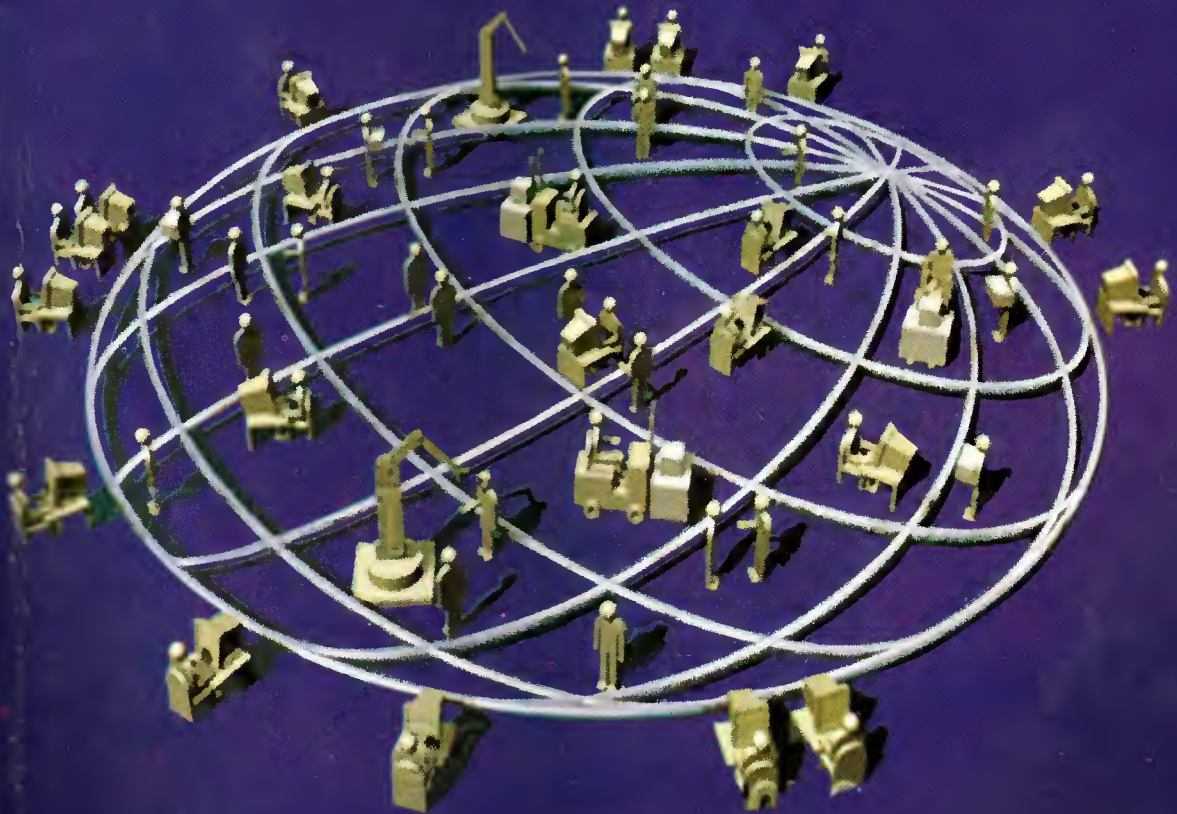




Beginner's Guide to Networking

ကွန်ပျူတာမှ ကွန်ယက်ဆီသို့

တည်ဆောက်အသုံးပြုခြင်းနှင့် အခြေခံသဘောတရားများ



မျိုးသူရ

ကွန်ပျူတာမှ ကွန်ယက်ဆီသို့

မျိုးသူရ



Beginner's Guide to Networking

တွန့်ပျူတာမှတွန့်ယတ်ဆီဆို့
တည်ဆောက်အသုံးပြုခြင်းနှင့်အခြေခံသဘောတရားများ

မျိုးသူရ



ဖြန့်ချိရေး

ဗျာဏ်ပွင့်စာပေ

အမှတ်(၃၆၇)၊ ဗိုလ်ချုပ်အောင်ဆန်းလမ်း၊ ဗိုလ်ချုပ်တော်လမ်းမတစ်လျှောက်၊ ရန်ကင်းမြို့

ဖုန်း-၇၀၀၅၇၉၊ ၀၉၅၁၄၀၅၅၈

openeyes@mail4u.com.mm



Beginner's Guide To Networking



CONTENT

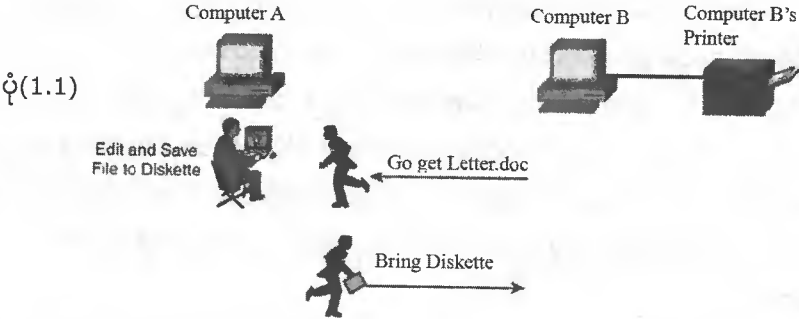
CHAPTER	TITLE	PAGE
Chapter -1	Introduction to Networking	1
Chapter -2	Set of Rules (Standards)	11
Chapter -3	Recognize and Recover Error	17
Chapter -4	An Ethernet Frame	26
Chapter -5	Central Device (HUB)	37
Chapter -6	Network Addressing & IP Routing	47
Chapter -7	OSI Model	63
Chapter -8	Network Hardware	73
Chapter -9	Network Standards	86
Chapter -10	Network Topology	91
Chapter -11	Network Media (or) Transmission Media	100
Chapter -12	Building A Peer-To-Peer Network	127
Chapter -13	Wireless Network	145
Chapter -14	Creating User Accounts	155
Chapter -15	Internet Access	201

Introduction to Networking

Network ဘယ်ကစသလဲလို့ မေးလာခဲ့ရင်တော့ network အစ ကွန်ပျူတာကလို့ ပြောရမှာ ဖြစ်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ ကွန်ပျူတာတွေ မပေါ်ခင်တုန်းက network ဆိုတာမရှိခဲ့ပါဘူး။ နည်းနည်းလေးထပ်ပိုပြောရရင် ကမ္ဘာ့ပထမဆုံးကွန်ပျူတာတစ်လုံးကို တီထွင်ခဲ့ပြီးချိန်ထိလည်း network ဆိုတာမရှိသေးပါဘူး။ ဒုတိယမြောက် ကွန်ပျူတာရယ်လို့ ပေါ်လာတဲ့အချိန်ကစပြီး တဖက်ကွန်ပျူတာထဲမှာ ရှိနေတဲ့ file တွေ၊ folder တွေကို မိမိကွန်ပျူတာထဲမှာရှိနေသကဲ့သို့ ထိုင်ရာမထယူငင်အသုံးပြုနိုင်အောင် နည်းလမ်းအမျိုးမျိုးတို့ဖြင့် တီထွင်ကြံဆခဲ့ကြပါတယ်။

အဲဒီလို network တွေမပေါ်ခင်က၊ တနည်းဆိုရရင် ကွန်ပျူတာတွေကို ချိတ်ဆက်မသုံးခင်ကဆိုရင် file၊ folder အစရှိတဲ့ data တွေကို floppy (သို့) CD ထဲကူးယူပြီး အခြားကွန်ပျူတာရှိရာသို့ သယ်ဆောင်သွားရပါတယ်။ အဲဒီလိုကွန်ပျူတာတွေကြားမှာ လူးလားခေါက်ပြီး အခြားကွန်ပျူတာတွေကြားမှာ လူးလားခေါက်ပြီး data များအား လူကိုယ်တိုင် သယ်ဆောင်ဖလှယ်ခြင်းကို sneakernet လို့ခေါ်ပါတယ်။

Sneakernet

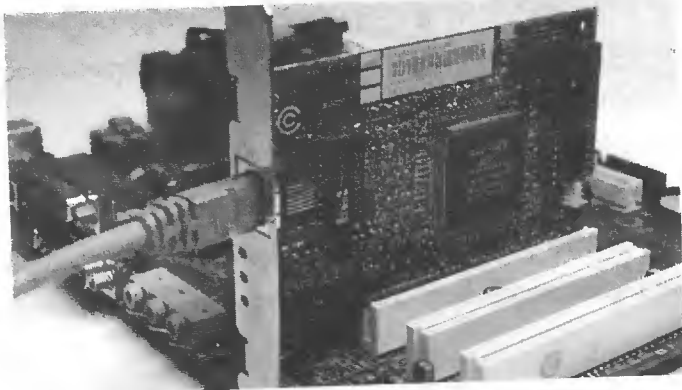


sneakernet ရဲ့ အဓိကပြဿနာကတော့ အချိန်ကုန် လူပင်ပန်းခြင်းပင်ဖြစ်ပါတယ်။ အဲဒီပြဿနာကို network တွေတည်ဆောက်ခြင်းအားဖြင့် ငွေကုန်ကြေးကျများစွာမရှိပဲ ဖြေရှင်းနိုင်ကြသည့် အတွက် အဖွဲ့အစည်းကြီးကြီးမှာပဲဖြစ်ဖြစ်၊ သေးသေးမှာပဲဖြစ်ဖြစ် network အသုံးပြုမှုတွင်ကျယ်လာခြင်း ဖြစ်ပါတယ်။ အခြေခံအားဖြင့် network ဆိုတာ အနည်းဆုံးကွန်ပျူတာ ၂လုံး (သို့) ၂လုံးကနေ ရာထောင်ချီတဲ့ ကွန်ပျူတာတွေသည် တစ်လုံးနှင့်တစ်လုံး အပြန်အလှန် ဖလှယ်နိုင်အောင် resource တွေဖြစ်ကြတဲ့ disk drive၊ modem၊ printer အစရှိသည်တို့ကို မျှဝေသုံးစွဲနိုင်အောင် cable ဖြင့်ချိတ်ဆက်ထားခြင်းဖြစ်ပါတယ်။ (အချို့ network တွေမှာတော့ cable အစားကြိုးမဲ့ wireless ကိုအသုံးပြုကြပါတယ်။)

သူ့ရဲ့သဘောကတော့ ရှင်းရှင်းလေးပါပဲ။ တဖက်ကွန်ပျူတာထဲမှာရှိနေတဲ့ information တွေကို လူကိုယ်တိုင် သယ်ဆောင်ဖလှယ်စရာမလိုပဲ ဒီဘက်ကွန်ပျူတာကနေ ထိုင်ရာမထယူသုံးနိုင်ရင် အဲဒါ net-work ဖြစ်ပါတယ်။ ထိုကဲ့သို့ information တွေကို တဖက်နှင့် တဖက်အပြန်အလှန်ဖလှယ်နိုင်အောင် ဘာတွေလိုအပ်မလဲ။

အဲဒါကတော့ network မှာပါဝင်မယ့် ကွန်ပျူတာအရေအတွက်၊ နေရာချတည်ဆောက်ပုံ အခင်းအကျင်းအစီအမံပေါ်မူတည်ပြီး အသုံးပြုရမယ့် device တွေကွဲပြားခြားနားစွာလိုအပ်မှာဖြစ်ပါတယ်။ အခြေခံအကျဆုံး လိုအပ်ချက်ကတော့ network ချိတ်ဆက်မည့်ကွန်ပျူတာတိုင်းတွင် NIC (Network Interface Card) တစ်ခုစီရှိဖို့လိုခြင်းဖြစ်ပါတယ်။

ပုံ(1.2)



NIC ကို network adapter network card ရယ်လို့လည်း အမည်အမျိုးမျိုးဖြင့် ခေါ်လေ့ ရှိကြပါတယ်။ ပုံမှန်အားဖြင့် ကွန်ပျူတာတွင် motherboard ပေါ်မှာ သီးခြားစိုက်သွင်း တပ်ဆင်ရပါတယ်။ ဒါပေမယ့် အချို့သော motherboard တွေပေါ်မှာ တစ်ပါတည်း အသေထည့်သွင်း တပ်ဆင်ထားခြင်း မျိုးလည်းရှိပါတယ်။ ဘယ်လိုအနေအထားနှင့်ပုံရိရှိ network card တို့ရဲ့အဓိကလုပ်ဆောင်မှုက ကွန်ပျူတာ data တွေကို ဗို့အားတစ်ခုရှိသော electric signal များအဖြစ်ပြောင်းပြီး transmit လုပ်ခြင်းနှင့် ဝင်လာတဲ့ electric signal တွေကို ကွန်ပျူတာမှ နားလည်နိုင်သော data များအဖြစ်သို့ ပြောင်းလဲ receive လုပ်ခြင်းတို့ဖြစ်ပါတယ်။

ကွန်ပျူတာတွေဆိုတာက စာလုံးတွေပဲဖြစ်ဖြစ်၊ ပုံတွေပဲဖြစ်ဖြစ်၊ အရောင်တွေ၊ ကိန်းဂဏန်းတွေ အစရှိတဲ့ မည်သည့် information မျိုးကိုမဆို binary data များအဖြစ်သာ နားလည်သိမ်းဆည်းနိုင်စွမ်း ပါတယ်။ binary data မှာဆိုရင် 1 နှင့် 0 နှစ်မျိုးသာပါရှိပါတယ်။ 1 များ၊ 0 များ ပေါင်းစပ်ပါဝင်တဲ့ အစုတစ်စုသည် ကိန်းတစ်လုံး (သို့) စာလုံးတစ်လုံးကို ကိုယ်စားပြုနိုင်ပါတယ်။ ဥပမာ binary number တစ်ခုဖြစ်တဲ့ 0001 ဆိုပါတော့။ အဲဒီ 0001 အစုတစ်စုသည် decimal number "1" ဆိုတာကို ရည်ညွှန်းပါတယ်။ နောက်တစ်မျိုး 0010 ဆိုတာသည် decimal ဂဏန်း 2 ဆိုတာကို ရည်ညွှန်းပါတယ်။ (binary မှ decimal သို့ decimal မှ binary သို့ ပြောင်းပုံများကို (စာ-၄၇) တွင်ကြည့်ပါ။

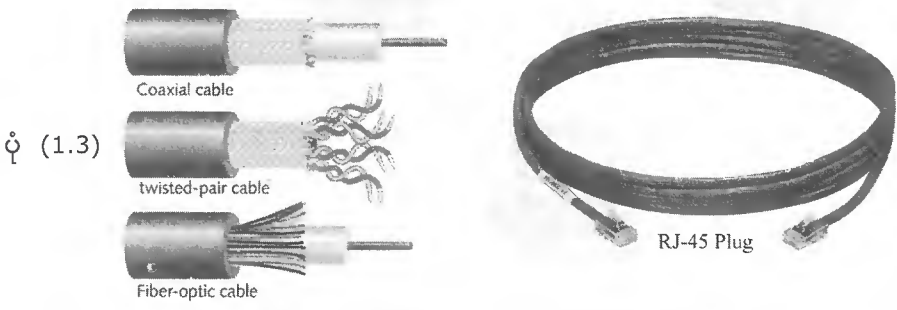
ဖော်ပြခဲ့တဲ့ အစုတစ်စုမှာပါတဲ့ 0 (သို့) 1 တစ်လုံးစီကို bit တစ်ခုလို့ခေါ်ပါတယ်။ bit သည် data capacity နှင့် ပတ်သက်၍ အငယ်ဆုံးအတိုင်းအတာ unit ဖြစ်ပြီး b ဖြင့် ကိုယ်စားပြုဖော်ပြလေ့ရှိပါတယ်။ အောက်မှာဆိုရင် data capacity နှင့် ပတ်သက်သော အတိုင်းအတာ ယူနစ်များကို ဖော်ပြထားပါတယ်။

- 1 bit = 1 (သို့) 0 (b)
- 8 bit = 1 byte (B)

1024 bytes	=	1 kilobyte (KB)
1024 kilobytes	=	1 Megabyte (MB)
1024 Megabytes	=	1 Gigabyte (GB)
1024 Gigabytes	=	1 Terabyte (TB)

file တွေဆိုတာလည်း bit တို့ဖြင့်ဖွဲ့စည်းထားခြင်းဖြစ်ပါတယ်။ 1 KB အရွယ်အစားရှိတဲ့ file တစ်ခုမှာ ဆိုရင် bit အရေအတွက် (1024 × 8) 8192 ပါရှိမှာဖြစ်ပါတယ်။ network ပေါ်မှာ file တွေ ပေးပို့ဖလှယ်ကြခြင်းသည် အမှန်တကယ်တော့ကွန်ပျူတာတစ်လုံးမှ bit တွေကိုအခြားကွန်ပျူတာတစ်လုံး ထံသို့ပေးပို့ခြင်းဖြစ်ပါတယ်။ ဆိုရင် file တစ်ခုကို network ပေါ်မှာ ပေးပို့ဖို့ရှိလာပြီဆိုရင် ပေးပို့မည့် ကွန်ပျူတာမှ NIC သည် file ထဲတွင်ပါဝင်သော information ကိုယ်စားပြု bit တွေကို electric signal များအဖြစ်ပြောင်းပြီး transmit လုပ်ပါတယ်။ အလားတူလက်ခံမည့်ကွန်ပျူတာမှ NIC သည်ဝင်လာတဲ့ electric signal တွေကို ကွန်ပျူတာမှ နားလည်အသုံးပြုနိုင်မည့် bit များအဖြစ်ပြောင်းပြီး receive လုပ်ကြရတယ်။ အနှစ်ချုပ်ဆိုရင် information ကိုယ်စားပြု bit တွေသည်ကွန်ပျူတာတစ်လုံးမှတစ်လုံးသို့ electric signal များအဖြစ်ဆက်သွယ်ထားသော transmission media ပေါ်မှဖြတ်သန်းရွေ့လျားကြခြင်း ဖြစ်ပါတယ်။

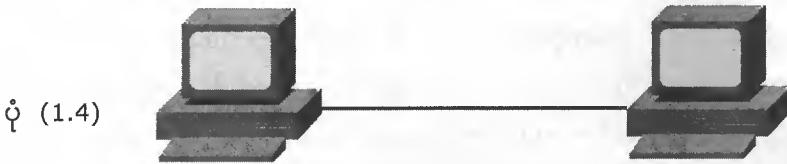
Transmission media ဆိုတာက ကွန်ပျူတာတွေ တစ်လုံးနှင့် တစ်လုံး data ပေးပို့ ဖလှယ်နိုင်အောင်ဆက်သွယ်ထားသော twisted pair coaxial၊ fiber optic အစရှိသော cable တို့ပင် ဖြစ်ပါတယ်။ wireless network တွေအတွက်ကျတော့ “လေ” သည် transmission media ဖြစ်ပါလိမ့်မယ်။



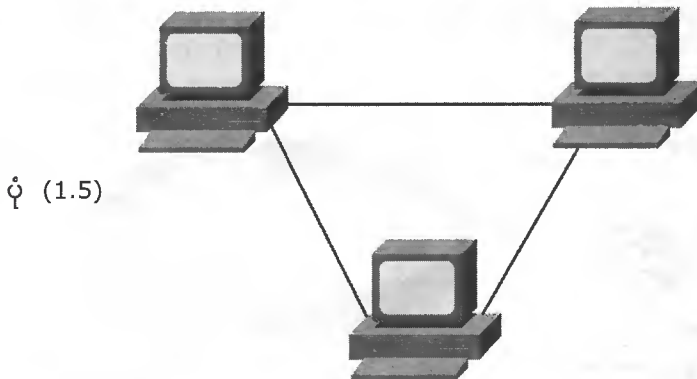
ယနေ့အသုံးအများဆုံး media ကတော့ အတွင်းမှာ ဝါယာနန်းကြိုးမျှင် ရှစ်ချောင်းပါတဲ့ twisted pair cable ပင်ဖြစ်ပါတယ်။ twisted pair cable ကိုအသုံးပြုတည်ဆောက်မည် network တွေအတွက် standard interface သည် RJ-45 (Registered-Jack) ဖြစ်ပါတယ်။ RJ-45 plug (connector) နှင့် RJ-45 jack (port) ဆိုပြီးအခေါ် ညမျိုးရှိပါတယ်။

Twisted pair cable ၏ ဟိုဘက်ဒီဘက် အစွန်း ညာဘက်မှာ RJ-45 plug ကို တပ်ဆင်ပြီး အသုံးပြုရန်သော network cable အဖြစ်သို့လုပ်ဆောင်ရပါတယ်။ ၎င်း network cable ကို RJ-45 jack (port) ပါသောကွန်ပျူတာ NIC တွင်ချိတ်ဆက်တပ်ဆင်ကြရပါတယ်။

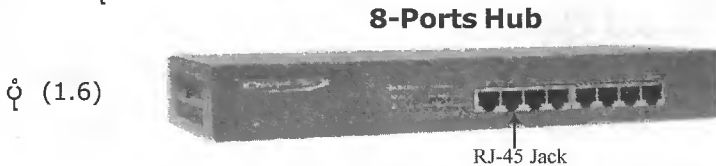
ကွန်ပျူတာ နှစ်လုံး၊ NIC နှစ်ခုနှင့် network cable တစ်ချောင်း ရှိပြီးဆိုရင် network ရယ်လို့ခေါ်ဆိုနိုင်တဲ့ ဝန်အကျဉ်းဆုံး network တစ်ခုကိုတည်ဆောက်နိုင်ပါပြီ။ တည်ဆောက်ပုံကတော့ ကွန်ပျူတာတစ်လုံးစီမှာ NIC တစ်ခုစီ စိုက်သွင်းတပ်ဆင်ပြီး cable ဖြင့် တိုက်ရိုက်ချိတ်ဆက်လိုက်ရုံ ဖြစ်ပါတယ်။



ဒါက ကွန်ပျူတာ ၂လုံးတည်းပါသည့် အရိုးရှင်းဆုံး network ဖြစ်ပါတယ်။ အကယ်၍ များကွန်ပျူတာ သုံးလုံးဆိုရင်ကော။ ဒီအဆင့်ထိအောင်လည်း NIC နှင့် cable ကိုသာသုံးပြီး network တစ်ခုဖြစ်အောင် ကြံဖန်တည်ဆောက်နိုင်ပါသေးတယ်။ ဆိုရရင် ကွန်ပျူတာတစ်လုံးစီမှာ NIC ၂ခုစီ စိုက်သွင်းတပ်ဆင်ပြီး တစ်လုံးလျှင် cable နှစ်ချောင်းနဲ့ ဖြင့် တိုက်ရိုက်ချိတ်ဆက် အသုံးပြုနိုင်ပါသေးတယ်။ ကွန်ပျူတာ တစ်လုံးကနေ transmit လုပ်မယ်ဆိုရင် ကျန်ကွန်ပျူတာ နှစ်လုံးထံရောက်မယ်ပေါ့။



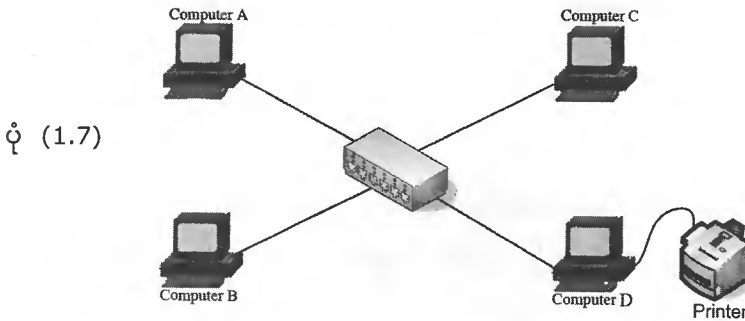
သို့သော် အရေအတွက် ဆယ်ဂဏန်းလောက်ရှိလာပြီဆိုရင်ပဲ အဲဒီလို ကွန်ပျူတာအချင်းချင်း တိုက်ရိုက်ချိတ်ဆက်တပ်ဆင်ဖို့ရန် ဘယ်လိုမှ မဖြစ်နိုင်တော့ပါ။ အရေအတွက်များလာတာနှင့်အမျှ တိုးလာမယ့် NIC တွေတပ်ဆင်ဖို့ရန် ကွန်ပျူတာထဲမှာ နေရာလွတ်မရှိပါဘူး။ ဤပြဿနာကို ပြေလည်စေရန် အတွက် Hub ဆိုတာပေါ်လာပါတယ်။



Hub ဆိုတာက port များစွာပါရှိပြီး ကွန်ပျူတာတစ်လုံးလျှင် cable တစ်ချောင်းစီဖြင့် ဗဟိုပြု ချိတ်ဆက် တပ်ဆင်ရသော central device ဖြစ်ပါတယ်။ ပါရှိတဲ့ port အရေအတွက်ပေါ်မူတည်ပြီး 8 port hub၊ 24 port hub ရယ်လို့လည်းခွဲခြားခေါ်ဝေါ်ကြပါတယ်။ မည်သို့ခေါ်ဝေါ် hub တို့ရဲ့အဓိကလုပ်ဆောင်မှုကတော့ port တစ်ခုကနေဝင်လာတဲ့ signal ကို ကျန် port များအားလုံးဆီသို့ ဖြန့်ဝေပေးခြင်းဖြစ်ပါတယ်။ သည့်အတွက် port တစ်ခုမှာတပ်ဆင်ထားတဲ့ကွန်ပျူတာကနေ transmit လုပ်လိုက်တဲ့ signal တွေသည် ကျန် port တွင်တပ်ဆင်ထားသောကွန်ပျူတာအားလုံးဆီသို့တပြိုင်နက် ရောက်ရှိနိုင်ပါတယ်။

network တစ်ခု တည်ဆောက်ရန်အတွက်ကွန်ပျူတာတစ်လုံးစီမှာ NIC (Network Interface Card) တစ်ခုစီ စိုက်သွင်းတပ်ဆင်ပြီး central device လို့ခေါ်တဲ့ hub (သို့) switch ဆီသို့ cable တစ်ချောင်း စီဖြင့် ချိတ်ဆက်တပ်ဆင်လိုက်ရုံဖြစ်ပါတယ်။ အောက်ဖော်ပြပါပုံ (1.7)သည် ကွန်ပျူတာလေးလုံးဖြင့် တည်ဆောက်ထားတဲ့ network တစ်ခုရဲ့ပုံကြမ်း ဖြစ်ပါတယ်။ ကွန်ပျူတာ လေးလုံးစလုံးသည် hub ဆီသို့ network cable တို့ဖြင့် ချိတ်ဆက်ထားတာကို မြင်နိုင်ပါတယ်။

Typical small office network



ပုံ (1.7)

အဲဒီလိုချိတ်ဆက်ပြီးပြီဆိုရင် Operating System (Windows 2000, Windows XP) တို့မှာလိုအပ်တဲ့ setting တွေကိုထည့်သွင်းပေးရုံဖြင့် အသုံးပြု၍ရနိုင်သော network တစ်ခုတည်ဆောက်ပြီးဖြစ်ပါလိမ့်မယ်။ အသုံးပြု၍ရနိုင်သော network တစ်ခုဖြစ်ပြီဆိုရင် ကွန်ပျူတာ A၊ B၊ C၊ D လေးလုံးစလုံးသည် file၊ folderအစရှိတဲ့ information တွေကိုအပြန်အလှန်ဖလှယ်နိုင်ကြပါပြီ။ ဒါ့အပြင် ကွန်ပျူတာ D မှာတပ်ဆင်ထားတဲ့ printerကို ကျန်ကွန်ပျူတာသုံးလုံးစလုံးကနေပြီး မိမိတို့ကွန်ပျူတာမှာ တပ်ဆင်ထားသကဲ့သို့အသုံးပြုနိုင်ကြပါပြီ။

Why Use Network?

file sharingနှင့် printer sharing တို့ကို network အသုံးပြုခြင်းရဲ့အဓိက အကြောင်းရင်း ၂ရပ်လို့ဆိုကြပါတယ်။ ဒါ့ကြောင့် network ပေါ်မှာ file တွေကို share ပေး၍အသုံးပြုခြင်းသည် ပထမဦးစားပေးရည်ရွယ်ချက်ဖြစ်ခဲ့မယ်ဆိုရင် printerတစ်လုံးတည်းကိုလူအများတစ်ပြိုင်နက်အသုံးပြုနိုင်အောင် share ပေး၍အသုံးပြုခြင်းသည် ဒုတိယရည်ရွယ်ချက် ဖြစ်ပါလိမ့်မည်။

● File Sharing

file sharing သည် ကွန်ပျူတာတွေကို စုပေါင်းချိတ်ဆက်ပြီး network အဖြစ်အသုံးပြုခြင်းရဲ့အဓိကရည်ရွယ်ချက်ဖြစ်ပါတယ်။ file sharing လုပ်ရန်မိမိကွန်ပျူတာထဲက folder (သို့) disk drive တစ်ခုခုကို network ပေါ်ကနေ အခြားသူများယူငင်အသုံးပြုနိုင်ရန် အတွက် share ပေးလိုက်ရုံ ဖြစ်ပါတယ်။ network တည်ဆောက်ထားတဲ့ အပေါ်မူတည်ပြီး နည်းလမ်းအမျိုးမျိုးတို့ဖြင့် share ပေးနိုင်ကြပါတယ်။

ဆိုရရင် file ကို attach တွဲပြီး တစ်ယောက်ယောက်ဆီကို email ဖြင့်ပို့မယ်၊ မိမိကွန်ပျူတာထဲက file တွေ၊ folder တွေကို အခြားသူများတိုက်ရိုက်ယူငင်အသုံးပြုနိုင်အောင် network ပေါ်မှာ share ပေးထားမယ်၊ ဒါမှမဟုတ် မိမိကွန်ပျူတာထဲက file ကို copy ကူးယူပြီး အခြားကွန်ပျူတာ တစ်လုံးလုံးထဲ လှမ်းထည့်ပေးမယ်၊ အစရှိသဖြင့် နည်းလမ်းအမျိုးမျိုးဖြင့် share လုပ်ပြီး အသုံးပြုနိုင်ကြပါတယ်။ ဘယ်လိုနည်းလမ်းပဲသုံးသုံး sneakernet မှာလို CD တွေ၊ floppy တွေဖြင့် သယ်ဆောင်ခြင်းမဟုတ်ပဲ cable ပေါ်ကနေပြီး ကွန်ပျူတာတစ်လုံးမှ အခြားကွန်ပျူတာတစ်လုံးသို့ data တွေပို့ရင် file sharing ပဲဖြစ်ပါတယ်။

● Printing Sharing

printer ကို share လုပ်၍အသုံးပြုခြင်းအားဖြင့် ကုန်ကျစရိတ်သက်သာစေခြင်းဆိုတဲ့ အားသာချက်ကိုရရှိစေပါတယ်။ ပုံ (1.2) တွင်ကြည့်ပါ။ ကွန်ပျူတာ D မှ printer ကို မိမိကွန်ပျူတာမှာ တပ်ထားသကဲ့သို့ အခြားကွန်ပျူတာ A၊ B၊ C တို့ကနေပြီးလှမ်းသုံးနိုင်ပါတယ်။ အကယ်၍များ network ချိတ်ဆက်ခြင်းမရှိခဲ့ဘူးဆိုရင် ကွန်ပျူတာ A၊ B၊ C တို့မှာ သီးခြား printer တစ်လုံးစီ ဝယ်ယူ တပ်ဆင်ရမှာဖြစ်ပါတယ်။

● Type of Networks

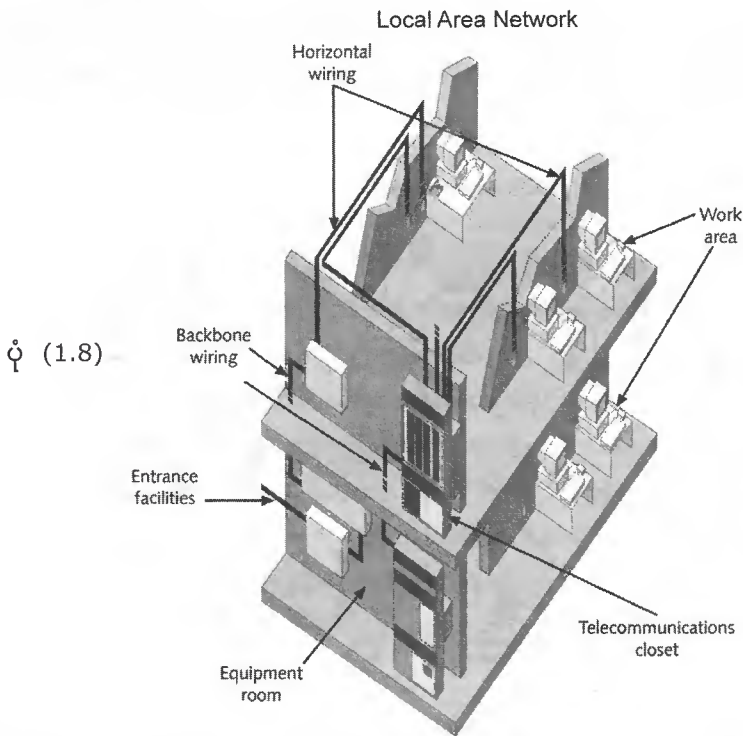
network အမျိုးအစားတွေကို structure နှင့် size ပေါ်မူတည်ပြီး ခွဲခြားလေ့ရှိကြပါတယ်။ structure ဆိုတဲ့ ဇွဲစည်းစီမံထားပုံပေါ်မူတည်ပြီး ခွဲမယ်ဆိုရင် peer-to-peer နှင့် client /server ဆိုပြီး နှစ်မျိုးရှိပါတယ်။ size ဆိုတဲ့ network ချိတ်ဆက်ထားတဲ့ဧရိယာအကျယ်အဝန်းပေါ်မူတည်ပြီး ခွဲမယ်ဆိုရင် အဓိကအားဖြင့် LAN | MAN | WAN ဆိုပြီး အခြေခံ အကျဆုံး network အမျိုးအစားသုံးမျိုးရှိပါတယ်။

● LAN (Local Area Network)

LAN ကို နယ်နိမိတ်အကန့်အသတ်အားဖြင့် အဆောက်အဦးတစ်ခုအတွင်းမှာရှိတဲ့ ရုံးတစ်ရုံးတစ်ရုံး network လို့ အဓိပ္ပါယ်ဖွင့်ဆိုကြပါတယ်။ ဟိုးယခင် LAN ရယ်လို့စတင် ချိတ်ဆက်အသုံးပြုလာခဲ့စဉ်တုန်း

က ဆိုရင် အကွာအဝေးအားဖြင့် ကွန်ပျူတာမှ hub ဆီသို့ 185m (ပေ၆၀၀) နှင့် ကွန်ပျူတာအရေအတွက် ၃၀ ထက် မပိုရလို့ ကန့်သတ်ချက်ရှိခဲ့ပါတယ်။ ယနေ့အချိန်မှာတော့ နည်းပညာတွေပိုမိုဖွံ့ဖြိုးတိုးတက်လာခြင်း နှင့်အတူ LAN ရဲ့အရွယ်အစား၊ တစ်နည်းဆိုရရင် အကွာအဝေးနှင့်ပတ်သက်တဲ့ ကွန်ပျူတာအရေအတွက် ပိုမိုများပြားလာပါတယ်။

အဲဒီလို LAN တွေရဲ့အရွယ်အစားပြောင်းလည်းလာသလို တည်ဆောက်ပုံ structure တွေလည်း ပြောင်းလဲလာပါတယ်။ ဟိုးယခင်တုန်းက LAN ဆိုတာနှင့် သူ၏ structure သည် peer-to-peer ဖြစ်ပါတယ်။ သို့သော် ယနေ့အချိန်မှာတော့ peer-to-peer လည်းဖြစ်နိုင်သလို client/server လည်းဖြစ်နိုင်ပါတယ်။



MAN (Metropolitan Area Network)

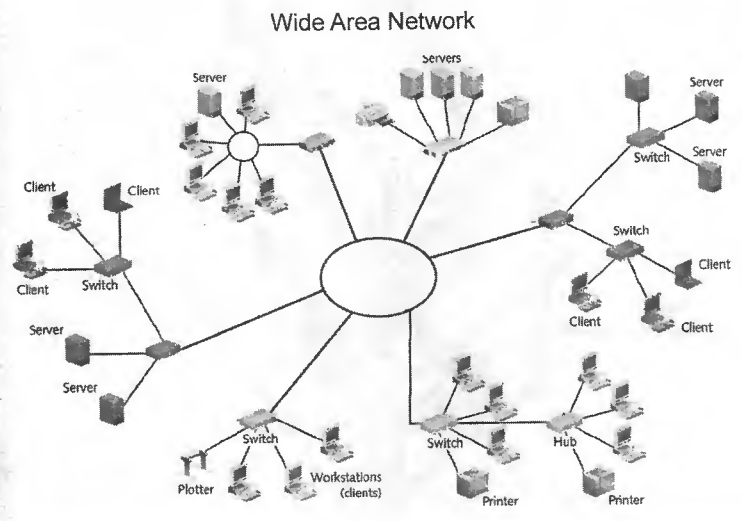
MAN ဆိုတာကတော့ LAN တွေထက်ကြီးမယ် WAN တွေလောက်လဲ မကြီးတဲ့ network မျိုးဖြစ်ပါတယ်။ ဆိုရရင် LAN နှစ်ခု (သို့) နှစ်ခုထက်ပိုတဲ့ LAN တွေကို စုပေါင်းချိတ်ဆက်ထားမယ်။ မြေပြင် ဧရိယာအကျယ်အဝန်းအားဖြင့်လည်း မြို့တစ်မြို့အတွင်းမှာသာ ရှိတဲ့ network မျိုးဖြစ်ပါတယ်။ ယနေ့အချိန်မှာတော့ MAN ဆိုတဲ့ အခေါ်အဝေါ်သည် အသုံးများတွင်ကျယ်ခြင်း မရှိတော့ပါဘူး။ network ဆိုတာနှင့် LAN (သို့) WAN နှစ်မျိုးထဲက တစ်မျိုးမျိုးဖြင့်သာ ခေါ်ဝေါ်သုံးစွဲကြပါတယ်။

WAN (Wide Area Network)

WAN ဆိုတာကို အလွယ်ပြောရရင်တော့ LAN ပေါင်းများစွာကို ချိတ်ဆက်ထားတဲ့ Network ကြီးတစ်ခုဖြစ်ပါတယ်။ ဘယ်လောက်ကြီးသလဲဆိုရင် အကွာအဝေး၊ ဧရိယာ ကန့်သတ်ချက်မရှိဘဲ တစ်မြို့မှ တစ်မြို့၊ တစ်နိုင်ငံမှတစ်နိုင်ငံ ကမ္ဘာအနှံ့ဖြတ်ပြီး ဆက်သွယ်ထားသော ကွန်ယက်မျိုးဖြစ်ပါတယ်။ အများအားဖြင့် နိုင်ငံအနှံ့၊ ကမ္ဘာနေရာအနှံ့မှာ ရုံးခွဲတွေရှိနေတဲ့ အဖွဲ့အစည်းတွေသာ အသုံးပြုလေ့ရှိတဲ့ network မျိုးဖြစ်ပါတယ်။

ဒါ့အပြင် မတူတဲ့အဖွဲ့ အစည်း အမျိုးမျိုးတို့မှ LAN တွေကို WAN အဖြစ်စုပေါင်းချိတ်ဆက် အသုံးပြုခြင်းမျိုးလည်းရှိပါတယ်။ LAN တွေကို တစ်ခုနှင့် တစ်ခုချိတ်ဆက်တဲ့ နေရာမှာ backbone (ပင်မ ဆက်ကြောင်း) အဖြစ် Radio link၊ Satellite link၊ Fiber cable တို့ထဲမှ တစ်ခုခုကို အသုံးပြုကြပါတယ်။ ယနေ့အသုံးပြုနေကြတဲ့ အင်တာနက်ဆိုတာလည်း ကမ္ဘာ့အကြီးဆုံး WAN တစ်ခုလို့ ဆိုနိုင်ပါတယ်။ ဒါကြောင့် အင်တာနက်ဆိုတာ ဆက် အသုံးပြုနေသော ကွန်ပျူတာသည် ကမ္ဘာ့အကြီးဆုံး WAN ၏ အစိတ် အပိုင်းတစ်ခုဖြစ်သွားပြီလို့ ဆိုနိုင်ပါတယ်။

ပုံ (1.9)



မှတ်ချက်။ ။ ကွန်ပျူတာ အရေအတွက် ထောင်သောင်းချီပြီး ပါဝင်နေစေကာမူ network အတွင်း မှာ ရှိနေတဲ့ ကွန်ပျူတာ တွေကို လုပ်ဆောင်မှု အရ ခွဲခြားကြည့်မယ်ဆိုရင် နှစ်မျိုးနှစ်စားသာ ရှိပါတယ်။ ပထမ တစ်မျိုးက မိမိမှာရှိတဲ့ resources (file၊ folder၊ printer) တွေကို ပေးသုံးမည့် ကွန်ပျူတာ (server) နှင့် ဒုတိယတစ်မျိုးက အခြားကွန်ပျူတာ တစ်လုံးလုံးမှာရှိနေတဲ့ resources တွေကို ယူသုံးမည့် ကွန်ပျူတာ (client) တို့ပင် ဖြစ်ကြပါတယ်။

အောက်ဖော်ပြပါဇယားမှာဆိုရင် အကွာအဝေး ဧရိယာ ပေါ်မူတည်ပြီး network အမျိုးအစား အကြမ်းမျဉ်းသတ်မှတ်မှုညွှန်ကြည့်ပုံတွေကိုဖော်ပြထားပါတယ်။

1 m	Square meter	Personal area network
10 m	Room	
100 m	Building	Local area network
1 km	Campus	
10 km	City	Metropolitan area network
100 km	Country	Wide area network
1000 km	Continent	
10,000 km	Planet	The Internet

ယခုဆက်လက်ပြီး structure ပေါ်မူတည်၍ ကွဲပြားလေ့ရှိတဲ့ peer-to-peer နှင့် client/server network တို့အကြောင်း ရှင်းလင်းဖော်ပြသွားပါမယ်။

Peer- to-Peer Network

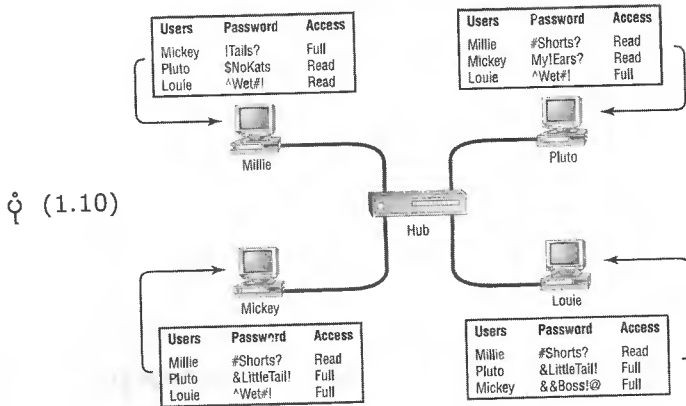
အရိုးရှင်းဆုံး network အမျိုးအစားဖြစ်ပါတယ်။ Peer-to-Peer network တစ်ခုမှာရှိတဲ့ ကွန်ပျူတာအားလုံးတို့သည် လုပ်ပိုင်ခွင့်အတူတူဖြစ်ကြပါတယ်။ သဘောကတော့ အဲဒီ network အတွင်းမှာရှိတဲ့ ကွန်ပျူတာအားလုံးတို့သည် decision maker များပဲဖြစ်ကြပါတယ်။ ဗဟိုထိန်းချုပ်မှုမရှိပဲ ကိုယ့်ဘာသာလွတ်လွတ်လပ်လပ်စီမံပိုင်ခွင့်ရှိကြပါတယ်။

တနည်းဆိုရရင် ကွန်ပျူတာတစ်လုံးသည် မိမိမှာရှိနေတဲ့ resources တွေ (file ၊ folder ၊ application ၊ modem ၊ printer) ကို ကြိုက်သလို share ပေးသုံးနိုင်သလို အခြားကွန်ပျူတာတစ်လုံးမှ share ပေးထားတဲ့ resources တွေ ယူသုံး ချင်ရင်လည်း ၎င်းကွန်ပျူတာထံမှ တိုက်ရိုက်ယူငင် အသုံးပြုနိုင်ပါတယ်။ ဒါကြောင့် peert-to-peer network ထဲမှာရှိတဲ့ ကွန်ပျူတာတွေသည် client နှင့် server နှစ်မျိုးလုံးဖြစ်နိုင်ပါတယ်။ ဆိုရရင် အခြားကွန်ပျူတာမှ resources တွေကိုယူသုံး နေချိန်တွင် မိမိကွန်ပျူတာသည် client ဖြစ်နေပြီး၊ မိမိကွန်ပျူတာမှ resources တွေကိုပေးသုံးနေချိန်မှာ server ဖြစ်နေပါလိမ့်မယ်။

ဒါ့အပြင် security ပိုင်းအနေနှင့်လည်း ဗဟိုထိန်းချုပ်မှု မရှိပါဘူး အသုံးပြုသူတစ်ယောက်သည် ကွန်ပျူတာတစ်လုံးမှနေပြီး အခြား ကွန်ပျူတာမှ share ပေးထားတဲ့ file တွေကိုလှမ်းသုံးတဲ့အခါ ထိုအသုံးပြုသူအား share file ကို delete လုပ်ခွင့်ပြုမယ်၊ မပြုဘူး။ ပြင်ဆင်ရေးသားခွင့် ပြုမယ်၊ မပြုဘူး အစရှိတဲ့ access right တွေကို သတ်မှတ်ပေးဖို့ရန် share ပေးထားတဲ့ ကွန်ပျူတာမှာသာ တာဝန်အပြည့်ရှိပါတယ်။

ဆိုရရင် security ပိုင်းအနေနှင့် တစ်နေရာရာမှ ဗဟိုပြု၍ထိန်းချုပ်မှု မရှိသည့်အတွက် share folder တစ်ခုတည်းကိုပင် ဘယ်သူ့ကိုတော့ read access ပေးမယ်၊ ဘယ်သူ့ကို write access၊ ဘယ်သူ့ကို full access ဆိုတာတွေကို share ပေးမည့် ကွန်ပျူတာတစ်လုံးချင်းစီမှာ သတ်မှတ် ပေးရမှာ ဖြစ်ပါတယ်။

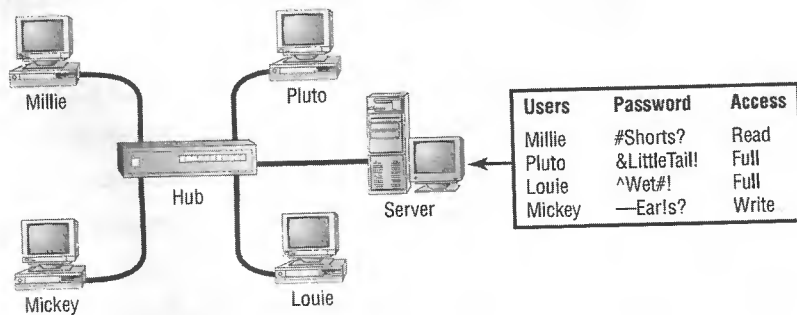
A Peer-to-Peer Network



● Client/Server Networks

Clients/Server Network တွေမှာဆိုရင် resources တွေပေးသုံးမယ့်ကွန်ပျူတာ (server) နှင့် resources တွေယူသုံးမယ့်ကွန်ပျူတာ (client) ဆိုပြီး ကွဲပြားမှုရှိလာပါတယ်။ တကယ့် client /server network အစစ်တွေမှာဆိုရင် resource တွေကို server ကွန်ပျူတာထဲမှာသာထားရှိပြီး ၎င်းတို့ကို client ကွန်ပျူတာများမှ access လုပ်ရပါတယ်။ client ကွန်ပျူတာအချင်းချင်းတိုက်ရိုက် share ပေးလို့မရပါဘူး။ server ကိုကြားခံအဖြစ်အသုံးပြုရပါတယ်။ network အတွင်း login ဝင်ရောက်အသုံးပြုခွင့်ရရန်လိုအပ်တဲ့ username၊ password တို့နှင့် login ဝင်ရောက်ပြီးတဲ့အခါဘယ် folder တွေကိုဖွင့်ကြည့်ခွင့်ရှိတယ်၊ မရှိဘူးအစရှိတဲ့ access right တွေကို database ဆောက်ပြီး server ကွန်ပျူတာထဲမှာသိမ်းဆည်းထားပါတယ်။ ဒါကြောင့် client/server network ထဲမှာရှိတဲ့ ကွန်ပျူတာများသည် ကိုယ်တိုင်စီမံပိုင်ခွင့် မရှိကြပါဘူး။ decision အားလုံးကို ဗဟိုကနေထိန်းချုပ်စီမံပေးပါတယ်။

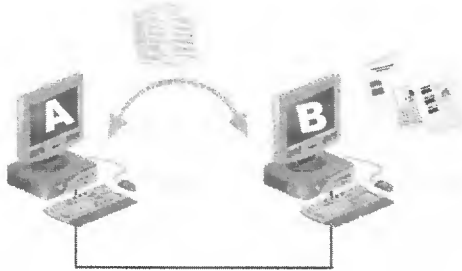
A Client/Server Network



ပုံ (1.11)

Set of Rules (Standards)

လူနှစ်ယောက်စကားပြောနေတယ်။တစ်ယောက်ကပြောနေချိန်တွင် တစ်ယောက်ကနားထောင်နေတယ်ဆိုပါစို့။ အဲဒီဖြစ်စဉ်မှာ တစ်ယောက်ကဘာပြောနေသလဲ ဆိုတာကို တစ်ဖက်လူကနားလည်ဖို့ရန် နှစ်ယောက်စလုံးတတ်ကျွမ်းသည့် ဘာသာစကားသည်တူရပါမယ်။ အဲဒီဖြစ်စဉ်ကိုပင် အခြားရှုထောင့် တစ်ခုကကြည့်မယ်ဆိုရင်ပြောကြတဲ့ "စကား" ဆိုတာတွေသည် "အသံ" တွေကိုပေါင်းစပ်ထားခြင်း ဖြစ်ပါတယ်။ တစ်ဖက်ကဘာသာစကားတစ်ခုနှင့်ပြောလိုက်လို့ထွက်လာတဲ့အသံတွေမိမိထံရောက်လာတဲ့အခါမှာလည်း ၎င်းဘာသာစကားဖြင့်ပင် အဓိပ္ပါယ်ဖော်ယူရပါတယ်။ network ချိတ်ဆက်ထားသော ကွန်ပျူတာတွေမှာလည်း ဒီသဘောပင်ဖြစ်ပါတယ်။

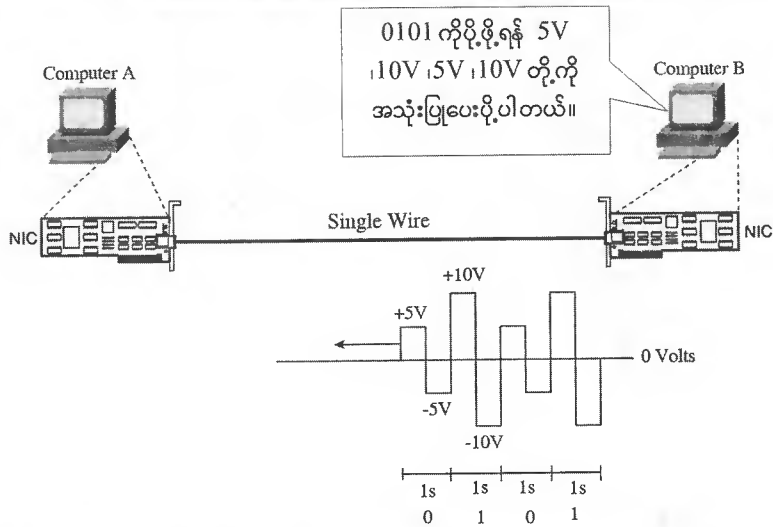


ပုံ (2.1)

ဥပမာ ကွန်ပျူတာ B ဘက်မှ Microsoft Word ဖြင့် ရေးထားသော file တစ်ခုကို ကွန်ပျူတာ A ဘက်က ယူသုံးမယ်ဆိုပါစို့။ ဒါဆိုရင် ကွန်ပျူတာ A ထဲမှာ Microsoft Word ကို install လုပ်ထားမှသာ ၎င်း file ကို အသုံးပြု၍ရမည်ဖြစ်ပါတယ်။ သဘောကတော့ file ၏ format ကိုနားလည်သော program သည် ကွန်ပျူတာ နှစ်လုံးစလုံးမှာ ရှိဖို့လိုခြင်းဖြစ်ပါတယ်။

file တွေဆိုတာကအမှန်တကယ်တော့ bit လို့ခေါ်တဲ့ binary number 0 (သို့) 1 တို့ဖြင့် ဖွဲ့စည်းထားခြင်းဖြစ်ပါတယ်။ ဒါကြောင့် file transfer လုပ်တယ်ဆိုတာကလည်း ကွန်ပျူတာတစ်လုံးမှ bit တွေကို အခြားကွန်ပျူတာဆီသို့ပေးပို့ခြင်းမျှသာ ဖြစ်ပါတယ်။ ဒီနေရာမှာ အရေးကြီးလာတာက ပေးပို့သူနှင့် လက်ခံသူတို့ကြားမှာ နားလည်မှုတွေ လိုက်နာရမယ့်စည်းမျဉ်းစည်းကမ်းတွေ ရှိလာပါတယ်။ ဥပမာအနေနှင့် NIC တစ်ခုစီ တပ်ဆင်ထားပြီး cable တစ်ချောင်းဖြင့်ချိတ်ဆက်ထားသော ကွန်ပျူတာ A နှင့် B တို့သည် အချက်အလက် data တွေကို ဘယ်လိုဖလှယ်ကြသလဲဆိုတာကို ကြည့်ရအောင်။

ကွန်ပျူတာ A ထဲမှ NIC သည်ပို့လိုတဲ့ bit တွေကိုဦးအားတစ်ခုရှိသော electric signal များအဖြစ် ပြောင်းပြီး ချိတ်ဆက်ထားသော cable ပေါ်မှတစ်ဆင့် ကွန်ပျူတာ B ထံသို့ transmit လုပ်ကြရပါတယ်။ အခြားတစ်ဖက်ကွန်ပျူတာ B ထဲမှ NIC သည်ရောက်လာတဲ့ electric signal များကို bit အဖြစ်သို့ပြန်ပြောင်းယူရပါတယ်။ electric signal မှ bit အဖြစ်သို့ တစ်ဖန် bit မှ electric signal အဖြစ်သို့ပြန်အလှန်ပြောင်းလဲခြင်းလုပ်ငန်းစဉ်ကို encode လုပ်တယ်လို့ခေါ်ပါတယ်။ အဲဒီလို တစ်ဖက်က transmit လုပ်လိုက်သော bit တွေကို အခြားတစ်ဖက်က လက်ခံယူနိုင်ကြရန်အတွက် NIC တို့ကြားမှာ standard (ဝါ) set of rule အချို့ကို နားလည်သဘောပေါက်ထားဖို့လိုပါတယ်။



ပုံ (2.2)

ဥပမာဆိုရင်ကွန်ပျူတာ B မှ NIC သည် binary 0 ကို 5V၊ binary 1 ကို 10V အဖြစ် transmit လုပ်လိုက်တယ်ဆိုပါစို့။ အကယ်၍များလက်ခံမည့် ကွန်ပျူတာ A မှ NIC အနေနှင့် binary 0 သည် 2V၊ binary 1 အတွက် 4V ဖြစ်တယ်လို့များ နားလည်ပြီးစောင့်ဆိုင်းနေမယ်ဆိုရင် ဘယ်လိုမှ မဖြစ်နိုင်ပါဘူး။ ဘာဖြစ်လို့လဲဆိုတော့ ကွန်ပျူတာ A သည်ရောက်လာတဲ့ electric signal တွေကို bit အဖြစ် မှန်မှန်ကန်ကန် ပြန်ဆိုနိုင်စွမ်းမရှိသောကြောင့် ဖြစ်ပါတယ်။ ဒါကြောင့် ဝို့ဘတ်က binary 0 သည် 5V၊ binary 1 သည် 10V ဖြစ်တယ်ဆိုရင် အခြားတစ်ဖက်ကလည်း အဲဒီ standard အတိုင်း (ဝါ) rule အတိုင်း နားလည်သဘောပေါက်မှု ရှိဖို့လိုအပ်ပါတယ်။

ဖော်ပြပါပုံ (2.2) မှာဆိုရင် ကွန်ပျူတာ A မှ B ထံသို့ 0101 (4bit) ဆိုတဲ့ binary number ကို ပို့လိုပါတယ်။ ဒါကြောင့် 5V၊ 10V၊ 5V နှင့် 10V တို့ကို အစဉ်လိုက် transmit လုပ်ရပါတယ်။ cable ၏ အခြားတစ်ဖက်မှာရှိတဲ့ ကွန်ပျူတာ B သည်လည်း 5V သည် "0"၊ 10V သည် "1" ဆိုတဲ့ တူညီသည့် encoding rule ကို သုံးပြီး ရောက်လာတဲ့ electric signal တွေကို ဘာသာပြန်ယူမှသာလျှင် ကွန်ပျူတာ A မှပို့လိုက်တာ 0101 ဖြစ်တယ်ဆိုတာကို နားလည်သိရှိနိုင်မှာ ဖြစ်ပါတယ်။

Network Speed

ဒီနေရာမှာ network speed အကြောင်းကို အနည်းငယ် ရှင်းပြလိုပါတယ်။ ရှေ့မှာဖော်ပြခဲ့သလို ဘယ်လောက် ဝိုအားရှိတဲ့ electric signal သည် 0 (သို့) 1 ဖြစ်တယ်ဆိုတဲ့ encoding rule ကို နားလည် နိုင်ကြရုံနှင့် data တွေကို မှန်မှန်ကန်ကန် ပေးပို့ရယူနိုင်ခြင်း မရှိသေးပါဘူး။ cable ပေါ်မှာ bit တွေကို တစ်စက္ကန့် လျှင်ဘယ်လောက်နှုန်း (rate) ဖြင့် transmit လုပ်ကြမယ်ဆိုတာကို နှစ်ဖက်စလုံးက သဘောတူလက်ခံ ကြရပါတယ်။

ပုံတွင်ကြည့်ပါ။ ကွန်ပျူတာ B သည် bit တွေကို transmit လုပ်တဲ့နေရာမှာ 0 သို့မဟုတ် 1 အား ရည်ညွှန်းထားတဲ့ ဝိုအားကို တစ်စက္ကန့်စီမှာ တစ်ခါပြောင်းပြီး ပေးပို့ပါတယ်။ အလားတူပင် ကွန်ပျူတာ A ဘက်မှာလည်း ဝိုအား (ဝါ) electrical signal တွေကို တစ်စက္ကန့်တိုင်းမှာ တစ်ခါဖမ်းယူတိုင်းတာပြီး 0 (သို့) 1

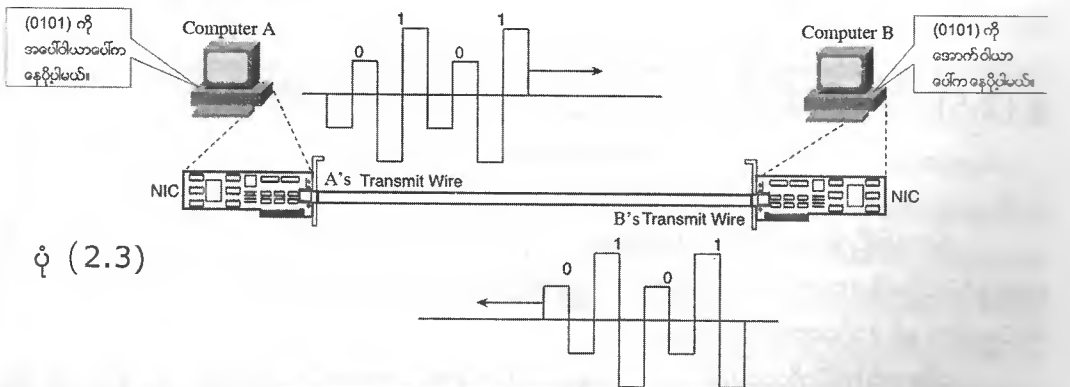
အဖြစ်သို့ ပြန်ယူရပါတယ်။ ဆိုရရင် ပို့တဲ့ဘက်က တစ်စက္ကန့်မှာ 1 bit ပို့ရင် လက်ခံတဲ့ ဘက်ကလည်း တစ်စက္ကန့်မှာ 1 bit နှုန်းဖြင့်ဖမ်းယူရပါတယ်။ ဒါဆိုရင် အဲဒီ ကွန်ပျူတာ နှစ်လုံးကြားမှာ လုပ်ဆောင်တဲ့ အမြန်နှုန်း network speed သည် 1bit per second (1bps) ဖြစ်ပါတယ်။ ဒါကြောင့် တစ်စက္ကန့်မှာ 10bit နှုန်းဖြင့် အပို့အယူလုပ်ကြမယ်ဆိုရင် network speed သည် 10bps ဖြစ်ပါလိမ့်မယ်။

အကယ်၍များ ဖော်ပြပါ ကွန်ပျူတာ A နှင့် B တို့ကြားမှာ တူညီတဲ့ transmission speed မရှိဘူး ဆိုလျှင် bit [0 (သို့) 1] တွေကို ပေးပို့ရယူနိုင်ကြမည်မဟုတ်ပါ။ ဥပမာဆိုရရင် ကွန်ပျူတာ B သည် သူ့ကိုယ်သူ 10bps နှုန်းဖြင့်လုပ်ဆောင်နိုင်တယ်လို့ သိထားတယ်ဆိုပါစို့။ တစ်စက္ကန့်ရဲ့ဆယ်ပုံတစ်ပုံမှာ 1bit ကို transmit လုပ်မယ်ပေါ့။ ဒီနေရာတွင် ကွန်ပျူတာ A ဘက်မှာက 20bps နှုန်းဖြင့်လုပ်ဆောင်မယ်ဆိုပါတော့။ ဒါဆိုရင် ကွန်ပျူတာ A သည် တစ်စက္ကန့်ရဲ့အပုံ ၂၀ပုံ ၁ပုံတိုင်းမှာ ဝင်လာတဲ့ signal တွေကို တိုင်းတာဖမ်းယူမှာ ဖြစ်ပါတယ်။ ဒါကြောင့် ကွန်ပျူတာ B မှ 10 bit ပို့လိုက်တယ်လို့ သိထားချိန်တွင် တစ်ဖက်ကွန်ပျူတာ A ကတော့ 20bit လက်ခံရရှိပြီလို့ ထင်နေပါလိမ့်မယ်။

bps (bit per second) ဆိုတဲ့ အခေါ်အဝေါ်သည် network တွေရဲ့လုပ်ဆောင်နိုင်မှု speed ကို ရည်ညွှန်းခြင်းဖြစ်ပါတယ်။ b သည် byte (8bit) မဟုတ်ဘူးဆိုတာကို အထူးသတိပြုစေလိုပါတယ်။ တကယ့် လက်တွေ့နယ်ပယ်မှာတော့ LAN တွေရဲ့ speed သည် ပုံမှန်အားဖြင့် အနည်းဆုံး 10mbps (Million bit per second) ရှိပါတယ်။

📌 The Need for a Two Lane

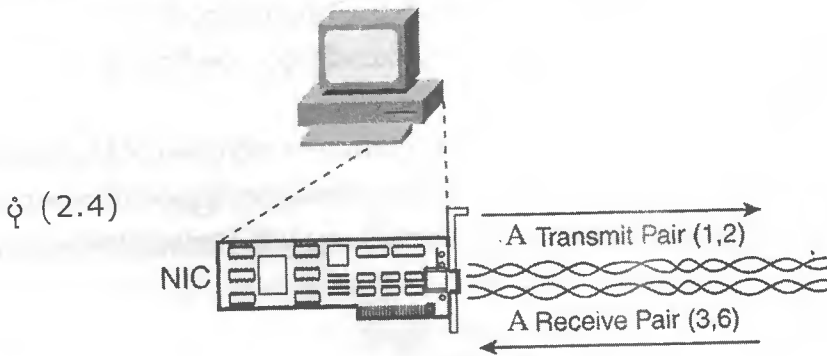
ရှေ့မှာဖော်ပြခဲ့တဲ့ပုံ (2.2) သည် ကွန်ပျူတာ B မှ A ထံသို့ electric signal များပေးပို့ကြပုံဖြစ်ပါတယ်။ အဲဒီပုံအရဆိုရင် ကွန်ပျူတာ A နှင့် B တို့သည် signal တွေကို တစ်ချိန်တည်း တစ်ပြိုင်နက် အပြန်အလှန် ပေးပို့ရန်မဖြစ်နိုင်ပါဘူး။ ဘာဖြစ်လို့လဲဆိုတော့ ဝါယာတစ်ချောင်းပေါ်မှာ တစ်ပြိုင်နက် transmit လုပ်ကြမယ်ဆိုရင် signal တွေတစ်ခုနှင့်တစ်ခုထပ်ကုန်ပြီး ပုံသဏ္ဍာန် ပျက်ယွင်းကာ ကွန်ပျူတာနှစ်လုံး စလုံးတို့သည် တစ်ဖက်မှဘာတွေပို့နေသလဲဆိုတာကို နားမလည်နိုင်တော့ပါဘူး။ အဲဒီပြဿနာကို ပြေလည်စေရန်အတွက် ကွန်ပျူတာ A မှ B သို့၊ တစ်ဖန် ကွန်ပျူတာ B မှ A သို့ဆိုပြီး ဝါယာနှစ်ချောင်းရှိဖို့လိုအပ် ပါတယ်။ ပုံ (2.3) အရမှသာလျှင် ကွန်ပျူတာ A နှင့် B တို့သည် တစ်ချိန်တည်း တစ်ပြိုင်နက် transmit/receive လုပ်နိုင်ကြပါလိမ့်မယ်။



ပုံ (2.3)

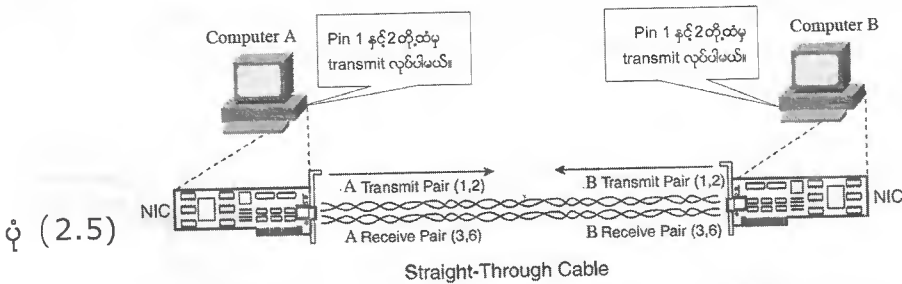
ယနေ့ network တွေမှာဆိုရင် ကွန်ပျူတာတွေထဲမှာ NIC တစ်ခုစီစိုက်သွင်းတပ်ဆင်ပြီးတစ်လုံးနှင့် တစ်လုံးကို twisted pair cable ဖြင့်ချိတ်ဆက်အသုံးပြုမှုသည် အများဆုံးဖြစ်ပါတယ်။

twisted pair (cat 5) cable ရဲ့အတွင်းမှာ ဝါယာကြိုးမျှင် ရှစ်ချောင်းပါရှိပါတယ်။ NIC တို့တွင် ချိတ်ဆက်တပ်ဆင်နိုင်ရန်အတွက် cable အစွန်းတစ်ဖက်စီတွင် RJ-45 connector တစ်ခုစီ တပ်ဆင်ရပါတယ်။ RJ-45 connector တွင် ဝါယာချောင်းအတွက် pin ခု ပါရှိပါတယ်။ NIC တွေသည် cable ပေါ်မှာ data တွေပေးပို့ဖို့ရန် RJ-45 ရဲ့ pin 1 နှင့် pin 2 ကိုအသုံးပြုပါတယ်။ data တွေကို receive လုပ်ရန် အတွက်ကတော့ pin 3 နှင့် 6 ကို အသုံးပြုပါတယ်။ (ဝါယာ ချောင်းပါသော်လည်း ဝါယာ လေးချောင်းကိုသာ အသုံးပြုတယ်ဆိုတာ သတိချပ်စေလိုပါတယ်။)



Straight through Vs Crossover Cable

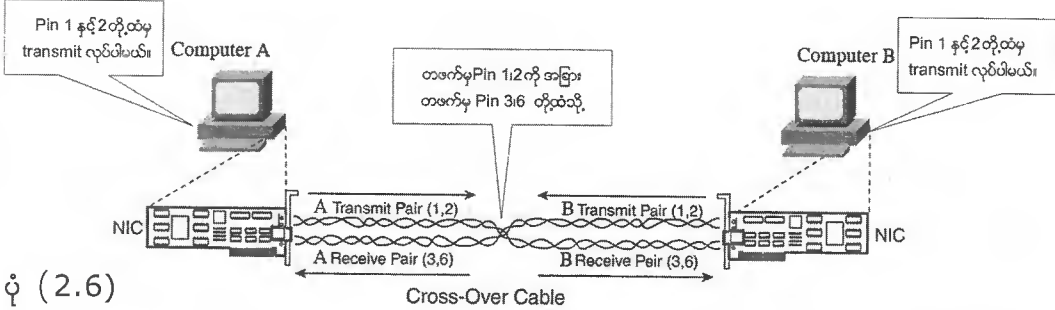
အကယ်၍များ NIC နှစ်ခုကြားမှာ ဆက်သွယ်ထားတဲ့ cabling မှန်ကန်မှုမရှိဘူးဆိုရင် ၎င်း NIC နှစ်ခုတို့သည် အပြန်အလှန် communication လုပ်နိုင်ကြမည်မဟုတ်ပါ။ အောက်ဖော်ပြပါပုံ (2.5) ကို ကြည့်ပါ။ NIC နှစ်ခုတို့ရဲ့ pin 1 အချင်းချင်း၊ pin 2 အချင်းချင်း တိုက်ရိုက်ချိတ်ဆက်ထားတာကို တွေ့ရပါမယ်။ အဲဒီလို ဆက်သွယ်ထားပုံအရ ကြည့်မယ်ဆိုရင် ၎င်း cable သည် straight-through ဖြစ်ပါတယ်။



ကောင်းပြီခါဆိုရင် ပုံ(2.5) မှာ မြင်ရတဲ့အတိုင်းပင် NIC နှစ်ခုစလုံးသည် twisted pair cable ရဲ့ pin 1 နှင့် 2 တို့ပေါ်မှ transmit လုပ်ကြမှာဖြစ်သည့်အတွက် တစ်ဖက် NIC မှလာတဲ့ signal များသည် တစ်ဖက် NIC မှ pin 1 နှင့် 2 သို့ရောက်ရှိမှာဖြစ်ပါတယ်။

သို့သော် NIC တို့သည် pin 1 နှင့် 2 မှနေ၍ signal များကို receive မလုပ်ပါဘူး။ pin 1 နှင့် 2 တို့သည်

transmit လုပ်ရုံသက်သက် ဖြစ်သလို pin3 နှင့် 6 တို့သည်လည်း receive လုပ်ရုံသက်သက်ဖြစ်ပါတယ်။ ဒါကြောင့်ကွန်ပျူတာ နှစ်လုံးစလုံးသည် transmit တော့လုပ်မယ် ဒါပေမယ့် မည်သည့် data မှ ရရှိမည် မဟုတ်ပါ။ဒါဆိုရင် ကွန်ပျူတာနှစ်လုံး အပြန်အလှန် communicate လုပ်နိုင်စေရန် ဘာတွေလုပ်ဆောင် ပေးဖို့လိုမလဲဆိုတာမျိုး မေးဖို့ရှိလာနိုင်ပါလိမ့်မယ်။ ခက်ခက်ခဲခဲ ဆန်းဆန်း ပြားပြားလုပ်ပေးဖို့ မလိုပါဘူး။ straightအစား cross cableကို ပြောင်းသုံးလိုက်ရုံဖြစ်ပါတယ်။ cross-over cableသည် ကွန်ပျူတာ A၏ NICမှ pin1 သည် ကွန်ပျူတာ B မှ NIC၏ pin3 သို့လည်းကောင်း၊ pin2သည် pin6 သို့၊ pin3သည် pin1 သို့၊ pin6သည် pin2 သို့အသီးသီးချိတ်ဆက်ပေးပါတယ်။ သို့မှသာ တစ်ဖက် pin1 နှင့် 2 မှလာတဲ့ signal တွေသည် အခြားတစ်ဖက် pin3 နှင့် 6 သို့ရောက်မှာဖြစ်ပါတယ်။



ပုံ (2.6)

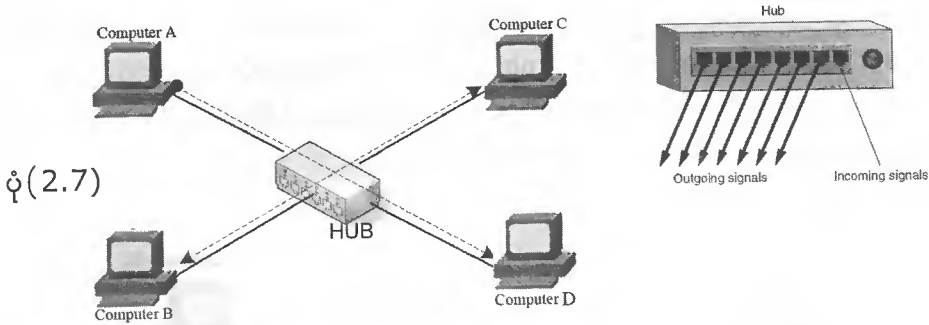
ဤနေရာတွင်မှဆက်ပြီး network တွေမှာ central device လို့ခေါ်တဲ့ hub တွေ ဘာကြောင့် အရေးပါသလဲဆိုတာနှင့် ကွန်ပျူတာတွေနှင့်ချိတ်ဆက်တဲ့နေရာမှာဘာကြောင့် straight-through cable ကို သုံးရသလဲ ဆိုတာကို ဆက်လက်ရှင်းလင်းသွားပါမယ်။

Why use central Device

ကွန်ပျူတာနှစ်လုံးကို cross cable သုံးပြီး တိုက်ရိုက်ချိတ်ဆက်သလိုမျိုး၊ ကွန်ပျူတာ ဆယ်လုံးကို cross cable တို့ဖြင့် network တစ်ခုဖြစ်အောင် တည်ဆောက်မယ်ဆိုရင် ဘယ်လိုအခက်ခဲတွေ ကြုံလာနိုင် မလဲ။ သေချာတာတစ်ခုကတော့ ကွန်ပျူတာတစ်လုံးစီမှာ NIC တွေအများကြီးလိုအပ်မှာဖြစ်သလို cross-over cable တွေလည်း အများကြီးလိုပါလိမ့်မယ်။ ဆိုရရင် ကွန်ပျူတာတစ်လုံးစီသည် ကျန်ကွန်ပျူတာ ကိုးလုံး တို့နှင့်ချိတ်ဆက်ဖို့ရန်အတွက် ကွန်ပျူတာတစ်လုံးစီမှာ NIC ကိုးခုတပ်ဆင်ဖို့ရန်နှင့် ချိတ်ဆက်ဖို့ရန် cross cable ကိုးချောင်းလိုအပ်မှာဖြစ်ပါတယ်။ ထိုအရေအတွက်ရှိတဲ့ NIC တွေကို တပ်ဆင်ဖို့ရန် ကွန်ပျူတာထဲမှာ နေရာလွတ်မရှိပါဘူး။ ကွန်ပျူတာအရေအတွက် ပိုများလာမယ်။ ရာထောင်ချီလာမယ်ဆိုရင် အဲဒီနည်းလမ်း အတိုင်း network တစ်ခုတည်ဆောက်ဖို့ရန် ဖြစ်နိုင်မဖြစ်နိုင် စဉ်းစားစရာတောင် လိုမယ် မထင်တော့ပါ။

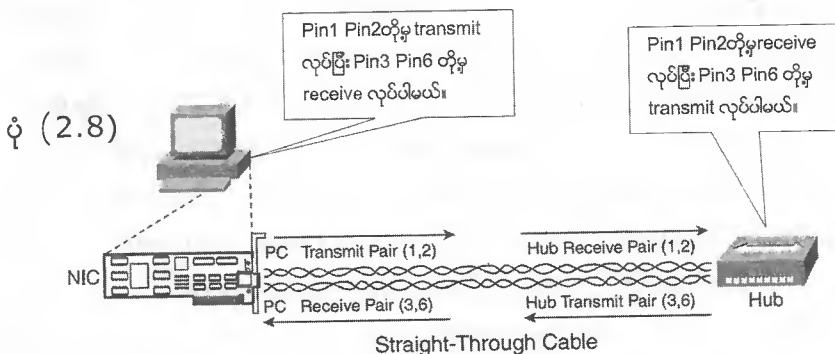
ဒီပြဿနာကို ပြေလည်စေမည့် cable တစ်ချောင်း၊ NIC တစ်ခုတည်းနှင့် network တွင်းမှာရှိတဲ့ ကျန်ကွန်ပျူတာအားလုံးတို့ကို ချိတ်ဆက်နိုင်တဲ့ အခြားနည်းလမ်းတစ်ခုရှိပါတယ်။ အဲဒါကတော့ hub ကိုအသုံး ပြုခြင်းဖြစ်ပါတယ်။ hub တစ်ခုရဲ့ လုပ်ဆောင်မှုတွေအများကြီး ရှိပါတယ်။ ဒါပေမယ့် အဓိက လုပ်ဆောင်မှုကတော့ port တစ်ခုကနေ ဝင်လာတဲ့ signal တွေကို အခြား port မှာတပ်ထားတဲ့ device

(ကွန်ပျူတာ၊ ပရင်တာ) တွေထံသို့ တစ်ပြိုင်နက်ဖြန့်ဝေပေးပါတယ်။ ပုံ (2.7) တွင်ကြည့်ပါ။ ကွန်ပျူတာ A မှပေးပို့လိုက်တဲ့ data တွေ hub ထံသို့ရောက်တဲ့အခါ hub သည် ကွန်ပျူတာ A မှပို့သမျှကို ကွန်ပျူတာ B၊ C၊ D တို့ထံသို့တစ်ပြိုင်နက်ဆက်လက်ပို့ဆောင်ပါတယ်။



အောက်ဖော်ပြပါ ပုံ (2.8) ကတော့ hub နှင့် ကွန်ပျူတာတို့အကြားမှာရှိတဲ့ cabling ဖြစ်ပါတယ်။ ကွန်ပျူတာဘက်က NIC တို့မှာဆိုရင် pin1 နှင့် 2 တို့သည် data transmit လုပ်ရန်ဖြစ်ပြီး pin3 နှင့် 6 တို့ကတော့ data receive လုပ်ရန်ဖြစ်ပါတယ်။ hub တွေကတော့ NIC တို့နှင့် ဆန့်ကျင်ဘက် ဖြစ်ပါတယ်။ pin1 နှင့် 2 တို့မှ receive လုပ်မှာဖြစ်ပြီး pin3 နှင့် 6 တို့မှ transmit လုပ်မှာဖြစ်ပါတယ်။ ဒါကြောင့် ကွန်ပျူတာနှင့် hub တို့ကြားမှာ အသုံးပြုရမယ့် cable သည် straight ဖြစ်မှသာ အလုပ်လုပ်နိုင်မှာ ဖြစ်ပါတယ်။

- hub တွေရဲ့ သဘာဝကို ပုံဖော်ကြည့်မယ်ဆိုရင်
- 1) pin1 နှင့် 2 တို့မှ receive လုပ်ပါတယ်။
 - 2) port တစ်ခုကနေ လက်ခံရရှိတဲ့ signal တွေကို အခြား port အားလုံးဆီသို့ (signal ဝင်လာသော port မှလွဲ၍) ဖြန့်ဝေပေးပါတယ်။
 - 3) ဖြန့်ဝေပေးပို့တဲ့နေရာမှာ ကွန်ပျူတာတွေ လက်ခံရယူနိုင်အောင် pin3 နှင့် 6 တို့မှ transmit လုပ်ပါတယ်။



Recognize and Recover Error

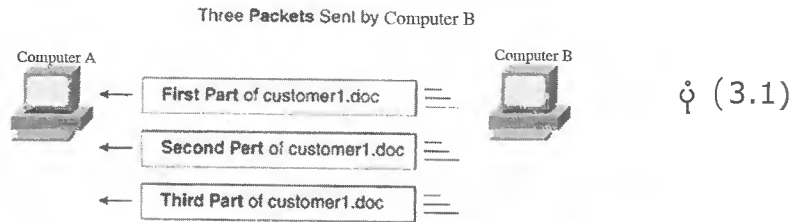
ရှေ့က chapter (2) မှာဖော်ပြခဲ့တာကတော့ data ပေးပို့ရယူခြင်းများကို လုပ်ဆောင်ကြတဲ့နေရာမှာ လိုက်နာရတဲ့ networking standard များစွာရှိတဲ့အထဲက အချို့ဖြစ်ပါတယ်။ ကွန်ပျူတာနှစ်လုံးအောင်အောင်မြင်မြင် communicate လုပ်နိုင်ကြရန်အတွက် လိုက်နာရမည့် အခြားသော standard များစွာရှိပါသေးတယ်။ ဥပမာဆိုရရင် ကွန်ပျူတာ B မှ data တွေကိုပေးပို့လိုက်တယ်။ ဒါပေမယ့် ကွန်ပျူတာ A ဘက်ကအပြည့်အဝလက်ခံမရရှိပဲ data အချို့ပျောက်ဆုံးနေတယ်ဆိုပါတော့။ အဲဒီဖြစ်စဉ်မှာ ကွန်ပျူတာ A နှင့် B တို့သည် ဘယ်လို စည်းမျဉ်းစည်းကမ်းတွေကို လိုက်နာပြီး data အားလုံး ပြည့်ပြည့်စုံစုံ မှန်မှန်ကန်ကန် ရရှိအောင် လုပ်ဆောင်ကြသလဲဆိုတာကို ကြည့်ရအောင်။

network အတွင်း ကွန်ပျူတာ တစ်လုံးမှ တစ်လုံးသို့ data တွေပေးပို့တဲ့နေရာမှာ bit တွေကို အရေအတွက် တစ်ခုဖြင့် အုပ်စုဖွဲ့ပြီးပေးပို့ကြခြင်းဖြစ်ပါတယ်။ ဥပမာ 1MB ရှိတဲ့ file ကို network ပေါ်မှာ ပို့မယ်ဆိုပါစို့။ 1MB တွင် အကြမ်းမုန်းအားဖြင့် bit အရေအတွက် ၈ သန်းခန့်ရှိပါတယ်။

1MB	=	1000kB
1000kB	=	1,000,000B
1,000,000B	=	8,000,000bit

file transfer လုပ်ရန်အတွက် အဲဒီ bit အရေအတွက် ၈ သန်းစလုံးကို ဒီအတိုင်းစီတန်းပြီး ဆက်တိုက်ပေးပို့ခြင်း မဟုတ်ပါဘူး။ အရေအတွက်တစ်ခုဖြင့် စိတ်ပိုင်းအုပ်စုဖွဲ့ပြီးပေးပို့ခြင်းဖြစ်ပါတယ်။ အဲဒီအရေအတွက်တစ်ခုပါတဲ့ bit အုပ်စုတစ်ခုကို packet လို့ခေါ်ပါတယ်။ အနည်းငယ်ထပ်ပြီး အသေးစိတ်ဆိုရရင် file တစ်ခု၏ပထမအပိုင်းသည် ပထမ packet၊ ဒုတိယအပိုင်းသည် ဒုတိယ packet အစရှိသဖြင့် file အရွယ်အစားကြီးရင် ကြီးသလို packet တွေ များလာမယ်ပေါ့။

Data Transmission Using Packets



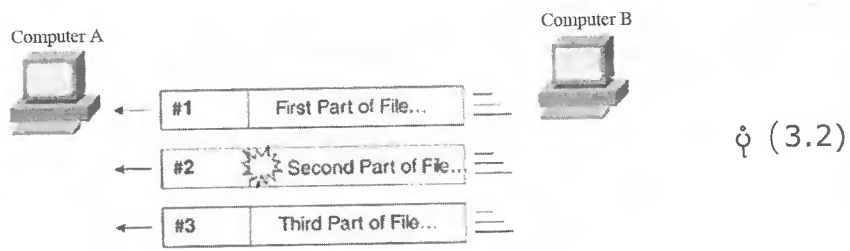
ဒီနေရာမှာ ဘာကြောင့် bit တွေကို packet တွေအဖြစ် အုပ်စုဖွဲ့ပြီး ပေးပို့ ကြသလဲဆိုတာကို အနည်းငယ်ရှင်းပြလိုပါတယ်။ ဥပမာ ရန်ကုန်ကနေ မန္တလေးကို နို့မှုန့် အထုပ်တစ်သိန်းပို့မယ်ဆိုပါတော့။ ဒါဆိုရင် အဲဒီအထုပ်တစ်သိန်းလုံးကို ပုံးတစ်ပုံးထဲမှာ စုထည့်ပြီး ပို့မယ်ဆိုရင် ဖြစ်နိုင်ပါ့မလား။ လုံးဝမဖြစ်နိုင်ပါလို့ဆိုရပါမယ်။ သို့သော် အထုပ် ၁၀၀ ကို တစ်ပုံးနှုန်းနှင့် ပုံး ၁၀၀၀ ခွဲပြီး ထည့်မယ်။ ပြီးရင် ပို့ရမယ် လိပ်စာကို ပုံး

အားလုံးပေါ်မှာတူအောင်ရေးပြီး ပို့မယ်ဆိုရင် အတင်အချ အသယ်အပို့ အစရှိတဲ့ စီမံခန့်ခွဲမှု ကိစ္စတွေလွယ်ကူစေပြီး ရည်ရွယ်ရာ ခရီးလမ်းဆုံးသို့ ရောက်အောင် ပို့နိုင်ပါလိမ့်မယ်။

packet တွေကို ခွဲပြီး ပို့ရခြင်းသည်လည်း ဒီသဘောပင်ဖြစ်ပါတယ်။ ဘီလီယံနဲ့ချီသော bit တွေကို တစ်စုတစ်စည်းထဲ ဆက်တိုက်ပို့မယ့်အစား packet တွေအဖြစ် ခွဲပြီး ပို့ခြင်းအားဖြင့် file transfer လုပ်တဲ့ နေရာမှာ အားသာချက်များ ရရှိစေပါတယ်။ အထူးသဖြင့် အချို့သော packet တွေမှာ error ဖြစ်လာပြီဆိုရင် ၎င်း error တွေကို ပြေလည်အောင် ဖြေရှင်းတဲ့နေရာမှာ များစွာ လွယ်ကူစေပါတယ်။

ဒီနေရာမှာ ဘာကြောင့်၊ ဘယ်လို error တွေဖြစ်သလဲဆိုတာကို အနည်းငယ်ရှင်းပြလိုပါတယ်။ NIC ၂ခုစလုံးသည် 5V ကို binary "0"၊ 10V ကို binary "1" လို့ နားလည်ထားတယ်ဆိုပါစို့။ ဒါဆိုရင် ပို့တဲ့ NIC ဘက်ကတော့ သူနားလည်လက်ခံထားတဲ့အတိုင်း 5V၊ 10V signal တို့ကို ထုတ်လွှတ်မှာဖြစ်ပါတယ်။ အကယ်၍ များအကြောင်းတစ်ခုခုကြောင့် လက်ခံတဲ့ NIC ဘက်ရောက်တဲ့အခါ 5V သည် 7.5V၊ 10V သည် 15V သို့ အသီးသီး ပြောင်းလဲသွားခဲ့မယ်ဆိုရင် ဘာတွေဖြစ်လာနိုင်မလဲ။ သေချာတာကတော့ ၎င်း 7.5V နှင့် 15V တို့ကို လက်ခံရရှိသည့် NIC ဘက်မှ နားလည်သဘောပေါက်နိုင်စွမ်းမရှိသည့်အတွက် bit များအဖြစ်သို့ ပြန်ဆို၍ မရနိုင်ပါဘူး။

အဲဒီလို transmission error တွေကို electrical interference လို့ခေါ်တဲ့ noise များကြောင့် cable အတွင်းမှာ ဖြတ်သန်းနေတဲ့ signal များ ပုံသဏ္ဍန်ပျက်ယွင်းသွားတဲ့ အခါမျိုးတွေမှာ တွေ့ရတတ်ပါတယ်။ အထူးသဖြင့် network cable အနီးအနားတွင် ဖုန်စုပ်စက် (သို့) မော်တာတွေကို အသုံးပြုလိုက်မိတဲ့ အခါမျိုးတွေမှာ cable အတွင်း စီးဆင်းနေတဲ့ လျှပ်စစ်ဗို့အားကို ပြောင်းလဲစေပြီး packet error များ ဖြစ်ပေါ်စေတတ်ပါတယ်။

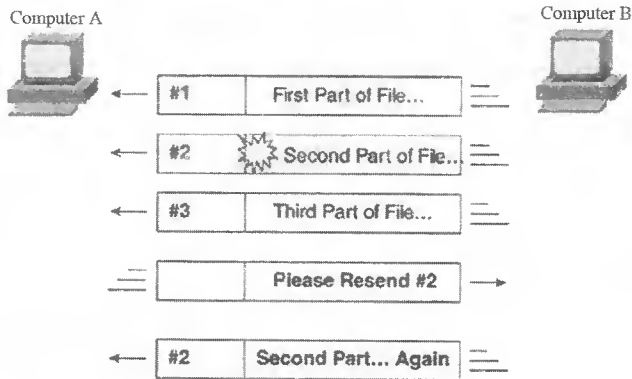


ဖော်ပြပါပုံ(3.2) တွင်ကြည့်ပါ။ ကွန်ပျူတာ A သည် ကွန်ပျူတာ B မှ ပို့လိုက်တဲ့ packet ၃ခုစလုံးကို လက်ခံရရှိပါတယ်။ ဒါပေမယ့် ဒုတိယ packet ထဲမှာ အမှားအယွင်းရှိနေသည့်အတွက် နားမလည်နိုင်သော bit အချို့ပါဝင်နေပါတယ်။ ဥပမာအနေနှင့် packet ၃ခုပေါင်းသည် စာပိုဒ် သုံးပိုဒ်ပါသော text file တစ်ခုဖြစ်တယ်ဆိုပါစို့။ ပထမ packet ထဲမှာ ပထမစာပိုဒ်၊ ဒုတိယ packet ထဲမှာ ဒုတိယစာပိုဒ်၊ တတိယ packet ထဲမှာ တတိယစာပိုဒ်လို့ စဉ်းစားကြည့်ရအောင်။ ဒါဆိုရင် ကွန်ပျူတာ B ဘက်မှာ ဒုတိယစာပိုဒ် မပါသော text tile တစ်ခုအဖြစ် ရှာလားလို့ မေးစရာဖြစ်လာနိုင်ပါလိမ့်မယ်။ အဲဒီလိုတော့ မဟုတ်ပါဘူး။

packet အားလုံးကို အမှားအယွင်းမရှိ စုံစုံလင်လင်ရရှိစေအောင် ဖြေရှင်းတဲ့ နည်းလမ်းတစ်ခု ရှိပါတယ်။ အဲဒါကတော့ ပေးပို့သည့် ကွန်ပျူတာ နှင့် လက်ခံရယူမည့် ကွန်ပျူတာတို့ကြားမှာ တူညီတဲ့ net- working protocol တစ်ခုကို အသုံးပြုကြရန်ပင်ဖြစ်ပါတယ်။ ပထမဦးစွာ ပေးပို့မည့်ကွန်ပျူတာ B အနေနှင့် packet တွေကို နံပါတ်စဉ်တပ်ရပါတယ်။ packet # 1 | packet # 2 | packet # 3 ပေါ့..

ဤတွင်မှ ကွန်ပျူတာ A ဘက်ကလည်း ကွန်ပျူတာ B ဘက်မှ တပ်ပေးလိုက်တဲ့ နံပါတ်စဉ် တွေကိုဖတ်ပြီး bit error ပါလာသည့် packet သည် packet # 2 ဖြစ်တယ်ဆိုတာကို သိရှိပါလိမ့်မယ်။ အဲဒီလို ကွန်ပျူတာ A ဘက်မှ ဘယ် packet လဲဆိုတာ အတိအကျသိမှသာလျှင် " ကွန်ပျူတာ B ရေ ငိုကို ဒုတိယ packet ပြန်ပို့ပေးပါဦး" ဆိုတာမျိုးပြန်လည် request လုပ်နိုင်မှာဖြစ်ပါတယ်။ သည်အခါမှ ကွန်ပျူတာ B ဘက်ကလည်း မိမိပို့လိုက်သမျှထဲက ဒုတိယ packet သည် လမ်းမှာ error ဖြစ်သွားပြီ ဆိုတာသိရှိပြီး ၎င်းဒုတိယ packet တစ်ခုတည်းကိုသာ ကွန်ပျူတာ A ထံသို့နောက်တစ်ကြိမ်ပြန်ပို့ပေးပါတယ်။ ဤနည်းဖြင့် ပို့လိုသမျှ packet အားလုံးတို့ကို တစ်ဖက်လက်ခံမည့် သူထံသို့ အောင်အောင် မြင်မြင် ရောက်ရှိအောင် လုပ်ဆောင်ကြပါတယ်။

A Simple Protocol for Error Recovery



ပုံ (3.3)

ဤဖြစ်စဉ်ကို ကြည့်မယ်ဆိုရင် အပိုင်း ၂ပိုင်းပါဝင်နေတာကို တွေ့ကြရပါလိမ့်မယ်။ ပထမအပိုင်းက error ဖြစ်နေတာဘယ် packet ဆိုတာကို အတိအကျသိရှိနိုင်အောင် လုပ်ခြင်းဆိုတဲ့ 'recognize' ဖြစ်ပါတယ်။ ဒုတိယအပိုင်းကတော့ bit error ကြောင့် ဆုံးရှုံးသွားတဲ့ packet ကို အစားပြန်ရအောင် လုပ်ဆောင်ခြင်းဆိုတဲ့ 'recover' ဖြစ်ပါတယ်။ recognize ဖြစ်ဖို့ရန် အရေးကြီးဆုံးက ပေးပို့သူ (ကွန်ပျူတာ B) ဘက်က နံပါတ်စဉ် တပ်ဖို့လိုသလို၊ အဲဒီနံပါတ်စဉ်ကို လက်ခံမည့်သူ (ကွန်ပျူတာ A) ဘက်ကလည်း နားလည်ဖို့ လိုပါတယ်။

ဥပမာ ရန်ကုန်ကနေ မန္တလေးကို အထုပ်သုံးထုပ်ပို့မယ်ဆိုပါတော့။ အထုပ်တွေပေါ်မှာ တစ်၊ နှစ်၊ သုံး လို့ မြန်မာလို ရေးပြီး ပို့လိုက်တယ်ပေါ့။ ဒါဆိုရင် တဖက်မန္တလေးဘက်က လက်ခံမည့်သူသည် မြန်မာစာတတ်မှ သာလျှင် ဘယ်အထုပ်မှာ အပျက်အစီးရှိလာတယ်ဆိုတာကို ပြောပြနိုင်ပါလိမ့်မယ်။ သဘောကတော့ ပေးပို့သူ နှင့် ရယူသူတို့ နားလည်အသုံးပြုတဲ့ ဘာသာစကား တူရမယ်ပေါ့။ ကွန်ပျူတာတွေမှာလည်း ဒီသဘောအတိုင်း ပါဝင်ပေးပို့မည့်ကွန်ပျူတာနှင့် လက်ခံမည့်ကွန်ပျူတာတို့အသုံးပြုသည့် protocol အတူတူပင်ဖြစ်ရပါမယ်။

နောက်တစ်ခါ error recovery လုပ်ငန်းစဉ်ပြီးဆုံးအောင်မြင်ဖို့ error ရှိနေသော packet တစ်ခု ရောက်လာပြီဆိုတာနှင့် ဘယ်လိုဆက်လုပ်ဆောင်ကြမယ်ဆိုတဲ့ လိုက်နာဆောင်ရွက်ရမည့် စည်းမျဉ်း စည်းကမ်းတွေ ရှိပါတယ်။ ဆိုရရင် လက်ခံသူဘက်က error ဖြစ်လာတဲ့ packet ကို ပြန်ပို့ပေးရန် request လုပ်ရမယ်။ အဲဒီ request အရ မူလပေးပို့သူဘက်က နောက်တစ်ကြိမ် ပြန်ပို့ပေးရမယ်ဆိုတာတွေသည် packet error ဖြစ်လာတဲ့အခါ လိုက်နာဆောင်ရွက်ရမယ့် "set of rules" တွေပဲဖြစ်ကြပါတယ်။ အဲဒီ "set of rules" တွေသည် protocol တစ်ခုနှင့်တစ်ခုမတူကြပါဘူး။ အကယ်၍များ တဖက်နှင့်တဖက် အသုံးပြုကြသည့် protocol မတူကြဘူးဆိုရင် ပြန်လည် request လုပ်ရကောင်းမှန်းမသိ၊ အစားပြန်ပို့ ပေးရကောင်းမှန်းမသိ ဖြစ်နေပါလိမ့်မယ်။ ဒါကြောင့် protocol တူမှသာလျှင် အောင်မြင်သော data ပေးပို့မှု တစ်ခုဖြစ်ပါလိမ့်မယ်။

protocol တူရမယ်ဆိုတဲ့ နေရာမှာလည်း protocol ဖြစ်ရင်ပြီးရော သုံးလို့မရပါဘူး။ သူ့နေရာနှင့်သူ အံဝင်ခွင့်ကျဖြစ်တဲ့ protocol ဖြစ်ရပါမယ်။ ဆိုရရင် "set of rules" ပေါ်မူတည်ပြီး protocol ပေါင်းများစွာ ရှိပါတယ်။ အင်တာနက် webpage တွေ ခေါ် ကြည့်တဲ့နေရာမှာ အသုံးပြုရတဲ့ protocol (HTTP)၊ email ပို့တဲ့နေရာမှာ အသုံးပြုတဲ့ protocol (SMTP) အစရှိသဖြင့် အသုံးပြုတဲ့နေရာပေါ်မူတည်ပြီး သုံးရမယ့် protocol တွေကွဲလွဲပါတယ်။ data recovery အတွက်ကို http သုံးလို့မရပါဘူး။ data recovery လုပ်နိုင်တဲ့ protocol - ဥပမာ transmission control protocol (TCP) - ကိုသာ အသုံးပြုရမှာဖြစ်ပါတယ်။ အနှစ်ချုပ် ဆိုရရင် ပေးပို့လိုက်တဲ့ဘက်က TCP ကိုသုံးပြီး ပို့မယ်ဆိုရင် တစ်ဖက် လက်ခံသူဘက်မှာ TCP ရှိမှသာလျှင် ပြည့်စုံအောင် မြင်သော data ပေးပို့မှု တစ်ခုဖြစ်ပါလိမ့်မယ်။

Networking Model

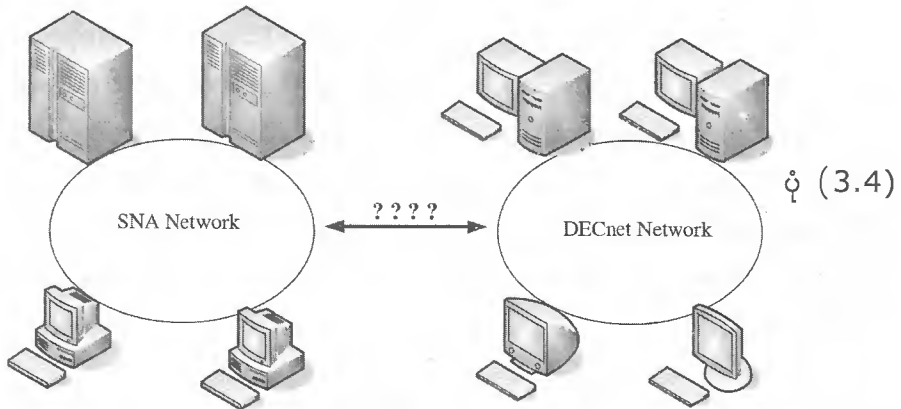
ကွန်ပျူတာတွေကို စုပေါင်း၍ network ချိတ်ဆက်အသုံးပြုခြင်းများကို 1960 ခုနှစ်လောက်ကစခဲ့ပြီး 1970 ဝန်းကျင်မှာတော့ အတော်လေးကို အသုံးများလာခဲ့ပါတယ်။ အဲဒီအချိန်တုန်းကတော့ ယနေ့လိုမျိုး ကြိုက်တဲ့ ကွန်ပျူတာဝယ်ယူပြီး network တစ်ခု တည်ဆောက်လို့ မရပါဘူး။ ဘယ်ကုမ္ပဏီမှ ထုတ်လုပ် ရောင်းချသော ကွန်ပျူတာလဲဆိုတာ အရေးကြီးပါတယ်။ ကုမ္ပဏီတစ်ခုတည်းမှ ထုတ်လုပ်သော ကွန်ပျူတာ အချင်းချင်းသာလျှင် အပြန်အလှန် communicate လုပ်နိုင်ကြပါတယ်။

ဆိုရရင် network ခေတ်ဦးကာလတွေတုန်းက ကွန်ပျူတာ ထုတ်လုပ်ရောင်းချသည့် အဓိက ကုမ္ပဏီကြီး ၂ခုသာရှိပါတယ်။ IBM (International Business Machines) နှင့် DEC (Digital Equipment Corporation) တို့ဖြစ်ပါတယ်။ ထိုကုမ္ပဏီ ၂ခုစလုံးသည် ကွန်ပျူတာတစ်လုံးနှင့်တစ်လုံး အပြန်အလှန် communicate လုပ်စေနိုင်သည့် ကိုယ်ပိုင် networking model တစ်ခုစီကို တီထွင် အသုံးပြုခဲ့ကြပါတယ်။ IBM မှဖန်တီးတီထွင်ထားတဲ့ network model ကို SNA (System Network Architecture) လို့ခေါ်ပြီး၊ DEC မှတီထွင်သော network model ကို DECnet လို့ခေါ်ပါတယ်။

၎င်း networking model ဂရုစလုံးသည် သူ့နည်းသူဟန်နှင့်ကောင်းပါတယ်။ ဒါပေမယ့် အဓိက ပြဿနာကတော့ ထို networking model ဂရုစကို ကိုယ်ပိုင်သီးခြားဟန်တို့ဖြင့် တည်ဆောက်ထားသည့် အတွက်ကြောင့် လုပ်ဆောင်ပုံခြင်းမတူကြပါ။ ဒါကြောင့် IBM ကွန်ပျူတာနှင့် DEC ကွန်ပျူတာတို့သည် communicate မလုပ်နိုင်ကြပါဘူး။ ဥပမာဆိုရရင် တယ်လီဖုန်း handset ထုတ်လုပ်သည့် ကုမ္ပဏီ (Motorola၊ Nokia) မတူတာနှင့် အဆက်အသွယ်လုပ်၍ မရသလိုမျိုး ဖြစ်နေပါလိမ့်မယ်။

အကယ်၍ များကုမ္ပဏီတစ်ခုတည်းမှာ IBM နှင့် DEC ကွန်ပျူတာ နှစ်မျိုးစလုံး ရှိနေမယ်ဆိုရင် IBM တွေက network တစ်ခု၊ DEC ကွန်ပျူတာတွေက သတ်သတ် network တစ်ခု သီးခြားတည်ဆောက် ရပါတယ်။ ၎င်း network ဂရုစတို့သည် ဟိုဘက်ဒီဘက် အဆက်အသွယ် လုပ်လို့မရပါဘူး။

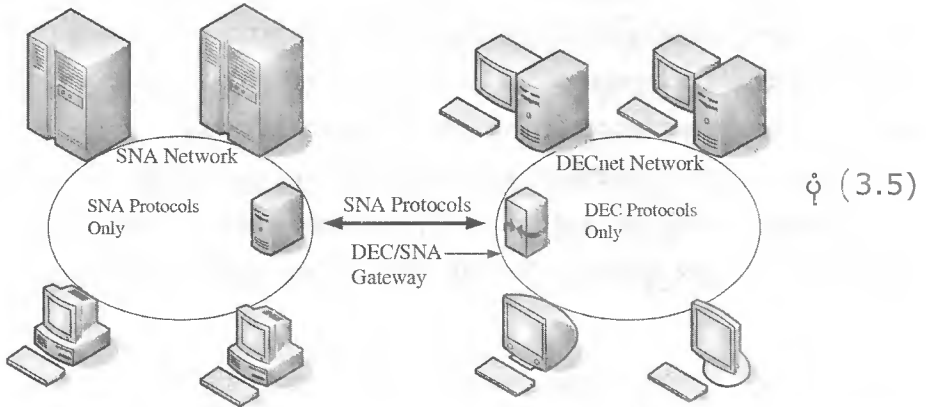
IBM and DEC Networks in a single company



အဲဒီပြဿနာကို ပြေလည်စေရန်အတွက် DEC သည် သူ၏ ကွန်ပျူတာတွေကို IBM မှ SNA model အားနားလည်လက်ခံပြီး အလုပ်လုပ်နိုင်စေရန် လုပ်ဆောင်ခဲ့ရပါတယ်။ ဘာကြောင့် NEC ဘက်မှလုပ်ဆောင် ခဲ့ရသလဲ ဆိုတော့ အဲဒီအချိန်အခါတုန်းက IBM ရောင်းအားသည် DEC ထက် ၁၀ဆခန့် ပိုများပါတယ်။ ဒါကြောင့် SNA မှ DECnet သို့၊ DECnet မှ SNA သို့ အပြန်အလှန် ပြောင်းလဲပေးမယ့် software တစ်ခုကို DEC မှ ရေးသားခဲ့ပါတယ်။

ဖော်ပြပါပုံ (3.5) ကို ကြည့်ပါ။ ၎င်း software ကြောင့်ပင် DEC ကွန်ပျူတာများသည် IBM ကွန်ပျူတာများနှင့် အပြန်အလှန် ဆက်သွယ်နိုင်ပါတယ်။ သို့သော်လည်း ပြည့်စုံကောင်းမွန်တဲ့ ဖြေရှင်းမှု မျိုးတော့မဟုတ်ခဲ့ပါဘူး။ ဒါကြောင့် နောက်ပိုင်းမှာ ပိုမိုကောင်းမွန်တဲ့ နည်းလမ်းတစ်ခုဖြင့် အစားထိုး ဖြေရှင်းခဲ့ကြပါတယ်။ အဲဒါကတော့ SNA၊ DECnet အစရှိတဲ့ ကိုယ်ပိုင် networking model အသုံးပြုမှုများ ကို ရပ်ဆိုင်းပြီး ဘုံပိုင်ဖြစ်တဲ့ TCP/IP Model (Open Public Model လို့လည်းခေါ်ပါတယ်။) ကို အစားထိုး အသုံးပြုခြင်း ဖြစ်ပါတယ်။

Using DEC-to-SNA Gateway



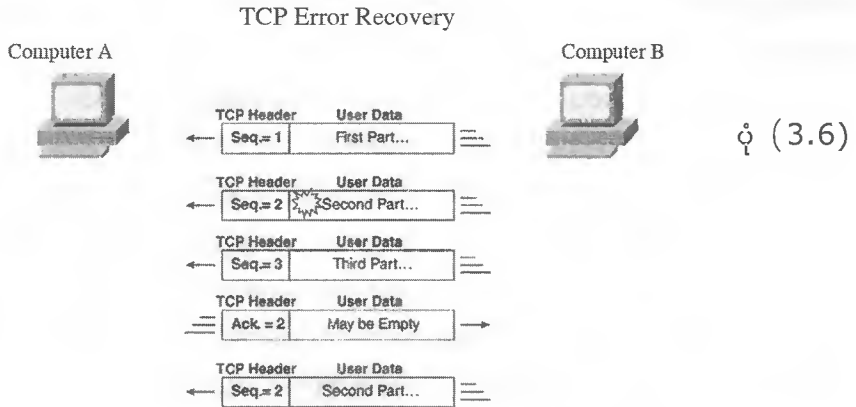
ဒါကြောင့် ယနေ့အချိန်မှာတော့ ကွန်ပျူတာတိုင်းသည် TCP/IP model လို့ခေါ်တဲ့ public networking model ကို အသုံးပြုကြပါတယ်။ အဲဒီလို ကွန်ပျူတာအားလုံးတို့သည် networking model တစ်ခုထဲကို အတူတူအသုံးပြုကြသည့်အတွက် တစ်လုံးနှင့်တစ်လုံး အလွယ်တကူ အပြန်အလှန် communicate လုပ်နိုင်ကြပါတယ်။ TCP/IP model သည် အမည်အားဖြင့် TCP နှင့် IP ဟူသော protocol အမည် ဂရုဖြင့်သာ ကိုယ်စားပြုခေါ်ဝေါ် ကြသော်လည်း အမှန်တကယ်တော့ TCP၊ IP၊ UDP အစရှိသော သီးခြား protocol ပေါင်းများစွာ ပါဝင်ပါတယ်။ TCP နှင့် IP သည် ၎င်း model ထဲကအသုံးအများဆုံး protocol ဂရုရဲ့ အမည်ဖြစ်ပါတယ်။

