentials បន្ទាប់មកចុច Next។

១៣. ចុច Install ក្រោយពី Confirmed ដែលបានជ្រើសរើសសម្រាប់ការ Install ត្រឹមត្រូវ

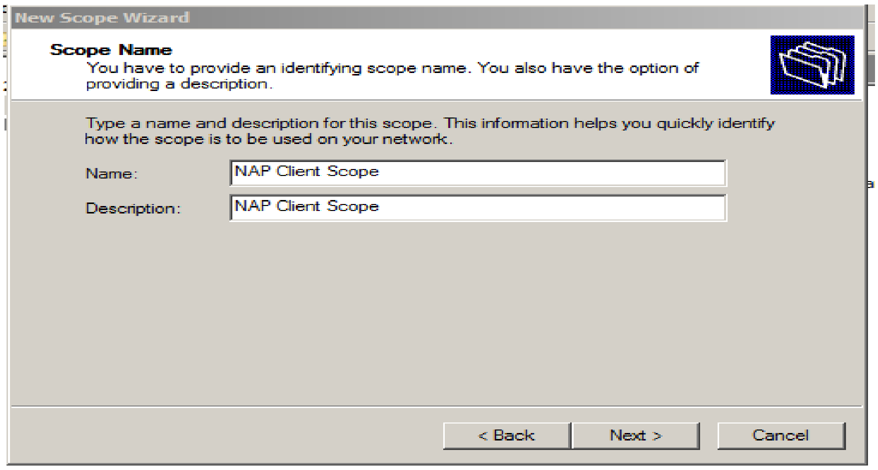


១៤. ជំហានបន្ទាប់គឺធ្វើវាមានទំនាក់ទំនងនៃការបង្កើត DHCP Scope មួយទៀត។ បើក DHCP Server MMC snap-in: Choose Start (Administrative Tools/ DHCP Server)។

១៥. ពង្រីក Server និង IPv4 នៅក្នុង Content Tree view



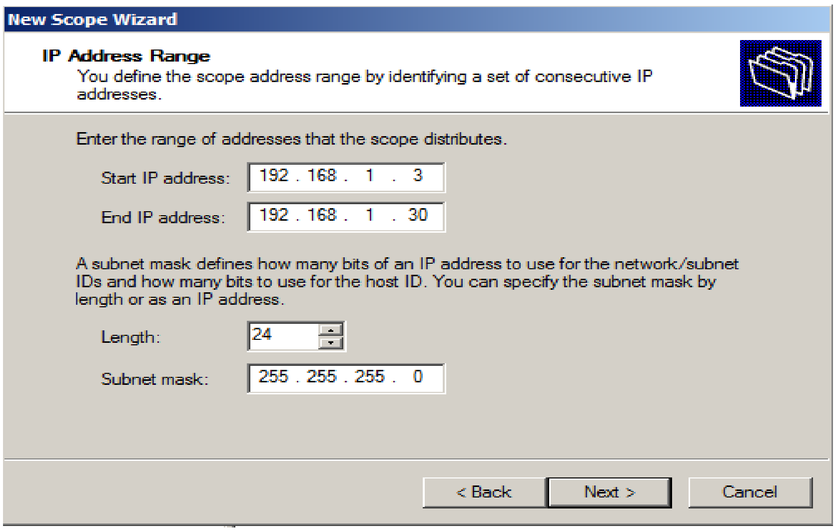
១៦. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ IPv4 ហើយជ្រើសរើស New Scope



១៧. ចុច Next លើ Welcome Screen

១៨. ចូលទៅក្នុង Scope Name Screen ហើយ Enter លើ NAP-Client Scope ទាំង Name និង Description fields ហើយចុចលើ Next

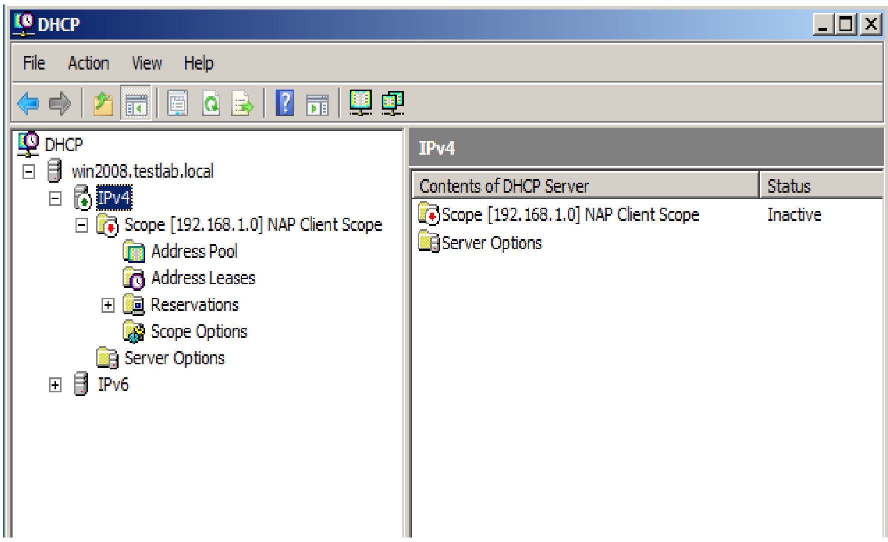
១៩.ចាប់ផ្តើមពី IP Address 192.168.1.3 ហើយបញ្ចប់ទៅវិញនូវ IP Address 192.168.1.30 បន្ទាប់មកចុច Next



២០. ចុច Next នៅក្នុង Lease Duration Screen

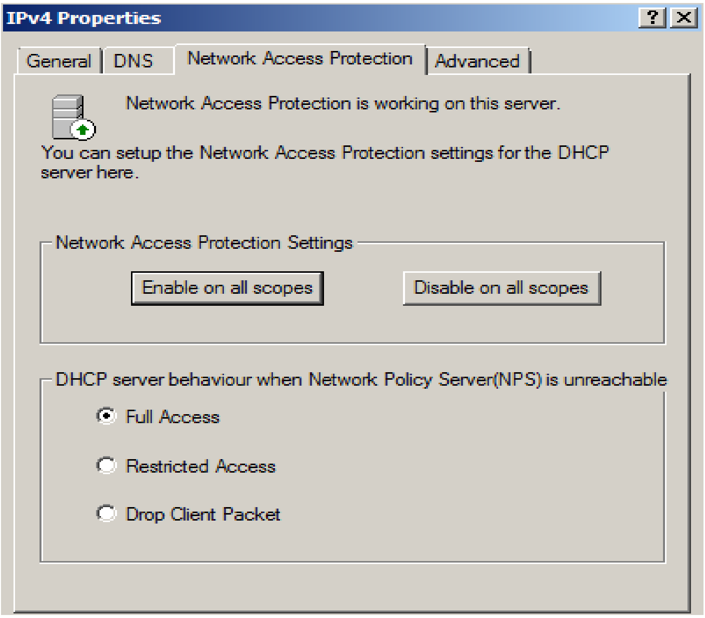
២១. ក្នុង DHCP Options Screen ជ្រើសរើសលេខដែលយើងនឹង Configure Options ពេលក្រោយហើយចុច Next

២២. បន្ទាប់មកចុច Finish



២៣. យើងត្រូវចូលទៅ Enable NAP ស្ថិតក្នុង DHCP Server ហើយ Right-Click IPv4 បន្ទាប់មកជ្រើសរើស Properties។

២៤. ចុច Network Access Protection Tab បន្ទាប់មកចុច Enable គ្រប់ Scope ទាំងអស់

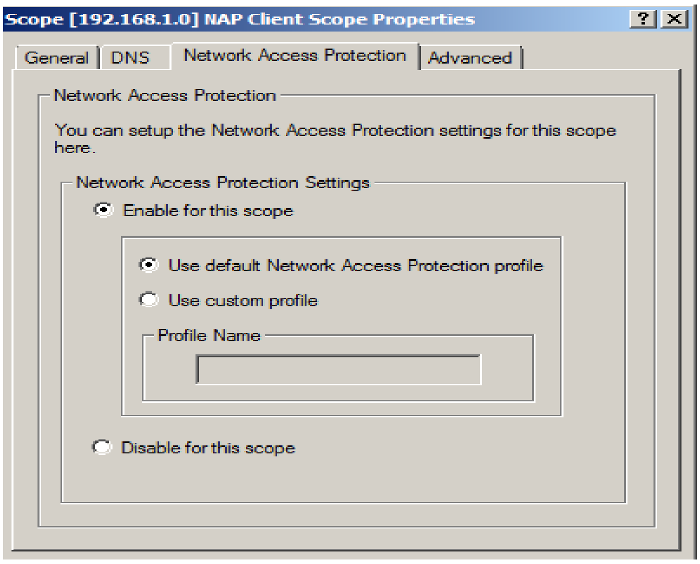


២៥. ចុច Yes នៅពេលដែលគេសួរថាយើងចង់ Overwrite NAP Settings

២៦. ចុច Ok ដើម្បីបង្កើតខាងដើម បន្ទាប់មកជ្រើសរើស Properties

២៧. ចុចដោយប្រើប៊ូតុងMouse ខាងស្តាំលើ Scope ដែលបានបង្កើតខាងដើមបន្ទាប់មកជ្រើសរើស Properties

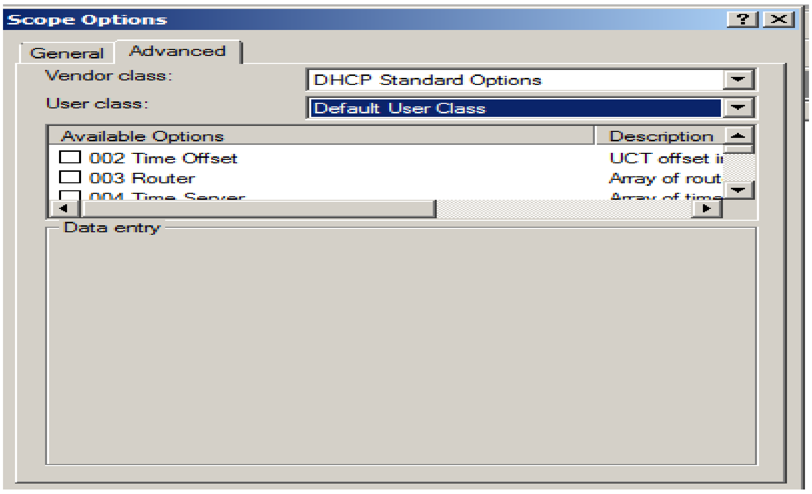
២៨. ចុច Network Access Protection Tab ដើម្បី Enable Network Access Protection Setting សម្រាប់ Scope។ ហើយ Check នៃការប្រើប្រាស់ Default Network Access Protection Profile ចុច Ok សម្រាប់ការ Save



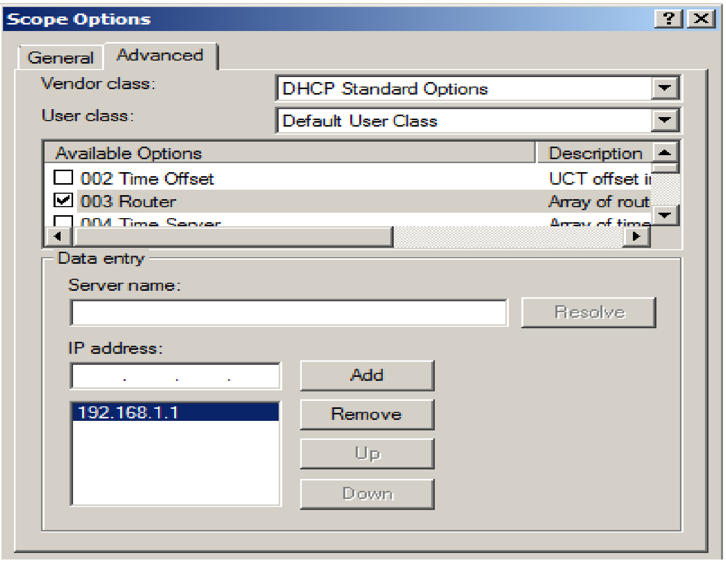
២៩. នៅក្នុង Scope នេះដែលយើងបានបង្កើត ចុចដោយប្រើប៊ូតុងMouse ខាងស្តាំលើScope Options ហើយជ្រើសរើស Configure Options

៣០. ចុចលើ Advance Tab

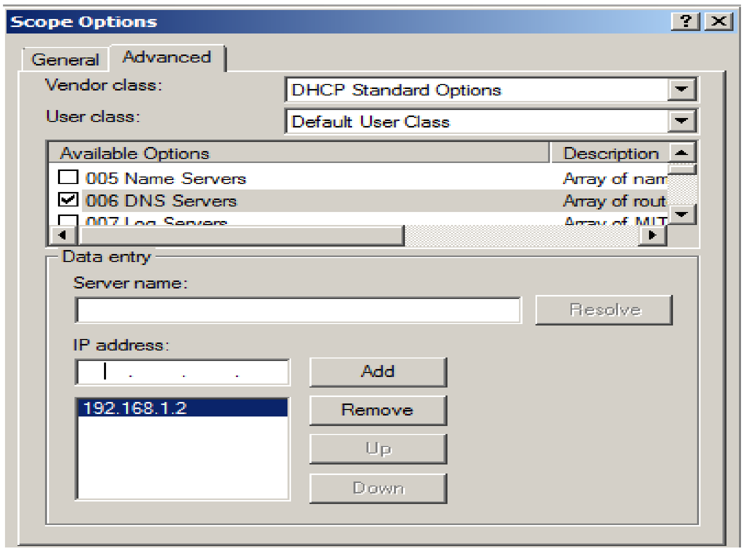
៣១. ជ្រើសរើស Default User Class នៅក្នុង User Class Drop-Down menu



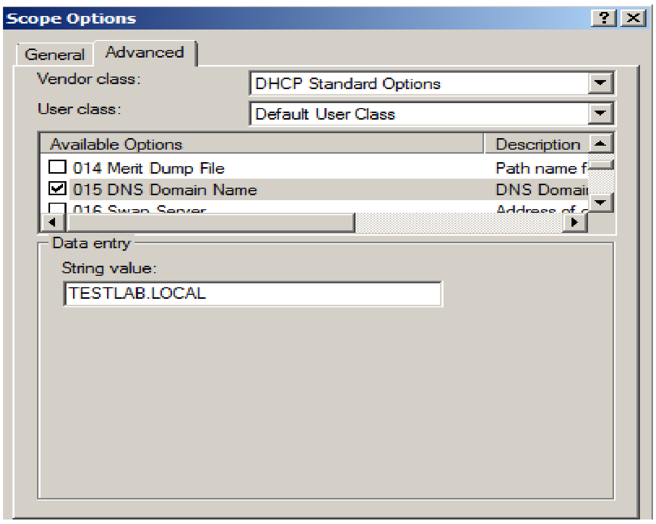
៣២. ចុចលើ 003 Router នៅខាងក្រោម Available Option ហើយ Enter លើ IP Address 192.168.1.1 បន្ទាប់មកចុចលើ Add។



៣៣. ចុចលើ 006 DNS Server នៅខាងក្រោម Available Option ហើយវាយបញ្ចូល IP Address 192.168.1.2 បន្ទាប់មកចុចលើ Add។



៣៤. ចុចលើ 015 DNS Domain Name ខាងក្រោម Available Option ហើយបញ្ចូល TESTLAB.LOCAL នៅក្នុង String Value Field



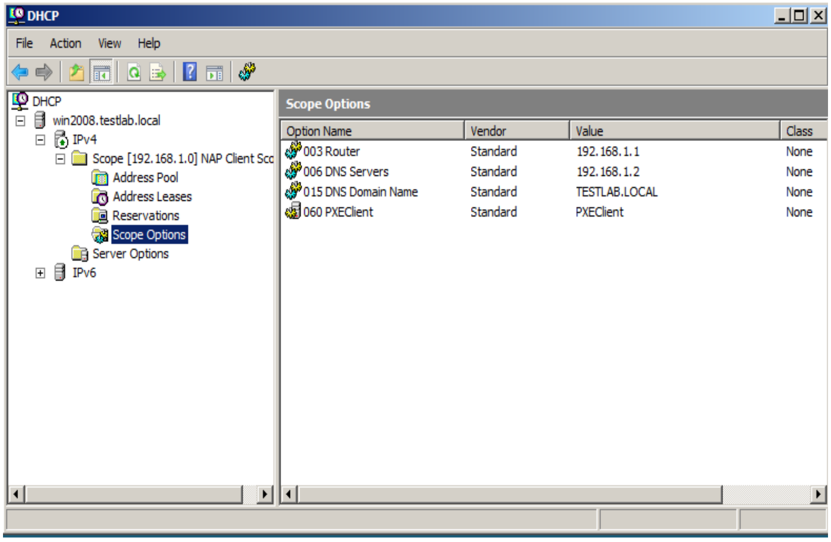
៣៥. ចុចលើ Apply ដើម្បីSaveនូវអ្វីដែលបានប្តូររបស់ Default User Class Drop-Down menu

៣៦. ជ្រើសរើស Default Network Access Protection Class ពី User Class Drop-down menu

៣៧. ចុចលើ 003 Router នៅខាងក្រោម Available Option ហើយវាយបញ្ចូលIP Address 192.168.1.1 បន្ទាប់មកចុច Add។

៣៨. ចុចលើ 006 DNS Server នៅខាងក្រោម Available Option ហើយវាយបញ្ចូលIP Address 192.168.1.2 បន្ទាប់មកចុច Add។

៣៩. ចុចលើ 015 DNS Domain Name និងវាយបញ្ចូល TESTLAB.LOCAL។



៤០. ចុចលើ Ok ដើម្បីSaveនូវអ្វីដែលយើងបានប្តូរ

៤១. ពង្រីកលើ IPv4 Note ចុចដោយប្រើប៊ូតុង mouse ខាងស្តាំលើ Scope ដែលយើងបានបង្កើតបន្ទាប់មកជ្រើសរើសActivate។

Configuring Client

នេះជាគឺហេដ្ឋារចនាសម្ព័ន្ធមួយដែល Client បានត្រៀមរួចរាល់ចូលរួមនៅក្នុង NAP។ NAP Serviceត្រូវបានគេកំណត់ឱ្យដំណើរ(Manually)នៅក្នុងWindow Vista អ្នកនិងត្រូវការ Configure ដើម្បី Run ជាស្វ័យប្រវត្តនិង Enable NAP Enforcement Client។ យើងត្រូវចូលបើក Security Center ឱ្យដំណើរការ Manually ពីព្រោះវាត្រូវបានបិទ(Disabled) ជា default ពេលដែល Window Vista ភ្ជាប់មកកាន់ Domain មួយ។

១. Log on to VISTAWKS

២. ចុចលើ Startនៅក្នុង Start Search field ហើយ Enter លើ gpedit.mscបន្ទាប់មកចុចENTER

៣. Expand Local កុំព្យូទ័រ Policy/កុំព្យូទ័រ Configuration/Administrative Templates/Windows Components/Security Center។

៤. ចុចពីរដងស្ទួនដើម្បីបើក Security Center (Domain PCs Only) បន្ទាប់ជ្រើសរើស Enabledហើយ Click OK។

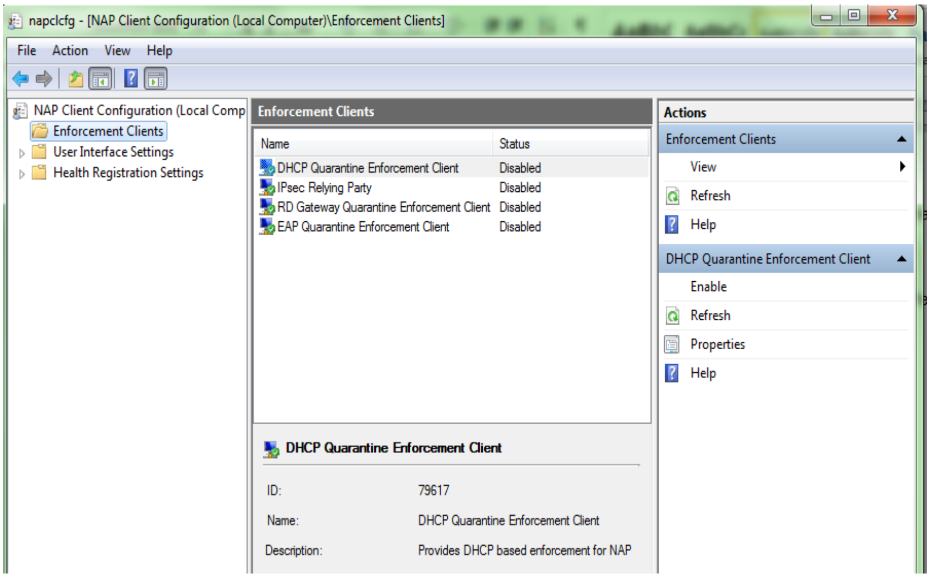
៥.បន្ទាប់មកបើក Control Panel

៦. ជ្រើសរើស System and Maintenance / Administrative Tools

៧. ចុចពីរដងស្ទួនលើ Services

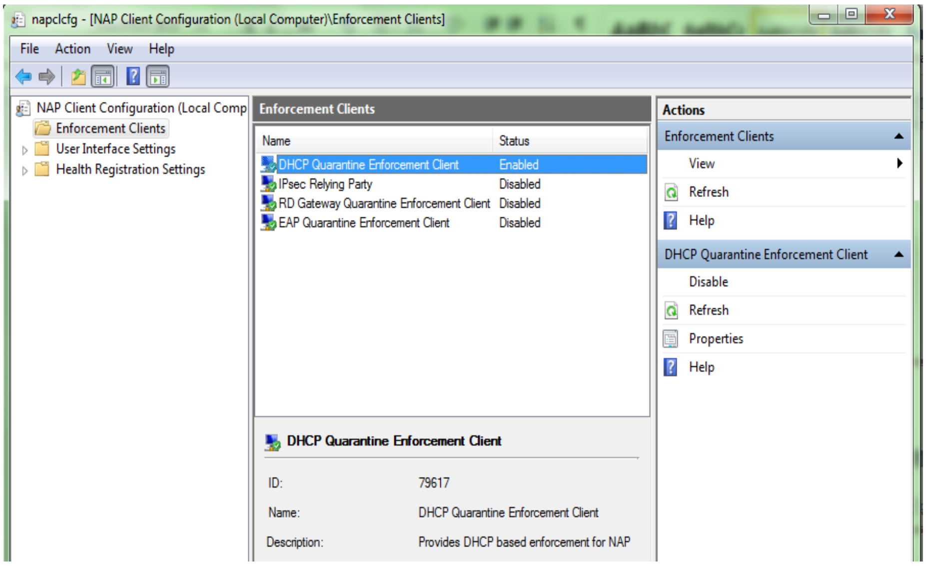
៨. ចុចពីរដងស្ទួនលើ Network Access Protection Agent ហើយប្តូរនូវ Startup Type ទៅជា Automaticបន្ទាប់មក Click OK។

៩. ចុចលើ Startនៅក្នុង Start Search field ហើយវាយបញ្ចូ napclcfg.mscបន្ទាប់មកចុចលើ ENTER វានឹងបើក NAP Client Configuration Console។



១០.ចុចលើ Enforcement Clients ដើម្បីបើក Enforcement Clients Window។

១១. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ DHCP Quarantine Enforcement Client ហើយចុច Enable នៅក្នុង Actions Pane។



១២. បិទ Windows បន្ទាប់មក Restart the កុំព្យូទ័រ។

១៤-២-៥- ការធ្វើតេស្ត NAP Client

Set គឺជាអ្វីដែលយើងត្រូវការផ្ទៀងផ្ទាត់ទៅគ្រប់ Setting ទាំងអស់ដែលកំពុងតែដំណើរការ។ បើសិនជាយើងអនុវត្តតាមជំហានទាំងអស់បន្ទាប់មក Rebooting Windows Vista client កុំព្យូទ័រដែលយើងនឹងត្រូវបានកំណត់ IP Address ពី DHCP Server យើងគួរតែធ្វើតាមធម្មតា បើយើងគ្មាន NAP Enable ពីព្រោះ Windows Vista Client កុំព្យូទ័រ មានបើក Firewall ជា Default គ្រប់ Network Interface ទាំងអស់ ដូច្នេះបើយើងបើក Security Center ពី Control Panel ហើយបិទ Firewall នៅលើ Network Interface ប្រហែលជា២វិនាទី Default Gateway និងត្រូវបានបាត់ហើយយើងអាចបន្តដាក់នៅក្នុង Access Mode ដែលត្រូវបានកំណត់។ បើយើងចុចពីរដងផ្ទួនគ្នាលើ NAP Client Message នៅលើ Taskbar យើងនិងឃើញRemediation Message ពី SHV កំពុងតែចាប់ផ្តើមដែលកុំព្យូទ័រមិនអាច Compliant ជាមួយនិងតម្រូវការនៃ Network ហើយត្រូវតែបើកកម្មវិធី Firewall CompatibleជាមួយនឹងSecurity Center។ បើយើងបើក Firewall ឡើងវិញ នោះ NAP Client និងលុបវាបន្ទាប់មកវាទាមទារ IP Address ជាមួយ Access ដែលមិនកំណត់វិញ ។

សំណួរត្រួតពិនិត្យ

១-តើ NAP (Network Access Prolicies) គឺជាអ្វី ?

២-ចូរបង្ហាញពីរបៀប Install NAP ?

៣-ចូរបង្ហាញពីរបៀប Configure NAP Client ?

៤-តើ NAP និង Firewall ដូចគ្នាឬទេ ?

៥-តើ OS ណាខ្លះមាន NAP ?

៦-ចូរពន្យល់ពី

ក-Protected Zone

ខ-Boundary Zone

គ-Quarintine Zone

ជំពូកទី១៥

Terminal Services

ក្រុមហ៊ុនកាន់តែច្រើនឡើងៗបានវាយតម្លៃទៅលើការអនុញ្ញាតឱ្យនិយោជិកប្រើប្រាស់ Applications ពីចម្ងាយដោយមានសុវត្ថិភាពខ្ពស់ហើយប្រើប្រាស់បានគ្រប់ពេលវេលានិងគ្រប់ទីកន្លែងទាំងអស់។ ទោះបីជា VPN ជាដំណោះស្រាយដ៏ល្អសម្រាប់ការប្រើប្រាស់ Applications ពីចម្ងាយយ៉ាងណាក៏ដោយក៏វាមានចំណុចខ្សោយដែរ។ ឧទាហរណ៍ អ្នកចង់កំណត់ឱ្យប្រើប្រាស់តែ Application មួយឬពីរប៉ុណ្ណោះ។ Terminal Service(TS) ក្នុង Windows Server 2008 មានសមត្ថភាពក្នុងការបំរើសេវានេះ។ វាក៏មានសមត្ថភាពជួយដល់អ្នកគ្រប់គ្រងលើប្រព័ន្ធ Network ក្នុងការគ្រប់គ្រងពីចម្ងាយលើ server របស់គេផង ដែរ។

Windows server 2008 បានបន្ថែមនូវលក្ខណ:ពិសេសបន្ថែមទៀតទៅឱ្យ terminal Service ដែលធ្វើឱ្យមានកាន់តែមានតម្លៃថែមទៀត។

តួនាទីនៃTerminal Service Gateway បានអនុញ្ញាតឱ្យភ្ជាប់តាមប្រព័ន្ធ Internet ដោយមានសុវត្ថិភាពខ្ពស់តាម HTTPS ដោយមិនចាំបាច់ប្រើ VPN ។

Terminal Server Remote Programគឺជាលក្ខណ:ពិសេសមួយទៀតដែលអនុញ្ញាតឱ្យ Application នីមួយៗអាច Run ពីចម្ងាយដូចជាលើកុំព្យូទ័រដោយផ្ទាល់។

១៥-១- តួនាទីដ៏សំខាន់របស់ Terminal Services

Terminal Service ក្នុង Windows Server 2008 បានកែប្រែតួនាទីជាច្រើនដោយរួមមានទាំងប្រសិទ្ធភាពនៃការប្រើប្រាស់សមត្ថភាពនិងសុវត្ថិភាព។ Windows server 2008 ភ្ជាប់មកជាមួយ Remote Desktop Connection 6.1 ។ ចំពោះការចាប់ផ្តើមដំបូងវាមាន 32-bit color និងមាន Font ល្អ។

Remote Desktop Connection 6.1

Remote Desktop Connection មាន Resolution អតិបរមារហូតដល់ 4096x2048 pixels ។ ដើម្បីដំណើរការ Remote Desktop connection ដោយប្រើ Resolution តាមតម្រូវការគេប្រើបញ្ជា

Mstsc.exe /w:1280 /h:1024

អ្នកក៏អាចពង្រីកទំហំអេក្រង់ដោយប្រើបញ្ជា

Mstsc.exe /span

១៥-២- Single-sign-ON

បើអ្នកសាកសួរទៅអ្នកប្រើប្រាស់ណាម្នាក់អំពី network security ថាតើអ្វីដែលគេមិនចូលចិត្តបំផុតគឺគេនឹងឆ្លើយថាពិបាកចាំនូវ Username និង Password។ តាមធម្មតានៅពេលដែលអ្នក Logon មកកាន់ Terminal Service វានិងទាមទារឱ្យអ្នកវាយបញ្ចូលនៅលេខសំងាត់ដើម្បីLogon មកកាន់ Terminal Server។ បើអ្នកចង់ប្តូរលេខសំងាត់វានិងទាមទារឱ្យអ្នកវាយបញ្ចូលលេខសំងាត់ជាច្រើនដង។

Terminal Service នៅលើ Windows server 2008 គាំទ្រនៅ Single-sign On មានន័យថា អ្នកប្រើលេខសំងាត់ដូចគ្នាអាច Logon មកកាន់ workstation និង Terminal Server

ដើម្បីប្រើប្រាស់ Single-sign On បាន System ត្រូវបំពេញល័ក្ខខណ្ឌ័ដូចខាងក្រោម

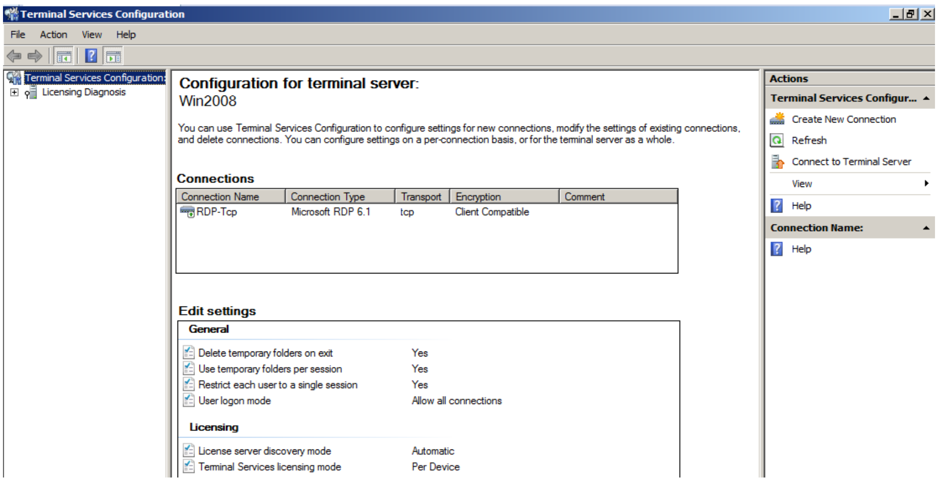
- Client ត្រូវជា Windows Vista ឬ Windows Server 2008

- User Account ត្រូវតែមានសិទ្ធិ Logon មកកាន់ Workstation(domain logon) និង Terminal Server
- Client និង Terminal Server ត្រូវតែជាផ្នែកមួយនៃ Domain

លំហាត់អនុវត្ត

ចំពោះ Server អ្នកត្រូវអនុវត្តដូចខាងក្រោម

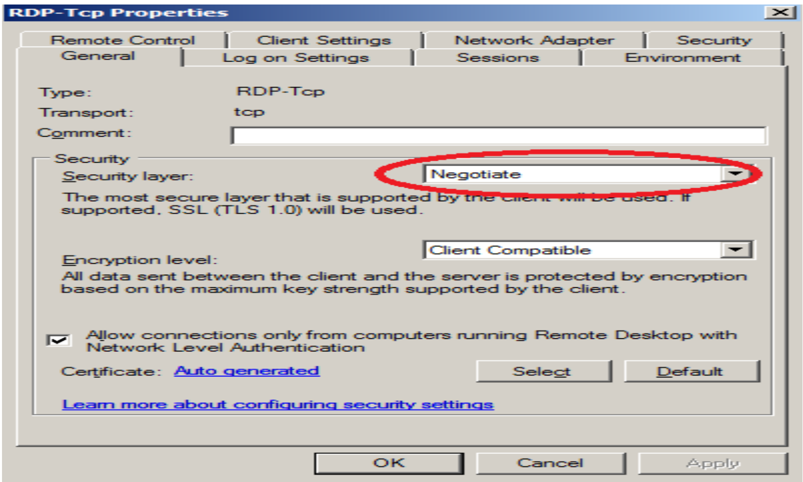
1- ជ្រើសរើសយក Start->RUN ហើយវាយពាក្យថា **tsconfig.msc**



នេះគឺជា Terminal Services Configuration Screen

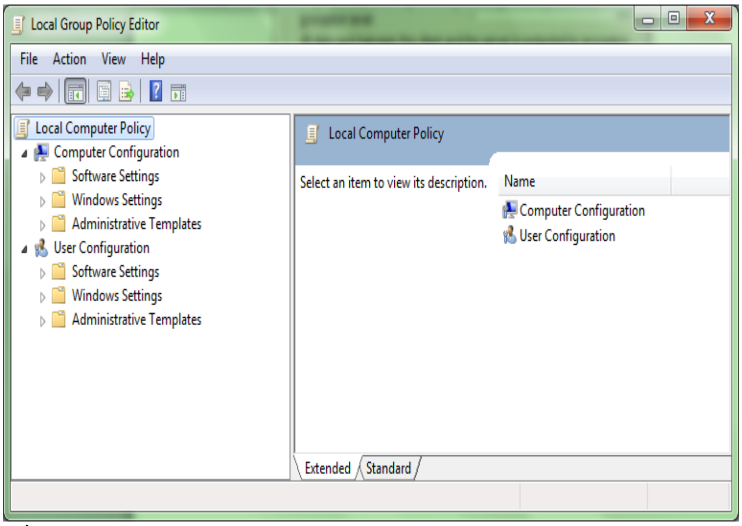
2- នៅក្នុងផ្នែកនៃ connection ចុចដោយប្រើ Button Mouse ខាងស្តាំលើ RDP-Tcp ហើយជ្រើសរើសយក Properties

3- នៅលើ General Tab ត្រូវប្រាកដថា Security level មានតម្លៃជា Negotiate or SSL(TSL1.0)



ចំពោះ client វិញត្រូវ Configure ដូចខាងក្រោម

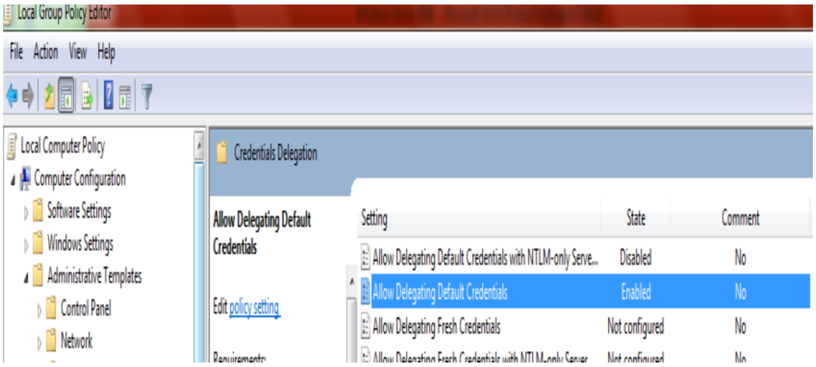
1- ជ្រើសរើសយក Start->Search ហើយវាបញ្ចូល **gpedit.msc**

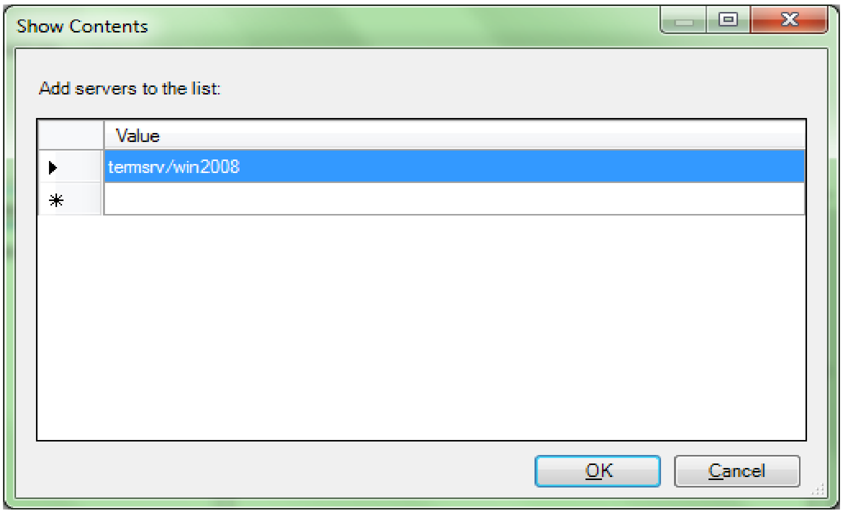


2- ជ្រើសរើសយកកុំព្យូទ័រ Configuration->administrative Templates->System->Credentials Delegation

3- ចុចពីរដងលើ Allow Delegation Default Credentials

4- ជ្រើសរើសយក Enabled ហើយបន្ទាប់មកចុចលើ Show button





5- វាយបញ្ចូលពាក្យថា **terms/win2008**

6- ចុចលើ Ok

7- Run បញ្ជា **gpupdate**

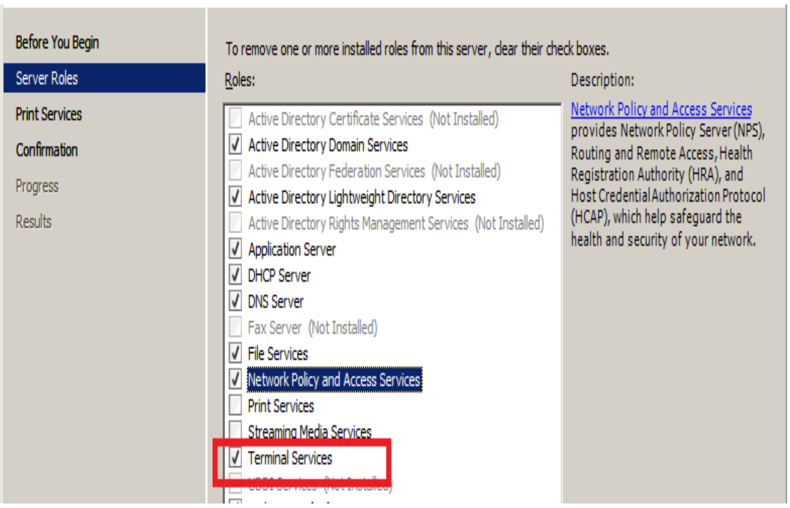
សាកល្បងដោយបើក Remote Desktop connection លើ Client ដោយប្រើ

Start->All Programs->Accessories->Remote Desktop conection ហើយបន្ទាប់មកភ្ជាប់មកកាន់ Server ។

១៥-៣- Installing Terminal Services

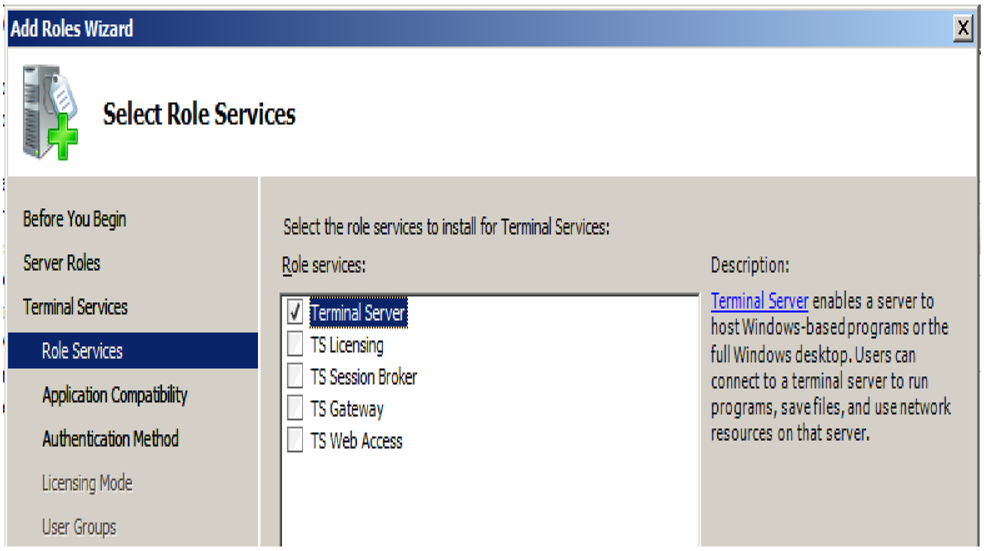
ដើម្បី Install Terminal Service អនុវត្តតាមជំហានខាងក្រោម

1- បើក Server Manager
2- ចុចលើ Add Role
3- ចុចលើ Next
4- Tick លើ Terminal Server Checkbox

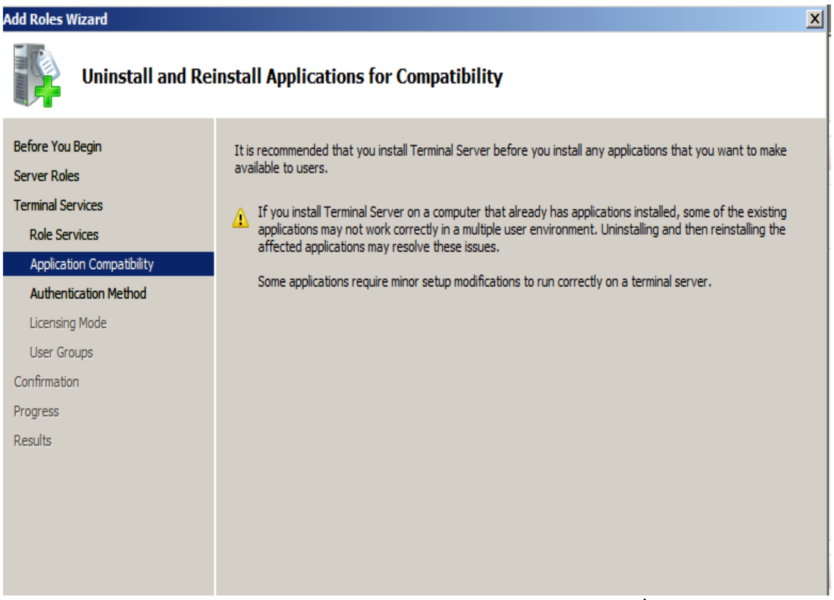


5- ចុចលើ next

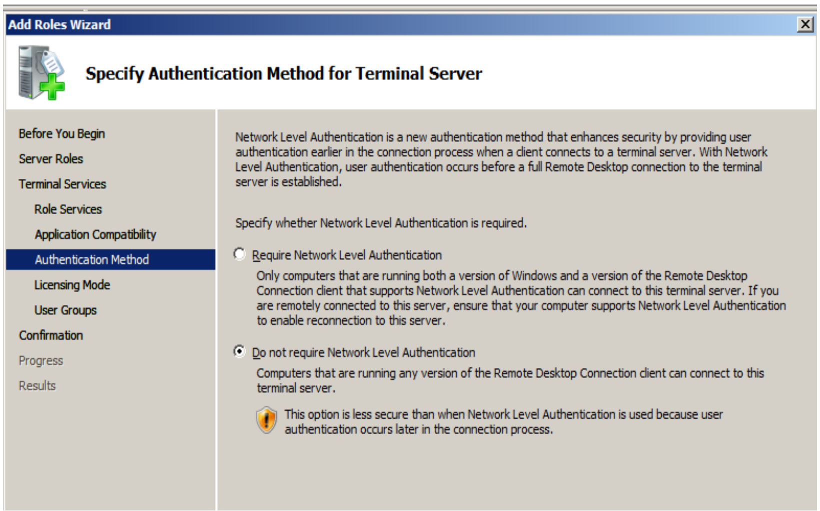
បើអ្នក Install វាលើ Domain Controller អ្នកនឹងឃើញនៅ Warning Message បង្ហាញថា Installing Terminal Services នៅលើ DC មិនត្រូវបានទាមទារនោះទេដោយសារតែមានការគិតគួរពីសមត្ថភាពនិងសុវត្ថិភាព



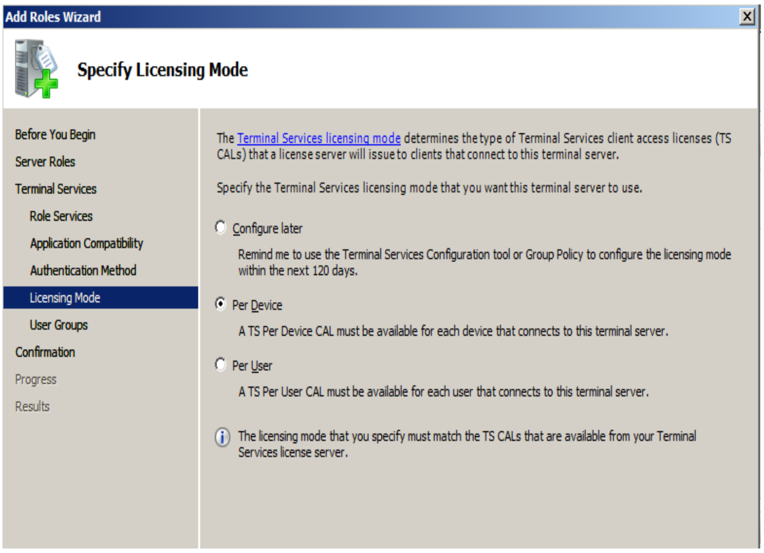
6- យើងត្រូវប្រាកដថា Checkbox របស់ Terminal Service ត្រូវបាន Check
7- ចុចលើ Next នៃ Uninstall and reinstall Application for compatibility Screen



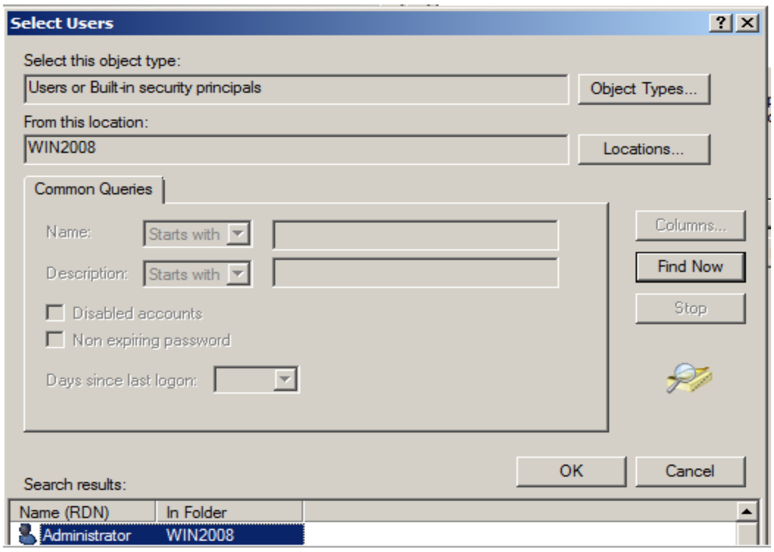
8- ចំពោះ authentication Method for Terminal Server Screen ជ្រើសរើសយក Do not Require Network Level Authentication



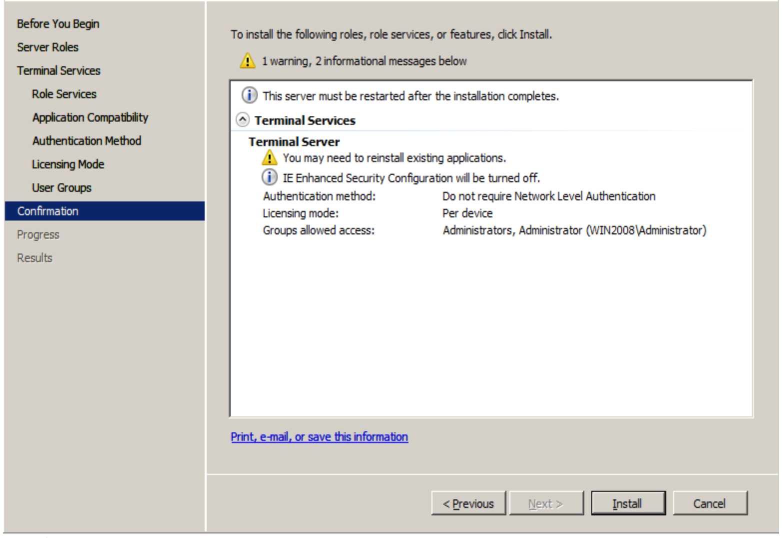
9- កំណត់ Licensing Mode



10- Add យក User ឬ Groups ដែលទទួលបានសិទ្ធិ Access ចំពោះ Terminal server



11- ចុចលើ Install



12- Restart your កុំព្យូទ័រ

១៥-៤- Terminal Services Licensing

Windows Server 2008 រួមមាន Service មួយហៅថា Terminal Service licensing ដែលត្រូវបានគេប្រើប្រាស់ដើម្បីគ្រប់គ្រងលើអាជ្ញប័ណ្ណនៃ Terminal Service ។

ប្រភេទនៃអាជ្ញាប័ណ្ណ

នៅពេលអ្នក Install Terminal Services នៅលើ Windows server 2008 វាទាមទារឱ្យបំពេញអាជ្ញាប័ណ្ណដែលមានប្រភេទជា

- Per device
- Per User

Per Device គឺជាប្រភេទនៃ Licensing mode ដែលត្រូវបានប្រើប្រាស់ដោយពឹងផ្អែកលើចំនួន Devices ដែលបានតភ្ជាប់។

Per User គឺជាប្រភេទនៃ Licensing mode ដែលគេហៅថា CAL(Client Access Licenses) ត្រូវបានប្រើប្រាស់ពឹងផ្អែកលើ User ដែល login ចូលក្នុង Network ។

Installing and Configuring TS Licensing

ដើម្បីទទួលបាន TS licensing ដំណើរការ គេត្រូវការបីជំហានគឺ

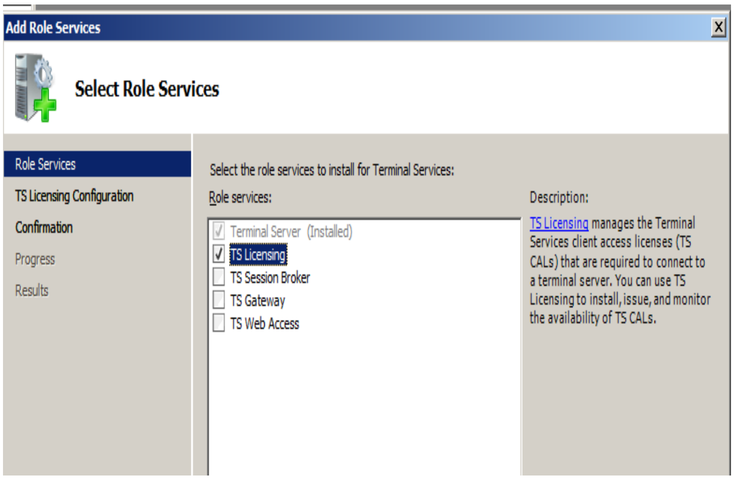
1- Install the TS Licensing role service
2- Activate the TS Licensing server
3- Install CALs on the TS Licensing server

Installing TS Licensing network ក៏ដូចគ្នាទៅនិងការ Install Terminal Server Role service ដែរ។

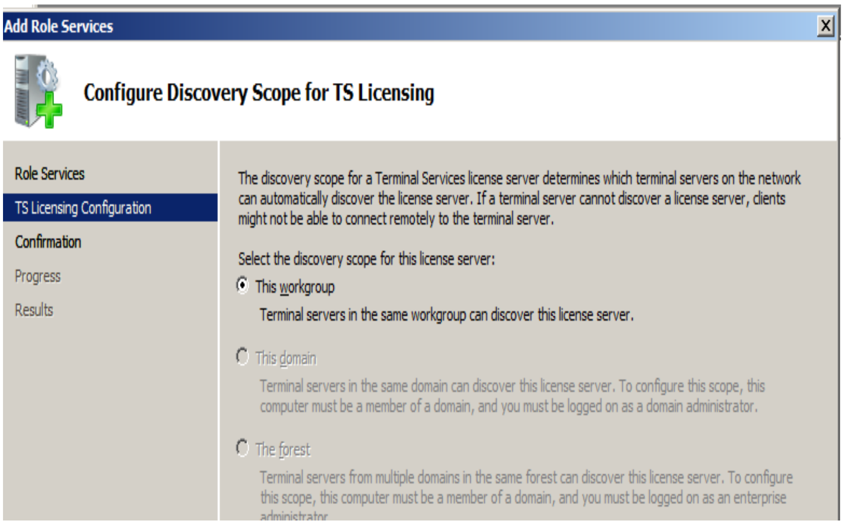
លំហាត់អនុវត្ត   Installing TS Licensing Role Service

ក្នុងលំហាត់នេះយើងនិងបន្ថែម TS Licesing role service ចំពោះ Terminal Server ដែលមានស្រាប់។

1- បើក Server Manager
2- ពង្រីក Manage Role ហើយជ្រើសរើសយក Terminal Services
3- ចុចលើ Add Role Service link



4- ជ្រើសរើសយក TS Licensing
5- Next
6- ជ្រើសរើសយក This workgroup

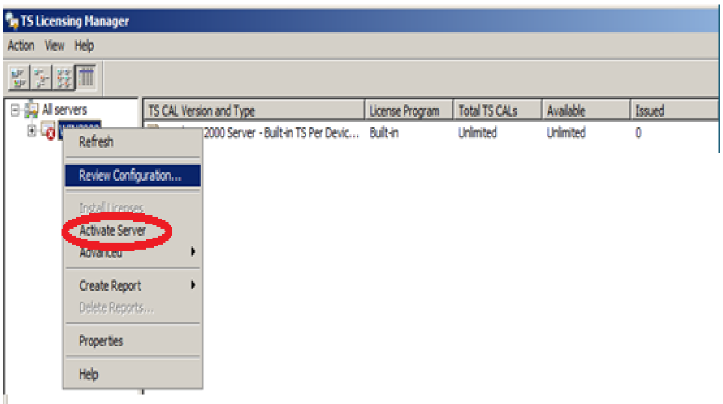


7- ចុចលើ Install on the confirm Installation Options
8- Close

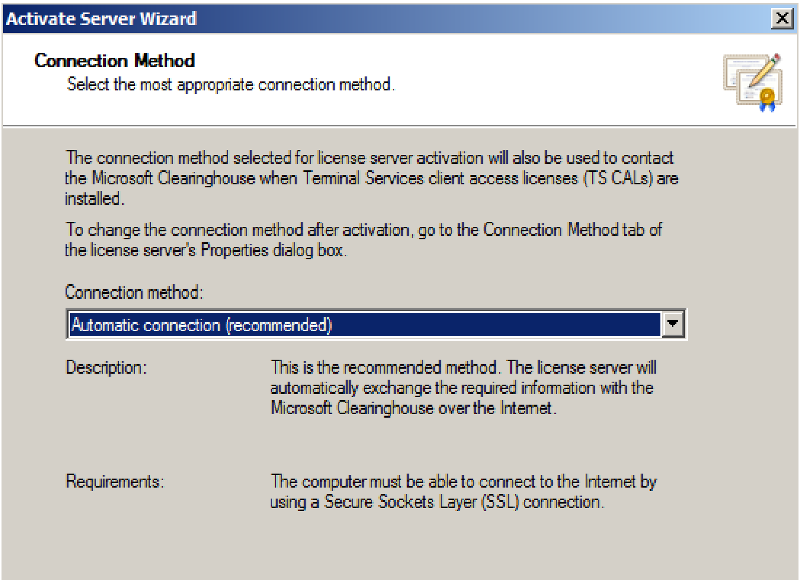
លំហាត់អនុវត្ត Activating TS Licensing Server

TS Licensing server មិនអាចដំណើរការបានល្អនោះទេលុះត្រាតែវាត្រូវបាន Activate ។ ដើម្បី Activate ត្រូវភ្ជាប់ជាមួយ Internet ។

1- ជ្រើសរើសយក Start=>Administrative Tools=> TS Licensing Manager
2- ចុចដោយប្រើ Button Mouse ខាងស្តាំលើ Server ដើម្បី Activate ហើយជ្រើសរើសយក Activate Server



3- Next
4- ជ្រើសរើសយក Automatic Connection(Recommended) ពី Connection Method



5- Next ហើយអនុវត្តតាមការណែនាំរបស់អេក្រង់រហូតដល់បញ្ចប់

លំហាត់អនុវត្ត Installing Client Access Licenses

បើអ្នកមិនបាន Install Client Access license ឱ្យ terminal Server Activated license ប្រើប្រាស់បានតែ 90 ថ្ងៃប៉ុណ្ណោះ។

1- ជ្រើសរើសយក Start=>Adminkstrative Tools=>Terminal Server Licensing
2- ចុចដោយប្រើប៊ូតុង Mouseខាងស្តាំលើ Server ដែលអ្នកចង់ Install CALs ម្តងទៀតហើយជ្រើសរើសយក Install license
3- ចុចលើ Next
4- នៅលើ License Program ជ្រើសរើសយកLicense Pack

5- បំពេញ License Code

6- ចុចលើ Finish

១៥-៥- Terminal Services Gateway

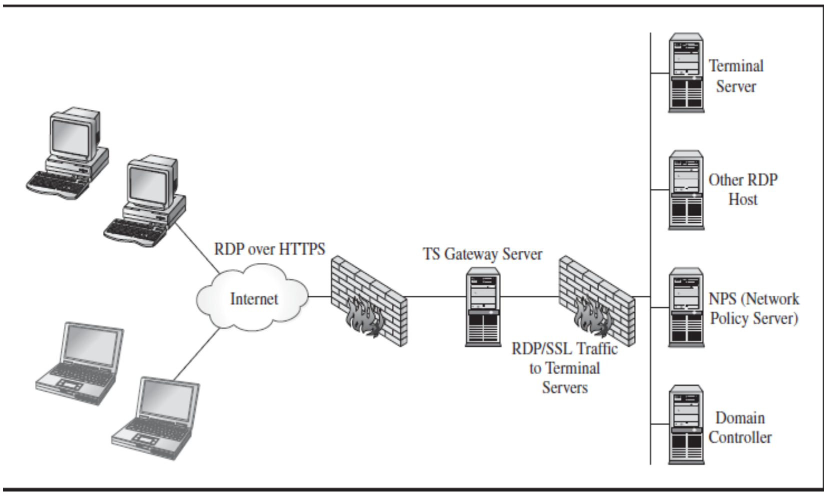
TS gateway អនុញ្ញាតឱ្យយើងអាចប្រើប្រាស់ Terminal servers ដែលស្ថិតនៅក្នុង Coporate netowk រួមទាំង server មានសុវត្ថិភាពដែលការពារដោយ Firewall ពីគ្រប់ទីកន្លែងទាំងអស់ គ្រប់ពេលវេលាទាំងអស់។ វាធ្វើការដោយ Encapsulate Remote Desktop Protocol (RDP) traffic លើ HTTPs tunnel នេះគឺជាគុណសម្បត្តិដ៏ធំដែលវាបានបើក port 3389 សម្រាប់ RDP connection។ វាបានបន្ថែមលក្ខណៈពិសេសនៃការបំបាត់ចោលការប្រើប្រាស់នៃ VPN ក្នុងករណីដែល VPN ត្រូវបានប្រើប្រាស់សម្រាប់តែ Access មកកាន់ Terminal Server ប៉ុណ្ណោះ។ TS gateway បានបញ្ចូលជាមួយ NAP ដែលអនុញ្ញាតឱ្យយើងធ្វើការកំណត់នៃការប្រើប្រាស់បន្ថែមទៀតដោយពឹងផ្អែកលើNAP Policies ។ ដើម្បីធ្វើឱ្យកាន់តែមានសុវត្ថិភាពខ្ពស់បន្ថែមទៀត អ្នកដាក់ TS Gateway Server ក្នុង Private Network របស់អ្នកដោយប្រើ MS ISA Server

ដើម្បីប្រើប្រាស់ TS Gateway បានត្រូវមាន Services ខាងក្រោម

- Windows server 2008
- Remote Procedure Call (RPC) over HTTP Proxy service
- Web Server (IIS7.0)
- Network Policy Server
- SSL certificate

១៥-៥-១- TS Gateway Architecture

អាស្រ័យទៅលើចំនួន Users និង Servers ដែលអ្នកត្រូវការប្រើប្រាស់ ដូច្នេះ services ជាច្រើនត្រូវការនៅលើ server តែមួយឬ នៅលើ Servers ជាច្រើន។
ក្នុងរូបភាពខាងក្រោមបង្ហាញពី client ភ្ជាប់ជាមួយ Terminal server ឬ RDP hosts ។



Terminal Services Gateway remote access

ពី Internet Client និងបង្កើត SSL tunnel មកកាន់ TS Gateway ។ មុនពេលទទួលបានការភ្ជាប់ វាត្រួតពិនិត្យមើលពីលេខសំងាត់របស់ Client ជាមួយ Connection Authorization Policy (CAPs) ដើម្បីកំណត់ឱ្យដឹងថា Client ទទួលបានសិទ្ធិភ្ជាប់មកកាន់ Gateway។ បើទទួលបានសិទ្ធិ បន្ទាប់មក Client ស្នើការស្នើសុំ resources ដែលមាននៅលើ Private Network ។ បន្ទាប់មក gateway ត្រួតពិនិត្យឱ្យដឹងថា Resources ដែលបានស្នើសុំមាននៅក្នុង Resource Authorization Policy (RAP) របស់ Gatway ឬទេ។ បើការត្រួតពិនិត្យទទួលបានជោគជ័យ បន្ទាប់មក gateway ភ្ជាប់មកកាន់ Resource ដែលបានស្នើសុំ។ វាបានបញ្ចប់ដោយបង្កើត Tunnel មួយដែលមានសុវត្ថិភាពរវាង Client និង Resource ដែលបានស្នើសុំ។

លំហាត់អនុវត្ត Installing និង Configuring TS Gateway

TS Gateway ពឹងផ្អែកលើផ្នែកជាច្រើន។ ក្នុងលំហាត់នេះផ្តោតទៅលើការអនុវត្តមួយផ្នែកនៃបញ្ហាដ៏ធំជាច្រើន។ យើងនិងអនុញ្ញាតឱ្យ Windows Vista អាច Access មកកាន់ Windows server 2008 Terminal server ដែលមានឈ្មោះថា Win2008 តាមរយៈ Terminal Services Gateway មានឈ្មោះថា WIN2K8TSG តាមជំហានដូចខាងក្រោម

1- Install TS Gateway role លើ Windows Server 2008 ដែលមានឈ្មោះថា WIN2K8TSG
2- Configure a certificate for the gateway
3- Define CAPs on the TS Gateway
4- Define RAPs on the TS Gateway
5- Connect to the terminal server ដែលមានឈ្មោះថា WIN2K8TS ពី Windows Vista

នៅក្នុងលំហាត់នេះសន្មត់ថា Service ខាងក្រោមត្រូវបាន Configure រួចហើយ

- An Active Directory domain controller
- Windows Server 2008 មានឈ្មោះថា WIN2K8TS កំពុងដំណើរការ
- Windows Vista/7 ជាសមាជិករបស់ Domain
- Terminal Service Gateway server មានឈ្មោះថា WIN2K8TSG ត្រូវបាន Install

Installing the TS Gateway Role

1- បើក Server Manager
2- ចុចលើ Add Roles link ដើម្បីដំណើរការ Add Roles Wizard
3- ចុចលើ Next
4- ជ្រើសរើសយក Terminal service ពី Server Role=>Next
5- ចុចលើ Next នៅលើ Introduction to Terminal service Screen
6- ជ្រើសរើសយក TS Gateway
7- ចុចលើ Next
8- ជ្រើសរើសយក Certicate for SSL Encryption Later ហើយបន្ទាប់មកចុចលើ Next
9- ជ្រើសរើសយក Later on the Create Authorization Policies for TS Gateway and then next
10- ចុចលើNext
11- ផ្ទៀងផ្ទាត់ Network Policy Server ត្រូវបានជ្រើសរើស=>Next

12- ចុចលើNext

13- ចុចលើNext

14- ចុចលើ Install

15- Close

១៥-៥-២- TS Gateway Certificates

TS Gateway ពឹងផ្អែកលើ Transport Layer Security (TLS) 1.0 (SSL 3.0) សម្រាប់ Encrypt ការប្រាស្រ័យទាក់ទងរវាង Client និង Gateway។ TLS 1.0 ទាមទារនូវ SSL-compatible x.500 certificate ត្រូវតែ Install នៅលើ Server ។

អ្នកអាចទទួលបាន Certificate តាមច្រើនរបៀបណាស់។ បើអ្នកមាន Certificate ដែលចេញដោយ Root certification authority (CA) ដែលបានចូលរួមក្នុង Microsoft's root Certificate Members Program ហើយបំពេញតាមតម្រូវការសម្រាប់ TS Gateway នោះអ្នកអាចប្រើប្រាស់វាយ៉ាងងាយ។ បើក្រុមហ៊ុនរបស់អ្នកមាន Enterprise CA អ្នកអាចប្រើប្រាស់វាដើម្បីផ្សព្វផ្សាយ Certificate ដែលបានផ្តល់ឱ្យដោយមានការយល់ព្រមពី root CA ។ បើអ្នកគ្មាន certificate ដែលមានស្រាប់នោះទេ អ្នកមានជម្រើសពីរយ៉ាងគឺ:

- អ្នកអាចទិញឬបង្កើតវាហើយទាញយក self-signed certificate

មានបញ្ហាតែមួយគត់ជាមួយការប្រើ self-signed certificate គឺ Client នឹងព្រមានថា certi -ficate នោះទទួលបានពីប្រភពដែលមិនអាចទុកចិត្តបាន។

