ជំពូកទី៣

ការណែនាំអំពី TCP/IP

* មូលដ្ឋានគ្រិះនៃ Network
  + 1.1 ប្រៀបធៀប OSI និង TCP/IP models
  + 1.2 ប្រៀបធៀប TCP និង UDP protocols
  + 1.7 អនុវត្តន៍វិធីសាស្ដ្រដោះស្រាយបញ្ហាដើម្បីដោះស្រាយបញ្ហា
  + 1.7a កែប្រែកំហុសជាមួយនិងឯកសារ
  + 1.7b មានការថយចុះឬកើនឡើង
  + 1.7c ផ្ទៀងផ្ទាត់និងត្រួតពិនិត្យដំណោះស្រាយ
  + 1.9 ប្រៀបធៀបប្រភេទ IPv4 address
    - 1.9a Unicast
    - 1.9b Broadcast
    - 1.9c Multicast
  + 1.10 ពិពណ៍នាពីតម្រូវការជាសំងាត់របស់ IPv4 addressing



The Transmission Control Protocol/Internet Protocol (TCP/IP) ត្រូវបានរចនាឡើង​និងបានប្រើប្រាស់ដោយ នាយកដ្ឋានការពារជាតិ ហៅកាត់ថា (DoD) ដើម្បីធានា​និងការការពារទិន្នន័យ ដូចជានៅពេលមានសង្គ្រាមកើតឡើង។ ដូចនេះប្រសិនបើវាអនុវត្តទៅតាមអ្វីដែលបានរចនានិងការប្រើប្រាស់បានត្រឹមត្រូវនោះ TCP/IP network និងមានសុវត្ថិភាព និង អាចទុកចិត្តបាន។ នៅក្នុងជំពូកនេះ ខ្ញុំនិងរៀបរាប់ពី protocol នៃ TCP/IP នៅក្នុងសៀវភៅនេះ ហើយអ្នកនឹកសិក្សាពីការបង្កើត TCP/IP network ជាមួយនិង Cisco routers and witches.

ពួកយើងនិងចាប់ផ្ដើមស្វែងរកជំនាន់របស់DoD នៃ TCP/IP បន្ទាប់មកយើងនិងប្រៀបធៀបជំនាន់របស់វា និង protocol ជាមួយនិង គំរូ OSI ដែលយើងបានពិភាក្សាមុននេះ។

នៅពេលដែលអ្នកយល់ពី Protocol និង ដំណើរការដែលបានប្រើនៅកម្រិតផ្សេងៗគ្នានៃ DoD model, ពួកយើងនិងចូលទៅជំហានបន្ទាប់ទៀតដែលផ្ដោតទៅលើពាក្យ IP addressing និង classes ផ្សេងៗ នៃ IP addresses ដែលប្រើនៅ​

នៅក្នុងបណ្ដាយសព្វថ្ងៃ។

Note: Subnetting គឺនៅតែសំខាន់, វានិងពិពណ៍នានៅជំពូកទី ៤, “Easy Subnetting.”

ពីព្រោះត្រូវដឹងពីប្រភេទនៃ IPv4 address ផ្សេងៗ ដែលចាំបាច់ត្រូវយល់ IP addressing, subnetting, និងប្រវែងអថេរ subnet masks (VLSMs), ពួកយើងនិងរកចំលើយនៃប្រធានបទនេះនៅខ្លឹមសារ, ចុងបញ្ចប់នៃជំពូកដោយពិភាក្សាពីប្រភេទ នៃ IPv4 addresses ដែលអ្នកនិងត្រូវការសម្រាប់ការប្រឡង។

ខ្ញុំនិងមិនពិពណ៍នាអំពី Internet Protocol ជំនាន់ទី ៦ឡើយ នៅក្នុងជំពូកនេះ ពីព្រោះ យើងនិងរៀនពីវានៅពេលក្រោយ, ក្នុងជំពូកទី ១៤, “Internet Protocol Version 6 (IPv6).” នឹងអ្វីដែលអ្នកត្រូវដឹង, អ្នកនឹង Internet Protocol version 4 ដែលបានសរសេរ ដូច IP , កម្រដូច Ipv4;។

Note: To find up-to-the-minute updates for this chapter, please see [www.lammle.com/ccna](http://www.lammle.com/ccna)

Or the book’s web page via www.sybe.com/go/ccna.

**ការណែនាំអោយស្គាល់ពី** TCP/IP

TCP/IP គឺជាស្នូលសំខាន់នៃបណ្ដាយnetwork, ដូចនេះយើងត្រូវប្រាកដថាអ្នកយល់ពីពាក្យបញ្ជាមុខងាររបស់វា។ យើងនិងចាប់ផ្ដើមសិក្សាពី TCP/IP ឡើងវិញ ហើយបន្ទាប់មកយើងនិងសិក្សាដល់ចំណុចបច្ចេកទេសសំខាន់ៗដែលបានកំណត់ដោយស្ថាបត្យករដើម។ វគ្គនេះយើងនិងសិក្សាពីរបៀបប្រៀបធៀប TCP/IP ទៅនិង OSI model។

**ប្រវត្តិសង្ខេបនៃ TCP/IP**

TCP កើតឡើងនៅលើឆាកក្នុងឆ្នាំ១៩៧៣, ក្នុងឆ្នាំ ១៩៧៨, វាបានចែកចាយទៅជា 2 protocol ផ្សេងគ្នា: TCP និង IP។

ក្រោយមក, ក្នុងឆ្នាំ១៩៨៣, TCP/IP វាជំនួយ Network Control Protocol (NCP) និង បានអនុញ្ញាតជាផ្លូវបញ្ជូនទិន្នន័យសម្រាប់ការតភ្ជាប់ផ្សេងៗទៅកាន់ ARPAnet។ DoD’s Advanced Research Projects Agency (ARPA) បានបង្កើត network បុរាណនេះកាលពីឆ្នាំ ១៩៥៧ ក្នុងការប្រឆាំងសង្គ្រាមត្រជាក់ចំពោះការដំណើរការSputnikរបស់សូវៀត

។ នៅក្នុងឆ្នាំ ១៩៨៣, ARPA បញ្ចូលឡើងវិញនូវ DARPA និងត្រូវបានបែងចែកទៅជា ARPAnet និង MILNET រហូតដល់ពួកត្រូវបានបញ្ចប់នៅឆ្នាំ ១៩៩០។

វាអាចជាការមិនចង់បានប៉ុន្ដែភាគច្រើននៃការងារអភិវឌ្ឍន៍នៅលើ TCP/IP បានកើតឡើងនៅឯ UC Berkeley នៅភាគខាងជើងរដ្ឋកាលីហ្វ័រញ៉ាដែលជាកន្លែងដែលក្រុមអ្នកវិទ្យាសាស្ដ្រកំពុងធ្វើការដំណាលគ្នាលើជំនាន់ Berkeley នៃ UNIX, ដែលឆាប់បានដឹងថាជា Berkeley Software Distribution (BSD)។ ជាការពិតដោយសារតែ TCP/IP ដំណើរការបានល្អដូច្នេះវាត្រូវបានខ្ចប់ក្នុងការចេញផ្សាយជាបន្ដបន្ទាប់របស់ BSD UNIX ហើយត្រូវបានផ្ដល់ជូនទៅសាកលវិទ្យាល័យនិងស្ថាប័ន

