សាកលវិទ្យាល័យ
អាយអាយស៊ី
នៃបច្ចេកវិទ្យា

IIC UNIVERSITY OF TECHNOLOGY

ការសិក្សានៅលើ Firewall

MikroTik Router Board

បង្រៀនដោយសាស្ត្រាចារ្យៈ   ឡា តា

២០១៦ ~ ២០១៧

អារម្ភកថា

ដោយសារតែការរីកចម្រើន ឥតឈប់ឈរនៃវិស័យបច្ចេកវិទ្យា បានអនុញ្ញាតឱ្យកុំព្យូទ័រ ទាំងអស់អាចមានទំនាក់ទំនងជាមួយគ្នាបានតាមរយៈប្រព័ន្ធអ៊ីនធឺណេត។ អ៊ីនធឺណេតបានផ្តល់នូវភាពសម្បូរបែបនៃឯកសារសម្រាប់ ប្រតិបត្តិការងារ ការសិក្សាស្រាវជ្រាវ តន្ត្រី រូបភាព វីដេអូឃ្លីប ហ្គេម សម្រាប់ការកំសាន្តជាដើម។ ស្របពេលដែលមានការប្រើប្រាស់ ដ៏ទូលំទូលាយរបស់ប្រព័ន្ធអ៊ីនធឺណេតនេះ ក៏មានជនខិលខូចមួយចំនួនដែលយើងហៅថា “Hacker” បានឆ្លៀតឱកាសវាយប្រហារអ្នកប្រើប្រាស់ប្រព័ន្ធអ៊ីនធឺណេតទូទាំងពិភពលោក ដែលមានតម្រូវការយកអ៊ីនធឺណេតមកប្រើប្រាស់ជាជំនួយការដល់បញ្ហានៅពេលដែលជួបប្រទះនូវភាពលំបាកអ្វីមួយ។

យើងខ្ញុំសង្ឃឹមថាសៀវភៅនេះ និងផ្តល់នូវសារៈប្រយោជន៍ ឬជាឯកសារសម្រាប់ជាជំនួយដល់និស្សិត មិត្តអ្នកអាន និងសាធារណៈជន បានសិក្សាស្វែងយល់ទៅលើការប្រើប្រាស់ MikroTik វាមានសមត្ថភាពក្នុងការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធឺណេត ចែកចាយទិន្នន័យ ការពារពីការជ្រៀតចូលមកក្នុងប្រព័ន្ធ Network ដោយគ្មានការអនុញ្ញាត បែងចែកល្បឿន Internet ធ្វើ Hotspot ធ្វើ VPN server និងផ្សេងៗជាច្រើនទៀត។

ទោះបីជាយ៉ាងណាក៏ដោយ សៀវភៅនេះនៅមានកម្រិត និងចំណុចខ្វះខាតមួយចំនួនពុំទាន់ត្រឹមត្រូវគ្រប់ជ្រុងជ្រោយនៅឡើយទេ។ យើងខ្ញុំសូមស្វាគមន៍ដោយសេចក្តីសោមនស្សរីករាយចំពោះការផ្តល់នូវយោបល់ និងការរិះគន់ ដើម្បីកែតម្រូវ ពាក្យពេចន៍ ឬឃ្លាប្រយោគណាដែលមានកំហុសឆ្គងក្នុងសៀវភៅនេះ ពីសំណាក់ សាស្ត្រាចារ្យ និស្សិត និងមិត្តអ្នកអាន ដែលបានអានសៀវភៅនេះ ក្នុងន័យស្ថាបនាឱ្យកាន់តែប្រសើរ។

សូមគោរពជូនពរ និងប្រសិទ្ធពរជ័យជូនដល់សាស្ត្រាចារ្យ និស្សិត និងមិត្តអ្នកអានទាំងអស់សូមជួបប្រទះតែសេចក្តីសុខ សេចក្តីចម្រើនគ្រប់ទិវារាត្រី។

គោលបំណងនៃការសិក្សា

គោលបំណងនៃការសិក្សាស្រាវជ្រាវលើ ការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធឺណេតដោយប្រើប្រាស់ MikroTik Router នេះគឺគ្រាន់តែចង់បង្ហាញស្ថានភាពជាក់ស្តែងនៅក្នុងការប្រើប្រាស់ Internet ដែលមិនបានការពារត្រឹមត្រូវ។ ការរៀបចំសៀវភៅនេះក្នុងគោលបំណងដើម្បីឆ្លុះបញ្ចាំងពីចំណេះដឹងទិដ្ឋភាពជាក់ស្តែងនៃការគ្រប់គ្រងទៅលើប្រព័ន្ធ Internet របស់លោកអ្នកឱ្យមានភាពប្រសើរឡើង។ ស្ថិតក្នុងអត្ថន័យនេះដែរយើងនឹងសិក្សាផ្អែកទៅលើគោលបំណងមានដូចជា÷

- អត្ថប្រយោជន៍របស់ MikroTik Router
- ការដំឡើង DHCP
- ការបង្កើត Users សម្រាប់ Login
- ការដំឡើង DNS Server
- ការដំឡើង Hotspot
- សិក្សាលើការកំណត់ល្បឿនអ៊ីនធឺណេត Control Bandwidth
- កំណត់ Advance Proxy និង Url-Filter ចំពោះបុគ្គលិក
- Block ឈ្មោះ Website មួយចំនួនដែលយើងមិនអនុញ្ញាតឱ្យប្រើប្រាស់។

មាតិកា

អារម្ភកថា.. i

គោលបំណងនៃការសិក្សា...ii

មេរៀនទី ១

ណែនាំឱ្យស្គាល់ពី Network

១.១ តើអ្វីជា Computer Network? 1

១.១.១ ការដំឡើងប្រព័ន្ធ Network ---2

១.១.២ LAN (Local Area Network) --3

១.១.៣ MAN (Metropolitan Area Network) --3

១.១.៤ WAN (Wide Area Network) --4

១.២ លក្ខណៈនៃការគ្រប់គ្រងប្រព័ន្ធ Network 5

១.២.១ លក្ខណៈ Peer-to-Peer Network---5

១.២.២ លក្ខណៈ Server-Based Network ---6

១.៣ សកម្មភាពដំណើរការរបស់ Network 8

១.៣.១ អត្ថប្រយោជន៍បណ្តាញណែតវើក---9

១.៣.២ គុណវិបត្តិបណ្តាញណោតវើក--- 10

១.៤ Internet... 11

១.៥ TCP/IP 12

១.៦ IP Address 12

១.៧ ស្តង់ដាររបស់ Network 14

១.៧.១ OSI Model--- 14

១.៧.២ មុខងាររបស់ស្រទាប់ Layers --- 14

១.៨ Router.. 17

១.៩ Gateway 18

១.១0 Network Interface Card (NIC) 18

១.១១ Modem 19

មេរៀនទី ២

ណែនាំឱ្យស្គាល់ពី Firewall

២.១ តើអ្វីជា Firewall?.. 21

២.២ ស្គាល់ពី Firewall.. 22

២.២.១ Software Firewalls-- 23

២.២.២ Hardware Firewalls-- 24

មេរៀនទី ៣

ការចាប់ផ្តើមធ្វើឱ្យ MikroTik ស្គាល់ Internet

៣.១ តើ Mikortik Router អាធ្វើអ្វីបានខ្លះ?.. 30

៣.២ របៀប Login នៅលើ MikroTik Router 30

៣.៣ របៀប Configure Internet នៅលើ MikroTik Router.. 32

មេរៀនទី ៤

ការដំឡើង Service មួយចំនួនលើ MikroTik

៤.១ បង្កើត Bride 37

៤.២ របៀប Setup DHCP Server នៅលើ MikroTik Router.. 38

៤.៣ របៀបបង្កើត HostSport នៅលើ LAN.. 41

៤.៤ របៀបបង្កើត Host Sport លើ Wireless 47

មេរៀនទី ៥

កំណត់ដំណើរការមួយឆ្លងកាត់ MikroTik

៥.១ របៀប Block Website នៅលើ Layer 7 49

៥.២ ការកំណត់ល្បឿនសម្រាប់ដំណើរការនៅលើ Websites 51

៥.៣ របៀប Blocked Host Device 53

៥.៣.១ Blocked តាមរយៈ Mac Address -------- 54

៥.៣.២ Blocked តាមរយៈ IP Address -------- 55

៥.៤ របៀប Setup Web Proxy 56

៥.៥ Block Website តាមរយៈ Web Proxy 66

មេរៀនទី ១

ណែនាំឱ្យស្គាល់ពី Network

១.១ តើអ្វីជា Computer Network?

បណ្តាញកុំព្យូទ័រ (Computer Network) គឺជាក្រុមនៃប្រព័ន្ធកុំព្យូទ័រដែលបានភ្ជាប់ជាមួយគ្នា ក្នុងគោលបំណងទំនាក់ទំនងគ្នាទៅវិញទៅមក ដើម្បីចែករំលែក ផ្លាស់ប្តូរធនធានសម្រាប់អ្នកប្រើប្រាស់ដ៏ច្រើន តាមរយៈឧបករណ៍តភ្ជាប់ ដូចជាខ្សែ (Hardware) ខ្សែកាបអុិបទិក (Optic cable) អុីនហ្វ្រារ៉េដ (Infra-Red សម្រាប់រយៈចម្ងាយជិត) ឬជា Wireless សម្រាប់រយៈចម្ងាយជិត ឬក៏ឆ្ងាយ រលកវិទ្យុ (Radio waves) ផ្កាយរណប (Satellites)។ បណ្តាញកុំព្យូទ័រមានច្រើនប្រភេទទៅតាមលក្ខណៈដែលបានកំណត់នីមួយៗ។

រូបភាពទី ១.១ Computer Network

បន្ទាប់ពីយើងបានភ្ជាប់ម៉ាស៊ីនកុំព្យូទ័រទាំងអស់ឱ្យស្គាល់គ្នារួចហើយ ពេលនេះយើងបានបណ្តាញកុំព្យូទ័រ (Computer Network) ដែលអនុញ្ញាតឱ្យយើងប្រើប្រាស់នូវប្រភពធនធានរួមគ្នាបានក្នុងពេលតែមួយ ឬពេលខុសគ្នា។ ឧទាហរណ៍ ដូចជាម៉ាស៊ីនបោះពុម្ភដែលស្ថិតនៅក្នុងបណ្តាញតែមួយ អាចអនុញ្ញាតឱ្យអ្នកប្រើកុំព្យូទ័រផ្សេងគ្នា អាចបោះពុម្ពឯកសារដោយផ្ទាល់បានដោយពុំចាំបាច់ពឹងលើម៉ាស៊ីនណាមួយឡើយ។ Network ត្រូវបានគេចែកជាបីប្រភេទធំៗគឺៈ LANs, MANs, និង WANs។

១.១.១ ការដំឡើងប្រព័ន្ធ Network

ក្រោយពីទទួលបាន ការពន្យល់ណែនាំជាច្រើនពីសំណាក់លោកគ្រូសាស្ត្រាចារ្យណែនាំនៃសាកលវិទ្យាល័យអាយអាយស៊ីនៃបច្ចេកវិទ្យា ផ្នែកវិទ្យាសាស្ត្រកុំព្យូទ័រ ព្រមជាមួយការខិតខំសិក្សាស្រាវជ្រាវឯកសារផ្សេងៗ ទៀតតាមរយៈ ការធ្វើបទសម្ភាសន៍ សៀវភៅ និងប្រព័ន្ធ Internet នោះ ធ្វើឱ្យយើងខ្ញុំមានការយល់ដឹងកាន់តែច្បាស់ អំពីគុណវិបត្តិ និងគុណសម្បត្តិរបស់ប្រព័ន្ធ Network ទ្រឹស្តី និងនិយមន័យទាំងឡាយ ដែលទាក់ទងនឹងប្រព័ន្ធ Network ដែលមានការរៀបរាប់ខាងក្រោម÷

✓ **គុណសម្បត្តិនៃប្រព័ន្ធ** Network

Computer Network អាចផ្តល់អត្ថប្រយោជន៍ដូចជា÷

- ធ្វើឱ្យ Computer ទាំងអស់ដែលស្ថិតនៅកន្លែងផ្សេងៗគ្នាអាចទំនាក់ទំនងគ្នាបាន
- ធ្វើឱ្យចំណេញពេលវេលាជាច្រើនក្នុងការបញ្ជូនព័ត៌មាន ព្រោះវាមានល្បឿនលឿនជាងការបញ្ជូនដោយដៃ
- អាច Share Files ឬ Data ទៅកាន់ Computer ផ្សេងៗទៀត ដែលស្ថិតនៅក្នុងប្រព័ន្ធ Network ជាមួយគ្នាបាន
- មានសុវត្ថិភាពខ្ពស់ និងមានភាពងាយស្រួលក្នុងការគ្រប់គ្រងទិន្នន័យ
- បង្កើតគ្រប់គ្រងឱ្យមានភាពងាយស្រួលទៅលើប្រព័ន្ធ ដោយវាគ្រប់គ្រងជាលក្ខណៈ Centralizing Administration
- អាចធ្វើឱ្យ Different System ធ្វើការជាមួយគ្នាបាន។

× **គុណវិបត្តិនៃប្រព័ន្ធ** Network

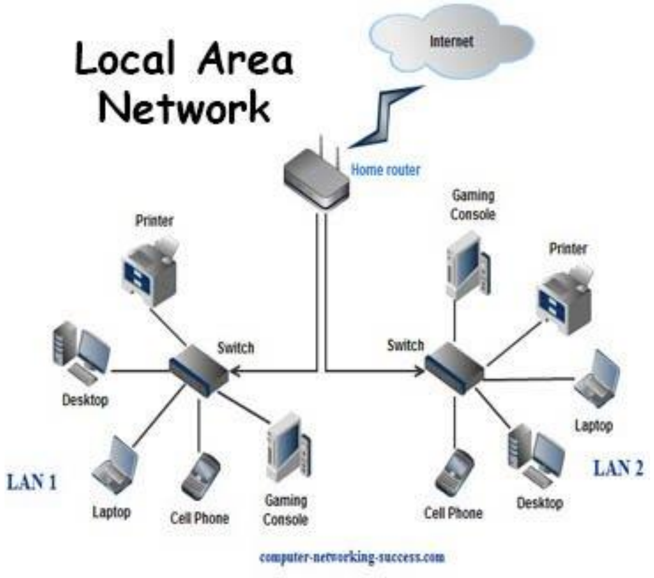
ទោះយ៉ាងណាក្តី ប្រព័ន្ធ Network ផ្តល់នូវផលប្រយោជន៍ជាច្រើនក៏ពិតមែន ប៉ុន្តែវាក៏នៅមានចំណុចមួយចំនួនគួរឱ្យយកមកពិចារណាផងដែរ ដូចជា÷

- ត្រូវការទិញឧបករណ៍ជាច្រើន ដែលមានតម្លៃថ្លៃ (Hardware & Software) និងត្រូវចំណាយថវិកាដើម្បី Maintenance
- ត្រូវមានការការពារខ្ពស់ចំពោះបញ្ហាសុវត្ថិភាព ព្រោះអាចមានអ្នកបន្លំ ឬកែប្រែឯកសាររបស់យើងតាមរយៈប្រព័ន្ធ Network នេះបានផងដែរ ដែលគេហៅពួកនោះថា Hacker

ការដំឡើងមានការលំបាក ជាពិសេសនៅពេលដែលចង់ឱ្យ Different System អាចធ្វើការជាមួយគ្នាបាន។

១.១.២ LAN (Local Area Network)

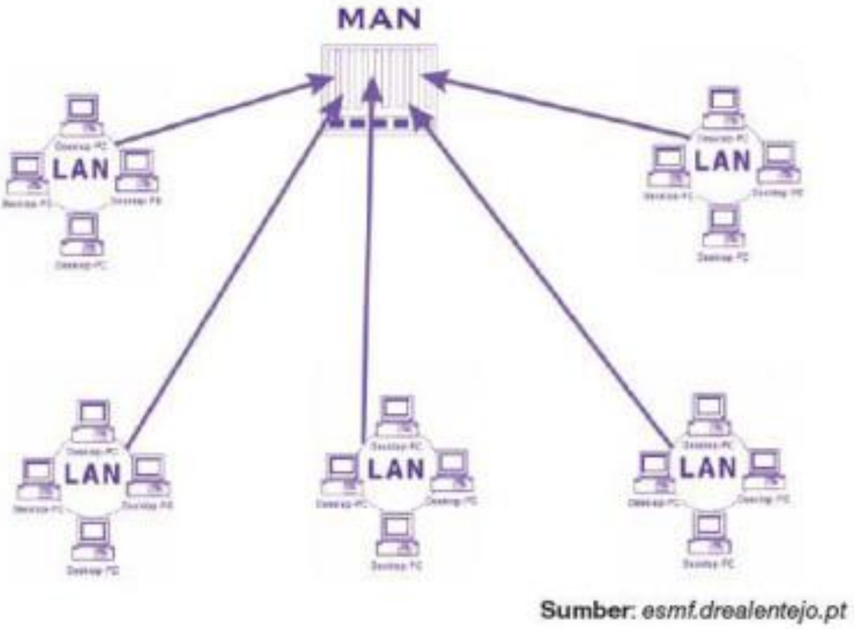
កាលពីដំបូងគេតភ្ជាប់ម៉ាស៊ីនពីរជាមួយការប្រើប្រាស់ខ្សែកាប ដើម្បីងាយស្រួលក្នុងការផ្លាស់ប្តូរព័ត៌មានគ្នាបានប៉ុណ្ណោះ។ ក្រោយមកទៀតប្រហែល ១០ ម៉ាស៊ីន ភ្ជាប់ជាមួយគ្នា និងជាមួយម៉ាស៊ីន Printer មួយ។ រហូតមកដល់ក្នុងចន្លោះឆ្នាំ ១៩៨០ ចំនួនម៉ាស៊ីនកើនឡើងដល់ ៣០ ម៉ាស៊ីនជាមួយចម្ងាយឆ្ងាយបំផុតគឺ ១៨០ម៉ែត្រ។ ដូចនេះតែងតែសមស្របជាមួយអគារ ឬបរិវេននៃអគារក្រុមហ៊ុនតូចៗ...។ ក្នុងពេលបច្ចុប្បន្ននេះជាមួយនឹងក្រុមហ៊ុនប្រព័ន្ធ Network ដូចនោះគឺជាការសមស្របបំផុត។ ប្រព័ន្ធ Network ភ្ជាប់ដោយសារ ខ្សែកាប ត្រូវបានកំណត់ព្រំដែននៃផ្ទៃដីតូច ដូចបានលើកឡើងខាងលើគេហៅថា Local Area Network (LAN)។



រូបភាពទី ១. ២ LAN (Local Area Network)

១.១.៣ MAN (Metropolitan Area Network)

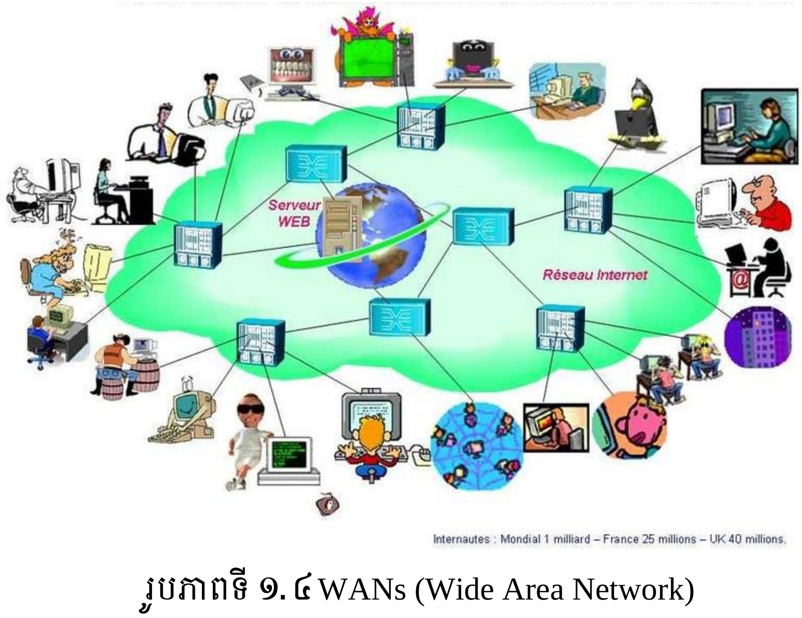
ជាប្រព័ន្ធ Network ដែលមានទំហំភូមិសាស្រ្តក្នុងតំបន់មួយ ឬទីក្រុងមួយ។ គេប្រើប្រាស់ MAN សម្រាប់ភ្ជាប់ LAN នឹង LAN តាមប្រព័ន្ធ Data Communication ពិសេសដែលមានល្បឿនខ្ពស់ជាង FDDI ជាដើម។



រូបភាពទី ១.៣ MANs (Metropolitan Area Network)

១.១.៤ WAN (Wide Area Network)

WAN គឺជាប្រព័ន្ធ Network ដែលមានទំហំភូមិសាស្ត្ររវាង ខេត្តនឹងខេត្ត ទីក្រុងនឹងទីក្រុង ឬ ប្រទេសនឹងប្រទេស។ លក្ខណៈរបស់ WAN គឺប្រើប្រព័ន្ធទូរគមនាគមន៍ ដែលការផ្សំនៃ LAN Network រួមជាមួយផ្នែកផ្សេងទៀត ដែលបានភ្ជាប់ឡើងជាមួយគ្នាដោយលក្ខណៈជា WAN។ ការភ្ជាប់ WAN រួមមាន Fiber Optic ផ្លូវបញ្ជូលផ្កាយរណប VI-BA (micro-view) ឬ PC client (Remote client) ទៅនឹង LAN។



រូបភាពទី ១.៤ WANs (Wide Area Network)

១.២ លក្ខណៈនៃការគ្រប់គ្រងប្រព័ន្ធ Network

លក្ខណៈរបស់ Network ត្រូវបានគេរចនាឡើង សម្រាប់ឱ្យកុំព្យូទ័រទាំងអស់អាចទំនាក់ទំនងគ្នាបានដោយឆ្លងកាត់ប្រព័ន្ធ Network តែមួយ ហើយលក្ខណៈរបស់ Network ត្រូវបានគេបែងចែកជា២ ដូចបានរៀបរាប់ខាងក្រោមនេះ។

១.២.១ លក្ខណៈ Peer-to-Peer Network

ប្រព័ន្ធ Network មានលក្ខណៈជា Local ដោយបណ្ដាសមាជិកនៅក្នុងប្រព័ន្ធ Network មានសិទ្ធិស្មើៗគ្នានៅក្នុងការ Share file, Folder, Printer, Scanner, CD/R។ ជាធម្មតាអ្នកណាក៏អាចមានសិទ្ធិដើម្បីគ្រប់គ្រង (Administration) ទៅលើប្រព័ន្ធ Network បានដែរ ព្រោះវាឥតមាន Server ឬ Client ច្បាស់លាស់។ ពេលវាដើរតួនាទីជា Client គឺនៅពេលដែលវាស្នើរ File។

✓ **គុណសម្បត្តិរបស់** Peer-to-Peer Network

ទោះបីជា Peer-to-Peer Network មានលក្ខណៈខ្វះខាតត្រង់ចំណុចសុវត្ថិភាព (Security) ក៏ដោយ ប៉ុន្តែអាចសមល្មមសម្រាប់ LAN ធម្មតាមួយ ចំពោះការិយាល័យផ្ដល់នូវ Share Resources និង Share Device សម្រាប់ Users រួមគ្នាប្រើបាន។ លើសពីនេះទៅទៀត ភាពប្រសើររបស់ Peer-to-Peer Network:

- មិនចំណាយពេលច្រើន ទៅលើការរៀបចំ
- មិនចាំបាច់ប្រើប្រាស់ ឬមានម៉ាស៊ីនមេដែលបើកពេញម៉ោង
- ងាយស្រួលដំឡើង និងងាយស្រួល Configure
- កុំព្យូទ័រនីមួយៗ មានលក្ខណៈឯករាជ្យ
- ងាយស្រួលត្រួតពិនិត្យ និងមានតម្លៃថោកសមរម្យ
- មិនពិបាកសម្រាប់គ្រប់គ្រង។

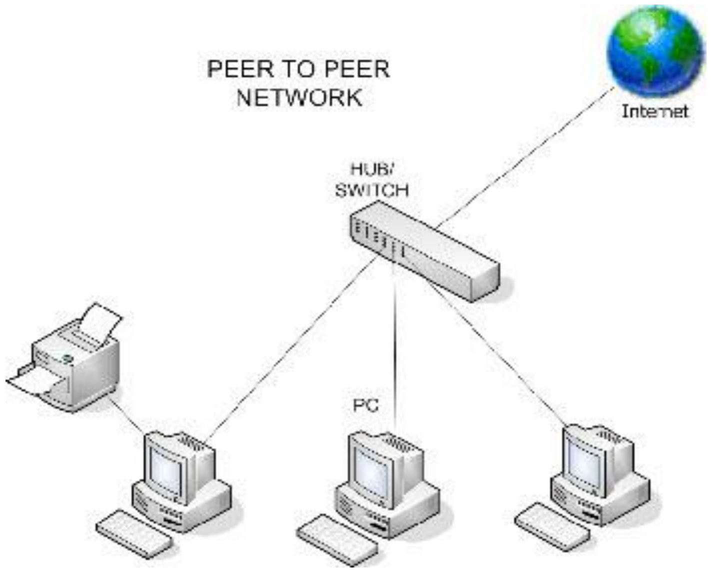
× **គុណវិបត្តិរបស់** Peer-to-Peer Network

រាល់កម្រោង ឬកម្មវិធីដែលបង្កើតឡើងមកតែងតែមានផលល្អ និងផលអាក្រក់ ហេតុនេះ ក្រៅពីមានគុណសម្បត្តិរបស់ Peer-to-Peer Network ក៏មានគុណវិបត្តិផងដែរដូចជា:

- គ្មានសុវត្ថិភាព (Security) នៅក្នុងបណ្ដាញណេតវើក

- កុំព្យូទ័រនីមួយៗត្រូវចំណាយពេល Back up data និងថែទាំរៀងៗខ្លួន
- រាល់ឯកសារដែលបានបាត់បង់ ពិបាកសម្រាប់ទាញយកមកវិញ
- នៅពេលប្រើប្រាស់កុំព្យូទ័រច្រើនគ្រឿង(លើសពីដប់ឡើងទៅ) មានការបង្កើននូវបញ្ហាច្រើន
- ការគ្រប់គ្រងរួមគ្នា ដើម្បីពិនិត្យការ Access ទៅកាន់ទិន្នន័យ (Data)

➢ **សម្គាល់:** ចំពោះ Windows បើចង់ប្រើជាលក្ខណៈ Peer-to-Peer នោះគឺគ្រាន់តែកំណត់ម៉ាស៊ីន Workstation ជា Stand alone ពុំមែនជា Domain Controller នោះឡើយ។



រូបភាពទី ១.៥ Peer to Peer Network

១.២.២ លក្ខណៈ Server-Based Network

Server-Based Network ជាប្រព័ន្ធណេតវើកដែលមានម៉ាស៊ីនមេ (Server) ជាអ្នកគ្រប់គ្រងប្រព័ន្ធណេតវើកទាំងមូល និងផ្តល់នូវសេវាកម្ម (Service) ទៅដល់អ្នកប្រើប្រាស់ (User) ទាំងអស់ ហើយម៉ាស៊ីនកូនទាំងនោះជាអ្នកប្រើប្រាស់ធនធាន (Resources) ដែលផ្តល់ដោយម៉ាស៊ីនមេ និងបញ្ចូលធនធាន (Resources) ទាំងនោះទៅឱ្យម៉ាស៊ីនមេជាអ្នកផ្ទុក និងជាអ្នកកំណត់សិទ្ធិក្នុងការប្រើប្រាស់កម្មវិធី ព្រមទាំងទិន្នន័យផ្សេងៗរបស់ម៉ាស៊ីនកូននៅលើណេតវើក។ លក្ខណៈពិសេសរបស់ Server-Based Network គឺសុវត្ថិភាព (Security) របស់ប្រព័ន្ធណេតវើកដែលទាក់ទងទៅនិងសិទ្ធិប្រើប្រាស់:

- ប្រើប្រាស់ណេតវើក តាមពេលវេលា
- ប្រើប្រាស់ធនធាន (Resources) និងសេវាកម្ម (Service)

- គ្រប់គ្រង Hardware, resource, printer, hard disk
- ងាយស្រួលក្នុងការគ្រប់គ្រងទិន្នន័យ (Data)…។

NOS (Network Operation System) ដែលគេនិយមប្រើគឺៈ Novell Netware, Microsoft NT Server, OS/2 LAN Server, Banyan Vines V6.0, Windows Server, Linux…។