Certificate ត្រូវតែបំពេញតាមលក្ខខណ្ឌតម្រូវការនៃ certificate

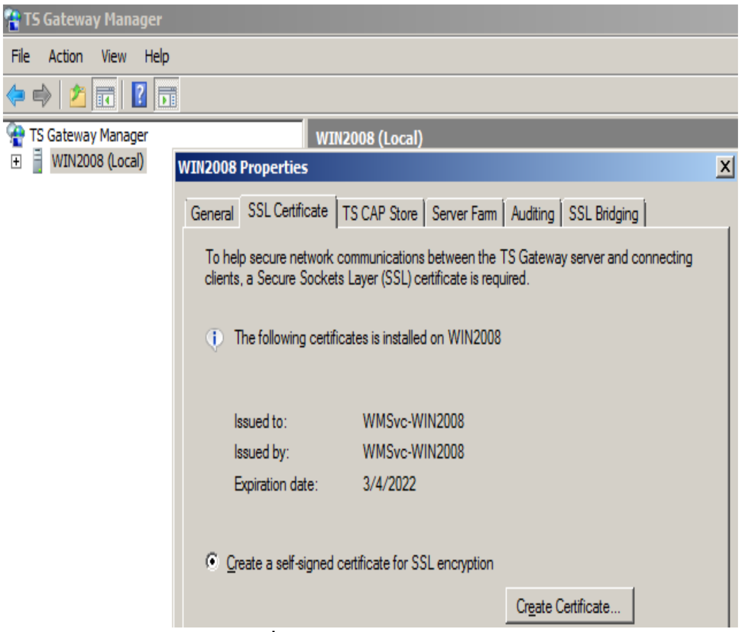
- ឈ្មោះត្រូវតែមានដូចឈ្មោះក្នុង TS Gateway Server
- EKU(Extended Key Usage គឺជា Server Authentication (1.3.6.1.5.3.1)
- វាត្រូវតែមានទំនាក់ទំនងជាមួយ Private Key
- មិនត្រូវហួសកំណត់
- បើអ្នកបាន Configure TS Gateway ជាមួយ NAP វាគាំទ្រ Encryption ។ OID (Object Identifier) សម្រាប់ប្រភេទនេះគឺ 2.5.29.15 ។

ការបង្កើត Self-signed Certificate

បើអ្នកគ្មាន certificate អ្នកអាចបង្កើតវាឬប្រើហើយបើអ្នកចង់សាកល្បងវា អ្នកអាចបង្កើតវា បាន។ ដើម្បីបង្កើតវា អ្នកអាចអនុវត្តតាមជំហានដូចខាងក្រោម:

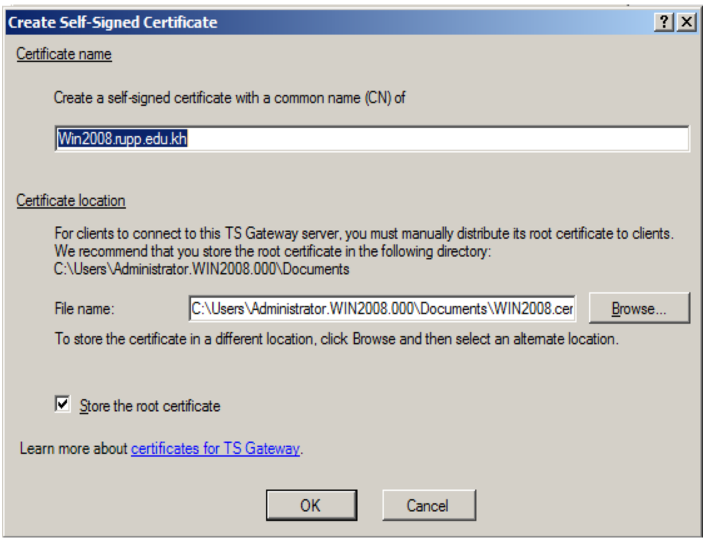
1- Start =>Administrative Tools=>Terminal Service=>TS Gateway Manager

2- Right-click លើឈ្មោះរបស់ Server ហើយជ្រើសរើសយក Properties



3- ចុចលើ SSL Certificate tab ហើយជ្រើសរើយក Create a Self-Signed Certificate for SSL Encryption ហើយបន្ទាប់មកចុចលើ Create Certificate button

4- ត្រូវចាំទីតាំង file ដែលយើងបានបង្កើតវា



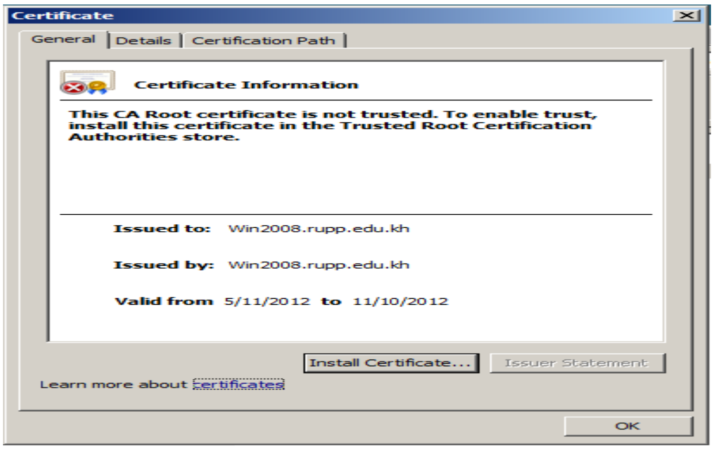
5- ចុចលើ Ok

6- ចុចលើ Ok

Installing a Certificate on the TS Gateway Server

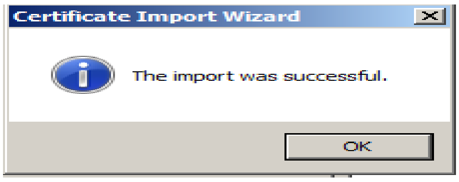
អ្នកត្រូវតែមាន Certificate ដែលអ្នកបានទាញយកវាមកប្រើលើ TS Gateway server ។ ក្នុងលំហាត់នេះអ្នកនិងដឹងពីរបៀបទាញយក Certificate

1- ស្វែងរកទីតាំង Certificate ដែលវាស្ថិតនៅ(ឧទាហរណ៍ c:\users\administrator\ WIN.2008. 000\Documents\WIN2008.cer)



2- ចុចលើ Install certificate

3- ចុចលើ Next



4- Ok

5- Ok

១៥-៥-៣- Configuring TS Gateway ដើម្បីប្រើ certificate

យើងត្រូវទទួលយក Certificate ដើម្បី Configure វាសម្រាប់ប្រើជាមួយ TS Gateway

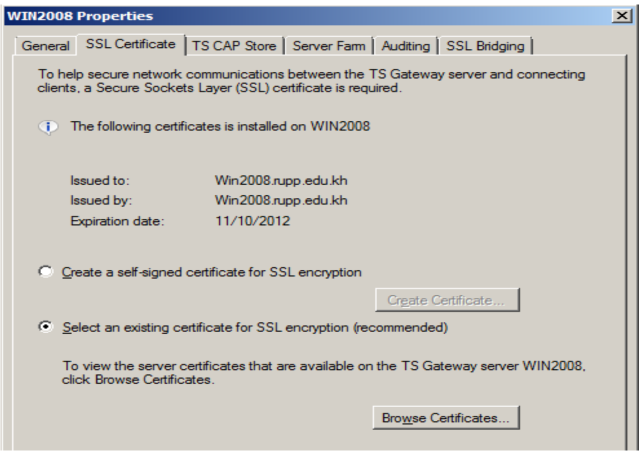
1- Start=>Administrative Tools=>Terminal Services=>TS Gateway Manager

2- ចុចដោយប្រើ Mouse ខាងស្តាំលើ TS Gateway server ហើយជ្រើសរើសយក Properities

3- នៅលើ SSL Certificate tab អ្នកនិងឃើញ

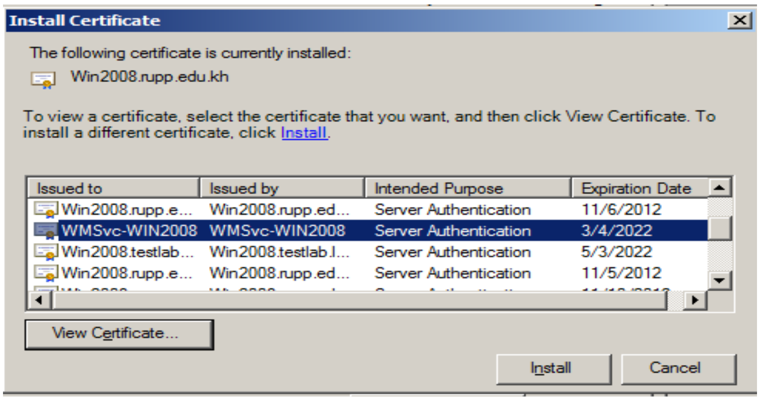
- Issued to
- Issued by
- Expiration Date

4- ចុចលើ Existing Certifcate ដែលអ្នកបានទាញយកវាពីមុនមក



5- ចុចលើ Browse Certificate

6- ជ្រើសរើសយក Server Certificate ដែលយើងបានទាញយកពីមុនមក



7- ចុចលើ Install

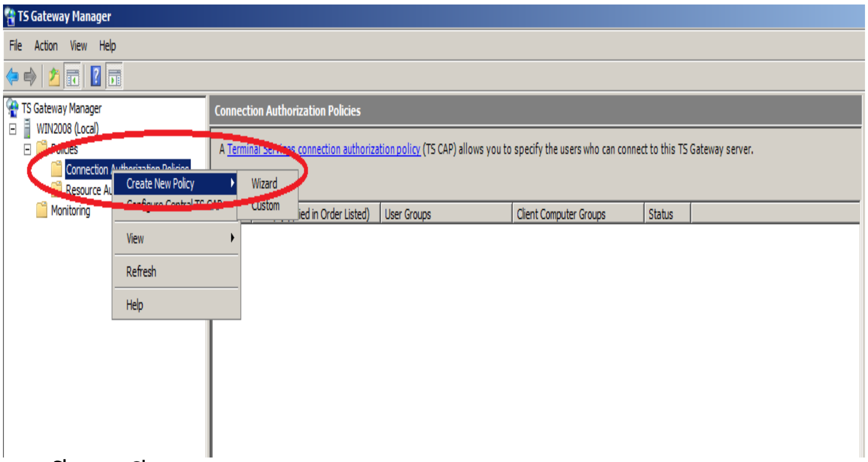
8- Ok

១៥-៥-៤- Configuring Connection Authorization Policies

Connection Authorization Policies កំណត់ថាតើនរណាអាចធ្វើអ្វីមួយចំពោះ TS Gateway

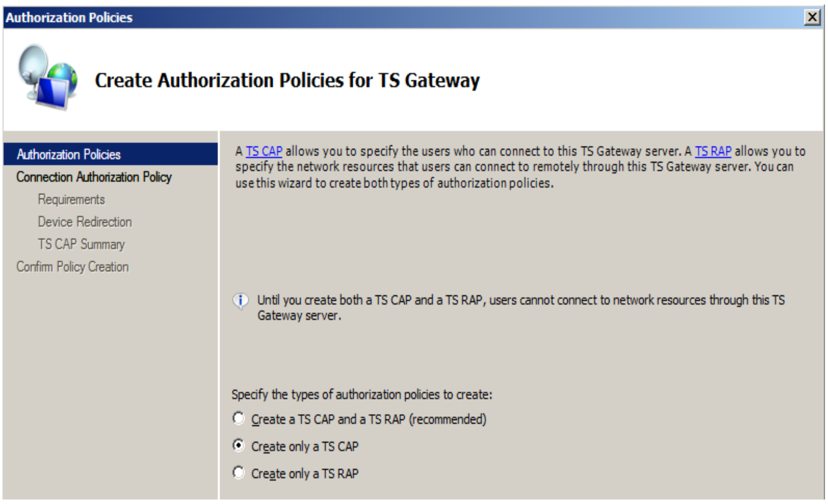
1- Start=>Administrative Tools=>Terminal services=>TS Gateway server Manager

2- ចុចលើសញ្ញា + ដើម្បីពង្រីក Tree node តំណាងឱ្យ TS Gateway server



3- ចុចលើសញ្ញា + ដើម្បីពង្រីកវាឱ្យឃើញ Connection Authorization Policies

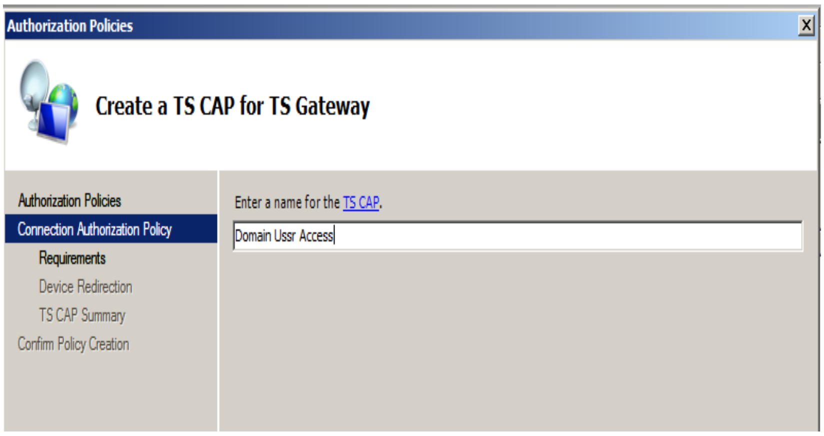
4- Select លើ Connection Authorization Policies=>Create New Policy=>Wizard

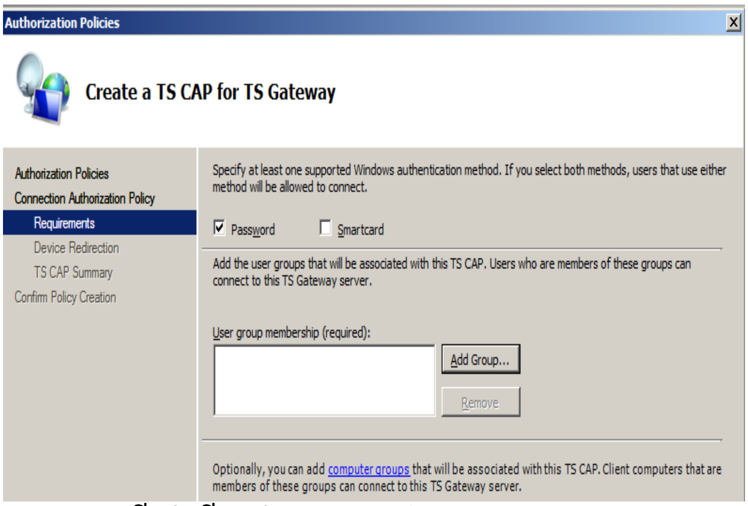


5- ជ្រើសរើសយក Create only a TS CAP ហើយបន្ទាប់មកចុចលើ Next

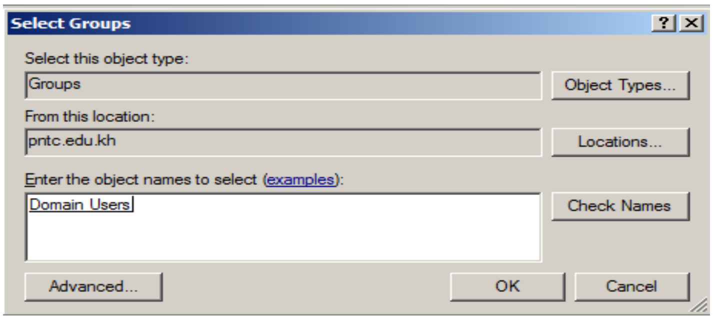
6- វាយបញ្ចូលឈ្មោះក្នុង TS CAP field ថា **Domain User Access** ហើយបន្ទាប់មកចុចលើ Next

7- ត្រូវ tick លើ checkbox នៃ Password ហើយមិន Tick លើ smartcard

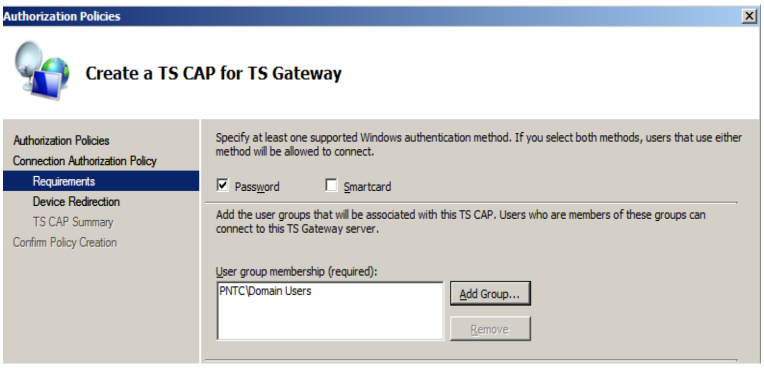




8- ចុចលើ Add Group button ដើម្បីជ្រើសរើសយក Group នៃ User ដូចជា **Domain Users**

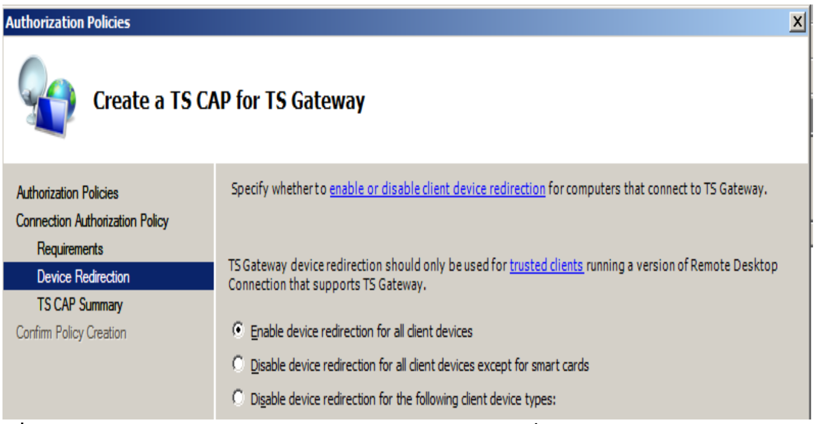


9- Ok



10- Next

11- ត្រូវជ្រើសរើសយក Enable Device Redirection for All Client Device



12- ចុចលើ close ដើម្បីបញ្ចាក់បន្ថែមលើ Policy ដែលទើបបានបង្កើត

១៥-៥-៣- Configuring Resource Authorization Policies

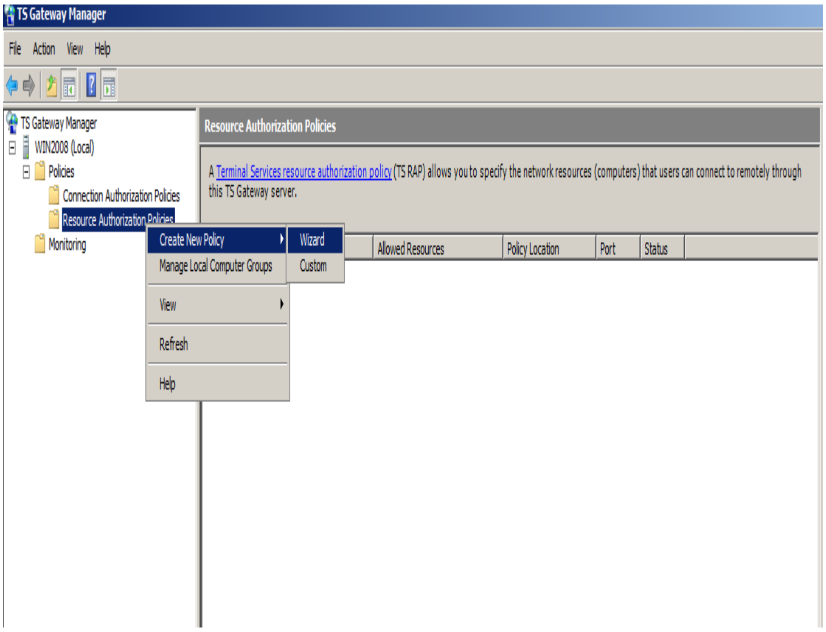
CAPs មានតួនាទីយ៉ាងកំណត់បំផុត។ គេបង្កើតវាសម្រាប់អនុញ្ញាតឱ្យ Access មកកាន់ TS Gateway។ ដើម្បីប្រើប្រាស់ resources នៅខាងក្រោយ gateway Resources ទាំងនោះត្រូវស្ថិតនៅក្នុងតារាងរបស់ RAPs។ នៅក្នុងឧទាហរណ៍នេះយើងនិង configure ចំពោះ Local resources group ដោយរួមមានទាំង Terminal server ដែលនៅក្នុងករណីនេះវាមានឈ្មោះថា WIN2008 ហើយបន្ទាប់មកអនុញ្ញាតឱ្យសមាជិកនៃ Domain Users group អាចភ្ជាប់មកកាន់វា។

1- ប្រើ Active Directory Users and កុំព្យូទ័រs ដោយបង្កើត កុំព្យូទ័រ Group ថ្មីមានឈ្មោះថា TS Servers ហើយបន្ទាប់មក Add WIN2008 ជាសមាជិករបស់ក្រុមនោះ

2- Start=>Administrative Tools=>Terminal Services=>TS Gateway Manager

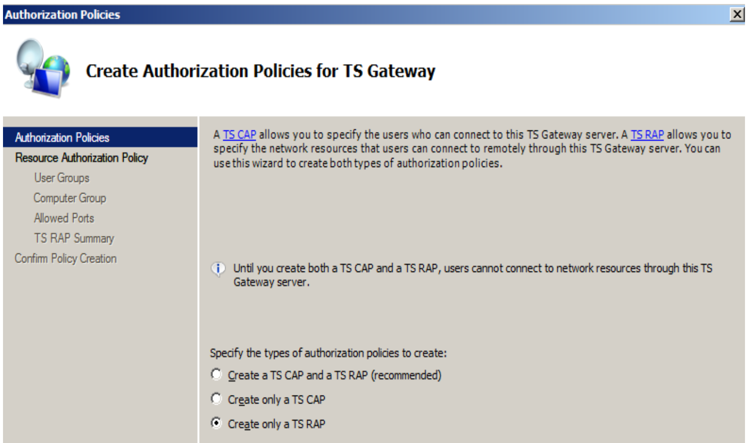
3- ពង្រីក Node ដើម្បីរក TSG Server

4- ពង្រីក Policy folder ហើយ Select លើ Resources Authorization Policies



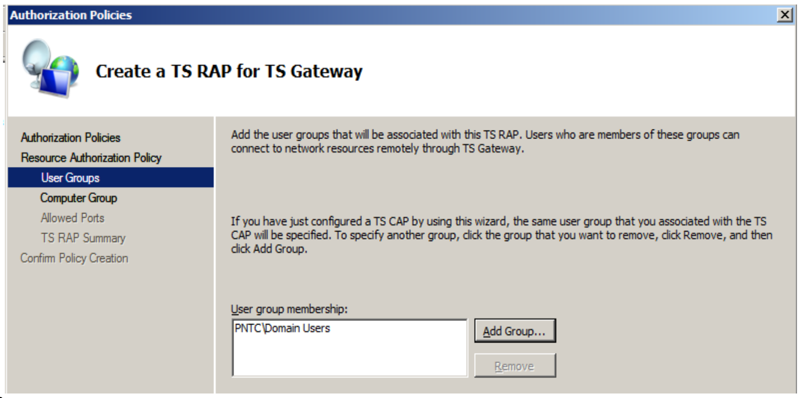
5- ជ្រើសរើសយក Create new Policy=>Wizard

6- ជ្រើសរើសយក Create Only a TS RAP ហើយបន្ទាប់មកចុចលើ Next

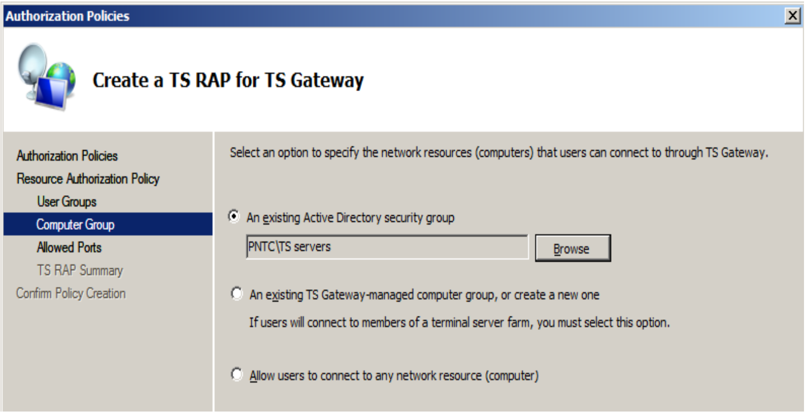


7- វាយបញ្ចូលឈ្មោះរបស់ Policy Name ជា **WIN2K8TS Access** ហើយបន្ទាប់មកចុចលើ Next

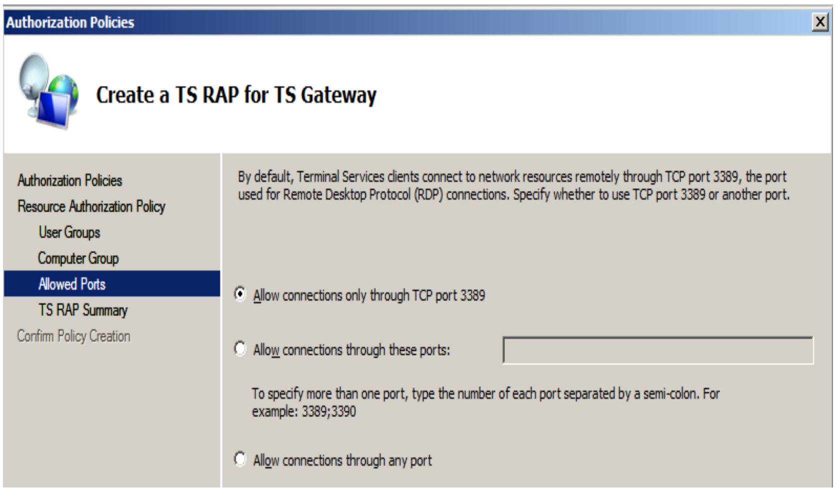
8- ចុចលើ Add Group ដើម្បីស្វែងរក **Domain Users** ហើយបន្ទាប់មកចុចលើ Ok



9- នៅលើ កុំព្យូទ័រ Group Screen ស្វែងរក Group មានឈ្មោះថា **TS Servers**



10- ចុចលើ Next លើ Allowed Port Screen



11- ចុចលើ Finish

១៥-៥-៤- ការភ្ជាប់មក Terminal Server ដោយប្រើ Client តាមរយៈ TS Gateway

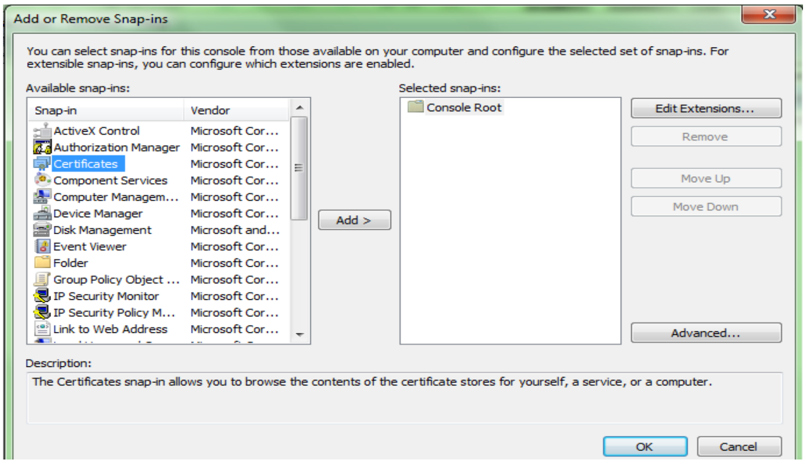
1- Logon មកកាន់ server

2- អនុវត្តតាមជំហានដែលត្រូវការក្នុងករណីដែលអ្នកប្រើ Self-signed certificate ។

3- Copy root certificate នៅលើ Server ទៅដាក់ក្នុង Workstation ។ ឧបមាថាអ្នក Copy វាដាក់ក្នុង C:\MyCertificates

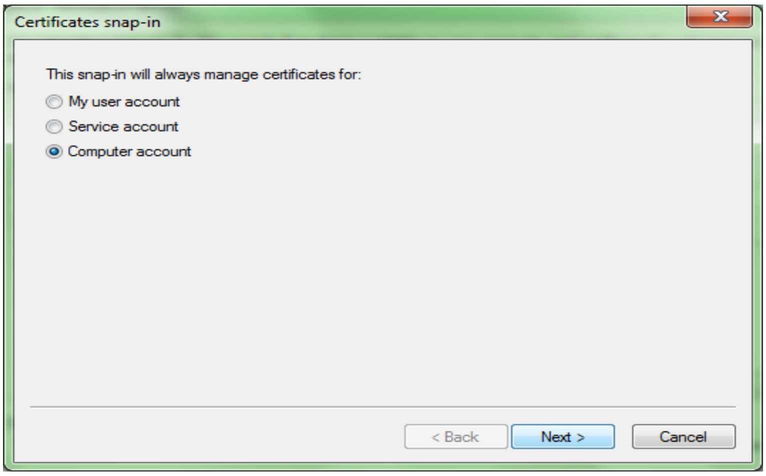
4- Start=>Type MMC

5- ជ្រើសរើសយក File=>Add/Remove Snap-in

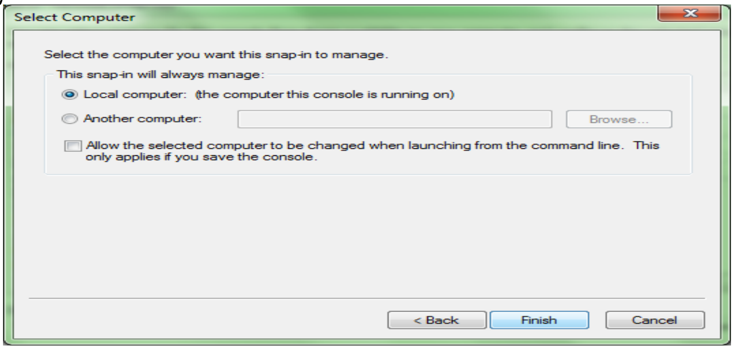


6- ចុចលើ Add

7- Select លើ កុំព្យូទ័រ Account ហើយ Next



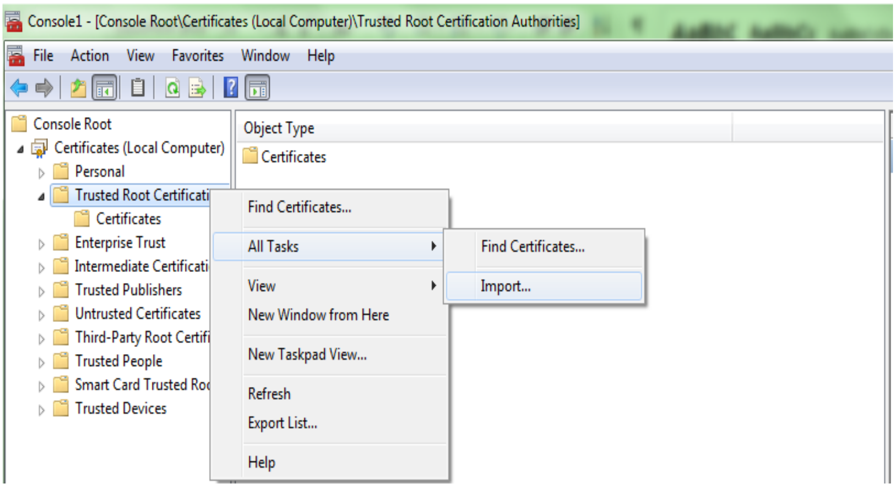
8- Select Local កុំព្យូទ័រ and then Next



9- Finish

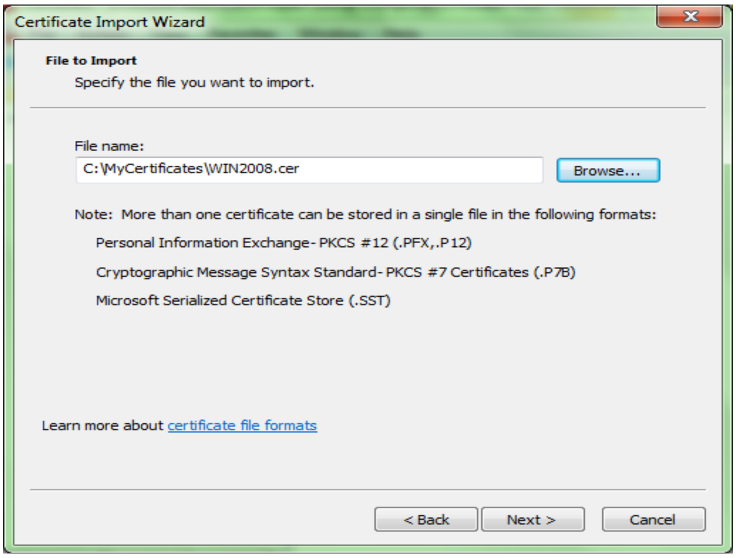
10- ពង្រីក Certificates Node

11- ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Trutsted root certification Authorizaties =>All Task=>Import

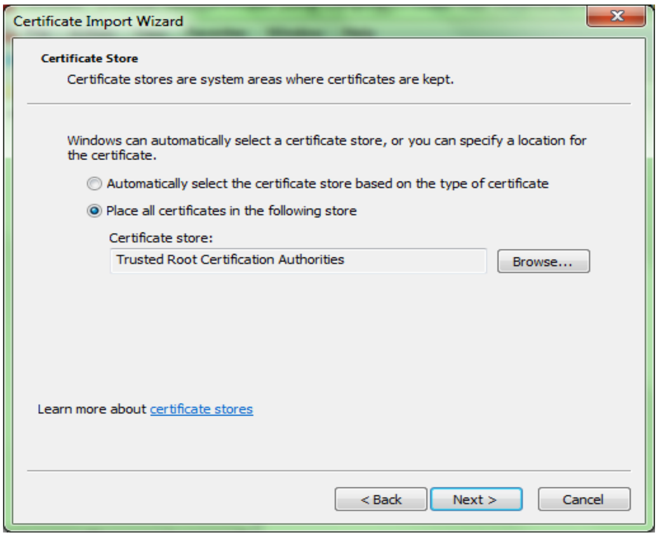


12- ចុចលើ Next

13- Browse រក File ដែលបាន Copy ពី Server



14- ចុចលើNext



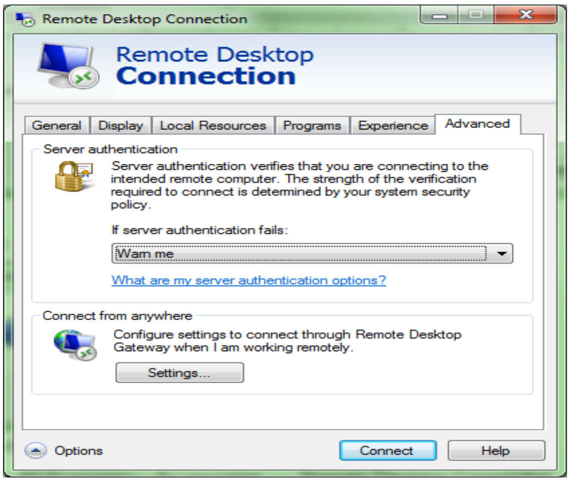
15- ចុចលើNext

16- ចុចលើFinish

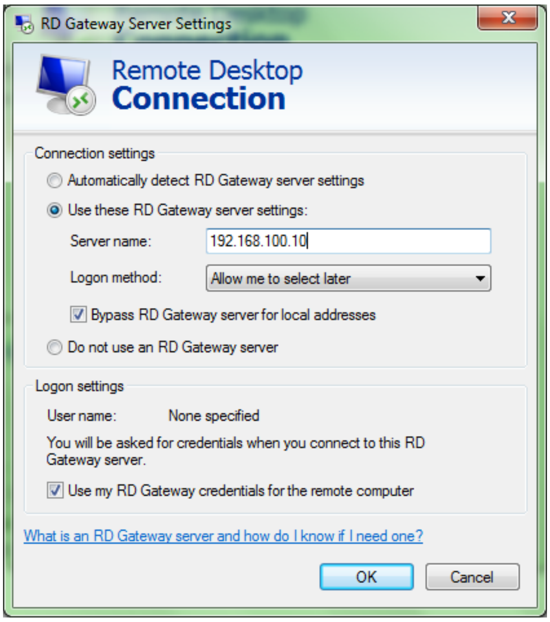
17- Close MMC

18- Start=>All Programs=>Accessories => Remote Desktop Connection

19- ចុចលើ Options



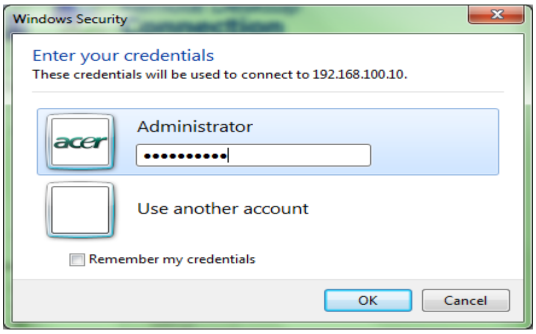
20- វាយបញ្ចូលឈ្មោះ TS Gateway Server ឬ IP address



21- ចុចលើOk

22- ចុចលើ Connect

23- វាយបញ្ចូល Password



24- ចុចលើOk

១៥-៦- Terminal Services Remote Programs

ចំណុចសំខាន់ៗដែលបានភ្ជាប់មកជាមួយ Terminal Services គឺវាបានអនុញ្ញាតប្រើប្រាស់ Desktop ពីរព្រមគ្នាគឺមួយជា Local Desktop និងមួយទៀតគឺ Remote Desktop ដែលបានមកពី Termin-al Server ។

Terminal Service Remote Programs ត្រូវបានប្រើប្រាស់សម្រាប់អនុញ្ញាតឱ្យអ្នកប្រើប្រាស់អាច Access applications ពីចម្ងាយតាមរយៈ Terminal Service ដូចជា Local Applications ដែរ។

អ្នកអាច Access Applications តាមវិធីសាស្ត្រដូចខាងក្រោមគឺ

- តាមរយៈ Remote Desktop Protocol (.RDP) file ឬ
- តាមរយៈនៃការបន្ថែម Applications ដោយផ្ទាល់នៅលើ Start Menu របស់ Users ដោយប្រើ MSI (Windows Installer) file

File MSI មានទំនាក់ទំនងជាមួយ Remote Program។ ឧទាហរណ៍ បើអ្នកចង់ឱ្យ Users ប្រើប្រាស់ Microsoft Office តាមរយៈ Terminal Services និង Remote Program អ្នកប្រើ Word(.doc) file ជាមួយ Remote Program នៅពេលអ្នកចុចពីរដងផ្ទួនគ្នាលើ Word file វានិងដំណើរការ Terminal service session ជាស្វ័យប្រវត្តិហើយចាប់ផ្តើម Remote Program ជាចុងក្រោយអ្នកអាច Setup Terminal Services Web Access ហើយអាច Access វាតាមរយៈ Web site ។

Remote Program គឺល្អសម្រាប់អ្នកប្រើប្រាស់ពីចម្ងាយ ឬ Roaming local Users ។ បើអ្នកមិនចង់ឱ្យ Application មួយដំណើរការលើ workstations ច្រើន អ្នកគ្រាន់តែបង្កើត Host មួយសម្រាប់ដំណើរការ Application លើវាហើយឱ្យUsers ដំណើរការ applications ចេញពីវាបានគ្រប់ទីកន្លែងទាំងអស់បាន។

តម្រូវការចាំបាច់

ដើម្បីប្រើប្រាស់ TS Remote Program បាន Client នីមួយៗត្រូវបំពេញតម្រូវការ

- Microsoft Windows Server 2008
- Microsoft Windows Vista
- Microsoft Windows Server 2003 with Service Pack 1 or later
- Microsoft Windows XP with Service Pack 2

Installing Applications

Windows Server 2008 រួមមាន Applications ដែលមានស្រាប់មួយចំនួនដូចជា Paint និង Notepad ប៉ុន្តែអ្នកប្រហែលជាមិនចង់ Setup វាជា Remote Program នោះទេ។ អ្នកប្រហែលជាត្រូវការ Applications ពិតប្រាកដដូចជា

- Microsoft Office

ដែលត្រូវដំឡើងលើ Terminal Server ហើយអនុញ្ញាតិឱ្យ Users អាចប្រើប្រាស់បានជា Remote ។

ការ Install application លើ Terminal Server វាក៏ដូចជាការ Install វាលើ Workstations នោះ ដែរ។ Terminal service មានទំនាក់ទំនងជាមួយ User Registry Key និង file ដែលត្រូវ load ក្នុង User Profile ។

នៅពេលដែលអ្នកត្រូវការ Install Applications លើ Terminal Server ជាដំបូងអ្នកត្រូវប្តូរ Server Mode ពី Execute Mode មកជា Install mode។ នៅពេល logon មកកាន់ Terminal server អ្នកអាចដំណើរការវាក្នុង Mode មួយនៃ mode ទាំងពីរ។ អ្នកនិងត្រូវដំណើរការវាក្នុង Execute Mode នៅពេលអ្នកត្រូវការដំណើរ Applications។ Terminal service monitor និងប្តូរ Mode ពី HKEY_CURRENT_USER registry មកជា Capture ដោយ Applications Installer ។

ការប្តូរ Server Mode ពី Execute mode មក Install mode

Change user /install

ការប្តូរពី Install mode មកជា Execute mode វិញ

Change user /execute

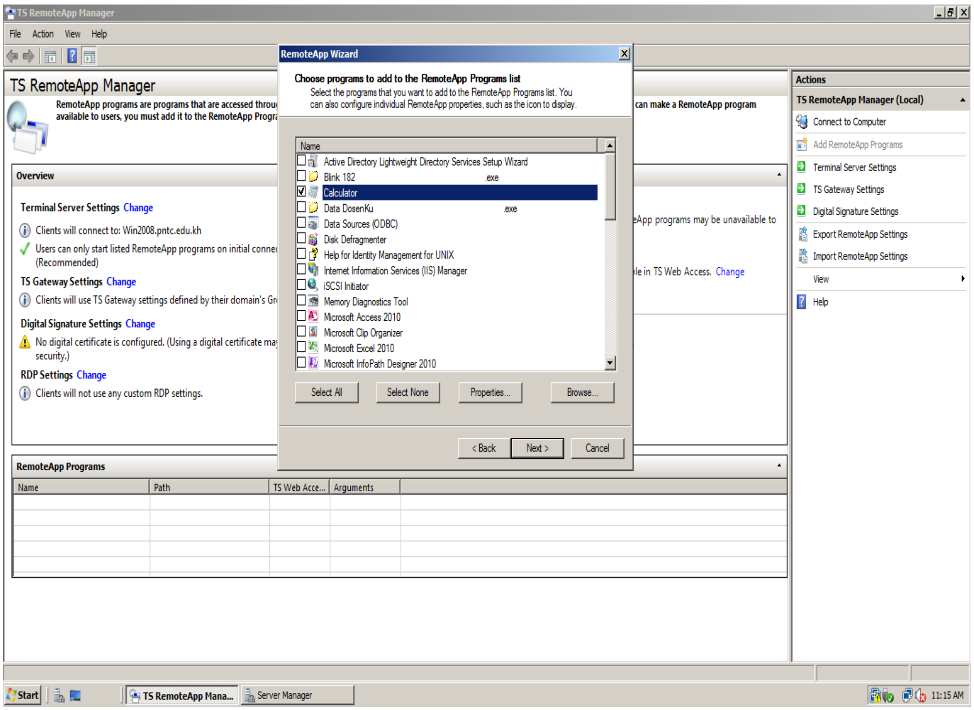
ចំណាំ

ការប្តូរពី Install mode និងត្រឡប់មកជា Execute mode វិញមិនត្រូវការនោះទេក្នុងករណីដែល Installer គឺជា MSI package ។

លំហាត់អនុវត្ត Configuring a Remote Program

នៅក្នុងលំហាត់នេះ យើងនិងបង្កើត Windows Calculator ជា Remote Program ។ យើងត្រូវបង្កើត RDP file និង MSI file ដែលយើងអាចចែកចាយឱ្យ Users ដែលនិងAccess remote program

1- Logon មកកាន់ server ដែលកំពុងដំណើរការ Terminal services
2- Start=>Run ហើយវាយបញ្ចូល **remoteprograms.msc** ហើយOK
3- ចុចលើ Add RemoteApps ពី Action list ដើម្បីដំណើរការ RemoteApp Wizard
4- ចុចលើ next
5- ជ្រើសរើសយក Calculator ហើយ next



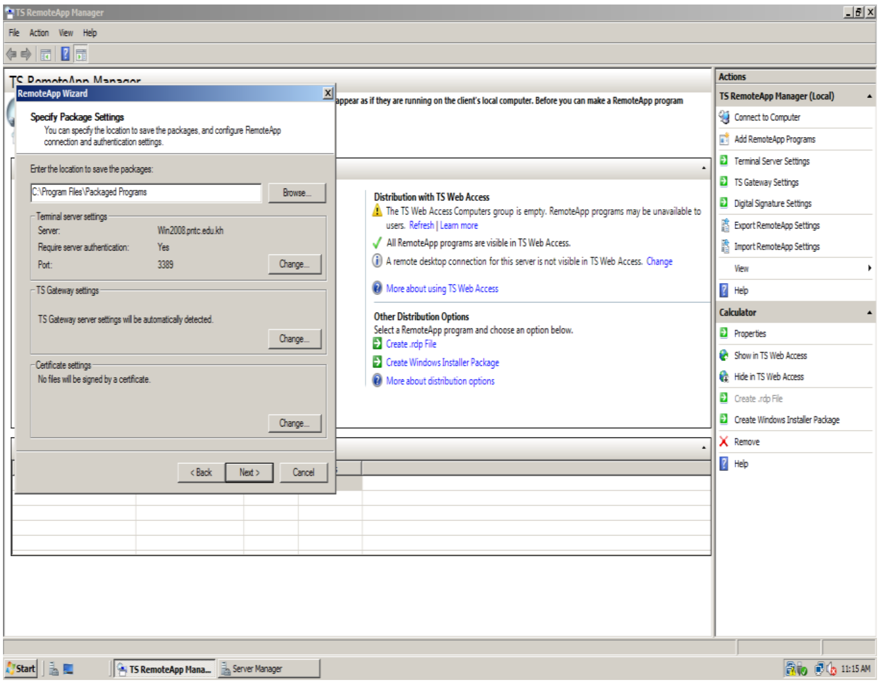
6- ចុចលើ Finish

7- Select លើ Calculator ពី RemoteApps

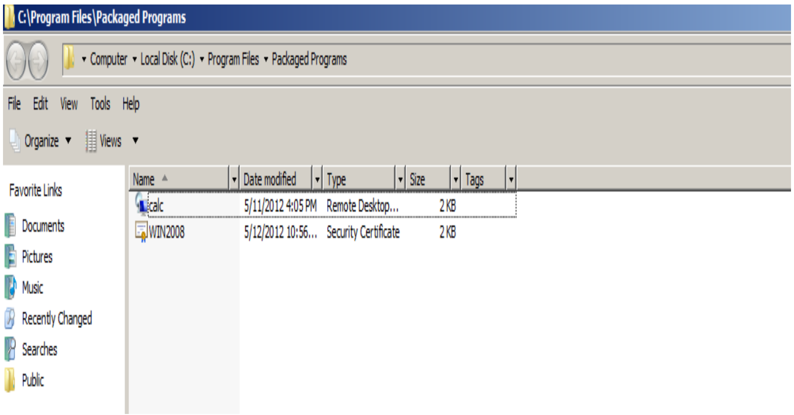
8- ពី Remote Calculators Action Pane Select លើ Create .RDP file

9- ចុចលើ Next

10- ត្រូវចាំពីទីតាំងនៃ RDP file ហើយចុចលើ Next



11- Finish



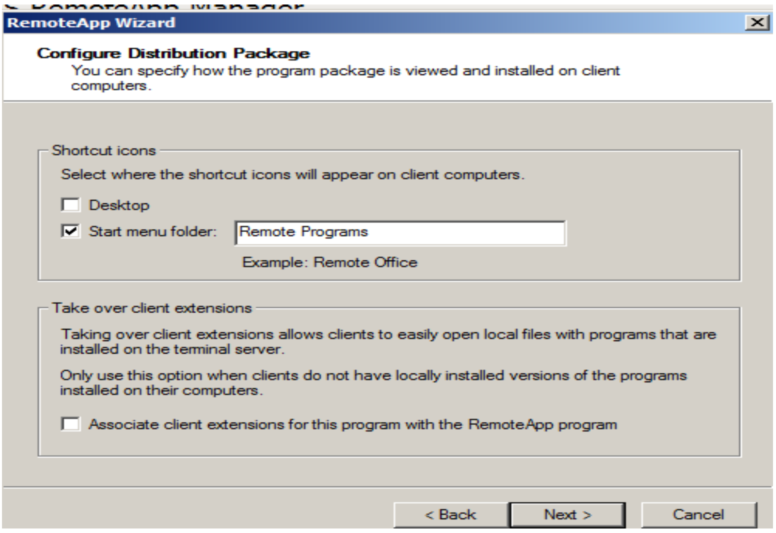
12- Close Windows

13- Select Calcualor ពី remote Program List

14- ក្នុង Remote Calculator Action Menu Select Create Windows Installer

15- ចុចលើNext

16- ចុចលើNext

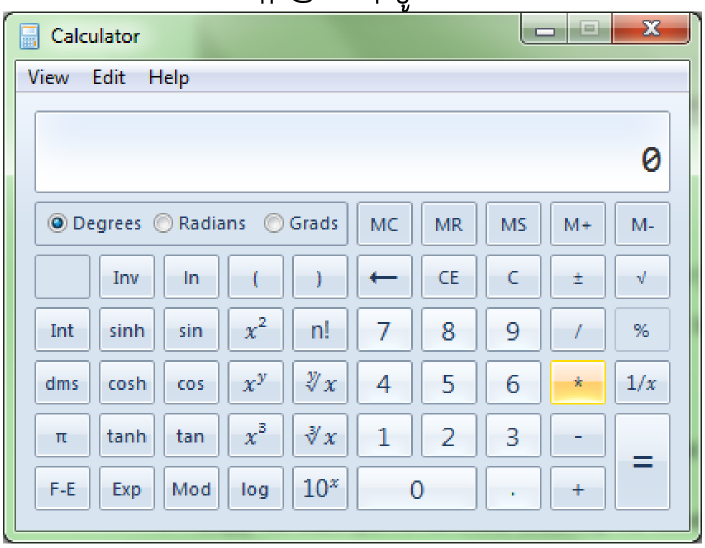


17- Finish

ដើម្បី Access remote program អ្នកអាច Copy calc.rdp ឬ Run calc.rap.msi file លើ Client ។ បើអ្នកInstall Calculator Link ដោយប្រើ .rap.msi file នោះ Icon ត្រូវបានបង្កើតនៅលើ Desktop និង Start Menu ដែលនិងត្រូវប្រើសម្រាប់ដំណើរការវា។

នេះគឺជារបៀបដំណើរការ Calculator ដោយប្រើ .rdp file:

1- Copy file calc.rpd ទៅដាក់លើ Desktop នៃ Windows Vista
2- ចុចពីរដងផ្ទួនគ្នាលើ calc.rdp file
3- វាយបញ្ចូលលេខសំងាត់ដើម្បី Logon មកកាន់ Terminal Server
4- ជ្រើសរើសយក Device នៅលើ client ដែលអ្នកចង់ដំណើរការ Remote Program Sesion and Next
5- Windows calculator Application និងបង្ហាញលើ កុំព្យូទ័រ client



១៥-៧- Terminal Server Web Access

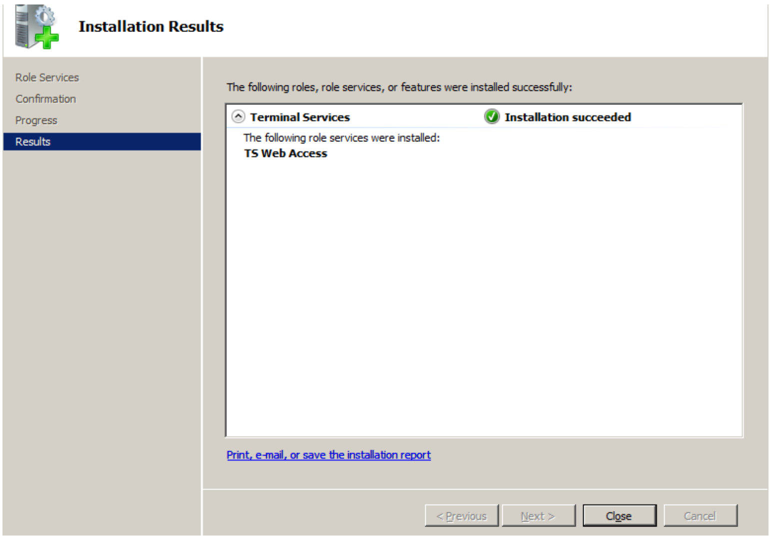
File .rdp និង.rap.msi ត្រូវបានប្រើប្រាស់សម្រាប់បង្ហាញ Icon លើ Desktop របស់ Client ដើម្បី access remote program ។ អ្នកក៏អាច Access វាតាមរយៈ Web site ដោយប្រើ TS Web Access ។

TS Web Access គឺជា Service មួយដែលអាច Install នៅលើ Windows Server 2008 ។

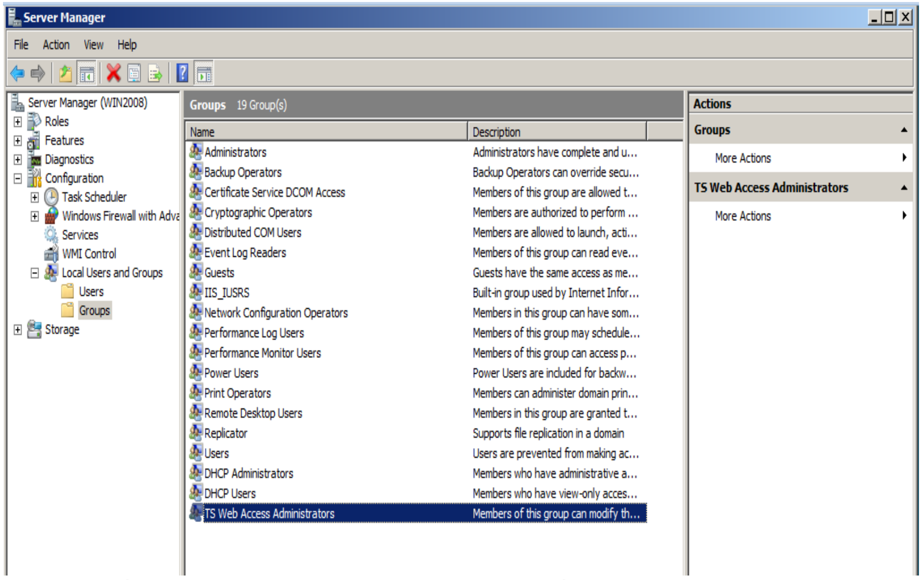
លំហាត់អនុវត្ត Installing and Configuring TS Web Access

1- Logon មកកាន់ Server
2- បើក Server Manager
3- ជ្រើសរើសយក Terminal Services
4- ចុចលើ Add Role Services
5- Select TS Web Access

6- ចុចលើ Next
7- ចុចលើ Next
8- ចុចលើ Install
9- ចុចលើ Close



10- Logon មកកាន់ Server
11- បើក Server Manager
12- ពង្រីក Configuration=>Local Users and Groups=>Group



13- ចុចពីរដងស្ទួនលើ TS Web Access Administrator ហើយ Add WIN2K8TSG ជាសមាជិក

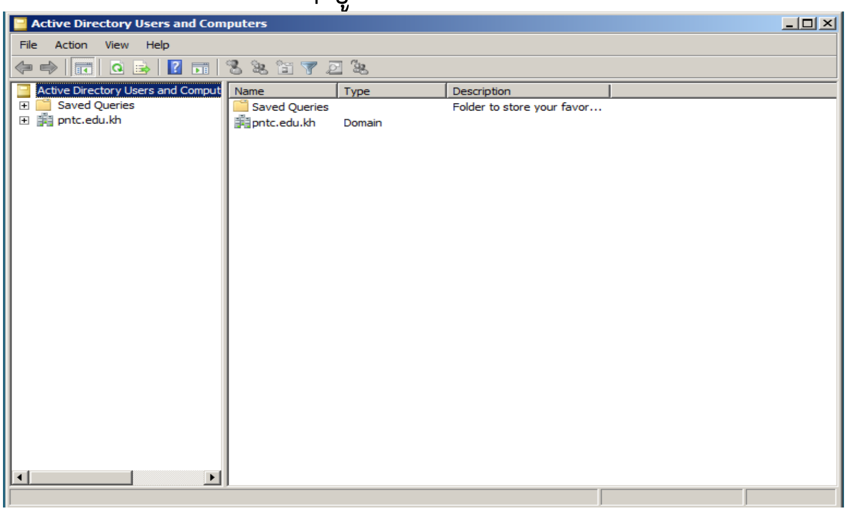
14- ចុចលើOk

15- នៅលើ WIN2K8TSG Share folder ដែលអ្នកទើបតែបានបង្កើត file មានឈ្មោះថា calc.rap.msi ហើយត្រូវកំណត់ឱ្យ Domain Users និង WIN2K8 TSG មានសិទ្ធិត្រឹមតែ Read-Only ប៉ុណ្ណោះ។

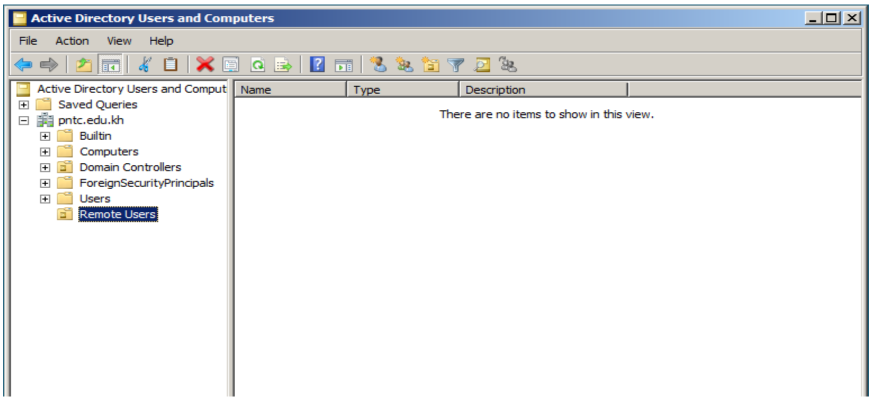
ចំណាំ Windows Server 2008 មិនបាន Install File Server ជា Default នោះទេ។

16- Logon មកកាន់ Domain controller

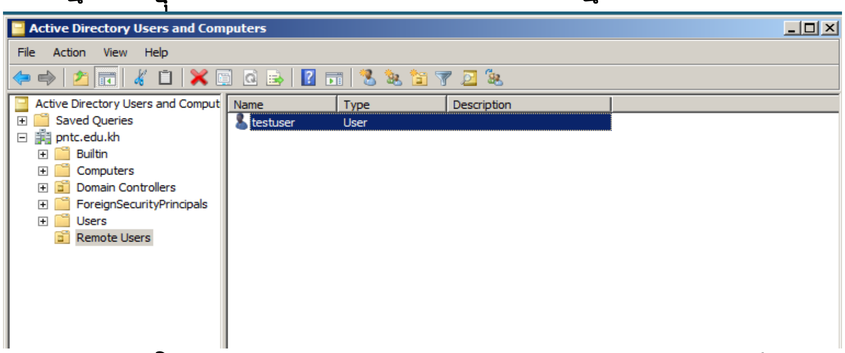
17- បើក Active Directory Users and កុំព្យូទ័រ



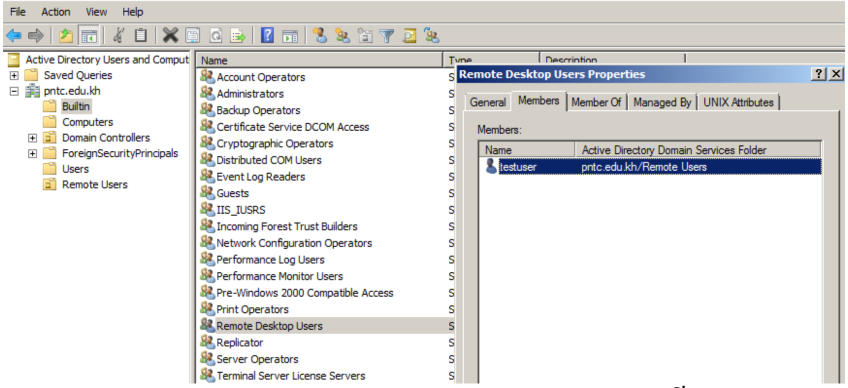
18- បង្កើត Ou ហើយដាក់ឈ្មោះថា **Remote Users**



19- បង្កើត User ធម្មតានៅក្នុង **Remote Users** OU ហើយដាក់ឈ្មោះថា **testuser**



20- Add **testuser** ជាសមាជិករបស់ Remote Desktop User local group នៅលើ WIN2K8STG (អ្នកក៏អាច Add **testuser** ជាសមាជិករបស់ Global Group ហើយបន្ទាប់មក Add Global Group នោះជាសមាជិករបស់ Remote Desktop Users local group នៅលើ WIN2K8STG)



21- ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ **Remote Users** Ou ហើយជ្រើសរើសយក Properties

22- ចុចលើ Group Policy tab

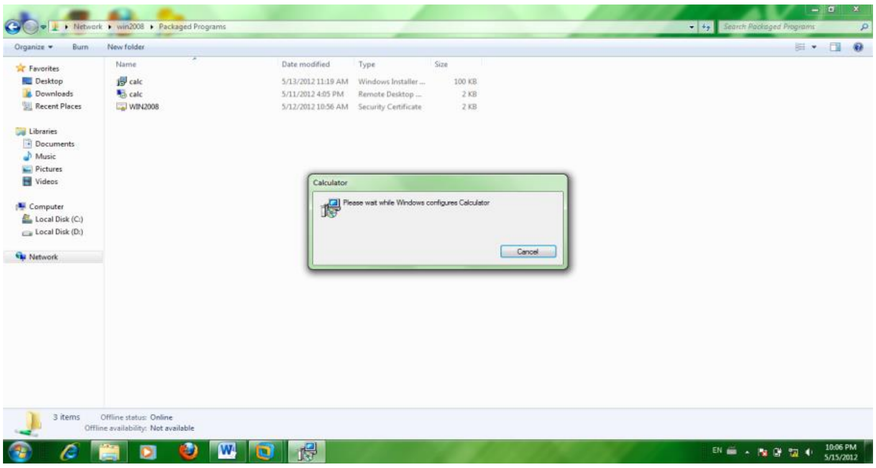
23- ចុចលើ New ដើម្បីបង្កើត GPO ថ្មីហើយដាក់ឈ្មោះថា **Remote Programs** ដូចទៅនិងឈ្មោះរបស់ GPO

24- Select **Remote Programs** GPO ហើយចុចលើ Edit

25- ពង្រីក User Configuration =>Software Settings

26- ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Software Installation ហើយ select New=>Package

27- Select \\WIN2008\PackagedPrograms$\calc.rap.msi



28- Select Published as the Deployment method ហើយចុចលើ OK

29- Close Group Policy Editor Windows

30- បង្កើត OU ថ្មីមានឈ្មោះថា Terminal Servers ហើយយក WIN2K8TS កុំព្យូទ័រ ដាក់ក្នុង OU ថ្មីនេះ
31- ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Terminal Server OU ហើយ Select Properties
32- នៅក្នុង Terminal servers Properties dialog box ចុចលើ Group Policy tab ហើយបន្ទាប់មកចុចលើ Add
33- ចុចលើ All tab បន្ទាប់មកចុចលើ **Remote Programs** ហើយចុចលើ Ok
34- ដោយបាន Select លើ **Remote Programs GPO** ចុចលើ Properties button ហើយបន្ទាប់មកចុចលើ Security tab
35- នៅក្នុង Permission area ផ្តល់សិទ្ធិឱ្យ WIN2K8TS មាន Read ហើយ Apply Group Policy permissions ឱ្យ Remote Programs GPO ហើយបន្ទាប់មកចុចលើ Ok
36- ចុចលើ Ok លើ Terminal Servers Properties dialog box ដើម្បី Save
37- ចំពោះ WIN2K8TS បើក Internet Explorer ហើយវាយ http://WIN2K8TS/ts
38- នៅលើ TS Web Access Web page ចុចលើ Configuration button
39- នៅក្នុង Editor Zone select Populate the Web Part from Active Directory Domain Services ហើយចុចលើ Apply
40- Logon ជាមួយ Windows Vista ជាមួយ testuser
41- បើក Internet Explorer ហើយ វាយ http://win2K8tsg ចូលក្នុង trusted sites
42- http://WIN2KTSG/ts
43- ចំណាំ Calculator icon ក្នុង RemoteApp Program ។ បើអ្នកមិនបានឃើញ Calculator Icon បង្ហាញនៅពេលអ្នកភ្ជាប់មកកាន់ TS Web Access វាអាចបណ្តាលមកពី Group Policy មិនបាន update ។ ព្យាយាមដោយប្រើបញ្ជា gpupdate ហើយបន្ទាប់មកត្រឡប់មក TS Web Access វិញ
44- ចុចលើ Calculator Icon
45- អ្នកនឹងទទួលបាន Trust warning មួយ។
46- វាយបញ្ចូលលេខសំងាត់ដើម្បី Logon មកកាន់ Server (WIN2K8TSG)
47- ចុចលើ Yes

១៥-៨- ទីតាំងកំណត់កម្មវិធីនិងសមត្ថភាពសម្តែង

នៅក្នុងមជ្ឍដ្ឋានផលិតកម្មអ្នកនឹងគ្រាន់តែមានTerminal Server ដើម្បី Host applications។ អ្នកត្រូវសម្រេចចិត្តថាតើ Server មួយណានិងត្រូវ Host applications ដោយពឹងផ្អែកលើលក្ខខណ្ឌវិនិច្ឆ័យពីរគឺ

- ចំនួន Users ដែលកំពុង Access applications ជំណាលគ្នាទាក់ទងជាមួយ Resources របស់ Server
- និងសមត្ថភាពរបស់ Applications ដែលមានត្រូវនិង Applications ផ្សេងៗទៀត

ឧទាហរណ៍ Application មានភាពអាស្រ័យគ្នាទៅនិង Version ដែលបានកំណត់ដូចជា Database client និង runtime engine ដូចជា Java runtime របស់ Sun អ្នកត្រូវការ Install applications នៅលើ Terminal Server ដាច់ដោយឡែកពី Applications ផ្សេងដែលមានភាពអាស្រ័យគ្នាដូចគ្នាដើម្បីជៀសវាងទំនាស់វិបត្តិកើតឡើង។

អ្នកត្រូវតែលើកកំពស់នូវសមត្ថភាព Tools ដែលមានក្នុង Windows server 2008 ដោយបង្កើត baseline សម្រាប់ terminal server ហើយកំណត់នូវសមត្ថភាពឱ្យ Applications ដែលបាន Install និង

បានប្រើប្រាស់។ CPU និង Memory utilization នៃ Applications អាស្រ័យលើ Application និងតួនាទីដែលកំពុងប្រើ ប្រាស់។

សំណួរត្រួតពិនិត្យ

១-តើ Terminal Service ត្រូវបានគេប្រើសម្រាប់ធ្វើអ្វី?