ផ្សេងទៀតប្រសិនបើពួកគេទិញខ្សែអាត់។ ដូចនេះ ជាមូលដ្ឋាន BSD Unix បានដាក់បញ្ជូលជាមួយ TCP/IP ដែលបានចាប់ផ្ដើមជាអ្នកចែកចាយនៅក្នុងបណ្ឌិតសភា។ ជាលទ្ធផលវាបានក្លាយជាមូលដ្ឋានគ្រិះនៃជោគជ័យដ៏ធំធេងនិងការរីកចម្រើនដែលមិនធ្លាប់មានពីមុនមកនៃអ៊ីនធឺរណែតនាពេលបច្ចុប្បន្នក៏ដូចជាអ៊ីនធឺណែតតូចជាងមុន, សំងាត់ និង សារជីវកម្មអ៊ីនធឺណែត។

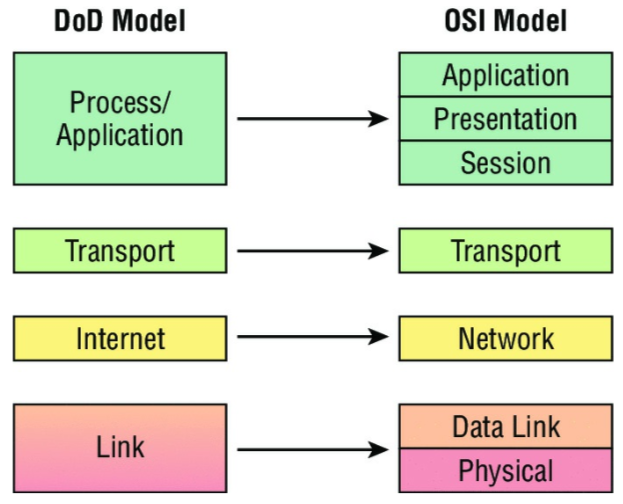
ដូចអ្វីដែលបានចាប់ផ្ដើមជាក្រុមតុចមួយនៃ TCP/IP បានវិវត្តហើយដូចដែលវាបានធ្វើ, រដ្ឋាភិបាលអាមេរិកបានបង្កើតកម្មវិធីមួយដើម្បីសាកល្បងស្ដង់ដារដែលបានបោះពុម្ពផ្សាយថ្មីៗហើយត្រូវប្រាកដថាពួកគេបានយកលក្ខណះវិនិច្ឆ័យជាក់លាក់។ នេះគឺដើម្បីការពារភាពថ្លៃថ្នូររបស់ TCP/IP និងដើម្បីធានាថាគ្មានអ្នកអភិវឌ្ឍន៍ផ្លាស់ប្ដូរអ្វីខ្លាំងពេកឬបន្ថែមលក្ខណះពិសេសណាមួយដែលមានកម្មសិទ្ធិឡើយ។ វាមានគុណភាពណាស់-វិធីបើកប្រព័ន្ធនេះទៅកាន់គ្រួសារ TCP/IP protocol-បិទប្រជាប្រិយភាពរបស់វាពីព្រោះគុណភាពនេះធានានូវការភ្ជាប់គ្នាយ៉ាងរឹងមាំរវាងផ្នែករឹងនិងកម្មវិធីសូហ្វវែរដែលមានខ្សែភ្ជាប់។

**TCP/IP and the DoD Model**

DoD model គឺជាមូលដ្ឋានកំណែបង្រួមនៃ OSI model ដែលមាន ៤ ស្រទាប់ ជំនួស ៧ ស្រទាប់:

* Process/Application layer
* Host-to-Host layer or Transport layer
* Internet layer
* Network Access layer or Link layer

ផ្ដល់នូវការប្រៀបធៀបនៃ DoD model និងគំរូ OSI model ដូចដែលអ្នកមើលឃើញ, ២ គឺស្រដៀងគ្នានៅក្នុងគំនិតប៉ុន្ដែគ្នាមានចំនួនស្រទាបខុសគ្នាដែលមានឈ្មោះខុសគ្នា។ ពេលខ្លះ Cisco អាចប្រើឈ្មោះផ្សេងៗគ្នាសម្រាប់ស្រទាប់តែមួយដូចជា “Host-to-Host” និង “Transport” នៅស្រទាប់ខាងលើស្រទាប់ Internet, ដូចជា “Network Access” និង “Link” ធ្លាប់ពណ៍នានៅស្រទាប់ខាងក្រោម។

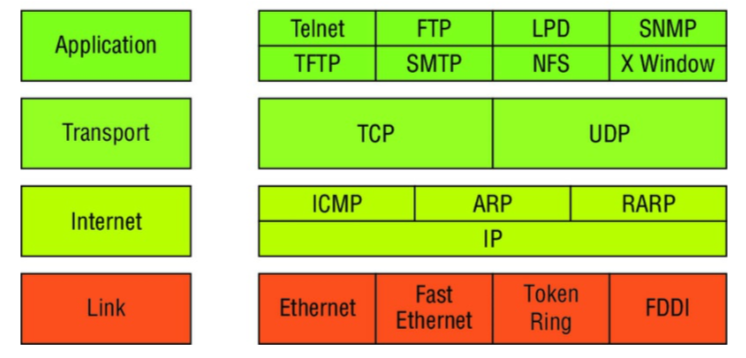


Note: When the different protocols in the IP stack are discussed, the layers of the OSI and DoD models are interchangeable. In other words, be prepared for the exam objectives to call the Host-to-Host layer the Transport layer!

Array ដ៏ធំនៃ protocol បានចូលរួមជាកម្លាំងនៅ DoD model’s Process/Application layer។ ដំណើរការទាំងនេះរួមបញ្ចូលសកម្មភាពនិងភារកិច្ចផ្សេងៗគ្នាផ្ដោតលើស្រទាប់ទាំងបីដែលត្រូវគ្នានៃ OSI (Application, Presentation, and Session)។ យើងនឹងផ្ដោតទៅលើកម្មវិធីសំខាន់ៗមួយចំនួនដែលមាននៅក្នុងCCNA។ និយាយឲ្យខ្លី ស្រទាប់ Process/Application កំណត់ Protocol សម្រាប់ទំនាក់ទំនង node-to-node និងត្រួតពិនិត្យលក្ខណះពិសេស user-interface។

