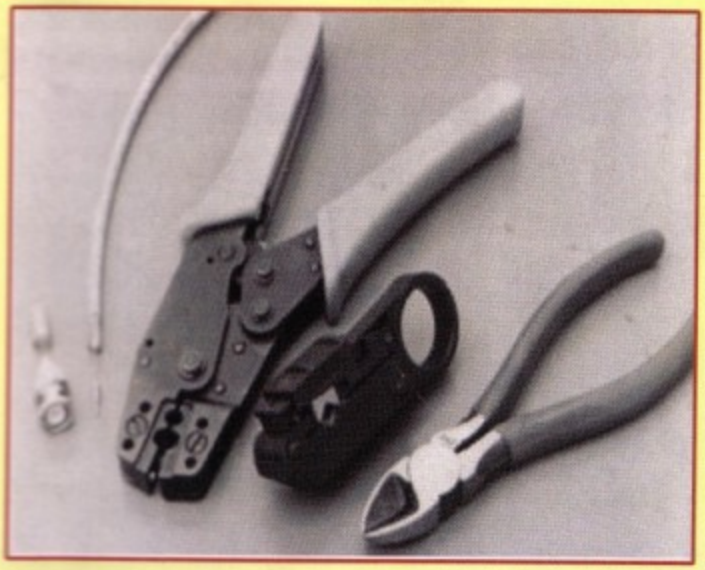
PRODUCT OF YOUTH

Road to MCSE

NETWORKING ESSENTIALS



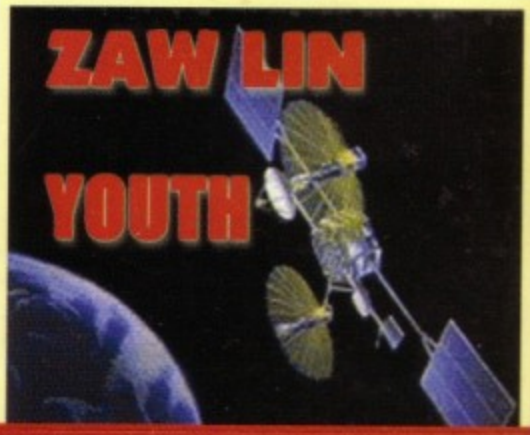
COMPUTER NETWORK STUDY GUIDE

ကွန်ပျူတာကွန်ရက်အကြောင်း
ထေထာရှုထမ်းညွှန်

Level : Basic, Intermediate

Network

- Infrastructure
- Planning
- Implementing
- Maintaining
- Cable Media
- Interface Card
- OSI Model
- Protocols
- TCP/IP
- Architecture
- Installation
- Enterprise
- WAN Concept
- Wireless LAN



ဘုရား

တရား

သံဃာ

တို့အား ဦးထိပ်မှနှဆင် ရှိခိုးကန်တော့ပါ၏။

❖ (ပေပေ)၊ (မေမေ)

❖ တယ်တယ်၊ မာမား

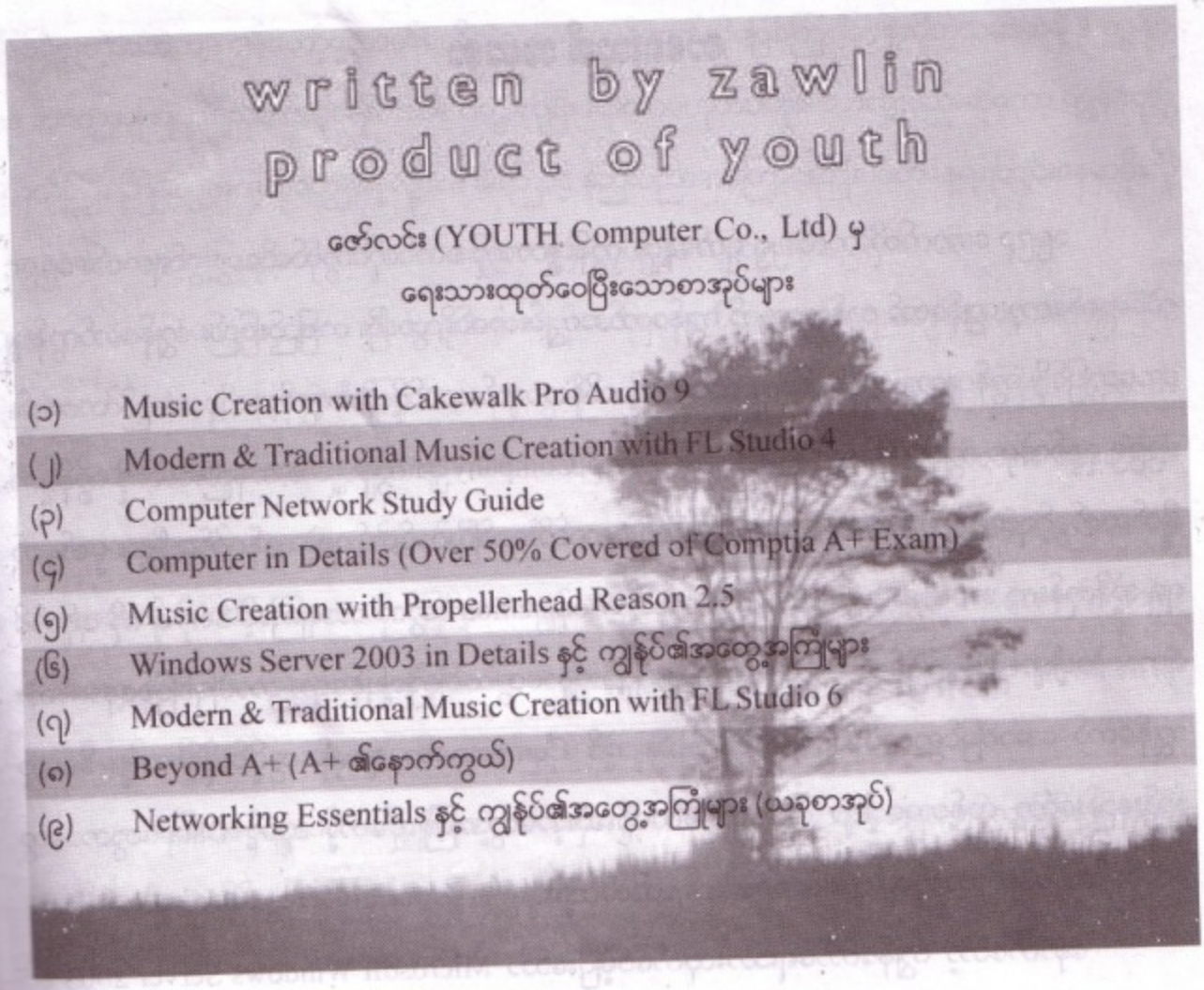
❖ ဆရာ ဦးသောင်းတင် နှင့် ဆရာမ ဒေါ်တင်တင်အေး

❖ ဆရာ ကိုညီညီထွေး

❖ ကိုကြီး နှင့် ကိုမိုး

❖ (ကိုပြုံး)

တို့အား ဤစာအုပ်ဖြင့် ကန်တော့ပါ၏။



ဇော်လင်း (YOUTH Computer Co., Ltd) မှ
ရေးသားထုတ်ဝေပြီးသောစာအုပ်များ

(၁) Music Creation with Cakewalk Pro Audio 9
(၂) Modern & Traditional Music Creation with FL Studio 4
(၃) Computer Network Study Guide
(၄) Computer in Details (Over 50% Covered of Comptia A+ Exam)
(၅) Music Creation with Propellerhead Reason 2.5
(၆) Windows Server 2003 in Details နှင့် ကျွန်ုပ်၏အတွေ့အကြုံများ
(၇) Modern & Traditional Music Creation with FL Studio 6
(၈) Beyond A+ (A+ ၏နောက်ကွယ်)
(၉) Networking Essentials နှင့် ကျွန်ုပ်၏အတွေ့အကြုံများ (ယခုစာအုပ်)

YOUTH Computer Co., Ltd မှဖန်တီးထုတ်ဝေသော စီဒီများ

(၁) ကွန်ပျူတာဖြင့် မြန်မာ့ဂီတသံများဖန်တီးရန် One Shot အဖြစ်အသင့်ပြုလုပ်ထားသော
မြန်မာ့တူရိယာသံများပါဝင်သောစီဒီ

(၂) ကွန်ပျူတာစက်ပိုင်းနှင့်စနစ်များအကြောင်းလေ့လာခြင်း
Computer Hardware & System Study Guide Interactive CD-Rom (Hello Computer)

(၃) ကွန်ပျူတာဖြင့်ရိုက်နှိပ်ထားသော နိုင်ငံတကာအဆင့်မှီ Music Sheet များပါဝင်သည့်
Rock Guitar တီးနည်း ဗီဒီဒီ (ညီညီထွေး Rock Guitar Study Guide)

၁၉၉၃ အောက်တိုဘာလ ၂၅ ရက်နေ့မှာ ကွန်ပျူတာကို စတင်ကိုင်တွယ်ထိတွေ့ခွင့်ရတယ်။ ၁၉၉၄ ထဲရောက်တော့ ကျွန်တော် ကွန်ပျူတာကို ကျွန်တော်အကျွမ်းတဝင်ရှိသွားပြီ။ တဖြည်းဖြည်း ကျွန်တော်ကွန်ပျူတာတွေပြင်ဖို့၊ ကွန်ပျူတာ ကွန်ရက်တွေ တပ်ဆင်ဖို့၊ ထိန်းကျောင်းတတ်ဖို့ကိုပါ ကျွန်တော်နားလည်လာတယ်။ ၁၉၉၅ ခုနှစ်ထဲမှာ ကျွန်တော့် သူငယ်ချင်းအဖေရဲ့ အသိ Company မှာ ကွန်ပျူတာ အနည်းငယ်ကို ကွန်ရက်ချိတ်ဆက်ခွင့်ရတယ်။ ကျွန်တော်ရဲ့ ပထမဦးဆုံး ဦးဆောင်ဦးရွက်ပြီးတပ်ဆင်ရတဲ့ ကွန်ရက်ပေါ့ဗျာ။ မှတ်မှတ်ရရ အဲ့ဒီတုန်းက အခက်အခဲများစွာကို ကြုံရတယ်။ Workstation တွေက ဘာကြောင့် Server ကို မချိတ်မိရတာလဲပေါ့ဗျာ။ ချိတ်မိပြန်တော့လည်း တစ်ခြား ပြဿနာတွေထပ်ကြုံရပြန်ရော။ ဘာပဲဖြစ်ဖြစ်နောက်ဆုံး ကျွန်တော် အောင်မြင်စွာတပ်ဆင်ပေးနိုင်ခဲ့တယ်။ အဲ့ဒီ Company က ဂျာမန်တွေပိုင်ဆိုင်တာဗျ။ ဒီတော့ နည်းနည်းတော့ လန့်တာပေါ့ဗျာ ကိုယ်က ပထမဦးဆုံးအတွေ့အကြုံဆိုတော့ သူတို့ Data တွေဘာတွေ မထိခိုက်အောင်တို့ဘာတို့ပေါ့ဗျာ။ အစစအရာရာတိတိကျကျပေါ့။

နောက်တော့ ကျွန်တော်ရေးသားထုတ်ဝေခဲ့ပြီးသော Microsoft Windows Server 2003 နှင့် ကျွန်ုပ်၏အတွေ့အကြုံများ စာအုပ်မှာ စာရေးသူအမှာစာမှာဖော်ပြပြီးအတိုင်းပေါ့ ၁၉၉၆ ဩဂုတ်လမှာ ကျွန်တော့် အစ်ကိုတွေရှိရာ ဘန်ကောက်မြို့ကိုသွားလည်ရင်းနဲ့ Novell ရဲ့ Certified Novell Administrator စာမေးပွဲကိုဝင်ရောက်ဖြေဆိုအောင်မြင်ခဲ့ပါတယ်။

ထားပါတော့လေ။ အဲ့ဒီကနေ ဒီနေ့အထိပေါ့။ တွေ့ကြုံခဲ့ရတဲ့အပိုင်းလေးတွေလည်း ရေးပြချင်တယ်။ နောက်ပြီးတော့ Networking Essentials ဆိုပြီး သီးသန့် စာအုပ်တစ်အုပ်လည်းပြုစုချင်တာကြောင့် ဒီစာအုပ်ကို ရေးသားထုတ်ဝေလိုက်ရခြင်းဖြစ်ပါတယ်။ အကြောင်းအရာတွေကတော့ ခက်လည်းမခက်အောင်၊ လိုသွားတာမျိုးလည်းမဖြစ်အောင် သေချာ အခန်းတွေခွဲထုတ်ပြီးပြုစုတာဖြစ်ပါတယ်။ အောက်ခြေကစတဲ့သူလည်း ဖတ်လို့ရအောင်၊ သိထားပြီးတဲ့သူတွေလည်း မှီငြမ်းလို့ရအောင်ပေါ့ဗျာ။

ဒါနဲ့ ပြောရဦးမယ်။ ကျွန်ုပ်၏အတွေ့အကြုံများဆိုတာ ကျွန်တော်ကြုံဖူးခဲ့သမျှထဲက အချို့ပေါ့ဗျာ။ တစ်ချို့ကျတော့လည်း မဆီလျော်တော့ ရေးတဲ့အထဲမပါဘူးပေါ့။ နောက်တစ်ခုက ကျွန်တော်က ကျွန်တော်

ခြစ်ခဲ့ဖူးတဲ့အထဲက ကျွန်တော့်လောက်မသိတဲ့သူတွေ ကျွန်တော်လိုမဖြစ်ကြပါစေနဲ့ဆိုတဲ့သဘောနဲ့ ဒီ ကျွန်ုပ်၏ အတွေ့အကြုံများ ဆိုတာကိုရေးတာပါ။ ဒါကို ဆိုပြီးရေးတာမဟုတ်ပါဘူး။ ဘာလို့လည်းဆိုတော့ ကျွန်တော့် ထက်ပိုပြီး ကြုံတွေ့ဖူးတဲ့သူတွေရှိနေလို့ပါပဲ။ အဲကြောင့် နည်းပညာအကြောင်းကြီးပဲဖတ်နေရရင်ပျင်းနေမှာစိုးလို့ ကျွန်ုပ်၏အတွေ့အကြုံများကို ပြင်ပလက်တွေ့ဘဝနှင့် ညှပ်ပြီးတင်ပြသွားတာဖြစ်ပါတယ်။

Level ကတော့ Intermediate ပေါ့။ ကျွန်တော့်မှာ တစ်ခြားရေးပြစရာတွေရှိနေသေးတာကြောင့် ကျွန်တော် Advance ဖြစ်တဲ့အကြောင်းအရာတွေကို မရေးဖြစ်သေးတာပေါ့။ Advance ကြတော့ ဒီထက် အချိန်ပိုလည်းပေးရမယ်လေ။ နောက်ပြီး Demand ကလည်း အရေးကြီးတယ်မဟုတ်လား။ နောက်ပိုင်း တော့ လူလည်းကျန်းမာရေးကောင်းမယ် (ရောဂါကတော့ထူးဆန်းတယ်ဗျ၊ အိတ်ကပ်ထဲပိုက်ဆံနည်းလာရင် ဖင်ကနာသလိုလို၊ ခေါင်းကနာသလိုလိုဖြစ်တာ၊ ကျွန်တော့်မဟေသီကပြောတာ ၉၆ ပါး မကလောက်ဘူးတဲ့)။ အဲ ဒီတော့ အင်အားလည်းစိုက်ထုတ်နိုင်မယ်။ အချိန်လည်းပိုပေးနိုင်မယ်ဆိုတဲ့အခါမျိုးကြမှ Advance ကို ရေးဖြစ်မယ်ထင်ပါတယ်။ အခုတော့ ဒီလောက်နှင့်ပဲ ကျေနပ်ကြပါဦးနော်။

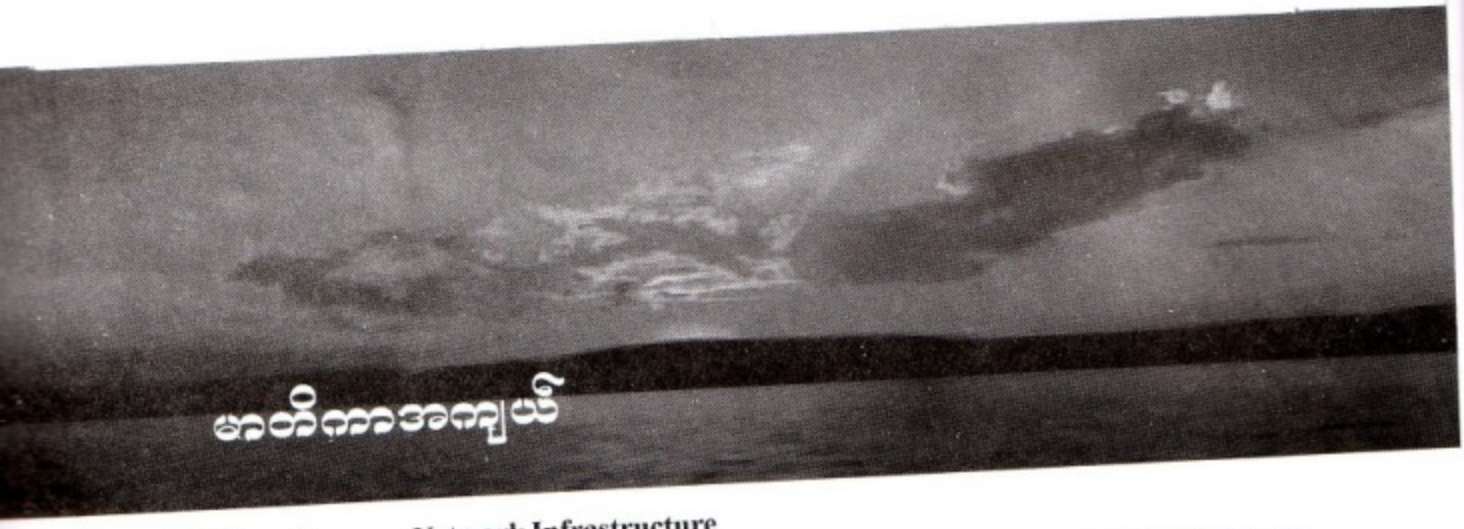
စာအုပ်စာပေများကို ဖတ်ရှုကြတဲ့အလေ့အကျင့်ကောင်းများ လူငယ်တွေမှာ ရရှိလာခြင်းဖြင့် နှစ်ဦးနှစ်ဖက်အကျိုးများနိုင် ပွားနိုင်ကြပါစေလို့ ဆုမွန်ကောင်းတောင်းပါတယ်။

စေတနာများစွာဖြင့်

ဇော်လင်း

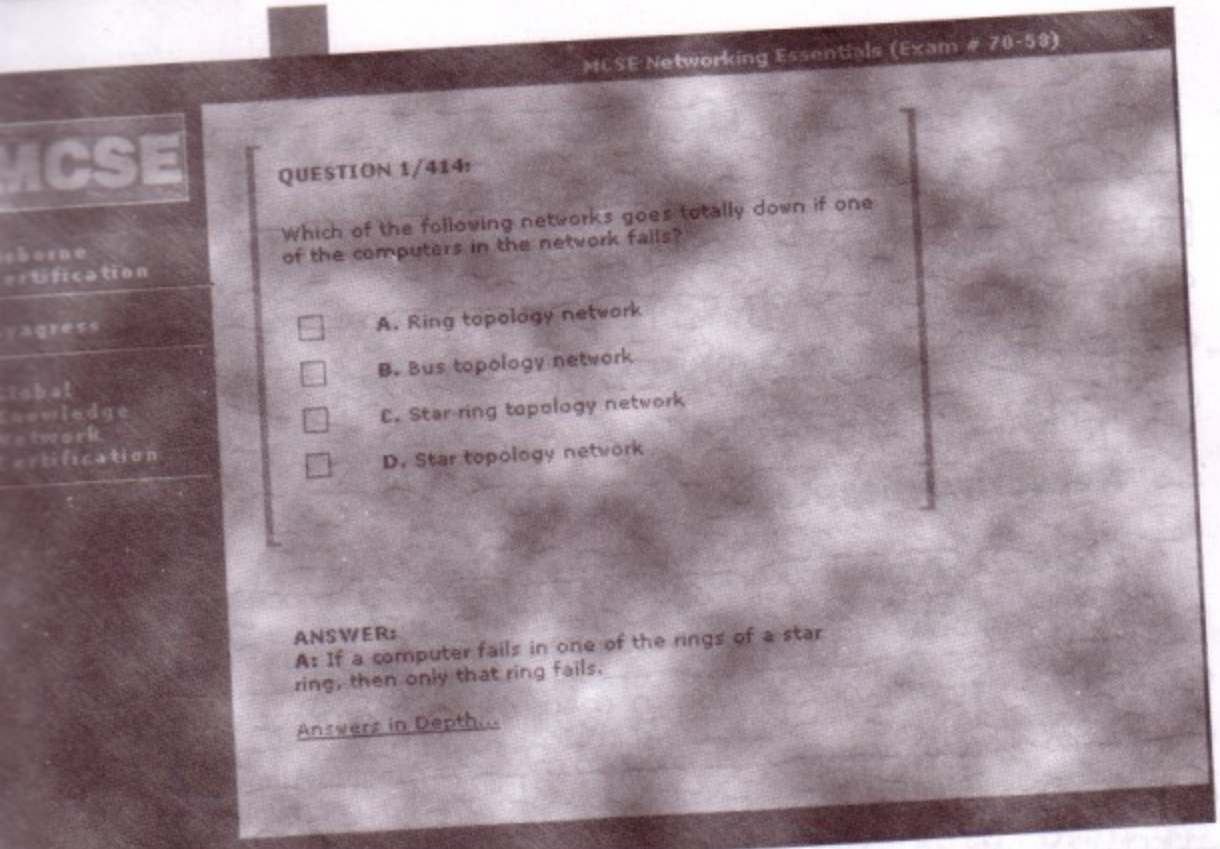
Technical Writer

YOUTH Computer Co., Ltd



အခန်းကဏ္ဍ ၁

CHAPTER 1 Network Infrastructure



UNIT 1

Network Infrastructure

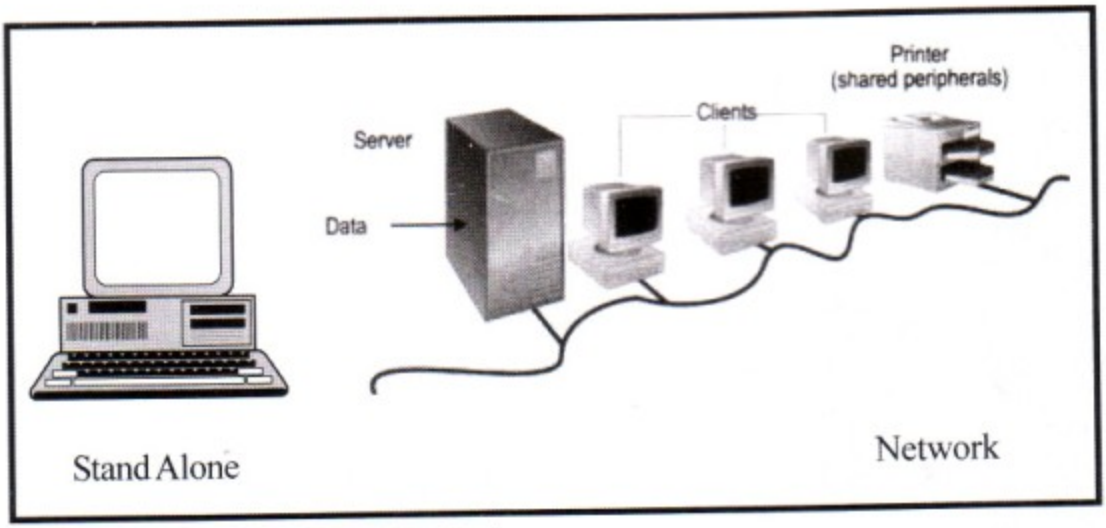
ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက်နှင့် ပတ်သက်နေသော အခြေခံအကြောင်းအရာတွေကိုလေ့လာကြမှာ ဖြစ်ပါတယ်။ ကွန်ပျူတာကွန်ရက်ရဲ့ အကျိုးကျေးဇူးတွေကိုပါ လေ့လာရမှာဖြစ်ပါတယ်။

ကျွန်တော်တို့ Networking Essentials ဆိုတဲ့ဒီစာအုပ်မှာ ပထမဦးဆုံးသင်ခန်းစာအနေနဲ့ Network (ကွန်ရက်)ဆိုတာဘာလဲ။ နောက်ပြီး ကွန်ပျူတာတွေကိုဘာကြောင့် ကွန်ရက်ချိတ်ဆက်ပြီးအသုံးပြုရသလဲ၊ ဒီလိုပြုလုပ်ခြင်းဖြင့် ဘယ်လိုအကျိုးကျေးဇူးတွေရသလဲ။ စတာတွေကို ကနဦးသင်ခန်းစာအနေနဲ့ တင်ပြပေးသွားမှာဖြစ်ပါတယ်။ အဲ့ဒီအပြင် ကွန်ရက်တစ်ခု၏ အခြေခံသဘောတရားများကိုလည်း ထည့်သွင်းဖော်ပြသွားမှာဖြစ်ပါတယ်။ ပထမဦးဆုံး ကွန်ပျူတာကွန်ရက်ဆိုတာ ဘာလဲဆိုတဲ့ အကြောင်းကိုပြောပြပါ့မယ်။ ကျွန်တော်တို့ သုည်ကနေဘဲ စကြတာပေါ့ဗျာ။

၁.၁ Network Concept ကွန်ရက်အဆိုအစ

ဒီနေ့ခေတ်မှာ စီးပွားရေးလုပ်ငန်းတွေမှ မဟုတ်၊ ပညာသင်ကြားရေး ကျောင်းနှင့်အိမ်တွေ၊ ဖျော်ဖြေရေးလုပ်ငန်းတွေမှာပါ နယ်ပယ် ကဏ္ဍအနေရာတော်တော်များများ ကွန်ပျူတာတွေသုံးနေတာ အားလုံးအသိပဲဖြစ်ပါတယ်။ အဲဒီလိုကွန်ပျူတာတွေကိုသုံးတဲ့နေရာမှာ ကွန်ပျူတာတစ်လုံးနှင့်တစ်လုံး ဆက်သွယ်ချိတ်ဆက်ထားခြင်းမရှိတဲ့ တစ်လုံးစီသီးခြားရပ်တည်ပြီးအသုံးပြုတဲ့ ကွန်ပျူတာကို Stand Alone Computer လို့ခေါ်ပါတယ်။ ဒီပေမယ့် လိုအပ်ချက်အရ ကွန်ပျူတာအသုံးပြုသူတွေဟာ ကွန်ပျူတာတွေကို အချင်းချင်းချိတ်ဆက်ပြီး အသုံးပြုလာတဲ့အခါမှာတော့ ကွန်ပျူတာ ကွန်ရက်ဆိုတာဖြစ်ပေါ်လာပါတယ်။ ဒီတော့ ကွန်ပျူတာကွန်ရက်ဆိုတာ ကွန်ပျူတာတွေကိုကြားခံပစ္စည်းတစ်ခုခုနဲ့ချိတ်ဆက်ပြီးအသုံးပြုခြင်းပဲဖြစ်ပါတယ်။ တကယ်တော့လည်း ကွန်ပျူတာနှင့်ပတ်သက်လို့ အနည်းငယ်ဗဟုသုတရှိသူတောင် ဒါကိုသိပြီးဖြစ်မှာပါ။ ဒီပေမယ့်လည်း ကျွန်တော့် အနေနဲ့အခြေခံကျကျ ရှင်းပြချင်တာက Stand Alone နှင့် Network ဆိုသည်တွင် လူတော်တော် များများသည် Stand Alone ကို စတန်းလုံး၊ စတန်းလုံး ဟူ၍အလွယ်တကူသမုတ်နေကြသဖြင့် ပြောပြလိုသည်မှာ ကွန်ပျူတာများကို တစ်လုံးနှင့်တစ်လုံး အပြန်အလှန်ဆက်သွယ်လို့ရအောင် ကြားခံပစ္စည်းတစ်မျိုးမျိုးကို အသုံးပြုပြီး ပင်ကူအိမ်သဖွယ်ချိတ်ဆက်ထားခြင်းကို ကွန်ပျူတာကွန်ရက် (Network) ဟုခေါ်ပြီး၊ အဲ့သလိုမှ မဟုတ်ဘဲ တစ်လုံးတည်းသီးခြားရပ်တည်ပြီး အသုံးပြုသည့်ကွန်ပျူတာကို Stand Alone ဟုခေါ်သည်။

ပုံ ၁.၁



၁.၂ Networking Advantages ဘာကြောင့်ကွန်ရက်ချိတ်ဆက်အသုံးပြုရသလဲ

ကွန်ပျူတာကို ဒီအတိုင်းသုံးရင်ရရဲ့သားနဲ့ ဘာကြောင့်များ ကွန်ရက်တွေချိတ်ဆက်ပြီးအသုံးပြုရသလဲ ဆိုတာကိုရှင်းပြခြင်းဟာ တစ်နည်းအားဖြင့် ကွန်ပျူတာတွေကို ကွန်ယက်ဆက်ပြီးအသုံးပြုခြင်းကြောင့် ရရှိလာတဲ့ အကျိုးကျေးဇူး (Benefits) တွေကိုဖော်ပြလိုက်သလိုပဲဖြစ်ပါတယ်။ ကဲအနည်းဆုံး ကွန်ပျူတာနှစ်လုံးကိုကြိုးနှင့်ချိတ်ပြီး တစ်လုံးနှင့်တစ်လုံး အပြန်အလှန်ဆက်သွယ်လို့ရသွားပြီဆိုရင်ပဲ ကွန်ပျူတာကွန်ရက်တစ်ခု ဖြစ်နေပါပြီ။ ဒီလိုချိတ်ဆက်ပြီးတော့ တစ်လုံးနှင့်တစ်လုံးအချက်အလက်တွေ ဖလှယ်လို့ရလာတာဟာ ကွန်ပျူတာကွန်ရက်တပ်ဆင်ရခြင်းရဲ့ ပထမဆုံးအကြောင်းအရင်းနှင့် အကျိုးကျေးဇူးပဲပေါ့။ ဒါကို အင်္ဂလိပ်လို Sharing လို့ခေါ်တာပ။ ဟုတ်ပါတယ်။ ကျွန်တော်တို့တွေဟာ ပြဿနာတစ်ခုကို ဝိုင်းဝန်းစုပေါင်းပြီး အဖြေရှာသလိုပါပဲ။ လုပ်ငန်းကြီးတစ်ခုကို လူတွေအများကြီးနှင့် တနည်းအားဖြင့် ကွန်ပျူတာတွေအများကြီးနှင့် တာဝန်တွေခွဲဝေပြီး အလုပ်လုပ်ဆောင်ကြတဲ့အခါမှာ တစ်ဦးနှင့်တစ်ဦး၊ တစ်လုံးနှင့်တစ်လုံး သတင်းအချက်အလက်တွေအပြန်အလှန် (Share) ဖလှယ်နိုင်ဖို့ ကွန်ပျူတာတွေကို ကွန်ရက်ချိတ်ပြီး အသုံးပြုကြရပါတော့တယ်။ ဒီတော့အခုပြောပြသလောက်ဝဆိုရင် ကွန်ပျူတာကွန်ရက်ကိုတပ်ဆင်ရတဲ့ အချက်တွေထဲက ကနဦး အရေးကြီးတဲ့အချက်က Sharing ဆိုတဲ့အချက်ပဲဖြစ်ပါတယ်။ ဒီ Sharing ဆိုတဲ့အကြောင်းကို ထပ်မံ၍အကျယ် ပြောပြကြကြေးဆိုရင် ဘာတွေကို Share လုပ်မှာလဲ။

၁။ Data ဆိုတဲ့အချက်အလက်တွေ

၂။ အသုံးချမည့် Software တွေနှင့်

၃။ အသုံးပြုမည့် Hardware တွေစသည်တို့ဖြစ်ကြပါတယ်။

နောက်တစ်ခုပြောပြချင်တာက အဲဒီလို Sharing လုပ်ရာမှာ တစ်ဦးနှင့်တစ်ဦး (တစ်လုံးနှင့်တစ်လုံး)အပြန်အလှန် Sharing လုပ်နိုင်ခြင်းနှင့် ၎င်းနည်းအပြင် ဗဟိုထိန်းချုပ်မှုတစ်ခုခုမှ သတင်းအချက်အလက် (Information and Data) ဖြစ်စေ၊ Software ဖြစ်စေ၊ ပံ့ပိုးပေးထားခြင်းစသည့် နှစ်နည်းဖြင့် Sharing လုပ်နိုင်ပါသည်။ Data ကို Sharing လုပ်ခြင်းဆိုသည်မှာ ဥပမာ ဆိုပါစို့။ ဝိုင်တစ်ခုကို Printer ထုတ်ချင်လို့အဲ့ဒီလူဟာသူထုတ်ချင်တဲ့ File ကို Disk ထဲမှာထည့်ပြီး Printer ချိတ်ထားတဲ့ Computer ဆီကိုသွား နောက်တော့ Copy ကူး ဒီမှမဟုတ်လည်းသက်ဆိုင်ရာ Program ကိုဖွင့်ပြီး Print ထုတ် ဒီလိုမျိုးလုပ်ရမှာဖြစ်ပါတယ်။ ဒီလိုတစ်နေရာမှတစ်နေရာ Data တွေကို Disk နှင့် Copy ကူးပြီးဟိုသယ်ဒီသယ်၊ ဟိုစက်ထဲထည့် ဒီစက်ထဲထည့်ဒီလိုမျိုး လုပ်ရတာကို Sneakernet လို့ခေါ်ပါတယ်။ အကယ်၍သာ ကွန်ပျူတာကွန်ရက်ချိတ်ထားခဲ့မယ်ဆိုရင်တော့ ဒီမျိုးလုပ်စရာမလိုဘဲ ကျွန်တော်တို့ ၎င်မကြွဘဲ ဝိုင်များအပြန်ပြန်အလှန်လှန်ဖလှယ်နိုင်ခြင်း၊ Print ထုတ်နိုင်ခြင်းတို့ လုပ်နိုင်မှာဖြစ်ပါတယ်။ ဒီဟာတကယ်တော့အသေးဆုံး ဥပမာတစ်ခုဖြစ်ပါတယ်။

၁၉၉၉ ခုနှစ်လောက်တုန်းကစက်ရုံတစ်ခုတွင်ဆင်ခဲ့သော Network တွင် - သူတို့သည်နေ့စဉ် ကုန်ရောင်းစာရင်းကို လူများခွဲ၍ရိုက်ထည့်ကြသည်။ တစ်ယောက်ချင်းစီက ရိုက်သည့်အကြောင်းအရာများသည် ဖိုင် တစ်ဖိုင်ချင်းစီသီးခြားခွဲပြီး သိမ်းတာမဟုတ်ဘဲ တစ်ဖိုင်ထဲမှာပင်စုပြုံသိမ်းခြင်းဖြစ်သည်။ ဆိုလိုသည်မှာ ကုန်ရောင်းစာရင်းများကိုရိုက်ထည့်နေချိန်တွင် တစ်ဦးမကသောရိုက်ထည့်သူများသည် ၎င်းဖိုင်တစ်ခုကိုပဲ အသုံးပြုနေကြသည်။ တစ်နည်းအားဖြင့်ဆိုသော် ၎င်းဖိုင်ကို (Sharing) မျှဝေသုံးစွဲနေကြခြင်းပင်ဖြစ်သည်။

ထို့အတူ ၂၀၀၀ ခုနှစ်တုန်းက ကျွန်တော်ကွန်ရက်ချိတ်ဆက်ပေးခဲ့သော Airline တစ်ခုတွင် Tour ကုမ္ပဏီတစ်ခုက လေယာဉ်လက်မှတ် Booking လုပ်သမျှကိုကွန်ပျူတာဖြင့် လက်ခံနေသူများသည် တစ်ဦးမက ရှိသည်။ ၎င်းတို့သည် တစ်ဦးချင်း တစ်နေရာစီထိုင်၍ ၎င်း Booking များကို ကွန်ပျူတာဖြင့်လက်ခံရာ၌ ဖိုင်များကိုသီးခြားစီခွဲပြီး သိမ်းတာမဟုတ်ဘဲ တစ်ဖိုင်ကိုအားလုံးတစ်ပြိုင်တည်း အသုံးပြုနေခြင်းဖြစ်သည်။ ဒီလိုတစ်ဖိုင်တည်းကိုပဲ စုပြုံပြီးစာရင်းသွင်းမှလည်း အချက်အလက်များသည် Update ဖြစ်မည်ဖြစ်သည်။ သို့သော် ၎င်းဖိုင်တစ်ဖိုင်ထဲကို လူအများကတစ်ပြိုင်တည်း အသုံးပြုခွင့်မရရင်လဲ Data ရိုက်ထည့်ချိန် ကြာမြင့်မည် ဖြစ်သည်။ အချုပ်ဆိုရသော် ၎င်းဖိုင်တစ်ဖိုင်ထဲကို မျှဝေသုံးစွဲနေခြင်းသည်ပင် Data Sharing ဖြစ်ပေတော့သည်။ ဒီ Data Sharing ကြောင့် ကျွန်တော်တို့သည် လုပ်ငန်းများကိုအတူတကွ တစ်ပြိုင်တည်းလုပ်ဆောင်နိုင်ခြင်း၊ ထိုင်ရာမှ မထဘဲ အခြား ကွန်ပျူတာမှ အချက်အလက်များကိုခေါ်ယူကြည့်နိုင်ခြင်းစသည့် စသည့် ကောင်းကျိုး များကိုရရှိစေသည်။

နောက်တစ်ခုပြောပြချင်တာကတော့ Software ဆိုတဲ့အသုံးချ Program တွေကို Sharing လုပ်ခြင်း ပင်ဖြစ်သည်။ ကျွန်တော်တို့ Software ဆိုတာရှိသလို Network Awares ဆိုတာလည်းရှိပါတယ်။ Network မှာတင်သုံးနိုင်တဲ့ Software တွေကိုပြောတာဖြစ်ပါတယ်။ ထပ်ရှင်းပြပါအုံးမယ်။ ဥပမာ ကွန်ရက်ရဲ့ ဗဟိုကနေထိန်းချုပ်ပေးတဲ့ Server ဆိုတဲ့ကွန်ပျူတာကြီးမှာ ပီပီတို့လုပ်ငန်းမှာအသုံးပြုမဲ့ Software ကို Install လုပ်ထားပြီး ကျန်မည်သည့် Work Station များတွင်၎င်း Software ကို Install လုပ်ထားခြင်းမရှိပေ။ ဆိုလိုသည်မှာ အသုံးပြုသူများ၏ ကွန်ပျူတာများတွင် ၎င်းတို့အသုံးပြုမည့် Software သည် Locally တည်ရှိ မနေဘဲ Server ကနေခေါ်ယူအသုံးပြုရခြင်းဖြစ်သည်။ ဒီတော့၎င်း Software ကိုတစ်ချိန်တည်းတစ်ပြိုင်တည်းမှာ လူအများသုံးနိုင်အောင် Sharing လုပ်ပေးထားရသည်။ ၎င်းကို Program Sharing ဟုခေါ်သည်။ ထပ်မံရှင်းပြပါ အုံးမယ်။ ၎င်း Network Software များသည် Server မှာတစ်စုံတင်ထားရုံဖြင့် လူအများတစ်ပြိုင်တည်း အသုံးပြုနိုင်သည်။ ဒီနေရာမှာ အရေးကြီးသိရမယ့်အချက်တစ်ခုရှိပါသည်။ ၎င်းမှာ Software များကို လိုင်စင်ဖြင့် ဝယ်ယူရာ၌ လူတစ်ဦး၏ပိုင်ဆိုင်မှုဖြင့်မတွက်ပဲ ကွန်ပျူတာအလုံးရေဖြင့် တွက်သည်ဆိုခြင်းပင်ဖြစ်သည်။ ဥပမာ ဦးလှတွင် ကွန်ပျူတာ ၁၀ လုံးရှိသည်။ ဦးလှသည် ၎င်းပိုင်ကွန်ပျူတာ ၁၀လုံးတွင် အသုံးပြုရန် Software တစ်ခုကို တစ်စုံသာဝယ်ပြီး စက် ၁၀လုံး စလုံးတွင်အသုံးပြုခွင့်မရှိပေ။ ၁ လုံးသာအသုံးပြုခွင့်ရှိသည်။ ၎င်း

Software သည် ခေါ်လာ ၂၀၀ တန်ပါက ယေဘုယျအားဖြင့် စက် ၁၀ လုံးစာအတွက် ၁၀ စုံ ခေါ်လာ ၂၀၀၀ ကျော်ကျမည်ဖြစ်သည်။ ထို့ကြောင့် Software ၁၀ စုံမဝယ်ဘဲ ၎င်း Software Network Version ကိုတစ်စုံသာဝယ်ပြီး Server မှာထိုင်ကာ တစ်ပြိုင်တည်း ၁၀ ယောက်အသုံးပြုခြင်းဖြင့် ဦးလှကို ကုန်ကျစရိတ် သက်သာစေသည်။ သို့သော် Network Version တွင်လည်း ၅ ယောက်အသုံးပြုမည် (5 User License) ဆယ်ယောက်သုံးမည် (10 User License)-(25 User License) စသည်ဖြင့် တစ်ပြိုင်တည်း ဘယ်နှစ်ယောက် သုံးမည်ဆေးမှုတည်ပြီး လိုင်စင်ဝယ်ရသည်။ နောက်မှထပ်တိုးလည်းရသည်။ ယခုပြောသည့် ပုံစံအရဆိုလျှင် ဦးလှသည် 10 User License ဝယ်ရမည်ဖြစ်သည်။ ဘယ်လိုပဲဖြစ်ဖြစ် ထိန်းချုပ်မှုစနစ်အရရော ကုန်ကျစရိတ် အရရော သက်သာသေးသည်။

နှုတ်ချက် ။ ။ ကွန်ပျူတာ ၁၀ လုံးတွင် Program တစ်ခုကိုစက်တစ်လုံးချင်းစီတွင် Locally Install လုပ်ထားခြင်းမဟုတ်ဘဲ ဗဟိုထိန်းချုပ်မှုစနစ်တစ်ခုထဲမှာပဲ Install လုပ်ကာစက်၁၀လုံးတွင် တစ်ချိန်တည်း တစ်ပြိုင်တည်း မျှဝေသုံးစွဲနိုင်သည့် Software ကို Network Awares ဟုခေါ်ခြင်းဖြစ်သည်။ ၎င်းသည်ပင်လျှင် Program Sharing ဖြစ်ပေတော့သည်။ ၎င်း Network Awares များသည် ဝယ်ယူထားသည့်လိုင်စင် ဆေးမှုတည်၍ပဲ အသုံးပြုလို့ရသည်။ ဆိုလိုသည်မှာ 5 User License ဆိုသည်မှာ တစ်ပြိုင်တည်း၅ယောက် သာအသုံးပြုခွင့်ရှိပြီး ဒီထက်ပိုသုံးခွင့်မရှိပေ။

ကျန်ပိုင်၏အတွေးခြည်း

ကျွန်တော်သည် ၁၉၉၅ ခုနှစ်ဝန်းကျင်တုန်းက သူငယ်ချင်း၏အကူညီတောင်းမှုဖြင့် အသိုက်မှကိုတစ်ခု တွင် ကွန်ပျူတာအနည်းငယ်ကို ကွန်ရက်ဆင်ပေးခဲ့ဖူးသည်။ အဲ့ဒီအချိန်တုန်းက Windows 95 ပင်မပေါ် သေးပေ။ (ရန်ကုန်ကိုမရောက်သေးတာလည်း ဖြစ်ချင်ဖြစ်မှာပေါ့) ထိုအခါကျွန်တော်သည် Windows for Workgroup ဟုခေါ်သည့် Windows Version 3.11 ကို Server မှာထိုင်ကာအသုံးပြုမည့် Workstation များတွင် Hard Disk ပင်မရှိဘဲ ချိတ်ဆက်အသုံးပြုစေခဲ့သည်။ Workstation များသည် Network Card ၏ Boot ROM မှတဆင့် Boot လုပ်ကာ Server ကို Connection လုပ်ကြသည်။ အသုံးပြုသူသည် Server ထဲက Windows Version 3.11 ကိုလှမ်းခေါ်ကာသုံးနိုင်သည်။ ထို့ကြောင့် ၎င်း Workstation များ တွင် Program များသိုးခြားစိရှိနေဖို့ မလိုအပ်နှင့် Hard Disk ပင်မရှိပေ။ ဤသို့နှင့်ပင်ကျွန်တော်လည်း Network တွေဆင်ပေးခဲ့ရာ လုပ်ငန်းတော်တော်များများသည် လုပ်ငန်းအတွက်ရည်ရွယ်ရေးထားသော Tailor Made Software များကို Network Version များအဖြစ် Server တွင်ထိုင်ကာမျှဝေသုံးစွဲကြသည်သာ ဖြစ်သည်။

Sharing တွေထဲကနောက် Sharing တစ်ခုကတော့ Hardware ဆိုတဲ့ Device ပစ္စည်းတွေကို

ဘုံ သုံးလို့ရအောင် Sharing လုပ်ခြင်းပင်ဖြစ်ပါသည်။ ဥပမာ ကွန်ပျူတာ ၁၀ လုံးရှိသော်ငြားလည်း ကွန်ပျူတာတိုင်းတွင် Printer ချိတ်ထားစရာမလိုသကဲ့သို့ ချိတ်ထားသော Printer တစ်လုံးထဲကိုပဲအားလုံးက ဘုံအဖြစ်ဝိုင်းဝန်း သုံးစွဲနေကြခြင်းသည် Printer Sharing သို့မဟုတ် Device Sharing ပင်ဖြစ်သည်။ ဤသို့ Sharing လုပ်ခြင်းကြောင့် ကျွန်တော်တို့သည်ထိုင်ရာမှမထဘဲ Print ထုတ်နိုင်ခြင်းပင်ဖြစ်သည်။ ထို့အပြင် CD ROM တစ်လုံးထဲ ကို ဘုံသုံးခြင်း Modem တစ်ခုထဲကိုပဲ ဘုံသုံးခြင်းစသည်တို့သည်လည်း Device Sharing ပင်ဖြစ်သည်။

တကယ်တော့ ကွန်ပျူတာကွန်ရက်ဆင်တယ်ဆိုတာ အခုလို Sharing လုပ်ဖို့ပဲမဟုတ်ဘူးဗျ။ တခြားအကြောင်းအရာတွေလည်းရှိသေးတယ်။ အဲဒါကတော့ Security ပဲဗျ။ ကွန်ပျူတာကွန်ရက်ဆင်ထားခြင်းအားဖြင့်လုပ်ငန်းနှင့်မသက်ဆိုင်တဲ့ လူတွေဟာဒီကွန်ရက်ကိုအသုံးပြုခွင့်မရှိပါဘူး။ လွယ်လွယ်ပြောရရင်တော့ ဗရမ်းဗတာမဖြစ်ဘူးပေါ့။ လုံခြုံတယ်ပေါ့ဗျာ။ အဲဒီတော့အခုလို Sharing လုပ်နိုင်ခြင်းနှင့် Security ကောင်းခြင်းတို့ကြောင့် ကွန်ပျူတာကွန်ရက်ကို ယနေ့ခေတ်မှာတပ်ဆင်အသုံးပြုမှုများ များပြားလာခြင်းဖြစ်သည်။

၁.၃ Network Infrastructure ဆိုတာ

Network တစ်ခုဖြစ်ပေါ်လာဖို့ချိတ်ဆက်မှုတွေ၊ Connectivity ဒါမှမဟုတ် Network တစ်ခုရဲ့ လုံခြုံမှု Security တွေ၊ လမ်းကြောင်းချိတ်ဆက်မှု Routing တွေ၊ ထိန်းချုပ်အုပ်ချုပ်မှု Management တွေ၊ ရယူသုံးစွဲမှု Access တွေ တခြားဒီ Network မှာပါဝင်ပတ်သက်နေတဲ့ အစိတ်အပိုင်းတွေ ၎င်းအစိတ်အပိုင်းတွေဟာ Network တစ်ခုရဲ့ Infrastructure ပဲဖြစ်ပါတယ်။ ဟုတ်ပါတယ် Network တစ်ခုမှာ Physically အရပဲဖြစ်စေ၊ Logically အရပဲဖြစ်စေ ပါဝင်ပတ်သတ်နေတဲ့အစိတ်အပိုင်းတွေကို ၎င်း Network ရဲ့ Infrastructure တနည်းအားဖြင့် Network Infrastructure လို့ခေါ်ပါတယ်။

၁.၄ Types of Network ကွန်ရက်အမျိုးအစားများ

ကွန်ရက်အမျိုးအစား (၃) မျိုးကိုအကြမ်းအားဖြင့် တွေ့နိုင်ပါတယ်။ အဲဒါကတော့-

၁။ Local Area Network (LAN)

၂။ Metropolitan Area Network (MAN)

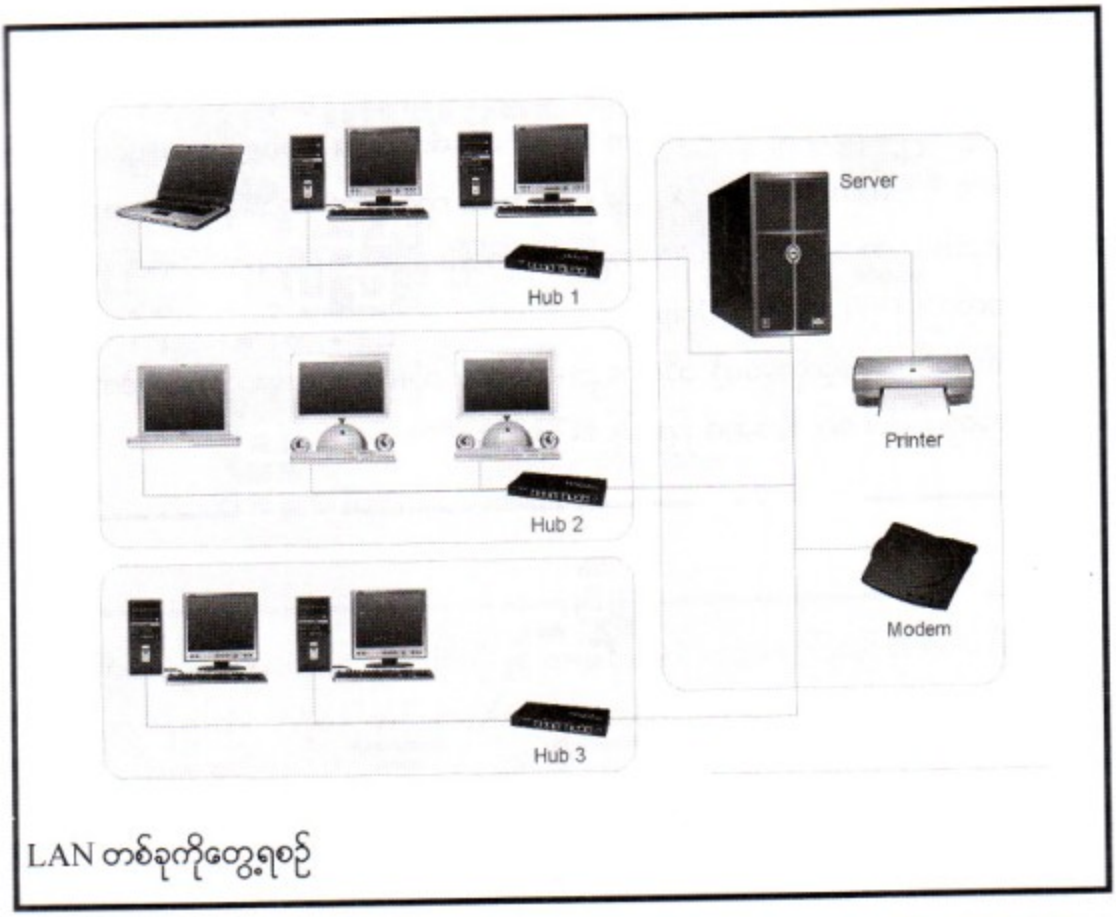
၃။ Wide Area Network (WAN)

Local Area Network (LAN) အကြောင်းသိစေအောင်းစရာ

အဆောက်အအုံတစ်ခုအတွင်းမှာပဲဆိုတဲ့ Area ငယ်လေးတစ်ခုထဲ တပ်ဆင်ထားတဲ့ Network ကွန်ရက်တစ်ခုပါပဲ။ ရုံးတွေ၊ ကုမ္ပဏီတွေ၊ ကျောင်းတွေမှာ တပ်ဆင်လေ့တပ်ဆင်ထရှိတဲ့ ကွန်ရက်ငယ်လေးတစ်ခုပါပဲ။ ဘာကြောင့်သူ့ကို ကွန်ရက်ငယ်လို့ပြောရသလဲဆိုရင် အဆောက်အအုံတစ်ခုရဲ့ ပြင်ပကိုကျော်ပြီး

ကျွမ်းကျင်ဖြန့်တဲ့ ကွန်ရက်တစ်ခုမဖြစ်နိုင်လို့ပါပဲ။ ဒါကတော့ သိအိုရီအရပေါ့လေ။ ဘယ်လိုပဲပြောပြော ပါ ကွန်ရက်အမျိုးအစားတွေရှိတဲ့အထဲမှာတော့ သူကသေးငယ်တဲ့ကွန်ရက်ပါပဲ။ သိအိုရီအရတော့ LAN အများဆုံး ၁၀၂၄ ပါဝင်ပြီး အဝေးဆုံးမီတာ ၉၀၀ အထိချိတ်ဆက်နိုင်ပါတယ်။ ဒါဟာလည်း ကွန်ရက် ချိတ်ဆက်ပေးတဲ့ ကြိုးပေါ်မူတည်ပါသေးတယ်။ တခြားကြိုးတစ်ခုနဲ့ တပ်ဆင်ကြည့်မယ်ဆိုရင် ဒီထက်လည်း ဖြန့်သွားနိုင်ပါတယ်။ အကျဉ်းချုံးမှတ်ထားရမှာကတော့ LAN ဆိုတာအဆောက်အအုံတစ်ခု ဒါမှမဟုတ် ဧရိယာငယ်တစ်ခုတည်းမှာပဲ တစ်နည်းအားဖြင့် ဧရိယာငယ်တစ်ခုတည်းမှာပဲ တပ်ဆင်တဲ့ကွန်ရက်ဆို တာပါပဲ။

ပုံ ၁.၂



LAN တစ်ခုကိုတွေ့ရစဉ်

Metropolitan Area Network (MAN) အကြောင်းဆိုအောင်းရော

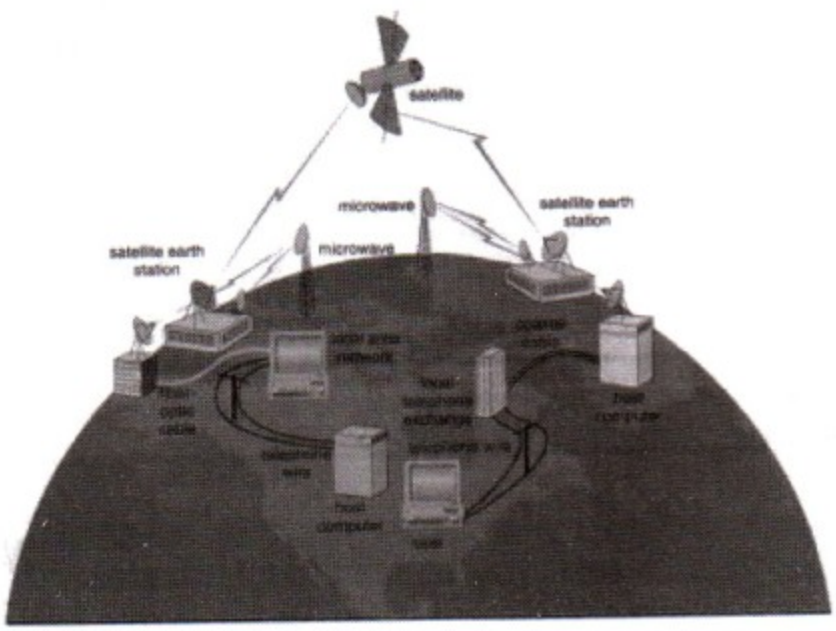
Local Area Network အရွယ်အစားနဲ့ Wide Area Network အရွယ်အစားတို့အကြားရှိသော ကွန်ရက်အမျိုးအစားဟာ Metropolitan Area Network ပဲပေါ့။ Metropolitan Area Network ဆိုတာ အပြင်မှာထက်စာအုပ်တွေမှာပဲ Reference အဖြစ်တွေ့ရတာများပါတယ်။ သူရဲ့သဘောက LAN တွေအများ ကြီးကို ၁၀၀ ကီလိုမီတာ အကျယ်အဝန်းလောက်မှာ ထပ်ဆင့်ချိတ်ဆက်ထားတာဖြစ်ပါတယ်။ သူဟာ LAN လို Private မဟုတ်ဘဲ Public ပိုဆန်တယ်။ နောက်ပြီး LAN ထက်ပိုတဲ့ High Speed နဲ့အချက်အလက်

တွေအပြင် အသံတွေကိုပါ အထက်ပါအကျယ်အဝန်းတွင် ပို့လွှတ်နိုင်ပါတယ်။ ဒါကလည်းသူက LAN နဲ့မတူတဲ့ Transmission Media နဲ့ Network Hardware တွေကိုသုံးထားတာကိုး။

Wide Area Network (Wan) အကြောင်းသိစေအောင်းရေး

Wide Area Network ဆိုတာကြတော့ တိုင်းနှင့်ပြည်နယ်တွေ အပြင်တစ်နိုင်ငံနှင့်တစ်နိုင်ငံကိုဖြတ်ကျော်ပြီး တစ်ကမ္ဘာလုံးအနေနဲ့ချိတ်ဆက်လိုက်တာဖြစ်ပါတယ်။ ယနေ့ခေတ်လူတိုင်းလိုလိုကြားဖူးနေကြတဲ့ Internet ဆိုတာ တကယ်တော့ ဒီ Wide Area Network (WAN) အမျိုးအစားပေါ့။ Internet ဆိုတာ ကွန်ရက်တွေကိုထပ်ဆင့်စုဆောင်းပြီး တစ်ကမ္ဘာလုံးအတိုင်းအတာနဲ့ ချိတ်ဆက်ထားတာဖြစ်ပါတယ်။ ကမ္ဘာ့အကြီးဆုံး ကွန်ပျူတာကွန်ရက်အသိုင်းအဝိုင်းကြီးပေါ့။ သူက ကွန်ရက်တွေကို ထပ်ဆင့်ချိတ်ဆက်ထားတာဖြစ်တာကြောင့် နည်းပညာအရသူ့ကို Internetwork လို့ခေါ်ပါတယ်။ တစ်နည်းအားဖြင့်ပြောရရင်တော့ Internet ဆိုတာ Internetwork ရဲ့အတိုကောက်ဖြစ်ပါတယ်။ ကွန်ပျူတာတွေ သန်းပေါင်းများစွာပါဝင်ဖွဲ့စည်းထားတဲ့ ဒီ Internet ဟာ ၁၉၇၀ လောက်ကတည်းကစတင်ပြီး ၁၉၉၄ ခုနှစ်မှ စတင်ပြီးပေါ်ပြူလာဖြစ် လာပါတယ်။ ဒါဟာလည်း GUI လို့ခေါ်တဲ့ Graphic User Interface ကြောင့် ကွန်ပျူတာကိုသုံးတဲ့ အထွေထွေလူတန်းစားစိတ်ဝင်စားမှုနှင့်လိုအပ်တဲ့ သီးခြားဌာနတစ်ခုထဲ သုံးရလောက်အောင်မခက်ခဲဘဲ အထွေထွေလူတန်းစားအတွက် သင့်တော်မှုတွေကြောင့်ပဲဖြစ်ပါတယ်။

ပုံ ၁.၃



Wide Area Network ကိုတွေ့ရစဉ်

ဆိုတာ Rule လေးတစ်ခုလောက်တော့လိုသဗျ။ ဆိုလိုတာကတစ်ဖက်ကပြောလိုက်တဲ့ ပို့လိုက်တဲ့ Signal ကို တစ်ဖက်ကဘယ်လိုဘာသာပြန်လဲပေါ့။ နောက်ပြီး တစ်ဖက်နှင့်တစ်ဖက် ဘယ်လို Initiate လုပ်ကြလည်းပေါ့။ နောက်တစ်ခုက Information တွေကို တစ်ဖက်နှင့်တစ်ဖက်ဖလှယ်တာတွေကိုရော ဘယ်လိုထိန်းချုပ်ကြသလဲပေါ့။ ကောင်းပါပြီ။ ဒီလို Network တစ်ခုမှာကွန်ပျူတာတွေတစ်လုံးနှင့်တစ်လုံးကြား Communicate ဖြစ်ဖို့က ဥပဒေသတွေပါဝင်တဲ့ စည်းကမ်းချက်တွေပါဝင်တဲ့ Software တစ်ခုရှိဖို့လိုအပ်ပါတယ်။ အဲဟာ Protocols ပဲပေါ့။ Protocols ဆိုတာ Communication ကိုထိန်းချုပ်ပေးတဲ့ Software တစ်ခုပဲဖြစ်ပါတယ်။ ဆိုလိုတာပြောရရင်တော့ Protocols ဆိုတာ Communication ကို Govern လုပ်ပေးတဲ့ Software ပေါ့ဗျာ။

ပုံ ၁.၅

ဘာသာစကားမတူ၍ Communication ပြုလုပ်၍မရပုံ

ဒီတော့ကား ကွန်ပျူတာတွေတစ်လုံးနှင့်တစ်လုံး ကြိုးလေးချိတ်ထားရုံ Network Card လေးတပ်ထားရုံနဲ့မပြီးဘဲ Communication ဖြစ်မြောက်ဖို့အတွက် Protocol ဆိုတာလိုအပ်တယ် အဲ့ဒီ Protocol တွေကတော့ဥပမာပြောရရင် -

(၁) TCP/IP (Transmission Control Protocol/Internet Protocol)

(၂) NetBEUI (Net BIOS Extended User Interface)

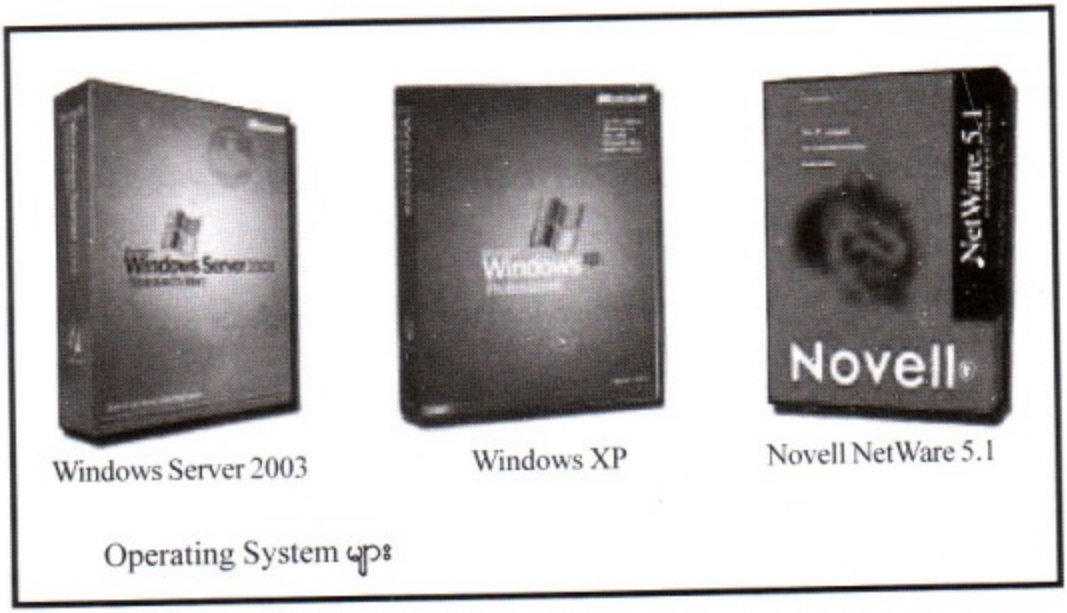
(၃) IPX/ SPX (Internetwork Packet Exchange/Sequence Packet Exchange) စသည် စသည်တို့ဖြစ်ကြပါတယ်။ တစ်ခြားလည်းရှိသေးတယ်ပေါ့ဗျာ။

၁.၃ Network Software ထိန်းချုပ်ခြင်းနည်းစနစ်

နောက်တစ်ခါလာပြန်ပြီ ဘာတဲ့ Network Software တဲ့ ဟုတ်ပါတယ်။ စိတ်မရှိပါနဲ့။ ကွန်ပျူတာတစ်လုံးနှင့်တစ်လုံးချိတ်ဆက်မိဖို့ ကွန်ပျူတာကို Network ကြိုးတွေနဲ့ချိတ်ဆက်ထားရုံ၊ Network Card တွေစိုက်ထားရုံ၊ အဲ အဲ Protocol လေးတင်ထားရုံနဲ့တင်မကပြန်ဘူးတဲ့ဗျ။ တစ်ခုတော့ရှိတာပေါ့ ကိုယ်တပ်ဆင်

ဒီလို Network က Client / Server Network မျိုး (နောက်သင်ခန်းစာတွင်ရှင်းပြထားသည်) ဆိုရင်ပေါ့။ ဟုတ်ပါတယ်။ အဲဒီလို Client / Server Network (Server Based Network) တွေမှာဆိုရင် အထက်ကတင်ပြပြီးသလို Network Card တွေ၊ Network ကြိုးတွေ၊ Network Protocol တွေနဲ့တင်မ လုံလောက်တော့ပါဘူး။ Network Software ဆိုတာကြီးပါ လိုလာပြန်သတဲ့၊ ဒီလိုပါ Network Software ဆိုတာတခြားတော့မဟုတ်ပါဘူး။ Network Operating System (NOS) ပါပဲ။ ဒီ NOS ဟာ ဘယ် တွန်ပျူတာ၊ ဘယ်အသုံးပြုသူ User ကတော့ဖြင့် Network ရဲ့ဘယ် Resources ကိုအသုံးပြုမယ် စတာတွေကို ထိန်းချုပ်ပေးရပါတယ်။ အဲဒီ NOS တွေကတော့ ဥပမာအားဖြင့် Microsoft Windows NT, Microsoft Windows Server 2000 or 2003, Novell Network စတာတွေဖြစ်ကြပါတယ်။ အဲဒီအထဲမှာမှ Windows NT Server, Windows Server 2000 or 2003, Novell Netware 5.1 တို့ဟာ Server Version တွေဖြစ်ကြပြီး၊ တဖက်က Client တွေကတော့ Microsoft Windows NT Workstation, Windows 2000 Professional, Windows XP တို့ဖြစ်နိုင်ကြပါတယ်။

ပုံ ၁.၆



Operating System များ

၁.၈ Network Services ကွန်ရက်ဝန်ဆောင်မှု

Network Services ဆိုတာ ကွန်ရက်ကလုပ်ဆောင်ပေးနိုင်တဲ့ ဝန်ဆောင်မှုတွေဖြစ်ပါတယ်။ အဲဒါတွေကတော့-

- File Services
- Print Services
- Communication Services

❖ Electronic Mail တို့ဖြစ်ကြပါတယ်။

ဒီ Services တွေကို ဘယ်သူက ဘယ်သူ့ကိုပေးနေတာလဲ။ အလဲသိဖို့လိုပါတယ်။ ဒီတော့ ဒီနေရာမှာ ဝန်ဆောင်မှုကိုပံ့ပိုးပေးသူနဲ့ ဝန်ဆောင်မှုကိုတောင်းဆိုသူ ဆိုပြီးရှိပါတယ်။ Service Provider နဲ့ Service Requester ပေါ့ဗျာ။ Service Provider ဆိုတာဝန်ဆောင်မှုကိုပံ့ပိုးပေးသူပါ။ Service Requester ဆိုတာကတော့ ဝန်ဆောင်မှုကိုတောင်းဆိုသူ အလိုရှိသူပါ။ ဥပမာပြောရရင် စားသောက်ဆိုင်တစ်ဆိုင်ကိုစားသုံးသူလာမယ်။ ထမင်းကြော်မှာမယ်။ ဒါဝန်ဆောင်မှုကိုတောင်းဆိုတာပဲ။ Service Requester ပေါ့။ စားသောက်ဆိုင်က စားသုံးသူကိုပံ့ပိုးပေးရတာဆိုတော့ Service Provider ပေါ့။ Service Requester တွေကကြိုက်တဲ့ဟင်းလျာကို ကြိုက်သလောက်မှာစားကြမှာ၊ အဲ့ဒီအပြင် မှာစားတဲ့အရေအတွက်ရော၊ မှာစားတဲ့ဦးရေရောမျှားမှာဖြစ်ပါတယ်။ ဒါပေမယ့်စားသောက်ဆိုင်က တစ်ဆိုင်တည်း။ ဒီတော့ Service Requester မှာ မှာသမျှကိုအားလုံးမလစ်ဟင်းအောင်လုပ်ပေးနိုင်ဖို့က Service Provider ဖြစ်တဲ့သူက အင်အားတောင့်တင်းမှဖြစ်မှာပါ။ Service Provider နဲ့ Service Requester မှာ အောက်ပါတို့ ပါဝင်ပါတယ်။

သူတို့ကတော့-

❖ Server- သူကတော့ Service Provider သက်သက်ပါ။

❖ Client- သူကတော့ Service Requester သက်သက်ပါ။ ဘယ်သူ့ကိုမှ Service Provider မလုပ်ပါဘူး။

❖ Peers- သူကတော့ Service Provider လဲလုပ်ပါတယ်။ Service Requester လဲလုပ်ပါတယ်။

ဆိုလိုချင်တာက Peer Network မှာပါဝင်တဲ့ကွန်ပျူတာတစ်လုံးဟာ တစ်ခြားကွန်ပျူတာကို Service Provide လဲလုပ်နိုင်သလို သူကိုယ်တိုင်ကလည်း လိုအပ်တဲ့အချိန်တွေမှာ Service Requester ပြန်လုပ်ပါတယ်။ ဒီတော့ ကွန်ရက်ထဲက မည်သည့်ကွန်ပျူတာတစ်လုံးဟာ ကွန်ရက်ဝန်ဆောင်မှုကို တောင်းလည်းတောင်းခံမယ်။ အဲ့ဒီအပြင်ဝန်ဆောင်မှုကိုလည်းပေးမယ်ဆိုရင် ဒါကို Peer-to-Peer Network လို့ခေါ်ပါတယ်။

၁.၉ **Network Types** ကွန်ရက်အမျိုးအစားများ

ကွန်ရက်ကိုအမျိုးအစားအရခွဲခြဲရမယ်ဆိုရင် (၂) မျိုးရှိသဗျ။ အဲ့ဒါကတော့-

၁။ Peer to Peer Network

၂။ Client/Server Network (Server ကို Based အခြေပြုထားသော Network)

ရယ်လို့နှစ်မျိုးရှိပါတယ်။ ဒီစာအုပ်မှာတော့ ကျွန်တော်တို့ဟာ Server Based Network ကိုပဲ အဓိကထားဖော်ပြသွားမှာဖြစ်ပါတယ်။

အခုနဲ့ Network Types နှစ်ခုဖြစ်တဲ့ Peer Network နဲ့ Server Based Network ကိုမရှင်းပြခင်မှာ Server ဆိုတာဘာလဲ Workstation ဆိုတာဘာလဲ စတာတွေကိုလေ့လာကြည့်ကြရအောင်။

Server ခံဦးခဏ်သူ

Server ဆိုတာဝန်ဆောင်မှုတောင်းဆိုတဲ့သူတွေကို ဝန်ဆောင်မှုပံ့ပိုးပေးရတဲ့အလုပ်တွေကိုလုပ်ပါတယ်။ သူကတစ်ဖက်သတ်ပါ။ သူကနေဝန်ဆောင်မှုပြန်မယူပါဘူး။ သူကဝန်ဆောင်မှုပေးတဲ့အလုပ်ကိုပဲလုပ်ပါတယ်။ ဒါပေသိ ရှေ့သင်ခန်းစာကပြောခဲ့တဲ့စားသောက်ဆိုင် ဥပမာအတိုင်းပေါ့။ ဝန်ဆောင်မှုကိုတောင်းဆိုသူတောင်းသလောက်ပေးနိုင်အောင် Server ကအင်အားတောင့်တင်းဖို့လိုပါတယ်။ ဥပမာ Multi Processor သုံးဖို့လိုကောင်းလိုမယ်။ RAM က ECC ပါဖို့လိုကောင်းလိုမယ်။ Hard Disk က SCSI ဖြစ်ဖို့လိုကောင်းလိုမယ်။ အမြင့်ဆုံးနဲ့အမြန်ဆုံးဖြစ်ဖို့လိုအပ်ပါတယ်။ အောက်မှာ Server အမျိုးအစားတွေကိုဆက်လက်ပြောပြပေး ထားပါတယ်။ Server တစ်မျိုးချင်းစီဟာသက်ဆိုင်ရာတာဝန်တစ်ခုကိုပဲလုပ်ကြပါတယ်။

- File Server - ဖိုင်များကိုသိမ်းဆည်းပေးထားခြင်းနှင့်တောင်းခံရင်း ဖြန့်ဝေပေးခြင်း။
- Print Server - ကွန်ရက်မှာရှိတဲ့ Print များကိုထိန်းချုပ်ခြင်းနှင့်အုပ်ချုပ်ခြင်း။
- Proxy Server - တခြားကွန်ပျူတာကိုယ်စားလုပ်ငန်းတွေကို လုပ်ဆောင်ပေးပါတယ်။ ဆိုလိုတာက ကိုယ်စားလို့ ဆိုလိုချင်တာပါ။
- Application Server - ကွန်ရက်မှာအသုံးပြုမယ့် Application တွေနဲ့ပတ်သက်လို့ဝန်ဆောင်မှုပေးပါတယ်။
- Web Server – Web Pages နဲ့တခြား Web Content တွေကိုသိမ်းထားပေးခြင်းနှင့် Hypertext Transfer Protocol (HTTP) ကိုအသုံးပြုပြီးတော့ လိုရာသို့ပေးပို့ခြင်း။

Mail Server - E-Mail များကိုလက်ခံခြင်းနှင့် ပေးပို့ခြင်းတို့ကိုလုပ်ဆောင်ပေးခြင်း။

အဲဒီအပြင် Fax Server, Remote Access Server, Telephony Server တို့ ဆိုတာရှိပါသေးတယ်။

Workstation တောင်းခံဝန်ဆောင်သူ

Workstation ဆိုတာဝန်ဆောင်မှုတောင်းဆိုတဲ့သူဖြစ်ပါတယ်။ ဒီနေရာမှာ Workstation ဆိုတာနဲ့ Client ဆိုတာကွဲပြားအောင်ပြောပြရပါအုံးမယ်။ ကွန်ရက်မှာချိတ်ဆက်ထားတာတွေက ကွန်ပျူတာချည်းပဲတူတ်ချင်မှတူတ်ပါလိမ့်မယ်။ ကွန်ပျူတာအပြင် ပရင်တာတွေလည်းပါနိုင်တယ်လေ။ ကွန်ရက်တစ်ခုမှာလိုအပ်ချက်တွေကိုတောင်းခံသူတွေအားလုံးဟာ Client ပါ။ ဆိုလိုချင်တာက ကွန်ရက်မှာရှိတဲ့ လိုအပ်ချက်ကိုတောင်းဆိုသူတိုင်းပါ။ ကွန်ပျူတာ၊ ပရင်တာအားလုံးပေါ့။ ဒါ Client ပဲ။ ဒါပေမယ့် Workstation ဆိုတာ

ကွန်ရက်ထဲက ဝန်ဆောင်မှုကိုတောင်းခံသူကွန်ပျူတာတွေပါပဲ။ ကွန်ပျူတာမဟုတ်တဲ့ တောင်းခံသူကိုတော့ Client လို့ခေါ်ပြီး ကွန်ပျူတာဆိုရင်တော့ Workstation လို့ခေါ်ပါတယ်။ ဒီတော့ Workstation တိုင်းဟာ Client ဖြစ်တယ်။ Client တိုင်းဟာ Workstation မဟုတ်ဘူး။

၁.၁၀ Peer to Peer Networking ဆိုတာ

Peer to Peer Network ဆိုတာကွန်ရက်အတွင်းမှာရှိနေတဲ့ ကွန်ပျူတာတွေဟာ တစ်ခုနှင့်မှာ ဝန်ဆောင်မှုကိုတောင်းခံပြီးတော့ တစ်ခုနှင့်မှာသူဟာတခြားသူတောင်းခံတဲ့ ဝန်ဆောင်မှုကိုပံ့ပိုးပေးတဲ့သူ ဖြစ်နိုင်ပါတယ်။ ဆိုလိုတာက သူလိုနေတဲ့အချိန်မှာ ကိုယ်ကပံ့ပိုးပေးပြီးတော့ကိုယ်လိုနေတဲ့ အချိန်ကျတော့ ကိုယ်ကပြန်တောင်းခံရပြန်ရော။ ဒီတော့ Peer Network မှာကိုယ်ဟာတောင်းခံတဲ့သူလည်းဖြစ်နိုင်တယ်။ ပံ့ပိုးတဲ့သူလည်းဖြစ်နိုင်တယ်။ တောင်းခံတဲ့အခါကြတော့ကိုယ်က Client ပေါ့။ ပံ့ပိုးတဲ့အခါကြကိုယ်က Server ဖြစ်သွားပြန်ရော၊ ဒီတော့ Peer Network မှာ Dedicated Server ဆိုတာမရှိဘူး။ Dedicated Server ဆိုတာ အဲဒီကွန်ပျူတာက တစ်ခုနှင့်လုံး Server အလုပ်ကြီးကိုပဲ သက်သက်လုပ်နေတာကိုပြောတာ။ အဲဒီလိုမရှိဘူး။ တစ်ခုနှင့်မှာ ကိုယ်ကတောင်းခံရင်း Client ဖြစ်သွားသလို တစ်ခုနှင့်မှာကိုယ်ကပံ့ပိုးရင် Server ဖြစ်သွားပြန်တယ်။ ဒါကြောင့် Peer Network ကို Workgroup လို့လည်းခေါ်ပါတယ်။ ဆိုလိုတာက သူငယ်ချင်းကို ကိုယ်ကစာပြပေးတယ် သူနားမလည်လို့ထားပါတော့ ဒီတော့ကိုယ်က Server တစ်ခါ ကိုယ်နားမလည်တဲ့ စာကြတော့ကိုယ်ကပြန်မေးရတယ်။ ဒီအခါကိုယ်က Client ဖြစ်သွားပြီး။ စားသောက်ဆိုင်တစ်ဆိုင်မှာ ကိုယ်ကထမင်းသွားစားတယ်။ ဒီတော့စားသောက်ဆိုင်က Server ပံ့ပိုးပေးတဲ့သူပေါ့ဗျာ။ စားသုံးသူကတော့ တောင်းဆိုတာဆိုတော့ Client ပေါ့။ တစ်နေ့ကြတော့ စားသုံးသူက ငါ တစ်နေ့တစ်နေ့မင်းဆီမှာ ထမင်းဝယ်စားနေတာကြာပြီ ဒီနေ့တော့ငါဆီကမင်းပြန်ဝယ်စား ဒါမျိုးလုပ်လို့မရဘူး။ ဒါဟာ Workgroup အတူတကွ ဖလှယ်ကြတဲ့ သဘောမဟုတ်ဘူး။

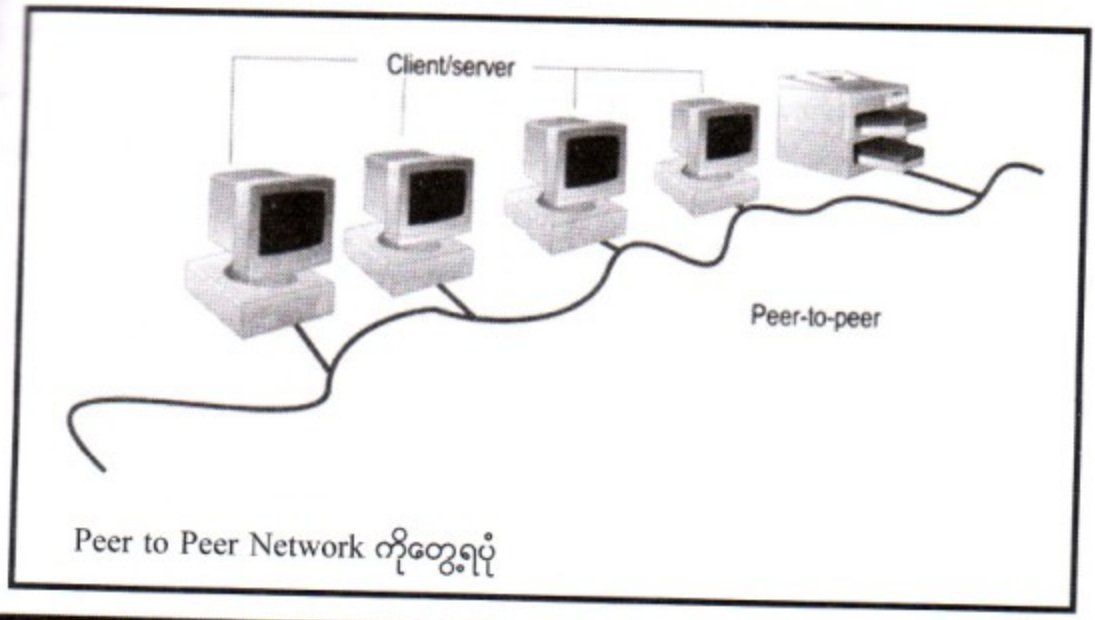
ဒီတော့ ပြောပြချင်တာက Peer Network မှာ Server ဆိုပြီးသက်သက်မရှိဘူး။ စက်တစ်လုံးဟာ Server လည်းဖြစ်သွားနိုင်သလို Client လည်းဖြစ်သွားနိုင်တယ်။ Centralized စနစ်မဟုတ်ဘူး။ ဗဟိုကနေထိန်းချုပ်ပေးတဲ့စနစ်မဟုတ်ဘူး ဒီတော့အသုံးပြုသူ User ဟာသူ့ကွန်ပျူတာထဲမှာရှိတဲ့ Resources တွေကိုပဲအသုံးပြုတယ်ဆိုရင် Local User ဟုခေါ်ပြီး ဒီကနေမှတခြား ကွန်ပျူတာဆီက Resources တွေကိုလှမ်းယူအသုံးချတယ်ဆိုရင်တော့ ဒါကို Remote User လို့ခေါ်ပါတယ်။

နောက်တစ်ခုက Peer Network အတွက် NOS ဆိုတဲ့ Network Operation System သီးခြားမလိုအပ်ပါဘူး။ ကိုယ့်စက်မှာအသုံးပြုနေတဲ့ Microsoft Windows နဲ့တင် Peer Network တစ်ခုကိုတည်ဆောက်လို့ရနေပါပြီ။

နောက်တစ်ခုထပ်ပြောချင်တာက Peer Network တစ်ခုမှာ ကွန်ပျူတာ ၅ လုံးရှိရင်အဲဒီကွန်ပျူတာ ၅ လုံးစလုံးက အကြောင်းအရာတွေကို ကိုယ်စီကိုယ်ငှ Share လုပ်ထားကြတယ်။ ဒီကွန်ပျူတာတစ်လုံးက

ခေါ်ကြည့်လို့ရသလို တတိယမြောက်လူကလည်း တခြားကွန်ပျူတာ ယူကြည့်လို့ရပြန်ရော၊ တကယ့်ကိုအတွင်းသိအဆင်းသိတွေပေါ့။ ဒါကြောင့် Security အရမကောင်းဘူး။ Security လိုအပ်တဲ့နေရာတွေမှာ Peer နောက်ပြီး Peer Network က ကွန်ပျူတာအလုံးအရေအတွက် သိပ်များ

အားသာချက်ကတော့ Peer Network မှာချိတ်ဆက်ထားတဲ့ကွန်ပျူတာတွေဟာ လုပ်ပိုင်ခွင့်ဆိုတဲ့ Rights တစ်လုံးတည်းမှာပဲလုပ်ပိုင်ခွင့်ကို Centralized လုပ်ထားတာမျိုးမရှိပါဘူး။ တခြားသူက ကိုယ့်ဆီက အချက်အလက်တွေကိုလိုချင်တဲ့အခါမှာ ကိုယ်က ပံ့ပိုးသူပြန်ဖြစ်သွား လုပ်ငန်းသဘောအရ အချက်အလက်လုံခြုံဖို့မလိုအပ်ပါက အခုလို Peer to Peer Network Security အရဆိုရင် အားနည်းလို့ပါ။ နောက်ပြီး Network Operating System သီးခြား



Peer to Peer Network ကိုတွေ့ရပုံ

Peer Network ၏ ကောင်းကျိုးများ

၁။ လွယ်ကူစွာတပ်ဆင်နိုင်ခြင်းနှင့် Configure လုပ်နိုင်ခြင်း။

၂။ ကွန်ပျူတာ တစ်လုံးချင်းစီကိုက Dedicated Server ပေါ်မမှီခိုဘဲသီးခြားစီရပ်တည်နိုင်ခြင်း။

၃။ အသုံးပြုသူတစ်ဦးချင်းစီကိုက ကိုယ့်ပိုင်ဆိုင်မှုများကိုခွဲဝေပေးခြင်း။

၄။ ကုန်ကျစရိတ်သက်သာခြင်း။

၅။ သီးခြားပစ္စည်းများ Software များမလိုအပ်ခြင်း။ ဥပမာ Network Operating System

၆။ ၎င်း Network ကြီးပုံမှန်အလုပ်လုပ်နေအောင်သီးခြား Administrator မလိုအပ်ခြင်း။

Peer Network ၏ အားနည်းချက်များ

၁။ Security အားနည်းခြင်း။

၂။ ခွဲဝေအသုံးပြုမည့် Resources များသည် Single Password နှင့်မထိန်းချုပ်ထားနိုင်ခြင်း။

၃။ Data များကို Backup ပြုလုပ်ရာတွင်လည်း ကွန်ပျူတာတစ်လုံးချင်းစီမှသီးခြားစီပြုလုပ်နေရခြင်း။

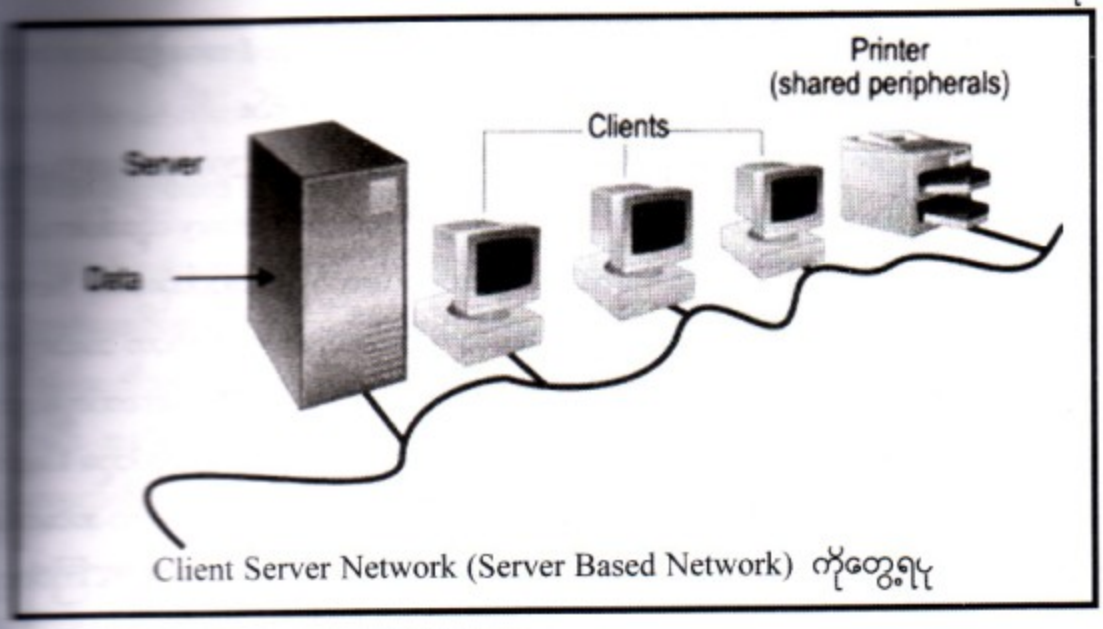
၄။ အသုံးပြုသူတစ်ဦးကအခြားကွန်ပျူတာတစ်လုံးစီမှ Resources ကိုလှမ်းယူသုံးလိုက်တိုင်း အသုံးခံရသည့်တစ်နည်းအားဖြင့် ပံ့ပိုးပေးရသည့်ကွန်ပျူတာမှာ Performance ကျသွားခြင်း။

၅။ အပြန်အလှန်ဖလှယ်နေခြင်းကြောင့် ဗဟိုထိန်းချုပ်မှုစနစ်မရှိခြင်း။

၆။ ကွန်ပျူတာ ၁၀ လုံးထက်ပို၍အသုံးပြုလျှင်မသင့်တော်ခြင်းတို့ကြောင့်ဖြစ်သည်။

၁.၁၁ Server Based Network ဆိုတာ

ကွန်ရက်တစ်ခုမှာ အသုံးပြုတဲ့သူတွေကို လိုအပ်တာတွေပံ့ပိုးပေးဖို့သီးခြား Dedicated Server ထိုင်လိုက်ပြီဆိုရင်တော့ ဒါဟာ Server Based Network ဖြစ်သွားပြီပေါ့။ Server Based Network ဆိုတာ ကျွန်တော်တို့သိခဲ့ကြတဲ့ Client Server Network ပါပဲ။ သူကတော့ ဝန်ဆောင်မှုကိုတောင်းခံသူကလည်း တစ်ဖက်သတ်တောင်းခံကြပြီးတော့ ပံ့ပိုးပေးတဲ့ Server ကလည်းပံ့ပိုးပေးတဲ့ အလုပ်ကိုပဲ တစ်ဖက်သတ်လုပ်ဆောင်ပါတယ်။ ခုနက ကျွန်တော်ပြောခဲ့တဲ့ စားသောက်ဆိုင်လိုပေါ့ဗျာ။ စားသုံးသူတွေက အမြဲတမ်းစားသုံးတဲ့ဘက်ကပဲပေါ့။ ရောင်းတဲ့သူဘက်ကလည်း အမြဲတမ်းပံ့ပိုးပေးတဲ့ဘက်ကပဲ။ ဒီတော့အသုံးပြုသူတွေဟာ Client/Workstation တွေမှာပဲ ထိုင်နေကြပြီး Server ဆီကိုဝန်ဆောင်မှုတွေတောင်းခံကြပါတယ်။ ဒါပေမယ့်လည်း Server မှာတော့တခါတရံ Configure လုပ်တာထိန်းချုပ်တာကလွဲလို့ သူကိုတခြားရည်ရွယ်ချက်နဲ့အသုံးမပြုပါဘူး။ ဆိုလိုတာက ဝန်ဆောင်မှုကိုတောင်းခံတဲ့သူကို နိုင်နိုင်နင်းနင်း ပံ့ပိုးပေးနိုင်အောင်လို့ပါ။ ဒီ Server Based ကွန်ရက်တွေကို Sharing အတွက်ရော Security အတွက်ရောလိုအပ်တဲ့လုပ်ငန်းတွေမှာအသုံးပြုကြပါတယ်။ Server Based Network တွေဟာတစ်နည်းအားဖြင့် ဗဟိုထိန်းချုပ်မှုစနစ်နဲ့ အလုပ်လုပ်တဲ့ Centralized ထိန်းချုပ်မှုဖြစ်ပါတယ်။ နောက်တစ်ခုက Server Based Network တွေဟာ NOS ကိုလိုအပ်ပါတယ်။



Client Server Network (Server Based Network) ကိုတွေ့ရပါ့

ဦး NOS ကို Server မှာ Install လုပ်ရမှာဖြစ်ပါတယ်။ အချုပ်ပြောရရင် Client Server Network ဆိုတာတော့ ကွန်ရက်ကြီး တစ်ခုလုံးကို စက်တစ်လုံးက Network Operating System ကိုအသုံးပြုပြီး ထိန်းချုပ်နေပါတယ်။ အဲဒီစက်ကတော့ Server ပဲဖြစ်ပါတယ်။

Client Server Network ဆိုတာဒီ Network မှာ Client လဲပါတယ်။ Server လဲပါတယ်။ Client မှန်သမျှအားလုံးဟာ Server ဆီက သူတို့လိုအပ်သမျှကို ဝန်ဆောင်မှုတွေတောင်းဆိုကြပါတယ်။ Server က Client တွေကို Service ပြန်ပေးပါတယ်။ Client Server Network ဟာ Peer to Peer Network ထက်သာတဲ့အချက်တွေများစွာရှိပါတယ်။ Client Server Network ဟာ Centralized ဖြစ်တာကြောင့် ကွန်ပျူတာတွေဟာအချက်အလက်တွေကို ရှာဖွေရတာလွယ်ကူပါတယ်။ ထိန်းချုပ်ရတာလည်း အဆင်ပြေသက်သာသွားပါတယ်။ အဲဒီအပြင် Security ကလည်းအင်မတန်ကိုတင်းကျပ်ပါတယ်။ ကွန်ရက်ကို အသုံးပြုမယ့် User တွေဟာ Client တွေမှာရှိနေကြပြီး မိမိတို့ကွန်ရက် အတွင်းဝင်ရောက်အသုံးပြုနိုင်ဖို့ Server ဆီမှာ ဝင်ခွင့်တောင်းရပါတယ်။

Logon ပေါ့။ Logon ဆိုတာမိမိနာမည် (ကွန်ရက်အတွင်းဝင်ဖို့ သတ်မှတ်ပေးထားသောနာမည်) Username နဲ့ Password စကားဝှက်ကိုရိုက်ထည့်လိုက်ရတာ။ အဲဒီအခါကျ Server က သူ့မှာယခင်ကတည်းက ကွန်ရက် အတွင်းဝင်ရောက်အသုံးပြုခွင့် ရရှိထားသူတွေရဲ့ Username (Database) ကိုကြည့်ပါတယ်။ မှန်တယ်ဆိုမှ အသုံးပြုခွင့်ပေးလိုက်တာပါ။ ဒါအကြမ်းအားဖြင့်ပြောတာပါ။ ဒါဟာလည်း Peer နဲ့ကွာခြားတဲ့အချက်ပဲပေါ့။ Peer ကြတော့ Server ဆိုတာမရှိဘူး။ လာသုံးတဲ့အခါရိုက်ထည့်တဲ့ Username ကိုရိုက်ထည့်တဲ့ ကွန်ပျူတာမှာပဲ စစ်လိုက်ပြီး မှန်ရင်အသုံးပြုခွင့်ပေးလိုက်တာပါ။ စက်တစ်လုံးမှာပဲ အသုံးပြုခွင့်ရှိတယ်။ Client Server မှာကြတော့ Username Database က Server မှာရှိတာပါ။ စက်တစ်လုံးမှာထိုင်ပြီး Logon လုပ်လိုက်တာနဲ့ မှန်ရင်အသုံးပြုခွင့် ရရှိသွားတာပါပဲ။ Server မှာပဲအသုံးပြုမယ့် User Accounts တွေ၊

Passwords တွေ၊ လုပ်ပိုင်ခွင့် Access Rights တွေကို Centralized အနေနဲ့သိမ်းထားတာကြောင့် ကွန်ရက်ကို ချုပ်ကိုင်ရတာ လွယ်ကူပြီး Security တင်းကျပ်မှုရှိလာပါတယ်။

အဲဒီလိုဖြစ်စဉ်ကို Microsoft Windows NT, Windows Server 2000 or 20003 တွေမှာဝင်းကို Domain Model လို့ခေါ်ပါတယ်။ တနည်းအားဖြင့် ၎င်းကို Active Directory လို့ခေါ်ပါတယ်။ Novell မှာတော့ Novell Directory Services (NDS) လို့ခေါ်ပါတယ်။ထပ်ပြီးရှင်းပြပါအုံးမယ်။ Server Based Network တွေဟာ Single Logon ဖြစ်ပါတယ်။ ဆိုလိုတာကအဲဒီ လူတစ်ယောက်ဟာ ဘယ်ကွန်ပျူတာမှာ ထိုင်ထိုင် ဒီ Logon လေးတစ်ခုကိုပဲအသုံးပြုပြီးဝင်ရပါတယ်။ ဆိုလိုတာ ကအဲဒီ User ဟာကွန်ပျူတာအလုံး ၂၀ ရှိလို့ အဲဒီကွန်ပျူတာတိုင်းမှာထိုင်သုံးလို့ Logon Name အခုနစ်ဆယ်ရှိ စရာမလိုပါဘူး။ Logon Name တစ်ခုတည်းနဲ့ပဲ မည်သည်စက်ကနေမဆို Access လုပ်လို့ရပါတယ်။ ဒါဟာထိန်းချုပ်ရတာ အင်မတန်လွယ်ကူသွားတာပေါ့။ ဒါကိုပဲ Centralized ဗဟိုထိန်းချုပ်မှုစနစ်လို့ခေါ်တာပါ။ Peer Network ကြတော့ အဲဒီလိုမဟုတ်ဘူးဗျ။ အဲဒီလူတစ်ယောက်ဟာကွန်ပျူတာအလုံး ၂၀ ရှိလို့အဲဒီ အလုံးပေါက်စေ့တိုင်းမှာထိုင်သုံးတဲ့အခါမှာ Logon Name နဲ့ Password ကိုတစ်ခုမက အများကြီးအသုံးပြုလို့ရတယ်။

Server Based Network ၏ ကောင်းကျိုးများ

၁။ User Accqunt, Security, Access Control စတာတွေဟာဗဟိုထိန်းချုပ်မှုဖြစ်တာတွေကြောင့် ကွန်ရက်ကိုအုပ်ချုပ်ရတာလွယ်ကူပါတယ်။

၂။ Server ကိုသက်သက်ထားပြီး တကယ့်ကိုစွမ်းအားမြင့်ပစ္စည်းတွေ သုံးထားတာကြောင့် Network ရဲ့ Resources ကိုသုံးစွဲရာမှာ Efficient ဖြစ်စေပါတယ်။

၃။ Network မှာရှိတဲ့ Resources တွေ့ကိုသုံးစွဲတဲ့အခါမှာ Network ကို Logon တစ်ခါဝင်ထားရုံနဲ့ လုပ်နိုင်ပါတယ်။

၄။ အသုံးပြုသူများသည်ဖြစ်စေ အရင်းအမြစ်များကိုအသုံးချမှုများသည်ဖြစ်စေ Server Based Network က Handle လုပ်နိုင်ပါတယ်။

Server Based Network ၏ အားနည်းချက်များ

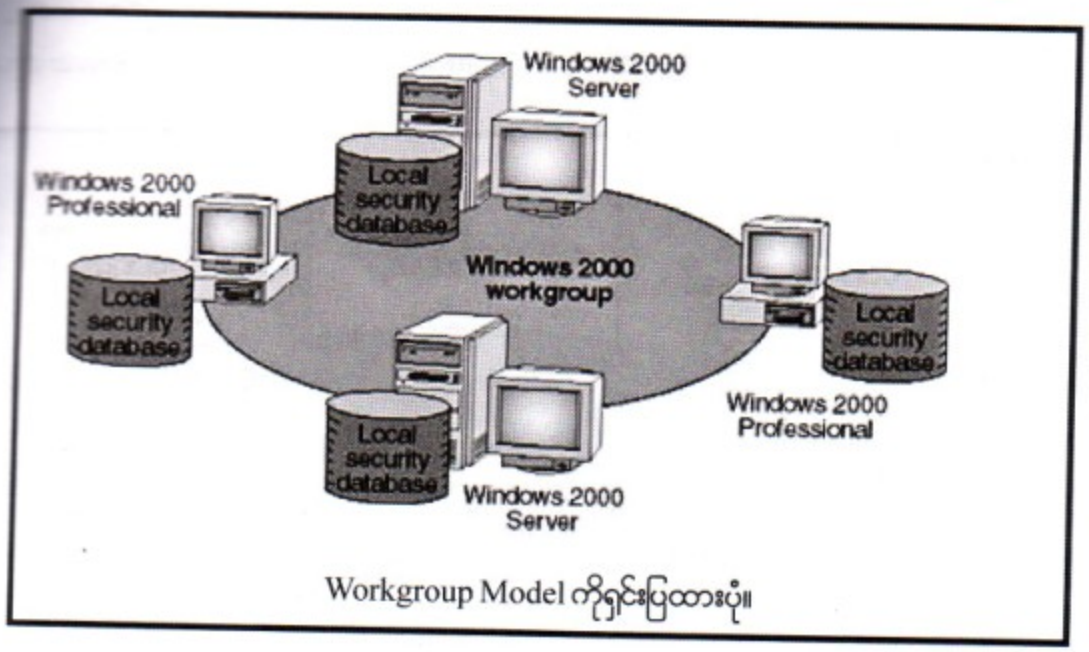
၁။ အဆိုးရွားဆုံးကတော့ Server Failure ဖြစ်သွားရင် Network ကြီးတစ်ခုလုံးအလုပ်လုပ်လို့မရ အောင်ဖြစ်သွားတော့တာပဲ။

၂။ ကုန်ကျစရိတ်တွေပိုများပါတယ်။ ကျွမ်းကျင်ဝန်ထမ်းတွေလည်း ရှိဖို့လိုအပ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ Server ကိုသီးသန့်ထားရခြင်း ၎င်းအတွက် NOS များတပ်ဆင်ရခြင်းတို့ကြောင့်ဖြစ်ပါတယ်။

Server Based Network ကိုအကြောင်းပြုပြီး ပိုပြီးနားလည်သွားအောင် Domain Model နှင့် Workgroup Model ကိုဆက်ပြီးရှင်းပြပါအုံးမယ်။

Workgroup Model အကြောင်း

ဦးစွာ Single Point မဟုတ်ဘူး။ Windows NT ကွန်ပျူတာတစ်လုံးချင်းစီမှာ ကိုယ်ပိုင် Directory Database ရှိရတယ်။ အသုံးပြုသူဟာ Logon လုပ်လိုက်တာနဲ့ လက်ရှိအသုံးပြုနေတဲ့ ကွန်ပျူတာထဲက Database ကိုသွားစစ်ပြီးဝင်ခွင့်ပေးလိုက်ပါတယ်။ ဒီတော့ အဲဒီအသုံးပြုသူဟာ နောက်ကွန်ပျူတာတစ်လုံးကို အသုံးပြုတော့မယ်ဆိုရင် အဲဒီအသုံးပြုသူရဲ့ Database တစ်နည်းအားဖြင့် Accounts ဟာ အသစ်ကြေညာပေးရပါတယ်။ မရှိရင်သုံးလို့မရဘူး။ ဒါကြောင့်မို့ Single Point မဟုတ်ဘူးလို့ပြောတာ။



Workgroup Model ကိုရှင်းပြထားပုံ။

၁.၁၃ Domain Model အကြောင်း

လိုအပ်တဲ့ Directory Services Database ကို Domain Controller မှာဘုံထားပြီး အသုံးပြုသူတွေက Share လုပ်ပြီးသုံးပါတယ်။ ဒါကြောင့် ဒါဟာ Single Point Administration ပါပဲ။

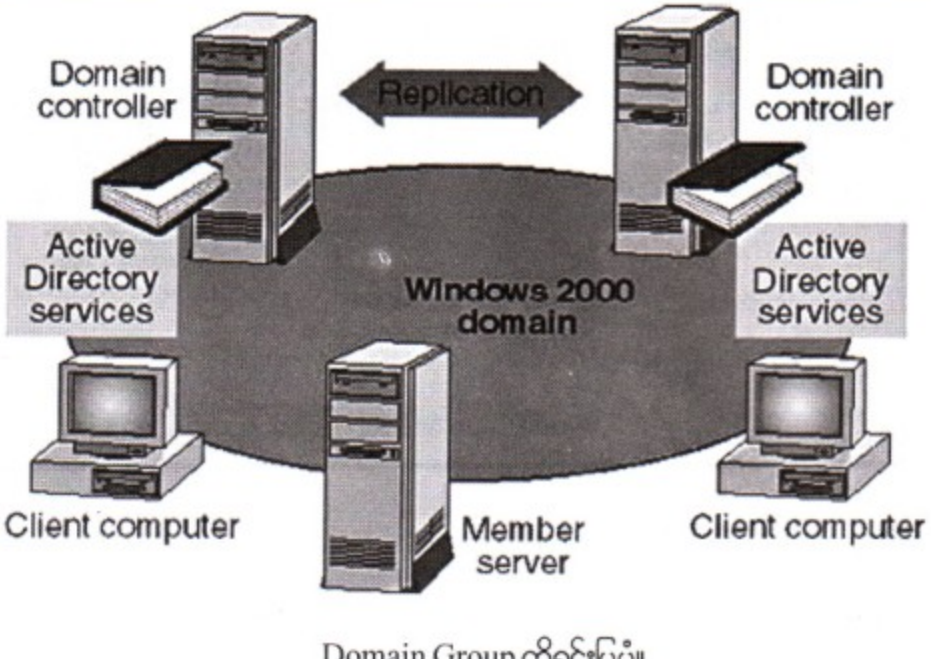
၁.၁၄ Server များ

Server ဆိုသည်မှာလည်းအသုံးချမှုပေါ် မူတည်ပြီးအမျိုးမျိုးရှိပါတယ်။ ဆိုလိုတာက Server တစ်လုံးထဲကိုလုပ်ငန်းမျိုးစုံသုံးနေရင် မနှိပ်မနင်းဖြစ်မှာစိုးတဲ့အတွက်ကြောင့်မို့လို့ လုပ်ငန်းပေါ်မူတည်ပြီး Server တွေလည်း အမျိုးအစားကွဲပြားလာရခြင်းဖြစ်သည်။

Domain Controller (Directory Server အခြေခံ)

ငင်း Server တွေမှာ Directory Services ဆိုတာရှိပါတယ်။ သူကဘာလုပ်ပေးလည်းဆိုတော့ အသုံးပြုသူတွေကို Network မှာရှိတဲ့ Resources တွေကိုအသုံးချရာ၌ လုံခြုံစိတ်ချရမှုရှိအောင်စီစစ်ပေးခြင်း ငင်းတို့နဲ့ပတ်သက်တဲ့ Information တွေကို သိမ်းဆည်းပေးခြင်း စတာတွေကိုလုပ်ဆောင်ရပါတယ်။ အသုံးပြုသူတွေဟာ ကွန်ရက်အတွင်းမှာရှိတဲ့ ဘယ် Resources ကိုမဆိုသုံးနိုင်အောင် ကွန်ပျူတာတွေကို Logical နည်းအရ ပေါင်းစည်းထားပါတယ်။ အဲဒါကို Domain လို့ခေါ်ပါတယ်။ ဘယ် User မဆိုသက်ဆိုင်ရာ Domain ရဲ့ အဖွဲ့ဝင်ဖြစ်နိုင်ပြီး ငင်း Domain အတွင်းရှိ Resources များနှင့် Information များကိုယူသုံးနိုင်စွမ်းရှိပါတယ်။ ဒါပေမယ့် အဲဒီအသုံးပြုတဲ့သူဟာ Domain ကို Logging လုပ်ရမှာဖြစ်ပါတယ်။ အဲဒီလို Logging လုပ်ဖို့ Logon Services တွေကွန်ပျူတာနှင့် User တွေကို Domain ထဲမှာစုစည်းပေးထားတဲ့ တနည်းအားဖြင့် Handle လုပ်ပေးတဲ့ Server ကို Domain Controller သို့မဟုတ် Directory Server လို့ခေါ်တယ်။

ပုံ ၁.၁၀



Domain Group ကိုရှင်းပြပုံ။

File and Print Server အခြေခံ

File and Print Server ကတော့ အဓိကအားဖြင့် Network မှာ File တွေကိုသိမ်းပေးထားခြင်း ပြန်ခေါ်ခြင်းစတဲ့ဝန်ဆောင်မှုတွေ Network Printer တွေကိုအသုံးပြုမှုစတာတွေကိုအဓိကထားပံ့ပိုးပေးရတာဖြစ်ပါတယ်။ ငင်းဟာအသုံးချမယ့် Software တွေကိုအသုံးပြုသူဟာ မိမိထိုင်နေတဲ့စက်မှာပင်အသုံးပြုပြီး

[illegible] File Server မှာသွားသိမ်းစေတာဖြစ်ပါတယ်။ ၎င်း File [illegible] Server တွေကို File Storage အတွက်လည်းအသုံးပြုနိုင်ပါတယ်။

[illegible]ication Server အခန်းကြောင်း

Application Server ကတော့ Client Server Application တွေကိုအသုံးပြုသူ Client တွေဘက် [illegible] Server ဘက်ကပံ့ပိုးပေးတာဖြစ်ပါတယ်။ အဲဒီအပြင်သူက ဥပမာ Database Server [illegible] လိုအပ်တဲ့ Data တွေကို Analysis လုပ်ခြင်းနှင့်ရှာဖွေမှုတွေဖြစ်တဲ့ Query Processing [illegible]ပေးတာမဟုတ်ဘဲ အဲဒီ Database ကြီးရဲ့မြောက်မြားလှစွာသော Data တွေကိုပါသိုလှောင် [illegible]ဆောင်နအဖြစ်လည်းလုပ်ဆောင်ပေးပါတယ်။ နောက်တစ်ခုက Application Serverတွေဟာ File [illegible] Server တွေနဲ့မတူညီတဲ့အချက်ကသူဟာလုပ်ငန်းတွေလုပ်ဆောင်ရာမှာလိုအပ်တဲ့ ဝန်ဆောင်မှုတွေ [illegible]ပေးမှုမက Client တွေဘက်က File and Print Services တွေကိုလည်းပံ့ပိုးပေးရပါသေးတယ်။

[illegible]unication Server အခန်းကြောင်း

အသုံးပြုသူ User တစ်ယောက်ဟာ နယ်တကာခရီးထွက်ပြီးကုန်ပစ္စည်းဖြန့်နေတဲ့လူတစ်ယောက် [illegible] အိမ်မဟုတ် ရုံးချုပ်မှပေးထားသောတာဝန်များကို အိမ်မှာပဲအလုပ်လုပ်နေတဲ့ Hone Based Worker [illegible] Modem ကိုအသုံးပြုပြီး Communication Server Network ထဲကိုဝင်ရောက်ပြီး အချက်အလက် [illegible]ပေးပို့ခြင်း၊ ဆက်သွယ်ခြင်းများပြုလုပ်လို့ရပါတယ်။ Microsoft Windows 2000 Server မှာဆိုရင် Remote Routing and Access Server (RRAS) ဆိုတဲ့တကယ့်ကိုစွမ်းအားပြည့် Communication Server ပါရှိပါတယ်။ ပြောရရင် Communication Server ဆိုတာတခြားကွန်ရက်တွေကို Modem ကနေ [illegible]ဆင့်ဆက်သွယ်မှုပြုလုပ်ပေးတာဖြစ်ပါတယ်။ နောက်ပြီး E-mail Message တွေကိုလည်းကွန်ရက်အတွင်း [illegible] Server တွေအကြား Handle လုပ်ပေးပါတယ်။

Mail Server အခန်းကြောင်း

Mail Server ကတော့ Network အတွင်းရှိအသုံးပြုသူ User တွေကိုယ်စား E-mail Message တွေကို Handle လုပ်ပေးပါတယ်။ Mail Server ဟာ Store and Forward ဝန်ဆောင်မှုကိုလည်း ပံ့ပိုးပေးပါတယ်။ ဆိုလိုတာက Server ဟာဝင်လာတဲ့ E-mail Message တွေကို User တွေဖွင့်မကြည့်ခင် သိမ်းပေး ထားရပါတယ်။ အဲဒီလိုပါပဲ ဒီဘက်ကပို့လိုက်တဲ့ E-mail Message တွေကိုတဖက်က Server

မချိတ်မိမချင်း ၎င်း Message များကိုသိမ်းပေးထားရပြီး တဖက်က Server ကိုချိတ်မိသည်နှင့် Message ကိုပေးပို့လိုက်ရပါတယ်။ ၎င်းကို Store and Forward လို့ခေါ်ပါတယ်။

Fax Server အကြောင်း

Fax Server ကတော့ Network အတွင်း Fax လမ်းကြောင်းတွေကို Manage လုပ်ပေးရပါတယ်။ ဆိုလိုတာက တယ်လီဖုန်းမှတဆင့်ဆင်လာတဲ့ Fax တွေကို Network မှာရှိတဲ့သက်ဆိုင်ရာလူတွေဆီကိုတဆင့် ပြန်လည်ဖြန့်ဝေပေးရပါတယ်။ အဲ့ဒီလိုပါပဲ Network အတွင်းမှာရှိတဲ့ အသုံးပြုသူတွေကပို့လိုက်တဲ့ Fax တွေကို Fax Server ကစုစည်းပြီးတယ်လီဖုန်းမှတဆင့် Fax တွေကိုပို့ပေးရပါတယ်။

၁.၁၅ Storage Area Network အကြောင်း

Network အကြောင်းကိုမိတ်ဆက်တင်ပြနေတဲ့ ဒီသင်ခန်းစာ(၁)မှာ နောက်ထပ်တင်ပြရမယ့် Network တစ်မျိုးရှိနေပါတယ်။ အဲ့ဒါကတော့ Storage Area Network ဖြစ်ပါတယ်။ ဒါဟာအခုနောက်ပိုင်းမှာလိုအပ်ချက်အရဖြစ်ပေါ်လာတဲ့ Network တစ်မျိုးလည်းဖြစ်ပါတယ်။ ဘယ်လို လိုအပ်ချက်မျိုးလည်းဆိုတော့ များပြားလှတဲ့ ထောင်ချီနေတဲ့အသုံးပြုသူ User တွေကသိမ်းဆည်းလိုက်တဲ့ များပြောင်လှသောအချက်အလက်တွေကိုထိန်းချုပ်ဖို့လိုအပ်ချက်ပဲဖြစ်ပါတယ်။ Storage Area Network ဆိုတာတကယ်တော့ တခြားမဟုတ်ပါဘူး။ Data နဲ့ Application တွေတည်ရှိရာ Storage System နှင့် Server အကြား High Speed Switch တစ်ခုနှင့်ချိတ်ဆက်ထားတာပဲဖြစ်ပါတယ်။ ပုံမှာပြထားတဲ့အတိုင်းပါပဲ Network ကသက်သက် SANs Components ကသက်သက်ဖြစ်ပါတယ်။ သူတို့နှစ်ခုကိုချိတ်ဆက်ပေးထားတဲ့ ချိတ်ဆက်မှုကို Side band Link လို့ခေါ်ပါတယ်။ SANs ရဲ့အဓိကရည်ရွယ်ချက်ကတော့ Network ကြီးတစ်ခုလုံးကသိမ်းဆည်းသမျှကိုတစ်နေရာထဲမှာစုပုံပြီး ဗဟိုစနစ်နှင့်သိမ်းဆည်းချင်လို့ပဲဖြစ်ပါတယ်။ အဲ့ဒီလိုသိမ်းဆည်းခြင်းဖြင့်ရရှိလာတဲ့ ကောင်းကျိုးတွေကတော့-

၁။ အလွန်လျင်မြန်တဲ့ High Speed Network နှင့် SANs ကိုချိတ်ဆက်လိုက်ပါကအချက်အလက်တွေကိုမြန်မြန်ဆန်ဆန် Access လုပ်နိုင်ပါတယ်။

၂။ သိမ်းဆည်းမှုမှန်သမျှကိုတစ်နေရာတည်းတွင် ပေါင်းစည်း၍သိမ်းဆည်းခြင်းဖြင့်အလွန်များပြားလှသော Data များကိုတစ်နေရာတည်းတွင်စုစည်းပြီးသားဖြစ်သွားသည့်အပြင် Backup လုပ်ရာ၌လည်းပိုမို အဆင်ပြေသွားသည်။

၃။ ၎င်း SANs များသည်တကယ်တော့ Disk Drive များကိုအထပ်လိုက်ချိတ်ဆက်ထားသည့် Disk Array များပင်ဖြစ်သည်။ ၎င်းစနစ် တော်တော်များများသည် Hot-Swappable ရသည်။ ဆိုလိုသည်မှာ အကြောင်းကိစ္စတစ်ခုခုကြောင့် Disk Drive တစ်ခုခုကို ဖြုတ်လို တပ်လိုပါက စနစ်များကို

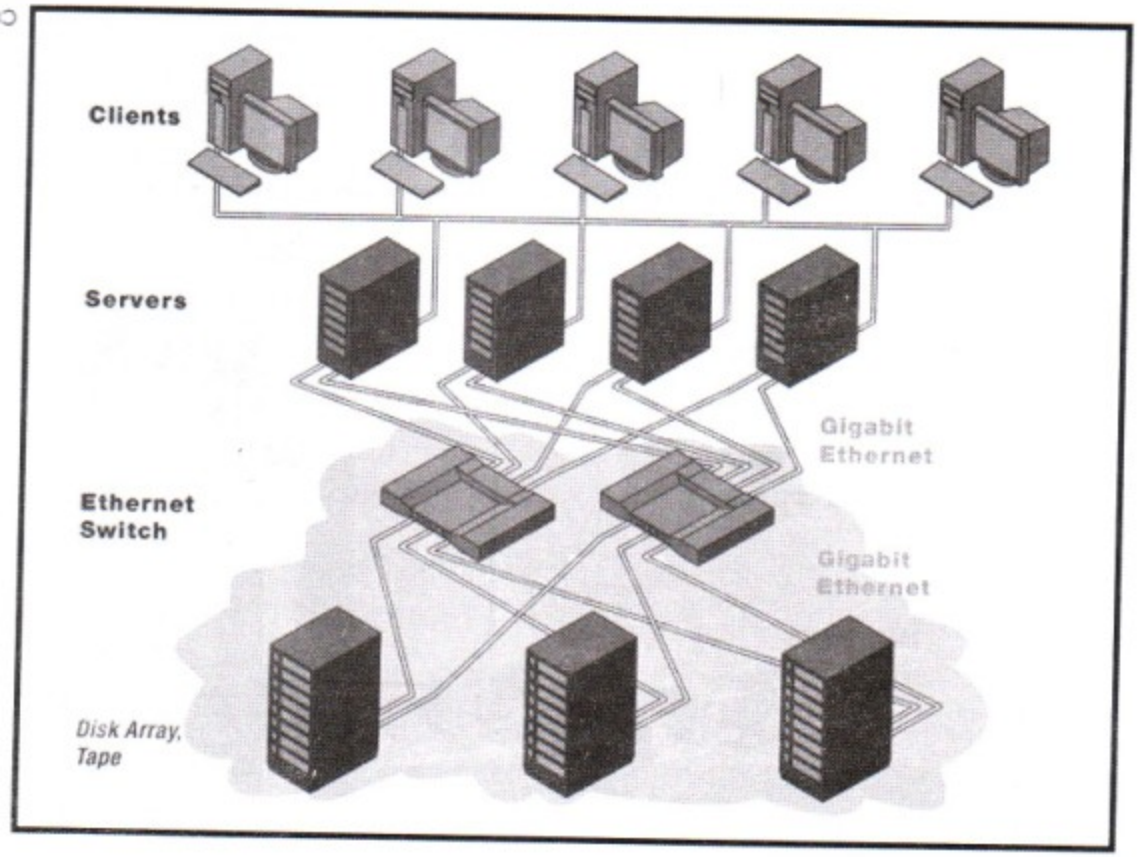
Shut Down လုပ်စရာမလိုဘဲ အလုပ်လုပ်နေစဉ်ကာလမှာပင်ဖြုတ်၊ တပ်လုပ်နိုင်သည်။

ဃ ယခုလိုတစ်နေရာတည်းတွင်အချက်အလက်များစုပုံသိမ်းဆည်းခြင်းဖြင့် နောက်ထပ်လုံခြုံရေးဆိုင်ရာစနစ်များထပ်မံရရှိလာခြင်းနှင့် Data များ Access လုပ်ခြင်းကိုထိန်းချုပ်လာနိုင်ခြင်းစသည့် ကောင်းကျိုးများကိုလည်းရရှိလာစေသည်။

ငြ အဲဒီ့အပြင်သိမ်းဆည်းမှု Data ပမာဏလျှင်မြန်စွာတိုးလာပါကလည်း စိတ်ပူစရာမလိုပေ။ အဘယ်ကြောင့်ဆိုသော် SANs သည် Storage Capacity ကိုလျှင်မြန်စွာတိုးချဲ့နိုင်ခြင်းဖြစ်သည်။

SANs ကို Storage Cluster ဟုလည်းခေါ်သည်။ SANs ကိုတပ်ဆင်ရာ၌ Server တိုင်းတွင် High Speed Network Card လိုအပ်သည်။ အဲဒီအပြင် Server မှ SANs ဆိုသည့် Storage Cluster ကိုဆက်သွယ်ဖို့ High Speed Switch လိုအပ်သည်။ SANs ဆိုသည် Storage Cluster ဘက်တွင်ဘာတွေပါဝင်သလဲဆိုတော့ အလွန်လျှင်မြန်ပြီး အလွန်စိတ်ချရသည့် Disk Array များပါရှိကြသည်။ ကြိုးမားသောအခွံအစည်း ကုမ္ပဏီတော်တော်များများသည် ယခုအခါသိမ်းဆည်းမှုနှင့် ပတ်သက်ပြီး SANs ကိုပြောင်းသုံးသောကြောင့်ပြီဖြစ်သည်။

ဇ သဘ

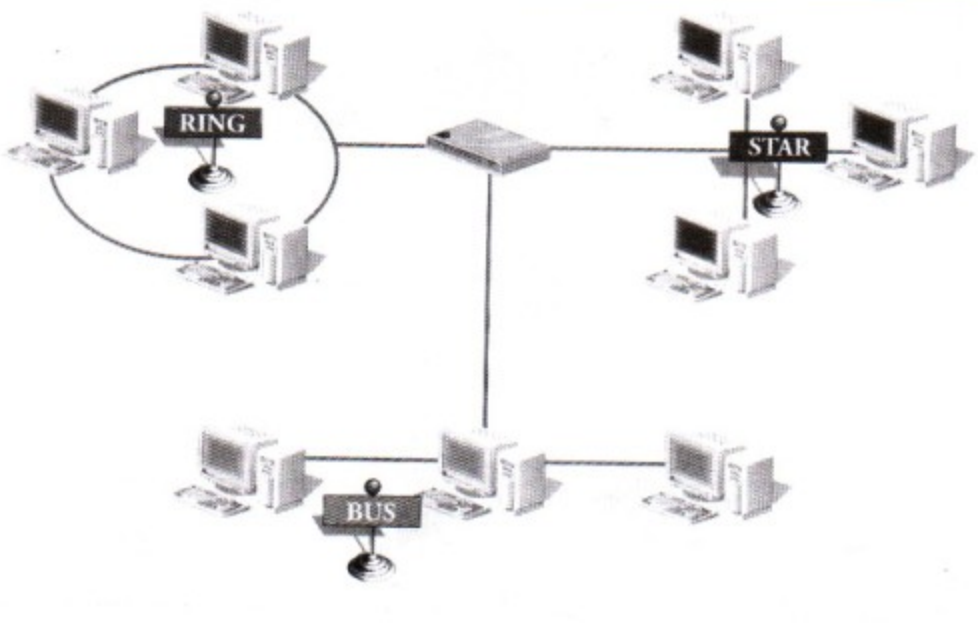


၁.၁၆ Hybrid Network အကြောင်း

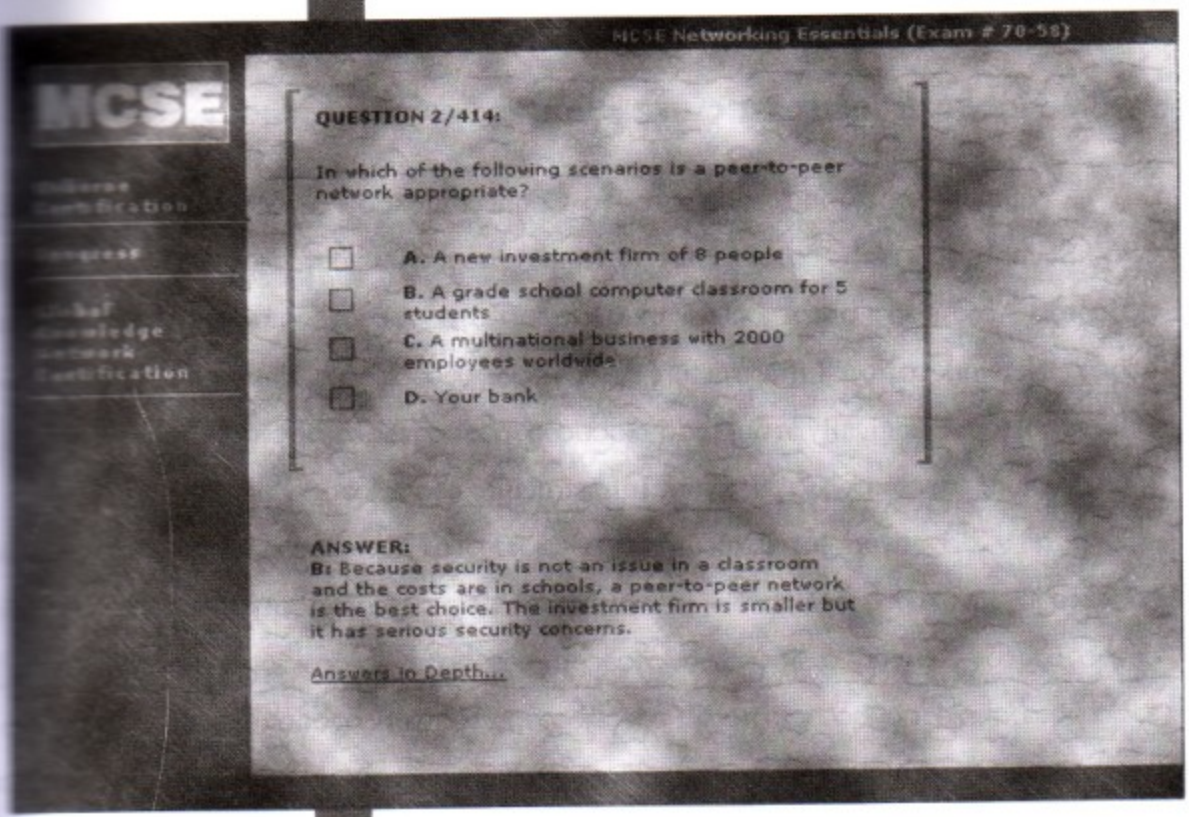
Microsoft Operating System များဖြစ်ကြသည့် Windows 98, Windows NT နှင့် Windows 2000 တို့သည်အပေါ်ကပြောခဲ့သည့် Peer to Peer Network မှာလည်းဝင်ဆန့်သည့် Client ဟုခေါ်သည့် Server Based Network မှာလည်းဝင်ဆန့်သည်။ ဆိုလိုသည်ကားရင်း Operating System များသည် Peer Network အဖြစ်တပ်ဆင်နိုင်သည့်အပြင် Server Based Network များတွင် Client အဖြစ်လည်းရပ်တည်နိုင်သည်။ ထပ်မံရှင်းပြရလျှင် Windows NT Server Version နှင့် Windows Server 2000, 20003 တို့သည် Server Operating System Function စစ်စစ်များကိုလုပ်ဆောင်ကြပြီး ခုနက ပြောခဲ့သော Operating System များမှာ Peer Network လည်းတပ်ဆင်နိုင်ပြီး Server Based Network တွင်ကြတော့လည်း Client အဖြစ်အသုံးတော်ခံနိုင်သည်။ ထို့ကြောင့်အချို့သော Network များအတွင်းမှ အချို့သော Workstation များသည် Peer to Peer Network ၏ Work Station တာဝန်ကို လုပ်နေသကဲ့သို့ တစ်ချိန်တည်းမှာပင် Server Based Network များ၏ Client အဖြစ်လည်းတာဝန်ထမ်းဆောင် နေရသည်။ ဤကဲ့သို့ ပုံစံနှစ်မျိုးရောယှက်နေသော Network မျိုးကို Hybrid Network သို့တည်းမဟုတ် Combination Network ဟုလည်းခေါ်သည်။

Hybrid Network တွေရဲ့ကောင်းတဲ့အကျိုးကျေးဇူးတွေကတော့ - မတူညီတဲ့ Topology တွေကို ချိတ်ဆက်ပေးလို့ရတယ်။

ပုံ ၁.၁၂



Hybrid Network ကိုတွေ့ရပုံ



UNIT 2

Planning, Implementing & Maintaining

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက် တစ်ခုကို တပ်ဆင်ပုံအဆင့်ဆင့်ကို လုပ်ငန်းခွင် အတွေ့အကြုံများနှင့် ရှင်းပြပေးထားပါတယ်။ စတင်စီစဉ်တာကနေ ထိန်းသိမ်းတဲ့ အဆင့်ထိ နားလည်ရလွယ်အောင် ရှင်းပြထားပါတယ်။

၂.၁ Network Infrastructure ဆိုတာ

Network တစ်ခုဖြစ်ပေါ်လာဖို့ချိတ်ဆက်မှု Connectivity တွေ၊ အဲမှမဟုတ် Network တစ်ခုရဲ့ လုံခြုံမှု Security တွေ၊ လမ်းကြောင်းချိတ်ဆက်မှု Routing တွေ၊ ထိန်းချုပ်အုပ်ချုပ်မှု Management တွေ ရယူသုံးစွဲမှု Access တွေ၊ တခြား ဒီ Network မှာပါဝင်ပတ်သက်နေတဲ့အစိတ်အပိုင်း- ငှင်းအစိတ်အပိုင်းတွေဟာ Network တစ်ခုရဲ့ Infrastructure ပဲဖြစ်ပါတယ်။ ဟုတ်ပါတယ်။ Network တစ်ခုမှာ Physically အရပဲဖြစ်စေ၊ Logically အရပဲဖြစ်စေ ပါဝင်ပတ်သက်နေတဲ့အစိတ်အပိုင်းတွေကိုငှင်း Network ရဲ့ Infrastructure တနည်းအားဖြင့် Network Infrastructure လို့ခေါ်ပါတယ်။

ကဲ အဲဆို Network Infrastructure ဆိုတာသိပြီးသွားပြီ။ တပြိုင်တည်းမှာပဲ ကျွန်တော့်ရဲ့ ကနဦးသင်ခန်းစာဟာဘာကြောင့် ဒီ Network Infrastructure အကြောင်းကိုအရင်စရင်းရလဲဆိုတာသိသွားပြီ။ ဟုတ်တယ်လေ။ Network တစ်ခုမှာပါဝင်ပတ်သက်နေတဲ့အစိတ်အပိုင်းတွေ အကြောင်းကိုသိမှ ကျန်တဲ့အကြောင်းကိုပြောကြရင်မကောင်းဘူးလား။ ဆိုလိုချင်တာက Network တစ်ခုကို Install လုပ်မယ့် Engineer တစ်ယောက်ဟာ ဒီ Network Infrastructure ဆိုတဲ့ Network တစ်ခုမှာပါတဲ့အစိတ်အပိုင်း အကြောင်းတွေကိုသိထားမှ သူဟာဘယ်လို Hardware ကိုသုံးမယ်၊ ဘယ်လို Software နဲ့လိုက်ဖက်မယ်။ ဘယ်နေရာမှာ တပ်ဆင်မယ်၊ ဘယ်လို Installation လုပ်ရမယ်။ ဘာတွေကို ဘယ်လို Configuration လုပ်ရမယ်ဆိုတာကို သူဆုံးဖြတ်လို့ရမယ်လေ။

ကဲ Network Infrastructure မှာဘာတွေပါလဲဆိုတာအကြမ်းဖျဉ်းထပ်ရှင်းပြမယ်။ ပိုပြီးနားလည်သွားအောင်လို့ပေါ့။ ကဲ Network တစ်ခုကိုစိတ်ကူးနဲ့ဆင်ကြည့်ရအောင်။ ဒီ Network Infrastructure ထဲက ပထမဦးဆုံးလုပ်ရမယ့်အပိုင်းက Design ပဲ။ Design ဆိုတာက Network ကိုမဆင်ခင်မှာ - ဒီ Network ဟာ Internet သုံးမလား။ မသုံးဘူးလားက အစပေါ့ဗျာ။ ဘယ်လို Hardware ကိုသုံးကြမလဲ။ ဘယ် Protocol ကိုသုံးကြမလဲ။ ဘယ်လို Layout ထားရှိမလဲ။ ဘယ် Operating System ကိုသုံးကြလို့ ဘယ် Application တွေတင်မလဲ စတာတွေကိုလွယ်လွယ်ပြောရရင် စာရွက်တစ်ရွက်ပေါ်ချရေးပြီး စီစဉ်ထားတာ။ ဒီအပိုင်းဟာ Design (Planning) အပိုင်းပေါ့။

နောက်တော့ဘာဆက်ဖြစ်လဲ။ ဒီလို Design လုပ်ထားတဲ့အစီအစဉ်တွေကို လက်တွေ့အကောင်အထည်ဖော်တဲ့အဆင့်ပေါ့ဗျာ။ ဒီအဆင့်ကိုတော့ Implementing, Implementation လက်တွေ့အကောင်အထည်ဖော်တဲ့အဆင့်လို့ခေါ်သဗျ။ ကျွန်တော်တို့ငယ်စဉ်ဘဝတုန်းကတော့ Design အဆင့်ကိုမလုပ်ကြဘူး။ တခါတည်းကို Implement လုပ်တော့တာ။ ဒီ Implementing မှာဘာတွေပါသလဲဆိုတော့ Design မှချမှတ်ထားခဲ့တဲ့အတိုင်းဖြစ်ဖို့ပစ္စည်းတွေဝယ်ရမယ်။ ကုန်ကျစရိတ်တွေသတ်မှတ်ရမယ်။ ပစ္စည်းတွေတပ်ဆင်ရမယ်။ ဆိုလိုတာကကွန်ပျူတာတွေ၊ ကြိုးတွေ၊ Hub တွေ၊ Switch တွေ၊ Router တွေစတာတွေကိုတပ်ဆင်ရမယ်။ ချိတ်ဆက်ရမယ်။ Printer တွေ၊ တခြားပစ္စည်းတွေတပ်ဆင် ချိတ်ဆက်မှုတွေလည်းပါတာပေါ့ဗျာ။

အဲ့သလိုနဲ့ဘာဆက်ဖြစ်သလဲဆိုတော့ - ကွန်ပျူတာတွေ၊ ပစ္စည်းတွေ၊ Hardware ပိုင်းဆိုင်ရာတွေ သူ့နေရာနဲ့သူ နေရာချပြီးပြီဆိုတာနဲ့ Operating System တို့၊ Application တို့စတင် Install လုပ်တော့တာ ပါပဲ။ ဒီနေရာမှာ Operating System ကတော့အဓိကပေါ့။ ဘာလို့လဲ ဆိုတော့ Network ချိတ်ဆက်မှုဖြစ်ပေါ် အောင် Protocol တို့၊ ဘာတို့ဆိုတာ ဒီ Operating System မှာလုပ်ရမှာကိုး။

ကဲ ဒီလို Hardware ပိုင်းဆိုင်ရာတွေလည်း သူ့နေရာနဲ့သူရှိပြီ။ Operating System တွေ၊ Software အားလုံး Install လုပ်ပြီးပြီ။ Network လည်းချိတ်ပြီးသွားပြီဆိုပေမယ့် Network Infrastructure ဟာ ပြည့်စုံသွားခြင်းမရှိသေးဘူး။ ဆိုလိုတာကကျန်သေးတယ်။ ဘာတွေကျန်သေးတာလဲ။ ဒီ Network ကြီးကို ဘယ်လို Maintenance လုပ်မလဲ။ ဘယ်လို Management လုပ်မလဲ။ ဘယ်လို Upgrade လုပ်မလဲ။ ဘယ်လို Troubleshoot လုပ်မယ်စတာတွေကျန်သေးတာပေါ့ဗျာ။ ဒီတော့ အဆင့်အားဖြင့် (၃) ဆင့် ခွဲထားတယ်ဗျ။ ဘာတွေလဲ -

(၁) Planning / Designing

(၂) Implementing

(၃) Maintenance ပေါ့ဗျာ။

ကဲဒီ (၃) ပိုင်းကိုတစ်ပိုင်းချင်းစီခွဲပြီး အနည်းငယ်ထပ်ရှင်းပြဦးအုံ့။

Planning ဆိုတာ

အင်းပြောရရင်တော့ လွယ်မလိုနဲ့ခက်ဆိုတာဒီအဆင့်ဗျ။ Network ကြီးတစ်ခုလုံးကိုဘယ်လိုတပ်ဆင် မယ်။ (Implement) တပ်ဆင်ပြီး Network ကိုဘယ်လို Maintenance လုပ်မယ်ဆိုတာတွေကိုဒီအဆင့်မှာ တစ်ခါတည်းလုပ်ပြီး Print ထုတ်ထားရမယ်။ အဲ့ဒီမှာ Network Layout တွေ၊ တပ်ဆင်မယ့် Hardware တွေ၊ ထည့်သွင်းမယ့် Software တွေ List ရှိရပါ့မယ်။ ပြောရမယ်ဆိုရင် ဒီ Network ကို Plan လုပ်တဲ့ Network Designer ဟာဒီလုပ်ငန်းရဲ့ပိုင်ရှင်ရော၊ အသုံးပြုသူရောနှစ်ဦးနှစ်ဖက်အတွက် Hardware/ Software လိုအပ်ချက်တွေ အကုန် Meet ဖြစ်နေအောင်စဉ်းစားပေးနိုင်ရမယ်။ စီစဉ်ပေးနိုင်ရမယ်။

ကျွန်ုပ်၏အတွေ့အကြုံ

ဒီ Planning နဲ့ပတ်သက်လို့ကျွန်တော့်အတွေ့အကြုံတစ်ခုပြောပြမယ်။ ဗဟုသုတအဖြစ်ပေါ့။ ဘယ်သူ့ကိုမှရည်ရွယ်တာမဟုတ်ပါ။ ကျွန်တော် ၁၉၉၈/၉၉ လောက်ကဆင်တဲ့ Network တစ်ခုအကြောင်း ပါ။ ကျွန်တော်တို့ဒီမှာက လုပ်ငန်းတစ်ခုက Network ဆင်ချင်ပြီဆိုရင် ကျွန်တော်တို့ကွန်ပျူတာလုပ်ငန်းတွေက အဲ့ဒီလုပ်ငန်းအရောက် Quotation တွေတင်ကြပါတယ်။ တစ်ဖက်လုပ်ငန်းက ကိုယ့်ကိုမရွေးမှာစိုးလို့ လိုအပ်တဲ့ Hardware ပစ္စည်းတွေကိုလည်းအကောင်းဆုံး ဒါမှမဟုတ်အသင့်တော်ဆုံးထက်ချေးသက်သာတဲ့

ပစ္စည်းကိုဦးစားပေးပြီးတင်တတ်ကြပါတယ်။ ဒါဟာအင်မတန်ဝမ်းနည်းစရာကောင်းတဲ့ကိစ္စပေါ့ဗျာ။

နောက်မှပေါ်တဲ့ပြဿနာနောက်မှရှင်းမယ်ဆိုပေမယ့် ကျွန်တော်တို့ဆီမှာက လုပ်ငန်းရှင်တွေက ကွန်ပျူတာ အကြောင်းအသေးစိတ်မသိကြသေးဘူး။ သူတို့ကသူတို့လုပ်ငန်းကိုကွန်ပျူတာဘက်ကူးပြောင်းနေချိန်မှာ ကျွန်တော်တို့က Quotation ရဖို့အဓိကထားကြတော့ နောက်ပိုင်း Hardware/Software ပြဿနာတွေတက်ပါတယ်။ တက်ရင်ဖြေရှင်းလို့ရတယ်ဆိုပေမယ့် လုပ်ငန်းကနှောင့်နှေးတာပေါ့ဗျာ။ ဒီတော့ လုပ်ငန်းရှင်ဘက်က ကွန်ပျူတာကိုသုံးဖို့စိတ်ပျက်လာတာပေါ့။ နောက်တစ်ခု ကွန်ပျူတာတစ်လုံးဝယ်ဖို့ဆိုတာ TV တစ်လုံးဝယ်သလိုမှမဟုတ်တာ။ ဒါကိုသူတို့ကမသိတော့ Quotation ခေါ်တယ်။ သင့်တော်တဲ့သူနဲ့ လုပ်လိုက်တယ်။ အဲ့ဒီလိုလုပ်တဲ့အချိန်ကျမှကျွန်တော်တို့က Planning အဆင့်ကိုကျော်လိုက်ပြီ။ Implement တမ်းလုပ်ကြတာ အဲ့ဒီအချိန်ကျမှ Planning လုပ်ရင်ပစ္စည်းအပြောင်းရွှေ့ရမယ်။ ငွေကြေးပိုလာမယ်ဆို လုပ်ငန်းရှင် (သူကိုယ်တိုင်တော့မဟုတ်ဘူးပေါ့ဗျာ။ လွှဲထားတဲ့သူတစ်ယောက်ပေါ့) ဖက်ကဘယ်လိုမြင်သလဲဆိုတော့ 'သူတို့က Quotation ရတော့မျှော်ပြောင်းတယ်' ဆိုပြီးဖြစ်မယ်။ ဒီဘက်က Site ကိုနားလည်ပေးမှာမဟုတ်ဘူး။ ဘာလို့လဲဆိုတော့ဒီမှာကခေတ်က Enter ဖြစ်ချိစဆိုတော့ ဒီလိုလွှဲထားခြင်းခံရတဲ့ပုဂ္ဂိုလ်က အဲသလောက်ထိ Knowledge ရှိချင်မှရှိမယ်။ နောက်ပြီး Director အဖွဲ့ကဒီပစ္စည်းနှင့်ဒီဈေးကိုရွေးပြီးပြီလို့ ပြောချင်ပြောမယ်။ ဒါကြောင့် ကျွန်တော်တို့ဆီမှာ Planning / Deisgn ကိုကျော်ပြီး Implement ကိုတမ်းလုပ်ကြရတယ်။ ဒီတော့ Owner / User Requirement ကို သိပ် Meet မဖြစ်ချင်ဘူး။ ဒီတော့ နောက်ပိုင်းမှာပြဿနာတွေ ပေါ်လာတတ်တယ်။ ကောင်းတာကလုပ်ငန်းရှင်ဖက်ကကိုယ်ကြိုက်နှစ်သက်တဲ့ ကွန်ပျူတာကုမ္ပဏီကို တစ်ကုမ္ပဏီချင်းခေါ်ယူပြီးဆွေးနွေးတာ အကောင်းဆုံးပါပဲ။ ပြီးမှကိုယ်ကြိုက်တဲ့ကုမ္ပဏီနဲ့ လုပ်ပေါ့။ ဒါမှလည်း Network ဆင်တဲ့ဘက်က Implement မလုပ်ခင် Planning ကိုလုပ်နိုင်မယ်။

LAN Network တစ်ခုကိုဆင်ရတဲ့ရည်ရွယ်ချက်တွေထဲမှာ – Data ကို Centralized လုပ်ပြီး Share လုပ်ကြမယ်။ ဒါအဓိကကျတယ်။ အခုဒီနေ့ခေတ်ကိုပြောတာမဟုတ်ဘူး။ အရင်တစ်ခေတ်က Security ကောင်းချင်လို့ Network ဆင်တာနည်းကြတယ်။ Confidential တွေဘာတွေကတချို့ကုမ္ပဏီတွေမှာ မတွင်ကျယ်သေးဘူး။ ဒီတော့ Network လာဆင်ပေးပါဆိုကျွန်တော်တို့ကလည်း Owner / User ကို လူကြီးမင်းတို့ ဘာဖြစ်လို့ Network ဆင်ချင်တာလဲလို့မမေးတော့ဘူး။ တကယ်ဆိုဘာအတွက် Network ဆင်တာလဲ၊ ဘာလုပ်ချင်တာလဲ၊ ဘယ်အရာကအဓိကလဲ။ ဒါတွေကိုမေးဖို့လိုပါတယ်။ Network Speed ကအစပေါ့။ နောက်ပြီး Security ကို ဘယ်လိုထိထိမိမိ အဆင့်လိုက်ဘယ်လို Cover လုပ်မလဲ။ ပြီးမှ ရလာတဲ့အချက်အလက်ကို စုစည်းပြီး Planning လုပ်ရပါတယ်။ ကဲ ဒီလောက်ဆို Planning ရဲ့အရေးပါပုံကို သဘောပေါက်လောက်ပါပြီ။ အစကောင်းမှအနှောင်းသေချာပေါ့ဗျာ။

ကျွန်တော်ဆင်ခဲ့ဖူးသော Network တစ်ခုတွင်ကြုံဖူးခဲ့သည်မှာ– အစကစပြောရရင်ဖြင့်ဇာတ်လမ်းကဒီလိုစတယ်။ Network ဆင်ဖို့အတွက်ကျွန်တော်တို့ကို ခေါ်တွေ့တယ်။ အားလုံးညှိကြတယ်။ ဒါပေမယ့် အဲ့ဒီလိုညှိတဲ့နေရာမှာ ကုမ္ပဏီရဲ့အကြီးအကဲမဟုတ်ဘဲ သူတို့လွှဲထားတဲ့တာဝန်ခံနဲ့ပဲညှိရတာပေါ့။ ကျွန်တော်

ထိုးသလောက်သူတို့ Network ဆင်တဲ့အကြောင်းရင်းကသူတို့သုံးတဲ့ Tailor Made Software က Network Version ကြီးဖြစ်နေလို့ဗျ။ ဒီတော့ကျွန်တော်လည်း အထွေအထူးပြောမနေတော့ဘူး။ တစ်ခါထဲ ဆင်တော့တာပဲ။ အဲဒီတုန်းက ၁၉၉၉ ခုနှစ်ဝန်းကျင်ဆိုတော့ ကျွန်တော့်အသက်က ၂၃ နှစ်လောက်ပဲရှိဦးမယ်။ ဒီတော့ ကျွန်တော်ရဲ့ဘဝအတွေ့အကြုံအရရော လုပ်ငန်းအတွေ့အကြုံအရရော လုပ်သက်နှံ့သေးတယ်လို့ ပြောလို့ ရတယ်။ ဆင်ရတာကြတော့ စက်ရုံကြီးဗျ။ ထားပါတော့ဗျာ အဲဒီလိုနဲ့ဆင်လိုက်ကြရော။ ကျွန်တော်တို့က သေသေချာချာ Planning မလုပ်ခဲ့ဘူးဗျ။ တကယ်တော့လုပ်ရကောင်းမှန်း မသိတာမဟုတ်ဘူး။ သူတို့က ခုနကပြောသလို ဈေးကိုပဲ ကြည့်ကြတာ ဈေးကိုကြိုက်ပြီဆိုတာနဲ့ဆင်ပေတော့ပဲ။ အဲဒီအချိန်ကျမှ ဒီလုပ်ငန်းမှာ ဒီဘာလိုတယ်လို့ ပြောပြီး ပစ္စည်းတွေထပ်တိုးရင် မင်းတို့ကဘာလို့ခုကြမှပြောသလဲဆိုပြီး ဖြစ်မယ်။ ဆိုလိုတာက Network တစ်ခုကိုဆင်တယ်ဆိုတာ လုပ်ငန်း၏ လိုအပ်ချက်ကိုသေချာစီစစ်ပြီး ဘာတွေလိုတယ်။ ဘာတွေလုပ်ရမယ်။ ဘယ်လောက်ကုန်ကျမယ်ဆိုတာကို တွက်ရတာဗျ။ ခုဟာက ဘာမှမမြင်ရဘဲ Quotation ကို Unseen တင်ရတော့တကယ်တမ်း Network ကိုဆင်လိုက်တဲ့အခါကြတော့ မကိုက်ညီမှုတွေအများကြီးဖြစ်တတ်တယ်ဗျ။ အဲဒီတုန်းကလည်းဖြစ်ခဲ့တယ်ပေါ့ဗျာ။ ပြောရရင် သုံးစွဲမှုများလာသည်နှင့်အမျှ ရက်တွေ လတွေ ကြာလာသည်နှင့်အမျှ Network ကြီးက လေးလာတယ်ဗျ။ Server ကလည်းတကယ်တော့ နိုင်နိုင်နင်းနင်း ရှိကြတာပါ။ ပိုဆိုးတာက ကျွန်တော်တို့ရှင်းပြသလောက် သူတို့နားမလည်ခြင်းပဲ။ ဘယ်လိုပဲဖြစ်ဖြစ် ကျွန်တော်တို့ ကြိုးစားတတ်မြဲတတ် အကောင်းဆုံးပံ့ပိုးပေးခဲ့တယ်။ ဒါပေမယ့်ဗျာ အဲဒီက တာဝန်ခံပြောတဲ့ စကားကတော့ သင်ခန်းစာရလောက်ပါပေတယ်။ သူပြောတာကအခုလို ကွန်ပျူတာတွေကိုကွန်ရက် ချိတ်ဆက်သုံးတာ Speed မြန်အောင်လို့ ချိတ်ဆက်သုံးရတယ်လို့ထင်ထားတာဟူ၍ဖြစ်သည်။ ကျွန်တော်ပြောချင်သည်က သူသည် ကျွန်ုပ်၏တာဝန်ခံဖြစ်၍ အစစအရာတာဝန်ယူထားရသော်လည်း အထက်က ကွန်ပျူတာကွန်ရက်ဆင်ဖို့ ပြောတယ်ဆိုရုံသာ ကျွန်တော်တို့ကိုခေါ်တွေ့ပြီး ဆင်လိုက်ရသည်။ အဘယ်သို့သောရည်ရွယ်ချက်ကြောင့် ဆင်ရသည်ကိုသူမသိပေ။ သူပြောချင်သည်က မြန်မယ်လို့ဆင်လိုက်တာ ခုကျတော့လည်း နှေးလိုက်တာ ဖြစ်သည်။ ကျွန်တော့်ဘက်က ပြန်ကြည့်တော့လည်း သူတို့က Network ဆင်ခိုင်းလို့ဆင်လိုက်တာ အကြောင့်ဆင်ရတယ်ဆိုတာကို သိမှာပဲလေဟုအထင်ရှိသည်။ ဒီတော့ နှေးတာမြန်တာကိုခရီးထား သူတို့၏ လုပ်ငန်းလိုအပ်ချက်အရ ကွန်ပျူတာတွေကို Network ချိတ်သုံးကိုသုံးမှရမည်။ နှေးသွားခြင်းသည် ပစ္စည်းက လုပ်ငန်းကိုမနိုင်ခြင်းဖြစ်သည်။ အဘယ်ကြောင့်ဆိုသော်လုပ်ငန်းသည် Data များ ဘယ်လောက် ရိုက်ထည့်ရသည်ဆိုတာကို ကျွန်တော်တို့ဘက်က ကြိုတင်မသိရှိရခြင်းဖြစ်သည်။ ထို့ကြောင့် အသိပေးလိုသည်မှာ Network ဆင်ဆိုင်းတိုင်းဘာလို့ Network ဆင်ရသလဲဆိုတာကိုတော့ သူတို့ကိုယ်သူတို့ သိမှာပဲလေဟူ၍ Network ဆင်သူဘက်မှအထင်မရှိပါနှင့်။ ကြိုတင်ညှိနှိုင်းစရာလုပ်စရာရှိတာ ပြောစရာရှိတာများကို လုပ်ငန်းမစခင်ကြိုတင် အသိပေးပြောဆိုပါလေ။

မှတ်ချက် ။ ။ နောက်ပိုင်းကြတော့ တစ်ချို့ ကိုယ်ပိုင်တဲ့ ကုမ္ပဏီတွေဆို Quotation တင်ကတည်းက တခါတည်း Planning ပါတွဲတင်ပါတယ်။ သေသေချာချာ Specification စုံလင်စွာနဲ့ Print ထုတ်ပြီးတော့ပေါ့ Network Layout တွေ၊ ဘာတွေကြတော့ Microsoft Visio Software နဲ့ ပြုလုပ်ပြီး Drawing ပုံ ထုတ်ပြီးတင်တာပေါ့။

၂.၃ Implementing ဆိုတာ

ကဲ အခု Planning လုပ်ပြီးသားကို Implement လုပ်ကြတော့မယ်။ ဒီထဲမှာဘာတွေပါဝင်မလဲ။ Cable ကြိုးတွေလိုက်တပ်ရမယ်။ Operating System တွေ Install လုပ်ရမယ်။ တခြား Software တွေလည်း Install လုပ်ရမယ်။ အဲပေမယ့်ဒီအချက်တွေကလက်တွေ့ လုပ်ငန်းခွင်မှာ Implement ဆိုတဲ့အခန်းကဏ္ဍမှာ ပါနေသော်လည်း စာမေးပွဲဖြေမည့်သူများအာရုံစိုက်ရမယ့်ကဏ္ဍတွေကတော့ -

(၁) Protocol တွေကိုဘယ်လိုရွေးချယ်မလဲ။ ဘယ် Protocol ကိုအသုံးပြုမလဲ။

(၂) ဘယ် Operating System နဲ့ ဘယ် Application ကိုသုံးမလဲ။ ဆိုလိုချင်တာက Domain မှာ တော့ Windows Server 2003 ကိုသုံးထားပေမယ့်တခြား Server တွေ၊ Client တွေမှာဘယ် Operating System ကိုသုံးမလဲ။

(၃) Owner ရော၊ အသုံးပြုသူတွေရောလိုအပ်ချက်နဲ့ကိုက်ညီမယ့် Security ကိုဘယ်လိုစီစဉ်မလဲ။

(၄) နောက်တစ်ခုက TCP/IP Protocols တွေနဲ့ပတ်သက်လို့၊ DNS တို့၊ WINS တို့၊ IPSec Protocol စသည့်နည်းပညာပိုင်းဆိုင်ရာလက်တွေ့လုပ်ဆောင်မှုတို့ပဲဖြစ်ကြပါတယ်။ ဆိုလိုချင်တာကအခုပြောတဲ့ လေးချက်က စာမေးပွဲဖြေမယ့်သူများ အာရုံစိုက်ရမှာပါ။ အဲပေမယ့် တကယ့်လက်တွေ့လုပ်ငန်းခွင်မှာလုပ်ရမှာက ဒီထက်ပိုပါလိမ့်မယ်။ ကြိုးဆင်တာတို့၊ Software တွေတင်တာတို့ပါပေါ့။ နောက်တစ်ခုက ကွန်ပျူတာတစ်လုံးကို ဘယ်လို Configuration တွေလုပ်ရတယ်ဆိုတဲ့ကဏ္ဍတွေကိုလည်း စာမေးပွဲကမေးတတ်တယ်။ ဥပမာ - Windows Server 2003 ပေါ့ဗျာ။ DNS Server Application တွေဘယ်လို Install လုပ်မလဲ။ ဘယ်လို Configuration လုပ်မလဲ စတာတွေလဲမေးတတ်ပါတယ်။

ကျွန်ုပ်၏အတွေ့အကြုံ

နိုင်ငံတကာမှာတော့ ကွန်ရက်ဆင်တဲ့အခါကြိုးတပ်တာတို့၊ ကြိုးဆင်တာတို့ကိုသက်ဆိုင်ရာ Specialized လုပ်တဲ့ကုမ္ပဏီတွေကို ခွဲဝေပေးတတ်ကြပါတယ်။ တစ်ခုတော့ရှိတာပေါ့လေ။ လုပ်ငန်းကလည်း ကြီးတာကိုး။ ဒီမှာတော့ဘယ်ရမလဲ။ မောင်ဇော်လင်းတို့ ကိုယ်တိုင်တွယ်တာပေါ့။ ကျွန်တော်တို့ဆီက EP နဲ့ပြီးထားတဲ့သူဆိုသိပ်ရှည်ရှည်ဝေးဝေးပြောမနေဘူး။ Conjute ရိုက်ခိုင်းလိုက်တာပဲ။ မီးကြိုးမရိုက်လည်း

ကျွန်ုပ်တို့ကြုံရိုက်ရတာပေါ့ဆိုပြီး သူလည်းကြုံးစားပန်းစားရိုက်တော့တာပဲ။ ဒီမှာကနိုင်ငံခြားလိုက္ခန်ပျူတာ ဆွေ ရာနဲ့ချီပြီးဆင်ရတဲ့ ရုံးခန်းအကျယ်ကြီးတွေက အများကြီးမရှိသေးဘူးလေ။ (မရှိဘူးလို့မပြောဘူးနော်) ကိုယ်တိုင်ပဲကြုံးတွေပြေးရတာပေါ့ဗျာ။ ဒီမှာကကျွန်တော်ဆင်ခဲ့ဖူးသမျှတော့ ညဖက်တွေကြီးပဲ။ လုပ်ငန်းရှင် ဆွေတာ Network ဆင်ဖို့လူသူကင်းတဲ့ ညဖက်ကိုပဲဆင်ခိုင်းတယ်။ နေ့ဖက်ဆိုသူတို့အလုပ်တွေရှုပ်နေလို့။ ဒီတော့ကိုယ့်အလုပ်မှာကတည်းကကွန်ပျူတာတွေကိုလိုအပ်တဲ့ Operating System တွေတင်ထားရတယ်လေ။ သိပ်အိုတဲ့ အရတော့ သက်ဆိုင်ရာ Site မှာကွန်ပျူတာတွေလိုက်ချ။ ကြိုးတွေတပ်၊ Operating System တွေတင်၊ Network တွေချိတ်၊ Configuration တွေလုပ်၊ Application တွေတင်စတာတွေလုပ်ရမှာ။ အခုတော့ Site ဆိုတာခင်ကတည်းကအားလုံးတင်ပြီးသား။

အလုပ်ကနေ ညနေစောင်းလောက်ထွက်သွား။ ဟိုရောက်တော့ ရုံးဆင်းဖို့ပြင်နေတဲ့ Manager (တာဝန်ခံ)ကိုအချိန်မှီတွေ့၊ သူပြောတာတွေမှတ်ထား၊ အားလုံးရုံးဆင်းသွားပြီ။ အစောင့်ပဲရှိတော့တယ်။ ကျွန်တော်တို့လုပ်ငန်းစပြီ။

- တစ်ယောက်ကသတ်မှတ်ထားတဲ့နေရာမှာကွန်ပျူတာတွေလိုက်ချတယ်။
- တစ်ယောက်ကသတ်မှတ်ထားတဲ့အတိုင်းအတာအတိုင်း ကြိုးတွေဖြတ်တယ်။ Marking တွေပေးတယ်။
- တစ်ယောက်က Trunking လိုက်ရိုက်တယ်။ ဝိုင်းကူမယ့်သူနဲ့ဆိုအားလုံးလေးယောက်။

ဒါဆိုမနက်ဆိုရင်အားလုံးပြီးပြီ။ လုပ်ငန်းပေါ်မူတည်ပြီးလူအင်အားကိုထပ်တိုးရတာပေါ့။ ဩော် တစ်ခု ကျန်သေးတယ်။ တာဝန်ခံလာရင်စစ်ဆေးစရာ၊ ပြစရာရှိတာတွေပြပြီး၊ လက်ကျန်ပိုက်ဆံလေးယူခဲ့ဖို့ (စာဖတ်ရတာပျင်းနေမှာစိုးလို့ပါ) မမေ့နဲ့ပေါ့ဗျာ။ တစ်ချို့ကုမ္ပဏီတွေကြအသုံးပြုပုံ Training တွေဘာတွေပေးရသေးတယ်ဗျ။

မှတ်ချက်။ ။ IPSec ဆိုတာ IP Security Protocol ကိုပြောတာပါ။ သူကကျွန်တော်တို့သိခဲ့ပြီးသား TCP/IP (Transmission Control Protocol / Internet Protocol) ကိုပဲ Security အရ Design လုပ်ပြီးချဲ့ထွင်ထားတာပါ။ Encrypt လုပ်ထားတဲ့ Network Layer ကို ဆက်သွယ်ဖို့ပါ။

Maintaining ဆိုတာ

Planning ကိုဦးဆုံးစလုပ်ပြီ။ ဒုတိယအဆင့်အနေနဲ့ Implement လုပ်ပြီးသွားပြီဆိုတာနဲ့ သက်ဆိုင်ရာ လုပ်ငန်းကနေဖုတ်ဖက်ချီပြီး ထပြန်လို့မရပြန်ဘူးဗျ။ Network Infrastructure ရဲ့သဘောအရ နောက်ထပ် တစ်ဆင့်ကျန်သေးတယ်။ အဲ့ဒါ Maintaining ပဲ။ အဲဒီ Maintaining အပိုင်းမှာဘာတွေပါဝင်သလဲဆိုတော့

(၁) လိုအပ်လို့ရှိရင် Operating System တွေ၊ Application တွေ၊ Update လုပ်ပေးရမယ်။

(၂) Network Traffic နဲ့လုပ်ငန်းဖြစ်စဉ်တွေကိုစောင့်ကြည့်ရမယ်။

(၃) ပြဿနာတွေကို Troubleshoot လုပ်ပြီးဖြေရှင်းပေးရမယ်။

ဒီအလုပ်တွေ အတွက် ဒီ Network Administrator ဟာ ၎င်းနည်းပညာနဲ့ပတ်သက်တဲ့ Knowledge တွေကိုအတွင်းကျကျသိထားဖို့လိုအပ်တယ်။ ဒါကတော့ လုပ်သက်နဲ့လည်းဆိုင်တာပေါ့ဗျာ။ ဒီ (၃) ချက်ထဲကပထမတစ်ချက်ကိုစပြောရရင် Network မှာသုံးနေတဲ့ Operating System တွေ၊ Application တွေကို Update လုပ်ရတာထင်သလောက်မလွယ်ဘူးဗျ။ သူတို့ Run နေတဲ့လုပ်ငန်းကြီးမထိခိုက်အောင်၊ မပျက်စီးအောင်လုပ်ဖို့လိုတယ်။ Software တွေကိုလိုင်စင်နဲ့ဝယ်ထားလို့ နောက်ဆုံးထွက်လာတဲ့ Version ကို Internet ကနေ Download လုပ်လိုက်တာကပြဿနာမရှိဘူး။ Update လုပ်တဲ့အခါမှာမမြင်နိုင်တဲ့ ပြဿနာတွေအများကြီးရှိတယ်။ လက်ရှိလုပ်ငန်းကိုထိခိုက်လို့မရတော့ ကိုယ့်မှာက Update မလုပ်ခင် သေချာစမ်းသပ်ပြီးမှပြဿနာမရှိဘူးသေချာမှ Update လုပ်သင့်တယ်။ Operating System ကို Update လုပ်လို့ရှိရင်လည်း လက်ရှိ Run နေတဲ့ Software တွေထဲမှာ Update လုပ်လိုက်တဲ့ Operating System နဲ့ မကိုက်ညီလို့ မ Run နိုင်တာမျိုးဖြစ်တတ်တယ်။ အထူးသတိထားပါလေ။

နောက်ဒုတိယတစ်ချက်က Network ကြီးတစ်ခုလုံးအလုပ်လုပ်တာ Running ဖြစ်နေတာသေချာရဲ့လား။ Smooth ဖြစ်ရဲ့လားဆိုတာ ကာလတစ်ခုပိုင်းခြားပြီးစောင့်ကြည့်နေဖို့လိုပါတယ်။ ဒီလုပ်ငန်းမှာ Microsoft Windows Server 2003 ရဲ့ Tools တွေဖြစ်တဲ့ Network Monitor ဆိုတာနဲ့ Performance Console တို့ကိုအသုံးပြုပြီး Logs တွေစစ်ဆေးရမယ်။ Network Traffic တွေ Analyze လုပ်ရမယ်။ Network Administrator ဟာဒီ Tools တွေနဲ့ရင်းနှီးနေရမယ့်အပြင် ကိုယ်ကိုင်တွယ်နေရတဲ့ Network Infrastructure နဲ့လည်းရင်းနှီးနေရမယ်။ ဒါမှလည်းပိမိရဲ့ Network ဟာပုံမှန်အလုပ်လုပ်နေတဲ့လမ်းကြောင်းကနေသွေဖီနေတယ်။ ပုံမှန်မဟုတ်တော့ဘူးဆိုတာတွေကို ဒီ Tools တွေနဲ့ ပေါင်းစပ်ပြီးသိနိုင်မယ်။

နောက်တစ်ချက်က Troubleshooting ပဲ။

ဒါလည်း Network Administrator တွေရဲ့အရေးကြီးပြီး အဓိကကျတဲ့ အလုပ်တစ်ခုပဲ။ ဘာလို့လည်းဆိုတော့လုပ်ငန်းတစ်ခုမှာ Network က Failure ဖြစ်မယ်ဆို လည်ပတ်နေတဲ့လုပ်ငန်းတွေ နှောင့်နှေးမယ်။ ထုတ်ကုန်တွေကျဆင်းလာမယ်။ လုပ်ငန်းထိခိုက်မယ်။ ကုမ္ပဏီဝင်ငွေတွေကျဆင်းနိုင်တယ်။ ဒါကြောင့်ပြဿနာဖြစ်ရင်ဘယ်နေရာမှာဖြစ်နေတယ်။ ဘယ်လိုအမြန်ဆုံး ဖြေရှင်းရမယ်။ ဒီလိုဖြစ်နေတဲ့ ပြဿနာကို အမြန်ဆုံးဖြေရှင်းနိုင်ဖို့က၊ Administrator ကဘက်စုံထောင့်စုံစဉ်းစားတတ်ရမယ်။ နောက်ပြီး မိမိလုပ်ငန်းခွင် Network Infrastructure ကိုလည်းရင်းနှီးနေရမယ်။

Maintaining နဲ့ပတ်သက်ပြီးပြောပြချင်တာက - ကျွန်တော်တို့ဆီမှာ Computer Network အကြီးအကြီးတပ်ဆင်ထားတဲ့လုပ်ငန်းတွေဆိုရင်တော့ Network Administrator တစ်ယောက်၊ ဒါမှမဟုတ် နီးစပ်ပြီးအလုပ်မှာခန့်ထားလိုက်ရင်ရတာပေါ့။ အကယ်၍ကွန်ရက် အကြီးကြီးမဟုတ်ရင်ဆက်ဆိုင်ရာလုပ်ငန်း တွေတာ Network Administrator တစ်ယောက်သီးသန့်မခန့်ထားချင်ဘူးဗျ။

ဖြစ်တော့မှ ဆင်ခဲ့တဲ့ကုမ္ပဏီတစ်ခုကို ဖုန်းဆက်ခေါ်တတ်ကြတယ်။ နောက်တစ်ခုက Maintenance Contract ဆိုပြီးအပတ်စဉ် လစဉ် Maintenance ဝင်ခိုင်းတာတွေရှိပါတယ်။ 1997 ခုနှစ်လောက်က သူငယ်ချင်းတစ်ယောက်ကြုံဖူးတာပြောပြမယ်။ အဲဒီ လုပ်ငန်းကလုပ်ငန်းအရတော့ကြီးတယ်။ ဒါပေမယ့် ကွန်ပျူတာတွေတော့အများကြီးမဆင်ထားဘူး။ ကွန်ရက်အကြီးကြီးလည်းမဟုတ်ဘူးပေါ့ဗျာ။ အဲဒီမှာ သူတာကွန်ပျူတာသမား Network လည်းကြည့်၊ တခြားကွန်ပျူတာနဲ့စာရင်းဇယားတွေလည်းဆွဲပေါ့။ ဒါပေမယ့် ခန့်ထားတဲ့ Post က Operator တော့မဟုတ်တာသေချာတယ်။ အဲဒီခေတ်တုန်းကကွန်ပျူတာသမား ဆိုတော့ စားရိက်မယ်၊ စာရင်းဇယားဆွဲမယ်လောက်ပဲသိကြတာ။ (လူတိုင်းကိုပြောတာမဟုတ်ဘူး အဲဒီရုံးက စာရင်းဌာနက ရုံးဝန်ထမ်းကောင်မလေးတွေ၊ စာရေးမလေးတွေက ဒီလူအားနေတယ်ဆိုပြီးဗလာစာအုပ်မှာ စာရင်းဆွဲဖို့ မှာထားခိုင်းရောဗျ) - Network ကသေးတော့အလုပ်လည်းဘယ်များမလဲဗျ။ နောက်ပြီး Network Administrator Post ဆိုတာလည်းသူတို့ကဘာမှန်းမသိဘဲဗျ။ ဒီကွန်ပျူတာ Network Administrator သမားခမြာ စာရေးမလေးတွေရဲ့ကူဖော်လှောင်ဖက်ဖြစ်ခဲ့ရတာပေါ့ဗျာ။ ကဲထားပါ။ လုပ်ငန်းနဲ့ ပတ်သက်တဲ့ အတွေ့အကြုံကိုပြောပြမယ်။

(၁) မထင်မှတ်တာတွေဖြစ်လာတတ်တယ်။ ပြဿနာကခက်မယ်ထင်ပေမယ့် လွယ်နေတတ်တယ်။ လွယ်မယ်ထင်နေမယ့်လည်း ခက်နေတတ်တယ်။ ဥပမာ -

CPU Fan မှာဖုံတွေဝင်နေပြီး Fan တွေရပ်နေတတ်တယ်။ CPU ကိုထိခိုက်နိုင်တယ်။

Hub ကို Power မပေးဘဲ (တနည်း) Hub ကိုမဖွင့်ဘဲ Network တွေမတက်ဘူးလို့ဖုန်းဆက်တယ်။ ဒါကြောင့်ဖုန်းဆက်ရင်ကွန်ပျူတာတစ်လုံးတည်း Network မတက်တာလား။ အားလုံးမတက်တာလား။ အားလုံးမတက်ရင် Hub ကို ဖွင့်ထား၊ မထားမေးပါ။

တခါတရံ Server Restart ဖြစ်နေတာကိုမသိတာလည်းဖြစ်တတ်တယ်။ ဥပမာ - Log File တွေကိုသူဘာသာသူ Clear မလုပ်ခိုင်းထားဘဲနေရင် Log File တွေသတ်မှတ် Size ပြည့်လာတဲ့ အခါမှာ Server မှာ Error တက်နေတာတွေ၊ Server Reset ဖြစ်ပြီး ပြန်မတက်တာတို့ဖြစ်တတ်တယ်။ ဘယ်လိုပဲဖြစ်စေ အကြောင်းအမျိုးမျိုးကြောင့် Server ပြန်မတက်ရင် ဝန်ထမ်းတွေက တစ်နေရာဗျာ။ Server ကိုသူတို့အုပ်ချုပ်သူ အခန်းထဲမှာသီးသန့်ထားလေ့ရှိတယ်။ ဒီတော့ Server ပြန်မတက်တာကို ဘယ်သူမှသတိမထားမိဘဲ Network Fail ဖြစ်တတ်တယ်။

(၂) Power Supply ဒုက္ခပေးတတ်တာကိုသတိထားပါ။ Power Supply ကလုံးဝပျက်သွားရင်ပျက်သွား၊ အကယ်၍မပျက်ဘဲ ကြောင်သွားရင်အဲ့ဒီကွန်ပျူတာကောင်းကောင်း အလုပ်မလုပ်တတ်ဘူး။ Error တစ်ခုပြီးတစ်ခုမရိုးအောင်ပေးတတ်တယ်။ ဆိုလိုတာက - Owner ဘက်က Network တစ်ခုဆင်ပြီး သွားတဲ့အခါမှာပြဿနာတစ်ခုခုဖြစ်ရင် Network ကြောင့်ဖဲလို့အပြဆင်နေတတ်တယ်။

(၃) Network ဆင်ကြတဲ့ကုမ္ပဏီတွေဟာအများအားဖြင့် Database ကိုသုံးကြတယ်။ တချို့ကတော့ Sharing လောက်ပဲသုံးကြတယ်။ Tour ကုမ္ပဏီတွေက Database တအားသုံးတယ်။ Power Failure ဖြစ်ရင် Database File တွေပျက်တတ်တယ်။ တစ်ချို့ရုံးတွေမှာ မီးအားနှင့် ပတ်သက်လို့ နှစ်လိုင်း သုံးလိုင်း ရှိတတ်တယ်။ ဘယ်လိုင်းကို Lighting သုံးပြီး၊ ဘယ်လိုင်းကိုကွန်ပျူတာသုံးဆိုပြီး ရှိတတ်တယ်။ ဒါတွေကိုလည်းဂရုစိုက်ပေးရတယ်။

(၄) တစ်ချို့လုပ်ငန်းတွေကညနေစောင်းမှ စာရင်းတွေလုသွင်းရတာမျိုးတွေရှိတတ်တယ်။ ဒီအချိန်မှာ Network Traffic ကျပ်တတ်တယ်။ အလုပ်ကများပေမယ့် စက်တွေရဲ့စွမ်းအားကို လျော့သုံးထားရင် Network Card ကို Server မှာပိုစိုက်ပြီး Loading Balance ဖြစ်အောင်လုပ်ပေးရတတ်တယ်။

(၅) Anti-Virus ကြောင့်တချို့ Program တွေ Loading အတက်မှာကြာတတ်တယ်။ လုပ်ငန်းပေါ်မူတည်ပြီး အဆင်ပြေအောင်ကြည့်လုပ်ပါလေ။

(၆) ကိုယ်ဆင်ထားတဲ့ Network မှာသုံးတဲ့ Software ဟာ Tailor Made ဖြစ်ရင်၊ ၎င်း Software ရဲ့လိုအပ်ချက်တွေကိုသိထားပါလေ။ ကြုံဖူးတဲ့အဖြစ်အပျက်တစ်ခုကိုပြောပြမယ်။ ဘယ်သူ့ကိုမှ မထိခိုက်၊ မရည်ရွယ်ဘူး။ Software ကုမ္ပဏီတစ်ခုကလူတစ်ယောက်က အဲ့ဒီလုပ်ငန်းမှာ လာပြီးပူပြင်မှုပြုလုပ်တယ်။ ဒီပူပြင်မှုရဲ့သဘောကလုပ်ပြီးရင် Restart လုပ်မှသက်ရောက်မယ်။ သူကကွန်ပျူတာကို Restart မလုပ်ရသေးဘူး။ ဒီတော့ပြောင်းလဲမှုကမဖြစ်သေးဘူး။ သူဟာကလုပ်ထားပြီးတာဘာကြောင့်ပြောင်းလဲမှုမဖြစ်ရတာလဲ။ ဒါ Network ချွတ်ယွင်းချက်ကြောင့်ဖဲ ဖြစ်မယ်ဆိုပြီးဖြစ်လာတယ်။ အပြစ်တင်ခံရဖူးတယ်။ ဒါ Restart လုပ်ရအုံးမှာလေဆိုမှ - သူမေ့နေမှန်းသိသွားတယ်။ ပညာရှိသတိဖြစ်ခဲ့ပေါ့ဗျာ။ ဒါလည်းကြုံဖူးတယ်။ ဒါဘယ်သူ့ကိုမှအပြစ်ပြောတာမဟုတ်ဘူး။ ကိုယ်က ဒီ Network မှာသုံးနေတဲ့ Software အကြောင်းကိုပါသိထားဖို့ပြောတာပါ။ ကဲ ဒီလောက်ပါပဲ။ ပြောရရင်တော့အများကြီးပေါ့။ များသောအားဖြင့်ဖြစ်တတ်တာလေးတွေကိုပြောပြတာပါ။

ကဲ ဒီလောက်ဆိုရင် Network တစ်ခုကိုတပ်ဆင်အသုံးပြုတာနဲ့ပတ်သက်ပြီး လုပ်ရမယ့်အဆင့်တွေအပြင် လုပ်ငန်းခွင်အတွေ့အကြုံတွေကိုပါ အတော်လေးသိသွားလောက်ပါပြီ။ ခု Physical and Logical Infrastructure အကြောင်းကိုဆက်လေ့လာရအောင်။

Physical and Logical Infrastructure ဆိုတာ

Network Infrastructure မှာ Physical Infrastructure နဲ့ Logical Infrastructure ဆိုပြီး ရှိ
Physical Infrastructure အကြောင်းကိုရှင်းပြပါ့မယ်။

Network ရဲ့ Physical Infrastructure ဆိုတာ Topology ကိုပြောတာပါ။ ဆိုလိုတာက အင်း
ဒီဆက်ပိုလွယ်အောင်ပြောရရင် Hardware ပိုင်းကိုပြောတာ။ ဘာတွေပါမလဲ။ ကြိုးတွေ၊ Router
Switches တွေ၊ Hub တွေ၊ Workstation တွေ၊ Server တွေစတာတွေပေါ့ဗျာ။

Logical Infrastructure ဆိုတာ Software ကိုပြောတာ။ အမျိုးမျိုးသော Software ပေါ့ဗျာ။
ပြောရရင်တော့ Network တစ်ခုကိုဘယ်လိုချိတ်မလဲ။ ဘယ်လိုထိန်းချုပ်မလဲ။ ဘယ်လိုလုံခြုံမှုကိုဖြစ်
မလဲ။ ဒါတွေကိုဖြစ်ပေါ်စေတဲ့ Software မျိုးစုံကို Logical Infrastructure လို့ခေါ်သဗျ။

တခါတရံမှာ Physical Infrastructure ကို Planning လုပ်တဲ့နေရာမှာ Logical Infrastruc-
ture ကိုမူတည်တတ်သဗျ။ ဆိုလိုချင်တာက သင်ဟာ Network ကို Ethernet နဲ့ဆင်မယ်ဆိုရင်သင်ဟာ
Ethernet နဲ့ပတ်သက်တဲ့ Hardware ပစ္စည်းတွေကိုပဲသင်ဝယ်ရမယ်။ ဒါကြောင့်သင့်ရဲ့ Physical Infra-
structure မှာဝယ်မယ့်ပစ္စည်းတွေ Plan လုပ်တဲ့နေရာမှာ တခါတရံ Logical Infrastructure ပေါ်မူတည်သွား
တတ်တယ်။ Logical ဘက်ကပြောရရင် Logical ဆိုတာ Physically အရကွန်ပျူတာတွေချထားတဲ့ Lay-
out တနည်း Topology အတိုင်း Communicate လုပ်ပေးရတာ။ ဒီ Logical မှာလည်းအခြေခံအားဖြင့်
နှစ်မျိုးရှိတယ်။