២-ចូរបង្ហាញពីបញ្ជាដែលត្រូវបានប្រើសម្រាប់បើក Remote Desktop ដែលមានទទឹងស្មើនិង១០២៤និងកំពស់ស្មើនិង២៨០។

៣-តើ Single sign-on គឺជាអ្វី?

៤-តើបញ្ជា gpupdate ប្រើសម្រាប់ធ្វើអ្វី?

៥-តើអ្វីទៅជា Terminal Service Gateway?

ជំពូកទី១៦

Windows DNS, BitLocker Driver Encryption, and Itanium Support

Windows Server 2008 បានបញ្ចូលនូវលក្ខណៈជាច្រើនរបស់ Windows Domain Name System(DNS)។ Active Directoryក៏ពឹងលើ DNS បើសិនជាយើងសំឡឹងមើលការផ្លាស់ប្ដូររបស់ Active Directory យើងអាចគិតពីលក្ខណៈស្រដៀងគ្នារបស់ Windows DNS DNS សម្រាប់ Windows Server 2008 អាចគាំទ្រ Background Zoon Loading, IPv6, GlobalName Zones, Read Only DNS និង លក្ខណៈសម្រាប់ DNS Clients ហៅថា Link-Local multicast name resolution (LLMNR) ការបន្ថែមដ៏ល្អទៅលើ Windows Server 2008 គឺការបញ្ចូលនូវ BitLooker Driver Encryption សម្រាប់បន្ថែមនូវ Security ឱ្យ Hardware និង Software ។ វាអាចជួយបង្ការ រឺ ការពារក្នុងការ Access ទៅ Server ដោយគ្មានការអនុញ្ញាត ទោះបីជា Physical Access ប្រើមធ្យោបាយដើម្បីទទួលបានActual drive ក៏ដោយ ។

សកម្មភាពពាណិជកម្មកុំព្យូទ័រត្រូវបានកើនឡើង ដូច្នេះវាតម្រូវការចាំបាច់នូវ 64-bit ។ Windows Server 2008 សម្រាប់ Itanium-base System គឺជា Version ខ្ពស់បំផុតរបស់ Windows Sever 2008 ដែលត្រូវបានបង្កើតឡើងទៅជា platform សម្រាប់application ដែលត្រូវការសម្រាប់ Local resource ដែលមានថាមពលខ្លាំង (processing power, memory ។ល។) មានន័យថាមាន load-balancing ឆ្លងកាត់ multiple server ។

១៦-១- Domain Name System

DNS គឺជាផ្នែករៀបចំឈ្មោះតាមលំដាប់នៃ TCP/IP។ វាជាឈ្មោះមួយផ្នែកដ៏សំខាន់ក្នុងការប្រើប្រាស់សម្រាប់ពារិបសាយរកតាម Internet និង នៅក្នុង Active Directory ។ វាក៏ជាតួនាទីដំបូងនិងល្អជាងគេក្នុងការបកប្រែឈ្មោះ Host រឺ Domain ឱ្យត្រូវជាមួយ IP Address និងផ្ទុយមកវិញ។ Active Directory ប្រើ DNS ដើម្បីទាញយក Record Type ហៅថា SRV Record ហើយស្វែងរក Key Active Directory Infrastructures ដូចជា Domain controller ។

នៅក្នុងជំពូកទី៤ យើងបានសិក្សារួចហើយនូវមូលដ្ឋានគ្រឹះនៃ DNS និង Active Directory លក្ខណៈសំខាន់ៗរបស់ DNS ដែលត្រូវបានអនុវត្តលើ Windows Server 2008 និងត្រូវសិក្សានៅក្នុងជំពូកនេះដែលបានរៀបរាប់ដូចខាងក្រោម :

- **Active Directory Domain Services Support** Windows DNS គឺជា DNS Server ក្រុមហ៊ុន Microsoft ណែនាំឱ្យប្រើសម្រាប់ភ្ជាប់ទំនាក់ទំនងទៅនិង Active Directory Domain Services (AD DS)។ ទោះបីជាបច្ចេកវិទ្យាជំនាន់ទីពារបស់ DNS Solution ដែលគាំទ្រប្រភេទនៃ SRV record សម្រាប់ Active Directory ក៏ដោយក៏នៅតែមិនអាចទទួលបាននូវផលប្រយោជន៍ពីវាក្នុងការបញ្ចូលនូវលក្ខណៈដូចជា លទ្ធភាពក្នុងការផ្ទុក DNS data ទៅក្នុង AD Domain រឺ application partition ។ Windows DNS ធ្វើការភ្ជាប់ទំនាក់ទំនងទៅនឹងលទ្ធភាពក្នុងការប្រតិបត្តិនូវ Secure Dynamic update របស់ DNS record ដោយ Clients ចូលរួមក្នុង Domain។ ចំពោះលក្ខណៈនេះគឺសម្រាប់ផ្ទុកនូវការកែតម្រូវនូវ DNS ដែលមាននៅក្នុង Hostname

- **Stub zones** គឺផ្ទុកតែ Partial copy របស់ Zone ដែលផ្ទុកនូវ Resource ដែលត្រូវការដោយ Authoritative DNS Server សម្រាប់ Zone ។ ការកើនឡើង DNS resolution ប៉ះពាល់ដល់ការរក្សាទុក Records របស់ authoritative DNS server សម្រាប់ child zones ។
- **Integration with other MS networking service** Windows DNS supports integration with service ដូចជា Windows Internet Name Service (WINS) និង Dynamic Host Configuration Protocol (DHCP) ។
- **Better administration tool** Windows Server 2008 បានមកជាមួយនូវការប្រែនូវ Interface ដើម្បីការគ្រប់គ្រងឱ្យមានភាពងាយស្រួលនិងបានបន្ថែមនូវ Wizard សម្រាប់ជួយសម្រួលដល់ Administration ។
- **Dynamic update support** Windows DNS គាំទ្រ dynamic update ដែលកំណត់ដោយ RCF 2136 ។ នេះជាលក្ខណៈដ៏សំខាន់បើសិនយើងប្រើ DHCP ក្នុងបរិបទនេះនិងតម្រូវការផ្ទុក DNS Records ដែលមានថ្មីៗដោយគ្មានការអន្តរាគមន៍ពីអ្នកគ្រប់គ្រងឡើយ។
- **Incremental zone transfers** ក្នុងការចម្លងយ៉ាងត្រឹមត្រូវគាំទ្រ Windows DNS បានធ្វើការបង្កើននូវការបំប្លែង Zone ទៅជា DNS Server ដូចនេះហើយទើបមានតែ Record ដែលត្រូវបានកែប្រែក្នុងការទទួលយកនូវការចម្លងទៅ Server ។
- **Conditional forwarder** យើងអាចធ្វើការ Forward នូវរាល់ Address ណាដែលមិនបានឆ្លើយតបទៅកាន់ DNS Server។ Conditional Forwarder អនុញ្ញាតឱ្យ Name Resolution ច្បាស់លាស់សម្រាប់ Domain ពិសេសទៅ DNS Serverច្បាស់លាស់ ។
  ឧទាហរណ៍:អ្នកអាចបង្កើតនូវ Conditional Forwarder សម្រាប់ Forward នៅការប៉ុនប៉ងស្វែងរក Hosts ក្នុង Microsoft.com Domain ទៅ DNS Server ច្បាស់លាស់ជំនួសឱ្យ Normal forwarder Server របស់អ្នក ។

១៦-១-១- Background Zone Loading

Windows Server 2008 DNS បញ្ចូលនូវចំនួននៃការងារដ៏ល្អមួយចំនួនព្រមទាំងបានបញ្ចូលនូវ Background zone loading។ លក្ខណទាំងនេះអនុញ្ញាតឱ្យ DNS server សម្រាប់ការឆ្លើយតបដំបូងទៅ Clients ដោយផ្ទាល់បន្ទាប់ពីចាប់ផ្តើមដំណើរការសារជាថ្មី ។ កាលពីមុន Server ត្រូវរងចាំធ្វើការទាញយក DNS data ពី AD DS។ ប៉ុន្តែទោះបីជាការឆ្លើយតបក្នុងការស្នើរកព័ត៌មាន Host ដែលយើងមិនទាន់បានយកវាពី AD DS នៅឡើយក៏វានៅតែមានការឆ្លើយតបក្នុងការបង្កើតសម្រាប់ការរក្សាទុកនូវព័ត៌មានជាច្រើនរបស់ Host នៅក្នុង File ។
ឧទាហរណ៍: ការស្នើនូវទំហំនៃ Internet ។

ពេលដែល Windows Server 2008 DNS ចាប់ផ្តើមដំណើរការឡើង ដំណើរការរបស់វានិងមានទម្រង់ដូចបានបង្ហាញខាងក្រោម :

1. កំណត់ឈ្មោះឱ្យដើម្បីបញ្ចូល Zone ទាំងអស់ ។
2. បញ្ចូល Root hints ។
3. បញ្ចូលនូវ file-backed zone(រាល់ព័ត៌មានរបស់ zone មិនត្រូវបានផ្ទុកក្នុង AD DS)
4. ចាប់ផ្តើមឆ្លើយតបដោយផ្ទាល់ទៅ clients requests ។
5. ធ្វើការពង្រីកនូវ Threads បញ្ចូល zone ទៅផ្ទុកក្នុង AD DS ។

ជំហានទី៤(ការឆ្លើយតបទៅ Clients) របស់ Windows Sever DNS Systems ដែលបានធ្វើការពឹងពាក់លើជំហានទី៥(ការទទួលរាល់ពត៌មានរបស់ zone ពី AD DS) ដើម្បីបំពេញការងារ។ ជាធម្មតាវាពឹងផ្អែកទៅលើចំនួននៃ Record របស់ DNS hosts ដែលវាមានដំណើរការយ៉ាងវែង ហើយមានការប៉ះពាល់ទៅលើ DNS server រហូតដល់វាមានការស្នើរកទិន្នន័យ។ ការរៀបចំដ៏ធំនិងត្រូវធ្វើការកត់សំគាល់យ៉ាងសំខាន់ក្នុងការប្រតិបត្តិដែលនាំមកផលប្រយោជន៍ជាមួយនិងស្ថាបត្យកម្មថ្មី ។

១៦-១-២- IPv6 Support

ទោះបីជា IPV6 មានការពេញនិយមតិចតួចនាពេលបច្ចុប្បន្នក៏ដោយ ប៉ុន្តែប្រសិនបើយើងមិនផ្លាស់ប្តូរទៅប្រើប្រាស់ IPv6 សម្រាប់អនាគតនោះទេ ការប្រើប្រាស់ IP Addresses និងត្រូវអស់។ IPv6 មាន128bits ចំណែកឯ IPv4 មានតែ 32bits ប៉ុណ្ណោះ។ ដើម្បីទទួលបានផលប្រយោជន៍ពីការប្រើប្រាស់ IPv6 យើងចាំបាច់ត្រូវមានឧបករណ៍សម្រាប់ IPv6-capable Networking ដែលដំណើរការតាមប្រព័ន្ធប្រតិបត្តិការមានដូចជា Windows Sever 2008 on sever side, Windows Vista ។

Microsoft បានដាក់បញ្ចូល IPv6 ទៅក្នុង Windows Server 2008 DNS ចាប់តាំងពីការប្រែប្រួលនូវគ្រប់ហេដ្ឋារចនាសម្ព័ន្ធដែលមានទំនាក់ទំនងជាមួយTCP/IP មក។ Wind ows Sever 2008 DNS អនុញ្ញាតឱ្យ DNS entries បញ្ជាក់ពី IPv4 រឺ IPv6 address។ លើសពីនេះទៅទៀតវាមាន Command-line tools សម្រាប់គ្រប់គ្រង DNSនោះគឺ DNSCMD .EXE ដែលអាចប្រើបានជាមួយ IPv6ផងដែរ ។ DNS មាន ip6.arpa domain namespace សម្រាប់ត្រលប់ name resolution របស់ IPv6 addresses ។

កំណត់សំគាល់

អ្នកត្រូវ Upgrade DNS clients របស់អ្នក ដើម្បីស្គាល់ IPv6 ព្រោះ name resolution រារាំង Severរបស់ Windows server 2008ឱ្យបង្ហាញនូវព័ត៌មានរបស់ IPv4(A)រឺIPv6 (AAAA)។ ប្រសិនបើ DNS client របស់អ្នកទទួលបានឆ្លើយតបរបស់ IPv6 address ពី DNS Server នោះវានឹងអាចបណ្តាលឱ្យមានបញ្ហាមួយចំនួន ។

១៦-១-៣- GlobalNames Zone

ប្រសិនបើអ្នកប្រើនូវប្រតិបត្តិការ WINS,អ្នកនឹងមានការចាប់អារម្មណ៍លើលក្ខណ:ពិសេសរបស់ Global - Names Zone ។ DNS ផ្តល់នូវ name resolution និង WINS ផ្តល់នូវ name មួយធ្វើឱ្យត្រូវគ្នាជាមួយ IP address។ WINS គឺអាស្រ័យលើ NetBIOS នៅលើ TCP/IP។ Windows Server 2008 អនុញ្ញាតឱ្យអ្នកបង្កើត Zone ថ្មីមួយដែលមានឈ្មោះថា Golbal-Names Zone។ Scope របស់ Zone នេះគឺជា forest level ដែលធ្វើឱ្យប្រាកដថា names ដែលឆ្លងកាត់ forest ទាំងមូលគឺមានតែមួយ ។

១៦-១-៣-១- Read-Only DNS Zone

ក្នុងជំពូកទី៤អ្នកបានអានពីលក្ខណ:ពិសេសថ្មីរបស់ Active Directory ក្នុង Windows Server 2008 ដែល Role ថ្មីនោះ ត្រូវបានគេហៅថា Read-Only Domain Controller (RODC)។ Windows Sever 2008 DNS មាន Zone ថ្មីមួយមានឈ្មោះថា Primary Read-Only Zone។ Zone នេះផ្តល់នូវ read-only copy នៃព័ត៌មានរបស់ DNS Zone ដើម្បីទាយយក RODCs។ RODCs ចម្លង DNS application partition និងរក្សាទុកក្នុង

read-only zone។ Administrators អាចមើលគ្រប់ព័ត៌មានក្នុង read-only copy ក្នុងDNS server ក៏ប៉ុន្តែប្រសិនបើមានការផ្លាស់ប្តូរក្នុង read-only mode នោះ វានឹងបង្ហាញព័ត៌មាននៅលើ sever វិញ ។

១៦-២- Windows Link-Local Multicast Name Resolution

Microsoft Windows link-local multicast name resolution (LLMNR)គឺជាវិធីងាយស្រួលដែល Windows Server 2008 អាចដោះស្រាយ host local នៃ network segment ដោយមិនចាំបាច់ប្រើ DNS កាលពីមុន លក្ខណៈពិសេសនេះត្រូវបានជួយសម្រួលដោយ WINS រឺ NetBIOS ក៏ប៉ុន្តែ WINSនិង NetBIOS ប្រើបានតែជាមួយ IPv4 ប៉ុណ្ណោះ។ បច្ចុប្បន្ន Windows Sever 2008 អាចប្រើប្រាស់ជាមួយ IPv6 វាជាវិធីមួយផ្សេងទៀតដើម្បីដោះស្រាយឈ្មោះដោយមិនចាំបាច់ DNS។ ហេតុអ្វីបានជាអ្នកត្រូវការ LLMNR ?

ប្រសិនបើអ្នកមានប្រព័ន្ធ Network តូចមួយកំពុងដំណើរការជា Workgroup ។ DNS server address នៃ Client របស់អ្នកបញ្ជាក់ពី DNS server នៅខាងក្រៅដែលបានភ្ជាប់ Internet។ តើអ្នកត្រូវស្វែងរកឈ្មោះនៃ Host ក្នុង network របស់អ្នកយ៉ាងដូចម្តេច ? ចម្លើយនោះគឺ LLMNR

ឧទាហរណ៍ អ្នកចង់អ្នកចង់ ping ទៅ host មួយដែលមានឈ្មោះថា WIN2K8TEST មកពី Server របស់អ្នក។ Server របស់អ្នកដំបូង queries ទៅកាន់ configure DNS server របស់វា។ ប្រសិនបើ DNS server ត្រូវបានរកឃើញ វាព្យាយាម queryដើម្បី ភ្ជាប់ hostname នៅក្នុង Server ។ ប្រសិនបើ server មិនអាចដោះស្រាយនូវ hostname បានទេ នោះ DNS server របស់អ្នកប្រាប់ថា host នៅខាងក្រៅមិនបានភ្ជាប់ Internet ទេ។ បន្ទាប់មកវា ផ្ញើ multicast query នូវ UDPសម្រាប់ hostname។ host នីមួយៗនៅលើnetwork ដែលគាំទ្រ LLMNRនិងត្រួតពិនិត្យរកមើល hostname ដែលត្រូវនឹងhostname ខ្លួនរបស់វា ។ ប្រសិនបើវាមិនអាចរកឃើញទេនោះ វានឹងបោះបង់ packet នោះចោល ។ ប៉ុន្តែបើវារកឃើញ host ហើយនោះវានឹងផ្ញើUDP packet ត្រលប់ទៅឱ្យ IP address របស់វាវិញ ។

LLMNR អាចឆ្លើយតបទៅនឹងការទាមទាររបស់ hostname តែមួយគត់ ។ ប្រសិនអ្នកចូលទៅ FQDN (Fully qualified domain name) LLMRNនឹងមិនដោះស្រាយ hostname ទេ LLMNRគឺទទួលខុសត្រូវសម្រាប់ធ្វើឱ្យច្បាស់ថា hostname របស់វាគឺមានតែមួយគត់នៅក្នុង segment របស់វា។ ការធ្វើបែបនេះគឺដើម្បីឱ្យ name resolution ផ្តល់លទ្ធផលមកមិនមានតម្លៃស្ទួន។ ប្រសិនបើ LLMNR-enabled host ទទួលបានការទាមទារសម្រាប់ name resolution ហើយវាមិនទាន់ត្រួតពិនិត្យមើលថាតើ name គឺមានតែមួយទេ វានឹងធ្វើការកត់ត្រានូវការឆ្លើយតបត្រលប់មកវិញដើម្បីស្វែងរក host address របស់វា ។ host ដែលបានបង្ហាញតម្លៃតែមួយគត់មានន័យថាវាទទួលនូវ hostname របស់វា។

LLMNR គឺមានតម្លៃ enabled ក្រោយពី installed Windows Server 2008 ។ ក្នុងករណីខ្លះsecurity policies របស់អ្នកអាចមានតម្លៃ disabled។ LLMNR អាចមានតម្លៃ disabled លើ network interfaceទាំងអស់ រឺ network interface ពិតប្រាកដណាមួយ។

ដើម្បី **disabled LLMNR** លើ **network interface** ទាំងអស់, យើងត្រូវបង្កើតហើយកំណត់តម្លៃ **registry** ទៅ០៖

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\DnsCache\

Parameters\EnableMulticast

ដើម្បី **disabled LLMNR** លើ **specific network interface** មួយ យើងត្រូវបង្កើតហើយកំណត់តម្លៃ **registry** ទៅ 0

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\<adapterGUID>\EnableMulticast

ចំណាំនៅគ្រប់ network adapter គឺផ្តល់ឱ្យGUIDខ្លួនវាតែមួយគត់។ អ្នកចាំបាច់ត្រូវស្វែងរកGUIDដែលត្រូវនឹងnetwork adapter របស់អ្នកហើយជំនួសវាដោយ <adapterGUID> ជាមួយនឹងតម្លៃ។

១៦-៣- Windows Bitlocker Drive Encryption

នៅក្នុងការប្រើប្រាស់ Server ពួកយើងនឹងជួបប្រទះឧបសគ្គដ៏ធំជាងគេនៅក្នុងការបញ្ជាទីតាំងគឺការធានានូវសុវត្ថិភាពនៃ Physical Security ។ ការចូលឬប្រើប្រាស់ Remote Datacenter ដោយ Physical គឺមិនអាចធានាសុវត្ថិភាពបានជាប្រចាំបានទេ។ នៅពេខ្លះ Server ចាំបាច់ត្រូវតែដាក់នូវកន្លែងដែលមិនសូវសាកសមហើយគ្រោះថ្នាក់នៃ Physical Compromise ក៏ធំដែរ។ ឧទាហរណ៍ អង្គការមួយដែលមានផ្កាយរណបតូច អាចត្រូវការផ្ទុកទិន្នន័យរបស់ពួកគេលើ Local Server ដើម្បីងាយស្រួលក្នុងការប្រើប្រាស់។ ក្នុង កាលៈទេសៈនេះ វាជារឿងធម្មតាទេ ដែលគេដាក់Server នៅក្នុងទូមួយឬក៏ក្រោមតុ ពេលខ្លះServer អាចដាក់នៅជាមួយនឹង Servers ដែលមកពីអង្គការផ្សេងគ្នានៅក្នុង Datacenter តែមួយ។ ដូច្នេះ វាមិនមានភាពងាយស្រួលក្នុងការគ្រប់គ្រងនិងដឹងថា នរណាដែលមិនមែនជាបុគ្គលិកអង្គការអ្នកអាចចូលទៅកាន់ និងប្រើប្រាស់ Server អ្នកផ្ទាល់បានទេ។

ទោះបីជា Systems Administrator គ្រប់រូបខិតខំជៀសវាងការដំឡើងដោយគ្មានសុវត្ថិភាពជាប្រចាំ ប៉ុន្តែការជម្រើសរបស់ពួកគេគឺមានកំណត់។ បញ្ហាធំបំផុតនៃការទុកដាក់ Serverនៅទីកន្លែងដ៏មិនសមស្របនេះគឺបុគ្គលដែលមិនមានការអនុញ្ញាតបានចូលទៅប្រើប្រាស់ដោយផ្ទាល់នូវ Server អាចនឹងព្យាយាមទាញយកទិន្នន័យភ្លាមៗនៅលើ Disk ដោយប្រើ boot CDs និង USB Drives ឬក៏បុគ្គលនោះអាចនឹងយក Hard Disk ទៅដាក់នៅកុំព្យូទ័រផ្សេង។ ការចូលទៅប្រើប្រាស់ System ដោយគ្មានការអនុញ្ញាតតម្រូវឱ្យយើងមានការការពារនូវទិន្នន័យដើម្បីជៀសវាង System អនុញ្ញាតឱ្យគេចូលប្រើប្រាស់ ទោះបីជាគេបានចូលទៅគ្រប់គ្រង System ផ្ទាល់។

BitLocker ត្រូវបានណែនាំនៅក្នុង Windows Vista Enterprise និង Ultimate Edition គឺជាកម្មវិធីពិសេសដែលអាចការពារទិន្នន័យពី Physical Access បាន។ វាការពារ Operating System Files និង Volume ផ្សេងៗទៀត ដែលអ្នកកំណត់ឱ្យ BitLocker ការពារ។ វាដំណើរការលើបណ្តុំ Trusted Platform Model (TPM) chip នៃប្រព័ន្ធដើម្បីប្រាកដថាគ្រឿងបំណែកទាំងឡាយដែលត្រូវបានដំណើរការក្នុងអំឡុងពេលដែល Operating Sys-tem boot មិនមានការប៉ះពាល់ឬអក់ខាន។ ការការពារនេះនៅតែមានប្រសិទ្ធភាពទោះបីជា Operating System មិនដំណើរការ។ TPMs មាន registers ពិសេសមានឈ្មោះថា Platform Configuration (PCRs) ដែលផ្ទុកនូវ Hash Value របស់គ្រឿងបំណែក Startupគ្រប់ប្រភេទ ដូចជា BIOS, Master Boot Record (MBR), boot sector និង boot manager code។

តម្រូវការចាំបាច់

តម្រូវការមួយចំនួនដែលចាំបាច់មុនពេលអ្នកបើកកម្មវិធីBitLocker Drive Encryption អ្នកអាចដំឡើងកម្មវិធីពិសេសនេះគ្រប់ពេលវេលាប៉ុន្តែបើអ្នកចង់ប្រើប្រាស់ឱ្យបានគ្រប់មុខងាររបស់កម្មវិធីនេះ។ System របស់អ្នកត្រូវតែស្របទៅនឹងតម្រូវការដូចខាងក្រោម៖

- System មួយដែលមាន chip version 1.2 TPM
- Trusted Compution Group (TCG) ដែលអាចប្រើប្រាស់ជាមួយ BIOS បាន
- មានយ៉ាងតិចចំនួន Partition ពីរនៅក្នុង System របស់អ្នកមួយគឺ System Partition សម្រាប់ផ្តើមនិងមួយទៀតសម្រាប់អ្នកដំណើរការ Operation System (Boot Partition)

- BIOS ដែលគាំទ្រ USB mass Storage Device សម្រាប់ឱ្យ boot ពី USB flash drive។

១៦-៣-១- BitLicker Architecture

BitLocker ប្រតិបត្តិនូវ full-volume encryption ដែលធ្វើឱ្យvolume មិនអាចមើលឃើញនៅក្នុង System ក្រៅពីក្នុងអំឡុងពេល startup។ ពីព្រោះនៅពេល startup វាទាមទារឱ្យយើងប្រតិបត្តិជំហានបន្ថែមខ្លះទៀតដើម្បីទទួលបានការអនុញ្ញាតប្រើប្រាស់ឬនៅមុនពេលដែលយើងអាច Unloked Volume។ Volumes ត្រូវបានការពារដោយ 256-bit full-volume encryption key។ Key នេះត្រូវបានការពារដោយ 256-bit volume master key ហើយ volume master key អាចការពារបានដោយមធ្យោបាយមួយចំនួនដែលអាស្រ័យទៅនឹង authenication method ដែលអ្នកបានកំណត់។ authenication method នោះមានដូចខាងក្រោម៖

- TPM only
- TPM plus PIN (4-20 digits)
- TPM pluse startup key
- Clear key
- Startup key or recovery key
- Recovery password

➢ **TPM Only Authenication**

ដូចទៅនឹងឈ្មោះរបស់វា TPM only authenication មានន័យថា volume ត្រូវបានបើកផ្ទាល់ពី TPM ដោយប្រើប្រាស់ 2048-bit key។ វាមានងាយស្រួលប្រើ ប៉ុន្តែក៏ផ្តល់នូវកម្រិតសុវត្ថិភាពទាបដែរ ពីព្រោះនៅពេលដែលមានគេចូលទៅបើក System វា boot System ជាធម្មតា ដោយសារតែTPM បាន unlock drive ជាស្វ័យប្រវត្តិនៅពេលដែល startup files មិនត្រូវបានផ្តល់ដំណឹង។ វាការពារទិន្នន័យដែលនៅលើ volume នៅពេលតែ volume ត្រូវបានអានពី system ដែលខុសគ្នាស្រឡះ។ នៅពេលដែលយើងប្តូរទីកន្លែងឱ្យ Hard Drives ឱ្យទៅដាក់ក្នុងកុំព្យូទ័រ ឬ motherboard ផ្សេង TPM នឹងរកឃើញភាពខុសគ្នា ហើយ Server នឹងមិនដំណើរការ លុះត្រាតែយើង Recovery វាវិញ។ វិធីសាស្ត្រ TPM only authenication ក៏អាចការពារ System ដោយធានាថា Startup files មិនត្រូវបានគេប្តូរ ព្រោះនៅពេលដែលវាត្រូវបានប្តូរ វាអាចបណ្តាលឱ្យបរាជ័យក្នុងការត្រួតពិនិត្យក្នុង TPM។ ជម្រើសនេះវាល្អចំពោះ Serversរបស់អ្នកនៅពេលដែលដាក់វានៅក្នុងទីកន្លែងដែលសុវត្ថិភាពមួយដើម្បីចាប់ផ្តើមដំណើរការហើយនឹង Servers ជាលក្ខណៈនៅទីឆ្ងាយនោះនឹងមិនងាយមានទំនាក់ទំនងនឹង System ក្នុងដំណើរការ startupទេ។

➢ **TPM Plus PIN**

នៅពេលដែល TPM only authentication បានទទួលរងការខូចខាតឬត្រូវបានគេបំបែក ហើយយើងពុំមាន authentication ផ្សេងទៀតនោះ។ វានៅតែមានភាពប៉ះពាល់ដល់យើងព្រោះ TPM ផ្ទុកនូវរាល់ទិន្នន័យដែលត្រូវការយកមកអនុញ្ញាតឱ្យ Unlock Volumes។ វិធីម៉្យាងសម្រាប់បន្ធូរបន្ថយគ្រោះថ្នាក់នេះគឺការបន្ថែមនូវ authen -tication ឱ្យបានច្រើនយ៉ាង។ ក្នុងករណីនេះ យើងគួរតែតម្រូវឱ្យមាន PIN មួយសម្រាប់បញ្ចូលបន្ថែមនៅក្នុងដំណើរការត្រួតពិនិត្យ TPM។ វិធីសាស្ត្រ TPM plus PIN រួមបញ្ចូលទិន្នន័យជាមួយ key TPM 2048-bit ដែលមានពី 4-20 digit pin ទៅ SHA256 ដើម្បី Unlock volume។ ការតម្រូវឱ្យបញ្ចូល PIN ពង្រឹងនូវកម្រិតនៃសុវត្ថិភាពដោយ Key មួយដែលនៅក្នុងចំណោម Key ទាំងអស់ដែលត្រូវការសម្រាប់យកទៅដូរយក Volume master key

គឺមិននៅក្នុង System ទៀតទេ។ វាជួរទៅនៅក្នុងខួរក្បាលរបស់មនុស្សវិញម្តង(សង្ឃឹមថាគេមិនសរសេរPIN នោះនៅក្នុងក្រដាសមួយសន្លឹក រួចដាក់នៅជិត Server) ។

- **TPM Plus Startup Key**

វិធីសាស្ត្រ authentication មួយនេះគឺស្រដៀងគ្នាទៅនឹងវិធីសាស្ត្រ TPM plus PIN ខុសត្រង់តែគេប្តូរពីការវាយ PIN ទៅជា Startup Key ផ្ទុកក្នុង USB flash drive ដែលតម្រូវឱ្យយើងដាក់បញ្ចូល។ TPM key 2048-bit នេះអាន hash values នៅក្នុង PCR ហើយ generates វាជា intermediate key មួយដែលមានទំហំ 256-bit ។ Intermediate key នេះបានភ្ជាប់ជាមួយនឹង 256-bit startup key ដោយប្រើប្រមាណវិធី XOR (Exclusive OR) ទៅប្តូរយក 256-bit intermediate key មួយទៀតដែលសម្រាប់យកមកដោះគន្លឹះ volume master key។

- **Clear Key**

វិធីសាស្ត្រនេះមិនមែនជាវិធីសាស្ត្រ authentication ទេ ប៉ុន្តែក្នុងទម្រង់នេះ volume master key ត្រូវបានរក្សាទុកនៅក្នុង symmetric format មួយនៃ boot volume ដើម្បីធ្វើឱ្យវាអានបានជាចាំបាច់។ វិធីសាស្ត្រនេះគ្មានសុវត្ថិភាពទេ ហើយវាដំណើរការនៅពេលដែលយើងបញ្ឈប់ BitLocker ឬក៏មានបានដំឡើងវា។ យើងអាចនឹងត្រូវប្រើវិធីសាស្ត្រ Clear Key ដែរ។ ឧទាហរណ៍ បើអ្នកត្រូវ Restart server ដែលកំពុងប្រើវិធីសាស្ត្រ TPM plus startup key ហើយប្រភេទ Server របស់អ្នកជាលក្ខណៈ Remote ដែលបណ្តាលឱ្យអ្នកមិនអាចដោតឧបករណ៍បញ្ចូល USB key ដើម្បីឱ្យ Server អនុញ្ញាតឱ្យ boot បាន។

- **Startup key or Recovery key**

Startup key ឬ Recovery key គឺជាជម្រើសតែមួយគត់ប្រសិនបើ System របស់អ្នកមិនមាន TPM រឺ TPM mode របស់អ្នកមិនដំណើរការ (វាត្រូវបានបិទ រឺមិនដំណើការ)។ អ្នកអាច configure server របស់អ្នកដោយទាញយកចំនួន Master key រឺ Recovery key ដោយផ្ទាល់ពី USB Flash Drive ណាមួយ។ Recovery Key អាចត្រូវការជាចាំបាច់ប្រសិនបើ Original authentication method មិនអាចដំណើការបាន ក្នុងករណីដូចជា TPM មិនដំណើរការរឺត្រូវបានគេប្តូរទីតាំង អ្នកប្រើប្រាស់មិនចងចាំ PIN Code រឺ USB key ដែលផ្ទុប់ Startup key មិនដំណើរការ។ Recovery key អនុញ្ញាតឱ្យ Key ថ្មីត្រូវបានបង្កើតយ៉ាងលឿននិងមានសុវត្ថិភាព។

- **Recovery Password**

Method របស់Recovery password គឺដូចគ្នាទៅនិង Method របស់ Recovery key ដែរ ខុសគ្នាត្រង់តែ Recovery password តម្រូវឱ្យអ្នកវាយបញ្ចូលនូវ Password តែប៉ុណ្ណោះ។ Recovery Password ត្រូវកាជាចាំបាច់នូវពេលណាដែលយើងធ្វើការបើកBitLocker នៅលើ System ណាមួយ។ Recovery Password ត្រូវបានគេដំឡើងក្នុងគោលបំណងឱ្យ Data ដែលស្ថិតនៅលើ Drive ចាំបាច់ត្រូវតែទាញយកមកវិញនៅពេលណាដែលគ្មាន Authentication Methods ណាមួយដំណើរការ។

Hands on Exercise: Preparing for installing BitLocker

ចំនុចដែលចាំបាច់បំផុតនៅក្នុង BitLocker Drive Encryption គឺតម្រូវឱ្យអ្នកមាន Partition Drive យ៉ាងហោចណាស់ពីរនៅលើ System របស់អ្នក។ Partition Drive ទីមួយគឺ active partition ចំណែក Partition Drive ដទៃទៀតត្រូវបានគេហៅថា System Partition។ Partition Drive ទីមួយត្រូវមានទំហំ 1.5GB និងប្រើប្រព័ន្ធ NTFS ។ Windows Server 2008 ត្រូវបានគេដំឡើងនៅលើ Partition Drive ទីពីរ។ Partition Drive ទីពីរអាចកំណត់បានគ្រប់ទំហំអាស្រ័យនិងតម្រូវការរបស់ Windows Server 2008 របស់អ្នក។ នៅក្នុងលំហាត់ខាងក្រោមនេះយើងនិងធ្វើការរៀបចំការដំឡើង BitLocker ដោយបង្កើតនូវ Partition Drive ពីរដោយប្រើ Command diskpart.exe ។

ចំណាំ៖ លំហាត់នេះនិងលុបរាល់ទិន្នន័យរបស់ Hard Drive នៅលើ System នៅពេលដែលអ្នកដំណើរការដូចខាងក្រោម។ អ្នកត្រូវប្រកត់ថាគ្មានទិន្នន័យសំខាន់នៅលើHard Drive ឡើយមុនពេលដំណើរការ។

1. អ្នកត្រូវ Booting System របស់អ្នកដោយប្រើ Windows Server 2008 DVD ។
2. ជ្រើសរើសភាសាដើម្បីធ្វើការដំឡើង, time and current format, និង keyboard រឺ input method បន្ទាប់មកជ្រើសរើស Button Next ។
3. នៅលើផ្ទៃ Install Now screen បន្ទាប់មកជ្រើសរើស Button Repair Your កុំព្យូទ័រ។
4. ប្រសិនបើ Partition Drive របស់អ្នកធ្លាប់បានដំឡើង Operating System នេះរួចមកហើយវានឹងជ្រើសរើសយកជម្រើស default នៅក្នុងប្រអប់ System Recovery Option ។
5. ជ្រើសរើស Command Prompt Link ដើម្បីបើកនូវ Command Prompt ថ្មីមួយដូចរូប10-1 ។
6. ជ្រើសរើស command Prompt ហើយវាយពាក្យ diskpart បន្ទាប់មក Enter ។

Figure 10-1. Make sure none of the operating systems are selected.

Figure 10-2. Click Command Prompt in the System Recovery Option dialog box.

7. វាយ **list disk** បន្ទាប់មកចុច enter។ បន្ទាប់មកវានិងបង្ហាញតារាង Detected Disk នៅលើ System របស់អ្នកដូចរូប ១០-៣។ អ្នកត្រូវកត់សំគាល់លេខ disk នៃ disk ដែលអ្នកចង់បំបែក។ នៅក្នុង System នេះ វាបង្ហាញ disk តែមួយគឺ (Disk 0) ដូចក្នុងរូប 10-3
8. វាយពាក្យ **select disk 0** បន្ទាប់មក enter។ Disk របស់អ្នកប្រហែលជា Disk 0 ដូចគ្នាដែរ ប៉ុន្តែប្រសិនបើមិនដូចប្តូរ 0 ជាមួយលេខ disk ដែលអ្នកបានឃើញពីខាងលើ។ អ្នកនិងបានឃើញសារបញ្ជាក់ថា disk ត្រូវបានជ្រើសរើស។
9. វាយ **clean** បន្ទាប់មកចុច enter។ វាយនិងធ្វើការលុបចោលនូវតារាង Partition ចាស់ចោល។
10. វាយពាក្យ Create Partition Primary Size=1500 និង Enter។ យើងនិងបង្កើតបាន Primary partition ១ទំហំ 1500MB។
11. វាយពាក្យ Assign Letter=Z និង Enter។ ដើម្បីដាក់ឈ្មោះរបស់ Partition អ្នកជា Z

Figure 10-3. Disks detedcted by diskpart.

12. វាយពាក្យ Active និង Enter ដើម្បីឲ្យ Partition drive របស់អ្នកចាប់ដំណើរការ
13. វាយពាក្យ Create partition primary និង Enter។ យើងនិងបានបង្កើត Primary Drive ទីពីរដែលមានទំហំស្មើនឹងទំហំដែលនៅសល់ក្នុង Drive របស់អ្នក។
14. វាយពាក្យ Assign Letter=C និង Enter។ ដើម្បីដាក់ឈ្មោះ Partition របស់អ្នកជា C
15. វាយ List Volume និង Enter។ វានិងបង្ហាញ list volume Partition Drive ដើម្បីប្រាកដថាអ្នកបានបង្កើត partition drive បានសម្រេចឬនៅ (រូប 10-4)។
16. វាយ Exit និង Enter ដើម្បីចាកចេញពី Diskpart។
17. វាយ **format C: /q /fs:NTFS** និង Enter។ វានិងធ្វើការកែប្រែ Format Drive Cរបស់អ្នកទៅជា NTFS Format។

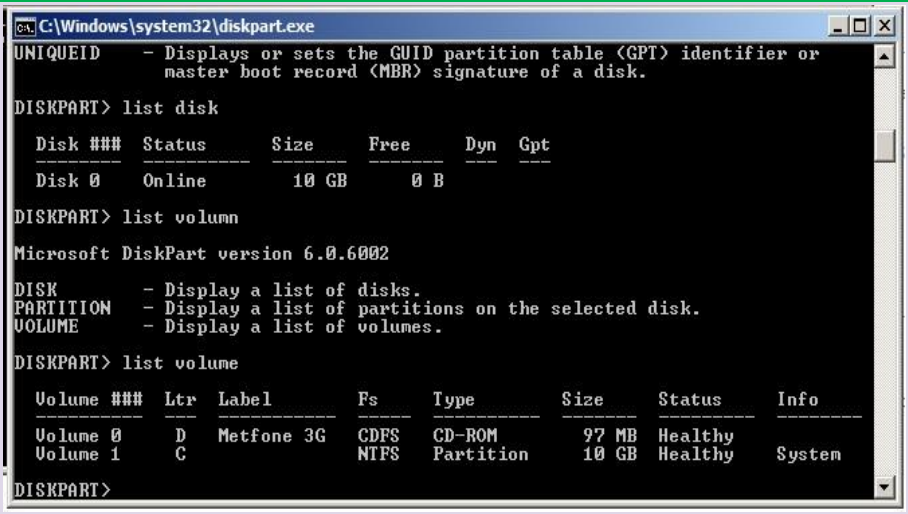


Figure 10-4. List of volumes on the system.

18. វាយ **format Z: /q /fs:NTFS** និង Enter។ វានិងធ្វើកាកែប្រែ Format Drive Z របស់អ្នកទៅជា NTFS Format។
19. បិទ Command Prompt។
20. បិទ System Recovery System Option Window ដើម្បីធ្វើកាបន្តការដំឡើង window server 2008។ កុំចុច Shut down ឬ Restart។
21. អ្នកនឹងត្រឡប់មកដល់ Install window screen រួចចុច Install now។
22. ពេលនេះអ្នកអាចបន្តការដំឡើង Window server 2008 តាមរបៀបធម្មតាវិញបាន។
23. Window Server 2008 បានរួមបញ្ចូល BitLocker Drive Encryption ជាលក្ខណៈពិសេស ប៉ុន្តែវាមិនដំឡើងតាម Default ទេ។ ប្រសិនបើអ្នកចង់ដំឡើងអ្នកត្រូវបើក Server Manager។

Figure 10-5

24. ចុច Feature Link
25. ជ្រើសរើស BitLocker Drive Encryption ដូចក្នុងរូប 10-5 ហើយចុច Next។
26. ចុច Install ដើម្បីបន្ត។

27. Restart កុំព្យូទ័រ របស់អ្នក។

ចំណាំ៖ អ្នកអាចដំឡើង Feature នេះបានតាមរយៈ Command ដូចខាងក្រោម៖

ServerManagerCmd.exe -install BitLocker –restart

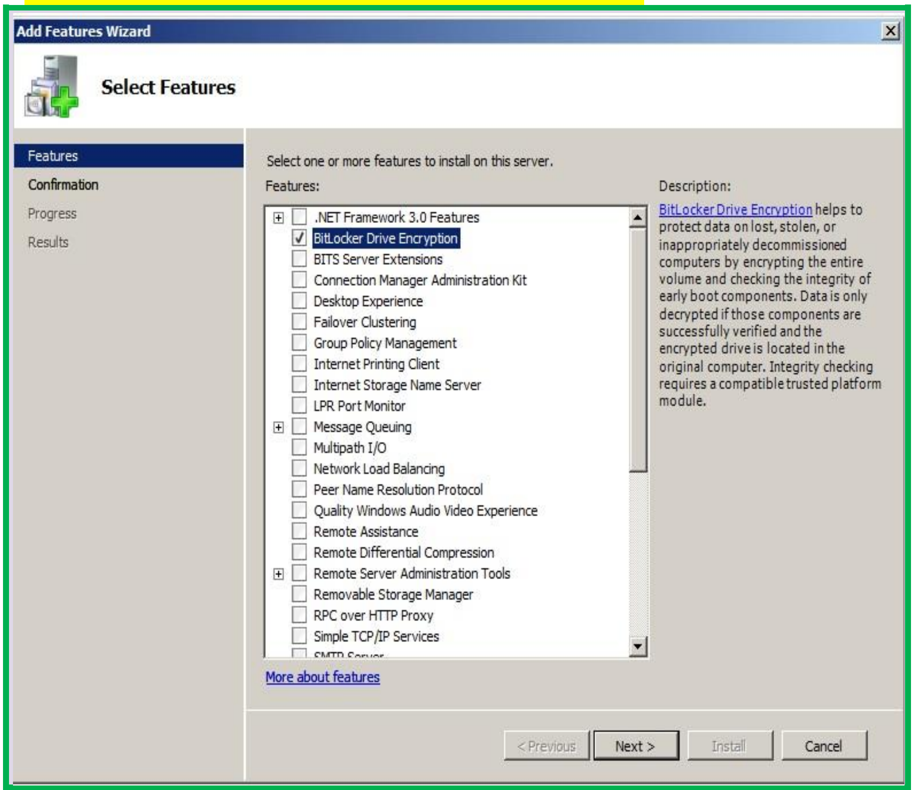


Figure 10-6. Add the BitLocker Drive Encryption feature.

Initializing BitLocker

Hands-On Exercise: Enabling BitLocker Drive Encryption

នៅក្នុងលំហាត់មួយនេះ អ្នកនឹងចេះនូវការបើក BitLocker Drive Encryption and encrypt the Windows installing volume ។

1. បើក Control Panel
2. ចុចពីរដងស្ទួនលើ BitLocker Drive Encryption
3. បើសិនអ្នកនៅមិនទាន់ initialized TPM របស់អ្នកនៅឡើយទេ អ្នកនឹងឃើញInitialize TPM Security Hardware Wizard។ ធ្វើតាម wizard ធម្មតា ហើយ restart កុំព្យូទ័ររបស់អ្នក។ បើអ្នកមិនទាន់មាន TPM module នៅកុំព្យូទ័ររបស់អ្នកទេ អ្នកនឹងត្រូវការធ្វើតាមជំហានដូចខាងក្រោមដើម្បីអនុញ្ញាតឱ្យអ្នកអាចបើក BitLocker ដោយគ្មាន TPM ។
   a. ជ្រើសរើស Start | Run
   b. វាយពាក្យ gpedit.msc ហើយចុច Enter
   c. ពង្រីក កុំព្យូទ័រ Configuration | Administrative Temples | Windows Components | BitLocker Drive Encryption
   d. Double-click Control Panel Setup: Enable Advanced Startup Options ដែលបានបង្ហាញ នៅ Figure 10-7

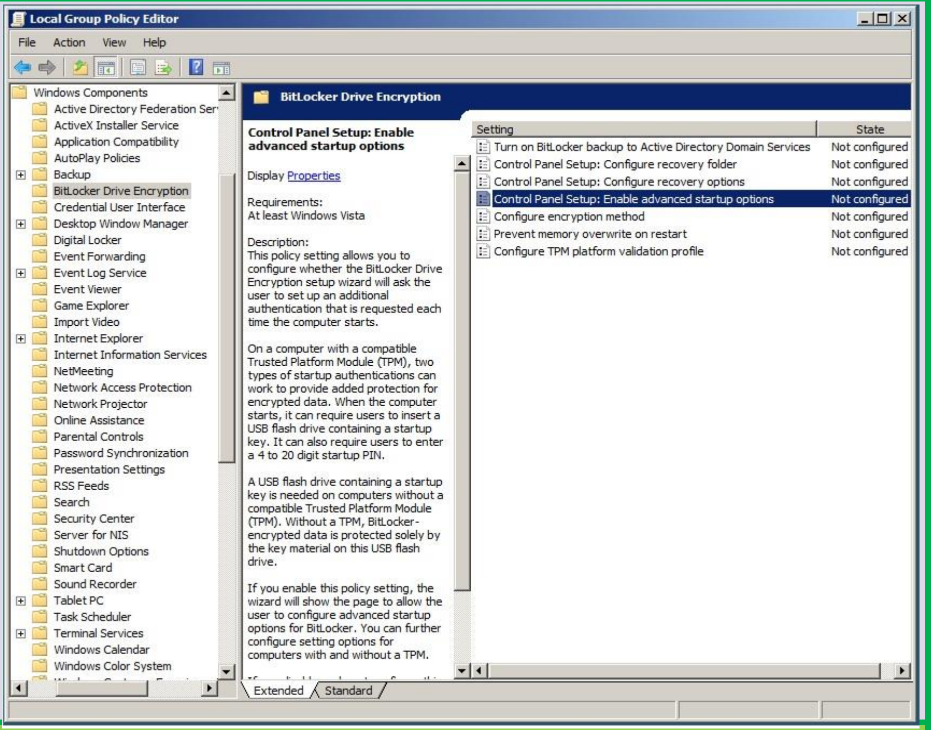


Figure 10-7. Access the BitLocker Drive Encryption Group Policy item.

e. នៅលើ Properties page ជ្រើសរើសយក Enabled ហើយគូសលើប្រអប់របស់ Allow BitLocker without a Compatibel TPM ។ នៅ drop-down lists ខាងក្រោម អ្នកអាចជ្រើសរើស startup key and pin options of your choice សម្រាប់កុំព្យូទ័ររបស់អ្នកជាមួយនឹង TPM ។ ហើយចុច Ok ។

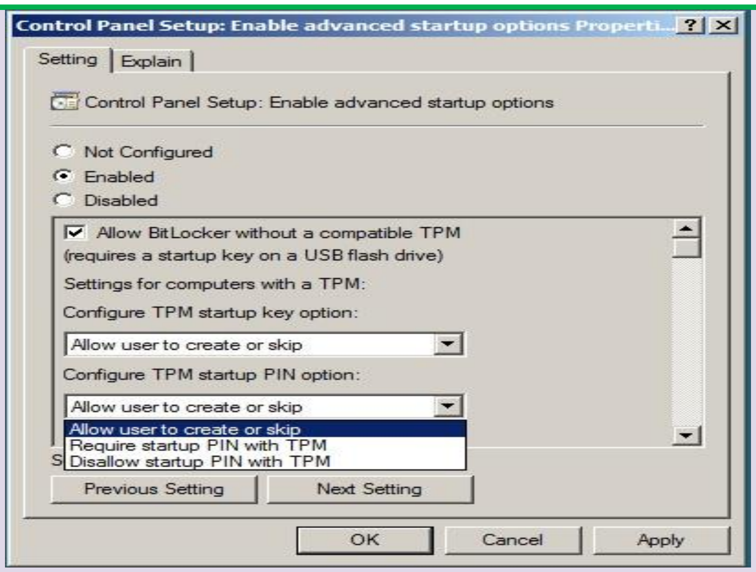


Figure 10-8. Allowing BitLocker without a compatible TPM.

f. បិទ local group policy editor ហើយបើក Command Prompt រួច run ហើយវាយពាក្យ gpupdate ។

g. ត្រលប់ទៅ BitLocker Drive Encryption Control Panel applet ។

4. ចុច Turn On BitLocker ដូចដែលបានបង្ហាញនៅ Figure 10-9

5. ចុច Continue with BitLocker Drive Encryption បានបង្ហាញនៅ Figure 10-10

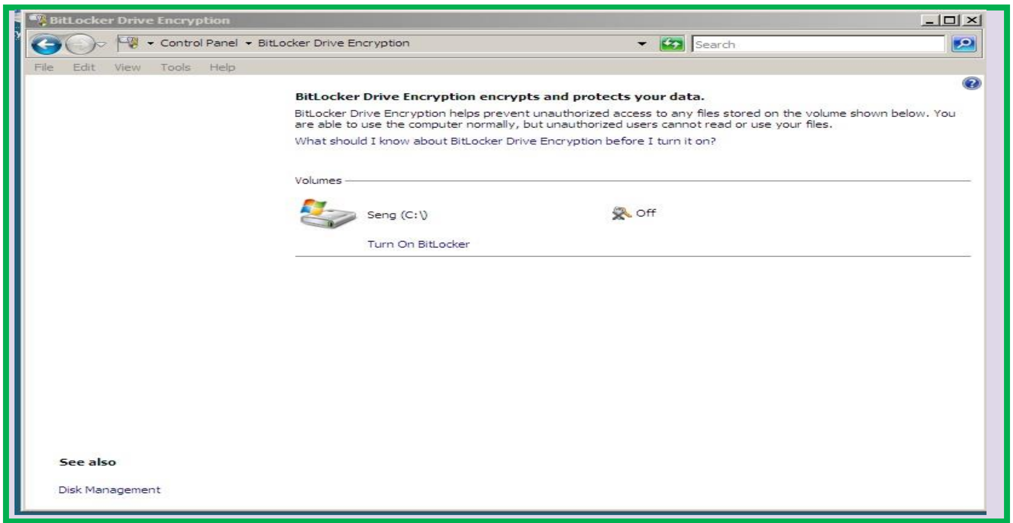


Figure 10-9. Turn on BitLocker.

Figure 10-10. Confirm that you want to encrypt the volume.

6. ចុច BitLocker startup preference អ្នកអាចជ្រើសរើសប្រើ BitLocker ដោយគ្មាន Additional Keys ដែលប្រើតែ TPM only authentication។ អ្នកអាចជ្រើសរើសយក Require PIN at Every Startup or Require a Startup USB Key at Every Startup ជម្រើសចុងក្រោយគឺ បើសិនអ្នកគ្មាន compatible TPM នៅលើប្រព័ន្ធអ្នក ។ វាបានបង្ហាញនៅរូបភាព១០-១១។
7. អ្នកនឹងត្រូវជ្រើសរើសទីតាំងដើម្បីរក្សាទុក recovery password។ វាត្រូវបានបង្ហាញនៅរូបភាព១០-១២។
8. ប្រាកដថាអ្នកបានគូសលើប្រអប់ Run BitLocker System Check ហើយចុច continue ។ វាបានបង្ហាញនៅរូបភាព១០-៣។
9. ចុច Restart Now ដើម្បីចាប់ផ្តើម encryption process

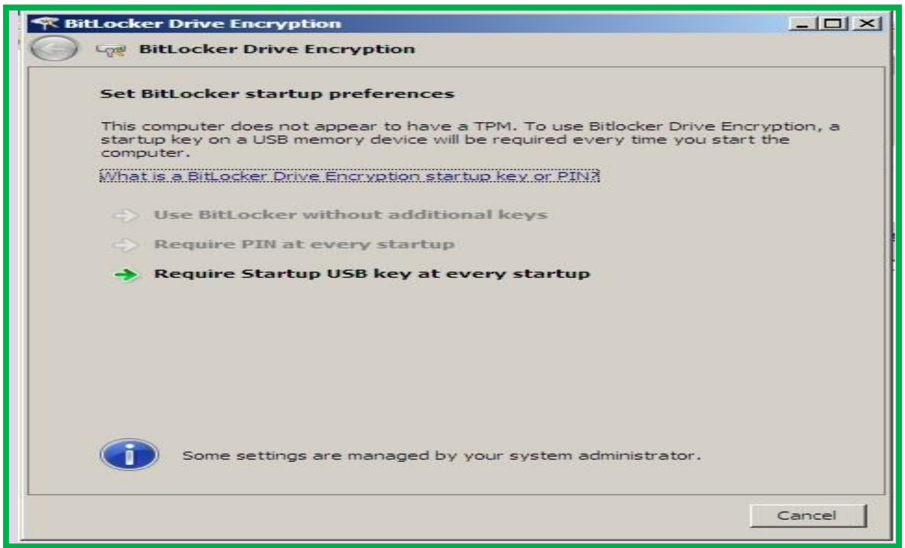


Figure 10-11. Confirm that BitLocker startup preferences.

១៦-៤- BitLocker Recovery

ពេលណាអ្នកនិយាយពី encryption យើងត្រូវតែរួមបញ្ចូលនូវការពិភាក្សាថាតើយើងអាច recovery data តាមរបៀបណា បើមេកានិចដើមសម្រាប់ដោះសោរការពារ មិនដំណើរការ ក្នុងករណីនេះអ្នកប្រហែលត្រូវការ TPM plus PIN authentication ។ ចុះបើសិនជាអ្នកប្រើប្រាស់ភ្លេច PIN code ឬ PCM មិនអាចធ្វើប្រតិបត្តិការត្រឹមត្រូវបាន នៅពេលនោះ BitLocker នៅតែប្រកាន់តាមផ្នត់គំនិតដើមរបស់ខ្លួន ទោះបីជាអ្វីមួយត្រូវបានគេព្យាយាមបំផ្លាញក៏ដោយ BitLocker នៅតែរក្សាទិន្នន័យរបស់យើង Encrypt ដោយសុវត្ថិភាពដដែល។ ដំណើរការនៃការ Recover volume ដែលត្រូវបានការពារទិន្នន័យត្រូវការប្រើប្រាស់ Recovery key ឬ password ដើម្បីផ្តល់នូវច្រកក្រោយមួយឱ្យ Administrator ចូលក្នុង System សម្រាប់ដោះស្រាយបញ្ហាដូចខាងលើ។

បញ្ហាខាងក្រោមនេះដែលអ្នកនឹងអាចជួប ហើយត្រូវធ្វើ **recover**៖

- អ្នកប្រើភ្លេច PIN និងអ្នកគ្មានទិន្នន័យផ្សេងទៀត
- អ្នកប្រើអាចខូច ឬបាត់ USB flash drive ដែលផ្ទុកនៅ key
- មានភាព error នៅក្នុង TPM ឬក៏TPM ខុសគ្នា
- TPM បិទ ឬក៏បំបាត់ចោល
- File boot ខ្លះត្រូវបានកែប្រែ ដែលជាហេតុធ្វើឱ្យ signature មិនត្រូវនូវអ្វីដែលរក្សាទុកនៅក្នុង TPM

បើមានបញ្ហាអញ្ចឹងកើតឡើងមានតែធ្វើការ recovery ទេ នៅពេល Windows Server 2008 load អ្នកត្រូវតែដោត USB flash driver ដែលផ្ទុកនូវ recovery key ឬក៏វាយបញ្ចូល recovery password ។ encrypted drives នឹងមិនអាចអានបានទេ លុះត្រាតែអ្នក ដោះគន្លឹះវិញដោយប្រើ recovery key ឬក៏ password ។ ចំណាំ៖នៅពេលដែលវាយបញ្ចូល recovery password អ្នកត្រូវតែវាយបញ្ចូលជាមួយ function key ប្រសើរជាងលេខធម្មតា។ លេខ១-៩ តំណាងឱ្យ F1-F9 ចំនែកឯ F10 គឺតំណាងឱ្យលេខ 0 ។

Hand-On Exercise: Recover Access to BitLocker Encrypted Volumes

នៅក្នុងលំហាត់នេះ ពួកយើងនឹងដំណើរការម្តងទៀតនូវ BitLocker encrypted volumes ។ មធ្យោបាយដែលស្រួលបំផុតនូវដំណើរការវានៅក្នុង system របស់អ្នកគឺ ពេល TPM enabled ត្រូវបិទ TPM ហើយ restart កុំ

ព្យូទ័រ ។ ដំណាក់ការខាងក្រោយធ្វើនៅពេលដែលមិនអាចដំណើរការជាមួយvolumeបាន ព្រោះបាត់បង់ authen -ticaiton requirements

1. បើកុំព្យូទ័ររបស់អ្នកបិទ សូមបើកកុំព្យូទ័រ ហើយអ្នកនឹងឃើញ BitLocker Drive Encryption Recovery Console ។
2. បើសិនអ្នកមាន USB flash drive មាននូវ recovery password ដោត flash ទៅនឹងកុំព្យូទ័រនិងចុច ESC ។ វានឹងបញ្ចូល recovery password ឱ្យអ្នកដោយស្វ័យប្រវត្ត និង restart កុំព្យូទ័រ។ ឬក៏បើអ្នកមិនមាន USB flash drive មាននូវ recovery password ទេ ប៉ុន្តែមាន password available មួយ សូមចុច Enter ហើយវាយបញ្ចូល recovery password ដោយប្រើ function keys ហើយ ចុច Enter ដើម្បី restart ។

១៦-៤-១- ការមិនឱ្យលុប BitLocker Drive Encryption

នៅពេលខ្លះអ្នកប្រហែលជាចង់បិទ BitLocker រយៈពេលខ្លីឬក៏ឈប់ប្រើ BitLocker តែម្តងឬក៏ decrypt គ្រប់ drive ទាំងអស់វិញ។ ហេតុផលមួយដែលយើងតែងតែជួបគឺ យើង បិទBitLocker រយៈពេលខ្លី គឺដើម្បី update operating system ឬក៏ធ្វើការផ្លាស់ប្តូរ TPM ។ ដើម្បី disable ឬ enable BitLocker គឺទាមទារឱ្យយើងវាយបញ្ចូល recovery key ។

Hands-On Exercise: Disable BitLocker Driver Encryption

ឧទាហរណ៍ថា អ្នកមាន BitLocker រួចហើយ ហើយ encrypted driver មានយ៉ាងហោចណាស់មួយ៖

1. បើក BitLocker Driver Encryption ពី Control Panel
2. នៅ BitLocker Page ជ្រើសរើស volume ដែលអ្នកចង់បិទ BitLocker
3. នៅ prompted for the level of decryption ជ្រើសរើសយក Disable BitLocker Drive Encryption (បើចង់ disable វាមួយរយៈពេលខ្លី) ឬក៏យក Decrypt Volume (បើចង់ disable វារហូត)។

១៦-៥- WINDOWS SERVER 2008 ITANIUM SUPPORT

Windows Server 2008 សម្រាប់ Itanium processor ត្រូវបានបង្កើតជាមួយនឹងមុខងារចម្បងមួយគឺ Application ឬ database server ដែលបានពង្រីកនូវ local processing power និង RAM។ តួនាទីនិងលក្ខណៈពិសេសជាច្រើនគឺមិនគាំទ្រជាមួយនឹង Itanium-based system នៅពេលដំណើរការក្នុង Windows Server 2008។ បើអ្នកកំពុងតែប្រើWindows Server 2008 Itanium-based system ភាគច្រើន application របស់អ្នកត្រូវតែដើរលើ Windows Server 2008 សំរាប់ Itanium-based system ។

Windows Server 2008 មិនគាំទ្រ Terminal Services នៅក្នុង application modeដែលនៅក្នុង Itanium-based system ទេ។ ហើយវាមិនគាំទ្រ system ជាច្រើនដែលបង្កើតដោយ distributed systems ផងដែរ។ បើអ្នកកំពុងប្រើ Itanium-based system មានតួនាទីខ្លះមិនគាំទ្រជាមួយនឹង Itanium-based system។ ឧទាហរណ៍ SharePoint គឺមិនគាំទ្រជាមួយ Windows Server 2008 លើ Itanium-based system ទេ។ ដើម្បីមើលនូវការគាំទ្រនិងតារាងមិនគាំទ្រទាំងស្រុងនៅលើ Itanium-based system សូមចូលទៅគេហទំព័ររបស់ Microsoft's Windows Server Web Site។ Windows Server 2008 នៅលើ Itanium-based system គឺតួនាទីរបស់វាមានជំនាញខាង application server ។ ពីព្រោះការបង្កើតវាឡើងមានលក្ខណៈពិសេសជាច្រើនមិនគាំទ្រ។

សង្ខេបជំពូក

នៅក្នុងជំពូកនេះបានផ្តល់នូវការផ្លាស់ប្តូររបស់ DNS និងពិភាក្សាអំពីការប្រើ BitLocker Drive Encryptoin ដើម្បីជួយការពារ system ។ Windows Server 2008 អាចគាំទ្រ IPv6 ។ ជាការពិតណាស់ Microsoft បានបង្កើនមុខងារឱ្យ DNS នៅក្នុង Window Server 2008 ដើម្បីអាចផ្តល់នូវកន្លែងផ្ទុក IPv6 ចាប់តាំងពី WINS និង NetBIOS អាចប្រើបានជាមួយ IPv6 មក Local-Link multicast name resolution(LLMNR) បានបង្កើត address ឱ្យ host នៃ IP address នៅលើ local segment ដោយមិនចាំបាច់ប្រើ WINS or NetBIOSទៀតទេ។ លើសពីនេះទៅទៀត ការណែនាំរបស់ read-only domain controllers role ក្នុង Windows Sever 2008 បានបង្ហាញលើ read only DNS zones ក្នុង Windows DNS server system ។

BitLocker បានផ្តល់នូវ Layer បន្ថែមសម្រាប់ការពារសុវត្ថិភាព Server។ វាបានបន្ថែមការស្មុគស្មាញបន្តិចជាពិសេសពេលយើងកំពុងតែអនុវត្តការ update ឱ្យ system ដែលអាចប៉ះពាល់ដល់ផ្នែកគ្រឿងបំនែកដែលទាក់ទងជាមួយការ boot ក៏ប៉ុន្តែវាអាចការពារការចូលទៅប្រើប្រាស់ផ្ទាល់ដោយគ្មានការអនុញ្ញាត។ បើអ្នកមាន Sever មួយមានលក្ខណៈជា remote ដែលអ្នកមិនអាចធានាការពារសុវត្ថិភាព នៃការចូលប្រើប្រាស់ផ្ទាល់ការប្រើ BitLocker បានផ្តល់នូវដំណោះស្រាយមួយដែលធ្វើឱ្យអ្នកទុកចិត្តបាន។ បន្ថែមពីនេះទៅទៀត អត្ថប្រយោជន៍នៃការប្រើប្រាស់វិធីសាស្ត្រ authentication រួមគ្នាច្រើនដូចជា TPM plus PIN។ នៅពេលដែលមានព្រឹត្តិការណ៍មិនងាយកើតឡើងដូចជា TPM ត្រូវបានគេបំបែកឬទទួលរងការខូចខាត PIN code បានបន្ថែមនៅការការពារមួយស្រទាបទៀតទៅឱ្យ System។ Windows Server 2008 នៅតែបន្តគាំទ្រ Itanium-based systems ។ ដោយសារវាគឺជាទម្រង់ពិសេសរបស់ Windows Server 2008។ វាផ្តល់នូវការគាំទ្រដែលមានកំណត់ចំពោះមុខងារមិនទាក់ទងផ្ទាល់ទៅនឹងសមត្ថិភាពរបស់ server ទៅឱ្យ host application។ អ្នកគួរតែរក្សាការប្រើប្រាស់ Windows Server 2008 ដែលមាន Itanium-based systems ទៅឱ្យ application ណាដែលទាមទារ performence និងការគាំទ្រដែលមានទំហំធំដែលវាបានផ្តល់ឱ្យ ។

សំណួរត្រួតពិនិត្យ

១-តើ Bitlocker Driver Encryption ប្រើសម្រាប់ធ្វើអ្វី?
២-តើ DNS ត្រូវបានគេប្រើសម្រាប់ធ្វើអ្វី?
៣-តើ LLMNR ត្រូវបានគេប្រើសម្រាប់ធ្វើអ្វី?
៤-ចូរបង្ហាញពីរបៀបបិទ LLMNR ចំពោះ Network Interface ណាមួយ?
៥-ចូរបង្ហាញពីរបៀបបិទ LLMNR ចំពោះ Network cards ទាំងអស់?
៦-ចូរបង្ហាញពីរបៀបបើក Bitlocker Driver?
៧-តើ Bitlocker Driver Encryption មានក្នុង Windows ណាខ្លះ?
៨-ចូរបង្ហាញពីរបៀបបិទ Bitlocker Driver Encryption?