ស្រទាប់ Host-to-Host ឬ ស្រទាប់ Transport ស្របគ្នានឹងមុខងាររបស់ស្រទាប់ OSI’s Transport, ដែលកំណត់ protocol សម្រាប់រៀបចំកម្រិតសេវាកម្មបញ្ជូនសម្រាប់កម្មវិធី។ វាដោះស្រាយបញ្ហាដូចជាការបង្កើតការប្រាស្រ័យទាក់ទងពី end-to-end ដែលអាចទុកចិត្តបាននិងធានាបាននូវការចែកចាយទិន្នន័យដោយគ្មានកំហុស។ វាគ្រប់គ្រងកញ្ចប់ព័ត៌មានតាមលំដាប់លំដោយនិងរក្សាភាពត្រឹមត្រូវទិន្នន័យ។ ស្រទាប់អ៊ិនធឺរណែតត្រូវគ្នានឹងស្រទាប់បណ្តាញ OSI រចនា protocol ទាក់ទងនឹងការបញ្ជូនតក្កវិទ្យាតាមបណ្តាញទាំងមូល។ វាយកចិត្តទុកដាក់លើអាស័យដ្ឋានរបស់ម៉ាស៊ីនដោយផ្តល់ឱ្យពួកគេនូវអាស័យដ្ឋាន IP (អ៊ិនធឺរណែត protocol) និងដោះស្រាយការបញ្ជូនកញ្ចប់ព័ត៌មានក្នុងចំណោមបណ្តាញជាច្រើននៅផ្នែកខាងក្រោមនៃគំរូ DoD ស្រទាប់បណ្តាញ loyerorLink អនុវត្តការផ្លាស់ប្តូរទិន្នន័យរវាងម៉ាស៊ីននិងបណ្តាញ។ សមមូលនៃទិន្នន័យភ្ជាប់និងស្រទាប់រូបវន្តនៃគំរូ OSI ស្រទាប់បណ្តាញចូលដំណើរការត្រួតពិនិត្យអាសយដ្ឋានផ្នែករឹងនិងកំណត់protocolសម្រាប់ការបញ្ជូនទិន្នន័យ។ មូលហេតុដែល TCP / IP បានក្លាយជាការពេញនិយមដូច្នេះគឺដោយសារតែមានបណ្តាញ! មិនបានកំណត់លក្ខណៈរូបវន្តជាក់លាក់ទេដូច្នេះវាអាចដំណើរការលើរូបវ័ន្តដែលមានស្រាប់និងអនាគត។ គំរូ DoD និង OSI គឺដូចគ្នានៅក្នុងការរចនានិងគំនិតហើយមានមុខងារស្រដៀងគ្នានៅក្នុងស្រទាប់ស្រដៀងគ្នា។ Eigure 3.2 បង្ហាញពីឈុតprotocol TCP / IP និងរបៀបដែល protocol របស់វាទាក់ទងនឹងស្រទាប់គំរូរបស់។

**DoD Model**

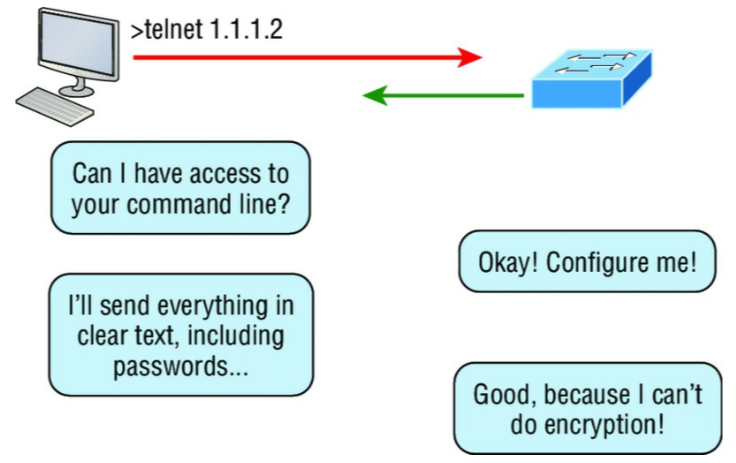
**FIGURE 3.2** protocol TCP / IP នៅក្នុងផ្នែកខាងក្រោមយើងនឹងពិនិត្យមើលprotocol ផ្សេងៗគ្នាលម្អិតបន្ថែមទៀតដោយចាប់ផ្តើមពីអ្វីដែលបានរកឃើញនៅស្រទាប់ Process/Application protocol

**The Process/Application Layer Protocol**

លេចចេញមកខ្ញុំនឹងរៀបរាប់អំពីកម្មវិធីនិងសេវាកម្មផ្សេងៗគ្នាដែលត្រូវបានប្រើជាធម្មតានៅក្នុងបណ្តាញ IP ហើយទោះបីជាមានprotocol ជាច្រើនទៀតត្រូវបានកំណត់នៅទីនេះក៏ដោយក៏ផ្តោតសំខាន់លើprotocol ដែលពាក់ព័ន្ធបំផុតទៅនឹងគោលបំណង CCNA ។ នេះគឺជាតារាងprotocol និងកម្មវិធីដែលយើងនឹងបង្ហាញនៅក្នុងផ្នែកនេះ៖

* Telnet
* SSH
* FTP
* TFTP
* SNMP
* HTTP
* HTTPS
* NTP
* DNS
* DHCP/bootP
* APIPA

**Telnet**

Telnet គឺជាស្តង់ដារអ៊ិនធឺរណែតដំបូងមួយដែលត្រូវបានបង្កើតឡើងក្នុងឆ្នាំ ១៩៦០ ហើយគឺជា protocol នៃ protocol ពិសេសរបស់វាគឺត្រាប់តាមស្ថានីយ។ វាអនុញ្ញាតឱ្យអ្នកប្រើនៅលើម៉ាស៊ីនភ្ញៀវពីចម្ងាយដែលហៅថាអតិថិជន Telnet ចូលប្រើធនធានរបស់ម៉ាស៊ីនផ្សេងទៀតគឺម៉ាស៊ីនមេ Telnet ដើម្បីចូលប្រើចំណុចប្រទាក់បន្ទាត់ពាក្យបញ្ជា។ Telnet សំរេចបានតាមវិធីនេះដោយទាញល្បឿនលឿននៅលើម៉ាស៊ីនមេ Telnet ហើយធ្វើឱ្យម៉ាស៊ីនភ្ញៀវលេចចេញដូចជាស្ថានីយដែលភ្ជាប់ទៅនឹងបណ្តាញមូលដ្ឋាន។ ការព្យាករណ៍នេះពិតជារូបភាពសូហ្វវែរដែលជាស្ថានីយនិម្មិតដែលអាចទាក់ទងជាមួយម៉ាស៊ីនពីចម្ងាយដែលបានជ្រើសរើស។ គុណវិបត្តិមួយគឺថាមិនមានបច្ចេកទេសក្នុងការអ៊ិនគ្រីបដែលអាចរកបាននៅក្នុង protocol Telnet ទេដូច្នេះអ្វីៗទាំងអស់ត្រូវផ្ញើជាអក្សរច្បាស់លាស់រួមទាំងលេខសម្ងាត់! FIGURE 3.3 បង្ហាញពីឧទាហរណ៍របស់អតិថិជន Telnet ដែលព្យាយាមភ្ជាប់ទៅម៉ាស៊ីនមេ Telnet ។