အဲ့ဒါကအတိုအကျ ဖြစ်ထည်ရှိတာနဲ့၊ အတိုအကျမရှိတာ၊ တနည်းအားဖြင့်မြင်ရတာနဲ့ မမြင်ရတာ၊
မြင်ရတဲ့အတိုအကျဖြစ်မရှိတဲ့အတွင်းသဘောက Protocol ကိုပြော။ Protocol ဆိုတာ Communication
ကို (Govern) ထိန်းချုပ်ပေးတဲ့ Software ။ မြင်ရတဲ့အပြင်ဖြစ်တည်ရှိတာကဂင်းကိုအသုံးပြုမယ့် Soft-
ware တွေကိုပြောတာ။ အကျယ်ရှင်းပြအုံးမယ်။

ဥပမာ TCP/IP ကိုသုံးမယ်။ ဟုတ်ပြီ TCP/IP က Protocol ပဲ။ အတွင်း Software ပေါ့ဗျာ။ ဒီ
TCP/IP ကိုတင်ပေးမယ့် Software တနည်းအားဖြင့် Implement လုပ်ပေးမယ့် Software ဆိုပါစို့။
Microsoft Windows Operating System တစ်ခုခု ဒါကအပြင်ပန်းအနေနဲ့မြင်ရတဲ့ Software ။ ဒါပါပဲ။
ချုပ်ပြီးပြန်ပြောမယ်။ Logical မှာ Protocol ရှိမယ်။ ဂင်း Protocol ကိုတင်ပေးမယ့် Software ရယ်
ဆိုပြီးနှစ်ခုရှိမယ်။

ဒီသင်ခန်းစာကတော့ Network တစ်ခုကိုတပ်ဆင်တဲ့နေရာမှာ အရေးကြီးပြီး အခြေခံကျတဲ့ Network Design အကြောင်းကိုလေ့လာကြရမှာဖြစ်ပါတယ်။ နောက်ပြီး Network တစ်ခုကို မဆောက်ခင်မှာ ဘာတွေ Planning လုပ်ရမယ်။ နောက်ပြီး ဘယ်လိုတပ်ဆင်ကြရမယ်ဆိုတဲ့ Implement အဆင့်၊ တပ်ဆင်ပြီးသား Network ကိုဘယ်လိုထိမ်းသိမ်းစောင့်ရှောက်ရမယ် (Maintaining) အဆင့်တွေကို သဘောတရားအားဖြင့်ရှင်းပြထားတဲ့ အကြောင်းတွေပါဝင်ပါတယ်။

Network Design ဆိုတာကျွန်တော် ခုပြောသွားတဲ့အဆင့်သုံးဆင့်ထဲက Planning အဆင့်ပဲ ဖြစ်ပါတယ်။ ဒီတော့ပထမဦးဆုံးဖြစ်တဲ့ ဒီ Network Design အဆင့်ကိုလုပ်ဖို့အတွက် ကျွန်တော်တို့တွေ့ထား Topology ဆိုတာကိုနားလည်းထားရမှာဖြစ်ပါတယ်။ Topology ဆိုတာ တကယ်တော့ အလွယ်ပြောရင် Network ရဲ့ Layout (အထိုင်ဒီဇိုင်း) ပဲဖြစ်ပါတယ်။ ဆိုလိုတာက Computer တွေအခြားသော အသုံးပြုမယ့် Resources တွေကိုဘယ်လိုချိတ်ဆက်မယ်ဆိုတဲ့ အထိုင်ဒီဇိုင်းဖြစ်ပါတယ်။ အဲ့ဒီအပြင် Topology ဆိုတာ ဒီ Network တစ်ခုမှာပါဝင်နေတဲ့အစိတ်အပိုင်း Components တွေတစ်ခုချင်းစီကို တစ်ခုနှင့်တစ်ခု ဘယ်လို ဆက်သွယ်ကြမယ် Communicate ဖြစ်ကြမယ်ဆိုတာတွေကိုပါ လုပ်ဆောင်ပါတယ်။

၂.၆ Network Topologies

ယေဘုယျအားဖြင့်တော့ Network Topologies ဟာ(၃)မျိုးရှိပါတယ်။ အဲ့ဒါတွေကတော့

(၁) Bus

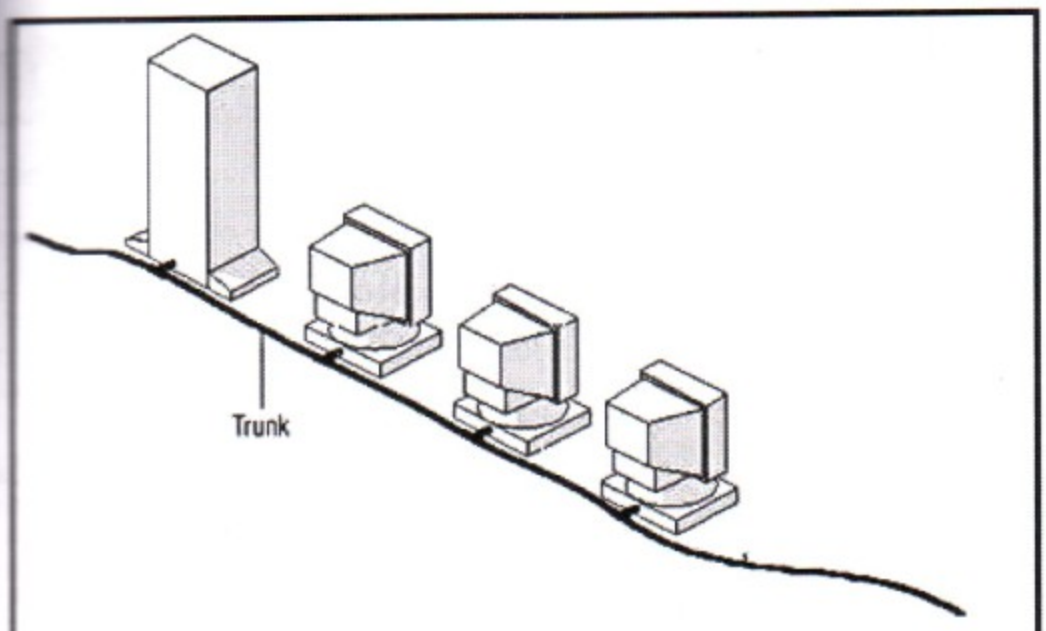
(၂) Star နဲ့

(၃) Ring တို့ဖြစ်ကြပါတယ်။

၂.၆.၁ Bus Topology

Bus Topology ဆိုတာကွန်ပျူတာကို Cable Segments တွေနဲ့ Series သဖွယ်စိတန်းချိတ်ဆက်တဲ့နည်းပညာဖြစ်ပါတယ်။ သူ့ကို Linear Bus လို့လည်းခေါ်ပါတယ်။ တနည်းအားဖြင့် ကွန်ပျူတာ ဒါမှမဟုတ် ပရင်တာ (ဆို့ပြောရင်တော့ Point ပေါ့) တွေကို Point to Point တစ်ခုမှတစ်ခုချိတ်ဆက်ခြင်း မဟုတ်ဘဲ ကွန်ရက်ကိုချိတ်ဆက်ပေးတဲ့ ကြိုးတစ်လျှောက် Point တွေအများကြီးချိတ်ဆက်ထားတာပါ။ ဒါကို Multi Point လို့ခေါ်ပါတယ်။ အခုလို Multi Point အနေနဲ့ တဆက်တည်း ချိတ်ဆက်ထားတာဆိုတော့ အကယ်၍များ ကြားခံချိတ်ဆက်ပေးတဲ့ ကြိုးသာတစ်ခုခုဖြစ်ခဲ့မယ်ဆိုရင် ကွန်ရက်တစ်ခုလုံးဟာ အလုပ်လုပ်မှာမဟုတ်တော့ပါဘူး။ ဘာကြောင့်လဲဆိုတော့ တစ်ဆက်တည်းချိတ်ဆက်ထားတာကိုး။ ဒီမှာက ကြားခံဆက်သွယ်ပေးတဲ့ ကြိုး Resistant ရှိအောင်လို့ကြိုးရဲ့ အစွန်းနှစ်ဖက်မှာ Resistor တွေရှိနေပါတယ်။ အခုလို အလယ်က

ကြိုးကပျက်နေတော့ ၎င်းကြိုးသည် Data ကိုသယ်ဆောင်ပေးနိုင်မှာမဟုတ်တော့ပါဘူး။



Bus Topology ကိုသရုပ်ပြထားပုံ

ဒါကိုဆက်လက်ပြီး အသေးစိတ်ပြောရမယ်ဆိုရင် Bus Topology ရဲ့ Bus Communication အကြောင်းကိုလေ့လာကြရမှာဖြစ်ပါတယ်။ တကယ်တော့ ဘယ်ကွန်ပျူတာမဆိုပါ။ Network ထဲမှာရှိတဲ့ ဘယ်ကွန်ပျူတာမဆိုဟာဘယ် Topology ကိုပဲအသုံးပြုထားပါစေ။ Data ဆိုတဲ့အချက်အလက်တွေကို Cable ဆွဲတစ်လျှောက် Electronic Signals တွေအဖြစ်နဲ့ ပေးပို့တာဖြစ်ပါတယ်။ ဒီတော့ ဒီ Signal အကြောင်းတွေကို ဆက်ပြီးလေ့လာရအောင်။ အဲ့ဒါတွေကတော့ -

1. Signal Sent
2. Signal Bounce နှင့်
3. Cable Termination တို့ဖြစ်ကြပါတယ်။

Sending the Signal

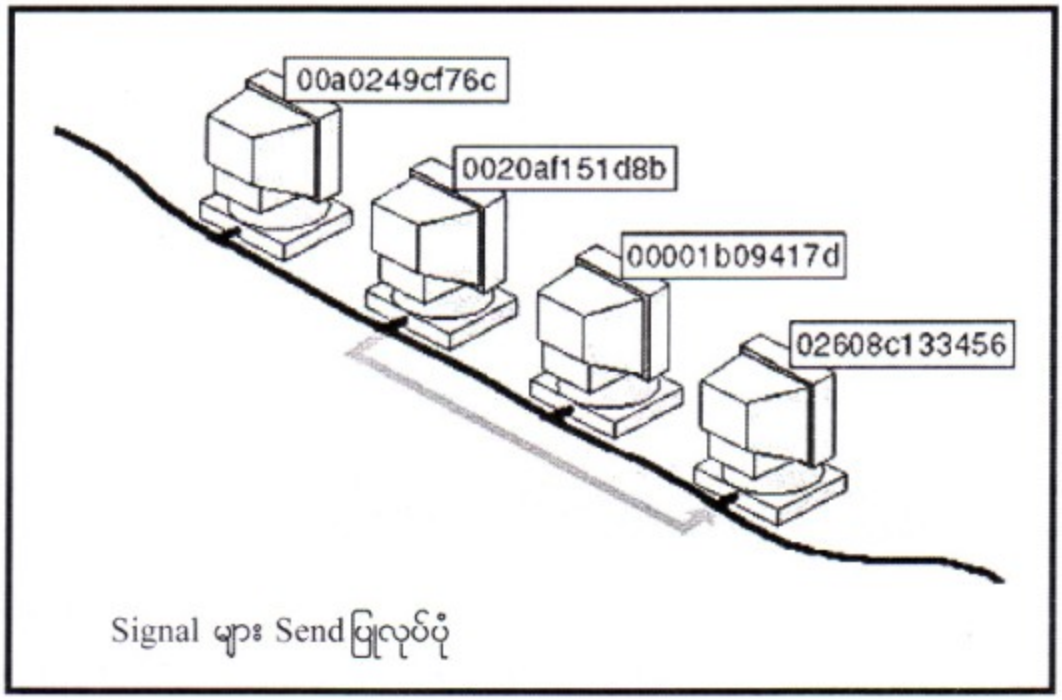
ကွန်ပျူတာတစ်လုံးကနေ Data တွေကိုပို့လွှတ်လိုက်တဲ့အချိန်မှာ Data တွေကိုအပိုင်းလိုက် ခွဲပြီးတော့ Packets အထုပ်လေးတွေအဖြစ်ပြုလုပ်လိုက်ပြီးမှ Network တစ်လျှောက် Electronic Signal အဖြစ်ပို့လွှတ်လိုက်တာဗျ။ ဒီ Signal တွေဟာ ဒီ Bus Topology ရဲ့ Backbone တစ်လျှောက်သွားလာ နေကြတဲ့အချိန်မှာ ဒီ Network မှာရှိတဲ့ကွန်ပျူတာတိုင်းဟာ အဲ့ဒီ Signal ကိုရရှိကြတယ်ဗျ။ ဒါပေသိ အဲ့လေ

ဒါပေမယ့် ဒီ Data Packets လေးမှာက သူဘယ်သူ့ဆီသွားရမယ်ဆိုတဲ့ Address လိပ်စာလေးပါတယ်ဗျ အဲ့ဒီသက်ဆိုင်သူ ကွန်ပျူတာကပဲ ဒီ Data ကိုနွေးထွေးစွာကြိုဆိုလိုက်တာပေါ့။

ပြောရအုံးမယ်။ ဒီ Bus မှာပေါ့နော်။ ကွန်ပျူတာတစ်လုံးစီကပဲ Data တွေကို တစ်ကြိမ်စီပို့လွှတ်လို့ ပါတယ်။ ဒီတော့ဗျာ ပြောရမယ်ဆိုရင် ဒီ Bus ကိုသုံးပြီး ကွန်ပျူတာတွေအများကြီးချိတ်ထားမယ်ဆိုရင် Performance ကျလာတာပေါ့။ ဘာဖြစ်လို့လဲဆိုတော့ ဟုတ်တယ်လေ။ တစ်ကြိမ်မှာ ကွန်ပျူတာတစ်လုံးပဲဆို တော့ ဒီ Network မှာအသုံးပြုသူ User တွေဟာ Transmission Time ကိုခဲ့ဝေအသုံးချနေရလို့ပါ။ တစ်ယောက်က Data တွေကိုပို့လွှတ်နေတဲ့အချိန်မှာ တခြားကွန်ပျူတာတွေက Data တွေကို ပို့လွှတ်ခွင့် စောင့်ဆိုင်းနေရတာပေါ့။ အသုံးပြုသူ User ကတော့ဘယ်သိမှာလဲ။ ဒါက နောက်ကွယ်မှာဖြစ်နေတာလေ။ ဒါကြောင့် Bus က အလုံးအရေအတွက်များလာရင် Performance ကျလာတတ်တယ်။

Network ရဲ့ Performance ကိုကျစေတတ်တဲ့ အခြားသောအကြောင်းအရာတွေလည်းရှိသေး တယ်ဗျ။ အဲ့ဒါတွေကတော့ အဲ့ဒီကွန်ရက်မှာချိတ်ထားတဲ့ကွန်ပျူတာတွေကိုကပဲ နိမ့်နေလို့လား၊ Data အပို့အလွှတ်အသွားအလာများနေလို့လား အသုံးပြုနေတဲ့ Software ကပဲနဂိုကတည်းကနေးလို့လား။ နောက် Network မှာသုံးထားတဲ့ Network Cable အမျိုးအစားချိတ်ဆက်ထားတဲ့ ကွန်ပျူတာတွေရဲ့တစ်လုံးနှင့် တစ်လုံးအကွာအဝေး စတာတွေပေါ့ဗျာ။ ဒီတော့ကျွန်တော်တို့ဟာ Network ကို Planning လုပ်နေတဲ့ အချိန်မှာဘယ် Topology ကိုသုံးမလဲဆိုတာအပြင် ဒါတွေပါထည့်စဉ်းစားဖို့လိုအပ်ပါတယ်။

ပုံ ၂.၂



Signal များ Send ပြုလုပ်ပုံ

Passive Topology နှင့် Active Topology

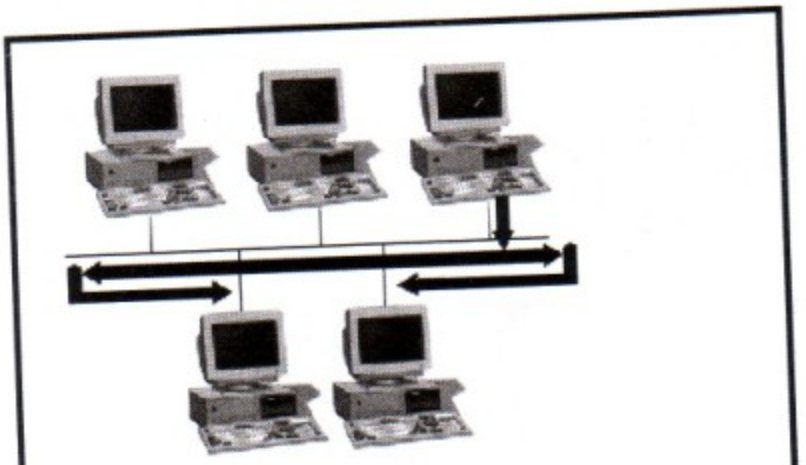
Bus Topology နဲ့ပတ်သတ်ပြီးနားလည်ထားရမယ့် နောက်ထပ်အချက်တစ်ခုရှိပါတယ်။ အဲဒါကတော့ Bus Topology ဟာ Passive Topology ဖြစ်ပါတယ်။ Passive Topology ဆိုတာဒီလိုဗျ ဒီ Bus Topology နှင့်ချိတ်ဆက်ထားတဲ့ ကွန်ပျူတာတွေဟာ ဘယ်ကွန်ပျူတာကတော့ဖြင့် Data တွေပို့လွှတ်လိုက်ပြီဆိုတာကိုပဲ လက်ခံဖို့အတွက်အသင့်ရှိနေကြတယ်။ Data တွေကို ကွန်ပျူတာတစ်လုံးမှနောက်ကွန်ပျူတာတစ်လုံးသို့ Data တွေရွေ့လျားစေဖို့ လုပ်ဆောင်ခြင်းအလျဉ်းမရှိကြပါဘူး။ ဒီကြောင့်မို့ အကယ်၍များကွန်ပျူတာတစ်လုံးလုံးကများ Fail ဖြစ်သွားခဲ့ရင် ဒီလိုဖြစ်မှုဟာ Network ကြီးကိုသွားပြီးမထိခိုက်ပါဘူး။ (Computer Fail ဖြစ်ရင်လို့ပြောတာနဲ့ Cable Segment Fail ဖြစ်ရင်လို့ပြောတာ မဟုတ်ပါ)

Active Topology ကြတော့ သူနှင့်ဆန့်ကျင်ဘက်ဗျ။ Network တစ်ခုအတွင်းမှာရှိတဲ့ကွန်ပျူတာတွေဟာသူတို့ဆီရောက်လာတဲ့ Signals တွေကို Regenerate ပြန်လုပ်ပေးရပါတယ်။ ပြောရမယ်ဆိုရင် Data တွေဟာ ကွန်ပျူတာတစ်လုံးကနေ နောက်တစ်လုံးကိုသွားဖို့အတွက် သူတို့မှာတာဝန်ရှိတယ်လို့ပြောချင်တာပ။

Signal Bounce

အကယ်၍ Bus Toplology မှာ Cable တွေကို Termination လုပ်မထားရင် Signals တွေဟာ Bus Topology မှာ Network ရဲ့ကြိုးရှိသလောက်တစ်ဖက်စွန်းမှ နောက်တစ်ဖက်စွန်းထိ သွားလာလှုပ်ရှားကြရပါတယ်။ ဒီတော့အခြားကွန်ပျူတာကနေ Data တွေကို Send လုပ်မရဘူးဖြစ်နေတာပေါ့။ ဒါကြောင့် သူတို့ဟာ Network တစ်လျှောက်ရွေ့နောက် Bouncing ဖြစ်နေကြပါတယ်။ ဒါကိုပဲ Signal Bounce လို့ခေါ်တာပါ။ Signals တွေဟာသူတို့ရည်ရွယ်ရာနေရာကိုရောက်ရှိသွားမှရပ်သွားမှာဖြစ်ပါတယ်။ ဒါကြောင့် ဒီလိုရောက်ရှိသွားဖို့ Signal Bounce မဖြစ်စေဖို့ Cableတွေကိုအစွန်းတစ်ဖက်ဆီမှာ Terminate လုပ်ပေးရပါတယ်။

ပုံ ၂-၃



Signal Bounce ဖြစ်နေပုံ

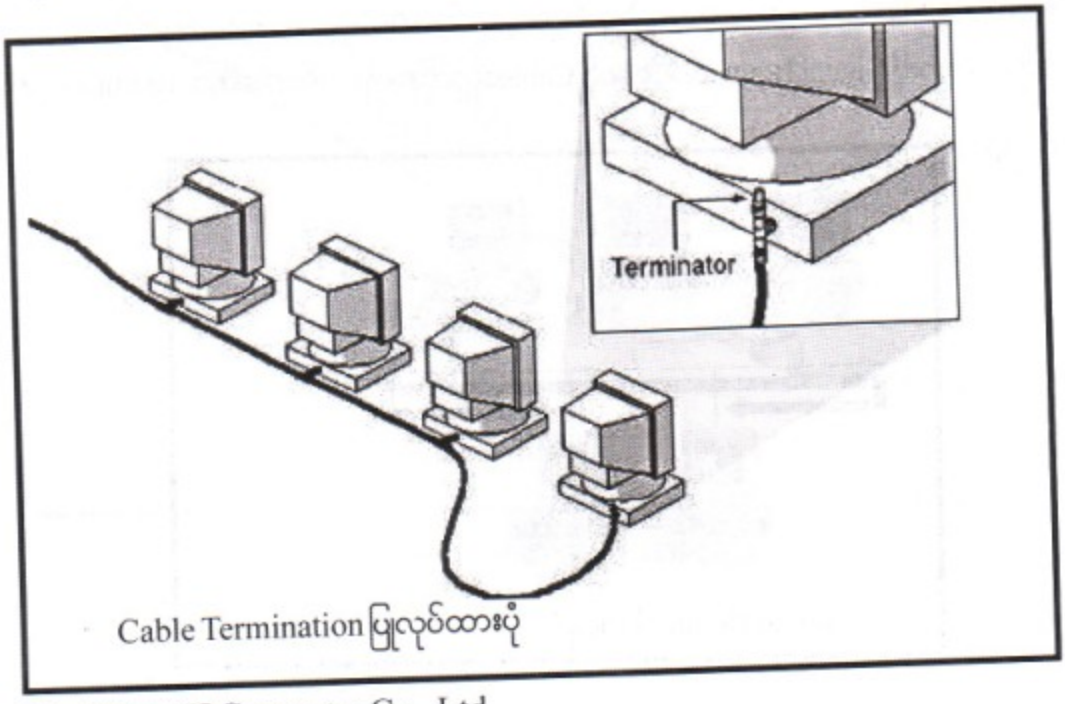
Cable Termination

Cable Termination ဆိုတာရှေ့မှာလည်းပြောခဲ့ပါတယ်။ ကြိုးတွေမှာရှိတဲ့ Resisitance ကို တစ်ဖက်အစွန်းတွေဆီမှာ သက်ဆိုင်ရာကြိုးရဲ့ Resistance နှင့်ညီမျှတဲ့ Resistor ကို Terminator အဖြစ်ပိတ်ပေးထားရပါတယ်။ အဲ့မှလည်းခုနက Signals Bounce အရပြန်ပြောရရင် Signal တွေဟာအဆုံးကိုတွေ့မှာပေါ့။ အဆုံးကိုတွေ့မှ စုန်ချည်ဆန်ချည် သွားနေတာရပ်မှာပေါ့။ အဲ့ဒီလိုအဆုံးအစွန်းကို မတွေ့လို့စုန်ချည်ဆန်ချည် ဖြစ်နေတာကို Signal Bounce ဖြစ်တယ်ခေါ်တာ။ ဒီတော့ Signal Bounce ဖြစ်နေရင် တခြားကွန်ပျူတာတွေက Data တွေကိုမပို့လွှတ်နိုင်ဘူးဖြစ်နေတာပေါ့။

ဒီတော့ တစ်ဖက်တစ်ချက်မှာရှိနေကြတဲ့ Resistor / Terminator တွေဟာ သူတို့ဆီကို/ အစွန်းဆီကို ရောက်လာတဲ့ Signals တွေကိုသိမ်းဆည်းလိုက်ပါတယ်။ ဒီလိုသိမ်းဆည်းလိုက်ခြင်းဖြင့် Network ကြိုးတစ်လျှောက် Signal တွေ Clear ဖြစ်သွားပါတော့တယ်။ ဒီတော့မှ နောက်ထပ် Signal Sending ထပ်ဖြစ်တာပါ။ အဲကြောင့်မို့ Bus Topology မှာပွင့်နေတဲ့အဆုံးဆိုတာမရှိစေရဘူး။ ရှိနေရင် Terminator ပိတ်ပေးထားရတယ်။ အဲဒီလိုမပိတ်ထားရင်အဆုံးကို Signal တွေမရောက်ရှိတဲ့ Signal Bounce ဖြစ်နေတတ်တယ်။ Signal Bounce ဖြစ်နေရင် Data Send လုပ်လို့မရတော့ဘူး။ ကြိုးတစ်လျှောက် Signal Clear ဖြစ်နေမှ Data Send လုပ်ကြတယ်။ ဒီတော့ Signal Bounce ဖြစ်နေရင် Sending လုပ်မယ့်ကွန်ပျူတာတွေမှာ Data တွေဟာ ပြူတစ် ပြူတစ်ဖြစ်နေကြတယ်။ 'ဟာ ဟိုကောင် တိုဖက်လျှောက်လိုက် ဒီဖက်လျှောက်လိုက်နဲ့ သူရှိနေတာနဲ့ ငါတို့သွားလိုရာမရောက်တော့ဘူး။ သူ့ကိုထိန်းသိမ်းမယ့် Terminator ကိုရှာလို့မတွေ့ဘူးဖြစ်နေတယ်ကွ' အဲဆို တစ်နေရာရာမှာ Open Connection ဖြစ်နေလို့ပေါ့။

အဲဆို Communication မဖြစ်နိုင်တော့ဘူး။ အဲကိုပဲ Network Fail ဖြစ်တယ်လို့ခေါ်တယ်။ ဥပမာ

ပုံ ၂.၄

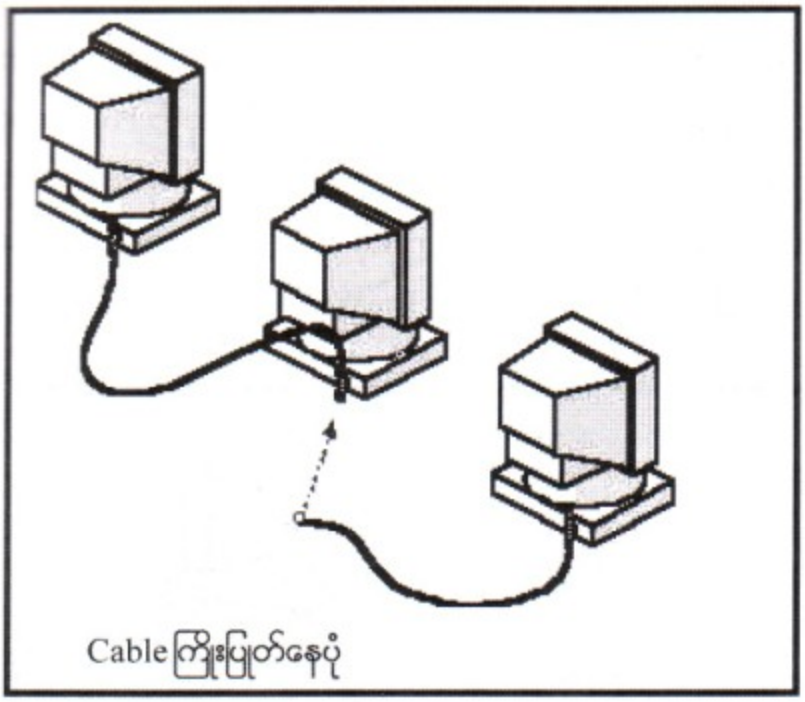


Cable Termination ပြုလုပ်ထားပုံ

ကွန်ပျူတာတွေကိုအိမ်မှာဆင်ထားတယ်။ ဘုံဘိုင်မှာ၊ ဘောစင်မှာ၊ ရေအိမ်မှာ ခေါင်းလှည့်လိုက်ရင် အဲဒီမယ့် ခေါင်းကိုမတပ်ဘဲထားရင် ရေတွေထွက်ကျကုန်မှာပေါ့။ အဲကြောင့် သုံးသည်ဖြစ်စေ၊ ရေပိုက်ခေါင်းမှာအပိတ်ရှိရမယ်။ မဟုတ်ရင် Communication မဖြစ်ဘူး။

Failure

အားလုံးရှိများ Bus Topology မှာ Network ကြိုး Segment တစ်ခုဟာ ခေါင်းမမှိလို့ပဲဖြစ်ဖြစ်၊ ကြိုးလို့ ပေါက်လို့ပဲဖြစ်ဖြစ်ပေါ့။ အဲဆိုခုနကလို ရေပိုက်ပေါက်ပါပြီ။ Communication Failure တစ်ကြိုးမကောင်းတာနဲ့ Netwrok ကြိုးတစ်ခုလုံး Failure ဖြစ်ပြီ ဖြစ်ပါတယ်။ အဲဟာ တကယ့်ကို အားနည်းချက်တစ်ခုပါပဲ။ မှတ်ထားပါ။ Cable Failure ဖြစ်ရင် Terminator မတပ်ထားရင်ဘယ်လိုပဲဖြစ်ဖြစ် အချက်ပြမတွေ့ရင်၊ ပွင့်နေရင် Signal Bounce ဖြစ်ပါတယ်။ Signal Bounce ဖြစ်ရင် Communication ပြတ်တောက်ပါတယ်။



Cable ကြိုးပြုတ်နေပုံ

Bus Topology ရဲ့ ကောင်းတဲ့အချက်တွေကတော့

(၁) ကြိုးရဲ့အလျားကုန်ကျမှုနည်းတယ်။ ကြိုးနည်းနည်းပဲလိုတယ်ပေါ့ဗျာ။

(၂) ကြိုးတပ်ဆင်ရလွယ်ကူတယ်။ ကြိုးတန်ပိုးကလည်းချေးမကြီးဘူး။

(၃) ကွန်ပျူတာတွေကိုတပ်ဆင်ရတာလည်းလွယ်ကူတယ်။ Bus Topology မှာမှ Thinnet ကိုအသုံးပြုမယ်ဆိုရင်တော့ Sector တွေထပ်တိုးရတာလည်းလွယ်ကူတယ်။

(၄) ကွန်ပျူတာတစ်လုံး Failure ဖြစ်ရုံနဲ့ Network ကြီးတစ်ခုလုံးကျမသွားနိုင်ဘူး။

Bus Topology ရဲ့ ပေကောင်းတဲ့အချက်များ

(၁) ကွန်ပျူတာ (Point) အရေအတွက်များလေ Performance ကျလေဖြစ်ပါတယ်။

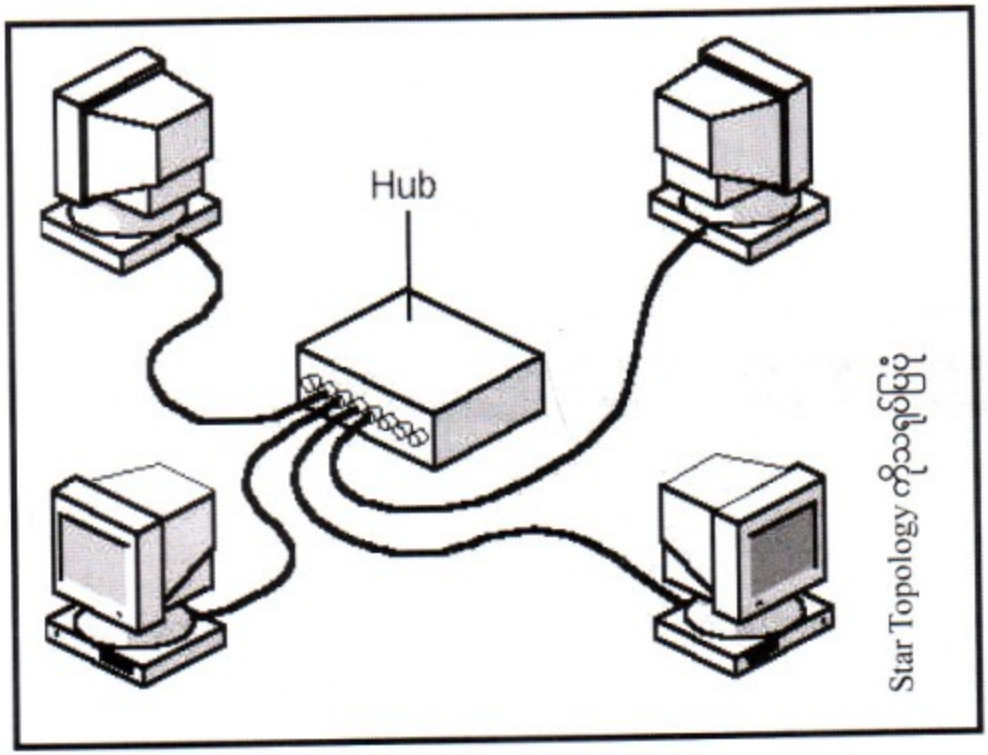
(၂) Cable တစ်ပိုင်း Failure ဖြစ်တာနဲ့ Network ကြီးတစ်ခုလုံးကျသွားတယ်။

(၃) Cable ဘယ်နေရာမှာ Failure ဖြစ်နေသလဲဆိုတာကို လိုက်ရှာရတာ လက်ပေါက်ကပ်ပါတယ်။

၂.၆.၂ Star Topology

Star Topology ဆိုတာ Bus Topology လိုတစ်ဆက်တည်းချိတ်ဆက်ထားတာမဟုတ်ဘဲ ကွန်ပျူတာ တစ်လုံးချင်းစီက သီးခြားကြိုးတစ်ကြိုးစီအသုံးပြုပြီးတော့ Hub လို့ခေါ်တဲ့ Central Point ဆီကို ချိတ်ဆက်ထားတဲ့ကွန်ရက်ကိုပြောတာဖြစ်ပါတယ်။ အခုလိုချိတ်တာကို Point to Point Connection လို့ပြောတာပါ။ ဒီလို Point to Point ချိတ်မှတော့ ချိတ်ရတဲ့ကြိုးပမာဏက Bus Topology ထက်တော့ပိုပြီးပေါ့။ ဒါပေမယ့် ကြိုးတွေ ပိုကုန်လို့ ကုန်ကျစရိတ်များတယ်လို့ အပြစ်တင်မစောပါနဲ့အုံး။ သူက Point တစ်ခုချင်းစီကို ကြိုးတစ်ကြိုးစီယူထားတာဆိုတော့ အကယ်၍များ အဲ့ဒီကြိုးကတစ်ခုခုဖြစ်သွားရင် အဲ့ဒီသက်ဆိုင်ရာ Point ပဲ Connection ပြတ်ပါတယ်။ သူတစ်ခုပဲဒုက္ခရောက်ပါတယ်။ ကျန်တဲ့ Point တွေကိုတာမှထိခိုက်ခြင်းမရှိပါဘူး။ ဆိုလိုချင်တာက Bus Topology လိုကွန်ရက်ကြိုးတစ်ခုလုံး Break Down ဖြစ်မသွားပါဘူး။

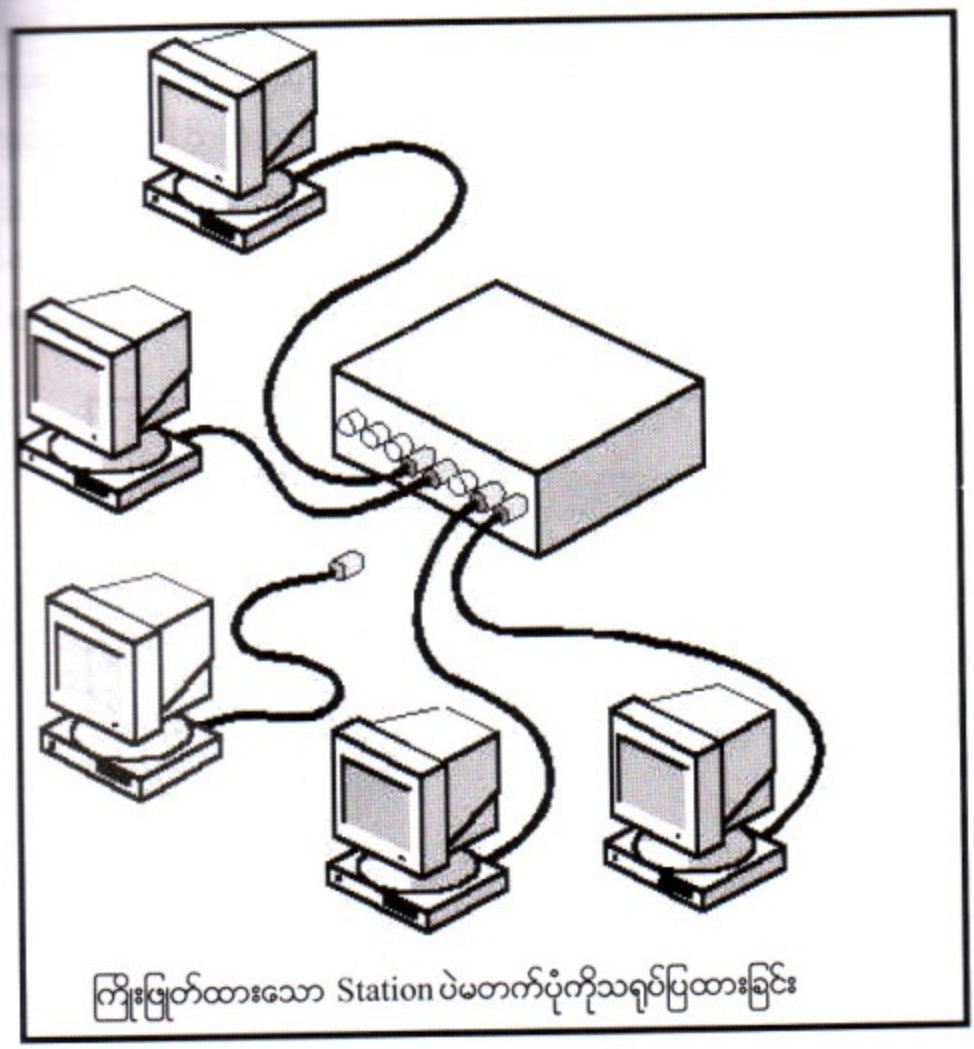
ပုံ ၂.၆



[illegible] အပြစ်ရှာဖွေရတာ အင်မတန်လွယ်ကူပါတယ်။ ကဲ သင်ဘာကိုရွေးမလဲ။
[illegible] ဒီမှမဟုတ် သင့်အိတ်ထဲက ငွေကြေးအခြေအနေကိုကြည့်မလား။
[illegible] ဆောင်းကျူးဆိုးကျိုးဆိုတာ ရှိလို့နေပြန်ပါတယ်။ ဒီကတော့ နေရာတိုင်းမှာအကောင်းကြီး
[illegible] သူ့ရဲ့ကောင်းကျိုးဆိုးကျိုးတွေကိုဆက်လက်လေ့လာရအောင်။

[illegible]တွေတော့ - အပြစ်ရှာရတာလွယ်ကူတယ်။ ကြိုးလေးတစ်ကြိုးပျက်ရုံနဲ့ ကွန်ရက်ကြီး
[illegible]ကို မထိခိုက်နိုင်ဘူး။ Connection လုပ်ရတာလည်းလျှင်မြန်တယ်။

[illegible]တွေကတော့ - ကုန်ကျစရိတ်ကကွန်ရက်ကြီးလာတာနဲ့အမျှပိုလာမယ်။ ကြိုးလေးတစ်ကြိုး
[illegible]ကွန်ရက်ကြီးတစ်ခုလုံးမထိခိုက်နိုင်ဘူးဆိုပေမယ့် အကယ်၍သာ Hub တစ်ခုခုဖြစ်သွားရင်
[illegible] ကွန်ရက်ကြီးတစ်ခုလုံးကို ထိခိုက်သွားနိုင်ပါတယ်။



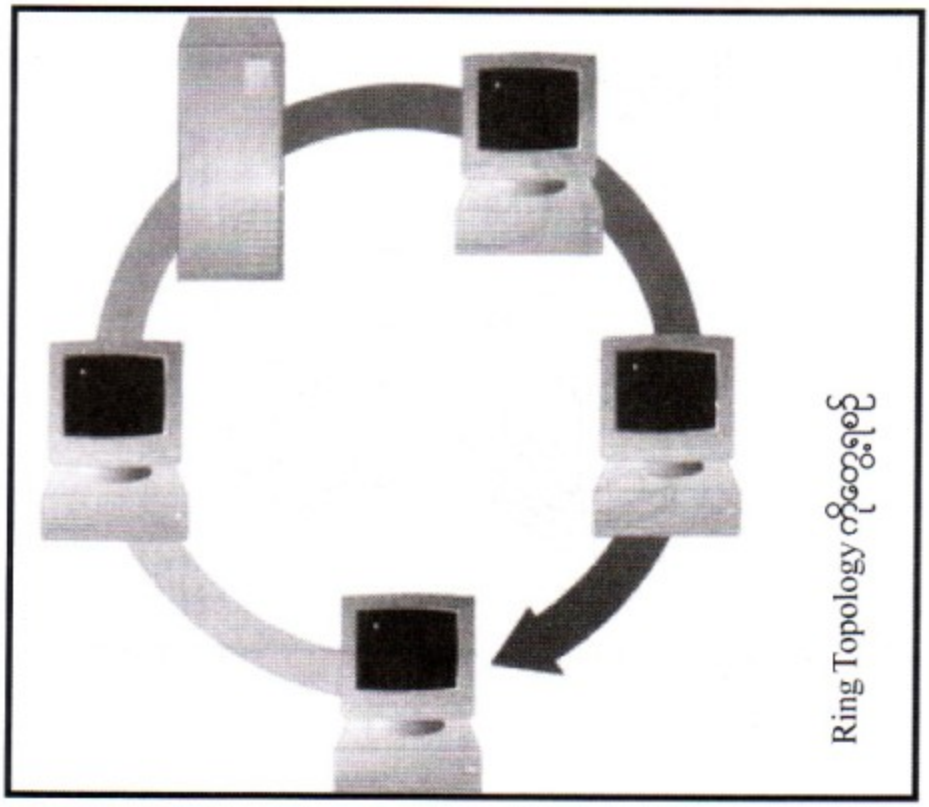
ကြိုးဖြတ်ထားသော Station ပဲမတက်ပုံကိုသရုပ်ပြထားခြင်း

ကွန်ရက်တွေမတက်လို့လာကြည့်ပေးပါအုံးလို့ ဖုံးဆက်တိုင်းမေးရမှာက ကွန်ရက်ကြိုးတစ်ခုထဲမတက်တာလား။ ကွန်ရက်ထဲကတစ်လုံးပဲမတက်တာလားဆိုတာကိုပါပဲ။ အကယ်၍ကွန်ရက်ကြိုးတစ်ခုထဲမတက်ဘူးဆိုရင် ဒီ Star Topology တွေမှာ ဖြစ်တတ်တာက Hub ကို Power မဖွင့်မိခြင်း သို့မဟုတ် Power Fail ဖြစ်နေတာကိုမသိခြင်းတို့ကြောင့် Hub အလုပ်မလုပ်နိုင်ဖြစ်ကာ Network ကြိုးတစ်ခုထဲ Failure ဖြစ်နေတတ်ပါတယ်။

၂.၆.၃ Ring Topology

Ring Topology ဆိုတာ Signals တွေဟာ ဦးတည်ရာတစ်ဖက်တည်းကို စက်ဝိုင်းလိုလှည့်ပတ်ကာသွားလာနေတဲ့သဘောကိုပြောတာဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင်တော့ စက်ဝိုင်းပုံတစ်လျှောက် ကွန်ပျူတာများကိုချိတ်ဆက်ထားရတာဖြစ်ပါတယ်။ စက်ဝိုင်းလိုဖြစ်နေတာကြောင့် သူမှာ အစဆိုတာလည်းမရှိသလို အဆုံးဆိုတာလည်းမရှိပါဘူး။ နောက်ပြီး Terminator တွေလည်းမလိုအပ်တော့ပါဘူး။ ကွန်ပျူတာတိုင်းဟာ သူ့ထံသို့ရောက်လာတဲ့ Data Packet လေးတွေကို သူတို့ဘယ်အထိသွားရမယ်ဆိုတာကို ကြည့်ပြီးထပ်ဆင့်ပို့ပေးရပါတယ်။ ဒါကြောင့် Point တိုင်းမှာ Receiver လည်းရှိပါတယ်။ Transmitter လည်းရှိပါတယ်။ Point တစ်ခုဟာ သူ့မတိုင်ခင် Point ဆီကပို့လွှတ်လိုက်တဲ့အချက်အလက်တွေကို လက်ခံရပြီး၊ နောက် Point တစ်ခုကို ပြန်လည်ပို့လွှတ်ရတာကြောင့်ပါ။ စဉ်းစားကြည့်ပါ။ အဲ့ဒီ Ring မှာ Point တစ်ခု Failure ဖြစ်သွား

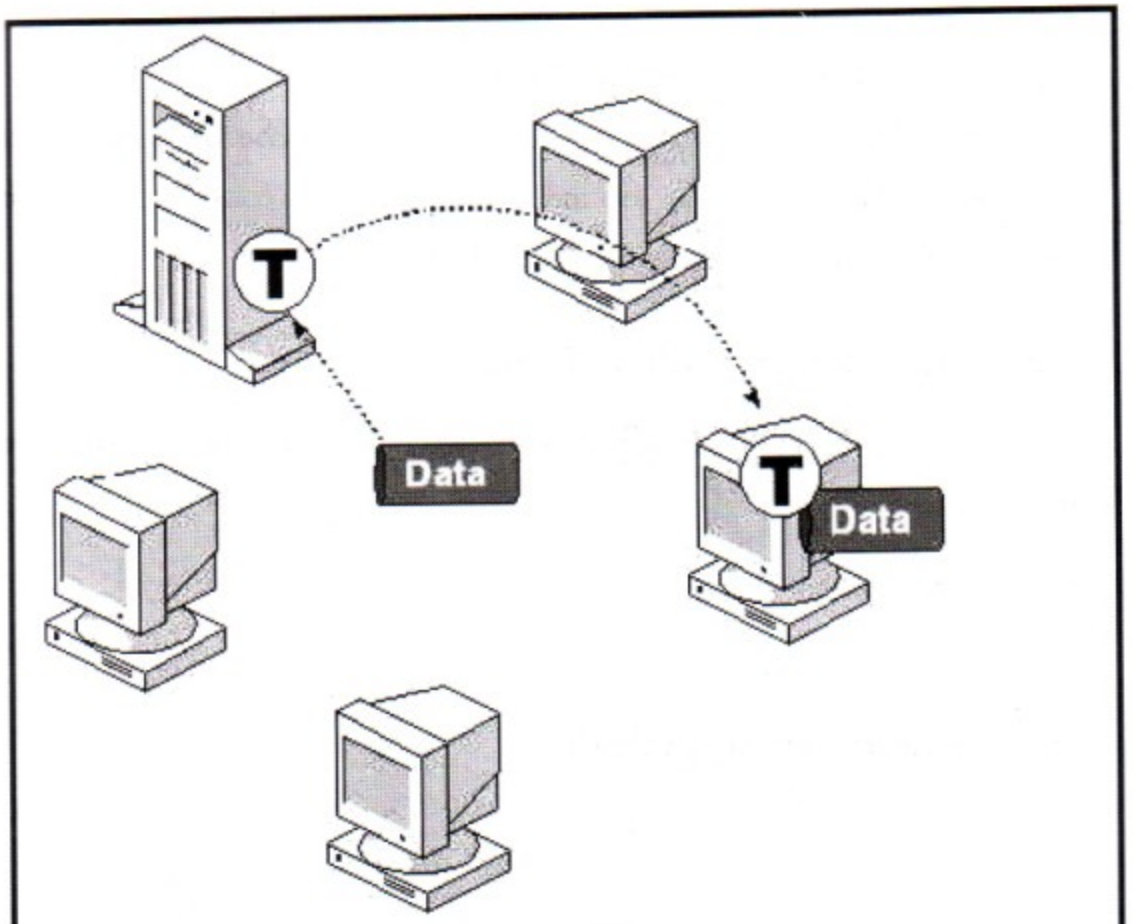
ပုံ ၂.၈



Ring Topology ကိုတွေ့ရစဉ်

Ring တစ်ခုလုံး Network Down သွားမှာပါ။ အဲဒီလိုအချက်တွေကြောင့်ပါပဲ။ ကွန်ရက်ဆင်တော့မယ် Ring ကိုမရွေးချယ်ကြပါဘူး။ ဒါကြောင့်လည်း ကွန်ပျူတာကွန်ရက်လောကမှာ Ring Topology တွဲ့ကွန်ရက်ကိုသိပ်မတွေ့ရတာပါဘဲ။ သူမှာလည်း ကောင်းတဲ့အချက် ဆိုးတဲ့အချက်ရှိတယ် ဆိုပေမယ့် အချက်ကနည်းပြီး မကောင်းတဲ့အချက်ကများနေပါတယ်။ ကွန်ပျူတာတစ်လုံး Failure ဖြစ်သွားတာနဲ့ Network တစ်ခုလုံး Failure ဖြစ်သွားတတ်တယ်။

ဒီနေရာမှာ Token Passing ဆိုတဲ့အကြောင်းလေးကို အနည်းငယ်ပြောပြလိုပါတယ်။ Token Passing ဆိုတာ Data ကို Sending လုပ်ရာမှာ Ring (စက်ဝိုင်း) သဖွယ် အလုပ်လုပ်ပေးနေတာဖြစ်ပါတယ်။ အဲဒီတော့ Token ဆိုတာ Data Packet အသေးလေးတစ်ခုပါပဲ။ သူက ကွန်ပျူတာတွေကို တစ်လုံးချင်း ဖြတ်သွားလည့်ပတ်ပေးနေတာဖြစ်ပါတယ်။ အကယ်၍ကွန်ပျူတာတစ်လုံးလုံးဟာ အချက်အလက်တွေကို ပေးပို့ချင်ပြီဆိုရင် ၎င်းက အဲဒီ Token လေးကို Modifies လုပ်လိုက်ပါတယ်။ ကိုယ်ပို့ချင်တဲ့ Data နဲ့ Address (ရည်ရွယ်ရာ) ကိုထည့်ပြီး လှည့်လိုက်တာပေါ့ဗျာ။ အဲဒီအခါကျမှ ပို့ရမယ့်အချက်အလက်တွေဟာ Ring သဖွယ်လှည့်ပတ်သွားလာနေကြရာ ရည်ရွယ်ရာကို မရောက်မချင်းပါဘဲ။ ဒါမှမဟုတ် ပေးပို့သူဆီ ပြန်မ ရောက်မချင်းပါပဲ။ အဲဒီလိုနဲ့အချက်အလက်ဟာ ရည်ရွယ်ရာကိုရောက်သွားပြီဆိုပြန်တော့လည်း အဲဒီ လက်ခံရရှိ



Ring Topology တွင် Token Passing ဖြစ်နေပုံ

သူက သူလက်ခံရရှိပြီးကြောင်းကို တစ်ခါပြန်ပြီး Message ပြန်ပို့လိုက်ပြန်ပါတယ်။ Sender ဆီကိုပဲ Message ပြန်ပို့တယ်ဆိုတာ လူကလုပ်နေတာမဟုတ်ဘူးနော်။ သူ့ဘာသာသူလည်ပတ်နေတာ။ အဲဒီလို လည်ပတ်နေတာဖြစ်ပါတယ်။

Ring Topology က Ring သာပြောတယ်။ လူတွေကစက်ထိုင်းပုံထိုင်နေရမှာ မဟုတ်ဘူး။ ကြိုးတပ်ဆင်တာတော့လည်း Star ပုံစံတပ်ဆင်ရတာပါ။ Central Hub က Token ကို Virutal Ring အနေနဲ့လှည့်ပတ်စေတာဖြစ်ပါတယ်။

IBM Token Ring Network တွေမှာတော့ Ring ကို Single Ring အဖြစ်အသုံးပြုပြီး Fiber Distributed Data Interface (FDDI) မှာတော့ Ring ကိုအပိုထားရှိဖို့ရယ် မြန်ဆန်အောင်ဆိုပြီး Dual Counter-Rotating Ring ကိုအသုံးပြုပါတယ်။ ပုံမှန် Single Ring ကတော့ အကယ်၍များပေါ့ ဒီ Ring ထဲကကွန်ပျူတာတစ်လုံး Fail ဖြစ်သွားတာနဲ့ Network ပါ Failure ဖြစ်သွားမယ်။ Dual Ring ကတော့ ပြဿနာမရှိဘူးပေါ့။ ခုနောက်ပိုင်း Modern ဖြစ်တဲ့ Ring Topology တွေဟာ Smart Hub ဆိုတာကို အသုံးပြုကြပါတယ်။ သူက Ring ထဲမှာ ကွန်ပျူတာတစ်လုံး Failure ဖြစ်ရင်ငင်းကို Ring မှဖယ်ထုတ်ခြင်းဖြင့် Network Failure ဖြစ်မှုကိုကာကွယ်ပေးပါတယ်။ နောက်ပြီးကွန်ပျူတာတွေက Data Send လုပ်ခြင်းကို မျှမျှတတ ဖြစ်အောင်လုပ်ပေးပါတယ်။ ဆိုလိုတာကကွန်ပျူတာ တစ်လုံးတည်းကနေပဲ Data တွေပို့နေလို့ ကျန်တဲ့ကွန်ပျူတာတွေမပို့ရ မဖြစ်ရလေအောင်ပေါ့။

နောက်ပြီး အဲဒီ Ring မှာလှည့်ပတ်တဲ့ Token လေးက လည်ပတ်နှုန်းတအားမြန်တာဗျ။ ဘယ်လောက်တောင်မြန်သလဲဆိုရင် ဥပမာ မီတာ ၂၀၀ အလျားရှိတဲ့အရှည်ကိုပေါ့ တစ်စက္ကန့်အတွင်းမှာအချိန် ၁၀၀၀ ပတ်နိုင်ပါတယ်။ ကဲ Hub အကြောင်းဆက်လေ့လာရအောင်။

၂.၇ Hubs အကြောင်းသိကောင်းစရာ

Hubs တွေကို တနည်းအားဖြင့် Wiring Concentrators လို့ခေါ်ပါတယ်။ Hubs သုံးမျိုးရှိပါတယ်။ အဲဒါတွေကတော့

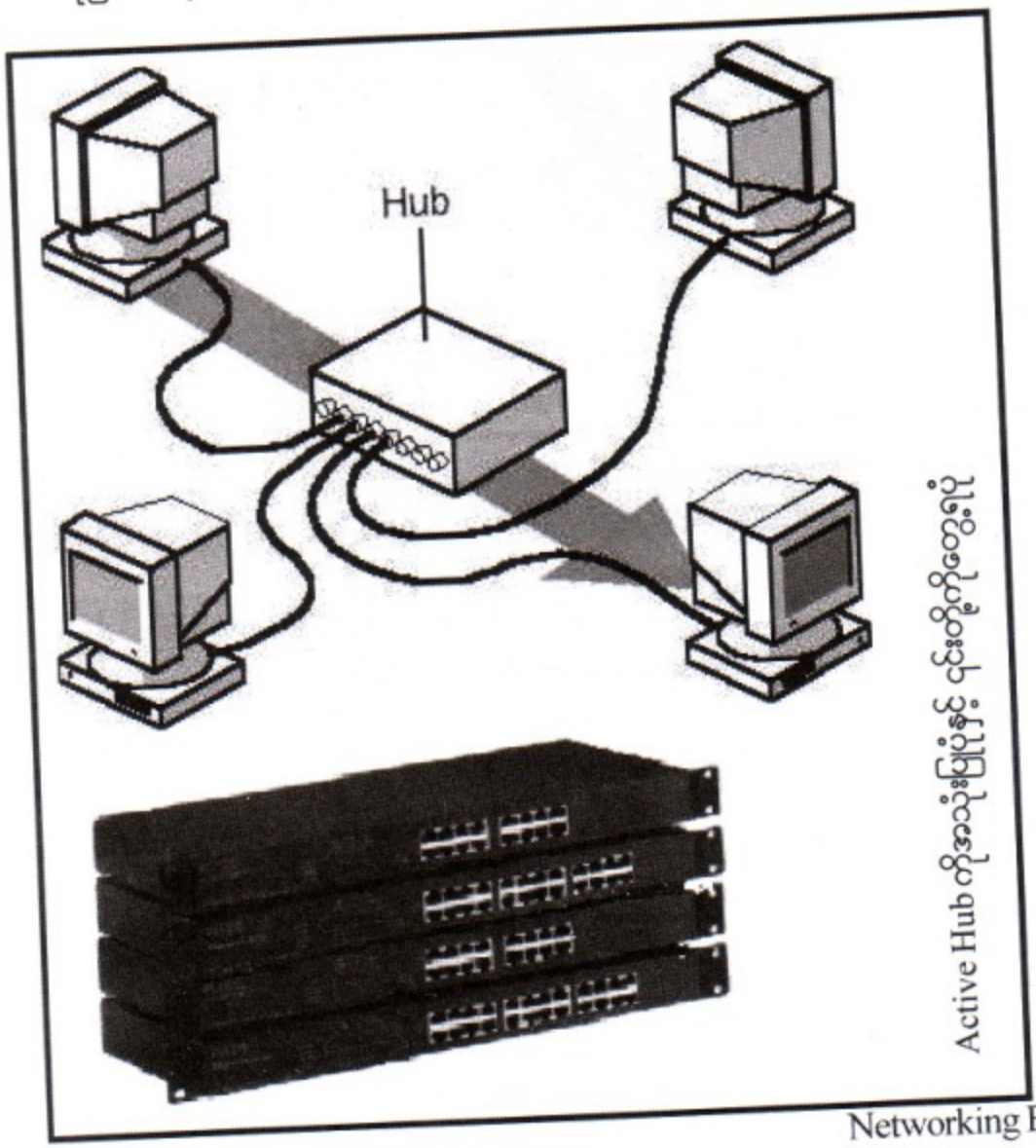
(၁) Active Hubs

(၂) Passive Hubs နဲ့

(၃) Intelligent Hubs တို့ပဲဖြစ်ပါတယ်။

Active Hubs အကြောင်းသိကောင်းစရာ

Active Hubs ဆိုတာကွန်ရက်ထဲမှာ ကွန်ပျူတာတွေတနည်းအားဖြင့် Node တွေကိုအချင်းချင်း ချိတ်ဆက်တာဖြစ်ပါတယ်။ Node တွေနဲ့သီးခြားစီရှိနေတဲ့ Cable ကြိုးတွေဟာဒီ Active Hubs မှာဗဟိုချက် အနေနဲ့ လာရောက်တွေ့ဆုံတပ်ဆင်ရမှာဖြစ်ပါတယ်။ သူဟာ Electronic Singals တွေကို Amplify လည်း လုပ်နိုင်ပါတယ်။ Clear လည်းလုပ်ပါတယ်။ Signal တွေက Clean လုပ်ပစ်လိုက်တဲ့ Process ကိုတော့ Signal Regeneration လို့ခေါ်ပါတယ်။ Signal Regeneration လုပ်ခြင်းကြောင့် အကျိုးကျေးဇူးနှစ်ခုရှိ ပေါ်တယ်။ အဲဒါကတော့ Signal Regeneration လုပ်ပြီးတဲ့အခါ Signal တွေဟာ Robust ပေါ့။ ပြန်အား ကောင်းလာတယ်။ သန်မာလာတယ်ပေါ့။ အဲဒီတော့ Error တွေသိပ်မပါဝင်တော့ဘူးပေါ့။ တနည်းအားဖြင့် Error တွေကို Less Sensitive ဖြစ်သွားတာပေါ့။ နောက်တစ်ခုက Note တစ်ခုနဲ့တစ်ခုကြား သွားနိုင်တဲ့ အတွာအဝေးကိုလည်း တိုးမြှင့်သွားနိုင်ပါတယ်။ ဒါကြောင့် Active Hubs တွေဟာ အခုပြောပြမယ့် Passive Hubs ထက်ပိုပြီးအရေးပါတယ်။



Active Hub တို့အသုံးပြုပုံနှင့် ၎င်းတို့ကိုတွေ့ရပုံ

Passive Hubs အကြောင်းသိကောင်းစရာ

Passive Hubs ဆိုတာ သူ့မှာ ဘာ Electric Component မှမပါပါဘူး။ နောက်ပြီး Data Signal တွေနဲ့ပတ်သက်လို့ Active Hubs လို ဘာ Process မှလည်းမလုပ်ဘူး။ ဒီတော့ Passive ဆိုတာ Work-station တွေမှာ Cable ကြိုးတွေကို ၎င်းသို့လာရောက်ချိတ်ဆက်ခြင်းဖြင့် Electrical Connection လုပ်ပေးခြင်းသက်သက်ဖြင့်သာ သုံးသည်။ Passive Hubs ဟာ Active Hubs လို လျှပ်စစ်ပါဝါ မလိုအပ်ပါ။ သူဟာ Data Signals တွေကို Clean-up မလုပ်တဲ့အပြင် Amplified လည်းမလုပ်ပါ။ ARCnet Network တွေမှာ Passive Hubs ကို အသုံးပြုလေ့ ပြုထ ရှိပါတယ်။ Token Ring Network တွေဟာလည်း Passive Hubs ကို အသုံးပြုလေ့ ပြုထ ရှိပါတယ်။

ပုံ ၂.၁၁

BNC ခေါင်းနှင့် Passive Hub ကိုတွေ့ရပုံ

Hybrid Hubs

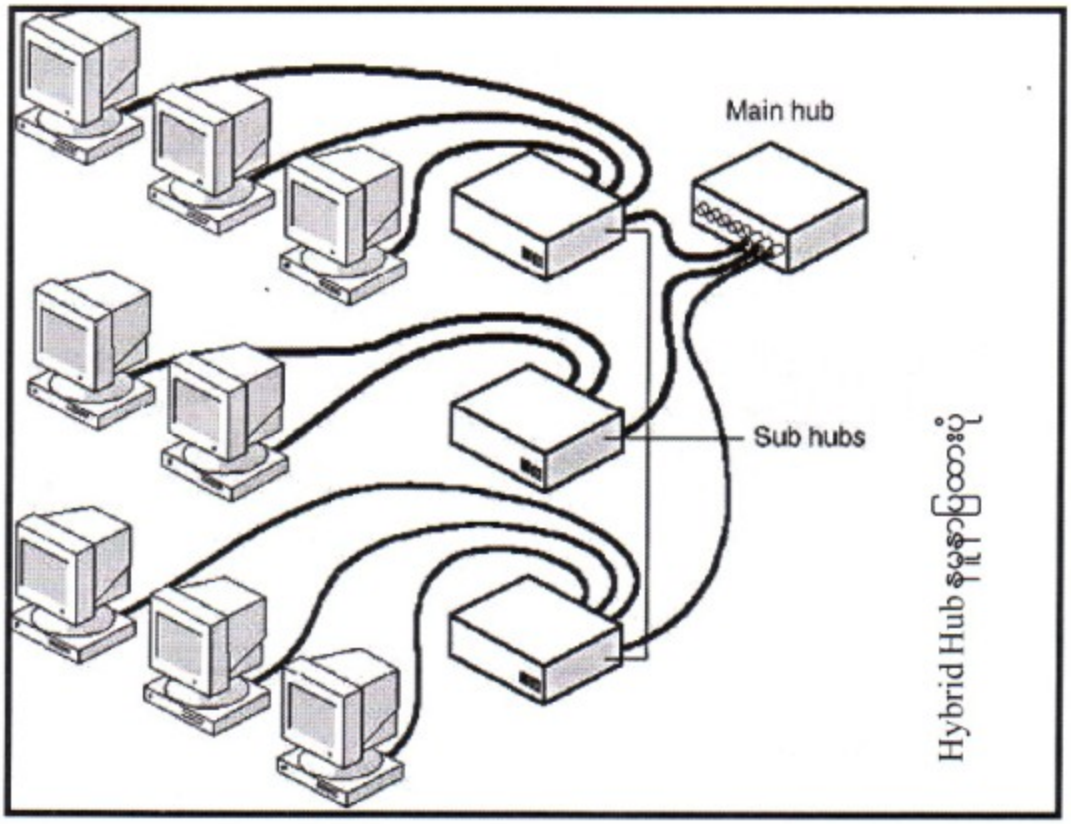
မတူညီတဲ့ Cables အမျိုးအစားတွေကိုအတူတကွချိတ်ဆက်တဲ့အခါမှာ အသုံးပြုပါတယ်။ Hybrid Hubs တွေရဲ့ကောင်းတဲ့အကျိုးကျေးဇူးတွေကတော့ - မတူညီတဲ့ Topology တွေကိုချိတ်ဆက်နိုင်ရတယ်။ Network ရဲ့ Effeciency ကိုမြင့်တက်စေပါတယ်။

၁၉၉၇ ခုနှစ်ကတည်းက ပြောခဲ့တာပ

အမှန်တကယ်တတ်ကျွမ်းလိုသူတိုင်းအတွက် **YOUTH Computer Centre**

Produced by YOUTH Computer Co., Ltd

ပုံ ၂.၁၂



Hybrid Hub နမူနာပြထားပုံ

၂.၈ Switch အကြောင်းသိကောင်းစရာ

Switching Hub ဆိုသည်မှာ Hub တွေရဲ့နောက်ဆုံးပေါ်နည်းပညာနဲ့ ဖွဲ့စည်းတည်ဆောက်ထားခြင်းဖြစ်ပါတယ်။ Switching ရဲ့သဘောတရားကတော့ Signals တွေကို အလွန်လျင်မြန်စွာနဲ့ လမ်းကြောင်းတွေလွှဲပေးနိုင်တာဖြစ်ပါတယ်။ သူဟာ Data Packet လေးတွေကို ၎င်း Hub မှာရှိတဲ့ Ports တွေအားလုံးဆီကို မသွားစေဘဲ Data Packets လေးကို လိုအပ်တဲ့ သက်ဆိုင်ရာ Computer ဆက်သွယ်ထားတဲ့ Portsတစ်ခုတည်းကိုပဲ ရောက်ရှိစေပါတယ်။

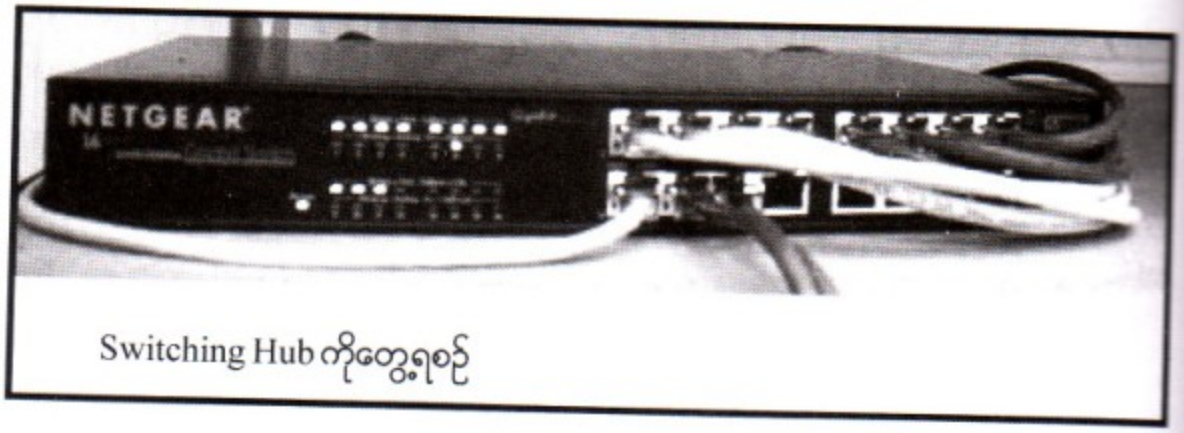
Switching Hub တွေဟာ သူနဲ့ချိတ်ထားတဲ့ Connection တွေရဲ့ Address ကိုဇယားတစ်ခုအဖြစ် မှုလုပ်ပေးထားပါတယ်။ ၎င်းဇယားကို MAC Addresses Table လို့ခေါ်ပါတယ်။ MAC ဆိုတာ Medium Access Control Layer ပါ။ အဲ့ဒီ ဇယားထဲမှာ ၎င်း Hubs နဲ့ချိတ်ဆက်ထားတဲ့ Connection တွေရဲ့ Address ရှိနေတာကြောင့် Station နှစ်ခု Communicate လုပ်တဲ့နေရာမှာ သူဟာမြန်ဆန်စွာလုပ်ဆောင်နိုင်တာဖြစ်ပါတယ်။

Hub Vs Switch

Station ဟာ Data တွေကို Switching Hub ဆီပို့လွှတ်လိုက်ပါတယ်။ ၎င်း Data တွေဟာ

Switching Hub ဆိုကိုရောက်လာတဲ့အထိကတော့ ယခင်သာမန် Hub တွေလိုပါပဲ။ ဒါပေမယ့် Switching Hub ဟာ Data တွေကိုရလာတဲ့အခါ ၎င်း Hub ရဲ့ Port အားလုံးကို Data တွေထပ်ဆင့်ပို့လွှတ်ခြင်း မလုပ်ဘဲ MAC Addresses Table မှာရှိတဲ့ Address တွေကိုသွားရောက်ကြည့်ရှုပြီး သက်ဆိုင်ရာ Port တွေဆီကို Data တွေ ပို့လွှတ်လိုက်ပါတော့တယ်။

ပုံ ၂.၁၃

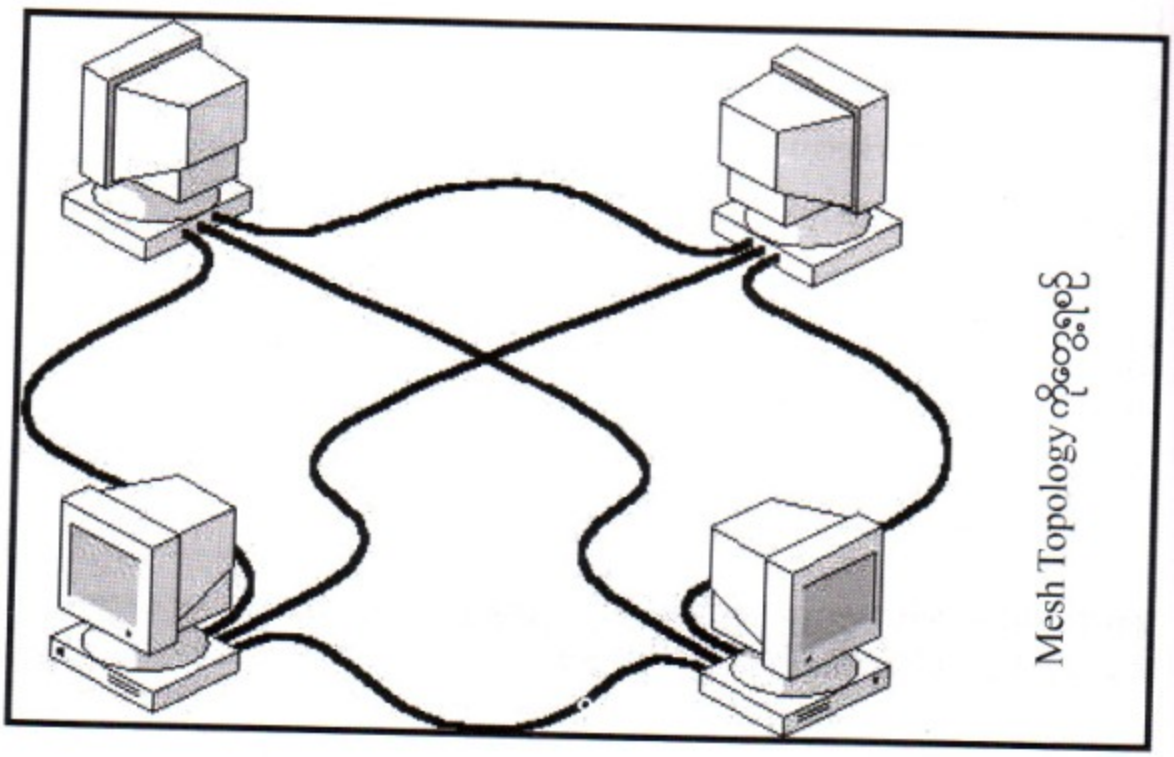


Switching Hub ကိုတွေ့ရစဉ်

၂.၉ Mesh Topology

Mesh Topology ဆိုတာ ကွန်ရက်တစ်ခုအတွင်းမှာရှိတဲ့ Point တစ်ခုချင်းဆီကနေ သူတို့အချင်းချင်းကို Point to Point တိုက်ရိုက်ချိတ်ဆက်ထားတာကိုခေါ်တာပါ။ တကယ့် Mesh Topology ကိုသုံးပြီး ကွန်ရက်တစ်ခုကိုဆင်မယ်ဆိုရင်တော့ ကြိုးတွေအများကြီးကုန်ကျမှာဖြစ်ပါတယ်။

ပုံ ၂.၁၄



Mesh Topology ကိုတွေ့ရစဉ်

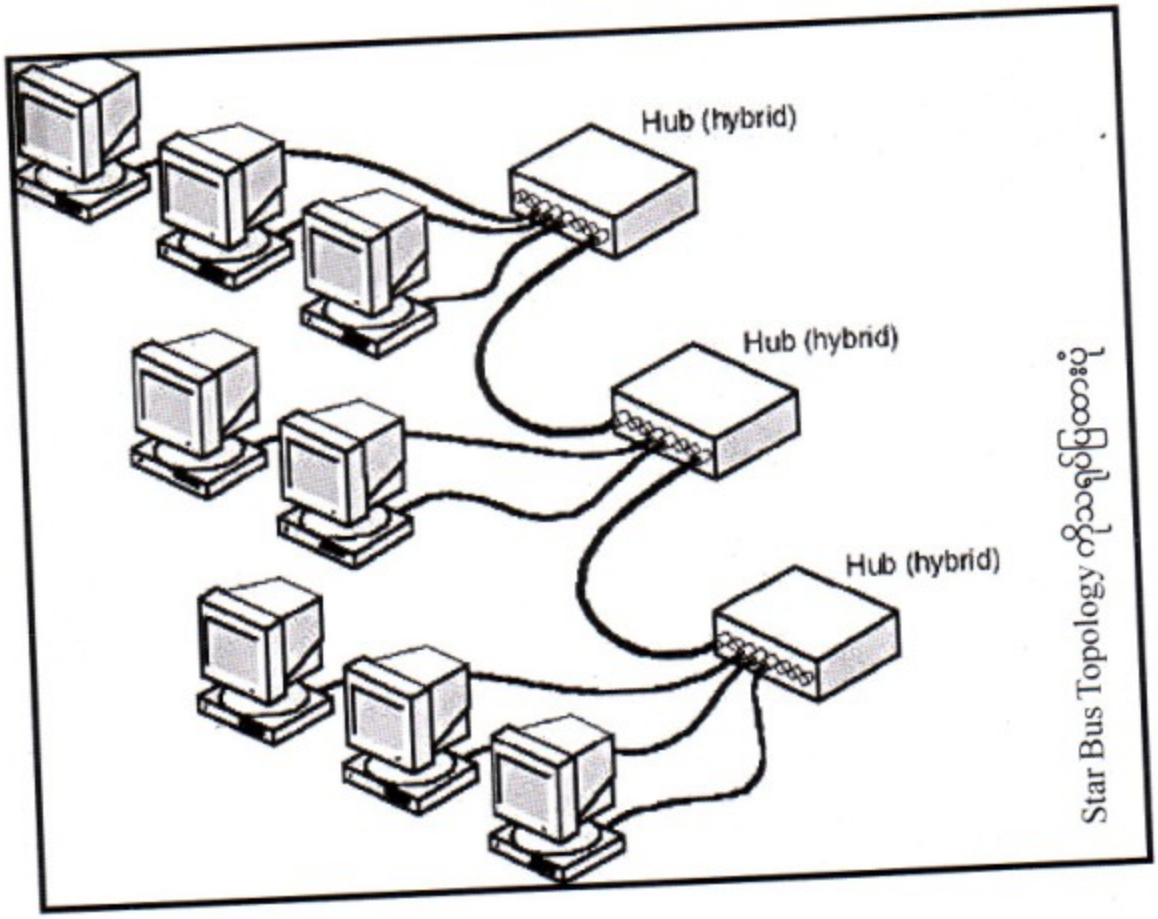
❖ ကောင်းကျိုးတွေကတော့ - ကြိုးအပိုတွေအများကြီးနဲ့ ကွန်ရက်ကိုချိတ်ဆက်ထားတာကြောင့် တစ်ကြိုးမကပျက်သွားရင်တောင် ကွန်ရက်တစ်ခုလုံးကိုအချက်အလက်တွေပေးပို့နိုင်နေတုန်းပါပဲ။

❖ ဆိုးကျိုးတွေကတော့ - ကြိုးပိုကုန်တာပေါ့။

၂.၁၀ Star Bus Topology

Star Bus Topology ဆိုတာကတော့ အခြားမဟုတ်ပါဘူး။ နာမည်ကိုကြည့်လိုက်ကတည်းက Star Bus ဆိုမှတော့ Star နှင့် Bus ပေါင်းထားတာပေါ့။ ပုံကိုကြည့်လိုက်ရင်လည်းတွေ့မှာပါ။ Hub တွေကို Backbone ကိုအသုံးပြုပြီး Hub နှစ်ခု သုံးခုချိတ်လိုက်ပြီး အဲ့ဒီကနေမှပြန်ပွားလာတာပါ။ Hub တစ်ခု Failure ဖြစ်သွားပေမယ့်လည်း အခြား Hub နှင့်ချိတ်ဆက်ထားသော ကွန်ပျူတာတွေအလုပ်လုပ်နိုင်ပါတယ်။

ပုံ ၂.၁၅



Star Bus Topology ကိုသရုပ်ပြထားပုံ

၂.၁၀ Star Ring Topology

Network ကြိုးတွေတပ်ဆင်ထားတာကတော့ Star ဖြစ်ပြီး Network Traffic အလုပ်လုပ်တာကြတော့ Ring ပုံစံနှင့် အလုပ်လုပ်တာဖြစ်သောကြောင့် ၎င်းကို Star Ring Topology လို့ခေါ်ပါတယ်။ Star Ring Topology ကိုတော့ ပုံ ၂.၁၂ ကိုပြန်ကြည့်ပေးပါ။

MCSE

Osborne Certification

Syngress

Global Knowledge Network Certification

QUESTION 3/414:

Which of the following is an example of a LAN?

- ☐ **A.** Two computers in Biloxi connected by leased line to computers in Rapid City
- ☐ **B.** A computer in San Antonio connects via modem to a computer network in Charlotte
- ☐ **C.** 1,700 computers are connected to a network located in a 17-storey office building
- ☐ **D.** The office in Louisville is connected to the office in Naples by a Public Data Network

ANSWER:
C: 1,700 computers are connected to a network located in a 17-storey office building

Answers in Depth...

UNIT 3

Networking Media

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက်တပ်ဆင်ရာမှာလိုအပ်တဲ့ ကြားခံပစ္စည်းတွေအကြောင်းကို လေ့လာကြရမှာဖြစ်ပါတယ်။ Essentials ဆိုတဲ့အတိုင်း မဖြစ်မနေကို သိရမယ့်သင်ခန်းစာတွေဖြစ်ပါတယ်။

ဒီသင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက်တစ်ခုကိုတပ်ဆင်ဖို့အတွက် လိုအပ်တဲ့ကြေးခံပစ္စည်းတွေဖြစ်ကြတဲ့ ကြိုးတွေ၊ Connection ချိတ်ဆက်မှုတွေနဲ့ ၎င်းတို့နှင့်ပတ်သက်နေသောအကြောင်းအရာများ Terms များကိုလေ့လာကြမှာဖြစ်ပါတယ်။ Network Cable အမျိုးအစားတွေထဲက အဓိကအားဖြင့် သိထားသင့်သော ကြိုး (၃) မျိုးအကြောင်းကိုလည်း လေ့လာကြမှာဖြစ်ပါတယ်။ နောက် Baseband အကြောင်း Broadband အကြောင်းကိုလည်းလေ့လာကြမယ်။ သူတို့တစ်ခုချင်းစီကို ဘယ်အချိန်တွေမှာအသုံးပြုတတ်သလဲ ဆိုတာကိုလည်း လေ့လာကြမှာဖြစ်ပါတယ်။

ဒီကနေ့ အသုံးပြုနေတဲ့ Network အများစုမှာ ဒီ Network အတွင်းမှာရှိတဲ့ကွန်ပျူတာအပါအဝင် အသုံးပြုတဲ့ပစ္စည်းတွေကို Cable ကြိုးတွေနဲ့ပဲ ချိတ်ဆက်အသုံးပြုကြပါတယ်။ Signal တွေကိုဘယ်လိုသယ်ဆောင်ပါဆိုတဲ့ နည်းလမ်းတွေထဲက ဘယ်နည်းလမ်းကိုပဲသုံးသုံး ဒီကြိုးတွေကပဲ ကွန်ပျူတာအပါအဝင် Network ထဲကချိတ်ဆက်ထားသောပစ္စည်းတွေအကြား အချက်အလက်တွေကိုသယ်ယူပေးခဲ့တာဖြစ်ပါတယ်။ ဒီလို Cable တွေဟာအရေးပါအရာရောက်တယ်ဆိုပေမယ့် ကနေ့ခေတ်မှာ Network ထဲကကွန်ပျူတာအပါအဝင် ချိတ်ဆက်ပစ္စည်းအားလုံး သို့မဟုတ် တစ်ချို့တစ်လေဟာ Cable ကြိုးကိုပဲအသုံးပြုပြီး Network ချိတ်ဆက်တပ်ဆင်ထားကြတာ မဟုတ်ပါဘူး။ ခုဆိုရင် Network ကိုအသုံးပြုသူတော်တော်များများဟာ တဖြည်းဖြည်းနှင့် ကြိုးမဲ့ဆက်သွယ်ရေး (Wireless Technologies) ကိုအသုံးပြုလာကြပြီ ဖြစ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ Cable ကြိုးတွေအသုံးပြုဖို့မသင့်လျော်တဲ့နေရာတွေ၊ ကြိုးတွေပြေးဖို့နေရာ အခက်အခဲရှိသူတွေ၊ အိမ့်မဟုတ်အသုံးပြုသူတွေကိုယ်တိုင်ကလည်း Mobile ဖြစ်နေလို့စတဲ့ အချက်လေးတွေကြောင့် ကနေ့ Wireless နည်းပညာကိုအသုံးပြုသူ တိုးပွားလျှက်ရှိပါတယ်။ ဒီတော့ ကျွန်တော်တို့က ဒီကြားခံဆက်သွယ်ပေးတဲ့ Networking Media ဆိုတဲ့အကြောင်းကိုလေ့လာရာမှာ လက်ဖြင့်ကိုင်တွယ်ထိတွေ့လို့ရတဲ့ Tangible Physical Media ဆိုတာနဲ့ လက်ဖြင့်ကိုင်တွယ်ထိတွေ့လို့မရတဲ့ Intangible Media ဆိုပြီး နှစ်မျိုးလေ့လာရမှာဖြစ်ပါတယ်။

၃.၁ ကိုင်တွယ်ထိတွေ့နိုင်သော Cable များအကြောင်း

လက်ဖြင့်ကိုင်တွယ်ထိတွေ့နိုင်သော Cable များဟာအုပ်စုအားဖြင့် (၃) အုပ်စုဖြစ်ပါတယ်။ တကယ်တော့ Cable အုပ်စုတွေဟာ ဘယ်လိုပဲအမျိုးအစားတွေကွဲပြားပါစေ။ အဓိကကတော့ Signal တွေဟာ ဒီကြိုးတွေပေါ်မှာဘယ်လိုသွားကြမလဲဆိုတာလည်း အရေးကြီးတာမို့ ပြောရမယ်ဆိုရင် နှစ်ပိုင်း တစ်ခါထပ်ရှိပြန်ပါတယ်။ အဲဒါက Electrical Transmission လား။ အိမ့်မဟုတ် Light Transmission လားပေါ့။ ကဲ ဘာပဲဖြစ်ဖြစ် ဒီအုပ်စု (၃) စုကို ကြည့်မယ်ဆိုရင်

(၁) Coaxial Cable

(၂) Twisted-Pair Cable (UTP နှင့် STP)

(၃) Fiber-Optic Cable

ဒီကြိုးတွေတစ်မျိုးချင်းစီဟာလည်း ပုံသဏ္ဌာန်ကအစ တစ်ခုနှင့်တစ်ခု မတူညီတဲ့ Design တွေ၊ မတူညီတဲ့အသုံးပြုမှုတွေ၊ သူတို့ကိုအသုံးပြုတဲ့အခါ ကုန်မယ့်ကုန်ကျစရိတ်တွေ၊ သူတို့ရဲ့လုပ်ဆောင်ချက်စွမ်းဆောင်နိုင်မှုတွေ၊ တပ်ဆင်တဲ့အခါသတိထားရမယ့် ကိစ္စတွေစသည်ဖြင့် မတူညီတာတွေအများကြီးကို ကျွန်တော်တို့ လေ့လာကြရအောင်။

၃.၂ ဘဲ့ ဆိုထားရမယ့် Cable Characteristics များ

ကဲ ကြိုးအုပ်စုတွေကို တစ်ခုချင်းစီအသေးစိတ်မလေ့လာမှီ ဘုံသိထားသင့်တဲ့ ကြိုးတွေရဲ့ Characteristics တွေကို အရင်လေ့လာကြည့်ရအောင်။ ဘာလို့လည်းဆိုတော့ ကြိုးတွေရဲ့ အခြေခံ Characteristic တွေက တူနေကြလို့ပါပဲ။ ဒါပေမယ့်လည်း တစ်ခုတော့ရှိတာက ဒီ ဝါယာကြိုးကိုအခြေခံထားတဲ့ လျှပ်ကူး Conductive Cable တွေနဲ့ Fiber-Optic Cable နဲ့ကြပြန်တော့လည်း Data သယ်ယူမှုပုံစံတွေ ဘာတွေက ကွဲပြားသွားပြန်ပါတယ်။ အခုလောလောဆယ်တော့ အောက်မှာဖော်ပြထားတဲ့အချက်တွေက ဒီ ဝါယာကြိုးကို အခြေပြုထားတဲ့ Cable ရော၊ အလင်းကိုအခြေပြုထားတဲ့ Fiber Cable ရောနှင့် သက်ဆိုင်ပါတယ်။

Bandwidth Rating

Cable တာသတ်မှတ်ထားတဲ့ အချိန်အတိုင်းအတာတစ်ခုအတွင်းမှာ အချက်အလက်တွေကို ဘယ်လောက် bits အရေအတွက် ဘယ်လောက် bytes သယ်ဆောင်နိုင်သလဲဆိုတာဖြစ်ပါတယ်။ ကြိုးတစ်ကြိုးချင်းစီဟာ သူ့ Bandwidth နှင့် သူရှိကြပါတယ်။ ပုံမှန်အားဖြင့်တော့ bits per second (Megabits per Second, Mbps) နှင့် တိုင်းတာပါသည်။ ကျွန်တော်ရေးသားခဲ့ပြီးသော Computer Network Study Guide စာအုပ်ကို မဖတ်ဖူးသူများအတွက် အဲ့ဒီစာအုပ်တွင်းက Bandwidth ဖော်ပြချက်ကို ပြန်လည်ဖော်ပြအပ်ပါသည်။

Bandwidth ဆိုတာကြားခံပစ္စည်း (ကြိုး၊ ရေဒီယိုလှိုင်းစသည်) ၏ Data ကိုပို့လွှတ်နိုင်သောပမာဏကိုတိုင်းတာခြင်းပင်ဖြစ်ပါသည်။ အဲ့ဒီကြားခံပစ္စည်းဟာ Data ကိုများများပို့လွှတ်နိုင်တာကို Higher Bandwidth လို့ခေါ်ပါတယ်။ တကယ်တော့ Bandwidth ဆိုတဲ့စကားလုံးက ဒီ ကြားခံပစ္စည်းသယ်နိုင်တဲ့ Frequency အတိုင်းအတာကိုဆိုလိုချင်တာလည်းဖြစ်ပါတယ်။ ဒီထက်ပိုနားလည်အောင် ဥပမာပေးပြီး ပြောရရင် လက်မဝက်အကျယ်ရှိတဲ့ ရေပိုက်ခေါင်းတစ်ခုဟာ တစ်မိနစ်ကို ရေနှစ်ဂါလံပို့လွှတ်နိုင်တယ် ဆိုကြပါစို့။ ဒါဆို Bandwidth စကားနဲ့ပြောရမယ်ဆိုရင် Bandwidth = 2 Gallons Per Minute ပေါ့။ ၄ လက်မကျယ်တဲ့ မီးသတ်ပိုက်ခေါင်းတစ်ခုကြတော့ တစ်မိနစ်ကိုရေဂါလံ ၁၀၀ ပို့လွှတ်နိုင်မယ်။ ဒီလိုပဲကြိုးပေါ်မူတည်ပြီး Bandwidth ကမတူညီကြပါဘူး။

ကဲ ခုနကအကြောင်းကိုဆက်ပြောကြရအောင်။ Frequency ရဲ့ယူနစ်ကတော့ Hz (Hertz) ဖြစ်ပြီး Cycle Per Second ပေါ့။ ဥပမာ စကားပြောတယ်လိုဖုန်းလိုင်းကြိုးရဲ့ Bandwidth က 400 မှ 400 Hz အထိရှိပါတယ်။ ဒီတော့ ဒါကို တနည်းအားဖြင့်ပြောရရင် ဒီလိုင်းကြိုးဟာ တစ်စက္ကန့်ကို 400-4000 Cycles ပို့လွှတ်နေတာဖြစ်ပါတယ်။

ဒါပေမယ့် အသံမဟုတ်ဘဲ Data အနေနဲ့ကြတော့ Bits ဆိုတဲ့ စကားလုံးကိုသုံးပါတယ်။ Bits per Second ပေါ့။ ဥပမာ Ethernet ဆိုရင် သိအိုရီအရတော့ တစ်စက္ကန့်ကို 10 Million Bits per Second ပို့လွှတ်နိုင်တယ်။ Bandwidth = 10 Mbps ပေါ့။ အဲ့ဒီအပြင် Bandwidth ဟာကြိုးရဲ့ အတိုအရှည်အလျားပေါ်လည်းမူတည်သေးတယ်။ ယေဘုယျအားဖြင့်ပြောရရင်တော့ တိုတဲ့ကြိုးဟာ ရှည်တဲ့ကြိုးထက် Bandwidth ပိုများပါတယ်။ ဒါကြောင့် ကြိုးတွေနဲ့ ကွန်ပျူတာကိုချိတ်ဆက်တဲ့နေရာမှာ ပိုနေရင် ခွေမထားဘဲ ဖြတ်တောက်ပြီးအသုံးပြုဖို့ပါပဲ။ ကြိုးလိုင်းဟာဘယ်လောက်ထိပဲ ရှည်ရမယ်ဆိုတဲ့ သတ်မှတ်ချက်လေးတွေတော့ရှိပါတယ်။ အဲ့ဒီအတိုင်းအတာထက်ပိုသွားရင်တော့ Bandwidth ကိုထိခိုက်နိုင်ပါတယ်။ Data Signals တွေမှာ Error တွေဝင်လာတတ်တဲ့သဘောပါ။

Maximum Segment Length

Cable တစ်ကြိုးချင်းစီဟာ ဘယ်လောက်ပဲ Data တွေကို ဝေးဝေးပို့နိုင်ပါတယ်ဆိုစေဦးတော့ တကယ်တော့ပို့လိုက်တဲ့အချက်အလက်ကို လုံးဝမှန်ကန်စွာဖတ်နိုင်ပါတယ်ဆိုတဲ့ အခြေအနေရဲ့ ရှေ့ပိုင်းအထိသာ အချက်အလက်တွေကို ပို့ပေးနိုင်ပါတယ်။ ဒီ နောက်ကွယ်မှာတော့ အချက်အလက်တွေ Signal တွေဟာ အားနည်းသွားတဲ့အနေအထားဖြစ်သွားပြီး အဲ့ဒီလိုဖြစ်သွားတာကို Attenuation လို့ခေါ်ပါတယ်။ ဒီတော့ Attenuation အဖြစ်ခင်အထိ Data ပို့နိုင်တဲ့ Cable ရဲ့ တစ်ဖြတ်စာအလျားဟာ Maximum Segment Length ပဲဖြစ်ပါတယ်။ ဒါပမယ့်သိပ်ကြီးတဲ့ Network တွေမှာ ဆင့်ပွားဆင့်ပွားချိတ်တဲ့ Interconnect Network တွေမှာ Signal တွေကိုပြန်လည်အားကောင်းလာအောင်လုပ်ပေးနိုင်တဲ့ Hardware ပစ္စည်းတွေနဲ့ချိတ်ဆက်ပြီး အားနည်းသွားသော Signal များကိုပြန်လည်မြှင့်တင်ပါတယ်။

Attenuation ဆိုတာကြားခံပစ္စည်းတစ်လျှောက် Signal တွေသွားရာလမ်းတစ်လျှောက်မှာ ဘယ်လောက်တောင်အားနည်း (Weaken) ဖြစ်သွားသလဲဆိုတဲ့ Signals ပမာဏပဲဖြစ်ပါတယ်။ အားလုံးသော Electronic Transmission တိုင်းမှာ သတ်မှတ်ထားတဲ့အကွာအဝေးပမာဏကို ကျော်လွန်လာရင် Signal တွေမှာ Noise တွေပါလာပြီး ၎င်းတို့ကို Original Signal မှ ဖယ်ထုတ်ပို့လွှတ်စစ်ပစ္စည်းတွေဟာ ခဲယဉ်းပါတယ်။ ဆိုလိုချင်တာက ပို့လွှတ်မှုကို လက်ခံတဲ့ပစ္စည်းဟာ သူ့ဆီရောက်လာတဲ့ Signal တွေမှာ Noise တွေပါလာတာကို ဒီအတိုင်းလက်ခံပြီး ၎င်း Noise တွေကိုမူလ Signal အဖြစ်မှထုတ်ဖို့ ခဲယဉ်းတယ်လို့ဆိုလိုတာပါ။ ဥပမာ ပြောရရင် လွှင့်ထုတ်ရာနေရာ၏ တော်တော်ဝေးဝေးမှာရှိနေတဲ့ ရေဒီယိုကိုကြည်ကြည်လင်လင်ကြားဖို့ Tune

လုပ်ရသလိုပါပဲ။ အကယ်၍များ ကျွန်တော်တို့ဟာ ရေဒီယိုကအသံလှိုင်းချိန်တဲ့ဟာကို ကိုယ်လိုချင်တဲ့ နေရာမှာ ချိန်သွင်းပြီး (သို့မဟုတ်) ဖမ်းလို့ရတဲ့ Signal ကိုချုပ်ထားလို့ရမယ်ဆိုရင်တောင် လွှင့်ထုတ်တဲ့နေရာက အသံထက်ပိုပြီး Noise တွေကိုကြားနေရအုံးမှာပဲ။ အခုပြောပြနေတာတွေက ကျွန်တော်တို့ပတ်ဝန်းကျင်မှာ ကြုံတွေ့ခဲ့ဖူးမှာပါ။ ဒါ Attenuation ပါပဲ။

Maximum Number of Segments Per Inter Network

Network တစ်ခုမှာအများဆုံးရရှိနိုင်တဲ့ Network ရဲ့အလျားပဲဖြစ်ပါတယ်။ အသုံးပြုတဲ့ ကြိုးပေါ်မူတည်ပြီး ရရှိနိုင်တဲ့အလျားဟာ ကွဲပြားမှာဖြစ်ပါတယ်။ ရှင်းပြရမယ်ဆိုရင် Signals ဟာကြိုးတစ်စရဲ့ တစ်ဖက်စွန်းကနေ နောက်တစ်ဖက်စွန်းကိုသွားလို့ ကြာတဲ့အချိန်ကို Latency လို့ခေါ်ပါတယ်။ ဒီတော့ Network ကြီးက အဲသလိုအဖြတ်ဖြတ်နဲ့ ကြိုး Segment လေးတွေချိတ်ဆက်ရာကနေ ကြီးလာတော့တယ်။ ဒီနေရာမှာ Latency ကစကားပြောလာပါတယ်။ Signal တစ်ခုဟာကြိုးတစ်ဖက်ရဲ့ အစကနေ Network တစ်ခုရဲ့ အဆုံးကိုသွားရာမှာ Latency ကြောင့် Signal တွေဟာ အစွန်းကိုမရောက်နိုင်တော့ဘူး။ ဒါကြောင့် Network တစ်ခုမှာ သတ်မှတ်ထားတဲ့ Network ကြီးတစ်ခုလုံးရဲ့ အလျား တစ်နည်းအားဖြင့် Network ထဲက အပိုင်းပိုင်းဖြစ်နေသော Cable Segment များပါဝင်မှုဟာ သက်ဆိုင်ရာအသုံးပြုထားတဲ့ Cable ရဲ့ အလျားကိုကျော်လို့မဖြစ်ပါဘူး။ ဒီထက်ရှင်းအောင်ပြောရမယ်ဆိုရင်တော့ Cable Segment တစ်ခုဟာ ၅ မီတာရှည်မယ်။ နောက် Segment တစ်ခုက ၁၀ မီတာရှည်မယ်။ နောက် Segment တစ်ခုက ၆ မီတာရှည်မယ်။ ဒီသုံးခုပေါင်းလိုက်တော့ ဖြစ်ပေါ်လာမယ့် Network တစ်ခုက ၂၁ မီတာရှိမယ်။ အဲ့ဒါကိုပြောတာပါ။ Network တစ်ခုမှာပါဝင်တဲ့ Segment များရဲ့အလျားစုစုပေါင်းခြင်းဟာ Network ကြီးတစ်ခုလုံးရဲ့ အလျားပဲမဟုတ်လား။ အဲဒီအလျားမှာလဲ ကိုယ်အသုံးပြုတဲ့ Cable ကြိုးပေါ်မူတည်ပြီး Network ကြီးတစ်ခုလုံးဟာ ဘယ်နှစ်မီတာ မကျော်ရဘူးဆိုတဲ့ ကန့်သတ်ချက်မျိုးပြောချင်တာပါ။

Maximum Number of Devices Segment

Segment တစ်ခုမှာ ပစ္စည်းတွေအများဆုံးဘယ်လောက် တပ်ဆင်ရမလဲဆိုတာ ကန့်သတ်ထားသင့်တယ်။ ဆိုလိုတာက ဒီလိုဗျ။ Network ပစ္စည်းတစ်ခုဟာ Network ကြိုးမှာ တပ်ထားတိုင်း တပ်ထားတိုင်း Insertion Loss ဆိုတာဖြစ်ပေါ်နေတယ်။ အဓိပ္ပါယ်ကတော့ Signal တွေအားနည်းသွားတယ်ဆိုတဲ့ Attenuation ဟာ ဒီ Cable ကြိုးတွေမှာ တပ်ထားတဲ့ပစ္စည်းအရေအတွက်နဲ့လည်းဆိုင်တယ်လို့ ပြောချင်တာဖြစ်ပါတယ်။ ဒီတော့ Signal တွေဟာ ဒီပစ္စည်းတွေကိုဖြတ်သန်းပြီးသွားရာမှာ နောက်ဆုံးကျန်ရှိနေတဲ့ Signal ရဲ့အခြေအနေ တစ်နည်းအားဖြင့် ပစ္စည်းတွေဆီကိုရောက်တဲ့အခါမှာ Signal ဟာကောင်းမွန်စွာရှိနေစေဖို့ Segment တစ်ခုမှာ ပစ္စည်းဘယ်လောက်ပဲတပ်သင့်တယ်ဆိုတဲ့ ကန့်သတ်ချက်မူမျိုးလည်းရှိသင့်ပါတယ်။

ဒီတော့ Cable တစ်ခုရဲ့ အမှန်တကယ်ရှိသင့်တဲ့ အရှည်ဆုံးအလျားကိုတွက်ယူရာမှာ ဒီပစ္စည်းတွေတပ်ထားလို့ Insertion Loss ဖြစ်နေတယ်ဆိုတာကို ထည့်စဉ်းစားပေးဖို့မမေ့ပါနဲ့။

Interference Susceptibility

ကြိုးတစ်မျိုးချင်းစီဟာ ပတ်ဝန်းကျင်မှာရှိတဲ့ EMI လို့ခေါ်တဲ့ Electromagnetic Interference နှောင့်ယှက်မှုကိုအနည်းနှင့်အများတော့ ခံကြရတာဖြစ်ပါတယ်။ အဲဒီ EMI ဆိုတဲ့နှောင့်ယှက်မှုအပြင် ဒီပတ်ဝန်းကျင်မှာတခြားသောနှောင့်ယှက်မှုတစ်ခုရှိသေးတယ်ဗျ။ အဲဒါက RFI ဆိုတဲ့ Radio Frequency Interferences ပါပဲ။ ၎င်းတာ Broadcast Signal ကြောင့်ဖြစ်ပေါ်လာတာဖြစ်ပါတယ်။ ဒီ EMI တွေ RFI တွေဟာ Motors တွေ Transformers တွေအခြားသောလျှပ်စစ်သက်ရောက်မှုရှိတဲ့ပစ္စည်းတွေကနေဖြစ်ပေါ်လာတာဖြစ်ပါတယ်။ ဒါပေမယ့် RFI တာအများအားဖြင့် Brokdcast Signal ကြောင့်ဖြစ်တာမို့ အနီးနားမှာ Radio တွေ Television တွေရှိနေမယ်ဆိုရင် Network Cable ကြိုးတွေဆီက Signal တွေဟာဒီနှောင့်ယှက်မှုတွေကြောင့် Loss ဖြစ်နိုင်ပါတယ်။

Electromagnetic Interference ဖြင့်ပတ်ဝန်းကျင်နှောင့်ယှက်မှု

Electromagnetic Interference (EMI) ဆိုတာပြင်ပကလျှပ်စစ်သံလိုက်ဓာတ်တို့ကကြားခံပစ္စည်းထဲက Signals တွေကိုမှုလပုံပန်းသဏ္ဍာန်ပျက်ပြားအောင်တိုက်ခိုက်နှောင့်ယှက်မှုကိုခေါ်တာပါ။ ရေဒီယိုက AM လိုင်းကိုဖမ်းပြီးနားထောင်နေတုန်းမှာ အဲဒီအနီးအနားမော်တာတွေပါဖွင့်ထားရင် ကျွန်တော်တို့ဟာ ရေဒီယိုသံကိုကောင်းစွာမကြားရဘဲ Noise တွေပါလာတာကိုပါကြားရပါလိမ့်မည်။ ၎င်းသည် EMI ပင်ဖြစ်သည်။ Attenuation နှင့်ကွာခြားသည်မှာ ၎င်းသည် အကွာအဝေးကြောင့်သူ့ကိုအလိုအလျောက် Data weaken ဖြစ်တာမဟုတ်ဘဲပြင်ပမှနှောင့်ယှက်မှုကြောင့် Noise များပါလာခြင်းဖြစ်ပါသည်။

Connection Hardware

Connection Hardware ဆိုသည်မှာ Network ကြိုးတွေမှာတပ်ဆင်တဲ့ Network ခေါင်းပဲဖြစ်ပါတယ်။ ကြိုးတစ်မျိုးချင်းစီမှာ အသုံးပြုတဲ့ Network ခေါင်းတွေဟာမတူညီကြပါဘူး။ ဈေးလည်းကွာတတ်ပါတယ်။ တပ်ဆင်တဲ့အခါမှာလိုအပ်တဲ့ Tools တွေလည်းကွာတတ်ပါတယ်။

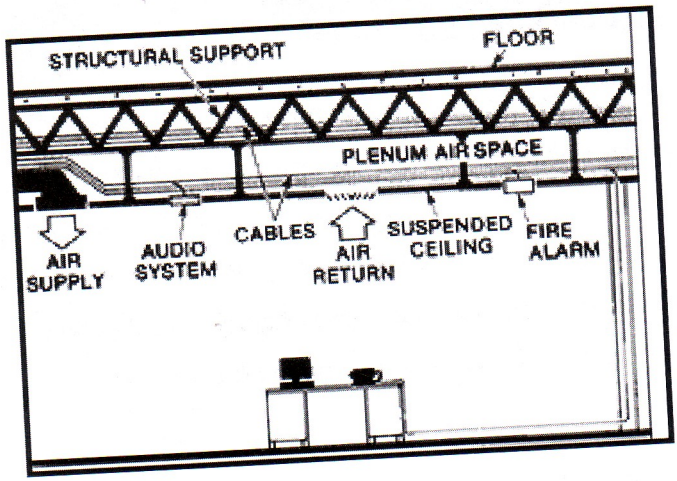
Cable Grade

များသောအားဖြင့် Cable တွေရဲ့လျှပ်ကာအခွံတွေမှာ တနည်းအားဖြင့် Cable တွေရဲ့အပေါ်ယံ Cover တွေမှာ Cable တွေရဲ့တိကျတဲ့ ဒါမှမဟုတ်သတ်သတ်မှတ်မှတ်အကြောင်းအရာအချက်အလက်တွေပါရှိရပါတယ်။ ဆိုလိုတာက အဆောက်အအုံပိုင်းဆိုင်ရာနှင့် မီးနှင့်ပတ်သက်သော Code တွေပါရှိရပါတယ်။ ဘာအတွက်လဲဆိုတော့ မီးလောင်ကျွမ်းမှုနဲ့ထွက်ရှိလာသောအခိုးအငွေ့များမှာ အဆိပ်ဖြစ်ပေါ်မှုတို့ကိုရှောင်ကျဉ်နိုင်ရန်ဖြစ်ပါတယ်။ ဥပမာပြောရရင် Polyvinyl Chloride လို့ခေါ်တဲ့ PVC Cover တွေဟာ ကျွန်တော်တို့အိမ်သုံးပစ္စည်းတော်များများမှာတွေ့ရတတ်တဲ့ ဈေးသက်သာတဲ့လျှပ်ကာအခွံတစ်မျိုးပဲဖြစ်ပါတယ်။ အကယ်၍ များကံမကောင်းအကြောင်းမလှလို့ အဲဒီကြိုးမီးလောင်ခဲ့ရင်ထွက်ပေါ်လာတဲ့အခိုးငွေ့တွေဟာ အဆိပ်အတောက်ဖြစ်တတ်တဲ့အပြင်ဒီလိုကြိုးမျိုးကို မျက်နှာကျက်တွေရဲ့အပေါ်မှာ ဒါမှမဟုတ် နံရံတွေရဲ့အထဲမှာတပ်ဆင်ဖို့မသင့်လျော်ပါဘူး။ ဒီတော့ကိုယ်အသုံးပြုမဲ့ Network ကြိုးမျိုးဟာအန္တရာယ်ဖြစ်မှုတွေနဲ့လည်း ကင်းရှင်းနေရအုံးမှာဖြစ်ပါတယ်။

Plenum

စီးပွားရေးအဆောက်အအုံတွေမှာအထပ်တစ်ထပ်နှင့်တစ်ထပ်ကြားရှိနေတဲ့ Slab ကြမ်းခင်းဟာ အထပ်တစ်ထပ်အတွက်ကြမ်းပြင်ဆိုပေမယ့် သူ့အောက်ကအထပ်အတွက်ကတော့ မျက်နှာကျက်ဖြစ်နေပါလိမ့်မယ်။ ဒါပေမယ့် အဲဒီလိုအဆောက်အအုံတွေမှာ Air-Con ပိုက်လိုင်းတွေနှင့် မီးပိုက်တွေဟာငင်းမျက်နှာကျက်ကိုကပ်ပြီးပြေးထားတာကြောင့် သူတို့ကိုဖုံးပေးထားနိုင်မယ့် နောက်ထပ်အလှမျက်နှာကျက်တစ်ခုထပ်လိုလာပါတယ်။ ဒီတော့ ကြည့်လိုက်လို့ရှိရင် Air-Con ပိုက်တွေ၊ မီးပိုက်တွေကိုမမြင်ရတော့ဘူး။ အဲဒီလိုပဲ ကွန်ကရစ်ကြမ်းခင်းကြီးကိုလည်းမမြင်ရတော့ဘူး။ အဲဒီကွန်ကရစ်ကြမ်းခင်းမျက်နှာကျက်ကြီးနှင့်အလှတပ်ဆင်ထားသောမျက်နှာကျက်နှစ်ခုအကြားကို Plenum လို့ခေါ်ပါတယ်။

ပုံ ၃.၁



ကျွန်တော်တို့ဟာ Network ကြိုးတွေကို အဲဒီ Plenum ထဲမှာပြေးမယ်ဆိုရင် အသုံးပြုမယ့်ကြိုးတွေဟာ Plenum-Rated ဖြစ်နေရပါမယ်။ ဆိုလိုတာက ၎င်းကြိုးတွေရဲ့ Cover ဟာ Teflon နဲ့ပြုလုပ်ထားပါတယ်။ ဒီကြိုးတွေဟာ မီးလောင်မှုအခွင့်အရေးနည်းပါးပြီး ထွက်လာတဲ့အခိုးအငွေ့တွေဟာလည်း အဆိပ်အတောက်မဖြစ်စေပါဘူး။ ဆိုလိုတာက အကယ်၍များမီးလောင်ခဲ့ရင်ပေါ့။

Bend Radius

တစ်ချို့ Cable တွေဟာဘယ်လိုပဲကွေးညွှတ်ခြင်း Bending လုပ်ပါစေ ထိခိုက်မှုနည်းလှပါတယ်။ ဒါပေမယ့် သိပ်ကိုကျေးကြိုးတဲ့ကြိုးတွေဖြစ်ကြတဲ့ Fiber-Optic Cable နှင့် Heavy Duty ထမ်းဆောင်ရတဲ့ Coaxial Cable (Thicknet) တွေမှာ သိပ်ပြီးတော့ကွေးကောက်ပြီးကြမ်းကြမ်းတမ်းတမ်းကိုင်တွယ်လို့မရပါဘူး။ သတိထားပြီးဂရုတစိုက်ကိုင်တွယ်ရမှာဖြစ်ပါတယ်။ ဒီလိုအထိမခံအရွေ့မခံ Sensitive ဖြစ်တဲ့ Cable ကြိုးတွေကို ကိုင်တွယ်ရာမှာ ကွေးမိရင်တောင် 60° (၆၀ ဒီဂရီ) ထက်ပိုမကွေးမိစေဖို့ဂရုပြုရမှာဖြစ်ပါတယ်။ အတိုချုပ်ပြောရရင်တော့ ကြိုးတွေကိုသတ်မှတ်ထားတဲ့ ဒီဂရီထက်ပိုမကွေးမိစေဖို့ပါပဲ။

Material Costs

Cable တစ်မျိုးချင်းစီမှာ သတ်မှတ်ထားတဲ့အကွာအဝေးတစ်ခုချင်းစီအတွက် သက်ဆိုင်ရာကုန်ကျစရိတ်တွေရှိနေပါတယ်။ ကြိုးတွေကိုနှိုင်းယှဉ်ပြီးဝယ်ယူရာမှာ ကိုယ်ကစျေးသက်သာတာကို ဝယ်လိုက်တယ်ဆိုပေမယ့် ခုနကပြောခဲ့တဲ့မီးလောင်လွယ်တဲ့ ကြိုးအမျိုးအစားတွေကို ရှောင်ဖို့နဲ့ အကယ်၍မီးလောင်ခဲ့မယ်ဆိုရင်တောင် ထွက်ပေါ်လာတဲ့ အငွေ့တွေဟာအဆိပ်အတောက်မဖြစ်စေဖို့ စတဲ့အချက်တွေကို ဂရုပြုပြီးဝယ်ယူတပ်ဆင်ရမှာဖြစ်ပါတယ်။

Installation Cost

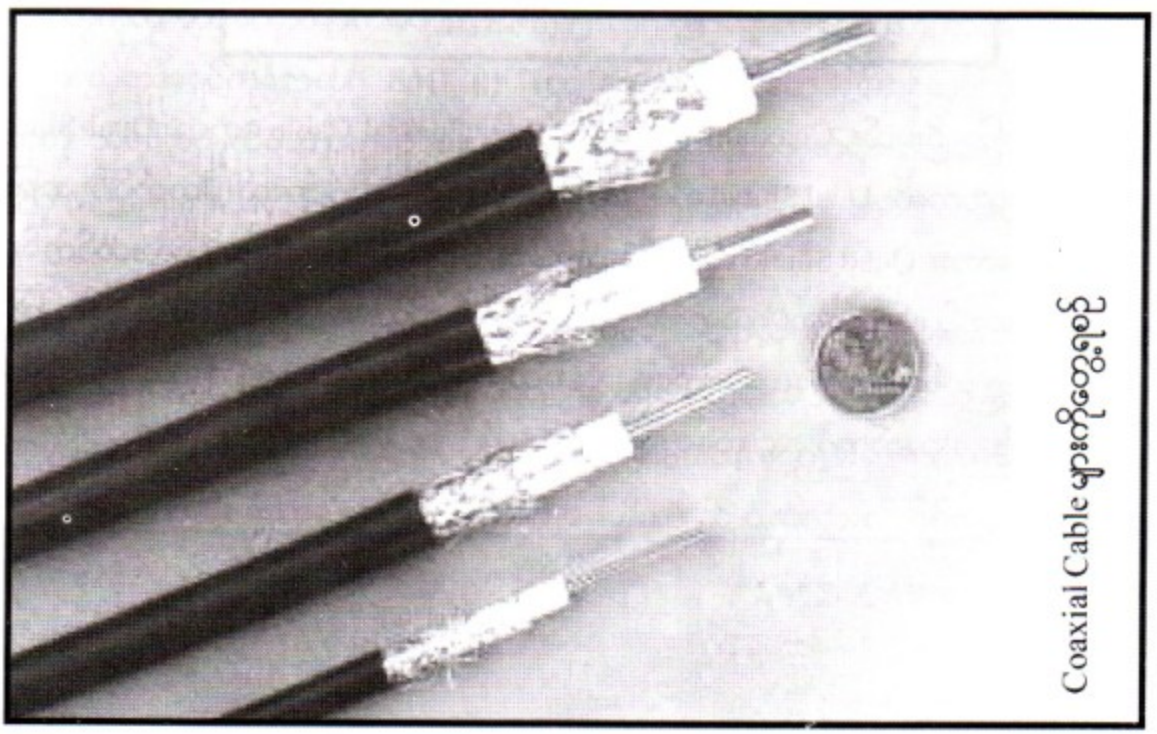
Cable ကြိုးတွေတပ်ဆင်တဲ့နေရာမှာလည်း အလုပ်သမားစရိတ်တွေ၊ တပ်ဆင်တဲ့အခါမှာ အသုံးပြုမည့်ပစ္စည်းတွေအတွက် ကုန်ကျစရိတ်ဟာ Cable ကြိုးတွေထက်ပိုကုန်သွားနိုင်ပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့ဟာ Network တစ်ခုကိုမတပ်ဆင်ခင် Cable Plant (Design ဆွဲခြင်း၊ တပ်ဆင်ခြင်း၊ ပြဿနာ အဖြေရှာခြင်းနှင့်လိုအပ်တဲ့ Connectors တွေ၊ Cable ကြိုးတွေ၊ Wall Plates တွေ၊ Patch Panels တွေ၊ နောက်ပြီး Punchdown Blocks တွေ အစရှိသည်တို့တွေ) ကိုသေချာစွာတွက်ချက်ပြီး ဆောင်ရွက်မှ ကုန်ကျစရိတ်လည်းအပိုမကုန်မှာ၊ နောက်ပြီးတပ်ဆင်မှုလည်း အမှန်တကယ်သေချာမှာဖြစ်ပါတယ်။

ကဲ့ဒီလောက်ဆိုရင် Cable တွေနဲ့ပတ်သက်လို့ ဘုံ သိထားရမယ့်အချက်တွေကို သိရှိလောက်ပါပြီ။ ဆက်လက်ပြီးတော့လေ့လာကြရအောင်။

၃.၄ Coaxial Cable အကြောင်း

Coaxial Cable ဆိုတာက ဒီနေ့ခေတ်မှာအတော့်ကို အသုံးနည်းသွားပြီဖြစ်ပေမယ့် ကျွန်တော်တို့ Networking Essential လို့ပြောလိုက်တာနဲ့ သူ့ကိုချန်ထားခဲ့လို့မရဘူး ဖြစ်ပါတယ်။ တကယ့်ကို Network လောကမှာ ထင်ရှားမင်းမူခဲ့တဲ့ Cable ဖြစ်ပါတယ်။ Coaxial တာရော်သက်သာတယ်။ တပ်ဆင်ရတာလွယ်ကူတယ်။ ဒါကြောင့် Network တပ်ဆင်သူများဟာ နှစ်ပေါင်းတော်တော်များများ Coaxial Cable ကို အသုံးပြုခဲ့ကြပါတယ်။

ပုံ ၃.၂

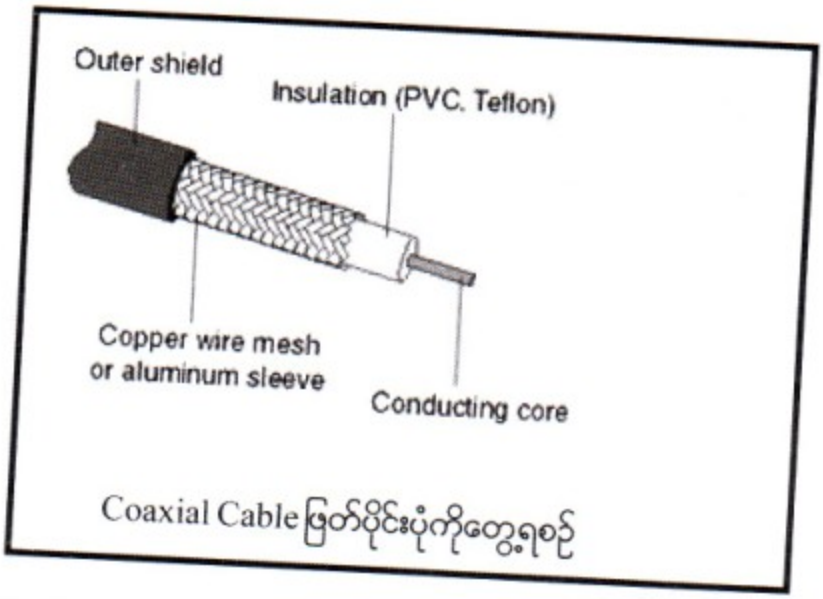


Coaxial Cable များကိုတွေ့ရစဉ်

Coaxial Cable ရဲ့ဖွဲ့စည်းပုံကိုပြောပြရမယ်ဆိုရင် အလယ်တည့်တည့်မှာ တစ်ခုတည်းသောလျှပ်ကူး (Single Conductor) ဆိုတာပါရှိပါတယ်။ သူကအဓိကပေါ့နော်။ Signal သယ်တာပေါ့။ ဒီလျှပ်ကူးကို PVC ဒါမှမဟုတ် Teflon ဆိုတဲ့အရာနဲ့ ပတ်ပတ်လည်ကာထားတယ်။ ဒါကို Insulation Layer လျှပ်ကာလို့ခေါ်ပါတယ်။ အဲ့ဒီရဲ့အပြင်မှာတော့ သံဇကာကွက်ပုံစံ Shield ဆိုတာရှိပါတယ်။ Shield ဆိုတာပြင်ပက Electromagnetic Interferenace စတဲ့ EMI တို့ RFI တို့ကိုကာကွယ်ပေးတာဖြစ်ပါတယ်။ အပြင်ဘက်ဆုံးအလွှာကတော့ Cover ပဲဖြစ်ပါတယ်။ Shealth လို့လည်းခေါ်ပါတယ်။ ဒီတော့ ပုံမှာလည်းမြင်နေရပါတယ်။ အတွင်းအကျဆုံး Core Conductor ကပဲ Signal တွေကိုသယ်ဆောင်တာဖြစ်ပြီး ကျန်တဲ့အပိုင်းတွေက Core

Conductor တွေကို ကာကွယ်ပေးထားတာဖြစ်ပါတယ်။

ပုံ ၃.၃



Coaxial Cable ဖြတ်ပိုင်းပုံကိုတွေ့ရစဉ်

ပြောရဦးမယ်။ Coaxial Cable မှာမှ တချို့ Coaxial Cable တွေက Dual-Shield Version တွေလည်းလာတယ်။ Dual Shield ဆိုတဲ့အတိုင်း Shield နှစ်ထပ်ပါပါတယ်။ ဒီထက်ပိုပြီး အကြမ်းခံတာမျိုးလိုချင်သေးလား။ Quad Shield ဆိုတာရှိသေးတယ်။ Quad Shield ဆိုတော့ လေးထပ်ကွမ်း Shield ကို လေးထပ်တောင်လုပ်ထားတာ။ ရှယ်တကာ့ရှယ်ပဲ။ ဒီပေမယ့် သိထားရမှာက Shield ပိုလာလေ ကြိုးကစွေးကြီးလာလေပဲဗျ။ တစ်ခုကတော့ကောင်းတာပေါ့လေ။ ပြင်ပကနှောင့်ယှက်မှုတွေကိုကြတော့ အတော်လေးကာကွယ်နိုင်တာပေါ့။ အောက်ကပုံ ၃.၄ မှာတွေ့လား။

ပုံ ၃.၄

ကဲ့ဒီတစ်ခါ Shield ဆိုတဲ့အကြောင်းကိုအနည်းငယ် ရှင်းပြပါဦးမယ်။ Shield ဆိုတာ အကာအကွယ်ပဲဗျ။ Core Conductor ကနေ Signals တွေသယ်လာတာကို ပြင်ကအနှောင့်အယှက်တွေ ဝင်ရောက်လာမှုကို အကာအကွယ်ပေးတာပဲဖြစ်ပါတယ်။ External Interference ပေါ့ဗျာ။ EMI နဲ့ RFI ပေါ့။ ဆိုလိုတာက Signals တွေဟာ Core Conductor ကနေ လိုရာအရပ်ကိုစီးဆင်းသွားလာနေချိန်မှာ ၎င်း Cable ဖြတ်သန်းသွားလာရာလမ်းတစ်လျှောက်မှာ အသုံးပြုတဲ့ TV, Speaker, Motor စတာတွေကနေ ဖြစ်ပေါ်လာသော Electromagnetic Interference နှင့် Radio Frequency Interference တို့ကြောင့် Core Conductor ထဲက Signals တွေဟာ ၎င်း Interference ကြောင့်ရှေ့ဆက်မသွားနိုင်ဘဲ ဖြစ်ကုန်ကြပါတယ်။ ဥပမာ ကောင်လေးတွေက ကျောင်းသွားတယ်ပေါ့ဗျာ။ လမ်းမှာလမ်းသရဲ ကောင်မလေးတွေနဲ့ တွေ့တယ်ပေါ့ဗျာ။ တစ်ချို့ကောင်လေးတွေက ဦးတည်ရာကျောင်းကိုမရောက်တော့ဘူး။ ကောင်မလေးတွေနောက် ကောက်ကောက်ပါသွားတယ်။ ဒီတော့ Core Conductor ထဲက Signals ကကောင်လေးတွေ။ လမ်းမှာတွေ့ရတဲ့ကောင်လေးတွေကိုလိုက်တဲ့ ကောင်မလေးတွေက EMI တို့ RFI တို့ပေါ့နော်။ ကဲဒီတော့ ကောင်လေးတွေဆိုတဲ့ Signals တွေ လိုရာအရပ်ကိုရောက်ဖို့ EMI, RFI ဆိုတဲ့ကောင်မလေးတွေရဲ့ နှောင့်ယှက်မှုမှကင်းဝေးဖို့ Shield ဆိုတဲ့ သံဇကာကွက်ကကာကွယ်ပေးထားရတယ်။ အဲ့သလိုမှမဟုတ်ရင် Signals တွေပြင်ပက နှောင့်ယှက်မှု Magnetic Wave / Frequency / Radio Frequency တွေကြောင့် တစ်ချို့ လမ်းမှာကျကျန်ရစ်ခဲ့ကြမယ်။

ဒီနေရာမှာသိထားရမှာက Core Conductor ဟာလျှပ်ကူးဖြစ်တယ်။ နောက် Shield ဆိုတဲ့ သံဇကာကွက်ကလည်း Conductor လျှပ်ကူးဖြစ်တယ်။ ဒီတော့ သူတို့နှစ်ခုသွားထိလို့မရဘူး။ သွားထိရင် Short Circuit တွေဖြစ်ကုန်မှာ။ ဒါကြောင့် ဒီ Core Conductor နှင့် ဒီ Shield နှင့်ကြားမှာ လျှပ်ကာဆိုတဲ့ Insulation အလွှာတစ်ခုထားပြီး ခံထားတာ။ ဒီလျှပ်ကာက ပေါက်သွားလို့ ပျက်သွားလို့ ဖြစ်လို့မရဘူး။ Conductor နှစ်ခုကိုပူးမသွားအောင် ကာပေးထားရတာ။ အကယ်၍ Insulation Layer ပေါက်သွားလို့ Conductor နှစ်ခုသွားပူးရင် Short ဖြစ်ပြီး Signals တွေရှေ့ဆက်မသွားနိုင်ပြန်ဘူး။ Coaxial Cable ရဲ့ Shield ပါတဲ့ကောင်းတဲ့အချက်ကြောင့် ၎င်းဟာတကယ့်ကို Noisy Enviroment တွေမှာ (EMI, RFI ထုတ်လွှတ်သော နေရာပတ်ဝန်းကျင်) တောင်အသုံးပြုလို့ရပါတယ်။ တစ်ခုတော့ရှိတာပေါ့။ ပိုကောင်းအောင် သတ္တုပိုက်လိုင်း၊ ပြွန်မကြီးသဖွယ် အပို Shield ထပ်ကာပေးရင် ပိုကောင်းတယ်။ ဒီ Coaxial မှာကောင်းတဲ့အချက်ကတော့ Shield ပါတယ်ဆိုတာပါပဲ။

မှတ်ချက်။ ။ ဒီ Cable ဟာ Network သမိုင်းမှာ LAN အတွက်ပထမဆုံး Cables ကြိုးပဲပေါ့။ ဝင်ရိုးတစ်ခုထဲပေါ်မှာပဲ Conductor နှစ်ခုပါရှိနေတာကြောင့် Coaxial Cable တုခေါ်သည်။

၃.၄ Coaxial Cable အမျိုးအစားများ

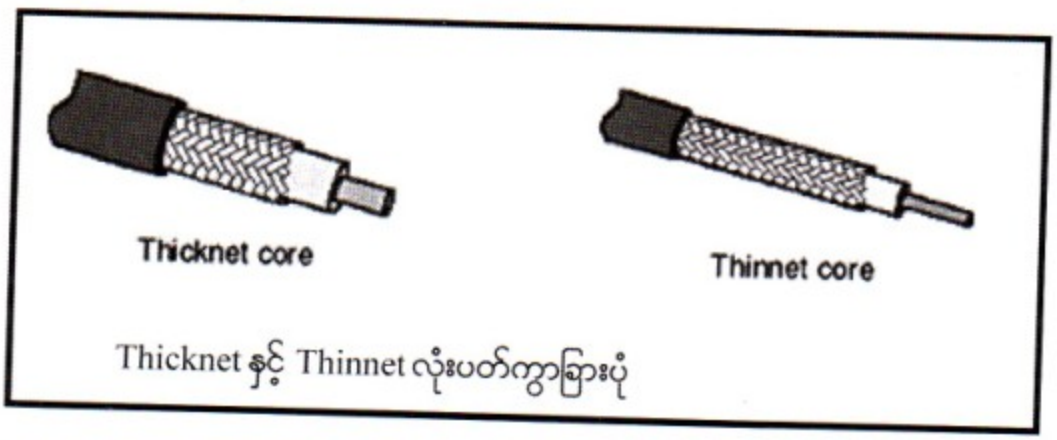
Ethemet မှာတော့ Coaxial Cable အမျိုးအစား (၂) မျိုးရှိပါတယ်။ တစ်ခုကတော့ Thin Ethernet ဖြစ်ပါတယ်။ ၎င်းကို Thinnet, Thinwire ဒါမှမဟုတ် Cheapernet လို့လည်းခေါ်ပါတယ်။ နောက်တစ်ခုက Thicknet ဖြစ်ပါတယ်။ ၎င်းကိုကြတော့ Thickwire လို့လည်းခေါ်ပါတယ်။ IEEE ဆိုတဲ့ Institute of Electrical and Electronics Engineers ကတော့ ၎င်း Thinnet ကို 10Base2 လို့ခေါ်ပြီး Thicknet ကိုတော့ 10Base5 လို့ခေါ်ပါတယ်။ ဒီ 10Base2, 10Base5 ဆိုတဲ့အခေါ်အဝေါ်ကိုရှင်းပြရမယ်ဆိုရင်-

(၁) 10 ဆိုတာ ဒီ Cable ရဲ့ Bandwidth ကိုပြောတာပါ။ အဓိပ္ပါယ်က 10 Mbps (10 Megabits per Second) ဖြစ်ပါတယ်။

(၂) Base ဆိုတာကတော့ Baseband Signaling ကိုပြောတာဖြစ်ပါတယ်။

(၃) 2 တို့ 5 တို့ဆိုတာကြတော့ အများဆုံးရနိုင်တဲ့ Segment ရဲ့ Length ပဲဖြစ်ပါတယ်။ အဓိပ္ပါယ်က 2 ဆိုတာ မီတာ ၂၀၀၊ 5 ကြတော့ မီတာ ၅၀၀ ဖြစ်ပါတယ်။ အပေမယ့် တကယ်တမ်းကြတော့ Thinnet က ၁၈၅ မီတာပဲရတာပါ။ ခေါ်ရလွယ်အောင် မီတာ ၂၀၀ ဆိုပြီးပြောတာပါ။ Thicknet ကြတော့ မီတာ ၅၀၀ ရပါတယ်။

ပုံ ၃.၅



Thicknet နှင့် Thinnet လုံးပတ်ကွာခြားပုံ

ဒီ Coaxial နှင့်ပတ်သက်ပြီးထပ်မံမှတ်ထားရမယ့် အခေါ်အဝေါ်တစ်ခုက RG ဆိုတာပဲဖြစ်ပါတယ်။ RG ဆိုတာ Radio Goverment ဖြစ်ပါတယ်။ ဒီလိုဗျ Coaxial Cable မှာမှ မူကွဲတွေအများကြီးရှိသေးတာကလား။ ဘယ်လိုကွဲတာလဲဆိုတော့ Impedence မတူဘူးပေါ့ဗျ။ အင်းပြောရရင် အဓိကကွာခြားတာကတော့ Centre Core Conductor ပဲ။ ဥပမာပြောရရင် တစ်ချို့ Core Conductor ကနန်းကြိုးမျှင်တစ်ချောင်းထဲ၊ ဘိုလိုပြောရင်တော့ Solid Wire ပေါ့။ အဲ တစ်ချို့ ကြပြောတော့လည်း Braided Core ပေါ့။ ဒီလိုလေ နန်းကြိုး မျှင် အများကြီးကိုလိမ်ထားတာ။

ပုံ ၃.၆

Briaded Core နှင့် Solid Core ကို ယှဉ်တွဲပြထားပုံ

ကဲ့ဒီတော့အမျိုးမျိုးသော Coaxial Cable များကိုအောက်ဖော်ပြပါ ဇယားပုံမှာလေ့လာနိုင်ပါတယ်။

Designation	Type	Impedance	Discription
RG-58/U	Thinwire	50 ohms	Solid copper core (U stands for utility grade; not recognized as valid thinwire cable by IEEE 802.3 specifications.)
RG-58 A/U	Thinwire	50 ohms	Standed copper core (A/U indicates a thinned copper braid as the center conductor with foam dielectric insulator.)
RG-58 C/U	Thinwire	50 ohms	Malitary version of RG-58 A/U (Uses a solid dielectric insulator)
RG-59	CATV	75 ohms	Broadband cable; used for cale television (CATV) and sometimes for ARCnet
RG-6	Broadband	75 ohms	Larger diameter, higher bandwidth than RG-59; used as CATV drop cable
RG-62	Baseband	93 ohms	Used for ARCnet and IBM 3270 terminals
RG-8	Thickwire	50 ohms	Solid core; approximately 0.4* in diameter
RG-11	Thickwire	75 ohms	Standard core, approximately 0.4* in diameter; used for CATV trunk lines

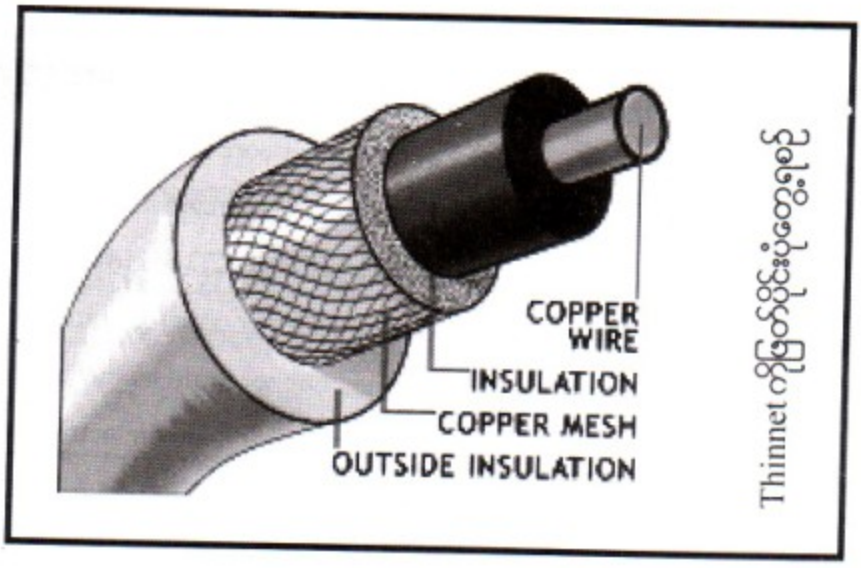
မှတ်ချက်။ ။ Impedence ဆိုတာ Cable ကြိုးမှာစီးဆင်းနေတဲ့ Current ရဲ့ Electrical Resistance ပဲဖြစ်ပါတယ်။ Impedence ကို Ohms နှင့်တိုင်းတာပါတယ်။

CATV ဆိုသည်မှာ Cable Television ဖြစ်ပါသည်။

၃.၅ Thinnet အကြောင်း

Thinnet က Thinwire ဆိုတဲ့အတိုင်းကြိုးရဲ့အချင်းဟာ ၀.၂၅လက်မ (စင်တီမီတာနဲ့ပြောမယ်ဆိုရင် တော့ ၀.၆၄ စင်တီမီတာ) ရှိပါတယ်။ ကြိုးကပျော့ပျော့ပါပဲ။ ခွေလို့ ပြုလို့လည်းရပါတယ်။ Flexible ဖြစ်တယ် ပေါ့ဗျာ။ ဒီ Thinwire Cable တွေဟာ ဈေးလည်းသက်သာတယ်။ တပ်ဆင်ရလည်းလွယ်ကူတယ်။ အောက်မှာ Thinwire တွေနှင့်ပတ်သက်နေသောအကြောင်းအရာများကိုဆက်လက်လေ့လာကြည့်ပါဦး။

ပုံ ၃.၇



Thinnet ကိုဖြတ်ပိုင်းပုံတွေ့ရှုခြင်း

Installation တပ်ဆင်ခြင်း

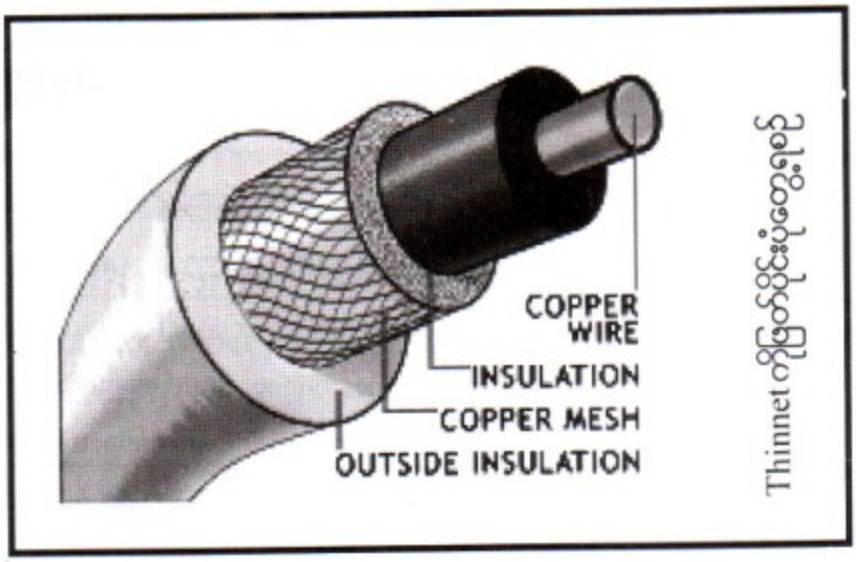
Coaxial Cable ကိုပုံစံနှစ်မျိုးနဲ့ချိတ်ဆက်အသုံးပြုလို့ရပါတယ်။ အဲ့ဒါတွေကတော့ တစ်ခုမှတစ်ခုသို့ ချိတ်ဆက်ခြင်း From Device to Device (Ethernet) နှင့် အလယ်ဗဟိုအမှတ်တစ်ခုမှ တစ်ခုချင်းစီသို့သီးခြားစီချိတ်ဆက်ခြင်း Star (ARCnet) တို့ပဲဖြစ်ပါတယ်။

ဒီနေရာမှာ ကွန်ပျူတာလို့မပြောဘဲ ပစ္စည်းလို့ပဲပြောပါရစေ။ Network တစ်ခုမှာကွန်ပျူတာသာမက Printer နှင့် တစ်ခြားပစ္စည်းတွေပါ Point တစ်ခုအနေနဲ့တိုက်ရိုက်ချိတ်ဆက်လို့ရလို့ပါ။ ဒီတော့ ပစ္စည်းတွေကို တစ်ခုနှင့်တစ်ခုချိတ်ဆက်ရာမှာ ၎င်း Coaxial Cable ကို T-Connector များအသုံးပြုပြီး ချိတ်ပါတယ်။ Cable တစ်လျှောက်လုံးရဲ့အဆုံးနှစ်ဖက်ဆီမှာ Terminator လို့ခေါ်တဲ့ သတ်မှတ်ထားသော Resistor ပါဝင်တဲ့ Special Connector တစ်ခုနဲ့ အဆုံးသတ်ပိတ်ထားရပါမယ်။ ပုံ ၃.၈ မှာ Thinnet Cable နှင့် Network ချိတ်ဆက်ထားပုံကိုပြထားပါတယ်။ ပုံ ၃.၉ မှာ တပ်ဆင်ရာ၌ ပါဝင်သည့်ပစ္စည်းများကို တပ်ဆင်ပုံနှင့်တကွ ပြပေးထားပါတယ်။

၃.၅ Thinnet အကြောင်း

Thinnet က Thinwire ဆိုတဲ့အတိုင်းကြိုးရဲ့အချင်းဟာ ၀. ၂၅လက်မ (စင်တီမီတာနဲ့ပြောမယ်ဆိုရင် တော့ ၀.၆၄ စင်တီမီတာ) ရှိပါတယ်။ ကြိုးကပျော့ပျော့ပါပဲ။ ခွေလို့ ပြုလို့လည်းရပါတယ်။ Flexible ဖြစ်တယ် ပေါ့ဗျာ။ ဒီ Thinwire Cable တွေဟာ ဈေးလည်းသက်သာတယ်။ တပ်ဆင်ရလည်းလွယ်ကူတယ်။ အောက်မှာ Thinwire တွေနှင့်ပတ်သက်နေသောအကြောင်းအရာများကိုဆက်လက်လေ့လာကြည့်ပါဦး။

ပုံ ၃.၇



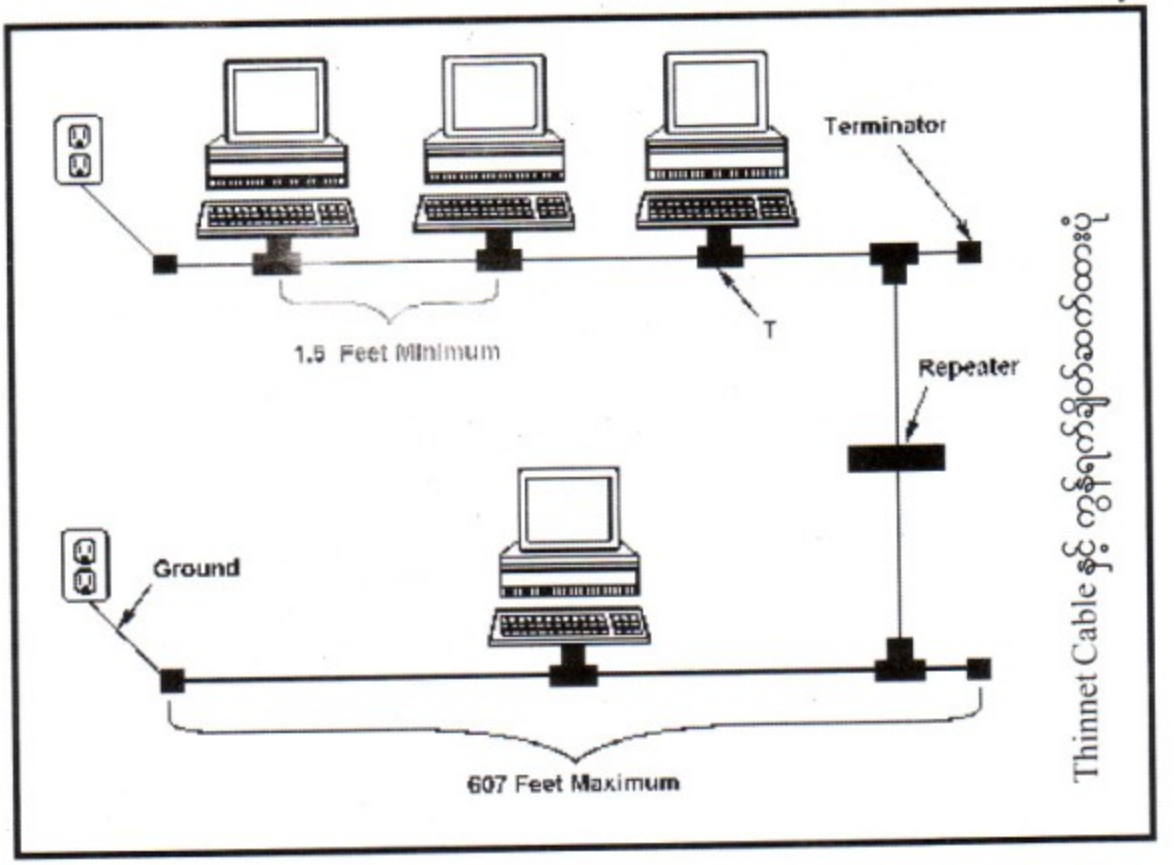
Thinnet ကိုဖြတ်ပိုင်းပုံတွေ့ရစဉ်

Installation တပ်ဆင်ခြင်း

Coaxial Cable ကိုပုံစံနှစ်မျိုးနဲ့ချိတ်ဆက်အသုံးပြုလို့ရပါတယ်။ အဲဒါတွေကတော့ တစ်ခုမှတစ်ခုသို့ ချိတ်ဆက်ခြင်း From Device to Device (Ethernet) နှင့် အလယ်ဗဟိုအမှတ်တစ်ခုမှ တစ်ခုချင်းစီသို့သီးခြား စီချိတ်ဆက်ခြင်း Star (ARCnet) တို့ပဲဖြစ်ပါတယ်။

ဒီနေရာမှာ ကွန်ပျူတာလို့မပြောဘဲ ပစ္စည်းလို့ပဲပြောပါရစေ။ Network တစ်ခုမှာကွန်ပျူတာသာမက Printer နှင့် တစ်ခြားပစ္စည်းတွေပါ Point တစ်ခုအနေနဲ့တိုက်ရိုက်ချိတ်ဆက်လို့ရလို့ပါ။ ဒီတော့ ပစ္စည်းတွေကို တစ်ခုနှင့်တစ်ခုချိတ်ဆက်ရာမှာ ၎င်း Coaxial Cable ကို T-Connector များအသုံးပြုပြီး ချိတ်ပါတယ်။ Cable တစ်လျှောက်လုံးရဲ့အဆုံးနှစ်ဖက်ဆီမှာ Terminator လို့ခေါ်တဲ့ သတ်မှတ်ထားသော Resistor ပါဝင်တဲ့ Special Connector တစ်ခုနဲ့ အဆုံးသတ်ပိတ်ထားရပါမယ်။ ပုံ ၃.၈ မှာ Thinnet Cable နှင့် Network ချိတ်ဆက်ထားပုံကိုပြထားပါတယ်။ ပုံ ၃.၉ မှာ တပ်ဆင်ရာ၌ ပါဝင်သည့်ပစ္စည်းများကို တပ်ဆင်ပုံနှင့်တကွ ပြပေးထားပါတယ်။

ပုံ ၃.၈



Cost (ကုန်ကျစရိတ်)

ကုန်ကျစရိတ်အနေနဲ့ဆိုရင်တော့ တခြားကြိုးတွေထက်စာရင် အနည်းဆုံးကုန်ကျစရိတ်လို့တောင် ပြောလို့ရပါတယ်။ Ethernet ချင်းတူရင်တောင် Thick Ethernet က Thin Ethernet ထက်ပိုကုန်ကျမှုရှိပါတယ်။

Bandwidth Data (အချက်အလက်သယ်ဆောင်နိုင်သောပမာဏ)

LANs မှာတပ်ဆင်အသုံးပြုကြတဲ့ Coaxial Cable ဟာ ARCnet မှာဆိုရင် 2.5 Mbps နဲ့ Ethernet ဆိုရင် 10 Mbps Bandwidth ရှိပါတယ်။ ဒါ Thin Ethernet အတွက်ပြောတာပါ။ Thick Ethernet ဆိုရင် ဒီထက် Bandwidth ပိုပါတယ်။

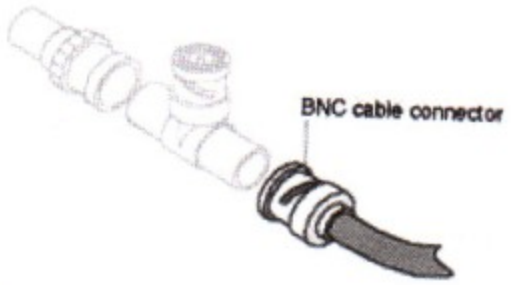
Attenuation (အားနည်းသွားသောအချက်အလက်ပမာဏ)

တကယ်တော့ ဘယ်ကြားခံကြိုးမဆို Attenuation တော့ရှိပါတယ်။ ဒါပေမယ့် Coaxial Cable က တခြား Cable ထက်စာရင် ဥပမာ Twisted Pair လိုကြိုးမျိုးထက်စာရင် Attenuation ပိုကောင်းပါတယ်။ ဆိုလိုချင်တာက Data ဟာတော်ရုံတန်ရုံ Weaken ဖြစ်မသွားဘူးလို့ပြောချင်တာပါ။

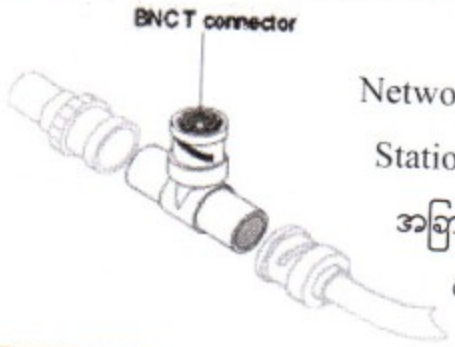
EMI Characteristics (ခြင်ဝန့်ခြင်ရောက်နှောင့်ယှက်မှု)

ဘယ် Copper ကြိုးမဆို EMI ကိုကြောက်ကြရပါတယ်။ သို့သော်ငြားလည်း မောင်မင်းကြိုးသား Coaxial က Shield ပါတာကြောင့် EMI ရဲ့ဒဏ်ကိုအတော်လေးကာကွယ်နိုင်ပါတယ်။

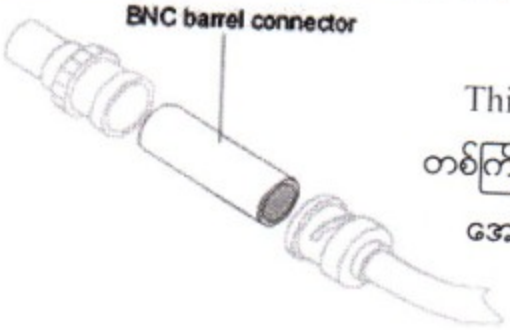
ပုံ ၃.၉



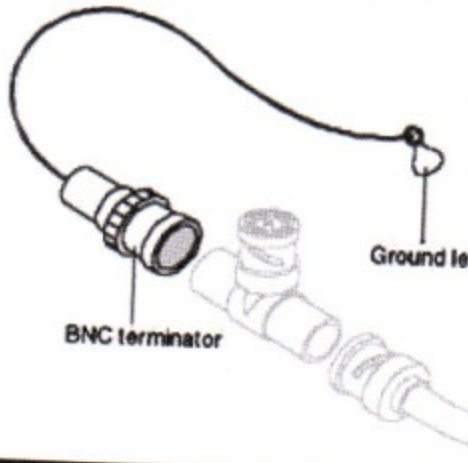
N Series Connector



T Connector
Network Card တွင်တိုက်ရိုက်ချိတ်ရန်
Station တစ်ဖက်ကလာသောကြိုးနှင့်
အခြား Station ကလာသောကြိုး
တို့ချိတ်ဆက်ရာတွင်သုံး



Barrel Connector
Thinnet Cable များ တစ်ကြိုးနှင့်
တစ်ကြိုး လိုအပ်သည့်အလျားထိရောက်
အောင်ချိတ်ဆက်ရာတွင်အသုံးပြု



Terminator
Siganl များကို အဆုံးရှဲ့ စုပ်ယူလိုက်ရာ
တွင်အသုံးပြုသည်။ မဟုတ်ပါက Signal
Bounce ဖြစ်နေလိမ့်မည်။

မှတ်ချက်။ ။ EMI နှင့် Attenuation ကွာခြားချက်မှာ EMI သည် Attenuation လို Cable ပေါ်မှ Signal တာ Transmitter နှင့်ဝေးလာသောအကွာအဝေးကြောင့် Signal များအလိုအလျောက် Data Weaken ဖြစ်လာတာမဟုတ်ဘဲ ပြင်ပမှနောင့်ယှက်မှုကြောင့် Noise များဖြစ်ပေါ်လာခြင်းဖြစ်သည်။

ဥပမာပြောရရင် လျှပ်စစ်ဓါယာကြိုးတွေနှင့် အိမ်တွေဆီကို ဓါတ်အားလွှဲရုံကနေ ဖိအားနှင့် ဓါတ်အားတွေလွှဲလိုက်တဲ့အခါ ၎င်း ဓါတ်အားလွှဲရုံ (Transmitter) နှင့်ဝေးလာလေ ကြိုးရဲ့ Resistance ကြောင့် လိုရာအရောက်တွင် ပို့လိုက်သောဓါတ်အားမပြည့်တော့၊ ထိုအခါ Transformer များနှင့် ဓါတ်အားကိုပြန်တင်လေသည်။ ဒါ Attenuation ပဲ။

Charactristic	Value
Maximum cable length	185 meters (607 feet)
Bandwidth	10 Mbps
Bend radius	360 degrees /ft
Installation/maintenance	Easy to install and reroute; flexible
Cost	Cheapest from of coax cable; prefabricated cables average $1/foot
Connector type	British Naval Connector* (BNC)
Interference rating	Good: lower than thicknet, higher than TP

10Base2 (Thin Net) အကြောင်းသိကောင်းစရာ

10Base2 ဆိုတာ Thin Net ကိုပြောတာပါ။ ယေဘုယျအားဖြင့်တော့ ကွန်ရက်ပေါ်မှာ Signals တွေကို Translate လုပ်ဖို့ Network Card ပေါ်က Transceiver ကိုအသုံးပြုပါတယ်။

မှတ်ချက်။ ။ Transceiver ဆိုသည်မှာ ၎င်းပစ္စည်းတစ်ခုထဲမှာပင် Data တွေကို Transmit လုပ်ပေးသည့် Transmitter လည်းပါရှိပြီး Receive လည်းလုပ်ပေးနိုင်သည့် Receiver လည်းပါရှိပါသည်။ တနည်းအားဖြင့် Transceiver ပစ္စည်းတစ်ခုတည်းတွင် Transmitter ရော Receiver ပါ ပါရှိသည်ဟု ဆိုလိုခြင်းဖြစ်သည်။

ဒီတော့ပြောပြချင်တာက Netwrok Card တစ်ခုဟာ Thin Net အတွက်ရော Network Card ပေါ်က Built In Transceiver က Support လုပ်ပေးတာပါ။ သို့သော် Thick Net အတွက်ကတော့ ဒီ Network Card ပေါ်က Built In Transceiver နဲ့မလုံလောက်တော့ဘူး။ သူ့အတွက် External Transceiver လိုအပ်ပါတယ်။

Thin Net Cabling အတွက် RG-58A/U (သို့မဟုတ်) RG-58 C/U Coaxial Cable ကိုအသုံးပြု

ရမှာဖြစ်ပါတယ်။ တပ်ဆင်ပုံတပ်ဆင်နည်းကတော့ Network Card ပေါ်မှာရှိတဲ့ BNC Connector ကို T-connector နဲ့ချိတ်ဆက်ပြီး Network ကြိုးတွေကို ၎င်း T-Connector တွေမှာ တောက်လျှောက်စီတန်းချိတ်ဆက်ရမှာဖြစ်ပါတယ်။ Connector တွေရဲ့အဆုံးမှာတော့ 50 Ohm Terminator လေးတွေ ပိတ်ပေးထားရပါတယ်။

Advantages 10Base2 (အကျိုးကျေးဇူးများ)

10Base2 ကိုသုံးခြင်းအားဖြင့် ရရှိလာတဲ့အဓိကအချက်ကတော့ ကုန်ကျစရိတ်သက်သာခြင်းပါပဲ။ တနည်းအားဖြင့်ပြောရလျှင်လည်း ဈေးအသက်သာဆုံးလို့ပြောလို့ရပါတယ်။ အဲ့ဒီအပြင်တပ်ဆင်ရတာလည်း လွယ်ကူတယ်။ နောက်ပြီးတော့ ဒီ Network Node တွေက တိုက်ရိုက်ချိတ်လို့ရတယ်။ ကြားခံနောက်ထပ် ဘာပစ္စည်းနဲ့ ကြိုးမှမလိုအပ်ဘူး။ Network ကြိုးကို Network Card ရဲ့ T-Connector မှာချိတ်လိုက်ရုံလို့ ပြောတာပါ။

Troubleshooting 10Base2 (အခြစ်ရှာဖွေခြင်း)

(၁) တစ်ခုနှင့်တစ်ခုကြား အနည်းဆုံး Cable ကြိုးရဲ့အလျားဟာ 1.5 ပေ ဒါမှမဟုတ် 0.5 မီတာရှိရပါမယ်။

(၂) Network Segment တစ်ခုဟာ ၆၀၇ ပေ သို့မဟုတ် ၁၈၅ မီတာထက်ပိုလို့မရပါဘူး။

(၃) T-Connector ဟာ Network Card မှာတပ်ဆင်ရမှာဖြစ်ပါတယ်။

(၄) Network ကြိုးတစ်ခုလုံးဟာ ၃.၃၅ ပေ သို့မဟုတ် ၉၂၅ မီတာကျော်လို့မရပါဘူး။

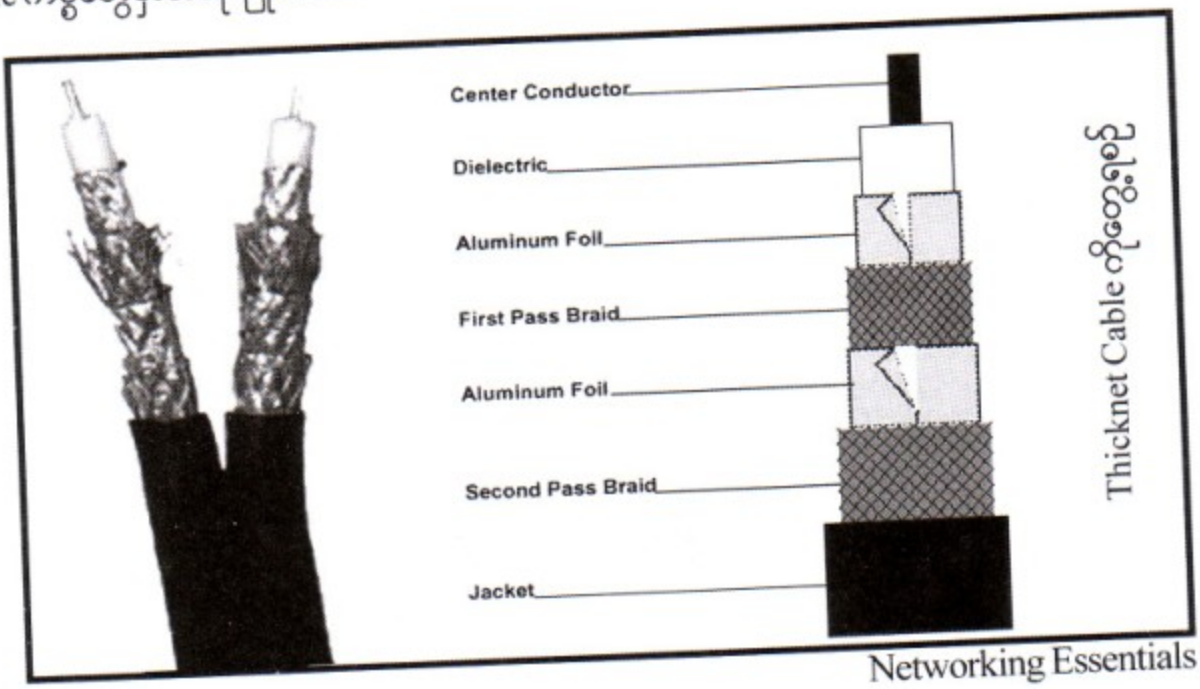
(၅) Network Segment တစ်ခုမှာ အသုံးပြုချိတ်ဆက်ထားတဲ့ပစ္စည်းဟာ Repeaters အပါအဝင် Note အရေအတွက် ၃၀ အများဆုံးပါ။ အစွန်းနှစ်ဖက်မှာ Terminator များမှ တစ်ခုဟာ Ground Wire ရှိနေပြီး ၎င်းကို မီးပလပ်တစ်ခုမှာသေသေချာချာ Screen နဲ့ချိတ်ဆက်တပ်ဆင်ပြီးတော့ Ground ချထားရမှာ ဖြစ်ပါတယ်။

(၆) Network ကြိုးတစ်ခုလုံးမှာ Segments ၅ခုထက်တော့ ပိုလို့မရပါဘူးဗျာ။ ဒီတော့ Segments 5 ထိယူတယ်ပဲထားအုံး။ Segment တစ်ခုစီချိတ်တဲ့ Repeaters ဟာလေးခုထက်တော့မပိုတော့ဘူးပေါ့။ ဘာကြောင့် Thin Net ကို 10Base2 လို့ခေါ်ရသလဲဆိုတော့ သူ့ရဲ့ Bandwidth က 10 Mbps သွားနိုင်ပြီး Maximum Segment အရှည်ဆုံး ၂၀၀ မီတာနီးပါးရတာကြောင့် ၎င်းတို့ကိုအစွဲပြုပြီး 10Base2 လို့ခေါ်ရတာပါ။ အမှန်တကယ် Segment တစ်ခုရဲ့ Maximum Length ၁၈၅ မီတာပါ။ ရှေ့မှာဖော်ပြပြီးခဲ့ပါပြီ။

Thickwire Ethernet

Thickwire Ethenet ဟာအတော်လေးကို တောင့်တင်းမာကြောတဲ့ Coaxial Cable ပဲဖြစ်ပါတယ်။ Cable ရဲ့အချင်းဟာ ၀.၄ လက်မရှိပါတယ်။ စင်တီမီတာနဲ့ပြောရရင်တော့ ၁ စင်တီမီတာရှိပါတယ်။ ကြိုးက အတော်တုတ်တယ်လို့ပြောလို့ရပါတယ်။ ဒီ Thicknet Cable ဟာ ဒီ Networking နည်းပညာမှာ ပထမဆုံး အသုံး Cable အမျိုးအစားဖြစ်တာကြောင့် ၎င်းကို Standard Ethernet လို့လည်းခေါ်ကြပါတယ်။ ဒါပေမယ့် အသုံး ဒီ Cabel ဟာရှေးလည်းကြီး၊ သယ်ဆောင်ရတာလည်းမလွယ်ကူ စတာတွေကြောင့် Ethernet Cabling မှာ အခုဆိုသူ့ကိုသိပ်မရွေးချယ်ကြတော့ပါဘူး။ Thickwire ကြိုးကပိုပြီးတုတ်လာတယ်ဆိုတာ အလည်း ကောင်းတဲ့အချက်ရှိသေးတယ်ဗျ။ အဲ့ဒါကပြင်ပကနှောင့်ယှက်တဲ့အနှောင့်အယှက်တွေကို ပိုပြီး ခံနိုင်ရည်ရှိလာတယ်။ နောက်ပြီး Conductivity ပေါ့။ လျှပ်ကူးတဲ့သဘောကလည်းပိုကောင်းလာပါတယ်။ ဆောင်းမှာပေါ့။ မျက်စိထဲမြင်အောင်ပြောရရင် ဒီ Cable က ကျွန်တော်တို့ ဓါတ်မီးတိုင်ကနေ အိမ်မီတာထဲဝင်တဲ့ 7064 လို Power မီးကြိုးလိုပုံစံပဲလေ။ Copper Wire (Conductor နှန်းမျှင်ကြိုး) ကတုတ်တယ်။ မျှင်မျှင်လေး မဟုတ်ဘူး။ နောက်ပြီး Single တစ်ကြိုးတည်းမဟုတ်ဘူး။ သူ့ကိုခွေထားတဲ့ပုံစံကို မြင်အောင်ပြောရမယ်ဆိုရင် ရစ်ဘီးအကြိုးကြိုးနဲ့ခွေထားရတာ။ ကျွန်တော်တို့လမ်းမမှာ တယ်လီဖုန်းကြိုးတို့ မီးကြိုးတို့ မြေအောက်ထဲချင် ကြိုးကြိုးတွေကရစ်ဘီးအကြိုးကြိုးနဲ့လေ မြင်ဖူးမှာပါ။ အဲ့ဒီသဘောမျိုးခွေထားရတာ။ နောက်ပြီး Cable Length ပေါ့။ အများဆုံးရတဲ့ Cable Segment Length လည်းပိုလာတယ်လေ။ အဲ့ဒီအပြင် Segment တစ်ခုမှာတပ်နိုင်တဲ့ ပစ္စည်းအရေအတွက်လည်းပိုလာပါတယ်။ ဟုတ်တယ်နော်။ ဒီတော့ Signal တွေကိုဝေးဝေး လည်းသယ်ပေးနိုင်တယ်။ Interference ကိုခံနိုင်တဲ့အားကလည်း Thinnet ထက်နှစ်ဆ ပိုကောင်းလာတဲ့ အတွက်ကြောင့် ၎င်းကို Heavy-Duty ကိစ္စတွေ၊ Cable ကိုအရှည်ကြီးဆက်သွယ်ရမယ့် နေရာတွေစတဲ့ Backbone ကိစ္စတွေမှာအသုံးပြုပါတယ်။

ပုံ ၃.၁၀



ကဲ့ Thicknet ကို Backbone အဖြစ်သုံးပြီးအတွင်းမှပြန်လည်ချိတ်ဆက်ခြင်း Interconnect ကို
မျိုး- (ရိုးရိုးပြောစမ်းပါ) - အင်း ရိုးရိုးပြောရရင်ကွန်ပျူတာက Network Card နှင့်ချိတ်ဆက်တဲ့အခါ Thick
လာမချိတ်ဘဲ Thinwire နှင့်ပဲချိတ်ပါတယ်။ ဆိုလိုတာက Thickwire ကို Backbone အဖြစ်အသုံး
ကြပါတယ်။

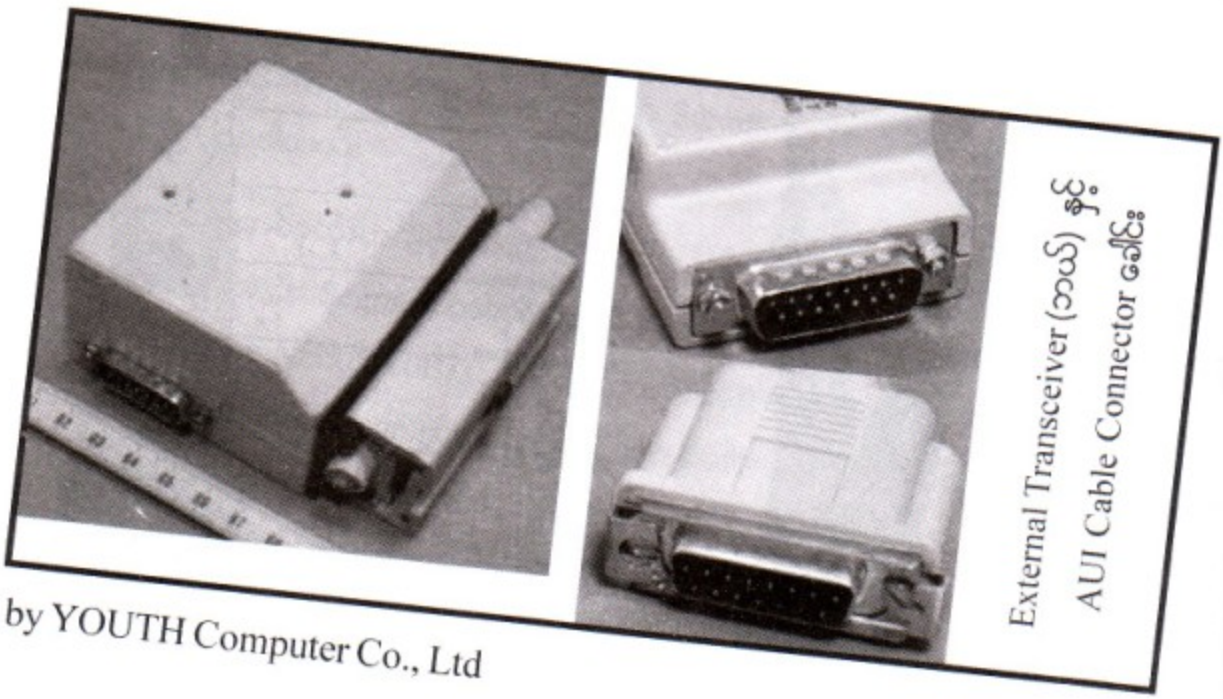
Thicknet ကိုတပ်ဆင်ခြင်း ၀.