Transmission Control Protol (TCP)

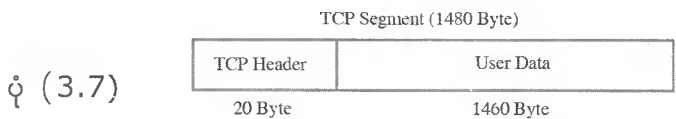
TCP ရဲ့လုပ်ဆောင်မှုနှင့် ပါတ်သက်ပြီး ပြောရရင် သူ့မှာ feature များစွာရှိပါတယ်။ အဲဒီများစွာထဲက သိသာထင်ရှားဆုံးက 'segmentation' နှင့် 'error recovery' ဆိုတဲ့ feature တို့ပင်ဖြစ်ပါတယ်။ segmentation သည် အရွယ်အစားကြီးမားတဲ့ data တွေကို မပို့ခင်မှာ packet များအဖြစ်သို့ စိတ်ပိုင်းခြင်း လုပ်ငန်းစဉ်ရဲ့အစလို့ဆိုနိုင်ပါတယ်။

ဆိုရရင် ရှေ့မှာဖော်ပြခဲ့တဲ့ ရန်ကုန်မှ မန္တလေးသို့ နို့မှုန့် အထုပ် ၁သိန်းပို့တဲ့ ဥပမာလိုပါပဲ။ ကွန်ပျူတာတစ်လုံးမှ ပေးပို့ဖို့ရှိလာတဲ့ data သည် အရွယ်အစားကြီးနေတယ်ဆိုရင် ဒီအတိုင်းမပို့ပဲ နိုင်နိုင် နှင်းနှင်းဖြင့် ပေးပို့၍ရနိုင်သော အပိုင်းငယ်လေးများအဖြစ် စိတ်ပိုင်းခြင်းကို TCP မှလုပ်ဆောင်ပြီး၊ ၎င်း လုပ်ငန်းစဉ်ကို segmentation လို့ခေါ်ပါတယ်။ ထိုမှတစ်ဖန် TCP သည် segmentation လုပ်ငန်းစဉ် ပြီးဆုံး၍ ရရှိလာမည့် data အပိုင်းငယ်လေးများရှေ့တွင် TCP header တွေကို ထည့်သွင်းပေးပါတယ်။ TCP header ထည့်သွင်းပြီးသော data အပိုင်းငယ်ကို 'TCP segment' လို့ခေါ်ပါတယ်။ (packet မဖြစ်သေးတာ ကို သတိပြုပါ)။ TCP header ကို ထည့်သွင်းခြင်းရဲ့ အဓိကရည်ရွယ်ချက်ကတော့ error recovery အတွက်ဖြစ်ပါတယ်။

ရှေ့မှာဖော်ပြခဲ့တဲ့ ပုံ (3.3) သည် error recovery လုပ်နိုင်တဲ့ protocol အားလုံးကို ခြုံငုံမိ အောင်ဖော်ပြထားခဲ့ခြင်းဖြစ်ပါတယ်။ ယခုဖော်ပြသွားမယ့်ပုံ(3.6) သည် ၎င်းပုံ(3.3) နှင့် ဆင်တူပါတယ်။ ဒါပေမယ့် TCP အတွက်ကိုဦးတည်ဖော်ပြမှာ ဖြစ်သည့်အတွက်ကြောင့် အချို့နေရာတွေမှာ ကွဲလွဲမှုတွေ ရှိလာပါလိမ့်မယ်။



ပုံ(3.6) တွင်ကြည့်ပါ။ TCP segment တစ်ခုရဲ့ရှေ့ပိုင်းမှာ TCP header ဆိုတာနှင့် သူ့နောက်မှာ 'Data' ဆိုတာကိုတွေ့ရပါလိမ့်မယ်။ error recovery အတွက် TCP သည် segment တွေကို နံပါတ်စဉ် တပ်ဖို့လိုပါတယ်။ သည့်အတွက် TCP header သည် sequence number <Seq> လို့ခေါ်တဲ့ segment နံပါတ်စဉ်ထည့်သွင်းဖို့ နေရာဖြစ်လာပါတယ်။ ဒါ့အပြင် TCP header သည် acknowledge number <ACK> ကို ထည့်သွင်းရမယ့် နေရာတစ်ခုလည်း ဖြစ်ပါတယ်။ acknowledge number ရဲ့အဓိက ရည်ရွယ်ချက်ကတော့ ဘယ် segment မှာ error ရှိနေသလဲဆိုတာကို ပေးပို့သူအား ပြန်လည်ပြောပြ နိုင်ရန်ဖြစ်ပါတယ်။



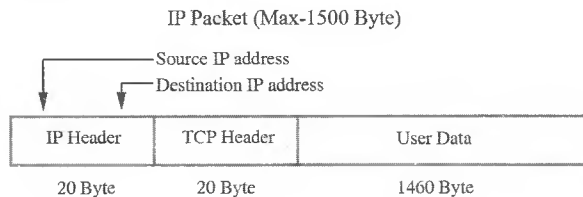
segment တစ်ခုရဲ့အရွယ်အစားသည် 1480 byte ဖြစ်ပါတယ်။ TCP header သည် 20 byte နေရာယူပါတယ်။ ဒါကြောင့် segment တစ်ခုမှာ data ပမာဏ အများဆုံး 1460 byte ထည့်သွင်း နိုင်တယ်လို့အကြမ်းချဉ်းမှတ်သားထားနိုင်ပါတယ်။

Internet Protocol (IP)

TCPသည် segment (Data + TCP header) တွေကို အခြားကွန်ပျူတာ တစ်လုံးဆီသို့ပို့လို ပါတယ်။ ဒါပေမယ့် segment တွေကို ပို့ဖို့ရန် လိုအပ်တဲ့ အသေးစိတ် လုပ်ငန်းစဉ်တွေကို TCP မှ မသိပါ။ TCP သည် segmentation၊ error recovery နှင့် အခြားလုပ်ငန်းစဉ် အချို့နှင့် သာသက်ဆိုင်ပါတယ်။ ဒါကြောင့် data တွေကို ပို့ဖို့ရန် IP ရဲ့ အကူအညီကို ရယူပါတယ်။ TCP မှ segmentation လုပ်ပြီး ခြုံရရှိလာသော segment တို့၏ ရှေ့တွင် IP မှ header တစ်ခုကို ထည့်သွင်းပါတယ်။ IP မှ ထပ်မံထည့်သွင်းသော ၎င်း header ကို 'IP header' ဟုခေါ်ပြီး source နှင့် destination IP address ပါရှိပါတယ်။

ဆိုရရင် IP မှ ထည့်သွင်းသော IP header ထဲတွင် IP address ၂ ခုပါရှိပါတယ်။ တစ်ခုက source IP address ဖြစ်ပြီး၊ ကျန်တစ်ခုက destination IP address ဖြစ်ပါတယ်။ အမြန်ချောပို့ လုပ်ငန်းတစ်ခုမှ တဆင့် မိမိရဲ့ မိတ်ဆွေထံသို့ ပါဆယ်ထုပ် တစ်ထုပ် ပို့မယ်ဆိုပါစို့။ ဒါဆိုရင် ချောပို့လုပ်ငန်းက ထုတ်ပေးတဲ့ form ပုံစံ စာရွက်ထဲမှာ မိမိပို့လိုတဲ့ လိပ်စာ (ဝါ) လက်ခံရယူမည့်သူ လိပ်စာကို အတိအကျ ဖြည့်စွက်ရပါတယ်။ ဒါ့အပြင် အကြောင်းတစ်ခုခုကြောင့် ပေးပို့၍ မရခဲ့ဘူးဆိုရင် ၎င်းပါဆယ်ကို ချောပို့လုပ်ငန်းမှ မိမိထံသို့ ပြန်ပို့ပေး နိုင်အောင် မိမိလိပ်စာ (ဝါ) ပေးပို့သူ၏ လိပ်စာကို ဖြည့်စွက်ပေးရပါတယ်။

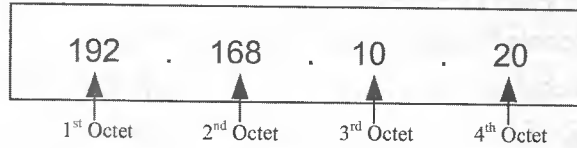
ထိုနည်းတူစွာပင် ကွန်ပျူတာတစ်လုံးမှ အခြားကွန်ပျူတာတစ်လုံးသို့ data ပေးပို့ရန်အတွက် လက်ခံရယူမည့် ကွန်ပျူတာ၏ IP address ကို IP header တဲရှိ destination IP address နေရာတွင် ထည့်သွင်းရပါတယ်။ အလားတူပင် ပေးပို့သည့် ကွန်ပျူတာ၏ IP address ကို source IP address နေရာတွင် ထည့်သွင်းရပါတယ်။ IP header ထည့်သွင်းပြီးပါက segment မှာညှပ် IP packet (IP header + Data) ဖြစ်လာပါတယ်။ 4 byte ပမာဏရှိတဲ့ IP address ၂ ခုအပါအဝင် IP header သည် 20 byte ရှိပါတယ်။ ဤတွင်မှ ဆက်ဆိုရရင် IP packet တစ်ခု၏ အမြင့်ဆုံး ပမာဏသည် 1500 byte ဖြစ်တယ်လို့ အကြမ်းမျဉ်းမှတ်သားထားနိုင်ပါတယ်။



ပုံ (3.8)

IP address အကြောင်းကို အနည်းငယ်ရှင်းပြလိုပါတယ်။ စာပို့တဲ့အခါ စာအိတ်ပေါ်မှာ အိမ်အမှတ်၊ လမ်း၊ ရပ်ကွက်၊ မြို့နယ်၊ တိုင်းအစရှိသဖြင့် လိပ်စာကို ဘယ်လိုရေးရမယ်ဆိုတဲ့ format ရှိသလို IP address မှာလည်း internet protocol မှ သတ်မှတ်ပေးထားသော format ရှိပါတယ်။ IP address တွေသည် 32 bit binary ဂဏန်းတွေဖြစ်ပါတယ်။ သို့သော် အသုံးပြုသူတို့အနေနှင့် 32 bit binary ဂဏန်းများကို မှတ်သား ချရေးဖို့ရန်များစွာအခက်အခဲရှိသည့်အတွက် address တွေကို decimal ဂဏန်းများဖြင့် အသုံးပြုကြပါတယ်။

ဒါကြောင့် IP addressတို့ရဲ့ရေးသားပုံကို dotted decimalလို့ခေါ်ပါတယ်။



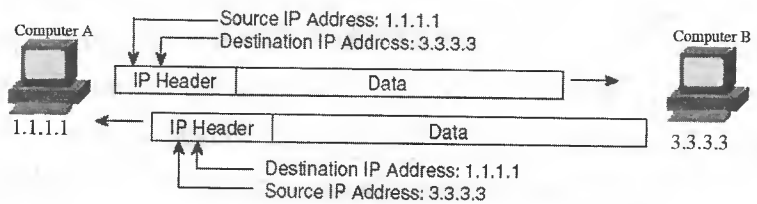
ပုံ (3.9)

decimal numberတစ်ခုစီကို octetတစ်ခုလို့ခေါ်ပါတယ်။ decimal octetတစ်ခုသည် 8 bit ကိုကိုယ်စားပြုပါတယ်။ ဒါကြောင့် IP addressတစ်ခုတွင် 4 octetပါရှိသည့်အတွက် IP addressတစ်ခုလုံးသည် 32 bit(4 Byte)ဖြစ်ပါတယ်။

ကွန်ပျူတာမှာတပ်ဆင်ထားသည့် NIC တိုင်းအတွက် IP address တစ်ခုစီ သတ်မှတ်ပေးဖို့ လိုပါတယ်။ အဲဒီလိုသတ်မှတ်ပေးရသည့်နေရာမှာ IP addressတစ်ခုသည် networkထဲရှိအခြားမည်သည့် addressနှင့်မှထပ်တူမညီတဲ့ decimalဂဏန်းတွေတွေဖြစ်ရပါမယ်။

အောက်ဖော်ပြပါပုံကတော့ ကွန်ပျူတာ A နှင့် ကွန်ပျူတာ B တို့ အပြန်အလှန် data ဖလှယ်ကြပုံ ဖြစ်ပါတယ်။ ထိုပုံအရ ကွန်ပျူတာ A ၏ IP addressသည် 1.1.1.1 ဖြစ်ပြီး ကွန်ပျူတာ B ၏ IP address သည် 3.3.3.3 ဖြစ်ပါတယ်။

ပုံ (3.10)



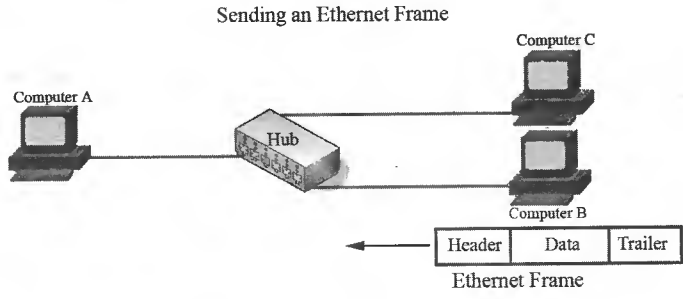
An Ethernet Frame

ကွန်ပျူတာတစ်လုံးကနေ networkပေါ်မှတစ်ဆင့် dataတွေပေးပို့ခင်မှာ ရှေ့က chapter-2 မှာ ဖော်ပြခဲ့တဲ့ အသေးစိတ်အခြေခံအချက်တွေနှင့် ပြီးပြည့်စုံပြီးသားဖြစ်ရပါမယ်။ ဆိုရရင် ကွန်ပျူတာ နှစ်လုံးတည်း ချိတ်ဆက်မယ်ဆိုရင် cross cable ၊ hub ကိုဗဟိုပြုချိတ်ဆက်မယ်ဆိုရင် straight cable အစရှိသဖြင့် သင့်လျော်မှန်ကန်သော cabling ဖြင့် install လုပ်ပြီးသားဖြစ်ရပါမယ်။ နောက်တစ်ချက်အနေနှင့် ဘယ်လောက်ရှိတဲ့ ဗို့အားဆိုရင် 0 ၊ ဘယ်လောက်ဆိုရင် 1 ဆိုတဲ့ encoding rule ကို နားလည်ပြီးသား ဖြစ်ရပါမယ်။ (NIC ထုတ်လုပ်စဉ်ကတည်းက ethernet standard အတိုင်း သတ်မှတ်ပြီးသားဖြစ်ပါတယ်)။

ဖော်ပြပါအချက်တွေပြည့်စုံခဲ့ပြီဆိုရင်တောင်မှ ကွန်ပျူတာတွေသည် data packet တွေကို network ပေါ်မှာ ဒီအတိုင်းပို့လို့မရသေးပါဘူး။ မပို့ခင်မှာ data packet တွေကို ethernet frame အတွင်း ထည့်သွင်း တည်ဆောက်ရပါတယ်။ ဆိုရရင် ပေးပို့မယ့် data packet တွေရဲ့ရှေ့မှာ header နှင့် နောက်မှာ trailer တို့ကိုထည့်သွင်းပြီး frame တစ်ခုအဖြစ်သို့ တည်ဆောက်ရပါမယ်။ အဲဒီဖြစ်စဉ်ကို encapsulation လို့ခေါ်ပါတယ်။

encapsulation သည် ဘာနှင့်အလားသဏ္ဍန်တူသလိုဆိုတော့ စာကိုစာအိတ်အတွင်း ထည့်သွင်းပြီး စာတိုက်မှတစ်ဆင့် ပေးပို့ခြင်းဖြစ်စဉ်နှင့် ဆင်တူပါတယ်။ စာပို့တဲ့အခါ မိမိကြိုက်သလို လက်လွတ်စပယ် ပေးပို့လို့မရပါဘူး။ စာတိုက်လုပ်ငန်းမှ သတ်မှတ်ထားတဲ့ စည်ကမ်းဘောင်ထဲမှ ဖြစ်ဖို့လိုပါတယ်။ ဆိုရရင် စာအိတ်ပေါ်မှာ လိပ်စာရေးတာကအစ ဘယ်လိုပုံစံရေးရမယ် အစရှိတဲ့ စည်းစနစ်တွေရှိပါတယ်။

ထိုနည်းတူစွာပင် ethernet frame တစ်ခုကိုတည်ဆောက်တဲ့နေရာမှာလည်း header ထဲမှာ ဘာတွေပါရမယ်၊ trailer ထဲမှာ ဘာတွေပါရမယ်ဆိုတဲ့ ethernet standard အရ သတ်မှတ်ချက်တွေ ရှိပါတယ်။ အဲဒီသတ်မှတ်ချက်တွေကို လိုက်နာမှသာလျှင် NIC တစ်ခုသည် data packet တွေကို frame တစ်ခုအဖြစ်သို့ မှန်မှန်ကန်ကန် တည်ဆောက်နိုင်မှာဖြစ်ပါတယ်။ header နှင့် trailer အပါအဝင် data တွေကို encapsulate လုပ်ပြီး၍ ရလာမည့် bit အစုအဝေးသည် ethernet frame တစ်ခုဖြစ်ပါတယ်။ အောက်ပုံ (4.1) တွင်ကြည့်ပါ။ ကွန်ပျူတာ B မှ ကွန်ပျူတာ A ထံသို့ frame တစ်ခုပေးပို့နေပုံဖြစ်ပါတယ်။



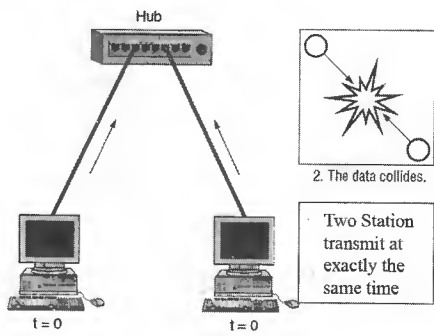
ပုံ (4.1)

ဘာကြောင့် frame တွေအဖြစ်တည်ဆောက်ပြီးမှ ပို့ရသလဲ။ ဒီအတိုင်းပို့လို့မရဘူးလားလို့ မေးလာ ခဲ့ရင်တော့ ဒါဟာ သတ်မှတ်ချက်၊ မဖြစ်မနေလိုက်နာရမယ့်လုပ်ထုံးလုပ်နည်းပဲလို့ ဆိုရမှာဖြစ်ပါတယ်။ ဥပမာ စာအုပ်ထုပ် တစ်ထုပ်ကိုဆိုင်တစ်ဆိုင်သို့ ပို့ရမယ်။ ပို့မယ့်နေရာကနေ ဆိုင်အထိစက်ဘီးနဲ့ဖြစ်ဖြစ်၊ ကားနဲ့ပဲဖြစ်ဖြစ် သယ်သွားလို့ရနိုင်တယ် ဆိုပါတော့။ ဒါပေမယ့် ဖြတ်သန်းသွားရမယ့် လမ်းမပေါ်မှာ စက်ဘီး၊ ဆိုင်ကယ်ဖြတ်သန်းခွင့်မပြုဘူး။ ကားဖြင့်သာ ဖြတ်သန်းမောင်းနှင်ခွင့်ရှိတယ်လို့ ဥပဒေရှိနေရင် မဖြစ်မနေမော်တော်ကားထဲထည့်ပြီး သယ်ဆောင်ကြရမှာဖြစ်ပါတယ်။ ထိုနည်းလည်းကောင်းပါပဲ ethernet standard အရ LAN ပေါ်မှာ data တွေကို ဒီအတိုင်း သယ်ဆောင်ခွင့်မပြုပါဘူး။ ပို့လိုတဲ့ data တွေကို မော်တော်ကားနှင့်တူတဲ့ ethernet frameတွေထဲထည့်ပြီးသယ်ရမှာဖြစ်ပါတယ်။ ဒါကြောင့် dataတွေကို frameတစ်ခုထဲထည့်ပြီးပြီဆိုမှ LANပေါ်မှာ ပေးပို့နိုင်ကြမှာဖြစ်ပါတယ်။

Collision

ပို့လိုတဲ့ data တွေကို frame တစ်ခုထဲမှာ ထည့်သွင်းခဲ့ပြီးပြီဆိုရင် LAN (network) ပေါ်မှာ ပို့ဖို့ရန် အဆင်သင့်ဖြစ်သွားပါပြီ။ ဒါတောင် ပို့ချင်သလို ပို့လို့မရသေးပါဘူး။ ethernet standard အရ သတ်မှတ်ထားတဲ့ စည်းမျဉ်းစည်းကမ်းတွေကို လိုက်နာရပါဦးမယ်။ ဥပမာဆိုရရင် ကားတစ်စီးကို မောင်းတဲ့အခါ မိမိ သွားလိုတဲ့နေရာရောက်အောင်မောင်းချင်သလို မောင်းသွားလို့မရပါဘူး။ မီးနီပြရင် ရပ်ရမယ်။ တစ်ကြိမ်မှာ ကားတစ်စီးသာဖြတ်သန်းခွင့်ပြုထားတဲ့ တံတားပေါ်မှာ အခြားကားတစ်စီးစီး မောင်းနေရင် စောင့်ရမယ် ရှင်းသွားပြီဆိုမှ ဖြတ်သန်းမောင်းနှင် ရမယ် အစရှိတဲ့ စည်းမျဉ်းစည်းကမ်း ဥပဒေတွေကို လိုက်နာရပါသေးတယ်။ ဥပဒေလက်လွတ် မောင်းချင်သလိုမောင်းကြမယ်ဆိုရင်တော့ ယဉ်တိုက်မှုတွေဖြစ်ပြီပေါ့။ ကားတွေလိုပဲ LAN ပေါ်မှာ ဖြတ်သန်းနေတဲ့ frame တွေသည်လည်း တစ်ခုနှင့် တစ်ခုတိုက်မိတတ်ကြပါတယ်။ အဲဒီဖြစ်စဉ်ကို collision လို့ခေါ်ပါတယ်။

An Ethernet Frame Collision



ပုံ (4.2)

collision သည် frame နှစ်ခု (သို့) နှစ်ခုထက်ပိုတဲ့ frame တွေသည် network cable (twisted pair) တစ်ချောင်း၏ တစ်နေရာရာမှာ တစ်ချိန်တည်းတစ်ပြိုင်နက် ဆုံမိတဲ့အခါမျိုးတွေမှာ ဖြစ်လေ့ရှိပါတယ်။

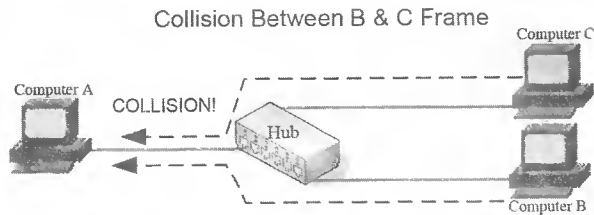
ယာဉ်စည်းကမ်းတွေလိုပဲ ethernet standard အရ frame တွေကို ဘယ်အချိန်မှာ ဘယ်လို ပို့ရမယ်၊ ဘယ်အချိန်မှာတော့ဖြင့် မပို့ရဆိုပြီး သတ်မှတ်ချက်တွေရှိပါတယ်။ ၎င်း ethernet စည်းကမ်း တွေသည် frame တစ်ခုနှင့်တစ်ခုတိုက်မိခြင်းဆိုတဲ့ collision မဖြစ်အောင်ကာကွယ်ပေးပါတယ်။ ဒီနေရာမှာ စိတ်ဝင်စားစရာကောင်းတာကတော့ hub ကို အသုံးပြုတဲ့ LAN တွေမှာဆိုရင် ethernet စည်းမျဉ်း၊ စည်းကမ်းတွေကို ဘယ်လောက်ပင်လိုက်နာလိုက်နာ collision ဖြစ်နိုင်တယ်ဆိုတဲ့အချက်ဖြစ်ပါတယ်။

Collision happens on Ethernet

ယာဉ်စည်းကမ်း၊ လမ်းစည်းကမ်းတွေကို အပြည့်အဝလိုက်နာနေလျှင်တောင်မှ တခါတလေ ယာဉ်တိုက်မှုနှင့် ကြုံရနိုင်သလိုပါဘဲ LAN ထဲမှာရှိတဲ့ ကွန်ပျူတာတွေသည် ethernet rule တွေအတိုင်း လုပ်ဆောင်နေသော်ငြားလည်း collision နှင့် ကြုံရတတ်ပါတယ်။ ဘာကြောင့် ဘယ်လို collision ဖြစ်ရသလဲဆိုတာကို သဘောပေါက်စေရန်အောက်ဖော်ပြပါအချက်နှစ်ချက်ကို အရင်လေ့လာကြည့်ရအောင်။

နှစ်ခု (သို့) နှစ်ခုထက်ပိုသော signal တို့ ဝါယာတစ်ချောင်းအတွင်း တစ်ပြိုင်နက် ဖြတ်သန်းသွား တဲ့အခါ ထို signal တို့ တစ်ခုနှင့်တစ်ခုရောထွေးသွားပြီး signal တစ်ခုတည်းကဲ့သို့ ဖြစ်သွားကာ လက်ခံမည့်ကွန်ပျူတာအနေနှင့် 0 လား၊ 1 လားဆိုတာကို မသိနိုင်အောင် ပုံသဏ္ဍန်ပျက်ယွင်းသွား တတ်ပါတယ်။

hub တွေသည် signal ကို လက်ခံရရှိသော port မှလွဲ၍ ကျန် port များအားလုံးဆီသို့ တစ်ပြိုင်နက် ဖြန့်ဝေပေးပါတယ်။

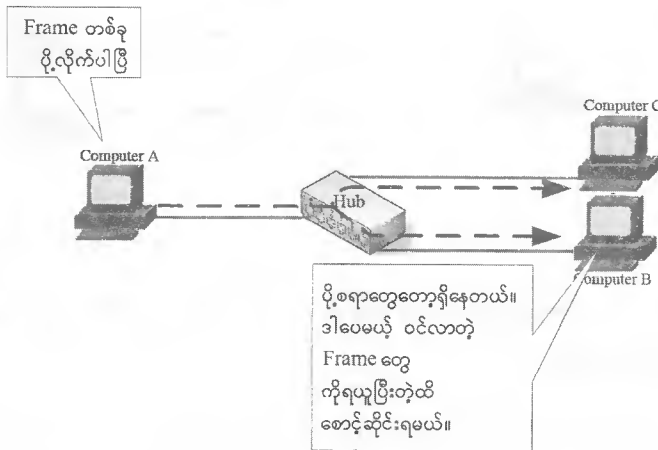


ပုံ (4.3)

ဖော်ပြပါအချက်နှစ်ချက်ကို အခြေခံပြီးပုံ (4.3) မှာဖော်ပြထားသကဲ့သို့ ကွန်ပျူတာ B နှင့် C တို့မှ A ထံသို့ frame တွေကို တစ်ပြိုင်နက်ပို့လွှတ်ကြမယ်ဆိုရင် ဘာတွေဖြစ်လာနိုင်မလဲ စဉ်းစားကြည့်ပါ။ ကွန်ပျူတာ B နှင့် C တို့မှ frame တစ်ခုစီ ပို့လိုက်သော်လည်း ကွန်ပျူတာ A တွင် မညီသည့် frame ကိုမှ မှန်မှန်ကန်ကန် နားလည်လက်ခံနိုင်ခြင်းမရှိပါ။ ဘာဖြစ်လို့လဲ ဆိုတော့ hub သည် ကွန်ပျူတာ A ထံသို့ frame နှစ်ခုစလုံးကို cable ပေါ်မှာ တစ်ပြိုင်နက်ပို့လွှတ်သဖြင့် collision ဖြစ်သွားသောကြောင့်ဖြစ်ပါတယ်။

To Avoid Collision

collision ဖြစ်စဉ်ကို လျော့ချရန်အတွက် ethernet standard အရ သတ်မှတ်ထားတဲ့ algo-rithm တစ်ခုရှိပါတယ်။ CSMA/CD (Carrier Sense Multiple Access / Collision Detection) လို့ခေါ်ပါတယ်။ CSMA/CD ဆိုတဲ့အမည်ထက် သူ့နောက်က idea ကို နားလည်ထားဖို့ရန်အလွန်အရေးကြီးပါတယ်။ သူ့ရဲ့အခြေခံအကျဆုံးနှင့် အရိုးရှင်းဆုံး idea ကတော့ "listen before sending" ဖြစ်ပါတယ်။ သဘောကတော့ မိမိမှာပို့စရာ frame တစ်ခုရှိနေမယ်။ ဒါပေမယ့် ယခုလတ်တလော မိမိထံဝင်လာတဲ့ frame တွေကို လက်ခံနေရမယ်ဆိုရင် ပို့လို့မရသေးပါဘူး။ စောင့်ဆိုင်းရယူပြီးမှ ပို့ရပါမယ်။



ပုံ (4.4)

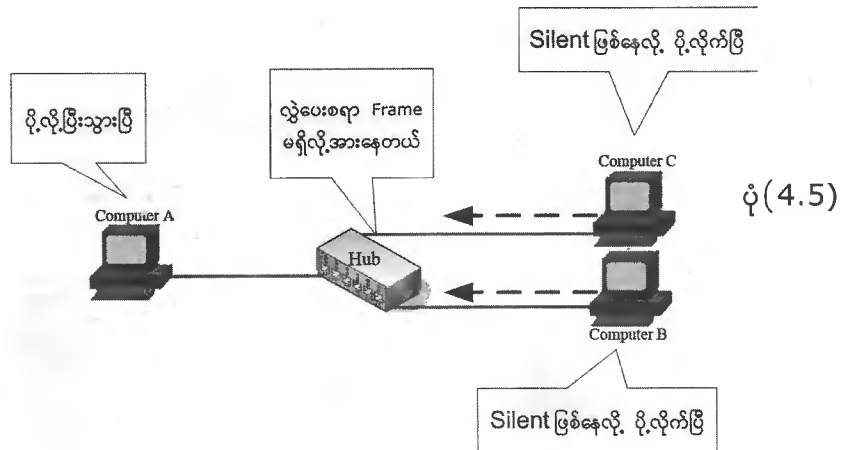
ဒီနေရာမှာ သတိပြုရမှာက hub တို့ရဲ့ broadcast လုပ်တတ်တဲ့ သဘာဝအရ ကွန်ပျူတာတစ်လုံးမှ fram တစ်ခု ပို့ပြီဆိုတာနှင့် hub မှာချိတ်ဆက်ထားသမျှ ကျန်ကွန်ပျူတာအားလုံးစီရောက်မယ်ဆိုတာ ဖြစ်ပါတယ်။ အဲဒီတော့ ရောက်လာတဲ့ frame သည် မိမိထံသို့ ရည်ရွယ်ပေးပို့သော frame ဟုတ်မဟုတ် ဆိုတာကို နောက်မှ ဆန်းစစ်ရမယ်။ လတ်တလောကတော့ စောင့်ဆိုင်းလက်ခံရမယ်။

What to do When a Collision Happen

CSMA/CD logic အရ လိုက်ပါ လုပ်ဆောင်နေသော်လည်း collision ဖြစ်နိုင်ပါ သေးတယ်။ ဥပမာဆိုရရင် ကွန်ပျူတာ B နှင့် C တို့မှာ ပို့စရာ frame တွေ အဆင်သင့် ရှိနေတယ်။ ဒါပေမယ့် ကွန်ပျူတာ A မှ ပို့နေတဲ့အတွက် B နှင့် C တို့မှ စောင့်ဆိုင်းနေရပါတယ်။ ကွန်ပျူတာ A မှ frame ပို့လွှတ်မှုပြီးဆုံးသွားတဲ့အခါ LAN ပေါ်မှာ ဘာ signal မှ မရှိတော့ပါဘူး။ တစ်နည်းဆိုရရင် silent ဖြစ်သွားပြီပေါ့။ ပုံ (4.5) မှာ ကြည့်ပါ။

ethernet standard အရ LAN ပေါ်တွင် signal မရှိဘူးဆိုရင် မည်သည့်ကွန်ပျူတာကနေ မဆို transmit လုပ်နိုင်ပါတယ်။ ပုံ (4.5) အရ ဆက်ရရင် ကွန်ပျူတာ B နှင့် C တို့ဘက်မှလည်း မိမိတို့ထံသို့ မည်သည့် signal မှ ဝင်မလာတော့ဘူးဆိုရင် LAN သည် silent ဖြစ်သွားပြီလို့ အလိုလိုသိရှိကြပါတယ်။

အဲဒီလို LAN ပေါ်မှာအားနေတယ်လို့သိရှိချိန်မှာပြိုင်တူလိုလိုဖြစ်နေသည့်အတွက်၎င်းကွန်ပျူတာ နှစ်လုံး စလုံးမှ မိမိတို့ထံမှာ အဆင့်သင့်ရှိနေသော frame တွေကို LAN ပေါ်သို့ တစ်ပြိုင်နက် လွှတ်တင်မိကြပါလိမ့်မယ်။ ပုံ (4.5) သည်ကွန်ပျူတာ B နှင့် C တို့မှတစ်ပြိုင်နက် transmit လုပ်ကြရာဝယ် collision ဖြစ်သွားပုံဖြစ်ပါတယ်။

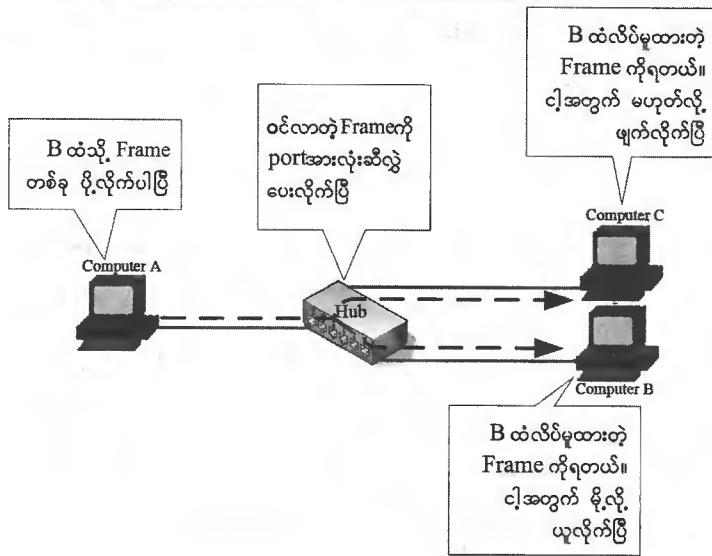


collision ဖြစ်ပြီဆိုတာနှင့် CSMA/CD logic အရ အောက်ဖော်ပြပါအဆင့်များအတိုင်း လုပ်ဆောင်ဖြေရှင်းကြပါလိမ့်မယ်။

- 1) collision ဖြစ်စဉ်မှာပါဝင်တဲ့ ကွန်ပျူတာ (B နှင့် C) တို့သည် collision ဖြစ်သွားတာကို network ပေါ်ရှိအခြားကွန်ပျူတာများ သိရှိနိုင်အောင် Jamming signal ကို transmit လုပ်ပါလိမ့်မယ်။ သဘောကတော့ မိမိတို့ရှေ့ကပေးပို့ခဲ့သော frame သည် အမှားအယွင်း ဖြစ်သွားပြီလို့ အကြောင်းကြားတဲ့သဘောဖြစ်ပါတယ်။
- 2) collision ဖြစ်စဉ်မှာ ပါဝင်တဲ့ ကွန်ပျူတာ (B, C) တို့သည် error ဖြစ်သွားတဲ့ frame ကို ပြန်လည်ပို့ရန် တစ်လုံးနှင့်တစ်လုံးမတူညီနိုင်တဲ့ အချိန် တစ်ခုကိုစောင့်ဆိုင်းရပါတယ်။
- 3) စောင့်ဆိုင်းကြရမယ့် အချိန်ပြည့်တာနှင့် frame ကိုနောက်တစ်ကြိမ် ပြန်ပို့ဖို့ရန် ကြိုးစားပါတော့တယ်။ စောင့်ဆိုင်းရတဲ့ အချိန်သည် random time ဖြစ်၍ တစ်လုံးနှင့်တစ်လုံး မတူနိုင်တော့သည့်အတွက် collision မဖြစ်နိုင်တော့ပါ။

Ethernet Address (Media Access Control Address)

hub ကိုအသုံးပြုထားတဲ့ ethernet LAN တွေမှာဆိုရင်ကွန်ပျူတာတွေသည် ethernet frame များစွာကို လက်ခံရယူကြရပါတယ်။ ဒါပေမယ့် အဲဒီများစွာထဲကမှ အချို့သာလျှင် မိမိထံသို့ဦးတည် ပေးပို့လာသော frame တွေဖြစ်ပါလိမ့်မယ်။ သဘောကတော့ရောက်လာသမျှ frame အားလုံးသည် မိမိအတွက်မဟုတ်ကြပါဘူး။ ပုံ (4.6) တွင်ကြည့်ပါ။



ပုံ (4.6)

ကွန်ပျူတာ A မှ B ထံသို့ data ပို့လိုတယ်။ ဒါပေမယ့် hub တို့ရဲ့လုပ်ဆောင်မှုအရ ကွန်ပျူတာ B နှင့် C နှစ်လုံးစလုံးသည် မိတ္တူယူထားတဲ့ frame တွေကို တစ်ပြိုင်နက် ရရှိကြမှာဖြစ်ပါတယ်။ ဒါပေမယ့် ကွန်ပျူတာ C အနေနှင့် မိမိနှင့် မဆိုင်သည့်အတွက် ရောက်လာတဲ့ frame တွေကို လျစ်လျူရှုပါလိမ့်မယ်။ ကွန်ပျူတာ B အနေနှင့် ကတော့ မိမိအတွက် ဆိုတာသိရှိပြီး လက်ခံယူနိုင်ရပါမယ်။ ဒါဆိုရင် ကွန်ပျူတာ B နှင့် C တို့သည် မိမိတို့နှင့်ဆိုင်တယ်။ မဆိုင်ဘူးဆိုတာကို ဘယ်လိုခွဲခြားသိနိုင်မလဲလို့ မေးစရာရှိလာပါလိမ့်မယ်။ အဲဒီဖြစ်စဉ်ကို နားလည်ဖို့ရန် ethernet address (ဝါ) MAC address သည် ဘာလဲဆိုတာကို သိထားဖို့လိုပါလိမ့်မယ်။

NIC တိုင်းတွင် အခြားမည့်သည့် NIC နှင့်မှ မတူညီနိုင်သည့် ကိုယ်ပိုင် ethernet address တစ်ခုစီ ရှိကြပါတယ်။ ၎င်း address ကို NIC ထုတ်လုပ်စဉ်က တည်းက အသေထည့်သွင်း သတ်မှတ်ပြီးသား ဖြစ်ပါတယ်။ သဘောကတော့ မော်တော်ကားတွေမှာပါတဲ့ frame နံပါတ်လိုမျိုး ဖြစ်ပါတယ်။ ပြုပြင်ပြောင်းလဲလို့ မရပါဘူး။ သူ့ကို ethernet address အပြင် MAC address၊ hardware address၊ physical address ရယ်လို့ အမည်အမျိုးမျိုးဖြင့် ခေါ်ဝေါ်သုံးစွဲ ကြပါတယ်။

ethernet address (ဝါ) MAC address ကို hexa decimal (hex) ဖြင့်ဖော်ပြလေ့ရှိပါတယ်။ hex မှာဆိုရင် 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F ဆိုပြီး ကိန်းဂဏန်း ၁၆ လုံးပါရှိပါတယ်။ (decimal သည် 0 ကနေ 9 အထိသာ ဖြစ်ပါတယ်)။ A သည် 10၊ B သည် 11 အစရှိသဖြင့် F သည် 15 ဖြစ်ပါတယ်။ hex digit တစ်ခုစီသည် 4 bit ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါ ဇယားမှာဆိုရင် hex digit တစ်ခုစီကို ကိုယ်စားပြုတဲ့ binary number များဖြင့် ယှဉ်တွဲဖော်ပြထားပါတယ်။

<u>Binary Digit</u>	<u>Hex Number</u>	<u>Binary Digit</u>	<u>Hex Number</u>
0000	0	0011	3
0001	1	0100	4
0010	2	0101	5

Binary Digit Hex Number

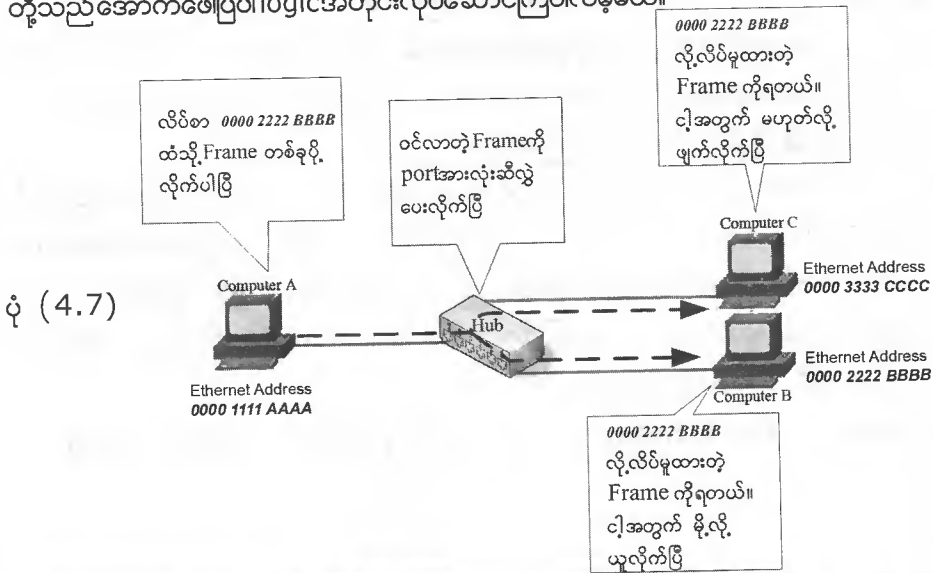
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

ethernet standard သတ်မှတ်ချက်အရ MAC address တစ်ခုတွင် hex digit ၁၂လုံး ပါရှိပါတယ်။ ဤတွင်မှ hex digit တစ်ခုအတွက် 4bit နှုံးဖြင့် MAC တစ်ခုလုံးသည် 48 bit (6byte) ဖြစ်ပါတယ်။ MAC address တစ်ခု၏ format သည် အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

00-50-FC-63-5A-E6 (0050 FC63 5AE6)

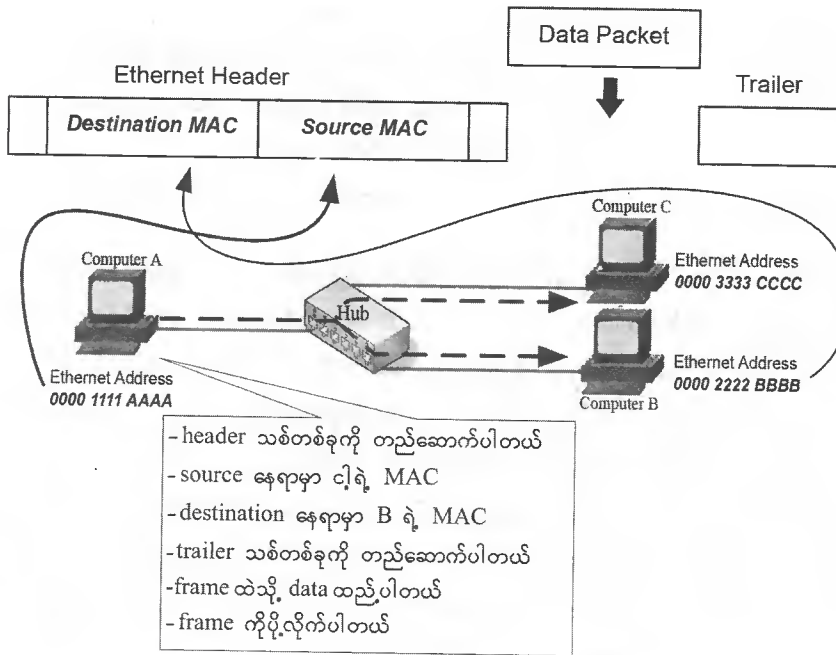
မိမိကွန်ပျူတာတွင် တပ်ထားသော NIC ၏ MAC address ကို ကြည့်ရန် command window တွင် **ipconfig /all** ဟု ရိုက်ထည့်ပြီး enter ခေါက်ပါ။ physical address နေရာတွင် 12 hex digit ကို တွေ့ရပါလိမ့်မယ်။

ကွန်ပျူတာ A မှ သည် B ထံသို့ data ပို့ရန်အတွက် frame ကို တည်ဆောက်တဲ့ နေရာမှာ ethernet header ထဲရှိ destination address field ထဲတွင် ကွန်ပျူတာ B ၏ ethernet address ကို ထည့်သွင်း ရပါတယ်။ ၎င်း destination address field ထဲရှိ ethernet address ကို ကြည့်ပြီး ကွန်ပျူတာ B နှင့် C တို့သည် အောက်ဖော်ပြပါ logic အတိုင်း လုပ်ဆောင်ကြပါလိမ့်မယ်။



ပုံ (4.7)

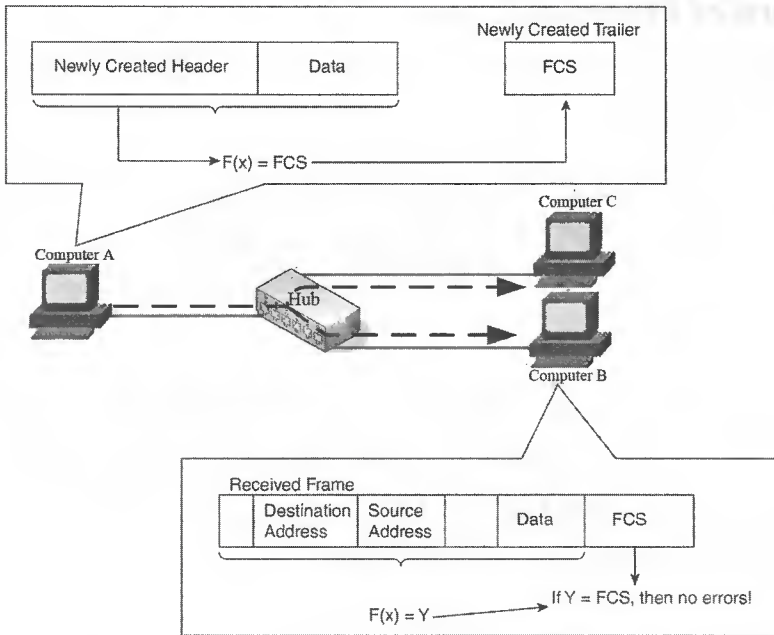
ethernet headerထဲမှာ destination addressအပြင် source addressဆိုတာလည်း ပါရှိပါသေးတယ်။ source address နေရာတွင် ပေးပို့သော ကွန်ပျူတာမှ NIC ၏ MAC ကိုထည့်သွင်း ရပါတယ်။ ကွန်ပျူတာ A မှ B သို့ပို့မယ်ဆိုရင် source နေရာ၌ ကွန်ပျူတာ A ၏ MAC နှင့် destination နေရာတွင် ကွန်ပျူတာ B ၏ MAC တို့နေရာယူပါလိမ့်မယ်။



ပုံ (4.8)

အနှစ်ချုပ်ဆိုရရင် ကွန်ပျူတာ A သည် network ပေါ်သို့ transmit လုပ်နိုင်ရန် ပေးပို့မည့် data packet တွေရဲ့ရှေ့မှာ ethernet header နှင့် နောက်မှာ trailer တို့ကို ထည့်သွင်းပြီး frame တစ်ခု အဖြစ်သို့တည်ဆောက်ရပါတယ်။ header ထဲရှိ source နေရာမှာ ကွန်ပျူတာ A မှ NIC ၏ MAC ၊ Destination နေရာမှာ ကွန်ပျူတာ B မှ NIC ၏ MAC တို့အသီးသီးနေရာယူကြပါလိမ့်မယ်။

(ethernet trailer ထဲမှာ ဘာတွေပါပြီး ဘယ်လို အလုပ်လုပ်သလဲ ဆိုတာကို error detection တွင် ဆက်လက်ဖော်ပြပါမယ်)။ အဲဒီလို frame တစ်ခု အဖြစ်သို့ရောက်အောင် စုစည်းတည်ဆောက်ပြီး ပြီဆိုရင် ဘယ်အချိန်မှာ frame တွေပို့လွှတ် ရမလဲ ဆိုတာကို CSMA/CD logic ကိုအသုံးပြု၍ ဆုံးဖြတ်ပြီး ပေးပို့ကြပါတယ်။



ပုံ (4.9)

အကယ်၍များ လွဲနေပြီ ဆိုရင်တော့ error ဖြစ်လာပြီပေါ့။ ဤနည်းအားဖြင့် လက်ခံရရှိချိန်တွင် frame ထဲမှာ bit error ပါမပါဆိုတာကို စစ်ဆေးသိရှိနိုင်ကြပါတယ်။ အကယ်၍ bit error ဖြစ်လာပြီဆိုတာနှင့် လက်ခံသည့်ကွန်ပျူတာဘက်က ဘယ်လိုလုပ်ဆောင်မလဲဆိုတဲ့ တုန့်ပြန်မှုသည် အရေးကြီးလာပါတယ်။

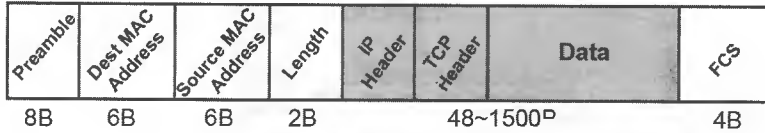
ethernet standard အရ error ပါလာတဲ့ frame ကို စွန့်ပစ်ဖယ်ရှားရမယ်လို့ သတ်မှတ်ထားပြီးသား ဖြစ်ပါတယ်။ ဆိုရရင် ethernet သည် error detection လို့ခေါ်တဲ့ frame တစ်ခု network တလျှောက်ဖြတ်သန်းလာချိန်မှာ error ဖြစ်လာတယ်၊ မဖြစ်လာဘူးဆိုတာကို သိရှိနိုင်ရန် အထိသာလုပ်ဆောင် နိုင်ပါတယ်။ error recovery လို့ခေါ်တဲ့ FCS check အရ အောင်မြင်မှုမရှိတဲ့ frame ကို နောက်တစ်ကြိမ် ပြန်ပို့ပေးရန် request လုပ်ရတဲ့ လုပ်ငန်းစဉ်တွေကို လုပ်ဆောင်နိုင်ခြင်းမရှိပါဘူး။ error recovery ကို TCP မှသာ လုပ်ဆောင် ပါတယ်။

ဒါကြောင့် network တွေတည်ဆောက်ပြီး ကွန်ပျူတာတွေတစ်လုံးနှင့် တစ်လုံး data တွေ အပြန်အလှန် ဖလှယ်နိုင်ကြရန် ethernet နှင့် TCP တို့ရဲ့ ပူးပေါင်းလုပ်ဆောင်မှု အခန်းကဏ္ဍသည် လွန်စွာအရေးပါ ပါတယ်။ LAN ပေါ်မှာ data တွေဘယ်လိုပို့ကြမလဲ၊ error ဖြစ်လာတဲ့ frame တွေကို စွန့်ပစ်ခြင်း အပါအဝင် error detection ကို ဘယ်လိုလုပ်ဆောင်ကြမလဲ ဆိုတာတွေကို ethernet ပိုင်းမှလုပ်ဆောင်ပါတယ်။ error recovery လုပ်ဖို့လိုအပ်လာ ပြီဆိုရင် TCP မှ ဆက်လက် လုပ်ဆောင် ပါလိမ့်မယ်။

Structure of Ethernet Frame

အောက်ဖော်ပြပါရှင်းလင်းချက်တွေကတော့ frameတစ်ခုမှာပါဝင်တဲ့ fieldအမျိုးမျိုးတို့ရဲ့အခြေခံအချက်အလက်တွေပဲဖြစ်ပါတယ်။

Ethernet 2 Frame Format



ပုံ(4.10)

● Preamble

ethernet frameမှ headerတစ်ခုရဲ့အစသည် preambleဖြစ်ပါတယ်။ စုစုပေါင်း 8 byte နေရာယူပါတယ်။ preambleသည် 1 နှင့် 0 တို့တစ်လှည့်စီပါသော bit stream တစ်ခုဖြစ်ပါတယ်။ ဆိုရရင် ရှေ့က 7 byte သည် 10101010 ခုနှစ်ခါဖြစ်ပြီး နောက်ဆုံး 1 byte သည် 10101011 ဖြစ်ပါတယ်။ frame တစ်ခုရဲ့အစဖြစ်တယ်ဆိုတာကို ရည်ညွှန်း ရုံသက်သက် ဖြစ်ပါတယ်။

● Destination MAC Address

Frame ကိုလက်ခံရယူခွင့်ရှိမည့် ကွန်ပျူတာမှ NIC၏ MAC address ပါရှိပါတယ်။ ပုံမှန်အားဖြင့် 6 byte (48 bit) နေရာယူပါတယ်။

● Source MAC Address

frame ပေးပို့မည့် ကွန်ပျူတာမှ NIC၏ MAC address ပါရှိပါတယ်။ destination address ကဲ့သို့ပင် 6 byte (48 bit) နေရာယူပါတယ်။

● Length Field

ဒီနေရာတွင်ပါရှိသော code တွေသည် data field ထဲတွင် ဘယ် network protocol (ဥပမာ IP, IPX) ကို သုံးထားသလဲဆိုတာကို ညွှန်ပြပါတယ်။ ပုံမှန်အားဖြင့် 2 byte နေရာယူပါတယ်။

● Data

အမှန်တကယ်ပေးပို့လိုတဲ့ data packet တွေဖြစ်ပြီး အရွယ်အစားမှာ 48 မှ 1500 byte အတွင်း ရှိပါတယ်။

● FCS

Frame Sequence Check ဖြစ်ပါတယ်။ transmit လုပ်တဲ့အခါ error ဖြစ် မဖြစ်ဆိုတာကို ထောက်လှမ်းနိုင်ရန်ဖြစ်ပါတယ်။

ဖြန့်ဝေပေးပါတယ်။ အဲဒီအချိန်အတွင်းမှာပင် ကွန်ပျူတာ D မှ C ထံသို့ frame အချို့ပေးပို့လိုသော်လည်း CSMA/CD logic အရ collision မဖြစ်အောင်စောင့်ဆိုင်းရပါတယ်။ ဘာနှင့်တူသလဲဆိုတော့ ကားလမ်းမကတော့အကျယ်ကြီးပဲ (ဥပမာ - ခြောက်လမ်းသွား) ဒါပေမယ့် တစ်ကြိမ်မှာ ကားတစ်စီးသာ ဖြတ်သန်းသွားလာ ခွင့်ပြုထားသလိုဖြစ်နေပါတယ် ရှေ့ကကားသည် လမ်းမပေါ်မှာ မရှိတော့ဘူးဆိုမှ နောက်တစ်စီး ဖြတ်သန်းခွင့်ပြုသလိုမျိုးပေါ့။

Switch (Dozens of Lane)

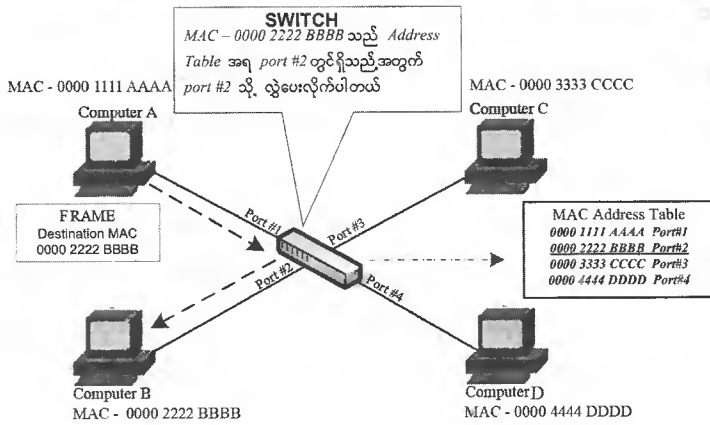
switch ပဲသုံးသုံး၊ hub ပဲသုံးသုံး cabling ကတော့ အတူတူပါပဲ။ ကွန်ပျူတာတစ်လုံးကို cable တစ်ချောင်းစီဖြင့် hub အစား switch ဆီသို့ချိတ်ဆက်ခြင်းပင်ဖြစ်ပါတယ်။ switch တွေသည် hub တွေထက် ဘာကြောင့်စွမ်းဆောင်ရည်ပိုရသလဲဆိုတာကို သဘောပေါက်နားလည်ရန် hub တို့ရဲ့လုပ်ဆောင်ပုံ logic နှင့် switch တို့ရဲ့လုပ်ဆောင်ပုံ logic တို့ကို ယှဉ်ကြည့်ဖို့လိုပါလိမ့်မယ်။

Switch : Frame တစ်ခုကို လက်ခံ ရရှိပြီဆိုတာနှင့် အဲဒီ frame ထဲမှာပါတဲ့ destination MAC address ကို ကြည့်ရှုစစ်ဆေးပါတယ်။ ပြီးတဲ့အခါမှာ ၎င်း destination address နှင့်ဆိုင်သော ကွန်ပျူတာ တပ်ဆင်ထားရာ port ဆီသို့သာ လျှင် frame ကိုပေးပို့ပါတယ်။

hub နှင့် နှိုင်းယှဉ်ကြည့်ရအောင်။ switch သည် port တစ်ခုကဝင်လာတဲ့ frame ကို ကျန် port အားလုံးဆီသို့ဖြန့်ဝေမှုမလုပ်ပါဘူး။ ဝင်လာတဲ့ ethernet frame ကို စစ်ဆေးမယ်၊ destination MAC address ကိုရှာမယ်၊ ပြီးရင် တကယ်ရောက်ဖို့လိုတဲ့ နေရာတစ်ခုတည်းသို့သာ forward လုပ်ပေးမှာ ဖြစ်ပါတယ်။ intelligence ရှိလာတဲ့ သဘောဖြစ်ပါတယ်။

switch တွေသည်လည်း hub မှာကဲ့သို့ပင် pin 1 နှင့် 2 တို့မှ receive လုပ်ပြီး pin 3 နှင့် 6 တို့မှ transmit လုပ်ပါတယ်။ သည့်အတွက် ကွန်ပျူတာမှ switch ဆီသို့ ချိတ်ဆက်တဲ့နေရာမှာလည်း straight-through cable၊ RJ-45 connector တို့ကိုသာ အသုံးပြုကြရပါတယ်။ ဒါကြောင့် network တစ်ခုကို အပြင်ပန်းအရ ကြည့်မယ်ဆိုရင် switch ပဲသုံးသုံး၊ hub ပဲသုံးသုံး အတူတူပင်ဖြစ်ပါတယ်။ အကယ်၍များ hub နေရာမှာ switch ကိုအစားထိုးအသုံးပြုချင်ရင် ဒီအတိုင်း ဖြုတ်လဲလိုက်ရုံဖြစ်ပါတယ်။ ဒါကြောင့် switch နှင့် hub တို့သည် physically အရ ကွာခြားချက်မရှိကြပါဘူး။ ဝင်လာတဲ့ frame ကို အားလုံးဆီသို့ မိတ္တူပွားပြီး ပေးပို့ခြင်းနှင့် ရောက်ဖို့လိုတဲ့ device တစ်ခုတည်းဆီသို့သာ ပို့ဆောင်ခြင်းဆိုတဲ့ logic သာ ကွာခြားပါတယ်။

switch တွေသည် ဝင်လာတဲ့ frame ကို forward လုပ်နိုင်ရန်အတွက် **MAC Address Table** ကို အသုံးပြုကြရပါတယ်။ ၎င်းကို switch address table လို့လည်းခေါ်ပါတယ်။ အဲဒီ table ထဲမှာ network အတွင်း ချိတ်ဆက်တပ်ဆင်ထားတဲ့ ကွန်ပျူတာတို့ရဲ့ MAC address တွေကို မှတ်သားသိမ်းဆည်း ထားပါတယ်။ ပုံ (5.2) တွင်ကြည့်ပါ။



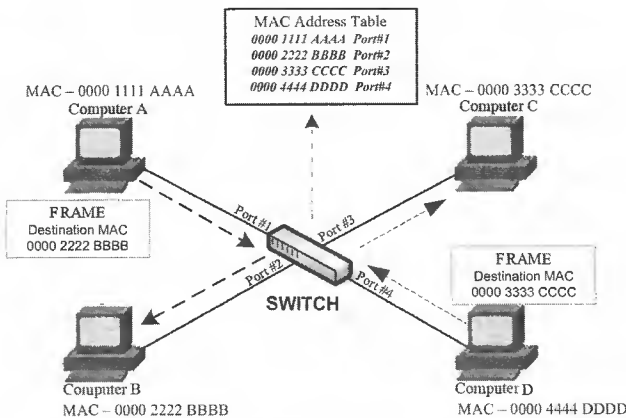
ပုံ (5.2)

Tableသည်ကွန်ပျူတာ B၏ MAC address မှာ 0000 2222 BBBBဖြစ်တယ်ဆိုတာကို switch အားပြောပြနိုင်ပါတယ်။ ဒါကြောင့် 0000 2222 BBBBဆိုတဲ့ address ပါတဲ့ frameကို လက်ခံရရှိတဲ့အခါ switchသည် ၎င်း frameကို port # 2 တစ်ခုတည်းဆီသို့သာ ဆက်လက်ပို့ဆောင်ပေးပါလိမ့်မယ်။

အဲဒီလို port အားလုံး သို့ မဟုတ်ပဲ port တစ်ခုတည်းသို့သာ သီးသန့်ပေးပို့နိုင်ကြသည့်အတွက် switch တွေကို အသုံးပြုခြင်းအားဖြင့် LAN တို့၏စွမ်းဆောင်ရည်ကို တိုးမြှင့်စေတယ်ဆိုတဲ့ အကျိုးဆက်ကို ရရှိစေပါတယ်။

ပုံ (5.2) နှင့် ပုံ (5.3) တို့ကို သတိထားနိုင်ယှဉ်ကြည့်ပါ။ ပုံ (5.2) မှာဆိုရင် ကွန်ပျူတာ A မှ B ထံသို့ ပို့လိုက်တဲ့ frame တွေသည် ကွန်ပျူတာ D နှင့် C တို့ထံသို့ရောက်ရှိခြင်းမရှိပါဘူး။ အကယ်၍ များ တစ်ချိန်တည်း မှာ ကွန်ပျူတာ D မှ C ထံသို့ပို့စရာ frame တွေရှိလာပြီဆိုရင် CSMA/CD logic အရ လတ်တလော လက်ခံရယူ နေသော frame ရှိမရှိဆိုတာကို စစ်ဆေးရပါတယ်။ ဤနေရာမှာတော့ ကွန်ပျူတာ D သည် မည်သည့် frame ကိုမှ လက်ခံရယူနေခြင်းမရှိသည့်အတွက် စောင့်ဆိုင်းစရာမလိုပဲ ကွန်ပျူတာ C ထံသို့ ချက်ချင်းပို့နိုင်ပါတယ်။

ပုံ (5.3)



ပုံ (5.3) ကိုကြည့်ပါ။ ကွန်ပျူတာ A နှင့် D တို့မှ frame တွေကို တစ်ပြိုင်နက် ပို့လွှတ်နေကြပုံ ဖြစ်ပါတယ်။ ဤဖြစ်စဉ်တွင် hub နှင့်သာဆိုရင် ကွန်ပျူတာတစ်လုံးမှသာ transmit လုပ်နိုင်ပါလိမ့်မယ်။ ကွန်ပျူတာနှစ်လုံးတို့တစ်ပြိုင်နက် transmit လုပ်နိုင်ခြင်းအားဖြင့် LAN ထဲမှာ forward လုပ်နိုင်တဲ့ frame ပမာဏနှစ်ဆရှိလာမှာဖြစ်ပါတယ်။

မူလအစ ethernet specification အရ transmission rate သည် 10mbps ဖြစ်ပါတယ်။ ပုံ(5.3) မှာဆိုရင် data ပေးပို့နေတဲ့ လမ်းကြောင်း ၂ ကြောင်းရှိပါတယ်။ တစ်ကြောင်းစီသည် 10mbps ဖြစ်သည်။ အဲဒီလို 10mbps နှုံးဖြင့်တစ်ပြိုင်နက်လမ်းကြောင်း နှစ်ကြောင်း ပို့လွှတ်နိုင်မှုကြောင့် ၎င်း switch ရဲ့ capacity ကို 20mbps လို့ဆိုနိုင်ပါတယ်။ capacity ကိုပိုမိုသဘောပေါက်နားလည်စေရန် 24port ပါတဲ့ switch တစ်ခုဖြင့် စဉ်းစားကြည့်ရအောင်။

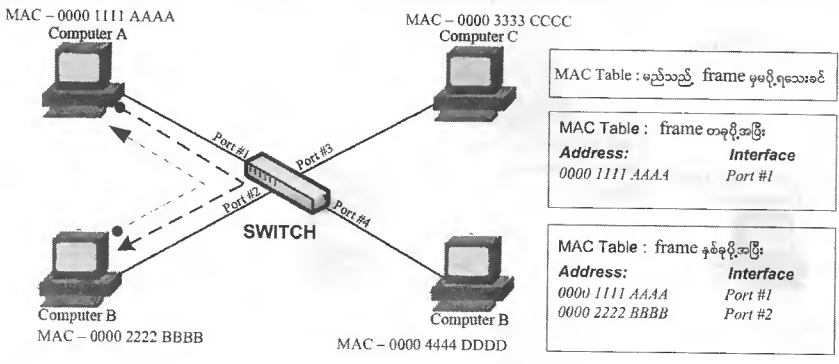
port1 မှာတပ်ဆင်ထားတဲ့ device ကနေ port2 မှာတပ်ဆင်ထားတဲ့ device ဆီကိုပို့မယ်၊ port3 ကနေ port4၊ အစရှိသဖြင့်နောက်ဆုံးမှာတော့ port 23 ကနေ port 24 ဆိုပါတော့။ အဲဒီဖြစ်စဉ်မှာဆိုရင် မဂဏန်းကိုယ်စားပြု port ၁၂ ခုကနေ တပြိုင်နက်ပို့မှာဖြစ်သည့်အတွက် switch capacity သည် $12 \times 10 = 120\text{mbps}$ ဖြစ်ပါလိမ့်မယ်။ တနည်းဆိုရရင် switch သည် 'capacity' 120mbps ထိ support လုပ်နိုင်တယ်လို့ဆိုနိုင်ပါတယ်။ ဒါကမူလ ethernet standard ကိုအခြေခံပြီး ဥပမာအနေနှင့် ဖော်ပြ တာပါ။ ယနေ့အချိန်မှာတော့ fast ethernet (100mbps) ၊ gigabit ethernet (1000mbps) အစရှိ သဖြင့် network တွေမှာ အသုံးပြုတဲ့ ethernet standard တွေ ဖွံ့ဖြိုးတိုးတက်လာတာနှင့်အမျှ switch capacity သည်လည်း အဆများစွာမြင့်မားလာပါတယ်။ ဒါကြောင့်ယနေ့ဈေးကွက်တွင်း ဝယ်ယူရရှိနိုင်တဲ့ switch တွေရဲ့ capacity ကို ကြော်ငြာရောင်းချတဲ့နေရာမှာ Gbps (Giga bit) ဖြင့် ဖော်ပြလေ့ရှိပါတယ်။

Learning MAC Address Table

switch တွေသည် forward လုပ်တဲ့နေရာမှာ frame ထဲတွင် ပါလာတဲ့ destination MAC နှင့် MAC address table တို့ကို တိုက်ဆိုင်စစ်ဆေးပြီး ရည်ရွယ်ရာ ကွန်ပျူတာတစ်လုံးတည်ဆီသို့ ရောက်အောင်ဆောင်ရွက်ပေးတယ်လို့ရှေ့မှာဖော်ပြခဲ့ပြီးပါပြီ။ ယခုဆက်လက်ပြီးတော့ MAC Address table ကိုဘယ်လိုတည်ဆောက်သလဲဆိုတာကိုရှင်းလင်းဖော်ပြသွားပါမယ်။ ပုံ (5.4) တွင်ကြည့်ပါ။

switch ကို ပါဝါဖွင့်လိုက်တဲ့ အချိန်မှာဆိုရင် address table ထဲမှာ ဘာမှ မရှိသေးပါဘူး။ NIC တစ်ခုကနေ frame တစ်ခုပို့လိုက်တိုင်း NIC သည် သူ့ရဲ့ MAC Address ကို frame ထဲရှိ source MAC address နေရာမှာထည့်သွင်းပို့လွှတ်လိုက်ပါတယ်။ အဲဒီ NIC မှလာတဲ့ frame တွေသည် switch ထံရောက်သည့်အခါ switch သည် frame တစ်ခုစီမှာပါတဲ့ source MAC address ကိုစစ်ဆေးရပါတယ်။ ဖော်ပြပါပုံမှာ (5.4) ဆိုရင် frame နှစ်ခုပို့လွှတ်မှုကိုပြထားပါတယ်။ တစ်ခုက ကွန်ပျူတာ A မှဖြစ်ပြီး၊ တစ်ခုက ကွန်ပျူတာ B မှဖြစ်ပါတယ်။

ပုံ (5.4)



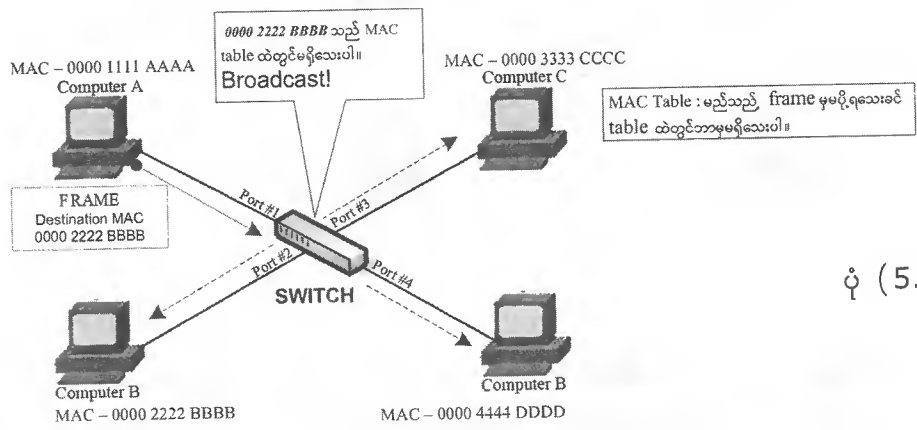
1) ကွန်ပျူတာ A မှ frame တစ်ခုကိုပို့တဲ့အခါ ၎င်း၏ MAC address (0000 1111 AAAA) သည် ethernet header ထဲရှိ source address နေရာမှာပါသွားပါတယ်။ switch သည် ဝင်လာတဲ့ frame ၏ source address ကိုကြည့်ပြီး ပို့လွှတ်သူ၏ MAC address ကိုသိနိုင်ပါတယ်။ ဒါကြောင့် frame ဝင်လာတဲ့ port မှာ ဘယ် MAC address ရှိသော ကွန်ပျူတာ တစ်ဆင့်ထားတယ်ဆိုတာကို switch မှ ထောက်လှမ်းသိရှိနိုင်ပါတယ်။ ပုံအရ MAC address (0000 1111 AAAA) သည် port #1 မှာတစ်ဆင့်ထားတယ်ဆိုတာကို switch မှ သိရှိနိုင်ပါတယ်။ ဤတွင်မှ port #1 နှင့် MAC (0000 1111 AAAA) တို့ကို address table ထဲမှာထည့်သွင်းမှတ်သားထားလိုက်ပါတယ်။

2) ကွန်ပျူတာ B မှ frame တစ်ခုပို့လိုက်တဲ့အခါ switch သည် ဝင်လာတဲ့ frame ၏ source address ကိုကြည့်ပြီး ကွန်ပျူတာ B ၏ MAC address သည် (0000 2222 BBBB) ဖြစ်တယ်ဆိုတာကို ထောက်လှမ်းသိရှိနိုင်ပါလိမ့်မယ်။ ဤတွင်မှ frame တွေကိုလက်ခံရရှိသော port #2 နှင့် MAC (0000 2222 BBB) တို့ကို address table ထဲမှာ ထည့်သွင်းမှတ်သားထားလိုက်ပါတယ်။

ဤနည်းဖြင့် switch ၏ port တွေမှာ တစ်ဆင့်ထားသမျှသော device တို့၏ MAC တို့ကို ထောက်လှမ်းစုဆောင်းပြီး ဘယ် port ကနေသွားရင် ဘယ် MAC ကို ရောက်သလဲဆိုတာကို သိနိုင်မည့် MAC address table တစ်ခုတည်ဆောက်ခြင်းဖြစ်ပါတယ်။

MAC address table ဆောက်ထားတာက တော့ ဟုတ်ပါပြီ အကယ်၍ များ MAC table မဆောက်ရသေးခင် frame တွေကို ပို့မယ်ဆိုရင် switch တွေမှ ဘယ်လိုလုပ်ဆောင်မလဲ ဆိုတာမျိုး စဉ်းစားစရာ ရှိလာနိုင်ပါတယ်။ အဲဒီလို table ထဲမှာ MAC address တွေထည့်ရသေးခင်နှင့် ဝင်လာတဲ့ frame ထဲက destination address သည် MAC address table ထဲတွင် မရှိသေးတဲ့အခါမျိုးတွေမှာ switch သည် hub တွေကဲ့သို့ လုပ်ဆောင်ပါတယ်။

ဆိုရရင် switch သည် port တစ်ခုမှ ရောက်ရှိလာတဲ့ frame ကို ကျန် port များအားလုံးသို့ forward လုပ်ပေးပါတယ်။



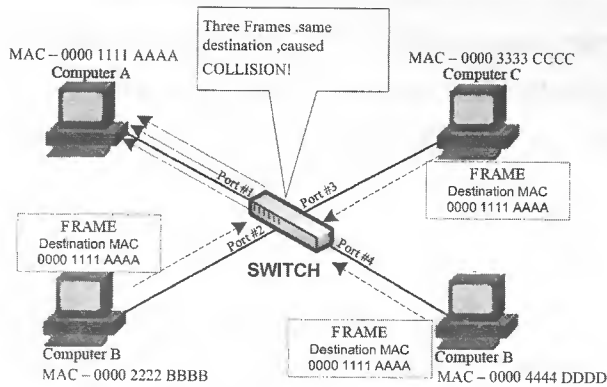
ပုံ (5.5)

ပုံမှာဖော်ပြထားသည့်အတိုင်းပင် switch သည် frame ကို port အားလုံးဆီသို့ဖြန့်ဝေလိုက်တဲ့အခါ ကွန်ပျူတာ B ၊ C ၊ D ဆီသို့ရောက်ရှိသွားပါတယ်။ ကွန်ပျူတာ B မှ reply လုပ်တဲ့အခါ (ACK ပြန်ပို့တဲ့အခါ) ၎င်း ကွန်ပျူတာ၏ MAC address ကို table ထဲသို့ထည့်သွင်းလိုက်ပါတယ်။ ဒါကြောင့် နောက်တစ်ကြိမ် ကွန်ပျူတာ B သို့ပို့သည့်အခါတိုင်း အားလုံးဆီသို့ forward လုပ်စရာမလိုတော့ပဲ ကွန်ပျူတာ B ရှိရာ port တစ်ခုတည်းဆီသို့သာဦးတည် forward လုပ်နိုင်ကြပါတယ်။

Switch Buffer

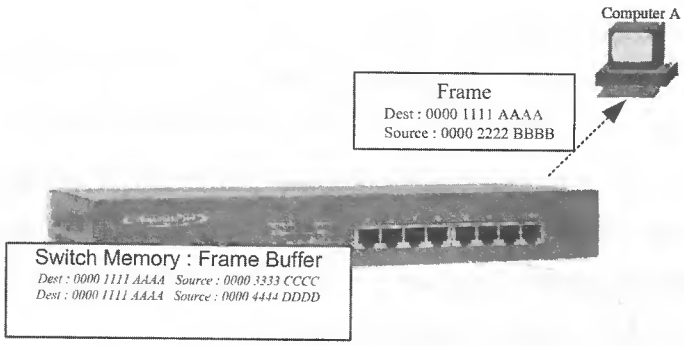
switch အသုံးပြုတဲ့ network တွေမှာဆိုရင် ကွန်ပျူတာများစွာကိုမှ တစ်ပြိုင်နက် transmit လုပ်နိုင်တယ်ဆိုတာကိုဥပမာပုံ (5.3) နှင့် တကွ ပြခဲ့ပြီးပါပြီ။ အဲဒီဥပမာဖြစ်စဉ်တုန်းက ကွန်ပျူတာ A မှ B သို့၊ ကွန်ပျူတာ D မှ C သို့ဆိုပြီး သူ့အတွဲနှင့်သူ သီးခြားစီပို့လွှတ်မှုဖြစ်စဉ်ကို မူတည်၍ဖော်ပြခဲ့ခြင်းဖြစ်ပါတယ်။ ယခုဖော်ပြမှာက ကွန်ပျူတာ A တစ်လုံးတည်းဆီသို့ ကျန်ကွန်ပျူတာ ၃ လုံးမှ တစ်ပြိုင်နက်ပေးပို့ကြမယ့် ဖြစ်စဉ်ကြောင့် ဘယ်လိုအကျိုးဆက်တွေဖြစ်လာနိုင်မလဲဆိုတာကိုဦးတည်မှာဖြစ်ပါတယ်။

ရှေ့မှာဖော်ပြခဲ့တဲ့ switch တွေရဲ့ပုံမှန်လုပ်ဆောင်မှုအတိုင်းသာဆိုရင် ကွန်ပျူတာ B ၊ C ၊ D သုံးလုံး စလုံးမှလာတဲ့ frame သုံးခုကို ကွန်ပျူတာသို့ တစ်ပြိုင်နက် လွှဲပေးမှာဖြစ်ပါတယ်။ ဒါဆိုရင် frame ၃ ခု တစ်ပြိုင်နက်ဆိုပြီး collision ဖြစ်ပြီလို့ဆိုနိုင်ပါတယ်။



ပုံ (5.6)

ဒါပေမယ့် တကယ့်လက်တွေ့မှာတော့ frame သုံးခုစလုံးကို ကွန်ပျူတာ A တံသို့ တစ်ပြိုင်နက် ပေးပို့ခြင်း ရှောင်ရှားရန် switch ထဲမှာ buffer ကိုထည့်သွင်းတည်ဆောက်ထားပါတယ်။ buffer ဆိုတာ တာတော့ frame တွေကို ယာယီသိုလှောင်သိမ်းထားပေးမည့် switch ထဲတွင်ရှိသော memory area တစ်ခု ဖြစ်ပါတယ်။ frame သုံးခုထဲကတစ်ခုကို ကွန်ပျူတာ A တံသို့ပေးပို့နေချိန်မှာ ကျန် နှစ်ခုကို buffer ထဲ ခေတ္တသိမ်းဆည်းထားပါတယ်။ ပထမ frame ကိုပို့ပြီးသွားပြီဆိုမှ ဒုတိယ frame ကို buffer ထဲက ထုတ်ယူပေးလို့ရပါတယ်။ နောက်ဆုံး တတိယ frame ပေါ့။ အဲဒီလို destination တူနေတဲ့ frame တွေကို လက်ခံရရှိပြီဆိုရင် buffer ထဲထည့်သွင်းပြီး တစ်ခုပြီးမှ တစ်ခု forward လုပ်ခြင်းဖြင့် collision ဖြစ်ခြင်းမှ တာကွယ်ပေးပါတယ်။



ပုံ (5.7)

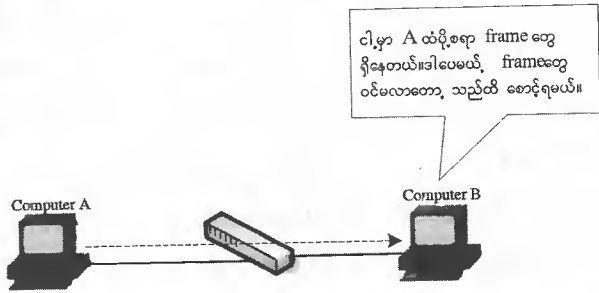
switch ရဲ့လုပ်ဆောင်မှု logic ကို အောက်ပါအတိုင်း မှတ်သားထားနိုင်ပါတယ်။

frame တစ်ခုကို လက်ခံရရှိတဲ့အခါ destination ethernet address ကိုကြည့်ရှုစစ်ဆေးပါတယ်။ အဲဒီ address သို့ရောက်ရှိနိုင်မည့် port တစ်ခုတည်းဆီသို့သာ ဆက်လက် forward လုပ်ပေးပါတယ်။

port တစ်ခုတည်းဆီသို့ frame များစွာ ပေးပို့ဖို့ရှိလာပြီဆိုရင် frame တစ်ခုကို အရင်ပို့ပြီး ကျန်တာတွေကို buffer ထဲ ခေတ္တထည့်သွင်းထိန်းသိမ်းထားပါတယ်။ ပြီးမှတစ်ခုချင်း ထုတ်ယူပေးပို့ပါတယ်။ collision မဖြစ်တော့သည့်အတွက် data ပို့လွှတ်မှု မြန်ဆန်ပြီး LAN performance ကို တိုးမြှင့်စေပါတယ်။

Using Full duplex

CSMA/CD logic အရ ကွန်ပျူတာမှ NIC သည် frame တစ်ခုအား ပေးပို့ခြင်းနှင့် ရယူခြင်းကို တစ်ပြိုင်နက် လုပ်လို့မရပါဘူး။ အောက်ပုံ (5.8) တွင်ကြည့်ပါ။ ကွန်ပျူတာ A မှ B ထံသို့ frame တစ်ခုပေးပို့နေပါတယ်။ ထို့အတူ ကွန်ပျူတာ B ဘက်ကလည်း frame တစ်ခုပေးပို့ဖို့ရှိနေပါတယ်။

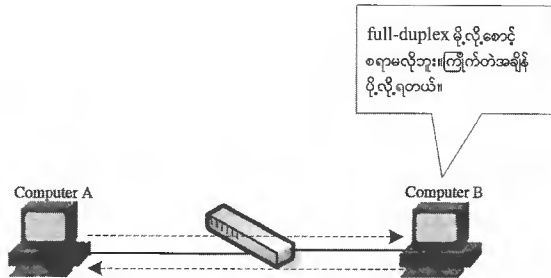


ပုံ (5.8)

ကွန်ပျူတာ B ဘက်မှ CSMA/CD ကိုလိုက်နာလုပ်ဆောင်မယ်ဆိုရင် လတ်တလော လက်ခံရယူနေခြင်း ပြီးဆုံးမှ မိမိပို့လိုတဲ့ frame ကို ပို့ရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာ တစ်ခုလောက်စဉ်းစားကြည့်ပါ။ ကွန်ပျူတာ B သည် ပို့စရာရှိတဲ့ frame တွေကို pin1 နှင့် pin2 တို့မှ ပေးပို့မှာဖြစ်သလို၊ switch ဘက်မှလည်း ကွန်ပျူတာ B ၏ pin3 နှင့် 6 တို့ထံသို့သာ ပေးပို့မှာဖြစ်ပါတယ်။ ဒါဆိုရင် physically အရပေးပို့ခြင်းနှင့် ရယူခြင်း တို့သည် သီးခြား ဝါယာများ ပေါ်မှာသာ လုပ်ဆောင်ကြမှာဖြစ်သည့်အတွက် ဘယ်လိုနည်းနှင့်မှ collision မဖြစ်နိုင်ပါဘူး။ ဒီဖြစ်စဉ်မှာ ကွန်ပျူတာ B မှပို့စရာအဆင့်သင့်ရှိသော်လည်း မပို့ရသေးခြင်းသည် CSMA/CD မှ ကွန်ပျူတာ B အားစောင့်ဆိုင်းခိုင်းသောကြောင့်ဖြစ်ပါတယ်။

ဒါဆိုရင် တစ်ခုလောက်စဉ်းစားကြည့်ရအောင်။ ကွန်ပျူတာ B ဘက်က NIC မှ CSMA/CD ကို ရပ်ဆိုင်းလိုက်ရင် ဘာတွေဖြစ်လာနိုင်မလဲ။ ဆိုရရင် CSMA/CD ကို disable လုပ်လိုက်တယ်ပေါ့။ အဲဒီလိုသာ ဆိုရင် ကွန်ပျူတာ B မှ NIC သည် frame ပေးပို့ရယူခြင်းများကို တစ်ပြိုင်နက် လုပ်ဆောင်နိုင်ပါလိမ့်မယ်။ သဘောကတော့ ကွန်ပျူတာ A မှလာတဲ့ frame တွေကို လက်ခံရယူနေစဉ်အတွင်းမှာပင် မိမိဘက်က ပို့စရာရှိတာကိုလည်း ပို့လာနိုင်ပါလိမ့်မယ်။ အဲဒီလို တစ်ချိန်တည်းမှာပင် အပို့အယူ တစ်ပြိုင်နက် လုပ်ဆောင် နိုင်ခြင်းကို full-duplex လို့ခေါ်ပါတယ်။

ဤတွင်မှ ဆက်ဆိုရရင် CSMA/CD logic အရ အချိန်တစ်ခုတည်းမှာ အပို့(သို့)အယူ တစ်မျိုးကိုသာ လုပ်ဆောင်ခြင်းသည် half duplexဖြစ်ပါတယ်။



ပုံ (5.9)

Auto Negotiation

network speed ပေါ်မူတည်ပြီး ethernet အမည်အမျိုးမျိုးကွဲပြားကြပါတယ်။ ဥပမာ NIC တစ်ခုသည် 10mbpsဖြင့်အလုပ်လုပ်တယ်ဆိုရင် ethernetဖြစ်ပါတယ်။ ထိုနည်းတူစွာပင် NICတစ်ခုသည် fast ethernetလို့ဆိုတာနှင့် 100mbpsနှုံးဖြင့်အလုပ်လုပ်တယ်လို့ရည်ညွှန်းနိုင်ပါတယ်။ အောက်ပါဇယားမှာဆိုရင် speed ပေါ်မူတည်ပြီး ကွဲပြားတတ်တဲ့ ethernetအခေါ်အဝေါ်များကို ယှဉ်တွဲဖော်ပြထားပါတယ်။

Ethernet Specifications

Common Name	IEEE Standard	Speed	Type of Cabling
Ethernet	802.3	10 Mbps	Both
Fast Ethernet	802.3u	100 Mbps	Both
Gigabit Ethernet	802.3z	1 Gbps	Optical
Gigabit Ethernet	802.3ab	1 Gbps	Copper
10 Gigabit Ethernet	802.3ae	10 Gbps	Optical

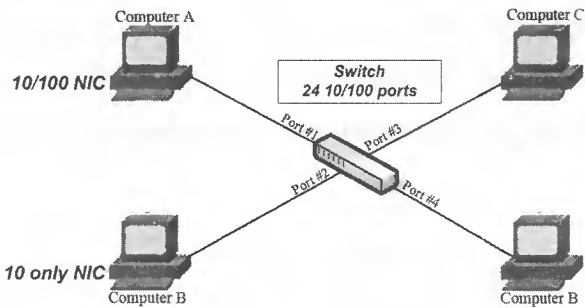
switchတွေသည် ethernet frame၏ headerထဲတွင်ပါသော information ပေါ်တွင်မှီတည်ပြီး လုပ်ဆောင်ကြခြင်းဖြစ်ပါတယ်။ ethernet မှသည် fast ethernet၊ gigabit ethernet အစရှိသဖြင့် ဧည့်သို့ပင် အဆင့်ဆင့်ဖွံ့ဖြိုးတိုးတက်လာခဲ့သော်လည်း အသုံးပြုသည့် headerများကတော့ အားလုံးအတူ တူပင် ဖြစ်ကြပါတယ်။ ဒါကြောင့် မည်သည့် speed ဖြင့် လုပ်ဆောင်နေစေကာမူ switchတွေရဲ့ forward လုပ်ခြင်း၊ table ဆောက်ခြင်းတို့သည် ပြောင်းလဲခြင်းမရှိပါဘူး။

အရေးကြီးတာက switch နှင့် NIC တို့ကြားမှာ လုပ်ဆောင်တဲ့ speed တူဖို့လိုပါတယ်။ ဆိုရရင် NIC ကနေ switch ဆီသို့ 10mbps နှုန်းဖြင့်ပို့မယ်ဆိုရင် switch ကနေ NIC ထံကိုလည်း 10mbps နှုန်းဖြင့်သာ ပို့ရပါမယ်။ အကယ်၍များ NIC က 10mbps ဖြင့်လုပ်ဆောင်ပြီး switch က 100mbps ဖြင့်လုပ်ဆောင်မယ် ဆိုရင် ဘယ်လိုမှ မဖြစ်နိုင်ပါဘူး။

ဒါဆိုရင် ဟိုးယခင်ကတည်းက မိမိမှာရှိနေသော 10mbps ထိသာ support လုပ်တဲ့ NIC တပ်ထားသည့် ကွန်ပျူတာကို ယနေ့ 100mbps ဖြင့်လုပ်ဆောင်နေသော network တွေမှာ အသုံးပြု၍ မရနိုင်တော့ဘူးလားလို့ မေးစရာရှိလာနိုင်ပါတယ်။

အဲဒီပြဿနာကို ပြေလည်စေရန်အတွက် IEEE မှ auto-negotiation ကိုဖော်ဆောင်ခဲ့ပြီးသား ဖြစ်ပါတယ်။ auto-negotiation သည် switch port တစ်ခုစီနှင့် NIC တို့ကြားမှာ ဘယ်လောက် speed ဖြင့်လုပ်ဆောင်ကြမလဲဆိုတာကို အလိုလျှောက်ညှိနှိုင်းပေးပါတယ်။ အဲဒီလိုညှိနှိုင်းတဲ့နေရာမှာ speed အပြင် full duplex လား၊ half duplex လား ဆိုတာကိုပါ ထည့်သွင်းညှိနှိုင်းပေးမှာဖြစ်ပါတယ်။

auto-negotiation လုပ်ဆောင်ရန်အတွက် switch နှင့် NIC တို့သည် speed အမျိုးမျိုးတို့ကို support လုပ်ဖို့လိုပါတယ်။ ယနေ့ ဈေးကွက်အတွင်း ဝယ်ယူနိုင်တဲ့ switch နှင့် NIC တို့သည် 10/100 များ ဖြစ်ပါတယ်။ သဘောကတော့ 10mbps နှင့် 100mbps တို့ထဲက တစ်မျိုးမဟုတ်တစ်မျိုးဖြင့် လုပ်ဆောင် နိုင်တယ်လို့ ဆိုလိုခြင်းဖြစ်ပါတယ်။



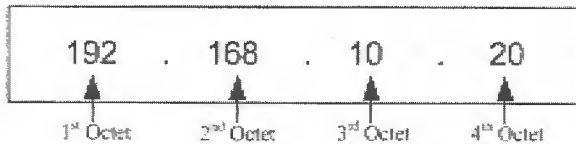
ပုံ (5.10)

ဖော်ပြပါပုံ (5.10) တွင်ကြည့်ပါ။ ကွန်ပျူတာ A မှာ တပ်ဆင်ထားတဲ့ NIC သည် 10/100 card ဖြစ်ပါတယ်။ ကွန်ပျူတာ B မှာတပ်ဆင်ထားတဲ့ NIC ကတော့ 10mbps တစ်မျိုးကိုသာ support လုပ်သော NIC ဖြစ်ပါတယ်။ ဒါဆိုရင် ကွန်ပျူတာ A နှင့် switch တို့သည် auto-negotiation လုပ်ပြီး သူတို့နှစ်ဦးစလုံးရဲ့ အမြင့်ဆုံး speed ဖြစ်တဲ့ 100mbps, full-duplex ဖြင့်လုပ်ဆောင်ကြပါလိမ့်မယ်။ ကွန်ပျူတာ B မှ တပ်ထားသည့် NIC သည် 10mbps တစ်မျိုးတည်းဖြင့်သာ လုပ်ဆောင်နိုင်ပြီး auto-negotiation ကို support မလုပ်ပါဘူး။ ဒါကြောင့် ကွန်ပျူတာ B နှင့် switch တို့ကြားမှာ 10mbps, half duplex ဖြင့်သာ လုပ်ဆောင်ပါလိမ့်မယ်။

Network Addressing & IP Routing

TCP/IP ရှိ ကွန်ပျူတာ NIC တိုင်းတွင် physical နှင့် logical ဆိုပြီး address နှစ်မျိုးစီ ရှိကြတယ်ဆိုတာကို သိခဲ့ကြပြီး ဖြစ်ပါလိမ့်မယ်။ အနည်းငယ် ပြန်ပြောရရင် physical address (MAC) ကို NIC ထုတ်လုပ်စဉ် ကတည်းက စက်ရုံမှာ အသေထည့်သွင်း သတ်မှတ်ပြီးသား ဖြစ်ပါတယ်။ logical address တွေကွန်ပျူတာမှာ အသုံးပြုသည့် protocol ၏ စည်းကမ်းသတ်မှတ်ချက်နှင့် အညီ user တို့မှလိုသလို ပြောင်းလဲသတ်မှတ်ပေးနိုင်တဲ့ address မျိုးဖြစ်ပါတယ်။ TCP/IP network တွေမှာဆိုရင် internet protocol သည် logical addressing ကိုတာဝန်ယူရတဲ့ protocol ဖြစ်ပါတယ်။ ဒါကြောင့် TCP/IP ကို အခြေခံသော network တိုင်းတွင် logical address ကို IP address ရယ်လို့ ခေါ်ဆိုကြခြင်း ဖြစ်ပါတယ်။

IP address တစ်ခုကို 1st octet၊ 2nd octet၊ 3rd octet နှင့် 4th octet ဆိုပြီး လေးပိုင်း ဖိတ်ပိုင်းထားပါတယ်။ octet တစ်ခုစီသည် 8 bit နှုံးဖြင့် IP address တစ်ခုလုံးအတွက် 32 bit (4 byte) ဖြစ်ပါတယ်။ IP address တွေကို ရေးသားတဲ့နေရာမှာ အလွယ်တကူမှတ်သား အသုံးပြုနိုင်စေရန် decimal value များကို အသုံးပြုကြပါတယ်။



ဒီနေရာတွင် ဖော်ပြပါ IP address ကို ဥပမာထားပြီး decimal မှ binary သို့ ပြောင်းလဲပုံကို အနည်းငယ် တွက်ပြလိုပါတယ်။

Position in a binary number (power of two)

2 ⁷	2 ⁶	2 ⁵	2 ⁴	2 ³	2 ²	2 ¹	2 ⁰
128	64	32	6	8	4	2	1

(128+64) ဆိုရင် 192 ဖြစ်ပါလိမ့်မယ်။ ဤတွင်မှ 1st Octet ဖြစ်သည်။ 192 အတွက် binary value သည် အောက်ပါအတိုင်း ဖြစ်လာပါမည်။

	128	64	32	16	8	4	2	1
Binary	1	1	0	0	0	0	0	0
Decimal	(128x1)+(64x1)+(32x0)+(16x0)+(8x0)+(4x0)+(2x0)+(1x0)							
	128 + 64							
	192							

(128+32+8)ဆိုရင် 168 ဖြစ်ပါလိမ့်မယ်။ ဤတွင်မှ 2nd Octet ဖြစ်သည်။ 168အတွက် binary valueသည် အောက်ပါအတိုင်းဖြစ်လာပါမည်။

	128	64	32	16	8	4	2	1
Binary	1	0	1	0	1	0	0	0
Decimal	$(128 \times 1) + (64 \times 0) + (32 \times 1) + (16 \times 0) + (8 \times 1) + (4 \times 0) + (2 \times 0) + (1 \times 0)$							
	128	+	32	+	8			
	168							

3rd Octet ဖြစ်သည့် 10 အတွက် binary valueသည်

Binary	0	0	0	0	1	0	1	0
--------	---	---	---	---	---	---	---	---

4th Octet ဖြစ်သည့် 20 အတွက် binary valueသည်

Binary	0	0	0	1	0	1	0	0
--------	---	---	---	---	---	---	---	---

ဤတွင်မှ dottec decimal ဖြင့်ရေးသားထားသည့် 192.168.10.20 သည် အောက်ဖော်ပြပါ binary number တို့ဖြစ်လာပါတယ်။

1100000 101010000 00001010 00010100

Ip address တွေရဲ့ အဓိကရည်ရွယ်ရင်းကတော့ network တစ်ခုမှာရှိနေတဲ့ ကွန်ပျူတာတွေသည် မိမိနှင့်မကူတဲ့အခြား network တစ်ခုမှာရှိနေတဲ့ ကွန်ပျူတာတို့နှင့် အပြန်အလှန် communicate လုပ်နိုင်ကြစေရန် ဖြစ်ပါတယ်။ ဤတွင်မှ network တူတယ်၊ မတူဘူး ဘယ်လိုခွဲခြားသိနိုင်မလဲဆိုတာကို ဆက်လက်ရှင်းပြသွားပါမယ်။

IP address တစ်ခုမှာဆိုရင် network ID နှင့် host ID ဆိုပြီး အပိုင်း ၂ပိုင်းရှိပါတယ်။ network တစ်ခုတည်း အောက်မှာရှိတဲ့ ကွန်ပျူတာတွေသည် network ID တူရပါမယ်။ host ID တူလို့ မရပါဘူး။ host ID သည် ကွန်ပျူတာတစ်လုံးစီအတွက် သီးသန့်ကိုယ်ပိုင် အမှတ်ဖြစ်ပါတယ်။

ဥပမာ လမ်းတစ်လမ်း မှာရှိနေတဲ့ အိမ်တွေကို လိပ်စာသတ်မှတ်ပေးမယ်ဆိုပါတော့။ ဒါဆိုရင် အိမ်တစ်အိမ်ရဲ့ လိပ်စာကို "လမ်း ၅၀၊ အိမ်နံပါတ် ၁" လို့ပေးပြီး တာနှင့်အခြားအိမ်တွေကို "လမ်း ၅၀၊ အိမ်နံပါတ် ၂" "လမ်း ၅၀၊ အိမ်နံပါတ် ၃" အစရှိသဖြင့် တစ်လုံးနှင့် တစ်လုံး အိမ်နံပါတ် မတူအောင် ပေးရပါမယ်။ သို့သော် လမ်း ၅၀ သည် group name ဖြစ်သည့်အတွက် ဤလမ်းအတွင်းရှိ အိမ်လိပ်စာတိုင်း၏ ရှေ့မှာ တစ်စိတ်တစ်ပိုင်း နေရာယူပါတယ်။ ပြီးမှ အိမ်တစ်လုံးချင်းစီအတွက် နံပါတ်စဉ် သတ်မှတ်ရပါတယ်။ သို့မှသာ "လမ်း ၅၀၊ အိမ်နံပါတ် ၁" လို့ လိပ်မူလိုက်တာနှင့် ဤလမ်း၊ ဤအိမ်သို့ ဆိုက်ဆိုက် မြိုက်မြိုက်

နောက်နိုင်မှာဖြစ်ပါတယ်။ ဤ ဥပမာကို IP address တို့နှင့် ယှဉ်ကြည့်မယ်ဆိုရင် လမ်း ၅၀ သည် network ID ဖြစ်ပြီး နောက်က အိမ်နံပါတ်တွေသည် host ID ဖြစ်ပါလိမ့်မယ်။

IP address တစ်ခုကို ကြည့်လိုက်တာနှင့် ဘယ်ဟာက network ID၊ ဘယ်ဟာက host ID လဲဆိုတာကို network class ပေါ်မူတည်ပြီး ခွဲခြားနိုင်ပါတယ်။ အဓိကအားဖြင့် class A ၊ class B ၊ class C ဆိုပြီး network class သုံးမျိုးရှိပါတယ်။ ထို network class တွေသည် IP address ၏ 1st octet ထဲမှ ကိန်းဂဏန်းပေါ် မူတည်ပြီး ကွဲပြားကြခြင်း ဖြစ်ပါတယ်။

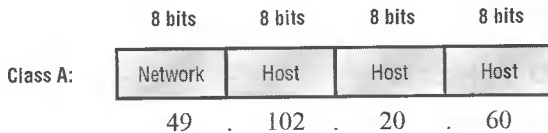
Commonly used TCP/IP classes

Network Class	Beginning Octet	Number of Networks	Maximum Addressable Hosts per Network
A	1-126	126	16,777,214
B	128-191	>16,000	65,534
C	192-223	>2,000,000	254

ပုံ (6.2)

Class A Address

IP address တစ်ခု၏ 1st octet ထဲမှ ကိန်းဂဏန်းသည် 1-126 အတွင်းမှ တစ်ခုခုဖြစ်မယ်ဆိုရင် class A ဖြစ်ပါတယ်။ class A address တစ်ခု၏ 1st octet သည် network ID ဖြစ်ပြီး ကျန် octet သုံးခုတို့သည် host ID ဖြစ်ကြပါတယ်။ ဒါကြောင့် class A ၏ တည်ဆောက်ပုံသည် အောက်ပါအတိုင်း ဖြစ်လာပါမည်။



ပုံ (6.3)

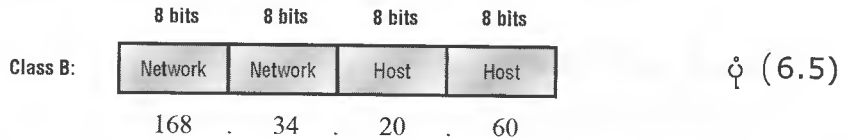
ဥပမာအနေနှင့် 49.102.20.60 ဆိုတဲ့ IP address တစ်ခု၏ network နှင့် host ID တို့ကို ခွဲကြည့်ရအောင်။ ပထမဦးစွာ ဘယ် network class အောက်မှာ အကျုံး ဝင်နေသလဲဆိုတာကို အရင် သိအောင် လုပ်ရပါမယ်။ ရှေ့ဆုံး 1st octet ထဲက '49' သည် 1-126 ကြားရှိသဖြင့် ၎င်း IP address သည် class A ဖြစ်ပါတယ်။ ဤတွင်မှ '49' သည် network ID ဖြစ်ပြီး '102.20.60' သည် host ID ဖြစ်ပါတယ်။

နောက်ထပ် class A address တစ်ခုကို ကြည့်ရအောင်။ ဥပမာ 32.10.10.70 ဆိုပါတော့။ ရှေ့ဆုံးက 32 သည် 1-126 ကြားရှိသဖြင့် ၎င်း address သည်လည်း class A ဖြစ်ပါတယ်။ ဤတွင်မှ 32 သည် network ID ဖြစ်ပြီး 10.10.70 သည် host ID ဖြစ်ပါတယ်။ ဖော်ပြခဲ့တဲ့ IP address ယခုတို့သည် class A ချင်းတူသော်လည်း network ID ချင်း မတူကြသည့်အတွက် network မတူကြပါဘူး။ အောက်ဖော်ပြပါ IP address တွေကတော့ network တစ်ခုတည်း အောက်မှာရှိတဲ့ ဥပမာ class A IP address တွေပဲဖြစ်ကြပါတယ်။

Network ID	Host ID	
49	102 . 20 . 60	ဝံ (6.4)
49	20 . 201 . 63	
49	10 . 22 . 88	
49	2 . 253 . 25	

Class B Address

IP addressတစ်ခု၏ 1st octetထဲမှ ကိန်းဂဏန်းသည် 128-191အတွင်း ဖြစ်မယ်ဆိုရင် ၎င်း addressသည် class Bဖြစ်ပါတယ်။ class B addressတစ်ခု၏ 1stနှင့် 2nd octetနှစ်ခုတို့သည် network ID ဖြစ်ကြပါတယ်။ ဒါ့ကြောင့် class B၏တည်ဆောက်ပုံသည် အောက်ပါအတိုင်း ဖြစ်လာပါမည်။



အောက်ဖော်ပြပါ IP addressရှိသော ကွန်ပျူတာတွေသည် networkတစ်ခုတည်းအောက်မှာ ရှိကြပါတယ်။

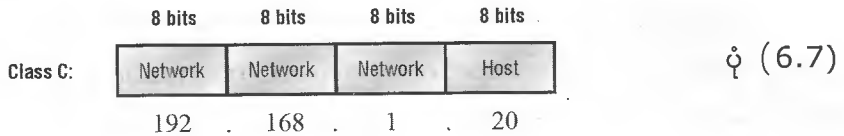
Network ID	Host ID	
168 . 34	20 . 60	ဝံ (6.6)
168 . 34	201 . 63	
168 . 34	22 . 88	
168 . 34	253 . 25	

ဤဥပမာ IP addressတွေတွင် ဘုံအဖြစ်ပါရှိသော 1stနှင့် 2nd octetကိုကိုယ်စားပြုသော 168.34 သည် network IDဖြစ်ပါတယ်။ နောက်က 3rdနှင့် 4th octetတို့သည် host IDကိုကိုယ်စားပြုပါတယ်။

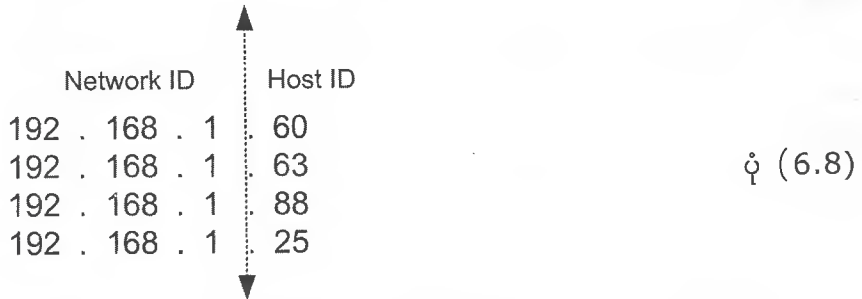
Class C address

IP addressတစ်ခု၏ 1st octetထဲမှ ကိန်းဂဏန်းသည် 192-223အတွင်း ဖြစ်မယ်ဆိုရင် ၎င်း addressသည် class Cဖြစ်ပါတယ်။ class C addressတစ်ခု၏ 1st၊ 2nd၊ 3rd octetသုံးခုတို့သည် network IDဖြစ်ပြီး ကျန် 4th octetတစ်ခုတည်းသာလျှင် host IDဖြစ်ပါတယ်။

ဒါကြောင့် class C ၏ တည်ဆောက်ပုံသည် အောက်ပါအတိုင်း ဖြစ်လာပါမည်။



အောက်ဖော်ပြပါ IP address ရှိသော ကွန်ပျူတာတွေသည် network တစ်ခုတည်းအောက်မှာ ရှိပါတယ်။



ဤဥပမာ IP address တွေတွင် ဘုံအဖြစ်ပါရှိသော 1st, 2nd, 3rd octet တို့ကို ကိုယ်စားပြုသည့် 192.168.1 သည် network ID ဖြစ်ပြီး နောက်က 4th octet ကို ကိုယ်စားပြုသော ကိန်းဂဏန်းတွေသည် host ID ဖြစ်ပါတယ်။

Subnet Mask

subnet mask သည်လည်း IP address တစ်ခု၏ ဘယ်အပိုင်းသည် network ID၊ ဘယ်အပိုင်းသည် host ID ဆိုတာကို ခွဲခြားပေးပါတယ်။ IP address တွေကဲ့သို့ပင် subnet mask တို့ကို octet လေးခု 32 bit ဖြင့်ဖွဲ့စည်းထားပြီး dotted decimal ကိန်းဂဏန်းများဖြင့်ပင် ဖော်ပြကြပါတယ်။ subnet mask သည်လည်း network class ပေါ်မူတည်ပါတယ်။ ဒါကြောင့် IP address ၏ 1st octet ထဲမှကိန်းဂဏန်းကို ဖတ်ပြီး class A လား၊ B လား၊ C လားဆိုတာကို အရင်သိအောင် လုပ်ရပါမယ်။ အောက်ဖော်ပြပါ ဇယားမှာဆိုရင် 1st octet၊ network class နှင့် subnet mask တို့ရဲ့ဆက်သွယ်ချက်တွေကို ဖော်ပြထားပါတယ်။