**Figure 3.3 Telnet**

ប្រភេទថេបថេបនៃប្រភេទរបៀបអត្ថបទអាចប្រតិបត្តិនីតិវិធីដែលបានកំណត់ដូចជាការបង្ហាញដែលផ្តល់ឱ្យខ្ញុំនូវឱកាសដើម្បីជ្រើសរើសជម្រើសនិងកម្មវិធីនៅលើម៉ាស៊ីនមេដែលគេបោក។ អ្នកប្រើប្រាស់ចាប់ផ្តើមវគ្គ Telnet ដោយដំណើរការកម្មវិធីអតិថិជន Telnet ហើយបន្ទាប់មកចូលទៅម៉ាស៊ីនមេ Telnet session ដោយភ្ជាប់ទិន្នន័យនៅលើ TCP ដែលធ្វើឱ្យវាហ្មត់ចត់ណាស់ដែលខ្ញុំនៅតែមានសព្វថ្ងៃនេះមានលក្ខណៈសាមញ្ញនិងងាយស្រួលប្រើដោយមានផ្នែកខាងទាប។ ជាមួយនឹងអ្វីគ្រប់យ៉ាងមាននៅក្នុងអត្ថបទច្បាស់លាស់មិនត្រូវបានណែនាំនៅក្នុងផលិតកម្ម

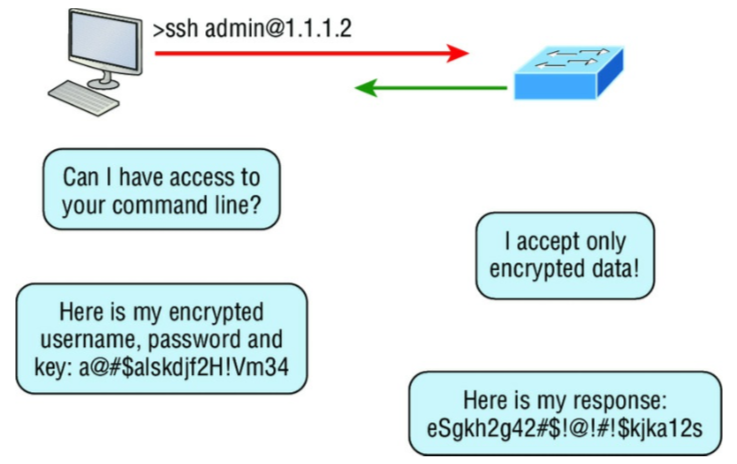
**Secure Shell (SSH)**

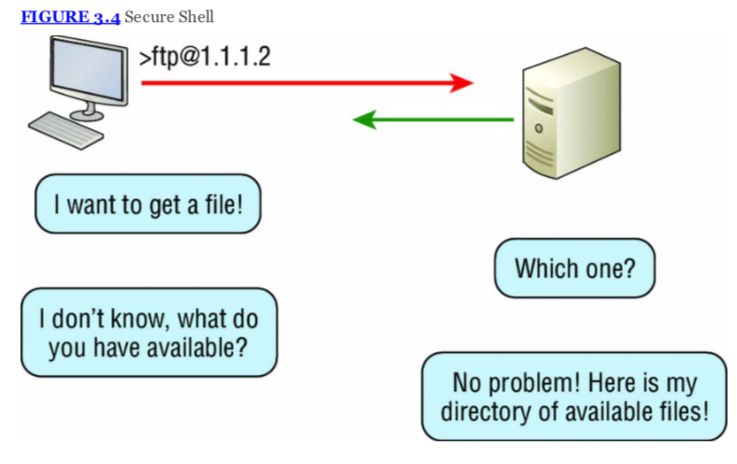
protocol សុវត្ថិភាពសែលអេសអេស (SSH) បង្កើតសម័យមានសុវត្ថិភាពដែលស្រដៀងនឹង Telnet តាមរយៈការតភ្ជាប់តាម TCP / IP ស្តង់ដារហើយត្រូវបានប្រើសម្រាប់ធ្វើអ្វីៗដើម្បីជូតកម្មវិធីនៅលើប្រព័ន្ធពីចម្ងាយនិងការផ្លាស់ប្តូរឯកសារពីប្រព័ន្ធមួយទៅប្រព័ន្ធមួយទៀត។ ហើយវាធ្វើអ្វីៗទាំងអស់នេះខណៈពេលដែលរក្សាការតភ្ជាប់អូអេសអេសដែលព្យាយាមភ្ជាប់ទៅម៉ាស៊ីនមេ SSH។ អតិថិជនត្រូវផ្ញើទិន្នន័យដែលបាន encrypted!

អ្នកអាចគិតថាវាជា protocol ជំនាន់ថ្មីដែលឥឡូវនេះជាកន្លែងនៃវត្ថុបុរាណនិងមិនប្រើហើយសូម្បីតែ Telnet

**File Transfer Protocol (FTP)**

File Transfer Protocol (FTP) ពិតជាអនុញ្ញាតឱ្យយើងផ្ទេរឯកសារហើយវាអាចសម្រេចបានរវាងម៉ាស៊ីនអូអេសណាមួយដែលប្រើវា។ ប៉ុន្តែ FTP មិនមែនគ្រាន់តែជា protocol ប៉ុណ្ណោះទេ។ វាក៏ជាកម្មវិធីផងដែរ។ ប្រតិបត្តិការជា protocol FTP ត្រូវបានប្រើដោយកម្មវិធី។ ក្នុងនាមជាកម្មវិធីមួយវាត្រូវបានជួលដោយអ្នកប្រើដើម្បីអនុវត្តការងារឯកសាក៏រដោយ។ FTP ក៏អនុញ្ញាតឱ្យចូលប្រើទាំងថតនិងឯកសារហើយអាចសម្រេចបាននូវប្រភេទនៃប្រតិបត្តិការថតមួយចំនួនដូចជាការផ្លាស់ប្តូរទីតាំងទៅកន្លែងផ្សេងគ្នា (Figure ៣.៥)។