အကယ်၍များပေါ့နော်။ ကွန်ပျူတာက Network Card မှာ Thinwire ကိုမတပ်ဘဲ Thickne
ကိုတိုက်ရိုက်လာတပ်မယ်ဆိုရင်-

ကျွန်တော် Thinnet တုန်းကလည်းပြောပြခဲ့ပြီးပါပြီ။ Thicknet အတွက် Network Card ပေါ်မှာပါတဲ့
Transceiver နှင့်မလုံလောက်ပါဘူး။ External Transceiver လိုအပ်ပါတယ်။ ဒီ Thicknet Cable တွေတာ
အဲ့ဒီ Transceiver မှာတပ်ရတာဖြစ်ပါတယ်။ နားလည်လွယ်အောင်အချက်နှင့်ပြောပြမယ်။ ပုံကိုလည်းကြည့်ပေါ့

(၁) ကွန်ပျူတာ Network Card ကနေ Transceiver ကို Transceiver ကြိုးနဲ့ဆက်သွယ်ရမှာဖြစ်ပါ
တယ်။ ၎င်းကို AUI (Attachment Universal Interface) လို့ခေါ်ပါတယ်။ ဒီလိုလေဗျာ။ Net
work Card မှာ Thinnet မှာအသုံးပြုခဲ့တဲ့ BNC Connector လို DIX Connector ဆိုတာရှိ
ပါတယ်။ ဒီတော့ AUI Cable၊ တစ်ဖက်က DIX မှာတပ်၊ နောက်တစ်ဖက်က External Trans
ceiver မှာတပ်။ အခုကွန်ပျူတာနှင့် External Transceiver အဆက်အသွယ်ရသွားပြီဖြစ်ပါတယ်။
ဒီ AUI Cable ဟာ (ကွန်ပျူတာနှင့် External Transceiver အကွာအဝေး) မီတာ ၅၀ ထက်မကျော်
သင့်ပါဘူး။ ပေနှင့်ပြောမယ်ဆိုရင် ၁၆၄ ပေလောက်ရှိပါတယ်။

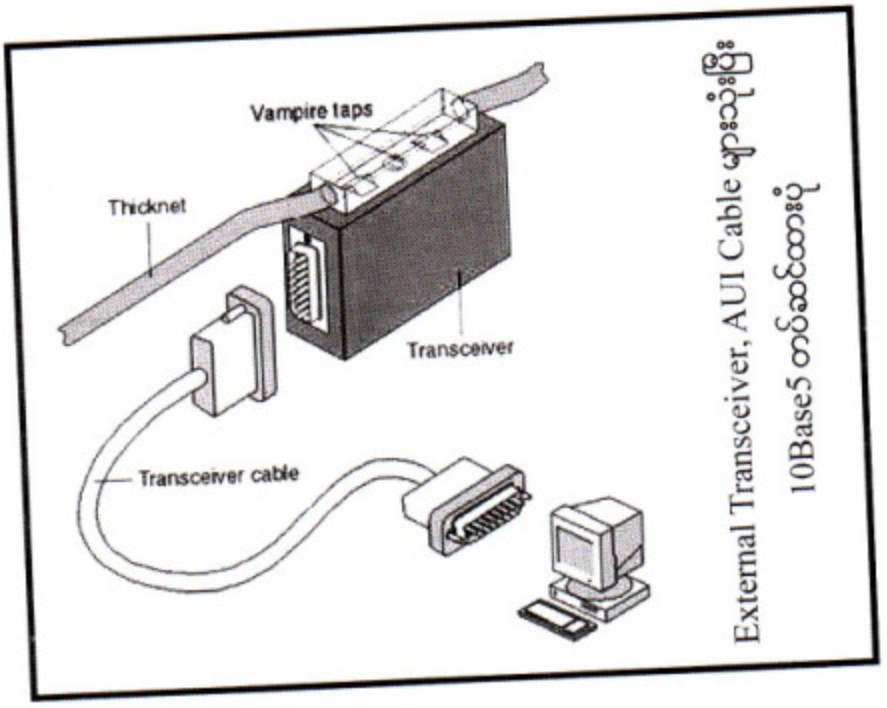
ပုံ ၃.၁၁



External Transceiver (ဘယ်) နှင့်
AUI Cable Connector ခေါင်း

(၂) ပုံမှာပြထားသလို Transceiver တွေကိုတစ်ခုနှင့်တစ်ခု ချိတ်ဆက်ဖို့ကတော့ Thicknet ကိုသုံးပြီး တပ်ဆင်သွားရမှာဖြစ်ပါတယ်။ Thicknet ကို Transceiver မှာချိတ်ရမှာ Vampire Tap ဆိုတာကို အသုံးပြုပါတယ်။

ပုံ ၃.၁၂



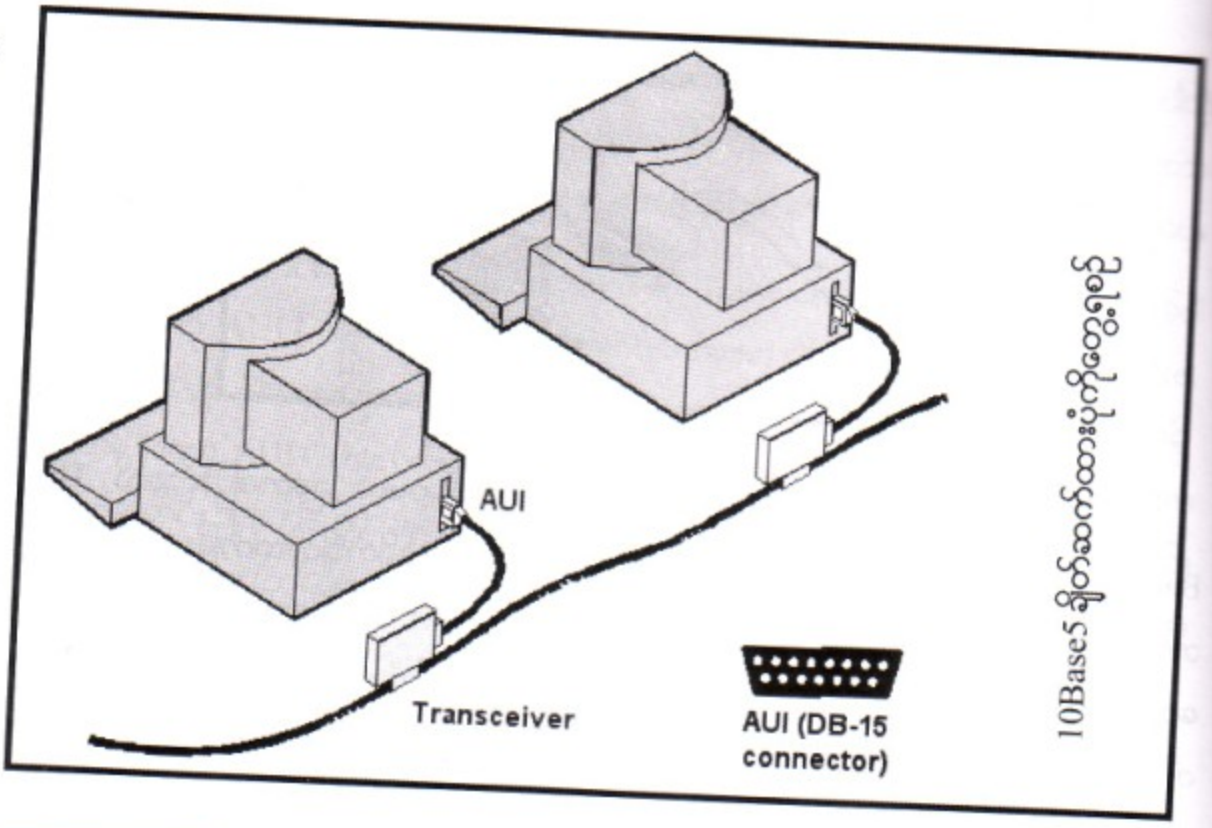
ကဲဘယ်လိုတပ်ဆင်ရမလဲဆိုတာတော့သိသွားပြီ။ ဒါပေမယ့် ခုနကပြောခဲ့သလို Thicknet ကို Backbone အဖြစ်ပဲအသုံးများကြတယ်။ ခုလို ကွန်ပျူတာနှင့် တိုက်ရိုက်ချိတ်ဆက်ပြီး အသုံးပြုမှုနည်းတယ်။ ဘာလို့လဲဆိုတော့ ကြည့်လေ။ Thicknet အပြင် Transceiver တွေလိုအပ်မယ်။ Transceiver Cable တွေလိုအပ်မယ်။ ဒီတော့ ကုန်ကျစရိတ်တက်လာမယ်။ ပြန်ပြောပါအုံးမယ်။ Thicknet ကို ကွန်ပျူတာတွေမှာ တိုက်ရိုက်ချိတ်ရင် Thinnet ထက်ပိုကုန်ကျစရိတ်များတာကြောင့် Thicknet ကို Backbone အဖြစ်ပဲ သုံးပါတယ်။ ပြန်ပြောပါ။ အတန်းထဲမှာဆို စာသင်သားတွေလို ခုလိုပြန်ပြောပါဆိုပြီးမေးလိုက်မယ်။ Thicknet ကိုကွန်ပျူတာနှင့် တိုက်ရိုက်ချိတ်ရင် Thinnet ထက်ဘာကြောင့်ကုန်ကျစရိတ်များရတာလဲ။ အဖြေ Transceiver တွေ၊ Transceiver Cable တွေလိုအပ်လာလို့ပါ။ ဒါကြောင့် Thicknet ကို Backbone အဖြစ်အသုံးများပါတယ်။

10Base5 ရဲ့အဓိကအားဖြင့်ကောင်းမွန်တဲ့အချက်ကတော့ 10Base2 ရဲ့ Cable Length ကနဲ့ သတ်ချက်ကိုကျော်လွန်ပြီး ချိတ်ဆက်နိုင်တာပါပဲ။ ဘာပဲဖြစ်ဖြစ် 10Base5 မှာတော့ သူ့ကိုယ်ပိုင်ကန့်သတ်ချက်ကလေးတွေတော့ရှိပါတယ်။ ဒါကိုတော့သိထားဖို့လိုအပ်ပါတယ်။

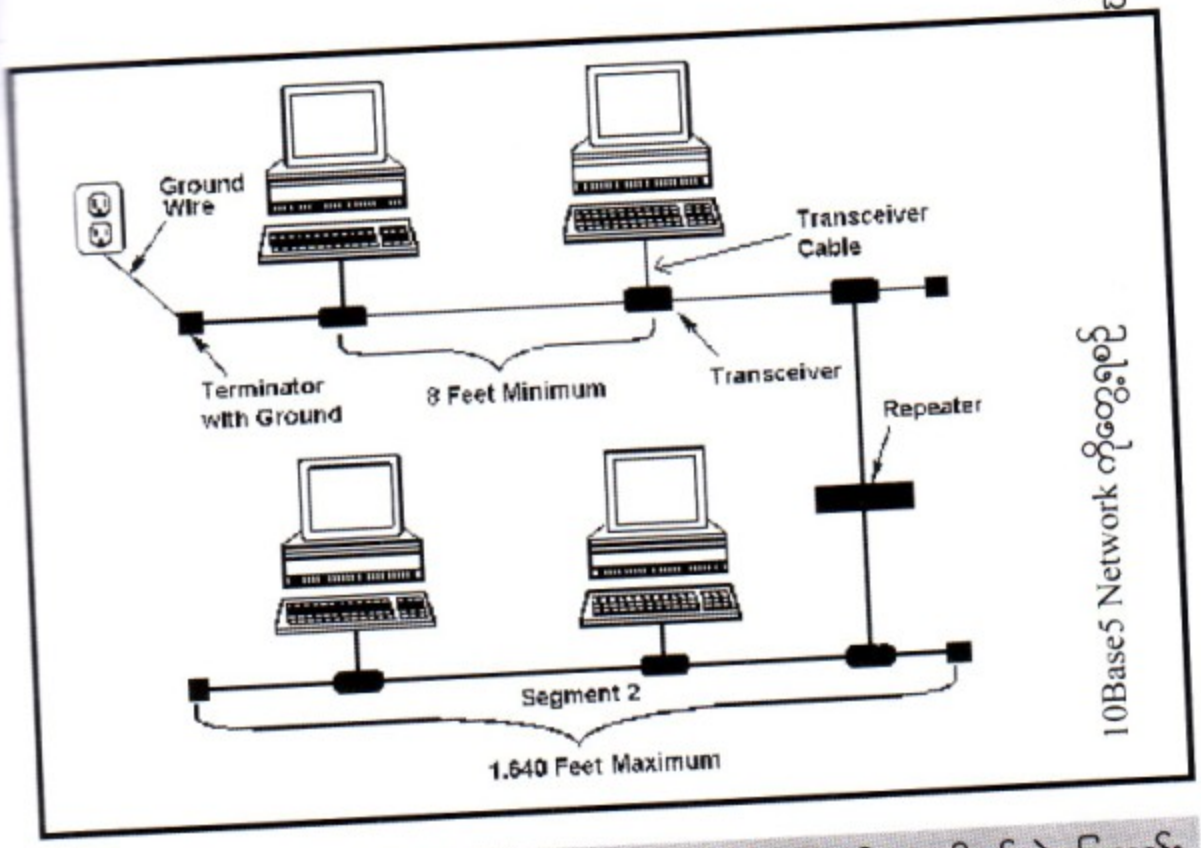
❖ Transceivers နှစ်ခုကြားမှာရှိတဲ့ Cable ရဲ့အကွာအဝေးဟာ အနည်းဆုံး ၂၅ မီတာ ရှိရပါမယ်။ ၂၅၀ မီတာလောက်ပါ။

- Network Segment တစ်ခုရဲ့ အလျားဟာအများဆုံး ၁၆၄၀ ပေ-မီတာ ၅၀၀ ထက်မပိုသင့်ပါဘူး။
- Network ကြိုးတစ်ခုလုံးဟာ ပေ ၈၂၀၀ ဒါမှမဟုတ် မီတာ ၂၅၀၀ ကျော်လို့မရပါဘူး။
- Transceiver နှစ်ခုထဲက တစ်ခုဟာ Ground ချရမှာဖြစ်ပါတယ်။
- Transceiver နဲ့ Network Card ကြားထဲက Cable ဟာ တတ်နိုင်သလောက်တိုရမှာဖြစ်ပါတယ်။ မီတာ ၅၀၀ ထက်တော့ မကျော်သင့်ပါဘူး။
- Network Segment တစ်ခုမှာ Repeater အပါအဝင် Node 10 ထက်မပိုရပါဘူး။

ပုံ ၃.၁၃



Charactristic	Value
Maximum cable length	500 meters (1640 feet)
Bandwidth	10 Mbps
Bend radius	30 degrees /ft
Installation/maintenance	Hard to install and reroute; rigid
Cost	More expensive than thinwire, cheaper than fiber
Connector type	(BNC)
Interference rating	Good: lowest of all electrical cable types



10Base5 Network ကိုတွေ့ရဉီ

ချက်။ ။ Ethernet မှာအသုံးပြုခဲ့တဲ့ Coaxial Cable တိုင်းဟာတပ်ဆင်ရာမှာလိုအပ်တဲ့အခြားစွဉ်း
းတွေကတော့ BNC Connector နှင့် Cable တွေရဲ့အဆုံးမှာတပ်ပေးရတဲ့ Terminator တွေပါဖြစ်ပါတယ်။
erminator ဆိုတာတကယ်တော့ Resister တွေပါပဲ။ Coaxial Cable တွေဟာ Terminator မတပ်ထားရင်
ဆော်လည်းကောင်း၊ သေချာမတပ်ရင်သော်လည်းကောင်းအလုပ်မလုပ်နိုင်ပါဘူး။ ဒီလိုပါ။ သေချာမတပ်ဘူး
ဆိုတာ ကြိုးကအသုံးပြုတဲ့ Resister Ohm နှင့် Terminator ရဲ့ Resister က Ohm တို့တူရမယ်။ ဒါမှ
Coaxial Cable တွေကအလုပ်လုပ်တယ်။ Terminator ဆိုတာ Cable တစ်လျှောက်စီးဆင်းလာတဲ့ Sig-
nals တွေကိုစုပ်ယူထားလိုက်တာဖြစ်ပါတယ်။ အဲဒီမှနောက်ထပ် Signal တွေထပ်မံသွားလာလို့ရမှာဖြစ်ပါတယ်။

၁း၃ အခြားသော Coaxial Cable များ

Coaxial Cable မှာ Thinnet နှင့် Thicknet အပြင်အခြားသော Coaxial Cable တွေရှိသေးတယ်ဆို
ာကိုပြောခဲ့ပြီးပါပြီ။ ဒီအထဲမှာအကျဉ်းချုပ်အနည်းငယ်ပြောပြချင်တဲ့ Cable ကတော့နှစ်မျိုးရှိပါတယ်။ တစ်ခုက
တော့ Broadband Cable Television မှာသုံးတဲ့ CATV System ကြိုးရယ်၊ နောက်တစ်ခုက ARCnet
Network တွေမှာသုံးတဲ့ Cable ရယ်ဖြစ်ပါတယ်။

ARCnet ဆိုတာ Attached Resource Computing Network ဖြစ်ပါတယ်။ ၁၉၈၀ ခုနှစ်က
Data Point ကော်ပိုရေးရှင်းကထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ Bandwidth ကတော့ 2.5Mbps ပဲရပါတယ်။
ဒီအချက်ကြောင့်ယနေ့ခေတ်ကွန်ရက်တွေမှာအသုံးနည်းလာရခြင်းပဲဖြစ်ပါတယ်။ ဒီ RG-62 ဆိုတဲ့ ARCnet

Cable ဟာ 93Ohm ရှိပြီး နဂိုမူလတုန်းက Mainframe တွေကိုချိတ်ဆက်အသုံးပြုတဲ့ IBM 3270 Terminals တွေမှာချိတ်ဆက်အသုံးပြုဖို့ဖြစ်ပါတယ်။

နောက် CATV Cable အဖြစ်နဲ့အသုံးပြုတဲ့ကြိုးအမျိုးအစားနှစ်မျိုးကတော့ RG-59 နှင့် RG-6 Cable တို့ဖြစ်ကြပါတယ်။ ၎င်းနှစ်မျိုးစလုံးဟာ 75Ohm တွေဖြစ်ကြပါတယ်။ RG-6 ကတော့ လိုင်းတွေကို ပွားထုတ်တဲ့နေရာမှာအသုံးပြုပြီး RG-59 ကတော့တစ်အိမ်ချင်းစီကိုတိုက်ရိုက်ချိတ်ဆက်ရာမှာအသုံးပြုပါတယ်။ နောက် Heavy Duty တွေအဖြစ်အသုံးပြုတဲ့ CATV Cable တွေကြတော့ RG-11 ကိုအသုံးပြုပါတယ်။

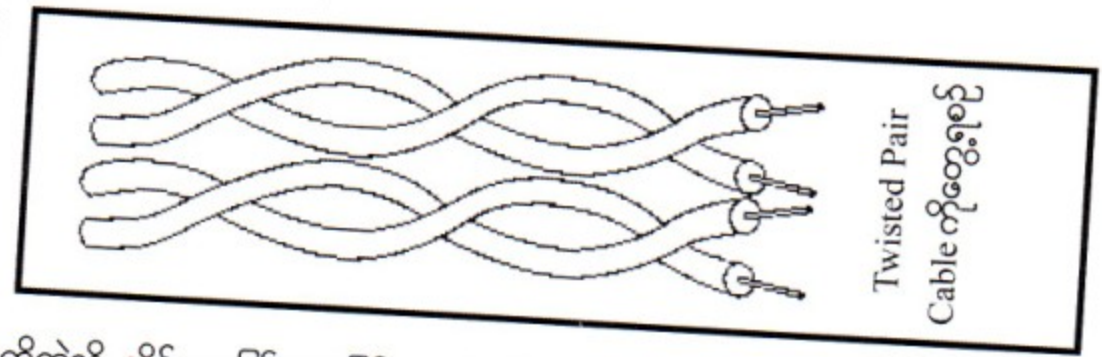
၃.၈ Twisted Pair Cable အကြောင်း

Copper Cable တွေထဲမှာတော့ ဒီဘက်ခေတ်မှာ အတော်ကိုထင်ရှားတဲ့ Cable ပဲဖြစ်ပါတယ်။ သူကိုထင်ရှားကျော်ကြားလာစေတဲ့ အချက်တွေအများကြီးထဲမှာ တပ်ဆင်ရာမှာ စရိတ်ကသက်သာခြင်းလည်း ပါဝင်နေပါတယ်။

Twisted Pair ဆိုတာ တကယ်တော့ Copper Wire နှစ်ကြိုးကို အတူတကွလိမ်ပတ်ထားတာပဲဖြစ်ပါတယ်။ အဲဒီလိုလိမ်ထားခြင်းဟာ Twisted Pair Cable ရဲ့အဓိကကျတဲ့ အချက်ပဲဖြစ်ပါတယ်။ ကြိုးကိုလိမ်ထားခြင်းအားဖြင့် Copper Cable တွေရဲ့ EMI အပေါ်တိမ်းညွတ်မှုကိုလည်း လျော့ချပေးသည်။ ထို့အပြင် မိမိကြောင့်ဖြစ်ပေါ်သည့် ရေဒီယိုလှိုင်း (Radio Frequency) ပျံနှံ့မှုနှုန်းကိုလည်း ၎င်းအနီးနားရှိ တခြားကြိုးများနှင့် လျှပ်စစ်ပစ္စည်းများမထိခိုက်အောင် လျော့ချပေးသည်။

ဥပမာပြောရရင် TV Antenna တွင်အသုံးပြုသောကြိုးအပြား (Shield လိုကြိုးအလုံးမဟုတ်) Radio Frequency Signals များ တမင်တကာ Radiate ဖြစ်နေစေရန်ကြိုးကိုလိမ်မထားဘဲ အပြိုင်ထားထားခြင်းဖြစ်သည်။

ပုံ ၃.၁၅



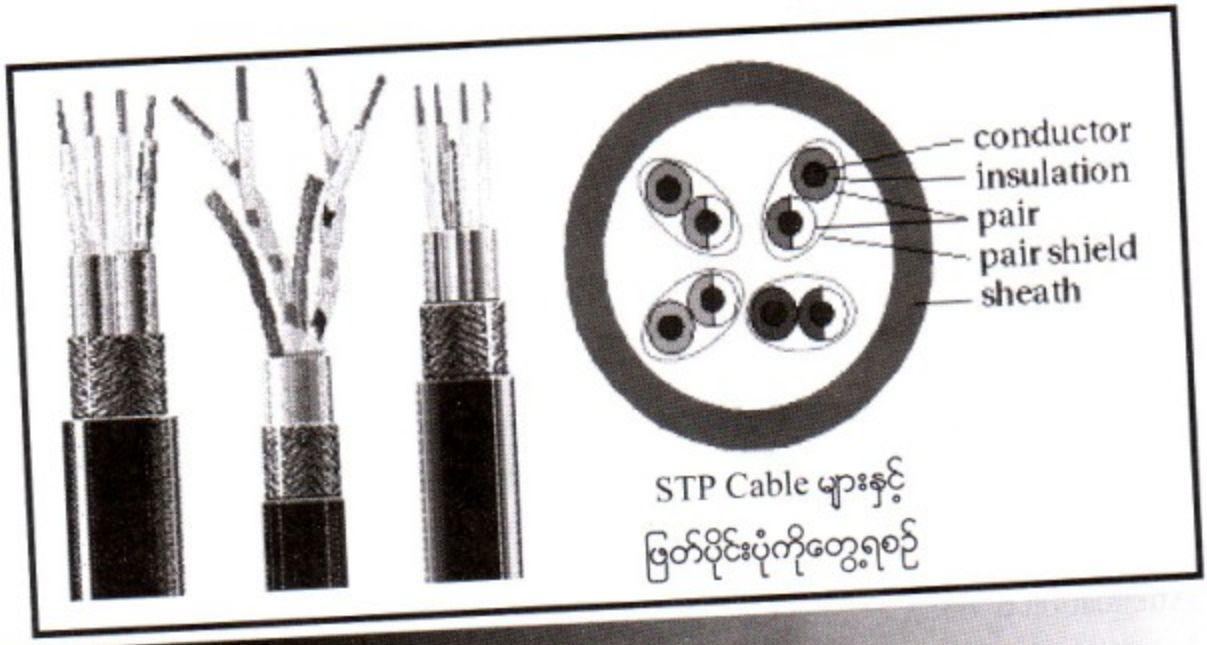
ထိုကဲ့သို့ လိမ်ထားခြင်းအားဖြင့် အချင်းချင်း EMI ဖြစ်မှုကိုလည်း ထိန်းချုပ်ပေးထားပြန်သည်။ တိယာကြိုးနှစ်ခုကို အနီးအနားထားလျှင် တစ်ခုမှတစ်ခုသို့ အချင်းချင်း Noise တွေထုတ်လွှတ်တတ်သောသဘောရှိလေသည်။ ၎င်းဖြစ်တတ်သည့်သဘောကို Crosstalk ဟုခေါ်လေသည်။ ကြိုးကိုယခုကဲ့သို့ အစုလိုက်လိမ်ထားခြင်းအားဖြင့် Crosstalk ဖြစ်မှုကိုလည်းလျော့ချပေးလေသည်။ LANs မှာအသုံးပြုတဲ့ Twisted

Pair Cable နှစ်မျိုးရှိပါတယ်။ Shielded (Shield ပါတာနဲ့) နှင့် Unshielded (Shield မပါတာ) တို့ပဲဖြစ်ပါတယ်။ Twisted Pair Wire ကြိုးတွေဟာ Shield ပါတာရော၊ Shield မပါတာရောပုံစံအမျိုးမျိုးလာကြတာ။ Pair ဆိုတဲ့အစုံအနေနဲ့ ၁စုံ၊ ၂စုံ၊ ၄စုံ၊ ၆စုံ စသဖြင့်ရှိကြပါတယ်။

Shield Twisted Pair (STP) အကြောင်း

STP ဆိုတဲ့အတိုင်း Shielded ဆိုတဲ့အတိုင်းပါပဲ။ ကြိုးမှာ Shield ပါပါတယ်။ ဒီလို Shield ပါလာခြင်းကြောင့် Crosstalk ကိုလျှော့ချနိုင်တဲ့အပြင် EMI ဆိုတဲ့ External Interfarence ကိုလည်း လျှော့ချပေးနိုင်ပါတယ်။ ဒီ STP Wire အတွင်းမှာ Shield တာသံဇကာအကွက်ပုံစံအားလုံးကိုအပေါ်ကနေ အုပ်ပြီးပတ်ပတ်လည်ပါတဲ့အပြင် များသောအားဖြင့် STP Cable တော်တော်များများဟာတစ်ကြိုးချင်းစီမှာပါ အပေါ်ကပတ်အုပ်ထားတဲ့ Shield ပါရှိပြန်ပါတယ်။ အဲသလိုကောင်းမွန်တဲ့ Shield ပါရှိခြင်းကြောင့် STP တာ Cable Transmission ပိုင်းဆိုင်ရာ၊ Interference ပိုင်းဆိုင်ရာပိုကောင်းပါတယ်။ UTP ထက်စာရင် တောင် ပိုဝေးဝေးနှင့်ပိုကြိုးတဲ့ Bandwidth နှင့်သွားနိုင်ပါတယ်။

ပုံ ၃.၁၆



STP Cable များနှင့်
ဖြတ်ပိုင်းပုံကိုတွေ့ရစဉ်

Cost (ကုန်ကျစရိတ်)

STP Cable ဟာ Thin Coaxial နဲ့ နောက်ပြီးရင်ပြောပြမယ့် Unshielded Twisted Pair (UTP) ထက်စာရင်တော့ ကုန်ကျစရိတ်ပိုတယ်ဆိုပေမယ့် Thick Coaxial နဲ့ Fiber Optic တို့ထက်တော့ ကုန်ကျစရိတ် သက်သာပါတယ်။

Installation (တပ်ဆင်မှု)

မတူညီတဲ့ကွန်ရက်အမျိုးအစားတွေပေါ်မူတည်ပြီး တပ်ဆင်ရာမှာ လိုအပ်တဲ့အချက်တွေကလည်း

ကွဲပြားသွားပါတယ်။ အဓိကကွာခြားသွားတာကတော့ Connector ပါပဲ။ ဥပမာ Apple Talk ဆိုရင် ကြိုးဆင်ရာမှာ Connector ကို ခဲလည်းဆော်ရမယ်။ နောက်ပြီး ကြိုးတပ်ဆင်ပုံနဲ့ပတ်သက်ပြီး အလေ့အကျင့်ရှိထားဖို့လည်းလိုအပ်တယ်။ IBM Token Ring ကြတော့ Unisex ဆိုတဲ့ Data Connector ကိုသုံးတယ်။ ခေါင်းနာမည်ကထူးဆန်းတယ်နော်။ Unisex တဲ့။ ဘာဖြစ်လို့လဲဆိုတော့ ၎င်း Connector မှာ Male ရော Female ရောပါနေလို့ပါ။ သူကြတော့ သုံးရိုးသုံးစဉ်ဖြစ်တဲ့ ဓားတို့ ပလာရာအကြိုးတို့နဲ့တပ်ဆင်ဖို့အတွက် သူတို့ရှိရင်လုံလောက်ပါတယ်။

ဒါပေမယ့် IBM Data Connector ကတော့ Pins နှင့် Socket နှစ်ခုပေါင်းမှတစ်ခုမဟုတ်ဘဲ။ Connector တစ်ခုတည်းမှာ Pins ရော Socked ပါ တစ်ခါတည်းတွဲပါတာကြောင့် သူကို Unisex Connector လို့ခေါ်ပါတယ်။ IBM Data Connector တစ်ခုဟာ တခြား IBM Data Connector တစ်ခုကို ချိတ်ဆက်နိုင်ပါတယ်။ ဒီထက်ပိုထူးခြားတာတွေက STP Cable တွေဟာ အတော့်ကိုကြီးတာပါပဲ။ IBM Type 1 Cable ဆိုရင် အချင်း 1½ လက်မရှိပါတယ်။ ကဲစဉ်းစားသာကြည့်ပေတော့။ သယ်ဖို့ပြုဖို့တောင် အတော်လေး ဒုက္ခရောက်မယ်။

Capacity (အချက်အလက်သယ်ယူနိုင်စွမ်းဆောင်ရည်)

STP Cable တွေဟာ သိအိုရီအရတော့ 500 Mbps လောက် Bandwidth ရှိပါတယ်။ သို့သော်လည်း Meter 100 လောက်ရှည်တဲ့ Connection ဆိုရင်တော့ 15 Mbps လောက်ပဲရှိပါတော့တယ်။ ဒါပေမယ့် STP ကလည်းအခက်သားလား။ သူကအမျိုးမျိုးသော ပုံစံရှိနေတာကြောင့် Token-Ring Network တွေရဲ့ Bandwidth ဆိုရင်ကတော့ 16 Mbps ပါပဲ။

Attenuation (အားနည်းသွားသောအချက်အလက်ဆောင်ရည်)

အနည်းငယ်သော ရာဂဏန်းမီတာလောက်အရှည်ရှိတဲ့ ဒီ Twisted Pair ကြိုးအမျိုးမျိုးတို့ဟာ Attenuation ရဲ့ ကန့်သတ်ခြင်းကိုခံကြရတယ်ဆိုပေမယ့် တကယ်တမ်းကြတော့ Meter 100 ကိုတောင် မလွန်ဆန်နိုင်ကြပြန်ပါဘူး။

EMI Characteristics (ပြင်ပမှဝင်ရောက်နှောင့်ယှက်မှု)

Coaxial Cable တုန်းကလိုပါပဲ။ Shield ပါတဲ့အတွက်ကြောင့် EMI ကိုခုခံနိုင်မှုဟာ အတော်လေးကောင်းလာပါတယ်။ ဒါက တချို့သော အခြေအနေတွေမှာ Unshielded Twisted Pair ဆိုတဲ့ UTP Cable အစား STP ကိုရွေးသင့်တဲ့အချက်တစ်ချက်ပဲပေါ့။

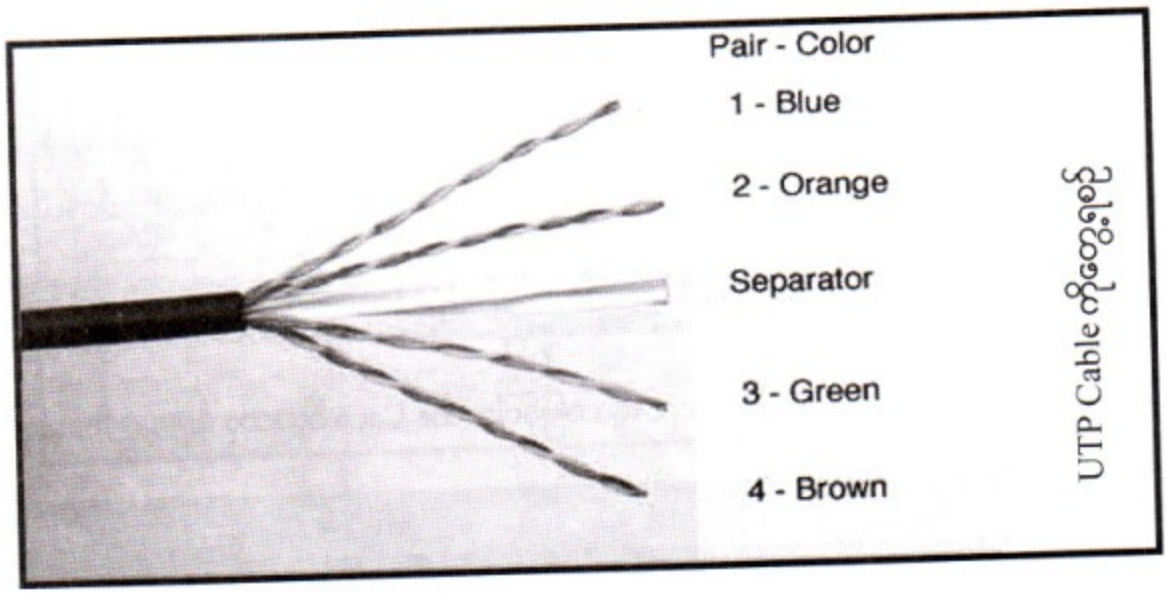
၃.၁၀ Unshielded Twisted Pair Cable အကြောင်း

UTP ကို IEEE ရဲ့ Ethernet Specification အရပြောရင် 10BaseT လို့ခေါ်ပါတယ်။ ဒီနေရာမှာ T က UTP ကိုပြောတာဖြစ်ပါတယ်။

Unshield Twisted Pair ဆိုတဲ့အတိုင်း UTP ဟာ Lock of Shield (Shield မပါ) ပါ။ EMI နဲ့ Attenuation ကလွဲလို့ UTP ဟာ STP နဲ့အချို့အချက်တွေမှာ သွားတူနေပါတယ်။ ကြိုးကကြိုးထဲမှာပဲ လိမ်ထားတဲ့ကြိုးအစုံလေးတွေ ပါဝင်ပါတယ်။ အဲဒီကြိုးအစုံလေးတွေဟာ အစုံမှန်းသိအောင် အရောင်နဲ့ ခွဲခြားပြထားပါတယ်။

UTP ရဲ့အများဆုံးသော Segment အလျားဟာ မီတာ ၁၀၀။ ပေနဲ့ပြောရင် ၃၂၈ ပေရှိပါတယ်။ UTP Cable ကို EIA လို့ခေါ်တဲ့ Electronic Industries Alliance နှင့် TIA လို့ခေါ်တဲ့ Telecommunications Industries Associations နောက် ANSI လို့ခေါ်တဲ့ American National Standards Institute သူတို့သုံးအုပ်စုက Commercial Building Wiring Standard ဆိုပြီး ANSI / EIA / TIA 568 ကို သတ်မှတ်ခဲ့ပါတယ်။ အဲဒီသတ်မှတ်ချက်အရ UTP မှာ Cable အမျိုးအစား ၅ မျိုးရှိပါတယ်။ Category 1 to 5 အထိရှိပါတယ်။ ကျွန်တော်တို့ကတော့အတိုကောက် Cat 1, Cat 2 စသဖြင့်ပဲ အတိုကောက်ပြောပါတယ်။

ပုံ ၃.၁၇



Category 1

Telephone ကြိုးအဖြစ်အသုံးပြုကြပါတယ်။ ၎င်းဟာ Voice အဆင့်ကိုပဲသယ်ဆောင်နိုင်ပါတယ်။ Data မသယ်ဆောင်နိုင်ပါဘူး။

Category 2

ဒင်းမှာ Wire ကြိုး ၄ စုံရှိပါတယ်။ Bandwidth ကတော့ 4 Mbps အထိရပါတယ်။ ဒင်း 4 Mbps ဟာ Network လောကအတွက်တော့ နှေးလွန်းပါတယ်။ ဒါကြောင့် CAT 2 ကို Network လောကမှာ အသုံးပြုခဲပါတယ်။

Category 3

ဒင်းကတော့ Bandwidth 10 Mbps ရပါတယ်။ အင်း 16 Mbps လောက်အထိရပါတယ်။ ဒင်းဟာ Data Grade Cable ဖြစ်ပေမယ့် အခု ဒီ Cat 3 ကိုတယ်လီဖုန်းစနစ်တွေမှာ စံအဖြစ်အသုံးပြုနေပါပြီ။

Category 4

ဒင်းကတော့ Bandwidth 16 Mbps - 20 Mbps လောက်အထိရပါတယ်။ ဒင်းမှာ Wire ကြိုးလေးစုံ ပါရှိပါတယ်။ ဒင်းကို Voice ထက်စာရင် Data တွေသယ်ဖို့အတွက်အသုံးပြုကြပါတယ်။

Category 5

ဒင်းကတော့ Bandwidth က 100 Mbps ရှိပါတယ်။ Cat 5 ဟာ Wire ကြိုးလေးစုံပါရှိပါတယ်။ Data Grade Cable ဖြစ်ပါတယ်။ Ethernet Cabling မှာ ဒီ Cat 5 တစ်မျိုးပဲအသုံးပြုပါတယ်။

Category 6

အခုနောက်ပိုင်း Cat 6 ဆိုတာလည်းရှိလာပြန်ပါတယ်။ Cat 6 ကတော့ 1000 Mbps ဖြစ်ပါတယ်။ Data Grade ဖြစ်ပါတယ်။

Cost (ကုန်ကျစရိတ်)

UTP Cable ဟာ မည်သည့် Cable အမျိုးအစားနှင့်မဆို ဈေးအနည်းဆုံးဖြစ်ပေမယ့် Category 5 ကတော့ အတော်လေးကုန်ကျစရိတ်ရှိနေပြန်ပါတယ်။ ဒီကနေ့ UTP နဲ့ကွန်ရက်ဆင်မယ်ဆိုရင်လည်း Cat 5 ကိုပဲအသုံးပြုရမယ်ဆိုတာ သိထားပါအုံး။

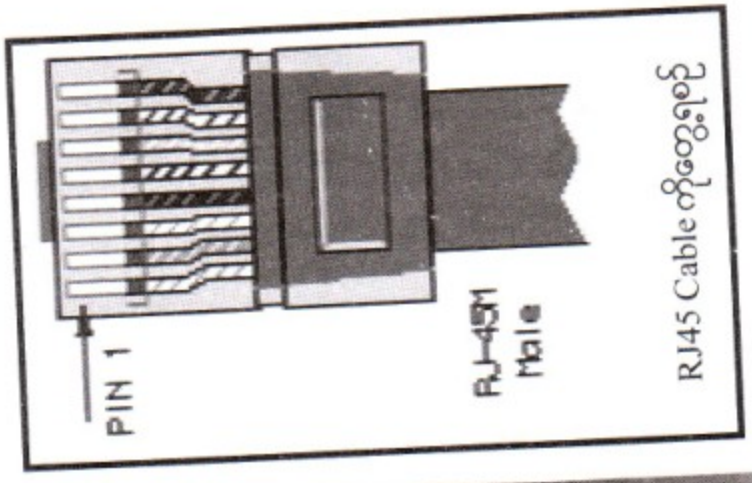
Installation (တပ်ဆင်ခြင်း)

UTP Cat 5 ကိုတပ်ဆင်ဖို့အတွက်ကတော့ Knife တို့ Wire Stripper တို့ ညှပ်တဲ့ Clipper တို့ လိုအပ်ပါတယ်။ အထူးတလည် သင်ကြားတတ်မြောက်ထားဖို့လည်းလိုပါတယ်။

အခုလိုကြိုးတွေညှပ်တဲ့နေရာမှာ မိမိတွင် Cable Tester ပေါ့။ ညှပ်ပြီးသားကြိုးတွေကို ကောင်းကောင်း ပြန်စစ်ဆေးလို့ရတဲ့ ကိရိယာလေးရှိနေရင်အဆင်ပြေပါတယ်။ ကြိုးရဲ့ အပြင် Cover ကိုလိုသလောက် ချွတ်ပါတယ်။ အထဲမှာ ဝါယာကြိုးရှစ်ကြိုးထွက်လာတယ်။ ရှစ်ကြိုးဆိုတော့ လေးစုံပေါ့။ အဲဒီတုန်းက အရောင် တူတာလေးတွေကို Twist လုပ်ပြီး လေးစုံရတော့ Connector ထဲကိုထိုးထည့်လိုက်ပါတယ်။ ထိပ်ဖျား လေးတွေ ညီညီညာညာနဲ့ Connector ထဲကိုဝင်ရောက်သွားဖို့လိုအပ်ပါတယ်။ အဆင့်တိုင်းမှာ Cat 5 ရဲ့ နှုန်းအတိုင်းဖြစ်စေဖို့ ဂရုပြုဆောင်ရွက်ရပါတယ်။ ပြီးတော့မှ Clipper ထဲထည့်ပြီး ဖိချလိုက်ရပါတယ်။ အဲဒီအခါ Clipper ထဲကအသွားကလေးတွေဟာ ခုနက ဝါယာကြိုးရှစ်ကြိုးကို ကိုက်ဖောက်လိုက်သလို ဖြစ်သွားပြီး အပြင်ပလပ်စတစ်ပြုသွားပြီး အတွင်း Copper ပေါ်လာပါတော့တယ်။ ၎င်း Copper က Connector ရဲ့ Conductor အပိုင်းနဲ့သွားထိဖို့လိုအပ်ပါတယ်။

အဲဒီတော့မှ Communicate လုပ်လို့ရမှာပါ။ အခုပြောခဲ့တဲ့ အဆင့်တွေမှာ တစ်ခုခုလွဲချော်သွားလို့ မရပါဘူး။

ပုံ ၃.၁၈



Capacity (စမာဏ)

Cat 5 ကတော့ 100 Mbps Bandwidth ပါပဲ။

Attenuation (အားနည်းသွားသောအချက်အလက်စမာဏ)

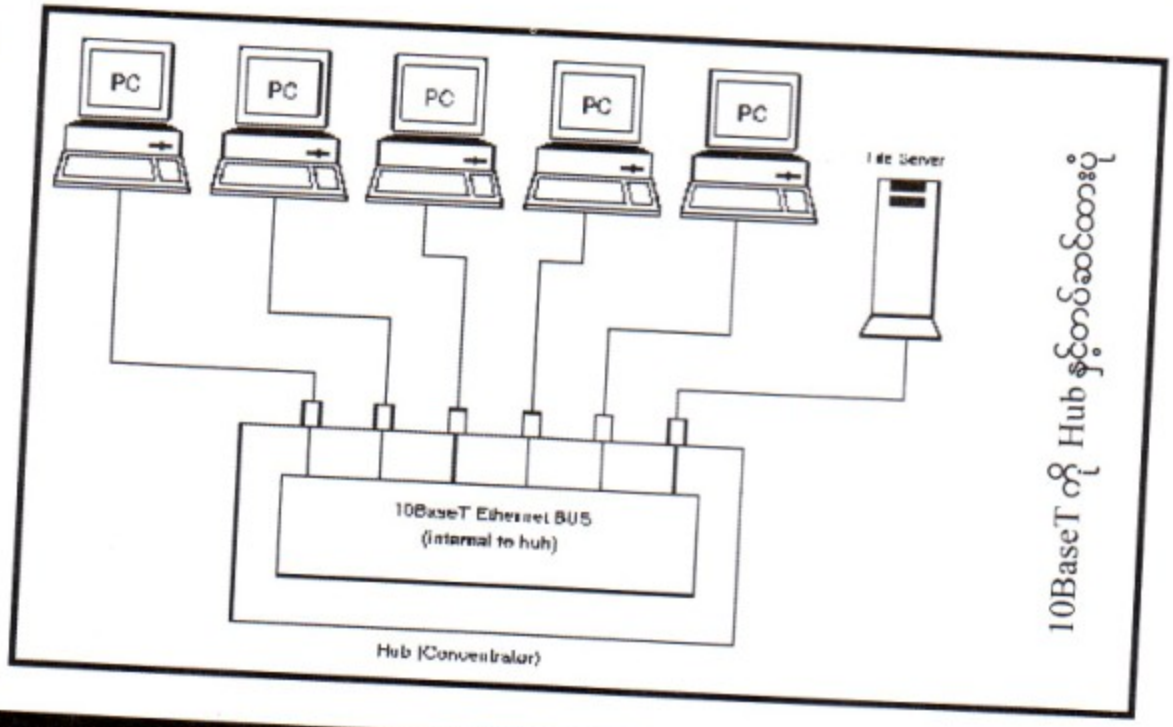
UTP Cable တွေဟာ အနည်းငယ်သော ရာဂဏန်းအထိ ရှည်လျားနိုင်တယ်ဆိုပေမယ့် များသော အားဖြင့် Meter 100 မှာ သွားအဆုံးသတ်ဖို့တော့ပြောချင်ပါတယ်။

EMI Characteristics (ပြင်ပမှဝင်ရောက်နှောင့်ယှက်မှု)

Shield မပါတဲ့အတွက်ကြောင့် UTP ကြိုးတွေဟာ EMI ကို Coaxial နဲ့ STP ကြိုးတွေထက်ပိုပြီး တိမ်းညွတ်လွယ်ပါတယ်။ ဒီတော့ Motor တွေ၊ မီးချောင်းတွေနားမှာ UTP ကိုဖြတ်သန်းပြီးမတပ်ဆင်သင့်ပါဘူး။ နောက်ပြီး Noise တွေထုတ်လွှတ်နိုင်တဲ့ စက်ရုံအတွင်းမှာလည်း UTP ကိုသုံးဖို့မသင့်လျော်ပါဘူးလို့ အကြံပေးပါရစေ။

10BaseT ဆိုတာ Unshielded Twisted Pair ကိုပြောတာပါ။ Fiber Optic ကိုသာ Ethernet LAN မှာအသုံးမပြုခဲ့ဘူးဆိုရင် သင်ဟာ UTP ကိုရွေးမိမှာပါပဲ။ UTP ဟာ IEEE 802.3 Standard ကို အခြေခံထားတဲ့ရေပန်းစားလှသော Cable ပဲဖြစ်ပါတယ်။ 10BaseT ဟာ Star Topology မှာသုံးဖို့ဖြစ်ပါတယ်။ Topology ကဲ့သွားတာကလွဲလို့ကျန်တဲ့ Function တွေအားလုံးဟာ Linear Bus နဲ့အတူတူလောက်ပါပဲ။ 10BaseT ဟာ RJ-45 Connector ကိုအသုံးပြုပါတယ်။ Network Card တွေမှာ BNC Connector ရယ်၊ RJ-45 Connector ရယ်၊ DIX Connector ရယ်တွေဟာ တစ်ခု (သို့မဟုတ်) နှစ်ခု (သို့မဟုတ်) အားလုံးပါတတ်ကြပါတယ်။ ပုံမှာ Ethernet UTP ကိုဘယ်လိုတပ်ဆင်အသုံးပြုရသလဲဆိုတာကို ပြထားပါတယ်။ အဲဒီမှာပြထားတဲ့ Hub ကိုတနည်းအားဖြင့် Concentrator လို့ခေါ်ပါတယ်။

ပုံ ၃.၁၉



Advantages of 10BaseT (အကျိုးကျေးဇူးများ)

10BaseT ကိုအသုံးပြုခြင်းအားဖြင့် များစွာသောအကျိုးကျေးဇူးတွေကိုရရှိစေပါတယ်။ အဓိကအားဖြင့် 10BaseT ဟာကြိုးတွေ တစ်နေရာတည်းမှာသွားစုံစေတဲ့ Centralized က တနည်းအားဖြင့် Con-

centrator ကိုအသုံးပြုတာကြောင့် Network ကို Manage လုပ်ရတာဟာ အင်မတန်လွယ်ကူစေပါတယ်။ အဲဒီအပြင် Linear Bus လို တန်းဆက်မဟုတ်တာကြောင့် Network ဟာပိုပြီးစိတ်ချရမှုနဲ့ ပြည့်စုံနေပါတယ်။ ပုံမှာပြထားသလိုပါပဲ။ Node တွေဟာ Hub ဆီကိုသီးခြား Cable Segment အနေနဲ့ ဆက်သွယ်ထားတာကြောင့် Segment တစ်ခုမှာပြဿနာပေါ်ပေါက်နေသော်လည်း တခြား တခြားသော Segment တွေဟာ အနှောင့်အယှက်ကင်းစွာနဲ့ အလုပ်လုပ်နိုင်ကြပါတယ်။ ဘာကြောင့်လဲဆိုတော့ သူကတန်းဆက်ထားတာ မဟုတ်လို့ပါဘဲ။ Linear Bus ကိုတန်းဆက်ထားတာကြတော့ Cable တစ်လျှောက်တစ်နေရာရာမှာ တစ်ခုခု ဖြစ်နေရင် အစွန်းနှစ်ဖက်ကျတဲ့ Node မှ Connection မရတော့ပါ။ Network Down သွားတာပေါ့။ 10BaseT က Hub ကိုအသုံးပြုပြီး Star Topology နဲ့တပ်ဆင်ထားတာကြောင့် ကွန်ရက်မှာရှိတဲ့ Node တွေဟာ Hub ကို Cable တစ်ကြိုးချင်းစီသွားထားတာကြောင့် Segment တစ်ခုမှာ တစ်ခုခုဖြစ်နေခဲ့ရင် ဒီ Segment တစ်ခုပဲသက်ရောက်မှုရှိပါတယ်။ တခြား Segment တွေကိုဒုက္ခမပေးပါဘူး။ နောက်ထပ်ကောင်းတဲ့ အချက်တွေရှိပါသေးတယ်။ 10BaseT နဲ့ဆင်ထားတဲ့ Network မှာ Node တွေထပ်တိုးချင်ရင် တနည်း အားဖြင့်ပြောရရင် Network ကိုတဖြည်းဖြည်းနဲ့ချဲ့သွားချင်ရင်လဲ UTP Cable Segment အခုလို Hub မှာသွားတပ်လိုက်ရုံနဲ့ အလွယ်တကူချဲ့သွားလို့ရပါတယ်။ ပြောရရင်တော့ Flexible ဖြစ်တယ်ပေါ့ဗျာ။

ကုန်ကျစရိတ်အနေနဲ့ကလည်း ဒီလောက်ကြီးမားလှတယ်လို့တော့ မဟုတ်ပါဘူးခင်ဗျာ။ တခြား Cable တွေထက်စာရင်တောင် သက်သာတယ်လို့ပြောလို့ရနေပါတယ်။

မှတ်ချက်။ ။ ကွန်ရက်တစ်ခုဟာ Bus Topology နဲ့မဆင်ဘဲ Star နဲ့သာတပ်ဆင်အသုံးပြုမယ်ဆိုရင် ကွန်ရက်ဟာပိုပြီး စိတ်ချရတယ်။ တပ်ဆင်ရလွယ်ကူတယ်။ ထိန်းချုပ်ရတာလွယ်ကူတယ် စသည်ဖြင့် ပြောခဲ့ပြီးပြီနော်။ ဘာဖြစ်လို့လဲဆိုတော့ Node တွေဟာ Hub ကိုဆက်သွယ်တပ်ဆင်ရာမှာ သီးခြားစီဖြစ်နေလို့ပါပဲ။ အကယ်၍များ ၎င်းကွန်ရက်မှအသုံးပြုတဲ့ Hub ဟာ သူ့ကိုသူ ထိန်းချုပ်ရတဲ့ Intelligent ဖြစ်တဲ့သဘောလို့ ပြောလို့ရတဲ့ Management Software ကိုသာ တနည်းအားဖြင့်ရှိခဲ့ရင် အဲဒီ Software ကနေမှ သံသယ ဖြစ်တဲ့ Port တွေကို Disconnect လုပ်လို့ရပါတယ်။

Troubleshooting 10BaseT (အခြေခံရှာဖွေခြင်း)

အကယ်၍ ကျွန်တော်တို့ဟာ UTP Cable ကိုအသုံးပြုပြီး Network ကိုဆင်ရာမှာ ၎င်း Network ကို 100 Mbps နဲ့အလုပ်လုပ်စေချင်ရင်တော့ ၎င်းကွန်ရက်ဆင်ထားတဲ့ အစိတ်အပိုင်းများအားလုံး ဥပမာ (ကြိုး၊ Network Card / Hub) စသည်တို့အားလုံးဟာ Cat 5 Cabling System နှင့်ညီမျှနေဖို့ လိုအပ်ပါတယ်။ ကြိုးကလည်း Cat 5 ဆိုတော့ 100 Mbps Bandwidth ရှိမယ်။ Network Card ကိုရွေးချယ်ရာမှာလည်း 10 Mbps နဲ့ 100 Mbps ကိုရွေးဖို့လိုမယ်။ Hub မှာလည်းဒီအတိုင်းပဲ။ သူတို့အားလုံး

100 Mbps ဖြစ်နေမှ ၎င်းကွန်ရက်ဟာ 100 Mbps နဲ့အလုပ်လုပ်နိုင်တာပါ။ အဲ့ဒါအပြင် တပ်ဆင်ရာမှာလည်း အထူးသဖြင့် Cat 5 ကြိုးကိုအထူးသတိထားကိုင်တွယ်ဖို့လိုပါတယ်။ ဥပမာ တအားကြိုး ကြိုးကိုဆွဲဆန့်ဖိတာမျိုးပေါ့။ အဲ့ဒီအပြင် Node တစ်လုံးနှင့်တစ်လုံးကြားမှာ ဆက်သွယ်တဲ့ Cat 5 Cable ဟာကြားမှာ Patch Panel ပဲသုံးထား သုံးထား Wall Panel တွေကပဲတဆင့် သွားသွား ကြားထဲကကြိုးတွေအားလုံး Cat 5 ဖြစ်ဖို့လိုပါတယ်။

Charactristic	Value
Maximum cable length	100 meters (328 feet)
Bandwidth	10 Mbps
Bend radius	TP not subject to bend radius limitations
Installation/maintenance	Easy to install, no need to reroute; the most flexible
Cost	Least expensive of all cabling options
Connector type	RJ-45 for device and wall-plate connections
Interference rating	Low: Most susceptible of all electrical cable types

ဒီ Twisted Pair နှင့်ကွန်ရက်တွေကိုတပ်ဆင်တဲ့အခါမှာ - ထပ်မံပြီးလိုအပ်တဲ့ သိသင့်တဲ့ပစ္စည်းအကြောင်းကို ဆက်လေ့လာကြည့်ရအောင်။ ဘာဖြစ်လို့လဲဆိုတော့ ကွန်ရက်တွေကိုဆင်တဲ့နေရာမှာ ကျွန်တော်တို့အတွေ့အကြုံအရ ပြောရရင် ၁၀ ပေ ပတ်လည်အခန်းထဲမှာပဲ ဆင်ဖူးသလို၊ ရုံးခန်းတွေကိုဖြတ်ကျော်ပြီး ရုံးတစ်ရုံးရဲ့ တိုဖက်ထိပ်၊ ဒီဖက်ထိပ်ချိတ်ဆက်ခဲ့ရဖူးပါတယ်။ အခန်းကျဉ်းလေးထဲမှာ ဆင်ခဲ့ရတာ ဘာပြဿနာမှမရှိပေမယ့်တစ်နေရာကနေ တစ်နေရာဆင်တဲ့အခါမှာတော့ အခုလို Patch Panel တွေနဲ့ ဆင်ဖို့လိုအပ်ပါတယ်။ အဲ့ဒီတုန်းကတော့ ကုန်ကျစရိတ်လည်း သက်သာအောင်ဆိုပြီး ကြိုးတွေကို နံရံတွေမှာ ရိုက်ပြီး Hub ဆီကို တောက်လျှောက်ချိတ်ဆက်ခဲ့ကြတာပေါ့။ Patch Panel ရဲ့သဘောကတော့ ပုံမှာပြထားတာကိုကြည့်လိုက်တာနဲ့ရှင်းနေပြီဖြစ်ပါတယ်။ Patch Panel မှာ ဘာ Electronic Circuit မှမပါဝင်ပါဘူး။ သူက ရုံးခန်းကို Cable ကြိုးတွေနဲ့ရှုပ်ပွမနေစေဘဲ တွဲနွေ့ရနေစေပါတယ်။ ရုံးခန်းတွေမှာကွန်ပျူတာတွေကို တိုရွှေ့ဒီရွှေ့ပြုလုပ်ချင်တဲ့အခါကြတော့ Patch Panel သုံးခြင်းအားဖြင့် ပိုမိုလွယ်ကူစေပါတယ်။ ဥပမာပြောပြပါအုံးမယ်။ Station ကနေလာတဲ့ကြိုးဟာ လမ်းတစ်လျှောက် အုတ်နံရံတွေ၊ ရုံးခန်းငယ်တွေကိုဖြတ်သန်းပြီးမှ Central Hub ကိုရောက်ပါတယ်။ အဲ့ဒီကြိုးဟာ Station ကနေ Hub အထိ တဆက်တည်း တလျှောက်တည်း ချိတ်ဆက်ထားတာပါ။ ဒီတော့ UTP Cable ကိုပဲကြည့်ရအောင်။ UTP Cable ကို ဒီလိုတောက်လျှောက် ချိတ်တော့မယ်ဆိုရင် လိုအပ်တာထက်ကိုမသွားဖို့ လိုအပ်ပါတယ်။ အဲ့ဒီတုန်းက UTP Cable 1 Meter ကို 1 Fec လောက်ရှိပါတယ်။ ဒီတော့ Station နဲ့ Hub က မီတာ (၃၀) ကွာဝေးတယ်ဆိုရင် မီတာ (၃၀) ကြိုး အတိအကျကို

ကွန်ရက်ဆင်ခိုင်းတဲ့ ကုမ္ပဏီတက်က ဖြတ်စေချင်ပါတယ်။ ကျွန်တော်တို့ကတော့ (၁) မီတာ လောက်ပိုဖြတ်ပါ တယ်။ အတိအကျလုပ်ထားတဲ့အခါကြတော့ ကွန်ပျူတာကရွှေ့မရ၊ ပြုမရဖြစ်တတ်ပါတယ်။ ဘာကြောင့်လဲ ဆိုတော့ကြိုးက Station နဲ့ Hub ဆီကိုအတိအကျဖြတ်ထားတာကိုး။ ရုံးသန့်ရှင်းရေးလုပ်လို့ အမြင်ဆန်းသစ် အောင် ပစ္စည်းတွေကိုတိုရွှေ့ ဒီရွှေ့ရင်းနဲ့ Station ကို ဒီနေရာမှာမထားချင်တော့ဘူး။ တိုတို ဒီဒီရွှေ့ချင်ရင် ကြိုးကကွက်တိဖြတ်ထားတာကြောင့် Station ကိုရွှေ့လို့မရပါဘူး။ UTP ကြိုးကထပ်ဆက်လို့မှမရတာ။ အဲကြောင့် မီတာ (၃၀) လိုအပ်ရင် မီတာ (၃၀) ကွက်တိမဖြတ်ဖို့ (၁) မီတာလောက်ပိုထားတာပေါ့။ အဲပေမယ့် (၁) မီတာပိုတော့ 1 Fec ပိုပေးရတာပေါ့။ သူတို့က ဘယ်လိုထင်သလဲဆိုတော့ ကြိုးပိုရောင်းတယ်လို့ထင်တယ်။ နောက်ဖြစ်မယ့်ပြဿနာ သူတို့မသိဘူး။ နောက်ပြီး ကြိုးဆိုတာအများကြီးပိုဖြတ်ထားပြီး ခွေထား လို့ကောင်းတဲ့အရာမှမဟုတ်တာ။ အဲကြောင့် Patch Panel ကိုသုံးခြင်းအားဖြင့် Station ကိုရွှေ့ပြောင်းချင်တဲ့အခါ Station နဲ့ Wall Jack အကြား ကြိုးလိုပဲထပ်ညှပ်ရတယ်။ မီတာ (၃၀) စာ ကြိုးတစ်လျှောက်လုံး အလဟသ အဖြစ်တော့ပါဘူး။ ဒီတော့ Update လုပ်ရတာလွယ်ကူတယ်။ သပ်သပ်ရပ်ရပ်ရှိတယ်။ ရွှေ့ရပြုရလွယ်ကူတယ်။ Modern Office မှာစနစ်တကျရှိတယ်ပေါ့ဗျာ။ တစ်ခုတော့သတိထားရမှာက Station ကနေ Wall Jack, Wall Jack ကနေ Patch Panel, Patch Panel မှ Hub အထိ Cable Length ကိုတွက်ရမှာဖြစ်ပါတယ်။ 10BaseT မှာဆို ဒါကကွန်ရက် Segment တစ်ခုက မီတာ (၁၀၀) ကျော်လို့မရပါဘူး။ ဒါကို သတိမထားမိဘဲ တချို့က Wall Jack to Patch Panel အထိပဲ Cable Length ကိုသွားတွက်မိမှာစိုးလို့ပါ။

Punchdown Blocks

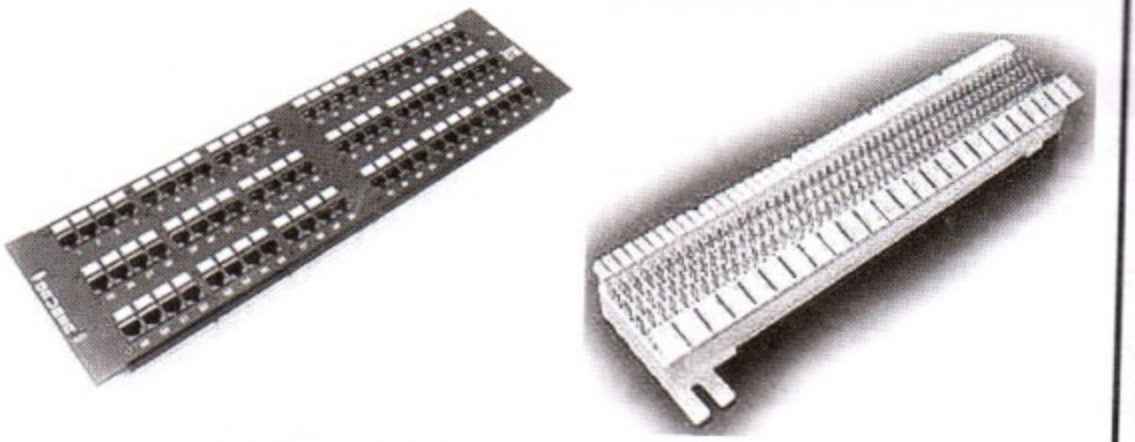
သူက Cable တွေကိုစုစည်းပေးထားနိုင်ပါတယ်။ ဒီအတွက် ကြိုးတွေကနံရံမှာပြန့်ကျဲမနေဘဲ စုစုစည်းစည်း ဖြစ်နေစေပါတယ်။ များသောအားဖြင့်ရုံးလုပ်ငန်းတွေမှာ ၎င်းကိုတယ်လီဖုန်းအတွက်ဖြစ်စေ Network Wire ကြိုးအတွက်ဖြစ်စေ Cable Management ပြုလုပ်ရာတွင်အသုံးပြုပါတယ်။

Patch Panels

သူကတော့ Connection တွေကို ကိုယ့်စိတ်ကြိုက် ကိုယ်ကြိုက်သလိုပုံစံမျိုးနှင့် တပ်ဆင်ခွင့်ရအောင် ပြုလုပ်လို့ရပါတယ်။ ဒီ Patch Panels ဆိုတာ ဒီလို Network အတွက်ပဲအသုံးပြုလို့ရတာမဟုတ်ပါဘူး။ ကျွန်တော်တို့ Audio Studio တွေမှာဆိုရင် Instruments တစ်ခုခုကိုတီးမယ်ဆိုရင် Instruments ကလာတဲ့ Cable ကို ဒီ Patch Panel မှာလာတပ်လိုက်ရုံပဲ။ တီးတိုင်းတီးတိုင်း လိုအပ်တိုင်းလိုအပ်တိုင်းမှာ Cable ကို အစအဆုံး ဆင်လိုက်ဖြုတ်လိုက်လုပ်နေရင်ပင်ပန်းမယ်။ ဘယ်ကနေဘယ်ကိုသွားတတ်တယ်ဆိုတဲ့ ပုံသေရှိတဲ့ Connection တွေကို Patch Panel နှင့်ဆင်ထားလိုက်တာ။ Patch Panel ရဲ့နောက်ဖက်မှာ တစ်နည်းအားဖြင့် Patch Panel ရဲ့အထွက်ဟာ Connection တွေကိုဆင်ထားပြီးသား ကိုယ်က Patch

Panel ရဲ့အဝင် ရှေ့ဖက်မှာ Cable ကိုတပ်ပေးရုံနဲ့ နောက်ဖက်ကနေတခြားကို Connection သွားဖြစ်စေ ပါတယ်။ ဒီ Patch Panel တွေဟာ 100 ကနေ 155 Mbps အထိ Bandwidth ရှိကြပါတယ်။ နောက်ပိုင်းမှာ 1000 Mbps Bandwidth ရှိတဲ့အထိ Patch Panel တွေဖြစ်ပေါ်လာပါလိမ့်ဦးမယ်။

ပုံ ၃.၂၀

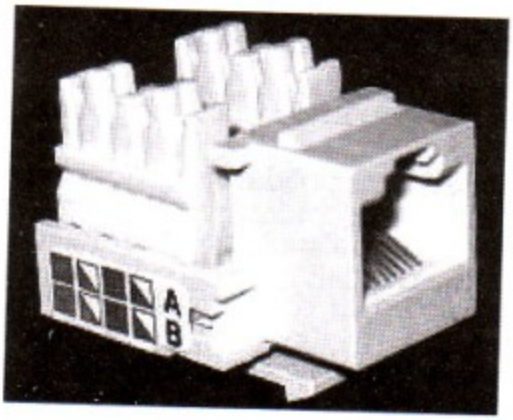


Patch Panel နှင့် Punchdown ကိုတွေ့ရစဉ်

Wall Plates

Wall Plates ဆိုတာက သိပ်မထူးဆန်းပါဘူး။ Office တွေမှာမြင်တွေ့နေရတဲ့ မီးပလပ်ပေါက်တွေ လိုပဲလေ။ ကြိုးတွေကိုလက်ခံတဲ့ပလပ်ပေါက်ဖြစ်ပါတယ်။ ဒီလိုဗျ။ ကွန်ပျူတာကထွက်လာတဲ့ Network Cable ကို Hub အထိတိုက်ရိုက်သွားချိတ်စရာမလိုဘဲ ဒီ Wall Plates မှာတပ်လိုက်ရုံပါပဲ။ ဒီ Wall Plates ထဲက နောက်ဖက်ကကြိုးက ဟိုဖက်က Hub ကိုသွားချိတ်ထားပါလိမ့်မယ်။

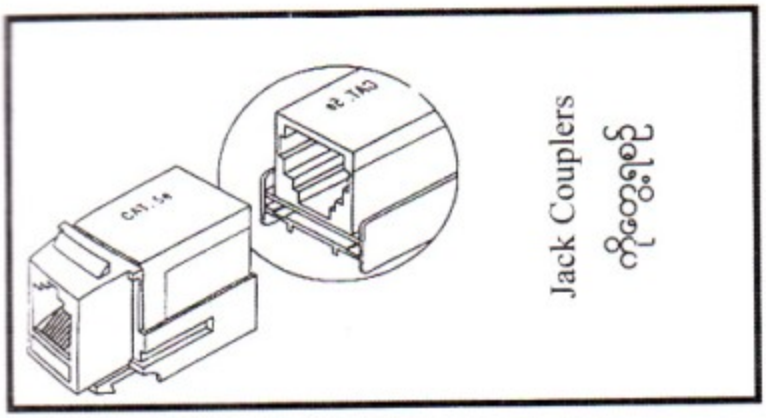
ပုံ ၃.၂၁



Wall Plates ကိုတွေ့ရစဉ်

Couplers

Jack Couplers ဆိုတာ RJ-45 Patch Cords နှစ်ခုကိုဆက်စပ်ပေးနိုင်တဲ့ အမလက်ခံပလပ်ပေါက်
ဖြစ်ပါတယ်။ ဒီတော့ လိုရာမရောက်တဲ့ကြိုးတစ်စကို လွှင့်ပစ်စရာမလိုဘဲ နောက်တစ်ကြိုးနှင့်ချိတ်ဆက်ပြီး
အသုံးချနိုင်သို့ရောက်အောင်ချိတ်ပေးနိုင်သွားတာပေါ့။



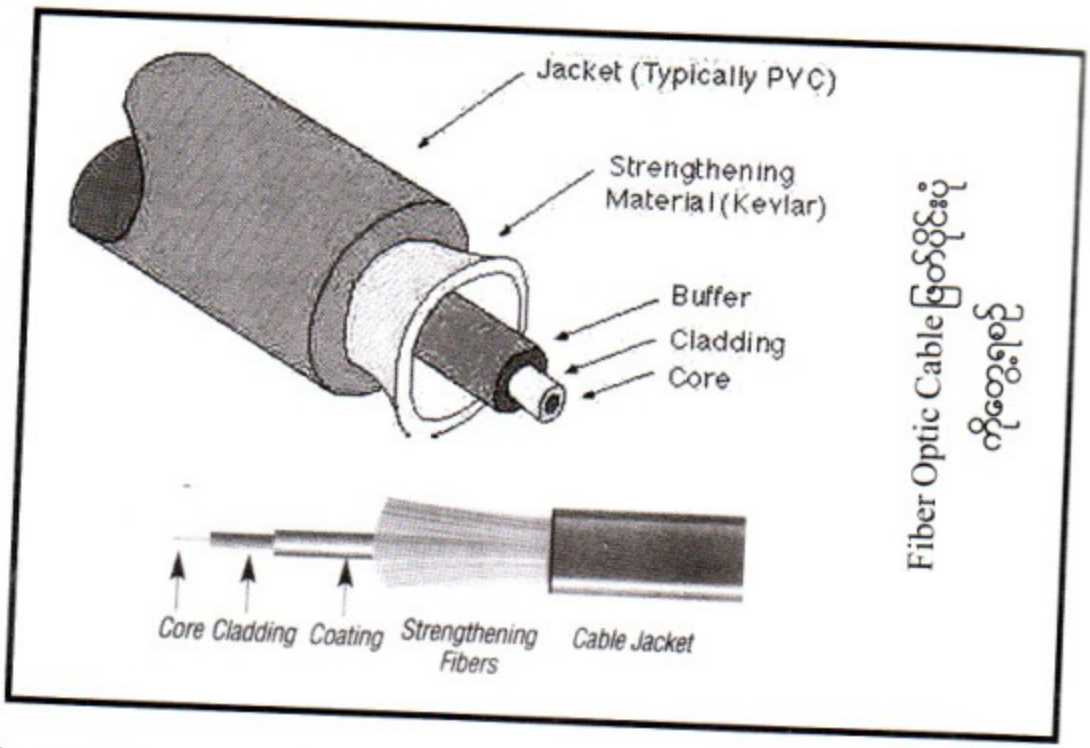
Fiber-Optic Cable

အလွန်တရာမြင့်မားလှတဲ့ Bandwidth ကြောင့် ဒီနေ့ခေတ်ရဲ့ Data ပို့လွှတ်မှုတွေမှာသုံးဖို့ အင်မတန်
လျော်ကန်သင့်မြတ်တဲ့ Cable ပဲဖြစ်ပါတယ်။ အဲ့ဒီအပြင် EMI ပြဿနာမရှိပါဘူး။ နောက်ပြီး Cable တွေဟာ
ကြာရှည်လည်းခံတယ်။ နောက်ပြီး ကိုလိုဒိတာ အတော်လေးကိုရှည်တဲ့အထိ ခရီးဆုံးနိုင်ပါတယ်။ မကောင်းတဲ့
အချက်နှစ်ချက်တော့ရှိတယ်။ အဲ့ဒါကစျေးကြီးတယ်။ ကုန်ကျစရိတ်များတယ်ပေါ့။ နောက်တစ်ခုက တပ်ဆင်ရာ
မှာခက်ခဲတယ်။

ပုံ ၃.၂၃ မှာ Fiber Optic ပုံကိုပြထားပါတယ်။ အလယ်က Conductor က Fiber ပေါ့။ ဒါပေမယ့်
သူက အင်မတန်သန့်ရှင်းပြီးတောက်ပြောင်နေတဲ့ မှန်နဲ့ (သို့မဟုတ်) အနည်းငယ်သော Signal တွေလောက်သာ
Loss ဖြစ်နိုင်တဲ့ ပလပ်စတစ်နဲ့လုပ်ထားတာဖြစ်ပါတယ်။ အဲ့ဒါကိုမှ Cladding ဆိုတာနဲ့ အပြင်ကနေရံထားတယ်။
Cladding ကတော့အလင်းပြန်အောင်လုပ်ထားတာ။ ဒါမှာ Signal တွေဟာ အလင်းလိုပြန်ပြီး Fiber ဆီပြန်
ရောက်သွားမှာ။ သူ့ကြောင့် Signal Loss ဖြစ်ခြင်းကို လျော့ချနိုင်တာဖြစ်ပါတယ်။ အပြင်ဘက်ဆုံးကတော့
Plastic Cover ပေါ့။

Optical Fiber ကြိုးတွေဟာ Electrical Signal နဲ့အလုပ်လုပ်တာမဟုတ်ပါဘူး။ ပုံ ၃.၂၄ ကိုကြည့်ပါ။
Data Signals တွေကို Light Signals အဖြစ်ပြောင်းပြီးအလုပ်လုပ်တာပါ။ ဒီလိုအလင်းနဲ့အလုပ်လုပ်ရာမှာ
နှစ်မျိုးရှိပါတယ်။ တစ်ခုကတော့ လေဆာ (Laser) ပါ။ နောက်တစ်ခုကတော့ Light Emitting Diode
(LED)။ LED ကတော့ Fiber Optic ဖြစ်ပေမယ့်စျေးသက်သာတာပေါ့။ ဒါပေမယ့် အတော်အသင့် Quality
အားနည်းတဲ့ အလင်းကြောင့် သူ့ကိုသိပ်ပြီး Heavy မဖြစ်တဲ့ လုပ်ငန်းဒေသတွေမှာပဲသုံးသင့်ပါတယ်။ (La

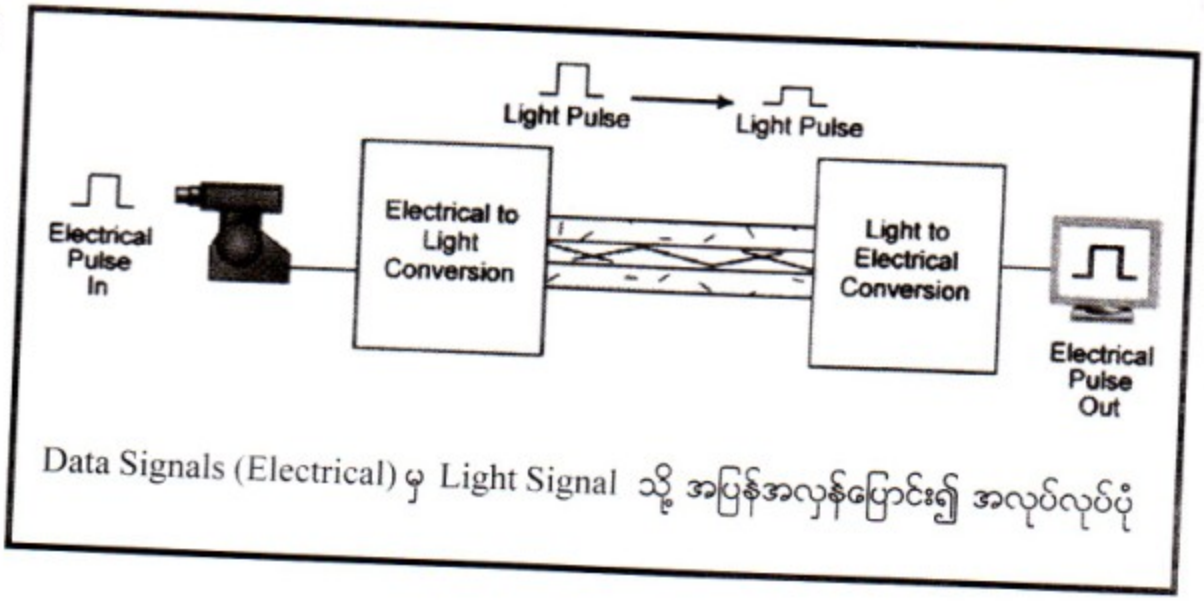
ပုံ ၃.၂၃



Fiber Optic Cable ဖြတ်ပိုင်းပုံ
ကိုတွေ့ရမှာဖြစ်ပါတယ်။

ser) အလင်းတန်းနဲ့ကြတော့ LED နဲ့မတူတော့ဘူး။ သူက တကယ့်ကိုအလင်းစစ်ပဲ။ အရောင်ကတစ်ရောင်တည်းပဲ။ ရောင်စုံမဟုတ်ဘူး။ အလင်းတန်ဟာ သူတို့ရဲ့ ခရီးကိုအပြိုင်သွားကြတာ။ အပြိုင်သွားတယ်လို့ပြောတာ တခြားမဟုတ်ဘူး။ LED ကြတော့ အလင်းကဖြာပြီးသွားလို့။ ဒါကတော့ မျက်စေ့ထဲမြင်အောင်သရုပ်ဖော်ပြတာပေါ့နော့။ ကဲ ဒါထားပါအုံး။ ဆက်ရအောင်။ ဒီ Laser အလင်းတန်းကို ဘယ်လိုဖြစ်ပေါ်စေသလဲဆိုရင် Injection Laser Diode (ILD) ဆိုတဲ့ပစ္စည်းလေးကြောင့်ပါ။ ဒီ Laser အလင်းတန်းဟာ သိပ်ဝေးတဲ့ခရီးအကွာအဝေးကို Data တွေပို့လွှတ်ရာမှာမြင့်မားသော Bandwidth တွေကို လိုချင်တယ်ဆိုရင်တော့ အသုံးပြုဖို့အသင့်လျော်ဆုံးပါပဲ။

ပုံ ၃.၂၄

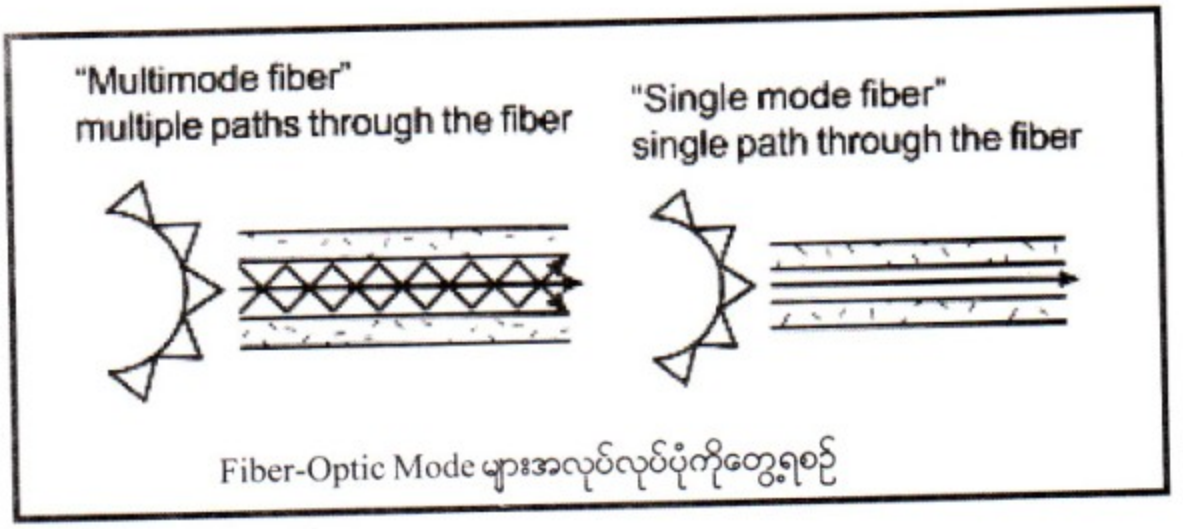


Data Signals (Electrical) မှ Light Signal သို့ အပြန်အလှန်ပြောင်း၍ အလုပ်လုပ်ပုံ

Mode (အလင်းဆုတ်လွှတ်မှု)

Mode မှာနှစ်မျိုးရှိတယ်။ Single Mode နဲ့ Multi Mode ဆိုပြီးတော့ပါ။ Signal Mode ကတော့ Laser အလင်းတန်းနဲ့အလုပ်လုပ်ပြီးတော့ Multi Mode ကတော့အလင်းတန်းများစွာကိုဖြတ်သန်းသွားလာခွင့်ပြုပြီး အသင့်တော်ဆုံးကတော့ Quality နိမ့်တဲ့ အလင်းတန်းအတွက်ပါပဲ။ တနည်းအားဖြင့် LED အတွက်ပါ။ ခုနကပြောခဲ့သလိုပါပဲ။ အဝေးဆုံးခရီးနဲ့ အမြင့်မားဆုံး Bandwidth ကိုလိုချင်ရင်တော့ သင်ဟာ ဈေးကြီးကြီးပေးရတဲ့ Single Mode ကို Laser အလင်းတန်းနဲ့တွဲသုံးရမှာပါ။ ပုံမှာ Single Mode နဲ့ Multi Mode ကွဲပြားပုံကိုပြထားပါတယ်။

ပုံ ၃.၂၅



Fiber-Optic Mode များအလုပ်လုပ်ပုံကိုတွေ့ရစဉ်

နောက်တစ်ခုက Fiber Core နဲ့ Cladding တို့ရဲ့ Diameter ဟာ အင်မတန်သေးငယ်တဲ့အရွယ်ကြောင့် သူတို့ကို Micron မီတာရဲ့အပုံတစ်သန်းနဲ့တိုင်းတာပါတယ်။ အောက်မှာ Fiber Optic Cable တချို့ကိုပြထားပါတယ်။

Core	Cladding	Mode
8.3 micron	125 micron	Single
62.5micron	125 micron	Multi
50 micron	125 micron	Multi
100micron	140 micron	Multi

ကဲ ကျွန်တော်တို့ အခုအပေါ်က ဇယားကို မြင်ရတဲ့အခါမှ ကြိုးဟာအင်မတန်သေးငယ်တာကို သတိထားမိပါလိမ့်မယ်။ အဲဒီမှာ ကြုံတွေ့ရတဲ့ အဓိကပြဿနာတစ်ခုကတော့ ကြိုးကိုတပ်ဆင်တဲ့အခါ တနည်း

Install လုပ်တဲ့အခါအင်မတန်တိကျသေချာမှုတွေ လိုအပ်တယ်ဆိုတာပါပဲ။ အကယ်၍ တစ်ခုခုလွဲချော်ခဲ့မယ်ဆိုရင် အားလုံးပြီးလို့ Fiber Optic ကြိုးနှစ်ခုကို ဆက်လိုက်တဲ့အခါကြမှ ပြဿနာကပေါ်တတ်ပါတယ်။ ဘာပြဿနာလဲဆိုတော့ အင်မတန်သေးငယ်တဲ့ အလယ် Core ဟာ အလွန်အမင်းသေးငယ်တဲ့ ဒဿမကိန်းပေါင်းများစွာနဲ့ တိကျစွာ တန်းတန်းရှိနေရမှာ ဖြစ်ပါတယ်။ အဲဒီလိုမဖြစ်ရင်တော့ Signal တွေ Loss ဖြစ်တတ်ပါတယ်။

ဘယ် Cable အမျိုးအစားမဆို ကောင်းကျိုးနဲ့ဆိုးကျိုး အတူတွဲနေတဲ့ပြီးရှိတတ်သလို Fiber Optic Cable ဟာလည်း ကောင်းကျိုးဆိုးကျိုးတွဲလို့နေပြန်ပါတယ်။

Cost (ကုန်ကျစရိတ်)

UTP Cable နဲ့တပ်ဆင်ဖို့ Ethernet Network Card ကုန်ကျစရိတ်ထက် ဆယ်ဆမကပိုနေတဲ့ Fiber Opitc Network Cable ဟာ Fiber Optic ရဲ့ဆိုးကျိုးတွေကိုဖော်ပြနေသလိုပါပဲ။ Fiber Opitc ဟာတကယ့်ကိုကုန်ကျစရိတ်အများဆုံးပါပဲ။

Installation (တပ်ဆင်ခြင်း)

Fiber Optic ဟာစျေးလည်းကြီးသလို Install လုပ်ရာမှာလည်း လက်ပေါက်ကပ်လှပါတယ်။ ခက်ခဲတယ်ပေါ့။ Fiber Optic ကို Install လုပ်ဖို့အထူးကျွမ်းကျင်ဖို့လည်းလိုအပ်ပါတယ်။ တကယ့်ကို ပြည့်စုံကောင်းမွန်လှတဲ့ ကိရိယာနဲ့နည်းပညာတွေဟာလည်း လိုအပ်တာပေါ့ဗျာ။ အဲဒီအပြင် ကြိုးကိုတပ်ဆင်နေစဉ်ကာလအတွင်းမှာ ညှင်ညှင်သာသာကိုင်တွယ်ရပါတယ်။ အထူးဂရုစိုက်ဖို့လိုတာပေါ့ဗျာ။ ကွေးမိ၊ ညှစ်မိ သွားရင်လည်းကြိုးဟာပျက်စီးသွားတတ်ပါတယ်။ နောက်ပြီးတပ်ဆင်နေတုန်းမှာ ကြိုးကို ဆွဲမဆန့်မိစေရန် ဂရုပြုဖို့အထူးမှာကြားလိုပါတယ်။

Capacity (စမတ)

Bandwidth ကတော့တခြား Copper Cable တွေနဲ့လားလားမှမတူပါဘူး။ တကယ့်ကိုမြင့်မားတဲ့ Bandwidth ပါပဲ။ 2 Gbps အထိရပါတယ်။ ဒီထက်ပိုပြီးထူးခြားတာက Fiber Opitc ကြိုးဟာ ခရီးဝေးဝေးသွားသည့်တိုင်အောင် High Data Rate ကိုပိုင်ဆိုင်နေတာပါပဲ။ UTP ဆိုရင် Meter 10 အောက်ပဲ 100 Mbps ပဲသွားနိုင်တာ။ Fiber Optic ကြိုးဟာ 100 Mbps နဲ့သာဆိုရင် 100 Meter မပြောနဲ့ ကီလိုမီတာတော်တော်လေးအထိသွားနိုင်ပါတယ်။

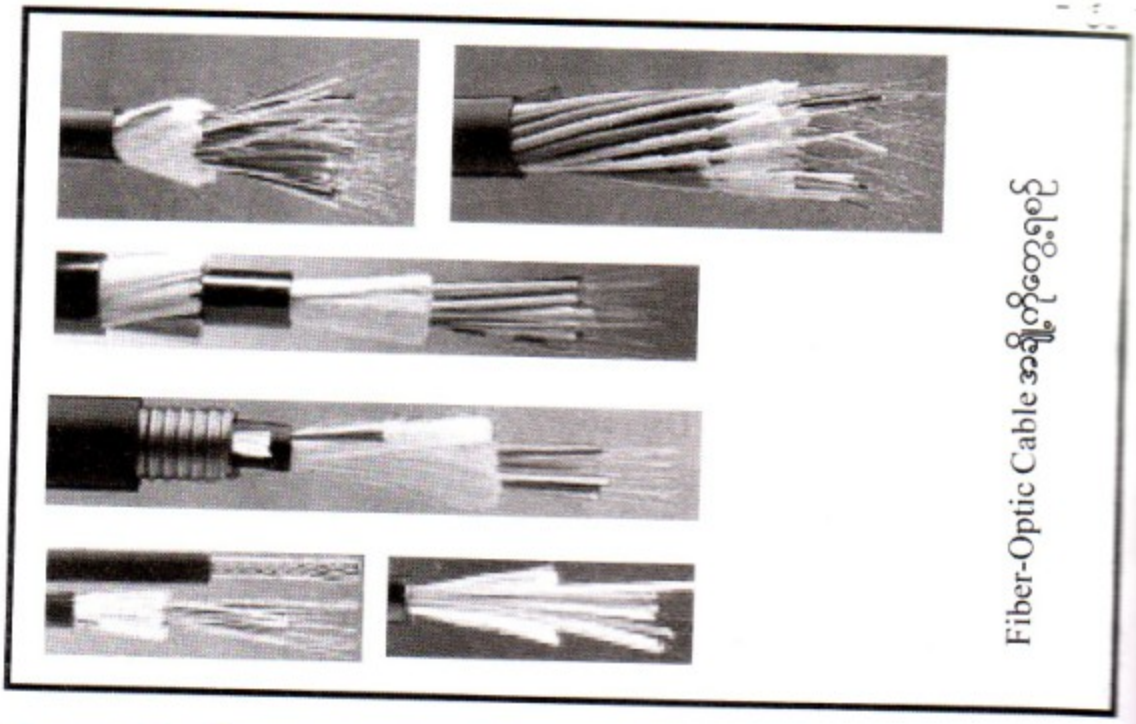
Attenuation (အားနည်းသွားသောအချက်အလက်ဝေးပုံ)

Attenuation ကတော့ ကိုလိုမိတာတော်တော်လေးအထိ Data တွေကိုသယ်သွားနိုင်တာကြောင့် Copper Cable ထက်စာရင် Attenuation ဟာပြောစရာမရှိသလောက်ပါပဲ။

EMI Characteristics (ပြင်ပမှဝင်ရောက်နှောင့်ယှက်မှု)

Fiber Optic ကြိုးတွေဟာ Data တွေကိုပို့လွှတ်ရာမှာ Electrical Signal ကိုအသုံးမပြုတာကြောင့် Electromagnetic Interference ကိုလုံးလုံးလျားလျားကာကွယ်ပြီးသား ဖြစ်နေပါတယ်။ ဘယ်လိုပြောရမလဲ။ ဓာတ်မတူတော့ ဘေးနားမှာသူဆိုတဲ့ EMI ဘယ်လိုပဲရှိနေရှိနေ အထဲက Signal တွေကအပြင်က EMI ကိုစိတ်မဝင်စားဘူး။ မျိုးမှမတူဘဲ။ ပုံပြင်ထဲကလိုပဲ ကြွက်မလေးဘယ်လောက်လှလှ၊ ခြင်္သေ့မင်းက ဘယ်စိတ်ဝင်စားမလဲ။ ဒီတော့ EMI ရန်ကတော့ကင်းပါတယ်။ အဲ့ဒီအပြင် Fiber Optic ဟာတခြားလျှပ်စစ်နဲ့ပတ်သက်သော (Electrical Effect) ရန်များမှလည်းကင်းဝေးပြန်ပါတယ်။ ဥပမာ တစ်ခုပြောရရင်လျှပ်စစ်ဝါယာကြိုးကို အဆောက်အအုံနှစ်ခုကိုဆက်သွယ်မယ်ဆိုရင်တောင် အဆောက်အအုံနှစ်ခုရဲ့မတူညီတဲ့ Ground Potentials ကြောင့် ပြဿနာတွေပေါ်ပေါက်တတ်ကြပါတယ်။ ရံဖန်ရံခါပေါ့နော်။ ဒီတော့ Fiber Optic မှာ ဒီပြဿနာတွေကင်းတယ်။ ဒါကြောင့်မို့ မတူညီတဲ့အဆောက်အအုံနှစ်ခုကို Network ချိတ်တော့မယ်ဆိုရင် အကောင်းဆုံးနည်းလမ်းကတော့ Fiber Optic ကိုသုံးဖို့ပါပဲ။ ပြောပြချင်တာကတော့ Fiber Optic ဟာ Electrical Signal ကိုအသုံးမပြုခြင်းကြောင့် ပတ်ဝန်းကျင် Electrical Effect တွေကို ရှောင်ရှားနိုင်ပါတယ်။ ဒါကြောင့် စိတ်အချရဆုံးနဲ့ အကောင်းဆုံး Network တစ်ခုဆင်ချင်တယ်ဆိုရင် Fiber Optic ကိုပဲရွေးချယ်ရမှာ ပဲလို့ ပြောပါရစေ။

Charactristic	Value
Maximum cable length	2 km (6562 feet) - 100 km (62.4 miles)
Bandwidth	10 Mbps - 1 Gbps
Bend radius	30 degrees/ft
Installation/maintenance	Difficult to install and rerout, sensitive to strain and bending
Cost	Most expensive of all cabling options
Connector type	Several types; ST, SC, MIC, and SMA
Interference rating	None: Least susceptible of all cable types



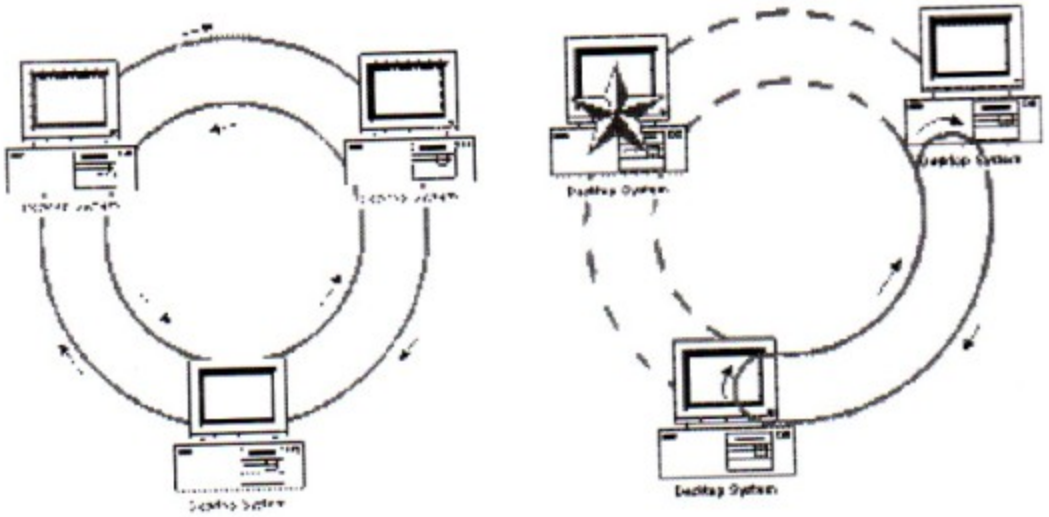
Fiber-Optic Cable အချို့ကိုတွေ့ရစဉ်

၃.၁၂ FDDI အကြောင်း

FDDI ဆိုတာ Fiber Distributed Data Interface ကိုပြောတာပါ။ IEEE 802.5 ကိုအခြေခံတဲ့ LAN Standard တစ်ခုပဲဖြစ်ပါတယ်။ FDDI ဟာ Fiber Optic Cable ရဲ့ LED နဲ့ Laser နှစ်ခုစလုံးကို သယ်ဆောင်နိုင်တဲ့ LAN ဆက်သွယ်ရေးစနစ်ဖြစ်ပါတယ်။ Fiber Optic Cable ဟာ တကယ့်ကို Glass စစ်စစ်နဲ့ပြုလုပ်ထားပြီးတော့ သူဟာအလွန်သေးငယ်တဲ့ Wire အိမှမဟုတ် Fiber အတွင်းမှာတည်ရှိပါတယ်။ တနည်းအားဖြင့်ပြောရရင် Wire သို့မဟုတ် Fiber ရှိမယ်။ သူ့ရဲ့အတွင်းမှာ Pure Glass ပေါ့။ အဲဒီလို Fiber တွေအများကြီးကို အစည်းသဖွယ်စုချည်ထားလိုက်တော့ အလည်မှာစုစုလေးဖြစ်နေတာပါ။ အဲကို Core လို့ ခေါ်ပါတယ်။ အဲဒီ Core ကိုမှ နောက်ထပ် Glass-T တစ်ခုနဲ့ဖုံးအုပ်ဝိုင်းရံလိုက်ပါတယ်။ အဲကိုတော့ Cladding လို့ခေါ်ပါတယ်။ LED ဟာအဲဒီ Cable မှာရှိတဲ့ Core တစ်လျှောက် Signal တွေကိုပို့လွှတ်ပေးပါတယ်။ ဒီ Core မှာရှိတဲ့ Fiber တစ်ခုချင်းစီမှာသွားနေတဲ့ Signal တွေဟာတစ်ချိန်မှာ Direction တစ်ဖက်ထဲကိုပဲသွားနိုင်ပါတယ်။ Fiber တွေကိုစုစည်းထားပြီး Core သဖွယ်ပြုလုပ်ထားခြင်းဖြင့် LED ဟာ Signal တွေကိုတချိန်တည်းမှာအများကြီးပို့လွှတ်နိုင်ပါတယ်။

တကယ်တော့ FDDI ဟာ Fibre Optic Cable ကိုအသုံးပြုပြီးမှ Topology ရဲ့ Token Ring ကို Access လုပ်တာဖြစ်ပါတယ်။ အဲပေမယ့် Token Ring နဲ့မှာက Token Ring က 4 or 16 Mbps ပဲ Data Transfer ဖြစ်ပါတယ်။ FDDI ကတော့ 100 Mbps Data Rate ရှိပါတယ်။ 100 Mbps ဆိုတာကလဲ မိုင်ပေါင်း (၆၀) ကျော် ကီလိုမီတာ(၁၀၀)လောက်အထိကိုသွားနိုင်တာပါ။ နောက်ပြီး Token Ring က Ring တစ်ခုတည်းကိုအသုံးပြုတယ်ဆိုပေမယ့် FDDI က Ring နှစ်ခုကိုအသုံးပြုပါတယ်။ အဲကို Dual Counter Rotating Ring လို့ခေါ်ပါတယ်။ တန်ပြန် (ဆန့်ကျင်ဘက်) လည်နေတဲ့ကွင်းနှစ်ကွင်းပေါ့ဗျာ။ သူ့ကြောင့်

ပုံ ၃.၂၇



FDDI Workstation များအလုပ်လုပ်နေပုံ နှင့် FDDI Workstation တစ်လုံး Down နေ၍ ကျန်သည့် Workstation များတွင်ပဲ FDDI အလုပ်လုပ်ပုံ

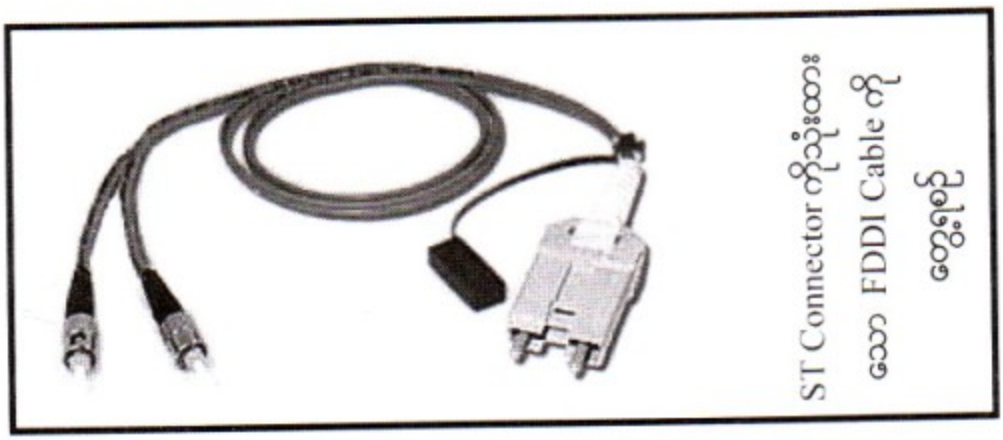
FDDI ဟာ ကွင်းတစ်ခုကိုဖြတ်ပြီး Data တွေပို့လွှတ်နေချိန် နောက်ကွင်းတစ်ခုမှာ Backup အဖြစ်မဟုတ် တခြား Services တွေကိုလုပ်လာနိုင်ပါတယ်။ ပြောရမယ်ဆိုရင် FDDI က Multiple Token ကို အသုံးပြုတယ်ပေါ့ဗျာ။

Token Ring နဲ့တူတာကလည်းရှိတာပေါ့။ FDDI ဟာ Token Ring လိုပဲ Token ကို Network တစ်လျှောက် Data Frame တွေသယ်ယူပို့ဆောင်တဲ့နေရာမှာ သုံးပါတယ်။ Data Frame ဟာ လိုရာ Network Node ကိုရောက်ပြီဆိုတာနဲ့ Token ဟာ Network မှာရှိတဲ့ ချိတ်ထားတဲ့နောက် Node တစ်ခုဆီကိုရောက်သွားပါတယ်။ အဲဒါက Ring တစ်ခုပေါ့။ FDDI Network ရဲ့ဒုတိယ Ring ကတော့ ပထမ Ring နဲ့ဆန့်ကျင်ဘက်လားရောအတိုင်း လည်နေပါတယ်။ ဒီလို Counter တန်ပြန်လည်ပတ်နေမှုကြောင့် Network မှာ Fiber Break ဖြစ်သွားခဲ့ရင်တောင် Network ကို Ring အစားဖြည့်ပေးနိုင်ပါသေးတယ်။ အဲဒီပေမယ့် တစ်ခုတော့ရှိပါတယ်။ အဲဒါဟာ Station တွေရဲ့ Class ပေါ်မှာမူတည်ပါသေးတယ်။ ဆိုလိုချင်တာက Network Station တစ်ခုချင်းစီဟာ Ring တစ်ခု အဖြစ်မဟုတ် Ring နှစ်ခုစလုံးကို Attach လှမ်းလုပ်နိုင်ပါတယ်။ အဲဒီဟာ ခုနကပြောသလို Station တွေရဲ့ Class ပေါ်မူတည်တာပါ။ Class ကနှစ်မျိုးရှိပါတယ်။ Class A ရယ် Class B ရယ်ပါ။

Class A ကိုတော့ Single Attach Stations (SAS) လို့ခေါ်ပါတယ်။ သူကတော့ တစ်ကြိမ်မှာ Ring တစ်ခုကိုပဲ Attach လုပ်လို့ရပါတယ်။ Class B ကိုတော့ Dual Attached Station (DAS) လို့လည်းခေါ်ပါတယ်။ သူကတော့ Ring နှစ်ခုလုံးကိုတပြိုင်တည်း Attached လုပ်နိုင်ပါတယ်။ အကယ်၍များ Net-

work အတွင်း Devices တစ်ခုခုက ပုံမှန်မဟုတ်ခဲ့ရင် တနည်းအားဖြင့် Unstable ဖြစ်ခဲ့ရင် Ring နှစ်ခုလုံး ကိုဖြတ်တောက်ပစ်လိုက်ပါတယ်။ ဒီလို Fault ဖြစ်နေတဲ့ Node တွေကို Network မှာ တသီးတခြားထားလိုက်တာမျိုး နောက်တစ်နည်းရှိပါသေးတယ်။ အဲဒါကတော့ Station တွေကိုကြိုးတွေမှတဆင့် အချင်းချင်း ချိတ်ဆက်ပေးတဲ့ Connectrator ကပြုလုပ်ပေးတာဖြစ်ပါတယ်။ Connectrator ဟာ Theory အရပြောရင်တောင် Token Ring တွေမှာသုံးတဲ့ MAU တွေလိုပါပဲ။ Connectrator ဟာ Network Station တွေအတွက် Centralized Cable Connection လုပ်ပေးတာပါ။ ဒီပေမယ့် MAU တွေနဲ့မတူတဲ့အချက်ရှိနေပြန်ပါတယ်။ အဲဒါကတော့ Connectrator တွေဟာ Station နဲ့ Communicate လုပ်ပေးနိုင်ရုံသာမက Station နဲ့ Connectrator အကြားဆက်သွယ်မှုကောင်းမကောင်း ပြည့်စုံခြင်းရှိမရှိကိုပါ စစ်ဆေးပေးနိုင်ပါသည်။

ပုံ ၃.၂၈



ST Connector ကိုသုံးထားသော FDDI Cable ကို တွေ့ရစဉ်

Advantage of Using FDDI အကြောင်းသိကောင်းစရာ

အကယ်၍များ Cable Break ဖြစ်သွားခဲ့ရင် ၎င်းကိုသီးခြားထားပြီး Communication ကိုဆက်လက်ဖြစ်ပေါ်စေတဲ့နေရာမှာတော့ FDDI ဟာ အင်မတန်ကိုစိတ်ချရပါတယ်။ ဒါဟာ ကောင်းတဲ့အချက်တစ်ခုဆိုပေမယ့် ကောင်းတဲ့အချက်တွေဟာ သူတစ်ခုထဲမှာတော့မဟုတ်ပါဘူး။ FDDI ဟာ Token Ring Network ရဲ့သဘောတရားကိုအခြေခံကောင်းယူပြီး Performance ကောင်းသထက်ကောင်းအောင် လုပ်ဆောင်နိုင်ခဲ့ပါတယ်။ FDDI ရဲ့ကောင်းတဲ့အကြောင်းအရာတွေကို အချက်အလိုက်ဖော်ပြရရင်ဖြင့် -

- ❖ Information Security - Fiber Optic Cable ဟာ Wiretap ပြုလုပ်ဖို့ခဲယဉ်းခြင်း။
- ❖ Physical Security - Fiber Optic Cable ဟာတခြား Cable တွေထက်စာရင် ကျိုးပဲ့ပျက်စီးမှုကို ခံနိုင်ရည်ပိုရှိခြင်း။
- ❖ Electrical Security - Fiber Optic Cable ဟာလျှပ်ကူးမှုမရှိတဲ့အပြင် Electrical နှောင့်ယှက်မှုဆိုတဲ့ Interference အပေါ်မှာလည်း တိမ်းညွတ်မှုမရှိပါဘူး။

- ၎င်းအချက်အတွေအပြင် FDDI ဟာ တခြား Cable ထက်စာရင် Data တွေကိုခရီးဝေးဝေးပို့နိုင်တဲ့ အချက်ကလည်းရှိနေပြန်ပါတယ်။ အဲဒီအပြင် FDDI ဟာ Built in Management သုံးခုပါရှိပြန်ပါတယ်။
- Ring Management (RMT) - Network Ring တွေကိုရှာဖွေခြင်း၊ အပြစ်တွေကိုဖြေရှင်းခြင်း စသည်တို့လုပ်ဆောင်ရပါတယ်။
- Communiaction Management (CMT) - သူကတော့ Network တွေမှာ Station တွေထပ်ထည့်ခြင်း၊ ဖြုတ်ချခြင်းတွေကိုထိန်းချုပ်တဲ့ အလုပ်တွေကိုလုပ်ရပါတယ်။
- Station Management (MT) - သူကတော့ Ring တွေကိုစောင့်ကြည့်တဲ့ Software တွေအတွက်ဖြစ်ပါတယ်။

မှတ်ချက်။ ။ Fiber Optic Cable တွေကိုကိုင်တွယ်ရင်းနဲ့ယောင်ပြီးတော့ Eye Protection မပါဘဲ Fiber Optic Cable ကိုမိမိမျက်လုံးနဲ့တိုက်ရိုက်မကြည့်သင့်ပါဘူး။ အကယ်၍ Fiber Optic Port ဟာ Transmit လုပ်နေလား မလုပ်ဖူးလားကို Check လုပ်စေချင်ရင်တော့ အခန်းကိုမှောင်အောင်ပြုလုပ်ထားပြီး ၎င်းနေရာမှာ မှောင်နေပြီဆိုမှ Port အပေါ်မှာစာရွက်အပိုင်းလေးကာလိုက်ပါ။ အကယ်၍ Transmit လုပ်နေမယ်ဆိုရင် Transmit လုပ်နေတဲ့အလင်းရောင်ဟာ ၎င်းစာရွက်အပေါ်မှာအလင်းလာပြန်နေပါလိမ့်မယ်။

Disadvantage of Using FDDI အကြောင်းသိကောင်းစရာ

FDDI ကိုအသုံးပြုခြင်းအားဖြင့် မကောင်းတဲ့အဓိကအချက်နှစ်ချက်တော့ရှိပါတယ်။ အဲဒီတွေကတော့

- FDDI ဟာတကယ့်ကိုရှုပ်ထွေးလှတဲ့ နည်းပညာသစ်တစ်ခုဖြစ်ပါတယ်။ ဒါကြောင့် Install လုပ်ဖို့အထူးကျွမ်းကျင်ဖို့လိုအပ်ပါတယ်။ နောက်ပိုင်းမှာလည်း FDDI Network ကို Maintain လုပ်ဖို့လည်းလိုပါတယ်။
- ကြိုးအရေရော၊ Connectrator ရော၊ NIC ရော ပတ်သက်ရာ ပတ်သက်တဲ့ပစ္စည်းတွေမှန်သမျှတခြားထက်စာရင် ဈေးကြီးနေပါတယ်။

FDDI Cabling အကြောင်းသိကောင်းစရာ

Fiber Optic Cable တွေဟာအမျိုးမျိုးရှိပေမယ့် နမူနာတစ်ခုအဖြစ်ပြောပြချင်တာကတော့ -

- Fiber Optic Cable ရဲ့ Core ဟာ Silica နဲ့ပြုလုပ်ထားပါတယ်။

- Core ရဲ့အပြင်ဘက်မှာ Primary နဲ့ Secondary Buffer ရှိပါတယ်။
- အပြင်ဘက်ဆုံးအလွှာကတော့ Jacket ဖြစ်ပါတယ်။
- Jacket နဲ့ Secondary Buffer အကြားမှာ Cable တောင့်တင်းဖို့အတွက် Kevlar ဆိုတာ ရှိကောင်းရှိနိုင်ပါတယ်။

FDDI Troubleshooting အခြေခံသိကောင်းစရာ

ဘယ်ကွန်ရက်အမျိုးအစားပဲဖြစ်ဖြစ် Troubleshoot လုပ်တဲ့အခါမှာ ပထမဦးဆုံးထင်ရှားတဲ့ ပြဿနာတွေကို ဦးစွာစစ်ဆေးကြည့်ပါ။ ဥပမာ Connector တွေများ Loose ဖြစ်နေလို့လား။ Cable တွေ များပျက်စီးနေလို့လား စသည်ဖြင့်ပေါ့။ ပြီးမှတခြား စစ်ဆေးစရာရှိတာတွေကိုစစ်ဆေးရမှာပါ။ ကဲ အောက်ပါ အချက်တွေကို လေ့လာကြည့်ရအောင်။ ပြဿနာတစ်ခုခုဖြစ်ပြီဆို ဒီအချက်တွေများလာပြီဆို စမ်းစစ်ကြည့်ပေါ့။ အဖြစ်တတ်တဲ့ သဘောတရားတွေပါ။

- Fiber Optic မှာ Multi Mode နဲ့ Single Mode ဆိုပြီးတော့ရှိတာမှာ၊ ဆက်သွယ်ထားတဲ့အကွာအဝေးပေါ်မူတည်ပြီး ၎င်းတို့ကိုမှန်ကန်အောင်ဆောင်ရွက်ပေးဖို့လိုအပ်ပါတယ်။ အကယ်၍များဆက်သွယ်မယ့် အကွာအဝေးဟာ ပေအနေနဲ့ အနည်းငယ်သော ထောင်ဂဏန်းလောက်သာဆိုရင်တော့ Multi Mode Fiber ကိုရွေးသင့်ပါတယ်။ အကယ်၍ ကီလိုမီတာအနေနဲ့ဖြစ်လာပြီဆိုရင်တော့ Single Mode Fibre ကို သုံးသင့်ပါတယ်။

- Fiber Optic Cable မှာအလွန်သေးငယ်သော Break တစ်ခုဖြစ်သွားရင်တောင် အဲဟာ Network Communication ကိုသွားထိခိုက်စေပါတယ်။ အဲနဲ့ပတ်သက်လို့ Cable ကိုကောင်းကောင်းအလုပ်လုပ်မလုပ်ဆိုတာကို Detect လုပ်ပေးနိုင်တဲ့နည်းတွေရှိပါတယ်။ Optical Power Meter နှင့် Light Energy ကိုအသုံးပြုပြီးတော့ Cable ကို Test လုပ်လို့ရပါတယ်။ OTDR ဆိုတဲ့ Optical Time Domain Reflectrometer ကိုအသုံးပြုမယ်ဆိုရင်တော့ ဒီနည်းဟာ နည်းတွေထဲကဈေးအကြီးဆုံးပဲပေါ့။

- Connector တွေညစ်ပတ်နေတာဟာလည်း Communication Problem ဖြစ်စေပါတယ်။ Fiber Optic Light ကိုအသုံးပြုပြီး Data တွေကို Transmit လုပ်တာဆိုတော့ Connector တွေကဖုံတွေ မရှိဖို့နဲ့ မညစ်ပတ်ဘဲသန့်ရှင်းနေဖို့လိုအပ်ပါတယ်။ ဒီတော့ အဝတ်မှာအရက်ပျံလေးစွတ်ပြီးတော့ Connector တွေကို Clean လုပ်ပေးပေါ့။ အရက်ပျံမသုံးဘဲ တခြား ရေတို့ မှန်ကြည်ဆေးရည်တို့ စသည်တို့ကို မသုံးစေချင်ပါဘူး။

- Connector တွေမကောင်းလို့ဘဲဖြစ်ဖြစ် Terminate မှားလုပ်တာပဲဖြစ်ဖြစ် Communication ကို ထိခိုက်စေပြန်ပါတယ်။ ဒီလိုဖြစ်ရင်တော့ မကောင်းတဲ့ Connector ကိုပြန်လဲလိုက်ပါ။ Terminate

မှားလုပ်ထားလို့ Open ဖြစ်နေတဲ့ Segment တွေကိုလည်းပြန်ပိတ်လိုက်ပါ။

❖ Fiber Optic Cable မှာ Communication Delay ကြန့်ကြာမှုဟာ (၄) မိလီစက္ကန့်လောက်တောင် ဖြစ်လေ့ဖြစ်ထမရှိပါဘူး။ ဒီလိုဖြစ်လို့ အံဟာပြဿနာတစ်ခုလိုဖြစ်နေခဲ့မယ်ဆိုရင် NetWare ၏ Packet Burst Protocol ကိုသုံးဖို့အကြံပေးပါရစေ။ သူက Transmission Delay ကိုလျော့ချပေးနိုင်ပါတယ်။

❖ အကယ်၍ Network ဟာလျှင်မြန်စွာ အလုပ်မလုပ်နိုင်ဘဲ Speed နဲ့သက်ဆိုင်နေပြီဆိုရင်တော့ Fiber Optic Cable အမျိုးအစားနဲ့ သက်ဆိုင်နေပါပြီ။ အကယ်၍ဒီလိုအခြေအနေမှာ Plastic Fiber ကို အသုံးပြုထားတာဆိုရင် Glass Fibre ကိုပြောင်းသုံးဖို့လိုပါတယ်။ အကုန်လုံးမဟုတ်တောင် တစ်ပိုင်းတစ်စပေါ့။

၃.၁၃ ဘယ် Cable ကိုသုံးကြမလဲ

အခုဖော်ပြခဲ့တဲ့ Cable အမျိုးအစားတွေထဲက ကိုယ့်လုပ်ငန်းနှင့်ကိုက်ညီမယ့် သင့်လျော်မယ့် Cable ကိုရွေးချယ်တပ်ဆင်အသုံးပြုရမှာဖြစ်ပါတယ်။ ဒီတော့ ကိုယ့်လုပ်ငန်းနှင့်အပ်စပ်မယ့် Cable မျိုးကိုရွေးချယ်စဉ်းစားတဲ့အခါမှာ အောက်ပါအချက်တွေကိုထည့်သွင်းစဉ်းစားရပါမယ်။

Network ကိုဘယ်လောက်မြန်စေချင်သလဲ

ဒါဆိုရင်တော့ Bandwidth ကိုစဉ်းစားပါ။ Bandwidth ကောင်းတဲ့ Cable ဟာချေးပိုကြီးသလိုတပ်ဆင်တဲ့အခါမှာလည်း ကုန်ကျစရိတ်ပိုကုန်ပါတယ်။ Higher ဖြစ်တဲ့ Bandwidth တော့လိုချင်ပါရဲ့။ Fiber Optic ကိုမသုံးနိုင်ဘူးဆိုရင် ကျွန်တော်တို့ဟာ Shield ကိုထူထူသုံးထားလို့ သယ်ရပြုရမလွယ်ကူတဲ့ Cable တွေနဲ့တွေ့တော့မှာဖြစ်ပါတယ်။

Cable အတွက်ပိုက်ဆံဘယ်လောက်သုံးမလဲ

ဒါကတော့ Budget အပိုင်းပေါ့။ Cable ကြိုးကိုရွေးချယ်ဖို့ ပိုက်ဆံဘယ်လောက်သုံးမယ်။ ပိုက်ဆံသုံးတဲ့အပေါ်မူတည်ပြီး ကိုယ်ရဲ့ Network ဟာတစ်စစီအပိုင်းလိုက် ကျယ်ပြန့်နေရင်လည်း ကျယ်ပြန့်နေမယ်။ ပိုက်ဆံဟာ ကြိုးကိုရွေးချယ်တဲ့ နေရာမှာလုံးဝအဓိကကျတဲ့သဘောလည်းဆောင်ပါတယ်။

Network ရဲ့ သွားရာလမ်းကြောင်း

ဒါဆိုရင် Capacity ကိုစဉ်းစားရမှာဖြစ်ပါတယ်။ ဒီလိုပါ Network ကို Planning လုပ်ကတည်းက Network တစ်ခုဟာကြီးသလား သေးသလား။ Network မှာအသုံးပြုနေတဲ့ User ကဘယ်လောက်ရှိသလဲ။

ဒါ Capacity ပေါ့။ သုံးတဲ့သူများရင် Capacity ကြီးမယ်။ ဆိုလိုတာက ကားလမ်းမမှာကားတွေများရင် လမ်းကြောင်းတွေပိတ်ဆို့မယ်။ Traffic ပေါ့။ အခုဒါကိုပြောနေတာ။ ဒီတော့အသုံးပြုသူနည်းသလား များသလား။ Capacity များသလား။ နည်းသလားပေါ်မူတည်ပြီး Network ရဲ့ Traffic က ဘယ်လိုစီစဉ်ရမယ် ဆိုတာကိုထည့်တွက်ရမှာဖြစ်ပါတယ်။

အသုံးပြုမည့်ပတ်ဝန်းကျင်ကဘယ်လိုလဲ

ဒီ Network တည်ရှိမယ့်နေရာရဲ့ ဝန်းကျင်ကဘယ်လိုလဲဆိုတာကတော့ Enviromental Considerations ပဲဖြစ်ပါတယ်။ Network တည်ရှိမယ့် ဝန်းကျင်ကဘယ်လောက်တောင် Noisy ဖြစ်သလဲပေါ့။ နောက် Data Security ကရော ကိုယ့်အတွက်ဘယ်လောက်အရေးပါသလဲပေါ့။ ဒီလိုကိစ္စမျိုးကျတော့ တခြားအကြောင်းအရာတွေထက် သူ့ကိုဦးစားပေးစဉ်းစားပေးရမယ်။ ကိုယ်တပ်ဆင်မယ့် Network မှာ ဒီကိစ္စမျိုးတွေပါလာပြီဆိုရင် Fiber-Optic ကိုရွေးချယ်ရပါလိမ့်မယ်။

Cable သွားရာလမ်းကြောင်း

ဒါကတော့ Placement ပေါ့။ ဒီလိုဗျ။ ကိုယ်တပ်ဆင်တဲ့ ကွန်ရက်ရဲ့တည်နေရာရုံးခန်းဟာ အခန်းကျဉ်းလား၊ ကျယ်လား၊ တစ်နေရာနှင့်တစ်နေရာ Cable တွေကိုချိတ်ဆက်တဲ့နေရာမှာ သတိထားရမှာက ထောင့်ချိုးတွေများလား၊ ဒါမျိုးဆို Cable က Flexible ဖြစ်မှရမယ်။ ဥပမာ Thinnet တို့ UTP တို့ဆိုးမှရမယ်။ မဟုတ်ရင် ကွေးလို့ပြုလို့ရမှာမဟုတ်ဘူး။

ကွန်ရက်မှာပစ္စည်းဘယ်နှစ်ခုတပ်ဆင်အသုံးပြုမလဲ

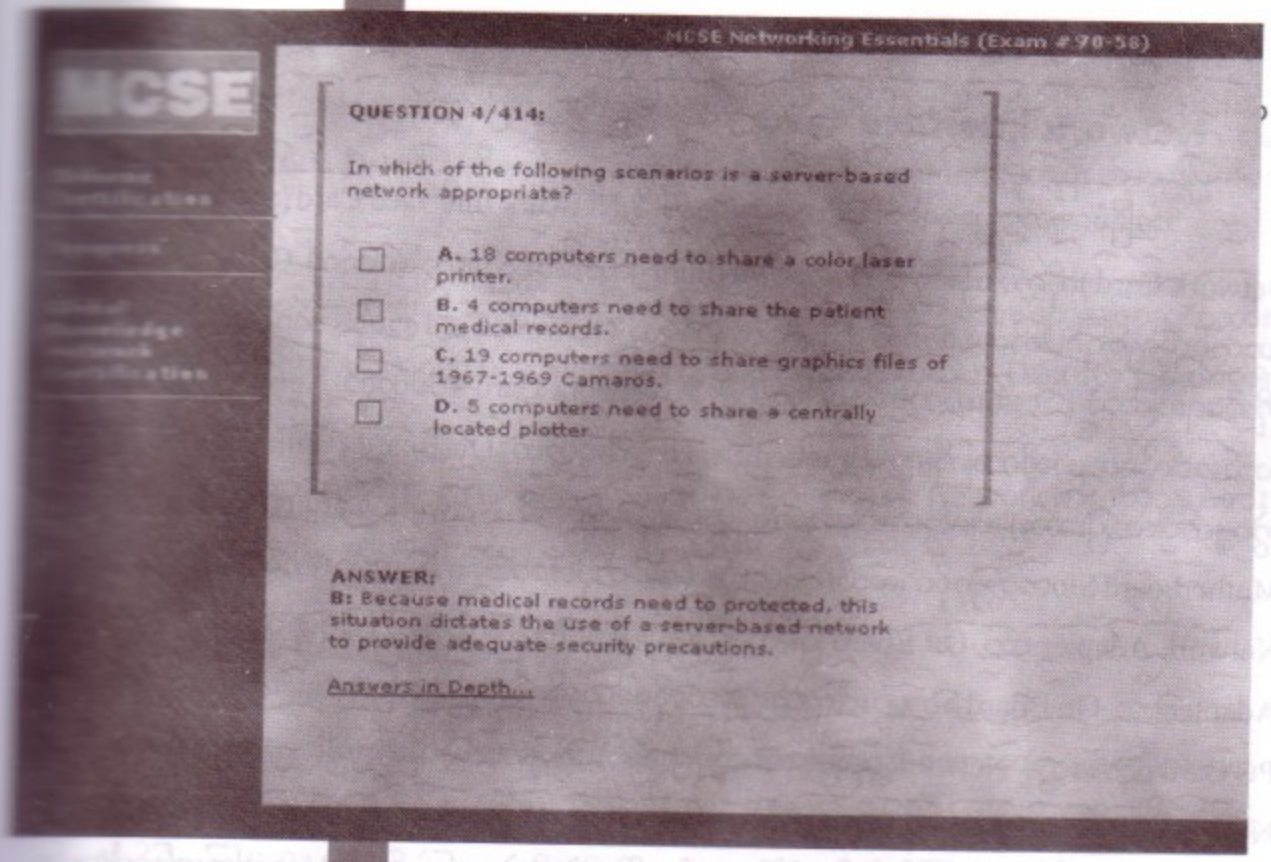
ဒါ Scope ပေါ့။ Network တစ်ခုမှာ ကိုယ်တပ်ဆင် အသုံးပြုမယ့် ပစ္စည်းကဘယ်လောက်တောင် တပ်ဆင်မှာလဲပေါ့။ အကယ်၍ပစ္စည်းအရေအတွက်ဟာ ၅၀-၁၀၀ လောက်ဖြစ်မယ်ဆိုရင် Network ဟာ Segment တစ်ခုမက လိုလာပါလိမ့်မယ်။

ကွန်ရက်ကဘယ်လောက်ထိကျယ်မှာလဲ

ကွန်ရက်ကကျယ်ပြန့်ကြီးမားလေ အသုံးပြုရမယ့် Cable က Higher Bandwidth ဖြစ်ဖို့လိုလေ ကုန်ကျစရိတ်လည်းများလေဖြစ်ပါတယ်။ ဒီတော့ ဒီလိုနေရာမျိုးမှာ Fiber Optic ကိုမရွေးဘူးဆိုရင် Twisted Pair ကိုပဲရွေးပါ။ သတိထားရမှာက Hub တွေကိုနေရာချခြင်းပါပဲ။ Hub တွေကိုပြီးစလွယ်နေရာမချဘဲ

[illegible]ကြီးငယ်ပြီး နေရာချမယ်ဆိုရင် ဒီ Network ကိုအသုံးပြုမယ့် User တွေဟာအုပ်စုလိုက်ဘယ်လောက်ပဲ ကွယ်ပြန် နေပါစေ။ TP Cable ကအရောက်သွားနိုင်ပါလိမ့်မယ်။

Type	Maximum Length	Bandwidth	Installatio	Interference	Cost
UTP	100m	10-100 Mbps	Easy	High	Cheapest
STP	100m	16-100 Mbps	Moderate	Moderate	Moderate
10Base2	185m	10 Mbps	Easy	Moderate	Cheap
10Base5	500m	10 Mbps	Hard	Low	Expensive
Fiber	2-100 km	100 Mbps-10 Gbps	Very hard	None	Most expensive



UNIT 4

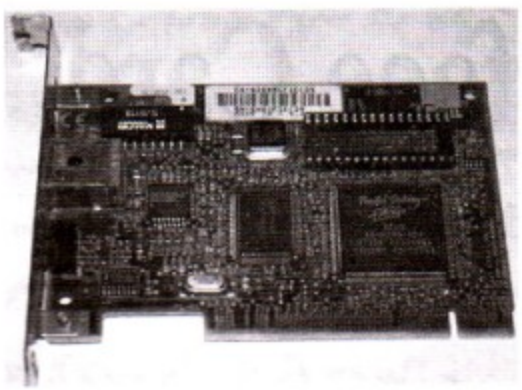
Network Interface Card

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာ Network Interface Card တွေ အကြောင်းကိုလေ့လာကြမှာဖြစ်ပါတယ်။ သူလည်းပဲ Essentials ပါပဲ။ တူတ်ပါတယ်လေ။ တကယ်တော့ ဒီတစ်အုပ်လုံး တာ Essentials ပါပဲ။

၄.၁ Network Interface Card

အခြေခံကျကျပြောရရင်တော့ ကွန်ပျူတာမှာ ဒီ Network Interface Card (အတိုကောက် NIC Network Card)ဆိုတာကြီးရှိမှ Network Medium (ကြားခံပစ္စည်းတွေဖြစ်ကြတဲ့ Cable ကြိုး)တွေကို လာတပ်လို့ရမှာဖြစ်ပါတယ်။ ဒီတော့ အခုလေ့လာကြမယ့် Network Card အခန်းဟာလည်း အတော်လေး ကိုအရေးပါလှတဲ့ သင်ခန်းစာတစ်ခုဖြစ်ပါတယ်။ ဒီ Network Card ဒါမှမဟုတ် Network Adapter လို့ လည်းခေါ်လို့ရတယ်ဆိုတာကြီးက Branded Server ကြီးတွေမှာ On Board (Built - in တစ်ခါတည်း တွဲလျက်ပါလာပြီးသား) ပါလာတတ်တာများပါတယ်။ ဒါမှမဟုတ် Network Card ကို ကွန်ပျူတာထဲက Motherboard Slot တွေမှာစိုက်လည်းရပါတယ်။ ခုနောက်ပိုင်းတော်တော်များများ Motherboard တွေမှာ Network Adapter ဟာ On Board ဖြစ်လာကြပါပြီ။ Laptops ကွန်ပျူတာတွေမှာလည်း ဒီ Network Adapter ဟာ On Board တွေများပါတယ်။ အဲ့သလိုမှမဟုတ်ရင်လည်း အခြား Interface တွေဖြစ်ကြတဲ့ PC Card စတာတွေနဲ့ Network ကိုတပ်ဆင်လို့ရပါတယ်။ ကဲဗျာ ဘယ်လိုပဲဖြစ်ဖြစ် ကွန်ပျူတာတစ်လုံးမှာ Network Medium လာတပ်ဖို့ Network Card ကတော့ရှိနေရမှာအသေအချာပါပဲ။ ကျွန်တော်တို့ဟာ ဒီ သင်ခန်းစာမှာ Network Card တွေ ဘယ်လိုအလုပ်လုပ်သလဲဆိုတဲ့အကြောင်းကို လေ့လာကြမှာဖြစ်ပါတယ်။ နောက်ပြီးတော့ Network Card ကိုကွန်ပျူတာမှာဘယ်လိုတပ်ဆင်မလဲ။ ဘယ်လို Configuration လုပ်မလဲဆိုတာကိုပါ လေ့လာကြမှာဖြစ်ပါတယ်။

ပုံ ၄.၁



Network Card ကိုတွေ့ရစဉ်

၄.၂ Network Card အခြေခံ

Network Card တစ်ခုဟာ ဘယ်ကွန်ပျူတာမှာပဲ တပ်ထားတပ်ထား သူလုပ်ဆောင်တဲ့ လုပ်ဆောင်ချက် အဓိကအားဖြင့်ပေါ့နော် (၂)ချက်ရှိပါတယ်။ အဲ့ဒါတွေကတော့-

(၁) Network Connection များပြုလုပ်ခြင်းနှင့် ၎င်း Connection များကို Manage လုပ်ခြင်း။

(၂) ကွန်ပျူတာထဲက Data တွေကိုအသုံးပြုထားတဲ့ သက်ဆိုင်ရာ Medium ပေါ်လိုက်ပြီး ဘာသာပြန်ပေးရတယ်။

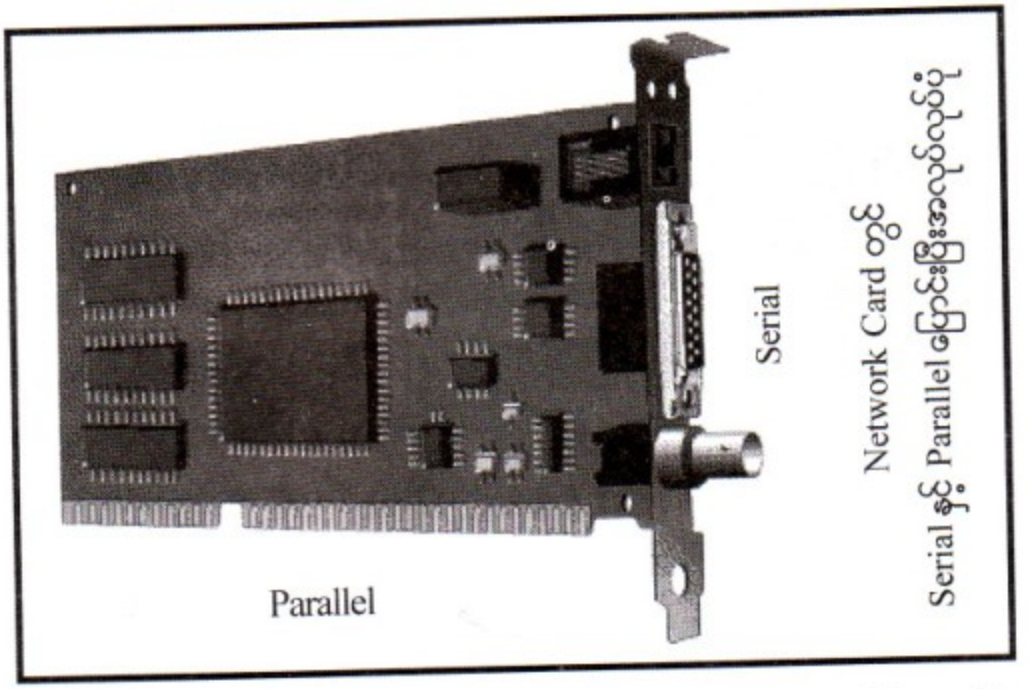
ဒါမှ Data တွေဟာ Signal တွေဖြစ်သွားပြီး ကွန်ပျူတာရဲ့ပြင်ပကို Message တွေအဖြစ်ထွက်သွားနိုင်မယ်။ အဲဒီလိုပဲ တစ်ခါအပြင်ကဝင်လာတဲ့ Signals တွေကိုလည်းကွန်ပျူတာထဲမှာ Data တွေ ပြန်ဖြစ်သွားအောင်လို့ ဘာသာပြန်ပေးရပါတယ်။

အတိုချုပ်ပြောရရင်တော့ Network Card တွေဟာ ကွန်ပျူတာနှင့် Network ကိုဆက်သွယ်ပေးတယ်။ ထိန်းချုပ်ပေးတယ် ဆိုပါတော့ဗျာ။

၄.၃ Network Card များအလုပ်လုပ်ပုံ

ကျွန်တော်တို့ကွန်ပျူတာမှာ Network Card တပ်ဆင်ထားခြင်းရဲ့သဘောသဘာဝအရကိုက Network Adapter တွေဟာ Network ကရရှိလာတဲ့ Data တွေကိုပုံစံပြောင်းခြင်းအလုပ်ကိုလည်း လုပ်ဆောင်ပေးရပါတယ်။ ဘယ်လိုပုံစံပြောင်းပေးရတာလဲလို့ဆိုတော့- ကျွန်တော်တို့သိကြတဲ့အတိုင်းပေါ့ဗျာ။ Computer တွေမှာက Bus ရဲ့ Data Line တွေက Parallel မဟုတ်လား။ ဒီလိုလေဗျာ CPU နဲ့ ဒီ Bus မှာ တပ်ထားတဲ့ Adapter Card တွေရဲ့အကြား Data တွေကို Send လုပ်တာက Parallel အပြိုင် Data Lines ကိုအသုံးပြုတာပါ။ ဒီ Network Adapter လည်း ဒီအတိုင်းပါပဲ။ Network Card နှင့် CPU အကြား Data တွေကို Send လုပ်ရာမှာ Parallel Data Lines ကိုအသုံးပြုပါတယ်။ ဒါကို Parallel Transmission

ပုံ ၄.၂

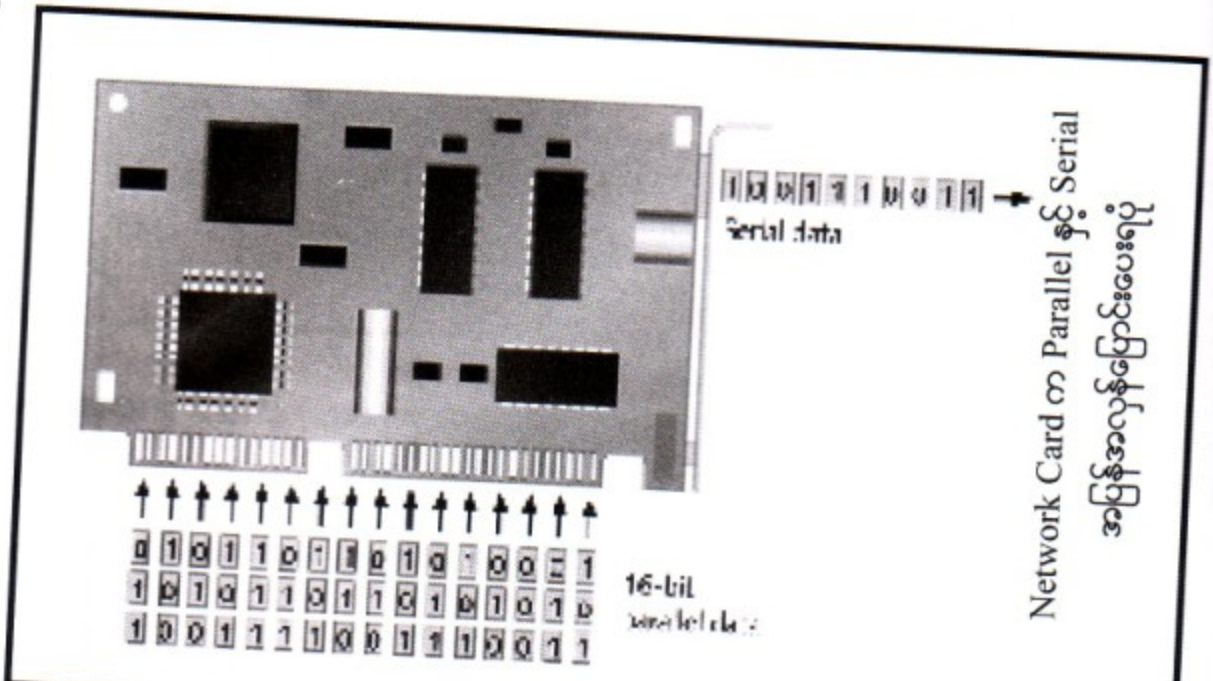


လို့ခေါ်ပါတယ်။ ပြန်ပြောပြပါဦးမယ်။ ကွန်ပျူတာထဲမှာ CPU နှင့် Network Adapter အကြားဆက်သွယ်မှုကို Parallel Transmission ဖြစ်ပါတယ်။ Parallel Transmission ဟာ Data တွေကိုပို့လွှတ်ရာမှာစီတန်းပြီးသွားတာမဟုတ်ဘဲအပြိုင်သွားတဲ့ Transmission ဖြစ်ပါတယ်။ ဥပမာ ကားတွေအပြိုင်ယှဉ်ပြိုင်မောင်းသလိုမျိုးပေါ့။

ဒါပေမယ့် ကွန်ပျူတာအတွင်းမှာ Network Adapter နှင့် ဆက်သွယ်မှုဟာ Parallel Transmission ဖြစ်ပေမယ့် Networking Media (ဥပမာ_ Cable ကြိုး)ပေါ်မှာ Data တွေ Signals တွေဟာ အပြိုင်သွားကြတဲ့ Parallel Transmission ပုံစံမဟုတ်တော့ဘူးဗျ။ ဥပမာပြောရရင် ပုရွက်ဆိတ်တွေတန်းစီပြီးသွားသလိုမျိုး။ ဒီလို Transmission မျိုးကိုကြတော့ အပြိုင်သွားတာမဟုတ်ဘဲ တန်းစီပြီးသွားတာကြောင့် Serial Transmissin လို့ခေါ်ပါတယ်။ ကဲ ကောင်းပြီ Network Medium မှာ Signals တွေဟာ Serial Transmission နှင့် Flow ဖြစ်ကြတယ်။ ခုနက Network Card နှင့် CPU အကြားကြတော့ Parallel Transmission ဖြစ်တယ်။

ရော့ ခက်ပြီ။ ဟုတ်ပါတယ်။ ဒီတော့ပြင်ပကလာတဲ့ တစ်နည်းအားဖြင့် Network Medium ကလာတဲ့ Serial Data တွေကိုရယူပြီး Network Adapter ဟာ CPU ဆီ Signal တွေကိုအပြိုင်စနစ်အဖြစ် ပြောင်းလဲပို့မှပေးပို့ရပါတယ်။ ဒီလိုပါပဲ။ CPU ဆီကအပြိုင်လာတဲ့ Data တွေကို Network Adapter ကရယူပြီး Serial အဖြစ်ပြောင်းပြီးမှ Network Medium မှာ Signal အဖြစ် Flow ဖြစ်ပေါ်စေပါတယ်။ ပြန်ပြောပါဦးမယ်။ Network Medium တွေကနေတန်းစီပြီးဝင်လာတဲ့ Signals တွေကို Network Adapter ဟာ bits တွေအဖြစ်ပြောင်းလဲပါတယ်။ ပြီးတော့ Parallel ဖြစ်အောင် bits တွေကိုပြန်ချလိုက်ပါတယ်။ ပြီးမှ Parallel Transmission အဖြစ် CPU ကို Data တွေပို့တာဖြစ်ပါတယ်။ CPU ဆီကနေ Network Adapters ဆီ ပြန်လာမယ်ဆိုရင်လည်း ဒီအတိုင်းပြောင်းပြန် ပြန်လုပ်ပြီးပို့တာဖြစ်ပါတယ်။

ပုံ ၄.၃



ဒီနေရာမှာ လူကြီးမင်းတို့အနေနဲ့ Parallel နှင့် Serial အကြောင်းကိုသိထားပြီး သိထားကောင်း ဖြစ်နေပါလိမ့်မယ်။ ဒါပေမယ့် ဒီအကြောင်းအနည်းငယ်လောက်ပြောရအောင်။ Parallel Transmission ဟာယဉ်လျက် အပြိုင်သွားတာဖြစ်တာကြောင့် ပုရွက်ဆိတ်တွေလိုတန်းစီပြီးသွားတဲ့ Serial Transmission ဆက်တော့ပိုမြန်ပါတယ်။ ဒီတော့ ပြောချင်တာကအခုမှလာမှာ။ ဒီလိုဗျ။ CPU ကအပြိုင်လာတဲ့ Data တွေ Serial အဖြစ် Network Medium ပေါ်မပို့ခင်၊ အပြင်ကတန်းစီပြီးဝင်လာတဲ့ Signal တွေ Data bits အဖြစ် CPU ဆီအပြိုင်မပို့ခင် Network Adapter ပေါ်မှာ Hold လုပ်ထားရသေးသဗျ။ မျက်စိ(ဧစ္ဆ) ထဲမြင်သလားမသိဘူး။ ပြောရရင် Network Adapter ပေါ်က Memory မှာ Hold လုပ်သေးတယ်ပေါ့ဗျာ။ ဒါကို Buffer လို့ခေါ်တယ်။ သေချာရှင်းအောင်ပြောရမယ်ဆိုရင် CPU ကနေအပြင်ကိုထွက်ဖို့လာတဲ့ Data တွေက Parallel လာတာမဟုတ်လား။ ဒါတွေကို Serial အဖြစ် စိတန်းဖို့လိုတယ်လေ။ နောက်တစ်ခုကဝင်လာတဲ့ Data တွေကလည်း စီတန်းပြီးဝင်လာတာမဟုတ်လား။ အဲ့ဒါတွေကို CPU ဆီမပို့ခင် Parallel အဖြစ် ပြန်လည် စီတန်းရသေးတယ်လေ။ ဒီအတွက် ကျွန်တော်တို့ဟာ စီတန်းဖို့စုရပ်တစ်ခုတော့ရှိရမယ်လေ။ ဒါဟာ Buffer ပဲပေါ့။

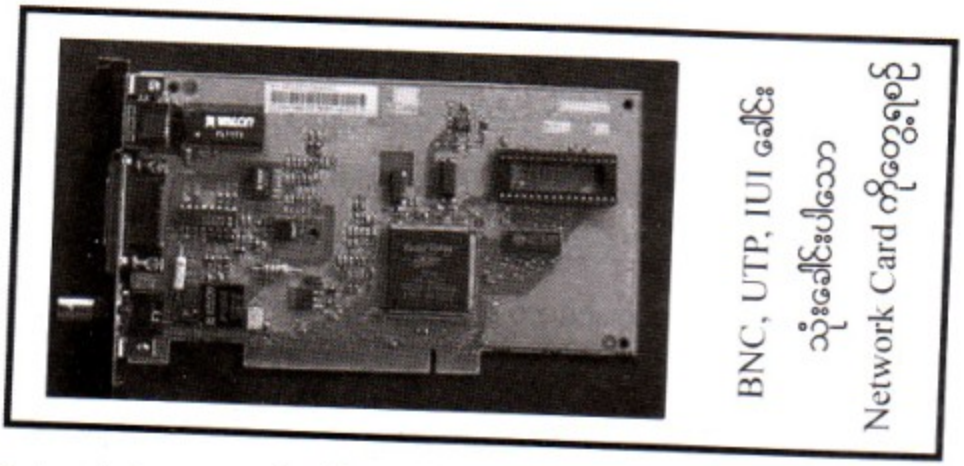
ကွန်ပျူတာစကားအရပြောရမယ်ဆိုရင်တော့ အဲ့ဒီလို Data တွေအပြိုင်စုစည်းပြီးပေးပို့တဲ့အခါမှာ အသုံးပြုတဲ့လမ်းကြောင်းကို Bus လို့ခေါ်ပါတယ်။ ကွန်ပျူတာထဲမှာ Data တွေဟာ တစ်နေရာမှ တစ်နေရာကို သွားတဲ့အခါကြ ဒီ Bus တွေကနေသွားတာဖြစ်ပါတယ်။ PC တွေရဲ့စစချင်း ကနဦး Bus တွေကတော့ 8 bit ဖြစ်ပါတယ်။ ဆိုလိုတာက အပြိုင် ၈ လိုင်းသွားတယ်ပေါ့ဗျာ။ တစ်ခါသွားရင် တစ်လိုင်းမှာတစ်ခုနှင့်ဆိုတော့ ပေါင်း ၈ခုပို့နိုင်တာပေါ့။ ဒါကို Bus Width လို့ခေါ်ပါတယ်။ Bus Width ဆိုတာ Bus မှာအပြိုင်ဘယ်နှစ်လိုင်းရှိသလဲဆိုတာကိုပြောတာပါ။ Bus မှာ အပြိုင် ၈လိုင်းသွားနိုင်ရင် ဒီ Bus ရဲ့ Bus Width က 8 bit အကျယ်ရှိတယ်လို့ဆိုလိုချင်တာဖြစ်ပါတယ်။ ISA Bus မှာဆိုရင်တော့ နှစ်မျိုးရှိပါတယ်။ ISA 8 bit နှင့် ISA 16 bit တို့ဖြစ်ကြပါတယ်။ EISA နှင့် MCA တို့မှာလည်း 16 bit နှင့် 32 bit ဆိုပြီး ရှိပါတယ်။ ထို့အတူ PCI Bus မှာဆိုရင်လည်း 32 bit နှင့် 64 bit ဆိုပြီး နှစ်မျိုးရှိပါတယ်။ ဒီအကြောင်းကို ပြီးမှသိခြားဖော်ပြပါဦးမယ်။

Network Adapter တစ်ခုဟာ Data တွေကို Network Medium မှတစ်ဆင့် Transmit လုပ်ပို့ရာ၌ Network Adapter မှာ Transceiver ဆိုတာပါကိုပါရှိရမှာဖြစ်ပါတယ်။ ၎င်းပါရှိတဲ့ Transceiver ဟာလည်း Network ကအသုံးပြုထားတဲ့ Network Medium (Cable) လာတပ်မယ့်ခေါင်းနှင့်အတူ အလုပ်လုပ်နိုင်အောင်လည်း ကိုက်ညီနေရပါမယ်။ ဥပမာဗျာ - Network Card က Ethernet တော့ Ethernet ပဲ။ ဒါပေမယ့် ဒီ Network Card က 10BaseT RJ-45 သုံးထားသလား၊ Thinnet ဖြစ်တဲ့ BNC ကိုသုံးထားသလား စသည့်အသုံးပြုထားတဲ့တစ်ခုနှင့် ကိုက်ညီ တဲ့တွဲအလုပ်လုပ်မယ့် Transceiver မျိုးလည်း ဖြစ်ရမယ်လို့ ပြောတာပါ။

ဒီနေရာမှာ အကြောင်းစပ်လို့ Network Card ရဲ့ Connector တွေအကြောင်းပြောပြဦးမယ်။ ပုံမှာလည်း မြင်တွေ့ရမှာပါ။ Female BNC Connector ကတော့ Thinnet အတွက်ပဲဖြစ်ပါတယ်။ AUI

Connector ကတော့ Thicknet အတွက်ပဲဖြစ်ပါတယ်။ RJ-45 Connector ကတော့ 10BaseT အတွက်ပဲ ဖြစ်ပါတယ်။ ဒီနေရာမှာ Network Card ဟာ အမျိုး Connector (၃)ခုစလုံးတစ်ခါတည်းပါချင်လည်းပါမယ်၊ နှစ်ခုပါချင်လည်းပါမယ်။ တစ်ခုတည်းလည်းဖြစ်ချင်ဖြစ်မယ်။ ဒီ Card ကအသုံးပြုထားတဲ့ Connector ပေါ်မူတည်ပြီးတော့ Card ရဲ့ အလုပ်လုပ်ဆောင်မှု လျှပ်စစ်ပတ်လမ်းလည်းပြောင်းလဲတာပေါ့။ ပြောရမယ်ဆိုရင် Thinnet နှင့် 10BaseT ကိုသာသုံးထားတဲ့ Network Card ဟာဝင်း Connector အတွက်လိုအပ်တဲ့ Transceiver ဟာ ဒီ Network Card ပေါ်မှာတင် ပါပါတယ်။ သိုးခြားထပ်မလိုဘူး။ ဆိုလိုတာက Thinnet နှင့် 10BaseT အတွက်လိုအပ်တဲ့ Transceiver က အဲ့ဒီ Network Card ပေါ်တွင် ပါပြီးသားဖြစ်ပြီး Thicknet အတွက်ကတော့ External Transceiver လိုအပ်ပါတယ်။ ပြောရမယ်ဆိုရင် Thicknet အတွက် Transceiver တာ On Board (Built-in ပါပြီးသား) မဟုတ်ဘဲ အဲဒီ Network Card ရဲ့ AUI Connector မှာ External Transceiver ကိုလာတပ်ပေးရမှာဖြစ်ပါတယ်။ အဲ့သလိုမှမဟုတ်ဘဲ Network Card ဟာ အခြားသော Media တွေကိုပါသုံးထားဦးမယ်ဆိုရင်ပေါ့ဗျာ။ ဥပမာ Fiber Optic Cable အတွက် အိမ့မဟုတ် အခြို့သော Wireless နည်းပညာများကိုပေါ့နော် စသဖြင့် တစ်ခုခုကိုသုံးထားမယ်ဆိုရင်တော့ အဲ အခြားသော သက်ဆိုင်ရာ နည်းပညာများအလိုက် သိုးခြားသင်ခန်းစာများနှင့် ရှင်းမှဖြစ်ပါတော့မယ်။

ပုံ ၄.၄



BNC, UTP, IUI ချိတ်သုံးခြင်းပါသော Network Card ကိုတွေ့ရစဉ်

Network Card အလုပ်လုပ်ပုံအကြောင်းကို ကျွန်တော် အခုရှင်းပြနေစဉ်မှာ CPU ကနေ Parallel လာတဲ့ Data တွေကို အပြင်သို့ပို့ရန် Serial ပြောင်းခြင်း၊ အပြင်ကလာတဲ့ Incoming Serial Signal များကို CPU ဆီသို့မပို့မီ Parallel ပြောင်းခြင်း စတဲ့အလုပ်တွေကိုသိသွားပြီးနောက်မှာ အဲ့ဒီလိုဖြစ်စဉ်တွေကို Serial ကနေ Parallel ပြောင်း၊ Parallel ကနေ Serial ပြောင်း ဒီကြားမှာ Network Card ဟာ Data များကိုထုတ်ပိုးခြင်းဆိုတဲ့ Data Packaging အလုပ်ကိုပါလုပ်နေရတယ်ဆိုတာကိုပါသိထားရမှာ ဖြစ်ပါတယ်။ ဟုတ်ပါတယ်။ Network Card ဟာ Data bits တွေကို Packets အဖြစ် ဖြစ်လာအောင် အစီအစဉ်တကျ ပြုလုပ်ပေးရပါတယ်။ ပြီးတာနှင့် ထုတ်ပိုးပြီးတဲ့ Packets လေးတွေကို တစ်ခုပြီးတစ်ခုတန်းစီပြီး Serial အဖြစ် Network Medium ပေါ်တင်ပေးလိုက်တာဖြစ်ပါတယ်။ အဝင် Message တွေအတွက်ကတော့ (Network Medium ကလာတဲ့ Data တွေ) Network Card ကဝင်လာတဲ့ Signal တွေကို ဦးဆုံး Data

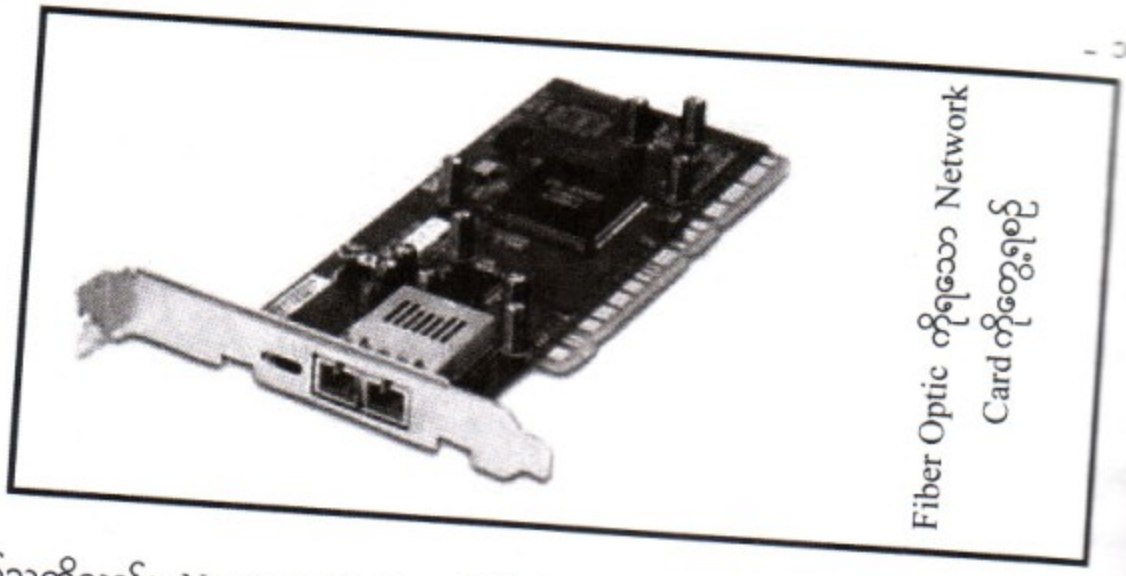
Packets အဖြစ်ပြန်ပြုလုပ်ရပါသေးတယ်။ ဒီတော့မှ Signals ကနေ Data Packets လေးတွေဖြစ်သွားပြီး ၎င်းတို့ကို တစ်ခါ Data Pacts အတွင်းပါရှိတာတွေကို (Extracts) ဆွဲထုတ်ပြီးသကာလ Parallel ဖြစ်အောင်ပြုလုပ်ပြီး CPU ဆီကိုပေးပို့ပါတယ်။ ဒီနေရာမှာ ရင်းနှီးနေရမယ့်အချေအတေါ်တစ်ခုကတော့ Packets ဆိုတာပါပဲ။ Network Transmission မှာက Data တွေကိုပေးပို့ခြင်း၊ လက်ခံခြင်းဆိုတဲ့အခါတွေမှာ Data တွေကို ခုလို Packets လေးတွေထုပ်ပြီးပေးပို့တာဖြစ်ပါတယ်။

နောက်တစ်ခုအရေးကြီးတာပြောရအုံးမယ်။ Network Card က အရေးကြီးလုပ်ဆောင်နေတဲ့ အချက်တွေဟာ Packet တွေကိုပြုလုပ်ခြင်း၊ ပေးပို့ခြင်းနှင့် လက်ခံခြင်းတွေပဲမဟုတ်ဘူးဆိုတာပါပဲ။ Network Card က ဘာတွေထပ်လုပ်ရသေးလည်းဆိုတော့ ဒီ Packet တွေကိုပေးပို့တဲ့အခါမှာဖြစ်ပေါ်နိုင်မယ့် Packet Level Error တွေ၊ ရောက်လာတဲ့ Packet တွေပြည့်စုံမှုရှိမရှိဆိုတာတွေ၊ နောက်ပြီးဖတ်လို့မရတဲ့ Packet တွေ၊ ဒါတွေနဲ့ ပတ်သက်ပြီးလုပ်ဆောင်ပေးရသေးတယ်ဗျ။ Network Card ရဲ့ နောက်ထပ် အရေးကြီးလုပ်ဆောင်ရတဲ့ကိစ္စတစ်ခုကတော့ - အသုံးပြုတဲ့ Medium မှာ Data Transmission ပြုလုပ်နိုင်ရန်အတွက် Data တွေကို Package လုပ်ပေးရခြင်းနှင့် Transmission ပြုလုပ်ရန် ပြင်ဆင်ပေးရခြင်း၊ နောက်ပြီး Data တွေကို ဘယ်အချိန်မှာပို့လွှတ်ရမလဲဆိုတာကိုသိဖို့ Medium ကို Access လုပ်ရခြင်း၊ ၎င်းဖြစ်စဉ်ကို Manage လုပ်ရခြင်းတို့ဖြစ်ကြပါတယ်။

နောက်ပြီး Network Adapter ဟာသူ့ဆီကိုရောက်ရှိလာတဲ့ Network Packets လေးတွေမှာ အခြားသော ကွန်ပျူတာတစ်လုံးရဲ့ Network Card Address ပါရှိလာမှုကိုရှာဖွေခြင်းများပြုလုပ်ရပါတယ်။ ပြောရမယ်ဆိုရင်တော့ဗျာ။ Network Card ဟာ တံခါးမှူးလိုပေါ့။ ဝင်လာတဲ့ Data တွေ၊ ထွက်သွားမယ့် Data စတာတွေအတွက် တံခါးမှူးလုပ်ပေးနေရပြီ။ Communication ဖြစ်အောင်လည်း ပြုလုပ်ပေးနေရတာပေါ့။

တစ်ခို့ Network Card တွေကြတော့ ထူးခြားတာက - သူကဗျာ Network Card က သူ့ဆီကိုဝင်လာမယ့် Data Packets လေးတွေကိုကြိုတင်ပြီးမြင်နေရတယ်။ ဒါတွေကဘယ်မှာသုံးသလဲဆိုတော့ Network ကိုစောင့်ကြည့်တဲ့ Scanning Software တွေပေါ့။ အဲ့ဒီမှာ ၎င်း Software က Network မှာသွားလာလှုပ်ရှားနေကြတဲ့ Traffic ကိုခြုံပြီးကြည့်နေတယ်။ ပြီးတော့ ဒါမှမဟုတ်လည်း Packets တစ်ခုချင်းစီကို အသေးစိတ်စစ်ဆေးပါတယ်။ ဒီတော့ Network Card ဟာ သူ့ဆီကိုလာမယ့် Packets တွေကိုကြိုသိနေတယ် လို့အကျဉ်းချုပ်ပြောချင်တာပေါ့ဗျာ။ ဒီလိုနဲ့ မရွေးချယ်ချင်တဲ့ Packets တွေရှိရင် Network Card ဟာ တံခါးမှူးတွေလိုပဲ ဂိတ်ကိုပိတ်လိုက်ပါတယ်။ ဒီလို အလုပ်လုပ်တဲ့ Function ကို Promiscuous လို့ခေါ်ပါတယ်။ အဓိပ္ပါယ်ကတော့ အလွယ်ပြောရရင် မရွေးချယ်ဘူးလို့ဆိုလိုချင်တာဖြစ်ပါတယ်။ ဒါဟာတကယ်တော့ ပုံမှန် Network အသုံးပြုသူတွေအတွက်မလိုအပ်လှပါဘူး။

Network Card နဲ့ ဂိတ်တံခါးမှူးတာဝန်ဟာ ဒီမှာတင်မပြီးဆုံးသေးပါဘူး။ အရေးကြီးတဲ့ နောက်တစ်ခုရှိပါသေးတယ်။ Wire ကြိုးကိုဖြတ်သန်းပြီးပေးပို့လိုက်တဲ့ Data တွေဟာ ဘယ်ကိုထွားမှာလဲဆိုတဲ့ သက်ဆိုင်ရာ



Fiber Optic ကိုရသော Network Card ကိုတွေ့ရစဉ်

လက်ခံမည့်သူကိုလည်း Network Card ကဆုံးဖြတ်ပေးရပါသေးတယ်။ အို စာဖတ်သူလူကြီးမင်း အသင်ရှုပ်မသွားပါနဲ့။ Network Card တစ်ခုချင်းစီမှာ မတူညီတဲ့ Identifier ရှိပါတယ်။ အဲကို Network Address လို့ခေါ်ပါတယ်။ ဒီ Address က ဘယ်ကလာသလဲဆိုတော့ ၎င်း Network Card ပေါ်က Read Only Memory (ROM) ထဲ Program လုပ်ထားတဲ့ Data ဆိုကရတာဖြစ်ပါတယ်။ ဒီအကြောင်းအရာက အတိုချုပ်ပြောရမယ်ဆိုရင် IEEE (Institute of Electrical & Electronics Engineer) က Network Card ထုတ်လုပ်သူတွေကို Network Card ထုတ်လုပ်ရာမှာ Network Card တစ်ခုချင်းစီ မတူညီတဲ့ Network Address ကို ဘယ်လိုပေးရမလဲဆိုတဲ့ Addressing Scheme ကို Design သတ်မှတ်ပေးထားပြီးသားဖြစ်ပါတယ်။ ဒီတော့ ပြောရမယ်ဆိုရင် Network Card အသစ်တစ်ခုတည်ဆောက်ပြုလုပ်တိုင်းမှာ မတူညီတဲ့ Address တစ်ခုချင်းစီပါပြီးသား ဖြစ်တာကြောင့် Network Card တပ်ထားတဲ့ ကွန်ပျူတာတိုင်းမှာ မတူညီတဲ့ Network Address တွေပိုင်ဆိုင်ထားကြပါတယ်။ ဒီတော့Network Card ရဲ့ ဂိတ်တံခါးမှူးတာဝန် အကြောင်းကို ပြန်ဆက်ပြောရမယ်ဆိုရင်ဖြင့် Decode လုပ်ထားတဲ့ Packet ထဲက Address bit ကိုကြည့် လိုက်ပြီး ကိုယ့်ဆီကနေရင် ကိုယ်ရဲ့ Address နှင့်တိုက်ယူလိုက်တာပဲဖြစ်ပါတယ်။ ဒီလိုမှ မဟုတ်လည်း သက်ဆိုင်ရာ Address ဆီကို Deliver ဖြစ်သွားမှာဖြစ်ပါတယ်။

Network Card ရဲ့ Address ပိုင်းဆိုင်ရာကို ဆက်ပြောရဦးမယ်ဆိုရင် – ဘယ် Network Card ပေါ်က Address ပဲဖြစ်ဖြစ် ၎င်း Address ကို MAC Address လို့ခေါ်ပါတယ်။ MAC ဆိုတာ Media Access Control ဖြစ်ပါတယ်။ ၎င်းဟာ Network Card ရဲ့ Media Access Control Function ကိုလုပ်ဆောင်ပေးတာဖြစ်ပါတယ်။ ဒီ MAC အကြောင်းကို ကျွန်တော်တို့ OSI သင်ခန်းစာကြမှ လေ့လာရမှာ ဖြစ်ပါတယ်။ ဒီ Address တာ Hexadecimal Format ဖြင့် နှစ်လုံးတွဲစီကို Colon ခြားကာ အားလုံး ၆တွဲရှိတာဖြစ်ပါတယ်။ ဥပမာ –

00 : 60: 97: 33: 90: A3

Produced by YOUTH Computer Co., Ltd

စသဖြင့်ပါ။ ၎င်း ၆တွဲထဲက ပထမ ၃တွဲကတော့ ထုတ်လုပ်သူကိုရည်ညွှန်းတာဖြစ်ပြီး နောက် (၃) တွဲကတော့ မတူညီတဲ့ Network Address ပဲဖြစ်ပါတယ်။ ကဲ ဒီလောက်ဆိုရင် Network Card ရဲ့လုပ်ဆောင်ချက်တွေကို သိလောက်ပါပြီ။ Network Card ဟာ Data တွေကို Network မှ CPU, CPU မှ Network အပြန်အပြန် အလှန်လှန်ပေးပို့ခြင်းကို Transfers လုပ်ရတဲ့ အပြင် Parallel နှင့် Serial ပြောင်းခြင်းစတာတွေကိုလည်း လုပ်ရတယ်။ နောက်ပြီး အသုံးပြုထားတဲ့ Network Medium ကိုလိုက်ပြီး ဘယ်လို Data Transmit လုပ်ရမယ်ဆိုတာကိုလည်းဆုံးဖြတ်ရပါတယ်။ Network Card ရဲ့လုပ်ဆောင်ချက်တွေကိုစာဖွဲ့ပြီးမပြောဘဲ အချက်နှင့်ပြောရမယ်ဆိုရင်-

(၁) Network Card ဟာကွန်ပျူတာမှ Data များကို Network Medium မှာ Flow ဖြစ်သွားစေရန် အတွက်ပြင်ဆင်ပေးရမယ်။ ပြုလုပ်ပေးရမယ်။

(၂) ပြီးရင်ကွန်ပျူတာတွေဆီကိုအချက်အလက်များပေးပို့ခြင်းကိုတာဝန်ယူရမယ်။

(၃) အဲ့ဒီလိုအချက်အလက်တွေပေးပို့တဲ့အခါမှာလည်း Network Medium မှာ Traffic Flow ဖြစ်မှုကို လည်းထိန်းချုပ်ပေးရမယ်။

(၄) ကွန်ပျူတာဆီကို Cable တွေမှတစ်ဆင့်ရောက်ရှိလာတဲ့အချက်အလက်တွေကို CPU နားလည် စေမယ့် bit အဖြစ်ပြန်လည်ပြောင်းပေးရမယ် စတာတွေပဲဖြစ်ပါတယ်။ အိုအချုပ်ပြောတာပါ။

၄.၄ Bus အကြောင်း

Network Card လာတပ်မယ့် Bus တွေနှင့်ပတ်သက်လို့ရှင်းပြချင်ပါသေးတယ်။ ပြီးမှ Connector တွေအကြောင်းရှင်းပြပါမယ်။ Cable တပ်ဆင်ပုံကတော့ ပြီးခဲ့တဲ့သင်ခန်းစာမှာဖော်ပြခဲ့ပြီးဖြစ်ပါတယ်။ ကဲ Bus ဆိုတာတကယ်တော့ ကွန်ပျူတာ Hardware ပိုင်းသင်ခန်းစာနှင့်ဆက်နွယ်နေတာဖြစ်ပါတယ်။ ဒီ စာအုပ်မှာ Bus နှင့် Connector သင်ခန်းစာကိုတော့ တစ်လက်စထဲပဲဖော်ပြလိုက်ပါတော့မယ်။ ကွန်ပျူတာတွေ စတင်လာကတည်းက Bus ဆိုတာကရှိခဲ့တာလားဗျ။ အဲ့ဒီတုန်းကတော့ 8 bit Bus ပေါ့။ ကဲဒီတော့ PC Bus ရဲ့အဓိက Bus များကိုအောက်မှာရှင်းပြလိုက်ပါတယ်။

ISA (Industry Standard Architecture)

ဒီ ISA Bus ကတော့ ကွန်ပျူတာတွေစတင်ကတည်းက ပထမဦးဆုံးပါလာတဲ့ Bus တွေပဲဖြစ်ကြပါတယ်။ ၎င်းဟာ 8 bit ရှိပါတယ်။ အဲ ဒီပေမယ့် ၁၉၈၄ ခုနှစ်မှာ IBM က Advanced Technology လို့ဆိုတဲ့ AT PC တွေကိုထုတ်လုပ်လိုက်တဲ့အခါမှာတော့ ၎င်းဟာ 16 bit ဖြစ်သွားပါတယ်။ ဒီ AT ကွန်ပျူတာတွေ

မတိုင်ခင်တုန်းကတော့ Extended Technology လို့ခေါ်တဲ့ XT Pc တွေပေါ့။ ဒီ ISA Bus တွေရဲ့ Speed က 10MHZ လောက်ထိပဲရှိပါတယ်။ ပြောရမယ်ဆိုရင် 286 Processor တွေစတင်တဲ့ Speed နှင့်တူတူ လောက်ရှိပါတယ်။ ဘာလိုပဲဖြစ်ဖြစ်ပါ ဒီ ISA Bus တွေဟာ ဒီနေ့ထက်ထိ ကွန်ပျူတာတွေမှာ Low Performance Bus အတွက်ရှိနေရဆဲပဲဖြစ်ပါတယ်။ အထူးသဖြင့်တော့ Slow Devices တွေဖြစ်ကြတဲ့ Floopy Drives တို့၊ Speed နှေးတဲ့ Serial Interface အတွက်ရှိနေရဆဲပဲဖြစ်ပါတယ်။

EISA (Extended ISA)

၁၉၈၈ လောက်တုန်းကပေါ့။ တကယ့်ကိုစွမ်းဆောင်ရည်မြင့်မားတဲ့ High-End Network Server တွေမှာအသုံးပြုတဲ့ ဒီ PC Bus တွေဟာ 16 bit လောက်နဲ့တော့ လုံလောက်တဲ့စွမ်းဆောင်မှုမျိုးမပေးနိုင်တော့ပါဘူး။ ဒီတော့ PC Clone Verdor အဖွဲ့အစည်းကနေပြီးတော့ Compaq Computer ကိုဦးဆောင်စေကာ 32 bit EISA Bus ကိုထုတ်လုပ်ခဲ့ပါတယ်။ ဒီ EISA Bus မှာထူးခြားတာက Mechanical ပိုင်းရော Electrical ပိုင်းရော လှည့်စားမှုတစ်ခုပေါ့ဗျာ။ အဲဒါကဘာလဲဆိုတော့ ဒီ EISA Slot မှာ 32 bit EISA Adapter လာစိုက်လို့လည်းရသလို 16 bit ISA Adapter လည်းလာစိုက်လို့ရသဗျ။ ဒီ EISA Slot ဟာ Slot မြောင်းက နည်းနည်းနက်နက်ထားတယ်ပေါ့။ 32 bit ကနက်တယ်။ အဲ့ဒီ EISA Bus မှာ ISA 16 bit Adapter ကို စိုက်လိုက်ရင် အဲ့ဒီလောက်အနက်ထိမသွားဘူး။ ပြန်ပြောပြမယ်။ EISA Bus မှာ ISA 16 bit Card လာစိုက်ရင် Slot မြောင်းရဲ့အောက်ဆုံးအနက်အထိစိုက်မဝင်သွားဘူး၊ အောက်အနက်အထိဝင်သွားရင် 32 bit ဖြစ်သွားရော။ ဒီတော့ EISA Slot မှာ 32 bit EISA Card လာစိုက်မှ အောက်ခြေဆုံးအနက်အထိဝင်သွားမယ်။ EISA Bus ရဲ့ Width က 32 bit ဖြစ်ပေမယ့် Bus Speed ကတော့ ISA 16 bit နှင့်အတူတူပါပဲ။ 10 MHZ ပဲဖြစ်ပါတယ်။ ဒီပေမယ့် EISA ကနောက်ဆုံးပေါ် (အဲ့ဒီတုန်းကပေါ့နော်) ဆန်းသစ်တဲ့ Bus Control တွေပါလာ ပါတယ်။ ISA ထက်စာရင်ပေါ့နော်။ ဘယ်လို Bus Control လည်းဆိုတော့ ပြောရရင် Bus Mastering ပေါ့။ Bus Mastering ကအချုပ်ပြောရရင် အချက်အလက်တွေကို အခြားပစ္စည်းတွေဆီကို ပေးပို့ရာမှာ CPU ကိုစောင့်နေစရာ မလိုပါဘူး။

MCA (Micro Channel Architecture)

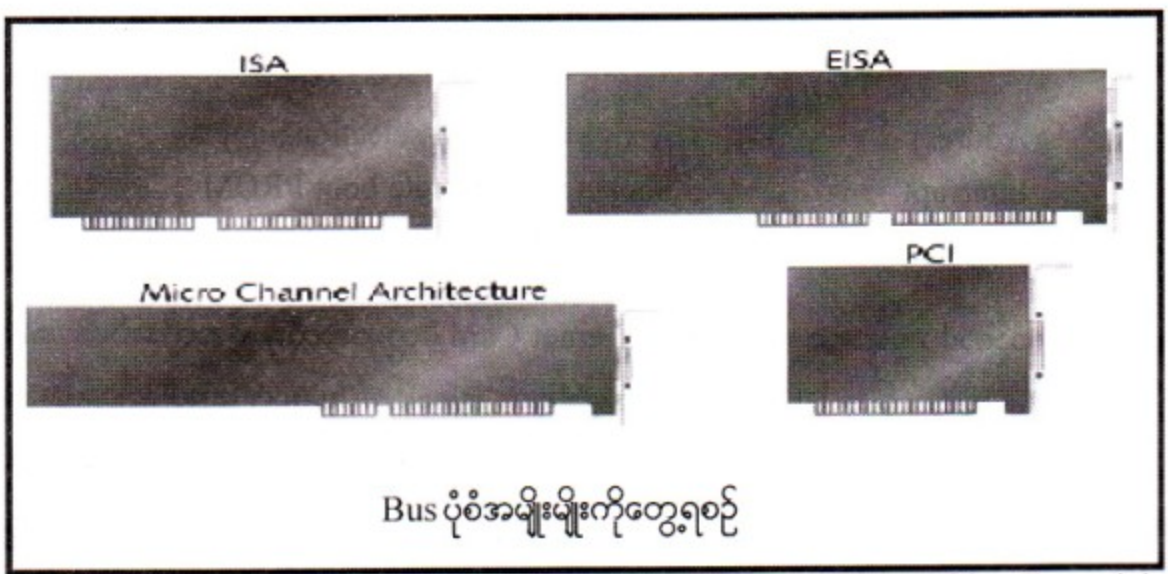
အပေါ်ကရှင်းပြခဲ့တဲ့ EISA ဖြစ်ပေါ်လာနေချိန်နှင့် တစ်ပြိုင်နက်မှာပဲ IBM ဟာ သူရဲ့ PS/2 Computer တွေမှာ 32 bit MCA Bus ကိုစတင် မိတ်ဆက်လာပါတော့တယ်။ MCA Bus က 16 bit နှင့်ပဲဖြစ်စေ 32 bit နှင့်ပဲဖြစ်စေ Bus Speeds အမျိုးမျိုး Support လုပ်နိုင်ပါတယ်။ MCA ဟာ PC မဟုတ်တဲ့အပိုင်းတွေမှာ 66 MH_z အထိအလုပ်လုပ်နိုင်ပြီးတော့ PC တွေမှာဆိုရင်ဖြင့် 5 MHZ မှ 20 MHZ အထိအလုပ်လုပ်ပေးနိုင်တာကြောင့် ISA ထက်တော့ ပိုပြီးမြန်တယ်လို့ပြောရပါမယ်။ နောက်ပြီးသူက Bus Mastering လည်း

လုပ်ပေးနိုင်ပါတယ်။ ဒါပေမယ့်ပေါ့ခင်ဗျား IBM က ၎င်းရဲ့ MCA ကိုဈေးကွက်အတွက်ဖွင့်မပေးခဲ့ဘူးခင်ဗျ။ ဒါကြောင့်စာဖတ်သူလူကြီးမင်းတိုင်း MCA ကိုကြားဖူးချင်မှကြားဖူးပါလိမ့်မယ်။ IBM ဟာ ၎င်း PC တွေမှာ ISA နှင့် PCI ကို Support လုပ်နေသည့်တိုင် ၎င်းရဲ့ RISC/6000 နှင့် ES/9370 ကွန်ပျူတာတွေမှာ MCA ကိုအသုံးပြုနေဆဲပဲဖြစ်ပါတယ်။

PCI (Peripheral Component Interface)

သိပ်ကိုမြန်ဆန်လာတဲ့ CPU တိုင်းဟာ ပိုမိုမြန်ဆန်တဲ့ BUS ကိုလိုအပ်စမြဲပဲ။ အဲ့ဒီမှာ ထုတ်လုပ်သူတွေဟာ Local Bus ကိုထုတ်လုပ်ဖို့အကြံရှိခဲ့ကြပါတယ်။ ၎င်းဟာ ယခင်နည်းပညာဟောင်းများလိုပါပဲ။ CPU ဟာ RAM နှင့်အဆက်အသွယ်ပြုလုပ်ပြီးတော့ Co-Processor ကအခြားသော Peripherals တွေနှင့် အဆက်အသွယ်ပြုလုပ်ပါတယ်။ ဒီ ၁၉၉၀ နှစ်များဝန်းကျင်တွေမှာ ဒီ Local Bus ဟာ စံ စနစ်တွေ အမျိုးမျိုး ပေါ်ပေါက်လာခဲ့သော်လည်း ၁၉၉၅ ခုနှစ်မှာ Intel ရဲ့ PCI Bus ဟာ 32 bit ဖြင့် စံ ပေါ်ပေါက်လာခဲ့တာကြောင့် Local Bus လည်းရပ်တန့်ခဲ့ရပါတယ်။ ကနေ့ခေတ်မှာတော့ PCI Bus တွေဟာ 64 bit နှင့် ဖြစ်ကြပြီး နောက်ပိုင်းမှာတော့ 128 bit ဖြစ်ပေါ်လာဖို့ရှိပါတယ်။ PCI ရဲ့ Bus Speed ဟာ 33 MHz ဖြစ်ပေမယ့် PCI 2.1 ကတော့ 66 MHZ ဖြစ်ပါတယ်။ PCI ဟာ Bus Mastering လည်းရပါတယ်။ နောက်ပြီးတော့ ပြောရမယ်ဆိုရင် Microsoft ရဲ့ Plug and Play နည်းပညာနှင့်အလုပ်လုပ်တဲ့ ပထမဦးဆုံးသော Bus လည်းဖြစ်ပါတယ်။ နောက်တစ်ခုပြောရမယ်ဆိုရင် PCI က Interrupt ကိုလည်း Sharing လုပ်ပေးနိုင်ပါတယ်။ ဒါဟာကောင်းတဲ့အချက်တစ်ခုပေါ့။ ဘာလို့လည်းဆိုတော့ PCI Adapters တွေကိုတစ်ခုထက်မက ကွန်ပျူတာတွေမှာတပ်ထားမယ်ဆိုရင် ၎င်းတို့ဟာ Adapter တစ်ခုချင်းစီအတွက်မတူညီတဲ့ IRQ တွေ မလိုအပ်ဘဲ IRQ တစ်ခုထဲမှာပင် Share လုပ်ပြီးသုံးနိုင်ပါတယ်။ ဆိုလိုချင်တာက ကွန်ပျူတာထဲက PCI Card မှန်သမျှ အားလုံးအတွက်လွတ်နေတဲ့ Free ဖြစ်တဲ့ IRQ တစ်ခုပဲလိုအပ်ပါတယ်။

ပုံ ၄.၆



Bus ပုံစံအမျိုးမျိုးကိုတွေ့ရစဉ်

၄.၅ Ethernet Board Settings အကြောင်းသိကောင်းစရာ

ဟိုတစ်ချိန်တုန်းကပေါ့ ကြာတော့ကြာပါပြီ။ အဲဒီတုန်း Ethernet NIC (Network Interface Card) (Network Card ကိုပြောတာ) တွေမှာ သူတို့နဲ့ Address နဲ့ Interrupts တွေသတ်မှတ်ပေးဖို့ Jumper တွေပါရှိကြပါတယ်။ အဲဒီ Jumper တွေကိုအသုံးပြုပြီး ၎င်း Network Card ရဲ့ Address ရဲ့ Interrupts တွေကိုသတ်မှတ်ရပါတယ်။ ဒီပေမယ့်နောင်းပိုင်း Ethernet NIC တွေကတော့ ဒီလိုမဟုတ်တော့ပါဘူး။ သူတို့မှာ Network Card နဲ့အတူပါလာတဲ့ Driver Disk ထဲမှာ Diagnostic Program တွေပါလာပါတယ်။ အဲဒီ Program ကိုအသုံးပြုပြီးတော့ Interrupt နဲ့ Memory Address Setting တွေကိုပြင်လို့ရပါတယ်။ ပိုပြီးလွယ်သွားတာပေါ့။ သတ်မှတ်ပြီးရင်တော့ ၎င်းတို့ကို Program ထဲမှာပဲသိမ်းပေးရတယ်။ အချက်အလက်တွေကိုတော့ Network Card ပေါ်မှာပါတဲ့ အထူးပြုလုပ်ထားတဲ့ Memory Chip ပေါ်မှာသိမ်းရတာပေါ့ဗျာ။ Ethernet Network တွေမှာ Transmission Media ဥပမာ Network ကြိုးတွေလာချိတ်ဖို့ ခေါင်း Connection တစ်ခု (သို့မဟုတ်) နှစ်ခု ဒီမှမဟုတ် သုံးခုအထိရှိတတ်ပါတယ်။ အဲဒီတွေကတော့ -

- ❖ Coaxial Cable တနည်း Thin Ethernet အတွက် BNC Connection
- ❖ UTP ဆိုတဲ့ Unshielded Twisted Pair အတွက် RJ-45 Connection
- ❖ Thick Ethernet တွေမှာအသုံးပြုတတ်တဲ့ External Transceives တွေချိတ်ဆက်ဖို့အတွက် DIX Connector တို့ပဲဖြစ်ကြပါတယ်။

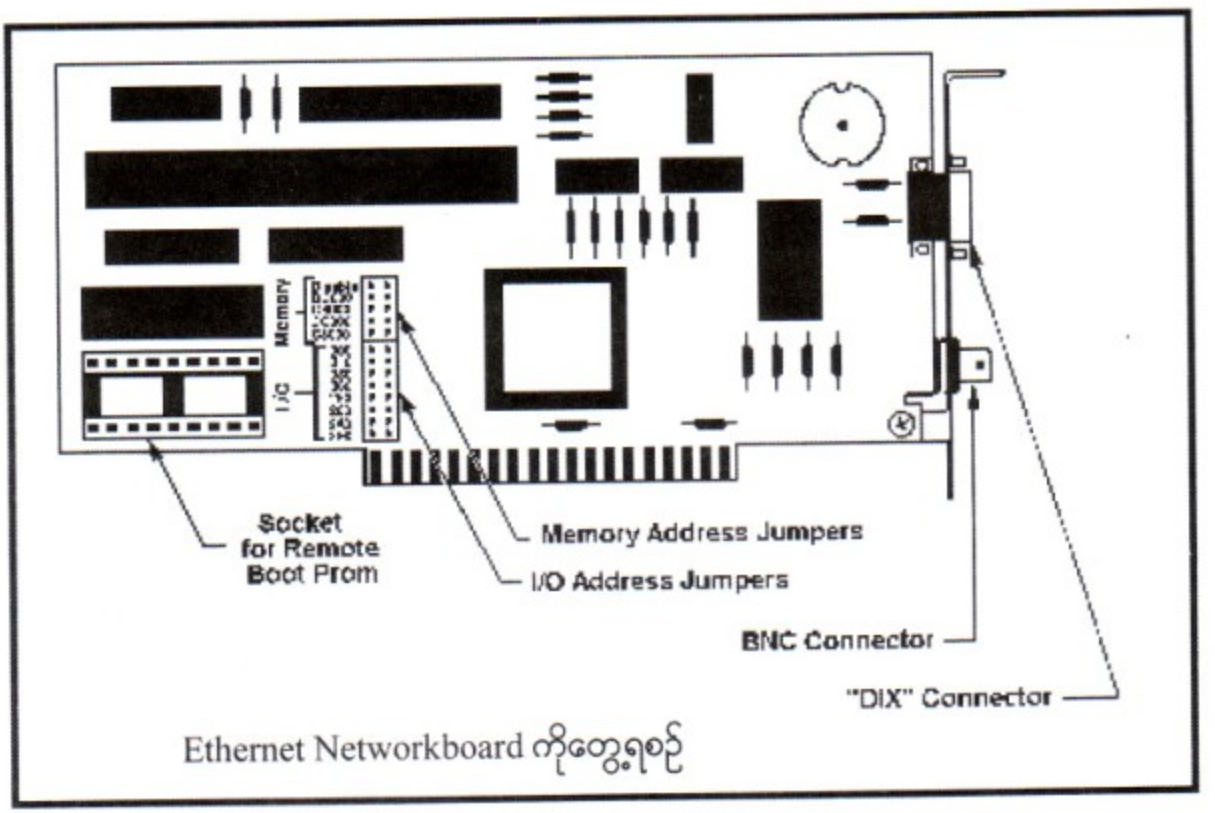
Digital, Intel နဲ့ Xerox တို့ဟာ သူတို့ထုတ်လုပ်ခဲ့တဲ့ Ethernet ကိုအထိမ်းအမှတ်အဖြစ်နဲ့ သူတို့ရဲ့ အစ စကားလုံးဖြစ်တဲ့ DIX ကိုယူသုံးခဲ့ကြပါသေးတယ်။ တကယ်တော့ DIX ဆိုတာ 15 Pin Connector ပါပဲ။ တကယ်တော့ Ethernet ဆိုတာ အရင်တုန်းကနာမည်ကိုပဲ နှုတ်ကျိုးနေကြတာပါ။ တကယ်တော့ IEEE 802.3 Standard နှင့်အညီမြှင့်တင်ပြီးဖြစ်တဲ့ Ethernet ဟာ Ethernet II ပါ။ Ethernet NIC တွေမှာ ပါဝင်တဲ့ အစိတ်အပိုင်းတွေကိုပြောပြပါအုံးမယ်။

Address	Active connector selection jumper
Interrupt	Socket for a remote boot PROM
Connectors	Shard momeory selection

သူကတော့များသောအားဖြင့် Ethernet Card တွေမှာအသုံးပြုဖို့အလိုအပ်ပါ။ ဒီပေမယ့် တချို့ Network Card တွေမှာ DIP Switches ဒီမှမဟုတ် Block of Jumper များပါရှိပါတယ်။ ဘယ်အတွက်လည်းဆိုတော့ Active Connector ကိုရွေးဖို့ပါ။ ကျွန်တော်ခုနကပြောခဲ့တယ်လေ။ Ethernet Card တွေမှာ Transmission Media နဲ့ချိတ်ဆက်ဖို့ Connector တွေဟာတစ်ခုမကပါနိုင်တယ်လေ။ ဒီတော့ ကျွန်တော်တို့က

အဲဒီ Connector တွေထဲကကြိုက်တဲ့ Connector တစ်ခု၊ နှစ်ခု သုံးခုတပြိုင်တည်းသုံးလို့မရတော့ဘူး။ ကဲ ဘယ် Connector သုံးမလဲဆိုတာကိုတော့ ခုနကပြောခဲ့တဲ့ DIP Switch ဒါမှမဟုတ် Jumper တွေနဲ့ ချိတ်ဆက်ပေးရတာပါ။ အခုနောင်းပိုင်း Network Card တွေကြတော့ Jumper နဲ့ Setting လုပ်မယ့်အစား Diagnose ဒါမှမဟုတ် Configuration Software တွေနဲ့ ၎င်း Setting တွေကိုသတ်မှတ်ကြတယ်။ အခုလို Setting သတ်မှတ်ပေးတာကို Active Connector ရွေးချယ်ပေးတယ်လို့ခေါ်တာပေါ့။

ပုံ ၄.၇



Ethernet Networkboard ကိုတွေ့ရစဉ်

၄.၆ Transmission Media Adapters များအကြောင်းသိကောင်းစရာ

တခါတရံ ကွန်ရက်တွေကိုချိတ်ဆက်တဲ့နေရာမှာ တစ်ဖက်ကခေါင်းတစ်မျိုး နောက်တစ်ဖက်က ခေါင်းကတစ်မျိုးဆိုရင် သူတို့နှစ်ခုကိုလိုက်လျောညီထွေဖြစ်သွားအောင် ပြုလုပ်ပေးတဲ့ပစ္စည်းကို Adapter လို့ခေါ်ပါတယ်။ အခုကွန်ရက်မှာတော့ Transmission Media Adapter လို့ခေါ်ပါတယ်။ အဲဒီမှာ ဘာတွေ ပါဝင်လဲဆိုတော့ -

- ❖ Transervices (or MAUs) - Thick Coax Ethernet နဲ့ Computer တွေကိုဆက်သွယ်ဖို့ ဖြစ်ပါတယ်။
- ❖ Media Filer - STP DB-15 (Token Ring) နဲ့ UTR RJ-45 Connector ကို Adapt လုပ်ပေးသည်။
- ❖ Parallel Port Adapter - Laptop Computer များ သူတို့ရဲ့ Parallel Port မှတဆင့် ကွန်ရက်