✓ **គុណសម្បត្តិរបស់ Server-Based Network**

ទោះបីជាការដំឡើង (Installation), ការរៀបចំ (Configure) និងការគ្រប់គ្រង (Management) Server-Based Network មានលក្ខណៈស្មុគស្មាញជាង Peer-to-Peer Network ក៏ដោយ វាមានគុណសម្បត្តិច្រើនជាង Peer-to-Peer Network ដូចជាៈ

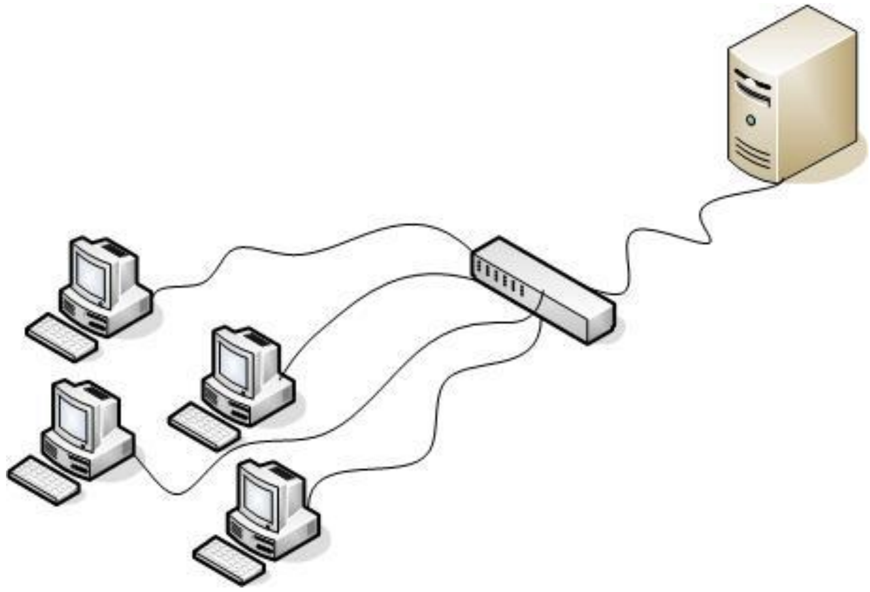
- ណេតវើកមានលក្ខណៈធំទូលាយ អ្នកប្រើប្រាស់អាចចាប់ពី ១០នាក់ឡើងទៅ
- ងាយស្រួលគ្រប់គ្រងពេលមានបញ្ហា
- អ្នកប្រើប្រាស់អាចប្រើធនធានបានទាំងអស់ ដែលមាននៅលើម៉ាស៊ីនមេទៅតាមសិទ្ធិរៀងៗខ្លួន
- ណេតវើកមានសុវត្ថិភាពខ្ពស់ ព្រោះនៅពេលអ្នកប្រើប្រាស់ Login ត្រូវតែវាយ Username និង Password
- អាចគ្រប់គ្រងម៉ាស៊ីនមេពីចំងាយបាន
- ងាយស្រួលក្នុងការ Backup ទិន្នន័យរបស់អ្នកប្រើប្រាស់
- ងាយស្រួលក្នុងការគ្រប់គ្រង User account និង Access control។

× **គុណវិបត្តិរបស់ Server-Based Network**

យើងឃើញថា Server-Based Network មានគុណសម្បត្តិច្រើន តែក៏មានគុណវិបត្តិរបស់វាដែរដូចជាៈ

- មានផលអាក្រក់នៅពេលដែលម៉ាស៊ីនមេមិនដំណើរការ វានាំឱ្យណេតវើកទាំងមូលឈប់ដំណើរការ និងនាំឱ្យមានការបាត់បង់នូវធនធានរបស់ណេតវើកផ្សេងទៀត

- ការរៀបចំ (Configuration) មានលក្ខណៈស្មុគស្មាញ ត្រូវការអ្នកដែលមានចំណេះដឹងផ្នែក Computer Network
- ចំណាយថវិកាច្រើនទៅលើម៉ាស៊ីនមេ ត្រូវការផ្នែករឹង (Hardware) និងផ្នែកទន់ (Software) ដែលមានគុណភាព។



រូបភាពទី ១.៦ **Server-Based Network**

១.៣ សកម្មភាពដំណើរការរបស់ Network

សកម្មភាពដំណើរការរបស់ណេតវើក គឺជាដំណើរក្នុងប្រព័ន្ធណេតវើកដែលត្រូវការប្រើប្រាស់ និងចែកចាយប្រភពធនធាននៅលើបណ្តាញនោះ។ បណ្តាម៉ាស៊ីនកូនទាំងអស់មានលទ្ធភាពប្រើប្រាស់នូវធនធានរួមបានក្នុងករណីដែលគេផ្តល់សិទ្ធិដល់ម៉ាស៊ីនកូនទាំងនោះ។ ម៉ាស៊ីនកូនមានលទ្ធភាពរក្សាទុកនូវឯកសាររួមគ្នាបាន ថែមទាំងប្រើប្រាស់ផ្នែករឹង (Hardware) រួមគ្នាបានទៀតផង ដូចជា Hard disk, Printer ជាដើម។ ក្នុងទីនេះសូមលើកយកពីសមាសភាគទាំងប្រាំរបស់ Data Communication មកបង្ហាញដើម្បីបញ្ជាក់អំពីសកម្មភាពដំណើរការណេតវើកក្នុងការចែកចាយទិន្នន័យក្នុងបណ្តាញដូចតទៅ។

Message: គឺជាទិន្នន័យ (Data) ដែលត្រូវធ្វើការទំនាក់ទំនងគ្នា (ទិន្នន័យដែលចរាចរសម្រាប់ការចែករំលែកក្នុងបណ្តាញនោះ) ។ ទិន្នន័យ (Data) នេះអាចជាអក្សរ ជាលេខ ជារូបភាពជាសម្លេង និងជាវីដេអូជាដើម។

Sender : គឺជាឧបករណ៍ដែលផ្ញើនូវទិន្នន័យ (Data Message) ដែលវាអាចជា Computer, Workstation, Telephone, Handset, Video camera, និងផ្សេងទៀត។

Receiver: ជាឧបករណ៍ដែលទទួលទិន្នន័យ។ Receiver នេះអាចជា Computer, Handset, Workstation, Telephone, Television, និងផ្សេងទៀត។

Medium: គឺជាផ្លូវចរាចររបស់ Data Message ចេញពី Sender ទៅកាន់ ReceiverMedium នេះអាចជា:

- Guided media ដែលមានដូចជា Twisted-pair, coaxial និង fiber-optic cable
- Unguided media ដែលមានដូចជា Radio waves, microwave និង infrared

Protocol: គឺជាបណ្តុំច្បាប់ទាំងឡាយ ដែលគ្រប់គ្រងការទំនាក់ទំនងគ្នារបស់ទិន្នន័យ។ វាជាអ្នកសម្របសម្រួលធ្វើឱ្យស្គាល់គ្នារវាងឧបករណ៍ ដែលត្រូវមានការទំនាក់ទំនងគ្នា។ បើគ្មាន Protocol ទេ ឧបករណ៍ទាំងនោះពុំអាចទំនាក់ទំនងគ្នាបានឡើយ។ ប្រៀបដូចជាមនុស្សម្នាក់ចេះតែភាសាបារាំងស្តាប់មិនយល់មនុស្សម្នាក់ផ្សេងទៀតដែលនិយាយភាសាជប៉ុន។

១.៣.១ អត្ថប្រយោជន៍បណ្តាញណែតវើក

បណ្តាញណេតវើកបានផ្តល់អត្ថប្រយោជន៍ជាច្រើនដល់អ្នកប្រើប្រាស់ដូចជា ÷

File Sharing: ប្រព័ន្ធណេតវើកអនុញ្ញាតឱ្យរាល់បណ្តាម៉ាស៊ីនទាំងអស់នៅក្នុងបណ្តាញអាចមានសិទ្ធិចែកចាយនូវឯកសារ ដល់គ្នាបានយ៉ាងលឿន និងឆាប់រហ័សហើយយើងអាចប្រើប្រាស់វាជំនួស Diskette ឬ USB Flash ដើម្បីថតចម្លង និងយកឯកសារពីកុំព្យូទ័រមួយទៅកុំព្យូទ័រមួយទៀតឬពីការិយាល័យមួយទៅដាក់ការិយាល័យមួយផ្សេងទៀតដោយងាយស្រួល។ ក្នុងការចែកចាយឯកសារជា File នេះមានពីរប្រភេទគឺ:

- វិធីទីមួយ: រាល់សមាជិកទាំងអស់អាចចែកចាយនូវឯកសារដោយផ្ទាល់ គឺមានន័យថាគ្រប់ម៉ាស៊ីនក្នុងបណ្តាញនោះ អាចផ្ទុកឯកសារក្នុងម៉ាស៊ីនខ្លួនឯងហើយឱ្យម៉ាស៊ីនផ្សេងទៀតចូលមកយកដោយផ្ទាល់តែម្តង (វិធីទី១នេះគឺជា Peer-to-Peer Network)។

- វិធីទីពីរៈ រាល់សមាជិកទាំងអស់ បើចង់ចែកចាយឯកសារ ត្រូវយកឯកសារនោះទៅផ្ទុកក្នុងម៉ាស៊ីនរួមមួយដែលហៅថាម៉ាស៊ីនមេ (Server) បន្ទាប់មកទើបម៉ាស៊ីនផ្សេងទៀតអាចចូលទៅយកពីម៉ាស៊ីនមេនោះមកប្រើបាន (វិធីទី២នេះ គឺជា Server-Based Network)។

Resource Sharing: ក្នុងបណ្តាញណេតវើកក៏អាចប្រើប្រាស់នូវផ្នែករឹង (Hardware) មួយចំនួនរួមគ្នាបានដែរ ដូចជាការផ្តល់សិទ្ធិឱ្យប្រើប្រាស់នូវ Hard disk, Printer, Scanner និង CD ROM ជាដើម តែវាក៏អាស្រ័យទៅលើបណ្តាញណេតវើកនោះដែរ។

Program Sharing: បណ្តាញណេតវើកមានលទ្ធភាពអាចចែកចាយនូវកម្មវិធីដើម្បីប្រើប្រាស់រួមគ្នាបាន ដោយយកកម្មវិធីទាំងនោះទៅក្នុង Hard disk រួម។ វាជួយកាត់បន្ថយការចំណាយថវិកាទៅលើការទិញ Hardware, Software និង Licensed Copy ដោយយើងមានចាំបាច់ដំឡើងវានៅលើរាល់កុំព្យូទ័រ Clients នោះទេ។

Security: ចំពោះ File និង Directory ដែលបានចែករំលែកនៅលើបណ្តាញណេតវើក គឺត្រូវបានដាក់លេខសម្ងាត់ (Password) និងកំណត់សិទ្ធិលើអ្នកប្រើប្រាស់ ក្នុងការទាញយកឯកសារមកប្រើប្រាស់បានយ៉ាងល្អ។

Communication: ទោះបីជាណេតវើករបស់យើងមិនទាន់បានតភ្ជាប់នូវ Internet ក៏ដោយក៏កុំព្យូទ័រទាំងអស់នៅលើបណ្តាញណេតវើក អាចធ្វើការទំនាក់ទំនងគ្នាបានល្អនៅលើប្រព័ន្ធនោះដែរ។

Flexible Access: អ្នកប្រើប្រាស់អាចយក Files ពីកុំព្យូទ័រណាមួយក៏បាន ដែលឋិតនៅលើណេតវើក។ ហើយថែមទាំងអនុញ្ញាតឱ្យអ្នកប្រើប្រាស់ អាចប្រើប្រាស់កុំព្យូទ័រណាក៏បានដែលស្ថិតនៅលើណេតវើកដើម្បីធ្វើការងារ។

១.៣.២ គុណវិបត្តិបណ្តាញណេតវើក

ទោះបីបណ្តាញណេតវើក បានផ្តល់ប្រយោជន៍ជាច្រើនក៏ដោយ ក៏វានៅតែជួបប្រទះគុណវិបត្តិមួយចំនួនដូចខាងក្រោម÷

- Virus Attachment: មេរោគកុំព្យូទ័រអាចឆ្លងរាលដាលពីកុំព្យូទ័រមួយទៅកុំព្យូទ័រមួយទៀតនៅពេលដែលអ្នកប្រើប្រាស់ថតចម្លងយកឯកសារពីកុំព្យូទ័រដទៃនៅលើណេតវើក
- ចំណាយថវិកាច្រើនក្នុងការដំឡើងប្រសិនបើមានម៉ាស៊ីនមេ

- បើម៉ាស៊ីនមេមានបញ្ហា ឬមិនទាន់បើក ម៉ាស៊ីនកូនមិនអាចដំណើរការទិន្នន័យប្រើប្រាស់បានទេ ចំពោះណេតវើកប្រើជា Server-Based Network
- ក្នុងណេតវើកមួយបើមានកុំព្យូទ័រតិច ប្រតិបត្តិការការងាររបស់វាលឿន តែបើមានកុំព្យូទ័រច្រើន វានឹងធ្វើឱ្យការប្រតិបត្តិការការងារយឺត
- មានប្រភេទផ្នែករឹង (Hardware) ខ្លះមិនធ្វើការទំនាក់ទំនងដើម្បីធ្វើការជាមួយគ្នាបាន។

១.៤ Internet

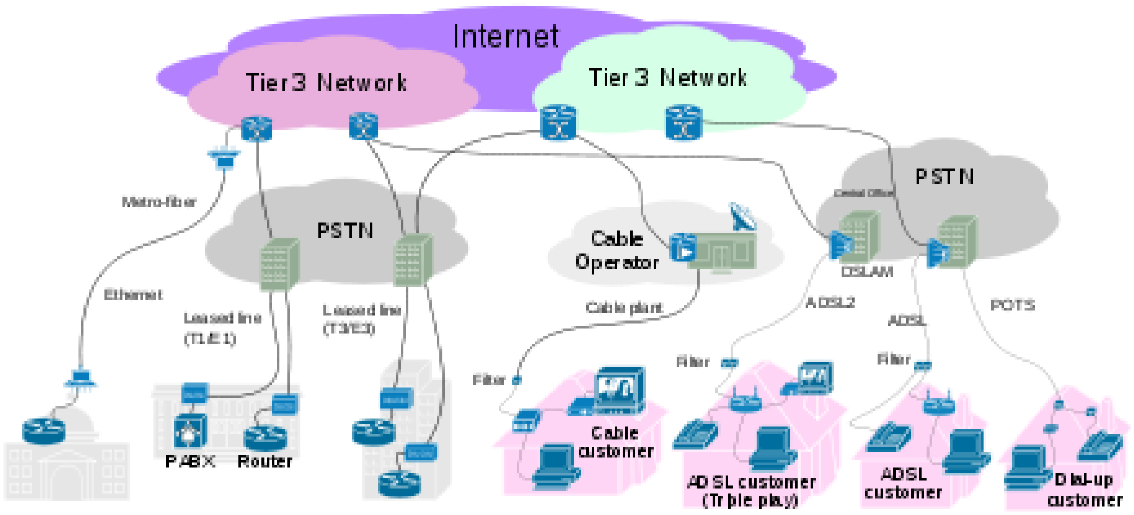
នាពេលបច្ចុប្បន្ន Internet ត្រូវទទួលស្គាល់ថា ជាប្រភពដើមពី ទំនាក់ទំនងរវាងប្រព័ន្ធ Network (Computer Communication Network) និងបណ្តាសេវាកម្ម (Service) ដែលជាប្រព័ន្ធ WAN ភ្ជាប់ LAN ឬ LAN ទូទាំងពិភពលោក។ Internet បង្កើតឡើង គឺសម្រាប់ផ្លាស់ប្តូរព័ត៌មាន នៅលើពិភពលោកតាមរយៈសេវាកម្ម។

- WWW (World Wide Web)
- FTP (File Transfer Protocol), Gopher
- Telnet ភ្ជាប់ពី Terminal ទៅ Host (VIP: Virtual)
- E-mail (Website ទាក់ទងតាមរយៈ Link Page)

➢ **សម្គាល់ ÷** Internet គឺជាប្រព័ន្ធ Network នៅខាងក្នុងរបស់ក្រុមហ៊ុន ឬអង្គការ។ ពួកវាប្រើបច្ចេកទេស Internet service។

ឧទាហរណ៍ៈ HTTP Service និង Service Web Browser Internet ជា LAN ដែលប្រើ Internet Service ប៉ុន្តែមិនចាំបាច់ភ្ជាប់ទៅ Internet។

Internet គឺជាប្រព័ន្ធ Network ស្ថិតនៅខាងក្រៅរបស់ក្រុមហ៊ុន ឬអង្គការ។ វាប្រើ Internet technology។ ឧទារហណ៍ៈ HTTP Service និង Service Web browser។ ដូចនេះ Internet មានន័យថាគឺជាប្រព័ន្ធ Network TCP/IP មួយដែលប្រើ Technology របស់ Internet ប៉ុន្តែវាភ្ជាប់ទៅ Internet។



រូបភាពទី ១.៧ Internet

១.៥ TCP/IP

TCP (Transmission Control Protocol) គឺជាសំណុំនៃ Protocols ដែលបង្ហាញពីរបៀបផ្លាស់ប្តូរ និងទិន្នន័យ។ គេពេញនិយមប្រើលើ Local Network, Intranet និង Internet ដែលបានបង្កើតឡើងនៅឆ្នាំ ១៩៧០ ដោយក្រសួងការពារជាតិ របស់សហរដ្ឋអាមេរិកសម្រាប់ប្រើលើ Network ពិសោធន៍មួយឈ្មោះ APANET (Advance Project Agency Network) ដើម្បី Transfer File បន្ទាប់មក TCP/IP ត្រូវបានបើកសម្រាប់ភ្ជាប់ Local Network របស់វិទ្យាស្ថានស្រាវជ្រាវដែលក្រោយមកទៀតក៏បាន ភ្ជាប់ជាមួយ Local Network របស់វិទ្យាស្ថានដ៏ទៃទៀត ជាបន្តបន្ទាប់រហូតក្លាយជា Internet នាពេលបច្ចុប្បន្ន។

IP (Internetworking Protocol) គឺជាការបញ្ជូនដោយស្វ័យប្រវត្តិប្រើនៅលើ TCP/IP ហើយមិនភ្ជាប់ជាមួយ Datagram Protocol។ IP មានសារៈសំខាន់ដែលជាដៃគូជាមួយនឹង TCP។ IP បញ្ជូន data ជាកញ្ចប់ដែល ហៅថា Datagram នីមួយៗគឺត្រូវបានរាប់បញ្ជូន។ Datagram ធ្វើចរាចរមានភាពខុសៗគ្នា និងគ្មានតុល្យភាព IP មិនរក្សាទុក Track នៃ Route ហើយគ្មានតុល្យភាពក្នុង Datagram។

១.៦ IP Address

IP address គឺជាអត្តសញ្ញាណនៃ Network ID និង Host ID។ IP address មានប្រវែង32 bit ចែកចេញជាបួន decimal integer។ ប្រសិនបើ Intranet Network មួយមិនត្រូវបានភ្ជាប់ជាមួយ Internet គឺការប្រើប្រាស់ IP address តាមបែបណាក៏បានដែរ ដែលគេឱ្យឈ្មោះ Local IP។ ចំពោះ

Public IP ត្រូវបានគ្រប់គ្រងដោយ Inter NIC (Internet work Information Center) បណ្ដាញ Address ទាំងនេះត្រូវបានផ្ដត់ផ្គង់តាមបែប IP ផ្អែកលើ Class ឬតាមបែប CIDR Blocks ហើយត្រូវមានតែមួយគត់នៅក្នុង Internet។

- IP Address មានចំនួន៥ Class:

Address Class	1st Octet Range
Class A	1 – 127
Class B	128 – 191
Class C	192 – 223
Class D	224 – 239
Class E	240 – 255

តារាងទី ១.២ Class IP Address

- Class IP Address

  Class D និង E ប្រើសម្រាប់ multicasting

IP Address	1st Octet	2nd Octet	3rd Octet	4th Octet
Class A	Network	Host	Host	Host
Class B	Network	Network	Host	Host
Class C	Network	Network	Network	Host

តារាងទី ១.៣ Network Address and Host Address

Subnet masks គឺប្រើដើម្បីបញ្ជាក់ ផ្នែកមួយណារបស់ IP Address ៣ Network Address និង ផ្នែកមួយណាជា Host Address។ ជាទូទៅ Subnet mast ត្រូវដាក់ដូចខាងក្រោម÷

Class A	255.0.0.0
Class B	255.255.0.0
Class C	255.255.255.0

ឧទាហរណ៍: ក្នុង Class B Network Address 135.67.0.1 បើ Subnet Mask គឺ 255.255.0.0 ពេលនេះ 135.67 គឺជា Network address ហើយ 0.1 ជា Host address។

១.៧ ស្តង់ដាររបស់ Network

១.៧.១ OSI Model

OSI Model (Open System Interconnection) គឺបានបង្កើតឡើងដើម្បីជួយសម្រួលដល់មុខងារនៃដំណើរការរបស់ Network (network processes function) ដែលវាជា Primary Model មួយសម្រាប់ការទំនាក់ទំនងនៅក្នុង Network។

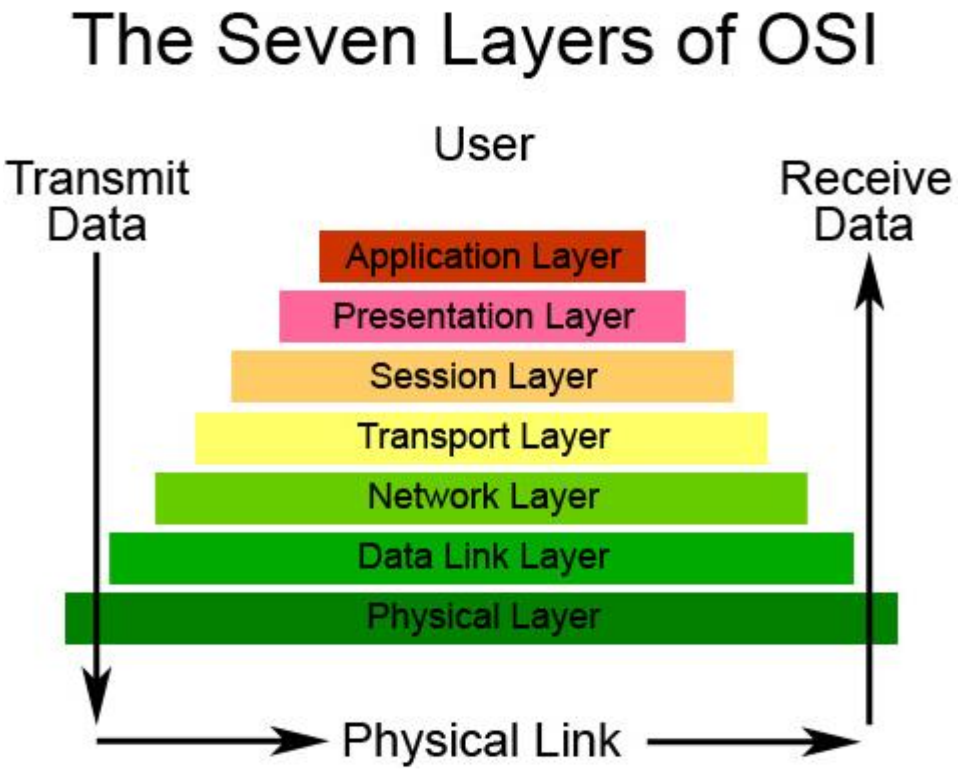
OSI Model ត្រូវបាន Released នៅឆ្នាំ 1984 ដែលវាបានរៀបរាប់ពី Scheme នីមួយៗនៅក្នុង Network។ វាបានផ្តល់ Vendors ជាមួយនឹង Standards ដើម្បីធានាបាននូវ Compatibility ដែលខ្ពស់រវាងប្រភេទនៃ Network។ Technologies ដែលត្រូវបានបង្កើតឡើងដោយក្រុមហ៊ុននានាទូទាំងពិភពលោក។ក្នុងនោះ OSI Model គឺជាជម្រើសដ៏ល្អមួយក្នុងការសិក្សាពីការបញ្ជូន Data និងទទួល Data on the Network។

១.៧.២ មុខងាររបស់ស្រទាប់ Layers

OSI Model គឺត្រូវបានបែងចែកជា ៧ Layers ដែលក្នុង Layers នីមួយៗគឺបែងចែកពីមុខងារធ្វើការនៅក្នុង Network។ សារៈសំខាន់មួយទៀតគឺ OSI Model បង្កភាពងាយស្រួលក្នុងការស្វែងយល់ពី Information ដែលត្រូវបានឆ្លងកាត់នៅក្នុង Network។

Layers ទាំងប្រាំពីរ របស់ OSI Model មានដូចជា ÷

7- Application Layer
6- Presentation Layer
5- Session Layer
4- Transport Layer
3- Network Layer
2- Data Link layer
1- Physical Layer



រូបភាពទី ១.៨ The Seven Layers of OSI

- Application Layer: វាគឺជា Layer ដែលស្ថិតនៅជិត User ជាងគេដោយផ្តល់នូវ Network Services ដល់ user ដើម្បីប្រើប្រាស់ application ណាមួយ។ វាមានលក្ខណៈខុសពី Layer ដទៃទៀតដោយវាមិនផ្តល់ Services ទៅកាន់ Layer ដទៃទៀតនោះទេ ប៉ុន្តែវាផ្តល់ services ទៅកាន់ Application ដែលនៅខាងក្រៅ OSI Model វិញ។
- Presentation Layer: វាគឺជាអ្នកធានានូវព័ត៌មានដែល Application Layer បាន send ចេញគឺអាច read បានពី System ដទៃទៀត។ ឧទាហរណ៍ Computer បានធ្វើការទំនាក់ទំនងទៅកាន់ Computer ផ្សេងទៀតដោយប្រើប្រាស់ Extended Binary Codedinterchange code (BECDIC) ប៉ុន្តែ Computer ផ្សេងទៀតបានប្រើប្រាស់ ASCII ដើម្បីបង្ហាញតួអក្សរដូចគ្នា។ ប្រសិនបើមានការចាំបាច់ណាមួយ Presentation Layer អាចធ្វើការ Translate រវាង data formats ទាំងនេះអាចធ្វើការទំនាក់ទំនងគ្នាបាន។
- Session Layer: គឺជា Layer មួយដែលបង្កើតការគ្រប់គ្រង និងផ្តាច់ Session រវាង Hosts ពីរដែលបានទំនាក់ទំនងគ្នា ហើយវាជាអ្នកផ្តល់ Services ទៅកាន់ Presentation Layer។ វាជា

អ្នកគ្រប់គ្រងនូវទំនាក់ទំនងរវាង Hosts ពីរ និងគ្រប់គ្រងពី Data ដែលបាន Exchange។ ឧទាហរណ៍: Web Server គឺមាន Users ជាច្រើនប្រើប្រាស់ ដូច្នេះវាបង្ករឱ្យមានការទំនាក់ទំនងកាន់តែច្រើនឡើងៗ ដែលវាជាតួនាទីរបស់ Session Layer ក្នុងការ Handle ការងារទាំងនេះ។

- Transport Layer: គឺជា Layer មួយដែលធ្វើការបំបែក (Segment) Data ដែលត្រូវពី Host មួយទៅមួយទៀតហើយផ្គុំវាឡើងវិញនៅពេលទៅដល់ Host មួយទៀត។ ឧទាហរណ៍: នៅក្នុងស្ថាប័នធំៗដែលមានសាខាច្រើនហើយត្រូវការ Data ពីតំបន់មួយ ទៅតំបន់មួយផ្សេងទៀត ដូច្នេះ Transport Layer ធ្វើការបំបែក data ដែលមានទំហំធំឱ្យទៅជាតូចៗ ហើយបញ្ជូនម្តងមួយៗ ទៅកាន់តំបន់ផ្សេងទៀត ដើម្បីការពារមិនឱ្យdata ត្រូវបាត់បង់នៅពេលបញ្ជូន។ ចំពោះ Application, Presentation, and Session Layer គឺគិតអំពី data សម្រាប់ប្រើប្រាស់ជាមួយនិង Application ចំណែក Lower four Layer គឺគិតអំពីការបំបែក data ដើម្បីបញ្ជូន។
- Network Layer: វាគឺជាអ្នកផ្តល់នូវការតភ្ជាប់ និងជ្រើសរើសផ្លូវដ៏សមស្របក្នុងការភ្ជាប់ ទំនាក់ទំនងរវាង Host System ដែលស្ថិតនៅក្នុង Network ផ្សេងគ្នា។ ដោយសារការរីកចំរើននៃបច្ចេកវិទ្យា Internet ហើយចំនួនអ្នកប្រើប្រាស់កាន់តែច្រើនឡើងក្នុងការ Access Information ទៅកាន់ Website នោះ Network Layer គឺមានតួនាទីជាអ្នកគ្រប់គ្រង លើការទំនាក់ទំនងទាំងនេះដោយមានសុវត្ថិភាព។
- Data Link Layer: វាគឺមានតួនាទីក្នុងការកំណត់ពីទំរង់ Data ដែលត្រូវបាន Formatted សម្រាប់ការបញ្ជូន និងគ្រប់គ្រងពីរបៀប Access ទៅកាន់ Network Layer នេះមានមុខងារក្នុងការកំណត់ពី Devices ដែលត្រូវធ្វើការភ្ជាប់ទំនាក់ទំនងគ្នារួមទាំងការកត់ត្រាពីការគ្រប់គ្រង Signal រវាង Devices នីមួយៗ។
- Physical Layer : វាមានតួនាទី ក្នុងការកំណត់ពី Electrical, Mechanical, Procedural សម្រាប់បើកដំណើរការ គ្រប់គ្រង និងបិទដំណើរការ Physical link រវាង End System។ វាជាអ្នកបំលែង Data ទៅជា Binary Digit សម្រាប់ទៅតាមខ្សែ ឬបំលែង Data ទៅជា Signal សម្រាប់បញ្ជូនតាមរលកធាតុអាកាស។