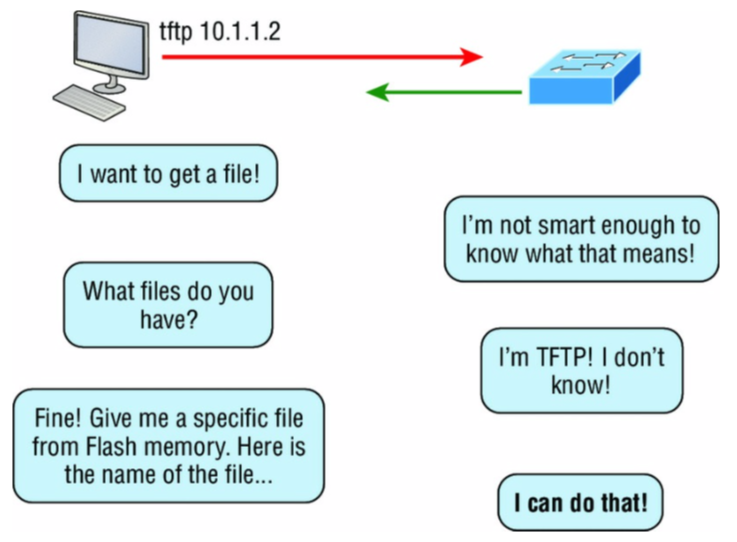


**Figure 3.5 TFTP**

ប៉ុន្តែការចូលប្រើម៉ាស៊ីនតាមរយៈ FTP គ្រាន់តែជាជំហានដំបូងប៉ុណ្ណោះ។ អ្នកប្រើត្រូវតែចូលការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវដែលជាធម្មតាត្រូវបានការពារដោយពាក្យសម្ងាត់និងឈ្មោះអ្នកប្រើដែលបានអនុវត្តដោយអ្នកគ្រប់គ្រងប្រព័ន្ធដើម្បីដាក់កម្រិតការចូលប្រើ។ អ្នកអាចយល់អំពីបញ្ហានេះដោយប្រើឈ្មោះអ្នកប្រើអនាមិកប៉ុន្តែអ្នកនឹងត្រូវបានកំណត់នៅក្នុងអ្វីដែលអ្នកនឹងអាចចូលដំណើរការបានទោះបីជាអ្នកប្រើដោយដៃជាអ្នកប្រើកម្មវិធីក៏ដោយមុខងាររបស់ FTP ត្រូវបានកំណត់ចំពោះការចុះបញ្ជីនិងរៀបចំថតឯកសារវាយមាតិកាឯកសារ។ និងចម្លងឯកសាររវាងម៉ាស៊ីន។ វាមិនអាចប្រតិបត្តិឯកសារពីចម្ងាយជាកម្មវិធីបានទេ។

**Trivial File Transfer Protocol (TFTP)**

Trivial File Transfer Protocol (TFTP) គឺជាការដកចេញឯកសារស្តុករបស់ FTP។ ប៉ុន្តែវាងាយស្រួលប្រើ! protocol នៃជម្រើសប្រសិនបើអ្នកដឹងច្បាស់នូវអ្វីដែលអ្នកចង់បាននិងកន្លែងដែលត្រូវរកវាពីព្រោះវាលឿនហើយដូច្នេះ TFTP មិនបានផ្តល់នូវមុខងារជាច្រើនដែល FTP ធ្វើទេពីព្រោះវាមិនមានលទ្ធភាពរុករកថតបានទេមានន័យថាវាអាចផ្ញើនិងទទួលឯកសារបាន។ (Figure ២.៦) ។ យ៉ាងណាក៏ដោយវាត្រូវបានប្រើយ៉ាងខ្លាំងសម្រាប់ការគ្រប់គ្រងប្រព័ន្ធឯកសារនៅលើឧបករណ៍ស៊ីស្កូដូច។ ខ្ញុំនិងបង្ហាញអ្នកក្នុងជំពូកទី ៧”Managing a Cisco Internetwork”។



**Figure 3.6 TFP**

protocol តូចតាចក៏លោតចូលផ្នែកទិន្នន័យបញ្ជូនទិន្នន័យប្លុកតូចជាងភីភីភីផងដែរ។ គ្មានការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវជាមួយ FTP ទេ។ អូសេវេនមានអសន្តិសុខជាងមុនហើយមានគេហទំព័រមួយចំនួនគាំទ្រវាដោយសារតែហានិភ័យសុវត្ថិភាពជាប់នឹងខ្លួន។

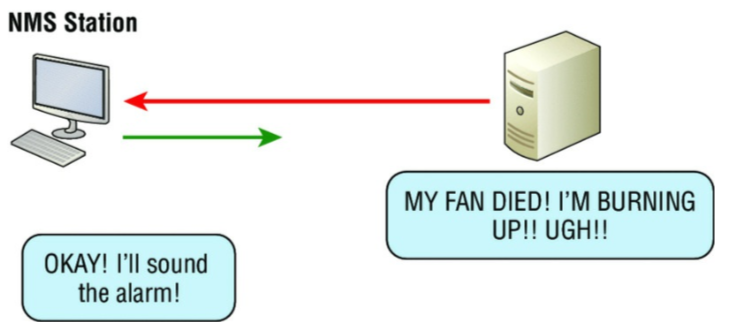
**នៅពេលណាអ្នកគួរប្រើ FTP?**

អ្នកទាំងអស់គ្នានៅឯសាន់ហ្រានស៊ីស្កូរបស់អ្នកបានផ្ញើអ៊ីមែលទៅពួកគេ! តើអ្នកធ្វើអ្វី? ម៉ាស៊ីនមេអ៊ីម៉ែលជាច្រើននឹងបដិសេធអ៊ីមែលនោះដោយសារការកំណត់ទំហំ ISP ជាច្រើនមិនអនុញ្ញាតឱ្យផ្ញើឯកសារដែលមានទំហំធំជាង ៥ មេកាបៃឬ ១០ មេកាបៃហើយបើទោះបីជាគ្មានដែនកំណត់លើម៉ាស៊ីនមេក៏ដោយវានៅតែត្រូវការពេលមួយរយៈដើម្បីផ្ញើ ឯកសារដ៏ធំនេះ។ FTP ដើម្បីជួយសង្គ្រោះ! ប្រសិនបើអ្នកត្រូវការផ្តល់ឱ្យអ្នកណាម្នាក់នូវឯកសារធំឬអ្នកត្រូវការយកឯកសារធំពីនរណាម្នាក់ FTP ជាជម្រើសដ៏ល្អ។ ដើម្បីប្រើ FTP អ្នកត្រូវតំឡើងម៉ាស៊ីនមេ FTP នៅលើអ៊ិនធឺរណែតដើម្បីឱ្យឯកសារអាចចែករំលែកបានក្រៅពីដោះស្រាយបញ្ហាទំហំ FTP លឿនជាងអ៊ីមែល។ លើសពីនេះទៀតដោយសារតែវាប្រើ TCP និងតម្រង់ទិសដៅនៃការតភ្ជាប់ប្រសិនបើវេនងាប់ពេលខ្លះ FTP អាចចាប់ផ្តើមនៅកន្លែងដែលវាទុកចោល។ សាកល្បងជាមួយ email client!

**Simple Network Management Protocol (SNMP)**

Simple Network Management (SNMP) ប្រមូលនិងរៀបចំការបង្កើតបណ្តាញដ៏មានតំលៃដូចដែលអ្នកបានឃើញនៅក្នុង Figure 3.7 ។ វាប្រមូលទិន្នន័យដោយធ្វើការស្ទង់មតិលើឧបករណ៍នៅលើបណ្តាញគ្រប់គ្រងបណ្តាញអ៊ីម៉ា (NMS) នៅចម្ងាយថេរឬចៃដន្យដែលតម្រូវឱ្យមាន m បង្ហាញព័ត៌មានជាក់លាក់ឬសូម្បីតែស្នើសុំព័ត៌មានជាក់លាក់ពីឧបករណ៍។ លើសពីនេះទៀតឧបករណ៍បណ្តាញអាចជូនដំណឹងដល់ស្ថានីយ៍ NMS អំពីបញ្ហានៅពេលវាកើតឡើងដូច្នេះបណ្តាញអ្នកគ្រប់គ្រងត្រូវបានជូនដំណឹង។