(Network) ချိတ်ဆက်ပေးသည်။

❖ SCSI Port Adapter - SCSI Interface ကိုသုံးပြီးကွန်ရက်ချိတ်ဆက်ပေးသည်။

၄.၇ Transceivers များအကြောင်းသိကောင်းစရာ

Transervicers တွေဟာအမြဲတမ်း Thick Coaxial မှာအသုံးပြုသော်လည်း Thin Coaxial နဲ့ UTP တို့နဲ့အသုံးပြုတာတွေလည်းရှိပါတယ်။ တကယ်တော့ UTP နဲ့ Thin Ethernet အတွက်လိုအပ်တဲ့ Transceivers ဆိုတာ Network Card မှာပါပြီးသား။ ဒါကြောင့် Ethernal Transceivers ဆိုတာမလိုအပ်ဘူး။ Transceivers ဆိုတာ Transmitter နဲ့ Receiver ဆိုတဲ့ပစ္စည်းနှစ်ခု Function နှစ်ခုကိုပေါင်းထားတာပါပဲ။ Transceiver ထဲက Transmitter ဆိုတာ ကိုယ်ပို့ချင်တဲ့ Computer ထဲက Signal ကိုကွန်ရက်ပေါ်တင်တဲ့အခါလိုအပ်တဲ့ Signals အဖြစ်ပြောင်းပေးလိုက်ပါတယ်။ ဥပမာပြောရရင် ကွန်ရက်ဟာ UTP Cable ကိုအသုံးပြုခဲ့ရင် Transmitter ဟာကွန်ပျူတာထဲကပို့လွှတ်ချင်တဲ့ Signal ကို UTP Cable နဲ့ Connector တို့နဲ့လျောက်ပတ်တဲ့ Electrical Signals အဖြစ်ပြောင်းပေးတယ်။ အကယ်၍ကွန်ရက်ဟာ Fiber Optic Cable ကိုအသုံးပြုမယ်ဆိုရင်တော့ Computer ထဲကပို့ချင်တဲ့ Signals ကိုကွန်ရက်ပေါ်တင်ဖို့ရာ Light Signals အဖြစ်ပြောင်းပေးပါလိမ့်မယ်။

Transceiver ရဲ့ Receiver အပိုင်းကတော့ကွန်ရက်ပေါ်က Signals ကိုရရှိတာနဲ့အထက်ကပြောတဲ့အလုပ်ကိုပြောင်းလုပ်ပါတယ်။ တနည်းအားဖြင့်ပြောရရင် Computer အတွင်းထဲက လိုအပ်တဲ့ Signals ပုံစံပြန်ရအောင် ဘာသာပြန်ပေးရတာပါ။

၄.၈ Network Interface Cards (NIC) များအကြောင်းသိကောင်းစရာ

NIC ဆိုတဲ့ Network Card ဟာ Computer အတွင်းက Motherboard ပေါ်မှ Expension Slot မှာတပ်ဆင်ရတာဖြစ်ပါတယ်။ သူ့ကို ဘယ်မှာသုံးမလဲ။ ကွန်ပျူတာတွေ ကွန်ရက် (အချင်းချင်း) ချိတ်ဆက်တဲ့နေရာမှာပေါ့။

Transceiver ဆိုတာ NIC ပေါ်မှာပါပြီးသားပါ။ အဲ့ဒီအပြင် NIC မှာ Connection အမျိုးမျိုးရှိပါတယ်။ အင်း ပြောရမယ်ဆိုရင်တော့ Thicknet ကလွဲလို့ NIC တွေဟာကွန်ရက်နဲ့ တိုက်ရိုက်ချိတ်ဆက်ရတာတွေပါ။ Ethernet NIC ဆိုရင် အောက်ပါ Connector များကို Support လုပ်ပါတယ်။ အဲ့ဒီလို Support လုပ်ရာမှာ NIC တစ်ကဒ်ထဲမှာ တစ်ခုဖြစ်စေ၊ နှစ်ခုဖြစ်စေ၊ အားလုံးဖြစ်စေ Support လုပ်ပါတယ်။ သူတို့တွေကတော့-

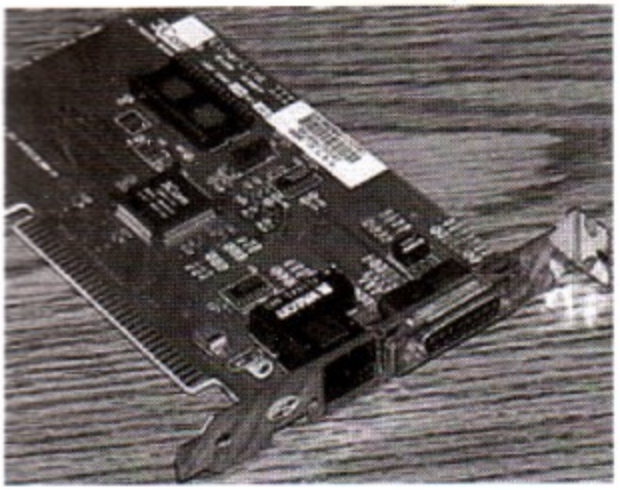
❖ UTP Ethernet အတွက် RJ-45 Connector

❖ Thin Ethernet အတွက် BNC Connector

- Thick Ethernet အတွက် AUI Connector တို့ပဲဖြစ်ပါတယ်။

Token Ring NIC တွေကတော့ အောက်ပါ တစ်ခု (သို့မဟုတ်) နှစ်ခုစလုံးကို Support လုပ်ပါတယ်။

- STP အတွက် DB=15 Connector
- UTP အတွက် RJ-45 Connector တို့ပဲဖြစ်ကြပါတယ်။



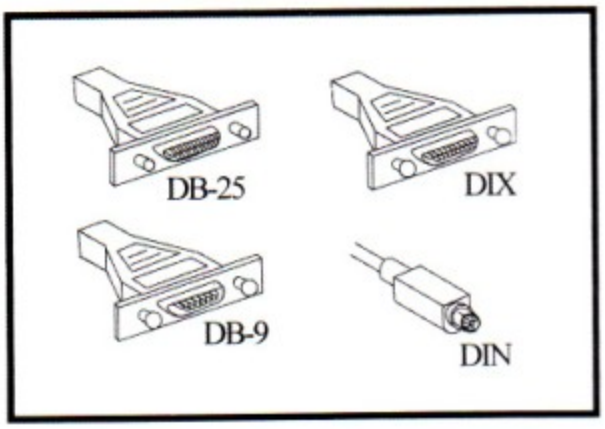
RJ-45 နှင့် AUI ပါဝင်သော
PCI Network Card ကိုတွေ့ရစဉ်

Connectors for Multi-Wire Cable များအကြောင်းသိကောင်းစရာ

ယေဘုယျအားဖြင့် Modem ကိုချိတ်ဆက်တဲ့နေရာမှာသုံးတဲ့ RS232 Serial Cable ဝါယာကြိုး (၂၅) ကြိုးတောင် ပါပါတယ်။ ဒါပေမယ့်လည်း အားလုံးအလုပ်လုပ်တယ်ဆိုတာရှားပါတယ်။ D-Type ဆိုတဲ့ Connector တွေအများကြီးရှိတဲ့အထဲက တချို့ကိုပဲမှာပြထားပါတယ်။ ဥပမာ DB-25 တို့ DB-9 တို့ စသည်ဖြင့်ပေါ့။ အဲ့ဒီမှာပါတဲ့ နံပါတ် ၂၅ တို့ ၉ တို့ဆိုတာက Pin ဒါမှမဟုတ် Spoken အရေအတွက်ကိုပြောတာပါ။ တော်တော်များများနေရာတွေမှာ DB-9 Connector ကိုသင်တို့တွေ့ဖူးကြပါလိမ့်မယ်။ DB9 ကိုများသောအားဖြင့် Token Ring Network Card တွေတပ်ဆင်အသုံးပြုကြပါတယ်။

DIX Connector ကတော့ DB-15 Connector လိုပါပဲ။ သူကတော့ Thick Ethernet တွေမှာချိတ်ဆက်အသုံးပြုပါတယ်။ ဒါပေမယ့် DIX က Standard DB-15 နဲ့ကွာခြားတာက Connector ကိုသွားတပ်တဲ့နေရာမှာ ပြန်ပြုတ်မထွက်အောင် ကြပ်ပေးတဲ့ Screw အစား DIX က Clip လေးနဲ့လာတာဖြစ်ပါတယ်။ DIN Connector ကတော့ Pin အရေအတွက်နဲ့ Pin အနေအထားပေါ်မူတည်ပြီး အမျိုးမျိုးအသုံးပြုကြတာရှိပါတယ်။ Networking နဲ့ပတ်သက်တဲ့နေရာမှာဆိုရင်တော့ Macintosh တွေရဲ့ Apple Talk Networks တွေမှာ DIN Connector တွေကိုအသုံးပြုကြပါတယ်။ Multi-Wire Cable တွေနဲ့ပတ်သက်လို့ကတော့ ဒီလောက်ပါပဲ။

ပုံ ၄-၉



၄.၁၀ Connectors for Coaxial Cable များအကြောင်းသိကောင်းစရာ

Coaxial Cable မှာဆိုရင်တော့ဖြင့် ယေဘုယျအားဖြင့် Connectors နှစ်ခုအသုံးပြုပါတယ်။ သူတို့ကတော့ BNC Connector နဲ့ N-Connector တို့ပဲဖြစ်ပါတယ်။ ပထမဦးစွာ BNC Connector အကြောင်းကို ပြောပြပါမယ်။ BNC ဆိုတာ BayoNet Connector ပါ။ တချို့နေရာတွေမှာ Bayonet Coaxial လို့လည်း တွေ့ဖူးပါတယ်။ ချိတ်ဆက်အသုံးပြုပုံကို ပုံမှာပြထားပါတယ်။ အောက်ကအချက်အလက်တွေနဲ့ တွဲကြည့်ပါ။ PC ထဲက Network Card ဟာ Network ကိုဆက်သွယ်ဖို့အတွက် T-Connector ကိုအားပြုပါတယ်။ ဆိုလိုချင်တာက T-Connector ကို Network Card မှာတပ်ပါ။ ပြန်ပြောပါအုံးမယ်။ Network Card ရဲ့ ခေါင်းမှာ ကြိုးကိုဘယ်တော့မှ တိုက်ရိုက်မတပ်ရဘူးနော်။ T-Connector ကိုသာလျှင် Network Card ရဲ့ ခေါင်းမှာ တိုက်ရိုက်လာတပ်ရမှာဖြစ်ပါတယ်။

BNC Connector တွေဟာ ကြိုး Segment တစ်ခုရဲ့တစ်ဖက်တစ်ချက်စီမှာရှိနေမယ်။ ၎င်းတို့ကို T-Connector မှာလာတပ်ရတာဖြစ်ပါတယ်။

Cable တွေရဲ့အဆုံးနှစ်ဖက်မှာ Terminator ပိတ်ပေးထားရပါတယ်။ Terminator ဆိုတာ Cable ကြိုးရဲ့သရုပ်သဏ္ဌာန်နဲ့ ကိုက်ညီတဲ့ Resistor ပါဝင်သော အထူးပြုလုပ်ထားတဲ့ Connector ပဲဖြစ်ပါတယ်။

Terminator နှစ်ခုအနက် တစ်ခုကို Ground ချရပါမယ်။ Ground ချတယ်ဆိုတာ Wire တစ်ခုကို Connector မှာ Attach လုပ်ထားပြီး ကျန်တစ်ဖက်ကို လျှစ်စစ်ပလပ်ပေါက်တစ်ခုရဲ့ Ground Point မှာ ချည်ပေးထားရမှာဖြစ်ပါတယ်။ ကဲ N-Connector အကြောင်းလေ့လာကြည့်ရအောင်။ N-Connector ကို Thick Ethernet မှာအသုံးပြုပါတယ်။ သူကတော့ BNC လို Twist Lock မဟုတ်ပါဘူး။ Twist Lock ဆိုတာ ခေါင်းကိုတပ်ပြီးရင် လှည့်လိုက်ရတာပါ။ ဥပမာ မီးလုံးကို မီးခေါင်းမှာတပ်ရင် တပ်ပြီးလှည့်ရတယ် မဟုတ်လား။ Twist Lock ဆိုတာအဲ့ဒါကိုပြောတာ။ N-connector တွေက BNC လို Twist Lock မလုပ်ဘဲ ဝက်အူရစ်ရပါတယ်။ အဲ Thin Ethernet လိုပါပဲ။ အဆုံးနှစ်ဖက်မှာ Terminator ကိုတပ်ဆင်ပေးရပါတယ်။ ၎င်းတို့အနက်တစ်ခုကို Ground ချပေးရပါတယ်။ Workstation တွေဟာ Thick Ethernet

ကြိုးနဲ့ တိုက်ရိုက် မချိတ်ဆက်ရပါဘူး။ ဒီ Thicknet ကြိုးတွေဟာ MAU (Medium Attachment Unit) လို့ခေါ်တဲ့ Transceiver နဲ့ချိတ်ဆက်တာပါ။ ၎င်း MAU မှတဆင့် Workstation တွေဆီကို AUI Cable နဲ့ တဆင့်ပြန်ချိတ်ဆက်ရပါတယ်။ သင်ခန်းစာ ၃ မှာလည်းပြထားပါတယ်။ Workstation တွေဟာ AUI Cable မှတဆင့် MAU ကိုချိတ်ဆက်ရပါမယ်။ MAU တွေကသာ Thicknet ကြိုးနဲ့ချိတ်ရမှာဖြစ်ပါတယ်။ Transceiver တွေဟာ Cbale ကိုချိတ်ဆက်တဲ့နေရာမှာလည်း နည်း နှစ်နည်းရှိပါတယ်။

ပထမနည်းကတော့ ရှေးနည်းပါ။ အခုတော့အသုံးနည်းသွားပါပြီ။ သူက သမာရိုးကျပဲ။ Thicknet ကြိုးကိုဖျက် N-Connector မှာချိတ်။ ပြီးရင် Thicknet Transceiver ရဲ့ T-Connector မှာတပ်ပေးလိုက်ရုံပါပဲ။ ဒီလိုနဲ့တစ်လုံးပြီးတစ်လုံးချိတ်ဆက်ရမှာဖြစ်ပါတယ်။

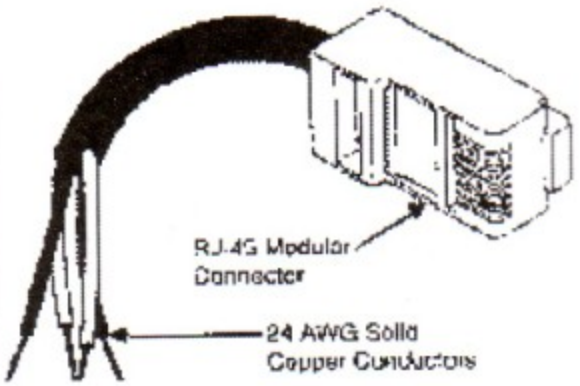
ဒုတိယနည်းကတော့ Clamp-on Transceiver ကိုအသုံးပြုပါတယ်။ သူ့မှာ Pin တွေပါရှိပါတယ်။ သူဟာတောက်လျောက်သွားနေတဲ့ Thicknet ကြိုးကိုလိုက်ဖျက်စရာမလိုဘဲ သူ့ Pin တွေနဲ့ Penetrate ထိုးဖောက်လိုက်တာပါ။ ဒီတော့ Clamp-on Transceiver ရဲ့ချွန်ထက်တဲ့သွားတွေဟာ Cable ထဲကိုထိုးဖောက်ဝင်ရောက်ပြီး Connector ရသွားပါတယ်။ ဒါကို Vampire Taps လို့လည်းခေါ်ပါတယ်။ သွားတွေလို Pin တွေက ကြိုးတွေကိုထိုးဖောက်နစ်ဝင်သွားလို့ပါ။ သင်ခန်းစာ ၃ တွင် ပုံများဖော်ပြပြီးဖြစ်ပါတယ်။

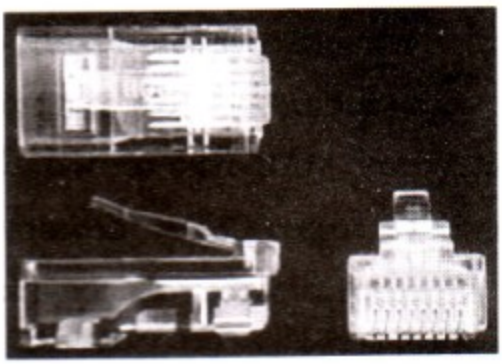
၄.၁၁ Connectors for Twisted Cable များအကြောင်းသိကောင်းစရာ

UTP Cabel တွေမှာ အများဆုံးအသုံးပြုဖြစ်တဲ့ Cable ကတော့ RJ-45 Connector ပါပဲ။ ပုံမှာလည်းပြထားပါတယ်။ ဒီ Connector တွေဟာ တခြား Connector တွေနဲ့ယှဉ်ရင် Cabel တပ်ဆင်တဲ့နေရာမှာလွယ်ကူတဲ့အပြင် Network Card မှာသွားတပ်တာ ပြန်ဖြုတ်တာဟာလည်း အင်မတန်လွယ်ကူပါတယ်။ တပ်မယ်ဆိုရင်လည်း Network Card ရဲ့အပေါက်မှာထိုးထည့်လိုက်ရုံပဲ။ ကလစ်ဆိုတဲ့အသံလေးမြည်တောင်သွားသေးတယ်။ ပြန်ထုတ်ရင်လည်း ခေါင်းမာပေါ်ကအတံလေးကိုဖိပြီးဆွဲထုတ်လိုက်ရုံပဲ။ လှည့်စရာ၊ ချွတ်စရာမလိုပါဘူး။ RJ-45 မှာ pin 8 pin ရှိတယ်။ တခါတရံသင်ဟာ RJ-11 Connector တွေကိုလည်းတွေ့ရတတ်ပါတယ်။ ဒါပေမယ့် သူကတော့ 4 pin ပဲပါပါတယ်။

STP Cable အတွက် Connector အကြောင်းကိုလည်းပြောပြပါအုံးမယ်။ STP ဆိုတာ IBM Token Ring တွေရဲ့တော်တော်များများမှာအသုံးပြုတာပါ။ IBM ကတော့ Connector ကိုပဲအသုံးပြုတာပါ။ IBM Data Connector ကတော့ အထူးအဆန်းပါပဲ။ ဘာဖြစ်လို့လဲဆိုတော့ ပုံမှန် Connector တွေဟာ တစ်ခုထဲမှာ အင်္ဂါနှစ်မျိုးနဲ့မလာပါဘူး။ ဥပမာ ဖို ဖြစ်ရင်ဖြစ်၊ မ ဖြစ်ရင်ဖြစ်ပေါ့။ IBM Connector တွေဟာ IBM Connector အချင်းချင်းချိတ်ဆက်ကြရပါတယ်။

ပုံ ၄.၁၀



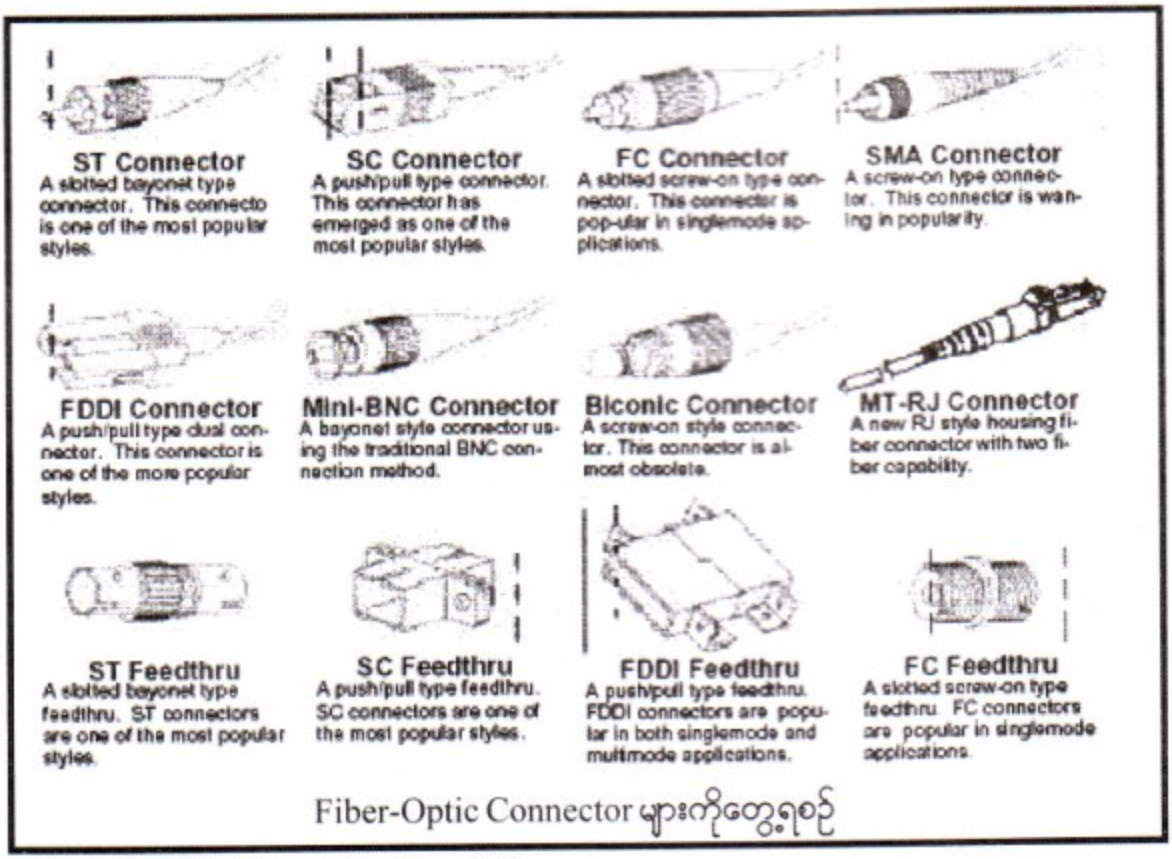


RJ-45 Connector များကိုတွေ့ရစဉ်

၄.၁၂ Connectors for Fiber Optic Cable ဓာတ်အင်းကြောင်းသိကောင်းစရာ

တကယ်တော့ Fiber Optic မှာသုံးတဲ့ Connector တွေအမျိုးမျိုးရှိကြပါတယ်။ အများဆုံးကတော့ ST-Connector ကိုအသုံးပြုကြပါတယ်။ FDDI နဲ့ SMA Connector များကိုလည်း တော်တော်များများအသုံးပြုကြပါတယ်။ ယနေ့ခေတ်မှာတော့ SMA ကအသုံးများဆုံးလို့ ပြောလို့ရပါတယ်။ SMA ရဲ့ တကယ့် Technical Name က FSMA ပါ။ Field-Installable Sub Miniature Assembly ဖြစ်ပါတယ်။

ပုံ ၄.၁၁



Fiber-Optic Connector များကိုတွေ့ရစဉ်

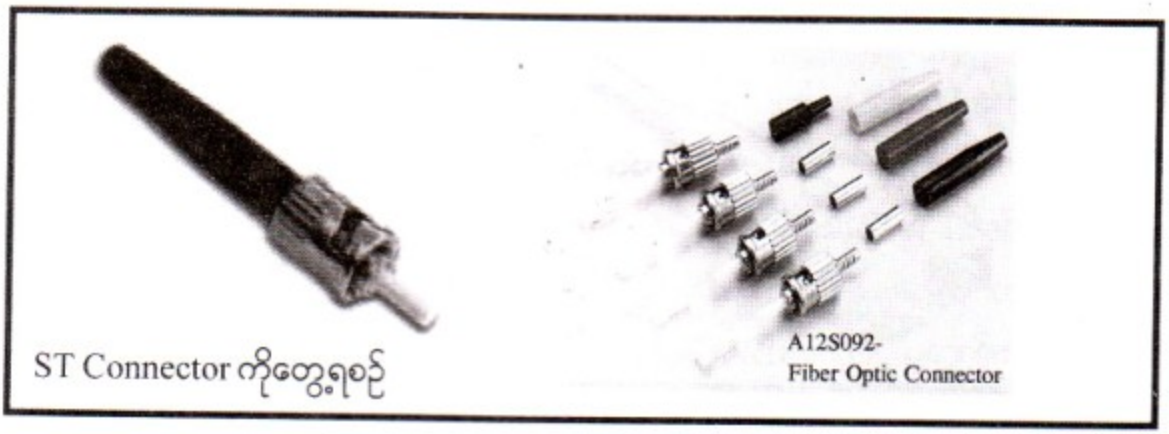
FDDI ဆိုတာ Fiber Distrubuted Data Interface ဖြစ်ပါတယ်။ FDDI ဟာ Fiber Optic Cable အတွက်ဆိုပေမယ့် သူက Ring Topology မှာအသုံးပြုပါတယ်။ သူဟာ ၆၂ မိုင် (ကီလိုမီတာ ၁၀၀) အထိလောက်တော့ 100 Mbps Bandwidth နဲ့ Data တွေကိုပို့လွှတ်နိုင်ပါတယ်။

နောက်ထပ် ထပ်ပြီးတော့ပြောပြချင်တဲ့ Fiber-Optic Connector တွေကတော့ - ဒီလိုဗျ။ ကိုယ် အသုံးပြုတဲ့ Fiber-Opitc ရဲ့အလင်းထုတ်လွှတ်မှု၊ အလင်းကို Detect လုပ်မှု၊ အလင်းရဲ့သွားလာမှု စတဲ့အချက် တွေပေါ်မှာမူတည်ပြီး အသုံးပြုတဲ့ Connector တွေကွဲပြားသွားပါတယ်။ ပုံ ၄.၁၀ ကိုကြည့်ပါ။

ST (Straight Tip)

Fiber-Optic Cable ကို Ethernet ကွန်ရက်တွေမှာ Backbone အဖြစ်အသုံးပြုတဲ့အခါတွေမှာ ဒီ ST Connector တွေကိုအသုံးပြုကြပါတယ်။ ဒီ ST Connector က BNC Connectors လိုပဲ တပ်ပြီးလို့ရှိ ရင်လှည့်လိုက်ရတယ်။ ST Connector တွေဟာပစ္စည်းတွေမှာတိုက်ရိုက်သွားတပ်တဲ့ Fiber တွေမှာသွားတပ် ရင်လည်းရပါတယ်။

ပုံ ၄.၁၂

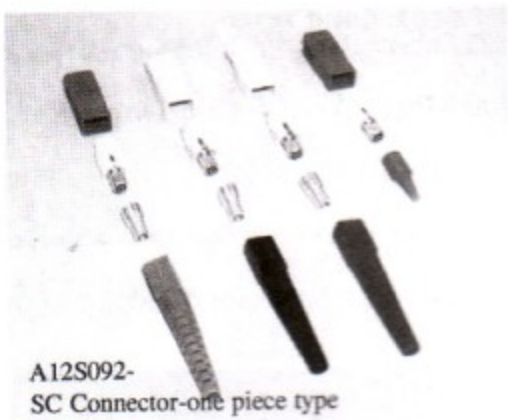


ST Connector ကိုတွေ့ရစဉ်

SC (Straight Connection)

SC Connectors ကဖိပြီးတပ်ရမှာ - တပ်ဆင်ရာမှာ အနည်းငယ်လည်းလွယ်ကူသလို ဖိပြီတပ်ရ တာကြောင့် တပ်ဆင်တဲ့နေရာလည်းအနည်းငယ်ပဲလိုအပ်ပါတယ်။ SC Connectors တွေကို Fiber Optic Cable တွေအချင်းချင်း ချိတ်ဆက်ရာမှာအသုံးပြုမယ်ဆိုပြီးနိုင်ပါတယ်။ SC Connectors တွေဟာ ဒီတစ်ခုထဲမှာ ပဲ Fiber Optic ကို Sending လုပ်နိုင်အောင်ရော၊ Receiving လုပ်နိုင်အောင်ရော လက်ခံပါရှိပါတယ်။ အဲကြောင့် တပ်ဆင်တဲ့အခါ ပြောင်းပြန်မတပ်မိဖို့ ဂရုစိုက်ရပါမယ်။

ပုံ ၄.၁၃

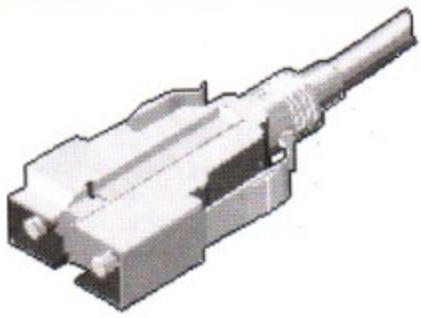


SC Connector ကိုတွေ့ရစဉ်

MIC (Medium Interface Connector)

MIC Connector တွေက FDDI လို့ခေါ်တဲ့ Fiber Distributed Data Interface မှာအသုံးပြုပါတယ်။ MIC Connector ဟာ SC Connector လို အဝင်ရောအထွက်ပါ လက်ခံပေါက်ပါရှိပါတယ်။

ပုံ ၄.၁၄

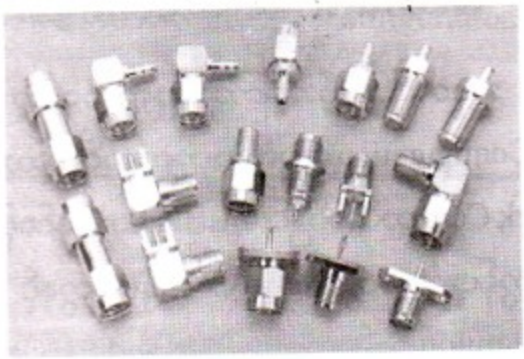


MIC Connector ကို
တွေ့ရစဉ်

SMA (Subminiature Type A)

Amphenol ကုမ္ပဏီက SMA Connector ကို Microwave မှာအသုံးပြုဖို့ ဒီဇိုင်းဆွဲခဲ့ပေမယ့် နောက်ပိုင်းမှာ Fiber Optic မှာအသုံးပြုဖို့ ပြုပြင်ပြောင်းလဲခဲ့ပါတယ်။ SMA မှာ Versions နှစ်မျိုးရှိပါတယ်။ 905 နှင့် 906 ဆိုတာပါ။ 905 က Straight Ferrule လို့ခေါ်ပြီး 906 ကတော့ Stepped Ferrule ဖြစ်ပါတယ်။ SMA က ST Connectors လိုဖြစ်ပါတယ်။ Fiber တစ်ခုချင်းစီအတွက် သီးသန့် Connectors နှစ်ခုလိုအပ်ပါတယ်။

ပုံ ၄.၁၅



SMA Connector ကိုတွေ့ရစဉ်

၄.၁၃ Networking အတွက် အခြားသော Interface များ

အခုပြောပြမယ့် Interface တွေကတော့ အထက်ကပြောခဲ့တဲ့ PC တွေရဲ့ Bus တွေကိုအစားထိုးဝင်ရောက်ဖို့မဟုတ်ဘဲ ကွန်ပျူတာတွေဟာ ကွန်ရက်တွေကို အခြားသောနည်းလမ်းနှင့် ချိတ်ဆက်ဖို့အတွက်ပဲ ဖြစ်ပါတယ်။ အဲ့ဒါတွေကတော့ USB ဆိုတဲ့ Universal Servial Bus နှင့် Firewire လို့လူသိများကြတဲ့ IEEE 1394 တို့ပဲဖြစ်ကြပါတယ်။

USB ကတော့ Fire Wire နှင့် ယှဉ်ပြောရရင် သူက Low-Speed Serial Interface ပေါ့။ သူ့ရဲ့ အမြင့်ဆုံး Bandwidth က 12Mbps ပဲရှိပါတယ်။ သူ့ကိုအဓိကအားဖြင့်တော့ Low Speed အရံပစ္စည်းတွေ ဖြစ်ကြတဲ့ Mouse, Keyboard, Joysticks စတာတွေမှာသုံးခဲ့ပေမယ့် အခုဆိုရင် Printer တွေ၊ Scanners တွေ၊ တယ်လီဖုန်းတွေ၊ အချို့သော Video ပစ္စည်းတွေပါကွန်ပျူတာမှာသုံးလာကြပါတယ်။ USB ဟာ PCs ရော၊ Macintosh မှာပါရေရေလည်လည်အသုံးများလာပေမယ့် Networking အတွက်ကတော့အသုံးပြုမှုဟာ နည်းပါးလွန်းပါသေးတယ်။

Firewire ကို IEEE 1394 လို့လည်းခေါ်ကြပါတယ်။ Firewire ကတော့ High Speed Serial Bus ဖြစ်ပါတယ်။ အဲ့ဒီ Firewire က Apple Computer နှင့် Texas Instrument တို့ပူးပေါင်းထုတ်လုပ်ခဲ့တာ ဖြစ်ပါတယ်။ ၎င်းဟာ Bandwidth ကို 400 Mbps အထိရရှိပါတယ်။ IEEE အဖွဲ့ရဲ့ ဦးဆောင်မှုနှင့် ထွက်ရှိလာမယ့် 1394b ဆိုရင် Bandwidth က 3200 Mbps အထိရရှိပါတယ်။ Firewire ကို High Bandwidth လိုအပ်တဲ့ Multimedia Application နှင့် Video ပိုင်းဆိုင်ရာတွေမှာ အသုံးပြုပါတယ်။ ၎င်း Firewire ကို Networking ပိုင်းမှာလည်းအသုံးပြုပါတယ်။ Digital Camera နှင့် Video ပစ္စည်းတွေကို ကွန်ပျူတာမှာတပ်တဲ့အခါမှာလည်းအသုံးပြုပါတယ်။

၄.၁၄ Network Card Configuration လုပ်ခြင်းနှင့်ပတ်သက်၍

အခုတင်ပြမယ့်အကြောင်းအရာကတော့ Network Card ကိုကွန်ပျူတာမှာတပ်ဆင်ပြီးသကာလ ၎င်းကို Configuration လုပ်ရာမှာ အကျိုးဝင်မယ့်သင်ခန်းစာတွေဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင် ဒီအကြောင်းက Network Card တပ်ဆင်ခြင်း Installation သင်ခန်းစာရဲ့တစ်ပိုင်းတစ်စပဲဖြစ်ပါတယ်။ ဒီနေ့ခေတ်မှာ အသုံးပြုနေတဲ့ ကွန်ပျူတာတွေတွေ့ Network Card တွေနှင့် Operating System တွေကြောင့် Network Card ကို Configuration လုပ်တာဟာ Plug and Play နှင့်သွားမှာဖြစ်ပါတယ်။ ဒီတော့ Plug and Play ဆိုတာ သိတဲ့အတိုင်း Card စိုက်ပြီး Windows တက်လာရင် Driver တန်းတင်ရုံဖြစ်ပါတယ်။ ဒီတော့ ပြောရရင် Manual Configuration မဟုတ်ဘူးလေ။ Auto Configuration ပါ။ ဒီတော့ Windows 95/98 နောက်ပြီး Windows 2000, Windows XP စသဖြင့်ပေါ့ဗျာ။ ဒီ Operating System မဟုတ်တဲ့ကွန်ပျူတာတွေ၊ Plug and Play မလုပ်တော့တဲ့ ကွန်ပျူတာတွေမှာ Network Card စိုက်ရင် Auto Configuration မဟုတ်ဘဲ Manual Configuration ဖြစ်တာကြောင့် အခုရှင်းပြမယ့်သင်ခန်းစာတွေကိုကောင်းစွာနားလည်ထားရမှာဖြစ်ပါတယ်။ ဒါပေသိ အခုခေတ်မှာက Plug and Play ကြောင့် အားလုံး Auto ဖြစ်နေသည့်တိုင် ဒီသင်ခန်းစာတွေကို Network သမားတစ်ယောက်အနေနဲ့သိထားသင့်ပါတယ်။

ကဲ Network Card ကို Configuration လုပ်ရာမှာသိထားသင့်တဲ့အချက်(၃)ချက်ကတော့ -

(၁) Interrupt Request (IRQ)

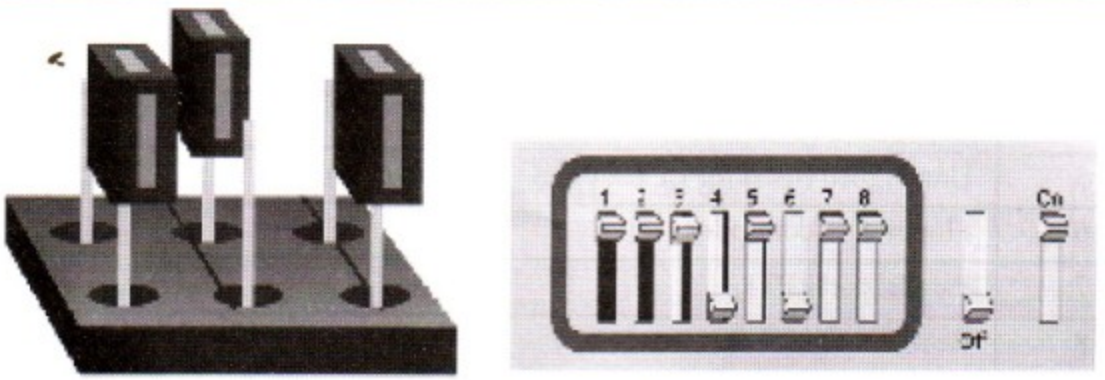
(၂) Base I/O Port

(၃) Base Memory Address

ဒီနေရာမှာသိရမှာက အချို့သော Network Card တွေဟာ Configuration လုပ်ရာမှာ Software နှင့်လုပ်ရပေမယ့် အချို့သော Network Card ကတော့ ၎င်းပေါ်မှာပါရှိတဲ့ Jumpers တွေ DIP Switch တွေနဲ့ Manually Configuration လုပ်ပေးမှရပါမယ်။ အခု Software နှင့် Configured လုပ်မယ့် Network Card ရဲ့သတိထားစရာအချက်ကိုပြောပြပါတော့မယ်။ အဲ့ဒါက Network Card ကိုတပ်ထားမယ်။ ပြီးတော့ ကွန်ပျူတာကိုဖွင့်လိုက်မယ်။ ဒီအချိန်မှာ Network Card ရဲ့ပတ်သက်ရာပတ်သက်ကြောင်း တွေဟာ အခြား Adapters တွေနှင့်သွားပြီး Conflicts ဖြစ်နိုင်ပါသေးတယ်။ ဖြစ်ခဲ့မယ်ဆိုရင် ကျွန်တော်တို့က အခြား Adapter ရဲ့ပတ်သက်ရာပတ်သက်ကြောင်းတွေကိုရွှေ့ပေးရမှာဖြစ်ပါတယ်။ Hardware နဲ့ပဲ Configured လုပ်မယ့် Network Card ကြတော့ Configuration ကိုနည်းလမ်း ၂ လမ်းနှင့်ပြုလုပ်နိုင်ပါတယ်။ အဲ့ဒါက Jumper နှင့်လုပ်တဲ့ Card လည်းရှိမယ်။ DIP (Dual Inline Package) Switch များနှင့်လည်း ပြုလုပ်လို့ရပါတယ်။ ဒီလို Hardware နှင့် Configured လုပ်တာကြတော့ အဆင်မပြေရင် ကွန်ပျူတာ ပြန်ပိတ်ပြီး

တစ်ခါ Setting ပြန်ပြောင်း တစ်ခါစက်ပြန်ဖွင့်၊ ဒီလိုလုပ်ရပါတယ်။ Software Configuration ကတော့ Hardware လောက်တော့ သိပ်ဒုက္ခမရောက်ပါဘူး။

ပုံ ၄.၁၆



Jumpers နှင့် DIP Switches များကိုတွေ့ရစဉ်

၄.၁၅ IRQ ကိုသတ်မှတ်ခြင်း

ကနဦး IRQ အကြောင်းကိုအရင်ရှင်းပြပါအုံးမယ်။ ကွန်ပျူတာတွေမှာက များသောအားဖြင့် CPU ကတစ်ခုတည်းရှိပေမယ့် Adapters (Expension Card) တွေကြတော့ တစ်ခုမကအများကြီးရှိနိုင်ပါတယ်။ ဒါတွေကို ရွတ်ပြရမယ်ဆိုရင်တော့ ဟုတ်လား။ Server ပဲဖြစ်ဖြစ် ရိုးရိုး Desktop Computer ပဲဖြစ်ဖြစ် Disk Controller တစ်ခု ဒါမှမဟုတ် တစ်ခုမကရှိနိုင်မယ်။ Floppy Controller ရှိမယ်။ Graphic Card ရှိမယ်။ တစ်ခု ဒါမှမဟုတ် တစ်ခုထက်ပိုတဲ့ Serial Controllers တွေရှိမယ်။ တစ်ခု ဒါမှမဟုတ် တစ်ခုထက်ပိုနိုင်တဲ့ Network Card တွေရှိမယ်။ Sound Card တွေရှိနိုင်မယ်။ အဲ့ဒီအပြင် အခြား Adapter တွေလည်းရှိနိုင်မယ်။ ဒီတော့ CPU ကတစ်ခုတည်း CPU က ဂရုပြု ဂရုစိုက်ရမယ့် Adapter တွေကအများကြီး ဒီတော့ Adapter တစ်ခုချင်းစီက CPU ကို Request လုပ်တဲ့အခါ Adapter တွေ တစ်ခုနှင့်တစ်ခုကို ရာထူးအကြီးအငယ် ခွဲထားလိုက်တယ်။ လုမပြောနဲ့။ အဆင့်ခွဲထားမယ်။ ဒါမျိုးပါ။ ဒါကို Interrupt Request လို့ခေါ်ပါတယ်။ CPU ကိုဂရုပြုဖို့ တောင်းဆိုတာကိုခေါ်တာပါ။ ဒီတော့ PC တွေမှာ Adapters တွေ Peripherals တွေက သူတို့ CPU ရဲ့ ဂရုပြုမှု၊ ဝန်ဆောင်မှုတွေကို လိုအပ်လာတဲ့အခါမှာ CPU ဆီကို Signal ပို့ပြီး Interrupt လုပ်ဖို့သတ်မှတ်ထားတဲ့ Lines တွေကို Interrupt Request Lines လို့ခေါ်ပါတယ်။ IRQ တွေဟာ ဂဏန်း (နံပါတ်) နှင့် သတ်မှတ်ထားတာဖြစ်ပါတယ်။ ကွန်ပျူတာတိုင်းမှာရှိတဲ့ Peripheral တိုင်းမှာ CPU ဆီကို Signal ပို့ဖို့ကိုယ်ပိုင် IRQ Line တွေရှိကြပါတယ်။ IRQ နံပါတ်တွေဟာ Peripheral ကနေ CPU ဆီကို Signal ပို့လွှတ်မယ့် Line ရဲ့ Address နှင့်ဆက်နွယ်ပါတယ်။

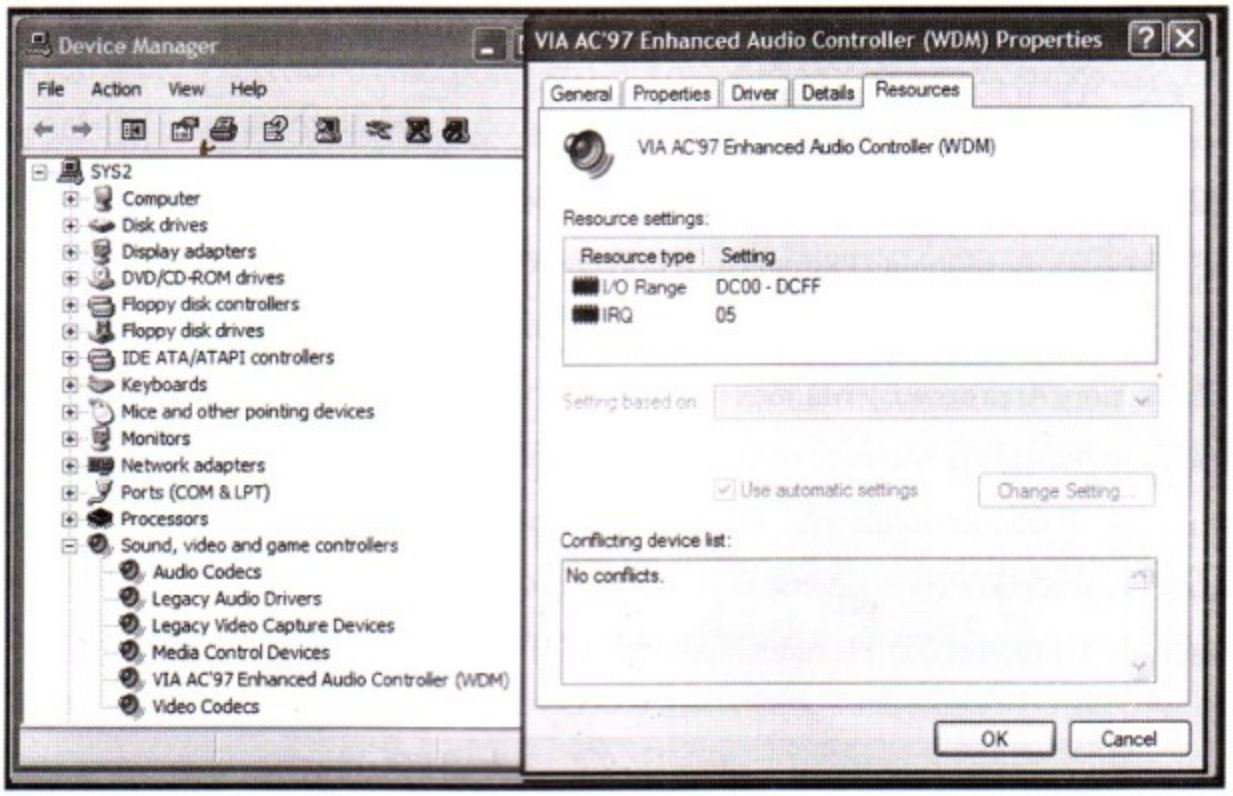
IRQ တိုက်တာကို အင်္ဂလိပ်လို IRQ Conflicts ဖြစ်တယ်လို့ခေါ်ပါတယ်။ ကိုယ်တပ်လိုက်တဲ့ Adapter တစ်ခုဟာ တခြားသော Adapter တစ်ခုရဲ့ IRQ နှင့် သွားပြီးတိုက်နေတာကိုပြောတာပါ။

IRQ	Typical Assigment
0	PC system timer
1	Keyboard
2	Cascading IRQ controller or video adapter
3	Unassigned (used for COM2/COM4 or bus mouse)
4	COM1/COM3
5	Unassigned (used for LPT2, often for sound card)
6	Floppy disk controller
7	Parallel port LPT1
8	Real-time clock
9	Cascading IRQ controller, sometimes sound card
10	Unassigned (used for primary SCSI controller)
11	Unassigned (used for secondary SCSI controller)
12	PS/2 mouse (if none present, unassigned)
13	Math co-processor (if none present, unassigned)
14	Primary hard drive controller, usually IDE (if no IDE drives, unassigned)
15	Secondary hard drive controller, usually IDE (if absent, unassigned)

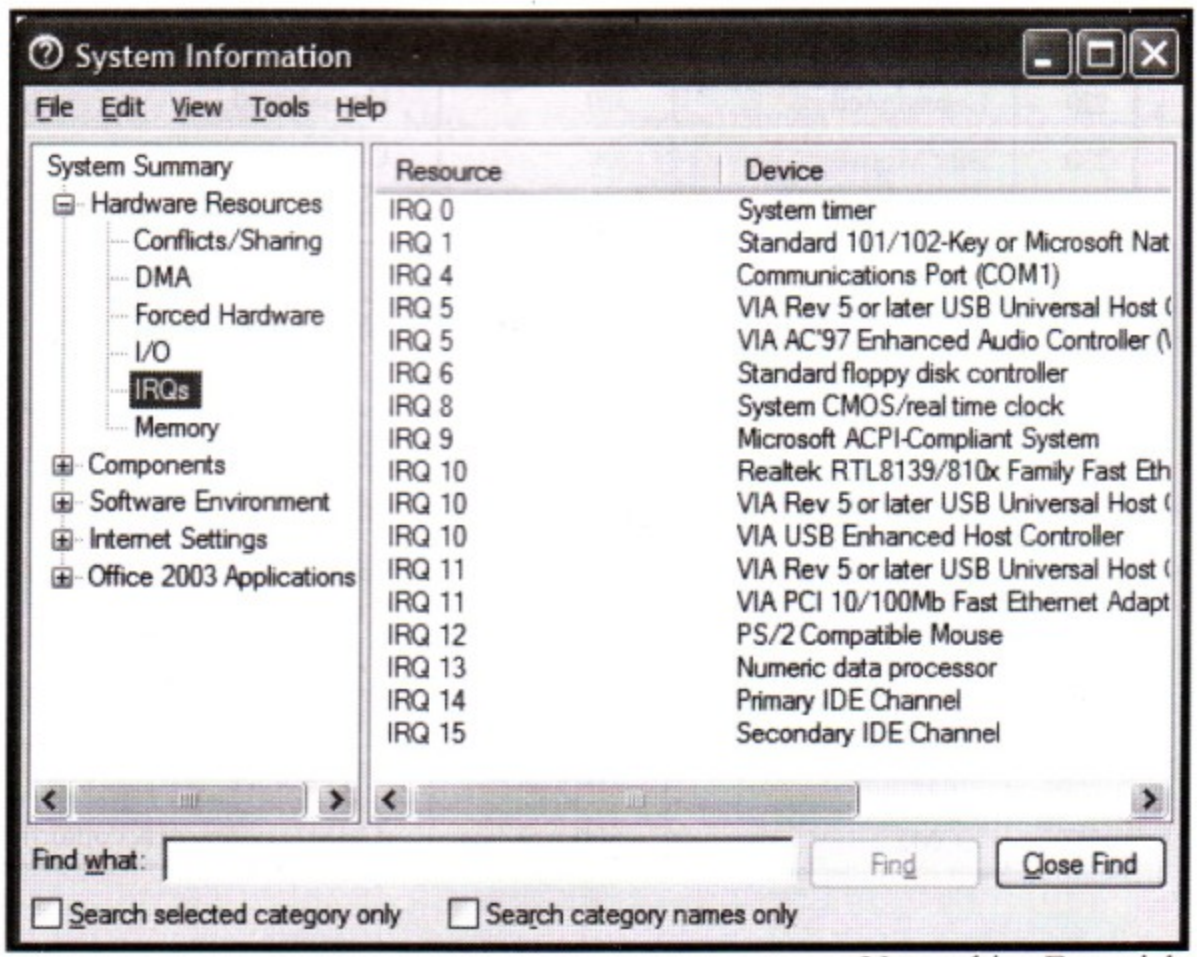
အဲဒီလိုဖြစ်ခဲ့မယ်ဆိုရင်တော့ ဒီ IRQ Conflicts ဖြစ်နေတဲ့ ပစ္စည်းနှစ်ခုစလုံး သို့မဟုတ် တစ်ခုခုဟာ အလုပ်မလုပ်တော့ပါဘူး။ အဲဒီအခါ ကျွန်တော်တို့ဟာ Adapter တစ်ခုရဲ့ IRQ ကိုရွှေ့ပေးရမှာဖြစ်ပါတယ်။ Software နှင့် Configuned လုပ်ရမယ့် Network Card ဆိုရင် Device Manager မှာ ၎င်း IRQ ကို ရွှေ့ပေးနိုင်ပါတယ်။ အဲဒီနေရာမှာ IRQ အပြင် DMA, I/O နှင့် Memory Resources တို့ကိုလည်း တွေ့မြင်နိုင်ပါတယ်။ ပုံ ၄.၁၇ ကိုကြည့်ပါ။ Hardware ကိုအားပြုပြီး Configured လုပ်ရတဲ့ Network Card လိုမျိုးကြတော့ အခုလို Conflicts ဖြစ်ပြီဆိုကွန်ပျူတာကို တစ်ခါပြန်ပိတ်၊ စက်ဖုံးဖွင့် Network Card မှာတစ်ခါ Jumper ပြန်ပြောင်း ပြီးရင် Card ပြန်စိုက် စက်ဖုံးပိတ်၊ စက်ဖုံးကိုပြန်ဖွင့် Conflicts ဖြစ်သေးလားကြည့် စသည်ဖြင့်ပေါ့။ ဒီတော့ Hardware နှင့် Configured လုပ်တဲ့ Network Card တွေကိုအသုံးပြုသူဟာ Network Card ကို ကွန်ပျူတာမှာ မစိုက်ခင်မှာ IRQ ဇယားကိုကြည့်ပေါ့။ Windows 95 မတိုင်ခင် (ဥပမာ စက်ရုံသုံးကွန်ပျူတာတွေ၊ အမြင့်ကြီး မလိုတဲ့ကွန်ပျူတာတွေ၊ ယနေ့ထိ Windows 95 မတိုင်ခင် သုံးနေတဲ့သူတွေ၊ အသုံးပြုတဲ့သူတွေဆိုရင် ဒီ Hardware နှင့် Configured လုပ်တဲ့ Network Card ကိုသုံးတဲ့သူဟာ DOS ထဲက Diagnostic Software ဖြစ်တဲ့ MSD-EXE (Microsoft Diagnostic Software) ကို Run ပြီး IRQ အလွတ်ကိုအရင်ကြည့်ပါ။ ပြီးတော့ IRQ လွတ်တဲ့နေရာကို ၎င်း Network Card IRQ အဖြစ် သတ်မှတ်ပြီးမှ ကွန်ပျူတာမှာတပ်ပါ။ ဒီဆို ပြဿနာမရှိတော့ဘူးပေါ့။ Start Menu, Run အောက်ကနေ

Winmsd လို့ရိုက်လိုက်ရင်လည်းရတယ်။ ပုံ ၄.၁၈ ကိုကြည့်ပါ။

ပုံ ၄.၁၇



ပုံ ၄.၁၈



၄.၁၆ Base I/O Ports အကြောင်း

CPU ဟာပစ္စည်းတစ်ခုခုဆီကနေ Interrupt ကိုလက်ခံရရှိပြီးတဲ့အခါ ကဲ့ CPU ကတော့ အဲ့ဒီပစ္စည်းကသူ့ကိုအလိုရှိနေပြီဆိုတာ သိလိုက်ရပြီ။ ဒီတော့ CPU က အဲ့ဒီပစ္စည်းကို ကဲ့ ကောင်းပြီ။ မင်းကို ငါအာလုပ်ပေးရမလဲလို့မေးတော့ သက်ဆိုင်ရာပစ္စည်းက CPU ကို သူဘာတွေလိုချင်သလဲဆိုတာ ပြောပြပါတော့တယ်။ ပြီးတဲ့အခါ CPU က အဲ့ဒီပစ္စည်းကို သူတောင်းဆိုတာတွေပြန်လည်ပြီးတော့ Data တွေပေးပို့ပါတယ်။ ပစ္စည်းတစ်ခုရဲ့ Base Input / Output (I/O) Port ဟာ CPU နှင့် IRQ တောင်းခံတဲ့ပစ္စည်းတို့ Message တွေအပြန်ပြန်အလှန်လှန် သယ်ယူထားရှိဖို့အတွက် လိုအပ်တဲ့ Memory Area ကိုသတ်မှတ်ပေးပါတယ်။ အဲ့ဒီ Memory Area လေးဟာ Mailbox သဖွယ်အလုပ်လုပ်ပါတယ်။ ဆိုလိုတာက CPU ကလည်း သက်ဆိုင်ရာပစ္စည်းကိုပေးချင်တဲ့ Message ကိုဂင်းနေရာမှာထားခဲ့သလို ပစ္စည်းဘက်ကလည်း CPU ဆီကိုပို့ချင်တဲ့ Message ကိုအဲ့ဒီမှာထားခဲ့ပါတယ်။ အပြန်ပြန်အလှန်လှန်ပေါ့။ ဒီ I/O Port ဟာ IRQ လိုပါပဲ။ Unique ဖြစ်ရပို့မယ်။ ဆိုလိုတာက ပစ္စည်းတစ်ခုရဲ့ I/O Port နှင့် နောက်တစ်ခု I/O Port သွားတူနေလို့ တိုက်နေလို့ မရပါဘူး။ ဒီ I/O Port ဟာ Hexadecimal ဂဏန်း (၃) လုံးနှင့်သတ်မှတ်ထားပါတယ်။

Port	Device	Port	Device
200	Game Port	300	NIC
210	Unassigned	310	NIC
220	Unassigned	320	Unassigned
230	Bus Mouse	330	Unassigned
240	Unassigned	340	Unassigned
250	Unassigned	350	Unassigned
260	Unassigned	360	Unassigned
270	LPT3	370	LPT2
280	NIC	380	Unassigned
290	Unassigned	390	Unassigned
2A0	Unassigned	3A0	Unassigned
2B0	Unassigned	3B0	LPT1
2C0	Unassigned	3C0	EGA/VGA video
2D0	Unassigned	3D0	CGA video
2E0	Unassigned	3E0	Unassigned
2F0	COM2	3F0	COM1, floppy disk contorller

၄.၁၃ Base Memory Address အကြောင်း

သက်ဆိုင်ရာ IRQ တောင်းခံတဲ့ပစ္စည်းနှင့် CPU တွေဟာတကယ်တမ်း Data တွေအပြန်အလှန်ပို့ကြပြီဆိုရင်တော့ ပေးပို့တဲ့ Data Volume ဟာနည်းနည်းတော့များပါတယ်။ ဆိုလိုတာက သက်ဆိုင်ရာပစ္စည်းဟာ CPU ရဲ့ Attention ဂရုပြုမှုကိုလိုအပ်ပါတယ်ဆိုတဲ့အကြောင်းကိုသိစေရန် ပေးပို့တဲ့ Signal တို့၊ ဘာကိုအလိုရှိပါတယ်ဆိုတဲ့ ပေးပို့တဲ့ Message တွေထက် တကယ်ပေးပို့တဲ့ Data ရဲ့ ထုကိုင်းများတယ်လို့ပြောချင်တာပါ။ Network Card ဘက်ကပြောမယ်ဆိုရင် ဒီလို Data တွေအများကြီးကို Handle လုပ်ဖို့အတွက် တစ်နည်းအားဖြင့်ပြောရရင် Input နှင့် Output လုပ်ဖို့အတွက် Buffer ကမရှိမဖြစ်လိုအပ်တယ်ဗျ။ ဒါမှ များပြားလှတဲ့ Data တွေကို Packets လေးတွေလုပ်ပြီး Serial အဖြစ်တန်းစီရပါတယ်။ ရောက်လာတဲ့ Incoming Data တွေကိုလည်း Packets အဖြစ်မှပြန်ဖြေပြီး ဘာသာပြန်ကာ CPU ဆီကိုပို့ဖို့ Parallel ပြန်လုပ်ရပါတယ်။ ဒီအတွက် Buffer ဆိုတာလိုအပ်ပါတယ်။

ဒီတော့ Network Card ဟာ Outgoing Data တွေကို Network မှတဆင့် ပို့လွှတ်ဖို့ ဒါမှမဟုတ် ဝင်လာတဲ့ Incoming Data တွေကို သက်ဆိုင်ရာ Application ကိုပေးပို့ဖို့ အမှန်တကယ်မပို့မီ ယာယီသိုလှောင်စရာ Buffer ကို Memory ထဲမှာသတ်မှတ်ပါတော့တယ်။ ဒီ Network Card အတွက် Buffer Space ရဲ့ စတင်တဲ့ Address ဟာ Base Memory Address ပဲဖြစ်ပါတယ်။ Membase လို့လည်းခေါ်ပါတယ်။ Buffers တွေဟာပုံမှန်အားဖြင့်တော့ Upper Memory Area လို့ခေါ်တဲ့ 640 KB နှင့် 1 MB ကြားမှာပဲနေရာယူလေ့ရှိပါတယ်။ HMA (High Memory Area) လို့လည်းခေါ်ပါတယ်။ Hex အရပြောရရင် A0000 ကနေ FFFFF အထိဖြစ်ပါတယ်။ များသောအားဖြင့် Network Card တွေက D8000 မှာစတည်းချကြတာများပါတယ်။ အကယ်၍များ Network Card တွေအများကြီးစိုက်ထားရင်တော့တစ်မျိုးပေါ့။

မှတ်ချက် ။ ။ ဒီနေရာမှာ ပစ္စည်းတော်တော်များများဟာ Membase Address ကိုမလိုအပ်ကြပါဘူး။ ဒါပေမယ့် ဒီ Membase ဟာ Network Card အတွက်တော့အရေးကြီးပါတယ်။ Membase ဟာ IRQ, I/O Port တို့လိုပါပဲ။ Unique ဖြစ်ဖို့လိုအပ်ပါတယ်။ တခြား Adapter နှင့်သွားတူလို့မရပါဘူး။ ဒီတော့တပ်လိုက်တဲ့ Network Card ဟာ IRQ, I/O Port တို့ Conflicts မဖြစ်ဘဲ အလုပ်မလုပ်သေးဘူးဆိုရင် ဒီ Membase ကိုကြည့်ရတော့မှာဖြစ်ပါတယ်။ သတိထားစရာပြောရဦးမယ်။ Network Card ထုတ်လုပ်သူအချို့ဟာ ဒီ Membase Address မှာ 0 တစ်လုံးဖြုတ်ထားပါတယ်။ ဥပမာပြောရရင် D8000 ဆိုရင် D800 လို့ပဲပြမှာဖြစ်ပါတယ်။ အဲ့ဒါကိုကြည့်ပြီးသင်ရှုးကြောင်ကြောင်ဖြစ်မသွားပါနဲ့။ သင်သိထားရမှာ HMA က A0000 ကစတာဆိုတော့ D800 ဆိုတာမဖြစ်နိုင်ဘူး။ D8000 ပဲဖြစ်ပါတယ်။ 0 တစ်လုံးဖြုတ်ပြထားတယ်ဆိုတာသတိပြုပါ။

၄.၁၈ Network Card ကိုရွေးချယ်ခြင်း

Network Card ဟာ Network ရဲ့ Performance ကိုအတော်လေးလွှမ်းမိုးထားပါတယ်။ ဆိုလိုတာက Network Card ကနှေးနေရင် ကိုယ်က Network ကို Access လုပ်တဲ့အခါနှေးနေမှာဖြစ်ပါတယ်။ ဒီတော့ ဒီလိုနှေးနေတဲ့ Network Card တစ်ခုကို Network ရဲ့ဘယ်နေရာမှာပဲတပ်ထားတပ်ထား Network မှာရှိတဲ့ User အားလုံးကိုနှေးကွေးသွားစေပါတယ်။ ဒီလိုလေဗျာ။ ကားလမ်းမမှာ ကားတွေမပိတ်အောင် သက်မှတ်ပိုင်နှုန်းအတိုင်းမောင်းရတယ်ဆိုတာသိတယ်မဟုတ်လား။ ဒီလမ်းမှာတစ်နာရီမှိုင် ၄၀ နှင့်မောင်းရမယ်။ လျှောမမောင်းပါနဲ့။ လျှောမောင်းရင်နောက်ကကားတွေပိတ်ကုန်မယ်။ ဒီတော့နှေးတဲ့ကားတစ်စီးကအဲ့ဒီလမ်းပေါ် တက်မောင်းရင် ကျန်တဲ့ကားတွေပါခရီးဖင့်ကုန်တာပေါ့။ ဒီသဘောပါ။

ဒီတော့ Network Card ကိုရွေးချယ်တဲ့အခါမှာ တစ်ခုတော့ရှိတာပေါ့နော်။ ပထမဦးဆုံးကိုယ်အသုံးပြုမယ့် Network နည်းပညာနဲ့ Match ဖြစ်မယ့် Connector ပါတဲ့ Network Card ကိုရွေးချယ်ရမှာဖြစ်ပါတယ်။ ဒါအရေးကြီးဆုံးပေါ့။ အဲ့ဒီ Physical ပိုင်းဆိုင်ရာကို တူညီပြီဆိုတော့မှ ဒီ Card ရဲ့ Speed နောက်ပြီး Data ဘယ်လောက်ထိသယ်ယူပို့ဆောင်နိုင်သလဲ ဒါတွေကိုဆက်ကြည့်ရမယ်။ ကျွန်တော်တို့ကတော့ ဒီလို Network Card ကိုရွေးချယ်တဲ့အခါမှာ အကောင်းဆုံး Network Card ကို Server မှာဦးစားပေးတပ်တာပေါ့။ ငွေကြေးတတ်နိုင်ရင်တော့ ဒီ အကောင်းဆုံးရွေးချယ်ထားတဲ့ Network Card ကိုပဲ Server ရော Client မှာပါ အကုန်အတူတပ်ဆင်လိုက်တာပေါ့။ အဲ့ဒီအပြင် အခုအောက်မှာဖော်ပြထားတဲ့ Hardware ပိုင်းဆိုင်ရာ Enhancement တွေကိုလည်းလေ့လာကြည့်လိုက်ပါဦး။ အောက်ပါအချက်တွေက Network Card ကိုပိုမိုမြှန် ဆန်စေပါတယ်။

Direct Memory Access (DMA)

DMA ဟာ Adapter (Network Card) ကို Data တွေ Transfer လုပ်တဲ့နေရာမှာ (ငှားရဲ့ကိုယ်ပိုင် Card ပေါ်က Buffer ကနေ ကွန်ပျူတာ Memory ဆီ) CPU ရဲ့အကူအညီကိုရယူစရာမလိုဘဲ Memory သို့တိုက်ရိုက် Access လုပ်စေနိုင်ပါတယ်။

Shared Adapter Memory

သူကတော့ Adapter (Network Card) ရဲ့ Buffer ကို ကွန်ပျူတာရဲ့ RAM နှင့် Map လုပ်လိုက်တယ်။ Map ဆိုတာ ဒီနေရာမှာ အတူတူပဲဆိုတဲ့သဘောခံဆောင်ရအောင်။ ကဲ အခု Card ရဲ့ Buffer နှင့် RAM ထဲကနေရာတစ်ခုကို အတူတူပဲလို့ကွန်ပျူတာကသိနေပြီ။ ဒီတော့ ကွန်ပျူတာကတစ်စုံတစ်ခုကို RAM မှာသွားရေးမယ်ဆိုတိုင်း Network Card ပေါ်က Buffer မှာပဲသွားရေးဖြစ်တယ်။ ဒီနေရာမှာ ကွန်ပျူတာဟာ Card ပေါ်က RAM ကို သူ့ကိုယ်ပိုင်သဖွယ်သဘောထားပါတယ်။

Shared System Memory

အပေါ်ကရှင်းပြခဲ့တဲ့အချက်နှင့်ပြောင်းပြန်ဖြစ်ပါတယ်။ Network Card ဟာ System RAM ကို သူ့ကိုယ်ပိုင်သဖွယ်သဘောထားပြီးအလုပ်လုပ်ပါတယ်။ Network Card ပေါ်က On-Board Processor က Computer ပေါ်က System RAM ကို သူ့ Buffer နှင့်ကိုက်ညီမယ့် ဘယ်နေရာဘယ်အပိုင်းဆိုပြီး သတ်မှတ်လိုက်ပါတယ်။ ပြီးမှ Data ရေးတာပါ။ ဒီတော့ အခုပြောတဲ့ Shared System Memory က Card ဖက်ကနေ System RAM ကိုရေးချင်တဲ့အခါမှာသုံးပြီး အပေါ်က Shared Adapter Memory က ကွန်ပျူတာဖက်ကနေ Adapter ကိုလှမ်းရေးချင်တဲ့အခါမှာသုံးပါတယ်။

Bus Mastering

Bus Mastering ဆိုတာက DMA လိုပဲ။ DMA က Data တွေကို Transfer လုပ်ရာမှာ CPU အကူအညီမပါဘဲ Card က Memory ကိုတိုက်ရိုက် Access လုပ်နိုင်သလို အခု Bus Mastering ကလည်း CPU ၏ အကူအညီမပါဘဲ Bus ကနေမှ Memory ကို Data များ Transfers လုပ်ရာ၌ Initiate လုပ်ခြင်း Manage လုပ်ခြင်းတွေကို Card ကနေ Control လုပ်နိုင်ပါတယ်။ ဒီ အချက်ဟာ CPU ကိုများစွာအားလပ်သွားစေပါတယ်။ ဆိုလိုတာက တခြားကိစ္စတွေကို CPU က ပိုအာရုံစိုက်သွားနိုင်စေတာပေါ့။ ဒါကြောင့် Network Performance ဟာ ၂၀ ရာခိုင်နှုန်းမှ ၆၀ ရာခိုင်နှုန်းအထိတက်လာနိုင်ပါတယ်။ ဒီ Card တွေက Bus Mastering မရတဲ့ Card တွေထက်တော့ ဈေးပိုကြီးပါတယ်။

RAM Buffering

သူကကြတော့ Network Card မှာ Additional Memory ပေါ့။ Memory အပိုပါလာတယ်ဗျ။ ဘာလုပ်ဖို့အတွက်လည်းဆိုတော့ ဝင်လာမယ့် Data တွေ၊ ထွက်သွားမယ့် Data တွေအတွက် ယာယီနေရာပေါ့ဗျာ။ ဒီအတွက် Network Card ဟာ Data တွေကိုဆွဲယူတဲ့အခါမှာ ခေတ္တရပ်တန့်ခြင်းပြုစရာမလိုတဲ့အပြင် Data များများဆွဲယူနိုင်ပါတယ်။ ဒီအချက်ဟာ Network ရဲ့ Overall Performance ကိုတက်လာစေပါတယ်။

On-board Co-Processor

ဒါကတော့ Network Card အချို့မှာပဲပါပါတယ်။ ဒီ Co-Processor ပါခြင်းဖြင့် Data တွေနှင့်အလုပ်လုပ်တဲ့နေရာမှာပေါ့နော် Packet တွေကိုထွက်သွားစေဖို့ ထုတ်ပိုးခြင်း၊ ဝင်လာတဲ့ Packet တွေပြန်ဖြေခြင်းစတဲ့ကိစ္စတွေမှာ CPU ရဲ့ Service ကိုမလိုအပ်တော့ဘူးပေါ့။ ကနေ့ခေတ်မှာတော့ တော်တော်များများ Net-

work Card တွေမှာ ဒီ Processor တွေပါလာတတ်ကြပါတယ်။

Security Features

ဒါကတော့ အချို့သော High-End Network Card တွေမှာပါရနိုင်ပါတယ်။ ဒီအချက်ရဲ့ထူးခြားတဲ့ အချက်ကတော့ အဲဒီ Network Card ဟာ အားလုံးသော Protocol တွေနှင့် အလုပ်လုပ်နိုင်တဲ့အပြင် IPSec Protocol နှင့် အခြားသော Encryption Services နှင့်ပတ်သက်နေသောကိစ္စရပ်တွေကိုပါ Handle လုပ်နိုင်ပါတယ်။ IPSec ဆိုတာ IP Security ပါ။ ၎င်းဟာ လုံခြုံရေးဆိုင်ရာ Protocol တစ်ခုဖြစ်ပါတယ်။ Secure Transprot Mechansian လို့ ခေါ်ပါတယ်။ ၎င်းဟာ Network Traffic တွေ မလိုလားအပ်တဲ့ ရယူသုံးစွဲမှု၊ အချောင်သုံးစွဲမှု၊ စပ်စုမှု စတဲ့ Snooping တွေမှ ကာကွယ်ပေးပါတယ်။

Traffic Managment or Gromming

သူကလည်း တကယ့်ကို High End Network Card အချို့မှာပဲပါရှိနိုင်ပါတယ်။ ဒီ Services ကတော့ Remote Managment Software နှင့် Services တွေကို Support လုပ်ရန် Network ရဲ့ Access Level ရယူနိုင်မှုကို ပိုမိုကောင်းမွန်စေပါတယ်။ ၎င်းကို QOS (Quality of Service) လို့လည်း ခေါ်ပါတယ်။ Video နှင့် အခြားသော Multimedia Streaming လုပ်တဲ့အချိန်မှာ လိုအပ်တဲ့ Bandwidth ကိုရယူပေးနိုင်ပါတယ်။

Improved Fault Tolerance

သူကတော့ Network Card အပိုတွေစိုက်ထားတဲ့အခါမျိုးတွေမှာ Network Card တစ်ခုက Fail ဖြစ်သွားလို့ Network ရပ်တန့်မသွားအောင်အပိုထည့်ထားတဲ့ Network Card က ထ Run သွားတာဖြစ်ပါတယ်။ ဒါလည်း တကယ့်ကို High End ဖြစ်တဲ့ Network Card အချို့တွေမှာပဲပါပါတယ်။ နားလည်အောင် ပြန်ပြောရမယ်ဆိုရင် Network Card အပိုထည့်ထားခြင်းကြောင့် မူလအလုပ်လုပ်နေတဲ့ Network Card ပျက်သွားတဲ့အခါ Running လုပ်နေတဲ့ Network Traffic တာရပ်တန့်လိုက်ခြင်းမပြုဘဲ အပိုထည့်ထားတဲ့ Network Card ကိုပြောင်းပြီးဆက်အလုပ်လုပ်စေပါတယ်။

မှတ်ချက်။ ။ မိမိတပ်ဆင်ထားသော ကွန်ရက်တွေမှာ အသုံးပြုတဲ့ Application တွေဟာ - ဥပမာ Card တွေပါလာမယ်။ Database Managment System (DBMS) တွေပါလာပြီဆိုရင် သတိထားပါ။ ၎င်းတို့အသုံးပြုတဲ့ Data တွေဟာ Large Amount of Volumes ။ ဒါကြောင့် Network Card ကို သေချာရွေးချယ်ပြီးတပ်ဆင်ပါ။ ကြုံခဲ့ပုံးလို့ပါ။

ကျွန်ုပ်၏အတွေ့အကြုံ

ကျွန်တော်ဆင်ခဲ့ဖူးတဲ့ ကွန်ရက်တွေမှာ သတိထားမိသလောက်က နိုင်ငံခြားသားကုမ္ပဏီတွေက Network Card ကို 3 Com တံဆိပ်ကိုပဲတပ်ဆင်ခိုင်းပါတယ်။ မြန်မာ Local ကုမ္ပဏီတွေဆိုရင်တော့ ကျွန်တော်တို့ပေးတဲ့ Network Card ကိုပဲသုံးလိုက်ကြတာပဲ။ အဲ နိုင်ငံခြားကုမ္ပဏီအချို့ကတော့ 3 Com တံဆိပ် Network Card ကိုပဲ ကျွန်တော့်ကိုသုံးခိုင်းခဲ့ဖူးပါတယ်။ နောက်တစ်ခု ဒီကနေ့မျိုးဆက်သစ်လူငယ်တွေ ကွန်ရက်တွေသွားတပ်ဆင်တဲ့အခါ သတိပေးချင်တာက နိုင်ငံခြားသားကုမ္ပဏီတွေက DBMS ကိုတအားသုံးတယ်ဆိုတာပါပဲ။ ဥပမာ Microsoft Access ပေါ့။ ဒါမျိုးဆို Network တပ်ဆင်သူဟာ Network System သာမက DBMS သုံးနေစဉ် ရုတ်တရက်မီးအားပျက်တောက်မှ မရှိအောင်ပါစီစဉ်ပေးရတတ်ပါတယ်။ UPS ကိုပြော တာမဟုတ်ဘူး။ တစ်ချို့ရုံးတွေက မီတာနှစ်လုံးရှိရင် မီးလိုင်းနှစ်လိုင်းမှာ မီးအားပိုငြိမ်တဲ့လိုင်းမှာ အဲ့ဒီအတွက် Power Socket တွေသက်သက်ခွဲထားတတ်တယ်။ မှားတပ်မိလို့ ဒုက္ခရောက်ဖူးတယ်။

အခြား Network Card များ

ကဲ Network Card တွေမှာမှ ပုံမှန် Network Interface နှင့် မဟုတ်တဲ့ပုံမှန်ထက်ထူးကဲတဲ့စွမ်းဆောင်မှုမျိုးတွေအတွက် အထူးပြုလုပ်ထားသော Network Card တွေရှိပါသေးတယ်။ အဲ့ဒါတွေကတော့ Wireless Adapters အပါအဝင် Diskless Workstation (Disk မပါရှိသော Workstation) အတွက် Interface တွေဖြစ်ပါတယ်။ Wireless ကတော့ ဘာမှပြောစရာမရှိပေမယ့် Diskless Workstation ဆိုတာ Workstation မှာ Disk မရှိတာကြောင့် Boot လုပ်ဖို့ကိုတောင် Network ကနေ Boot လုပ်ပေးရတာပါ။ ကဲ ဆက်လေ့လာကြည့်ရအောင်။

Wireless Adapter

Wireless Network Adapter တွေဟာ ပုံမှန်အားဖြင့် Cable နှင့်တပ်ဆင်ရတဲ့ Network Card တွေထက်ပိုပြီး အထူးပြုလုပ်ထားတဲ့အချက်တွေပါဝင်နေတတ်ပါတယ်။ Wireless Network ဟာ အဓိက Network Operating System တွေဖြစ်ကြတဲ့ Windows NT, Windows 2000, Netware စတာတွေအတွက်ပဲရပါသေးတယ်။ ဒီ Wireless Adapter မှာပါဝင်တဲ့အရာတွေကတော့ -

(၁) Indoor အင်တီနာနှင့် အင်တီနာကြိုး

(၂) သက်ဆိုင်ရာ Network Environment မှာ သုံးဖို့ ၎င်း Adapter အတွက် Software

(၃) ကနဦး Installation နှင့် နောက်ပိုင်းပြဿနာတွေ Troubleshoot လုပ်ဖို့ Diagnostic Software

(၄) နောက် Installation Software တို့ဖြစ်ကြပါတယ်။

ၦင်းဟာ LAN တစ်ခုလုံး ကြိုးမဲ့ Wireless မှာအသုံးပြုနိုင်ဖို့ပါ။ အဲ့သလိုမှမဟုတ်ဘဲ Wireless Network နှင့် Wire ကြိုးချိတ်ထားတဲ့ Network ပေါင်းချင်ရင်တော့ Wireless Access Point ပစ္စည်းတစ်ခုရှိဖို့လိုအပ်ပါတယ်။

Remote Boot Adapter

အချို့အခြေအနေတွေမှာဗျာ- အဖွဲ့အစည်းကုမ္ပဏီတွေက Workstation တွေကို Disk Driver တွေမပါဘဲ အသုံးပြုချင်တတ်ကြပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ လုံခြုံရေးအခြေအနေအရသော်လည်းကောင်း၊ အများသုံးအဖြစ် အသုံးချချင်တဲ့အခါမှာသော်လည်းကောင်း၊ အခြားသော Public Access အဖြစ်အနေနှင့်သော်လည်းကောင်း အသုံးချချင်လို့ဖြစ်ပါတယ်။ ဒီနေရာမှာ ရှင်းပြချင်တာက Disk မပါဘဲ ဒီ Workstation ကဘယ်လိုသုံးသလဲဆိုတော့ အကြောင်းအရာတွေ Program တွေကို Network ကနေပဲရယူသုံးစွဲတာပေါ့ဗျ။ Boot လုပ်တဲ့အခါကြတော့ရော Boot က နှစ်နည်းလုပ်လို့ရတယ်။ Network Card မှာ Boot PROM (Programmable Read Only Memory) တပ်ပြီး ၦင်း ROM ကနေ Boot လုပ်လို့ရတယ်။ ကျွန်တော်ဆင်ခဲ့တုန်းက Boot PROM မပါတဲ့ Network Card တွေဆို တကူးတက Boot PROM လိုက်ရှာလိုက်မလုပ်တော့ဘူး။ Floopy Disk နှင့်ပဲ Boot လုပ်လိုက်တယ်။ ဆိုလိုတာက Boot လုပ်ပြီး Network Connection လုပ်ဖို့ လိုအပ်တဲ့ File တွေကို Boot PROM ထဲမှာ ထည့်ထားရင်ထည့် မထည့်ရင် Floopy Disk ထဲမှာ ထည့်ထားလို့ရပါတယ်။ Boot PROM ထဲမှာက ပုံမှန်အားဖြင့်တော့ 0.5 MB လောက်တော့ နေရာရှိပါတယ်။ အဲ့ဒီနေရာဟာ Boot လုပ်ဖို့အတွက် Hardware Code နှင့် Network Connection စတင်ဖို့အတွက်လိုအပ်တဲ့ File တွေထားဖို့လုံလောက်ပါတယ်။ Disk Less Workstation များ Network Connection ဖြစ်သွားပြီး နောက်ပိုင်းလိုချင်တဲ့အချက်အလက်တွေကို Network ကနေဆွဲချတော့မှာ ဖြစ်ပါတယ်။

၄.၁၉ Network Card Driver ဘင်္ခြင်း

Network Adapter ကိုတပ်ဆင်ပြီးသကာလ အသုံးပြုဖို့အတွက် Device Driver ကိုတင်ပေးရမှာဖြစ်ပါတယ်။ ဟိုအရင်တုန်းကတော့ Network Card ရောင်းတဲ့သူတိုင်းဟာ သူတို့ရဲ့ Network Card ကို သူတို့ Driver နှင့်သူတို့လာကြပါတယ်။ ဒါပေမယ့် အခုနောက်ပိုင်းမှာတော့ Operating System တွေက ကွန်ပျူတာမှာ ဆော့ဆင်ထားတဲ့ Card တွေကို ၦင်း Operating System နှင့်ဆက်သွယ်ဖို့ Device Driver ကို Developed လုပ်လာကြပါတယ်။ ကဲဒီတော့ ကျွန်တော်တို့ အဓိက ၃ မျိုးဖြစ်တဲ့ Driver Standard တွေကိုလေ့လာကြရအောင်။

Network Device Interface Specification (NDIS)

သူက Network Interface Driver နှင့် MAC Sublayer အကြားဆက်နွယ်မှု Interface ကို ပြုလုပ်ပေးတယ်။ NDIS ရဲ့အဓိက အကျိုးကျေးဇူးကတော့ NIC ကိုတပြိုင်တည်း Protocols တွေအများကြီး ချိတ်ဆက်ခွင့်ပြုတာပဲဖြစ်ပါတယ်။ ၎င်းဟာ Windows 95 ကနေစပြီး ဒီနေ့ထိ Operating System အထိအားလုံးအကျုံးဝင်ပါတယ်။

Win32 Driver Model (WDM)

သူကတော့ ဒီနေ့ခေတ် 32 bit Windows Operating System အတွက် ပြည့်စုံတဲ့ Driver ကိုသတ်မှတ်ပေးပါတယ်။ WDM နည်းပညာကတော့ Drivers ကိုအမျိုးမျိုးသော Bus နှင့် Drive Class အဖြစ်ပိုင်းလိုက်ပါတယ်။ ဘယ်လိုပိုင်းလိုက်တာလဲဆိုတော့ လုပ်ဆောင်ချက်ပိုင်း၊ Adapter ရဲ့ဘုံအပိုင်းဆိုင်ရာတွေကိုထိန်းချုပ်တဲ့ Drivers အပိုင်း၊ နောက်ပြီး ဘာလာတပ်သလဲ (Ethernet, Token Printer, Scanner စသဖြင့်) ဆိုတာပေါ်မူတည်ပြီး အလုပ်လုပ်ဖို့အပိုင်းဆိုပြီး ပိုင်းထားပါတယ်။ ဒီတော့ ထုတ်လုပ်သူတွေဟာ Device Driver တွေကိုပြုလုပ်ရာမှာ သူ့အပိုင်းနှင့်သူ Concentrate လုပ်နိုင်ပါတယ်။ WDM ဟာ တော်တော်များများပစ္စည်းတွေအတွက် Plug and Play Support လုပ်ပါတယ်။

Open Data Link Interface (ODI)

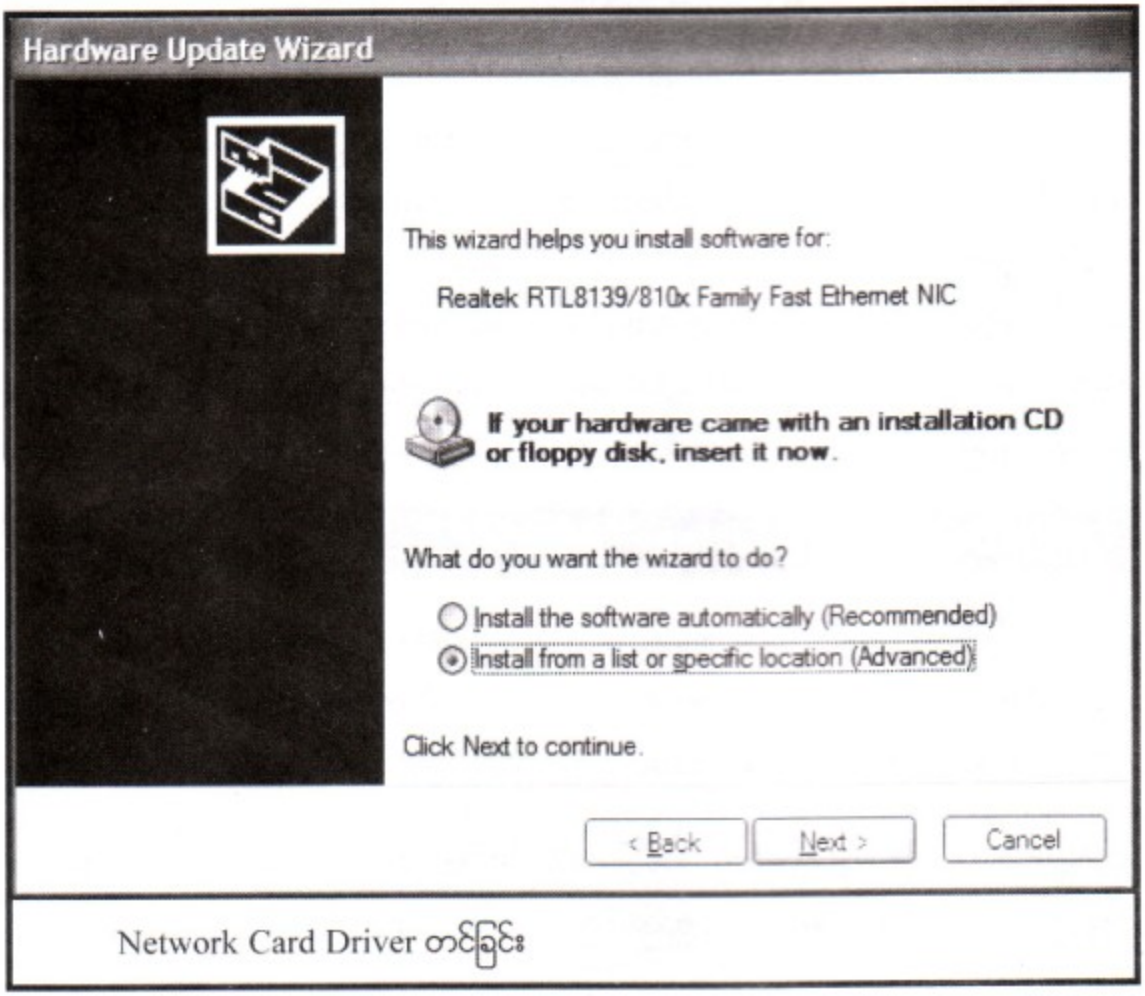
ODI ကို Apple Computer နှင့် Novell တို့က Define လုပ်ခဲ့တာဖြစ်ပါတယ်။ ODI ဟာ NIC ကို Multiple Protocols အသုံးပြုခြင်းတစ်ခုတည်းကိုပဲ ခွင့်ပြုရုံသာမက Driver ပြုလုပ်မှုကို ရိုးရှင်းစေပါတယ်။ ODI ဟာ NDIS နှင့်ဆင်ပါတယ်။ ဒါပေမယ့် Driver နည်းပညာအရ သပ်သပ်ဆိုဖြစ်ပါတယ်။

မှတ်ချက်။ ။ အခုပြောခဲ့တဲ့ အပေါ်ကအကြောင်းအရာတွေဟာ Network Interface အတွက်ပဲ ပြောပြခဲ့တာမဟုတ်ပါ။ အခြားသောပစ္စည်းတွေရဲ့ Driver သဘောတရားတွေနှင့် အကုန်အကျုံးဝင်ပါတယ်။

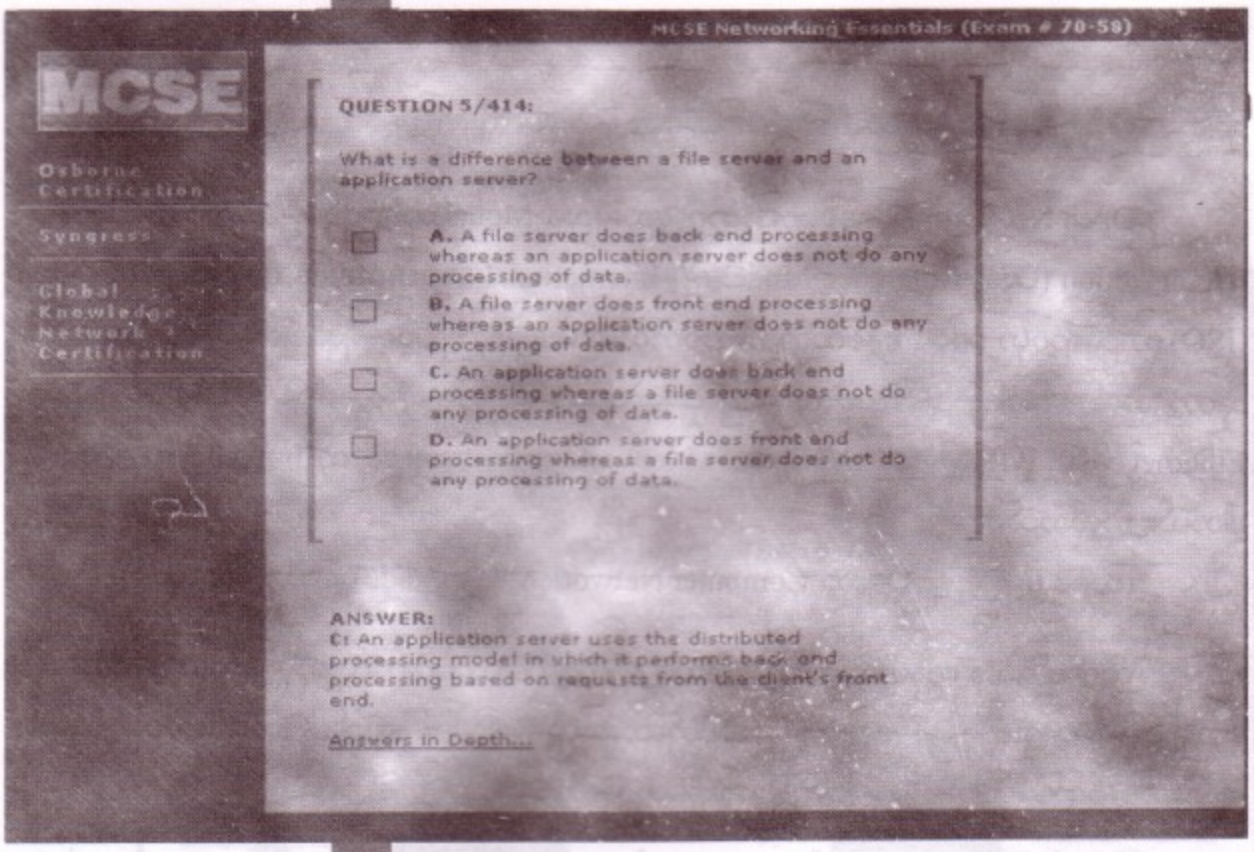
ကဲ Network Card ကို Driver တင်ကြည့်ရအောင်။ ကျွန်တော့်အနေနှင့် ကြုံတွေ့ခဲ့ဖူးသလောက် အကြံဉာဏ်ပေးချင်တာကတော့ Network Card Driver ကိုတင်တဲ့နေရာမှာ Operating System က Support လုပ်တဲ့ Driver ကိုအသုံးပြုခြင်းထက် ထုတ်လုပ်သူကထည့်ပေးလိုက်တဲ့ Driver ကိုပဲအသုံးပြုစေချင်ပါတယ်။ ဒီတော့ Network Card ကိုဝယ်ယူတဲ့အခါမှာ ကိုယ်အသုံးပြုမယ့် Operating System အတွက် ဒီ Network Card က Driver Support လုပ်ရဲ့လား။ ဝယ်ကတည်းကကြည့်ပါ။ Network Card ကို ကွန်ပျူတာမှာစိုက်ပြီးသကာလ Driver CD ကိုထည့်ပြီး Install လုပ်နိုင်ပါပြီ။ တချို့ Driver တွေကို ကိုယ်ပိုင်

Installation Software နှင့်လာတက်ပြီး အဲသလိုမဟုတ်ရင်တော့ Device Manager ကနေ Install သွားလုပ်ပေးပါ။ Install လုပ်နေစဉ်/လုပ်ပြီးမှာ IRQ တွေ I/O Port တွေစစ်ပေးပါ။ Conflicts ဖြစ်မဖြစ်ပေါ့။ အားလုံးကောင်းမွန်စွာ Install လုပ်ပြီးရင်တော့ အသုံးပြုလို့ရပါပြီ။ သိပ်ပြီးသေချာချင်ရင်တော့ ဒီ Network Card ရဲ့ IRQ တို့ I/O Port တို့ကို စသဖြင့်ပတ်သက်ရာလေးတွေကို ကောက်နှုတ်ပြီး ကွန်ပျူတာမှာ Sticker နှင့်ကပ်ထားပေးလည်းရပါတယ်။ နောက်ပိုင်း Network Troubleshoot လုပ်တဲ့အခါ စနစ်ကျတာပေါ့။ မလုပ်လည်းရပါတယ်။

ပုံ ၄.၁၉



Network Card Driver တင်ခြင်း



UNIT 5

OSI Reference Model

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက် ဆက်သွယ်ရေး နှင့် ပတ်သက်နေတဲ့ နည်းပညာ အကြောင်းတွေကို လေ့လာရမှာဖြစ်ပါတယ်။ Protocols တွေအတွက် စံသတ်မှတ်ထားသော OSI Model ကိုအဓိကထားလေ့လာမှာဖြစ်ပါတယ်။

၅.၁ OSI Reference Model ဆိုတာ

Open Networking စနစ်များအတွက်နည်းပညာ Model တစ်ခုဖြစ်တဲ့ ဒီ Open System Interconnection (OSI) Reference Model ကို International Organization for Standardization (ISO) က ဥရောပမှာ ၁၉၇၄ ခုနှစ်ကတည်းကစတင် Developed လုပ်ခဲ့တာဖြစ်ပါတယ်။ ကနဦးမှာတော့ သူဟာ အကြောင်းကြောင်းကြောင့် အောင်မြင်မှုမရခဲ့ပါဘူး။ အလွှာ (၇) လွှာပါတဲ့ ဒီ OSI Model ဟာ Ethernet တို့ TCP/IP တို့ စတဲ့ အမျိုးမျိုးသော Networking Protocol တွေကို Implement လုပ်ပေးနိုင်ပါတယ်။ ဆိုလိုသည်ကား -

(ယခင် ရေးသားပြီးခဲ့သော Computer Network Study Guide မှကောက်နုတ်ချက်)

တကယ်တော့ ကွန်ပျူတာအချင်းချင်းဆက်သွယ်ဖို့ဆိုတာအတော်လေးကိုရှုပ်ထွေးတဲ့ကိစ္စတစ်ခုပါ။ ဒီထက်ပိုပြီးရှုပ်ထွေးတဲ့ကိစ္စတစ်ခုတော့ သတ်မှတ်ထားသော Rule တစ်ခုတည်းနဲ့ အားလုံးကိုတပြိုင်တည်းပြေလည်ဖို့ဆိုတာပါပဲ။ ဘယ်လိုအကြောင်းအရာတွေလဲဆိုတော့ - ဥပမာပြောရရင်

၁။ မတူညီတဲ့ Computer အမျိုးအစားတွေကို ဆက်သွယ်နိုင်ဖို့

၂။ ပို့လိုက်တဲ့ Data တွေဟာ ရည်ရွယ်ရာ Target ကိုတိုက်ရိုက်ရောက်အောင် ဘယ်လိုသွားမလဲ။

၃။ ရရှိလာတဲ့ Message တွေကရောမှန်ကန်မှုရှိသလား၊ ဘယ်လိုပြန်စစ်မလဲ။

၄။ Data Flow Rate ကို ဘယ်လိုထိန်းကျောင်းမလဲ။ စသည့်အချက်ကလေးတွေအများကြီးပေါ့။

သူတို့တွေအားလုံး တစ်ပြိုင်တည်းပြေလည်ဖို့ Model တစ်ခုရှိပါတယ်။ ဒါဟာ ခုပြောနေတဲ့ အလွှာ (၇) လွှာနဲ့ OSI ပဲပေါ့။ သူ့ကို Protocol Stack လို့လဲခေါ်ပါတယ်။ ဒီ အလွှာ (၇) လွှာနဲ့ နာမည်တွေကို ကျွန်တော်တို့ မှတ်မိလွယ်အောင် အောက်ပါအတိုင်းမှတ်သားနိုင်ပါတယ်။ အပြန်အလှန် မှတ်လို့ရအောင် နှစ်ခုပေးထားတာပါ။ ကြိုက်တာတစ်ခုမှတ်ထားလဲရပါတယ်။

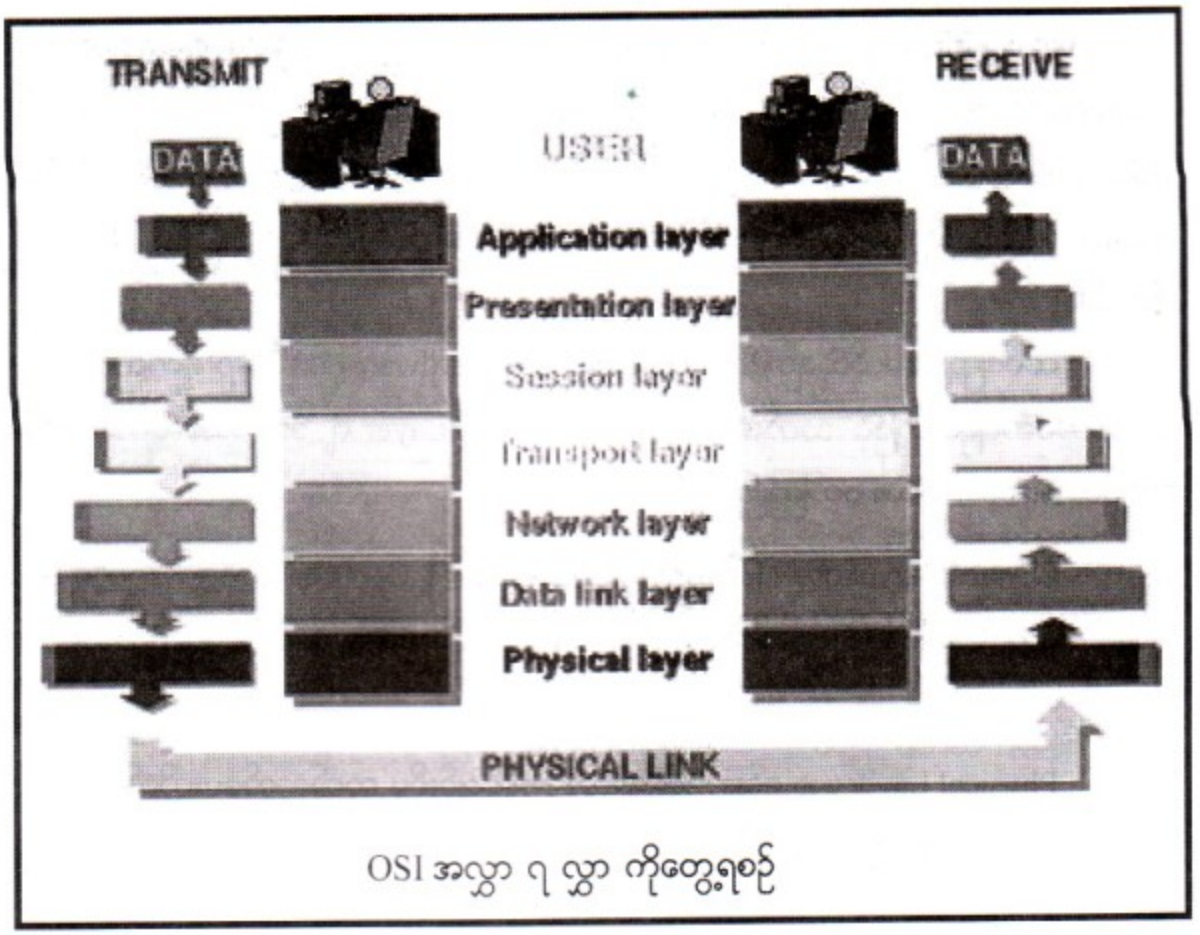
All People Seem To Need Data Processing

Please Do Not Throw Sausage Pizza Away

အဲဒီမှာ Layer 1 က Physical Layer ပါ။ Application Layer ကတော့ Layer 7 ပါ။ Layer 1 ဆိုတဲ့ Physical Layer Protocol က Network Media ပေါ်မှ Communication ကို Control လုပ်ပါတယ်။ Layer 7 ဆိုတဲ့ Application Layer ကတော့ Computer မှာသုံးနေတဲ့ Application တွေအတွက် Network Service ကို ချိတ်ဆက်ပေးပါတယ်။ ကြားထဲက အလွှာ (၅) ခုကတော့ အလယ်အလတ်ဆက်သွယ်ရေးတာဝန်တွေကိုလုပ်ကြရပါတယ်။ OSI Model ဟာ ဆက်သွယ်ရေးလုပ်ငန်းဆောင်တာတွေကို အလွှာတွေအဖြစ်အနေနဲ့ ခွဲခြားလိုက်ပါတယ်။ ဆက်သွယ်ရေးဖြစ်ဖို့အတွက် အလွှာတစ်လွှာချင်းစီမှာရှိတဲ့ မတူညီတဲ့

Protocol တွေကဖြေရှင်းဆောင်ရွက်ကြပါတယ်။ အဲဒီ Protocol တွေဟာ ဆက်သွယ်ရေးမဖြစ်မမြောက်မခြင်း တစ်ခုနဲ့တစ်ခု Stack သဖွယ် အထပ်လိုက်လုပ်ဆောင်ကြရပါတယ်။

ပုံ ၅.၁



OSI အလွှာ ၇ လွှာ ကိုတွေ့ရစဉ်

ထပ်ပြီးတော့ပြောရမယ်ဆိုရင် အမျိုးမျိုးသော Networking Protocol တွေဖြစ်ကြတဲ့ TCP/IP အိမ္မာမဟုတ် Ethernet စတာတွေကို Implement လုပ်ပေးနိုင်မယ့် Functions တွေဟာ အလွှာ (၇) လွှာသော OSI Model မှာပါရှိပါတယ်။ ကဲ တစ်လွှာချင်းစီကိုဆက်လက်လေ့လာကြရအောင်။

၅.၂ Physical Layer ဆိုတာ

Physical Layer သည် OSI ရဲ့ အလွှာ (၇) လွှာထဲက အောက်ဆုံးအလွှာဖြစ်ပါတယ်။ Physical Layer ဆိုတာ Network Medium (ဥပမာ Network ကြိုး) တွေရဲ့ သဘောသဘာဝတွေကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ နောက်ပြီး ၎င်း Network Medium မှတဆင့် Signals တွေ ဘယ်လို Transmit လုပ်မယ်ဆိုတာတွေကို သတ်မှတ်ပေးတာဖြစ်ပါတယ်။ ဒီထက်ပိုပြီးပြောရမယ်ဆိုရင်တော့ ၎င်းဟာ Network Medium ဖြစ်တဲ့ Wire ကြိုးထဲကို သက်ဆိုင်ရာ Bits တွေ စီးဝင်စေဖို့ Physical Interface နဲ့ Mechanisms ကိုဖြစ်တည်အောင်ပြုလုပ်ပေးရပါတယ်။ နောက်တစ်နည်းအရပြောရရင် ၎င်းအလွှာဟာ Voltage

တွေ၊ Current တွေ၊ Modulation တွေ၊ Bit Synchronization တွေ၊ Connection တွေရဲ့ Actication နဲ့ Deactivation တွေကိုပါ သတ်မှတ်ပေးရပါတယ်။ အဲဒီအပြင် ၎င်းအလွှာနဲ့ထိတွေ့မယ့် Transmission Media (ဥပမာ- Network ကြိုး) ဟာ (UTP-Unshielded Twisted Pair, STP - Shielded Twisted Pair, Coaxial, Fiber Optic) စသည်ဖြင့် အမျိုးမျိုးဖြစ်နိုင်တာကြောင့် ၎င်းဟာ အမျိုးမျိုး သော Electrical Characteristics တွေကိုလည်း သတ်မှတ်ပေးရပြန်ပါတယ်။ ၎င်းအလွှာတွေမှာပါတဲ့ Protocol တွေကတော့ IEEE 802.3, RS-232c နဲ့ X.25 တို့ဖြစ်ကြပါတယ်။ နောက်ထပ်ပြောပြချင်တာက Repeaters တွေ၊ Network Card တွေ၊ Transceivers တွေအပြင် Cable တွေဟာ၎င်းအလွှာနဲ့ နှစ်ပါးသွား လုပ်ဆောင်ရပါတယ်။

ထပ်ပြောပြရမယ်ဆိုရင် Physical Layer ဟာ Hardware ပိုင်းဆိုင်ရာ ချိတ်ဆက်ခြင်း၊ ထိန်းသိမ်းခြင်းနှင့်တပ်ဆင်ခြင်းတို့ဖြင့် သက်ဆိုင်ပါတယ်။ Physical Layer ရဲ့ အချက်အလက်တွေကိုအောက်မှာ ဖော်ပြထားပါသေးတယ်။ ဖတ်ကြည့်လိုက်ပါအုံး။

- ❖ Physical Layer ဟာ Network Interface Card နဲ့ Cable ဘယ်လိုချိတ်ဆက်မှုပြုရမယ်ဆိုတာတွေ၊ Cable ရဲ့ Pin အရေအတွက်နဲ့ Pin တစ်ခုချင်းစီရဲ့ လုပ်ဆောင်မှုတွေကအစသတ်မှတ်ပေးရပါတယ်။
- ❖ Physical Layer ဟာ ၎င်းအပေါ်ရှိအလွှာ တစ်ခုချင်းစီမှ ထုတ်လွှတ်ပေးလိုက်သော ပို့လွှတ်ရမည့် Signals များကို သယ်ယူပို့ဆောင်ပေးပါတယ်။
- ❖ ဒီတော့ Physical Layer ဟာ Signals ပို့ဆောင်ပေးရမယ်ဆိုတော့ကား - Network Cable ကိုဖြတ်ပြီး Data ပို့ရန် ဘယ်လိုနည်းပညာကိုသုံးပြီးပို့ရမယ်ဆိုတာကိုပါ သတ်မှတ်ပေးရပါတယ်။ Signals တွေဆိုတော့ဗျာ- ပြောရရင် ကွန်ပျူတာ တစ်လုံးနှင့်တစ်လုံးအကြားပို့လွှတ်တဲ့ Bit (0 and 1) တွေပေါ့။
- ❖ Physical Layer ဟာပို့လွှတ်လိုက်တဲ့ Bit တွေ Synchronize ဖြစ်ဖို့နဲ့ Data များကို Encode လုပ်ဖို့အတွက်လည်းပံ့ပိုးပေးပါတယ်။

၅.၃ OSI Physical Layer အကြောင်းသိကောင်းစရာ

တကယ်တော့ Physical Layer ဟာဘယ်လို Medium (ဥပမာ Network ကြိုး) မျိုးကိုမှ သတ်မှတ်တာမဟုတ်ပါဘူး။ သူသတ်မှတ်လုပ်ဆောင်ပေးတာက Medium ရဲ့လိုအပ်ချက်တွေကိုပါ။ အသုံးပြုတဲ့ Medium ပေါ်မူတည်ပြီး Physical Layer ရဲ့ Specification တွေဟာကွာခြားပါတယ်။ ဆိုလိုချင်တာက UTP အတွက် Ethernet ရဲ့ Physical Layer မှ Specification ဟာ Coaxial အတွက် Ethernet ရဲ့

Physical Layer မှ Specification နဲ့တော့ကွာခြားနေမှာဖြစ်ပါတယ်။ ဒါဟာ Physical Layer ရဲ့ရည်ရွယ်ချက်ပါပဲ။ အခု Connection Types တွေအကြောင်းလေ့လာရအောင်။ သူ့ရဲ့လုပ်ဆောင်ရမယ့် တာဝန်တွေကတော့ ခုနကပြောခဲ့တဲ့ Transmission Technique တွေရယ်၊ Pin Layout ရယ်၊ Connector Type ရယ်တို့ကိုထိန်းချုပ်ပို့ပါဖြစ်ပါတယ်။

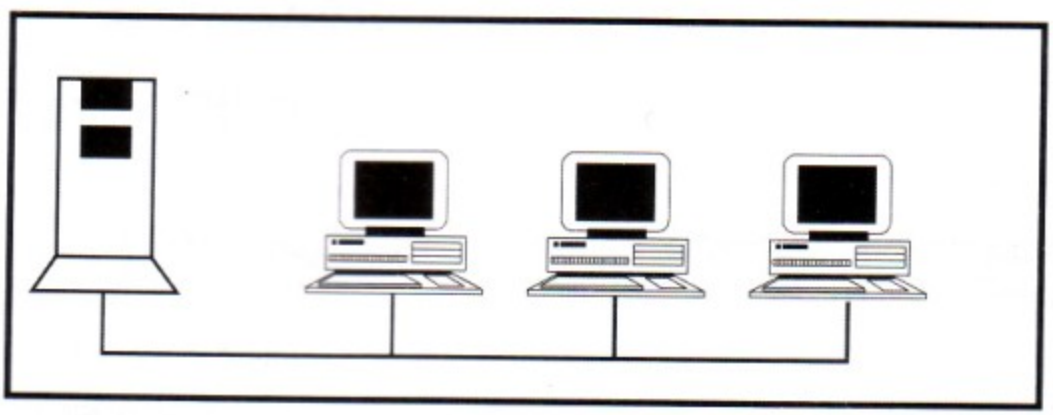
၅.၄ Connection Types (ချိတ်ဆက်နည်းများ)

ဘယ်လို Connection မျိုးဖြစ်ပါစေ။ တကယ်တမ်းတော့ အခုအောက်မှာပြထားတဲ့ Connector Types နှစ်ခုထဲမှာပဲ အကျုံးဝင်တာဖြစ်ပါတယ်။

- ❖ Multipoint Connections
- ❖ Point to Point Connections

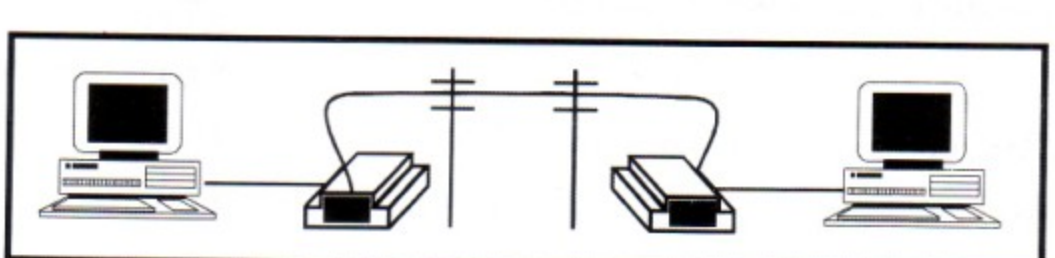
Multipoint Connection ဆိုတာပစ္စည်းတစ်ခု (ဥပမာ-ကွန်ပျူတာ) မှတခြားနှစ်ခု (သို့မဟုတ်) နှစ်ခုထက်ပိုတဲ့ပစ္စည်းတွေကို ချိတ်ဆက်ပေးနိုင်တာကိုပြောတာဖြစ်ပါတယ်။ ပုံကိုကြည့်ပါ။ တစ်နည်းအားဖြင့်ပြောရရင် Multipoint Connection ကိုအသုံးပြုပြီးတော့ ချိတ်ဆက်ထားတဲ့ပစ္စည်းတိုင်းဟာ တူညီတဲ့ Network Transmission Medium (ဥပမာ Network ကြိုး) ပေါ်မှာ Shared လုပ်ပြီး ချိတ်ဆက်ထားတာပါ။

ပုံ ၅.၂



Point to Point Connection ဆိုတာကြတော့ ပစ္စည်းတစ်ခုမှ တခြားပစ္စည်းတစ်ခုကိုပဲ ချိတ်ဆက်လို့ရပါတယ်။ ပုံကိုကြည့်ပါ။ ကြိုးမားတဲ့ကွန်ရက်တွေဟာ တကယ်တော့ Point to Point တွေနဲ့တည်ဆောက်နိုင်ကြပါတယ်။

ပုံ ၅.၃



၅.၅ Physical Topologies အခြေခံသိကောင်းစရာ

Network Medium တွေရဲ့ အပြင်အဆင်အနေအထား Layout ကိုဖော်ပြပေးထားတဲ့ Network တစ်ခုရဲ့ Physical Topology ပါပဲ။ မတူညီတဲ့ Physical Topologies တိုင်းမှာမတူညီတဲ့ Characteristics တွေရှိကြပါတယ်။ ပြောရရင်တော့ Performance တို့၊ ဘယ်လို Installation လုပ်ရမှာတို့ ဘယ်လို Trouble-shoot လုပ်ရမှာတို့၊ ဘယ်လို Configuration လုပ်ရမှာတို့ပဲဖြစ်ကြပါတယ်။

၅.၆ Physical Topologies Based on Multipoint Connections အခြေခံသိကောင်းစရာ

Multipoint Connection မှာအခြေပြုတဲ့ Topology ဟာတစ်ခုတည်းရှိပါတယ်။ အဲ့ဒါကတော့ Bus ပါပဲ။ ပုံ ၅.၂ မှာပြထားပါတယ်။ သတိထားမိလား။ အားလုံးသောချိတ်ဆက်ထားတဲ့ပစ္စည်းတွေဟာ ဘုံဖြစ်တဲ့ Transmission Medium ပေါ်မှာချိတ်ဆက်ထားရတာပါ။ တချို့နေရာတွေမှာ ၎င်းကို Backbone Net-work လို့လည်းခေါ်ပါတယ်။ ၎င်းနှင့်ပတ်သက်နေသောအကြောင်းအရာများကိုပြုခဲ့တဲ့သင်ခန်းစာများတွင်ဖော်ပြ ခဲ့ပြီးဖြစ်ပါတယ်။

၅.၇ Physical Topologies Based on Point to Point Connections အခြေခံသိကောင်းစရာ

Point to Point Connections တွေမှာတွေ့ရတဲ့ Topology အမျိုးမျိုးကို ပုံ ၅.၄ မှာပြထားပါတယ်။ တစ်ဖက်မှာလည်းဖော်ပြထားပါတယ်။

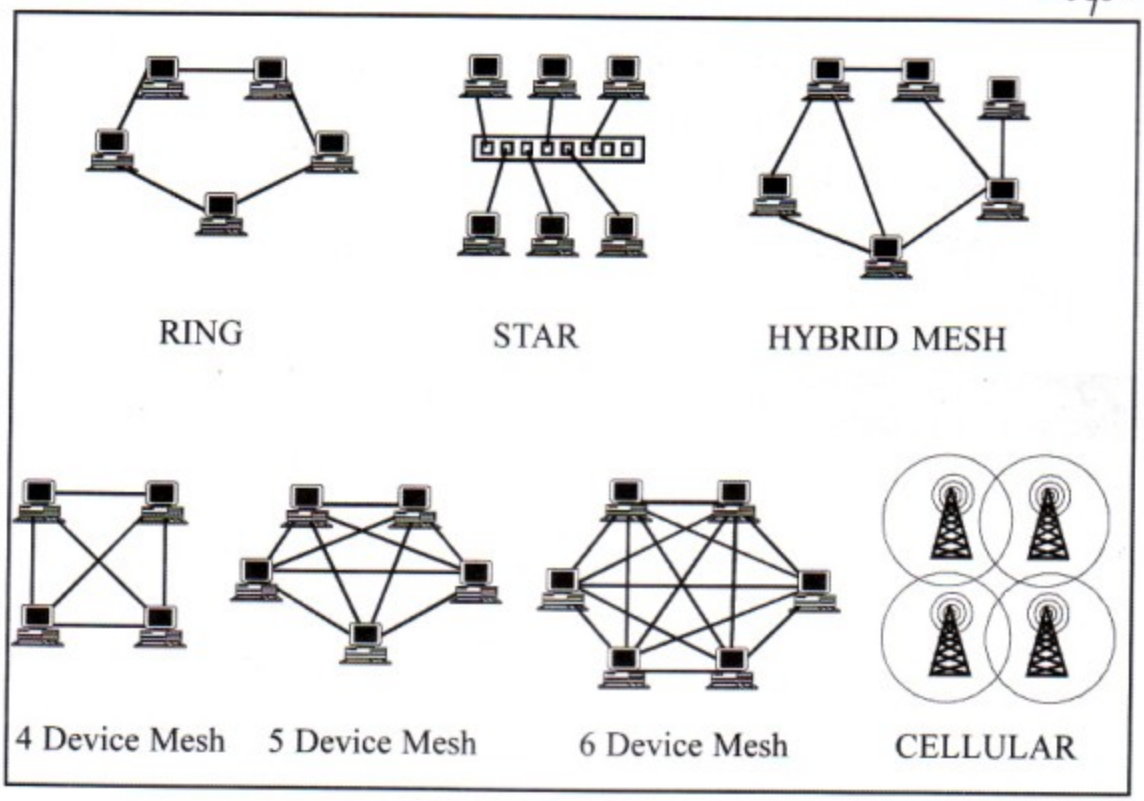
Star Topology အခြေခံသိကောင်းစရာ

Star Topology ဆိုတာ ပစ္စည်းတစ်ခုချင်းစီက Central Hub ဆီကိုချိတ်ဆက် ဆက်သွယ်တဲ့ စနစ်ဖြစ်ပါတယ်။ Central Hub က Data Signals တွေကိုသက်ဆိုင်ရာမှနေ ကွန်ရက်တွေမှတဆင့် ရောက်ရှိလာပြီး တဖန်သက်ဆိုင်ရာ Destination တွေအရောက် ပြန်လည်လမ်းခွဲပို့ဆောင်ရပြန်ပါတယ်။

Mesh Topology အခြေခံသိကောင်းစရာ

ကွန်ရက်ပေါ်မှာ ပစ္စည်းတွေကိုနှစ်ခုတစ်စုံချင်း Point to Point ချိတ်ဆက်ထားတာကို Mesh လို့ခေါ်ပါတယ်။ သူကတော့ ကွန်ပျူတာအရေအတွက်နဲ့ Connection အရေအတွက် မကာမိပါဘူး။ ဥပမာ ပြောရရင်ပစ္စည်း၄ခု ချိတ်ဆက်လိုက်တယ်ဆိုရင် (၄×၃× ½) Connection ဖြစ်သွားပြီ။

ပုံ ၅.၄



Total 24 Connection ဖြစ်စေပါတယ်။ ဒီပေမယ့် အကယ်၍များပစ္စည်းတိုးခဲ့ချိတ်ဆက်ထားရာကနေ ခြောက်ခု များဖြစ်သွားမယ်ဆိုရင်တော့ Connections ဟာ (၅×၄×၄×၂) ဖြစ်သွားပြီးတော့ Connection အရေ (၁၂၀) ဖြစ်သွားပါတယ်။ ဒီကြောင့်မို့ သူ့ကိုသိပ်ကြိုးတဲ့ ကွန်ရက်တွေမှာအသုံးပြုခဲ့ပါတယ်။ ဒီပေမယ့် သူ့မှာကောင်းကျိုးအချက်နှစ်ခုတော့ရှိပါတယ်။ တစ်ခုကတော့ ပစ္စည်းတိုင်းဟာ တခြားချိတ်ဆက်ထားတဲ့ ပစ္စည်းတိုင်းကို ချိတ်ဆက်ထားမှုဟာ အာမခံအပြည့်အဝရှိတာပါပဲ။ ဘာဖြစ်လို့လဲဆိုတော့ ပစ္စည်းတိုင်းကို တိုက်ရိုက်ချိတ်ဆက်ထားတာကိုး။ နောက်တစ်ခုကတော့ Fault Tolerance အင်မတန်ကောင်းမွန်မြင့်မားတာပဲဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ ပစ္စည်းတိုင်းကိုတိုက်ရိုက်စီ Connections တွေ အများကြီးနဲ့ ချိတ်ဆက်ထားတာကြောင့် ကြားခံ Media တွေတစ်ခုခုဖြစ်ပျက်သွားခဲ့ရင်တောင် ဒီကွန်ရက်ကြီးဟာ Message တွေကို ၎င်းကွန်ရက်မှာရှိတဲ့ပစ္စည်းတိုင်းကို ပေးပို့နိုင်သေးလို့ပဲဖြစ်ပါတယ်။

Hybrid Netwrok ဆိုတာလည်း ဒီအတိုင်းပါပဲ။ ပိုမိုတဲ့ဆက်သွယ်ဆောင်ရွက်မှု (Redundant Links) တွေရှိနေတာကြောင့် Network ဟာ ဘယ်တော့မှ မကျသေလောက်ပါပဲ။ ဒါ Redundant Links တွေရဲ့ကောင်းမွန်တဲ့ အာမခံချက်ပဲပေါ့။

Ring Topology အခြေခံသိကောင်းစရာ

Ring Topology ဆိုတာကတော့ စက်ပိုင်းသဖွယ်ပတ်လည်ရိုက်နေတဲ့ ဆက်သွယ်မှုစနစ်ကိုပြောတာပါ။ Signal တွေဟာငင်းစက်ပိုင်းတစ်လျှောက်လားရာတစ်ဖက်တည်းနဲ့ သွားလာနေကြပါတယ်။ ပစ္စည်းတစ်ခု

ချင်းစီဟာ ၎င်းဆက်သွယ်မှုစနစ်ဖြစ်မြောက်အောင်မြင်အောင် ဝိုင်းဝန်းလုပ်ဆောင်ပေးရတာတစ်ခုတော့ရှိပါတယ်။ အဲ့ဒါကတော့ ဒီကွန်ရက်တွေထဲမှာရှိတဲ့ပစ္စည်းတိုင်းဟာ Repeater သက့ဲသို့ Transmit and Receive ပါလုပ်နေရပါတယ်။ ဒါမှလည်း မိမိဆီ Signal တွေရောက်မှာဖြစ်သလို ပြန်ပြီး Retransmit လုပ်မှလည်း ဒီ Ring ထဲမှာရှိတဲ့တခြားပစ္စည်းတစ်ခုစီကို Signal တွေရောက်ရှိမှာဖြစ်ပါတယ်။ နောက်တစ်ခုကလည်း Low ဖြစ်လာတဲ့ Signal တွေကိုတခါပြန်ပြီး Regenerate လုပ်သလိုလည်းဖြစ်စေပါတယ်။

Cellular Topology အခြေခံသိကောင်းစရာ

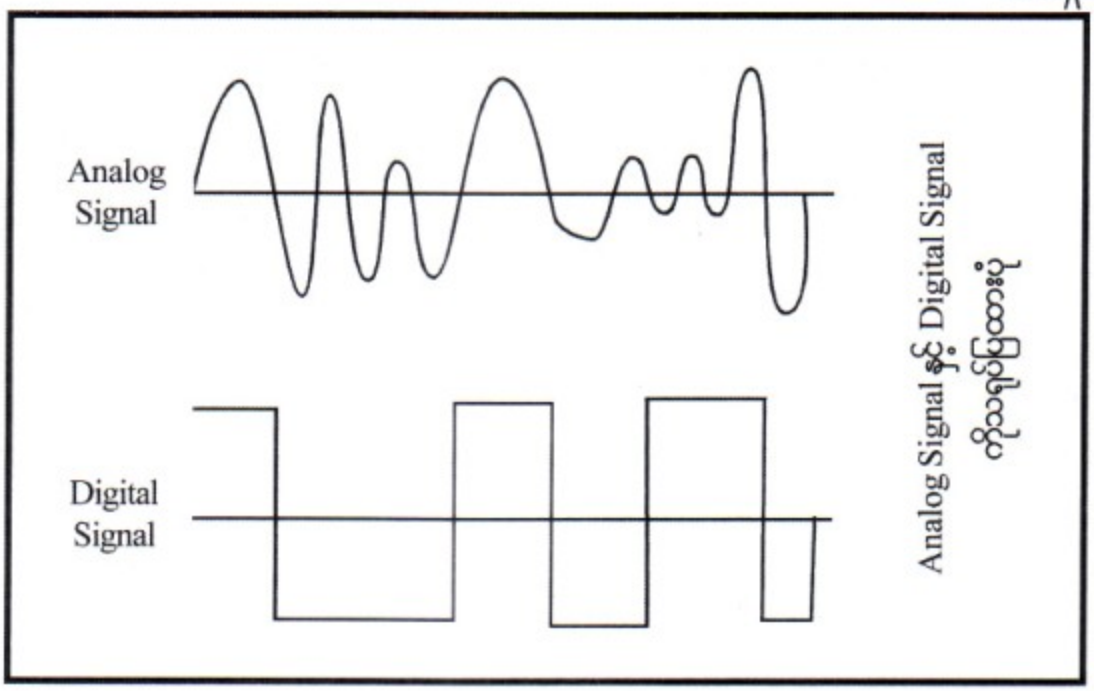
Transmission နဲ့ Receiver တွေကိုအသုံးပြုပြီး သတ်မှတ် Area တွေကိုထပ်ကာထပ်ကာနဲ့ ချိတ်ဆက်ထားတာဖြစ်ပါတယ်။ Cellular Network ဆိုတာကတော့ Area တွေကိုသတ်မှတ်ချက်အလိုက် ဝိုင်းထုတ်ပစ်လိုက်ပါတယ်။ Cells တွေသဖွယ်ပေါ့။ ပြီးမှငင်းတို့ကို Central Station တွေကနေ ဝန်ဆောင်မှုပေးပါတယ်။ ပစ္စည်းတွေက Radio Signals ကိုသုံးပြီး Central Station နဲ့ချိတ်ဆက်ကြရပါတယ်။ ၎င်း Central Station မှတခြား Station တွေကို Message တွေပြန်လမ်းခွဲပေးပါတယ်။ ၎င်းကို Area ဟာ ပထဝီအနေအထားတော်တော် ကျယ်ကျယ်လုပ်ဆောင်လိုတဲ့နေရာမှာသုံးပါတယ်။

၅.၈ Digital & Analog Signaling အခြေခံသိကောင်းစရာ

Information တွေကို Communication လုပ်ပေးတဲ့ဖြစ်စဉ်ကို Signaling လို့ခေါ်ပါတယ်။ အဲ့ဒီလို Information တွေကို Communicate လုပ်ပေးတဲ့နေရာမှာ ပုံစံ(၂)မျိုးရှိပါတယ်။ အဲ့ဒါကတော့ Analog နဲ့ Digital ဆိုတာပဲဖြစ်ပါတယ်။ Information တွေဟာ အဲ့ဒီပုံစံနှစ်မျိုးကို တစ်မျိုးသို့ မကြာခဏပြောင်းရပါတယ်။ ဆိုလိုချင်တာက Signal တွေကိုလက်ခံရရှိပြီးတဲ့အခါမှာ ရရှိလာတဲ့ Signal တွေကို နဂို Information တွေအဖြစ်ပြန်ပြောင်းရပါတယ်။ ဒါဟာ Encoding ပါပဲ။ တနည်းအားဖြင့်ပြောရရင် Information တွေ Communicate ဖြစ်နေတာ Analog နဲ့ Digital Signal တွေတလှည့်စီဖြစ်ပေါ်နေလို့ပါ။ ဒါကို Modulation သို့မဟုတ် Encoding လို့ခေါ်ပါတယ်။

မှတ်ချက်။ ။ ပုံ ၅.၅ မှာလည်းပြထားပါတယ်။ Analog Signal, Digital Signal နဲ့ကွာခြားပုံကို သိသာထင်ရှားစွာတွေ့ရမှာပါ။ Analog ကတော့ မတူညီတဲ့အမျိုးမျိုးသောတန်ဖိုးတွေနဲ့ ပြောင်းလဲသွားလာနေသော်လည်း Digital ကတော့ State နှစ်ခုထဲနဲ့ပဲဖြစ်တယ်ဆိုတာကိုတွေ့ရမှာပါ။ State နည်းတယ်လို့ ပြောရမှာပေါ့။

ပုံ ၅.၅



Digital Signaling Technique အခြေခံသဘောတရား

Computer ရဲ့ Data တွေဟာ Digital ဖြစ်နေတာကြောင့် Network တာလည်း Digital Signals ကိုအသုံးပြုပါတယ်။ Digital Signal ကနေ Digital Data ကိုပြောင်းလဲတဲ့ (Encode) Modulating နဲ့ပတ်သက်တဲ့ Methods နှစ်ခုရှိပါတယ်။ အဲဒါကတော့ -

- ❖ Current State နဲ့
- ❖ State Transition တို့ဖြစ်ကြပါတယ်။

Analog Signaling Technique အခြေခံသဘောတရား

Analog Signals တွေဟာတစ်ခုမှ များစွာသောတန်ဖိုးအထိပြောင်းလဲနေတတ်ပါတယ်။ ဒီလိုပြောင်းလဲနေတဲ့အပေါ်မူတည်ပြီး Data အဖြစ် ဖြစ်လာအောင်ပြုလုပ်ပါတယ်။ Analog Waveform နှင့်ပတ်သက်လို့ပြောရရင်တော့ သူဟာ Sine Wave ပုံဖြစ်ပါတယ်။ သူ့မှာလည်း Characteristics တွေရှိပါတယ်။ အဲဒါတွေကတော့-

- ❖ Frequency နဲ့
- ❖ Amplitude တို့ဖြစ်ကြပါတယ်။

၅.၉ Bit Synchronization အကြောင်းသိကောင်းစရာ

Modulation Method များဖြစ်ကြသည့် Current State နှင့် Transition State နှစ်ခုစလုံးတွင် Signals များကိုလက်ခံမည့်ပစ္စည်းများသည် ၎င်းထံသို့ရောက်လာမည့် Signal များကိုစောင့်ကြည့်နေပါသည်။ ၎င်းနေရာတွင် Timing (တိုင်မင်)မှန်ကန်ဖို့သည် အင်မတန်အရေးကြီးပါသည်။ အဘယ်ကြောင့်ဆိုသော် လက်ခံမည့် Receiver သည်ဘယ်အချိန်တွင် Signal များရောက်ရှိလာမည်ကိုသိရှိရန် လိုအပ်သောကြောင့် ဖြစ်သည်။ ထိုသို့စစ်ဆေးရာ၌ အကယ်၍များ Timing (တိုင်မင်)များမှားခဲ့သော်၊ မှားယွင်းသော Data များကိုထုတ်ယူကောင်းယူသွားနိုင်ပါသည်။ အောက်တွင် Signal များကို Timing (တိုင်မင်)ပြုလုပ်ခြင်း Method နှစ်မျိုးကိုဖော်ပြပေးထားပါသည်။ ၎င်းတို့မှာ -

- ❖ Asynchronous Communication
- ❖ Synchronous Communication တို့ဖြစ်ကြပါသည်။

Asynchronous Communication အကြောင်းသိကောင်းစရာ

ပို့လွှတ်သူ Sender နှင့် လက်ခံရရှိသူ Receiver တို့နှစ်ခုစလုံးတွင် Internal Clocks များ ပါရှိသော်လည်း ၎င်းတို့ Clocks အချင်းချင်းတိုက်ရိုက် Synchronized များမလုပ်ထားပါ။ Message တစ်ခုချင်းစီအစတွင် Start bit ဆိုတာပါရှိပြီး ၎င်းသည် Message များ၏ Timing များကိုလက်ခံရရှိမည့် ပစ္စည်း၏ Internal Clock နှင့် Synchronized လုပ်ပေးနိုင်သည်။ Stop bit ၏သဘောတရားသည် Message ပြီးဆုံးပြီဟုဆိုလိုခြင်းဖြစ်သည်။ Asynchronized Technique ဆိုသည်မှာ တကယ်တော့ Character များကိုသာ Transmit ပြုလုပ်ခြင်းဖြစ်ပြီး ပေးပို့မည့် Message ၏တစ်စိတ်တစ်အေဖြစ်သော 7 or 8 bit ကိုသာကန့်သတ်၍ပို့လွှတ်သည်။ ထို့ကြောင့်စနစ်များအလုပ်လုပ်စေရန် ပို့လွှတ်သူနှင့် လက်ခံရရှိသူ နှစ်ခုစလုံးတို့သည် Data များကို သယ်ယူပို့ဆောင်ရာတွင် မည်သည့်နှုန်းနှင့် အလုပ်လုပ်ကြမည်ကို အထွေထွေသဘောတူညီချက်ဖြင့် သဘောတူညီထားကြရသည်။

Synchronous Communication အကြောင်းသိကောင်းစရာ

ပေးပို့သူနဲ့လက်ခံသူတို့ကို တိုင်မင်ကိုက်ညီနေဖို့ (Synchronized) Synchronous Communication ဟာ Clock ကိုအသုံးပြုရပါတော့မယ်။ ဒီလိုလုပ်ရာမှာလည်းနည်းလမ်း (၃)လမ်းရှိပါတယ်။ အဲဒါတွေကတော့ -

- ❖ Guaranteed State Change
- ❖ Separate Clock Signals

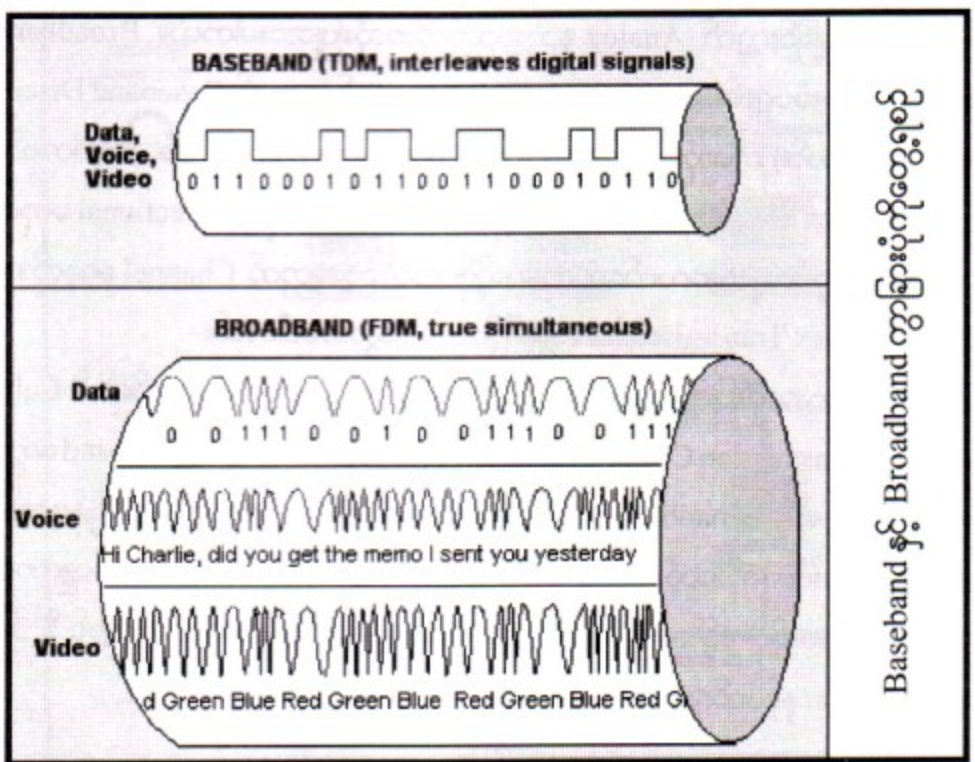
❖ Oversampling တို့ဖြစ်ကြပါတယ်။

၅.၁၀ Baseband Transmission အကြောင်းသိကောင်းစရာ

Baseband ကတော့ Communication တစ်ခုပဲရပါတယ်။ တစ်နည်းအားဖြင့်ပြောရရင်တော့ Medium ရဲ့ Data သယ်နိုင်မှုပမာဏအားလုံးကို Communication Channel တစ်ခုအပေါ် ပုံအောထားတာ ဖြစ်ပါတယ်။

Baseband Transmission ဟာ Digital Signal / Digital Encoding ကိုအသုံးပြုပါတယ်။ Frequency တွေဟာ Fixed ဖြစ်ပါတယ်။ တရားသေပေါ့။ Signals တွေကတော့ Electricity ဖြစ်ချင်လည်းဖြစ်မယ်။ Signal ရဲ့ပုံစံကတော့ (ပြတ်တောင်းပြတ်တောင်း) Discrete Pulse လို့ဆိုပါတယ်။ Baseband ဟာ Communication Channel တစ်ခုကိုပဲအသုံးပြုနေပါတယ်။ Signal တွေကို ၎င်း Channel တစ်ခုတည်းမှာပဲ Baseband ကိုအပြည့် ပုံအောအသုံးပြုပါတယ်။ ဆိုလိုချင်တာက ဆက်သွယ်ဖို့အတွက်ပစ္စည်းတွေဟာ ဘယ်လောက်ပဲ Baseband Cable ကို လာတပ် လာတပ် Baseband System ဟာ Channel တစ်ခုသာလျှင် အသုံးပြုလို့ရတယ်လို့ ဆိုလိုတာဖြစ်ပါတယ်။ Baseband Transmission ဟာအကယ်၍များ Cable တစ်ကြိုးတည်းကိုသာအသုံးပြုမယ်ဆိုရင် Half Duplex Transmission ပဲရပါတယ်။ အကယ်၍ Baseband ကို Full Duplex Transmission နှင့် အသုံးပြုချင်တယ်ဆိုရင် ပစ္စည်းတစ်ခုချင်းစီမှာ Network အတွက် Cable နှစ်ကြိုး Interfure နှစ်ခုအသုံးပြုရမှာဖြစ်ပါတယ်။ ဒါမှတစ်ခုကို Data Sending အတွက်အသုံးပြုပြီး နောက်တစ်ခုကို Data Receiving အတွက်အသုံးပြုပါတယ်။

ပုံ ၅.၆



Network Cable တစ်လျှောက်မှာ Signal တွေသယ်လာကြတဲ့အခါ Transmit စဖြစ်တဲ့နေရာနှင့် ပိုပြီးတော့ဝေးလာလေ Signal ဟာအားပျော့လာလေဖြစ်ပါတယ်။ အဲ့ဒီအပြင် Transmitter နှင့်ဝေးလာလေ Distortion ဝင်လာလေဖြစ်ပါတယ်။ ဒါကတော့ ကျွန်တော်ရှေ့မှာပြောခဲ့ပြီးသားပဲလေ။ Cable တွေမှာအများဆုံးသွားနိုင်တဲ့အလျား Maximum Segment Length ဆိုတာရှိပြီးသားလေ။ ဒီတော့ Baseband စနစ်တွေဟာလည်း Ethernet လိုပါပဲ။ Repearters လို့ခေါ်တဲ့ ပစ္စည်းနှင့် Cable Segment တွေကလာတဲ့ Signal တွေကို နောက် Cable Segment တစ်ခုစီမသွားခင် Signal အားပြန်ကောင်းလာအောင် Refresh လုပ်ပါတယ်။ ဒီလိုနည်းနဲ့ Repeater ကိုအသုံးပြုပြီး Signal တွေကိုနဂိုမူလအတိုင်း ပြန်ဖြစ်အောင်ပြုလုပ်နိုင်ပါတယ်။ Baseband Transmission Cable တစ်ကြိုးတည်းကိုပဲ Direction နှစ်ဖက်သွား Bi-Directional ကိုအသုံးပြုပြီး Transmission ရောလက်ခံခြင်း Reception ကိုပါလုပ်ဆောင်ပါတယ်။

၅.၁၁ Broadband Transmission အကြောင်းသိကောင်းစရာ

Medium ဟာ သူရဲ့ Data သယ်နိုင်မှုပမာဏကို နှစ်ခုဒါမှမဟုတ်နှစ်ခုထက်ပိုတဲ့ Communication Channel တွေကို Share လုပ်ပေးနိုင်တာကတော့ Broadband ပဲဖြစ်ပါတယ်။

Broadband Transmission ကတော့ Cable တွေကိုအသုံးပြုပြီး အချက်အလက်တွေကိုပေးပို့ရာမှာ Baseband နှင့်မတူတဲ့ Transmission နည်းကိုအသုံးပြုပါတယ်။ (မှန်လိုက်တာ)။ ဒီလိုပါ Broadband စနစ်ဟာ Baseband လို Digital Pulse မဟုတ်တဲ့ Analog နည်းပညာကိုအသုံးပြုပါတယ်။ ဆိုလိုတာက Broadband ဟာအချက်အလက်တွေကို Encode လုပ်တယ်ဆိုတဲ့နေရာမှာ Baseband မှာလို Binary ပုံစံ 0 နှင့် 1 ကိုအသုံးပြုခြင်းထက် Analog နည်းပညာကိုအသုံးပြုထားပါတယ်။ Broadband Signals တွေဟာ အသုံးပြုရာကြားခံပစ္စည်း (ဥပမာ Cable) Medium တစ်လျှောက် Baseband Discrete Signal လို (ပြတ်တောင်းပြတ်တောင်း) ကိုမသုံးဘဲ တရစပ်ဖြစ်တဲ့ Continuous Signal ကိုအသုံးပြုပါတယ်။ နောက်ပြီးတော့ ကွာခြားသေးတာက Broadband Signal တွေဟာ Baseband လို Bidirectional မဟုတ်ဘဲ One-Way ဖြစ်ပါတယ်။ ဒီတော့ အချက်အလက်တွေကိုပေးပို့ဖို့ လက်ခံဖို့အတွက် Channel နှစ်ခုလိုအပ် ပါတယ်။ ဒါဟာလည်း Full-Duplex Transmission အတွက်ပိုကောင်းသွားစေပါတယ်။

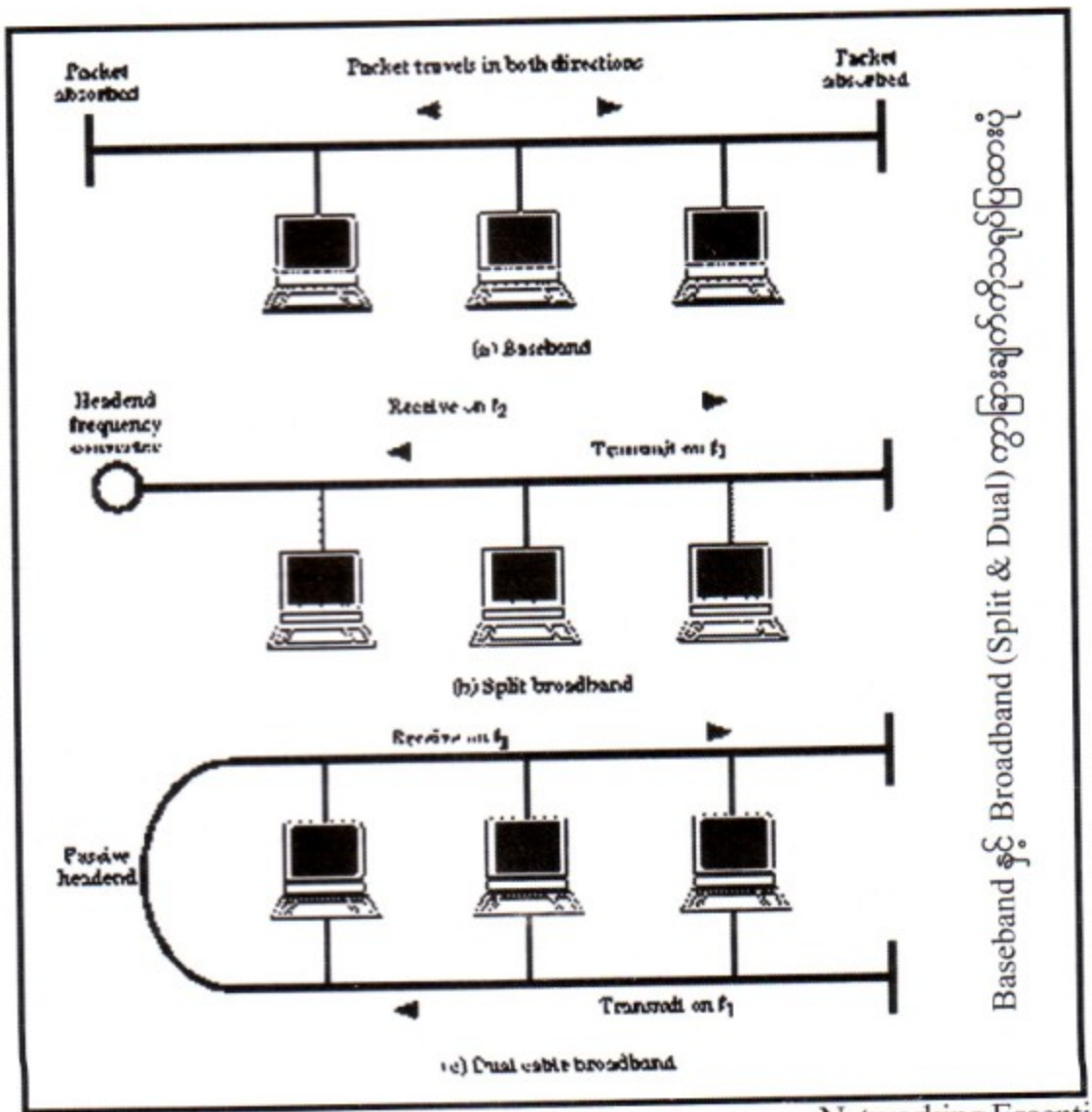
Broadband မှာအသုံးပြုတဲ့ Cable ဟာ Bandwidth သာတောင်းခံမယ်ဆိုရင် ဒီ Cable တစ်ကြိုးတည်းမှာပဲ Analog Transmission Channels အများကြီးအလုပ်လုပ်နိုင်ပါတယ်။ Baseband တွေလို Analog Signal တွေကိုမသုံးထားတဲ့ Broadband ဟာအားပျော့လာတဲ့ Signal တွေကို အားပြန်ကောင်းလာစေဖို့ Baseband လို Repeaters ကိုအသုံးမပြုဘဲ Amplifiers ကိုအသုံးပြုပါတယ်။ ကွန်ပျူတာတစ်လုံးဟာ အချက်အလက်တွေကိုပေးပို့ဖို့ နှင့် လက်ခံဖို့အတွက် Channels နှစ်ခုလိုအပ်တာကြောင့် ဒီ 2-Way Network Communication နှင့်ပတ်သက်လို့ပြောပြစရာ အကြောင်းနှစ်ခုရှိလာပါတယ်။

(၁) တစ်ခုက ကြိုးတစ်ခုတည်းကို အသုံးပြုပြီး Bandwidth ကို Channels နှစ်ခုခွဲထုတ်လိုက်ပါတယ်။ Channels တစ်ခုက Transmit လုပ်နေတဲ့အခါ နောက် Channels တစ်ခုက Received လုပ်ပါတယ်။ Channels တစ်ခုစီမှာမတူညီတဲ့ Frequency နဲ့ပေါ့။

(၂) နောက်တစ်ခုက Cable နှစ်ကြိုးကိုအသုံးပြုထားတဲ့ Dual Cable Broadband ကိုအသုံးပြုမယ်ဆိုရင် ကွန်ပျူတာဖြစ်စေ၊ ကွန်ရက်ဆက်စပ်ပစ္စည်းဖြစ်စေ ၎င်းကြိုးနှစ်ခုစလုံးကို တစ်ပြိုင်တည်းတပ်ထားရမှာဖြစ်ပါတယ်။ တစ်ကြိုးက Transmit လုပ်ပြီးတစ်ကြိုးက Received လုပ်မှာဖြစ်ပါတယ်။

ပုံမှန်အတိုင်းဆိုရင်တော့ Broadband ဟာ Baseband ထက် Bandwidth ပိုကြီးပါတယ်။ ဒါပေသိ အဲလေ ဒါပေမယ့် Broadband က Baseband စနစ်ထက်စာရင်ငွေကုန်ကြေးကျ ပိုများပါတယ်။ ဘာလို့လဲဆိုတော့ Broadband က Cables Channels ပိုသုံးရတယ်။ နောက် Channel တစ်ခုချင်းစီအတွက် Amplifiers တွေပိုသုံးရတယ်။ ဒါကြောင့်ပါ။

ပုံ ၅.၇



Baseband နှင့် Broadband (Split & Dual) ကွာခြားချက်ကိုသရုပ်ပြထားပုံ

၅.၁၂ Data Link Layer ဆိုတာ

Data Link Layer ကတော့ ကွန်ပျူတာမှာ Run လုပ်နေတဲ့ Softwar နဲ့ (ကြားခံပစ္စည်း-ဥပမာ- Network Cable) တို့ နှစ်ခုအကြားဆက်သွယ်မှုကိုသတ်မှတ်ပေးပါတယ်။ အားလုံးသိကြတဲ့အတိုင်းပါပဲ၊ Data Link Layer ကတော့ OSI Model ရဲ့ ဒုတိယအလွှာပဲဖြစ်ပါတယ်။ ၎င်းဟာ Data Frame တွေကို Physical Layer အတွက် အကြမ်းထည် Bits (Raw Bits) တွေအဖြစ်ပြောင်းလဲပေးရပါတယ်။ နောက်ပြီး Framing, Flow Control, Error Control, Retransmission of Frames စသည့်လုပ်ငန်းဆောင်တာတွေ အတွက်လည်း Data Link Layer မှာတာဝန်ရှိနေပြန်ပါတယ်။ နောက်ထပ်လည်းလုပ်ငန်းဆောင်တာ တာဝန် တွေရှိပါသေးတယ်။

Local ကွန်ရက်တစ်ခုအတွင်း စတင်ရာမှ ဦးတည်ရာသို့ တိုက်ရိုက်သွားနိုင်သောလမ်းကြောင်း Direct Traffic ကိုခွင့်ပြုသည့် Packet Addressing နဲ့ မြောက်များစွာသောကွန်ပျူတာတွေဟာ Network တစ်ခုကို Conflict မဖြစ်ဘဲအတူတကွ Share လုပ်နိုင်အောင်ခွင့်ပြုတဲ့ Media Access Control တို့နဲ့ ပတ်သက်သော လုပ်ငန်းဆောင်တာများကိုလည်းလုပ်ဆောင်ရပါတယ်။ နောက်ပြီး Network တစ်ခုလုံးကို Data တွေ ပို့လွှတ်ရန် Data များကို Encapsulate လုပ်ဖို့အတွက် Data Frame တွေရဲ့ ပုံစံတွေကိုလည်း သတ်မှတ်ပေးရပါတယ်။ ပြောရမယ်ဆိုရင် ခုနက ပြောခဲ့တဲ့ Media Access Control Addresses တွေဟာ ဒီအလွှာမှာ အလုပ်လုပ်ကြပါတယ်။ နောက်ပြီး Bridge နဲ့ Network Card တို့ကလည်း ဒီ အလွှာမှာအလုပ်လုပ်ကြပါတယ်။

ရှိပါသေးတယ်။ Data Link Layer ဟာ သူ့အပေါ်မှာရှိတဲ့ Network Layer အတွက် Data များချိတ်ဆက်ပေးခြင်း နှင့် ၎င်းဖြစ်စဉ်ကိုထိန်းသိမ်းပေးခြင်းတို့ကိုလည်းလုပ်ဆောင်ရပါတယ်။ နောက်ပြီး ကွန်ရက်အတွင်းက ကွန်ပျူတာနှစ်လုံးဆီသို့ Data ပို့လွှတ်ကြရာဝယ် Data ဟာအလိုရှိရာအရပ်သို့ သေချာစွာရောက်ရှိအောင်လို့ ဆောင်ရွက်ကြပ်မတ်ရတာလည်း ဒီအလွှာရဲ့တာဝန်ပဲဖြစ်ပါတယ်။ ကျွန်တော်တို့ရဲ့ ကွန်ရက်ဟာ LAN (Local Area Network) ပဲဖြစ်ပါစေ သို့တည်းမဟုတ် WAN (Wide Area Network) ပဲဖြစ်ပါစေ သက်ဆိုင်ရာ Protocols တွေဟာ ဒီအလွှာပေါ်မှာ အလုပ်လုပ်ဆောင်ကြရပါတယ်။

Data Link Layer နဲ့ ပတ်သက်လို့ အနှစ်ချုပ်ကိုပြန်ပြောပါအုံးမယ်။

- ❖ Identifies Devices on the Network - ကွန်ရက်တွင်ရှိသော ပစ္စည်းများကိုသတ်မှတ်ခြင်း။
- ❖ Controls (& Possibly Corrects) Errors- အမှားတွေပါလာခဲ့ရင် အမှန်လုပ်ပါတယ်။ ထိန်းသိမ်းပေးပါတယ်။
- ❖ Controls Access to the Network Medium - Network Medium ကို Access လုပ်ဖို့ Controls လုပ်ပါတယ်။

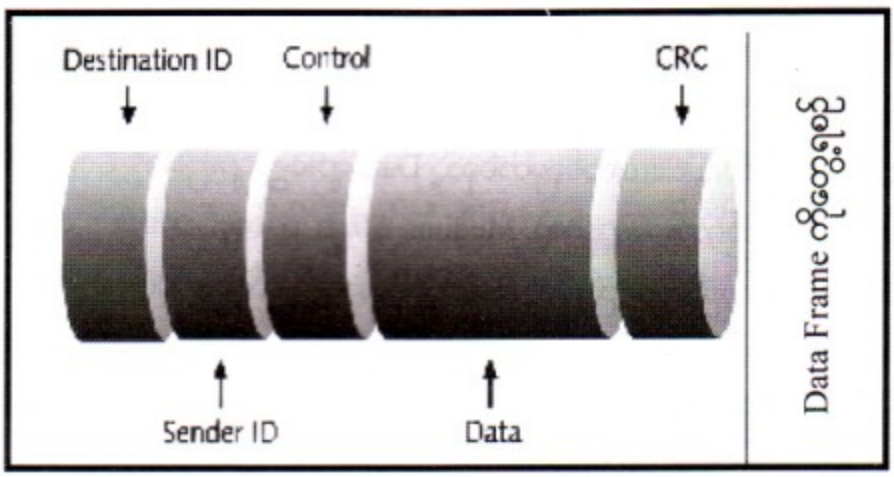
❖ Define the Logical Topology of the Network – ကွန်ရက်ရဲ့ Topology ကိုလည်းသတ်မှတ်ပေးပါတယ်။

❖ Controls Data Flow – အချက်အလက်သွားလာမှုကိုလည်းထိန်းချုပ်ပေးပါတယ်။

Data Link Layer ဟာ ၎င်းအပေါ်က Network Layer မှ Data Frame တွေကို ၎င်းအောက်ရှိ Physical Layer သို့ Transmit လုပ်ပေးပါတယ်။

Data Link Layer ဟာ ကွန်ပျူတာ တစ်လုံးကနေ နောက်တစ်လုံးကို Data များပေးပို့ရာတွင် Physical Layer ကိုဖြတ်ကျော်ကာ အမှားအယွင်းမရှိပို့ဆောင်ပေးခြင်းကိုလည်းတာဝန်ယူရပါတယ်။ ဘယ်လိုတာဝန်ယူသလဲဆိုတော့ Data Link Layer မှပေးပို့လိုက်တဲ့ Data Frame တစ်ခုကို လက်ခံရာဖက်မှ Data Link Layer ကနေ လမ်းမှာ ပြဿနာဖြစ်ခဲ့မဖြစ်ခဲ့ကို ကြည့်ပါတယ်။ ဆိုလိုသည်ကား ပို့လွှတ်လိုက်စဉ်အတွင်းမှာ Data Frame တွေဟာမပျက်စီးခဲ့ဖူးဆိုရင် ပို့လွှတ်လိုက်တဲ့ဖက်က Data Link Layer ကို ကောင်းစွာ လက်ခံရရှိပြီဖြစ်ကြောင်း ပြန်ကြားပါတယ်။ အဲ့သလိုမှ မဟုတ်ဘဲ လမ်းမှာပျက်စီးခဲ့တယ်ဆိုရင် ပို့လွှတ်တဲ့ဖက်က Data Link Layer က ပြန်၍ပို့ပေးရပါတယ်။

ပုံ ၅.၈

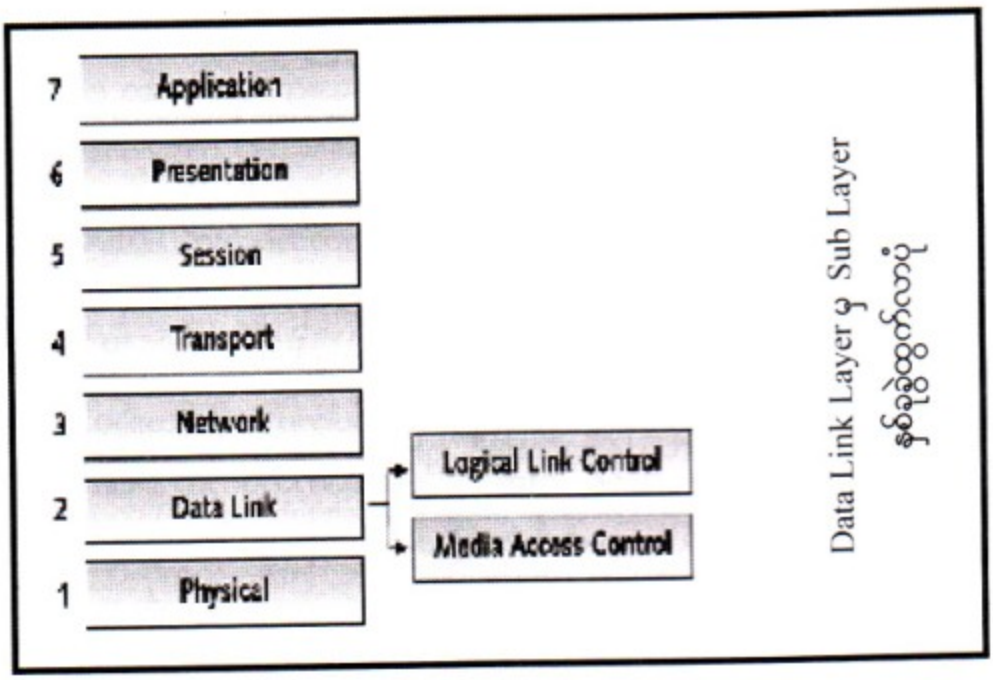


Data Link Layer ကို အပိုင်း (၂) ပိုင်းဖြင့် ခွဲခြားထားပါသေးတယ်။ တနည်းအားဖြင့်ပြောရရင် Sub Layer ပေါ့ဗျာ။ အဲ့ဒါကတော့ Logical Link Control (LLC) ဆိုတဲ့ ဆင့်ပွား Layer နဲ့ Media Access Control (MAC) ဆိုတဲ့ ဆင့်ပွား Layer တို့ပဲ ဖြစ်ကြပါတယ်။

Logical Link Control ဆိုတဲ့ ဆင့်ပွားအလွှာကတော့ ပစ္စည်းတွေနဲ့အဆက်အသွယ်ရရှိပြုလုပ်ပေးရခြင်းနှင့်ထိန်းသိမ်းပေးရခြင်းတို့ကိုပြုလုပ်ပေးရပါတယ်။ နောက်ပြီး Node တစ်ခုနှင့်တစ်ခုကြား Error Checking လည်းပြုလုပ်ပေးရပါတယ်။ Data Frame တွေကိုလည်း Synchronize လုပ်ပေးရပါတယ်။ ၎င်း Frame များစီးဆင်းမှုကိုလည်းထိန်းချုပ်ပေးရပါတယ်။ Flow Control လုပ်ပေးရတာကိုပြောတာပါ။

နောက်ပြီး MAC Sub Layer နဲ့ Network Layer အကြား Interface လုပ်ပေးပါတယ်။

ပုံ ၅.၉



Media Access Control (MAC) ဆိုတဲ့ဆင့်ပွားအလွှာကတော့ Logical Link Control အောက်ကအလွှာဖြစ်ပါတယ်။ သူကတော့ Station သည် Medium မှ Data များကိုလှမ်းယူခြင်း Access ကိုပံ့ပိုးပေးပါသည်။ တနည်းအားဖြင့် Network Card တစ်ခုမှတစ်ခုသို့ Data များရွှေ့လျားခြင်းကို Control လုပ်ပါတယ်။ ထပ်ရှင်းပြပါဦးမယ်။ ဆိုလိုသည်ကား မတူညီတဲ့ Medium ပေါ်မှာ တစ်နည်းအားဖြင့် တစ်ခုတည်းသော Medium ပေါ်မှ အမျိုးအစားမတူညီတဲ့ပစ္စည်းတွေအသုံးပြုလို့ရအောင် ထိန်းချုပ်ပေးတာဖြစ်ပါတယ်။

Media Access Control နဲ့ပတ်သတ်ပြီးထပ်ပြောပြချင်တာက ဘယ် Medium မဆိုပါ။ တစ်ကြိမ်မှာ Signal တစ်ခုပဲသွားလာဖို့တတ်နိုင်ပါတယ်။ အကယ်၍များ ကွန်ပျူတာနှစ်လုံးဟာ တစ်ကြိမ်ထဲမှာပဲ Signal တွေပို့လွှတ်လိုက်ရင် Signal တွေဟာလမ်းမှာပင်ပျောက်ဆုံးသွားတတ်ကြပါတယ်။ ဒီတော့ Media Access Control ဆိုတာ အဲ့ဒီလိုမဖြစ်အောင် Medium ကို Access လုပ်ခိုင်း Control လုပ်ပေးရတာပါ။

Data Link Layer အတွက်နိုင်ုံးချုပ်ထပ်မံ၍စုစည်းပြီးတင်ပြလိုတာက Local Area Network အတွက် Data Link Protocols တွေဖြစ်ကြတဲ့ IEEE 802.3 ကတော့ Baseband Ethernet Network တွေအတွက် CSMA/CD လို့ခေါ်တဲ့ Carrier Sense Multiple Access with Collision Detection ဆိုတဲ့ Access Method ကိုပံ့ပိုးပေးပါတယ်။ နောက်တစ်ခုက Baseband Token Ring Network အတွက် IEEE 802.5 သူကတော့ ၎င်း Token Ring Network တွေအတွက် Passing Access Method တွေကိုပံ့ပိုးပေးပါတယ်။

Wide Area Network အတွက် Data Link Layer Protocol အကြောင်းပြောပြပါအုံးမယ်။

Data Link Layer Protocol တာ LAN Traffic လမ်းကြောင်းတွေကို WAN အဖြစ်ပို့လွှတ်ဖို့အတွက် Frame တွေအဖြစ်ပြုလုပ်ပေးရပါတယ်။ WAN Transmission ပြုလုပ်ဖို့အတွက် LAN Traffic တွေကို Encapsulate လုပ်ပြီး Frame အဖြစ်ပြောင်းလဲပေးရတဲ့ Data Link Mehtod တွေအထဲက ဘုံ သုံးဖြစ်ကြတဲ့ Method တွေကိုပြောပြရမယ်ဆိုရင်-

Point to Point Technologies မှာဆိုရင် (PPP) လို့ခေါ်တဲ့ Point to Point Protocol နှင့် (HDLC) လို့ခေါ်တဲ့ High Level Data Link Control Protocol တို့ပဲဖြစ်ကြပါတယ်။

Multipoint Technologies အရဆိုရင် Frame Relay, ATM လို့ခေါ်တဲ့ Asynchronous Transfer Mode, (SMDS) လို့ခေါ်တဲ့ Switched Multi Megabit Data Services နဲ့ X.25 တို့ဖြစ်ကြပါတယ်။

ကျွန်ုပ်၏အတွေ့အကြုံ

ကျွန်တော် Bank တစ်ခုမှာ Network ဆင်ပြီး ၎င်း Bank ကို Maintenance Contract ယူစဉ် ကာလတွင်းက ရန်ကုန်ဘဏ်ကနေ နယ်ဘဏ်ခွဲကိုအချက်အလက်တွေပေးပို့ခြင်း (သို့မဟုတ်) နယ်ဘဏ်ခွဲကနေ ရန်ကုန်ဘဏ်ကိုအချက်အလက်များပေးပို့ခြင်းကို သူတို့ကလုပ်ဆောင်လိုပါတယ်။ ဆိုလိုချင်တာက နယ်ဘဏ်ခွဲက သတ်မှတ်ထားတဲ့ကွန်ပျူတာတစ်လုံးကနေပို့ချင်တဲ့ဖိုင်တစ်ခုကို ရန်ကုန်ဘဏ်ဆီ သတ်မှတ်ထားတဲ့ ကွန်ပျူတာတစ်လုံး၏အခန်းထဲသို့ပေးပို့လိုက်တာပဲဖြစ်ပါတယ်။ ဒီလိုသတ်မှတ်ထားတဲ့ ကွန်ပျူတာနှစ်လုံး တည်းတိုက်ရိုက်ဆက်သွယ်ထားတာဟာ Point to Point Connection ဖြစ်ပါတယ်။ ရည်ရွယ်ချက်ကလည်း ကွန်ပျူတာအများကြီးချိတ်စရာမလိုဘဲ လိုအပ်တဲ့ File ကိုသာ သက်ဆိုင်ရာကွန်ပျူတာကို Telephone လိုင်းမှတဆင့် Modem ခံကာ သက်ဆိုင်ရာခွဲပြုချက်ရယူပြီး Point to Point ချိတ်ပေးရုံဖြစ်ပါတယ်။ ဒီအချိန်မှာ (PPP) ဆိုတဲ့ Point to Point Protocol ကိုသုံးတာဖြစ်ပါတယ်။ ၎င်းဖြစ်စဉ်ပြုလုပ်ဖို့အတွက် အထူးထူး အပြားပြားသော Software တွေမလိုအပ်ပါဘူး။ သက်ဆိုင်ရာကွန်ပျူတာတွေမှာရှိတဲ့ Windows Operating System တွေနဲ့ပင် ၎င်းဝန်ဆောင်မှုကိုရရှိမှာဖြစ်ပါတယ်။ တကယ်တော့ (PPP) ဆိုတဲ့ Point to Point Protocol တာနောက်ကွယ်ကပါ။ ကျွန်တော်တို့က ဘောင်မှာပြထားတဲ့အတိုင်း Incoming Connection နှင့် Receiving Connection ပဲလုပ်လိုက်တာပါ။ သူကသူ့ဘာသာသူ (PPP) ကိုအသုံးပြုသွားတာဖြစ်ပါတယ်။

သူ့ကိုလုပ်ချင်ရင်တော့ -

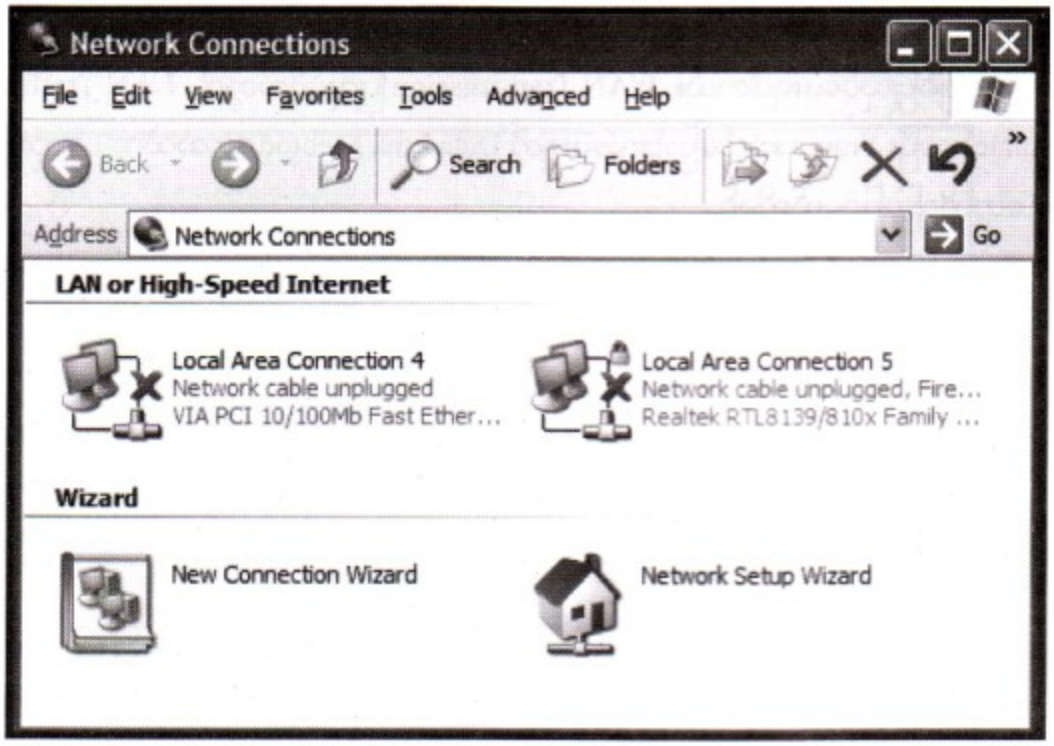
(၁) My Network Places မှာ Right Click နှိပ်ပြီး Properties လို့ပြောပါ။ ပုံ ၅.၁၀ ပေါ်လာပါလိမ့်မယ်။

(၂) New Connection Wizard ကိုရွေးပါ။ Box ပေါ်လာရင် Next လို့ပြောပါ။

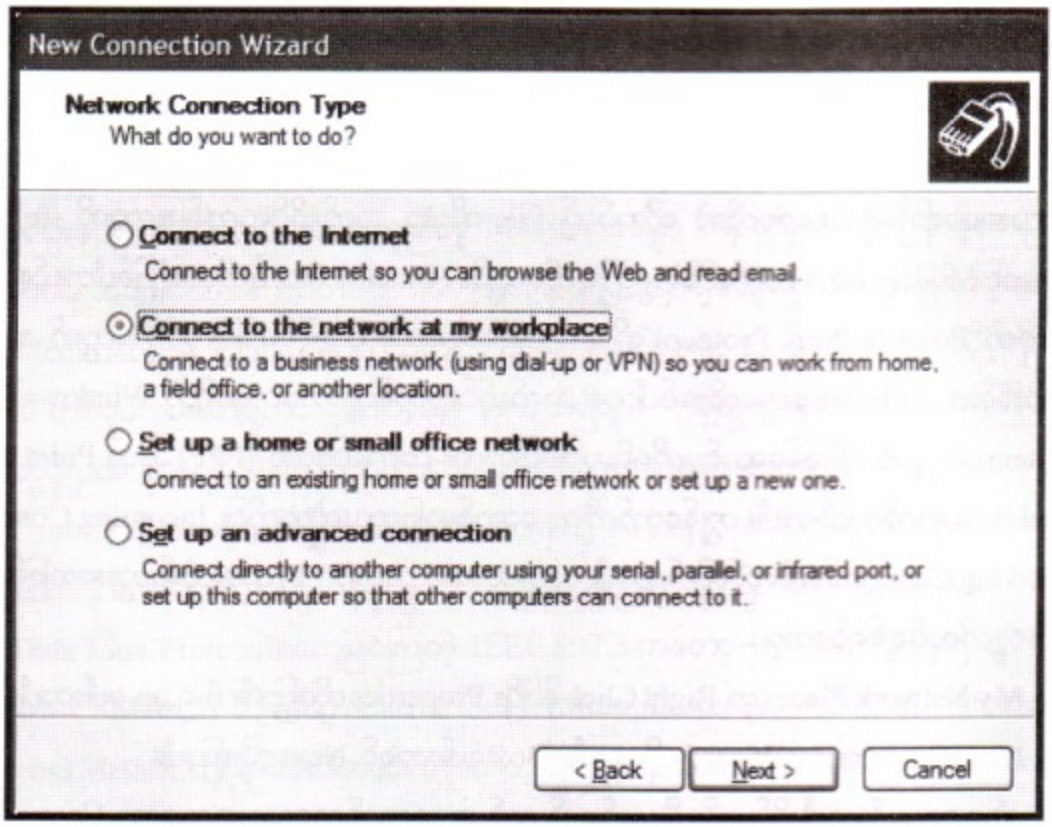
(၃) ပုံ ၅.၁၁ ပေါ်လာပါလိမ့်မယ်။ ပို့လွှတ်မယ့် ကွန်ပျူတာဘက်ကရွေးရမှာကတော့ Connect to the Network at my Workplace ဖြစ်ပါတယ်။ ရွေးပြီးရင် Next လို့ပြောပါ။ ပုံ ၅.၁၂ ပေါ်လာပါလိမ့်မယ်။

(၄) အဲ့ဒီမှာ Dial-up Connection ကိုရွေးရမှာဖြစ်ပါတယ်။ ပြီးရင် Next လို့ပြောပါ။

ပုံ ၅.၁၀



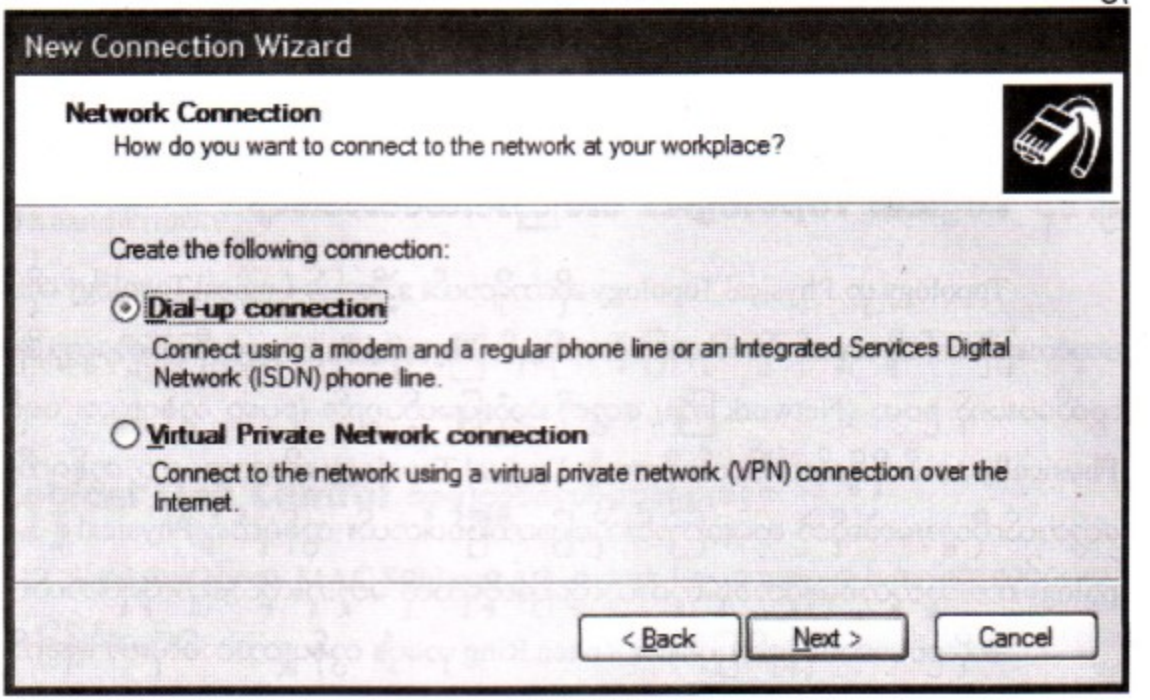
ပုံ ၅.၁၁



(၅) ပေါ်လာသည့် Box တွင် ကိုယ်စားပြု နာမည်တစ်ခု ရိုက်ထည့်ပေးပါ။ Next လို့ပြောပါ။

(၆) ပေါ်လာသည့် Box တွင် ကိုယ်ဆက်သွယ်မည့် ဖုန်းနံပါတ် ကိုရိုက်ထည့်ပါ။ Next လို့ပြောပါ။

ပုံ ၅.၁၂



(၇) ပေါ်လာသည့် Box တွင် Finish လို့ပြောပါ။ ဒီဆို ဆက်သွယ်မည့်တစ်ခြမ်း (One Sided) ပြီးသွားပါပြီ။

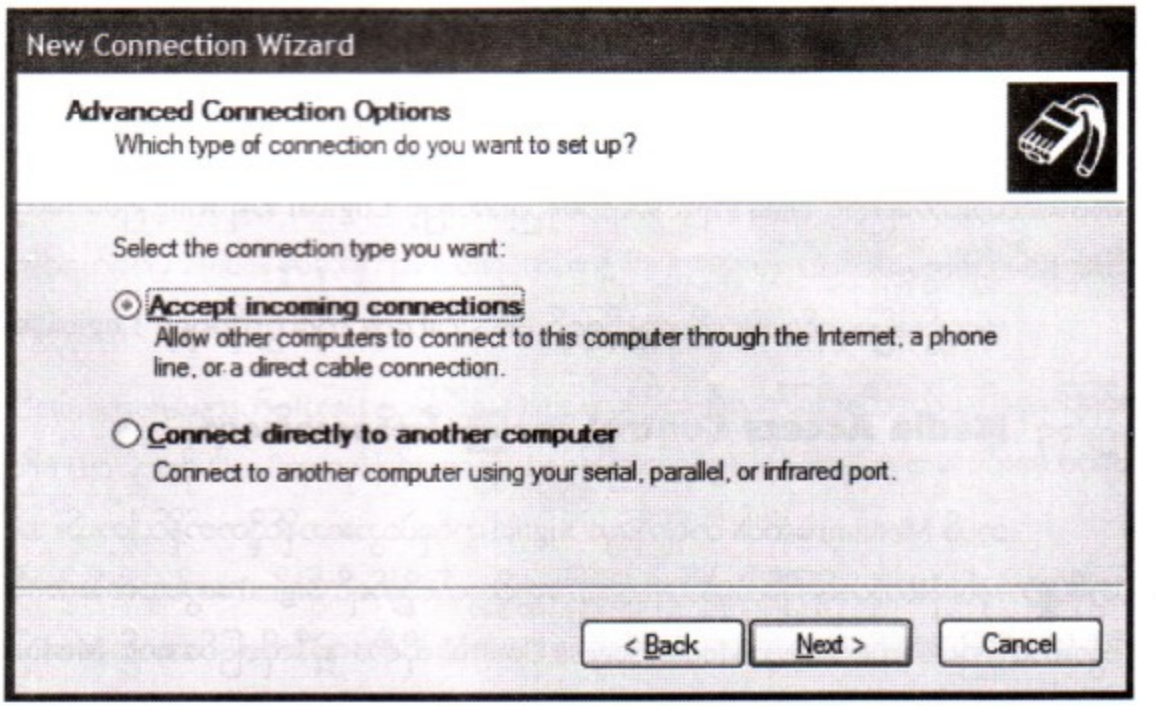
(၈) ဒီတစ်ခါ လက်ခံတဲ့ကွန်ပျူတာဖက်က လုပ်ရမည့်အဆင့်ကိုဖော်ပြပေးပါ့မယ်။ ပုံ ၅.၁၁ အထိပြန်လာပါ။