Default Subnet Masks for Standard IP Address Classes

Class	Subnet Mask Bit Pattern	Subnet Mask
A	11111111 00000000 00000000 00000000	255.0.0.0
B	11111111 11111111 00000000 00000000	255.255.0.0
C	11111111 11111111 11111111 00000000	255.255.255.0

ပုံ (6.9)

IP Routing

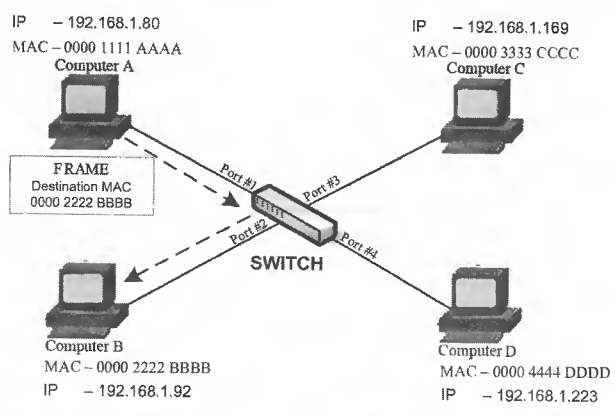
ကွန်ပျူတာတစ်လုံးမှ ပေးပို့လိုက်တဲ့ data တွေသည် router တွေကိုဖြတ်ပြီး ရည်ရွယ်ရာ ကွန်ပျူတာဆီသို့ ရောက်ရှိခြင်း ဖြစ်စဉ်ကို routing လို့ခေါ်ပါတယ်။ routing လုပ်ဖို့ရန် router (device) လိုပါတယ်။ ထို့အတူ "router မရှိတဲ့ network တစ်ခုမှာ routing လည်းမရှိ" လို့မှတ်သားထားနိုင်ပါတယ်။ router သည်လည်း switch ကဲ့သို့ packet forwarding device တစ်မျိုးဖြစ်ပါတယ်။ ဒါပေမယ့် မတူတဲ့အချက်က switch တွေသည် MAC address တွေကိုအခြေခံ၍ packet တွေကို forward လုပ်ခြင်း ဖြစ်ပြီး router တွေကတော့ network ID အပေါ်အခြေခံပြီး forward လုပ်ကြမှာဖြစ်ပါတယ်။

ကွန်ပျူတာတစ်လုံးနှင့် တစ်လုံးတို့ data အပြန်အလှန် ပို့ကြတိုင်း routing လုပ်ဖို့ရန် လိုအပ် မလိုအပ်ဆိုတာကို internet protocol သည် packet ထဲမှ IP header ထဲတွင်ရှိသော source နှင့် destination IP address တို့ကိုကြည့်ပြီး ဆုံးဖြတ်မှာ ဖြစ်ပါတယ်။ ဘယ်လိုအခြေအနေမှာ routing လုပ်ဖို့ လိုအပ်တယ်။ ဘယ်လိုအခြေအနေမှာတော့ မလိုအပ်ဘူးဆိုတာကို လေ့လာကြည့်ရအောင်။

ပေးပို့သည့်ကွန်ပျူတာနှင့် လက်ခံမည့် ကွန်ပျူတာတို့၏ network ID သည် အတူတူပင် ဖြစ်ကြမယ် ၊ တစ်နည်းဆိုရရင် ၎င်းကွန်ပျူတာနှစ်လုံးစလုံးသည် same network ထဲမှာ ရှိမယ်ဆိုရင် routing မလိုပါဘူး။

network ID မတူတဲ့ ကွန်ပျူတာတွေ (ဝါ) same network မဟုတ်ကြတဲ့ ကွန်ပျူတာ တွေ အပြန်အလှန် communicate လုပ်ဖို့လိုလာတဲ့အခါ routing လိုပါလိမ့်မယ်။

ပထမဦးစွာ routing မလိုတဲ့ ဖြစ်စဉ်ကို ဖော်ပြပါမယ်။ တစ်နည်းဆိုရရင် same network ထဲမှာ ရှိတဲ့ ကွန်ပျူတာတွေ တစ်လုံးနှင့်တစ်လုံး data ပေးပို့ ဖလှယ်ကြတဲ့နေရာမှာ လုပ်ဆောင်ပုံ အဆင့်ဆင့် ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါပုံ (6.10) မှာဆိုရင် ကွန်ပျူတာ A၊ B၊ C နှင့် D တို့သည် same network တစ်ခုတည်းမှာ ရှိကြပါတယ်။ ဤတွင်မှ ကွန်ပျူတာ A မှ B သို့ data ပေးပို့တဲ့ ဖြစ်စဉ်ကို ကြည့်ရအောင်။



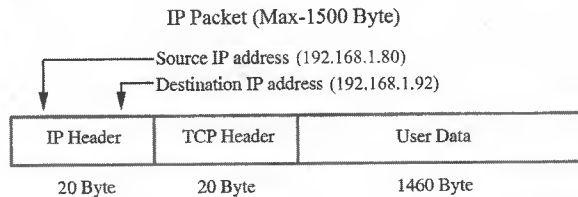
ပုံ (6.10)

step1) Segmentation

ကွန်ပျူတာ A မှ TCP သည် ပို့လိုတဲ့ data တွေကို အပိုင်းငယ်လေးများ ဖြစ်အောင် စိတ်ပိုင်းပြီး အပိုင်းငယ်တစ်ခုစီ၏ ရှေ့တွင် TCP header ကိုထည့်သွင်းပါတယ်။ TCP header ထည့်သွင်းပြီး၍ ရလာမည့် segment တစ်ခုစီကို addressing နှင့် routing လုပ်ရန်အတွက် IP ထံသို့ လွှဲပေးလိုက်ပါတယ်။

step2) IP packets

ကွန်ပျူတာ A မှ internet protocol သည် TCP segment တစ်ခုစီ၏ ရှေ့တွင် IP header ကိုထည့်သွင်းပြီး IP packet များအဖြစ်ဖန်တီးယူပါတယ်။ ၎င်း packet ထဲတွင် source နှင့် destination IP address တို့ပါရှိပါတယ်။ source နေရာတွင် ကွန်ပျူတာ A ၏ IP address (192.68.1.80) နှင့် destination နေရာတွင် ကွန်ပျူတာ B ၏ IP address (192.168.1.92) တို့ဖြစ်ကြပါတယ်။



ပုံ (6.11)

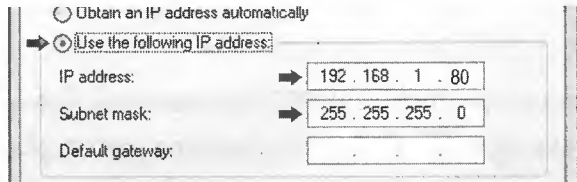
step3) ANDing

packet တွေအဖြစ် ဖန်တီးပြီးတဲ့အခါ destination IP address (ကွန်ပျူတာ B ၏ address) သည် local လား၊ remote လားဆိုတာကို ကွန်ပျူတာ A ၏ internet protocol မှ ဆုံးဖြတ်ပေးရပါတယ်။ ဆိုရရင် ကွန်ပျူတာ B သည် ကွန်ပျူတာ A နှင့် network တစ်ခုတည်းလား သို့မဟုတ် မတူတဲ့အခြား network လားဆိုတာကို တွက်ချက်ဆုံးဖြတ်ရန်ဖြစ်ပါတယ်။ internet protocol သည် IP address နှင့် subnet mask တို့ကို ANDing လုပ်ပြီး ဘယ်ဟာက network ID၊ ဘယ်ဟာက host ID ဆိုတာကို ခွဲခြားပါတယ်။ ANDing ပြီး၍ ရလာမည့် အဖြေသည် network ID ဖြစ်ပါတယ်။

ANDing လုပ်ရန်အတွက် binary value နှစ်ခုတို့ကို နှိုင်းယှဉ်ရပါတယ်။ value ၂ခုစလုံးသည် 1 ဖြစ်မယ်ဆိုရင် ANDing လုပ်ပြီးရလာမည့်အဖြေသည် 1 ဖြစ်ပါတယ်။ အကယ်၍ တစ်ခု (သို့) ၂ခုစလုံးသည် 0 ဖြစ်ပါက အဖြေသည် 0 ဖြစ်ပါတယ်။ ဥပမာအနေနှင့် IP address (192.168.1.92) နှင့် subnet mask (255.255.255.0) တို့ကို ANDing လုပ်ကြည့်ရအောင် - - -

	192	.168	.1	.92
IP Address	: 11000000	10101000	00000001	01011100
Subnet Mask	: 11111111	11111111	11111111	00000000
Network ID	: 11000000	10101000	00000001	00000000
	192	.168	.1	.0

ဤနည်းဖြင့် internet protocol သည် source နှင့် destination IP address တို့ကို တွက်ချက်ပြီး လာမည့်အဖြေနှစ်ခုတို့ကို တိုက်ဆိုင်စစ်ဆေးပါလိမ့်မည်။ တူတယ်ဆိုရင် ကွန်ပျူတာ A၊ B နှစ်လုံးစလုံးသည် network တစ်ခုတည်းအတွင်းမှာ ရှိတယ်ဆိုတာ သိရှိပြီး routing လုပ်ရန်မလိုဟု ဆုံးဖြတ်ပါလိမ့်မည်။ အောက်ဖော်ပြပါပုံကတော့ Windows XP တွင် NIC တစ်ခုအတွက် ထည့်သွင်းထားသော IP address နှင့် subnet mask တို့ဖြစ်ပါတယ်။

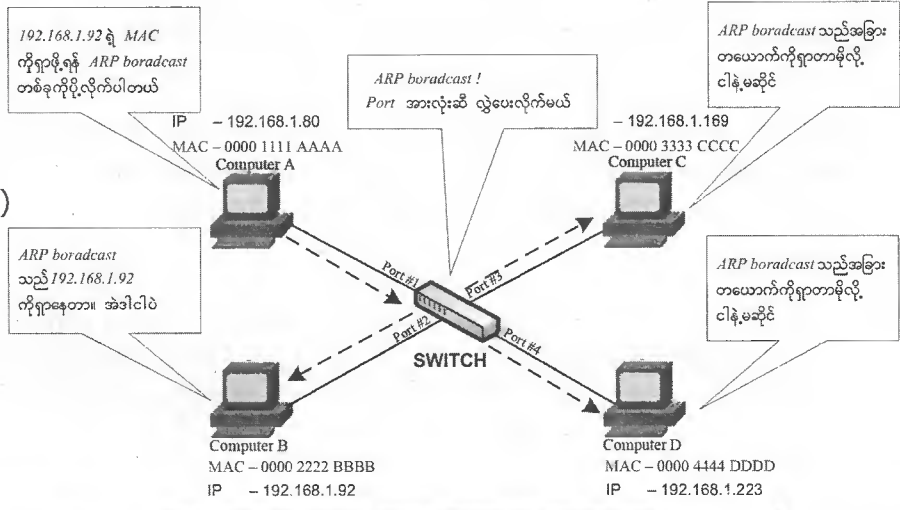


step4) MAC address

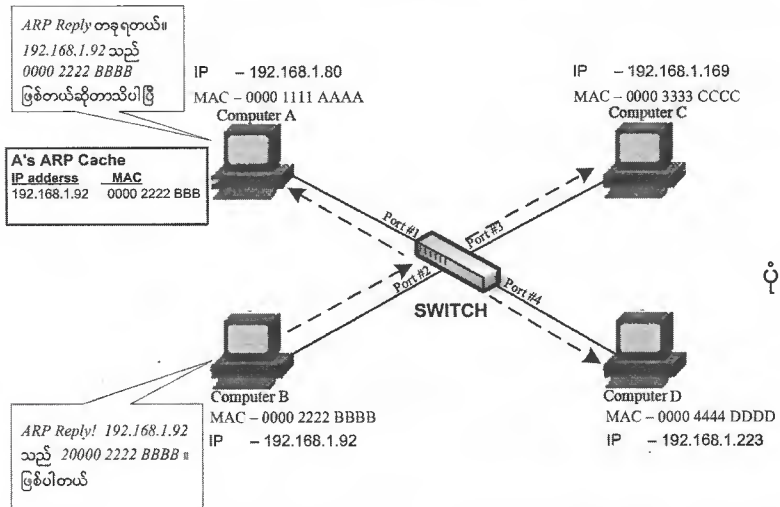
packet တွေကို ဒီအတိုင်းပို့လို့ မရပါဘူး။ packet တွေရဲ့ရှေ့မှာ header နှင့် နောက်မှာ trailer တို့ကို ထည့်သွင်း၍ ethernet frame တစ်ခုအဖြစ် တည်ဆောက်ပြီးမှ ပို့လို့ရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာ သိဖို့ရန်အရေးကြီးလာတာက network တစ်ခုတည်းမှာရှိတဲ့ ကွန်ပျူတာတွေချင်း hardware address (MAC) ဖြင့်သာ communicate လုပ်တယ်ဆိုတာကို နားလည်ထားဖို့လိုပါလိမ့်မယ်။ ဒါကြောင့် packet မှသည် frame အဖြစ်ပြောင်းပြီး ပေးပို့ဖို့ရန် ကွန်ပျူတာ B ၏ MAC address သိကို သိရပါမယ်။

ကွန်ပျူတာတစ်လုံးသည် same network ထဲမှာရှိတဲ့ IP သိပြီးသား အခြားကွန်ပျူတာတစ်လုံး၏ MAC ကို သိလိုတဲ့အခါ Address Resolution Protocol ကို အသုံးပြုကြပါတယ်။ ဤဖြစ်စဉ်မှာဆိုရင် ကွန်ပျူတာ A သည် ကွန်ပျူတာ B ၏ MAC ကို ရရန်အတွက် ARP ကို အသုံးပြုပြီး message တစ်ခုကို network ပေါ်သို့ broadcast လုပ်လိုက်ပါလိမ့်မယ်။ အဲဒီ ARP broadcast ကို နားလည်လွယ်အောင် ပြောရရင် "IP address 192.168.1.92 ရှိသော ကွန်ပျူတာ ခင်ဗျား ကျေးဇူးပြု၍ သင့်၏ MAC address အား ကျွန်ုပ်တို့ပေးပါ" ဟူသော message မျိုးဖြစ်ပါတယ်။ ဤတွင်မှ IP address 192.168.1.120 ရှိသော ကွန်ပျူတာ B သည် ၎င်း၏ MAC ကို ကွန်ပျူတာ A ထံသို့ ပို့ပေးပါလိမ့်မယ်။

ပုံ (6.12)



ကွန်ပျူတာ A သည် ရရှိလာမယ့် ကွန်ပျူတာ B ၏ MAC address နှင့် IP address တို့ကို ARP cache လို့ခေါ်တဲ့ database ထဲမှာ ယှဉ်တွဲသိမ်းဆည်းပါလိမ့်မယ်။ အဲဒီလို သိမ်းဆည်းထားခြင်းဖြင့် နောက်တစ်ခါ ကွန်ပျူတာ B နှင့် ဆက်သွယ်စရာရှိလာပြီဆိုရင် ARP broadcast လုပ်စရာ မလိုပဲ ကွန်ပျူတာ B ၏ MAC ကို ARP cache ထဲမှ အဆင်သင့်ယူသုံးနိုင်ပါလိမ့်မယ်။

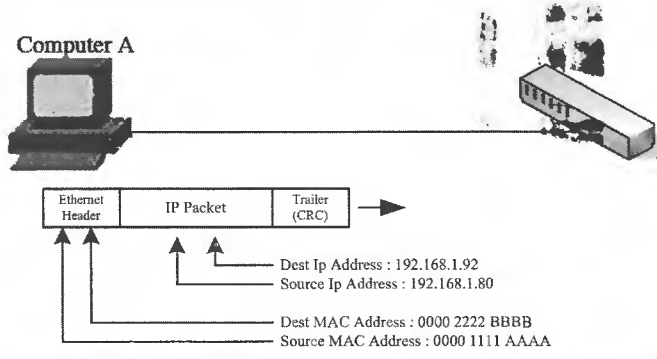


ပုံ (6.13)

မှတ်ချက်။ ။ command windows တွင် c:\>arp-a ဟုရိုက်ပါက ARP cache ထဲမှာရှိနေတဲ့ information တွေကိုဖော်ပြပါလိမ့်မယ်။

step5) Framing

ကွန်ပျူတာ B ရဲ့ MAC address ကိုရပြီဆိုရင် ethernet frame တစ်ခုအဖြစ်သို့ စတင် တည်ဆောက်မှာဖြစ်ပါတယ်။ ၎င်း frame ရဲ့ header ထဲမှာ အဓိကအားဖြင့် ကွန်ပျူတာ A ၏ MAC၊ ကွန်ပျူတာ B ၏ MAC နှင့် frame အဆုံး FCS field ထဲမှာ CRC value (cyclic redundancy check) တို့ပါရှိပါလိမ့်မယ်။ ပြီးပြည့်စုံသော frame တစ်ခုဖြစ်ပြီး သွားတဲ့အခါ bit များအဖြစ်ဖြင့် twisted pair cable ပေါ်သို့ တင်ပေးလိုက်ပါမယ်။



ပုံ (6.14)

step6) Switch Address Table

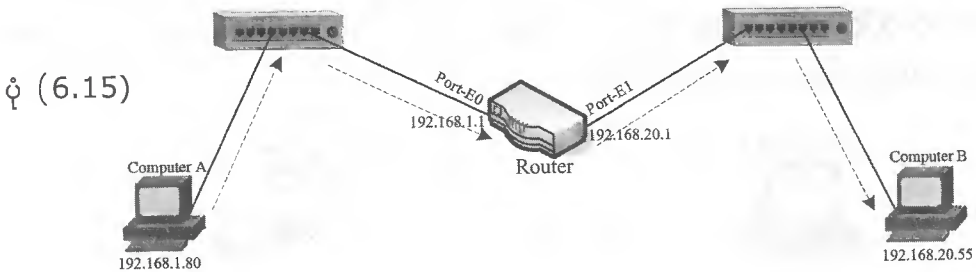
ကွန်ပျူတာ A မှ ပို့လိုက်တဲ့ bit တွေသည် cable ပေါ်မှတစ်ဆင့် switch ထံသို့ရောက်ရှိလာပါတယ်။ switch သည် bit တွေကို လက်ခံရယူပြီး frame အဖြစ်သို့ ပြန်လည်တည်ဆောက်ယူပါတယ်။ frame တစ်ခုအဖြစ်ရရှိပြီဆိုတာနှင့် destination MAC ကိုဖတ်ပြီး (switch table) ထဲမှာ တိုက်ဆိုင်စစ်ဆေးရှာဖွေပါလိမ့်မယ်။ တွေ့ပြီဆိုရင် frame ကိုကွန်ပျူတာ B တပ်ဆင်ထားရာ port ဆီသို့ လွှဲပေးလိုက်ပါတယ်။ ထိုမှတစ်ဖန် bit အဖြစ်ဖြင့် cable ပေါ်မှတစ်ဆင့် ကွန်ပျူတာ B ထံသို့ရောက်သွားပါလိမ့်မယ်။

step7) Cyclinc Redudancy Check

ကွန်ပျူတာ B မှ NIC သည် ဝင်လာတဲ့ bit တွေကို frame အဖြစ်သို့ ပြန်လည်တည်ဆောက်ယူပါတယ်။ frame အဖြစ်ရရှိပြီဆိုတာနှင့် header နှင့် data တို့ကို ပုံသေနည်း တစ်ခုထဲ ထည့်ပြီး တွက်ထုတ်ပါလိမ့်မယ်။ ရလာမည့် value နှင့် trailer FCS ထဲမှာပါလာတဲ့ value တို့ကို တိုက်ဆိုင်စစ်ဆေးပါတယ်။ မိမိတွက်ထားတဲ့ အဖြေနှင့် မတူဘူးဆိုရင် frame ကို စွန့်ပစ်ဖယ်ရှား ပါလိမ့်မယ်။ တူတယ်ဆိုမှ frame ကို လက်ခံရယူပါလိမ့်မယ်။ ဒါဆိုရင်ကွန်ပျူတာ A မှ B သို့ data ပေးပို့မှုဖြစ်စဉ် အောင်မြင်ပြီးဆုံးသွားပြီလိုဆိုနိုင်ပါပြီ။

📌 Sending Data to Different Network

ယခုဆက်လက်ပြီး routing လိုတဲ့ဖြစ်စဉ်ကိုဖော်ပြပါမယ်။ တစ်နည်းဆိုရင် network ID မတူတဲ့ ကွန်ပျူတာတွေတစ်လုံးနှင့်တစ်လုံး data ပေးပို့ဖလှယ်ကြတဲ့နေရာမှာ လုပ်ဆောင်ပုံအဆင့်ဆင့်ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါပုံ (6.15) တွင်ကြည့်ပါ။ ကွန်ပျူတာ A နှင့် B တို့သည် သီးခြား network တစ်ခုစီအောက်မှာ ရှိကြပါတယ်။ ထို network နှစ်ခုတို့ကြားမှ router ခံပြီး ချိတ်ဆက်ထားပါတယ်။ ဤတွင်မှ ဆက်ပြီး ကွန်ပျူတာ A မှ ကွန်ပျူတာ B သို့ data ပေးပို့တဲ့ ဖြစ်စဉ်ကို ကြည့်ရအောင်။



step1) Segmentation

ကွန်ပျူတာ A မှ transport control protocol (TCP) သည် ပို့လိုတဲ့ data တွေကို စိတ်ပိုင်းပြီး segment ဖြစ်အောင် ဖန်တီးပါတယ်။

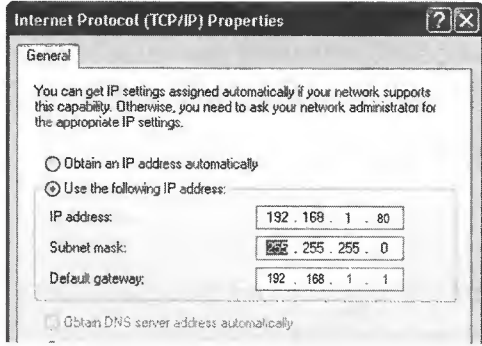
step2) IP packet

ကွန်ပျူတာ A မှ internet protocol သည် source နေရာမှာ ကွန်ပျူတာ A ၏ IP address (192.168.1.80) နှင့် destination နေရာတွင် ကွန်ပျူတာ B ၏ IP address (192.168.20.55) ကို ထည့်သွင်းပြီး packet များအဖြစ်ဖန်တီး ယူပါတယ်။

step3) ANDing

ဒီအဆင့်မှာဆိုရင် IP address နှင့် subnet mask တို့ကို ANDing လုပ်ပြီး address ၏ ဘယ်အပိုင်းက network ID၊ ဘယ်အပိုင်းက host ID လဲဆိုတာကို ခွဲခြားပါတယ်။ ဆိုရရင် source အတွက်တစ်ခါ၊ destination အတွက်တစ်ခါ စုစုပေါင်း ANDing နှစ်ခါ လုပ်ပါလိမ့်မယ်။

ANDing လုပ်ပြီး၍ ရလာမည့်အဖြေ (network ID) နှစ်ခုတို့သည် မတူတဲ့အတွက် ကွန်ပျူတာ B သည် အခြား network တစ်ခုမှာရှိနေသည်ဟု သိပါလိမ့်မယ်။ ဤတွင်မှ packet တွေကို အခြား network ဆီသို့ route လုပ်ပေးနိုင်တဲ့ default gateway သို့ အရင်ပို့ရမယ်လို့ ကွန်ပျူတာ A ၏ internet protocol မှ ဆုံးဖြတ်ပါလိမ့်မယ်။ ဆုံးဖြတ်ပြီးတာနှင့် default gateway ၏ IP address ကို ကွန်ပျူတာ A ၏ window registry ထဲတွင် ရှာဖွေပါလိမ့်မယ်။ အောက်ဖော်ပြပါပုံကတော့ ကွန်ပျူတာ A ၏ တွင် ထည့်သွင်းထားသော IP address၊ subnet mask နှင့် default gateway တို့ဖြစ်ပါတယ်။



ပုံ (6.16)

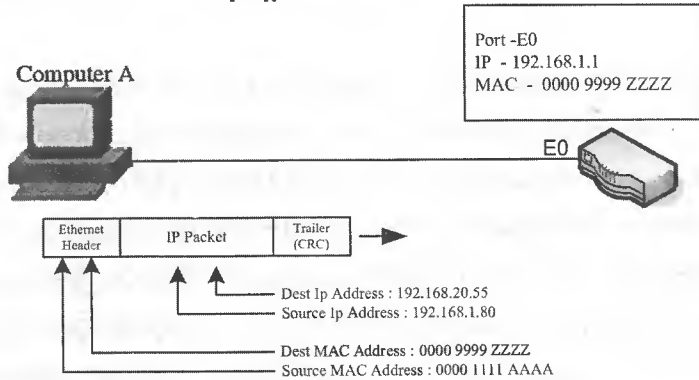
step4) Mac Address

ကွန်ပျူတာ A ၏ default gateway သည် 192.168.1.1 ဖြစ်ပါတယ်။ တစ်နည်းဆိုရရင် ကွန်ပျူတာ A တပ်ထားသော ဘက်က router မှ NIC ၏ IP address ဖြစ်ပါတယ်။ packet တွေကို default gateway သို့ ပို့ရန်အတွက် IP address '192.168.1.1' ဖြစ်သော router မှ NIC ၏ MAC ကို သိဖို့ရန် လိုလာပါတယ်။

ကွန်ပျူတာ A သည် default gateway ၏ MAC ကို နည်းလမ်း နှစ်သွယ်ဖြင့် ရရှိနိုင်ပါတယ်။ ပထမနည်းက ARP cache ထဲမှာ ရှာဖွေခြင်းဖြစ်ပါတယ်။ default gateway ၏ MAC သည် ARP cache ထဲမှာ အဆင်သင့်ရှိနေတယ်ဆိုရင် ၎င်း MAC address ကို ယူသုံးပါလိမ့်မယ်။ အကယ်၍ မရှိသေးဘူးဆိုရင် ARP broadcast လုပ်ပြီး ရှာဖွေပါလိမ့်မယ်။

step5) Framing

default gatewayရဲ့ MACကိုရပြီးဆိုရင် packetမှသည် frameအဖြစ်သို့စတင်တည်ဆောက်မှာ ဖြစ်ပါတယ်။ ethernet headerထဲရှိ sourceနေရာမှာကွန်ပျူတာ A၏ MAC destinationနေရာမှာ default gateway ၏ MAC တို့ပါရှိပါလိမ့်မယ်။



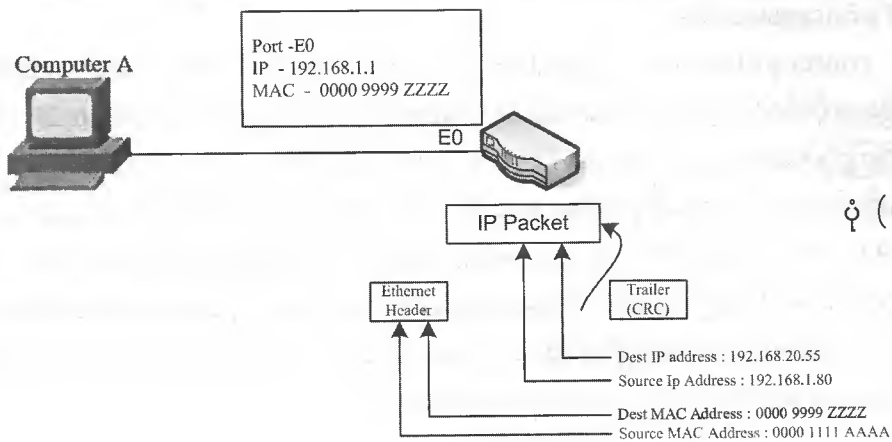
ပုံ (6.17)

destination **IP address** နေရာမှ ရှိတာက ကွန်ပျူတာ B ၏ IP address၊ destination **MAC address** နေရာမှာရှိတာက default gateway ၏ MAC ဖြစ်တယ်ဆိုတာကို အထူးသတိပြုဖို့ လိုပါတယ်။ FCS field ထဲမှာတော့ CRC value တစ်ခုပါပါလိမ့်မယ်။ ပြီးပြည့်စုံသော frame တစ်ခု တည်ဆောက်ပြီးသွားတဲ့အခါ bit တွေအဖြစ်ဖြင့် twisted pair cable ပေါ်သို့တင်ပေးလိုက်ပါတယ်။ ထို cable ပေါ်မှ တဆင့် default gateway လို့ခေါ်တဲ့ router ၏ network interface (192.168.1.1) သို့ရောက်ရှိသွားပါလိမ့်မယ်။

step6) Decapsulation

router မှ network interface သည် ဝင်လာတဲ့ bit တွေကို frame အဖြစ်သို့ ပြန်လည် တည်ဆောက်ပြီး FCS field ထဲရှိ CRC value ကို စစ်ဆေးပါလိမ့်မယ်။ မိမိတွက်ထားတဲ့ အဖြေနှင့် ကိုက်မယ်၊ တစ်နည်းဆိုရရင် bit error ဖြစ်မလာဘူးလို့သိတာနှင့် destination MAC ကိုဆက်လက် စစ်ဆေးပါလိမ့်မယ်။ destination နေရာမှာပါတဲ့ MAC သည်လည်း မိမိရဲ့ MAC နှင့် ကိုက်တယ်ဆိုရင် frame ထဲမှ packet တစ်ခုကိုသာ ထုတ်ယူပြီး ကျန်အစိတ်အပိုင်း (ethernet headen trailer) တွေကို ရှင်းလင်းဖယ်ရှားပစ်လိုက်ပါတယ်။ အဲဒီဖြစ်စဉ်ကို decapsulation လို့ခေါ်ပါတယ်။ ထုတ်ယူ လိုက်တဲ့ ၎င်း packet ကို router မှ internet protocol သို့ လွှဲပြောင်းပေးလိုက်ပါတယ်။

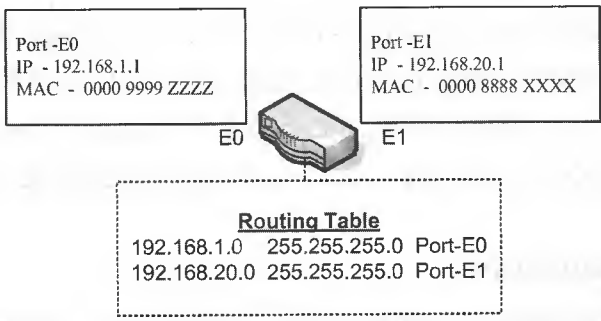
internet protocol သည် packet ကို လက်ခံရယူပြီး destination နေရာရှိ IP address ကို ANDing လုပ်ပြီး ကြည့်ရှုစစ်ဆေးပါတယ်။ destination နေရာမှ IP address သည် 192.168.20.55 ဖြစ်ပြီး မိမိရဲ့ IP address သည် 192.168.1.1 ဖြစ်နေသည့်အတွက် network မတူဘူးဆိုတာကို သိရှိပါလိမ့်မယ်။ ဤတွင်မှ routing လုပ်ငန်းစဉ်စပါတော့တယ်။



ပုံ (6.18)

routing ဆိုတာကတော့ routerတွေသည် ဝင်လာတဲ့ packetတွေထဲမှ destination IP address ကိုကြည့်မယ်၊ ပြီးရင် ၎င်း packetအား နောက် တဆင့် ဘယ်နေရာသို့ လွှဲပြောင်းပေးပို့ရမလဲ ဆိုတာကို routing table ကြည့်ပြီး ဆုံးဖြတ်တဲ့ လုပ်ငန်းစဉ်ဖြစ်ပါတယ်။

routing ရဲ့လုပ်ငန်းစဉ်ကို သဘောပေါက်နားလည်ရန်အတွက် routing table သည် အရောကျပါတယ်။ routing table မှာဆိုရင် ဝင်လာတဲ့ packet တွေကို ရည်ရွယ်ရာ network ဆီသို့ရောက်အောင် router တွေသည် ဘယ်လို forward လုပ်ရမယ် ဆိုတာကို ညွှန်ကြားပေးနိုင်တဲ့ network ID တွေ၊ subnet number တွေပါရှိပါတယ်။ အလွယ်ပြောရရင် ဘယ် network ကို သွားချင်ရင် ဘယ် port ကို သွားပါဆိုတာကို network administrator များ router ထဲမှာ ဝင်ရောက် ရေးသားသော table ဖြစ်ပါတယ်။

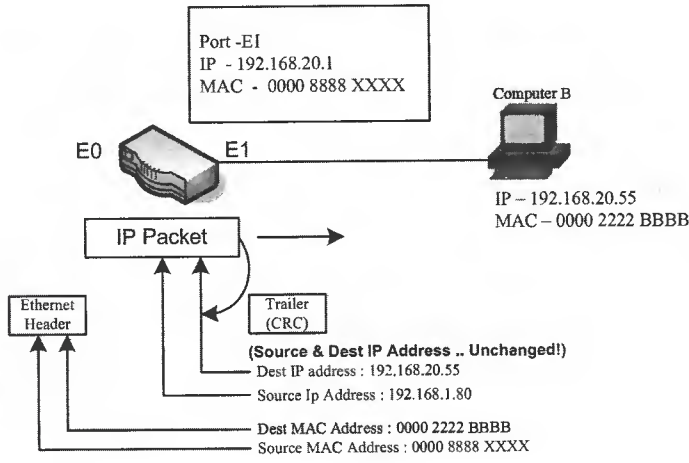


ပုံ (6.19)

ဖော်ပြပါပုံ(6.19)တွင်ကြည့်ပါ။ routing table ထဲမှာ network ID 192.168.20.0 နှင့် သက်ဆိုင်တဲ့ information ရှိရှိပါမယ်။ အဲဒီ table အရပင် router သည် ကွန်ပျူတာ A မှ ပို့လိုက်တဲ့ packet ကို ရည်ရွယ်ရာ network 192.168.20.0 သို့ရောက်ရန်အတွက် port E1 192.168.20.1 သို့ပို့ရမယ်ဆိုတာ နားလည်ပြီးလွှဲပေးပါလိမ့်မယ်။

step7) Encapsulation

router မှ ethernet 1(192.168.20.1) သည် တဖက် ethernet 0(192.168.1.1)မှ လွှဲပေးလိုက်တဲ့ packet ကို ရတဲ့အခါ ၎င်း packet ထဲမှာ ပါလာတဲ့ destination IP address ကိုကြည့်ပါတယ်။ ၎င်း IP address (192.168.20.55) နှင့်ဆိုင်သော MAC သည် မိမိရဲ့ ARP cache ထဲရှိမရှိ ဆိုတာကို ပထမဦးစွာ စစ်ဆေးပါတယ်။ မရှိဘူးဆိုရင် ထုံးစံအတိုင်း ARP broadcast လုပ်ပြီး 192.168.20.55 ရဲ့ MAC ကို ရှာဖွေ ပါလိမ့်မယ်။ MAC ကို ရပြီဆိုရင် packet ကို frame အတွင်း သွတ်သွင်းပြီး ကွန်ပျူတာ B ထံသို့ ပို့ပေးပါလိမ့်မယ်။ router တွေသည် ဝင်လာတဲ့ frame တွေထဲက packet တွေကိုသာ ထုတ်ယူပြီး အခြားတစ်နေရာသို့ လွှဲပေးတဲ့အခါ မိမိဖာသာ frame တစ်ခုအဖြစ်သို့ ပြန်တည်ဆောက်တယ်ဆိုတာ သတိချပ်စေလိုပါတယ်။



ပုံ (6.20)

ကွန်ပျူတာ B မှ လည်းရောက်လာတဲ့ frame ကို ပထမဦးစွာ bit error ပါမပါ စစ်ဆေး ပါတယ်။ error ကင်းတယ်ဆိုရင် destination နေရာမှာရှိတဲ့ MAC သည် မိမိရဲ့ MAC ဟုတ် မဟုတ် ဆိုတာ ဆက်လက်စစ်ဆေးပါတယ်။ မိမိရဲ့ MAC နှင့် ကိုက်တယ်ဆိုရင် ၎င်း frame ကို လက်ခံယူခြင်းဖြင့် ကွန်ပျူတာ A မှ ပို့လိုက်တဲ့ data တွေသည် ကွန်ပျူတာ B သို့ ရောက်ရှိသွားပြီလို့ ဆိုနိုင်ပါတယ်။

Name Resolution

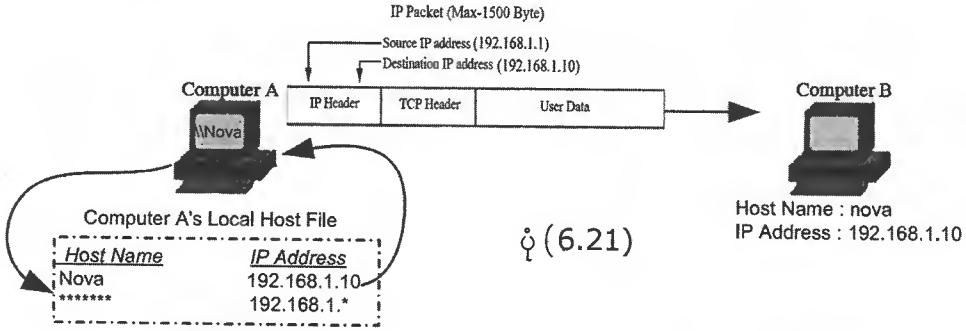
ကွန်ပျူတာတွေအနေနှင့် data ပေးပို့ဖလှယ်ကြတဲ့ နေရာမှာ IP address နံပါတ်တို့ကို အသုံးပြု နိုင်ကြသော်လည်း လူသားတို့အနေနှင့်ကျတော့ IP address တို့ကို မှတ်သားထားဖို့ရန် များစွာအခက် အခဲရှိပါတယ်။ ဤပြဿနာကို ပြေလည်စေရန် ကွန်ပျူတာတစ်လုံးစီကို မှတ်ရဖတ်ရလွယ်သည့် အမည်တစ်ခုစီ သတ်မှတ်ပြီး IP address အပြင် ၎င်းကွန်ပျူတာအမည် (host name) ဖြင့်ပါ အပြန်အလှန် communicate လုပ်ဆောင်နိုင်ကြစေရန် နည်းလမ်းတစ်ခုကို ကြံစီဖော်ဆောင်ခဲ့ကြပါတယ်။ ဤတွင်မှ name resolution ရဲ့အခန်းကဏ္ဍသည် အရေးပါလာပါတယ်။

name resolution ဆိုတာက ကွန်ပျူတာအမည်နှင့် သက်ဆိုင်သော IP address ကိုသိအောင် လုပ်ဆောင်ခြင်း process ပင်ဖြစ်ပါတယ်။ ဆိုရရင် router တွေသည် packet ၏ IP header ထဲတွင် ပါလာသော destination IP ကိုဖတ်၍ ဘယ်ကိုဆက်လက်ပို့ဆောင်ရမလဲဆိုတာကို ဆုံးဖြတ်ကြရပါတယ်။ အဲဒီ IP header ထဲတွင် လက်ခံမည့် ကွန်ပျူတာအမည်ကို ထည့်သွင်းဖို့ရန် နေရာလွတ်မရှိပါဘူး။ destination IP address ကိုသာ ထည့်သွင်းနိုင်မှာ ဖြစ်ပါတယ်။ ဒါကြောင့် အသုံးပြုသူတစ်ယောက်က host name ဖြင့် အဆက်အသွယ်လုပ်ဖို့ရန် ကြိုးစားတဲ့အခါ သူ၏ ကွန်ပျူတာသည် လက်ခံမည့် ကွန်ပျူတာ၏ host name ဖြင့် သက်ဆိုင်သော IP address ကိုသိအောင် ကြိုးပမ်းရပါတော့တယ်။ ရပြီဆိုမှ destination IP address ကို ထည့်သွင်းပြီး ရည်ရွယ်ရာကွန်ပျူတာဆီသို့ ရောက်အောင် ပို့လွှတ်နိုင်ပါလိမ့်မယ်။

Local Host File

နာမည်တော့သိတယ်။ ဒါပေမယ့် ဆက်သွယ်ရမယ့် ဖုန်းနံပါတ်မသိတော့တဲ့ လူတစ်ယောက်ထံ ဆက်သွယ်ဖို့လိုအပ်လာတဲ့အခါမျိုးမှာ လွယ်ကူရိုးရှင်းဆုံးနည်းလမ်းကတော့ ဖုန်းမှတ်စုစာအုပ်ထဲမှာ ရှာဖွေခြင်းဖြစ်ပါလိမ့်မယ်။ အရေးကြီးတာက အဲဒီဖုန်းစာအုပ်ထဲမှာ ထိုသူအမည်နှင့် ဖုန်းနံပါတ်တို့ရှိနေဖို့လိုခြင်း ဖြစ်ပါတယ်။

ကွန်ပျူတာတွေမှာ ဖုန်းစာအုပ်နှင့်တူတဲ့ file တစ်ခုရှိပါတယ်။ local host file လို့ခေါ်ပါတယ်။ အဲဒီ file ထဲမှာဆိုရင် ကွန်ပျူတာအမည် (host name) များနှင့် သက်ဆိုင်ရာ IP address များကို ယှဉ်တွဲ မှတ်သားထားပါတယ်။



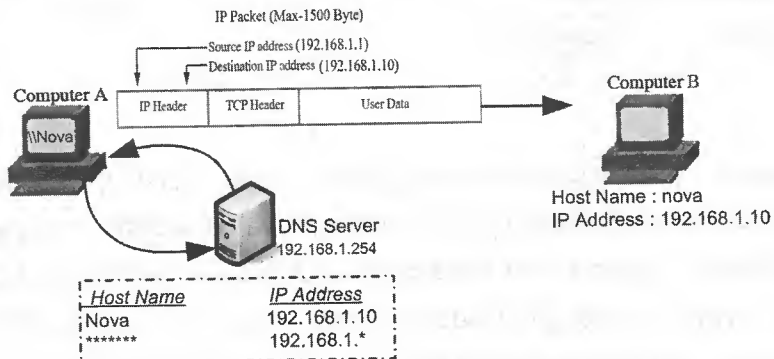
ကွန်ပျူတာ A မှ အသုံးပြုသူတစ်ယောက်သည် host name (nova) ကိုသုံးပြီး ကွန်ပျူတာ B နှင့် အဆက်အသွယ်လုပ်မယ်ဆိုပါစို့။ ဒါဆိုရင် ကွန်ပျူတာ A သည် 'nova' ဟုအမည်ရှိသော ကွန်ပျူတာ B ၏ IP address ကိုသိအောင် မိမိရဲ့ local host file ထဲတွင် ရှာဖွေပါလိမ့်မယ်။ host file ထဲတွင် host name (ဥပမာပုံအရ - nova) နှင့်အတူတွဲလျက် IP address (ပုံအရ - 192.168.1.10) ကိုတွေ့ပြီးဆိုလျှင် Nova အမည်ရှိသော host name ၏ IP ပဲဆိုတာ သိရှိပြီး destination နေရာတွင် ထည့်သွင်းပေးပို့ပါလိမ့်မယ်။ Local host file ရဲ့သဘောတရားနှင့် အလုပ်လုပ်ပုံတို့သည် အလွန်ကိုရိုးရှင်းလွယ်ကူပါတယ်။ သို့သော် ဖုန်းမှတ်စုစာအုပ်ကို အသုံးပြုသကဲ့သို့ပင် အချို့သော အားနည်းချက်တွေလည်း ရှိပါတယ်။

ဆိုရရင် မိမိတို့ရဲ့ ဖုန်းစာအုပ်ထဲတွင် ကိုယ်ရေးကိုယ်တာနှင့် ဆိုင်သော အရေးကြီး ဖုန်းနံပါတ် လောက်သာ မှတ်သား သိမ်းဆည်းထားနိုင်သလို local host file သည်လည်း ကွန်ပျူတာ အရေအတွက် နည်းတဲ့ သာမန် network ငယ်တွေ အတွက်လောက်သာ name resolution ကိုနိုင်နိုင်နင်းနင်း လုပ်ပေး နိုင်ပါတယ်။ တကယ့် network ကြီးတွေနှင့် server name အသစ်များ နေ့စဉ်ထပ်တိုးနေလေ့ရှိတဲ့ အင်တာနက်လို ကမ္ဘာအကြီးဆုံး network မျိုးတွေမှာတော့ name resolution အတွက် DNS server ထားရှိအသုံးပြုကြရပါတယ်။

📦 DNS Server

DNS server ဆိုတာက DNS software ကို install လုပ်ထားတဲ့ ကွန်ပျူတာပင်ဖြစ်ပါတယ်။ ၎င်း server ထဲတွင် network တွင်းရှိ ကွန်ပျူတာအားလုံးတို့ရဲ့ host name နှင့် သက်ဆိုင်ရာ IP address များရဲ့ list ကို သိမ်းဆည်းထားပါတယ်။ ယေဘုယျအားဖြင့် local host file တို့နှင့် အတူတူပင်ဖြစ်ပါတယ်။ ဒါပေမယ့် ၎င်း list သည် ရှေ့မှာ ဖော်ပြခဲ့သလို ကွန်ပျူတာတိုင်းတွင်ရှိမှာ မဟုတ်ပဲ DNS server တစ်လုံးတည်းမှာသာရှိမှာ ဖြစ်ပါတယ်။ အဲဒီလို ကွန်ပျူတာတိုင်းမှာ ပျောက်သောက်ရုံနေတာထက် တနေရာတည်းမှာ ရှိနေတာကို အတူတကွ ဝိုင်းဝန်းအသုံးပြုကြခြင်းအားဖြင့် အားလုံးတညီတညွတ်တည်း ဖြစ်ပြီး အသုံးပြုမှု ပိုမိုလွယ်ကူစေပါတယ်။ ဒီနေရာမှာ အရေးကြီးလာတာက ကွန်ပျူတာတိုင်းသည် DNS ၏ IP ကို သိဖို့လိုခြင်းပင်ဖြစ်ပါတယ်။ ဒါကတော့ လွယ်ပါတယ်။ ကွန်ပျူတာတိုင်းရဲ့ control panel ထဲရှိ network properties တွင် DNS server ၏ IP address ကို အသုံးပြုသူတို့မှ ထည့်သွင်းပေးလိုက်ရုံဖြစ်ပါတယ်။ (DNS server IP ထည့်သွင်းပုံအဆင့်ဆင့်ကို စာ (209) တွင်ကြည့်ပါ။)

DNS server နှင့် အခြားကွန်ပျူတာတို့ name resolution အတွက် ဆက်သွယ်လုပ်ဆောင် ကြပုံသည် ရိုးရိုးရှင်းရှင်းပင်ဖြစ်ပါတယ်။ ဆိုရရင် ရှေ့မှာဖော်ပြခဲ့တဲ့ ဥပမာပုံ (6.21) နှင့် ခပ်ဆင်ဆင်ဖြစ်ပါတယ်။ သိလိုသော host name ၏ IP address ကို local host file ထဲတွင် ရှာဖွေမည့်အစား DNS server ထံသို့ request လုပ်ပြီး တောင်းယူခြင်းသာ ကွာခြားပါတယ်။



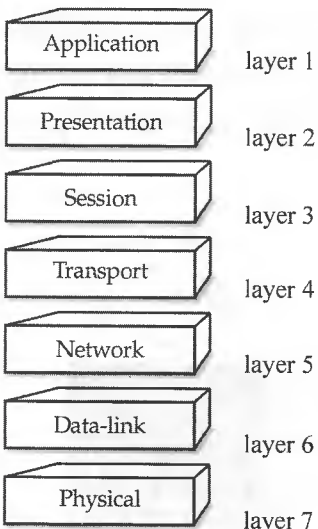
ပုံ (6.22)

OSI Model

ဟိုက်ဒရို အက်တမ်နစ်လုံးနှင့် အောက်စီဂျင် အက်တမ်တစ်လုံးပါသော ပုံကိုမြင်ရုံဖြင့် ရေမော်လီကျူးတစ်ခုဖြစ်တယ်ဆိုတာ ဉာဏ်း ဓာတုဗေဒလောကသင်ဘူးသူတိုင်း သိကြပါတယ်။ ရေမော်လီကျူးတွေကို မျက်စိဖြင့်မမြင်နိုင်သော်လည်း ၎င်းသရုပ်ဖော်ပုံကို ကြည့်ခြင်းအားဖြင့် ရေမော်လီကျူးတို့ရဲ့ဖြစ်တည်နေပုံ conceptကိုအလွယ်တကူသဘောပေါက်နားလည်ကြပါတယ်။

အဲဒီလိုပဲ နည်းပညာသစ် theoretical concept တစ်ခုကိုရှင်းလင်းဖော်ပြတဲ့နေရာမှာ အများအားဖြင့် ၎င်းသီအိုရီ သဘောတရားကို ခြုံငုံမိသည့် သရုပ်ဖော် model များဆောက်ပြီး ရှင်းလင်း တင်ပြလေ့ရှိပါတယ်။ networkingတွင်လည်း ဒီသဘောပင်ဖြစ်ပါတယ်။ networkပေါ်မှာကွန်ပျူတာတို့ အပြန်အလှန် dataပေးပို့လှယ်နေကြပုံကိုမျက်စိဖြင့်မမြင်နိုင်ကြသော်လည်း modelတစ်ခုကိုအသုံးပြုပြီး သူတို့ ဘယ်လို communicate လုပ်နေကြသလဲဆိုတာကို သဘောပေါက်နားလည်စေရန် ဖော်ဆောင် ပေးနိုင်ပါတယ်။ ၎င်း network modelကို OSI(Open Systems Interconnection) model လို့ခေါ်ကြပါတယ်။ layer ၇ခုဖြင့်ရှင်းလင်းဖော်ပြလေ့ရှိသဖြင့် Seven Layers လို့လည်းလူသိများပါတယ်။

The seven layers of the OSI Model



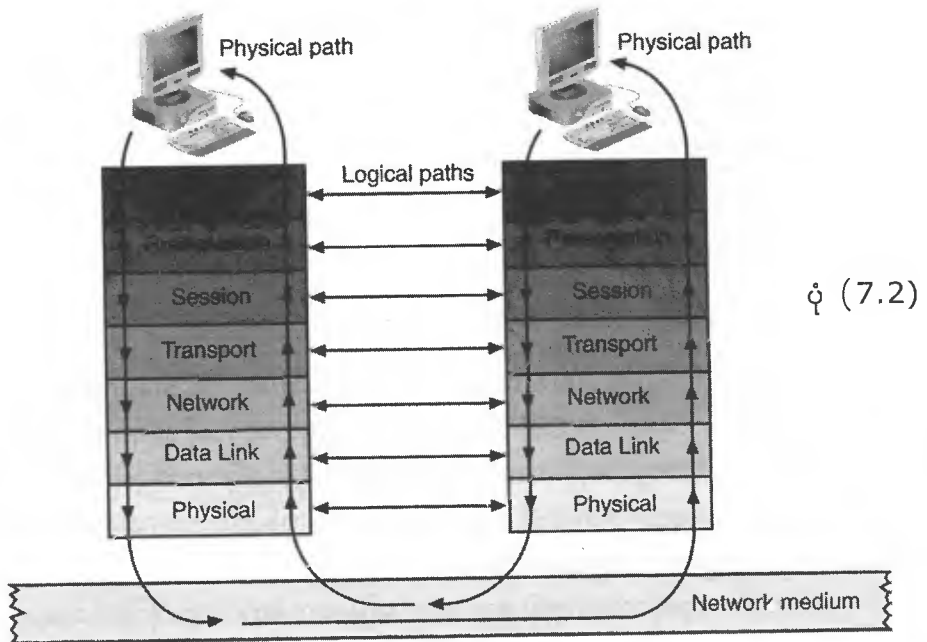
ပုံ (7.1)

၁၉၈၀ ပြည့်နှစ်ဦးမှစ၍ (International Organization for Standardization) ISO မှ OSIကိုစတင်ဖော်ဆောင်ခဲ့ပါတယ်။ OSI modelသည်ကွန်ပျူတာတွေနှင့်အခြား connecting device တွေရဲ့ကြားမှာ အဆက်အသွယ်လုပ်ဆောင် သမျှအားလုံးတို့ရဲ့အခြေခံအုတ်မြစ်ဖြစ်ပါတယ်။ ဒီနေရာမှာ အထူးသတိပြုဖို့ရန်ရှိလာတာကတော့ OSIသည် TCP/IPတို့လိုကွန်ပျူတာမှာ installလုပ်ပြီးအသုံးပြုရတဲ့ protocolမဟုတ်ဘူးဆိုတာပဲဖြစ်ပါတယ်။

protocol တွေဆိုတာက ကွန်ပျူတာတွေ အပြန်အလှန်ဆက်သွယ်ကြတဲ့ နေရာမှာ တဖက်နှင့် တဖက်လိုက်နာလုပ်ဆောင်ကြရမယ့် ruleတွေဖြစ်ကြပါတယ်။ အနည်းငယ်ထပ်အကျယ်ချဲ့ရရင် protocol တစ်ခုဆိုတာသည်ပရိုဂရမ်မာ တစ်ယောက်ယောက်ကနေပြီး function (သို့) functionများစွာတို့ကိုလုပ်

ဆောင်နိုင်စေရန် ရေးသားထားတဲ့ set of instruction တွေပဲဖြစ်ပါတယ်။ အချို့ protocol တွေသည် OS (window XP၊ 2000) နှင့် အတူပါရှိပြီး သားဖြစ်သလို အချို့ကတော့ software program တွေနှင့် အတူ install လုပ်ရပါမယ်။ ဤတွင် မှဆက်ပြီး OSI model နှင့် protocol တို့ရဲ့ ဆက်နွယ်မှုကို ကြည့်ရအောင်။

OSI model သည် လိုက်နာလုပ်ဆောင်သင့်တယ်လို့ အကြံပြုထားတဲ့ model သက်သက်သာ ဖြစ်ပါတယ်။ ကိုယ်တိုင် protocol တွေဖန်တီးမည့် programmer တွေအနေနှင့် OSI model အောက်မှာ မဖြစ်မနေ အကျိုးဝင်အောင် ရေးသားရမယ်လို့ ကန့်သတ်ချက်တော့ မရှိပါဘူး။ ဒါပေမယ့် OSI model ကို လိုက်နာပြီး ပုံစံထုတ်ရေးသားထားတဲ့ protocol တွေသာလျှင် အခြား network တွေနှင့် ပေါင်းစပ် ချိတ်ဆက်တဲ့ နေရာမှာ များစွာအခက်အခဲမရှိအပြန်အလှန် communicate လုပ်နိုင်မှာ ဖြစ်ပါတယ်။ TCP/IP protocol ကို OSI model မပေါ်ခင်ကတည်းက အသုံးပြုလာခဲ့ခြင်းဖြစ်ပါတယ်။ ဒါကြောင့် TCP/IP အပါအဝင် အဲဒီအခါက အသုံးပြုနေသော protocol တွေကို OSI ဘောင်အတွင်းဝင်အောင် ထည့်သွင်း စဉ်တုန်းက များစွာသော အခက်အခဲတွေရှိခဲ့ပါတယ်။ OSI Model နှင့် မကိုက်ညီသော (ဝါ) OSI Model ကို လိုက်နာမှုမရှိသော ကိုယ်ပိုင် protocol တွေသည် တစ်ခုနှင့် တစ်ခု စုပေါင်း ချိတ်ဆက်တဲ့ နေရာမှာ ကမ္ဘာသုံးဖြစ်မလာတော့ပဲ တဖြေးဖြေးကွယ်ပျောက်သွားခဲ့ပါတယ်။ အနှစ်ချုပ်ဆိုရရင် OSI model သည် network ပေါ်မှာ အပြန်အလှန် communicate လုပ်နေသော ကွန်ပျူတာ နှစ်လုံးတို့ကြားမှာ ဖြစ်ပေါ်နေတဲ့ theoretical representation တစ်ခုပင်ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါပုံတွင် ကွန်ပျူတာ တစ်လုံးမှ အခြားကွန်ပျူတာ တစ်လုံးသို့ data သွားရာလမ်းကြောင်းကို OSI model ဖြင့် ဖော်ပြထားပါတယ်။



ပုံ (7.2)

Flows of data through the OSI Model

ကွန်ပျူတာနှစ်လုံးတို့ဖြင့်အပြန်အလှန် communicate လုပ်လိုတဲ့အခါမှာ source လို့ခေါ်တဲ့ data ပေးပို့မယ့် ကွန်ပျူတာ၏ application layer မှစပြီး data တွေပေးပို့ပါလိမ့်မည်။ ၎င်း data တွေသည် packet ပုံစံဖြင့် OSI model ၏အောက်ဆုံး layer ဖြစ်သော physical layer ထိတိုင်အောင် ဆင်းသွားပါလိမ့်မယ်။ physical layer သည် network အတွင်းပို့လွှတ်မယ့် data တွေရဲ့ခရီးအစဖြစ်ပါတယ်။ physical layer ၌ data တွေကို cable ပေါ်သို့ စတင် transmit လုပ်ပါတယ်။ အဲဒီလို transmit လုပ်လိုက်တဲ့ data တွေသည် ရည်ရွယ်ရာ ကွန်ပျူတာဖြစ်တဲ့ destination သို့ရောက်တဲ့အခါ physical layer မှစပြီး OSI model ရဲ့ layer တွေကို တဆင့်ပြီးတဆင့် ဖြတ်တက်ပြီး နောက်ဆုံး application layer သို့ရောက်သွားပါမယ်။

အဲဒီ data ပေးပို့မှုဖြစ်စဉ်သည် millisecond အတွင်းပြီးမြောက်မှာဖြစ်ပါတယ်။ ဒါက data သွားပုံလမ်းကြောင်းဖြစ်ပါတယ်။ ကွန်ပျူတာ တစ်လုံးနှင့် တစ်လုံး communicate လုပ်ပုံကို logically အကြည့်မယ်ဆိုရင် layer တူအချင်းချင်းသာ communicate လုပ်ကြပါတယ်။ ဆိုရရင် ကွန်ပျူတာတစ်လုံးမှ application layer protocol သည် တစ်ဖက်ကွန်ပျူတာ၏ application layer protocol ဖြင့်သာ information တွေဖလှယ်ကြပါတယ်။ အခြား layer protocol များသည် Application layer ၏ data တွေကို ဝင်ရောက်စွက်ဖက်ဖို့ရန် မကြိုးစားကြပါဘူး။

Application Layer

OSI model ရဲ့အမြင့်ဆုံး၊ အသုံးပြုသူ user တို့နှင့်အနီးကပ်ဆုံး layer ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါ protocol များကတော့ application layer မှာ အလုပ်လုပ်ကြသည့် အသုံးများတဲ့ protocol များဖြစ်ကြပြီး application layer protocol များလို့လည်း ခေါ် ကြပါတယ်။

- HTTP (Hypertext Transfer Protocol)
- SMTP (Simple Mail Transfer Protocol)
- FTP (File Transfer Protocol)
- DNS (Domain Name System)

အမည်အားဖြင့် application layer လို့တွင်သည့်အတွက် software application တွေဖြစ်ကြတဲ့ Word တို့၊ Excel တို့၊ Internet Explorer တို့သည် ဒီ layer မှာအလုပ်လုပ်ကြတယ်လို့ အထင်မှားစရာဖြစ်ပါတယ်။ application layer ထဲမှာ ဒီ software application တွေမပါဘူး။ software application တစ်ခုသည် network နှင့် ဆိုင်တဲ့ service တစ်ခုခုကိုလုပ်ဆောင်ရန်လိုအပ်လာတဲ့အခါမှာ application layer protocol များမှ တဆင့်လုပ်ဆောင်ကြပါတယ်။ ဥပမာအနေနှင့်ဆိုရရင် application software တွေ network ပေါ်မှာ အလုပ်လုပ်ရန် လိုအပ်တဲ့ protocol တွေကတော့ email ပို့ရန်အတွက် SMTP၊ အင်တာနက်ပေါ်မှ webpage တွေကို ခေါ် ကြည့်ရန်အတွက် http ၊ FTP server တွေပေါ်မှ file တွေကို download လုပ်ယူရန် FTP တို့ဖြစ်ကြပါတယ်။

◆ Presentation Layer

application layer အောက်ကပ်လျက်၊ OSI model ရဲ့ ခြောက်ခုမြောက် layer ဖြစ်ပါတယ်။ presentation layer ရဲ့ အဓိကလုပ်ဆောင်မှုသုံးခုရှိပါတယ်။

- data presentation
- data Compression
- data Encryption

Data presentation ရဲ့ သဘောကတော့ ဒီဘက်ကပို့လိုက်တဲ့ data တွေကို တစ်ဖက်လက်ခံသူဘက်မှ process လုပ်၍ ရနိုင်အောင် ပြောင်းပေးခြင်းဖြစ်ပါတယ်။ ဆိုရရင် presentation layer သည် translator သဘောဆောင်ပါတယ်။ Windows အပါအဝင်၊ UNIX၊ Macintosh (apple) အစရှိတဲ့ ယနေ့အသုံးအများဆုံးကွန်ပျူတာတွေရဲ့ language သည် ASCII (American Standard Code for Information Interchange) ဖြစ်ပါတယ်။ ဒါပေမယ့် IBM Mainframe ကဲ့သို့သော အချို့ကွန်ပျူတာတွေသည် EBCDIC Language (Extended Binary Coded Decimal Interchange Code) ကို အသုံးပြုကြပါတယ်။ ဒါကြောင့် Windows ကွန်ပျူတာနှင့် IBM Mainframe တို့ကြားမှာ data ဖလှယ်ချင်တယ်ဆိုရင် ASCII မှ EBCDIC သို့ EBCDIC မှ ASCII သို့ အပြန်အလှန် translate လုပ်ပေးဖို့လိုပါတယ်။ အဲဒီလို translation ကဲ့သို့ လုပ်ငန်းစဉ်ကို presentation layer protocol များမှ လုပ်ဆောင်ပါတယ်။

presentation layer ရဲ့ ဒုတိယလုပ်ဆောင်မှုကတော့ network ပေါ်မှ ပို့လွှတ်မယ့် data တွေရဲ့ အရွယ်အစားငယ်သွားအောင် compress လုပ်ပစ်ခြင်းဖြစ်ကြပါတယ်။ ဒီဘက် presentation layer မှ compress လုပ်ပြီး ပို့လိုက်သမျှ data တွေကို တစ်ဖက်ကွန်ပျူတာတွေရဲ့ presentation layer ရောက်တဲ့အခါ ပြန်လည် uncompress လုပ်ယူပါလိမ့်မယ်။

နောက်ဆုံးတစ်ခု presentation layer ရဲ့ လုပ်ဆောင်မှုကတော့ data encryption နှင့် decryption ဖြစ်ပါတယ်။ ဥပမာ secure communication ကို အသုံးပြုပြီး အင်တာနက်ပေါ်မှတစ်ဆင့် Bank account တွေကို ဖွင့်ကြည့်မယ်ဆိုရင် presentation layer protocol သည် account data တွေကို encrypt လုပ်ပြီးမှ ပေးပို့ပါလိမ့်မယ်။ မိမိကွန်ပျူတာထံ ရောက်လာတဲ့အခါ presentation layer မှာ ပြန်လည် decrypt လုပ်ပြီး ဖတ်ရှု၍ရနိုင်သော စာသားများအဖြစ် မြင်ရမှာဖြစ်ပါတယ်။

◆ Session Layer

session ဆိုတဲ့ အခေါ်အဝေါ်သည် network ပေါ်မှာ device နှစ်ခုတို့ data တွေကို အပြန်အလှန် ပေးပို့ဖလှယ်နိုင်ကြစေမည့် connection ကို ရည်ညွှန်းပါတယ်။ session layer ရဲ့ အဓိကလုပ်ဆောင်မှုကို ခွဲခြားကြည့်မယ်ဆိုရင် အဓိကအားဖြင့် သုံးခုရှိပါတယ်။

- Establishing a session
- Maintaining a session
- Ending a session.....တို့ဖြစ်ကြပါတယ်။

networkပေါ်မှာ ကွန်ပျူတာနှစ်လုံးတို့ dataပေးပို့ဖလှယ်ကြမယ်ဆိုရင်ပထမဦးစွာပေးပို့သူနှင့် ရယူသူတို့ကြားမှာ အချိတ်အဆက် တစ်ခုရှိလာအောင် ညှိနှိုင်းဆောင်ရွက်မှုများကို session layer protocol များမှ လုပ်ဆောင်ကြပါတယ်။ အချိတ်အဆက်ရသွားပြီဆိုတာနှင့် communicate လုပ်ကြမယ့် transmission rate ပေါ်မူတည်ပြီး simplex၊ half duplex နှင့် full duplex ဟူသော mode သုံးခု ထဲကဘယ် mode ဖြင့်လုပ်ဆောင်ကြရမလဲဆိုတာကို ဆုံးဖြတ်ပေးပါတယ်။ ထိုဖြစ်စဉ်မှာ dialog control လို့ခေါ်ပါတယ်။ အဲဒီလို session တစ်ခုစတင်ပြီးတာနှင့် ကွန်ပျူတာနှစ်လုံးတို့ communication လုပ်နေသမျှ ကာလပတ်လုံးတည်မြဲအောင် session layer protocol များမှ ထိန်းသိမ်းထားပေးပါတယ်။ တစ်ဖက်နှင့်တစ်ဖက် communication လုပ်ခြင်းပြီးဆုံးသွားပြီဆိုတဲ့အခါကျမှသာ session အား အဆုံးသတ်ပိတ်ခြင်းကို ဆက်လက်လုပ်ဆောင်ကြပါတယ်။

ဥပမာအင်တာနက်အသုံးပြုရန် ISP သို့ modem ဖြင့် လှမ်းချိတ်ဆက်တဲ့အခါ ISP server ကွန်ပျူတာ၏ session layer protocol နှင့် မိမိကွန်ပျူတာမှာရှိတဲ့ session layer protocol တို့ ညှိနှိုင်းပြီး connection တစ်ခုတည်ဆောက်ကြပါတယ်။ connect ဖြစ်ပြီးသွားလို့အသုံးပြုနေချိန်အတွင်း မမျှော်လင့်ပဲ ပြင်ပ ပယောဂတစ်ခုခုကြောင့် လိုင်းပြတ်တောက်သွားတဲ့အခါမျိုးမှာ အသုံးပြုသူတို့ဘက်မှာရှိတဲ့ session layer protocol များမှ disconnect ဖြစ်သွားတယ်ဆိုတာသိရှိပြီး ပြန်လည်ချိတ်ဆက်ဖို့ကြိုးစာပါလိမ့်မယ်။ သတ်မှတ်ထားတဲ့အချိန်တစ်ခုထိတိုင်အောင် ISP server နှင့် ပြန်လည်ချိတ်ဆက်လို့မရသေးဘူးဆိုမှ session ကိုပိတ်ပစ်ပြီး communication အဆုံးသတ်သွားပြီဆိုတာကို dial-up software မှ အကြောင်းကြား ပါလိမ့်မည်။

The Transport Layer

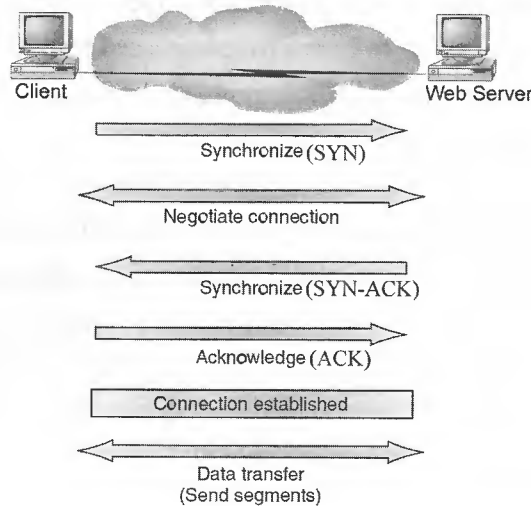
upper layer ကလာတဲ့အရွယ်အစားကြီးမားတဲ့ data တွေကို network ပေါ်မှာပေးပို့၍ ရနိုင်သော အရွယ်အစား ဖြစ်အောင် အစိတ်စိတ်အမွှာမွှာစိတ်ပိုင်းခြင်းကို transport layer မှ လုပ်ဆောင်ပါတယ်။ အဲဒီလုပ်ငန်းစဉ်ကို segmentation လို့ခေါ်ပြီး ရရှိလာတဲ့ data အပိုင်းအစတွေကို segment တွေလို့ ခေါ်ပါတယ်။ ဒါကြောင့် transport layer ရောက်တဲ့အခါ data အဖြစ်မှ segment အဖြစ်သို့ ပြောင်းသွား ပြီဆိုတာကို သတ်မှတ်စေလိုပါတယ်။

transport layer ရဲ့ အဓိကလုပ်ဆောင်မှုကတော့ တစ်ဖက်ကပေးပို့လာတဲ့ data တွေကို လက်ခံရယူတဲ့အခါ အမှားအယွင်းမရှိ ပြည့်ပြည့်စုံစုံရရှိအောင် တာဝန်ယူဆောင်ရွယ်ပေးရပါတယ်။ error recovery လုပ်ငန်းစဉ်သဘော ဖြစ်ပါတယ်။ ဒါအပြင် flow control လို့ခေါ်တဲ့ လက်ခံသူဘက်မှ data တွေကို ဘယ်လောက်မြန်နှုံးဖြင့် လက်ခံရယူနိုင်သလဲဆိုတဲ့ အပေါ်မူတည်ပြီး transmit လုပ်ခြင်းကို ထိန်းကျောင်းပေးပါတယ်။ transport layer protocol ပေါင်းများစွာရှိပါတယ်။ transmission method ပေါ်မူတည်ပြီး connection-oriented နှင့် connectionless ဆိုပြီး နှစ်မျိုးကွဲပါတယ်။

Connection-Oriented

ပေးပို့လိုက်သော data packet အားလုံးရရှိပြီးတဲ့ လက်ခံသူဘက်မှ မူလပေးပို့သူထံသို့ ACK (acknowledgement) ပြန်ပို့ပေးပါက connection-oriented protocol ဖြစ်ပါတယ်။

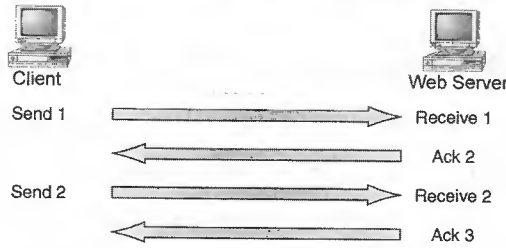
(ACKဆိုတာကတော့ပေးပို့တဲ့ dataသည် ပျောက်ပျက်ဆုံးရှုံးမှုမရှိဘူးဆိုတာကိုရည်ညွှန်းတဲ့ message ဖြစ်ပါတယ်။)ဆိုရင် ပေးပို့သမျှ data အားလုံးတိတိကျကျမှန်မှန်ကန်ကန်ရောက်ရှိကြောင်းကိုအာမခံပေးနိုင်သော protocol ဖြစ်ပါတယ်။ TCP သည် အသုံးပြုမှုအများဆုံး connection-oriented protocol ဖြစ်ပါတယ်။ဥပမာအနေနှင့်အင်တာနက်မှ webpageတစ်ခုကိုခေါ်ကြည့်တဲ့ဖြစ်စဉ်ကိုကြည့်ရအောင်။



ပုံ (7.3)

အင်တာနက်မှ webpageတစ်ခုကိုခေါ်ကြည့်တဲ့အခါပထမဦးစွာ clientကွန်ပျူတာမှ TCPသည် SYN (synchronization) packet တစ်ခုကို web server ထံသို့ လှမ်းပို့လိုက်ပါတယ်။ တဖန် web serverဘက်မှလည်း SYN-ACK packet တစ်ခုကိုပြန်ပို့ပါလိမ့်မယ်။ သဘောကတော့ သူ့ဘက်ကလည်း ချိတ်ဆက်ဖို့ရန် ဆန္ဒရှိပါတယ်ဆိုတဲ့ သဘောမျိုးဖြစ်ပါတယ်။ ထို့နောက်မှ clientကွန်ပျူတာဘက်မှ ACKကို ထပ်မံတုံ့ပြန်ပေးပို့ပါလိမ့်မယ်။ ထိုအဆင့်သုံးဆင့်တို့လုပ်ဆောင်ပြီး သွားတဲ့အခါ clientကွန်ပျူတာနှင့် web serverတို့ကြားမှာ connection တစ်ခုချိတ်ဆက်ပြီး ဖြစ်သွားပါတယ်။ အဲဒီလို TCP မှ connection တစ်ခု တည်ဆောက်ပြီး သွားတဲ့အခါမှသာ webpage အတွက် လိုအပ်တဲ့ http request ကို ဆက်လက် transmit လုပ်ပါလိမ့်မယ်။

ACK (Acknowledgment) ဆိုတာကိုပေးပို့လိုက်တဲ့ data သည် မပျောက်မပျက်ဆုံးရှုံးမှုမရှိပဲ လက်ခံရရှိတယ်ဆိုတဲ့အကြောင်းကို သိရှိနိုင်ဖို့ရန် အသုံးပြုကြပါတယ်။ connection oriented packet တွေသည်ပေးပို့သမျှသော data unit တစ်ခုစီအတွက်လက်ခံရယူမှုထံမှ ACK ကိုရရှိဖို့ရန် မျှော်လင့်ပါတယ်။ ရှေ့တဖော်ပြခဲ့တဲ့ webpage ဥပမာကို ဆက်ရမယ်ဆိုရင် clientကွန်ပျူတာမှ TCP protocol သည် http request တစ်ခုကို ပေးပို့ပြီးတာနှင့် webserver ထံမှ ၎င်း http request ကိုလက်ခံရရှိကြောင်းကို ရည်ညွှန်းတဲ့ ACK ကိုရရှိဖို့ မျှော်လင့်စောင့်ဆိုင်းနေပါတယ်။ အကယ်၍များ အချိန်အတိုင်းတာတစ်ခု အတွင်းမှာ ACK ကို မရဘူးဆိုရင် ကွန်ပျူတာမှ protocol သည် မိမိပေးပို့ခဲ့သော data ပျောက်ပျက်ဆုံးရှုံး သွားပြီဟု မှတ်ယူပြီး နောက်တစ်ကြိမ်ထပ်မံပေးပို့ပါလိမ့်မယ်။



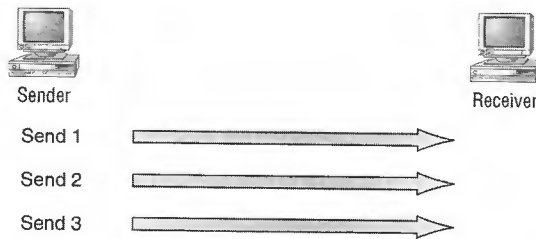
ပုံ (7.4)

ဒါကြောင့် reliability အကြောင်းမယ်ဆိုရင် connection-oriented protocol တွေသည် အတော်လေးမြင့်တယ်လို့ပြောနိုင်ပါတယ်။ packet တစ်ခုကိုပေးပို့တဲ့နေရာမှာပြသနာရှိလာပြီဆိုရင် အဲဒီ packet ကို ပြန်ပို့ပေးရန် မူလပေးပို့သူထံ request လုပ်နိုင်ပါတယ်။ ဒါပေမယ့် ရှေ့မှာဖော်ပြခဲ့သလို (ACK, SYNC) အစရှိတဲ့ packet တွေကို ပိုမိုလွတ်လပ်ရသည့်အတွက် အချိန်ပိုကြာပါတယ်။ connection-oriented ရဲ့ပေါ်လွင်တဲ့ လက္ခဏာတွေကတော့

- reliability
- slower connection
- packets are resent တို့ဖြစ်ပါတယ်။

● Connectionless Protocol

transmit မလုပ်ခင် ပေးပို့သူနှင့် ရယူသူတို့အကြားမှာ connection တစ်ခုဆောက်စရာ မလိုသည့်အပြင် ပေးပို့တဲ့ data တွေ error ကင်းကင်းနှင့် ရောက်မရောက်ဆိုတာမျိုး တာဝန်ယူစရာမလိုတဲ့ protocol သည် connectionless protocol ဖြစ်ပါတယ်။ တနည်းဆိုရရင် လက်ခံသူဘက်မှ data ရရှိကြောင်း ACK ပြန်ပို့စရာမလိုတဲ့ protocol မျိုး ဖြစ်ပါတယ်။ ပေးပို့တဲ့ ကွန်ပျူတာအနေနှင့်လည်း မိမိပို့သမျှ data အားလုံးကောင်းကောင်းမွန်မွန်စုံစုံလင်လင်ရောက်ရှိတယ်လို့မှတ်ယူပြီး ပို့ရုံဖြစ်ပါတယ်။



ပုံ (7.5)

connection-oriented တွေနှင့် ယှဉ်ကြည့်မယ်ဆိုရင် တဖက်နှင့် တဖက် data ပေးပို့ ဖလှယ် ကြတဲ့နေရာမှာပိုပြီး မြန်မယ်။ ဒါပေမယ့် data တွေအားလုံးရောက်မရောက် ဆိုတဲ့နေရာမှာတော့ reliable မဖြစ်ပါဘူး။ ဒါကြောင့် reliability ထက် speed ကပိုပြီး အရေးကြီးတဲ့ အချို့သော application တွေမှာ connectionless protocol ကို အသုံးပြုကြပါတယ်။ ဥပမာ အင်တာနက်ပေါ်မှ audio တွေ၊ video တွေလွှင့် တဲ့ အခါမျိုးတွေမှာ ဖြစ်ပါတယ်။ အသုံးအများဆုံး connectionless protocol ကတော့ UDP (User Datagram Protocol) ဖြစ်ပါတယ်။

Network Layer

network layer protocol တို့ရဲ့ အဓိကလုပ်ဆောင်မှုကတော့ addressing နှင့် routing တို့ ဖြစ်ပါတယ်။ addressing ဆိုတာကတော့ device (ကွန်ပျူတာ) တစ်ခုကို network ထဲမှအခြားမည်သည့် device နှင့်မှမတူနိုင်တဲ့ address number တစ်ခုသတ်မှတ်ပေးခြင်းဖြစ်ပါတယ်။ device တစ်ခုမှာဆိုရင် address နှစ်မျိုးရှိပါတယ်။ IP address (logical address) နှင့် MAC address တို့ဖြစ်ပါတယ်။

NIC အားလုံးတို့မှာ MAC address လို့ခေါ်တဲ့ တကယ့် physical address တစ်ခုစီရှိကြတယ် ဆိုတာသိပြီးဖြစ်ပါလိမ့်မယ်။ MAC address ကိုစက်ရုံမှာ NIC ထုတ်လုပ်စဉ်ကတည်းက တစ်ပါတည်းအသေ ထည့်သွင်း သတ်မှတ်ထားခြင်းဖြစ်ပြီး ပြောင်းလဲ၍မရပါဘူး။ ဒါ့အပြင် NIC တစ်ခု၏ MAC address သည် ကမ္ဘာပေါ်ရှိအခြားမည်သည့် NIC တို့နှင့်မှမတူနိုင်တဲ့ ကိုယ်ပိုင် address ဖြစ်ပါတယ်။ network address (logical address) ကိုတော့ network layer protocol တွေဖြစ်ကြတဲ့ IP၊ IPX တို့ကို အသုံးပြုပြီး သတ်မှတ်ပေးနိုင်ပါတယ်။ internet protocol (IP) ကို အသုံးပြုပြီး သတ်မှတ်ပေးတဲ့ logical address သည် IP address ဖြစ်ပါတယ်။

ဥပမာအနေနှင့်ဆိုရင် logical address (IP address) သည် လူတစ်ယောက်အမည် (ဥပမာ- အောင်အောင်) နှင့် တူပြီး MAC address တွေကတော့ ထိုသူ၏ မှတ်ပုံတင်အမှတ် (ဥပမာ- ၁၂/ရပန- ၁၂၃၄၅၆) နှင့် တူပါတယ်။ ဤတွင်မှဆက်ဆိုရင် “အောင်အောင်” ဆိုတဲ့အမည်ဖြင့် တစ်နိုင်ငံလုံးတွင် လူများစွာရှိနိုင် သော်လည်း မှတ်ပုံတင်နံပါတ် (၁၂/ရပန- ၁၂၃၄၅၆) သည် လူတစ်ဦးတစ်ယောက်တည်း နှင့်သာ သက်ဆိုင်မှာဖြစ်ပါတယ်။ ဒါပေမယ့် စာသင်ခန်းတစ်ခုထဲမှာတော့ “အောင်အောင်” ဆိုသူသည် တစ်ယောက်ပဲရှိရပါမယ်။ သို့မှသာ “အောင်အောင် ရှိပါသလား” ဆိုတဲ့မေးခွန်းမျိုးကိုမေးတဲ့နေရာမှာ မှတ်ပုံတင်အမှတ်ကို အသုံးပြုစရာမလိုပဲ သက်ဆိုင်သူမှပြန်လည်ဖြေကြားနိုင်မှာဖြစ်ပါတယ်။

network layer protocol တွေသည် transpot layer segment တွေမှာ source နှင့် destination address ထည့်သွင်းခြင်းများကိုလုပ်ဆောင်ပါတယ်။ ထည့်သွင်းပေးမည့် လိပ်စာနှစ်ခုစလုံးသည် logical address များပဲဖြစ်ပါတယ်။ ဒီနေရာမှစ၍ data တွေသည် segment မှ packet များ ဖြစ်လာပါတယ်။ network layer protocol တွေသည် packet တွေကို ရည်ရွယ်ရာ destination သို့ မပေးပို့ခင် ဘယ်လမ်းကြောင်းမှ ပေးပို့ခြင်းသည် အကောင်းဆုံးဖြစ်မလဲဆိုတာကိုလည်း ဆုံးဖြတ် ပေးရပါတယ်။ အဲဒီလိုအမြန်ဆုံး ရောက်ရှိနိုင်မယ့်လမ်းကြောင်း ရွေးချယ်ဆုံးဖြတ်ခြင်းလုပ်ငန်းစဉ်ကို routing လို့ခေါ်ပါတယ်။ အထူးသဖြင့် network တစ်ခုမှအခြား network တစ်ခုသို့ပေးပို့တဲ့အခါမျိုးမှာ routing သည် လွန်စွာအရေးပါပါတယ်။ route လုပ်ပေးနိုင်သော protocol ပေါင်းများစွာရှိသော်လည်း internet protocol (IP) သည် အသုံးအများဆုံးဖြစ်ပါတယ်။ webpage ခေါ် ကြည့်တဲ့ဥပမာနှင့် ကြည့်မယ်ဆိုရင် IP သည် http request တစ်ခုအား ဘယ်ကလာပြီး ဘယ်ကိုသွားမယ်ဆိုတာကို ညွှန်ကြား ခိုင်းစေသော protocol ဖြစ်ပါတယ်။

hardwareအနေနှင့်ပြောရရင် ဒီ network layerမှာအလုပ်လုပ်တဲ့ deviceတွေကို layer-3 deviceတွေလို့ခေါ်ပါတယ်။ Router သည် အသုံးအများဆုံး layer-3 deviceပဲဖြစ်ပါတယ်။

DATA Link Layer

OSI model၏ဒုတိယ layerဖြစ်သော data link layerရဲ့အဓိကလုပ်ဆောင်မှုကတော့ network layerကလာတဲ့ packet တွေကို header နှင့် trailer တို့ထည့်သွင်းပြီး frame အဖြစ်သို့ တည်ဆောက်ခြင်းဖြစ်ပါတယ်။ headerထဲမှာဆိုရင် sourceနှင့် destination addressတို့ကိုထည့်သွင်းပေးပါတယ်။ ဒီ layerမှာထည့်တဲ့ addressတွေသည် MAC address (ဝါ) physical address (ဝါ) hardware addressပဲဖြစ်ပါတယ်။ အပေါ်က network layerမှာတုန်းကတည်းက source နှင့် destination addressတွေသည် logical address (ဝါ) IP addressဖြစ်ပါတယ်။

data link layerကထည့်သွင်းသည့် MAC addressနှင့် network layerကထည့်သွင်းသည့် IP address တို့ နှစ်ခုစလုံးမပါဘူးဆိုရင် packet တွေသည် ရည်ရွယ်ရာ ခရီးလမ်းဆုံးသို့ရောက်မှာ မဟုတ်ပါဘူး။ IP address သည် packet တွေကို လက်ခံရယူမည့် ကွန်ပျူတာရှိရာ network သို့ မှန်မှန်ကန်ကန်ရောက်ရှိရန်အတွက်ဖြစ်ပါတယ်။ frameတစ်ခု networkအတွင်းရောက်ရှိလာပြီဆိုတာနှင့် networkမှာရှိတဲ့ကွန်ပျူတာတိုင်းသည် အဲဒီ frameအတွင်းမှာပါလာတဲ့ destination MAC address ကိုကြည့်ရှုစစ်ဆေးကြပါတယ်။ destination MAC addressသည် မိမိ၏ MAC addressနှင့်တူနေတယ်ဆိုရင် အဲဒီ frameကို လက်ခံရယူပြီး network layerသို့ လွှဲပေးပါလိမ့်မယ်။ အကယ်၍များမတူဘူးဆိုရင် မိမိအတွက်မဟုတ်ဘူးဆိုတာသိရှိပြီး ၎င်း frameကိုလျစ်လျူရှုလိုက်ပါလိမ့်မယ်။ ဤနည်းဖြင့် data တွေသည် ရည်ရွယ်ရာခရီးလမ်းဆုံးသို့ရောက်နိုင်ကြပါတယ်။

ရောက်ရှိလာတဲ့ frameတွေသည် error-frameဖြစ်မဖြစ်ဆိုတာကို စစ်ဆေးဖို့ရန် လက်ခံသည့် ကွန်ပျူတာမှာ တာဝန်ရှိပါတယ်။ ဒါကြောင့် error detection လုပ်ငန်းစဉ်ကိုလက်ခံသည့်ကွန်ပျူတာ၏ data link layerမှာပင်လုပ်ဆောင်ပါတယ်။ data တွေသည်ပေးပို့စဉ်ကအတိုင်း ဟုတ်မဟုတ်ဆိုတာကို FCS check ဖြင့် စစ်ဆေးပါတယ်။ (စာ - 33 တွင်ကြည့်ပါ) အကယ်၍လမ်းမှာ error ဖြစ်ခဲ့မယ်ဆိုရင် နောက်တစ်ကြိမ်ပြန်ပို့ပေးရန် data link layerမှာပင်ညွှန်ကြားပါလိမ့်မယ်။

နောက်ထပ်အရေးကြီး လုပ်ဆောင်မှုကတော့ collisionဖြစ်ခြင်းမှကာကွယ်နိုင်ရန် အချိန်တစ်ခုတွင် deviceတစ်ခုသာ transmitလုပ်နိုင်အောင် ထိန်းကျောင်းပေးခြင်းဖြစ်ပါတယ်။ အသုံးအများဆုံးနည်းလမ်း နှစ်ခုကတော့ SCMA/CD နှင့် token passingတို့ဖြစ်ကြပါတယ်။ ethernet networkတွေမှာ CSMA/CD ကိုအသုံးပြုပြီး token ring networkတွေမှာတော့ token passing ကိုအသုံးပြုကြပါတယ်။

hardwareအနေနှင့်ပြောရရင် ဒီ data link layerမှာအလုပ်လုပ်တဲ့ device တွေကို layer-2 deviceတွေလို့ခေါ်ပါတယ်။ bridgeနှင့် switchတို့သည်အသုံးအများဆုံး layer-2 deviceများပဲဖြစ်ပါတယ်။

Physical Layer

OSI model ရဲ့ အောက်ဆုံး layer ဖြစ်ပါတယ်။ network တစ်ခုတည်ဆောက်ရာမှာ အသုံးပြုရမယ့် cable အမျိုးအစား၊ ဘယ်လောက်အကွားအဝေးထိကြိုးအရှည်ထားရှိနိုင်မလဲနှင့် အသုံးပြုရမည့် connector တို့ကို ဆုံးဖြတ်ပေးပါတယ်။ physical layer ရဲ့ နောက်ထပ်ပီသေသတစ်ခုကတော့ data link layer မှလာသော frame များကို လက်ခံရယူပြီး signal များအဖြစ် transmit လုပ်နိုင်စေရန် လျှပ်စစ်ဓိုအား ထုတ်ပေးပါတယ်။ ထိုအတူ ဝင်လာတဲ့ လျှပ်စစ်ဓိုအားတွေကို physical layer မှာပင် ထောက်လှမ်းပြီး signal များအဖြစ် လက်ခံရယူပါတယ်။ သဘောကတော့ bit တွေပို့ပြီး bit တွေ လက်ခံရယူခြင်းဖြစ်ပါတယ်။ connectivity device လို့ခေါ်တဲ့ hub နှင့် repeater တို့သည် physical layer မှာ လုပ်ဆောင်ပါတယ်။ NIC တွေကတော့ physical နှင့် data link layer နှစ်ခုစလုံးမှာ အလုပ်လုပ်ပါတယ်။

Network Hardware

Network Interface Card (NIC)

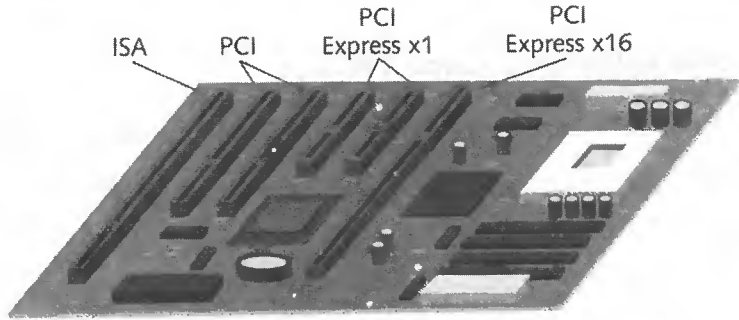
NICကို network adapter ၊ network card ရယ်လို့လည်း အမည်အမျိုးမျိုးဖြင့် ခေါ်ဆိုကြပါတယ်။ server ဖြစ်စေ client ဖြစ်စေ network ချိတ်ဆက် အသုံးပြုမည့် ကွန်ပျူတာတိုင်းတွင် NIC ရှိဖို့လိုပါတယ်။ ပုံမှန်အားဖြင့် NIC တို့သည် ကွန်ပျူတာ motherboard ပေါ်မှာ သီခြားစိုက်သွင်းတပ်ဆင်ရသည့် adapter card များပဲဖြစ်ပါတယ်။ ဒါပေမယ့် ယနေ့မှာတော့ motherboard ပေါ်မှာ built-in အဖြစ် တပါတည်း အသေထည့်သွင်းတည်ဆောက်ထားလေ့ရှိပါတယ်။ အဲဒီလိုကွန်ပျူတာတွေမှာတော့ NIC သီခြားဝယ်ယူတပ်ဆင်စရာမလိုပါဘူး။

အရေးကြီးတာက NIC သည် မိမိအသုံးပြုမည့် cable နှင့် ကိုက်ညီမှု ရှိဖို့ပင် ဖြစ်ပါတယ်။ ဥပမာ မိမိ network သည် thinnet cable (coaxial cable) ကို သုံးမယ်ဆိုရင် NIC သည် BNC connector ဝါရှိပါမယ်။ အကယ်၍ twisted pair ဖြစ်မယ်ဆိုရင် RJ-45 connector ဝါသော NIC ဖြစ်ရပါမယ်။ (ယနေ့ဈေးကွက်အတွင်း ဝယ်ယူရရှိနိုင်သော NIC နှင့် ကွန်ပျူတာမှာ built-in အဖြစ်ပူးတွဲပါရှိပြီးသား NIC အားလုံးတို့သည် RJ-45 connector များပဲဖြစ်ပါတယ်။) ဒါ့အပြင် NIC အများစုတို့သည် 10mbps (သို့) 100mbps နှစ်မျိုးစလုံးနှင့် အလုပ်လုပ်နိုင်ကြပါတယ်။ 10/100 card တွေလို့ခေါ်ပါတယ်။ ဒီ 10/100 card တွေသည် network speed နှင့် ကိုက်ညီအောင် ချိန်ညှိပြီး အလုပ်လုပ်နိုင်ကြသည့်အတွက် ရှေ့က အသုံးပြုခဲ့သော 10mbps network တွေမှာမည့်သည့်ပြဿနာမှ မရှိပဲ တပ်ဆင်အသုံးပြုနိုင် ကြပါတယ်။

Type of NIC

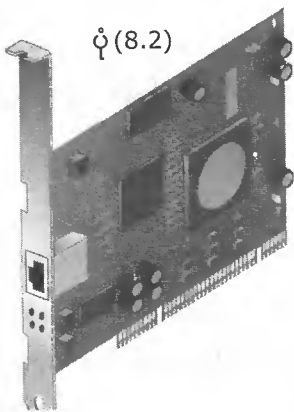
motherboard ပေါ်မှာ expansion slot တွေပါရှိပါတယ်။ internal modem ၊ sound card ၊ NIC အစရှိသော expansion card များကို ဤ slot များတွင် စိုက်သွင်းတပ်ဆင်အသုံးပြုကြရပါတယ်။ BUS အမျိုးအစားပေါ်မူတည်ပြီး ISA ၊ PCI express ဟူ၍ slot အမျိုးအစားများလည်း ကွဲပြားကြပါတယ်။ ထို slot အမျိုးအစားများသည် အရောင်အသွေးအားဖြင့် သော်လည်းကောင်း၊ ပါဝင်သော pin အရေအတွက် အားဖြင့် သော်လည်းကောင်း လုံးဝတူညီမှုမရှိသည့်အတွက် အလွယ်တကူခွဲခြားသိနိုင်ပါတယ်။

ဥပမာ ISA slot သည် အမည်းရောင်ဖြင့် လာလေ့ရှိပြီး၊ PCI slot များကတော့ အဖြူရောင် ဖြစ်ပါတယ်။ pentium II နှင့် pentium III အသုံးပြုသော motherboard အများစုတို့တွင် PCI နှင့် ISA slot နှစ်မျိုးစလုံးတွေ့နိုင်ပြီး PIV motherboard များပေါ်မှာတော့ PCI slot တစ်မျိုးတည်း ပါရှိတတ်ပါတယ်။ ဒါပေမယ့် ယနေ့ နောက်ဆုံးပေါ် PIV motherboard တွေမှာတော့ PCI နှင့် PCI express နှစ်မျိုးကို တွေ့ရတတ်ပါတယ်။ PCI slot မှာတပ်ဆင်နိုင်တဲ့ NIC ကို PCI NIC ၊ PCI express မှာတပ်ဆင်နိုင်သည့် NIC ကို PCI express NIC အစရှိသဖြင့် NIC အမျိုးအစားများ ကွဲပြားကြပါတယ်။



ပုံ (8.1)

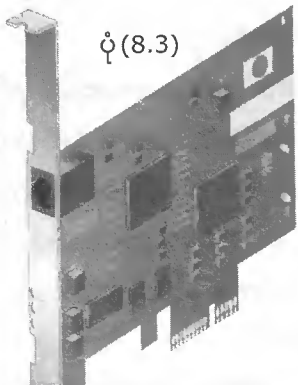
NICတစ်ခုကို ရွေးချယ်တဲ့နေရာမှ အဓိကအားဖြင့် မိမိကွန်ပျူတာရဲ့ဘယ် expansion slotမှာ တပ်ဆင် အသုံးပြုမှာလဲဆိုတဲ့အချက်ပေါ်မူတည်ပြီး ၎င်း slotနှင့် ကိုက်ညီသော interfaceပါရှိသည့် NIC ကိုရွေးချယ်ကြရပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ ယနေ့ဈေးကွက်အတွင်းမှာ အလွယ်တကူ ဝယ်ယူ ရရှိနိုင်သည့် NICအားလုံးနီးပါးတို့၏ access method ၏ ethernet transmission speedသည် 10/100 connector သည် RJ-45 ပင်ဖြစ်ကြပါတယ်။ ဈေးနှုန်းအနေနှင့် ကြည့်မယ်ဆိုရင် brand ကောင်းရင် ဈေးပိုကြီးမယ်ပေါ့။



ပုံ (8.2)

● PIC NIC

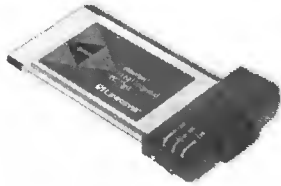
ယနေ့အသုံးအများဆုံး NIC အမျိုးအစားဖြစ်ပါတယ်။ ဈေးကွက်အတွင်း အလွယ်တကူဝယ်ယူလို့ရနိုင်တဲ့ အမျိုးအစားလည်း ဖြစ်ပါတယ်။



ပုံ (8.3)

● PCI Express

PCI expressသည် ယနေ့နောက်ဆုံးပေါ်BUSအမျိုးအစား တစ်ခုပင်ဖြစ်ပါတယ်။ မဝေးကွာလှတော့တဲ့ နှစ်အနည်းငယ်အတွင်းမှာ PCIတို့နေရာတွင် အစားထိုးရန်ရည်ရွယ်ထားသည့် BUS ဖြစ်ပြီး အချို့က PCIeဟု သုံးစွဲလေ့ရှိပါတယ်။



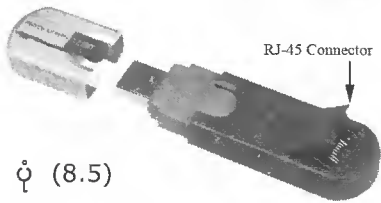
ပုံ(8.4)

● PCMCIA

built-in NICမပါသော laptopကွန်ပျူတာတွေမှာ PCMCIA NICကိုတပ်ဆင်အသုံးပြုနိုင်ကြပါတယ်။

● USB NIC

USB portမှတပ်ဆင်အသုံးပြုရတဲ့ network adapterအမျိုးအစားဖြစ်ပါတယ်။ USBသည် printer ၊ modem၊ scanner၊ network adapter အစရှိတဲ့ peripheral အမျိုးမျိုးတို့ တပ်ဆင်အသုံးပြုနိုင်တဲ့ standard interfaceတစ်ခုဖြစ်ပါတယ်။ USB 1.1 နှင့် USB 2.0 ဆိုပြီး standard



ပုံ (8.5)

နှစ်မျိုးရှိပါတယ်။ USB 1.1 ၏အမြင့်ဆုံး data transfer rateသည် 12mbpsဖြစ်ပြီး USB 2.0သည် 480mbps ဖြစ်ပါတယ်။ ယနေ့ဈေးကွက်တွင်း ရရှိ နိုင်တဲ့ ကွန်ပျူတာ သစ်တွေမှာပါတဲ့ port တွေသည် USB 2.0 ဖြစ်ပါတယ်။ တစ်ဖက်ပါ ပုံကတော့ USB NIC တစ်ခုရဲ့ပုံဖြစ်ပါတယ်။ တစ်ဖက်မှာ USB connector ဖြစ်ပြီး အခြားတဖက် စွန်းမှာတော့ RJ-45 connectorပါရှိပါတယ်။

● Onboard NIC (built-in)

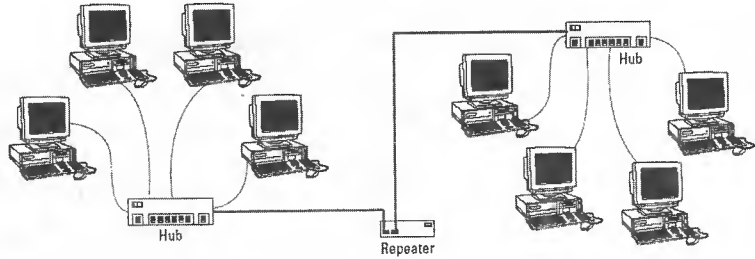
ယနေ့နောက်ပိုင်း ကွန်ပျူတာအများစုတို့မှာဆိုရင် motherboard ပေါ်မှာ တပါတည်းအသေ ထည့်သွင်းတည်ဆောက်ထားတဲ့ onboard NICတွေပါရှိတတ်ပါတယ်။ အဲဒီ NIC တွေအသုံးပြုခြင်းအားဖြင့် ကွန်ပျူတာထဲမှာ slot နေရာလွတ်တွေ ပိုမိုရရှိပြီး အခြား peripheral တွေကို ပိုမိုချိတ်ဆက် အသုံးပြုနိုင် စေပါတယ်။ ကွန်ပျူတာတစ်လုံးမှာ on-board NIC ပါရှိတယ်ဆိုရင် RJ-45 connector ကို desktop ကွန်ပျူတာတွေရဲ့ နောက်ဖက် laptop ကွန်ပျူတာတွေရဲ့ ဘေးဘက်မှာတွေ့ရပါလိမ့်မယ်။ (အချို့ laptop ကွန်ပျူတာမှာတော့ နောက်ဘက်မှာပါလေ့ရှိပါတယ်။)

ပုံ (8.6)



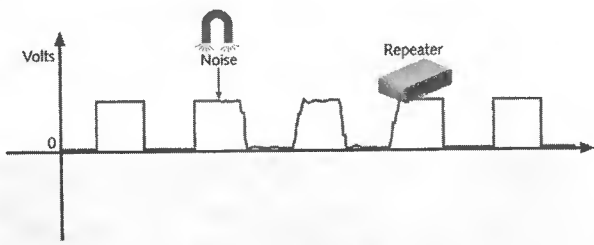
Repeaters

repeaterဆိုတာက cableကို အသုံးပြု၍ ရနိုင်တဲ့ အရှည်ထက်ပိုမို သွယ်တန်းလိုတဲ့ အခါမျိုးတွေမှာ ကြားခံ အသုံးပြုရတဲ့ device တစ်ခုဖြစ်ပါတယ်။ အထူးသဖြင့် coaxial cable ကို backbone အဖြစ် အသုံးပြုရတဲ့ network တွေမှာ အသုံးများခဲ့ပါတယ်။ ယနေ့အချိန်မှာတော့ အသုံးပြုမှု မရှိသလောက် နည်းပါးလာပြီဖြစ်သော device အမျိုးအစားတစ်ခုလည်း ဖြစ်ပါတယ်။



ပုံ (8.7)

ရူပဗေဒသဘောအရ ကြည့်မယ်ဆိုရင် ကြားခံ medium (ဥပမာ copper) တစ်ခုပေါ်မှာ ဖြတ်စီးနေသော လျှပ်စစ်စီးကြောင်း (current) သည် အကွာအဝေးတစ်ခုကို ရောက်တဲ့အခါ distortion ဖြစ်သွားတတ်ပါတယ်။ ဒီသဘောပါပဲ network cable တစ်ချောင်းပေါ်မှတစ်ဆင့် ပို့လွှတ်လိုက်တဲ့ digital signal တွေသည်လည်း အကွာအဝေးတစ်ခုကို ကျော်လွန်သွားတဲ့အခါ ပုံသဏ္ဍာန်ယိုယွင်းသွားတတ်ပါတယ်။ သို့သော် မူလ transmit လုပ်တဲ့ဆီကနေ ဘယ်နေရာလောက်ထိဆိုရင် signal တွေသည်များစွာ ယိုယွင်းမှု မရှိသေးပါဘူးလို့ အာမခံနိုင်တဲ့ အကွာအဝေး သတ်မှတ်ချက်အတိအကျ ရှိပါတယ်။ အဲဒါကတော့ အသုံးပြုတဲ့ cable အမျိုးအစား ပေါ်မူတည်ပြီး ကွာခြားချက်တွေရှိပါတယ်။ ဥပမာ thinnet coaxial ကို 185m ထိ သွယ်တန်းနိုင်တယ် ဆိုတာမျိုးပေါ့။ အကယ်၍ များ 185m ထက်ပိုတဲ့နေရာထိ သွယ်တန်းဖို့လိုလာပြီ ဆိုရင်တော့ ကြားမှာ repeater ကို အသုံးပြုဖို့ လိုလာပါလိမ့်မယ်။

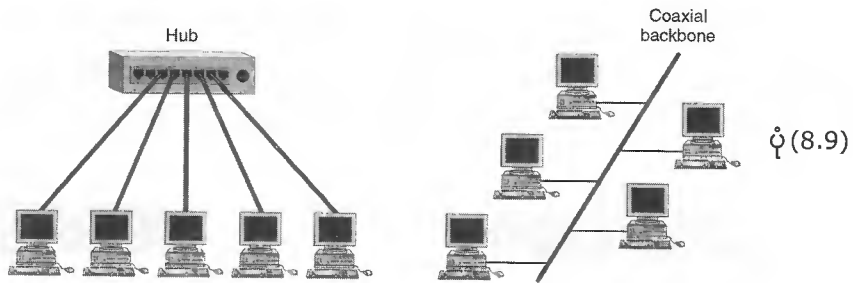


ပုံ (8.8)

repeater တို့ရဲ့ အဓိက လုပ်ဆောင်မှုက တစ်ဖက်က ဝင်လာတဲ့ signal တွေကို မူလအခြေအနေ တိုင်း ပြန်လည်ရောက်ရှိအောင် မြှင့်တင်ပြီးမှ ရှေ့ဆက် transmit လုပ်ပေးခြင်း ဖြစ်ပါတယ်။ ဆိုရရင် source တစ်ခုကနေ transmit လုပ်လိုက်တဲ့ signal တွေသည် 185m အကွာအဝေးရောက်တဲ့အခါ အနည်းငယ် ယိုယွင်းလာမယ်။ အဲဒီအခါ repeater က မူလအခြေအနေတိုင်း ပြန်လည်ရရှိအောင် repeat လုပ်ပြီး transmit လုပ်တဲ့အခါ နောက်ထပ် 185m အကွာအဝေးကို ဆက်သွားနိုင်မယ်ပေါ့။

HUB

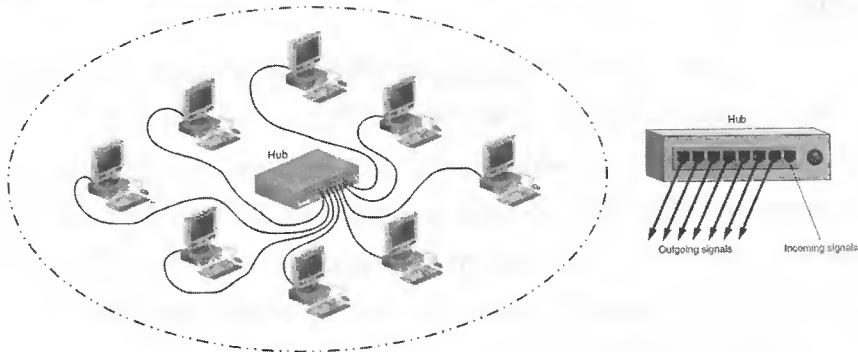
twisted pair cableကိုအသုံးပြုတည်ဆောက်တဲ့ networkတွေမှာဆိုရင် ကွန်ပျူတာတစ်လုံးစီ (d) device တစ်ခုစီသည် ကိုယ်ပိုင် cable တစ်ချောင်းစီဖြင့် hub ကို ဗဟိုထား၍ လာရောက် ချိတ်ဆက် ကြရပါတယ်။ coaxial cableကိုသုံးတဲ့ networkတွေမှာတော့ deviceအားလုံးတို့သည်တစ်ခုတည်းသော coaxial backboneဆီသို့ ချိတ်ဆက်တပ်ဆင် ကြရပါတယ်။ hub ကိုအသုံးပြုလာတဲ့ အချိန်ကစပြီး INC connecton vampire tap တို့ရဲ့အခန်းဂဏ္ဍ မှေးမှိန်ခဲ့ရပါတယ်။ အောက်ဖော်ပြပါပုံ (7.8) သည် hub၊ twisted pairတို့ဖြင့်တည်ဆောက်ထားသော networkနှင့် coaxial cableကိုအသုံးပြုထားသော networkတို့ရဲ့သရုပ်ဖော်ပုံများပဲ ဖြစ်ပါတယ်။