**NMS Station**

****

**Figure 3.7 SNMP**

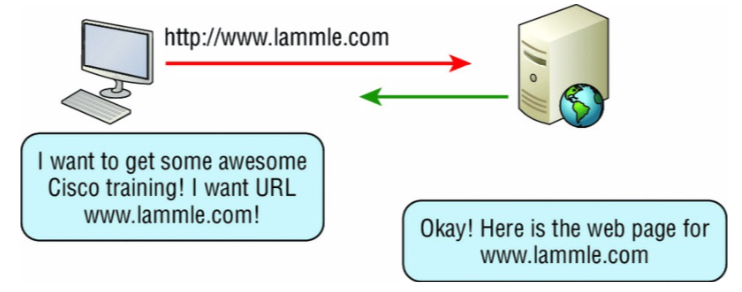
ពេលណាល្អ។ SNMP ទទួលបានអ្វីមួយដែលគេហៅថាជាមូលដ្ឋាន - របាយការណ៍ដែលកំណត់លក្ខណៈនៃប្រតិបត្តិការរបស់បណ្តាញដែលមានសុខភាពល្អ។ protocol នេះក៏អាចដើរតួជាអ្នកឃ្លាំមើលលើបណ្តាញផងដែរដោយជូនដំណឹងដល់អ្នកគ្រប់គ្រងភ្លាមៗអំពីវេននៃព្រឹត្តិការណ៍ណាមួយ។ អ្នកឃ្លាំមើលបណ្តាញទាំងនេះត្រូវបានគេហៅថាដំណើរស្វែងរក។

**SNMP Version 1,2 and 3**

កំណែ SNMP និងមានច្រើនគួរសម។ នេះមិនមានន័យថាអ្នកនឹងមិនឃើញវានៅក្នុងធ្នូ K ទេហើយពេលនោះអ្នកនឹងជួបតែកម្រប្រសិនបើអ្នកមិនធ្លាប់មាន។ SNMPV2 បានផ្តល់ចលនាពិសេសក្នុងការអនុវត្ត។ ប៉ុន្តែការបន្ថែមដ៏ល្អបំផុតមួយត្រូវបានគេហៅថា GETBULK ដែលអនុញ្ញាតឱ្យម្ចាស់ផ្ទះទាញយកទិន្នន័យមួយចំនួនធំក្នុងពេលតែមួយ។ ទោះបីជាយ៉ាងណាក៏ដោយ v2 bever ពិតជាចាប់បាននៅក្នុងពិភពបណ្តាញហើយឥឡូវនេះ SNMP v 3 គឺជាស្តង់ដារ។ មិនដូចវីដែលប្រើតែយូភីភី។ ៣ ប្រើទាំង TCP និង UDP និងបន្ថែមសុវត្ថិភាពបន្ថែមទៀតការផ្ទៀងផ្ទាត់ភាពត្រឹមត្រូវសារនិងការអ៊ិនគ្រីប

**Hypertext Transfer Protocol (HTTP)**

វេបសាយថូទាំងអស់ដែលមានបណ្តាញក្រាហ្វិចអត្ថបទតំណភ្ជាប់ការផ្សាយពាណិជ្ជកម្មនិងអ្វីៗផ្សេងទៀតពឹងផ្អែកលើប្រូតូកូលផ្ទេរប្រូតូ (TFTP) ដើម្បីធ្វើឱ្យវាអាចធ្វើទៅបានទាំងអស់ (រូបភាពទី ៨) វាត្រូវបានប្រើដើម្បីគ្រប់គ្រងទំនាក់ទំនងរវាងកម្មវិធីរុករកគេហទំព័រនិងគេហទំព័រ។ ហើយបើកធនធានត្រឹមត្រូវនៅពេលអ្នកចុចលើតំណភ្ជាប់នៅកន្លែងណាដែលប្រភពធនធាននោះអាចរស់នៅបាន



**FIGURE 3.8 HTTP**

ដើម្បីឱ្យ browser បើកទំព័របណ្តាញវាត្រូវរកម៉ាស៊ីនមេពិតប្រាកដដែលមានគេហទំព័រត្រឹមត្រូវបូករួមទាំងព័ត៌មានលំអិតពិតប្រាកដដែលបញ្ជាក់ព័ត៌មានដែលបានស្នើសុំ។ ព័ត៌មាននេះត្រូវបានបញ្ជូនត្រលប់ទៅកម្មវិធីអ៊ីនធឺណិតវិញ។ សព្វថ្ងៃមានការសង្ស័យយ៉ាងខ្លាំងដែលថាម៉ាស៊ីនមេវែបមានទំព័រតែមួយដើម្បីបង្ហា

គេហទំព័រផែនទីទាំងអស់នោះរួមមានក្រាហ្វិកអត្ថបទតំណភ្ជាប់ការផ្សាយពាណិជ្ជកម្មនិងផ្អែកលើការពឹងផ្អែកលើប្រូតូកូលប្រូតូកូល (HTTP) ដើម្បីធ្វើឱ្យវាអាចធ្វើទៅបាន (Figure 3.8) ។ វាត្រូវបានប្រើដើម្បីគ្រប់គ្រងការដកស្រង់រវាងកម្មវិធីរុករកបណ្តាញនិងម៉ាស៊ីនមេគេហទំព័រហើយបើកធនធានត្រឹមត្រូវនៅពេលដែលអ្នកចុកនៅកន្លែងណាដែលធនធាននោះអាចរស់នៅបាន។

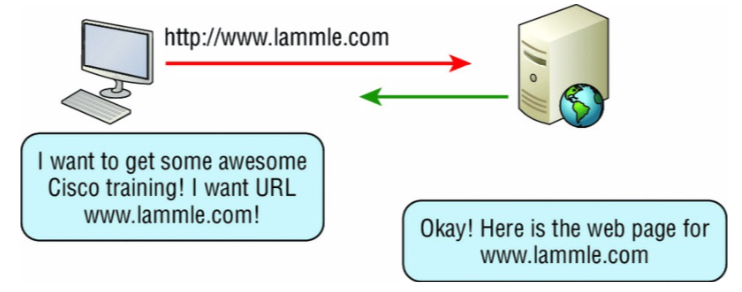
http://www.lammle.com។

ដូច្នេះជាមូលដ្ឋាន URL នីមួយៗកំណត់ protocol ដែលត្រូវបានប្រើដើម្បីផ្ទេរទិន្នន័យឈ្មោះរបស់ម៉ាស៊ីនមេនិងគេហទំព័រជាក់លាក់នៅលើម៉ាស៊ីនមេនោះ។