(၉) ၎င်းတွင် Setup an Advanced Connection ကိုရွေးပါ။ ပြီးရင် Next လို့ပြောပါ။

(၁၀) ပုံ ၅.၁၃ ပေါ်လာလိမ့်မည်။ Accept Incoming Connection ကိုရွေးပါ။ ပြီးရင် Next လို့ပြောပါ။

(၁၁) ဖုန်းလိုင်းနှင့်ချိတ်တာဖြစ်ပြီးလိုအပ်သလိုဆက်ပြောသွားက ပြီးသွားပါပြီ။

ပုံ ၅.၁၃



(၁၂) နှစ်ဖက်ချိတ်ထားပြီးဖြစ်သော်လည်း တစ်ဖက်ကပဲ အခြားတစ်ဖက်က ဖွင့်ထားသောလက်ခံကွန်ပျူတာထဲသို့ချိတ်ဆက်ပြီး ဖိုင်ပို့ခြင်း၊ ရယူခြင်းကိစ္စများပြုလုပ်လို့ရသွားပါပြီ။

၅.၁၃ Logical Topologies အကြောင်းသိကောင်းစရာ

Topology မှာ Physical Topology ဆိုတာရှိတယ်။ အဲဒီအပြင် Logical Topology ကိုပါနောက်ပိုင်းလေ့လာရအုံးမယ်လို့ ရှေ့သင်ခန်းစာမှာပြောခဲ့တယ်နော်။ Physical Topology ဆိုတာကတော့ ဒီကြားခံဆက်သွယ်ပေးမယ့် ဥပမာ (Network ကြိုး) တွေကိုအသုံးပြုမယ့်ပစ္စည်း (ဥပမာ ကွန်ပျူတာ၊ ပရင်တာ) တို့နဲ့ Physically ဘယ်လိုချိတ်ဆက်မယ်ဆိုတာပါ။ Logical Topology ဆိုတာကတော့ ကွန်ရက်မှာ Signal တွေဘယ်လိုသွားမလဲဆိုတဲ့ လမ်းကြောင်းကိုပြောတာဖြစ်ပါတယ်။ ကွန်ရက်ရဲ့ Physical နဲ့ Logical Topology ဟာ သူတို့တစ်ခုနှင့်တစ်ခု တူတယ်လို့ပြောလို့ရသလို မတူဘူးလို့လဲပြောလို့ရပါတယ်။

အဲကို ဥပမာတစ်ခုနဲ့ရှင်းပြပါ့မယ်။ Token Ring မှာပေါ့။ ကွန်ပျူတာတစ်လုံးက နောက်ကွန်ပျူတာတစ်လုံးဆီကို Signal တွေကိုပို့လွှတ်လိုက်ပါတယ်။ အဲကိုခုနက ပို့လိုက်တဲ့ကွန်ပျူတာရဲ့ နောက်ကွန်ပျူတာဆီက Receiver ကလက်ခံရယူပါတယ်။ ပြီးတော့ သူကနေတစ်ခါ Transmit ပြန်လုပ်ပြီးနောက်တစ်လုံးက Receive ပြန်လုပ်ပါတယ်။ ဒီလိုနဲ့တစ်ပတ်ပြန်လည်သွားမှာဖြစ်ပါတယ်။ ပြောရရင်တော့ တစ်ပတ်လည်တယ်ဆိုကတည်းက အဲ Circle ပေါ့။ Ring ပေါ့။ အဲကြောင့် Ring Topology လို့ပြောတာ။ ခုနကပြောခဲ့တယ်မဟုတ်လား။ Logical Topology ဆိုတာကွန်ရက်မှာ Signal တွေဘယ်လို Flow ဖြစ်စေသလဲဆိုတာလေ။ အခု Signal တွေကို Ring လိုတစ်ပတ်လည်စေတဲ့ Flow နဲ့လမ်းကြောင်းပေးထားပါတယ်။ အဲကြောင့် အဲကို Logical Ring Topology လို့ပြောရမှာဖြစ်ပါတယ်။

Token Ring လို့သာပြောတာ တကယ့် Wire ကြိုးတွေကိုဆင်တဲ့အခါမှာ မျက်စိထဲမြင်သလို စက်ဝိုင်းပုံစံဆင်ရတာမဟုတ်ပါဘူး။ Hub ကိုအသုံးပြုရမှာပါ။ ကွန်ပျူတာတွေကို Hub ဆီ Join ရမှာဖြစ်ပါတယ်။ ဆိုလိုချင်တာက တကယ်ဆင်လိုက်တဲ့အခါကြတော့ ကွန်ပျူတာတစ်လုံးချင်းစီက Hub ကိုသီးခြားကြိုးတွေနဲ့ တပ်ဆင်ထားတာကြောင့် Data Flow အရတစ်နည်းအားဖြင့် Logical အရ Ring ဖြစ်ပေမယ့် Physical အရ Star ဖြစ်သွားပါတယ်။

အကျဉ်းပြောရရင်တော့ ထိတွေ့လို့ရရင် Physical ပေါ့။ ထိတွေ့လို့မရရင် Logical ပေါ့။

၅.၁၄ Media Access Control အကြောင်းသိကောင်းစရာ

ဘယ် Medium မဆိုပါ။ တစ်ကြိမ်မှာ Signal တစ်ခုပဲသွားလာနိုင်ဖို့တော်နိုင်ပါတယ်။ အကယ်၍များကွန်ပျူတာနှစ်လုံးဟာတစ်ကြိမ်ထဲမှာပဲ Singanl တွေပို့လွှတ်လိုက်ရင် Signal တွေဟာလမ်းမှာပင်ပျောက်ဆုံးသွားတတ်ကြပါတယ်။ ဒီတော့ Media Access Control ဆိုတာ အဲ့ဒီလိုမဖြစ်အောင် Medium ကို Ac-

cess လုပ်တိုင်း Control လုပ်ပေးတဲ့ဖြစ်စဉ်ပါ။ အဲဒီလို Media Access Control လုပ်ရာမှာ အဆင့်(၃)ဆင့် ရှိပါတယ်။ အဲဒါကတွေကတော့ -

- ❖ Contention
- ❖ Demand Priority
- ❖ Token Ring
- ❖ Polling တို့ဖြစ်ကြပါတယ်။ ၎င်းတို့အကြောင်းကို သင်ခန်းစာ ၆ တွင် အသေးစိတ်ဖော်ပြပေးထားပါတယ်။

၅.၁၅ Logical Link Control အကြောင်းသိကောင်းစရာ

LLC Sublayer ဆိုတာ MAC Sublayer နဲ့ Network Layer အကြား Interface လုပ်ပေးတဲ့ Sub Layer ဖြစ်ပါတယ်။

မှတ်ချက် ။ ။ Data Link Layer တွင်အလုပ်လုပ်သောအဓိက Devices နှစ်ခုရှိပါသည်။ ၎င်းတို့မှာ Bridges, Switches တို့ဖြစ်ကြပါသည်။ သက်ဆိုင်ရာသင်ခန်းစာတွင် ၎င်းတို့အကြောင်းကိုဖော်ပြပြီး/မည်။

၅.၁၆ Network Layer ဆိုတာ

Network Layer ကတော့ မတူညီတဲ့ Network တွေပေါ်မှာရှိကြတဲ့ ကွန်ပျူတာတွေအချင်းချင်း Communications ဖြစ်စေဖို့အတွက် လိုအပ်တဲ့ Functions တွေသတ်မှတ်ပေးခြင်းကိုပံ့ပိုးပေးပါတယ်။ ၎င်းရဲ့ Function တွေအထဲက ဦးစွာအတိုချုပ်ပြောပြရမယ်ဆိုရင်-

- ❖ ကွန်ရက်ပေါ်မှာ Data Packets လေးများကို လမ်းကြောင်းလွှဲခြင်း (Routing) နှင့် Logical Addressing တာဝန်
- ❖ ကွန်ရက်ပေါ်မှ Nodes နှစ်ခုအကြား Connection နဲ့ Path တွေကိုဖြစ်ပေါ်စေခြင်းနှင့်ဖြုတ်ချခြင်းဆိုသည့်တာဝန်
- ❖ Connections များကို Reset လုပ်ခြင်း၊ Data များကိုထုတ်လွှတ်ခြင်းနှင့်သယ်ယူပို့ဆောင်ခြင်း၊ ရရှိလာသည့် Data များကို Confirm လုပ်ခြင်းစသည့် တာဝန်များကိုင်း Network Layer မှထမ်းဆောင်ရပါတယ်။

ဒီတစ်ခါ အချက်အလက်လိုက်မပြောဘဲ စကားပြေပုံစံပြန်ရှင်းပြပါအုံးမယ်။ Network အလွှာဆိုတဲ့ (3) လွှာမြောက်အလွှာဟာ Signal များကို Addressing ဆိုတဲ့လိပ်စာသတ်မှတ်ပေးခြင်း၊ Physical Ad-

dress များသတ်မှတ်ပေးခြင်း၊ Logical Address များကိုသတ်မှတ်ပေးခြင်းတို့ကိုလုပ်ဆောင်ရပါတယ်။ နောက်ပြီး Layer ဟာ ဖြစ်တည်ရာကနေ ဦးတည်ရာ Computer ဆီသွားရာလမ်းကြောင်း (Routing) ကိုလည်းသတ်မှတ်ပေးပါတယ်။

Network တွင်းလမ်းကြောင်းကျပ်တည်းမှု၊ ပိတ်ဆို့မှုစတဲ့ Traffic ပြဿနာတွေကိုလည်း ၎င်း Network Layer မှ Manage လုပ်ပါတယ်။ ဆိုလိုတာက Packet Sequencing ပါ။ ပေးပို့သူနဲ့ လက်ခံသူ ကြား Error Detection ပြုလုပ်ခြင်း၊ Congestion ဆိုသည့်လမ်းကြောင်းကျပ်တည်းမှုကိုထိန်းချုပ်ခြင်းတို့ကို လုပ်ဆောင်ကြရပါတယ်။ ဥပမာပြောရရင် မတူညီတဲ့ Network Medium ပေါ်မှာ ကွန်ပျူတာတစ်လုံးကပို့ လိုက်တဲ့ Data ပမာဏဟာကြီးနေလို့ပို့မနိုင်ဘူးဆိုရင် ဒီ Network Layer ဟာ ၎င်း Data ကိုအပိုင်းငယ်လေး အဖြစ်ပြုလုပ်ပြီးပို့လွှတ်လိုက်ပါတယ်။ တိုတက်ကိုရောက်တဲ့အခါ Network Layer က ၎င်းအပိုင်းငယ်ကလေး တွေကိုပြန်ပေါင်းလိုက်ပါတယ်။

TCP/IP Protocol ကိုအခြေပြုထားတဲ့ ကွန်ရက်တွေဆိုရင် IP Address, Network Address တွေနဲ့ IP Routers တွေဟာ ၎င်း Network Layer မှာအလုပ်လုပ်ဆောင်ကြပါတယ်။

၅.၁၃ OSI Network Layer အကြောင်းသိကောင်းစရာ

OSI Model ရဲ့တတိယအလွှာဖြစ်တဲ့ Network Layer ဟာ Data Packet လေးတွေဟာသက်ဆိုင်ရာ Destination ကိုမှန်ကန်စွာရောက်သွားစေဖို့ Guide လုပ်ပေးပါတယ်။

ဒီအလွှာနဲ့ပတ်သက်နေတဲ့အကြောင်းအရာနှစ်ခုကတော့ -

- ❖ Logical Network Addressing
- ❖ Routing တို့ဖြစ်ကြပါတယ်။

၅.၁၈ Addressing အကြောင်းသိကောင်းစရာ

ကွန်ရက်မှာချိတ်ဆက်ထားတဲ့ ပစ္စည်းတစ်ခုချင်းစီတိုင်းမှာ မတူညီတဲ့ Physical Device Address တွေသတ်မှတ်ပြီးသားရှိကြပါတယ်။ ဒီအလွှာဟာ Address Types နှစ်မျိုးကိုအသုံးပြုပါတယ်။ အဲဒါတွေကတော့ ❖ Logical Network Address နဲ့

❖ Services Address တို့ဖြစ်ကြပါတယ်။

Logical Network Address အကြောင်းသိကောင်းစရာ

Internetwork အတွင်းမှာရှိတဲ့ ကွန်ရက်တွေဆီကို Data Packet လေးတွေ လမ်းလွဲလမ်းညွှန်လုပ်တဲ့နေရာမှာသုံးပါတယ်။ ပြောခဲ့ပြီးခဲ့တဲ့အတိုင်းပါပဲ ကွန်ရက်ထဲကပစ္စည်းတိုင်းမှာ Address တွေရှိကြ

ပါတယ်။ (MAC Address) ပေါ့။ စက်ရုံမှာကတည်းကပစ္စည်းတွေကိုသူတို့ရဲ့ သက်ဆိုင်ရာ Protocol အပေါ်မူတည်ပဲ Address ပေးခဲ့တာပါ။ ဒါပေမယ့် ကွန်ရက်တွေဟာ ကိုယ့်ကိုယ်ပိုင် Address ပေးသောစနစ်ကိုကျင့်သုံးတဲ့ Protocol ကိုအသုံးပြုပြီး ဆက်သွယ်ကြပါတယ်။ အကယ်၍များ Data Link Layer Physical Address ဟာ MAC Address ဖြစ်ခဲ့မယ်ဆိုရင် ခုနကပြောခဲ့တဲ့ ကိုယ်ပိုင် Address ပေးတဲ့စနစ်ကိုကျင့်သုံးတယ်ဆိုတဲ့ Address ဟာ Network Layer မှာသတ်မှတ်ပေးတဲ့ Logical Address ဖြစ်သွားပါတယ်။ Logical Network Address တိုင်းဟာ Protocol ပေါ်မှီခိုပါတယ်။ မူတည်ပါတယ်။ ခုနကပြောခဲ့တဲ့ စက်ရုံမှာ သတ်မှတ်တဲ့ Address ဟာ Protocol ပေါ်မမှီခိုပါဘူး။ ဥပမာပြောရရင် TCP/IP Address ဟာ IPX Address နဲ့မတူနိုင်ပါဘူး။ နောက်ပြီး Protocol နှစ်ခုဟာ ကွန်ပျူတာတစ်လုံးထဲမှာ Conflicts မဖြစ်ဘဲရှိနေနိုင်ပါတယ်။ မတူညီတဲ့ Stations နှစ်ခုဟာ ကွန်ရက်တစ်ခုအတွင်းမှာ မတူညီတဲ့ Protocol တစ်ခုတည်းကိုသာ အသုံးပြုမယ်ဆို Logical Network Address မတူညီကြပါဘူး။ အကယ်၍တူနေမယ်ဆိုရင် ၎င်းတို့ကို ကွန်ရက်မှာမချိတ်မိနိုင် မတွေ့ဘူးဖြစ်နေပါလိမ့်မယ်။

မှတ်ချက် ။ ။ TCP/IP ဖြစ်စေ IPX ဖြစ်စေ Network Address တိုင်းမှာ Network Portion နဲ့ Node Portion ဆိုပြီးရှိပါတယ်။ Network Portion ဆိုတာ Station ချိတ်ထားတဲ့ Network Segment နံပါတ်ပါပဲ။ Station Portion နံပါတ်ဆိုတာ ၎င်း Network Segment မှာရှိတဲ့သူများနှင့်တူခြင်းမရှိတဲ့ Station နံပါတ်ပါပဲ။ ဒီတော့က Network Address ဆိုတာ ၎င်း Portion နှစ်ခုကိုပေါင်းစည်းထားတဲ့ကွန်ရက်တစ်ခုလုံးမှာ ထပ်တူညီခြင်းမရှိတဲ့နံပါတ်ပါပဲ။

IPX Address ဟာ Network Portion အတွက် 8 Digit Hexadecimal ယူပါတယ်။ ဒီနံပါတ်ကတော့ Network Administrator ကပေးတာ ဒါမှမဟုတ် Program ကပေးတာဖြစ်ပါတယ်။ Node Portion ကတော့ Manufacturer ကသတ်မှတ်တဲ့ 12 Digit Hexadecimal MAC Address ဖြစ်ပါတယ်။ ဒီအပိုင်းနှစ်ပိုင်းကို Colon နဲ့ခွဲထားပါတယ်။ အောက်မှာဥပမာပြောထားပါတယ်။

Network Address Node Address

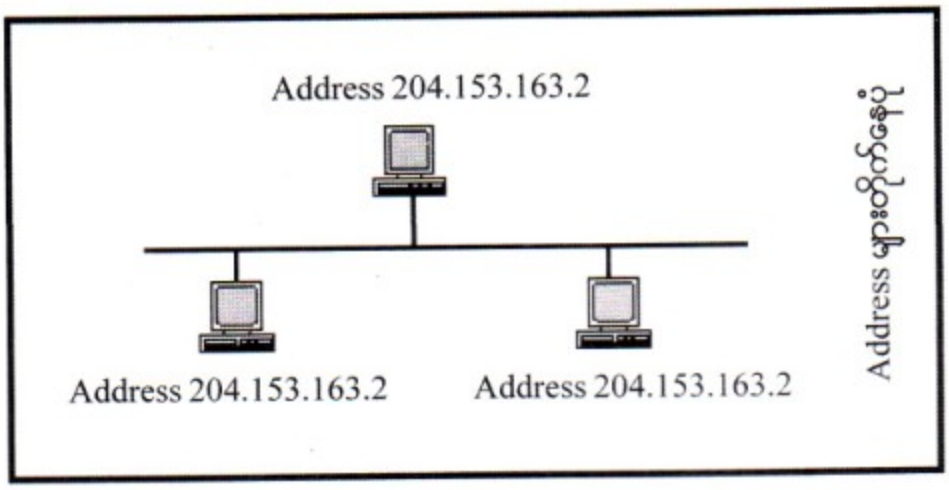
00004567:006A7C11FB56

TCP/IP Address ကတော့ Colon အစား Dot ကိုသုံးပါတယ်။ ဒီလိုပုံစံပါ။ xxx.xxx.xxx.xxx ဖြစ်ပါတယ်။

199.217.67.34 IP Address

255.255.255.0 Subnet Mask

ပုံ ၅.၁၄



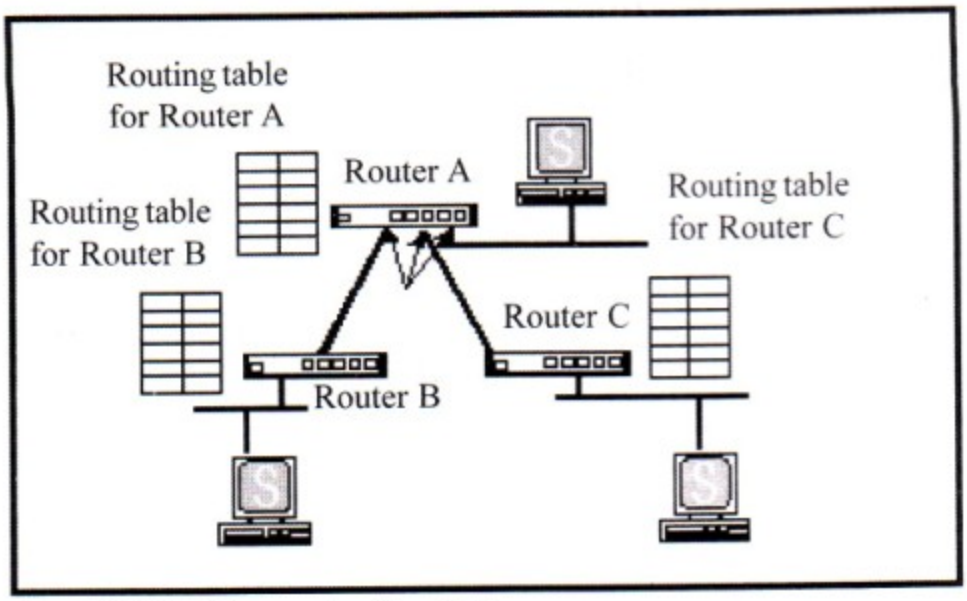
၅.၁၉ Routing အကြောင်းသိကောင်းစရာ

အချက်အလက်တွေကိုသယ်ဆောင်သွားရာမှာ ဘယ်လမ်းကြောင်းကနေသယ်သွားမလဲဆိုတာကို ရွေးချယ်လို့ရတဲ့ Routers ကိုအသုံးပြုပြီးချိတ်ဆက်ထားတဲ့ Network Segments တွေတစ်လျှောက်အချက်အလက်တွေသွားလာလှုပ်ရှားနေတဲ့ဖြစ်စဉ်ကို Routing လို့ခေါ်ပါတယ်။ ကွန်ရက်တွေမှာ Routers တွေအချင်းချင်းပြန်ချိတ်ထားခြင်းအားဖြင့် ဖြစ်ပေါ်လာတဲ့အစုကို Internetwork လို့ခေါ်ပါတယ်။ Routers ဟာလမ်းကြောင်းတွေနဲ့ပတ်သက်တဲ့အကြောင်းအရာတွေကိုတော့ Routers ရဲ့ Routing Tables ကနေရပါတယ်။

အဲဒီ Tables မှာဘာတွေပါသလဲဆိုတော့ အချက်အလက်တွေကိုသက်ဆိုင်ရာ Network Segment တွေဆီကိုပေးပို့ဖို့ အချက်အလက်တွေကိုဘယ် Router မှာထားပေးထားရမလဲဆိုတဲ့အချက်အလက်တွေရှိပါတယ်။ ဒီအချက်အလက်တွေဟာ Routing Table ကိုနည်းလမ်းနှစ်ခုဖြင့်ရရှိပါတယ်။ အဲဒါတွေကတော့

- Through Static Routing
- Through Dynamic Routing တို့ဖြစ်ကြပါတယ်။

ပုံ ၅.၁၅



၅.၂၁ Static Routing အကြောင်းသိကောင်းစရာ

Static Routing မှာ Network Administrator ဟာ Routers ရဲ့ Routing Table ကို လူကိုယ်တိုင် Updates လုပ်ရပါတယ်။ Administrator ဟာကွန်ရက်တိုင်းကို Routing Table ထဲရိုက်ထည့်ရပါတယ်။ အကယ်၍များကွန်ရက်ဟာ Segments တွေအများကြီးရှိခဲ့ရင် ဒီလိုသာလူကိုယ်တိုင်လိုက်လုပ်နေရတော့ အချိန်ကုန်တာပေါ့။ ဒါမှမဟုတ် Windows NT Server ကို Router အနေနဲ့အသုံးပြုမယ်ဆိုရင်တော့ ဒီလမ်းကြောင်းတွေနဲ့ပတ်သက်လို့ ထပ်ထည့်ခြင်း၊ ပြောင်းခြင်းနဲ့ ဖျက်ချခြင်းတို့ကို Route Command သုံးပြီးပြုလုပ်လို့ရပါတယ်။

၅.၂၁ Dynamic Routing အကြောင်းသိကောင်းစရာ

Dynamic Routing မှာ Routers ဟာ Route Discovery Protocol ဆိုတဲ့ Routing Protocol နဲ့တခြား Routers တွေကိုလှမ်းပြောပါတယ်။ ဘယ်ကွန်ရက်တွေကို ဘယ် Routers နဲ့ချိတ်ထားသလဲပေါ့။ Routers ဟာကွန်ရက်မှာရှိတဲ့တခြား Routers တွေဆီကိုအထူးအချက်အလက်များပေးပို့ပြီး Updates လုပ်ပါတယ်။ အဲ့ဒီလိုတခြား Rotuers တွေကလည်းသူတို့ဘာသူတို့ Updates လုပ်ကြပါတယ်။ ဒါကြောင့် လူကိုယ်တိုင် Updates လုပ်စရာမလိုပါဘူး။ Dynamic Routing ဟာ ဒီနေ့ခေတ်မှာရေပန်းစားနေတဲ့ Routing Technology တစ်ခုဖြစ်ပါတယ်။

Dynamic Routing မှာမှ Route Discovery Protocols နှစ်ခုပါရှိပါတယ်။ အဲ့ဒါကတော့ -

- ❖ Distance Vector Routing
- ❖ Link State Routing တို့ဖြစ်ကြပါတယ်။

Distance Vector Routing အကြောင်းသိကောင်းစရာ

Distance Vector မှာ Routers ဟာငုံးရဲ့ Routing Table ကိုတခြား Routers တွေဆီပို့လွှတ်လိုက်ပါတယ်။ အဲ့ဒီ Routing Table ကိုလက်ခံရရှိတဲ့ Routers ဟာ လမ်းကြောင်းစာရင်းမှာ တစ်ခါပတ်ပြီးတိုင်း ၁ ခါပတ်ပြီးကြောင်း ၁ ထည့်ပိုင်းပါတယ်။ ဒါကို Hop လို့ခေါ်ပါတယ်။ ဒါဟာစက္ကန့် ၆၀ တိုင်းမှာဖြစ်ပေါ်နေပါတယ်။

Link State Routing အကြောင်းသိကောင်းစရာ

Link State Routing ကြတော့ Distance Vector လို့မဟုတ်ဘဲ သူတို့ရဲ့ Routing Tables ကို ငါးမိနစ်ကြာဒါမှမဟုတ် ၅ မိနစ်တိုင်းကြမှပို့လွှတ်ပါတယ်။ နောက်ပြီးတော့ရှိပါသေးတယ်။ အဲ့ဒါက အကယ်၍များ Update လုပ်ရမယ်ဆိုရင် Update လုပ်ရတဲ့အကြောင်းကိုပဲပို့လွှတ်ပါတယ်။ ဒါကြောင့် Link State က

Distance Vector ထက်ပိုပြီး Effecient ဖြစ်ပါတယ်။

မှတ်ချက် ။ ။ဒီအလွှာမှာ အလုပ်လုပ်တဲ့ပစ္စည်းတွေကတော့ Routers, Brouter, Layer 3 Switches တို့ပဲဖြစ်ကြပါတယ်။

၅.၂၂ Transport Layer ဆိုတာ

❖ ကွန်ရက်တောက်လျှောက် ပေးပို့သူမှ လက်ခံသူဆီကို Data တွေသယ်ဆောင်သွားခြင်းကို ထိန်းချုပ်ပေးပါတယ်။ ဒါကဘိုပြီးပြောတာပါ။

❖ Data ဟာ လက်ခံရရှိပြီးတာနဲ့ ရရှိပြီးကြောင်းအသိအမှတ်ပြု Acknowledgement လုပ်ပေးရပါတယ်။ ဒါကလည်းအမှားကင်းစင်အောင်ထိန်းချုပ်တဲ့နည်းတစ်ခုပဲလေ။ ဒီလို Acknowledgement လုပ်ပေးမှ Data ရမရကိုသေချာသိပြီးမရလို့ရှင်းလည်းလိုအပ်ပါက နောက်တဖန်ပြန်ပို့နိုင်ရန် (Retransmitting Data) ဖြစ်ပါတယ်။

❖ ပို့ဆောင်ရာလမ်းမှာ Data Packet လေးတွေပြုတ်ကျမကျန်ခဲ့စေဖို့လည်း Transmission Speed ကိုထိန်းညှိပေးခြင်း (Flow Control) ကိုလည်းလုပ်ပါတယ်။ ဒီလို Flow Control လုပ်တဲ့နေရာမှာလည်း Data တွေကိုပို့လွှတ်လိုက်တဲ့ဘက်က Transmitting Device (ဥပမာ Network Card) ကဟိုဖက်က လက်ခံရာဘက်က Receiving Device လက်ခံနိုင်လောက်တဲ့ပမာဏအပဲပေးပို့စေခြင်းကိုပါထိန်းချုပ်ပေးပါတယ်။ Receiving Device ဘက်ကလက်မခံနိုင်လောက်တဲ့ Data ပမာဏထက် ပိုမပို့ဘူးလို့ဆိုလိုချင်တာဖြစ်ပါတယ်။ ဥပမာ ဗျာ။ Construction တစ်ခုမှာ အပေါ်နဲ့အောက် အုတ်ကိုပစ်ပေးတဲ့သူနဲ့ဖမ်းယူတဲ့သူ၊ ပစ်ပေးတဲ့သူကမြန်မြန်ပစ်နိုင်လို့မြန်မြန်ပစ်ရင် အပေါ်ဖက်ကဖမ်းတဲ့သူကမဖမ်းနိုင်တဲ့အခါအန္တရယ်ဖြစ်သွားမှာပေါ့။ ဒီတော့ အပေါ်ကဖမ်းနိုင်တဲ့နှုန်းနဲ့ အောက်ကနေအုတ်တွေကိုပစ်တင်ပေးမယ်။ ဒီသဘောပါ။

❖ အစွန်းတစ်ခုမှ နောက်အဆုံးတစ်ခုအထိ အစမှအဆုံးအတွင်း Data Packet များပျက်စီးမှုမရှိ Error Detection လည်းလုပ်ဆောင်ရပါတယ်။

❖ နောက်တစ်ခုကစိတ်ထင်တိုင်း ရှည်ချင်တိုင်းရှည်နေသော Data များကိုအသုံးပြုတဲ့ Network Medium ကလက်ခံနိုင်တဲ့ Data Packet Size အဖြစ် တုံးပစ် ပိုင်းပစ်ပါတယ်။ လက်ခံရာဖက်ကိုပြန်ရောက်ပြီဆိုမှ ၎င်းအတုံးအပိုင်းများကိုပြန်လည်စီးခြင်း အပိုင်းကိုလည်းလုပ်ဆောင်ပါတယ်။

❖ TCP/IP ရဲ့ TCP (Transmission Control Protocol) ဟာဒီဖက်အလွှာမှာအလုပ်လုပ်တာဖြစ်ပါတယ်။

မှတ်ချက်။ ။ ဒီနေရာမှာရှည်လျားတဲ့ Data တွေကို (Chunk) အပိုင်းလိုက်ပိုင်းပြီးလက်ခံရာဖက်ကို ပြန်ရောက်မှ ပြန်ပေါင်းစည်းတယ်ဆိုတာ Network Layer မှာလည်းပြောခဲ့တယ်နော်။ ဒါပေမယ့်သိရမှာက ဒီ Transport Layer ကမှဒီအဖြစ်အပျက်တွေကိုလုပ်ဆောင်တာပါ။ Network Layer ကဒီလိုလုပ်ဆောင်တယ်ဆိုတာ Medium တစ်ခုမှနောက်မတူညီတဲ့ Medium တစ်ခုကိုကူးလိုက်တဲ့အချိန်မှာ Data Chunk တာကြီးနေမယ်ဆိုရင်ပိုင်းပြီး၊ ၎င်းအပိုင်းလေးတွေကိုလက်ခံရာဖက်ကြမှပြန်ပေါင်းစည်းတယ်လို့ပြောတာပါ။ တော်ကြာရောနေမှာစိုးလို့ပါ။

၅.၂၃ OSI Transport Layer အကြောင်းသိကောင်းစရာ

OSI Model ရဲ့လေးလွှာမြောက်ဖြစ်တဲ့ ဒီ Transprot Layer ဟာအချက်အလက်များသွားလာမှုကို ထိန်းချုပ်ပေးခြင်းနှင့် အမှားတွေကို Recover လုပ်ပေးခြင်းတို့ကို လုပ်ဆောင်ပေးပါတယ်။ Reliable end-to-end error and flow control လို့ဆိုပါတယ်။ သူဟာ Message တွေကိုသင့်တော်တဲ့အရွယ်အစားရအောင် ပိုင်းပါတယ်။ ပြီးတော့ ရည်ရွယ်ရာကိုရောက်ပြီဆိုတော့မှပြန်ပြီး Assemble လုပ်ပါတယ်။

ခုနကပြောခဲ့တဲ့ Error နဲ့ Flow ကို Control လုပ်ခြင်းကိုပံ့ပိုးဖို့အတွက် ဒီ Transport Layer မှာရှိတဲ့ Protocol ဟာ Connection Services များကိုအသုံးပြုပါတယ်။ Connection Services နှစ်မျိုးရှိပါတယ်။ အဲဒါကတော့ -

- ❖ Connection-Oriented
- ❖ Connectionless တို့ဖြစ်ကြပါတယ်။

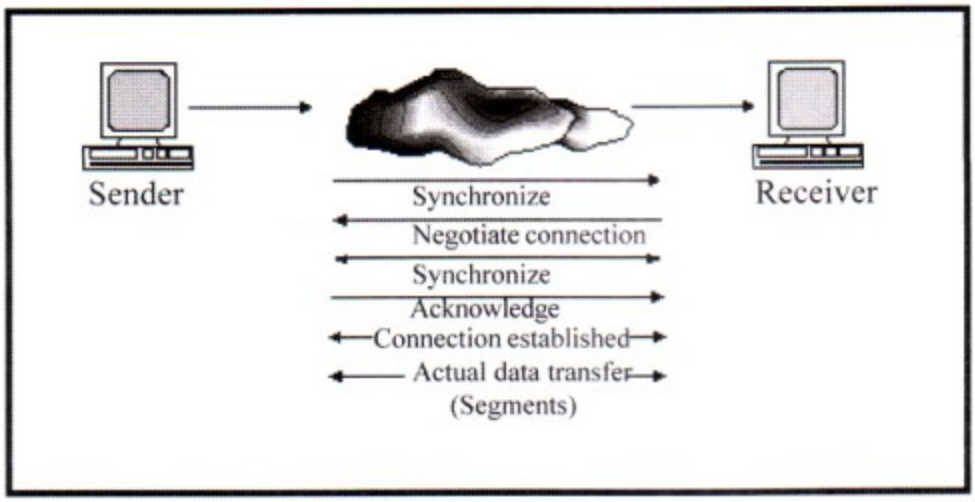
Connection Oriented အကြောင်းသိကောင်းစရာ

Connection-Oriented Services ဟာပို့လွှတ်သူ Stations နဲ့လက်ခံသူ Stations တို့နှစ်ခုအကြား Virtual Connection တွေထူထောင်ဖို့အတွက် Acknowledgments (သဘောတူခြင်း၊ လက်ခံရရှိခြင်း) နဲ့ Responses (အဖြေတုံ့ပြန်မှု) ကိုအသုံးပြုပါတယ်။ Acknowledgement ကိုအသုံးပြုရတာ ကတော့ Connection တွေချိတ်ဆက်ထားမှုကိုသေချာဖို့အတွက်ပါ။

ဒီ Connections ဟာ တယ်လီဖုန်းစကားပြောတာနဲ့ပုံစံတူပါတယ်။ ဖုန်းစကားပြောဖို့အတွက် ဖုန်းနံပါတ်နှိပ်လိုက်ပါတယ်။ တစ်ဖက်ကလက်ခံစကားပြောမယ့်သူက ဖုန်းကိုကောက်ကိုင်လိုက်ပြီး ဟဲလိုဆိုပြီးပြောမယ်။ ဒီအချိန်သင်က ကိုယ့်နာမည်ကိုပြောပြီးသင်ပြောချင်တဲ့ အကြောင်းအရာကိုစပြီးပြောဆိုပါတယ်။ တစ်ချိတစ်ရံကိုယ်ပြောနေတာကိုနားထောင်နေလို့ တစ်ဖက်ကအသံတိတ်နေတာကို သူဆက်ပြီးမျှားနားထောင်နေသေးရဲ့လားလို့ ဆိုပြီးနားထောင်နေသေးရဲ့လားလို့မေးပါတယ်။ ပြောလို့ဆိုလို့ပြီးတဲ့အချိန်ကြတော့ အဲဒါနော်ဆိုပြီးနှစ်ဦးသဘောတူဖုန်းချလိုက်ပါတယ်။ အခုပြောပြနေတဲ့ Connection Oriented Services ဟာလည်းဖုန်းပြော

သလိုပါပဲ။ ဗုန်းနဲ့စကားလုံးတွေအစား ကွန်ပျူတာ၊ Network Card နဲ့အချက်အလက်အထုပ်ကလေးတွေပါ။ ပုံမှာပြထားတာက ကွန်ပျူတာနှစ်လုံးကြား Connection Oriented Services ကိုအသုံးပြုပြီး ဆက်သွယ်မှုကို ပြုထားပုံဖြစ်ပါတယ်။

ပုံ ၅.၁၆



Connectionless အခြေခံသဘောတရား

Connectionless Services ကြတော့ Error နဲ့ Flow Control တွေမပါရှိပါဘူး။ အဲပေမယ့် ကောင်းကျိုးတစ်ခုကိုတော့လုပ်ပေးနိုင်ပါတယ်။ အဲ့ဒါကတော့ Speed ပါပဲ။ စဉ်းစားကြည့်လို့ရပါတယ်။ အဲ့ဒါကတော့ Connection တွေကို Maintain လုပ်ပေးခြင်းလည်းမရှိတဲ့အပြင် သူဟာ Speed ကို Error Control နဲ့လဲလှယ်လိုက်လို့ပါ။ သဘောကိုပြောပြတာနော်။

ဥပမာပြောရရင် Connectionless Services ဟာ Post Card တစ်ခုနဲ့အလားတူပါတယ်။ Post Card ဆိုတာက Happy Birthday လား၊ New Year အတွက်လား၊ ရည်ရွယ်ရာ ဦးတည်ချက်တစ်ခုပဲ၊ တခြားအကြောင်းမပါဘူး။ အဲပေမယ့် Error Control မပါတာကြောင့် Message တစ်ချို့တစ်ဝက်ပျောက်ခဲ့ရင် အဲကိုပြန်ပို့ပေးရတာတော့ရှိပါမယ်။

၅.၂၄ Name Resolution အခြေခံသဘောတရား

Network Address ဟာ အမြဲတမ်း Binary Numbers နဲ့ပါ။ များသောအားဖြင့် 32 bit ရှိပါတယ်။ ဒီနံပါတ်တွေဟာ Decimal အဲ့မှမဟုတ် Hexadecimal အဖြစ်ဖော်ပြပါတယ်။ ဘာလို့လဲဆိုတော့ လူတွေအနေနဲ့သတ်မှတ်ရတာလွယ်အောင်လို့ဖြစ်ပါတယ်။ ဒီ Decimal နဲ့ Hexadecimal တွေဟာ စကားလုံးအနေနဲ့အသိအမှတ်မပြုပေမယ့် ဒီ Transprot Layer မှာ Protocol တွေနဲ့ဘာသာပြန်ပြီး Transport Layer ရဲ့ Logical Name အဖြစ်ပြောင်းယူကြပါတယ်။

၅.၂၅ Session Layer ဆိုတာ

၅ လွှာမြောက်ဖြစ်တဲ့ Session Layer ဟာကွန်ရက်ကြီးတစ်လုံးမှဆက်သွယ်မှုကိုအခြေခံပြီး ကွန်ပျူတာနှစ်လုံး Dialog လုပ်နိုင်အောင် Function တွေအများကြီးလုပ်ဆောင်ပေးရပါတယ်။

Session Layer က Network ပေါ်က ကွန်ပျူတာတွေရဲ့ Dialog ဖလှယ်မှုတွေကို ဖြစ်တည်အောင် လုပ်ပေးရုံမျှမက ရပ်တန့်စေခြင်းကိုလည်းလုပ်ဆောင်ရပါတယ်။ တစ်ခုတော့ရှိပါတယ်။ Session Layer ရဲ့ အောက်ကအလွှာ(၄)ခု လုပ်ဆောင်ကြတဲ့ Data သယ်ယူပို့ဆောင်ရေးနဲ့၊ ၎င်း Data များသယ်ယူပို့ဆောင်ရာတွင် ပြန်ဆန်မှု၊ စိတ်ချရမှုတို့ကိုတော့လုပ်ကိုင်ခြင်းမရှိပါဘူး။ ပြန်ပြောရမယ်ဆိုရင် Session Layer ဟာ ကွန်ရက်တွင်းကကွန်ပျူတာနှစ်လုံး တိုက်ရိုက် Conversation လုပ်ခြင်းနှင့် Data Exchange လုပ်ခြင်းကိစ္စတွေအတွက် တာဝန်ရှိစေတာပါ။

Session Layer ရဲ့နောက်ထပ်တာဝန်တစ်ခုကတော့ - ကွန်ရက်ထဲက ကွန်ပျူတာနှစ်လုံးပေါ်က Application (၂)ခု တစ်ခုနှင့်တစ်ခု လှမ်းချိတ်တဲ့အခါ ၎င်း Application တွေရဲ့ Security ဆိုင်ရာ Function များနဲ့ Logical Network Names ဆိုင်ရာအမည်များ အသိအမှတ်ပြုခြင်း (Naming Recognition) များ၊ Communication Ports (ဆက်သွယ်ရေးဆိုင်ရာလမ်းကြောင်းများ) သတ်မှတ်ခြင်းတို့ကိုပါလုပ်ဆောင်ရပါတယ်။ ဥပမာ- Session Layer ပေါ်မှာ Run လုပ်တဲ့ NetBIOS Protocol လိုပေါ့။

မှတ်ချက်။ ။ OSI Reference Model ရဲ့ ၅ လွှာမြောက်ဖြစ်တဲ့ Session Layer ဟာ သာမာန် Local Area Network Protocol ဖြစ်တဲ့ TCP/IP တို့ IPX/SPX (Internetwork Packet Exchange/ Sequence Packet Exchange) စသည်တို့မှာ ကျယ်ပြန့်စွာအလုပ်လုပ်ဆောင်လေ့မရှိပါဘူး။

၅.၂၆ OSI Session Layer အခြေခံဒီဇိုင်းစရာ

OSI Model ရဲ့ Session Layer မှာအလုပ်လုပ်တဲ့ Protocol ဟာ Dialogs တွေကိုတည်ဆောက်ပေးရခြင်း၊ ထိမ်းသိမ်းပေးရခြင်း၊ အပိုင်းလိုက်ဖြတ်ပေးရခြင်းတို့ကို လုပ်ဆောင်ပေးရပါတယ်။ ဒါဟာ Transport Layer ရဲ့ပံ့ပိုးမှုတစ်ခုဖြစ်တဲ့ Connection Services နဲ့ကွာခြားသွားတဲ့အချက်ပါပဲ။ ဘာဖြစ်လို့လဲဆိုတော့ Section Layer ဟာ OSI ရဲ့ Upper Layer ဖြစ်သွားတာကြောင့်ပါ။ Dialog Control ပတ်သက်လို့ သုံးမျိုးရှိပါတယ်။ အဲ့ဒါတွေကတော့ -

- ❖ Simplex Dialogs
- ❖ Half-Duplex Dialgos
- ❖ Full-Duplex Dialogs တို့ဖြစ်ကြပါတယ်။

Simplex Dialog အကြောင်းသိကောင်းစရာ

အချက်အလက်များကိုပို့လွှတ်ရာ၌ တစ်ဖက်သတ်စနစ်ကိုကျင့်သုံးသည်။ ဥပမာပြောရရင် အဆောက်အအုံတစ်ခုအတွင်းရှိမီးသတ် Alarm စနစ်တစ်ခုသည် ၎င်းအဆောက်အအုံအတွင်း အကယ်၍များမီးလောင်ခဲ့လျှင် မီးသတ်ဌာနသို့အလိုအလျောက်အကြောင်းကြားမည်။ ထိုဖြစ်စဉ်တွင် ၎င်းမီးသတ် Alarm သည် မီးသတ်ဌာနမှပြန်လည်ပေးပို့သော Message ကိုလက်ခံ၍မရပေ။ လက်ခံစရာလည်းမလိုအပ်ပေ။ ထို့ကြောင့် ၎င်းကို Simplex Transmission ဟုခေါ်သည်။

Half-Duplex Dialog အကြောင်းသိကောင်းစရာ

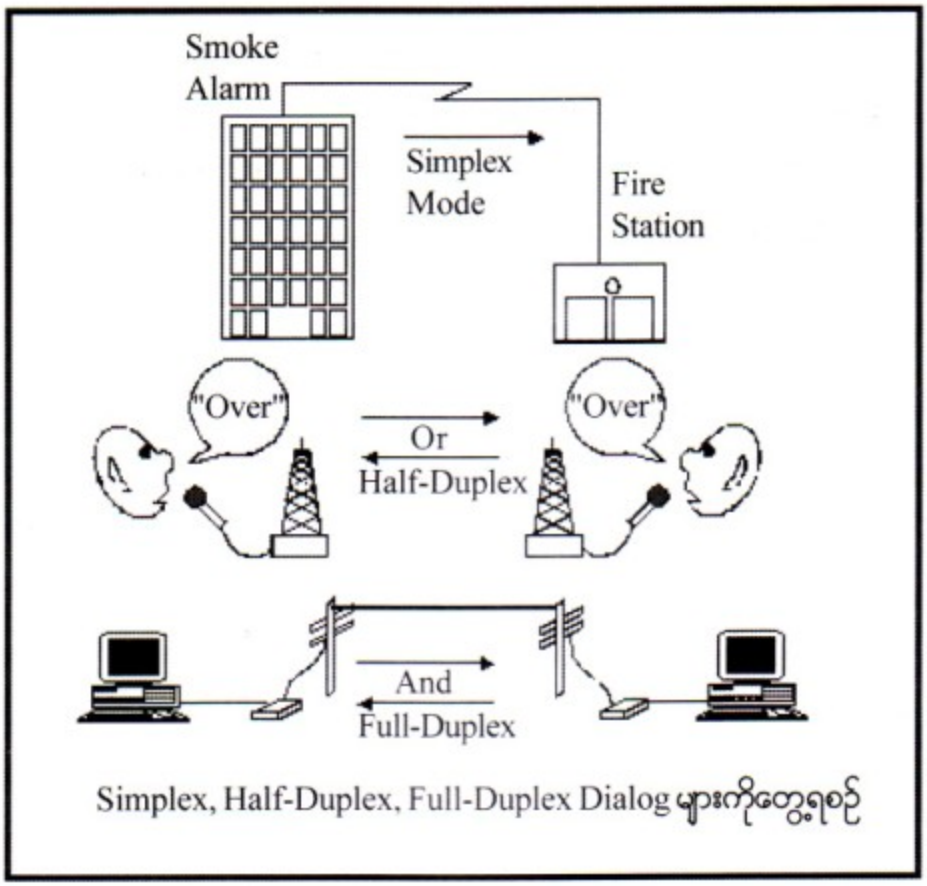
ဒီတစ်ခါတစ်ဖက်သတ်တော့မဟုတ်ပေ။ နှစ်ဦးနှစ်ဖက်အပြန်အလှန်အချက်အလက်များပေးပို့လို့ရသော်လည်း တစ်ကြိမ်တွင် တစ်ဖက်သာပို့ဆွဲ့ရှိသည်။ ပစ္စည်းတစ်ခုကအချက်အလက်ကိုပေးပို့ပြီးပြီဆိုမှနောက်ပစ္စည်းတစ်ခုက ပေးပို့ဆွဲ့ရှိသည်။ ဥပမာ Radio Operator များအချင်းချင်းစကားပြောရာ၌ တူညီတဲ့ Communication Channel တစ်ခုတည်းတွင်စကားပြောနေကြသော်လည်း တစ်ယောက်ပြောပြီးမှ နောက်တစ်ယောက်ကပြောခွင့်ရှိသည်။ တစ်ယောက်ပြောနေချိန်တွင် နောက်တစ်ယောက်ကယှဉ်၍ပြောခွင့်မရှိပေ။ တစ်နည်းအားဖြင့်ပြိုင်တူပြောခွင့်မရှိပေ။

Full-Duplex Dialog အကြောင်းသိကောင်းစရာ

နှစ်ဦးနှစ်ဖက်တစ်ကြိမ်တည်းအပြန်အလှန်အချက်အလက်များပေးပို့လို့ရအောင် မတူညီတဲ့ Communication Channel ကိုသီးခြားဆီအသုံးပြုထားပါတယ်။ စကားပြောတယ်လီဖုန်းဟာ Full-Duplex ပစ္စည်းတွေဖြစ်ကြပါတယ်။ ကွန်ပျူတာအများစုရဲ့ Modems များဟာလည်း Full-Duplex နဲ့အလုပ်လုပ်နိုင်ကြပါတယ်။

မှတ်ချက် ။ ။ Half-Duplex နဲ့ Full-Duplex ဟာပိုမိုရှုပ်ထွေးတဲ့နည်းပညာကိုအသုံးပြုထားသောကြောင့်ပို၍ကုန်ကျစရိတ်များပါတယ်။

ပုံ ၅.၁၇



Simplex, Half-Duplex, Full-Duplex Dialog များကိုတွေ့ရစဉ်

၅.၂၃ Presentation Layer ဆိုတာ

၆ လွှာမြောက်ဖြစ်တဲ့ ဒီ Presentation Layer ကိုတခါတရံ Syntax Layer လို့လဲအခေါ်ရှိကြပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ ၎င်းရဲ့တာဝန်က ကွန်ပျူတာရဲ့ Native syntax ကနေတခြားကွန်ပျူတာဖတ်လို့ရတဲ့ Syntax ဖြစ်အောင်ပြောင်းလဲပေးရလို့ပါပဲ။

အနှစ်ချုပ်ပြီးထပ်ပြောရမယ်ဆိုရင် Application Layer ကနေဆင်းသက်လာတဲ့ Data အတိုင်း Network Transmission လုပ်မရတာကြောင့် Transmission လုပ်လို့ရအောင် Format ပြောင်းပေးရတာပါ။ Syntax ပြောင်းပေးရတာပါ။ အဲကြောင့် Syntax Layer လို့လည်းတခါတရံခေါ်တယ်လို့ပြောတာပါ။ ဒီ Layer ဟာ -

- ❖ Data တွေကိုလည်း Encrypt လုပ်ပေးရပါတယ်။
- ❖ Data တွေကို Compression လည်းလုပ်ပေးရပါတယ်။
- ❖ Character Set တွေကိုလည်းပြောင်းလဲပေးရပါတယ်။
- ❖ Graphic Command တွေကိုလည်းဘာသာပြန်ပေးရပါတယ်။

မှတ်ချက်။ ။ တကယ့်ပြင်ပလောကမှာ လက်ရှိအသုံးပြုနေတဲ့ Protocol တွေ ဥပမာ TCP/IP လို မျိုးပေါ့။ သူဆိုရင် Presentation Layer Protocol ကိုသီးခြားအသုံးမပြုပါဘူး။ တချို့လည်းပြောကြတယ်။ ကြားဖူး၊ ဖတ်ဖူးတယ်။ ဘာတဲ့ Presentation Layer ဆိုတာ တကယ့် Networking လောကမှာ Encode, Decode လုပ်တာပါတဲ့။ ဒါလည်းခြုံငြေပြာတာဖြစ်နိုင်ပါတယ်။

၅. ၂၈ OSI Presentation Layer အကြောင်းသိကောင်းစရာ

Presentation Layer လို့ပြောလိုက်ကတည်းက ကွန်ရက်အသုံးပြုသူလူတချို့က ဘယ်လိုတွက်လိုက်သလဲဆိုတော့ ဒီအလွှာဟာ Data တွေကိုအသုံးပြုသူ User တွေကိုတင်ပြခြင်း (Presentation) လုပ်ခြင်းလို့ မှားပြီးမှတ်ယူလိုက်တတ်ကြပါတယ်။ တကယ်တော့ Presentation Layer ဆိုတာ Lower Layer Data တွေကို Upper Layer ကအလုပ်လုပ်နိုင်တဲ့ Format ပုံစံမျိုးပြောင်းရပါတယ်။ အဲ့ဒီအပြင် Presentation Layer ဟာ Data ကို Encryption လုပ်ပါတယ်။ Compression တွေလုပ်ပေးပါတယ်။ နောက်ထပ်ပြောရမယ်ဆိုရင် Presentation Layer ဟာ Character Set နဲ့ပတ်သက်တဲ့ Translation တွေလဲပြုလုပ်ရပါတယ်။ ကွန်ပျူတာတွေ Binary Number ကနေ Text အဖြစ်ပြောင်းလဲတဲ့နေရာမှာ Character Code Table ဟာတစ်ခုထဲရှိတာမဟုတ်ပါဘူး။ ကွန်ပျူတာစနစ်တော်တော်များများကတော့ ASCII (American Standard Code for Information Interchange) ဆိုတာကိုအသုံးပြုကြပေမယ့် Mainframe နဲ့ကွန်ပျူတာနဲ့ တချို့သော IBM Network စနစ်တွေမှာ ASCII ကိုမသုံးဘဲ EBCDIC (Extended Binary Coded Decimal Interchange Code) ကိုအသုံးပြုကြပါတယ်။ ဒါပေမယ့် သိထားရမှာကသူတို့နှစ်ခုဟာ လုံးဝမတူပါဘူးဆိုတာပါပဲ။ Presentation အလွှာများအလုပ်လုပ်တဲ့ Protocol ဟာသူတို့နှစ်ခုကြားလည်း Translate လုပ်ပေးနိုင်ပါတယ်။ ဒီ Data Transalation ဆိုတဲ့နေရာမှာလည်း ယေဘုယျအားဖြင့် (၄) မျိုးရှိပါတယ်။ အဲ့ဒါတွေကတော့ -

- ❖ Bit Order
- ❖ Byte Order
- ❖ Character Code
- ❖ File Syntax တို့ဖြစ်ကြပါတယ်။

၅. ၂၉ Character Code Translation အကြောင်းသိကောင်းစရာ

ကွန်ပျူတာစနစ်အများစုဟာ Character အဖြစ်ပြောင်းပြန်ပြန်နိုင်ဖို့ (Character Sets) အောက်ပါ Binary Number Scheme တစ်ခုခုကိုသုံးကြပါတယ်။

၅.၃၀ Application Layer ဆိုတာ

Application Layer ကတော့ အပေါ်ဆုံးအလွှာပါ။ Layer 7 ပေါ့။ သူကတော့ ကွန်ပျူတာမှာ Run နေတဲ့ Software နဲ့ Network ကို Communicate လုပ်ပေးထားတဲ့ Protocol နဲ့ကြား Interface လုပ်ပေးပါတယ်။ ဥပမာပြောရမယ်ဆိုရင်- ဒီ Layer ဟာ E-mail, File Transfers, Telnet နဲ့ FTP (File Transfer Protocol) Application တွေကို Interface ပြုလုပ်ခြင်း အပိုင်းတွေမှာပံ့ပိုးပေးရတာပါ။

ကွန်ပျူတာပေါ်မှာ Run လုပ်နေတဲ့ Application တွေဟာ Application Layer Protocol က Support လုပ်တဲ့ ဝန်ဆောင်မှုတွေကို အသုံးပြုကြသလို ၎င်း Application Layer ကိုယ်တိုင်ကတော့ သူ့အောက်ကအလွှာတွေကပံ့ပိုးပေးတဲ့ ဝန်ဆောင်မှုတွေကိုသုံးရပါတယ်။

၅.၃၁ OSI Application Layer Concept အကြောင်းသိကောင်းစရာ

Application Layer ဆိုတာကွန်ရက်ရဲ့ဝန်ဆောင်မှု (Network Services) တွေကိုပံ့ပိုးပေးရတာပါ။ ဘယ်လိုဝန်ဆောင်မှုတွေလဲဆိုတော့ Files, Services, Print Services, Database Services etc., တို့ဖြစ်ကြပါတယ်။ ဒါကို အတော်များများက အထင်မှားနေတာတွေရှိနေကြပါတယ်။ ဆိုလိုချင်တာက Application Layer ဟာ ကွန်ပျူတာအသုံးပြုတဲ့သူတွေသုံးတဲ့ Application တွေဖြစ်တဲ့ Wordprocessor တို့ ဘာတို့ညာတို့ကို ထောက်ပံ့ပေးရတဲ့ တာဝန်ရှိတယ်လို့ထင်နေကြပါတယ်။ တကယ်တော့ Application Layer ဟာအထက်ကပြောခဲ့တဲ့အတိုင်း ကွန်ရက်ရဲ့ဝန်ဆောင်မှုတွေကိုပေးရတာပါ။

Application Layer ဟာကွန်ရက်ရဲ့ဝန်ဆောင်မှုတွေနဲ့ပတ်သက်တဲ့ တာဝန်ခံစိုးကိုထမ်းဆောင်ရပါတယ်။ တစ်ခုကတော့ သူလုပ်ပေးနိုင်တဲ့ ဝန်ဆောင်မှုတွေကို ကြေညာပါတယ်။ နောက်တစ်ခုကတော့ ကွန်ရက်ဝန်ဆောင်မှုတွေကို အသုံးပြုတာပါပဲ။

၅.၃၂ Advertising Services အကြောင်းသိကောင်းစရာ

Application Layer ရဲ့ပထမတာဝန်တစ်ခုဖြစ်တဲ့ Advertising Service ကတော့ သူလုပ်ပေးနိုင်တဲ့ဝန်ဆောင်မှုတွေကို ကွန်ရက်ကိုကြေညာရပါတယ်။ ဒီနေရာမှာ Application Layer ဟာ Advertising *Services* နှစ်မျိုးဖြစ်တဲ့ *Active & Passive Methods* နှစ်ခုလုံးနဲ့ အလုပ်လုပ်နိုင်ပါတယ်။

Active Service Advertisement အကြောင်းသိကောင်းစရာ

Server ကနေ ဝန်ဆောင်မှုတွေကိုကြေညာလိုက်တဲ့အချိန်မှာတော့ Active Service ဟာ သူတို့လုပ်ပေးနိုင်တာတွေကိုစပြီး Announce လုပ်ပါတော့တယ်။ Clients တွေဟာသူတို့လိုချင်တဲ့ ဝန်ဆောင်မှုတွေနဲ့

တကွ တုံ့ပြန်မှုကိုပြုလုပ်ပါတော့တယ်။

Netware တာ SAP (Service Advertisement Protocol) လို့ခေါ်တဲ့ Active Services Advertisement Protocol နဲ့အလုပ်လုပ်ပါတယ်။

Passive Service Advertisement အခြေခံသဘောတရား

Server တာသူတို့ရဲ့ဝန်ဆောင်မှုနဲ့လိပ်စာတွေကို Central Service Registry နဲ့အတူ List လုပ်ထားနိုင်ပါတယ်။ Clients တွေဟာ ဘယ်လိုဝန်ဆောင်မှုတွေရနိုင်သလဲဆိုတာရယ်၊ ၎င်းတို့ကိုဘယ်လိုရယူမလဲဆိုတာရယ်ကိုတော့ စုံစမ်းရပါတယ်။ ဒါကို Passive Service Advertisement လို့ခေါ်ပါတယ်။

၅.၃.၃ Service Use Methods အခြေခံသဘောတရား

Client တွေဟာသူတို့လိုချင်တဲ့ Service တွေကို ဘယ်လို Access လုပ်ရမယ်ဆိုတာနဲ့ပတ်သက်ပြီး နည်း (၃) နည်းရှိပါတယ်။ အဲဒါတွေကတော့ -

- ❖ OS Call Interruption
- ❖ Remote Operation
- ❖ Collaboration တို့ဖြစ်ကြပါတယ်။

၅.၃.၄ OSI Layer များအနှစ်ချုပ်

Layer	တာဝန်	ဤအလွှာနှင့်ပတ်သက်သူ
Physical	Physical ဆိုတဲ့အတိုင်း ကွန်ရက်ရဲ့ ရုပ်ပိုင်းဆိုင်ရာတွေကိုတာဝန်ယူရတယ်။ ဘာတွေလဲဆိုတော့ Connections တွေ၊ ကြားခံပစ္စည်း Media တွေ၊ အပေါ်အလွှာတွေကဆင်းသက်လာတဲ့ Data တွေကို Electrical Impulses (လျှပ်စစ်တွန်းအား) (ဥပမာ- Voltage တွေ၊ Current တွေ၊ Modulation နဲ့ Bit Synchronization) တွေအဖြစ်ပြောင်းလဲပေးရပါတယ်။	Twisted Pair, Coaxial, AUI Network Card

Layer	တာဝန်	ကျင့်သုံးနည်းပတ်သက်သူ
Data Link	Data Packet တွေကိုထုတ်ပိုးပါတယ်။ ပို့လွှတ်ပါတယ်။ Checking လုပ်ပါတယ်။ Data Link Layer ဟာ Physical Layer Token Ring ကိုအသုံးပြုပြီး Data တွေကိုပို့လွှတ်ခြင်း နှင့် လက်ခံရယူခြင်းတို့ကိုလုပ်ဆောင်ရပါတယ်။ နောက်ပြီး Network Layer ကိုလည်း ဝန်ဆောင်မှုတွေပံ့ပိုးပေးရပါသေးတယ်။	MAC Addressing Ethernet Token Ring
Network	Netwrok Layer ကိုအလွယ်မှတ်ရင်လမ်းကြောင်းရှာတယ် လို့မှတ်ထားလို့ရတယ်။ စတင်ရာ (Server) နဲ့ ရောက်ရှိရာ (Destination) အကြားလမ်းကြောင်း(Route) ကိုရှာဖွေပေးရပါတယ်။ Address တွေကိုသတ်မှတ်ပေးရပါတယ်။ Logical Connections တွေကိုပြုလုပ်ပေးခြင်း နှင့် ထိန်းသိမ်းခြင်းတို့ကိုလုပ်ဆောင်ရပါတယ်။	IPX, IP
Transport	Flow Control ကိုလုပ်ဆောင်ရပါတယ်။ ဒီအချုပ်ပါပဲ။ နောက်ပြီးဒီဖက်မှ တိုဖက်ထိတစ်နည်း အားဖြင့် အစွန်းတစ်ဖက်မှ နောက်အစွန်းတစ်ဖက်ထိဆက်သွယ်မှု Communication ဖြစ်စဉ်ကြီးကိုပံ့ပိုးပေးရပါတယ်။	TCP, NetBEUI SPX
Session	Connection တစ်ခုအတွင်းမှာရှိကြတဲ့ Data Packet နဲ့ Dialog တွေကို Sequence စီတန်းခြင်းနှင့် ထိန်းညှိခြင်း (Sync ကိုက်အောင်လုပ်ခြင်း - Synctronize) ကိုလုပ်ပါတယ်။ ဒီအလွှာဟာတစ်နေရာမှတစ်နေရာသို့ Transmission ပြီးဆုံးသည်အထိတစ်ခုနှင့်တစ်ခုချိတ်ဆက်ထားမှု Connection ဖြစ်နေစေဖို့စောင့်ထိန်းပေးပါတယ်။	Telnet

Layer	တာဝန်	ကျင့်သုံးနည်းပတ်သက်သူ
Presentation	ဒီအလွှာကတော့ Character Set တွေကိုဘာသာပြန်ခြင်း၊ Data တွေကိုဝှက်ပြီးပို့ခြင်း (အသုံးပြုလို့မရအောင်ပြုလုပ်ပြီးပို့ခြင်း Encrypt) Data များကို ချုံ့ခြင်း (Compression) နှင့် ချုံ့ထားသော Data များကိုပြန်ဖြေခြင်း (Decompression) တို့ကိုလုပ်ဆောင်ရပါတယ်။ နောက်ပြီး Application Layer ကို Data အဖြစ်ပြန်လည်တင်ပြခြင်းတို့ကိုလုပ်ဆောင်ရပါတယ်။	ASCII EBCDIC
Application	ကွန်ပျူတာမှာ Run နေတဲ့ Application နဲ့ ကွန်ရက်အကြား Interface လုပ်ပေးခြင်း။ တစ်နည်းအားဖြင့် ကွန်ရက်ကိုအသုံးပြုသူ User နှင့် ကွန်ရက်အကြားများစွာသော Network ဝန်ဆောင်မှုတွေကိုသတ်မှတ်လုပ်ပေးရပါတယ်။	FTP HTTP

၅.၃၅ IEEE 802 Networking Specifications အကြောင်း

၁၉၇၀ ခုနှစ်များနောင်းပိုင်းက နောင်တစ်ချိန်ရဲ့ စီးပွားရေးလုပ်ငန်းတွေ၏ ကွန်ပျူတာကဏ္ဍမှာ Local Area Network (LANs) ဟာလွန်စွာမှအရေးပါလာမယ်လို့ သိလာကြပါတယ်။ ဒီသိရှိမှုကနေဖြစ်ပေါ်လာတဲ့ လှုံ့ဆော်မှုကြောင့် IEEE လို့ခေါ်တဲ့ Institute of Eelectrical and Electronic Engineers အဖွဲ့ဟာ LAN Standard တွေကိုစတင်သတ်မှတ်ပါတော့တယ်။ ဘယ်အတွက်လည်းဆိုတော့ ထုတ်လုပ်သူတွေအများကြီးက ထုတ်လုပ်လိုက်တဲ့ Network Interface တွေနဲ့ Cable တွေဟာတူညီတဲ့ Specification ရှိစေဖို့အတွက် အိမှမဟုတ် တစ်ယောက်ကထုတ်တာနဲ့ နောက်တစ်ယောက်ကထုတ်တာ Compatible ဖြစ်တော့မပေါ့။ ဒီ Project ကို Project 802 လို့ခေါ်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ 1980 ခုနှစ် February လကစတင်ခဲ့လို့ 802 ဆိုပြီးခေါ်လိုက်ပါတယ်။ အဲ့ဒီအချိန်ကစပြီး ယနေ့တိုင် Networking လောကမှာ IEEE 802 Specification တွေဟာ စတင်အမြစ်တွယ်လာတော့တာပဲဖြစ်ပါတယ်။

အဲ့ဒီတုန်းက OSI Reference Model က Stanardized မလုပ်ရသေးဘူးလေ။ ၁၉၈၃-၈၄ ခုနှစ်လောက်ထိပေါ့။ IEEE 802 Standard က OSI ထက်စောတယ်လို့ပြောလို့ရပါတယ်။ ဘယ်လိုပဲဖြစ်ဖြစ် နောက်ဆုံးမှာ ၎င်းတို့နှစ်ခုဟာ အတူတကွလောက် Developed ဖြစ်ခဲ့တာဖြစ်ပါတယ်။ နောက်တော့ တစ်ခုနှင့်

Sandard	Name	Explanation
802.1	Internetworking	Covers routing, bridging, and internetwork Communications
802.2	Logical Link Control	Relates to error-and flow control over data frames
802.3	Ethernet LAN	Covers all forms of Ethernet media and Interfaces, from 10 Mbps to 1 Gbps (Gigabit Ethernet)
802.4	Token Bus LAN	Covers all forms of token bus media and Interfaces
802.5	Token Ring LAN	Covers all forms of token bus media and Interfaces
802.6	Metropolitan Area Network	Covers MAN technologies address ing, and services
802.7	Broadband Technical Advisory Group	Covers broadband networking media, interface and other equipment
802.8	Fiber-Optic Technical Advisory Group	Covers use of fiber-optic media and technologies for various networking type
802.9	Integrated Voice/Data Networks	Covers integration of voice and data traffic over a single networking medium
802.10	Network Security	Covers network access controls, encryption certification, and other security topics
802.11	Wireless Networks	Sets standards for wireless network ing for many different broadcast frequencies and usage techniques
802.12	High-speed Networking	Covers a variety of 100 Mbps-plus technologies, including 100VG-AnyLAN

တစ်ခုအပြိုင်သဖွယ်ဖြစ်လာပါတယ်။ ဒါပေမယ့် သိထားရမှာက IEEE ဟာ ISO ရဲ့ Participants တစ်ခုပဲ ဆိုတာရယ်။ ဒီ ISO ကပဲ OSI ကိုထုတ်ခဲ့တယ်ဆိုတာရယ်ကိုပါပဲ။ Project 802 ဟာ Network Adapt-

ers, Cable ကြိုး၊ Connectors အချက်ပြစနစ် Signaling Technologies, Media Access Controls (MACs) စတဲ့ကွန်ရက်ပိုင်းဆိုင်ရာတွေအပေါ် စံသတ်မှတ်ဖို့အာရုံစိုက်ခဲ့ပါတယ်။ အဲ့ဒီမှာ အများစုက OSI Model ရဲ့အောက်ဆုံးအလွှာနှစ်လွှာဖြစ်တဲ့ Physical နှင့် Data Link အလွှာပေါ်မှာပဲ အခြေတည်တာဖြစ်ပါတယ်။ တိတိကျကျပြောရမယ်ဆိုရင်တော့ 802 Specification တွေဟာ Network မှာ NICs တွေဘယ်လို Access လုပ်ကြမလဲဆိုတာနှင့် အမျိုးမျိုးသော Networking Media တွေမှာ ဒီမှမဟုတ် ၎င်းတို့ကိုဖြတ်သန်းပြီး Data တွေကိုဘယ်လိုပို့မလဲဆိုတာပဲဖြစ်ပါတယ်။ အဲ့ဒီအပြင် ကွန်ရက်မှာပစ္စည်းတွေကိုချိတ်ဆက်ခြင်း၊ အုပ်ချုပ်ခြင်း၊ ဖြုတ်ချခြင်းစတာတွေကိုရောပေါ့။ ဇယားမှာလည်း IEEE 802 Specifications များကိုဖော်ပြထားပါတယ်။

၅.၄၆ OSI Model တွင်ချဲ့ထွင်ထားသော IEEE 802

OSI Model ရဲ့အောက်ဆုံးအလွှာနှစ်ခုဖြစ်တဲ့ Physical နှင့် Data Link Layer ဟာ Networking Media တွေကိုကွန်ပျူတာတွေကို ဘယ်လိုချိတ်ဆက်မလဲဆိုတာရယ်၊ ကွန်ပျူတာတွေက Media (ဥပမာ Network ကြိုး) တွေကို Access လုပ်ရာမှာ ၎င်း Media နှင့်ဆက်သွယ်ထားတဲ့ အခြားကွန်ပျူတာတွေကိုမထိခိုက် မနှောင့်ယှက်စေဘဲ ဘယ်လို Access လုပ်မလဲ စတာတွေကိုသတ်မှတ်ပေးရပါတယ်။ Ethernet နှင့် Token Ring အပါအဝင် LAN နည်းပညာမှာအထက်ပါလုပ်ငန်းများပိုမိုအောင်မြင်ကောင်းမွန်စေရန် Project 802 ဟာအထက်ပါလုပ်ငန်းများကို 802.1 မှ 802.5 အထိဆိုပြီး တာဝန်ယူလိုက်ပါတယ်။ ထပ်ရှင်းပြပါအုံးမယ်။ တစ်လုံးမကသောကွန်ပျူတာတွေ Network ကို Access လုပ်ရာမှာ Network မှာရှိတဲ့ အခြားကွန်ပျူတာတွေ Access လုပ်ခြင်းကို ထိခိုက်မှုမရှိစေရန် IEEE 802 Specification ဟာ OSI Model ရဲ့ Physical နှင့် Data Link အလွှာတွေမှာ Expand လုပ်လိုက်တာဖြစ်ပါတယ်။ ပုံမှာလည်းတွေ့မြင်ရမှာပါ။ 802 ဟာ Data Link အလွှာကို ဆင့်ပွားအလွှာနှစ်ခုခွဲထုတ်လိုက်ပါတယ်။ ၎င်းဆင့်ပွားအလွှာနှစ်ခုကတော့ -

(၁) LLC လို့ခေါ်တဲ့ Logical Link Control - အမှားပြင်ဆင်ခြင်း (Error Connection) နှင့် Data စီးဆင်းမှုကိုထိန်းချုပ်ခြင်း (Flow Control)

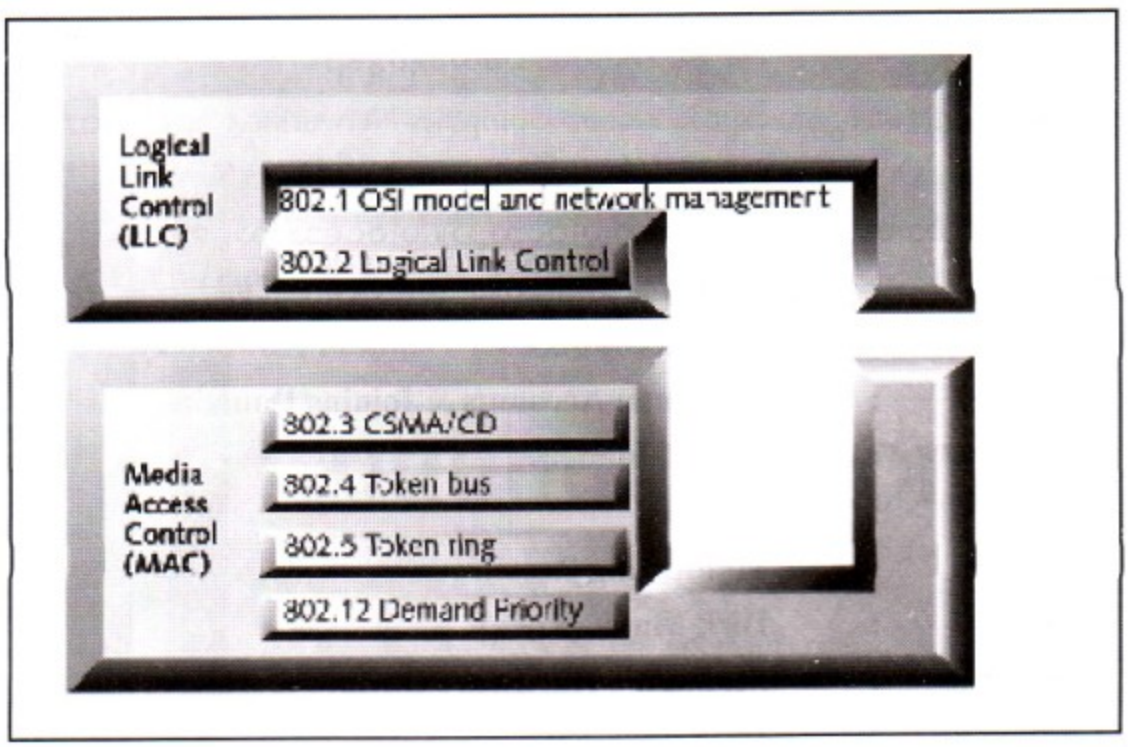
(၂) MIC လို့ခေါ်တဲ့ Media Access Control - Access လုပ်ခြင်းကို ထိန်းချုပ်ရန်။

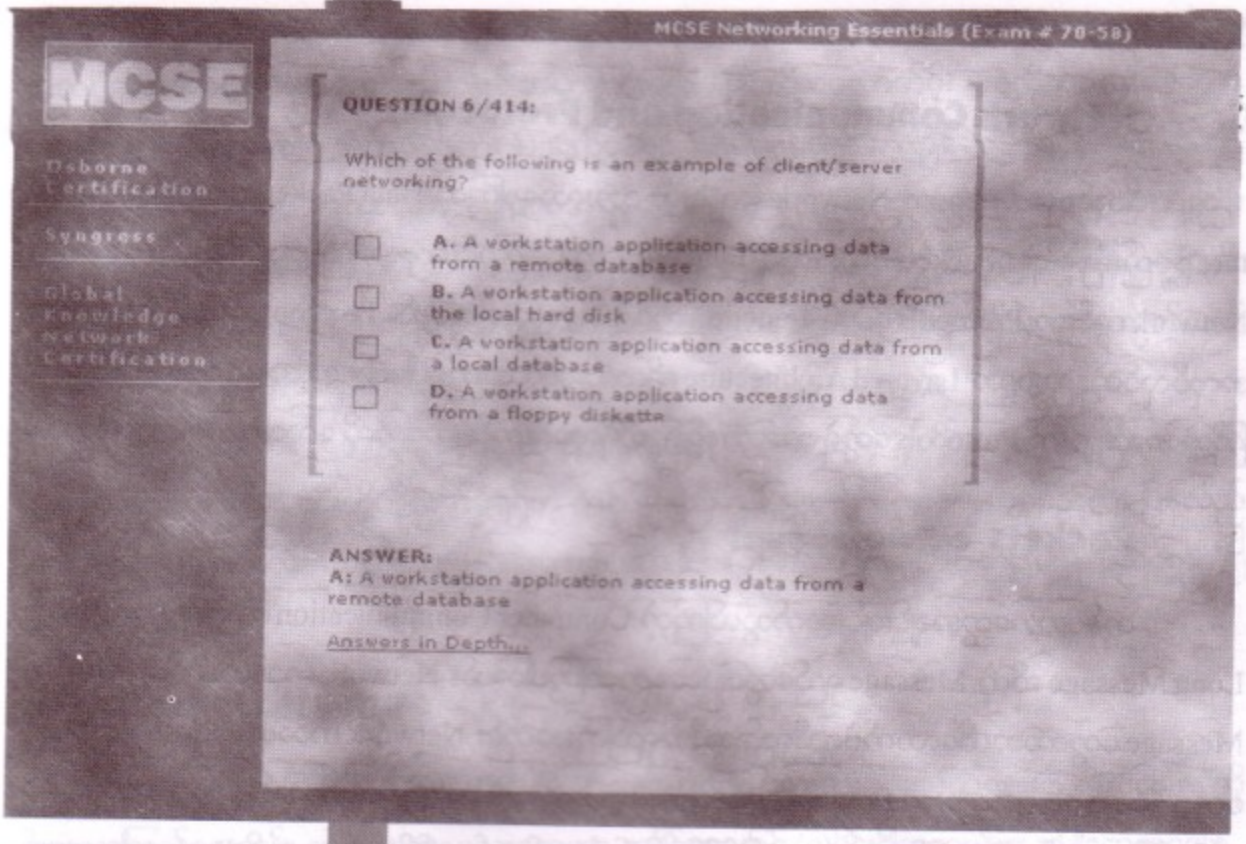
802.2 လို့သတ်မှတ်ထားတဲ့ Logical Link Control ဆင့်ပွားအလွှာဟာ Data Link Communication ကိုထိန်းချုပ်ပေးတဲ့အပြင် (SAPs) က Service Access Points လို့ခေါ်တဲ့ Logical Interface Points အသုံးပြုမှုကိုလည်း သတ်မှတ်ပေးပါတယ်။ SAPs ဆိုတာ အခြားကွန်ပျူတာဟာ LLC ဆင့်ပွားအလွှာမှ

အချက်အလက်များ OSI အပေါ်အလွှာများသို့ ပြောင်းရွှေ့သည့်အခါမှာ သုံးတာဖြစ်ပါတယ်။

Media Access Control (MAC) ဆင့်ပွားအလွှာကတော့ Physical Layer နှင့်အတူ Network Card တွေအများကြီးခွဲဝေ Access လုပ်နိုင်အောင် ပံ့ပိုးပေးနိုင်ပါတယ်။ MAC တာကွန်ပျူတာရဲ့ Network Card နှင့်တိုက်ရိုက်ဆက်သွယ်တာဖြစ်ပါတယ်။ အဲဒီအပြင်သူက ကွန်ရက်မှာရှိတဲ့ ကွန်ပျူတာတွေကြား Data ပို့လွှတ်ရာ၌ အများကင်းအောင်လုပ်ပေးဖို့တာဝန်လည်းရှိပါတယ်။ Data Link Access တွေဟာ NIC တိုင်းရဲ့ PROM မှာတစ်ခါတည်း ထည့်သွင်းထားပြီးသားဖြစ်ပြီး ၎င်းကို MAC-Layer Address လို့ခေါ်ပါတယ်။ ဘာဖြစ်လို့လည်းဆိုတော့ ၎င်းဟာ 802.2 Specification အရ ဒီဆင့်ပွားအလွှာမှာ အလုပ်လုပ်လို့ပဲဖြစ်ပါတယ်။ အောက်ဖော်ပြပါပုံမှာ IEEE 802 ဟာ LLC နှင့် ဘယ်လို Map လုပ်ထားသလဲဆိုတာနှင့် MAC ဆင့်ပွားအလွှာဟာလည်း CSMA/CD Networking, Token Bus Networking, Token Ring Networking နှင့် Demand Priority တွေကိုဘယ်လိုပံ့ပိုးသလဲ ဆိုတာကိုဖော်ပြထားပါတယ်။

ပုံ ၅.၁၈





UNIT 6

Network Communications & Protocols

တကယ်တော့ ဒီ သင်ခန်းစာဟာ ခုနက သင်ခန်းစာရဲ့ အဆက်လို့တောင် ပြောမယ်ဆိုပြောလို့ရပါတယ်။ စံ သတ်မှတ်ထားတဲ့ OSI ထက် လက်တွေ့တကယ်အသုံးပြုနေတဲ့ Protocols တွေအကြောင်းကိုလေ့လာရမှာဖြစ်ပါတယ်။

၆.၁ Network Communication and Protocols

ဒီသင်ခန်းစာကတော့ Network အတွင်းမှာ သွားလာနေကြတဲ့ Data Packets လေးတွေရဲ့ Structure ဖွဲ့စည်းပုံနှင့် ၎င်း Packets လေးတွေရဲ့ Function တွေအကြောင်းလေ့လာကြမှာဖြစ်ပါတယ်။ နောက်ပြီး Network တွင်းက Protocols တွေရဲ့ Function ကိုလည်းလေ့လာကြမယ်။ Protocols တွေရဲ့ အလွှာလိုက် အလုပ်လုပ်တဲ့နည်းပညာ Layered Architecture ကိုလည်းလေ့လာကြရပါမယ်။ အဲ့ဒီအပြင် ဘုံ အသုံးပြုလေ့ရှိကြတဲ့ အသုံးများတဲ့ Protocols တွေရဲ့ သဘောနှင့် သူတို့ရဲ့လုပ်ဆောင်ချက်တွေကို လေ့လာကြရမှာဖြစ်ပါတယ်။

၆.၂ Packets များ၏တာဝန်များ

ကွန်ပျူတာတွေအချင်းချင်းဆက်သွယ်ကြတဲ့ Computer Communication မှာ ပုံမှန်အားဖြင့်တော့ Long Message ဆိုတဲ့ Message ရှည်တွေပါဝင်နေတတ်ကြပါတယ်။ Network မှာသယ်ယူပို့ဆောင်ရာမှာ Message တွေဟာဘယ်လောက်ပဲရှည်ရှည် အဲဒီအရှည်ကြီးအတိုင်း Network ကသယ်ယူပို့ဆောင်ခြင်းမပြုပါဘူး။ ဒီတော့ ၎င်းရှည်လျားတဲ့ Data အပိုင်းအစကိုသေးငယ်တဲ့အပိုင်းအဖြစ် ပုံစံပြန်ပြောင်း ပြီးတော့ ထိန်းချုပ်ရထိန်းသိမ်းရလွယ်ကူတဲ့အပိုင်းလေးတွေအဖြစ်ပိုင်းလိုက်ပါတယ်။ ၎င်းအပိုင်းလေးတွေကို Packet ဒါမှမဟုတ် Frame လို့ခေါ်ပါတယ်။ ဒီနေရာမှာသိစေချင်တာက အဲ့သလိုအပိုင်းလေးတွေကို Packets ဒါမှမဟုတ် Frame လို့ခေါ်တယ်လို့သုံးနှုန်းခဲ့တယ်နော်။ များသောအားဖြင့် Packet နှင့် Frame ဟာ အဓိပ္ပါယ်တူ ပြောင်းလဲသုံးလို့ရပေမယ့် တခါတရံ မတူညီတဲ့ Network တွေမှာ ဒီ Packet နှင့် Frame အသုံးအနှုန်းဟာ အနည်းငယ်ကွဲလွဲမှုရှိနေပါတယ်။ ဒါကိုတော့ သိစေချင်ပါတယ်။ ကဲ အခုကစပြီး Packets တွေအကြောင်း လေ့လာကြရအောင်။

Network ဟာ Data တွေကို ဘာဖြစ်လို့များပိုင်းလိုက်ရပါသလဲ။ ဒီလိုပြောဖို့အတွက် အချက်နှစ်ချက်ရှိပါတယ်။ ဆိုလိုတာက - Network ဟာ Data တွေကို ပိုင်းခြင်းနှစ်ချက်ရှိတယ်ပေါ့ဗျာ။ အဲ့ဒါကတော့

(၁) Data တွေကိုမပိုင်းဘဲအကြီးကြီးအတိုင်းပဲ Network မှာသယ်ယူပို့ဆောင်ရေးလုပ်နေတာဟာ Network ကိုနှောင့်နှေးစေပါတယ်။ အကယ်၍များပေးပို့သူရော၊ လက်ခံသူပါ Bandwidth ကို ရနိုင်သလောက်သုံးဆွဲလိုက်မယ်ဆိုရင် (Data ကကြီးတာကိုး) အခြားသော ကွန်ပျူတာတွေက ဆက်သွယ်မှုကိုမပြုလုပ်နိုင်တော့ပါဘူး။ ဒါဟာအသုံးပြုသူကိုအကျိုးယုတ်စေပါတယ်။

(၂) ဒုတိယအချက်တော့ Data ကိုမပိုင်းဘဲ အကြီးအတိုင်းပဲပို့ရင် Network ကစိတ်မချရဘူးဗျ။ အကယ်၍များပေါ့နော်။ ဒီကြီးမားတဲ့ Data Packet ကြီးကို Transmission ပြုလုပ်နေစဉ်အတွင်းမှာ Error များတစ်ခုခုဖြစ်ပေါ်သွားလို့ကတော့ ဒီ Packet ကြီးတစ်ခုလုံး ပြန်ပို့ရမှာဖြစ်ပါတယ်။ ဒီတော့ အချိန်ဖင့်တာပေါ့ဗျာ။

ဒီတော့ အဲ့သလိုလုပ်မယ့်အစား အဲ့ဒီ Data ကိုအကြီးကြီးရှိရင်းစွဲအတိုင်း သယ်ယူပို့ဆောင်ကြမယ့်

အစား သေးငယ်တဲ့အပိုင်းလေးတွေအဖြစ် အများကြီးပေါ့။ Data ရှိသလောက်ပိုင်းပစ်လိုက်တယ်။ ဒီတော့ ဘာထူးလာသလဲဆိုတော့ အကယ်၍များ Data ပို့နေစဉ် Error ဖြစ်ခဲ့ရင် အဲ့ဒီဖြစ်ခဲ့တဲ့ Packets လေးကိုပဲ ပြန်ပို့ပေးရတယ်။ ဒီတော့ကောင်းတာပေါ့ဗျာ။ အချိန်မကြာဘူး။ ခုနကဆို များသွားရင်အကုန် အကြီးကြီး ပြန်ပို့ရမှာ ဒီတော့ Network ဟာစိတ်လည်းချရတယ်။ အများပြင်ရာမှာလည်းလွယ်ကူတယ်။ မြန်ဆန်တယ်။ နောက် Data တွေကို Packet အဖြစ် ပိုင်းလိုက် ခွဲလိုက်ခြင်းဖြင့် ဆက်သွယ်မှုဟာမြန်ဆန်လာမယ်။ သွက်လက်လာမယ်။ အဲ့ဒီအတွက်ကြောင့် Network ကို ကွန်ပျူတာတွေပိုသုံးနိုင်လာမယ်။

ဒီပေမယ့် တစ်ခုတော့ရှိတယ်ဗျ။ အဲ့ဒီ Data Packet လေးတွေဟာ သူတို့သွားရမယ့် ရည်ရွယ်ရာကို ရောက်သွားတဲ့အခါမှာ ၎င်းတို့ကိုလက်ခံရရှိတဲ့ ကွန်ပျူတာဟာ Packets လေးတွေကိုစုစည်းပြီး ပြန်လည်ပေါင်းစည်းပေးရပါတယ်။ Collect and Reassembles ပေါ့ဗျာ။ အဲဒီတော့ မူလ Data အဖြစ်ပြန်လည်ရောက်ရှိတော့တာဗျ။

၆.၃ Packet Structure

အခု ကျွန်တော်တို့ Data Packets လေးတွေရဲ့ ဖွဲ့စည်းတည်ဆောက်ထားပုံ Structure ကို လေ့လာကြည့်ရအောင်။ ကဲ Packets လေးတွေဟာ အပိုင်းအားဖြင့် (၃)ပိုင်းရှိကြတယ်ဗျ။ အဲ့ဒါတွေကတော့-

(၁) Header

(၂) Data

(၃) Trailer တို့ဖြစ်ကြပါတယ်။

ပုံမှာလည်းတွေ့မြင်နိုင်ပါတယ်။

Packet Header

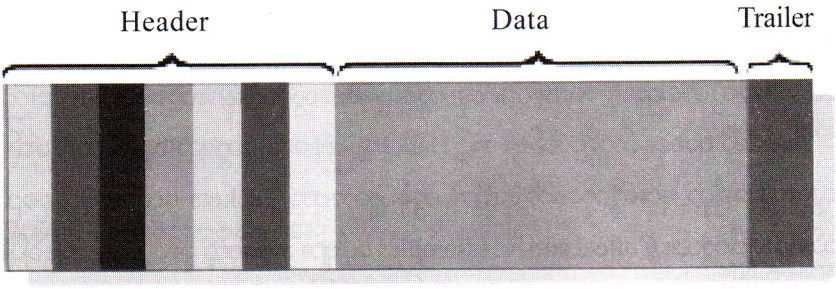
Packet တစ်ခုရဲ့ Header အပိုင်းမှာတော့ အဲ့ဒီ Packet ဖြစ်တည်လာခဲ့တဲ့ ဖြစ်တည်ရာ Source Address နှင့် ၎င်း Packet ဘယ်ဆီသွားရမယ်ဆိုတဲ့ Destination Address တို့ပါရှိပါတယ်။ အဲ့ဒီအပြင် ၎င်း Data Packet လေး Transmission ဖြစ်ဖို့အတွက် Alert Signal ဆိုတာပါရှိပါတယ်။ နောက်ပြီး Transmission Synchronize (ချိန်ကိုက်နိုင်ဖို့) ဖြစ်ဖို့အတွက် Clocking Information တွေပါဝင်ပါတယ်။

Data Section

Packet တစ်ခုရဲ့ Data Section မှာဘာတွေပါသလဲဆိုတော့ ကျွန်တော်တို့ပို့လွှတ်လိုက်တဲ့ တကယ့် Actual Data တွေပါသဗျ။ အဓိကအပိုင်းကြီးပေါ့ဗျာ။ ဒီအပိုင်းရဲ့အရွယ်အစားဟာ 512 bytes ကနေ 16

kilobytes အထိရှိနိုင်ပါတယ်။ ဘယ်အပေါ်မူတည်သလဲဆိုတော့ Network အမျိုးအစားပေါ်မူတည်ပါတယ်။ ၎င်း Data Section ကို Payload လို့လည်းခေါ်ပါတယ်။

ပုံ ၆.၁



Packet Structure ဖွဲ့စည်းပုံကိုတွေ့ရစဉ်

Packet Trailer

Packet ရဲ့အဖြီးပိုင်း နောက်တွဲ (Trail) ပိုင်းကတော့ ၎င်း Packets ရဲ့အတွင်းမှာပါတဲ့ အကြောင်းအရာတွေကိုစစ်ဆေးနိုင်ဖို့အတွက် လိုအပ်တဲ့အချက်အလက်တွေပါဝင်တယ်။ အဲ့ဒီအချက်အလက်တွေထဲမှာ Cyclical Redundancy Check ဆိုတဲ့ CRC Value တွေပါပါတယ်။ CRC Value ဆိုတာ ၎င်း Packet ကိုပို့လိုက်တဲ့ကွန်ပျူတာက Packet နှင့်ပတ်သက်နေတဲ့ တွက်ချက်ထားတဲ့ နံပါတ်တစ်ခုပဲဖြစ်ပါတယ်။ Packet ကိုလက်ခံမယ့်ကွန်ပျူတာဟာ Packet ကိုလက်ခံရရှိချိန်မှာ သူကလည်း သူ့ဘာသာသူ CRC နံပါတ်ကိုပြန်လည်တွက်ချက်ပါတယ်။ ပြီးရင် Trailer မှာပါတဲ့ CRC နံပါတ်နှင့်တိုက်ကြည့်ပါတယ်။ အဲ့သလိုတိုက်ကြည့်လိုက်တဲ့အခါမှာ ဒီ CRC နံပါတ်နှစ်ခုဟာတူညီခဲ့မယ်ဆိုရင် Packet ကိုကောင်းမွန်စွာလက်ခံရရှိတဲ့ သဘောဖြစ်ပါတယ်။ အကယ်၍များ အဲ့ဒီ CRC နံပါတ်နှစ်ခုဟာ မကိုက်ညီခဲ့ဘူးဆိုရင်တော့ လက်ခံမယ့်ဘက်က ၎င်း Packet ကိုလက်ခံခြင်းမပြုဘဲ ပယ်ချလိုက်မှာဖြစ်ပါတယ်။ ပြီးတော့ တစ်ဖက်ကို ၎င်း Packet ကိုပြန်ပို့ပေးရန်တောင်းဆို လိုက်ပါတယ်။

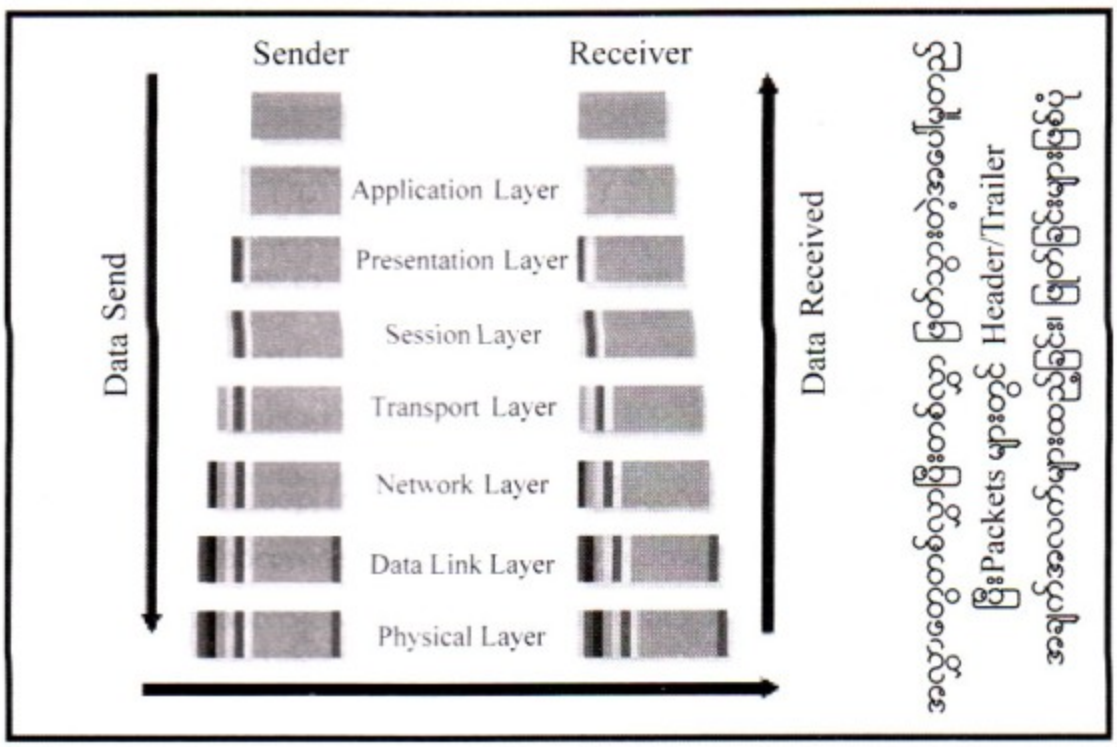
၆.၄ Packet များဖြုတ်ခြင်း

ကျွန်တော်တို့ ပြီးခဲ့တဲ့ သင်ခန်းစာတစ်ခုလုံးမှာလည်း OSI Model အကြောင်းကိုလေ့လာခဲ့ပြီးကြပါပြီ။ အခုလည်းကြည့်ရအောင်။ Data ဟာ Network မှာ ဖြတ်သန်းသွားတဲ့အခါမှာ Data ကို ပေးပို့လိုက်တဲ့ဖက်က OSI အပေါ်ဆုံးအလွှာကနေဆင်းသက်လာစေပြီးတော့ တစ်ဖက်ကလက်ခံတဲ့သူဆီမှာ OSI အလွှာကိုအောက်ကနေ အပေါ်အလွှာအထိပြန်တက်သွားတာဖြစ်ပါတယ်။ အဲ့ဒီမှာ OSI အလွှာတစ်ခုချင်းစီဟာ Header

နှင့် Trailer အချက်အလက်တွေကိုထည့်သွင်းခြင်းနှင့် ဖြုတ်ချခြင်းတို့ကိုလုပ်ဆောင်ပေးပါတယ်။ ဥပမာ ပြောရမယ်ဆိုရင် Sending Computerr ဆီက Session Layer ကနေထည့်ပေးလိုက်တဲ့ Information ကိုလက်ခံရယူသူ ကွန်ပျူတာဖက်က Session Layer ကရယူပြီး Read လုပ်ပါတယ်။

ပေးပို့မယ့် Data တွေဟာ OSI Model ကိုဝင်ရောက်လာတဲ့အခါ အလွှာတွေထဲက Transport Layer ဟာ ၎င်း Data တွေကို Packets အဖြစ်နှင့် ခွဲထုတ်လိုက်ပါတယ်။ ဒီလိုခွဲထုတ်တဲ့အခါမှာ ဒီ Transport Packet ရဲ့ Structure ဖွဲ့စည်းပုံကို ဒီကွန်ပျူတာတွေမှာ အသုံးပြုတဲ့ Protocol ကသတ်မှတ်ပေးပါတယ်။ Transport Layer က Data တွေကို Packets အဖြစ်နှင့် ခွဲထုတ်လိုက်တဲ့အခါမှာ လက်ခံမယ့်ဘက်ကွန်ပျူတာက ၎င်း Packets လေးတွေကိုအစီအစဉ်တကျ ပြန်လည်ဖွဲ့စည်းပေးနိုင်ရန်အတွက် Sequence Information ကိုပါထည့်ပေးထားရပါတယ်။ Data ဟာ Physical အလွှာကိုရောက်ရှိချိန်မှာတော့ အထက်ကအလွှာ ၆ လွှာရဲ့ အချက်အလက်တွေ Data မှာပါလာပြီဖြစ်ပါတယ်။

ပုံ ၆.၂



၆.၅ Broadcast Packets ဆိုတာ

ကျွန်တော်ရှေ့မှာပြောခဲ့ပြီးခဲ့တဲ့အတိုင်းပါပဲ။ Packets တိုင်းနဲ့ Header တိုင်းမှာ အဲ့ဒီ Packets ဖြစ်တည်ရာလိပ်စာနှင့် အဲ့ဒီ Packets သွားရမယ့်လိပ်စာ (Source and Destination Address) တွေပါရှိကြပါတယ်။ ဒါပေသိ အဲလေ ဒါပေမယ့် တော်တော်များများအခြေအနေတွေမှာတော့ Packets အတော်များများဟာ သူတို့သွားရမယ့် ဦးတည်ရာက ကွန်ပျူတာတစ်လုံးတည်းမို့ Destination Address ကတစ်ခုတည်းလေ။ ကျွန်တော်ပြောချင်တာက အကယ်၍များ ဒီ Packets က Network မှာရှိတဲ့ ကွန်ပျူတာ

တွေအားလုံးဆီကိုသွားရမယ်ဆို ဘယ်လိုဖြစ်မလဲ။ သဘောပေါက်လားမသိဘူး။ လိပ်စာတွေအများကြီးဖြစ်နေ မှာပေါ့။ ဒီလိုဗျာ။

အချို့သောအခြေအနေတွေမှာ Packets တွေမှာ ကွန်ရက်မှာရှိတဲ့ ကွန်ပျူတာတွေအားလုံးဆီကို သွားရမယ်ဆိုကြပါစို့။ အဲဒါကို ကျွန်တော်တို့ Broadcast Packets လို့ခေါ်ပါတယ်။ Network အတွင်းက ကွန်ပျူတာတွေထဲက Network Card တွေဟာ ဒီ Network အတွင်းမှာသွားလာနေကြတဲ့ Packets တွေ အားလုံးကိုမြင်တွေ့နေရပြီး Packets တွေထဲက Header Section မှာပါတဲ့ လားရာ (Destination Address) ဟာ သူတို့ကိုယ်ပိုင် Address နှင့်တူခဲ့မယ်ဆိုရင် ၎င်း Packets ကိုဖတ်လိုက်ပြီး OSI ရဲ့အပေါ်အလွှာ အထိရောက်အောင် သယ်ယူသွားပါတယ်။ အခု Broadcast Packets အခြေအနေမှာတော့ Packets ထဲက Destination လားရာ Address ဟာ ကွန်ပျူတာတိုင်းက ဖတ်နိုင်အောင်နှင့် ရယူနိုင်အောင်ခွင့်ပြုပေးထား ပါတယ်။ ဒါကို Broadcast Packets လို့ခေါ်ပါတယ်။

အဲဒီလိုအလားတူ နောက်ထပ် Packets တစ်ခုက Multicast Packets ဖြစ်ပါတယ်။ သူလည်း ကွန်ရက်အတွင်းက ဘယ်ကွန်ပျူတာအတွက်မဆိုပြုလုပ်ထားတဲ့ Packets ဖြစ်ပါတယ်။ ဒီ Multicast Packets ဆိုတာ ကျွန်တော်တို့ Video ဒါမှမဟုတ် Audio Broadcast လုပ်တဲ့ Broadcast Application တွေမှာအလုပ်လုပ်တာဖြစ်ပါတယ်။ အဲဒီမှာထုတ်လွှင့်တဲ့ တစ်ခုထဲသောဌာနကထုတ်လွှင့်လိုက်တဲ့ Data တွေကို တစ်ခုမကသော လက်ခံသူတွေကဖမ်းယူပါလိမ့်မယ်။ ဆိုလိုချင်တာက ဖမ်းယူတဲ့သူအများကြီးထဲက သူတို့နား ထောင်ချင်တဲ့ အချိန်၊ ကြည့်ချင်တဲ့အချိန်တွေမှာဖမ်းယူမှာဖြစ်ပါတယ်။

၆.၆ Protocols ဆိုတာ

Protocols ဆိုတာ ဆက်သွယ်မှု (Communication) ဖြစ်အောင် ဦးဆောင်ဦးရွက် Govern လုပ်ပေးတဲ့ Software တစ်ခုဖြစ်ပါတယ်။ ၎င်းမှာ ဆက်သွယ်မှုဖြစ်အောင်လိုအပ်တဲ့ Rules တွေ Procedures တွေပါတာပေါ့။ ဒီထက်ပိုပြီးရှင်းအောင်ပြောရမယ်ဆိုရင် ကွန်ပျူတာနှစ်လုံး ဆက်သွယ်သမှုပြုတဲ့အခါ တစ်လုံးနှင့် တစ်လုံးဟာတူညီတဲ့ ဘာသာစကားတစ်ခုကိုသုံးမှ ဆက်သွယ်မှု Communication ဖြစ်တော့မှာပေါ့။ ဆိုလိုတာက ကွန်ပျူတာတစ်လုံးက ဗမာစကားပြောနိုင်ပြီး တစ်လုံးကအင်္ဂလိပ်စကားပြောနေရင် Communication ဘယ်ဖြစ်တော့မလဲ။ ဒီတော့ အလွယ်မှတ်ထားနိုင်တာက Communication ဖြစ်အောင် လုပ်ပေး တာက Protocols ပဲ။

ကနေ့ခေတ်မှာ Protocols တွေဟာ တစ်ခုမကရှိပါတယ်။ ဒါပေမယ့်လည်း Protocols တိုင်းဟာ အခြေခံဆက်သွယ်မှု Basic Communication ကို ပံ့ပိုးပေးတာခြင်းတူပေမယ့် လုပ်ဆောင်ချက်နှင့် ရည်ရွယ် ချက်တွေကတော့ ကွဲပြားလေ့ရှိပါတယ်။ Protocols တွေဟာ သူတို့ရဲ့ Function တွေကို OSI Model မှာ အလုပ်လုပ်ကြတဲ့အခါ သူတို့ဟာ OSI ရဲ့အလွှာတစ်ခု ဒါမှမဟုတ် အလွှာတစ်ခုထက်ပိုကာ အလုပ်လုပ်

ကြပါတယ်။ တစ်ချို့ ရှုပ်ထွေးတဲ့ Protocols တွေကတော့ OSI Model ရဲ့ အလွှာအမြင့်တွေမှာ အလုပ်လုပ်ကြပါတယ်။

Protocols ဟာ တစ်ခုတည်းမဟုတ်ဘဲ နှစ်ခုတစ်စုံ အလုပ်ကိုအတူတကွလုပ်ခဲ့မယ်ဆိုရင် ၎င်းကို Protocols Stack သို့တည်းမဟုတ် Protocols Suite လို့ခေါ်ပါတယ်။ အဲ့ဒီ Protocols Stack ကို ဥပမာအားဖြင့် ဖော်ပြရမယ်ဆိုရင် TCP/ IP (အင်တာနက်အတွက်Protocol Suite) ဖြစ်ပြီး နောက်တစ်ခုက IPX/ SPX (Novell NetWare Protocol Suite) တို့ဖြစ်ကြပါတယ်။

၆.၇ Protocols က အသုံးပြုသော Data ဖိုဒြင်းနည်းလမ်းများ

ကွန်ရက်မှာ Data တွေကိုပေးပို့တဲ့နေရာမှာ ပေးပို့တဲ့ Methods နှစ်မျိုးရှိပါတယ်။ အဲ့ဒီတွေကတော့

(၁) Connectionless နှင့်

(၂) Connection Oriented တို့ဖြစ်ကြပါတယ်။

Connetion Less

Connectionless ဆိုတဲ့နည်းကိုသုံးတဲ့ Protocols တွေဟာ Data တွေကိုပေးပို့ရာမှာ ကွန်ယက်ပေါ်ကို Data တွေတင်ပေးလိုက်ရုံပဲဖြစ်ပါတယ်။ အဲ့ဒီ Data တွေကို သက်ဆိုင်ရာက သူဘာသာသူရယူသွားမယ်ဆိုတဲ့သဘောပဲဖြစ်ပါတယ်။ ဒီတော့ Connectionless Protocols ဟာလုံးဝစိတ်ချရတဲ့အနေအထားမှာတော့ မရှိပါဘူး။ ဒါပေမယ့် Connectionless Protocols ကမြန်တယ်ဗျ။ ဘာလို့လဲဆိုတော့ သူကကိစ္စတွေအများကြီး မရှိပါဘူး။ ဆိုလိုတာက Connection တွေကို စတင်ပြုလုပ်ခြင်း Establishing၊ ထိန်းချုပ်ခြင်း Managing နှင့် Connection တွေကို ဖျက်ချခြင်း Tear Down စတာတွေကိုမပြုလုပ်ရတာကြောင့် အချိန်မကုန်ဘဲ မြန်ဆန်တာဖြစ်ပါတယ်။ ၎င်း Connectionless နည်းကိုသုံးတဲ့ Protocol ဟာ ကွန်ရက်မှာ Data တွေကို သယ်ယူပို့ဆောင်တဲ့အခါ Packet တွေကိုစိတန်းခြင်း၊ Sequencing နှင့် Sorting ပြုလုပ်ခြင်းတို့ကို Higher Layer က တာဝန်ယူခြင်းကြောင့် Communication ကမြန်ဆန်ချောင်းလည်းဖြစ်ပါတယ်။ ဒီ Connectionless ဆက်သွယ်မှုထဲက Package လေးတွေကို Datagram လို့လည်းခေါ်ပါတယ်။

Connection Oriented

Connection Oriented Protocols ကြတော့ Connectionless ထက်ပိုပြီး Reliable စိတ်ချရတယ်ဗျ။ ဒါပေသိ သူ့လောက်တော့ မမြန်ဘူး။ Connection Oriented Protocol ကိုအသုံးပြုတဲ့အခါ ကွန်ပျူတာနှစ်လုံးဟာ သူတို့အချင်းချင်းဆက်သွယ်မှု Communication ကိုမပြုမီ အပေါ်တွန်းကပြောခဲ့သလို

Connection ကိုဦးစွာတည်ဆောက် Establish အရင်လုပ်ရပါတယ်။ Connection ဟာ Established ဖြစ်ပြီးတာနဲ့ Data တွေဟာ တန်းစီပြီးထွက်လာကြပါတော့တယ်။ Packets တစ်ခုချင်းစီဟာ ရည်ရွယ်ရာကို ရောက်ပြီဆိုတာနှင့် ရရှိပြီးဖြစ်ကြောင်း အသိအမှတ်ပြု Acknowledge ထုတ်ပေးပါတယ်။ အကယ်၍များ Error တစ်ခုခုဖြစ်ပေါ်ခဲ့မယ်ဆိုရင်တော့ Packet ကိုပြန်ပို့ပေးခိုင်းပါတယ်။ ဆက်သွယ်မှုပြီးဆုံးတဲ့အခါ Connection ကိုဖြုတ်ချလိုက်ပါတယ်။ Terminate လုပ်လိုက်တယ်ပေါ့ဗျာ။ ဒီတော့ပြန်ပြောရရင် Data တွေကိုအားလုံးလက်ခံရရှိကြရဲ့လား။ ရရှိလာတဲ့ Data တွေကရောမှန်ကန်ရဲ့လား။ အားလုံးသေချာအောင် ပြုလုပ်ရပါတယ်။ ဒီလိုမှမဟုတ်ဘဲ သတ်မှတ်ချိန်အတွင်း အောင်မြင်ပြည့်စုံတဲ့ Communication မဖြစ်ရင်လည်း သင့်တော်တဲ့ Error Message ကိုထုတ်ပေးရပြန်ပါတယ်။

နောက်ထပ်နည်းလမ်းများ

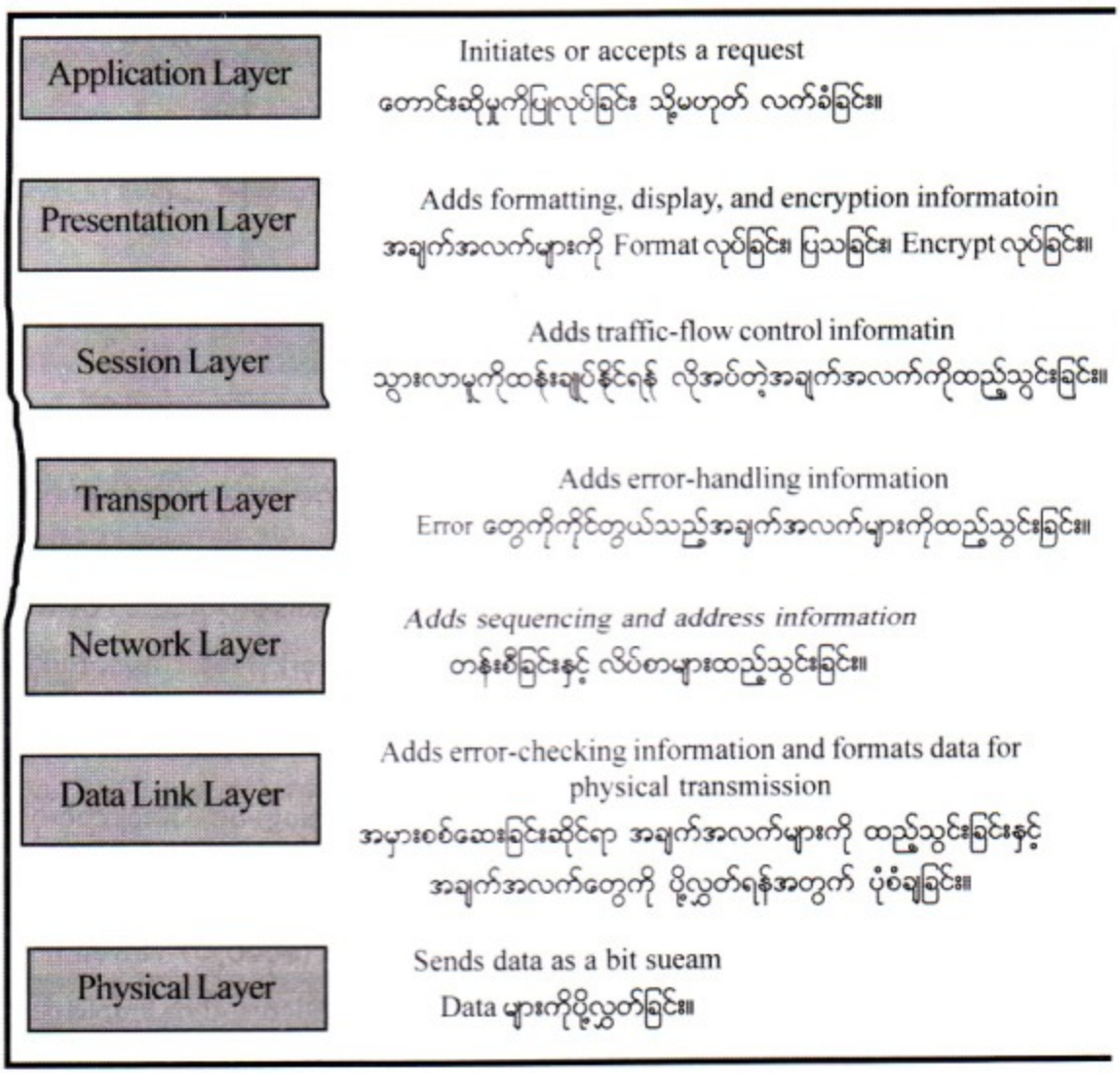
OSI Model ရဲ့ Network Layer ဟာ Data တွေကိုများစွာသော ကွန်ရက်တစ်လျှောက် ရွှေ့လျားစေဖို့တာဝန်ရှိပါတယ်။ အဲကို ပြီးခဲ့တဲ့သင်ခန်းစာတွေတုန်းက ပြောခဲ့ပြီးပါပြီ။ ဒီလိုမျိုး Data တွေရွှေ့လျားစေဖို့တာဝန်ရှိတဲ့ပစ္စည်းကတော့ Router ဖြစ်ပြီး ၎င်းဖြစ်စဉ်ကိုတော့ Routing လို့ခေါ်တာဖြစ်ပါတယ်။ အဲပေမယ့် သိထားရမှာက Protocol Suite တိုင်းဟာ Network Layer Protocol Suite တွေမဟုတ်ကြသလို Network Layer တိုင်းမှာလည်း အလုပ်လုပ်ကြတာမဟုတ်ပါဘူး။ ဒီတော့ Network Layer မှာ အလုပ်လုပ်တဲ့ Protocol Suite ကို Routable လို့ခေါ်ပြီး Network Layer မှာအလုပ်မလုပ်တဲ့ Protocol ကတော့ Nonroutable လို့ခေါ်ပါတယ်။ TCP/ IP နှင့် IPX/ SPX တို့ဟာ ကြီးမားတဲ့ကွန်ရက်တွေအတွက် သင့်တော်တဲ့ Routable Protocols တွေဖြစ်ကြပါတယ်။ NetBEUI ကတော့ သေးငယ်တဲ့ကွန်ရက်တွေအတွက် သင့်တော်တဲ့ Nonroutable Protocol ဖြစ်ပါတယ်။ အဲပေမယ့်သိရမှာက ကွန်ရက်ဟာထပ်မံပြီးကြီးထွားလာဦးမယ်ဆိုရင်တော့ NetBEUI က Performance ကျလာတတ်ပါတယ်။ အဲကြောင့်မို့ ကျွန်တော်တို့ဟာ ကွန်ရက်ကိုတပ်ဆင်ရာမှာ လက်ရှိကွန်ရက်ရဲ့အရွယ်အစားနှင့် နောက်ထပ်တိုးလာမယ့် ကွန်ရက်ရဲ့အရွယ်အစားကိုကြည့်ပြီး ဘယ်လို Protocol ကိုသုံးရမယ်ဆိုတာ ရွေးချယ်ရပါတယ်။

၆.၈ Layer နည်းဥပဒေခဲ့က Protocols များ

ကျွန်တော်တို့ဟာ Protocols အများစုကိုရှင်းပြတဲ့အခါမှာဖြစ်စေ၊ အလွှာလိုက်ရှင်းပြတဲ့အခါမှာဖြစ်စေ OSI Model တွေရဲ့အလွှာနှင့်ယှဉ်ပြီးပြောကြပေမယ့် တကယ်တမ်းမှာ Protocols တွေဟာ OSI Model နှင့်တစ်ထပ်တည်းကျအောင် Map လုပ်ထားချင်မှ လုပ်ထားပါလိမ့်မယ်။ ဆိုလိုတာက Protocol Suite အဲမှမဟုတ် Protocol Stack တွေဟာ Protocols တွေကိုပေါင်းထားပြီးအတူတကွ Network Communications ဖြစ်အောင်ပြုလုပ်ကြတာဖြစ်ပါတယ်။ ဒီတော့ ဒီ Protocol Stack တွေမှာမှ Protocol တစ်ခုချင်းစီဟာ

အလွှာတစ်လွှာချင်းစီအတွက် ကိုယ်ပိုင်သတ်မှတ်ထားတဲ့ Rules တွေ တိကျတဲ့ Function တွေနှင့် အလုပ်လုပ်ကြတာပါ။ အခုပြောခဲ့သမျှအားလုံးကို အချုပ်ပြန်ပြောရရင် Protocols တွေဟာ OSI Model နှင့်ယှဉ်ပြီး ပြုလုပ်ထားပေမယ့် တစ်လွှာချင်းစီအလိုက်တော့ ထပ်တူကျချင်မှာကျလိမ့်မယ်။ ပြီးခဲ့တဲ့သင်ခန်းစာတုန်းက ပြောခဲ့တဲ့ OSI Model ကိုပြန်ပြီးတော့ အောက်မှာရှင်းပြထားပါတယ်။

ပုံ ၆.၃



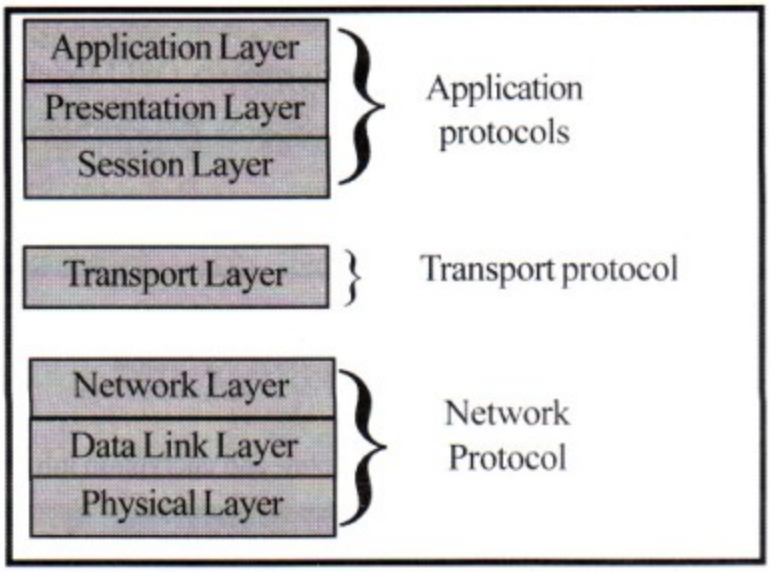
အောက်မှာဆက်လက်ပြီးလေ့လာကြည့်ပါဦး။ Protocol တွေဟာ အုပ်စုလိုက်ခွဲမယ်ဆိုရင် (၃)မျိုးရှိတယ်ဆိုတဲ့အကြောင်းပြောထားပါတယ်။ အဲဒီ Protocol အုပ်စု(၃)မျိုးကတော့

(၁) Application Protocols

(၂) Transport Protocols

(၃) Network Protocols တို့ဖြစ်ကြပါတယ်။

ပုံ ၆.၄



Network Protocols

Network Protocol တွေဟာ ဘာတွေကိုပံ့ပိုးပေးကြသလဲဆိုတော့ (Addressing) လိပ်စာပိုင်းဆိုင်ရာနှင့် (Routing) လမ်းကြောင်းလွှဲခြင်းဆိုင်ရာအချက်အလက်တွေ၊ အမှားစစ်ဆေးခြင်း (Error Checking) ပိုင်းဆိုင်ရာတွေပြန်ပို့ပေးပါဆိုတဲ့တောင်းဆိုမှု (Retransmission Request) တွေ၊ ဆက်သွယ်မှုအတွက် လိုအပ်တဲ့ (Rules) တွေစသည်ဖြင့်ဖြစ်ကြပါတယ်။ Network Protocols ကပံ့ပိုးပေးတဲ့ ဝန်ဆောင်မှု Services ကိုပြောရမယ်ဆိုရင် Link Service ပဲဖြစ်ပါတယ်။ Network Protocols အချို့ကိုအောက်မှာ ဖော်ပြပေးထားပါတယ်။

(၁) IP (Internet Protocol) -လိပ်စာပိုင်းဆိုင်ရာ (Addressing) နှင့် လမ်းကြောင်းပိုင်းဆိုင်ရာ (Routing) အချက်အလက်တွေကိုပံ့ပိုးပေးပါတယ်။

(၂) IPX (Internetwork Packet exchange) နှင့် NWLink (အဓိကမဟုတ် Novell IPX ODI Protocol) - Novell ရဲ့ Protocol နှင့် Microsoft က Implement လုပ်တဲ့ Novell ရဲ့ Protocol တို့ဖြစ်ကြပါတယ်။ Packet များ Routing လုပ်ဖို့အတွက် ဖြစ်ပါတယ်။

(၃) NetBEUI - IBM နှင့် Microsoft တို့က Developed လုပ်ခဲ့သော Network Protocol ဖြစ်ပါတယ်။ သူကတော့ NetBIOS အတွက် Transport Sevices ကိုပံ့ပိုးပေးပါတယ်။

(၄) DDP (Delivery Datagram Protocol) - Apple Talk မှာအသုံးပြုတဲ့ Apple ရဲ့ Data Transport Protocol ဖြစ်ပါတယ်။

(၅) DLC (Data Link Control) - အဓိကအားဖြင့်တော့ Network မှာချိတ်ဆက်ထားတဲ့ Hewlett- Pack and (HP) Printors တွေနှင့် Main frames တွေနှင့်ချိတ်ဆက်တဲ့ IBM Terminals တွေမှာအသုံးပြုတဲ့ Network Protocol ဖြစ်ပါတယ်။

Transport Protocol များ

Transport Protocol ဟာအချက်အလက်တွေကို ကွန်ပျူတာဆီပေးပို့ခြင်းတွေကို ကိုင်တွယ်ပါတယ်။ Data တွေကိုသယ်ယူပို့ဆောင်ရာမှာစိတ်ချရတဲ့ Protocol ဖြစ်ပါတယ်။

(၁) TCP (Transmission Control Protocol). TCP/IP Protocol ဖြစ်ပါတယ်။

(၂) SPX (Sequenced Packet exchange) နှင့် NWLink (Microsoft မှအကောင်အထည်ဖော်သော SPX) - Data သယ်ယူပို့ဆောင်ရာတွင် အာမခံချက်ကောင်းကောင်းဖြင့် စိတ်ချရသော Novell ၏Connection - Oriented Protocol ဖြစ်ပါသည်။

(၃) ATP (Apple Talk Transmission Protocol) and NBP (Name Binding Protocol) - Apple Talk ၏ Session နှင့် Data တွေကိုသယ်ယူပို့ဆောင်ပေးသော Protocol ဖြစ်ပါသည်။

(၄) Net BIOS / Net BEUI - Net BIOS က ကွန်ပျူတာတွေကြားဆက်သွယ်မှု Communication ကိုပြုလုပ်ပေးခြင်း (Establishes) နှင့် ထိန်းချုပ်ခြင်း (Manage) ကိုပြုလုပ်ပေးပါတယ်။ Net BEUI ကတော့ ဖြစ်ပေါ်လာတဲ့ဆက်သွယ်မှု (Communication) ပေါ်မှာ Data တွေကိုသယ်ယူပို့ဆောင်ပေးပါတယ်။ Net BIOS ဟာ TCP/IP နှင့် IPX/SPX ပေါ်မှာပါ Run နိုင်သောကြောင့် Net BIOS ကို အသုံးပြုလျှင် Net BEUI ကိုအသုံးပြုဖို့မလိုအပ်ပါဘူး။

Application Protocol များ

Application Protocols တွေဟာ OSI Model ရဲ့အပေါ်အလွှာတွေမှာ Operate လုပ်တာဖြစ်ပါတယ်။ Application တစ်ခုမှအခြား Application တစ်ခုသို့ ဝန်ဆောင်မှုပေးတာဖြစ်ပါတယ်။

၁။ SMTP - (Simple Mail Transport Protocol) - TCP/IP Protocol Suite ရဲ့ အဖွဲ့ဝင်တွေဖြစ်ကြပါတယ်။ E-Mail တွေကို Transfer လုပ်ဖို့တာဝန်ယူရပါတယ်။

၂။ FTP - (File Transfer Protocol) - TCP/IP Protocol Suite ရဲ့ နောက်ထပ်အဖွဲ့ဝင်တစ်ခုပဲဖြစ်ပါတယ်။ File တွေကို Transfer လုပ်ပေးတဲ့ Protocol ဖြစ်ပါတယ်။

၃။ SNMP - (Simple Network Management Protocol) - TCP/IP Protocol ထဲကပဲဖြစ်ပါတယ်။ Network Devices တွေကိုစောင့်ကြည့်ခြင်းနှင့်ထိန်းချုပ်ခြင်းတို့မှာအသုံးပြုပါတယ်။

၄။ NLP - (NetWare Lone Protocol) - Novell ၏ Client Shells နှင့် Redirector ဖြစ်ပါတယ်။

၅။ AFP (Apple Tallk File Protocol) - Apple ၏ Remote File ထိန်းချုပ်ခြင်း Protocol ဖြစ်ပါတယ်။

၆.၉ Comman Protocols များ

ကျွန်တော်ပြောခဲ့ပြီးပါပြီ။ Protocols တွေကတော့အများကြီးပေါ့ဟုတ်လား။ ဒါပေမယ့် Protocol တစ်ခုချင်းစီတိုင်းမှာ အားသာချက်၊ အားနည်းချက်လေးတွေရှိကြတယ်ဗျ။ တစ်ချို့ Protocol တွေက ကွန်ပျူတာအချင်းချင်းဆက်သွယ်တဲ့အခါမှာသုံးကြပြီး အချို့ကတော့ Wide Area Network (WAN) ပေါ်ကနေ Local Area Network (LAN) တပ်ဆင်ခြင်းတွေမှာလည်းအသုံးပြုကြပါတယ်။ အောက်မှာဘုံအသုံးပြုတတ်ကြတဲ့ Protocols တွေကိုပြပေးထားပါတယ်။

(၁)	TCP/IP	(၂)	DLS
(၃)	NWLink (IPX/SPX)	(၄)	XNS
(၅)	NetBIOS/NetBEUI	(၆)	DECNet
(၇)	Apple Talk	(၈)	X.25 တို့ဖြစ်ကြပါတယ်။

၆.၁၀ NetBIOS နှင့် NetBEUI

၁၉၈၀ အစောပိုင်းနှစ်များကတည်းက IBM ဟာ Sytek ဆိုတဲ့ကုမ္ပဏီကိုငှားရမ်းပြီး ရိုးရှင်းပြီးအခြေခံကျတဲ့ Network Programming Interface ကိုပြုလုပ်စေပါတယ်။ အဲဒါဟာ NetBIOS ဆိုတဲ့ Network Basic Input/Output System ဆိုတာဖြစ်လာစေတာပါပဲ။ ၁၉၈၀ နှစ်များအလယ်ပိုင်းလောက်ကြတော့ Microsoft ရယ်၊ 3 Com ရယ်၊ IBM ရယ် သုံးခုပေါင်းပြီး OS/2 နှင့် LAN Manager အတွက် Protocol Suite ကိုထုတ်လုပ်ခဲ့ပါတယ်။ NetBIOS ဟာ Application Layer တွေကိုပံ့ပိုးပေးနိုင်တာကြောင့် အခုအခါမှာတော့ ၎င်းအဖွဲ့အစည်းဟာ အောက်ပိုင်းအလွှာတွေကိုပံ့ပိုးပေးမယ့် Lower-Layer Protocol ကိုထုတ်လုပ်ခဲ့ပါတယ်။ အဲဒါဟာ NetBIOS ကို Extend လုပ်ထားတာကြောင့် NetBIOS Extended User Interface (NetBEUI) လို့ခေါ်ပါတယ်။ ၎င်းဟာ OSI Model ရဲ့ အလွှာ ၂၊ ၃ နှင့် ၄ တို့ကိုပေါင်းကူးဆက်စပ်ပေးထားတာဖြစ်ပါတယ်။ NetBIOS နှင့် NetBEUI တို့ဟာ စပြီးအခြေတည်လာကတည်းက Small to Medium အရွယ်အစားရှိတဲ့ Network တွေအတွက်သာလျှင်ဖြစ်ပါတယ်။ ကွန်ပျူတာနှင့်

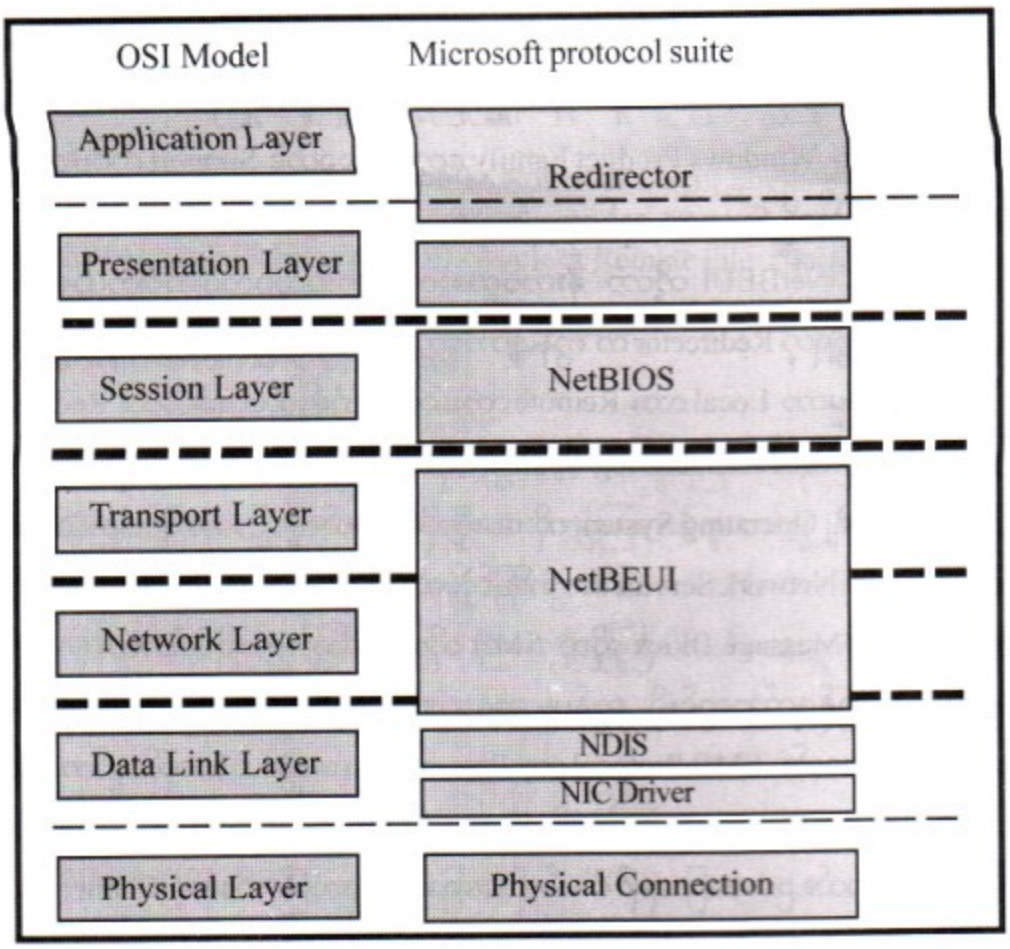
ပြောမယ်ဆိုရင်တော့ ကွန်ပျူတာ ၂လုံးကနေ ၂၅၀လုံးအထိလောက်အတွက်သာ ဒီဆိုင်းဆွဲထုတ်လုပ်ထားတာ ဖြစ်ပါတယ်။ NetBIOS ရော NetBEUI ရောပါ ယနေ့အထိအသုံးပြုလျက်ရှိကြပါသေးတယ်။ Microsoft ဟာ NetBEUI ကို ၎င်းရဲ့ Windows Product Family တွေမှာ ယခုတိုင် Support လုပ်ပါတယ်။ Windows 2000 မှာတောင် ၎င်းကို Support လုပ်ထားပါသေးတယ်။

NetBIOS နှင့် NetBEUI တို့ဟာ နီးကပ်စွာအတူတကွအလုပ်လုပ်ကြပါတယ်။ ပုံမှာလည်း တွေ့နိုင်ပါတယ်။ အဲဒီမှာတွေ့ရတဲ့ Redirector က ကွန်ပျူတာတွေဆီတောင်းဆိုမှုတွေကို ဘာသာပြန်ပေးတယ်။ နောက်ပြီး ၎င်းတောင်းဆိုမှုဟာ Local လား Remote လားဆိုတာ ဆုံးဖြတ်ပေးပါတယ်။ Redirector ဟာ Local Request တွေကို Local Operating System ကိုပေးပို့လိုက်ပါတယ်။ ဆိုလိုတာက ဒီစက်ကတောင်းဆိုတာကို ဒီစက်ရဲ့ Operating System ကို ပေးပို့လိုက်တယ်လို့ပြောတာဖြစ်ပါတယ်။ အကယ်၍ တောင်းဆိုမှုဟာ Remote Network Service အတွက်ဖြစ်ခဲ့မယ်ဆိုရင် ၎င်းရဲ့အောက်ဖက်ကိုလွှဲလိုက်ပါတယ်။ ဒီနေရာမှာတော့ Server Message Block ဆိုတဲ့ SMB တို့ရောက်သွားတာဖြစ်ပါတယ်။

SMB ဟာ ကွန်ရက်အတွင်းရှိ ကွန်ပျူတာတွေအချင်းချင်းအကြား အချက်အလက်တွေကို ပေးပို့လွှဲပေးနေတာဖြစ်ပါတယ်။ SMB Protocol ဟာ Presentation အလွှာမှာ အလုပ်လုပ်တာဖြစ်ပါတယ်။ Microsoft Network တွေဟာ Redirector နှင့် Server Software တွေအကြား Communication ဖြစ်ဖို့ အသုံးပြုနေကြပါတယ်။ ဥပမာပြောရရင် ဘယ်လိုအခြေအနေမျိုးလည်းဆိုတော့ Client ကွန်ပျူတာက File Server ကနေ File List ကိုတောင်းခံတဲ့အခါမျိုးတွေမှာပေါ့။ SMB ဟာ Microsoft LAN Manager Server ဆီကို Client Connecetion ချိတ်ဖို့တောင်းခံတဲ့အခါမှာလည်း အသုံးပြုပါတယ်။ Redirector ဟာ အခြားပစ္စည်းတစ်ခု အလုပ်လုပ်ဖို့ရန် လိုအပ်တဲ့ Transmission အတွက် SMB တောင်းဆိုမှုတွေကိုပြန်လည် ထုတ်ပိုးပေးရပါသေးတယ်။

Session Layer ဟာ ကွန်ပျူတာနှစ်လုံးဆီကအသုံးပြုတဲ့ Application တွေအကြား ဆက်သွယ်မှုကို ထိန်းချုပ်ပေးရန်တာဝန်ရှိပါတယ်။ NetBIOS က ဒီအလွှာမှာအလုပ်လုပ်ပြီး ဒီ Connection တွေကို ဖြစ်ပေါ်စေဖို့ နှင့် ထိန်းသိမ်းဖို့ရန် အလုပ်လုပ်ပါတယ်။ NetBEUI ကတော့ Transport Layer မှာ အလုပ်လုပ်ပြီး ကွန်ပျူတာနှစ်လုံးကြားဆက်သွယ်မှုကို ထိန်းချုပ်ပေးရပါတယ်။ ၎င်းဟာ Network Layer မှာလည်း အလုပ်လုပ်ပါတယ်။ ဒါပေမယ့် ၎င်းဟာ Nonroutable Protocol ဖြစ်တာကြောင့် ဒီအလွှာကိုကျော်ထားပါတယ်။ ပုံမှာလည်း တွေ့မှာပါ။ NetBEUI Packet တွေဟာ မူရင်းနှင့် လားရာအချက်အလက် (Source နှင့် Destination Network Information)တွေအတွက် Space မပါရှိပါဘူး။

ပုံ ၆.၅



NetBIOS

NetBIOS ဟာပြောပြခဲ့ပြီးတဲ့အတိုင်း Session အလွှာမှာအလုပ်လုပ်ပြီး Peer to Peer Network Application ကို Support လုပ်ပါတယ်။ NetBIOS ကွန်ရက်မှာ ကွန်ပျူတာတစ်လုံးချင်းစီကို မတူညီတဲ့ Character ၁၅လုံးနှင့် သတ်မှတ်ပေးရပါတယ်။ NetBIOS ဟာ ကွန်ပျူတာရဲ့ နာမည်ကိုကြေညာပေးပါတယ်။ ပြောရမယ်ဆိုရင် ကွန်ပျူတာဟာ ကာလအပိုင်းအခြားတစ်ခုအလိုက် NetBIOS နာမည်ကိုကြေညာပေးနေတာကြောင့် အခြားကွန်ပျူတာတွေက ဆက်သွယ်နိုင်တာဖြစ်ပါတယ်။ Network မှာရှိတဲ့ ကွန်ပျူတာတိုင်းဟာ ထုတ်လွှင့်တဲ့ ကွန်ပျူတာရဲ့ နာမည်နှင့် Hardware Address တွေကိုသိမ်းဆည်းထားကြရပါတယ်။ အကယ်၍များ ကွန်ပျူတာဟာ နောက်ကွန်ပျူတာတစ်ခုနှင့်ဆက်သွယ်ချင်တဲ့အခါ အဲ့ဒီကွန်ပျူတာရဲ့ နာမည်ကသိမ်းထားတဲ့အထဲ မရှိရင် အဲ့ဒီကွန်ပျူတာရဲ့ Hardware Address ကိုသိလိုပါတယ်ဟူ၍ တောင်းဆိုခြင်းကိုပြုရပါတယ်။

NetBIOS ဟာ Connection Oriental Protocol ဖြစ်တာကြောင့် Network Connection တွေကိုဖြစ်ပေါ်စေခြင်း (Establishing)၊ ထိန်းသိမ်းပေးရခြင်း (Maintaining) နှင့်ရပ်စဲပစ်ခြင်း (Terminating) တို့ကိုပါလုပ်ဆောင်ရပါတယ်။ အကယ်၍များလိုအပ်ခဲ့ရင် NetBIOS ကို Connectionless

ဆက်သွယ်မှုအဖြစ်အသုံးပြုနိုင်ပါတယ်။ NetBIOS ဟာ NetBEUI နှင့် နီးကပ်စွာဆက်နွယ်သလို အခြားသော Lower Layer အလွှာနိမ့် Protocol တွေဖြစ်ကြတဲ့ TCP/IP နှင့် IPX/SPX တို့နှင့်လည်း တွဲလုပ်နိုင်ပါတယ်။ NetBIOS ဟာ Nonroutable Protocol ဖြစ်ပါတယ်။ အဲပေမယ့် Transport ကိစ္စတွေအတွက် Routable Protocol ကို အသုံးပြုထားရင် ၎င်းဟာ Router လုပ်လို့ရနိုင်ပါတယ်။

NetBEUI

NetBEUI ဟာ သေးငယ်တယ်။ မြန်တယ်။ Nonroutable ဖြစ်တဲ့ Transprot အလွှာနှင့် Data Link အလွှာ Protocol ဖြစ်ပါတယ်။ သေးငယ်တဲ့ကွန်ရက်တွေမှာ NetBIOS နှင့်အတူ အသုံးပြုနိုင်အောင် ဒီဇိုင်းဆွဲထားတာဖြစ်ပါတယ်။ NetBEUI 3.0 ဟာ IBM ရဲ့ NetBEUI ကို Microsoft က ပိုမိုကောင်းမွန်အောင်ပြုလုပ်ထားတာကြောင့် ၎င်းဟာ Microsoft ကွန်ရက်တွေမှာပဲ အလုပ်လုပ်ပါတယ်။ ပြောရမယ်ဆိုရင် Microsoft ရဲ့အားလုံးသော Windows Product Family တွေတိုင်းမှာပါပါတယ်။ ဟိုးအရင်က Windows for Workgroup ကနေစပြီးတော့ပေါ့။ Network ကသေးငယ်မယ်ဆိုရင်တော့ NetBEUI ကို သုံးရတာအဆင်ပြေမှာပါ။ မြန်လည်း မြန်တယ်လေ။ NetBIUI ဟာ Route မလုပ်ပေးနိုင်ပါဘူး။ အဲကြောင့် သေးငယ်တဲ့ကွန်ရက်တွေအတွက်ပဲကောင်းပါတယ်။

၃.၁၁ IPX/ SPX အကြောင်း

IPX/ SPX ဟာ Novell ရဲ့ NetWare Network Operating System မှာသုံးတဲ့ Protocol Suite ဖြစ်ပါတယ်။ Novell ဟာ ဒီ IPX/ SPX Protocol Suite ကို ယနေ့ခေတ် NetWare နောက်ဆုံး Version အထိ Support လုပ်ထားဆဲဖြစ်ပါတယ်။ အဲဟာ တကယ်တော့ယခင် NetWare Version အဟောင်းတွေကိုသုံးနေဆဲ၊ သုံးနေခဲ့မယ်ဆိုရင် Backward Compatibility ရအောင်လို့ဖြစ်ပါတယ်။ ဘာလို့ အဲလိုပြောရလဲဆိုရင် ကနေ့ခေတ်မှာ NetWare ကိုသုံးနေခဲ့မယ်ဆိုရင်တောင် TCP/IP ဆိုတဲ့ Protocol ဟာ Network လောကမှာရွေးချယ်စရာ Protocol Suite တစ်ခုဖြစ်နေလို့ပါပဲ။

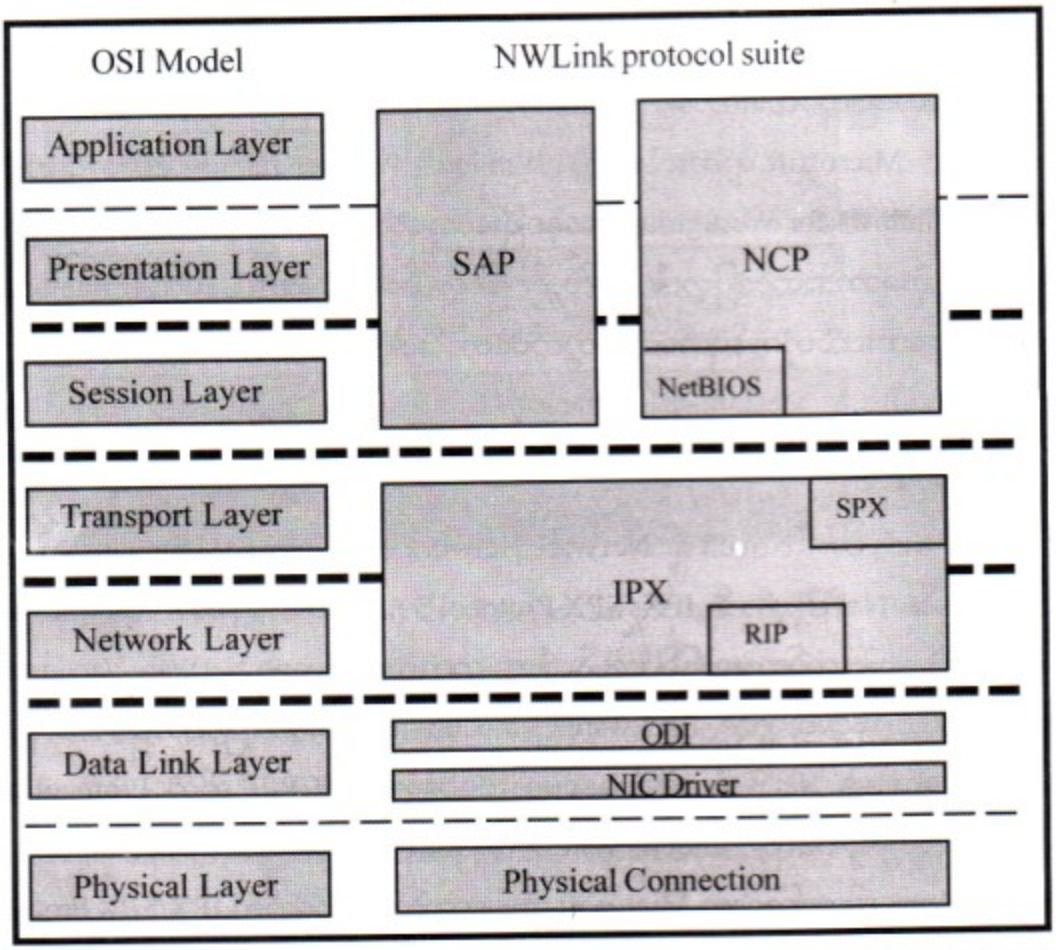
NWLink ဆိုတာကြတော့ Microsoft ကအကောင်အထည်ဖော်တဲ့ IPX/SPX Protocol Suite ဖြစ်ပါတယ်။ Novell NetWare နှင့် IntraNetWare တို့မှာအသုံးပြုပါတယ်။ ပုံမှာလည်း NWLink ကို OSI Model နှင့် နှိုင်းယှဉ်ပြီးပြထားပါတယ်။ Windows 98 မှာ Microsoft ဟာ ၎င်းကိုနှစ်မျိုးခေါ်ပါတယ်။ Windows 98 Release 1 မှာ IPX/SPX - Compatible Protocol လို့ခေါ်ပြီး Windows 98 Release 2 မှာတော့ Novell IPX ODI Protocol လို့ခေါ်ပါတယ်။

NetWare Version အဟောင်းနှင့် Server တွေကို Connections ချိတ်ဆက်လို့ရရန် Windows NT နှင့် Windows 2000 မှာလည်း NWLink ဟာပါရှိပြန်ပါတယ်။ ၎င်းဟာ Route လုပ်ပေးနိုင်သော

Protocol ဖြစ်ပါတယ်။ IPX/SPX ဟာ NetBEUI ထက်စာရင် Network ကိုချဲ့ထွင်ရ ပိုလွယ်ပါတယ်။

IPX/SPX အိမှမဟုတ် NWLink ကိုအသုံးပြုရာမှာ အရေးတကြီး အဓိကစဉ်းစားရမှာက ဘယ် Ethernet Frame Type ကိုအသုံးပြုသလဲဆိုတာပါပဲ။ လောလောဆယ် ဒီနေရာမှာ Frame Type ဆိုတာ ဘာလဲဆိုတဲ့အကြောင်းကို ရှင်းပြဦးမှာမဟုတ်ပါဘူး။ သိထားရမှာက ကွန်ရက်အတွင်းရှိ ကွန်ပျူတာတွေဟာ ဆက်သွယ်မှုကိုပြုလုပ်နိုင်ရန် Frame Type ကိုတူညီစွာအသုံးပြုရမယ်ဆိုတာပါပဲ။ အကယ်၍များ ကွန်ရက်ထဲက ကွန်ပျူတာတွေဟာ IPX/SPX ကိုအသုံးပြုထားပြီး ကွန်ရက်ချိတ်ဆက်ရာမှာ ဆက်သွယ်မှုမဖြစ်ဘူး၊ Communicate မဖြစ်ဘူးဆိုရင် ကွန်ပျူတာတိုင်းမှာ အဲဒီ Frame Type ကိုပြန်စစ်ပေးဖို့လိုပါလိမ့်မယ်။

ပုံ ၆.၆



Open Data-Link Interface (ODI)

ODI ဟာ Microsoft ရဲ့ Network Device Interface Specification ဆိုတဲ့ NDIS ပဲဖြစ်ပါတယ်။ ၎င်းဟာ Network Driver တစ်ခုတည်းနဲ့ Multiple Protocol ကို Support လုပ်နိုင်ပါတယ်။ ကွန်ပျူတာထဲက Network Card တစ်ခုတည်းနှင့် Multiple Protocol ကို အသုံးပြုပြီး ကွန်ရက်ဆက်သွယ်မှု ပြုလုပ်နိုင်ပါတယ်။

Internetwork Packet Exchange (IPX)

IPX ဟာ Transport အလွှာနှင့် Network အလွှာ Protocol ဖြစ်ပါတယ်။ ၎င်းဟာ ကွန်ရက်ပေါ်မှာ အားလုံးသော Address ပိုင်းဆိုင်ရာနှင့် Route လမ်းကြောင်းပိုင်းဆိုင်ရာတွေကိုကိုင်တွယ်တာဖြစ်ပါတယ်။ Workstation ကတော့ Network Card ရဲ့ MAC ဆိုတဲ့ Hardware Address ကိုအသုံးပြုပြီး Identify လုပ်ပါတယ်။ ၎င်း IPX ဟာ Connectionless Protocol ဖြစ်ပါတယ်။ ဒါကြောင့် မြန်တော့ မြန်တယ် စိတ်သိပ်မချရပါဘူး။

Routing Information Protocol (RIP)

အကြမ်းအားဖြင့်တော့ TCP/IP ရဲ့ RIP Protocol ပေါ်အခြေခံထားပါတယ်။ Server နှင့် Router တွေဟာ Network Address နှင့် Topology တွေရဲ့ Information တွေကိုလဲလှယ်ရန် IPX RIP ကိုအသုံးပြုကြပါတယ်။ RIP ဟာ Distance - Vector Protocol ဖြစ်ပါတယ်။ ၎င်းဟာ Points တွေကြားထဲက Hops တွေကိုအသုံးပြုပြီး ပို့လွှတ်သူ (Sender) နှင့် လက်ခံသူ (Receiver) အကြား Packet တွေကို အကောင်းဆုံး ဘယ်လမ်းကြောင်းနှင့် သယ်ဆောင်မလဲဆိုတာ ဆုံးဖြတ်ပေးပါတယ်။

Sequenced Packet Exchange (SPX)

SPX ဟာ IPX နှင့်ပေါင်းစပ်ပြီးတော့ Connection Oriented Services ကိုပံ့ပိုးပေးပါတယ်။ Connection Oriented Protocol တိုင်းဟာ Transmission အရ နှေးကွေးပေမယ့် စိတ်ချရတဲ့ Transmission ကိုဖြစ်စေပါတယ်။

NetWare Core Protocol (NCP)

Transport Layer နှင့် ၎င်းရဲ့ အပေါ်ကအလွှာတွေဖြစ်ကြတဲ့ Session, Presentation နှင့် Application အလွှာက NCP ရဲ့ Functions ဟာ Client / Server နှစ်ခုစလုံးနှင့် ပတ်သက်သော လုပ်ဆောင်ချက် Function တွေတော်တော်များများကိုပံ့ပိုးပေးပါလိမ့်မယ်။ NCP ဟာ IPX / SPX အိမ့မဟုတ် NWLink ကိုဖြတ်သန်းပြီး Redirection လုပ်ခြင်းကိုကိုင်တွယ်ပေးပါတယ်။ ရှင်းအောင်ပြောရမယ်ဆိုရင် File များကို Sharing လုပ်ခြင်းနှင့် Print ထုတ်ခြင်းတို့ကို Sharing လုပ်ခြင်းတို့ဖြစ်ပါတယ်။

Service Advertising Protocol (SAP)

File နှင့် Print Server တွေဟာ ၎င်းတို့ရဲ့ ဝန်ဆောင်မှုကို ကွန်ရက်ပေါ်က ကွန်ပျူတာတွေသိအောင် ကြေညာဖို့အတွက် SAP ကိုအသုံးပြုပါတယ်။ အဲ့ဒီလိုကြေညာတဲ့အခါ ကာလအပိုင်းအခြားတစ်ခုကို အသုံးပြုတာပေါ့။ ပြောရမယ်ဆိုရင် စက္ကန့် ၆၀ကြာတိုင်းမှာပါ။ SAP Packet တွေဟာ ကွန်ပျူတာတွေအားလုံးကို

လုပ်ပေးနိုင်တဲ့ Service တွေကိုသိစေရန်နှင့် ဒီ Service ကိုပေးတဲ့ Service ရဲ့ Address ကိုပါသိအောင် Broadcast လုပ်ပေးတာက စတွန့် ဖေတိုင်းမှာပါ။ အခုနောက်ပိုင်း Network Version အသစ်တွေဟာ SAP ကိုမသုံးတော့ပဲ Novell Directory Service နှင့် ၎င်းနှင့်ဆက်နွယ်နေသော Protocol တွေကိုအသုံးပြုကြပါတယ်။ ဒါဟာ ဘာကြောင့်လဲဆိုတော့ တစ်မိနစ် တစ်ခါခြားကြေညာနေတဲ့ SAP ဟာကြီးမားတဲ့ကွန်ရက်တွေမှာ ပြဿနာတွေဖြစ်လာနိုင်လို့ပါ။ ကြီးမားတဲ့ကွန်ရက်တွေမှာက ကြေညာရမယ့် ဝန်ဆောင်မှုတွေက အမြောက်အမြားဖြစ်နေလို့ပါ။

Service Lookup Protocol (SLP)

NetWare ရဲ့ အခုနောက်ပိုင်း Version တွေမှာ (ပြောရမယ်ဆိုရင် Version 4.0 နှင့် ၎င်းနောက်ပိုင်း) Novell Directory Services ဟာ Server တွေအတွက် Service ကိုကြေညာစေပြီး Client တွေအတွက် ကြတော့ ဝန်ဆောင်မှု Services ကိုလှမ်းကြည့်စေတဲ့ Method ကိုအသုံးပြုပါတယ်။ SLP ဟာ IP ကို အခြေခံထားတဲ့ NetWare Protocol အသစ်ဖြစ်ပါတယ်။ SLP ဟာ Client တွေက Service ကိုအလိုရှိလို့ လှမ်းကြည့်တဲ့အချိန်မှာသုံးတဲ့ IP တစ်ခုတည်းကိုသာသုံးတဲ့ Network တွေမှာပဲရှိနိုင်ပါတယ်။

၆.၁၂ Apple Talk

Apple Talk ဟာ Apple Macintosh ကွန်ရက်တွေမှာ Transport ပြုလုပ်ဖို့ သတ်မှတ်ပေးတာဖြစ်ပါတယ်။

၆.၁၃ Xerox Network System (XNS)

Xerox ဟာ XNS ဆိုတဲ့ Xerox Network System ကို ၎င်းရဲ့ Ethernet Network တွေမှာသုံးရန် ထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ XNS ဟာ ကနေ့ Network တွေမှာ တွေ့ရခဲပါတယ်။

၆.၁၄ DEC Net

Digital Equipment Corporation ရဲ့ ကိုယ်ပိုင် Protocol ဖြစ်ပါတယ်။ DNA ဆိုတဲ့ Digital Network Architecture မှာ ၎င်း DECNet ကိုသုံးပါတယ်။ DECNet ဟာ Digital System အတွက် ပြည့်စုံတဲ့၊ Route လုပ်နိုင်တဲ့ Protocol တစ်ခုဖြစ်ပါတယ်။ Digital System ဆိုတာ Digital Equipment Corporation ရဲ့ System ကိုပြောတာပါ။

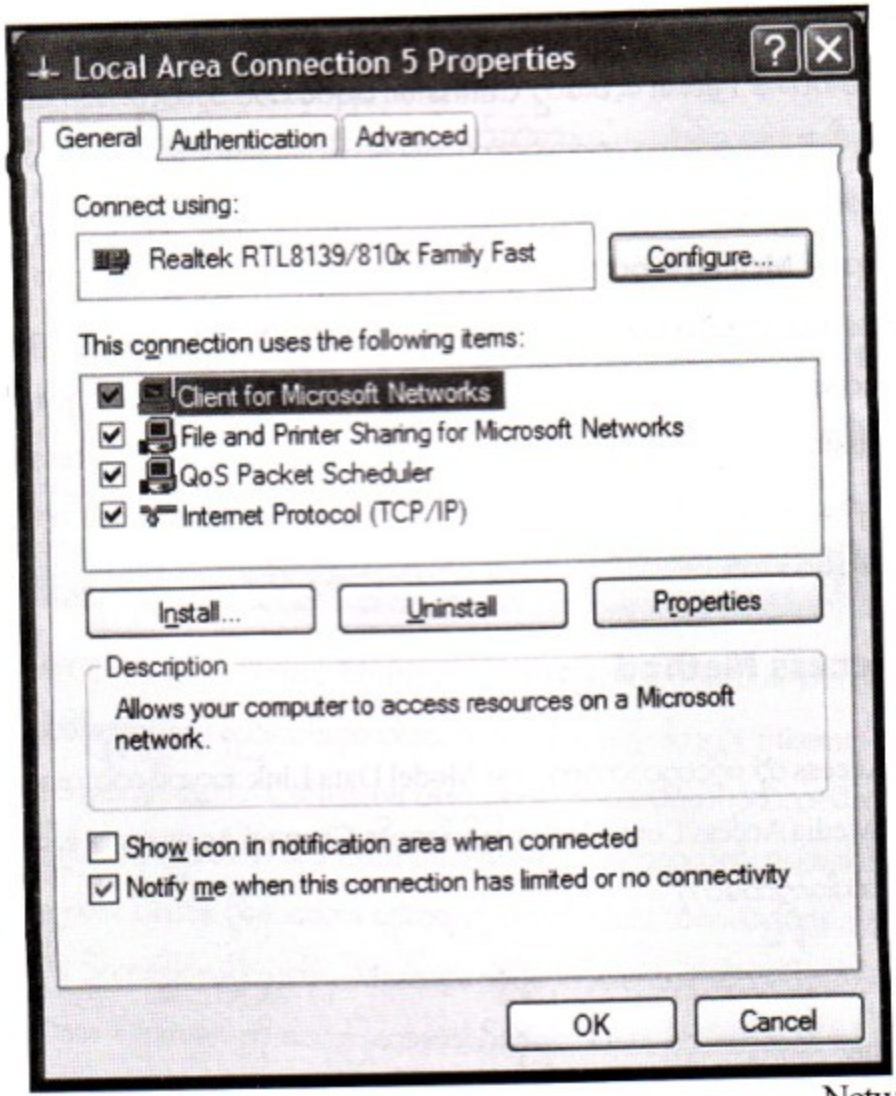
၆.၁၅ X.25

X.25 ဟာ Wide-Area Protocol ဖြစ်ပါတယ်။ ၎င်းဟာ Remote Terminate တွေ Mainframe ကိုချိတ်ဆက်ရန်နှင့် Packet Switching အသုံးပြုသော Network တွေမှာ အသုံးပြုတာ ဖြစ်ပါတယ်။ ခုချိန်မှာ Wide-Area ကိုဆက်သွယ်ပေးနိုင်မယ့် အခြားသော Communication Type တွေရှိနေပေမယ့် X.25 ကတော့ ကနေ့ထိကျယ်ပြန့်စွာ အသုံးပြုနေဆဲဖြစ်ပါတယ်။

၆.၁၆ Protocols များကို တင်ခြင်းနှင့် ဖြုတ်ခြင်း

Protocol ကိုတင်ခြင်းနှင့်ဖြုတ်ခြင်းအတွက် My Network Places ၏ Properties ကိုခေါ်ရပါမည်။ ပြီးနောက် ပေါ်လာသည့် Box တွင် Local Area Connection ကိုဖွင့်ရပါမည်။ ထိုအခါ အောက်ပါ Box ပေါ်လာပါမည်။ ၎င်း Box ကနေ Protocol တင်ခြင်းနှင့်ဖြုတ်ခြင်းများပြုလုပ်နိုင်ပါသည်။

ပုံ ၆.၇



၆.၁၃ Access Method

ကဲ ဒီတစ်ခါ ကျွန်တော်တို့ Access Method အကြောင်းကိုလေ့လာကြရအောင်။ Access Method ဆိုတာ တစ်ခြားတစ်ဖက်ကလှည့်ပြောရရင် ကွန်ပျူတာတွေဟာ Data တွေကို Cable ပေါ် ဘယ်လိုတင်လိုက်သလဲဆိုတာနှင့် ၎င်းတို့ဟာ Data တွေမပျက်စီးဘဲ ရည်ရွယ်ရာသို့ ရောက်ရှိကြောင်း ဘယ်လိုသိကြသလဲဆိုတာပဲ ဖြစ်ပါတယ်။ ကွန်ပျူတာတွေအများကြီးဟာ ကွန်ရက်ကိုချိတ်ဆက်လိုက်တဲ့အခါမှာ ဒီကွန်ပျူတာတွေအားလုံးဟာ Cable ကြိုးကိုမှီခိုအားပြုပြီး မျှဝေသုံးစွဲရတော့တာပါပဲ။ ဆိုလိုတာက ဒီကြိုးကနေ ကွန်ပျူတာတွေဆီက Data တွေဟာ ကွန်ရက်တစ်လျှောက်ရောက်ရှိသွားမှာဖြစ်ပါတယ်။ ဒီတော့ ဒီနေရာမှာ Collission ဆိုတာကို သိရတော့မယ်။ Collission ဆိုတာ တိုက်မိတာပဲ။ ဥပမာ ရထားလမ်းတစ်လမ်းထဲမှာ ရထားနှစ်စီး ဝင်လာလို့ တိုက်မိတာ Collision ပေါ့။ အခုလည်းပဲ ကွန်ပျူတာနှစ်လုံးက Data ကိုတစ်ချိန်တည်း တစ်ပြိုင်တည်း ပို့လွှတ်လိုက်ရင် အဲဒီ Collision ဖြစ်ပြီး Data နှစ်ခုစလုံးပျက်စီးသွားရော။ ဒီတော့ Data တွေကိုပို့လွှတ်တဲ့နေရာမှာ ကျွန်တော် အစောပိုင်းကပြောခဲ့သလို Data ကိုအပိုင်းပိုင်း ပိုင်းလိုက်ပြီး ရည်ရွယ်ရာကိုပို့မယ်။ ဒီဆက်ပိုပြောရရင် ၎င်း Data အပိုင်းလေးတွေကို အထုပ်လေးတွေ ပြန်ထုပ်ပြီး မပျက်စီးအောင်ပို့မယ်။ ဒီတော့ ပိုင်းပြီးပို့ရုံနဲ့ မလုံလောက်ဘူး။ ဆိုလိုတာက ဒီ Packet လေးတွေ Collission မဖြစ်အောင် ဘယ်လိုကာကွယ်မလဲဆိုတဲ့ Rules တွေရှိဖို့လိုလာပြီ။ ဒီ Rules တွေဟာ တကယ်တော့ကွန်ပျူတာက Data Channel လို့ခေါ်တဲ့ Cable ပေါ်က Data တွေကို ဘယ်လို Access လုပ်မလဲဆိုတာပါပဲ။ တစ်နည်းအားဖြင့် ပြောရင်တော့ Channel Access Method ပေါ့ဗျာ။ ဒီ Method တွေဟာ နှစ်လုံးနှင့် ၎င်းထက်ပိုသောကွန်ပျူတာတွေက ပို့လိုက်တဲ့ ဝင်တိုက်မိနိုင်သော Messages တွေကိုကာကွယ်ပြီး ရည်ရွယ်ရာကိုဘယ်လိုပို့မလဲဆိုတာကို ပံ့ပိုးပေးမှာဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင်တနည်းနည်းပေါ့ဗျာ။ တစ်ကြိမ်မှာ ကွန်ပျူတာတစ်လုံးကပဲ Data ပို့ဖို့ပါ။ အဲ့မှမဟုတ်လည်း Data တွေ Collission မဖြစ်အောင် အခြားနည်းလမ်းနှင့် ကာကွယ်ပါ။ စတာကို Access Methods လို့ခေါ်ပါတယ်။ ဒီနေရာမှာ တစ်ခုသိထားရမှာက Network မှာက ကွန်ပျူတာအားလုံးဟာ တူညီတဲ့ Access Method ကိုအသုံးပြုဖို့လိုပါတယ်။ အဲ့သလိုမှမဟုတ်ရင် Data တွေကို လက်ခံရရှိနိုင်မှာမဟုတ်ပါဘူး။

၆.၁၈ အခြား Access Method များ

ဒီ Channel Access ကို ကိုင်တွယ်တာက OSI Model Data Link အလွှာရဲ့ဆင့်ပွားအလွှာတစ်ခုဖြစ်တဲ့ MAC ဆိုသော Media Access Control အလွှာဖြစ်ပါတယ်။ Channel Access ဟာ အဓိကအားဖြင့် အုပ်စု (၅)ခုရှိပါတယ်။ အဲ့ဒါတွေကတော့ -

(၁) Contention

(၂) Token Passing

(၃) Demand Priority

(၄) Polling

(၅) Switching တို့ဖြစ်ကြပါတယ်။

ခေါင်းစဉ် ၁၉ Contention

အစည်းအဝေးတစ်ခုမှာ တိုလူကပြောလိုက် ဒီလူကပြောလိုက် တစ်ချိန်တည်း တစ်ပြိုင်တည်းမှာပဲ သူရော ကိုယ်ရောလုယက်ပြီး ပြောနေကြရင် အဲဒါ ထိရောက်တဲ့ဆွေးနွေးပွဲဖြစ်လာမှာမဟုတ်ပါဘူး။ အစည်းအဝေးတစ်ခုမှာ အဓိပ္ပါးမဖြစ်အောင် Moderator ဆိုတဲ့ ခုံသမာဓိ အဖွဲ့မဟုတ် ပြန်ဖြေပေးသူရှိဖို့လိုအပ်သလိုပဲ။

ကဲ အခုလည်း Network မှာ အဓိပ္ပါးဖြစ်တတ်ပုံကိုပြောရမယ်ဆိုရင် ကွန်ပျူတာဟာ Data ကိုပို့ရတော့မယ်ဆိုရင်/ ပို့ရတော့မယ်ဆိုတာနဲ့ Data ကိုပို့လိုက်တော့တာပဲ။ သေးငယ်တဲ့ ကွန်ရက်တစ်ခုမှာ အနည်းငယ်သော Data တွေကိုပဲ အပို့အယူလုပ်နေသည့်တိုင် ကွန်ပျူတာတွေဆီက ပို့လိုက်တဲ့ Data တွေဟာ Collission ဖြစ်ကြပါတယ်။ ဖြစ်တော့ Data ကို Reset ပေါ့ ပြန်ပို့ပါတယ်။ ပြန်ပို့လည်း Collission ထပ်မဖြစ်ဘူးလို့ မပြောနိုင်ဘူးလေ။ ဒီအတိုင်းဆိုရင် ကွန်ပျူတာကွန်ရက်ဆိုတာ သုံးမရဖြစ်သွားမှာပေါ့။

ဒီ Contention ကို အခြေခံထားတဲ့ ကွန်ရက်တွေမှာတော့ Access Methods နှစ်မျိုးထပ်ခွဲပါတယ်။ အဲဒါကတော့ -

(၁) CSMA/CD - Carries Sense Multiple Access with Collission Detection

(၂) CSMA/CA - Carries Sense Multiple Access with Collission Avoidance

တို့ဖြစ်ကြပါတယ်။

CSMA/CD

CSMA/CD (Carrier Sense Multiple Access with Collission Derection) ဟာ Network Traffic ကိုထိန်းညှိပေးတဲ့ နည်းလမ်းကောင်းတွေထဲက တစ်ခုဖြစ်ပါတယ်။ Ethernet ကိုအသုံးပြုထားတဲ့ အခါမှာ ဒီ Access Method ဟာ Collission မဖြစ်အောင် ဘယ်လိုကာကွယ်သလဲဆိုရင် သူက Data Channel ပေါ့ (Cable ကိုပြောတာ)။ အဲဒီ Data Channel ကိုလှမ်းကြည့်လိုက်တယ်။ အဲဒီမှာ အခြားကွန်ပျူတာက Data များပို့ထားသလား၊ ပို့နေသလား ဆိုတာကြည့်လိုက်တယ်။ အကယ်၍များ ဘယ်ကွန်ပျူတာကမှ Data Channel မှာ ပို့ထားခြင်းမရှိဘူးဆိုမှ Message ကိုပို့လိုက်ပါတယ်။ အဲဒါသလိုမှမဟုတ်ဘဲ ကွန်ပျူတာတစ်လုံးလုံးက Data Channel ကိုအသုံးပြုထားတယ်ဆိုရင် Data ကို မပို့လွှတ်သေးဘဲ အချိန်တစ်ခု

(တစ်ခေါက်နှင့် တစ်ခေါက်မတူသောအချိန်) အတိုင်းအတာတစ်ခုစောင့်ပြီး ပြန် Check လုပ်ပါတယ်။ အဲ့သလိုပဲ ပေါ့ဗျာ။ Channel မှာ ဘယ်ကွန်ပျူတာကမှ Data မပို့တော့ဘူးဆိုတော့မှ လက်ရှိကွန်ပျူတာက Data ကို ပေးပို့ပါတော့တယ်။

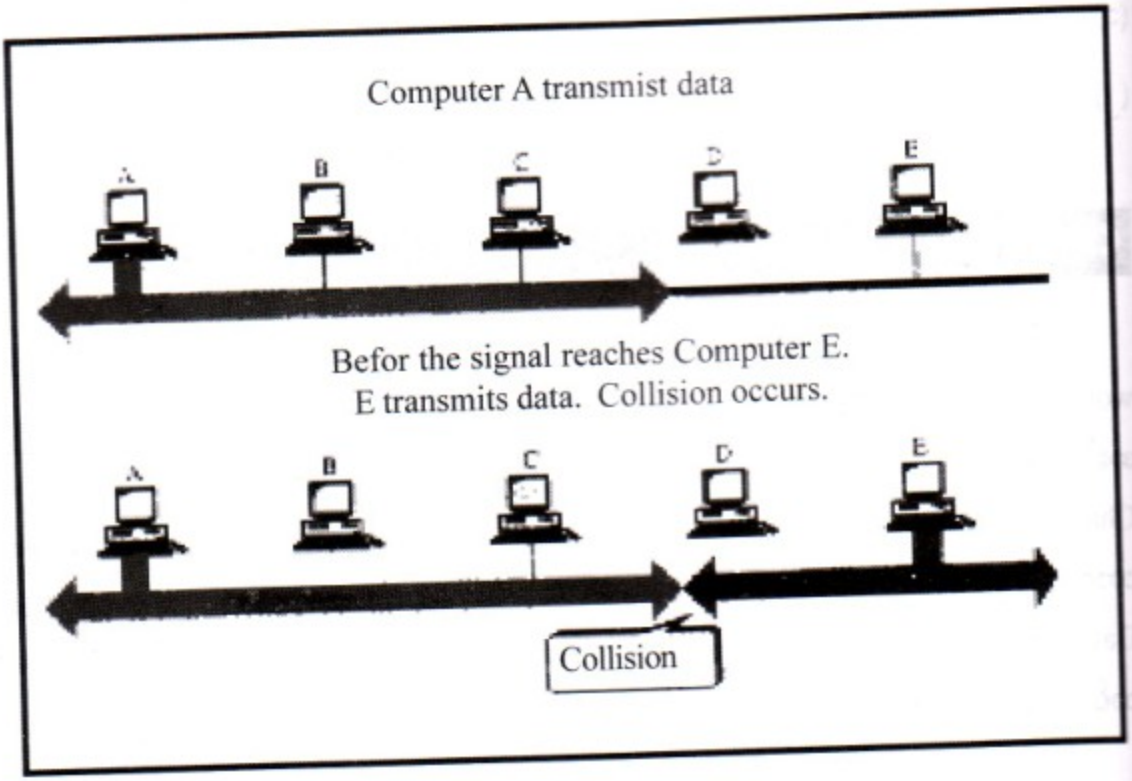
မှတ်ချက်။ ။ CSMA/CD မှာပြောစရာတစ်ခုရှိတာက Network မှာရှိတဲ့ ကွန်ပျူတာတိုင်းဟာ ဒီ Data တွေသွားရာလမ်း (Cable) Data Channel ကိုညီတူမျှတူထိန်းချုပ်ပိုင်ခွင့်ရှိပါတယ်။ ဆိုလိုတာက Traffic လမ်းကြောင်းနှင့် ပတ်သက်လာရင် Workstation ကလာတဲ့ Traffic ထက် Server ကလာတဲ့ Traffic ကိုဦးစားပေးမယ်တို့ ဘာတို့ဆိုတာမျိုးမရှိပါ။

CSMA/CD ဟာ Collission ကို ကောင်းစွာကာကွယ်ပေးနိုင်တယ်ဆိုပေမယ့် သူ့မှာကန့်သတ်ချက်လေးတွေရှိနေပါသေးတယ်။ ပြောရမယ်ဆိုရင် -

(၁) မီတာ ၂၅၀၀ ကျော်သွားတဲ့အခြေအနေမျိုးမှာ Attenuation နှင့် Signal Length ကန့်သတ်ချက်ကြောင့် CSMA/CD ဟာသက်ရောက်မှုမရှိတော့ပါ။ အလုပ်မလုပ်ပေးနိုင်တော့ပါ။

(၂) ကွန်ရက်မှာ ကွန်ပျူတာတွေများလာလေလေ Collission ဖြစ်နိုင်ခြေများလာလေဖြစ်ပါတယ်။ ဒီတော့ Collission ဖြစ်လေ Data တွေကိုပြန်လည်ပေးပို့ခြင်း Retransmission လုပ်ရလေဖြစ်ပါတယ်။ ဒါဟာ Network ကိုနှေးသွားစေပါတယ်။

ပုံ ၆.၈



(၃) အကယ်၍များ ကွန်ပျူတာတစ်လုံးလုံးက Data အများကြီးပို့လိုက်တဲ့အခါ Network Channel မှာတခြားသူက သူပို့ပြီးတာကိုထိုင်စောင့်နေရမယ်။ ဟိုဖက်က Data အများကြီးပို့နေတာကို လက်ငါးကြီးအုပ်သလိုဖြစ်သွားပြီး တစ်ဖက်လူအတွက်က ငုတ်တုတ်မေ့နေတော့တာပဲ။ ပြောရရင် အခြားလူတွေအတွက် Network ဟာနေးသွားတာပေါ့။

CSMA/CA

CSMA/CA (Carrier Sense Multiple Access with Collission Avoidance) ဆိုတာက CSMA ရဲ့ နောက်ထပ် Channel Access နည်းတစ်ခုပဲဖြစ်ပါတယ်။ သူကတော့ CA ပေါ့။ CA ဆိုတာ CD မဟုတ်ဘူးပေါ့။ CD ဆိုတာ Collission ကို Detect လုပ်တာ။ CA ဆိုတာ Collission ကို Avoid (ရှောင်တာ)လုပ်တာ။ သူက Collission မဖြစ်အောင် Detect လုပ်မယ့်အစားရှောင်တာဖြစ်ပါတယ်။ ဘယ်လိုပုံစံမျိုးလဲဆိုတော့ Data နှင့်အတူ Signal တစ်ခုပါရှိတယ်ဗျ။ အဲ့ဒီ Signal ကို Intent-to Transmit လို့ခေါ်ပါတယ်။ မြန်မာလိုပြောရရင်တော့ Signal ပို့လွှတ်ထားတယ်ပေါ့ဗျာ။ ကွန်ပျူတာကအဲ့ဒီဆို Data ကိုမပို့သေးဘဲစောင့်နေပြီးအဲ့ဒီ Intent-to Transmit ဆိုတဲ့ Signal ရမှသာလျှင်လက်ရှိကွန်ပျူတာက (နားလည် လွယ်အောင်ရှင်းပြရရင်) ဒီတစ်ခေါက် ငါပို့မယ်ဟေ့ဆိုပြီး အဲ့ဒီ Intent-to-Signal ကိုပြန်ပို့ပြီး Data ပို့ပါတယ်။

ဒီနည်းက CSMA/CD ထက်စာရင် Collission ကိုရှောင်ရမှာ ပိုစိတ်ချရတယ်ဆိုပေမယ့် အဲ့ဒီ Intent-to-Signal ဆိုတာကြီးကိုပို့နေရတာက Network Speed ကိုကျသွားစေပါတယ်။ ဒါကြောင့် CSMA/CD ကိုပိုပြီးအသုံးများကြပါတယ်။ CSMA/CA ကိုတော့ Apple ရဲ့ Local Talk တွေမှာပဲ အဓိကထားသုံးခဲ့ကြပါတယ်။

၆.၂၀ Token Passing

ကျွန်တော်တို့ Topology တွေအကြောင်းပြောတုန်းကလည်း Token Passing ဆိုတာကိုပဲပြောခဲ့ဖူးတယ်။ ဒီ Token Passing ဆိုတဲ့ Channel Access Method မှာ Token လို့ခေါ်တဲ့ အထူးပြုလုပ်ထားတဲ့ Packet လေးကို ကွန်ပျူတာတစ်လုံးမှ နောက်တစ်လုံးသို့အစဉ်လိုက်တိုင်းပေးပို့ပါတယ်။ Token ကိုရရှိတဲ့ ကွန်ပျူတာကသာလျှင် Data ကိုပေးပို့နိုင်ပါတယ်။ ဒီ Token ဆိုတာကြီးကိုလည်း ကွန်ပျူတာတစ်လုံးဟာ အကြာကြီးကိုင်ထားလို့မရဘူး။ သတ်မှတ်ထားတဲ့အချိန်တစ်ခုပဲ ကိုင်ထားလို့ရတာပါ။ Token ကိုအလှည့်ကျရရှိတဲ့ ကွန်ပျူတာဟာ Data ကိုပေးပို့စရာမရှိဘူးဆိုရင် ၎င်း Token ကိုနောက်ထပ်ကွန်ပျူတာတစ်လုံးသို့ပို့လိုက်ပါတယ်။ ဒီတော့ အချုပ်ပြန်ပြောရရင် Token ရှိတဲ့ကွန်ပျူတာကသာ Data ကို Transmit လုပ်နိုင်တာဖြစ်သောကြောင့် Collission ကိုကာကွယ်ပြီးသားဖြစ်သွားပါလိမ့်မယ်။ ဒီတော့ Collission ဖြစ်ပေါ်လို့ဖြေရှင်းနေရမယ့်အချိန်ပုပ်တာမျိုး မရှိတော့ပါဘူး။ ကွန်ရက်တွေမှာရှိတဲ့ ကွန်ပျူတာတိုင်းဟာ Media ကို

