Hacker Highschool

SECURITY AWARENESS FOR TEENS



LESSON 3

အင်တာနက် အောက်၌

BENEATH THE INTERNET

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM

သတိပေးချက်

ဤ Hacker Highschool စီမံကိန်း သည်၊ လေ့လာသင်ယူရေး ကရိယာ တစ်ခုဖြစ်ပြီး လေ့လာရေး အချက်များပါဝင်သည့်အလျောက် အနာသတရာယ်ရှိပါသည်။ အကယ်၍ အချို့သောသင်ခန်းစာများအား၊ တလွဲအသုံး ချခြင်း၊ အဖျက်အမှောင့်ရည်ရွယ်ချက်ဖြင့်သုံးခြင်းသည်၊ ကိုယ်တိုင်နစ်နာမှုများဖြစ်စေနိုင်ပါသည်။ နည်းပညာအချက်အလက်များမှ ဖြစ်နိုင်ချေရှိသောရလာဒ်များကို သေချာစွာလေ့လာမထားပါက၊ ဘေးထွက်ဆိုးကျိုးများ ဖြစ်ပေါ်လာနိုင်ပါသည်။ ဤသင်ခန်းစာများကိုအသုံးပြုသော ကျောင်းသား၊ သူများသည်၊ လေ့လာခြင်း ၊ ကြိုးစားအားထုတ်ခြင်းနှင့် လက်တွေ့အသုံးချခြင်းများ ပြုလုပ်ရာတွင် ကောင်းစွာသင်ကြားခြင်းများကို သင်ယူခြင်းအပြင်၊ စနစ်တကျ ကြီးကြပ်ခြင်းကို ခံယူသင့်ပါသည်။ မည်သို့ဖြစ်စေ ISECOM အဖွဲ့အစည်းမှ ဤသင်ခန်းစာများတွင်ပါဝင်သော မည်သည့်သတင်းအချက်အလက်များကိုမဆို လွဲမှားစွာအသုံးပြုခြင်းအတွက်တာဝန်ယူနိုင်မည် မဟုတ်ပါ။

အောက်ပါသင်ခန်းစာများ၊ လေ့ကျင့်ခန်း စာအုပ်များကို မည်သူမဆို ISECOM ၏စည်းကမ်းချက်များ အားလိုက်နာ၍ ဖတ်ရှုလေ့လာနိုင်ပါသည်။ ပဂဿဂလိကနည်းပညာကျောင်း၊ နိုင်ငံတော် နည်းပညာကျောင်းများ၊ အခြေခံအလယ်တန်း၊အထက်တန်းများတွင် Hacker Highschool စီမံကိန်းမှ ဆောင်ရွက်မှုများ အားလုံးကို စီးပွားဖြစ်အသုံးပြုခြင်းများအား တားမြစ်ပါသည်။ ဤစာအုပ်ပါ အချက်အလက်များအား ကူးယူ၍၊ မည်သည့် ပုံစံဖြင့်ဖြစ်စေ ပြန်လည်ထုတ်လုပ်ရောင်းချခြင်းများအား တားမြစ်ပါသည်။

ဤစာအုပ်ပါအချက်အလက်များမှမည်သည့်အမျိုးအစားဖြစ်စေ၊သင်ခန်းစာဖြစ်စေ (သို့)လေ့ကျင့်ခန်း များဖြစ်စေ ပါဝင်မှုများအား ခွင့်ပြုချက်လိုင်စင် မရှိပဲ တန်ဖိုးတစ်ခုခုဖြင့်ရောင်းချခြင်းကို ပြင်းထန်စွာတားမြစ်ထားပါ သည်။

လိုင်စင်ဂယ်ယူရန် http://www.hackerhighschool.org/licensing.html HHS website တွင်ဂယ်ယူနိုင်ပါသည်။ ဤ HHS စီမံကိန်းတွင် အဖိုးတန်မှု၊အကျိုးရှိမှုများ ရှိမည်ဆိုလျင်၊ HHS အား License ဂယ်ယူခြင်း၊ လူဒါန်းခြင်း၊အထောက်အပံ့ပေးခြင်းများ ဖြင့် ကူညီပေးပါရန် တောင်းဆိုပါသည်။

Table of Contents

Contributors

Pete Herzog, ISECOM
Glenn Norman, ISECOM
Marta Barceló, ISECOM
Chuck Truett, ISECOM
Bob Monroe, ISECOM
Kim Truett, ISECOM
Gary Axten, ISECOM
Marco Ivaldi, ISECOM
Simone Onofri, ISECOM
Greg Playle, ISECOM
Tom Thomas, ISECOM
Mario Platt
Ryan Oberto, Johannesburg South Africa
Vadim Chakryan, Ukraine
Peter Houppermans

Translators

Htet Aung @ Starry Sky, Myanmar

ISECOM

မိတ်ဆက်ခြင်း နှင့် ရည်ရွယ်ချက်များ

ရှေးယခင်အချိန်များက အင်တာနက်ပေါ်မလာခင် အီလက်ထရွန်နစ်ဆက်သွယ်ရေးဆိုတာ မှော်ပညာဆန်ဆန်ဖြစ်ခဲ့ပါတယ်။ ကွန်ပြူတာထုတ်လုပ်သူများအားလုံးသည် စက်တွေကဂါယာတွေအပေါ်မှာမည်သို့ဆက်သွယ်သင့်တယ်ဆိုတဲ့ ကြံဆမှုကိုယ်စီ ရှိနေခဲ့ကြပါတယ်။ ကွန်ပြူတာ Wang က Burroughs စက်နဲ့ဆက်သွယ်ရန်ဖြစ်နိုင်ချေကိုတော့ မည်သူမျှထည့်မစဉ်းစားခဲ့ ကြပါ ဘူး။

သိပသပံပညာရှင်တွေနဲ့ ကျောင်းသားတွေက mainframe ကွန်ပြူတာတစ်လုံးကို သုံးခွင့်ရရန် terminal တွေကိုအသုံးပြုတတ် လာတဲ့အခ ါ ကမဿဘာကြီးပြောင်းလဲလာခဲ့ပါတယ်။ IBM mainframe တစ်လုံးရောက်လာတာနဲ့ ပိုင်ရှင်တွေက သူတို့ PC တွေမ့ တဆင့် အဲဒီ IBM ကိုအသုံးပြုချင်ခဲ့ကြပါတယ်။ မကြာခင်မှာပဲ modems တွေက dail-up ချိတ်ဆက်မှုတွေပြုလုပ်ခဲ့ပြီး user တွေက terminal emulator တွေထဲမှာ အလုပ်လုပ်ခဲ့ကြတယ်။ Networking ကမှော်ပညာတစ်ခုဖြစ်လာခဲ့ပြီး အတွင်းလူတွေ ကတော့ **guru** များလို့ခေါ်ကြပါတယ်။

လူထုထံလမ်းဖွင့်ပေးလိုက် တဲ့ စစ်တပ်စီမံကိန်းတစ်ခုအဖြစ်စတင်ခဲ့တဲ့ အင်တာနက်ပေါ်လာတဲ့အခါ ကမဿဘာကြီးကညင်သာစွာ ထပ်မံပြောင်းလဲခဲ့ပါတယ်။ Networking က ရုံးတစ် ခု (သို့) အများဆုံး နယ်ပယ်တစ်ခုကိုကန့်သတ်ထားခြင်းကြောင့် အမြဲတမ်း အတွင်းနယ်ပယ်ဖြစ်ခဲ့ပါတယ်။ ဒါဆို အဲဒီမတူညီတဲ့ ကွန်ယက်တွေ ဘယ်လိုဆက်သွယ်ကြမလဲ?

အဖြေကတော့ တည်ရှိနေတဲ့ကွန်ယက်တွေကို ယေဘူယျအားဖြင့် internet protocol(IP) လို့ခေါ်တဲ့၊ ကမဿဘာ့အခြေခံလိပ်စာ ပေးတဲ့စနစ် "wedge" ပဲဖြစ်ပါတယ်။ Packet တွေက အီလက်ထရွန်တွေ၊ အလင်းရောင်တန်း တွေ (သို့) ရေဒီယိုလှိုင်းတွေ ကဲ့သို့ ခရီးနှင်ကြပေမယ့်၊ အဲဒီစနစ်တွေကခင်ဗျားအတွက် အဓိကမကျပါဘူး၊ ခင်ဗျားရဲ့ IP နဲ့ ခင်ဗျားဆက်သွယ်မယ့် စက်ရဲ့ IP ကသာအဓိကကျတာပါ။

အဲဒီအယူအဆကို ရှုပ်ထွေးစေတဲ့ အရာတစ်ခုက IP တစ်ခုမှာ လူတစ်ဦးထက်ပိုရှိနေနိုင်ခြင်းပဲဖြစ်ပါတယ်။ ဥပမာအားဖြင့်၊ Networking လောကမှာ ဆာဗာတစ်လုံးက HTTP နှင့် HTTPS နှစ်ခုစလုံးနှင့် FTP ပါ ဂန်ဆောင်မှုပေးတဲ့အခါ ထိုရှုပ်ထွေးစေမှု ဖြစ်တတ်ပါတယ်။ အဲဒီအတိုကောက်တွေရဲ့ နောက်ဆုံးက P တွေကို သတိထားကြည့်ပါ။ အဲဒါက "ဆက်သွယ်မှုပုံစံတစ်ခု" ဖြစ်တဲ့ **protocol** အတွက်ရည်ညွှန်းချက်ပဲဖြစ်ပါတယ်။

ယဿခုသင်ခန်းစာက Windows, Linux နဲ့ OSX တွေမ့ ာ protocol တွေနဲ့ ၎င်းတို့ရဲ့ port တွေအလုပ်လုပ်ပုံကိုနားလည်စေရန် ကူညီပါလိမ့်မယ်။ ထိုအပြင် (ပြီးခဲ့တဲ့ သင်ခန်းစာတွေမှာဖေါ်ပြခဲ့တဲ့) ခင်ဗျားစက် ရဲ့ ကွန်ယက်ဆိုင်ရာလုပ်ဆောင်နိုင်စွမ်းကို ဖော်ထုတ်ပေးတဲ့ အသုံးဝင်မှုတွေကို ရင်းနှီးမှုရစေပါလိမ့်မယ်။

ဒီသင်ခန်းစာပြီးဆုံးတဲ့အခါ အောက်ပါ အခြေခံဗဟုသုတများရရှိပါလိမ့်မယ်။

- the concepts of networks and how communication takes place
- IP addresses
- ports and protocols

အခြေခံ Networking အယူအဆများ

Networking အစကတော့ local area network (**LAN**) ပဲဖြစ်ပါတယ်။ LAN တွေမှာ ရုပ်ပိုင်းဆိုင်ရာနေရာတစ်ခုထဲမှာ တည်ရှိနေတဲ့ ကွန်ပြူတာတွေအချင်းချင်း **administrators** များက အသုံးပြုခွင့်ကိုထိန်းချုပ်ပြီး printer နဲ့ drive နေရာတွေ ကဲ့သို့ရင်းမြစ်များ မျှဝေရန် ဆောင်ရွက်နိုင်ပါတယ်။ အောက်ပါအခန်းမှာ ယေဘူယျ network သုံးပစ္စည်းများနှင့် topology များ ဖေါ်ပြထားပါတယ်။

Devices

Hacker တစ်ယောက်အနေနဲ့ ခင်ဗျား အသက်မွေးမယ်ဆိုရင်တော့၊ ရှေ့ဆက်ပြီး network diagram များ၊ များစွာတွေ့ရမှာ ဖြစ်ပါတယ်။ ၎င်းက ယေဘူယျ အသုံးဝင်သောသဘောသဘာဝများကိုနားလည်ရန် အသုံးဝင်ပါတယ်။

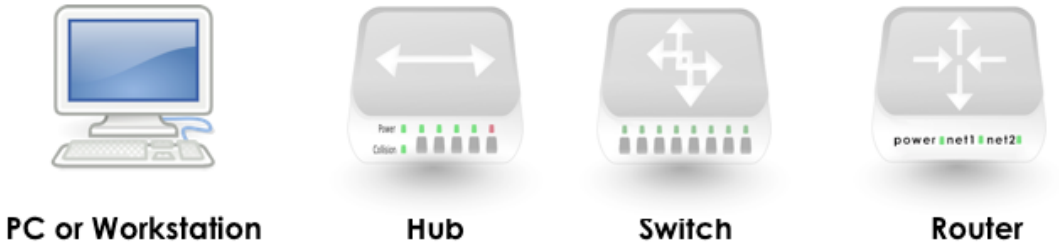


Figure 3.1: Common Network Symbols

Hub တစ်လုံးက တယ်လီဖုန်းလိုင်းအဖွဲ့အစည်း အဟောင်းတစ်ခုနဲ့ တူပါတယ်။ ။ လူတိုင်းက ဂါယာကြိုးတစ်ခုတည်းပေါ်မှာ ရှိနေပြီး အဲဒီပေါ်မှာပြောနေသမျှတွေကို လူတိုင်းကြားနေရပါတယ်။ အဲဒါက LAN ကို လျှင်မြန်စွာ ဆူညံလာစေပါတယ်။

Switch ကတော့ ပိုကောင်းလာပါတယ်။ ။ လမ်းကြောင်းတွေကို စစ်ထုတ်ထားတဲ့အတွက် ကွန်ပြူတာနှစ်လုံးထဲအချင်းချင်း သီးသန့်ဆက်သွယ်နိုင်ပါတယ်။ ဒါပေမယ့် hub လိုပဲ ၎င်းကို LAN ပေါ်မှာပဲအသုံးပြုပါတယ်။