**Hypertext Protocol Secure Protocol Secure (HTTPS)**

Protocol Transfer Protocol Secure (HTTPS) ត្រូវបានគេស្គាល់ថាជា protocol ផ្ទេរ Hypertext ដែលមានសុវត្ថិភាព។ វាប្រើស្រទាប់រន្ធរន្ធសុវត្ថិភាព (SSL) ។ ពេលខ្លះអ្នកនឹងឃើញថាវាត្រូវបានគេសំដៅថាជា HTTP ឬ S-HTTP ដែលមាន protocol ខុសគ្នាបន្តិចបន្តួចប៉ុន្តែចាប់តាំងពីក្រុមហ៊ុន Microsoft គាំទ្រ HTTPS វាបានក្លាយជាស្តង់ដារឌីជីថលសម្រាប់ធានាការទំនាក់ទំនងតាមអ៊ីនធឺណិត។ ប៉ុន្តែគ្មានបញ្ហាអ្វីដូចដែលបានបង្ហាញនោះទេវាគឺជាកំណែសុវត្ថិភាពរបស់ HTTP ដែលផ្តល់ជូនអ្នកនូវឧបករណ៍សុវត្ថិភាពទាំងមូលសម្រាប់រក្សាប្រតិបត្តិការរវាងកម្មវិធីរុករកអ៊ីនធឺណិតនិងម៉ាស៊ីនមេ។ វាជាអ្វីដែលកម្មវិធីអ៊ីនធឺណិតរបស់អ្នកត្រូវការបំពេញបែបបទចុះឈ្មោះចូលផ្ទៀងផ្ទាត់និងអ៊ិនគ្រីបសារ HTTP នៅពេលអ្នកធ្វើអ្វីៗតាមអ៊ីនធឺណិតដូចជាធ្វើការកក់ចូលប្រើធនាគារបស់អ្នកឬទិញអ្វីមួយ។

protocol ពេលវេលាបណ្តាញ (NTP) Kudos ដល់សាស្រ្តាចារ្យ David Mills នៃសាកលវិទ្យាល័យ Delaware សម្រាប់ការបង្កើត protocol ងាយស្រួលនេះដែលត្រូវបានប្រើដើម្បីធ្វើសមកាលកម្មនាឡិកានៅលើកុំព្យូទ័ររបស់យើងទៅនឹងប្រភពពេលវេលាមួយ (ឧទាហរណ៍នាឡិកាអាតូមិច) ។ protocol ពេលវេលាបណ្តាញ (NTP) ដំណើរការដោយឧបករណ៍ធ្វើសមកាលកម្មដើម្បីធានាថាកុំព្យូទ័រទាំងអស់នៅលើបណ្តាញដែលបានផ្តល់ឱ្យព្រមព្រៀងគ្នាតាមពេលវេលា (រូបភាពទី ៩ ៩) នេះមើលទៅហាក់ដូចជាសាមញ្ញណាស់ប៉ុន្តែវាសំខាន់ណាស់ពីព្រោះប្រតិបត្តិការជាច្រើនដែលបានធ្វើនៅថ្ងៃនេះគឺពេលវេលានិងកាលបរិច្ឆេទ បោះត្រា។ គិតអំពីមូលដ្ឋានទិន្នន័យ - ម៉ាស៊ីនមេអាចធ្វើឱ្យរញ៉េរញ៉ៃហើយថែមទាំងគាំងទៀតប្រសិនបើវាមិនសមកាលជាមួយម៉ាស៊ីនដែលភ្ជាប់ជាមួយវាដោយគ្រាន់តែចំណាយពេលតែប៉ុន្មានវិនាទី! nchinnentered ដោយម៉ាស៊ីននៅនិយាយថាម៉ោង 1:50 ព្រឹកនៅពេលដែលម៉ាស៊ីនមេកត់ត្រាពីប្រតិបត្តិការនោះថាបានកើតឡើងនៅម៉ោង ១:៤៥ ទៀបភ្លឺដូច្នេះជាមូលដ្ឋាន NTP ធ្វើការដើម្បីការពារសេណារីយ៉ូមួយដែលមិនមានបញ្ហា“ ត្រលប់ទៅអនាគត។ ពីការធ្លាក់ចុះបណ្តាញ - ពិតជាសំខាន់ណាស់!



**Figure 3.9 NTP**

ខ្ញុំនឹងជួយអ្នកបន្ថែមទៀតអំពី NTP ក្នុងជំពូកទី ៧ រួមទាំងវិធីកំណត់រចនាសម្ព័ន្ធ protocol នេះនៅក្នុងសេវាកម្មឈ្មោះស៊ីស្ទ័រស៊ីអេសអេសមេនឌីសមេនឌីសស៊ីធីឌីដោះស្រាយឈ្មោះម៉ាស៊ីនពិសេស។ ឈ្មោះតាមអ៊ិនធឺរណែតដូចជា w.lammle.com ។ ប៉ុន្តែអ្នកមិនចាំបាច់ប្រើ DNS ទេ។ អ្នកគ្រាន់តែវាយបញ្ចូលអាសយដ្ឋានអាយភីនៃទឹកកកណាមួយដែលអ្នកចង់ទំនាក់ទំនងនិងស្វែងរកអាសយដ្ឋាន IP របស់ URL ដោយប្រើភីងជីង។ ឧទាហរណ៍ភីងនឹងត្រលប់មកវិញនូវអាសយដ្ឋាន IP ដែលត្រូវបានដោះស្រាយដោយអាសយដ្ឋាន IP IP កំណត់អត្តសញ្ញាណម៉ាស៊ីននៅលើបណ្តាញនិងអ៊ិនធឺរណែតប៉ុន្តែ DNS ត្រូវបានបង្កើតឡើងដើម្បីធ្វើឱ្យជីវិតរបស់យើងកាន់តែងាយស្រួល។ គិតអំពីរឿងនេះ: តើនឹងមានអ្វីកើតឡើងប្រសិនបើអ្នកចង់ផ្លាស់ប្តូរគេហទំព័ររបស់អ្នកទៅអ្នកផ្តល់សេវាកម្មផ្សេងទៀត? អាសយដ្ឋាន IP នឹងផ្លាស់ប្តូរហើយគ្មាននរណាម្នាក់អាចដឹងថាតើលេខថ្មីគឺជាអ្វីទេ។ DNS អនុញ្ញាតឱ្យអ្នកប្រើឈ្មោះដែនដើម្បីបញ្ជាក់អាសយដ្ឋាន IP ។ អ្នកអាចផ្លាស់ប្តូរអាសយដ្ឋាន IP ឱ្យបានញឹកញាប់តាមដែលអ្នកចង់បានហើយគ្មាននរណាម្នាក់ដឹងពីភាពខុសគ្នានោះទេ។

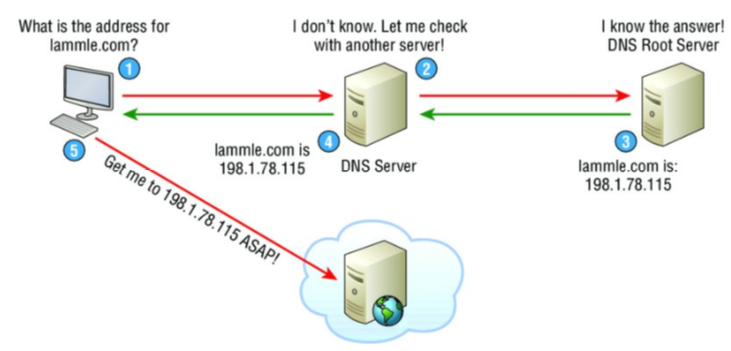
o ដោះស្រាយអាស័យដ្ឋាន DNS ពីម៉ាស៊ីនអ្នកតែងតែវាយបញ្ចូល URL ពីកម្មវិធីរុករកដែលអ្នកចូលចិត្តដែលនឹងបញ្ជូនទិន្នន័យទៅចំណុចប្រទាក់ស្រទាប់កម្មវិធីដើម្បីបញ្ជូននៅលើបណ្តាញ។ កម្មវិធីនេះនឹងស្វែងរកអាស័យដ្ឋាន DNS ហើយផ្ញើសំណើរ UDP ទៅម៉ាស៊ីនមេ DNS របស់អ្នកដើម្បីដោះស្រាយឈ្មោះ (Figure 3.10)។