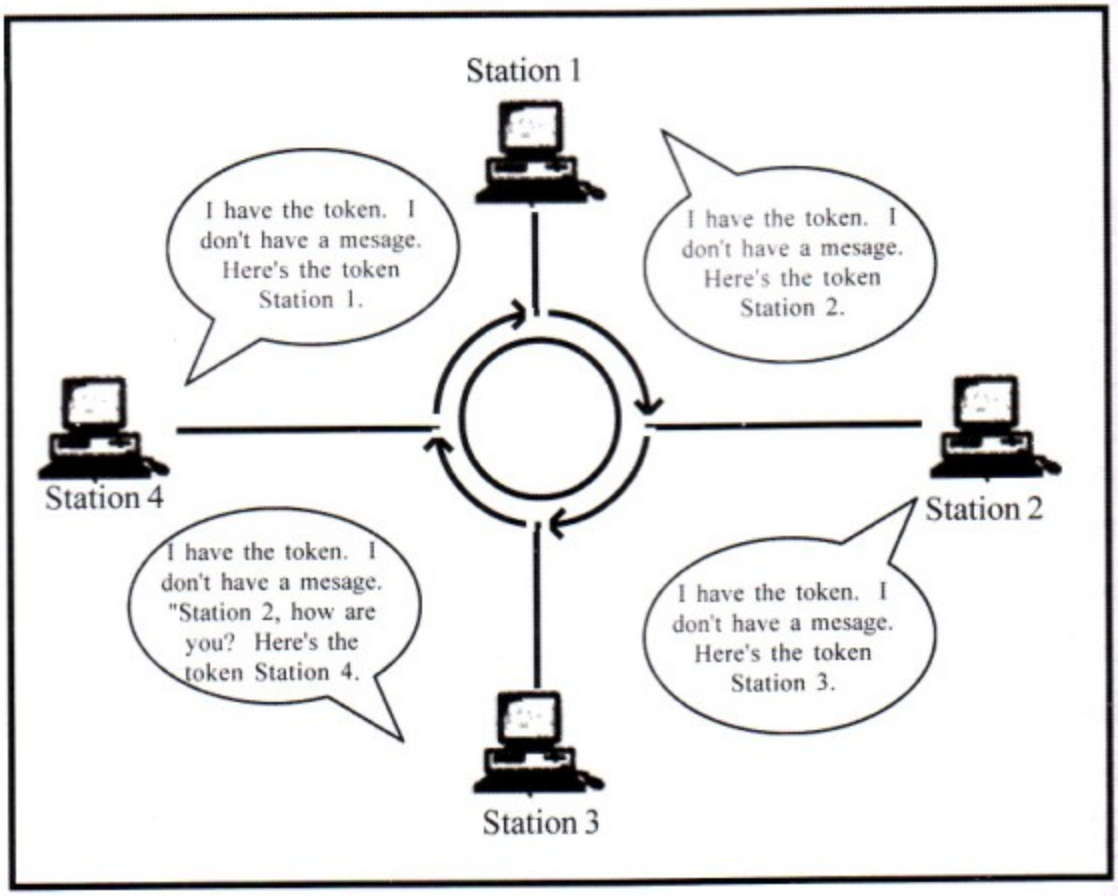
Access လုပ်ရာဝယ် ညီတူညီမျှအခွင့်အရေးရရှိပါတယ်။ ဒါကြောင့် Token-Passing Network ကို Time-Sensitive ဖြစ်တဲ့နေရာမျိုးတွေမှာ အသုံးများပါတယ်။ ဥပမာပြောရရင် Banking Transaction တွေ အချိန်ကို အတိအကျလိုအပ်တဲ့ Database လုပ်ငန်းမျိုးတွေမှာဖြစ်ပါတယ်။ Ring Topology မှာ Traffic ဟာ Direction တစ်ဖက်တည်းကိုပဲသွားနေတာကြောင့် တစ်ချိန်တည်း တစ်ပြိုင်တည်းမှာ Collission မဖြစ်စေဘဲ Token နှစ်ခုကို လည်ပတ်စေနိုင်ခြင်းဖြစ် Access Method ဟာ ပိုမြန်လာစေနိုင်ပါတယ်။

ဒီနေရာမှာ Token Passing ဟာအားနည်းတဲ့အချက် (၂)ချက်ရှိပါတယ်။

(၁) Token ရမှ Data ကို ပို့လို့ရတယ်ဆိုတာကို သိခဲ့ပြီးကြပါပြီ။ ကဲ Token ရပါပြီတဲ့ ပို့ရမယ့် Data က ကြီးနေလို့ ခွဲပို့လိုက်ပြီ။ ဒီတော့ Token က တစ်ခြားနောက်တစ်ယောက်ဆီရောက်သွားပြီ။ ဒီမှာက Data ကကြီးတော့ ခွဲပို့လိုက်ရတာ ပို့ဖို့ကျန်သေးတယ်။ ခက်ပြီး ဒီတော့ ကျန်တဲ့ Data ကိုပို့ဖို့ ၎င်းဟာ Token သူ့ဆီပြန်ရောက်လာအောင် တစ်ပတ်ပြန်စောင့်ရပါသေးတယ်။

(၂) Token ကိုပြုလုပ်ခြင်း၊ လွှဲပေးခြင်းဆိုတဲ့ ရှုပ်ထွေးတဲ့ကိစ္စတွေကြောင့် အသုံးပြုရတဲ့ပစ္စည်းတွေဟာ Contention-Based Network တွေမှာထက် ကုန်ကျစရိတ်ပိုများပါတယ်။

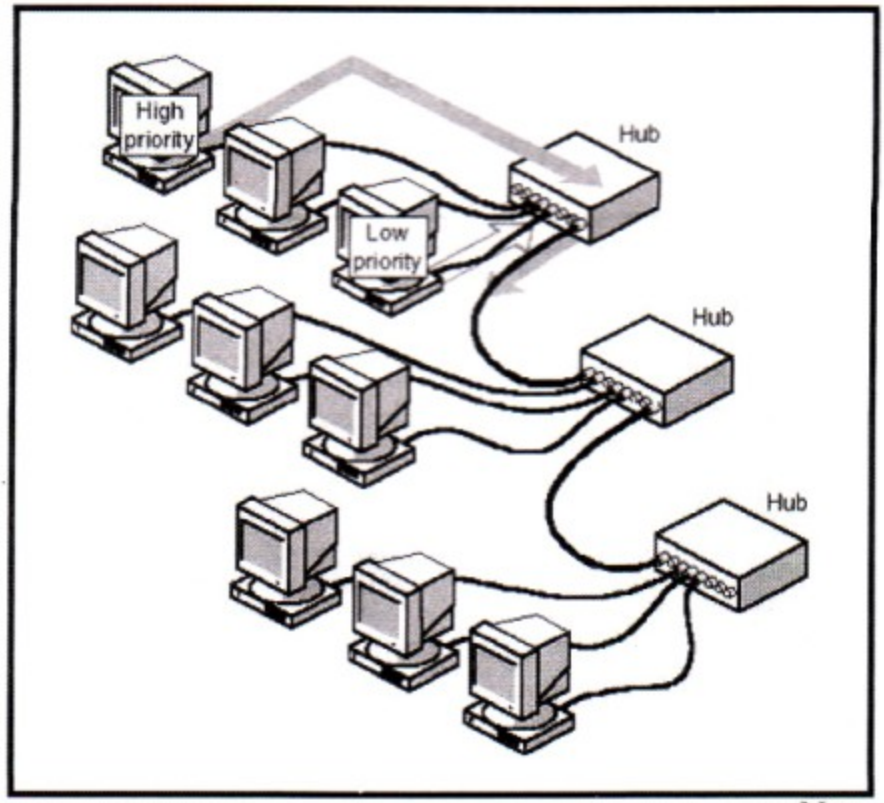
ပုံ ၆.၉



၆.၂၁ Demand Priority

ဒီ Access Method မှာတော့ Network ရဲ့ Access ကို Intelligent Hub ကထိန်းချုပ်ပါတယ်။ ၎င်း Hub ဟာ Connection တွေအားလုံးကိုရှာဖွေပေးပါတယ်။ အဲဒီကွန်ရက်မှာရှိတဲ့ Computer, Bridge, Router နှင့် Switch တွေဟာ Data ကိုပေးပို့ချင်ပြီဆိုရင် သူတို့ဟာ အဲဒီ Hub ဆီကို Demand Signal ဆိုတာကိုပေးပို့လိုက်ပါတယ်။ အဲဒီအခါ Hub က ဒီ Demand Signal ရရှိတာကြောင့် အသိအမှတ်ပြု Acknowledgment ကိုပြန်ပို့ပေးလိုက်တဲ့အခါ ကွန်ပျူတာဟာ Data ကိုစတင်ပေးပို့လို့ရပြီဖြစ်ပါတယ်။ ဒီ Method ဟာ အခြား Channel Access Method နှင့်မတူတဲ့ အချက်က Demand Priority ဟာ Priority မြင့်တဲ့ Computer ကိုအခြားထက်ခွင့်ပြုတာပဲဖြစ်ပါတယ်။ ဆိုလိုတာက ရာထူးမြင့်တဲ့သူကိုဦးစားပေးတဲ့ သဘောမျိုးပါ။ ထပ်ရှင်းပြပါဦးမယ်။ အကယ်၍များ ကွန်ပျူတာအများကြီးဟာ တစ်ပြိုင်တည်း ၎င်း Demand ကိုအလိုရှိခဲ့သော် Priority မြင့်တဲ့ ကွန်ပျူတာက အရင် Transmit လုပ်ခွင့်ရမှာဖြစ်ပါတယ်။ ဒီ Demand Priority နည်းဟာမြန်ဆန်တဲ့နည်းတစ်ခုတော့ဖြစ်ပါတယ်။ ဘာလို့လဲဆိုတော့ Data မပို့တဲ့ ကွန်ပျူတာတွေရဲ့ လိပ်စာတွေနှင့် အလုပ်လုပ်ပြီးအချိန်ကုန်မယ့်အစား Hub ဟာ Service ကိုတောင်းခံတဲ့ ကွန်ပျူတာကိုပဲ Response လုပ်ရလို့ဖြစ်ပါတယ်။ အဲဒီအပြင် Demand Priority နည်းဟာ CSMA/CD နှင့် CSMA/CA တို့လို Network ကို Packet တွေ Broadcast လုပ်မယ့်အစား ကွန်ပျူတာကနေ Hub ဆီသို့နှင့် Hub မှ ရည်ရွယ်ရာဆီသို့သာ တိုက်ရိုက်ပေးပို့ကြပါတယ်။ ဒါဟာ Network မှာမသက်ဆိုင်တဲ့

ပုံ ၆.၁၀



Traffic ကိုရှင်းလင်းဖယ်ရှားပစ်လိုက်တာပဲဖြစ်ပါတယ်။ Demand Priority နည်းဟာ ပုံမှာပြထားတဲ့ Design ပေါ်ကိုတော့မှီခိုပါတယ်။ ဒီနည်းမှာ မကောင်းတဲ့အချက်တစ်ခုကတော့ ဈေးပဲ။ ဘာလို့လဲဆိုတော့ သူ့အတွက်က အထူးပြုလုပ်ထားတဲ့ Hub နှင့် အခြားပစ္စည်းတွေလိုအပ်လို့ပဲ။ ဒီနည်းကို 100 VG-AnyLAN တစ်ခုတည်းပဲအသုံးပြုပါတယ်။

၆.၂၂ Polling

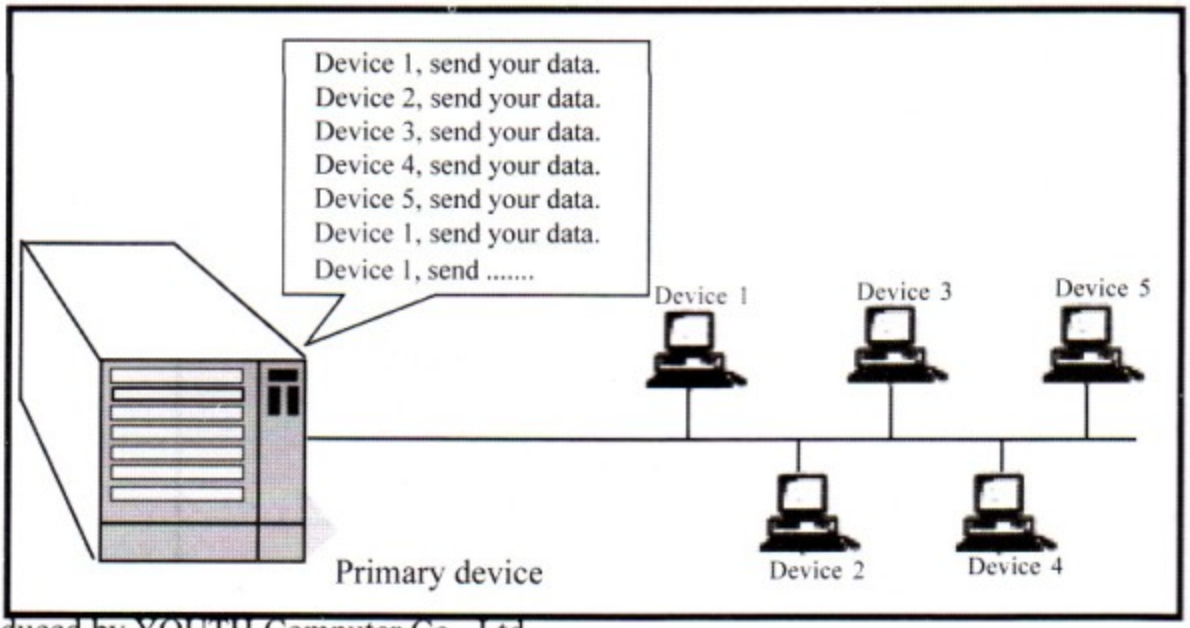
Polling ကတော့ Network မှာ Access ကို Control လုပ်တဲ့နည်းတွေထဲက ရှေးကြတဲ့ နည်းတစ်ခုပဲဖြစ်ပါတယ်။ ပုံမှာမြင်ရတဲ့အတိုင်းပါပဲ။ သူ့မှာ ဗဟိုထိန်းချုပ်မှု Central Controller ဆိုတာပါရှိပါတယ်။ အဲဒါကို Primary Device လို့ခေါ်ပြီး ကွန်ရက်ထဲက ကွန်ပျူတာတွေထဲက Data ပို့လိုက်တဲ့ ကွန်ပျူတာက Secondary Device ဖြစ်သွားပါတယ်။ ဒီတော့ ပုံမှာမြင်ရတဲ့အတိုင်းပါပဲ။ ကွန်ပျူတာဟာ အတိုင်းအတာတစ်ခုသော Data တွေကိုပို့ခွင့်ရပြီးနောက် အခြားကွန်ပျူတာအလှည့်ဖြစ်သွားပါတယ်။ တစ်လှည့်စီပေါ့ဗျာ။ အင်းအလှည့်ကျပေါ့။

Polling မှာ ကောင်းတဲ့အချက်တွေ အများကြီးရှိတယ်ဗျ။

(၁) Token Passing လိုပဲပေါ့။ ကွန်ပျူတာအားလုံးဟာ Data Channel ကို Access လုပ်ရတာညီတူအခွင့်အရေးရှိပါတယ်။ ကွန်ပျူတာတစ်လုံးထဲကနေမှ Access ကိုလက်ဝါးကြီးအုပ်လို့မရပါဘူး။

(၂) ဗဟိုထိန်းချုပ်ပေးတဲ့ Central Controller က ဗဟိုထိန်းချုပ်မှု Centralized Management ကိုပေးပြီး၊ ဥပမာ Server လို ကွန်ပျူတာမျိုးက အခြားကွန်ပျူတာထက် အဆင့်မြင့်တာကြောင့် အခွင့်အရေးပိုရတဲ့

ပုံ ၆.၁၁



သဘောဖြစ်ပြီး အခြားကွန်ပျူတာတွေထက်ပိုပြီး Data ကိုအချိန်ပိုကြာကြာသုံးနိုင်ပါတယ်။

အားနည်းတဲ့အချက်ကတော့ Primary Device Fail ဖြစ်သွားရင် Network တစ်ခုလုံး Fail ဖြစ်သွားပါလိမ့်မယ်။ ဒါကြောင့် ၎င်းကို IBM SNA Network တွေကလွဲလို့ အခြားမှာ အသုံးပြုတာ မတွေ့ရပါဘူး။

၆.၂၃ Switching

Switch လို့ခေါ်တဲ့ အထူးပြုလုပ်ထားတဲ့ပစ္စည်းလေးနှင့် Nodes တစ်ခုချင်းစီကို Network အဖြစ် ချိတ်ဆက်လိုက်တဲ့အခါမှာတော့ Media ကို Access လုပ်မှုအပိုင်းကို ၎င်း Switch က Control လုပ်သွားပါတော့တယ်။ ဒီ Channel Access ကို Control လုပ်တဲ့နည်းကို Switching လို့ခေါ်ပါတယ်။ နှစ်ခု သို့မဟုတ် နှစ်ခုထက်ပိုတဲ့ ပို့လွှတ်ခြင်းဖြစ်ရပ်တွေဟာ လက်ခံရာကို တစ်ပြိုင်တည်းရောက်ရှိတဲ့အခါမှာ ဖြစ်စေ၊ Switch ကကိုင်တွယ်နိုင်တဲ့အများဆုံး Multiple Connection ကိုကျော်ပြီးတစ်ပြိုင်တည်း ပို့လွှတ်မှုတွေ တောင်းဆို လာတဲ့အခါဖြစ်စေ အခြေအနေအရပ်ရပ်ကို ရင်ဆိုင်ရခြင်းဟာ Switch မှာပဲဖြစ်ပေါ်လေ့ရှိပါတယ်။ အဲ့ဒီကို ထူးခြားတဲ့အခြေအနေတွေကလွဲလို့ ပြဿနာတွေဟာ Network Switch အတွက်ဖြစ်ပေါ်လေ့မရှိပါဘူး။ ဘာလို့လည်းဆိုတော့ ၎င်းဟာ မည်သည့် Nodes တစ်စုံကိုမဆိုချိတ်ဆက်ပေးနိုင်ပြီး လိုအပ်ပါက Data တွေကိုဖလှယ်ပေးနိုင်လို့ပါပဲ။ ဒီထက်ပိုပြီးပြောရမယ်ဆိုရင် ကွန်ပျူတာနှစ်လုံးကြားက Connection တိုင်းဟာ Data တွေဖလှယ်ချင်ရင်သုံးလို့ရအောင် သီးသန့် Reserved လုပ်ထားတာဖြစ်ပါတယ်။ အဲ့ဒီ Connection ဟာ အဲ့ဒီမှာ အသုံးပြုထားတဲ့ Network နည်းပညာပေါ်မူတည်ပြီးရရှိတဲ့ Bandwidth အကုန်လုံးကို အသုံးပြုလို့ ရပါတယ်။

Switching မှာ ကောင်းတဲ့အချက်တွေအများကြီးရှိပါတယ်။

(၁) Switching ဟာ Channel ကို Access လုပ်ရာမှာ ကွန်ပျူတာတစ်လုံးတည်းကနေ လက်ဝါးကြီးအုပ်ထားတဲ့ ပုံစံမျိုးလုပ်လို့မရပါ။

(၂) Switching က ဗဟိုထိန်းချုပ်မှု Centralized Management လည်းရပါတယ်။ နောက်ပြီး Routers လိုဟာမျိုး၊ Server လိုဟာမျိုးတွေက အခြားကွန်ပျူတာတွေထက် အခွင့်အရေးပိုရပါတယ်။

အားနည်းချက်ကတော့ ကုန်ကျစရိတ်မြင့်မားတာပါပဲ။ ပြောရရင် Switch ကိုကျွေးကြီးနေတာပဲ။

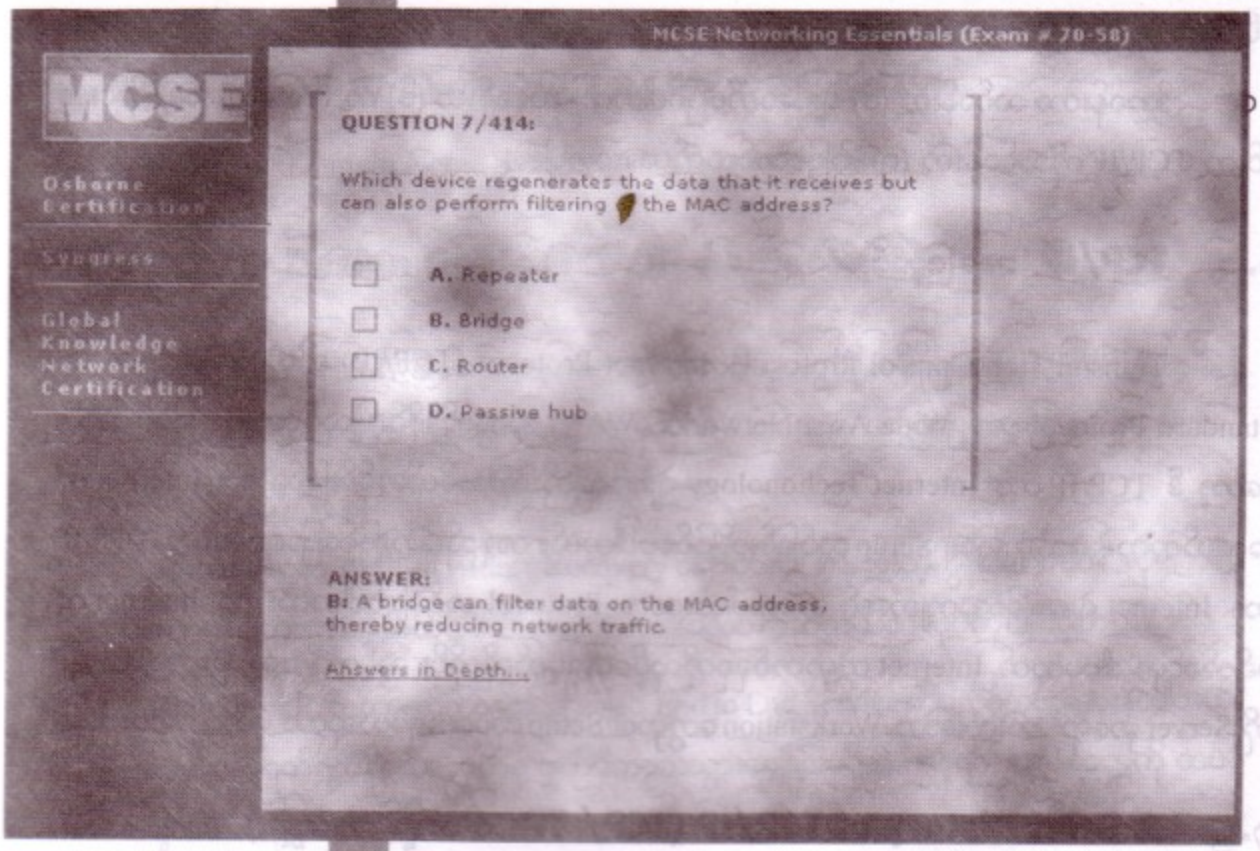
ခေတ်ပေါ်နှင့်မြန်မာ့ရိုးရာတူရိယာသံစဉ်များကို ကွန်ပျူတာဖြင့်ဖန်တီးခြင်း

Modern & Traditional Music Creation with FL Studio 6 (Fruity Loops)

စာအုပ် မြန်မာဘာသာဖြင့် ထွက်ပြီ၊

ခေတ်ပေါ်နှင့်မြန်မာ့ရိုးရာ တူရိယာသံစဉ်များကို ကွန်ပျူတာဖြင့်ဖန်တီးခြင်း (Modern & Traditional Music Creation with FL Studio 6) (စာမူခွင့်ပြုချက်အမှတ်-၄၀၁၀၆၂၀၆၀၈) စာအုပ်အား ဦးဇော်လင်း (YOUTH Computer) မှ ရေးသားပြုစု၍ YOUTH Computer(ဖုံး-၀၉၅၀၀၃၅၉၆) မှတစ်နိုင်ငံလုံးသို့ဖြန့်ချိပါမည်။ ဂီတဝါသနာပါသော လူကြီး၊လူငယ်များအတွက် ယနေ့ခေတ်တွင်အလွန်အရေးပါလာသော Music Programming & Sequencing (MIDI/Wave) ကို ရှင်းလင်းချက်သင်ခန်းစာ၊ ရုပ်ပုံများ၊ ဂီတဆိုင်ရာရှင်းလင်းချက်များ၊ ကွန်ပျူတာပိုင်းဆိုင်ရာသိသင့်သည့်အချက်များ၊ သီချင်း Notes များအပါအဝင် အသေးစိတ်စိတ်ဝင်စားဖွယ်တင်ပြထားပါသည်။ ထို့အပြင် Background Music များဖန်တီးခြင်း၊ Synthesizer များအသုံးပြုခြင်း၊ စကားပြောသံနှင့်တခြားစိတ်ဝင်စားဖွယ် Sound Effect များထည့်သွင်းခြင်း၊ Mixing နှင့် Mixing Down ပြုလုပ်ခြင်း၊ Flying Fader (Mixing Automation) များကိုရှင်းပြခြင်း၊ Effect များထည့်သွင်းခြင်း၊ (Compressor & Parametric Equalizer) များ၏ သဘောများကို ရှင်းပြခြင်း၊ Guitar Vamp များကို ကိုယ့်စိတ်ကြိုက်ပြန်ရေးခြင်း၊ စက်ရုပ်၊ ဂြိုလ်သားအသံများဖန်တီးခြင်း စသည်ဖြင့်အကြောင်းအရာစုံလင်စွာပါရှိပါသည်။ ဂီတဖြင့်အသက်မွေးဝမ်းကျောင်းပြုသူများ၊ ဂီတကိုဝါသနာထုံသူများအပြင် ယနေ့ခေတ် အသံနှင့်ပတ်သက်သည့်လုပ်ငန်းများဖြစ်ကြသည့် ရုပ်ရှင်၊ ဗွီဒီယို၊ ကြော်ငြာ၊ အင်တာနက်ကြော်ငြာ၊ သင်ကြားရေးစီဒီ၊ ကာတွန်းစီဒီ စသည့်လုပ်ငန်းများအတွက်လည်း အသုံးတည့်မည့်စာအုပ်လည်းဖြစ်ပါသည်။ ဂီတနားလည်ပြီး ကွန်ပျူတာမသိ၊ ကွန်ပျူတာသိပြီးဂီတမသိ နှစ်ဦးနှစ်ဖက်လုံးအသုံးပြုလို့ရအောင် ပြုစုထားသောစာအုပ်လည်းဖြစ်ပါသည်။ ယနေ့ခေတ်တွင် သင်သည်အတီးသမားဖြစ်စေ၊ အဆိုသမားဖြစ်စေ၊ ဝါသနာပါသည်ဖြစ်စေ Music Programming & Sequencing ကိုသိထားသင့်ပေသည်။

Produced by YOUTH Computer Co., Ltd



UNIT 7

TCP/IP

ဒီ သင်ခန်းစာကာလည်း ရှေ့သင်ခန်းစာနဲ့ ဆက်နွယ်ပြီး ဖြစ်လာတဲ့သင်ခန်းစာလို့ပြောရင်တောင်ရပါတယ်။ TCP/IP ဆိုတာလည်း Communication Protocols နှင့် ပတ်သက်နေတာ ပဲ မဟုတ်ပါလား။

ဒီအခန်းဟာ သင်ခန်းစာ (၆) ရဲ့အဆက်ပဲဖြစ်ပါတယ်။ သင်ခန်းစာ (၆) က Protocol အကြောင်းပါ။ ၎င်းက TCP/IP ကိုသင်ခန်းစာ (၇) အဖြစ်တင်ဆက်ထားတာပါ။

၇.၁ TCP/IP အကြောင်း

Transmission Control Protocol / Internet Protocol (TCP/IP) ဆိုတဲ့ ဒီ IT Industry Standard Protocol တာ Wide Area Networks (WAN) အတွက်ဒီဇိုင်းပြုလုပ်ထားတာဖြစ်ပါတယ်။ ဒီတော့ ဒီ TCP/IP ဟာ Internet Techonology ရဲ့အရေးကြီးဆုံးအစိတ်အပိုင်းဖြစ်သလို၊ Internet ကို အလွယ်တကူနဲ့အသုံးပြုခြင်း၊ Setup လုပ်ခြင်းတို့ဖြစ်စေပါတယ်။ တနည်းအားဖြင့်ပြောရရင်တော့ TCP/IP ဟာ Internet ရဲ့အခြေခံအကျဆုံးနှင့် အရေးပါဆုံးသော Protocol တစ်ခုဖြစ်ပါတယ်။ ကဲ Internet ကို မချိတ်ခင်မှာ ဒါမှမဟုတ် Internet ထဲမှာတစ်ခုခုကိုလုပ်တော့မယ်ဆိုတိုင်း သင်ဟာ ပထမဦးစွာ TCP/IP ကို Server မှာရော အားလုံးသော Workstation တွေမှာပါ Setup လုပ်ပေးရမယ်ဆိုတာ မှတ်ထားပေးပါအုံး။

၇.၂ A Brief History of TCP/IP (TCP/ TP ၏သမိုင်းအကျဉ်း)

TCP/IP Protocol ဟာ ၁၉၇၃ ခုနှစ်ဝန်းကျင်မှာစတင် Introduce လုပ်ခဲ့တယ်ဆိုပေမယ့် ၁၉၈၃ ခုနှစ်ကြမှ စံ (Standardized Version) အဖြစ်စတင်ခဲ့ပြီး Wide Area Network တွေအသုံးပြုဖို့ဖြစ်ပေါ်လာတာပါ။ အဲ့ဒီနှစ်မှာပဲ TCP/IP ဟာ သူ့ရဲ့ရှေ့က ARPAnet အတွက် Official Transport Mechanism ဖြစ်ခဲ့ပါတယ်။ ဒါတွေကိုခြုံပြီးပြောရရင် -

- ❖ ၁၉၇၀ - Advanced Research Agency Network (ARPANET) Hosts တာ Network Control Protocol (NCP) ကိုစတင်အသုံးပြုခဲ့ပါတယ်။
- ❖ ၁၉၇၂ - ပထမဦးဆုံးသော Telnet Specification ဖြစ်တဲ့ Ad hoc Telnet Protocol ဟာ RFC 318 အဖြစ်တင်သွင်းခဲ့ပါတယ်။ RFC ဆိုတာ Request for Comments ပါ။
- ❖ ၁၉၇၃ - RFC 454 ဖြစ်တဲ့ File Transfer Protocol စတင်ပါတယ်။
- ❖ ၁၉၇၄ - Transmission Contorl Program (TCP) ကိုအသေးစိတ်သတ်မှတ်ကြပါတယ်။
- ❖ ၁၉၈၁ - IP Standard ကို RFC 791 မှာထုတ်ပြန်ပါတယ်။
- ❖ ၁၉၈၂ - Defense Communications Agency (DCA) နဲ့ ARPA တို့ Transmission Control Protocol (TCP) နှင့် Internet Protocol (IP) ကိုထုတ်ပါတယ်။

❖ ၁၉၈၃ - ARPANET ဟာ NCP မှ TCP/IP ကိုပြောင်းပါတယ်။

❖ ၁၉၈၄ - Domain Name System (DNS) စတင်ပါတယ်။

၇.၄ TCP/IP Design Goals (TCP/IP ၏ရည်ရွယ်ချက်)

❖ အားလုံးသော Hardware နှင့် Software ထုတ်လုပ်သူတွေကို မမှီခိုရစေဖို့။ TCP/IP ဟာ ဒီနေ့အထိ IBM, Novell, Microsoft, DEC စသည့် Company တွေအပြင် တခြား Company တွေနဲ့လည်း ချိတ်ဆက်ထားခြင်းလည်းမရှိပါဘူး။

❖ နောက်ပြီး သူမှာ Built-in Failure Recovery ပါရှိပါတယ်။ ကြီးမားတဲ့ကွန်ရက်အစိတ်အပိုင်းတစ်ခု ပျောက်ပျက်သွားသည့်တိုင် ဒီ Protocol ဟာ အလုပ်ကိုဆက်လက်လုပ်ကိုင်နိုင်ပါတယ်။

❖ High Error Rates ကိုချုပ်ကိုင်နိုင်သည့်အပြင် End to End Service ကိုပြည့်စုံစွာပံ့ပိုးပေးနိုင်ပါတယ်။ ဘယ်ကွန်ရက်ရဲ့ ဝန်ဆောင်မှုကိုမှ ပျက်တောက်သွားစေခြင်းမရှိဘဲ ကွန်ရက်အသစ်တွေကို ထပ်မံချိတ်ဆက်နိုင်ပါတယ်။

❖ IP Protocol ဟာ Header မှာ 20 Byte ရှိပါတယ်။ တခြားကွန်ရက်တွေနှင့်နှိုင်းယှဉ်ရင် ပိုမိုပြီး Performance ကောင်းစေပါတယ်။

၇.၅ Benefits of Using TCP/IP
(တခြားကွန်ရက်တွေထက်သာတဲ့ TCP/IP ၏အကျိုးကျေးဇူးများ)

❖ TCP/IP ဟာဘယ် Hardware နဲ့ Software ထုတ်လုပ်သူတွေကိုမှ မမှီခိုရခြင်း။

❖ TCP/IP ဟာ အချက်အလက်တွေကို မည်သည့်မတူညီတဲ့ ကွန်ပျူတာစနစ် အမျိုးမတူတ် မည်သည့် မတူညီတဲ့ စက်ထိန်းချုပ်မှုစနစ် (Operating System) အကြားပေးပို့နိုင်ပါတယ်။ ဥပမာ အသေးစား ကွန်ပျူတာကနေ အကြီးစား Mainframe ကွန်ပျူတာတွေအထိပေါ့။

❖ TCP/IP ဟာအခြေခံ Hardware အားဖြင့် Ethernet, Token Ring, X.25, Dial Up Networking တို့နဲ့မတူညီကြပါဘူး။

❖ TCP/IP ဟာ လမ်းကြောင်းလွှဲပေးနိုင်တဲ့ Protocol တစ်ခုဖြစ်တာကြောင့် ကွန်ရက်တွေရဲ့ Traffic ကိုလျော့ချပေးနိုင်ပါတယ်။

❖ အဲဒီအပြင် TCP/IP ဟာ အချက်အလက်တွေကိုပေးပို့တဲ့နေရာမှာ စိတ်ချရတဲ့အပြင် မြန်ဆန်မှုလည်း

ရှိပါတယ်။

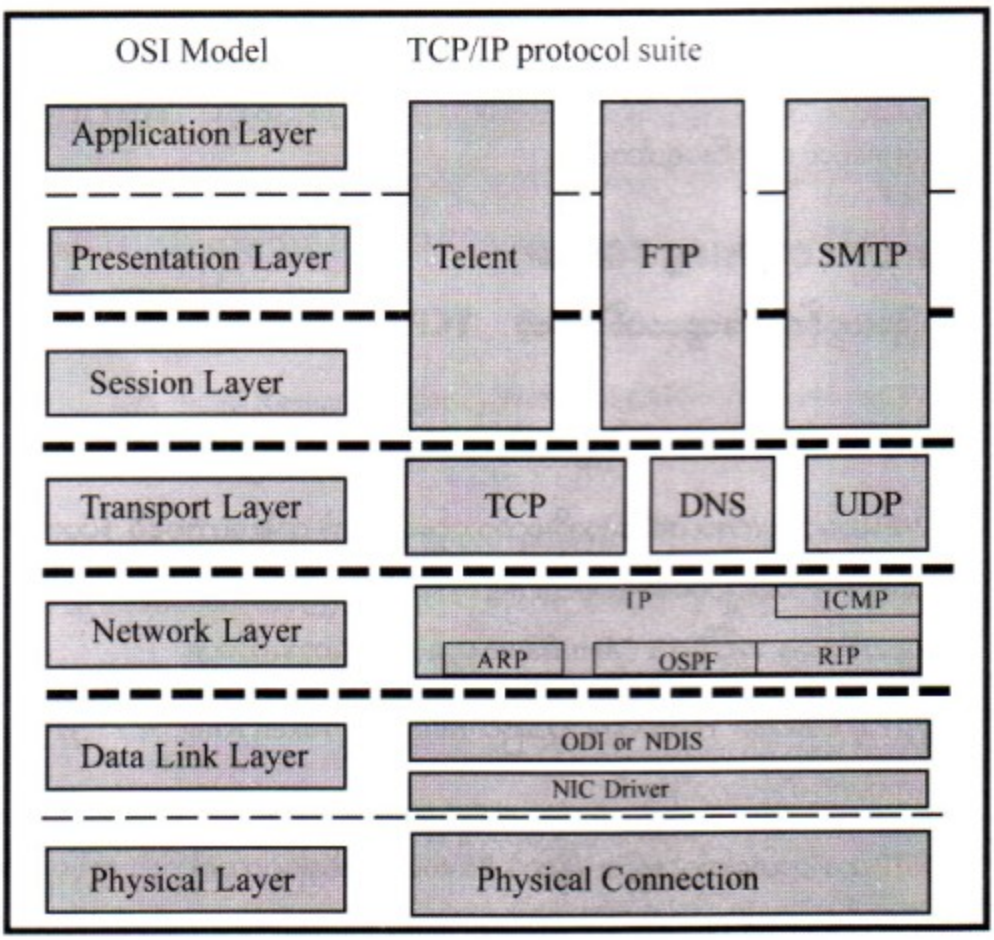
❖ TCP\IP ဟာလိပ်စာတွေနဲ့ပတ်သက်လို့ Common Addressing ကိုအသုံးပြုတာကြောင့် ဘယ်စနစ်မဆို တခြားစနစ်တွေနဲ့ လိပ်စာပိုင်းဆိုင်ရာမှာ အပေးအယူတည့်လို့နေပါတယ်။ ကြီးမားတဲ့ ကွန်ရက်တွေဖြစ်တဲ့ Internet အထိပေါ့။

၃.၅ TCP/IP Vs OSI Model

(တခြားကွန်ရက်တွေထက်သာတဲ့ TCP/IP ၏အဓိကဝိုင်းဝန်းများ)

ရှေ့သင်ခန်းစာတွေမှာ OSI Model အကြောင်းကိုလေ့လာခဲ့ကြပြီးပါပြီ။ OSI Model ဟာအလွှာ (၇) လွှာရှိတယ်ဆိုတာကို သိခဲ့ကြပြီးပါပြီ။ အခု TCP/IP ဟာ အလွှာ (၅) လွှာရှိပါတယ်။ ကဲ လေ့လာကြည့်ရအောင်။ ဩော် ပြောရအုံးမယ်။ အလွှာတွေမှာသိထားရမှာက အောက်အလွှာပံ့ပိုးမှုနဲ့ အပေါ်အလွှာဟာ လုပ်ဆောင်ချက်တွေကိုတည်ဆောက်ပါတယ်။

ပုံ ၇.၁



- OSI Application Layer - ဆိုတာအပေါ်ဆုံးအလွှာပါ။ ကွန်ရက်ရဲ့ ဝန်ဆောင်မှုတွေကို ပံ့ပိုးပေးပါတယ်။
- OSI Presentation Layer - ဆိုတာအချက်အလက်တွေကို ပုံစံပြောင်းခြင်း၊ တင်ပြခြင်း၊ ဘာသာပြန်ခြင်းတို့ကိုပြုလုပ်ရပါတယ်။
- OSI Session Layer - ဆိုတာ လုံခြုံမှုကိုဆောင်ရွက်ရခြင်း၊ Logging လုပ်ခြင်း Administrative နှင့်ပတ်သက်တဲ့ တာဝန်များနဲ့ဆက်စပ်လုပ်ပေးရပါတယ်။
- OSI Transport Layer - ဆိုတာ Messages များတည်ဆောက်ခြင်းနဲ့ပတ်သက်တဲ့ Protocols တွေကိုသတ်မှတ်ပေးရခြင်းနှင့် အမှားများကိုစစ်ဆေးခြင်းဖြင့် Transmission ထိန်းချုပ်ပေးရပါတယ်။
- OSI Network Layer - အချက်အလက်တွေဟာ ပို့လွှတ်တဲ့နေရာကိုမှန်ကန်စွာရောက်ဖို့ လမ်းကြောင်းတွေရဲ့ Protocol တွေကိုသတ်မှတ်ပေးရပါတယ်။
- OSI Data Link Layer - အချက်အလက်တွေကို Synchronizing လုပ်ခြင်းနဲ့ အချက်အလက်ပေးပို့ခြင်းကိုထိန်းချုပ်ပေးခြင်းအားဖြင့် တစ်နေရာမှတစ်နေရာကို အချက်အလက်တွေပို့လွှတ်ပါတယ်။
- OSI Physical Layer - Transmission Medium ဥပမာ Network ကြိုးနဲ့ Interface Hardware ဥပမာ Network Card တို့အကြားဆက်သွယ်မှုကိုပြုလုပ်ပါတယ်။

  ကဲ ဒီတစ်ခါ TCP/IP ရဲ့ အလွှာ (၅)ခုကိုလေ့လာကြည့်ရအောင်။
- TCP/IP Application Layer- အပေါ်ဆုံးအလွှာဖြစ်ပါတယ်။ Application တွေဖြစ်ကြတဲ့ FTP, Telnet တို့ဘာတို့ ညာတို့က ဒီအလွှာနဲ့အလုပ်လုပ်ကြပါတယ်။
- TCP/IP Transport Layer - TCP နဲ့ တခြား Protocol တွေဟာပို့လွှတ်ရမယ့် အချက်အလက်တွေကိုထုတ်ပိုးပါတယ်။
- TCP/IP Internet Layer - အချက်အလက်အထုတ်အပိုးထဲကို IP Information တွေထည့်ပေးလိုက်ပါတယ်။
- TCP/IP Network Interface Layer - Physical Layer နဲ့ အဆက်အဆံပြုလုပ်ပါတယ်။
- TCP/IP Physical Layer - သူကတော့ OSI Model ရဲ့ပထမဆုံးအလွှာလိုပါပဲ။ Transmission Medium ဥပမာ Network ကြိုးနဲ့ Interface Hardware ဥပမာ Network Card တို့အကြားဆက်သွယ်မှုကိုပြုလုပ်ရပါတယ်။

၃.၆ Transmission Control Protocol အကြောင်း

Transmission Control Protocol ဆိုတာ ၎င်း Protocol ရဲ့ Transmission Layer ဖြစ်ပါတယ်။ ကွန်ရက်မှာ အချက်အလက်တွေအပြန်အလှန်ပေးပို့တဲ့နေရာမှာ သေချာမှုတွေ၊ စိတ်ချရမှုတွေဖြစ်ပေါ်အောင် လုပ်ပေးရပါတယ်။ ၎င်းအပြင်သူ့ဟာ အချက်အလက်တွေကို အပိုင်းပိုင်း ဝိုင်းလိုက်ပြီးတော့ လိုအပ်တဲ့အကြောင်းအရာတွေနဲ့ ထုပ်ပိုးလိုက်ပါတယ်။ အဲဒီလို ထုပ်ပေးလိုက်တဲ့ အစိတ်အပိုင်းတစ်ခုကို Datagrams လို့ခေါ်ပါတယ်။ အချက်အလက်တွေကိုပို့ရာမှာ ရည်ရွယ်ရာရောက်ဖို့ TCP ဟာ ၎င်း Datagram ရဲ့ရှေ့မှာ Header ကိုထည့်လိုက်ပါတယ်။ ခုနတုန်းကပြောတဲ့အကြောင်းအရာတွေဆိုတာ အချက်အလက်တွေနဲ့ တွဲမယ့် Header ကိုပြောတာပါ။ ဒီတော့ Header နဲ့အချက်အလက်ပေါင်းထားတာက Datagram ပါ။ Header မှာမှ Source, Destination Port Numbers, Sequence of Datagram, Checksum တို့ကတော့ အရေးကြီးဆုံးပါ။

Source Port Number နဲ့ Destination Port Number ကတော့အချက်အလက်တွေပို့လွှတ်တဲ့နေရာမှာ ကွန်ပျူတာတစ်လုံးချင်းစီပေါ်မှာ မှန်ကန်စွာ Run လုပ်နိုင်အောင်ဖို့ပါ။

ကဲ ဒီတော့ TCP Header ပါဝင်တဲ့ Datagram တစ်ခုကိုလေ့လာကြည့်ရအောင်။

Source Port			Destination Port
Sequence Number			
Acknowledgment Number			
Offset	Reserved	Flags	Window
Checksum			Urgent Pointer
Options			Padding
Start of Data			

- Sequence Number - ဆိုတာကတော့ အချက်အလက်တွေ လိုရာကိုရောက်ပြီးသွားတဲ့အခါမှာတော့ ပို့လိုက်တဲ့ အစီအစဉ်အတိုင်းဖြစ်ဖို့ဆောင်ရွက်ရပါတယ်။
- Acknowledgment Number - ဆိုတာကတော့ အချက်အလက်တွေဟာလိုရာခရီးကိုရောက်ပြီဆိုတာနဲ့ Receiver ဟာ Sender ကို Acknowledgment ပြန်ပို့ပါတယ်။ အကယ်၍ လမ်းမှာအချက်အလက်တွေ ဆုံးရှုံးခဲ့ရင် Receiver ဟာ Serder ကို Acknowledgment မပို့ပါဘူး။ Receiver ဟာသတ်မှတ်ချိန် အတွင်းမှာမှ Acknowledgment ကိုမရရင် မရခဲ့တဲ့ Acknowledgment နဲ့သက်ဆိုင်တဲ့ အချက်အလက်ကို ပြန်ပို့ပါတယ်။

- ❖ Offset - ဆိုတာကတော့ Header ရဲ့အလျားကိုသတ်မှတ်ထားတာပါ။
- ❖ Reserved - ဆိုတာကတော့ နောင်သုံးဖို့သတ်မှတ်ထားတာပါ။
- ❖ Flags - ဆိုတာကတော့လက်ရှိအချက်အလက်အထုပ်ကလေးဟာ လက်ရှိအချက်အလက်ရဲ့ နောက်ဆုံးပါ။ ဒါမှမဟုတ် ဒီအချက်အလက်အထုပ်ကလေးဟာအလျင်လိုပါတယ်။
- ❖ Windows - ဆိုတာကတော့အချက်အလက်တွေကိုပေးပို့တဲ့နေရာမှာပြန်ဆန်စေဖို့ အချက်အလက်ရဲ့ အထုပ်အပိုးအရွယ်အစားကိုတိုးလို့ရအောင်ပံ့ပိုးပေးပါတယ်။
- ❖ Checksum - ဆိုတာကတော့ ပို့လိုက်တဲ့အချက်အလက်တွေဟာ လက်ခံရရှိတဲ့အချက်အလက် တွေနဲ့ ထပ်တူဖြစ်ရဲ့လားဆိုတာစစ်ဆေးရပါတယ်။
- ❖ Urgent Pointer - ဆိုတာကတော့အလျင်လိုတဲ့ အချက်အလက်တွေရဲ့နေရာကိုညွှန်ပါတယ်။
- ❖ Options - ဆိုတာကတော့နောင်တစ်ချိန်သုံးဖို့ချန်ထားခြင်း ဒါမှမဟုတ် အထူးရွေးချယ်မှု တစ်ခုဖြစ် ပါတယ်။
- ❖ Padding - ဆိုတာကတော့ 32 Bit မှာ ဆုံးသွားပြီဆိုတဲ့ Header ရဲ့အဆုံးဖြစ်ပါတယ်။

TCP Communication ကိုအချုပ်ပြောပြရရင်-

- ❖ Acknowledgment ကြောင့် အချက်အလက်ကို လက်ခံတဲ့သူဟာ အချက်အလက်လက်ခံပြီး ကြောင်း ပို့လွှတ်သူကိုသိစေအပ်ပါတယ်။
- ❖ Sequencing ကြောင့် အချက်အလက်တွေဟာ ရည်ရွယ်ရာကိုရောက်ရှိချိန်မှာ အစီအစဉ်ကျပါတယ်။
- ❖ Checksum ကြောင့်အချက်အလက်တွေမှာ ဆုံးရှုံးမှုနဲ့ တစ်ပိုင်းတစ်စပျက်စီးမှုတွေကို အလွယ်တကူ သိရှိနိုင်ပါတယ်။
- ❖ ဒီလိုတစ်ပိုင်းတစ်စ ဒါမှမဟုတ် ဆုံးရှုံးသွားတဲ့ အချက်အလက်တွေကိုပြန်လည်ပို့လွှတ်နိုင်ပါတယ်။

၃.၇ Internet Protocol အကြောင်း

Transmission Control Protocoal ဆိုတာ ၎င်း Protocol ရဲ့ Transmission Layer ဖြစ်ပါတယ်လို့ ပြောခဲ့တယ်နော်။ Internet Protocol ကြတော့ ဒီ TCP/IP ရဲ့ Network Layer အပိုင်းဖြစ်ပါတယ်။ ဆိုလိုချင်တာက ဒီအပိုင်းမှ အချက်အလက်တွေကို ဟို မှ သည်၊ သည် မှ ဟို ကိုပေးပို့တာဖြစ်ပါတယ်။ ဒါကို Routing လို့ခေါ်ပါတယ်။

End to End Connection နဲ့ အချက်အလက်တွေကို စတင်မပို့ခင်မှာ IP ဟာ Information

တွေကိုမထိန်းချုပ်ပါဘူး။ Internet Protocol ဟာ TCP အပေါ်မှီခိုနေရပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့- အချက်အလက်တွေဟာ လိုရာကိုအမှန်တကယ် ပြည့်စုံစွာရောက်ရှိသွားရဲ့လား၊ အကယ်၍ မရောက်ခဲ့ရင် လည်းပြန်ပို့လွှတ်ဖို့ဆိုတာက TCP ဆီကအကြောင်းပြန်မှုပါ။ ဒါကြောင့် IP ဟာ TCP အပေါ်ကို မှီခိုနေရပါတယ်။ တကယ်တော့ IP ဟာအချက်အလက်တွေကို သက်ဆိုင်ရာနေရာကို ပေးပို့ဖို့တစ်ခုတည်းလုပ်ရတာပါ။ IP ဟာ TCP ဆီကနေ အချက်အလက်ကိုရတာနဲ့ သူ့ကိုယ်ပိုင် IP Header တစ်ခုကို Datagram မှာထည့်လိုက်ပြန်ပါတယ်။ IP ရဲ့ Header မှာအကြောင်းအရာတွေအများကြီးရှိပေမယ့် Source & Destination Address, Protocol Number, Checksum တို့ကအရေးကြီးဆုံးဖြစ်ပါတယ်။

- ❖ Version ဆိုတာကတော့ IP Version နံပါတ်ကိုဖော်ပြတာပါ။ ဒီနေရာမှာ Version 4 ဟာလက်ရှိ Standard ဖြစ်ပြီးတော့ အကယ်၍ 5 တို့ 6 တို့ဆိုရင် Special Protocol ကိုအသုံးပြုထားတာကိုပြောတာပါ။
- ❖ IHL (Internet Header Length) - ဆိုတာကတော့ Information ရဲ့ Header အလျားကိုသတ်မှတ်တာဖြစ်ပြီး ၎င်းအလျားဟာ တရားသေမဟုတ်ဘဲ ပြောင်းလဲနိုင်ပါတယ်။

Version	IHL	TOS	Total Length	
Identifiacation			Flags	Fragmentation Offset
Time to Live	Protocol		Header Checksum	
TCP Header				
Start of Data				

- ❖ TOS (Type of Service) - ဆိုတာကတော့ လိုအပ်တဲ့ဝန်ဆောင်မှုအမျိုးအစား ဒီမှမဟုတ် အရေးပါမှုကိုညွှန်ပြတာပါ။
- ❖ Total Length - ဆိုတာကတော့ Datagram ရဲ့အလျားကိုဖော်ပြတာပါ။ အနည်းဆုံး 576 Bytes ကနေ အများဆုံး 65,536 Bytes အထိရှိတတ်ပါတယ်။
- ❖ Identification - ဆိုတာကတော့ လက်ခံရရှိတဲ့ဘက်ကနေမှ ပျံ့ကျဲ (Fragmented) နေတဲ့ Datagram ကိုပြန်ပြီးဖွဲ့စည်းဖို့အတွက် အချက်အလက်တွေကို ပံ့ပိုးပေးရပါတယ်။
- ❖ Flags - ဆိုတာကတော့ ၎င်းရဲ့ ပထမ Bit ဟာဒီ Datagram ဟာ Fragmented မဖြစ်သင့်ဘူး ဆိုတာရယ် ဒုတိယ Bit ဟာ ဒီ Datagram ဟာ Fragmented ဖြစ်နေတဲ့အချက်အလက်တွေရဲ့

နောက်ဆုံး Datagram ဖြစ်တယ်ဆိုတာပါ။

- ❖ Fragmentation Offest - ဆိုတာကတော့ အချက်အလက်တွေရဲ့ မူရင်းနေရာကိုညွှန်ပြပါတယ်။ အဓိပ္ပာယ်လျှင် ပြန်လည်ဖွဲ့စည်းလို့ရမည်မဟုတ်ပါလား။
- ❖ Time of Live - ဆိုတာကတော့ Datagram ကစောင့်ဆိုင်းနားခိုရမယ့်အချိန်ကိုပြောတာပါ။ Seconds နဲ့ဖော်ပြပါတယ်။
- ❖ Protocol - ဆိုတာကတော့ Protocol အမျိုးအစားတွေကိုသတ်မှတ်ပေးတာပါ။ TCP/IP မဟုတ်တဲ့ Protocol တွေကိုလည်းအသုံးပြုခွင့်ပေးထားပါတယ်။ ဒီနေရာမှာ 6 လို့ပြောရင် TCP ဖြစ်ပြီး 17 လို့ပြောရင် User Datagram Protocol (UDP) ဖြစ်ပါတယ်။
- ❖ Header Checksum - ဆိုတာကတော့ Error Checking အတွက်ဖြစ်ပါတယ်။
- ❖ TCP Header - ဆိုတာကတော့ TCP ကထည့်ပေးလိုက်တဲ့ Header ဖြစ်ပါတယ်။

၇.၈ Internet Control Message Protocol (ICMP)

ICMP ဟာ Network Layer Protocol ဖြစ်ပါတယ်။ Control Messages တွေဖြစ်ကြတဲ့ Error Message တို့၊ Flow Control Instructions တို့၊ Confirmations တို့ကိုပေးပို့တဲ့နေရာတွေမှာ အသုံးပြုပါတယ်။ ထပ်ရှင်းပြရမယ်ဆိုရင် TCP/IP Utility တစ်ခုဖြစ်တဲ့ PING Utility ဟာ Remote Host ကနေ Response တုံ့ပြန်မှုရဖို့တောင်းဆိုတဲ့အခါမှာ ၎င်းကိုအသုံးပြုရကောင်း ပြုရနိုင်ပါတယ်။ PING Utility ဟာ ICMP ကိုဘယ်နေရာမှာအသုံးပြုတာလဲဆိုတော့ Remote ကို Responses လုပ်တဲ့ Return Message တွေမှာပါ။ PING ရိုက်လာလျှင်သူကသွားပြီး IP Address တို့ ဘာတွေစုံစမ်းတယ်။ ပို့စရာရှိတာတွေပို့ကြတယ်။ အောင်မြင်တယ်ဆိုရင်လည်း အောင်မြင်ကြောင်း၊ သတ်မှတ်ထားတဲ့အချိန်မှာ Host ကို မရောက်လျှင်လည်း မအောင်မြင်ကြောင်းပြန်ပြောတဲ့ Message ကိုပေးရာမှာအသုံးပြုတယ် လို့ပြောချင်တာပါ။

၇.၉ Address Resolution Protocol (ARP)

ARP ဆိုတာကလည်း Network Layer Protocol ပဲဖြစ်ပါတယ်။ ၎င်းဟာ Logical IP Address နှင့် Physical (MAC) Address ကိုပူးပေါင်းဆက်စပ်ပေးတဲ့နေရာမှာ အသုံးပြုပါတယ်။

၃.၁၁ User Datagram Protocol (UDP)

UDP ဆိုတာ Connectionless Transport အလွှာ Protocol ဖြစ်ပါတယ်။ ၎င်းဟာ ပြန်တယ်ဆိုပေမယ့် TCP လောက်တော့စိတ်မချရပါဘူး။ ဒါပေမယ့်လည်း TCP/IP ရဲ့အနည်းငယ်မျှသော အပေါ်ပိုင်းအလွှာ Services တွေလောက်ပဲ TCP ကိုသူတို့ရဲ့ Transport Protocol အဖြစ်သုံးတာပါ။ ဥပမာပြောရရင် Network File System လိုဟာမျိုးက UDP ကို Transport Protocol အဖြစ်အသုံးပြုပါတယ်။

၃.၁၁ Domain Name System (DNS)

DNS ဆိုတဲ့ Domain Name Service ဟာ Hosts Name နဲ့ Domain Name တွေကို IP Address အဖြစ်အပြန်အလှန်ပြောင်းတဲ့နေရာမှာ အသုံးပြုပါတယ်။ DNS ဟာ TCP/IP ကွန်ရက်ရဲ့ မရှိမဖြစ်လိုအပ်လှတဲ့အစိတ်အပိုင်းဖြစ်ပါတယ်။ ဥပမာပြောရရင် သင်ဟာ အင်တာနက်ကိုဝင်လိုက်တယ်ဆိုကြပါစို့။ http://www.microsoft.com ထဲကိုဝင်လိုက်ပြီး Microsoft Home Page ပေါ်လာမယ်ဆိုကြပါစို့။ ဒီတစ်ခါ Web Browser က TCP/IP ကို DNS Server ဆီလှမ်းမေးခိုင်းပါတယ်။ www.Microsoft.com ရဲ့ IP Address ကိုပါ။ Web Browser ဟာ IP Address ကိုရပြီဆိုတာနဲ့ Microsoft Web Server ကိုလှမ်းချိတ်လိုက်ပြီး Home Page ကိုခေါ်လိုက်ပါတယ်။

DNS Tables ဆိုတာ Hosts Name, Domain Name နဲ့ IP Address တွေဖွဲ့စည်းထားတဲ့ Record တွေပါဝင်ပါတယ်။ Record အမျိုးအစားတွေအမျိုးမျိုးရှိပါတယ်။ အဲဒီတွေကတော့ Address Record, Mail Exchange Record, CNAME Record တို့ဖြစ်ကြပါတယ်။ Address Record ကိုတော့ A လို့အမှတ်အသားထားပြီး၊ Mail Exchange Record ကိုတော့ MX လို့သတ်မှတ်ပြီး၊ CNAME Record ကိုတော့ CNAME လို့သတ်မှတ်ပါတယ်။ အောက်မှာ DNS Table ဥပမာလေးတွေကြည့်ရအောင်။

mail.company.com	IN	A	204.176.47.9
www.microsoft.com	IN	A	198.105.232.6
yourhost.company.com	IN	MX	10 mail.company.com.
ftp.company.com	IN	CNAME	www.company.com

၃.၁၂ File Transfer Protocol (FTP)

FTP ဆိုတာ Upper Layer Protocol ဖြစ်ပါတယ်။ ပုံမှာလည်း တွေ့နိုင်ပါတယ်။ သူက Session အလွှာရယ်၊ Presentation အလွှာရယ်၊ Application အလွှာရယ်မှာ ပူးပေါင်းပြီးအလုပ်လုပ်တာဖြစ်ပါတယ်။ FTP ဟာ File တွေကို Transfer လုပ်ခြင်း၊ Service ကိုပံ့ပိုးပေးတဲ့အပြင် File နှင့် Directory တွေ

Manipulation လုပ်တဲ့ Services တွေကိုပါပံ့ပိုးပေးပါတယ်။ Manipulation Services ဆိုတာ File တွေ၊ Directory တွေကို List ကြည့်ခြင်း၊ ကော်ပီကူးခြင်း၊ Delete လုပ်ခြင်းစတာတွေပေါ့။ ဒီ FTP ရှိနေတဲ့အပေါ် အလွှာတွေတစ်လွှာချင်းစီဟာ သူတို့ရဲ့သတ်မှတ်ထားတဲ့ဝန်ဆောင်မှုတွေကို FTP ကိုပံ့ပိုးပေးပါတယ်။ ဥပမာ ပြောရရင် Session Layer ဟာ Connection များကိုဖြစ်ပေါ်ပေးရခြင်း (Establishment) နှင့်ပြန်ဖြုတ်ပေးရခြင်း (Release) လုပ်ပေးရခြင်းတို့ကို လုပ်ဆောင်ပေးရတယ်။

၇.၁၃ Telnet

Telnet ဆိုတာ Remote Terminal Emulasion Protocol ဖြစ်ပါတယ်။ ၎င်းဟာ အပေါ်အလွှာသုံးလွှာစလုံးမှာ အလုပ်လုပ်တာဖြစ်ပြီး များသောအားဖြင့် ချိတ်ဆက်မှုဖြစ်ပေါ်အောင်ပံ့ပိုးပေးရတာဖြစ်ပါတယ်။ ဘယ်လိုချိတ်ဆက်မှုတွေကို ပံ့ပိုးပေးရတာလဲဆိုတော့ မတူညီတဲ့စနစ်တွေအကြားမှာ ချိတ်ဆက်မှုဖြစ်အောင်ပါ။ ဥပမာ PC နှင့် Router အကြားဆက်သွယ်မှုမျိုးပါ။ Telnet ကြောင့် Remote Equipment တွေဖြစ်တဲ့ ဥပမာပြောရရင် Router တို့ Switch တို့ကိုစောင့်ကြည့်နိုင်မယ်။ Monitor Setting ချိန်နိုင်မယ်။ (Configured) နှင့် Remote System ကို Operate လုပ်နိုင်ပါတယ်။ Telnet ဆိုတဲ့ စကားလုံးဟာ တစ်စုံတစ်ခုရဲ့ အတိုကောက် မဟုတ်ပါဘူး။

၇.၁၄ Simple Mail Transport Protocol (SMTP)

SMTP ဆိုတာ ပုံ (၇.၁) မှာလည်းမြင်တွေ့ရမှာပါ။ ခုနကလိုပဲ အပေါ်အလွှာ (၃)လွှာမှာအလုပ်လုပ်တဲ့ နောက်ထပ် Protocol တစ်ခုပဲဖြစ်ပါတယ်။ ဒီ Protocol ဟာ သူ့နာမည်အတိုင်းပါပဲ။ TCP/IP ဆီသို့ Messaging Service များပံ့ပိုးပေးခြင်းကိုလုပ်ဆောင်ပါတယ်။ အဲ့ဒီအပြင် SMTP ဟာ အင်တာနက်လိုဖြတ်ပြီးသွားတဲ့ အများစုသော E-Mail တွေရဲ့အခြေခံလည်းဖြစ်ပါတယ်။

၇.၁၅ Routing Information Protocol (RIP)

RIP ဆိုတာ အရိုးရှင်းဆုံးသော IP ကိုအခြေခံထားတဲ့ Protocol ပဲဖြစ်ပါတယ်။ တစ်နည်းအားဖြင့် Distance Vector Protocol လည်းဖြစ်ပါတယ်။ ၎င်းကို လမ်းကြောင်းရှာဖွေတဲ့အခါမှာ အသုံးပြုပါတယ်။ အခြားသော Routing Protocol တွေလိုပါပဲ။ Network ရဲ့ လမ်းကြောင်းနှင့် အခြေအနေတွေကိုစုဆောင်းရန်နှင့် ဖလှယ်ရန်အတွက် RIP ဟာ Network Layer မှာအလုပ်လုပ်ပါတယ်။ လက်ရှိအကောင်အထည်ဖော်နေတဲ့ RIP ကိုတော့ RIPV2 လို့ခေါ်ပြီး ၎င်းဟာ မူလ RIP ထက်စာရင်ပိုမိုခိုင်မာအားသာတဲ့ Performance ရရှိလာတဲ့အပြင် ပိုမိုပြီးတော့လည်း စိတ်ချရမှုရှိလာပါတယ်။ ၎င်းကိုသေးငယ်တဲ့ TCP/IP Network တွေမှာ

ကျယ်ပြန့်စွာအသုံးပြုနေကြဆဲဖြစ်ပါတယ်။ RIP ဟာကြီးမားပြီး ရှုပ်ထွေးတဲ့ TCP/IP Network တွေနဲ့ မသင့်တော်ပါဘူး။ အဲဒီမျိုးဆိုရင်တော့ ယေဘုယျအားဖြင့် ဒီအသုံးပြုတဲ့ကွန်ရက်အတွင်းမှာ လမ်းကြောင်းရှာခြင်းကိစ္စကို OSPF ကဆောင်ရွက်ပါတယ်။

၃.၁၆ Open Shortest Path First (OSPF)

OSPF ဟာ TCP/IP ကိုအသုံးပြုတဲ့ ကွန်ရက်တွေမှာအကောင်းဆုံးလမ်းကြောင်းကိုရှာဖွေပေးမယ့် Routers တွေက ၎င်းကို Link-State Routing Protocol အဖြစ်အသုံးပြုပါတယ်။

၃.၁၇ IP Address အခြေခံ

TCP/IP ဟာငြား TCP/IP ကွန်ရက်ပေါ်ကကွန်ပျူတာတိုင်းမှာ တစ်လုံးနဲ့တစ်လုံးမတူညီတဲ့ ကိုယ်ပိုင်လိပ်စာတွေကိုလိုအပ်ပါတယ်။ IP Address ဟာယေဘုယျအားဖြင့် အပိုင်းလေးပိုင်းရှိပြီး 32 bit ဖြစ်ပါတယ်။ IP Address ရဲ့အပိုင်းလေးပိုင်းဟာ တစ်ခုနဲ့တစ်ခုကြားမှာ Decimal Point လေးတွေနဲ့ခြားထားပါတယ်။ ပေးလို့ရတဲ့အတိုင်းအတာကတော့ ၁ ကနေ ၂၅၄ အထိဖြစ်ပါတယ်။

ကွန်ရက်အမျိုးအစားပေါ်မူတည်ပြီးတော့ IP ကို ကွန်ရက်ရဲ့လိပ်စာ (Address for the Network) နဲ့ Hosts ရဲ့လိပ်စာ (Address for the Host) ဆိုပြီးခွဲခြားထားလိုက်ပါတယ်။ ယေဘုယျအားဖြင့်တော့ ရှေ့ပိုင်းက Address for the Network ဖြစ်ပြီးကျန်တဲ့အပိုင်းကတော့ Address for the Hosts ဖြစ်ပါတယ်။ ပုံ ၁၁ (က) ကိုကြည့်ပါ။ အကယ်၍သင်ဟာ အင်တာနက်ကိုချိတ်မယ်ဆိုရင်တော့ အောက်ပါအမျိုးအစားတွေကို သိဖို့လိုပါတယ်။

❖ Class A - ဆိုတာကတော့ အလွန်ကြီးမားတဲ့ ကွန်ရက်တွေမှာအသုံးပြုပါတယ်။ ရှေ့ဆုံးက Bits ဟာ Zero ဖြစ်ပါတယ်။ ကျန်တဲ့ 7 Bits ဟာ ကွန်ရက်ပေါင်း ၁၂၇ ခုသတ်မှတ်ပေးနိုင်ပြီး နောက်က 32 Bits ကို ရှေ့က 8 Bits နှတ်တော့ ကျန်တဲ့ 24 Bits က ကွန်ရက်တစ်ခုချင်းစီကနေ Hosts ပေါင်း 16,777,216 ကိုကိုင်တွယ်နိုင်ပါတယ်။ Class A ကွန်ရက်များမရနိုင်တော့ပါ။

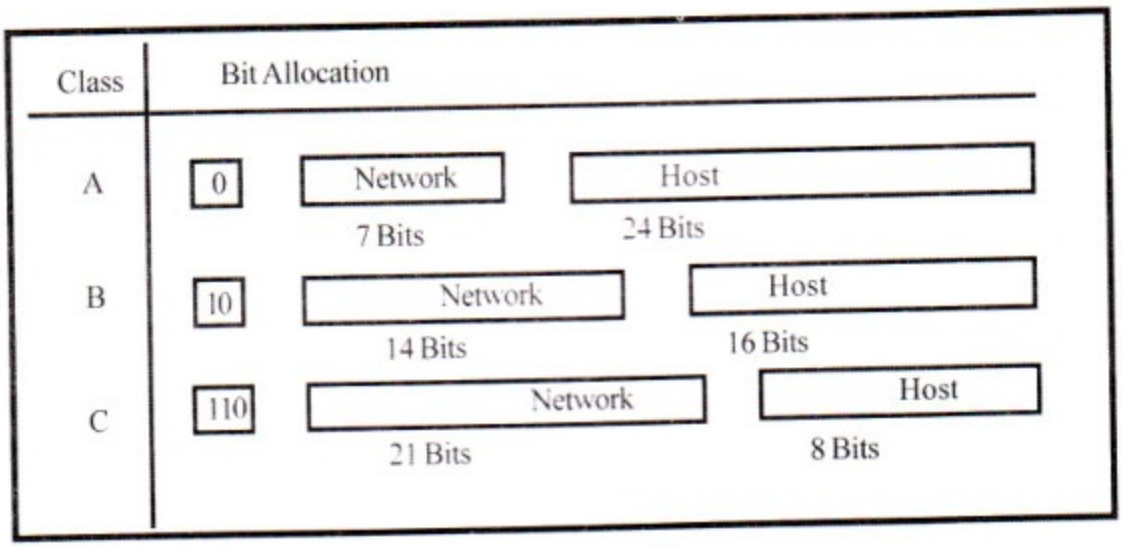
ပထမ 8 Bits ဟာတစ်နည်း အပိုင်းလေးပိုင်းထဲက ပထမဆုံးအပိုင်းဟာ Network Address အပိုင်းဖြစ်ပြီး ကျန်သုံးပိုင်းဟာ Host Address အပိုင်းဖြစ်ပါတယ်။ Network Address တန်ဖိုးဟာ ၁၂၆ အောက်မှ ၁၂၆ အထိပေးလို့ရပါတယ်။ ဘာလို့လဲဆိုတော့ အပေါ်မှာပြောထားတဲ့အတိုင်း ကွန်ရက်က ၁၂၇ အထိပဲ သတ်မှတ်နိုင်တယ်လေ။

မှတ်ချက် ။ ။ အဲ့ဒီနေရာမှာ ၁၂၇ ဆိုတာ Loopback Test Address အတွက် Reserved လုပ်ထားတာပါ။ သင်ဟာ 127.0.0.1 ဆိုတဲ့စိကို Message ပို့လိုက်ရင် အကယ်၍များကွန်ရက်မှာဘာအမှားတစ်ခုမှမရှိရင် ၎င်းဟာသင့်ဆီကိုပြန်ရောက်လာပါလိမ့်မယ်။

❖ Class B - ဆိုတာကတော့ အလယ်အလတ်တန်းစား ကွန်ရက်တွေမှာသုံးဖို့ပါ။ ရှေ့ဆုံး ၂ ခုသော Higher Order Bits ဟာအမြဲတမ်း 10 ဖြစ်ပြီး၊ ကျန်တဲ့ 14 Bits ဟာ ကွန်ရက်ပေါင်း 16,384 ကိုသတ်မှတ်နိုင်ပြီး ပေါင်းလို့ရတဲ့ Bits ဟာ 16 Bits ရှိတာကြောင့် နောက်ကျန်တဲ့ 16 Bits ဟာကွန်ရက် တစ်ခုချင်းစီကနေ Hosts ပေါင်း 65,535 ကိုင်တွယ်နိုင်ပါတယ်။ သူလည်း Class A ကွန်ရက်လိုအားလုံး အသုံးပြုနေကြတာကြောင့်မရနိုင်တော့ပါ။

ဒီတော့ အပေါ်ကမှတ်ချက်အတိုင်းအရဆိုရင် နံပါတ်က ၁၂၇ အထိရှိနေပြီးတာကြောင့် Class B ကွန်ရက်ရဲ့ Address ဟာ 128 ကနေစရပါတယ်။ 191 အထိပါ။ ပထမအပိုင်းနဲ့ ဒုတိယအပိုင်းဟာ Network Address ဖြစ်ပြီး၊ ကျန်တဲ့နှစ်ပိုင်းဟာ Hosts Address ဖြစ်ပါတယ်။

ပုံ ၇.၂



❖ Class C - ဆိုတာကတော့ ကွန်ရက်အငယ်စားအတွက်ပါ။ ရှေ့ဆုံးက ၃ ခုသော Higher Order Bits ဟာအမြဲတမ်း 110 ပါ။ ကျန်တဲ့ 21 Bits ဟာကွန်ရက်ပေါင်း 2,097,157 ကိုသတ်မှတ်ပြီး 32 Bits မှာကျန်ခဲ့တဲ့ 8 Bits ကတော့ကွန်ရက်တစ်ခုချင်းစီမှာ Hosts ပေါင်း 254 အများဆုံးပဲရနိုင်ပါတယ်။ Class C ကွန်ရက်တွေရနိုင်ပါသေးတယ်။

Class C ကွန်ရက်ကတော့ 192 ကနေ 223 အတွင်းရပါတယ်။ ပထမအပိုင်း ၃ ပိုင်းကတော့ Network Address ဖြစ်ပြီး ကျန်တစ်ပိုင်းကတော့ Hosts Address အပိုင်းဖြစ်ပါတယ်။ 223 အထက်ကတော့ Reserve ဖြစ်ပါတယ်။

၇.၁၈ Subnets အကြောင်း

မူလပထမ Designers တွေဟာ အင်တာနက်ကို အခုလောက်ထိကြီးလာလိမ့်မယ်လို့ စိတ်ကူးမယဉ်ခဲ့ကြပါဘူး။ ပြောရရင် ဘယ်သူမှလည်း PC တွေမှာ Memory ကို 640 KB ထက် ပိုလိုအပ်လိမ့်မယ်လို့ ထင်ခဲ့ကြလို့လဲ ဆိုသလိုဖြစ်နေပါလိမ့်မယ်။ အဲ့ဒီအချိန်နဲ့ တစ်ပြိုင်တည်းဆိုသလို 32 Bits ရှိတဲ့ Address ကိုအထက်မှာပြောပြခဲ့တဲ့အတိုင်း ပိုင်းလိုက်ကြပါတယ်။ ပိုင်းလိုက်ကြတဲ့အကြောင်းအရင်းကတော့ ခုနကပြောသလို အင်တာနက်ကြီးက ဒီလောက်ထိကြီးလာမယ်မထင်တော့ ကြီးထွားလာမယ့် Network Address တွေအတွက် Reverse လုပ်ထားမယ့်အစား အခုလိုခွဲပစ်လိုက်ခြင်းဖြင့် လမ်းကြောင်းလွှဲ (Routing) ရတာလွယ်ကူသွားမယ်ဆိုပြီးတော့ပါ။ ဒီပြဿနာကိုဖြေရှင်းဖို့အတွက် တစ်နည်းအားဖြင့် နောက်ထပ်အသစ်ပေါ်လာတဲ့ Network Address အသစ်တွေအတွက် နောက်ထပ် ထပ်ပိုင်းထားတဲ့ 32 Bits Address ဆိုတာပေါ်ပေါက်လာပြန်ပါတယ်။ ဒါကို Subnetting လို့ခေါ်ပါတယ်။

ဒီတော့ IP Subnet ဟာ IP Address ကိုပြုပြင်ပါတော့တယ်။ ဒီတော့ IP Address မှာရှေ့ပိုင်းက Network Address ဖြစ်တယ်နော်။ နောက်ပိုင်းက Host Address ဖြစ်တယ်နော်။ ဒါအပေါ်မှာ ပြောခဲ့ပြီးပြီ။ အခုသူက နောက်က Host Address ကို Network Address အဖြစ်ယူလိုက်ပါတယ်။ တစ်နည်းအားဖြင့် ပြောရရင် Network Address နဲ့ Host Address ကိုပိုင်းထားတဲ့ကြားက လိုင်းကိုညာဖက်ကိုရွှေ့လိုက်သလိုပေါ့ဗျာ။ ဒီတော့ Network Address Bits ကများလာတယ်။ ဒါကြောင့် ရနိုင်တဲ့ကွန်ရက်ကများလာတယ်။ ဒါပေမယ့် Host Address Bits ကလျော့လာတာကြောင့် ကွန်ရက်တစ်ခုမှာ ရနိုင်တဲ့ Host အရေအတွက်လျော့ကျသွားပါတယ်။

IP Address တစ်ခုကို Subnet လုပ်တော့မယ်ဆိုရင် Bit Pattern မှာမလိုအပ်တဲ့ Bits တွေကို ဖယ်ထုတ်ပါတယ်။ ဒါကို Bit Mask လုပ်တယ်။ တစ်နည်းအားဖြင့် Subnet Mask လို့ခေါ်ပါတယ်။ Subnet Masks နဲ့အလုပ်လုပ်တာ ကွန်ရက်ကိုထိန်းချုပ်မှုစနစ်မှာ အတော့်ကိုရှုပ်ထွေးပါတယ်။ ဒီလိုပြောလို့ အားငယ်စိတ်ပျက်မသွားပါနဲ့ဦး။ ကွန်ရက်တစ်ခုမှာ နောက်ထပ် ထပ်ခွဲထားတဲ့ကွန်ရက် (Segment) မရှိရင် တစ်နည်းအားဖြင့်ကွန်ရက်တစ်ခုမှာ Routers မရှိရင် Subnetting လုပ်စရာမလိုပါဘူး။ အကယ်၍ကွန်ရက်တစ်ခုမှာ နှစ်ခု ဒါမှမဟုတ် ငါးထက်ပိုတဲ့ Segments တွေရှိနေပြီဆိုမှ လုပ်ရမှာဖြစ်ပါတယ်။ အောက်မှာ ပထမဖော်ပြခဲ့ပြီးတဲ့ Standard IP Address အမျိုးအစားတွေနဲ့ တွဲပြီး Subnet Mask များကိုဖော်ပြပေးထားပါတယ်။

ပုံ ၇.၃

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

Subnetting လုပ်ခြင်းကြောင့်ရရှိလာသော အကျိုးကျေးဇူးများမှာ -

- ❖ Routing Tables ၏အရွယ်အစားကိုလျှော့ချနိုင်ခြင်း
- ❖ ကွန်ရက်၏လမ်းကြောင်းပိတ်မှုကိုလျှော့ချနိုင်ခြင်း
- ❖ ကွန်ရက်ကိုသီးခြားစီရှင်ခေခြင်း
- ❖ အပြန်အနှန်းကိုမြှင့်တင်နိုင်ခြင်း
- ❖ IP Address Space ပိုရလာခြင်း
- ❖ ကွန်ရက်ရဲ့လုံခြုံမှုစွမ်းရည်ပိုလာခြင်း တို့ဖြစ်ကြပါတယ်။

TCP/IP Class	Class A	Class B	Class C
Format	net.node.node.node	net.node.node.node	net.node.node.node
Default Subnet	255.0.0.0	255.255.0.0	255.255.255.0
Range for First Octet	1-127	128-191	192-223
Sample Address	125.162.102.134	158.192.102.123	204.124.142.126
Total Node Addresses Per Network	(2^24)-2 16,777,214	(2^16)-2 65,534	(2^8)-2 254
Total Network Addresses	2^(8-1) 127	2^(16-2) 16,384	2^(24-3) 2,097,152

၃.၁၉ Name Resoluting Method အကြောင်း

IP Address ဆိုတာရှည်လျားတဲ့ Dotted Decimal တွေမဟုတ်လား။ တစ်နေရာကိုဝင်ဖို့အရေး Address ကိုမှတ်မိဖို့ဆိုတာမလွယ်ဘူးလေ။ ဒါကြောင့် Internet Host Name ကိုလိုအပ်တာပေါ့။ တကယ်တော့ Internet Host Name ဆိုတာတိကျစွာသတ်မှတ်ထားတဲ့ IP Address ရှိသောပစ္စည်းရဲ့ နာမည်ပဲဖြစ်ပါတယ်။ နောက်ပြီးတော့ အင်တာနက်မှအသုံးပြုတဲ့ Fully Qualified Domain Name ရဲ့ အစိတ်အပိုင်းတစ်ခုလည်းဖြစ်ပါတယ်။ Fully Qualified Domain Name မှာအပိုင်းနှစ်ပိုင်း ပါပါတယ်။ Host Name နဲ့ Domain Name ပါ။ IP Address အတွက် Host Name ရှာဖွေခြင်းလုပ်ငန်းစဉ်ကို Name Resolution လို့ခေါ်ပါတယ်။

၃.၂၀ Internet Domain Organization အကြောင်း

com	-	Commercial Organization စီးပွားရေးအဖွဲ့အစည်း
edu	-	Education Establishment ပညာရေးအဖွဲ့အစည်း
gov	-	A branch of the U.S. Government အမေရိကန်အစိုးရအဖွဲ့အစည်း
int	-	An International Organization နိုင်ငံတကာအဖွဲ့အစည်း ဥပမာ UN
net	-	Network Organization ကွန်ရက်အဖွဲ့အစည်း
org	-	Non Profit Organization အမြတ်အတွက်လုပ်တာမဟုတ်သောအဖွဲ့အစည်း

Local ISP တွေဟာ .net Member တွေဖြစ်ကြပါတယ်။ စီးပွားရေး Company တွေကတော့ .com ပါ။ .gov နဲ့ .mil ကတော့ အမေရိကန်ရဲ့အစိုးရပိုင်းနှင့်စစ်ပိုင်းဆိုင်ရာ အသုံးပြုထားတာကြောင့် တခြားသော နိုင်ငံတွေရဲ့ Domain တွေဟာ ဥပမာ .ca ဆို Canada,.jp for Japan, .au for Australia စသည်တို့ဖြစ်ကြပါတယ်။ အကျယ်ကို တစ်ဖက်စာမျက်နှာတွင်ကြည့်။

၃.၂၁ Windows ဗေါ်ကာ TCP/IP နှင့်ဝင်သက်ခြင်း

TCIP/IP ကို System နိမ့်တွေဖြစ်တဲ့ Windows 98, Windows NT, Windows 2000 ပေါ်မှာ Configure မလုပ်ခင် အောက်ပါအချက်လေးတွေကိုသိထားသင့်ပါတယ်။ အဲ့ဒါတွေကတော့ -

(၁) Dynamic Host Configuration Protocol (DHCP)

(၂) Domain Name System (DNS)

(၃) Windows Internet Naming Service (WINS)

(၄) Host Files တို့ဖြစ်ကြပါတယ်။

Domain Name	Interpretation	Domain Name	Interpretation
aq	Antarctica	hu	Hungary
ar	Argentina	ie	Ireland
at	Austria	il	Israel
au	Australia	in	India
be	Belgium	is	Iceland
bg	Bulgaria	it	Italy
br	Brazil	jp	Japan
ca	Canada	kr	South Korea
ch	Switzerland	kw	Kuwait
cl	Chile	lu	Luxembourg
cn	China	mx	Mexico
cr	Costa Rica	my	Malaysia
cs	Czech and	mm	Myanmar
	Slovak Republics	nl	Netherlands
de	Germany	no	Norway
dk	Denmark	nz	New Zealand
ec	Ecuador	pl	Poland
ee	Estonia	pt	Portugal
eg	Egypt	se	Sweden
es	Spain	sg	Singapore
fi	Finland	su	Soviet Union
fr	France	th	Thailand
gb	Great Britain	tw	Taiwan
gr	Greece	ve	Venezuela
hk	Hong Kong	yu	Yugoslavia
hr	Croatia	za	South Africa

၇.၂၂ Dynamic Host Configruation Protocol (DHCP)

အသုံးပြုသူ ၁၀၀ မကသုံးနေတဲ့ TCP/IP Networks ကြီးတွေမှာ Workstation တိုင်းကိုလိုက်ပြီး TCP/IP Parameters အားလုံး Configure လုပ်ရတာ ဘယ်လောက်တောင်အချိန်ကုန်လိုက်မလဲ။ ဒါကြောင့် System စီမံခန့် TCP/IP Confitration အချက်အလက်တွေကို အလိုအလျောက်သတ်မှတ်ပေးမယ့် Protocol ဟာဖြစ်ပေါ်လာရပါတော့တယ်။ ဒါဟာ DHCP ပဲပေါ့။ ၎င်း DHCP ဟာ TCP/IP ကွန်ရက်တွေမှာ Host တွေကို TCP/IP Address, Subnet Mask နှင့် Default Gateway တွေကိုအလိုအလျောက်သတ်မှတ်ပေးပါတယ်။ DHCP ကိုအသုံးပြုချိန်မှာ ကျွန်တော်တို့တွေဟာ TCP/IP Information တွေကိုနည်းလမ်းနှစ်လမ်းနှင့်သတ်မှတ်ပေးနိုင်ပါတယ်။ အဲဒါကတော့ -

(၁) Static Assignment နှင့်

(၂) Dynamic Assignment တို့ပဲဖြစ်ကြပါတယ်။

Static Assignment

TCP/IP Address Information တွေကို Static Method နှင့်သတ်မှတ်ပေးတဲ့အခါ ကျွန်တော်တို့ဟာ Address ကိုကြိုတင်သတ်မှတ်ပေးဖို့ လိုကိုလိုအပ်ပါတယ်။ ဒီတော့ ကျွန်တော်တို့ဟာ DHCP Server Configuration မှာ MAC Address, Computer Name နှင့် TCP/IP Address တို့ကိုဖြည့်ပေးရမှာဖြစ်ပါတယ်။ DHCP Server ဟာ ၎င်း Station အတွက် IP Address တောင်းဆိုမှုကိုလက်ခံရရှိတဲ့အခါ ၎င်းဟာ တောင်းခံတဲ့ Station ရဲ့ (ခုနကဖြည့်ထားတဲ့) MAC Address ကိုကြည့်ပြီး (၎င်း MAC Address ပေါ်မူတည်ပြီး) TCP/IP Information တွေကိုသတ်မှတ်လိုက်ပါတယ်။ ဒီ Static Assignment နည်းမှာ DHCP Server ဟာဖြည့်ထားတဲ့ DHCP Server ကိုကြည့်ပြီး TCP/IP Configuration ကို Workstation ဆီ ပို့လွှတ်လိုက်ရုံကိုသာလုပ်ရတာဖြစ်ပါတယ်။ ဒီ ဖြစ်စဉ်ကို Client Reservation လို့ခေါ်ပါတယ်။

Dynamic Assignment

၎င်းကို ဘယ်အခါမှာတွေ့ရသလဲဆိုတော့ DHCP Server ကနေ Device ဆီကို TCP/IP Address ယာယီယူသုံးတာကိုပြောတာဖြစ်ပါတယ်။ ဒီနည်းကိုသုံးမယ်ဆိုရင်တော့ ကျွန်တော်တို့က ပစ္စည်းမှာယာယီယူသုံးထားတဲ့ Address အတိုင်းအတာတစ်ခုကို TCP/IP Address အဖြစ်သတ်မှတ်ပေးရမှာဖြစ်ပါတယ်။ ၎င်းကို Pool of Address လို့ခေါ်ပါတယ်။ ပစ္စည်းဟာ TCP/IP Address ဟာ Expires ဖြစ်သွားပါတယ်။ အဲဒီ Expire ဖြစ်သွားတဲ့ TCP/IP Address ဟာနောက်ပစ္စည်းတစ်ခုက Address ကိုတောင်းဆိုလာတဲ့

အခါသတ်မှတ်ဖို့ဖြစ်သွားပါတော့တယ်။ ဒီလိုလုပ်ခြင်းဟာ အသုံးပြုသူ Users တွေ TCP/IP Address ပို့ယူခြင်းမှလည်းကာကွယ်ပေးပါတယ်။ DACP Servers ဟာ Automatic Mode နှင့်လည်းအလုပ်လုပ်နိုင်ပါတယ်။ ၎င်း Automatic Mode နှင့်ဆိုရင် Hosts က Power up ဖြစ်တာနှင့် Address တွေကိုသတ်မှတ်ပေးနိုင်ပါတယ်။ အဲဒီအခါ Address ကို Client Computer ဆီသို့ယာယီ(ငှားရမ်း)ပေးသုံးပါတယ်။ အချိန်အတိုင်းအတာတစ်ခုပေါ့။

၃.၂၉ Domain Name System (DNS)

ရှေ့တွင်ဖော်ပြပြီး။

၃.၂၄ Windows Internet Naming Service (WINS)

WINS ဆိုတဲ့ Windows Internet Naming Service ဟာ Microsoft Networking Topology အတွက်မရှိမဖြစ်ဖြစ်ပါတယ်။ ပထမဦးဆုံး WINS အကြောင်းကိုမပြောခင်မှာ NetBIOS နဲ့ NetBEUI ကိုအရင်လေ့လာကြည့်ရအောင်။

NetBIOS ဆိုတာ Network Basic Input Output System ပါ။ ၁၉၈၃ ခုနှစ်မှာ IBM နဲ့ Sytek ကဒီဇိုင်းလုပ်ခဲ့တဲ့ Application Program Interface ပါ။

NetBEUI ဆိုတာ NetBIOS Extended User Interface ဖြစ်ပါတယ်။ ဒါဟာ IBM ရဲ့ NetBIOS ကို Extention လုပ်ထားတဲ့ Microsoft ရဲ့ Transport Protocol ပါ။

ဟုတ်ပါပြီ။ ဒီဆို WINS ဆိုတာဘာလဲ ဆက်လေ့လာကြည့်ရအောင်။ WINS ဆိုတာ ခုနကပြောခဲ့တဲ့ DNS လိုပါပဲ။ IP Address တွေကိုမှတ်ထားမယ့်အစား Host Name နဲ့ Domain Name ပါဝင်တဲ့နာမည်တွေကိုမှတ်ထားမယ်။ နာမည်နဲ့လိပ်စာအကြား အပြန်အလှန်ပြောင်းပို့ဆိုတာ DNS လိုမယ်။ အခုလည်းဒီလိုပဲ။ ကွန်ရက်ထဲမှာ Network Resources တွေရှိမယ်။ ဥပမာ Print Server ဒါမှမဟုတ် Printer ပေါ့။ ဒီတော့ Network Resources တွေကိုလှမ်းပြီး Access လုပ်ခဲ့အခါ ကွန်ရက်ဟာ TCP/IP ကို အသုံးပြုနေတယ်ဆိုတာ မမေ့ပါနဲ့အုံး။ ဘာလို့လဲဆိတော့ TCP/IP ဟာ Address ကိုပဲသိပြီး Resources Name တွေကိုမသိလို့ပါ။ သင်ဟာ ကွန်ရက်ထဲက Print Server တစ်ခုလှမ်း Access လုပ်တယ်။ Print Server တွေအများကြီးရှိချင်ရှိမယ်။ တစ်ခုတည်းပဲရှိချင်လည်း ရှိမယ်။ ဘာပဲဖြစ်ဖြစ် သင်ဟာ List ထဲက သင်သွားချင်တဲ့ Print Server ရဲ့နာမည်ကိုရွေးရမယ်။ အဲ့ဒီမှာ ပြဿနာ TCP/IP ဟာ Address ကိုပဲသိပြီး NetBIOS Name တွေကိုမသိပါ။ ဒီမှာ WINS ဆိုတာ လိုအပ်လာတော့တာပါပဲ။

ဒီတော့ သင်ဟာသိထားရမှာက TCP/IP ကိုအသုံးပြုထားတဲ့ Windows NT Network မှာ Resources တွေကို Access လုပ်တိုင်း လုပ်တိုင်းမှာ၊ သင့်ရဲ့ System ဟာ Host Name ဒါမှမဟုတ် IP

Address ကိုသိဖို့လိုအပ်တယ်ဆိုတာပါပဲ။ အကယ်၍ WINS သာရှိနေမယ်ဆိုရင်တော့ WINS ဟာ Name ကနေ Address ကို Cross Reference လုပ်ပေးတာကြောင့် Resources တွေက အသုံးပြုထားတဲ့ NetBIOS တွေနဲ့ ရှေ့ကိုဆက်သွားလို့ရပြီပေါ့။

ခ. ၂၅ Host Files

DNS နှင့် WINS ကို အခြေခံတဲ့ Name Resolution စနစ်တွေပဲဖြစ်ပါတယ်။ အကယ်၍များ ကျွန်တော်တို့ရဲ့ Network ဟာသေးငယ်တာကြောင့် DNS Server အသုံးမပြုခဲ့ဘူးဆိုရင် ကျွန်တော်တို့ဟာ Host Files ဆိုတာကို အသုံးပြုလို့ရပါတယ်။ Host File ဆိုတာ Host Name နှင့်အတူ IP Address တွေ ပါရှိတဲ့ Text File လေးကိုခေါ်တာဖြစ်ပါတယ်။ Unix Computer ဟာ Host Name ကိုအသုံးပြုပြီး Microsoft Computer က NetBIOS Computer Name ကိုအသုံးပြုပါတယ်။ အများဆုံးသုံးဖြစ်တဲ့ Host Files နှစ်ခုကတော့ Hosts နှင့် Lmhosts တို့ပဲဖြစ်ကြပါတယ်။

Host File

ဒင်း Hosts ဖိုင်ဟာ ဖိုင်နာမည်အားဖြင့် hosts အိမ့မဟုတ် hosts.txt ဆိုပြီးရှိပါတယ်။ ဒင်း File ဟာ DNS လိုပါပဲ။ Host Names နှင့် သူတို့ရဲ့ TCP/IP Address တွေ List အလိုက်ရှိပါတယ်။ TCP/IP Stack ဟာ DNS Server ဆီမှာ (DNS မှ မရှိဘဲ) DNS ကိုသွားပြီးတောင်းဆိုမယ့်အစား Station ရဲ့ Address ကို အဲ့ဒီဖိုင်မှာ ရှာဖွေတာဖြစ်ပါတယ်။

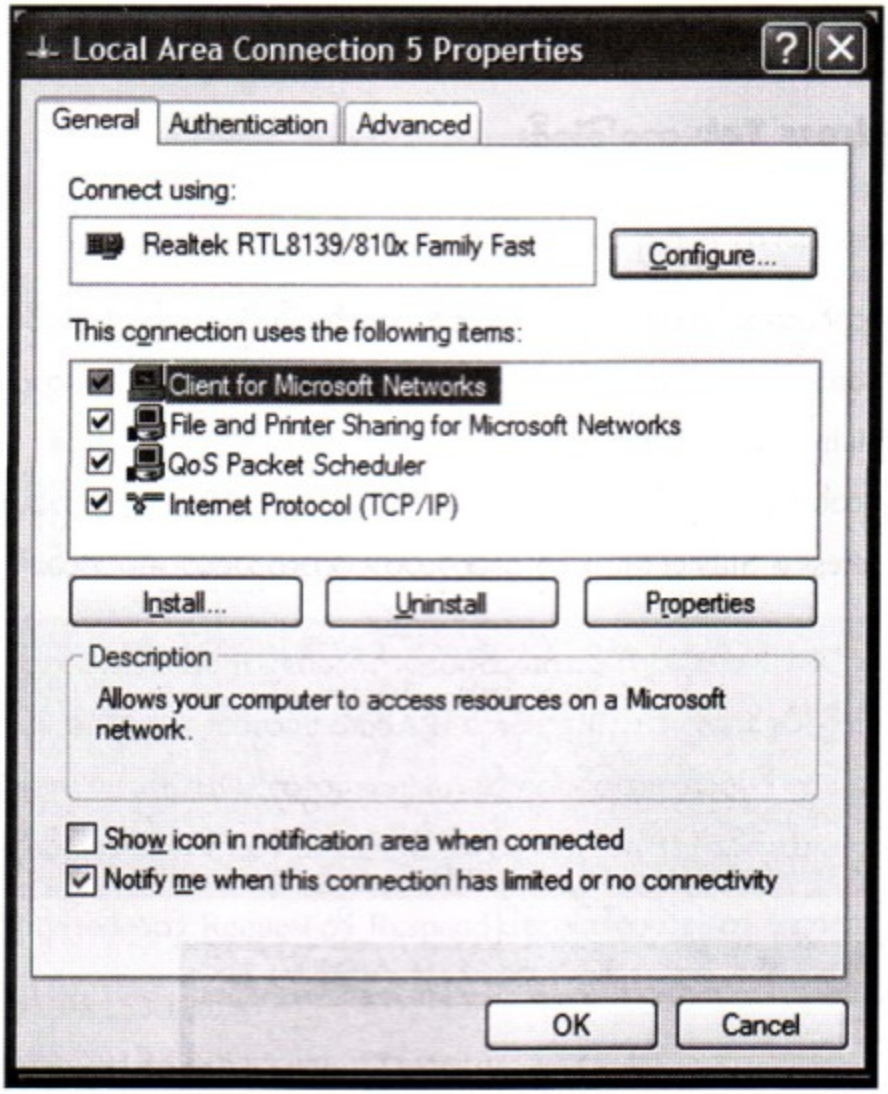
Lmhosts File

ဒင်းဖိုင်ကတော့ WINS လိုပါပဲ။ ဒင်းမှာ NetBIOS Computer Names နှင့် သူတို့ရဲ့ TCP/IP Address တွေ List အလိုက်ရှိပါတယ်။ ဒင်းဖိုင်အတွင်းက အကြောင်းအရာတွေဟာ TCP/IP ကွန်ရက်ပေါ်ကနေ Computer NetBIOS Name ကို Access လုပ်ပေးနိုင်ခွင့်ရှိပါတယ်။

ခ. ၂၆ TCP/IP ကို Windows XP Station များတွင်အသုံးပြုဖို့ပြင်ဆင်ခြင်း

Protocol ကိုတင်ခြင်းနှင့်ဖြုတ်ခြင်းအတွက် My Network Places ၏ Properties ကိုခေါ်ရပါမည်။ ပြီးနောက် ပေါ်လာသည့် Box တွင် Local Area Connection ကိုဖွင့်ရပါမည်။ ထိုအခါ အောက်ပါ Box ပေါ်လာပါမည်။ ဒင်း Box ကနေ Protocol တင်ခြင်းနှင့်ဖြုတ်ခြင်းများပြုလုပ်နိုင်ပါသည်။

ပုံ ၇.၄



အဲ့ဒီမှာ TCP/IP ကို Install လုပ်ပြီးတာကိုတွေ့ရပါလိမ့်မယ်။

ပထမဦးဆုံးအဆင့်ထဲကိုက TCP/IP ဟာ တင်ထားပြီးသားဖြစ်နေရင်တော့ အထက်ပါအဆင့်ကို လုပ်စရာမလိုတော့ပါဘူး။

ကဲ အဲ့ဒီမှာ တင်ထားပြီးသား TCP/IP ကိုရွေးပါ။ ပြီးတော့ Properties ကိုရွေးပါ။ ဒီအခါ TCP/IP ရဲ့ Properties တွေပေါ်လာပါလိမ့်မယ်။ အဲ့ဒီမှာ ဘာတွေပါဝင်သလဲ။

- ❖ IP Address
- ❖ Bindings
- ❖ Gateway
- ❖ Advanced
- ❖ WINS Configuration
- ❖ DNS Configuration
- ❖ NetBIOS (If used) တို့ပါဝင်ပါတယ်။

တစ်ခုချင်းစီဟာ Windows မှာ TCP/IP အသုံးပြုဖို့သက်ဆိုင်ရာ Setting တွေရှိကြပါတယ်။

၃.၂၃ IP Address Tab အကြောင်း

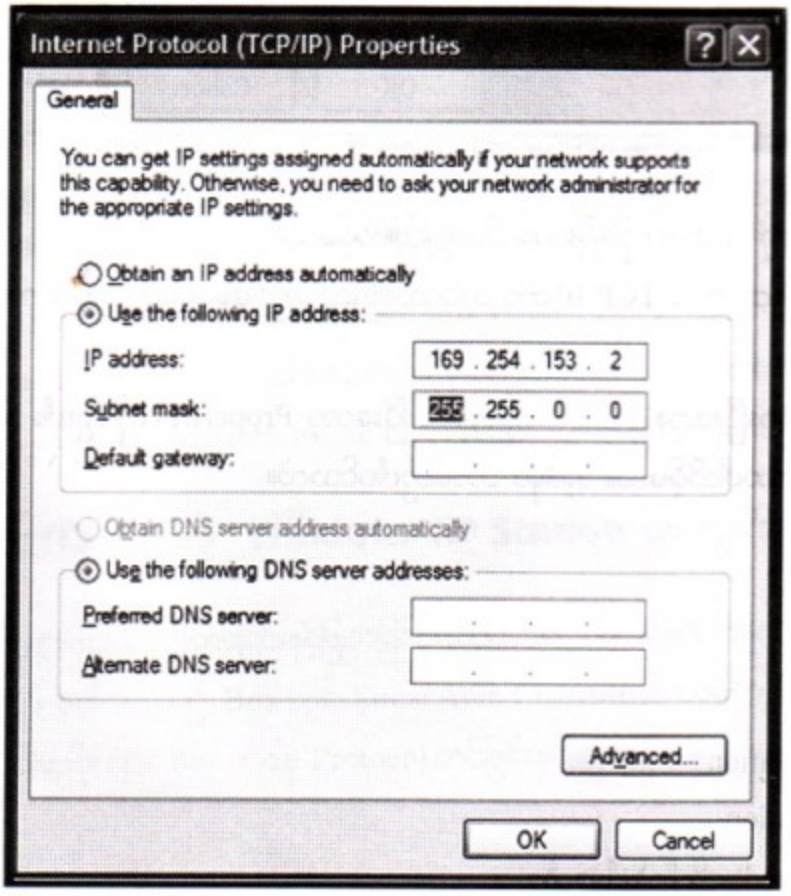
IP Address Tab ကို ပုံ ၇.၅ မှာတွေ့မြင်ရပါလိမ့်မယ်။

အကယ်၍သင်ဟာ အင်တာနက်ကို တိုက်ရိုက်ချိတ်ဆက်မယ်ဆိုရင် သင့်ရဲ့ ISP ဆီက Dynamic Host Configuration Protocol (DHCP) Server ကနေ Address ကိုလှမ်းယူလို့ရပါတယ်။ အဲ့ဒါဆိုရင်တော့ သင်ဟာ Obtain an IP address Automatically ဆိုတာကိုရွေးရမှာဖြစ်ပါတယ်။

အကယ်၍သင်ဟာ Specify an IP Address ကိုရွေးမယ်ဆိုရင်တော့ သင့်ကွန်ပျူတာအတွက် လိုအပ်မယ့် IP Address နဲ့ Subnet Mask ကို သင်ကိုယ်တိုင်ရိုက်ထည့်ရမှာဖြစ်ပါတယ်။

မှတ်ချက်။ ။ DHCP ကိုသုံးရတဲ့ ဦးဆုံးရည်ရွယ်ချက်ကတော့ IP Address တွေကို Centralize Manament လုပ်ချင်လို့ပါပဲ။ ဒီတော့ DHCP ကိုသုံးရင် IP Address တွေဟာ Client တွေရဲ့ အခြေခံလိုအပ်ချက်အတိုင်း အလိုအလျောက်ဝေငှသွားမှာဖြစ်ပါတယ်။ Address တွေဟာ DHCP မှာ Centralize လုပ်ထားခြင်းဖြင့် သင်ဟာ ကွန်ရက်မှာရှိတဲ့ IP Address တွေကို Single Server ကနေ ထိန်းချုပ်လို့ရနေပါတယ်။

ပုံ ၇.၅



၃. ၂၈ TCP/IP Utility များ

Ping Utility အကြောင်း

Ping Utility ဟာ TCP/IP Utility ထဲမှာ အခြေခံအကျဆုံး Utility ဖြစ်ပါတယ်။ Ping ဟာ Command Line Utility ဖြစ်ပါတယ်။ Ping ကိုသုံးရခြင်းအဓိကအားဖြင့် ရည်ရွယ်ချက်နှစ်မျိုးရှိပါတယ်။ အဲ့ဒါတွေကတော့ -

- To find out if you can reach a host
- To find out if a host is responding တို့ဖြစ်ကြပါတယ်။

သူ့ကိုအသုံးပြုရမယ့်ပုံစံ (Synatx) ကတော့ -

ping < hostname or IP Address> ဖြစ်ပါတယ်။

သင်ဟာမည်သည့် IP Address ကိုမဆို Ping ရိုက်လိုက်ရင် သင်ရိုက်လိုက်တဲ့ Address ပိုင်ရှင် Host မှ TCP/IP Stack ထဲကအပိုင်းတစ်ပိုင်းဖြစ်သော ICMP (Internet Control Message Protocol) က ခုနက သင်ရိုက်လိုက်တဲ့ Request ကို Respond ပြန်လုပ်ပါတယ်။ ကဲ အောက်ပါအတိုင်းပါပဲ။

```
Ping 204.153.163.2
Pinging 204.153.163.2 with 32 bytes of data:
Reply from 204.153.163.2: bytes=32 time<10ms TTL=128
Reply from 204.153.163.2: bytes=32 time<10ms TTL=128
Reply from 204.153.163.2: bytes=32 time<10ms TTL=128
Reply from 204.153.163.2: bytes=32 time<10ms TTL=128
```

ကဲ ဒီတော့ သင်ဟာ ရည်ရွယ်ရာဖြစ်တဲ့ Address ကိုရိုက်လိုက်တဲ့အခါ ၎င်းက Basic Request ကိုပြန် Respond လုပ်တယ်မဟုတ်လား။ ပြန်လုပ်တယ်ဆိုကတည်းက Host ကိုရှာတွေ့လို့ပေါ့။ အဲဒါဟာ Ping ကိုအသုံးပြုရတဲ့ ရည်ရွယ်ချက် ခုနကဖော်ပြခဲ့တဲ့အတိုင်း Host ကိုရှာလို့တွေ့တယ်။ Host ကနေမှ Request ကို Respond ပြန်လုပ်ပါတယ်ဆိုတဲ့ ရည်ရွယ်ချက်နဲ့လည်းညီညွတ်သွားပါတယ်။

TCP/IP ကိုအသုံးပြုထားတဲ့ Workstation တွေမှာကွန်ရက်ဆင်ပြီးသွားတဲ့အခါ အထက်ပါနည်းအတိုင်း Connection မိမမိကိုလည်း စမ်းစစ်လို့ရပါတယ်။ ပုံ ၇.၆ မှာ TCP/IP Switch တွေကိုဖော်ပြပေးထားပါတယ်။

ပုံ ၇.၆

```
C:\>ping

Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] target_name

Options:
    -t              Ping the specified host until stopped.
                    To see statistics and continue - type Control-Break;
                    To stop - type Control-C.
    -a              Resolve addresses to hostnames.
    -n count        Number of echo requests to send.
    -l size         Send buffer size.
    -f              Set Don't Fragment flag in packet.
    -i TTL          Time To Live.
    -v TOS          Type Of Service.
    -r count        Record route for count hops.
    -s count        Timestamp for count hops.
    -j host-list    Loose source route along host-list.
    -k host-list    Strict source route along host-list.
    -w timeout      Timeout in milliseconds to wait for each reply.
```

ARP Utility အကြောင်း

ARP (Address Resolution Protocol) တာ OSI Model ရဲ့ Network Layer မှာရှိတာဖြစ်ပါတယ်။ အခုပြောမယ့် ARP Utility တာ ARP Table ကိုကြည့်ဖို့အတွက်သုံးတာဖြစ်ပါတယ်။ ၎င်းတာ TCP/IP Name-Resolution နှင့်ပတ်သက်တဲ့ Information တွေပါတဲ့ File ပဲဖြစ်ပါတယ်။ အောက်မှာ ARP Command ကို Swithc -a နှင့်တွဲသုံးပုံကိုဖော်ပြပေးထားပါတယ်။

ပုံ ၇.၇

```
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]

  -a               Displays current ARP entries by interrogating the current
                   protocol data.  If inet_addr is specified, the IP and Physical
                   addresses for only the specified computer are displayed.  If
                   more than one network interface uses ARP, entries for each ARP
                   table are displayed.
  -g               Same as -a.
  inet_addr        Specifies an internet address.
  -N if_addr       Displays the ARP entries for the network interface specified
                   by if_addr.
  -d               Deletes the host specified by inet_addr. inet_addr may be
                   wildcarded with * to delete all hosts.
  -s               Adds the host and associates the Internet address inet_addr
                   with the Physical address eth_addr.  The Physical address is
                   given as 6 hexadecimal bytes separated by hyphens. The entry
                   is permanent.
  eth_addr         Specifies a physical address.
  if_addr          If present, this specifies the Internet address of the
                   interface whose address translation table should be modified.
                   If not present, the first applicable interface will be used.
```

ARP တာ TCP/IP Address ကို MAC Address အဖြစ် Map လုပ်ပေးနိုင်ပါတယ်။ ရှေ့မှာလည်းပြောခဲ့ဖူးပါတယ်။ Data Link Layer မှာ MAC Layer ဆိုတာရှိပါတယ်။ ၎င်းတာ TCP/IP (Logical) မှ Physical Address ကို Map လုပ်တဲ့ Table ကိုထိန်းချုပ်ပါတယ်။ အကယ်၍များ TCP/IP Address တာလိုအပ်တဲ့အချိန် Table မှာသူမရှိခဲ့ရင် ARP တာရှာဖွေရေး Packet တစ်ခုပြုလုပ်ပြီးရှာဖွေစေပါတယ်။

အကြောင့် ARP Utility ဟာ TCP/IP ကနေ Physical Address ကိုကြည့်ချင်တဲ့အခါမှာဖြစ်စေ၊ ပြုပြင်ချင်တဲ့ အခါမှာဖြစ်စေအင်မတန်အသုံးတည့်ပါတယ်။ ARP Utility ဟာအခြားသော Command Line Utilities တွေလိုပါပဲ။ Utility နှင့်တွဲဖက်အသုံးပြုမယ့် Switch တွေရှိပါတယ်။ ပုံ ဂ.ဂ မှာဖော်ပြပေးထားပါတယ်။

NBTSTAT အကြောင်း

NBTSTAT (NetBIOS - TCP/IP Statistics) Utility ကို Administrator တွေဟာ NBI (NetBIOS over TCP/IP) လို့ခေါ်တဲ့ TCP/IP Connections ကိုအသုံးပြုထားသော NetBIOS (Computer Name) ရဲ့အချက်အလက်တွေကိုကြည့်တဲ့အခါမှာသုံးပါတယ်။ ဒီ Utility ဟာ WINS Name-Resolution ရဲ့ Error တွေကို Troubleshoot လုပ်တဲ့အခါမှာအသုံးပြုပါတယ်။

ပုံ ဂ.၈

```
Displays protocol statistics and current TCP/IP connections using NBI
(NetBIOS over TCP/IP).

NBTSTAT [ [-a RemoteName] [-A IP address] [-c] [-n]
        [-r] [-R] [-RR] [-s] [-S] [interval] ]

  -a   (adapter status) Lists the remote machine's name table given its name
  -A   (Adapter status) Lists the remote machine's name table given its
                        IP address.
  -c   (cache)          Lists NBT's cache of remote [machine] names and their IP
 addresses
  -n   (names)          Lists local NetBIOS names.
  -r   (resolved)       Lists names resolved by broadcast and via WINS
  -R   (Reload)         Purges and reloads the remote cache name table
  -S   (Sessions)       Lists sessions table with the destination IP addresses
  -s   (sessions)       Lists sessions table converting destination IP
                        addresses to computer NETBIOS names.
  -RR  (ReleaseRefresh) Sends Name Release packets to WINS and then, starts Refr
esh

  RemoteName    Remote host machine name.
  IP address    Dotted decimal representation of the IP address.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display. Press Ctrl+C to stop redisplaying
                statistics.
```

NETSTAT အကြောင်း

NETSTAT Utility ကလက်ရှိချိတ်ဆက်ထားတဲ့ TCP/IP Network Connections တွေအားလုံးကိုပြပေးတာဖြစ်ပါတယ်။ အဲ့ဒီအပြင် ၎င်းဟာ လက်ရှိချိတ်ဆက်ထားမှု Connections တွေရဲ့ Ports နှင့် Statistics ကိုပါပြပေးပါတယ်။ NETSTAT ရဲ့ Switch တွေကိုသုံးပြီး Router Table ကိုလည်းကြည့်နိုင်ပါတယ်။ ပုံ ဂ.၉ ကိုကြည့်ပါ။

FTP အကြောင်း

FTP ဆိုတဲ့ File Transfer Protocol ဟာ TCP Transport Protocol ကိုအသုံးပြုပြီး Files တွေ

ပုံ ၇.၉

```
Displays protocol statistics and current TCP/IP network connections.

NETSTAT [-a] [-b] [-e] [-n] [-o] [-p proto] [-r] [-s] [-v] [interval]

  -a            Displays all connections and listening ports.
  -b            Displays the executable involved in creating each connection or
                listening port. In some cases well-known executables host
                multiple independent components, and in these cases the
                sequence of components involved in creating the connection
                or listening port is displayed. In this case the executable
                name is in [] at the bottom, on top is the component it called,
                and so forth until TCP/IP was reached. Note that this option
                can be time-consuming and will fail unless you have sufficient
                permissions.
  -e            Displays Ethernet statistics. This may be combined with the -s
                option.
  -n            Displays addresses and port numbers in numerical form.
  -o            Displays the owning process ID associated with each connection.
  -p proto      Shows connections for the protocol specified by proto; proto
                may be any of: TCP, UDP, TCPv6, or UDPv6.  If used with the -s
                option to display per-protocol statistics, proto may be any of:
                IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, or UDPv6.
  -r            Displays the routing table.
  -s            Displays per-protocol statistics.  By default, statistics are
                shown for IP, IPv6, ICMP, ICMPv6, TCP, TCPv6, UDP, and UDPv6;
                the -p option may be used to specify a subset of the default.
  -v            When used in conjunction with -b, will display sequence of
                components involved in creating the connection or listening
                port for all executables.
  interval      Redisplays selected statistics, pausing interval seconds
                between each display.  Press CTRL+C to stop redisplaying
                statistics.  If omitted, netstat will print the current
                configuration information once.
```

ရွှေ့ပြောင်းခြင်းနှင့်ကော်ပီကူးခြင်းတွေမှာအသုံးပြုပါတယ်။ ၎င်း FTP Protocol ဟာအဓိကအားဖြင့် TCP/IP Environment တွေမှာ Workstation တွေဆီ Files တွေကို Transfer လုပ်ရာမှာအသုံးပြုတာဖြစ်ပါတယ်။ ဒီ Protocol ဟာ OSI Model ရဲ့ထိပ်ဆုံးအလွှာသုံးခုဖြစ်ကြတဲ့ Session, Presentation နှင့် Application အလွှာတွေမှာအလုပ်လုပ်တာဖြစ်ပါတယ်။ FTP Utility နှင့် Protocol ဟာအလွှာတစ်ခုချင်းဆီမှာ မတူညီတဲ့ လုပ်ဆောင်ချက်တွေရှိကြပါတယ်။

၁။ OSI Model ရဲ့ Session အလွှာမှာဆိုရင်တော့ - FTP Protocol ဟာ Connection များကိုပြုလုပ်ခြင်း၊ ဖြုတ်ချခြင်းနှင့် Files များကို Transfer လုပ်ခြင်းတွေမှာ Support လုပ်ပါတယ်။

၂။ OSI Model ရဲ့ Presentation အလွှာမှာဆိုရင်တော့ - FTP Protocol ဟာဘာသာပြန်ခြင်း၊ Translation ကိစ္စတွေကိုထိန်းချုပ်ပေးပါတယ်။ ဒါကြောင့် FTP ဟာ Hosts တွေအကြား Files တွေကို Transfer လုပ်နိုင်လာတာဖြစ်ပါတယ်။

၃။ OSI Model ရဲ့ Application အလွှာမှာဆိုရင်တော့ - FTP Protocol ဟာပူးပေါင်းခြင်း၊ Collaborative Service, File အဖြစ်ပြုလုပ်ခြင်း စတဲ့ Network Services တွေကို ပံ့ပိုးပေးပါတယ်။

Tracert အစောကြောင်း

Trace Route လို့ခေါ်တဲ့ ဒီ Tracert Utility ဟာ Packets တွေရည်ရွယ်ရာကိုသွားနေစဉ်မှာပင်

လမ်းကြောင်းတွေကိုခြေရာကောက်ပေးပါတယ်။

ပုံ ၇.၁၀

```
C:\>tracert

Usage: tracert [-d] [-h maximum_hops] [-j host-list] [-w timeout] target_name

Options:
    -d                  Do not resolve addresses to hostnames.
    -h maximum_hops     Maximum number of hops to search for target.
    -j host-list        Loose source route along host-list.
    -w timeout          Wait timeout milliseconds for each reply.
```

Telnet အခြေခံများ

Telnet Utility ဟာ Terminal Emulation တွေက အသုံးပြုတဲ့ Remote Application တွေကို Access လုပ်နိုင်ပါတယ်။ ၎င်းဟာ ဒီ Terminal တွေကိုချိတ်ဆက်ထားတဲ့သက်ဆိုင်ရာ Ports တွေကိုလည်း Diagnose လုပ်နိုင်ပါတယ်။ သူဟာ FTP Protocol လိုပါပဲ။ Telnet Protocol ဟာ OSI Model ရဲ့အပေါ် သုံးလွှာဖြစ်တဲ့ Session, Presentation နှင့် Application အလွှာတွေမှာအလုပ်လုပ်ပါတယ်။ တစ်လွှာချင်းစီမှာ Telnet Protocol နှင့် Utility တာလုပ်ဆောင်ချက်တွေမတူညီကြပါဘူး။

၁။ Telnet ဟာ OSI Model ရဲ့ Session Layer မှာဆိုရင် - Dialogue တွေထိန်းချုပ်ခြင်း။ Connection များဖန်တီးခြင်း၊ ဖြုတ်ချခြင်း၊ ဒိုင်များ Transfer လုပ်ခြင်းတို့ကို ပံ့ပိုးပေးပါတယ်။

၂။ OSI Model ရဲ့ Presentation Layer မှာဆိုရင်တော့ - Byte Order နှင့် Characters Codes တွေကိုအသုံးပြုပြီး ဘာသာပြန်ခြင်းကိုစီမံအုပ်ချုပ်ပါတယ်။

၃။ OSI Model ရဲ့ Application Layer မှာဆိုရင်တော့ - Remote Operations တွေအတွက် Functions တွေကိုပံ့ပိုးပေးပါတယ်။

Ipconfig အခြေခံများ

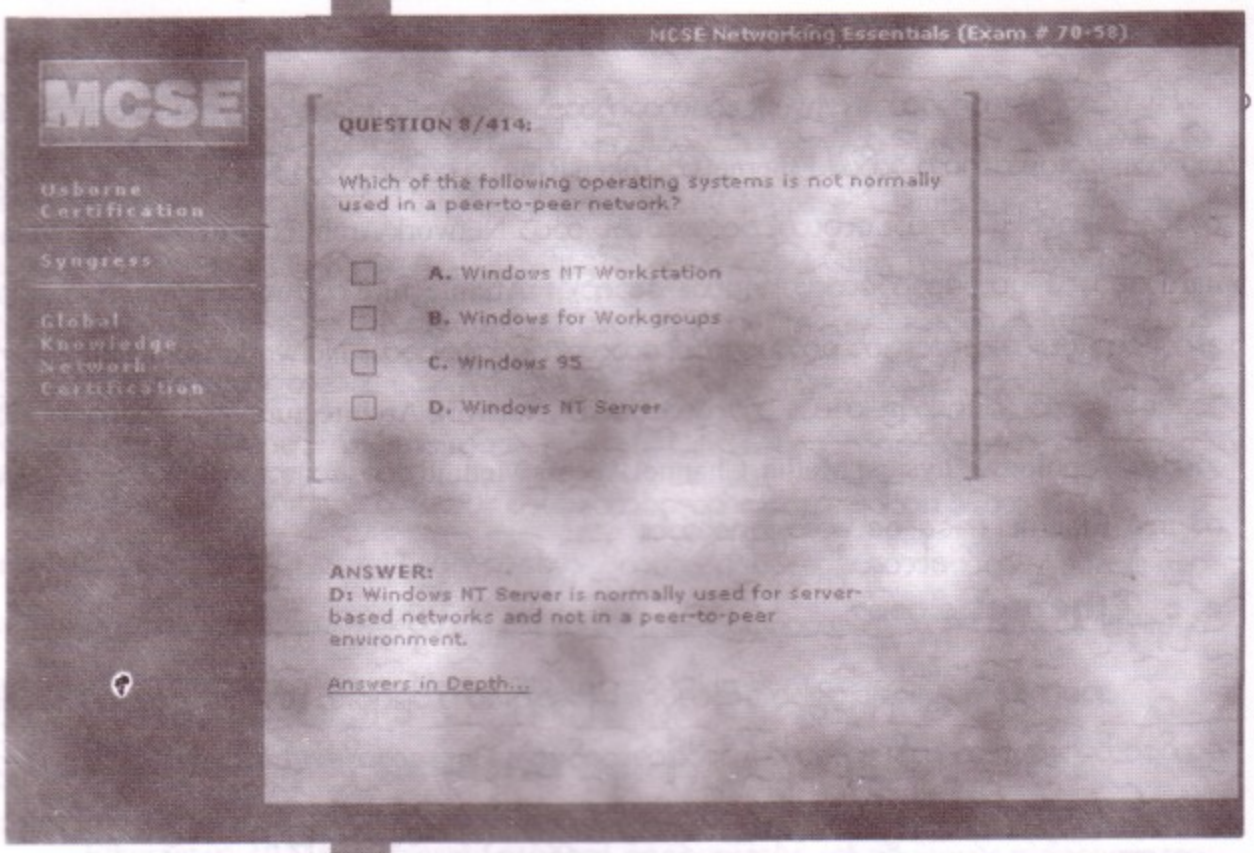
ဒီ Utility ကတော့ Windows NT အတွင်းမှာသုံးရတဲ့ Utility ပဲဖြစ်ပါတယ်။ သူကတော့ Command Line Utility ဖြစ်ပါတယ်။ ဒီတော့ အောက်ပါအတိုင်းလုပ်ကြည့်ရအောင်။

Command Prompt ကနေ ipconfig လို့ရိုက်လိုက်ရင်တစ်ဖက်ပါပုံစံကိုတွေ့ရပါလိမ့်မယ်။

```
C:\>ipconfig
Windows NT IP Configuration
Ethernet adapter E100B1
        IP Address . . . . . .:204.153.163.2
        Subnet Mask. . . . . .:204.153.163.2
        Default Gateway. . . . . .:
```

အောက်မှာ ipconfig ရဲ့ Switch တွေကိုဖော်ပြပေးထားပါတယ်။

Switch	Description
/?	ipconfig နဲ့တွဲပြီးအသုံးပြုလို့ရတဲ့ Switch တွေရဲ့ List ကိုဖော်ပြတာပါ။
/all	TCP/IP Information တွေအားလုံးကိုပြပါတယ်။
/Release	DHCP ကရသမျှ TCP/IP Information တွေကို Release လုပ်ပါတယ်။
/Renew	DHCP ကရသမျှ TCP/IP Information တွေကို Release နှင့် Renew လုပ်ပါတယ်။



UNIT 8

Network Architectures

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက် တစ်ခုလုံးနှင့်ပတ်သက်နေသော နည်းပညာတွေကိုလေ့လာကြမှာ ဖြစ်ပါတယ်။ နည်းနည်းရှုပ်ထွေးလာတဲ့ သဘောလေးတွေတော့ ရှိပါတယ်။

ဒီသင်ခန်းစာကတော့ Network နှင့်ပတ်သက်သည့်နည်းပညာများကို အဓိကထားလေ့လာကြမှာဖြစ်ပါတယ်။ နည်းပညာဆိုတာ ဒီလိုပါ။ Ethernet တို့ Token Ring တို့ စတဲ့မတူညီတဲ့ Network နည်းပညာတွေကိုလေ့လာကြမှာဖြစ်ပါတယ်။ လေ့လာကြတဲ့အထဲမှာမှ ဘယ် Network Architecture ကတော့ဖြင့် Standard ဖြစ်သလဲ စတာတွေကိုလေ့လာကြမယ်။ နောက်ပြီး Architecture တစ်ခုချင်းစီရဲ့ ကန့်သတ်ချက်၊ အကျိုးကျေးဇူးနှင့်အားနည်းချက် စတာတွေကိုပါ လေ့လာကြမှာဖြစ်ပါတယ်။ Network Architecture ဆိုတဲ့ ဒီသင်ခန်းစာဟာ အရေးကြီးပါတယ်။ ဘာလို့လဲဆိုတော့ Network Architecture လို့ပြောလိုက်ရင် အဲ့ဒီအထဲမှာ Topology, Physical Media, Channel Access Method စတာတွေအားလုံး ပါဝင်သွားလို့ပါပဲ။ ကဲ အခု Ethernet ကနေ စလေ့လာကြရအောင်။

၈.၁ Ethernet ၏အစ

အစကနေ စပြောရရင် ၁၉၆၀ နောက်ပိုင်း၊ နောက်ပြီးတော့ ၁၉၇၀ အစောပိုင်းတွေမှာ အဖွဲ့အစည်းတော်တော်များများဟာ ကွန်ပျူတာကိုဘယ်လိုချိတ်ဆက်မလဲ။ Data တွေကိုအချင်းချင်း ဘယ်လိုဖလှယ်ကြမလဲ။ ဒါတွေအတွက် နည်းလမ်းတွေရှာခဲ့ကြတယ်ပေါ့ဗျာ။ အဲ့ဒီလို ရှာဖွေကြတဲ့နည်းလမ်းတွေထဲက Project တစ်ခုဖြစ်တဲ့ Hawaii တက္ကသိုလ်က ALOHA Project ပဲဖြစ်ပါတယ်။ အဲ့ဒီကနေမှတဆင့် Robert Metcalf နှင့် David Boggs ဆိုသူတို့က Xerox ၏ Palo Alto Research Centre (PARC) မှာ ၁၉၇၂ ခုနှစ်မှာ ကနဦး Ethernet Version ကိုထုတ်ခဲ့ကြပါတယ်။ နောက်ပြီး ၁၉၇၅ မှာ PARC ဟာ ပထမဦးဆုံးသော ဈေးကွက်ဝင် Ethernet ကိုထုတ်ခဲ့ကြပါတယ်။ ၎င်း Version ဟာ ကွန်ပျူတာအလုံး ၁၀၀ ကိုချိတ်ဆက်ထားတဲ့ စုစုပေါင်း Cable (၁) ကီလိုမီတာအတွင်း Data တွေကို 3 Mbps လောက်အထိ Transmit လုပ်နိုင်ပါတယ်။ အဲ့သလိုခဲ့ပေါ့ဗျာ Xerox က Intel Corporation နှင့် Digital Equipment Corporation တို့နှင့်ပူးပေါင်းပြီး DIX ဆိုကာ Xerox ရဲ့ Ethernet အပေါ်အခြေခံပြီး 3 Mbps ကနေ 10 Mbps အထိတိုးမြှင့် Transmit လုပ်နိုင်ခဲ့ကြပါတယ်။ ၁၉၉၀ နှစ်ထဲမှာတော့ ၎င်း Version ကို IEEE အဖွဲ့ဟာ သူ့ရဲ့ 802.3 Specification တွေပေါ်အခြေခံပြီး OSI Model ရဲ့ Physical အလွှာနှင့် Data Link အလွှာတွေမှာ Ethernet Network ဘယ်လိုအလုပ်လုပ်ရမယ်ဆိုတာကိုသတ်မှတ်ခဲ့ပါတယ်။

၈.၂ Ethernet အခြေခံများ

ကနေ့ခေတ်မှာတော့ Ethernet ဟာ ရေပန်းအစားဆုံးသော Network Architecture တစ်ခုဖြစ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ သူမှာကောင်းကျိုးတွေအများကြီးရှိတယ်ဗျ။ အဲ့ဒီအထဲမှာ လွယ်ကူစွာ Install လုပ်နိုင်ခြင်းနှင့် ကုန်ကျစရိတ်သက်သာခြင်းတို့ပါဝင်ပါတယ်။ ပြောရမယ်ဆိုရင် တစ်ခြား Network Architecture တွေထက်စာရင် Install လုပ်ရတာရော၊ အသုံးပြုရတာရောလွယ်ကူတဲ့အပြင် ကုန်ကျစရိတ်ကအစသက်သာပါတယ်။ Ethernet ရေပန်းစားရခြင်းနောက်တစ်ချက်က ဒီ Network Media ပေါ့။ ကြားခံပစ္စည်း

ကွန်ပျူတာတစ်လုံးနှင့်တစ်လုံးကြား ချိတ်ဆက်ပေးတဲ့ ကြားခံပစ္စည်းအမျိုးမျိုးကို Support လုပ်ပေးနိုင်တယ်။ Ethernet Version အများစုဟာ 10 Mbps အဆမတုတ် 100 Mbps နှင့် Transmit လုပ်ကြပါတယ်။ အခုနောက်ပိုင်း Ethernet တွေကတော့ 1000 Mbps တန်ဖိုးအားဖြင့် 1 Gbps Transmit လုပ်နိုင်ပါတယ်။ အားလုံးသော Ethernet တွေဟာ Network Card မှာပါလာတဲ့ Hardware ပိုင်းဆိုင်ရာ Address တွေကို Data Packet လေးတွေပို့တဲ့အခါ ၎င်း Address ကို Packet အတွင်းထည့်သွင်း အသုံးပြုပါတယ်။ ဒီ Network Card မှာပါလာတဲ့ Address ဆိုတာ Network Card ကိုထုတ်လုပ်ကတည်းက Room ထဲမှာ တခါတည်း Burned လုပ်ပြီးထည့်ထားတာပါ။ တစ်ခုနှင့်တစ်ခုလည်းမတူညီကြပါဘူး။ ဒီတော့ Data ပို့တဲ့အခါ Packet လေးတွေထုပ်ပိုးပြီး Send လုပ်လိုက်တော့ ပို့လွှတ်လိုက်တဲ့ ကွန်ပျူတာဖက်က Address ရော လက်ခံမယ့်ဖက်က Address ရော ပို့လိုက်တဲ့ Packet ရဲ့ Header ပိုင်းမှာထည့်ပေးလိုက် ပါတယ်။ ဒီနေရာမှာ အခုပြောခဲ့တဲ့ Address ဟာ ခုနက Network Card က Address ကိုပြောတာဖြစ်ပါတယ်။

၈.၃ 10 Mbps ရှိ IEEE Standards များ

Ethernet မှာ 10 Mbps Transmit လုပ်နိုင်တဲ့ စံစနစ်များအုပ်စု (၄) ခုရှိပါတယ်။ အဲဒီတွေကတော့

(၁) 10Base5 : Thicknet Coaxial Cable ကိုအသုံးပြုသော Ethernet

(၂) 10Base2 : Thinnet Coaxial Cable ကိုအသုံးပြုသော Ethernet

(၃) 10BaseT : Unshielded Twisted Pair (UTP) ကိုအသုံးပြုသော Ethernet

(၄) 10BaseF : Fiber-Optic Cable ကိုအသုံးပြုသော Ethernet တို့ဖြစ်ကြပါတယ်။

10Base5 အကြောင်း

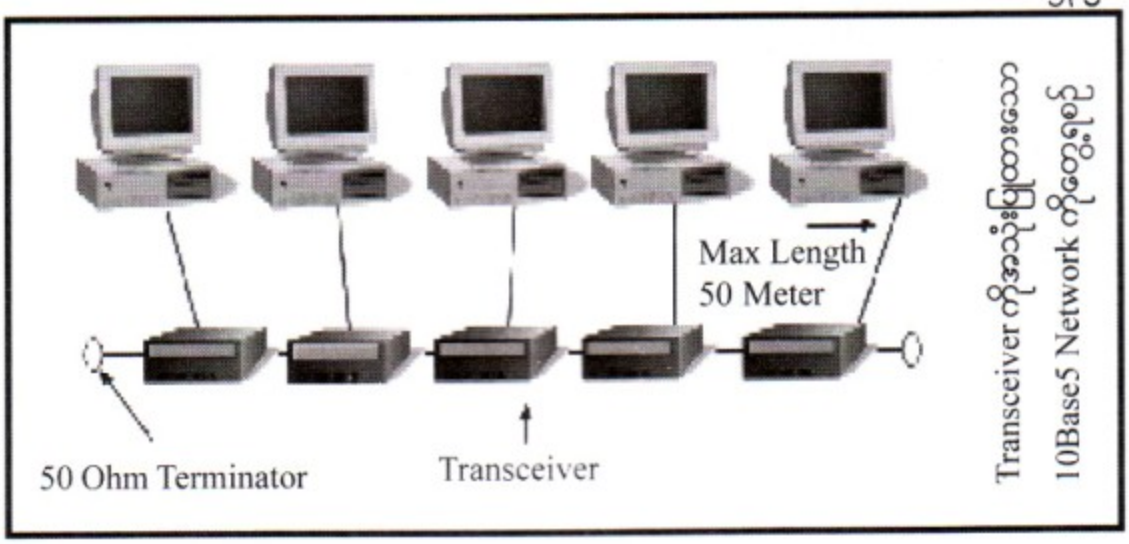
10Base5 Ethernet ကို Standard Ethernet လိုလည်းခေါ်ပါတယ်။ ဘာလို့လည်းဆိုတော့အဲဒီ 10Base5 Medium ကEthernet စတင်ကတည်းကအသုံးပြုခဲ့လို့ပဲဖြစ်ပါတယ်။ ဒီ Network နည်းပညာက Transceivers တွေကိုအသုံးပြုပါတယ်။ Thicknet Cable တွေဟာ ၎င်း Transceiver က Vampire Tap များနှင့်ချိတ်ဆက်တာဖြစ်ပါတယ်။ Vampire Tap က Cable ရဲ့ လျှပ်ကူး Conductor အထိ ထိုးဖောက်စိုက်ဝင် သွားမှာဖြစ်ပါတယ်။ Thicknet Cable တွေဟာကွန်ပျူတာမှာ Network Card ကိုတိုက်ရိုက်လာတပ်ထားကြ တာမဟုတ်ပါဘူး။ အပေါ်ကပြောခဲ့သလို ပုံမှာပြထားသလို Thicknet Cable ဟာ Transceiver တွေနှင့်သာ ချိတ်ဆက်ထားတာပါ။ တစ်ခါ Transceivers တွေကနေ ကွန်ပျူတာဆီက Network Card ရဲ့ AUI ခေါ် DIX ဆီကို Drop Cable နှင့်ဆက်သွယ်တာဖြစ်ပါတယ်။ ဒီတော့ ကွန်ပျူတာတိုင်းဟာ Thicknet ကိုဆက်သွယ် ဖို့ Transceivers နှင့် Drop Cable ရှိရမှာဖြစ်ပါတယ်။ 10Base5 Ethernet ရဲ့ Cable အကွာအဝေး

ကန့်သက်ချက်တွေဟာ အခြားသော Ethernet တွေထက်စာရင် ပိုပြီးတော့စည်းကမ်းချက် များပြားလွန်းလှ ပါတယ်။ ပြောရမယ်ဆိုရင် Transceiver တွေဟာ တစ်ခုနှင့်တစ်ခုအနည်းဆုံး ၈ပေ ခွာထားရမှာဖြစ်ပါတယ်။ Cable Segment တစ်ပိုင်းဟာအများဆုံ မီတာ ၅၀၀ အထိပဲရနိုင်ပါတယ်။ Repeater တွေသုံးပြီးချိတ်ဆက် မယ်ဆိုရင် အဲ့ဒီလို မီတာ ၅၀၀ အကွာရှိတဲ့ Cable Segment ပေါင်း ၅ခု အထိချိတ်ဆက်နိုင်ပါတယ်။ ဒီတော့ Network တစ်ခုလုံးရဲ့ စုစုပေါင်းအလျားဟာ မီတာ ၂၅၀၀ အထိရရှိနိုင်ပါတယ်။ ကွန်ပျူတာ နှင့် Transceiver အကြားချိတ်ဆက်ထားတဲ့ Drop Cable ဟာ မီတာ ၅၀ လောက်ပဲရှိရပါ့မယ်။ Network တစ်ခုလုံးရဲ့ Total Length ကိုတိုင်းတာရာမှာ ဒီ Drop Cable တွေရဲ့အလျားကိုထည့်တွက်စရာမလိုပါ။

ကျွန်တော်တို့ Coaxial Ethernet Network တိုင်းမှာ (Coaxial Ethernet ဆိုတာ 10Base5 နှင့် 10Base2 ကိုပဲပြောတာ။ Ethernet တိုင်းလို့မပြောဘူး) 5-4-3 Rules ဆိုတာရှိပါတယ်။ 5-4-3 Rules ဆိုတဲ့ အဲ့ဒီမှာ Repeaters ၄ခုပါရှိမယ်။ Repeater ၄ခုကြောင့် Network ဟာ အပိုင်း၅ပိုင်းပါရှိပါတယ်။ ၎င်းအပိုင်း၅ပိုင်းမှာမှ ပစ္စည်းတွေချိတ်ဆက်ထားတဲ့အပိုင်းက ၃ပိုင်းပဲရှိပါတယ်။ ဒါကို 5-4-3 Rules လို့ခေါ်ပါ တယ်။ ဒီ Rules ဟာ Attenuation ကြောင့် Signal Loss ဖြစ်မှုကိုကာကွယ်ပေးပါတယ်။ ပုံ ၈.၂ ကိုကြည့်

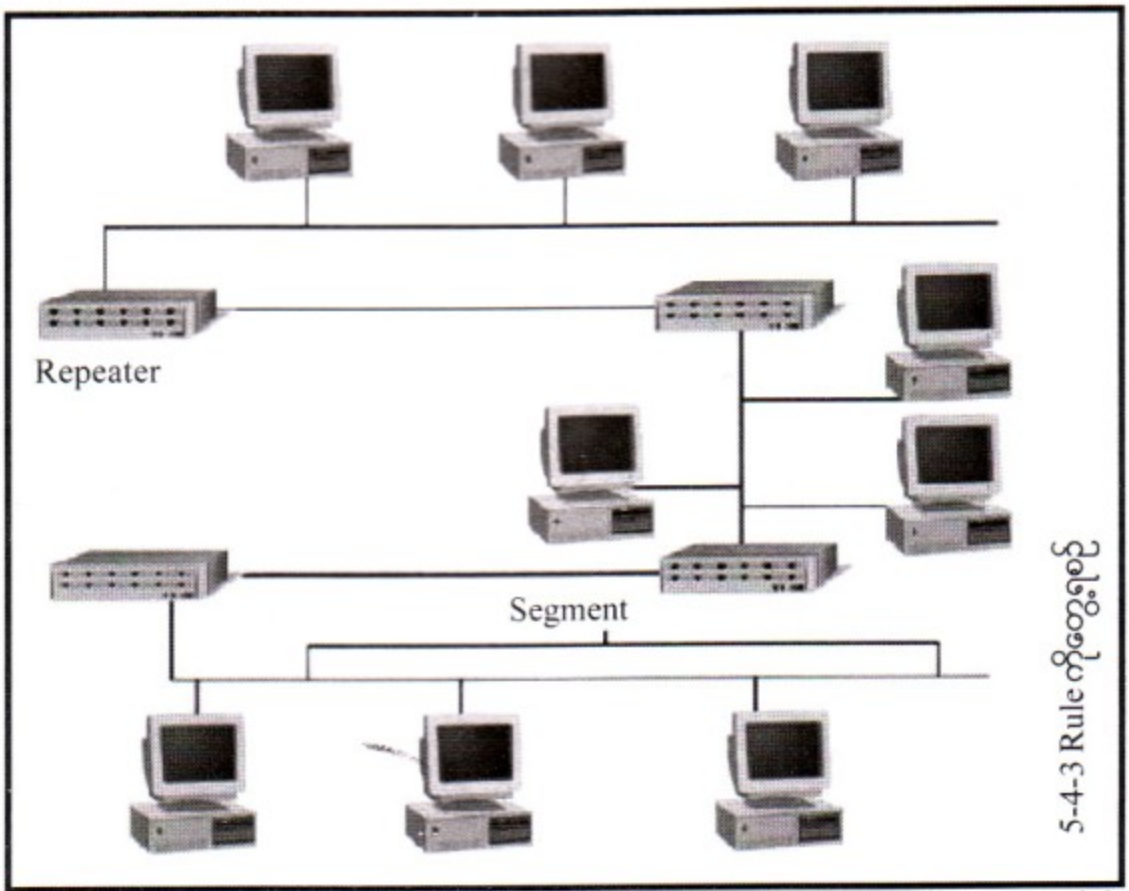
Category	Specification
IEEE Specification	802.3
Advantages	Long maximun cable length
Disadvantage	Difficult to install: cost
Topology	Linear bus
Cable Type	50-ohm thicknet
Channel access method	CSMA/CD
Transceiver location	Connected to cable at vampire tap
Maximum cable segment length	500 meters (1640 feet)
Maximum total network length	2500 meters (8200 feet)
Maximum drop cable length	50 meters (164 feet)
Maximum distance between transceivers	2.5 meters (8 feet)
Maximum number of segment	5 connected by 4 repeaters
Maximum number of populated segments	3
Maximum devices per segment	100
Maximum devices per network	1024
Transmission speed	10 Mbps

ပုံ ၈.၁



10Base5 Cable ဟာ Ethernet Architecture ရဲ့ကနဦး Cable အမျိုးအစားဖြစ်ပေမယ့် ၎င်းရဲ့ကန့်သတ်ချက်တွေနှင့်ခက်ခဲတဲ့ Installation တွေကြောင့် အသုံးပြုခဲပါတယ်။ ကနေ့ခေတ်မှာတော့ 10Base5 ကို Backbone Network တွေထဲမှာပဲအသုံးများပါတယ်။ အဲ့ဒီ Backbone ကနေမှ 10BaseT နှင့် 10Base2 တို့ဟာ Multiport Repeater ကိုသုံးပြီးပြန်ခွဲထွက်လာကြမှာဖြစ်ပါတယ်။ အောက်မှာ 10Base5 နှင့်ပတ်သက်နေသော Specification များကိုဖော်ပြပေးထားပါတယ်။

ပုံ ၈.၂



10Base2 အကြောင်း

Ethernet ဟာ မူလပထမ 10Base5 ပြီးတဲ့နောက် 10Base2 ကိုထုတ်ပါတယ်။ 10Base2 မှ 2 ဆိုတာဟာ Cable Segment တစ်ခုဟာ မီတာ ၂၀၀ အထိရှိနိုင်တယ်လို့အစွဲပြုထားပါတယ်။ အဲပေမယ့် တကယ်တမ်းမှာတော့ 10Base2 ရဲ့ Segment ဟာ ၁၈၅ မီတာအထိပဲရပါတယ်။ 10Base2 ဟာ Coaxial Cable ကိုပဲအသုံးပြုတာဖြစ်ပါတယ်။ အဲပေမယ့် 10Base5 လို Thicknet မဟုတ်တော့ဘဲ ပျော့ပျောင်းပြီး (Flexible) တပ်ဆင်ကိုင်တွယ်ရလွယ်ကူတဲ့ Thinnet ဖြစ်ပါတယ်။ 10Base2 ဟာ 10Base5 နှင့်မတူတဲ့ နောက်တစ်ချက်က 10Base2 ဟာ Network Card မှာပါတဲ့ Transceiver ကိုအသုံးပြုပါတယ်။ 10Base5 လို External Transceiver မလိုအပ်ပါ။ အဲကြောင့် Thinnet Cable ဟာ Network Card နှင့်တိုက်ရိုက်လာချိတ်တာဖြစ်ပါတယ်။ ရှေ့သင်ခန်းစာမှာတုန်းကပြောခဲ့သလိုပါပဲ။ 10Base2 ဟာ Network Card ကနေ Cable ကိုချိတ်ဆက်ဖို့ BNC Connector ကိုသုံးပါတယ်။ Topology ကတော့ Bus Topology ဖြစ်ပါတယ်။ Cable တွေရဲ့အဆုံးမှာတော့ Terminator တွေတပ်ပေးရပါတယ်။ Cable Length ဟာအနည်းဆုံး (၅မီတာ) လောက်တော့ရှိဖို့လိုအပ်ပါတယ်။ Thinnet Cable ဟာ TV အင်တာနက်ကြိုး အဲလေ အင်တီနာကြိုးလို့ ပြောတာတွေဖူးမှာပါ။ Shield ကြိုးလို့လည်းခေါ်ပါတယ်။ အဲ့ဒါ Thinnet Cable ပဲ။ အဲပေသိ TV အင်တီနာမှာသုံးတဲ့ Thinnet Cable က 75 Ohm ဖြစ်ပြီး Network မှာသုံးတဲ့ Thinnet က 50 Ohm ဖြစ်ပါတယ်။ Cable Type အနေနှင့်ပြောရမယ်ဆိုရင်တော့ RG-58 A/U နှင့် RG-58 C/U တို့ဖြစ်ကြပါတယ်။ ဒီ Cable မှာ RG-58U ဆိုတာရှိသေးတယ်။ သူက 10Base2 Ethernet နှင့်အလုပ်မလုပ်နိုင်ပါဘူး။ 10Base2 မှာလည်း 10Base5 လို 5-4-3 Rule ဆိုတာရှိပါတယ်။ 10Base2 မှာက Cable Segment ဟာ ၁၈၅ မီတာရှိပြီး 5-4-3 Rule အရ Repeaters လေးခုပါရပြီး Segments က ငါးခုဖြစ်ပါတယ်။ အဲကြောင့် ၁၈၅ မီတာ ၅ဆဖြစ်ကာ Network တစ်ခုရဲ့ Total Length က (Network တစ်ခုရဲ့အစွန်းနှစ်ဖက်က) ၉၂၅ မီတာအထိဖြစ်သွားပါတယ်။ အဲ့ဒီ Segment ၅ခုမှာမှ ၃ခုသာလျှင်ပစ္စည်းတွေချိတ်ဆက်တာဖြစ်ပြီး ပစ္စည်းမချိတ်ဆက်ထားတဲ့ Repeater တွေက Repeater အချင်းချင်း Inter Link ပြန်ချိတ်ထားတာဖြစ်ပါတယ်။ 10Base2 ဟာ Cable Segment တစ်ခုမှာပစ္စည်းပေါင်း ၃၀ခုအထိချိတ်ဆက်နိုင်ပါတယ်။ Thinnet မှာအားသာတဲ့အချက်ရှိတာက တပ်ဆင်ရတာလွယ်ကူတာနှင့်ကုန်ကျစရိတ်သက်သာခြင်းကြောင့် Thicknet ထက်ပို၍လျှပ်ပြန်စွာလူကြိုက်များလာတဲ့ Network Media ဖြစ်လာပါတယ်။ အဲပေမယ့်လည်းနောက်ထပ် Ethernet Standard တွေထပ်မံပေါ်ထွက်လာတော့သူလည်း အစားထိုးခံရတာပါပဲ။ Thinnet ကိုကနေ့ခေတ်မှာ Small Office လေးအချို့တွေမှာပဲအသုံးပြုပါတော့တယ်။ တစ်ဖက်စာမျက်နှာမှာ 10Base2 Specification တွေကိုပြပေးထားပါတယ်။

Category	Specification
IEEE Specification	802.3
Advantages	Inexpensive: easy to install and configure
Disadvantage	Difficult to troubleshoot
Topology	Linear bus
Cable Type	50-ohm thinnet-RG-58A/U or RG-58C/U
Channel access method	CSMA/CD
Transceiver location	On NIC
Maximum cable segment length	185 meters (670 feet)
Maximum total network length, end to end	925 meters (3035 feet)
Maximum distance between devices	5 meters (20 Inches)
Maximum number of segment	5 connected by 4 repeaters
Maximum number of populated segments	3
Maximum devices per segment	30
Maximum devices per network	1024
Transmission speed	10 Mbps

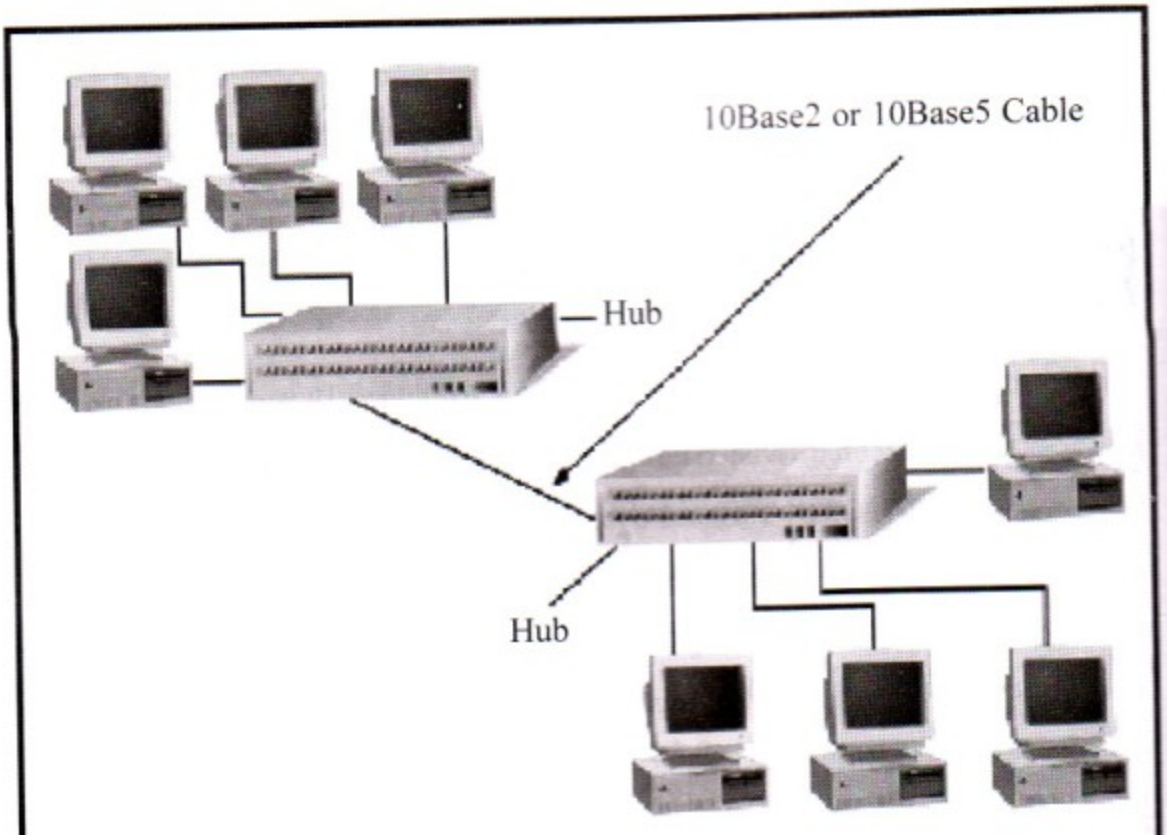
10BaseT အကြောင်း

10BaseT Ethernet ဟာပုံမှန်အားဖြင့်တော့ Unshielded Twisted Pair (UTP) Cable ကိုအသုံးပြုတာဖြစ်ပေမယ့် Shielded Twisted Pair (STP) Cable နှင့်လည်း Transmit လုပ်နိုင်ပါတယ်။ ကနေ့ခေတ်မှာခုနကပြောတဲ့ 10Base5 တို့ 10Base2 တို့ထက်ပိုပြီးရေပန်းစားပါတယ်။ ဘာလို့လည်းဆိုတော့ 10BaseT ဟာပြဿနာဖြေရှင်းရတာလွယ်ကူတဲ့ Star Topology ကိုသုံးထားလို့ဖြစ်ပါတယ်။ ဒါပေမယ့် 10BaseT ဟာအတွင်းမှာတော့ Bus Signalling ကိုအသုံးပြုတာဖြစ်ပါတယ်။ ဒီ 10BaseT မှာအသုံးပြုထားတဲ့ Active Hubs ဟာ Repeater သကဲ့သို့ Signal တွေကိုအားကောင်းလာအောင်ချဲ့ထွင်ပေးပါတယ်။ ဒါကြောင့် 10BaseT မှာ 5-4-3 Rule ဆိုတာမရှိပါဘူး။ 5-4-3 Rule ဟာအဆုံးမှအဆုံးသို့ဆိုတဲ့ End-to-End Rule ဖြစ်ပါတယ်။ Total Population Rule မဟုတ်ပါဘူး။ ဒီ 10BaseT ဟာ 5-4-3 Rule နှင့်မသက်ဆိုင်သောကြောင့် သူကစုစုပေါင်း Total Population နှင့်တွက်ပါတယ်။ 10BaseT Network တစ်ခုမှာ Hubs တွေအများကြီးနှင့်တပ်ဆင်လိုက်မယ်ဆိုရင် စုစုပေါင်း ၁၀၂၄ ကွန်ပျူတာအထိရရှိနိုင်ပါတယ်။ ဒီလိုလေဗျာ။ End-to-End ဆိုတာ 10Base5 တို့ 10Base2 တို့မှာ မျက်စိနှင့်မြင်ကြည့်လိုက် Cable Segment တစ်လျှောက်မှာ

ကွန်ပျူတာတွေ ပစ္စည်းတွေချိတ်ဆက်ထားတာ အခုကြတော့ 10BaseT ကဒ်လိုမဟုတ်ဘူးဗျ။ ကြိုးအရှည်ကြိုး ပေါ်မှာကွန်ပျူတာတွေက မှီခိုနေတာမဟုတ်ဘဲ ကြိုးတစ်စ ကြိုးတစ်ချောင်းအစွန်းတစ်ဖက်မှာ ကွန်ပျူတာ တစ်လုံးပဲရှိတယ်။ ဒါကြောင့် ကြိုးတစ်ကြိုးပျက်သွားရင် ကွန်ပျူတာတစ်လုံးပဲထိခိုက်မယ်။ 10Base5, 10Base2 တို့ကို Network ကြိုးတစ်ခုလုံး Failure ဖြစ်မသွားဘူး။ 10BaseT Cable မှာ Cable Grade တွေရှိပါတယ်။ အမျိုးအစားတွေပေါ့ဗျာ။ အင်္ဂလိပ်လိုတော့ Category ပေါ့။ Category 5 အထိရှိပါတယ်။ 10BaseT Ethernet ဟာ Category 3, 4 နှင့် 5 နဲ့ပဲအလုပ်လုပ်ပါတယ်။ ခုနောက်ပိုင်းမှာတော့ 10BaseT နှင့် Network ဆင်မယ်ဆိုရင် Category 5 UTP ကိုပဲအသုံးပြုကြပါတယ်။ ဘာလို့လည်းဆိုတော့ ၎င်းက 100 Mbps အထိရလို့ပါ။

10BaseT Cable အတွက်အဓိကကန့်သတ်ချက်ကတော့ Cable Distance ပါပဲ။ Cable Segment အလျားဟာအများဆုံး မီတာ ၁၀၀ အထိပဲရပါတယ်။ ဘယ် Twisted Pair Cable မဆိုပါ။ အဲ့ဒီတော့ ပုံမှာပြထားသလို 10BaseT Hub တွေ တစ်ခုနှင့်တစ်ခုဝေးကွာလို့ချိတ်ချင်ရင် 10Base5 ဒါမှမဟုတ် 10Base2 နှင့်ပြန်ချိတ်ပါတယ်။

ပုံ ၈.၃



ဝေးကွာလွန်းတဲ့ Hub နှစ်ခုကို 10Base2 or 10Base5 Cable နှင့်ချိတ်ဆက်ထားပုံ

Category	Specification
IEEE Specification	802.3
Advantages	inexpensive: easy to install & troubleshoot
Disadvantage	Small Maximum cable segment length
Topology	Star
Cable Type	Category 3,4, or 5 UTP
Channel access method	CSMA/CD
Transceiver location	On NIC
Maximum cable segment length	100 meters (328 feet)
Maximum distance between devices	N/A
Maximum number of segment	1024
Maximum devices per segment	2
Maximum devices per Network	1024
Transmission speed	10 Mbps

10BaseF အကြောင်း

10BaseF ဆိုတာ Fiber Optic Cable ကိုအသုံးပြုထားတဲ့ Ethernet ပဲဖြစ်ပါတယ်။ ၎င်းကို အခြေခံအားဖြင့် အမျိုးအစား (၃) ပိုင်းခွဲခြားထားပါတယ်။ အဲဒါတွေကတော့ -

(၁) 10BaseFL ဆိုတာရှိပါတယ်။ LAN တွေမှာ ကွန်ပျူတာတွေကိုချိတ်ဆက်တဲ့နေရာမှာသုံးပါတယ်။

(၂) 10BaseFP ဆိုတာရှိပါတယ်။ Passive Hub ကိုသုံးပြီး ကွန်ပျူတာတွေကိုချိတ်ဆက်ရာမှာသုံးပါတယ်။ အမျိုးအစားကတော့ Cable Segment အများဆုံးအလျားကတော့ မီတာ ၅၀၀ အထိပဲဖြစ်ပါတယ်။

(၃) 10BaseFB ဆိုတာရှိပါတယ်။ ၎င်းကတော့ Hubs တစ်ခုနှင့်တစ်ခုကြား Backbone အဖြစ်အသုံးပြုပါတယ်။

၎င်းတို့တစ်ခုချင်းစီဟာ Star Topology ကိုပဲအသုံးပြုပါတယ်။ ၎င်းတို့ဟာ 10BaseT လိုပါပဲ။ Network တစ်ခုထဲမှာပင် Repeaters တွေကိုသုံးပြီးအများဆုံး ၁၀၂၄ Node အထိရနိုင်ပါတယ်။ Fiber Optic ဟာ EMI ရဲ့နှောင့်ယှက်ခြင်းမှ ကင်းဝေးပါတယ်။ ၎င်းဟာ Transmit Speed အလွန်ကောင်းပါတယ်။ ဒါပေမယ့်တပ်ဆင်ရခက်ခဲခြင်းနှင့် ကုန်ကျစရိတ်များခြင်းတို့ စတဲ့အားနည်းချက်တော့ရှိပါတယ်။

Category	Specification
IEEE Specification	802.3
Advantages	Long distance
Disadvantage	High cost; difficult installation
Topology	Star
Cable Type	fiber-optic
Channel access method	CSMA/CD
Transceiver location	On NIC
Maximum cable segment length	200 meters (6561 feet), except for 10BaseFP at 500 meters (1635 feet)
Maximum number of segment	1023
Maximum devices per segment	2
Maximum devices per Network	1024
Transmission speed	10 Mbps

၈.၄ 100 Mbps ၌ IEEE စနစ်များ

ဒီကနေ့ခေတ်မှာ ကျယ်ပြန့်စွာအသုံးပြုနေတာကတော့ 100 Mbps Transmit လုပ်နိုင်တဲ့ Ethernet Standard ပဲဖြစ်ပါတယ်။ အဲဒါတွေကတော့ 100VG-AnyLAN နှင့် 100BaseT တို့ဖြစ်ကြပါတယ်။ ဒီလို High Speed ကြောင့် ၎င်းတို့ဟာရုပ်ပိုင်းဆိုင်ရာ၊ ဗီဒီယိုပိုင်းဆိုင်ရာ၊ CAD/CAM တွေမှာပါ အသုံးတည့်လာပါတယ်။

100VG-Any LAN အကြောင်း

Ethernet Standard တစ်ခုဖြစ်တဲ့ 100VG-Any LAN ကို 100BaseVG, 100VG, VG အဲဒီအပြင် Any LAN လို့ပါခေါ်ပါသေးတယ်။ ၎င်းကို HP နှင့် AT&T တို့ကထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ ၎င်း Ethernet နှင့် Token Ring နည်းပညာတွေကိုပေါင်းထားတာဖြစ်ပြီး၊ အသုံးပြုတဲ့ Channel Access ကတော့ Demand Priority Method ဖြစ်ပါတယ်။ ၎င်း Network ၏ Communication ကိုထိန်းချုပ်ပေးတဲ့ သူကတော့ Intelligent Hub ပဲဖြစ်ပါတယ်။ ကွန်ပျူတာက Data တွေကိုပို့လွှတ်တဲ့အခါ ပထမဆုံး Hub ဆီသို့ Demand Packet ကိုပို့လွှတ်လိုက်ပါတယ်။ ပြီးတော့မှ Hub ကကွန်ပျူတာရဲ့ ဘယ် Channel ကတော့ဖြင့်အားနေတယ်။ အဲဒီကနေ မင်းရဲ့ Data ကိုပို့လိုက်ဆိုပြီးပြန်ပြောပါလိမ့်မယ်။ ၎င်း Hub တွေဟာ

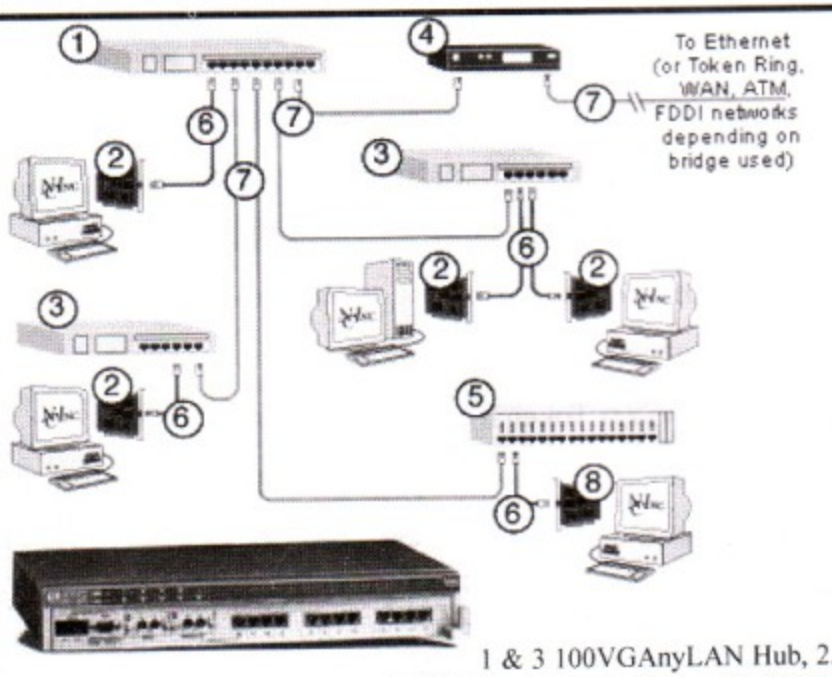
တစ်ခုမက ဆင့်ကဲဆင့်ကဲချိတ်ဆက်ထားလို့ရပါတယ်။ 10BaseT တုန်းကလိုပဲပေါ့။ Star Topology ပေါ့။ Root Hub လို့ခေါ်တဲ့ Parent Hub ဟာငြင်းကနေ Hub တွေအများကြီးချိတ်ဆက်လို့ရပါတယ်။

100VG-Any LAN ဟာ Voice Grade ရှိတဲ့ UTP Cable နှင့်တောင် Run လုပ်နိုင်ဖို့ဒီဇိုင်းဆွဲထုတ်လုပ်ထားတာဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင် UTP Cable Category 3 နှင့် ၎င်းအထက်တွေမှာ အသုံးပြုနိုင်ပါတယ်။ 100VG မှာတစ်ခုပြောစရာရှိတာက ၎င်းဟာ UTP Cable မှာ Wire ကြိုး (၄) စုံရှိဖို့လိုအပ်ပါတယ်။ အဲ့ဒီမှာနှစ်စုံက Data ကို Transmit လုပ်ဖို့အတွက်ဖြစ်ပြီး နောက်နှစ်စုံက Data ကို Receive လက်ခံဖို့အတွက်ဖြစ်ပါတယ်။ 10BaseT ဆိုရင်တော့ နှစ်စုံပဲအသုံးပြုပါတယ်။ တစ်ချို့ 10BaseT တွေမှာကြတော့ ဝါယာကြိုးနှစ်စုံကို Data အတွက်အသုံးပြုပြီး၊ ကျန်တဲ့ကြိုးနှစ်စုံကိုတော့ အသံ Voice အတွက်အသုံးပြုပါတယ်။ ဒီလိုပုံစံမျိုးနဲ့ 100VG-Any LAN ကိုသုံးဖို့အဆင်ပြေမှာမဟုတ်ပါ။ Cable ကိုငြင်း 100VG သုံးနိုင်ရန် Upgrade လုပ်ရမှာပါ။ ကုန်ကျစရိတ်သက်သာချင်တယ်ဆိုရင်တော့ 100VG ကိုမသုံးဘဲအခြားသော 100 Mbps Ethernet ကိုအသုံးပြုပါတယ်။ ဘာဖြစ်လို့တုန်းဗျ ခင်ဗျား (ခင်ဗျား) ဒီလိုဗျ။ ဒီ 100VG က Channel Access မှာ CSMA/CD ကိုမသုံးဘဲ Demand Priority ကိုသုံးတာကြောင့်ဖြစ်ပါတယ်။ နောက်ပြီး 100VG ကအခြားသော Ethernet တွေထက်ပိုပြီးတော့ Performance ကောင်းပါတယ်။ ဘာလို့လဲဆိုတော့ Hub က Network ရဲ့ Traffic အားလုံးကိုထိန်းချုပ်ပေးလို့ပါ။ ဒီလိုလေဗျာ။ ဒီ Network ကြီးတစ်ခုလုံးကို Packet တွေကို Data ပို့ဖို့ Broadcast လုပ်တာမျိုးမဟုတ်ဘဲ Hub က Network ကိုထိန်းချုပ်သွားတာဖြစ်လို့ပါ။ ထပ်ပြောပြမယ်ဆိုရင် 100VG က မဆိုင်တဲ့ Traffic တွေကိုဖယ်ရှားပစ်ပါတယ်။ အဲကြောင့် Network Effrciency တက်လာတယ်။ နောက်ပြီး ၎င်း 100VG က Data ကိုပို့ရာမှာ ရှာရိုးပေါက်အောင်လှည့်လည်နေတာမဟုတ်ဘဲ Destination ကွန်ပျူတာဆီကိုတိုက်ရိုက်ပို့တာဖြစ်ပါတယ်။ အဲကြောင့် Privacy လည်းပိုကောင်းလာပါတယ်။ Demand Priority ဟာဝင်လာတဲ့ Incoming Services တွေမှာဦးစားပေးစနစ်ကိုကျင့်သုံးပါတယ်။ ဥပမာပြောရရင်ဗျာ။ File Server အိမ့မဟုတ် Database Server တွေဆီကလာတဲ့ Data ကိုသာမန်ကွန်ပျူတာကလာတဲ့ Data ထက်ပိုဦးစားပေးလက်ခံတယ်ပေါ့ဗျာ။

100VG ရဲ့အကြီးမားဆုံးသော အကျိုးကျေးဇူးကတော့ အခြားသော Network Architecture ကို Support လုပ်နိုင်ပါတယ်။ ၎င်းဟာ Network Card ကိုငြင်း Network Card ရဲ့ Driver နှင့်ပဲ Setup လုပ်ထားမယ်ဆိုရင် 100VG ဟာ Ethernet Frame မဟုတ်ဘဲ Token Ring Frame ကိုတောင် Configured လုပ်နိုင်ပါတယ်။ ဆိုလိုတာက ကိုယ့်မှာ Token Ring Network ရှိပြီးသားဆိုရင် ပေါင်းစပ်နိုင်အောင်လို့ပေါ့ဗျာ။ နောက်ပြီး Bridge ကိုသုံးပြီးတော့လည်းသက်ဆိုင်ရာ Frame Type ကိုအသုံးပြုမယ်ဆိုရင် 100VG Network ဟာ Token Ring နှင့်ဖြစ်စေ Ethernet Network နှင့်ဖြစ်စေ အချက်အလက်တွေလွယ်ကူစွာဖလှယ်နိုင်ပါတယ်။ 100VG ရဲ့ကောင်းတဲ့အချက်တွေကြီးပြောလာတာ ထပ်ပြောရမယ်ဆိုရင် ၎င်းဟာ Category 3 UTP ကိုသုံးမယ်ဆိုရင်တောင် Cable Segment အလျားကိုအများဆုံး 100 Meters အထိရရှိနိုင်ပါတယ်။ နောက်တစ်ခုကအခြားသော Ethernet UTP တွေနှင့်မတူတဲ့အချက်က Category 5 UTP

Category	Specification
IEEE Specification	802.12
Advantages	Fast, easy to configure and troubleshoot; supports token ring and Ethernet packets
Disadvantage	High cost; limited distance over UTP
Topology	Star
Cable Type	Category 3 or higher UTP and STP, fiber-
	optic
Channel access method	Demand priority
Transceiver location	On NIC
Maximum cable segment length	100 meters (328 feet) Category 3 UTP, 150 meters (492 feet) Category 5 UTP, 2000 meters (6561 feet) fiber-optic
Maximum number of segment	1023
Maximum devices per segment	1
Maximum devices per network	1024
Transmission speed	100 Mbps

ပုံ ၈.၄



100VG AnyLan နှစ်ပုံစံကို 100VG AnyLan Hub နှင့်ဆောက်ထုတ်ခြင်း

1 & 3 100VGAnyLAN Hub, 2. 100VGAnyLAN NIC,
4. 100VG to Ethernet Bridge, 5. 10/100 Mbps Ethernet Switch,
6. 4 Pair Cat 5 Color Coded Patch Cables, 7. 4 Pair Cat 5 UTP Cable, 8. 10 Base-T NIC

Produced by YOUTH Computer Co., Ltd

ကိုသာသုံးထားမယ်ဆိုရင် အများဆုံး Cable Segment အလျားဟာ မီတာ၁၅၀ အထိရှိနိုင်ပါတယ်။ 100VG Fiber-Optic Cable ကိုလည်းအသုံးပြုနိုင်ပါတယ်။ ၎င်းနှင့်ဆိုရင်တော့ မီတာ ၂၀၀၀ လောက်အထိ Transmit လုပ်နိုင်ပါတယ်။ 100VG ကကုန်ကျစရိတ်တော့ကြီးတယ်ဗျ။ Network Card ကလည်းသူ့ဟာနှင့်သူပဲ။ Hub ကြတော့လည်း Demand Priority Channel Access ရတဲ့ဟာမှ။ ဒီတော့ အခြားသော Ethernet ထက်စရိတ်ပိုကြီးတော့တာပေါ့။

100BaseT အကြောင်း

100BaseT ကို 100BaseFX ဒါမှမဟုတ် Fast Ethernet လို့လည်းခေါ်ပါတယ်။ ၎င်းဟာ 10BaseT ရဲ့ Extention လည်းဖြစ်ပါတယ်။ 3 Com Intel နှင့်အခြားသောအဖွဲ့အစည်းတို့ဟာ 802.3 Ethernet Standard ကိုပြင်ဆင်ခဲ့ခြင်းအားဖြင့် Category 5 UTP ကိုသုံးကာ 100 Mbps ဖြင့် Transmission လုပ်နိုင်စေပါတယ်။ 100BaseT ဟာ 100VG တုန်းကလိုပဲပါပဲ။ Hub တွေကိုဆင့်ကဲဆင့်ကဲ ချိတ်ဆက်ပြီးအသုံးပြုနိုင်ပါတယ်။ 100BaseT မှာဆင့်ပွားအမျိုးအစားနောက်ထပ် (၃)မျိုးရှိပါတယ်။

Category	Specification
IEEE Specification	802.3
Advantages	Fast, easy to configure and troubleshoot;
Disadvantage	High cost; limited distance
Topology	Star
Cable Type	Category 3 or higher UTP -100BaseT4; Category 5 UTP-100BaseTX Fiber-optic-100BaseFX
Channel access method	CSMA/CD
Transceiver location	On NIC
Maximum cable segment length	100 meters (328 feet) 100BaseT4 2000 meters (6561 feet)-100BaseFX
Maximum number of segment	1023
Maximum devices per segment	1
Maximum devices per network	1024
Transmission speed	100 Mbps

အဲ့ဒါတွေကတော့ -

(၁) 100BaseT4: ဝါယာကြိုးလေးစုံပါသော Category 3,4,5 UTP Cable

(၂) 100BaseTX: နှစ်စုံပါရှိသော Category 5 UTP Cable

(၃) 100BaseFX: နှစ်မျှင်ပါသော Fiber-Optic Cable တို့ဖြစ်ကြပါတယ်။

ဒင်း Fast Ethernet ကိုအသုံးပြုရာမှာသတိထားရမှာက ကြိုးတစ်မျိုး (Category) ချင်းစီရဲ့လိုအပ်ချက်တွေပဲဖြစ်ပါတယ်။ သဘောကတော့ 100BaseTX ဆိုရင် Category 5 UTP ကိုလိုအပ်တယ်ဆိုပေမယ့် ကြိုးကိုနှစ်စုံပဲအသုံးပြုပါတယ်။ 100BaseT4 ကြတော့ Category 3 နှင့်အထက်အသုံးပြုတယ်ဆိုပေမယ့် ကြိုးကိုလေးစုံစလုံးအသုံးပြုပါတယ်။ 100BaseTX ကတော့ တခြားထက်ပိုမိုကျယ်ပြန့်စွာအသုံးပြုနေတာကြောင့် ယေဘုယျအားဖြင့်ဝင်းကိုပဲ Fast Ethernet လို့ခေါ်ပါတယ်။

၈.၅ 1 Gbps ရှိသော Ethernet အကြောင်း

IEEE ဟာ 1000BaseX ဆိုတဲ့မူအောက်မှာပဲ အမျိုးမျိုးသော Gigabit Ethernet Standard တွေကိုသတ်မှတ်ခဲ့ပါတယ်။ 1000BaseX ဆိုတဲ့ ဒီနေရာမှာ X ဆိုတာ အခြားစာလုံးတစ်ခုအစားထိုးဝင်ရောက်လာမယ့်သဘောဖြစ်ပါတယ်။ 1 Gbps မှာအသုံးပြုတဲ့ Signaling Method ဟာ မြန်လွန်းတာကြောင့် အခြားသောနှေးကွေးတဲ့ Slower Ethernet နည်းပညာတွေမှာသုံးတဲ့ Method နှင့်ကွဲပြားမှုတော့ရှိပါတယ်။ တကယ်တော့ Gigabit Ethernet Specificaiton ဟာ ၁၉၉၄တုန်းက ANSI X3.230 မှာအခြေခံထားတာဖြစ်ပြီး သူက Fiber Channel အတွက်ဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင် Stronge Area Network ဖြစ်တဲ့ SAN တွေမှာသုံးဖို့ Develop ဖြစ်လာတဲ့ Fiber Optic အခြေပြု Network ဖြစ်ပါတယ်။ 1000BaseX ဟာ 8B/10B Coding စနစ်ကိုအသုံးပြုပါတယ်။ 8B/10B ဆိုတာ Data Packaged တစ်ခုမှာအမှန်တကယ်ရှိတဲ့ Data က 8 bits ဖြစ်ပြီး ကျန် 2 Bits က Error Connection Data ဖြစ်ပါတယ်။ Gigabit Ethernet နှင့်ပတ်သက်လို့ရှင်းပြစရာရှိပါသေးတယ်။ ဒီလိုပါ။ အဲ့ဒီ Gigabit Ethernet မှာ 1000BaseT ဆိုတာရှိသဗျ။

သူက ကျွန်တော်အခုအပေါ်ကပြောနေတဲ့ 1000BaseX နှင့်မတူဘဲကွဲပြားတယ်ပေါ့ဗျာ။ နောက်ပြီး 1000BaseT က Fiber Channel ရဲ့ Physical Layer Specification နှင့်လည်းကိုက်ညီမှုမရှိဘူး။ မဆည်းကပ်ဘူးပေါ့ဗျာ။ 1000BaseX Standard နှင့်အကျိုးမဝင်ဘူးပေါ့ဗျာ။ အဲ့ကြောင့် 1000BaseT Standard ဆိုတာသက်သက်ဖြစ်လာပါတယ်။

ဒီတော့က 1000BaseX နှင့် 1000BaseT တို့အတွက် 802.3 Specification ဟာနှစ်ခုသီးခြားစီဖြစ်ပေါ်လာရတော့တယ်။ အဲ့ဒါက -

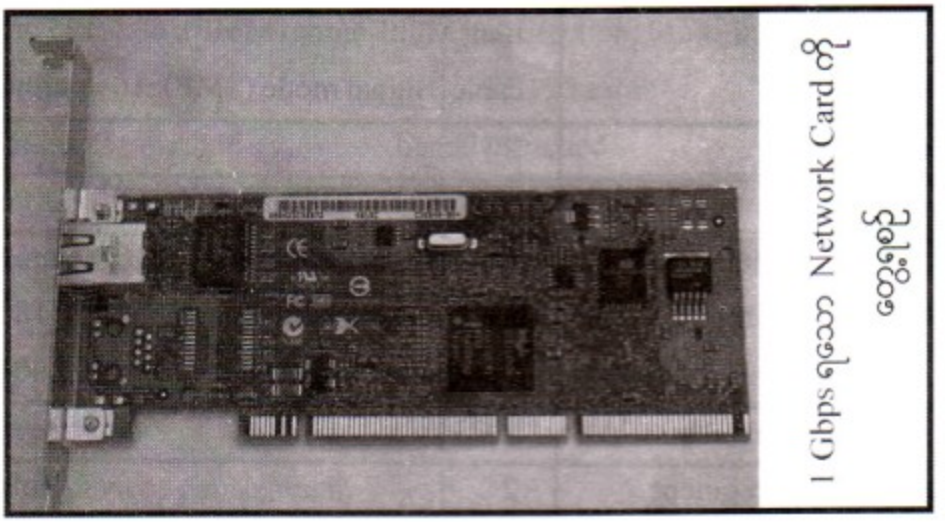
(၁) 802.3Z-1998 ဆိုတာရှိတယ်။ ဒင်းဟာ 1000BaseX Specification တွေဖြစ်ကြတဲ့ L (Long Wavelength Laser/ Fiber Optic), S (Short Wavelength Laser/ Fiber-Optic) နှင့် C (Copper