ជំពូកទី១៧

Routing និង Remote Access

ពេលដែលយើងនិយាយអំពីការតភ្ជាប់ទៅកាន់ Systems ដែលជា Local Network យើងចាប់ផ្តើមស្វែងយល់ពីពិភពនៃ Routing and Remote Access Services (RRAS)។ Routingជាបំនែកនៃ RRAS ដែលផ្តល់ឱ្យនូវ LAN-to-LAN LAN-to-WAN virtual private networks(VPNs)ហើយនិង Network Address Translation (NAT) services។ ចំណែកឯ Remote Access ផ្តល់នូវការតភ្ជាប់ពីចម្ងាយពី LAN ឆ្ពោះទៅកាន់ dial-up ឬ VPNs access។ ការសាយភាយនៃរលកជាតុអាកាស VPN គឺកំពុងពេញនិយម វាអាចផ្តល់នូវល្បឿនលឿននិង មានលទ្ធភាពក្នុងការតភ្ជាប់ពីចម្ងាយបានយ៉ាងល្អ ហើយនិងមានតម្លៃថោកជាងសេវា dial-up ដែលតម្រូវការ Hardware ជាពិសេសដូចជា Modem ។ RRAS មានចាប់តាំងពី Window NT 4.0 ប៉ុន្តែវាបានវិវត្តន៍ទៅជា RRAS។ឥឡូវវាជាផ្នែកមួយនៃWindows Server 2008 ដ៏មានសារៈសំខាន់។សមាសជាតុនៃ RRAS រួមមាន Windows Server 2008 ដែលមានសមត្ថភាពក្នុងការដាក់បញ្ចូលគ្នាជាមួយនិង Network Access Protection (NAP)ផ្តល់ឱ្យ administrator សម្រាប់ត្រួតពិនិត្យទៅលើ Systems ដែលអនុញ្ញាតឱ្យភ្ជាប់ទៅកាន់ network មួយ។ទោះបីជាមានការបែងចែកនៃការប្រើប្រាស់ Hardware routers ដើម្បីផ្តល់នូវសេវា routing ក៏ដោយក៏ RRAS បានផ្តល់ឱ្យនូវជម្រើសនៃការប្រើប្រាស់ Windows server មួយដូច router ដែរ។

១៧-១- Routing Services

Windows Server 2008 RRAS ផ្តល់ឱ្យនូវ multiprotocol routing services សម្រាប់ការតភ្ជាប់ LAN-LAN, LAN-WAN, VPN និង NAT។ ដើម្បីប្រើប្រាស់លក្ខណៈពិសេសនៃ routing នៃ RRAS អ្នកត្រូវយល់ឱ្យច្បាស់អំពី Network Protocols។ គោលដៅកំណត់គឺ Hosts នៅលើ Network Segment មួយទំនាក់ទំនងជាមួយនិង Hosts នៅលើ Network Segment មួយផ្សេងទៀតហើយនេះគឺជាទំនាក់ទំនងនៃ Internetwork។ ទោះបីជា Windows Server 2008 បានផ្តល់នូវ routing service ចំពោះ RRAS។ ប៉ុន្តែ RRAS មិនធ្វើការប្រៀបធៀបចំពោះបរិក្ខា router ដែលបានកំណត់ទុកនោះទេ។ អ្នកឆ្ងល់ថាលក្ខណៈពិសេសនេះគួរតែបិតនៅក្នុង Operating System នៅពេលធ្វើការរៀបចំប្រើប្រាស់ routers និងជាធម្មតាជ្រើសយក routerដែលបានកំណត់ទុកជា multihomed Windows Server។ កាលៈទេសៈដ៏ល្អការប្រើប្រាស់ Windows Server 2008 ហើយនិងRRAS គឺជាជម្រើសដ៏ល្អបំផុត ។ បន្ទាប់ពីនោះវាគ្មានតម្លៃអ្វីទេក្រៅពី Network Interface ហើយវាជាជម្រើសដ៏ល្អប្រសិនបើអ្នកចង់ភ្ជាប់ពីការិយាល័យផ្កាយរណបតូចទៅកាន់ការិយាល័យធំរបស់អ្នកជាមួយនិងតម្លៃទាប ហើយអ្នករំពឹងទុកថាដំណើរការដាក់លើ Server ដូចទៅនិងលទ្ធផលនៃតួនាទី routing ដែរ។ routing បានប្រើប្រាស់តិចតួចនៃលក្ខណៈពិសេសចម្បងពីរដែល RRAS អាចផ្តល់ឱ្យ។

១៧-២- Routing Basics

មុននិងឈានដល់ចំណុចស៊ីជំរៅមួយចំនួនយើងគួរស្វែងយល់ពីដំណើរការរបស់ Routing ទោះបីជា RRAS ផ្តល់នូវ multiprotocol routing ។ ទាំងនេះជាចំនុចដែលសិក្សាទៅលើ TCP/IP ចាប់តាំងពីពេលនោះការប្រើប្រាស់ Protocol នៅលើ Window network មួយជាការធម្មតាហើយ packets ដែលប្រើនៅក្នុងTCP/IP ទាក់ទងទៅនឹង source និងdestination address Subnet mask មួយឆ្លើយតបទៅនិង address នីមួយៗដើម្បី

កំណត់IP address ជា network address ដែលអាស្រ័យទៅនិង host ផងដែរ។ នៅពេលដែល packet មួយបានបញ្ជូនគោលដៅទៅកាន់ host មួយ។ ជាដំបូងវាកំណត់នូវ destination address នៅលើ Subnet ដូចគ្នា។ ប្រសិនបើវានៅលើ Subnet ដូចគ្នា នោះ Packet ដែលសំខាន់ជាងគេបានបញ្ជូនតាមខ្សែ Network ជាច្រើនសម្រាប់ destination host ធ្វើការជ្រើសយក ។ ប្រសិនបើ packet កំណត់គោលដៅជាផ្នែកនៃ Network ខុសគ្នា នោះវាបញ្ជូន Packet នេះទៅកាន់ router ដោយបានកំណត់យ៉ាងច្បាស់ដោយrouting table របស់វា។ទំនួលខុសត្រូវរបស់ router គឺត្រួតពិនិត្យទៅលើ packet ដែលបានបញ្ជូនnetworkខុសគ្នាដើម្បីកំណត់កន្លែងបញ្ជូនបន្ត។ Router អាចស្គាល់នូវ interface របស់វាដោយបញ្ជូន packet ទៅដល់គោលដៅចុងក្រោយ ។ router អាច configure ជាមួយនិង links ទៅកាន់គោលដៅដូចគ្នា។ ឧទាហរណ៍ router អាចភ្ជាប់ទៅកាន់ network ដទៃតាម T1 line នឹងទៅជា ISP ហើយ T-1 និងបំពេញនូវ ISP ខុសៗគ្នាដទៃទៀត ។ ប៉ុន្តែប្រសិនបើមានការភ្ជាប់ណាមួយបរាជ័យនោះ router ក៏នៅតែ Access បានដដែលនៅលើ network ។

សម្រាប់ឧទាហរណ៍នៅក្នុងរូបភាព១១-១ ដែល networks 2 ត្រូវបានធ្វើការបែងចែកដោយ routers 2 ដែលបានធ្វើការភ្ជាប់ដោយផ្ទាល់។

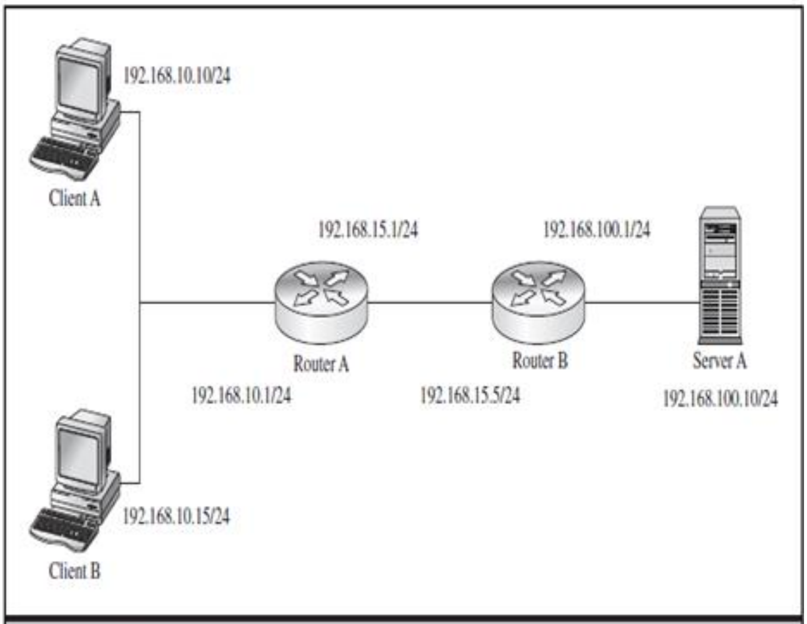


Figure 11-1. Two networks separated by two routers that are directly connected

ដោយ Client A ត្រូវការបញ្ជូន packet មួយទៅកាន់ Server A ដែលមាន IP address 192.168.100.10/24.។ ក្នុងការបញ្ហារបស់ Clients ដើម្បីបញ្ជូន packet ទៅកាន់ Server វាត្រូវការបញ្ជូនទៅកាន់ Router A តាមរយៈ interface 192.168.10.1/24 ហើយវាបញ្ជូនបន្តទៅកាន់ Router B តាមរយៈ interface 192.168. 15.1។ ពេលនោះ Router B បានទទួល data តាមរយៈ interface 192.168.15.5 និងឆ្ពោះទៅកាន់ Server ដែលមាន interface 192.168. 100.1។ នៅពេលដែល Router ទទួលយក packet ដែលបានកំណត់ទុកសម្រាប់ 192. 168.100 .10/24 ។ Router A ជាអ្នកកំណត់គោលដៅសម្រាប់ interface (192.168.10.1 ឬ 192.168. 15.1) មិនមែន network ទេ។ ក្នុងការ configure Router A ដើម្បីបញ្ជូន packet ទៅកាន់ Router B យើងមានមធ្យោបាយបីគឺ

- *Default Route* គឺវាដូចទៅនិងdefault gateway ដែរ។ វាអាច configure ទៅកាន់ interface 192.168.15.5 របស់ Router B។

- *Static Route* គឺថា Router A អាចមាន Entry មួយអាចកំណត់ packet ទុកសម្រាប់ 192.168.100.0 ហើយ network បញ្ជូនឆ្ពោះទៅកាន់ Router B.
- *Dynamic Routes* វាប្រើ dynamic routing protocol ដើម្បីគ្រប់ដណ្តប់ទៅលើ192.168.100.0 ហើយ network អាច access ចំពោះ Router B បាន។

១៧-៣- Dynamic Routing

Dynamic routing ធ្វើការទៅតាមការហៅរបស់ Router Discovery ដែលបានរកឃើញជាស្វ័យប្រវត្តនូវ routers ដទៃដែលបាន configure សម្រាប់ Dynamic routing ។ វា អាចចែកចាយព័ត៌មានទៅកាន់ network ដទៃដែល access តាមរយៈ interface និងការប្រើប្រាស់ព័ត៌មានទាំងនោះដោយបង្កើត dynamic routing table។ Dynamic routing អាចដោះស្រាយបញ្ហាដែលមាននៅលើ network ដូចជាការផ្លាស់ប្តូរ protocols។ Windows Server 2008 មានការគាំទ្រទៅនិង Routing Information Protocol (RIP) version 2 ដូចនិង dynamic routing protocol សម្រាប់ IPv4។

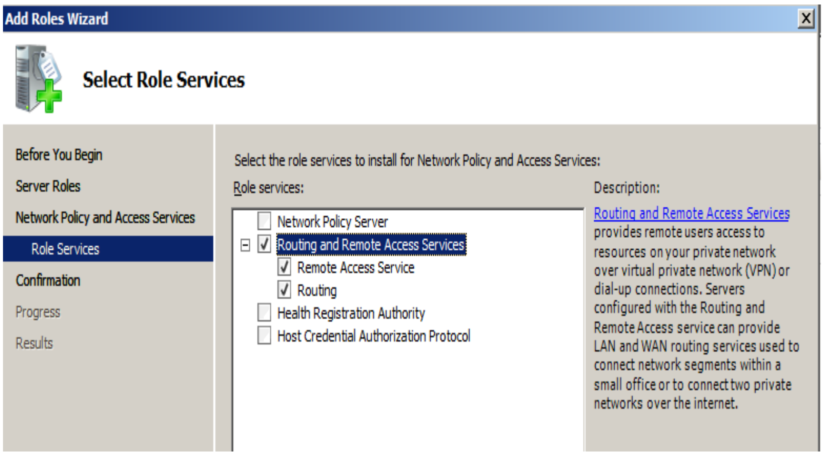
១៧-៣-១- Routing Information Protocol

RIP គឺជា dynamic routing protocol ដែលងាយស្រួលក្នុងការ configure ។ RIP បានធ្វើការ configure ដើម្បី broadcast នូវតារាងដែលបានស្គាល់អំពី Network របស់វា ។ Router បានទទួលយក messages និងបន្ថែម route មួយទៅឱ្យ Networks នៅក្នុង Routing table ផ្ទាល់របស់វា។ RIP ប្រតិបត្តិក្នុង mode មួយក្នុងចំណោម modes ពីរគឺការ Update តាមខួបនិងការ Update ជាស្វ័យប្រវត្តិ។ Update តាមខួបបានធ្វើការ update បញ្ជូនលើមូលដ្ឋានគ្រឹះនៃខួបមួយកំណត់យ៉ាងច្បាស់ដោយ administrator។ នេះជាការកំណត់ជា default សម្រាប់ RIP ប្រសិនបើ route មិនដំណើរការនោះការ update និងមានបញ្ហាដូចជា route និងលុបចេញពី routing table

Installing Routing និង Remote Access

មុននិងអ្នកអាច configure RRAS អ្នកត្រូវ install RRAS ជាមុនសិន។ សូមធ្វើតាមជំហានដូចខាងក្រោម៖

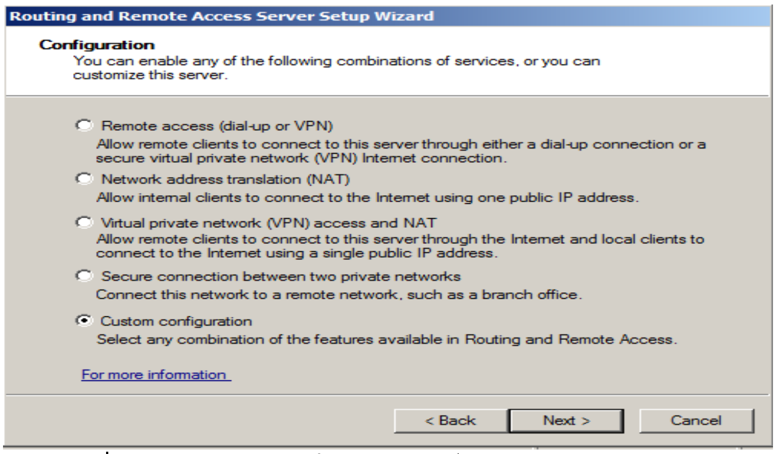
1. បើក Server Manager
2. ចុចលើ Add Roles link ដើម្បីដំណើរការ Add Roles Wizard.
3. ចុចលើ Next
4. ជ្រើសរើសយក Network Policy and Access Services នៅលើ Select Roles screen ហើយបន្ទាប់មកចុចលើ Next.
5. ចុចលើ Next នៅលើ Introduction to Network Policy and Access Services screen.
6. ជ្រើសរើសយក Routing and Remote Access Services on the Select Role Services screen (រូបភាព ១១-២)ហើយបន្ទាប់មកចុចលើ Next.
7. Confirm the installation options and click Install.
8. ចុចលើ Close នៅពេលការដំឡើងបានបញ្ចប់



Configuring and Enabling RRAS

យើងអាច configure RRAS សម្រាប់ LAN routing និង RRAS services ដោយអនុវត្តដូចខាងក្រោម

1. ចុចលើ Routing and Remote Access ពី Administrative Tools Start menu item ដើម្បីបើក Routing and Remote Access management console.
2. ចុចដោយប្រើប៊ូតុងMouse ខាងស្តាំលើឈ្មោះរបស់ server ហើយជ្រើសរើសយក Configure and Enable Routing and Remote Access ។ នេះបង្ហាញពីការបើក Routing and Remote Access Server Setup Wizard.



3. ចុចលើ Next ចំពោះអេក្រង់ដែលបានបង្ហាញពីការស្វាគមន៍
4. ជ្រើសរើសយក Custom Configuration នៅលើ Configuration screen ដូចបានបង្ហាញក្នុងរូបភាព១១-៣ ហើយចុចលើ Next.
5. ជ្រើសរើសយក LAN Routing ពី Custom Configuration screen(រូបភាព១១-៤)ហើយបន្ទាប់មកចុចលើ Next.
6. ចុចលើ Finish
7. ជ្រើសរើសយក Start Service នៅពេលដែលវាបង្ហាញឱ្យ start RRAS service.

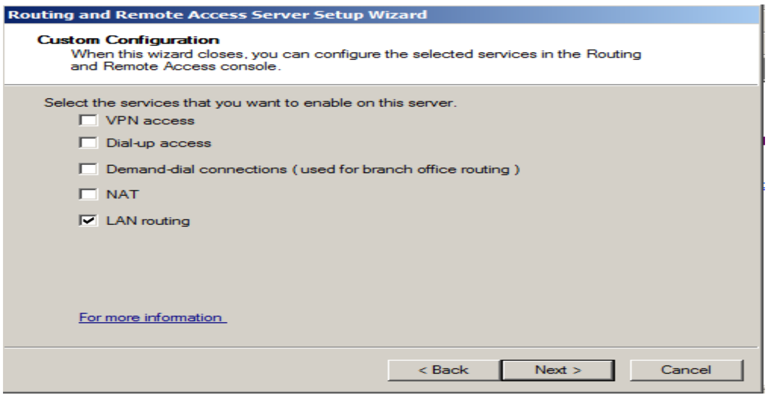
Configuring Network Interface for Routing

នៅពេលបើក Routing and Remote Access management console ហើយ Expand លើកុំព្យូទ័រ name ។ យើងនិងឃើញ nodes 4 នៅក្នុង navigation tree ដូចជា

- Network Interface

- Remote Access Logging & Policies
- IPv4
- IPv6

ដូចដែលបានបង្ហាញ Figure 11-5



រូបភាព១១-៤ បង្ហាញពីការជ្រើសរើសយក LAN Routing

ដោយចុចលើ Network Interface យើងអាចធ្វើការភ្ជាប់ ការផ្តាច់ បើកឬបិទនៅ interface មួយចំនួន។ ហើយមាន network protocol សំខាន់ៗចំនួនពីរដែលគាំទ្រនិង Windows Server 2008 គឺ IPv4 និង IPv6។ នៅពេលដែលអ្នកពង្រីកទៅលើ protocol អ្នកនិងឃើញ item ចំនួនពីរគឺ General និង Static Routes។ ហើយ General option បានបង្ហាញ Interface នីមួយៗម្តងទៀត។ ដោយវាបង្ហាញនូវឈ្មោះរបស់ interface ប្រភេទ IP addresses ចំនួន bytes ដែលកំពុងទទួល bytes ដែលកំពុងបញ្ជូនចេញ ការច្រោះ លក្ខណៈនៃការគ្រប់គ្រងនិងលក្ខណៈនៃដំណើរការ (រូបភាព១១-៦)។ អ្នកអាចស្វែងរកដើម្បីបន្ថែមព័ត៌មានដោយចុចលើប៊ូតុង Mouse ខាងស្តាំលើ interface និង ជ្រើសរើសយក item ដែលសមរម្យ។ Item ដែលបានបង្ហាញរួមមានTCP /IP information, address translation, IP addresses, IP routing tables,TCP connection, and UDP listener ports។ ដើម្បី additional properties ទៅឱ្យ interface network មួយយើងត្រូវ double click ទៅលើ interface។ IPv4 propertiesបានបង្ហាញនូវ across tabs ចំនួនបី: General ,Multicast Boundaries ,និងMulticast Heartbeat ដូចដែលបានបង្ហាញក្នុង(រូបភាព១១-៧)។

រូបភាព១១-៥-Routing and Remote Access Interface

ពេលវេលាស្ថិតនៅ(TTL)និងការកំណត់នៃការរកឃើញ។ General Tab មានភ្ជាប់ជាមួយនៃទំហំព័ត៌មាន មានន័យថាគឺស្វែងរកតែកំហុសក្នុងការគ្រប់គ្រងកុំព្យូទ័ររបស់អ្នក។ ការកំណត់ទាំងនេះបានពិណ៌នានៅក្នុងតារាង (រូបភាព ១១-១)។

១៧-៤- Routing Protocols

Window Server 2008 បានផ្តល់នូវ protocol មួយចំនួនដែលគាំទ្រទៅនិងវាដូចជា

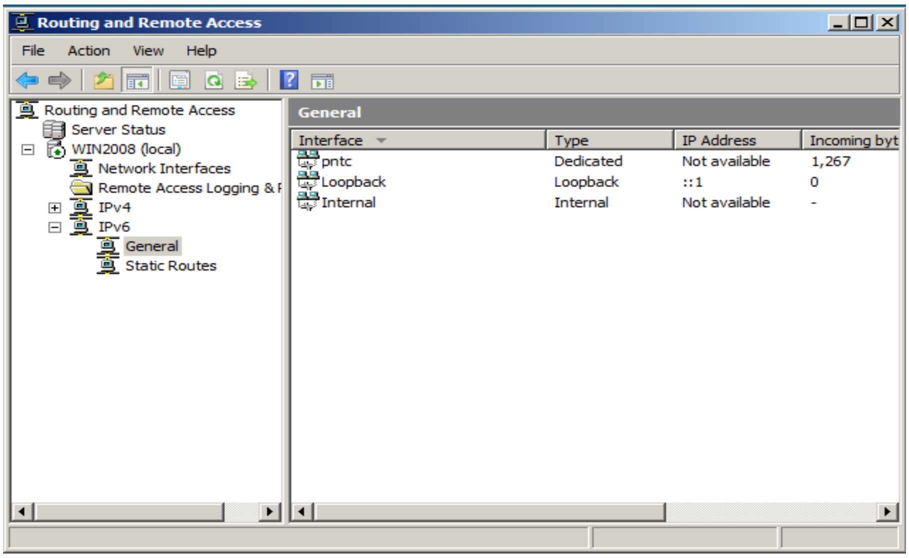
-Dynamic Host Configuration Protocol(DHCP) Relay Agent

-ភ្នាក់ងារបញ្ជូនបន្តរបស់DHCPv6

-ក្រុមអ្នកគ្រប់គ្រងInternet (IGMP)Router និង Proxy

-NAT

-RIPv2សម្រាប់ Protocol Internet ។

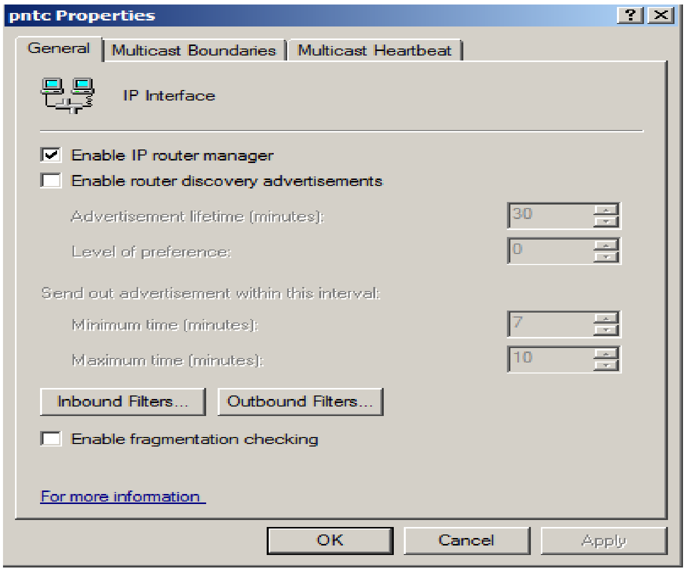


រូបភាព១១-៦-Ipv4 General network interface information

ភ្នាក់ងារបានរត់បណ្តាក់គ្នាលើ DHCP ជួយសម្រួលដល់ការឆ្លោះទៅកាន់ Router DHCP មានទាំងស្តង់ដារ IPv4 និង IPv6 ស៊េរីថ្មី ។ IGMP គឺត្រូវបានគេប្រើប្រាស់វិភាគទៅលើ Routers និងគ្រប់គ្រងទៅលើ Multicast Group។ NAT ជាធម្មតាត្រូវបានប្រើប្រាស់នៅពេល ដែលអ្នកចង់តភ្ជាប់រឹលាក់ចំនួនលេខនៃ internal host ពី network ផ្សេងៗទៀត ។ ឧទាហរណ៍ ប្រសិនបើអ្នកចង់តភ្ជាប់ Internet ទៅ កុំព្យូទ័រ របស់អ្នកគឺត្រូវតែកំណត់ IP Address មួយតែប៉ុណ្ណោះដែលអ្នកអាចប្រើប្រាស់ NAT បកប្រែ Internal IPAddress និងមួយទៀតតាមរយៈ external IP Address។ RIPv2 គឺត្រូវបានប្រើប្រាស់សម្រាប់ dynamic route រុករកនៅចន្លោះ Routers ចាប់ពី15 Router ឡើងទៅ។

Hands-on Exercise :Installing and Configure RIPv2 for IP

នៅក្នុងលំហាត់នេះពួកយើងដំឡើង RIPv2 សម្រាប់ IP និងរូបសណ្ឋានផ្សេងៗគ្នា។ យើង configure RIP ដើម្បីធ្វើការតែមួយគត់ជាមួយនិង RIPv2-compatible routers ឱ្យបង្កើនបានលទ្ធផលល្អ។

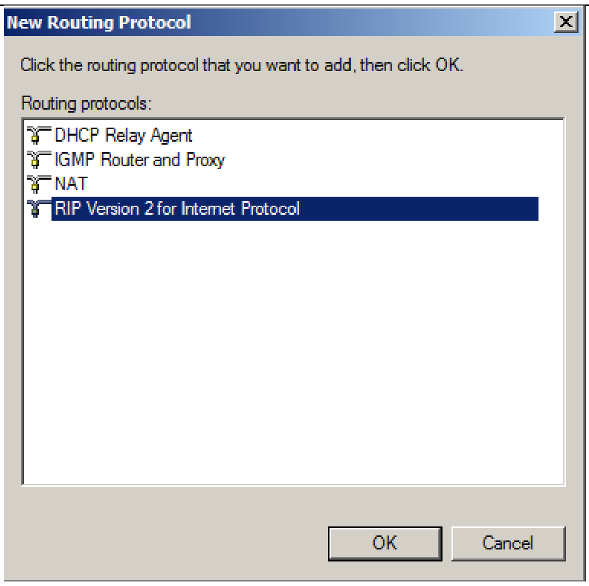


រូបភាព 11-7 IPv4 network interface properties

1. បើកRouting និងការគ្រប់គ្រងRemote Access console
2. ពង្រីកលើឈ្មោះ Server របស់អ្នក
3. ពង្រីក IPv4
4. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំហើយយកGeneral ហើយជ្រើសយក New Routing Protocol
5. ជ្រើសរើសយក RIP Version 2 សម្រាប់Internet Protocol (គំនូស 11-8) ហើយចុច OK
6. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ RIP icon ដែលទើបនិងបង្កើតថ្មី នៅពីក្រោម IPv4 ហើយ Select New Interface
7.Select Local Area Connection ហើយចុចOk(គំនូស11-9)
8. Select Periodic Update Mode ដូចវិធី Operation Mode
9. Select លើ RIP version 2 Multicast សម្រាប់សំនុំរបស់ Protocol

Setting	Description
Enable IP Router	ការដោតភ្ជាប់ដើម្បីបញ្ជូនទៅ Interface នេះចូលរួមប្រតិបត្តិការក្នុង IP address ។ វាជា Administrator ដែលមានសមត្ថភាពខ្ពស់សម្រាប់ឱ្យវាដំណើរការនិងបិទវាចោលវិញ។ លុះត្រាតែប្រអប់ដែលបានគូសននេះប្រាប់ពីព័ត៌មានដែលទាក់ទងនិង អាចឱ្យជ្រើសរើសយក។
EnableRouter Discovery Advertisements	ការកំណត់ដើម្បីបញ្ជូន Router ដោយស្វ័យប្រវត្តជួយឱ្យ Router រក ឃើញ Router តាមរយៈសារ។ នៅពេលពិនិត្រវាមានសមត្ថភាពដើម្បីផ្សព្វផ្សាយនូវអ្វីដែលទាក់ទងOption ។
Advertisement Lifetime (Minutes)	បង្ហាញអំពីលេខនៃការផ្សព្វផ្សាយត្រឹមត្រូវ។កាលណាការប្រកាសផុតកំណត់វាមិនពន្យាពេលក្នុងការទទួលយកតាមរយៈ Client ។
Level of Preference	កំណត់តម្លៃប្រាប់ Router នូវ Level នៃការចូលចិត្តប្រើ។ មាន Client ច្រើនដែលនិយមប្រើជាមួយ Router នេះ។

SendOut Advertisements Within This Interval	កំណត់ពេលវេលានៅចន្លោះ អប្បបរមានិងអតិបរមានៅពេលមានព័ត៌មានបានផ្ញើរ។នេះជាតម្លៃដែលផ្តល់ដោយ Router ក្នុងពេលមួយដោយចៃដន្យដែល Router ទាំងអស់ផ្តល់ព័ត៌មានក្នុងពេលដូចគ្នានោះ
Inbound Filters	ការកំណត់តម្រង់សំនុំណាមួយដែលព្រមទាំងស្រុងចំពោះInterface នេះ។ ឧទាហរណ៍អ្នកអាចបិទរាល់ traffic ទាំងអស់ដែលមកពី Network និងកំណត់ដោយ Protocol ដូចគ្នា។
Outbound Filters	ការងារ Inbound Filters លើកលែងអនុវត្តទៅក្រៅ packet តាម Interface នេះ។
Enable Fragmentation Checking	តាមរយៈ Router ដែលបានបិទ Packet នីមួយៗដែលមានប្រយោជន៍ ទប់ស្កាត់ Denial-to-service ចូលទៅផ្នែកនៃសំនុំ។ការប្រើបែបនេះត្រូវ ប្រយ័ត្ន ព្រោះការអនុវត្តប្រើ Fragmented Packet និងអាចជ្រើសរើស ទប់ស្កាត់ Application សម្រាប់ទំនាក់ទំនងគ្នា។



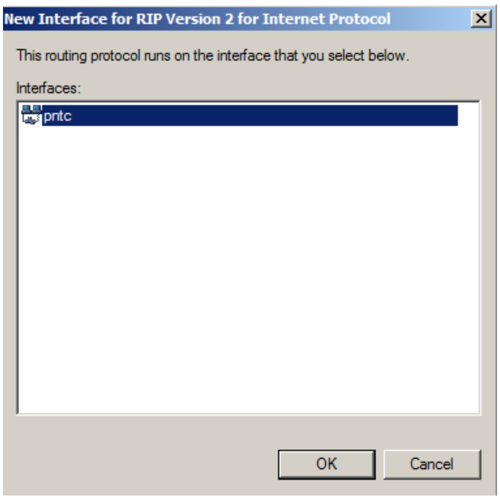
រូបភាព 11-8 Installing RIPv2 for IP

10. Select លើ RIP Version 2 ហើយកំណត់បញ្ចូលPacket Protocol ។ General Tab នឹងបង្ហាញលើគំនូសទី 11-10។

11. ចុចលើ Security tab ហើយបង្កើតការបញ្ជូនទាំងអស់ដែលព្រមទទួល incoming route និង routes ទាំងអស់ត្រូវបានប្រកាសសម្រាប់Outgoing routes(គំនូសទី11-11)។

12.ចុចលើ Neighbors tab។ នៅទីនេះអ្នកអាចឱ្យអត្ថន័យទៅលើ Router និងមានអន្តរកម្មជាមួយ RIP Router ដទៃទៀត ។ ជ្រើសរើសដោយប្រើ Broadcast រឺ Multicast , មួយប៉ុណ្ណោះដូចបានបង្ហាញនៅក្នុងគំនូស11-12។ ប្រសិនបើអ្នកចង់ផ្តល់នូវភាពជាក់លាក់របស់ Router អាចទំនាក់ទំនងជាមួយ RIP ណាមួយ អ្នកអាចចូលទៅ IP Address របស់Neighbors ។

13. ចុចលើ advanced tabs ប្តូរ Periodic Announcement Interval រយៈពេល 60នាទីបន្ទាប់មកចុចលើ OK ហើយ Save (តំនួស 11-13)។



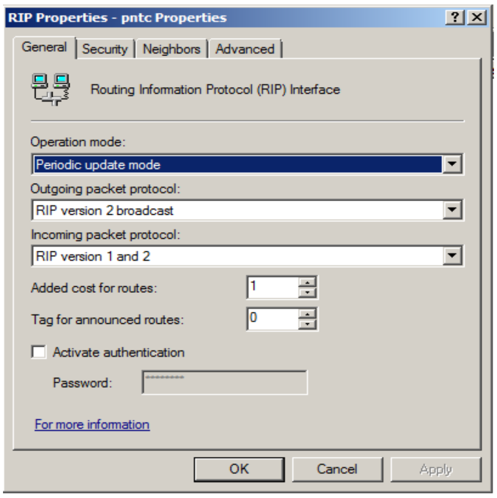
រូបភាព 11-9 Creating a new RIPv2 interface

សូមពិនិត្យមើល RIPv2 Properties

លំហាត់ពីមុនបានបិទបាំងការដំឡើងនឹងការភ្ជាប់ RIPv2 សម្រាប់ IP ទៅលើ Server 2008 វាមានចំនួនយ៉ាងតិចប៉ុណ្ណោះដែលបានបិទការកំណត់សម្រាប់ RIPv2។ ក្រលេកមើលភាពជិតជិតផ្សេងៗគ្នានៃការងារអ្នកអាចកំណត់ហើយលទ្ធផលវាមាននៅលើលក្ខណៈនៃ RIP **(តំនួស11-10)**។

អ្នកអាចប្តូរការកំណត់ជាបន្តបន្ទាប់ដែលមាននៅលើ General tab ដូចជា៖

+Operation Mode អាចជា Periodic Update (Default សម្រាប់ LAN របស់កុំព្យូទ័រ) Auto-Static Update (Default សម្រាប់ demand-dial interfaces)។ ជាធម្មតាអ្នកចង់ Auto-Static ដរាបណាការទាក់ទងគឺមិនបានតភ្ជាប់ ប៉ុន្តែអ្នកចង់ឱ្យRouter របស់អ្នកស្ថិតនៅចន្លោះនៃការ update នៅពេលធ្វើការតភ្ជាប់ទៅខាងក្រោម



រូបភាព 11-10 RIP Properties General Tab

-Outgoing Packet Protocol:គ្រប់គ្រងសំនុំ RIP បញ្ជូនចេញមក Router ។ RIPv2 Multicast ភាគច្រើនមានសមត្ថភាពប្រើប្រាស់ Multicast ច្រើនជាង broadcast ដែលបញ្ជូនទៅ Updates ឱ្យ router។ RIPv1, RIPv2 broadcast ជាវិធីធម្មតាសម្រាប់សំនុំ broadcasting RIP ។ អ្នកគួរតែជ្រើសរើសយកRIP Version 1 Broadcast

តែមួយប្រសិនបើអ្នកត្រូវការភាពចុះសំរុងជាមួយនឹង RIPv1 router។ Silent RIP អាចជ្រើសរើសបានផងដែរ ប្រសិនបើអ្នកមិនចងឱ្យ router នេះបញ្ចូលទៅ RIP advertise-ment ណាមួយ។ ទាំងនេះវាមានប្រយោជន៍ ប្រសិនបើអ្នកធ្វើតាមការណែនាំរបស់ router ហើយទទួលព័ត៌មានពីក្នុង router ផ្សេងទៀតប៉ុន្តែវាមិនមានចំនែកក្នុងតារាងជាមួយនឹងអ្វីមួយផ្សេងទៀត ។

-Incoming Packet Protocol: ប្រាប់ឱ្យដាក់លាក់ថាតើត្រូវ PIPv1, RIPv2 មួយណារីសេចក្តីជូនដំណឹងទាំងពីរប្រភេទនៃ RIP។ អ្នកអាចមិនអើពើចំពោះសំនុំដែលបានបញ្ជូនចូលមកប្រសិនបើជ្រើសរើសយកការមិន update មកពី router ណាមួយផ្សេងទៀត។

-Added Cost for router:បន្ថែមតម្លៃទាំងស្រុងទៅលើinterface នេះ។ ត្រូវយកចិត្តទុកដាក់នៅពេលធ្វើការប្រើប្រាស់នេះប្រសិនបើការវាយតម្លៃនេះត្រូវបញ្ចប់ដល់កម្រិតខ្ពស់routerប្រហែលជាមិនត្រូវបានប្រើប្រាស់ទាំងអស់។

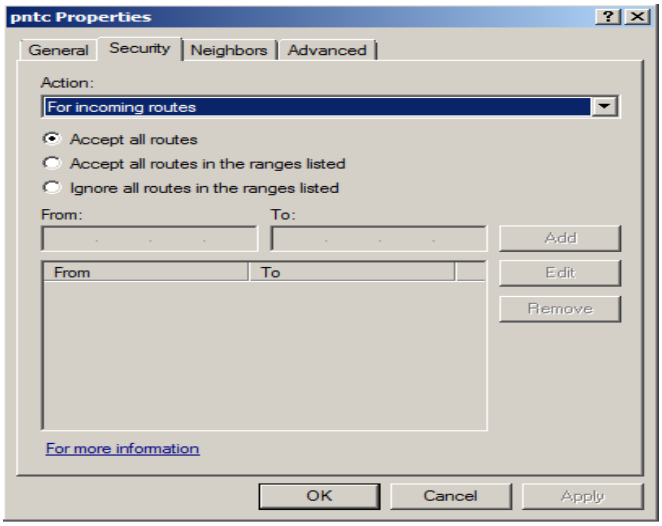
នៅទីនេះអ្នកអាចធ្វើការភ្ជាប់ ផ្តាច់ការភ្ជាប់ បើកឬក៏បិទលើផ្នែកណាមួយនៃ Hardware របស់កុំព្យូទ័រ ដែលជាទូទៅការប្រើប៊ូតុងរបស់ Mouse ខាងស្តាំទៅលើ Interface ហើយធ្វើការជ្រើសរើសឱ្យបានត្រឹមត្រូវ។ តាំងពីមុនមកដល់ឥលូវយើងមានកង្វះច្រើនអំពី routing ហើយវាដំណើរការវែងឆ្ងាយដែលវារំលងដំណើរការនៃការកត់ត្រានិងគោលការណ៍។ ពីរចំណុចដែលសំខាន់គឺ IPv4 និង IPv6 ដែលត្រូវបានជ្រើសរើស។ Protocol ទាំងពីនេះគឺវាគាំទ្រជាមួយ Window server 2008 ។

នៅពេលអ្នកពង្រីក Protocol ទាំងពីរនេះអ្នកនិងឃើញហេតុការណ៍ពីរចំណុច General និង Static Routes ។ General វាបង្ហាញពី Interface ម្តងទៀតប៉ុន្តែពេលដែលវាបង្ហាញនេះគឺចំពោះព័ត៌មានដែលមានលក្ខណៈសំខាន់ដល់ Protocol នៅលើ Interface Network តែប៉ុណ្ណោះ។វាបង្ហាញអំពីឈ្មោះ Interface ប្រភេទ IP Address ចំនួន Bytes ដែលកំពុងទទួលបាន ចំនួន Bytes ដែលកំពុងបញ្ជូនចេញនិងលក្ខណៈនៃការគ្រប់គ្រងហើយនឹងមានប្រតិបត្តិការខ្ពស់ (**គំនូស 11-6**)។ អ្នកនិងអាចធ្វើការសួរទៅលើ interface Network ដើម្បីធ្វើការស្វែងរកព័ត៌មានបន្ថែមដោយគ្រាន់តែធ្វើការប្រើប៊ូតុង Mouse ខាងស្តាំហើយជ្រើសរើសលើចំនុចនោះ។ ចំនុចនោះបានបង្ហាញពីការដាក់បញ្ចូលព័ត៌មាន TCP/IP,Address translation,IP Address ,IP routing table ,TCP Connections ,និងUDP Listener ports។

ការបន្ថែម Properties អំពី Interface network អាចទទួលបានដោយគ្រាន់តែចុចពីរដងស្ទួនគ្នាទៅលើ Interface។ ក្នុងបរិវេណ IPv4 បានបង្ហាញពីការឆ្លងកាត់ Tabsបីគឺ: General Multicase,Bounderies និង Multicast Heart beat ដែលបានបង្ហាញនៅក្នុង(**គំនូស11-7**)។ បន្ទាប់មកមានTabs ពីរដែលមានគុណភាពក្នុងការបញ្ជូន Multicasting នៃIPv4 និងធ្លាប់បានប្រើប្រាស់នូវទំហំឯកសណ្ឋានរបស់វា។

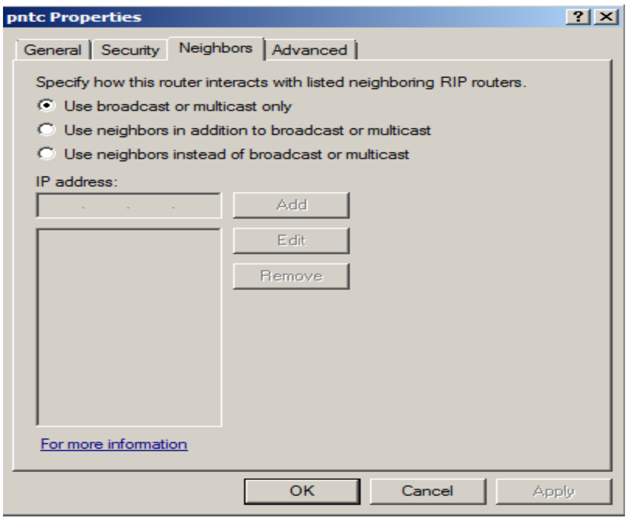
Tag for Announced Routes: ការបញ្ជូនដោយធ្វើការបង្ហាញប្រាប់ពីប្រព័ន្ធដំណើរការ។ លក្ខណៈនេះគឺមិនអាចប្រើបាននៅក្នុង Window Server 2008 ប៉ុន្តែអាចប្រើតាមវិធីផ្សេងទៀតបាន។

- Activate Authentication/Password:គឺជាការបង្កើតPassword មួយដែលសម្រាប់ការពាររាល់ការ Update ពីការកើតឡើងនៅក្នុងពេលដំណើរការលុះត្រាតែគេដាក់ Password បានត្រឹមត្រូវ។ ទាំងអស់នេះនឹងអាចមានគុណប្រយោជន៍សម្រាប់ការពារនូវការកើតឡើងដោយចៃដន្យពីការ Update នៅចន្លោះពេលដំណើរការដែលយើងមិនបាន ដឹង។ ម៉្យាងវិញទៀតរូបភាពដែលបានបង្ហាញគឺពុំបានគិតអំពី Security តាំងពីការបញ្ចូល Password ផ្ញើរទៅខាងក្រៅនៅក្នុង Clear Text។



រូបភាព 11-11 RIP properties Security tab

- ប្រព័ន្ធការពារនេះនឹងជួយការពារអ្វីៗទាំងអស់ដែលធ្វើឱ្យ RRAS ទទួលយកបាន។ ប្រសិនបើ Network របស់អ្នកមួយនេះមានភាពល្បីល្បាញ (មួយណាដែលនឹងត្រូវធ្វើវា) ហើយអ្នកគួរតែត្រូវកំណត់នូវការទទួលយករីប្រព័ន្ធដំណើរការណាដែលមានការចាប់អារម្មណ៍ ហើយធ្វើការយ៉ាងច្បាស់លាស់ទៅលើ Networks ដែលអ្នកបានដឹងអំពីវា។ នេះអាចជួយការពារហើយធ្វើការប្រឆាំងនឹង Error ដែលកើតមានលើការផ្ញើរព័ត៌មានមិនបានត្រឹមត្រូវ ។

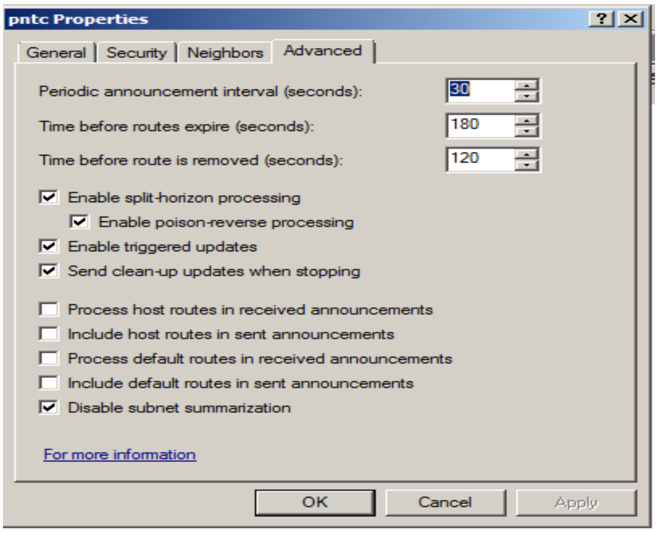


រូបភាព 11-12 RIP properties Neighbors tab

ការពិពណ៌នាខាងលើបង្ហាញអំពី Properties នីមួយៗនៅលើ Security Tab ដែលបង្ហាញរូបនូវ (11_11) :

- Action : ជាការប្រកាសនៃការអនុវត្តចូលក្នុង Setting រឺតាមវិធីផ្សេងទៀត។
- Accept/Announce all Routes: ទោះជាមានអ្វីទាំងអស់នៅក្នុងប្រព័ន្ធដំណើរការច្បាស់លាស់ ដោយមានការទទួលស្គាល់ រឺធ្វើការប្រាប់តាមវិធីផ្សេងទៀត។
- Accept / Annouce All Route in the Ranges listed : ធ្វើការបើក Fields ដែលអ្នកអាចបន្ថែមនូវ IP Ranges ដែលអ្នកនឹងត្រូវធ្វើការបញ្ជូន រឺ ធ្វើការ Update តាមវិធីផ្សេងទៀត។

_ Ignore/Do not Announce All Routes In the Ranges Listed : ផ្ទុយមកវិញ នៃការ Accept/Announce គ្រប់ដំណើរការទាំងអស់គឺស្ថិតនៅក្នុង Ranges Listed។



រូបភាព 11-13 RIP properties Advanced tab

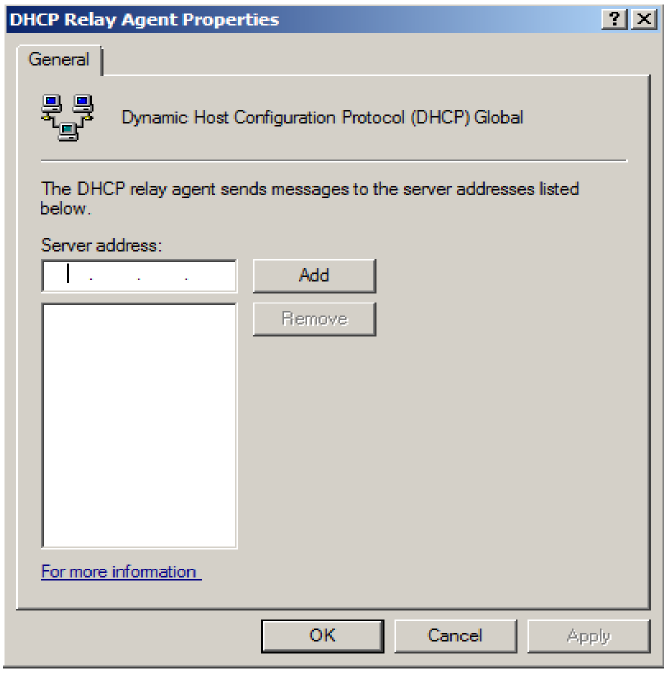
ទោះបីជា RIPv2 អាចប្រើបានដោយគ្មាន Broadcast ឬ Multicast ពេលផ្ញើរឬទទួលព័ត៌មានពីប្រព័ន្ធដំណើរការជាច្រើនដែលមានភាពល្អប្រសើរនៃ RIP, អ្នកក៏អាចបង្កើតការupdate បន្ថែមថ្មីៗដែលមានសមត្ថភាពបានពីការចង្អុលបង្ហាញពីអ្នកដែលនៅជិត។ ក្នុងការបង្ហាញនេះអ្នកអាចបញ្ជាក់យ៉ាងច្បាស់ទៅកាន់ router ណាដែលអ្នកចង់ផ្ញើរព័ត៌មានដែលទាក់ទងនិងការUpdateនេះជាការកាត់បន្ថយបរិមាណនៃការធ្វើចរាចរដែលបានបង្កើតដោយ RIP ហើយនិងផ្តល់ឱ្យអ្នកសម្រាប់ធ្វើការត្រួតពិនិត្យយ៉ាងច្បាស់លាស់ដែលជាអ្នកធ្វើការទំនាក់ទំនងជាមួយ Routers។

- Use Broadcast or Multicast Only ដាក់កំណត់ RIP ធ្វើការប្រើប្រាស់ Broadcast និង Multicast តែមួយគត់សម្រាប់ប្រកាសប្រាប់ប្រព័ន្ធព័ត៌មាន។ នេះគឺជាការកំណត់ជា default
- Use Neighbors in Addition to Broadcast or Multicast ផ្តល់ឱ្យអ្នកកំណត់នូវ Neighbors ទៅកាន់ router មួយណាដែលនិងប្រកាសនូវ route ដោយផ្ទាល់។ ប៉ុន្តែវានៅតែបន្តធ្វើការប្រកាសប្រើ Neighbors ជំនួសឱ្យ Broadcast ឬ Multicast ធ្វើការកំណត់លើដំណើរការតែមួយលើប្រព័ន្ធដំណើរការព័ត៌មានទៅកាន់ IP Addressច្បាស់លាស់។

Advanced Tab ផ្ទុកលេខនៃProperties ពិសេសដទៃទៀតរបស់RIPដែលអាចប្រើនិងធ្វើការធ្វើតាមសេក្តីលំអិត។

- Periodic Announcement Interval (Seconds): លេខដែលនៅចន្លោះទី2នៃ Announcements
- Time Before Route Expire (Seconds): ការសរុបពេលវេលាមុនពេលប្រព័ន្ធដំណើរការដល់កម្រិតនៃការផុតកំណត់។ បើសិនជា Router ទទួលយកនូវការUpdate សម្រាប់ Route វានឹងធ្វើការកំណត់ឡើងវិញនូវចំនួននៃRouter ដូចនេះចំនុចនេះសម្រាប់តែRoute តែមួយគត់ដែលអ្នកមិនទទួលយកការ Update ។

- Time Before Route IS Removed (Seconds): មុនពេលផុតកំណត់ចំនួនពេលវេលារបស់ប្រព័ន្ធដំណើរការត្រូវបានលុប ដោយទទួលបានជោគជ័យពី Routing Table
- Enable split-horizon processing:ចុចបើកនូវទ្រង់ទ្រាយដើមរបស់វានិងធ្វើការការ ពារនូវប្រព័ន្ធដំណើរការ loop ពីព្រោះ spit-horizon processing ការពារ broad -casting អំពីដំណើរការដាក់លាក់នៅលើsegmentពីកន្លែងដែលវាធ្លាប់បានធ្វើការឆ្លងកាត់ហើយ។
- Enable Poison-Reverse Processing: នៅពេលដែលប្រើវាជាចំណុចប្រសព្វជា មួយ spit-horizon (សំដៅទៅកាន់ dependency)ការពារប្រព័ន្ធដំណើរការloopsដោយបាន broadcasting រួចមកពី Network មួយ វានិងជួប unreachable(matric 16)។
- Enable Triggered Updates:រក្សាRouter របស់អ្នកធ្វើការ updateជារៀងរាល់ថ្ងៃឱ្យបានឆាប់រហ័សតាមដែលអ្នកអាចធ្វើបានហើយដោយធ្វើការបង្ហាញភ្លាមៗរាល់ពេលដែលផ្លាស់ប្តូរrouterម្តងៗ
- Send Clean-Update When Stopping: នៅពេលបើក RRAS ដើម្បីបង្ហាញពីប្រព័ន្ធដំណើរការណាមួយ
- Process Host Routes in Received Announcement : ជាទូទៅ RRASស្គាល់នូវបណ្តា host-specific នៅក្នុងប្រព័ន្ធព័ត៌មានដែលវាទទួលបានក្នុងការផ្សព្វផ្សាយព័ត៌មានប្រសិនបើអ្នកចង់ឱ្យ RRAS ស្គាល់បណ្តា host ច្បាស់លាស់គឺអ្នកអាចកែវាដោយជ្រើសរើសនូវ option។
- Include Host Routes In Sent Announcements:
- Include Default Routes In Sent Announcements: ជ្រើសយក ប្រសិនបើអ្នកចង់ធ្វើការបញ្ជូនទម្រង់ទូទៅដែលបានដឹងពីប្រព័ន្ធដំណើរការសម្រាប់ឱ្យប្រព័ន្ធដំណើរការធ្វើការបង្ហាញដោយផ្ទាល់ខ្លួនរបស់វាផ្ទាល់
- Disable Subnet Summarization:ចំនួននៃពេលវេលា Route មួយត្រូវបានដៅទុក ជាមុននៅពេលផុតកំណត់។ ប្រសិនបើ Routerទទួលយកនូវការ Update ដូចនេះសម្រាប់ Route មួយ។ វាធ្វើការកំណត់ឡើងវិញនូវចំនួននៃ Router ដូចនេះចំនុចនេះគឺសម្រាប់តែ Route តែមួយមួយគត់ដែលអ្នកមិនទទួលយកនូវការ Update។ នៅពេលបាន Checked ប្រាប់ទៅកាន់ RRAS ហើយផ្ញើនូវរាល់ Route Information សម្រាប់ Routers នៅក្នុង Subnet ដទៃ ជាងការសង្ខេបវានៅក្នុងទម្រង់ជា Class-based Network ID។

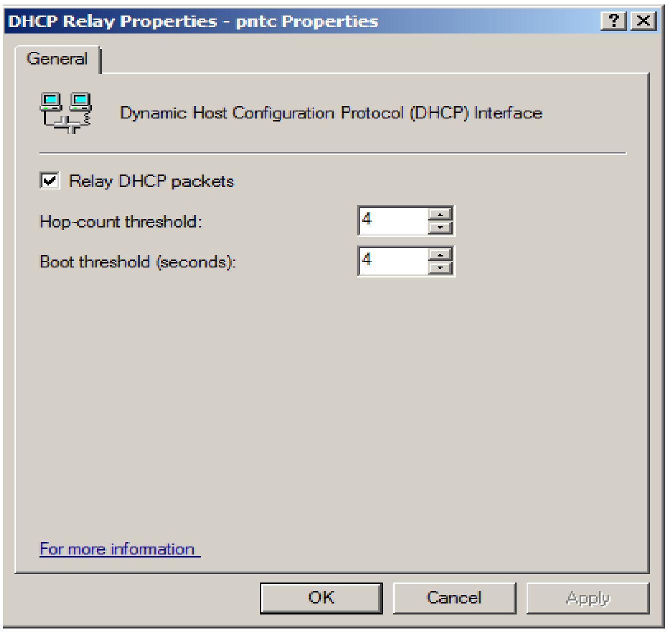


រូបភាព 11-14 DHCP Relay Agent Properties Windows

DHCP Relay Agent:

DHCP Relay Agent ត្រូវបាន Install ដូចដែលអ្នក Install RIP ដែរ លើកលែងតែអ្នកជ្រើសDHCP Relay Agent ជំនួសឱ្យ RIP នៅពេលជ្រើសយកនូវ Routing Protocol។ គោលបំនងនៃ DHCP Relay Agent គឺ អនុញ្ញាតឱ្យកុំព្យូទ័រដែលត្រូវបាន Configure នោះមានការប្រើប្រាស់ IP Address DHCP ទាំងនោះពី DHCP servers នៅក្នុងSubnet ផ្សេងគ្នាដែលត្រូវបំពេញ។ ដើម្បីបែងចែកឱ្យដាច់ស្រឡះថា តើ DHCP មួយណាដែល Replay agent ត្រូវបញ្ជូនទៅកាន់ អ្នកគ្រាន់តែចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំទៅលើ DHCP replay Agent នៅលើ IPv4 នៃ Servers RRAS configuration ចុចយក Properties និងបញ្ចូល IP Address សម្រាប់DHCP server (ដូចបង្ហាញក្នុងរូប ១១.១៤) បន្ទាប់មកអ្នកនឹងអាចបង្កើតInterface សម្រាប់DCHP replay agent ដើម្បី បើកReplay សម្រាប់ Network Interface ជាក់លាក់មួយ។

រូបភាព ១១.១៥ បង្ហាញ Properties សម្រាប់ DHCP Replay Agent Interface ថ្មីដែលបង្កើតជាមួយ Area Location Network Interface។ ក្នុងWindow នេះអាចបើកឬបិទReplay នៃ DHCP packet ក៏ដូចជា Configure hop-count និង boot hold DCHP Replay Agent គឺស្រដៀងគ្នាលើកលែងតែ forwards request ទៅ IPv6 Addressជំនួសវិញ។



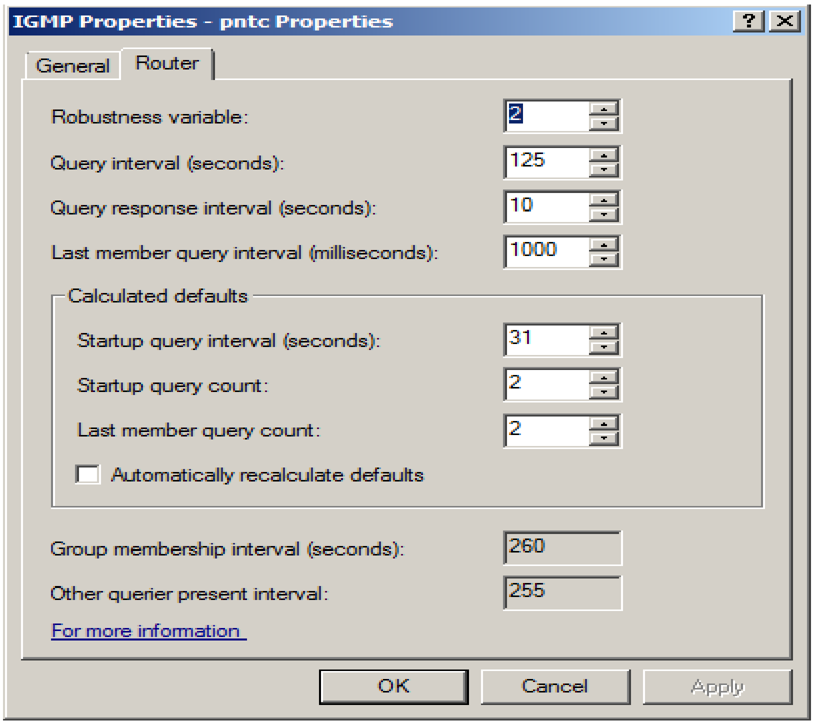
រូបភាព 11-15 DHCP Relay Local Area Connection Properties Windows

១៧-៥- Internet Group Management Protocol

Internet Group Management Protocol (IGMP) នៅក្នុង routing service ផ្សេងទៀតអ្នកអាច install លើ RRAS។ អ្នក Install ហើយអ្នកនិងធ្វើតាម Routing Protocol ផ្សេងៗទៀតសំដៅទៅលើលំហាត់មុនៗដែលយើងបាន Install RIP បន្ទាប់ពី Install រួចអ្នកអាចភ្ជាប់វាទៅនិង Various Network interface ហើយអ្នកអាចបើកឬបិទ IGMP នៅលើ interface ដែលបានផ្តល់ឱ្យ configure នូវម៉ូដរបស់វា (router ឬ proxy) ហើយធ្វើការកំណត់កំណែទម្រង់របស់វា ។ នៅពេល configure ក្នុង IGMP router mode option ផ្សេងៗមាននៅក្នុងក្នុងIGMP Properties Router tab (មើលរូប១១.១៦)។

១៧-៦- Network Address Translation

NAT បានបន្ថែមលក្ខណៈពិសេសទៅ RRAS ក្នុងWindow Serverគ្រប់ទីកន្លែង។ដាក់ស្តែងCable/DSI ស្ទើរតែទាំងអស់ធ្វើការជាមួយ router ក្នុង NAT mode: external interface ត្រូវបាន configure ជាមួយ IP Address ដែលអាចប្រើបានជាផ្លូវការមួយសម្រាប់Internet ហើយជាធម្មតាត្រូវបានconfigured ជាមួយPrivate Address បន្ទាប់មកត្រូវបាន NATED ទៅកាន់ external address។



រូបភាព 11-16 IGMP Properties Router tab

វាអនុញ្ញាតឱ្យកុំព្យូទ័រជាច្រើនអាចចែកចាយនូវ resource និងភ្ជាប់ទៅកាន់ internet តែមួយ។ ជាមួយ Window Server 2008 អ្នកអាចធ្វើការបញ្ចប់ដោយជោគជ័យក្នុងការប្រើប្រាស់ RRAS តែមួយ។ NAT ក្នុង RRAS អាចចែកចាយ IP address ទៅកាន់ interface ណាមួយដែលអ្នកbបានបង្កើតវាឡើងដូច private interface ដូចនេះអ្នកអាចធ្វើការភ្ជាប់ និងអាចធ្វើទៅបានយ៉ាងលឿននិងងាយស្រួល។ ការ configure DHCP ជាអ្នកកំណត់ទីតាំងដែលបានពី NAT Properties window ខាងក្រោមនៃ Address Assignment tab ដូចដែលបានបង្ហាញក្នុង រូបភាព ១១-១៧។

Hands-on Exercise: Installing and configuring NAT

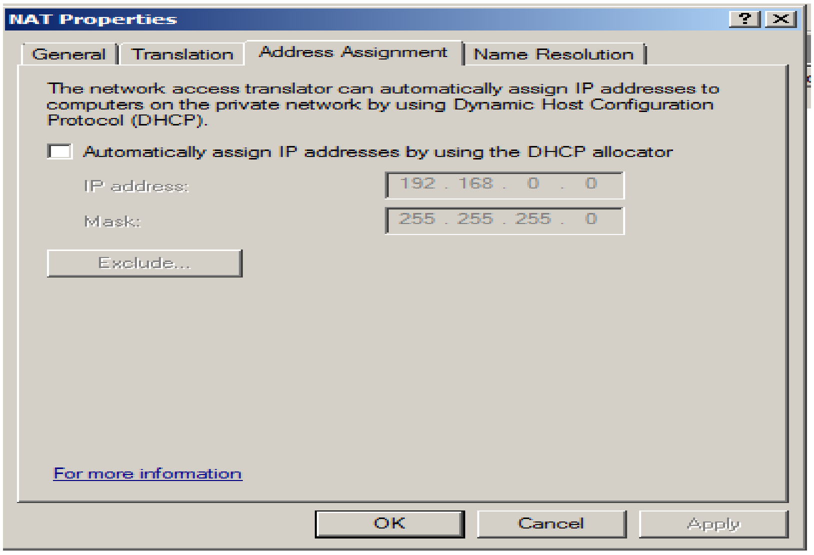
នៅក្នុងលំហាត់នេះ យើងដំឡើង NAT routing protocol។ យើងនឹងមានផ្ទាំងconfigure របស់Network Interface មួយ

១. ត្រូវ install NAT routing protocol ដោយអនុវត្តទៅតាមលំហាត់ដើម្បី Install RIPv2 លើកលែងតែ Select លើ NAT instead of RIPv2 for IP ។

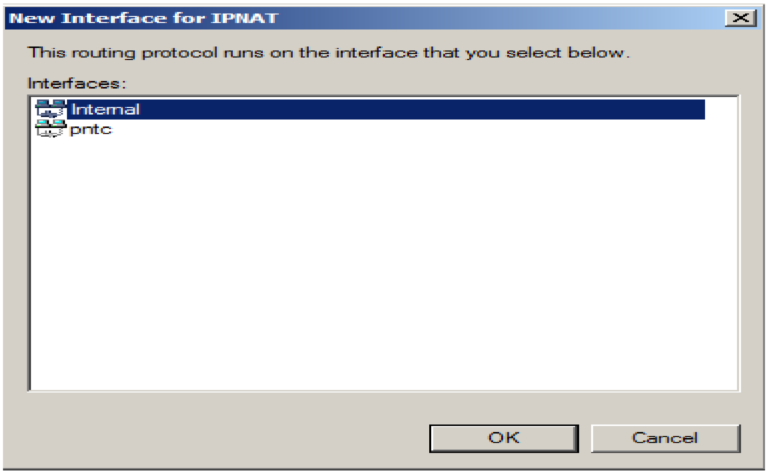
២. នៅក្នុង Routing and Remote Access management console គឺ ពង្រីកលើserver របស់អ្នកហើយពង្រីកលើ IPv4 បន្ទាប់មកចុចដោយប្រើប៊ូតុងMouse ខាងស្តាំលើ NAT ហើយជ្រើសរើសយក New Interface ។

៣.ជ្រើសរើសយក Network Interface របស់អ្នកមួយ។ នៅក្នុងករណីនេះជ្រើសរើសយក Local Area Connection(ដូចរូប ១១.១៨) រួចចុច OK។

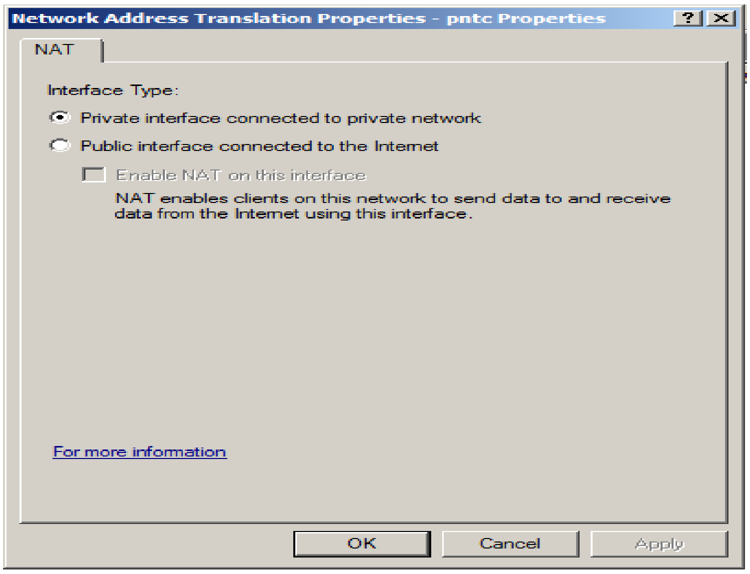
៤. ជ្រើសរើសយកPrivate Interface ភ្ជាប់មកកាន់ Private Network រួចចុចOK(ដូចរូប ១១. ១៩)។