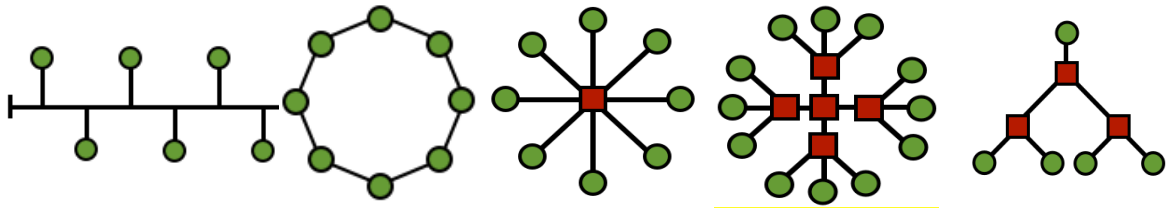
router ကိုတော့ LAN တွေကြားမှာ သုံးပါတယ်။ ။ ၎င်းကို အင်တာနက်နဲ့ အခြား network တွေဝင်ရောက်ရန်အသုံးပြုပြီး ၎င်းက IP address ကိုအသုံးပြုပါတယ်။ ၎င်းက ပို့ခံလိုက်ရတဲ့ packet တွေကို ကြည့်ပြီး ထို packet တွေကဘယ်ကိုသွားရမယ် ဆိုတာ ဆုံးဖြတ်ပေးပါတယ်။ အကယ်၍ packet တစ်ခုက "အခြား" network တစ်ခုနဲ့သက်ဆိုင်တယ်ဆိုရင်၊ ၎င်းက ယာဉ်ထိန်းရဲတစ်ယောက်ကဲ့သို့ အဲဒီ packet ကို သက်ဆိုင်ရာနေရာသို့ ပို့လိုက်ပါတယ်။

Topologies

Topology ဆိုတာ "ကျွန်တော်တို့ ချိတ်ဆက်တဲ့နည်းလမ်း" ဆိုတာကို နောက်နည်းလမ်းတစ်မျိုးဖြင့်ခေါ်ဆိုခြင်းဖြစ်ပါတယ်။ ကျွန်တော်တို့ topology တွေနဲ့စပ်လျဉ်း၍ ချမှတ်တဲ့ဆုံးဖြတ်ချက်တွေက အသုံးပြုတဲ့နည်းပညာတွေ၊ နည်းပညာ နှင့် ရုပ်ပိုင်း ဆိုင်ရာ အကန့်အသတ်တွေ၊

စွမ်းဆောင်ရည် နှင့် လုံခြုံရေး လိုအပ်ချက်တွေ၊ အဖွဲ့အစည်း၏ အရွယ်အစား နှင့် သဘာဝ စသည်တို့ အပေါ်မူတည်၍ ကောင်းကျိုးတွေသာမက ဆုတ်ရုတ်မှုများလည်းဖြစ်စေနိုင်ပါတယ်။

LAN တစ်ခုရဲ့ ရုပ်ပိုင်းဆိုင်ရာတည်ဆောက်မှုက၊ အောက်ပါ ရုပ်ပိုင်းဆိုင်ရာ topology များကဲ့သို့ ဖြစ်ပါတယ်။



Bus **Ring** **Star** **Extended Star** **Hierarchic**

Figure 3.2: Toplogies

bus topology တစ်ခုမှာ၊ ကွန်ပြူတာအားလုံးကို ကြိုးတစ်ချောင်းထဲပေါ်မှ ၁ ချိတ်ဆက်ထားပြီး၊ ကွန်ပြူတာတစ်လုံးချင်းစီက အခြားမည်သည့်အလုံးနှင့်မဆို တိုက်ရိုက်ဆက်သွယ်နိုင်ပါတယ်။ ဒါပေမယ့် bus ရဲ့ မည်သည့်အစိတ်အပိုင်းမဆို ပြတ်တောက ် သွားတဲ့အခ ါ network တစ်ခုလုံး ချိတ်ဆက်မှုပြတ်တောက်သွားပါတယ်။

ring ချိတ်ဆက်မှုမှာ၊ ကွန်ပြူတာတစ်လုံးချင်းစီကို တစ်လုံးပြီး၊တစ်လုံးဆက်၍ချိတ်ဆက်ထားပြီး နောက်ဆုံးတစ်လုံးကို ပထမဆုံးတစ်လုံးနှင့် ချိတ်ဆက်ထားသဖြင့် ကွန်ပြူတာတိုင်းက ဘေးချင်းကပ်လျက်ကွန်ပြူတာတွေကိုပဲ တိုက်ရိုက် ဆက်သွယ် နိုင်ပါတယ်။

Bus topology များကိုတော့ ဒီနေ့ခေတ်မှာ မသုံးသလောက်ရှိနေပါပြီ။ Ring နည်းပညာများကိုတော့ ပုံမှန်အားဖြင့် မှားယွင်းတ ဲ့ tolerance တွေမဖြစ်ရန်နှင့် ခိုင်မာမှုရှိစေရန်အတွက ် traffic များအ ား ဆန့်ကျင်ဘက်တွေကိုပို့ပေးခြင်းကဲ့သို့ ဆန့်ကျင်လျက် လည်ပတ်နေသော ring နှစ်ခုဖြင့် အပြန်အလှန်ချိတ်ဆက်မှုအဆင့်တွေမှာ သုံးလေ့ရှိပါတယ်။

star topology မှာတော့၊ ကွန်ပြူတာများကို အချင်းချင်းတိုက်ရိုက်ချိတ်ဆက်ခြင်းမပြုလုပ်ပဲ၊ ၎င်းတို့အား ကွန်ပြူတာတစ်လုံးမှ တစ်လုံးသို့ အချက်အလက်များကို လက်ဆင့်ကမ်းပို့ပေးတ ဲ့ hub (သို့) switch များဖြင့်ချိတ်ဆက်ထားပါတယ်။

အကယ်၍ hub (သို့) switch များ အချို့ကို အချင်းချင်းချိတ်ဆက်ထားရင်၊ **extended star** topology ကိုရရှိမှာဖြစ်ပါတယ်။

star (သို့) extended star topology တစ်ခုမှာ၊ ဗဟိုအမှတ်အားလုံးက အခြေခံအားဖြင့်တူညီကြတဲ့ **peers** တွေဖြစ်ကြပါ တယ်။ star (သို့) extended star topology ကတော့ ဒီနေ့ခေတ် အသုံးများတဲ့ LAN topology ဖြစ်ပါတယ်။

မည်သို့ဖြစ်စေ၊ အကယ်၍ခင်ဗျားက star (သို့) extended star နှစ်ခုကို ကွန်ယက်နှစ်ခုကြားမှာ လမ်းကြောင်းထိန်းချုပ် ကန့်သတ်တဲ့ ဗဟိုအမှတ်ကိုသုံးပြီး အတူတကွချိတ်ဆက်တဲ့အခါ **hierarchical** ကွန်ယက် topology တစ်ခုရရှိပါလိမ့်မယ်။ **hierarchical** ကို ကြီးမားတဲ့ လုပ်ငန်းတွေမှာသုံးကြပါတယ်။

ကစားပွဲစတင်ခြင်း - နောက်ဖေးပေါက်(Back Door)ကို ဖွင့်ထားခြင်း

နွေရာသီရဲ့လောင်ကျွမ်းနေတဲ့နေရောင်ခြည်အောက်မှာ၊ လေအေးပေးစက်တပ်ဆင်ထားတဲ့ မြို့နယ်ရဲ့စခန်းဂ၏အငယ်စား ကွန်ယက် တပ်ဆင်ခြင်းတွင် ကူညီပေးရန် Jace က ဆန္ဒရှိခဲ့ပါတယ်။ သူတို့က ကွတ်ကီးတွေ၊ အပူဒဏ်မှကင်းလွတ် နိုင်ခြင်း၊ စကားစမြည်ပြောခြင်းနှင့် backdoors များ ထည့်သွင်းနိုင်ရန် အခွင့်အရေးများဖြင့် သူမကိုကမ်းလှမ်းခဲ့ပါတယ်။ Jace က ဆယ်စုနှစ်များစွာကအသုံးပြုခဲ့တဲ့ စတီးအလုပ်စားပွဲတွေအောက်မှာတွားသွားခြင်းဖြင့် wifi access point ပှက်၍ ထားနိုင်ရန်၊ ဖုံးကွယ်နေတဲ့ချောင်လေးတစ်ခုကို ရှာတွေ့ခဲ့ပါတယ်။ သူမက access point ကိုပလပ်တပ်လိုက်ပြီး အမှိုက် အနည်းငယ်ကို ထိုအပေါ်မှာတင်ခဲ့ပြီး၊ သူမ ကြိုတင်တပ်ဆင်ထားတဲ့ နံရံကပ်အပေါက်များဆီသို့ Ethernet ကြိုးသွားရန် ကြိုးလျှောက်လမ်းတစ်ခု တူးနေခဲ့ပါတယ်။

ကြီးမားတဲ့လက်တစ်ခုက သူမအပေါ်က စားပွဲခုံပေါ်ရိုက်ချလိုက်ပါတယ်။ Jace ကလန့်ပြီးထလိုက်သဖြင့်ခုံနှင့် ဆောင့် မိကာ"Ow! My head!"လို့ အော်လိုက်ပြီး "ရှင့်ဆာဗာတွေကိုတပ်ဆင်ဖို့ ငါ့ကိုမလုပ်စေချင်ဘူးလား?" လို့မေးလိုက် ပါတယ်။

ရဲသားက သူ့ရဲ့လည်ချောင်းကိုရှင်းလိုက်ပြီး ပါမောက္ခသခရူးတစ်ယောက်လေသံဖြင့် "ကောင်းပြီ ငါပြောမယ်၊ ဒါပေမယ့် လျှပ်စစ်ရောင်ခြည် လျှပ်ခံပစ္စည်း (flux ray resistor)တစ်ခုက micro-channel ဖြတ်သန်းစီးဖင်မှကို ဘယ်လို ခုခံ နိုင်တယ်ဆိုတာတော့သိပ်မသေချာဘူး။ အထူးသဖြင့် ပြီးခဲ့တဲ့ လရောင်ဖြာတဲ့ အဂၤါနေ့တုန်းကပေါ့။" လို့ပြောလိုက်ပါ တယ်။

Jace က ဆယ်ကျော်သက်တွေလောင်ရယ်တဲ့ပုံစံဖြင့် သူမခြေဖဝါးတွေကိုတဖျတ်ဖျတ်ရိုက်လိုက်ပါတယ်။ "ကြည့်ရတာ ခင်ဗျားကပေါက်ကရလေးဆယ်တွေပြောဖို့ လွယ်ကူတယ်ထင်တယ်။ ပြီးတော့ ကျွန်မကွတ်ကီးတွေ ဘယ်တော့ရမှာလဲ၊ အရာရှိ Kickam?" လို့ပြောလိုက်ပါတယ်။

"ကျေးဇူးပြုပြီး ငါ့ကို Hank လို့ခေါ်ပါ၊ Jace။ မင်းငါ့ကို အရာရှိ Kickam လို့ခေါ်တဲ့အခါ ငါအဖိုးကြီးတစ်ယောက်လို ခံစားရတယ်။" လို့ သူက မနှစ်သက်စွာပြောပေမယ့် သူမကတော့ ဒါက social engineering ဆိုတာသိသွားပါတယ ် - အမှန်တကယ် သူမကို cookies တွေအကြောင်းမေ့သွားအောင် အာရုံပြောင်းလိုက်တာဖြစ်ပါတယ်။

"သတင်းဆိုးတွေမပြောချင်ပါဘူး၊ Hank ရေ၊ ဒါပေမယ့်ရှင်က အဖိုးအိုတစ်ယောက်ပါပဲ။"

"ဟာ၊ ဒါငါ့ကို စိတ်ထိခိုက်စေတယ်။ ငါက မအိုသေးပါဘူး၊ အသိသာကြီးပါ။" လို့ Jace ရဲ့ စုတ်ဖွာနေတဲ့ဖိနပ်တွေ စားပွဲကြီးအောက်မှာပျောက်ကွယ်သွားတဲ့အခါ ပေါလစ်နိုင်နိုင်တိုက်ထားတဲ့နက်ပြောင်နေတဲ့ သူ့ရဲ့shoes ကို ဆက်၍ ငေး ကြည့်ရင်း ဆန့်ကျင်တုန့်ပြန်လိုက်ပါတယ်။

ထို့နောက ် သစ်ခေါက်ညှိရောင်မျက်လုံးတွေနဲ့ပင့်ကူမျှင်တွေဖုံးနေတဲ့မျက်နှာတစ်ခုပေါ်လာပါတယ်။ Jace ရဲ့လက်တစ်ဖက် အောက်မှာတော့ ကြိုးဘီးတစ်လုံးရှိနေသေးပါတယ်။ Hank က သူမမျက်နှာနှင့် ပုခုံးပေါ်ကပင့်ကူမျှင်တွေကို ကူပြီး ဖယ်ရှားပေးလိုက်ပါတယ်။

"ကူညီပါဦး၊ ရက်စက်တဲ့ ရဲကြီးရေ" လို့ jace က ရယ်စရာပြောပါတယ်။

"ကဲ ရန်လိုတဲ့လူဆိုးရေ၊ မင်းရဲ့ ပညာသားပါပြီးယုတ်မာတဲ့ အကြံအစည်တွေကို သင်ပေးပါဦး" လို့ အမွှေးထူထူနဲ့ တောင့်တင်းတဲ့ ဥပဒေဘက်တော်သား Hank က အသနားခံသည့် လေသံဖြင့် ပြန်ပြောပါတယ်။