Jumper Cables) စတာတွေပေါ်သက်ရောက်ပါတယ်။ Cover ဖြစ်တယ်ပေါ့ဗျာ။

(၂) 802.3ab-1999 ဆိုတာရှိတယ်။ သူကတော့ 1000BaseT ဖြစ်တယ်။ ၎င်းဟာ ဝါယာကြိုးလေးစုံပါဝင်သော 100 Ohm ရှိတဲ့ Category 5 Cable အမျိုးအစားကိုသုံးတယ်ဆိုတာလိုအပ်ပါတယ်။

Gigabit Ethernet တွေဟာ Network Card ပဲဖြစ်စေ၊ Switches ပဲဖြစ်စေ၊ အခြားဆက်သွယ်ရေးပစ္စည်းတွေပဲဖြစ်စေ၊ Full Duplex နှင့်အလုပ်လုပ်ကြပါတယ်။

ပုံ ၈.၅



1 Gbps ရသော Network Card တို့

1000BaseLX အဓိပ္ပာယ်

1000BaseLX ဟာ Fiber Optic Media ကိုအသုံးပြုပါတယ်။ အဲ့ဒီမှာ L ဆိုတာက Long Wavelength ကိုဆိုလိုတာဖြစ်ပါတယ်။ အဓိပ္ပါယ်ကအသုံးပြုတဲ့ Cable (Medium) မှာ Signal တွေကိုပို့ဖို့အသုံးပြုတဲ့ Laser တစ်မျိုးပဲဖြစ်ပါတယ်။ ဒီ Long Wavelength ရှိတဲ့ Laser ဟာ 1270 မှ 1355 Nonometers အကြား Wavelength ရှိပါတယ်။ ၎င်းဟာ Optical Fibers တွေမှာ Single Mode ရော Multiple Mode နှင့်ပါအလုပ်လုပ်ပါတယ်။ Long Wavelength Laser ဟာ Short Wavelength Laser ထက်စရိတ်ပိုများတယ် ဆိုပေမယ့် ၎င်းဟာ Signal တွေကိုခရီးဝေးဝေးထိပို့ဆောင်ပေးနိုင်ပါတယ်။

တစ်ဖက်စာမျက်နှာမှာ 1000BaseLX Ethernet ရဲ့ Specification ကို တွေ့မြင်နိုင်ပါတယ်။

Category	Summary
IEEE Specification	802.3z
Advantages	Fast; support full-duplex communications
Disadvantage	High cost; hard to deploy and install
Topology	Star
Cable Type	Two standard of fiber-optic cable per connection; Multi-mode (MMF): 62.5/125 or 50-125 cable; Signal mode (SMF): 10 micron cable
Channel access method	Switched
Transceiver location	On NIC
Maximum cable segment length	Half-duplex MMF, SMF: 316 meters (1036 ft): full-duplex MMF: 550 meters (1804 ft): full-duplex SMF; 5000 meters (16,404 ft)
Maximum number of segments	1023
Maximum devices per segment	2
Maximum devices per Network	1024
Transmission speed	1000 Mbps (uses 8B/10B encoding); 2000 Mbps in full-duplex mode

1000BaseSX အကြောင်း

1000BaseSX ဟာ Fiber-Optic ကိုအသုံးပြုပါတယ်။ S ကတော့ Short Wavelength ကို ဆိုလိုပါတယ်။ ခုနက အပေါ်မှာပြောခဲ့သလိုပါပဲ။ Medium ပေါ်မှာ Signal တွေကိုပို့လွှတ်တဲ့အခါအသုံးပြုတဲ့ Laser တစ်မျိုးဖြစ်ပါတယ်။ ၎င်းရဲ့ Wavelength ဟာ 770 မှ 860 Nonometers အထိရှိပါတယ်။ ၎င်းဟာ Optical Fibers တွေမှာ Multi Mode နှင့်ပဲအလုပ်လုပ်နိုင်ပါတယ်။ Short Wavelength ဟာ Long Wavelength လောက် Data တွေကိုဝေးဝေးမပို့နိုင်ဘူးဆိုပေမယ့် ဈေးတော့သက်သာပါတယ်။

တစ်ဖက်စာမျက်မှာ 1000BaseSX Ethernet နှင့်ပတ်သက်လို့လေ့လာကြည့်ပါအုံး။

Category	Summary
IEEE Specification	802.3z
Advantages	Fast; support full-duplex communications
Disadvantage	High cost; hard to deploy and install
Topology	Star
Cable Type	Two standard of fiber-optic cable per connection; Multi-mode (MMF): 62.5/125 or 50-125 cable
Channel access method	Switched
Transceiver location	On NIC
Maximum cable segment length	Half-duplex 62.5 MMF, 275 meters (902 ft): Half-duplex 50 MMF: 550 meters (1804 ft): full-duplex SMF; 5000 meters (16,404 ft)
Maximum number of segments	1023
Maximum devices per segment	2
Maximum devices per Network	1024
Transmission speed	1000 Mbps (uses 8B/10B encoding); 2000 Mbps in full-duplex mode

1000BaseCX အကြောင်း

1000BaseCX က Shield ပါသော Balanced ဖြစ်တဲ့ Copper Jumper Cable ကိုအသုံးပြုပါတယ်။ အဲ့ဒီမှာ C ဆိုတာက Copper ကိုဆိုလိုချင်တာပါ။ သူက Electrical Signal ကိုအသုံးပြုပါတယ်။ ၎င်း Jumper Cable တွေပုံမှန်အားဖြင့်တော့ ပစ္စည်းတွေကိုအချင်းချင်းချိတ်ဆက်ခြင်း Interconnections နှင့် Switch ဖြင့် VLANs များ Inter Link ချိတ်ဆက်ရာမှာအသုံးပြုပါတယ်။ ၎င်း Jumper Cable ကို Twinax အိမှုမဟုတ် Short-Haul Copper Cables လို့လည်းခေါ်ပါသေးတယ်။ ၎င်း Cable ရဲ့ Segment Length ဟာ ၂၅မီတာအထိပဲရှိနိုင်ပါတယ်။ အဲ့ကြောင့် ၎င်းကိုအဓိကအားဖြင့်နီးကပ်စွာရှိတဲ့ ပစ္စည်းတွေကို ချိတ်ဆက်ခြင်းနှင့်တပ်ဆင်ထားသောပစ္စည်းများကိုချိတ်ဆက်ရာမှာ အသုံးပြုပါတယ်။ 1000BaseCX Ethernet နှင့်ပတ်သက်လို့ တစ်ဖက်စာမျက်နှာမှာလေ့လာကြည့်ပါအုံး။

Category	Summary
IEEE Specification	802.3z
Advantages	Fast; support full-duplex communications
Disadvantage	High cost; short-haul only
Topology	Star
Cable Type	Two standard of copper cable (twinax); sold in prefabricated length only
Channel access method	Switched
Transceiver location	On NIC or switch
Maximum cable segment length	Half-duplex 25 meters (82 ft): full-duplex 25 meters (82 ft)
Maximum number of segments	1023 (normally, far fewer are used)
Maximum devices per segment	2
Maximum devices per Network	1024
Transmission speed	1000 Mbps (uses 8B/10B encoding),
	2000 Mbps in full-duplex mode

1000BaseT အကြောင်း

1000BaseT ကို IEEE Standard 802.3ab ဆိုပြီး ၁၉၉၉ ဇွန် ကတည်းက ထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ ၎င်းဟာ Gigabit Ethernet ကို Balance Category 5 Copper ဝါယာဖြင့် မီတာ(၁၀၀) အထိ Support လုပ်နိုင်ပါတယ်။ ဝါယာကြိုးလေးစုံလိုအပ်ပါတယ်။ ပြောရမယ်ဆိုရင် သူကဝါယာကြိုးတစ်စုံမှာ 250 Mbps နှင့် ကြိုးလေးစုံပေါင်းမှ 1 Gbps စုစုပေါင်းရရှိလာတာဖြစ်ပါတယ်။ 1000BaseT ဟာလည်း အထူးပြုလုပ်ထားတဲ့ ဆက်သွယ်ရေးပစ္စည်းတွေနှင့်ပဲ အလုပ်လုပ်ဆောင်ပါတယ်။ ရှင်းပြရမယ်ဆိုရင် Full-Duplex Transmission ရအောင် Hybrids လို့ခေါ်တဲ့ အထူးပြုလုပ်ထားတဲ့ပစ္စည်းနှင့် Multiple Signals တွေကိုပေါင်းစည်းခြင်း၊ Interference ကို Cancel လုပ်တဲ့ Concellers စတာတွေလိုအပ်ပါတယ်။

တစ်ဖက်စာမျက်နှာမှာ 1000BaseT Ethernet ကိုဖော်ပြပေးထားပါတယ်။

Category	Summary
IEEE Specification	802.3ab
Advantages	Fast; supports full-duplex communications
Disadvantage	High cost; short-haul cable segment only
Topology	Star
Cable Type	Four-pair, balance Category 5 cable; 100-ohm impedance
Channel access method	Switched
Transceiver location	On NIC
Maximum cable segment length	Half-duplex; 100 meters (328 ft): full-duplex; 100 meters (328 ft)
Maximum number of segments	1023
Maximum devices per segment	2
Maximum devices per Network	1024
Transmission speed	1000 Mbps (uses 100BaseTX or
	100BaseT2 signaling)

၈.၆ Ethernet Frame Type အခြားခြင်း

Ethernet နှင့်အခြားသော Network Architectures တွေနှင့် အဓိကကွာခြားတဲ့အချက်တစ်ခုက Ethernet ဟာ Data တွေကို Network Medium (Cable) ပေါ်ကိုမတင်မီ ဘယ်လိုတင်ရမလဲဆိုတာကို ပုံစံအမျိုးမျိုးရှိပါတယ်။ ကျွန်တော်ရှေ့သင်ခန်းစာတုန်းကလည်း ပြောဖူးပါတယ်။ Data တွေကို Network ပေါ်တင်တဲ့အခါ အထုပ်ကလေးတွေထုပ်ပြီးတင်တာ Packets Frame လေးတွေပြုလုပ်ပြီးတော့လေ။ အဲ့ဒီလို Packets လေးအဖြစ်တင်ရာမှာ Packets ရဲ့တည်ဆောက်ပုံ Structure ကိုအမျိုးမျိုးရှိတယ်လို့ပြောချင်တာပါ။ အမျိုးမျိုးဆိုတော့ သိပ်အများကြီးတော့မဟုတ်ပါ။ လေးမျိုးရှိပါတယ်။ ဟုတ်ပါတယ်။ Ethernet Frame Type လေးမျိုးရှိပါတယ်။ တစ်ခုနှင့်တစ်ခုဟာမတူညီကြတဲ့အပြင် အခြားတစ်ခုနှင့်လည်း တွဲအလုပ်မလုပ်ပါဘူး။ Ethernet ပစ္စည်း (ဥပမာ ကွန်ပျူတာ) နှစ်ခု တစ်ခုနှင့်တစ်ခုချိတ်ဆက်မိဖို့က တစ်ဖက်နှင့်တစ်ဖက် Frame Type တော့တူဖို့လိုပါတယ်။ ကဲ Frame Type လေးမျိုးကတော့ -

(၁) Ethernet 802.3 ကယေဘုယျအားဖြင့် Novell Netware 2.X နှင့် 3.X Network တွေရဲ့ IPX-SPX ကအသုံးပြုပါတယ်။

(၂) Ethernet 802.2 က Novell Netware 3.12 နှင့် 4.X Network တွေရဲ့ IPX/ SPX ကအသုံးပြုပါတယ်။

(၃) Ethernet SNAP ကိုတော့ EtherTalk နှင့် Mainframe Environments တွေမှာအသုံးပြုပါတယ်။

(၄) Ethernet II ကိုတော့ TCP/IP ကအသုံးပြုပါတယ်။

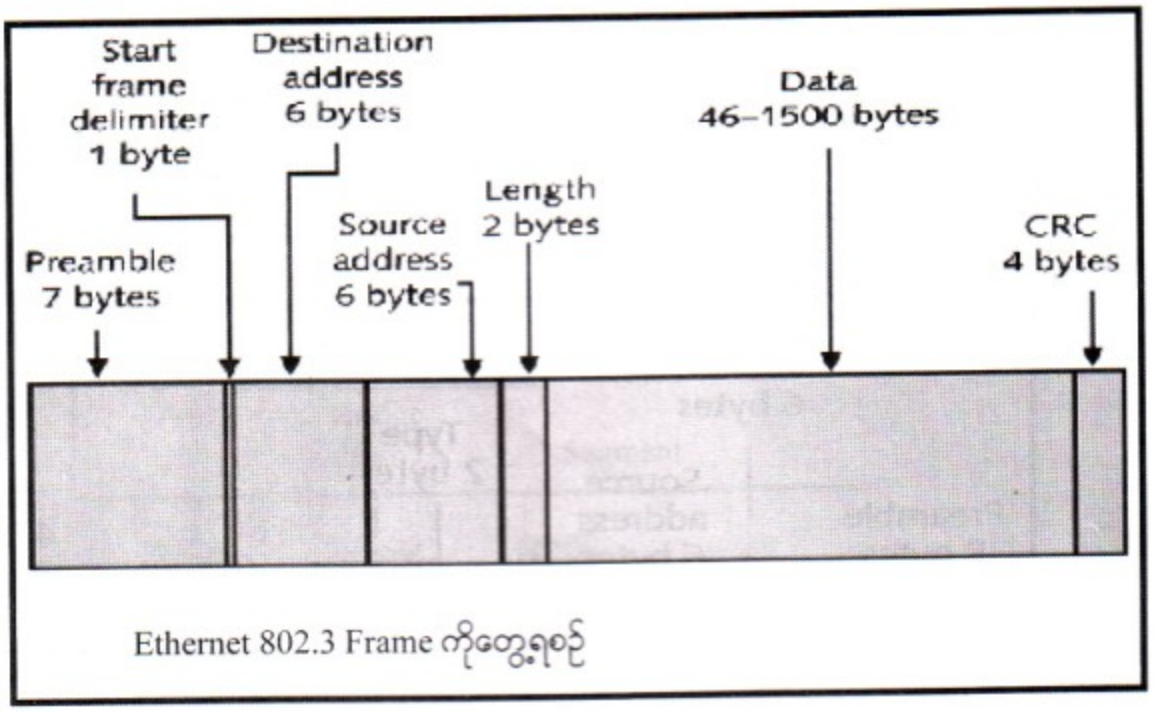
Ethernet Frame Type တိုင်းရဲ့ Packets အရွယ်အစားဟာ 64 မှ 1518 bytes အတွင်းရှိနိုင်ပါတယ်။ ပုံမှန်အားဖြင့်တော့ အခြေအနေအများစုမှာ Network ဟာ Frame Type တစ်ခုကိုပဲလိုအပ်ပါတယ်။ ဒါပေမယ့်ပေါ့နော်။ ဥပမာပြောရရင် File Server လို Database Server လိုမျိုးကြတော့ Frame Type တစ်ခါမက Support လုပ်ထားဖို့လိုအပ်တယ်။ ဘာလို့လဲဆိုတော့ ဒီ Server ကိုချိတ်ထားတဲ့ Client တွေထဲက Client တစ်ခုက Frame Type တစ်မျိုးနှင့် Server ကိုဆက်သွယ်နိုင်သလို တခြား Client တစ်ခုကလည်း Server ကိုအခြားသော Frame Type နှင့်ဆက်သွယ်နိုင်တယ်လေ။ ဘယ် Client က ဘယ် Frame Type နှင့်ဆက်သွယ် ဆက်သွယ် Server က Communication ဖြစ်နိုင်အောင် Server မှာ Multiple Frame Type Support လုပ်ထားဖို့လိုအပ်တယ်လို့ပြောချင်တာပါ။ ခုနကပြောခဲ့တယ်လေ။ Network Communication ဖြစ်ဖို့ တူညီတဲ့ Frame Type ရှိရမယ်လို့။

Ethernet 802.3 အကြောင်း

ဒင်းကိုတခါတရံမှာ Ethernet Raw လို့လည်းခေါ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ ဒင်း Ethernet 802.3 Frame Type ဟာ IEEE 802.3 Specification မပြည့်စုံသေးမှီမှာ ထုတ်လုပ်ခဲ့လို့ဖြစ်ပါတယ်။ အဲကြောင့် ပြောရမယ်ဆိုရင် 802.3 Frame ဟာ 802.3 Specification နှင့် Comply (လိုက်လျောညီထွေမှု) မဖြစ်ပါဘူး။ ဒင်းကို Novell ရဲ့ Netware 2.X နှင့် 3.X အသုံးပြုတဲ့ကွန်ရက်တွေမှာပဲ တွေ့ရပါတယ်။

တစ်ဖက်ကပုံဟာ 802.3 ရဲ့ Frame ဖွဲ့စည်းထားပုံဖြစ်ပါတယ်။ ဒင်းဟာ Preamble (အစပထမ) 7 Byte နှင့် SFD လို့ခေါ်တဲ့ Start Frame Delimiter နှင့်စထားပါတယ်။ SFD ဆိုတာ Frame စပြီဆိုပြီး ညွှန်ပြတာဖြစ်ပါတယ်။ ပြီးတော့ သူ့ရဲ့နောက်က Destination Address နှင့် Source Address ကလိုက်လာပါတယ်။ အဲ့ဒီနောက်ကမှ Data ကလိုက်လာမှာပါ။ Data ရဲ့ Length ကတော့ ခုနကပြောခဲ့တဲ့အတိုင်း 64 ကနေ 1518 Bytes အထိပြောင်းလဲနိုင်ပါတယ်။ နောက်ဆုံးမှာတော့ CRC လို့ခေါ်တဲ့ Cylical Redundany Check က 4 Bytes နှင့် လိုက်လာပါတယ်။ CRC ဆိုကတည်းကရယ်ရွယ်ရာကို Data ရောက်တဲ့အခါ ပျက်စီးမှု ရှိမရှိစစ်ဆေးသူဖြစ်ပါတယ်။

ပုံ ၈.၆



Ethernet 802.3 Frame ကိုတွေ့ရစဉ်

Ethernet 802.2 အခြေခံများ

Ethernet 802.2 Frame ဟာ Ethernet 802.3 Standard နှင့်လုံးဝ Comply ဖြစ်ပါတယ်။ IEEE 802.2 အုပ်စုဟာ OSI Model Data Link Layer ရဲ့ဆင့်ပွားအလွှာတစ်ခုဖြစ်တဲ့ Logical Link Control (LLC) နှင့်ပတ်သက်ဆက်နွယ်တာဖြစ်ပါတယ်။ Ethernet 802.2 ဟာ Ethernet 802.3 မှာပါတဲ့ Fields အားလုံးပါတဲ့အပြင် LLC နှင့်ပတ်သက်သောနောက်ထပ် Fields ၃ခုပိုပါဝင်လာပါတယ်။

Ethernet SNAP အခြေခံများ

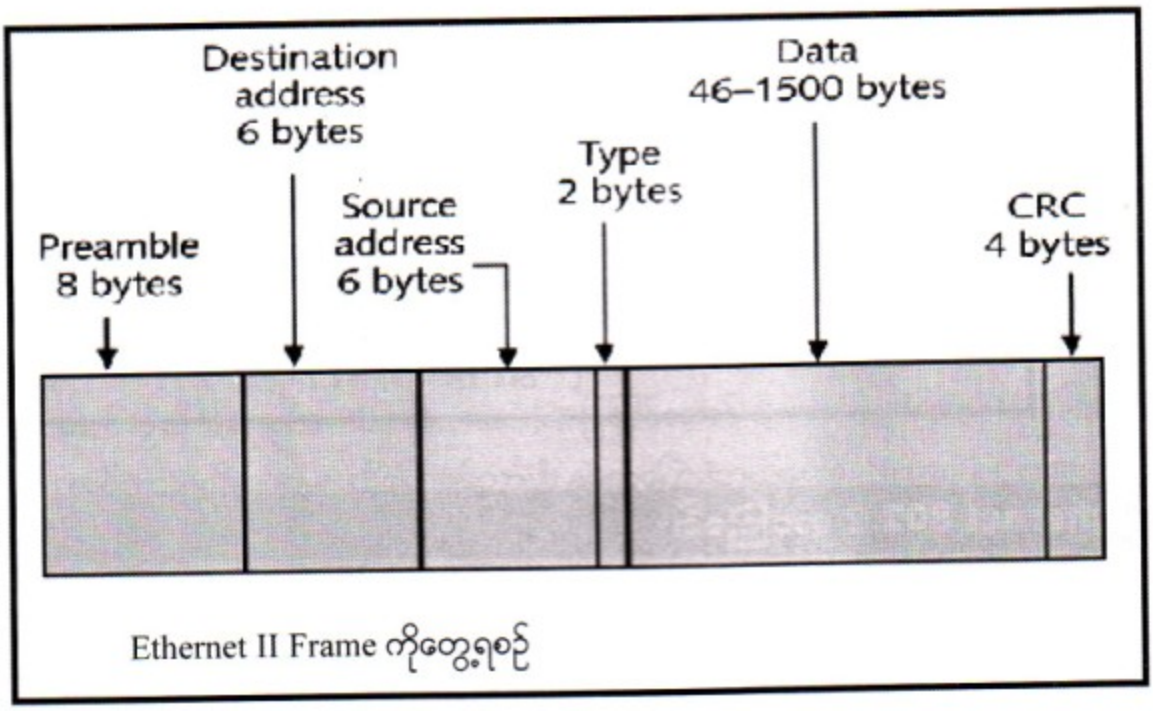
SNAP ဆိုတာ Sub Network Address Protocol လို့ဆိုပါတယ်။ AppleTalk Phase 2 ကွန်ရက်တွေမှာအသုံးပြုလေ့ရှိပါတယ်။ ၎င်းဟာ Ethernet 802.2 Frame ကို Enhancements လုပ်ထားတာဖြစ်ပြီး ၎င်းမှာ Protocol Type Field ဆိုတာပါလာပါတယ်။ ၎င်း Protocol Type Field ဟာ Frame ရဲ့ Data ပိုင်းကအသုံးပြုထားသော Network Protocol ကိုညွှန်ပြတာဖြစ်ပါတယ်။

Ethernet II အခြေခံများ

Ethernet II Frame ဟာ TCP/IP ကွန်ရက်တွေမှာအသုံးပြုတာဖြစ်ပါတယ်။ Ethernet II က 802.2 Frames နှင့်အနည်းငယ်ကွဲပြားမှုရှိပါတယ်။ ယှဉ်ကြည့်ရင်သိနိုင်ပါတယ်။ ပထမ 7 Byte ဟာ Ethernet

II မှာ 8 Byte ဖြစ်သွားပါတယ်။ ဘာလို့လည်းဆိုတော့ SFD 1 Byte စာ Seperate လုပ်မထားတော့ဘဲ ပေါင်းလိုက်လို့ပါ။ နောက်ပြီး Length-Field အစား Type Field ဆိုပြီးဖြစ်လာကာ ၎င်း Type Field ဟာ Ethernet SNAP တုန်းကလိုပဲ Frame ရဲ့ Data Section ဟာမည်သည့် Netwrok Protocol ကိုသုံးထားသလဲဖော်ပြတာဖြစ်ပါတယ်။

ပုံ ၈.၇



Ethernet II Frame ကိုတွေ့ရစဉ်

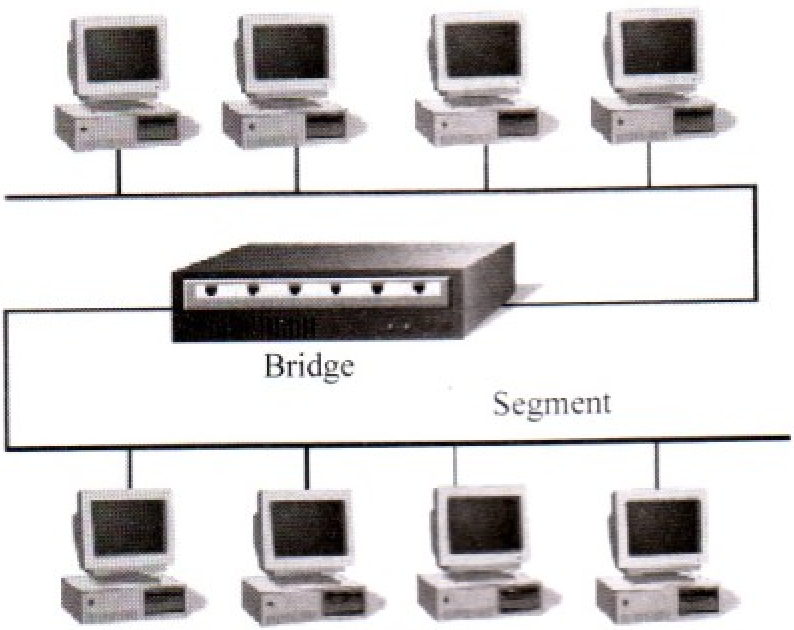
၈.၇ Segmentation အခြေခံ

ကွန်ရက်တစ်ခုမှာအသုံးပြုနေတဲ့ ကွန်ပျူတာအရေအတွက်များလာတာဟာ ကွန်ရက်ကိုနှေးကွေးစေပါတယ်။ ဒီပြဿနာကိုပြေလည်စေဖို့က ကွန်ရက်တွေကိုထိန်းချုပ်ရလွယ်ကူအောင် Segmenting အပိုင်းပိုင်းပိုင်းလိုက်တာပဲဖြစ်ပါတယ်။ ကွန်ရက်အပိုင်း (Segments) နှစ်ခုကို Bridge သို့မဟုတ် Router နှင့်ချိတ်ဆက်ပေးခြင်းအားဖြင့် ကျွန်တော်တို့တွေဟာ ကွန်ရက်လမ်းကြောင်းပိတ်ဆို့ခြင်းတွေကို လျော့ချနိုင်တဲ့အပြင်၊ ရည်ရွယ်ရာကိုလည်း တိုက်ရိုက်သွားနိုင်ပါတယ်။ ဘာလို့လည်းဆိုတော့ Segment လေးတွေခွဲလိုက်တဲ့အခါ Segment တစ်ခုအတွင်းမှာရှိတဲ့ ကွန်ပျူတာတွေဟာနည်းသွားတာကြောင့်ပါ။ ပုံ ၈.၈ ကိုလေ့လာကြည့်ပါ။

၈.၈ Token Ring ဆိုတာ

Token Ring ဆိုတဲ့ အထူးပြုလုပ်ထားတဲ့ Packet လေးကို တစ်ခုမှတစ်ခုသို့ ပေးပို့တဲ့နည်းပညာကို အသုံးပြုထားတာကတော့ Token Ring ဆိုတာပါပဲ။ Token Ring IEEE 802.5 Standard ဖြစ်ပါတယ်။ Note တိုင်းဟာ Multistation Access Unit (MSAU or MAU) လို့ခေါ်တဲ့ Concentrator မှာ ချိတ်ဆက်

ပုံ ၈.၈



Bridge ခံလိုက်ခြင်းဖြင့် ဝန်ကိုလျော့ကျသွားစေတယ်။

ထားရမှာဖြစ်ပါတယ်။ Token Ring မှာသုံးတဲ့ Network Card ဟာ 4 Mbps ဒါမှမဟုတ်၊ 6 Mbps နဲ့ အလုပ်လုပ်နိုင်ပါတယ်။ 4 Mbps သာအလုပ်လုပ်နိုင်တဲ့ Network Card တွေလည်းရှိပါတယ်။ သူတို့ကတော့ 4 Mbps ဆိုတဲ့အတိုင်းအတာနဲ့ပဲ အလုပ်လုပ်ပါတယ်။ ဒါပေမယ့် Network တစ်ခုလုံးမှာရှိတဲ့ Network Card တွေအားလုံးကတော့ တူညီတဲ့နှုန်းတစ်ခုနဲ့ပဲ အလုပ်လုပ်ကြမှာဖြစ်ပါတယ်။ Token Ring ဟာ Ring နည်းပညာနဲ့ Token တွေကို Station တစ်ခုမှတစ်ခုကို ပေးပို့နေတယ်ဆိုသော်ငြားလည်း တကယ်တမ်း Physically ထင်ထားတာက Star Topology ပါ။ ဒီနေရာမှာ Token Ring အလုပ်လုပ်ပုံနဲ့ ပတ်သက်လို့ ပြောပြပါအုံးမယ်။ Node တစ်ခုချင်းစီဟာ သူတို့ရဲ့အနီးဆုံး Node မှာ Token နဲ့ Data Frame ကိုရရှိကြပါတယ်။ အဲ့ဒီနောက် နောက် Node တစ်ခုကို Pass လုပ်ကြပြန်ပါတယ်။ ဒီတော့ Token တိုင်းဟာအနည်းဆုံးတော့ Ring တစ်ပတ်လည်ပါတယ်။ ပြီးမှ Original Node ကိုပြန်ရောက်ပါတယ်။ ပြောပြပါအုံးမယ်။ Ring Topology ထဲကကွန်ပျူတာတိုင်းဟာ အခြားကွန်ပျူတာနှစ်လုံးနဲ့ တိုက်ရိုက်ချိတ်ဆက်ထားပါတယ်။ ဒါမှ တစ်ခုကနောက်ကလိုက်လာပြီး တစ်ခုကရှေ့ကသွားနိုင်မှာဖြစ်ပါတယ်။

၈.၉ Token Ring Board Setting အကြောင်းသိကောင်းစရာ

Token Ring Network တွေဟာ Ethernet Network တွေလိုပါပဲ။ Card တစ်ခုချင်းစီရဲ့ Node/ Address တွေကို ထုတ်လုပ်တဲ့သူတွေကိုယ်တိုင်က Card မှာတခါတည်း Burn လုပ်ထားပြီးသားပါ။ ကြတော့လည်း ကိုယ့်ရဲ့အကြောင်းအရာနဲ့ မညီညွတ်ရင်တော့ Card ကိုရောင်းတဲ့သူက Supp Software နဲ့ ဒီ Node Address တွေကိုပြန်ပြုပြင်လို့ရပါတယ်။ Token Ring Network Card တွေဟာ

Node တစ်ခုမှာ အများဆုံးနှစ်ကဒ်စိုက်လို့ရပါတယ်။

၈.၁၀ Token Ring Cabling အကြောင်းသိကောင်းစရာ

Token Ring Cable ဟာ Client နဲ့ MSAU ကိုဆက်သွယ်ပေးရတာပါ။ အဲ့ဒီအပြင် MSAU အချင်းချင်း တစ်ခုမှတစ်ခုကို ဆက်သွယ်ပေးရပါသေးတယ်။ MSAU အချင်းချင်းဆက်သွယ်တဲ့ Cable ကိုတော့ Patch Cable လို့ခေါ်ပါတယ်။ များသောအားဖြင့် Patch Cable တွေဟာ IBM Type 6 Cable တွေဖြစ်ကြပါတယ်။

မှတ်ချက်။ ။ IBM Type 6 Cable ဆိုတာ Standard Copper Wire နှစ်ပင်လိမ်နှစ်စုံကို အပြင်က သံဇကာကွက်ပုံစံ Shield ကာထားတဲ့ ကြိုးတစ်မျိုးဖြစ်ပါတယ်။

MSAU တွေ IBM Token Ring Networks တွေရဲ့ Central Device တွေပဲဖြစ်ကြပါတယ်။ Token Ring Network တွေအတွက် IBM ကထုတ်ထားတဲ့ 8228 MSAU ဆိုတာရှိပါတယ်။ တကယ်တော့ သူလည်း Hub တစ်မျိုးပါပဲ။ ပုံမှာ 8228 MSAU ကိုအသုံးပြုပြီး Token Ring Cabling ကိုပြထားပါတယ်။ ဒီ 8228 MSAU တိုင်းမှာ Connector ဆယ်ခုတပ်လို့ရပါတယ်။ ကျန်တဲ့နှစ်ခုကတော့ Lable တပ်ထားတဲ့ အတိုင်း RI (Ring In) နဲ့ RO (Ring Out) ပဲဖြစ်ပါတယ်။ ဒီ RI နဲ့ RO Connectors တွေဟာ များပြားသော 8228 MSAU တွေကိုအသုံးပြုပြီး Network ကြီးတစ်ခု တပ်ဆင်နိုင်ရန်ဖြစ်ပါတယ်။ မျက်စိထဲမှာမြင်အောင် ကြည့်ကြည့်ပါ။ ဘယ်လောက်ပဲ 8228 MSAU များမှာ ပထမတစ်ခုရဲ့ RI က နောက်ဆုံးတစ်ခုရဲ့ RO မှာသွားချိတ်လိုက်ပါတယ်။ ကြားထဲက 8228 တွေကတော့ တစ်ခုက RO ဆို နောက်တစ်ခုက RI မှာပေါ့။

8228 တွေဟာ တကယ်တမ်းကြတော့ Mechanical Devices တွေလို့လဲ ပြောလို့ရပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ သူမှာ Relay တွေပါနေလို့ပါ။ ဒီ Relays တွေရဲ့ရည်ရွယ်ချက်ကတော့ Switch သဖွယ် In & Out လုပ်ဖို့အတွက်ပဲဖြစ်ပါတယ်။ Client User MSAU ကိုလာတဲ့ Voltage နဲ့အလုပ်လုပ်တဲ့ ဒီ Relay တွေဟာ Ports တစ်ခုချင်းစီကို Control လုပ်ထားပါတယ်။ 8228 ကိုပထမဦးဆုံး Setup လုပ်တဲ့အခါမှာတော့ သူနဲ့အတူပါလာတဲ့ Setup Tool ဆိုတာကိုအသုံးပြုပြီးတော့ Relay တွေကို (Initialized) အခြေအနေသတ်မှတ်ပေးရပါတယ်။ ဘယ်လိုလုပ်ရမလဲဆိုတော့ ဒီ Setup Tool လေးကို Port တစ်ခုချင်းစီမှာ လိုက်ထည့်ရမှာပါ။ Ports တစ်ခုထဲကို Setup Tool လေးထည့်လိုက်ပြီးရင် ခဏစောင့်၊ Post ဟာသေချာစွာ Initialized လုပ်ပြီးရင် Setup Tool လုပ်ပြီးရင် မီးလေးလင်းလာလိမ့်မယ်။ ပြီးရင် အဲ့ဒီအတိုင်းနောက် Port တစ်ခုကိုလုပ်ပါ။

IBM Token Ring Network တွေဟာ Connector နှစ်မျိုးအသုံးပြုကြပါတယ်။ တစ်ခုက 9-Pin D Connector ဖြစ်ပြီး နောက်တစ်ခုက IBM Data Connector ပဲဖြစ်ပါတယ်။ 9-Pin D Connec-

tor ကိုတော့ NIC ဘက်မှာတပ်ချိတ်ရမှာဖြစ်ပါတယ်။ IBM Data Connector ကတော့ MSAUs အိမ့်မဟုတ် Repeater တွေဘက်မှာ တပ်ဆင်ရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာ ဘယ်လိုအသုံးပြုတပ်ဆင်ရသလဲဆိုတာကို ပြောပြပါအုံးမယ်။

MSAU အိမ့်မဟုတ် Repeater အချင်းချင်း ဆက်သွယ်ဖို့အသုံးပြုတာ Patch Cable ပါ။ Patch Cable ဟာ အဆုံးနှစ်ဖက်စလုံးမှာ IBM Data Connector ရှိပါတယ်။

နောက်တစ်ခုကတော့ Token Ring Adapter Cables ပါ။ သူကတော့ တစ်ဖက်မှာ IBM Data Connector ဖြစ်ပြီး တစ်ဖက်က 9-Pin Connector ပါ။ ဒီ Adapter Cable တွေဟာ Client အိမ့်မဟုတ် Server တွေမှာရှိတဲ့ NIC ကနေ MSAU တွေဆီကို ဆက်သွယ်ဖို့ဖြစ်ပါတယ်။ အဲ့ဒီနေရာမှာ 9-Pin Connector က NIC မှာတပ်ရပြီး IBM Data Connector ကတော့ MAU တွေမှာတပ်ဆင်ရမှာဖြစ်ပါတယ်။

Token Ring Network တွေကိုမဆင်ခင်မှာ -

- ❖ ကြိုးတွေမဆင်ခင် MSAU နဲ့အတူပါလာတဲ့ Setup Tool ကိုအသုံးပြုပြီး Port တစ်ခုချင်းစီကို Initialize လုပ်ပေးပါ။
- ❖ MSAU ကိုတစ်ခုထက်ပိုသုံးရင် MSAU တိုင်းရဲ့ RO ကိုနောက် MSAU တိုင်းရဲ့ RI နဲ့ချိတ်ဆက်ဖို့ မမေ့ပါနဲ့။ အိမ့် Loop ဖြစ်ပြီး Ring ဖြစ်သွားမှာပါ။ Token Ring Network တွေမှာလည်း အမျိုးမျိုးသော စည်းကမ်းချက်တွေရှိလို့နေပြန်ပါတယ်။ ဒီအကြောင်းကိုပြောမယ်ဆိုရင်ဖြင့် Token Ring Cabling နဲ့ မတူညီတဲ့ System နှစ်ခုကိုအရင်ပြောပြရအုံးမှာဖြစ်ပါတယ်။ သူတို့ကတော့ Small Movable နဲ့ Large Non-Movable တို့ဖြစ်ကြပါတယ်။

Small Movable System အကြောင်းသိကောင်းစရာ

- ❖ သူကတော့ Clients နှင့် Server နှစ်ခုပေါင်းမှ (၉၆)ခုအထိပဲ ခွင့်ပြုပါတယ်။
- ❖ MSAU ကတော့ (၁၂) ခုထိရပါတယ်။
- ❖ Clients နှင့် Server နောက်ပြီး MSAU အိတွေကိုဆက်သွယ်ဖို့ Type 6 Cable ကိုအသုံးပြုပါတယ်။
- ❖ Cable ဟာ Flexible ဖြစ်ပါတယ်။ ပျော့ပျောင်းပြီး ကွေးကောက်လို့ရတယ်ပေါ့ဗျာ။ အိပေမယ့် အကွာအဝေးကတော့ ကန့်သတ်ချက်ရှိပါတယ်။ အိကြောင့်မို့ Small Network တွေနဲ့ပဲ အဆင်ပြေပါတယ်။
- ❖ MSAU နှစ်ခုကြားဆက်သွယ်ထားတဲ့ Patch Cable ဟာအနည်းဆုံး ၈ပေရှိရပါမယ်။ အများဆုံး ပေ (၁၅၀) ထက်မပိုရပါဘူး။ များသောအားဖြင့် Patch Cable တွေဟာ 8, 30, 75 နှင့် (၁၅၀)ဆိုတဲ့

အလျား တွေနဲ့လာတတ်ကြပါတယ်။

❖ MSAU တွေအားလုံးကိုချိတ်ဆက်ထားတဲ့ Patch Cable ရဲ့ အများဆုံးသောအလျားဟာ ပေ(၄၀၀) ထက်မပိုရပါဘူး။

❖ MSAU နဲ့ Node တို့ချိတ်ဆက်တဲ့ Adapter Cable ကတော့ အများဆုံးသောအလျားပေ (၁၅၀) ထက်မပိုရပါဘူး။

Large Non-Movable System အကြောင်းသိထောင်းစရာ

Small Movable System နဲ့ကွာခြားသွားတာကတော့
အများဆုံး (၂၆၀) Nodes ရပါတယ်။
MSAU ကတော့ (၃၆) ခုပါ။
Type-1 သို့မဟုတ် Type-2 Cable ကိုအသုံးပြုရပါတယ်။

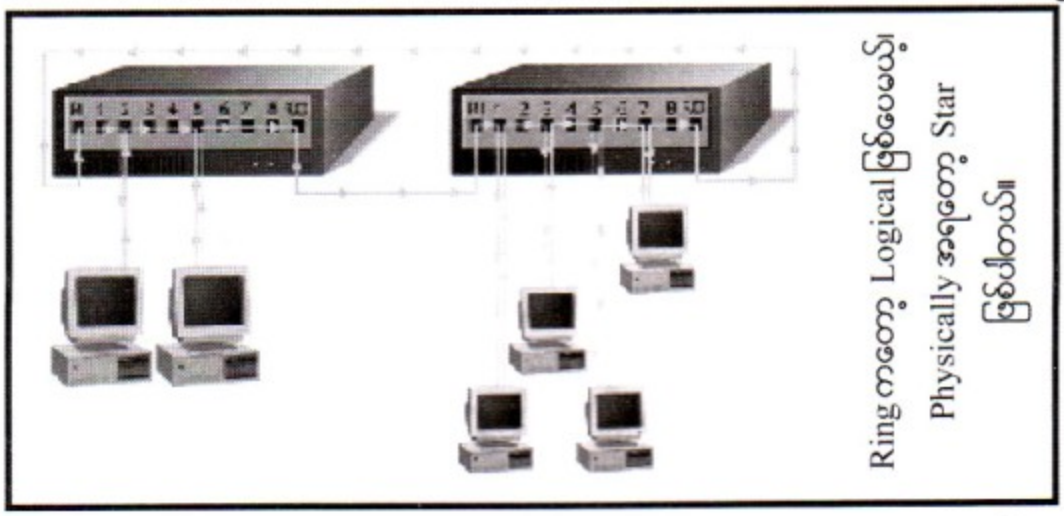
မှတ်ချက်။ ။ IBM Type-1 Cable ဆိုတာ Type-6 Cable လိုအပြင်က Shield နဲ့ပဲဖြစ်ပါတယ်။ အဲပေမယ့် သူကအထဲမှာ လိမ်ထားတဲ့ကြိုးနှစ်စုံက Type-6 လို Standard Copper Wire မဟုတ်ပါဘူး။ Solid Copper Wire ဖြစ်ပါတယ်။

IBM Type-2 Cable ဆိုတာ STP လိမ်ထားသောကြိုးနှစ်စုံနဲ့ Telephone System အတွက် လိမ်ထားသောကြိုး ၄စုံ၊ အားလုံးလိမ်ထားသော ကြိုး ၆စုံ နဲ့ဖြစ်ပါတယ်။

Token Ring Network တွေဟာ UTP Cable ကိုလည်းအသုံးပြုချင်ရင် သုံးလို့ရပါတယ်။ ဒီ UTP Cable ကိုတော့ IBM Type-3 Cable လို့ခေါ်ပါတယ်။ IEEE 802.5 အရဆိုရင် Token Ring တွေ အသုံးပြုတဲ့ UTP Cable ဟာ 4 Mbps ပါ။ အဲပေမယ့် လက်ရှိ Token Ring တွေမှာအသုံးပြုနေတဲ့ Level 5 UTP Cable ဟာဆိုရင်ဖြင့် 16 Mbps ဖြစ်ပါတယ်။

UTP Cable ကို Token Ring မှာအသုံးပြုမယ်ဆိုရင်တော့ သင်သိရမှာက Media Filter ကိုအသုံးပြုရမယ်ဆိုတာပါပဲ။ ဘာကြောင့်လဲဆိုတော့ Token Ring NIC တွေမှာပါတဲ့ Port က UTP မဟုတ်ဘူးလေ။ RJ-45 Port မှရမှာပေါ့။ ဒီတော့ NIC နဲ့ UTP အကြားဆက်သွယ်ဖို့ Media Filter လိုပါတယ်။ ရှေ့က သင်ခန်းစာမှာ Media Filter အကြောင်းပြောပြထားပါသေးတယ်။ အဲပေမယ့်လည်း နောက်ပိုင်းလာတဲ့ Token Ring NIC အသစ်တွေကတော့ Built-in Media Filter ပါပြီးသားမို့ UTP Cabling အတွက် RJ-45 Port အဆင်သင့်ဖြစ်ပါတယ်။

ပုံ ၈.၉



၈.၁၁ Beaconing ဆိုတာ

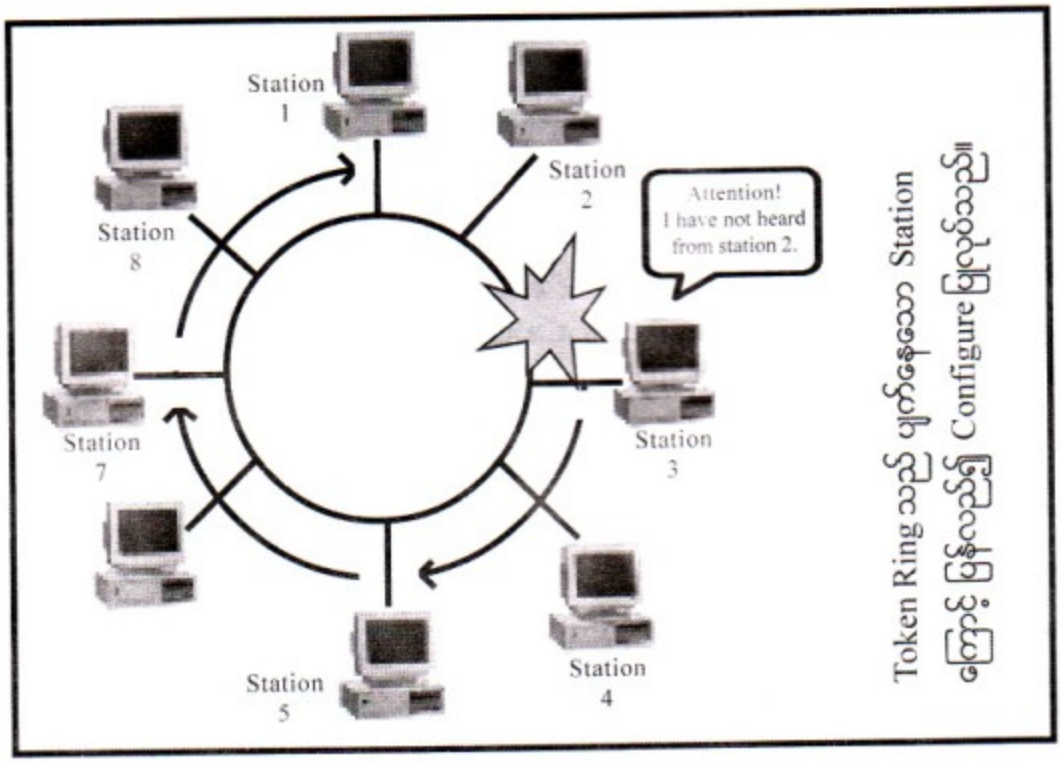
Token Ring Architecture မှာ အခြား Architecture တွေနှင့်မတူညီဘဲထူးခြားတာလေးက ပြဿနာ Faults တွေကိုသိနိုင်ခြားဘေးဖယ် ပေးထားနိုင်ခြင်းပါပဲ။ ၎င်းဖြစ်စဉ်ကို Beaconing လို့ခေါ်ပါတယ်။ Token Ring ထဲမှာရှိတဲ့ ကွန်ပျူတာတွေထဲက ပထမဦးဆုံး Power ဖွင့်လိုက်တဲ့ ကွန်ပျူတာ Ring မှာ Data တွေကောင်းမွန်စွာသွားလာနိုင်ခြင်းရှိမရှိကို စစ်ဆေးပေးတဲ့သူဖြစ်လာပါတယ်။ ၎င်းကွန်ပျူတာကို Active Monitor လို့ခေါ်ပြီး ၎င်းဟာ Beaconing Process ကိုထိန်းချုပ်ရပါတယ်။ ကွန်ရက်မှာရှိတဲ့ အခြားသော ကွန်ပျူတာတွေကတော့ Standby Monitors လို့ခေါ်ပါတယ်။

ကဲ ဆက်ရအောင်။ ခုနစ်စက္ကန့်ကြာတဲ့အချိန်တိုင်းမှာ Active Monitor ဟာသူ့အောက်ကပ်လျက် ကွန်ပျူတာကို အထူးပြုလုပ်ထားတဲ့ Packet လေးတစ်ခုပို့လိုက်ပါတယ်။ အဲ့ဒီ Packet လေးထဲမှာ အခု Packet လေးကိုပို့လိုက်တဲ့သူက မင်းရဲ့အထက်ကကွန်ပျူတာပါ။ Active Monitor ဖြစ်ပါတယ်။ လိပ်စာကတော့ ဒီလောက်ဖြစ်ပါတယ်။ ပြန်ပြောမယ်နော်။ Active Monitor ကသူ့အောက်က ကွန်ပျူတာကို သူ Active Monitor ဖြစ်ကြောင်း သူ့ Address နှင့်အတူ မင်းရဲ့အပေါ်ကကွန်ပျူတာဖြစ်ကြောင်းစာလွှာပါးလိုက်တယ်ပေါ့ဗျာ။ ကျွန်တော်တို့ Token Ring ကိုမျက်စိထဲမြင်အောင်ပြောရရင် ပျော်ပွဲစားထွက်တဲ့အခါ ပါဆယ်ဂိမ်းဆော့သလိုပဲ။ အားလုံးပတ်လည်ထိုင်ပြီး အထုပ်တစ်ထုပ်ကို Pass လုပ်ရတယ်မဟုတ်လား။ ဒီတော့ ကိုယ့်ရဲ့ လက်ဝဲဘက်က အောက်အိမ်ပေါ့ဗျာ။ Token Ring စကားနှင့်ပြောရင် NADN (Nearest Active Downstream Neighbour) လို့ခေါ်ပါတယ်။ လက်ယာဖက်အိမ်က အပေါ်အိမ်ပေါ့ဗျာ။ Token Ring အရင်းကို NAUN (Nearest Active Upstream Neighbour) လို့ခေါ်ပါတယ်။ ကဲ Active Monitor ရဲ့အောက်ဖက်က NADN ကတော့ Packet လေးကိုရသွားပြီး ၎င်းက Packet လေးကိုစစ်ဆေးလိုက်ပြီး ခုနကလိပ်စာနေရာမှာ သူ့လိပ်စာပြင်လိုက်ပြီး သူ့အောက်က NADN ကိုတစ်ခါ Pass လုပ်ပြန်ပါတယ်။ အဲ့ဒီမှာပါတဲ့ Address ကသူ့ရဲ့ Address ဖြစ်တာကြောင့် သူ့အောက်ကသူ ပို့လိုက်တဲ့ Packet ကိုရတဲ့

NADN ဖက်ကပြန်ကြည့်ရင် ၎င်း Address ဟာလက်ခံရရှိသူ ကွန်ပျူတာရဲ့ အပေါ်ဖက်က NAUN Address ဖြစ်နေပါလိမ့်မယ် ဒီလိုနဲ့ အခုဖြစ်စဉ်မှာ တတိယမြောက်ကွန်ပျူတာဟာ တစ်ခါ Packet ကိုစစ်ဆေးပါတယ်။ သူ့အပေါ်က NAUN ရဲ့ Address ကဘာလဲ။ Active Monitor ရဲ့ Address ကဘာလဲပေါ့။ ဒီလိုပဲ သူကလည်း သူ့အပေါ်ကလာတဲ့ NAUN Address မှာ သူ့လိပ်စာထည့်ပြီးတော့ NADN ကိုပို့လိုက်ပြန်ပါတယ်။ ဒီတော့ Packet လေးမှာ ပို့လိုက်တဲ့ကွန်ပျူတာရဲ့ Address နဲ့ Beconing ကို Manage လုပ်တဲ့ Active Monitor ရဲ့ Address က အမြဲပါနေပါလိမ့်မယ်။

ဒီလိုနဲ့ ၎င်း Packet ဟာ Active Monitor ကိုပြန်ရောက်တဲ့အချိန် Active Monitor ကသိလိုက်ပြီး OK တယ်ပေါ့။ Ring ဟာ တစ်ပတ်လည်နိုင်တယ်ပေါ့ဗျာ။ နောက်တစ်ခုက Station တိုင်းဟာ ၎င်းတို့အထက်က NAUN Address တွေကိုသိသွားကြတာပေါ့။ အကယ်၍များ Station တစ်ခုဟာ သူ့အပေါ်က Packet ကို ခုနစ်စက္ကန့်ကြာလို့မမရရင် ဒါဆက်သွယ်ရေးပျက်တောက်ပြီ။ တစ်ခုခုကြောင့်ပေါ့။ အဲ ဗိုလ်လိုပြောရရင်တော့ Something Wrong ပြီပေါ့ဗျာ။ ဒီတော့ သူက သူ့လိပ်စာပါတဲ့ Packet ကို ပို့လိုက်ပါတယ်။ နောက်ပြီး အဲ့ဒီ Packet မှာ သူ့အပေါ်က NAUN Address လည်းပါတယ်ပေါ့ဗျာ။ အဲ့ဒီ Station ကို Beacon အဖြစ်သတ်မှတ်လိုက်ပါတယ်။ ဒီ Packet ကိုရတဲ့ Station တိုင်းဟာ အခု ဘယ်သူ့ပြဿနာဖြစ်နေလည်းဆိုတာကိုသိရှိသွားကြပါပြီ။ ဒီနည်းနှင့် ခုနစ်စက္ကန့်ကြာတိုင်းမှာ မိမိအပေါ်အိမ် NAUN က Packet မရတိုင်း Ring ကိုပြန်ပြီး Reconfigure လုပ်ကြပါတယ်။ ဒီလိုနှင့် ပြဿနာဖြစ်တဲ့နေရာကိုရှောင်ကြပါတယ်။ ဒီနည်းဟာ Automatic Fault Tolerance ဖြစ်ပါတယ်။ ဒီနည်းဟာ Network Architecture အများစုမှာတောင် မရှိတဲ့နည်းပညာဖြစ်ပါတယ်။

ပုံ ၈.၁၀



IBM Token Ring Cabling နှင့်တစ်ဖက်မှာ Token Ring အနှစ်ချုပ်ကိုလေ့လာကြည့်ပါဦး။

Cable Type	Description
Type - 1	STP with two pairs of 22-AWG solid copper wire surrounded by a braided shield and casing. This cable is used to connect computers to MAUs and can be run through conduit or inside walls.
Type - 2	STP with two pairs of 22-AWG solid copper wire for data and four pairs of 26-AWG wire for voice. Used to connect both data and voice without running two cables.
Type - 3	UTP voice-graded cable with 22 AWG or 24 AWG, each pair twisted twice every 3.6 meters (12 feet). Cheaper alternative to Type-1, but limited to 4Mbps.
Type - 5	Fiber-Optic cable, 62.5 or 100-micron diameter, used for linking MAUs over distance.
Type - 6	STP Cable with two twisted paris of 26-AWG standard wire surrounded by braided shield and casing. Similar to Type - 1, except that the standed wire allowsgreater flexibility bus less distance (two-thirds that of Type-1). Gener ally used as a patch cable or forextensions in wiring closets.
Type - 8	STP cable for used under carpets. Similar to Type - 6, except it is flat.
Type - 9	Plenum-rated Type - 6 cable.

၈.၁၂ AppleTalk အဓိကြောင်း

၁၉၈၃ ခုနှစ်မှ ပထမဆုံးစတင်မိတ်ဆက်ခဲ့ပါတယ်။ Apple Computer Inc က ၎င်းရဲ့ Macintosh ကွန်ရက်တွေမှာအသုံးပြုဖို့ AppleTalk Architecture ကိုဒီဇိုင်းဆွဲထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ AppleTalk ဟာရိုးရှင်းတယ်။ အသုံးပြုရတာလည်းလွယ်ကူတဲ့ နည်းပညာဖြစ်ပါတယ်။ Macintosh ကွန်ပျူတာတွေမှာ Network Interface ဟာ Built-in ပါလာပြီးသားဖြစ်တာကြောင့် ကွန်ရက်ဆင်မယ်ဆို Cable ကြိုး တခါတည်း Network Port မှာတန်းတက်လာရုံပါပဲ။ AppleTalk ကွန်ရက်ဟာ Macintosh Environment တွေမှာရေပန်းစားတဲ့ Network ဖြစ်ပါတယ်။ တကယ်တော့ AppleTalk ဆိုတာ Networking Protocol ကိုပြောတာဖြစ်ပြီး ၁၉၈၉ မှာ Apple ဟာ AppleTalk ရဲ့ Definition ကို Protocol အနေနှင့်သာ မဟုတ်ဘဲ Network Architecture တစ်ခုလုံးပေါ်မှာ သက်ရောက်စေခဲ့ပြီး Cabling System ကိုပါရည်ညွှန်း တဲ့ Local Talk ဆိုတဲ့ Term ကိုပါထပ်ထည့်ခဲ့ပါတယ်။

Category	Token Ring Summary
IEEE Specification	802.5
Advantages	Fast and reliable
Disadvantage	More expensive than ethernet; difficult to troubleshoot
Topology	Ring; cabled as star
Cable Type	IBM cable types (STP and UTP)
Channel access method	Token passing
Maximum cable segment length	45 meters (150 feet)-UTP 101 meters (330 feet)-STP
Maximum number of segment	33 hubs
Maximum devices per segment	Depends on hub
Maximum devices per network	72 with UTP, 260 with STP
Transmission speed	4 Mbps or 16 Mbps

AppleTalk ဟာပစ္စည်းတစ်ခုရဲ့ Address ကိုသတ်မှတ်ရာမှာ တရားသေမဟုတ်သော Dynamic နည်းကိုအသုံးပြုတယ်။ ကွန်ပျူတာက Power ဖွင့်လိုက်တဲ့အခါ သူဟာ Address တစ်ခုကိုသူ့ဘာသာသူ ရွေးချယ်လိုက်ပါတယ်။ ပုံမှန်အားဖြင့်တော့ နောက်ဆုံးသုံးခဲ့သော Address ကိုပဲပြန်သုံးတတ်ပါတယ်။ ပြီးလည်း ပြီးရော အဲဒီ Address ကို Network မှာသုံးထားသလား။ မသုံးထားဘူးလားသိချင်လို့ သူဟာ Broadcast လုပ်လိုက်ပါတယ်။ အကယ်၍များ အဲဒီ Address ဟာဘယ်သူမှ ယူမသုံးထားဘူးဆိုရင် ၎င်းဟာ အဲဒီ Address ဖြင့် Data တွေကို Transmit လုပ်ပါတယ်။ အကယ်၍များ အဲဒီ Address ဟာမလွတ်ဘူး။ ပစ္စည်းတစ်ခုခုကယူသုံးထားတယ်ဆိုရင် (အဲဒီ Network မှာပေါ့နော်) ၎င်းကွန်ပျူတာဟာ နောက်ထပ် Address တစ်ခုခုကို ကျဘမ်း (Random) ယူပြီး Network ကို Broadcast လုပ်ပြန်ပါတယ်။ ဒီလိုနဲ့ပဲ ဘယ်သူမှ သုံးမထားတဲ့ Address မရမချင်း ကွန်ပျူတာကနံပါတ် Address တစ်ခုရွေးလိုက် Braodcast လုပ်လိုက်နှင့် လုပ်နေပါတော့မယ်။

ကဲထားပါတော့ AppleTalk နှင့်ပတ်သက်ပြီး ထပ်ပြောပြစရာတွေရှိသေးတယ်။ ဒီ AppleTalk မူရင်း Version ကြီးကို AppleTalk Phase 1 လို့ခေါ်ပြီး Network တစ်ခုမှာ ကွန်ပျူတာ ၃၂ လုံးချိတ်ဆက်နိုင်ပါတယ်။ Hubs တွေ Repeater တွေနှင့်ချိတ်ဆက်လိုက်မယ်ဆိုရင်တော့ ကွန်ပျူတာအရေအတွက်ဟာ 254 အထိတိုးလာနိုင်ပါတယ်။

၁၉၈၉ မှာတော့ Apple ဟာ AppleTalk Phase 2 ကိုစတင်မိတ်ဆက်ခဲ့ပြီး EtherTalk နှင့် TokenTalk ကိုပါမိတ်ဆက်ခဲ့ပါတယ်။ ၎င်းဟာ AppleTalk Protocol ကို Ethernet ကွန်ရက်ပေါ်မှာရော

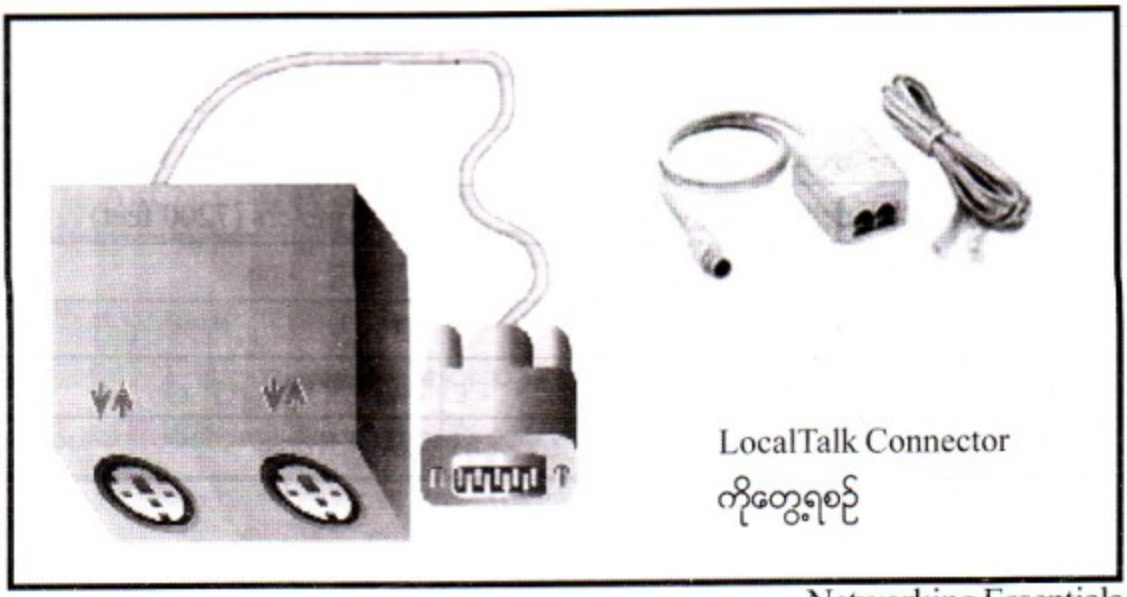
Token Ring ကွန်ရက်ပေါ်မှာရော အသီးသီးအလုပ်လုပ်စေနိုင်ပါတယ်။ ဒီမှာတစ်ခုသတိထားစရာရှိပါတယ်။ AppleTalk Phase 2 ဟာ LocalTalk Network အနေနှင့်သုံးမယ်ဆိုရင်တော့ ကွန်ပျူတာဟာ ခုနက ပြောခဲ့သလိုအများဆုံး 254 အထိပဲရှိမှာဖြစ်ပါတယ်။ ကဲ ကဲ ကိန်းဂဏန်းတွေသုံးပြီး အတိအကျပြန်ပြောရရင် AppleTalk Phase 2 ဟာ Local Talk နှင့်ဆိုရင် ကွန်ပျူတာကိုအများဆုံး 254 လုံး၊ EtherTalk နှင့်ဆိုရင် 1024 လုံး၊ UTP ကိုသုံးထားတဲ့ TokenTalk ဆိုရင် 72 လုံး၊ STP ကိုသုံးထားတဲ့ TokenTalk နှင့်ဆိုရင် 260 လုံးထိရပါတယ်။ ၁၉၉၆ နောက်ပိုင်း Macintoshes Version အသစ်တွေမှာတော့ Local Talk ထက် Ethernet Interface ကိုပိုပြီး Support လုပ်လာကြပါတယ်။

၈.၁၃ LocalTalk အကြောင်း

Apple ကွန်ပျူတာကော်ပိုရေးရှင်းဟာ Bus Topology နှင့် STP Cable ကိုအသုံးပြုထားသော LoaclTalk Network Architecture ကိုဒီဇိုင်းဆွဲ ထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ ရုံးခန်းငယ်နှင့်အိမ်တွေမှာ Data တွေဆက်စပ်ပစ္စည်းတွေဖလှယ်ဖို့ပေါ့ဗျာ။ ပုံမှာမြင်တဲ့အတိုင်းပေါ့ဗျာ။ LocalTalk Connector မှာ ချိတ်ဆက်ဖို့ Connector (၃) ခုရှိပါတယ်။ တစ်ခုကကွန်ပျူတာမှာတပ်ဖို့ နောက်တူညီတဲ့ အပေါက်နှစ်ခုက ပစ္စည်းတွေကိုချိတ်ဆက်ဖို့ ဖြစ်ပါတယ်၊ LocalTalk က Bus Topology လို့သာပြောတာဗျ။ တကယ်တမ်းကြတော့ Network က Tree Sturcture ပုံစံကြီးဖြစ်နေတယ်ဗျ။

LocalTalk ဟာ CSMA/CA Channel Access Method ကိုအသုံးပြုပါတယ်။ ကျွန်တော်ပြီးခဲ့တဲ့ သင်ခန်းစာမှာ CSMA/CA အကြောင်းကိုရှင်းပြခဲ့ပြီးပါပြီ။ အဲ့ဒီတုန်းကလည်း CSMA/CA က Collission ကိုရှောင်ရှားနိုင်ပေမယ့် နှေးကွေးတယ်ဆိုတဲ့အကြောင်းကို Apple Network မှာသုံးတဲ့အကြောင်းရှင်းပြခဲ့ ဖူးပြီးပါပြီ။ LocalTalk Network တွေရဲ့အများဆုံး Transmission Speed က 230.4 Kbps အထိပဲရှိနိုင်ပါတယ်။

ပုံ ၈.၁၁



LocalTalk Connector ကိုတွေ့ရစဉ်

၈.၁၄ Ethernet နှင့် Token Talk အခြားခြင်း

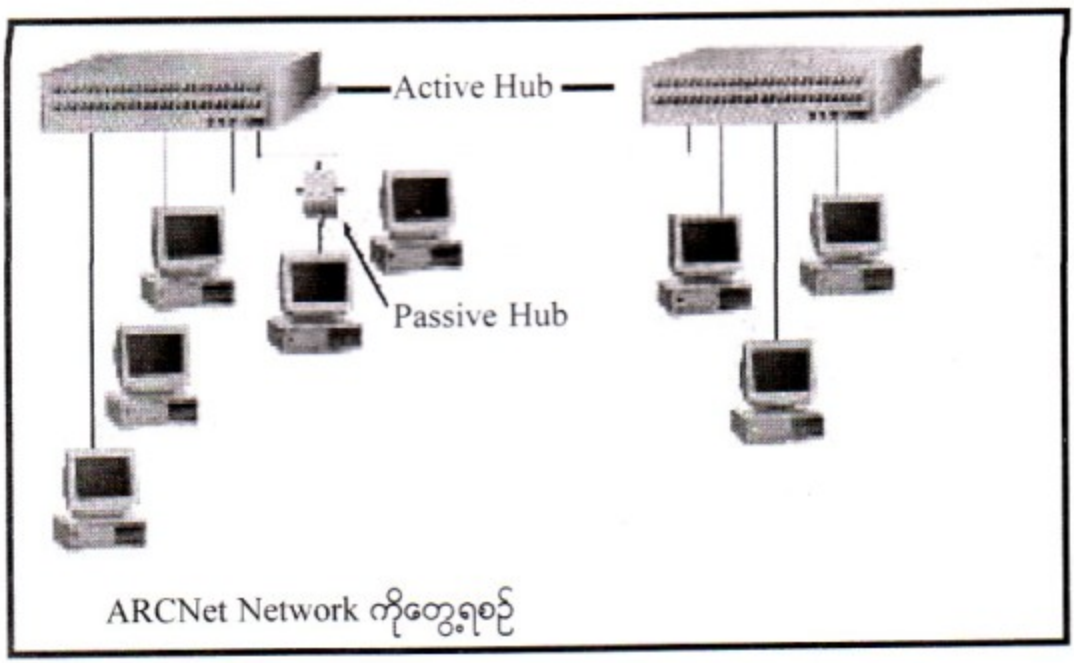
Local Talk ရဲ့ Speed ကနှေးသတ်ချက်ကိုကျော်လွန်စေခြင်းငှာ Apple ဟာ Ethernet နှင့် Token Talk ကိုဖန်တီးခဲ့ပါတယ်။ Ethernet ဆိုတာ Apple Talk Protocol ပါပဲ။ အဲပေမယ့် ၎င်းဟာ 10 Mbps ရှိတဲ့ IEEE 802.3 Ethernet ကွန်ရက်မှာအလုပ်လုပ်တာဖြစ်ပါတယ်။ ထို့အတူ Token Talk ဆိုတာဟာလည်း 4 or 6 Mbps ရတဲ့ IEEE 802.5 Token Ring Network ပေါ်မှာအလုပ်လုပ်တာဖြစ်ပါတယ်။ ၎င်း Protocol နှစ်ခုစလုံးဟာ Apple Talk Phase 2 ကို Support လုပ်ပြီးသူတို့ကိုအသုံးပြုမယ့် Network Card ဟာ EtherTalk အတွက်ရော၊ Token Talk အတွက်ပါလိုအပ်တဲ့ Driver နှင့် Protocol တွေအသီးသီးပါရှိရပါမယ်။ အဲ့ဒီအပြင် Macintosh Computer က ဒီ PC EtherNet နှင့် Token Ring Network တွေကို ချိတ်ဆက်နိုင်ရန်အတွက် Software ပါရှိရပါသေးတယ်။ ၁၉၉၆ နောက်ပိုင်းမှာတော့ Apple ကွန်ပျူတာတွေမှာ EtherNet Interface တွေ တစ်ခါတည်းပါလာအောင် ထုတ်လုပ်ခဲ့ပါတယ်။ သို့တည်းမဟုတ် EtherNet ဖြစ်စေ၊ Token Ring ဖြစ်စေ ၎င်း ကွန်ပျူတာမှာတပ်လိုကလည်း ဈေးအနည်းဆုံးနဲ့ တပ်နိုင်အောင် Apple ကစီစဉ်ခဲ့ပါတယ်။ အောက်မှာ Local Talk နှင့်ပတ်သက်တဲ့ အချက်အလက်တွေပါရှိပါတယ်။ လေ့လာကြည့်ပါအုံး။

Category	Specification
IEEE Specification	None
Advantages	Very Simple; easy to configure
Disadvantage	Slow
Topology	Bus
Cable Type	STP
Channel access method	CSMA/CD
Transceiver location	Connected to cable at vampire tap
Maximum cable segment length	300 meters (1000 feet)
Maximum overall network length	2400 meters (7200 feet)
Maximum number of segment	8
Maximum devices per segment	32
Maximum devices per network	254
Transmission speed	230.4 Kbps

၈.၁၅ ARCnet အကြောင်းသိကောင်းစရာ

Attached Resource Computer Netowrk ဆိုတဲ့ (ARCnet) ကို Data Point ကော်ပိုရေးရှင်းက 1972 ခုနှစ်မှစတင်မိတ်ဆက်ခဲ့ပါတယ်။ ၎င်းဟာ Data ပို့ခြင်းအတွက် Token Passing Channel Access Method ကိုအသုံးပြုပြီး Transmission Speed ကတော့ 2.5 Mbps အထိရပါတယ်။ Token Ring လိုပါပဲ။ ARCnet ဟာတကယ်တမ်းလက်တွေ့မှာပါ ဝါယာကြိုးတွေကို Bus သို့မဟုတ် Star Topology အတိုင်း တပ်ဆင်ရပြီးတော့ Virtually သာ Ring ဖြစ်ပါတယ်။ ARCnet ဟာ UTP နှင့်ဖြစ်စေ Coaxial Cable နှင့်ဖြစ်စေ Fiber Optic Cable နှင့်ဖြစ်စေအလုပ်လုပ်နိုင်ပါတယ်။ ARCnet ရဲ့ Data Transmission ဟာ EtherNet ရဲ့ Data Transmission လိုပါပဲ။ Data ဟာ Network ကြီးတစ်ခုလုံးအထိ ပျံနှံ့အောင် လွှင့်ထုတ်လိုက်ပါတယ်။ ကွန်ပျူတာတစ်လုံးချင်းစီဟာ သူတို့နှင့်သက်ဆိုင်ရာလိပ်စာပါတဲ့ Data ကိုပဲရယူကြပြီး Network အတွင်းရှိကိုယ်နှင့်မသက်ဆိုင်သော Data များကိုလျစ်လျူရှုလိုက်ပါတယ်။ ARCnet ဟာ Token Passing Channel Access Method ကိုအသုံးပြုထားသော်လည်း ARCnet အတွင်းက Hub နှင့်ဝါယာကြိုးချိတ်ဆက်ထားပုံက Token Ring Network ၏ Local Ring နှင့်မတူဘဲ EtherNet ၏ Star Topology ပုံစံနှင့်ဆင်တူနေပါတယ်။

ပုံ ၈.၁၂



ARCNet Network ကိုတွေ့ရစဉ်

ARCNet မှာအသုံးပြုတဲ့ Token Ring Method ဟာ Token Ring မှာအသုံးပြုတဲ့ Token Passing Method နှင့်ကွဲပြားခြားနားမှုရှိပါတယ်။ ပြီးခဲ့တဲ့သင်ခန်းစာမှာပြောခဲ့ပြီးတဲ့အတိုင်းပါပဲ။ Token Ring Network မှာအထူးပြုလုပ်ထားတဲ့ Token လေးကို ကွန်ပျူတာတစ်လုံးမှတစ်လုံးဆီသို့ ပေးပို့လိုက်ပါတယ်။ အံပေမယ့် ARCNet မှာတော့ ဒီလိုမဟုတ်ဘူးဗျ။ Token လေးကိုကွန်ပျူတာတစ်လုံးကနေ နောက်ထပ်

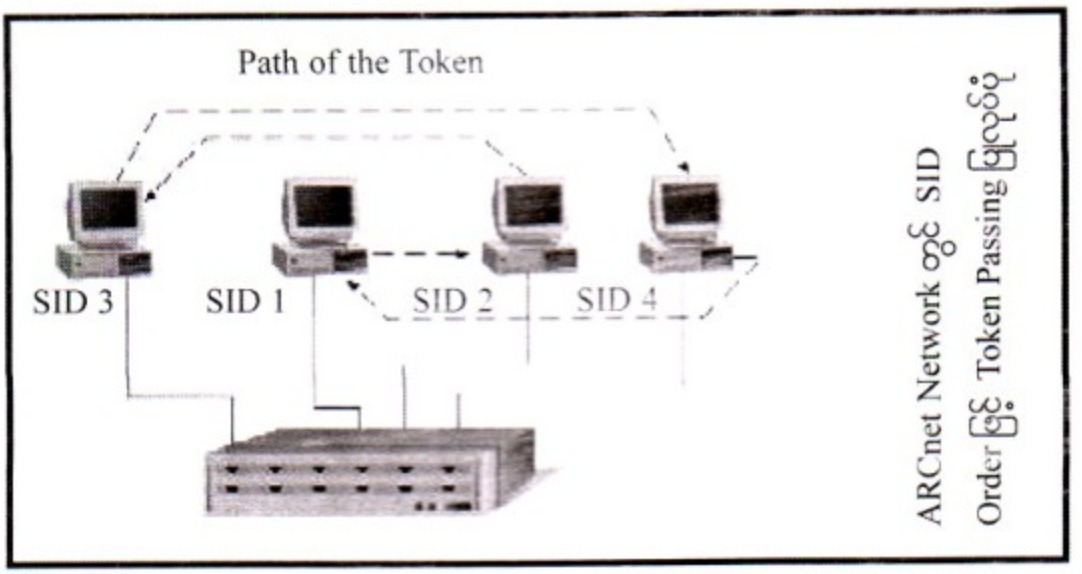
ကပ်လျက်တစ်လုံးဆီကို ပေးပို့တာမဟုတ်ဘဲ SID လို့ခေါ်တဲ့ Station Identifiers ပေါ်အခြေခံပြီး ကွန်ပျူတာ တစ်လုံးနဲ့တစ်လုံးကြား Token လေးကိုပေးပို့တာဖြစ်ပါတယ်။ ပြန်ရှင်းပြပါအုံးမယ်။ Token Ring မှာအသုံးပြုတဲ့ Token Passing Method ဆိုတာအထူးပြုလုပ်ထားတဲ့ Token လေးကိုကွန်ပျူတာတစ်လုံးမှ နောက်တစ်လုံးဆီသို့ဆင့်ကဲ ဆင့်ကဲပေးပို့သွားတာဖြစ်ပါတယ်။ ကျွန်တော်တို့ပါဆယ်ဂိမ်းဆော့သလိုပေါ့။ ARCNet မှာသုံးတဲ့ Token Passing Method ကြတော့ Token လေးကိုကွန်ပျူတာတစ်လုံးမှတစ်လုံးသို့ အစဉ်လိုက်အတိုင်း ပါဆယ်ဂိမ်းဆော့သလိုပေးပို့ခြင်းမဟုတ်ဘဲ SID ပေါ်မူတည်ပြီးပေးပို့သွားတာဖြစ်ပါတယ်။ ARCNet ရဲ့ Network Card တွေဟာဂင်းတို့ရဲ့ Address ကို Ethernet နှင့် Token Ring Network Card တွေလို Burred လုပ်ထားခြင်းမရှိပါဘူး။ ဒီတော့ကွန်ပျူတာတစ်လုံးချင်းစီမှာရှိတဲ့ Network တွေရဲ့ SID ကို ၎င်း Network Card ပေါ်မှာရှိတဲ့ DIP Switch တွေနှင့်သတ်မှတ်ပေးရတာဖြစ်ပါတယ်။ ARCNetwork Card တွေဟာကွန်ပျူတာမှာ တပ်ဆင်လိုက်တာနဲ့ ဒီ DIP Switch တွေကိုအသုံးပြုပြီး ၎င်းကွန်ပျူတာအတွက် SID ကိုသတ်မှတ်ပေးရပါတယ်။ Switch ဟာ (၁) ကနေမှ ၂၅၅ အထိပေးလို့ရပါတယ်။ အဲ့ဒီတော့ Network မှာ Token ဟာ SID 1 လို့သတ်မှတ်ထားတဲ့ ကွန်ပျူတာကနေမှတဆင့် SID 2 လို့သတ်မှတ်ထားတဲ့ ကွန်ပျူတာဆီကိုသွားပါတယ်။ ၎င်းကတဆင့် SID 3 လို့သတ်မှတ်ထားတဲ့ကွန်ပျူတာဆီကို သွားပါတယ်။ အဲ့ဒီလိုနဲ့ ဆင့်ကဲဆင့်ကဲသွားတယ်ပေါ့ဗျာ။ အဲဒီ Network မှာကွန်ပျူတာဘယ်နှစ်လုံးပဲရှိရှိ နောက်ဆုံးကွန်ပျူတာ ရဲ့ SID ကတော့ 255 ဖြစ်ရမှာဖြစ်ပါတယ်။ ဒီနောက်ဆုံး ကွန်ပျူတာက Token ကိုရရှိပြီးတဲ့အခါမှာ သူကနေမှ SID 1 ကွန်ပျူတာသို့ Token ကိုပြန်ပို့လိုက်ပါတယ်။ အဲ့ဒီလိုနဲ့ Token ဟာလည်ပတ်နေပါတယ်။

မှတ်ချက်။ ။ SID ဆိုတာ ဒီ ARCNet မှာတော့ Station Identifier လို့ဆိုလိုပေမယ့်လည်း Microsoft Windows Network မှာတော့ SID ဆိုတာ Security Identifier လို့ဆိုလိုပါတယ်။ ကျွန်တော် ရေးသားခဲ့ပြီးသော Microsoft Windows Server 2003 in Detail စာအုပ်မှာဖော်ပြခဲ့ပြီးဖြစ်ပါတယ်။

Token ကိုဆင့်ကဲဆင့်ကဲပေးပို့ဖို့ရာ လက်ရှိ Station ကနေကြည့်မယ်ဆိုရင် နောက် Station ရဲ့ SID ကိုတော့ Net Station Identifier (NID) လို့ခေါ်ပါတယ်။ ကွန်ရက်ဟာစတင်တဲ့အချိန်မှာဖြစ်စေ (ဒီနေ့ဖို့အလုပ်စလုပ်တယ်ပေါ့ဗျာ) ဒါမှမဟုတ်ကွန်ရက်ထဲကို ကွန်ပျူတာတွေထပ်တိုးတဲ့အခါမှာဖြစ်စေ ကွန်ရက်ဟာပြန်လည်ပြီးတော့ Configuration လုပ်ပါတယ်။ အနိမ့်ဆုံးသော SID ကိုပိုင်ဆိုင်ထားတဲ့ (ဥပမာ SID 1) ကွန်ပျူတာဟာ Token ကိုစတင်ပို့ဆောင်ပြီးတော့ Station တွေဟာကွန်ရက်မှာသူတို့ရဲ့ ကိုယ်ပိုင် SID ထက် ၁ကြီးတဲ့ SID ပိုင်ဆိုင်ထားသော ကွန်ပျူတာတွေဆီကို ဆင့်ကဲဆင့်ကဲပေးပို့ကြရတာ ဖြစ်ပါတယ်။ အကယ်၍အဲ့သလိုပေးပို့နေရင်းနဲ့ သူ့ထက် SID ၁ကြီးတဲ့ကွန်ပျူတာက မတုံ့ပြန်ဘူးဆိုရင် SID နံပါတ်ကို နောက်ထပ် ၁ တိုးပြီးတော့ထပ်ပို့ပါတယ်။ အဲ့သလိုမှ မတုံ့ပြန်သေးဘူးဆိုရင်လည်း တုံ့ပြန်တာတဲ့ အထိ ၁ ကိုတိုးပြီး တိုးပြီးတော့ပို့သွားရပါတယ်။ ဆိုလိုချင်တာက SID 3 က SID 4 ကိုပို့လိုက်တယ်။ ဒါပေမယ့်

SID 4 ကမရှိခဲ့ဘူးဆိုရင် SID 3 ကတို့ပြန်မှုကိုမရဘူးဖြစ်နေပါတယ်။ ဒီအခါမှာ SID 3 ဟာ ၁ တိုးပြီးတော့ SID 5 ကိုပို့ပါတယ်။ အဲ့ဒီလိုနဲ့ SID 3 ကတို့ပြန်မှုကိုရတဲ့အထိ ၁တိုးပြီးပို့သွားတာကိုပြောချင်တာပါ။ အဲဒီလိုနဲ့ SID 255 ကိုရောက်သွားတဲ့အချိန်မှာ ၎င်းရဲ့ရှေ့မှာ NID မရှိတော့တာကြောင့် တို့ပြန်မှုမရဘူးဖြစ်နေ ပါတယ်။ ဒီအခါမှာ တစ်ပတ်ပြည့်အောင် Token ကို SID 1 သို့ပြန်ပို့လိုက်ပါတယ်။ ရှင်းအောင်ထပ်ပြောရမယ် ဆိုရင် ARCNet ရဲ့ Token Passing Method ဟာပါဆယ်ဂိမ်းကစားသလို ပါဆယ်ထုပ်ဆိုတဲ့ Token ကို ထိုင်နေတဲ့ သူတွေဆီအစဉ်လိုက်ပေးပို့တာမဟုတ်ဘဲ ၎င်းပါဆယ်ဂိမ်းကိုဆော့နေတဲ့သူ ကျောနံပါတ်စဉ်လိုက် အတိုင်းပေးပို့တာဖြစ်ပါတယ်။ ထိုင်နေတဲ့ သူတွေဟာ ကျောနံပါတ်စဉ်လိုက်အတိုင်း တန်းစီပြီးထိုင်နေတာဖြစ်ချင် မှဖြစ်ပါ လိမ့်မယ်။ ဒီတော့ပါဆယ်ထုတ်ဆိုတဲ့ Token လေးဟာမျက်စိထဲမြင်ကြည့်လိုက်ပါ။ အစဉ်လိုက်အတိုင်း မသွားဘဲ ဟိုရောက်လိုက် ဒီရောက်လိုက် ဖြစ်နေပါလိမ့်မယ်။

ပုံ ၈.၁၃



အချုပ်ပြောရမယ်ဆိုရင် Token Ring မှာသုံးတဲ့ Token Passing Access Method ဟာ ပါဆယ်ဂိမ်းဆော့သလို ဒီပါဆယ်ဆိုတဲ့ Token လေးကိုအစဉ်လိုက်အတိုင်းပေးပို့တာဖြစ်ပြီး ARCNet မှာသုံးတဲ့ Token Passing Access Method ကြတော့ ဒီပါဆယ်ဆိုတဲ့ Token လေးကိုပါဆယ်ဂိမ်းဆော့သလို ထိုင်နေတဲ့သူတွေဆီ အစဉ်လိုက်အတိုင်းပေးပို့တာမဟုတ်ဘဲ သူတို့ရဲ့ SID နံပါတ်အစဉ်အတိုင်းပေးပို့သွားတာ ဖြစ်ပါတယ်။ ဒီတော့ SID 1 ဘေးမှာထိုင်နေတဲ့သူဟာ SID 2 ဖြစ်ချင်မှဖြစ်မယ်။ ဒါကြောင့် SID 1 ဟာ SID 2 ဆိုတဲ့ကစားဖော်ဆီကို ဒီပါဆယ်ထုပ်ကိုကျော်ပြီး ပစ်ပေးရလိမ့်မယ်။ ပုံမှာကြည့်လိုက်ရင်တော့ အရှင်းဆုံး ဖြစ်သွားမှာပါ။ ARCNet မှာ SID တွေကိုလူကနေမှ Manualy Configuration လုပ်ပေးရတာကြောင့် သတိတော့အတော်ထားရပါတယ်။ ဒီလိုလေဗျာ။ Ethernet နှင့် Token Ring မှာကြတော့ကွန်ပျူတာမှာ Network Card ကိုစိုက်လိုက်တာနဲ့ မတူညီတဲ့ Address တစ်ခုဆီကိုပေးချလိုက်တာဗျ။ ဒီတော့ Address တွေဟာတစ်ခုနှင့်တစ်ခုတူနေစရာအကြောင်းမရှိဘူး။ ARCNet မှာကြတော့ ဒီ SID ကိုလူကသတ်မှတ်

ပေးရတော့ တခါတရံသွားတူနေတတ်တယ်။ ဒါဆိုရင် ပြဿနာတက်ပြီ။ နောက်ပြီး SID သတ်မှတ်တဲ့ပေါ်မူတည်ပြီး Network က လေးကျသွားတာမျိုးလည်းဖြစ်နိုင်သေးတယ်။ ဒါကြောင့် ARCNet ကို Administration လုပ်ရတာအတော်ကို စိတ်ညစ်စိုင်းကောင်းတယ်။ ARCNet ဟာ Token Passing ကိုအသုံးပြုထားတာကြောင့် Data Access အပိုင်းမှာကွန်ပျူတာအားလုံးဟာ ညီတူမျှတူဖြစ်ကြတယ်။ ဆိုလိုတာက ပြီးခဲ့တဲ့သင်ခန်းစာမှာရှင်းပြခဲ့ပြီးသလို Data Access ပိုင်းဆိုင်ရာမှာ Server ဖြစ်နေလို့ Station ဖြစ်နေလို့ဦးစားပေးခြင်းမရှိဘူး။ ARCNet ဟာတပ်ဆင်ရတာလွယ်ကူပြီး ကုန်ကျစရိတ်လည်းသက်သာတဲ့နည်းပညာလည်းဖြစ်ပါတယ်။ အဲဒီအပြင် တခြားနည်းပညာတွေထက်စာရင် Data ကိုပိုပြီး ခပ်ဝေးဝေးပို့နိုင်ပါတယ်။ အဲဒီအပြင် အမျိုးမျိုးသော Media (Cable) တွေနဲ့လည်းအသုံးပြုနိုင်ပါတယ်။ တစ်ခုတော့ရှိပါတယ်။ ARCNet ဟာနှေးတော့နှေးပါတယ်။ 2.5 Mbps ပဲ Transmit လုပ်နိုင်ပါတယ်။ နောက်ထပ်ပေါ်လာတဲ့ ARCNet Version အသစ်ကတော့ ARCNet Plus လို့ခေါ်ပြီး ၎င်းဟာ 20 Mbps အထိ Transmit လုပ်နိုင်ပါတယ်။ ဒါပေမယ့်လည်း သူဟာ ဒီနေ့ခေတ် ကွန်ရက်မျိုးကွက်ကို မကိုင်လှုပ်နိုင်ပါဘူး။

၈.၁၆ ARCNet Hub အကြောင်း

ARCNet Network နည်းပညာမှာ Hubs နှစ်မျိုးကိုအသုံးပြုပါတယ်။ အဲဒါတွေကတော့ Active Hub နှင့် Passive Hub ဖြစ်ပါတယ်။ ၎င်း Hub များအကြောင်းကို ပြီးခဲ့တဲ့သင်ခန်းစာတွေမှာ ဖော်ပြပြီးတာကြောင့် ထပ်မံမဖော်ပြတော့ပါဘူး။

၈.၁၇ ARCNet Cable အကြောင်း

ARCNet ဟာ Coaxial Cable နှင့်တပ်ဆင်မယ်ဆိုရင်တော့ RJ-62 A/U 93 Ohm ရှိတဲ့ Coaxial Cable နှင့်တပ်ဆင်ရတာဖြစ်ပါတယ်။ ၎င်းကိုတပ်ဆင်ပုံကတော့ Ethernet 10Base2 ကိုတပ်ဆင်ပုံနှင့်အလားသဏ္ဌာန်တူပါတယ်။ Ethernet ဟာ UTP Cable နှင့်လည်းတပ်ဆင်လို့ရပါသေးတယ်။ UTP နှင့်ဆိုရင်တော့ Cable အရှည်ဆုံးအလျားကို 121 မီတာအထိရရှိနိုင်ပါတယ်။ ထို့အပြင် ARCNet ဟာ Fiber Optic Cable နှင့်လည်းတပ်ဆင်လို့ရနိုင်ပါတယ်။ ၎င်း Fiber Optic နှင့်ဆိုရင်တော့ Cable ရဲ့အလျားဟာ 3485 မီတာအထိ ရပါတယ်။ အောက်မှာ ARCNet နှင့်ပတ်သက်၍ အချုပ်ဖော်ပြထားပါတယ်။

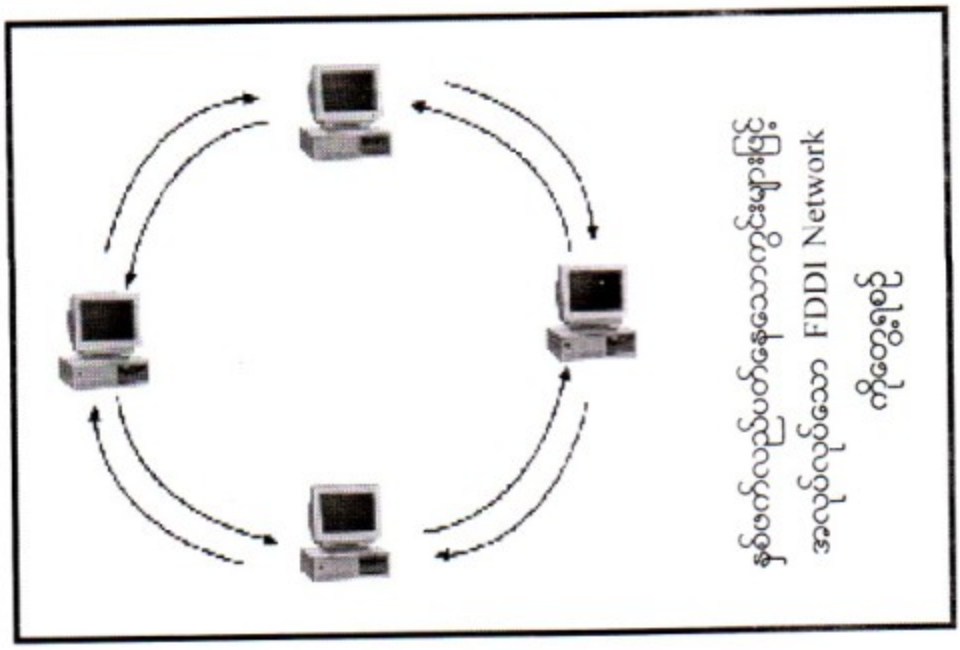
Category	Summary
IEEE Specification	No IEEE, ANS'878.1
Advantages	Indexpensive: easy to install; reliable
Disadvantage	Slow; does not connect well to other architecture
Topology	Bus and star
Cable Type	RG-62 A/U coaxial; UTP; fiber-optic
Channel access method	Token passing
Maximum cable segment length	600 meters (2000 feet)-RG-62 A/U 121 meters (400 feet)-UTP 3845 meters (11,500 feet)-fiber-optic 30 meters from passive to active hub
Maximum number of segment	Depends on topology
Maximum number of devices per segment	Depends on topology
Maximum number of devices per network	255
Transmission speed	2.5 Mbps

၈.၁၈ FDDI အကြောင်း

FDDI ကတော့ Token Passing Access Method ကိုအသုံးပြုထားတဲ့ Fiber Distributed Data Interface ပဲဖြစ်ပါတယ်။ ၎င်းဟာပုံမှာပြထားတဲ့အတိုင်းလည်ပတ်နေတဲ့ Rotating Rings ကို အပိုထား ရှိခြင်းကြောင့် Rings ကနှစ်ခုဖြစ်နေပါတယ်။ FDDI ဟာ 100 Mbps Transmit နှုန်းနဲ့ မိုင် ၆၀ ပတ်လည် (ကီလိုမီတာ ၁၀၀)အတွင်းမှာ Nodes ပေါင်း ၅၀၀ အထိတပ်ဆင်နိုင်ပါတယ်။ Token Ring လိုပါပဲ။ FDDI ဟာ Token Passing ကိုအသုံးပြုတယ်ဆိုပေမယ့် FDDI ဝါယာကြိုးတပ်ဆင်ပုံဟာ Physically အရ Star ပုံစံမဟုတ်ဘဲ Ring ပုံစံတပ်ဆင်ပါတယ်။ နောက်တစ်ခုက FDDI မှာ Hubs တွေမရှိဘဲ ပစ္စည်းတစ်ခုနှင့်တစ်ခု တိုက်ရိုက်ချိတ်ဆက်တာဖြစ်ပါတယ်။ ဘာပဲဖြစ်ဖြစ် Concentrator ကိုအသုံးပြုပြီး Central Connection Point ထားပြီးသုံးမယ်ဆိုရင်လည်းရပါတယ်။ FDDI ရဲ့ Token Passing ဟာ Token Ring နှင့် ARCnet တို့က Token Passing နှင့်ကွဲပြားမှုရှိပါတယ်။ FDDI ဟာ Token Ring မှာလို Token ကို Ring အလိုက်ပေးပို့ ပေမယ့် Token Ring နှင့်ကွဲသွားတဲ့အချက်က ကွန်ပျူတာဟာ Data တွေကိုပေးပို့တဲ့အခါ Token Data Frame ကိုတစ်ခုထက်ပိုပြီးပေးပို့ရတဲ့ အခြေအနေမျိုးမှာ ၎င်းဟာ နောက် Ring အပြည့် တစ်ပတ်မလည်ခင်

နောက်ထပ် Frame ကိုထပ်မံ Send လုပ်နိုင်ပါတယ်။ ဒါဟာဖြစ်နိုင်ရဲ့လား။ ဖြစ်နိုင်ပါတယ်။ ဘာလို့လည်းဆိုတော့ ပေးပို့သူ ရဲ့လက်ထဲမှာ Token ရှိနေသေးသရွေ့ အခြားမည်သူတစ်ဦးတစ်ယောက်ကမှ Active မဖြစ်နိုင်ပါဘူး။ ကွန်ပျူတာတွေဟာ Data ကို Send မလုပ်မီ Network ရဲ့ Latency ကိုတွက်ချက်ပြီးတော့ရယ်၊ နောက်ပြီး သင့်တော်တဲ့အချိန် Interval ကိုစောင့်ဆိုင်းပြီးတော့ရယ်ပေါ့ဗျာ။ Data ကို Collision မဖြစ်အောင်ရှောင်ကြဉ်ကြပါတယ်။ ဒီနည်းဟာ Network မှာ Data ကိုပိုမိုမြန်ဆန်အောင်လည်း Transmit လုပ်နိုင်ပါတယ်။ ထပ်မံရှင်းပြရရင်တော့ ကွန်ပျူတာဟာ Data ကိုပို့ပြီးပြီးချင်းပဲ Token ကို Pass လုပ်လိုက်ပါတယ်။ Data က ရည်ရွယ်ရာမှာလက်ခံရရှိကြောင်း စောင့်စရာမလိုပါဘူး။

ပုံ ၈.၁၄



FDDI ဟာ Station ကိုပဲဖြစ်စေ၊ Data အမျိုးအစားပေါ်ကိုပဲဖြစ်စေ ဦးစားပေးအဆင့် Priority Level သတ်မှတ်ပေးလို့ရပါတယ်။ ဒါလည်းရှင်းပြခဲ့ဖူးပြီးပါပြီ။ Server တွေဟာ Workstation ထက် Priority ပိုမြင့်ပါတယ်။ Data အရေးပြောရင်လည်း Time-Sensitive Data တွေကလည်း Priority ပိုမြင့်ပါတယ်။ ပြောခဲ့ဖူးတဲ့အတိုင်းပါပဲ။ FDDI ဟာမတူညီတဲ့ Direction နှင့် Ring နှစ်ခုကိုအသုံးပြုပါတယ်။ FDDI က အသုံးပြုသော Network Card နှစ်မျိုးရှိပါတယ်။ အဲ့ဒါတွေကတော့ -

(၁) DAS လို့ခေါ်တဲ့ Dual Attachment Stations နှင့်

(၂) SAS လို့ခေါ်တဲ့ Single Attachment Station တို့ဖြစ်ကြပါတယ်။

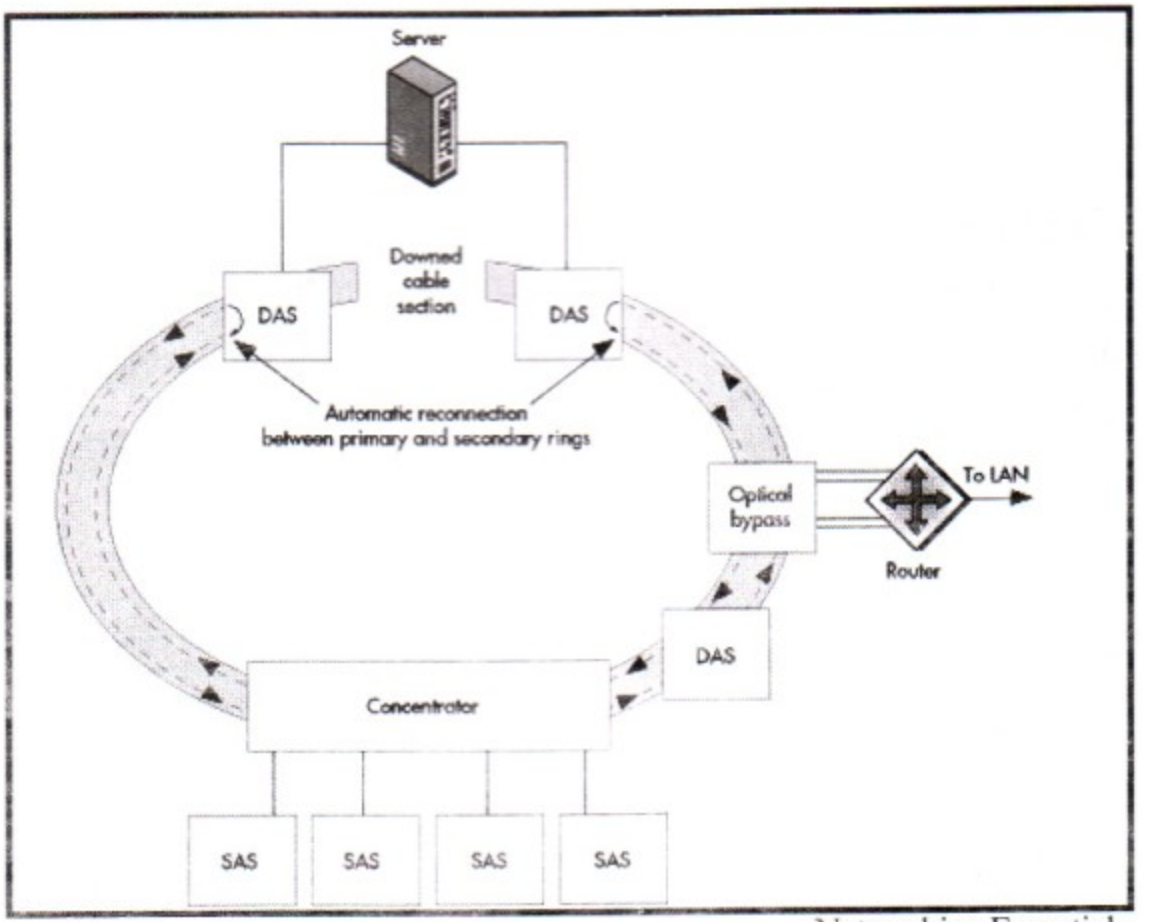
DAS ဟာ Ring နှစ်ခုစလုံးကိုချိတ်ဆက်ထားတာကြောင့် Server တွေ Concentrators တွေ အခြားသောစွမ်းဆောင်ရည် စိတ်ချရမှုအပြည့် အသုံးချလိုသော ပစ္စည်းတွေမှာအသုံးပြုလို့ရပါတယ်။ SAS ကြတော့ Ring တစ်ခုတည်းကိုပဲချိတ်ဆက်တာဖြစ်သောကြောင့် Concentrators တွေနှင့်ချိတ်ဆက်တဲ့

Workstations တွေမှာအသုံးပြုနိုင်ပါတယ်။ ဒါတောင် ဒီ Workstation တွေမှာ ကောင်းကျိုးရှိနိုင်ပါတယ်။ ဘာလို့လည်းဆိုတော့ Concentrators က Dual Rings နှင့်ချိတ်ဆက်ထားတာကိုး။

အောက်မှာ FDDI နှင့်ပတ်သက်၍အချုပ်ဖော်ပြထားပါသေးတယ်။

Category	Summary
IEEE Specification	No IEEE, ANSI X3T9.1
Advantages	Very fast; reliable; long distance; highly secure
Disadvantage	Expensive; difficult to install
Topology	Ring
Cable Type	Fiber-optic
Channel access method	Token passing
Maximum toal network length	100 km (600 miles)
Maximum number of devices per network	500
Transmission speed	100 Mbps

ပုံ ၈.၁၅



၈.၁၉ Asynchronous Transfar mode (ATM) အကြောင်း

အခြားသော Network နည်းပညာများနှင့် မတူတဲ့နောက်ထပ်နည်းပညာတစ်ခုကတော့ ATM ပဲဖြစ်ပါတယ်။ ၎င်းဟာ LAN ရော WAN မှာပါ High Speed နဲ့လုပ်နိုင်တဲ့ Network နည်းပညာဖြစ်ပါတယ်။ ဘယ်လောက်တောင်မြန်သလဲဆိုရင် 155 Mbps မှ 622 Mbps အထိ အလုပ်လုပ်နိုင်ပါတယ်။ ATM တာ ၎င်း၏ Network တွင်ပေးပို့သူနှင့် လက်ခံသူတို့အဆက်အသွယ်ရရှိစေရန် Connection Oritent ကိုအသုံးပြုသည်။

ATM သည် Data များပေးပို့ခြင်းလုပ်ငန်းကို Cell ဖြင့်အလုပ်လုပ်သည်။ ၎င်း Cell သည် 53 Byte ရှိပြီး 48 Byte မှာ Data ဖြစ်၍ 5 Byte မှာ Header ဖြစ်သည်။ ATM တာ Cell တွေရဲ့အရွယ်အစားကို တသမတ်ထဲ သတ်မှတ်ထားခြင်းကြောင့် Data ကပေးပို့ရာတွင် အလွန်လျင်မြန်စွာ ပေးပို့နိုင်ခြင်းဖြစ်သည်။ ပြောရမယ်ဆိုရင်တော့ဗျာ Network မှာက အရွယ်အစားအမျိုးမျိုးရှိတဲ့ Frame တွေကိုပေးပို့တာထက်စာရင် တူညီတဲ့အရွယ်အစားရှိတဲ့ Frame တွေကိုပေးပို့ရတာက ပိုရှင်းမြန်ဆန်စေပါတယ်။ (ATM) မှာ Cell တွေဟာ တူညီတဲ့အရွယ်အစားရှိတာကြောင့် ပေးပို့သည့်ကြာချိန် Transfer Time ကိုချိန်ထိုးရရှောကြောင့် Data စီးဆင်းမှုကိုများစွာအထောက်အကူပြုစေပါတယ်။ ၎င်းအပြင် Bandwidth ကိုချိန်ဆ ရာမှာလည်းအထောက် အကူပြုစေပါတယ်။ ဒါကြောင့် (ATM) ကို Quality လိုအပ်တဲ့ဝန်ဆောင်မှုတွေဖြစ်တဲ့။ အင်း ဘိုလိုပြောရရင် တော့ QoS လို့ခေါ်တဲ့ Quality of Services စတဲ့လုပ်ငန်းတွေအတွက် သင့်တော်တယ်ပေါ့ဗျာ။ ဘယ်လို လုပ်ငန်းမျိုးတွေလဲဆိုတော့ Audio ပိုင်းဆိုင်ရာတွေ Multimedia ပိုင်းဆိုင်ရာတွေ Video Confrencing စတဲ့ Time-Sensitive ဖြစ်ကြသောလုပ်ငန်းတွေပေါ့ဗျာ။ ဒါကိုသေချာစိတ်နှံပြီးပြောရမယ်ဆိုရင်တော့ တစ်နည်းအားဖြင့် (ATM) လုပ်ပေးနိုင်တာက

(၁) Voice
(၂) Data
(၃) Fax
(၄) Real-time Video
(၅) CD-Quality Audio
(၆) Imaging
(၇) Multimegabit Data Transmission

တို့ဖြစ်ကြပါတယ်။

ATM Network ကိုအသုံးပြုဖို့အတွက် ကျွန်တော်တို့သိထားရမှာကၤ၎င်း Network မှာအသုံးပြုတဲ့ ဆက်စပ်ပစ္စည်းတွေဟာ ATM Compatible ဖြစ်ဖို့လိုအပ်ပါတယ်။ ၎င်းပစ္စည်းများကိုဖော်ပြရမယ်ဆိုရင်တော့

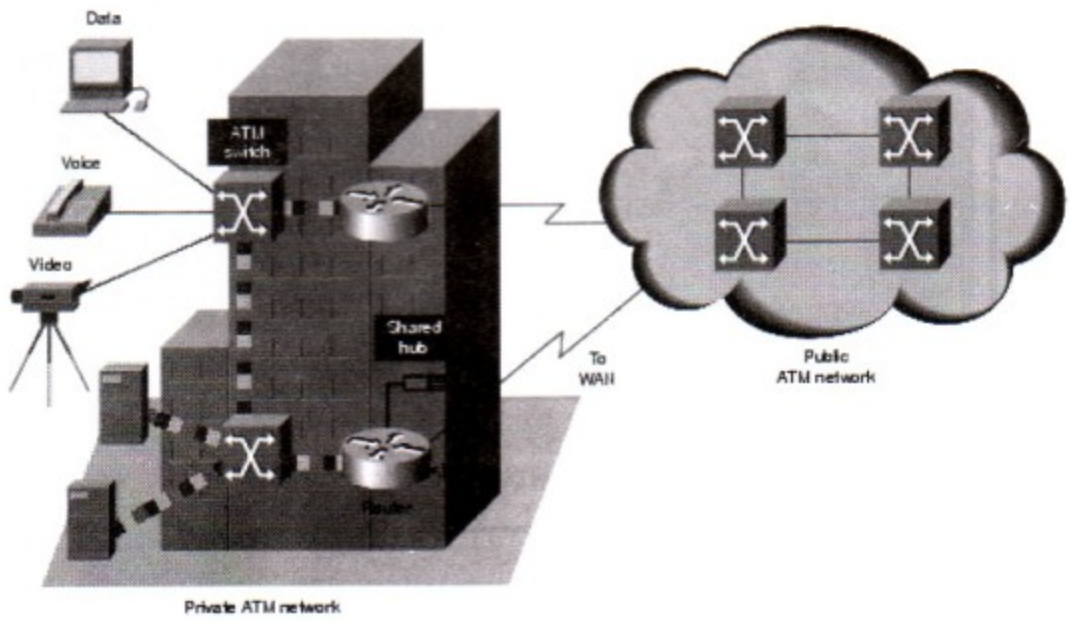
- Carries Services နှင့်ချိတ်ဆက်အသုံးပြုရန် Routers များနှင့် Switch များ။
- အဖွဲ့အစည်းကြီးများအတွင်း LAN အချင်းချင်းချိတ်ဆက်အသုံးပြုရန် Backbone Device များ။
- Multimedia Application များအသုံးပြုရန်အတွက် Desktop Computer များကို High-Speed ATM နှင့်ချိတ်ဆက်ပေးနိုင်သော Switch များနှင့် Adapter များတို့ဖြစ်ကြပါတယ်။

ATM Switch တွေဟာ Multiport Device တွေဖြစ်ကြပြီး ၎င်းတို့ဟာကွန်ရက်အတွင်းရှိ Computer များတစ်လုံးမှတစ်လုံးသို့ Data ပေးပို့ရန် Hub အဖြစ်လည်းကောင်း Remote Network များတွင် Data များမြန်မြန်ပေးပို့နိုင်ရန် Router အဖြစ်လည်းကောင်းအသုံးပြုနိုင်ပါတယ်။ ATM အတွက်အသုံးပြုဖို့သင့်တော်သော Media တွေကတော့ -

- FDDI (100 Mbps)
- Fiber Channel (155 Mbps)
- OC 3 SONET (155 Mbps) တို့ဖြစ်ကြပါတယ်။

(ATM) ၏ Bandwidth ဟာ Optical Carries နှင့်လည်းဖော်ပြလေ့ရှိပါတယ်။ အတိုကောက်ဆိုရင် OC-X ပေါ့။ အဲ့ဒီနေရာမှာ X ဆိုတာကတော့အသေမဟုတ်ဘဲ နံပါတ်တစ်ခုအစားထိုးဝင်ရမှာဖြစ်ပါတယ်။ ဥပမာပြောရရင် OC-1 ဟာ 51.84 Mbps သယ်ဆောင်နိုင်ပါတယ်။ အောက်မှာ ATM အတွက်ရော Sonet (Sychronous Optical Network) အတွက်ပါ Optical Carries Hate ကိုဖော်ပြပေးထားပါတယ်။ အဲ့ဒီအထဲမှာမှယနေ့ဈေးကွက်တွင်ရှိနိုင်သော ATM ၏ Signal Rate မှာ OC-3 မှ OC-12 အထိဖြစ်ပါသည်။

ပုံ ၈.၁၆



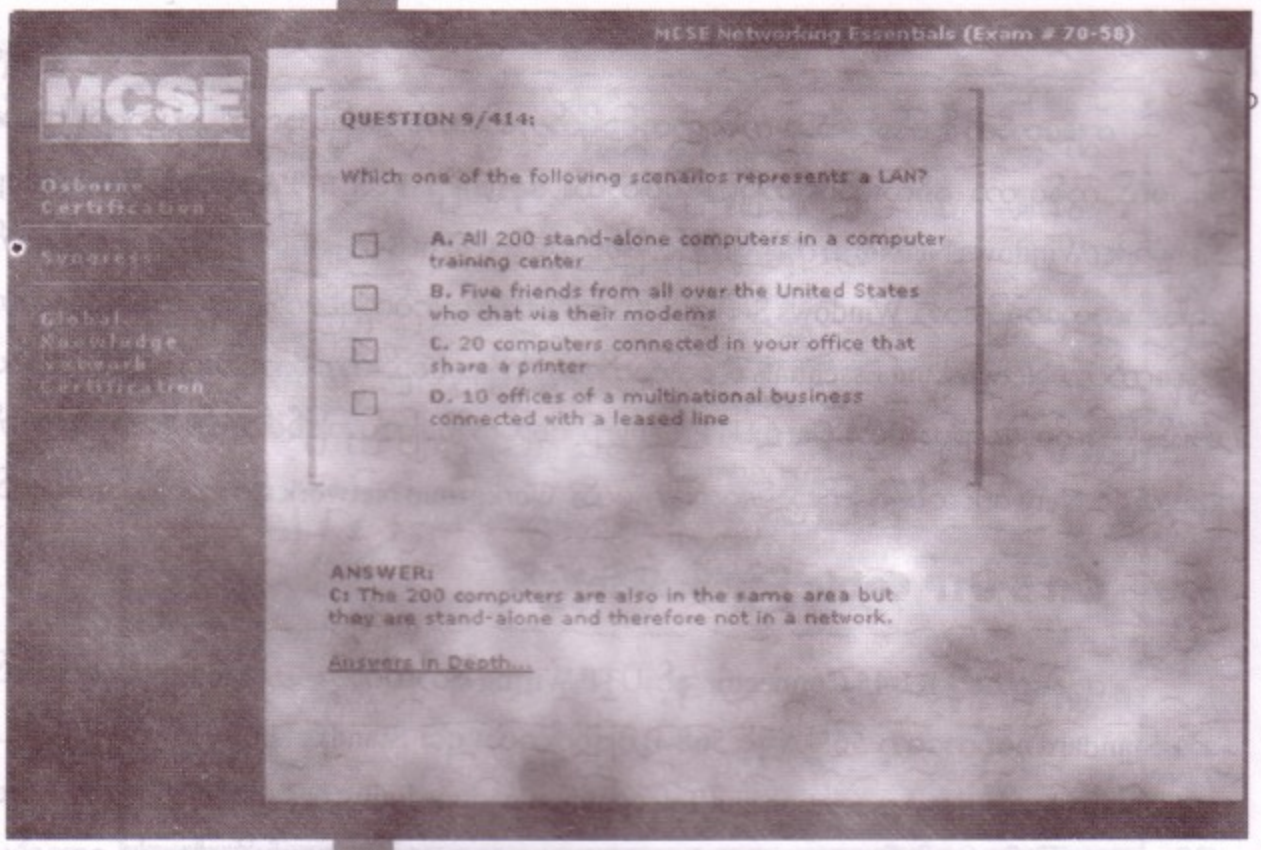
ATM Network တစ်ခုကိုတွေ့ရစဉ်

Sonet ဆိုသည်မှာ Network တစ်ခုမှ Voice Video တွေကိုအခြားတစ်နေရာသို့ သယ်ယူပို့ဆောင်ပေးနိုင်သော Fiber Optic ကိုအခြေခံထားသောစနစ်တစ်ခုဖြစ်ပါတယ်။ ၎င်းသည် 1 Gbps နှုန်းအထက် Data များပေးပို့နိုင်ပါသည်။

Optical Carrier Designation	Signaling Rate
OC-1	51.84 Mbps
OC-3	155.52 Mbps
OC-9	466.56 Mbps
OC-12	622.08 Mbps
OC-24	1.244 Gbps
OC-36	1.866 Gbps
OC-46	2.488 Gbps
OC-96	4.976 Gbps
OC-192	9.953 Gbps
OC-255	13.271 Gbps
OC-768	39.813 Gbps

ပုံ ၈.၁၇

ATM 4 Port Switch နှင့် 8 Port Switch ကိုတွေ့ရစဉ်



UNIT 9

Simple Network Installation

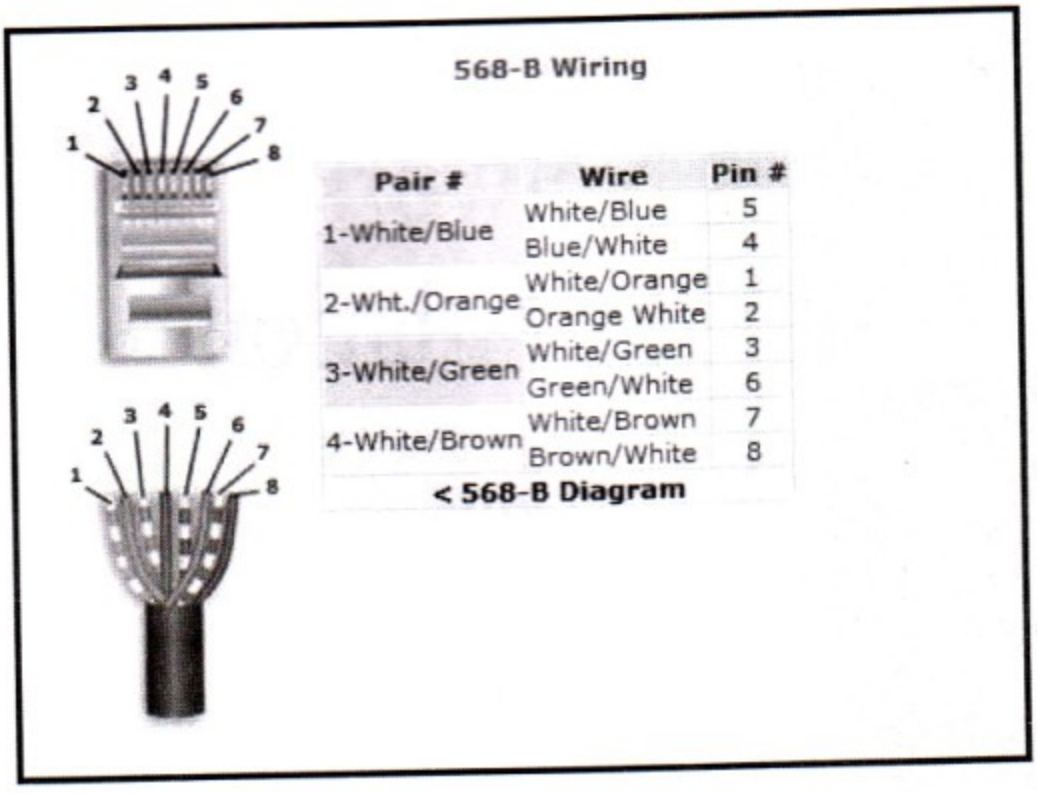
ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကွန်ပျူတာကွန်ရက် တစ်ခုကို ဘယ်လိုတပ်ဆင်ကြမလဲဆိုတာကို လေ့လာကြရမှာ ဖြစ်ပါတယ်။ အခုမှ လက်တွေ့ ချိတ်ဆက်မည့်သူများ သေချာ တစ်ဆင့်ချင်းဖတ်ကြည့်သွားပြီး လုပ်ကြည့်ပါ။

ကျွန်တော်တို့ ဒီသင်ခန်းစာမှာ ကွန်ရက်တစ်ခုချိတ်တတ်အောင် အခြေခံအဆင့်ပြောပြမှာဖြစ်ပါတယ်။ ဒါပေမယ့် ကွန်ပျူတာ နှစ်လုံးကိုပဲချိတ်ပြမှာဖြစ်ပါတယ်။ နောက်ပြီး Peer to Peer ဆိုတဲ့ Workgroup Network (Windows Network) ကိုပဲ ချိတ်ပြမှာဖြစ်ပါတယ်။ Client Server ချိတ်ချင်ရင်တော့ ကျွန်တော် ရေးသားထုတ်ဝေခဲ့ပြီးသော Windows Server 2003 in Details စာအုပ်ကိုပြန်ဖတ်စေလိုပါတယ်။ ဒီနေရာမှာ ကျွန်တော်ဟာ Networking Essentials နှင့်ပတ်သက်နေတဲ့ ကြိုးညှပ်နည်းကိုအဓိကထားပြောပြချင်တာဖြစ်ပါတယ်။ ကြိုးဆိုတဲ့နေရာမှာလည်း Cat 5 UTP Cable ညှပ်နည်းကိုပဲပြောပြမှာဖြစ်ပါတယ်။ ဒီတော့ အခုဖတ်ပြီးသွားရင် Network ဆင်ဖို့ရာကြိုးညှပ်တတ်သွားမယ်။ Workgroup Network ချိတ်တတ်သွားလိမ့်မယ်။

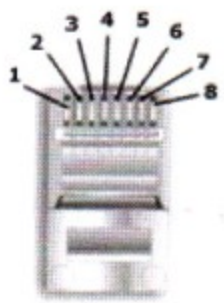
၉.၁ Cat 5 UTP Cable ကြိုးအရောင်တွဲခြင်း

ကျွန်တော်တို့ RJ-45 Connector နှင့် UTP Wiring ချိတ်ဆက်ဖို့ရာ Standard နှစ်ခုရှိပါတယ်။ အဲဒီ Standard နှစ်ခုကတော့ 568-A နှင့် 568-B ပဲဖြစ်ပါတယ်။ ၎င်း Standard နှစ်ခုစလုံးဟာ EIA/TIA (Electronic Industries Association and Telecommunications Industries Association) နှင့် Agree ဖြစ်နေတာကြောင့် ၎င်းတို့ကို EIA/TIA 568-A, EIA/TIA 568-B လို့လည်းခေါ်လို့ရပါတယ်။ အောက်မှာ ၎င်း Standard နှစ်ခုစလုံးရဲ့ကြိုးတွဲရမယ့်ပုံကိုဖော်ပြပေးထားပါတယ်။

ပုံ ၉.၁



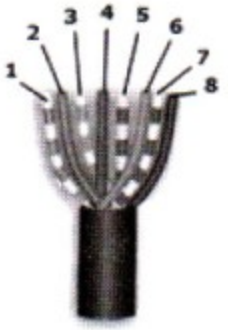
ပုံ ၉.၂



568-A Wiring

Pair #	Wire	Pin #
1-White/Blue	White/Blue	5
	Blue/White	4
2-White/Green	White/Green	1
	Green/White	2
3-White/Orange	White/Orange	3
	Orange/White	6
4-White/Brown	White/Brown	7
	Brown/White	8

< 568-A Diagram



(၁) ကြိုးညှပ်ရာမှာ ၎င်း Standard နှစ်ခုထဲက ဘယ်နည်းကိုသုံးသုံးအတူတူပါ။ ကွဲပြားမှုမရှိပါဘူး။ အဲပေမယ့် 568-B ကပိုအသုံးများပါတယ်။

(၂) ပုံမှန်ဆိုရင်တော့ ကြိုးရဲ့ တစ်ဖက်စွန်းမှာ ညှပ်ထားတဲ့ အရောင်အစဉ်အတိုင်း တစ်ဖက်အစွန်းမှာလည်း ဖြစ်ရပါတယ်။ နှစ်ဖက်တူရတယ်ပေါ့ဗျာ။

(၃) အဲပေသိ Crossover Cable အတွက်ဆိုရင်တော့ တစ်ဖက်အစွန်းကို 568-A နှင့် ညှပ်ပြီး တစ်ဖက်အစွန်းကိုတော့ 568-B နှင့်ညှပ်ရမှာဖြစ်ပါတယ်။

(၄) Crossover Cable ဆိုတာ Hub to Hub ချိတ်တာဖြစ်ပါတယ်။ အဲပေမယ့် ၎င်းကို Hub မပါဘဲ Station နှစ်ခုတိုက်ရိုက်ချိတ်ဆက်တဲ့အခါမှာလည်းအသုံးပြုနိုင်ပါတယ်။

အခုကျွန်တော် Crossover Cable ကိုညှပ်ပြပြီး ၎င်းကြိုးနှင့် ကွန်ပျူတာနှစ်လုံးကိုတိုက်ရိုက် Hub မပါဘဲချိတ်ဆက်ကာ Windows Network ကိုချိတ်ပြမှာဖြစ်ပါတယ်။ Crossover Cable ကို ဆောင်ထားခြင်းဖြင့် Network Server လိုက်မည်သူတွေတာ မိမိ Laptop နှင့် ၎င်းဌာနရှိ Server ကိုတိုက်ရိုက်ချိတ်ဆက်ပြီး Server ၏ Network Card အလုပ် လုပ်မလုပ်ကိုစမ်းသပ်နိုင်ပါတယ်။

၉.၂ Cat 5 UTP Cable ကြိုးစည်ပိတ်ခြင်း

၁။ အပြင်အလွှာကို ၁ လက်မလောက် ခွာထုတ်လိုက်ပါ။

၂။ ကြိုးတစ်မျှင်ချင်းစီလိမ်နေခြင်းမှာဖယ်ထုတ်လိုက်ပါ။ ဖြောင့်နေအောင်ဖြန့်လုပ်ပါ။

၃။ ကိုယ်တပ်ဆင်ချင်တဲ့ Standard အတိုင်းကြိုးအရောင်များကိုစီပါ။ ပုံမှာပြထားတဲ့ထားပါ။

၄။ ပြီးလျှင် ကိုယ်တပ်ဆင်ချင်တဲ့ Standard အတိုင်း ကြိုးအရောင်များအစဉ်ကျမကျ ပြန်စစ်ပါ။

၅။ ကြိုးအခွံအဆုံးမှ လက်မဝက်အကွာတွင် ကြိုးပေါ်ခွံအမှတ်အသားပေးထားပါ။ မလုပ်ချင်လည်းရပါတယ်။

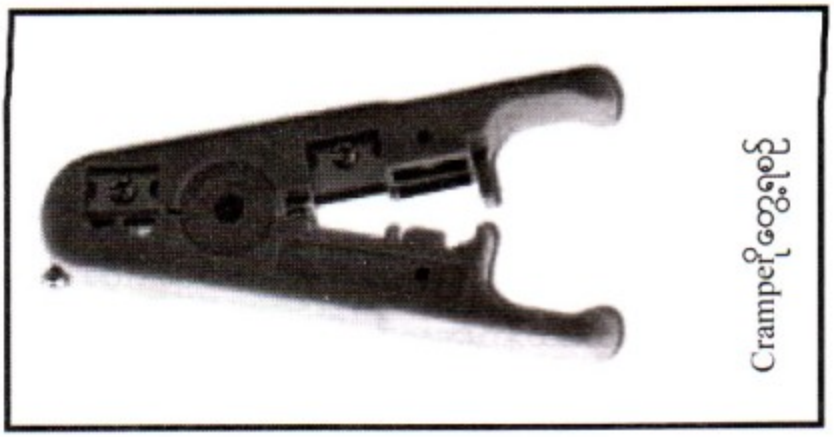
၆။ ကြိုးများကို လက်မနှင့်လက်ညှိုးကြားညှပ်ပြီးဖိပေးပါ။

၇။ ခုနက အမှတ်အသားပေးခဲ့သောနေရာတွင် တိကန် ဖြစ်နေအောင် ကြိုးကိုညှပ်ချပါ။ ကတ်ကြေးနဲ့ဖြစ်ဖြစ်ပေါ့။ ဒီနေရာမှာ အရမ်းအရေးကြီးတယ်။ ကြိုးတွေဟာ တညီတညွတ်သွားရမယ်။ အဖျားတွေဟာ ညီနေဖို့လိုအပ်တယ်။ RJ-45 ခေါင်းဟာလက်မဝက်အလျားရှိပြီး ၉၀ ဒီဂရီ အဖျားရှိတာကြောင့် အရှည်လက်မဝက်မှာ တိကန်ဖြတ်ချခိုင်းတာဖြစ်ပါတယ်။

၈။ ကြိုးတွေကို ခေါင်းထဲထိုးထည့်လိုက်ပါတော့။

၉။ ကြိုးတွေဟာခေါင်းရဲ့ အဆုံးထဲထိရောက်သွားအောင်ဖိသွင်းပေးဖို့လိုပါလိမ့်မယ်။ ကြိုးအခွံဟာ ခေါင်းရဲ့ နောက်ဖက်ခြမ်းမှာဝင်သွားဖို့လိုအပ်ပါတယ်။ ဒါမှညှပ်ချလိုက်ရင် ကြိုးက ခေါင်းထဲကနေ ပြန်မထွက်ပဲဖြစ်နေမှာဖြစ်ပါတယ်။ ကဲပြီးရင် ၎င်းကြိုးဝင်နေပြီးသော ခေါင်းကို Cramping Tool ထဲထည့်ပြီး ညှပ်ချလိုက်ပါတော့။ အားသုံးရတယ်ဆိုပေမယ့်အချိန်အဆလိုပါတယ်။ အရမ်းကြိုးလည်းဖိမချလိုက်ပါနဲ့။ အားနှင့်မဖိပဲလည်းမနေပါနှင့်။ ခေါင်းထဲက ရွှေဝါရောင်အသွားလေးတွေကို ကြိုးလေးတွေကိုက်ဖောက်သွားလောက်ရုံပေါ့။

ပုံ ၉.၄



Crimperကိုတွေ့ရစဉ်

၁၀။ ဒီဆိုပြီးပါပြီ။ ဒီနည်းအတိုင်း အခြားတစ်ဖက်ကိုလုပ်ပါ။ ပုံမှန်ဆိုရင် ကြိုးအရောင်အစဉ်ဟာ နှစ်ဖက်တူရမယ်။ Crossover ဆိုရင်တော့ တစ်ဖက်က 568-A ဖြစ်ပြီး တစ်ဖက်က 568-B ဖြစ်ရပါမယ်။ အခုစာဖတ်သူကတော့ Crossover ပဲညှပ်ပေးပါ။

၁၁။ ကြိုးအလုပ် လုပ်မလုပ်စမ်းကြည့်လို့ရပါပြီ။

ကဲ ကြိုးတော့ညှပ်ပြီးသွားပြီ။ Network ချိတ်ဖို့ပဲကျန်တော့တယ်။ ကဲ Network မချိတ်ခင် Cat 5 Cable ရဲ့ ဆောင်ရန်ရှောင်ရန်တွေကိုအရင်လေ့လာကြည့်ရအောင်။

၉.၃ Cat 5 UTP Cable ဆောင်ရန်ရှောင်ရန်

၁။ ကြိုးညှပ်တဲ့အခါဘယ်တော့မှ ကြိုးရဲ့ အပြင်အခွံကို တစ်လက်မထက် ပိုမခွာထုတ်ပါနှင့်။

၂။ ကြိုးကိုခွေတဲ့အခါမှာ အရမ်းကြီး ခေါက်ပြီးမခွေပါနှင့်။ ပြေပြေလေးခွေနိုင်ပါသည်။

၃။ ကြိုးကိုတင်းနေအောင်ချည်နှောင်ခြင်း၊ ဆွဲဆန့်ခြင်းမျိုးမပြုလုပ်ပါနှင့်။

၄။ ကြိုးကိုဆွဲခြင်းအတွက်သီးသန့်ထုတ်လုပ်ထားခြင်းမဟုတ်သော ဆီ၊ ချောဆီများကိုအသုံးမပြုပါနှင့်။ ၎င်းတို့သည် လျှပ်ကာခြင်းလုပ်ငန်းကိုထိခိုက်စေပါတယ်။

၅။ လျှပ်စစ်နှင့်ပတ်သက်သောအရာများနှင့်တွဲမထားပါနှင့်။

၆။ ကွန်ရက်တစ်ခုထဲမှာပဲကြိုးကို 568-A နှင့် 568-B ရောမသုံးပါနှင့်။ ပရိုဂျက်မစခင်ဘာကိုသုံးမလဲ အရင်စဉ်းစားပါ။ ကွန်ရက်တစ်ခုလုံးမှာရှိတဲ့ ကြိုးတွေအားလုံးနှင့် Jacks တွေ Patch Panel တွေမှာပါ အားလုံး 568-A ဆိုလည်း 568-A, B ဆိုလည်း B တစ်မျိုးကိုပဲသုံးပေးပါ။

၇။ ကြိုးတွေများလာရင်ရှုပ်လာနိုင်တာမို့ ကြိုးအစွန်းတွေမှာ Label ကပ်ပေးပါကပိုကောင်းပါသည်။ ဥပမာ ကြိုးနံပါတ် ၁ ဆို အစွန်းနှစ်ဖက်မှာ ၁ ဆိုပြီး တိတ်ပတ်ထားလိုက်ပေါ့။

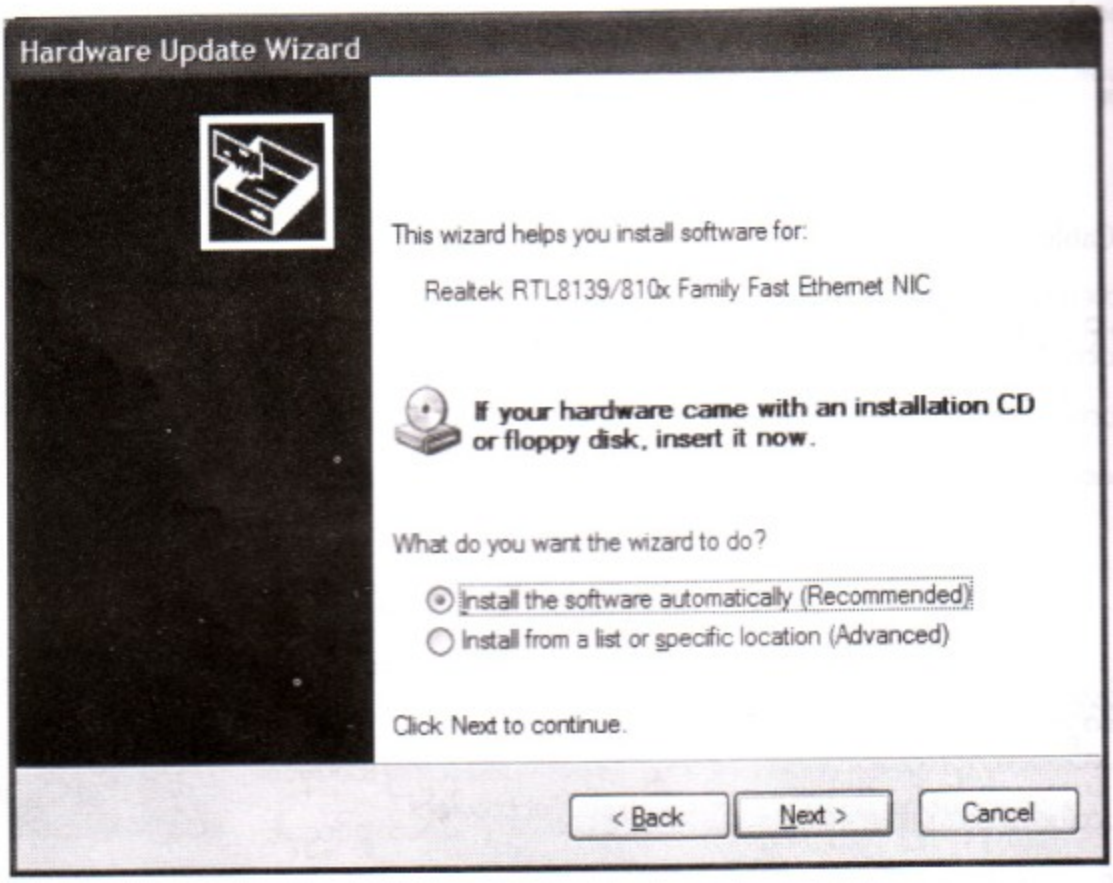
၉.၄ Peer Network ချိတ်ဆက်ခြင်း

၁။ ခုနကညွှန်ထားသောကြိုးကို အခုချိတ်ဆက်ဖို့ အဆင့်သင့်ဖြစ်နေတဲ့ ကွန်ပျူတာနှစ်လုံးရဲ့ Network Card (RJ-45 Port) တွေမှာ တိုက်ရိုက်ချိတ်ဆက်လိုက်ပါ။

၂။ အခုလိုအပ်တာက Windows XP တင်ထားတဲ့ Network Card (RJ45 Port) ပါသောကွန်ပျူတာနှစ်လုံးဖြစ်ပါတယ်။ ခုနက ကောင်းမွန်စွာညွှန်ထားသောကြိုးရှိနေရပါမယ်။ Hub မလိုအပ်ပါဘူး။ တိုက်ရိုက်ချိတ်မှာပါ။ CD-Rom Drive လိုအပ်ပါတယ်။ Windows XP CD နှင့် Network Card Driv er CD တို့လိုအပ်ပါတယ်။

၃။ ပထမဦးစွာ ကွန်ပျူတာတစ်လုံးချင်းစီရဲ့ Windows XP မှာ Network Card ကို Driver တင်ပေးပါ။

ပုံ ၉.၅

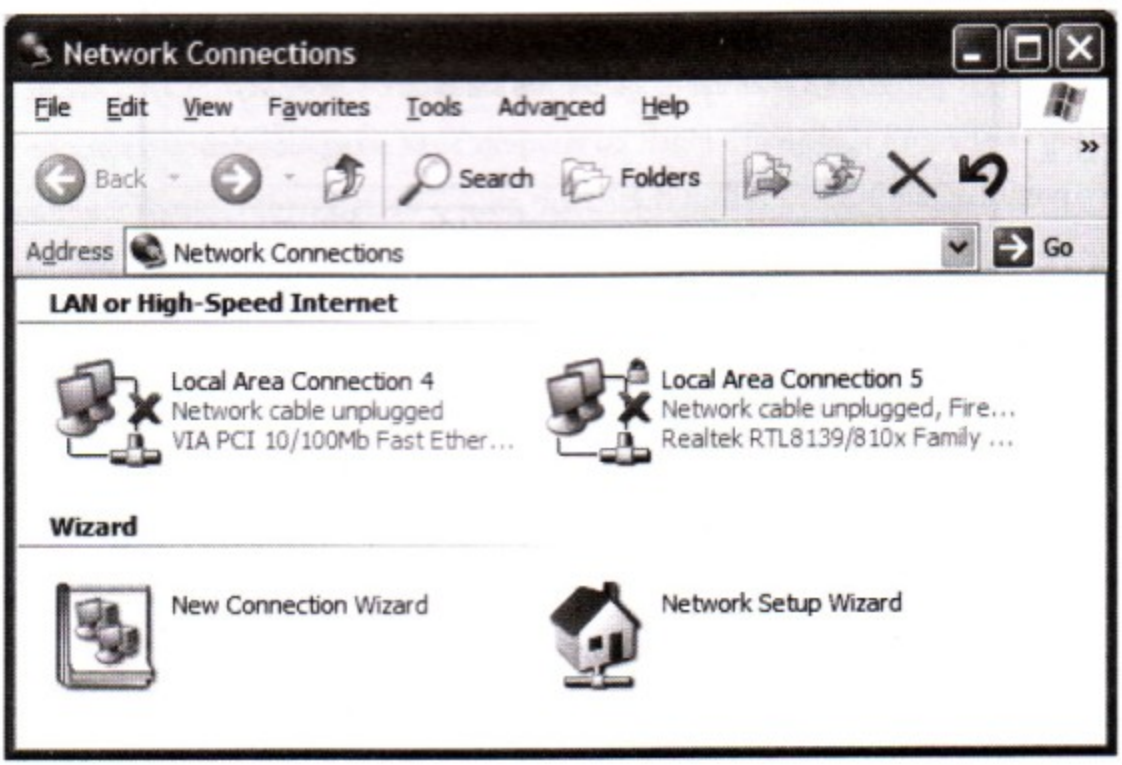


၄။ Network Card Driver တင်ပြီးသွားပါက Device Manager တွင် ပုံ ၉.၆ သို့လာပေါ်နေပါလိမ့်မည်။ ထို့အတူ Windows XP ၏ Desktop ပေါ်တွင် My Network Places ဆိုသည့် Icon လေးပေါ်နေပါလိမ့်မယ်။

ပုံ ၉.၆

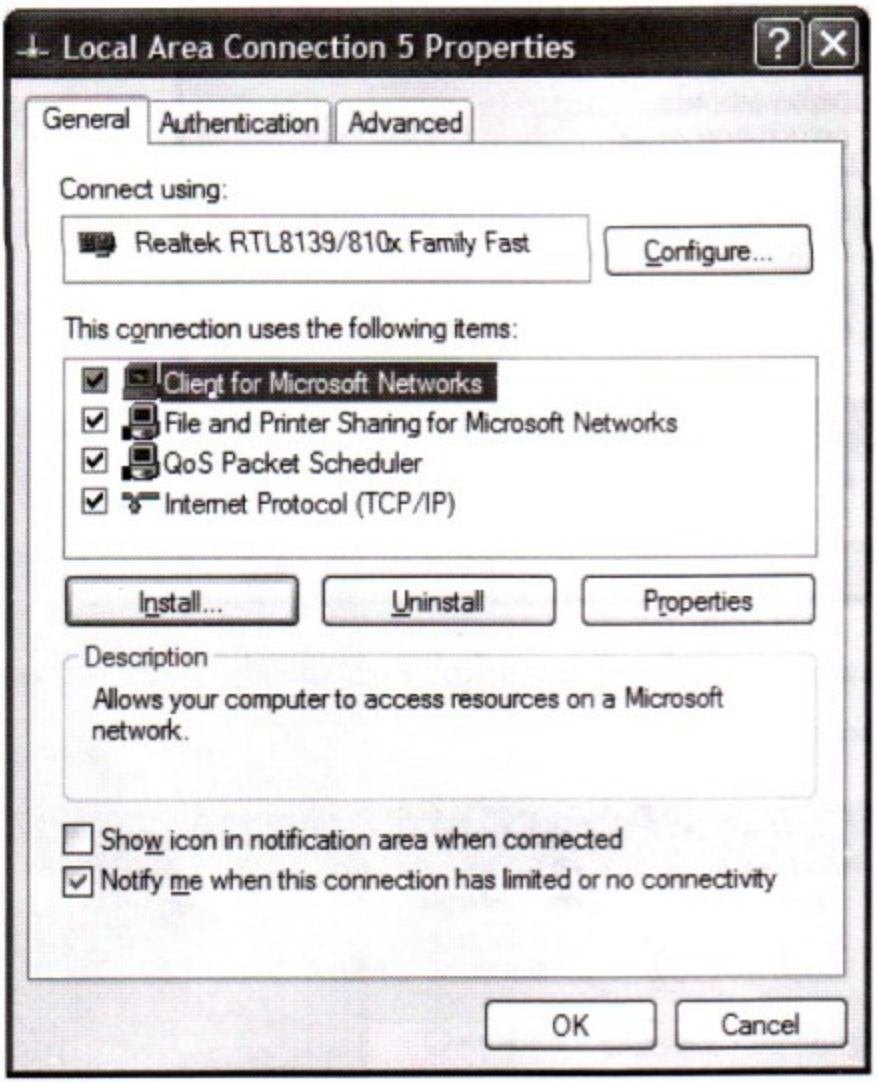
၅။ ၎င်း My Network Places ဆိုသည့် Icon ပေါ်တွင် Right Click နှိပ်ကာ Properties တက်ပြပါ။ ပုံ ၉.၇ ပေါ်လာပါလိမ့်မယ်။

ပုံ ၉.၇



၆။ ကျွန်တော့်စက်တွင် Network Port နှစ်ခုရှိနေသောကြောင့် ပုံ ၉.၇ တွင် Local Area Connection နှစ်ခုရှိနေတာဖြစ်ပါတယ်။ စာဖတ်သူ လူကြီးမင်းစက်မှာ တစ်ခုပဲရှိချင်ရှိနေမှာပါ။ ၎င်း Local Area Connection Icon ပေါ်တွင် Double Click နှိပ်ပါ။ ပုံ ၉.၈ ပေါ်လာပါလိမ့်မယ်။

ပုံ ၉.၈



၇။ Windows Network ချိတ်ရာတွင်

(၁) Network Card Driver တက်နေရပါမည်။

(၂) Protocol (Eg., TCP/IP or NetBEUI) တက်နေရပါမည်။

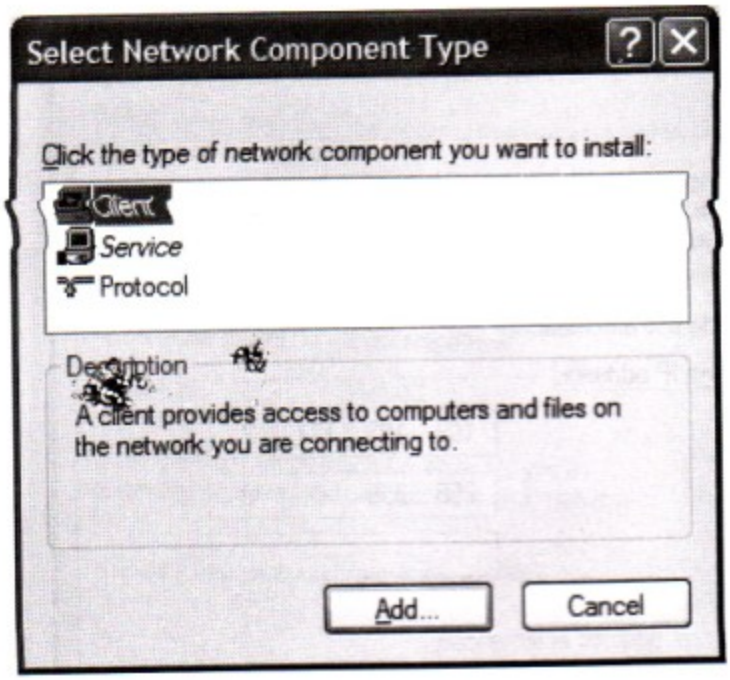
(၃) Client (Client for Microsoft/Novell Network) တက်နေရပါမည်။

(၄) Service (File & Print Sharing Service) တက်နေရပါမည်။

၎င်း ၄ ချက် လိုအပ်ပါသည်။ ယခုအခါ TCP/IP Protocol ကိုသုံးပါမည်။ Windows System အချင်းချင်းချိတ်ဆက်မည်ဖြစ်ပါသောကြောင့် Client သည် Client for Microsoft Network ဖြစ်နေရပါမည်။ ပုံ ၉.၈ အရ ၎င်း ၄ ချက်စလုံး သူ့ဘာသာသူတင်ပေးထားပြီးဖြစ်ကြောင်းတွေ့ပါလိမ့်မည်။ ၎င်း ၄ ချက်

မပြည့်စုံသေးလျှင် ပုံ ၉.၈ ရှိ Install ဆိုသည့် ခလုတ်ကိုနှိပ်ကာ ပုံ ၉.၉ ပေါ်လာပြီး Install လုပ်ပေးနိုင်ပါလိမ့်မည်။

ပုံ ၉.၉



၈။ ယခုအဆင့်အနေဖြင့် IP Address ကိုပေးမည်ဖြစ်ရာ ပုံ ၉.၈ တွင် Internet Protocol (TCP/IP) ဆိုတာကိုရွေး၍ Properties ခလုတ်ကိုနှိပ်ပါ။ ပုံ ၉.၁၀ တွင်ပြထားသည့်အတိုင်းရိုက်ထည့်ပါ။ ပြီးရင် OK ပြောပါ။ နောက် ပုံ ၉.၈ ကို Close လုပ်လိုက်ပါ။ နောက် ကွန်ပျူတာတစ်လုံးတွင် ဒီအဆင့်ကိုရောက်သည့်အခါ IP Address ကို ယခု Address နှင့်မတူအောင်ပေး ပေးပါ။ မသကာ နောက်ဆုံးတစ်လုံးပဲလွဲလိုက်ပေါ့။

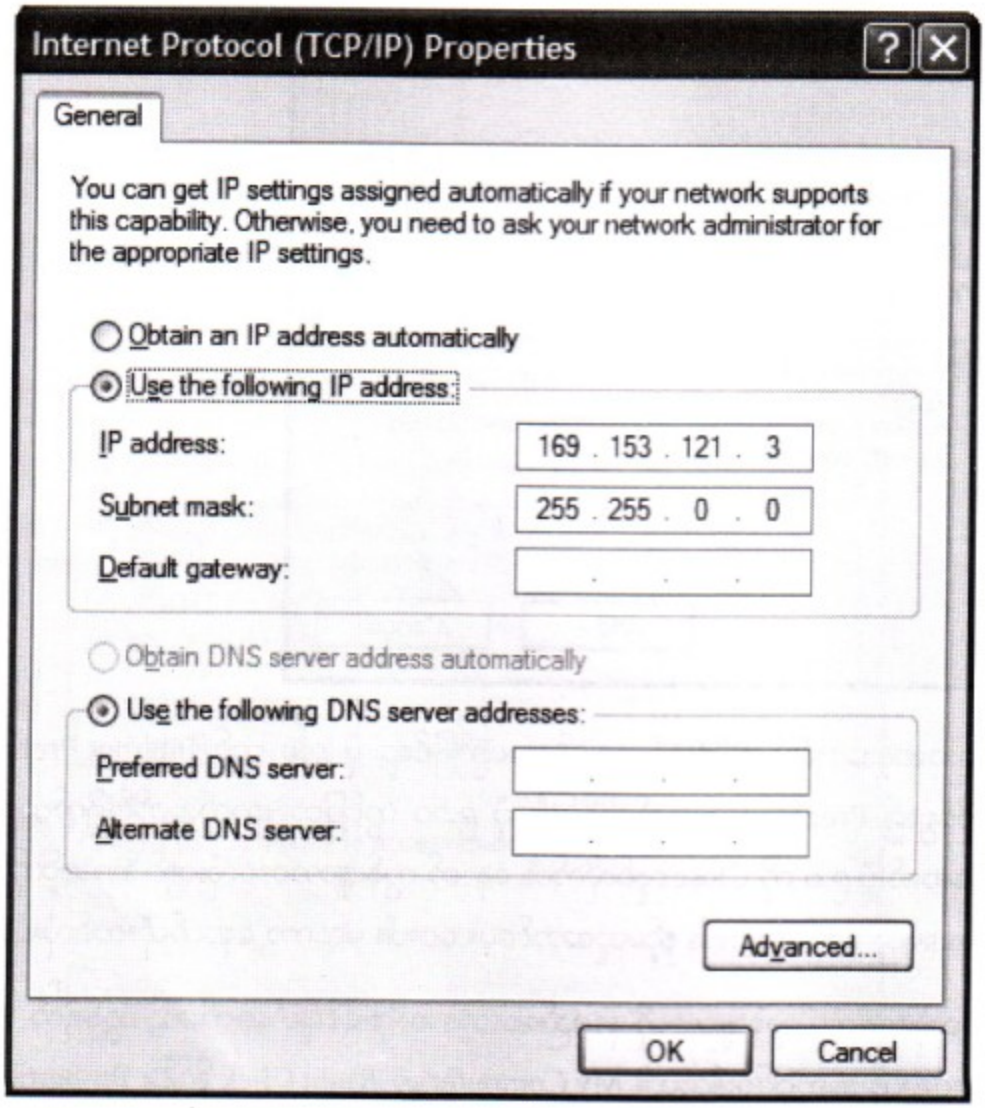
၉။ ဒီအဆင့်ကတော့ ကွန်ပျူတာကို နာမည်ပေးတဲ့အဆင့်၊ မိမိချိတ်ဆက်မယ့် ကွန်ရက် Workgroup ရဲ့ နာမည်ကိုပေးမယ့် အဆင့်ဖြစ်ပါတယ်။ My Computer မှာ Right Click နှိပ်ပြီး Properties လို့ပြောပါ။ ပြီးရင် Computer Name (Tab) ကိုသွားပါ။ ပုံ ၉.၁၁ ပေါ်လာပါလိမ့်မယ်။ ၎င်းတွင် Change Button ကိုနှိပ်ပါ။ ပုံ ၉.၁၂ ပေါ်လာပါလိမ့်မယ်။

၁၀။ ၎င်းတွင် ကွန်ပျူတာနာမည်ရော၊ Workgroup Name ရောပေးပါ။ ဥပမာ – ကွန်ပျူတာနာမည်က Sys1, Sys2, Bo, Aung, Aye စသည်ဖြင့်ပေါ့။ Workgroup Name ကတော့ များသောအားဖြင့်လုပ်ငန်းအဖွဲ့အစည်းနာမည်ပေးကြတာများပါတယ်။ ဥပမာ YOUTH ပေါ့။ ဒီနေရာမှာသိရမှာက ကွန်ပျူတာနာမည်က တစ်လုံးနှင့်တစ်လုံးမတူအောင်ပေးပါ။ Workgroup Name ကတော့တူရမယ်။ ကွန်ပျူတာအားလုံးမှာ Workgroup Name ကတစ်ခုပဲဖြစ်ရမယ်။ ကဲ Box တွေကို OK ပြောပြီးပြန်ထွက်ပါ။

၁၁။ လိုအပ်သော ဖိုင်များ ကော်ပီကူးဖို့ Windows XP CD တောင်းကောင်းတောင်းပါလိမ့်မယ်။ အားလုံးပြီးသွားရင် Restart လုပ်ပါ။ ပြန်တက်လာရင် နောက်တစ်လုံးကို ဒီအဆင့်တွေအတိုင်းလုပ်ပါ။ ပြီးရင် Win-

dows XP ကို Login လုပ်ပြီး နှစ်လုံးချိတ်မိ မမိကိုကြည့်ရအောင်။

ပုံ ၉.၁၀



၁၂။ ချိတ်မိ မမိကြည့်ဖို့ My Network Places ထဲကိုဝင်လိုက်ပါ။ အဲ့ဒီ အထဲကမှာ Entire Network ထဲကိုထပ်ဝင်ပါ။ ပြီးရင် Microsoft Windows Network ထဲကိုဝင်လိုက်ပါ။ အဲ့ဒီမှာ မိမိရဲ့ Workgroup Name ကိုတွေ့ရပါလိမ့်မယ်။ ပုံ ၉.၁၃ ကိုကြည့်။ အဲ့ဒါကိုထပ်ဝင်လိုက်မှ မိမိချိတ်ထားသော ကွန်ပျူတာနှစ်လုံးကိုတွေ့ရမှာပါ။ မတွေ့ရင် Refresh (F5) လုပ်ကြည့်ပါဦး။ တစ်ဖက်နှင့် တစ်ဖက် ဘယ်ကကြည့်ကြည့် နှစ်လုံးစလုံး (Hub နှင့်ကိုယ့်ချိတ်ထားရင်ချိတ်ထားသလောက်) တွေ့နေရပါ့မယ်။ သူက ချိတ်ထားတာမှန်ရင် မတက်ဘူးတို့ဘာတို့ မဖြစ်တတ်ဘူး။ တက်ကိုတက်ရမယ်။ အကယ်၍မတက်လျှင် လုပ်ခဲ့ပြီးသော အလုပ်များကို ပြန်စစ်ပါလေ။ ပြန်လုပ်ပါလေ။

ပုံ ၉.၁၃

চিত্র ৫.১১

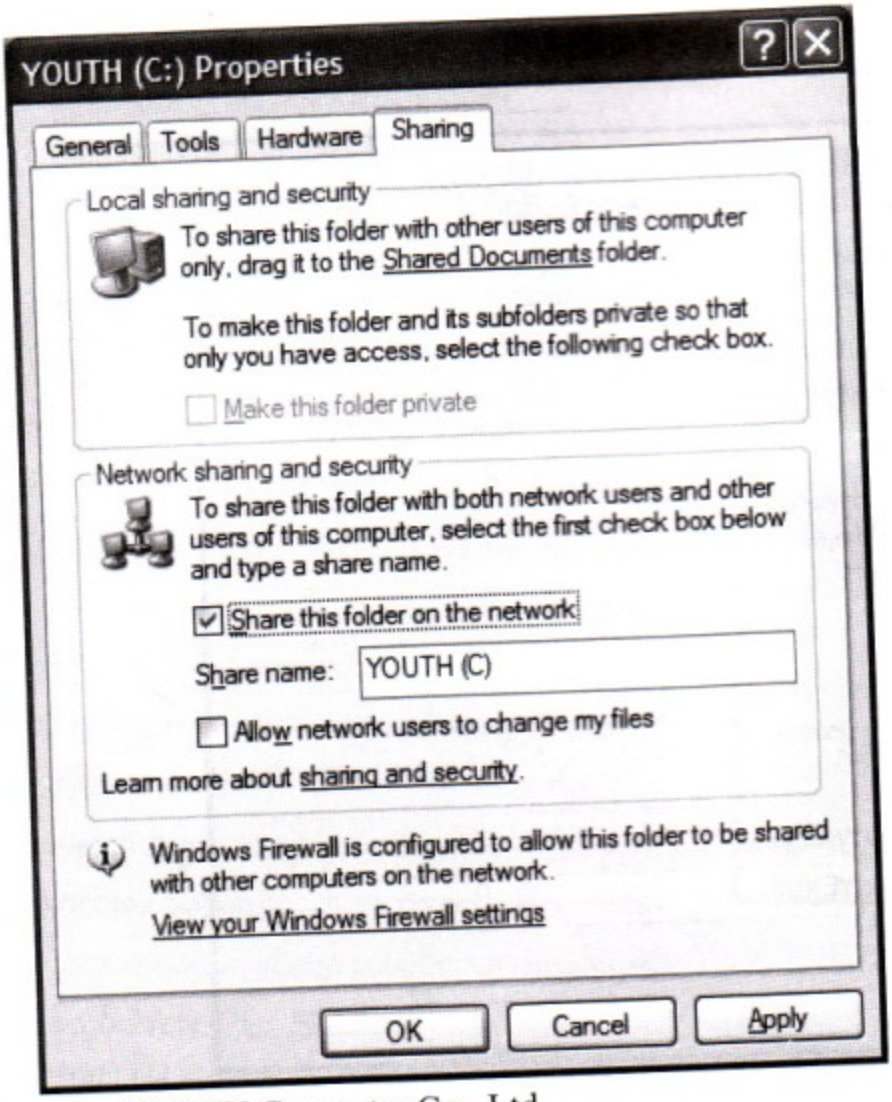
চিত্র ৫.১১

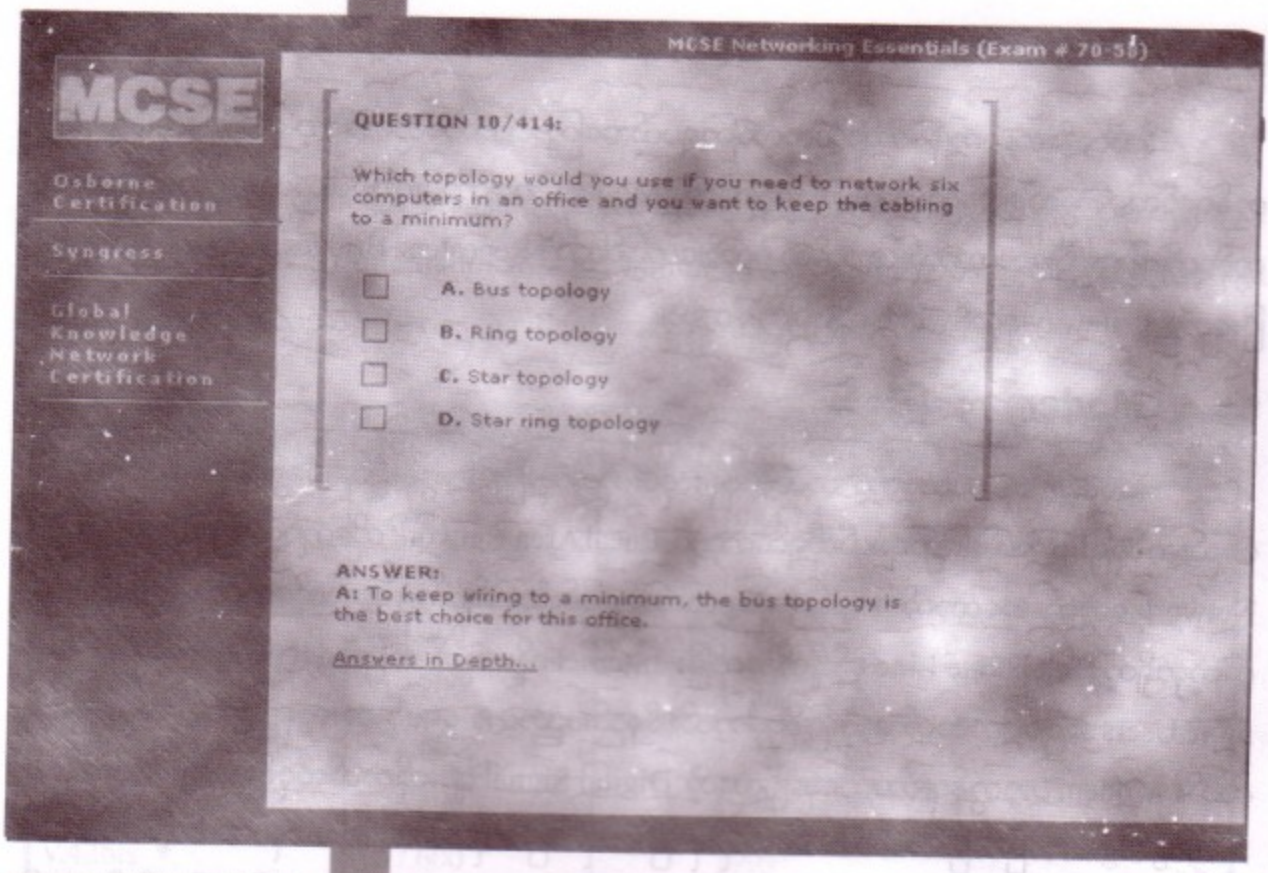
၉.၅ Share လုပ်ခြင်း

၁။ ကွန်ရက်ချိတ်ဆက်လိုက်တယ်ဆိုကတည်းက တစ်လုံးနှင့်တစ်လုံးအပြန်အလှန် Share လုပ်ချင်လို့မဟုတ်လား။ ဒီတော့ တစ်လုံးမှာရှိတဲ့ ကိုယ်ပေးသုံးချင်တဲ့အခန်းတွေကို ဒီမှမဟုတ် Hard Disk ကြီးတစ်ခုလုံးပေးသုံးချင်ရင်လည်း အောက်ပါအတိုင်း Share လုပ်ကြည့်ရအောင်။

၂။ ပထမတစ်လုံးတွင် My Computer ကိုဖွင့်ပါ။ Hard Disk C: ပေါ် နှိပ်ပြီး Sharing & Security လို့ပြောပါ။ ပေါ်လာသည့် Box တွင် If you understand risk etc., ဆိုတာကိုနှိပ်လိုက်ပါ။ ပုံ ၉.၁၄ ပေါ်လာပါလိမ့်မယ်။ ဝိုင်းထားတာကို On လိုက်ပါ။ ပြီးရင် OK ပြောပါ။ My Computer မှာ Hard Disk Icon တွင် လက်ကလေးပေါ်လာပြီးပါက Share လုပ်ပြီးသွားပါပြီ။ တဖက်ကွန်ပျူတာကနေပုံ ၉.၁၃ အတိုင်း ဝင်လာပြီး ချိတ်ထားသောမိမိထိုင်နေသည့် ကွန်ပျူတာမဟုတ်သည့် ကွန်ပျူတာ Icon လေးကို ဖွင့်လိုက်ပါက ယခု Share လုပ်ထားသော Hard Disk ကြီးပေါ်လာက အခြားစက်မှ ဖိုင်များကို ယူသုံး၍ရပြီဖြစ်သည်။

ပုံ ၉.၁၄





UNIT 10

Enterprise & Distributed Networks

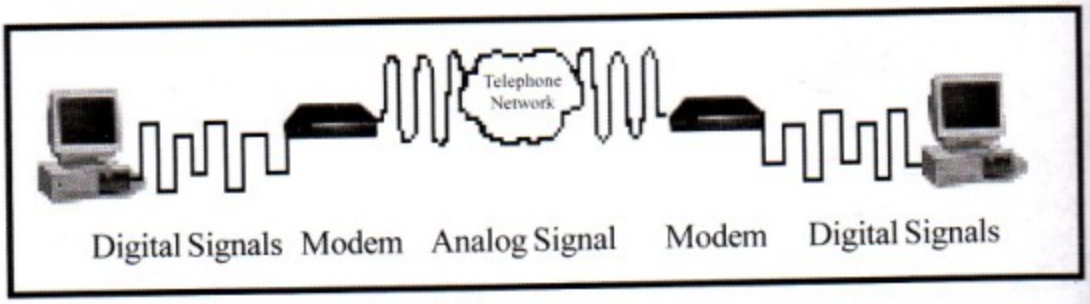
ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကြီးမားတဲ့ကွန်ပျူတာကွန်ရက်တွေကို ဘယ်လိုတပ်ဆင်ကြမလဲဆိုတဲ့အကြောင်းကို လေ့လာကြမှာဖြစ်ပါတယ်။ နည်းနည်းတော့ သိအိုရီဆန်မှာ ဖြစ်ပါတယ်။

ဒီသင်ခန်းစာမှာကျွန်တော်တို့လေ့လာကြရမယ့်အကြောင်းအရာတွေကတော့ ပထမဦးဆုံးအနေဖြင့် ကွန်ရက်ဆက်သွယ်ရေးတွေမှာအသုံးပြုနေကြတဲ့ Modem အကြောင်းပဲဖြစ်ပါတယ်။ နောက်ပြီးတော့ ကွန်ရက်အကြီးကြီးတွေမှာအသုံးပြုတတ်တဲ့ ပစ္စည်းတွေဖြစ်ကြတဲ့ Repeaters, Bridges, Routers, Brouters ပြီးတော့ Gateway နှင့် Switch တို့ဖြစ်ကြပါတယ်။

၁၀.၁ Modem အကြောင်း

Modem ဆိုတာကတော့ တယ်လီဖုန်းလိုင်းကိုအသုံးပြုပြီး ကွန်ပျူတာတွေကိုချိတ်ဆက်ပေးတဲ့ ပစ္စည်းတစ်ခုဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင်တော့ဗျာ Local Area Network ကိုကျော်လွန်ပြီးချဲ့ထွင်လိုက်တဲ့ Network တွေကို အထောက်အကူပေးတဲ့ပစ္စည်းတစ်ခုဖြစ်ပါတယ်။ ကျွန်တော်တို့တွေဟာ Modem ကို ကိုယ့်မှာရှိတဲ့ Telephone Line နှင့်ချိတ်ဆက်ပြီး Internet သို့မဟုတ် အခြား Network တစ်ခုကို Remote Users အဖြစ်ချိတ်ဆက်အသုံးပြုနိုင်ပါတယ်။ ဒီနည်းပညာဟာ ရေပန်းစားတဲ့နည်းတစ်ခုလည်းဖြစ်ပါတယ်။ Modem ဟာကွန်ပျူတာကနေရရှိလာတဲ့ Digital Signal များကိုတယ်လီဖုန်းလိုင်းပေါ်သို့တင်ရန် Analog Signal အဖြစ်ပြောင်းပစ်ပါတယ်။ ယခုလိုပြောင်းလိုက်ခြင်းကို Modulation လုပ်တယ်လို့ခေါ်ပါတယ်။ အဲ့ဒီလိုနဲ့ ကွန်ပျူတာတစ်လုံးကနေပို့လိုက်တဲ့ Signal တွေဟာ တယ်လီဖုန်းလိုင်းမှတဆင့် တစ်ဖက်ကိုရောက်ရှိသွားပြီး ၎င်းဖက်မှ Modem ကတယ်လီဖုန်းလိုင်းပေါ်မှ Analog Signal ကို ကွန်ပျူတာသို့ဝင်ရန် တစ်ဖန် Digital Signal သို့ပြန်လည်ပြောင်းပစ်ခြင်းကို Demodulation ဟုခေါ်ပါသည်။ ထိုကဲ့သို့ Modulation ဆိုသည့် ဖြစ်စဉ်နှင့် Demodulation ဆိုသည့်ဖြစ်စဉ်နှစ်ခုကိုပြုလုပ်ပေးခြင်းကြောင့် Modulator / Demodulator Modem ဟုခေါ်ခြင်းဖြစ်ပါတယ်။ Modem တွင် Internal Modem နှင့် External Modem ဟူ၍နှစ်မျိုးရှိပါသည်။ Internal Modem ဆိုတာကြတော့ Expension ကဒ်လေးသာမို့ကွန်ပျူတာရဲ့ Expension Slot လေးမှာစိုက်လိုက်ရုံပါပဲ။ External Modem ကြတော့သူ့ဘာသာသူကိုယ်ပိုင်သီးခြား Box တစ်ခုနဲ့ထွက်လာတာဗျ။ သူ့ကိုသီးခြား Power လည်းပေးရတယ်။ ကွန်ပျူတာနှင့်ဆက်သွယ်ဖို့ကြတော့ ကွန်ပျူတာဖက်မှ Serial Port ကို RS 232 Communications Interface ကိုအသုံးပြုပြီးချိတ်ဆက်တာဖြစ်ပါတယ်။ Internal Modem ဖြစ်စေ External Modem ဖြစ်စေ Standard တယ်လီဖုန်းကြိုးနှင့်ဆက်သွယ်နိုင်ရန် RJ-11 Connectors ကိုအသုံးပြုထားပါတယ်။ ဒါကတော့ Modem နှင့်ပတ်သက်လို့အခြေခံ သိထားသင့်တဲ့ အကြောင်းအရာတွေပဲဖြစ်ပါတယ်။

ပုံ ၁၀.၁



၁၀.၂ Modem Speed အကြောင်း

Modem ရဲ့ Data တွေ Transmit လုပ်နိုင်တဲ့နှုန်းကို Bit Per Second (bps) နှင့်တိုင်းတာပါတယ်။ အောက်မှာ ITU လို့ခေါ်တဲ့ International Telecommunications Union ကထုတ်လုပ်ခဲ့သော Modem Speed ကိုသတ်မှတ်သည့် V-Series Standards အချို့ကိုဖော်ပြပေးထားပါတယ်။

Standard	bps	Year Introduced
V.22 bis	2400	1984
V.32	9600	1984
V.32bis	14,400	1991
V.32ter	19,200	1993
V.FastClass (V.F.C)	28,800	1993
V.34	28,800	1994
V.42bis	57,600	1995
V.90	115,200	1998

အဲ့ဒီဇယားမှာတွေ့ရတဲ့ Bis နှင့် Ter ဆိုတာ ပြင်သစ်ဘာသာစကားဖြစ်ပါတယ်။ Bis ဆိုတာက Second လို့အဓိပ္ပါယ်ရပြီး Ter ကတော့ Third လို့အဓိပ္ပါယ်ရပါတယ်။ ဆိုလိုချင်တာကတော့ အဲ့ဒီမှာကြည့်လိုက်ပါ။ V-32 bis ဆိုတာက V-32 ၏ဒုတိယ Version လို့အဓိပ္ပါယ်ရတယ်။ အဲ့ဒီဇယားကိုကြည့်ပြီး ပြောရမယ်ဆိုရင် V-22 bis ဟာစာလုံးတစ်ထောင်ရှိတဲ့ စာတစ်စောင်ကို Transmit လုပ်မယ်ဆိုရင် 25 Seconds အချိန်ယူပြီးတော့ V-34 Modem ဟာဆိုရင်ဖြင့် ၎င်းစာစောင်ကို 2 Second နှင့် Transmit လုပ်နိုင်ပါတယ်။ V-42 bis Modem ဆိုရင်တော့ ၎င်းကို 1 Second နှင့် Transmit လုပ်နိုင်ပါတယ်။

တကယ်တော့ Modem ရဲ့ Speed ကိုတိုင်းတာတဲ့ အခေါ်အဝေါ်တစ်ခုရှိပါတယ်။ အဲ့ဒါကတော့ Baud Rate ပဲဖြစ်ပါတယ်။ Baud ဆိုတာ 1 bit သာရှိတဲ့ အချက်အလက်ကိုသယ်ဆောင်သွားသော အသံလှိုင်းတစ်ခုပဲဖြစ်ပါတယ်။ အရင်ခေတ်တုန်းက Modem တွေမှာဆိုရင် ဒီ Baud ဆိုတဲ့အခေါ်အဝေါ်နဲ့ bps ဆိုတာကို လဲလှယ်ပြီးသုံးနိုင်ပါတယ်။ ဆိုလိုချင်တာက နှစ်ခုက အတူတူပဲပေါ့ဗျာ။ ပြောရမယ်ဆိုရင် 300 bps ရှိတဲ့ Modem ဟာ 1 Second မှာ လှိုင်းပေါင်း 300 ဖြစ်ပေါ်နေပါတယ်။ ဒါပေမဲ့ ခုနောက်ပိုင်း Modem တွေကြတော့ Compression နည်းပညာကိုအသုံးပြုထားတာကြောင့် 1 Second မှာရှိတဲ့ လှိုင်းအရေအတွက်ထက် 1 Second မှာပေးပို့တဲ့ bps က ပိုများလာပါတယ်။ ဥပမာပြောရရင်ဖြင့် 28,800 bps Transmit လုပ်နိုင်တဲ့ Modem တစ်ခုဟာ တကယ်တမ်း Baud Rate နဲ့ ပြောမယ်ဆိုရင် 9600 Baud သာရှိပါတယ်။

၁၀.၃ Modem အမျိုးအစားများ

ယနေ့ခေတ်မှာ အသုံးပြုနေတဲ့ Modem အမျိုးအစားနှစ်မျိုးရှိပါတယ်။ အဲဒါတွေကတော့-

(1) Asynchronus နှင့်

(2) Synchronous တို့ ဖြစ်ကြပါတယ်။

ဘယ်ဟာကို အသုံးပြုသင့်သလဲဆိုတာတော့ သင်အသုံးပြုမယ့် တယ်လီဖုန်းလိုင်းနှင့် Network ရဲ့ တောင်းဆိုမှုတွေအပေါ် မူတည်မှာဖြစ်ပါတယ်။

၁၀.၄ Asynchronous အကြောင်း

Asynchronous ဆက်သွယ်ရေးဆိုတာ Modem ကိုအသုံးပြုပြီး ဆက်သွယ်ကြတဲ့အထဲမှာ ရေပန်းစားဆုံးနည်းလမ်းတစ်ခုဖြစ်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ သူကပုံမှန်တယ်လီဖုန်းလိုင်းကို အသုံးပြုထားလို့ပါပဲ။ Asynchronous Modem ဟာ Data byte တစ်ခုချင်းစီကို 1 နှင့် 0 အဖြစ်ပြောင်းလဲ စီတန်းထားပါတယ်။ ပုံမှာလည်းပြထားပါတယ်။ အဲဒီမှာ Start နှင့် Stop bits ဆိုတာ byte တစ်ခုနှင့် တစ်ခုကြား ခြားထားတာပဲ ဖြစ်ပါတယ်။ ၎င်း Start နှင့် Stop bits Sequence ကိုပေးပို့သူရော လက်ခံသူဘက်ကပါ သဘောတူညီထားဖို့ လိုအပ်ပါတယ်။

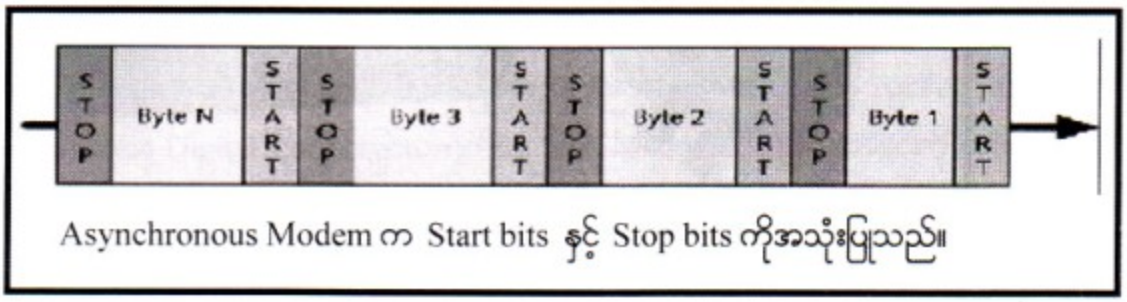
Asynchronous ဆက်သွယ်ရေးလို့ပြောတဲ့အတိုင်းပါပဲ။ ကွန်ပျူတာနှစ်လုံးကြား ဆက်သွယ်မှုဟာ Synchronize ဖြစ်ခြင်းမရှိပါဘူး။ ဆိုလိုတာက သူ့မှာချိန်ကိုက်ပြီးလုပ်ဆောင်မှုတွေမရှိပါဘူး။ ပေးပို့တဲ့ဘက်က ကွန်ပျူတာက Data တွေကို စီတန်းပြီးအဆက်မပြတ်ပေးပို့နေပြီး လက်ခံတဲ့ကွန်ပျူတာက Data တွေကို လက်ခံပြီး ဘာတွေပို့လိုက်သလဲဆိုတာကို ပြန်လည်စစ်ဆေးပါတယ်။

Modem အများစုဟာ သူ့ကိုတွေ့ရှိတဲ့ Error တွေကို မှန်အောင်ပြုလုပ်ပေးပါတယ်။ အများစစ်ဆေးရန်အတွက် Data Byte တစ်ခုချင်းစီရှိတဲ့ Start နှင့် Stop bits တွေမှာရှိတဲ့ Parity bit ပါရှိပါတယ်။ Data တွေကိုပေးပို့တဲ့ ကွန်ပျူတာဟာ ၎င်းပေးပို့လိုက်တဲ့ Data Stream မှာ Data ပါဝင်မှုကိုရေတွက်ပါတယ်။ အကယ်၍ ပါဝင်မှုဟာ 'မ' ဂဏန်းဖြစ်နေရင် Parity Bit ကို one (1) အဖြစ်သတ်မှတ်ပါတယ်။ လက်ခံတဲ့ဘက်က ကွန်ပျူတာကလည်း ၎င်းလက်ခံရရှိတဲ့ Data ကိုပြန် Count လုပ်ပါတယ်။ 'မ' ဂဏန်းလား 'စုံ' ဂဏန်းလားပြန်စစ်ပါတယ်။ ပြီးရင် Parity Bit နှင့် ပြန်တိုက်ပြီးစစ်ပါတယ်။ ကိုက်ညီတယ်ဆိုရင် Data တွေကောင်းမွန်စွာရောက်ရှိပါတယ်။ အဲသလိုမှမဟုတ်ရင်တော့ Modem က Data တွေကို ပြန်လည်ပေးပို့ခိုင်းပါတော့တယ်။

Modem အများစုဟာ သူတို့ရဲ့ Data ပေးပို့မှု Transmission မှာပြန်ဆန်တဲ့ Transmission Speed ရရှိစေဖို့ Data Compression လုပ်ကြပါတယ်။ ၎င်း Data Compression Standard တွေထဲက အများဆုံး ဘုံ သုံးဖြစ်တဲ့တစ်ခုကတော့ Microcom ရဲ့ MNP Class 5 ပဲဖြစ်ပါတယ်။ အကယ်၍များ

နှစ်ဖက်စလုံးက Modem နှစ်ခုစလုံးဟာ MNP 5 ကို အသုံးပြုခဲ့မယ်ဆိုရင် Data ပေးပို့တဲ့ အချိန်တစ်ဝက် လောက်လျော့ချပစ်နိုင်ပါတယ်။