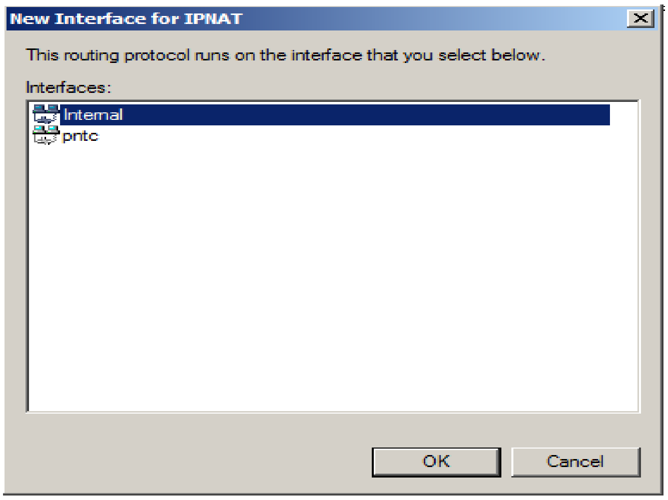
រូបភាព 11-17 NAT Properties Address Assignment tab



រូបភាព១១-១៨ ការបង្កើត IPNAT interface ថ្មី

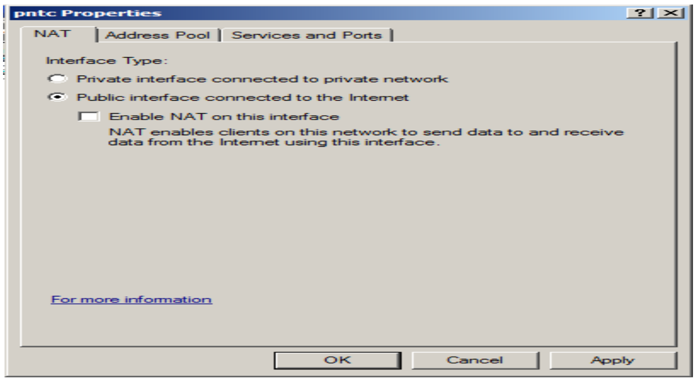


រូបភាព១១-១៩ Configuring private network interface



រូបភាព១១-២០ Creating another new IPNAT interface

៥.ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ NAT រួចជ្រើសរើសយកNew Interface។
៦. ពេលនេះជ្រើសរើសយក Network Interface របស់អ្នកដទៃផ្សេងទៀត វានឹងឃើញ Local Area Connection 2 (ដូចរូប ១១.២០)រួចចុច OK។
៧. ជ្រើសរើសយក Public Interface ដែលភ្ជាប់មកកាន់ Internet រួចគូសទៅលើ Enable NAT នៅលើ Interface នេះដូចបង្ហាញក្នុងរូប ១១.២១។
៨.ចុចលើActive Pool Tab បន្ទាប់ចុចAdd រួច Enter ទៅលើបណ្តុំនៃ IP address នៃISP របស់អ្នក(ដូចឃើញក្នុងរូបភាព១១.២២)។ NAT ប្រើសម្រាប់ RRAS តម្រូវឱ្យអ្នកស្គាល់ external IP ឬ បណ្តុំនៃ IP address របស់អ្នក
៩.ចុចលើ Service និង portsTab ប្រសិនបើអ្នកចង់ឱ្យService Network របស់អ្នកអាចដំណើរការសម្រាប់Internet Users បានប្រើ Tab នេះ ដើម្បីបង្កើត NAT port ។



រូបភាព១១-២១ Configuring external network interface for NAT

១៧-៧- Static Routes

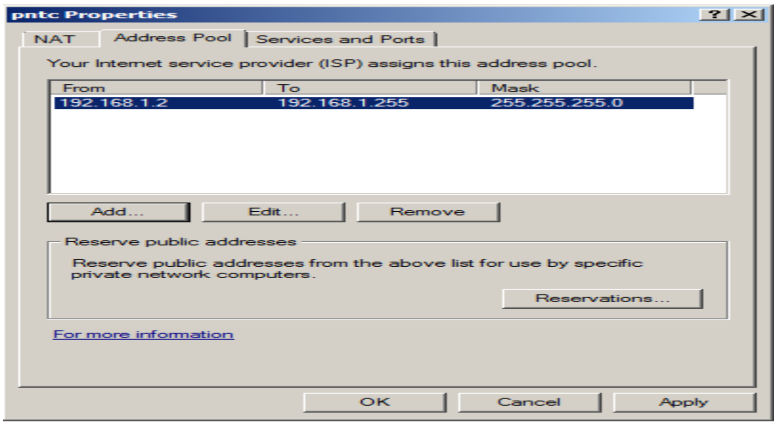
Static Route គឺគ្មាន Codes អ្វីលំបាកនៅលើ Network ឬ Host នោះទេ។ អ្នកអាចកំណត់ Static Routes បានទាំងIPv4 និងIPv6 protocol។ Static Routes មាន Option ដ៏ល្អក្នុងការកំណត់ Routes ដោយមិនចាំបាច់មានការ Resort ឬ dynamic Protocol អ្នកអាចប្រើ matric នីមួយៗរបស់ routes ដែលអ្នកបានបង្កើត

ដើម្បីកំណត់ relative cost របស់វា។ Routes អាចត្រូវបានបង្កើតមកពី RRAS management console interface ឬដោយប្រើ command line។ Adding, Viewing, និងmodifying នៃrouting table កើតពីcommand prompt មួយគឺ route add command។ ឧទាហរណ៍ ការបន្ថែម route ទៅកាន់ Network ដែលមាន 172.16.0.0 មាន Subnet mask 255.255.0.0 ដោយឆ្លងកាត់ gateway មាន IP Address 192.168.10.254 និងមាន matric ១ អ្នកអាចប្រើ command ដូចខាងក្រោម

Route add 176.16.0.0 255.255.0.0 192.168.10.254 1 16

ប៉ារ៉ាម៉ែត្រចុងក្រោយនៃ command នេះ(១៦)សំដៅទៅលើលេខដែលតំណាងនៅក្នុងNetwork Interface ដែលអ្នកចង់ឱ្យ Route នេះបាន។ នៅលើ Server ជាដំបូងការភ្ជាប់ Local Area Network មាន Interface លេខ១៦។សំនួរសួរថា តើអ្នកអាចដឹងថា Interface Number នៅទីតាំងដំបូងដោយរបៀបណា?អ្នកអាចដឹងបានដោយប្រើCommand ដូចខាងក្រោម

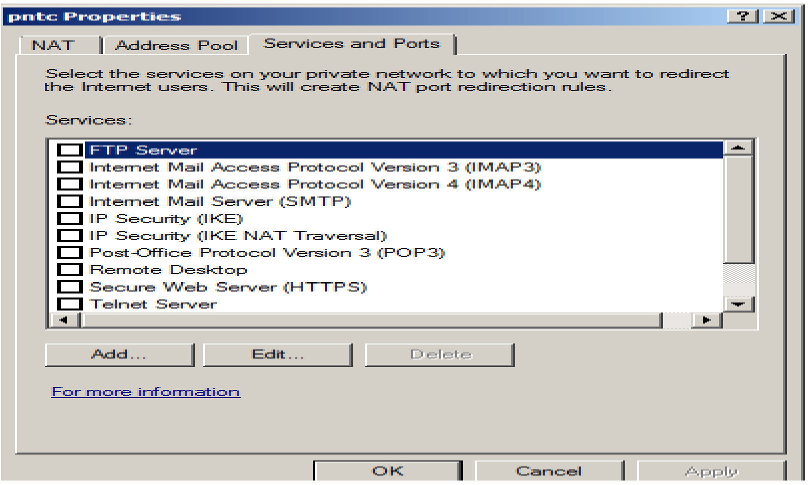
Route print



រូបភាព១១-២២-ការ Configure address pool ដែលកំណត់ដោយ ISP

Command នេះបង្ហាញព័ត៌មាននៃ bit ដូចជា interface នៅលើ server របស់អ្នក អញ្ចឹងដែលមាន route ខ្លះបានកំណត់សម្រាប់ប្រើ IPv4 និង IPv6។ រូបភាព ១១-២៤ បង្ហាញពីការលទ្ធផលនៃCommand **route print**។ ផ្នែកដំបូងនៃលទ្ធផលរបស់ Command គឺជា interface list។ Interface Number គឺជាតារាងដែលអនុវត្តតាម MAC address ហើយបន្ទាប់Interface Description។ អ្នកប្រើ Interface Number ដែលបានមកពី command នេះ នៅពេលអ្នកត្រូវបញ្ជាក់អំពី Interface ដោយ Command **route add**។

ទោះបីជាការប្រើ command prompt សម្រាប់ការបន្ថែម route អាចមានប្រយោជន៍គឺវាមានលក្ខណៈងាយស្រួលជាងក្នុងការប្រើ RRAS គ្រប់គ្រង interface ដើម្បីកំណត់ Static route។ ដើម្បីបង្កើត static route ថ្មីមួយដោយប្រើ interface ក្នុងពង្រីក protocol(IPv4 ឬ IPv6) នៅក្នុង RRAS management interface។ Select ទៅលើ static route ថ្មីមួយហើយបញ្ចូលព័ត៌មានដែលពាក់ពន្ធ័។ ដូចរូប ១១.២៥បង្ហាញពីរបៀបនៃការបំពេញប្រអប់ static route ថ្មីមួយសម្រាប់បន្ថែមព័ត៌មាន route ដែលយើងបានបន្ថែមដោយប្រើ command prompt។



រូបភាព១១-២៣-Configuring NAT port redirection rules

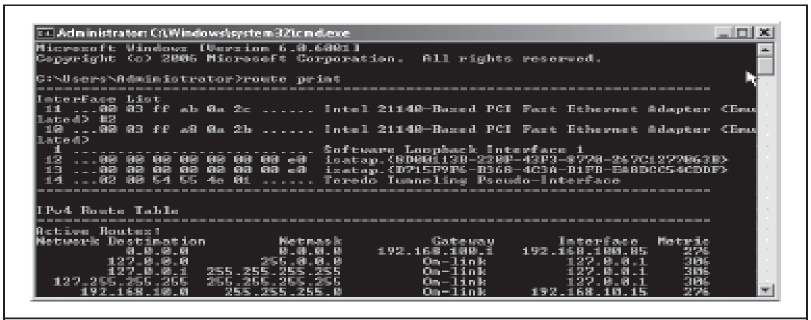
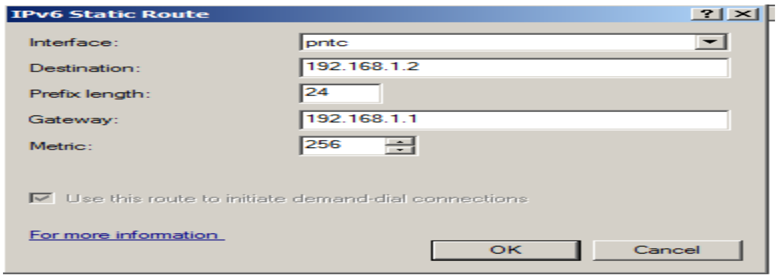


Figure 11-24. Output of the route print command



រូបភាព១១-២៥ ការបន្ថែម static route មួយដោយប្រើ RRAS management console

១៧-៨- Remote Access

Window Server 2008 ផ្តល់ឱ្យវិធីសាស្ត្រពីរផ្សេងគ្នាសម្រាប់ការ access ពីចម្ងាយគឺ dialup និង VPN។ Dialup ដាក់ស្នែងតម្រូវឱ្យមាន modem ឬ modem bank មួយដើម្បីភ្ជាប់ពីចម្ងាយបានដោយប្រើ POTS (plain old telephone system) ឬ ISDN។ ចំនែកVPNs ត្រូវបានរចនាឡើងដើម្បីកាត់បន្ថយការ ចំណាយសរុបរបស់ remote access ដោយឥទ្ធិពលនៃ internet សម្រាប់បង្កើតផ្លូវរូងមួយដែលមានសុវត្ថិភាពសម្រាប់ការទំនាក់ទំនងរវាងកុំព្យូទ័រដែលនៅឆ្ងាយនិង corporation private network។ VPN មានចំនួនអ្នកប្រើកើនឡើងនិងចំនេញពេលវេលា ហើយងាយស្រួល access ទៅកាន់ Internet គ្រប់ទីកន្លែង។ ផ្នែកដ៏ល្អបំផុតរបស់ VPN technology គឺតម្រូវការទាំងអស់របស់អ្នកត្រូវការមកពីប្រតិបត្តិការ network ដែលមានទំនាក់ទំនងនិងការភ្ជាប់ internet លឿនអាចផ្តល់សេវាទៅកាន់ការភ្ជាប់ដែលបង្កើតឡើងដោយ អ្នកប្រើប្រាស់ពីចម្ងាយ។

Dial-Up Networking

Dial-up networking(DUN)គឺជាវិធីសាស្រ្តដ៏សាមញ្ញបំផុតមួយសម្រាប់ផ្តល់ឱ្យaccess ពីចម្ងាយ។ វាប្រើ modem ភ្ជាប់ដោយផ្ទាល់ទៅកាន់ corporate private network របស់អ្នកលើបណ្តាញទូរសព្ទ័។ DUN ផ្តល់គុណសម្បត្តិដែលមានសុវត្ថិភាពត្រឹមត្រូវសម្រាប់ការភ្ជាប់ពីឧបករណ៍បញ្ជូននិងឧបករណ៍ទទួលរវាង host ដែលនៅឆ្ងាយមួយនិង private network របស់អ្នក។ វាអាច access បានយ៉ាងងាយស្រួលតាំងពីអ្នកបានភ្ជាប់ពីទីកន្លែងដែលអ្នកចង់ភ្ជាប់ទៅកាន់បណ្តាញទូរស័ព្ទ។បញ្ហាគឺវាទាក់ទងល្បឿនយឺតនៃការភ្ជាប់របស់modem ដែលអាចជំនះទៅលើទៅលើ process ហៅថា *multilinking* ជាកន្លែងដែលមានការតភ្ជាប់ឆ្លងកាត់ multiple phone ឬ ISDN lines អាច Virtual group បានទាំងអស់គ្នា។

DUN គឺចំណាយតម្លៃដើម្បីគ្រប់គ្រងតាំងពីអ្នកបានផ្តល់និងចំណាយសម្រាប់បណ្តាញដែលមានខ្សែទូរសព្ទ័ច្រើនដែលអាចឱ្យភ្ជាប់បង្កើតបាន។ អ្នកប្រើដែលអ្នកមាននៅលើ lines បានមកពីក្រុមហ៊ុនផ្តល់សេវារបស់អ្នក។

១៧-៨-១- Point–to-Point Protocol

Point-to-Point Protocol (PPP) គឺត្រូវបានប្រើសម្រាប់ DUN វាអនុញ្ញាតឱ្យ hosts មានទំនាក់ទំនងគ្នាដោយប្រើ TCP/IPលើ serial Link ដូចជា DUN ឬ serial cable connection។ PPP ប្រើ៦ protocol ផ្សេងៗគ្នា។ នេះជាតារាងតាមលំដាប់លំដោយនៃការប្រើវា

- Link Control Protocol (LCP): LCP ឋិតនៅក្នុងការទទួលខុសត្រូវក្នុងការចរាចរចំពោះការភ្ជាប់ដែលជាអ្នកmaintain link ទាំងនេះពេលវាដំណើរការ។
- Challenge Handshake Authentication Protocol (CHAP) CHAP ឋិតនៅ
  ក្នុង Charge of authenticating ដែលclient ប្រើ login credential សម្រេចថា អ្នកប្រើមានការ access ឬ អត់។
- Callback Control Protocol (CBCP) Protocol នេះគ្រប់គ្រងទៅលើការ ហៅត្រឡប់វិញដែលអាចឱ្យអ្នក Configure Server ដើម្បីរងចាំហើយនិងម៉ាស៊ីន Client ហៅត្រឡប់វិញដើម្បីបង្កើតការទំនាក់ទំនង។ វាប្រើសម្រាប់សុវត្ថិភាពបានផងដែរ ប្រសិនបើអ្នកដឹងពិតប្រាកដពីកន្លែងដែល client បានភ្ជាប់ទៅកាន់ទីតាំងដែលបានហៅមក ការរងចាំ និងការភ្ជាប់ឡើងវិញទៅកាន់ client ដោយប្រាកដថាការភ្ជាប់នេះមិនអាចបង្កើតឡើងបានពីលេខផ្សេងបានទេ។
- Compression Control Protocol (CCP) ដូចដែលអ្នកបានគិតទុក Protocol នេះគឺឋិតនៅក្នុងក្នុងការទទួលខុសត្រូវដែល parameter compress រវាងserver និងclient.
- IP Control Protocol (IPCP) Protocol នេះឋិតនៅក្នុងការទទួលខុសត្រូវចំពោះការចរាចរ IP ដូចជា maximum transmission unit (MTU)។
- Internet Protocol (IP) ចំនុចនេះPPPដើរតួដូចជា TCP/ IP connection ដែរ

១៧-៩- Virtual Private Network

VPN ផ្តល់ដំណោះស្រាយយ៉ាងល្អនិងងាយស្រួលសម្រាប់ការ Remote Access ទៅតាមតម្រូវការ។ ពួកវាមានតម្លៃថោកទាំងការអនុវត្តនិងការគ្រប់គ្រង ព្រោះថាអ្នកចាំបាច់ត្រូវភ្ជាប់ Network Bandwidth របស់អ្នកទៅ Internet។ ការកើនឡើងយ៉ាងឆាប់រហ័សដែលអាចទុកចិត្តបានហើយភ្ជាប់ទំនាក់ទំនងដែលមានល្បឿនលឿនតាមរយៈរលកធាតុអាកាសដែលផ្សាយទៅទីឆ្ងាយបានយ៉ាងល្អ ការប្រើប្រាស់ Wireless Internet Access នៃ VPN អាចបង្កើតបានច្រើនជាង Accessible Dial-up។ ទោះបីជាយ៉ាងណា បច្ចេកទេសនៃការចាប់ផ្តើមបញ្ជូន Packet តាម Internet សារៈសំខាន់គឺ Security Risk ជាកន្លែងដែលមិនអាចមើលឃើញដោយភ្នែក រឿងខ្លះអាចកើតឡើង ,ការរំខានទាំងអស់នោះអាចត្រូវបានកាត់បន្ថយដោយការបង្កើតផ្លូវសម្រាប់បញ្ជូន Data ដែលមានសុវត្ថិភាពហើយត្រូវបាន Encrypt។ Client របស់អ្នកអាចប្រើប្រាស់នូវ Internet អ្វីក៏ដោយដែលអាចភ្ជាប់ការទំនាក់ទំនងពួកគេទៅ Internetដើម្បីទទួលបាននូវ VPN Server។ ពួកគេនិងបង្កើតការ Access រួមគ្នាទាំងអស់ជា Private Network ដូចដែលបានបង្ហាញក្នុងលេខ ១១-២៦។ Client ទាំងអស់គឺត្រូវការ Internet ដើម្បីភ្ជាប់ការទំនាក់ទំនងរបស់ពួកគេព្រោះថាភាពជាក់ស្តែងពួកគេអាចភ្ជាប់ការទំនាក់ទំនងពីគ្រប់ទីកន្លែងមាន Internet Service ផ្តល់ឱ្យភ្ជាប់ទំនាក់ទំនងបានរវាងគ្នាវា ប្រសិនបើវាមិនត្រូវបានបិទដោយអ្នកផ្តល់ Internet Service។ Internet Service ទាំងអស់នោះរួមបញ្ចូលទាំងតាមផ្ទះ សណ្ឋាគារ និងនៅតាមព្រលានយន្តហោះហើយទោះបីជាប្រព័ន្ធរលកធាតុអាកាសដែលផ្តល់ឱ្យតាមរយៈ Wireless Hotspot ឬក៏តាមរយៈ Wireless Broadband Cards ក៏ដោយ។

Encapsulation and Tunneling (ការវេចខ្ចប់ និងផ្លូវបញ្ជូន)

VPNs ដំណើរការដោយការវេចខ្ចប់យ៉ាងត្រឹមត្រូវនូវ Data ដែលអ្នកអាចនឹងចង់បញ្ជូនតាមរយៈ Remote Host ទៅក្នុង Protocol ផ្សេងទៀត។ ដូចច្នេះវាអាចមានភាពមាំមួននិងសុវត្ថិភាពក្នុងការបញ្ជូននៅលើ Internet។ ផ្នែកដែលល្អបំផុតគឺ Application របស់អ្នកនឹងមិនត្រូវមានទាមទារឱ្យមានការផ្លាស់ប្តូរអ្វីទាំងអស់ក្នុងការធ្វើឱ្យដំណើរការ។ អ្វីទាំងអស់ដែលត្រូវការគឺVPN Client ហើយនឹង Server ដែលមាន Encrypt និងវេចខ្ចប់ Packet តាមច្បាប់ក្បួនហើយបន្ទាប់មកការងារនេះត្រូវបានធ្វើសារឡើងវិញនៅផ្នែកមួយផ្សេងទៀតដូច្នេះ Application អាចដំណើរការបានដូចធម្មតាដោយមិនចាំបាច់ Encrypt Dataក្នុង Window Server 2008 មានដំណើរការ 3 ប្រភេទផ្សេងគ្នានូវ Protocol នៃប្រេកបញ្ជូនដំណើរការទាំង 3 ប្រភេទនោះមាន

-Point-To-Point Tunneling Protocol Protocol បញ្ជូនពីចំនុចមួយទៅចំនុចមួយផ្សេងទៀត

-Protocol បញ្ជូនដែលប្រើស្រទាប់ទី2 នៃ OSI model នៅលើ Internet (L2TP)

-ការបញ្ជូនដែលមានសុវត្ថិភាពនៃSocket (SSTP) ។

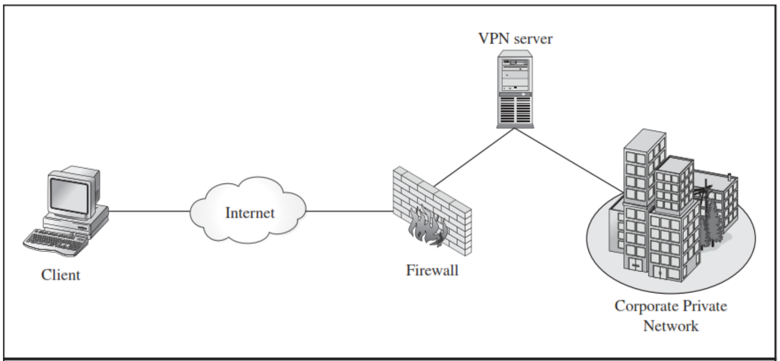


Figure 11-26. Typical VPN

Tunneling យោងទៅលើការបង្កើតទំនាក់ទំនងជាក់ស្តែងរវាង Network ពីរនៅលើ Networkផ្សេងទៀតឬក៏សំនុំនៃ Network ដែលជាកន្លែងដែលទិន្នន័យចាប់ផ្តើមបញ្ជូនឱ្យគ្នារវាង Network ពីរផ្សេងគ្នាធ្វើសហប្រតិបត្តិការក្នុងផ្លូវបញ្ជូនដែលមិនអាចបកស្រាយបានដោយអ្នកកណ្តាលណាមួយឡើយ។ ដូចជា Internet ជាដើម។ PPTP គឺសាមញ្ញនិងងាយស្រួលរៀបចំឡើង។ ការស្នើសុំការភ្ជាប់ទំនាក់ទំនងត្រូវបានរៀបចំឡើងហើយបន្ទាប់មក Server ត្រូវបានការឆ្លើយតបសំនួរ ជាមួយ Client ។

ចាប់ពីពេលដែល User ត្រូវបានយល់ព្រម Tunnel គឺត្រូវបានបង្កើតហើយ Sessionគឺត្រូវបានវេចខ្ចប់តាមរយៈ Generic Routing Encapsulation (GRE) Protocol ទៅតាមប្រភេទ Packet នីមួយៗដែលសាមញ្ញគឺវាផ្ទុក Data ដែលបានវេចខ្ចប់។ ទិន្នន័យទាំងនោះជាប្រភេទ Encrypt ដែលប្រើប្រាស់ Microsoft Point-To-Point Encryption(MPPE)ផងដែរ។ បន្ទាប់មក Data គឺត្រូវបានបញ្ជូនតាមរយៈ Tunnel ដោយគ្រាន់តែវាត្រូវបានដំណើរការលើ Private Network ដែលត្រឹមត្រូវ លើកលែងតែ PPTP Layer ដែលគ្រប់គ្រងថែរក្សានូវ Encryption និង Encapsulation ទាំងអស់ដែលដំណើរការបានយ៉ាងល្អ ការដំណើរការត្រលប់មកវិញគឺត្រូវបានធ្វើនៅខាងឧបករណ៍ទទួលជាចុងក្រោយ។ Layer 2 Tunneling Protocol /IP Security) L2TP/IPsec)គឺមានការស្មុគស្មាញថែមទៀតសម្រាប់ Tunneling Protocol ប៉ុន្តែការស្មុគស្មាញរបស់វាគឺកើតឡើងនៅផ្នែកខាងក្រៅនៃសមត្ថភាពរបស់វាដើម្បីបង្កើតភាពដែលអាចបត់បែនបានថែមទៀតសម្រាប់ L2TP ។

១៧-២០- ការភ្ជាប់តាម SSTP

SSTP គឺជាការកែច្នៃបង្កើតឡើងសម្រាប់ការភ្ជាប់ទំនាក់ទំនងយ៉ាងងាយមួយរវាង Client/Server VPN server។ ប៉ុន្តែវាមានភាពស្មុគស្មាញបន្តិចដែរក្នុងការបង្កើត site-to-site VPN នោះ។ ផ្នែកទាំងអស់នៃការភ្ជាប់ទំនាក់ទំនងគឺបំពេញការឆ្លើយតបយ៉ាងល្អសម្រាប់ការប្រើប្រាស់ផ្នែកមួយនៃ Tunneling Protocol ពីរផ្សេទៀតដែល SSTP ភ្ជាប់ការទំនាក់ទំនងដំបូងទទួលអ្វីៗដែលមានតាមជំហាននៃការបង្កើត Tunnel ការបង្កើតការផ្ទៀងផ្ទាត់និងគ្រប់គ្រងការទំនាក់ទំនងតាមរយៈអាយុកាលរបស់វា។ជំហានក្នុងការភ្ជាប់ទំនាក់ទំនង

1. SSTP Client បង្កើតTCP Connection ទៅកាន់ Port 443នៅលើ Server
2. ការបង្ហាញប្រាប់ Client នូវអ្វីដែលបានបង្កើត Connection ដោយការបញ្ជូន Message "Hello"ទៅ SSL Client ។
3. Server បញ្ជូន Certificate កុំព្យូទ័រ របស់វាទៅឱ្យ Client។
4. Client ធ្វើការបញ្ជានូវ Server Certificate ហើយបង្កើត SSL Session Key ដែលបាន Encrypt ហើយប្រើប្រាស់ Public Keyនៃ SSTP Server។
5. Client ធ្វើការបញ្ជូន SSL Session Key ទៅឱ្យ SSTP Server។
6. Server ស្រង់យក SSL Session Key ប្រើប្រាស់ Key Private របស់វាហើយ SSL Key គឺនឹងត្រូវប្រើប្រាស់សម្រាប់ការភ្ជាប់ទំនាក់ទំនងនៅពេលក្រោយៗទៀត។
7. Client ធ្វើការផ្ញើរ HTTPS request ទៅកាន់Server។
8. Client ធ្វើការចរចារការភ្ជាប់ SSTP Tunnelជាមួយ Server។
9. Client ធ្វើការចរចារការភ្ជាប់ទំនាក់ទំនង PPP ជាមួយ Server ដែលផ្ទៀងផ្ទាត់ User និងការ Configure IPv4 និង IPv6 Setting។
10. ការទំនាក់ទំនងរវាង Server និង Client គឺត្រូវធ្វើការបញ្ជូនលើ Tunnel PPP link ។

បញ្ហាទាំងនេះគឺត្រូវបានដោះស្រាយដោយបង្កើតវាជាគូរជាមួយ IPsec ទៅនឹងការគ្រប់គ្រងសុវត្ថិភាពនៃការរួមបញ្ចូលគ្នានិង Encryptions សម្រាប់ Channel បន្ទាប់មក L2TP យកផលប្រយោជន៍នៃសុវត្ថិភាព Channel ទៅបង្កើត Tunnel រវាង Client និងServer។ វាមិនត្រូវការបារម្ភណ៍អំពី Encryption ឬក៏ authentication ទៀតទេចាប់តាំងពីវាត្រូវបានបង្កើតរួចរាល់ដោយគូររបស់វាគឺ IP security។ Secure Socket Tunneling Protocol (SSTP) គឺជាTunneling Protocolថ្មីដែលណែនាំជាមួយនឹង Window Server 2008។ វាគឺមានកាចាប់អារម្មណ៍យ៉ាងខ្លាំងនូវ Protocol ថ្មីព្រោះបានបង្កើត Address ដោយឡែកពីគេ បញ្ហាPPTP និង L2TP កើតមាននៅពេលដែលធ្វើការឆ្លងកាត់ Firewall ដែ Configure យ៉ាងជឿជាក់។

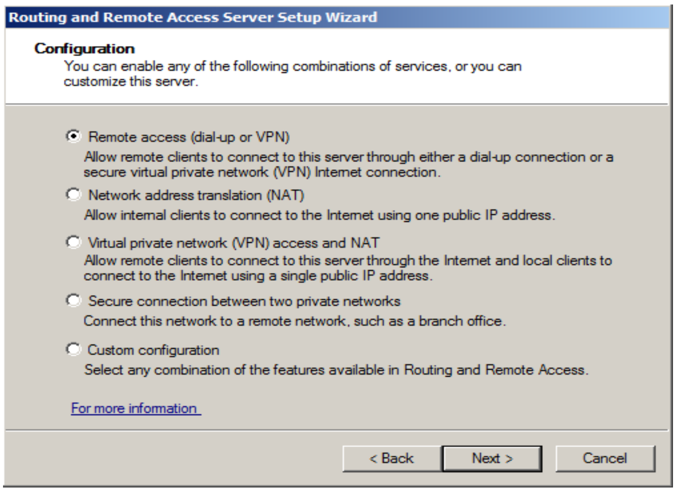
SSTP Session គឺបានបង្កើតការប្រើប្រាស់ HTTP នៅលើ SSL (HTTPS) Session រវាងServer និង Client។វាកាត់បន្ថយតម្លៃសម្រាប់ការអនុវត្ត VPN access ព្រោះវាធ្វើឱ្យងាយស្រួលសម្រាប់ការអភិវឌ្ឍន៍របស់អ្នក។ អ្នកអាចជំនួស RRAS Server របស់អ្នកដោយសុវត្ថិភាពនៅពីក្រោយ NAT ហើយអ្នកមិនចាំបាច់ត្រូវការ VPN Software ដែលជាអ្នកទី៣ មួយចំនួនដើម្បីបង្កើតការទំនាក់ទំនងនោះទេ។ ដូចគ្នាជាមួយនឹងបច្ចេកវិទ្យារបស់ SSL-Based ទាំងអស់អ្នកត្រូវមាន Root CA សម្រាប់ Server របស់ កុំព្យូទ័រ Certificate ដែលបាន Install នៅលើ SSTP Client សម្រាប់ការភ្ជាប់ទំនាក់ទំនងទៅការងារ, ប្រសិនបើអ្នកមាន CA ផ្ទាល់ខ្លួន អ្នកគួរតែមានការបែងចែក Root CA របស់អ្នក់ សម្រាប់ការប្រើប្រាស់ Group policy។

Hand-on Exercise: Configuring RRAS សម្រាប់ Remote Access

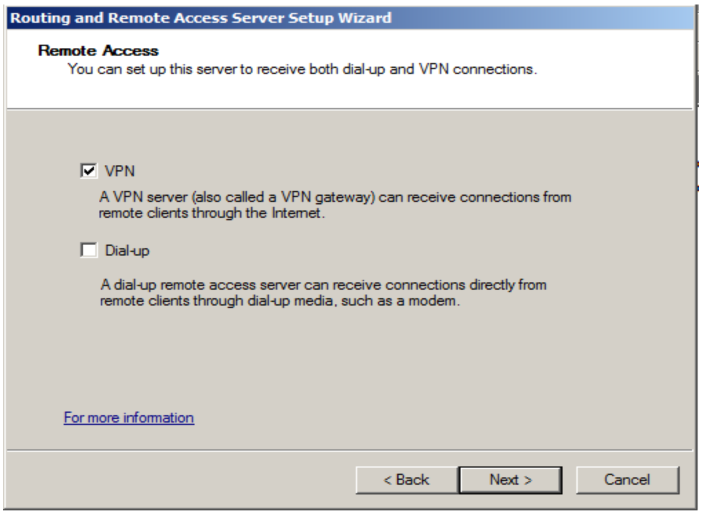
ផ្នែកតូចមួយនៃព័ត៌មានដែលត្រូវបង្ហាញមុនគេគឺសរុបអត្ថន័យទូទៅនូវរបៀបដែល DUN និងVPN ដំណើរការ។ ការពិភាក្សានៅលើបច្ចេកវិទ្យា DUN VPN និង Protocolអាចមានច្រើនហួរហែរ។ ប៉ុន្តែអ្វីដែលអ្នកបានអានទាំងអស់នោះអ្នកត្រូវតែដឹងការ Configure remote access on Window Server 2008។

នៅក្នុងលំហាត់នេះគឺយើង Install និងConfigure RRAS សម្រាប់ Remote access ។ Server របស់អ្នកត្រូវតែជាផ្នែកនៃ Domain និងDHCP Serverត្រូវតែនៅលើ Network ដែលអ្នកអាចAssign IP Address ទៅឱ្យ VPN Client :

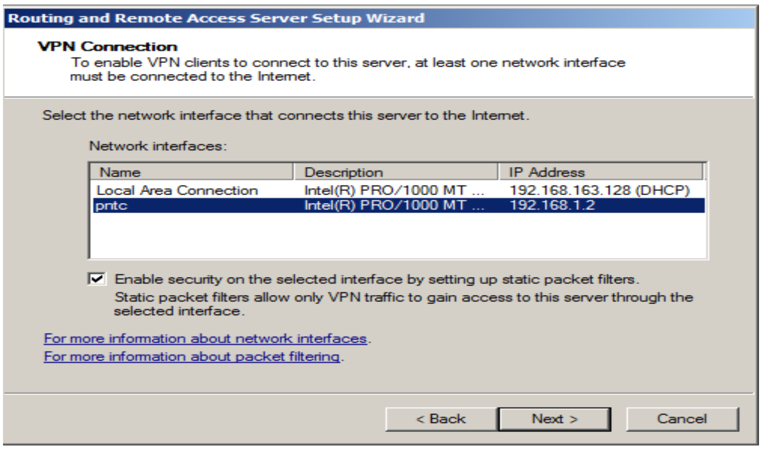
1. Log on នៅក្នុងServer ដោយប្រើ Account ដែលជាសមាជិកនៃ Domain Administrator Group
2. Install Routing ហើយនិងRemote Access Role Server ប្រសិនបើវាមិនទាន់បានInstall រួចរាល់។
3. បើកនូវ Routing និង Remote Access Management Console។
4. ចុច Mouse ស្តាំនៅលើឈ្មោះរបស់Server ហើយជ្រើសយក Configure ហើយ Enable Routing និង Remote Access Server Setup Wizard។
5. ចុច Next នៅលើ Welcome Screen ។
6. ជ្រើសយក Remote Access (Dial-up ឬក៏ VPN)ហើយបន្ទាប់មកចុច Next។



រូបភាព១១- ២៧-Configuring RRAS for remote access



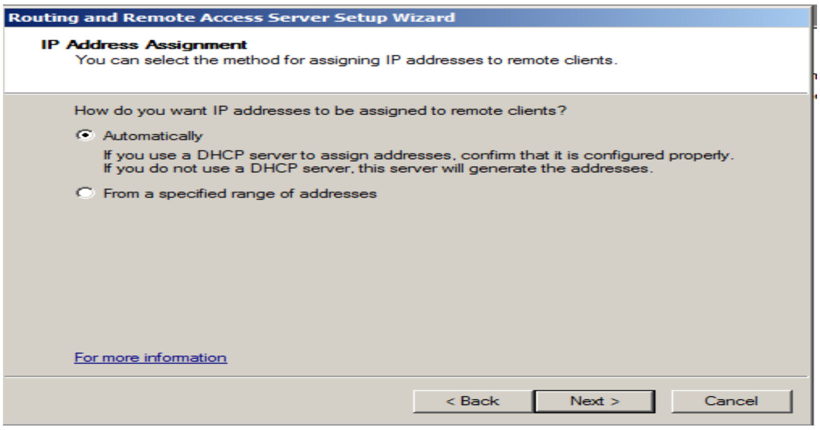
រូបភាព១១- ២៨-ការកំណត់ពីរបៀបភ្ជាប់ចំពោះ remote access



រូបភាព 11-29 កំណត់ទៅលើ Internet facing network interface

7. នៅក្នុងការ Remote Access Screen, ជ្រើសរើសយកទាំង VPN ហើយនិង Dial-up, ដែលយើងនិងត្រូវការ ប្រើវានៅពេលក្រោយ បន្ទាប់មកចុចលើ Next។

8. នៅលើ VPN Connection Server,ជ្រើសរើសយក Network Interface ដែលបានភ្ជាប់ ទៅកាន់ Internet, ហើយ Check ប្រអប់ Enable Security on the Selected Interface by Setting up Static Filter ប្រសិនបើវាមិនទាន់ត្រូវបានCheck បន្ទាប់មក Click Next
9. នៅលើ IP Address Assignment Screen, ជ្រើសរើសយក Automatically ដើម្បីបង្ហាញប្រាប់ពីរបៀបដែលអ្នកចង់ Assign IP address បន្ទាប់មក Click Next។
10. នៅក្នុងផ្ទាំង Managing Multiple Remote Access Server Screen, ជ្រើសរើស No, use Routing and Remote Access to Authenticate Connection request ពេលដែលយើងមិនប្រើ RADIUS តាមលំហាត់ បន្ទាប់មក Click Next។
11. ពិនិត្យមើលលើ Setup Summary បន្ទាប់មកចុចលើ finish។
12. ចុចលើ Ok នៅលើ Message box ដែល Pop-up ព័ត៌មានរបស់អ្នកដែលអ្នកត្រូវតែConfigure Property នៃ DHCP relay Agent ជាមួយនិង IP address នៃ DHCP Server។



រូបភាព១១-៣០ បង្ហាញពីរបៀបកំណត់ IP addresses

១៧-២១- DHCP Integration with RRAS

ពេលដែលអ្នកប្រើប្រាស់ RRAS សម្រាប់DUN ឬក៏VPN, ការភ្ជាប់ Client គឺត្រូវការទទួល IP address ដើម្បីទំនាក់ទំនងជាមួយនឹង HOST ផ្សេងទៀតនៅលើ Network របស់អ្នក, ត្រូវប្រាកដថាអ្នកចង់ប្រើនូវ IP នោះដោយ DHCP លុះត្រាតែអ្នកមានតម្រូវការជាក់លាក់ណាមួយដើម្បីប្រើប្រាស់ Static IP address អ្នកអាចបង្កើត Static address pool ដើម្បីលៃលក Dynamic IP address ទៅឱ្យ RRAS Client ដោយមិនប្រើ DHCP។

ប្រសិនបើ RRAS Server របស់អ្នកកំពុងដំណើរការផងដែរនូវ DHCP server, Server របស់អ្នកនិងអាចកំណត់ IP address ជាស្វ័យប្រវត្តិ ប្រសិនបើអ្នកកំពុងដំណើរការ DHCP Server ដាច់ដោយឡែកអ្នកនឹងត្រូវ Configure ទៅលើ DHCP relay Agent នៅលើ RRAS Server។

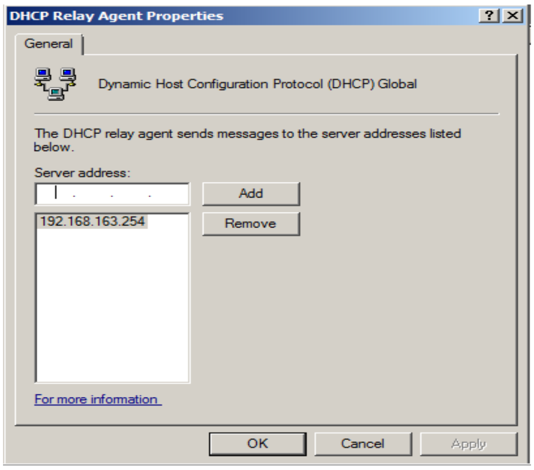
Hand-On Exercise: Configuring DHCP Relay Agents សម្រាប់ RRAS

ប្រសិនបើអ្នកមិនមាន DHCP Server ដែលសម្រាប់ install នៅលើ RRAS របស់អ្នកនោះទេ។អ្នកត្រូវការ configure ទៅកាន់ DHCP Relay Agents ដូច្នេះអ្នកអាច configure DHCP Relay Agents ដែល Windows Server 2008 មានការគាំទ្រទាំង protocol IPv4 និង IPv6 ដោយឯករាជ្យ។ Ex: អ្នកអាចត្រួតត្រាទៅលើ clients ពី DHCP server មួយហើយIPv6 Addresses ត្រូវបាន handle (ស្តាប់បង្គាប់) ដោយ server ដទៃ។ នៅក្នុងលំហាត់នេះយើង configure IPv4 DHCP Relay Agents ដើម្បីទៅកាន់ DHCP server របស់យើង។

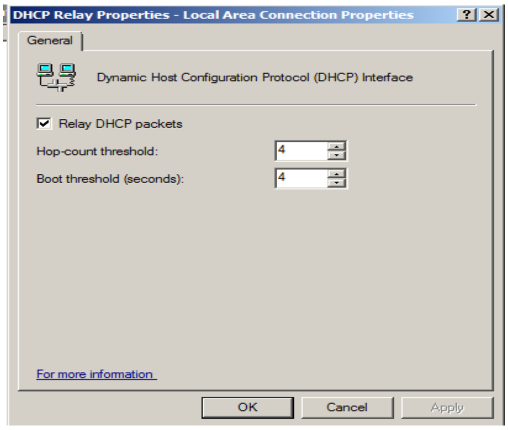
1. បើក Routing and Remote Access management console.
2. ពង្រីក server name ហើយបន្ទាប់មកពង្រីក IPv4.
3. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ DHCP Relay Agent ហើយជ្រើសរើសយក Properties
4. នៅក្នុង DHCP Relay Agent Properties window, add the IP addresses for your DHCP servers (រូបភាព១១-៣២)
5. ចុចលើ OK ដើម្បី save
6. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ DHCP Relay Agent ហើយជ្រើសរើសយកNew Interface
7. ជ្រើសរើសយក network interface ដែលបានភ្ជាប់ទៅកាន់ subnet របស់ clients ដែលត្រូវការស្នើ DHCP របស់ពួកគេហើយបន្ទាបើមកចុចលើ OK
8. នៅក្នុង Internal Properties window ត្រូវច្បាស់ថា Relay DHCP Packet ត្រូវបាន check ហើយ hop-count and boot thresholds មានតម្លៃសមរម្យសម្រាប់ network របស់អ្នក(រូបភាព១១-៣៣)ហើយបន្ទាប់មកចុចលើ OK ។

Configuring RRAS Server Properties

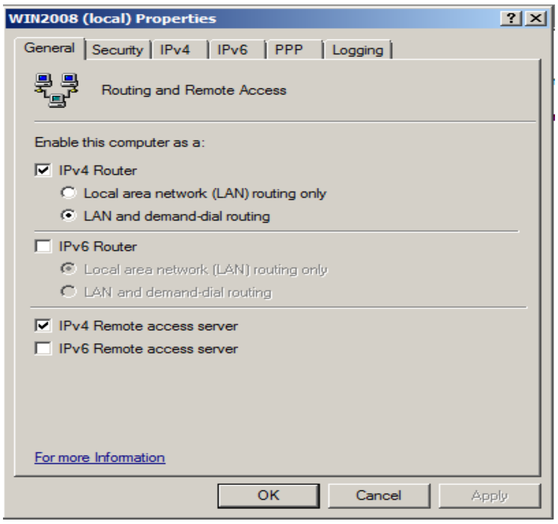
ជម្រើសទូទៅសម្រាប់ RRAS ជាការពិតត្រូវបាន configure នៅឯកម្រិត server ប្រសិនបើអ្នកបើក Properties Server របស់អ្នកពីខាងក្នុង RRAS management Console ។ អ្នកនិងឃើញ ៦ Tab សម្រាប់ការ Configure Properties Server របស់អ្នក។ ក្នុងចំនោម Tabទាំងអស់មានមួយដែលសំខាន់ជាងគេគឺ General Tab(រូបភាព១១-៣៤)។ នៅលើProperties Sheet នេះ អ្នកអាចគ្រប់គ្រងថាតើ RRAS Server និងដើរតួនាទីជា Routerមួយហើយវា Enable រឺ disable Remote Access Serverវាគឺមានអត្ថប្រយោជន៍ប្រសិនបើអ្នកត្រូវការ Access មួយណាដែលអ្នកចង់លុបចេញពី Configuration របស់អ្នក។ Security Tab (រូបភាព១១-៣៥) ផ្ទុកនូវ Option សម្រាប់ Configuring ត្រឹមត្រូវតាមច្បាប់អ្នកផ្តត់ផ្គងសម្រាប់ធ្វើឱ្យមានសុពលភាពដើម្បីសំគាល់អ្នកប្រើប្រាស់ដើម្បី Remote Access ។នេះមួយណាក៏បានអាចនៅក្នុង Standard Windows Authentication RADIUS សម្រាប់ Centralized remote access management solution។ អ្នកក៏អាចបន្ថែមនូវ authentication methods របស់អ្នកដោយចុចលើប៊ូតុង Authentication Method ដើម្បីដំណើរការបន្ថែម Properties (ដូចបង្ហាញក្នុងរូបភាព១១-៣៦) អ្នកអាច Configure Extensible Authentication Protocol (EAP) Method, MS-CHAPv2, CHAPនិងPAP, អនុញ្ញាតថែមទៀតនូវRemote System ដើម្បីភ្ជាប់ Unauthentication (ទោះបីយ៉ាងណាអ្នកប្រសិនបើអ្នកមិនធ្លាប់ប្រើប្រាស់វាទេលុះត្រាតែអ្នកស្គាល់ស្ថានភាពរបស់ Troubleshooting authentica -tion មួយរបស់អ្នកដែលអ្នកគិតថាកំពុងបង្កបញ្ហា។



រូបភាព១១-៣២-DHCP Relay Agent Properties windows



រូបភាព១១-៣៣-internal Properties window

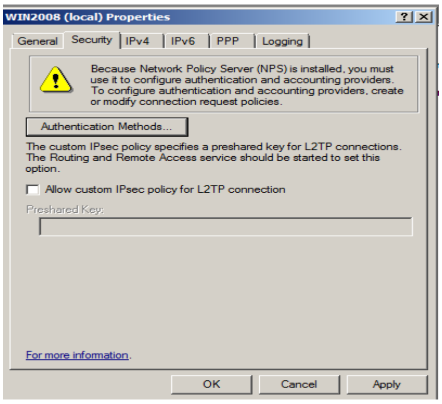


រូបភាព១១-៣៤-RRAS Server properties General tab

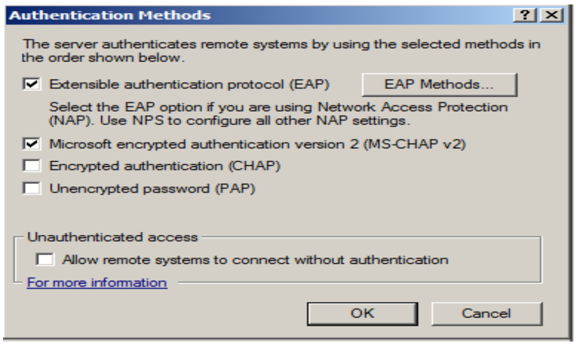
IPv4 និង IPv6 ត្រួតពិនិត្យការបញ្ជូនIPឱ្យProtocol ទាំងនោះ។ Tab PPP អនុញ្ញាតឱ្យអ្នក Configureទំនាក់ទំនង របស់Option ភ្ជាប់ទៅនឹងPPPជាច្រើន។អ្នកអាចភ្ជាប់ការទំនាក់ទំនងជាច្រើននិង enable Dynamic Bandwidth Control ។ អ្នកក៏អាច Configure ផងដែរថាតើផ្នែកបន្ថែម Link Control Protocol (LCP) រឺក៏ Software

Compression គឺនិង enable Default,គ្រប់Option ទាំងអស់នេះគឺត្រូវបានប្រើប្រាស់,(ដូចបានបង្ហាញក្នុងរូបភាព ១១-៣៧។

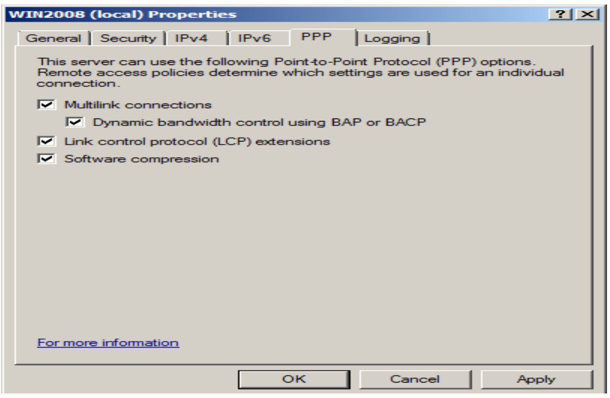
ទោះបីជា Option ទាំងអស់នេះឱ្យ PPP ជាអ្នកបង្កើតភាពដែលអាចបត់បែនបាននិងតួនាទី អ្នកគួរតែពិនិត្យចំនុចនីមួយៗនៃជម្រើសទាំងនេះដោយប្រុងប្រយ័ត្ននិងកំណត់ថាតើសមស្របទៅនិងបរិយាកាសដែរ រឺទេ។
ឧទាហរណ៍តើអ្នកពិតជាឱ្យអ្នកប្រើរបស់អ្នកធ្វើអ្វីមួយដើម្បីដំណើរស្ទះចរាចរលើបន្ទាត់ជាច្រើនឬទេ?ប្រសិនបើអ្នកមានផ្ទៃកបន្ថែម Enable តើវាបង្កើតឱ្យស្គាល់ដើម្បីប្រើSoftware Compression ដោយស្វាមស្វាត់រឺទេ?



រូបភាព១១-៣៥ RRAS Server Properties Security tab



រូបភាព១១-៣៦-RRAS Authentication Methods

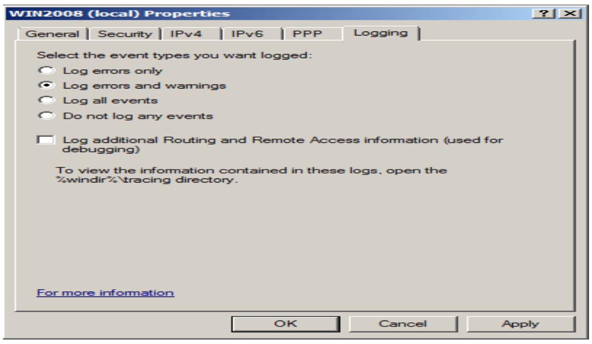


រូបភាព១១-៣៧-RRAS Server Properties PPP tab

នៅចុងក្រោយគឺ Logging tab (រូបភាព១១-៣៨) ដោយ default, RRAS Loge ទាំងពីរ Errors Warningការ log ទាំងនេះគឺបានផ្ទុកនៅក្នុង %WIDR%\ Logsfolders អ្នកអាចជ្រើសរើសដើម្បី Log តែ Error មួយគត់, Errors

និងWarning គ្រប់ព្រឹត្តិការណ៍, រឺក៏មិនគ្រប់ព្រឹត្តិការណ៍ទាំងអស់។ Option មួយផ្សេងៗទៀតអនុញ្ញាត្តិឱ្យ Log ចូលធ្វើឱ្យព័ត៌មានដែលអ្នកអាចជួយបានសម្រាប់ debugging។ Option នេះគួរតែប្រើប្រាស់បានដោយសន្សំសំចៃចាប់តាំងពីវាធ្វើការដំឡើង Log ទំហំនៃ Log ដែលសំខាន់ៗ កំណត់គួរតែល្មមតម្រូវការជាច្រើនសម្រាប់អ្នក។

ប្រសិនបើអ្នកចង់បណ្តោយការ Log ចូល,ឯចំនុចតូចមិនសំខាន់បំផុត អ្នកគួរតែ Log ចូលតែError ដូចដែលអ្នកមានអ្វីមួយធ្លាក់ត្រឡប់ក្រោយលើពេលបានជួបប្រទះនូវ Errors ជាច្រើន។



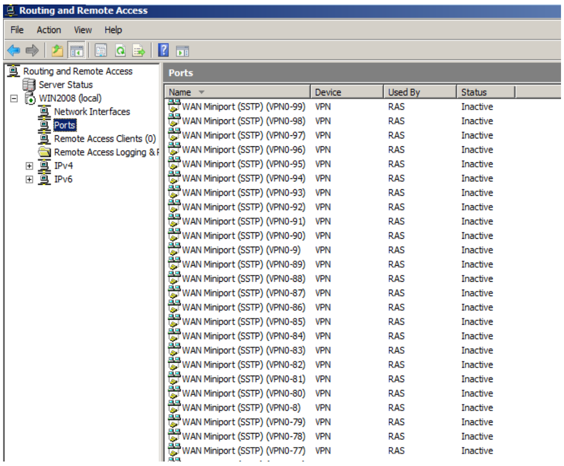
រូបភាព១១-៣៨-RRAS Server Properties Logging tab

Hardware-On Exercise: Configuring VPN Using PPTP

Windows Server 2008 គាំទ្រទៅនិង PPTP, L2TP/IPSec, និងSSTP ប្រសិនបើអ្នកអនុវត្តតាមលំនាំលំហាត់សម្រាប់ការ configure Remote Access។ Server របស់អ្នកត្រូវ setup ដើម្បីទទួលយកការភ្ជាប់ទៅកាន់ VPN។ Server របស់អ្នកត្រូវបាន configure ជា default ដើម្បីដឹងពីចំនួន port របស់ VPN នីមួយៗ។យើងអាចបង្កើនចំនួន SSTP connections រហូតដល់ 256 ដែល PPTP និង L2TP មិនអាចធ្វើទៅបានសម្រាប់ remote access។

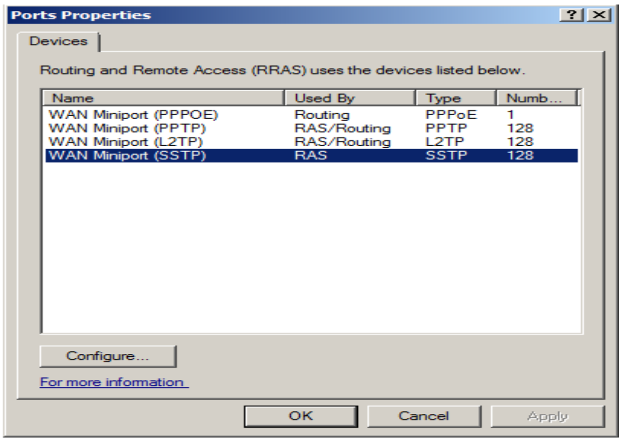
សម្រាប់ PPTP, L2TP/IPSec, និងSSTP ។ ជាការពិតណាស់ server hardware របស់អ្នកនឹងកំណត់ចំនួន VPN clients យ៉ាងជាក់លាក់។ ជាdefault កំណត់បានចាប់ពី១២៨ការភ្ជាប់សម្រាប់ PPTP, L2TP នឹង SST

1. បើក Routing and Remote Access management Console.
2. ពង្រីក server name node ហើយជ្រើសរើសយក Ports ។
3. ចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ Ports ហើយជ្រើសរើសយក Properties



រូបភាព១១-៣៩-RRAS Server VPN ports

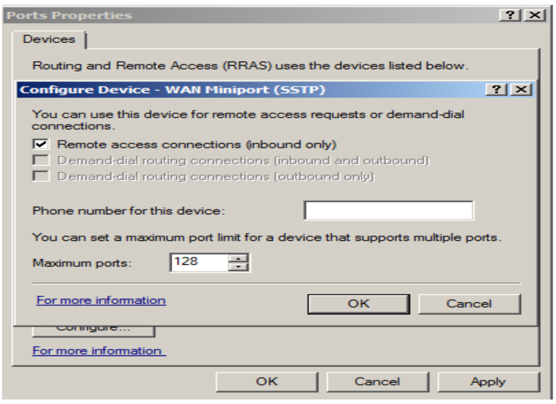
4. អ្នកនិងឃើញតារាងនៃ devices ទាំងអស់ដែល RRAS កំពុងប្រើ។ យើងចាប់អារម្មណ៍តែលើWAN Miniport (PPTP), WAN Miniport (L2TP)និង WAN Miniport (SSTP) មើលក្នុងរូបភាព១០-៤០
5. ចុចពីរដងស្ទួនគ្នាលើ WAN Miniport (SSTP).
6. យើងត្រូវប្រាកដថា Remote Access Connections (Inbound Only) ត្រូវបានជ្រើសរើសហើយទុកកន្លែងលេខទូរស័ព្ទនៅទទេ។ ប្តូរលេខ Port អតិបរមាមកជា២៥៦ហើយបន្ទាប់មកចុចលើ OK មើលរូបភាព១១-៤១
7. ចុចពីរដងស្ទួនលើ WAN Miniport (PPTP).



រូបភាព១១-៤០ RRAS Server Port properties

8. ដោះគ្រប់ការប្រអប់នោះចេញហើយបន្ទាប់មកចុចលើ OK (រូបភាព១១-៤២)។ ដោះលើប្រអប់នៃ Remote Access Connections (Inbound Only) ដើម្បីឱ្យវាបិទ PPTP ដោយមានប្រសិទ្ធភាព។
9. ចុចពីរដងស្ទួនលើ WAN Miniport (L2TP).
10. ដោះគ្រប់ប្រអប់ទាំងអស់ហើយបន្ទាប់មកចុចលើ OK.
11. Click OK on the Ports Properties dialog box to save the changes.