လုပ်ဆောင်မှုအရ ကြည့်မယ်ဆိုရင် hub တွေသည် repeater နှင့် အတူတူပင် ဖြစ်ကြပါတယ်။ ဆိုရရင် OSI physical layer မှာ အလုပ်လုပ်ကြတာချင်းတူသလို ဝင်လာတဲ့ signal တွေကို မူလအခြေ အနေတိုင်း ပြန်လည်ရရှိအောင် repeat လုပ်ပြီး transmit လုပ်ကြပုံချင်းလည်း တူပါတယ်။ ဒါကြောင့် hub ကို port များစွာပါရှိသော repeater (multi-port repeater) လို့လည်း ခေါ်ကြပါတယ်။ ဟိုးယခင်တုန်း ကတော့ hub အသုံးပြုမှုလွန်စွာတွင် ကျယ်ခဲ့ပါတယ်။ ယနေ့အချိန်မှာတော့ network performance ကို ပိုမိုတိုးမြှင့် စေရန် hub တို့၏နေရာမှာ switch တို့ဖြင့် အစားထိုး အသုံးပြုလာနေကြပြီ ဖြစ်ပါတယ်။

ဒီနေရာမှာ hub ကို အသုံးပြုမှုနှင့် network performance တို့ဘယ်လို ဆက်နွယ်မှု ရှိသလဲ ဆိုတာကို အနည်းငယ်ရှင်းပြလိုပါတယ်။ hub တစ်ခုသည် သူ၏ port တစ်ခုကနေဝင်လာတဲ့ signal ကို ကျန်ရှိသမျှ port အားလုံးဆီ တစ်ပြိုင်နက် forward လုပ်ပါတယ်။ ဥပမာ port ၈ ခုပါတဲ့ 8-port hub ၏ port နံပါတ် 1 မှာတပ်ဆင်ထားတဲ့ ကွန်ပျူတာကနေ transmit လုပ်လိုက်တယ်ဆိုပါတော့။ ထိုအချိန်အတွင်းမှာ port 2 ကနေ 8 အထိမှာ တပ်ဆင်ထားသမျှသော ကွန်ပျူတာအားလုံးတို့ကို transmit မလုပ်နိုင်အောင် တားမြစ်ထားပြီး ဝင်လာတဲ့ signal ကိုသာ လက်ခံရယူနိုင်ကြစေပါလိမ့်မယ်။ တနည်းဆိုရရင် collision မဖြစ်အောင် အချိန်တစ်ခုတွင် ကွန်ပျူတာတစ်လုံးမှသာ transmit လုပ်နိုင်စေခြင်း ဖြစ်ပါတယ်။ အဲဒီ အချိန်တစ်ခုတွင် ကွန်ပျူတာ တစ်လုံးမှသာ transmit လုပ်နိုင်သည့် ဖြစ်စဉ်တွင် ပါဝင်နေသော network တစ်ခုအတွင်းရှိ ကွန်ပျူတာတွေသည် collision domain တစ်ခုဖြစ်ပါတယ်။ ဆိုရရင် 8-port hub မှာ တပ်ဆင်ထားတဲ့ ကွန်ပျူတာလုံးသည် collision domain တစ်ခုကို ကိုယ်စားပြုကြပါတယ်။

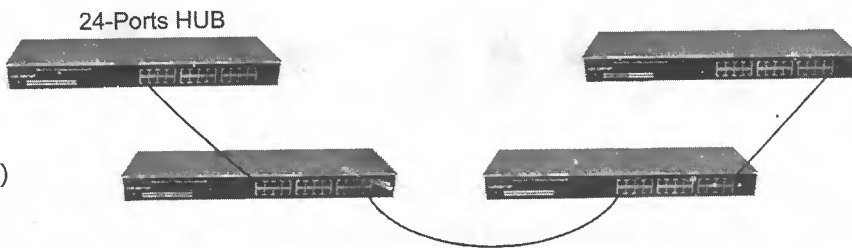
ပုံ (8.10)



Single Collision Domain

ဒါဆိုရင် 24-port hub လေးလုံးကို cascade ချိတ်ဆက်ပြီး port အရေအတွက် 96 ခုထိပါရှိတဲ့ network တစ်ခုမှာ collision domain ဘယ်နှစ်ခု ရှိသလဲ ဆိုတာကို စဉ်းစားကြည့်ရအောင်။ အောက်ဖော်ပြပါပုံ (8.11) ကတော့ 24-port လေးခုကို cascade ချိတ်ဆက်ထားပုံဖြစ်ပါတယ်။

ပုံ (8.11)



port အရေအတွက် စုစုပေါင်း ၉၆ ခုရှိသော်လည်း ကွန်ပျူတာ ချိတ်ဆက်တပ်ဆင်အသုံးပြုနိုင်သည့် port သည် ၉၀ သာရှိပါလိမ့်မယ်။ ၆ ခုက cascade ချိတ်ဆက်ရန်အတွက် အသုံးပြုကြရပါတယ်။ သဘောကတော့ ကွန်ပျူတာအလုံး ၉၀ ပါရှိတဲ့ network ပေါ့။

hub တို့၏ သဘာဝအတိုင်း port တစ်ခုကနေ ဝင်လာတဲ့ signal ကို ကျန် port များအားလုံးဆီ ဖြန့်ဝေပေးပို့သည်အတွက် မည်သည့် hub ၏ port တစ်ခုကနေမဆို transmit လုပ်တိုင်း ကျန် hub နှင့် port များ အားလုံးဆီသို့ရောက်ရှိကြပါတယ်။ ဖော်ပြပါပုံ (8.11) အရ ကွန်ပျူတာတစ်လုံးက transmit လုပ်နေချိန်တွင် ကျန်ကွန်ပျူတာ ၉၅ လုံးတို့သည် transmit မလုပ်နိုင်ဘဲ ဝင်လာသည့် signal ကိုစောင့်ဆိုင်းလက်ခံကြရပါတယ်။

ဒါကြောင့် မည်သို့ပင် ကွန်ပျူတာတွေ hub တွေများနေစေကာမူ အချိန်တစ်ခုတွင် ကွန်ပျူတာတစ်လုံးမှသာ transmit လုပ်နိုင်ကြသည့်အတွက် ၎င်း ကွန်ပျူတာ ၉၀ လုံးသည် collision domain တစ်ခုတည်းသာ ဖြစ်ကြပါတယ်။

ဒီနေရာမှာ သိထားဖို့ရန် အရေးကြီးလာတာက collision domain တစ်ခုတည်း အောက်မှာ ရှိသော ကွန်ပျူတာတွေသည် transmit လုပ်တဲ့နေရာမှာ network bandwidth ကိုမျှဝေသုံးစွဲရတယ်ဆိုတာပဲဖြစ်ပါတယ်။

ဒါကြောင့် collision domain တစ်ခုမှာ transmit လုပ်လိုတဲ့ ကွန်ပျူတာအရေအတွက် များလာတာနှင့်အမျှ ကွန်ပျူတာတစ်လုံးအတွက်ရရှိမည့် bandwidth ကိုယ်တာလျော့နည်းလာပါလိမ့်မယ်။ bandwidth ကိုမျှဝေသုံးစွဲခြင်းသည် 8-port hub တစ်ခုလောက်သာအသုံးပြုတဲ့ သာမန် network ငယ်တွေမှာ မသိသာပေမယ့် ဖော်ပြခဲ့တဲ့ ဥပမာလိုမျိုး hub လေးခုလောက်ကို cascade ချိတ်ပြီး ကွန်ပျူတာ များစွာဖြင့် တည်ဆောက်ထားတဲ့ network တွေမှာတော့ network speed သည် အတော်လေးကို သိသာ လှပါတယ်။

ဥပမာ ကွန်ပျူတာ ၉၀ ပါတဲ့ network သည် 100mbps ဖြင့် လုပ်ဆောင်တဲ့ fast ethernet network ဆိုပါတော့။ အကယ်၍ များတိုက်တိုက်ဆိုင်ဆိုင် ၄င်း ကွန်ပျူတာ ၉၀ စလုံးမှ transmit လုပ်ဖို့ ရှိလာပြီဆိုရင် ကွန်ပျူတာတစ်လုံးအတွက်ရရှိလာမည့် bandwidth ကိုယ်တာသည် အောက်ပါအတိုင်း ဖြစ်လာပါလိမ့်မယ်။

$$\text{bandwidth available} = \frac{100\text{mbps}}{90} = 1.1\text{mbps}$$

ဒါက အဆုံးစွန်ဆုံး အခြေအနေထိ တွက်ပြီးပြောတာပါ။ တကယ့်လက်တွေ့မှာတော့ အချိန် တစ်ခုတည်း အတွင်းမှာ ကွန်ပျူတာအားလုံး တစ်ပြိုင်နက် transmit လုပ်ဖို့ရန် ရှိကြမှာမဟုတ်ပါဘူး။ သို့သော် ငြားလည်း hub အသုံးပြုထားသော network အတွင်းရှိ ကွန်ပျူတာအရေအတွက် ၈၀ ရာခိုင်နှုန်း လောက်က transmit လုပ်ဖို့ရန် ရှိလာပြီဆိုရင်တောင်မှ အတော်လေးနေးလာတာကို ကြုံရတတ်ပါတယ်။

How to Choose a HUB

ethernet network တည်ဆောက်ရန် hub တစ်ခုကို ရွေးချယ်တဲ့နေရာမှာ အောက်ဖော်ပြပါ အချက်များ ပေါ်မူတည်၍ စဉ်းစားကြရပါတယ်။

The Type of Media Connection

ပုံမှန်အားဖြင့် hub အများစုတို့တွင် RJ-45 port များသာ ပါရှိတတ်ပါတယ်။ ဒါပေမယ့် အချို့သော 10 base T hub ကတွေမှာတော့ RJ-45 port တို့နှင့်အတူ BNC port တစ်ခုပါရှိတတ်ပါတယ်။

The Number of port

အများအားဖြင့် hub တစ်ခုတွင် port အရေအတွက် 4 ခုကနေ 24 ခုထိ ပါလေ့ရှိပါတယ်။ 24 port hub လေးခုကို cascade ချိတ်ပြီး port အရေအတွက် 96 ထိ အသုံးပြုနိုင်ပါတယ်။ port အရေအတွက် စုစုပေါင်း 96 ခု ရှိသော်လည်း ကွန်ပျူတာချိတ်ဆက်တပ်ဆင်အသုံးပြုနိုင်သည့် port သည် 90 သာ ဖြစ်ပါလိမ့်မယ်။ ခြောက်ခုက cascade ချိတ်ဆက်ရန်အတွက် အသုံးပြုကြပါတယ်။

■ Speed

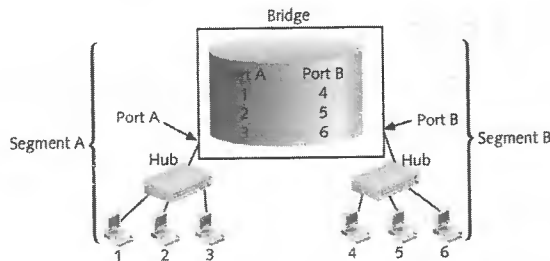
ပုံမှန်အားဖြင့် hub တွေသည် 10mbps နှုံးဖြင့် transmit၊ receive လုပ်ဆောင်ကြပါတယ်။ နောက်ပိုင်းထုတ်လုပ်တဲ့ အချို့သော hub တွေသည် 10mbps နှင့် 100mbps တို့ထဲက တစ်မျိုးမဟုတ် တစ်မျိုးဖြင့် လုပ်ဆောင်နိုင်ကြပါတယ်။

■ Manage and Unmanage HUB

hub တစ်ခု၏ လုပ်ဆောင်မှုသည် ပုံမှန်အခြေအနေတွင် ရှိမရှိဆိုတာကို ကွန်ပျူတာ တစ်လုံးလုံးက နေပြီး software ဖြင့်ဝင်ရောက် ကြည့်ရှုစစ်ဆေးနိုင်ပါက manage hub ဖြစ်ပါတယ်။ အဲဒါမျိုးလုပ်လို့ မရဘူးဆိုရင်တော့ unmanage hub ဖြစ်ပါတယ်။

📦 Bridge

Bridge သည် repeater တို့ကဲ့သို့ပင် network segment နှစ်ခုတို့ကို ကြားခံချိတ်ဆက်ရာတွင် အသုံးပြုရသည့် device တစ်ခုပင်ဖြစ်ပါတယ်။ အပြင်ပန်းအရ ကြည့်မယ်ဆိုရင်လည်း repeater တို့ကဲ့သို့ပင် အဝင် port တစ်ခုနှင့် အထွက် port တစ်ခုတို့သာ ပါရှိပါတယ်။ ဒါပေမယ့် လုပ်ဆောင်မှုအရတော့ မတူပါဘူး။ ဆိုရရင် repeater တို့ကဲ့သို့ ဝင်လာတဲ့ signal တိုင်းကို repeat လုပ်ပြီး အခြား တစ်ဖက် port ကနေ ထုတ်ပေးခြင်းမျိုး မဟုတ်ပါဘူး။ ဒီဘက် segment တစ်ခုကနေလာသည့် signal (ဝါ) frame တွေထဲမှာပါတဲ့ MAC address ကိုကြည့်ပြီး အခြားတစ်ဖက်က segment ဆီသို့ ဆက်လက်ပေးပို့ဖို့ လိုမလိုဆိုတာကို ဆုံးဖြတ်ပြီး လိုအပ်မှ forward လုပ်မှာဖြစ်ပါတယ်။



ပုံ (8.12)

Bridge တစ်ခုရဲ့ လုပ်ဆောင်မှုတွေကို ခွဲခြားကြည့်မယ်ဆိုရင် အဓိကအားဖြင့် ၂ပိုင်းရှိပါတယ်။

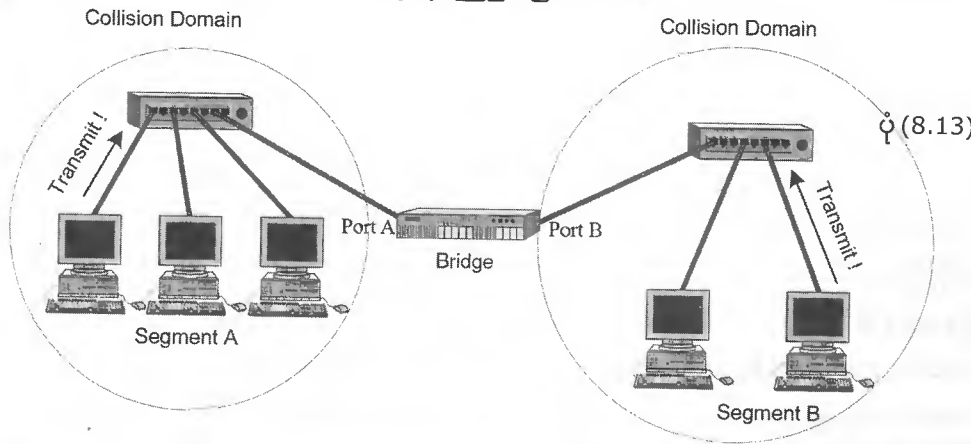
- 1) Bridge တွေထဲမှာ bridging table ဆိုတာကို တည်ဆောက်ထားပါတယ်။ အဲဒီ table ထဲမှာဆိုရင် network segment တစ်ခုစီမှာရှိနေတဲ့ ကွန်ပျူတာတိုရဲ့ MAC address တွေကို ထည့်သွင်းမှတ်သားထားပါတယ်။
- 2) Frame တစ်ခုရောက်လာပြီဆိုရင် destination MAC ကိုကြည့်ပြီး အဲဒီ frame ကို ဆက်လက် forward လုပ်သင့်မလုပ်သင့် ဆုံးဖြတ်ရပါတယ်။ ဥပမာအနေနှင့် ပုံ (8.12) ကိုကြည့်ရအောင်။ *

segment A မှ ကွန်ပျူတာ 2 ထံသို့ data ပေးပို့လိုတယ်ဆိုပါစို့။ ဒါဆိုရင် ကွန်ပျူတာ 1 မှ ပို့လိုက်တဲ့ frame သည် segment A ထဲရှိ hub မှတစ်ဆင့် ကျွန်ုပ်ကွန်ပျူတာ 2၊ 3 နှင့် bridge တို့ထံသို့ တပြိုင်နက် ရောက်ရှိ သွားပါလိမ့်မယ်။ Bridge သည် frame ထဲမှာပါတဲ့ destination MAC (ကွန်ပျူတာ 2 ရဲ့ MAC) ကို ဖတ်ရှုပြီး bridging table ထဲမှာ တိုက်ဆိုင် စစ်ဆေးရှာဖွေပါတယ်။ အဲဒီအခါမှာ ကွန်ပျူတာ 2 သည် port A ဘက်ခြမ်းမှာပင်ရှိတယ်ဆိုတာ သိရှိပြီး frame ကို port B ဘက်သို့ ဆက်လက် forward မလုပ်တော့ပဲ filter လုပ်လိုက်ပါလိမ့်မယ်။ ထိုအချိန်အတွင်းမှာပင် ကွန်ပျူတာ 1 မှ ပို့လိုက်တဲ့ frame သည် hub မှတစ်ဆင့် ကွန်ပျူတာ 2 ထံသို့ ရောက်ရှိလက်ခံပြီး ဖြစ်ပါလိမ့်မယ်။

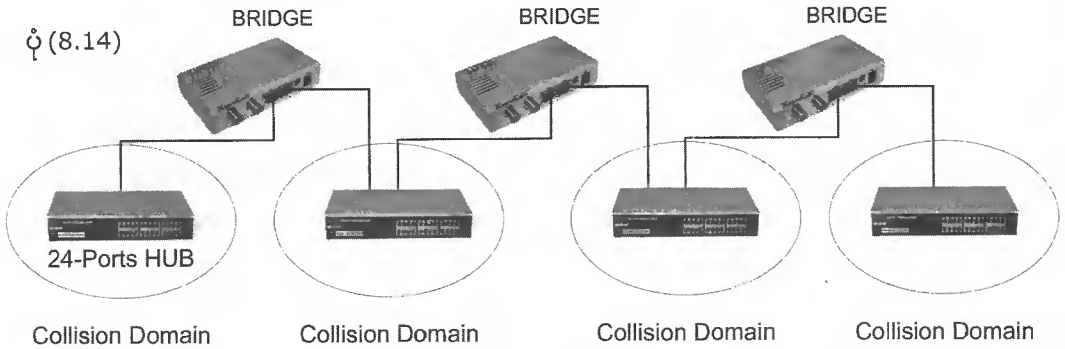
နောက်တစ်ခါ ကွန်ပျူတာ 1 မှ ကွန်ပျူတာ 5 ထံသို့ ပေးပို့မှု ဖြစ်စဉ်ကို ကြည့်ရအောင်။ ကွန်ပျူတာ 1 မှ ပို့လိုက်တဲ့ frame သည် bridge ထံသို့ ရောက်ရှိလာတဲ့အခါ bridge သည် destination MAC (ကွန်ပျူတာ 5 ၏ MAC) ကို ကြည့်ပြီး bridging table ထဲမှာ တိုက်ဆိုင် စစ်ဆေးရှာဖွေပါလိမ့်မယ်။ စစ်ဆေးပြီးသွားတဲ့အခါ ကွန်ပျူတာ 5 သည် port B ဘက်မှာ ရှိတယ်ဆိုတာ သိရှိပြီး frame ကို port B သို့ ဆက်လက် forward လုပ်လိုက်ပါတယ်။ ဤနည်းဖြင့် frame သည် segment B ထဲရှိ hub မှတစ်ဆင့် ကွန်ပျူတာ 5 ထံသို့ ရောက်ရှိ ပါလိမ့်မယ်။

Bridge and Network performance

Bridge တွေကို အသုံးပြုခြင်းအားဖြင့် network တစ်ခုကို collision domain များစွာ ရရှိအောင် စိတ်ပိုင်းနိုင်ကြပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ bridge ၏ port တစ်ခုစီသည် collision domain တစ်ခုဖြစ်ပါတယ်။ ပုံ (8.13) ကို ကြည့်ပါ။ port A သည် collision domain တစ်ခုဖြစ်ပြီး port B သည်လည်း collision domain တစ်ခုပင်ဖြစ်ပါတယ်။ ဒါကြောင့် segment A ထဲမှ ကွန်ပျူတာ တစ်လုံးလုံးက transmit လုပ်နေချိန်တွင် segment B ထဲမှ ကွန်ပျူတာ တစ်လုံးလုံးမှ နေပြီးတော့လည်း transmit လုပ်နိုင်ပါတယ်။ သဘောကတော့ network တစ်ခုတည်းမှာ collision domain ၂ ခု ဖြစ်လာသည့်အတွက် ကွန်ပျူတာ ၂ လုံးတို့မှ တပြိုင်နက် transmit လုပ်နိုင်ကြခြင်း ဖြစ်ပါတယ်။



အဲဒီလို network တစ်ခုအတွင်း collision domain အရေအတွက်များလာတာနှင့်အမျှ collision ဖြစ်ပွားမှုကိုလျော့နည်းစေခြင်းနှင့် ကွန်ပျူတာတစ်လုံးအတွက် bandwidth ကိုယ်တာပိုမိုရရှိစေခြင်း တို့ကြောင့် network performance ကိုတိုးမြှင့်စေပါတယ်။ ရှေ့မှာဖော်ပြခဲ့တဲ့ 24-port hub လေးခုကို cascade ချိတ်သုံးထားတဲ့ network ထဲမှာ bridge တွေကို ထဲ့ပြီး တည်ဆောက်တဲ့အခါ ဘယ်လိုဖြစ်လာမလဲ ဆိုတာကိုစဉ်းစားကြည့်ရအောင်။

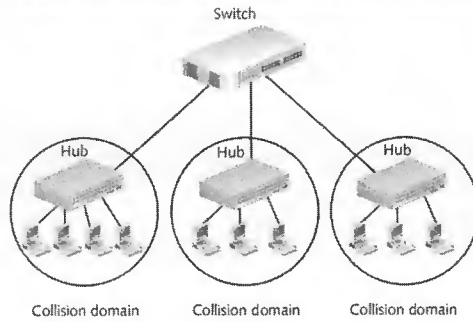


ဖော်ပြပါပုံ (8.14) အတိုင်း hub ၂ခုတို့ကြားမှ bridge တစ်ခုစီ ထည့်သွင်း တည်ဆောက်ခြင်းအားဖြင့် တစ်ချိန်တည်း တစ်ပြိုင်နက် transmit လုပ်နိုင်မည့် အရေအတွက်သည် ကွန်ပျူတာတစ်လုံးမှ လေးလုံးသို့ တိုးမြှင့်လာပါလိမ့်မယ်။ ထိုနည်းတူစွာပင် ကွန်ပျူတာတစ်လုံးအတွက် ရရှိမည့် bandwidth ကိုယ်တာလည်း တိုးမြှင့်လာပါလိမ့်မယ်။ intelligence ရှိလာတယ်ဆိုတဲ့သဘော ဖြစ်ပါတယ်။

bridge တွေသည် OSI model ၏ data link layer မှာအလုပ်လုပ်ကြပါတယ်။ ဒါကြောင့် layer 2 device လို့လည်း ခေါ်ဆိုကြပါတယ်။ ယနေ့ network တွေမှာတော့ bridge အသုံးပြုမှုသည် အတော်လေးကိုနည်းပါးသွားပါပြီ။ သို့သော်ငြားလည်း bridge တို့ရဲ့အခြေခံလုပ်ဆောင်မှုလောက်ကိုတော့ သိထားဖို့လိုအပ်လှပါတယ်။

Switch

အခြေခံအားဖြင့် switch ဆိုတာ port များစွာပါရှိသည့် bridge တစ်မျိုးဖြစ်ပါတယ်။ လုပ်ဆောင်ပုံကို ကြည့်မယ်ဆိုရင်လည်း bridge တို့နှင့် ဆင်တူပြီး data link layer မှာပင် အလုပ် လုပ်ကြပါတယ်။ switch မှာပါရှိတဲ့ port တစ်ခုစီသည် ကိုယ်ပိုင် collision domain တစ်ခုကိုကိုယ်စား ပြုပါတယ်။ ဒါကြောင့် switch port တစ်ခုမှာတစ်ဆင့်ထားသော ကွန်ပျူတာသည် ကျန် port တွေမှာ တစ်ဆင့်ထားသော ကွန်ပျူတာ တွေနှင့် bandwidth ကိုမျှဝေအသုံးပြုစရာမလိုပါဘူး။ switch တစ်ဆင့် ထားသော ကွန်ပျူတာတိုင်းသည် bandwidth ကိုအပြည့်အဝအသုံးပြုခွင့်ရကြပါတယ်။



ပုံ (7.15)

ဒါ့အပြင် switch တွေသည် မိမိထံမှာ ချိတ်ဆက်တပ်ဆင်ထားသော device တို့၏ MAC address တို့ကို ၎င်း device တပ်ဆင်ထားသော port နံပါတ်တို့နှင့် အတူ ယှဉ်တွဲမှတ်သားထားပါတယ်။ ဒါ့အပြင် port တစ်ခုကနေဝင်လာတဲ့ frame တွေကို forward လုပ်တဲ့နေရာမှာ ရည်ရွယ်ရာ device တစ်ခုတည်းသို့သာ ဦးတည်ပေးပို့နိုင်ကြသည့်အတွက် network အတွင်းမလိုလားအပ်သော လမ်းကြောင်း ပိတ်ဆို့မှုများကို ရှင်းလင်းဖယ်ရှားနိုင်ပါတယ်။

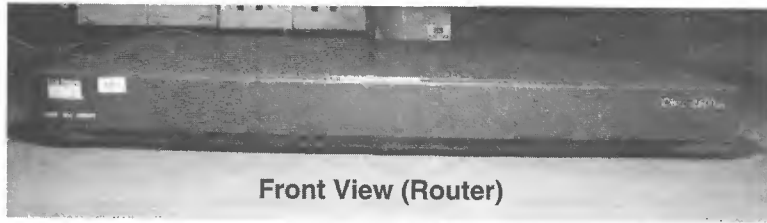
အဲဒီလို network performance ကို တိုးမြှင့်နိုင်စေခြင်းဆိုတဲ့ အချက်တွေကြောင့်လည်း switch တွေကို မဖြစ်မနေထည့်သွင်းအသုံးပြုရမည့် device တစ်ခုအဖြစ် သဘောထားလာကြပြီလို့ ဆိုရလောက်အောင် လူသုံးများလာကြပြီ ဖြစ်ပါတယ်။ အပြန်အလှန်အားဖြင့် အသုံးများတွင် ကျယ်လာခြင်းနှင့်အတူ ဈေးနှုံးမှာလည်း hub တို့နှင့် ယှဉ်နိုင်လောက်အောင် တဖြေးဖြေးကျဆင်းလာနေသည့်အတွက် ယနေ့ network အများစုမှာ hub တို့၏နေရာတွင် switch တွေကို အသုံးပြုလာနေကြပြီ ဖြစ်ပါတယ်။

Router

Bridge တွေသည် data link layer မှာ အလုပ်လုပ်ကြသည့်အတွက် physical layer တွင် အလုပ်လုပ်သော repeater တွေထက် layer ပိုမြင့်သလို အသိဉာဏ်လည်း ပိုပါတယ်။ ဆိုရရင် repeater တွေကဲ့သို့ signal တွေထဲမှာ ဘယ်လို information (ဥပမာ - MAC၊ IP၊ data) တွေပါသလဲဆိုတာကို လုံးဝမသိပဲ ဝင်လာသမျှကို အခြားတစ်ဖက် port ဆီ forward လုပ်ခြင်းမဟုတ်ပါဘူး။ ဝင်လာတဲ့ အထဲက destination MAC address ကို ဖတ်မယ်ပြီး ရင်တဖက် port ဆီကို ဆက်လက် forward လုပ်သင့်မလုပ်သင့် ဆုံးဖြတ်နိုင်ပါတယ်။

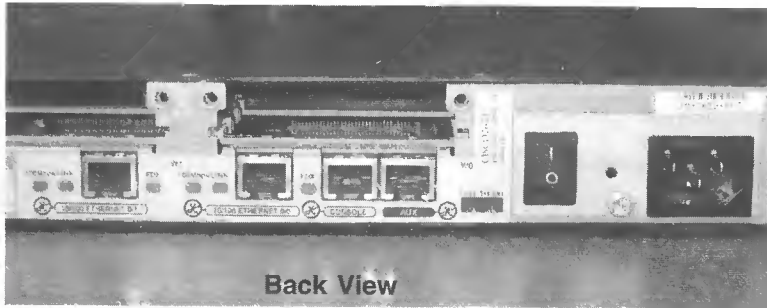
သို့သော် bridge တွေသည်လည်း MAC address လောက်ကလွဲပြီး frame ထဲမှာ ပါသည့် ကျန်တဲ့ information တွေကို သိနိုင်စွမ်းမရှိပါဘူး။ Router တွေကတော့ network layer မှာ အလုပ်လုပ်သည့်အတွက် IP address အထိဖတ်နိုင်ပါတယ်။ packet တစ်ခုဝင်လာပြီဆိုရင် destination IP address ကိုဖတ်ပြီး ဘယ် network ဆီသို့လွှဲပေးရလဲဆိုတာကို သိကြပါတယ်။ ပြီးရင် အဲဒီ network သို့အမြန်ဆုံး ရောက်နိုင်မယ့် လမ်းကြောင်းကို ရွေးချယ်ဆုံးဖြတ်ပြီး ပေးပို့နိုင်ကြပါတယ်။

Router တစ်လုံးမှာဆိုရင်ပုံမှန်အားဖြင့် processor၊ operating system၊ memory၊ input/output connector များနှင့် console port တို့ပါရှိပါတယ်။



Front View (Router)

ပုံ (8.16)



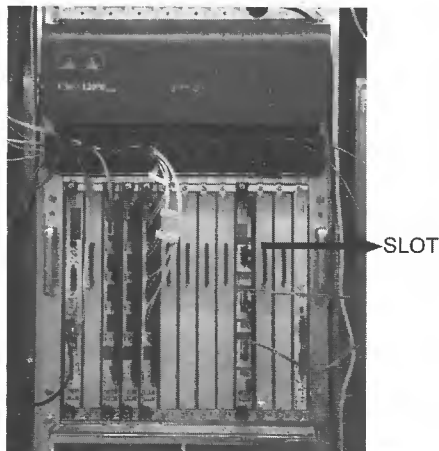
Back View

console port ဆိုတာကတော့ routing table ရေးခြင်း၊ password ထည့်ခြင်း အစရှိတဲ့ management ကိစ္စများကိုရပ်ဖို့ရန် ကွန်ပျူတာနှင့်ချိတ်ဆက်ရသော port ဖြစ်ပါတယ်။ အဓိကအားဖြင့် modular နှင့် SOHO (small office home office) ဆိုပြီး router နှစ်မျိုးရှိပါတယ်။

Modular Router

Network interface card များစွာကိုစိုက်သွင်းတပ်ဆင်နိုင်ရန် slot များစွာပါရှိတဲ့ router ကို modular router လို့ ခေါ်ပါတယ်။ ဆိုရရင် network interface လေးခုတပ်ဆင်နိုင်အောင် slot လေးခုပါက 4 slot modular router လို့ခေါ်ပါတယ်။ interface တစ်ခုသည် သီးခြား network ID တစ်ခုဖြစ်ပါတယ်။

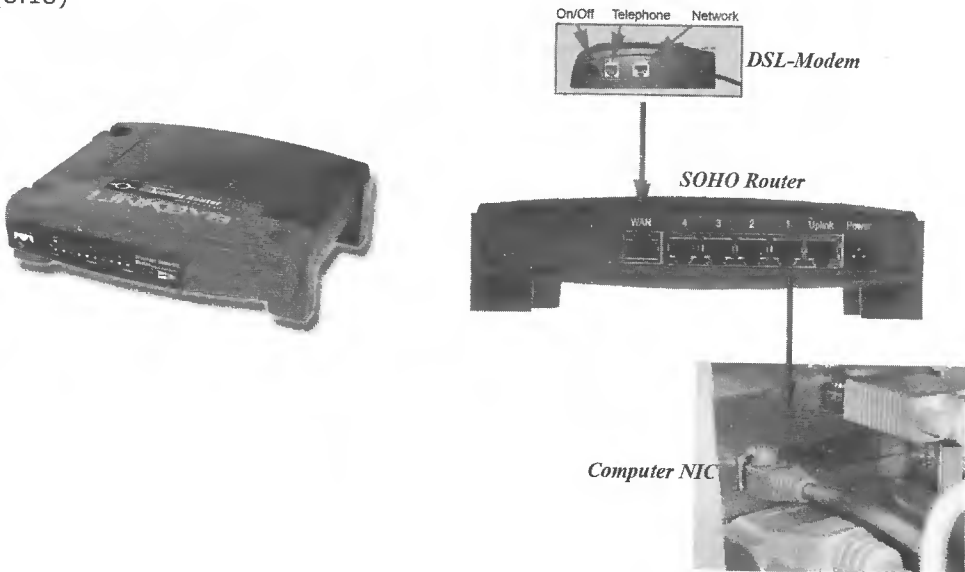
ပုံ (8.17)



SOHO router

SOHO router မျိုးကတော့ရောက modular တွေလို configuration များစွာလုပ်စရာမလိုပဲ သာမန်အိမ်သုံး၊ ရုံးသုံး network ငယ်တွေမှာ အသုံးပြုနိုင်တဲ့ အမျိုးအစားဖြစ်ပါတယ်။ အထူးသဖြင့် ADSL Broadband တို့ဖြင့် အင်တာနက် ချိတ်ဆက်တဲ့ network တွေမှာ internet gateway အဖြစ်အသုံးပြုကြပါတယ်။ ဒီrouter တွေသည် network ၂ခုကိုသာလျှင် route လုပ်ပေးနိုင်ပါတယ်။ ဆိုရရင် တဖက်က ISP network (WAN) နှင့်တဖက်က မိမိရဲ့ network (LAN) တို့ဖြစ်ပါတယ်။

ပုံ (8.18)



Network Standards

1980 ပြည့်နှစ် ဖေဖော်ဝါရီလတွင် IEEE သည် networking standard တွေကို သတ်မှတ်ရန်အတွက် ကော်မတီတစ်ရပ်ကိုဖွဲ့စည်းပြီး 802 project ကိုစတင်ဖော်ဆောင် ခဲ့ပါတယ်။ ၎င်း ကော်မတီမှ သတ်မှတ်သော standard တစ်ခုစီသည် ရှေ့တွင် 802 ဖြင့်စပါတယ်။ 802 ဆိုတာကတော့ ကော်မတီ ဖွဲ့စည်းသည့် 1980(80)၊ ဖေဖော်ဝါရီလ (2) ကို ရည်ညွှန်းပါတယ်။ 802 standard တစ်ခုစီရဲ့နောက်တွင် . (dot) ပါပြီး ၎င်း . (dot) နောက်တွင် ဂဏန်းတစ်လုံး (သို့) နှစ်လုံး ပါတတ်ပါတယ်။ (ဥပမာ - 802.3၊ 802.11) တို့ ကိန်းဂဏန်းတွေသည် 802 အောက်တွင်ရှိသော သီးခြား standard တစ်ခုစီကို ရည်ညွှန်းပါတယ်။

standard တစ်ခုစီသည် network speed၊ access method အသုံးပြုရမည့် cable အမျိုးအစား၊ ဝယ်ယူရမည့် NIC အမျိုးအစား၊ Topology အစရှိသည်တို့ကို သတ်မှတ်ပေးပါတယ်။ ယနေ့ အချိန်ထိတိုင်အောင် IEEE (I triple E) မှ သတ်မှတ်ပေးထားသော network standard ဆယ့်နှစ်မျိုး ရှိပါတယ်။ အဲဒီ standard တွေကတော့ အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

IEEE 802 Networking Standards

Standard	Topic
802.1	LAN/MAN Management (and Media Access Control Bridges)
802.2	Logical Link Control
802.3	CSMA/CD
802.4	Token Bus
802.5	Token Ring
802.6	Distributed Queue Dual Bus (DQDB) Metropolitan Area Network (MAN)
802.7	Broadband Local Area Networks
802.8	Fiber-Optic LANs and MANs
802.9	Isochronous LANs
802.10	LAN/MAN Security
802.11	Wireless LAN
802.12	Demand Priority Access Method
802.15	Wireless Personal Area Network
802.16	Wireless Metropolitan Area Network
802.17	Resilient Packet Ring
802.18	LAN/MAN Standards Committee

အဲဒီအထဲကအချို့ကို ယနေ့တိုင်အောင် အသုံးပြုနေကြဆဲဖြစ်သလို အချို့ကတော့ အသုံးမရှိသလောက် နည်းပါးနေပါပြီ။ ယနေ့ network တွေတည်ဆောက်တဲ့နေရာမှာ အဓိကအားဖြင့် IEEE 802.3 (Ethernet)၊ IEEE 802.5 (Token Ring) နှင့် IEEE 802.11 (Wireless) တို့သုံးမျိုးထဲမှ ရွေးချယ်နိုင်ပါတယ်။

ဒါပေမယ့် ethernet သည် အသုံးအများဆုံး ဖြစ်ပါတယ်။ ဘယ်လောက်ထိ အသုံးများသလဲဆိုရင် ယနေ့ network ရယ်လို့ဆိုလိုက်တာနှင့် ethernet ပင်ဖြစ်ပါလိမ့်မယ်။ ဒီ chapter အောက်မှာတော့ 802.3 နှင့် 802.5 တို့အကြောင်းကိုသာရှင်းလင်း ဖော်ပြသွားမှာဖြစ်ပြီး 802.11ကိုတော့ chapter(13) ကျမှဆက်လက်ဖော်ပြပါမယ်။

Ethernet (802.3)

Ethernet ကို 1970 ပြည့်နှစ်တွင် Xerox corporation မှ စတင်ဖော်ဆောင်ခဲ့ပါတယ်။ နောက်ပိုင်းမှာတော့ DEC ၊ Intel နှင့် Xerox တို့ သုံးဦးပေါင်းပြီး ပိုမိုဖွံ့ဖြိုးတိုးတက်အောင် လုပ်ဆောင် ခဲ့ကြပါတယ်။ အဲဒီအချိန်တုန်းကတော့ ထိုကုမ္ပဏီ သုံးခုတို့၏ ရှေ့ဆုံးစာလုံးသုံးခုပေါင်းပြီး DIX ethernet လို့ ခေါ်ဆိုခဲ့ကြပါတယ်။ ထိုအစောဆုံး Ethernet version မှာဆိုရင် coaxial cable ကို သုံးပြီး 3Mbps ဖြင့် လုပ်ဆောင်နိုင်ပါတယ်။ သိပ်မကြာခင်မှာပင် 10Mbps သို့ရောက်ရှိခဲ့ပါတယ်။ 1980 ပြည့်နှစ်ရောက်တဲ့အခါမှာ တော့ IEEE ၏ 802 project ကော်မတီမှ Ethernet ကို 802.3 လို့သတ်မှတ်ခဲ့ပါတယ်။

၎င်း 802.3 standard ကိုပင် လွန်ခဲ့သည့် ဆယ်စုနှစ် ၂ခုအတွင်း ethernet version အမျိုးမျိုးတို့ဖြင့် ပြုပြင်ပြောင်းလဲ အသုံးပြုခဲ့ကြသည့်အတွက် အခေါ်အဝေါ်တွေမှာ အနည်းငယ်ရှုပ်ထွေးမှု ရှိခဲ့ပါတယ်။ version ပြောင်းတာနှင့် အမျှ အဓိကပြောင်းလဲမှု ရှိတာက speed ပင်ဖြစ်ပါတယ်။ ဆိုရရင် 3Mbps ဖြင့်စခဲ့တဲ့ ethernet သည် လွန်ခဲ့သည့် ၁၀နှစ်တာကာလအတွင်း (1990 ခုနှစ်) မှာ 100Mbps၊ 1000Mbps (Gbps) ထိအောင် တိုးတက်လုပ်ဆောင်နိုင်ခဲ့ပြီး ယနေ့အချိန်မှာတော့ fiber cable တွေကို အသုံးပြုပြီး 10 Gigabit ethernet အဖြစ် အသုံးပြုနေနိုင်ပြီဖြစ်ပါတယ်။

Ethernet Specifications

Common Name	IEEE Standard	Speed	Type of Cabling
Ethernet	802.3	10 Mbps	Copper/Optical
Fast Ethernet	802.3u	100 Mbps	Copper/Optical
Gigabit Ethernet	802.3z	1 Gbps	Optical
Gigabit Ethernet	802.3ab	1 Gbps	Copper
10 Gigabit Ethernet	802.3ae	10 Gbps	Optical

အဲဒီလို တိုးတက်ပြောင်းလဲမှုပေါင်းများစွာဖြင့် speed အမျိုးမျိုးတို့ဖြင့် ethernet version အမျိုးမျိုး ပြောင်းလဲခဲ့သော်လည်း ethernet တွေမှာမပြောင်းလဲနိုင်တဲ့ အရာတစ်ခုရှိပါတယ်။ အဲဒါကတော့ ethernet standard တွေကိုလိုက်နာအသုံးပြုတဲ့ network မှာရှိတဲ့ ကွန်ပျူတာတွေတစ်လုံးနှင့် တစ်လုံး ဘယ်လိုဆက်သွယ်လုပ်ဆောင်ကြမလဲဆိုတဲ့ access method ဖြစ်ပါတယ်။ ethernet network တွေမှာ အသုံးပြုတဲ့ access method ကို CSMA/CD လို့ခေါ်ပါတယ်။ CSMA/CD ရဲ့အဓိကလုပ်ဆောင်ပုံတွေကို chapter (3) တွင် ရှင်းလင်းဖော်ပြခဲ့ပြီး ဖြစ်ပါတယ်။ ဒီနေရာမှာတော့ CSMA/CD ရဲ့အဓိပ္ပာယ်ကို ခြုံငုံမိအောင် ဦးစားပေး ရှင်းလင်းဖော်ပြသွားမှာ ဖြစ်ပါတယ်။

CSMA/CD တွင်ကွန်ပျူတာတစ်လုံးမှ data ပို့လိုတဲ့အခါပထမဦးစွာ transmission media လို့ခေါ်တဲ့ cable ပေါ်မှာအခြားကွန်ပျူတာတစ်လုံးလုံးမှ transmit လုပ်ထားသော signal (carrier) တွေ ရှိမရှိဆိုတာကိုထောက်လှမ်း (sense) ရပါတယ်။ မအားဘူးဆိုရင်ခေတ္တစောင့်ဆိုင်းပြီးနောက်တစ်ကြိမ်ထပ်မံ ထောက်လှမ်းရပါတယ်။ အားသွားပြီဆိုမှမိမိပို့လိုတဲ့ data တွေကိုစတင် transmit လုပ်နိုင်မှာဖြစ်ပါတယ်။ ဒီအထိသည် carrier sense ဖြစ်ပါတယ်။

သဘောကတော့ transmission media အားနေတယ်လို့ ထောက်လှမ်းသိရှိပြီဆိုတာနှင့် မည်သည့်ကွန်ပျူတာကနေမဆို transmit လုပ်နိုင်ကြပါတယ် (multiple access ဖြစ်ပါတယ်)။ အတယ်၍များ network တွင်းမှာရှိတဲ့ ကွန်ပျူတာ နှစ်လုံးသည် တစ်ချိန်တည်း၊ တစ်ပြိုင်နက် transmission media ကိုထောက်လှမ်းမယ်။ transmission media ပေါ်မှာဘာ signal မှမရှိဘူး။ အားနေတယ်လို့ ၂လုံးစလုံးကထောက်လှမ်းသိရှိပြီး ပြိုင်တူ transmit လုပ်ကြမယ်ဆိုရင် signal တွေ တစ်ခုနှင့် တစ်ခုထပ်သွားပြီး ပုံသဏ္ဍန်ပျက်ယွင်းသွားကာ ဘာကိုဆိုလိုသလဲ ဆိုတာကို အဓိပ္ပာယ် ဖော်မရတော့ပါ။ အဲဒီဖြစ်စဉ်ကို collision လို့ခေါ်ပါတယ်။

CSMA/CD ၏နောက်ဆုံးအပိုင်းဖြစ်တဲ့ CD (collision detection) သည် collision ဖြစ်တာကို အမြန်ဆုံးသိရမယ်။ သိပြီးတဲ့အခါ ဘယ်လို ဆက်လက်ဖြေရှင်း မလဲဆိုတဲ့ နည်းလမ်းကို ရည်ညွှန်းပါတယ်။ ဆိုရရင်ကွန်ပျူတာတစ်လုံးသည်မိမိ transmit လုပ်လိုက်တဲ့ data တွေ collide ဖြစ်သွားပြီလို့သိတာနှင့် ချက်ချင်း ရပ်လိုက်ကာ အချိန်တစ်ခုစောင့်ဆိုင်းပြီးမှ ပြန်လည် transmit လုပ်ကြပါတယ်။ အဲဒီ "wait and retransmission" လုပ်ငန်းစဉ်ကို data ပေးပို့ခြင်းလုံးဝအောင်မြင်သည်အထိ ထပ်ခါတလဲလဲ လုပ်ဆောင် ကြပါတယ်။

Ethernet Feature

Speed	10Mbps, 100Mbps (Fast Ethernet), 1000Mbps (Gigabit Ethernet), and 10,000Mbps (10G Ethernet)
Access Method	CSMA/CD
Topology	Star, bus (bus is not widely used today)
Media	Copper wire and fiber-optic cable

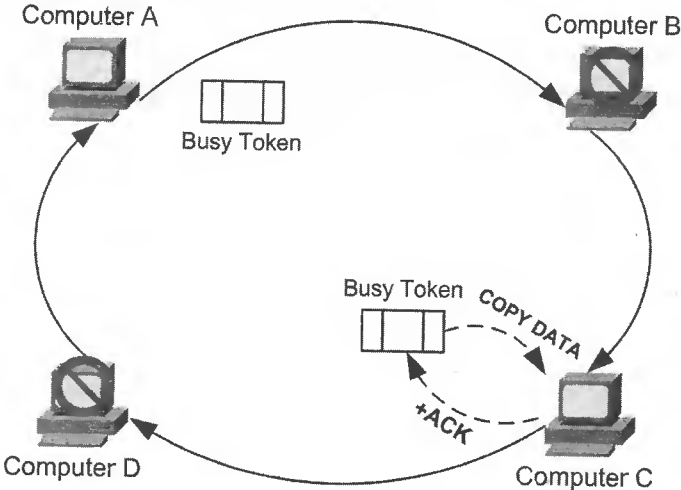
Token Ring (802.5)

ယနေ့အချိန်မှာတော့ ring network တွေ တည်ဆောက်အသုံးပြုမှု နည်းပါးလာခြင်းနှင့်အတူ token Ring ကို အသုံးပြုမှုသည်လည်း အတော်လေးကို နည်းပါးလာနေပါတယ်။ ဒါပေမယ့်လည်း networking ကိုလေ့လာတဲ့နေရာမှာ သိထားသင့်သော access method တစ်ခုပင်ဖြစ်ပါတယ်။ token Ring ကို 1980 ဝန်းကျင်ခန့်က IBM မှ စတင်ဖော်ဆောင်ခဲ့ပြီး 1988 ခုနှစ်မှာတော့ IEEE/ANSI တို့မှ 802.5 လို့သတ်မှတ်ခဲ့ကြပါတယ်။ 1990 ပြည့်နှစ်အစောပိုင်းကာလတွေတုန်းက ethernet နှင့်အပြိုင် လူသုံးများသော access method တစ်ခုလည်းဖြစ်ခဲ့ပါတယ်။ အဲဒီအချိန်လောက်မှာပဲ ကုန်ကျစရိတ်

သက်သာခြင်း၊ speed ပိုမြန်ခြင်းတို့တွင် ethernet သည်လျှင်မြန်စွာ ဖွံ့ဖြိုးတိုးတက်လာခဲ့သည့်အတွက် token ring သည်နောက်ကောက်ကျခဲ့ရပါတယ်။

token ring network တွေမှာဆိုရင် ကွန်ပျူတာတစ်လုံးမှတစ်လုံးသို့ data ပေးပို့ရယူကြရန် token လို့ခေါ်သည့် 3bytes အရွယ်အစားရှိ packet ကိုအသုံးပြုကြရပါတယ်။ ၎င်း token သည် free နှင့် busy ဆိုတဲ့ အခြေအနေ နှစ်ခုထဲက တစ်ခုမှာ အမြဲတမ်းရှိနေပါတယ်။ network အတွင်းရှိ မည်သည့် ကွန်ပျူတာကမှ transmit လုပ်ဖို့မရှိဘူးဆိုရင် ၎င်း token သည်စက်ဝိုင်းပုံ ring တစ်လျှောက်အဆက်မပြတ် လှည့်ပတ်နေပါလိမ့်မယ်။ အဲဒီအခြေအနေမှာဆိုရင် token သည် free token ဖြစ်ပါတယ်။ ကွန်ပျူတာ တစ်လုံးသည် transmit လုပ်ဖို့ရန်ရှိလာပြီဆိုရင် free token ကိုလက်ဝယ်ရရှိအောင်စောင့်ဆိုင်းရယူရပါတယ်။ free token ကိုလက်ဝယ်ရရှိပြီဆိုရင် header | data | trailer တို့ကို ထည့်သွင်းပြီး frame တစ်ခုအဖြစ်သို့ ပြောင်း၍ ring ပေါ်သို့ တင်ပေးလိုက်ပါတယ်။ အဲဒီအခြေအနေမှာဆိုရင် busy token ဖြစ်သွားပါပြီ။

ပုံ (9.1)



ဥပမာပုံ(9.1) မှာရှိတဲ့ကွန်ပျူတာ A သည် ကွန်ပျူတာ C ထံသို့ data ပေးပို့ရန် free token ကို ရယူလိုက်ပါတယ်။ အဲဒီနောက်မှာ ကွန်ပျူတာ C ၏ လိပ်စာထည့်သွင်းပြီး busy token အဖြစ်ပြောင်း၍ ring ပေါ်သို့တင်ပေးလိုက်ပါတယ်။ ကွန်ပျူတာ B သို့ရောက်ရှိတဲ့အခါ token ထဲတွင်ပါလာသော destination address ကိုကြည့်၍ မိမိအတွက် မဟုတ်ဘူးဆိုတာသိရှိပြီး token ကို ring ပေါ်သို့ပြန်တင်ပေးလိုက်ပါတယ်။

ကွန်ပျူတာ C သို့ ရောက်ရှိလာတဲ့အခါမှာတော့ မိမိအတွက်ဆိုတာ သိရှိပြီး token ထဲတွင် ပါလာသော data များကို မိတ္တူကူးယူပါလိမ့်မယ်။ ရယူပြီးသွားတဲ့အခါ 'လက်ခံရရှိပါတယ်' ဆိုတဲ့ ACK (acknowledgement) ကို ၎င်း token ထဲထပ်ပေါင်းထည့်ပြီး ring ပေါ်သို့ပြန်တင်ပေးလိုက်ပါတယ်။ ထို busy token သည် ကွန်ပျူတာ D ကိုဖြတ်ပြီး မူလပေးပို့သူ ကွန်ပျူတာ A ထံသို့ပြန်လည်ရောက်ရှိပါလိမ့်မယ်။

အဲဒီအခါ ကွန်ပျူတာ A မှ မိမိပို့လိုက်သည် token သည် network တစ်ပတ်ပြည့်အောင်သွားပြီးပြီ ဆိုတာသိရှိပြီး data များကိုဖျက်၍ free token အဖြစ် ring ပေါ်ပြန်တင်ပေးလိုက်ပါတယ်။

နောက်ထပ် transmit လုပ်မည့်သူမရှိမချင်း၎င်း free token သည် network ring တစ်လျှောက် အဆက်မပြတ် လှည့်ပတ်နေပါလိမ့်မယ်။ token passing ရဲ့လုပ်ဆောင်နေပုံကို စဉ်းစားကြည့်မယ်ဆိုရင် token သည် ring တစ်လျှောက် အဆက်မပြတ် လှည့်ပတ်နေရသည့်အတွက် နှေးလိမ့်မယ်လို့ ထင်စရာရှိပါတယ်။ ဒါပေမယ့် token သည် အလင်းအလျှင်၏ ၇၀ ရာခိုင်နှုန်းခန့်ဖြင့် လှည့်ပတ်နေသည့်အတွက် network တစ်ခုကို တစ်စက္ကန့်တွင် အကြိမ်တစ်သောင်းခန့်ပတ်နိုင်ပါတယ်။

token ring ရဲ့ထူးခြားသိသာတဲ့အားသာချက်ကတော့ collision လုံးဝမဖြစ်နိုင်ခြင်းဖြစ်ပါတယ်။ သို့သော် token ring network တစ်ခုကို တည်ဆောက်မယ်ဆိုရင် ethernet network တွေထက် ပိုမိုကုန်ကျပါတယ်။ ဒါ့အပြင် ဆက်ကြောင်းတနေရာရာမှာ ချွတ်ယွင်းချက် ရှိနေပြီဆိုရင် network တခုလုံးသုံးမရဖြစ်စေတတ်တဲ့အားနည်းချက်တွေလည်းရှိပါတယ်။ token ring network တွေသည် 4 (သို့) 16 (သို့) 100 Mbps နှုန်းဖြင့် လုပ်ဆောင်နိုင်ပါတယ်။ အမြင့်ဆုံး 100Mbps ဖြင့် လုပ်ဆောင်နိုင်သည့် token ring standard ကို HSTR (high-speed token ring) လို့ခေါ်ပါတယ်။ HSTR ကို twisted pair (သို့) fiber cable တို့သုံးပြီး တည်ဆောက်နိုင်ပါတယ်။

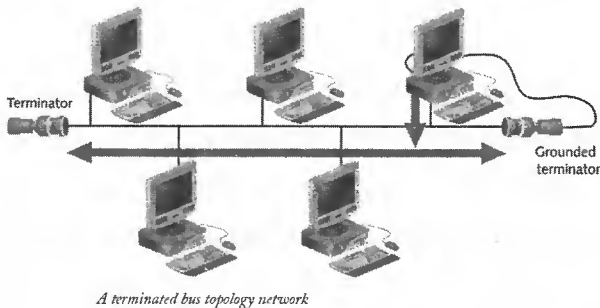
Network Topology

အခြေခံအားဖြင့် topology ဆိုတာက ကွန်ပျူတာတွေ၊ ပရင်တာတွေ အစရှိတဲ့ node တွေကို ဘယ်လိုနေရာချပြီး network တစ်ခုအဖြစ် တည်ဆောက်ထားသလဲဆိုတဲ့ အခင်းအကျင်းပုံသဏ္ဍာန်ပင် ဖြစ်ပါတယ်။ တစ်နည်းအားဖြင့် network တစ်ခုရဲ့ မြေပုံလို့လည်းဆိုနိုင်ပါတယ်။ topology လေးမျိုးရှိပါတယ်။ BUS၊ STAR၊ RING နှင့် MESH တို့ဖြစ်ပါတယ်။ အချို့သော network တွေကို အဲဒီလေးမျိုးထဲက ပြုပြင်စေ၊ ခုနစ်မျိုးဖြစ်စေ ပေါင်းစပ်တည်ဆောက်ထားခြင်းမျိုးလည်းရှိပါတယ်။ အဲဒီလို ကပြား network မျိုးတွေကို hybrid topology network တွေလို့ခေါ်ဆိုနိုင်ကြပါတယ်။

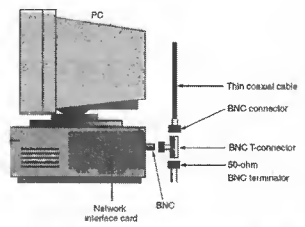
network တစ်ခုကိုတည်ဆောက်ဖို့ရန် ပုံစံမထုတ်ခင်မှာ ဖော်ပြခဲ့တဲ့ topology လေးမျိုး အကြောင်းကို သိထားဖို့လိုပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ topology ပြောင်းတာနှင့် network အမျိုးအစား (ethernet token ring) အသုံးပြုရမည့် cable နှင့် သွယ်တန်းချိတ်ဆက်ထားရှိမှု အခင်းအကျင်းအစီအမံ၊ connecting device လို့ခေါ်တဲ့ switch နှင့် NIC အမျိုးအစားတို့မတူပဲ ကွဲပြားခြားနားစွာ လိုအပ်ကြမှာ ဖြစ်ပါတယ်။ ဒါ့အပြင် network မှာ ချွတ်ယွင်းချက်ရှိလာလို့ troubleshoot လုပ်ရန်ပဲဖြစ်ဖြစ်၊ network infrastructur ကိုပြောင်းလဲဖို့ရန် ကွန်ပျူတာတွေ၊ ပရင်တာတွေ ထပ်တိုးတပ်ဆင်ဖို့ရန် လိုအပ်လာတဲ့ အခါမျိုးတွေမှာ network topology ကို သိထားမှသာလျှင် ဖြေရှင်းနိုင်ကြမှာ ဖြစ်ပါတယ်။

BUS Topology

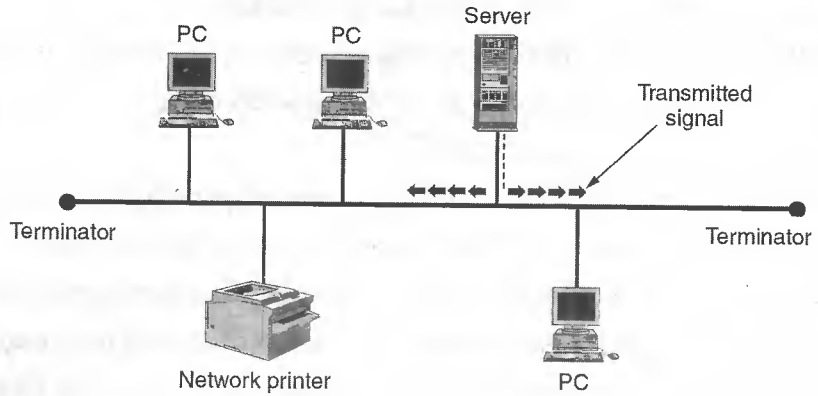
BUS သည် တစ်ချိန်တုန်းကတော့ အသုံးပြုမှုအများဆုံး network topology ဖြစ်ပြီး ယနေ့အခါ မှာတော့ အတော်လေးကို တွေ့ရခဲတဲ့ topology မျိုးဖြစ်ပါတယ်။ BUS topology ဖြင့်တည်ဆောက် တဲ့အခါ network ရဲ့ တစ်ဖက်အစကနေ အခြားတစ်ဖက်အဆုံးထိ ကန့်လန့်ဖြတ် cable (coaxial cable) တစ်ချောင်းကို သွယ်တန်းရပါတယ်။ ပြီးမှလိုတဲ့ နေရာကနေ T-connector ၊ BNC-connector တို့ဖြင့် ကွန်ပျူတာတွေကို ချိတ်ဆက်တပ်ဆင်ရပါတယ်။ ၎င်းကျောရိုး single cable ကို BUS လို့ခေါ်ပါတယ်။ cable အမျိုးအစားကတော့ coaxial cable ဖြစ်ပါတယ်။



ပုံ (10.1)



အဲဒီလို cable တစ်ချောင်းတည်းဖြင့် ကွန်ပျူတာအားလုံးကို ချိတ်ဆက်ထားသည့်အတွက် ကွန်ပျူတာတစ်လုံးနှင့် တစ်လုံး data တွေပေးပို့ဖလှယ်ကြတဲ့နေရာမှာ ၎င်း cable ကိုပင် အားလုံးမျှဝေ သုံးစွဲကြရပါတယ်။ ဒါကြောင့် အချိန်တစ်ခုတွင် ကွန်ပျူတာတစ်လုံးတည်းမှသာ transmit လုပ်နိုင်ကြပါတယ်။



ပုံ (10.2)

ကွန်ပျူတာတစ်လုံးမှ အခြားတစ်လုံးဆီသို့ data ပို့မယ်ဆိုရင် ပို့လိုတဲ့ ကွန်ပျူတာမှ data တွေ ပို့လိုက်ပြီဆိုတာကို network ပေါ်မှာ broadcast လုပ်ပါတယ်။ broadcast လုပ်လိုက်သည့်အတွက် ကွန်ပျူတာတစ်လုံးမှ တစ်လုံးသို့ ဖြတ်သန်းပြီး network ထဲမှာရှိတဲ့ ကွန်ပျူတာအားလုံးတို့ထံသို့ signal များရောက်ရှိလာမှာဖြစ်ပါတယ်။ ဒါပေမယ့် အဲဒီ signal တွေထဲမှာ ဘယ်ကွန်ပျူတာအတွက်သာဆိုတဲ့ လိပ်စာပါရှိသည့်အတွက် signal များကို လက်ခံရရှိသော်လည်း မသက်ဆိုင်သည့် ကွန်ပျူတာများအနေနှင့် ၎င်း signal တွေကို လျစ်လျူရှုလိုက်မှာ ဖြစ်ပါတယ်။

သက်ဆိုင်ရာကွန်ပျူတာမှသာလျှင် signal တွေထဲမှာပါရှိတဲ့ လိပ်စာကို ကြည့်၍ မိမိအတွက်ဆိုတာ သိရှိပြီး data တွေကို လက်ခံမှာဖြစ်ပါတယ်။ တနည်းဆိုရရင် BUS topology network ထဲမှာရှိတဲ့ ကွန်ပျူတာတွေသည် cable (BUS) တလျှောက် signal တွေ ရွေ့လျား ဖြတ်သန်းခြင်းနှင့် ပါတ်သက်ပြီး မည်သည့်တာဝန်မှ မရှိပါဘူး။ ၎င်းတို့ဆီ ဦးတည်ရောက်ရှိလာတဲ့ signal တွေကို မိမိနှင့်ဆိုင်၊ မဆိုင် သတိထားစောင့်ကြည့်ရုံသာ ဖြစ်ပါတယ်။

BUS network တွေရဲ့အစနှင့် အဆုံး (သို့) cable bus ရဲ့အစနှင့်အဆုံး နေရာတွေမှာ terminator လို့ခေါ်တဲ့ 50 ohm resistor တွေလိုတပ်ဆင်ထားရပါတယ်။ terminator တွေရဲ့အဓိကလုပ်ဆောင် မှုကတော့ သူတို့ထံရောက်လာတဲ့ signal တွေကို cable ပေါ်ကနေပျောက်သွားအောင် အဆုံးသတ်ရှင်းထုတ် ပေးခြင်းဖြစ်ပါတယ်။ အကယ်၍ များ terminator တွေသာတပ်ဆင်ထားမှုမရှိဘူးဆိုရင် signal တွေသည် cable ရဲ့အစွန်းနှစ်ဖက်ကြားမှာ အဆုံးမရှိရွေ့လျားဖြတ်သန်းနေပါလိမ့်မယ်။ ဒါဆိုရင် cable (bus) ပေါ်မှာ signal တစ်ခုရှိနေသမျှ ကာလပတ်လုံး နောက်ထပ် signal သစ်များကို ထပ်မံ transmit မလုပ်နိုင်တော့ပါ။ အဲဒီဖြစ်စဉ်ကို signal bounce လို့ခေါ်ပါတယ်။

signal bounce ကိုပိုမို သဘောပေါက်နားလည်အောင် အနီးစပ်ဆုံး ဥပမာဆောင်ရရင် ပဲတင်သံ

ဖြစ်နိုင်တဲ့ လှိုင်းခေါင်းထဲမှာလူနှစ်ယောက် ဟိုဘက်ဒီဘက်ရပ်ပြီး စကားအော်ပြောကြပုံနှင့်တူတယ် လို့ဆိုနိုင်ပါလိမ့်မယ်။ တဖက်ကပြောတဲ့စကားသံတွေသည်ပဲ့တင်ထပ်နိုင်သလိုအခြားတစ်ဖက်ကပြန်ပြောတဲ့ အသံတွေသည်လည်းပဲ့တင်သံများဖြစ်ပေါ်နိုင်ပါတယ်။ ဒါဆိုရင်ရှေ့ကပြောခဲ့တဲ့စကားသံကြောင့်ပဲ့တင်ထပ်ပြီး ဆူညံနေသည့်အတွက်အချိန်တစ်ခုကြာပြီးသည့်တိုင် နောက်ထပ်စကားပြောနိုင်ကြမှာ မဟုတ်ပါ။ ဒီနေရာမှာ ပဲ့တင်သံသည် ဘယ်တော့မှ အသံတိမ်မသွားနိုင်ပဲ ဒီအတိုင်းဆက်မြည်နေမယ်လို့ စဉ်းစားကြည့်မယ်ဆိုရင် နောက်ထပ်လည်း စကားဆက်ပြောနိုင်ကြတော့မည် မဟုတ်ပါ။ BUS network တွေမှာတော့ အဲဒီလို ပြဿနာမျိုးမဖြစ်ရလေအောင် terminator တွေကသူတို့ဆီရောက်လာတဲ့ signal တွေ၊ တစ်နည်းဆိုရရင် ရှေ့က signal တွေကို အဆုံးသတ် ရှင်းလင်း ဖယ်ရှားခြင်းဖြင့် နောက်ထပ် signal အသစ်များ transmit လုပ်စေနိုင်ပါတယ်။

BUS network တွေရဲ့အဓိကအားနည်းချက်ကတော့ကွန်ပျူတာတွေထပ်တိုးတပ်ဆင်တာနှင့်အမျှ network ရဲ့လုပ်ဆောင်မှု မြန်နှုံးကျဆင်းလာခြင်းပင် ဖြစ်ပါတယ်။ ဘာဖြစ်လို့လဲ ဆိုတော့ ကွန်ပျူတာ အားလုံးသည် bus တစ်ခုတည်းကို မျှဝေသုံးစွဲရသည့်အတွက် တစ်လုံးက transmit လုပ်နေချိန်မှာ ကျန်တာတွေကစောင့်ဆိုင်းပြီးအလှည့်ကျ transmit လုပ်ရပါတယ်။ ဒါကြောင့်အရေအတွက်များလာတာနှင့် အမျှ transmit လုပ်မည့် ကွန်ပျူတာများလာမှာ ဖြစ်သလို မိမိအလှည့်ကျဖို့ရန် အချိန်ပေးပြီး စောင့်ဆိုင်း ရပါလိမ့်မယ်။ အဲဒီလိုစောင့်ဆိုင်းရတာကိုအသုံးပြုသူများအနေနှင့် မသိနိုင်ပါဘူး။ data transfer လုပ်ရတာ နှေးတယ်လို့ပဲခံစားရမှာဖြစ်ပါတယ်။

နောက်တစ်မျိုးအားနည်းချက် ကတော့ cable ရဲ့ဘယ်နေရာမှာ ချွတ်ယွင်းချက် ရှိနေသလဲ ဆိုတာကို troubleshoot လုပ်ဖို့ရန် ခက်ခဲခြင်းဖြစ်ပါတယ်။ ဘာကြောင့် ခက်ခဲရသလဲဆိုတာကို ငယ်ငယ်တုန်းကနို့ဆီခွက်မှာအပေါက်ဖောက် ကြီးနှင့်တန်းပြီး လူလေးငါးယောက် ဆက်သွယ်စကားပြောကြတဲ့ တယ်လီဖုန်းဆက် ကစားနည်းနှင့်ယှဉ်ပြီး စဉ်းစားကြရအောင်။ ထို ကစားနည်းတွင် တစ်ဖက်အစွန့် ပထမတစ်ယောက်က ခွက်နားကပ်ပြီး အကြောင်းအရာတစ်ခုကို ခပ်တိုးတိုးပြောမယ်။ ဒုတိယလူက သူကြားတဲ့အတိုင်းတတိယတစ်ယောက်ကိုပြန်ပြောမယ်။ အဲဒီလိုနည်းနှင့် နောက်ဆုံးတစ်ယောက်နားထဲကို ရောက်မယ်ပေါ့။ တခါတလေမှာ ဒုတိယ၊ တတိယ အစရှိတဲ့ ကြားလူတွေက ကြားတာတွေကိုနားလည်သလို ပြန်ပြောရင်းနှင့် နောက်ဆုံးတစ်ယောက် ရောက်တဲ့အခါ ပထမဆုံးတစ်ယောက်က ဘာပြောလိုက်သလဲ ဆိုတာကို နားမလည် နိုင်လောက်အောင်ဖြစ်တတ်ပါတယ်။ အဲဒီဖြစ်စဉ်တွင် ဘယ်သူကြောင့် ဘယ်နေရာမှာ မှားသွားသလဲဆိုတာကို အဖြေရှာဖို့အတော်လေးခက်ပါလိမ့်မယ်။ BUS network တွေမှာလည်း ထိုနည်း လည်းကောင်းပါဘဲ။ ပို့တဲ့ ကွန်ပျူတာကတော့ပို့လိုက်တာပဲ။ လက်ခံတဲ့ ကွန်ပျူတာရောက်တဲ့အခါမှာတော့ "error occured" လို့သာပြောနိုင်တယ်။ ဘယ်နေရာ၊ ဘယ် point ၏ ချွတ်ယွင်းချက်ကြောင့်လဲဆိုတာကို ရှာဖွေဖို့ရန် ခက်ခဲတတ်ပါတယ်။

နောက်ဆုံးအားနည်းချက်ကတော့ BUS ရဲ့တစ်နေရာရာမှာဆက်သွယ်မှုပြတ်တောက်နေပြီဆိုတာနှင့် network တစ်ခုလုံးသုံးမရဖြစ်စေတတ်ပါတယ်။ အဲဒီလိုအားနည်းချက်တွေကြောင့်အခြား network တွေနှင့်ယှဉ်လျှင် ကုန်ကျစရိတ်သက်သာသော်လည်း ယနေ့အခါမှာတော့အသုံးပြုမှုမရှိသလောက်နည်းပါလာတာကိုတွေ့ရပါမယ်။

Ring Topology

ring topology မှာဆိုရင် ကွန်ပျူတာတစ်လုံးစီသည် ဘေး ဥဘက်မှာရှိတဲ့ အနီးဆုံးကွန်ပျူတာ ဟုလုံးစီသို့ cable ဖြင့် ချိတ်ဆက်သွယ်တန်းပြီး network တစ်ခုလုံးကို စက်ဝိုင်းပုံဖြစ်အောင် နေရာချ ချိတ်ဆက်ထားပါတယ်။ ဆိုရရင် နောက်ဆုံးကွန်ပျူတာသည် ပထမဆုံး နေရာချထားသော ကွန်ပျူတာကို ပြန်လည်ချိတ်ဆက်ထားသည့်အတွက် BUS မှာကဲ့သို့အစနှင့်အဆုံးဆိုတာမရှိပဲ network တစ်ခုလုံးသည် စက်ဝိုင်းပုံဖြစ်နေပါလိမ့်မယ်။ ring network တွေမှာအသုံးပြုတဲ့ cable သည် twisted pair (သို့) fiber cable ဖြစ်ပါတယ်။ IEEE သတ်မှတ်ချက်အရ ring topology network တွေသည် 802.5 ဖြစ်ပါတယ်။



ပုံ (10.3)

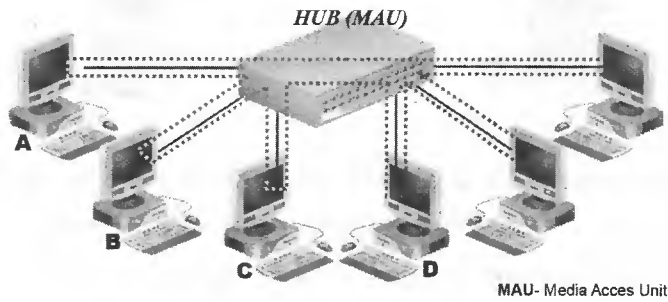
ring network ပေါ်မှာ data တွေကို transmit လုပ်တဲ့အခါစက်ဝိုင်းပတ်လမ်းတစ်လျှောက် နာရီလက်တံအတိုင်း လားရာတစ်ဖက်တည်းသွားပါတယ်။ ကွန်ပျူတာတစ်လုံးစီသည် မိမိနှင့် သက်ဆိုင်သော (ဝါ) မိမိထံ လိပ်စာတပ်ထားသော data packet တွေကိုသာ လက်ခံရယူပြီး မသက်ဆိုင်ပါက ဆက်လက် forward လုပ်ပေးပါတယ်။ အဲဒီလို forward လုပ်တဲ့နေရာမှာ ကွန်ပျူတာ တစ်လုံးစီသည် repeater အဖြစ်ပါလုပ်ဆောင်သည့်အတွက် ring topology network ထဲမှာရှိတဲ့ ကွန်ပျူတာ တွေသည် data ပို့လွှတ်ခြင်းကို အားလုံးပူးပေါင်းဆောင်ရွက်ရတယ်လို့ ဆိုနိုင်ပါတယ်။

အဲဒီအချက်သည် bus topology နှင့်မတူတဲ့အချက် ဖြစ်ပါတယ်။ ဒါကြောင့် bus topology ကို passive topology လို့ခေါ်ပြီး ring topology ကို active topology လို့ခေါ်ကြပါတယ်။ နောက်ထပ်မတူတဲ့အချက်က ring topology သည် အဆုံးအစမရှိသည့်အတွက် ပို့လွှတ်လိုက်တဲ့ data (busy token) တွေသည် မူလပေးပို့သည့် ကွန်ပျူတာဆီ ပြန်ရောက်တဲ့အခါ ခရီးစဉ် အဆုံးသတ် ရပါတယ်။

ring network တစ်ခုမှာ ကွန်ပျူတာတွေကို တစ်လုံးနှင့် တစ်လုံးစီတန်းချိတ်ဆက် ပြီး network တစ်ခုလုံးကို စက်ဝိုင်းပုံဖြစ်အောင် တည်ဆောက်ထားတယ်လို့ ဆိုခဲ့ပါတယ်။ သို့သော် ring network တစ်ခုကို အပြင်ပန်းအရ ကြည့်မယ်ဆိုရင် တည်ဆောက်ပုံမှာ star topology network တွေနှင့် အတူတူဖြစ်နေတာကို တွေ့ရပါလိမ့်မယ်။ star topology network တွေနှင့် တူတယ် ဆိုရင် ဘယ်မှာ စက်ဝိုင်းပုံ ရှိလို့တုန်းဟု မေးစရာရှိလာနိုင်ပါတယ်။

အပြင်ပန်းတည်ဆောက်ပုံအရတော့ star network တွေမှာ switch (သို့) hub တွေကိုဗဟိုထားပြီး ကွန်ပျူတာတွေက လာရောက်ချိတ်ဆက်ကြသလို ring network တွေမှာလည်း ထိုနည်းအတိုင်းဖြစ်သည့်အတွက် အတူတူပဲလို့ထင်စရာ ရှိပါတယ်။ ဒါပေမယ့် star network တွေမှာ ethernet technology ကို အသုံးပြုပြီး ring network တွေမှာ token ring technology ကို အသုံးပြုပါတယ်။ အဲဒီကွာခြားချက်အရပင် star နှင့် ring network တွေမှာအသုံးပြုတဲ့ switch တို့၊ NIC တို့သည်လည်း မတူကြပါဘူး။ ethernet switch၊ ethernet adapter (NIC)၊ token ring switch (MAU)၊ token ring adapter (NIC) အစရှိသဖြင့် အမျိုးအစားမတူပဲ ကွဲပြားကြပါတယ်။

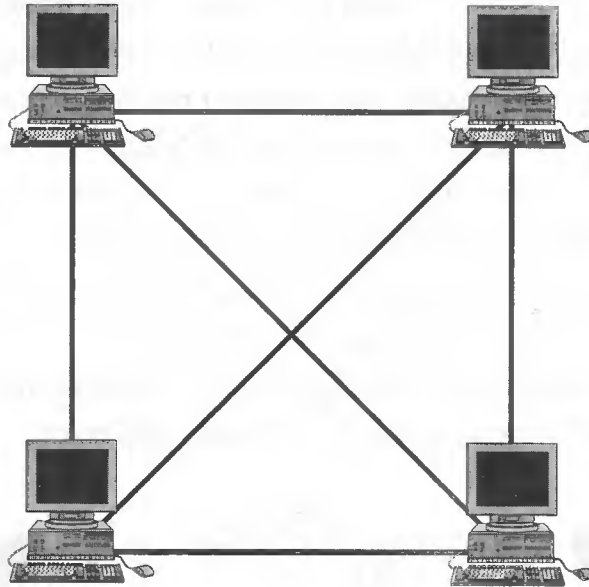
token ring switch တွေသည် ethernet switch တွေနှင့်ပုံသဏ္ဍာန်အရဆင်တူသော်လည်း အတွင်းပိုင်းမှာ data သွားတဲ့အခါ ရှေ့မှာဖော်ပြခဲ့သလိုပင် စက်ပိုင်းပုံဖြစ်အောင်တည်ဆောက်ထားပါတယ်။ အောက်ဖော်ပြပါပုံ(10.4)တွင် ကြည့်ပါ။ အရောင်ခြယ်ထားတဲ့ လိုင်းတွေသည် cable များကို ရည်ညွှန်းပြီး အစက်ချပုံဖော်ထားတဲ့လိုင်းတွေကတော့ data ဖြတ်သန်းစီးဆင်းပုံဖြစ်ပါတယ်။



ပုံ (10.4)

ring Topology ရဲ့အဓိက အားနည်းချက်ကတော့ ကွန်ပျူတာတစ်လုံးပျက်ပြီဆိုရင် network တစ်ခုလုံးသုံးမရဖြစ်စေပါတယ်။ ဥပမာဆိုရရင် ကွန်ပျူတာ A ကနေ D ကို message တစ်ခုကိုပို့မယ်ဆိုပါစို့။ ဒါဆိုရင် ကွန်ပျူတာ A မှပို့လိုက်သည့် message သည် ကွန်ပျူတာ D သို့မရောက်ခင်ကြားမှာရှိတဲ့ ကွန်ပျူတာ B နှင့် C တို့မှ NIC ၂ခုကိုဖြတ်သန်းသွားရပါမယ်။ အကယ်၍ များကွန်ပျူတာ B နှင့် C တို့ထဲကတစ်လုံးလုံးသည် ပုံမှန် လုပ်ဆောင်နိုင်မှု မရှိတော့ဘူးဆိုရင် ကွန်ပျူတာ A မှပို့လိုက်တဲ့ message သည် ကွန်ပျူတာ D ထံသို့ ရောက်ရှိ နိုင်တော့မည် မဟုတ်ပါ။ ဒါအပြင် data transmit လုပ်တဲ့နေရာမှာ network အတွင်းရှိ ကွန်ပျူတာအားလုံး ပါဝင် လုပ်ဆောင်ကြရသည့်အတွက် ကွန်ပျူတာ အရေအတွက်များလာတာနှင့် အမျှ အချိန်ပိုကြာတာကို ကြုံတွေ့ရနိုင်ပါတယ်။ အဲဒီလိုအားနည်းချက်တွေကြောင့် ယနေ့ network တွေမှာ ring topology ကို အသုံးပြုမှု နည်းလာတာကို တွေ့ရပါလိမ့်မယ်။

Mesh Topology



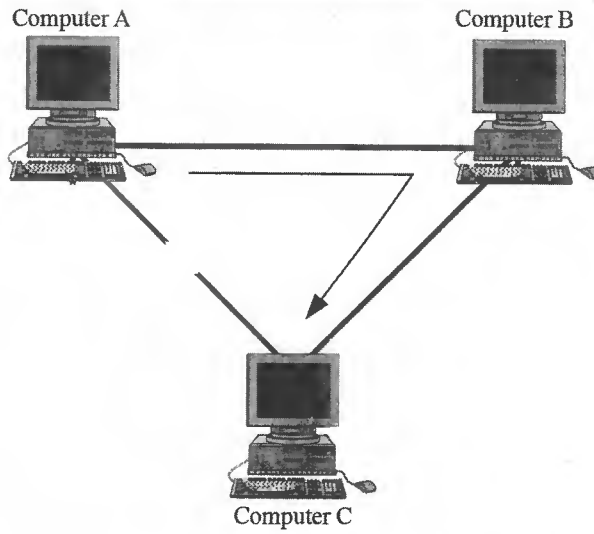
ပုံ (10.5)

mesh topology မှာဆိုရင် ကွန်ပျူတာ တစ်လုံးစီကနေ network တွင်းမှာရှိတဲ့ အခြားကွန်ပျူတာ အားလုံးစီကို သီးခြား cable တစ်ချောင်းစီဖြင့် point-to-point ချိတ်ဆက်ထားပါတယ်။ ဥပမာဆိုရင် ကွန်ပျူတာလေးလုံးကို full mesh ဖြင့်ချိတ်ဆက်မယ်ဆိုရင် connection အားလုံး ဘယ်လောက်ရှိမလဲ ဆိုတာကို အောက်ဖော်ပြပါ ပုံသေနည်းဖြင့်တွက်ထုတ်နိုင်ပါတယ်။

$$\begin{aligned}
 \text{စုစုပေါင်း connection အရေအတွက်} &= n(n-1)/2 \\
 &= 4(4-1)/2 \\
 &= 6
 \end{aligned}$$

n သည်ကွန်ပျူတာ အရေအတွက် ဖြစ်ပါတယ်။ ဒါကြောင့် connection အားလုံး ၆ခုရှိမှာဖြစ်ပြီး ကွန်ပျူတာ တစ်လုံးစီမှာ (ဝါ) node တစ်ခုစီမှာ NIC ဥခုစီရှိမယ်လို့ အဓိပ္ပာယ်ရပါတယ်။ ကွန်ပျူတာ အရေအတွက်များလာတာနှင့်အမျှ connection အရေအတွက်များလာမှာဖြစ်ပြီး network တည်ဆောက်မှု နှင့်စီမံခန့်ခွဲမှုကိစ္စတွေမှာ များစွာအခက်အခဲရှိလာနိုင်စေသော topology မျိုးဖြစ်ပါတယ်။

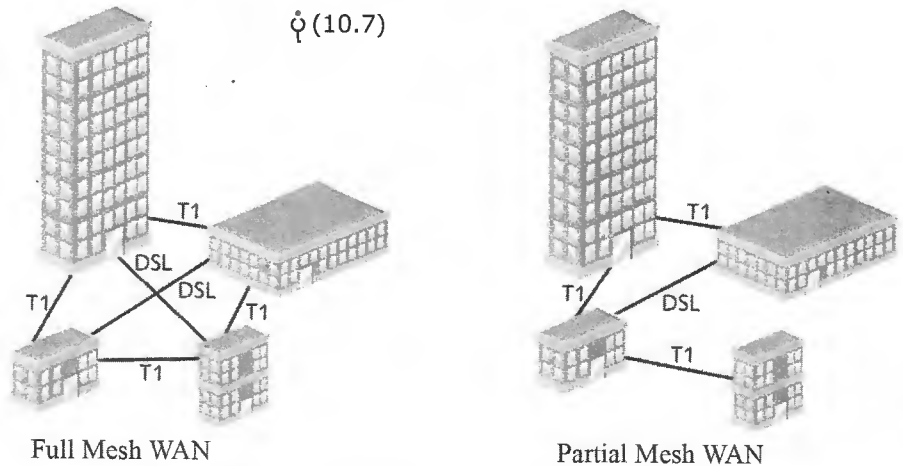
ဘာကြောင့် အသုံးပြုသလဲလို့ ဆိုရရင်တော့ သူ့ရဲ့အားသာချက်ဖြစ်တဲ့ fault-tolerance မြင့်ခြင်းကြောင့်ဖြစ်တယ်လို့ဆိုရမှာဖြစ်ပါတယ်။ point-to-point connection တစ်ခုမှာချွတ်ယွင်းချက် ရှိနေပြီဆိုရင် data သည်အခြား connection များမှဖြတ်သန်းပြီးရည်ရွယ်ရာ node ဆီသို့ရောက်အောင် ပေးပို့နိုင်ကြပါတယ်။ ဥပမာ ကွန်ပျူတာ A၊ B၊ C သုံးလုံးပါတဲ့ mesh topology network တစ်ခုကို ကြည့်ရအောင်။



ပုံ (10.6)

ကွန်ပျူတာ A မှ C သို့ message တစ်ခုပို့လိုက်တယ်ဆိုပါစို့။ အကယ်၍များ A နှင့် C ကြားမှာ ချိတ်ဆက်ထားတဲ့ connection ပြတ်တောက်သွားမယ်ဆိုရင် A မှပို့လိုက်တဲ့ message များသည် B ဘက်ကနေပတ်ပြီး C ထံသို့ ရောက်ရှိသွားမှာ ဖြစ်ပါတယ်။ အဲဒီလို အခြား network မျိုးတွေထက်ပိုပြီး အမှားခံနိုင်မှု မြင့်မားသော်လည်း အခြားတဖက်က ကြည့်မယ်ဆိုရင် cable အများကြီးသုံးရမယ်။ ကုန်ကျစရိတ် အလွန်များမယ်ပေါ့။ ဒါကြောင့် LAN တွေမှာ အသုံးပြုမှုဟာ အတော်လေးကို ရှားပါတယ်။ LAN တွေကို စုပေါင်းချိတ်ဆက်တဲ့ WAN တွေမှာသာ အသုံးပြုလေ့ရှိပါတယ်။

ပုံ (10.7)



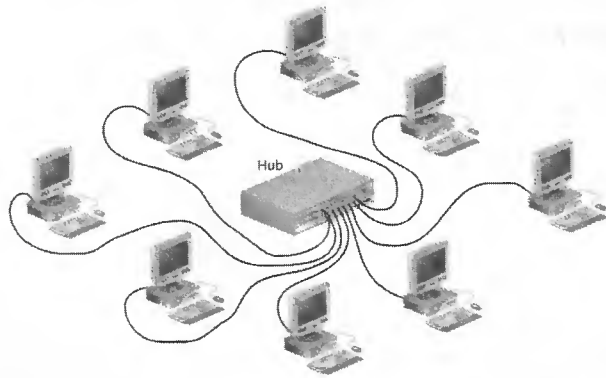
WAN ထဲမှာရှိတဲ့ site တစ်ခုကနေ အခြား site အားလုံးစီကို တိုက်ရိုက် ချိတ်ဆက်မယ်ဆိုရင် full-mesh wan လို့ခေါ်ပါတယ်။ WAN ကြီးလာတာနှင့်အမျှ ကုန်ကျစရိတ်ကလည်း ဆတိုးတက်လာမှာ ဖြစ်ပါတယ်။

ကုန်ကျစရိတ် လျော့ချရန်အတွက် မဖြစ်မနေ တကယ့်အရေးကြီးတဲ့ site တွေကိုပဲ mesh topology ကို အသုံးပြုပြီး ကျန်တာတွေကို star (သို့) bus topology တစ်ခုခုဖြင့် ချိတ်ဆက်လေ့ရှိကြပါတယ်။ အဲဒီလို network မျိုးတွေကို partial mesh topology လို့ခေါ်ပါတယ်။ ယနေ့ အချိန်မှာတော့ ကုန်ကျစရိတ် သက်သာတဲ့ partial mesh topology ကို အသုံးပြုမှုပိုများပါတယ်။

Star Topology

star topology မှာဆိုရင် device အားလုံးတို့သည် ကိုယ်ပိုင် cable တစ်ချောင်းစီဖြင့် central device လို့ခေါ်တဲ့ switch (သို့) hub ဆီသို့ ချိတ်ဆက်တပ်ဆင်ကြရပါတယ်။ အပြင်ပန်းအရ ကွန်ပျူတာတွေ နေရာချထားပုံကို ကြည့်မယ်ဆိုရင် တစ်လုံးနှင့် တစ်လုံးဘေးချင်းယှဉ်ပြီး ချထားတာမျိုး တွေနိုင်သလို အဆောက်အဦအနံ့ဟိုတစ်လုံး၊ ဒီတစ်လုံး ဖြန့်ချိတာမျိုးလည်း တွေနိုင်ပါတယ်။ မည်သို့ပင်ရှိနေပါစေ ကွန်ပျူတာ တစ်လုံးမှတစ်လုံးသို့ ပေးပို့ရယူသမျှ data အားလုံးတို့သည် ဗဟိုပြုထားသော hub (သို့) switch ကို ဖြတ်သန်း သွားရပါတယ်။ star network တွေကို တည်ဆောက်တဲ့နေရာမှာ twisted pair (သို့) fiber ကို အသုံးပြုနိုင်ပါတယ်။ fiber cable ကို အသုံးပြုတည်ဆောက်နိုင်တယ် ဆိုတာက သိထားရုံဖြစ်ပါတယ်။ star network အားလုံးနီးပါးတို့တွင် twisted pair ကို အသုံးပြုတည်ဆောက်ကြပါတယ်။ အောက်ဖော်ပြပါပုံ (10.8) သည် star topology ကို ပုံဖော်ထားခြင်း ဖြစ်ပါတယ်။

ပုံ (10.8)



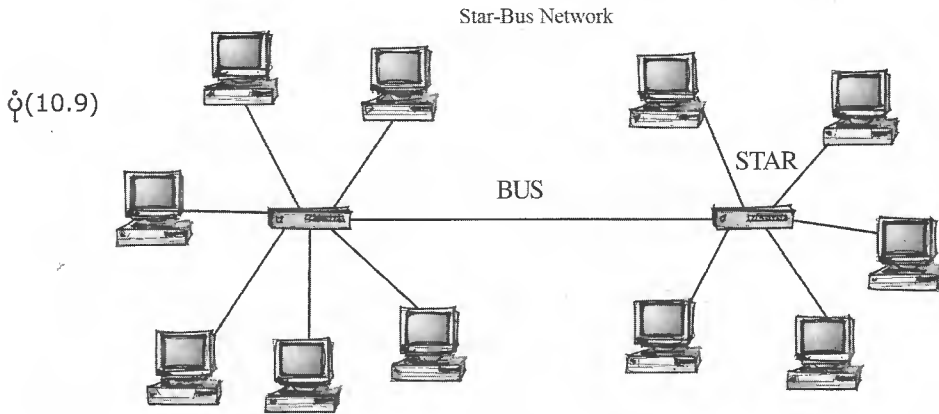
ကွန်ပျူတာတစ်လုံးအတွက် ကိုယ်ပိုင်သီးသန့် cable တစ်ချောင်းစီ အသုံးပြုခြင်းဖြစ်သည့်အတွက် ကွန်ပျူတာတစ်လုံးမှာ ချွတ်ယွင်းချက်ရှိလာပြီဆိုရင် network ပေါ်ရှိအခြားကွန်ပျူတာများအပေါ်မှာ မည်သည့် အကျိုးအပြစ်မှ သက်ရောက်မှုမရှိပါဘူး။ တနည်းဆိုရင် ချွတ်ယွင်းချက်ရှိနေသည့် အဲဒီကွန်ပျူတာကိုသာ network ပေါ်မှာ အသုံးပြု၍ မရနိုင်ပဲ ကျန်ရှိနေသော အခြားကွန်ပျူတာများကို ပုံမှန်အတိုင်း ဆက်လက်အသုံးပြု ရနိုင်ပါတယ်။

ဒါ့အပြင် အခြား user တွေ အသုံးပြုနေမှုကို အနှောက်အယှက် မဖြစ်စေပဲ network တွင်းသို့ ကွန်ပျူတာတွေ ထပ်တိုးတပ်ဆင်ခြင်း၊ မလိုအပ်ပဲ ကွန်ပျူတာတွေ ဖယ်ရှားခြင်း အစရှိသည့် စီမံခန့်ခွဲခြင်း လုပ်ငန်းများအား အလွယ်တကူ လုပ်ဆောင်နိုင်ကြပါတယ်။ trouble shooting နှင့် ပါတ်သက်ရင်လည်း

အခြားသော Ring၊ BUS network တွေနှင့်ယှဉ်ရင်ပိုမိုလွယ်ကူစေပါတယ်။ ဒါကြောင့် STAR သည်ယနေ့ လူသုံးအများဆုံး topology ဖြစ်ပါတယ်။ ဘယ်လောက်ထိများသလဲဆိုရင် ယနေ့ network လို့ ဆိုလိုက်တာနှင့် topology သည် star ပင်ဖြစ်ပါတယ်။

Hybrid Topology

သာမန်အိမ်သုံး network အသေးစားတွေကလွဲပြီး အတော်အတန်ကြီးတဲ့ network တွေမှာဆိုရင် topology တစ်မျိုးတည်းသီးသန့် သုံးပြီး တည်ဆောက်တာမျိုးက ရှားပါတယ်။ star နှင့် BUS ပေါင်းမယ်၊ star နှင့် ring ပေါင်းမယ် အစရှိသဖြင့် topology တွေကို ပေါင်းစပ် အသုံးပြုမှုက ပိုများပါတယ်။ ဥပမာ အနေနှင့် star နှင့် bus ပေါင်းတဲ့ network တစ်ခုကိုပုံ (10.9) မှာလေ့လာနိုင်ပါတယ်။



● Network Media (or) Transmission Media

network တွင်းမှာရှိတဲ့ ကွန်ယူတာတွေ တစ်လုံးနှင့် တစ်လုံး data တွေကို အပြန်အလှန် ပေးပို့ရယူကြတဲ့နေရာမှာ ကြားခံ media အမျိုးမျိုးကို အသုံးပြုကြပါတယ်။ copper ၊ glass နှင့် air တို့သည် အဓိကအသုံးအများဆုံး transmission media တွေ ဖြစ်ကြပါတယ်။ အဲဒီသုံးမျိုးထဲကမှ ဟိုးယခင်ကနေ ယနေ့တိုင်အောင် network တွေကို တည်ဆောက် အသုံးပြုတဲ့နေရာမှာ copper ဖြင့်ပြုလုပ်ထားသော cable တွေကို အသုံးပြုမှုသည် အများဆုံးဖြစ်ပါတယ်။ copper cable အမျိုးအစားတွေကတော့ coaxial cable၊ unshield twisted pair (UTP) နှင့် shield twisted pair (STP) တို့ဖြစ်ကြပါတယ်။ မြန်နှုံးမြင့် network မျိုးကို အလိုရှိတဲ့ အဖွဲ့အစည်းတွေကတော့ glass ဖြင့်ပြုလုပ်ထားသော fiber optic media ကို ရွေးချယ်အသုံးပြုကြပါတယ်။ ဒါ့အပြင် cable လုံးဝအသုံးမပြုတဲ့ wireless network တွေသည် data တွေကို လေထဲမှတစ်ဆင့်ပေးပို့ကြသည့်အတွက် လေသည်၎င်းတို့ရဲ့ transmission media ဖြစ်ပါတယ်။ အထူးသဖြင့် cable ဖြင့်သွယ်တန်း install လုပ်ဖို့ရန် မဖြစ်နိုင်တဲ့ နေရာမျိုးတွေမှာ wireless နည်းပညာကို အသုံးပြုကြလေ့ရှိပါတယ်။

network media တစ်မျိုးစီသည် network တစ်ခု၏ လုပ်ဆောင်နိုင်မှု performance ပေါ်မှာ များစွာ သက်ရောက်မှု ရှိပါတယ်။ အရေးကြီးတာကတော့ မိမိတို့ရဲ့ လိုအပ်ချက်နှင့် ကိုက်ညီတဲ့ media ကို ရွေးချယ်နိုင်ဖို့ လိုပါတယ်။ ဆိုရရင် ethernet network ရယ်လို့ စကတည်းကိုက အသုံးပြုလာခဲ့ကြသည့် ရှေးအကျဆုံး coaxial cable ဖြင့်တည်ဆောက်ထားတဲ့ network တွေသည် 10Mbps ထိသာ support လုပ်နိုင်ပါတယ်။ အဲဒီအချိန်အခါ 1980 ဝန်းကျင်တဝိုက်တုန်းက အသုံးပြုသူတို့၏ လိုအပ်ချက်နှင့်၎င်း speed (10Mbps) သည် ကောင်းစွာလုံလောက်ပါတယ်။ ဒီဘက်ခေတ် ရောက်တဲ့အခါမှာတော့ အသုံးပြုပုံတွေ ပြောင်းလာပြီး bandwidth လိုအပ်ချက်တွေ များလာတဲ့အတွက် 10Mbps သည် လုံလောက်မှု မရှိပါဘူး။ အနည်းဆုံး 100Mbps နှင့် အထက် လုပ်ဆောင်နိုင်တဲ့ network မျိုးတွေဖြစ်ဖို့ လိုအပ်လာပါတယ်။

ဒါကြောင့် 10Mbps ဖြင့်သာလုပ်ဆောင်နိုင်တဲ့ coaxial တို့ရဲ့အခန်းကဏ္ဍမှ မှုန်သွားပြီး အနည်းဆုံး 100Mbps ကို support လုပ်ပေးနိုင်တဲ့ UTP နှင့် fiber ၂မျိုးတို့ကို အစားထိုး အသုံးပြုလာကြပါတယ်။ အဲဒီ ၂မျိုးထဲကမှ ကုန်ကျစရိတ်လည်း သက်သာမယ်၊ တစ်ဆင့်အသုံးပြုရတာလည်း လွယ်ကူမယ်၊ ယနေ့အသုံးပြုမှု လိုအပ်ချက်နှင့် ကိုက်ညီသော speed ဖြင့်လိုက်ပါလုပ်ဆောင်နိုင်သော UTP (cat 5) သည် အသုံးပြုမှုသည် အများဆုံးဖြစ်ပါတယ်။ ဒါကြောင့် network media (ဝါ) transmission media တွေ အကြောင်းကို ရှင်းတဲ့နေရာမှာ UTP cable ကိုဦးတည်ပြီး သိသင့်သိထိုက်သည်များကိုဦးစားပေးရှင်းလင်းဖော်ပြသွားပါမယ်။

● Cable Standard

Cable Standard အမျိုးမျိုးရှိကြပါတယ်။ ယနေ့ network တွေကို တည်ဆောက်တဲ့နေရာမှာ အသုံးပြုတဲ့ cable standard တွေသည် ရှေ့ကအသုံးပြုခဲ့သော standard တွေကို အခြေခံပြီး ပေါ်ပေါက်လာခဲ့ခြင်းဖြစ်ပါတယ်။ ဒါကြောင့် အချို့သော cable standard တွေကို ယနေ့အချိန်မှာ အသုံးမရှိတော့ပါဘူး။

သို့သော်လည်းရှေ့ကသုံးခဲ့တဲ့ standard တွေကိုနားလည်သဘောပေါက်ထားခြင်းအားဖြင့်ယနေ့သုံးနေတဲ့ standard တွေကိုလေ့လာတဲ့နေရာမှာ များစွာ အထောက်အကူ ရစေနိုင်ပါလိမ့်မယ်။ အထူးသဖြင့် cable standard တစ်ခုအောက်မှာ အကျိုးဝင်တဲ့အသုံးပြုရမည့် cable အမျိုးအစား၊ segment တစ်ခုအဖြစ် အများဆုံးသွယ်တန်းအသုံးပြုနိုင်မည့်ကြိုးအရှည်၊ network speed ၊ cable အမျိုးအစားပေါ်မူတည်ပြီး ကွဲပြားလေ့ရှိတဲ့ topology တို့ကိုသိထားသင့်ပါတယ်။ cable အမျိုးအစားမတူတာနှင့် cable standard မတူတာတွေ ရှိသလို၊ အသုံးပြုထားသည့် cable တူသော်လည်း network speed ပေါ်မူတည်ပြီး cable standard ကွဲပြားမှုတွေရှိပါတယ်။

ဥပမာအားဖြင့် cable standard ၂ခုဖြစ်ကြတဲ့ 100BASE-T နှင့် 100BASE-F တို့ကိုယှဉ်ကြည့်ရအောင်။ "100BASE-T" မှာရှိတဲ့ 100 သည် network speed ဖြစ်သော 100Mbps ကို ရည်ညွှန်းပြီး T က cable အမျိုးအစားသည် twisted pair ဆိုတာကိုရည်ညွှန်းပါတယ်။ 100BASE-F မှာပါရှိတဲ့ နောက်က F သည် fiber cable ကိုရည်ညွှန်းပါတယ်။ ၎င်း cable standard ၂ခုတို့သည် လုပ်ဆောင်သော speed ခြင်းတူသော်လည်း cable type ပေါ်မူတည်ပြီး ကွဲပြားကြပါတယ်။

cable type တူသော်လည်း network speed မတူသည့်အတွက် cable standard ကွဲလွဲပုံကို လေ့လာကြည့်ရအောင်။ ဥပမာ 10BASE-T နှင့် 100BASE-T ဆိုပါတော့။ ၎င်း standard ၂ခုစလုံးမှာ အသုံးပြုတဲ့ cable သည် twisted pair ပင်ဖြစ်ပါတယ်။ ဒါပေမယ့် network speed သည် 10Mbps ဖြစ်ပါက 10BASE-T ဖြစ်ပြီး၊ 100Mbps ဖြစ်ပါက 100BASE-T ဖြစ်ပါလိမ့်မယ်။

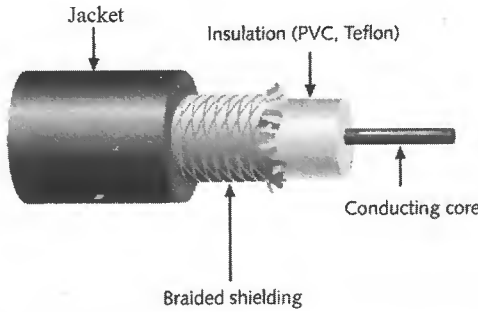
network တစ်ခုကိုစတင်တည်ဆောက်တဲ့အခါမှာပဲဖြစ်ဖြစ် ရှိပြီးသား network ထဲမှာ device (switch၊ hub) တွေထပ်တိုးတပ်ဆင်လိုတဲ့ အခါမျိုးမှာပဲဖြစ်ဖြစ် cable standard သည်လွန်စွာအရေး ပါပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ ယနေ့အခါ device တစ်ခုရဲ့ specification ကိုဖော်ပြတဲ့နေရာတွင် 100BASE-T၊ 1000BASE-T အစရှိသဖြင့် cable standard ဖြင့်ဦးစားပေး ဖော်ပြလေ့ရှိပါတယ်။ ဒါကြောင့် device တစ်ခုကိုဝယ်ယူတော့မယ်ဆိုရင် cable standard ကိုကြည့်တာနှင့် ဘယ်လောက် speed ဖြင့်လုပ်နိုင်သလဲ၊ ဘယ် cable အမျိုးအစားကိုသုံးရမှာလဲ၊ ဘယ် topology မှာသုံးရမှာလဲဆိုတာကို နားလည် သဘောပေါက်ထားနိုင်မှသာလျှင် မိမိ လိုအပ်ချက်နှင့် ကိုက်ညီတဲ့ device ကို ရွေးချယ် နိုင်ကြမှာ ဖြစ်ပါတယ်။

Coaxial Cable (Coax)

coax လို့ခေါ်တဲ့ coaxial cable ကို 1970 ခုနှစ်မှစပြီး နှစ်ပေါင်းအတော်ကြာသည်အထိ net-work တွေရဲ့အဓိက transmission media အဖြစ် ကျယ်ကျယ်ပြန့်ပြန့် အသုံးပြုခဲ့ကြပါတယ်။ ယနေ့ထိ တိုင်အောင်လည်း အချို့သော network တွေမှာ ဆက်လက် အသုံးပြုနေကြဆဲ ဖြစ်ပါတယ်။ သို့သော် ယနေ့ တည်ဆောက်တဲ့ network တွေမှာတော့ twisted pair နှင့် fiber cable တို့သည် coax တို့နေရာတွင် အစားထိုး နေရာယူသွားကြပြီဖြစ်ပါတယ်။

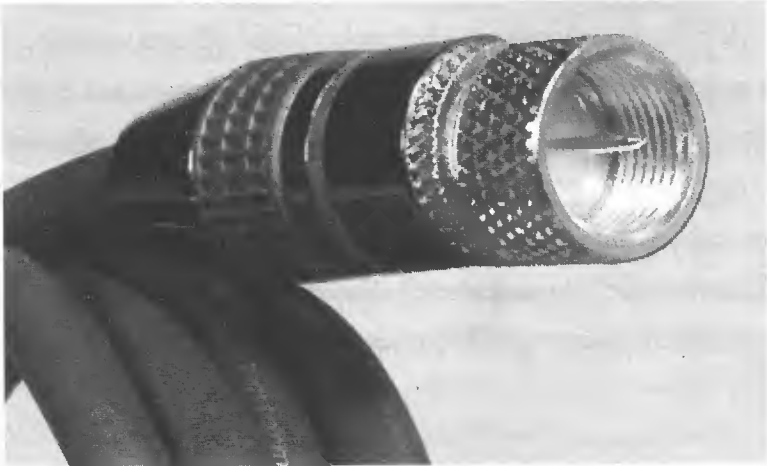
coaxial cable အလယ်အူတိုင်တွင် copper core တစ်ချောင်းပါရှိပြီး ၎င်းကို insulation၊ metal shield၊ jacket တို့ဖြင့် အထပ်ထပ် ဖုံးအုပ်ထားပါတယ်။ copper core သည် signal များကို သယ်ဆောင်ရန်ဖြစ်ပြီး shield ကတော့ပြင်ပမှ EMI သက်ရောက်ခြင်းများမှကာကွယ်ရန်နှင့် signal အတွက် ground ဖြစ်ပါတယ်။

ပုံ (11.1)



insulation ကတော့အများအားဖြင့် PVC (poly Vinyl Chloride) လို့ခေါ်တဲ့ပလတ်စတစ် တမျိုးဖြစ်ပါတယ်။ ၎င်းသည် copper core နှင့် shield တို့ထိတက်မှုမရှိအောင်ကြားခံဖြစ်ပါတယ်။ အကယ်၍ core နှင့် shield တို့ တနေရာရာမှာထိတာနှင့် short circuit ဖြစ်ပြီး အသုံးပြု၍ မရနိုင်ပါ။ အပေါ်ဆုံးလွှာ jacket သည်ပြင်ပယောဂကြောင့်အလွယ်တကူထိခိုက်ပျက်စီးခြင်းမျိုး မဖြစ်အောင်ကာကွယ်ပေးပါတယ်။ PVC သို့မဟုတ် ဈေးပိုကြီးတဲ့ မီးခံပလတ်စတစ်တမျိုးလည်း ဖြစ်နိုင်ပါတယ်။

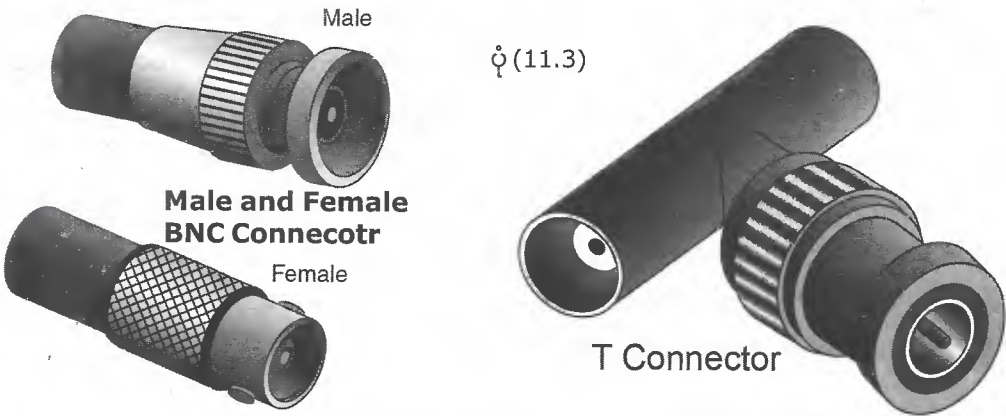
ပုံ (11.2)



shield ပါရှိသည့်အတွက် coaxial cable တွေသည်ပြင်ပပတ်ဝန်းကျင် noise တို့၏အနှောက် အယှက်မှပိုမိုခံနိုင်ရည်ရှိပါတယ်။ သည့်အတွက်ကြောင့် segment တစ်ခုခုအရှည်ကို 100m ထိသာအသုံး ပြုနိုင်တဲ့ twisted pair တွေထက်ပိုသောအကွာအဝေးထိအသုံးပြုနိုင်ပါတယ်။ အခြားတဖက်ကကြည့်မယ် ဆိုရင် coax သည် twisted pair တွေထက်ဈေးပိုကြီးပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ coax ထုတ်လုပ်ရန် အတွက် ကုန်ကြမ်းပိုမို အသုံးပြုရခြင်းသည် အဓိကအကြောင်းအရင်း ဖြစ်ပါတယ်။

specification ပေါ်မူတည်ပြီး coaxial cable အမျိုးအစားပေါင်းရာနှင့်ချီ ပြီးရှိပါတယ်။ (အိမ်တွေမှာ TV နှင့် အင်တီနာ ချိတ်ဆက်တဲ့နေရာမှာ သုံးတဲ့ ကြိုးသည်လည်း coax အမျိုးအစားပေါင်း များစွာထဲကတစ်မျိုးဖြစ်ပါတယ်။) အဲဒီများစွာထဲက ၂မျိုးလောက်သာ network cable အဖြစ်အသုံးပြုကြ ပါတယ်။ အမျိုးအစားတစ်ခုကို RG number တစ်ခုဖြင့် သတ်မှတ် ခေါ်ဆိုကြပါတယ် (ဥပမာ - RG 8၊ RG 58)။ RG ဆိုတာကတော့ radio guide ကိုရည်ညွှန်းပါတယ်။

Coaxial Cable Connector



Cable Standard (Coaxial Cable)

cable standard သည် အသုံးပြုမည့် cable အမျိုးအစား၊ segment တစ်ခုအဖြစ် ထားရှိ အသုံးပြုနိုင်မည့် ကြိုးအရှည် အစရှိသော အချက်တွေပေါ်တွင် မူတည်ပြီး ကွဲပြားကြတယ်ဆိုတာကို ရှေ့စာမျက်နှာမှာဖော်ပြခဲ့ပြီး ဖြစ်ပါတယ်။ coaxial cable ကို bus topology ဖြင့်တည်ဆောက်တဲ့ network တွေမှာအသုံးပြုကြပါတယ်။

coaxial cable အမျိုးအစားပေါင်းများစွာရှိသည့်အနက်က network media အဖြစ်အသုံးပြု၍ ရနိုင်တဲ့ coax က ၂မျိုးသာရှိပါတယ်။ ပထမတစ်မျိုးက ethernet network ရယ်လို့ ကနဦးမူလအစက တည်းကိုက အသုံးပြုလာခဲ့ကြတဲ့ RG-8 coaxial ဖြစ်ပါတယ်။ ၎င်း cable သည် လုံးပတ်အချင်း 1cm ခန့်ရှိပါတယ်။ ဒုတိယတစ်မျိုးက RG-58 cable ဖြစ်ပြီး လုံးပတ်မှာ 0.64cm ခန့်ရှိပါတယ်။ ထို coax ၂မျိုး တို့ပေါ်မူတည်၍ 10BASE-5 နှင့် 10BASE-2 ဆိုပြီး cable standard နှစ်မျိုးရှိပါတယ်။

Coaxial Cable Specifications

Table with 4 columns: RG Rating, Popular Name, Ethernet Implementation, Type of Cable. Rows include RG-58 A/U (Thinnet, 10Base2, Stranded copper) and RG-8 (Thicknet, 10Base5, Solid copper).