១.៨ Router

Router គឺជា Device មួយដែលត្រូវបានប្រើប្រាស់ដើម្បីធ្វើការតភ្ជាប់ Network ផ្សេងគ្នាឱ្យអាចធ្វើការទំនាក់ទំនងគ្នាបាន។ ចំពោះ Network ផ្សេងគ្នាដែលបានប្រើប្រាស់ Protocol ដូចគ្នា (TCP/IP) ហើយប្រើប្រាស់ Router ដើម្បីធ្វើការតភ្ជាប់នោះគឺ Router អាចត្រូវបានហៅថា Bridge។ ប៉ុន្តែនៅពេល Router ត្រូវបានតភ្ជាប់ Network ផ្សេងគ្នា ហើយប្រើប្រាស់ Protocol ខុសគ្នា (PCT/IP with other) នោះគឺRouter ត្រូវបានហៅថា Gateway វិញ។ Protocol ដែលខុសពី PCP/IP មានដូចជា : IPX/SPX, DECnet, OSI, DDP, XNS,...។

រូបភាពទី ១.៩ Router

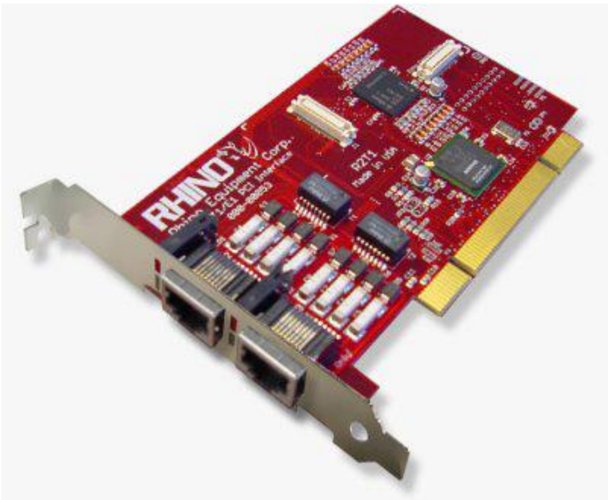
១.៩ Gateway

Gateways គឺជា device ឬ Computer ដែលត្រូវប្រើប្រាស់ដើម្បីធ្វើការតភ្ជាប់ Network ដែលមាន Protocol ផ្សេងគ្នាឱ្យអាចធ្វើការទំនាក់ទនងគ្នាបាន។ ជាទូទៅ Computer ដែលមាន Network Card ចាប់ពី ២ឡើងទៅបានហៅថា Gateway ហើយចំពោះ Router ក៏ត្រូវបានចាត់ទុកថាជា Gateway ផងដែរ។

រូបភាពទី ១.១០ ឧបករណ៍ Gateway

១.១០ Network Interface Card (NIC)

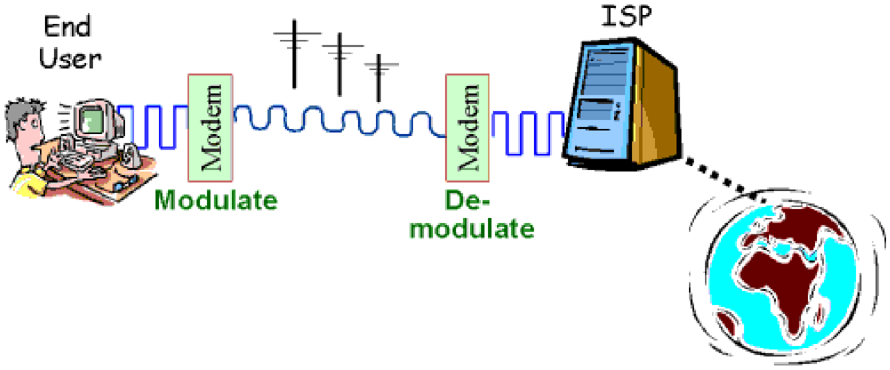
Network Interface Card (NIC) គឺជា Card ដ៏សំខាន់មួយដើម្បីបើកដំណើរការនៃការភ្ជាប់ Network របស់ Computer។ ប្រសិនបើ Computer មួយគ្មាន Network Interface Card (NIC) នោះគឺមិនអាចធ្វើការភ្ជាប់ Network បានទេ។ ចំពោះ Network Interface Card អាចត្រូវបានហៅថា Network Adapter ផងដែរ។ Computer ភាគច្រើនត្រូវបានភ្ជាប់ Network Card ជាប់ Board រួចជាស្រេច។



រូបភាពទី ១.១១ Network Interface (NIC)

១.១១ Modem

Modem (Modulator/DEMddulator) ក៏ជា Device មួយដែលត្រូវបានប្រើប្រាស់ដើម្បីធ្វើការតភ្ជាប់ Network ជាពិសេសភ្ជាប់ទៅកាន់ Internet។



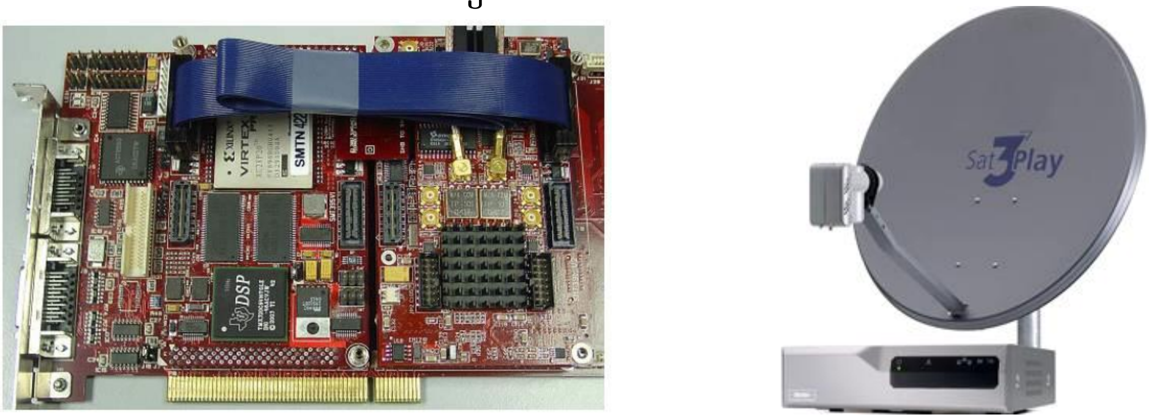
រូបភាពទី ១.១២ Modem

ក្នុងនោះប្រភេទនៃ Modem ដែលបានភ្ជាប់ទៅកាន់ Internet ត្រូវបានបែងចែកជាពីរប្រភេទដូចជា Internal Modem and External Modem។

Internal Modem គឺជា Device ដែលត្រូវបាន Install នៅខាងក្នុង Desktop ឬ Laptop Computer ផ្ទាល់តែម្តងដែលអនុញ្ញាតឱ្យ Computer ធ្វើការទំនាក់ទំនងទៅកាន់ Network Or Internet បាន។ ចំពោះ Internal Modem មានពីរប្រភេទផ្សេងទៀត រួមមាន Dial-up And WIFI (Wireless) ដែលដំណើរការរបស់វាគឺចរាចរតាមរយៈ Telephone Line និងទាមទារនូវ phone Number ដើម្បីធ្វើការ Access ទៅកាន់ Network។ ភាពខុសគ្នារបស់វាគ្រាន់តែការភ្ជាប់ពី Computer ទៅ Modem មានខ្សែ ឬឥតខ្សែតែប៉ុណ្ណោះ។ ចំពោះ Computer មាន Modem Card Build-in នៅក្នុង Board ប៉ុន្តែ computer ខ្លះទៀតប្រើប្រាស់ PC Card Modem។ ជាមួយនឹងការ Dial-up Internet Connection គឺត្រូវប្រើប្រាស់ខ្សែ RJ-11 ហើយល្បឿននៃការ បញ្ជូនទិន្នន័យត្រឹមតែ 56 Kbps តែប៉ុណ្ណោះ។

រូបភាពទី ១.១២ Dial-Up Modem for Desktop PC and Laptop PC

External Modem គឺជា Modem ប្រភេទដែលមាន Interface សម្រាប់ដោតភ្ជាប់ គឺតាមរយៈ Serial Port or USB Modem។ ក្នុងនោះ External Modem មាន២ប្រភេទទៀតដែលសំខាន់ដូចជា Cable Modem and DSL Modem។ Internet Connection តាមរយៈសេវាកម្មខ្សែកាបទូរស្សន៍។ វាប្រើប្រាស់ខ្សែ Coaxial ដែលមាន Bandwidth ធំជាង Dial-up Modem។ វាបានផ្តល់ល្បឿនក្នុងការ Download ប្រមាណ 38 Mbps និងល្បឿននៃការ Upload ប្រមាណ 1 Mbps។



រូបភាពទី ១.១៣ Cable Modem and Satellite Modem

ចំពោះ DSL (Digital Subscriber Line) Modem វិញគឺភ្ជាប់ DSL Modem ទៅកាន់ Computer or Router ដើម្បីភ្ជាប់ Internet។

រូបភាពទី ១.១៤ DSL (Digital Subscriber Line) Modem

មេរៀនទី ២

ណែនាំឱ្យស្គាល់ពី Firewall

២.១ តើអ្វីជា Firewall?

Firewall គឺជាមធ្យោបាយឬជាផ្លូវមួយដែលអាចឱ្យប្រព័ន្ធណែតវើកដែលស្ថិតនៅក្នុង LAN មួយមានទំនាក់ទំនងជាមួយនឹង LANs, MANs or WANs ផ្សេងៗទៀតបាន។

Firewall គឺជាប្រព័ន្ធសុវត្ថិភាពមួយ ដែលគេបង្កើតវាឡើងដើម្បីការពារការជ្រៀតចូលមកក្នុងប្រព័ន្ធ Network ដោយគ្មានការអនុញ្ញាត។ វាអាចផ្តល់នូវការប្រើប្រាស់ជាប្រព័ន្ធ Network ដែលផ្តល់នូវសុវត្ថិភាពខ្ពស់ដល់ប្រព័ន្ធ Network។ យើងអាចប្រើប្រាស់ Firewall ជាលក្ខណៈ Software និង Hardware ឬក៏យើងអាចប្រើប្រាស់បានទាំងពីរតែម្តងក៏បាន។ Firewall អាចការពារប្រព័ន្ធ Network ដែលភ្ជាប់ទៅកាន់ប្រព័ន្ធ Internet ពីពួក Hacker ដែលព្យាយាម ចូលមកកាន់ប្រព័ន្ធ Network របស់យើងតាមរយៈ Internet។ រាល់ទិន្នន័យដែលចេញ ឬចូលមកក្នុងប្រព័ន្ធ Network របស់យើងត្រូវឆ្លងកាត់តាម Firewall ហើយ Firewall វាជាអ្នកត្រួតពិនិត្យថា តើទិន្នន័យប្រភេទណាគួរអនុញ្ញាតឱ្យឆ្លងកាត់ ឬមិនអនុញ្ញាតឱ្យឆ្លងកាត់។ Firewall មានសមត្ថភាពក្នុងការគ្រប់គ្រងលើប្រព័ន្ធ Network ឱ្យមានសុវត្ថិភាពល្អប្រសើរ និងអាចត្រួតពិនិត្យការទំនាក់ទំនងក្នុងប្រព័ន្ធ Network។

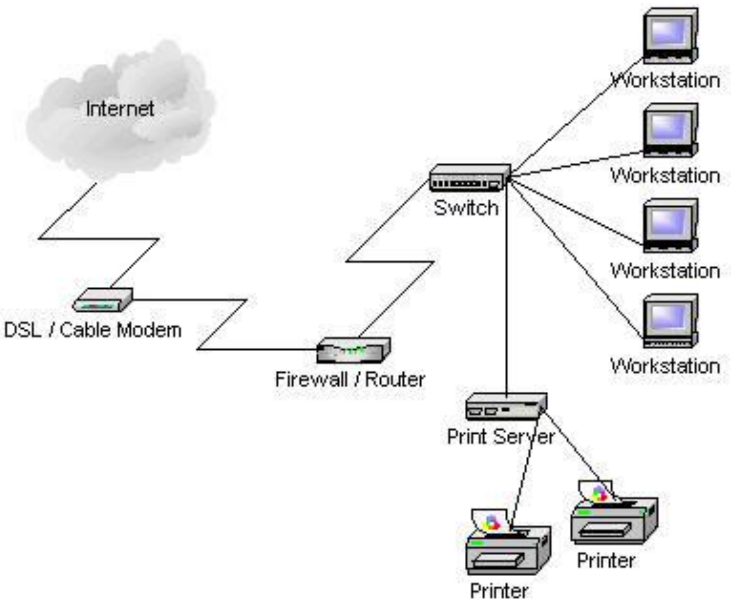
Firewall ធ្វើការចាត់ចែងនូវដំណើរការផ្លាស់ប្តូរ Data ពីប្រព័ន្ធ Internet មកម៉ាស៊ីន Computer ហើយអ្វីដែលពិសេសជាងនេះទៅទៀតគឺ ការត្រួតពិនិត្យទៅលើច្រកចូល និងច្រកចេញការទំនាក់ទំនងរវាងម៉ាស៊ីននីមួយៗនៅលើប្រព័ន្ធ Network ទាំងអស់។

រូបភាពទី ២.១ Firewall

២.២ ស្គាល់ពី Firewall

Firewall ចែកចេញជាពីរផ្នែកគឺផ្នែកទន់ (Software) និងផ្នែករឹង (Hardware based)។ ផ្នែកទន់ជាប្រភេទ Firewall ដែលប្រើប្រាស់នូវ Software ក្នុងការគ្រប់គ្រង ដូចជា Microsoft ISA, IP Fire, IP Cop, PF Sense… និង Firewall ប្រភេទ Hardware ដែលគេនិយមប្រើដូចជា Router CISCO, MikroTik …។ Firewall ផ្តោតសំខាន់លើសុវត្ថិភាពបណ្តាញ និងត្រួតពិនិត្យនូវរាល់ការចរាចរចេញ និងចូល (incoming and outgoing) ក្នុងបណ្តាញដោយធ្វើការវិភាគនូវរាល់កញ្ចប់ទិន្នន័យ (Data Packets) មុន និងអនុញ្ញាតថាតើគួរឱ្យឆ្លងកាត់ ឬក៏អត់ ដោយផ្អែកលើលក្ខខណ្ឌដែលបានកំណត់រួចជាស្រេច (Based on applied rule set)។

យើងអាចឱ្យនិយមន័យពាក្យថា Firewalls ទៅតាមកម្រិតនៃការយល់ដឹងរបស់យើងបាន។ Firewall បង្កើតឱ្យមានសុវត្ថិភាពសម្រាប់បណ្តាញខាងក្នុងដែលគួរឱ្យជឿទុកចិត្ត និងបង្កើតជាឧបសគ្គរវាងបណ្តាញផ្សេងទៀត ដូចជាអ៊ីនធឺណេត ដែលត្រូវបានសន្មតថាជាប្រព័ន្ធពុំសូវមានសុវត្ថិភាព និងទុកចិត្តបានឡើយ។ ប្រព័ន្ធប្រតិបត្តិការកុំព្យូទ័រជាច្រើនមាន Firewall ជាផ្នែកទន់ ដែលមានមូលដ្ឋានដើម្បីការពារប្រឆាំងនឹងការគំរាមកំហែងពីសាធារណៈ ឬអាចថា Firewall គឺជាកម្មវិធីផ្នែកទន់ ឬបំណែកនៃផ្នែករឹងដែលជួយឆ្លុះបញ្ចាំងចេញពីពពួក Hacker ពពួកមេរោគ និងមេរោគ ដែលព្យាយាម ជ្រៀតចូលកុំព្យូទ័ររបស់អ្នកប្រើនៅលើអ៊ីនធឺណេត។



រូបភាពទី ២.២ Network Firewall

២.២.១ Software Firewalls

Software Firewall គឺជាប្រភេទ Firewall ដែលមានសមត្ថភាពខ្ពស់ ក្នុងការគ្រប់គ្រងទៅលើប្រព័ន្ធ Network និងប្រព័ន្ធ Internet។ Software Firewall វាជាប្រភេទ Software ដែលមិនតម្រូវឱ្យយើងទៅទិញវានៅទីផ្សារនោះទេគឺយើងអាចទាញវាចេញពី Internet បានហើយភាគច្រើននៃ Software Firewall គឺមិនត្រូវបានគិតលុយនោះទេ (Download free) ដោយគ្រាន់តែទាញយកហើយ យើង Software ដែលយើងបានទាញនោះទៅដំឡើងនៅលើកុំព្យូទ័រណាមួយទៅជាការស្រេច។ Software Firewall វាមានច្រើនប្រភេទណាស់ហើយប្រភេទទាំងនោះមានដូចជា÷

- IP Fire
- ISA Server 2004/2006
- IP Cop
- Linux
- Pf Sense

រូបភាពទី ២.៣ IPCop Software Firewall

រូបភាពទី ២.៤ ISA Software Firewall

២.២.២ Hardware Firewalls

Hardware Firewalls ជា Router board ដែលវាមានសមត្ថភាពក្នុងការគ្រប់គ្រង Internet និងធ្វើការបែងចែកនូវល្បឿន Internet ដែលធ្វើឱ្យវាមានភាពងាយស្រួលក្នុងការគ្រប់គ្រង និងបែងចែក ពីព្រោះវាមិនត្រូវការអ្នកត្រួតពិនិត្យជាប្រចាំទេ គឺយើងគ្រាន់តែធ្វើការ Configure តែម្តងវាជាការស្រេចក្នុងការប្រើប្រាស់។

រូបភាពទី ២.៥ Router Board គ្មានអង់តែន

រូបភាពទី ២.៦ Router Board មានអង់តែនពីរ

រូបភាពទី ២.៧ Router Board មានអង់តែនបី

២.២.២.១ អ្វីទៅជា MikroTik

MikroTik គឺជា RouterOS និង Hardware ដែល RouterOS ជាប្រព័ន្ធប្រតិបត្តិការរបស់ MikroTik Router BOARD Hardware។ វាមានសមត្ថភាពក្នុងការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធឺណេត ចែកចាយទិន្នន័យ ការពារការជ្រៀតចូលមកក្នុងប្រព័ន្ធ Network ដោយគ្មានការអនុញ្ញាត បែងចែកល្បឿន Internet ធ្វើជា Hotspot ធ្វើ VPN Server និងផ្សេងៗជាច្រើនទៀត។

រូបភាពទី ២.៨ MikroTik Router

២.២.២.២ ប្រវត្តិរបស់ MikroTik

MikroTikls Ltd., ត្រូវបានគេស្គាល់ជាអន្តរជាតិថា “MikroTik” ដែលជាក្រុមហ៊ុនផ្គត់ផ្គង់ខាងផ្នែកសម្ភារៈ Network ហើយត្រូវបានគេរកឃើញនៅឆ្នាំ ១៩៩៥ បង្កើតឡើងដោយលោក John Trully និង Arnis Riekstins។ ហើយមានទីតាំងនៅទីក្រុង Riga ដែលជារដ្ឋធានីនៃប្រទេស Latvia។ លើកដំបូងដែលពួកគេប្រើខឺណែលលីនុច 2.2 ដែលត្រូវបានអភិវឌ្ឍរួមគ្នាជាមួយបុគ្គលិក ៥ ទៅ ១៥នាក់។ បច្ចុប្បន្ននេះ MikroTik បានផ្តល់នូវ Hardware និង Software សម្រាប់ការតភ្ជាប់ Internet ស្ទើរតែគ្រប់ប្រទេសនៅទូទាំងពិភពលោក។

តាមបទពិសោធន៍របស់ក្រុមហ៊ុនក្នុងការប្រើប្រាស់កុំព្យូទ័រ ជាស្តង់ដារឧស្សាហកម្មផ្នែករឹង និងប្រព័ន្ធ Router ពេញលេញត្រូវបានអនុញ្ញាតឱ្យប្រើប្រាស់នៅក្នុងឆ្នាំ ១៩៩៧ ដើម្បីបង្កើតប្រព័ន្ធប្រតិបត្តិការ RouterOS ដែលផ្តល់នូវភាពទូលំទូលាយ ការត្រួតពិនិត្យ និងអាចប្រើប្រាស់សម្រាប់ចែកចាយទិន្នន័យគ្រប់ប្រភេទ។

នៅក្នុងឆ្នាំ ២០០២ ក្រុមហ៊ុនបានសម្រេចចិត្តបង្កើត Hardware និងម៉ាក RouterBOARD ដោយខ្លួនឯង ដើម្បីបង្កើតជា Routers និងប្រព័ន្ធ Wireless ISP។ ការដាក់ឱ្យប្រើប្រាស់នោះមានទៅតាម Version នៃ MikroTik RouterOS ដូចជា÷

ជំនាន់របស់ MikroTik RouterOS	**កាលបរិច្ឆេទបានចេញជាផ្លូវការ**
RouterOS version 3	January 2008
RouterOS version 4	October 2009
RouterOS version 5	March 2010
RouterOS version 6	May 2013

តារាងទី ២.១ តារាងប្រវត្តិរបស់ MikroTik RouterOS

មេរៀនទី ៣

ការចាប់ផ្ដើមធ្វើឱ្យ MikroTik ស្គាល់ Internet

៣.១ តើ Mikortik Router អាធ្វើអ្វីបានខ្លះ?

Mikortik Router គឺជា RouterOS និង Hardware វាមានសមត្ថភាពក្នុងការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធឺណេត ចែកចាយទិន្នន័យ ការពារការជ្រៀតចូលមកក្នុងប្រព័ន្ធ Network ដោយគ្មានការអនុញ្ញាត និងបែងចែកល្បឿន Internet បានល្អប្រសើរ។

បន្ទាប់ពីសិក្សាទៅលើការគ្រប់គ្រងប្រព័ន្ធអ៊ីនធឺណេត ដោយប្រើប្រាស់ Mikortik Router មកខ្ញុំសង្កេតឃើញថាការគ្រប់គ្រងអ៊ីនធឺណេតមានប្រសិទ្ធភាពខ្ពស់ ព្រមទាំងមានលទ្ធភាពច្រើនសម្រាប់ ÷

– អាចគ្រប់គ្រងអ្នកប្រើប្រាស់អ៊ីនធឺណេតបាន

–MikroTik Router ពិតជាមានសុវត្ថិភាពខ្ពស់

– មានភាពងាយស្រួលក្នុងការគ្រប់គ្រងទៅលើប្រព័ន្ធ Internet

– បិទនូវ Website អាសអាភាស និង Website ណាដែលគ្មានប្រយោជន៍

– ការកំណត់ទំហំទិន្នន័យ នៃអ្នកប្រើប្រាស់ក្នុងការទាញយក និងបញ្ជូនចេញ

– កំណត់ល្បឿន Internet

– អាចទប់ស្កាត់ពីការវាយប្រហារពីពពួក Hacker

– ដឹងនូវ IP Address របស់ម៉ាស៊ីនណាមួយ ដែលបើកនូវ Website ណាមួយ

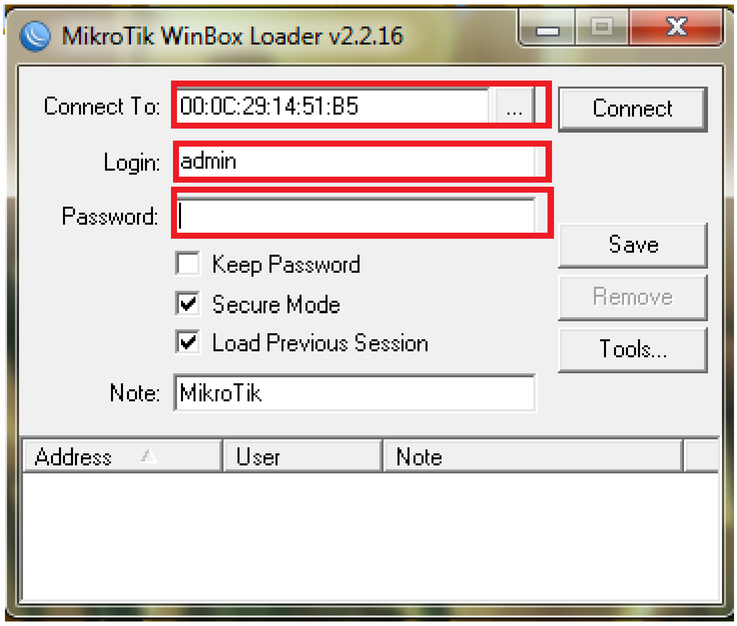
– កំណត់ល្បឿនទាញយក (Download) និង (Upload) ដើម្បីរក្សាស្ថេរភាពអ៊ីនធឺណេតនៅក្នុងក្រុមហ៊ុន

– ការប្រើប្រាស់មានសុវត្ថិភាព ព្រោះមានប្រព័ន្ធសុវត្ថិភាពច្រើន។

៣.២ របៀប Login នៅលើ MikroTik Router

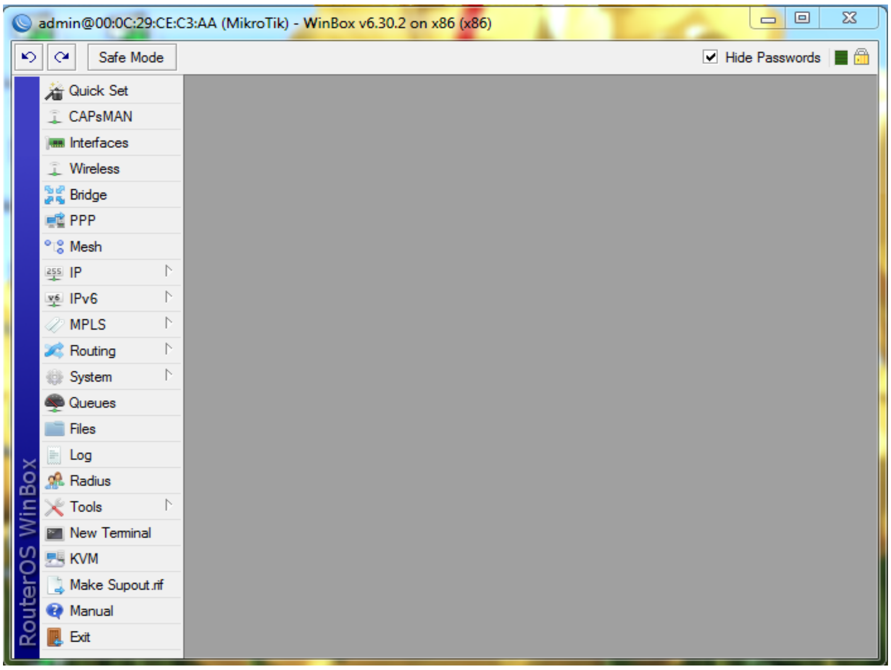
ដើម្បី Login ចូលក្នុង MikroTik Router បានយើងត្រូវភ្ជាប់ខ្សែ Network ពី Computer ទៅកាន់ Router ជាមុនសិន។ ក្នុងការ Login គឺមានច្រើនរបៀប យើងអាច Login តាមរយៈ Browser or WinBox ក៏បាន។ នៅក្នុងពេលនេះ យើងខ្ញុំសូមលើកយកកម្មវិធី Winbox មកបង្ហាញដូចតទៅជាដំបូង