ဒီလိုဆိုတော့ ခံစားချက်ကောင်းတာပေါ့၊ ထို့ကြောင့် သူမက "ဒီ ကွန်ယက်ချိတ်ဆက်တဲ့ ပညာရပ်ကို ရှင်သိချင်တာ သေချာလား?" လို့ မေးလိုက်ပါတယ်။ သူကတော့ လိုလိုချင်ချင်ဖြင့် ခေါင်းတညိတ်ညိတ် လုပ်နေခဲ့ပါတယ်။ Jace က ခုန်ဆွဆွဖြစ်နေတဲ့ဦးခေါင်းပဲလို့ ထင်ခဲ့ပါတယ်။

"ကောင်းပြီ၊ ကျွန်မလုပ်ခဲ့တာက ပစသညစည်းကိရိယာများ၊ ကွန်ပြူတာများ၊ hub များ၊ ပလပ်များ၊ switch များ၊ router နှင့် firewall များ ဘယ်မှာရှိတယ်၊ ဘယ်ကိုသွားမယ်ဆိုတာပြတဲ့ မြေပုံအညွှန်းကဲ့သို့ ကွန်ယက်သွင်ပြင်တစ်ခု စီစဉ်ပုံစံချတာ ပါပဲ။ အခုလို စီမံကိန်းမျိုးကို မြေပုံအညွှန်းမပါပဲ စလို့မရဘူးလေ။" လို့ သူမက ဖျတ်ခနဲကြည့်ပြီး ပြောလိုက်ပါတယ်။ "အခုလုပ်နေတာတွေ အားလုံးက node အားလုံးက အခြားnode တွေကို ပြတ်တောက်ခြင်းတစ်ခုမှမရှိပဲ ဆက်သွယ်နိုင် သလားဆိုတာ သေချာစေရန်လုပ်ဆောင်ခြင်းပါပဲ။ အဲဒါကြောင့်၊ bus တည်ဆောက်ပုံမှာ node တစ်ခုကျသွားခဲ့ရင် အခြား node များလည်းကျသွားတဲ့အတွက် bus တည်ဆောက်မှုပုံစံက ပြသသသနာဖြစ်နေသလိုပေါ့။" Hank က ခေါင်း တညိတ်ညိတ်လုပ်နေပြီး Jace က စကားဆက်ခဲ့ပါတယ်။

"networking က ဒီရဲဆိုင်၊ အဲ၊ ရဲစခန်းဖြစ်ပြီး တစ်စုံတစ်ယောက်က မသကသငသစရာ လူတစ်ယောက်ကို ခေါ်လာခဲ့တယ်လို့ စဉ်းစားကြည့်လိုက်ပါ။ အဲဒီမသကသသငသဖွယ်ဖြစ်သူကိုရိုက်နှက်ရန် တစ်ဦးတစ်ယောက်ရဲ့အချိန်ကိုမလုယူပဲ မျှတတဲ့အလှည့် ကိုယ်စီ ရဲတိုင်း ရထိုက်ပါတယ်။ အကယ်၍ ဒီဒုကသခသည်၊ အဲ မသကသငသစရာလူလို့ ဆိုလိုတာပါ၊ သူကို နောက် အကျဉ်းတစ် ခုဆီကို ပြောင်းရွှေ့လိုက်ရင်၊ သူဘယ်ရောက်သွားတယ်ဆိုတာကို၊ သူကိုရိုက်နှက်ရဉီးမည့်ရဲတိုင်း သိဖို့လိုပါတယ်။

"ဟ ား Jace, ကြည့်ရတာ ငါတို့လိုအေးချမ်းတဲ့ရဲတွေအကြောင်း အခုလိုဆက်ပြောနေမယ်ဆိုရင် မင်းလည်းရိုက်နှက် မှု ကောင်းကောင်းတစ် ခု လိုလာတော့မယ်ထင်တယ်။" လို့ Hank က သူသေနတ်ခါးပတ်ကိုဆွဲလိုက်ပြီး မဖြစ်စလောက် ဟမ်းဗိုက်ကြွက်သားကို ချပ်လျက် ပြောလိုက်ပါတယ်။

Jace က "ဟွန်း" ဟု ရယ်စရာနှင့် ငေါ့လိုက်ပါတယ်။ "ဒါဆို၊ အဲဒီမသကသငသဖွယ်ဖြစ်သူက အချက်အလက် packet တစ်ခု ဖြစ်ပြီး ရှင်တို့လူရမ်းကားရဲတွေက ကွန်ယက်သုံးပစသညစည်းတွေပဲပေါ့။ ပြီးတော့ ပစသညစည်းတိုင်း၊ switch၊ router၊ firewall၊ အခြား ဆာဗာ (သို့) ဘယ်အရာမဆိုတိုင်းက အဲဒီအချက်အလက် packet ဆက်သွယ်တဲ့အရာကိုသိဖို့ လိုအပ်ပါတယ်။ ရှင်သိပါတယ်၊ ရဲတွေရဲ့ နံပါတ်တုတ်တွေနဲ့ရိုက်သလိုပေါ့။ အဲဒါကို ရှင်တို့ကတော့ သစ်သားခေါင်းလျှော်ရည်ပေးခြင်းလို့ ခေါ်တယ်လို့ ကျွန်မထင်တယ်။"

Hank က သူဆီမှာမရှိတဲ့နံပါတ်တုတ်ကို စမ်းလိုက်ပါတယ်။

Jace က တခစ်ခစ် ရယ်လျက်၊ ကြိုးရစ်ဘီးကို ဒိုင်းကာကဲ့သို့မလိုက်ပြီး "ဟား၊ ကျွန်မမှာ ဂါယာကြိုးတစ်ဘီးရှိတယ်နော် ပြီးတော့ သုံးလိုက်ရမှာဂန်မလေးဘူးနော်။ ကော်ဖီခွက်ကိုချထားပြီး ဘယ်သူကိုမှမနာကျင်စေနဲ့။" လို့ပြောရင်း ရယ်မော လျက် တံဆိပ်မချိတ်ထားတဲ့ Hank အပေါ်သို့ ပစ်လွှဲချလိုက်ပါတယ်။ ဂိုး၊ ဒီလူက တကယ့်ကိုသန်မာတာပဲ၊ သူမ နားလည်လိုက်ပါတယ်။ သူမပုခုံးပေါ်ရောက်နေတဲ့သူလက်က သူမအားသတိဂင်စေခဲ့ပါတယ်။

သူမက ရုက်သွေးဖြာလျက်၊ သွက်သွက်လေး ပြန်ထလိုက်ပါတယ်။ "ကဲ ဒီမှာ device နှစ်မျိုးရှိတယ်။ ကောင်းမွန်တဲ့ device နဲ့ ညံ့ဖျင်းတဲ့အရာတွေပေါ့၊ ရဲတွေလိုပဲပေါ့။" နီးကပ်လာတဲ့ ယူနီဖေါင်းဂတ်လေးယောက်က မသင့်လျော်သော အချိန်မှာ တိုက်တိုက်ဆိုင်ဆိုင်ပေါ်ထွက်လာခဲ့ပြီး "ညံ့ဖျင်းတဲ့အရာတွေပေါ့၊ ရဲတွေလိုပဲပေါ့။" ဆိုတာကိုပဲ နားကြားမှားခဲ့ပါ တယ်။ "ကောင်းမွန် တဲ့ devices များကသူတို့လုပ်သမျှအားလုံးမှတ်မိသလို၊ သူတို့လုပ်ဆောင်မှုတွေအတွက် မှတ်တမ်းများ ထားပါတယ်။" လို့ ထစ်ထစ်အအဖြင့် Jace က ဆက်ပြောခဲ့ပါတယ်။

"ပြီးတော့ ညံ့ဖျင်းတဲ့တစ်ခုကရော? ရဲတွေလိုပဲပေါ့ လား?" လို့ ရဲမူးချပ်က မေးလိုက်ပါတယ်။

ကစားပွဲ ပြီးဆုံး

The TCP/IP (DoD) Model

TCP/IP ကို United States ရဲ့ **DOD (Department of Defense)** နှင့် **DARPA (Defense Advanced Research Project Agency)** တို့က ၁၉၇၀ ခုနှစ်မှာ ဖေါ်ထုတ်ခဲ့ကြပါတယ်။ TCP/IP ကို မည်သူမဆို computer တွေကိုချိတ်ဆက်နိုင်ရန် အောင်၊ အချက်အလက်တွေ လဲလှယ်ဆက်သွယ်နိုင်အောင်ရည်ရွယ်၍ အကန့်အသတ်မရှိသောစံနှုန်းဖြစ်ရန် ပုံဖေါ်ခဲ့ပါတယ်။ နောက်ဆုံးမှာတော့ ၎င်းက အင်တာနက်ရဲ့အခြေခံဖြစ်လာခဲ့ပါတယ်။

ယေဘူယျအားဖြင့်၊ အရိုးရှင်းဆုံး TCP/IP ပုံစံကို **DOD Model** လို့ခေါ်ပြီး ကျွန်တော်တို့အဲဒီကနေစမှာပါ။

Layers - အလွှာများ

ရိုးရှင်းသော DoD model က device နှစ်ခုကြားက ဆက်သွယ်မှုဖြစ်စဉ်ကို ပိုင်းခြားထားတဲ့ သီးခြားစီရှိသော စုစုပေါင်းအလွှာ လေးခုကို ပြဋ္ဌာန်းထားပါတယ်။ အဲဒီ အချက်အလက်တွေဆက်သွယ်တဲ့ အလွှာတွေကတော့ -

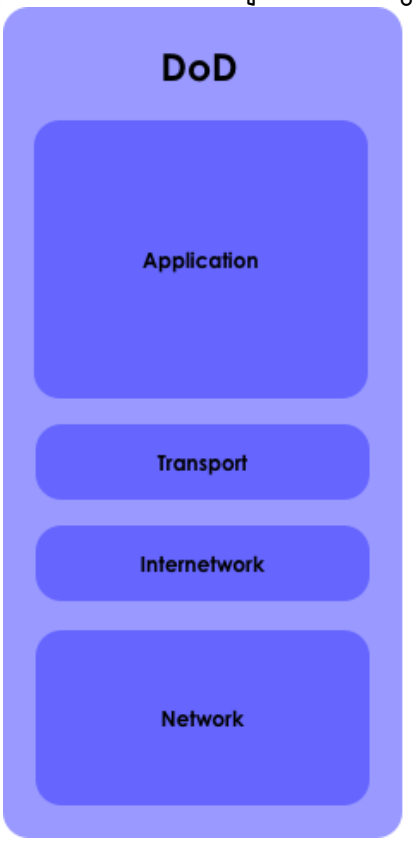


Figure 3.3: The DoD Model

Application

Application အလွှာက တကယ့်ကို ခင်ဗျားထင်ထားတဲ့အရာပဲ ဖြစ်ပါတယ် - အဲဒီအလွှာက Firefox, Opera, email clients, social networking sites, instant messaging နှင့် chat application တွေလို application တွေနဲ့ အင်တာနက်ကို ချိတ်ဆက်တဲ့ application အချို့ - ရုံးသုံး application တွေ၊ ဥပမာ၊ အွန်လိုင်းမှာ clip art တွေရွေးချယ်မှုကဲ့သို့ application အလုပ်လုပ်တဲ့အလွှာဖြစ်ပါတယ်။ application အလွှာက အခြားအလွှာတွေ တာဝန်ယူထားတဲ့ လုပ်ငန်းတွေကိုဖန်တီးပါတယ်။ အကောင်းဆုံးနှိုင်းယှဉ်ပြနိုင် တဲ့ ဥပမာတစ်ခုကတော့ စာပို့စနစ်ပဲဖြစ်ပါတယ်။ အဲဒီ စာပို့စနစ် application က မည်သို့အသုံးပြု ရမယ်ဆိုတဲ့အညွှန်းများဖြင့်

ရစ်ပတ်ထုပ်ပိုးထားတဲ့ package တစ်ခုကိုဖန်တီးပြီး အဲဒီ package ကို စာပို့ခန်း (Transport အလွှာ) ထဲပို့လိုက်ပါတယ်။

Transport

Transport အလွှာက **sessions** လို့ခေါ်တဲ့ ကွန်ယက်ချိတ်ဆက်မှုတွေကို ဖွဲ့စည်းပါတယ်။ အင်တာနက်လောကမှာတော့၊ Transport အလွှာရဲ့ အဓိက protocol က **TCP, the Transmission Control Protocol** ဖြစ်ပါတယ်။ TCP က အဲဒီ Package ရဲ့အပေါ်မှ နောက်ထပ် "ရစ်ပတ်ထုပ်ပိုးမှု" ဖြစ်တဲ့ (package ၃ခု အနက် သဿဃခု) မည်သည့် package ဖြစ်တယ်၊ အဲဒီ package က လက်ခံသူထံ ရောက်၊မရောက် မည်သို့စစ်မလဲ၊ အဲဒ ီ packageက ပကတိအတိုင်း ရှိတယ်၊မရှိဘူ း ဆိုတဲ့ ညွှန်းချက်များဖြင့် အပေါ်မှထပ်၍ထုတ်ပိုးလိုက်ပါတယ်။

ခင်ဗျား အမေဆီစာတစ်စောင် email ပို့မယ်ဆိုပါဆို့။ အဲဒီစာက သေးသေးကြီးကြီး အင်တာနက်ပေါ်မှ အစိတ်အပိုင်းတစ်ခုလုံး ပို့ဖို့တော့ အလွန်ကြီးနေတာကြောင့် TCP က **segments** တွေအဖြစ်စိတ်ပိုင်းလိုက်ပြီး အပိုင်းသေးလေးတွေကို ၎င်းတို့ရဲ့ အဆုံးပိုင်းမှ ာ error-checking code လေးတစ်ခုနှင့်အတူ အစဉ်လိုက်နံပါတ်တွေတပ်လိုက်ပါတယ်။ အကယ်၍ packet တစ်ခုက ရွှေ့ပြောင်းနေချိန်အတွင်း ပျက်စီးမှုဖြစ်တယ်ဆိုရင်၊ TCP ကပြန်ပို့ပေးဖို့ တောင်းဆိုမှာပါ။ လက်ခံရရှိခြင်းအဆုံးမှ ာ TCPက အဲဒီ အစိတ်ပိုင်းလေးတွေကို မူလအတိုင်းမှန်ကန်စွာပြန်စီပြီးနောက် ခင်ဗျားအမေက သူမရဲ့ email ထဲမှာအဲဒီစာကို လက်ခံရရှိမှာပါ။