ចំណាំ នៅពេលអ្នក configure VPN client ដើម្បីភ្ជាប់មកកាន់RRAS ពេលក្រោយ អ្នកនិងត្រូវការ User Account ដែលមានសិទ្ធិភ្ជាប់។ គេអាចធ្វើទៅបានដោយប្រើ Remote Access Policy ដោយអនុញ្ញាតឱ្យឬបដិសេធ remote access តាមរយៈ Dial-in tab នៃ User Account Properties ក្នុង Active Directory Users and កុំព្យូទ័រ ដូចក្នុងរូបភាពខាងក្រោម ១១-៤១។



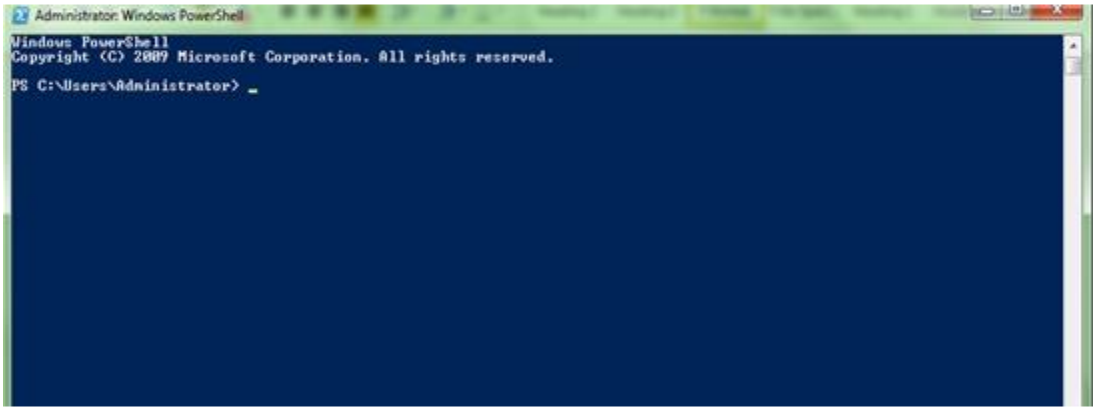
រូបភាព១១-៤១ SSTP Port Properties

ជំពូកទី១៨

Windows PowerShell

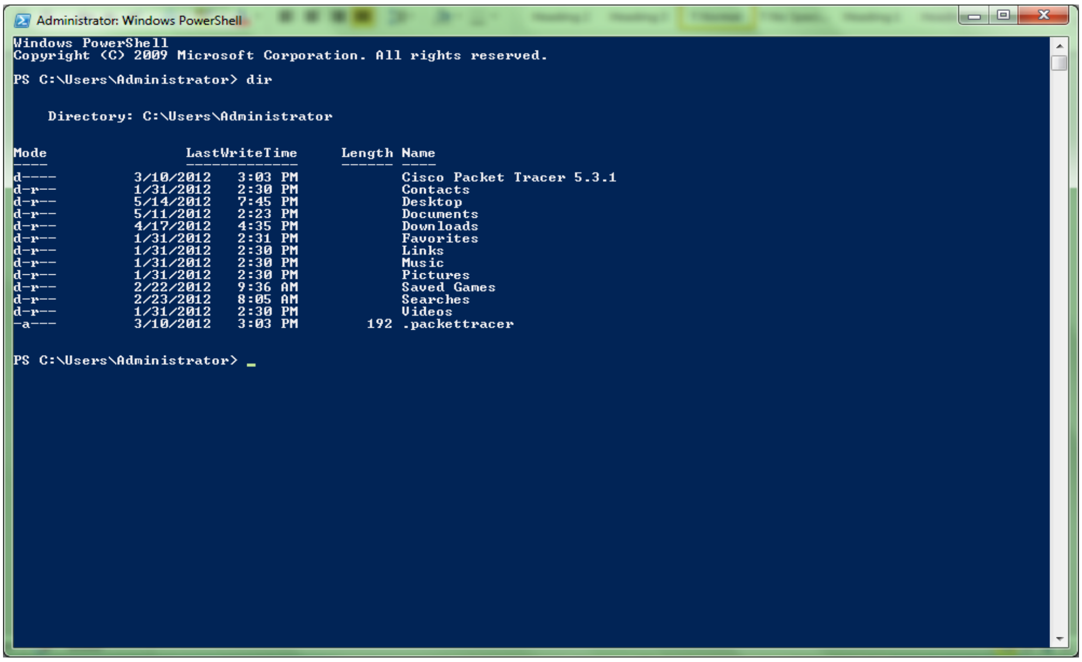
១៨-១- សេចក្តីផ្តើម

វាមានលក្ខណៈប្រហាក់ប្រហែលទៅនិង MS-DOS ចាស់នោះដែរ លើកលែងតែវាមានបង្ហាញពាក្យថា Windows PowerShell ជាចំណងជើងខាងលើ។



រូបភាព ១២-១ Windows PowerShell

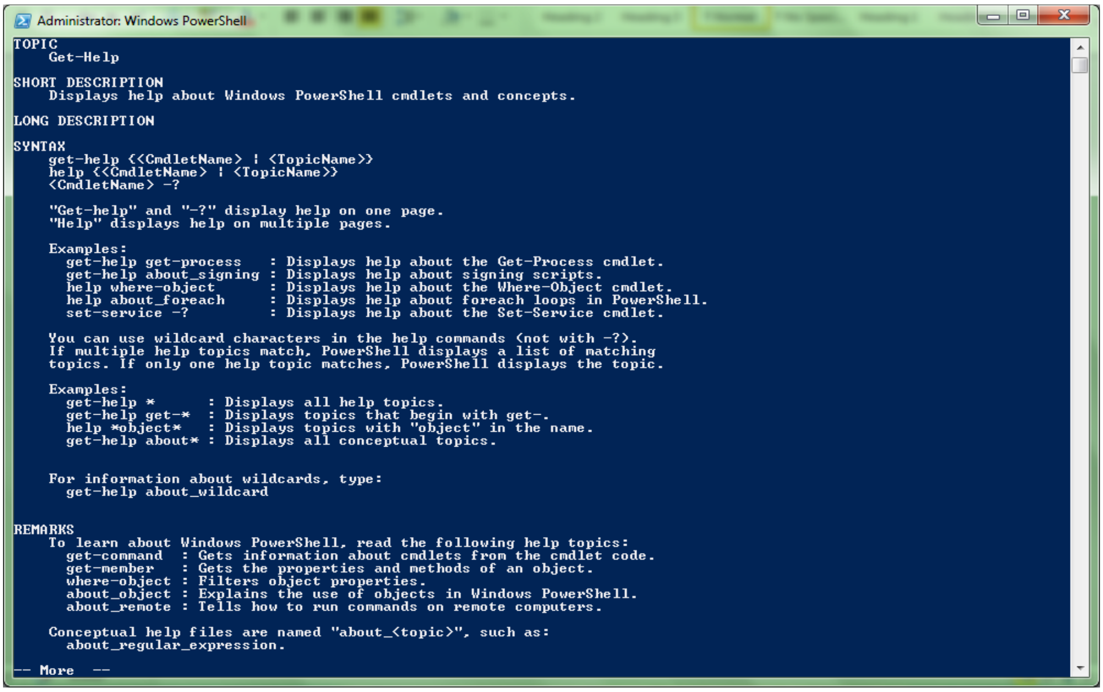
Path សម្រាប់ Prompt ភ្ជាប់មកជាមួយអក្សរ PS មានផ្ទៃខាងក្រោយពណ៌ខៀវ។ អ្នកក៏អាចប្រើបញ្ជាដូចក្នុង MS-DOS ដែរដូចជាបញ្ជា CD,DIR,COPY MOVE,DEL ។ល។



រូបភាព១២-២ បង្ហាញពីការប្រើបញ្ជា dir

តាមការពិតបញ្ជានេះគឺជា aliases នៃ PowerShell cmdlets ប៉ុណ្ណោះ។

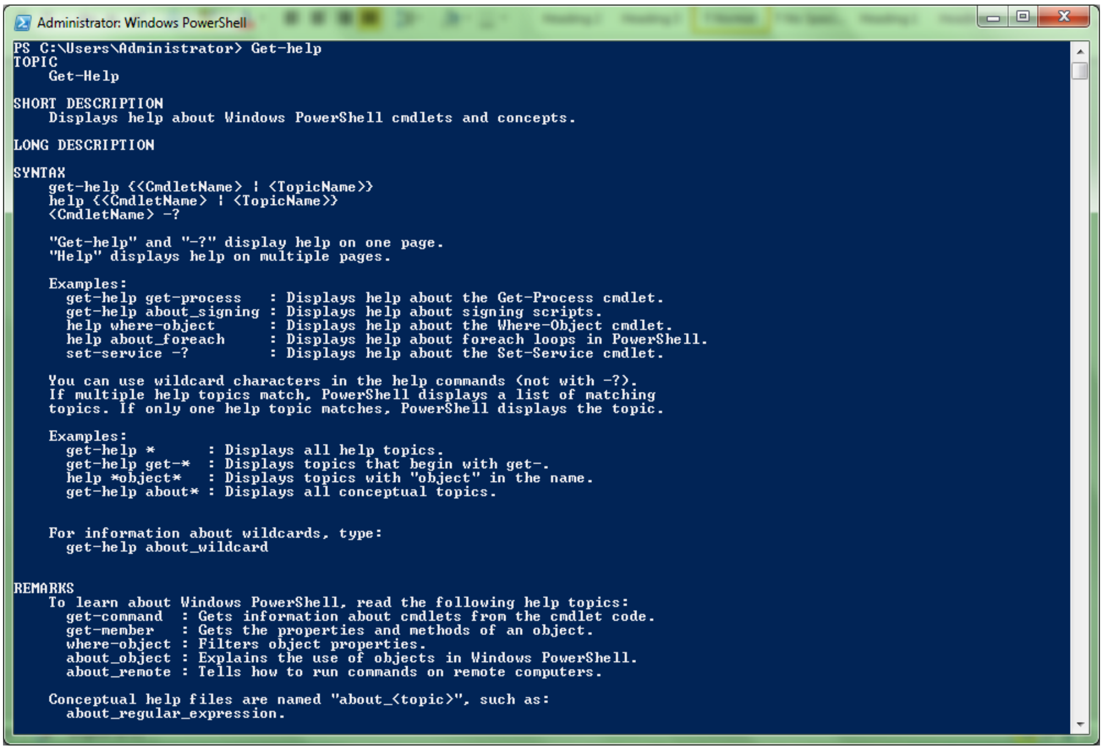
ដើម្បីបង្ហាញរាល់បញ្ជាដែលមានក្នុង Windows PowerShell យើងត្រូវប្រើបញ្ជា help



```
TOPIC
    Get-Help

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION

SYNTAX
    get-help {<CmdletName> | <TopicName>}
    help {<CmdletName> | <TopicName>}
    <CmdletName> -?

    "Get-help" and "-?" display help on one page.
    "Help" displays help on multiple pages.

    Examples:
      get-help get-process    : Displays help about the Get-Process cmdlet.
      get-help about_signing  : Displays help about signing scripts.
      help where-object       : Displays help about the Where-Object cmdlet.
      help about_foreach      : Displays help about foreach loops in PowerShell.
      set-service -?          : Displays help about the Set-Service cmdlet.

    You can use wildcard characters in the help commands (not with -?).
    If multiple help topics match, PowerShell displays a list of matching
    topics. If only one help topic matches, PowerShell displays the topic.

    Examples:
      get-help *       : Displays all help topics.
      get-help get-*   : Displays topics that begin with get-.
      help *object*    : Displays topics with "object" in the name.
      get-help about*  : Displays all conceptual topics.

    For information about wildcards, type:
      get-help about_wildcard

REMARKS
    To learn about Windows PowerShell, read the following help topics:
      get-command  : Gets information about cmdlets from the cmdlet code.
      get-member   : Gets the properties and methods of an object.
      where-object : Filters object properties.
      about_object : Explains the use of objects in Windows PowerShell.
      about_remote : Tells how to run commands on remote computers.

    Conceptual help files are named "about_<topic>", such as:
      about_regular_expression.

-- More  --
```

រូបភាព១២-៣ ការប្រើបញ្ជា help ដើម្បីមើលរាល់បញ្ជាដែលមានក្នុងPowerShell

បើអ្នកចង់ដឹងអំពីបញ្ជាពិសេសណាមួយ អ្នកអាចប្រើបញ្ជា **Get-help**

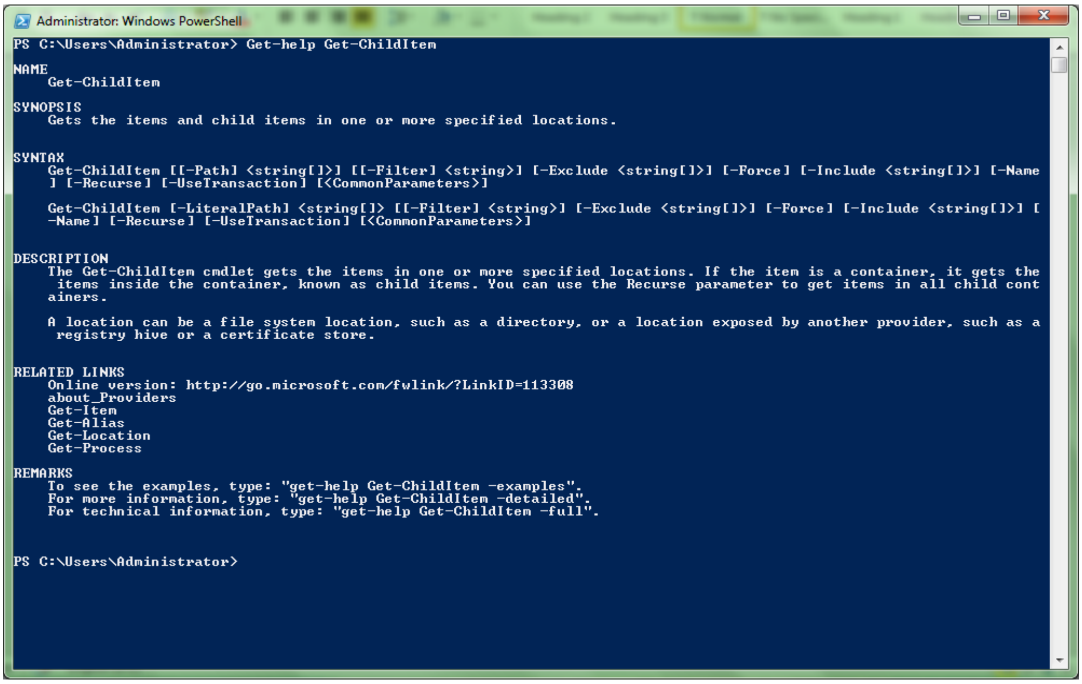


```
PS C:\Users\Administrator> Get-help
TOPIC
    Get-Help

SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.

LONG DESCRIPTION

SYNTAX
    get-help {<CmdletName> | <TopicName>}
    help {<CmdletName> | <TopicName>}
    <CmdletName> -?

    "Get-help" and "-?" display help on one page.
    "Help" displays help on multiple pages.

    Examples:
      get-help get-process    : Displays help about the Get-Process cmdlet.
      get-help about_signing  : Displays help about signing scripts.
      help where-object       : Displays help about the Where-Object cmdlet.
      help about_foreach      : Displays help about foreach loops in PowerShell.
      set-service -?          : Displays help about the Set-Service cmdlet.

    You can use wildcard characters in the help commands (not with -?).
    If multiple help topics match, PowerShell displays a list of matching
    topics. If only one help topic matches, PowerShell displays the topic.

    Examples:
      get-help *       : Displays all help topics.
      get-help get-*   : Displays topics that begin with get-.
      help *object*    : Displays topics with "object" in the name.
      get-help about*  : Displays all conceptual topics.

    For information about wildcards, type:
      get-help about_wildcard

REMARKS
    To learn about Windows PowerShell, read the following help topics:
      get-command  : Gets information about cmdlets from the cmdlet code.
      get-member   : Gets the properties and methods of an object.
      where-object : Filters object properties.
      about_object : Explains the use of objects in Windows PowerShell.
      about_remote : Tells how to run commands on remote computers.

    Conceptual help files are named "about_<topic>", such as:
      about_regular_expression.
```

រូបភាព១២-៣ លទ្ធផលនៃ Get-help

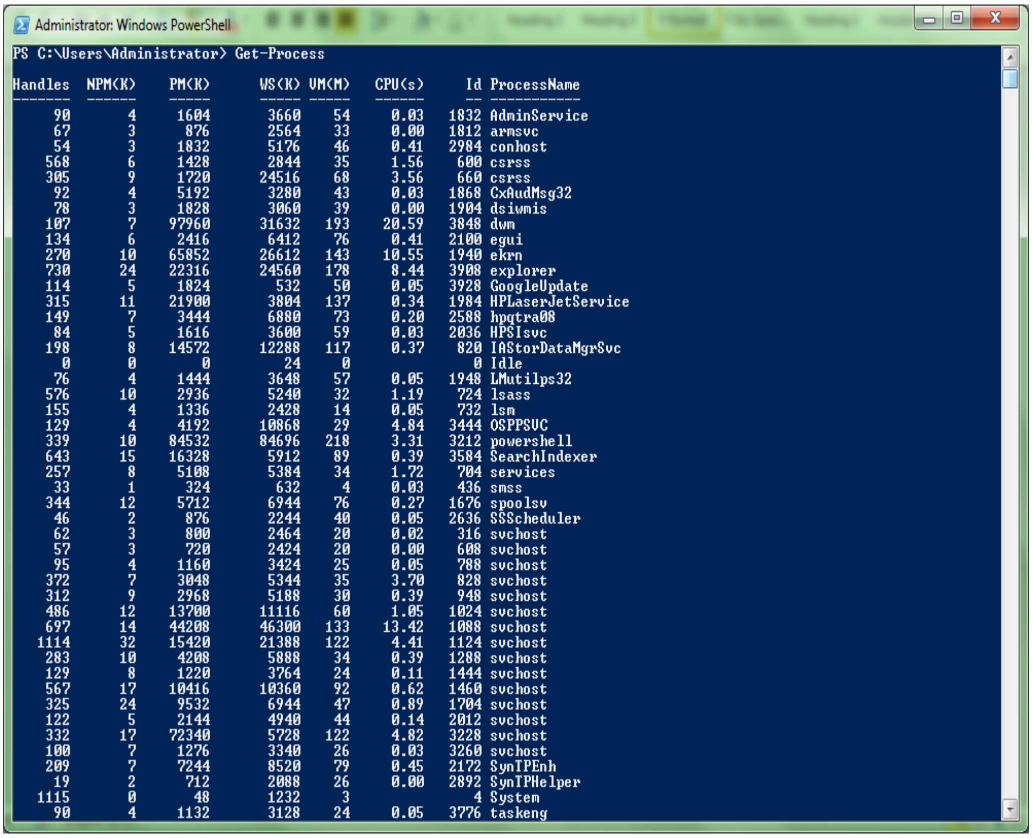
ឧទាហរណ៍ បើអ្នកចង់ដឹងពី Get-ChildItem គេប្រើបញ្ជា

Get-help Get-ChilItem


```
PS C:\Users\Administrator> Get-help Get-ChildItem

NAME
    Get-ChildItem

SYNOPSIS
    Gets the items and child items in one or more specified locations.


SYNTAX
    Get-ChildItem [[-Path] <string[]>] [[-Filter] <string>] [-Exclude <string[]>] [-Force] [-Include <string[]>] [-Name
    ] [-Recurse] [-UseTransaction] [<CommonParameters>]

    Get-ChildItem [-LiteralPath] <string[]> [[-Filter] <string>] [-Exclude <string[]>] [-Force] [-Include <string[]>] [
    -Name] [-Recurse] [-UseTransaction] [<CommonParameters>]


DESCRIPTION
    The Get-ChildItem cmdlet gets the items in one or more specified locations. If the item is a container, it gets the
     items inside the container, known as child items. You can use the Recurse parameter to get items in all child cont
    ainers.

    A location can be a file system location, such as a directory, or a location exposed by another provider, such as a
     registry hive or a certificate store.


RELATED LINKS
    Online version: http://go.microsoft.com/fwlink/?LinkID=113308
    about_Providers
    Get-Item
    Get-Alias
    Get-Location
    Get-Process

REMARKS
    To see the examples, type: "get-help Get-ChildItem -examples".
    For more information, type: "get-help Get-ChildItem -detailed".
    For technical information, type: "get-help Get-ChildItem -full".


PS C:\Users\Administrator>
```

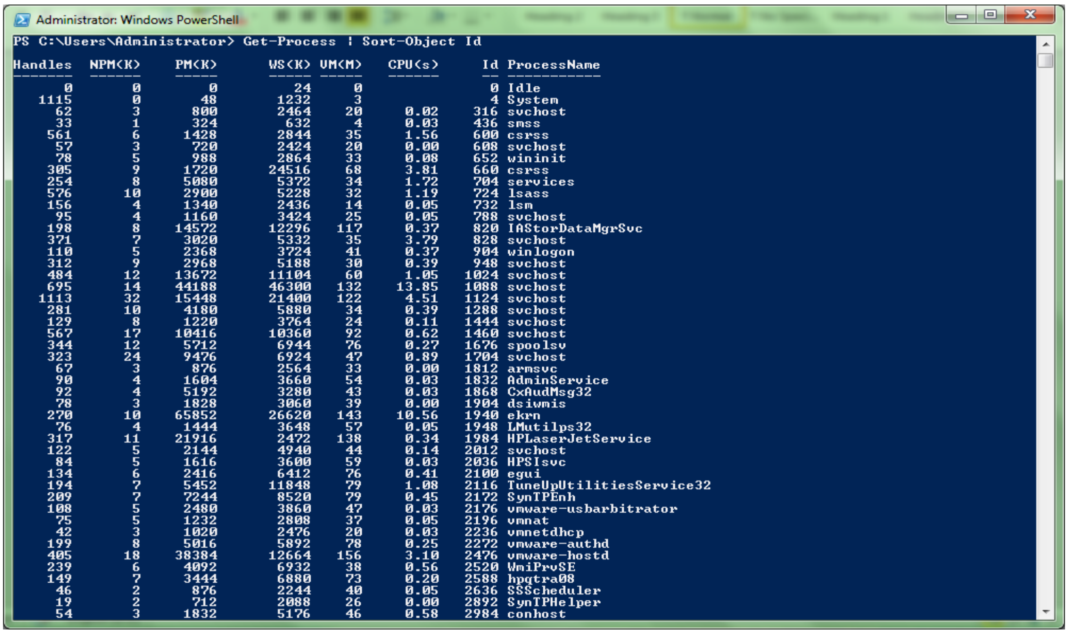
រូបភាព១២-៤ លទ្ធផលនៃ Get-help Get-ChildItem

ដើម្បីបង្ហាញគ្រប់ Processes ទាំងអស់ គេប្រើបញ្ជា Get-Process


```
PS C:\Users\Administrator> Get-Process

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
     90       4     1604       3660    54     0.03   1832 AdminService
     67       3      876       2564    33     0.00   1812 armsvc
     54       3     1832       5176    46     0.41   2984 conhost
    568       6     1428       2844    35     1.56    600 csrss
    305       9     1720      24516    68     3.56    660 csrss
     92       4     5192       3280    43     0.03   1868 CxAudMsg32
     78       3     1828       3060    39     0.00   1904 dsiwmis
    107       7    97960      31632   193    20.59   3848 dwm
    134       6     2416       6412    76     0.41   2100 egui
    270      10    65852      26612   143    10.55   1940 ekrn
    730      24    22316      24560   178     8.44   3908 explorer
    114       5     1824        532    50     0.05   3928 GoogleUpdate
    315      11    21900       3804   137     0.34   1984 HPLaserJetService
    149       7     3444       6880    73     0.20   2588 hpqtra08
     84       5     1616       3600    59     0.03   2036 HPSIsvc
    198       8    14572      12288   117     0.37    820 IAStorDataMgrSvc
      0       0        0         24     0              0 Idle
     76       4     1444       3648    57     0.05   1948 LMutilps32
    576      10     2936       5240    32     1.19    724 lsass
    155       4     1336       2428    14     0.05    732 lsm
    129       4     4192      10868    29     4.84   3444 OSPPSVC
    339      10    84532      84696   218     3.31   3212 powershell
    643      15    16328       5912    89     0.39   3584 SearchIndexer
    257       8     5108       5384    34     1.72    704 services
     33       1      324        632     4     0.03    436 smss
    344      12     5712       6944    76     0.27   1676 spoolsv
     46       2      876       2244    40     0.05   2636 SSScheduler
     62       3      800       2464    20     0.02    316 svchost
     57       3      720       2424    20     0.00    608 svchost
     95       4     1160       3424    25     0.05    788 svchost
    372       7     3048       5344    35     3.70    828 svchost
    312       9     2968       5188    30     0.39    948 svchost
    486      12    13700      11116    60     1.05   1024 svchost
    697      14    44208      46300   133    13.42   1088 svchost
   1114      32    15420      21388   122     4.41   1124 svchost
    283      10     4208       5888    34     0.39   1288 svchost
    129       8     1220       3764    24     0.11   1444 svchost
    567      17    10416      10360    92     0.62   1460 svchost
    325      24     9532       6944    47     0.89   1704 svchost
    122       5     2144       4940    44     0.14   2012 svchost
    332      17    72340       5728   122     4.82   3228 svchost
    100       7     1276       3340    26     0.03   3260 svchost
    209       7     7244       8520    79     0.45   2172 SynTPEnh
     19       2      712       2088    26     0.00   2892 SynTPHelper
   1115       0       48       1232     3              4 System
     90       4     1132       3128    24     0.05   3776 taskeng
```

រូបភាព១២-៥ លទ្ធផលនៃ Get-Process

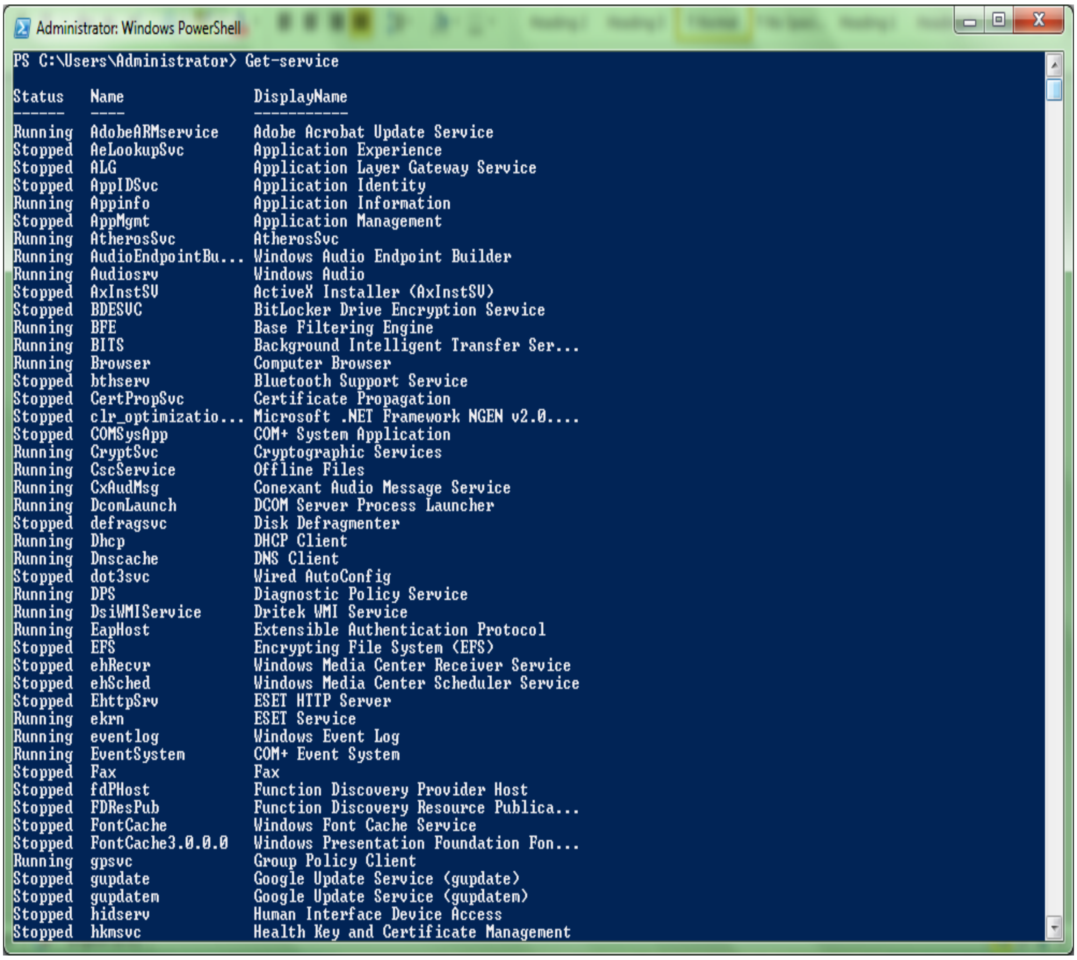
ដើម្បីបង្ហាញ Process តាមការរៀបជាលំដាប់ គេប្រើបញ្ជា Get-Process | sort-Object Id



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-Process | Sort-Object Id

Handles  NPM(K)    PM(K)      WS(K) VM(M)   CPU(s)     Id ProcessName
-------  ------    -----      ----- -----   ------     -- -----------
      0       0        0         24     0               0 Idle
   1115       0       48       1232     3               4 System
     62       3      800       2464    20     0.02    316 svchost
     33       1      324        632     4     0.03    436 smss
    561       6     1428       2844    35     1.56    600 csrss
     57       3      720       2424    20     0.00    608 svchost
     78       5      988       2864    33     0.08    652 wininit
    305       9     1720      24516    68     3.81    660 csrss
    254       8     5080       5372    34     1.72    704 services
    576      10     2900       5228    32     1.19    724 lsass
    156       4     1340       2436    14     0.05    732 lsm
     95       4     1160       3424    25     0.05    788 svchost
    198       8    14572      12296   117     0.37    820 IAStorDataMgrSvc
    371       7     3020       5332    35     3.79    828 svchost
    110       5     2368       3724    41     0.37    904 winlogon
    312       9     2968       5188    30     0.39    948 svchost
    484      12    13672      11104    60     1.05   1024 svchost
    695      14    44188      46300   132    13.85   1088 svchost
   1113      32    15448      21400   122     4.51   1124 svchost
    281      10     4180       5880    34     0.39   1288 svchost
    129       8     1220       3764    24     0.11   1444 svchost
    567      17    10416      10360    92     0.62   1460 svchost
    344      12     5712       6944    76     0.27   1676 spoolsv
    323      24     9476       6924    47     0.89   1704 svchost
     67       3      876       2564    33     0.00   1812 armsvc
     90       4     1604       3660    54     0.03   1832 AdminService
     92       4     5192       3280    43     0.03   1868 CxAudMsg32
     78       3     1828       3060    39     0.00   1904 dsiwmis
    270      10    65852      26620   143    10.56   1940 ekrn
     76       4     1444       3648    57     0.05   1948 LMutilps32
    317      11    21916       2472   138     0.34   1984 HPLaserJetService
    122       5     2144       4940    44     0.14   2012 svchost
     84       5     1616       3600    59     0.03   2036 HPSIsvc
    134       6     2416       6412    76     0.41   2100 egui
    194       7     5452      11848    79     1.08   2116 TuneUpUtilitiesService32
    209       7     7244       8520    79     0.45   2172 SynTPEnh
    108       5     2480       3860    47     0.03   2176 vmware-usbarbitrator
     75       5     1232       2808    37     0.05   2196 vmnat
     42       3     1020       2476    20     0.03   2236 vmnetdhcp
    199       8     5016       5892    78     0.25   2272 vmware-authd
    405      18    38384      12664   156     3.10   2476 vmware-hostd
    239       6     4092       6932    38     0.56   2520 WmiPrvSE
    149       7     3444       6880    73     0.20   2588 hpqtra08
     46       2      876       2244    40     0.05   2636 SSScheduler
     19       2      712       2088    26     0.00   2892 SynTPHelper
     54       3     1832       5176    46     0.58   2984 conhost
```

រូបភាព១២-៦ ការរៀប Process តាមលំដាប់

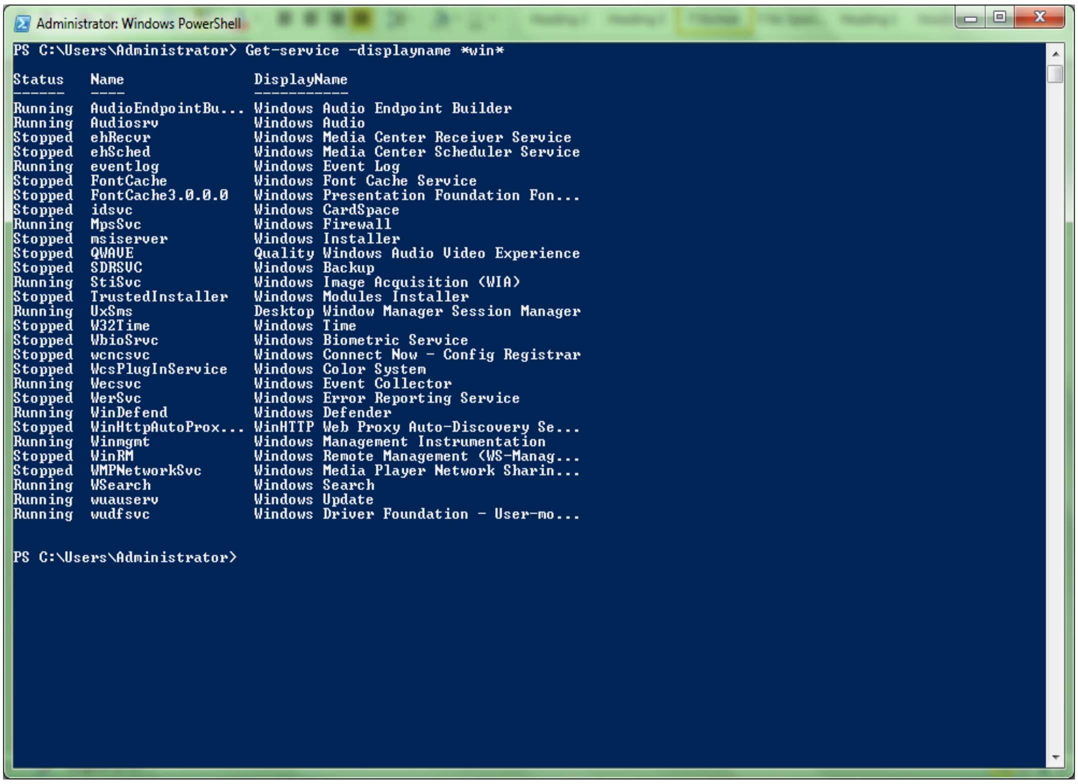
ដើម្បីបង្ហាញគ្រប់ Services ដែលមាននៅក្នុង System គេប្រើបញ្ជា **Get-Service**



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> Get-service

Status   Name               DisplayName
------   ----               -----------
Running  AdobeARMservice    Adobe Acrobat Update Service
Stopped  AeLookupSvc        Application Experience
Stopped  ALG                Application Layer Gateway Service
Stopped  AppIDSvc           Application Identity
Running  Appinfo            Application Information
Stopped  AppMgmt            Application Management
Running  AtherosSvc         AtherosSvc
Running  AudioEndpointBu... Windows Audio Endpoint Builder
Running  Audiosrv           Windows Audio
Stopped  AxInstSV           ActiveX Installer (AxInstSV)
Stopped  BDESVC             BitLocker Drive Encryption Service
Running  BFE                Base Filtering Engine
Running  BITS               Background Intelligent Transfer Ser...
Running  Browser            Computer Browser
Stopped  bthserv            Bluetooth Support Service
Stopped  CertPropSvc        Certificate Propagation
Stopped  clr_optimizatio... Microsoft .NET Framework NGEN v2.0....
Stopped  COMSysApp          COM+ System Application
Running  CryptSvc           Cryptographic Services
Running  CscService         Offline Files
Running  CxAudMsg           Conexant Audio Message Service
Running  DcomLaunch         DCOM Server Process Launcher
Stopped  defragsvc          Disk Defragmenter
Running  Dhcp               DHCP Client
Running  Dnscache           DNS Client
Stopped  dot3svc            Wired AutoConfig
Running  DPS                Diagnostic Policy Service
Running  DsiWMIService      Dritek WMI Service
Running  EapHost            Extensible Authentication Protocol
Stopped  EFS                Encrypting File System (EFS)
Stopped  ehRecvr            Windows Media Center Receiver Service
Stopped  ehSched            Windows Media Center Scheduler Service
Stopped  EhttpSrv           ESET HTTP Server
Running  ekrn               ESET Service
Running  eventlog           Windows Event Log
Running  EventSystem        COM+ Event System
Stopped  Fax                Fax
Stopped  fdPHost            Function Discovery Provider Host
Stopped  FDResPub           Function Discovery Resource Publica...
Stopped  FontCache          Windows Font Cache Service
Stopped  FontCache3.0.0.0   Windows Presentation Foundation Fon...
Running  gpsvc              Group Policy Client
Stopped  gupdate            Google Update Service (gupdate)
Stopped  gupdatem           Google Update Service (gupdatem)
Stopped  hidserv            Human Interface Device Access
Stopped  hkmsvc             Health Key and Certificate Management
```

រូបភាព១២-៧ បង្ហាញពីលទ្ធផលនៃ Get-service command

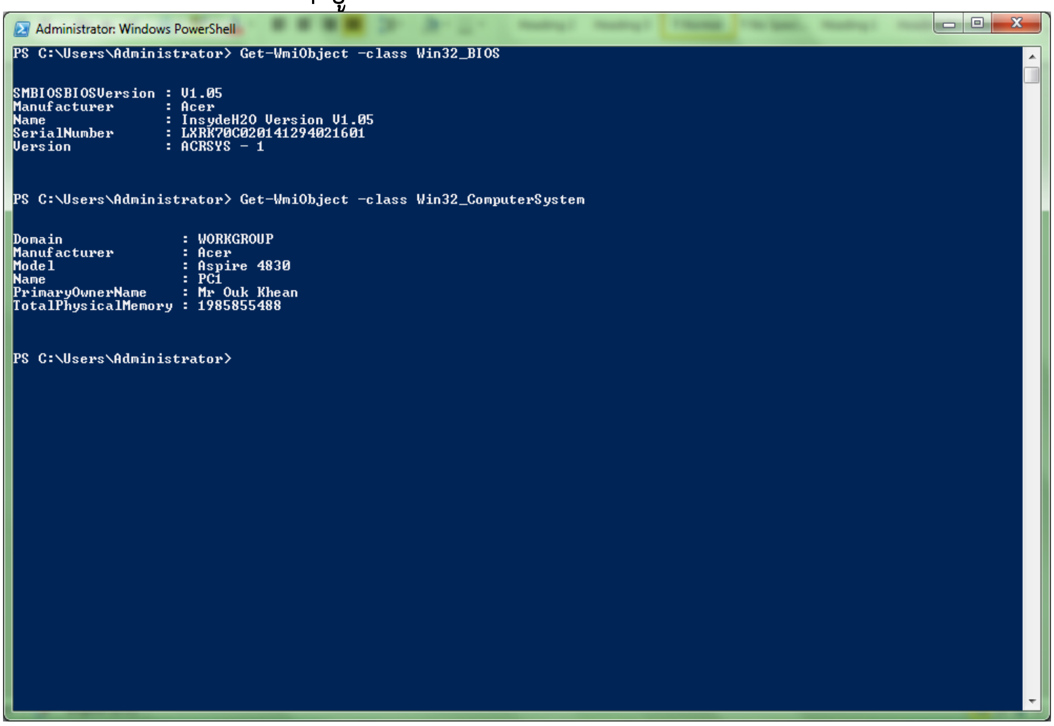
ដើម្បីបង្ហាញពីលក្ខណ:របស់ Services ដែលមានពាក្យថា win



រូបភាព១២-៨ បង្ហាញពី Service ដែលមានពាក្យថា win

បើយើងចង់ដឹងព័ត៌មានអំពី BIOS និង System អ្នកអាច query Win32_BIOS និង Win32_កុំព្យូទ័រ System WMI class ជាមួយបញ្ជា Get-WmiObject –class Win32_BIO

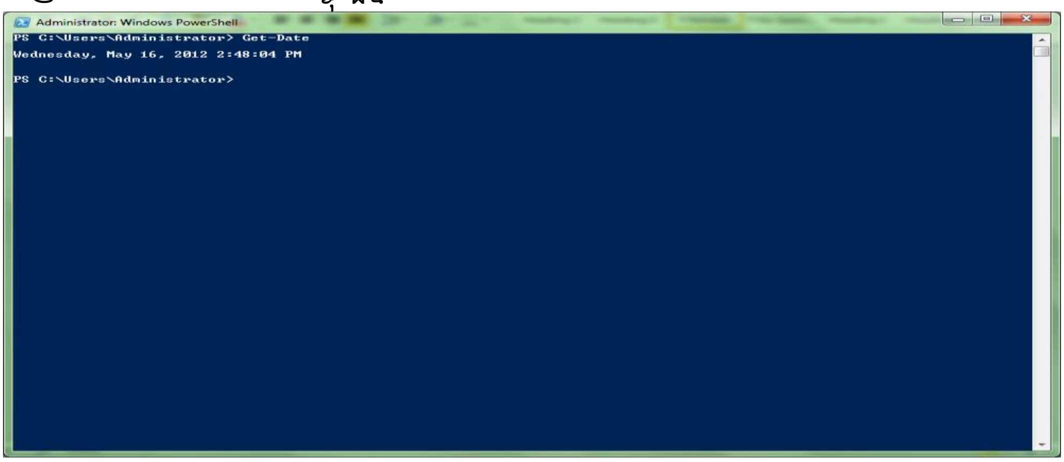
Get-WmiObject –class Win32_កុំព្យូទ័រSystem



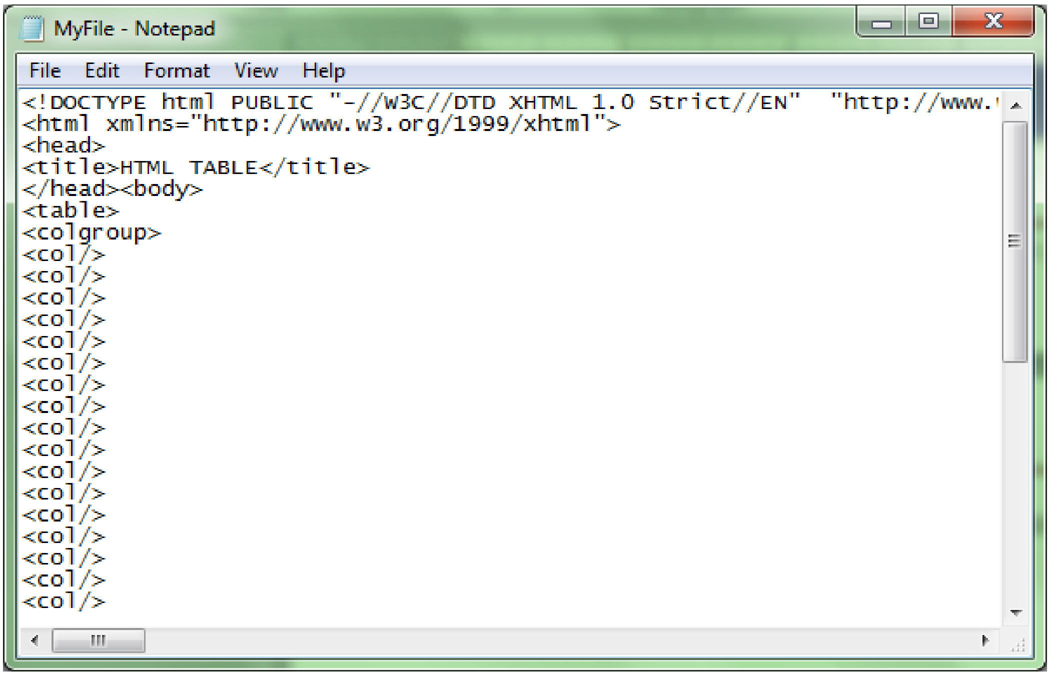
រូបភាព១២-៩ បង្ហាញពីលទ្ធផលនៃបញ្ជាខាងលើ

១៨-២- CMDLETS

Cmdlets អនុវត្តតាមឈ្មោះ **verb-noun**។ ហេតុផលងាយបំផុតគឺឈ្មោះរបស់វាពិពណ៌នាអំពីខ្លួនវា។ ឧទាហរណ៍ Get-Service cmdlets ត្រូវបានប្រើសម្រាប់ទទួលព័ត៌មានអំពី Service ។ Get-Date cmdlets សម្រាប់ទាញយក date និង Time បច្ចុប្បន្ន ។



ឧបមាថាអ្នកចង់បំប្លែងលទ្ធផលជា HTML ។ គេប្រើបញ្ជា Get-ChildItem | convertTo-HTML > MyFile.html



រូបភាពនៃ១២-១០ បង្ហាញពីលទ្ធផលនៃ Get-ChildItem | convertTO-HTML > MyFile.html

១៨-៣- Windows PowerShell and .NET

Windows PowerShell ត្រូវបានបង្កើតឡើងដើម្បីបំពេញតម្រូវការ Script language ដែលផ្តល់ឱ្យនូវ Interface ជាមួយ .NET ។

១៨-២-១- Windows PowerShell, Scripting and Security

តាមធម្មជាតិនៃ PowerShell command-line គឺជា shell ដែលត្រូវបានគេសរសេរដោយ Script អ្នកអាចបង្កើត Script សម្រាប់ Windows PowerShell បានយ៉ាងងាយ ។ មាន Execution Policy បួនយ៉ាងគឺ

- Restricted (Default) No Script are allowed
- AllSigned Only Signed Scripts are allowed
- RemoteSigned locally executed scripts are allowed. Any thing else must be signed
- Unrestricted All scripts are allowed

ដើម្បីប្តូរ Execution មកជា RemoteSigned

Set-ExecutionPolicy RemoteSigned

លំហាត់អនុវត្ត បង្កើត PowerShell ដំបូង

1- បើក Notepad ហើយវាយបញ្ចូលឃ្លាខាងក្រោម

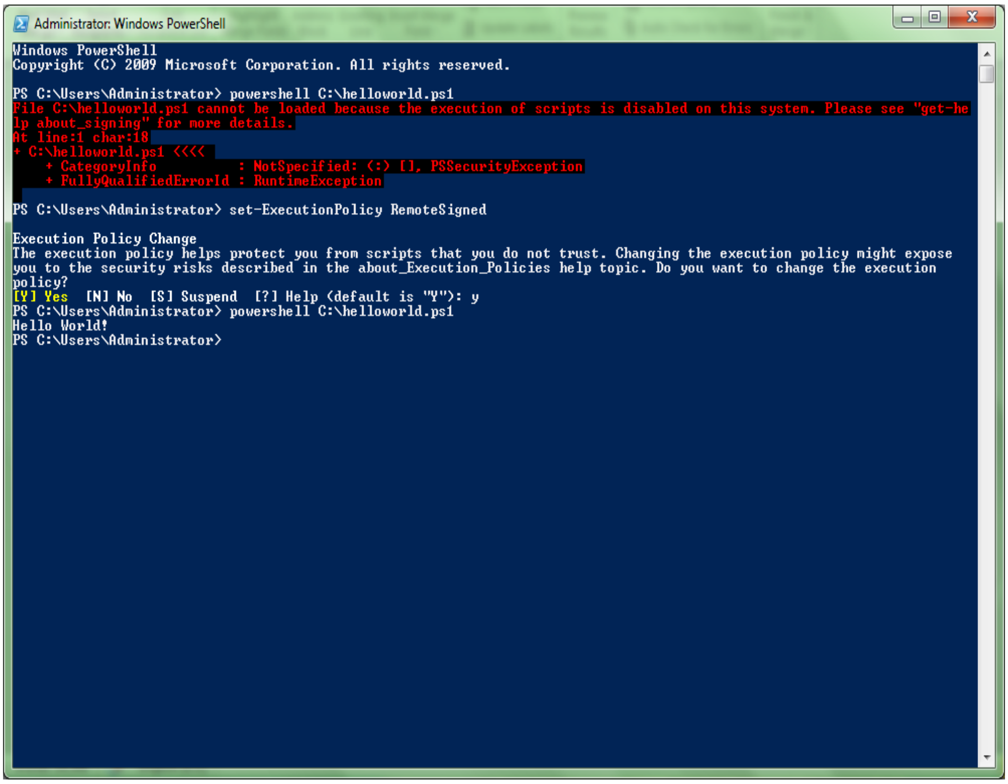
$s="Hello World !"

Write-host $s

2- Save file c:\helloworld.ps1

3- Run

Powershell C:\helloworld.ps1



អថេរ (Variables)

អថេរមាននៅគ្រប់ Script language ទាំងអស់។ នៅក្នុង Windows PowerShell អ្នកអាចប្រើឈ្មោះអ្វីក៏បានជាអថេរ ប៉ុន្តែវាត្រូវចាប់ផ្តើមជាមួយសញ្ញាដុល្លា ($) ។ អ្នកអាចប្រើ បន្សំនៃតួអក្សរ លេខ និងនិមិត្តសញ្ញា។ អ្នកក៏អាចប្រើសញ្ញាដកឃ្លាបានដែរជាមួយអថេរដោយអ្នកគ្រាន់តែប្រើសញ្ញា {} ។

ឧទាហរណ៍

$MyName = "Ouk Khean"

$x = 5

${Variable with space} = "See the curly brace"

Windows PowerShell ក៏មាន Typecased variable ដែរ។ នេះមានន័យថាអ្នកអាចប្រាប់ PowerShell ប្រភេទនៃអថេរដែលត្រូវរក្សាទុកវា។

ឧទាហរណ៍

```
$a = 2
Write-host {$a + 2}
```

យើងបានកំណត់តម្លៃលេខ 2 ទៅឱ្យអថេរ $a ហើយបន្ទាប់មកបង្ហាញលទ្ធផលនៃ $a + 2 ។ តាមការសង្ឃឹមទុកជាមុនលទ្ធផលគឺស្មើនិង៤។

សូមពិនិត្យមើល Code

```
$a  = 2
$s = "some string "
----some more code……
$a = "Ouk Khean"
…….some more code…..
Write-host {$a + 2}
```

នៅក្នុងឧទាហរណ៍នេះអ្នកអាចបង្កើតអថេរពីរគឺ $aមានតម្លៃ២ចំណែកឯ $s មានតម្លៃជា Some String ។ សន្មត់ថាអ្នកបានកំណត់តម្លៃដោយចៃដន្យដោយ "Ouk Khean"ទៅឱ្យអថេរ $a នៅពេលដែលអ្នកចង់កំណត់តម្លៃទៅឱ្យ $s ។ បើអ្នកមាន QUERTY keyboard អក្សរ A key នៅជាប់នឹងអក្សរ s ដូច្នេះអាចមានកំហុសកើតឡើង។ ដូច្នេះមានតម្លៃស្មើនិង៤។ បើវាជា Script ដែលមាន Code ច្រើន នោះ Error កើតឡើងនិងពិបាកស្វែងរក។

ដើម្បីជៀសវាងប្រភេទនៃបញ្ហានេះកើតឡើង អ្នកអាចប្រើ typedcast ចំពោះអថេរនីមួយៗ ដូចខាងក្រោម

```
[int] $a + 2
[string] $s = "some String"
…..some more code….
$a = "Ouk Khean "
……some more code…..
Write-host {$a + 2 }
```

យើងបានប្រាប់ Windows PowerShell ឱ្យដឹងថាអថេរ $a ត្រូវរក្សាទុកតម្លៃជា integer ចំណែកឯអថេរ$s វិញត្រូវរក្សាទុកតម្លៃជា String។ បើអ្នក Run កូដនេះវានិងបង្ហាញ Error ឱ្យដឹងថា "Ouk Khean" មិនអាចបំប្លែងជា System.Int32 នោះបានទេ។

១៨-៣- ប្រភេទនៃអថេរ Windows PowerShell ដែលនិយមប្រើ

ដោយសារតែ Windows PowerShell ត្រូវបានបង្កើតឡើងជាផ្នែកមួយនៃ .NET framework អ្នកអាចប្រើអថេរឬ Object Type ដែលមាននៅក្នុង .NET framework នៅពេលកំណត់អថេរ។ អថេរដែលគេនិយមប្រើមានដូចខាងក្រោម

- [Boolean] True or false
- [int] 32-bit integer
- [char] single character
- [string] String of Characters
- [single] Single-precision floating number(a number containing decimals –i.e 1.232)
- [double] Double-precision floating point number(the same as single except it allows for a greater range of values and precision)
- [datetime] Date or time
- [adsi] ADSI object
- [wmi] WMI instance or collection
- [wmiclass] WMI class

Array គឺជា simple data structure ដែលជាក្រុមនៃតម្លៃឬObject ដែលអាច Access បានដោយប្រើឈ្មោះដូចគ្នា ប៉ុន្តែប្រើ index ដើម្បី Access ធាតុនីមួយៗ។ បើអ្នកពិនិត្យមើល VBScript code អ្នកនិងឃើញវាមានលក្ខណៈដូចខាងក្រោម

```
Dim myArr[2]
myArr[0] = "First"
myArr[1]= "Second "
myArr[2]= "third"
Wscript.Echo myArr( 1 )
```

នេះមិនមែនជា VBscript tutorial នោះទេ ដូច្នេះយើងនិងមិនសិក្សាឱ្យស៊ីជំរៅទៅលើវានោះទេ។ នៅក្នុង Code នេះបានបង្ហាញពី Array ដែលមានបីធាតុ។

ចំពោះ Code ខាងក្រោមនេះបង្ហាញពី Array ក្នុង Windows PowerShell:

```
$myArr = "First ", "Second ", "third "
$myArr[1]= "2nd "
Write-host $myArr
```

លទ្ធផលនៃ Code ដ៏ខ្លីនេះគឺ first 2nd third ដែលត្រូវបង្ហាញលើបន្ទាត់តែមួយ។ ដូចទៅនិង Programming Language ជាច្រើនដែរ Array មាន index 0 ដូច្នេះ $myArr[0] គឺជាធាតុទី១។$myArr[1] គឺជាធាតុទី២។ល។

នៅក្នុង Windows PowerShell គេសរសេរ

```
$myArr = "First", "second","third"
$myArr = $myArr + "fourth ", "fifth"
Write-host $myArr[4]
```

ក្នុង Code នេះវានិងបង្ហាញនូវ String ទី៥។ ចំណាំថា អ្វីដែលអ្នកត្រូវធ្វើគឺពង្រីក Array ដែលមានស្រាប់សម្រាប់បន្ថែម data ថ្មីដោយប្រើសញ្ញា + ។

១៨-៤- ឃ្លាប្រយោគមានលក្ខខណ្ឌ

លក្ខណៈពិសេសមួយដែលត្រូវការក្នុង Script គឺសមត្ថភាពកំណត់ឃ្លាលក្ខខណ្ឌដូចជា *if x equal 2 then do this otherwise do something else* ។ អ្នកមិនអាចប្រើ Logic ណាមួយក្នុង Script បាននោះទេ។

ឧទាហរណ៍

```
$a = 5
If ( $a -eq 1 ) {
Write-host "One"
}
Elseif ( $a –eq 2 ) {
Write-host "Two"
}
Else {
Write-host "Anything but One or Two!"
}
```

ជាដំបូងអ្នកបានកំណត់តម្លៃឱ្យអថេរ $a ស្មើនិង៥។ បន្ទាប់មកត្រួតពិនិត្យមើលឱ្យដឹងថា$a មានតម្លៃ 1 ឬទេ បើស្មើ ១ នោះលទ្ធផលគឺ១។ បើមិនស្មើ១នោះទេ វានិងត្រួតពិនិត្យថាតើវាស្មើ២ឬទេ បើស្មើ២វានិងបង្ហាញលទ្ធផល២។ បើមិនបំពេញលក្ខខណ្ឌណាមួយទេវានិងបង្ហាញថា Anything but One or Two ។

១៨-៥- Operator ក្នុង PowerShell

ក្នុង Windows PowerShell មាន Operators ដូចខាងក្រោម

- -eq Equal to
- -ne Not equal to
- -notmatch Does not match
- -gt Grater than
- -ge Greater than or equal to
- -lt Less than
- -le Less than or equal to

ឧទាហរណ៍

```
$color = "blue"
Switch ( $color ) {
red { write-host "color Red"; break}
blue { write-host "color blue"; break}
yellow { write-host "color yellow"; break}
```

```
white { write-host "color white"; break}
green { write-host "color green"; break}
orange { write-host "color yellow"; orange}
black { write-host "color black"; break}
```

១៨-៦- Going Loopy

ចំណុចមួយដ៏សំខាន់ដែល Network Administrator ត្រូវសរសេរ Script គឺដើម្បីឱ្យកិច្ចការដំណើរការជាស្វ័យប្រវត្ត។

Loops គឺជាបញ្ហាមួយដ៏ងាយបំផុត។ អ្នកអាចប្រើ Loops ក្នុង Windows PowerShell ដូចជា For , Foreach, while, and Do…while ។

```
For ( <init>;<condition>;<repeat> ){
<code> to run in the loop>
}
```

ឧទាហរណ៍

```
For( $i=1;$i –lt 101;$1++ ) {
White-host $i
}
```

<init> ត្រូវបាន execute តែម្តងគត់ហើយត្រូវបានប្រើដើម្បីចាប់ផ្តើម។ នៅក្នុងឧទាហរណ៍នេះ $i មានតម្លៃស្មើ១។ <condition> សម្រាប់កំណត់ឱ្យលក្ខខណ្ឌពិតមុនពេលដែល Block code ត្រូវបាន Execute ។ យើងបានកំណត់ $i តូចជាង ១០១ ដែលវាអាច Execute block នៃ Code បាន។ <repeat> ត្រូវបាន Execute នៅរាល់ពេលដែល Code ត្រូវបាន Execute ។ នៅក្នុងករណីនេះវានិងកើនឡើងម្តង១ៗគ្រប់ជំហាននៃ Execute ។ វាប្រើសញ្ញា $i++ មានន័យថា $i=$i + 1 ។

ចំពោះ Foreach វិញត្រូវបានគេប្រើប្រាស់សម្រាប់ loop ដែលឆ្លងកាត់តាមការប្រមូលផ្តុំនៃ Items វាមិនដូច For loop នោះទេដែលអ្នកអាចកំណត់អថេរ លក្ខខណ្ឌឈប់ និងការធ្វើឡើងវិញប្រចាំដែលៗ ។ ចំពោះ Foreach វិញត្រូវបានបង្កើតឡើងសម្រាប់ធ្វើការប្រមូលផ្តុំប៉ារ៉ាម៉ែត្ររបស់វា ហើយដំណើរការបណ្តុំនៃកូដសម្រាប់ Item នីមួយៗដែលមាននៅក្នុងcollection នោះ។

ឧទាហរណ៍

```
Foreach ( $<item> in $<collection> ){
<command_block>
}
Foreach ( $file in Get-ChildItem C:\windows ) {
Write-host $file
}
Syntax for a while loop
While ( <condition> ) {
<code_block>
```

}

ឧទាហរណ៏

```
$i = 1
While ( $i –lt 101 ) {
Write-host $i
$i ++
}
```

Do …while statement

```
$a = 1
do {
        write-host $a
$a++
} while ( $a –lt 10 )
Write-host "Done"
```

Code នេះយើងព្យាយាមរាប់ពី ១ ទៅ ១០។ $a ចាប់ផ្តើមជាមួយតម្លៃ 0 ។

១៥-៧- PowerShell in Action

បើអ្នកជាអ្នកគ្រប់គ្រង់លើ Windows system អ្នកត្រូវបង្ហាញថា Powershell ធ្វើឱ្យជីវិតកាន់តែងាយស្រួលមុនពេលយើងចាប់ផ្តើមប្រើវា។ យើងត្រឡប់មក Get-Service cmdlet ។ Get-Service បង្ហាញលទ្ធផលជា collection នៃ service Objects ដោយរួមមាន Properties ។ ឧបមាថាអ្នកចង់បង្ហាញតារាង Service ដែលកំពុងដំណើរការដោយពឹងផ្អែកលើ Data ដែលបានទាញយកដោយ Get-Service ។

```
Get-Service | Foreach {if ( $_.Status –eq "Running" ) { write-host $_.DisplayName} )
```

យើងត្រូវពន្យល់អំពីអ្វីដែលថ្មីនៅទីនេះ។ ចំពោះ Get-Service គឺជា command មួយដែលយើងបានសិក្សារួចមកហើយ។ វាដំណើរការហើយផ្តល់ឱ្យលទ្ធផលរបស់វាត្រូវបានផ្តល់មកឱ្យ Pipe ដែលជា Input សម្រាប់ផ្នែកបន្ទាប់ដែលជា ForEach loop ។ ដោយសារតែ Get-Service បង្ហាញជា collection នៃ Service Objects ដូច្នេះ ForEach គឺជា Loop មួយដ៏ល្អ។ នៅខាងក្នុងនៃឃ្នាបអង្កាញ់គឺជា Block code ។ នៅក្នុងករណីនេះ យើងកំពុងប្រើ If ដើម្បីត្រួតពិនិត្យឱ្យដឹងថាលក្ខណៈរបស់ Service គឺ running ហើយបើវាដូច្នេះមែន វានិងបង្ហាញឃ្លាថា Dislpay name ។ វាត្រូវបង្ហាញឱ្យអ្នកឃើញនូវបញ្ហាពីរយ៉ាងគឺ:

- ទី១ $_ notation
- និងទី២គឺ . (dot)

អថេរ$_ គឺជាអថេរមួយដែលបានកំណត់ក្នុង system ជាស្វ័យប្រវត្ត។ ក្នុងpipe វារក្សាទុកនៅ Objects ថ្មីៗរបស់ Pipe ។ នៅក្នុងឧទាហរណ៏នេះចំពោះគ្រប់ជំហាននីមួយៗនៃ Loop $_និងយោងទៅរក Service នីមួយៗក្នុង Collection ដែលបានបង្ហាញដោយ Get-Service .(dot) គឺជា member operator សម្រាប់ Object ។ គ្រប់ Object មានសំនុំនៃ Properties ។

ឧទាហរណ៏

Automatic Variables

While $_ ត្រូវបានប្រើប្រាស់ជា automatic variable , numerous automatic variable ដែលត្រូវបានកំណត់ដោយ System ។

ខាងក្រោមនេះគឺជាអថេរដែលនិយមប្រើប្រាស់

- $_ មាន pipeline object ថ្មីៗ
- $? មាន True បើ Operation ចុងក្រោយទទួលបានជោគជ័យ បើពុំនោះទេវានិងជា false
- $Args មាន Array នៃប៉ារ៉ាម៉ែត្រដែលត្រូវបញ្ជូនឱ្យ Function
- $foreach សំដៅទៅលើ Enumerator នៅក្នុង Foreach loop
- $Home គឺជា Home Directory របស់ User ដែលមានតម្លៃសមមូលទៅនិង %homedrive%%homepath%
- $LASTTEXITCODE មាន exit code នៃ Win32 executable execution
- $PsHome គឺជា Directory ដែល Windows Powershell ត្រូវបាន Install
- $Host មានព័ត៌មានអំពី console host ថ្មីដូចជា version number

Service មួយមាន status name និង Displayname ក្នុងចំណោមលក្ខណៈផ្សេងៗទៀត។ ដើម្បី Access properties នីមួយៗនៃ Object អ្នកអាចប្រើ .(dot) notation ដើម្បីទទួលបាន Property ដោយប្រើ Syntax objectname.propertyname ។

នេះគឺជាដំណោះស្រាយចំពោះបញ្ហាដែលមានជាញឹកញាប់។ អ្នកដំណើរការ text file មួយដែលមាន folder ហើយអ្នកចង់ឱ្យ Windows PowerShell ដំណើរការ Files ទាំងអស់ក្នុង Folder នោះហើយប្តូរ extension ពី .TXT មកជា .BAK ។

គេសរសេរតែមួយបន្ទាត់គត់គឺ

```
Get-ChildItem E:\Logs\ *-include *.txt | foreach {move-item $_($_-replace(".txt",".bak"))}
```

១៨-៨- សិក្សាអំពី Regisrty

អ្នកមិនអាចគ្រប់គ្រងទៅលើ Windows និងលើ registry តែក្នុងរយៈពេលមួយថ្ងៃបាននោះទេ។ វាគឺជាចំណុចសំខាន់បំផុតនៃការ Configure System និង Application ។ អ្នកអាចប្រើបញ្ជា regedit.exe ដើម្បី Edit Registry ។ អ្នកអាចប្រើបញ្ជា reg.exe ដើម្បីដំណើរការជាមួយ Registry ក្នុង Windows PowerShell បានយ៉ាងងាយពីព្រោះ PowerShell បានចាត់ទុក Registry ដូចទៅនិង Directory Tree ដែរ។ អ្នកអាចចាត់ទុក registry key ជា Folders ហើយ registry value គឺជា files ។

Registry key ដ៏សំខាន់ដែលយើង accessគឺRun key។ Key នេះរក្សាទុកតារាងនៃ User login ។ ដើម្បី Access HKEY_LOCAL_MACHINE run key ពី PowerShell Console អ្នកអាច run:

```
CD HKLM:
CD software\microsoft\windows\currentversion\run
```

ចំណាំ វាដូចជាយើងចូលក្នុងរចនាសម្ព័ន្ធនៃ Directory នោះដែរ លើលែងតែ Drive ពិសេសហៅថា HKLM ប៉ុណ្ណោះ។ បើអ្នកចង់ទទួលបានតារាងនៃតម្លៃលើ Run Key អ្នកអាចប្រើ DIR command។ បើអ្នកព្យាយាម run វាអ្នកនិងមិនទទួលបានអ្វីទាំងអស់ DIR បង្ហាញតែ Registry key វាមិនបង្ហាញ Registry value នោះទេ។ ដើម្បីទទួលបានតម្លៃនៃ Registry ពិតប្រាកដក្នុង Run key អ្នកត្រូវតែប្រើ Get-ItemProperty cmdlet ពីព្រោះ

Registry value ត្រូវបានចាត់ទុកថា Properties នៃ Registry Keys។ Get-Item Property ត្រូវការឱ្យអ្នកកំណត់ពីផ្លូវនៃ Object ដែលអ្នកចង់ទទួលបាន Property ។

ឧទាហរណ៍

ដើម្បីទទួលបាន Registry value អ្នកត្រូវប្រើ

Get-ItemProperty

Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion

អ្នកនិងទទួលបានលទ្ធផលនៃ Get-ItemProperty។ ក្នុងHKLM:\Software\Microsoft\Windows \Current Version\run ដូចបានបង្ហាញក្នុងរូបភាព។

ដោយសារតែ Get-ItemProperty មិនត្រូវបានគេបង្កើតឡើងសម្រាប់ registry key នោះទេ វាបង្ហាញបន្ថែមនូវ metadata ដោយគិតទាំង Object ដែលកំពុងដំណើរការ។ ក្នុងករណីនេះវានិងបង្ហាញពីទីតាំងនៃ Registry key គឺ Path មក Parent key name drive (hive)នៃ Key ហើយចុងក្រោយនិងបង្ហាញពីតម្លៃក្នុង Run Key ។

១៨-៩- Working with Dates and Times

ការដឹងពីកាលបរិច្ឆេទនិងពេលវេលា និងការប្រើប្រាស់ម៉ាស៊ីនគិតលេខគឺជាការងារដ៏ចាំបាច់សម្រាប់គ្រប់អ្នកគ្រប់គ្រងលើប្រព័ន្ធ Network។ PowerShell បានភ្ជាប់មកជា មួយនូវកាលបរិច្ឆេទនិងពេលវេលាសម្រាប់ជួយដល់ការកិច្ចការមួយចំនួន។ ដើម្បីទទួលបាន date និង time cmdlet ប្រើ Get-Date (ប្រហែលជា Get-DateTime អាចសមរម្យជាង) ។ ការដំណើរការ Get-Date និងបង្ហាញថ្ងៃ កាលបរិច្ឆេទ និងម៉ោង។

បើអ្នកចង់ឱ្យវាបង្ហាញតែ date ឬ time អ្នកត្រូវកំណត់ដូចខាងក្រោម

Get-Date –displayhint date

Get-Date -displayhint time

Date និង time ត្រូវបានបង្ហាញលើ time zone ថ្មីៗដែលបាន Configure នៅលើ Server។ បើអ្នកបំរើការនៅក្រុមហ៊ុនសាកលលោក នៅពេលខ្លះវាដំណើរការបានល្អនៅពេលកំណត់ date និង time ដោយប្រើ UTC (Univer -sal Time Code)។ នេះមិនមែនជាបញ្ហានោះទេ ពីព្រោះ cmdlet មាន ToUniversalTime method ស្រាប់។

វាអាចបង្ហាញដោយប្រើ

(Get-Date).ToUniversalTime( )

Method មួយដ៏ល្អនៃ Get-Date គឺ IsDaylightSavingTime method ។ វានិងបង្ហាញពី date និង time ក្នុង local time ។

(Get-Date).IsDaylightSavingTime( )

នៅពេលយើងសរសេរ Script បង្កើត log files យើងត្រូវដាក់ឈ្មោះឱ្យវាដោយពឹងផ្អែកលើ current date និង time ។

$filename = "myfile "

$datestring = Get-Date –uformat %Y%M%d

$newfilename = $filename + "_ "+$datestring+ ".txt "

Write-host $newfilename

-uformat នៃ Get-Date cmdlet សម្រាប់តំណាងឱ្យ UNIX format ។

%Y តំណាងឱ្យឆ្នាំដែលមាន 4 digits ដោយចាប់តាំងពីឆ្នាំ២០០៧ មក %M តំណាងឱ្យខែដែលមាន 2 digits ដូចជា 09 ហើយ %d តំណាងឱ្យថ្ងៃដែលមាន 2 digits ដូចជា 21 ។

តារាងខាងក្រោមនេះបង្ហាញពីតម្លៃដែលអ្នកអាចប្រើប្រាស់បាន។អ្នកត្រូវប្រើសញ្ញា(%)ខាងមុខនៃតួអក្សរ។

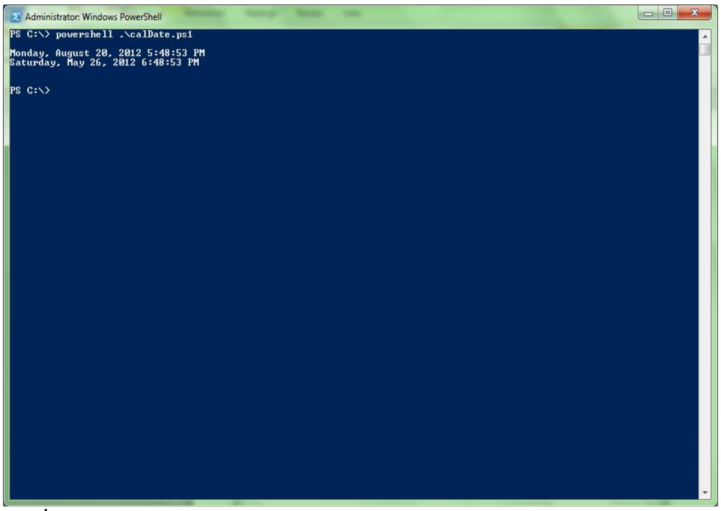
- C (អក្សរធំ C) គឺជាសត្តវត្សនៃឆ្នាំ។ វាប្រើលេខពីរខ្ទង់នៃឆ្នាំ ដូជជា 20 សម្រាប់ 2007
- Y Four Digit year
- y two digit year
- b Abbreviated month name
- B Full month name
- M two digit month
- W (Capital W) Week of the year (00-52)
- V(Capital V) Week of the year (01-53)
- a Abbreviated day of the week
- A Full day of the week
- u Day of the week as a number starting with 1 for Monday
- d Two digit day of the Month
- j Day of the year
- r Time in 12 –hour format
- R Time in 24-hour format (no second)
- T Time in 24-hour format
- p A.M or P.M.
- Z (Capital Z) Timezone offset from UTC
- H Hour in 24-hour format
- I Hour in 12-hour format
- m Minutes
- S (Capital S) seconds

ការគណនាអំពី date គឺជាវិធីមួយទៀតនៃ date ដែលសំខាន់និងតួនាទីនៃពេលវេលា។ ឧទាហរណ៍ ហេតុអ្វីបានជាអ្នកមិនចង់ដឹងពី date និង time ក្នុងរយៈពេលបីខែពីពេលនេះទៅ? តើ 145 ម៉ោងចាប់ពីពេលនេះទៅស្មើប៉ុន្មាន?