យើងបើកកម្មវិធី WinBox រួចចុច Scan. MikroTik ថ្មីគឺមិនទាន់មាន IP ទេ ដូចនេះយើងត្រូវ Scan រក MAC Address (A Media Access Control Address) ដើម្បី Login ។



រូបភាពទី ៣.១ ការ Login នៅលើ MikroTik តាមរយៈ Winbox

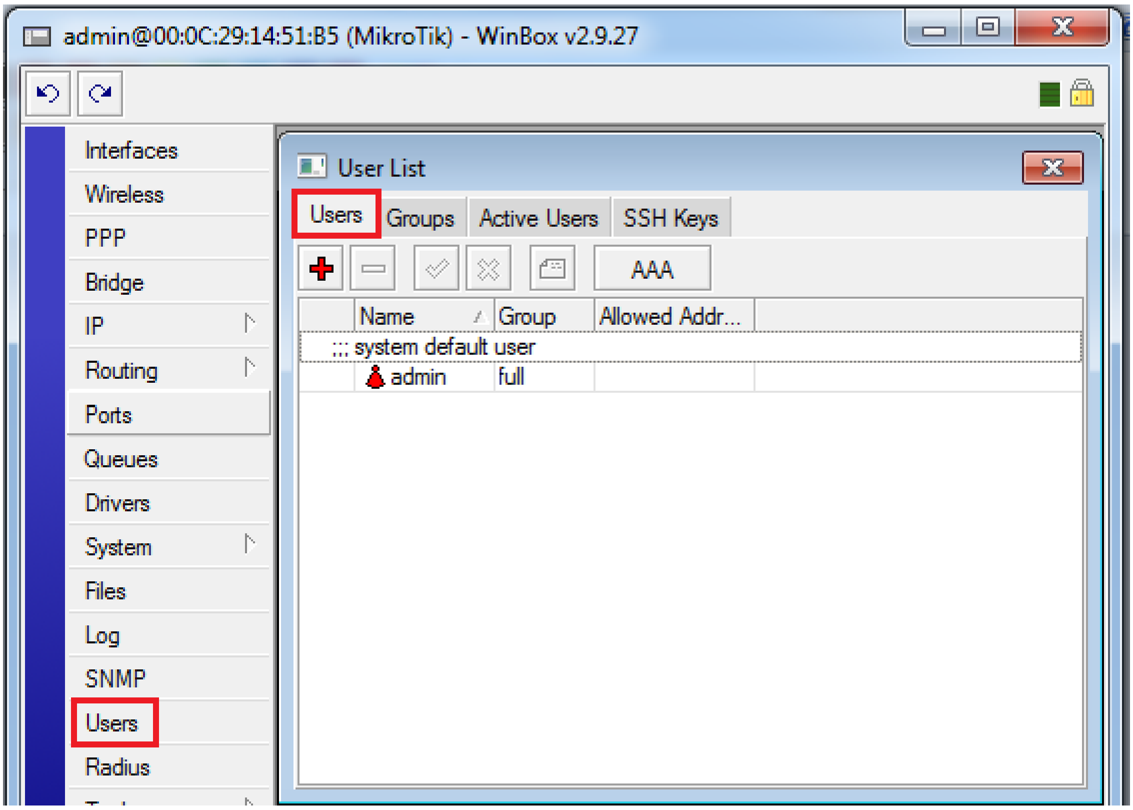
ក្រោយនៅពេលដែល Login ដោយប្រើ Winbox ដើម្បី Remote ចូលទៅក្នុង MikroTik Desktop ឬ Interface តាមរយៈ Mac Address រួចហើយ យើងនឹងឃើញ Interface ដែលមាន Tool និង Option ជាច្រើន។



រូបភាពទី ៣.២ Interface នៃ MikroTik RouterOS

ជាទូទៅគេត្រូវ តែបង្កើត User Admin នៅក្នុង MikroTik Router ដើម្បីងាយស្រួលក្នុងការគ្រប់គ្រង System និង លើ User ផ្សេងទៀត។ ដើម្បីបង្កើត User យើងត្រូវចូលទៅក្នុង Winbox System Tools => User ក្រោយមក វានឹងលោតផ្ទាំងមួយ សម្រាប់ឱ្យយើងធ្វើការកំណត់ នូវឈ្មោះ និងសិទ្ធិរបស់ User នីមួយៗ។ User មានបីប្រភេទដូចជា÷

- User Admin
- User Read
- User Write

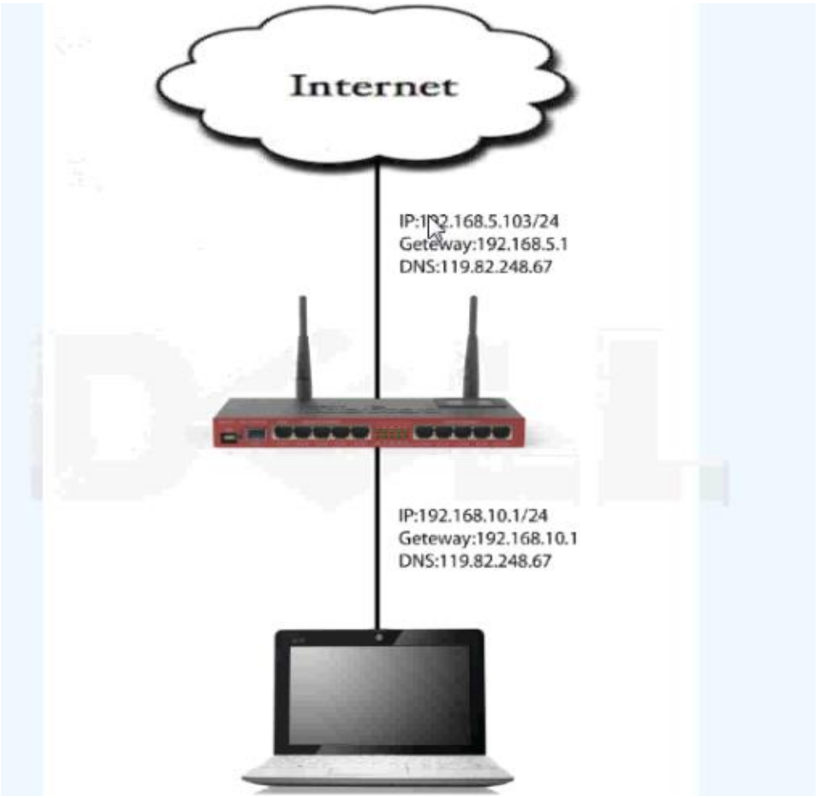


រូបភាពទី ៣.៣ បង្កើត User

៣.៣ របៀប Configure Internet នៅលើ MikroTik Router

ដើម្បី Configure Internet នៅលើ MikroTik Router យើងត្រូវមាន IP Public, Gateway, DNS ពី ISP ជាមុនសិន។ ក្រោយមកយើងធ្វើការ Login on WinBox បន្ទប់មកចូល Interface ដើម្បីកំណត់ Interface ណាមួយជា WAN រឺជា LAN។

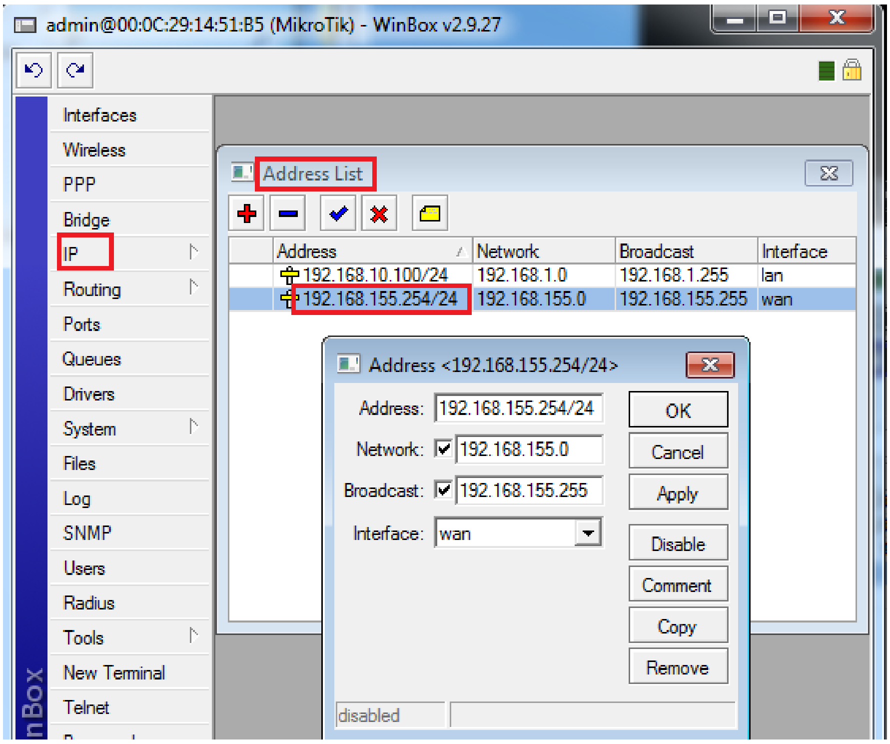
- WANs គឺជាកន្លែងសម្រាប់បញ្ចូល IP Public from ISP
- LANs គឺជាកន្លែងបញ្ចេញ IP ទៅឱ្យ PC



រូបភាពទី ៣.៤ ការតភ្ជាប់ Internet

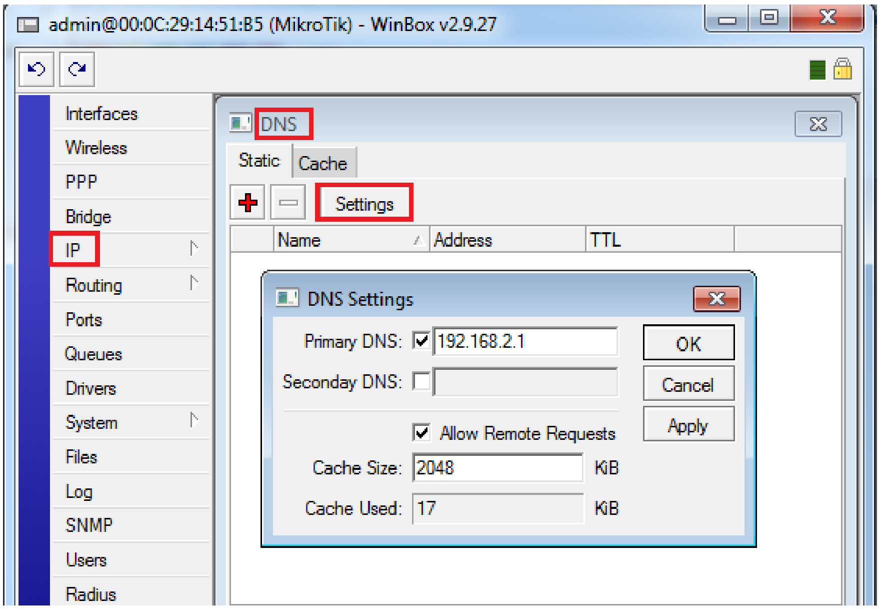
ជាដំបូងយើងចូល Interface => ពេលនោះយើងនឹងឃើញ ផ្ទាំងមួយ ដែលបង្ហាញនូវ Interface ទាំងអស់នៃ Ports របស់ Router។ ក្រោយពីការកំណត់ Interface រួចយើងត្រូវបញ្ចូល IP របស់ WAN។ ដើម្បីបញ្ចូល IP យើងចូលទៅ IP => Address => Add => ធ្វើការ Assign IP from ISP ក្រោយមកយើងធ្វើការ Select ដើម្បីកំណត់ទៅលើ Interface WAN។

បន្ទាប់មកយើងចុច Add ដើម្បីកំណត់ IP របស់ LAN ដើម្បីបោះ IP ទៅក្រៅកាន់Clients Ex:192.168.1.1/24 ដើម្បីទទួលបាននូវ Sub netmask => 255.255.255.0។



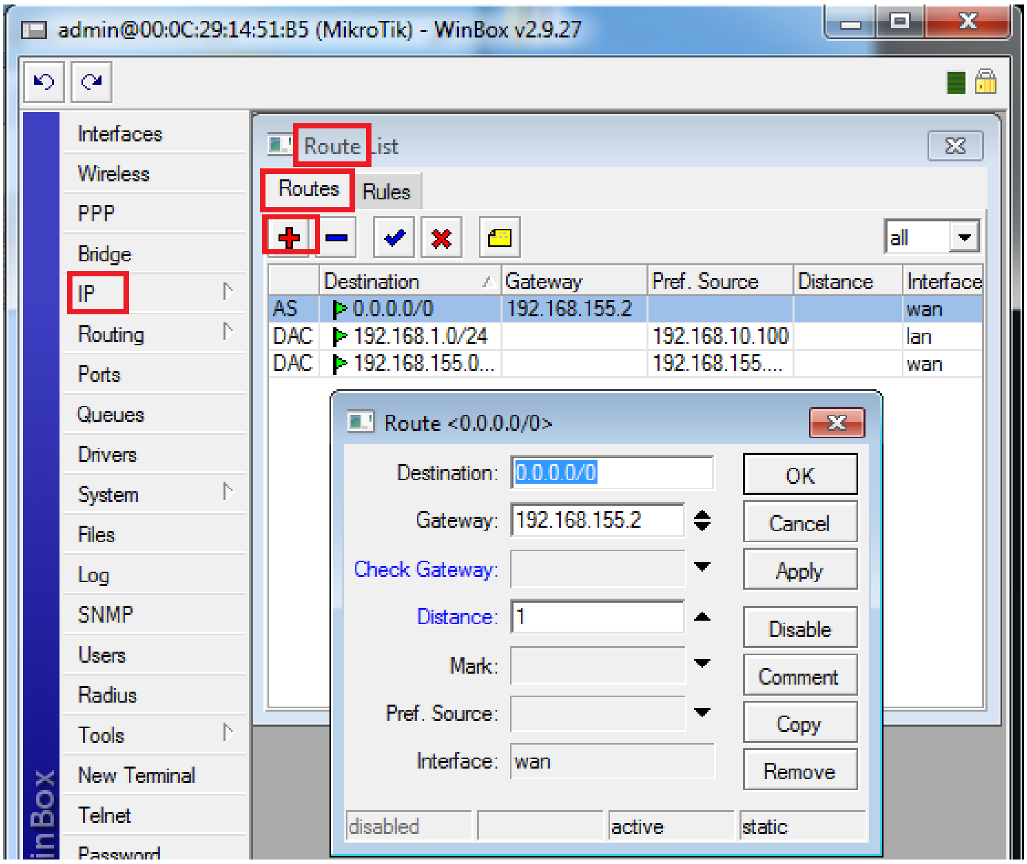
រូបភាពទី ៣.៥ ការ Configure Internet

បន្ទាប់មកទៀតយើងត្រូវបញ្ចូល DNS ដើម្បីបញ្ចូល DNS យើងត្រូវចូល IP => DNS => Server ធ្វើការបញ្ចូល DNS ពី ISP => Apply => Ok ។



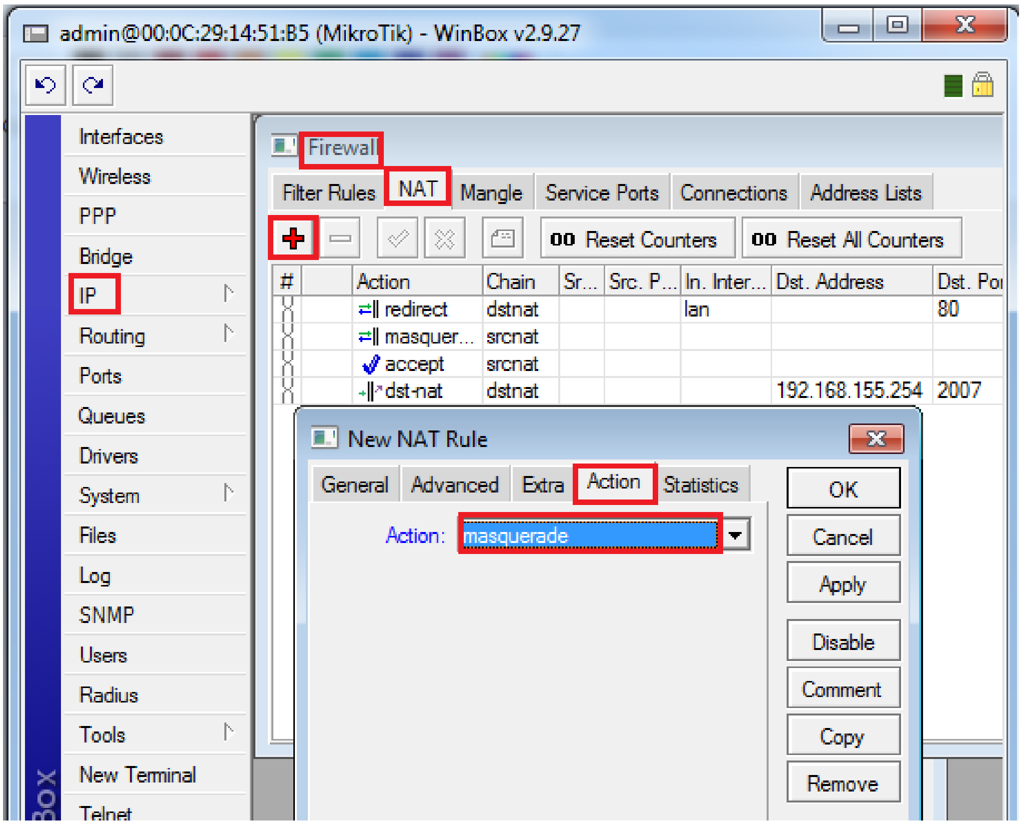
រូបភាពទី ៣.៦ ការដាក់ភ្ជាប់ DNS

ម្យ៉ាងវិញទៀតយើងធ្វើការ Routes ដើម្បីឱ្យវា Routes Gateway WAN and LAN ស្គាល់គ្នា យើងចូលទៅ IP => Routes => Add => Gateway ដែលយើងត្រូវបញ្ចូល Gateway របស់ ISP => Apply => OK ។



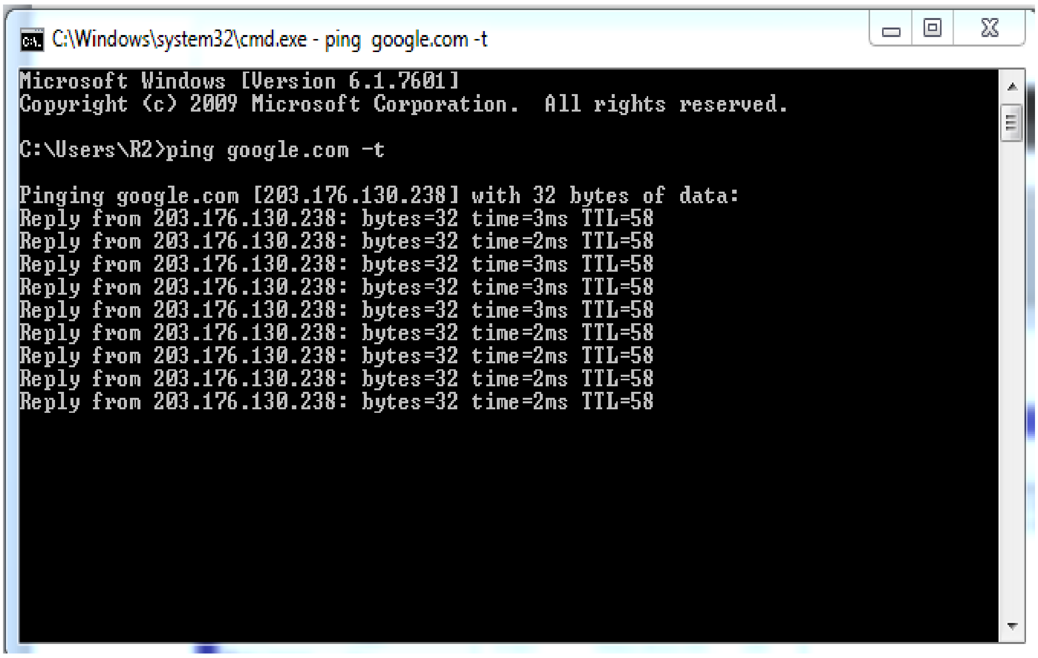
រូបភាពទី ៣.៧ ភ្ជាប់ IP ពី WANs ទៅ LANs

ពេលនោះគឺ MikroTik របស់យើងគឺមាន Internet ហើយប៉ុន្តែនៅលើ PC របស់យើងគឺមិនទាន់មាន Internet នៅឡើយទេ។ ដូចនេះ ជាចុងក្រោយយើង បញ្ចូល IP លើ PC របស់យើងផ្តល់និងចូលទៅកាន់ Firewall ដើម្បីបើកឱ្យ Internet ដំណើរការនៅក្នុង PC ។ ដើម្បីកំណត់បានយើងត្រូវចូលទៅ IP => Firewall => Nat => Add New Nat Rule => Action => Select យកពាក្យ “masquerade” ដើម្បី Allow Internet ហើយចុចពាក្យថា Apply និង OK ជាការស្រេច។



រូបភាពទី ៣.៨ ការបើក Internet ឱ្យ Clients ប្រើប្រាស់

រួចយើងធ្វើការ Ping to google.com នោះយើងនឹងបានដឹងថា PC របស់យើងមាន Internet ឬក៏អត់ Internet ។ ចូល Start+Run => Cmd => Type “ping google.com -t” ជាការស្រេច។



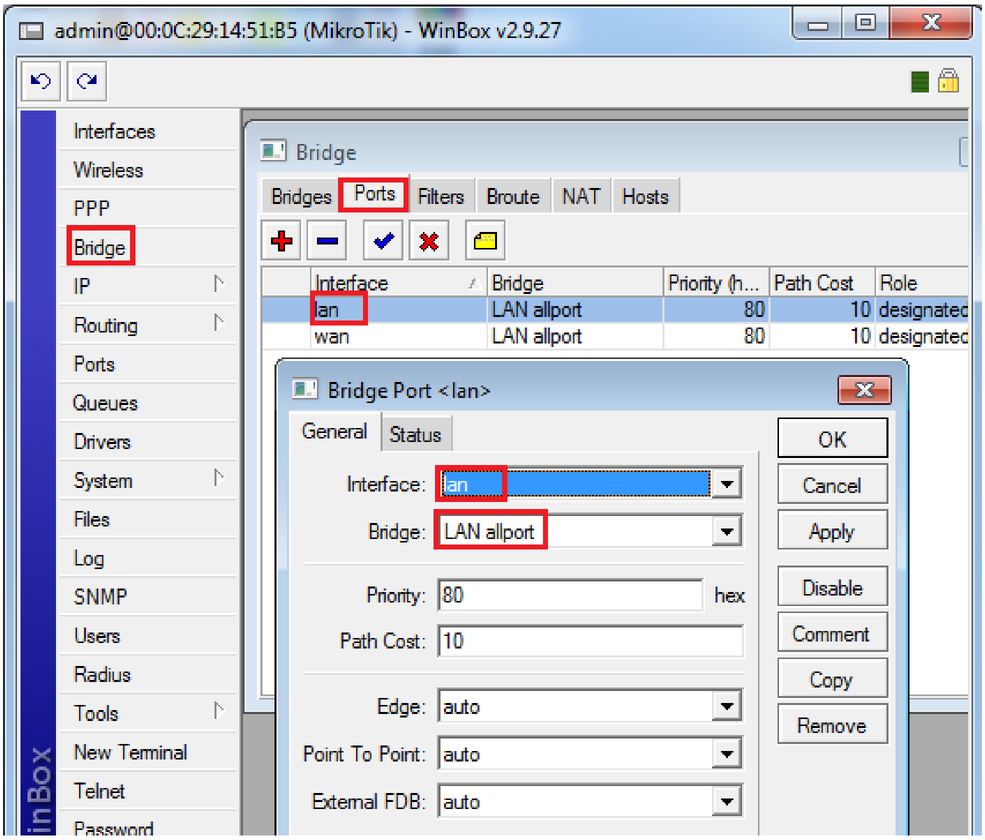
រូបភាពទី ៣.៩ Internet Testing

មេរៀនទី ៤

ការដំឡើង Service មួយចំនួនលើ MikroTik

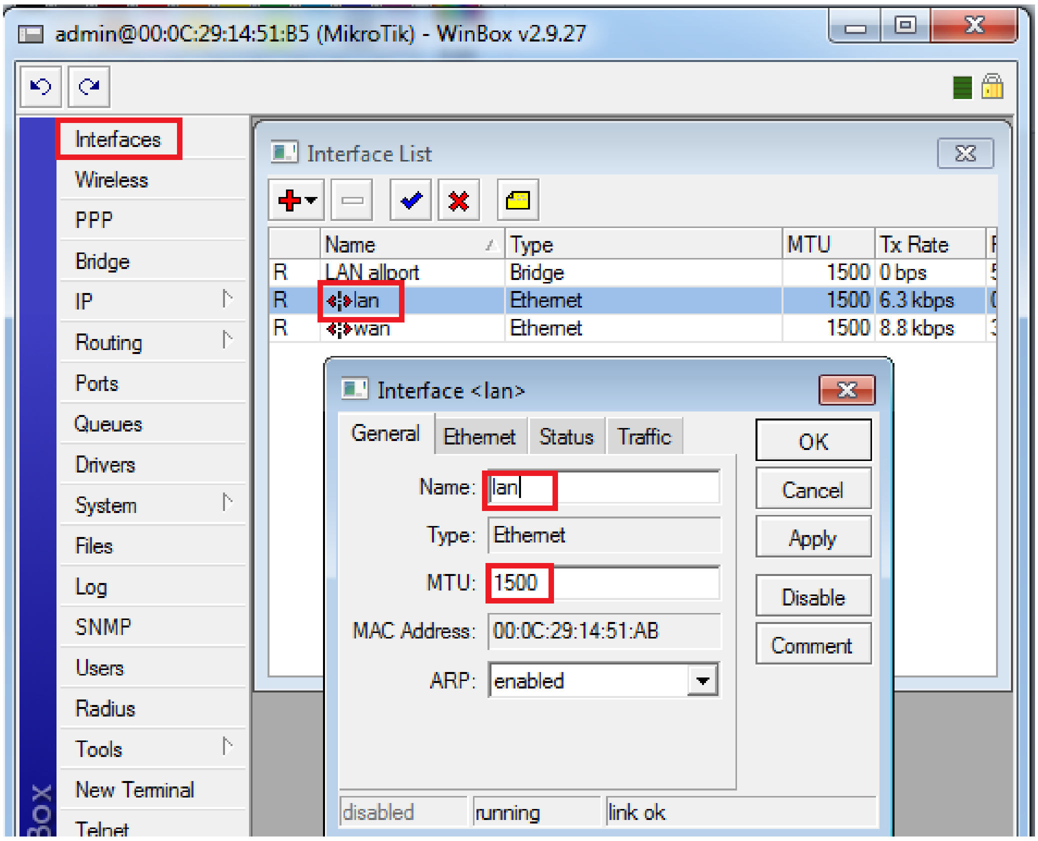
៤.១ បង្កើត Bride

នៅពេលនេះ PC របស់យើងមាន Internet ពិតមែន តែយើងអាចប្រើបានត្រឹមតែមួយ Port ប៉ុណ្ណោះ។ ដូច្នេះដើម្បីឱ្យ port ទាំងអស់មាន Internet យើងត្រូវ Port => Add Port ទាំងអស់ឱ្យស្គាល់គ្នា។ យើងត្រូវចូល Bridge យើងធ្វើការបង្កើត Bridge មួយជាមុនសិន ឧទាហរណ៍: យើងបង្កើត Bridge មួយឈ្មោះថា LAN_allport។ បន្ទាប់មកយើងចូល Ports ចុចពាក្យ Add Select យក Interface LAN ដែលជា Port ទី២ របស់យើង Add ទៅក្នុង LAN_allport ដែលយើងទើបបង្កើត។ ហើយយើងត្រូវ Add Port ផ្សេងៗទៀតចូលក្នុង Bridge LAN_allport ជាមួយ Port ទី២ ដែរ។



រូបភាពទី ៤.១ ការ Config Port ឱ្យស្គាល់ Internet

រួចយើងចុចទៅលើក Interface ហើយយើងយកពាក្យ Lan ត្រង់ MTU យើងត្រូវវាយលេខ 1500 រួចចុច Apply និង Ok ជាការស្រេច។