ဒါပေမယ့် TCP တစ်ခုတည်း မြို့ထဲက ကစားပွဲမဟုတ်ဘူးဆိုတာ မမေ့ပါနဲ့၊ **UDP** ကလည်း ဒီအလွှာရဲ့ လုပ်ငန်းဖြစ်ပြီး အထူးသဖြင့် ၎င်းက session များမဖွဲ့စည်းပါဘူး။ ၎င်းက **datagrams** များစီးဆင်းမှုတစ်ခုကို ထုတ်လွှတ်လိုက်ပါတယ်။ ထိုအချက် က segments များနှင့်ဆင်တူပေမယ့် UDP က မည်သည့်အခါမှ ခင်ဗျားလက်ခံရရှိရဲ့လားလို့ ပြန်မစစ်ပါဘူး။

TCP ဖြစ်ဖြစ်၊ UDP ဖြစ်ဖြစ် trafficအားလုံးကို transport အလွှာမှာ တိကျသော **Port နံပါတ်** များဖြင့် သတ်မှတ်ပါတယ်။

Internetwork

ဤအလွှာကတော့ ပေးပို့သူ နှင့် လက်ခံရရှိသူတို့ရဲ့ လိပ်စာတွေ နှင့် **packet** တွေက ဘယ်မှာစပြီး၊ ဘယ်မှာဆုံးတယ် ဆိုတဲ့ အချက်အလက်တွေကို ပေါင်းထည့်ပေးပါတယ်။ ၎င်းက package တွေကို မှန်ကန်တဲ့လိပ်စာထံပို့ပေးရတဲ့ ပစသာစည်းပို့ကုမသာပဏီန ဲ့ တူပါတယ်။ ၎င်းက Transport အလွှာရဲ့လုပ်ငန်းဖြစ် တဲ့ packet အားလုံးရောက်သွားလား၊ မပျက်မစီးပဲရှိရဲ့လား စတဲ့အချက် တွေကိုတော့ မလုပ်ဆောင်ပါဘူး။ ဤအဆင့်ရဲ့ အဓိက protocol ကတော့၊ **IP (Internet Protocol)** ပဲဖြစ်ပါတယ်။ ပြီးတော့ ဒီအလွှာက packet တွေအကောင်းဆုံးလမ်းကြောင်းကနေ မှန်ကန်တဲ့နေရာကိုရောက်ရှိဖို့ IP addresses များကို အဓိကအသုံးပြုတဲ့အလွှာဖြစ်ပါတယ်။

Network Access

ဤအလွှာကတော့၊ အင်တာနက်ကိုချိတ်ဆက်တဲ့အခါအသုံးပြုတဲ့ အခြေခံရုပ်ပိုင်းဆိုင်ရာကွန်ယက်ဖြစ်ပါတယ်။ အကယ်၍ ခင်ဗျားက dial up အသုံးပြုနေတယ်ဆိုရင်၊ ဖမ်းနည်းပါတယ်၊ ခင်ဗျားသုံးနေတာ ရိုးရှင်းတဲ့ **PPP** ချိတ်ဆက်မှုပဲဖြစ်ပါတယ်။ အကယ်၍ ခင်ဗျားမှာ **DSL** ရှိရင်၊ ခင်ဗျားသုံးနေတာ **ATM** (သို့) **Metro Ethernet** ဖြစ်နိုင်ပါတယ်။ ပြီးတော့ ခင်ဗျားမှ ာ cable internet ရှိရင်၊ ခင်ဗျားသုံးနေတ ာ **DOCSIS** ရုပ်ပိုင်းဆိုင်ရာကွန်ယက်တစ်ခုပါ။ TCP/IP က အားလုံးကိုအတူတကွ ချိတ်ဆက်ပေးနိုင်တာကြောင့်၊ ခင်ဗျား ဘာအမျိုးအစားသုံးနေတယ်ဆိုတာ အရေးမကြီးပါဘူး။ ဤ network access အလွှာမှာ Ethernet ကြိုးတွေနဲ့

network interface card (NIC) များ၊ ကြိုးမဲ့ကွန်ယက်ကဒ်များ နှင့် access point များပါဝင်ပါ တယ်။ ၎င်းက အမှတ်တစ်ခုကနေ နောက်တစ်ခုသို့ ချိတ်ဆက်သွားလာနေသည့်အလျောက် အနိမ့်ဆုံးအရာတွေနှင့် သုည (bits)တွေကို ကိုင်တွယ်ထိန်းချုပ်ထားပါတယ်။

Feed Your Head: "OSI အမျိုးအစား" ကိုသိမြင်ခြင်း

ကွန်ယက်အမျိုးအစားများအပေါ်မှာ ရွေးချယ်ခြင်းတစ်ခုအတွက် ဤ သင်ခန်းစာအဆုံးမှာ "**OSI အမျိုးအစား**" များကို တွေ့နိုင်ပါတယ်။

Protocols

ကဲအခုတော့၊ ခင်ဗျားအင်တာနက်ကိုချိတ်ဆက်ပြီးပါပြီ။ ကြည့်ရတာတော့ရိုးရှင်းပါတယ်၊ ဒါပေမယ့် ခင်ဗျားရောက်နေတဲ့ပုံမှန် အခြေအနေကို ထည့်စဉ်းစားကြည့်ရင် - ခင်ဗျား ညီအကို၊မောင်နှမတွေက အင်တာနက်ပေါ်က ရုပ်ရှင်တွေကြည့်ပြီးအချိန်ဖြုန်း နေကြတဲ့အချိန် မှာ ခင်ဗျားက အင်တာနက်ပေါ်က အနာသတရာယ်မရှိသော၊အရေးကြီးသော လေ့လာစူးစမ်းမှုတွေကို ဦးဆောင်နေပါ တယ်။ ဘာကြောင့် အဲဒီအင်တာနက်စီးဆင်းမှုနှစ်ခုက မရောနှောသွားတာလဲ? ကွန်ယက်က ၎င်းတို့ကွဲပြားတယ်ဆိုတာ မည်သို့ ပြောသလဲ?

အဖြေကတော့ မတူညီတဲ့လမ်းကြောင်းတွေဆက်သွယ်ဖို့ အသုံးပြုတဲ့ဘာသာစကားတစ်ခုဖြစ် တဲ့ **protocols** များဖြစ်ပါတယ်။ web traffic တွေက file တွေ email တွေ အခြားနေရာတွေဆီပြောင်းရွှေ့ပေးနိုင်တဲ့ protocol တစ်ခုကိုသုံးပါတယ်။ အားလုံးက digital ဖြစ်နေသကဲ့သို့ပဲ **protocols** တွေက ကွန်ယက်အဆင့်မှာ နာမည်တွေအသုံးမပြုပဲ၊ IP address နှင့် **port နံပါတ်များ**များသာ အသုံးပြုပါတယ်။

Application layer protocols

FTP (သို့) **File Transfer Protocol** ကို device နှစ်ခုကြားမှာ ဖိုင်များရွှေ့ပြောင်းပို့ဆောင်ရန်အသုံးပြုပါတယ်။ ၎င်းက port တစ်ခုကို အချက်အလက်တွေပို့ဆောင်ရန်သုံးပြီး၊ အခြ ာ ား port တစ်ခုကို ထုတ်လွှင့်ချက်ထိန်းချုပ်မှုတွေပို့ရန် အသုံးပြုပါ တယ်။ ("ကျေးဇူးပါ၊ကျွန်တော် ဒီfile ကိုရပါတယ်")။ အခြေခံအသုံးများတဲ့ port တွေကတော့ 20 နှင့် 21 (TCP) port တွေပဲဖြစ်ပါတယ်။

HTTP (သို့) **Hyper-Text Protocol** ကို web page များအတွက် အသုံးပြုပါတယ်။ ဤလမ်းကြောင်းက ပုံမှန်အားဖြင့် TCP port 80 ကိုသုံးပါတယ်။ **HTTPS** ကတော့ လုံခြုံရေးပုံစံဖြစ်ပြီး ၎င်းကကွန်ယက်လမ်းကြောင်းကို ကွယ်ပုက်ထားပေးပါ တယ်။ ပုံမှန် TCP port 443 ကိုသုံးပါတယ်။

SMTP (သို့) Simple Mail Transfer Protocol ကို email ပို့ရန်သုံးပါတယ်။ port နံပါတ်ကတော့ 25 ဖြစ်ပါတယ်။

DNS (သို့) Domain Name Service ကတော့ ISECOM.org ကဲ့သို့ domain တစ်ခုကို 216.92.116.13 ကဲ့သို့ IP address တစ်ခုသို့ ပြောင်းလဲပေးပါတယ်။ ၎င်းက port နံပါတ် 53 (UDP) ကိုအသုံးပြုပါတယ်။

Transport layer protocols

TCP နှင့် **UDP** ကိုတော့ transport အလွှာက အချက်အလက်တွေ ပို့ဆောင်ဖို့ အဓိကအသုံးပြုပါတယ်။

TCP (သို့) **Transmission Control Protocol** ကတော့ ကွန်ယက်တစ်ခုပေါ်က host နှစ်ခုအကြား စိတ်ပိုင်းဆိုင်ရာ ချိတ်ဆက်မှု (**session** တစ်ခု) ဖြစ်ပါတယ်။ ၎င်းက ထိုချိတ်ဆက်မှုကို handshake သုံးမျိုးဖြင့် ဖွဲ့စည်းထားပါတယ်။

1. ကျွန်တော့်ကွန်ပြူတာက ခင်ဗျားကွန်ပြူတာကို ဆက်သွယ်ချင်တဲ့အခါ ၎င်းက **SYN synchronize packet** တစ်ခုပို့လိုက်ပါတယ်။ ထို packet က "စံချိန်မှတ်တမ်းတွေချိန်ကိုက်ရအောင်၊ ဒါမှငါတို့အချိန်မှတ်တမ်းတွေနဲ့အတူ လမ်းကြောင်းတွေဆက်သွယ်နိုင်မယ်" လို့ သာမန်အားဖြင့်ပြောပါတယ်။
2. ခင်ဗျားရဲ့ကွန်ပြူတာက (အကယ်၍ ၎င်းကဆက်သွယ်မှုကိုလက်ခံလိုက်တဲ့အခါ) **SYN/ACK acknowledgment packet** ဖြင့်အကြောင်းပြန်ပါတယ်။
3. ကျွန်တော့်ကွန်ပြူတာက **ACK** packet ဖြင့် သဘောတူညီမှုကိုတံဆိပ်ကပ်လိုက်ပါတယ်။

ဒါပေမယ့် ဒီဆက်သွယ်မှုပုံစံက TCP မှာသာရှိတာပါ။ **UDP (သို့) User Datagram Protocol** ကတော့ ခင်ဗျားဆက်သွယ်မှု ရတယ်၊မရဘူးဆိုတာ ဂရုမစိုက်တဲ့ **transport protocol** တစ်ခုဖြစ်ပါတယ်။ ၎င်းက မီးသတ်ပိုက်လိုပါပဲ၊ ရေစီးကြောင်းကို ရတယ်၊ မရဘူး ဆိုတာပဲရှိပါတယ်။ ထိုအချက် ကို **UDP** ကိုအလွန်လျင်မြန်စေပါတယ်၊ ဒါကြောင့် **UDP** က အဓိကမကျတဲ့ **frame** တစ်ခုလိုနေတဲ့ ရုပ်ရှင် နှင့် အသံဖိုင်တွေ သို့မဟုတ် **online** ဂိမ်းကစားခြင်း၊ သိပ်အရေးမကြီးတဲ့ **frame** တစ်ခုလိုအပ်နေတဲ့ (ခင်ဗျားရပ်တည်မှုအပေါ်မူတည်ပါတယ်) အချက်အလက်တွေရယူဖို့ လွန်စွာအသုံးဝင်ပါတယ်။

Internet layer protocols

IP (သို့) **Internet Protocol** က အခြေခံ protocol တစ်ခုဖြစ်ပြီး မည်သည့်ကွန်ပြူတာနှစ်လုံးကိုဖြစ်စေ ကွန်ယက်တိုင်းကို ဖြတ်သန်း၍ အချိန်မရွေးနေရာမရွေး ချိတ်ဆက်ပေးနိုင်တဲ့ protocol ဖြစ်ပါတယ်။ ၎င်းက စာပို့ပေးတဲ့ စာပို့လုလင်ကဲ့သို့ packets များကို ၎င်းတို့သွားရမည့်နေရာဆီ အရောက်ပို့ဆောင်ပေးခြင်းကို လုပ်ဆောင်ပါတယ်။

Internet Control and Management Protocol (ICMP)

ICMP ကတော့ ကွန်ယက်ကိုထိန်းသိမ်းစောင့်ရှောက်ရန်နှင့် ပြဿနာသနာဖြေရှင်းပေးရန် ကွန်ယက်သုံးပစ္စည်းများနှင့် ကွန်ယက် အုပ်ချုပ်ရေးမှုးများသုံးတဲ့ protocol ဖြစ်ပါတယ်။ ၎င်းမှာ **ping (Packet InterNet Groper)** ကဲ့သို့ command များနှင့် ကွန်ယက်ကိုစမ်းသပ်ရန်နှင့် အမှားများအစီရင်ခံရန် အလားတူ command များ ပါဝင်ပါတယ်။ ping ကဲ့သို့ command တွေကို host နှင့် network များကိုသိရှိနိုင်ရန် သုံးနိုင်တဲ့အတွက် စနစ်အများစုမှာ **ICMP** ကို တစ်စက္ကန့်လျင် တစ်ကြိမ်သာအကြောင်းပြန်ရန်ကန့်သတ်ထားပါတယ်။