● 10BASE-5 (Thicknet)

10BASE-5 ကို thicknet လို့လည်းခေါ်ကြပါတယ်။ ထို့အတူ RG-8 ကို thicknet cable ရယ်လို့ ခေါ်ဆိုလေ့ရှိပါတယ်။ 10BASE-5 တွင် ပါရှိသည့် ရှေ့က 10 သည် 10Mbps၊ BASE သည် baseband transmission နှင့် 5 သည် cable segment တစ်ခုအဖြစ်ထားရှိ အသုံးပြုနိုင်မည့် ကြိုးအရှည် 500m ကိုရည်ညွှန်းပါတယ်။ ယနေ့အချိန်မှာတော့အသုံးပြုမှုမရှိတော့သော cable standard တစ်ခုဖြစ်ပါတယ်။

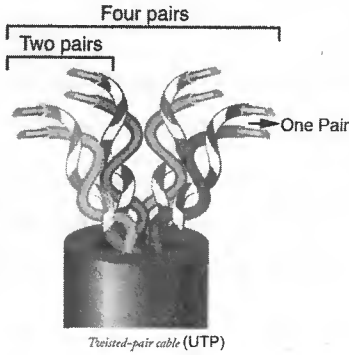
● 10BASE-2 (Thinnet)

10BASE-2 ကို thinnet လို့လည်းလူသိများပါတယ်။ အသုံးပြုရတဲ့ cable ကတော့ RG-58 cable ဖြစ်ပါတယ်။ thinnet cable လို့လည်း ခေါ်ကြပါတယ်။ 10BASE-2 မှာပါရှိတဲ့ ရှေ့က 10 သည် 10Mbps၊ BASE သည် baseband transmission နှင့် 2 သည် အမြင့်ဆုံး သွယ်တန်းနိုင်သည့် ကြိုးအရှည် 185m (အကြမ်းအားဖြင့် 200m) ကို ရည်ညွှန်းပါတယ်။ အကွားအဝေးအားဖြင့် မီတာ 500 မီတာ အထိ သွယ်တန်းနိုင်သည့် thicknet cable ကို မမီပါဘူး။ သို့သော်လည်း ကြိုးလုံးသေးသည့် အတွက် ပိုမိုပျော့ပြောင်းပြီး install လုပ်ရာမှာ လွယ်ကူစေပါတယ်။ ဈေးနှုန်းမှာလည်း သက်သာပါတယ်။ ဒါကြောင့် thicknet ထက်ပိုမိုလူကြိုက်များပြီး 1980 တစ်ဝက်က ethernet network တွေမှာတွင်တွင်ကျယ်ကျယ် အသုံးပြုခဲ့သော cable standard တစ်ခုလည်း ဖြစ်ပါတယ်။

● Twisted Pair Cable

twisted pair cable တစ်ချောင်းရဲ့အပေါ်ခွံကို ကြည့်လိုက်မယ်ဆိုရင် အတွင်းမှာ ဝါယာတွေကို အရောင်များအလိုက် တစ်ချောင်းနှင့် တစ်ချောင်း လိမ်ပတ်ထားတာကို တွေ့ရပါလိမ့်မယ်။ အဲဒီလိမ်ပတ်တဲ့ ချောင်းတစ်စုံစီသည် one pair ဖြစ်ပါတယ်။ ထိုကဲ့သို့ ဝါယာတွေကို အစုလိုက် လိမ်ပတ်ထားသည့် အတွက် twisted pair လို့ခေါ်ခြင်းဖြစ်ပါတယ်။

ပုံ (11.4)



Twisted-pair cable (UTP)

twisted pair cable တစ်ချောင်းတွင် 1 pair မှ 4200 pair ထိ ပါလေ့ရှိပါတယ်။ ဒါပေမယ့် ကွန်ပျူတာ network တွေအတွက်တော့ 4 pair သာပါရှိသော twisted pair cable ကို standard အဖြစ် အသုံးပြုကြပါတယ်။

UTP (Unshield Twisted pair) နှင့် STP (Shield Twisted Pair) ဆိုပြီး network ချိတ်ဆက် ရာတွင်အသုံးပြုသည့် cable ၂မျိုးရှိပါတယ်။ UTP သည်ယနေ့အသုံးပြုမှုအများဆုံး network cable ဖြစ်ပြီး STP ကတော့အသုံးမရှိသလောက်နည်းပါးလာနေပြီဖြစ်ပါတယ်။

UTP (unshield twisted pair)

UTP ကတော့တယ်လီဖုန်းနှင့်ကွန်ပျူတာ network တွေမှာအဓိက အသုံးပြုကြသည့်အတွက် လူအများစုတို့နှင့်ရင်းနှီးပြီးသား cable အမျိုးအစားပင်ဖြစ်ပါတယ်။ လွန်ခဲ့တဲ့နှစ်ပေါင်းများစွာကတည်းက telephone system တွေမှာအသုံးပြုလာခဲ့ပြီး LAN များမှာတော့ 1980 ပြည့်နှစ်နှောင်းပိုင်းမှစတင် အသုံးပြုလာခဲ့ခြင်းဖြစ်ပါတယ်။ အခြား cable တွေနှင့်ယှဉ်လျှင်ဈေးနှုန်းသက်သာခြင်းသာမကပေါ့ပါးခြင်း၊ ပျော့ပျောင်းခြင်း၊ တပ်ဆင်အသုံးပြုရလွယ်ကူခြင်းစသည့်အားသာချက်များကြောင့်ယနေ့ networkအများ စုတို့မှာ UTP တွေကိုပဲ network cable အဖြစ်အဓိကထားအသုံးပြုလျက်ရှိနေပါတယ်။

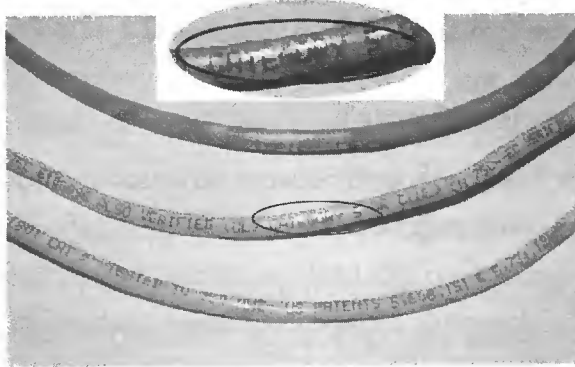
UTP အမျိုးအစားများစွာရှိပါတယ်။ ဆိုရရင် "no of pair" ၊ "no of twist" ၊ "wire thick- ness" တို့ပေါ်မူတည်ပြီး category 1 (Cat1)၊ Cat 2၊ Cat 3 . . . Cat 5 အစရှိသဖြင့်အမျိုးအစား တွေကွဲပြားကြပါတယ်။ အဲဒီများစွာအထဲကမှ network cable လို့ဆိုလိုက်တာနှင့် အသုံးပြုသူတို့၏ မျက်စိထဲမှာမြင်ယောင်လာစေမည့် cable ကတော့ Cat 5 ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါဇယားမှာဆိုရင် UTP cable အမျိုးမျိုးတို့ရဲ့ specification များကိုဖော်ပြထားပါတယ်။

Twisted-pair cable categories		
Category	Maximum data rate	Intended use
1	1 Mbps	Voice only
2	4 Mbps	4Mbps Token Ring
3	16 Mbps	10BaseT Ethernet
4	20 Mbps	16Mbps Token Ring
5	100 Mbps (2-pair)	100BaseT Ethernet
	1000 Mbps (4-pair)	1000BaseTX
5e	1000 Mbps (2-pair)	1000BaseT
6	1000 Mbps (2-pair)	1000BaseT and faster broadband applications

CAT5 Specification

Cat 3၊ Cat 5 နှင့် Cat 5e တို့တွင်ပါသော twisted pair အရေအတွက်တို့သည် အတူတူပင် ဖြစ်သည့်အတွက် ဘယ်ဟာက Cat5 ဖြစ်သလဲဆိုတာကို ခွဲခြားဖို့ရန် အနည်းငယ်ခက်ခဲနိုင်ပါတယ်။ သို့သော်လည်း မျက်စိဖြင့် ကြည့်ရုံဖြင့် မြင်နိုင်တဲ့ အချို့အချက်အလက်များပေါ် အခြေခံပြီး အလွယ်တကူ ခွဲခြားနိုင်ပါတယ်။

ဆိုရရင် Cat 5 cable ၏အပေါ်ခွဲမှာထုတ်လုပ်ရောင်းချသောကုမ္ပဏီအမည်နှင့် specification တို့ကို ရိုက်နှိပ်ထားလေ့ရှိပါတယ်။



ပုံ (11.5)

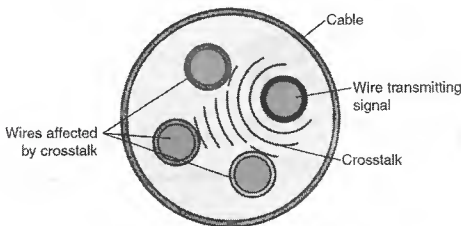
■ Number of pairs

Cat 5 တွင် 4 pairs (8 wires) ပါရှိပါတယ်။

■ Number of Twisted

cable အမျိုးအစား (category) ပေါ်မူတည်ပြီး တစ်လက်မအတွင်းမှာ twisted ဘယ်နှစ်ခါ လုပ်ထားသလဲဆိုတဲ့ အကြိမ်အရေအတွက်သည်လည်း ကွဲပြားမှု ရှိပါတယ်။ ဝါယာတွေကို တစ်ချောင်းနှင့် တစ်ချောင်းလိမ်ထားရတဲ့အကြောင်းရင်းကတော့ crosstalk ဖြစ်ခြင်းမှကာကွယ်ရန်ဖြစ်ပါတယ်။

ပုံ (11.6)



Crosstalk between wires in a cable

crosstalk ဆိုတာက ဝါယာတစ်ချောင်းမှာ ဖြတ်စီးနေသော signal တွေသည် ဘေးချင်း ကပ်လျက်ဝါယာများ ပေါ်သို့ ကူးပြောင်းပြီး ၎င်းဝါယာ များတွင်ဖြတ်စီးနေသော signal များကို အနှောက် အယှက် ပြုခြင်းဖြစ်စဉ်ပင် ဖြစ်ပါတယ် ပုံ (11.6)။ crosstalk ဖြစ်စဉ်ကို တယ်လီဖုန်းစနစ်မှာတော့ အလွယ်တကူ သိရှိနိုင်ကြပါတယ်။ ဖုန်းဖြင့်စကား ပြောတဲ့အခါ မပီမသကြားရခြင်းနှင့် အခြားလိုင်းမှ

စကား သံများ ကိုကြားရခြင်းတို့ဖြစ်ပါတယ်။ ကွန်ပျူတာက network တွေမှာတော့ crosstalkကြောင့် bit error ဖြစ်ပြီး data ပေးပို့ရယူခြင်းများကို နှောင့်နှေး ကြန့်ကြာစေပါတယ်။ Twisted အရေအတွက်များလာလေ crosstalk ဖြစ်ဖို့ အခွင့်အလမ်းနည်းလေဖြစ်ပါလိမ့်မယ်။ သို့သော်လည်း twist အရေအတွက် များတာနှင့်အမျှ ပိုကောင်းတယ်ရယ်လို့ မဟုတ်ပါဘူး။ လိမ်ထားတဲ့အရေ အတွက်များတာနှင့်အမျှ ဝါယာပိုသုံးရပြီး attenuation (loss of signal) လည်းများလာမှာ ဖြစ်ပါတယ်။

ဒါကြောင့် cable ထုတ်လုပ်ရောင်းချသူများအနေနှင့် cable တွေကို ထုတ်လုပ်တဲ့နေရာမှာ crosstalk လည်းမဖြစ်အောင်၊ attenuation ကျခြင်းကိုလည်း အနည်းဆုံးဖြစ်အောင် ချိန်ညှိပြီး ထုတ်လုပ်ကြရပါတယ်။ Cat 5 နှင့် အထက် cable တွေမှာဆိုရင် အများအားဖြင့် twisted အရေအတွက်သည် တစ်ပေအတွင်းမှာ 12 ကြိမ်ထက်ပိုတတ်ပါတယ်။

■ Wire Gauge

copper wire တွေရဲ့အချင်းကို AWG (American Wire Gauge) ယူနှစ်ဖြင့်တိုင်းတာပါတယ်။ AWG နံပါတ်ကြီးလေ copper ဝါယာ၏ လုံးပတ်အရွယ်ငယ်လေဖြစ်ပါတယ်။ ဆိုရရင် AWG 22 သည် AWG 24 ထက်လုံးပတ်ပိုကြီးပါတယ်။ ဝါယာလုံးပတ်ပိုကြီးတာနှင့်အမျှ ပိုမိုတောင့်ခိုင်မာပြီး resistance ကိုလည်း လျော့နည်းစေပါတယ်။ ဒါပေမယ့် လုံးပတ်ပိုကြီးမယ်ဆိုရင် cable တွေကို ထုတ်လုပ်တဲ့နေရာမှာ copper ပိုသုံးရတဲ့အတွက် ဈေးကြီးမယ်။ အလေးချိန်ပိုလာတဲ့အတွက် install လုပ်ရတဲ့နေရာမှာ ပိုမိုခက်ခဲလာစေမယ်အစရှိတဲ့အားနည်းချက်တွေကိုလည်း ကြုံတွေ့ရမှာဖြစ်ပါတယ်။ ယနေ့ဈေးကွက်တွင်းမှာ ဝယ်ယူရရှိနိုင်တဲ့ Cat 5 cable များသည် 24 AWG (သို့) 22 AWG ဖြစ်ပါတယ်။

📦 Network Cable (Step-by-Step Guide)

ယခုဆက်လက်ပြီး Cat 5 ဖြင့်အသုံးပြုရနိုင်သော network cable တစ်ချောင်းဖြင့်ပြုလုပ်ရန် သိသင့်သိထိုက်သော အခြေခံ အချက်အလက်များနှင့် လုပ်ဆောင်ပုံ အဆင့်ဆင့်တို့ကို အောက်ဖော်ပြပါ ခေါင်းစဉ်များဖြင့် ရှင်းလင်းတင်ပြသွားပါမယ်။

- cable length
- connector
- color code
- straight through cable
- crossover cable
- How to make a network Cable

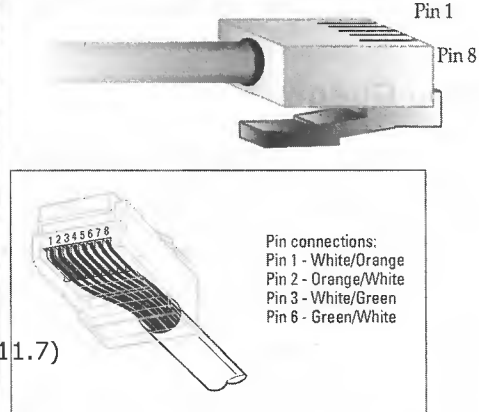
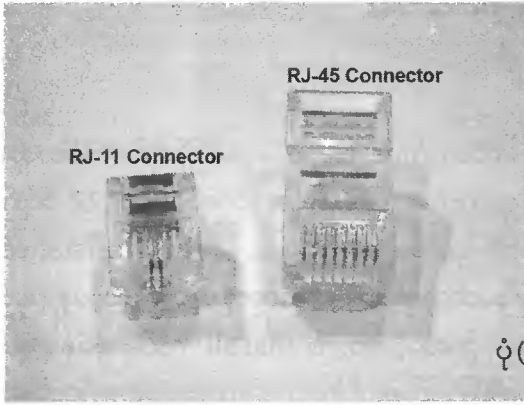
🕒 Cable Length

Cat 5 ကိုအများဆုံးထားရှိအသုံးပြုနိုင်မည့်ကြိုးအရှည်က 100m (328 ft) ဖြစ်ပါတယ်။

🕒 Connector

Rj-45 သည်ယနေ့အသုံးအများဆုံး network cable connector ပင်ဖြစ်ပြီး NIC၊ switch၊ hub တို့ကိုချိတ်ဆက်ရန်အတွက် UTP (Cat 3၊ Cat 5၊ Cat 5e) နှင့် STP cable ၂မျိုးစလုံးမှာအသုံးပြုကြပါတယ်။ RJ ဆိုတာက "registrated jack" ကိုဆိုလိုခြင်းဖြစ်ပြီး RJ-45 နှင့် RJ-11 ဟူ၍ connector နှစ်မျိုးရှိပါတယ်။ RJ-11 ကိုတယ်လီဖုန်းနှင့် modem တွေမှာအသုံးပြုပါတယ်။

ပုံသဏ္ဍာန်ဆင်တူသော်လည်း 4pair (8wire) ထည့်သွင်းတပ်ဆင်နိုင်သည့် RJ-45 သည် 2 pair (4wire) သာထည့်သွင်းတပ်ဆင်နိုင်သည့် RJ-11 ထက်အရွယ်အစားပိုကြီးပါတယ်။ အောက်ဖော်ပြပါပုံမှာဆိုရင် RJ-11 နှင့် RJ-45 connector တို့ကိုယှဉ်တွဲဖော်ပြထားပါတယ်။ ပုံ (11.7)



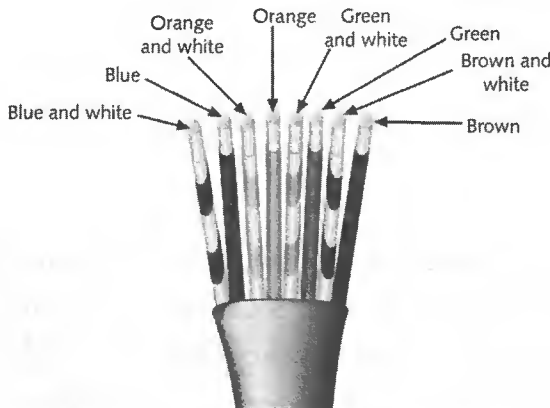
ပုံ(11.7)

● Color Code

Cat 5 မှာဝါယာချောင်းပါပါတယ်။ pair အနေနှင့်ပြောရရင် 4 pair ဖြစ်ပါတယ်။ pair တစ်ခုစီမှာ ပါတဲ့ ဝါယာ ၂ချောင်းတွင် တစ်ချောင်းက အရောင်ပြည့်ဖြစ်ပြီး နောက်တစ်ချောင်းက အဖြူနှင့် စင်းကြားဖြစ်ပါတယ်။ ဆိုရရင် တစ်ကြိုးက အစိမ်းဆိုရင် ၎င်းကြိုးနှင့် လိမ်ထားသော ကြိုးသည် ဖြူစိမ်းကျား ဖြစ်ပါလိမ့်မည်။ အရောင်တွေပေါ်မူတည်ပြီး pair အမှတ်စဉ်သတ်မှတ်ချက်တွေရှိပါတယ်။ ပုံ (11.8)

Color Codes for Four-Pair UTP Cable

Pair Number	Tip Color	Ring Color
Pair 1	White/Blue	Blue
Pair 2	White/Orange	Orange
Pair 3	White/Green	Green
Pair 4	White/Brown	Brown



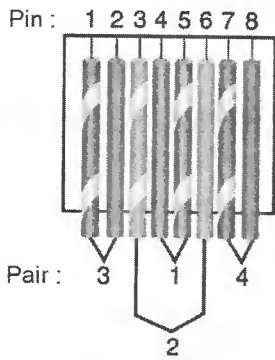
ပုံ(11.8)

A CAT 5 UTP cable with pairs untwisted

ဒီ cable တို့ရဲ့အရောင်တွေသည် အလွန်အရေးကြီးပါတယ်။ ကြိုးအရောင်များအလိုက် RJ-45 connector ထဲမှာထည့်သွင်းနေရာချမှပေါ်မူတည်ပြီး cable type များလည်းကွဲပြားကြပါတယ်။ straight through နှင့် crossover ဟူ၍ cable type ၂မျိုးရှိပါတယ်။ ၎င်း ၂မျိုးစလုံးသည် အသုံးပြုသည့် cable (Cat 5) ကော၊ connector (RJ-45) ပါအတူတူပင်ဖြစ်ကြပါတယ်။

● Straight-through Cable

straight-through မှာလည်း T-568A (type A) နှင့် T-568B(typeB) ဆိုပြီး ၂မျိုးရှိပြန်ပါတယ်။ ၎င်းတို့ ၂ခုရဲ့ကွားခြားချက်က pin assigment ပဲဖြစ်ပါတယ်။ ဆိုရင် type A မှာအစိမ်း (pair 3)သည် RJ-45 ၏ pin 1 နှင့် 2 မှာ နေရာယူပြီး လိမ္မော် (pair 2) သည် pin3 နှင့် pin6 တို့မှာဖြစ်ပါတယ်။ ပုံ (11.9)

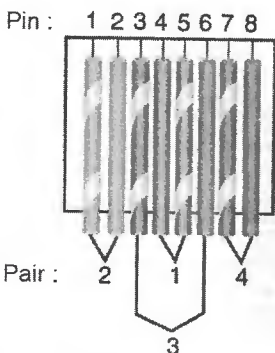


Pin #	Color	Pair #	Function
1	White with green stripe	3	Transmit +
2	Green	3	Transmit -
3	White with orange stripe	2	Receive +
4	Blue	1	Unused
5	White with blue stripe	1	Unused
6	Orange	2	Receive -
7	White with brown stripe	4	Unused
8	Brown	4	Unused

TIA/EIA 568A standard terminations

View of RJ-45 Plug from above ပုံ (11.9)

type B မှာဆိုရင်လိမ္မော် (pair 2) သည် RJ-45 ၏ pin1 နှင့် 2 မှာဖြစ်ပြီးအစိမ်း (pair 3) သည် pin3 နှင့် 6 တို့မှာအသီးသီးရှိကြပါတယ် ။ပုံ (11.10)။ တူညီတဲ့အချက်က ၎င်း type A/B ၂ခုစလုံးသည် အပြာ (pair 1 - pin4&5) နှင့်ညို (pair 4 - pin7&8) 1 တို့ကိုအသုံးမပြုကြပါဘူး။



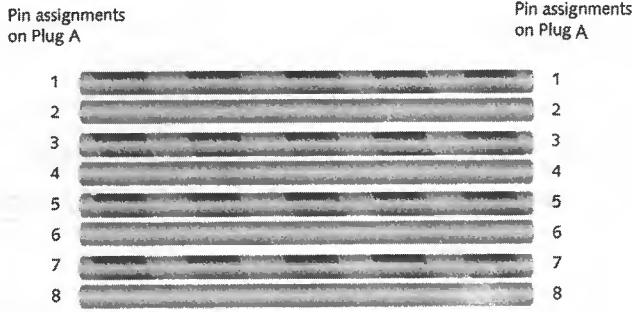
Pin #	Color	Pair #	Function
1	White with orange stripe	2	Transmit +
2	Orange	2	Transmit -
3	White with green stripe	3	Receive +
4	Blue	1	Unused
5	White with blue stripe	1	Unused
6	Green	3	Receive -
7	White with brown stripe	4	Unused
8	Brown	4	Unused

TIA/EIA 568B standard terminations

View of RJ-45 Plug from above ပုံ (11.10)

straight through ဖြစ်ဖို့ရန် အရေးအကြီးဆုံးက ခေါင်းနှစ်ဘက်စလုံးသည် pin assignment အတူတူပင်ဖြစ်ရပါမယ်။ ဆိုရရင် တဖက်က type A ဆိုရင် နောက်တဖက်ကလည်း type A ပင်ဖြစ်ရပါမယ်။ အလားတူပင် တဖက်က type B ဆိုရင် နောက်တဖက်ကလည်း type B ပင်ဖြစ်ရပါမယ်။ ပုံ (11.11)

ပုံ (11.11)



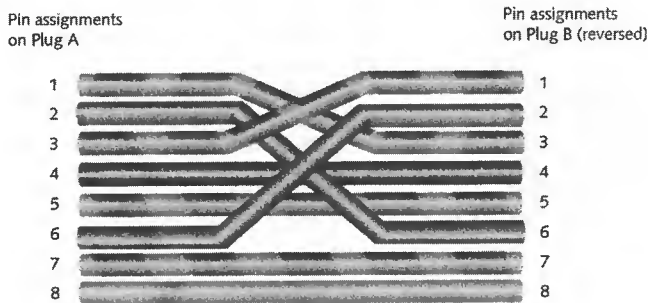
RJ-45 terminations on a straight cable

straight through ကို patch cable လို့လည်းခေါ်ကြပါတယ်။ အဓိကအားဖြင့် ကွန်ပျူတာမှ hub (သို့) switch တို့နှင့်ချိတ်ဆက်တဲ့နေရာမှာ သုံးပါတယ်။

● Cross Cable

cross cable ဖြစ်ဖို့ရန် အတွက် တဖက်က type A ဆိုရင် ကျန်တစ်ဖက်က type B ဖြစ်ရပါမယ်။ ဒါကြောင့် network cable တစ်ချောင်းကို straight လား၊ cross လား ခွဲခြားချင်ရင် RJ-45 ခေါင်း ၂ခုကို ယှဉ်ကြည့်လိုက်ရုံဖြစ်ပါတယ်။ ယှဉ်ကြည့်လို့လုံးဝတူညီတယ်ဆိုရင် straight ဖြစ်ပြီး မတူပါက crossover ဖြစ်ပါတယ်။ ပုံ (11.12)။ crossover cable ကို အဓိကအားဖြင့် hub အချင်းချင်း၊ switch အချင်းချင်း cascade ချိတ်ဆက်တဲ့နေရာမှာ အသုံးများပါတယ်။ ဒါ့အပြင် hub တွေ၊ switch တွေ မသုံးပဲ ကွန်ပျူတာ ၂လုံးကို တိုက်ရိုက်ချိတ်ဆက်တဲ့နေရာတွေမှာလည်း crossover ကို အသုံးပြုကြပါတယ်။

ပုံ (11.12)



RJ-45 terminations on a crossover cable

How to Make Network Cable

step1) Cable Cutter

အသုံးပြု၍ ရနိုင်သော network cable တစ်ချောင်း ပြုလုပ်ရန်အတွက် ပထမဦးဆုံး အနေနှင့် မိမိအလိုရှိသလောက်ကြိုးအရှည်ရအောင် တိုင်းဖြတ်ရပါမယ်။ တကယ်လိုအပ်တဲ့အတိုင်းအတာထက် အနည်းငယ်ပိုထားပါကပိုကောင်းပါတယ်။ ပုံ (11.13)

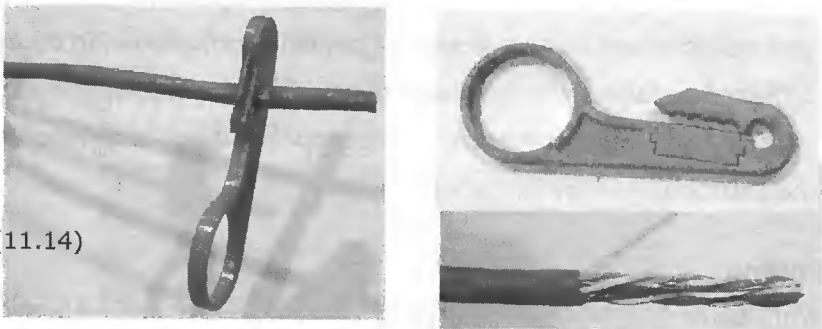
ပုံ (11.13)



step2) Stripper

Cat 5 cable တဖက်စွန်းကနေ ၂လက်မအရှည်လောက်မှန်းပြီး အပေါ်ခွံကို နှာပြစ်ရပါမယ်။ အဲဒီလို နှာရန်အတွက် stripper tool ကို အသုံးပြုပြီး လုပ်ဆောင်ခြင်းသည် အကောင်းဆုံးဖြစ်ပါတယ်။ stripper မရှိရင် တော့ခဲတံချွန်ခါး (သို့) ခါးခပ်ပါးပါး တစ်ချောင်းဖြင့်လည်း လုပ်ဆောင်နိုင်ပါတယ်။ အထူးသတိထားဖို့လိုပါတယ်။ လက်ဆမမှန်ပါက အပေါ်ခွံ jacket အောက်မှာရှိသော ဝါယာများ (twisted pair) ပေါ်မှာ ပြတ်ရှုရာများ ဖြစ်ပေါ်စေတတ်ပါတယ်။ မည်သို့ပင်ဖြစ်စေ stripper ပဲသုံးသုံး၊ ခါးပါးပဲသုံးသုံး ဝါယာ twisted pair တွေမှာ ထိခိုက် ပျက်စီးမှု ရှိမရှိဆိုတာကို သေသေချာချာ စစ်ဆေးရပါမယ်။ အကယ်၍များ ဝါယာတစ်ချောင်းချောင်းမှာ အထိခိုက်ရှိလာပြီဆိုရင် နှမြောမနေပါနှင့် နှာထားတဲ့အရင်းနေရာက ဖြတ်ထုတ်ပြီး အစအဆုံးပြန်လည်လုပ်ဆောင်ပါ။ ပုံ (11.14)

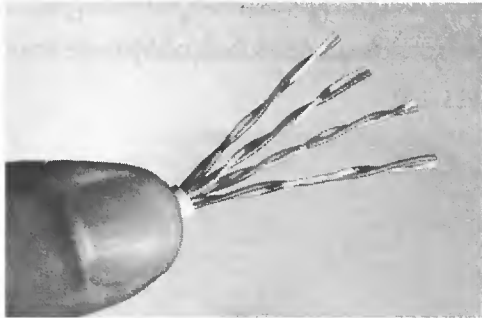
ပုံ (11.14)



step3) Spread the Wire

နှာထားတဲ့အရင်းနေရာမှာ သေသေချာချာဖိကိုင်ပြီး twisted pair လေးခုကို သီးခြားစီဖြစ်အောင် ခွဲထုတ်ရပါမယ်။ ပြီးရင် ဝါယာတွေကို မိမိအလိုရှိသော standard (Type A (သို့) Type B) အတိုင်း ဖြစ်အောင် တစ်ချောင်းချင်းစီ ဖြေပြီး နေရာချစီတန်းရပါမယ်။ ပုံ (11.15)

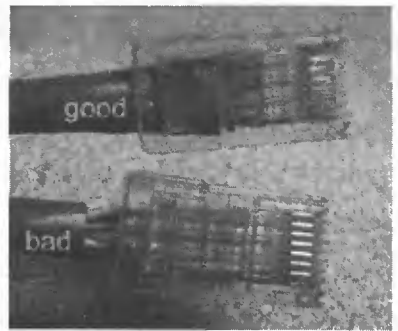
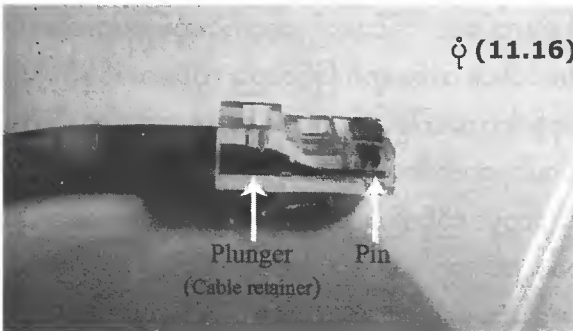
သင့်လျော်သော color code အတိုင်းစီပြီးပြီဆိုရင် connector ထဲထည့်သွင်းဖို့ရန် အတွက်လိုအပ်တဲ့ အရည် (1/2 လက်မခန့်) သာထားရှိပြီးကျန်တဲ့အဖျားပိုင်းကို cutter ဖြင့်ဖြတ်ပစ်ရပါမယ်။



ပုံ (11.15)

step4) Insert the conductors in the connector

ဒီအဆင့်မှာဆိုရင် cable ကို Rj-45 connector ထဲသို့လျှောသွင်းရပါမယ်။ ဝါယာတွေသည် အစဉ်အတိုင်း စီတန်းပြီး နေရာတကျ ဝင်သွားဖို့လိုပါတယ်။ အဲဒီလို ထည့်သွင်းခဲ့ပြီးပြီဆိုရင် connector ရှိ plunger နှင့် pinတို့ ှနေရာကိုပြန်လည်စစ်ဆေးဖို့လိုပါမယ်။ အောက်ပုံ(11.16)တွင်ကြည့်ပါ။



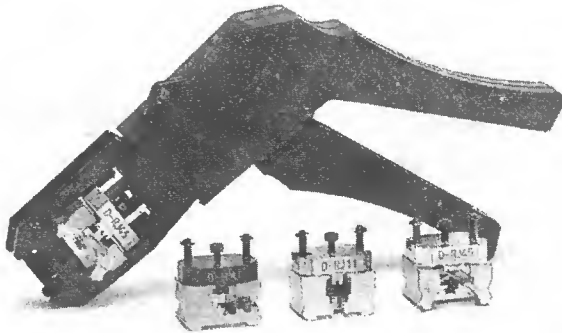
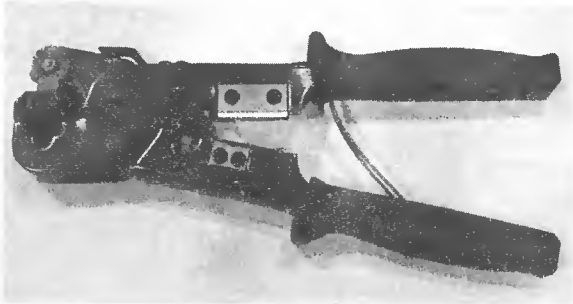
plunger နေရာထိကို cat 5 cable ၏အပေါ်ခွံ (jacket) ရောက်ရပါမယ်။ Pin တွေအောက်မှာ ဝါယာ ချောင်းလုံး တညီတည်းရှိရပါမယ်။ တခါတလေ ဝါယာဖြတ်ခဲ့တဲ့ နေရာမှာ မညီခဲ့ဘူးဆိုရင် အချို့ ဝါယာတွေက blade အောက် connector ဆုံးထိရောက်နေချိန်မှာ အချို့တော့ blade အောက်မရောက်သေးပဲလွတ်နေတာမျိုးကြုံရတတ်ပါတယ်။

step4) Crimping

network cable တစ်ချောင်းပြုလုပ်ခြင်းရဲ့နောက်ဆုံးအဆင့်ဖြစ်ပါတယ်။ Rj-45 ခေါင်းနှင့် Cat 5 cable ခေါင်းတို့ကို ခိုင်ခိုင်မြဲမြဲချိတ်ဆက်သွားအောင် crimping tools (crimper) ကို အသုံးပြုပြီး ဖိညှပ်ရပါမယ်။ အသုံးပြုမည့် crimper သည် အရည်အသွေးကောင်းဖို့လိုပါတယ်။ crimper မကောင်းရင် connector ပါပျက်ပြီး သုံးမရ ဖြစ်စေတတ်ပါတယ်။

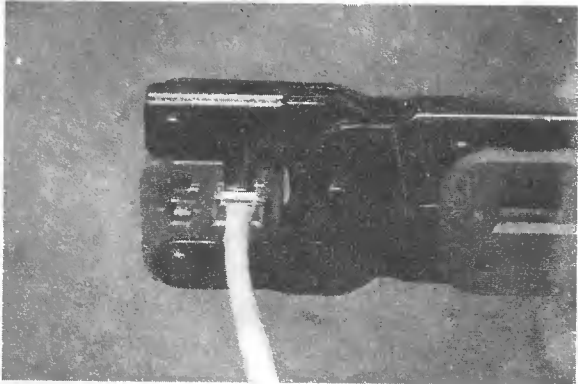
crimper အမျိုးမျိုးရှိပါတယ်။ အချို့က ဘယ်လို connector မျိုး (ဥပမာ - Rj-45 နှင့် Rj-11

၂မျိုး) အတွက်သာဆိုပြီး အကန့်အသတ်ဖြင့် အသုံးပြုနိုင်သလို အချို့ crimper များမှာတော့ connector အမျိုးမျိုးတို့အတွက် ပုံဖော်ထားသည့် သတ္တုဘလောက်တုံးလေးများကို ပြောင်းလဲတပ်ဆင်ခြင်းဖြင့် Rj-45၊ Rj-11၊ Rj-12 အစရှိသဖြင့် connector အတော်များများအတွက် အသုံးပြုရနိုင်ပါတယ်။ပုံ (11.17)



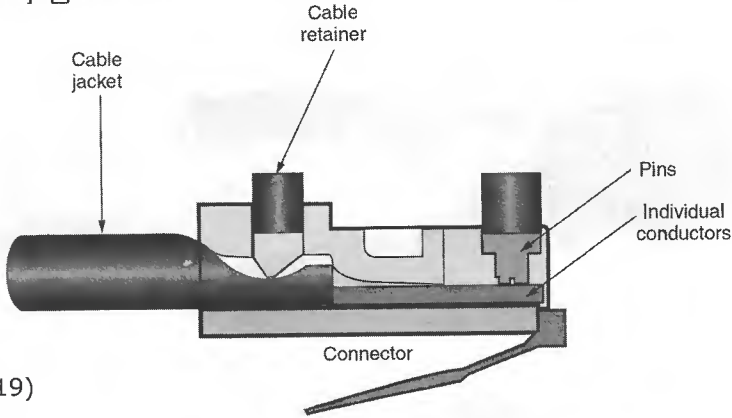
ပုံ (11.17)

crimping လုပ်ရန်အတွက် Rj-45 connector ကို crimper ထဲသို့သေချာစွာထည့်သွင်းပြီး crimper လက်ကိုင်ကို တစ်ချက်တည်းနှင့် အဆုံးထိရောက်အောင် ဖိညှပ်ရပါမယ်။ crimper တွေကို အသုံးပြုမည့် connector ပေါ်မူတည်ပြီး သင့်လျော်သောအား ထိသာသက်ရောက်မှုရှိရန် ပုံစံထုတ်ထားသည့်အတွက်အားလွန်သွားမှာစိုးရိမ်စရာမရှိပါဘူး။ ရဲရဲတင်းတင်းသာဖိချပါ။ ဖိညှပ်နေစဉ်အတွင်း connector ဆီမှ "ကလစ်" ဆိုတဲ့အသံမျိုးကြားရတတ်ပါတယ်။ပုံ (11.18)



ပုံ (11.18)

အင်္ဂလိပ် crimper ဖြင့် ဖိချလိုက်စဉ်အတွင်း connector ပေါ်မှာ အားသက်ရောက်မှု ှနေရာရှိပါတယ်။ ပုံ (11.19)။ ပထမတစ်နေရာက cutting blade များပေါ်မှာဖြစ်ပြီး ဒုတိယနေရာက plunger ပေါ်မှာဖြစ်ပါတယ်။



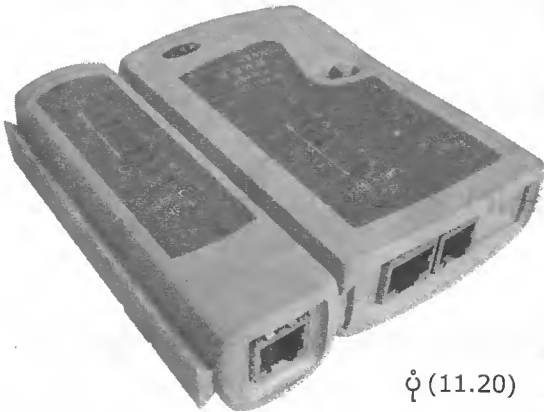
ပုံ (11.19)

crimper ကို ဖိချလိုက်တဲ့အားကြောင့် cutting blade များသည် twisted pair ဝါယာများ ပေါ်မှာ ဖုံးအုပ်ထားသော insulator ကို ဖောက်ထွက်ပြီး conductor (copper) များနှင့် တဖက်တည်းဖြစ်သွားပါတယ်။ အကယ်၍ များ နွှာထားသည့် twisted pair တို့သည် ရှည်နေပါက plunger သည် cable ၏ အပေါ်ခွံ (jacket) ပေါ်မရောက်တော့ပဲ twisted pair များပေါ်ရောက်သွား မှာဖြစ်ပါတယ်။ အင်္ဂလိပ်အခါမျိုးမှာ connector နှင့် cable တို့သည် ခိုင်ခိုင်မြဲမြဲ ချိတ်ဆက်မှု မရှိတော့ပဲ မလိုလားအပ်သော ပြဿနာများကို ကြုံတွေ့ရတတ်ပါတယ်။ အားလုံးအောင်အောင်မြင်မြင် ပြီးဆုံးခဲ့ပြီဆိုရင် cable ရဲ့အခြားတဖက်မှာ connector နောက်တခုကို တပ်ဆင်လိုက်ပါ။

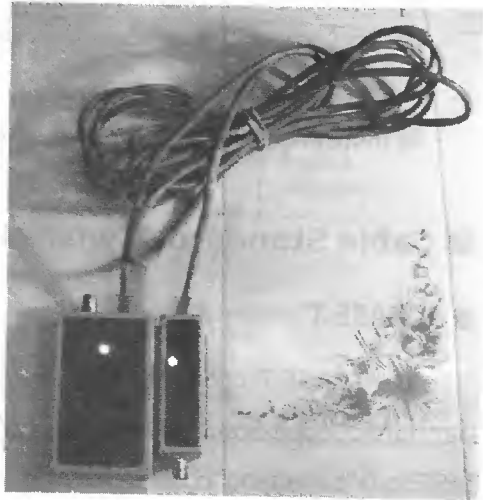


step6) Testing

network cableတစ်ခုကိုပြုလုပ်ခဲ့ပြီးပြီဆိုရင်ကောင်းမွန်စွာလုပ်ဆောင်နိုင်သောအခြေအနေတွင် ရှိမရှိဆိုတာကို cable tester ဖြင့် စမ်းသပ်စစ်ဆေးနိုင်ပါတယ်။ပုံ (11.20) cable tester တွင် LED မီးသီးငယ်များပါရှိပါတယ်။ ၎င်းမီးသီးတွေသည်straight throughတွင်ဘယ်လိုလင်းမယ်၊ cross cable တွင်ဘယ်လိုလင်းမယ်အစရှိသည့်ညွှန်ကြားချက်များကို cross testerဝယ်ယူစဉ်ကပါရှိခဲ့သော manual များတွင် ရှာဖွေ ဖတ်ရှုနိုင်ပါတယ်။

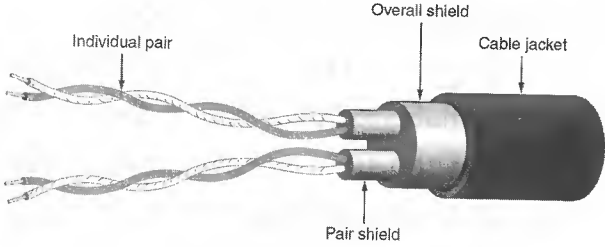


ပုံ (11.20)



STP (Shield Twisted Pair)

STP သည် UTP နှင့်များစွာဆင်တူပါတယ်။ အဓိက ကွာခြားချက်ကတော့ ဝါယာတွေကို pair များအလိုက် သီးခြား လျှပ်ကာ ပစ္စည်းတစ်ခုဖြင့် ငုံ့၍ဖုံးအုပ်ထားရုံမက အားလုံးကို ခြံပြီး ပါးလွှာသော သတ္တုပြားဖြင့် ထိန်းကာရံထားပါတယ်။ ၎င်းသတ္တုပြားကို shield လို့ခေါ်ပါတယ်။ (အချို့သော cable တွေမှာဆိုရင် သည် သတ္တုပြားမဟုတ်ပဲ သတ္တုနန်းမျှင်များကိုစကာကွက်စိတ်ပုံစံရက်လုပ်ထားလေ့ရှိ ပါတယ်)။ ၎င်း shield တို့သည်ပြင်ပသက်ရောက်မှုမရှိနိုင်အောင်အကာအကွယ်တစ်ခုပင်ဖြစ်သည့်အတွက် STP cable ကို noise များသည့် ပတ်ဝန်းကျင် တနည်းဆိုရရင် radio station၊ TV tower တို့ကဲ့သို့ strong broadcast signalထုတ်လွှတ်သည့်နေရာမျိုးတွေမှာပါအသုံးပြုနိုင်ပါတယ်။



STP cable ဖြင့် အများဆုံး သွယ်တန်းနိုင်သည့် အကွာအဝေးသည်လည်း UTP များကဲ့သို့ 100m (289ft) ဖြစ်ပြီး token ring network တွေမှာ အသုံးပြုခဲ့ကြပါတယ်။ သို့သော် ယနေ့ အချိန်မှာတော့ တဖြည်းဖြည်းနှင့် အသုံးမရှိသလောက် နည်းပါးလာပြီဖြစ်ပါတယ်။ အဲဒီလို အသုံးနည်းလာခြင်းရဲ့ အဓိက အကြောင်းအရင်းများစွာထဲက အချို့မှာ

- ကုန်ကျစရိတ်မြင့်မားခြင်း
- အရွယ်အစားပိုမိုကြီးမားပြီး ပျော့ပြောင်းမှု မရှိသည့်အတွက် cabling လုပ်တဲ့နေရာမှာ များစွာ အခက်အခဲရှိခြင်း
- install လုပ်ဖို့ရန် အချိန်ပိုယူရခြင်းတို့ဖြစ်ပါတယ်။

🔌 Cable Standard (Twisted pair)

🔌 10BASE-T

10 BASE T သည် ရှေ့က 10 BASE 2 နှင့် 10 BASE 5 တို့နေရာတွင် အစားထိုးအသုံးပြုလာခဲ့သော standard တစ်ခုဖြစ်ပါတယ်။ 10 သည် အမြင့်ဆုံးလုပ်ဆောင်နိုင်သော speed 10Mbps ကို ရည်ညွှန်းပြီး BASE သည် "baseband" လို့ခေါ်သည် transmission method ကို ရည်ညွှန်းပါတယ်။ T ကတော့ twisted pair ဖြစ်ပါတယ်။ 10BASE-T network တစ်ခု တည်ဆောက်ရန်အတွက် အသုံးပြုရမည့် cable သည် အနိမ့်ဆုံး Cat 3 ဖြစ်ရပါမယ်။ ယနေ့အချိန်မှာတော့ အနိမ့်ဆုံး Cat 5 ကိုပင် standard အဖြစ် အသုံးပြုနေကြပါပြီ။

cable segment တစ်ချောင်းရဲ့ ကွန်ပျူတာမှ hub ဆီသို့ အများဆုံး သွယ်တန်းနိုင်တဲ့ အကွာအဝေးသည် 100m ဖြစ်ပါတယ်။ ဤတွင်မှ ဆက်ဆံရရင် hub (သို့) switch တစ်ခုတည်းသာ အသုံးပြု ထားသော network တစ်ခုအတွင်းရှိ ကွန်ပျူတာ ၂ လုံးတို့ကြား အကွာအဝေးသည် အများဆုံး 100m ဖြစ်ပါတယ်။ အကယ်၍ များထိုထက်ပိုပြီး ခပ်ဝေးဝေးသို့ သွယ်တန်းဖို့ရှိလာပြီဆိုရင် hub (သို့) repeater တွေကို ကြားခံ၍ စီတန်းချိတ်ဆက်ခြင်းဖြင့် ဖြေရှင်းနိုင်ကြပါတယ်။

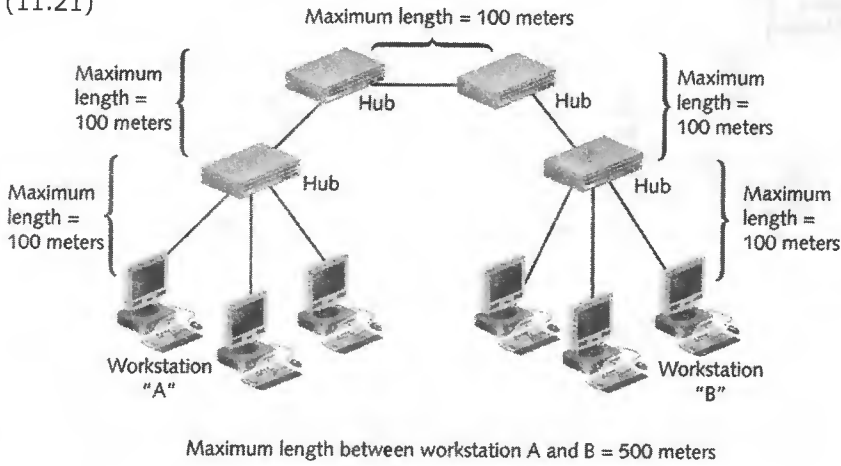
သို့သော် hub တွေ၊ repeater တွေ မြောက်များစွာခံပြီး ကြိုက်သလောက် အကွာအဝေး (၂ပမာ - km) ထိ သွယ်တန်းချင်လို့တော့ မရပါဘူး။ အကန့်အသတ်ရှိပါတယ်။ ဆိုရရင် "10 BASE T" standard ဖြင့် တည်ဆောက်မည့် network တွေသည် 5-4-3 rule ကိုလိုက်နာကြရပါတယ်။ 5-4-3 ဆိုတာက 5 သည် segment၊ 4 သည် repeater (သို့) hub၊ 3 သည် populated segment တို့ကို ရည်ညွှန်းပါတယ်။

ဖော်ပြပါ ပုံ (11.21) မှာ 10BASE T network တစ်ခုရဲ့ အမြင့်ဆုံး သွယ်တန်းနိုင်တဲ့ အကွာအဝေးကို ပုံဖော်ထားခြင်းဖြစ်ပါတယ်။ ဖော်ပြပါပုံ မှာဆိုရင် 100m အရှည် segment ၅ ခု၊ hub လေးလုံးနှင့် တဆက်လျှင် populated segment ၂ ခုတို့ကို တွေ့ရပါမယ်။

100m segment ငါးခုရအောင် ချိတ်ဆက်ထားသည့်အတွက် ထို network အတွင်းရှိ ကွန်ပျူတာ A နှင့် B တို့ကြား အကွာအဝေးသည် 500m ဖြစ်ပါတယ်။

10BASE-T Network

ပုံ (11.21)

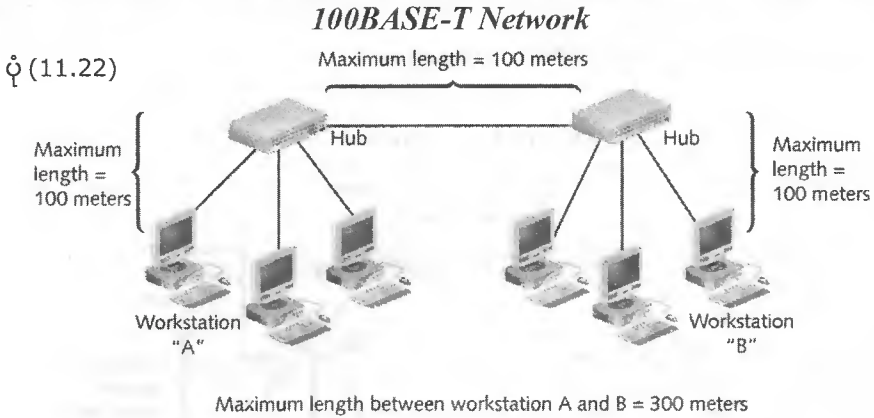


100BASE-T (Fast Ethernet)

network အရွယ်အစား ကြီးမားလာပြီး ပါဝင်တဲ့ ကွန်ပျူတာအရေအတွက်များလာတဲ့ အခါမှာ 10Mbps ဆိုတဲ့ speed သည် လုံလောက်ခြင်း မရှိတော့ပါဘူး။ သည့်အတွက် ပိုမိုမြန်ဆန်သောနှုန်းဖြင့် လုပ်ဆောင်နိုင်ရမယ်။ လက်ရှိအသုံးများနေတဲ့ 10 BASE T နှင့် အလုပ်လုပ်ပုံ တည်ဆောက်ပုံခြင်း လည်းတူတဲ့ standard တစ်ခုကို အစားထိုး အသုံးပြုလာခဲ့ကြပါတယ်။ ၎င်း standard ကတော့ 100Mbps ဖြင့်လုပ်ဆောင်နိုင်တဲ့ fast Ethernet (ဝါ) 100BASE-T ဝဲဖြစ်ပါတယ်။ IEEE မှ 802.3u လို့သတ်မှတ်ပါတယ်။

10BASE-T မှာကဲ့သို့ပင် 100BASE-T network ရှိကွန်ပျူတာတွေကို နေရာချတပ်ဆင်တဲ့ နေရာမှာ star topology ကိုပင် အသုံးပြုကြပါတယ်။ ဒါ့အပြင် အသုံးပြုသော cable သည် Cat 5 connector သည် Rj-45 နှင့် cable segment တစ်ချောင်းရဲ့အရှည်သည် အများဆုံး 100m ပင်ဖြစ်ပါတယ်။ ထို့အတူ ကွန်ပျူတာ တစ်လုံးနှင့် တစ်လုံး အကွာအဝေးပိုမိုရရှိအောင် ကြားမှာ switch တွေ၊ hub တွေစီတန်းချိတ်ဆက်ပြီး သွယ်တန်းနိုင်ပါတယ်။ ဒါပေမယ့် 100BASE-T network တွေသည် 5-4-3 rule ကို လိုက်နာခြင်း မရှိပါဘူး။ ဘာဖြစ်လို့လဲဆိုတော့ ပိုမို မြန်ဆန်သော နှုန်းဖြင့် လုပ်ဆောင်ရမှာဖြစ်သည့်အတွက် ကွန်ပျူတာတစ်လုံးနှင့်တစ်လုံး နီးနီးကပ်ကပ် communicate လုပ်နိုင်မှသာလျှင် data ပေးပို့ရယူမှုတွေမှာ အမှားအယွင်း ကင်းနိုင်မှာဖြစ်ပါတယ်။

ဒါကြောင့် 100BASE-T network တွေမှာ segment ၃ခုနှင့် hub (သို့) switch ၂ခုသာခွင့်ပြုပါတယ်။ ပုံ (11.22) တွင်ကြည့်ပါ။ segment တစ်ခုသည် 100m ဖြစ်ပါတယ်။ ဤတွင်မှ ဆက်ဆိုရရင် ကွန်ပျူတာနှစ်လုံးအများဆုံးထားရှိနိုင်သည့် အကွာအဝေးသည် 300m ဖြစ်ပါတယ်။

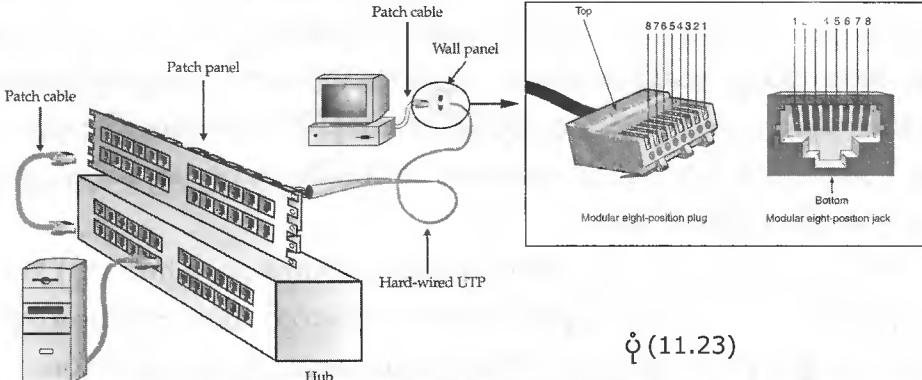


100BASE-T (Gigabit Ethernet)

ယနေ့အချိန်မှာတော့ အချို့သော network တွေအတွက် 100Mbps ဆိုတဲ့ မြန်နှုန်းသည်လည်း ပြည့်စုံလုံလောက်ခြင်းမရှိတော့ပါဘူး။ အဲဒီလို network မျိုးတွေအတွက် Gigabit Ethernet လို့ခေါ်သည့် 1000 BASE-T standard ကိုအသုံးပြုနိုင်ပါတယ်။ Gigabit Ethernet သည် twisted pair ပေါ်မှာ data တွေကို 1000Mbps (1Gbps) နှုံးဖြင့် အပို့အယူလုပ်နိုင်အောင် ပုံစံထုတ်ထားသော standard ဖြစ်ပါတယ်။ IEEE သတ်မှတ်ချက်အရ 802.3ab လို့ခေါ်ပါတယ်။

1000BASE-T network တည်ဆောက်ရန် Cat 5 နှင့် အထက် အသုံးပြုရန် လိုအပ်ပါတယ်။ အလွန်မြန်ဆန်သောနှုန်းဖြင့် data အပို့အယူလုပ်နိုင်ရန်အတွက် 4 pair (8wire) လုံးကိုအသုံးပြုကြပါတယ်။ 10BASE-T နှင့် 100BASE-T တွေမှာတုန်းက 2 pair (4wire) ကိုသာ အသုံးပြုတယ်ဆိုတာ သတိချပ်စေလိုပါတယ်။ 1000BASE-T network တို့မှာလည်း segment တစ်ခု၏အရှည်သည် အများဆုံး 100m ဖြစ်ပါတယ်။ ဒါပေမယ့် ကွန်ယူတာ ၂လုံးကို အဝေးဆုံးထားရှိ အသုံးပြုနိုင်သည့် အကွာအဝေးသည် 200m သာဖြစ်ပါတယ်။ သဘောက switch တွေကို ကြားခံစီတန်းချိတ်ဆက်အသုံးမပြုနိုင်ဆိုတဲ့ သဘောဖြစ်ပါတယ်။

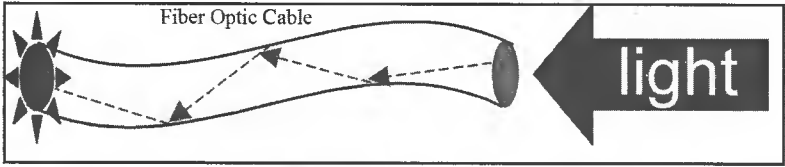
Twisted Pair wiring



ပုံ (11.23)

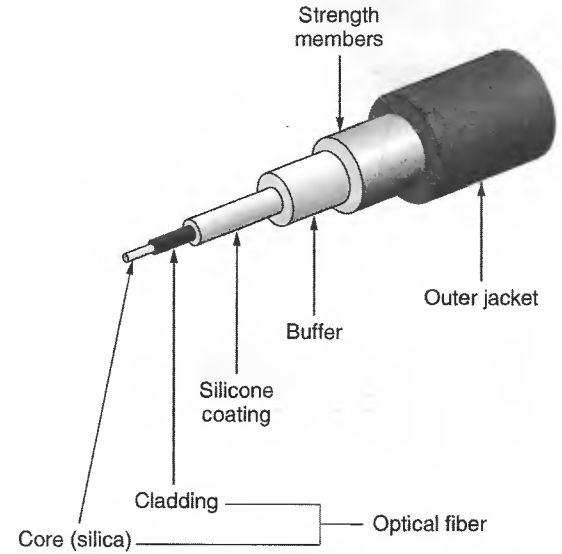
Fiber Optic Cable

Fiber-Optic technology သည် network တွေမှာ ပုံမှန် အသုံးပြုနေကျ copper media (UTP, STP, Coaxial) တို့ထက်ပိုမို ရှုပ်ထွေးပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ wire များမှာကဲ့သို့ electric signal မဟုတ်ပဲ light ကို အသုံးပြုပြီး data တွေကို transmit လုပ်သောကြောင့် ဖြစ်ပါတယ်။ ဆိုရရင် 1 နှင့် 0 တို့ကို ကိုယ်စားပြုသော electric signal များကို အလင်း on off အဖြစ် ပြောင်းပြီး ပေးပို့ပါတယ်။ အလင်းပင်ရင်း အဖြစ် laser (သို့) led ကို အသုံးပြုပါတယ်။



ပုံ (11.24)

အလင်းပင်ရင်းသည် transmit လုပ်လိုသော data (1,0) ပေါ်မူတည်ပြီး laser (သို့) led ကို ဖွင့်လိုက် ပိတ်လိုက် လုပ်ပေးပါတယ်။ အဲဒီအလင်းပင်ရင်းမှ ထွက်လာသော အလင်းတန်းသည် ဦးတည်သွားရောက်ရမယ့် ခရီးဆုံးဆီသို့ fiber cable တွင်းမှ ဖြတ်သန်းသွားရပါတယ်။ fiber cable ရဲ့တဖက်စွန်း ခရီးဆုံးနေရာမှာရှိတဲ့ sensor သည် အလင်းကိုရရှိခြင်း၊ မရရှိခြင်းဆိုတဲ့ အခြေအနေ နှစ်ခုပေါ်မူတည်ပြီး on နှင့် off ကို 0 နှင့် 1 ကိုယ်စားပြုသော electric signal များအဖြစ် ပြန်ပြောင်းပေးပါတယ်။ fiber cable ၏ အလယ်အပိုင်းတွင် ဖန် (သို့) ပလတ်စတစ်ဖြင့် ပြုလုပ်ထားသော core တစ်ခုပါရှိပြီး ၎င်းအပေါ်မှာ အလွှာအထပ်ထပ်ဖြင့် ဖုံးအုပ်ထားပါတယ်။ အောက်ဖော်ပြပါပုံ (11.25) တွင် ကြည့်ပါ။



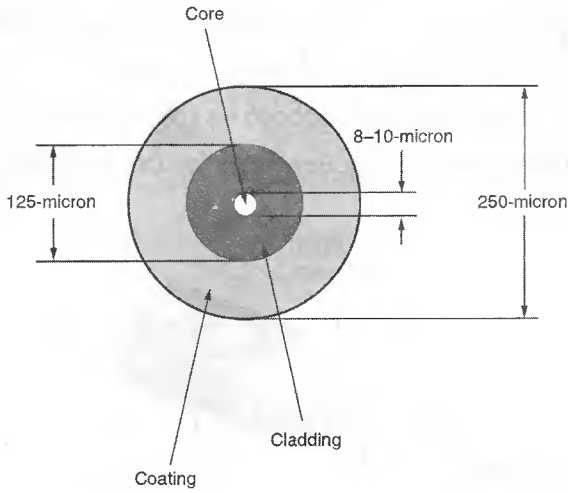
ပုံ (11.25)

plastic (သို့) silica glass core ပေါ်မှာ ကပ်လျက် ဖုံးအုပ်ထားသည့် အလွှာကတော့ cladding ပဲဖြစ်ပါတယ်။ cladding သည် core အတွင်းမှာ အလင်းပြန်စေပါတယ်။ core နှင့် cladding တို့ပေါ်မှာ

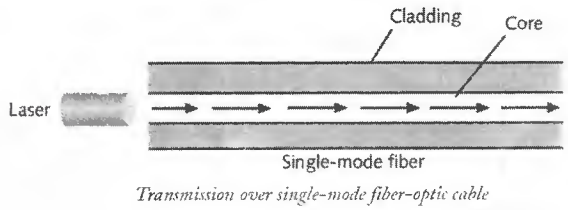
ဖုံးအုပ်ထားတဲ့ အလွှာကိုတော့ coating လို့ခေါ်ပါတယ်။ ၎င်း coating သည် light transmission နှင့် သက်ဆိုင်မှုမရှိပဲ core နှင့် cladding တို့ကိုထိချက်ပျက်စီးစေခြင်းများမှကာကွယ်ရန် သက်သက်ဖြစ်ပါတယ်။ ဒါ့အပြင်လည်းပဲ ကြိုးရဲ့ကြံ့ခိုင်မှုကိုများစွာ အထောက်အကူပြုပါတယ်။ Fiber-optic cable အမျိုးမျိုး ရှိပါတယ်။ အခြေခံအကျဆုံး ကွာခြားချက်ကတော့ signal mode လား၊ multimode လားဆိုတာပဲ ဖြစ်ပါတယ်။

● Single Mode Fiber (SMF)

Single mode fiber တွင် ဝါရှိသော core သည် လွန်စွာသေးငယ်သည့်အတွက် အလင်းတန်း တစ်ခုသာဖြတ်သန်းသွားနိုင်ပါတယ်။ အများအားဖြင့် core ၏ အချင်းသည် 8micron မှ 10micron အတွင်းဖြစ်ပါတယ်။ ပုံ (11.26) ။ one micron သည် 0.00004 လက်မခန့်နှင့်ညီမျှပါတယ်။ ဒါ့ကြောင့်ပုံမှန် SMF ရဲ့ core သည် 8micron (ဝါ) 0.0003 လက်မခန့်သာ ရှိသည့်အတွက် လူ့ဆံပင်တစ်ချောင်းထက်ပင် ငယ်ပါသေးတယ်။ cladding က 125 micron (ဝါ) 0.005 လက်မခန့်နှင့် coating layer သည် 250 micron (ဝါ) 0.01 လက်မဖြစ်ပါတယ်။



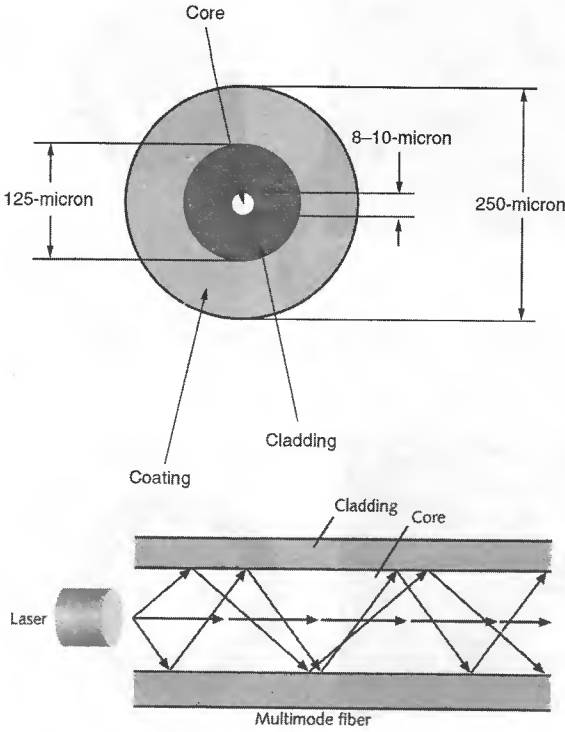
ပုံ (11.26)



အလင်းတန်းတစ်ကြောင်းသာ ဖြတ်သန်းသွားနိုင်သည့် SMF သည် နေရာဝေးဝေးသို့ data rate ပိုမိုမြင့်မားသော နှုန်းဖြင့် transmit လုပ်နိုင်ပါတယ်။ ဒါ့ကြောင့် network တွေမှာ back bone အဖြစ် အသုံးပြုကြပြီး အလင်းပြင်းအားပိုကောင်းသည့် laser ကို အလင်းပင်ရင်း အဖြစ်အသုံးပြုကြပါတယ်။

● Multimode Fiber (MMF)

Multimedia fiberမှာပါတဲ့ coreသည် SMFတို့နှင့် ယှဉ်လျှင် အရွယ်အစား ပိုကြီးသည့်အတွက် အလင်းတန်းများသည် angle အမျိုးမျိုးတို့ဖြင့် အလင်းလမ်းကြောင်းများစွာ ဖြတ်သန်းနိုင်ကြပါတယ်။ ဆိုရင် core ၏ အချင်းသည် 50 မှ 115 micron တွင်းရှိပြီး အများအားဖြင့် 62.5 micron (ဝါ) 0.002 လက်မခန့် ရှိပါတယ်။ cladding နှင့် coating layer ဂရုစလုံးရဲ့အရွယ်အစားသည် SMF ကဲ့သို့ပင် ဖြစ်ပါတယ်။ ပုံ (11.27)



ပုံ(11.27)

Transmission over multimode fiber-optic cable

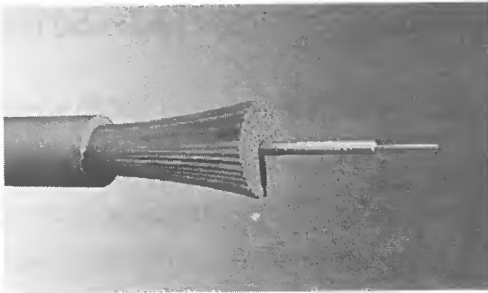
Multimedia fiber ကိုအသုံးပြုနိုင်မည့် အကွာအဝေးနှင့် transmit လုပ်နိုင်မည့် data rate တို့သည် single mode fiber မှာလောက် မများပါဘူး။ ဒါပေမယ့် အလင်းပင်ရင်း အဖြစ်ဈေးနှုန်းသက်သာ သည့် LED ကို လက်ခံ အသုံးပြုနိုင်ခြင်းနှင့် core ရဲ့အရွယ်အစား ကြီးမားသည့်အတွက် cable ဆက်ခြင်းကို ပိုမိုလွယ်ကူစွာ လုပ်ဆောင်စေနိုင်သော အားသာချက်တွေရှိပါတယ်။ ဒါ့ကြောင့် အကွာအဝေး သိပ်အရေး မကြီးတဲ့ network တွေမှာ backbone အဖြစ်လည်း အသုံးပြုကြလေ့ရှိပါတယ်။

● Number of Optical Fiber

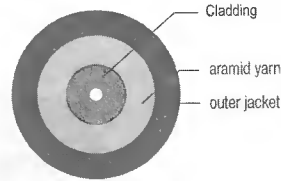
ယခုဖော်ပြသွားမှာကတော့ ပါဝင်တဲ့ fiber နန်းကြီးမျှင် အရေအတွက် ပေါ်မူတည်ပြီး ကွဲပြားတဲ့ fi-ber cable အခေါ်အဝေါ်များပဲဖြစ်ပါတယ်။ fiber နန်းကြီးမျှင် လို့ဆိုတဲ့နေရာမှာ singal mode လည်းဖြစ် နိုင်သလို multimode လည်းဖြစ်နိုင်ပါတယ်။ မည်သည့် fiber နန်းကြီးမျှင်ပဲသုံးသုံး ပါဝင်တဲ့ အရေအတွက် ပေါ်မူတည်ပြီး အဓိကအားဖြင့် cable ခုမျိုး ရှိပါတယ်။ simplex, duplex နှင့် multifiber cable တို့ဖြစ်ပါတယ်။

● Simplex Cable

Simplex cableအတွင်းမှာ fiber နန်းကြိုးမျှင်တစ်ချောင်းသာ ပါရှိပါတယ်။ အဲဒီလို နန်းကြိုးမျှင် တစ်ချောင်းသာပါရှိသည့်အတွက် ကြိုးရဲ့ကြိုင်ခိုင်မှုကို တိုးမြှင့်စေရန် ထူထဲသော coating၊ strength member ၊ အပေါ်ခွံ jacket တို့ဖြင့် ဖုံးအုပ်ထားပါတယ်။ ပုံ (11.28)



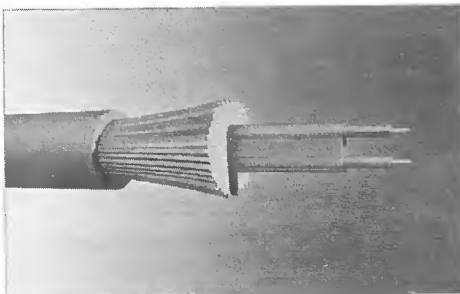
Cable Components



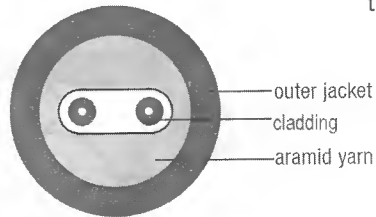
ပုံ (11.28)

● Duplex Cable

Duplex Cable မှာဆိုရင် fiber နန်းကြိုးမျှင် ၂ ချောင်း ပါရှိပါတယ်။ LAN back bone အဖြစ် အသုံးအများဆုံး cable လည်းဖြစ်ပါတယ်။ ပုံ (11.29)

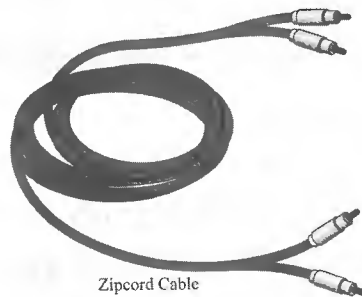


Cable Components



ပုံ (11.29)

duplex တော့ duplex ပါပဲ။ ဒါပေမယ့် တကယ့် technically အရ duplex မဟုတ်သော zipcord လို့ခေါ်သည့် cable တစ်မျိုးရှိပါတယ်။ အမှန်တကယ်က simplex ၂ ချောင်းကို တစ်ချောင်းထဲကဲ့သို့ ဖြစ်အောင် ပူးထားခြင်းမျိုးဖြစ်ပါတယ်။ fiber နန်းကြိုးမျှင် ၂ ချောင်းပါရှိသော duplex လို့ခေါ်ခြင်း ဖြစ်ပါတယ်။ ပုံ (11.30) ၎င်း zipcord တွေကို အဓိကအားဖြင့် patch cable အဖြစ်အသုံးပြုကြပါတယ်။

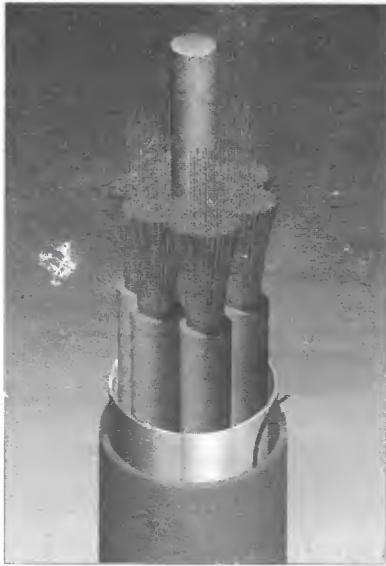


Zipcord Cable

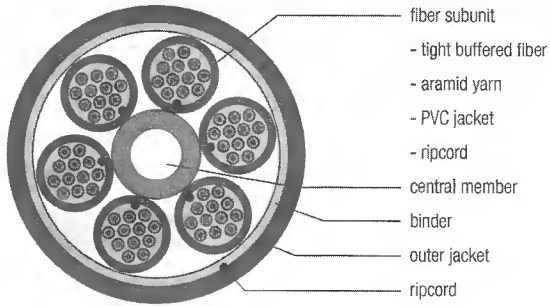
ပုံ (11.30)

☛ Multifiber Cable

Cable တစ်ချောင်းထဲမှာ fiber နန်းကြီးမျှင် ၂ ချောင်းအထက်ပါရှိသော မည်သည့် cable ကိုမဆို multifiber လို့ခေါ်ပါတယ်။ ဆိုရရင် multifiber cable တစ်ချောင်းမှာ fiber နန်းကြီးမျှင် သုံးချောင်းမှ ရာနှင့်ချီပြီးပါရှိနိုင်ပါတယ်။ပုံ (11.31)



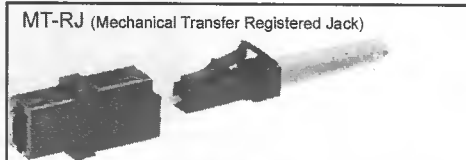
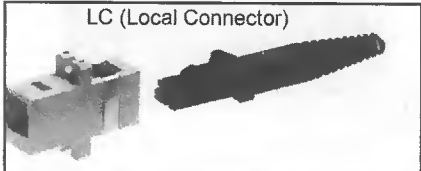
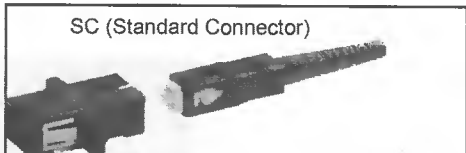
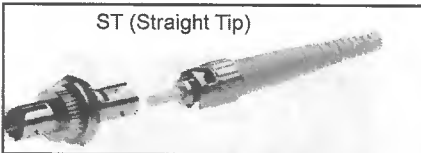
Cable Components



ပုံ (11.31)

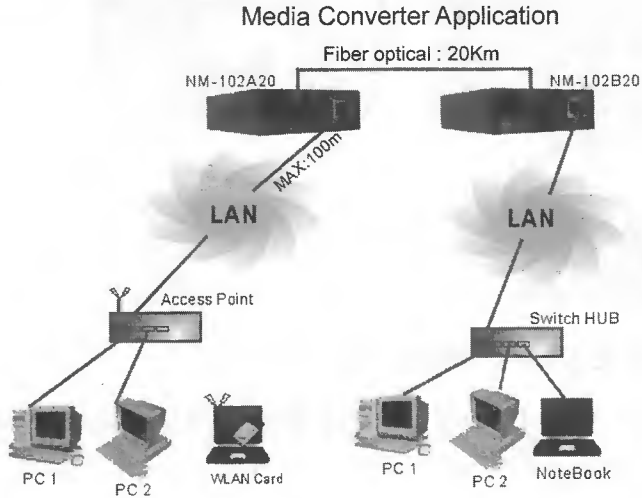
☛ Fiber Optic Cable Connectors

Fiber-optic connector အမျိုးအစားများစွာရှိပါတယ်။ အဲဒီအထဲကမှ လေးမျိုးလောက်သာလျှင် တွင်တွင်ကျယ်ကျယ် အသုံးပြုကြပါတယ်။ ST (straight Tip)၊ SC (standard Connector)၊ LC (local connector) နှင့် MT-RJ (Mechanical Transfer Register Jack) တို့ပဲဖြစ်ပါတယ်။ ၎င်း connector များကို single mode နှင့် multi mode ၂ မျိုးစလုံးအတွက် အသုံးပြုကြပါတယ်။ ယနေ့လက်ရှိ fiber network တွေမှာဆိုရင် အများအားဖြင့် ST နှင့် SC တို့ကိုသာ အသုံးပြုကြလေ့ရှိပါတယ်။ MT-RJ ကတော့ နောက်ဆုံးပေါ် connector အမျိုးအစား ဖြစ်ပါတယ်။



Media Converter

မတူတဲ့ media ၂ခု (ဥပမာ - twisted pairနှင့် fiber) တို့ကို ချိတ်ဆက်အသုံးပြုနိုင်ရန် ကြားခံ device တစ်ခုရှိဖို့ လိုပါတယ်။ ဆိုရရင် twisted pair ပေါ်မှာ data တွေသည် signal များအဖြစ် ဖြတ်သန်းသွားလာပြီး fiberပေါ်မှာတော့ light wave signal များအဖြစ် ဖြတ်သန်းပေးပို့ကြသည့်အတွက် ၎င်း media ၂ခုတို့ကို ဒီအတိုင်း သူတို့ချည်းသက်သက်တိုက်ရိုက် ချိတ်ဆက်လို့မရပါဘူး။ တဖက် twisted pair ကလာတဲ့ electric signal အတွေ့ကို light wave signal တွေအဖြစ်ပြောင်းပြီး fiber ပေါ်တင်ပေးမယ်။ ထို့အတူ fiber cable ပေါ်ကလာတဲ့ light wave signal တွေကို electric signal တွေအဖြစ်ပြောင်းပြီး twisted pair ပေါ်တင်ပေးမယ့် ကြားခံ device တစ်ခုလိုပါတယ်။ အဲဒီလို မတူညီတဲ့ media ၂ခုတို့ ကြားမှာ ကြားခံချိတ်ဆက်ပြီး signal တွေဖလှယ်ပေးနိုင်မယ့် device ကို media converter လို့ခေါ်ပါတယ်။



အောက်ဖော်ပြပါပုံ (11.32) ကတော့ media converter တစ်ခုရဲ့ပုံဖြစ်ပါတယ်။ တဖက်မှာ twisted pair cable တို့အတွက် Rj-45 port တစ်ခုပါရှိပြီး အခြားတဖက်မှာ fiber cable အတွက် SC port တစ်ခုပါရှိပါတယ်။

ပုံ (11.32)



Cable Standard (Fiber Optic Cable)

10BASE-FL

10BASE-FL standardမှာပါတဲ့ **10**သည် 10Mbps၊ **BASE**သည် baseband transmissionနှင့် **F**သည် fiber cableကိုရည်ညွှန်းပါတယ်။ 10BASE-FL၏ speedသည် 10Mbpsသာဖြစ်သော်လည်း segment တစ်ခု၏ အရှည်ကို 1000m အထိသွယ်တန်း အသုံးပြုပါတယ်။ repeater ခံပြီး ချိတ်ဆက်မယ်ဆိုရင် 2000m ထိရရှိနိုင်ပါတယ်။ ဒါ့ကြောင့် speed သည်သိပ်အရေးမပါဘဲ အကွာအဝေးကိုဦးစားပေးတဲ့ အချို့ network တွေမှာ ယနေ့တိုင်အောင် အသုံးပြုနေကြဆဲဖြစ်ပါတယ်။

Characteristics of 10BASE-FL

	Speed	Max. Length	Topology	Cable Type
10BASE-FL	10Mbps	2 kilometers	Star	Fiber-optic

100BASE-FX

10BASE-FX standardသည် fiber cableနှင့် baseband transmissionတို့ကိုအသုံးပြုပြီး 100Mbpsဖြင့်လုပ်ဆောင်နိုင်သော networkကိုရည်ညွှန်းပါတယ်။ 100BASE-FXအတွက်အနည်းဆုံး fiber နန်းကြိုးမျှင် ၂ချောင်းပါသော multimode fiber ဖြစ်ဖို့လိုပါတယ်။ half-duplex mode ဖြင့် သုံးမယ်ဆိုရင်တစ်ကြိုးသည် sendingအတွက်ဖြစ်ပြီးနောက်တစ်ကြိုးသည် receivingအတွက်သီးခြားစီဖြစ်ပါတယ်။ full-duplexဖြင့် သုံးမယ်ဆိုရင်တော့ နှစ်ကြိုးစလုံးကို sendingကော receivingအတွက်ပါ သုံးမှာဖြစ်ပါတယ်။ half-duplex modeဖြင့် segmentတစ်ခုရဲ့အရှည်ကို 412mထိသာအသုံးပြုနိုင်ပြီး၊ full duplex modeဖြင့်သုံးမယ်ဆိုရင်တော့ 2000mထိအသုံးပြုနိုင်ပါလိမ့်မယ်။ 100BASE-FXသည်လည်း 100BASE-T ကဲ့သို့ပင် Fast Ethernet ပင်ဖြစ်ပြီး IEEE ၏ standard သတ်မှတ်ချက်အရ 802.3u ပင်ဖြစ်ပါတယ်။

Characteristics of 100BASE-FX

	Speed	Max. Length	Topology	Cable Type
100BASE-FX	100Mbps	2 kilometers	Star	Fiber-optic

1000BASE-LX

1000 BASE-LXသည် 1000 mbpsနဲ့ဖြင့်လုပ်ဆောင်နိုင်တဲ့ "Gigabit Ethernet" standardတွေထဲမှာတော့အသုံးအများဆုံးဖြစ်ပါတယ်။ LXသည် "long wavelength" ကိုရည်ညွှန်းပါတယ်။ ယနေ့ထွက်ပေါ်လာသမျှ gigabit technologyတွေထဲမှာတော့အဝေးဆုံးသွယ်တန်းအသုံးပြုနိုင်တဲ့ stan

-dard တစ်ခုလည်းဖြစ်ပါတယ်။ အဝေးဆုံးလို့ဆိုတဲ့နေရာမှာ multi modeလား၊ single modeလားဆိုတဲ့ အချက်ပေါ်တော့ မူတည်ပါသေးတယ်။ multimode fibersနှင့်ဆိုရင် segmentတစ်ခု၏အရှည်ကို 550m ထိ အသုံးပြုနိုင်ပါတယ်။ single mode နှင့်ဆိုရင်တော့ 5000m (5km) ထိအသုံးပြုနိုင်ပါတယ်။ သူ့ရဲ့ အကွာအဝေး အားသာချက်အရပင် 1000BASE-LX ကို backbone အဖြစ်ရွေးချယ် အသုံးပြု လေ့ရှိပါတယ်။

Characteristics of 1000BASE-LX

	Speed	Max. Length	Topology	Cable Type
1000BASE-LX	1000Mbps	550 Meters	Star	Fiber-optic (MMF)
1000BASE-LX	1000Mbps	5000 Meters	Star	Fiber-optic (SMF)

10 Gigabit Fiber-Optic Standard

နောက်ဆုံးပေါ်နှင့်အမြန်ဆုံး cable standardသည် 10G standardဖြစ်ပါတယ်။ 10 Gသည် 10Gbpsကိုရည်ညွှန်းပါတယ်။ 10GBASE-SR၊ 10GBASE-LR၊ 10GBASE-ERဆိုပြီး 10G standard သုံးမျိုးရှိပါတယ်။ ၎င်းတို့၏ အဓိကကွာခြားချက်ကတော့ ဘယ်လောက်အကွာအဝေးထိ သွယ်တန်း အသုံးပြုနိုင်မလဲဆိုတဲ့ transmission distanceပင်ဖြစ်ပါတယ်။

10GBASEX Cable Standards

	10GBASE-SR	10GBASE-LR	10GBASE-ER
Maximum Distance	82 meters	10 kilometers	40 kilometers

Building A Peer-To-Peer Network

အခြားသော network တွေနှင့် ယှဉ်လျှင် peer-to-peer network တွေသည် တည်ဆောက်ရတာ လွယ်ကူသလို အသုံးပြုမှုအပိုင်းမှာလည်းများစွာ နားလည်တတ်ကျွမ်းဖို့မလိုပဲ knowledge အနည်းငယ်ရှိရုံဖြင့် အသုံးပြုနိုင်ကြပါတယ်။ ဒါ့အပြင် ငွေကြေး အမြောက်အများ သုံးစွဲစရာမလိုပဲ စရိတ်စကအကျဉ်းဆုံးဖြင့်တည်ဆောက်နိုင်တဲ့ network မျိုးလည်းဖြစ်ပါတယ်။ peer-to-peer network တစ်ခုကိုမတည်ဆောက်ခင် အောက်ဖော်ပြပါ device တွေအဆင်သင့်ရှိဖို့လိုအပ်ပါလိမ့်မယ်။

■ Network Interface Card (NIC)

ကွန်ပျူတာတစ်လုံးစီအတွက် NIC တစ်ခုစီရှိရပါမယ်။ built-in NIC ပါတဲ့ကွန်ပျူတာတွေအတွက် တော့သီးခြား NIC မလိုပါဘူး။

■ HUB (or) Switch

ကွန်ပျူတာတွေအားလုံး ချိတ်ဆက် တပ်ဆင်နိုင်ရန် လုံလောက်သော port အရေအတွက်ပါသော hub (သို့) switch မျိုးဖြစ်ရပါမယ်။

■ Cable

ကွန်ပျူတာတစ်လုံးစီအတွက် straight-through cable တစ်ချောင်းစီလိုပါတယ်။

■ Computer

1995 မှစ၍ ယနေ့တိုင်အောင် Microsoft မှ ဖြန့်ချိရောင်းချခဲ့သော Windows Operating System အားလုံးတို့တွင် peer-to-peer network တစ်ခု တည်ဆောက်ရန် လိုအပ်တဲ့ software အားလုံးတို့သည် built-in အဖြစ် အဆင်သင့်ပါရှိပြီးသား ဖြစ်ပါတယ်။ Microsoft ထံမှ ထွက်ရှိပြီးသမျှထဲက နောက်ဆုံးထုတ် windows 2000 professional နှင့် Windows XP တို့သည် အသုံးပြုရတာလည်း လွယ်ကူသလို network ပိုင်းနှင့် ပတ်သက်ရင်လည်း အတော်လေးကို စိတ်ချလက်ချ အသုံးပြုနိုင်တဲ့ Desktop OS တို့ပင်ဖြစ်ပါတယ်။

Windows 2000 Pro နှင့် Window Xp တို့တွင် တူတဲ့အချက်အတော်များပါတယ်။ ၎င်းတို့ ၂ခုစလုံးတွင် desktop ပေါ်ရှိ "my network place" နှင့် "my computer icon" တို့မှတစ်ဆင့် network ပိုင်းနှင့် ပတ်သက်သော configuration များကို လုပ်ဆောင်နိုင်ကြပါတယ်။ အထူးသဖြင့် Window XP နှင့်ဆိုရင် NIC အများစုကို အလိုအလျှောက် ထောက်လှမ်းသိရှိပြီး လိုအပ်သော driver software တွေကို သူ့ဘာသာ install လုပ်ပေးနိုင်ပါတယ်။

ဖော်ပြပါပစ္စည်းတွေအဆင်သင့်ရှိပြီဆိုရင် network တစ်ခုတည်ဆောက်လို့ရပါပြီ။ peer-to-peer network တည်ဆောက်ပုံကို အပိုင်း ၃ ပိုင်းခွဲပြီး ဖော်ပြသွားပါမယ်။

■ Part 1 - Installing Network Adapter

ပထမဦးစွာ NIC ကို ကွန်ပျူတာမှာ စိုက်သွင်းတပ်ဆင်မယ်။ ပြီးရင် NIC အတွက် လိုအပ်တဲ့ driver ကို install လုပ်ရပါမယ်။

■ Part 2 - Configuring Your Network

အသုံးပြု၍ ရနိုင်သော network တစ်ခု အဖြစ်ရရှိအောင် ကွန်ပျူတာတွေမှာ လိုအပ်တဲ့ setting (ဥပမာ IP address | computer name | workgroup name) တို့ကို configure လုပ်ပေးရပါမယ်။

■ Part 3 - Testing Your Computer Connectivity

ကွန်ပျူတာတစ်လုံးနှင့် တစ်လုံး အပြန်အလှန် communicate လုပ်နိုင်သော အခြေအနေတွင် ရှိမရှိဆိုတာကို စစ်ဆေးကြမှာဖြစ်ပါတယ်။

🔍 Part 1-Installing Network Adapter

Network Card မှ မဟုတ်ပါဘူး။ မည်သည့် device ကိုမဆို ကွန်ပျူတာမှာ တပ်ဆင်အသုံးပြုမယ်ဆိုရင် အောက်ဖော်ပြပါအဆင့် ၂ဆင့်ကို လုပ်ဆောင်ကြရမှာဖြစ်ပါတယ်။

- 1) device ကို ကွန်ပျူတာမှာ ချိတ်ဆက် တပ်ဆင်ခြင်း
- 2) ၎င်း device အတွက် လိုအပ်တဲ့ driver ကို install လုပ်ခြင်းတို့ဖြစ်ပါတယ်။

ဒီနေရာမှာ အထူးသတိပြုရမည့် အချက်ကတော့ မိမိရွေးချယ် အသုံးပြုမည့် adapter ပေါ်မူတည်ပြီး တပ်ဆင်ပုံနှင့် driver install လုပ်ပုံများသည် အနည်းငယ်ကွဲလွဲမှုများ ရှိလာနိုင်မှာဖြစ်ပါတယ်။ ဆိုရရင် laptop ဖြင့် အသုံးပြုသူများ၊ USB NIC အသုံးပြုသူများအနေနှင့် ကတော့ network adapter ကို laptop ရှိ card slot (သို့) USB port တစ်ခုခုမှာ တပ်ဆင်ပြီး ၎င်း adapter အတွက် driver ကို install လုပ်လိုက်ရုံဖြစ်ပါတယ်။



သို့သော် PCI NIC ကို desktop ကွန်ပျူတာမှာ တပ်ဆင်မယ်ဆိုရင်တော့ ကွန်ပျူတာပါဝါပိတ်၊ အဖုံးဖွင့်ပြီး motherboard ပေါ်ရှိ လွတ်နေတဲ့ PCI slot နေရာမှာ စိုက်သွင်းတပ်ဆင်ရမှာ ဖြစ်သည့်အတွက် အနည်းငယ်ပိုမိုခက်ခဲစေမှာဖြစ်ပါတယ်။ ဒါ့ကြောင့် ဒီနေရာမှာတော့ မည်သူမဆို အလွယ်တကူ တပ်ဆင်နိုင်တဲ့ PC card တို့၊ USB NIC တို့ တပ်ဆင်ပုံကို အထူးတလည် ဖော်ပြတော့မှာ မဟုတ်ပဲ အနည်းငယ်ပိုမိုရှုပ်ထွေးတဲ့ PCI NIC တပ်ဆင်ပုံ အဆင့်ဆင့်ကိုသာ ဖော်ပြသွားမှာ ဖြစ်ပါတယ်။ ပြီးမှမည်သည့် network adapter ကိုပဲသုံးသုံး မဖြစ်မနေ လုပ်ဆောင်ဖို့ရန်လိုသော driver installation ကို ဆက်လက်ဖော်ပြသွားမှာ ဖြစ်ပါတယ်။

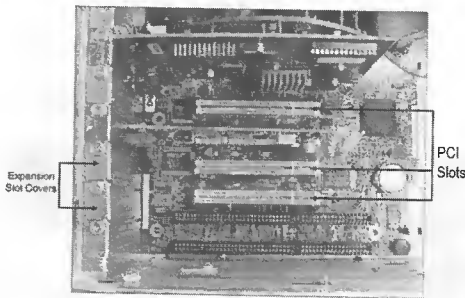
Installing PCI Network Adapter In Desktop PC

PCI Network Adapter တစ်ခုကို desktop PC တစ်လုံးမှာ တပ်ဆင်ခြင်းကို အောက်ပါအဆင့်များအတိုင်းလုပ်ဆောင်နိုင်ပါတယ်။

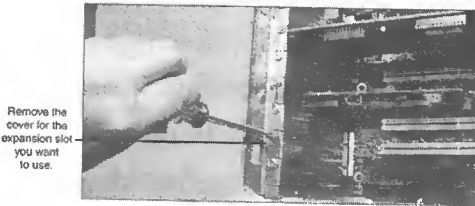
step1) ကွန်ပျူတာကို shutdown လုပ်ပြီးသွားပြီဆိုရင် နံရံမှလာသော ပါဝါကြိုးကို ဖြုတ်ထားလိုက်ပါ။

step2) ပထမဦးစွာ casing ရဲ့ဘေးတစ်ဖက်တစ်ချက်မှာရှိတဲ့ အဖုံးများကို ဖွင့်ရပါမယ်။ အများအားဖြင့် casing ရဲ့နောက်ဖက်မှ screw လေးလုံး (သို့) ခြောက်လုံးကို ဖြုတ်လိုက်ရုံသာ ဖြစ်ပါတယ်။ သို့သော်လည်း casing ရဲ့ design ပေါ်မူတည်ပြီး အဖွင့်အပိတ်လုပ်ပုံများ ကွဲပြားနိုင်ပါတယ်။ casing ကိုဖွင့်ပြီးသွားတဲ့အခါ ပုံ (12.1) မှာ ပြထားတဲ့အတိုင်း အဖြူရောင် PCI slot များကို မြင်ရပါလိမ့်မယ်။

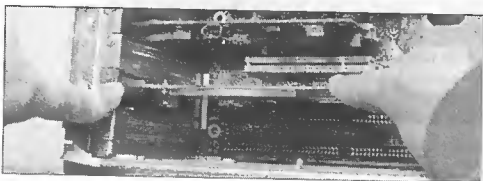
ပုံ (12.1)



step3) NIC တပ်ဆင်လိုတဲ့ PCI slot နေရာရှိ cover ကို ဖယ်ရှားလိုက်ပါ။ ပုံ (12.2)



step4) NIC ကို သေသေချာချာ ခိုင်ခိုင်မြဲမြဲနှင့် အထိုင်ကျသွားသည်အထိ ဂရုတစိုက်တပ်ဆင်ပါ။ screw ကို သေသေချာချာစုပ်ပါ။ ပုံ (12.3)



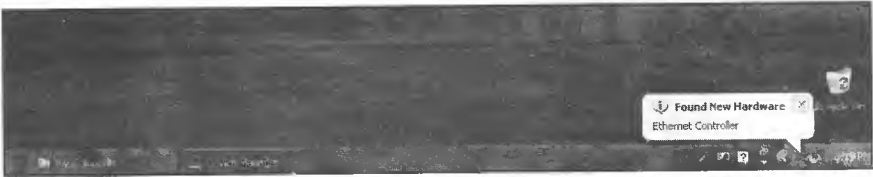
step5) casing ၏ဘေးတစ်ဖက်တစ်ချက်ရှိ အဖုံးကို ပြန်ပိတ်ပါ။ ပါဝါကြိုး ပြန်တပ်ပြီး ခလုတ်ဖွင့်ပါ။

● Installing Driver for NIC

windows XP သည် "plug and play" system တစ်ခုပင်ဖြစ်ပါတယ်။ သဘောကတော့ "plug and play" device တစ်ခုကိုကွန်ပျူတာမှာတပ်ဆင်လိုက်တာနှင့် windows XPမှအလိုလျောက် ထောက်လှမ်းသိရှိနိုင်ခြင်းကိုဆိုလိုပါတယ်။ ဥပမာအားဖြင့် network adapter ကို ကွန်ပျူတာမှာ တပ်ဆင်ပြီး reboot လုပ်တာနှင့် windows XPသည်၎င်း card ကိုထောက်လှမ်းသိရှိပြီး သူ့ဖာသာသူ အလိုလျောက် install လုပ်ဖို့ကြိုးစားပါလိမ့်မယ်။ အဲဒီလို ကွန်ပျူတာမှ အလိုလျောက် ထောက်လှမ်းသိရှိ နိုင်တဲ့ deviceတွေကို plug and play device တွေလိုခေါ်ပြီး ယနေ့ဈေးကွက်အတွင်းမှာဝယ်ယူရရှိနိုင်တဲ့ NICအားလုံးနီးပါးတို့သည် plug and playများပဲဖြစ်ပါတယ်။

NIC ကို တပ်ဆင်ပြီး reboot လုပ်လိုက်သည့်အခါမှာသော်လည်းကောင်း၊ USB port မှာ တပ်ဆင်လိုက်သည့်အခါမှာသော်လည်းကောင်း windows XP သည်၎င်း NICကို ထောက်လှမ်းသိရှိပြီး found new hardware ဆိုတဲ့ messageကို taskbar ပေါ်မှာဖော်ပြပါလိမ့်မယ်။

ပုံ (12.4)



windows XP မှ device ကို တွေ့ရှိပြီးဆိုရင် အသုံးပြုရန်ရနိုင်သော အဆင့်သို့ရောက်အောင် လိုအပ်သော driver များကို စတင် install လုပ်ဖို့ရန် ကြိုးစားပါလိမ့်မယ်။ ပုံမှန်အား ဖြင့် NIC တစ်ခုကို ဝယ်ယူတိုင်း၎င်းအတွက် driverကို CDဖြင့် တစ်ပါတည်း ပူးတွဲရရှိမှာဖြစ်ပါတယ်။ ဒါ့အပြင်လည်းပဲ Windows XPတွင် အချို့သော device များအတွက် driverများ ပါရှိပြီးသား ဖြစ်ပါတယ်။

အဲဒီလိုမိမိတပ်ဆင်လိုက်တဲ့ deviceအတွက် driver software သည် windows XP ထဲမှာ ရှိပြီးသားဆိုပါက ၎င်းရှိပြီးသား driver ဖြင့်ပင်အလိုလျောက် ဆက်လက် install လုပ်ပါလိမ့်မယ်။ driver installationအောင်မြင်စွာပြီးဆုံးသွားပြီဆိုရင်စတင်အသုံးပြုနိုင်ရန် အဆင်သင့်ဖြစ်ပါပြီဆိုတဲ့ message alertကို taskbar ပေါ်တွင်တွေ့ရပါလိမ့်မယ်။

ပုံ (12.5)



အကယ်၍ windows XP သည် deviceကိုတွေ့ရှိသော်လည်း သင့်လျော်သော driver software ကိုရှာမတွေ့ပါက "Found New Hardware" wizard ပေါ်လာမှာ ဖြစ်ပါတယ်။ ဒီနေရာကနေ ရှေ့ဆက် installလုပ်ဖို့ရန် မိမိမှာရှိတဲ့ driverပေါ်မူတည်ပြီး နည်းလမ်း ၂ခုရှိပါတယ်။ ဆိုရရင် အင်တာနက်မှ

downloadဆွဲထားသော driver fileတွေချည်းသက်သက်လား၊ autorun programပါရှိသော driver CDလားဆိုတဲ့ပေါ်မူတည်ပြီးလုပ်ဆောင်ပုံများကွဲပြားမှာဖြစ်ပါတယ်။

မိမိမှာမူလစဉ်းဝယ်ယူစဉ်ကတည်းကပူးတွဲပါရှိသော autorun-programပါရှိသည့် CDရှိပါက "found new hardware" wizardကို cancelလုပ်လိုက်ပါ။ manufacture CD ကိုထည့်သွင်းလိုက်ပါက ရွေးချယ်စရာ optionတွေပါရှိတဲ့ autorun programပွင့်လာပါလိမ့်မယ်။ပုံ (12.6)

ပုံ (12.6)



Install Driver တွင် click နှိပ်ပြီးပေါ်လာတဲ့ ညွှန်ကြားချက်များ အတိုင်း လိုက်ပါ install လုပ်လိုက်ရုံဖြစ်ပါတယ်။ installပြီးသွားတဲ့အခါ restartလုပ်ဖို့လိုကောင်းလိုပါလိမ့်မယ်။ restartလုပ်ပြီး စက်ပြန်တက်လာတဲ့အခါ ၎င်း device သည် အသုံးပြုဖို့ရန် အဆင်သင့်ဖြစ်နေပါလိမ့်မယ်။

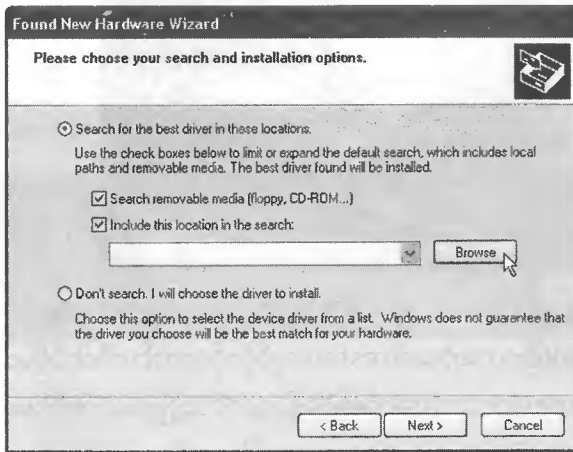
အကယ်၍မိမိရဲ့driver CDမှာ auto program မပါရှိဘူးသို့တည်းမဟုတ်အင်တာနက်မှ downloadရယူထားသော driver fileတွေချည်းသက်သက်ဆိုရင် အသုံးပြုသူမှ driver fileများရှိရာနေရာ (CD drive၊ Floppy drive) ကို ညွှန်ပြပေးခြင်းဖြင့် ပြီးဆုံးအောင်မြင် သည်အထိ ဆက်လက်လုပ်ဆောင် သွားကြရမှာ ဖြစ်ပါတယ်။ အောက်ဖော်ပြပါပုံ (12.7)ကတော့ found new hardware wizard ပင်ဖြစ်ပြီး ရွေးချယ်စရာ option ၂ခုပါလေ့ရှိပါတယ်။

ပုံ (12.7)

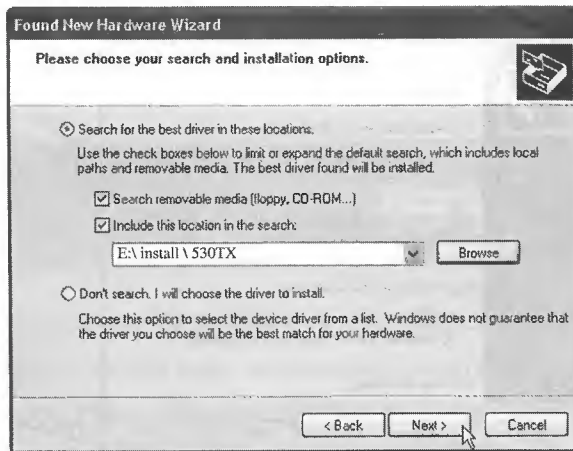


ပထမ option ကတစ်ဆင့်ထားသည့် ပစ္စည်းသစ်အတွက် လိုအပ်သော driver ကို windows XP မှ အလိုလျောက်ရှာဖွေ install လုပ်ရန်ဖြစ်ပြီး ဒုတိယ option ကတော့ driver file များရှိရာနေရာကို ညွှန်ပြပေးရန်တို့ဖြစ်ပါတယ်။

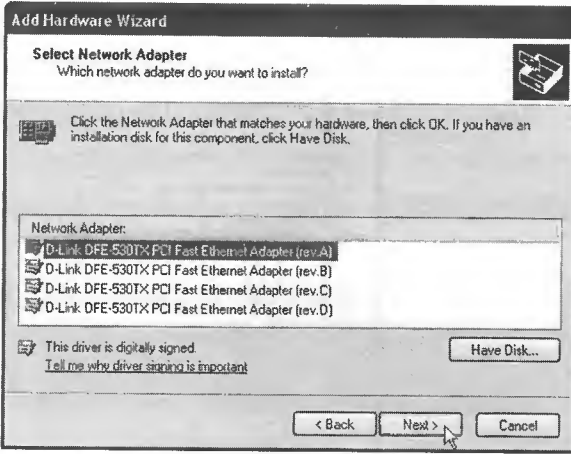
ဒုတိယ option ကိုရွေးချယ်သင့်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ windows XP မှ အလိုလျောက်ရှာဖွေ install လုပ်နိုင်ခြင်းမရှိသည့်အတွက် ယခုလို ကိုယ်တိုင်ကိုယ်ကျ လိုက်ပါ လုပ်ဆောင် နေရခြင်း ဖြစ်သည့်အတွက်ကြောင့် ထပ်မံရှာဖွေခိုင်းပါကလည်း အောင်မြင်ဖို့ရန် အခွင့်အလမ်းနည်း ပါးလှပါတယ်။ ဒါကြောင့် ဒုတိယ option ကိုရွေးချယ်ပြီး **Next** button တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ အောက်ဖော်ပြပါ wizard ကိုတွေ့ရပါမယ်။



ဒီ wizard ထဲမှာဆိုရင် driver file ရှိရာနေရာကို ရွေးချယ်ညွှန်ပြပေးရပါမယ်။ ပထမ option ဖြစ်တဲ့ **search for the best driver** ကို ရွေးချယ်လိုက်ပါ။ ထို့နောက် driver file များရှိရာ နေရာကို **Browse** button တွင် click လုပ်ပြီး ညွှန်ပြပေးရပါမယ်။ ညွှန်ပြပေးပြီးဆိုရင် **Next** တွင် click နှိပ်လိုက်ပါ။