ដើម្បីទទួលបានចម្លើយអ្នកត្រូវ run

```
(Get-Date).AddMonths(3)
(Get-Date).AddHours(145)
```

Get-Date Method បានបន្ថែមវិនាទី នាទី ម៉ោង ថ្ងៃនិងឆ្នាំហៅថា AddSeconds, AddMinutes, AddHours។ល។

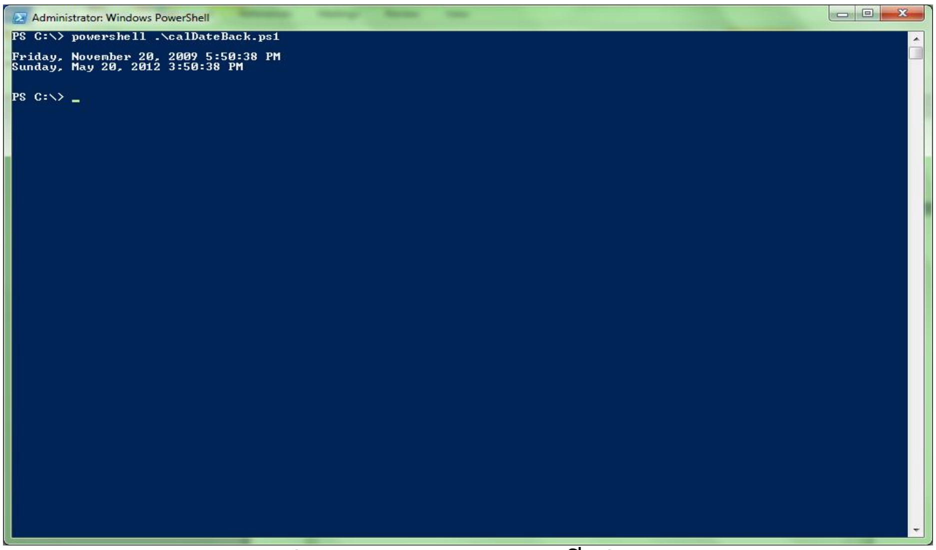


តើមានអ្វីកើតឡើងបើអ្នកចង់រក date និង time ចំពោះព្រឹត្តិការអ្វីមួយដែលមានមុនពេលបច្ចុប្បន្ន? គ្មាន SubtractSeconds ឬ MinuteSeconds method ក្នុង Get-Date ។

ដើម្បីរក date និង time ក្នុងរយៈពេល៣០ម៉ោងកន្លងទៅឬកាលពី២ឆ្នាំមុន យើងត្រូវប្រើ

(Get-Date).AddHours(-30)

(Get-Date).AddYears(-2)



អ្នកអាចកំណត់ System time ដោយប្រើ Set-Date cmdlet ។ ដើម្បីកំណត់នៅ date និង time ពិតប្រាកដ អ្នកអាចប្រើ -date ដូចខាងក្រោម

Set-Date –date "9/5/2007 9:00AM "

បើម៉ោងនាឡិកា កុំព្យូទ័រ របស់អ្នកយឺតជា២ម៉ោង អ្នកអាចប្រើ

Set-Date (Get-Date).AddHours(2)

ពេលខ្លះអ្នកត្រូវគណនានូវម៉ោងពីរផ្សេងគ្នា ដូចជាអ្នកត្រូវការកំណត់ម៉ោងនៃ Script ឬ Logon script ។ យើងអាចប្រើ New-Timespan cmdlet ។

ឧទាហរណ៍ អ្នកត្រូវការកំណត់នូវពេលវេលាដើម្បី execute Script អ្នកត្រូវប្រើ

$Starttime = Get-Date

……Do lots of stuff here……

$endtime = Get-Date

$timediff = New-Timespan $starttime $endtime

Write-host $timediff.milliseconds + "milliseconds "

ចូរចំណាំពីរបៀបដែលយើងបានប្រើ milliseconds property នៃ timespan ដើម្បីបង្ហាញពីចំនួន milliseconds ។

យើងមានជម្រើសដូចខាងក្រោម

- Days
- Hours
- Minutes
- Seconds
- Milliseconds
- Tricks
- Total Days
- Total Hours
- Total Minutes
- Total Seconds
- Total Milliseconds

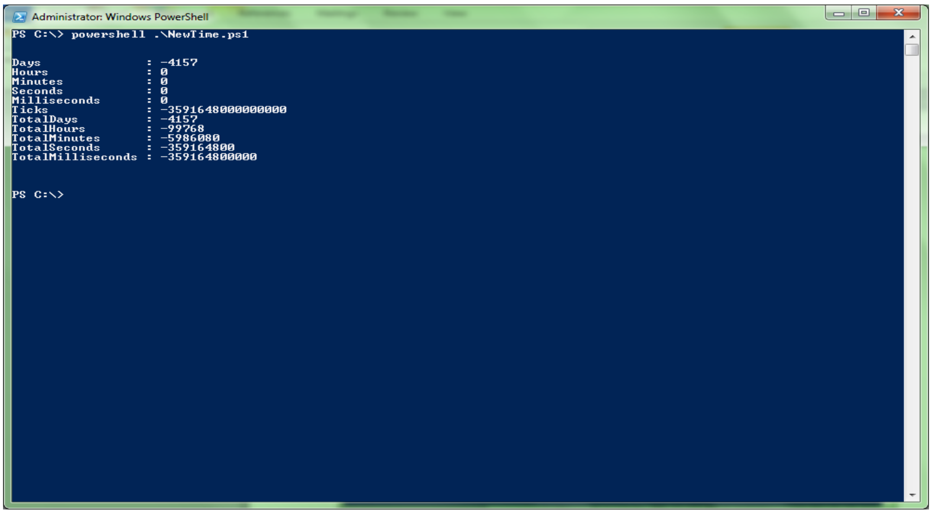
តើអ្នកត្រូវធ្វើដូចម្តេចដើម្បីឱ្យដឹងពីរយៈពេលក្នុងពេលបច្ចុប្បន្ននិងកាលបរិច្ឆេទនៃ January 1,2001 ?

ដើម្បីតំណាងឱ្យ January 1 2001 យើងត្រូវប្រើ

Get-Date –month 1 -day 1 –year 2001

យើងត្រូវដាក់វាបញ្ចូលគ្នាដោយប្រើ New-Timespan

New-Timespan $(Get-Date –month 1 -day 1 –year 2001)



សង្ខេបមេរៀន

នៅក្នុងជំពូកនេះយើងបានដំណើរការ Windows PowerShell ក្នុង Windows Server 2008 ហើយធ្វើឱ្យយើងមានការសមទៅនិង command-line interface ក្នុង Windows PowerShell ។ វាបានបង្រៀនយើងឱ្យចេះប្រើអថេរ បង្កើតឃ្លាមានលក្ខខណ្ឌ និងការប្រើ Loop ជាដើម។

ជាដំបូងយើងបានដឹងពីរបៀបប្រើប្រាស់PowerShell ដើម្បីធ្វើកិច្ចការដ៏សំខាន់ជួយដល់អ្នកគ្រប់គ្រង់លើ Windows។ Windows PowerShell បានព្រងីកសមត្ថភាពដោយបានធ្វើឱ្យយើងអាចប្រើ.NETនៅលើ Server ។

នៅក្នុងជំពូកនេះបានជំរុញឱ្យយើងស្រាវជ្រាវអំពី Shell ថ្មី។ ចំណុចមួយដ៏សំខាន់អំពី Windows Powershell គឺវាអាចដំណើរការមិនគ្រាន់តែនៅលើ Windows Server ២០០8 ប៉ុណ្ណោះទេ ប៉ុន្តែវាថែមទាំងដំណើរការនៅលើ Windows xp SP2,Windows Server 2003 និង Windows Vista ផងដែរ។ Windows PowerShell បានជួយឱ្យអ្នកគ្រប់គ្រង់លើប្រព័ន្ធ Network ចំណាយពេលវេលាតិចហើយទទួលបាននូវផលប្រយោជន៍ច្រើន។

ការប្រើប្រាស់ Windows PowerShell បានផ្តល់ឱ្យនូវ command shell ដែលជួយឱ្យអ្នកគ្រប់គ្រងមានលទ្ធភាពលើ Windows ដោយប្រើ Command ដោយមានប្រសិទ្ធិភាពខ្ពស់ដូច UNIX system កាលពីប៉ុន្មានទសវត្សមុន។

សំណួរត្រួតពិនិត្យ

១-តើ Windows PowerShell គឺជាអ្វី?

២-តើ Windows Powershell ផ្តល់ឱ្យនៅផលប្រយោជន៍ណាខ្លះ?

៣-ចូរសរសេរ Script មួយដើម្បីធ្វើការ Backup ទិន្នន័យ?

៤-ចូរសរសេរ Script មួយដើម្បីគ្រប់គ្រងលើប្រព័ន្ធ Network?

ជំពូកទី១៩

Enterprise Public Key Infrastructure

ប្រព័ន្ធសុវត្ថិភាពក្នុងប្រព័ន្ធការប្រាស្រ័យទាក់ទងត្រូវបានទទួលតែក្នុងករណីដែលអ្នកទទួល ទទួលបាន ហើយអានវាប៉ុណ្ណោះ។ បើនិយាយពីអ្វីដែលមាននៅក្នុងពិភពលោកយើងនេះ វាមានន័យថា បើអ្នកខ្សឹបដាក់ត្រចៀកនរណាម្នាក់ឬធ្វើកិច្ចប្រជុំដោយបិទទ្វានោះមានតែអ្នកដែលបានស្តាប់ឬចូលរួមទេដែលបានលឺឬដឹង។ បើនិយាយអំពីផ្នែក Physical វិញ វាគឺជាការធ្វើឱ្យទទួលបានសារនោះក្នុងកម្រិតមួយយ៉ាងតិចបំផុតក្នុងការផ្ទេរវា។ បើអ្នកត្រូវការឱ្យមានសុវត្ថិភាពខ្ពស់លើការប្រាស្រ័យទាក់ទងក្នុងរយៈចម្ងាយឆ្ងាយ អ្នកត្រូវប្រើប្រព័ន្ធ Digital គឺ e-mail ។

បញ្ហាដែលកើតឡើងគឺអ្នកមិនអាចគ្រប់គ្រងលើវាហើយដឹងថានរណាបានអានវានោះទេក្នុងកំឡុងពេលនៃការបញ្ជូននោះ។

ដំណោះស្រាយចំពោះបញ្ហានោះគឺត្រូវធ្វើ Encryption ចំពោះ Message ទោះបីជាវាត្រូវបានទទួលដោយសំងាត់ក៏ដោយក៏មិនអាចអានវាបានដែរមុនពេលវាត្រូវបាន Decrypt វាមកវិញ។

Encrypttion ត្រូវបានអនុវត្តតាមរបៀបជាច្រើន។ វិធីដ៏ល្អដើម្បីបញ្ជូន Message គឺប្រើ key ហើយបន្ទាប់មកប្រើ key ដដែលសម្រាប់បើកវាវិញ។

Public Key Infratructur (PKI) គឺជាវិធីសាស្រ្តមួយដែល Encrypt និង Decrypt data ដោយប្រើ Digital Keys ដែលត្រូវបានអនុវត្តចំពោះ data ដើម្បីបង្កើតបានជា *cipher text* ហើយអាចបញ្ជូនបានគ្រប់ទីកន្លែងទាំងអស់ក្នុងពិភពលោក។ អ្នកមិនចាំបាច់បារម្ភអំពីការលួចទទួលយម data នោះទេពីព្រោះថា Data មិនអាចប្រើប្រាស់បាននោះទេបើគ្មាន Key។ PKI ជាទូទៅប្រើ Key ពីរដើម្បី Encrypt និង Decrypt data គឺ public key និង private key។ Public key អាចឱ្យអ្នកទាំងអស់គ្នាស្គាល់បានហើយត្រូវបានប្រើប្រាស់សម្រាប់Encrypt data។ ទោះបីជាយ៉ាងណាក៏ដោយ data អាច Decrypt បានតែអ្នកដែលស្គាល់ Private key ប៉ុណ្ណោះ។

ក្នុងសៀវភៅនេះខ្ញុំបានលើកយកពី Services មួយចំនួនដែលប្រើ Digital Certificate ដើម្បីធ្វើការ Encrypt និង Authentication Service។ Certificate គឺជា Key ដែលបង្កើតឡើងដោយ PKI system ក្នុងករណីនេះគឺ certification authority (CA)។ ឧទាហរណ៍ នៅពេលដែលអ្នកធ្វើការទិញ online អ្នកបានបញ្ជូននូវ Web site របស់អ្នកលក់ទៅឱ្យអ្នកលក់ដូរវិញដោយប្រើ SSL (Secure Socket Layer) ដែលជា Digital certificate ត្រូវបានបង្កើតដោយ PKI system ដើម្បីជានាអត្តសញ្ញាណរបស់ Server និងបង្កើតឡើងនៅការភ្ជាប់មួយដែលមានសុវត្ថិភាពខ្ពស់រវាង client និង Server។ PKIគឺផ្តល់ឱ្យនៅ Encryption និង Identity Management service ដោយប្រើ Public និង Private key សម្រាប់ Encrypt និង Decrypt data

Enterprise PKI system អនុញ្ញាតឱ្យអ្នកដាក់ Key នៅចំណុចកណ្តាលនិង certicate management ដែលបានមកពីការបង្កើត ការចេញឱ្យប្រើ និងបានមកពីការបង្កើតវាឡើងវិញ។

១៩-១- PKI ប្រើប្រាស់

គេអាចប្រើ PKI ចំពោះ Applications មួយចំនួនដែលគាំទ្របច្ចេកវិទ្យា។ គ្រប់ Services ទាំងអស់ដែលប្រើប្រាស់ PKI ធ្វើដូច្នោះពីព្រោះថាដរាបណា Private Key ត្រូវបានរក្សាទុកដោយមានសុវត្ថិភាព PKI គឺជាវិធី

សាស្ត្រមួយដ៏មានប្រជាប្រិយភាពបំផុតសម្រាប់ Encrypt ហើយនិងផ្តល់ឱ្យនូវ Signing data តាមប្រព័ន្ធ Digital ។ PKI រួមមានសមាសធាតុជាច្រើនដែលត្រូវបានប្រើសម្រាប់គោលបំណងផ្សេងៗគ្នា។ សមាសធាតុដ៏សំខាន់គឺ CA ។

អ្នកអាចប្រើ PKI ក្នុង Scenarios ដូចខាងក្រោម

- សម្រាប់ e-mail ដែលជា Digital សម្រាប់បញ្ជាក់នូវភាពត្រឹមត្រូវនៃភាពដើមរបស់វា
- Encrypt e-mail ដូច្នោះវាអាចមើលបានតែអ្នកដែលត្រូវបានគេកំណត់ឱ្យតែប៉ុណ្ណោះ
- អនុញ្ញាតឱ្យកុំព្យូទ័រធ្វើការប្រាស្រ័យទាក់ទងដោយមានសុវត្ថិភាពដោយប្រើ certificate ទោះបីជាតាម Network ដែលគ្មានសុវត្ថិភាពយ៉ាងណាក៏ដោយដូចជា IPSec
- ធ្វើឱ្យ Web site traffic មានសុវត្ថិភាពដោយប្រើ SSL និង Certificate ជាពិសេសសម្រាប់ e-commerce
- ផ្ទៀងផ្ទាត់ចំពោះភាពត្រឹមត្រូវនៃ software រួមមាន Device Driver ដោយប្រើ signed published certificate.
- គាំទ្រ authentication តាមរយៈ certificate ដោយដំណើរការតាម smart cards
- Authenticate network connection ដោយប្រើ 802.1x
- Encrypt user files ដោយប្រើ Encrypted File System (EFS)

PKI ត្រូវបានប្រើប្រាស់ដើម្បីឱ្យមានការប្រាស្រ័យទាក់ទងមានសុវត្ថិភាពនៅគ្រប់កាលៈទេសៈ។ ជាទូទៅ PKIគឺជាដំណោះស្រាយមួយដ៏ល្អនៅពេលដែលអ្នកត្រូវការទំនាក់ទំនងដែលមានសុវត្ថិភាពខ្ពស់។ សុវត្ថិភាពរបស់ PKI គឺពឹងផ្អែកលើសុវត្ថិភាពនៃ Private Key និងចំនួន bit ដែលត្រូវបានប្រើសម្រាប់ Encrypt ។

ឧទាហរណ៍ ការប្រើ 128 bit Encryption គឺជាចំណុចខ្សោយនៃ Key សម្រាប់ Encrypt ។ ដើម្បីឱ្យមានសុវត្ថិភាពកាន់តែខ្ពស់គេប្រើ 4096 bit ឬក៏ច្រើនជាងនោះសម្រាប់ Encrypt ដើម្បីធ្វើឱ្យមានការពិបាកកាន់តែខ្លាំងក្នុងការ crack ។

១៩-២- Digital Signatures

Digital Signatures មិនអាចការពារ Data ពីការអាននោះទេ។ ផ្ទុយទៅវិញ Encrypt ត្រូវបានប្រើសម្រាប់ភ្ជាប់ទៅនិង Message ដើម្បីធានាថាមានភាពត្រឹមត្រូវ។ មនុស្សភាគច្រើនបានគិតថា Digital Signature មានតួនាទីដូចជាហត្ថលេខាធម្មតាដែរ។ តាមការពិតវាដូចគ្នាមែននៅពេលប្រើវា។ ការពិតក្នុងការប្រើប្រាស់គឺនៅពេលអ្នកប្រើប្រាស់វា Digital signature នៅលើ Data ដូចជា e-mail message ដែរហើយ Signature វាខុសគ្នាគ្រប់ពេលវេលានៃការប្រើប្រាស់វា។

Digital Signature ធ្វើការដោយបញ្ជូន Data ដែលអ្នកបានចុះហត្ថលេខាតាមរយៈ Hashing algorithm ដែលត្រូវបានប្រើប្រាស់ដើម្បីបង្កើតបានជា Message *digest* ។

Digest នេះត្រូវបាន Encrypt ដោយប្រើ Key ឯកជនរបស់អ្នកបញ្ជូនដែលបង្កើតបានជា digital signature ។ បន្ទាប់មក Message ត្រូវបានបញ្ជូនទៅឱ្យអ្នកទទួលដែលភ្ជាប់មកជាមួយនូវ public key ឬពឹងផ្អែកលើអ្នកទទួលដែលមាន public key រួចជាស្រេច។ អ្នកទទួលក៏ Decrypt វាមកវិញដោយប្រើ public key របស់អ្នកផ្ញើ។ បើ Digital Signature ត្រូវបាន Decrypt ទទួលបានជោគជ័យដោយប្រើ Public key នោះវាធានាថា Message ដែលទទួលបានពីអ្នកទទួលមិនត្រូវបានគេលួចតាមផ្លូវបញ្ជូននោះទេ។ លក្ខណៈពិសេសនេះមានសារៈសំខាន់ណាស់ចំពោះឧស្សាហកម្ម Software សព្វថ្ងៃនេះ។

១៩-៣- Digital Certificates

Digital certificate គ្មានអ្វីក្រៅពី public key ត្រូវបាន Encapsulate ដែលមានទម្រង់ជា Metadata ដោយគិតទៅលើការប្រើប្រាស់និងភាពដើមរបស់វា។ ជាពិសេស Digital certificate មិនគ្រាន់តែមាន publick key នោះទេវាថែមទាំងមានម្ចាស់នៃ certificate និង CA របស់វា។ ទោះបីជាក្នុងន័យបច្ចេកទេសយ៉ាងណាក៏ដោយ នរណាម្នាក់ក៏អាចបង្កើត Digital certificate បានដែរ។

ឧទាហរណ៍ បើអ្នកប្រើ self-generate certificate សម្រាប់ SSL-enable Web site client ដែលគ្មាន CA register នៅក្នុងDatabase certificate ដែលមានទំនុកចិត្តនិងទាមទារនូវ certificate នោះពីប្រភពដែលមិនទុកចិត្តឬក៏មិនអនុញ្ញាតឱ្យភ្ជាប់ជាមួយបាន។ Digital certificate ដូចគ្នាទៅនិងលិខិតឆ្លងដែននោះដែរ។

១៩-៤- Certification Authorities

CA គឺជាសមាសធាតុដ៏សំខាន់របស់ PKI។ បើគ្មាន CAs នោះទេ វានិងគ្មាន Digital certificate ឬ Public key ហើយក៏គ្មាន Digital signature នោះដែរ។ CA ត្រួតពិនិត្យលើ Certificate គឺវាទទួលខុសត្រូវក្នុងការបង្កើត និងការផ្សព្វផ្សាយ certificate ឱ្យអ្នកប្រើប្រាស់ដែលមានសិទ្ធិនិងកុំព្យូទ័រ។ បើ certificate ត្រូវបានគេដឹងអ្នកអាចបង្កើតវាឡើងវិញម្តងទៀតដោយបន្ថែមវាចូលក្នុង*Certificate Revocation List(CRL)* ។

CA គឺគ្មានអ្វីក្រៅពីការបង្កើត certificate នោះទេ។ តើកត្តាអ្វីខ្លះការពារនរណាម្នាក់ពីការបង្កើត certificate និងធ្វើអ្វីតាមគេចង់បាន ?

នរណាក៏ដោយអាច setup CA ឱ្យដំណើរការតែម្នាក់ឯងបានហើយចេញនូវ certificate សម្រាប់ applications មួយចំនួនបាន។ នៅក្នុងការពិត certificate ត្រូវបានប្រើប្រាស់សម្រាប់មានប្រតិកម្មជាមួយ entities គ្រប់ក្រុមហ៊ុនទាំងអស់។ អ្នកឬក៏នរណាម្នាក់ក៏អាចបន្ថែម root certificate ឱ្យគ្នាទៅវិញទៅមកបានចំពោះតារាងនៃ certificate ដែលទុកចិត្តបានឬក៏អ្នកអាច Configure CA របស់អ្នកជាផ្នែកមួយនៃរចនាសម្ព័ន្ធនៃ CA ដ៏ធំមួយបាន។

ឧទាហរណ៍ អ្នកអាចមាន root certificate នៃ CA ដែលបានយល់ព្រមរួមគ្នាដោយ CA ប្រភេទនៃពាណិជ្ជកម្មដែលទុកចិត្តបាន។

CA ផ្នែកពាណិជ្ជកម្មដ៏ធំមួយគឺទទួលខុសត្រូវផ្ទៀងផ្ទាត់ទៅលើអត្តសញ្ញាណនៃមនុស្សដែលបានអនុវត្តចំពោះ certificate មួយនៃ CA ឬក៏ស្វែងរកលទ្ធភាពដើម្បីចេញ certificate ផ្ទាល់ខ្លួនរបស់គេ។ ក្រុមហ៊ុនដូចជា Verisign បានអនុវត្តប្រភេទនៃការផ្ទៀងផ្ទាត់និងការចុះហត្ថលេខាលើ service ។

១៩-៥- ប្រភេទនៃ CAs

Certificate Service គឺជាផ្នែកមួយនៃ Windows Server 2008 ដែលមានពីរប្រភេទនៃការ Configure គឺ:Enterprise និង Stand-alone។ វាទាំងពីរអាចបង្កើតបានជា certificate ភាពខុសគ្នាគឺអាស្រ័យទៅលើភាពអាស្រ័យគ្នាគឺប្រភេទនៃ certificate ដែលអាចប្រើបាននិងអ្វីដែលគេអាចពង្រីកដើម្បីប្រើបាន។ ប្រភេទនៃ CA នេះត្រូវបានប្រើប្រាស់សម្រាប់បង្កើតរចនាសម្ព័ន្ធនៃ certificate ដែលរួមមាន root CA និងផ្នែកនៃ CAs ។

Enterprise CAs

ដូចដែលអ្នកបានសង្ឃឹមទុកជាមុន ការដំឡើងនៃ Enterprise CA ទាមទារនូវ Active Directory Domain Service (AD DS) ដែលមានស្រាប់។ Enterprise CA ត្រូវបានបង្កើតឡើងសម្រាប់ចេញ certificate មានលក្ខណៈ: ជាស្វ័យប្រវត្តឬមានលក្ខណ:ធ្វើឡើងដោយដៃចំពោះ Users កុំព្យូទ័រនិងកូននៃ CA ។ អ្នកត្រូវតែជា Enterprise Administrator ដែលអាចដំឡើង Enterprise CA ដែលត្រូវការនូវបច្ចេកវិទ្យាដូចខាងក្រោម :

- Active Directory
- Group Policy ដើម្បីផ្សព្វផ្សាយ certificate ឱ្យ client នូវ root certificate
- Authentication នៃ Domain ដោយប្រើ smart cards ដែលមាន certificate
- Enterprise Exit Module ដែលត្រូវបានប្រើសម្រាប់គ្រប់គ្រងលើ certificate ក្រោយពេលដែលបានចេញឱ្យ

ដោយសារតែ Enterprise CA ត្រូវបានបញ្ចូលជាមួយ AD យ៉ាងជ្រៅនោះ វាបានបន្ថែមនូវគុណសម្បត្តិដែលអាចផ្ទៀងផ្ទាត់បានចំពោះ User ជាស្វ័យប្រវត្តិជាមួយ AD មុនពេលដែលចេញនូវ certificate សមរម្យដែលពឹងផ្អែកលើគំរូដែលមានស្រាប់។ លើសពីនេះទៅទៀត metadata ទាក់ទងជាមួយ certificate ដូចជា ឈ្មោះនិងព័ត៌មានសម្រាប់ទាក់ទង។

ជាចុងក្រោយ Enterprise CA ទទួលយកឬបដិសេធការស្នើសុំ certificate ចាប់តាំងពីវាបានត្រួតពិនិត្យលើលក្ខខណ្ឌនិច្ច័យដែលត្រូវការបំពេញការស្នើសុំ។

Stand-alone CAs

នៅពេលដែល Enterprise CA ផ្តោតយ៉ាងខ្លាំងទៅលើការផ្តល់ certificate service សម្រាប់ក្នុងអង្គការហើយមានសមត្ថភាពចេញជាស្វ័យប្រវត្តិលើ certificate Stand-alone CA ត្រូវបានដាក់ឱ្យប្រើចំពោះ certificate នៅ entities ខាងក្រៅ។ Stand-alone CA មិនត្រូវការ AD នោះទេ CAs និងដំណើរស្នើសុំសម្រាប់ System នីមួយៗដែលមិនស្ថិតនៅក្នុងការគ្រប់គ្រង។ គ្រប់ certificate ដែលបានស្នើសុំទាំងអស់មកកាន់ Stand-alone CA ត្រូវបានសំគាល់ថាជាការបើកចំហរហូតទាល់តែពេលវេលាដែល Administrator អាចផ្ទៀងផ្ទាត់ព័ត៌មានហើយធ្វើការសម្រេចចិត្តសមរម្យដើម្បីទទួលយកឬបដិសេធការស្នើសុំនោះ។ ដោយសារតែវាមិនបានបញ្ចូលជាមួយAD certificate ដែលបានបង្កើតរួចហើយត្រូវតែចែកចាយដោយអ្នកគ្រប់គ្រងហើយដំណើរការចូលមកក្នុង Certificate របស់អ្នកប្រើប្រាស់។ Certificate ដែលចេញដោយ Stand-alone CAs មិនអាចប្រើសម្រាប់ authenticate ហើយ Logon មកកាន់ system ដោយប្រើ smart card នោះទេ។

Certificate Templates

Certificate template គឺជាសំនុំនៃក្បួនច្បាប់ដែលគ្រប់គ្រង់ទៅលើ certificates និងបង្កើតទម្រង់នៃ certificate ថ្មី។ ឧទាហរណ៍ template ត្រូវបានប្រើសម្រាប់អនុញ្ញាតឱ្យ certificate ប្រើប្រាស់បានតែចំពោះ IPSec communication ប៉ុណ្ណោះឬសម្រាប់តែ signing e-mail ។

១៩-៦- Cryptographic Service Providers

Cryptographic service providers (CSPs)គឺជាសំនុំនៃ hardware ឬ software ដែលត្រូវបានគេប្រើប្រាស់សម្រាប់អនុវត្តទៅលើអនុគមន៍ cryptograhy។ ឧទាហរណ៍ អ្នកអាចប្រើ CSP ដែលអាចដឹងពីរបៀបដែល sign e-mail message តាម Digital ឬ authenticate នូវ Wireless LAN ដែលប្រើ 802.1x ។ Windows Server 2008 រួមមានសំនុំនៃ CSPs ដែលគេនិយមប្រើវា។

Recovery Keys

អង្គការជាច្រើនបានចាប់អារម្មណ៍ទៅលើថាតើមានអ្វីដែលបានកើតឡើងខ្លះបើKeyត្រូវបានបាត់បង់? ឧទាហរណ៍ បើប្រធាននៃធនធានមនុស្សបាន Encrypt នូវគ្រប់ Files ទាំងអស់ដោយប្រើ EFS ហើយបន្ទាប់មកបានបាត់ Key ។ តើអង្គការនោះ Access data តាមរបៀបណា?

ដំណោះស្រាយគឺត្រូវប្រើ **Recovery Keys** ។ Recovery Keys ត្រូវបានអនុវត្តតាម certifi-cate ពិសេសដែលអាចប្រើប្រាស់បានដោយ Recovery agents សម្រាប់ Decrypt data ។

Recovery agents គឺជាមនុស្សដែលអាច Recover data បានមកវិញដោយប្រើ Keys។ ទោះបីជា recovery key អនុញ្ញាតឱ្យ Decrypt data យ៉ាងណាក៏ដោយក៏វាមិនអាចបង្កើតឡើងវិញនូវ Key ដើមបានដែរ សម្រាប់ Encrypt data។ វាមានសារៈសំខាន់ណាស់ពីព្រោះថាវាអាច Recover data បានមកវិញ។

លំហាត់អនុវត្ត Installing AD Certificate Services

Enterprise PKI សម្រាប់ Windows Server 2008 គេសំដៅទៅលើ Active Directory Certificate services គឺជាតួនាទីដែលអ្នកអាច Install នៅលើ Windows Server 2008 ដែលអនុញ្ញាតឱ្យ Server របស់អ្នកមានតួនាទីជា CA ។

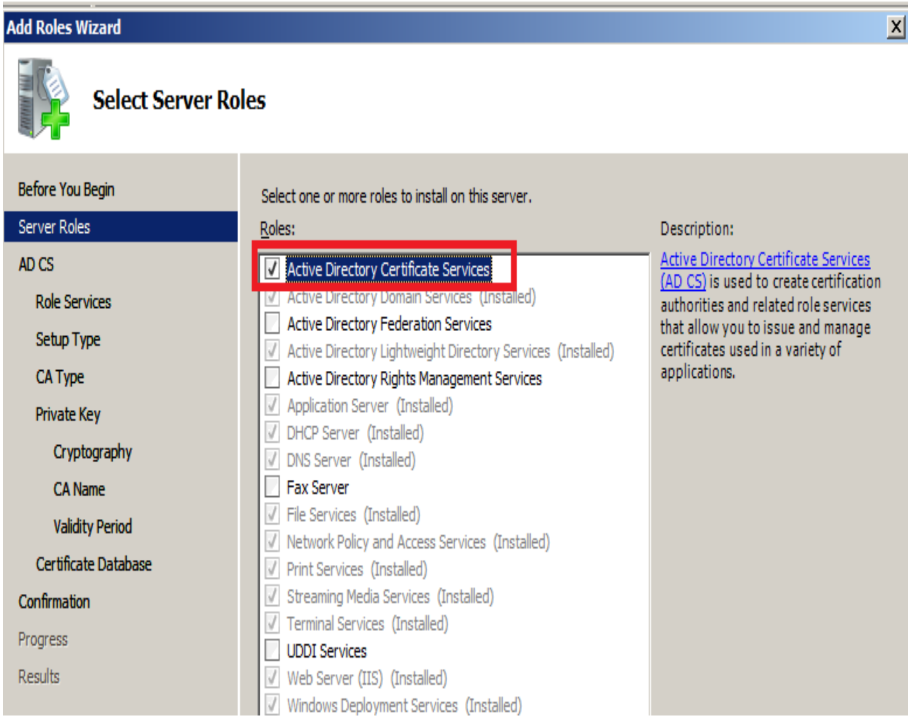
នៅក្នុងឧទាហរណ៍នេះ យើងនិងដំឡើង AD certificate Services role នៅលើ Server ។ ប៉ុន្តែមុននិង Install តួនាទីនេះ យើងនិងធ្វើការសម្រេចចិត្តនូវចំណុចមួយចំនួនដូចជា:

- តើវាជា Enterprise CA ឬជា Stand-alone CA ?
- តើយើងនិងអនុញ្ញាតឱ្យ certificate ត្រូវបានស្នើតាម Web site ឬយ៉ាងណា ?

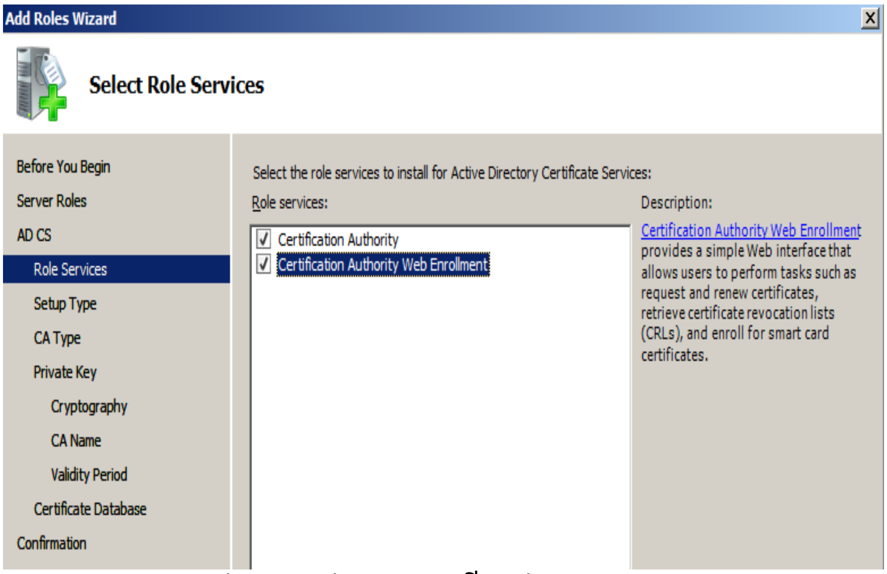
នៅក្នុងឧទាហរណ៍នេះយើងនិង Install ហើយ Configure AD certificate Services ជា Enterprise CA យើងក៏អនុញ្ញាតឱ្យ certificate ស្នើសុំតាមរយៈ Web site ផងដែរ។

ចំណាំ: Server ដែលអ្នកនិង Install AD certificate services ត្រូវតែជាសមាជិករបស់ Domain ហើយអ្នកត្រូវតែ Install វាដោយប្រើ User Account ដែលមានសិទ្ធិបន្ថែម CA ជា enterprise root CA។

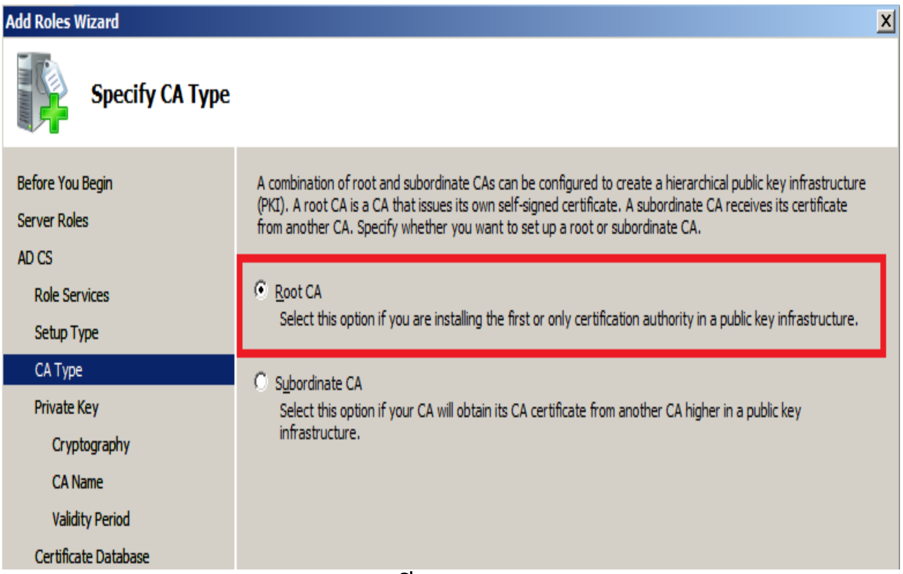
1- បើក Server manager
2- ចុចលើ Add Roles ដើម្បីបើក Add Roles Wizard
3- ចុចលើ Next
4- ជ្រើសរើសយក Active Directory Certificate Services ហើយបន្ទាប់មកចុចលើ Next
5- ចុចលើ Next



6- ជ្រើសរើសយក Certification Authority and Certification Authority Web Enrollment role services ហើយចុចលើ Next

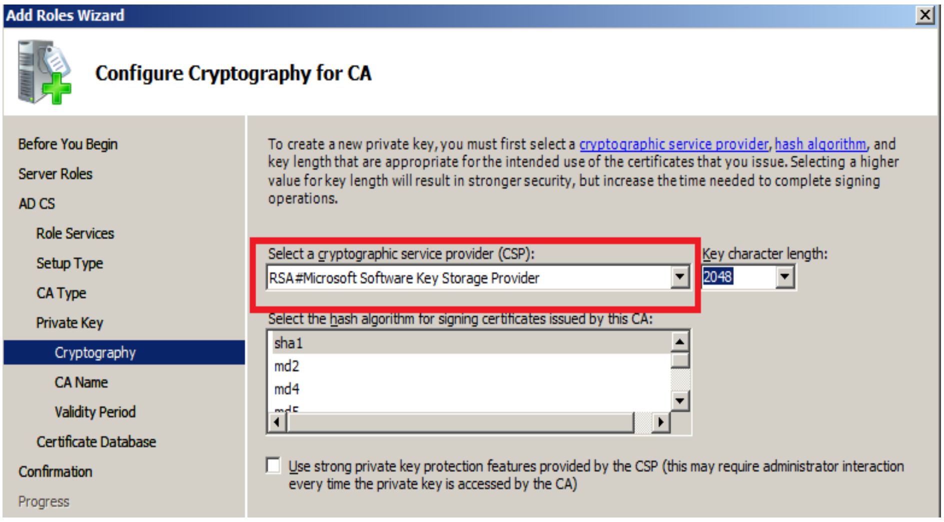


7- ជ្រើសរើសយក Enterprise ហើយចុចលើ Next ។ ជ្រើសរើសយក Root CA ជា CA type

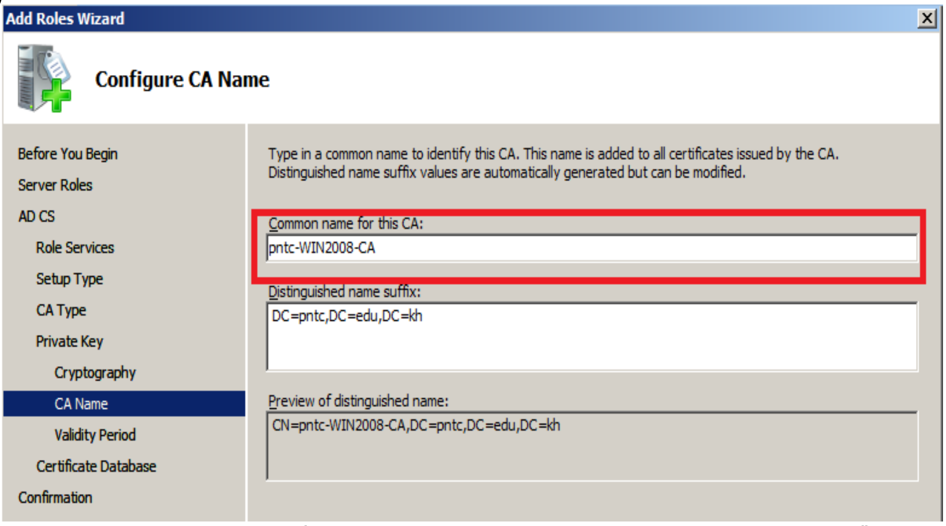


8- ជ្រើសរើយក Create a new Private Key ដើម្បី Setup private key ហើយចុចលើ Next.

9- ជា Default CSP ត្រូវបានជ្រើសរើសយកសម្រាប់ CA គឺ RSA#Microsoft Software Key Storage Provider.



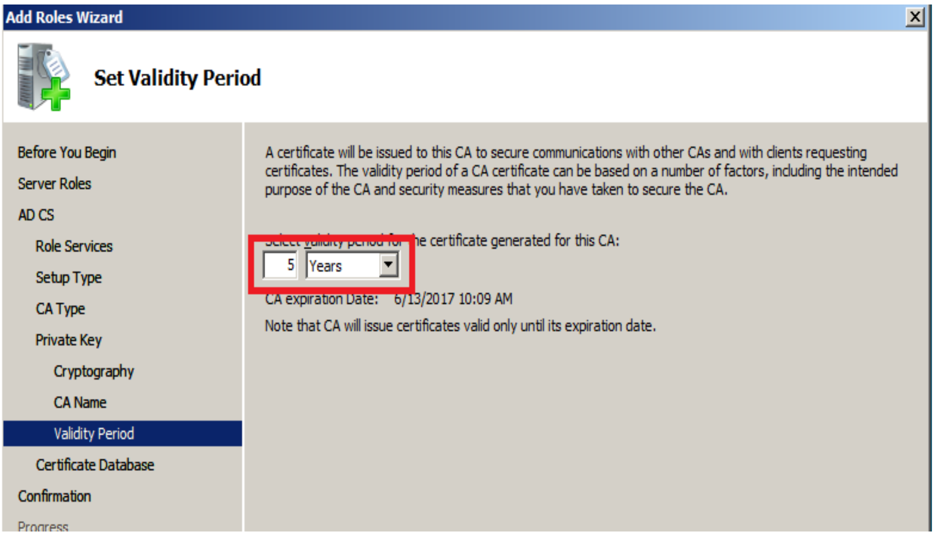
10- វាយបញ្ចូលឈ្មោះរបស់ CA ។ ជា Default field នេះត្រូវបានកំណត់ជា DOMAIN SERVER-CA



11- ជា default រយៈពេលដែលអាចប្រើប្រាស់បានជាផ្លូវការសម្រាប់ root certificate នេះគឺ៥ឆ្នាំ។

12- កំណត់ទីតាំង Certificate Database និង Certificate Database Log ។ ជា Default វាទាំងពីរមានទីតាំងស្ថិតនៅក្នុង %WINDIR%\System32\CertLog

13- ចុចលើ Next

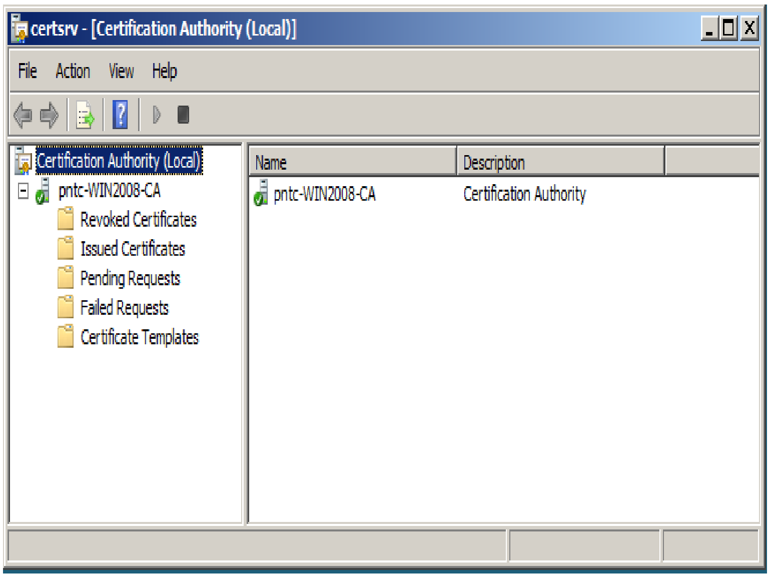


14- ចុចលើ Next

15- ចុចលើ Close នៅពេល Install ត្រូវបានបញ្ចប់

១៩-៧- Certification Authority Management Console

អ្នកអាចគ្រប់គ្រង CA ដោយប្រើ Certification Authority MMC snap-in ដែលស្ថិតនៅក្នុងAdministrator Tools Start Menu ។ នៅពេលដែលអ្នកពង្រីកនៅCA Server នៅក្នុង Management Console អ្នកនិងឃើញ Folders ចំនួន៥ ដែលជួយអ្នកក្នុងការគ្រប់គ្រងលើ templates requests និង certificate ដូចក្នុងរូបភាពខាងក្រោម។

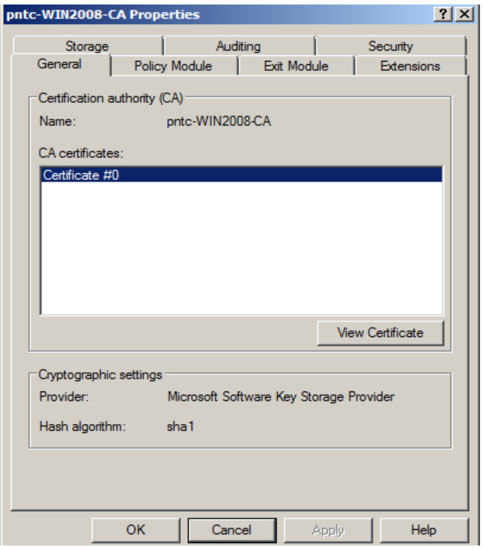


រូបភាពបង្ហាញពី Certificate authority MMC snap-in

Certificate ដែលបានបង្កើតឡើងវិញនិង Certificates folders ដែលបានចេញឱ្យប្រើត្រូវមាន Certifcateដែលបានបង្កើតឡើងវិញនិង certificateដែលបានចេញឱ្យប្រើដោយ Server។ Request Folderដែលកំពុងបើកចំហមាន certificate ណាមួយដែលស្នើសុំតម្រូវការការយល់ព្រមនៅពេលដែល Server ត្រូវបាន Configure ជា Stand-alone CA ។ Failed Request រួមមានគ្រប់ការស្នើសុំទាំងអស់ចំពោះ Certificate ដែលបរាជ័យ។ Certificate Templates folder មាន Template គ្រប់ប្រភេទទាំងអស់នៃ certificate ដែល CA អាចចេញឱ្យប្រើ។

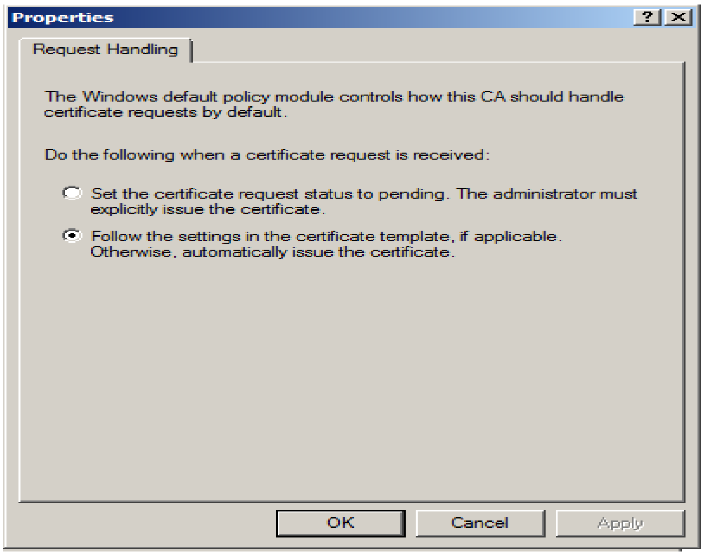
CA Server នីមួយៗមានសំនុំនៃ properties ដែលអ្នកអាច Configure ។ ដើម្បី Access properties ទាំងនេះ ចុចដោយប្រើប៊ូតុងខាងស្តាំនៃ Mouse លើឈ្មោះរបស់ CA Server ហើយជ្រើសរើសយក Properties។ អ្នកនឹងឃើញ Tab ចំនួនដប់ដែលបានប្រើសម្រាប់បង្ហាញពី Configuration របស់ Server។

General tab បង្ហាញក្នុងរូបភាពខាងក្រោមបង្ហាញថា CA certificate ត្រូវបានកំណត់ឱ្យ Server



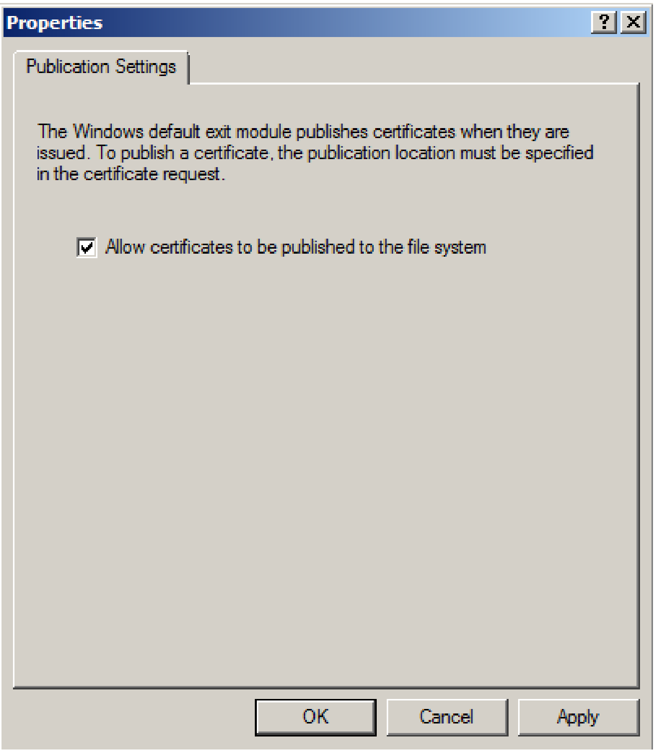
បើវាជា Clean Install អ្នកនិងឃើញតែ certificate មួយគត់គឺជា Certificate ដែលត្រូវបានបង្កើតក្នុងកំឡុងពេលនៃការ Install ។

Policy Module tab បង្ហាញអំពី Policy module ដែលមានសកម្មភាពត្រូវបានប្រើប្រាស់ដោយ Server ។ នៅក្នុងករណីនេះ យើងបាន Install តែ Windows Default policy module ដូច្នេះ module នោះត្រូវបានបង្ហាញ។ ចំពោះ Windows Default module បើអ្នកចុចលើ Properties tab អ្នកអាច Configure ឱ្យ Server ដឹងពីរបៀបផ្តល់ការស្នើសុំ។



Windows default policy module request handling

Exit module ត្រូវបានប្រើប្រាស់សម្រាប់បង្កើតដំណើរការឱ្យអ្វីដែលបានកើតឡើងក្រោយពី certificate ត្រូវបានចេញឱ្យប្រើប្រាស់។ Windows Default Exit module ត្រូវបានគេប្រើប្រាស់ ត្រូវបាន Configure ដើម្បីផ្សព្វផ្សាយ certificate ថ្មី ឱ្យ Active Directory ។ អ្នកក៏អាចផ្សព្វផ្សាយនូវ certificate ថ្មីផងដែរឱ្យ File system ដោយបើក Properties Windows នៃ Windows Default exit module ហើយគូសខ្វែងលើ Allow Certificate ដែលត្រូវផ្សព្វផ្សាយមកឱ្យ File system checkbox ។

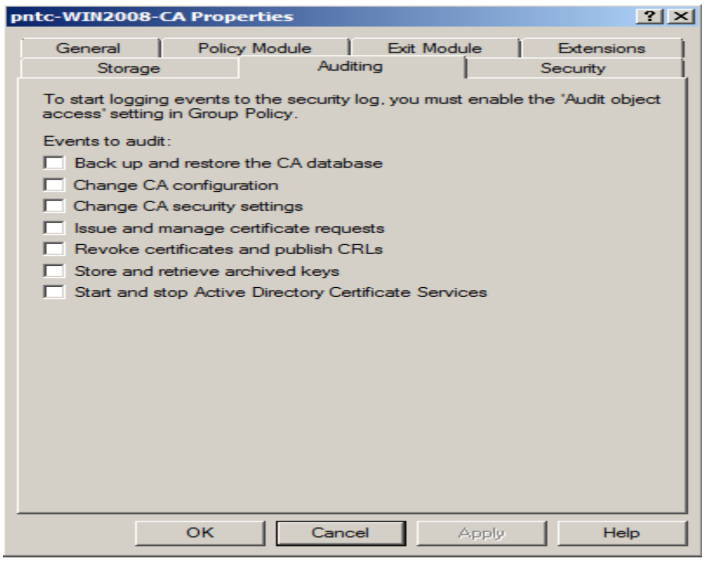


Certificates ទាំងនេះស្ថិតនៅក្នុង **%SYSTEMROOT%\system32\certsrv\certenroll** ។

Enrollment Agent tab ដូចបង្ហាញក្នុងរូបភាពខាងក្រោមមានជម្រើសសម្រាប់ Confi-gure ថាតើ Account មួយណាអាចដើរតួនាទីជា enrollment agent ហើយ certificate template មួយណាត្រូវបានអនុវត្ត។

ជា Default មិនបានកំណត់ចំពោះ Enrollment agents នោះទេ ប៉ុន្តែបើអ្នកត្រូវការកំណត់ឱ្យនរណាម្នាក់ដែលមានសិទ្ធិ Access នេះគឺជាពេលវេលាដែលត្រូវប្រើប្រាស់វា។

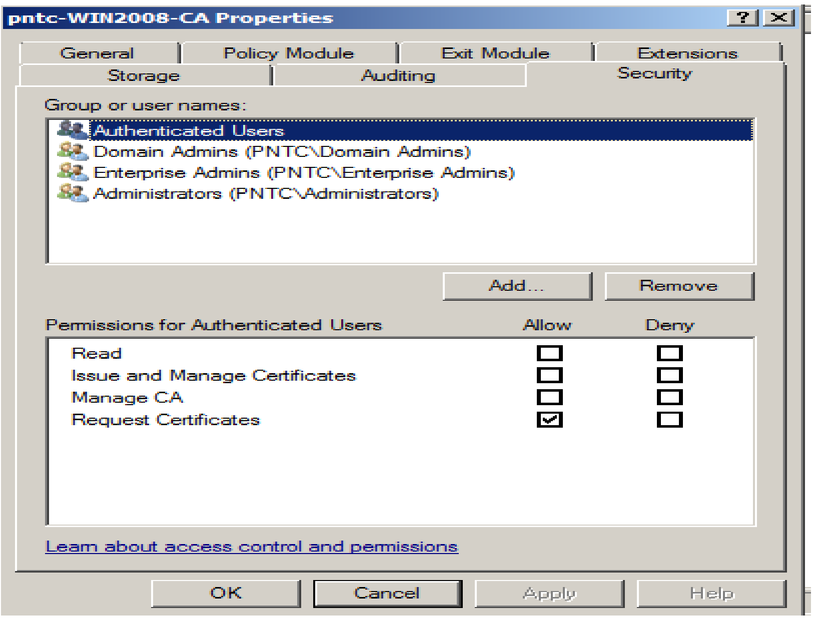
Auditing tab អនុញ្ញាតឱ្យអ្នក Configure នៅអ្វីដែលជា CA events log ចំពោះ Security log ។



Auditing tab

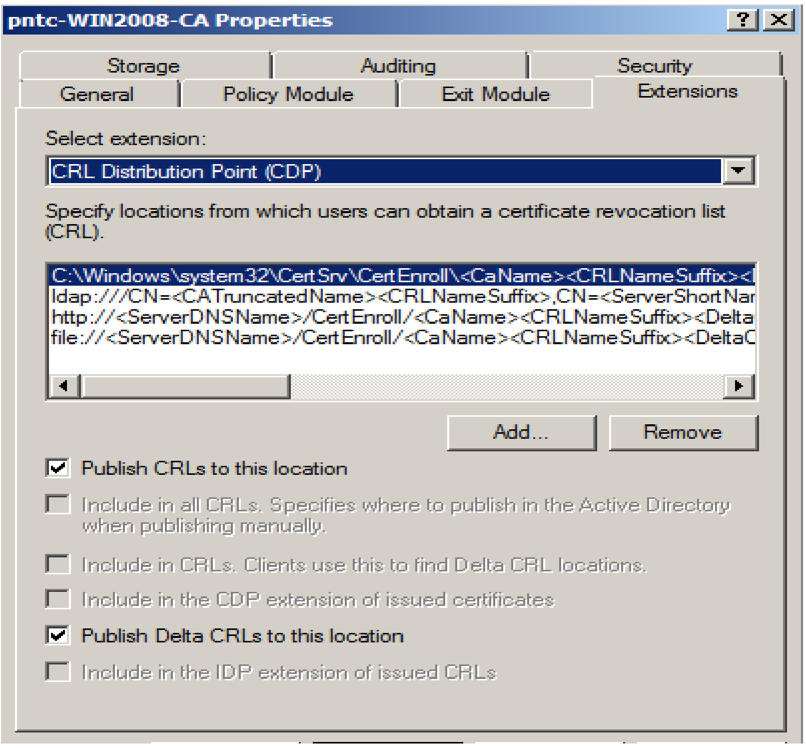
ជាមួយគ្រប់ប្រភេទទាំងអស់នៃ Auditing tab អ្នកគួរជ្រើសរើសយក Events ដែលសំខាន់សម្រាប់អ្នក ។ ដូច្នេះអ្នកអាចកំណត់ត្រានូវអ្វីដែលកើតឡើងដោយមិនចាំបាច់រៀបចំវានោះទេ។

Security permissions នៅជុំវិញ CA store ត្រូវបាន Configure នៅក្នុង Security tab ។



Security tab

Extentsions tab អនុញ្ញាតឱ្យអ្នក Configure ដើម្បីកំណត់ទីតាំង CA extensions ផ្សេងៗទៀតដូចជា CRL Distribution Point ។



Extensions tab

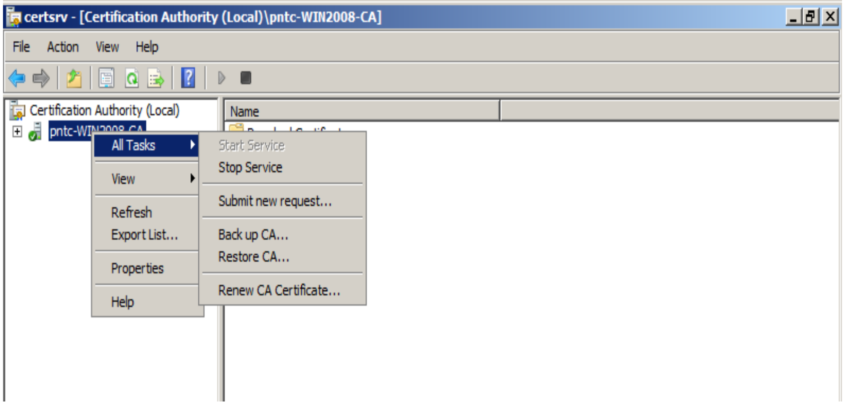
Storage tab បង្ហាញពីទីតាំង certificate database និង request log ស្ថិតនៅ។ អ្នកមិនអាចប្តូរតម្លៃនោះបានទេ ប៉ុន្តែព័ត៌មាននេះត្រូវបានផ្តល់ឱ្យ ដូច្នេះអ្នកអាចរកវាបានដោយងាយ។

Active Directory checkboxត្រូវបានគូសយកហើយមានពណ៌ប្រផេះបើអ្នកមានEnterprise CA ។ ម្យ៉ាងវិញទៀតបើអ្នកមាន Stand-alone CA server ដែលជាសមាជិករបស់ Active Directory Domain អ្នកអាចជ្រើសរើសយកវាក៏បានដើម្បីរក្សាទុក Configura-tion ក្នុង AD ផងដែរ។

លំហាត់អនុវត្ត Backing Up Your CA

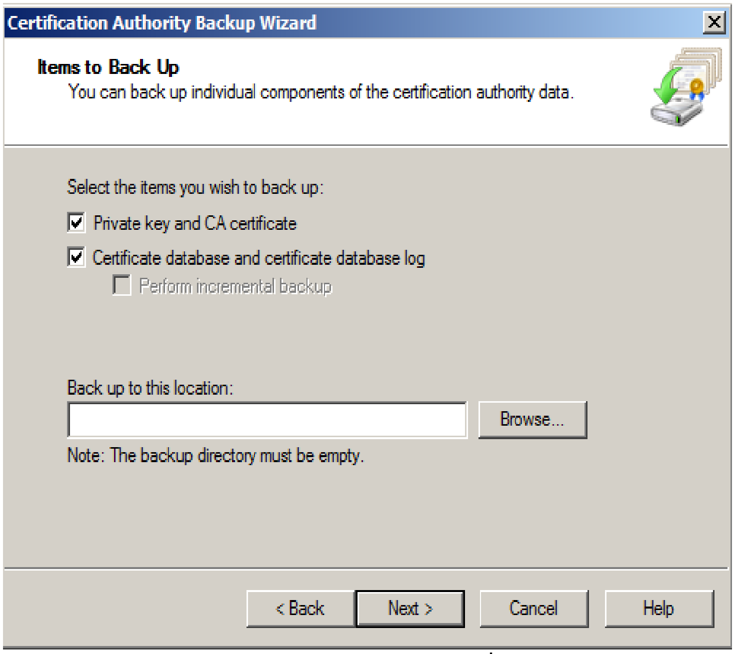
ការថតចម្លង CA ទុកគឺជាការងារមួយដ៏សំខាន់ពីព្រោះថាទោះបីជាយើងមានសមត្ថភាពទាញយកមកវិញដោយប្រើ Recovery agent ក៏ដោយ ការបង្កើត PKI ហាមឃាត់មិនឱ្យបង្កើតឡើងវិញនូវ Key ដូចគ្នាទេ។ ដូច្នេះថតចម្លងវាទុកគឺជាវិធីដ៏ល្អដែលយើងអាចទាញវាមកវិញបាននូវ Private Key CA certificates និង Certificate database តាមជំហានដូចខាងក្រោម៖

1- បង្កើត Filder មួយស្ថិតនៅលើ Local Drive ដែលនិងរក្សាទុក CA មានន័យថា c:\CABAckup
2- បើក Certification Authority management console
3- ចុចលើ Mouse ដោយប្រើ Button ខាងស្តាំលើ CA server instance ហើយជ្រើសរើសយក All Tasks ហើយបន្ទាប់មកទៀតយក Backup CA



4- ចុចលើ Next

5- Tick លើ Private key and CA certificate



6- វាយបញ្ចូល Password បញ្ជាក់បន្ថែមដែលនិងត្រូវប្រើដើម្បីធ្វើឱ្យ Private Key និង CA certificate មានសុវត្ថិភាពហើយចុចលើ Next

7- Next

8- Finish

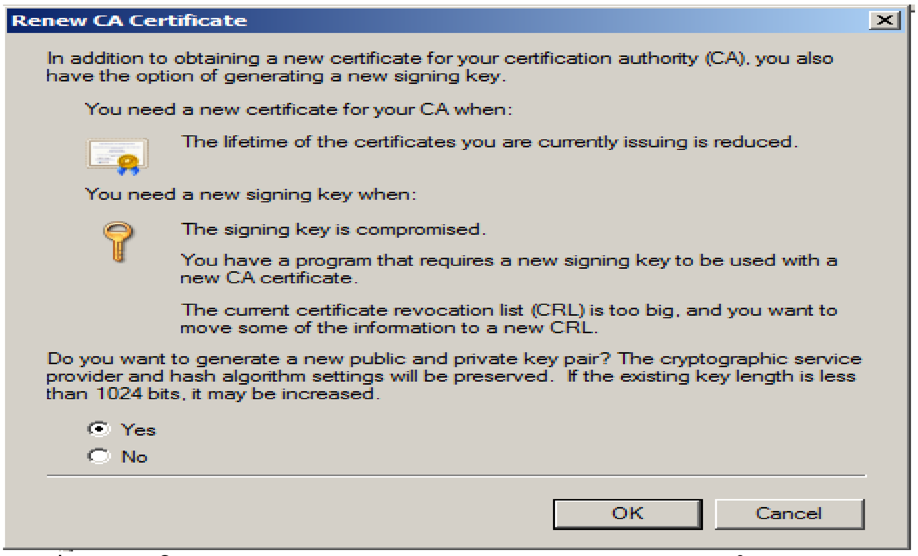
លំហាត់អនុវត្ត ធ្វើឱ្យ CA certificate ថ្មីឡើងវិញ

ក្នុងកំឡុងពេលនៃការ Install CA អ្នកអាចបង្កើត CA certificate ដោយផ្តល់នូវ Password សម្រាប់ Key ឯកជនហើយកំណត់ពីរយៈពេលដែល Certificate អាចប្រើប្រាស់បាន។ នៅក្នុងករណីណាមួយនោះអ្នកត្រូវបង្កើតវាឡើងវិញឬវានិងផុតកំណត់។

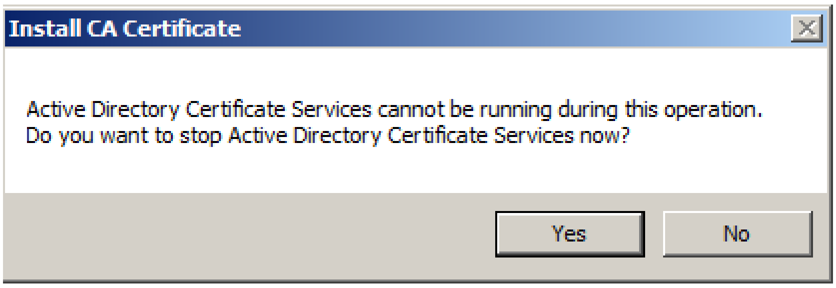
អ្នកត្រូវបង្កើតវាឡើងវិញក្នុងករណីវាត្រូវបានគេស្គាល់ឬអ្នកត្រូវបានបង្កើត CA certificate ថ្មីដើម្បីបង្កើត CRL ថ្មី

1- បើក Certificate Authority Management console

2- ចុចលើ CA server របស់អ្នកដោយប្រើ Mouse ខាងស្តាំ បន្ទាប់មកជ្រើសរើសយក All Tasks ហើយយក Renew CA Certificate.