Port နှင့် protocol များကို ပေါင်းချုပ်ရန် အောက်ပါပုံအတိုင်းယှဉ်တွဲကြည့်ပါ။ ။

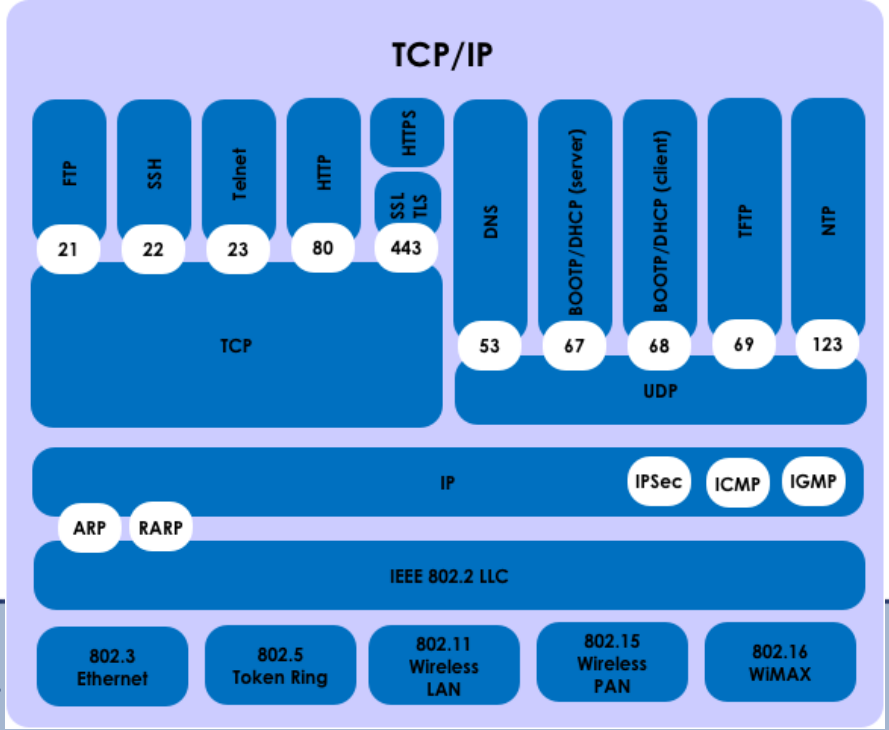


Figure 3.4: The TCP/IP Stack

IPv4 Addresses

ကျွန်တော်တို့က ISECOM.org ကဲ့သို့ နာမည်ကိုသာကောင်းမွန်စွာမှတ်မိနိုင်ကြတာကြောင့် Domain name များကလူသားများ အတွက် အသုံးဝင်ပါတယ်။ ဒါပေမယ့် ကွန်ယက်များကတော့ အဲဒီနာမည်တွေကို နားမလည်ပါဘူး၊ ၎င်းတို့က IP address နံပါတ်များကိုသာနားလည်နိုင်ကြပါတယ်။ ဒါကြောင့်၊ ISECOM.org လို့ခေါ်လိုက်တဲ့အခါ၊ ခင်ဗျားကွန်ပြူတာက သက်ဆိုင်ရာ IP address ကိုရှာဖွေတွေ့ရန်အတွက် DNS (Domain Name Service) ကို အသုံးပြုပြီး လျင်မြန်စွာရှာဖွေပါတယ်။

IP လိပ်စာ များကတော့ လမ်းလိပ်စာများနဲ့တူပါတယ်။ အကယ်၍ ခင်ဗျားက ပေးပို့စာ လက်ခံလိုချင်တဲ့အခါ၊ ခင်ဗျားမှာ လက်ခံ ရယူရန် လိပ်စာတစ်ခုရှိဖို့လိုပါတယ်။ **Ipv4** address မှာ 32 bits ပါဝင်ပြီး၊ ၎င်းကို dot များဖြင့်ခြားထားတဲ့ 8-bit **octets** လေးခုအဖြစ် ခွဲခြမ်းထားပါတယ်။ ထိုအချက်က အင်တာနက်ပေါ်မှာ Ipv4 အရ အထူးလိပ်စာပေါင်း 2^{32} (သို့) (၄,၂၉၄,၉၆၇,၂၉၆) ခုရှိတယ်လို့ ဆိုလိုတာဖြစ်ပါတယ်။ အဲဒီ IP လိပ်စာရဲ့ တစ်ပိုင်းက ကွန်ယက်အတွက် လိပ်စာပေးပြီး ကျန်တစ်ပိုင်းက အဲဒီကွန်ယက်ပေါ်က ကွန်ပြူတာတစ်ခုချင်းစီကိုလိပ်စာပေးပါတယ်။ အဲဒီအစိတ်အပိုင်းတွေကို နိုင်ငံ၊မြို့ (ကွန်ယက်) အပိုင်း လိပ်စာ နှင့် လမ်း (host) အပိုင်း လိပ်စာ များအဖြစ် မြင်ကြည့်ပါ။

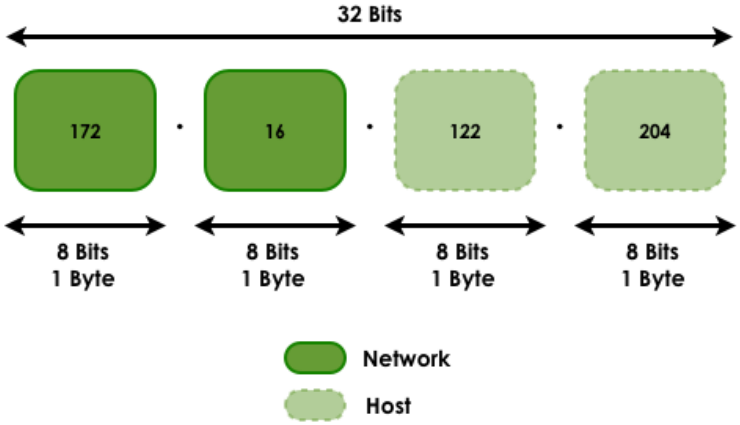


Figure 3.5: ကွန်ယက်နံပါတ်များနှင့် host ID များ

စာပို့ဝန်ဆောင်မှု နိုင်းယှဉ်ချက်ကို ပြန်ကြည့်ပါ၊ IP က packet တွေကို မှန်ကန်တဲ့စာပို့ရုံးဆီပို့ဆောင်ပေးတဲ့ သယ်ယူပို့ဆောင်ရေးယာဉ်တစ်စီးဖြစ်ပါတယ်။ TCP ကတော့ အပြင်မှရစ်ပတ်ထားတဲ့ ကုန်ပစ္စည်းပို့ဆောင်မှုတစ်ခုမှာပါဝင်တဲ့ အထုပ်စာရင်း ဖြစ်ပြီး (အထုပ်ပေါင်း ၆၅ထုပ် မှ နံပါတ် ၃အထုပ် လို့၊ ပြောတဲ့) ဘယ်တစ်ခုဖြစ်တယ်ဆိုတာလဲဖေါ်ပြပေးပါတယ်။ host-level လိပ်စာများကတော့ အဲဒီ packet က တိတိကျကျ ဦးတည်နေတဲ့ အိမ် (ကွန်ပြူတာ) ဖြစ်ပါတယ်။

> Public နှင့် **private (routable မလုပ်နိုင်တဲ့) IP address** ဟူ၍နှစ်ခုရှိပါတယ်။ Private IP address တွေကို private ကွန်ယက်များမှာ အသုံးပြုပြီး router များက အဲဒီ address များကို အင်တာနက်သို့တက်ရန် ခွင့်မပြုပါဘူး။

Private ကွန်ယက်များအတွင်းမှ IP address များက အဲဒီကွန်ယက်အတွင်းမှာ ပုံတူမဖြစ်သင့်ပါဘူး။ ဒါပေမယ့် ကွဲပြားခြားနားတဲ့၊ မချိတ်ဆက်ထားတဲ့ private ကွန်ယက်များမှာတော့ တူညီတဲ့ Ip address များထားနိုင်ပါတယ်။ IANA (Internet Assigned Numbers Authority) မှ private ကွန်ယက်များ (RFC 1918 လို့သိနိုင်ပါတယ်) အတွက်သုံးနိုင်ရန် သတ်မှတ်ပေးထားတဲ့ IP address များကတော့ -

10.0.0.0 through 10.255.255.255 (Class A)
172.16.0.0 through 172.31.255.255 (Class B)
192.168.0.0. through 192.168.255.255(Class C) တို့ဖြစ်ပါတယ်။

Classes - အတန်းများ

IP address များရဲ့ ဘယ်အပိုင်းကို့ ကွန်ယက်တွေကို လိပ်စာပေးဖို့သုံးမှာလဲ၊ ဘယ်အပိုင်းက ကွန်ပြူတာတစ်လုံးချင်းစီကို လိပ်စာပေးမှာလဲ ဆိုတာပေါ်အခြေခံ၍ class များခွဲခြားထားပါတယ်။

အပိုင်းတစ်ခုချင်းစီကို ချမှတ်ပေးထားသောအရွယ်အစားပေါ်မူတည်၍၊ အဲဒီကွန်ယက်အတွင်းမှာ ကွန်ယက်သုံးစက်ပစ္စည်းပိုမို သုံးနိုင်ခြင်း (သို့) ကွန်ယက်တွေပိုမိုချမှတ်နိုင်ခြင်းများ ရှိမှာပါ။

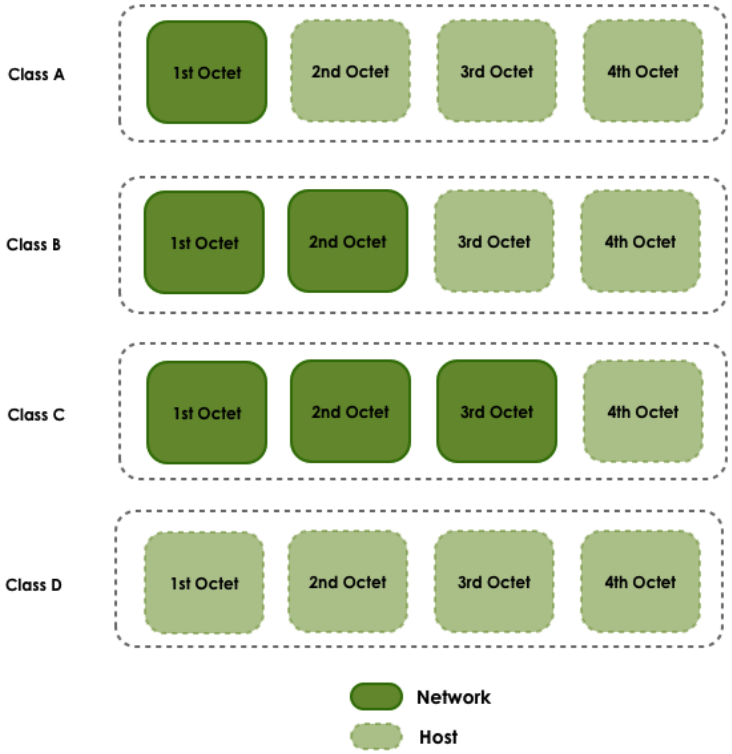


Figure 3.5: IP Class Divisions

Class A: ပထမဆုံး bit ကအမြဲ သုည်ဖြစ်သောကြောင့်၊ ဒီ class မှာ 0.0.0.0 (အစဉ်အလာအားဖြင့်၊ မည်သည့်အခါမှ အသုံးမပြုပါဘူး) နှင့် 126.255.255.255 အတွင်းရှိလိပ်စာများ ပါဝင်ပါတယ်။ မှတ်ချက်။ ။ 127.x.x.x လိပ်စာတွေကတော့ loopbak (သို့) localhost ဝန်ဆောင်မှုသုံးရန် သီးသန့်ဖယ်ထားပြီးသား (reserve)လိပ်စာတွေဖြစ်ပါတယ်။

Class B: ပထမဆုံး octet ရဲ့ ပထမဆုံး bit နှစ်ခုက တစ်၊သုံည "10" ဖြစ်သောကြောင့် ဒီ class မှာ 128.0.0.0 နှင့် 191.255.255.255 အတွင်းရှိလိပ်စာများ ပါဝင်ပါတယ်။

Class C: ပထမဆုံး octet ရဲ့ ပထမဆုံး bit သုံးခုက တစ်၊တစ်၊သုံည "110" ဖြစ်သောကြောင့် ဒီ class မှာ 192.0.0.0 နှင့် 223.255.255.255 အတွင်းရှိလိပ်စာများ ပါဝင်ပါတယ်။

Class D: ပထမဆုံး octet ရဲ့ ပထမဆုံး bit လေးခုက တစ်၊တစ်၊တစ်၊သုံးည "1110" ဖြစ်သောကြောင့် 224.0.0.0 နှင့် 239.255.255.255 အတွင်းရှိလိပ်စာများ ပါဝင်ပြီး group multicast သုံးရန်အတွက် သီးသန့်ထားသော လိပ်စာများဖြစ်သည်။

ကျန်တဲ့လိပ်စာများအားလုံးကို စမ်းသပ်ခြင်းများ (သို့) အလားအလာရှိသောကြိုတင်ခွဲဝေပေးခြင်းများအတွက် အသုံးပြုပါ တယ်။