တစ်ခါတလေ device အမျိုးအစားအမည်တစ်ခုထက်မကကို ဖော်ပြလေ့ရှိပါတယ်။ အဲဒီလို အခါမျိုးမှာ မိမိတပ်ဆင်ထားသော device နှင့် ကိုက်ညီသော အမည်ကို ရွေးချယ်ပြီးပါက **Next** တွင် click နှိပ်လိုက်ပါ။

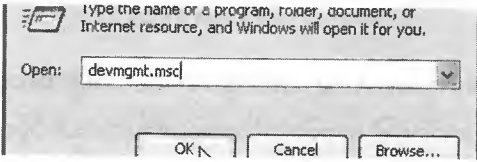


ကျန်ရှိနေသောအဆင့်များကို ပေါ်လာမည့် ညွှန်ကြားချက်များအတိုင်း ဆက်လက် လုပ်ဆောင်သွားလိုက်ပါ။ နောက်ဆုံးအဆင့်မှာတော့ **finish** button ပါတဲ့ wizard ကိုတွေ့ရပါလိမ့်မယ်။ ၎င်း **Finish** button တွင် click နှိပ်ပြီး device installation ကို အဆုံးသတ်လိုက်ပါ။

Managing Device Manager

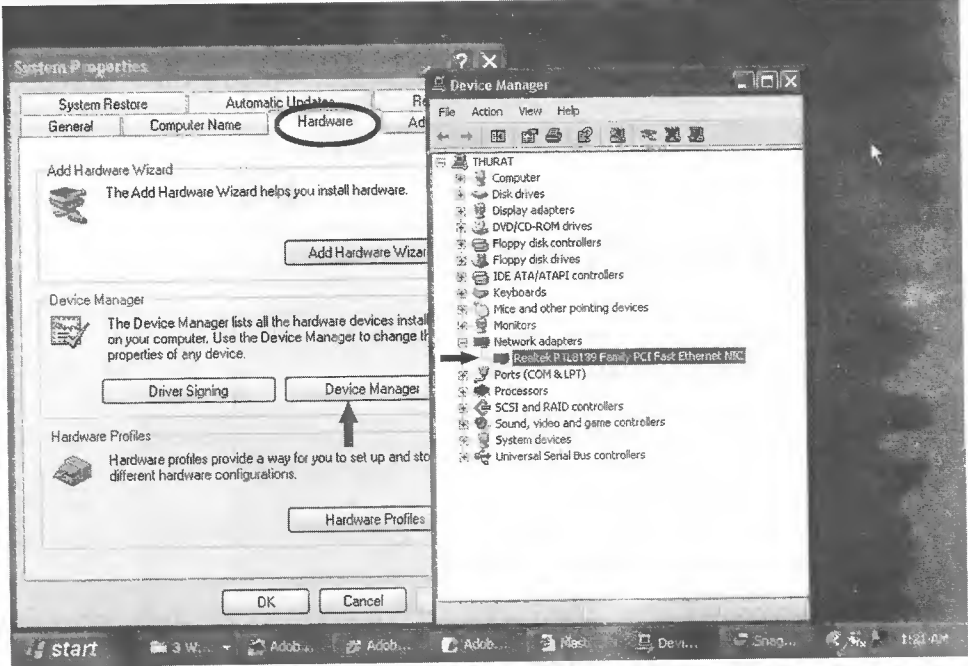
တစ်ခါတလေ ပစ္စည်းတစ်ခုကို ကွန်ပျူတာမှာတပ်ဆင်ပြီးတဲ့အခါမှာ ကောင်းစွာ အလုပ်မလုပ်နိုင်တာမျိုး ကြုံရတတ်ပါတယ်။ အဲဒီလို မိမိကွန်ပျူတာမှာတပ်ဆင်ခဲ့တဲ့ hardware device ပစ္စည်းတွေနှင့် ပတ်သက်ပြီး ပြဿနာ တစ်စုံတစ်ရာရရှိလာပြီဆိုရင် troubleshoot လုပ်ဖို့ အလွယ်ကူဆုံးကတော့ device manager ပင်ဖြစ်ပါတယ်။ device manager ထဲမှာဆိုရင် ကွန်ပျူတာမှာ တပ်ဆင်ထားသမျှသော device အားလုံးရဲ့ information များကို အသေးစိတ်ဖော်ပြထားပါတယ်။ device manager ကို ဖွင့်ရန်အတွက် အောက်ဖော်ပြပါ နည်းလမ်းများထဲမှ တစ်ခုခုကို အသုံးပြုနိုင်ပါတယ်။

Run program ထဲတွင် devmgmt.msc ဟု ရိုက်ထည့်ပြီး enter နှိပ်ပါ။



Desktop ပေါ်ရှိ 'My Computer' icon ပေါ်တွင် right click နှိပ်ပါ။ ကျလာမည့် submenu ထဲရှိ **Properties** တွင် click တစ်ချက်နှိပ်ပါ။ "system properties" dialog box ကျလာပါမည်။

hardware tab အောက်ရှိ **Device Manager** တွင် click နှိပ်ပါ။ device manager window ပွင့်လာပါလိမ့်မည်။



Device Managerတွင်ပစ္စည်းတွေကို category အလိုက်စုစည်းပေးထားပါတယ်။ category တစ်ခု၏ဘေးမှာရှိတဲ့ + သင်္ကေတပေါ်မှာ click နှိပ်မယ်ဆိုရင် အဲဒီ category အောက်မှာရှိသော device ကိုမြင်ရပါလိမ့်မယ်။

Device Manager ထဲတွင် လက်ရှိအချိန်မှာ အလုပ်လုပ်နိုင်ခြင်းမရှိသည့် device တွေကို ဘာကြောင့်အလုပ်မလုပ်နိုင်သလဲဆိုတာကို သိနိုင်စေရန် icon ငယ်ကလေးများဖြင့်ခွဲခြားဖော်ပြထားပါတယ်။ ၎င်း icon တို့၏ အဓိပ္ပာယ်မှာ အောက်ပါအတိုင်းဖြစ်ပါတယ်။

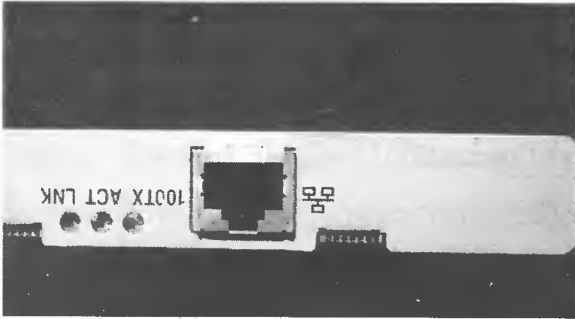
Disable device (x) - Device တစ်ခုသည် ကောင်းမွန်စွာ လုပ်ဆောင်နိုင်သည့် အခြေအနေ တွင်ရှိသော်လည်း အကြောင်းတစ်ခုခုကြောင့် အသုံးပြု၍မရနိုင်အောင် disable လုပ်ထားတဲ့အခါမျိုးမှာ အနီရောင်ကြက်ခြေခတ်ဖြင့် အမှတ်အသားပြုဖော်ပြထားပါလိမ့်မယ်။

Unknown device (?) - Window XP မှ ဘယ်လို device အမျိုးအစားဖြစ်သလဲဆိုတာကို ခွဲခြားမသိနိုင်တဲ့အခါမျိုးမှာ question mark ဖြင့် အမှတ်အသားပြုဖော်ပြထားပါလိမ့်မယ်။

Problem device (!) - Device သည် ကောင်းမွန်မှန်ကန်စွာ လုပ်ဆောင်နိုင်သည့် အခြေအနေကောင်း မရှိသည့်အခါ exclamation mark (!) ဖြင့် အမှတ်အသားပြုဖော်ပြထားပါလိမ့်မည်။

Interpreting LED Indicator

NICတစ်ခုကိုတပ်ဆင်ပြီးစအခါမှာပဲဖြစ်ဖြစ်၊ ရုတ်တရက်အသုံးပြု၍ မရနိုင်တော့တဲ့အခါမှာပဲဖြစ်ဖြစ် NICသည်ကောင်းမွန်စွာလုပ်ဆောင်နေနိုင်သောအခြေအနေတွင်ရှိမရှိဆိုတာကိုအမြင်ဖြင့်လည်းဆုံးဖြတ်နိုင်ကြပါတယ်။ ယနေ့ NIC အများစုတို့တွင် network နှင့် အပြန်အလှန်အဆက်အသွယ် ရှိနေသလား၊ မရှိဘူးလားကို ညွှန်ပြပေးနိုင်တဲ့ LED မီးသီးငယ်များ ပါရှိပါတယ်။ ပါရှိတဲ့ LED အရေအတွက်၊ နေရာနှင့် ဘယ်လိုလင်းရင် ဘာကိုရည်ညွှန်းတယ်ဆိုတာတွေသည် NIC အမျိုးအစားနှင့် ထုတ်လုပ်သော ကုမ္ပဏီပေါ်မူတည်ပြီး ကွဲလွဲမှုတွေရှိပါတယ်။ သို့သော်လည်း အခြေခံသဘောတရားအားဖြင့် အားလုံးအတူတူပင် ဖြစ်ပါတယ်။



ACT - ACT LED မီးသီး မှိတ်တုတ် မှိတ်တုတ်ဖြစ်နေတယ်ဆိုရင် transmit၊ receive လုပ်နေတယ်ဆိုတာကိုရည်ညွှန်းပါတယ်။ activity ရှိနေတဲ့သဘောဖြစ်ပါတယ်။

Link - Link LED မီးလင်းနေခြင်းသည် NIC ကောင်းမွန်စွာလုပ်ဆောင်နေနိုင်တာကိုရည်ညွှန်းပါတယ်။ ဆိုရရင် NIC အတွက် မှန်ကန်တဲ့ driver ကို တင်ပြီး၍ network နှင့်လည်း အဆက်အသွယ် ရပြီဆိုတဲ့သဘောဖြစ်ပါတယ်။

TX - TX LED မှိတ်တုတ်မှိတ်တုတ်ဖြစ်တယ်ဆိုရင် NIC ကောင်းတာသေချာပြီး network ပေါ်သို့ frame တွေပို့နေတယ်လို့ရည်ညွှန်းပါတယ်။

RX - RX LED မှိတ်တုတ်မှိတ်တုတ်ဖြစ်နေတယ်ဆိုရင် NIC ကောင်းမွန်တာသေချာပြီး network ပေါ်မှလာတဲ့ frame တွေကိုလက်ခံယူနေတယ်လို့ရည်ညွှန်းပါတယ်။

Part 2-Configuring Your Network

ကွန်ပျူတာမှာ NIC ကိုကောင်းမွန်မှန်ကန်စွာ install လုပ်ခဲ့ပြီးပြီဆိုရင် ၎င်း NIC နှင့် switch တို့ကို cable ဖြင့်ချိတ်ဆက်ပေးရပါမယ်။ ဤတွင်မှဆက်ပြီး အသုံးပြု၍ ရနိုင်သော network တစ်ခုအဖြစ်သို့ ရရှိအောင် ကွန်ပျူတာမှာ လိုအပ်တဲ့ network setting တွေကို configure လုပ်ပေးရပါမယ်။ configuring ပိုင်းကို နားလည်ထားဖို့ရန်အတွက် အလွန်အရေးကြီးပါတယ်။ configure ဘယ်လိုလုပ်ရသလဲဆိုတာကို နားလည်ထားမှသာလျှင် network တစ်ခုကို မိမိကိုယ်တိုင် တည်ဆောက်နိုင်ကြမှာဖြစ်သလို network အတွင်းမှာ ပြဿနာရှိလာတဲ့အခါမှာလည်း ဘာကြောင့်ဖြစ်ရသလဲဆိုတာကို troubleshoot လုပ်နိုင်ကြမှာ ဖြစ်ပါတယ်။ peer-to-peer network တစ်ခုအတွက် အဓိကအားဖြင့် ကွန်ပျူတာမှာ configure လုပ်စရာ ၂ ပိုင်းရှိပါတယ်။ NIC အတွက် IP address နှင့် ကွန်ပျူတာ အမည်၊ Workgroup အမည်ထည့်သွင်း သတ်မှတ်ပေးခြင်းတို့ဖြစ်ပါတယ်။

Configuring Network Connection (Assign IP Address)

ကွန်ပျူတာမှာ တပ်ဆင်ထားတဲ့ NIC အတွက် လိုအပ်တဲ့ driver ကို install လုပ်ပြီး၍ ကောင်းမွန်စွာ အလုပ်လုပ်နေနိုင်တာ သေချာတဲ့အခါ Windows XP သည် network connection တစ်ခုကို အလိုအလျောက် တည်ဆောက်ပေးပါလိမ့်မယ်။ သို့သော်လည်း မိမိလိုအပ်ချက်နှင့် ကိုက်ညီအောင် ၎င်း network connection ကို ပြန်လည် configure လုပ်ပေးရပါမယ်။ အထူးသဖြင့် NIC အတွက် IP address နှင့် subnet mask တို့ကို မဖြစ်မနေ ပြန်လည်ထည့်သွင်းသတ်မှတ်ပေးရပါမယ်။

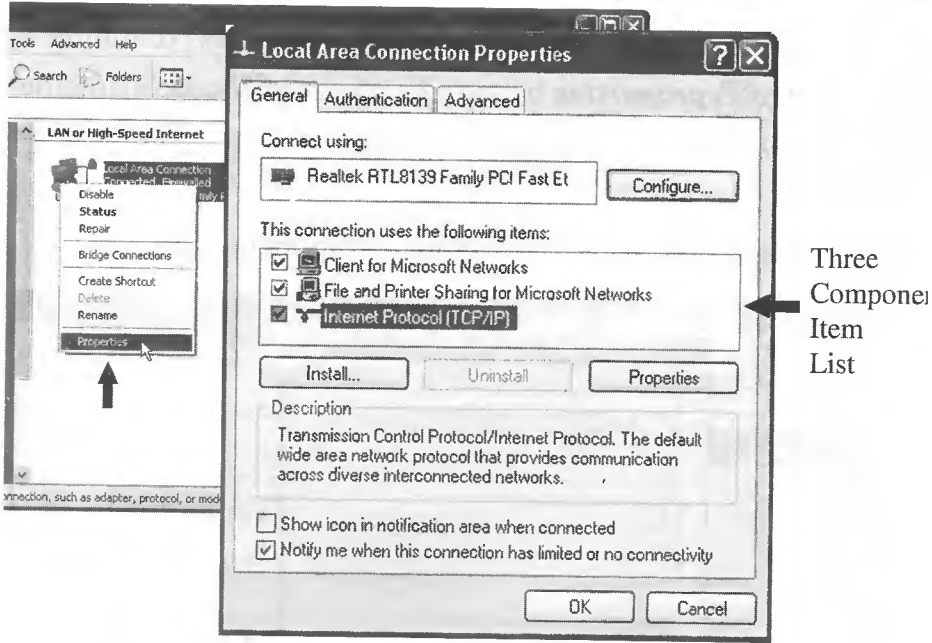
- 1) Start > control panel တွင် click နှိပ်ပါ။ "control panel" windows ပွင့်လာပါလိမ့်မယ်။
- 2) "control panel" ထဲရှိ "network connection" icon တွင် double click နှိပ်ပါ။ "local area connection" အမည်ဖြင့် network connection ကို မြင်ရပါမယ်။



အကယ်၍ local area connection ကို မတွေ့ရပါက ကွန်ပျူတာတွင် တပ်ဆင်ထားသော NIC ကို Windows XP မှ detect မရခြင်းကြောင့်ဖြစ်ပါတယ်။ NIC ကို မှန်ကန်စွာ တပ်ဆင်ထားခြင်းရှိမရှိနှင့် ကောင်းမွန်စွာ အလုပ်လုပ်နိုင်သော အခြေအနေတွင် ရှိမရှိဆိုတာကို စစ်ဆေးဖို့လိုလိမ့်မယ်။

မှတ်ချက်။ ။ desktopပေါ်ရှိ "my network place" icon"တွင် right click နှိပ်ပြီး ကျလာမည့် sub menu ထဲရှိ **properties** တွင် click နှိပ်ပါကလည်း ဒီအဆင့်သို့ ရောက်နိုင်ပါတယ်။

3) "local area connection" တွင် right click နှိပ်ပြီး ကျလာမည့် menu ထဲရှိ **properties** တွင် click နှိပ်ပါက properties dialog box ကျလာပါမည်။



properties dialog box မှာဆိုရင် general ၊ authentication ၊ advanced ဆိုတဲ့ tab သုံးခုပါရှိပါတယ်။ ပုံမှန် default အားဖြင့် properties dialog box ပွင့်လာတိုင်း general tab အောက်က စတင်ဖော်ပြမှာဖြစ်ပါတယ်။

general tab အောက်တွင် Window XP မှ အလိုအလျောက် install လုပ်ထားပေးတဲ့ component item list ပါရှိပါတယ်။ peer-to-peer (workgroup) network တည်ဆောက်ရန်အတွက်တော့ အဲဒီ list ထဲမှာရှိသမျှ item တွေအကုန်လုံးတော့မလိုပါဘူး။ အရေးကြီးတာကတော့ အောက်ဖော်ပြပါသုံးခု ဖြစ်ပါတယ်။

■ Client For Microsoft Network

Microsoft Window Network ကို ချိတ်ဆက်အသုံးပြုမည့်ကွန်ပျူတာတိုင်းမှာ ရှိရပါမယ့် item ဖြစ်ပါတယ်။

■ File and Printer for Microsoft Network

file တွေ၊ printer တွေ sharing လုပ်ပြီး ကွန်ပျူတာတွေ တစ်လုံးနှင့် တစ်လုံး အပြန်အလှန် မျှဝေသုံးစွဲနိုင်ရန် လိုအပ်တဲ့ item ဖြစ်ပါတယ်။

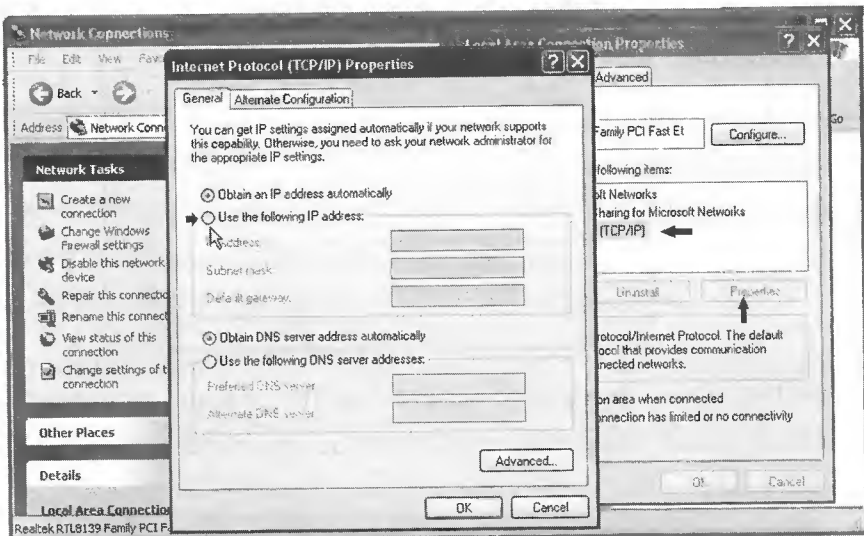
■ Internet Protocol (TCP/IP)

TCP/IP protocol မှတဆင့် အပြန်အလှန် communicate လုပ်ကြမယ့် ကွန်ပျူတာတိုင်းမှာ ရှိရမယ့် item ဖြစ်ပါတယ်။

ဖော်ပြပါ item ခုခုထဲက တစ်ခုခုသည် list ထဲမှာ ရှိမနေဘူးဆိုရင် **install** button တွင် click နှိပ်ပြီး ကိုယ်တိုင် install လုပ်ကြရမှာဖြစ်ပါတယ်။

4) NIC ကို IP address ထည့်သွင်းသတ်မှတ်ရန်အတွက် internet protocol (TCP/IP) တွင် highlight ဖြစ်အောင် select လုပ်ပြီး **properties** button တွင် click တစ်ချက်နှိပ်ရပါမယ်။ (Internet protocol ဘေးရှိ check box တွင် uncheck မလုပ်မီအောင် သတိထားပါ) Internet protocol properties ကျလာပါလိမ့်မည်။

5) Internet protocol properties ထဲမှာဆိုရင် ရွေးချယ်စရာ option ၂ ခုရှိပါတယ်။



A) obtain IP address Automatically

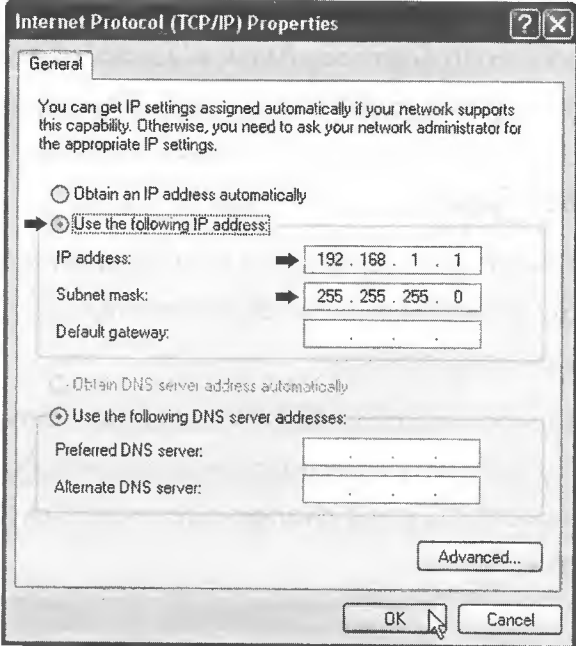
B) Use the following IP address

ပုံမှန်အားဖြင့်ပထမ option A (obtain IP address automatically) ကိုရွေးချယ်ထားပြီးသား ဖြစ်ပါလိမ့်မယ်။ NIC အတွက် IP address ကိုကိုယ်တိုင်ကိုယ်ကျ ထည့်သွင်းနိုင်ရန်အတွက် Use the following ဘေးရှိ radio button ကို click နှိပ်ပြီး ဖြစ်အောင် ရွေးချယ်ရပါမယ်။ အဲဒီလိုရွေးချယ်ပြီးတာနှင့် IP address နှင့် sub-net mask တို့ ထည့်သွင်း ရမယ့်နေရာတွေပေါ်လာပါလိမ့်မယ်။

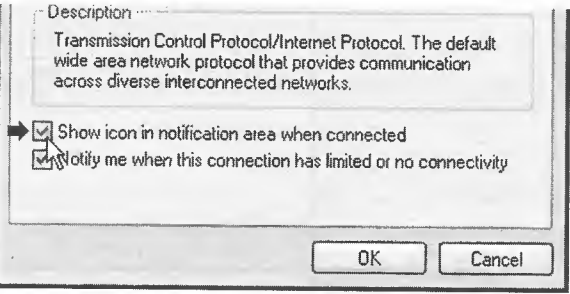
IP address နေရာတွင် မိမိထည့်သွင်းလိုသော Ip address ကို ရိုက်ထည့်ပါ။ IP address အတွက် ဘယ် Network ID၊ host ID သတ်မှတ်မလဲဆိုတာက မိမိရဲ့ ရွေးချယ်မှုဖြစ်ပါတယ်။ ကျန်အခြားသော ကွန်ပျူတာတွေအတွက် သတ်မှတ်တဲ့အခါတွင် ဒီနေရာမှာ ထည့်သွင်းခဲ့တဲ့ IP address နှင့် network ID တူသော host ID မတူသော address ဖြစ်ရပါမယ်။ ဥပမာ ဒီနေရာမှာ 192.168.1.10 ကိုသုံးမယ်ဆိုပါစို့။

ဒါဆိုရင် **192.168.1** သည် network ID ဖြစ်ပြီး **10** သည် host ID ဖြစ်ပါတယ်။ ကျန်ကွန်ပျူတာတွေ အတွက် IP address သတ်မှတ်တဲ့နေရာတွင် ရှေ့က **192.168.1** ဖြင့်စရပါမယ်။ နောက်ဆုံးဂဏန်း (host ID) အတွက်ကတော့ **1** မှ **254** အတွင်း တစ်လုံးနှင့်တစ်လုံး မတူနိုင်တဲ့ဂဏန်းမျိုးဖြစ်ရပါမယ်။

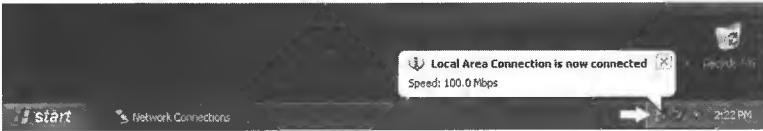
IP address ကိုထည့်သွင်းပြီးပါက subnet mask ထည့်သွင်းရမည့်နေရာတွင် cursor (mouse pointer) ချလိုက်ပါ။ မိမိထည့်သွင်းလိုက်တဲ့ IP address ၏ class ပေါ်အခြေခံပြီး Window XP မှ subnet mask ကိုအလိုအလျောက် ထည့်သွင်းပေးပါလိမ့်မယ်။ ဒီနေရာမှာတော့ IP address သည် class C ဖြစ်သည့်အတွက် subnet mask **255.255.255.0** ကိုအလိုအလျောက် ထည့်သွင်းပေးပါလိမ့်မယ်။



6) IP address ထည့်သွင်းခဲ့ပြီးပြီဆိုရင် **OK** button တွင် click တစ်ချက်နှိပ်ပါက "internet protocol" box ပျောက်သွားပြီး မူလ Local Area Connection သို့ပြန်ရောက်ပါလိမ့်မယ်။ ဒီ "Local Area Connection" dialog box ထဲရှိ **Show icon in notification** ဘေးတွင် check လုပ်ခဲ့မည်ဆိုပါက မိမိကွန်ပျူတာသည် network နှင့်ချိတ်ဆက်နေခြင်းရှိမရှိဆိုတာကို အလွယ်တကူ သိစေနိုင်ပါလိမ့်မယ်။



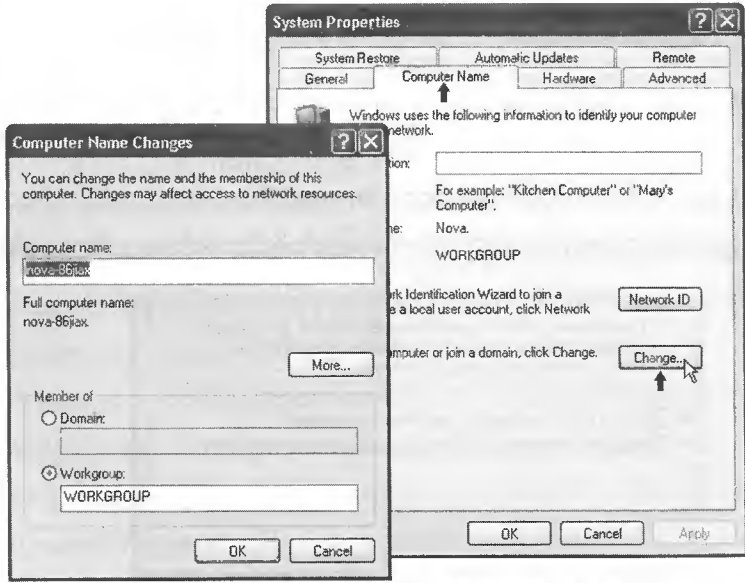
7) OK buttonတွင် click နှိပ်ပါက local area connection box ပျောက်သွားပြီး system tray ထဲတွင် "network connection" icon ကို မြင်ရပါလိမ့်မယ်။



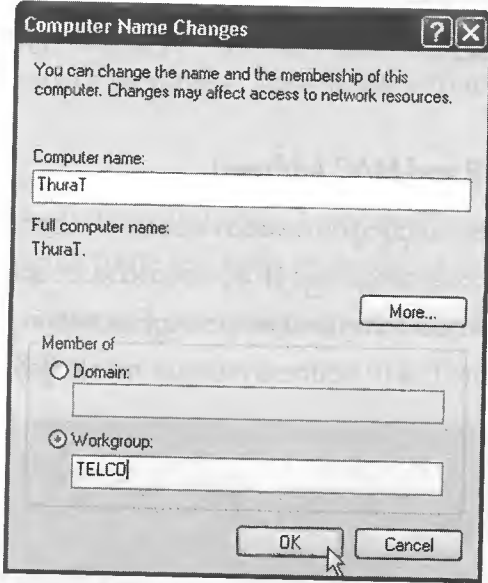
● Configuring Computer and Workgroup Name

Network တွင်းမှာရှိတဲ့ ကွန်ပျူတာတိုင်းတွင် အလွယ်တကူခွဲခြားနိုင်မယ့် ကိုယ်ပိုင်အမည်တစ်ခုစီ ရှိရပါမယ်။ workgroup ဆိုတာကတော့ ကွန်ပျူတာတွေကို logically အရအုပ်စုဖွဲ့ထားခြင်းမျိုး ဖြစ်ပါတယ်။ workgroup name မတူတဲ့ ကွန်ပျူတာတွေသည် တစ်လုံးနှင့် တစ်လုံးမမြင်နိုင်ကြပါဘူး။ ဒါ့ကြောင့် network တခုထဲမှာရှိတဲ့ ကွန်ပျူတာတွေသည် workgroup name တူရပါမယ်။ computer name ကတော့ ကိုယ်ပိုင်သီးခြား အမည်တစ်ခုစီဖြစ်ကြရပါမယ်။

- 1) desktop ပေါ်ရှိ "my computer" icon တွင် right click နှိပ်ပါ (သို့) start menu ထဲရှိ my computer တွင် right click နှိပ်ပါ။ ကျလာမည့် sub menu ထဲရှိ **properties** တွင် click တစ်ချက်နှိပ်ပါ။ "system properties" dialog box ပွင့်လာပါမည်။
- 2) "Computer Name" tab တွင် click တစ်ချက်နှိပ်ပါ။ full computer name နှင့် workgroup တို့နေရာတွင် Window XP မှ အလိုအလျောက်ထည့်သွင်းပေးထားသော အမည်များကို မြင်ရပါမယ်။ ကွန်ပျူတာနှင့် workgroup အမည်တို့ကို ပြောင်းရန် **change** button တွင် click နှိပ်ပါ။ "computer name change" box ကျလာပါမည်။



3) computer name နေရာတွင် ပေးလိုတဲ့ အမည်တစ်ခုကို ရိုက်ထည့်ပါ။ workgroup ဘေးရှိ radio button တွင် ဖြစ်အောင် select လုပ်ပြီး workgroup အမည်ကို ရိုက်ထည့်ပါ။ အမည်များကို ထည့်သွင်းခဲ့ပြီးပြီဆိုရင် OK button တွင် click နှိပ်ပါက ကွန်ပျူတာမှ reboot လုပ်ရန် တောင်းဆိုပါလိမ့်မယ်။ ပြုပြင်ပြောင်းလဲခဲ့သမျှ သက်ရောက်မှုရှိရန် **OK** button တွင် click နှိပ်ပြီး reboot လုပ်လိုက်ပါ။

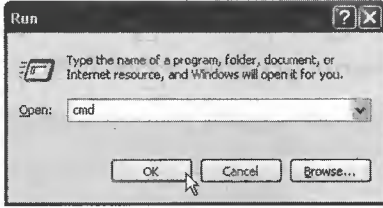


ဒါဆိုရင် network ချိတ်ဆက်ခြင်းအတွက် လိုအပ်တဲ့ setting တွေကို configure လုပ်ခဲ့ပြီးပြီလို့ ဆိုနိုင်ပါပြီ။ ကျန်ကွန်ပျူတာတွေမှာလည်း ဖော်ပြခဲ့တဲ့ configuration အဆင့်များအတိုင်း လုပ်ဆောင်ခြင်းဖြင့် peer-to-peer network တစ်ခုတည်ဆောက်ခြင်းပြီးဆုံးပါလိမ့်မယ်။

Part 3-Testing your Computer Connectivity

Network အတွင်းမှာရှိတဲ့ ကွန်ပျူတာတို့အတွက် IP address တွေထည့်သွင်းခဲ့ပြီးပြီ လိုအပ်တဲ့ network setting တွေကိုလည်း configure လုပ်ခဲ့ပြီးပြီဆိုရင် ကွန်ပျူတာတွေတစ်လုံးနှင့် တစ်လုံး အပြန်အလှန် communicate လုပ်နိုင်သင့်ပါပြီ။ အဲဒီလိုကောင်းမွန်စွာ လုပ်ဆောင်နိုင်တဲ့ အခြေအနေ ရှိမရှိနှင့် ထည့်သွင်းထားသော network setting တို့မှန်မမှန် ပြန်လည်စစ်ဆေးခြင်းများကို Window Xp တွင် built-in ပါရှိပြီးသား tools ၂ခုတို့ဖြင့် လုပ်ဆောင်နိုင်ကြပါတယ်။ ၎င်း tools ၂ခုတို့မှာ IPCONFIG နှင့် PING တို့ဖြစ်ပါတယ်။ ထို tools ၂ခုတို့ကို အသုံးပြုနိုင်ရန်အတွက် ပထမဦးစွာ command window ကို အရင် ဖွင့်ရပါမယ်။

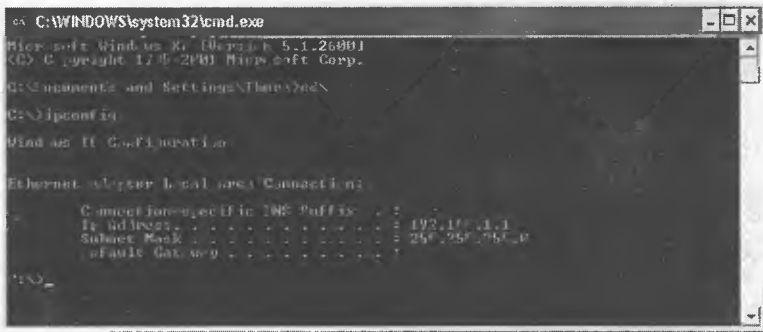
1) start > run တွင် click တစ်ချက်နှိပ်ပါ။ run program ပွင့်လာပါလိမ့်မယ်။ (Keyboard မှ windows key နှင့် R ကို တွဲနှိပ်ခြင်းဖြင့်လည်း run program ကိုဖွင့်နိုင်ပါတယ်။)



2) openနေရာတွင် **cmd** ဟုရိုက်ထည့်ပြီး Enter key နှိပ်ပါ။ အနက်ရောင်နောက်ခံဖြင့် command window ပွင့်လာပါလိမ့်မယ်။

● **IPCONFIG (Finding Your IP and MAC Address)**

ipconfig သည် ကွန်ပျူတာမှာထည့်သွင်းထားသော network configuring များကို ဖော်ပြပေးနိုင်သော tools တစ်ခုဖြစ်ပါတယ်။ အထူးသဖြင့် IP နှင့် ပါတ်ဘက်သော အချက်အလက်များကို ကြည့်ရှုစစ်ဆေးတဲ့နေရာမှာပိုအသုံးများပါတယ်။ command window တွင် ipconfig ဟုရိုက်ထည့်ပြီး Enter ကိုနှိပ်ပါ။ ကွန်ပျူတာမှာတပ်ဆင်ထားတဲ့ NIC ၏ IP address ၊ subnet mask တို့ကို မြင်ရပါမယ်။



ipconfig နောက်မှာ switch တွေပေါင်းစပ်အသုံးပြုမယ်ဆိုရင် ပိုမိုပြည့်စုံသော information တွေကို ထုတ်ပေးပါလိမ့်မယ်။ **ipconfig /?** ဟု ရိုက်ထည့်ပါက ipconfig နောက်မှာ ပေါင်းစပ်အသုံးနိုင်တဲ့ switch တွေကိုဖော်ပြပါလိမ့်မယ်။ ဥပမာ **ipconfig /all** ဟုရိုက်ထည့်ပါက IP information တို့အပြင် MAC address၊ host name၊ workgroup name အစရှိသော network configuration အပြည့်အစုံ ကိုဖော်ပြပါလိမ့်မယ်။

● **PING (Packet Internet Groper)**

PING သည် network connectivity ကို စစ်ဆေးရန်အတွက် အသုံးအများဆုံး tools တစ်ခုဖြစ်ပါတယ်။ ping တဲ့အခါ IP address (သို့) host name ကိုလှမ်း ping နိုင်ပါတယ်။

- ဥပမာ - ping 192.168.1.10 (IP Address)
- ping thurat (Host name)

အထူးသဖြင့်မိမိကွန်ပျူတာသည် network ပေါ်ရှိအခြားကွန်ပျူတာတို့နှင့်အပြန်အလှန် communicate လုပ်နိုင်သော အခြေအနေတွင်ရှိမရှိဆိုတာကို စစ်ဆေးရာတွင် သုံးကြပါတယ်။ အခြားကွန်ပျူတာ တစ်လုံးလုံးသို့ ping လိုက်တဲ့အခါ မိမိကွန်ပျူတာမှ request signal များသည် တဖက် ကွန်ပျူတာသို့ ရောက်ရှိသွားပါတယ်။ တဖက်ကွန်ပျူတာသည် လက်ခံရရှိလာသော request signal ထဲတွင်ပါလာသည့် source code လို့ခေါ်သည့် လိပ်စာကို ဖတ်ပြီးမှသာ ဘယ်ကွန်ပျူတာမှ request လုပ်သလဲဆိုတာကို သိနိုင်ပါတယ်။ ဤတွင်မှထိုကွန်ပျူတာထံသို့မိမိရှိနေကြောင်းကို reply ပြန်ပို့ပေးနိုင်ပါတယ်။ အဲဒီပြန်ပို့လိုက်တဲ့ message ထဲတွင် reply from time | TTL အစရှိတဲ့ information တွေမြင်ရပါလိမ့်မယ်။

Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128
Reply from 192.168.1.1: bytes=32 time<1ms TTL=128

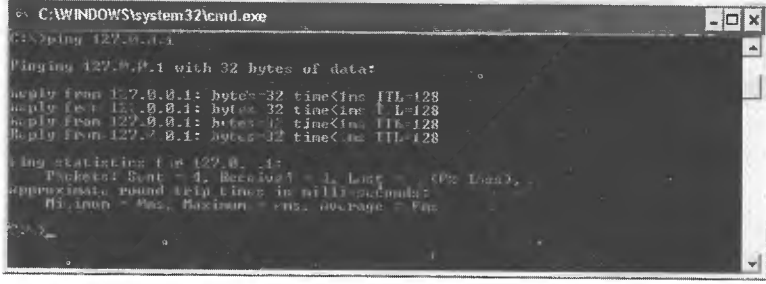
အကယ်၍ တနေရာရာမှ ချွတ်ယွင်းချက်ကြောင့် reply မပြန်နိုင်တဲ့အခါ request time out ဆိုတာကိုတွေ့ရပါလိမ့်မယ်။

Request timed out.
Request timed out.
Request timed out.

PING ကိုအသုံးပြုပြီး အောက်ဖော်ပြပါအဆင့်များအတိုင်း စစ်ဆေးနိုင်ကြပါတယ်။

1) loopback address (127.0.0.1) ကို ping ကြည့်ခြင်းအားဖြင့် မိမိကွန်ပျူတာမှ network adapter သည် ကောင်းမွန်စွာလုပ်ဆောင်နိုင်ခြင်း ရှိမရှိဆိုတာကို သိနိုင်ပါတယ်။ မည်သည့်ကွန်ပျူတာအတွက်မဆို ဒီ loopback address (127.0.0.1) သည်ပုံသေဖြစ်ပါတယ်။

ping 127.0.0.1



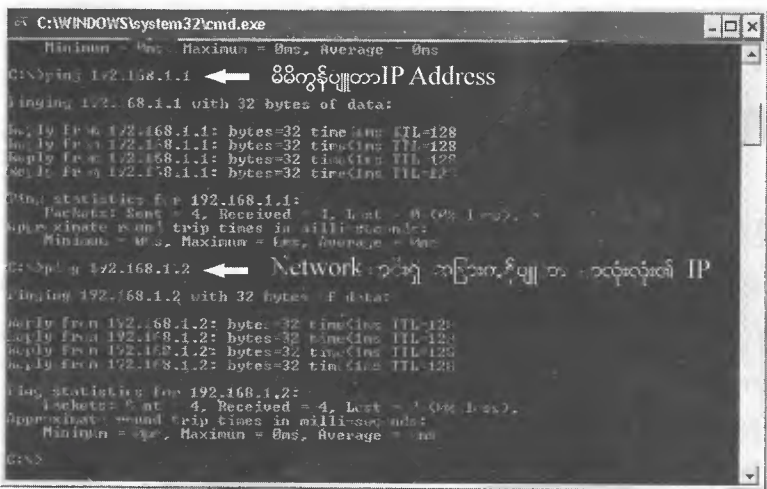
NIC ချွတ်ယွင်းချက်ရှိနေချိန်နှင့် driver file တွေပျက်သွားတဲ့အခါမျိုးမှသာ request time out ဖြစ်တတ်ပါတယ်။

2) မိမိကွန်ပျူတာ IP addressကို ping ကြည့်ရပါမယ်။

ဥပမာ - ping 192.168.1.1

စစ်ဆေးမှုမအောင်မြင်ဘူး(ဝါ) reply မပြန်နိုင်ဘူး ဆိုရင် ပထမဦးစွာ NIC မှာရှိတဲ့ LED မီးများ လင်းမလင်းဆိုတာကို စစ်ဆေးပါ။ LED မီးလင်းရဲ့သားနှင့်မှ reply မပြန်နိုင်ဘူးဆိုရင် Window ထဲမှာ network connectionကို disable ထုတ်ထားမိတာမျိုးလည်း ဖြစ်နေတတ်ပါတယ်။ device managerထဲရှိ network adapterကို စစ်ဆေးပါ။ အနီရောင်ကြက်ခြေခတ်ရှိနေပါက disable လုပ်ထားခြင်း ဖြစ်ပါတယ်။ (စာ-၁၃၂ကိုရှုပါ) adapterပေါ်တွင် right-click နှိပ်ပြီး enable ပြန်လုပ်လိုက်ရုံဖြစ်ပါတယ်။ enable/disable ကြောင့်မဟုတ်ဘူးဆိုရင် NIC ၊ cable ၊ switch တို့ကို ပြန်လည်စစ်ဆေးဖို့လိုပါမယ်။

3) network ထဲရှိအခြား ကွန်ပျူတာ (remote computer) တစ်လုံး၏ IP address ကို လှမ်း ping ကြည့်ပါ။ reply ပြန်ရတယ်ဆိုရင် ၎င်း ကွန်ပျူတာနှင့် မိမိတို့ကြားမှာ connectivity ပိုင်းနှင့် ပတ်သက်ပြီး ပြဿနာမရှိဘူးလို့ဆိုနိုင်ပါပြီ။



Wireless Network

Ethernet network တွေအသုံးပြုမှုတွင်ကျယ်နေသလိုပင် အခြားတဖက်မှာလည်း wireless network တွေကို လူကြိုက်များလာလျက်ရှိနေပါတယ်။ wireless network တွေကို တည်ဆောက်တဲ့ နေရာမှာ wire network တွေထက်ပိုမိုလွယ်ကူပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ သာမန်အိမ်သုံး၊ ရုံးသုံး wireless network တစ်ခုတည်ဆောက်ရန်အတွက် ပစ္စည်းပစ္စယများစွာမလိုပါဘူး။ wireless access point (wap) နှင့် wireless NIC ဆိုတဲ့ အဓိက ပစ္စည်း ဖျိုးသာလိုအပ်ပါတယ်။ ဒါကြောင့် wireless network တစ်ခုတည်ဆောက်ရန်အတွက် အခြေခံအကျဆုံး ဒီပစ္စည်း ဖျိုးအကြောင်းကိုတော့ သိထားဖို့လိုလိမ့်မယ်။

WAP (Wireless Access Point)

Wire network တစ်ခုတည်ဆောက်ရန်အတွက် ကွန်ပျူတာတွေ အတူတကွပဟိုပြုချိတ်ဆက် ကြရတဲ့ switch၊ hub တို့ရဲ့အခန်းကဏ္ဍသည် အလွန်အရေးကြီးပါတယ်။ ထိုနည်းတူစွာပင် wireless network တွေမှာလည်း ကွန်ပျူတာတွေအတူတကွပဟိုပြုဆက်သွယ်ကြရတဲ့ central device တစ်ခုလိုပါတယ်။ ၎င်း central device သည် WAP ပင်ဖြစ်ပြီး သူ၏လုပ်ဆောင်မှုသည်လည်း hub တစ်ခုကဲ့သို့ပင်ဖြစ်ပါတယ်။

WAP တစ်ခုမှာ အနည်းဆုံး အင်တင်နာ တစ်ချောင်း (အချို့တွင် ၂ ချောင်း) နှင့် wire network ဆီသို့ ချိတ်ဆက်အသုံးပြုနိုင်စေရန်အတွက် RJ-45 port တစ်ခုပါလေ့ရှိပါတယ်။ အောက်ဖော်ပြပါပုံ (13.1) ကတော့ WAP တစ်ခုရဲ့ပုံဖြစ်ပါတယ်။

ပုံ (13.1)



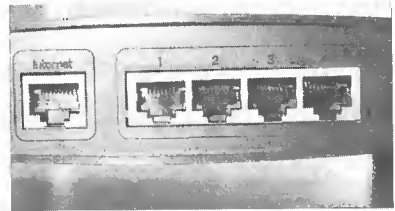
Wireless Router

WAP ကတော့ WAP ဝဲ။ ဒါပေမယ့် သူထဲမှာ router function ပါတယ်ဆိုရင် wireless router လို့ခေါ်ပါတယ်။ wire ဖြင့်ဖြစ်စေ၊ wireless ဖြင့်ဖြစ်စေ အင်တာနက်ချိတ်ဆက်တဲ့နေရာတွေမှာ အသုံးပြုနိုင်ပါတယ်။ ၎င်း wireless router အများစုတို့ရဲ့နောက်ဖက်မှာ ကွန်ပျူတာချိတ်ဆက်တပ်ဆင်နိုင်တဲ့

switch တစ်ခုပါတတ်ပါတယ်။ wireless NIC မရှိတဲ့ ကွန်ပျူတာ တစ်လုံးကို ဒီ port မှာ တိုက်ရိုက် တပ်ဆင် အသုံးပြုနိုင်ကြပါတယ်။ wire cat5 ဖြင့် အသုံးပြုနိုင်မယ့် ကွန်ပျူတာတွေနှင့် WAP နှင့် ဘယ်လောက်ဝေးဝေး နေရာထိ သယ်ဆောင်အသုံးပြုနိုင်မလဲဆိုတာကတော့ WAP နှင့် wireless NIC တို့၏ standard (ဥပမာ 802.11a, 802.11b) ပေါ်မူတည်ပါလိမ့်မယ်။ပုံ (13.2)



Front View

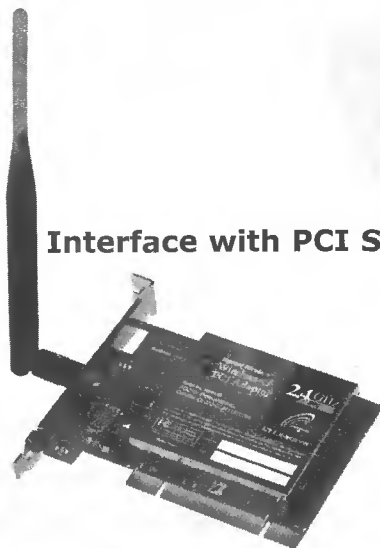


Back View

ပုံ (13.2)

● Wireless NIC

Wireless network တွင်းမှာ အသုံးပြုလိုတဲ့ မည်သည့် device မဆို wireless NIC တစ်ခုလိုပါတယ်။ အင်တီနာ တစ်ခုပါတာကလွဲရင် wireless NIC တွေသည်လည်း wire network တွေမှာ သုံးနေကြပုံမှန် NIC တို့လိုပင်ဖြစ်ပါတယ်။ တပ်ဆင်အသုံးပြုမယ့်ပေါ်မူတည်ပြီး အဓိကအားဖြင့် wireless NIC သုံးမျိုးရှိပါတယ်။ desk top ကွန်ပျူတာတွေအတွက် PIC card၊ desktop နှင့် laptop နှစ်မျိုးစလုံးမှသုံးနိုင်တဲ့ USB adapter ၊ laptop မှာသာသုံးနိုင်တဲ့ PC card တို့ဖြစ်ပါတယ်။ပုံ (13.3)

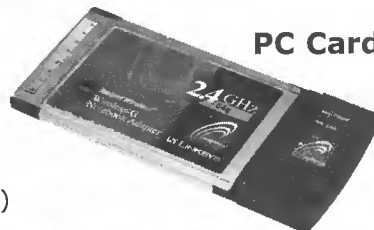


Interface with PCI Slot

USB Adapter



PC Card



ပုံ (13.3)

📶 Wireless LAN standard

Wireless နှင့်ပတ်သက်သောပထမဆုံး standard ကို 1997 တွင် IEEE မှအတည်ပြုသတ်မှတ်ခဲ့ပါတယ်။ အဲဒီမူလ wireless standard ကတော့ 802.11 ဝဲဖြစ်ပါတယ်။ 802.11 ရယ်လို့စတင်စဉ်က bandwidth သည် 2Mbps သာရှိပြီး အသုံးပြုသော frequency မှာ 2.4 GHz ဖြစ်ပါတယ်။ အဲဒီကာလနောက်ပိုင်း wireless နည်းပညာ တွေပိုမို ဖွံ့ဖြိုးလာခြင်းနှင့် အတူ standard သစ်များစွာ ထပ်မံထွက်ပေါ်လာခဲ့ပါတယ်။ ယနေ့အသုံးအများဆုံး 802.11 standard သုံးမျိုးရှိပါတယ်။ ၎င်းတို့မှာ IEEE 802.11a၊ 802.11b၊ 802.11g တို့ဖြစ်ပါတယ်။

📶 802.11a

802.11a သည်အခြား standard ၂ခုဖြစ်တဲ့ 802.11b၊ 802.11g တို့နှင့်မတူပဲတူမူကွဲပါတယ်။ အဓိကမတူတဲ့အချက်က frequency ဖြစ်ပါတယ်။ 802.11b နှင့် 802.11g တို့သည် 2.4GHz ကိုအသုံးပြုပြီး 802.11g ကတော့ 5GHz ကိုအသုံးပြုလုပ်ဆောင်ပါတယ်။ frequency မြင့်ခြင်းရဲ့အားသာချက်ကတော့ 802.11a standard အသုံးပြုထားတဲ့ network တွေသည် မိုက်ကရိုဝေ့မီးဖို၊ လက်ကိုင်ဖုန်း၊ မော်တာအစရှိတဲ့ ပြင်ပပတ်ဝန်းကျင်ရှိ အီလက်ထရောနစ် ပစ္စည်းတို့၏ နောက်ယှက်ခြင်းများရဲ့ဒဏ်ကို အခြား 802.11b၊ 802.11g တို့လောက်မခံရပါဘူး။ ဒါပေမယ့် high frequency ကို transmit လုပ်ဖို့ရန် ပါဝါပိုသုံးရခြင်းနှင့် lower frequency (2.4 GHz) တွေလောက် ဝေးဝေးသို့ transmit မလုပ်နိုင်ခြင်းစတဲ့ အားနည်းချက်တွေလည်းရှိပါတယ်။ 802.11a အင်တီနာသည် 20m (66ပေ) ထိသာ transmit လုပ်နိုင်ပါတယ်။ သဘောက ကွန်ပျူတာနှင့် WAP တို့သည် 20m အတွင်းသာ ရှိရမယ်ဆိုတာကိုရည်ညွှန်းပါတယ်။ သီအိုရီအရ 802.11a ၏ maximum data rate သည် 54 Mbps ဖြစ်ပြီး တကယ့်လက်တွေ့မှာတော့ 11 မှ 18Mbps အတွင်းသာ ဖြစ်ပါတယ်။

📶 802.11b

802.11b ကို IEEE မှ 1999 တွင် အတည်ပြုသတ်မှတ်ခဲ့ပါတယ်။ ၎င်း standard ကို wifi (wireless fidelity) ဟုလည်းလူသိများပါတယ်။ အသုံးပြုသော frequency မှာမူလ 802.11 standard အတိုင်း 2.4 GHz ဖြစ်ပါတယ်။ maximum data rate သည် သီအိုရီအရ 11Mbps ရှိပါတယ်။ ဒါပေမယ့် တကယ့်လက်တွေ့မှာတော့ 5Mbps ဝန်းကျင်ခန့်သာ ရရှိပါလိမ့်မယ်။ ဒါတောင်မှတို data rate ကို ရရှိရန် ကွန်ပျူတာနှင့် WAP တို့အကွာအဝေးသည် 30m (100ft) အတွင်း ရှိဖို့လိုပါတယ်။

📶 802.11g

802.11g သည် သီအိုရီအရ maximum data rate ကို 54Mbps ထိရရှိအောင် ပုံစံထုတ်ထားသော 802.11b လို့တောင်ဆိုနိုင်ပါတယ်။ တကယ့်လက်တွေ့မှာတော့ data rate သည် 20 နှင့် 25 Mbps ကြားရရှိနိုင်ပါတယ်။ 802.11b ကဲ့သို့ပင် 2.4 GHz ကိုအသုံးပြုပြီး အင်တီနာ၏ geographic range သည်လည်း 30m ပင်ဖြစ်ပါတယ်။ data rate မြင့်ရုံသာမက 802.11b network တို့မှာလည်း တွဲဖက်အသုံးပြုနိုင်သည့်

အတွက် လူသုံးများပါတယ်။ ဆိုရရင် 802.11b WAP အသုံးပြုထားတဲ့ network မှာ 802.11g NIC ကို တပ်ဆင်အသုံးပြုနိုင်ပါတယ်။

Wireless LAN Standards

Standard	Max Throughput	Encoding Scheme	Frequency Band(s)	Typical Max Range (Indoors)	Typical Max Range (outdoors)
Bluetooth	1Mbps	FHSS	2.4GHz	328ft/100m	N/A
802.11	1-2Mbps	FHSS/DSSS	2.4GHz	328ft/100m	1500ft/457m
802.11a	54Mbps	OFDM	5GHz	250ft/76m	1000ft/305m
802.11b	11Mbps	DSSS	2.4GHz	328ft/100m	1500ft/457m
802.11g	54Mbps	OFDM/DSSS	2.4GHz	328ft/100m	1500ft/457m

Wireless Access Method

Wireless network တွေသည် sending နှင့် receiving ကို တစ်ပြိုင်နက် မလုပ်နိုင်ကြသည့်အတွက် collision ဖြစ်ခြင်းမှရှောင်ရှားနိုင်အောင် wireless medium ပေါ်မှာမည်သည့် signal မှ မရှိပဲ လုံးဝကင်းရှင်းသည်ကို သေချာအောင် အချိန်တစ်ခုစောင့်ဆိုင်းပြီးမှ ပေးပို့ခြင်းဟူသော method ဖြင့် collision မဖြစ်အောင် ကြိုးစားကြရပါတယ်။ ၎င်း method သည် wire network (802.3) တွေမှာ အသုံးပြုသည့် CSMA/CD နှင့် မတူပဲ တူမူကွဲသည့် CSMA/CA (Collision Avoidance) ပင်ဖြစ်ပါတယ်။

CSMA/CA ကို အသုံးပြုသော ကွန်ပျူတာတွေသည် data မပို့ခင် network medium ကို အခြားကွန်ပျူတာ (သို့) device များမှ အသုံးချနေမှု ရှိမရှိဆိုတာကို ဦးစွာပထမစစ်ဆေးရပါတယ်။ ပေးပို့မည့် ကွန်ပျူတာ အနေနှင့် medium မအားသေးလို့ပါလို့ထောက်လှမ်းသိရှိမယ်ဆိုရင် အချိန် တစ်ခု (random) စောင့်ဆိုင်းပြီး အားမအားဆိုတာကို နောက်တကြိမ် ထပ်မံစစ်ဆေးရပါမယ်။ နောက်တစ်ကြိမ် ထပ်မံစစ်ဆေးလို့ network ပေါ်မှာမည်သည့်လှုပ်ရှားမှုမရှိပဲ အားနေတယ်လို့ထောက်လှမ်းသိရှိတယ်ဆိုလျှင် တောင်မှ ချက်ချင်း မပို့သေးပဲ အချိန်တစ်ခုစောင့်ဆိုင်းရပါတယ်။ ပြီးမှ ပို့လိုသမျှကို ပို့ရပါတယ်။

တစ်ဖက်လက်ခံ ရယူသည့် ကွန်ပျူတာအနေနှင့်လည်း ပေးပို့လိုက်သမျှ ပြုဆိုရင် ACK packet တစ်ခုကို မူလပေးပို့သူ source ကွန်ပျူတာထံသို့ ပြန်ပို့ပေးရပါတယ်။ အဲဒီ ACK packet ကို ရမှသာ source ကွန်ပျူတာအနေနှင့် မိမိပို့လိုက်သမျှ အားလုံးရည်ရွယ်ရာ destination ကွန်ပျူတာ ဆီ အောင်အောင်မြင်မြင် ရောက်ရှိပါတယ်လို့ မှတ်ယူပါလိမ့်မယ်။ အကယ်၍ ACK packet ကို မရခဲ့ဘူးဆိုရင် ပေးပို့မှု မအောင်မြင်ဟု မှတ်ယူကာ CSMA/CA process ကို နောက်တစ်ကြိမ် အစအဆုံး လုပ်ဆောင်ပါလိမ့်မယ်။

data ပေးပို့မှု အောင်မြင်ကြောင်းကို အတည်ပြုပေးနိုင်ရန် ACK packet တွေကို အသုံးပြုမှုသည် wire network (802.3) တို့နှင့် ယှဉ်လျှင် wireless network (802.11) တွေမှာ ပိုများပါတယ်။ ဒါကြောင့် သီအိုရီအရ တွက်ထုတ်ထားတဲ့ maximum data rate ချင်း တူသော်လည်း တကယ်လက်တွေ့ သုံးတဲ့ နေရာမှာတော့ wireless network တွေသည် wire network တွေလောက် အနီးစပ်ဆုံး မရနိုင်ပါဘူး။

ဆိုရင် wirelessထဲမှာ အမြန်ဆုံး standardဖြစ်တဲ့ 802.11g ၏ maximum data rateသည် 54 Mbps ဖြစ်ပါတယ်။ ဒါပေမယ့် တကယ့်လက်တွေ့သုံးတဲ့အခါမှာတော့ 802.11g network တစ်ခု၏ data rate သည် 20 မှ 25 Mbps အတွင်းသာ ရှိပါတယ်။

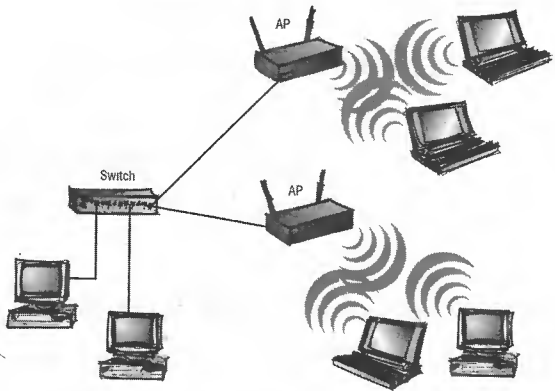
Wireless LAN Architecture

Wireless network တို့တွင် အခြေခံအကျဆုံးတည်ဆောက်ပုံနှစ်မျိုးရှိပါတယ်။ Ad-hoc နှင့် infrastructure mode တို့ပဲဖြစ်ပါတယ်။ Ad-hoc ဆိုတာက wireless router ၊ wap (wireless access point) တို့မပါဘဲ တည်ဆောက်ထားသည့် network ဖြစ်ပါတယ်။ သဘောကြားခံမလိုဘဲ wireless NIC တစ်ခုစီတပ်ထားတဲ့ ကွန်ပျူတာတွေ တစ်လုံးနှင့်တစ်လုံး တိုက်ရိုက်ဆက်သွယ်လုပ်ဆောင်ကြတဲ့ network ဖြစ်ပါတယ်။



ပုံ (13.5) Ad-Hoc Network

Ad-hoc မှာလိုကွန်ပျူတာတွေ တိုက်ရိုက်ဆက်သွယ်လုပ်ဆောင်ခြင်းမဟုတ်ဘဲ wireless router ၊ wap တို့ကိုကြားခံအသုံးပြုဆက်သွယ်ကြတယ်ဆိုရင် infrastructure mode လို့ခေါ်ပါတယ်။ infrastructure mode မှာဆိုရင် အနည်းဆုံး wap တစ်ခုပါရှိပါတယ်။ Ap သည် wire network နှင့် wireless network တို့ကိုကြားခံဆက်သွယ်ပေးနိုင်တဲ့ device တစ်ခုလည်းဖြစ်ပါတယ်။ အောက်ဖော်ပြ ပုံ (13.6) ကတော့ AP ၂ ခုပါတဲ့ infra mode LAN တစ်ခုရဲ့ပုံပဲဖြစ်ပါတယ်။



ပုံ (13.6) Infra Mode Network

Ad-hocသည်ကွန်ပျူတာအရေအတွက်လည်းနည်းမယ်၊တစ်လုံးနှင့်တစ်လုံးလည်းနီးနီးကပ်ကပ်ရှိနေနိုင်တဲ့ သာမန် network ငယ်တွေ အတွက်သာသင့်တော်ပါတယ်။ ကွန်ပျူတာအရေအတွက်လည်းများမယ်၊ အကွာအဝေးပိုမိုရောက်ရှိအောင် ထားရှိအသုံးပြုလိုတဲ့ အခါမျိုးမှာ AP တွေထပ်တိုးတပ်ဆင်၍ network ရေယာအကျယ်အဝန်းကို ချဲ့ထွင်အသုံးပြုနိုင်ကြပါတယ်။ ဒါကြောင့်အသုံးပြုသူများပြီးအတော်အတန်ကြီးသည့် network မျိုးတွေအတွက် infra mode LAN တွေသည် အသင့်တော်ဆုံးဖြစ်ပါတယ်။ သို့သော်အခြားတစ်ဖက်ကကြည့်မယ်ဆိုရင်တော့ Ad-hoc network တစ်ခုတည်ဆောက်ရန် ဈေးပိုကြီးတဲ့ WAP တို့မလိုဘဲ wireless NIC တစ်ခုစီသာရှိဖို့လိုတဲ့အတွက်ကုန်ကျစရိတ်အကျဉ်းဆုံး WLAN အမျိုးအစားဖြစ်ပါတယ်။ ဒါ့အပြင် Ad-hoc LAN တစ်ခုအဖြစ်သို့လုပ်ဆောင်တဲ့နေရာမှာများစွာ အခက်အခဲမရှိပဲအလွယ်တကူ setup လုပ်နိုင်ကြပါတယ်။

◆ Making the Ad-hoc LAN

Ad-hoc network တစ်ခုတည်ဆောက်ရန်အတွက်ပထမဦးဆုံးလိုအပ်ချက်ကတော့ကွန်ပျူတာတိုင်းတွင် wireless NIC တစ်ခုစီတပ်ဆင်ဖို့ရန်နှင့်လိုအပ်သော driver ကို install လုပ်ထားဖို့ရန်ဖြစ်ပါတယ်။ wireless NIC ကို ကွန်ပျူတာမှာတပ်ဆင်ခြင်းနှင့် driver ကို install လုပ်ပုံအဆင့်ဆင့်တို့သည် card အမျိုးအစားနှင့်ထုတ်လုပ်သောကုမ္ပဏီပေါ်မူတည်ပြီးကွဲလွဲမှုများရှိနိုင်ပါတယ်။ သို့သော်လည်းအခြေခံအားဖြင့်ရှေ့ wire network မှာတုန်းက ဖော်ပြခဲ့တဲ့ ethernet NIC တပ်ဆင် install လုပ်ပုံတို့နှင့်အတူတူပင်ဖြစ်ပါတယ်။ ဒါ့ကြောင့် အသေးမစိတ်တော့ပဲ တပ်ဆင် install ပြီး၍ အသုံးပြု၍ ရနိုင်သော network တစ်ခုအဖြစ်သို့ရောက်ရှိအောင် setup လုပ်ပုံများကို အပိုင်း ၂ ပိုင်းခွဲ၍ ဆက်လက်ဖော်ပြသွားမှာဖြစ်ပါတယ်။

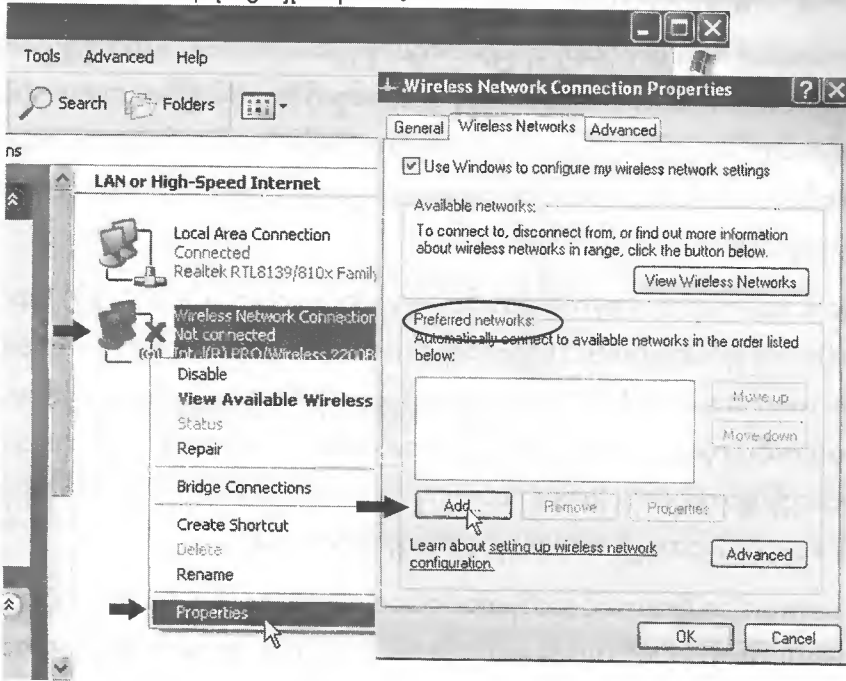
- >> ကွန်ပျူတာတစ်လုံးပေါ်မှာ network setup လုပ်ခြင်း
- >> ၎င်း network ကိုကျန်ကွန်ပျူတာများမှ နေ၍ချိတ်ဆက်ခြင်းတို့ဖြစ်ပါတယ်။

● Setting up on Ad-hoc Network on A Computer

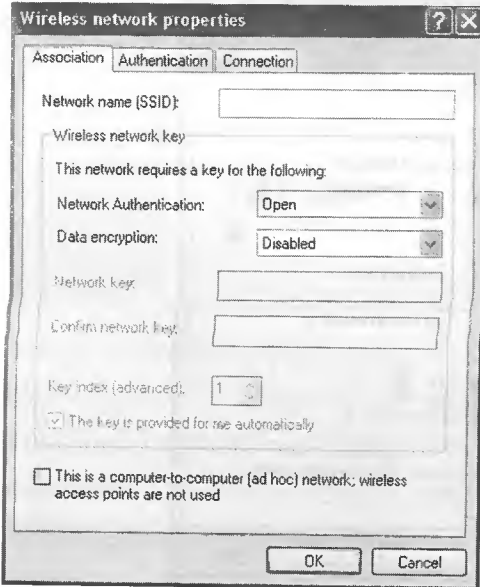
ကွန်ပျူတာတစ်လုံးမှာ wireless NIC ကိုတပ်ဆင် install ခဲ့ပြီးပြီဆိုရင် control panel မှတဆင့် သွားပြီး network connection ကိုဖွင့်လိုက်ပါ။ network connection window ထဲတွင် wireless connection icon ကိုတွေ့ရပါလိမ့်မယ်။ ယခုအချိန်တွင်ဒီကွန်ပျူတာ၏ဝန်းကျင်တွင်မည်သည့် wireless network မှမရှိသေးသည့်အတွက် connection icon တွင်အနီရောင်ကြက်ခြေခတ်ပြနေပါလိမ့်မယ်။ link မရှိတဲ့သဘောဖြစ်ပါတယ်။

1) wireless connection icon တွင် right-click နှိပ်ပြီး ကျလာမည့် sub-menu ထဲရှိ **properties** တွင် click နှိပ်ပါ။ TAB သုံးခုပါသော "connection properties" dialog box ကျလာပါမည်။ wireless tab အောက်သို့သွားပါ။ ယခုအချိန်ထိမည်သည့် wireless network ကိုမှမချိတ်ဆက်ရသေးသည့်အတွက်

preferred network နေရာတွင်ရှင်းနေပါလိမ့်မယ်။



2) Add buttonတွင် click နှိပ်ပါက အောက်ဖော်ပြပါပုံကို မြင်ရပါလိမ့်မယ်။



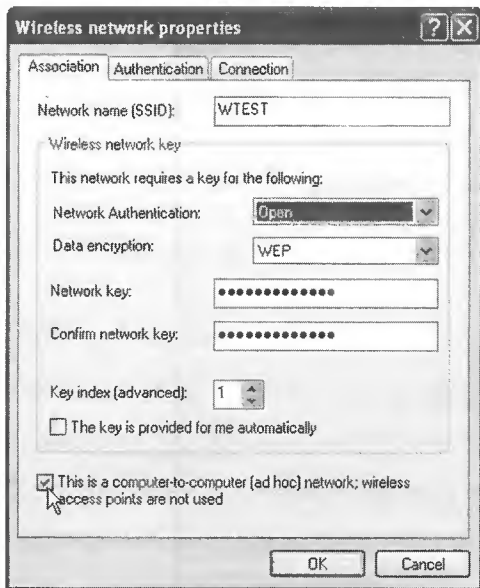
3) Network Name (SSID) နေရာတွင် နှစ်သက်ရာအမည်ကို ထည့်ပေးရပါမယ် (ဥပမာ - WTEST)။ အရေးကြီးတာက ဒီအမည်ကိုပင် network name အဖြစ် ကွန်ပျူတာအားလုံးတို့ တညီတညွတ်တည်း အသုံးပြုကြဖို့လိုပါတယ်။ network authentication နေရာမှာတော့ open ကိုပွဲရွေးချယ်ထားပါ။ ဒီနေရာမှာ

နောက်တစ်ချက် ရွေးချယ်စရာ option တစ်ခုက WEP (Wired Equivalent Privacy) ဖြစ်ပါတယ်။

4) မိမိ network ၏ security ပိုင်းကို တိုးမြှင့်ကာကွယ်ဖို့ရန်အတွက် WEP ကို အသုံးပြုကြလေ့ရှိပါတယ်။ WEP သည် network authentication နှင့် data တွေကို ဒီအတိုင်း transmit မလုပ်ပဲ encrypt လုပ်ပြီးပို့ရန်အတွက် key ကိုအသုံးပြုသော standard တစ်ခုဖြစ်ပါတယ်။ ၎င်း key ကို network key လို့ခေါ်ပါတယ်။ network key ကို ထည့်သွင်းပေးရန်အတွက် ပထမဦးစွာ data encryption နေရာတွင် WEP ကိုရွေးချယ်ပါ။

5) network key နေရာတွင် key ကိုရိုက်ထည့်ပါ။ key ကိုရိုက်ထည့်ရာမှာ ASCII (သို့) Hexadecimal format ကိုအသုံးပြုနိုင်ပါတယ်။ ASCII သုံးမယ်ဆိုရင် Keyboard ပေါ်က (upper/lower letter၊ number၊ punctuation အပါအဝင်) စာလုံးရေရှလုံး (သို့) ၁၃လုံး ရိုက်ထည့်ရပါမယ်။ Hex ကိုသုံးမယ်ဆိုရင် Aမှ F အထိ၊ 1မှ 9 အထိ စာလုံးရေ ၁၀လုံး (သို့) ၂၆လုံး ရိုက်ထည့်ရပါမယ်။ confirm နေရာတွင် ထို key ကို ပင်ထပ်မံ ရိုက်ထည့်ပါ။ ကွန်ပျူတာတစ်လုံးလုံးကနေ network ကို access လုပ်ဖို့ကြိုးစားတဲ့အခါ ဒီနေရာမှာ ထည့်ခဲ့တဲ့ network key ကို သိမှသာလျှင် access လုပ်ခွင့်ရကြမှာဖြစ်ပါတယ်။

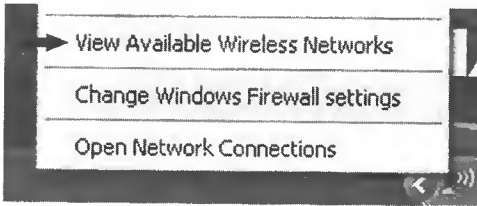
6) ပြီးရင် network အမျိုးအစားကို သတ်မှတ်ပေးရပါမယ်။ WAP (Access Point) မသုံးသောရိုးရိုး ad-hoc network ဖြစ်ကြောင်းကို 'this is a computer to computer (ad-hoc)' နေရာဘေးရှိ check box ထဲမှာ အမှန်ခြစ် ပေါ်အောင် click နှိပ်ပြီး ရွေးချယ်ပေးရပါမယ်။



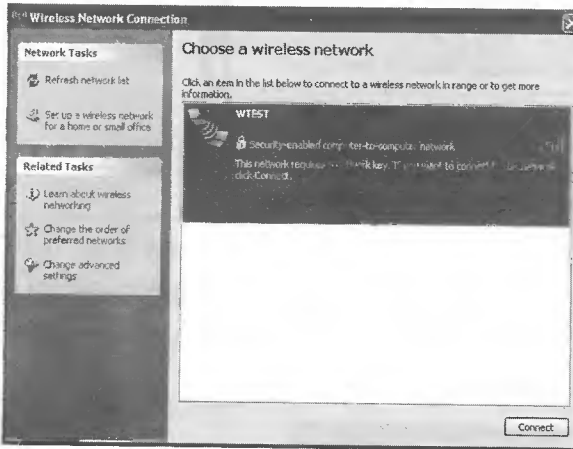
7) OK button တွင် click နှိပ်ပါက မူလ connection properties box သို့ပြန်ရောက်သွားပါလိမ့်မယ်။ ထိုနောက် connection rproperties ရှိ OK တွင် click နှိပ်ပြီး ပိတ်လိုက်ပါ။ ဒါဆိုရင် wireless ad-hoc network တစ်ခုကို အောင်မြင်စွာ တည်ဆောက်ပြီးပြီလို့ဆိုနိုင်ပါပြီ။

● Connecting to the Ad-hoc network

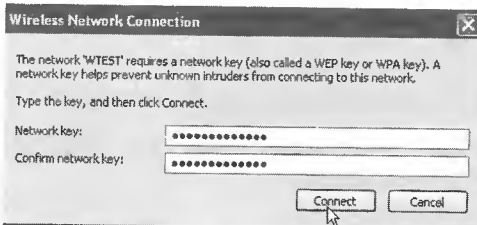
windows XPတွင် wireless networkချိတ်ဆက်အသုံးပြုရန်အတွက်အလွန်းရိုးရှင်းလွယ်ကူတဲ့ built-in featureတစ်ခုပါရှိပြီးသား ဖြစ်ပါတယ်။ ဆိုရရင် wireless NICတပ်ဆင်ထားသော ကွန်ပျူတာကို wireless network ဧရိယာ တစ်ခုအတွင်းသို့ သယ်ဆောင်သွားတာနှင့် taskbar ပေါ်တွင် connection နှင့် ပိတ်သက်သော pop-up menu တစ်ခု အလိုအလျှောက် ပေါ်လာပါလိမ့်မယ်။



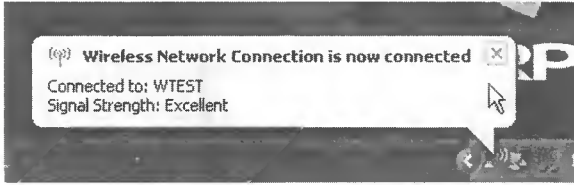
1) Task bar ပေါ်ရှိ connection icon ပေါ်တွင် right-click နှိပ်ပါ။ pop-up menu ထဲရှိ **view available wireless network** တွင် click တစ်ချက်နှိပ်ပါ။ wireless network connection window ပွင့်လာပါလိမ့်မည်။



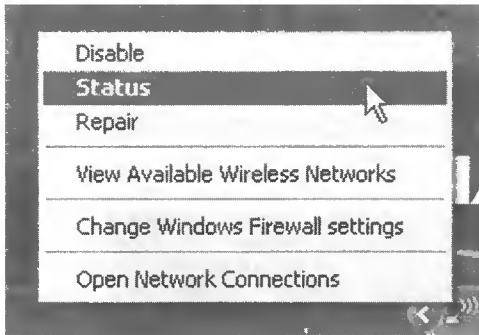
2) available wireless network နေရာတွင် network အမည်ကို တွေ့ရသင့်ပါတယ်။ (ဥပမာ - WTEST) (အကယ်၍ မတွေ့ပါက မိမိကွန်ပျူတာသည် အသုံးပြု၍ ရနိုင်သော ဧရိယာအတွင်း မှာမရှိသောကြောင့်ဖြစ်ပါလိမ့်မယ်။) network အမည်ပေါ်တွင် click တစ်ချက်နှိပ်ပြီး select လုပ်ပါ။ ပြီးလျှင် **Connect** ကိုနှိပ်ပါ။ network key တောင်းသော box ကျလာမည်။



3) network key နေရာတွင် ရှေ့က ကွန်ပျူတာမှာ AD-hoc network တည်ဆောက် စဉ်အခါ တုန်းက ထည့်သွင်းခဲ့သော key ကို ရိုက်ထည့်ပါ။ ပြီးရင် **connect** button တွင် click နှိပ်လိုက်ပါ။ မော်နီတာ screen ၏ ညာဘက်ထောင့် task bar ပေါ်တွင် network icon နှင့် ချိတ်ဆက်မိပါပြီဆိုသည့် အကြောင်းကို ဖော်ပြသော message တစ်ခုကို တွေ့ရပါလိမ့်မယ်။



4) Task bar ပေါ်ရှိ connection icon ပေါ်တွင် right-click နှိပ်ပါ။ pop-up button ထဲရှိ **status** တွင် click တစ်ချက်နှိပ်ပါ။ wireless network connection status ပွင့်လာပါလိမ့်မည်။



5) status window ထဲတွင် network အမည်၊ connection speed၊ signal strength တို့ကို မြင်ရပါမည်။ အသုံးပြုရအဆင်မပြေတဲ့ အခါမျိုးတွေမှာ ဘာကြောင့်ဖြစ်ရသလဲဆိုတာကို ဒီနေရာမှာ အကြမ်းဖျဉ်း ဝင်ရောက်စစ်ဆေးကြည့်ရှုနိုင်ကြပါတယ်။



Creating User Accounts

windows XPသည်တကယ့်multiuser systemဖြစ်ပါတယ်။ သဘောကတော့ ကွန်ပျူတာ တစ်ခုလုံးတည်းမှာပင်လူအများသီးခြားစီ အသုံးပြုနိုင်ခြင်းကိုဆိုလိုပါတယ်။ ရှေ့က win 98 အသုံးပြုသော ကွန်ပျူတာတွေမှာလည်း လူအများစုပေါင်းအသုံးပြုနိုင်ပါတယ်။ သို့သော် အဲဒီ windows 98 အသုံးပြု နေသော ကွန်ပျူတာတွေမှာဆိုရင် user တစ်ယောက် သိမ်းဆည်းထားသည့် file တွေ၊ folder တွေကို အခြားမည်သည့် user မဆို အလွယ်တကူ access လုပ်နိုင်ကြပါတယ်။ တစ်နည်းဆိုရရင် fileတွေ folder တွေကို ဖျက်ပစ်ခြင်း၊ software များ install/ unistall ပြုလုပ်ခြင်း၊ အရေးကြီးသော configuration များကို ပြောင်းလဲပြုပြင် ခြင်း အစရှိသည်တို့ကို မည်သူမဆို ပြုလုပ်နိုင်ကြသည့်အတွက် ကွန်ပျူတာသည် အကာကွယ်မဲ့နေပြီး မလိုလားအပ်သော ပြဿနာများကို ဖြစ်ပေါ်စေတတ်ပါတယ်။ *

windows XPမှာတော့ userတစ်ဦးကို accountတစ်ခုစီခွဲခြားထားရှိခြင်းဖြင့် ၎င်းပြဿနာများကို ဖြေရှင်းနိုင်ကြပါတယ်။ windows XP တွင် administratorနှင့် limited ဟူ၍ account ၂မျိုးရှိပါတယ်။ administrator accountသည် ကွန်ပျူတာတစ်ခုလုံးကို လိုသလိုပြုပြင်ပြောင်းလဲခြင်းများ ပြုလုပ်နိုင်ပြီး limited account များကတော့ အကန့်အသတ်ဖြင့်သာ အသုံးပြုနိုင်ပါလိမ့်မယ်။ အောက်ဖော်ပြပါ ဇယားမှာဆိုရင် administrator နှင့် limited account တို့၏ လုပ်ပိုင်ခွင့် ကွာခြားချက်များကို စုစည်း ဖော်ပြထားပါတယ်။

right	Administrator	Limited
Install hardware and software	✓	×
Make Systemwide Changes	✓	×
Access and read all non-private files	✓	×
Create and delete user Accounts	✓	×
Change other people Accounts	✓	×
Change account name or type	✓	×
Change own Account picture	✓	✓
Create, change, or remove own password	✓	✓

windows XPကို install ပြီးသွားတဲ့အခါ defaultအနေနှင့် administratorနှင့် Guest လို့ အမည်ရတဲ့ user account ၂ခုကို ကွန်ပျူတာမှာ အလိုအလျောက် create လုပ်ပြီးသား ဖြစ်ပါတယ်။

Administrator: administrator account သည် windows XPတွင်းသို့ logonဝင်ရာတွင် အသုံးပြုရတဲ့ပထမဆုံး accountပင်ဖြစ်ပါတယ်။ အဲဒီ accountဖြင့် logon ဝင်ပြီးမှသာ အခြား account သစ်များဖန်တီး တည်ဆောက်ခြင်း၊ ကွန်ပျူတာ configuration များအားပြင်ဆင် သတ်မှတ်ခြင်းတို့ကို လုပ်ဆောင်နိုင်ပါ လိမ့်မယ်။ administrator accountရဲ့အဓိကထူးခြားချက်ကတော့၎င်း ac- count ကို လုံးဝဖျက်ထုတ်ခြင်း (delete)၊ အသုံးပြု၍မရနိုင်အောင် ပိတ်ထားခြင်း (disable)တို့ကိုလုပ်ဆောင်၍မရပါ။ သို့သော် administrator အမည်အစားအခြားမည်တစ်ခုသို့ပြောင်းလိုကပြောင်းလဲအသုံးပြုနိုင်ပါတယ်။

Guest : guest account ကတော့ သူ့အမည်အတိုင်းပင် ကွန်ပျူတာမှာ ကိုယ်ပိုင် account မရှိသူများ logonဝင်ရောက်အသုံးပြုနိုင်စေရန်ဖြစ်ပါတယ်။ ပုံမှန် default အားဖြင့် disable လုပ်ထားပြီး အသုံးပြုလိုတဲ့ အခါမှာ enable လုပ်ဖို့လိုပါလိမ့်မယ်။

လုပ်ပိုင်ခွင့်များအရအကြမ်းဖျဉ်းချုံ့ပြီး ပြောရမယ်ဆိုရင်တော့ administratorသည် admin- istrator accountအမျိုးအစားဖြစ်ပြီး guestကတော့ limited accountအမျိုးအစားနှင့်ဆင်တူပါတယ်။ ၎င်း builtin account ၂ခုတို့အပြင် မိမိတို့ရဲ့အသုံးလိုမှုပေါ်မူတည်ပြီး user account များစွာကို ထပ်မံ create လုပ်ပြီး အသုံးပြုနိုင်ကြပါတယ်။

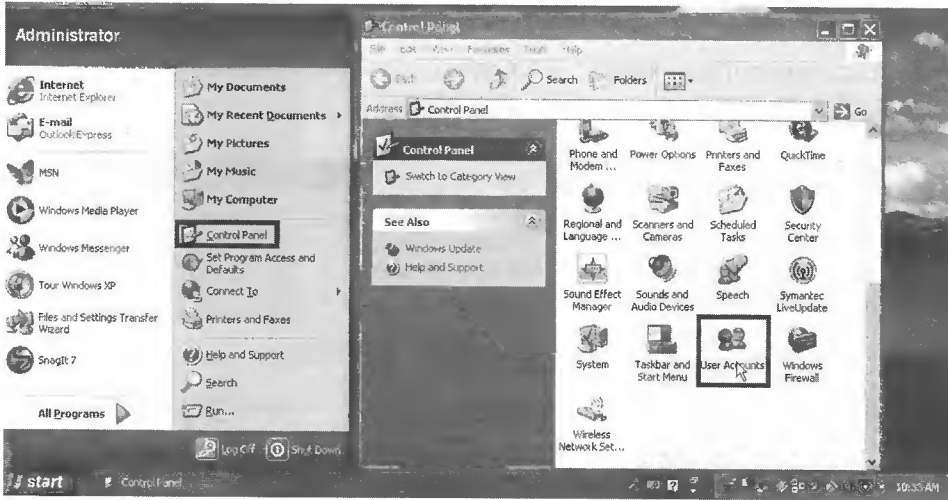
ထိုကဲ့သို့ဖန်တီးတဲ့နေရာမှာ ဘယ် user accountကို administrator accountအမျိုးအစား၊ ဘယ် user accountကိုတော့ limited အမျိုးအစားဖြင့် သတ်မှတ်မလဲ ဆိုတာကတော့ ကွန်ပျူတာ ad- ministratorရဲ့ရွေးချယ်မှုပင်ဖြစ်ပါတယ်။ အဲဒီလို account createလုပ်ခြင်းများကို computer man- agementနှင့် control panel ၂နေရာတို့မှတဆင့်လုပ်ဆောင်နိုင်ပါတယ်။

control panelမှတဆင့် account create လုပ်ခြင်းများကို မည်သူမဆို အလွယ်တကူ လုပ်ဆောင်နိုင်သော်လည်း computer managementမှတဆင့်လုပ်ဆောင်ရန်အတွက်မူ experienced userများနှင့်သာ သင့်တော်ပါတယ်။

Creating User Accounts In Control Panel

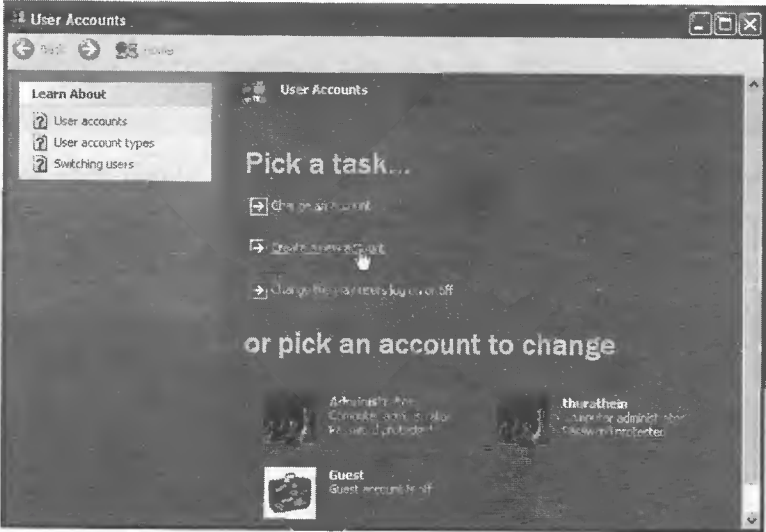
ယခုဆက်လက်ပြီး account createလုပ်ခြင်း၊ ရှိပြီးသား account တို့ကို manageလုပ်ခြင်း များအား control panel ထဲရှိ user accountမှတဆင့်လုပ်ဆောင်ပုံအဆင့်ဆင့်တို့ကို ဖော်ပြသွားမှာ ဖြစ်ပါတယ်။

1) ပထမဦးစွာ control panel သို့သွားရောက်ရန်အတွက် **start > control panel** တွင် click တစ်ချက်စီနှိပ်ပါ။ "control panel" Window ပွင့်လာပါလိမ့်မည်။



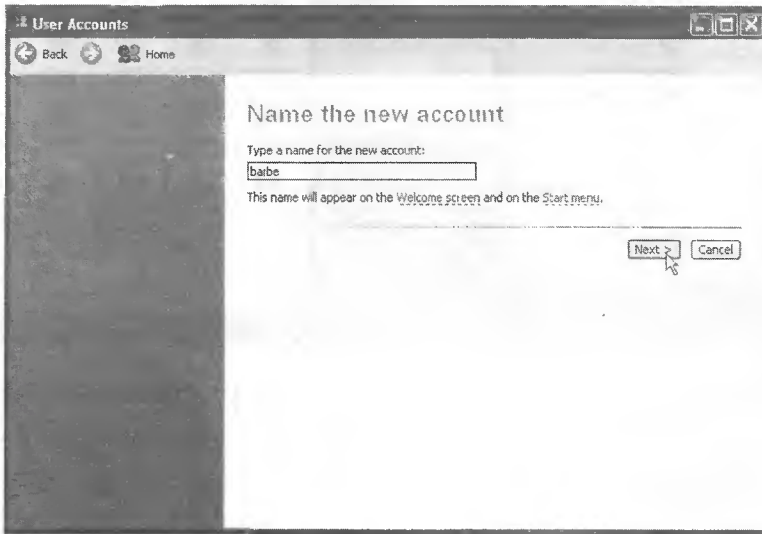
2) control panel ထဲရှိ user accountတွင် double clickနှိပ်ပါက user account windows ပွင့်လာပါလိမ့်မည်။ ၎င်း "user Account" window ထဲတွင် အောက်ဖော်ပြပါ လုပ်ငန်းစဉ်သုံးခုကို လုပ်ဆောင်နိုင်ကြပါတယ်။

- Change an account
- Create a new account
- Change the way users logon or logoff



1) Create A New Account

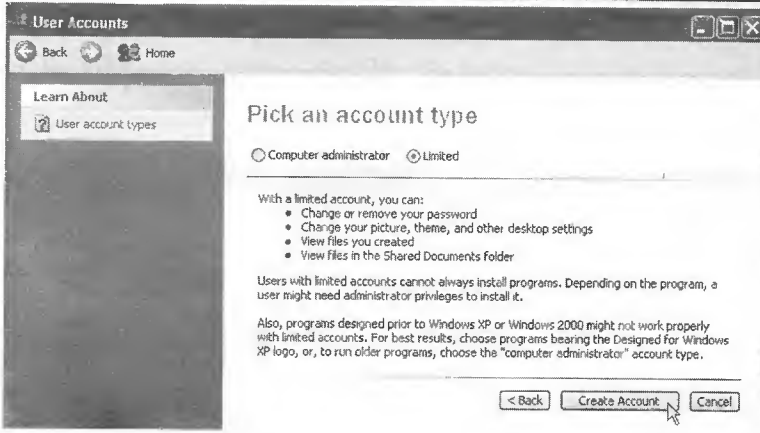
1) user accountအသစ်တစ်ခုကိုဖန်တီးရန်အတွက် **create new account**တွင် click တစ်ချက် နှိပ်ပါက username ကို ထည့်သွင်းပေးဖို့ရန် တောင်းခံပါလိမ့်မည်။ ဒီနေရာမှာ ထည့်သွင်းလိုက်မည့် username အား welcome screen နှင့် start menuတို့တွင် ဖော်ပြမှာ ဖြစ်ပါတယ်။ usernameအား ထည့်သွင်းပြီးပါက **Next** button တွင် click တစ်ချက်နှိပ်ပါ။



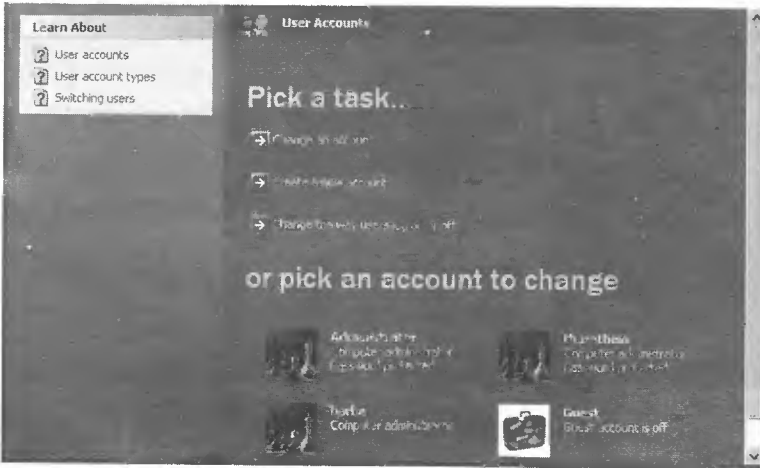
2) usernameကိုထည့်သွင်းခဲ့ပြီးပါက account typeကိုရွေးချယ်ပေးရမည့် windowကို မြင်ရပါမည်။ ဒီနေရာမှာ မိမိဖန်တီးမည့် account သည် administrator လား၊ limited လားဆိုတာကို ရွေးချယ် ပေးရပါမယ်။ အဲဒီလိုမရွေးချယ်ခင် မိမိသည်ဘယ်လို account မျိုးဖန်တီး မှာလဲဆိုတာကို သေသေချာချာ စဉ်းစားထားဖို့လိုပါတယ်။

ဆိုရရင် administrator လုပ်ပိုင်ခွင့်များကိုရရှိထားသည့် accountဖြင့်အသုံးပြုသူသည်အခြား accountများကိုဖျက်ထုတ်နိုင်ခြင်း၊ softwareများကိုဖြုတ်တပ်လုပ်နိုင်ခြင်း၊ ကွန်ပျူတာ၏အရေးကြီးသော configurationများကိုပြောင်းလဲနိုင်ခြင်း၊ hard diskတို့ကို formatရိုက်နိုင်ခြင်း၊ အစရှိသဖြင့် ကွန်ပျူတာ တစ်ခုလုံးကိုလိုသလို manageလုပ်နိုင်ရမှာဖြစ်ပါတယ်။ သည့်အတွက်ကြောင့်ကွန်ပျူတာတစ်ခုလုံးမှာ administrator accountများစွာထားရှိနိုင်သော်လည်းအသုံးပြုမည့်သူအပေါ်မူတည်ပြီး administrator အဖြစ် createလုပ်သင့်မလုပ်သင့် စဉ်းစားရမှာ ဖြစ်ပါတယ်။

limited account ရရှိထားတဲ့ အသုံးပြုသူသည် သူ၏ password နှင့် username များကို ပြောင်းလဲအသုံးပြုခြင်း၊ file နှင့် folder များဖန်တီးခြင်း၊ "share document" folder များအား ဖွင့်ကြည့်ခြင်းတို့ကို လုပ်ဆောင်နိုင်ပါတယ်။ သို့သော် အချို့သော software များကို install လုပ်ခြင်းနှင့် အခြားအရေးကြီး configuration များအား ပြောင်းလဲခြင်းတို့ကို လုပ်ဆောင်၍ ရမည်မဟုတ်ပါ။

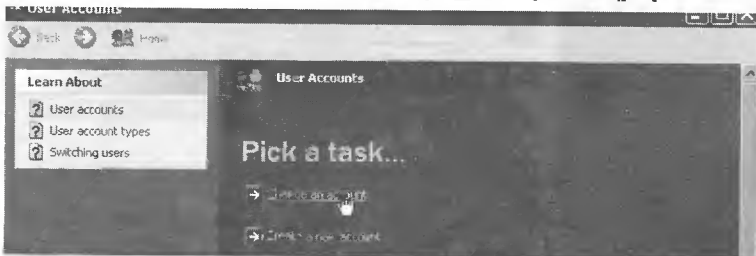


မိမိ create လုပ်မည့် account type ကို စဉ်းစားပြီး ပြီဆိုရင် administrator (သို့) limited ရှိ radio button တွင် ဖြစ်အောင် click နှိပ်ပြီး select လုပ်ပါ။ account type ကို ရွေးချယ်ပြီးပါက create account တွင် click တစ်ချက်နှိပ်ပါ။ ဒါဆိုရင် user account တစ်ခုကို create လုပ်ခြင်းပြီးဆုံးသွားပြီး မူလ user account windows တွင် account အသစ်၏ပုံနှင့် အမည်ကို မြင်ရပါလိမ့်မယ်။

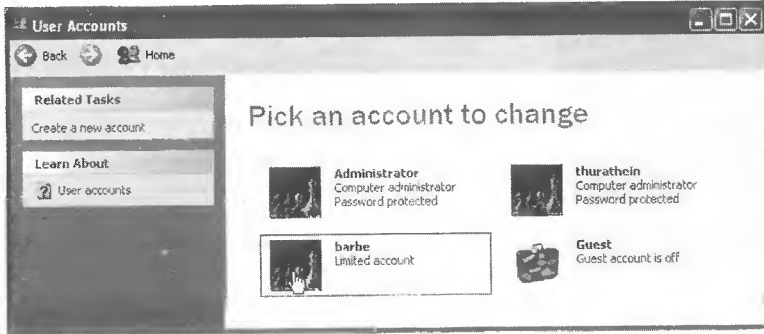


Change an account

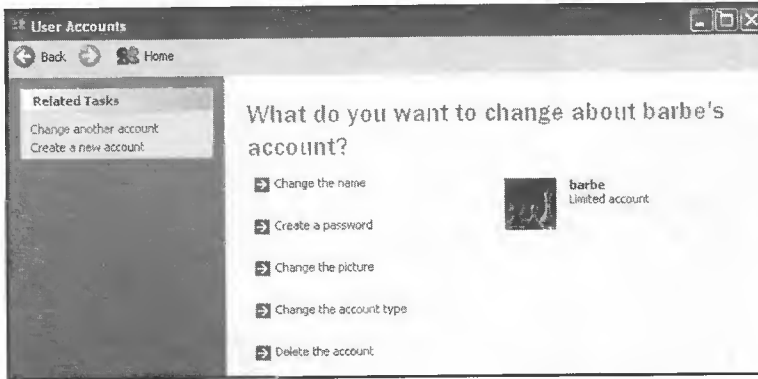
မိမိဖန်တီးထားခဲ့သော account များနှင့် ပတ်သက်ပြီး လိုသလို ပြုပြင်ပြောင်းလဲ ခြင်းတို့ကို ပြုလုပ်ရန်အတွက် change an account တွင် click နှိပ်ပြီး အလွယ်တကူ လုပ်ဆောင် နိုင်ကြပါတယ်။



1) user account windows ထဲရှိ **change an account** တွင် click တစ်ချက်နှိပ်ပါ။ ကွန်ပျူတာမှာ create လုပ်ထားသော user account list ကို ဖော်ပြထားသည့် window ကို မြင်ရပါမည်။

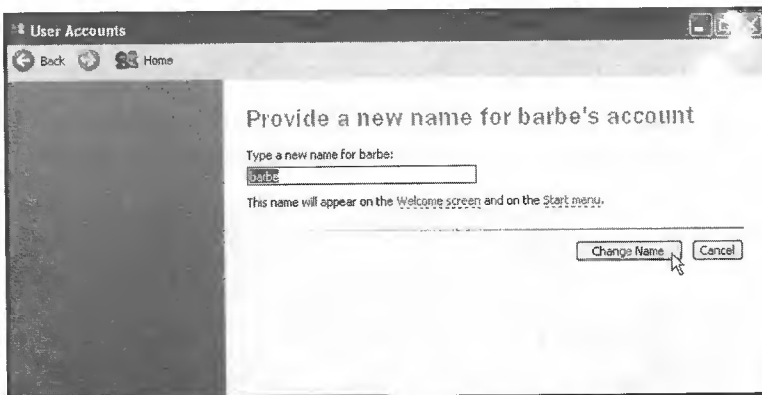


2) ၎င်း list ထဲမှ account picture တစ်ခုကို ရွေးချယ် click နှိပ်တဲ့အခါ ထို account ပတ်သက်ပြီး လုပ်ဆောင်နိုင်မည့် လုပ်ငန်းစဉ်များကို window တစ်ခုဖြင့် ဖော်ပြပါလိမ့်မယ်။



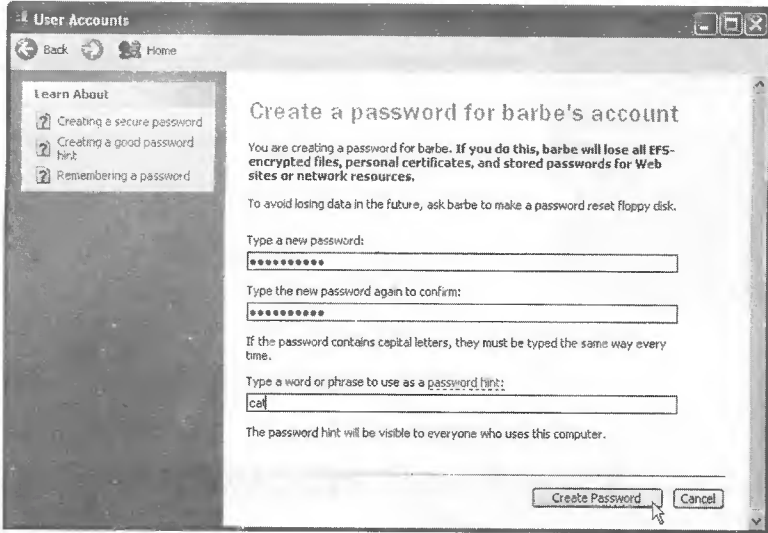
■ **change the name**

username ကို ဒီ change the name တွင် click နှိပ်ပြီး ပြောင်းလဲနိုင်ပါတယ်။



■ Create Password

မိမိ create လုပ်ခဲ့သော account အတွက် password သတ်မှတ်လိုပါက create password တွင် click နှိပ်ပြီး ထည့်သွင်းပေးနိုင်ပါတယ်။



new password နေရာတွင် password အဖြစ်ထည့်သွင်းလိုသော စာလုံးများကို ရိုက်ထည့်ရပါမယ်။ confirm နေရာတွင် password ကိုနောက်တစ်ကြိမ်ထပ်မံထည့်သွင်းပေးရပါမယ်။ password hint နေရာတွင် မိမိထည့်သွင်းခဲ့သော password ကို မေ့နေတဲ့အခါမျိုးမှာ ပြန်လည်မှတ်မိသိရှိစေရန်အစဖော် ပေးနိုင်မည့် စကားလုံး၊ စကားစုတို့ကို ရိုက်ထည့်ပေးနိုင်ရတယ်။ ၎င်း password hint ကို welcome screen တွင် မည်သူမဆို အလွယ်တကူ ကြည့်ရှုနိုင်မှာ ဖြစ်သည့်အတွက် ကြောင့် အလွန်သတိထားဖို့ လိုပါတယ်။

မှတ်ချက်။ ။ account သည် password ရှိပြီးသား ဖြစ်ပါက create password မပါတော့ဘဲ change the password နှင့် remove the password ဟူသော option ၂ခု ပါရှိပါလိမ့်မယ်။

■ Change the picture

account တစ်ခုကို create လုပ်ပြီးတာနှင့် ထို account အတွက် ရုပ်ပုံကို windows XP မှ အလိုလျောက် ထည့်သွင်း ပေးထားပြီးသားဖြစ်ပါတယ်။ အကယ်၍ အခြား ရုပ်ပုံတစ်ခုသို့ ပြောင်းလိုပါက change the picture တွင် click နှိပ်ပြီး ပြောင်းနိုင်ပါတယ်။

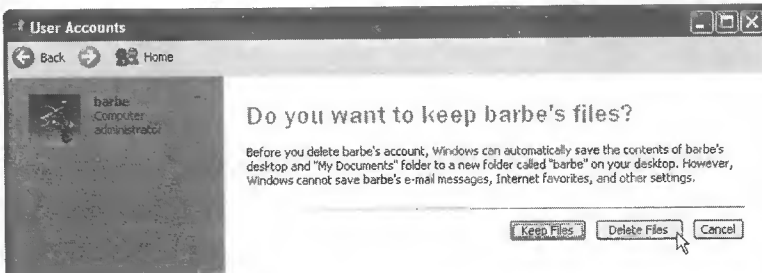
■ Change the account type

limited မှ administrator သို့ administrator မှ limited သို့ အစရှိသဖြင့် account type ကို ပြောင်းလိုပါက change the account type တွင် click နှိပ်ပြီး ပြောင်းနိုင်ပါတယ်။



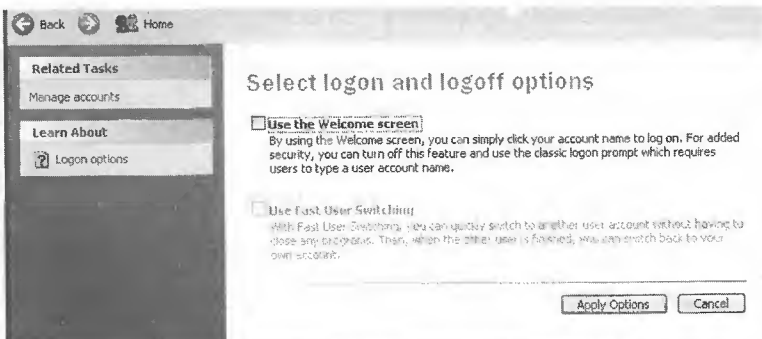
■ Delete the account

user accountကို အကြောင်းတစ်ခုခုကြောင့် ဖျက်ထုတ်လိုက်ရတဲ့အခါ **delete the account** တွင် click နှိပ်ပြီး ဖျက်ထုတ်နိုင်ကြပါတယ်။



● Change the way user logon and logoff

administrator သည် ကွန်ပျူတာမှာ ဝင်ရောက်အသုံးပြုမည့် user များအနေနှင့် logon ဝင်ရောက်အသုံးပြုသည့်အခါမှာသော်လည်းကောင်း၊ အသုံးပြုပြီးလျှင် logoff ထွက်တဲ့ အခါမှာသော်လည်းကောင်း ဘယ်လိုပုံစံဖြင့် logon/ logoffလုပ်ဆောင်ရမလဲဆိုတာကို change the way တွင် click နှိပ်ပြီး သတ်မှတ်ပေးနိုင်ပါတယ်။ အဲဒီလို change the way users log on or off တွင် click နှိပ်လိုက်တဲ့ အခါမှာ ရွေးချယ်စရာ option ၂ခုပါတဲ့ window ကို မြင်ရပါလိမ့်မယ်။

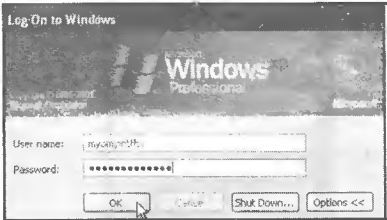


■ Use the welcome screen

☑ Use the Welcome screen ကို ရွေးချယ်ခဲ့မည်ဆိုပါက ကွန်ပျူတာပါဝါဖွင့်ပြီး စတင်အသုံးပြု ဖို့ရန် အဆင်သင့် ဖြစ်သွားပြီးတဲ့အခါ logon ဝင်ရောက်နိုင်မည့် account များကိုတန်းစီ ဖော်ပြထားတဲ့ screen ကိုမြင်ရစေမှာ ဖြစ်ပါတယ်။ အသုံးပြုသူများအနေနှင့် logon ဝင်ရောက်ရန်အတွက် မိမိရဲ့ account ပေါ်တွင် click နှိပ်ရမှာဖြစ်ပြီး အကယ်၍ လိုအပ်ပါက password ကို ရိုက်ထည့်ရမှာဖြစ်ပါတယ်။