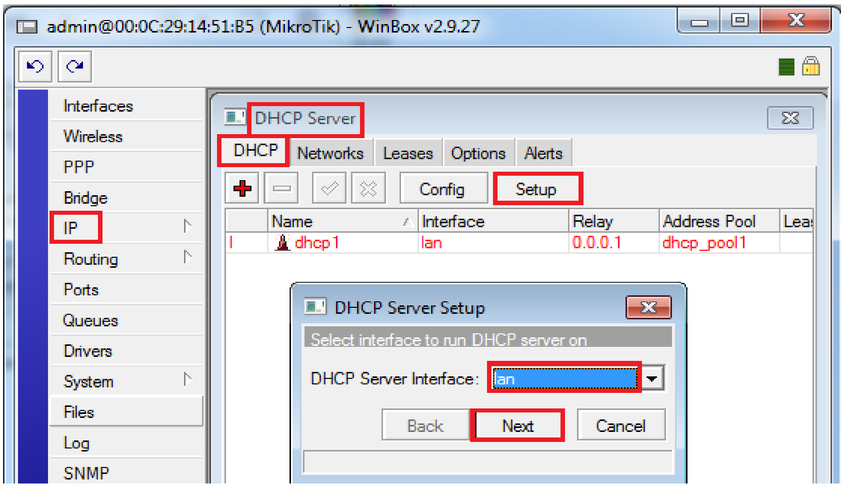


រូបភាពទី ៤.២ ការកំណត់ LANs

៤.២ របៀប Setup DHCP Server នៅលើ MikroTik Router

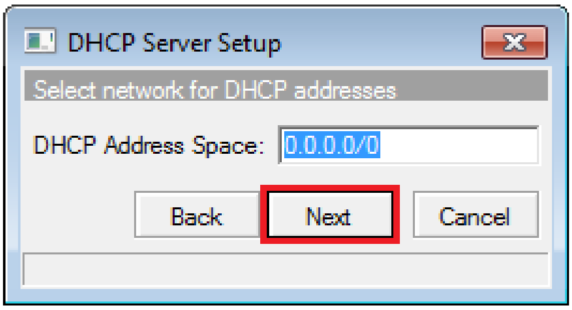
DHCP (Dynamic Host Configuration Protocol) មានន័យថា ការបោះ IP Address ទៅឱ្យ Client ដោយស្វ័យប្រវត្តិ។ ដើម្បី Setup DHCP Server យើងត្រូវ៖

=> IP => DHCP Server => DHCP Setup ធ្វើការជ្រើសរើស Port ដែលយើងចង់ Setup DHCP => DHCP Address Space ចុច Next => Gateway សម្រាប់ DHCP Network ចុច Next => Address to give out មានន័យថា កំណត់ IP ពីណាទៅដល់ណា ចុច Next => DNS Server ចុច Next => Lease Time ចុច Next ជាការស្រេច។ ក្រោយមកជាការស្រេច ពេលនោះយើងនិងទទួលបាន DHCP មួយ។ ក្រោយមកយើងត្រូវ DisableInternet ជាមុនសិនដើម្បីឱ្យវាទទួល DHCP ។



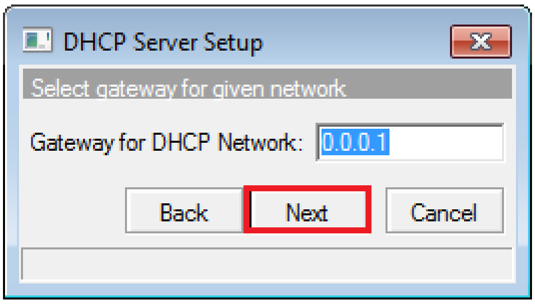
រូបភាពទី ៤.៣ Config DHCP

– ចុច Next



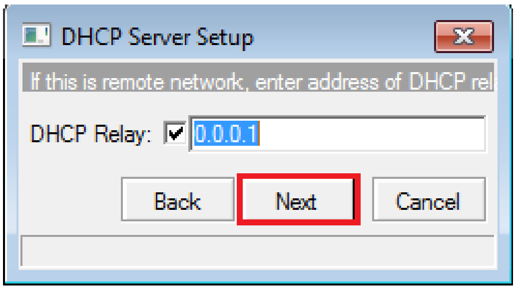
រូបភាពទី ៤.៤ DHCP Address Space

– ចុច Next



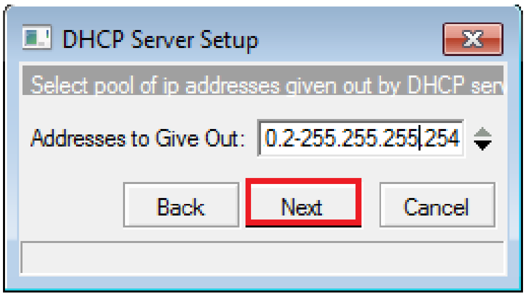
រូបភាពទី ៤.៥ Gateway for DHCP Network

– ចុច Next



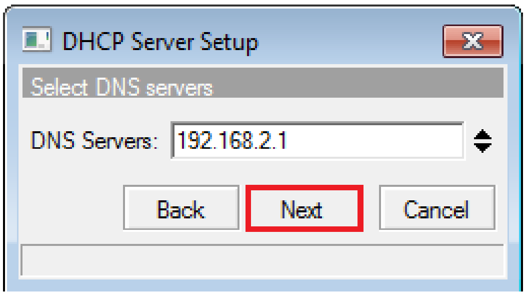
រូបភាពទី ៤.៦ DHCP Relay

- ចុច Next



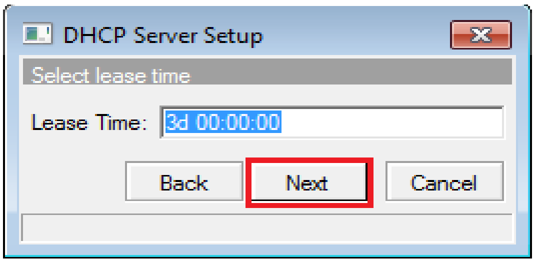
រូបភាពទី ៤.៧ Address to Give Out

- ចុច Next



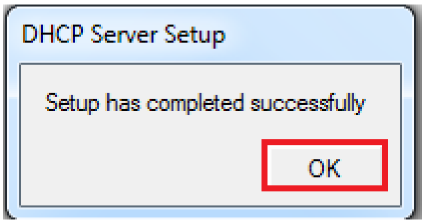
រូបភាពទី ៤.៨ DHCP Server

- ចុច Next



រូបភាពទី ៤.៩ Lease Time

- ចុច Ok ជាការស្រេច។



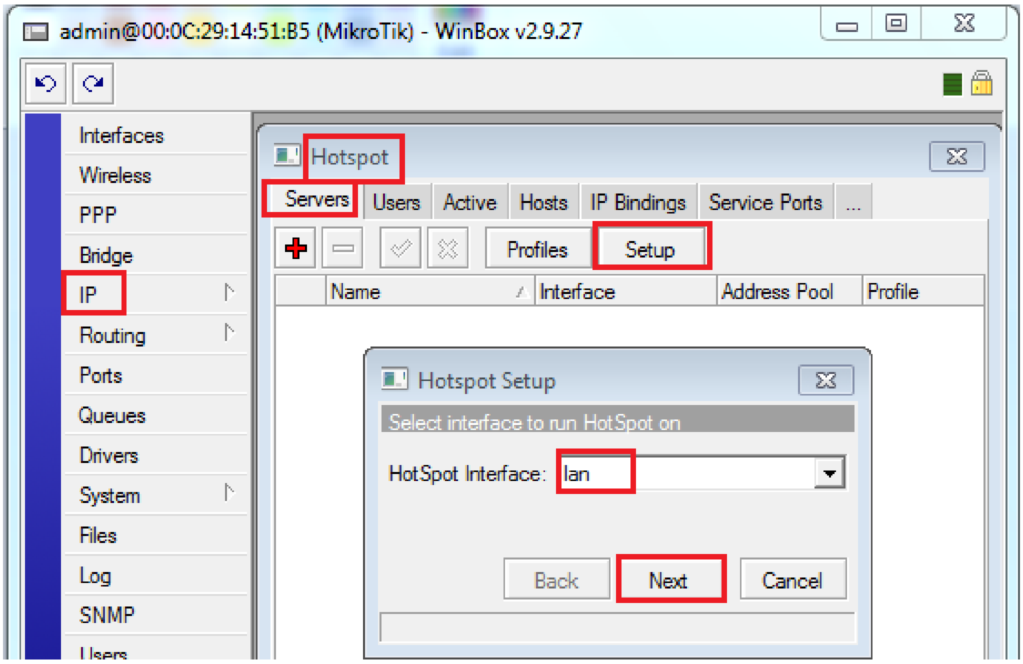
រូបភាពទី ៤.១០ បញ្ចប់ការ Config DHCP

៤.៣ រៀបចបង្កើត HostSport នៅលើ LAN

HotSport គឺជាអ្វី?

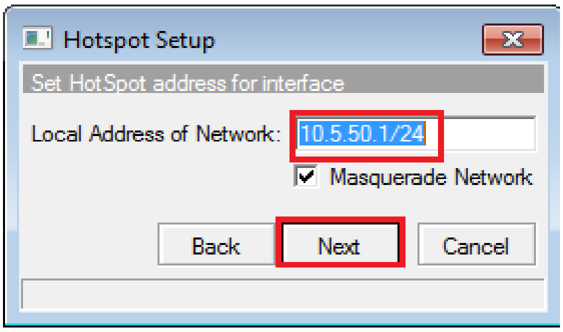
HotSport គឺជា Security មួយប្រើសម្រាប់នៅពេលដែល User ចង់ប្រើប្រាស់ Internet គឺត្រូវឆ្លងកាត់ការ Login ដោយប្រើប្រាស់ User Name និង Password ដែលកំណត់ដោយ User Admin នៅលើ MikroTik Router ដែលតម្រូវឱ្យអ្នកប្រើប្រាស់ Internet មាន User Name និង Password ទើបអាចទទួលបាន Internet ដើម្បីប្រើប្រាស់តាមតម្រូវការបាន។

ដើម្បីធ្វើ Hot Sport នៅលើ Router របស់យើងបាន យើងត្រូវចូលទៅ => IP => HotSport => HotSport Setup នៅពេលនោះវានឹងលោតផ្ទាំងមួយសម្រាប់ឱ្យយើងជ្រើសរើស Interface ក្រោយមកយើងត្រូវ ជ្រើសយក Interface LAN ចុច Next => Local Address of Network ចុច Next => Address Pool of Network ចុច Next => Select Certificate យើងយក none ចុច Next => IP Address of SMTP (Simple Mail Transfer Protocol) ចុច Next => DNS Server ចុច Next => DNS Name ឧទាហរណ៍ www.hotsport.com ចុច Next => Create Local HotSport User ក្រោយមកយើងត្រូវ បង្កើត User Admin និងដាក់ password ឱ្យវា រួចចុច Next។ ក្រោយមកយើងមាន User មួយ ។ បើយើងចូល => Server profile Tab យើងនឹងឃើញ Host Sport ដែលយើងទើបបង្កើត និងមួយទៀតជា default យើងធ្វើការ Double click on Server ដែលយើងទើបបង្កើត ពេលនោះយើងនឹងអាចធ្វើការកំណត់និងកែប្រែបានដូចជាឈ្មោះ password ឬកំណត់នូវការ ចងចាំ Password ពេល User Login ផងដែរ។



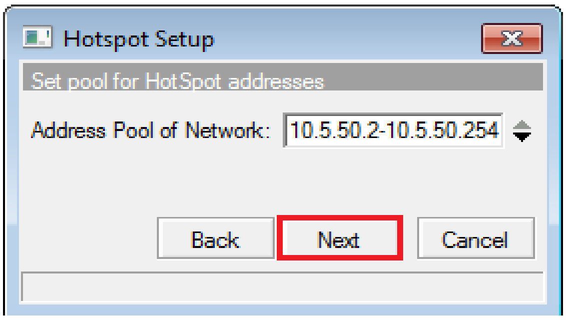
រូបភាពទី ៤.១១ ការបង្កើត HotSpot

- LAN ចុច Next => Local Address of Network



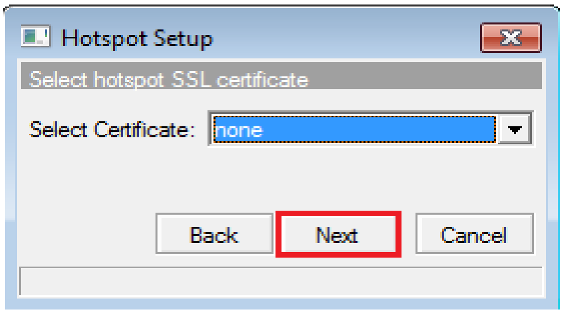
រូបភាពទី ៤.១២ Local Address of Network

- ចុច Next => Address Pool of Network



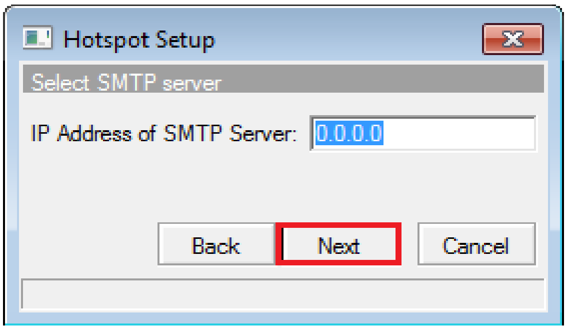
រូបភាពទី ៤.១៣ Address Pool of Network

- ចុច Next => Select Certificate យើងយក none



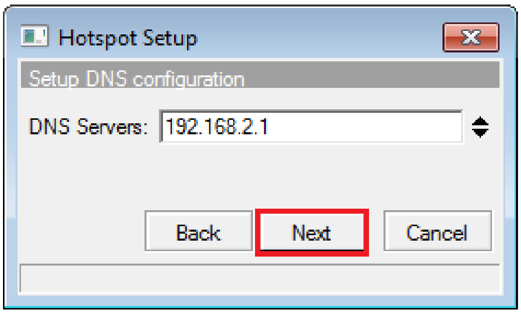
រូបភាពទី ៤.១៤ Select Certificate

- ចុច Next => IP Address of SMTP (Simple Mail Transfer Protocol)



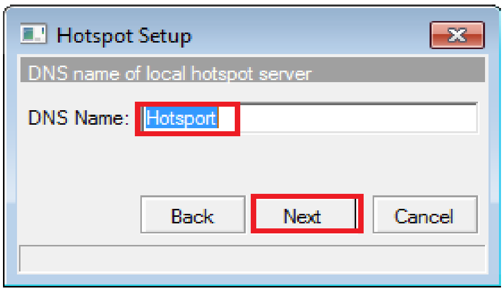
រូបភាពទី ៤.១៥ IP Address of SMTP

- ចុច Next => DNS Server



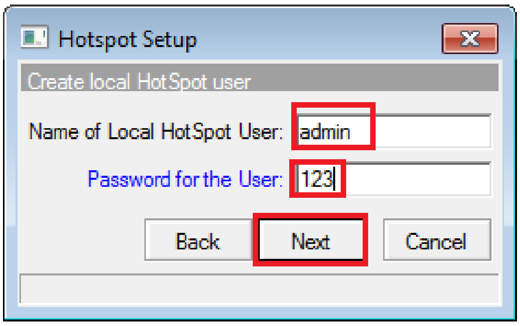
រូបភាពទី ៤.១៦ ដាក់ DNS Server

- ចុច Next => DNS Name ឧទាហរណ៍ www.hotsport.com



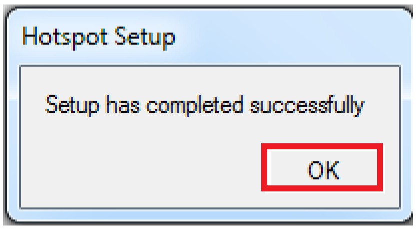
រូបភាពទី ៤.១៧ ដាក់ឈ្មោះ DNS

- ចុច Next => Create Local HotSport User ក្រោយមកយើងត្រូវ បង្កើត User Admin និង ដាក់ password ឱ្យវារួចចុច Next។



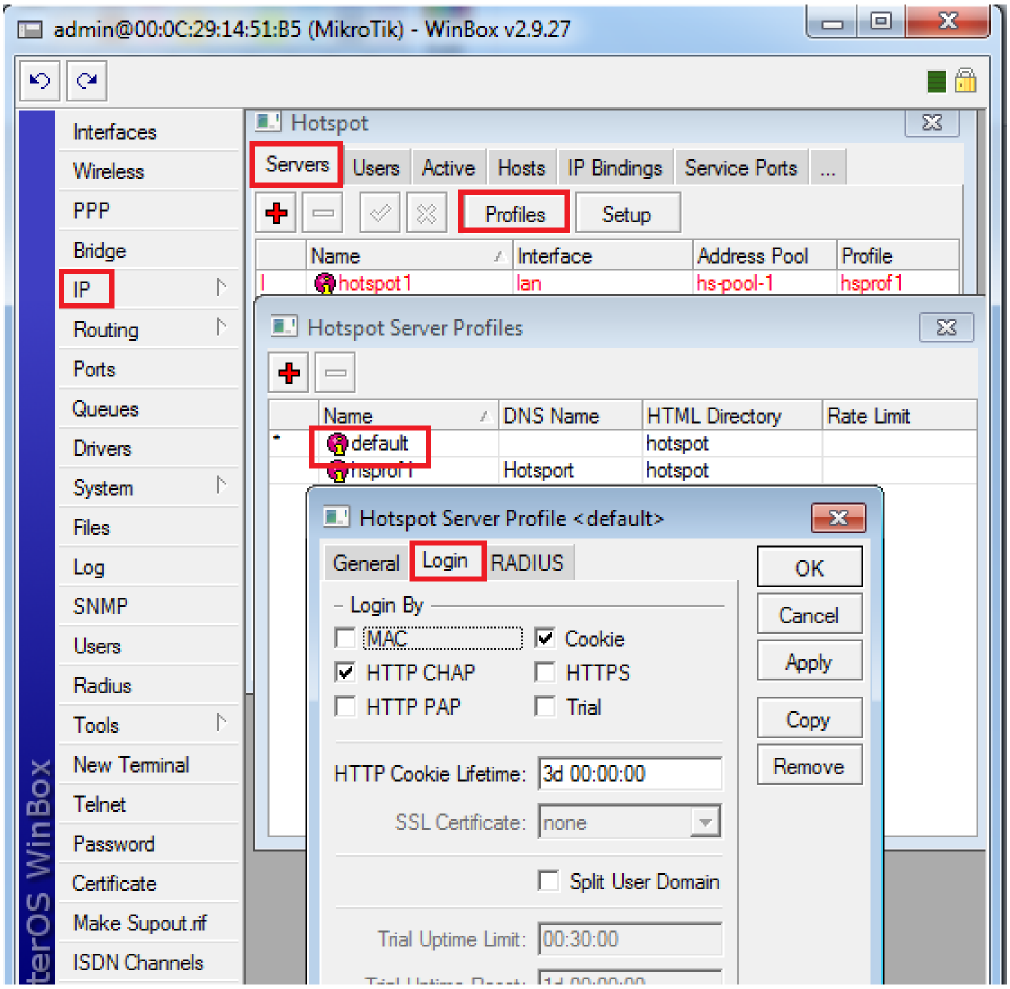
រូបភាពទី ៤.១៨ បង្កើត User HotSpot

- ចុច Ok ជាការស្រេច



រូបភាពទី ៤.១៩ បញ្ចប់ការបង្កើត HotSpot

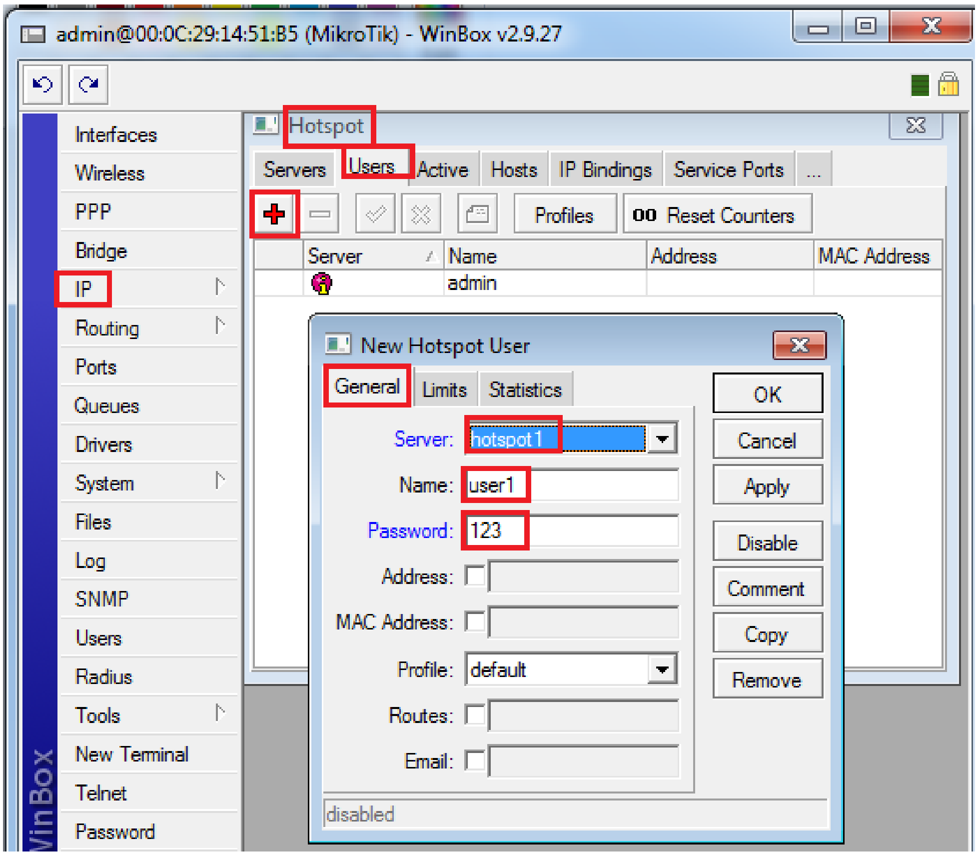
បើយើងចូល => Server profile Tab យើងនឹងឃើញ Host Sport ដែលយើងទើបបង្កើត និង មួយទៀតជា default យើងធ្វើការ Double click on Server ដែលយើងទើបបង្កើត ពេលនោះយើងនឹង អាចធ្វើការកំណត់ និងកែប្រែបានដូចជាឈ្មោះ password ឬកំណត់នូវការចងចាំ Password ពេល User login ផងដែរ។



រូបភាពទី ៤.២០ ការកំណត់ User Login

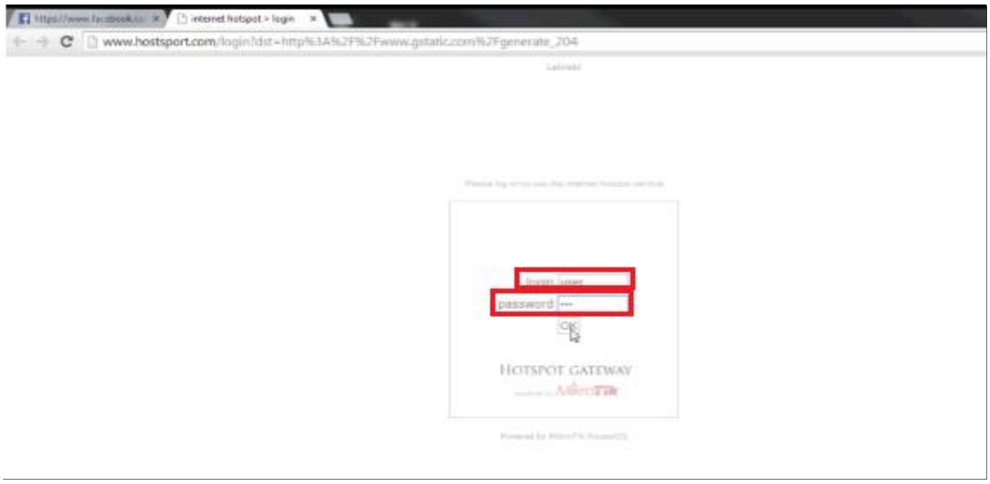
ក្រោយមកយើងឃើញ User Admin របស់យើងដែលយើងបានបង្កើតពីដំបូងតែយើងត្រូវបង្កើត User ធម្មតាមួយទៀតដែលមិនមានសិទ្ធិ ដូចជា User Admin។

យើងចូល Add ធ្វើការរើសយក Server ដែលយើងត្រូវកំណត់ (HotSport) ហើយឈ្មោះ User និង Password ចង់ដាក់អ្វីតាមចិត្ត។ ក្រោយពីការបង្កើតនិងធ្វើការកំណត់ផ្សេងៗរួចយើងត្រូវ Restart MikroTik របស់យើងមួយសិនដើម្បីឱ្យវា Refresh Configurations របស់យើង។



រូបភាពទី ៤.២១ ការបង្កើត User ធម្មតានៅលើ HotSpot

ក្រោយពីការបង្កើត និងធ្វើការកំណត់ផ្សេងៗរួចយើងត្រូវ Restart MikroTik របស់យើងមួយសិនដើម្បីឱ្យវា Refresh Configurations របស់យើង។ ក្រោយពីការ Restart កុំព្យូទ័ររបស់យើងមិនអាចប្រើ Internet បានទេលុះត្រាតែមាន User and Password ទើបអាចប្រើប្រាស់ Internet បាន។

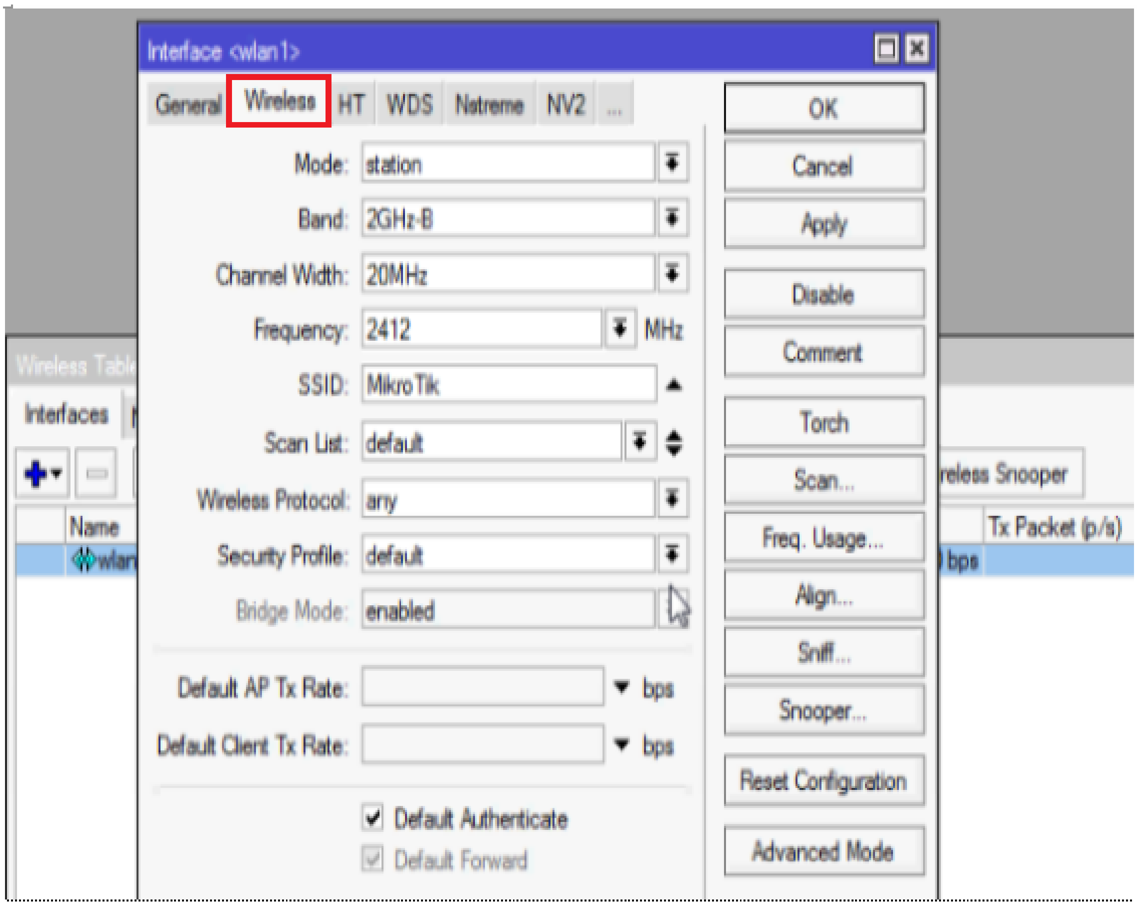


រូបភាពទី ៤.២២ Interface សម្រាប់ Login នៅលើ HotSpot

៤.៤ របៀបបង្កើត Host Sport លើ Wireless

ដើម្បីបង្កើត Host Sport នៅលើ Wireless បានយើងត្រូវធ្វើតាមជំហ៊ានៗដូចខាងក្រោម÷

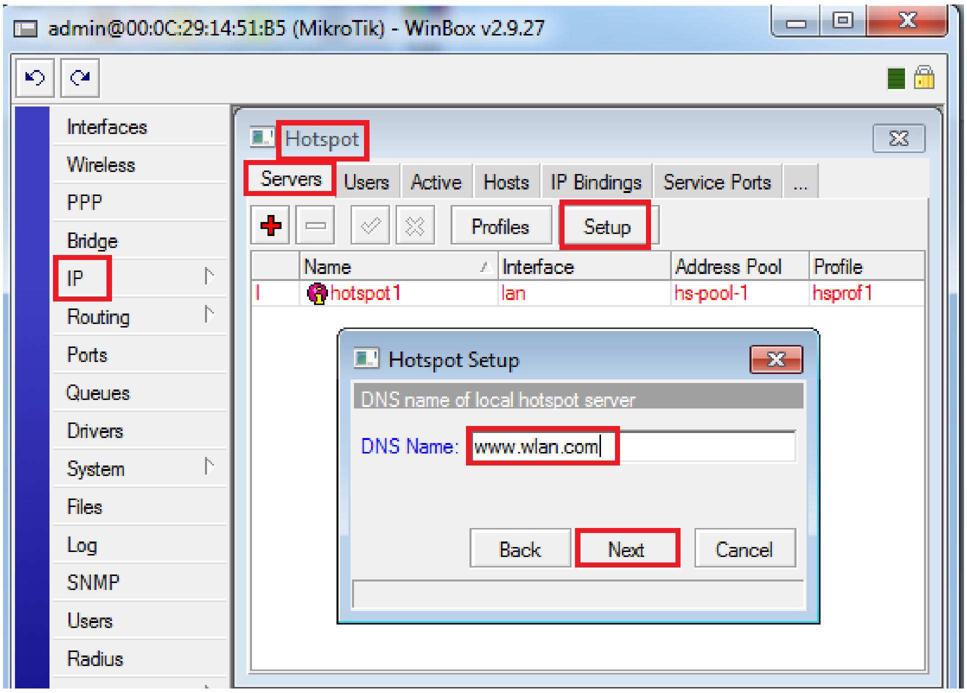
=>Wireless Tool => Interface => Enable Wireless => Double Click ដើម្បីចូលទៅដាក់ Name and Password => Wireless Tab => SSID ដើម្បីប្តូរឈ្មោះ។