Mask (သို့ netmask) ကို ဤ class တွေကို အုပ်စုခွဲရန် အသုံးပြုပါတယ်။ binary တွေမှာ၊ "1" bit တစ်ခုက ကွန်ယက်ပါဝင် မှု ပါဝင်တဲ့အပိုင်းကို ဖော်ပြပြီး "0" bit တစ်ခုက host တစ်ခုခြင်းစီပါဝင်တဲ့အပိုင်းကို ကိုယ်စားပြုဖော်ပြပါတယ်။ ပထမဆုံး class သုံးခုအတွက် အခြေခံ netmasks များကတော့ -

255.0.0.0 (Class A)
255.255.0.0 (Class B)
255.255.255.0(Class C)

အခြေခံ classes များကိုအသုံးပြုထားတဲ့ ကွန်ယက်များမှာ Class A ဖြစ်ရင် octet တစ်ခု၊ Class B ဖြစ်ရင် octet နှစ်ခု၊ Class C ဖြစ်ရင် octet သုံးခု စသည်ဖြင့် အသီးသီး mask လုပ်ထားသောကြောင့်၊ တကယ့်ကို မှတ်မိလွယ်ပါတယ်။ အခြေခံ classes များကိုအသုံးပြုခြင်းက အသုံးဝင်ပါတယ် ဒါပေမယ့် လူတိုင်းမသုံးကြပါဘူး။

Host တစ်ခုကို တိတိကျကျသိဖို့ ခွဲခြားကြည့်ရန်၊ ၎င်း၏IP address နှင့် network mask နှစ်ခုစလုံးသိရန်လိုအပ်ပါတယ်။

IP: 172.16.1.20
Mask: 255.255.255.0

Loopback Addresses

127.0.0.1 မှ 127.255.255.254 အထိ IP address များကို၊ မိမိကွန်ပြူတာကို တိုက်ရိုက်ပြန်ညွှန်းတဲ့၊ **loopback** (သို့) localhost address များအတွက် သီးသန့်ယူထားပြီးဖြစ်ပါတယ်။ ကွန်ပြူတာတိုင်းမှာ localhost address 127.0.0.1 ရှိပြီးဖြစ် ပါတယ်၊ ထို့ကြောင့် ၎င်း address ကိုအခြားစက်ပစ္စည်းတွေမှာ အသုံးပြုလို့မရနိုင်ပါဘူး။

အခြားအသုံးပြုလို့မရနိုင်တဲ့ address များလည်းရှိပါတယ်။ ၎င်းတို့က **network address** နှင့် **broadcast address** များဖြစ်ပါတယ်။

ကွန်ယက်လိပ်စာများ - Network Addresses

Network address ဆိုတာ အခြေခံအားဖြင့် IP address တစ်ခုရဲ့ ကွန်ယက်အပိုင်းပဲဖြစ်ပြီး **host အပိုင်းက သုည များ ဖြစ်ပါတယ်။** ၎င်း သုညက host တစ်လုံးသာမက၊ကွန်ယက်တစ်ခုလုံးကို သတ်မှတ်ပေးတဲ့အတွက် ၎င်း address ကို host တစ်လုံးလုံး အတွက်ပေးလို့မရပါဘူး။

IP: 172.16.1.**0**
Mask: 255.255.255.0

ထုတ်လွှင့်မှု လိပ်စာများ - Broadcast Addresses

Broadcast address ဆိုတာ အခြေခံအားဖြင့် IP address တစ်ခု၏ကွန်ယက်အပိုင်းဖြစ်ပြီး၊ **host အပိုင်းက တစ်များ ဖြစ်ပါတယ်။** ၎င်း address ကို host တွေအားလုံးက နားထောင် (listen) ကြသဖြင့် – (ဒါက broadcast ရဲ့ဆိုလိုရင်းပါပဲ - လူတိုင်း နားထောင်ကြပါတယ်) ၊ ၎င်းကို host တစ်လုံးတည်းအတွက်သတ်မှတ်၍ အသုံးပြုလို့မရပါဘူး။

IP: 172.16.1.**255**
Mask: 255.255.255.0

Ports

TCP နှင့် UDP နှစ်ခုစလုံးက application များဖြင့် အချက်အလက်တွေဖလှယ်ရန် **ports များ**ကို သုံးကြပါတယ်။ port တစ်ခုဆိုတာ လမ်းလိပ်စာတစ်ခုမှာ အခန်း(သို့)၊ အခန်းတွေ တစ်ခုရဲ့လိပ်စာပေါင်းထည့်သက့ဲသို့၊ address တစ်ခု၏ တိုးချဲ့ခြင်း တစ်ခုဖြစ်ပါတယ်။ လမ်းတစ်ခု၏လိပ်စာပါတဲ့ စာတစ်စောင်က မှန်ကန်တဲ့အဆောက်အဦးဆီရောက်နိုင်ပေမယ့်၊ အခန်းနံပါတ် မပါပဲ ထိုစာက မှန်ကန်တဲ့လက်ခံသူထံရောက်နိုင်မှာမဟုတ်ပါဘူး။

Ports များက ထိုနည်းတူစွာ လုပ်ဆောင်ပါတယ်။ အထုပ်ငယ် (packet) တစ်ခုကို မှန်ကန်တဲ့ IP address တစ်ခုထံပို့ဆောင် နိုင်ပေမယ့်၊ သက်ဆိုင် ရာ port မပါပဲ၊ ၎င်း packet ကို မည်သည့် application က လက်ခံမည်ကို သတ်မှတ်နိုင်ရန် နည်းလမ်း မရှိပါဘူး။ Port နံပါတ်တစ်ခုကလည်း 16 bit နံပါတ်တစ်ခု ဖြစ်ပါတယ်၊ ၎င်းမှာ ဆယ်လီစိတ်ကိန်းတန်ဖိုး ၀ မှ ၆၅၅၃၅ (၂ထပ်ညှဉ်း ၁၆) ပါရှိပါတယ်။

> နောက်တစ်နည်းတွေးကြည့်ရင် - ကွန်ပြူတာတိုင်းက စာပို့ရုံးဖြစ်ပါတယ်။ application တိုင်းမှာ ၎င်းတို့ကိုယ်ပိုင် စာတိုက်ပုံး ကိုယ်စီရှိကြပြီး၊ application နှစ်ခုက တူညီတဲ့စာတိုက်ပုံးတစ်ခုတည်းကို မျှဝေသုံးသင့်ပါဘူး။ port နံပါတ် ကတော့ စာတိုက်ပုံး နံပါတ်ပဲဖြစ်ပါတယ်။

Port နံပါတ်တွေက များစွာသောအချက်အလက်တွေကို သက်ဆိုင်သော application ထံဆက်သွယ်တဲ့အခါ ၎င်းဆက်သွယ်မှု တွေကို IP address တစ်ခုတည်းဆီ ချိတ်ဆက်နိုင်ရန် ဆောင်ရွက်ပေးပါတယ်။ အဲဒီ port နံပါတ်က၊ အမျိုးမျိုးသော client များဖြင့် တပြိုင်နက် ဆက်သွယ်ချိတ်ဆက်မှုတွေလုပ်ဆောင်နေချိန်မှာ၊ local client က တောင်းဆိုနေတာ မည်သည့် အချက် အလက် အမျိုးအစားဖြစ်တယ် ဆိုတာကို remote computer တစ်ခုပေါ်မှာအလုပ်လုပ်နေတဲ့ ပန်ဆောင်မှုအား သတင်းပို့ ပါတယ်။

ဥပမာ - local computer တစ်လုံးက web server port 80 နှင့် IP address 62.80.122.203 ဖြစ်တဲ့ www.osstmm.org website ကို ချိတ်ဆက်ရန် ကြိုးစားတဲ့အခါ၊ ၎င်း local computer က remote computer ကို ချိတ်ဆက်ရန်အသုံးပြုတဲ့ **socket address** က ။ ။

62.80.122.203:80

အခြေခံအသုံးများသော port များအကြားတွင် စံချိန်ကိုက်ခြင်းအဆင့်ကို ထိန်းသိမ်းရန်ရည်ရွယ်၍၊ IANA က ၀ မှ ၁၀၂၄ အထိ port နံပါတ်များအား အခြေခံ၊ **အထူးပြုသော** (သို့) **ထင်ရှားသော ပန်ဆောင်မှုများ** အတွက်အသုံးပြုရန် သတ်မှတ်ခဲ့ပါ တယ်။ ကျန်ရှိတဲ့ ၆၅၅၃၅အထိ port များကိုတော့ အထူးပန်ဆောင်မှုများ (သို့) dynamic allocations များအတွက်အသုံးပြု ပါတယ်။

IANA မှ ချမှတ်ထားသော - အခြေခံအသုံးများသော port များ (လူသိများသော) port များကို အောက်ပါအတိုင်း စာရင်းပြုထားပါတယ် -

Port Assignments		
Number	**Keywords**	**Description**
၅	rje	Remote Job Entry
၀		Reserved
1-4		Unassigned
၇	echo	Echo
၉	discard	Discard
၁၁	systat	Active Users
၁၃	daytime	Daytime
15	netstat	Who is Up or NETSTAT
၁၇	qotd	Quote of the Day
၁၉	chargen	Character Generator
၂၀	ftp-data	File Transfer [Default Data]
၂၁	ftp	File Transfer [Control]
၂၂	ssh	SSH Remote Login Protocol
၂၃	telnet	Telnet
၂၅	smtp	Simple Mail Transfer
၃၇	time	Time
၃၉	rlp	Resource Location Protocol
၄၂	nameserver	Host Name Server
၄၃	nicname	Who Is
၅၃	domain	Domain Name Server
၆၇	bootps	Bootstrap Protocol Server / DHCP Server
၆၈	bootpc	Bootstrap Protocol Client / DHCP Client
၆၉	tftp	Trivial File Transfer
၇၀	gopher	Gopher
၇၅		any private dial out service
၇၇		any private RJE service
၇၉	finger	Finger
၈၀	www-http	World Wide Web HTTP
၉၅	supdup	SUPDUP

Port Assignments		
၁၀၁	hostname	NIC Host Name Server
၁၀၂	iso-tsap	ISO-TSAP Class 0
၁၁၀	pop3	Post Office Protocol - Version 3
၁၁၃	auth	Authentication Service
၁၁၇	uucp-path	UUCP Path Service
၁၁၉	nntp	Network News Transfer Protocol
၁၂၃	ntp	Network Time Protocol
၁၃၇	netbios-ns	NETBIOS Name Service
၁၃၈	netbios-dgm	NETBIOS Datagram Service
၁၃၉	netbios-ssn	NETBIOS Session Service
140-159		Unassigned
160-223		Reserved

ဖွဲ့စည်းထုပ်ပိုးခြင်း - Encapsulation

အချက်အလက်အစိတ်အပိုင်းတစ် ခု - ဥပမာ - e-mail သတင်းတစ်ခုကို ကွန်ပြူတာတစ်ခုကနေ၊ အခြားတစ်ခုဆီသို့ ပို့ဆောင် တဲ့အခါ ၎င်းက ပြောင်းလဲမှုဖြစ်စဉ် တစ်ခုဖြစ်သွားပါတယ်။ Transport အလွှာကို ပို့မည့် အချက်အလက်ကို Application အလွှာက ထုတ်လုပ်ပါတယ်။

Transport အလွှာက ထိုအချက်အလက်ကို ရယူပြီး အစိတ်အပိုင်းများပိုင်း၍ port များ၊ အစိတ်အပိုင်းများ၏ အမှတ်စဉ် နံပါတ်များနှင့် အခြားကဏ္ဍသုခများပါဝင်သော ခေါင်းစည်း (header) တစ်ခုပေါင်းထည့်လိုက်ပါတယ်။

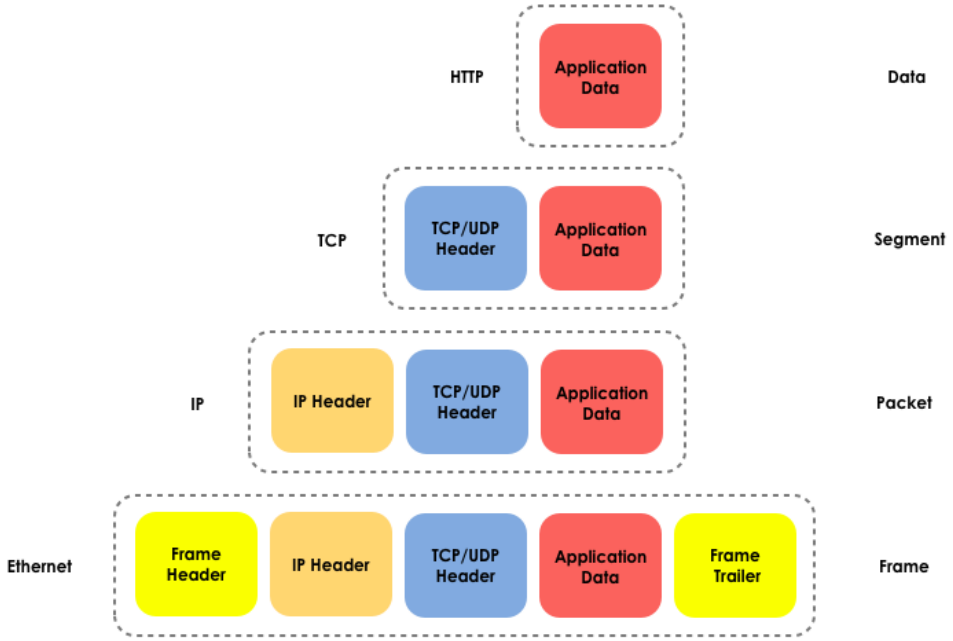


Figure 3.6: Encapsulation

ထိုနောက် ၎င်းအစိတ်အပိုင်းများကို ပေးပို့သူ နှင့် လက်ခံသူ IP address နှင့် ပို၍များပြားသော အချက်အလက်အပိုင်းများ ပါဝင်တဲ့ ခေါင်းစည်းတစ်ခု ထပ်ဖြည့်ပေးမည့် Network အလွှာဆီပေးပို့လိုက်ပါတယ်။

local network များစွာကို Ethernet ဖြင့်ထောက်ပံ့ပေးသော နောက်အလွှာတစ်ခုက နောက်ထပ်ခေါင်းစည်း ထပ်၍ပေါင်းထည့် ခြင်း စသည်ဖြင့်ပြုလုပ်ပါတယ်။ ထိုကဲ့သို့ လုပ်ငန်းစဉ်ကို **ဖွဲ့စည်းထုပ်ပိုးခြင်း - encapsulation** လို့ခေါ်ပါတယ်။