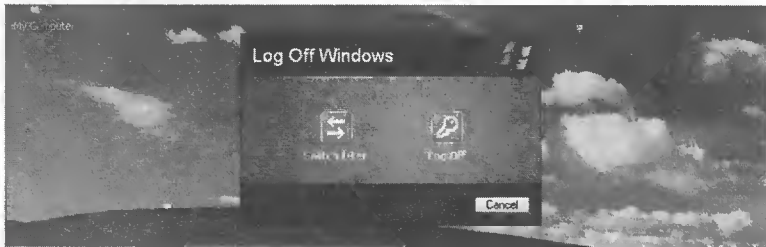


အကယ်၍ များ ကွန်ပျူတာလုံခြုံရေးကို ပိုမိုတိုးမြှင့်ကာကွယ်ထားချင်ရင်တော့ welcome screen ဘေး check box ကို uncheck လုပ်ခဲ့ရပါမယ်။ ဒါဆိုရင် ကွန်ပျူတာကို ပါဝါဖွင့်ပြီး စတင်အသုံးပြုဖို့ရန် အဆင်သင့်ဖြစ်တဲ့အခါမှာ welcome screen ပေါ်မလာတော့ပဲ "Ctrl + Alt + Del" ကိုနှိပ်ပါဆိုတဲ့ message ကို screen ပေါ်မှာမြင်ရမှာဖြစ်ပါတယ်။ အဲဒီအခါ keyboard မှ Ctrl၊ Alt နှင့် Delete တို့ကိုတပြိုင်နက် ဖိနှိပ်ရမှာဖြစ်ပါတယ်။ ပြီးမှ user name နှင့် password ၂ခုစလုံးကို အတိအကျရိုက်ထည့်ပြီး logon ဝင်ရောက် အသုံးပြုရမှာဖြစ်ပါတယ်။ ဒါကြောင့် welcome screen မှာကဲ့သို့ logon ဝင်ရောက်ခြင်းကို password တစ်မျိုးတည်းဖြင့် ကန့်သတ်ထားခြင်းမျိုးမဟုတ်ပဲ username နှင့် password ၂မျိုးစလုံးတို့ဖြင့် ကန့်သတ် ထားသည့်အတွက် security ပိုင်းကို ပိုမိုတိုးမြှင့်ကာကွယ်နိုင်တယ်လို့ဆိုနိုင်ပါတယ်။



Use fast user switching

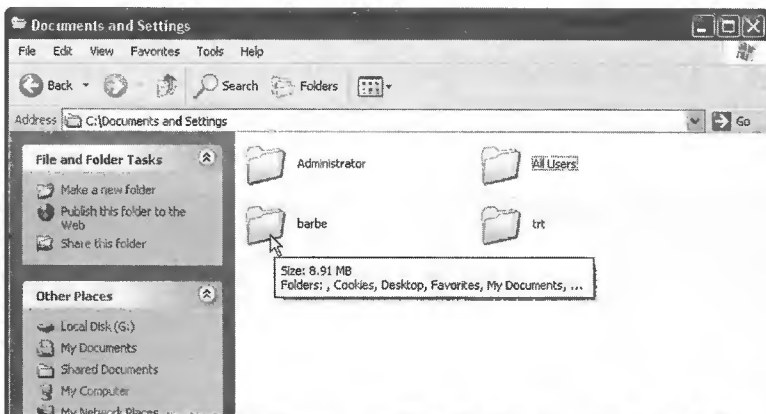
switching သည် ကွန်ပျူတာမှာ လက်ရှိဝင်ရောက်နေသော account ဖြင့် ဖွင့်ထားသော program များ၊ file များကို ပိတ်စရာမလိုပဲ အခြား account ဖြင့် ထပ်မံ logon ဝင်ရောက် အသုံးပြုနိုင်စေပါတယ်။ ဒီ feature သည် ကွန်ပျူတာတစ်လုံးတည်းကို လူအများစုပေါင်း အသုံးပြု ရတဲ့ လုပ်ငန်းများမှာ လွန်စွာ အသုံးတည့်ပါတယ်။ **Use Fast User Switching** ကို ရွေးချယ် ထားတဲ့ ကွန်ပျူတာတွင် logoff လုပ်ပါက ရွေးချယ်စရာ option ၂ ခုပါတဲ့ window ကို တွေ့ရပါမယ်။



switch user တွင် click နှိပ်ပါက welcome screen ကို ရောက်သွားပြီး အခြား account တစ်ခုဖြင့် ထပ်မံ logon ဝင်ရောက်နိုင်ပါတယ်။ ၎င်း ဒုတိယလူ အသုံးပြုပြီး သွား၍ logoff လုပ်တဲ့အခါ welcome screen ပေါ်လာပါလိမ့်မည်။ ပထမ account ဖြင့် logon ပြန်ဝင်လာတဲ့အခါမှာ မူလထားခဲ့စဉ်က အတိုင်းပင် မိမိလုပ်ငန်းများကို အရှိန်မပျက်ဆက်လက်လုပ်ဆောင်နိုင်စေပါလိမ့်မယ်။

User Profile

ကွန်ပျူတာမှာ user account တစ်ခုဖြင့် ပထမဆုံးအကြိမ် logon ဝင်ရောက် အသုံးပြု လိုက်တာနှင့် ၎င်း user အမည်ဖြင့် profile folder တစ်ခုကို C:\>document and setting အောက်မှာ အလိုလျောက် တည်ဆောက်ပြီး သား ဖြစ်ပါတယ်။ အဲဒီ profile ထဲမှာဆိုရင် my document၊ email နှင့် desktop setting များကို သိမ်းဆည်းထားပေးပါတယ်။



Creating User Accounts with Computer Management

Account သစ်များကို create လုပ်ခြင်း၊ ရှိပြီးသား account တို့အား manage လုပ်ခြင်းများကို computer management မှလည်းလုပ်ဆောင်နိုင်ကြပါတယ်။ ဒါဆိုရင် control panel ထဲရှိ user account မှ တစ်ဆင့် account ဆောက်ခြင်းနှင့် ဒီ management console ထဲမှတစ်ဆင့် account ဆောက်ခြင်းတို့သည် ဘာတွေကွာခြားနိုင်သလဲလို့ မေးစရာရှိလာနိုင်ပါတယ်။

Computer management ကိုအသုံးပြုမယ်ဆိုရင် account picture ရွေးချယ်ခြင်း၊ welcome screen နှင့် fast user switching တို့အားအသုံးပြုမပြု ဆိုတာကို ရွေးချယ်ပေးနိုင်ခြင်းတို့ကလွဲရင် control panel ထဲရှိ user account မှာ လုပ်ဆောင်နိုင်တာထက် ပိုပြီး account တွေကို ပိုမို manage လုပ်နိုင်ကြပါတယ်။ ဒါ့ကြောင့် user account create လုပ်ခြင်းကို ရင်းနှီးကျွမ်းဝင်လာသူများအနေနှင့် ဒီ computer management console ဖြင့် account များအားလိုသလို စီမံခန့်ခွဲခြင်းများကို ပိုမိုသဘောကျကြပါတယ်။

Accessing the Computer Management

Computer management သည် သူ့အမည်အတိုင်းပင် ကွန်ပျူတာ စနစ်တစ်ခုလုံးကို manage လုပ်နိုင်သည့် tools အတော်များများကို စုဝေးထားရာ console တစ်ခုပင်ဖြစ်ပါတယ်။ ဆိုရရင် account အသစ်ဆောက်ခြင်း၊ modify လုပ်ခြင်း၊ account များကို စုစည်း၍ group ဖွဲ့ခြင်းများသည်လည်း computer management ထဲရှိ tools များစွာထဲမှ တစ်ခုကို အသုံးပြု၍ လုပ်ဆောင်ခြင်းဖြစ်ပါတယ်။

computer management သို့ အောက်ဖော်ပြပါနည်းလမ်းများဖြင့် သွားရောက်နိုင်ပါတယ်။

- 1- Using control panel
- 2- right clicking and select manage
- 3- Using command line

1) Using Control Panel

control panel ထဲရှိ administrative tools ကို double click နှိပ်၍ ဖွင့်ပါ။ computer management ကို ထပ်မံ double click နှိပ်၍ ဖွင့်ပါက computer management window ပွင့်လာပါမည်။

2) Right Clicking and Select Manage

Desktop ပေါ်ရှိ my computer icon (သို့) start > my computer ပေါ်တွင် right click နှိပ်ပါ။ ကျလာမည့် shortcut menu ထဲရှိ **Manage** တွင် click နှိပ်ပါက computer management window ပွင့်လာပါလိမ့်မည်။

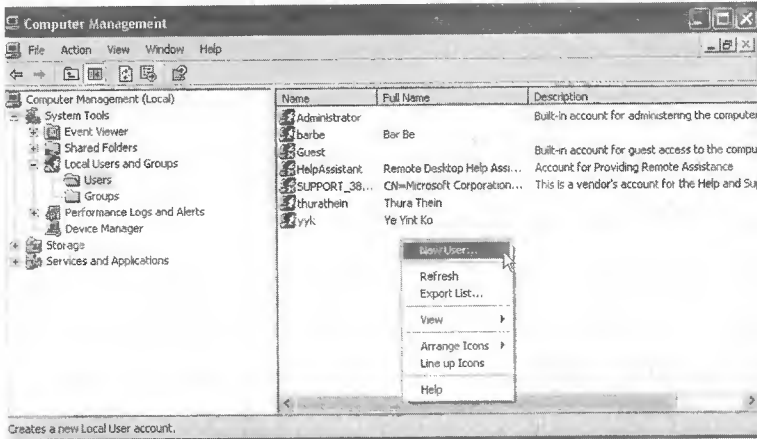
3) Using Command Line

Start > Run တွင် click နှိပ်၍ ဖွင့်ပါ။ Run dialog box ထဲတွင် **compmgmt.msc** ဟု ရိုက်ထည့်ပြီး **OK** button တွင် click နှိပ်ပါ။

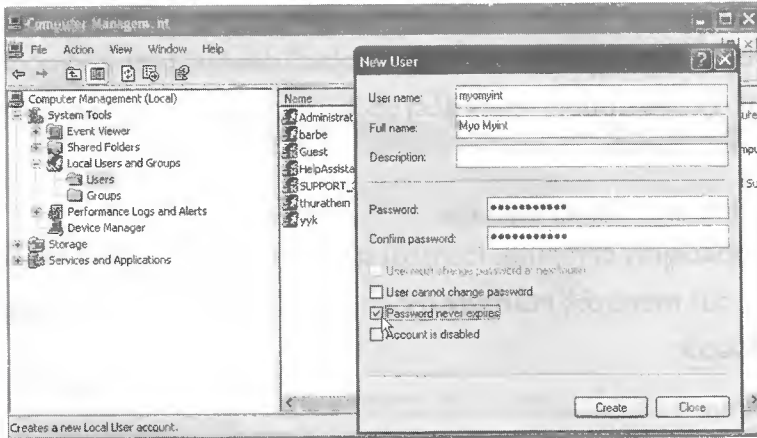
User Account Create

computer management ဖြင့် account create လုပ်ခြင်း၊ modify လုပ်ခြင်းများကို အောက်ပါအဆင့်များအတိုင်း လုပ်ဆောင်နိုင်ကြပါတယ်။

1) computer management windows ၏ ဘယ်ဘက်ခြမ်းရှိ tree-view ထဲတွင် System > Users and groups > Users တို့တွင် အဆင့်ဆင့်ဆန့်ထုတ်သွားပါက ညာဘက်ခြမ်းထဲတွင် ကွန်ပျူတာမှာ create လုပ်ထားသော account များကို တွေ့ရပါမယ်။ အနီးရောင်ကြက်ခြေခတ်ပြထားသော account များသည် disable လုပ်ထားသော account များပင်ဖြစ်ပါတယ်။



2) account list ထဲရှိ create လုပ်ထားပြီးသော account များနှင့် လွတ်တဲ့နေရာတွင် right click နှိပ်ပါ။ ကျလာမည့် sub-menu ထဲရှိ **New User** တွင် click နှိပ်ပါက "new user" dialog box ကျလာပါလိမ့်မည်။ "New User" dialog box ထဲရှိ user name၊ full name၊ description နှင့် password နေရာများတွင် မိမိဖန်တီးမည့် account နှင့် သက်ဆိုင်သော information များကို ရိုက်ထည့်ပါ။



password ထည့်သွင်းသတ်မှတ်လိုလျှင် password နှင့် confirm password နေရာတို့တွင် ရိုက်ထည့်ပြီး အောက်ဖက်တွင်ပါသော checkbox ထဲမှ တစ်ခုခုကို ရွေးချယ်ပေးရပါမယ်။

■ User must change password at next logon

ဒီ option ကို ရွေးချယ်ခဲ့မယ်ဆိုရင် ဤ account ကို အသုံးပြုသူ user သည် ပထမဆုံး အကြိမ် logon ဝင်ပြီးသည့်အခါတွင် လက်ရှိ password အစား သူ့စိတ်ကြိုက် အခြား password တစ်ခုခုကို ပြောင်းလဲအသုံးပြုရပါမယ်။ ဒီ option ကို deselect လုပ်မှသာ သူ့နောက်က အခြား option ၂ ခုကို ဆက်လက် ရွေးချယ်နိုင်ပါလိမ့်မယ်။

■ User Account Change Password

ဒီ option ကို ရွေးချယ်မယ်ဆိုရင် ဤ account အသုံးပြုသူ user သည် password ကို သူ့စိတ်ကြိုက် ပြောင်းလဲခွင့်မရှိပဲ administrator မှ ပေးထားသော password အတိုင်းသာ အသုံးပြုရနိုင်မှာ ဖြစ်ပါတယ်။

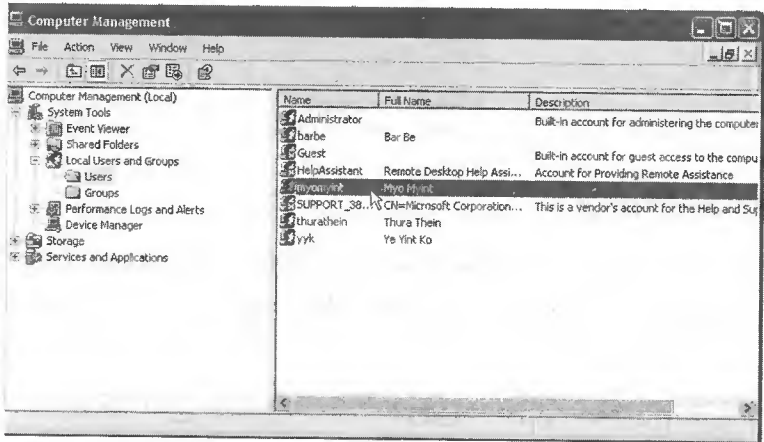
■ Password Never Expire

Windows XP ၏ security system သည် password တစ်ခု၏ သက်တမ်းကို 42 ရက်ထိသာ ခွင့်ပြုပါတယ်။ ဆိုရရင် 42 ရက်ပြည့်တာနှင့် password expire ဖြစ်သွားပြီး အခြား password တစ်ခုကို ပြောင်းလဲအသုံးပြုရန်အတွက် တွန်းအားပေးခိုင်းစေပါလိမ့်မယ်။ အဲဒီလိုမျိုး မဖြစ်စေချင်ရင်တော့ password never expire ဆိုတဲ့ option ကို ရွေးချယ်ခဲ့ဖို့ လိုပါတယ်။

■ Account Disable

User account တစ်ခုအား ကွန်ပျူတာမှာ log on ဝင်ရောက် အသုံးပြုမှုကို ယာယီပိတ်ထားလိုတဲ့အခါ ဒီ option ကို ရွေးချယ်ရမှာ ဖြစ်ပါတယ်။

3) အားလုံးပြီးပြီဆိုလျှင် **Create** button တွင် click တစ်ချက် နှိပ်လိုက်ပါ။ မိမိ create လုပ်ခဲ့သော account သစ်ကို computer management ရှိ user list ထဲတွင် တွေ့ရပါလိမ့်မယ်။



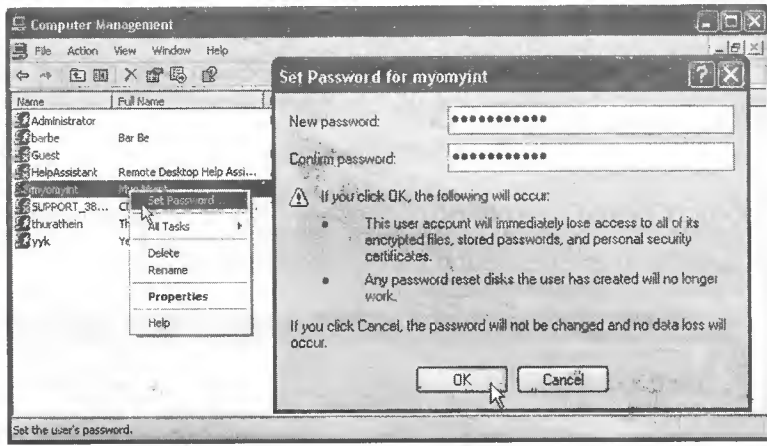
Managing User Accounts

Account များကို create လုပ်နိုင်သကဲ့သို့ပင် password ပြောင်းခြင်း၊ အမည်ပြောင်းခြင်း၊ disable လုပ်ခြင်းအစရှိသော account management လုပ်ငန်းများကိုလည်း computer management ထဲမှနေ၍ အလွယ်တကူလုပ်ဆောင်နိုင်ကြပါတယ်။ manage လုပ်လိုသော account တစ်ခုပေါ်တွင် right click နှိပ်ပါက submenu တစ်ခုကျလာပါလိမ့်မယ်။ sub menu ထဲတွင် ၎င်း account နှင့် ပတ်သက်ပြီး လုပ်ဆောင်နိုင်မယ့်လုပ်ငန်းစဉ်တွေကိုဖော်ပြထားပါတယ်။

Set password

Password မေ့သွားပြီး logon ဝင်ရောက်၍ မရနိုင်သော user များအတွက် administrator မှ password အသစ်တစ်ခု ပြောင်းလဲသတ်မှတ်ဖို့ လိုလာတဲ့အခါမျိုးမှာ ဒီ set password ကို အသုံးပြု၍ ဖြေရှင်းနိုင်ပါတယ်။

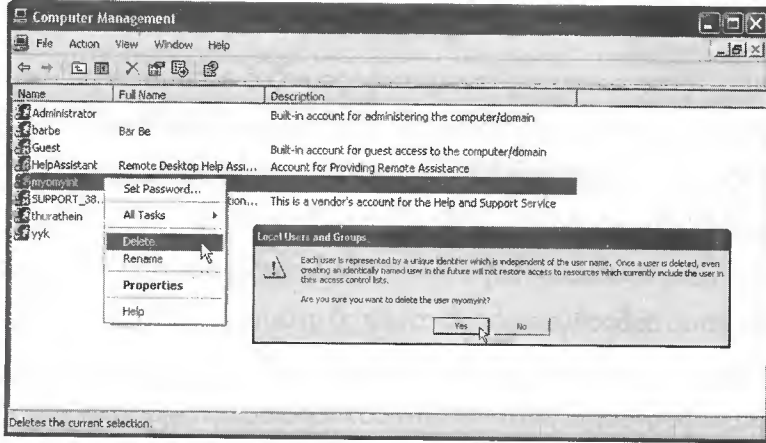
password ပြောင်းဖို့ရန် လိုအပ်နေသော account ပေါ်တွင် right click နှိပ်ပါ။ ကျလာမည့် submenu ထဲရှိ **Set Password** တွင် click နှိပ်ပါက password ပြောင်းခြင်းနှင့် ပတ်သက်ပြီး သတိပေးချက်များပါသော warning message ကျလာပါလိမ့်မယ်။ **Proceed** button တွင် click တစ်ချက်နှိပ်ပါ။ ထို့နောက် new password နှင့် confirm password တို့ကိုရိုက်ထည့်ပြီး **Ok** button တွင် click နှိပ်ပါ။



Deleting User Account

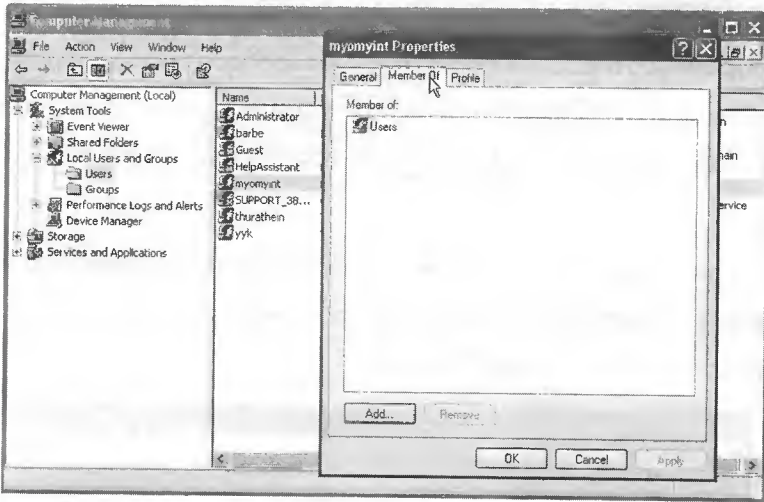
Account တစ်ခုကို ဘယ်တော့မှ ထပ်မံအသုံးပြုဖို့ရန်မလိုအပ်တော့ဘူးဆိုရင် ၎င်း account ကို ဖျက်ထုတ်သင့်ပါတယ်။ ဖျက်ထုတ်လိုသော account ပေါ်တွင် right click နှိပ်ပါ။ ကျလာမည့် submenu ထဲရှိ **Delete** တွင် click နှိပ်ပါ။

account ကိုဖျက်ထုတ်ဖို့ရန် အတည်ပြုချက်တောင်းခံပါလိမ့်မည်။ **YES** button တွင် click နှိပ်ပါက ၎င်း account ကို ဖျက်ထုတ် ပေးသွားပါလိမ့်မည်။



● User Properties

Properties တွင် click နှိပ်ပါက tab သုံးခုပါသော "user properties" dialog box ပွင့်လာပါလိမ့်မည်။ "general" tab အောက်မှာဆိုရင် account ကို create လုပ်ခဲ့တဲ့ အခါတုန်းက အတိုင်းပင် password never expire၊ account disable အစရှိသည့် option များပင်ပါရှိပြီး ၎င်း option များကို ပြောင်းလဲလိုက ဒီနေရာမှ ပြန်လည်သတ်မှတ်ပေးနိုင်ကြပါတယ်။



"member of" tab အောက်ကိုကြည့်မယ်ဆိုရင် user သည် ဘယ် group အောက်မှာပါသလဲဆိုတာကို သိနိုင်ပါတယ်။ ပုံမှန် default အားဖြင့် account သစ်တစ်ခုကို ဆောက်ပြီးတိုင်း user ဆိုတဲ့ group ထဲကိုသာ ထည့်သွင်းပေးထားမှာဖြစ်ပါတယ်။ user group ထဲမှာရှိသော account များသည် limited account အမျိုးအစားများပင် ဖြစ်ကြပါတယ်။ အကယ်၍ ၎င်း account ကို administrator အဖြစ်ပြောင်းလိုပါက **Add** button တွင် click နှိပ်ပြီး administrator group ထဲသို့ ထည့်သွင်းပေးနိုင်ပါတယ်။ ဒါဆိုရင် account သည် group ၂ ခု (user နှင့် administrator) အောက်တွင် ရောက်ရှိသွားပြီး ၎င်း group ၂ ခုလုံး၏ လုပ်ပိုင်ခွင့်များကို ရရှိသွားပြီဖြစ်ပါတယ်။

Creating and Managing Groups

Group ဆိုတာကတော့ အခွင့်အရေး အတူတူပေးလိုတဲ့ account တွေကို စုစည်းထားတဲ့ အုပ်စုကလေးများပဲဖြစ်ပါတယ်။ ဆိုရရင် group တစ်ခုမှာ member အဖြစ်ပါဝင်တဲ့ account အားလုံးတို့သည် တူညီသော လုပ်ပိုင်ခွင့်များကို ရရှိကြမှာဖြစ်ပါတယ်။ အဲဒီလို group တွေကို တည်ဆောက်အသုံးပြုခြင်းအားဖြင့် account တွေကို စီမံထိန်းချုပ်တဲ့နေရာမှာ ပိုမို လွယ်ကူစေပါတယ်။

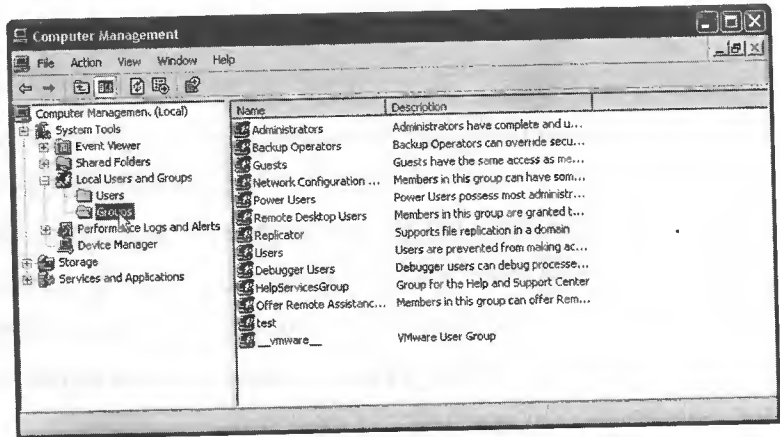
ဆိုရရင် user ဆယ်ယောက်ကို တစ်ယောက်ချင်းလိုက်၍ permission ပေးနေမယ့်အစား ၎င်း၁၀ယောက်ကို group တစ်ခုထဲမှာ ထည့်သွင်းထားပြီး ထို group ကို permission သတ်မှတ်ပေးလိုက်ရုံ ဖြစ်ပါတယ်။ ထို့အတူ permission ပြောင်းလဲသတ်မှတ်ပေးလိုပါကလည်း user ၁၀ယောက်အတွက် ၁၀ကြိမ် လိုက်ပြောင်းစရာမလိုပဲ group ၏ permission ကိုသာ ပြောင်းပေးလိုက်ရုံဖြင့် ကိစ္စပြီးမြောက်စေပါတယ်။

Windows XP မှ administrator | Power User | User | Backup operator | Guest အစရှိတဲ့ group များ ပါရှိပြီး သားဖြစ်ပါတယ်။ ၎င်း built-in group တွေအတွက် သက်ဆိုင်ရာ permission များကိုလည်း window XP မှ အလိုအလျောက် သတ်မှတ်ပေးပြီး သားဖြစ်ပါတယ်။ ဒါ့အပြင်လည်းပဲ မိမိတို့ရဲ့ လိုအပ်ချက်ပေါ်မူတည်ပြီး group အသစ်များကို ထပ်မံထည့်သွင်း တည်ဆောက်အသုံးပြုနိုင်ကြပါသေးတယ်။

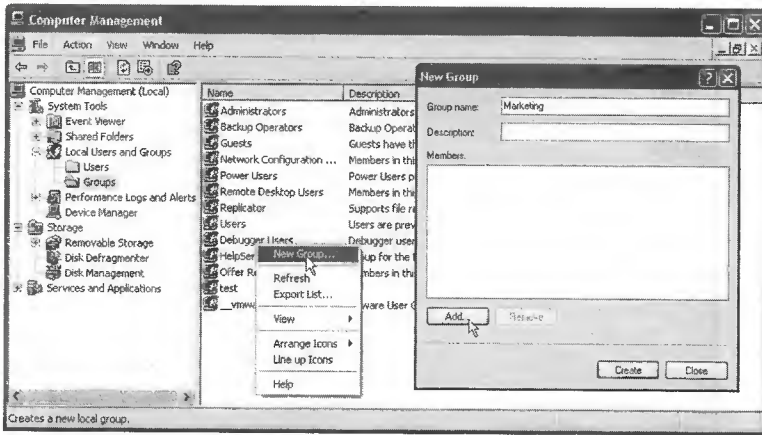
Creating Group

Group တစ်ခုကို တည်ဆောက်တဲ့နေရာမှာ လုပ်ဆောင်ရမယ့်အဆင့်များသည် account တစ်ခု တည်ဆောက်ပုံနှင့် များစွာ ကွာခြားမှု မရှိပါဘူး။ ဒါ့ကြောင့် ရှေ့မှာဖော်ပြခဲ့တဲ့ account create လုပ်ခြင်းကို ကျွမ်းကျင်ခဲ့မယ်ဆိုရင် group create လုပ်ခြင်းကို အခက်အခဲမရှိ အလွယ်တကူ လုပ်ဆောင်နိုင်ကြ ပါလိမ့်မယ်။

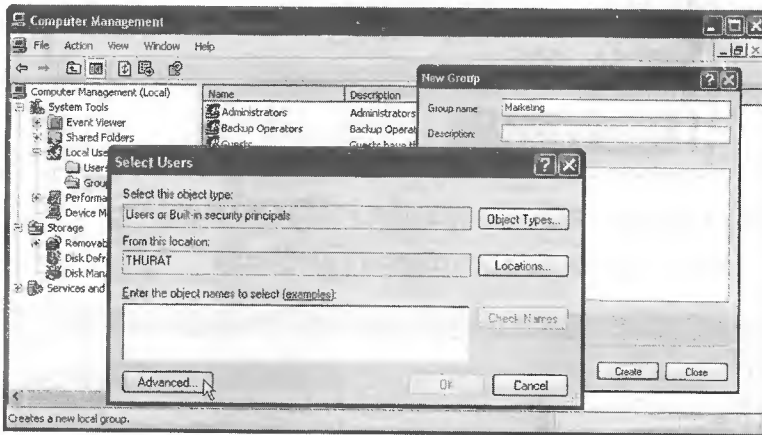
1) computer management window ၏ ဘယ်ဘက် tree view ထဲရှိ **system tools > users and groups > groups** တို့တွင် အဆင့်ဆင့်ဆန့်ထုတ်သွားပါက ညာဘက်ခြမ်းတွင် ကွန်ပျူတာမှာ create လုပ်ထားသော group list ကို တွေ့ရပါလိမ့်မယ်။



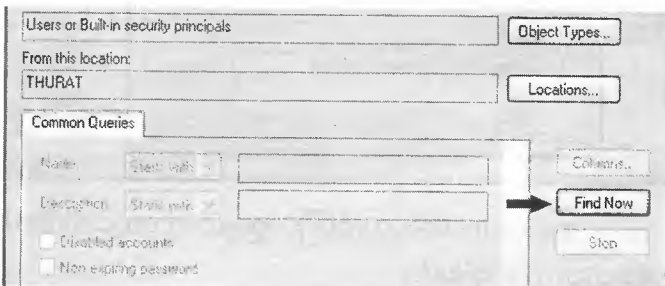
2) Group Listထဲရှိ create လုပ်ထားပြီးသော group တို့နှင့် လွတ်သည့် နေရာတွင် right click နှိပ်ပါ။ ကျလာမည့် submenu ထဲရှိ **new group** တွင် click နှိပ်ပါက "new group" dialog box ကျလာပါလိမ့်မယ်။



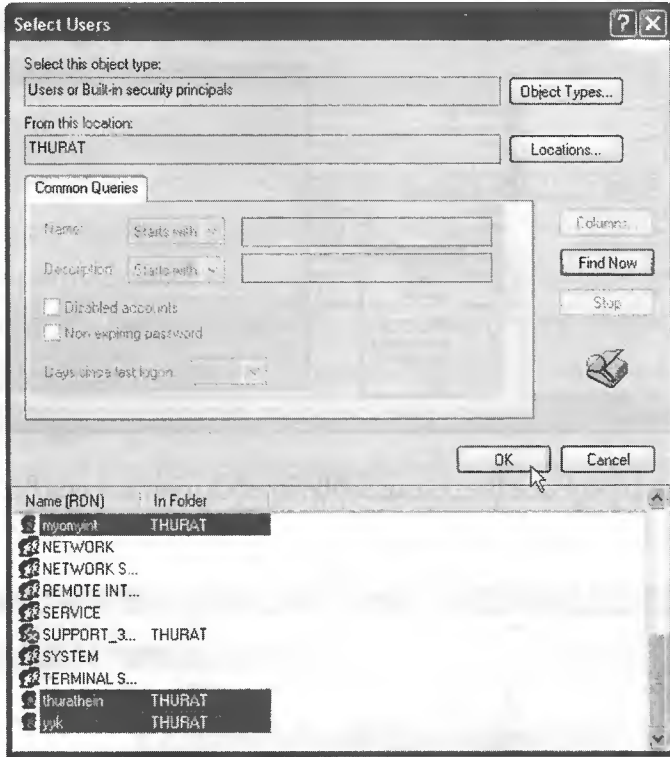
3) Group name နေရာတွင် ပေးလိုသော အမည်ကို ရိုက်ထည့်ပါ။ member များကို ထည့်ရန် အတွက်သာ **Add** တွင် click နှိပ်ပါက "select user" dialog box ကျလာပါလိမ့်မယ်။



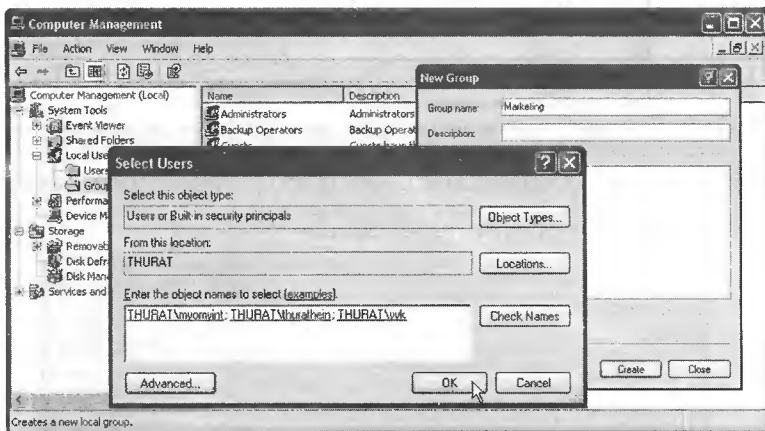
4) မိမိကွန်ပျူတာမှာ create လုပ်ထားသော account များကို ရှာဖွေရန် အတွက် **Advanced** button တွင် click နှိပ်ပါ။ "Find Now" button ပေါ်လာပါလိမ့်မည်။



5) **Find Now** button တွင် click နှိပ်ပါက မိမိကွန်ပျူတာမှာ create လုပ်ထားသော account အမည်များကိုဖော်ပြပါလိမ့်မယ်။

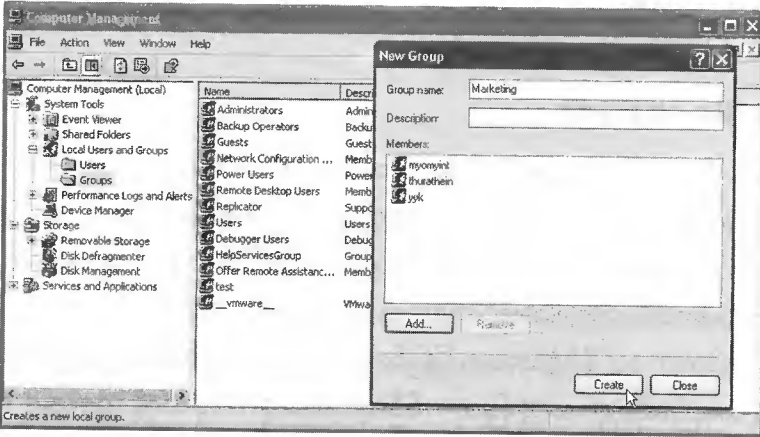


မိမိထည့်သွင်းလိုသော account ကို select လုပ်ပြီး **OK** button တွင် click နှိပ်ပါက ၎င်း account ကိုမူလ "select user" dialog box ထဲမှာဖော်ပြပါလိမ့်မယ်။

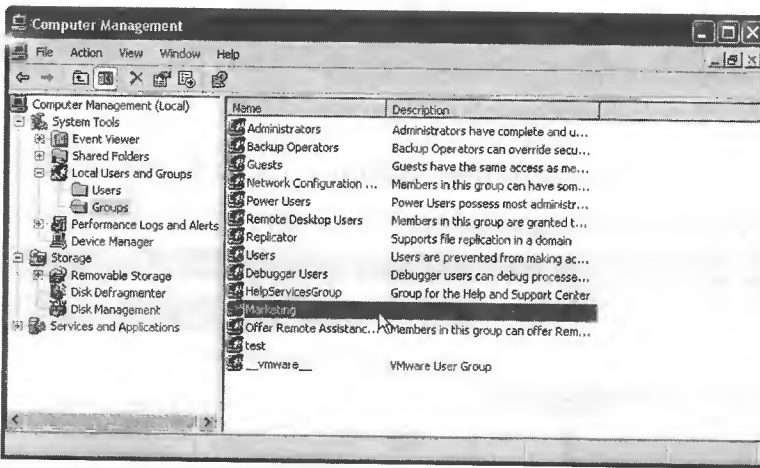


မှတ်ချက်။ ။ account တစ်ခုထက်ပိုပြီး ရွေးချယ်ထည့်သွင်းလိုပါက keyboard မှ control key ကိုနှိပ်ထားပြီး click ကိုနှိပ်ရပါမယ်။

6) OK button တွင် ထပ်မံ click နှိပ်ပါက မိမိရွေးချယ်ခဲ့သော account များကို member list ထဲမှာ တွေ့ရပါတယ်။ အကယ်၍ များမှားယွင်းထည့်သွင်းခဲ့မိခြင်းကြောင့် ပြန်လည်ဖျက်ထုတ်လိုပါက ဖျက်ထုတ်လိုတဲ့ account ကို select လုပ်ပြီး **Remove** တွင် click နှိပ်လိုက်ရုံဖြစ်ပါတယ်။



7) Account တွေကို ထည့်သွင်းပြီး ပြီဆိုရင် **Create** button တွင် click နှိပ်ပါက မိမိ create လုပ်ခဲ့သော group အသစ်ကို computer management ရှိ group list ထဲတွင် တွေ့ရပါလိမ့်မယ်။



မှတ်ချက်။ ။ တည်ဆောက်ခဲ့ပြီးသော group ထဲသို့ user အသစ်များ ထပ်ထည့်ခြင်း၊ အမည်ပြောင်းခြင်း၊ ဖျက်ထုတ်ခြင်းများကို user account များကို manage လုပ်စဉ်က အတိုင်း group အမည်တစ်ခုကို ရွေးချယ် right click နှိပ်ပြီး လုပ်ဆောင်နိုင်ကြပါတယ်။

File and Printer Sharing

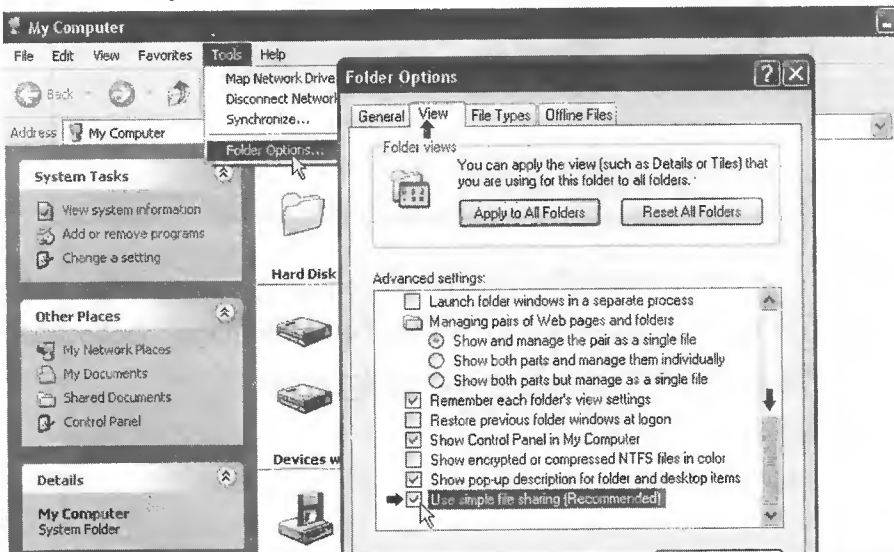
network ပေါ်မှာ file တွေ shareပေးခြင်းကိုနည်းလမ်း ၂မျိုးထဲကတစ်မျိုးမျိုးဖြင့်လုပ်ဆောင်နိုင်ပါတယ်။ထိုနည်းလမ်း ၂မျိုးကတော့ **simple file sharing** နှင့် **standard file sharing**တို့ပဲဖြစ်ပါတယ်။

simple file sharing

simple file sharing ဖြင့် file တွေ၊ folder တွေကို share ပေးခြင်းသည် အလွယ်ကူဆုံးနည်းလမ်းတစ်ခု ဖြစ်ပါတယ်။ ဆိုရရင် folder တစ်ခုကို share ပေးရန်အတွက် check box တစ်ခုကို ရွေးချယ်ပေးရုံဖြင့် window XP မှ သတ်မှတ်ပေးသော permission များဖြင့် အလိုလျောက် share လုပ်ပေးသွားမှာဖြစ်ပါတယ်။ အဲဒီလိုနည်းနှင့် share ပေးထားတဲ့ folder ထဲက file တွေကို network ပေါ်မှာ မည်သူမဆိုအလွယ်တကူ ဖတ်နိုင်ရုံသာမက ပြုပြင်ပြောင်းလဲခြင်း၊ ဖျက်ထုတ်ခြင်းများကိုပါ လုပ်ဆောင်နိုင်စေပါတယ်။ တနည်းဆိုရရင် အသုံးပြုသူတစ်ဦးချင်းစီအလိုက် လိုသလို အသေးစိတ်၊ အတိအကျ ကန့်သတ်၍ မရနိုင်သည့်အတွက် secure မဖြစ်ဘူးလို့ လည်း ဆိုနိုင်ပါတယ်။ သို့သော်လည်း security သိပ်အရေးမကြီးတဲ့ home network မျိုးတွေအတွက်ကတော့ လွန်စွာအသုံးတည့်သည့်နည်းလမ်းကောင်းတစ်ခုဖြစ်ပါတယ်။

folder တစ်ခုကို share မလုပ်ခင်ပထမဦးဆုံးအနေနှင့်မိမိကွန်ပျူတာမှာ simple file sharing အားရွေးချယ်ထားခြင်း ရှိမရှိဆိုတာကို စစ်ဆေးပြီး လိုအပ်ပါက **on/off** လုပ်ခြင်းကို အောက်ဖော်ပြပါ အဆင့်များအတိုင်း လိုက်ပါလုပ်ဆောင်ရန်လိုအပ်ပါတယ်။

1) Explorer window ရှိ **tools > folder option** တွင် click တစ်ချက်နှိပ်ပါ (သို့) control panel ထဲရှိ **folder option** တွင် double click နှိပ်ပါ။ "Folder Option" window ဖွင့်လာပါလိမ့်မည်။



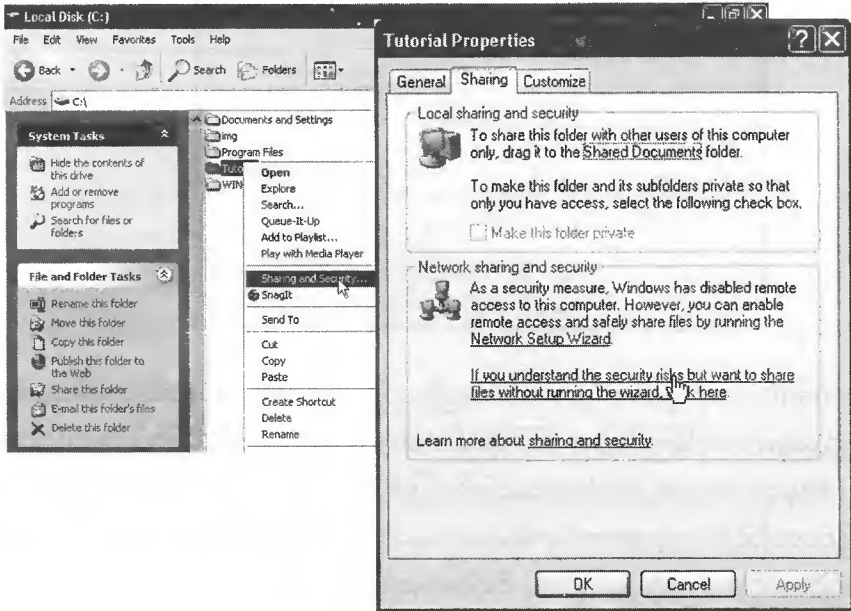
2) folder option dialog box ၏ **view** tab အောက်ရှိ advanced setting ဘေးမှ scroll bar ကိုအောက်သို့ဖွဲ့ချပါ။

3) use simple file sharing ဘေးရှိ checkbox ထဲတွင် အမှန်ဖြစ်ပေါ်အောင် click တစ်ချက်နှိပ်၍ on ပေးရပါမယ်။ (အလားတူပင် simple file sharing ကိုပိတ်လိုပါတာ (မသုံးလိုပါက) check box ထဲရှိ အမှန်ဖြစ်ကိုဖြုတ်ပေးရပါမယ်။)

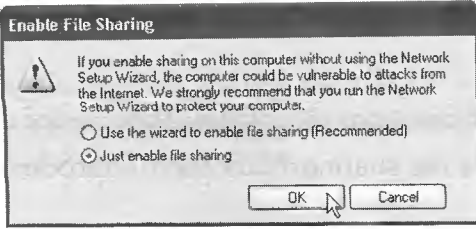
● **Sharing Your own folder**

share folder တစ်ခုကိုဆောက်ရန်အတွက် ကွန်ပျူတာ အတွင်းသို့ login ဝင်ရောက်မည့် account သည် administrator နှင့် power user group ထဲမှတစ်ခုခုဖြစ်ရပါမယ်။ သို့မှသာ disk တစ်ခုလုံးကိုဖြစ်စေ၊ folder တစ်ခုခုကိုဖြစ်စေ မိမိလိုသလိုရွေးချယ် share ပေးနိုင်မှာဖြစ်ပါတယ်။ အကယ်၍များ limited account တစ်ခုဖြင့် log in ဝင်ရောက်မယ်ဆိုပါက access လုပ်ခွင့်ပေးထားသော folder အချို့ကိုသာ share လုပ်နိုင်မှာဖြစ်ပါတယ်။

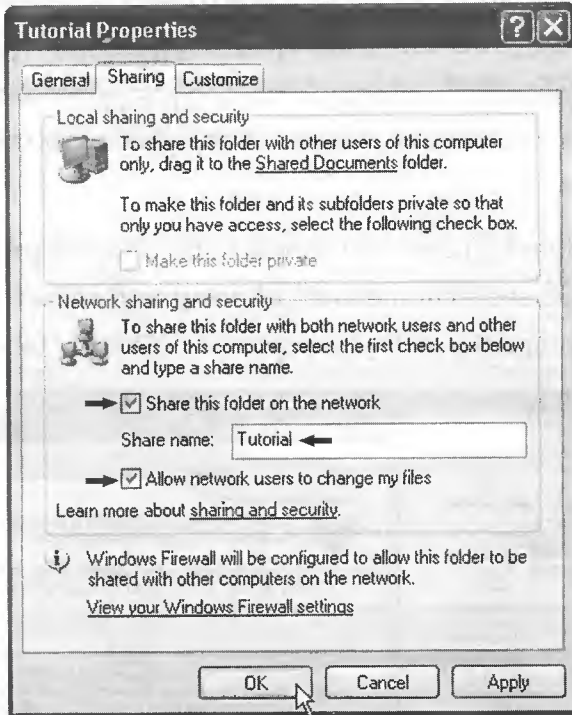
1) share ပေးလိုသော folder (သို့) disk icon ပေါ်တွင် right click တစ်ချက်နှိပ်ပါ။ short cut menu တစ်ခုကျလာပါလိမ့်မည်။ short cut menu ထဲရှိ **sharing and security** ကိုရွေးချယ် click နှိပ်ပါ။ sharing tab ပါသော properties dialog box ကျလာပါမယ်။ 'Sharing' tab တွင် တစ်ချက်နှိပ်ပါ။



2) sharing tab အောက်တွင်ရှိသောလင်းသားထားသော "If you understand the security . ." ပေါ်တွင် click တစ်ချက်နှိပ်ပါ။ ကျလာမည့် box ထဲရှိ just enable file sharing ကိုရွေးချယ်ပြီး **OK** button တွင် click နှိပ်ပါ။



3) Network sharing and security ရှိ share this folder on the network ဘေးရှိ checkbox ထဲတွင် အမှန်ဖြစ်ပေါ်အောင် click နှိပ်၍ ရွေးချယ်ပေးရပါမည်။



4) share name နေရာတွင် ဖော်ပြထားတဲ့ အမည်သည် network ပေါ်မှ တစ်စုံတစ်ယောက်သည် မိမိ ကွန်ပျူတာကို browse လုပ်ကြည့်တဲ့အခါ မြင်ရမည့် share folder အမည်ပင်ဖြစ်ပါတယ်။ (ဥပမာပုံအရ - Tutorial)။ ဒီနေရာမှ share folder အမည်ကို ပြောင်းလိုက ပြောင်းပေးနိုင်ပါတယ်။ သို့သော် အဲဒီလို ပြောင်းပေးခြင်းအားဖြင့် မိမိကွန်ပျူတာထဲမှာရှိနေသော မူရင်း folder အမည် ပြောင်းလဲမှုရှိမှာ မဟုတ်ဘဲ network ပေါ်မှ မြင်ရမည့် အမည်ကိုသာလျှင် ပြောင်းလဲပေးမှာ ဖြစ်ပါတယ်။

5) Network user များအား မိမိရဲ့ share folder နှင့် ၎င်း folder ထဲမှာရှိတဲ့ subfolder များ၊ file များကို ဖတ်ခွင့်ပေးမယ်။ ဒါပေမယ့် ပြင်ဆင်ခြင်း၊ ထပ်ထည့်ခြင်း အမည်ပြောင်းခြင်းတွေကို ပေးမလုပ်လိုဘူးဆိုရင် allow network ဘေးရှိ checkbox ကို clear လုပ်ပေးရပါမယ်။ အကယ်၍ allow network ဘေးရှိ

checkbox ကို on ထားခဲ့မယ်ဆိုရင် network ပေါ်မှ တစ်ယောက်ယောက်သည် မိမိကွန်ပျူတာကို ချိတ်ဆက်ပြီး share ပေးထားတဲ့ folder (သို့) disk ထဲရှိ file များကို ပြင်ဆင်ခြင်း၊ ဖျက်ပစ်ခြင်းများကို လုပ်ဆောင်နိုင်ပါလိမ့်မယ်။

6) **OK** buttonတွင် click နှိပ်ပါက disk (သို့) folder ကို share လုပ်ခြင်းပြီးဆုံးသွားပြီး network user အားလုံးတို့သည် my network place မှ တဆင့် မိမိ၏ share folder များကို ရှာဖွေကြည့်ရှု နိုင်ကြပြီ ဖြစ်ပါလိမ့်မည်။

Standard File Sharing

standard file sharing သည် simple file sharing ထက် အနည်းငယ် ပိုမိုရှုပ်ထွေးပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ simple file sharing မှာကဲ့သို့ အားလုံးကို တပြေးညီ အသုံးပြုခွင့် မပေးပဲ share folder တစ်ခုတည်းကိုပင် ဘယ် user တွေကိုတော့ read ရှု သက်သက်၊ ဘယ် user တွေကတော့ read လို့လည်းရမယ်၊ write လို့လည်းရမယ် အစရှိသဖြင့် လိုသလို ကန့်သတ်ပေးနိုင်သောကြောင့် ဖြစ်ပါတယ်။

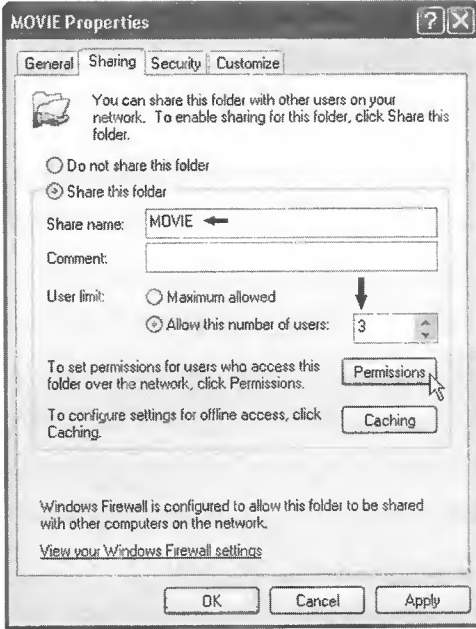
ထို့အတူ folder တစ်ခုကို share ပေးတဲ့နေရာမှာ လုပ်ဆောင်ရမယ့် အဆင့်အတော်များများသည် simple file sharing မှာကဲ့သို့ပင် ဖြစ်သော်လည်း အချို့သော အဆင့်တွေဖြစ်တဲ့ network user တွေထဲမှ ဘယ်သူတွေသည် share ပေးထားတဲ့ folder ကို access လုပ်ခွင့်ရှိမလဲနှင့် ဘယ်လောက်အတိုင်းအတာ (read၊ modify၊ full access) ထိ အသုံးပြုခွင့်ပေးမှာလဲ အစရှိသည်တို့အတွက် လုပ်ဆောင်ရမယ့် အဆင့်တွေပိုလာမှာ ဖြစ်ပါတယ်။ ဒါ့ကြောင့် standard share file ဖြင့် share ပေးပုံများကို share the folder နှင့် restric the share folder ဟူ၍ ဂရုစိုက်ခြင်းဖြင့် သွားမှာ ဖြစ်ပါတယ်။

မှတ်ချက်။ folder (သို့) disk တစ်ခုကို standard file sharing ဖြင့် share မပေးခင် မိမိကွန်ပျူတာမှာ simple file sharing ကို off လုပ်ထားခဲ့ရမှာ ဖြစ်ပါတယ်။ (စာမျက်နှာ ၁၇၂ တွင် ကြည့်ပါ)

Sharing the Folder

1) share ပေးလိုသော folder (သို့) disk တွင် right click တစ်ချက်နှိပ်ပါ။ shortcut menu တစ်ခုကျလာပါလိမ့်မည်။ shortcut menu ထဲရှိ **sharing and security** ကို ရွေးချယ် click နှိပ်ပါက sharing tab ပါသော properties dialog box ကျလာပါလိမ့်မည်။ ဒီနေရာမှာ မြင်ရမည့် sharing tab သည် simple file sharing မှာတုန်းက မြင်ရသည့် sharing tab နှင့် အနည်းငယ် ကွဲပြားနေတာကို တွေ့ရပါ လိမ့်မယ်။

2) **Share this folder** ဘေးရှိ radio button ပေါ်တွင် click နှိပ်၍ ဖြစ်အောင် select လုပ်ပါ။ အခြားရွေးချယ်စရာ option များပါ active ဖြစ်လာပါလိမ့်မည်။



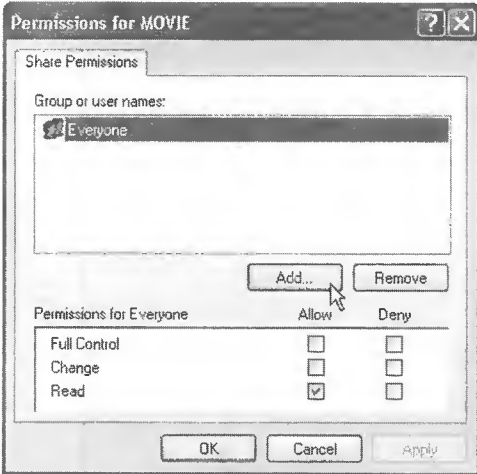
Share Name - networkပေါ်မှာမြင်ရမည့်share folderအမည်ကိုပြောင်းလိုပါကဤနေရာတွင်ပြောင်းပေးနိုင်ပါသည်။ဥပမာပုံအရ - **MOVIE**

User Limit - မိမိကွန်ပျူတာ၏share folderများကိုတပြိုင်နက်ချိတ်ဆက်အသုံးပြုနိုင်မည့်network userအရေအတွက်ကိုကန့်သတ်လိုပါက "allow this number of users" ဘေးရှိ radio buttonကို ဖြစ်အောင် select လုပ်ပြီး userအရေအတွက် (ဥပမာ - 3 or 4) ကန့်သတ်ထည့်သွင်းပေးနိုင်ပါတယ်။ ပုံမှန် defaultအားဖြင့် maximum allowကို ရွေးချယ်ထားပြီးဘေးဖြစ်ပြီးအများဆုံး user၁၀ဦးထိတပြိုင်နက်ဝင်ရောက်အသုံးပြုနိုင်မှာဖြစ်ပါတယ်။ တပြိုင်နက် ချိတ်ဆက် အသုံးပြုသူ အရေအတွက် များလာတာနှင့်အမျှ မိမိကွန်ပျူတာ၏လုပ်ဆောင်မှုအမြန်နှုန်းလည်းကျဆင်းလာမှာဖြစ်ပါတယ်။

Restricting the share folder

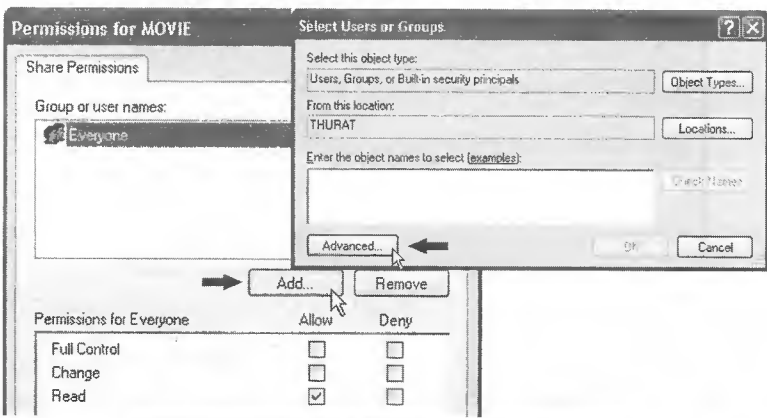
သာမန် shareပေးရုံသာသက်သက်ဆိုရင် step2 ပြီးကတည်းက **OK** buttonတွင် clickနိုင်ပြီး share ပေးခြင်းကို အဆုံးသတ်နိုင်ပါတယ်။ ဒီလိုသာ အဆုံးသတ်ခဲ့မယ်ဆိုရင် everyone လို့ခေါ်တဲ့ အသုံးပြုသူမည်သူမဆို Read Accessရရှိမှာဖြစ်သည့်အတွက် share folderထဲရှိ fileများကိုဖွင့်ဖတ်နိုင်စေပါလိမ့်မယ်။ ဒီလိုမှမဟုတ်ပဲ ဘယ်သူတွေကိုတော့ ပြင်ဆင်ဖြည့်စွက်ခွင့်ပေးမယ် ၊ ဘယ်သူတွေကိုတော့ ဖျက်ထုတ်ခွင့်ပေးမယ် အစရှိတဲ့အသုံးပြုသူတစ်ဦးချင်းစီအလိုက်အကန့်အသတ်ဖြင့်ခွင့်ပြုလိုတယ်ဆိုရင်တော့ ဆက်လက်ဖော်ပြသွားမည့်အဆင့်များကိုပါ လုပ်ဆောင်ခဲ့ဖို့လိုပါလိမ့်မယ်။

3) sharing tab အောက်တွင် ရှိသော **permission** button တွင် click တစ်ချက် နှိပ်ပါ "permission" dialog box ကျလာပါလိမ့်မည်။ ၎င်း permission dialog box ရဲ့အပေါ်ပိုင်းတွင် ယခုလက်ရှိ permission ပေးထားသော account (သို့) group တို့ကို တန်းစီ ဖော်ပြထားသည့် list ကိုတွေ့ရပါလိမ့်မည်။ အောက်ဖက်ပိုင်းမှာတော့ account (သို့) group တစ်ခုစီအတွက် ဘယ်လို permission မျိုးပေးထားသလဲ ဆိုတာကိုဖော်ပြထားပါလိမ့်မည်။



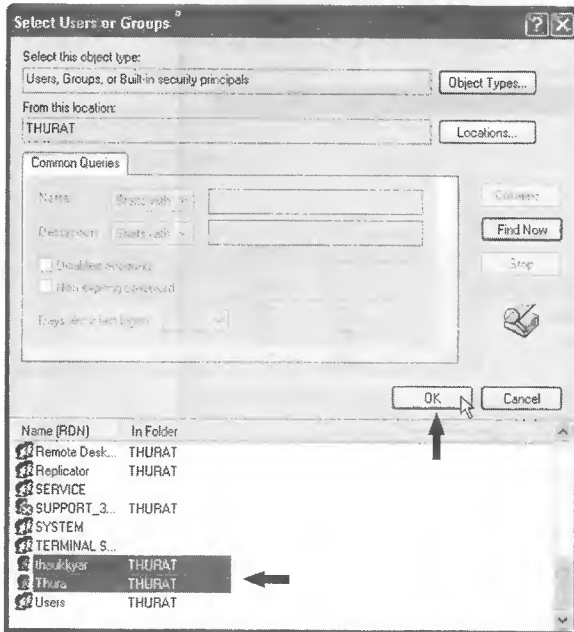
folder ကို ယခုမှတစ်ဆင့် share ပေးတဲ့အခါ everyone ဆိုတဲ့ group တစ်ခုတည်းကိုသာလျှင် list ထဲမှာတွေ့ရမှာဖြစ်ပြီး ပုံမှန် default အားဖြင့် ၎င်း Everyone group အတွက် permission သည် Read only ဖြစ်ပါတယ်။ သဘောကတော့ အသုံးပြုသူမည်သူမဆို ဒီ share folder ထဲမှာရှိတဲ့ file တွေကို ဖတ်ခွင့်သာ ရှိတယ်လို့ ဆိုလိုပါတယ်။ အဲဒီလိုမျိုးအားလုံးကို တပြေးညီတော့မပေးလိုဘူး။ အချို့ကို Read ပေးမယ်။ အချို့ကို Write ပေးမယ်အစရှိသဖြင့် တစ်ဦးချင်းစီ အလိုက်ခွင့်ပြုမယ်ဆိုရင် user account များ၊ group များ၊ permission များကို ပြင်ဆင်ပစ်ရပါမယ်။

4) account (သို့) group များကို ထပ်တည့်ရန်အတွက် **Add** button တွင် click နှိပ်ပါ။ "Select Users and Groups" dialog box ကျလာပါလိမ့်မည်။

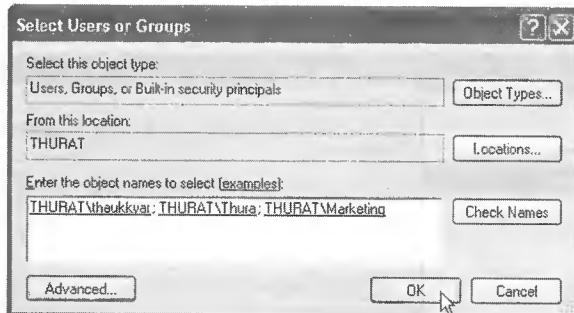


8) မိမိကွန်ပျူတာတွင် create လုပ်ထားသော account များ၊ group များကို ရှာဖွေရန်အတွက် **Advanced** button တွင် click နှိပ်ပါ။ "Find Now" button ပေါ်လာပါလိမ့်မည်။

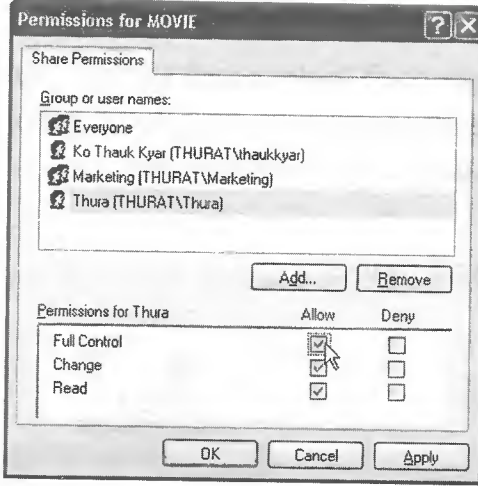
9) **Find Now** တွင် click နှိပ်ပါက မိမိကွန်ပျူတာမှာ create လုပ်ထားသော account များ၊ group များကို ရှာဖွေဖော်ပြပါလိမ့်မည်။



မိမိထည့်သွင်းလိုသော account (သို့) group တစ်ခုကို select လုပ်ပြီး ok button တွင် click နှိပ်ပါက ၎င်း account (သို့) group ကို မူလ "Select Users and Group" ထဲမှာ ဖော်ပြပါလိမ့်မည်။ (account တခုထက် ပိုပြီး ရွေးချယ် select လုပ်လိုပါက keyboard မှ 'Ctrl' key နှင့် တွဲနှိပ်ပြီး click နှိပ်ရပါမည်)



10) **OK** button တွင် ထပ်မံ click နှိပ်ပါက မိမိရွေးချယ်ခဲ့သော account (သို့) group ကို permission dialog box ထဲမှာ တွေ့ရပါမည်။ အကယ်၍ များ မှားယွင်း ထည့်သွင်းခဲ့မိခြင်းကြောင့် ပြန်ဖယ်ထုတ်လိုလျှင်လည်း ဖယ်ထုတ်လိုတဲ့ account ကို select လုပ်ပြီး **Remove** တွင် click နှိပ်လိုက်ရုံ ဖြစ်ပါတယ်။



11) account (သို့) group တွေကို ရွေးချယ် ထည့်သွင်းခဲ့ပြီးပြီဆိုရင် ၎င်း account (သို့) group တစ်ခုစီ အတွက် ခွင့်ပြုလိုသော permission များကို စတင်သတ်မှတ်ပေးနိုင်ပါပြီ။ list ထဲမှ account (သို့) group အမည်တစ်ခုခုကို select လုပ်ပြီး permission သုံးမျိုးထဲမှ ရွေးချယ်သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။

Read - "Read" permission ရရှိထားတဲ့ account ပိုင်ရှင်များသည် share folder ထဲတွင် ရှိသမျှတို့ကို ဖတ်နိုင်ပါတယ်။ ဒါပေမယ့် ပြင်ဆင်ခြင်း၊ အမည်ပြောင်းခြင်း၊ ဖျက်ခြင်းများကို ပြုလုပ်၍ မရပါ။

Change - "change" permission ရရှိထားသော account ပိုင်ရှင်များသည် share folder ထဲတွင် ရှိသမျှ file များကို ဖတ်ရုံမျှသာမက တော့ပဲ လိုသလိုပြင်ဆင် သိမ်းဆည်းခြင်း၊ အမည်ပြောင်းခြင်း၊ ဖျက်ထုတ်ပစ်ခြင်းများကို ပြုလုပ်နိုင်ကြပါတယ်။ ဒါ့အပြင်လည်းပဲ အခြား file များ၊ folder များကို share folder အတွင်း ထပ်မံ ထည့်သွင်းခြင်းများကိုလည်း လုပ်ဆောင်နိုင်ပါလိမ့်မယ်။

Full Control - full control သည် အမြင့်ဆုံး permission ဖြစ်ပါတယ်။ file တွေကို ဖျက်ရုံ၊ အမည်ပြောင်းနိုင်ရုံမျှမက share folder ၏ permission ပြောင်းခြင်းနှင့် ownership ယူခြင်းများအထိပါ လုပ်ဆောင်နိုင်စေပါတယ်။ ဒါကြောင့် account တစ်ခုကို full control မပေးခင် သေသေချာချာ စဉ်းစားဖို့ လိုပါတယ်။

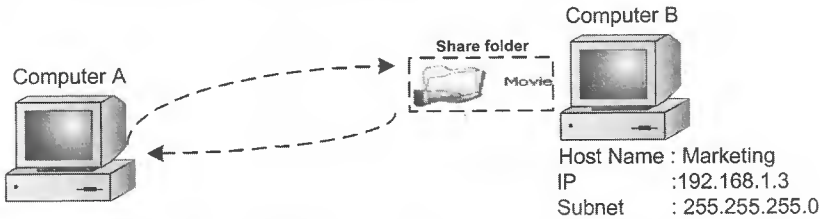
ပုံမှန် default အားဖြင့် အသစ်ထပ်မံ ထည့်သွင်းလိုက်သော account များသည် read permission ကိုသာ ရရှိမှာဖြစ်ပါတယ်။ full control ပေးလိုလျှင် account တစ်ခုစီကို ရွေးချယ်ပြီး full control ၏ Allow နေရာတွင် အမှန်ဖြစ်ပေါ်အောင် click နှိပ်၍ ရွေးချယ်ပေးရပါမယ်။

မှတ်ချက်။ ။ လူတိုင်းကို access လုပ်ခွင့်မပေးပဲ အသစ်ထည့်သွင်းထားသော account များကိုသာ ခွင့်ပြုလိုပါက Everyone ကို remove လုပ်ခဲ့ရပါမယ်။ network ပေါ်မှ အသုံးပြုသူသည် သူ့ကိုမဆို read ပေးချင်တယ်ဆိုရင် everyone ကို read access ပေးရမှာ ဖြစ်ပါတယ်။

Accessing Shared Folder

network ပေါ်မှာ share ပေးထားတဲ့ folder တွေကို နည်းလမ်း ၂မျိုးဖြင့် လှမ်း access လုပ်နိုင်ကြပါတယ်။ ဥပမာပုံအရ ကွန်ပျူတာ B မှာ share ပေးထားသည့် Movie ဆိုတဲ့ Folder ကို ကွန်ပျူတာ A မှ လှမ်း access လုပ်ပုံကို ဥပမာပေးဖော်ပြသွားမှာဖြစ်ပါတယ်။

- Using UNC Path
- Browsing via "my network places"



Using UNC Path

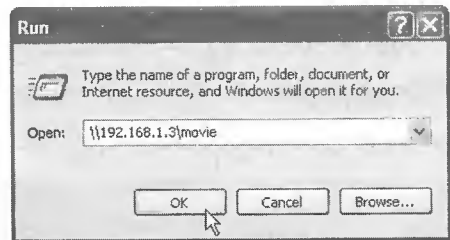
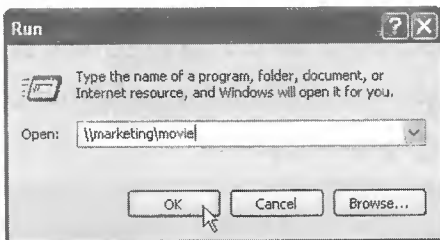
Universal Naming Convention (UNC) path ကို သုံးပြီး access လုပ်မယ်ဆိုရင်ပထမဦးစွာ "Run" program ကို အရင်ဖွင့်ရပါမယ်။ **Start > Run** တွင် click နှိပ်ပါ။ ပြီးရင် မိမိလှမ်းသုံးလိုတဲ့ share folder ရှိရာ လမ်းကြောင်းကို ရိုက်ထည့်ပေးရပါမယ်။ အဲဒီလိုလမ်းကြောင်းကို ရိုက်ထည့်တဲ့နေရာမှာ ရိုက်ချင်သလို ရိုက်လို့တော့မရပါဘူး။ ပုံစံရှိပါတယ်။ ထိုပုံစံကို UNC format လို့ခေါ်ပါတယ်။

- \\computer name\ share folder
- \\IP address\ share folder

ဥပမာ ကွန်ပျူတာ A မှာ log on ဝင်ရောက် အသုံးပြုနေသူ တစ်ဦးက ကွန်ပျူတာ B မှ share ပေးထားသော movie ဆိုတဲ့ folder ကို လှမ်းဖွင့်ကြည့်လိုတဲ့အခါမျိုးမှာ အောက်ပါ format အတိုင်း ရိုက်ထည့်ရပါမယ်။

\\marketing\movie

\\192.68.1.3\movie

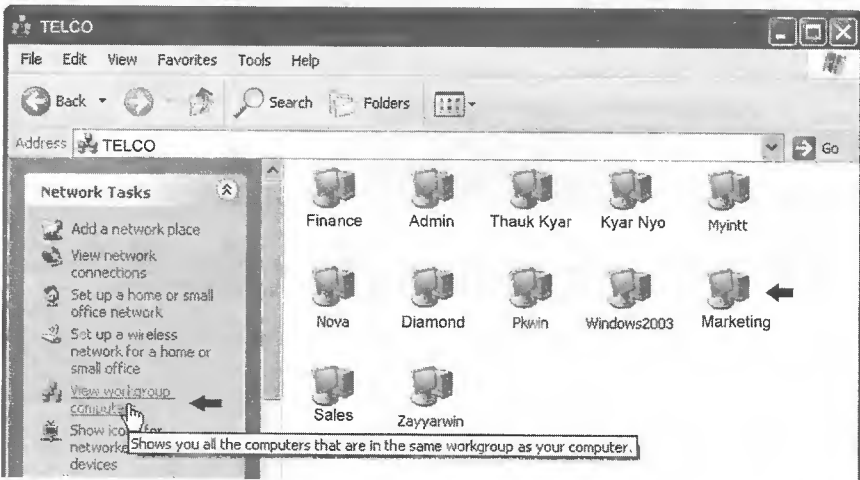


အရေးကြီးတာက share ပေးထားတဲ့ ကွန်ပျူတာ၏အမည် (သို့) IP Address ကို သိရပါမယ်။ နောက်တဆင့် share folder ရဲ့အမည်ကို သိမှသာလျှင် access လုပ်နိုင်ကြမှာဖြစ်ပါတယ်။

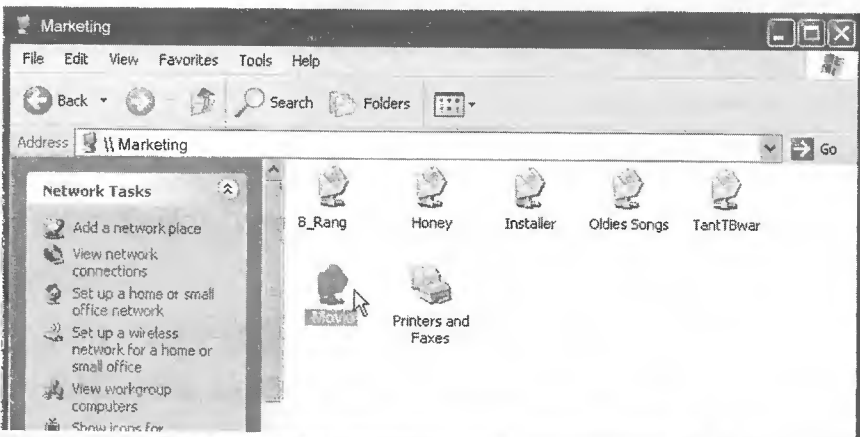
● Browsing Via "my network places" icon

ယခုဖော်ပြသွားမှာကတော့ "my network place" ကိုဖွင့်၍ share folder တွေကိုတဆင့်ပြီး တဆင့်ဝင်ရောက် ရှာဖွေ အသုံးပြုခြင်း ဖြစ်ပါတယ်။ ဤနည်းကို အသုံးပြုမယ်ဆိုရင် ကွန်ပျူတာအမည်နှင့် IP address တွေကို အလွတ်မှတ်မိဖို့ မလိုပါဘူး။ ကွန်ပျူတာအမည်ကိုတွေ့ရင် မိမိ access လုပ်လိုသော ကွန်ပျူတာဟုတ်မဟုတ်ဆိုတာလောက်ကိုခွဲခြားနိုင်ရင်ရပါပြီ။

- 1) Desktopပေါ်ရှိ **My Network Places** iconကို double click နှိပ်၍ဖွင့်ပါ။
- 2) "Network Tasks" အောက်ရှိ "View workgroup computers" ပေါ်တွင် click နှိပ်လိုက်ပါ။ မိမိနှင့်အတူ workgroup တစ်ခုတည်းအောက်မှာရှိနေသော ကွန်ပျူတာတွေရဲ့ list ကိုမြင်ရပါမယ်။



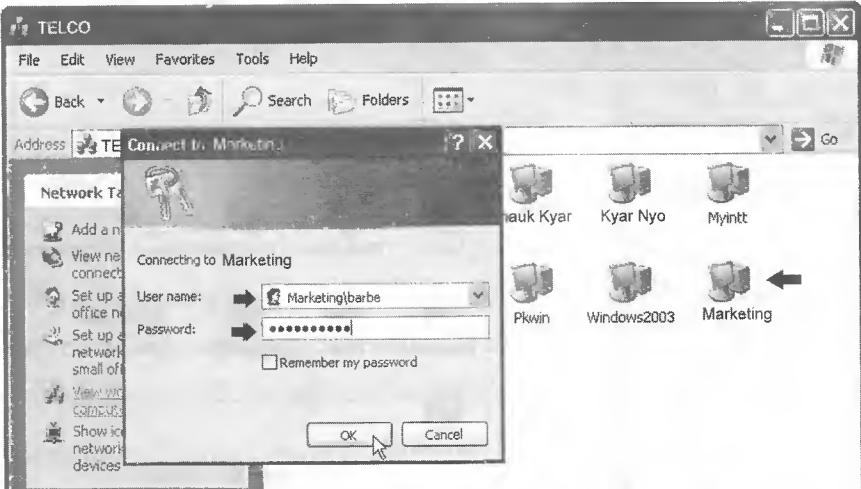
3) အသုံးပြုလိုသော share folder ရှိရာ ကွန်ပျူတာ အမည်ပေါ်တွင် double နှိပ်၍ဖွင့်ပါ။ မိမိမှာ ၎င်းကွန်ပျူတာကို လှမ်းဖွင့်ဖို့ရန် သင့်လျော်သော permission ရှိတယ်ဆိုရင် share ပေးထားတဲ့ folder တွေကိုတန်းစီမြင်ရပါမယ်။



ဒါက မိမိထိုင်သုံးနေသော ကွန်ပျူတာမှာ လက်ရှိ logon ဝင်ထားသော account သည် သင့်လျော်သော permission ရှိနေလို့ လွယ်လွယ်ကူကူတန်းမြင်ရခြင်းဖြစ်ပါတယ်။ အကယ်၍များ သင့်တင့်လျောက်ပတ်တဲ့ permission မရှိဘူးဆိုရင် အခြေအနေ ၂မျိုးနှင့် ကြုံရနိုင်ပါတယ်။ ပထမ အခြေအနေက user name နှင့် password တောင်းခံသော dialog box ကျလာခြင်းဖြစ်ပြီး၊ ဒုတိယ အခြေအနေက "access denied" ဆိုတဲ့ error message ကိုမြင်ရခြင်းဖြစ်ပါတယ်။

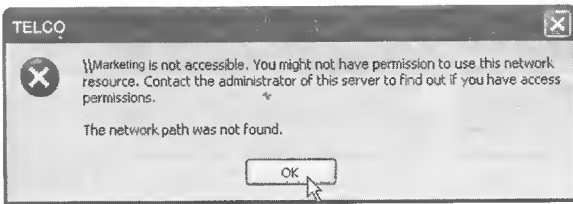
● User name နှင့် password တောင်းခြင်း

ဒီ dialog box ထဲမှာ access လုပ်ခွင့်ရှိတဲ့ account ၏ username နှင့် password တို့ကို ရိုက်ထည့်ရပါမယ်။ user name နေရာတွင် အောက်ဖော်ပြပါပုံစံအတိုင်းရိုက်ထည့်ရပါမယ်။



password နေရာတွင် ၎င်း account ၏ password ကိုရိုက်ထည့်ပါ။ **OK** တွင် click နှိပ်ပါက share ပေးထားသော folder များကိုမြင်ရပါမယ်။

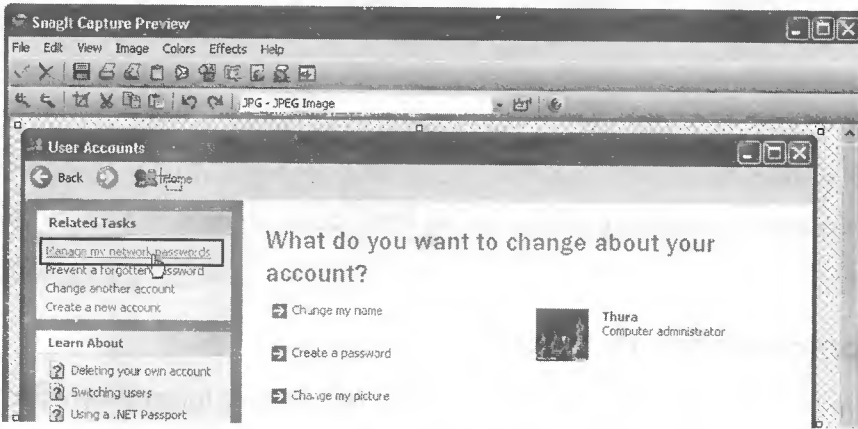
● "Access Denied" ဆိုတဲ့ error message ကိုမြင်ရခြင်း



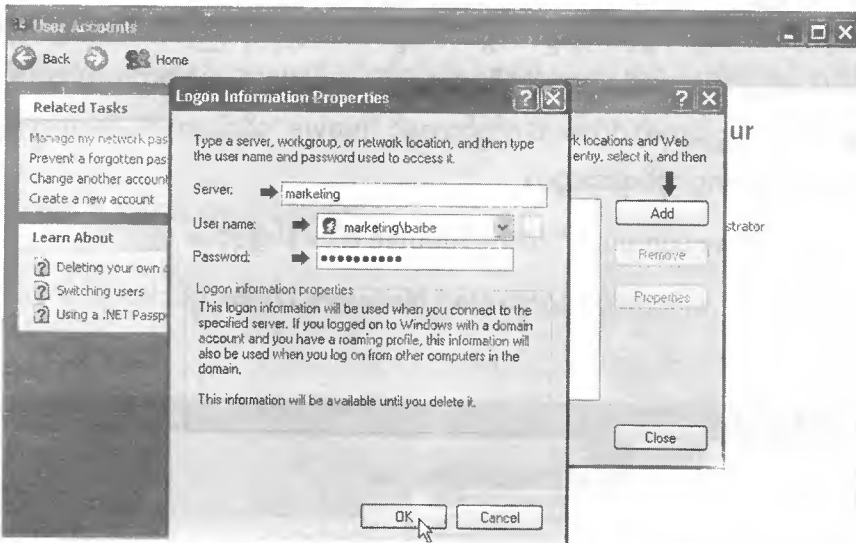
ကွန်ပျူတာကို browse လုပ်လိုက်တာနှင့် "access denied" တန်းပေါ်လာပါက "network password" ဆိုတာကိုထည့်ပေးဖို့လိုလာပါလိမ့်မယ်။

- 1) control panel ထဲရှိ user account ကို double click နှိပ်၍ဖွင့်ပါ။
- 2) မိမိ logon ဝင်ရောက်အသုံးပြုနေသော account icon ပေါ်တွင် click တစ်ချက်နှိပ်ပါ။

3) "related tasks" အောက်ရှိ manage my network password တွင် click တစ်ချက်နှိပ်ပါ။ "store username and password" box ကျလာပါမည်။



4) Add button တွင် click နှိပ်ပါ။ "logon information properties" dialog box ကျလာပါမည်။



- server - မိမိလှမ်း access လုပ်သော ကွန်ပျူတာအမည်။ (Marketing)
- username - computer name\user name (marketing\barbe)
- password - ABCdefGH

5) logon information တွေ ဖြည့်သွင်းခဲ့ပြီးပြီ ဆိုရင် OK button တွင် click နှိပ်ပြီး dialog box အားလုံးကိုပိတ်လိုက်ပါ။

6) log off ထွက်လိုက်ပါ။ ထိုမှတဖန် log on ပြန်ဝင်ပြီး ခုနက ကွန်ပျူတာကို ပြန်လည် access လုပ်ကြည့်ပါ။ share ပေးထားသော folder များကို မြင်ရပါလိမ့်မယ်။

simple file sharing ဖြင့် share ပေးထားပါက network အသုံးပြုသူ မည်သူမဆို(ဝါ) မည်သည့် account ဖြင့်မဆို အလွယ်တကူ access ရရှိနိုင်ပါတယ်။

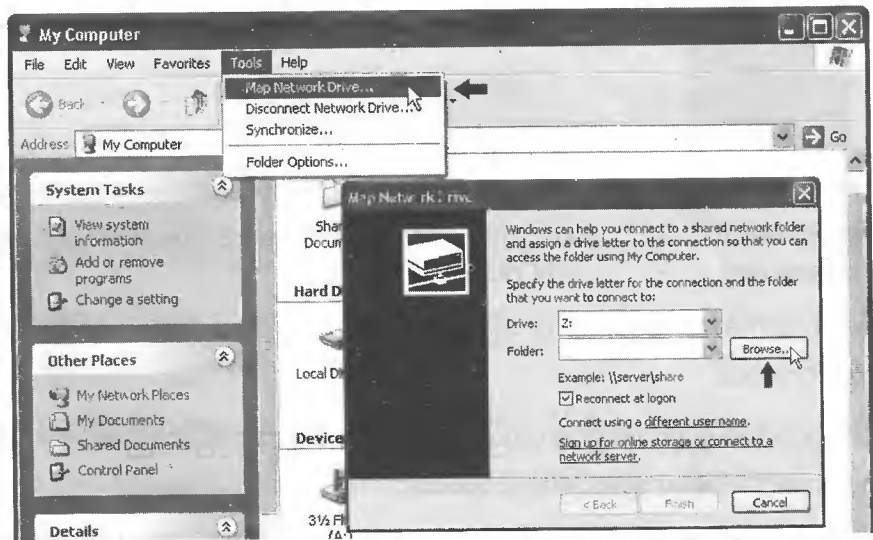
ဆိုရင် simple file sharing ဖြင့် share ပေးထားသော ကွန်ပျူတာပေါ်တွင် double click နှိပ်ပါက မည်သည့် username၊ password မှ မတောင်းပဲ share ပေးထားသော folder တွေ တန်းမြင်ရပါလိမ့်မယ်။

standard file sharing ဖြင့် share ပေးထားသော ကွန်ပျူတာ၊ folder တို့ကိုဖွင့်ပါက user name၊ password တောင်းခြင်း၊ permission မရှိပါက "access denied ဖြစ်ခြင်းများကို ကြုံတွေ့ရ ပါလိမ့်မယ်။

Mapping Network Drives

"Network Drive" ဆိုတာကမကြာခင်ကလွှဲလှမ်းအသုံးပြုတဲ့ share folder တစ်ခုကိုမိမိကွန်ပျူတာ မှာ drive တစ်ခုအနေနှင့် ရှိနေသလောက်ဖြစ်အောင် လုပ်ဆောင်အသုံးပြုခြင်း ဖြစ်ပါတယ်။ အဲဒီလို အသုံးပြုခြင်းအားဖြင့် "My network place" မှတစ်ဆင့်ပြီးတစ်ဆင့်သွားစရာမလိုပဲမိမိရဲ့ "my computer" ထဲမှာရှိနေတဲ့ drive တစ်ခုကို ဖွင့်သလိုမျိုး အလွယ်တကူ access လုပ်နိုင်ကြပါတယ်။ ဥပမာ ကွန်ပျူတာ B ထဲက movie ဆိုတဲ့ share folder ကို မိမိကွန်ပျူတာမှာ drive G အဖြစ်ထားမယ်ဆိုပါစို့။ ဒါဆိုရင် မိမိကွန်ပျူတာထဲမှာတွေ့နေရတဲ့ drive G ကိုဖွင့်တာနှင့် "movie" ဆိုတဲ့ share folder ကိုဖွင့်ပြီးသား ဖြစ်ပါလိမ့်မယ်။ Mapping လုပ်ရန်အတွက်

- 1) desktop ပေါ်ရှိ "my computer" icon ကို double click နှိပ်၍ဖွင့်ပါ။
- 2) "my computer" window ရှိ **Tools > Map Network Drive** တွင် click နှိပ်ပါက dialog box ကျလာပါလိမ့်မယ်။



3) driveနေရာရှိ drop down listထဲမှာ G: ကိုရွေးချယ်ပေးပါ။ (WinXPမှာအလိုအလျောက် Z: ကိုရွေးပြီးသား ဖြစ်ပါတယ်။)

4) **Browse** တွင် click နှိပ်ပါ။ share folder ကို ရှာဖွေညွှန်ပြရန် အတွက် "folder" dialog box ကျလာပါမည်။ မိမိကွန်ပျူတာမှာ drive တစ်ခုအဖြစ်ကဲ့သို့ထားလိုတဲ့ share folder ကိုတွေ့ပြီဆိုရင် select လုပ်ပြီး **OK** တွင် click နှိပ်ပါ။

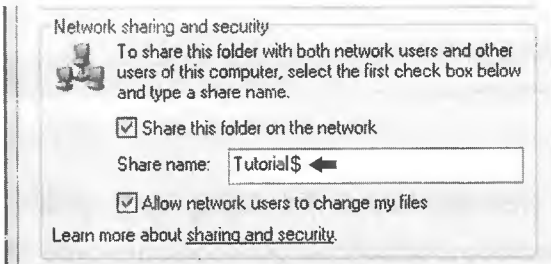


5) **Finish** တွင် click နှိပ်ပါ။ ဒါဆိုရင် mapping လုပ်ခြင်းပြီးဆုံးသွားပြီး "my computer" ထဲတွင် drive G: ဆိုတာကိုတွေ့ရပါလိမ့်မယ်။ drive G: ကို ဖွင့်လိုက်ပါက မိမိရွေးချယ်ခဲ့သော share folder ထဲက file တွေကိုမြင်ရပါလိမ့်မယ်။

📁 Hiding a Disk or Folder

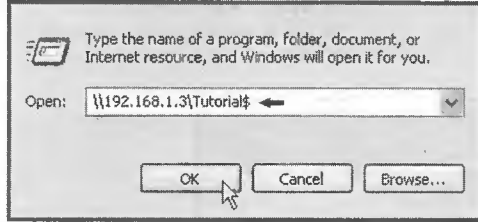
Network ပေါ်မှာ folder (သို့) disk ကို share တော့ပေးထားမယ်။ ဒါပေမယ့် share folder ကို "my network place" ကနေ ကြည့်ရှင်မမြင်နိုင်အောင် ဖျောက်ထားလို့ရပါတယ်။ သည့်အတွက် share folder အမည်ကိုအတိအကျသိတဲ့လူမှသာလျှင် access လုပ်နိုင်ကြမှာဖြစ်ပါတယ်။ သဘောကအဲဒီ share folder ကိုဖွင့်ဖို့ရန် လုံလောက်တဲ့ permission လည်းရှိရပါမယ်။ folder အမည်ကိုလည်း အတိအကျ သိရမှာဖြစ်သည့်အတွက် security ပိုကောင်းတယ်လို့ဆိုနိုင်ပါတယ်။ ထိုကဲ့သို့ share ပေးပုံပေးနည်းကို hidden share လို့ခေါ်ပါတယ်။ share ပေးဖို့ရန်အတွက် လုပ်ဆောင်ပုံတွေကတော့ ရှေ့မှာဖော်ပြခဲ့တဲ့ simple တို့၊ standard file sharing တို့နှင့် အတူတူပါပဲ။ share folder အမည်နောက်မှာ ဒေါ်လာ သင်္ကေတ (\$) ထပ်တိုးထည့်ပေးလိုက်ရုံဖြစ်ပါတယ်။

To Share




ဒါဆိုရင် share ပေးတာကတော့ ဟုတ်ပါပြီ။ မမြင်ရတဲ့ folder ကို ဘယ်လိုဖွင့်ရမလဲလို့ မေးစရာရှိလာပါလိမ့်မယ်။ hidden share တွေကို နည်း ၂ နည်းဖြင့် လှမ်း access လုပ်နိုင်ပါတယ်။ UNC patch နှင့် mapping network share တို့ပင်ဖြစ်ပါတယ်။

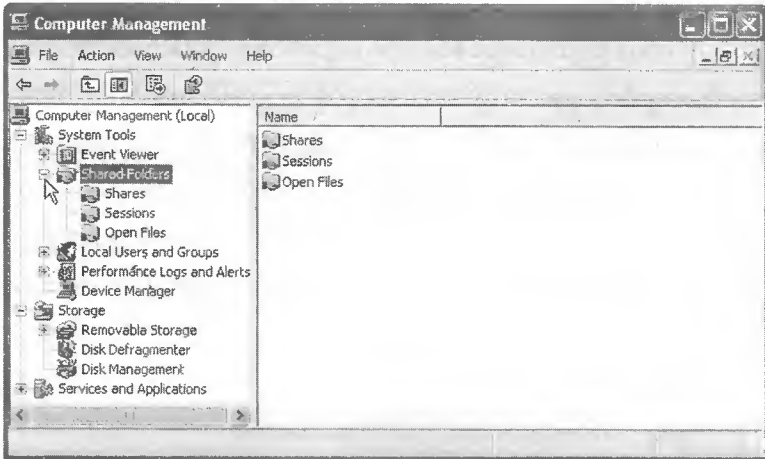
To access hidden share



Managing Share Folder

မိမိအသုံးပြုနေတဲ့ ကွန်ပျူတာမှာ ဘယ် folder ကို share ပေးထားသလဲ၊ ယခုလက်ရှိ ဘယ်သူတွေ ချိတ်ဆက်အသုံးပြုနေသလဲအစရှိသဖြင့် share folder များအပေါ်မှာ ထိထိရောက်ရောက် ထိန်းချုပ်ကွပ်ကဲမှုများကို computer management ထဲမှတစ်ဆင့် လုပ်ဆောင်နိုင်ကြပါတယ်။

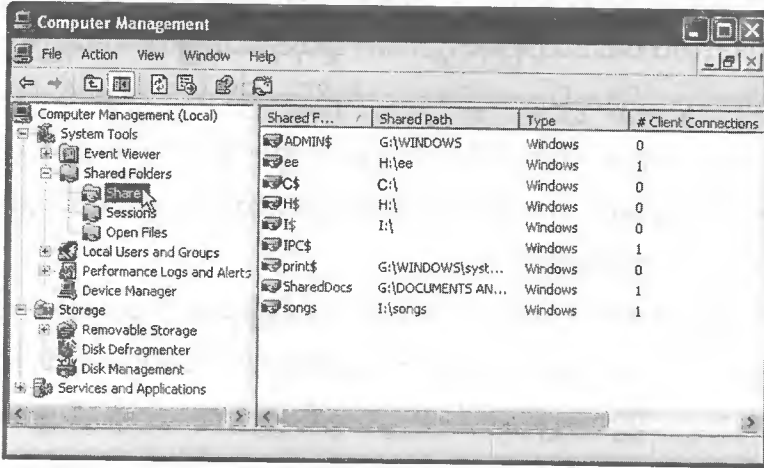
Desktop ပေါ်ရှိ "my computer" icon (သို့) **Start > My Computer** ပေါ်တွင် right click နှိပ်ပါ။ ကျလာမည့် short cut menu ထဲရှိ manage တွင် click တစ်ချက်နှိပ်ပါက "computer management" ပွင့်လာပါလိမ့်မည်။ ၎င်း console ၏ ဘယ်ဘက်ခြမ်းရှိ tree view ထဲရှိ system tools ဘေးမှ  ကို click နှိပ်ပြီး အဆင့်ဆင့်ဆန့်ထုတ်သွားပါက Shares | Session | Open files ဟူသော utility ဥရုကို တွေ့ရပါမယ်။



Viewing share

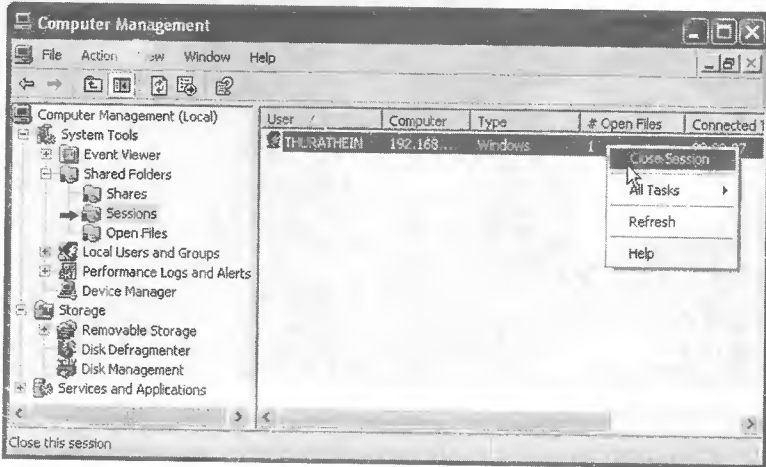
ဘယ်ဘက်ခြမ်း tree view ထဲရှိ **shares** ကို click နှိပ်၍ select လုပ်ပါက ညာဘက်ခြမ်းထဲတွင် မိမိကွန်ပျူတာမှာ share ပေးထားသမျှ အားလုံးတို့ကို တွေ့ရပါမယ်။ share type ၂ မျိုး နှစ်စားရှိပါတယ်။

ပထမတစ်မျိုးက အသုံးပြုသူ user များမှ create လုပ်ထားသော share folder များဖြစ်ပြီး၊ ဒုတိယ တစ်မျိုးကတော့ windows XP မှအလိုလျှောက် create လုပ်ထားသော (drive letter [C\$, H\$], ADMIN\$, IPC\$, Print\$) share များပဲဖြစ်ပါတယ်။



● Viewing session

Sessions ကို ရွေးချယ် select လုပ်ပါက share folder တွေကို ချိတ်ဆက် အသုံးပြုနေသော user များရဲ့ list ကို မြင်ရပါမယ်။ အဲဒီလိုဘယ်သူတွေ ဝင်ရောက် အသုံးပြုနေသလဲဆိုတာကို ကြည့်ရုံမျှမကပဲ disconnect လုပ်လိုက်လုပ်နိုင်ပါသေးတယ်။ user session တစ်ခုကို ရွေးချယ် right-click နှိပ်ပြီး **disconnect** တွင် click နှိပ်လိုက်ရုံဖြစ်ပါတယ်။



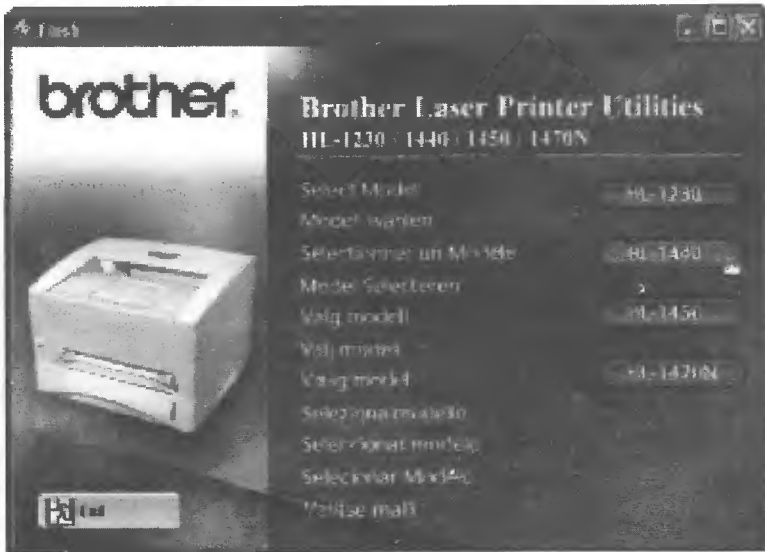
● Viewing Open Files

Open Files ကို ရွေးချယ် select လုပ်ပါက share folder များထဲမှ လက်ရှိဖွင့်ထားသော file တွေရဲ့ list ကို မြင်ရပါမယ်။

Adding a Printer

printer တစ်ခုလုံးကို ကွန်ပျူတာမှာ ချိတ်ဆက်တပ်ဆင်ရန်အတွက်ကတော့ အလွန်ပင် ရိုးရှင်းလွယ်ကူသည့်အတွက် မည်သူမဆို အလွယ်တကူ တင်ဆင်နိုင်ကြပါလိမ့်မယ်။ သို့သော်လည်း မိမိ printer သည် parallel port မှာ တပ်ဆင်အသုံးပြုရမည့် printer မျိုးဆိုရင်တော့ ဖြုတ်တပ်အနည်းငယ်သတိထားဖို့ လိုနေပါလိမ့်မယ်။ အထူးသဖြင့် ကွန်ပျူတာဖွင့်ထားလျက်နှင့် ဖြုတ်ခြင်း တပ်ခြင်းများကို မပြုလုပ်သင့်ပါဘူး။ ဒါကြောင့် parallel port မှာ တပ်ဆင်မယ်ဆိုရင် ကွန်ပျူတာ ပါဝါပိတ်ပြီး တပ်ဆင်ရပါမယ်။ USB printer များအတွက်ကတော့ ကွန်ပျူတာဖွင့်ထားခြင်းနှင့် ပိတ်ထားခြင်းတို့သည် အရေးမပါလှပါဘူး။ လွတ်တဲ့ USB port တစ်ခုခုမှာ ချိတ်ဆက်လိုက်ရုံဖြစ်ပါတယ်။

printer ကို ချိတ်ဆက်တပ်ဆင်ခဲ့ပြီးပြီဆိုလျှင် အသုံးပြုရအောင် မှန်ကန်တဲ့ driver ကို install လုပ်ပေးဖို့လိုပါတယ်။ ယနေ့ printer တစ်ခုလုံးကို ဝယ်ယူတဲ့အခါ ရရှိမယ့် driver installation CD များထဲတွင် auto program ပါရှိပြီးသားဖြစ်ပါတယ်။ သည့်အတွက်ကြောင့် printer ကို ကွန်ပျူတာမှာ တပ်ဆင်ပြီး တာနှင့် driver CD ကို ထည့်သွင်း၍ ပေါ်လာမည့် ညွှန်ကြားချက်များကို တပ်ဆင်ချင်းလိုက်ပါလုပ်ဆောင်သွားရုံဖြင့် printer ကို အသုံးပြုရနိုင်စေပါတယ်။



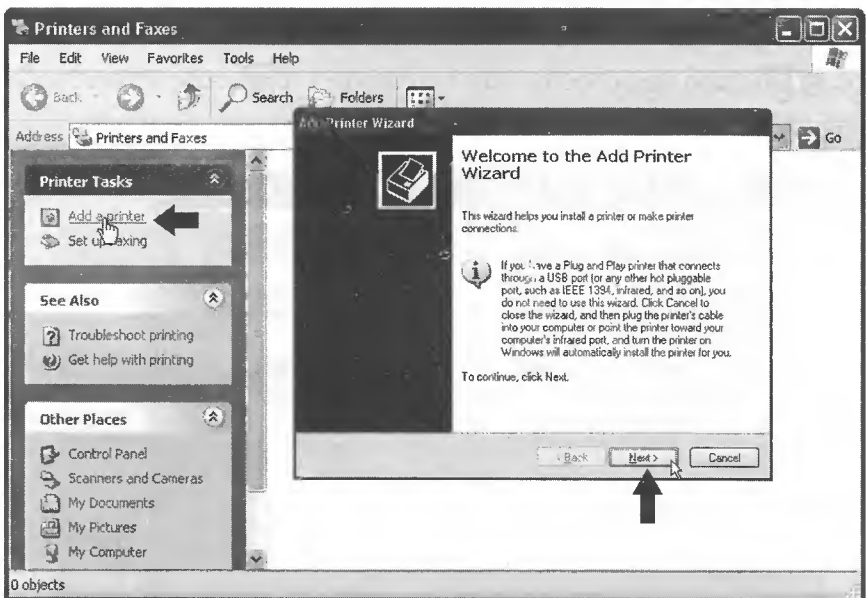
အကယ်၍ original driver CD မရှိဘူးဆိုရင်တော့ printer ထုတ်လုပ်ရောင်းချသည့် ကုမ္ပဏီ website များမှာ မိမိ printer နှင့် ကိုက်ညီသော driver ကို ရှာဖွေ download ရယူရမှာဖြစ်ပါတယ်။ အောက်ဖော်ပြပါ website များကတော့ ယနေ့လူသုံးအများဆုံး printer တို့အတွက် driver file များကို download ရယူနိုင်သော link များပဲဖြစ်ပါတယ်။

- Hewlett Packard - ■ <http://welcome.hp.com/country/us/eng/support.html>
- Canon - ■ <http://www.usa.canon.com/html/cprSupportDetail.jsp?navfrom=DrivD>
- Epson - ■ <http://www.epson.com/cgi-bin/Store/index.jsp>
- Lexmark - ■ <http://www.lexmark.com/US/support/drivers/>

မှတ်ချက် - driver file များကိုအင်တာနက်မှ download ရယူတဲ့နေရာမှာ အများအားဖြင့် compress လုပ်ထားသော zip file များအဖြစ်ရရှိမှာဖြစ်ပါတယ်။ ၎င်း zip file များကို ပြန်ဖြည့်ဖို့ရန်အတွက် Winzip/ WinRAR အစရှိသည့် software တစ်ခုခုကို မိမိကွန်ပျူတာမှာ install လုပ်ထားဖို့လိုပါတယ်။

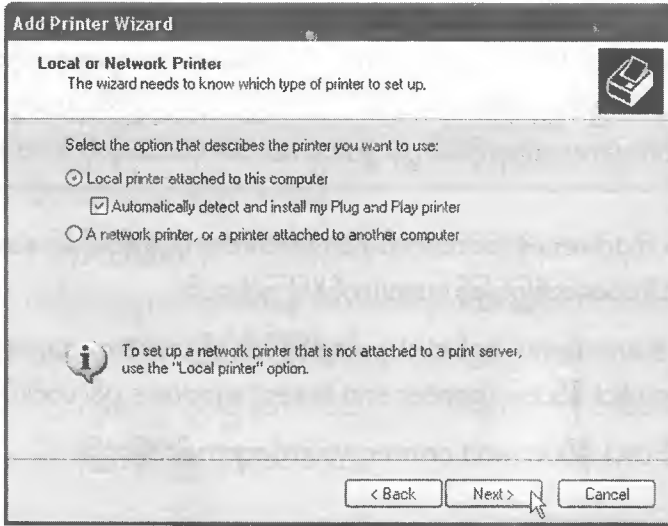
printer အတွက် driver ကို အင်တာနက်မှ download ရယူခဲ့ပြီး ပြီဆိုရင် အောက်ဖော်ပြပါ အဆင့်များအတိုင်း လိုက်ပါလုပ်ဆောင်ခြင်းဖြင့် install လုပ်နိုင်ကြပါတယ်။

- 1) Start > printers and faxes တွင် click တစ်ချက်နှိပ်ပါ (သို့) control panel ထဲရှိ printer and faxes တွင် double click နှိပ်ပါက "printer and faxes" windows ပွင့်လာပါလိမ့်မည်။
- 2) **Add printer** တွင် click နှိပ်ပါက add printer wizard ကျလာပါလိမ့်မည်။

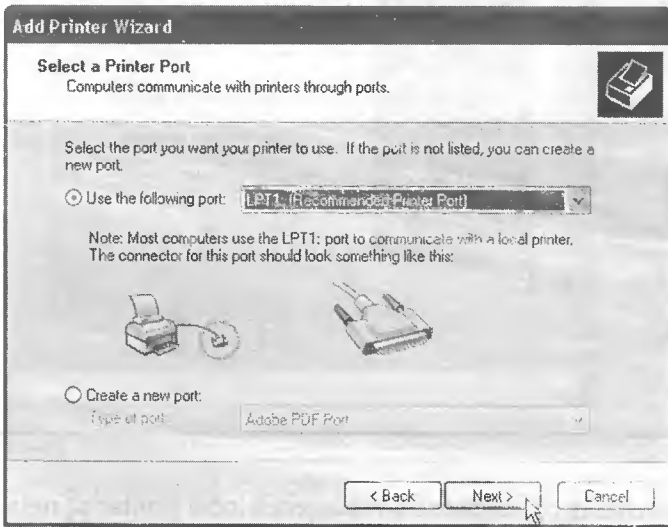


3) Welcome Wizard ရှိ **Next** တွင် click တစ်ချက်နှိပ်လိုက်ပါ။ local printers နှင့် network printer တို့ထဲမှ တစ်ခုခုကို ရွေးချယ်ပေးဖို့ရန်တောင်းဆိုပါလိမ့်မည်။

4) ယခုအချိန်သည် printer ကို မိမိကွန်ပျူတာမှာ တိုက်ရိုက်ချိတ်ဆက်တပ်ဆင် install လုပ်နေခြင်း ဖြစ်သည့် အတွက်ကြောင့် local printer ဘေးရှိ radio button ကို ဖြစ်အောင် click နှိပ်ပြီး ရွေးချယ်ပေးရပါမယ်။ ဒါ့အပြင် automatical detect နေရာရှိ check box ကို အမှန်ဖြစ်ဖြစ်အောင် select လုပ်ဖို့လိုပါတယ်။ ပြီးပြီဆိုလျှင် next တွင် click နှိပ်ပါ။