រូបភាពទី ៤.២៣ ការបង្កើត HotSpot នៅលើ Wireless

ក្រោយមកយើងចូល IP => Host Sport => Host Sport Setup => Host Sport => Interface ធ្វើការ Select Interface WLan => Local Address Of Network => Address Pool Of Network ចុច Next => Select Certificate យក none => IP Address of SMTP Server => DNS Server => DNS Name ។

ឧទាហរណ៍: www.wlan.com => User ដើម្បីបង្កើត User មួយទៀត => User => Add Server យក Host Sport Wlan រួចកំណត់ password Apply => OK គឺជាការស្រេច។



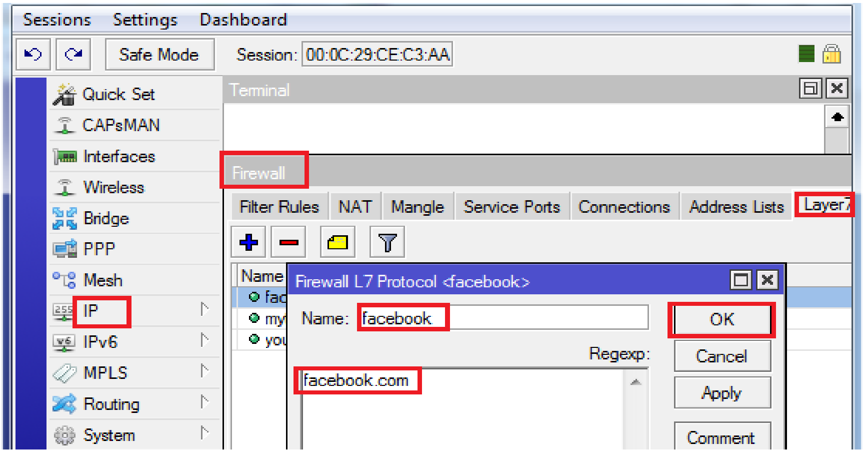
រូបភាពទី ៤.២៤ បញ្ចប់ការបង្កើត HotSpot នៅលើ Wireless

មេរៀនទី ៥

កំណត់ដំណើរការមួយឆ្លងកាត់ MikroTik

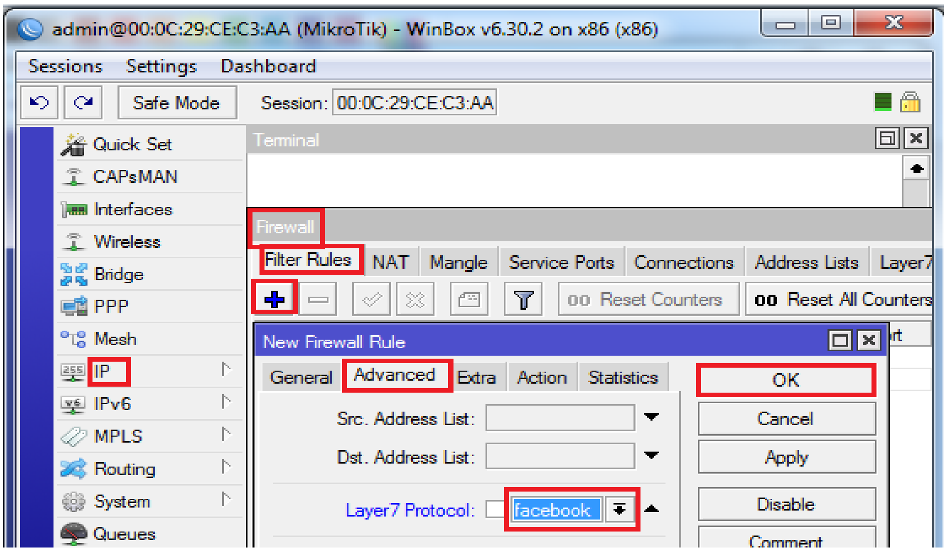
៥.១ របៀប Block Website នៅលើ Layer 7

ដើម្បី Block Website នៅលើ Layer 7 ជាដំបូងយើត្រូវ ចូលទៅកាន់ IP => Firewall ពេលនោះវានឹងបង្ហាញផ្ទាំងមួយដូចរូបខាងក្រោម÷



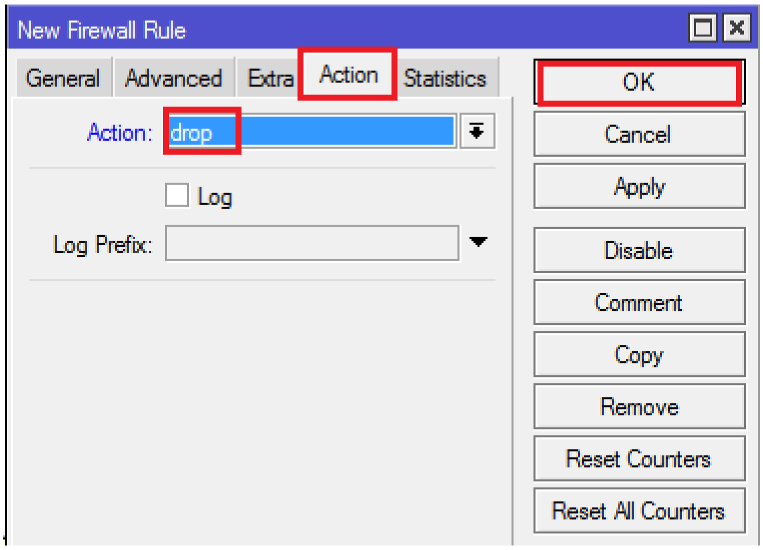
រូបភាពទី ៥.១ របៀប Block Website On Layer 7

ក្រោយមកយើងចូល Layer 7 Protocol ចុច Add បន្ទាប់មកវានឹងចេញផ្ទាំងមួយទៀតសម្រាប់ឱ្យយើងដាក់ឈ្មោះ Website ដែលយើងចង់ block ឧទាហរណ៍: facebook។ ហើយនៅក្នុង Regexp គឺជាកន្លែងសម្រាប់បញ្ចូល Address នៃ Website ដែលយើងចង់ Block ឧទាហរណ៍: www.facebook.com។



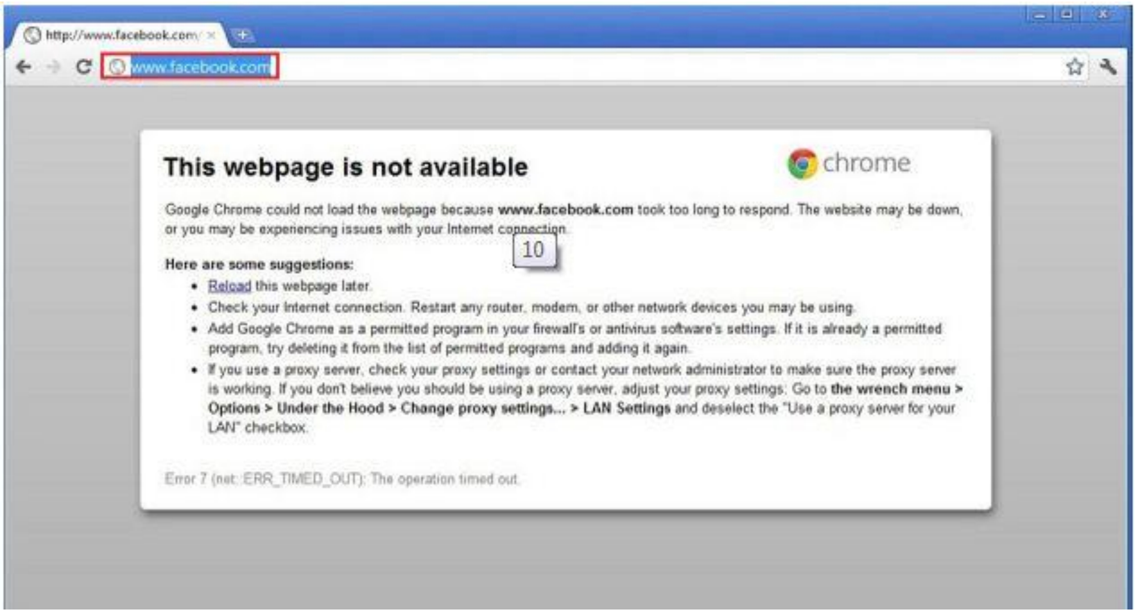
រូបភាពទី ៥.២ ការបញ្ចូល URL ដើម្បីធ្វើការ Block

ក្រោយមកយើងចូលក្នុង Filter Rules ចុច Add => Advanced => Layer7 Protocol យើងយកឈ្មោះ Website ដែលយើងបានកំណត់ (youtube) បន្ទាប់មកទៀតចូល Action យើងរើសយក drop => Apply and Ok។ ដល់ដំណាក់កាលនេះគឺយើងអាចធ្វើការសាកល្បងបានហើយ។ តែចំណុចមួយទៀតដែលយើងត្រូវធ្វើវាបន្ទាប់គឺ ការដាក់ Comment ដើម្បីឱ្យយើងងាយស្រួលនៅពេលដែលយើងចង់លុប កែ ឬ Disable និង Enable នៅលើ Drop of Website ណាមួយដោយត្រឹមត្រូវមិនអាចច្រឡំបានឡើយ។ ដូចនេះដើម្បីកំណត់ឈ្មោះបាន យើងត្រូវចូលនៅក្នុង Filter Rules ធ្វើការ double click drop ណាមួយដែលយើងចង់កំណត់រួចចូល Comment រួចបញ្ចូលឈ្មោះ website of drop => Apply and Ok។



រូបភាពទី ៥.៣ ការកំណត់សិទ្ធិ Cleints ទៅលើ URL

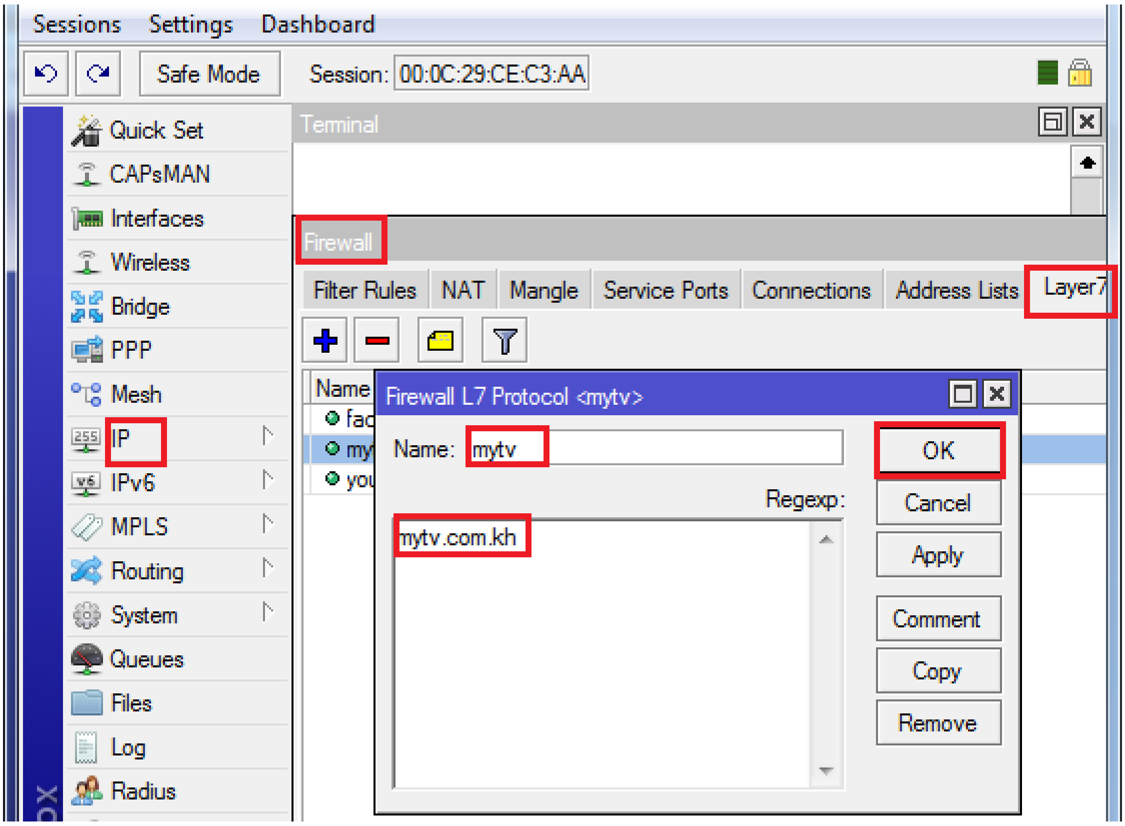
ជាចុងក្រោយយើងនឹងធ្វើការបន្តទៅបើក Browser ហើយចូលទៅ Website facebook: www.facebook.com នោះវានឹង Block Webpage នេះថា This webpage is not available មានន័យថា Webpage នេះត្រូវបាន Block ដោយជោគជ័យ។



រូបភាពទី ៥.៤ លទ្ធផលនៃការ Block

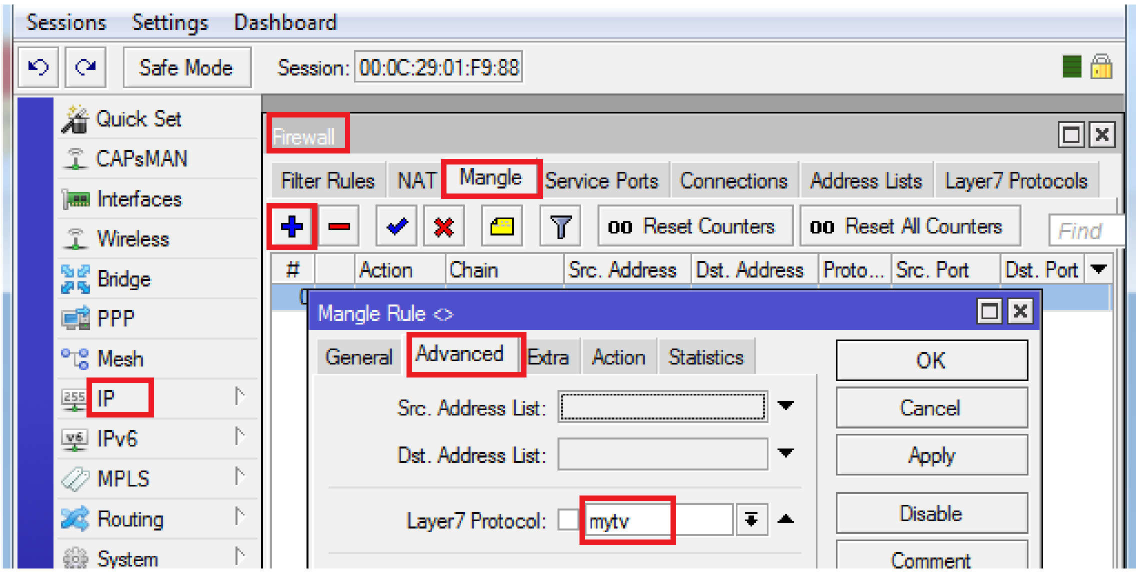
៥.២ ការកំណត់ល្បឿនសម្រាប់ដំណើរការនៅលើ Websites

ជាដំបូងយើងចូល IP => Firewall => Layer7 Protocol ធ្វើការដាក់ឈ្មោះ ឧទាហរណ៍: mytv និងដាក់ Address ឧទាហរណ៍: mytv.com.kh រួចចុច OK ។



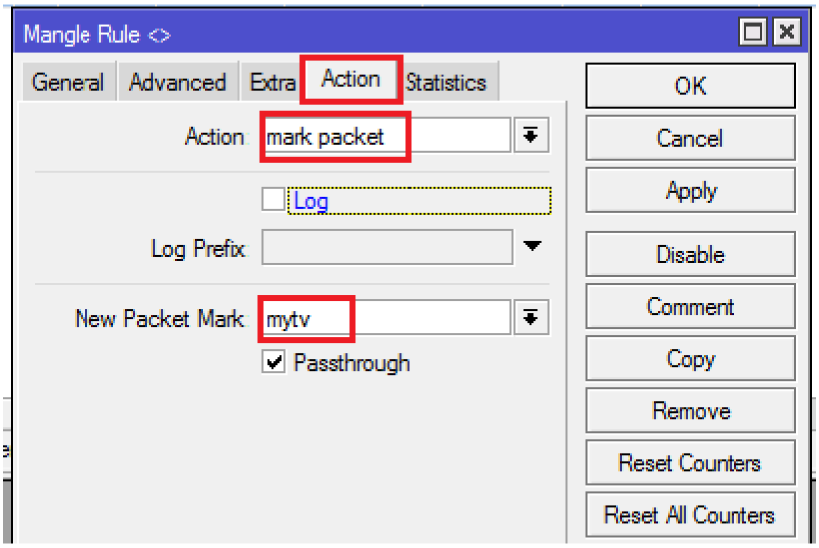
រូបភាពទី ៥.៥ របៀបកំណត់ល្បឿននៅលើ Websites

បន្ទាប់មកយើងចូល Mangle => Add => General យើងយក Prerouting => Advanced Layer7 Protocol យើងរើសយកឈ្មោះ Website ដែលយើងបានកំណត់គឺ mytv => Action រើសយក mark packet ហើយនៅត្រង់ New Packet Mark ជាកន្លែងដែលត្រូវបញ្ចូលឈ្មោះ Website mytv ម្តងទៀតរួចចុច OK។



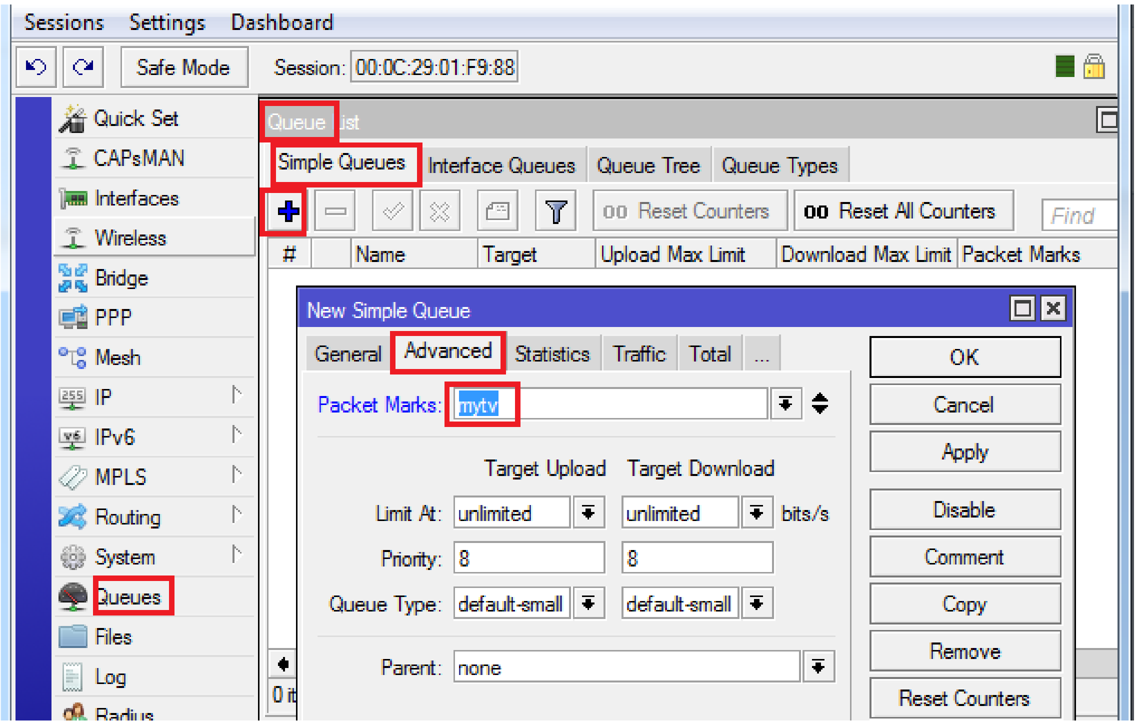
រូបភាពទី ៥.៦ ការកំណត់ឈ្មោះ URL ដើម្បីកំណត់ Speed

បន្ទាប់ទៀតយើងចូល IP => Firewall => Mangle => Add => advanced => Layer7 Protocol => mytv។



រូបភាពទី ៥.៧ ការកំណត់ Mangle Rule

បន្ទាប់មកទៀតយើងចូលក្នុង Queues => Simple Queues => Add => General ជាកន្លែងដែលសម្រាប់ឱ្យយើងដាក់ឈ្មោះ Website ឧទាហរណ៍ mytv។ ហើយនៅត្រង់ Target គឺជាកន្លែងកំណត់ IP នៅក្នុង LAN របស់យើងតែបើសិនយើងចង់កំណត់នៅលើ LAN ទាំងមូលតែម្តងគឺគ្រាន់តែយកតាម Default របស់វាគឺបានហើយ។ ឯនៅត្រង់ Target Upload និងនៅត្រង់ Target Download គឺជាកន្លែងសម្រាប់ឱ្យយើងធ្វើការកំណត់នូវល្បឿនរបស់ Website ដូចនេះយើងត្រូវធ្វើការកំណត់ទៅតាមតម្រូវការរបស់យើង។ ក្រោយមកយើងចូល Advanced ធ្វើការរើស ឈ្មោះ Website ដែលយើងបានកំណត់ពីមុនហើយនៅក្នុង Target Upload and Target Download គឺយើងត្រូវ រើសយកឱ្យដូច Target មុនរួចចុច Apply and OK ។ ក្រោយមកសូមធ្វើការសាកល្បង។



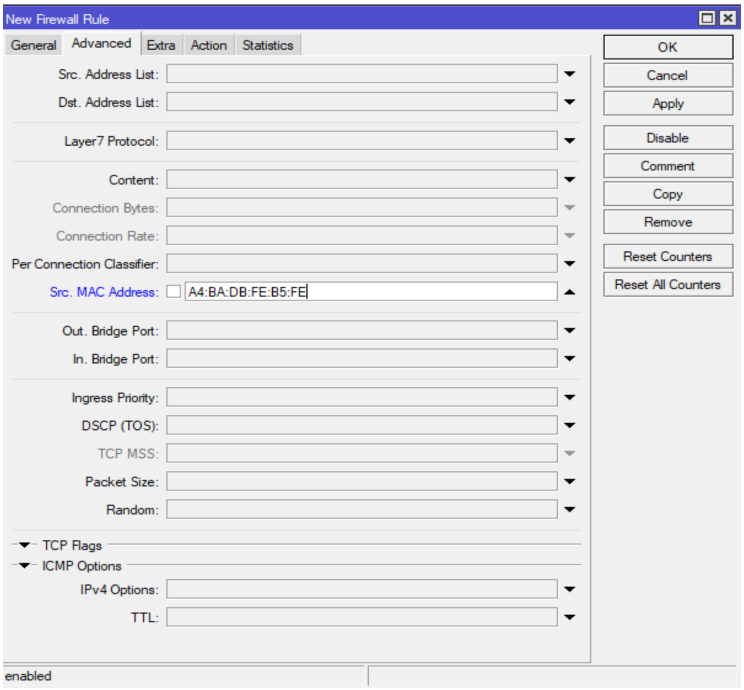
រូបភាពទី ៥.៨ ការដាក់ Speed

៥.៣ របៀប Blocked Host Device

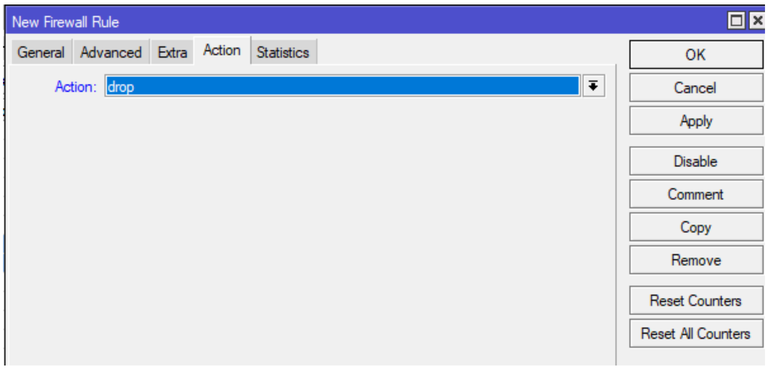
ក្នុងចំណុចនេះដែរគឺអាចធ្វើការ Block នូវឧបករណ៍ទាំងឡាយណាដែលបានភ្ជាប់មកជាមួយនឹងបណ្តាញ Network របស់យើង អាចដំណើរ Network បាន ឬមិនបាន ដោយការ Block នេះគឺយើងអាចធ្វើទៅបាន ២ របៀបដូចខាងក្រោម÷

៥.៣.១ Blocked តាមរយៈ Mac Address

ការ Block ឧបករណ៍តាមរយៈ MAC Address នេះគឺមានន័យថាយើងធ្វើការ Block ទៅលើឧបករណ៍មួយនោះខាច់ខាតគឺមិនអាចគេចចេញពីការ Block របស់យើងបានឡើយ តែវាមានពិបាកបន្តិចព្រោះយើងត្រូវតែស្គាល់ឧបករណ៍ដែលយើងចង់ធ្វើការ Block នោះឱ្យបានច្បាស់ហើយវាយបញ្ចូលនូវ MAC Address របស់វានោះឱ្យបានត្រឹមត្រូវ។ ភាគច្រើនដែលគេប្រើប្រាស់វិធីនៃការ Block នេះគឺសម្រាប់ទៅដូចជា Block WIFI, Block ម៉ាស៊ីនណាមួយដែលមើលឃើញថាធ្លាប់មានបញ្ហា, Block ទៅលើម៉ាស៊ីនណា Download ច្រើន ឬ Block ទៅលើម៉ាស៊ីនណាដែលយើងគិតថាគេបានលួច Hack ចូលប្រើប្រាស់បណ្តាញជាមួយយើង។