ပထမဆုံးထုပ်ပိုးမှုပြီးနောက်၊ အလွှာတစ်ခုချင်းစီက ပြီးခဲ့တဲ့အလွှာရဲ့အချက်အလက် ဖွဲ့စည်းထုပ်ပိုးမှုအား နောက်ဆုံးအလွှာ ရောက်တဲ့အထိ အဆင့်ဆင့်ဆက်လက်လုပ်ဆောင်ပါတယ်၊ ထိုသို့ လုပ်ဆောင်ခြင်းအတွင်းမှာပဲ အမှန်တကယ်အချက်အလက် ပေးပို့မှု ဖြစ်ပေါ်ပါတယ်။ ထို့ကြောင့် ဖွဲ့စည်းထုပ်ပိုးမှု - encapsulation ကို အောက်ပါအတိုင်းတွေ့မြင်နိုင်ပါတယ်။ ။

ဖွဲ့စည်းထုပ်ပိုးထားသောအချက်အလက်တွေ ဦးတည်ရာသို့ရောက်သွားတဲ့အခါ၊ ၎င်းတို့ကို (de-encapsulation) ပြန်လည် ဖြည်ချပါတယ်။ အလွှာတစ်ခုချင်းစီက အချက်အလက်တွေကို အလွှာနောက်တစ်ခုဆီပို့ဆောင်ပြီး ဆင့်စီထားတဲ့အတိုင်း၊ အောက်ဆုံးအလွှာမှာထည့်ထားတဲ့ခေါင်းစည်းမှာပါဝင်တဲ့အချက်အလက်တွေကို ဖယ်ရှားလိုက်ပါတယ်။ဤနောက်နဲတဲ့ addressing စနစ်မှာပါဝင်တဲ့ အချက်အလက်ရဲ့ နောက်ဆုံး bit ကတော့ ကွန်ပြူတာ NIC ရဲ့ unique address ပဲဖြစ်ပါတယ်။ ၎င်းကို **The Media Access Controller (MAC) address** လို့ခေါ်ပါတယ်။ ဤ address ကို ပုံမှန် အားဖြင့် ခြောက်၊ နှစ် အကဿခရာ၊ ဆယ့်ခြောက်လီစိတ်နံပါတ်များအား ကော်လံ (သို့) ဟိုင်ဖိုင် များဖြင့် ခွဲခြားဖော်ပြထားပါတယ်။ ၎င်းက network card ရဲ့ physical address ဖြစ်ပြီး မပြောင်းလဲနိုင်ပါဘူး (အမှန်တကယ်တော့၊ ၎င်းကိုပြောင်းနိုင်တဲ့နည်းလမ်း များရှိပါတယ် ဒါပေမယ့် တိတိကျကျကိုတော့ ခင်ဗျားကိုယ်တိုင်ရှာကြည့်ပါ)။ MAC address တစ်ခုက ဤကဲ့သို့ ဖြစ်ပါတယ် -

00-15-00-06-E6-BF

Exercises

3.1. သင်ခန်းစာ ၁ နှင့် ၂ မှာလေ့လာခဲ့တဲ့ command များကိုသုံးပြီး IP address၊ netmask၊ DNS၊ hostname နှင့် MAC address များရှာကြည့်ပါ။ ၎င်းတို့ကို ခင်ဗျားတွဲဖက် ရဲ့ ရလဒ်တွေနဲ့ နှိုင်းယှဉ်ကြည့်ပါ။ မည်သည့်အရာတွေက တူညီပြီး၊ မည်သည့်အရာတွေကွဲပြားနေပါသလဲ? အဲဒီNetwork အသုံးပြုနေတဲ့ IP address စနစ်ကို ကြည့်ပါ၊ ၎င်းက private (သို့) public network လား?

3.2. netstat

netstat command က – မည်သူနဲ့ချိတ်ဆက်နေတယ်၊ ချိတ်ဆက်နေတာမည်မျှကြာနေပြီလဲ၊ စသည်ဖြင့် ခင်ဗျား network စာရင်းကိုဖော်ပြပါလိမ့်မယ်။ Linux၊ Windows (သို့) OSX ရဲ့ command line interface မှာ

netstat လို့ ရိုက်လိုက်ပါ

CLI window မှာ၊ အခြေခိုင်နေသော ချိတ်ဆက် မှု (established connections) စာရင်းများကို တွေ့ပါလိမ့်မယ်။ အကယ်၍ နံပါတ်ပုံစံဖြင့် ရချင်တယ် ဆိုရင်တော့

netstat -n လို့ ရိုက်လိုက်ပါ။

ချိတ်ဆက်မှုတွေနှင့် active ဖြစ်နေတဲ့ (listening, ပွင့်နေသော) port များကို မြင်နိုင်ရန်

netstat -an လိုရိုက်ပါ။

အခြား ရွေးချယ်မှုများကြည့်ရန်

netstat -h လိုရိုက်ပါ။

netstat ရလဒ်မှာ ၊ local နှင့် remote IP address များနှင့် ၎င်းတို့ အသုံးပြုနေတဲ့ port များ စာရင်းပါတဲ့ ကော်လံများကို ရှာပါ။

```
Proto Recv-Q Send-Q  Local Address        Foreign Address     (state)
tcp4     0      0  192.168.2.136.1043  66.220.149.94.443   ESTABLISHED
```

port များကို ပုံမှန် IP address များနောက်မှာဖော်ပြပြီး၊ ၎င်းတို့ကို dot (သို့) ကော်လံဖြင့်ခွဲခြားဖော်ပြထားပါတယ်။ remote address သုံးတဲ့ port တွေက ဘာကြောင့်၊ local address သုံးတဲ့ port တွေနဲ့ မတူညီပါသလဲ?

Browser windows၊ tabs နှစ်ခုသုံးခုလောက်ဖွင့်ထား၍ website အမျိုးမျိုးခေါ်ထားပြီ း netstat ကိုထပ်ရိုက်ကြည့်ပါ။

အကယ်၍ tab အချို့ဖွင့်ထားတဲ့အခါ browser က မည်သို့သိနိုင်သလဲ၊ မည်သည့် အချက်အလက်တွေက မည်သည့် tab သို့ သွားပါသလဲ ?

Browser ကို အသုံးပြုထားတဲ့အခါ၊ ဘာကြောင့် listening port ကို မသတ်မှတ်ထားတာလဲ?

မည်သည့် protocols တွေကို သုံးတာလဲ?

တစ်ခုထက် ပိုတဲ့ ကိစ္စသစတွေအတွက် protocol တစ်ခုထဲကိုသုံးတဲ့အခါ ဘာဖြစ်သလဲ?

3.3. ကျွန်တော့်ရဲ့ ပထမဆုံး ဆာဗာ

ဤလေ့ကျင့်ခန်းကိုပြုလုပ်ရန်၊ ခင်ဗျားမှာ **netcat (nc)** program ရှိဖို့လိုအပ်ပါတယ်။ ၎င်း program က BackTrack နှင့် OSX မှာ အခြေခံအားဖြင့် ပါဝင်ပါတယ်။ ဒါပေမယ့်လည်း OS အားလုံးအတွက် nc installer ကို ဒေါင်းလုတ် လုပ်နိုင်ပါတယ်။

1. CLI မှာ

`nc -h` လို့ရိုက်ပါ။

netcat မှာပါတဲ့ ရွေးချယ်နိုင်မှုတွေကို ဖော်ပြပါလိမ့်မယ်။

ရိုးရှင်းတဲ့ server တစ်ခု ဖန်တီးရန် ၊ Linux ဖြစ်ဖြစ်၊ Windows ဖြစ်ဖြစ်

`nc -l -p 1234` လို့ရိုက်ပါ။

OSX မှာတော့

`nc -l 1234` လို့ရိုက်ပါ။

ခင်ဗျားက port 1234 ကို listening လုပ်ရန် server တစ်ခု စတင်လိုက်ပါပြီ။

2. ဒုတိယ CLI တစ်ခုထပ်ဖွင့်ပြီး

`netstat -a` လို့ရိုက်ပါ။

port 1234 ကို listening လုပ်နေတဲ့ ပန်ဆောင်မှုအသစ်တစ်ခုကို ဖော်ပြပါလိမ့်မယ်။

အဲဒီ server နှင့် အဆက်အသွယ်ရရန် ၊ ခင်ဗျားမှာ Client တစ်လုံးရှိရန်လိုပါတယ် ! ခင်ဗျားရဲ့ ဒုတိယ CLI မှာ

`nc localhost 1234` လို့ရိုက်လိုက်ပါ။

ဤ command က port 1234 ကို listening လုပ်နေတဲ့ server နှင့်ချိတ်ဆက်ပေးပါလိမ့်မယ်။ ယဉ်သခု၊ ဖွင့်ထားတဲ့ CLI နှစ်ခု စလုံးပေါ်မှာ၊ CLI Window တစ်ခုမှာ ရေးသမျှအားလုံးကို နောက် CLI Window တစ်ခုပေါ်မှာလည်း မြင်နိုင်ပါတယ်။

ထိုကဲ့သို့ လုပ်ဆောင်နိုင်ခြင်းကို သွယ်ဝိုက်စွာဆက်စပ်မှုတစ် ခု ရှိသကဲ့သို့ သုံးသပ်ကြည့်ပါ။ တစ်ယောက်ယောက်က ခင်ဗျားစက်ကို exploit လုပ်ရန် ဤစွမ်းအားကို မည်သို့ အလွဲသုံးစားပြုနိုင်ပါသလဲ?

Netcat ကဒင်းရဲ့ traffic အားလုံးကို ရှင်းလင်းစွာ ပို့ဆောင်ပါတယ်။ လုံခြုံစိတ်ချနိုင်တဲ့ အခြားနည်းလမ်းရှိပါသလား?

3. အဲဒီ server ကိုရပ်ဆိုင်းပစ်ရန် ပထမဆုံး CLI ကိုပြန်သွားပြီး Control-C ကိုနှိပ်ပါ။

4. ယဉ်သခု test ဆိုတဲ့ နာမည်နဲ့ "Welcome to my server" ဆိုတဲ့ စာသားပါတဲ့ ရိုးရိုး text file တစ်ခု ဆောက်လိုက်ပါ။

ဆောက်ပြီးတဲ့အခါ၊ အောက် ပါ command ကိုကြည့်ပြီး အပိုင်းတစ်ခုချင်းစီက ဘာလုပ်သလဲ? ဆိုတာ instructor ကို ဘာသာပြန်ပြပါ။ ထို့နောက် CLI window မှာ

`nc -l -p 1234 < test` လို့ရိုက်ပါ။

အခြား CLI တစ်ခုကနေ အဲဒီ server ကို

nc localhost 1234 လို့ရိုက်ပြီး ချိတ်ဆက်ပါ။

client များက အဲဒီ server ကို ချိတ်ဆက်လိုက်တဲ့အခါ၊ test file ရဲ့ ရလဒ်ကို မြင်နိုင်မှာပါ။
အဲဒီ server ကိုဆက်သွယ်ရန် မည်သည့် protocol ကို အသုံးပြုပါသလဲ?

Netcat က ထို protocol ကိုပြောင်းလဲခွင့်ပြုပါသလား ? အကယ်၍ ၊ ပြောင်းလဲနိုင်တယ်ဆိုရင်၊ မည်သို့ပြောင်းလဲပါသလဲ?