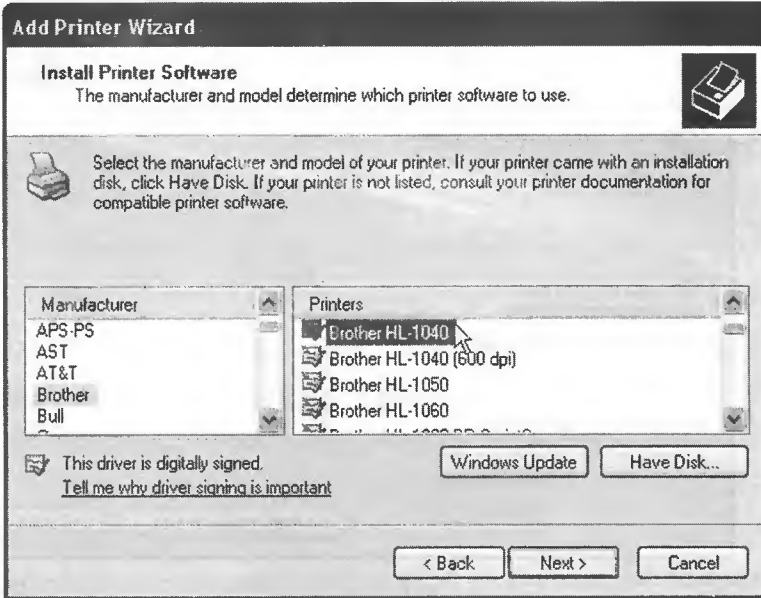


5) printer တပ်ဆင်ထားသော port ကို ရွေးချယ်ပေးရပါမယ်။ use the following port ဘေးရှိ radio button တွင် ဖြစ်အောင် ရွေးချယ်ပေးရပါမယ်။ list ထဲမှာ LPT 1 ဖြစ်အောင် select လုပ်ပြီး ပြီးပြီဆိုလျှင် next တွင် click နှိပ်ပါ။

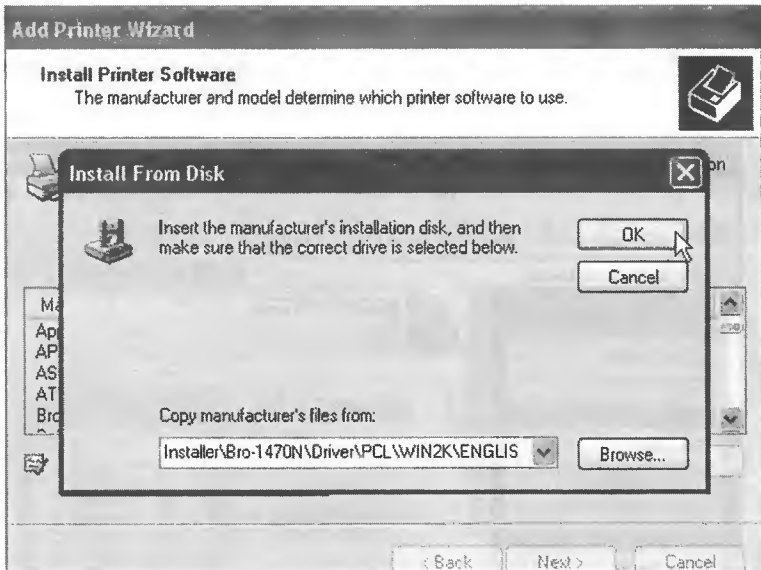


6) ဒီအဆင့်မှာဆိုရင် printer အတွက်လိုအပ်တဲ့ driver software ကို install လုပ်ပေးရပါမယ်။ manufacture list ထဲမှာ printer ထုတ်လုပ်သော ကုမ္ပဏီပေါ်တွင် click နှိပ်လိုက်ပါ။

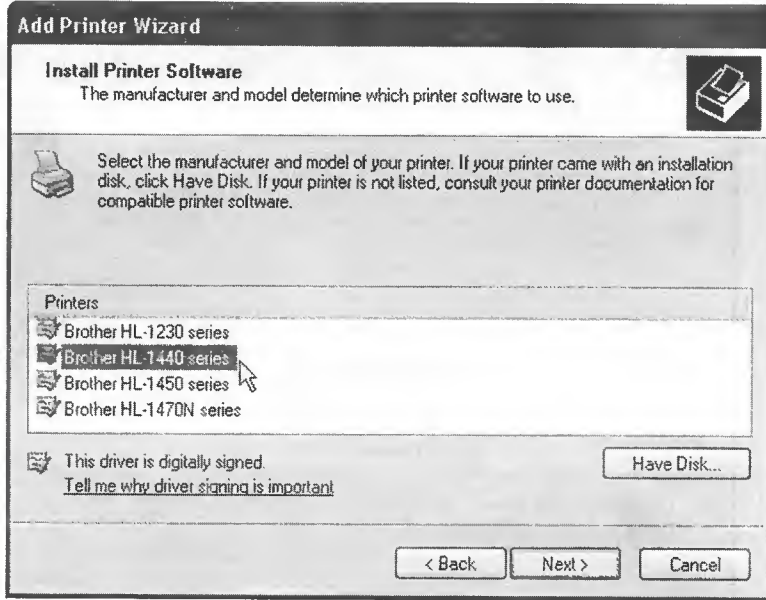
ညာဘက် printer listထဲတွင် မိမိတပ်ဆင်ထားသော printer model အမည်ကို ရွေးချယ်ပြီး Next တွင် click နှိပ်ရုံဖြစ်ပါတယ်။ အကယ်၍ အဲဒီ list တွေထဲမှာ မိမိ printer model အမည်ကို မတွေ့ဘူးဆိုရင်တော့ printer အတွက် driver CD ကို ထည့်သွင်းပြီး hard disk တွင် click နှိပ်ပြီး driver file များရှိသောနေရာကို ညွှန်ပြပေးရပါမယ်။



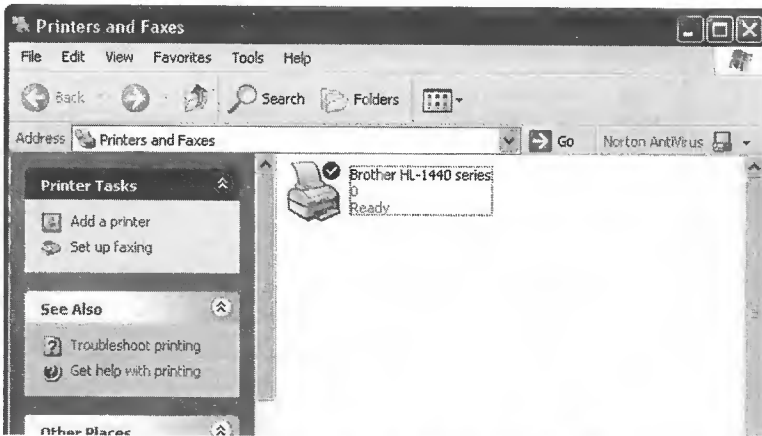
7) **Brother** တွင် click နှိပ်ပြီး driver file များရှိသောနေရာကို ညွှန်ပြပေးရပါမယ်။ ပြီးပြီဆိုလျှင် **OK** button တွင် click နှိပ်လိုက်ပါ။ install လုပ်မည့် printer အမည်ကို ဖော်ပြပါလိမ့်မည်။



8) တစ်ခါတလေ printer အမျိုးအစားအမည်တစ်ခုထက်မကကို ဖော်ပြလေ့ရှိပါတယ်။ အဲဒီလို အခါမျိုးမှာ မိမိတပ်ဆင်ထားသော printer နှင့် ကိုက်ညီသော အမည်ကို ရွေးချယ်ပေးဖို့ လိုပါလိမ့်မယ်။ printer အမျိုးအစားကို ရွေးချယ်ပြီးပါက **Next** တွင် click နှိပ်လိုက်ပါ။



printer အမည်ထည့်သွင်းခြင်း၊ default printer အဖြစ်သတ်မှတ်ခြင်း၊ test page ထုတ်ခြင်း အစရှိတဲ့ ကျန်ရှိနေသော အဆင့်များကို ပေါ်လာမည့် ညွှန်ကြားချက်များအတိုင်း ဆက်လက် လုပ်ဆောင် သွားလိုက်ပါ။ နောက်ဆုံးအဆင့်မှာတော့ finish button ပါတဲ့ wizard ကို တွေ့ရပါလိမ့် မယ်။ ၎င်း finish button တွင် click နှိပ်ပြီး printer installation ကို အဆုံးသတ်လိုက်ပါ။ လိုအပ်သော file များကို copy ကူးယူ install လုပ်ပါလိမ့်မယ်။ "printer and faxes" ထဲတွင် မိမိ install လုပ်ခဲ့သော printer ကို တွေ့ရပါမယ်။



Sharing Printer

Networkပေါ်မှာ printerတွေကို shareလုပ်၍ အသုံးပြုခြင်းသည် fileတွေ၊ folderတွေကို share လုပ်၍ အသုံးပြုခြင်းနှင့် သဘောတရားအားဖြင့် အတူတူပင်ဖြစ်ပါတယ်။ ဆိုရရင် network ပေါ်မှာ share ပေးထားတဲ့ fileတွေ၊ folderတွေကို မိမိကွန်ပျူတာမှာရှိနေသကဲ့သို့ ယူငင်အသုံးပြုနိုင်သည့်အတိုင်းပင် networkပေါ်မှာ shareပေးထားတဲ့ printerကိုလည်း မိမိကွန်ပျူတာမှာ တပ်ဆင်ထားသကဲ့သို့အသုံးပြုနိုင်စေ ပါတယ်။

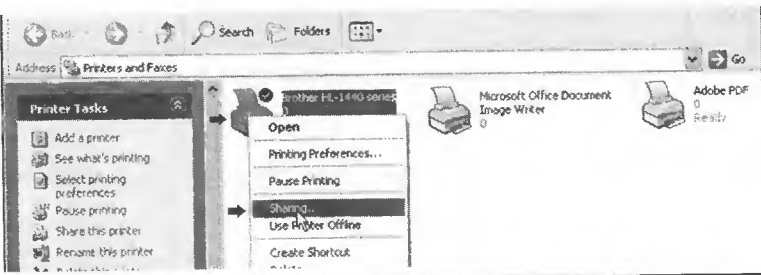
printer တွေကို share လုပ် အသုံးပြုရတဲ့ အကြောင်းရင်းများစွာရှိပါတယ်။ အဲဒီများစွာထဲက ကုန်ကျစရိတ်သက်သာစေခြင်းဆိုတဲ့ အချက်သည် အဓိကအကြောင်းရင်းတစ်ခု ဖြစ်ပါလိမ့်မယ်။ ဆိုရရင် ကွန်ပျူတာ သုံးလုံးလောက်ကနေပြီး တပြိုင်နက် printထုတ်ရန်အတွက် printer သုံးလုံးဝယ်ယူစရာ မလိုပဲ တစ်လုံးတည်းဝယ်ယူပြီး shareလုပ်၍အသုံးပြုခြင်းဖြင့် ကုန်ကျစရိတ်များစွာ သက်သာစေပါတယ်။

အဲဒီလို အားသာချက်တွေ ရှိသလို အားနည်းချက်များလည်း ရှိပါတယ်။ printer တပ်ဆင်ထား သည့်ကွန်ပျူတာ (host PC) သည် ချွတ်ယွင်းချက် တစ်ခုခုကြောင့် network နှင့် ချိတ်ဆက်နိုင်ခြင်း မရှိတော့ဘူးဆိုရင် ၎င်း printer ကို အခြား ကွန်ပျူတာများမှ အသုံးပြု၍ ရနိုင်တော့မည် မဟုတ်ပါ။ ဒါ့အပြင်လည်းပဲတစ်ပြိုင်နက် print ထုတ်မှုတွေများနေမယ် တနည်းဆိုရရင် printer မှာ print job တွေ များလာပြီဆိုရင် ၎င်း printer တပ်ဆင်ထားတဲ့ ကွန်ပျူတာ (print server) ရဲ့လုပ်ဆောင်မှု အမြန်နှုန်း ကျဆင်းလာတာကိုကြုံတွေ့ရမှာဖြစ်ပါတယ်။

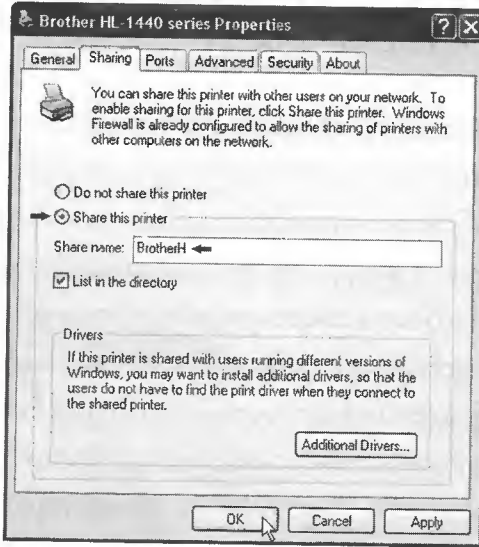
မည်သို့ပင်ဖြစ်စေ ကုန်ကျစရိတ်သက်သာခြင်း၊ share ပေးရုံဖြင့် အခြားကွန်ပျူတာများမှ အလွယ်တကူအသုံးပြုနိုင်ခြင်း၊ installလုပ်ရန်များစွာကျွမ်းကျင်မှုရှိရန်မလိုအပ်ခြင်း စသည့်အားသာချက်များ ကြောင့် ယနေ့ networkတွေ တည်ဆောက်ဖို့ရန် စဉ်းစားတဲ့နေရာမှာ printer ကို shareလုပ်သုံးရန်ဆိုတဲ့ အချက်သည်လည်း အဓိကရည်ရွယ်ချက်ပင်ဖြစ်လို့နေပါပြီ။

printerကို networkချိတ်ဆက်ထားသော ကွန်ပျူတာတစ်လုံးမှာ တပ်ဆင်ကာလိုအပ်သော driver များကို installလုပ်ပြီး၍ ကောင်းမွန်မှန်ကန်စွာ အလုပ်လုပ်နိုင်ပြီဆိုရင် စတင် share ပေးလို့ရပါပြီ။

1) **start > printers and faxes** တွင် clickတစ်ချက်စီနှိပ်ပါက "printers and faxes" window ပွင့်လာပါမည်။ shareပေးလိုသော printerအမည်ပေါ်တွင် right clickတစ်ချက်နှိပ်ပါ။ ကျလာမည့် short-cut menuထဲတွင်ရှိသော **Sharing** တွင် clickတစ်ချက်နှိပ်ပါ။ "sharing tab" အောက်မှနေ၍ printer ၏ properties dialog box ပွင့်လာပါလိမ့်မည်။



2) **Share this printer** ဘေးရှိ radio button ပေါ်တွင် ဖြစ်အောင် click နှိပ်၍ ရွေးချယ်ပေးရပါမည်။ ၎င်းနောက် folder တွေကို share ပေးသကဲ့သို့ပင် printer အတွက်လည်း အမည်တစ်ခုကို ပေးဖို့လိုပါတယ်။ **share name** နေရာတွင် character ရှစ်လုံးထက်မပိုသော နှစ်သက်ရာအမည် တစ်ခုကို ထည့်သွင်းနိုင်ပါတယ်။



3) **OK** button တွင် click နှိပ်လိုက်ပါ။ properties" dialog box ပျောက်သွားပြီး မူလ "Printers and Faxes" window ထဲရှိ printer icon ပေါ်တွင် လက်ညှိပေးလာပါလိမ့်မည်။ ဒါဆိုရင် printer တစ်လုံးကို share ပေးခြင်း ပြီးဆုံးပြီ ဖြစ်ပါတယ်။

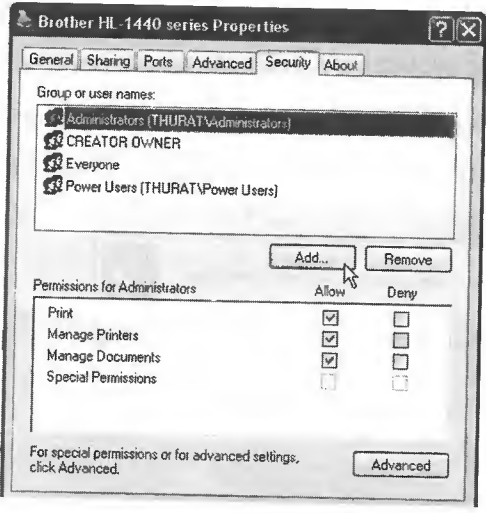
Managing Printer

Printer တစ်လုံးကို share ပေးပြီးသွားတဲ့အခါ ပုံမှန် default အားဖြင့် Everyone လို့ခေါ်သည့် network ပေါ်မှ အသုံးပြုသူမည်သူမဆို print ထုတ်နိုင်သည့် print permission ကို ရရှိပြီးသား ဖြစ်ပါတယ်။ administrator နှင့် power user group ထဲမှာပါရှိသူများကတော့ manage printer နှင့် manage document permission များကို အလိုအလျောက် ရရှိပြီးသား ဖြစ်ပါလိမ့်မယ်။ အောက်ဖော်ပြပါ ဇယားမှာဆိုရင် Print, Manage Printers နှင့် Manage Documents တို့ရဲ့ လုပ်ပိုင်ခွင့်များကို ဖော်ပြထားပါတယ်။

Basic Printer Permissions and Privileges

Permission	Privileges
Print	Print documents Control properties of owned documents Pause, restart, and remove owned documents
Manage Printers	Share printer Change printer properties Remove printer Change printer permissions Pause and restart the printer
Manage Documents	Pause, restart, move, and remove all queued documents

အဲဒီလို default တွေအတိုင်း မဟုတ်ပဲ permission တွေကို ပြင်ချင်တယ်ဆိုရင် printer properties ၏ security tab အောက်တွင် လိုသလို စိတ်ကြိုက် ပြင်ဆင်နိုင်ကြပါတယ်။

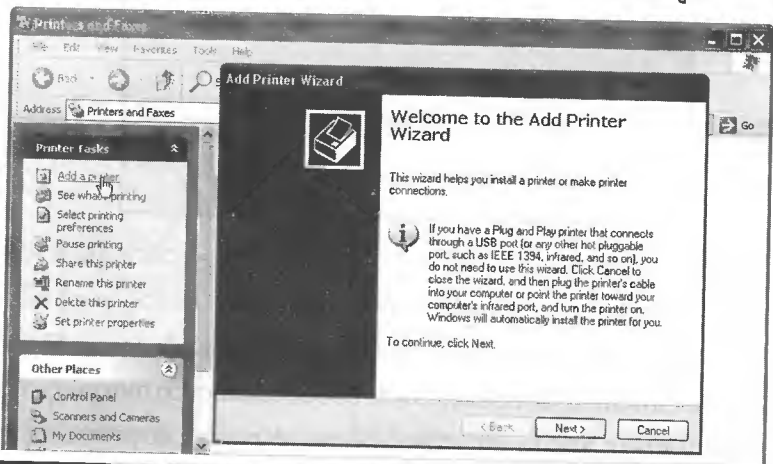


File တွေ folder တွေကို share ပေးစဉ်က အတိုင်းပင် user အသစ်တွေကို ထပ်ထည့်လိုပါက Add button တွင် click နှိပ်ပြီး ထပ်ထည့်နိုင်ပါတယ်။ အဲဒီလို ထည့်ပြီးသွားပြီဆိုရင် user account တစ်ခုစီကို ရွေးချယ် select လုပ်ပြီး permission သစ်များ သတ်မှတ်ပေးနိုင်ကြပါတယ်။

Using Printer On Other PC

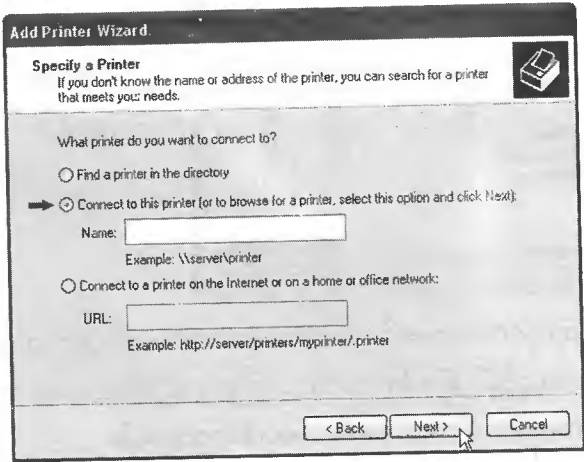
အခြားကွန်ပျူတာမှာ တပ်ဆင် share ပေးထားတဲ့ printer ကို အောက်ဖော်ပြပါ နည်းလမ်းများ အတိုင်း ချိတ်ဆက် အသုံးပြုနိုင်ကြပါတယ်။

- 1) **Start > Printers and Faxes** တွင် click တစ်ချက်နှိပ်ပါက "printers and Faxes" window" ပွင့်လာပါလိမ့်မည်။ **Add printer** တွင် click နှိပ်ပါက Add printer wizard ကျလာပါလိမ့်မည်။

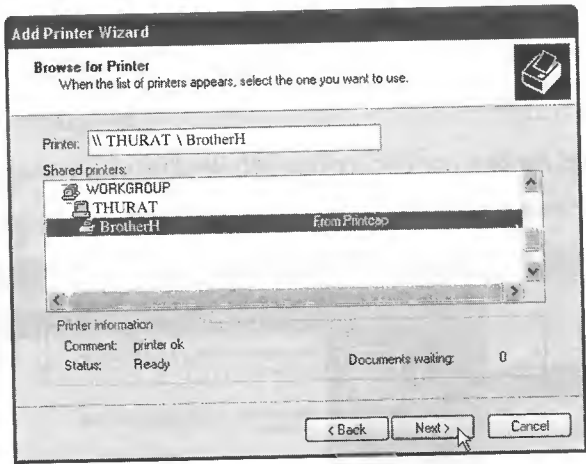


2) welcome wizard ရှိ **Next** တွင် click နှိပ်ပါက local printer နှင့် network printer တို့ထဲမှ တစ်ခုခုကို ရွေးချယ်ပေးဖို့ရန် တောင်းဆိုပါလိမ့်မယ်။ ယခုအချိန်သည် အခြားကွန်ပျူတာမှာရှိနေသော printer ကို ချိတ်ဆက်ရန် ကြိုးစားနေခြင်းဖြစ်သည့်အတွက်ကြောင့် "A network printer" ဘေးရှိ radio button ကို ဖြစ်အောင် ရွေးချယ်ပြီး **Next** တွင် click တစ်ချက်နှိပ်ပါ။

3) မိမိထည့်သွင်းလိုသော printer ကို ရွေးချယ်ညွှန်ပြရန် အတွက် "connect to this printer" ဘေးရှိ radio button ကို ဖြစ်အောင် ရွေးချယ်ပြီး **Next** တွင် click နှိပ်ပါ။



network တွင်းတွင် share ပေးထားသော printer များကို မြင်ရပါမယ်။

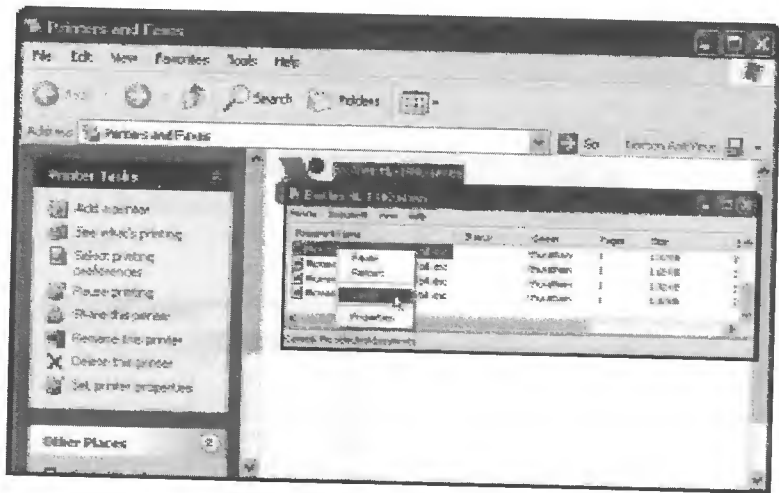


4) မိမိထည့်သွင်းလိုသော printer ကို select လုပ်ပြီး **Next** တွင် click နှိပ်ပါ။ default printer အဖြစ် သတ်မှတ်ခြင်း၊ test page ထုတ်ခြင်းအစရှိတဲ့ ကျန်ရှိနေသော အဆင့်များကို ပေါ်လာမည့် ညွှန်ကြားချက်များအတိုင်း ဆက်လက် လုပ်ဆောင်သွားလိုက်ပါ။ နောက်ဆုံးအဆင့်မှာတော့ **Finish** button တွင် click နှိပ်ပြီး printer installation ကို အဆုံးသတ်လိုက်ပါ။ လိုအပ်သော file များကို copy ကူးယူ install လုပ်ပါလိမ့်မယ်။ "printers and faxes" ထဲတွင် မိမိ install လုပ်ခဲ့သော printer ကို တွေ့ရပါမယ်။

Managing Print Documents

administrator rightကိုရရှိထားတဲ့အသုံးပြုသူများသည် printer queue ထဲမှာရောက်ရှိနေပြီး print ထုတ်ဖို့ရန်စောင့်ဆိုင်းနေသော documentတွေကို စီမံခန့်ခွဲပိုင်ခွင့် ရှိကြပါတယ်။ ဥပမာအသုံးပြုသူ တစ်ယောက်ယောက်မှ document တစ်ခုတည်းကိုပင် ကြိမ်ဖန်များစွာ မှားယွင်း၍ print ထုတ်မိတဲ့အခါ မျိုးမှာ printer queueထဲမှာပုံနေတဲ့ print jobကိုဖျက်ထုတ်ဖို့လိုအပ်ကောင်း လိုအပ်မှာဖြစ်ပါတယ်။

printer queueကို ဖွင့်ရန်အတွက် "printer and fax" windowထဲရှိ printer iconကို double click နှိပ်ရမှာဖြစ်ပါတယ်။ printer queue ထဲမှာဆိုရင် print လုပ်ဖို့ရန် စောင့်ဆိုင်းနေသော documentတွေကိုတန်းစီဖော်ပြထားမှာဖြစ်ပါတယ်။



မိမိ manage လုပ်လိုသော document တစ်ခုတွင် right click နှိပ်ပါက pause၊ resume၊ cancel၊ refresh၊ properties ဟူ၍ ရွေးချယ်စရာ option ၅ခုပါတဲ့ menu ကျလာ ပါလိမ့်မည်။ ၎င်း option တွေရဲ့ဆိုလိုရင်းနှင့် လုပ်ဆောင်မှုတွေက အောက်ပါအတိုင်း ဖြစ်ပါတယ်။

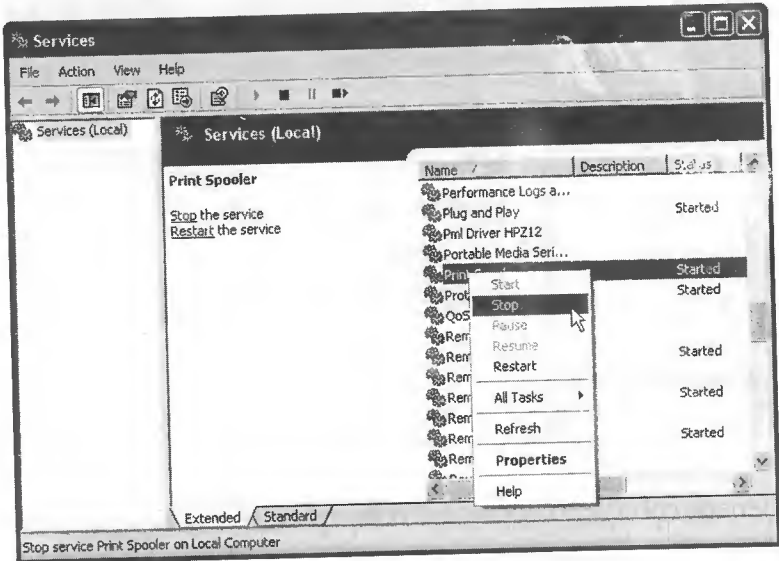
- pause** - document အား print ထုတ်နေခြင်းကို ခေတ္တရပ်ဆိုင်းထားရန်
- resume** - print ထုတ်ခြင်း ခေတ္တရပ်ဆိုင်းထားတဲ့ document ကို ပုံမှန်အတိုင်း ဆက်လက် print လုပ်ရန်
- restart** - တစ်စိတ်တစ်ပိုင်း print ထုတ်ပြီးသည်ဖြစ်စေ၊ လုံးဝမထုတ်ရသေးသည်ဖြစ်စေ အစမှအဆုံး ပြန်လည် print လုပ်ရန်
- cancel** - print job ကို delete လုပ်ရန်
- properties** - document ရဲ့ properties ပဲဖြစ်ပါတယ်။

မှတ်ချက်။ ။တစ်ခါတစ်လေ printer queထဲမှာရှိနေတဲ့ documentတွေကို delete(cancel) လုပ်၍မရနိုင်တာမျိုး ကြုံတွေ့ရတတ်ပါတယ်။ အဲဒီလိုအခါမျိုးမှာ printer spooler service ကို stop လုပ်ပါ။ ပြီးလျှင် ပြန်လည် start လုပ်ခြင်းဖြင့် ဖြေရှင်းနိုင်ကြပါတယ်။

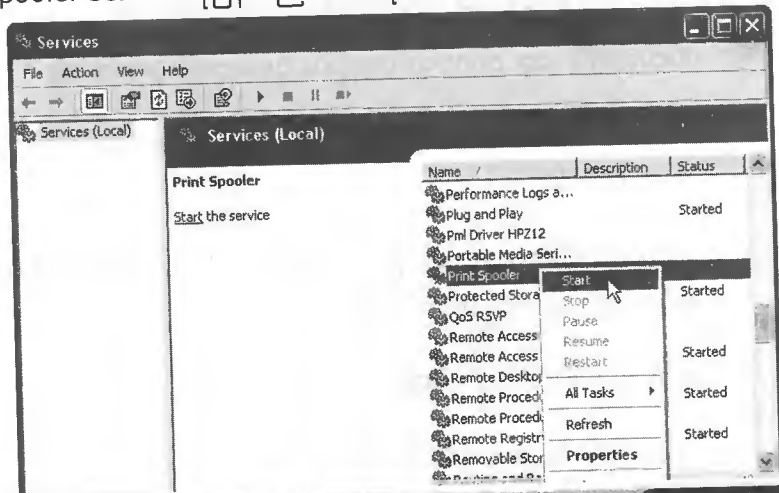
services program ကို ဖွင့်ရန်အတွက် အောက်ဖော်ပြပါ နည်းလမ်းများထဲမှ တစ်ခုခုကို အသုံးပြုနိုင်ပါတယ်။

- Run programထဲတွင် services.msc ဟုရိုက်ထည့်ပြီး enter နှိပ်ပါ။
- Start> Control Panel > administrative tools> computer management> servicesတွင် click နှိပ်ပါ။

1) Printer Spooler service ကို stop လုပ်ပါ။



2) Print Spooler serviceကိုပြန်လည် start လုပ်ပါ။



Internet Access

မိမိကွန်ပျူတာ (သို့) network ကို အင်တာနက်နှင့် ချိတ်ဆက်နိုင်ရန်အတွက် ISP ထံမှ connection တစ်ခုရရှိဖို့လိုပါလိမ့်မယ်။ ISP ဆိုတာက အင်တာနက်ချိတ်ဆက်အသုံးပြုနိုင်အောင် ဝန်ဆောင်မှုပေးတဲ့ company ဖြစ်ပါတယ်။ ISP နှင့် ချိတ်ဆက်မိပြီးဆိုတာနှင့် internet access ရပြီလို့မှတ်ယူနိုင်ပါတယ်။ အရေးကြီးတာက အဲဒီ connection အတွက် ကွန်ပျူတာဆက်စပ်ပစ္စည်းတွေ ဝယ်ယူတပ်ဆင်ရပါလိမ့်မယ်။ ဘယ်လို ပစ္စည်းမျိုးတွေ ဝယ်ယူတပ်ဆင်ရမလဲဆိုတာက ချိတ်ဆက်မည့်နည်းလမ်းနှင့် connection အမျိုးအစားတွေပေါ်မူတည်ပြီး ကွာခြားမှု ရှိမှာဖြစ်ပါတယ်။ အောက်ဖော်ပြပါ connection တွေကတော့ ယနေ့အသုံးအများဆုံးနှင့် ISP တို့ထံမှ ရရှိနိုင်သော connection အမျိုးအစားများဖြစ်ပါတယ်။

- » Dialup connection
- » DSL connection
- » Satellite
- » Broadband Wireless

connection type အလိုက် အသုံးပြုရနိုင်တဲ့ speed ကွာခြားချက် ရှိမှာဖြစ်ပါတယ်။ speed ပိုမြင့်တာကို ရွေးချယ်မယ်ဆိုရင် ဝန်ဆောင်မှုစရိတ်နှင့် အခြားကုန်ကျစရိတ်များလည်း ပိုမိုမြင့်မားလာမှာ ဖြစ်ပါတယ်။

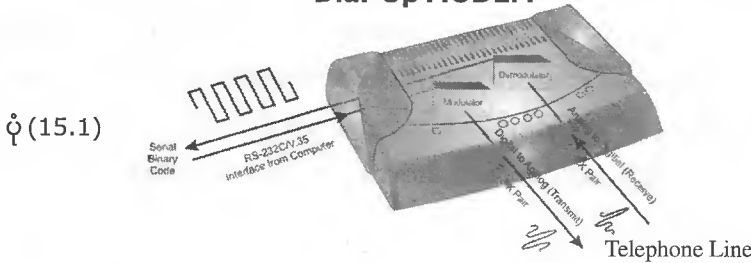
Dial-up connection

Dial-up connection သည် modem ကို အသုံးပြုပြီး တယ်လီဖုန်းလိုင်းမှတစ်ဆင့် အင်တာနက် ချိတ်ဆက်ရတဲ့ အခြေခံအကျဆုံး connection အမျိုးအစားဖြစ်ပါတယ်။ dial-up connection တစ်ခုအတွက် သီးခြားတန်ဖိုးကြီး ပစ္စည်းတွေ မလိုပဲ modem တစ်ခုရရှိရုံဖြင့် အင်တာနက်ချိတ်ဆက်နိုင်သည့် အတွက် အခြား connection တွေနှင့် ယှဉ်ရင် ကုန်ကျစရိတ်အသက်သာဆုံး ဖြစ်ပါတယ်။ အင်တာနက်အသုံး ပြုလိုတဲ့အခါတိုင်းတွင် modem မှတစ်ဆင့် ISP မှပေးထားသော ဖုန်းနံပါတ်ကို အမြဲတမ်း dial လုပ်ရပါတယ်။ ဤတွင်မှ dial-up connection ရယ်လို့ အမည်တွင်လာခြင်း ဖြစ်ပါတယ်။

modem သည် ကွန်ပျူတာမှလာတဲ့ digital signal တွေကို တယ်လီဖုန်းလိုင်းပေါ်ဖြတ်သန်း သွားနိုင်သည့် analog signal တွေအဖြစ် ပြောင်းခြင်း၊ တယ်လီဖုန်းလိုင်းမှလာတဲ့ analog signal တွေကို ကွန်ပျူတာမှ နားလည်နိုင်သော digital signal များအဖြစ် ပြောင်းခြင်းတို့ကို လုပ်ဆောင်ပေးသော ကြားခံ device ဖြစ်ပါတယ်။ အဲဒီ conversion အတွက် အချိန်ယူရပါတယ်။ ဒါကြောင့် dial-up connection သည် ကုန်ကျစရိတ်အသက်သာဆုံးဖြစ်သလို speed အားဖြင့်လည်း အနှေးဆုံးဖြစ်ပါတယ်။ modem တစ်ခု၏ သီအိုရီအရ အမြင့်ဆုံးလုပ်ဆောင်နိုင်သော standard speed သည် 56 kbps ဖြစ်ပါတယ်။ တကယ့်လက်တွေ့ အသုံးပြုမှုမှာတော့ အဲဒီလောက် မရနိုင်ပါဘူး။ အသုံးပြုသူ၏ ကွန်ပျူတာကနေ ISP မှ RAS (remote access server) ရောက်သည်ထိ ကြားမှာ ဖြတ်သန်းခဲ့ရတဲ့ တယ်လီဖုန်းလိုင်း၏ အရည်အသွေး၊ central office (CO) လို့ခေါ်တဲ့ အိတ်ချိန်းရုံး အရေအတွက်တို့ပေါ်မူတည်ပြီး 10 မှ 30 kbps ထိ လျော့နည်းသွားနိုင်ပါတယ်။

သို့သော်ငြားလည်း တယ်လီဖုန်းလိုင်းရှိသော မည်သည့်နေရာကနေမဆို အင်တာနက်ချိတ်ဆက်နိုင်ကြသည့် အတွက် broad band connection (မြန်နှုန်းမြင့်ဆက်ကြောင်း) မရနိုင်တဲ့ နေရာမျိုးနှင့် connection အတွက်ငွေကြေးများများ မစိုက်ထုတ်လိုတဲ့အခါမျိုးတွေမှာ ရွေးချယ်အသုံးပြုကြလေ့ရှိပါတယ်။

Dial-Up MODEM



DSL (Digital Subscriber Line)

အင်တာနက်ချိတ်ဆက်တဲ့နေရာမှာ modem တွေသည် အတော်လေးကို အရေးပါအရာရောက်လှ ပါတယ်။ ဖုန်းလိုင်းရှိတဲ့ မည်သည့်နေရာကမဆို modem ရှိတဲ့ ကွန်ပျူတာဖြင့် အင်တာနက်သို့ချိတ်ဆက်နိုင်ကြ ပါတယ်။ အဲဒီနေရာမရွေးတဲ့ အားသာချက်အရပင် dial-up connection ဖြင့် အင်တာနက် ချိတ်ဆက် အသုံးပြုမှုသည် ယနေ့တိုင်တွင် ကျယ်နေဆဲဖြစ်ပါတယ်။ ဒါပေမယ့် dial-up modem တွေမှာ အချို့သော အားနည်းချက်တွေလည်း ရှိပါတယ်။ အဓိကကတော့ modem တွေသည် လူတွေ ဖုန်းပြောသကဲ့သို့ တယ်လီဖုန်း လိုင်းကို အသုံးပြုခြင်း ဖြစ်ပါတယ်။ သည့်အတွက်ကြောင့် အင်တာနက် ချိတ်ဆက်ထားချိန်မှာ ဖုန်းသုံးလို့ မရပါဘူး။ ထို့အတူ ဖုန်းပြောနေချိန်မှာ အင်တာနက်သုံးလို့ မရပါဘူး။

နောက်ထပ်အားနည်းချက်ကတော့ speed ပင် ဖြစ်ပါတယ်။ သီအိုရီအရ dial-up connection ရဲ့ အမြင့်ဆုံး speed ဖြစ်တဲ့ 56 kbps သည် အသုံးပြုသူ user တစ်ဦးတစ်ယောက်အတွက် တော့ လုံလောက်ကောင်း လုံလောက်ပါလိမ့်မယ်။ အချို့သော အသုံးပြုသူတွေအတွက် ကံသေကံမပြောလို့ မရပါဘူး။

ယနေ့ email အသုံးပြုမှုပုံစံသည် ဟိုတုန်းကလို သာမန် message ပို့ရုံသက်သက်မဟုတ်ပါဘူး။ အတော်များများက file တွေ၊ program တွေကို email နှင့်အတူ တွဲပို့လေ့ရှိကြပါတယ်။ အဲဒီ attached file ကြီးရင်ကြီးသလို မိမိကွန်ပျူတာထဲရောက်ဖို့ရန် အချိန်များစွာပေးရပါတယ်။ web surf လုပ်တဲ့နေရာမှာလည်း ထိုနည်းလည်းကောင်းပါပဲ။ ယနေ့ webpage အတော်များများတွင် graphic တွေ၊ animation တွေများစွာ ထည့်သွင်းဖန်တီးထားလေ့ရှိသည့်အတွက် dial-up connection နှင့်သာဆိုရင် webpage တစ်ခု တက်လာဖို့ရန် အတော်လေးကြာတတ်ပါတယ်။

ခြုံငုံပြီးပြောရရင် ယနေ့အသုံးပြုမှု လိုအပ်ချက်တွေကို ပြည့်မှီအောင် မဖြည့်ဆည်းနိုင်တော့လို့ဆိုရ ပါလိမ့်မယ်။ ဤတွင်မှ တယ်လီဖုန်းလိုင်းကို သုံးပြီး ပိုမိုမြန်ဆန်သော နှုန်းဖြင့်လည်း data အပို့အယူလုပ်နိုင်ရမယ်။ ဖုန်းပြောခြင်းနှင့် အင်တာနက်အသုံးပြုခြင်းတို့လည်း တပြိုင်နက်လုပ်ဆောင်နိုင်မည့် နည်းပညာသစ်တစ်ခုဖြင့် အစားထိုးခဲ့ကြပါတယ်။ အဲဒီနည်းပညာကတော့ DSL ပင် ဖြစ်ပါတယ်။

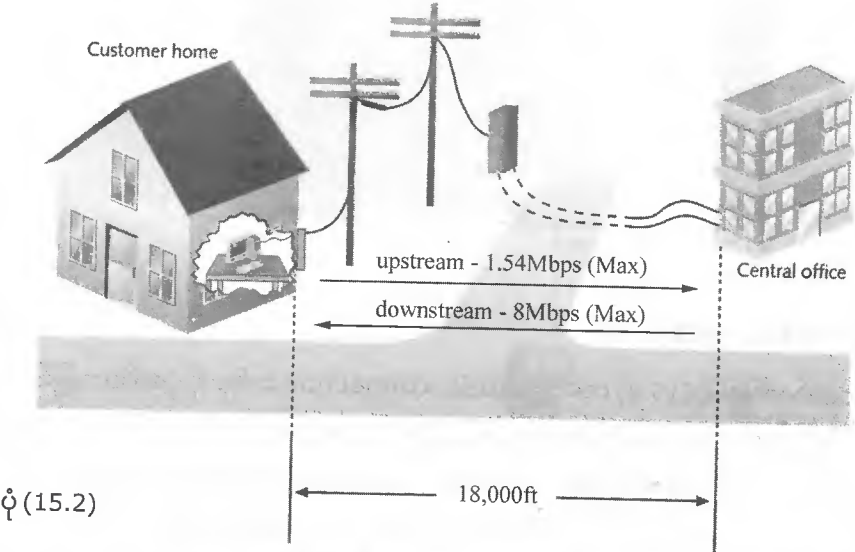
DSL သည် 1990 ပြည့်နှစ်လယ်လောက်မှ စတင်အသုံးပြုလာခဲ့သော WAN connection တစ်ခုဖြစ်ပါတယ်။ PSTN လို့ခေါ်တဲ့ယနေအသုံးပြုနေကြတဲ့တယ်လီဖုန်းလိုင်း (Public Switch Telephone Network) ပေါ်မှ တဆင့်အနည်းဆုံး 15000ft ထိကိုကြားမှာ signal ကို မြင့်တင်ပေးရသည့် repeater တို့ကဲ့သို့ device တွေမလိုအသုံးပြုနိုင်ခြင်း၊ တယ်လီဖုန်းလိုင်းတိုင်းတည်းကို analog signal (voice) တို့နှင့် share လုပ်ပြီး အသုံးပြုနိုင်ခြင်းတို့ကြောင့် အသုံးများတွင်ကျယ်လာခဲ့ပါတယ်။

Type of DSL

DSL speed သည် အသုံးပြုသူ user နှင့် တယ်လီဖုန်းအိတ်ချိန်း (Central office) CO တို့ကြား အကွားအဝေးအပေါ်များစွာမူတည်ပါတယ်။ အိတ်ချိန်းရုံးနှင့် အသုံးပြုသူတို့ကြား အကွားအဝေးသည် 18000ft ထက် မပိုရပါဘူး။ 18000ft ထက် ပိုခဲ့မယ်ဆိုရင်တော့ signal lost ဖြစ်ပြီး speed ကျခြင်းနှင့် connection ပိုင်းဆိုင်ရာ ပြဿနာများကြုံရတတ်ပါတယ်။

DSL အမျိုးအစားကို ခွဲခြားတဲ့နေရာမှာ ယေဘုယျအားဖြင့် Upstream နှင့် Downstream တို့ပေါ်မူတည်ပြီး ၂ မျိုး ၂ စားခွဲခြားပြောဆိုလေ့ရှိပါတယ်။ downstream ဆိုတာက CO ကနေ user ဆီသို့ data သွားနှံ့ခြင်း၊ upstream သည် user မှ CO သို့ဖြစ်ပါတယ်။ downstream သည် upstream ထက် ပိုမြင့်ပါက Asymmetric DSL (ADSL) ဟုခေါ်ပါတယ်။

အထူးသဖြင့် ADSL ကို အင်တာနက်ချိတ်ဆက်တဲ့ နေရာအတွက် အသုံးများပါတယ်။ နောက်တမျိုးကတော့ upstream နှင့် downstream တူတဲ့ symmetric DSL ဖြစ်ပါတယ်။ symmetric DSL (SDSL၊ HDSL) ကို banking system တွေမှာ အသုံးများပါတယ်။ အင်တာနက်အတွက် သီးသန့် အသုံးပြုလေ့မရှိပါဘူး။

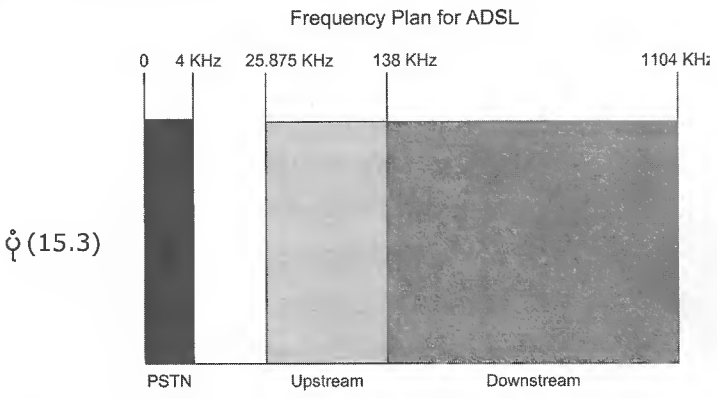


Asymmetric Digital Subscriber Line (ADSL)

ADSL Operation

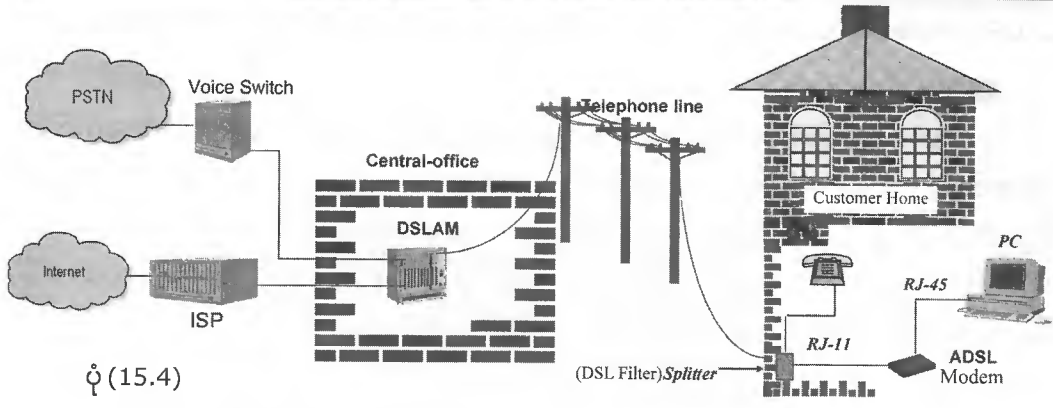
လူသုံးအများဆုံး DSL အမျိုးအစားဖြစ်သည့် ADSL ၏ အမြင့်ဆုံး downstream သည် 8Mbps ဖြစ်ပြီး upstream သည် 1.54Mbps ဖြစ်ပါတယ်။ ဒါပေမယ့် အသုံးပြုသူနှင့် CO တို့အကွာအဝေးပေါ် မူတည်ပြီး ကွာခြားမှုရှိသည့်အတွက် CO နှင့်နီးလေ speed မြင့်လေဖြစ်ပါလိမ့်မယ်။ ဆိုရင် central office နှင့် ပေ ၉၀၀၀ အကွာမှ အသုံးပြုသူအဖို့ ADSL ၏ အမြင့်ဆုံး downstream ဖြစ်တဲ့ 8Mbps ကို ရရှိနိုင်သော်လည်း ပေ 18000 လောက်က အသုံးပြုသူများအဖို့ အဲဒီလောက်ရမှာမဟုတ်ပါဘူး။ အကွာအဝေး အပြင်တယ်လီဖုန်းလိုင်းရဲ့ quality သည်လည်း လွန်စွာအရေးပါသော အချက်တစ်ချက်ဖြစ်ပါတယ်။ ဒါ့ကြောင့် အကွာအဝေးနှင့် လိုင်းအရည်အသွေးတို့သည် ADSL speed ကောင်းမကောင်းဆိုတာကို ဆုံးဖြတ်ပေးနိုင်တဲ့ အခြေခံအချက်တွေလို့ဆိုနိုင်ပါတယ်။

ဒီနေရာတွင် ADSL သည် တယ်လီဖုန်းလိုင်း တစ်လိုင်းတည်းကို voice signal တို့နှင့် ဘယ်လို မျှဝေသုံးစွဲသလဲဆိုတာကို ရှင်းပြလိုပါတယ်။ တယ်လီဖုန်းမှလာတဲ့ စကားသံ (analog signal) တွေရဲ့ frequency သည် 0 မှ 4000Hz တွင်းသာရှိပါတယ်။ ဆိုရင် စကားသံအများစုသည် pitch နှင့် tone ပေါ်မူတည်ပြီး 300Hz မှ 3300Hz တွင်းသာဖြစ်ပါတယ်။ DSL signal တွေအတွက် 4000Hz ထက်ပိုသော frequency ကို အသုံးပြုကြပါတယ်။ အဲဒီလို တယ်လီဖုန်းအတွက် အသုံးပြုရသည့် frequency range (0 to 4000Hz) နှင့် လွတ်ကင်းသည့် frequency ကို အသုံးပြုထားသည့်အတွက် ဖုန်းဖြင့် စကားပြောဆိုနိုင်ခြင်း၊ နားထောင်ခြင်းတို့ကို အနှောင့်အယှက်မပြုနိုင်ပါဘူး။



ADSL Connectivity

တဖက်ဖော်ပြပါပုံ(15.4) ကတော့ ADSL connection တစ်ခုကို ပုံဖော်ထားခြင်းဖြစ်ပါတယ်။ တကယ့်လက်တွေ့နှင့်ယှဉ်လျှင် အချို့နေရာတွေမှာ အနည်းငယ်ကွဲလွဲမှုများရှိနေနိုင်သော်လည်း အခြေခံအားဖြင့် ဒီအတိုင်းပင်ဖြစ်ပါတယ်။ အသုံးပြုရန်အတွက် ADSL connection တစ်ခုရရှိရန်အတွက် user ဘက်မှာ ရှိရမယ့် device တွေကတော့ DSL modem နှင့် DSL filter တို့ဖြစ်ကြပြီး central office ပိုင်းမှာ အဓိကအရေးအကြီးဆုံးက DSLAM (Digital Subscriber Line Access Multiplexer) ဖြစ်ပါတယ်။



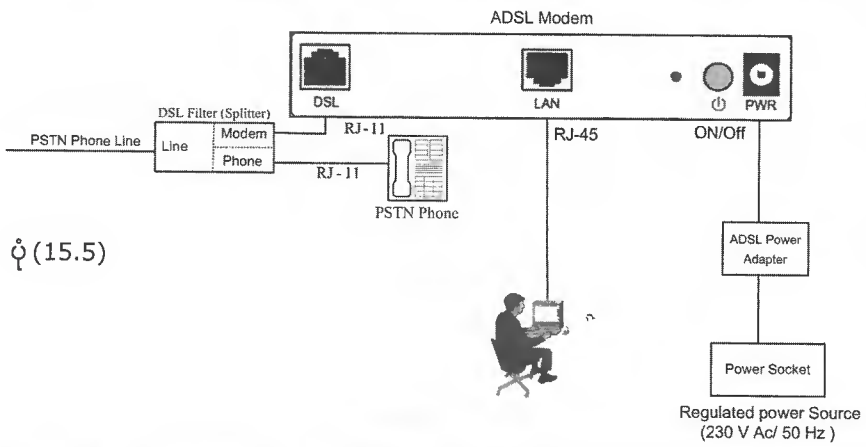
ပုံ (15.4)

ADSL အလုပ်လုပ်ပုံကို သဘောပေါက်နားလည်စေရန် ADSL connection ရှိပြီးသား ကွန်ပျူတာကနေ အင်တာနက်ကြည့်တဲ့ဖြစ်စဉ်ကိုဖော်ပြသွားပါမယ်။

1) Browser program (Internet Explorer) မှာ webpage လိပ်စာ (ဥပမာ - www.google.com) တစ်ခုကိုရိုက်ထည့်တဲ့အခါ http request သည် ကွန်ပျူတာ NIC မှတစ်ဆင့် ADSL modem ထံသို့ digital signal များအဖြစ်ရောက်ရှိသွားပါမယ်။

■ ADSL Modem

ADSL modem ဆိုတာကတော့ ကွန်ပျူတာမှလာတဲ့ digital signal တွေကို DSL signal တွေအဖြစ်သို့ တယ်လီဖုန်းလိုင်းကဝင်လာတဲ့ DSL signal တွေကို digital signal များအဖြစ်သို့ပြောင်းပေးနိုင်တဲ့ device တစ်ခုဖြစ်ပါတယ်။ သူ့ကို CPE (Customer Premise Equipment) လို့လည်းခေါ်ပါတယ်။ ADSL modem တစ်ခုမှာဆိုရင် ကွန်ပျူတာမှ NIC နှင့် ချိတ်ဆက်တပ်ဆင်နိုင်ရန် RJ-45 port တစ်ခု၊ တယ်လီဖုန်းလိုင်းအဝင်မှာခံထားသည့် DSL filter နှင့် ချိတ်ဆက်ရန် RJ-11 port တစ်ခုတို့ပါရှိပါတယ်။



ပုံ (15.5)

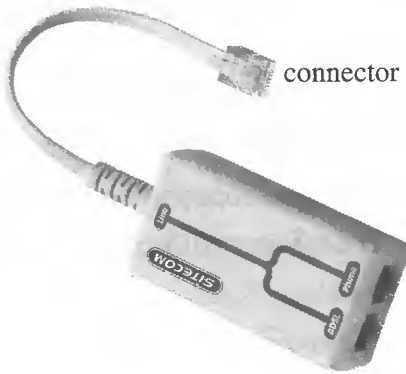
မှတ်ချက်။ ။ ကွန်ပျူတာတစ်လုံးထက်ပိုပြီး သုံးမယ်ဆိုရင် DSL modem ကို switch (သို့) SOHO router တို့ဆီသို့ချိတ်ဆက်ရပါမယ်။

2) DSL modemမှထွက်လာတဲ့DSL signalတွေသည်DSL filterထံသို့ရောက်ရှိပါတယ်။

■ DSL Filter

DSL filter ဆိုတာကတယ်လီဖုန်းလိုင်းအဆောက်အဦးအတွင်းသို့ဝင်ဝင်ချင်း main lineမှာကြားခံ တပ်ဆင်ရတဲ့ device တစ်ခုဖြစ်ပါတယ်။ အဲဒီ DSL filter တပ်ဆင်မှု မရှိဘူးဆိုရင် တယ်လီဖုန်းစကား ပြောခွက်ကလာတဲ့ analog signal (voice) တို့ကြောင့် DSL serviceကိုထိခိုက်စေနိုင် သလို၊ DSL signal (data) တို့ကြောင့်လည်း တယ်လီဖုန်းစကားပြောခြင်းကို အနှောင့်အယှက် ဖြစ်စေနိုင်ပါတယ်။ DSL filterတစ်ခုမှာဆိုရင် RJ-11 port နှစ်ခုပါရှိပါတယ်။

ပုံ (15.6)



portတစ်ခုကတယ်လီဖုန်းစကားပြောခွက်သို့ချိတ်ဆက်ရန်ဖြစ်ပြီးကျန် portတစ်ခုက DSL modemဆီသို့ချိတ်ဆက်ရန်ဖြစ်ပါတယ်။အခြားတစ်ဖက်မှာတော့တယ်လီဖုန်းလိုင်းအဝင်ကြိုးတပ်ဆင်ရန် RJ-11 port(သို့) connectorတစ်ခုပါလေ့ရှိပါတယ်။အင်တာနက်အသုံးပြုနေစဉ်အတွင်းဖုန်းပြောမယ်ဆိုရင် DSL modemမှလာတဲ့DSL signal (data)နှင့်တယ်လီဖုန်းခွက်ကလာတဲ့ analog signal (voice) တို့ဒီနေရာမှာပေါင်းဆုံပြီးအထွက်လိုင်းမှတဆင့် central officeသို့ရောက်ရှိကြမှာဖြစ်ပါတယ်။

3) DSL filter မှ ထွက်လာတဲ့ တယ်လီဖုန်းလိုင်းကြိုးသည် central office (အိတ်ချိန်းရုံး) ရှိ splitter ထံသို့ရောက်ရှိမှာဖြစ်ပါတယ်။(ယနေအခါမှာတော့ splitter ကိုDSLAM Unitထဲမှာ cardတခုအနေနှင့် ထည့်သွင်း တည်ဆောက် ထားလေ့ရှိပါတယ်။) splitterသည် ဝင်ရောက်လာတဲ့အထဲက voice နှင့် data တို့ကိုခွဲထုတ်ပေးမည့် deviceဖြစ်ပါတယ်။ဆိုရရင် voice (ဝါ) 4000Hzအောက် low frequency signalတွေကိုတယ်လီဖုန်းအိတ်ချိန်း (PSTN)ဘက်သို့ပို့ခြင်းနှင့် DSL signal (data)တွေကိုDSLAM (Digital Subscriber Line Multiplier) ဆီပို့ခြင်းတို့ကိုလုပ်ဆောင်ပါတယ်။

4) DSLAMသည် central office မှာပင်ထားရှိတဲ့ network deviceဖြစ်ပြီး ဝင်လာတဲ့ DSL signal တွေကို digital signalအဖြစ်သို့ပြောင်းပြီး ISP၏ routerထံသို့ပေးပါတယ်။ ဤနည်းဖြင့်ကွန်ပျူတာမှ http requestသည် ISPမှတဆင့် သက်ဆိုင်ရာ Web serverထံသို့ရောက်ရှိသွားပါလိမ့်မယ်။

Modem Installation

ဒီနေရာမှာ အသုံးပြုမည့် DSL modem သည် အင်တာနက်နှင့် ချိတ်ဆက်နိုင်ရန်အတွက် လိုအပ်သော setting များအားလုံးကို ထည့်သွင်းထားပြီး တာဝန်ပေးသော ISP မှ ထုတ်ပေးသော modem ဖြစ်ရပါမည်။

ပုံ (15.7)



Indicator (LED)

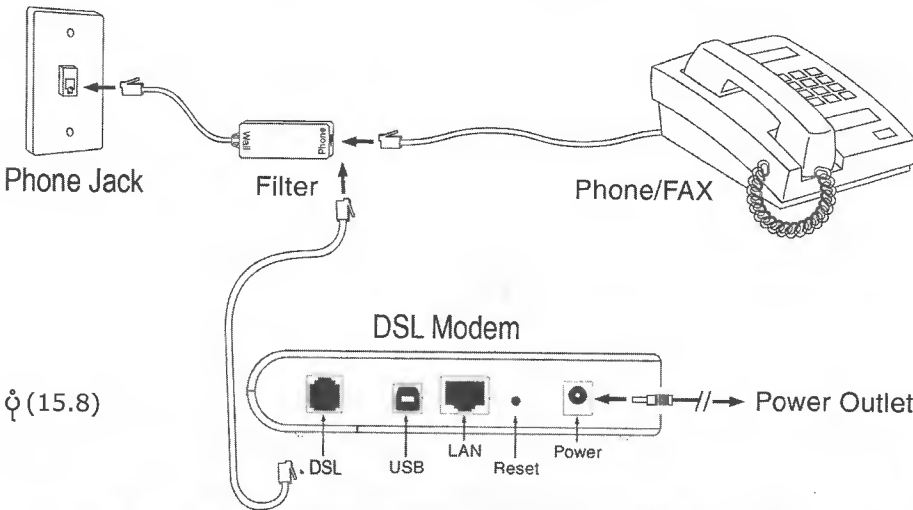
1) modem ကိုမတပ်ဆင်ခင် ပထမဦးစွာ တယ်လီဖုန်းလိုင်းအဝင်မှာ DSL filter (splitter) ကို အရင် တပ်ဆင်ရမှာဖြစ်ပါတယ်။ တပ်ဆင်ပုံကတော့

A- လက်ရှိသုံးနေတဲ့ တယ်လီဖုန်းပလပ်ကြိုးကို နံရံရှိ wall jack မှ ဖြတ်လိုက်ပါ။

B- splitter ကို wall jack မှ တပ်ဆင်ပါ။

C- ခုနက ဖြတ်ထားတဲ့ တယ်လီဖုန်းပလပ်ကြိုးကို splitter ရှိ တယ်လီဖုန်းတပ်ဆင်ရမယ့် RJ-11 port တွင် တပ်ဆင်ပါ။

2) Modem မှ DSL port နှင့် splitter မှ ကျန်လွတ်နေတဲ့ ADSL port တို့ကို တယ်လီဖုန်းကြိုးတစ်ချောင်းဖြင့် ဘိုက်ရိုက်ချိတ်ဆက်တပ်ဆင်ပါ။



ပုံ (15.8)

3) Modemနှင့်အတူတွဲပါလာတဲ့ AC/DC power adapterကို modem၏ PWR portတွင်တပ်ဆင်ပြီး ပါဝါပေးပါ။ ပြီးရင် DSL modem မှပါဝါခလုတ်ကို ဖွင့်လိုက်ပါ။ (အချို့ modem များတွင် ပါဝါခလုတ်မပါပါ။) ပါဝါပိုင်းအဆင်ပြေတယ်ဆိုရင် PWR မှ LED မီးလင်းလာပါလိမ့်မယ်။

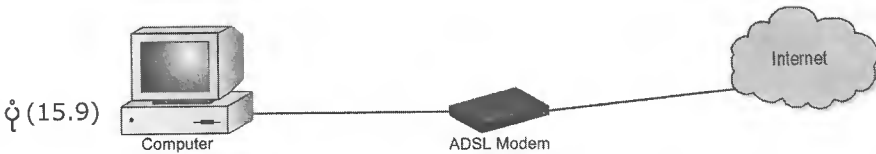
4) ပါဝါပြုဆိုရင် modem သည်ကောင်းမွန်စွာလုပ်ဆောင်နိုင်သော အခြေအနေတွင်ရှိမရှိဆိုတာကို သူ့ဘာသာ self-test လုပ်ပြီး စစ်ဆေးပါလိမ့်မယ်။ အဲဒီလို self-test လုပ်နေစဉ်အတွင်းမှာဆိုရင် DIAG (Diagnostic) မီးသည် စက္ကန့်အနည်းငယ်မျှလင်းနေပါလိမ့်မယ်။ စစ်ဆေးအောင်မြင်သွားပြီဆိုရင် DIAG မီးမှိတ်သွားရပါမယ်။

5) ပုံမှန်အခြေအနေမှာဆိုရင် PWR-LAN-DSL ဆိုတဲ့ LED သုံးခုသာ လင်းနေရမှာဖြစ်ပါတယ်။ သို့သော် ဒီနေရာမှာတော့ ကွန်ပျူတာနှင့်ချိတ်ဆက်ရန် LAN ကြိုးမတပ်ရသေးသည့်အတွက် PWR နှင့် DSL မီးတို့လင်းနေသင့်ပါတယ်။ DSL မီးလင်းပြီဆိုရင် တယ်လီဖုန်းလိုင်းကောင်းမွန်သည့်အတွက် modem နှင့် DSLAM တို့ချိတ်ဆက်မိပြီး အင်တာနက်ဆက်ကြောင်းသည် မိမိ modem ဆီသို့ ရောက်ရှိနေပြီလို့ မှတ်ယူနိုင်ပါတယ်။ ဒါဆိုရင် အင်တာနက်သုံးနိုင်အောင် မိမိကွန်ပျူတာနှင့် modem တို့ ချိတ်ဆက်ရန်သာ လိုပါတော့တယ်။

Connecting Your Computer to Modem

အင်တာနက်သုံးနိုင်အောင် ကွန်ပျူတာနှင့် modem တို့ချိတ်ဆက်တဲ့နေရာမှာ မိမိတို့ရဲ့အသုံး လိုမှုပေါ်မူတည်ပြီး နည်းလမ်းအမျိုးမျိုးတို့ဖြင့်ချိတ်ဆက်အသုံးပြုနိုင်ကြပါတယ်။ အသုံးလိုမှုဆိုတဲ့နေရာမှာ အဓိကအားဖြင့်ကွန်ပျူတာတစ်လုံးတည်းကနေအင်တာနက်သုံးမှာလား၊ သို့တည်းမဟုတ် network ထဲကရှိသမျှ ကွန်ပျူတာတွေ အားလုံးကနေ တပြိုင်နက်သုံးမှာလားဆိုတာကို ရည်ညွှန်းပါတယ်။ တစ်လုံးတည်းသာ internet access ထားရှိမယ်ဆိုရင်တော့ ဘာမှထွေထွေမလိုပါဘူး။ ကွန်ပျူတာနှင့် modem တို့ကို network cable သုံးပြီး တိုက်ရိုက်ချိတ်ဆက်လိုက်ရုံဖြစ်ပါတယ်။ ပုံ (15.9)။ ပြီးရင် ISP မှပေးထားတဲ့ IP address တစ်ခုကို ကွန်ပျူတာမှာ ထည့်သွင်းလိုက်ရုံဖြင့် အင်တာနက်အသုံးပြုလို့ရသွားပါလိမ့်မယ်။

Scenario 1-Directly connect to DSL Modem

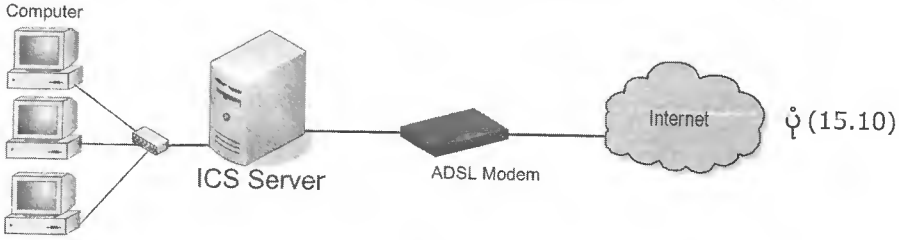


သို့သော် network တွင်းရှိ ကွန်ပျူတာအားလုံးမှာ internet access ရအောင် လုပ်မယ် ဆိုရင်တော့ "internet connection sharing" ဆိုတဲ့ အင်တာနက်ဆက်ကြောင်းတစ်ခုတည်းကို ကွန်ပျူတာများစွာတို့မှ မျှဝေသုံးစွဲနိုင်အောင် လုပ်ဖို့လိုလာပါလိမ့်မယ်။ "Internet connection" ကို

အောက်ဖော်ပြပါ နည်းလမ်း သုံးမျိုးထဲက တစ်မျိုးမျိုးဖြင့် မျှဝေသုံးစွဲနိုင်ကြပါတယ်။

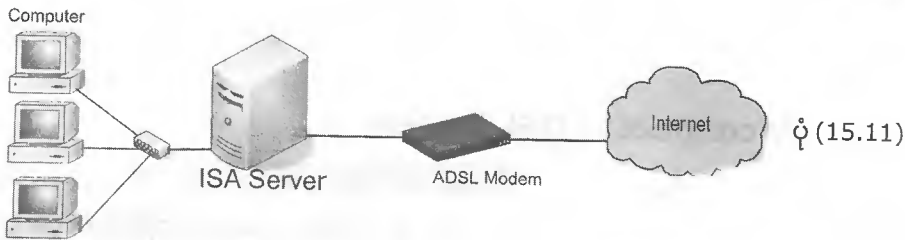
■ Scenario 2-ICS Server

Windows XP တွင် built-in ပါရှိပြီး သားဖြစ်သည့် ICS utility ကို အသုံးပြုခြင်း



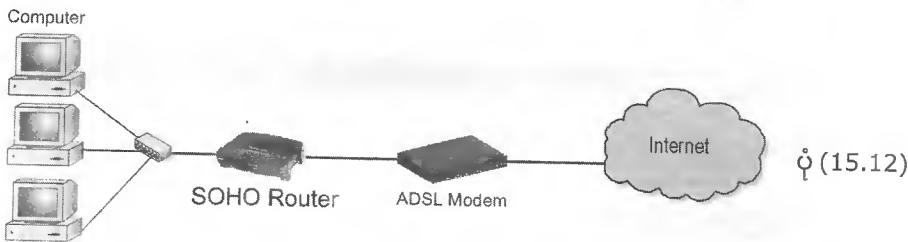
■ Scenario 3-ISA Server

ISA server (Internet Security and Acceleration server) ထားရှိအသုံးပြုခြင်း



■ Scenario 4-SOHO router

DSL modem နှင့် network တို့ကြားမှာ SOHO router ခံပြီး အသုံးပြုခြင်း



ဖော်ပြခဲ့တဲ့ နည်းလမ်း သုံးသွယ်ထဲက scenario 2 နှင့် 3 တို့သည် အပြင်ပန်းအရ တည်ဆောက်ပုံချင်း အတူတူပင် ဖြစ်ကြပါတယ်။ ဒါပေမယ့် ISA ထိုင်မယ်ဆိုရင် သူ့ကို install လုပ်ရန်နှင့် manage လုပ်ရန် အတွက် သာမန် knowledge နှင့် မရတော့ပါဘူး။ ISA server အကြောင်းကို သီးခြားထပ်မံလေ့လာ ဖို့လို ပါလိမ့်မယ်။ ဆိုရရင် ISA server နှင့် အကျွမ်းတဝင် မရှိပါက network administration နှင့် နောက်ပိုင်း ကြုံလာမယ့် trouble shooting ကိစ္စတွေမှာ များစွာ အခက်အခဲရှိလာနိုင်ပါတယ်။ ICS ကျတော့ security နှင့်

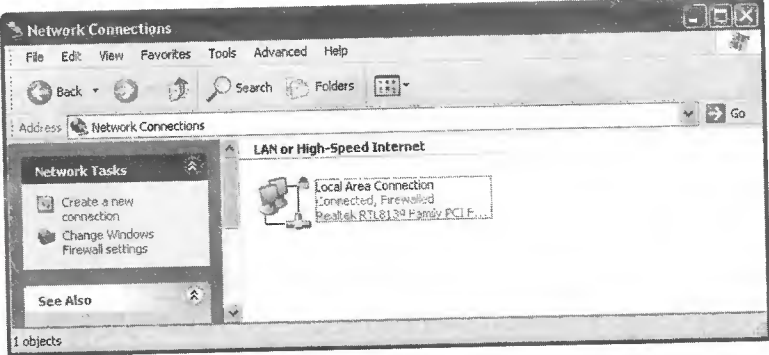
network administration ပိုင်းတွေမှာ ISA လောက်ထိရောက်မှုမရှိသော်လည်း အင်တာနက်ဆက်ကြောင်းကို မျှဝေသုံးစွဲရန်သာအဓိက ရည်ရွယ်တဲ့သာမန် အိမ်သုံးရုံးသုံး network ငယ်တွေမှာ လွန်စွာအသုံးများပါတယ်။

ဘာဖြစ်လို့လဲဆိုတော့ သာမန်အသုံးပြုသူတွေတောင်မှ အနည်းငယ်လေ့လာလိုက်ရုံဖြင့် ICS အကြောင်းကို နားလည်သဘောပေါက်ပြီး configuration ပိုင်းနှင့် trouble shooting ပိုင်းတွေကို လုပ်ဆောင်နိုင်ခြင်းသည်လည်း လူသုံးများရခြင်း၏အကြောင်းရင်းတစ်ရပ်ဖြစ်ပါလိမ့်မယ်။ တတိယနည်းလမ်းဖြစ်တဲ့ SOHO router ကိုကြားခံသုံးမယ်ဆိုရင်လည်း ISA server အသုံးပြုမှုလောက်စီမံခန့်ခွဲမှုကိစ္စတွေမများ ပေမယ့် သီခြား router တစ်လုံးထပ်မံ ဝယ်ယူ တပ်ဆင်ရမှာဖြစ်သည့်အတွက် ကုန်ကျစရိတ်ပိုပါလိမ့်မယ်။

ဤတွင်မှ DSL modem နှင့်ကွန်ပျူတာတို့ချိတ်ဆက်ပုံကိုဖော်ပြတဲ့နေရာမှာပထမဦးစွာကွန်ပျူတာတစ်လုံးတည်းသာအင်တာနက်အသုံးပြုမည့်ဖြစ်စဉ် (Scenario 1) အတွက်လိုအပ်တဲ့ installation နှင့် IP configuration များကိုဖော်ပြပါမယ်။ ပြီးတဲ့အခါမှာနည်းလမ်းသုံးသွယ်ထဲကဝန်အကျဉ်းဆုံးဖြစ်တဲ့ ICS utility (scenario-2) ဖြင့် ineternet connection မျှဝေသုံးစွဲပုံများကိုထပ်မံဖော်ပြသွားမှာဖြစ်ပါတယ်။

Directly connect to DSL Modem

ကွန်ပျူတာသည် NIC တစ်ခုနှင့် ၎င်းအတွက် လိုအပ်သော driver ကို install လုပ်ထားပြီး၍ ကောင်းမွန်စွာအလုပ်လုပ်နေနိုင်တာသေချာသောကွန်ပျူတာဖြစ်ရပါမယ်။ သေချာပြီဆိုရင်ကွန်ပျူတာမှ NIC နှင့် DSL modem မှ LAN port တို့ကို network cable ဖြင့်ချိတ်ဆက်လိုက်ပါ။ ကွန်ပျူတာပါဝါဖွင့်ပြီးသားဆိုရင် DSL modem မှ LAN ဖိလင်းလာပါလိမ့်မယ်။ ကွန်ပျူတာတွင် control panel မှတစ်ဆင့် network connection ကိုဖွင့်လိုက်ပါ။ (network connection ဖွင့်ပုံကိုစာ (၁၃၄) တွင်ကြည့်ပါ) အောက်ဖော်ပြပါအတိုင်း မြင်ရသင့်ပါတယ်။



ပုံ (15.13)

ဒါဆိုရင် အင်တာနက်အသုံးပြုရနိုင်သော ကွန်ပျူတာအဖြစ်သို့ရောက်ရှိအောင် IP configuration အပါအဝင်လိုအပ်သော setting များကိုစတင်ထည့်သွင်းနိုင်ပါပြီ။ အဲဒီလိုထည့်သွင်းနိုင်ရန်အတွက် ISP

မှအောက်ဖော်ပြပါ information များ ရှိပြီးသား ဖြစ်ရပါမယ်။ မိမိထံမရှိပါက တောင်းယူရပါမယ်။ ဥပမာအနေနှင့် ဖော်ပြရရင်

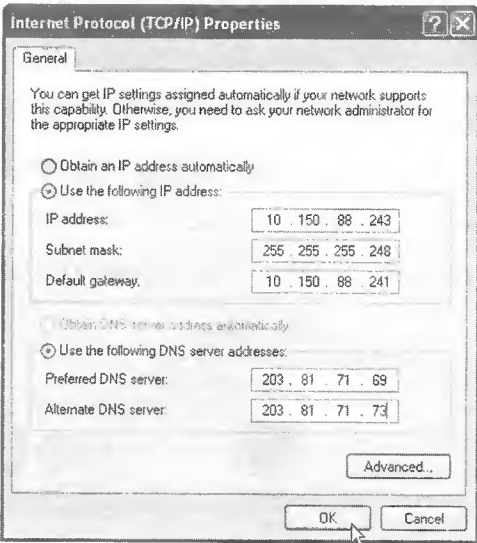
computer IP address	-	10.150.88.243
subnet mask	-	255.255.255.248
Default Gateway	-	10.150.88.241
primary DNS	-	203.81.71.69
secondary DNS	-	203.81.71.73

1) ဖော်ပြခဲ့တဲ့ information တွေအဆင်သင့်ရှိပြီဆိုရင် "network connection" window ထဲရှိ local area connection တွင် right click နှိပ်ပြီး ကျလာမည့် submenu ထဲရှိ **properties** တွင် click တစ်ချက်နှိပ်ပါ။ "Connection Properties" dialogue box ပွင့်လာပါလိမ့်မည်။

2) **Internet protocol (TCP/IP)** တွင် double click နှိပ်ပါက "TCP/IP properties" dialogue box ကျလာပါလိမ့်မယ်။ "use the following IP address" ဘေးရှိ radio button တွင် ဖြစ်အောင် ရွေးချယ် click နှိပ်ပြီး **IP address** ၊ **Subnet mask** နှင့် **Default gateway** တို့ကို တိုတိုရိုက်ထည့် ရပါမယ်။

3) "use the following DNS" ဘေးရှိ radio button တွင် ဖြစ်အောင် click နှိပ်ပြီး **primary DNS** နှင့် **secondary DNS server** တို့၏ IP address များကို ရိုက်ထည့်ပါ။

ပုံ (15.14)



4) "TCP/IP properties" dialog box ရှိ **OK** button တွင် click နှိပ်ပါက dialog box ဝိတ်သွားပြီး မူလ "Local Area Connection properties" သို့ပြန်ရောက်သွားပါမယ်။

5) "Local Area Connection properties" ရှိ **OK** button တွင် ထပ်မံ click နှိပ်လိုက်ပါ။ ဒါဆိုရင် ကွန်ပျူတာမှာ NIC အတွက် လိုအပ်တဲ့ setting တွေကို ထည့်သွင်းသတ်မှတ်ပြီး သွားပြီး အင်တာနက် ဆက်ကြောင်းသည် modem မှတဆင့် မိမိကွန်ပျူတာဆီရောက်ရှိလာပြီလို့မှတ်ယူနိုင်ပါပြီ။

● Testing Your Connectivity

ယခုဖော်ပြသွားမှာကတော့ မိမိကွန်ပျူတာသည် အင်တာနက်နှင့် ချိတ်ဆက်မိခြင်းရှိမရှိဆိုတာကို သေချာအောင်စစ်ဆေးပုံအဆင့်ဆင့်တို့ဖြစ်ပါတယ်။ ကွန်ပျူတာတစ်လုံးမှာ IP setting များထည့်သွင်းပြီးစ အခါမှာသော်လည်းကောင်း၊ အင်တာနက်ကြည့်နေရင်းနှင့် လတ်တလော အသုံးပြု၍ မရနိုင်တော့တဲ့အတွက် troubleshoot လုပ်လိုတဲ့အခါမှာသော်လည်းကောင်း ဖော်ပြသွားမယ့် အဆင့်များအတိုင်း စစ်ဆေး ဖြေရှင်းနိုင်ကြပါတယ်။

step1) IP configuration

command window တွင် **ipconfig/all** ဟုရိုက်ထည့်ပြီး enter နှိပ်ပါ။ မိမိကွန်ပျူတာ မှာထည့်သွင်းထားတဲ့ IP configuration များကို မြင်ရပါမယ်။ **Computer IP address** ၊ **Subnet mask** ၊ **Default gateway**၊ **DNS server** တို့ကိုမှန်မမှန် စစ်ဆေးပါ။

step2) PING computer IP address

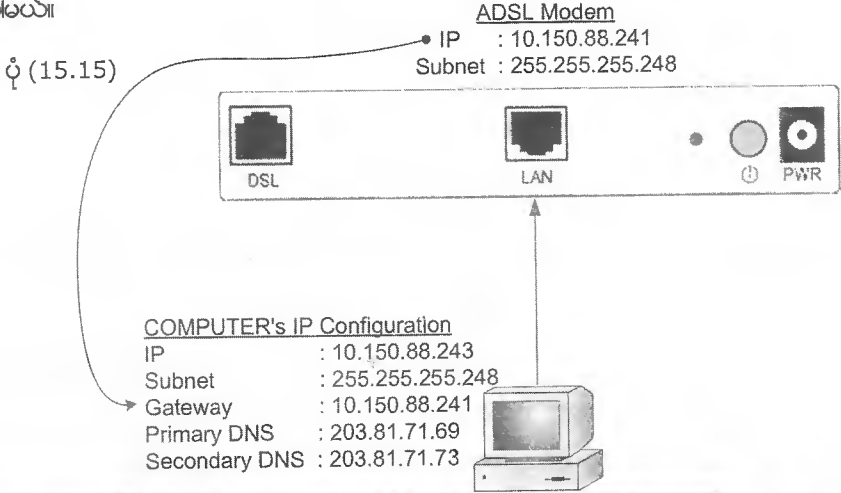
IP configuration အားလုံးမှန်တယ်ဆိုရင် ပထမဦးစွာ မိမိကွန်ပျူတာ IP address ကိုအရင် ping ရပါမယ်။

```
c:\>ping 10.150.88.243
```

reply ပြန်ရပါမယ်။ ဒါဆိုရင် မိမိကွန်ပျူတာမှ NIC သည် ကောင်းမွန်စွာလုပ်ဆောင်နိုင်သော အခြေအနေတွင်ရှိတယ်လို့မှတ်ယူနိုင်ပါပြီ။

step3) ping IP address of default gateway

default gateway ၏ ip address ကို ping ရပါမယ်။ ကွန်ပျူတာ၏ default gateway သည် modem မှ LAN IP address ဖြစ်ပါတယ်။ ပုံ(15.15) တွင်ကြည့်ပါ။ ၎င်း IP address ကို modem တွင် ISP မှထည့်သွင်း ထားပေးပြီးသား ဖြစ်ပါတယ်။ ထို default gateway နှင့် ကွန်ပျူတာ IP တို့သည် network ID တူရပါမယ်။



c:\>ping 10.242.80.80

reply ပြန်ရပါမယ်။ ဒါဆိုရင် မိမိကွန်ပျူတာနှင့် DSL modem တို့ကောင်းမွန်စွာချိတ်ဆက်မိပြီလို့ မှတ်ယူနိုင်ပါပြီ။

step4) Ping host name (or) IP address of remote host

ဒီအဆင့်မှာဆိုရင် remote host လို့ခေါ်တဲ့ ISP မှာရှိနေသော server ကွန်ပျူတာတစ်လုံးလုံး (ဥပမာ - proxy server mail server DNS server) ကိုသော်လည်းကောင်း၊ အင်တာနက်မှ webserver (ဥပမာ - google yahoo CNN) တစ်လုံးလုံးကို ကိုသော်လည်းကောင်း လှမ်း ping ကြည့်ခြင်းဖြင့် မိမိကွန်ပျူတာသည် ISP နှင့် ချိတ်ဆက်မိပြီ၊ မမိဘူးဆိုတာကို ဆုံးဖြတ်ပေးနိုင်ပါတယ်။

c:\>ping 203.81.71.69
c:\>ping www.google.com

ပုံမှန်အားဖြင့် reply ပြန်သင့်ပါတယ်။ reply ဖြစ်ပါက မိမိကွန်ပျူတာက ပေးပို့လိုက်တဲ့ ping packet တွေသည် ISP မှ server ထံသို့ ဂျောက်မယ်။ ထိုမှတစ်ဖန် server က သူ့ရှိနေကြောင်း ရည်ညွှန်းတဲ့ packet တွေကို မိမိကွန်ပျူတာထံသို့ ပြန်ပို့လိုက်တယ်။ ဤတွင် မှ မိမိကွန်ပျူတာမှ "reply from"၊ bytes-32၊ time အစရှိတဲ့ reply message တွေကို မြင်ရမယ်ပေါ့။ ဒါဆိုရင် ISP နှင့် ချိတ်ဆက်မိပြီလို့ဆိုနိုင်ပြီ။ ဆက်ဆိုရရင် ISP နှင့် ချိတ်ဆက်ပြီးဖြစ်သည့်အတွက် အင်တာနက်နှင့်လည်း အဆက်အသွယ်ရပြီလို့မှတ်ယူနိုင်ပါပြီ။

ဒါပေမယ့် ဒီနေရာမှာ အောင်မြင်တဲ့ reply message လည်း မဟုတ်၊ request tomeout လည်း မဟုတ်တဲ့ "destination host unreachable" ဆိုတာမျိုးကို မြင်ရတတ်ပါတယ်။ ၎င်း unreachable ဆိုတဲ့ message မျိုးကို အများအားဖြင့် ISP မှ ping test ခွင့်မပြုတဲ့ အခါမျိုးတွေမှာ တွေ့ရတတ်ပါတယ်။ modem နှင့် ISP တို့ကြားမှာ connection ရှိမရှိဆိုတာကို ခွဲခြားမရနိုင်တဲ့ message မျိုးလည်း ဖြစ်ပါတယ်။ တနည်းဆိုရရင် ချိတ်ဆက်မိပါသည်ဟု ပြော၍မရနိုင်သလို ချိတ်ဆက်မိခြင်းမရှိပါဘူးဟုလည်း ပြော၍မရနိုင်သော reply message ဖြစ်ပါတယ်။ အဲဒီလို ping test ခွင့်မပြုတာမျိုးနှင့် ကြုံလာပြီဆိုရင် မိမိ modem နှင့် ISP တို့ကြားမှာ connection ရှိမရှိဆိုတာကို စစ်ဆေးနိုင်တဲ့ အခြား command တစ်ခုရှိပါတယ်။ nslookup ဆိုတာပဲဖြစ်ပါတယ်။

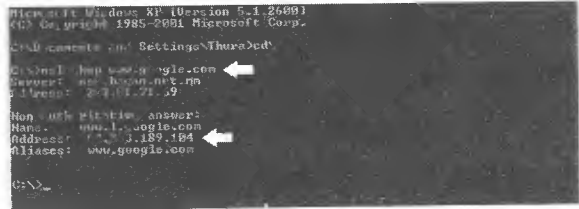
step5) Asking to DNS (Nslookup)

DNS server ဆိုတာက တော့ host name နှင့် သက်ဆိုင်ရာ IP address တို့ရဲ့စာရင်းကို သိမ်းဆည်းထားသော ကွန်ပျူတာဖြစ်ပြီး အဓိကလုပ်ဆောင်မှုက name resolution ဖြစ်ပါတယ်။ သဘောက www.google.com ရဲ့ ip ဘယ်လောက်လို့မေးလာခဲ့ရင် list ထဲမှာ ရှာဖွေပြီး 64.233.289.104 ပါလို့ ပြန်ဖြေခြင်းမျိုး ဖြစ်ပါတယ်။ အင်တာနက်သုံးတဲ့ ကွန်ပျူတာတွေမှာ ထည့်သွင်းထားသည့် DNS server (203.81.71.69၊ 203.81.71.73) ဆိုတာတွေသည် ISP တွင်ထားရှိသော DNS server ကွန်ပျူတာတွေ ဖြစ်ပါတယ်။ အဲဒီ DNS server တွေနှင့် အမေးအဖြေလုပ်လို့ရပြီဆိုရင် မိမိကွန်ပျူတာသည် ISP နှင့် အဆက်အသွယ်ရှိနေတယ်လို့ဆိုနိုင်ပါပြီပေါ့။

ပုဂံမာအနေနှင့် www.google.com ၏ IP ဘယ်လောက်လဲဆိုတာကို DNS server အားလှမ်းမေးကြည့်ရင်းဖြင့် မိမိကွန်ပျူတာသည် အင်တာနက်နှင့် ချိတ်ဆက်မိခြင်း ရှိမရှိဆိုတာကို စမ်းသပ်ကြည့်ရအောင်။။

command window တွင် **c:\>nslookup www.google.com** ဟု ရိုက်ထည့်ပြီး enter နှိပ်ပါ။ ISP ရှိ DNS server က မှ ပြန်ဖြေတယ်ဆိုရင် အောက်ပါပုံ (15.16) အတိုင်း မြင်ရပါလိမ့်မယ်။

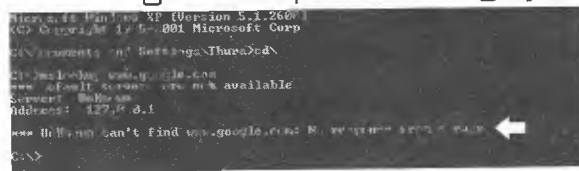
ပုံ (15.16)



အများအားဖြင့် primary DNS server မှ ပြန်ဖြေပါလိမ့်မယ်။ အကြောင်းတစ်ခုခုကြောင့် primary DNS server မှ ပြန်မဖြေနိုင်တဲ့အခါမှသာလျှင် secondary DNS server မှ ပြန်ဖြေမှာဖြစ်ပါတယ်။

DNS request သည် ISP ရှိ DNS server ထံသို့မရောက်တဲ့အခါ တနည်းဆိုရင် မိမိ modem နှင့် ISP တို့ကြားမှာ connection ပြတ်တောက်နေပါက အောက်ဖော်ပြပါပုံ (15.17) အတိုင်း မြင်ရပါလိမ့်မယ်။

ပုံ (15.17)



ISP နှင့် အဆက်အသွယ် ရှိရှိမှန်ရင် primary (သို့) secondary DNS server တစ်လုံးလုံးမှ ဖြေကိုဖြေမှာဖြစ်ပါတယ်။

● Internet Connection Sharing (Scenario 2)

● Preparing for ICS

ယခုဖော်ပြသွားမှာကတော့ network အတွင်းရှိ ကွန်ပျူတာတိုင်းကနေ အင်တာနက် အသုံးပြုနိုင်အောင် ပြင်ဆင်ပုံများပဲဖြစ်ပါတယ်။ သဘောကတော့ DSL modem နှင့် network ကွန်ပျူတာ တို့ကြားမှာ ICS server ထားမယ်။ ပြီးရင် ICS server မှတဆင့် network တွင်းရှိ အခြားကွန်ပျူတာများ အားလုံးဆီသို့ ဖြန့်ဝေပေးမယ်ပေါ့။ အရေးကြီးတာက ICS server အဖြစ်အသုံးပြုမည့် ကွန်ပျူတာတွင် NIC နှစ်ခုရှိရပါမယ်။ တစ်ခုက အင်တာနက် အတွက် (DSL modem ဖြင့်ချိတ်ဆက်ရန်) ဖြစ်ပါတယ်။ NIC နှစ်ခုရှိလာတဲ့အတွက် ၂ခုစလုံးမှာ IP configuration လုပ်ဖို့လိုလာပါလိမ့်မယ်။

DSL modem ဖြင့်ချိတ်ဆက်မယ့်အပိုင်းသည် ရှေ့မှာဖော်ပြခဲ့တဲ့ Scenario 1 အတိုင်းဖြစ်ပါတယ်။ ဒို့ကြောင့် ICS server ဖြင့် ယခုမှ စတင်ထိတွေ့မည့်သူများအနေနှင့် ကွန်ပျူတာတစ်လုံးမှာ NIC တစ်ခု တပ်ဆင်ပြီး **Scenario 1** ကလုပ်ငန်းစဉ်များအတိုင်း အင်တာနက်နှင့် ချိတ်ဆက်မိသည်အထိ လုပ်ဆောင်သင့်ပါတယ်။ connection ရတာသေချာပြီဆိုမှ နောက်ထပ် NIC တစ်ခုကို ထပ်တိုးတပ်ဆင်ပြီး ICS server အဖြစ်သို့ ရောက်ရှိအောင် လုပ်ဆောင်မယ်ဆိုရင် ပိုအဆင်ပြေပါလိမ့်မယ်။

ဆိုရရင် ဒီနေရာမှာ ICS server တည်ဆောက်ရန်အတွက် အသုံးပြုမည့် ကွန်ပျူတာသည် NIC တစ်ခုတပ်ဆင်ထားပြီး internet access ရရှိပြီးသားလို့ မှတ်ယူလိုက်ရအောင်။ ဤတွင်မှ switch နှင့်ချိတ်ဆက်ရန်အတွက်နောက်ထပ် NIC တစ်ခုကိုထပ်တိုးတပ်ဆင်ရပါမယ်။ NIC တပ်ဆင်ပြီးပါကလိုအပ်တဲ့ driver ကို install လုပ်ပြီး switch နှင့်ချိတ်ဆက်တပ်ဆင်ရပါမယ်။

Configuring ICS Server

step1) rename network connections

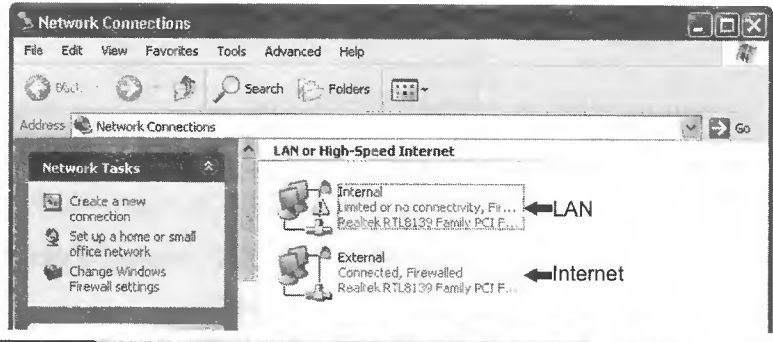
ICS server ကွန်ပျူတာအတွင်းသို့ administrator account ဖြင့် logon ဝင်ရောက်ပြီး network connection ကိုဖွင့်လိုက်ပါ။ NIC ၂ခုစလုံးကောင်းမွန်စွာအလုပ်လုပ်နေနိုင်တာ သေချာတယ်ဆိုရင် ပုံမှန် default အားဖြင့် "Local Area Connection" နှင့် "Local Area Connection 2" ဆိုပြီး "network connection" icon ၂ခုကိုတွေ့ရပါလိမ့်မယ်။

ပုံ (15.18)



ပထမဦးဆုံးလုပ်ဆောင်သင့်တာက ၎င်း network connection ၂ခုထဲက ဘယ်ဟာက local network၊ ဘယ်ဟာက အင်တာနက်ဆိုတာကို အလွယ်တကူခွဲခြားသိနိုင်အောင် အမည်ပြောင်းထားသင့်ပါတယ်။ အမည်ပြောင်းပုံကတော့ connection icon ပေါ်တွင် right click နှိပ်ပြီး ကျလာမည့် sub menu ထဲရှိ rename တွင် click နှိပ်လိုက်ပါ။ အမည်သစ်ပြောင်းပေးနိုင်ရန် အပြာရောင် high light ဖြစ်နေပါလိမ့်မယ်။ ဥပမာအနေနှင့် DSL modem သို့ ချိတ်ဆက်ထားတဲ့ အပြင် NIC ကို external၊ switch ထံသို့ချိတ်ဆက်ထားတဲ့အတွင်း NIC ကို internal လို့အမည်ပြောင်းလိုက်ကြရအောင်။

ပုံ (15.19)

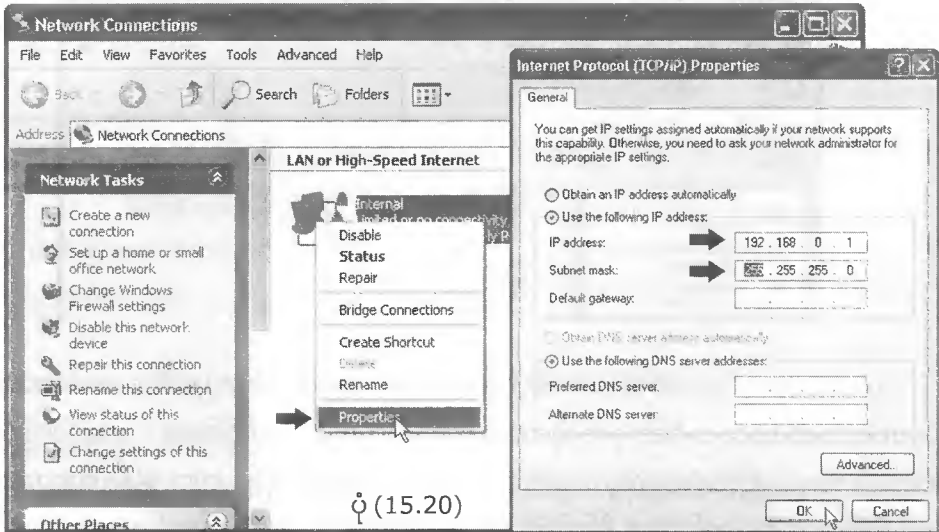


step2) Internal Connection

ထပ်တိုး တပ်ဆင်ထားသော အတွင်း NIC အတွက် IP address ထည့်သွင်းပေးရပါမယ်။ ၎င်း IP address ကို ISP ထံမှ တောင်းယူစရာ မလိုပါ။ မိမိစိတ်ကြိုက် IP address ကို ရွေးချယ်အသုံးပြုနိုင်ပါတယ်။ ဥပမာ အနေနှင့် "class C" ip address တစ်ခုဖြစ်တဲ့ 192.168.0.1 ကို ရွေးချယ်လိုက်ကြရအောင်။

Ip address ထည့်သွင်းရန်အတွက် "internal" icon တွင် right click နှိပ်ပြီး ကျလာမည့် sub menu ထဲရှိ **properties** တွင် click နှိပ်ပါ။ "properties" dialog box ပွင့်လာပါလိမ့်မည်။

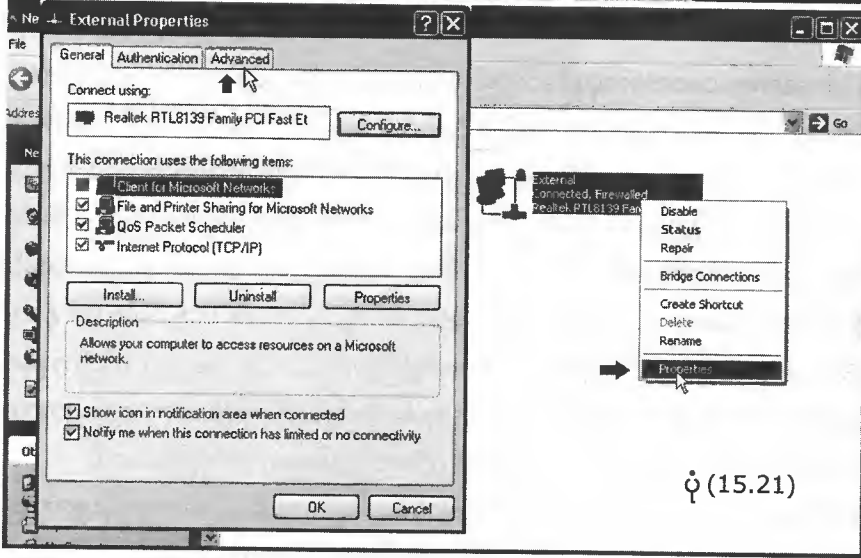
Internet protocol (TCP/IP) တွင် double click နှိပ်ပါက "TCP/IP properties" dialog box ကျလာပါလိမ့်မည်။ "the following IP address" ဘေးရှိ radio button ကို ဖြစ်အောင် ရွေးချယ် click နှိပ်ပြီး IP address နှင့် subnet mask တို့ကို ရိုက်ထည့်ရပါမယ်။ IP address (192.168.0.1) သည် class C ဖြစ်သည့်အတွက် subnet mask သည် 255.255.255.0 ဖြစ်ပါလိမ့်မယ်။



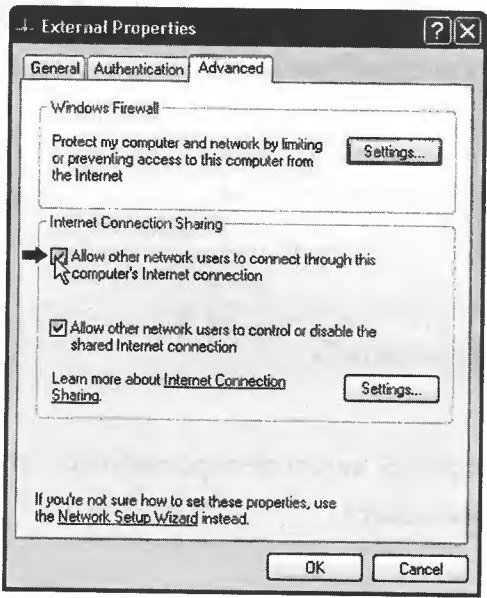
"TCP/IP properties" dialog box ရှိ **OK** button တွင် click နှိပ်ပါ။ "Internal" properties ရှိ **OK** တွင် ထပ်မံ click နှိပ်ပါ။ ဒါဆိုရင် အတွင်း NIC အတွက် IP address ကို ထည့်သွင်းပြီးသား ဖြစ်သွားပါပြီ။

step3) setting up internet connection sharing

"external" သည် လိုအပ်သော setting များ ထည့်သွင်းပြီး ဤ internet access ရရှိပြီးသား NIC ဖြစ်ရပါမည်။ (ရှေး **Scenario 1** က လုပ်ငန်းစဉ်များတွင် ကြည့်ပါ။) "external" လို့ အမည်ပေးထားသည့် connection icon ပေါ်တွင် right click နှိပ်ပြီး ကျလာမည့် sub menu ထဲရှိ **properties** တွင် click နှိပ်ပါ။ "external properties" dialog box ပွင့်လာပါလိမ့်မည်။



"External properties" dialog box ထဲရှိ "advanced" tab တွင် click တစ်ချက်နှိပ်ပါ။ advanced tab အောက်ရှိ "allow other network user" ဘေးရှိ check box ထဲတွင် အမှန်ခြစ် ဖြစ်အောင် select လုပ်ပါ။ ပြီးရင် "External" properties ရှိ **OK** button တွင် click နှိပ်ပါ။



ဒါဆိုရင် Connection sharing လုပ်ခြင်းပြီးဆုံးပြီး အင်တာနက်ဆက်ကြောင်းသည် External လိုအမည်ပေးထားသည်. NIC မှ Internal လိုအမည်ပေးထားသည်. NIC ဆီသို့ရောက်ရှိ လာပြီလို့မှတ်ယူနိုင်ပါပြီ။

Configuring Client Computers

ICS server သဘောကသူနှင့်ဆက်ဆံသူမှန်သမျှကိုသူ့မှာရှိတဲ့ internet connection ကိုမျှဝေသုံးစွဲခွင့်ပေးမယ်ဆိုတဲ့ သဘောဖြစ်ပါတယ်။ အဲဒီလိုမျှဝေပေးဖို့ရန် ICS server တွင် "allow the network user" ဆိုတာကိုရွေးချယ်ပေးခဲ့ပြီးဖြစ်သည့်အတွက် အဆင်သင့်ဖြစ်နေပြီဆိုနိုင်ပါတယ်။

ယခုဆက်လုပ်ရမှာက network တွင်းမှာရှိတဲ့ ကွန်ပျူတာတွေအနေနှင့် ICS server မှ မျှဝေပေးထားတဲ့ connection ကို သုံးနိုင်အောင် တနည်းဆိုရရင် ICS server နှင့် ဆက်သွယ်နိုင်အောင် လုပ်ဖို့ပင် ဖြစ်ပါတယ်။ ဘယ်လိုလုပ်ရမလဲဆိုတာကတော့ လွယ်ပါတယ်။ ICS server နှင့် network တစ်ခုတည်းကျအောင် လုပ်လိုက်ရုံဖြစ်ပါတယ်။ အရေးကြီးတာက ICS server သည် ကျန်ကွန်ပျူတာ အားလုံး၏အင်တာနက်ထွက်ပေါက်ဆိုတာကိုသိထားရပါမယ်။ ဒါကိုသိပြီးဆိုရင် client ကွန်ပျူတာအားလုံးတို့ရဲ့ gateway နေရာမှာ ICS server ရဲ့ IP address ကို ထည့်သွင်းပေးလိုက်ရုံဖြစ်ပါတယ်။

ICS server မှတဆင့်အင်တာနက်ဆက်ကြောင်းကိုမျှဝေသုံးစွဲမည့် client ကွန်ပျူတာ (ဥပမာပုံအရ A, B, C) တို့၏ TCP/IP properties တွင်အောက်ပါအချက်အလက်များကို သတ်မှတ်ထည့်သွင်းပေးရပါမယ်။

Computer IP address

ICS server ၏ NIC ၂ခုထဲမှအတွင်း NIC (internal) နှင့် network ID တူရမယ်။ host ID မတူတဲ့ IP address ကိုသုံးရပါမယ်။ ICS server ၏ IP address သည် 192.168.0.1 ဖြစ်ပါတယ်။ ဤတွင်မှ client ကွန်ပျူတာတို့တွင် 192.168.0.2 မှ 192.168.0.255 အတွင်းကြိုက်ရာပေးလို့ရပါတယ်။ တစ်လုံးနှင့်တစ်လုံး host ID မတူအောင်တော့ သတိထားပါ။

ဥပမာကွန်ပျူတာ	A	-	192.168.0.2
	B	-	192.168.0.3
	C	-	192.168.0.4

Subnet mask

Ip address သည် class C ဖြစ်သည့်အတွက် ကွန်ပျူတာတိုင်း၏ subnet mask သည် 255.255.255.0 အားလုံးအတူတူပင်ဖြစ်ကြရပါမယ်။

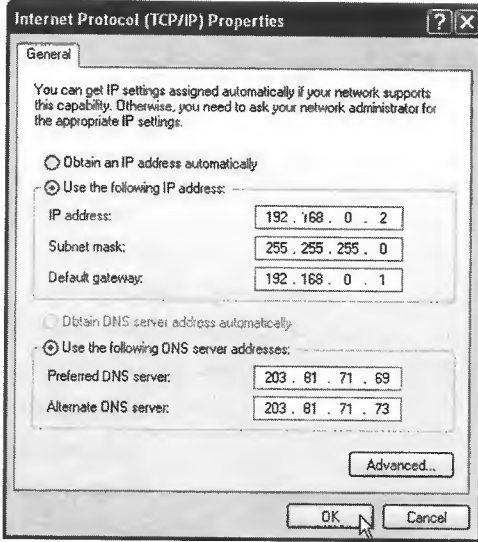
Default Gateway

default gateway နေရာတွင် ICS server ၏အတွင်းဘက် NIC (internal) ၏ IP address ဖြစ်တဲ့ 192.168.0.1 ကိုထည့်ပေးရပါမယ်။

DNS server

ISP မှပေးထားသော DNS server ၏ IP address များကို ထည့်ပေးရပါမယ်။ ဒါဆိုရင် client ကွန်ပျူတာတစ်လုံးအတွက်လိုအပ်တဲ့ IP configuration တွေထည့်သွင်းပြီးပြီလို့ဆိုနိုင်ပါပြီ။ တဖက်ဖော်ပြပါ ပုံကတော့ ကွန်ပျူတာ A အတွက် ထည့်သွင်းထားသည့် IP configuration ပဲဖြစ်ပါတယ်။

ပုံ (15.23)



ဤနည်းဖြင့် လိုအပ်သော setting တွေထည့်သွင်းပြီး၍ ICS server နှင့် အဆက်အသွယ် ရပြီဆိုလျှင် အင်တာနက်ဆက်ကြောင်းသည် network တွင်းရှိ ကွန်ပျူတာ (ဥပမာပုံအရ - ကွန်ပျူတာ A၊ B၊ C) တို့ထံသို့ရောက်ရှိလာပြီဖြစ်ပါတယ်။ ဤတွင်မှအင်တာနက်၊ အီးမေး(လ်) တို့အတွက် proxy server၊ mail server setting များထည့်သွင်း၍ အင်တာနက်ကြည့်ခြင်း၊ အီးမေး(လ်) ပို့ခြင်းများကိုလုပ်ဆောင်နိုင်ကြပါပြီ။

မှတ်ချက်။ ။ satellite link (IPstar) ပဲသုံးသုံး၊ broadband wireless ပဲသုံးသုံး ချိတ်ဆက်တပ်ဆင်အသုံးပြုပုံများသည် ADSL အသုံးပြုသကဲ့သို့ပင်ဖြစ်ပါသည်။ ဆိုရရင် satellite link ကိုသုံးမည်ဆိုပါက ADSL modem နေရာမှာ satellite modem (network box)၊ broadband wireless ကိုသုံးမည်ဆိုပါက indoor unit ဆိုတာသာကွာခြားပါမည်။ မည်သည့် device ကိုသုံးသုံး ကွန်ပျူတာတွင် IP configuration ထည့်သွင်းပုံ သဘောတရားများသည် အားလုံးအတူတူပင်ဖြစ်ကြပါတယ်။

Beginner's Guide to
Networking

ကွန်ပျူတာမှ ကွန်ယက်ဆီသို့
တည်ဆောက်အသုံးပြုခြင်းနှင့် အခြေခံသဘောတရားများ

မျိုးသူရ