ម៉ាស៊ីនមេ DNS ដំបូងរបស់អ្នកមិនដឹងចម្លើយទៅនឹងសំណួរទេបន្ទាប់មកម៉ាស៊ីនមេ DNS បញ្ជូនសំណើរ TCP ទៅម៉ាស៊ីនមេ DNS របស់វា។ នៅពេលដែលសំណួរត្រូវបានដោះស្រាយចំលើយត្រូវបានបញ្ជូនត្រលប់ទៅរកប្រភពដើមរបស់ម៉ាស៊ីនដែលមានន័យថាម្ចាស់ផ្ទះអាចស្នើសុំព័ត៌មានពីម៉ាស៊ីនមេវែបត្រឹមត្រូវ។

DNS ត្រូវបានប្រើដើម្បីដោះស្រាយឈ្មោះដែនដែលមានសមត្ថភាពពេញលេញ (FQDN) ឧទាហរណ៍ www.lammle.comឬ todd.lamle.com គឺជាឋានានុក្រមដែលអាចកំណត់ទីតាំងប្រព័ន្ធដោយផ្អែកលើឡូជីនរបស់វា។

កំណត់អត្តសញ្ញាណ។

ប្រសិនបើអ្នកចង់ដោះស្រាយឈ្មោះតូចអ្នកត្រូវតែវាយ FQDN នៃឬមានឧបករណ៍ដូចជាកុំព្យូទ័រឬរ៉ោតទ័របន្ថែមបច្ច័យសម្រាប់អ្នក។ ឧទាហរណ៍នៅលើរ៉ោតទ័រស៊ីស្កូអ្នកអាចប្រើពាក្យបញ្ជាអាយភីដើម្បីបន្ថែមការស្នើសុំនីមួយៗជាមួយដែន។ ប្រសិនបើអ្នកមិនធ្វើវាទេអ្នកនឹងត្រូវវាយ FQDN ដើម្បីទទួលបានឈ្មោះ DNS ដើម្បីដោះស្រាយឈ្មោះ។



**Figure 3.10 DNS**

រឿងសំខាន់ដែលត្រូវចងចាំអំពី DNS គឺថាប្រសិនបើអ្នកអាច ping ឧបករណ៍ជាមួយ

អាសយដ្ឋាន IP ប៉ុន្តែមិនអាចប្រើ FQDN របស់វាទេពេលនោះអ្នកអាចនឹងមានការបរាជ័យនៃការកំណត់រចនាសម្ព័ន្ធប្រភេទ DNS មួយចំនួន។

**Dynamic Host Configuration Protocol (DHCP)/Bootstrap Protocol (BootP)**

Dynamic Host Configuraton Protocol(DHCP) កំណត់អាសយដ្ឋាន IP ទៅឱ្យម៉ាស៊ីន។ វាអនុញ្ញាតឱ្យមានការគ្រប់គ្រងងាយស្រួលនិងដំណើរការល្អនៅក្នុងបរិស្ថានបណ្តាញតូចទៅធំ។ ផ្នែករឹងជាច្រើនអាចត្រូវបានប្រើជាម៉ាស៊ីនមេ DHCP រួមទាំងរ៉ោតទ័រស៊ីស៊ីកូ DICP ខុសគ្នាពីប៊្លូធូសនៅក្នុងនោះប៊្លុកភីផ្តល់អាស័យដ្ឋានអាយភីទៅម៉ាស៊ីនប៉ុន្តែម្ចាស់ម៉ាស៊ីន អាសយដ្ឋានផ្នែករឹងត្រូវតែបញ្ចូល m ដែលជាសម្ព័ន្ធមិត្តនៅក្នុងតារាង BootP ។ អ្នកអាចគិតពី DHCP ដែលជា BootP ដែលមានថាមពលប៉ុន្តែសូមចាំថា BootP ត្រូវបានប្រើដើម្បីផ្ញើប្រព័ន្ធប្រតិបត្តិការដែលម៉ាស៊ីនអាចបញ្ឈប់ពី DHCP មិនអាចធ្វើបាន។ ប៉ុន្តែនៅតែមានព័ត៌មានជាច្រើនដែលម៉ាស៊ីនមេ DHCP អាចផ្តល់ជូនដល់ម្ចាស់ផ្ទះនៅពេលដែលម្ចាស់ផ្ទះកំពុងស្នើសុំអាសយដ្ឋាន IP ពីម៉ាស៊ីនមេ DHCP ។ នេះគឺជាបញ្ជីព័ត៌មានទូទៅបំផុតដែលម៉ាស៊ីនបម្រើ DHCP អាចផ្តល់ជូននូវរបាំងអាស័យដ្ឋានអាយភីអាយអិម។

នេះគឺជា command ដែលគេច្រើនប្រើនៅក្នុង DHCP

* IP address
* Subnet mask
* Domain name
* Default gateway (routers)
* DNS server address
* WINS server address

អតិថិជនដែលផ្ញើសារ DHCP ស្វែងយល់ដើម្បីទទួលបានអាស័យដ្ឋាន IP ផ្ញើការចាក់ផ្សាយទាំងនៅស្រទាប់ទី ២ និងស្រទាប់ទី ៣ •ការចាក់ផ្សាយស្រទាប់ទី ២ សុទ្ធតែជាលេខកូដបាបដែលមើលទៅដូចនេះ៖ ffff: ff: ff: ff: ff ។ ការចាក់ផ្សាយស្រទាប់ទី ៣ គឺ ២៥៥.២៥៥.២៥៥.២៥៥ ដែលមានន័យថាបណ្តាញទាំងអស់និងម៉ាស៊ីន DHCP ទាំងអស់គ្មានការតភ្ជាប់ដែលមានន័យថាវាប្រើ User Datagram Protocol (UDP) នៅស្រទាប់ដឹកជញ្ជូនដែលត្រូវបានគេស្គាល់ផងដែរថាជាស្រទាប់ Host-to-Host ដែលយើងនឹង និយាយអំពីពេលក្រោយការមើលឃើញកំពុងជឿជាក់ដូច្នេះនេះគឺជាឧទាហរណ៍នៃលទ្ធផលពីអ្នកវិភាគរបស់ខ្ញុំដែលបង្ហាញពីស្រទាប់ទី ២ និង ការចាក់ផ្សាយស្រទាប់ទី ៣**។**