រូបភាពទី ៥.៩ វាយបញ្ចូល MAC Address ឧបករណ៍ណាដែលត្រូវ Block

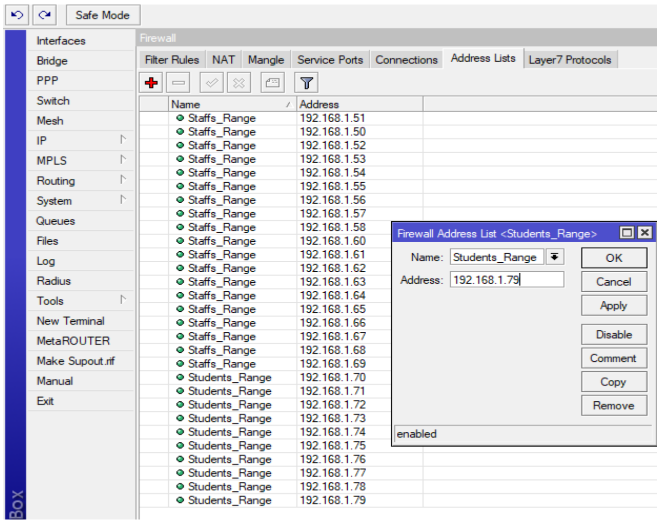


រូបភាពទី ៥.១០ ជ្រើសរើស Action

៥.៣.២ Blocked តាមរយៈ: IP Address

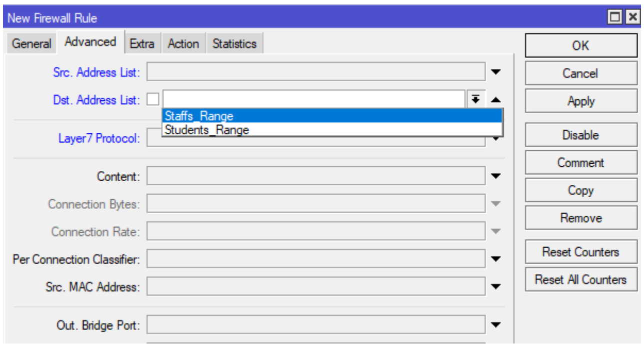
ការ Block ឧបករណ៍តាមរយៈ IP Address នេះគឺមានន័យថាយើងធ្វើការ Block ទៅលើ IP Address ចន្លោះពី IP Address ណាមួយទៅ IP Address ណាមួយទៀត ចេញពីលេខរៀងនៃ Network របស់យើង វាមិនមែនជាការ Block ទៅលើឧបករណ៍ណាមួយនោះទេព្រោះបើគេដឹងថាយើងធ្វើការ Block ចន្លោះពី IP Address ណាមួយនោះគេអាចប្តូរលេខ IP Address ម៉ាស៊ីនរបស់គេនោះ គេអាចជៀសផុតពីការ Block របស់យើងបាន។ ភាគច្រើនដែលគេប្រើប្រាស់វិធីនៃការ Block នេះគឺសម្រាប់ដូចជា Block ទៅលើការដាក់ Static IP Address ដែលកំណត់ដោយក្រុមហ៊ុនហើយ User មិនអាចប្តូរ IP Address បាន ឬ Block ទៅលើម៉ាស៊ីនណាដែលចាប់ IP Address តាម DHCP Server ជាដើម។

១. សូមចូលទៅកាន់ Firewall => Address List => Click on Add (✚) ហើយបំពេញលេខរៀង IP Address ជាមួយនឹងឈ្មោះរបស់លេខរៀង IP Address នោះដូចរូបខាងក្រោម÷

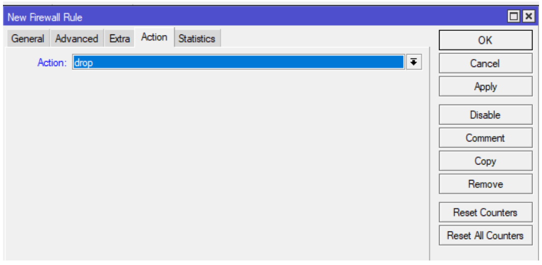


រូបភាពទី ៥.១១ បង្កើត Address List

២. សូមចូលទៅកាន់ Firewall => Filter Ruls=> Click on Add (✚) ហើយជ្រើសរើសខាងក្រោម÷



រូបភាពទី ៥.១២ ជ្រើសរើសឈ្មោះ Address List

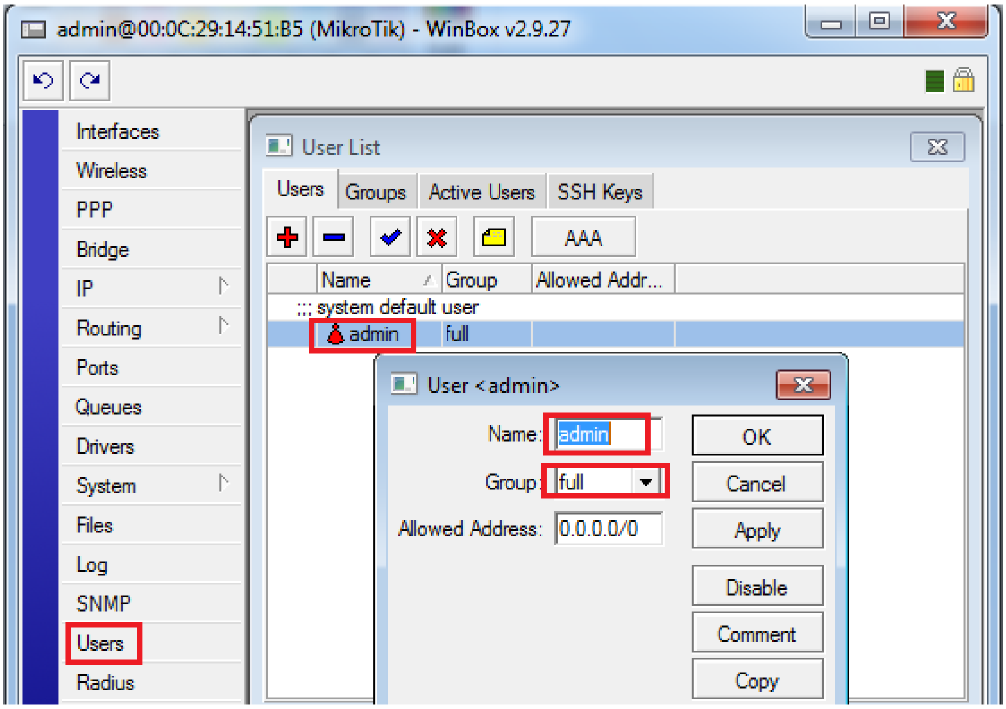


រូបភាពទី ៥.១៣ ជ្រើសរើស Action

៥.៤ របៀប Setup Web Proxy

ការ Setup Web Proxy គឺធ្វើដើម្បីគ្រប់គ្រងលើប្រព័ន្ធសុវត្ថិភាព នៅលើ Internet ដែលមានតួនាទី Block Website, Firewall, Monitor User។ ដូចនេះ យើងខ្ញុំនឹងធ្វើការដំឡើង Web Proxy នៅលើកម្មវិធី Winbox ដូចខាងក្រោមនេះ÷

ដំបូងយើងធ្វើការ Login ជា User Admin សម្រាប់ចូល Winbox ដូច្នេះយើងធ្វើការចូលតែម្តង។

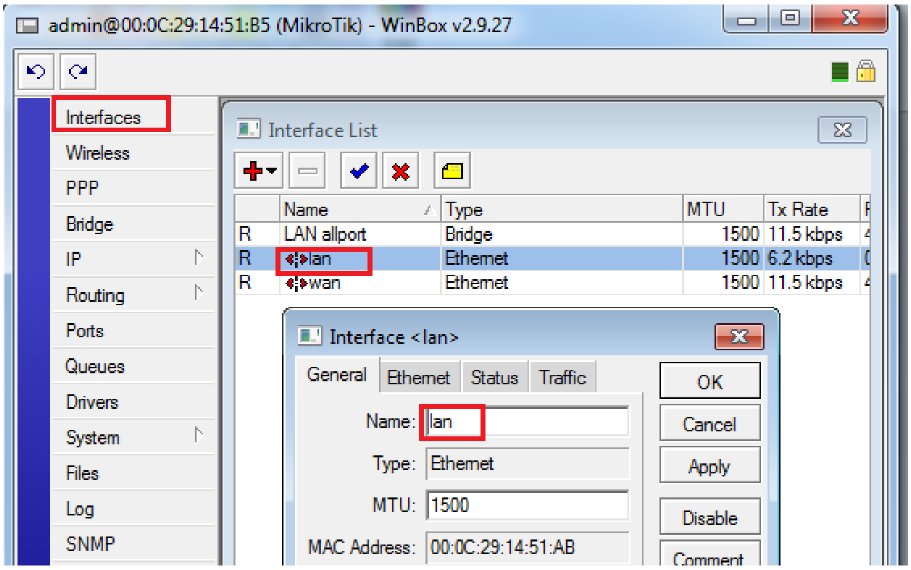


រូបភាពទី ៥.១៤ របៀប Setup Web Proxy

យើងនឹងឃើញ Interface Winbox។ យើងធ្វើការចូល ទៅ Tools Interface នឹងឃើញពាក្យថា Interface List ដូចខាងក្រោម÷

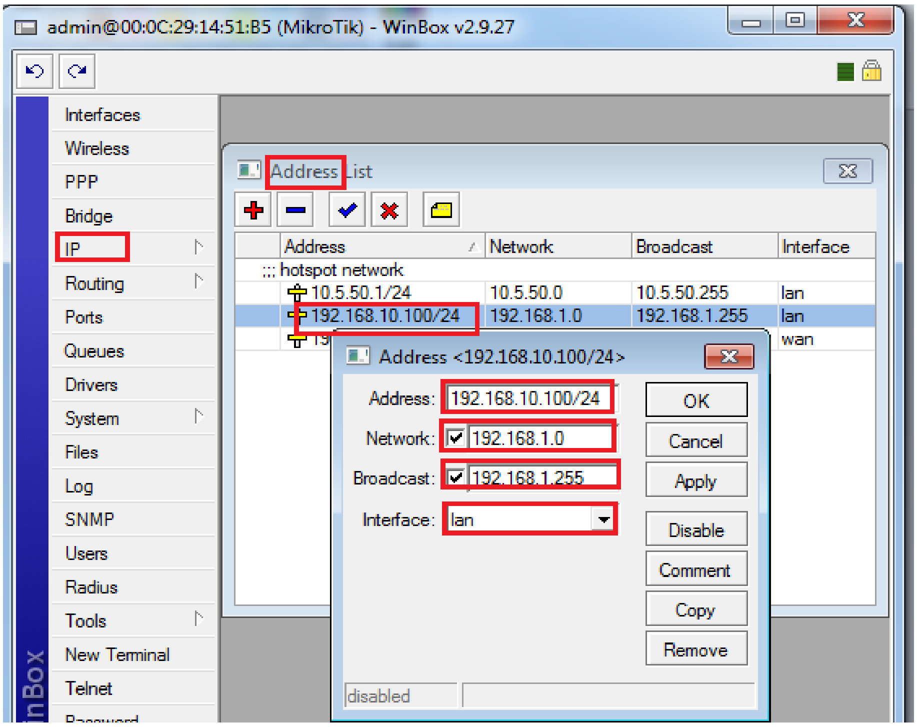
- Lan
- Wan

LAN ដែលមាន Mac Address 00:0C:29:14:51:AB។ ឯ WAN ក៏មាន Mac Address របស់វាដែរ។



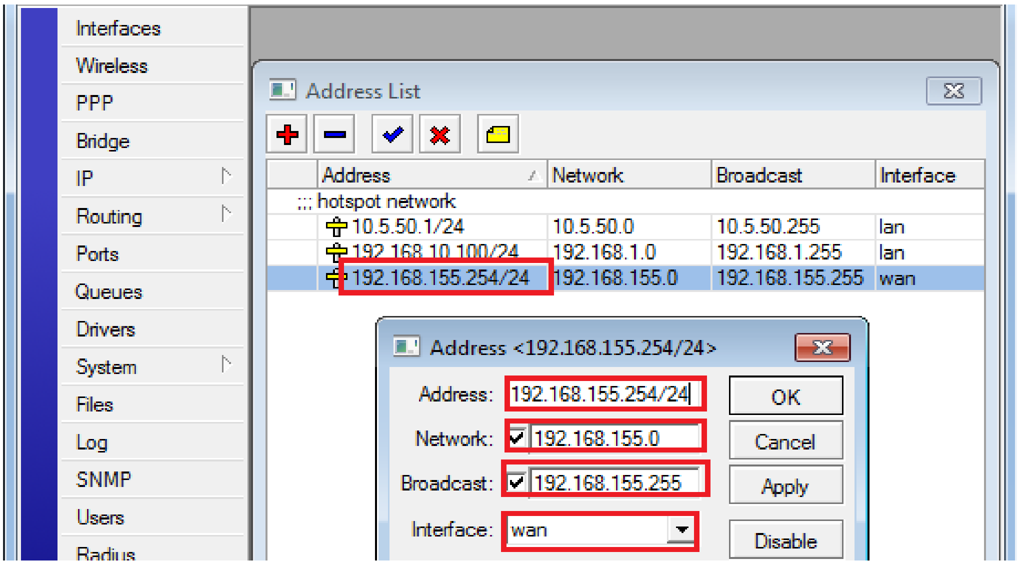
រូបភាពទី ៥.១៥ ការ Config នៅលើ LANs

បន្ទាប់មកទៀតយើងនឹងចូល Tools Address។ Address List នេះគឺ យើងបានកំណត់ IP Address, Network Address និង Broadcast ឱ្យវារួចរាល់ហើយ ដើម្បីសម្គាល់ IP Lan។



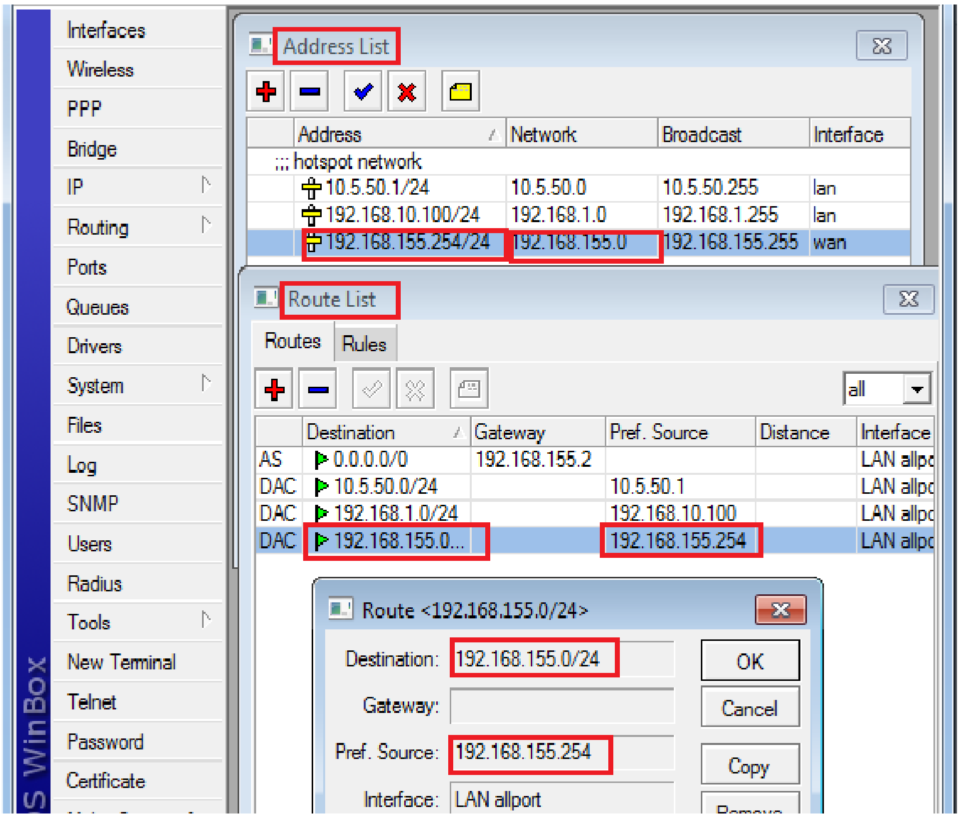
រូបភាពទី ៥.១៦ ការកំណត់ IP Address នៅលើ LANs

នេះជា Address របស់ WAN ដែលជា Public IP ដើម្បីឱ្យកុំព្យូទ័រអាចប្រើប្រាស់ Internet បាន។



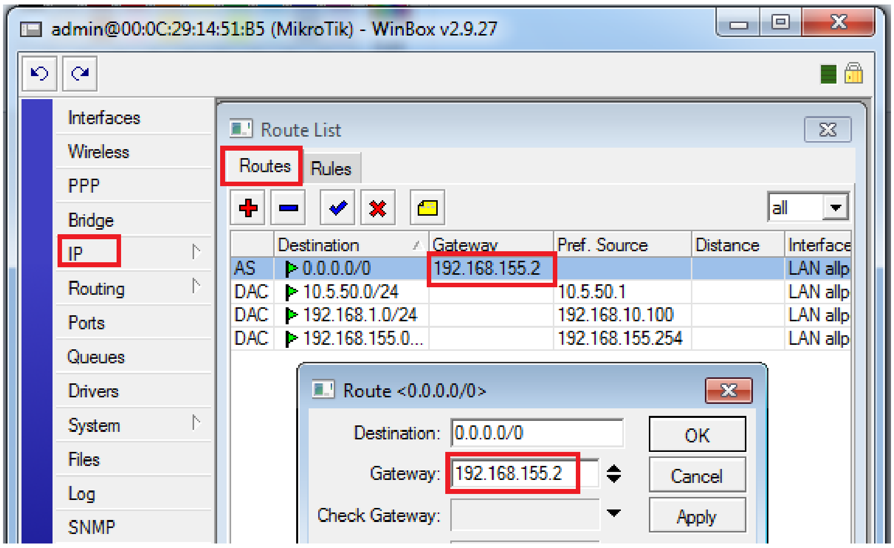
រូបភាពទី ៥.១៧ ការកំណត់ IP Address នៅលើ WANs

ដូច្នេះយើងធ្វើការ Routes ដើម្បីឱ្យ LAN និង WAN ដោយធ្វើការបន្ថែម ឬក៏បង្កើត Route ថ្មី IP Gateway ហើយ Apply និង OK ជាការស្រេច។



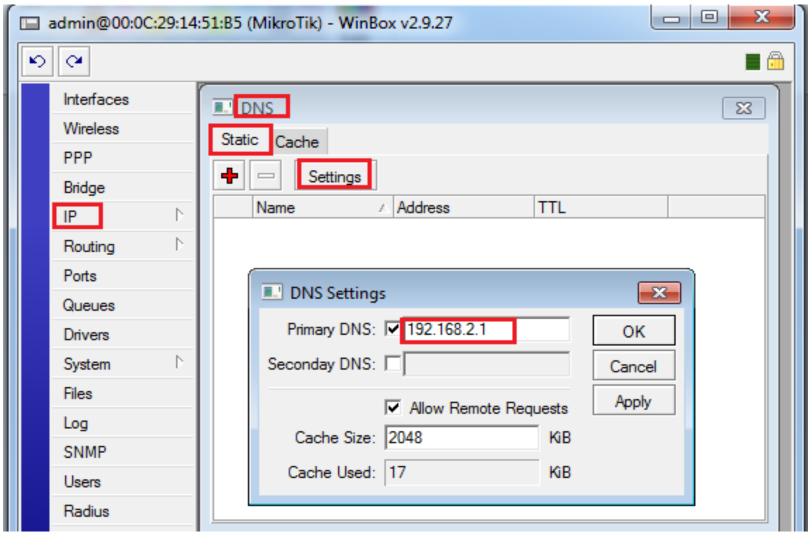
រូបភាពទី ៥.១៨ កំណត់ IP ដើម្បី Route

LAN ដែលយើងធ្វើការ Routes ឱ្យ LAN ក្នុង Network តែមួយស្គាល់គ្នាយើងត្រូវដាក់ IP Gateway ចូលទៅហើយ OK ជាការស្រេច។



រូបភាពទី ៥.១៩ Routing

បន្ទាប់មកទៀតយើងចូលទៅ IP => DNS => Setting ដើម្បីកំណត់ Primary DNS ដោយវាយបញ្ចូល IP DNS ហើយ Apply និង OK ជាការស្រេច។

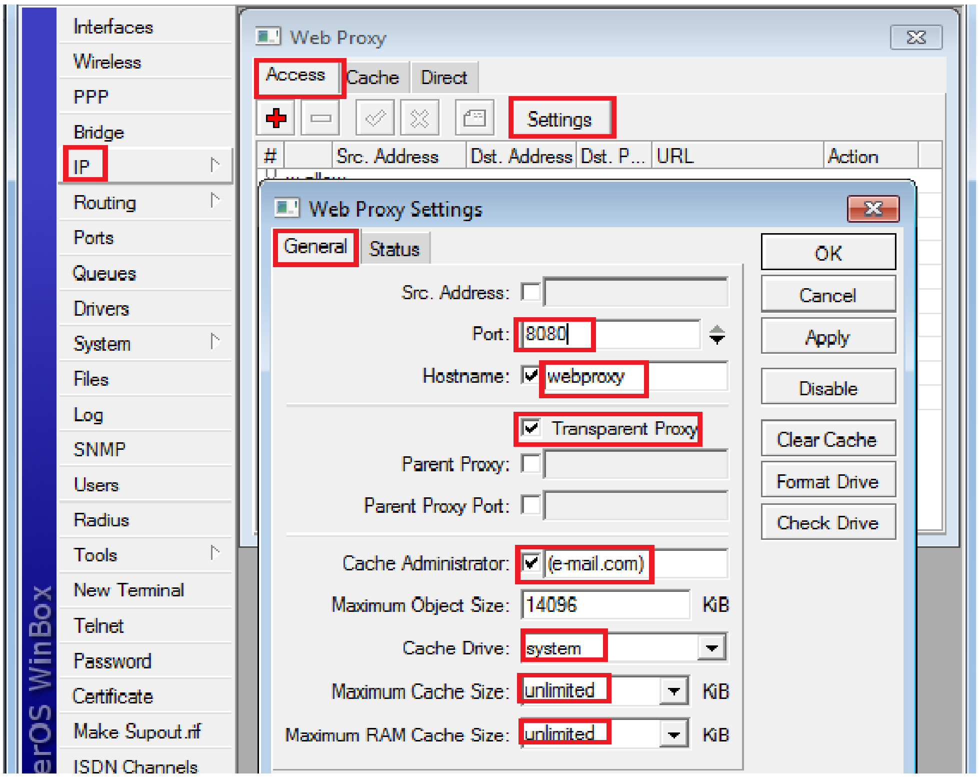


រូបភាពទី ៥.២០ កំណត់ Primary DNS

យើងចូលទៅ Web Proxy ដើម្បីកំណត់នូវមុខងារមួយចំនួនដូចខាងក្រោម÷

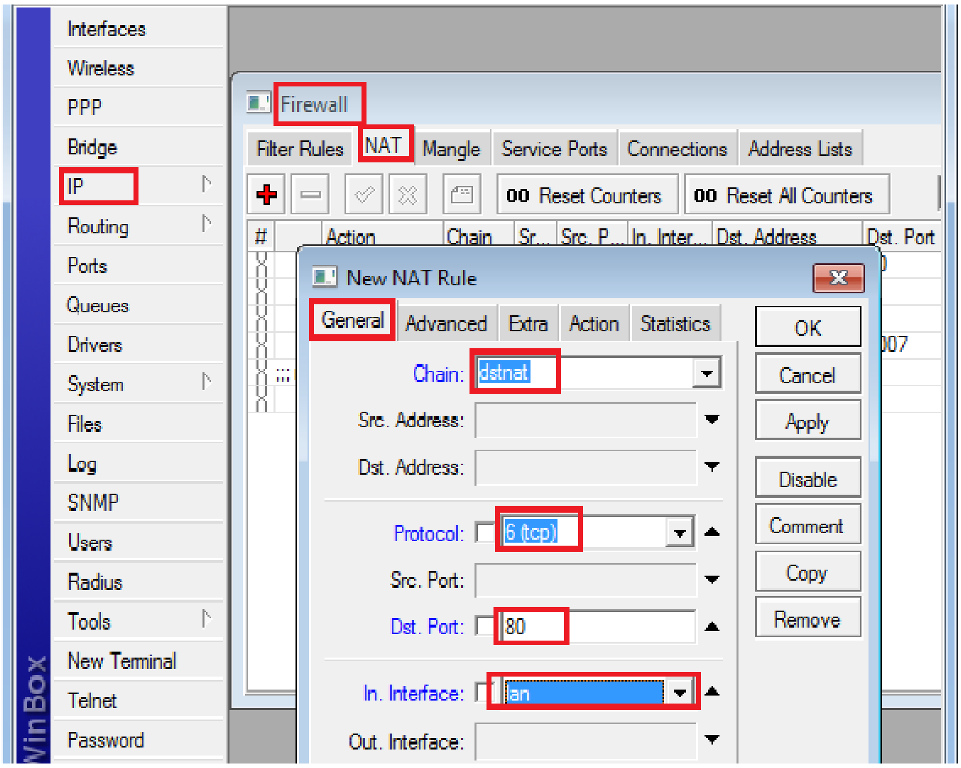
ដំបូងយើងចូលទៅ IP => Web Proxy => Access => Setting ក្រោយពីការចូលទៅ Setting វាលោតផ្ទាំងមួយជា Web Proxy Settings ដូច្នេះយើងធ្វើការកំណត់មុខងាររបស់វានៅក្នុង Interface នេះ។

យើងធ្វើការកំណត់នូវ Port 8080 ដែលជា Port Default, Hostname: Web proxy, Cache Administrator ដើម្បីភ្ជាប់ទៅ Administrator: (E-mail.com) ក្រៅពីនេះត្រូវមើល Interface ខាងក្រោម



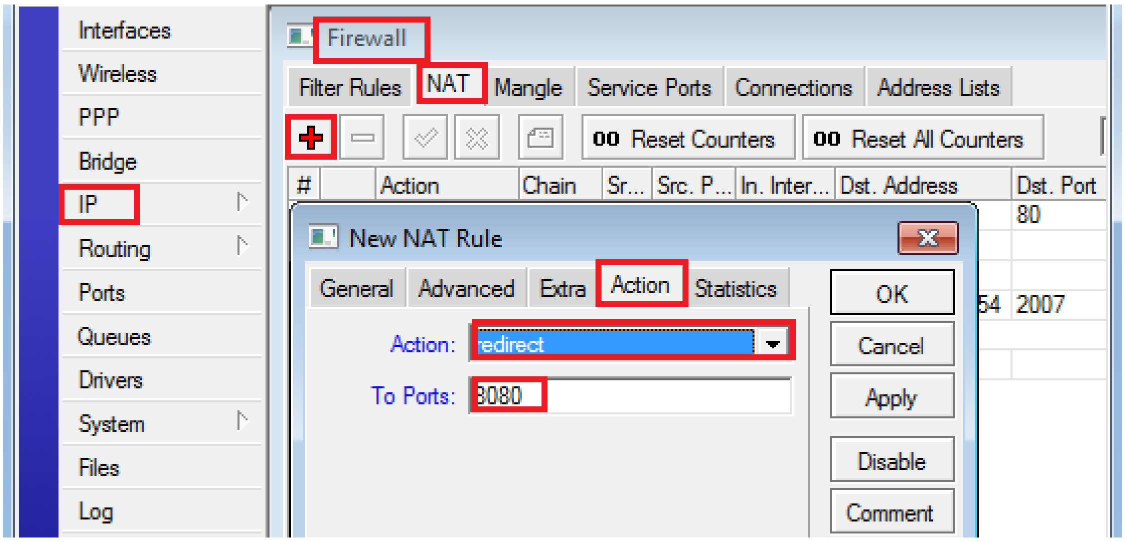
រូបភាពទី ៥.២១ ការកំណត់នូវមុខងារ

យើងចូលទៅ Firewall ដើម្បី Configure NAT ឱ្យមាន Internet ប្រើប្រាស់។ ចូលទៅ IP => Firewall => NAT => Add NAT Rule យើងមាន Interface មួយថ្មី យើងកំណត់តាមរូបខាងក្រោម។