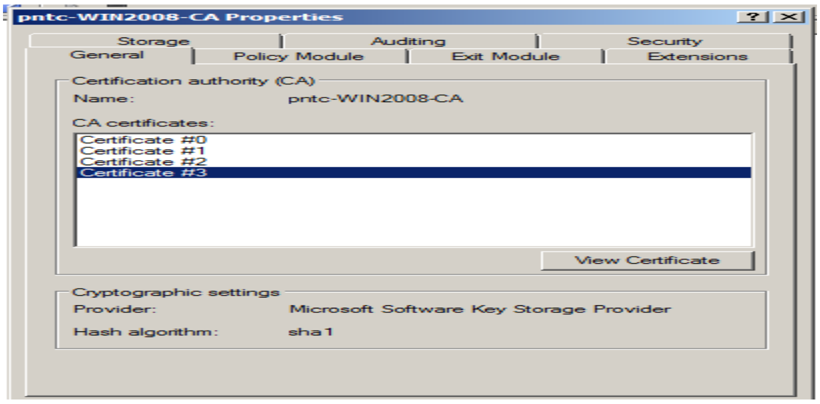
3- អ្នកមិនអាចបង្កើតវាឡើងវិញបានទេពីព្រោះ AD Certificate Serivce កំពុងដំណើរការហើយអ្នកត្រូវចុចលើ Yes ដើម្បីបិទវា។



4- ចុចលើ NO នៅពេលវាទារឱ្យបង្កើត Signing Key ថ្មីហើយចុចលើ Yes បើបង្កើតវា

5- ក្រោយ certificate ថ្មីត្រូវបានបង្កើតរួចហើយ AD certificate និងត្រូវដំណើរការ

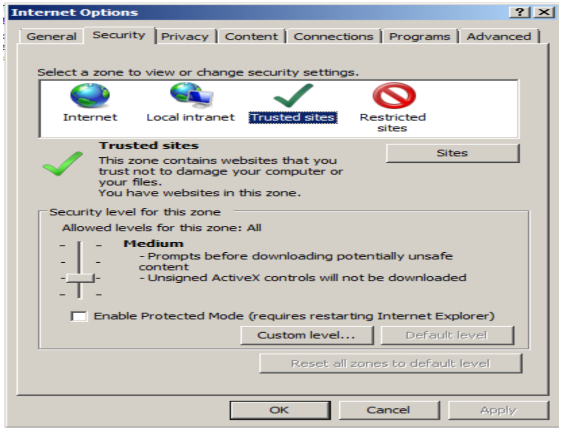
6- ដើម្បីផ្ទៀងផ្ទាត់ឱ្យដឹងថា certificate ថ្មីត្រូវបានបង្កើត ចុចលើ CA Server ដោយប្រើ button mouse ខាងស្តាំហើយជ្រើសរើសយក Properties ។ នៅលើ General Tab CA certificate និងត្រូវមើល ឃើញ។

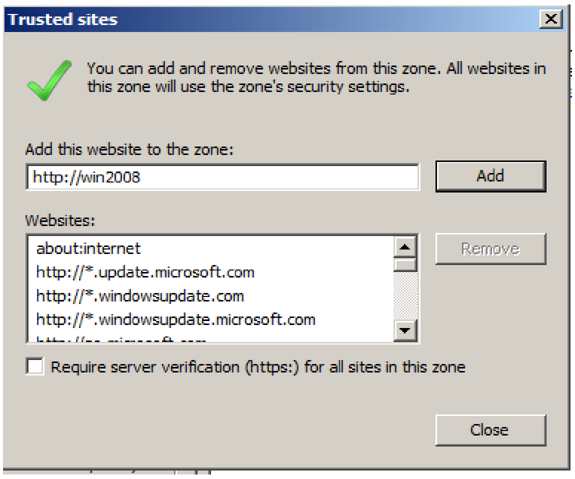


លំហាត់អនុវត្ត ការទទួលបាន Certificate ដោយប្រើ Web Enrollment

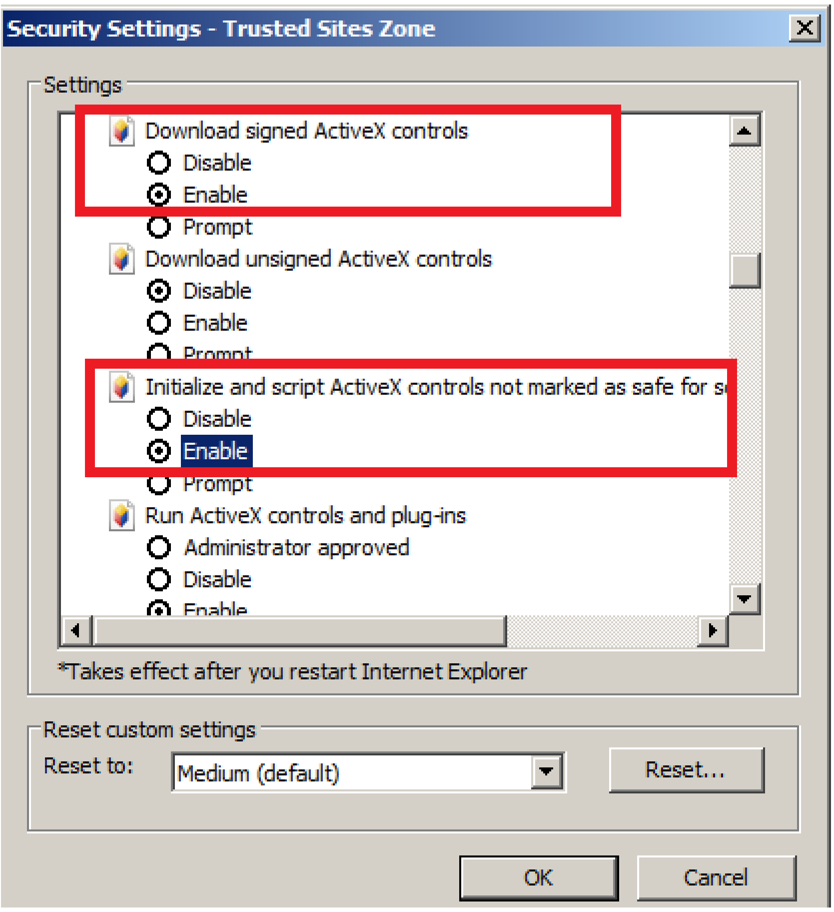
វិធីសាស្ត្រមួយដ៏ងាយបំផុតដើម្បីប្រាប់អ្នកប្រើប្រាស់ឱ្យទទួលបាន Certificate តាមរយៈ Web Enrollment Agent ។ អ្វីដែលគេត្រូវការគឺ Internet Explorer ហើយភ្ជាប់វាមកកាន់ CA server ។

1- បើក Internet Explorer =>Choose Tools=>Internet Options ហើយបើក Security tab ចុចលើ Trusted Sites=>Site button=>Add http:// **win2k 8ca** ដោយជំនួស win2k8ca ជាមួយ Server ដែលបានបង្ហោះ CA

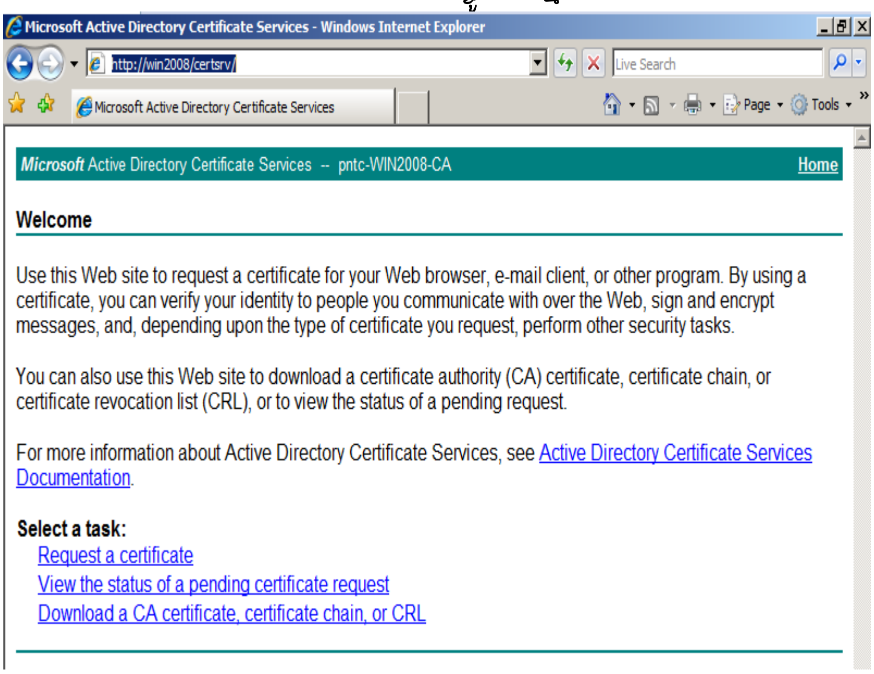




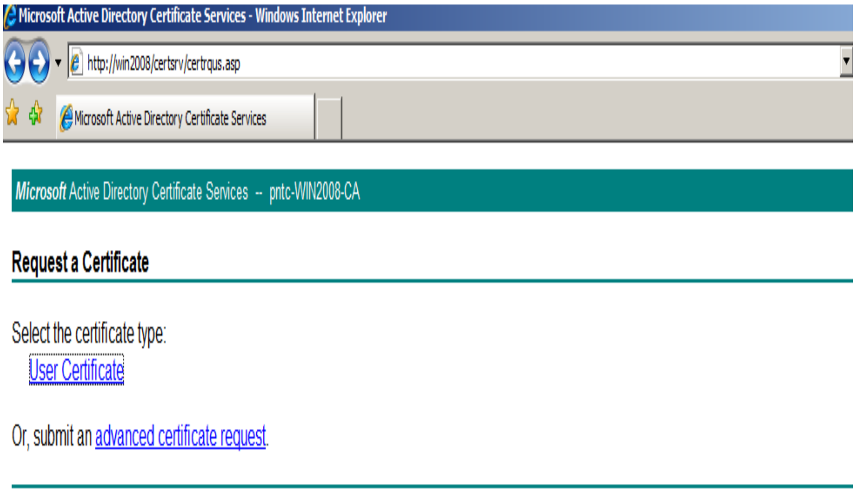
2- នៅក្នុង IE Trusted Sites Zone security settings ចុចលើ Custom Level button ហើយជ្រើសរើសយក Download Unsigned ActiveX Controls and Initialize and Script Active X ដូចក្នុងរូបភាព



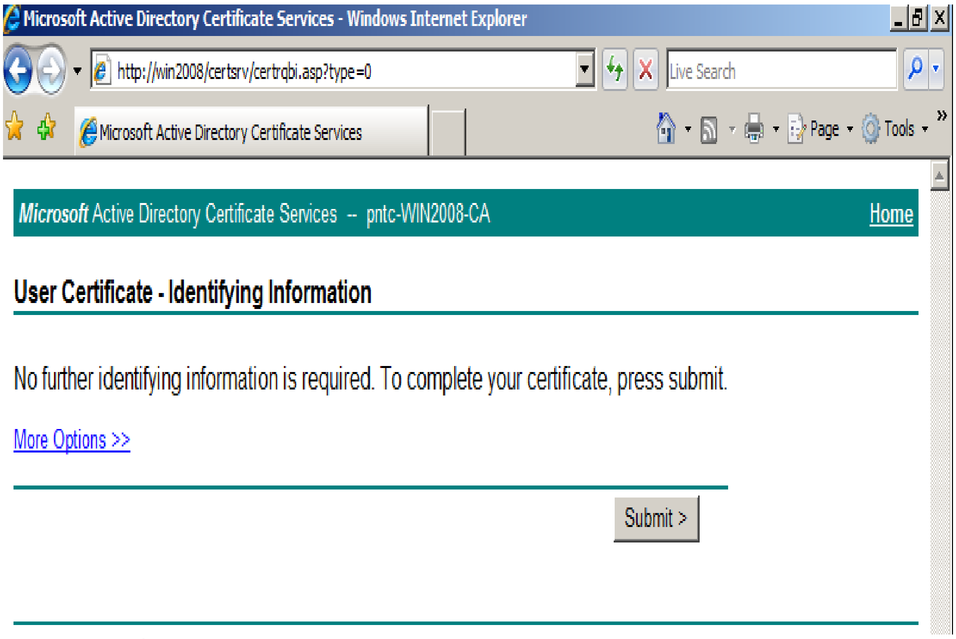
3- ត្រឡប់មក http://win2008/certsrv ហើយវាបញ្ចូលឈ្មោះ Domain



4- ជ្រើសរើសយក User Certificate



5- បើអ្នក Logon ជាមួយ Domain Credential អ្នកទទួលបាន



6- ចុងក្រោយចុចលើ Install

ជំពូកទី២០

ការពារចរាចរណ៍របស់ Network ដោយប្រើ IPsec

សេចក្ដីផ្ដើម

IPSec ការពារប្រព័ន្ធ Network ដោយធ្វើឱ្យ IP packet មានសុវត្ថិភាពដោយធ្វើការអ៊ិនគ្រីបហើយធ្វើឱ្យការប្រាស្រ័យទាក់ទងមានទំនុកចិត្ត។ អ្នកអាចប្រើ IPsec ដើម្បីធ្វើឱ្យការប្រាស្រ័យទាក់ទងរវាង Hosts ពីរមានសុវត្ថិភាពបានឬក៏ធ្វើឱ្យចរាចរណ៍របស់ Network ឆ្លងកាត់ប្រព័ន្ធ Internet មានសុវត្ថិភាពគឺVPN ។

២០-១- តើ IPsec ជាអ្វី ?

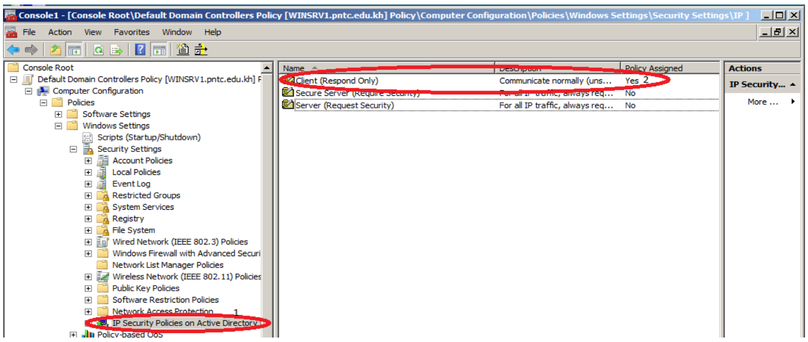
IPsec គឺជាវិធីសាស្ត្រមួយសម្រាប់ធ្វើឱ្យទិន្នន័យមានសុវត្ថិភាពដែលបញ្ជូនរវាងកុំព្យូទ័រពីរដោយប្រើ IP network ។

IPsec ផ្ដល់ឱ្យសុវត្ថិភាពទិន្នន័យរវាង IP address ពីរដូចខាងក្រោម:

- Data Authentication
    - Data origin authentication:អ្នកអាច Configure IPSecដើម្បីធានាថា Packet នីមួយៗដែលអ្នកបានទទួលពីអ្នកដែលមានទំនុកចិត្តគឺថាមកពីប្រភពដើម មិនមែនជា spoof នោះទេ
    - Data integrity: អ្នកអាច Configure IPsec ដើម្បីធានាថាវាមិនត្រូវបានកែប្រែក្នុងកំឡុងពេលនៃការផ្ទេរ។
    - Anti-replay protection:អ្នកអាច Configure IPsec ដើម្បីផ្ទៀងផ្ទាត់ឱ្យដឹងថា Packet នីមួយៗដែលទទួលបានតែមួយគត់ហើយមិនស្ទួន។
- Encryption
    - អ្នកអាច Configure IPsec ដើម្បីអ៊ិនគ្រីបទិន្នន័យហើយធានាថាទិន្នន័យមិនអាចអានបានបើវាត្រូវបានគេទទួលបានក្នុងពេលផ្ទេរ។

២០-២- គោលការណ៍នៃ IPsec

គោលការណ៍នៃ IPsec បានកំណត់ពីរបៀបដែលកុំព្យូទ័រឬក្រុមនៃកុំព្យូទ័របំរើសេវានៃការប្រាស្រ័យទាក់ទងតាម IPsec។ អ្នកអាចកំណត់គោលការណ៍នៃ IPsec បានចំពោះកុំព្យូទ័រមួយបានដោយប្រើ Local Security Policy ឬកំណត់ចំពោះក្រុមនៃកុំព្យូទ័រដោយប្រើ Group Policy ។



រូបភាព២០-១-Group Policy Object (GPO)

គ្រប់ IPsec Policy រួមមាន IPsec Policy rule មួយឬច្រើនដែលបានសម្រេចចិត្តថាពេលណានិង IP traffic ត្រូវបានការពារតាមរបៀបណា។

ឧទាហរណ៍នៃ IPsec Policy

ក្នុងរូបភាពខាងក្រោមបង្ហាញពី IPsec Policy និងពីរបៀបដែល Policy នោះត្រូវមានរួមទាំង rules, filters និង filter action ។ នៅក្នុងឧទាហរណ៍នេះ Policy រួមមានបី rules គឺ:

- Ruleទី១មានអាទិភាពជាងគេពីព្រោះវាបានកំណត់ពីចរាចរណ៍ដែលត្រូវការជាងគេបំផុត(Telnet or Post Office Protocol 3[POP3])ដោយ Address 192.168.3.32 or 192.168.3.200)
- Rule ទី២ បានកំណត់ចរាចរណ៍តាមប្រភេទ(telnet or POP3)
- Rule ទី៣ វាមិនសូវសំខាន់ណាស់ទេពីព្រោះវាបានអនុវត្តទៅលើគ្រប់ចរាចរណ៍ទាំងអស់ ដូច្នេះវាមានអាទិភាពទាប។

IPsec Policy

Policy Rule#1	Filter#1:telnet traffic from 192.168.3.32 Filter#2:POP3 traffic from 192.168.3.200	Negotiate Security (Required Encrypt)
Policy Rule#2	Filter#1:All Telnet traffic Filter#2:All POP3 Traffic	Block
Policy Rule#3	Filter#1:All Traffic	Negotiate Security (Required Authentication)

រូបភាព២០-២-បង្ហាញពី IPsec policies, rules filters and filter action

ដូចលទ្ធផលនៃ IPSec Policy រួមមាន rules បីប្រភេទ ដូច្នេះកុំព្យូទ័រដែលត្រូវបានកំណត់ Policy នេះឱ្យនិងព្យាយាមផ្ទៀងផ្ទាត់គ្រប់ទិន្នន័យទាំងអស់ពី Telnet និង POP3 ។ ចរាចរណ៍របស់ Telnet និង POP3 តាមលំនាំដើមត្រូវបានបិទលុះត្រាតែវាទទួលបានមកពី 192.168.3.32(សម្រាប់Telnet)ឬមកពី 192.168.3.200(សម្រាប់ POP3) នៅក្នុងករណីនេះចរាចរណ៍ត្រូវបានអនុញ្ញាតបើអ៊ិនគ្រីបត្រូវបានចរចារទទួលបានជោគជ័យ។

២០-៣- របៀបដែល IPsec ត្រូវបានបង្កើតឡើង

ដើម្បីបង្កើត SAs ជាស្វ័យប្រវត្តរវាង IPsec នោះគេត្រូវប្រើ IKE(Internet Key Exchage) protocol។ IKE បង្កើតគោលការណ៍យល់ព្រមដែលបានកំណត់ពី SA ដែលជាគោលការណ៍រួមមានសេវាសុវត្ថិភាពរបស់វា យន្តការការពារ កូនសោរគ្រីស្តូក្រាហ្វិករវាងការប្រាស្រ័យទាក់ទងដែលមានសិទ្ធិស្មើគ្នា។

ដើម្បីបង្កើត IPsec គេអនុវត្តតាមជំហានដូចខាងក្រោម:

១-បង្កើត(setup) SA mode

២-ទទួលយកការប្រាស្រ័យទាក់ទងនិងអាល់ហ្គូរីតសម្រាប់អ៊ិនគ្រីប

៣-បង្កើត SA mode ឆាប់រហ័ស

៤-បញ្ជូន Data

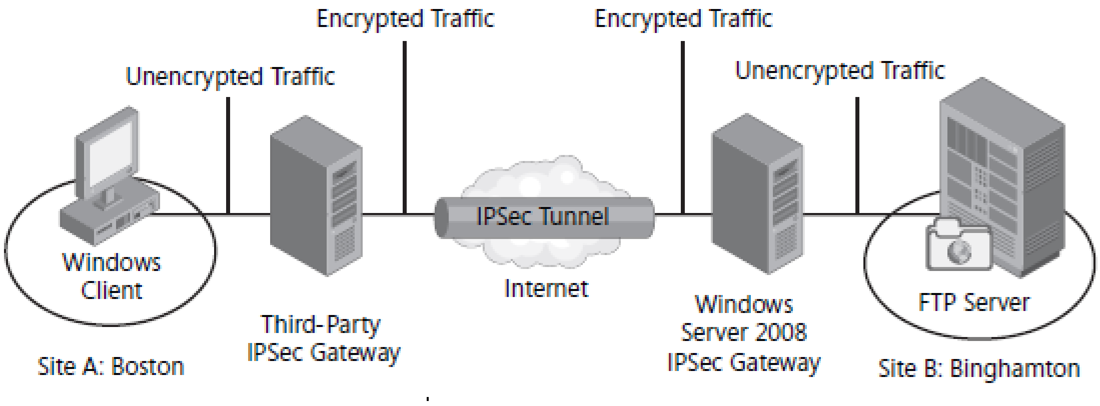
២០-៤- ការប្រើ IPsec នៅក្នុង Tunnel Mode

តាមលំនាំដើម IPsec ដំណើរការនៅក្នុង Transport mode ដែលត្រូវបានប្រើសម្រាប់សុវត្ថិភាពពីប្រភពដើមនិងប្រភពចុងនៃការប្រាស្រ័យទាក់ទងរវាងកុំព្យូទ័រ។ Transport mode ត្រូវបានប្រើនៅក្នុង IPsec ដែលពឹងផ្អែកលើ VPNs ដែលជា L2TP protocol សម្រាប់បង្កើតផ្លូវរូងនៃ IPsec តាមប្រព័ន្ធ Network សាធារណៈ។

ទោះបីជាយ៉ាងណាក៏ដោយនៅពេលដែល VPN gateway ពិសេសមិនត្រូវគ្នាជាមួយ L2TP/IPsec VPNs អ្នកអាចប្រើ IPsec នៅក្នុង Tunnel mode ជំនួសវិញ។ ជាមួយ Tunnel mode IP Packet ទាំងមូលត្រូវបានការពារហើយបន្ទាប់មកត្រូវបាន encapsulate ជាមួយ IP Packet header ដែលមិនបានការពារ។

ចំណាំ

Tunnel mode កំរប្រើណាស់។



រូបភាព២០-៣-បង្ហាញពីការបង្កើតផ្លូវរូងពី Gateway ទៅ Gateway រវាង Site

Authentocation Method សម្រាប់ IPSec

សញ្ញាណសំខាន់ដើម្បីអនុវត្តទៅលើ IPsecគឺថា IPsec ត្រូវការមេកានិក authentication ដែលមានចែករំលែករវាងកុំព្យូទ័រដែលកំពុងធ្វើការប្រាស្រ័យទាក់ទង។ អ្នកអាចប្រើវិធីណាមួយក្នុងចំណោមវិធីសាស្ត្រទាំងបីសម្រាប់ Authenticate host កំពុងធ្វើការប្រាស្រ័យទាក់ទងតាមរយៈ IPSec:

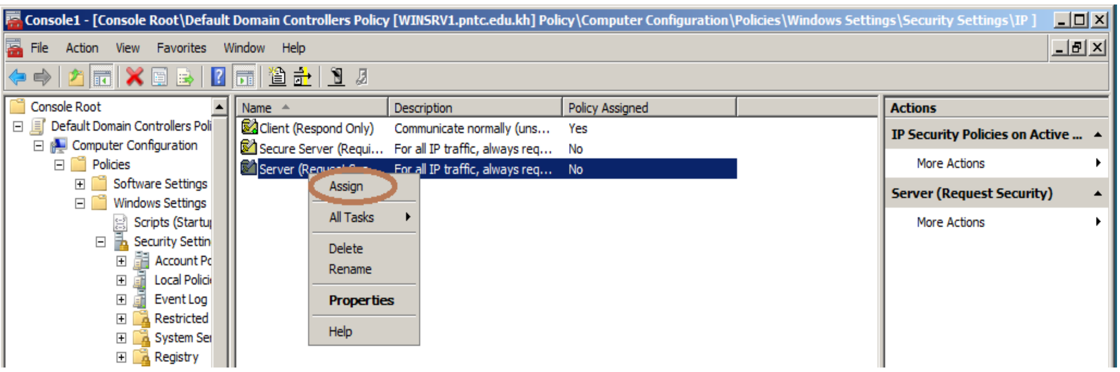
- Kerberos (Active Directory):ដោយសារតែ Kerberos គឺជា authentication protocol តាមលំនាំដើមនៅក្នុងមជ្ឈដ្ឋាននៃ Active Directory។ វិធីដ៏ងាយបំផុតសម្រាប់ Configure authentication IPsec គឺត្រូវអនុវត្ត IPsec ជាមួយ Active Directory Forest តែមួយគត់។
- Certificates:បើអ្នកត្រូវការអនុវត្ត IPsec នៅក្នុងមជ្ឈដ្ឋាននៃការផលិតដែលគ្មាន Authentication អ្នកគួរប្រើហេដ្ឋារចនាសម្ព័ន្ធនៃ certificate សម្រាប់ Authenticate IPsec peers។ នៅក្នុងដំណោះស្រាយនេះ Host នីមួយៗត្រូវតែទទួលនិងដំឡើង កុំព្យូទ័រ certificate ពី public or private CA ។
- Preshared Key:វាគឺជា password ដែលបានចែករំលែកដោយ Peers ហើយត្រូវបានប្រើសម្រាប់អ៊ិនគ្រីបនិងដេគ្រីបទិន្នន័យ។ នៅក្នុង IPsec អ្នកក៏អាចកំណត់ preshared key នៅលើ endpoints ដើម្បីបើកអ៊ិនគ្រីបរវាង Hosts ។ ទោះបីជា authentication នេះបានបើក IPSec SA ដើម្បីបង្កើតក៏ដោយ preshared key មិនបានផ្តល់កម្រិតដូចគ្នានៃ authentication ដែល certificate និង Kerberos បានធ្វើ។ បន្ថែមលើសពីនេះទៅទៀត Preshared key សម្រាប់ IPsec ត្រូវបានរក្សាទុកនៅក្នុងទម្រង់ជាអត្ត

បទធម្មតានៅលើកុំព្យូទ័រនីមួយៗឬនៅក្នុង Active Directory ដែលបានកាត់បន្ថយសុវត្ថិភាពនៃដំណោះស្រាយ។ ចំពោះហេតុផលនេះ វាទាមទារឱ្យអ្នកប្រើ preshared key តែក្នុងមជ្ឈដ្ឋានមិនមែនជាសង្វាក់ផលិតកម្មដូចជា Test Network ជាដើម

២០-៥- ការកំណត់ឱ្យដោយប្រើ IPsec Policy ដែលបានកំណត់ទុកជាមុន

នៅក្នុង Group Policy មាន IPsec បីត្រូវបានកំណត់ទុកជាមុន។ អ្នកក៏អាចកំណត់ IPsec Policy សម្រាប់ Domain ឬ Ou បានដែរដោយកំណត់នូវ Policy ណាមួយនៃ Policy ខាងក្រោម:

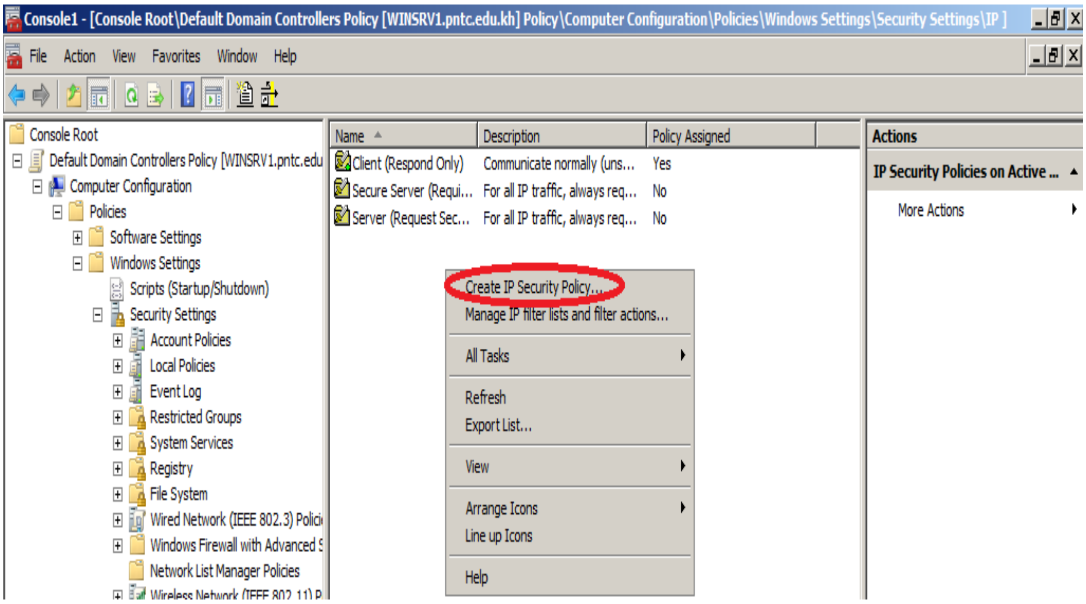
- Client(Respond Only):នៅពេលអ្នកកំណត់វាទៅឱ្យកុំព្យូទ័រមួយតាមរយ:GPO មួយកុំព្យូទ័រនោះនិងមិនចាប់ផ្តើមធ្វើការស្នើសុំដើម្បីបង្កើតIPsec channel ជាមួយកុំព្យូទ័រផ្សេងនោះទេ។ ទោះបីជាយ៉ាងណាក៏ដោយ កុំព្យូទ័រណាមួយដែលអ្នកបានកំណត់ client policy និងចរចារហើយបង្កើត IPsec នៅពេលមានការស្នើសុំដោយកុំព្យូទ័រផ្សេងទៀត។ តាមធម្មតាអ្នកត្រូវការកំណត់គោលការណ៍នេះទៅឱ្យ intranet កុំព្យូទ័រ ដែលត្រូវការធ្វើការប្រាស្រ័យទាក់ទងជាមួយ Server ដែលមានសុវត្ថិភាព ប៉ុន្តែមិនត្រូវការការគ្រប់ចរាចរទាំងអស់នោះទេ។
- Server(Request security):អ្នកគួរកំណត់គោលការណ៍នេះទៅកុំព្យូទ័រដែលត្រូវការអ៊ិនគ្រីប។ ចំពោះគោលការណ៍នេះកុំព្យូទ័រនេះទទួលយកចរាចរដែលគ្មានសុវត្ថិភាព ប៉ុន្តែជាទូទៅព្យាយាមនូវការប្រាស្រ័យទាក់ទងដែលមានសុវត្ថិភាពដោយធ្វើការស្នើសុំសុវត្ថិភាពពីអ្នកបញ្ជូន។ គោលការណ៍នេះអនុញ្ញាតឱ្យការប្រាស្រ័យទាក់ទងទាំងមូលគ្មានសុវត្ថិភាពបើកុំព្យូទ័រផ្សេងគ្មានបើក IPsec ។ ឧទាហរណ៍ ការប្រាស្រ័យទាក់ទងមួយជាមួយ Server ពិតប្រាកដមួយអាចមានសុវត្ថិភាពនៅក្នុង ខណ:ដែលវាអនុញ្ញាតឱ្យ Server ធ្វើការប្រាស្រ័យទាក់ទងនៅក្នុងលក្ខណ:គ្មានសុវត្ថិភាពដើម្បីតម្រូវទៅតាមការបញ្ចូលគ្នានៃ Client។
- Secure Server(Require security):អ្នកអាចកំណត់ Policy នេះទៅឱ្យ intranet servers ដែលត្រូវការការប្រាស្រ័យទាក់ទងដែលមានសុវត្ថិភាពដូចជាServerដែលផ្ទេរទិន្នន័យដ៏មានសារ:សំខាន់។



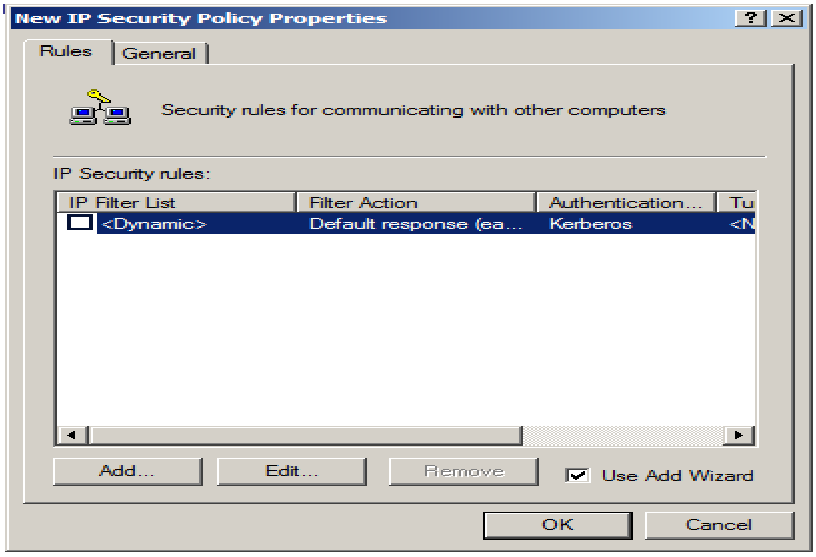
រូបភាព២០-៤-បង្ហាញពីការកំណត់ policy

បង្កើត IPsec Policy ថ្មី

បើក Local security Policy ឬ GPO។ ចំពោះ GPO វិញនៅក្នុង កុំព្យូទ័រ Configuration=>Windows Settings=>Security settings=>IP security Policies ហើយបន្ទាប់មកចុចលើ Panel ទី២ដោយប្រើប៊ូតុងរបស់ Mouse ខាងស្តាំ=>Create IP security Policy...

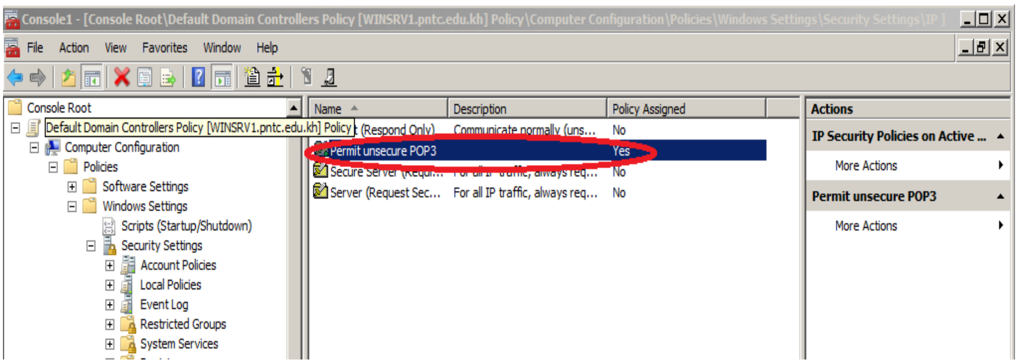


រូបភាព២០-៥-បង្ហាញពីការបង្កើត Policy ថ្មី



រូបភាព២០-៦-បង្ហាញពីផ្ទាំង IP security Rule ថ្មី

ដាក់ឈ្មោះថា Permit unsecure POP3



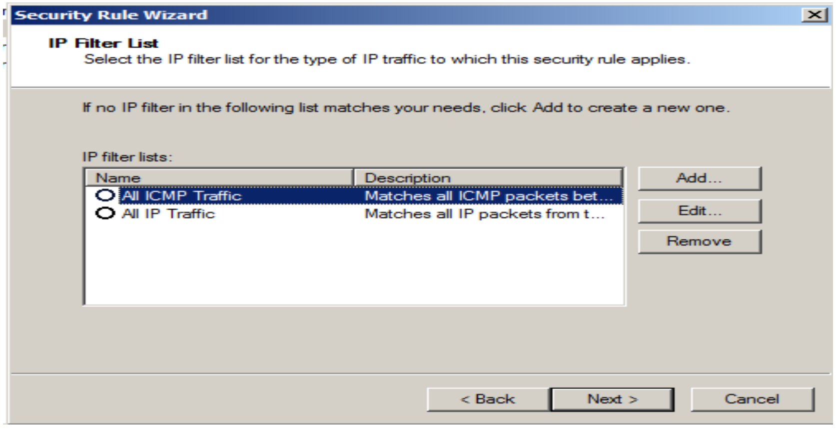
រូបភាព២០-៧-ដាក់ឈ្មោះឱ្យវាគឺ Permit unsecure POP3

ការប្រើ Create IP Security Rule wizard

បណ្តុំនៃ IPSec Policy configuration រួមមានការបង្កើតនិង Configuration IPSec rule សម្រាប់គោលការណ៍នោះ។

ខាងក្រោមនេះពិពណ៌នាអំពីការបង្កើត IP security wizard

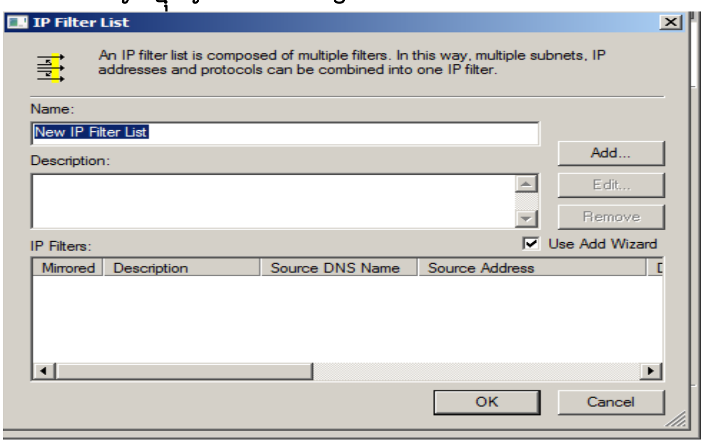
- Tunnel Endpoint page: Configure វានៅពេលអ្នកត្រូវការប្រើ IPsec នៅក្នុង Tunnel mode
- Network Type page: គេប្រើវាក្នុងករណីអ្នកចង់កំណត់ពីច្បាប់សម្រាប់ LAN ឬ remote access connection ។
- IP filter List Page :ដើម្បីកំណត់សំនុំនៃ IP filters ដែលអ្នកចង់ភ្ជាប់មកកាន់ច្បាប់នេះ។



រូបភាព២០-៨-ការបង្កើត IP filter ថ្មីដើម្បីភ្ជាប់ជាមួយ IPsec Policy rule

បង្កើត IP filter ថ្មីសម្រាប់បន្ថែមទៅឱ្យ IP filter List ថ្មីដែលអ្នកបានបង្កើតវា។

ចុចលើ Add នៅក្នុង IP filter List ដូចក្នុងរូបភាពខាងក្រោម៖

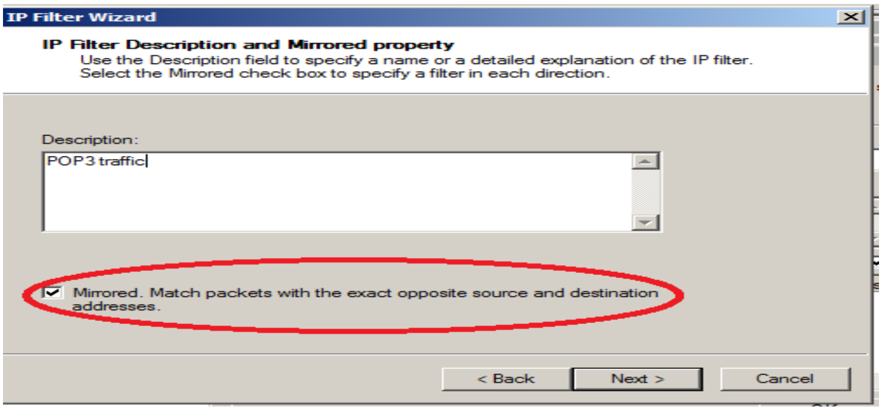


រូបភាព២០-៩-ការបង្កើត IP filter ថ្មីដើម្បីបន្ថែមចូលក្នុង IP filter list

ប្រើ IP filter Wizard ដើម្បីកំណត់ IP traffic អាស្រ័យទៅតាមប្រភពដើមនិងគោលដៅ។ អ្នកអាចកំណត់ពីប្រភពដើមនិងគោលដៅអាស្រ័យទៅលើ IP address,DNS name,server function ដូចជា DHCP server ,DNS Server,WINS server ឬក៏ default gateway ហើយ IP protocol មានដូចជា TCP/UDP port ។

អ្នកក៏អាចប្រើ IP filter wizard ផងដែរសម្រាប់បង្កើត "Mirrored"filter ។ Mirrored filter ត្រូវគ្នាជាមួយប្រភពដើមនិងគោលដៅជាមួយ Address ដែលផ្ទុយគ្នា។ ឧទាហរណ៍ អ្នកអាច Configure filter ដែលអាចចាប់យក POP3 traffic ដែលបានបញ្ជូនទៅនិងមកបានចំពោះ local address ។

ដើម្បី Configure filter ជា mirror filter ដោយទុកឱ្យប្រអប់ Mirrored checkbox មានការ Tick ដដែលដូចក្នុងរូបភាព។



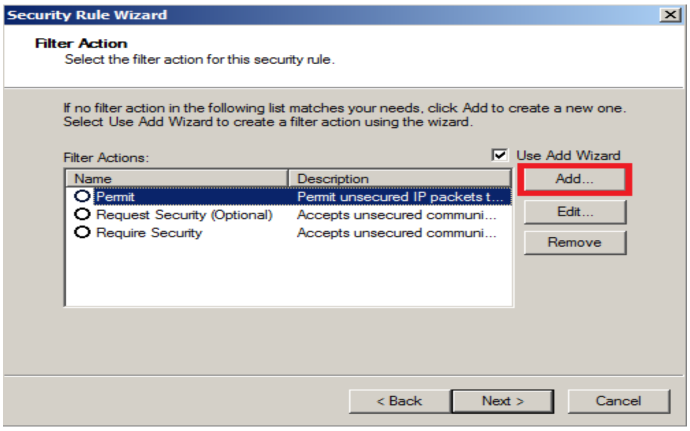
រូបភាព២០-១០-ការបង្កើត Mirrored filter

- Filter Action Page: ក្រោយពីអ្នកបានភ្ជាប់ IP filter ដែលពេញចិត្តទៅជាមួយ Rule រួចហើយ អ្នកអាចកំណត់ឱ្យបានច្បាស់លាស់ចំពោះ filter action សម្រាប់ rule នៅក្នុង Security wizard

នៅក្នុង Group Policy មាន IP filter បីប្រភេទដែលមានស្រាប់សម្រាប់ IPsec Policy rule:

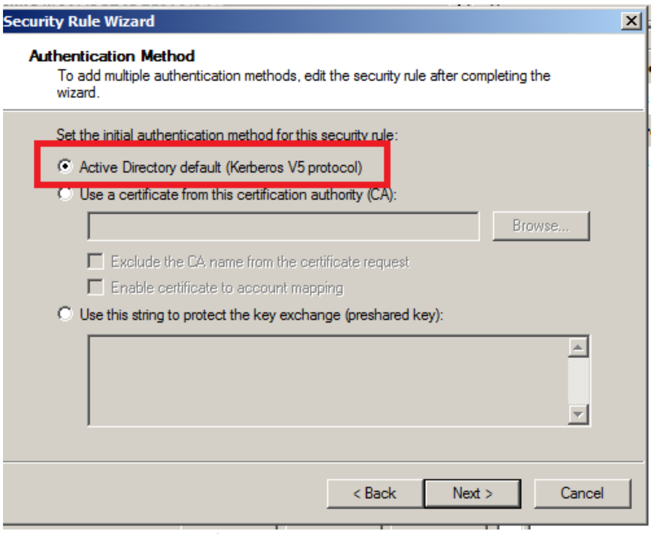
- Permit: filter action នេះអនុញ្ញាតឱ្យ IP packets ឆ្លងកាត់ផ្លូវដែលគ្មានសុវត្ថិភាព
- Request Security(optional):filter action នេះអនុញ្ញាតឱ្យ IP packets ឆ្លងកាត់តាមផ្លូវដែលគ្មានសុវត្ថិភាពប៉ុន្តែត្រូវការស្នើសុំឱ្យclientធ្វើការចរចារពីសុវត្ថិភាព(គេពេញចិត្តប្រើអ៊ិនគ្រីប)
- Require Security: filter action នេះបង្ហាញឱ្យ(trigger) local កុំព្យូទ័រដឹងដើម្បីធ្វើការស្នើសុំការប្រាស្រ័យទាក់ទងដែលមានសុវត្ថិភាពពីប្រភព client នៃ IP packet ។ បើវិធីសាស្ត្រនៃសុវត្ថិភាពនោះមិនអាចបង្កើតបានទេ local កុំព្យូទ័រ និងបញ្ឈប់ការប្រាស្រ័យទាក់ទងជាមួយ Client នោះ។

ដើម្បីបង្កើត filter action ថ្មី ចុចលើ Add button នៅលើ Filter Action នៃ Security Rule Wizard ដូចក្នុងរូបភាពខាងក្រោម:



រូបភាព២០-១១-ការបង្កើត Filter Action ថ្មី

- Authentication Method page: Security អាចធរធារបានតែក្រោយពី IPSec clients ត្រូវបាន authenticate។ តាមលំនាំដើម IPSec rule ពឹងផ្អែកលើ Active Directory service និង Kerberos protocol ដើម្បី authenticate client ។ ទោះបីជាយ៉ាងណាក៏ដោយអ្នកក៏អាចកំណត់ certificate authentication method សម្រាប់ IPsec ដោយអ្នកប្រើ Authentication Method page នៃ Security Rule Wizard ដូចក្នុងរូបភាពខាងក្រោម:



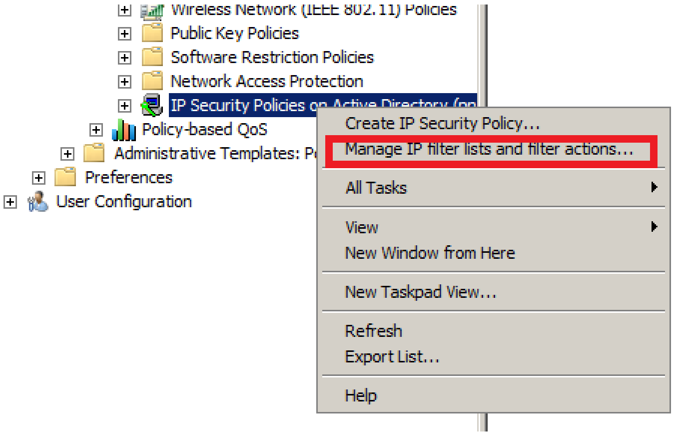
រូបភាព២០-១២-បង្ហាញពី authentication method សម្រាប់ IPsec ថ្មី

ចំណាំ: ផ្ទាំងខាងលើមិនបង្ហាញទេបើយើងជ្រើសរើសយក Permit on the Filter Action ។

២០-៦- ការគ្រប់គ្រង IP filter Lists និង Filter Action

ចំពោះ IP filters, IP filter lists និង filter action អ្នកអាចបង្កើតសម្រាប់ IPsec rule ដែលអាចចែករំលែកជាមួយ IPsec rule ផ្សេងៗទៀត។ អ្នកក៏អាចបង្កើតនិង Configure លក្ខណៈពិសេសទាំងនេះនៅខាងក្រៅនៃ Security Rule Wizard ផងដែរ។

ដើម្បីអនុវត្តវា យើងត្រូវចុចដោយប្រើប៊ូតុង Mouse ខាងស្តាំលើ IP security policies នៅក្នុង Local Security Policy ឬ GPO ហើយជ្រើសរើសយក Manage IP Filter Lists and Filter Actions ដូចខាងក្រោម:

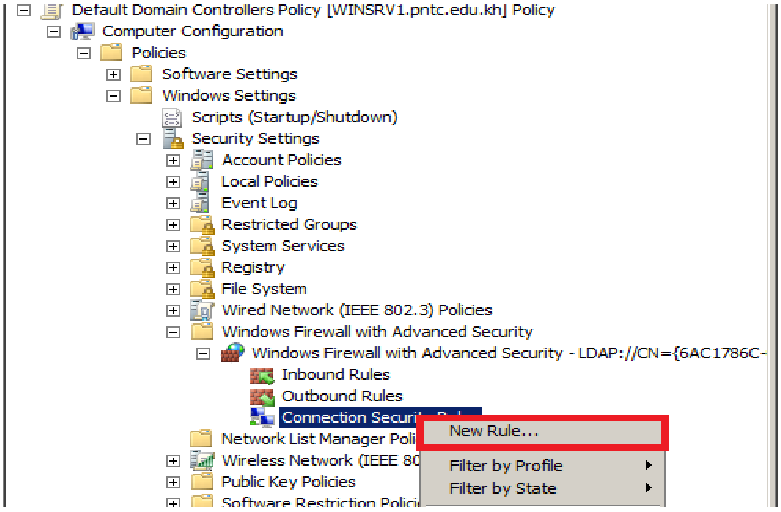


រូបភាព២០-១៣-ការគ្រប់គ្រងលើ IP filter lists and filter actions

២០-៧- ការបង្កើតនិងការ Configure ច្បាប់សម្រាប់សុវត្ថិភាពនៃការភ្ជាប់

ដើម្បីបង្កើត Connection Security Rule នៅក្នុង GPO ជាដំបូង browse និងពង្រីកកុំព្យូទ័រ Configuration\Policies\Windows Settings\Security Settings\Windows Firewall With Advanced Security\ Windows Firewall With Advanced Security-LDAP://Address.

នៅខាងក្រោម node នេះចុចដោយប្រើប៊ូតុងខាងស្តាំលើ connection security rule node ហើយបន្ទាប់មកពី Shortcut menu ជ្រើសរើសយក New Rule



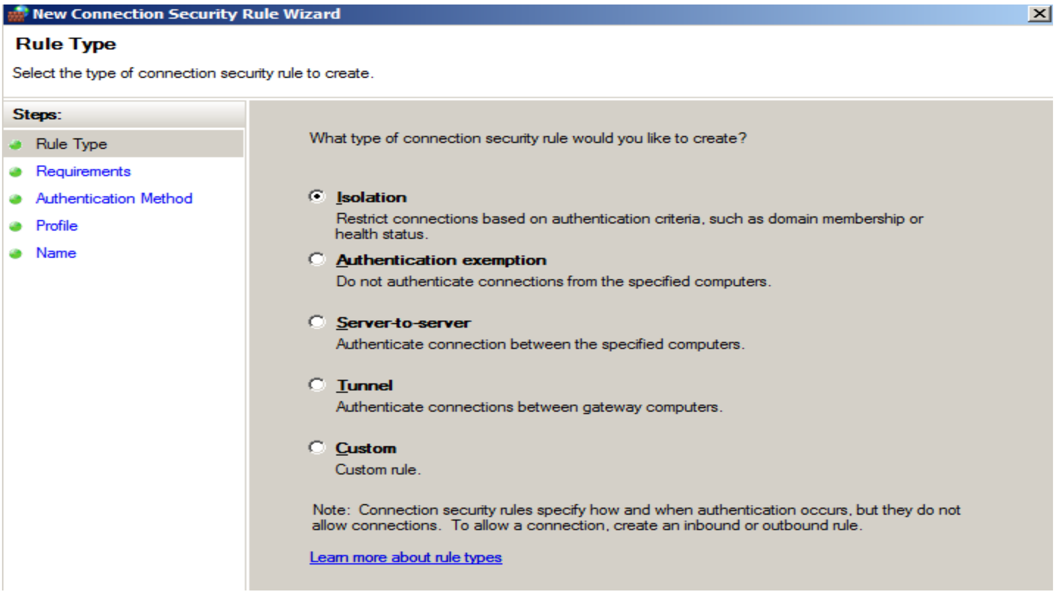
រូបភាព២០-១៤-ការបង្កើត Connection security Rule ថ្មី

២០-៧-១- ការប្រើ New connection Security Rule Wizard

ផ្ទាំងដែលអ្នកបានឃើញអ្នកអាចប្រើវាបានអាស្រ័យទៅលើប្រភេទនៃ Rule ដែលអ្នកចង់ប្រើវាដើម្បីបង្កើតទំព័រដំបូង។

ខាងក្រោមនេះពន្យល់ពី Rule ទាំង៥

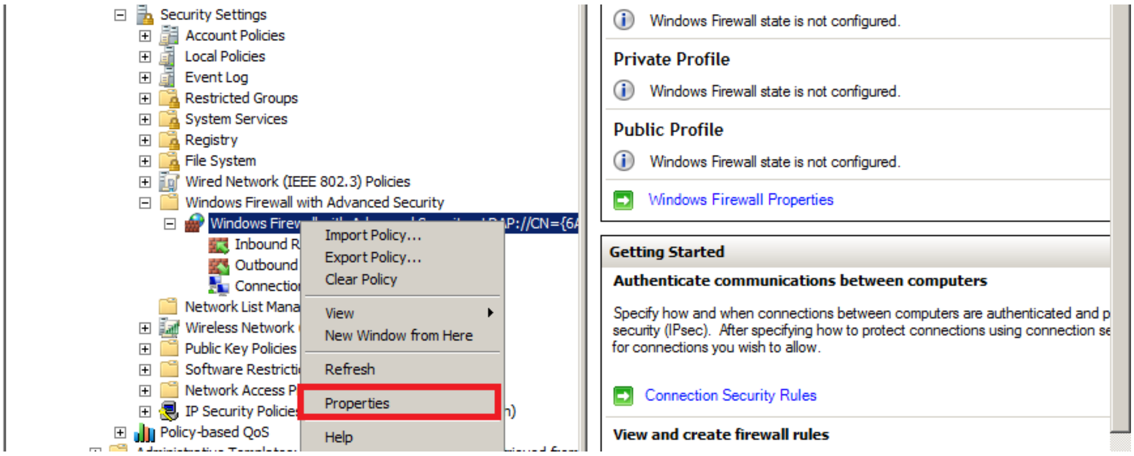
- Isolation Rule:នេះគឺជា Rule ទូទៅដែលត្រូវបានប្រើសម្រាប់ Authenticate គ្រប់ចរាចរណ៍សម្រាប់ជ្រើសរើសយក Network profiles ។ Profiles ទាំងបីនោះគឺ Domain, Private និង Public
- Authentication Exemption rule:អ្នកអាចប្រើប្រភេទនៃ Rule នេះដើម្បីកំណត់ពីកុំព្យូទ័រមួយឬក្រុមនៃកុំព្យូទ័រឬបណ្តុំនៃ IP address ដើម្បី authenticate ខ្លួនវាដោយមិនគិតពី connection security rule ផ្សេងៗទៀត។
- Server-to-server rule:ប្រភេទនៃ Rule នេះអនុញ្ញាតឱ្យអ្នក authenticate ការប្រាស្រ័យទាក់ទងរវាង IP addresses ឬសំនុំនៃ Addresses ដោយរួមមានទាំង កុំព្យូទ័រ និង subnets
- Tunnel rule:ប្រើប្រភេទនៃ Rule នេះដើម្បី Configure IPsec tunnel mode សម្រាប់ VPN gateways
- Custom rule:គេប្រើ Rule ប្រភេទនេះដើម្បីបង្កើត Rule មួយដែលត្រូវការ settings ពិសេសឬជាបន្សំនៃលក្ខណៈពិសេសពីប្រភេទផ្សេងៗ
- Endpoints page:គេប្រើទំព័រនេះដើម្បីកំណត់ពីកុំព្យូទ័រនៅឆ្ងាយជាមួយកុំព្យូទ័រដែលអ្នកចង់ធ្វើការចរចារអំពី IPsec communication



រូបភាព២០-១៥-ការជ្រើសរើសយក connection Security Rule Type

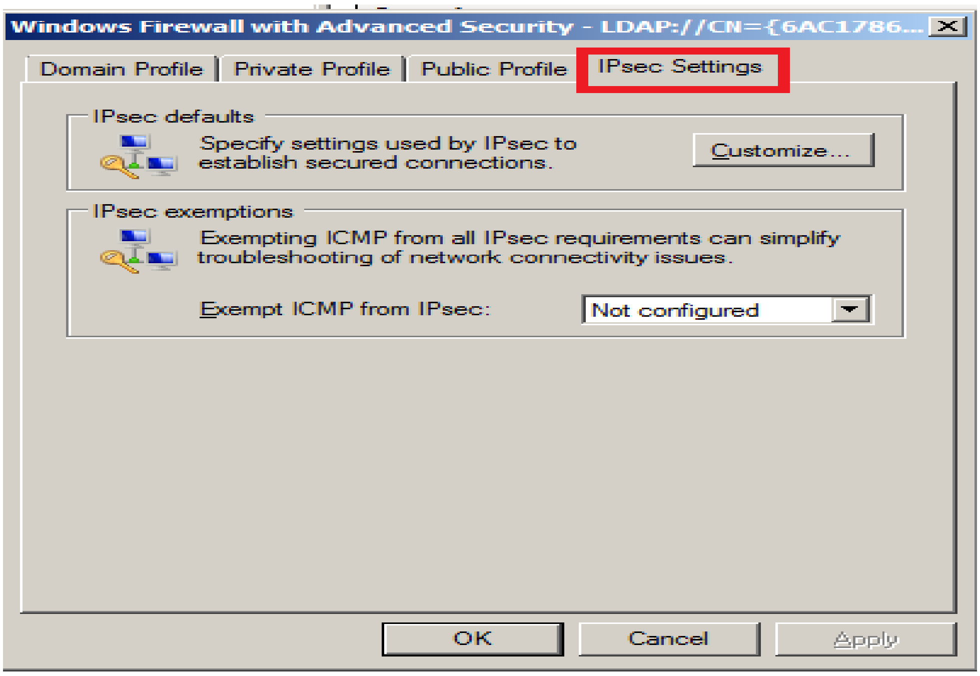
២០-៧-២- Configure IPsec settings សម្រាប់ Connection security Rules

អ្នកអាចកំណត់ពី IPsec settings នៅក្នុង WFAS node នៃ GPO ឬ WFAS console ។ ដើម្បី Access settings ទាំងនេះ ដាដំបូងបើក properties នៃ Windows Firewall with Advaced Security node ដូចក្នុងរូបភាព២០-១៦។



រូបភាព២០-១៦-បើក Windows Firewall Properties

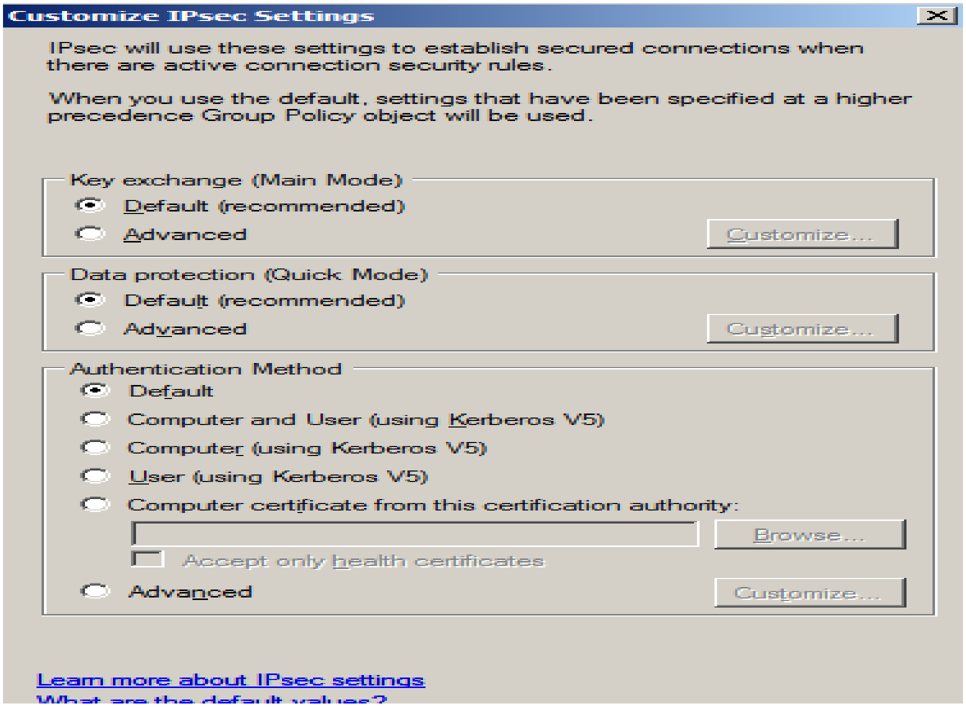
ហើយបន្ទាប់មកនៅក្នុង Properties dialog box បានបង្ហាញឡើង ចុចលើ IPsec settings tab ដូចក្នុងរូបភាពរូបភាព២០-១៧។



រូបភាព២០-១៧-Configuring IPsec settings

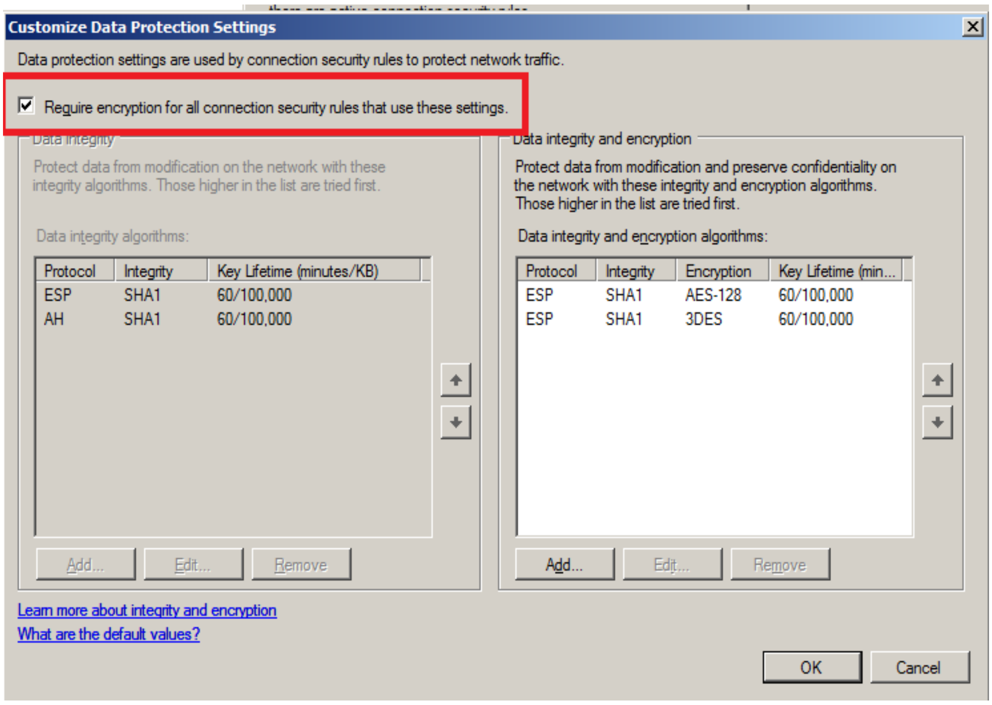
តាមរយៈនៃ tab នេះអ្នកអាច configure IPSec ពីរគឺ

- IPsec defaults
- ICMP exemption ពី IPSec
  - IPSec defaults ចុចលើ Customize button ដើម្បីបើក Customize IPsec Settings ដូចក្នុង



រូបភាព២០-១៨-setting IPSec default

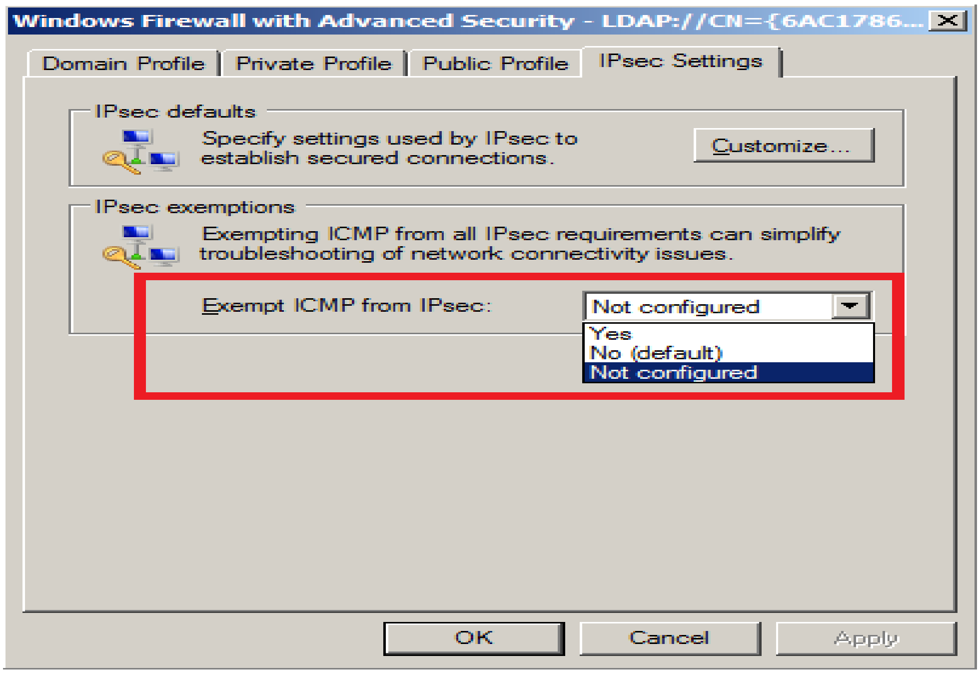
ឧទាហរណ៍ ដើម្បី Configure ការអ៊ិនគ្រីបទៅលើទិន្នន័យសម្រាប់ connection security rule ជាដំបូងជ្រើសរើសយក Advaced នៅក្នុង Data Protection Area ហើយបន្ទាប់មកចុចលើ customize។



រូបភាព២០-១៩-ទាមទារអ៊ិនគ្រីបសម្រាប់ connection security rule

Tick លើប្រអប់ Require Encryption For all Connection security rule ហើយបន្ទាប់មកចុចលើ Ok

- Exempt ICMP from IPSec:ដើម្បីការពារ ICMP (Ping and Tracert) message ពីការ authenticate អ៊ិនគ្រីបឬទាំងពីរ។ ទុក ICMP message មិនការពារអនុញ្ញាតឱ្យអ្នកអាចធ្វើការដោះស្រាយរល់បញ្ហា ដែលជាមូលដ្ឋានគ្រឹះនៅពេលដែល IPSec មិនអាចចរាចរបាន។



រូបភាព២០-២០-ការ Configure Exempt ICMP from IPsec

សង្ខេបមេរៀន

- IPSec អនុញ្ញាតឱ្យអ្នកការពារចរាចរណ៍ network ដោយផ្តល់នូវ data authentication ឬអ៊ិនគ្រីបឬទាំងពីរ។ Security នៅក្នុង IPsec ត្រូវបានផ្តល់ដោយ Protocol ពីរគឺ Authentication Header(AH)និង Encapsulating Security Payload(ESP)។
- នៅក្នុង Windows Server 2008 អ្នកអាចអនុវត្ត IPsec តាមរយៈ IPsec Policies ឬតាមរយៈ Connection security rules
- IPsec តាមលំនាំដើមដំណើរការក្នុង transport mode ដែលផ្តល់ឱ្យនូវសុវត្ថិ end-to-end រវាងកុំព្យូទ័រ។ Transport mode ក៏ត្រូវបានគេប្រើផងដែរក្នុងIPSec ដែលពឹងផ្អែកលើ VPN។ ចំណែកឯ L2PT protocol ត្រូវបានប្រើសម្រាប់បង្កើតផ្លូវរូងនៃ IPsec connection តាមរយៈប្រព័ន្ធ Network សាធារណៈ។

ឯកសារយោង

១- Windows server 2008 Administration by Steve Seguis

២- Windows Server 2008 R2 by Chalie Russel and Craig Zacker with the Window Server team at Microsoft

៣- Publisher: O'Reilly Media, Inc. | ISBN: 0596514115 | edition 2008 | File type: CHM | 492 pages | 13,5 mb