Feed Your Head: The OSI Model

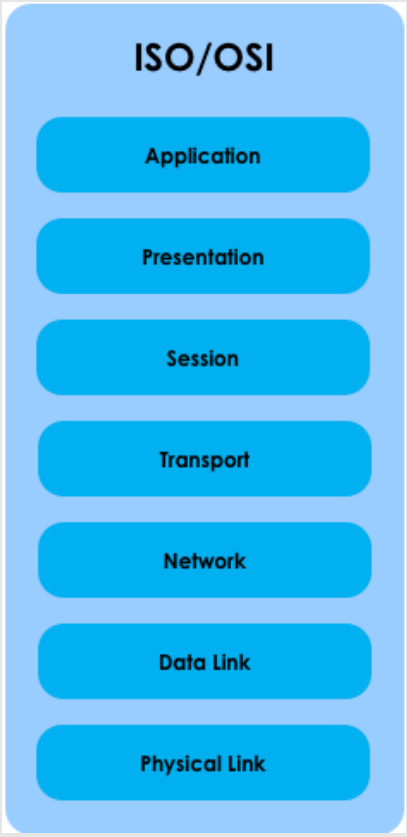


Figure 3.7: The ISO/OSI Model

OSI Model ကို ၁၉၈၀ ခုနှစ်တွင် (TCP/IP Model စတင်ခဲ့ပြီး ၁၀ နှစ်ခန့်အကြာ) **ISO** the International Standards Organization အဖွဲ့အစည်းမှစတင်ခဲ့ပါတယ်။ OSI က **Open System Interconnection** ၏အတိုကောက်ဖြစ်ပြီ း ကွန်ယက်ဖွံ့ဖြိုးရေးအဖွဲ့အစည်းမဟုတ် တဲ့ အဖွဲ့အစည်းတစ်ခုမှစတင်ခဲ့တဲ့ ကွန်ယက်၏သဘောသဘာ၀ နှင့် တည်ဆောက် မှုပုံစံကို စံချိန်ကိုက်ညီပေးရန် ဆောင်ရွက်ပေးပါတယ်။

OSI Model က ရိုးရှင်းသောစည်းမျဉ်းအနည်းငယ်ဖြင့် အဆင့်ဆင့်ထပ်စီထားသော model ဖြစ်ပါတယ်။ တူညီတဲ့ အခြေခံ လုပ်ငန်းများကို အလွှာတစ်ခုတည်းမှာ အုပ်စုဖွဲ့ထားပြီး၊ အလွှာတစ်ခုစီက ၎င်းအလွှာ၏ **အောက်ဘ်ခံ** ရှိသောအလွှာမှ ထောက်ပံ့မှုပေးခြင်းကိုရယူပြီး၊ ၎င်းအလွှာ၏ **အပေါ်ခံ** ရှိသောအလွှာကို ထောက်ပံ့ပေးပါတယ်(ဤအချက်ကိုမမေ့ပါ နှင့်)။

ဤ layer model က (သီအိုရ ီ မှာ) အလွှာတိုင်းမှာ ၎င်းတို့ကိုယ်ပိုင်သက်ဆိုင်ရာဆက်သွယ်မှုတွေပြုလုပ်နေခြင်း၊ အလွှာတစ်ခုတိုင်းမှဖွံ့ဖြိုးမှုအသစ်တွေကအခြားအလွှာတွေကို မဖြတ်တောက်ခြင်းများကြောင့် ကောင်းမွန်တဲ့ရည်ရွယ်ချက် တစ်ခု ပဲ ဖြစ်ပါတယ်။ ဤအဂၤါရပ်ကသာ သကၠသကရာဇ် ၂၀၀၀ ကတည်းကကြုံတွေ့နေရတဲ့၊ နေ့စဉ်နီးပါ း application အသစ်များ နှင့် ၀န်ဆောင်မှုအသစ်များ ပေါ်ထွက်လာခြင်းများနှင့်အတ ူ (internet boom) အင်တာနက်လျင်မြန်စွာ- ကျယ်ပြန့်လာမှုကို ဖြေရှင်းနိုင်ပါလိမ့်မယ်။

ဤ OSI စံနှုန်းမှာ ကျွန်တော်တို့ရှေ့မှာ ဆွေးနွေးခဲ့ကြတဲ့ (တူညီတဲ့အခြေခံလုပ်ငန်းများကို အုပ်စုဖွဲ့ထားခြင်း နှင့် အလွှာတစ်ခုစီကဝင်းအလွှာ၏အောက်ခြံရှိသောအလွှာမှထောက်ပံ့မှုပေးခြင်းကိုရယူပြီး၊ ၎င်းအလွှာ၏အပေါ်ခြံရှိသောအလွှာ ကိုထောက်ပံ့ပေးခြင်း) OSI model ၏ စည်းမျဉ်းနှစ်ခုအပြင်ပိုမိုတင်းကျပ်တဲ့စည်းမျဉ်းများပါရှိပါတယ်။ ကွန်ပြူတာတစ်လုံး မှ အခြားကွန်ပြူတာတစ်လုံးပေါ်ကတူညီတဲ့အလွှာတစ်ခုနှင့် တိုက်ရိုက်ချိတ်ဆက်မှုပြုတဲ့အခါအလွှာတိုင်း ပါ၀င်ပါတယ်။ ဆိုလိုတာက၊ ခင်ဗျား browser မှ ၁ www.google.com လို ခေါ်လိုက်တဲ့အခါ၊ ခင်ဗျားကွန်ပြူတာရဲ့ layer 7 interface အလွှာ (ခင်ဗျားရဲ့ web browser ပါ) နှင့် Google.com ၏ web server (Layer 7 interface အလွှာ တစ်ခုပါပဲ) ကြားမှာ တိုက်ရိုက်တုံ့ပြန် မှု တစ်ခုဖြစ်ပေါ်ပြီး၊ အခြားအလွှာများမှာလဲ ဤကဲ့သို့လုပ်ဆောင်ပါလိမ့်မယ်။

ထို့ကြောင့် ပထမဦးစွာ၊ မည်သည့်အရာတွေက OSI model အလွှာတွေဖြစ်သလဲဆိုတာနှင့် ၎င်းတို့ရဲ့ တာ၀န်အသီးသီးက ဘာတွေဖြစ်သလဲဆိုတာ အနက်ဖွင့်ကြည့်ရအောင်။

Application Layer	Application တစ်ခုကို ထို application နှင့် user interface ကြားတွင် တိုက်ရိုက်တုံ့ပြန်မှု ပြုရန် တာ၀န်ယူထားပါသည်။ ဥပမာ၊ IE (သို့) Firefox ကဲ့သို့ web browser များ အသုံးပြု ခြင်းများ ဖြစ်ပါသည်။
Presentation Layer	နှစ်ဦးနှစ်ဖက်လုံးကြားမ ၂ နားလည်နိုင်တဲ့နည်းလမ်းတစ်ခုဖြင့် အချက်အလက်များဖလှယ်နိုင် ရန် အာမခံပေးခြင်းအတွက် တာ၀န်ယူပါတယ်။ encryption ပုံစံအသုံးပြုသည့် ၀န်ဆောင်မှု တွေမှာတော့၊ ထို encryption တွေက presentation layer မှာဖြစ်ပေါ်ပါတယ်။
Session Layer	ကွန်ပြူတာနှစ်လုံးကြားက ဆွေးနွေးခန်းထိန်းချုပ်မှုအတွက် တာ၀န်ယူပါတယ်။ အခြေခံအ၁း ဖြင့် ကွန်ပြူနှစ်လုံးကြားမှာဖြစ်ပေါ်နေတဲ့ ဆက်သွယ်မှုအားလုံးကို တည်ထောင်ခြင်း၊ စီမံခြင်း နှင့် ရပ်ဆိုင်းခြင်း များကိုပြုလုပ်ပါတယ်။
Transport Layer	ကွန်ပြူတာများကြ ၁ ရိုးရှင်းသောအချက်အလက် မျ၁း လွှဲပြောင်းခြင်း၊ အပေါ်အလွှာများသို့ ယုံကြည် စိတ်ချရသောအချက်အလက်လွှဲပြောင်းခြင်းများ လုပ်ဆောင်ပါတယ်။ ထို့ကြောင့် ၎င်းအလ၀့ ၁ သည် ကွန်ယက်တစ်ခုပေါ်မှာယုံကြည်စွာသယ်ဆောင်ထားနိုင်သေ ၁ အပိုင်းကဏ္ဍသူ ငယ်အတွင်းမှ အချက်အလက်အားလုံးကိုစုစည်းရန် တာ၀န်ယူပါတယ်။ အကယ်၍ packet တစ်ခုက ပျောက်ဆုံးသွားခြင်း (သို့) မရောက်ရှိခြင်းများဖြစ်လျှင်၊ထို packet ကို ပြန်လည်ပို့ ဆောင်ပြီး၊ မှန်ကန်တဲ့အစီအစဉ်အတိုင်း ပြန်လည်စုစည်းထားရန်သည် Transport Layer၏ လုပ်ငန်း ဖြစ်ပါတယ်။
Network Layer	ဤအလွှာက ဆက်သွယ်မှု၏လိပ်စာတပ်ပေးခြင်းကဏ္ဍသူကိုတာ၀န်ယူထားပြီး ကွန်ယက်ပေါ်က IP လိပ်စာတစ်ခုချင်းစီအား တူညီမှုမရှိရန် စစ်ဆေးခြင်းသာမက ဘယ်အပိုင်းက အဆင်သင့် ဖြစ်နေလ ` (ကောင်းလား၊ဆိုးလား) ဆိုတာပါစစ်ဆေးပေးရပါတယ်။ ၎င်းက အချက်အလက ် တွေကို နောက်ဆုံးဦးတည်ရာနေရာရောက်တဲ့အထ ° hop တစ်ခုမှ၊ တစ်ခု အဆင့်ဆင့်သယ်ယူ ၍ ပို့ဆောင်ပေးပါတယ်။

Data Link layer	Data link အလွှာကိုတော့ ရုပ်ပိုင်းဆိုင်ရာအလွှာအား ဖြစ်ပေါ်နိုင်တဲ့ errors များမှ ပြန်လည်ပြင်ဆင်နိုင်ရန် စီစဉ်ထားပြီး ချိတ်ဆက်မှုကြားခံများဖြင့် ဆက်သွယ်လုပ်ဆောင်ပါတယ်။အခြေခံအားဖြင့် ၎င်းအလွှာက မရှိမဖြစ်လိုအပ်သော မည်သည့်ရုပ်ပိုင်းဆိုင်ရာ နည်းစနစ်များ (ရေဒီယိုလှိုင်းများ၊ fiber-optic ကြိုးများ၊ ကြေးနန်းကြိုးများ)ပေါ်မှမဆို အချက်အလက်များကို သယ်ယူပို့ဆောင်နိုင်ရန် (ဖွဲ့စည်းထုပ်ပိုးခြင်း - encapsulates) ပြုလုပ်ပါတယ်။
Physical layer	ဤအလွှာက ကရိယာများ၏ ရုပ်ပိုင်းဆိုင်ရာအသေးစိတ်ဖေါ်ပြချက်များကို အနက်ဖွင့်ပေးပြီး၊ ရွေးခြယ်ထားသောကြားခံများမှတဆင့် အချက်အလက်များကိုသယ်ယူပို့ဆောင်ရန် ရည်ရွယ် လုပ်ဆောင်ပါသည်။ WiFi ချိတ်ဆက်မှုတစ်ခုအတွက် ၎င်းက ရေဒီယို signal တစ်ခု၊ fiber ချိတ်ဆက်မှုအတွက် ၎င်းက အလင်းတစ်ခုဖြစ်ပြီး၊ ကြေးနီချိတ်ဆက်မှု အတွက်၎င်းက ဂါယာကြိုးပေါ်မှ လျပ်စစ် signal တစ်ခုဖြစ်ပါတယ်။

ဤ အလွှာခုနှစ်ခုတို့က ကွန်ပြူတာများအကြာ ၁ ။ ယုံကြည်စိတ်ချရသောဆက်သွယ်ရေးရရှိရန် လိုအပ်သောအရာမှန်သမျှနှင့် ညှိနှိုင်းဆောင်ရွက်မှုပြုပါတယ်။

ကျွန်တော်တို့ဆွေးနွေးခဲ့သမ ျ ျ model အမျိုးမျိုးတို့ကို ဘေးချင်းယှဉ်တွဲကြည့်လျင် အောက်ပါအတိုင်းတွေ့နိုင်ပါတယ် -

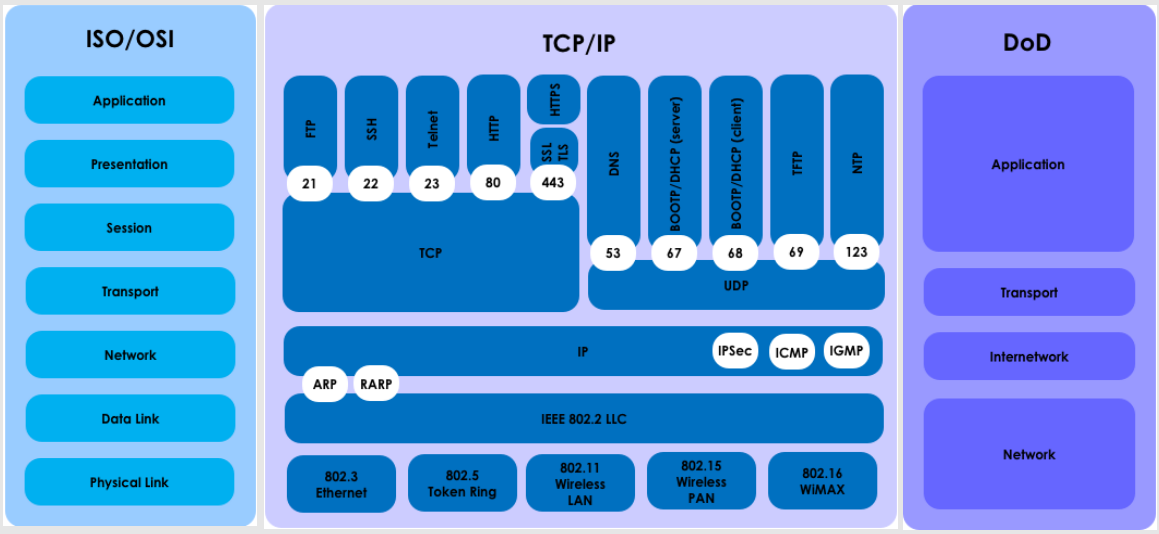


Figure 3.8: Networking Models Compared

Today's teens are in a world with major communication and productivity channels open to them and they don't have the knowledge to defend themselves against the fraud, identity theft, privacy leaks and other attacks made against them just for using the Internet. This is the reason for Hacker Highschool.

The Hacker Highschool project is the development of security and privacy awareness learning materials for junior high and high school students.

Hacker Highschool is a set of lessons and a practical means of making hackers. Beyond just providing cybersecurity awareness and critical Internet skills, we need to teach the young people of today how to be resourceful, creative, and logical, traits synonymous with hackers. The program contains free security and privacy awareness teaching materials and back-end support for teachers of accredited junior high, high schools, and home schooling. There are multiple workbooks available in multiple languages. These are lessons that challenge teens to be as resourceful as hackers, including safe Internet use, web privacy, researching on the internet, avoiding viruses and Trojans, legalities and ethics, and more.

The HHS program is developed by ISECOM, a non-profit, open-source research group focused on security awareness and professional security development and accreditation.

Hacker Highschool
SECURITY AWARENESS FOR TEENS

ISECOM