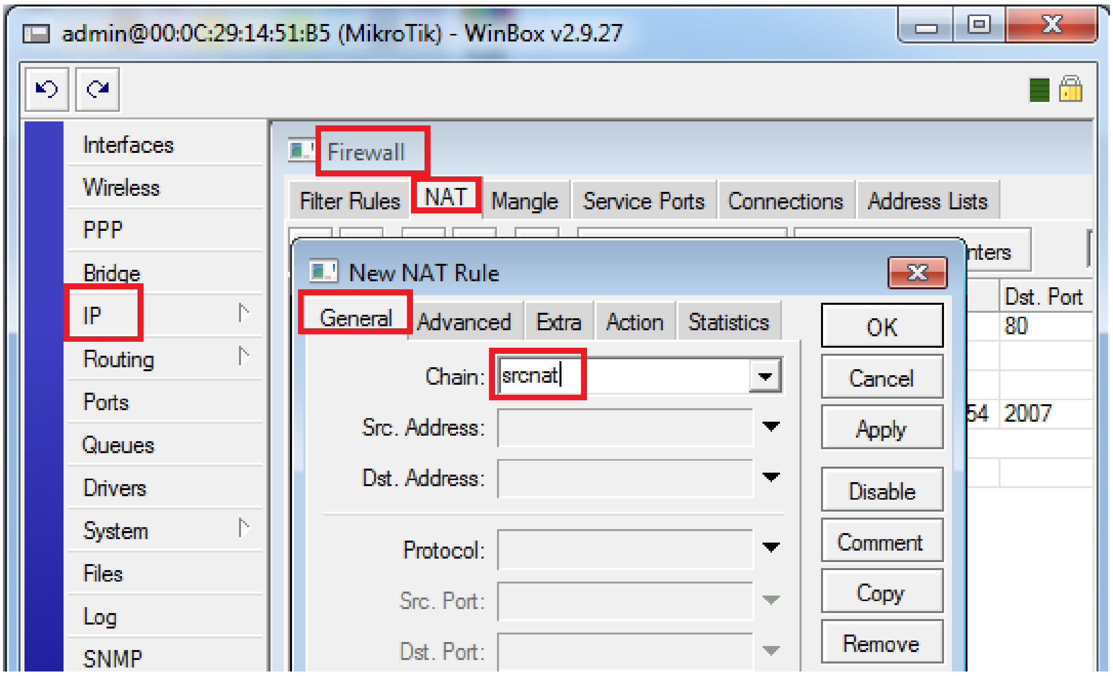
រូបភាពទី ៥.២២ Configure NAT

ហើយបន្ទាប់មកចូល Action ជ្រើសរើសពាក្យថា Redirect និង Port 8080 ហើយចុច OK ជាការស្រេច។



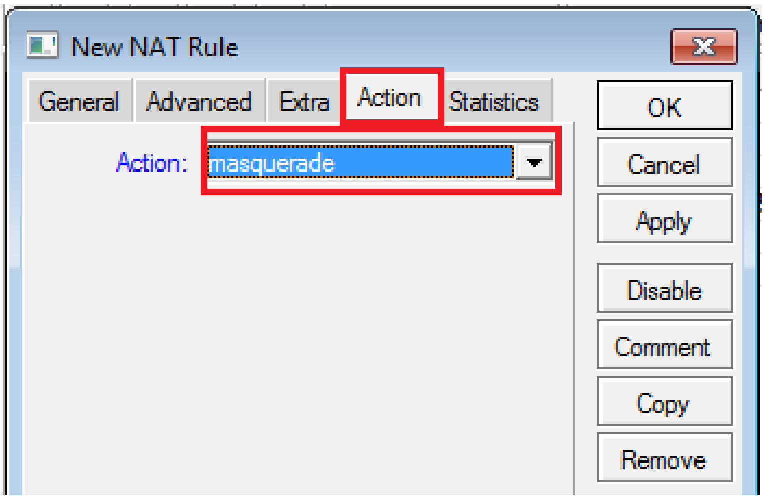
រូបភាពទី ៥.២៣ Redirect Action

នេះយើងបង្កើត srcnat មួយទៀតចូលទៅក្នុង Firewall ហើយធ្វើដូចរូបខាងក្រោម÷



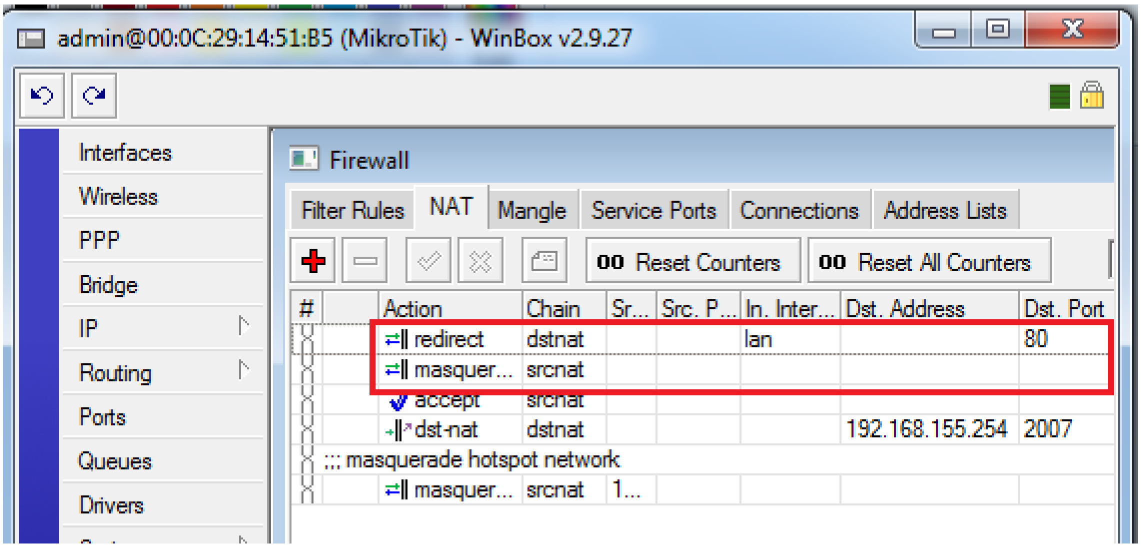
រូបភាពទី ៥.១២៤ Configure NAT Firewall

បន្ទាប់មកចូលពាក្យថា Action និង Select យក masquerade ដើម្បីឱ្យមាន Internet ប្រើប្រាស់។



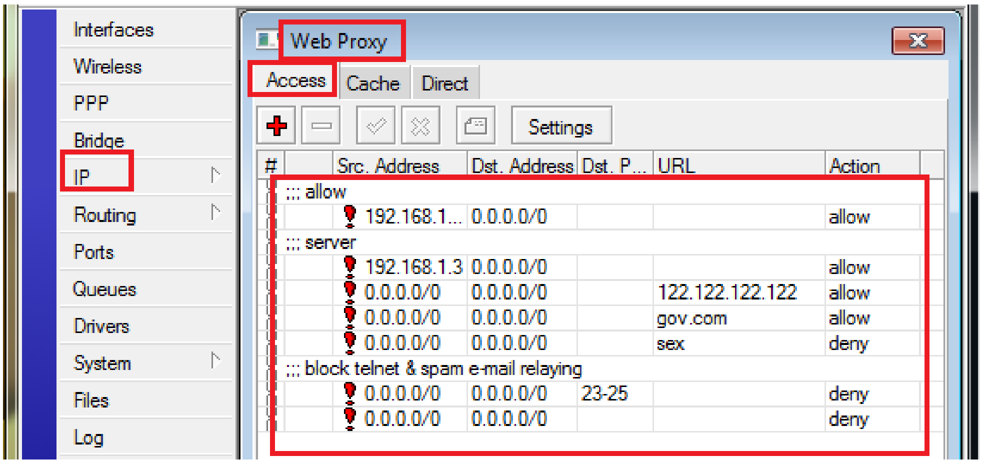
រូបភាពទី ៥.២៥ កំណត់ NAT Action

នេះគឺជាការបង្ហាញឱ្យមើល នូវអ្វីដែលយើងបង្កើតមុននេះបន្តិច។



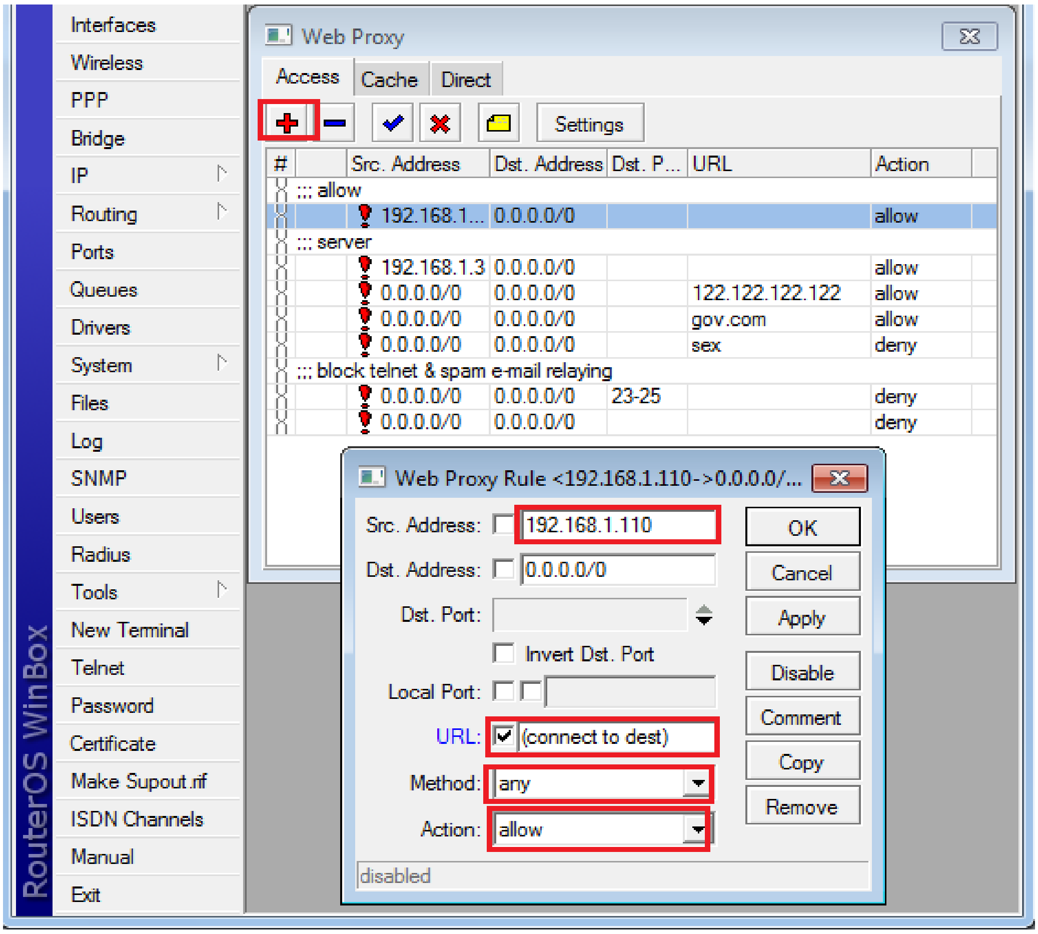
រូបភាពទី ៥.២៦ List Configuration

IP Address ដែលយើងបាន Configure ចូលទៅក្នុង Web Proxy នេះសម្រាប់ធ្វើការ Block Website និង Unblock Website មួយចំនួនដែលក្រុមហ៊ុនអនុញ្ញាត និងមិនអនុញ្ញាតប្រើប្រាស់នៅក្នុងការិយាល័យ។ ហើយ Website ខ្លះបានធ្វើឱ្យប៉ះពាល់ដល់ល្បឿនអ៊ីនធើណេត ក្នុងការបញ្ជូន និងទទួលទិន្នន័យផងដែរ។ ឬក៏ Block តាម IP Address របស់កុំព្យូទ័រនីមួយៗ នៅក្នុង LAN។



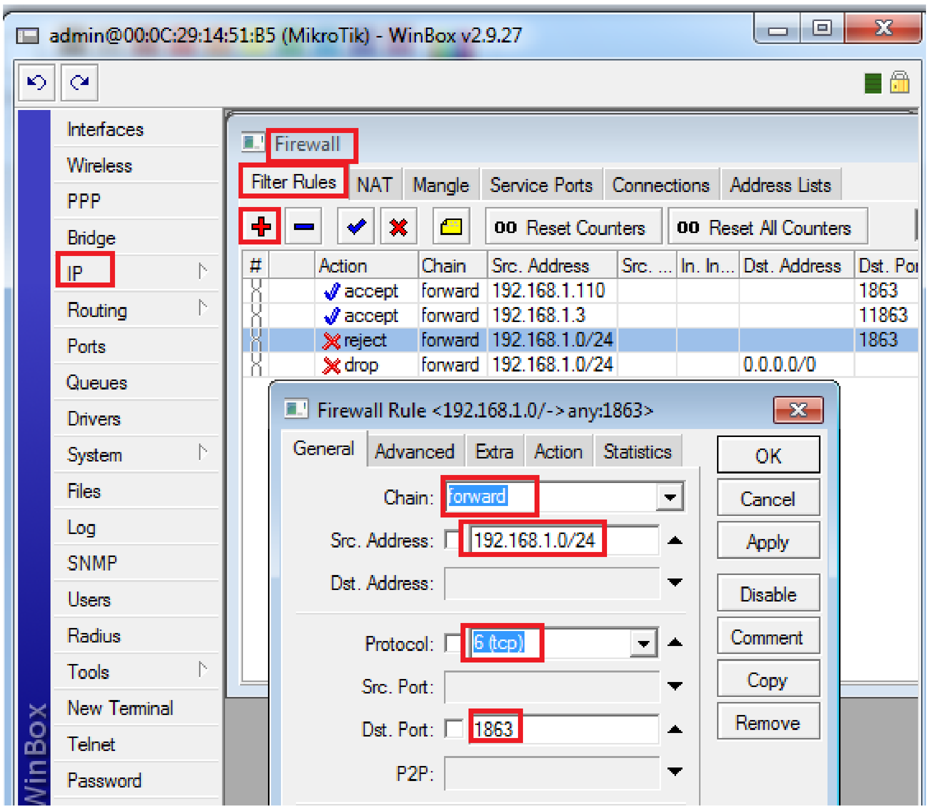
រូបភាពទី ៥.២៧ Block IP នៅលើ LAN

ដូច្នេះយើងខ្ញុំសូមលើកយក IP Address: 192.168.1.110 ដើម្បីអនុញ្ញាតឱ្យប្រើប្រាស់ Internet បានយើងគ្រាន់តែចូលទៅ IP => Web Proxy => Access => Add New ឬ ក៏ Select យក IP ខាងលើ ហើយជ្រើសរើសយកពាក្យថា Allow ហើយ OK ។



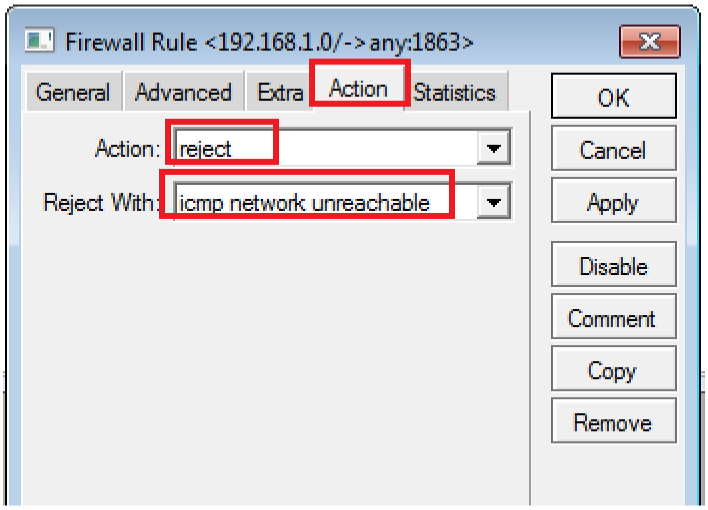
រូបភាពទី ៥.២៨ ការអនុញ្ញាតឱ្យ Clients អាចប្រើ Internet បាន

យើងនឹងធ្វើការ Block Network IP ជាបណ្តុំនៃ LAN ទាំងមូលតែម្តង។ ដំបូងយើងចូលទៅ IP => Firewall => Filter Rules => Add New => General ហើយកំណត់តាមរូបខាងក្រោមនេះ។ បន្ទាប់មកជ្រើសរើសយកពាក្យថា Action ហើយយកពាក្យថា reject និង icmp Network unreachable ហើយ OK។



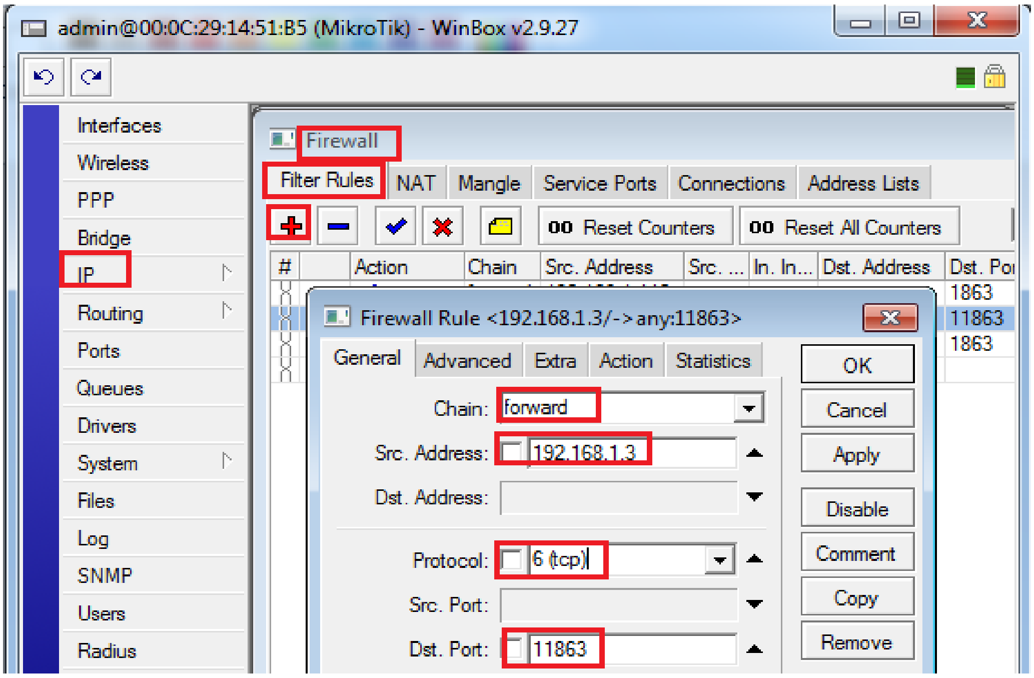
រូបភាពទី ៥.២៩ ការ Block IP នៅលើ LANs

- ចូល Action ជ្រើសរើសយក reject បន្ទាប់ខាងក្រោមយក icmp network unreachable



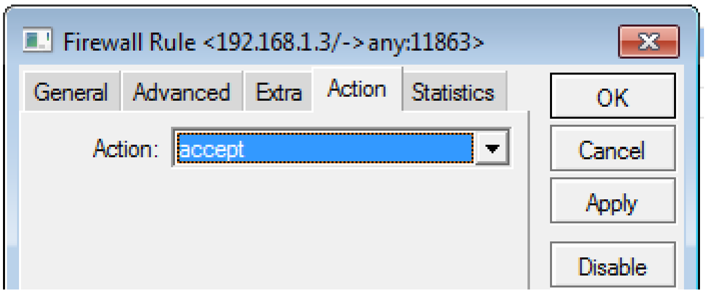
រូបភាពទី ៥.៣០ ការបិទ Intenet

- នេះជាការ Block IP Address របស់កុំព្យូទ័រនីមួយៗប៉ុណ្ណោះ



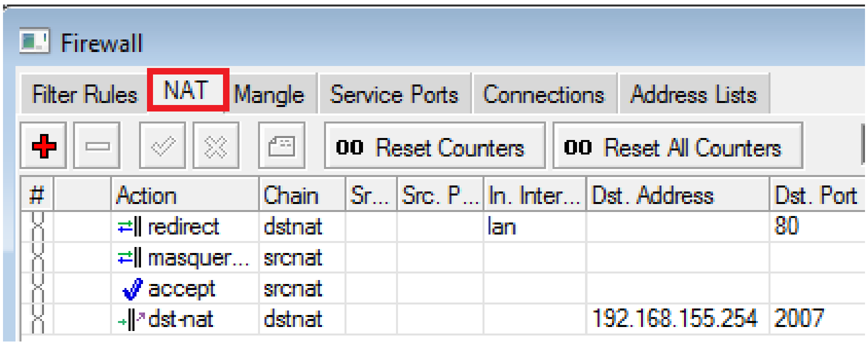
រូបភាពទី ៥.៣១ IP ដែលបាន Block

- ជ្រើសយក accept



រូបភាពទី ៥.៣២ ការអនុញ្ញាតឱ្យ Block

- ចុច NAT ដើម្បីមើល List IP ដែលយើងបាន Block

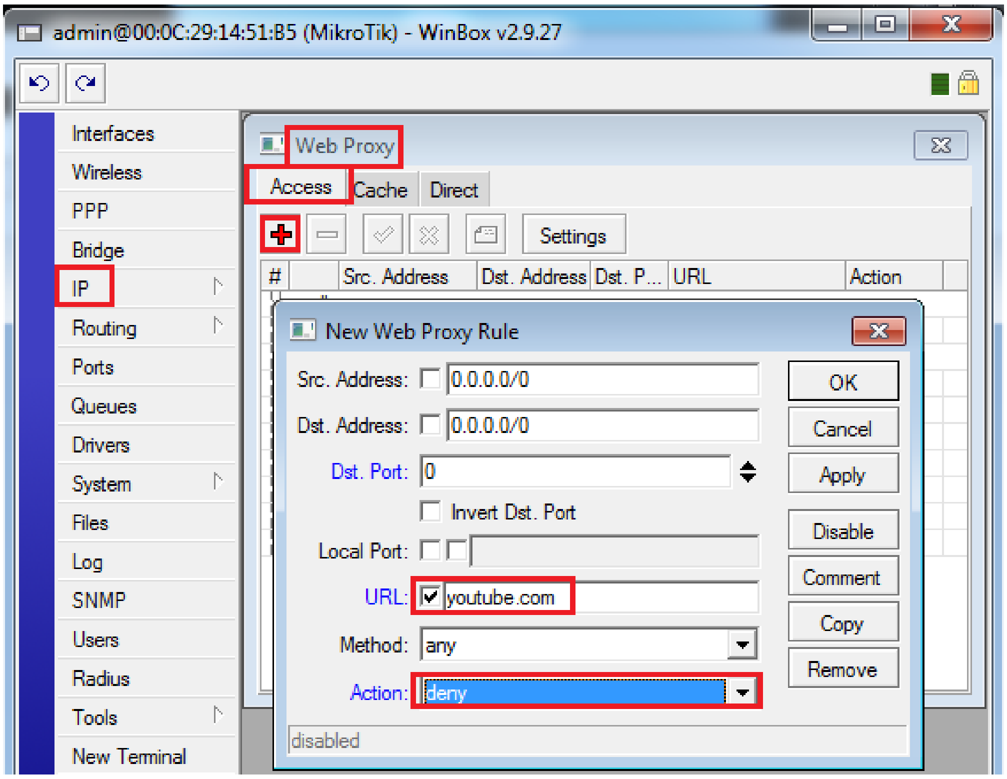


រូបភាពទី ៥.៣៣ List IP ដែលបាន Block

៥.៥ Block Website តាមរយៈ Web Proxy

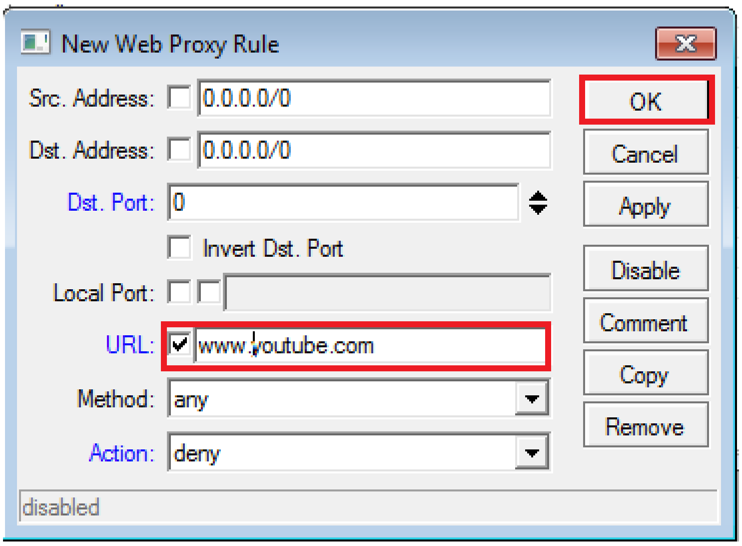
ដូច្នេះការ Block Website គឺធ្វើដើម្បីឱ្យការប្រើប្រាស់ Internet ឱ្យមានល្បឿនលឿន ក្នុងការបញ្ជូនទិន្នន័យ និងការទទួលទិន្នន័យនៅក្នុងក្រុមហ៊ុន។ ដូចនេះដើម្បី Block Website តាមកម្មវិធី Winbox នៅក្នុងប្រព័ន្ធ MikroTik យើងត្រូវធ្វើដូចខាងក្រោម÷

ដំបូងចូលទៅក្នុង MikroTik Tools => IP => Web Proxy យើងឃើញ Interface ដែលមាន Tools Access, Cache និង Direct។ យើងចូលទៅពាក្យថា Access => Add => ចូលទៅកំណត់តួនាទីរបស់វាក្នុង Interface New Web Proxy Rule សូមមើលរូបខាងក្រោម។



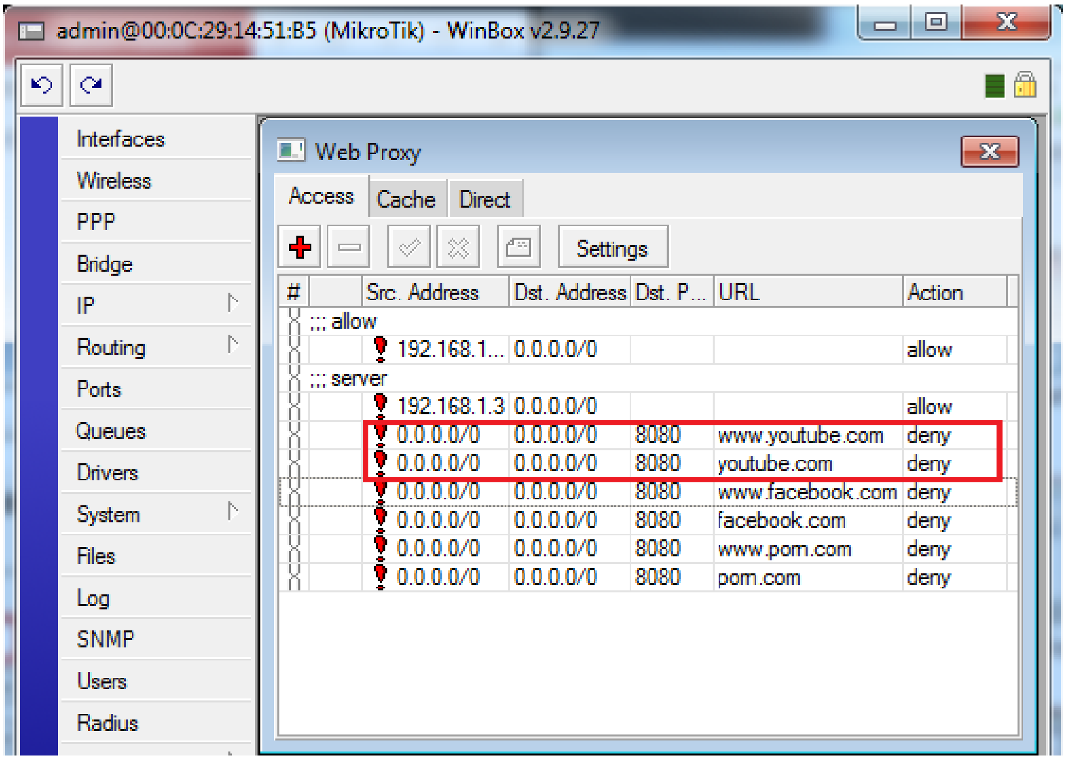
រូបភាពទី ៥.៣៤ ការ Block Website

នេះគឺជាការ Block Website youtube.com និងបើសិន User វាយអក្សរ youtube.com វានឹង Block Website តែម្តង។ ប្រសិនបើ User វាយអក្សរ www.youtube.com វាអត់ Block ទេដោយសារមានពាក្យ www នៅពីមុខដើម្បី Block Website www.youtube.com យើងត្រូវចូលតាមវិធីដដែល ប៉ុន្តែយើងគ្រាន់តែបន្ថែមអក្សរ www និង OK ជាការស្រេច។



រូបភាពទី ៥.៣៥ ការដាក់ URL ដើម្បី Block

នេះជា Website ដែលខ្ញុំ Block តាមវិធីខាងលើ ក្នុងប្រព័ន្ធ MikroTik។



រូបភាពទី ៥.៣៦ List Website ដែលបាន Block

ចប់ដោយសង្ខេប