ပုံ ၁၀.၂



Asynchronous Modem က Start bits နှင့် Stop bits ကိုအသုံးပြုသည်။

၁၀.၅ Synchronous Modem အကြောင်း

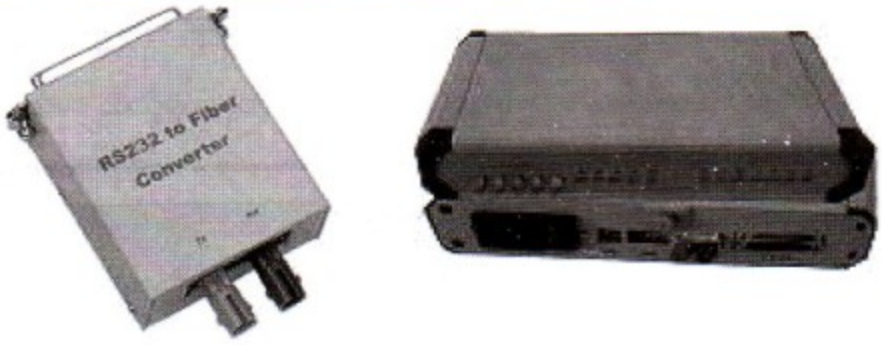
Asynchronous Modem ဟာ Data စီးကြောင်းတစ်ခုတွင် Data များ ဘယ်ကစပြီး ဘယ်မှာဆုံးသည်ကို Start bit နှင့် Stop bit ကို ကြည့်၍ဆုံးဖြတ်သော်လည်း Synchronous Modem ကြတော့ Timing ပေါ်မူတည်၍အလုပ်လုပ်သည် ဆက်သွယ်မှုတစ်ခုတစ်ခုက်ရှိ Modem နှစ်ခုဟာ Data များကို Frame တုခေါ်သည့် အစုလိုက် အုပ်စုများဖွဲ့၍ပေးပို့ခြင်းတွင်ချိန်ကိုက်၍အလုပ်လုပ်ဆောင်ကြသည်။ လွယ်လွယ်ပြောရရင်တော့ တိုဘက် Modem နှင့် ဒီဘက် Modem Timing ကိုက်၍ အလုပ်လုပ်ခြင်းကို ဆိုလိုခြင်းဖြစ်သည်။ နည်းပညာစကားအရပြောရရင်တော့ Communication ဖြစ်စေဖို့ Modem နှစ်ခုဟာ Synch ကိုက်နေဖို့လိုပါတယ်။ Synchronous Modem ဟာ Timing မှန်ကန်စေရန် သတ်မှတ်ထားတဲ့ Data Frame အုပ်စု တစ်စုနှင့်တစ်စုကြားမှာ Synch bit ကိုထည့်သွင်းထားပါတယ်။ ပုံတွင်လည်းတွေ့မြင်နိုင်ပါတယ်။ အကယ်၍များ Data ပို့နေစဉ် Error တွေ့ခဲ့မယ်ဆိုရင်တော့ Modem ဟာ Frame တွေကို ပြန်ပို့ပေးပါလို့ပြောလိုက်ရုံပါပဲ။ Synchronous Modem တွေဟာ Error Checking နှင့် ပတ်သက်လို့ခေါင်းသိပ်စားစရာမရှိတဲ့ အတွက်ကြောင့်မို့လို့ Data တွေကိုသယ်ယူပို့ဆောင်ရာမှာ Asynchronous Modem ထက်စာရင် သိသိသာသာ ပိုမြန်ပါတယ်။ အဲ့ဒီအပြင် Synchronous Protocol ဟာ Asynchronous Communication ထဲမှာမရှိတဲ့ Function အချို့ကိုလည်း ပံ့ပိုးပေးထားပါတယ်။ ဆိုလိုတာက Data တွေကို Block တွေအဖြစ်ပြုလုပ်ပေးတယ်။ ထိန်းချုပ်မှုအတွက်လိုအပ်တဲ့ အချက်အလက်တွေ ထည့်သွင်းပေးတယ်။ အမှားစစ်ဆေးဖို့အတွက် လိုအပ်တဲ့ အချက်အလက်တွေထည့်သွင်းပေးတယ် စသဖြင့် ပေါ့။ Synchronous ဆက်သွယ်ရေးမှာ အဓိကအားဖြင့် Synchronous Protocol သုံးမျိုးရှိပါတယ်။ အဲ့ဒါတွေကတော့ -

(၁) SDLC လို့ခေါ်တဲ့ Synchronous Data Link Control

(၂) HDLC လို့ခေါ်တဲ့ High Level Data Control

(၃) Bisync ဆိုတဲ့ Binary Synchronous Communication Protocol တို့ဖြစ်ကြပါတယ်။

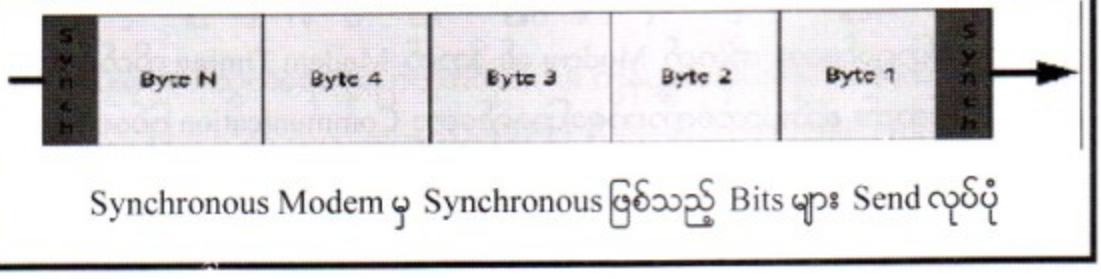
ပုံ ၁၀.၃



Asynchronous Modem နှင့် Synchronous Modem ကိုတွေ့ရစဉ်

Synchronous Modem တွေဟာ သာမန် Phone Line တွေနဲ့ အသုံးပြုလို့မရပါဘူး။ ၎င်းတို့ဟာ Dedicated လို့ခေါ်တဲ့ Lease Line တွေမှာအသုံးပြုဖို့ထုတ်လုပ်ထားတာဖြစ်ပါတယ်။ ဒီအချက်အလက်တွေကြောင့်ရယ် ဈေးကြီးတဲ့ပစ္စည်းတွေကိုအသုံးပြုကြရတာကြောင့်ရယ် Synchronous Communication မှာ Asynchronous ထက်စာရင် ကုန်ကျစရိတ်ပိုများပါတယ်။

ပုံ ၁၀.၄



Synchronous Modem မှ Synchronous ဖြစ်သည့် Bits များ Send လုပ်ပုံ

၁၀.၆ Digital Modem အကြောင်း

ယခုအခါ လျှင်မြန်စွာခေတ်စားလာသော Modem နောက်တစ်မျိုးကတော့ Digital Modem ပဲဖြစ်ပါတယ်။ တကယ်တော့ Modem ဆိုတာ Digital Signal ကနေ Analog Signal ကိုပြောင်းပေးသော ပစ္စည်းဖြစ်တာကြောင့် ဒီ Modem ကို Digital Modem ဟုခေါ်ဆိုခြင်းက တစ်မျိုးကြီးဖြစ်နေတာပေါ့ဗျာ။ ဆိုလိုတာက Modem ပါဆိုမှ Digital Modem ဆိုပြီးရှိသေးသလား။ ဒါမျိုးပြောစရာဖြစ်နေပါတယ်။ သူက ISDN လို့ခေါ်တဲ့ Indegrated Services Digital Network အတွက် Interface ပါတာကြောင့် ၎င်း Interface ကိုရည်ညွှန်းပြီး Digital Modem ဟုခေါ်ဆိုရခြင်းဖြစ်ပါတယ်။ နားလည်အောင်ထပ်ပြောရမယ်ဆိုရင်တော့ ISDN အတွက် အသုံးပြုတဲ့ Interface ကို ရံဖန်ရံခါ Digital Modem ဟုခေါ်ဆိုခြင်းဖြစ်ပါတယ်။ အဲ့ဒီမှာ ISDN အတွက် အသုံးပြုတဲ့ Adapter မှာ NT လို့ခေါ်တဲ့ Network Termination ပစ္စည်းနဲ့ TA လို့ခေါ်တဲ့ Terminal Adapter ပစ္စည်းစသည့်တို့ပါရှိပါတယ်။ ဒါပေမယ့်လည်းဗျာ လူတွေကတော့ အဲ့ဒီ

NT/ AT ပစ္စည်းကြီးကို Modem လို့ပဲခေါ်ဆိုနေကြတုန်းပါပဲ။

၁၉၉၈ ခုနှစ်ကတည်းက Cable Television နှင့် ဆက်သွယ်ရေးကုမ္ပဏီတွေဟာ ISDN နှင့် SOHO လို့ခေါ်တဲ့ Small Office/ Home Office တွေမှာအသုံးပြုတဲ့ အခြေခံကြေးလှတဲ့ Asynchronous Modem တွေကို High Speed Digital Connections များနှင့် အစားထိုးနိုင်ခဲ့ကြပါတယ်။ ဒီတော့ အပေါ်ကပြောခဲ့တဲ့ အကြောင်းအရာနှစ်ခုစလုံးမှာ အသုံးပြုတဲ့နည်းပညာဟာ Digital ကနေ Analog ပြောင်းခြင်း သို့မဟုတ် Analog ကနေ Digital သို့ပြောင်းခြင်းမဟုတ်သည့်တိုင် Modem ဆိုတဲ့အခေါ်အဝေါ်ကိုသုံးစွဲနေခြင်းပဲ ဖြစ်ပါတယ်။

၁၀.၃ သယ်ယူဆောင်ပေးမည့် Carriers များ

Remote Network Communication အတွက် Modem နှင့် Connection ရွေးချယ်မှုဟာ အောက်ပါအချက် (၃) ချက်ပေါ်မူတည်နေပါတယ်။ အဲဒါကတော့ -

(၁) Througput ဆိုတဲ့ ပေးပို့နိုင်တဲ့အမြန်နှုန်း

(၂) Distance ဆိုတဲ့ အကွာအဝေး

(၃) Cost ဆိုတဲ့ ကုန်ကျစရိတ်တို့ပဲဖြစ်ပါတယ်။

ဆိုလိုတာက ကျွန်တော်တို့ဟာ Network အတွက် ဘယ် Carrier ကိုအသုံးပြုမလဲဆိုတာ အထက်ပါ အချက် (၃) ချက်ပေါ်မူတည်ပြီး စဉ်းစားရမှာဖြစ်ပါတယ်။ ဒီတော့ ရွေးချယ်စရာ ဘယ်နှစ်ခုရှိသလဲဆိုတော့ လေးမျိုးရှိပါတယ်။ PSTN ဆိုတဲ့ Publish Switched Telephone Network ကိုအသုံးပြုပြီးရရှိတဲ့ ဒီလေးမျိုး ကတော့ -

(၁) Dial-Up

(၂) ISDN ဆိုတဲ့ Integrated Services Digital Network

(၃) DSL ဆိုတဲ့ Digital Subseriber Line

(၄) Dedicated Leased Line တို့ဖြစ်ကြပါတယ်။

Dial-UP Connections အခြေခံ

Dial-Up Connections ဟာ ကျွန်တော်တို့အသုံးပြုလိုတဲ့ Network ကိုလက်ရှိကိုယ့်မှာရှိနေတဲ့ တယ်လီဖုန်းလိုင်းကိုအသုံးပြုပြီး ယာယီ Connection ပြုလုပ်လိုက်တာပဲဖြစ်ပါတယ်။ Line ရဲ့အရည်အသွေး ဟာတစ်သတ်မတ်တည်းမရှိဘဲ ပြောင်းလဲသလို၊ Communication Speed ဟာလည်း 28, 800 bps အထိပဲရနိုင်ပါတယ်။ နောက်ပိုင်းမှာတော့ နည်းပညာအသစ်တွေပေါ်လာပြီး အချို့လိုင်းတွေမှာ 56 Kbps အထိရပါတယ်။ အချို့သောစမ်းသပ်မှုတွေမှာ Speed ဟာ 115 Kbps အထိရတယ်ဆိုပေမယ့် ဒါဟာ ယနေ့ခေတ်မှာ ကျယ်ပြန့်စွာအသုံးမပြုနိုင်သေးပါဘူး။

Integrated Services Digital Network အကြောင်း

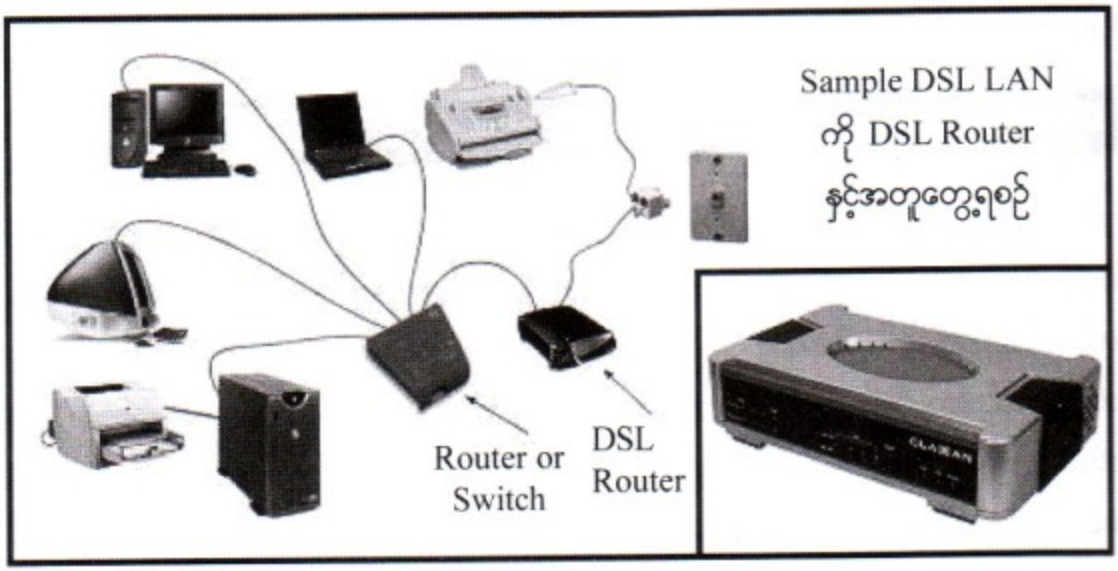
ISDN ဟာ Digital Phone Line ကိုအသုံးပြုပြီး အသံနှင့်အချက်အလက်များကို Transmit လုပ်နိုင်တဲ့ Dial-Up ပဲဖြစ်ပါတယ်။ BRI လို့ခေါ်တဲ့ Basic Rate Interface ISDN ဟာ အသံနှင့်အချက်အလက်တွေအတွက် 64 Kbps ရှိတဲ့ B-Channel နှစ်ခုနှင့် Signal Control အတွက် 16 Kbps ရှိတဲ့ D-Channel တစ်ခုပါရှိပါတယ်။

Primary Rate Interface ဆိုတဲ့ PRI ISDN ကြတော့ B Channel 23 ခုထိရရှိပြီး D-Channel ကတော့ တစ်ခုပါရှိပါတယ်။ ၎င်းဟာအဓိကအားဖြင့် WAN ချိတ်ဆက်မှုအတွက်အသုံးပြုပါတယ်။ ISDN ဟာ Digital Phone Line ရှိဖို့လိုအပ်တယ်ဆိုပေမယ့် ကုမ္ပဏီတော်တော်များများကတော့ ၎င်းကို Remote Offices ပေါ့။ ရုံးခွဲတွေနှင့်ချိတ်ဆက်တဲ့နေရာမှာ အသုံးပြုကြပါတယ်။ BRI ISDN ရဲ့ B Channel နှစ်ခုဟာ အလွယ်တကူပေါင်းစည်းလို့ရတာကြောင့် 128 Kbps အမြန်နှုန်းအထိရရှိသွားပြီး ပုံမှန် Standard Dial-Up Connection ထက်ပို၍ Bandwidth ကောင်းပါတယ်။

Digital Subscriber Line အကြောင်း

DSL Connections ဆိုတာ ကုန်ကျစရိတ်နည်းနည်းနှင့် အလယ်အလတ်သော Bandwidth ရရှိတဲ့ အားလုံးသော Digital Services တွေကိုကိုယ်စားပြုပါတယ်။ DSL Connectors တွေဟာ Bandwidth ကိုငွေနှင့်ဝယ်ယူရသလိုပါပဲ။ ဥပမာပြောရရင် 384 Kbps ရှိတဲ့ Upstream Connection (အသုံးပြုသူမှ Remote Connection ကိုပြောတာ) နှင့် Downstream Connection (Remote Connection မှအသုံးပြုသူဆီသို့) ဆိုရင် တစ်လကို ဒေါ်လာ ဒေါ်လာကျမယ်ဆိုရင် 1.5 Mbps Upstream နှင့် Downstream Connection ဆိုရင် ဒေါ်ဆက်ပိုကျပါတယ်။

ပုံ ၁၀.၅



Produced by YOUTH Computer Co., Ltd

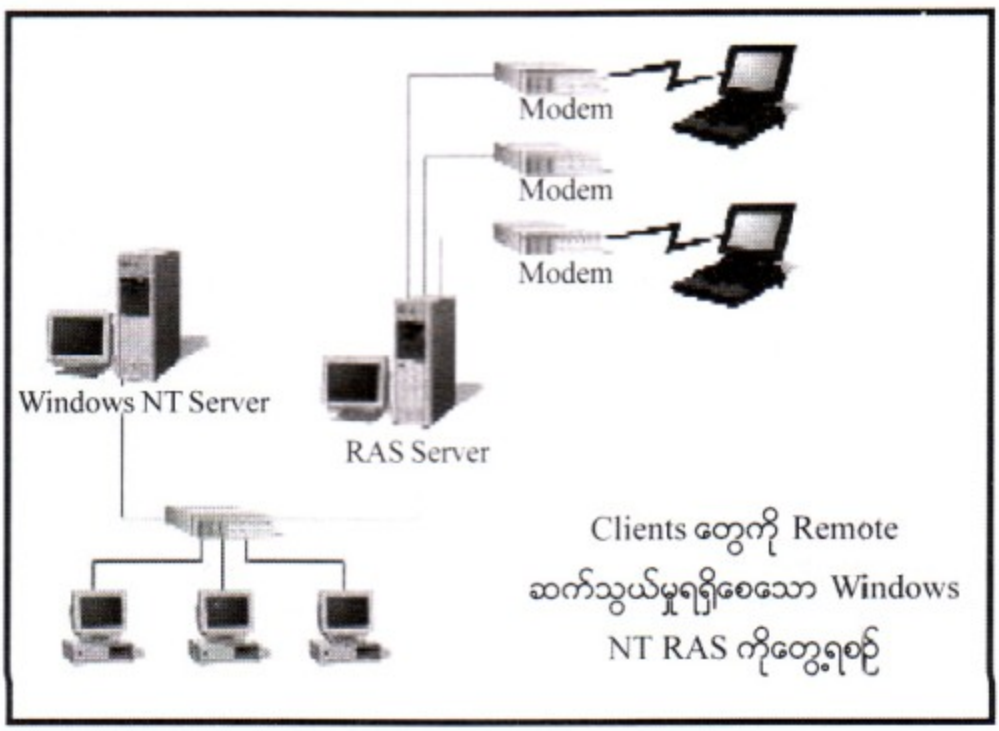
Dedicated Leased Line အခြေခံများ

Dedicated Leased Line ဟာအသုံးပြုသူနှစ်ဖက်ကို Continuous Connections ပံ့ပိုးပေးနိုင်ပါတယ်။ အခြားသော Connectors တွေထက်ပိုပြီးတော့ဈေးကြီးတယ်ဆိုပေမယ့် Speed ကတော့အတော်လေးကောင်းပါတယ်။ 56 Kbps ကနေ 45 Mbps အထိတောင်ရပါတယ်။

၁၀.၈ Remote Access Networking အခြေခံများ

ကျွန်တော်တို့တပ်ဆင်ထားတဲ့ ကွန်ရက်ကိုဒီထက်ပိုပြီး အကျိုးရှိစွာအသုံးချချင်တယ်ဆိုရင်တော့ ဒီလုပ်ငန်းခွင်က ကွန်ရက်ကိုအသုံးပြုသူသည် အလုပ်ကနေမဟုတ်ဘဲ ၎င်း၏နေအိမ်ကနေသော်လည်းကောင်း၊ Marketing ဆင်းနေစဉ် ရုံးချုပ်ကိုပြန်ဆက်သွယ်လိုလျှင်သော်လည်းကောင်း အစရှိသဖြင့်ပေါ့ဗျာ။ အခြားတစ်နေရာကနေ ရုံးမှာရှိတဲ့ကွန်ရက်ကို Dial-in ဆိုပြီးဆက်သွယ်လို့ရတယ်ဗျာ။ ဘယ်လိုဆက်သွယ်ရမလဲဆိုတော့ Microsoft Windows NT ရဲ့ Windows NT Remote Access Services (RAS) ဒါမှမဟုတ် Windows 2000 ရဲ့ Routing and Remote Access Services (RRAS) စတာတွေကိုအသုံးပြုနိုင်ပါတယ်။

ပုံ ၁၀.၆



Windows NT မှာဖြစ်စေ၊ Windows 2000 Server မှာဖြစ်စေ Remote Services ဟာ Remote Client (အဝေးမှလှမ်းအသုံးပြုသူ) ၂၅၆ခုအထိခွင့်ပြုပါတယ်။ ပုံမှာ Windows NT RAS ကိုပြထားပါတယ်။ Windows 2000 မှာဆိုရင်တော့ RRAS မှာ Routing Software ဆိုတာပါရှိပြီး ၎င်းဟာ Server ကို Low-End Routing Device အနေဖြင့်အလုပ်လုပ်ဆောင်နိုင်စေပါတယ်။ အဲဒီအပြင် RRAS မှာ Lo-

cal-Area အတွင်းလမ်းကြောင်းလွဲပေးတဲ့ Routing Services ပါရှိပါတယ်။ ဒါကြောင့်တစ်ခု သို့မဟုတ် တစ်ခုထက်ပိုတဲ့ Local Connection ဖြစ်စေ၊ Remote Connection ဖြစ်စေ Route လုပ်ပေးနိုင်စွမ်းရှိပါတယ်။

RAS ဖြစ်စေ RRAS ဖြစ်စေတစ်ခုခုကိုသုံးပြီး Network ကိုလှမ်းချိတ်တဲ့အခါ အဲဒီ User တာသာမန် Telephone Line ကိုအသုံးပြုပြီးချိတ်ဆက်နိုင်ပါတယ်။ အဲဒီလိုချိတ်ဆက်လိုက်လို့ Connection မိသွားပြီဆိုတာနှင့် လှမ်းချိတ်တဲ့ကွန်ပျူတာဟာ ဒီ Network မှာတိုက်ရိုက်ချိတ်ဆက်ထားသလိုမျိုး ဖြစ်သွားပါတယ်။ ဒါပေမယ့် နည်းနည်းတော့နေးပါတယ်။ နောက်ထပ်ပြောပြစရာရှိတာက RAS ရော RRAS ရောဟာ အင်တာနက်ကိုအသုံးပြုပြီးဝင်တဲ့ Virtual Dial-in Connections ကိုလည်းပံ့ပိုးပေးပါတယ်။ အသုံးပြုသူဟာ Server တစ်ခုကို Virtual Dial-in Connection နှင့်ချိတ်ဆက်ဖို့ရာသူဟာ ISP ဆိုတဲ့ Internet Service Provider နှင့်လှမ်းချိတ်ဆက်ပြီး ၎င်း ISP နှင့်ချိတ်ဆက်ထားသော Server ကို Virtual Dial-in Connection ပြုလုပ်လိုက်တာပါ။ ဒီ RAS ဖြစ်စဉ်ကို Client အသုံးပြုသူဖက်ကကြည့်မယ်ဆိုရင် ဒီ RAS ကိုသုံးဖို့ Client ဟာ သူသုံးနေတဲ့ Operating System ပေါ်မူတည်ပြီး Program နှစ်မျိုးဖြင့် Connection ပြုလုပ်နိုင်ပါတယ်။ တစ်ခုက Client ဟာ Operating System ကို Windows NT 3.51 ဒါမှမဟုတ် Windows for Workgroups ကိုသုံးထားမယ်ဆိုရင် RAS Client ဆိုတဲ့ Program ကိုသုံးပြီး RAS Connection ပြုလုပ်ရမှာဖြစ်ပါတယ်။ အကယ်၍များ Client ဟာ Windows 2000, Windows NT 4.0, Windows Mollennium, Windows 98 ဒါမှမဟုတ် Windows 95 စသည့်တစ်ခုခုကိုအသုံးပြုထားမယ်ဆိုရင်တော့ DUN ဆိုတဲ့ Dial-Up Networking Software ကိုသုံးပြီး RAS Connection ပြုလုပ်ရမှာဖြစ်ပါတယ်။ ကဲဆက်ပြီးကြည့်ရအောင်။ ဒီ RRAS အတွက်ပဲဖြစ်စေ၊ RAS အတွက်ဖြစ်စေ၊ DUN အတွက်ဖြစ်စေပေါ့နော်။ ဒီ Remote Access အတွက် Protocol နှစ်မျိုးရှိပါတယ်။ အဲဒါတွေကတော့ -

(၁) SLIP ဆိုတဲ့ Serial Line Internet Protocol

(၂) PPP ဆိုတဲ့ Point-to-Point Protocol တို့ဖြစ်ကြပါတယ်။

Serial Line Internet Protocol (SLIP) အကြောင်း

SLIP ဆိုတာဟာ အရင်တုန်းကကွန်ပျူတာတွေဟာ Modem ကိုအသုံးပြုပြီး အင်တာနက်ကိုချိတ်ဆက်တဲ့အခါ အသုံးပြုတဲ့ Older Protocol တစ်ခုပဲဖြစ်ပါတယ်။ မရှိမဖြစ်လိုအပ်တဲ့ Physical Layer Protocol တစ်ခုဖြစ်ပြီး ၎င်းဟာ Error Connection မပါတဲ့တယ်လီဖုန်းလိုင်းက ဆက်သွယ်မှုတစ်ခုပဲဖြစ်ပါတယ်။ SLIP ဟာ Error Checking နှင့် Connection ကိစ္စတွေမှာ Hardware ပေါ်မှီခိုနေတဲ့အပြင် TCP/IP Connection တစ်ခုပဲ Support လုပ်ပါတယ်။ နောက်ပြီး Address တွေဘာတွေ မလိုအပ်ဘူးဗျ။ ဘာလို့ လည်းဆိုတော့ ကွန်ပျူတာနှစ်လုံးကိုပဲ ချိတ်ဆက်တာကြောင့်ဖြစ်ပါတယ်။ SLIP ရဲ့ပံ့မှန်လုပ်ဆောင်မှုမှာ

Compression လုပ်ပေးနိုင်စွမ်းမရှိပေမယ့် CSLIP ဖြစ်တဲ့ Compressed SLIP မှာတော့ Compression လုပ်ပေးနိုင်ပါတယ်။

Point-to-Point Protocol (PPP) အကြောင်း

PPP ဆိုတာကတော့ SLIP ထက်စာရင် ကွန်ပျူတာတွေကိုချိတ်ဆက်ရာမှာပိုပြီးတော့ Dynamic ဖြစ်ပါတယ်။ တရားသေမဟုတ်ဘူးပေါ့ဗျာ။ SLIP နှင့် PPP အကြား အဓိကကြီးကြီးမားမားကွာခြားတဲ့အချက်ကတော့ PPP က Physical ရော Data Link အလွှာပါနှစ်ခုစလုံး Support လုပ်ပြီးတော့ ၎င်း PPP ဟာ Modem ကို Network Card လိုပုံစံမျိုးပြောင်းပစ်ပြီး အလုပ်လုပ်စေနိုင်ပါတယ်။ ဒါကြောင့် PPP ဟာ SLIP လို TCP/IP ပဲ Support လုပ်တာမဟုတ်တော့ဘဲ Protocol တွေတစ်ခုမက Support လုပ်လာနိုင်ပါတယ်။ PPP ဟာ IP, IPX နှင့် NetBEUI စသည်ဖြင့် တစ်ခုမကသော Protocol တွေကို Support လုပ်တဲ့အပြင် Compression Error Checking ပိုင်းဆိုင်ရာတွေကိုလည်း Support လုပ်ပါတယ်။ Compression ကို Support လုပ်ခြင်းကြောင့် PPP ဟာ SLIP ထက်ပိုမြန်တဲ့အပြင် Error Checking ပါခြင်းကြောင့် SLIP ထက် PPP ဟာပိုစိတ်ချရပါတယ်။

SLIP ရော PPP ရောဟာ TCP/IP ကိုသုံးပြီးချိတ်ဆက်မှုလုပ်လို့ရတာခြင်းတူပေမယ့် PPP က IP Address ကိုအသေမဟုတ်ဘဲ Dynamic Assignment လုပ်နိုင်ပါတယ်။ ဒီလိုလုပ်နိုင်ခြင်းကြောင့် Administrator ဟာ RAS နှင့် RRAS Modems တွေမှာ Address တွေကို Block အလိုက် Assign လုပ်ထားနိုင်ပါတယ်။ ဒါကြောင့် PPP ဟာပိုပြီးတော့ Flexible ဖြစ်တာပေါ့။ ဒီလိုနဲ့ PPP ဟာ SLIP နေရာမှာလျှင်မြန်စွာနေရာယူလာတဲ့ TCP/IP Connection ကိုသုံးထားသော Remote Protocol ဖြစ်လာပါတယ်။

၁၁.၅ ပိုမိုကြီးထွားလာနေသောကွန်ရက်များ

စီးပွားရေးလုပ်ငန်းတစ်ခုဟာကြီးထွားလာတာနှင့်အမျှ ကွန်ရက်ကိုအသုံးပြုမှုဟာလည်း ပိုပြီးတော့ Heavy ဖြစ်လာပါတယ်။ ဒီတော့ ကွန်ရက်တစ်ခုအတွင်းမှာ ကွန်ပျူတာတွေဟာကြပ်ညပ်နေပြီး၊ Traffic တွေလည်းကြပ်တည်းလာပါတယ်။ ဒီအခါကွန်ရက်ကြီးဟာလေးလံလာပြီး Performance လည်းကျလာမှာဖြစ်ပါတယ်။ အဲဒီအခါ ကျွန်တော်တို့ဟာကွန်ရက်ကိုချဲ့ထွင်ခြင်း ဒါမှမဟုတ် ကွန်ရက်ကိုသီးခြားစီ ကွန်ရက်နှစ်ခုအဖြစ်ခွဲထုတ်ပြီး Repeaters ဖြင့်ပြန်ချိတ်ဆက်ကာ အသုံးပြုခြင်းစတာတွေကို လုပ်ဆောင်ရမှာဖြစ်ပါတယ်။ အဲဒီလို Network ကိုချဲ့ထွင်ရာမှာ ကျွန်တော်တို့အသုံးပြုမယ့်ပစ္စည်းတွေကတော့ -

(၁) Repeaters

(၂) Bridges

(၃) Routers

(၄) Brouters

(၅) Gateways

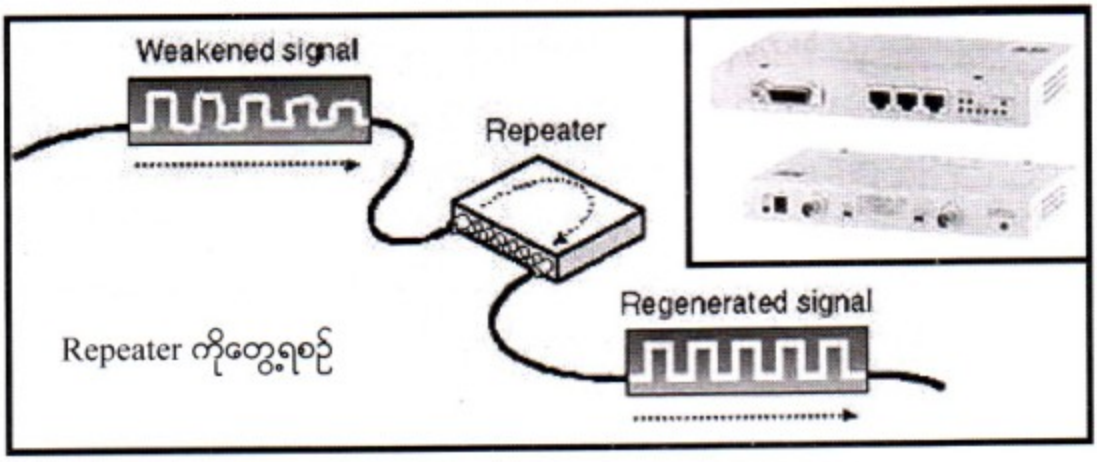
(၆) Switches တို့ဖြစ်ကြပါတယ်။ အခုကျွန်တော်တို့အဲ့ဒီပစ္စည်းတစ်ခုချင်းစီရဲ့ အကြောင်းကိုလေ့လာကြမှာဖြစ်ပါတယ်။

၁၀.၁၁ Repeaters အကြောင်း

ဦးဆုံးပြောပြချင်တာက ကြားခံပစ္စည်း (Media eg - Copper Cable) တိုင်းဟာ သူတို့ Data Signals တွေကိုသယ်ရမှာ Weaken ဖြစ်ကြတာချည်းပဲ။ ဆိုလိုချင်တာက ၎င်း Media တစ်ခုချင်းစီတိုင်းမှာသူတို့တတ်နိုင်သလောက်အကွာအဝေးအထိပဲ Data တွေသယ်သွားနိုင်ကြတာပါ။ ဒီတော့ ကိုယ်ဆင်ထားတဲ့ Network တွေရဲ့ Length ကိုထပ်ပြီးတိုးချဲ့ချင်တယ်ဆိုရင် Repeater ကိုသုံးရမှာဖြစ်ပါတယ်။ တနည်းအားဖြင့်ပြောရရင် ကွန်ရက်တစ်ခုရှိမယ်။ သူ့ Maximum Length ကုန်နေပြီ။ ကိုယ်ကသုံးမလောက်သေးဘူး။ ထပ်ဆင့်ချင်သေးတယ်။ မရတော့ပါဘူး။ ကွန်ရက်ရဲ့ Maximum Length ကိုရောက်နေပြီလို့ပြောထားပါတယ်။ ဒီတော့ Repeater ခံပြီးထပ်ဆင့်လိုက်ရင် လက်ရှိကွန်ရက်အတိုင်း နောက်ထပ်ရစေတာကြောင့် ကွန်ရက်နှစ်ခုချိတ်ထားပေးသလို ဒါမှမဟုတ် လက်ရှိကွန်ရက်ကိုနှစ်ဆဖြစ်သွားစေတာပါ။

Repeater ကိုထပ်ပြီး ပြောပြရဦးမယ်ဆိုရင် ကြားခံ Transmission Media တွေတိုင်းလိုလိုဟာ Attenuation ရှိကြပါတယ်။ ၎င်း Attenuation ကြောင့် Weakend ဖြစ်နေတဲ့ Data Signals တွေကို သူတို့ရဲ့နဂိုး Original အတိုင်းပုံစံပြန်ရအောင် Regenerate လည်းလုပ်ရင်း အများဆုံးသော Transmission အကွာအဝေးကိုလည်းတိုးမြှင့်သွားတာဖြစ်ပါတယ်။

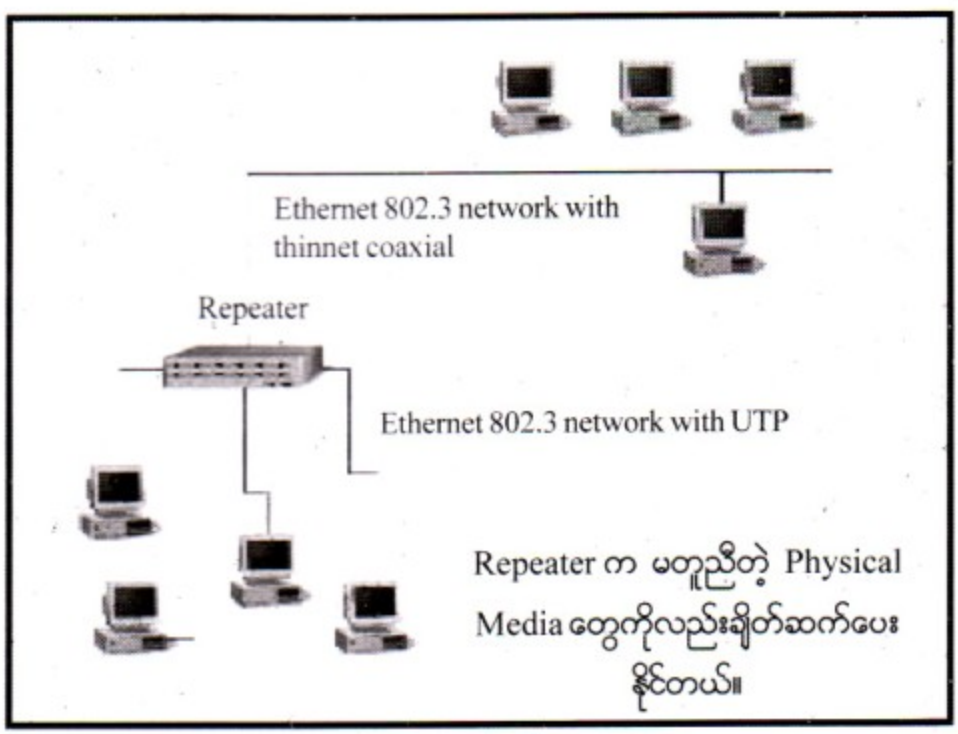
ပုံ ၁၀.၇



တစ်ချို့သော Repeater တွေဟာ Signal တွေအားကောင်းလာအောင် Amplify လုပ်လိုက်တဲ့အခါ

Data Signals တွေ Amplify ဖြစ်လာသလို ကွန်ရက်ပေါ်က Noise တွေလည်း Amplify ဖြစ်လာစေ ပါတယ်။ အဲဒီလိုအပြင် အကယ်၍များ Original ဖြစ်တဲ့မူလ Data Signal တွေဟာပျက်စီးနေရင်တောင် ၎င်းဟာ Signal တွေကိုပြန်ပြီး Clean-up မလုပ်နိုင်ပါဘူး။ ဒါပေသိ ဒီနေ့ တော်တော်များများ Repeater တွေဟာ အဆင့်မြင့်ကောင်းမွန်လာပါပြီ။ သူတို့တွေဟာ Signal တွေကို Amplify လည်းလုပ်ရင်း Regenerating လည်းလုပ်ရင်းနဲ့ Network Media တွေရဲ့ ကန့်သတ်ချက်တွေကိုကျော်လွန်ချဲ့ထွင်ကြပါတယ်။ သူတို့တွေဟာ သူတို့ဆီကိုရောက်လာတဲ့ Data တွေကို Identify လုပ်ပါတယ်။ ပြီးမှ Original Signal ရအောင် Regenerate လုပ်ကြပါတယ်။ ဒီလိုနဲ့ Noise တွေကိုလည်းလျော့ချရင်း Signal တွေကိုလည်း Amplify လုပ်ရင်းနဲ့ ရှိကောင်းရှိနေနိုင်တဲ့ အပျက်အစီးတွေနဲ့ နှောင့်ယှက်မှုတွေကိုလည်းရှင်းလင်းကြပါတယ်။ Repeater တွေကိုအသုံးပြုပြီး ကွန်ရက်တွေကိုအကန့်အသတ်မရှိ တိုးချဲ့လို့ရရင်ကောင်းမှာပဲဟုဆိုသော်ငြား လည်း တကယ့်တကယ်တမ်းမှာတော့ ကွန်ရက်တွေကို အရှည်အစားကန့်သတ်မှုက ရှိနေပြန်ပါတယ်။ ဒီအတွက် အဓိကကျတဲ့အချက်ကတော့ Signal များပျံ့နှံ့ခြင်း Propagation ကြောင့်ပဲဖြစ်ပါတယ်။ ကွန်ရက်တစ်ခုမှာ Data Signal တွေဟာ ၎င်း ကွန်ရက်၏အဝေးဆုံးသော Node ဆီကိုရောက်ရှိသွားတဲ့အချိန်ပမာဏ ကို Propagation Delay လို့ခေါ်ပါတယ်။ အကယ်၍များ သတ်မှတ်ထားသော Propagation Delay ဆိုတဲ့ အချိန်ကာလ အပိုင်းအခြားတစ်ခုမှာ ကွန်ရက်ဟာ Signal တွေကိုမတွေ့ခဲ့ဘူးဆိုရင်ဒါဟာ Network Error တစ်ခုခုဖြစ်နေပြီလို့ ယူဆနိုင်ပါတယ်။

ပုံ ၁၀.၈



Repeater တွေဟာ Fiber Optic နဲ့ဆင်တဲ့ Network တွေထက် Copper Wire နဲ့ဆင်တဲ့ Network တွေမှာ ပိုအသုံးများပါတယ်။ Repeater တွေဟာ ကွန်ရက်ကိုချိတ်ဆက်တဲ့နေရာမှာ OSI Model

ရဲ့ Physical Layer ကိုအသုံးပြုပါတယ်။ တနည်းအားဖြင့် OSI Model ရဲ့ Physical Layer ကို အားပြုပါတယ်။ Repeater ကိုအသုံးပြုရာမှာ Network နှစ်ခုဟာ Protocol နှင့် Speed တွေတူရပါမယ်။ အောက်မှာ Repeaters ရဲ့အားသာချက်နှင့်အားနည်းချက်များကိုဖော်ပြပေးထားပါတယ်။

Advantages	Disadvantages
Allow easy expansion of the network	Provide no addressing information over large distances
Have very little impact on network speed	Cannot connect different network architectures
Allow connection between different media	Do not help ease congestion problems
	Limit number of repaters in a network

၁၀.၁၁ Bridges အကြောင်း

တစ်နည်းအားဖြင့်ပြောရရင် Bridge ဆိုတာလည်းပိုမိုကောင်းမွန်လာတဲ့ Repeater တွေပါပဲ။ ဘာဖြစ်လို့လဲဆိုတော့ သူတို့ကလည်း Network တွေရဲ့ Maximum အရှည်အစားကိုထပ်ပြီး Extend လုပ်နိုင်လို့ပါပဲ။ အဲပေသိ ခုနကပြောသလိုပဲ Bridge ဟာ Repeater လိုပဲဆိုပေမယ့် Bridge ဟာ Repeater ထက်အားသာချက်တွေရှိလို့နေပြန်ပါတယ်။ ကဲ ဘယ်လိုအားသာချက်တွေလည်းဆိုတာကြည့်ကြရအောင်။

ပထမဦးဆုံးပြန်ပြီးမှတ်မိဖို့က Bridge တို့ Repeater တို့ရဲ့ လုပ်ဆောင်ပုံပါပဲ။ သူတို့က Network ကို Extend လုပ်ဖို့လို့ပြောခဲ့တယ်နော်။ တကယ်တော့ တစ်ဖက်ကပြန်စဉ်းစားကြည့်ရင် ကွန်ရက်နှစ်ခုကိုချိတ်ပေးထားတာပါပဲ။ မျက်စေ့ထဲမြင်အောင်ပြောရရင် ချောင်းခြားထားလို့ အနေဝေးနေတဲ့ ချောင်းရဲ့ အရှေ့ဖက်ရွာနှင့် အနောက်ဖက်ရွာလိုပါပဲ။ ဒီရွာနှစ်ခုအလယ်ကချောင်းခြားထားလို့ ဝေးနေပေမယ့်ချောင်းကိုတံတားထိုးပေးလိုက်မယ်ဆိုရင်တော့ ဒီရွာနှစ်ခုဟာ ကူးလူးဆက်ဆံသွားလို့ရမှာဖြစ်ပါတယ်။ အဲဒါဟာ Bridge တို့ Repeater တို့ရဲ့ သဘောတရားဖြစ်ပါတယ်။ အဲ့ဒီမှာ Repeater ဟာသူဆီကိုရောက်လာတဲ့ Signal တွေ အားလုံးကိုဖြတ်သန်းခွင့်ပြုပါတယ်။ Bridge ကြတော့ ဒီလိုမဟုတ်ပါဘူး။ Bridge ဟာသူဆီရောက်လာတဲ့ Signal တွေထဲကမှ ဘစ်ဖက်က Network ကိုသွားဖို့လိုအပ်တဲ့ Signal တွေကိုသာ Bridge ဟာဖြတ်သန်းခွင့်ပေးပြီး တစ်ဖက် Network ကို Signal တွေရောက်ရှိစေပါတယ်။ ဥပမာပြောရရင် ခုနက ရွာနှစ်ရွာလိုပေါ့။ Bridge ကိုရောက်လာမယ့် ကုန်သည်တစ်ယောက် သူဟာ အရှေ့ရွာမှာရှိ နေတဲ့ အိမ်တစ်အိမ်ကိုသွားမယ်။ လက်ရှိသူဟာလည်း အရှေ့ရွာမှာပဲ။ ပြီးတော့ သူဟာ သူရှာရမယ့် အိမ်အတွက် တံတားကိုဖြတ်ပြီး အနောက်ရွာကိုသွားချင်နေတယ်။ တကယ်ဆို သူလက်ရှိရောက်နေတဲ့ အရှေ့ရွာမှာပဲ သူရှာနေတဲ့အိမ်ကရှိနေတာ။ ဒီတော့ တံတားကိုဖြတ်ပြီး အနောက်ရွာကိုသွားဖို့မလိုဘူး။ ဒီနေရာသွားချင်နေတဲ့ ဒီကုန်သည်ကို တံတားနေရာမှာ Repeater ဆိုရင် Repeater က ကုန်သည်ကို ဘစ်ဖက်ကိုသွားခွင့်ပြုပြီး Bridge ကသွားခွင့်မပြု

ဘူး။ အဲဒီလို သွားခွင့်မပြုတော့ ဘာထူးခြားသွားလဲ။ တံတားပေါ်မှာ သွားသင့်တဲ့သူပဲသွားတယ်။ မဖြတ်သင့်တဲ့ သူကမဖြတ်တော့ တံတားကပြည့်ကျပ်မနေဘူးပေါ့။ လမ်းမှာကားတွေပိတ်နေလျှင် သွားရေးလာရေးကြန့်ကြာတာပေါ့။ ဒီတော့ Bridge က သူ့ကိုဖြတ်ပြီးတစ်ဖက်ကိုသွားဖို့လိုတဲ့ Signal တွေကိုသာ သွားခွင့်ပြုတယ်လို့ ပြောချင်တာပ။ ဘာကြောင့် Bridge ဟာ အဲဒီလို Signal တစ်ဖက်ကိုသွားဖို့ လိုမလိုဆိုတာ သူဘာဖြစ်လို့သိနေသလဲဆိုတာကိုပြောပြပါဦးမယ်။

ပထမဦးဆုံး ကွန်ရက်တစ်ခုမှာရှိတဲ့ ပစ္စည်းတိုင်းမှာ တစ်ခုနှင့်တစ်ခု မတူညီတဲ့ Unique Address ဆိုတာရှိပါတယ်။ အဲဒီ ကွန်ရက်မှာချိတ်ဆက်ထားတဲ့ Node တွေရဲ့ Address တွေဟာ Address တွေအနေနဲ့ Bridge မှာရှိနေတာကြောင့် Bridge ဟာ Signal တွေကိုသူ့ဆီကနေ တစ်ဖက်ကိုဖြတ်ရမလား မဖြတ်ရဘူးလားဆိုတာကို သူကဆုံးဖြတ်နိုင်နေတာဖြစ်ပါတယ်။ ကဲ ဘယ်လိုအလုပ်လုပ်သလဲဆိုတာကို တစ်ချက်ချင်းစစ်ကြည့်ပါဦးမယ်။ ကဲ ကွန်ရက်နှစ်ခုရှိတယ်ဆိုကြပါစို့။ LAN A ရယ်၊ LAN B ရယ်ပေါ့။

၁။ Bridge ဟာ LAN A ရော LAN B ရဲ့ Data Packet တိုင်းကိုရရှိပါတယ်။

၂။ အဲဒီလို သူ့ဆီရောက်လာတဲ့ Data Packet လေးတွေဆီကမှ LAN A မှာဘယ် Address တွေရှိပြီးတော့ ဘယ် Address တွေဟာ LAN B မှာရှိသလဲဆိုတာကိုသိသွားတာပါ။

၃။ ဒီတော့ LAN A မှာရှိတဲ့ Data တွေဟာ LAN A ကိုသွားချင်ရင်သော်လည်းကောင်း၊ LAN B မှာရှိတဲ့ Data တွေဟာ LAN B ကိုသွားချင်ရင်သော်လည်းကောင်း၊ Bridge ရဲ့ အကူအညီကိုမလိုအပ်ပါဘူး။ Bridge ကိုဖြတ်ပြီးတော့ သွားစရာလည်းမလိုပါဘူး။

၄။ LAN A မှာရှိတဲ့ Data Packet တွေဟာ LAN B ကိုသွားချင်တဲ့အခါမှာသော်လည်းကောင်း၊ LAN B မှာရှိတဲ့ Data Packet တွေဟာ LAN A ကိုသွားချင်ရင်သော်လည်းကောင်း၊ Bridge ကိုအသုံးပြုပါတယ်။

ဟိုတစ်ချိန်တုန်းက Bridge တွေမှာဆိုရင် ကွန်ရက်တွေမှာရှိတဲ့ Address တွေကိုမှတ်ထားတဲ့ Address Table ဟာ Network Administrator တွေက Manual သတ်မှတ်ပေးရတာပါ။ အခုနောက်ပိုင်း Bridge တွေကတော့ Learning Bridge လို့ခေါ်ပါတယ်။ သူတို့ကတော့ ကွန်ရက်မှာ Node တွေကိုထပ်တိုးသည်ဖြစ်စေ လျော့သည်ဖြစ်စေ Bridge မှာရှိတဲ့ Address Table ကို သူ့ဘာသာ Update လုပ်ယူပါတယ်။ Manual ပြန်သတ်မှတ်ပေးစရာမလိုပါဘူး။ သူအလုပ်လုပ်ပုံက ခုနကပြောခဲ့တဲ့ လေးချက်ထဲက နံတိယအချက်ဖြစ်ပါတယ်။

Bridge ကလုပ်ပေးနိုင်တဲ့ အလုပ်တွေကိုပြောပြပါဦးမယ်။ အဲဒါတွေကတော့ - အလုပ်တွေအရမ်းအများကြီး Heavy Duty လုပ်နေရတဲ့ Network ကို Bridge ခံပြီး Small Segment အဖြစ်ခွဲထုတ်ပေးနိုင်ခြင်း၊ နောက်တစ်ခုက Network ရဲ့ Maximum အရွယ်အစားကိုလည်းချဲ့နိုင်တာဖြစ်ပါတယ်။ ဒါပေသိ Bridge

ဟာမတူညီတဲ့ ကွန်ရက်နှစ်ခုကိုဆက်မပေးနိုင်ပါဘူး။ နောက်ပြီး Bridge တွေဟာ အလုပ်လုပ်တဲ့နေရာမှာ Node တွေရဲ့ Physical Address အပေါ်မူတည်ပြီးအလုပ်လုပ်ရပါတယ်။ ၎င်း Address တွေဟာ OSI Data Link Layer ရဲ့ Function တွေဖြစ်ပါတယ်။ ဒါကြောင့်မို့ Bridge ဟာလည်း Data Link Layer ရဲ့ Function တွေပါပဲ။

ကဲ Bridges နှစ်ပတ်သက်ပြီးထပ်မြောပြချင်သေးတာက Learning Bridges နှင့် Source Routing Bridge တို့အကြောင်းပဲဖြစ်ပါတယ်။

ပုံ ၁၀.၉

Bridge ကိုတွေ့ရစဉ်

Learning Bridges အကြောင်း

Learning Bridge ကို Transparent Bridge လို့လည်းခေါ်ပါတယ်။ Ethernet Network တွေမှာအသုံးပြုပါတယ်။ ဒီ Bridge တွေဟာ Data Packets တွေကိုလက်ခံရရှိတိုင်း Table ဇယားတစ်ခုတည်ဆောက်ထားပါတယ်။ ၎င်း Table ကို Bridge Table လို့ခေါ်ပါတယ်။ Bridge ကို စစဖွင့်ခြင်းတုန်းတော့ ဒီ Bridging Table မှာဘာမှမရှိသေးဘူးပေါ့။ နောက်တော့ Bridge ဟာ Packets လေးတွေလက်ခံရရှိလာတိုင်း အဲ့ဒီ Packets လေးတွေရဲ့ Network Segment ကို Bridge ဟာ ၎င်း Table မှာမှတ်သားထားလိုက်ပါတယ်။ အဲ့ဒီအပြင် ဒီ Packets လေးရဲ့ Sources and Destination Address ကိုပါမှတ်သားထားလိုက်ပါတယ်။ အဲ့ဒီလိုလုပ်ရင်းလုပ်ရင်းနဲ့ Bridges ဟာ MAC Address ကို List လုပ်ပြီးသားဖြစ်သွားသလို Address တစ်ခုချင်းစီရဲ့ Network Segment လေးတွေကိုလည်း List လုပ်ပြီးသားဖြစ်သွားပါတယ်။

Bridges ဟာ Packets တစ်ခုကိုလက်ခံရရှိချိန်မှာ ၎င်း Packets ရဲ့ Sources and Destination Address ကို Bridge Table မှာရှိတဲ့ Address နှင့်တိုက်ဆိုင်စစ်ဆေးကြည့်လိုက်တဲ့အခါ အဲ့ဒီ Address နှစ်ခုဟာ တူညီတဲ့ Network Segment တစ်ခုတည်းမှာရှိနေခဲ့ရင် ၎င်း Packets ကိုအခြားဘက်သို့ Retransmit လုပ်ခြင်းမပြုဘဲ ပယ်ဖျက်လိုက်ပါတယ်။ အကယ်၍များ Packets ရဲ့လားရာ Destination ဟာ အခြား Network Segment မှာဖြစ်နေခဲ့မယ်ဆိုရင် Bridges ဟာ Packets ကိုသူသွားရမယ့် Network Segment ဆီသို့ပေးပို့လိုက်ပါတယ်။ အကယ်၍များ Packets ဟာ Bridge ကိုရောက်လာလို့ Packets

ရဲ့ Destintation Network Segment ဟာ Bridging Table မှာမရှိသေးဘူးဆိုရင် Bridge သည် ၎င်း Packets ကိုသူထွက်လာခဲ့သော Network Segment မှလွဲ၍အားလုံးသော Segment ဆီသို့ Packets ကိုပေးပို့ လိုက်သည်။

Sources Routing Bridges အကြောင်း

၎င်းဟာအဓိကအားဖြင့် Token Ring Network တွေအသုံးပြုတဲ့ Bridges ဖြစ်ပါတယ်။ ၎င်း Bridges ဟာ Packets နှင့်အတူပါလာတဲ့ လမ်းကြောင်းနှင့်ပတ်သက်သောအချက်အလက်များပေါ် မူတည်၍ အလုပ်လုပ်ပါတယ်။ ဒီ Bridges တာပြောရမယ်ဆိုရင် သိပ်ပြီးတော့ ကြီးကြီးမားမားအလုပ်မလုပ်ရပါဘူး။ ဘာလို့လည်းဆိုတော့ အလုပ်အများစုကို Data ကိုပေးပို့တဲ့ Sending Computer ကလုပ်သွားလို့ဖြစ်ပါတယ်။ ဒီ Data ကိုပေးပို့တဲ့ Source (Sending Computer) တွေဟာ Explorer Packets ဆိုတာကိုအသုံးပြုပြီး သွားလိုရာကွန်ပျူတာဆီသို့ အကောင်းဆုံးသောလမ်းကြောင်းကို ရှာဖွေသတ်မှတ်ကြပါတယ်။ Data Packets ဟာရရှိလာတဲ့ လမ်းကြောင်းအချက်အလက်တွေပေါ်မူတည်ပြီး ကွန်ရက်မှာရည်ရွယ်ရာဆီကိုသွားတာဖြစ်ပါ တယ်။ ဒီအချိန်မှာ Source Routing Bridges ဟာ Packets ကိုလက်ခံရရှိတဲ့အခါ ၎င်း Packets ရဲ့ လမ်းကြောင်းကို မှတ်သားထားလိုက်ပါတယ်။ ဘာလို့လဲဆိုတော့ အဲ့ဒီလမ်းကြောင်းကို နောက်ထပ် Packets တွေသွားတဲ့အခါ ပြန်လည်အသုံးပြုဖို့ပါ။

ဘယ် Bridge ကိုအသုံးပြုတယ်ဆိုတာ ခဏထားပါအုံး။ တကယ်တမ်းပြောရမယ်ဆိုရင်တော့ Bridge တွေဟာ Packets တစ်ခုချင်းစီရဲ့ Source နှင့် Destination Address တွေကိုလိုက်စစ်နေရတဲ့အတွက်ကြောင့် Repeaters တွေထက်စာရင်တော့ အလုပ်လုပ်တာပိုနေးပါတယ်။ ဒါပေမယ့်လည်း Data တွေသွားတဲ့ Traffic လမ်းကြောင်းကိုစိစစ်ပြီးမှ သွားတဲ့အတွက် Birdge ဟာ Network ရဲ့ Data ပို့တဲ့နှုန်းကိုပြန်လည်းပြန်လာ စေနိုင်ပါတယ်။

အရေးတကြီးမှတ်စရာတစ်ခုကတော့ Bridges ဟာ Broadcast Packets ကြောင့်ပြန်ပေါ်လာတဲ့ Network Traffic ကိုတော့လျော့ချပေးနိုင်မှာမဟုတ်ပါဘူး။ Broadcast Packets ဆိုတာကွန်ပျူတာတစ်လုံး ဟာကိစ္စတစ်ခုကြောင့် အချက်အလက်တွေကို Network မှာရှိတဲ့ Computer တွေအားလုံးစီပေးပို့လိုက်တာကို ပြောတာဖြစ်ပါတယ်။ ကျွန်တော်ရှေ့မှာလည်းပြောခဲ့ဘူးပါတယ်။ Bridge တွေဟာ Repeater တွေလိုပါပဲ။ မတူညီတဲ့ Media (Cable) ကိုသုံးထားတဲ့ Network နှစ်ခုကိုချိတ်ဆက်ပေးနိုင်ပါတယ်။ ဘာဖြစ်လို့လည်း ဆိုတော့ Bridge တွေက OSI Model ရဲ့ Physical Layer မှာအလုပ်လုပ်တာကြောင့်ဖြစ်ပါတယ်။ ဥပမာ ပြောရရင် Bridge ဟာ 10BaseF Ethernet Network နှင့် 10BaseT Ethernet Network တို့ကို ချိတ်ဆက်ပေးနိုင်ပါတယ်။ နောက်တစ်ခုပြောစရာရှိတာက Bridge တွေဟာမတူညီတဲ့ Network နှစ်ခုကို ချိတ်ဆက်မပေးနိုင်ဘူးဆိုပေမယ့် Translation Bridge ကတော့ မတူညီတဲ့ Network နှစ်ခုကိုချိတ်ဆက်ပေး

ပါတယ်။ ဥပမာပြောရမယ်ဆိုရင် ၎င်း Translation Bridge ဟာ Ethernet Network နှင့် Token Ring Network တို့ကိုချိတ်ဆက်ပေးနိုင်ပါတယ်။ ပြောရမယ်ဆိုရင်တော့ဗျာ။ ဒီ Translation Bridge ဟာ Ethernet Network ဘက်ကကြည့်ရင် Ethernet Frame တွေကိုလက်ခံနိုင်တဲ့ Learning Bridge ပုံစံမျိုးဖြစ်နေပြီး Token Ring Network ဘက်ကြည့်ရင် Token Ring Packets တွေကိုလက်ခံနိုင်တဲ့ Source Rounting Bridge ပုံစံမျိုးဖြစ်နေပါတယ်။ Ethernet ကနေ FDDI Network ကိုပြောင်းပေးနိုင်တဲ့ Translation Bridge တွေလည်းရှိနေပါပြီ။ အောက်မှာ Bridge တွေရဲ့ အားနည်းချက် အားသာချက်များကိုပြပေးထားပါတယ်။

Advantages	Disadvantages
Easily extend network distances	Slower than repeaters
Filter traffic to ease congestion	Pass broadcast packets
Connect network with different media	More expensive than repeaters
Translation bridges can connect different network architectures.	

၁၁.၁၂ Routers အကြောင်း

Router တွေဟာ သီးခြားစီဖြစ်နေတဲ့ ကွန်ရက်နှစ်ခုကိုတစ်ခုတည်းဖြစ်သွားအောင် ချိတ်ဆက်ပေးနိုင်ဖို့အတွက် ပြုလုပ်ပေးထားတဲ့တကယ့်ကိုအဆင့်မြင့်ပစ္စည်းတွေဖြစ်ကြပါတယ်။ သီးခြားစီဖြစ်နေတဲ့ ကွန်ရက်နှစ်ခုကိုချိတ်ဆက်ပေးလိုက်တာဟာ ဥပမာပြောရမယ်ဆိုရင်ဖြင့် Ethernet Network နှင့် FDDI Network တို့ကိုချိတ်ဆက်လိုက်တယ်ဆိုပါစို့။ အဲ့ဒီ Network တစ်ခုချင်းစီမှာအသုံးပြုနေတဲ့သူတွေဟာ ဒီ Network တစ်ခုချင်းစီမှာရှိတဲ့ Resources တွေကိုအသုံးပြုသွားနိုင်မှာပါ။ ဒါကို Interwork လို့လည်းခေါ်ပါတယ်။ ထပ်မံရှင်းပြရမယ်ဆိုရင်တော့ဗျာ။ ဒီ Network နှစ်ခုဟာသီးခြား Function စီ အလုပ်လုပ်နေကြသော်လည်း အသုံးပြုသူတွေက ဒီ Network နှစ်ခုကြား အချက်အလက်တွေကိုဖလှယ်နိုင်သွားတာပေါ့။ ဒီ Inter Network ကိုကနေ့ခေတ်မှာ အကောင်းဆုံးဥပမာပြောရမယ်ဆိုရင်တော့ ဒါဟာ Internet ပဲဖြစ်ပါတယ်။ Internet ဆိုတာကလည်း အချက်အလက်တွေကိုဖလှယ်ဖို့အတွက် Network သေးသေးလေးတွေအများကြီးချိတ်ဆက်ထားတာပဲဖြစ်ပါတယ်။

Network ဟာကြီးထွားလာတာနှင့်အမျှ Network တစ်ခုလုံးမှာ Data ပို့ရာလမ်းကြောင်းတွေများပြားလာပြီး Fault Tolerance ကိုလည်းပံ့ပိုးပေးလာနိုင်ပါတယ်။ Bridge ကတော့ Data တွေကိုပို့ဖို့ Router လိုလမ်းကြောင်းအများကြီးနှင့် အလုပ်မလုပ်နိုင်ပါဘူး။ Bridge စွေနှင့်တူတဲ့အချက်က Router တွေဟာ Network Segment အများကြီးကိုချိတ်ဆက်ပေးနိုင်ခြင်း Traffic များကိုစီစစ်ပေးနိုင်ခြင်း (‘မင်းက

ဟိုဘက်ကိုသွားစရာမလိုတော့ဘူး။ ဒီဘက်မှာပဲနေ' ဆိုတာမျိုး) တို့ဖြစ်ပြီး Bridge နှင့်မတူတဲ့အချက်က Router တွေကရှုပ်ထွေးတဲ့ Network တွေကိုတပ်ဆင်ရာမှာအသုံးပြုနိုင်ခြင်းပါပဲ။ ပုံမှာလည်းပြထားပါတယ်။ Network Segment တစ်ခုချင်းစီမှာ Subnetwork ဒါမှမဟုတ် Subnet လို့ခေါ်ပါတယ်။ ဒီ Subnet တစ်ခုချင်းစီအတွက် Network Address ရှိသလို Subnet ထဲက Note တစ်ခုချင်းစီမှာလည်း Network Address ဆိုတာရှိပါတယ်။ ဒီ Network Address နှင့် Note Address ကိုပေါင်းပြီး အသုံးပြုပြီးတော့ Router ဟာ ပေးပို့ရမယ့် Packets တွေကို ဘယ်မှာဘယ်ဆီသို့ တနည်းအားဖြင့်ပြောရရင် Network ရဲ့ဘယ်နေရာမဆို ပေးပို့နိုင်သွားတာဖြစ်ပါတယ်။

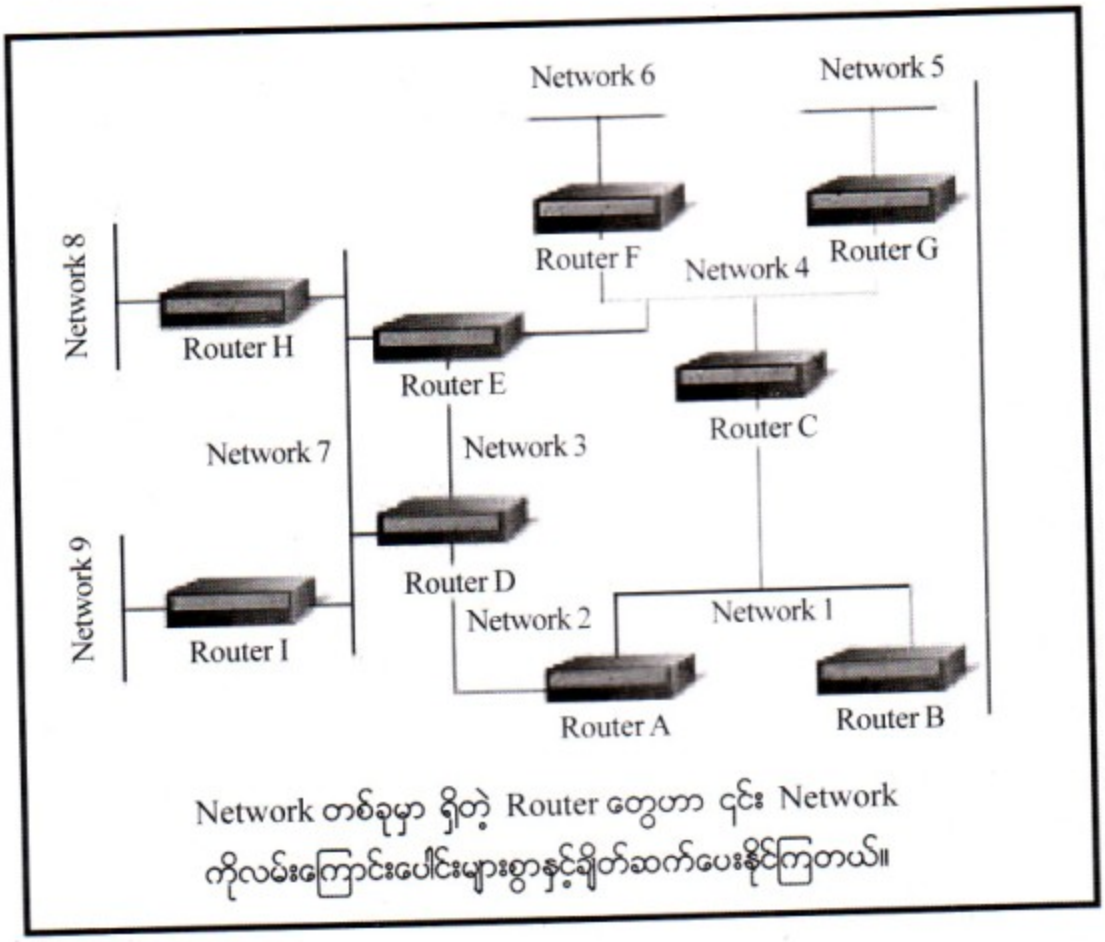
ထပ်ပြီးတော့ရှင်းပြရမယ်ဆိုရင် Routers တွေဟာ Data တွေကိုပေးပို့တဲ့အခါမှာ Packets လေးရဲ့ဦးတည်သွားရမယ့် Destination Note Address တနည်းအားဖြင့် MAC Address ကိုပဲကြည့်ရတာမဟုတ်ပါဘူး။ ၎င်း Packets သွားမယ့် Destination Network ကိုပါကြည့်ရပါတယ်။ ပြောရမယ်ဆိုရင် Routers တွေက OSI Model ရဲ့ Network Layer မှာအလုပ်လုပ်တာဖြစ်ပါတယ်။

ဒီလိုဆင့်ကဲဆင့်ကဲ ချိတ်ဆက်ထားတဲ့ Inter Network တစ်ခုမှာ Packet တစ်ခုကိုလိုရာအရပ်သို့ အောင်မြင်စွာပေးပို့နိုင်ဖို့ရာ Router ဟာ Packet ဖြတ်သန်းကြောင်းကို ရှာဖွေပေးရတာဖြစ်ပါတယ်။ Router ဟာပေးပို့ရမယ့် Packet ကိုလက်ခံရရှိချိန်မှာ Packet သွားရမယ့် Network Address ကိုစစ်ဆေးပြီး ၎င်း Address တာ Router ရဲ့ Routing Table မှာကြည့်လိုက်ပါတယ်။ ပြီးတာနဲ့ Router ဟာ Data ကိုပြန်လည်ထုတ်ပိုးလိုက်ပြီး Data ပေးပို့ရမယ့်လမ်းကြောင်းမှာရှိနေတဲ့ နောက် Packet တစ်ခုဆီကို Data ကိုပေးပို့လိုက်ပါတယ်။ Router တွေဟာ Bridge ထက်စာရင် OSI Model ရဲ့ Higher Layer တွေမှာ အလုပ်လုပ်တာကြောင့် Router တွေဟာမတူညီတဲ့ Network နည်းပညာတွေမှာ Data တွေကိုလွယ်ကူစွာဖြင့် ပေးပို့နိုင်ခြင်းဖြစ်ပါတယ်။ ဥပမာပြောရမယ်ဆိုရင်ဖြင့် Token Ring Network ကရရှိလာတဲ့ Data Packet တွေကို Ethernet Network ဆီကိုပေးပို့နိုင်တယ်။ Router တွေဟာ Token Ring Frame တွေကိုဖယ်ထုတ်လိုက်တယ်ပေါ့ဗျာ။ ပြီးတော့ အဲ့ဒီ Packet ကိုလည်းပေးပို့ရမယ့် Network Address ကြည့်လိုက်ပါတယ်။ ပြီးတော့ Data တွေကို Ethernet Network အဖြစ်ပြန်လည်ထုတ်ပိုးလိုက်ပါတယ်။ ဒီအဆင့်တွေပြီးတော့မှ Data ကို Ethernet Network ဆီသို့ပေးပို့လိုက်တာဖြစ်ပါတယ်။ ဒါပေမယ့် အဲ့ဒီမှာသိထားရမှာက အဲ့ဒီလိုအခြေအနေမျိုးတွေက Network ရဲ့ Speed ကိုကျသွားစေပါတယ်။ ဘာဖြစ်လို့ပါပဲ။ ရှင်းပြပါ့မယ်။ ဒီလိုဗျ။ Ethernet Frame တွေရဲ့ အများဆုံးသော Frame Size ဟာအနိုးစပ်ဆုံးပြောရရင် 1500 byte အထိသာရှိပါတယ်။ ဒါပေသိ Token Ring Frame Size ကြတော့ 4000 byte ကနေ 18000 byte အထိရှိနိုင်တယ်ဗျ။ ဒီတော့ကာ 18000 byte ရှိတဲ့တစ်ခုတည်းသော Token Ring Frame ကို Ethernet Frame အဖြစ်ပြောင်းတဲ့အခါ Router ဟာ Ethernet Frame 12 ခုတောင်ပြုလုပ်ရပါတယ်။ Router တွေဟာမည်မျှပင်မြန်ပါစေ။ ဒီလို Frame Type ပြောင်းလဲပစ်ရတာ Network ရဲ့ Speed ကိုထိခိုက်စေပါတယ်။

Bridge နဲ့ Router တွေရဲ့အဓိကကွာခြားတဲ့ အချက်တစ်ခုကတော့ Router ဟာ Data တွေကို

ပေးပို့ရာမှာ ဘယ်လမ်းကြောင်းကနေသွားရင် အကောင်းဆုံးလဲဆိုတာကိုရွေးချယ်တတ်သလို ဘယ် Router ကိုအသုံးပြုမလဲဆိုတာကိုရွေးချယ်တတ်ပါတယ်။ ရှေ့မှာပြောပြခဲ့သလိုပါပဲ။ Bridge တွေဟာ သူတို့လက်ခံရရှိလာတဲ့ Packet မှာဘယ်ကိုသွားရမယ်ဆိုတဲ့ Destination Packet ကိုမသိသေးဘူးဆိုရင် အဲဒီ Packet ကိုချိတ်ဆက်ထားတဲ့ Network Segment ဆီသို့ပေးပို့လိုက်ပါတယ်။ ဒါပေမယ့် အဲဒီလိုအဖြစ်အပျက်မျိုး Router မှာဖြစ်လာခဲ့မယ်ဆိုရင်တော့ ဆိုလိုတာက Router ဆီရောက်ရှိလာတဲ့ Packet တစ်ခုဟာ ဘယ်ကိုသွားရမယ်ဆိုတဲ့ Network Address မပါရှိခဲ့ဘူးဆိုရင် ၎င်း Packet ကိုပယ်ဖျက်လိုက်ပါတယ်။ တစ်ပိုင်းတစ်စပျက်နေတဲ့ Packet တွေနဲ့ Broadcasts တွေကိုလည်း Router ကပယ်ဖျက်တတ်ပါတယ်။ ပြောရမယ်ဆိုရင်တော့ Router ဟာသူနားမလည်တဲ့ Packet ဖြစ်စေ၊ ဘယ်ကိုပို့ရမလဲဆိုတာမသိတဲ့ Packet ဖြစ်စေ ပယ်ဖျက်တတ်ပါတယ်။

ပုံ ၁၀.၁၀



Network တစ်ခုမှာ ရှိတဲ့ Router တွေဟာ ၎င်း Network ကိုလမ်းကြောင်းပေါင်းများစွာနှင့်ချိတ်ဆက်ပေးနိုင်ကြတယ်။

၁၀.၁၃ Routing Table အကြောင်း

Router ကပြုစုထားတဲ့ Routing Table ဟာ Bridge ကပြုစုထားတဲ့ Bridging Table နှင့်ကွဲပြားမှုရှိပါတယ်။ Bridge တွေဟာ Network Segment တစ်ခုမှာရှိတဲ့ ပစ္စည်းတစ်ခုချင်းစီရဲ့ Hardware Ad-

dress ကိုမှတ်ထားတာဖြစ်ပြီး Router ရဲ့ Table ကတော့ Network Address နှင့် ၎င်း Network ကို Handle လုပ်နေတဲ့ Router တွေရဲ့ Address တွေပါဝင်ပါတယ်။ အောက်မှာဖော်ပြပြီးခဲ့တဲ့ပုံရဲ့ Router A ၏ Routing Table နမူနာကိုဖော်ပြထားပါတယ်။ အဲဒီ Table မှာ Next Hop ဆိုတာ Next Transmission ရဲ့ သွားရမယ့်နေရာဖြစ်ပြီး Cost ဆိုတာကတော့ Data ကအသုံးပြုရမယ့် Hops အရေအတွက်ကိုပြောတာဖြစ်ပါတယ်။

Network	Next Hop	Cost in Hops
1	Directly connected	0
2	Directly connected	0
3	Router D	1
4	Router C	1
5	Router C	2
6	Router C	2
7	Router D	1
8	Router D	2
9	Router D	2

Router မှာ Routing Table ပြုလုပ်ပုံပေါ်မူတည်ပြီး Router အမျိုးအစားနှစ်မျိုးရှိပါတယ်။ အဲဒါကတော့ -

(၁) Static Routing နှင့်

(၂) Dynamic Routing တို့ဖြစ်ကြပါတယ်။

၁၀.၁၄ Static Router အကြောင်း

Static Routing ကိုအသုံးပြုတဲ့ Router ဟာဆိုရင်ဖြင့် Administrator ဟာ Routing Table ကို Manually Update လုပ်ပေးဖို့လိုပါတယ်။ Router ဟာ အကယ်၍များအတိုဆုံးနှင့်အထိရောက်ဆုံးလမ်းကြောင်းကိုမလိုအပ်သည့်တိုင် အမြဲတမ်းရည်ရွယ် ကြိုပို့နေကျလမ်းကြောင်းအတိုင်းပဲပေးပို့ပါတယ်။ အကယ်၍များ Router ရဲ့ Table မှာ ပေးပို့ရာမှာ Destination မရှိခဲ့ရင် Router ဟာ Packet ကိုပယ်ဖျက်လိုက်ပါတယ်။

၁၀.၁၅ Dynamic Router အကြောင်း

Dynamic Routing ကိုအသုံးပြုတဲ့ Router တွေကြတော့ Discovery Process ဆိုတာကိုအသုံးပြုပြီး ရှိနေတဲ့ Router တွေရဲ့အချက်အလက်ကိုရှာဖွေပါတယ်။ Dynamic Routers တွေဟာ သူတို့အချင်းချင်းဆက်သွယ်လို့ရတဲ့အပြင် အခြား Routers တွေရဲ့ရရှိလာတဲ့အချက်အလက်တွေပေါ်မူတည်ပြီး Routing Table တွေကို Update လုပ်နိုင်ပါတယ်။ အကယ်၍များ Network တစ်ခုမှာ Multiple Routers (လမ်းကြောင်းတွေ အများကြီးရှိခဲ့မယ်ဆိုရင်) Router တာဘယ်လမ်းကြောင်းကအကောင်းဆုံးလဲဆိုပြီးတော့ ဆုံးဖြတ်နိုင်ပါတယ်။ Router တွေ အကောင်းဆုံးသောလမ်းကြောင်းဟာ ဘယ်လမ်းကြောင်းလဲလို့ရွေးချယ်ရာမှာ နည်းလမ်းနှစ်လမ်း ရှိပါတယ်။ အဲဒါတွေကတော့ -

(၁) Distance Vector Algorithm နှင့်

(၂) Link-State Algorithm တို့ပဲဖြစ်ကြပါတယ်။

Distance Vector Algorithm အကြောင်း

ဒီနည်းလမ်းကတော့ ကွန်ရက်နှစ်ခုအကြားသွားရမယ့်ခရီးမှာ ဖြတ်သွားရမယ့် Router အရေအတွက်ပေါ်အခြေခံပြီး Costs in Hops ကိုတွက်ပါတယ်။ ဒီတော့ လမ်းကြောင်းမှာ ဖြတ်သွားရမယ့် အနည်းဆုံး Hops ကိုရွေးချယ်ပါတယ်။ ဒီ Distance Vector Routing Protocol ဟာ RIP ဆိုတဲ့ Routing Information Protocol ပဲဖြစ်ပါတယ်။ ၎င်းကို TCP/IP ရော၊ IPX/SPX နှစ်ခုစလုံးမှာပါအသုံးပြုကြပါတယ်။

Link-State Algorithm အကြောင်း

ဒီနည်းလမ်းကတော့ Packet တစ်ခုအတွက်လမ်းကြောင်းမှာ အခြားသောအချက်အလက်တွေကိုပါထည့်သွင်း စဉ်းစားလာပါတယ်။ ဘယ်လိုအချက်အလက်တွေလဲဆိုတော့ Network Traffic, Connection Speed, Costs (Hops) တွေကိုပါထည့်သွင်းစဉ်းစားလာပါတယ်။ ဒီနည်း ဒီ Algorithm ကိုအသုံးပြုတဲ့ Routers အနေနဲ့ကတော့ ပိုပြီးတော့ Processing Power လိုအပ်တာပေါ့။ အဲပေမယ့် Packet တွေကို ထိထိရောက်ရောက်လိုရာကိုပေးပို့နိုင်တယ်လေ။ TCP/IP ရဲ့ Routing Protocol ဖြစ်တဲ့ OSPF (Open Shortest Path First) ဟာ ဒီ Link-State Algorithm ကိုအသုံးပြုပါတယ်။

Dynamic Routers တွေဟာ Maintain လုပ်ရတာလည်းလွယ်ကူသလို Static Routers တွေထက်စာရင် ပိုမိုကောင်းမွန်တဲ့လမ်းကြောင်းကို ရွေးချယ်ပေးနိုင်ပါတယ်။ အဲပေမယ့် Routing Table

ကို Update လုပ်ရတာရယ်၊ Discovery လုပ်ရတာရယ်ဟာ နောက်ထပ် Network Traffic တွေကိုဖြစ်ပေါ်စေပါတယ်။ ပုံမှန်သွားလာနေတဲ့ Traffic အပြင် သူတို့ရဲ့ Discovery လုပ်ဆောင်ဖို့သွားလာမှုတွေရှိလာတယ်လို့ပြောချင်တာပါ။ ဒီတော့ Data Traffic အပြင်သူတို့ Traffic တွေပါရှိလာတာပေါ့။ Distance Vector Protocol ဖြစ်တဲ့ RIP လို Protocol ဆိုရင် ဘယ်လောက်တောင်လဲဆို သူ့ရဲ့ Routing Table တစ်ခုလုံးကြီးကို Network တစ်ခုလုံးဆီသို့ စက္ကန့်သုံးဆယ်ကြာတိုင်း ပို့လွှတ်နေပါတယ်။

အောက်မှာ Routers တွေရဲ့ အားနည်းချက်နှင့်အားသာချက်ကိုဖော်ပြထားပါတယ်။

Advantages	Disadvantages
Connect network of different physical media and network architectures	More expensive and more complex than bridges or rpeaters
Choose the best path for a packet through an internetwork	Only work with routable protocols
Reduce network traffice by not forwarding broadcasts or corrupt packets	Dynamic routing updates create network traffic
	Slower than bridges because they must perform more intricate calcula tions on the packet

Protocol တိုင်းဟာ OSI Model ရဲ့အလွှာတိုင်းမှာ အလုပ်လုပ်ကြတာမဟုတ်ပါဘူး။ အဲ့ဒီအထဲမှာမှ Router လုပ်ပေးနိုင်သော Protocol ရှိသလို၊ Router လုပ်မပေးနိုင်သော Protocol များလည်းရှိပါတယ်။ Router လုပ်ပေးနိုင်သော Routable Protocol တွင် Network Layer Information များပါရှိပြီးတော့ Nonroutable Protocols မှာတော့ Network Layer Information များမပါရှိပါဘူး။ Routable Protocol တွေကတော့ -

(၁) TCP/IP
(၂) IPX/SPX
(၃) DECNet
(၄) OSI
(၅) DDP (Apple Talk)
(6) XNS တို့ဖြစ်ကြပါတယ်။

Router တို့တွေ့ရမည့် ပုံ ၁၁.၁၁

Nonroutable Protocol တွေကတော့-

(၁) NetBEUI

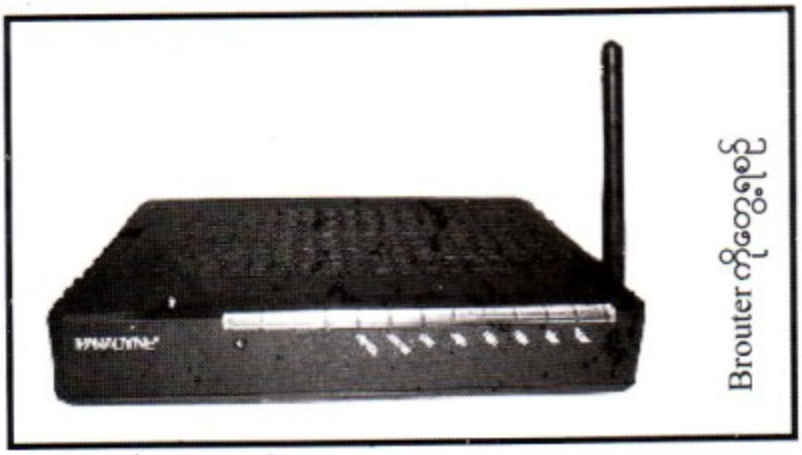
(၂) DLC (HP Prmtors နှင့် IBM Mainframe တွေမှာအသုံးပြုသည်။

(၃) LAT (Local Area Transport) တို့ဖြစ်ကြပါတယ်။

၁၀.၁၆ Brouters အကြောင်း

Brouter ဆိုရာမှာ B ဆိုတာက Bridge ကိုဆိုလိုချင်တာ။ ဒီတော့ရှင်းနေပြီ၊ အဲဒီပစ္စည်းက Bridge နှင့် Router ပေါင်းထားတာလို့ပြောလို့ရတယ်။ တကယ်တော့ Brouter ဆိုတာ Router မှာနောက်ထပ် Bridge Function ထပ်ဆောင်းထားတာပါ။ Brouter တွေဟာ Network Protocol Information တွေကို အခြေခံပြီး Data Backup တွေသယ်ယူပို့ဆောင်တာပါ။ အကယ်၍ Support မလုပ်တဲ့ Protocol တွေ အတွက် Brouter ထဲက Bridge က Bridge တွေရဲ့ ထုံးစံအတိုင်း Node တွေရဲ့ Address နှင့် Data Packets တွေကိုပို့ဆောင်ပေးပါတယ်။

ပုံ ၁၀.၁၂



Brouter ကိုတွေ့ရစဉ်

ထပ်မံရှင်းပြရရင်တော့ဗျာ။ Brouter ဟာ ဦးတည်ရာလိပ်စာပါတဲ့ Routable Packet ကို အကောင်းဆုံးလမ်းကြောင်းနှင့်ပို့ဆောင်နိုင်ဖို့ Rrouter သကဲ့သို့အလုပ်လုပ်ဆောင်ပါတယ်။ ဒါပေမယ့် Brouter ဟာ Router လုပ်မပေးနိုင်သော Packet တစ်ခုလက်ခံရရှိချိန်မှာ ပုံမှန် Router တွေသကဲ့သို့ပယ်ဖျက်ခြင်း မပြုဘဲ Brouter ဟာ Bridge ပုံစံသကဲ့သို့အလုပ်လုပ်ပြီး Packet ရဲ့ Hardware Address အတိုင်း Packet ကိုပေးပို့ပါတယ်။ ဒီလိုလုပ်နိုင်ဖို့ရာ Brouter ဟာ Hardware Address တွေပါဝင်သော Bridging Table ရော Network Address တွေပါသော Routing Table ရောကိုပါ တည်ဆောက်ရပါတယ်။

Brouters အထူးသဖြင့် Hybrid Networks တွေဖြစ်ကြတဲ့ Routable (လွှဲနိုင်သည်ရော)၊ Non-

Routable Protocols (မလွှဲနိုင်သည်ရော) စတဲ့ရောကျော်ဖြစ်နေတဲ့ Network တွေမှာအထူးအသုံးဝင်ပါတယ်။ ဥပမာပြောရရင် TCP/IP နှင့် NetBEUI နှစ်ခုသုံးထားတဲ့ Network မှာ Traffic ကို စစ်ထုတ်ချင်တယ်ဆိုရင် Brouter အသုံးပြုခြင်းဖြင့် TCP/IP Packets တွေကိုလိုရာအရပ်သို့ Router Function ဖြင့်ပို့ဆောင်ပေးနိုင်မည့်အပြင် NetBEUI Packets တွေကြပြန်တော့ Bridge Function ဖြင့်လိုရာသို့ပို့ဆောင်ပေးနိုင်ပါတယ်။

၁၀.၁၇ Gateways အကြောင်း

Gateways ဆိုတာကတော့ မတူညီတဲ့ Data Function အိမှမဟုတ် မတူညီတဲ့ Network နည်းပညာနှစ်ခုအကြား အချက်အလက်တွေကိုဘာသာပြန်ပေးနိုင်မယ့် ရှုပ်ထွေးနက်နဲတဲ့ Network သုံးပစ္စည်းတစ်ခုပဲဖြစ်ပါတယ်။ ဥပမာပြောရရင် Gateway ဟာ SNA (System Network Architecture) သုံးထားတဲ့ IBM Mainframe System နှင့် TCP/IP LAN အကြား Network ဆက်သွယ်မှုကိုပြုလုပ်ပေးနိုင်ပါတယ်။ နောက်ဥပမာတစ်ခုထပ်ပြောရမယ်ဆိုရင်တော့ Internet ကိုအသုံးပြုပြီး Microsoft Mail ကနေ SMTP လို့ဆိုတဲ့ Simple Mail Transport Protocol ကိုပြောင်းပေးနိုင်တဲ့ စနစ်လည်း ဖြစ်ပါတယ်။

ထပ်ရှင်းပြမယ်နော်။ Routers တွေက OSI Model ရဲ့ Network Layer မှာအလုပ်လုပ်တာဖြစ်တာကြောင့် Packets တွေကိုမတူညီတဲ့ Network နည်းပညာသုံးထားတဲ့ ဥပမာ Ethernet ကနေ Token Ring ဆီကိုပေးပို့ဆို ပေးပို့နိုင်ပါတယ်။ အိပေမယ့် Same Protocol (Protocol တူရမယ်) Ethernet, Token Ring ရောဟာ တူညီတဲ့ Protocol ကိုပဲ သုံးထားရမယ်။ Gateways ကြတော့ Protocol မတူလည်း Packet တွေကို Route လုပ်ပေးနိုင်ပါတယ်။ Routers တွေဟာ Data ကွေကိုမတူညီတဲ့ Frame အဖြစ်ပြန်လည်ထုတ်ပိုးနိုင်တယ်ဆိုခဲ့တယ်။ Gateways ကြတော့ Data ရဲ့ တကယ့် Format ကိုတောင်ပြောင်းလဲပစ်နိုင်ပါတယ်။

Gateway ဟာ PC ကနေ Mainframe ကွန်ပျူတာအထိတောင်ချိတ်ဆက်နိုင်ပါတယ်။ အိပေမယ့် အများစု Gateway တွေကတော့ သေးငယ်တဲ့ Network တွေမှာပဲတွေ့ရတတ်ပါတယ်။ Gateway ဟာ NetBEUI အိမှမဟုတ် TCP/IP အဲ့ဒီအပြင် Apple Talk အားလုံးကို Translation လုပ်နိုင်ပါတယ်။ Packet တွေဟာ Gateway ကိုရောက်ရှိချိန်မှာ အဲ့ဒီ Packets ရဲ့ Raw Data ကလွဲလို့အားလုံးသော Network Information တွေကိုဖယ်ရှားလိုက်ပါတယ်။ ပြီးတော့မှ Gateway ဟာ Data တွေကိုဘာသာပြန်၊ ပုံစံအသစ် New Format ပြုလုပ်ကာ OSI အလွှာအတိုင်းပြန်ဆင်းပြီး ပေးပို့ရမယ့် ကွန်ပျူတာ (Destination System) ရဲ့ Network Protocol ကိုသုံးပြီးပြန်ပို့ပေးပါတယ်။ ဘာဖြစ်လို့ OSI ကို အတက်အဆင်းလုပ်ရလဲဆိုတော့ Gateway က Data တွေကို Translate လုပ်ရာမှာယေဘုယျအားဖြင့် OSI Model ရဲ့ Upper အလွှာတွေ မှာအလုပ်လုပ်တာဖြစ်ပါတယ်။ ဥပမာ Application အလွှာပေါ့။ အိပေမယ့် အချို့ Gateway တွေကတော့ Network အိမှမဟုတ် Session Layer မှာတင် Translate လုပ်နိုင်ကြပါတယ်။

Gateway ဟာယေဘုယျအားဖြင့် အခြား Network ပစ္စည်းတွေထက် Install လုပ်ရတာ ခက်ခဲတယ်။ နှေးကွေးတယ်။ ကုန်ကျစရိတ်လည်းပိုများတယ်။

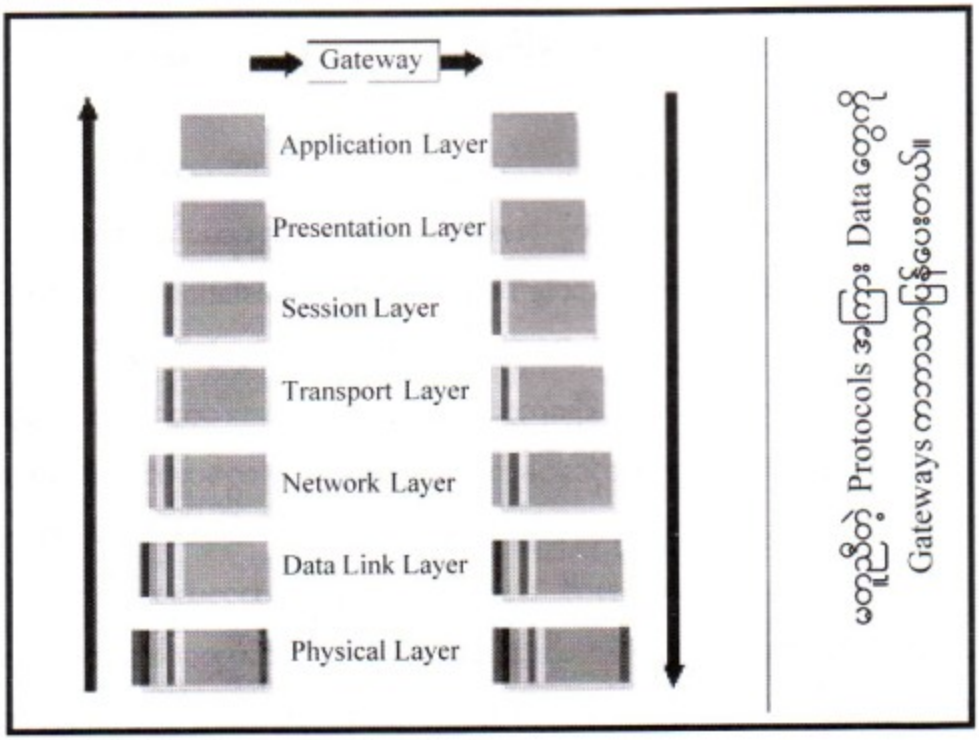
ပုံ ၁၀.၁၃

Gateway ကိုတွေ့ရဉီ

အောက်မှာ Gateway ရဲ့ အားနည်းချက်၊ အားသာချက်များကိုဖော်ပြပေးထားပါတယ်။

Advantages	Disadvantages
Connect completely different systems	More expensive than other devices
Dedicated to one task and perform that task well	More difficult ot install and configure
	Greater processing requirements means less speed than other devices

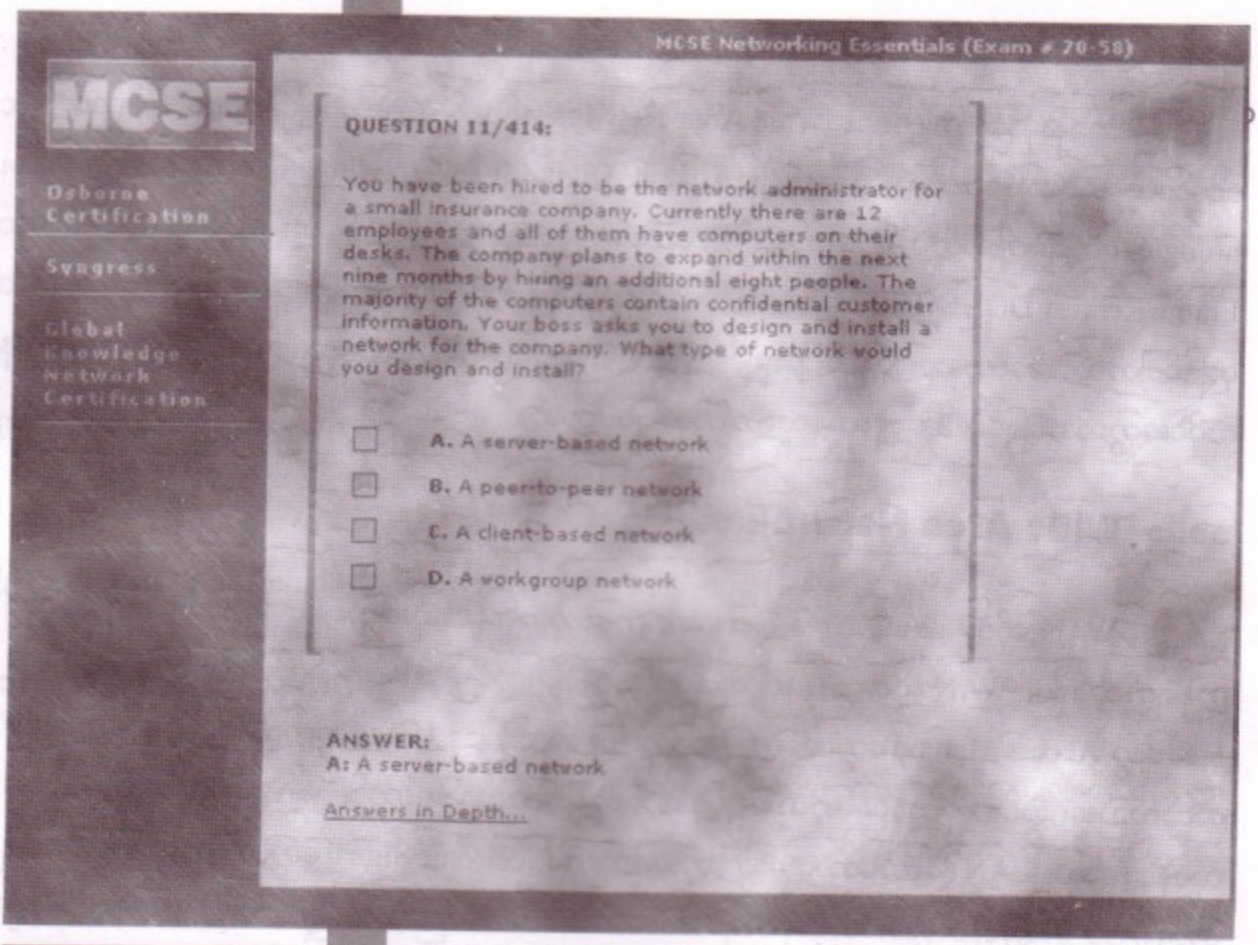
ပုံ ၁၀.၁၄



၁၀.၁၈ Switch အကြောင်း

Switch ဆိုတာ High Speed ဖြစ်တဲ့ Multiport Bridge ပဲဖြစ်ပါတယ်။ ကနေ့ခေတ်မှာဆိုရင် Switch တွေဟာ UTP Environment က Multiport Repeaters တွေ Connectors တွေကိုအစားထိုးဝင်ရောက်လာပြီ ဖြစ်ပါတယ်။ Switch ဟာ Intelligent ဖြစ်တဲ့ Hub လို့လည်းပြောလို့ရပါတယ်။ သူမှာ Bridging Table ဆိုတာရှိပြီး Network Segment တွေမှာရှိတဲ့ Hardware Address တွေကိုမှတ်ထားပါတယ်။ သူဟာ Bridge လိုပါပဲ။ Data သွားလိုတဲ့နေရာဟာ တဖက်က Network Segment မှာရှိမှသွားခွင့်ပြုတာပါ။ မဟုတ်ရင်သွားခွင့်မပြုပါ။ ဒီအချက်ကြောင့် Network ဟာအခြားပုံမှန်တွေထက်စာရင် ပိုပြီးတော့မြန်ဆန်လာပါတယ်။ ဒီထက်ပိုပြောရမယ်ဆိုရင်တော့ Switch တွေရဲ့နည်းပညာဟာ Switch တွေမှာရှိတဲ့ Port တစ်ခုချင်းစီရဲ့ Bandwidth ကိုသတ်မှတ်နိုင်ပါတယ်။ ဥပမာပြောရရင် Ethernet 10BaseT မှာပုံမှန် Hub တစ်ခုသုံးထားတယ်။ အဲဒီ Network ဟာအများဆုံး 10 Mbps ပဲ Bandwidth ရှိတယ်ဆိုပါစို့။ ဒီ Hub မှာရှိတဲ့ Port အားလုံးဟာ ဒီ 10 Mbps ကိုမျှဝေသုံးစွဲရပါတယ်။ Port တစ်ခုကို 10 Mbps ရတာမဟုတ်ပါ။ အဲဒီ Hub မှာ 16 Port ရှိတယ်ဆို 16 Port မှာမှ 10 Mbps ရတာပါ။ ဒီ Network မှာပုံမှန် Hub မသုံးဘဲ Switch ကိုသုံးထားမယ်ဆိုရင်တော့ Switch မှာရှိတဲ့ Port တိုင်းဟာ တစ် Port ချင်းစီကို 10 Mbps Bandwidth ရရှိတာဖြစ်ပါတယ်။

Over 50 % cover of
Certification
Exam
ZAW LIN (YOUTH)
Computer in Details
Computer Hardware
Maintanence
&
System Administration
ZAW LIN
(YOUTH)



UNIT 11

Wide Area Network Concept

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ Wide Area Network နှင့် ပတ်သက်နေသော အကြောင်းအရာတွေကိုလေ့လာကြမှာ ဖြစ်ပါတယ်။ အခြေခံထက်အနည်းငယ်ပိုတဲ့ Concept တွေ ပေးထားပါတယ်။

ဒီအခန်းမှာတော့ ကနဦး Wide Area Network နှင့်ပတ်သက်တဲ့အခြေခံ Concepts တွေကို စတင်လေ့လာရမှာဖြစ်ပါတယ်။ နောက်ပြီး Analog, Digital, Packet Switching စတဲ့ WAN Technologies တွေရဲ့မတူညီတဲ့ကွဲပြားချက်တွေကိုလည်း လေ့လာရမှာဖြစ်ပါတယ်။ အဲ့ဒီအပြင် ISDN, ATM, Frame Relay, FDDI, SONET နှင့် SMDS တို့ရဲ့အသုံးပြုပုံ အကျိုးကျေးဇူးများစသည်ဖြင့်လေ့လာကြရမှာဖြစ်ပါတယ်။ ဒီတော့အားလုံးခြုံပြောရရင် WAN Transmission, Connection နှင့် Components အပိုင်းတွေကိုအခြေခံမျှ ဒီအခန်းမှာလေ့လာကြမှာဖြစ်ပါတယ်။

၁၁.၁ Wide Area Netwrok အခြေခံ

WAN ဆိုတဲ့ Wide Area Network ကတော့အရိုးရှင်းဆုံးပြောရရင် ကြိုးမားတဲ့ဧရိယာရှိတဲ့ကွန်ရက်တစ်ခုပဲ၊ WAN ဆိုတာ LAN လိုပါပဲဗျာ။ သိပ်ပြီးကွာခြားသွားတယ်လို့တော့မရှိပါဘူး။ Interface တွေ Access Method တွေကတော့အတူတူပါပဲ။ အသုံးပြုသူ User တွေကသူတို့ရဲ့ LAN ကနေပြီးသော်လည်းကောင်း၊ ကိုယ့်နိုင်ငံ ကိုယ့်အရပ်ဒေသကနေသော်လည်းကောင်း WAN ကိုလှမ်းယူ Access လုပ်နိုင်ပါတယ်။ LAN နဲ့တော်တော်ကွာသွားတဲ့အချက်က Electronic Signal တွေဟာ ကမ္ဘာပတ်ပြီးလာရတာကြောင့် အချိန်နည်းနည်းစောင့်လိုက်ရတာလောက်ပဲ။ ဒါကလည်းအသုံးပြုထားတဲ့ Network Connection ရဲ့ Quality ပေါ်လည်းမူတည်ပါသေးတယ်။ နောက်တစ်မျိုးပြောရရင် LAN တစ်ခုချင်းစီကိုချိတ်ဆက်ပြီး Connection Level တက်လာအောင်ပြုလုပ်ထားတာဟာလည်း WAN ဖြစ်ပါတယ်။ ဒီလို Connection တွေရရှိလာအောင် Bridge တို့ Router တို့စတဲ့ အထူးပြုလုပ်ထားတဲ့ဆက်သွယ်ရေးပစ္စည်းတွေကို အသုံးပြုရမှာဖြစ်ပါတယ်။ ပြီးတော့ အင်တာနက်ဝန်ဆောင်မှုပေးမယ့် ISP-Internet Services Provider နှင့်ချိတ်ဆက်ထားရမှာဖြစ်ပါတယ်။ WAN တစ်ခုဖြစ်ပေါ်လာမှုမှာ အထက်ပါပစ္စည်း အထက်ပါအကြောင်းအရာနှင့်ပဲတည်ဆောက်လို့ရတာမဟုတ်ပါဘူး။ အောက်ဖော်ပြပါတို့နှင့်လည်း WAN ကိုချိတ်ဆက်ပေးနိုင်ပါတယ်။ အဲ့ဒါတွေကတော့ -

(၁) Packet Switching Networks

(၂) Fiber-Opitc Cable

(၃) Microwave Transmitters

(၄) Satellite Links

(၅) Cable Television Coaxial System တို့ပဲဖြစ်ကြပါတယ်။

ဒီနေရာမှာ WAN ကိုအသုံးပြုသူတွေဟာ အထက်ဖော်ပြပါရှုပ်ထွေးလှတဲ့နည်းပညာများကြောင့်

သူကိုအသုံးပြုမယ့် WAN ကို ကိုယ်တိုင်ပစ္စည်းဝယ်ယူခြင်း၊ တပ်ဆင်ခြင်းမျိုးမလုပ်ကြဘဲ Services Provider တွေဆီကနေပဲ ငှားရမ်းအသုံးပြုကြပါတယ်။ ဒီလိုငှားရမ်းအသုံးပြုတဲ့အခါမှာလည်း ကောင်းတဲ့အချက်ကဘယ်လောက်သုံးမလဲ။ နာရီ မိနစ်နှင့်တွက်ယူတာထက် များများသုံးမယ့်သူဆို Unlimited သုံးမယ်ဆိုရင် ပိုသက်သာတယ်ဗျ။ ဒီလို LAN နှင့် WAN အကြားဆက်သွယ်ပေးပို့မှုတွေဟာ အဓိကအားဖြင့် အောက်ပါနည်းပညာ (၃) ခုကိုအသုံးပြုလေ့ရှိကြပါတယ်။ အဲဒါကတော့ -

(၁) Analog Connectivity

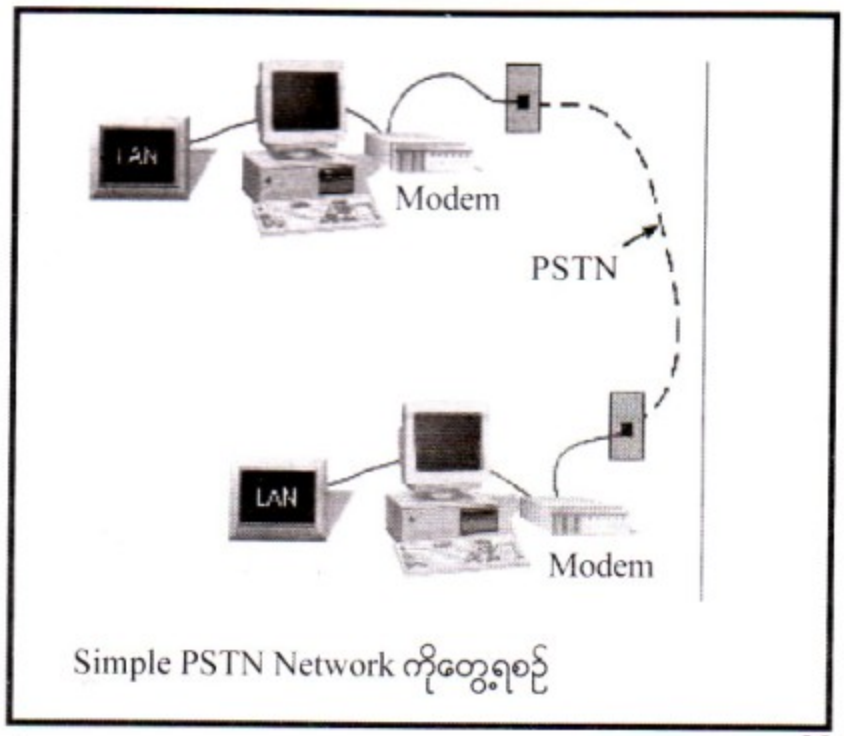
(၂) Digital

(၃) Packet Switching တို့ပဲဖြစ်ကြပါတယ်။

၁၁.၂ Analog Connectivity အကြောင်း

ကျွန်တော်တို့မှာရှိပြီးသား LAN နှင့်အခြား ကွန်ရက်တစ်ခုသော်လည်းကောင်း၊ အခြားသော Remote ကွန်ပျူတာကိုသော်လည်းကောင်း WAN Connection တစ်ခုပြုလုပ်ပြီးလှမ်းချိတ်လို့ရပါတယ်။ ဒီလိုကွန်ရက်ကိုတော့ PSTN- Public Switched Telephone Network ဒါမှမဟုတ် POTS - Plain Odd Telephone System လို့ခေါ်ပါတယ်။ PSTN ဆိုတာ Analog Phone Line နှင့် Modem ကိုအသုံးပြုပြီး ကွန်ပျူတာသုံးတဲ့ Digital Signal အဖြစ် Analog ကနေပြောင်းယူတာဖြစ်ပါတယ်။ ပုံမှာလည်းရိုးရှင်းတဲ့ PSTN Connection ကိုပြပေးထားပါတယ်။

ပုံ ၁၁.၁



Simple PSTN Network ကိုတွေ့ရစဉ်

PSTN မှာတစ်ခါပြောစရာရှိတာက အသုံးပြုတဲ့စနစ်ပေါ်နှင့် အသုံးပြုတဲ့ Media ပေါ်စသဖြင့်မူတည်ပြီး တော့ကား Quality ဟာပြောင်းလဲနိုင်ပါတယ်။ ဒါကြောင့်မို့လည်း PSTN ကိုဆက်သွယ်ရေးကိစ္စတွေမှာမူလ ကတည်းက Voice အတွက်ပဲအသုံးပြုခဲ့တာဖြစ်ပါတယ်။ PSTN ဟာ Quality မကောင်းပေမယ့် WAN ချိတ်ဆက်ဖို့အတွက်ကတော့ စီးပွားရေးအရကြည့်ရင် တွက်ချေကိုက်ပါတယ်။ နောက်တစ်ခုစဉ်းစားကြည့်ပိုက် ရင်လည်း PSTN ဟာ Modems ကိုအသုံးပြုပြီး ကွန်ပျူတာရဲ့ Digital Data ကနေ Analog တယ်လီဖုန်း လိုင်းကိုအသုံးပြုပြီး ပို့ရတာဖြစ်သောကြောင့် Data Transmission ဟာအဆမတန်ကိုနှေးကွေးပါတယ်။ နောက်တစ်ခုက PSTN က Circuit - Switched Network မျိုးဖြစ်တာကြောင့်ချိတ်ဆက်မှု Connection Quality ဟာတသမတ်တည်းမရှိတတ်ပါဘူး။ Connection အကွာအဝေးဟာပိုပြီးတော့ဝေးလာလေ Connection အရေအသွေးညံ့လာလေ ဒါမှမဟုတ် သုံးမရလေဖြစ်လာတတ်ပါတယ်။

ခုလောလောဆယ်မှာ တယ်လီဖုန်းကုမ္ပဏီတွေဟာ ၎င်းတို့ရဲ့ PSTN လိုင်းအချို့ကို ဒီဆက်ပိုကောင်း တဲ့ဆက်သွယ်မှုဖြစ်ပေါ်လာစေဖို့ Bandwidth ကောင်းစေဖို့ Fiber - Optic Cable များတပ်ဆင်နေကြပါတယ်။ ဒီလိုဆို Data Transmission ဟာပိုပြီးတော့စိတ်ချရမယ်။ ပိုပြီးတော့ကောင်းလာပါမယ်။ အောက်မှာ PSTN လိုင်းအမျိုးအစားနှင့် Quality လုပ်နိုင်စွမ်းအားတို့ကိုဖော်ပြပေးထားပါတယ်။

Line Type	Quality/Service Capability
1	Voice Only
2	Voice with minimal quality control
3	Voice and radio with tone conditioning
4	Less than 1200 bps data applications
5	Basic data
6	Voice and data over trunk circuits
7	Voice and data over private lines
8	Voice and ata over trunks between computers
9	Voice and video
10	Application relays, quality data

PSTN Connection ရဲ့အရည်အသွေးကိုကောင်းမွန်လာစေတဲ့ နည်းလမ်းတစ်ခုကတော့ - လိုအပ်မှ Dial Up လုပ်ပြီး Connection ရယူတဲ့ Random Circuits ကိုသုံးမယ့်အစား Dedicated လိုင်းကိုအသုံး ပြုဖို့ပါပဲ။ Dedicated လိုင်းတွေဟာလိုအပ်မှ Dial-Up လုပ်တဲ့ Dial-on-Demand Connection ထက်စာ ရင်ဈေးပိုကြီးသော်လည်း Quality ကြတော့ပိုကောင်းပါတယ်။ Data Transmission လည်းပိုကောင်းတယ်

ပေါ့ဗျာ။ Signal Quality လည်းပိုကောင်းသလိုနှောင့်ယှက်မှု Interference နှင့် Noice တွေကိုလည်း လျော့ချပေးတယ်ပေါ့ဗျာ။ ဒီတော့ အသုံးပြုသူဟာ Dial-Up ကိုပဲသုံးမလား။ PSTN Connection ကိုပဲသုံးမလားဆိုတာ အောက်ပါအချက်များနှင့်စဉ်းစားနိုင်ပါတယ်။

(၁) အသုံးပြုမည့်ကြာချိန် (Length of Connection Time)

(၂) ဘယ်လောက်ထိသုံးမလဲ၊ ဘယ်လောက်ထိကုန်ကျခံမလဲ။

(၃) အခြားသော Quality ပိုမိုကောင်းမွန်မှုများ

(၄) ၂၄ နာရီလုံး Connection ဖွင့်ထားဖို့လိုမလို၊ စသည်တို့ပဲဖြစ်ကြပါတယ်။

အကယ်၍များ Connection ကိုတစ်ခါတစ်လေမှသုံးမယ်။ သုံးစွဲမှုအချိန်ကိုလည်း ကန့်သတ်ထားမယ်ဆို Dial-Up လိုင်းကိုသုံးတာက ကုန်ကျစရိတ်ကိုသက်သာထိရောက်စေပါတယ်။ ဒီလိုမှမဟုတ်ဘဲ Constant Access မျိုးလိုချင်တယ်ဆိုရင်တော့ ဒီ Dial-Up ဟာသင့်ရဲ့လိုအပ်ချက်တွေကို အပြည့်ဝဆုံးလုပ်ဆောင်ပေးမှာမဟုတ်ပါဘူး။

၁၁.၃ Digital Connectivity အခြေခံများ

DDS ဆိုတဲ့ Digital Data Services လိုင်းဟာတိုက်ရိုက်ချိတ်ဆက်ခြင်း သို့တည်းမဟုတ် Point to Point Synchronous Communication ဖြစ်ပြီး Data Transmission Rates ကို 2.4, 4.8, 9.6, 56Kbps စသည်ဖြင့်ရရှိပါတယ်။ DDS တာအစွန်းနှစ်ဘက်အတွင်းမှာ Dedicated Digital Circuits ဖြင့် ချိတ်ဆက်ထားဖို့တိကျတဲ့ Transmission Rate နှင့် Quality ကိုပေးစွမ်းနိုင်ပါတယ်။ Digital Links ကိုသုံးခြင်းဖြင့်သိသာထင်ရှားစွာရရှိလာတဲ့ အကျိုးကျေးဇူးကတော့ Transmission ပြုလုပ်ရာမှာ 99% Error Free ဖြစ်တာပါပဲ။ ပုံမှန် PSTN Connection ဆိုရင် Error Rate က 40% အထိတောင်ပါရှိတတ်ပါတယ်။ DDS မှာမှအမျိုးအစားကွဲတွေရှိပါသေးတယ်။ အဲ့ဒီအထဲက အချို့ကိုဖော်ပြရမယ်ဆိုရင်တော့ -

(၁) ISDN

(၂) T1

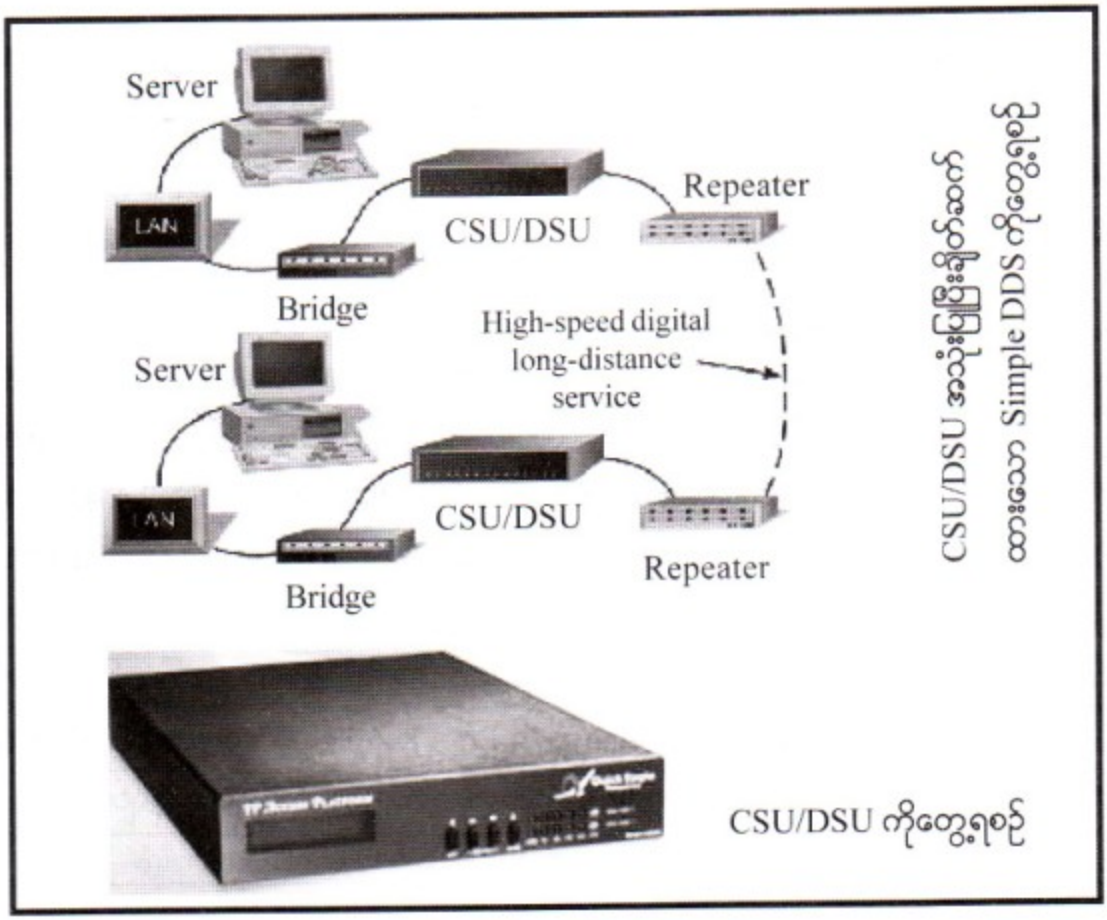
(၃) T3 နှင့်

(၄) Switched 56K တို့ပဲဖြစ်ကြပါတယ်။

DDS ဟာ Connection ဖြစ်တည်ဖို့အတွက် Modem ကိုအသုံးမပြုပါဘူး။ ဘာလို့လည်းဆိုတော့ ဒီ Communication တစ်လျှောက်လုံးဟာ လုံးဝ Digital ဖြစ်နေလို့ပါ။ ဒီတော့ Analog ကနေ Digital

ပြောင်းတာတို့ Digital ကနေ Analog ပြောင်းတာတို့မလိုတော့ဘူးလေ။ DDS ဟာ Modem ကိုသုံးမယ့်အစား CSU/DSU လို့ခေါ်တဲ့ Channel Services Unit / Data Services Unit ဆိုတဲ့အထူးပြုလုပ်ထားသော ဆက်သွယ်ရေးပစ္စည်းကို အသုံးပြုပါတယ်။ ကွန်ရက်ဟာ ၎င်း CSU/DSU ကိုသုံးပြီးတော့ Bridge ဒါမှမဟုတ် Router ဆီမှ Data တွေကိုလက်ခံပါတယ်။ ပုံမှာလည်းရိုးရှင်းတဲ့ DDS Network Connection ကိုပြထားပါတယ်။ CSU/DSU ဟာ Digital Network ကိုသုံးပြီးအခြားလက်ခံတဲ့ဘက်က CSU/DSU ဆီ Data တွေပို့နေတာဖြစ်ပါတယ်။ ပြောရမယ်ဆိုရင် Remote Network ကို Data တွေပို့ပေးနေတဲ့ Bridge ဒါမှမဟုတ် Router နှင့်ချိတ်ဆက်ထားတာပါပဲ။

ပုံ ၁၁.၂



T1 အကြောင်း

T1 ဟာကျွန်တော်တို့အသုံးပြုနေတဲ့ High Speed Digital Line ဖြစ်ပါတယ်။ DDS နည်းပညာဟာ ဝါယာကြိုးနှစ်ခုကိုအသုံးပြုပြီး Data တွေကို Full Duplex Transmit လုပ်ရာ ၎င်းရဲ့ Data ပို့တဲ့အမြင့်ဆုံး Rate ဟာ 1.544 Mbps အထိအများဆုံးပို့နိုင်ပါတယ်။ ဝါယာနှစ်ခုမှာတစ်စုံက Transmits လုပ်ပြီး နောက်တစ်စုံက Receives ပေါ့ဗျာ။ လက်ခံရယူတယ်ပေါ့။ T1 ဟာ Data ဖြစ်စေ၊ Voice ဖြစ်စေ နောက်ပြီး

Narrow Band Video စတာတွေကိုကောင်းစွာပေးပို့နိုင်ပါတယ်။ Low Quality ဖြစ်တဲ့လိုင်းတွေကို မသုံးလိုတဲ့အဖွဲ့အစည်းတွေအတွက် ဒီ T1 လိုင်းကိုဝယ်သည်ဖြစ်စေ၊ ငှားသည်ပဲဖြစ်စေ၊ ဈေးကတော့အသင့်အတင့်ကြီးပါတယ်။ အရမ်းကြီးမကြီးဘူးပေါ့ဗျာ။ T1 လိုင်းမှာသီးခြား Channel (24) လိုင်းပါရှိပြီးတော့ Channel တစ်ခုချင်းစီဟာ 64 Kbps Data Rate ရှိပါတယ်။ ဒီတော့ T1 ကြီးတစ်ခုလုံးကိုအငှားချထားမယ့်အစား T1 ရဲ့ Channel တစ်ခုကိုပဲဖြစ်စေ၊ တစ်ခုမကဖြစ်စေ အငှားချထားနိုင်ပါတယ်။ ဒီလို Services မျိုးကြတော့ Fractional T1 လို့ခေါ်ပါတယ်။ အချို့သော ဥရောပနိုင်ငံတွေမှာကြတော့ ဒီ Digital နည်းပညာပဲ ဒါပေမယ့် သူက T1 မဟုတ်ဘူး E1 တဲ့ Signal Rate က 2.048 Mbps ရှိပါတယ်။

ဒီနေရာမှာ T1 နှင့်ပတ်သက်ပြီးတော့ Multiplexing ဆိုတဲ့အကြောင်းကိုအနည်းငယ်ရှင်းပြပါအုံးမယ်။ Multiplexing ခေါ် Maxing ဟာ Cable Segment တစ်ခုထဲမှာ တစ်ခုမကသော Communication တွေ စီးဆင်းနိုင်အောင်ပြုလုပ်နိုင်ပါတယ်။ ရှင်းအောင်ပြောရမယ်ဆိုရင် ကြိုးကတစ်ကြိုးတည်းပေါ့ဗျာ။ ဒီကြိုးမှာ သွားလာနေတဲ့ Communication ကြတော့တစ်ခုမကဘူး။ ဒီလို Telephone Line တစ်ခုထဲမှာပဲ တစ်ခုမကတဲ့ Conversation တွေတစ်ပြိုင်တည်းသွားနိုင်ဖို့ Multiplexing ကို Bell Labs ကလွန်ခဲ့သောနှစ်ပေါင်းများစွာကတည်းက ထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ ဒီ Multiplexing နည်းပညာကိုအသုံးပြုပြီးတော့ Bell Labs ဟာ T-Carrier Network ကိုပြုလုပ်ခဲ့တာဖြစ်ပါတယ်။ သူဟာ ၎င်း Multiplexing ထက်ပိုမိုတတ်နိုင်လာအောင် နည်းပညာကိုတိုးချဲ့ထားပြီးတော့ ဒီ Cable တစ်ခုထဲမှာပဲ ဆက်သွယ်မှုများစွာကို တစ်ပြိုင်တည်းချိတ်ဆက်ပေးပါတယ်။ T1 ဟာ Multiplexing ကိုအသုံးပြုပြီးတော့ နေရာအသီးသီးကပြောရင် မတူညီတဲ့ Sources တွေဆီက Data တွေကိုပေါင်းစည်းပြီး Cable တစ်ခုတည်းနှင့်ပဲ ပို့ဆောင်ပေးနိုင်ပါတယ်။ အဲ့ဒီလို ပေါင်းစည်းထားတဲ့ Multiplex Data တွေကိုလက်ခံရရှိတဲ့အခါ မူလပုံစံပြန်ရအောင် Decode ပြန်လုပ်ရပါတယ်။

ခုနကပြောခဲ့တဲ့အတိုင်းပါပဲ။ T1 မှာ Channel 24 ခုရှိပါတယ်။ Channel တစ်ခုချင်းစီဟာ 64 Kbps Data Transmission ရှိပါတယ်။ Channel တစ်ခုချင်းစီဟာ Data တွေကို ၁ စက္ကန့်မှာ အကြိမ် ၈၀၀၀ Data Sampling လုပ်နိုင်ပြီး Data Sample တစ်ခုစီမှာ 8 bits ပါရှိပါတယ်။ ဒီတော့ စာဖတ်သူ မြှောက်ကြည့်လေ။ Data Sample တစ်ခုမှာ 8 bits။ ဒါမျိုး ၁ စက္ကန့်မှာ အကြိမ် ၈၀၀၀ လုပ်နိုင်တော့ Channel တစ်ခုစီဟာ ၁ စက္ကန့်မှာ 64 K ဖြစ်သွားတာပေါ့။ ဒီနှုန်းနဲ့ Data ပို့တာကို DS-O လို့ခေါ်ပါတယ်။ အာကယ်၍ T1 ရဲ့ Channel ၂၄ ခုစလုံးအပြည့်နှုန်းဆိုရင်တော့ ၎င်းကို DS-1 လို့ခေါ်ပါတယ်။ DS ဆိုတာ DDS ရဲ့အမျိုးကွဲပါပဲ။ တစ်ဖက်မှာ Data Rate တွေကိုပြထားပါတယ်။

Multiplexing ဟာ DS-1 ရဲ့ နှုန်းကို အထိမြှင့်နိုင်ပါတယ်။ ပုံမှန် Copper Wire ကတော့ T1 နှင့် T2 အထိပဲ Transmission လုပ်နိုင်ပါတယ်။ T3 နှင့် T4 လိုင်းဆိုရင်တော့ Microwave ဒါမှမဟုတ် Fiber Optic ကိုလိုအပ်ပါလိမ့်မယ်။

DS Level	Carrier	T1s	Channels	Data Rate (Mbps)
DS-0	N/A	N/A	1	064
DS-1	T1	1	24	1.544
DS-1C	T1C	2	48	3.152
DS-2	T2	4	96	6.312
DS-3	T3	28	672	44.736
DS-4	T4	168	4032	274.760

T3 အခြေခံချိတ်ဆက်မှု

T3 ဟာ T1 လို 28 လိုင်း အပြန်အလှန်ချိတ်ဆက်ထားတဲ့ Channels ပေါင်း 672 အထိရပါတယ်။ စာဖတ်သူခင်ဗျား 28 ကို T1 ရဲ့ 24 Channels နှင့် မြှောက်လိုက်တာပါပဲ။ Data Rate ကတော့ 44.736 Mbps အထိရပါတယ်ခင်ဗျား။ ဝန်ဆောင်မှုပေးတဲ့ ကုမ္ပဏီကြီးတွေဟာ T3 အားလုံးကိုဖြစ်စေ၊ Fractional T3 ဖြစ်စေ Transmission Rates ကို 6Mbps မှ အထက်အထိ အဌားချထားကြပါတယ်။

Switched 56K အခြေခံချိတ်ဆက်မှု

Switched 56K Leased လိုင်းတွေဟာ အရင်တစ်ခေတ်ကသုံးခဲ့တဲ့ Older Digital Point to Point Communication ပဲဖြစ်ပါတယ်။ အခုဖြစ်ပေါ်နေတဲ့ Fiber Optic တို့ Multiplexing တို့မပေါ်ခင် တုန်းကတော့ PSTN Connections တွေထက်စာရင် ဒီ 56K Digital Network က အကောင်း ဆုံးတစ်ခုပေါ့။ ၎င်းရဲ့ Circuit ဟာ တစ်ဦးတစ်ယောက်အတွက် လိုင်းဖွင့်ပေးထားတာမျိုးမဟုတ်တဲ့ Customer တစ်ဦးဦးက လိုအပ်လာတဲ့အချိန်ကြမှ လိုင်းကိုဖွင့်ပေးတာဖြစ်ပါတယ်။ ဒီတော့ အခုလို အဌားအသုံးပြုခက ၂၄ နာရီစလုံး အကောက်ခံတာမဟုတ်ဘဲ အသုံးပြုတဲ့မိနစ်ကိုအခြေခံပြီး ကောက်ခံတာ ဖြစ်ပါတယ်။ ကနေ့ခေတ်မှာဆိုရင် နေရာတော်တော်များများမှာရှိတဲ့ Cable Modem နှင့် DSL တွေ အဆင်သင့်ရရှိနိုင်မှုတွေပေါ်မူတည်၍ ၎င်း Switched 56K Service ကို Frame Relay Services အတွက် 56 kbps Channels တစ်ခုမက စုပေါင်းအသုံးပြုတဲ့အခါမှာပဲသုံးပါတော့တယ်။

၁၁.၄ Packet Switching Network အခြေခံချိတ်ဆက်မှု

Packet Switching Networks ကို အကွာအဝေး နီးနီးဖြစ်စေ၊ ဝေးဝေးဖြစ်စေ ဆက်သွယ်ရာမှာ အသုံးပြုနိုင်ပါတယ်။ ၎င်း Networks မျိုးဟာ မြန်ဆန်တယ်၊ သွက်လက်တယ်၊ စိတ်ချရတယ်ဆိုတဲ့ နည်းပညာ

ပျိုးပါ။ ဒီနည်းကို ဘာဖြစ်လို့ Packet Switching လို့ခေါ်လဲဆိုရင် Data လေးတွေကို အပိုင်းပိုင်း ဖြတ်ထုတ်ပြီး သေးငယ်တဲ့ Package လေးတွေအဖြစ်ပြန်ထုတ်လိုက်လို့ဖြစ်ပါတယ်။ ကဲ ဒါကြောင့် Packet လို့ခေါ်တယ် ပေါ့ဗျာ။ Switching လို့ဘာလို့ခေါ်ရသလဲဆိုတာကြတော့ သူကဒီ Packets လေးတွေကို ရည်ရွယ်ရာတစ် နေရာကိုရောက်အောင် နေရာပေါင်းစုံလမ်းကြောင်းပေါင်းစုံကနေသယ်ယူပို့ဆောင်ပေးနိုင်လို့ဖြစ်ပါတယ်။ အင်တာနက်ဟာ Packet Switching အတွက်အဓိကအကောင်းဆုံးဥပမာဖြစ်ပါတယ်။ Packet Switching Network ဟာ Data တွေကိုအောက်ပါပုံစံဖြင့် ကိုင်တွယ်ပါတယ်။ ကဲဘယ်လိုပုံစံပါလိမ့်။

(၁) မူရင်း Data တွေကို Packet တွေအဖြစ်ပိုင်းလိုက်ပါတယ်။

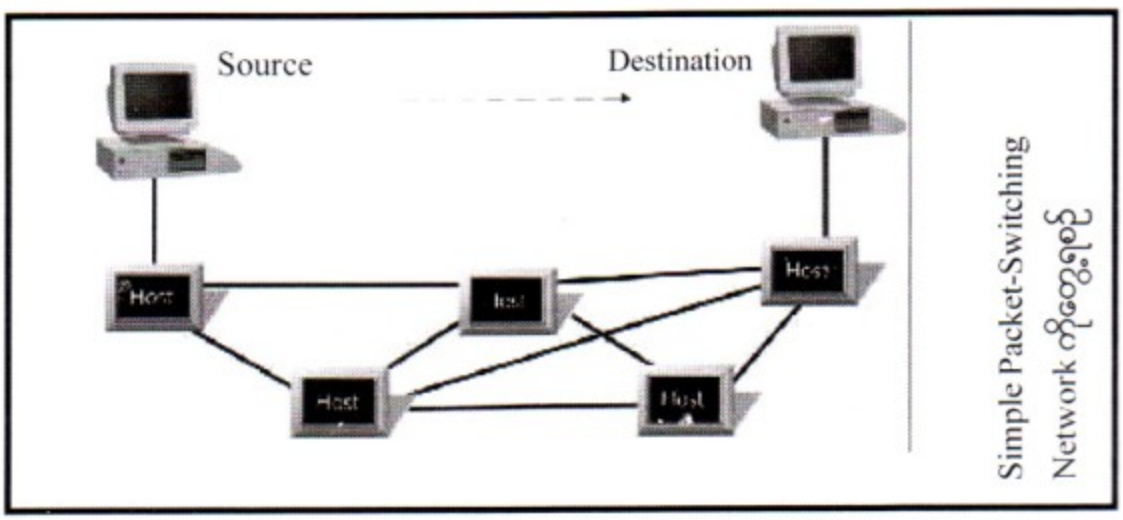
(၂) Packet တစ်ခုချင်းစီဟာတန်းစီအနေအထားမို့ ဘယ်ကိုသွားရမယ်ဆိုတဲ့ လိပ်စာနှင့် Sequence Order ကို Packet တိုင်းမှာ Label ချိတ်ထားပါတယ်။

(၃) ရည်ရွယ်ရာကိုရောက်ရန် Network မှာ Packet တွေဟာ တစ်ခုချင်းစီသီးခြားပေးပို့တာဖြစ်ပါတယ်။

(၄) Host ဟာ Packet ကို လက်ခံရရှိချိန်မှာ ၎င်း Packet ရဲ့ Header ကိုဖတ်လိုက်ပါတယ်။ အကယ်၍ များ Host ဟာ Packet ရဲ့ Header က Packet သွားရမယ့် Destination ရည်ရွယ်ရာဖြစ်နေခဲ့မယ် ဆိုရင် Host ဟာ ၎င်း Packet ကိုယူထားလိုက်ပါတယ်။ အကယ်၍မဟုတ်ဘူးဆိုရင်တော့ ၎င်း Host ဟာ Packet သွားရမယ့်နေရာကို အမြန်ဆုံး အတိုဆုံးလမ်းကြောင်းမှ တဆင့်ပေးပို့ပါတော့ တယ်။

(၅) ရည်ရွယ်ရာသို့ Packet တွေအားလုံး ရောက်ရှိချိန်မှာတော့ ၎င်းစက်ဟာ Packet တွေရဲ့ Header မှာပါတဲ့ Sequence နှင့်ပတ်သက်တဲ့ အချက်အလက်တွေကို ဖြည့်ပြီး မူလ Data ရအောင်ပြန်တည် ဆောက်ပါတော့တယ်။ ပြုတ်ကျပျက်စီးပျောက်ဆုံးတဲ့ Packets တွေကိုတော့ ပြန်လည်ပြီးပေးပို့ ဖို့လိုအပ်ပါတယ်။

ပုံ ၁၁.၃



Packet Switching ရဲ့အဓိကကောင်းတဲ့အကျိုးကျေးဇူးကတော့ ပေးပို့သူနှင့်လက်ခံသူအကြားမှာ Data ကိုပေးပို့ဖို့အတွက်လမ်းကြောင်းတစ်ခုတည်းကို မှီခိုတာမဟုတ်ပါဘူး။ Packet တစ်ခုချင်းစီရဲ့ Header မှာပါရှိတဲ့ Sequential နှင့်ပတ်သက်တဲ့စီတန်းအချက်အလက်ဟာအရေးကြီးပါတယ်။ ဘာလို့လဲဆိုတော့ Packet တွေဟာရည်ရွယ်ရာကိုရောက်လာတဲ့အခါ အစီအစဉ်အတိုင်းရောက်လာတာမဟုတ်တာကြောင့် ပြန်တန်းစီဖို့အခက်အခဲမရှိအောင်တို့ပဲဖြစ်ပါတယ်။ Packet လေးတွေဟာသေးငယ်တဲ့အတွက်ကြောင့် Data အဖြစ်ပြန်လည်ပေါင်းစည်းတဲ့အခါ တကယ်လို့များ Packet တစ်ခုကပျောက်ဆုံးနေခဲ့ရင် အဲ့ဒီပျောက်ဆုံးနေတဲ့ Packet လေးကိုပဲပြန်ပို့ပေးရမှာ ခုနက Packet လေးတွေဟာသေးငယ်တာကြောင့် ပြန်ပို့ချိန်အချိန်အနည်းငယ်ပဲကုန်မှာဖြစ်ပါတယ်။ ဒီ Packet Switching နှင့်ပတ်သက်ပြီး Virtual Circuits အကြောင်းကိုပြောပြပါအုံးမယ်။

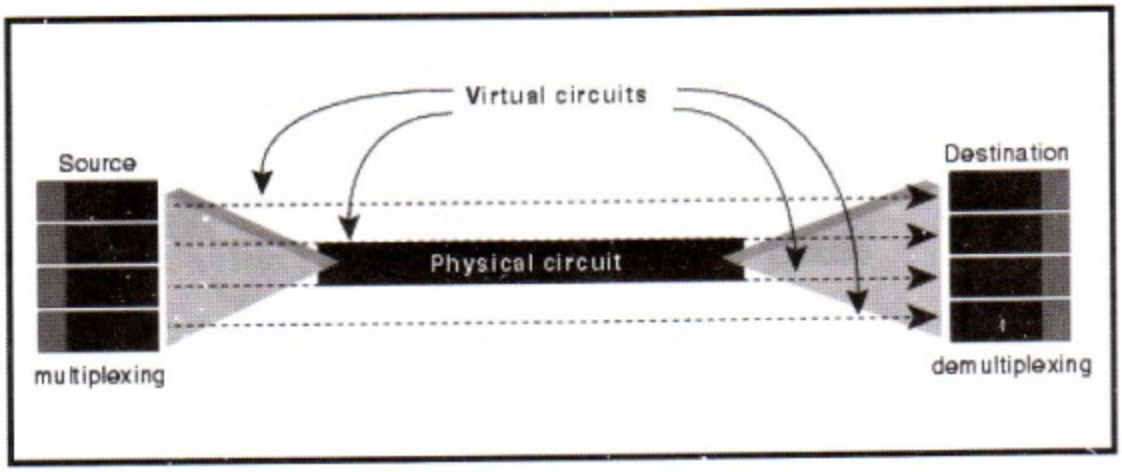
၁၁.၅ Virtual Circuits အကြောင်း

Packet Switching ကွန်ရက်တော်တော်များများဟာ ပေးပို့သူနှင့် လက်ခံသူအကြား Point နှစ်ခုမှာယာယီ Dedicated Line တွေကို ပံ့ပိုးပေးဖို့အတွက် Virtual Circuits ကိုအသုံးပြုပါတယ်။ ဒီ Virtual Circuit မှာတကယ့် Cable တွေအစား ပေးပို့ရမယ့် သတ်သတ်မှတ်မှတ်လမ်းကြောင်းအတွက် Logical ပိုင်းဆိုင်ရာစီတန်းထားတဲ့ Connection တွေပဲပါဝင်ပါတယ်။ ပေးပို့သူနှင့်လက်ခံသူအကြားမှာ နှစ်ဖက်ကွန်ပျူတာတွေဟာ လိုအပ်တဲ့ Bandwidth တွေပေးပို့မယ့်လမ်းကြောင်းတွေနှစ်ဦးနှစ်ဖက်သဘောတူပြီးတိုင်းမှာ ဒီလမ်းကြောင်းကိုပြုလုပ်ပါတယ်။ Transmission အရည်အသွေး Quality ကောင်းဖို့ရယ်ဆက်သွယ်မှု အောင်မြင်သေချာစေဖို့အတွက် Virtual Circuits ဟာ Data ရရှိကြောင်း Acknowledgement တွေ၊ Flow Control တွေ Error Control တွေနှင့်ထိတွဲဖက်အလုပ်လုပ်ဆောင်ပါတယ်။ Virutal Circuits အမျိုးအစားနှစ်မျိုးရှိပါတယ်။ အဲ့ဒါကတော့-

(၁) Switched နှင့်

(၂) Permanent တို့ဖြစ်ကြပါတယ်။

ပုံ ၁၁.၄



Switched Virtual Circuits အစည်းအဝေး

SVCs ဆိုတဲ့ Switched Virtual Circuit ဟာ Transmission ကိုလိုအပ်ရင် Establish လုပ်တယ်။ Transmission ပြီးသွားရင် Terminate လုပ်တယ်။ နောက်တစ်နည်းပြောရရင် ဒီလမ်းကြောင်းဟာ အသုံးပြုနေစဉ်ပဲနှစ်ဦးနှစ်ဖက်အကြားဆက်သွယ်မှုလမ်းကြောင်းရှိတယ်လို့ပြောချင်တာပါ။

Permanent Virtual Circuits အစည်းအဝေး

PVCs ဆိုတဲ့ Permanent Virtual Circuits ဟာ Leased (Dedicated) Line လိုပါပဲ။ နှစ်ဦးနှစ်ဖက်ကြားဆက်သွယ်ရေးလမ်းကြောင်းဟာ Logical Connection အနေနဲ့ အမြဲပွင့်နေပါတယ်။ ဒီလမ်းကြောင်းဟာအသုံးမပြုတဲ့အချိန်မှာလည်းရှိနေတယ်လို့ပြောချင်တာဖြစ်ပါတယ်။

၁၁.၆ Virtual Private Networks အစည်းအဝေး

ဒီနေရာမှာ အလျဉ်းသင့်လို့ VPNs ဆိုတဲ့ Virtual Private Network အကြောင်းကိုတင်ပြပါဦးမယ်။ VPNs ဟာယာယီဖြစ်စေ၊ အမြဲတမ်းဖြစ်စေ Public Network ဥပမာ အင်တာနက်လိုဟာမျိုးကိုသုံးပြီး Connection ပြုလုပ်နိုင်ပါတယ်။ ၎င်းမှာ Packets တွေဟာ Public Network တစ်လျှောက်သွားလာနေပေမယ့် ဒီပို့လွှတ်ထားတဲ့ Data တွေကိုတစ်စုံတစ်ယောက်ကိုစောင့်ကြည့်ခြင်း Decode ပြန်လုပ်ခြင်းတို့နဲ့ ထွင်းဖောက်ခြင်းတို့မှ မပြုလုပ်နိုင်ရန် Special Encryption ကိုအသုံးပြုပါတယ်။ ဒီတော့ကား ဒီမှာက Public Network မှာသွားလာနေပေမယ့် ဒီပေးပို့သူနဲ့လက်ခံသူ Connection တွေဟာ Public နှင့်မတူဘဲ Private လိုဖြစ်နေပါတယ်။

Windows 2000, Windows NT 4.0, Windows Millennium, Windows 98 တို့မှာ PPTP (Point-to-Point Tunneling Protocol) ဆိုတဲ့ အထူး TCP/IP Protocol ပါရှိပါတယ်။ ၎င်း PPTP ကိုအသုံးပြုပြီးတော့ အထက်ပါ OS တွေဟာ RAS-Remote Access Service Run ထားတဲ့ Windows NT Server အိမှမဟုတ် RRAS-Routing and Remote Access Service Run ထားသော Windows 2000 တွေကို Dial-in လုပ်လို့ရပါတယ်။ ၎င်းဟာ အင်တာနက်ကိုအသုံးပြုပြီး Private ဖြစ်တဲ့ Encrypted Dial-Up ကိုပံ့ပိုးပေးပါတယ်။ VPN ဟာ အင်တာနက်ကိုအသုံးပြုပြီး Connection ကိုအမြဲတမ်း ဖွင့်ထားလို့ရပါတယ်။

Windows 2000 ဟာအသစ်လည်းဖြစ်တယ်။ ပိုပြီးတော့လည်းစိတ်ချရတယ်ဆိုတဲ့ အခြားသော VPN Protocol တစ်ခုဖြစ်သော Layer 2 Tunneling Protocol - L2TP ကိုလည်း Support လုပ်ပါသေးတယ်။ Windows 2000 ဟာ PPTP အိမှမဟုတ် L2TP ကို IP Secure ဆိုတဲ့ IPSec နှင့်တွဲဖက်အသုံး

ပြုပြီး အင်တာနက်ကနေဖြစ်စေ၊ သီးခြား Private Carrier နှင့်ဖြစ်စေ စိတ်ချရတဲ့ Safe & Secure VPN Connection ပြုလုပ်ပေးနိုင်ပါတယ်။ ဒါဟာ Windows 2000 ကို Windows NT နှင့် Shares လုပ်ပေးနိုင်အောင်ချဲ့ထွင်ပေးလိုက်တာဖြစ်ပြီး Windows 2000 ဘက်မှာလည်း ပို Advance ဖြစ်တဲ့ Authentication နှင့် Encryption တို့ကိုလည်း Support လုပ်လာနိုင်ပါတယ်။ ကနေ့ခေတ်မှာဆိုရင်တော့ လိုအပ်ချက်တွေအရ Dial-up Connections, Dedicated PPTP နှင့် L2TP Connections တွေကိုအသုံးပြုမှု များပြားလို့လာပါတယ်။

၁၁.၇ Advanced WAN Technologies အခြေခံ

WAN နည်းပညာနှင့်ပတ်သက်ပြီးတော့ အခြေခံလေးတွေပြောပြပြီးတဲ့အခါမှာတော့ ဒီထက်ပိုပြီး Advanced ဖြစ်တဲ့ နည်းပညာတွေကို ထပ်မံလေ့လာကြရအောင်။

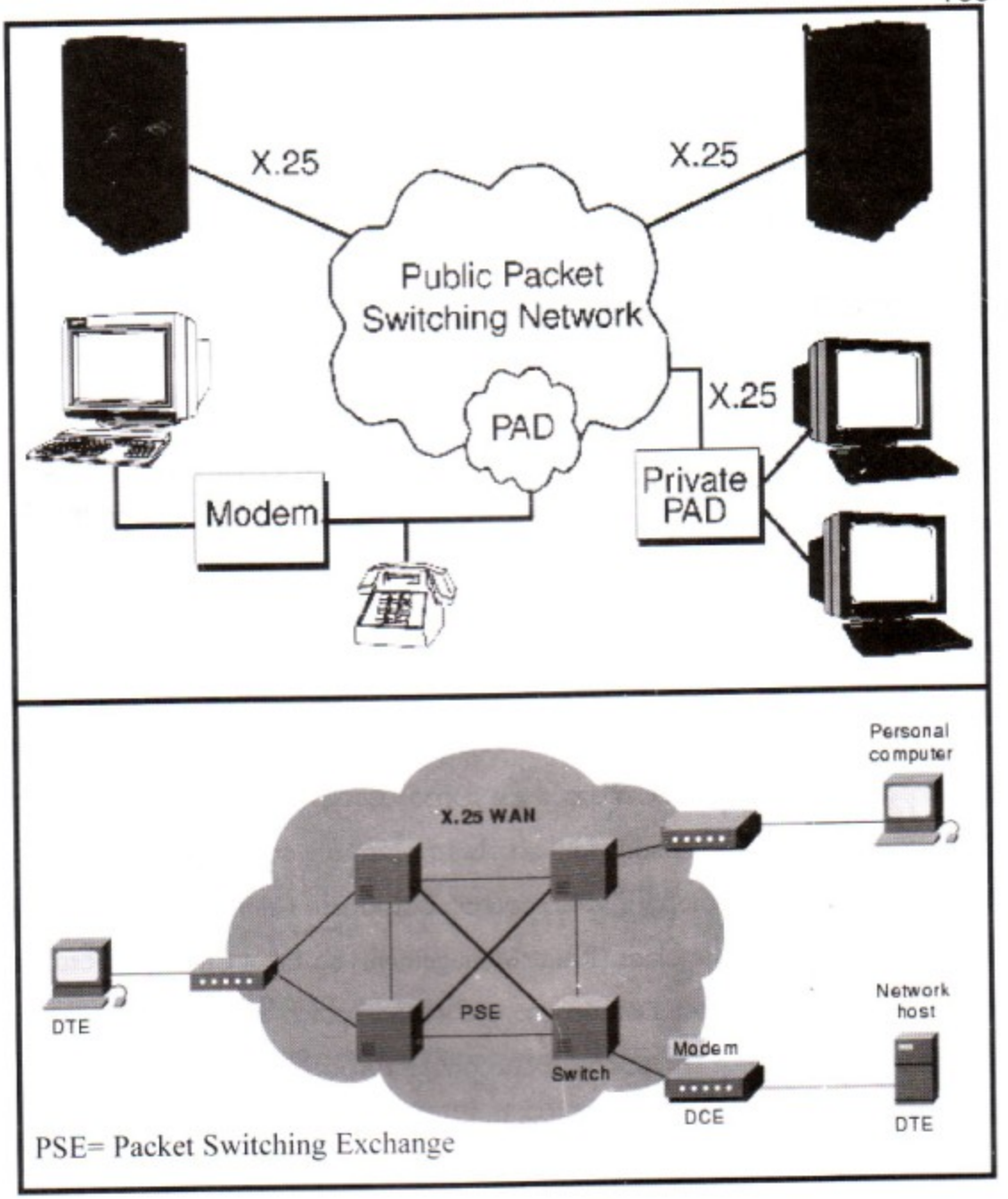
X.25 အခြေခံ

၁၉၇၀ နှစ်များအလယ်လောက်ကတည်းကပေါ်လာတဲ့သော X.25 ဟာ Public Packet Switching Network နှင့် သူတို့ရဲ့ Customers တွေကို (Interface) ဆက်သွယ်ပေးမှာဖြစ်ပါတယ်။ ၎င်းကို များသောအားဖြင့် Central Mainframe နှင့် Mainframe ၏ Remote Terminal များချိတ်ဆက်ရာတွင် အသုံးပြုပါတယ်။ X.25 ဟာ အဲ့ဒီလိုချိတ်ဆက်ထားတဲ့ Internetwork မှာ ပစ္စည်းတွေကို ဘယ်လို ချိတ်ဆက်ရမယ်ဆိုတာကိုသတ်မှတ်ပေးပါတယ်။ X.25 Networks တွေဟာ SVC (Switched Virtual Circuit) Network တွေဖြစ်ကြပြီး သူတို့ဟာ ဆင့်ကဲပေးပို့မှု Transmission upon Transmission ဖြင့် အကောင်းဆုံးသော လမ်းကြောင်းကိုဖန်တီးနိုင်ပါတယ်။

အရင်ခေတ်က X.25 Networks တွေဟာ ပုံမှန်တယ်လီဖုန်းလိုင်းကိုအသုံးပြုပြီး ဆက်သွယ်မှုပြုလုပ်ကြပါတယ်။ အဲ့ဒီမှာကြုံတွေ့ရတာတွေက Error တွေများတာရယ်၊ Data Lost ဖြစ်တာရယ်ကြောင့် နောက်ပိုင်းမှာ X.25 ကိုပိုမိုကောင်းမွန်စေသောဘာ Error Checking နှင့်ပြန်လည်ပေးပို့ခြင်း အစီအစဉ် Retransmission Schemes ကိုထည့်သွင်းခဲ့ပါတယ်။ ဒါပေမယ့် Speed ကတော့ လျော့သွားခဲ့ပါတယ်။ အဲ့ဒီ Error Control တွေကြောင့် X.25 ဟာ 64Kbps သာ Transmission လုပ်နိုင်ပါတော့တယ်။ ၁၉၉၂ မှာတော့ ၎င်း X.25 ကို ပိုမိုကောင်းမွန်အောင်ပြန်လုပ်ပြီးထုတ်တဲ့အခါ X.25 ဟာ Connection တစ်ခုတိုင်းမှာ 2Mbps အထိရလာပါတယ်။ ဒါပေမယ့် ဒီ Version အသစ်ကိုကျယ်ပြန့်စွာအသုံးမချနိုင်ခဲ့ပါဘူး။

X.25 ဟာ ပုံမှန်အားဖြင့်လည်း PDNS လို့ခေါ်တဲ့ Public Data Network တွေနှင့်လည်းတွဲဖက်အလုပ်လုပ်လေ့ရှိပါတယ်။ PDN Service ဆိုတာ AT&T, General Electric, Tymnet နှင့် အခြားသော စီးပွားရေးဝန်ဆောင်မှုပေးနေတဲ့အဖွဲ့အစည်းတွေကပေးနေတဲ့ Service တစ်ခုပါပဲ။ X.25 Network ကို

ပုံ ၁၁.၅



DTE လို့ခေါ်တဲ့ Data Terminal Equipment နှင့် DCEs လို့ခေါ်တဲ့ Data Communication Equipment ကိုသုံးပြီး အောက်ပါနည်းတစ်ခုခုနှင့်ချိတ်ဆက်နိုင်ပါတယ်။

(၁) ကွန်ပျူတာမှာ X.25 Network Card တပ်ဆင်လည်းကောင်း

(၂) Low-Speed Character-Based Terminals တွေမှာ X.25 Communication ကို Support လုပ်တဲ့ PAD (Packet Assembler/ Disassembler) တွေမှာတပ်ဆင်လည်းကောင်း

(၃) LAN/WAN တွေမှာ X.25 Gateway တပ်ဆင်သော်လည်းကောင်းချိတ်ဆက်နိုင်ပါတယ်။ X.25

Networks တွေဟာစိတ်ချရတယ်။ Error Free ဖြစ်တဲ့ ဆက်သွယ်ရေးကို ပံ့ပိုးပေးတယ် ဆိုတာ တောင်မှ X.25 နည်းပညာကိုအသုံးပြုမှဟာ နည်းလို့လာပါတယ်။ ဘာလို့လဲဆိုတော့ Speed မှာ ကန့်သတ်ချက်ရှိနေတာရယ်၊ ဒီထက်ပိုပြီး Speed ပိုကောင်းတဲ့ Frame Relay တို့ ATM တို့က Develop ပိုမိုဖြစ်လာခြင်းနှင့် အသုံးချလာခြင်းတို့ကြောင့်ဖြစ်ပါတယ်။

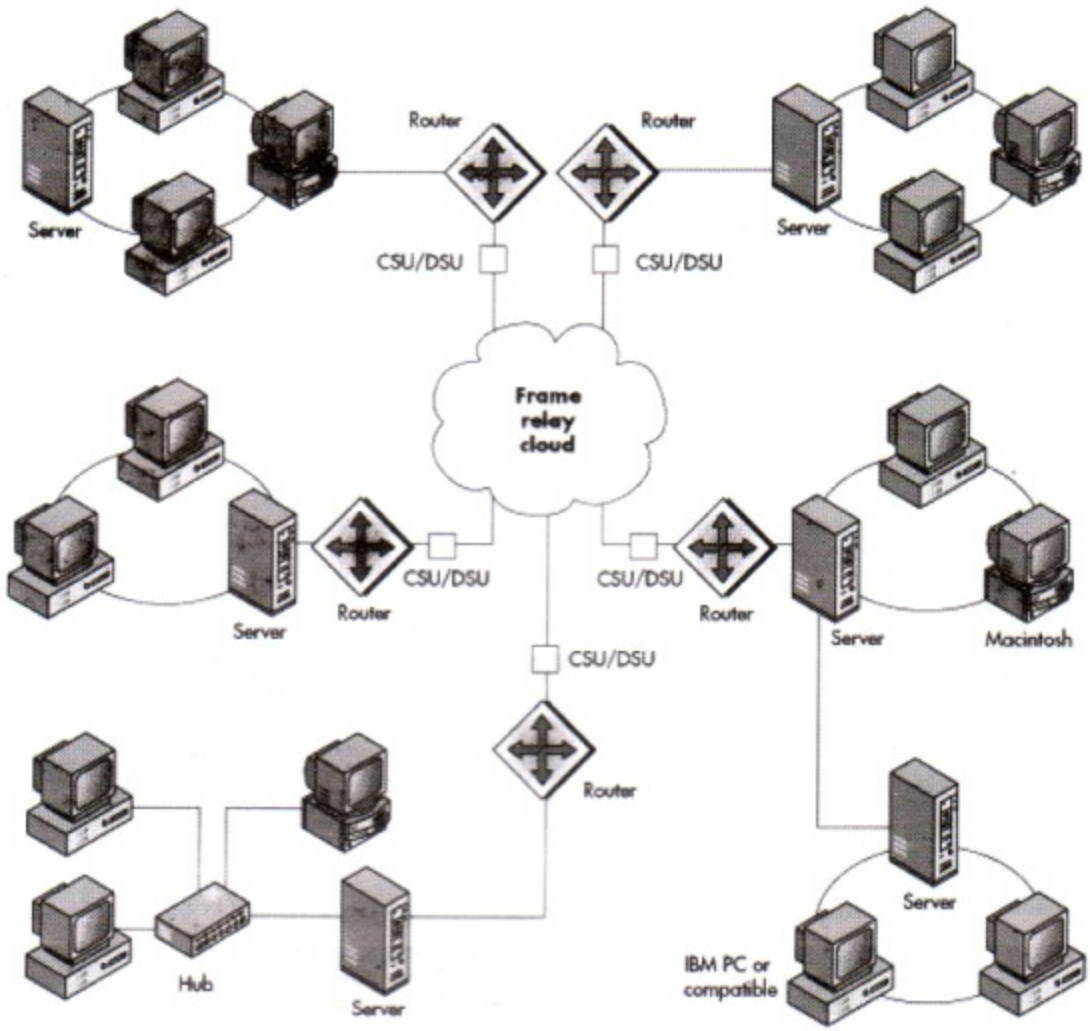
Frame Relay အကြောင်း

Frame Relay ဆိုတာ မြန်ဆန်တယ်၊ စိတ်ချရတယ်၊ Digital Packet Switching Network ဖြစ်တယ်ဆိုတဲ့ Point-to-Point PVC (Permenant Virtual Circuit) နည်းပညာနှင့် WAN ကိုဆက်သွယ်ရေးဖြစ်ပါတယ်။ ၎င်းဟာ X.25 နှင့် ISDN နည်းပညာများမှ Developed ဖြစ်လာတာဖြစ်ပါတယ်။ Frame Relay ဟာ Error Checking ကိုအသုံးမပြုပါဘူး။ Frame Relay Connections ကအများဆုံးအသုံးပြုတဲ့ Digital Fiber-Optic Links တွေဟာ Error Checking လုပ်ဖို့မလိုအပ်ပါဘူး။

Frame Relay ဟာ OSI Model ရဲ့ Data Link Layer ကနေ Data Transmission လုပ်ဖို့ အလျားမတူညီတဲ့ Pakcets အဖြစ်မဟုတ် Frame တွေကိုအသုံးပြုကြပါတယ်။ Frame Relay ဟာ Points တွေအကြားဆက်သွယ်ရေးမှာ PVC ကိုအသုံးပြုပြီး ဆက်သွယ်ရေးတစ်လျှောက် တူညီတဲ့လမ်းကြောင်းကိုပဲ အသုံးပြုကြပါတယ်။ အဖြစ်လည်း Bandwidth ကောင်းကောင်းရမယ်။ ပေးပို့မှုလည်းသေချာမှာဖြစ်ပါတယ်။ PVC ဆိုတာ Dedicated လိုင်းလိုပါပဲ။ အဲ့ဒီမှာ ဆက်သွယ်ရေးပစ္စည်း Communication Device တွေဟာ လမ်းကြောင်းလွှဲခြင်းကို ထိန်းချုပ်ခြင်း (Route Management) နှင့် Error Checking ပိုင်းဆိုင်ရာတွေကို မလုပ်ကြပါဘူး။ ဘာလို့လဲဆိုတော့ Data တွေဟာ ထွက်လာကတည်းက ဒီကိုသွားရမယ်ဆိုတာသိနေလို့ပါပဲ။ ပြောရရင် ဘယ်မှသဝေထိုးပြီး ရွာရိုးပေါက်အောင်လျှောက်သွားစရာမလိုဘူးလို့ပြောချင်တာပါ။ အဲကြောင့်လည်း Frame Relay နည်းပညာဟာ Transmission Rates ကို 56 Kbps ကနေ 1.544 Mbps (T1 Speed) အထိရရှိပါတယ်။

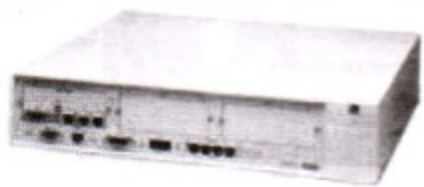
Frame Relay Services ဟာလျှင်မြန်စွာကြီးထွားလို့လာနေပါတယ်။ ဘာလို့လဲဆိုတော့ သူတို့ဟာ ATM ထက်စာရင် ဈေးလည်းမကြီးဘူး။ Customer ကိုလည်း သူတို့လိုအပ်တဲ့ Bandwidth အတိုင်း သတ်မှတ်ပြီးပေးနိုင်တယ်။ အသုံးပြုမှုရဲ့ ဝန်ဆောင်ခဟာ PVC ရဲ့ Bandwidth ကိုမူတည်ပြီးကောက်တာဖြစ်ပါတယ်။ အဲကို CIR- Committed Information Rate လို့ခေါ်ပါတယ်။ Frame Relay Connection တွေဟာ CSU/DSU အစုံလိုက်အသုံးပြုတာဖြစ်ပါတယ်။ T1 လိုင်းလိုပဲ တစ်ဖက်စီမှာ Router အဖြစ်မဟုတ် Bridge နှင့် တွဲဖက်ပြီးလုပ်တာဖြစ်ပါတယ်။

ပုံ ၁၁.၆

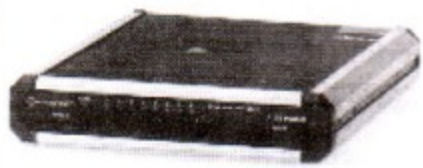


Frame Relay Network ကိုတွေ့ရစဉ်

ပုံ ၁၁.၁၇



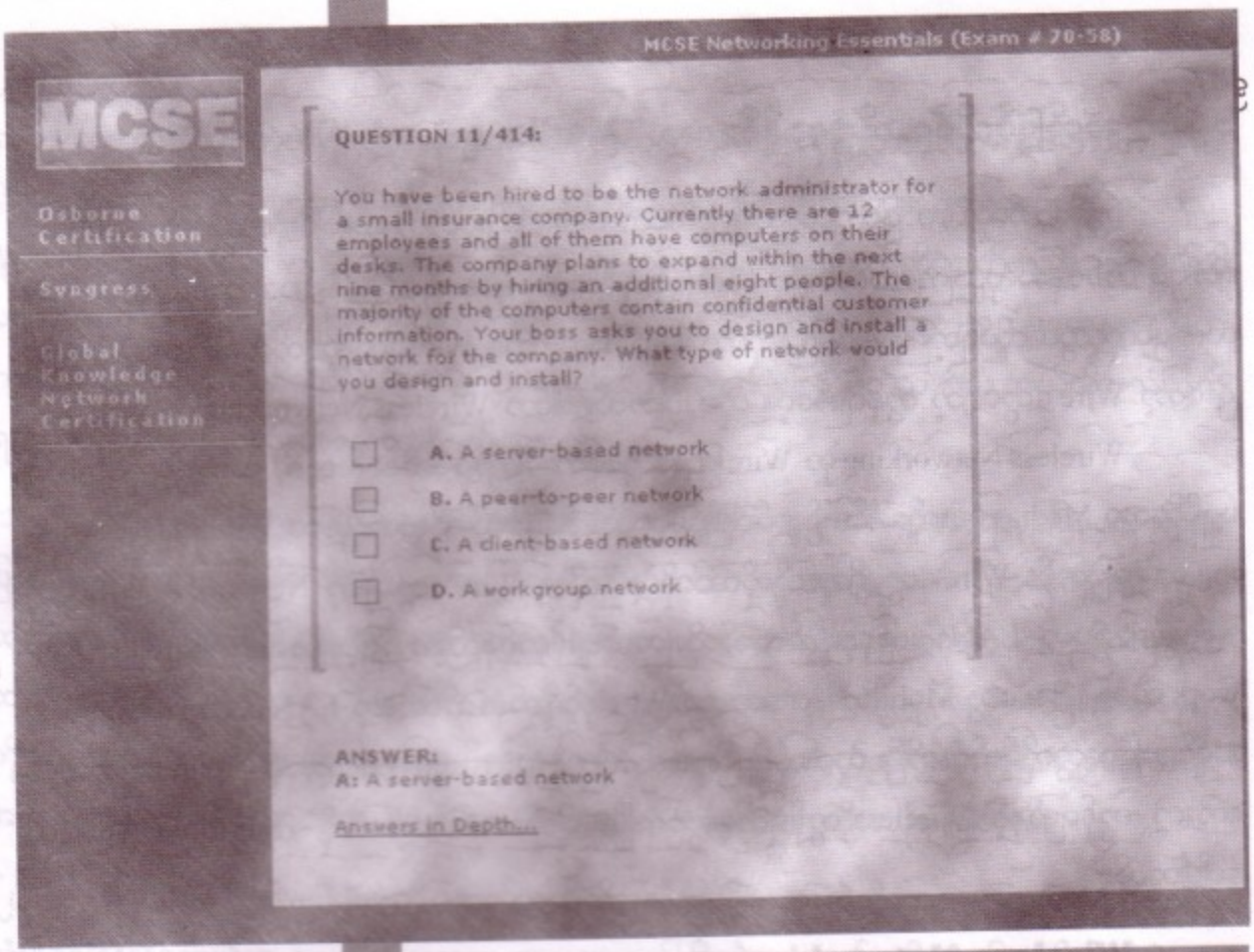
Frame Relay Switch



X.25 PAD

ISDN ရသော Digital Modem

ကိုတွေ့ရစဉ်



UNIT 12

Wireless Networking

ဒီ သင်ခန်းစာမှာ ကျွန်တော်တို့ ကြိုးမဲ့ကွန်ပျူတာကွန်ရက်နှင့် ပတ်သက်နေသော အကြောင်းအရာတွေကိုလေ့လာကြမှာ ဖြစ်ပါတယ်။ ဒီနေ့ခေတ်မှာ Wireless LAN တာ တဖြည်းဖြည်း ခေတ်စားလာပါတယ်။

၁၂.၁ လက်ဖြင့်ကိုင်တွယ်၍ဖရနိုင်သော Media များ

ကျွန်တော်တို့ လက်ဖြင့်ကိုင်တွယ်၍ရနိုင်သော Cable ကြိုးတွေကို ရှင်းပြပြီးခဲ့တဲ့နောက်မှာ ယခုအခါ ရှင်းပြဖို့ တစ်ဖန်အလှည့်ကြတာကတော့ လက်ဖြင့်ကိုင်တွယ်မရနိုင်တဲ့ Medias အကြောင်းပဲဖြစ်ပါတယ်။ လက်ဖြင့်ကိုင်တွယ်လို့မရတဲ့ကြားခံပစ္စည်းဆိုတာ အဆန်းသားလား။ Wire တွေနှင့်ချိတ်ဆက်ထားတဲ့ကွန်ရက်ပြီးတော့ Wire တွေမရှိတဲ့ ကွန်ရက်ပေါ့။ ဟုတ်ပါတယ်။ ဒါဟာ Wireless Networking ပဲပေါ့။

Wireless Networking မှာ Wire ကြိုးတွေမရှိတာကြောင့် ဒီသင်ခန်းစာကို လက်ဖြင့်ကိုင်တွယ်၍ မရနိုင်သော Medias များလို့ခေါင်းစဉ်တပ်လိုက်ပါတယ်။ ဒါပေမယ့် သိထားရမှာက Wireless Networking မှာ အမြဲတမ်း Wire တွေမရှိဘူးလို့ဆိုတာကိုပဲ။ ဒီလိုဗျ။ Wire တွေမရှိတဲ့ Network နဲ့ Wire ရှိတဲ့ Network ဥပမာ LANs တွေနှင့်ချိတ်ဆက်လို့ရတယ်ဗျ။ တစ်နည်းအားဖြင့်ပြောရရင် Wireless Network ထဲက User တွေ Mobile User တွေဟာ Wire နှင့်ချိတ်ဆက်ထားတဲ့ LAN ထဲက (Resources) အရင်းအမြစ်တွေကိုချိတ်ဆက်ပြီး ယူငင်သုံးစွဲလို့ရတယ်ပေါ့ဗျာ။ Microsoft ကတော့အခုလို Wired ချိတ်ဆက်ထားတဲ့ ကွန်ရက်နှင့် Wireless ကွန်ရက်တွေရောပြီး ချိတ်ဆက်ထားတာကို Hybrid Network လို့ ခေါ်ပါတယ်။

၁၂.၂ Wireless Networking ဆိုတာ

ဒီ Wireless Networking တွေမှာ Wireless နှင့်ဆက်သွယ်နေတဲ့နည်းပညာတွေနှင့် အောက်ပါ အခြေအနေမျိုးတွေရှိနိုင်ပါတယ်။

(၁) Wired နှင့်ချိတ်ဆက်ထားတဲ့ကွန်ရက်နှင့် Wireless ယာယီ Connections ချိတ်ဆက်လိုက ချိတ်ဆက်နိုင်တယ်။

(၂) Wired နှင့်ချိတ်ဆက်ထားတဲ့ကွန်ရက်နှင့် Wireless ချိတ်ဆက်ပြီး Backup လုပ်ခြင်း အရေးပေါ် ချိတ်ဆက်ခြင်းတို့ကိုလည်းပြုလုပ်နိုင်ပါတယ်။

(၃) Wire ကြိုးနှင့်ကွန်ရက်ကိုချိတ်ဆက်တဲ့နေရာမှာ Wire ရဲ့ကန့်သတ်သွားနိုင်တဲ့အကွာဝေးထက်ပိုပြီး Network ကိုချိတ်ဆက်နိုင်တယ်။

(၄) ဘာကိုပဲလုပ်ခွင့်ရှိတယ်ဆိုတဲ့တိကျတဲ့ကန့်သတ်ချက်များနှင့် သက်ဆိုင်ရာအသုံးပြုသူအချင်းချင်း အချက်အလက်တွေကိုဖလှယ်ခြင်းဖြင့် Mobile Networking တည်ဆောက်လို့ရတယ်။

Wireless Networking ဟာ လိုအပ်ရင်လိုအပ်သလောက်တိုးချဲ့လို့ရတယ်။ Network ကို Expand, Extend လုပ်လို့ရတယ်ပေါ့ဗျာ။ ဒါဟာ ကွန်ရက်တွေရဲ့အခြေခံသတ်မှတ်ချက်ကို ကျော်လွန်နိုင်တယ်

ဆိုတဲ့ ကောင်းတဲ့အချက်ပဲ ဖြစ်ပါတယ်။ သိတယ်မဟုတ်လား။ Wire နှင့်ချိတ်ဆက်တယ်ဆိုတာက Wire ရဲ့သွားနိုင်တဲ့အကွာအဝေး ကန့်သတ်ချက်ကရှိသေးတယ်လေ။ ဒါပေမယ့် ဒီလိုအချက်အတွေကြောင့်လည်း Wireless Networking ကကုန်ကျစရိတ်ပိုများတယ်ဗျ။ ကုန်ကျစရိတ်ပိုများတယ်ဆိုတာကိုလည်း သိပ်ကြည့်လို့ မရဘူးဗျ။ တခါတရံ ကုန်ကျစရိတ်များတယ်ဆိုပေမယ့်လည်း Wireless ပြန်ပေးတဲ့အကျိုးကျေးဇူးတွေက ကုန်တာထက်ကိုပိုပြီး ပြန်ရတတ်ပါတယ်။ ကဲ Wireless Networking နှင့်ပတ်သက်ပြီး ဘယ်လိုအသုံးပြုလို့ ရတယ်ဆိုတာကို ဆက်လက်လေ့လာကြည့်ရအောင်။

(၁) Wireless Networking ကို Mobile အဖြစ်အသုံးပြုပြီး အချက်အလက်တွေရယူခြင်း၊ ဖလှယ်ခြင်း ပြုလုပ်လို့ရပါတယ်။ ဒီလိုလေဗျာ။ ဥပမာပြောရရင် လူနာတင်ကားပေါ်က လူနာအခြေအနေကို ဆေးရုံက ဆရာဝန်ဆီပေးပို့နိုင်မယ်။ ကုန်ရောင်းထွက်တဲ့ကုန်ပို့တဲ့ကားဟာ ရောင်းပြီးသလောက်စာရင်းကို မိခင်ဌာနကို ဆက်သွယ်ပြီး Updates လုပ်နိုင်မယ်။ ဒီတော့ Mobile ဆိုတာက မိခင်ဌာနကနေ တခြားတစ်နေရာကိုသွားလာပြီး အလုပ်လုပ်နေတဲ့သူတွေ မိခင်ဌာနက Server ဆီကို အချက်အလက်တွေပေးပို့မယ်။ အခြေအနေတွေပြောပြမယ်။ ဒီအတွက် Wireless Telephone Connection ကိုအသုံးပြုပါတယ်။

(၂) Wireless Networking ကို နောက်ဘယ်လိုအသုံးပြုလို့ရသေးလဲဆိုတော့ - Network ကြိုးတစ်ခုလုံးရွှေ့သွားလို့ရတယ်ဗျ။ ဥပမာ - သဘာဝ ဘေးအန္တရယ်ကြုံတဲ့နေရာတစ်ခုကို ကယ်ဆယ်ရေးအဖွဲ့တွေသွားရောက်ကြပြီး ဒီ ကယ်ဆယ်ရေးအဖွဲ့ကအသုံးပြုနေတဲ့ Network ကိုသယ်သွားလို့ရတယ်။ ဘယ်လိုတုန်းဆိုတော့ ကိုယ်သုံးနေတဲ့ ကွန်ပျူတာ ဥပမာ Laptop တွေယူသွား အဲ့ဒီနေရာရောက် ကွန်ပျူတာဖွင့် Network ချိတ်။ ဘယ်လောက်အဆင်ပြေလဲ။ Cable (Wire) Network ဆို ဒါမျိုး Network ကြိုးရွှေ့သွားလို့မရဘူး။

(၃) အခြေအနေအကြောင်းအရာတွေ ပြောင်းလဲတတ်တဲ့နေရာမျိုးမှာ ပြောင်းလဲသမျှကိုအသိပေးဖို့လိုအပ်တဲ့အခါမျိုးမှာလည်း ဒီ Wireless Networking ကိုအသုံးပြုနိုင်ပြန်ပါတယ်။ ဥပမာ ရုပ်ရှင်ရိုက်ကွင်းတစ်ခုမှာ Stage ပေါ်မှာ ဘာတွေအပြောင်းအလဲ ဖြစ်လဲဆိုတာကို Studio နှင့်ချိတ်ဆက်ပြီး အကြောင်းကြားနိုင်ပါတယ်။

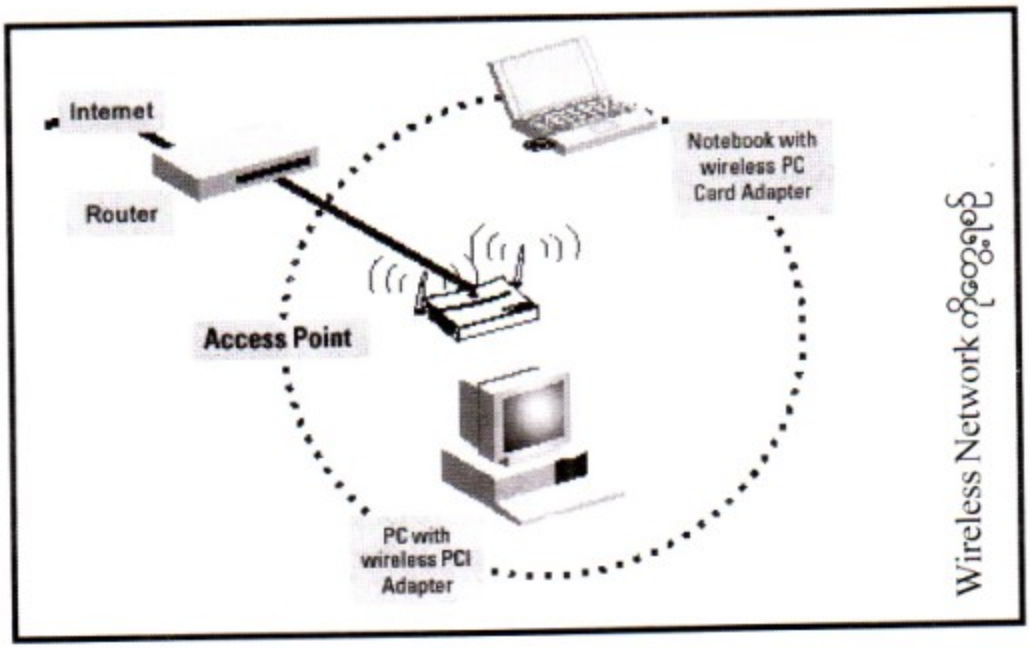
(၄) အလုပ်အရမ်းများတဲ့နေရာမျိုးတွေ ဥပမာပြောရရင် လက်ခံခြင်း၊ စစ်ဆေးခြင်း (Check-in and Reception) စတဲ့နေရာမျိုးတွေမှာ Wireless Networking ကိုအသုံးပြုခြင်းဖြင့် Customer Services ကိုပိုမိုကောင်းမွန်စေပါတယ်။ ဥပမာ ကားဌားထားတယ်ဆိုရင် ဌားထားတဲ့ကားဟာ Parking ကိုပြန်ရောက်နေပြီဆိုတာမျိုး လက်ခံခြင်း၊ စစ်ဆေးခြင်းကို Wireless ဖြင့်ပြုလုပ်လို့ရပါတယ်။

(၅) နောက်တစ်ခုက Cable ကြိုးမသွားနိုင်တဲ့နေရာမျိုးတွေမှာလည်း ဒီ Wireless Networking ကိုအသုံးပြုနိုင်ပါတယ်။ ဥပမာ သမိုင်းဝင်ရှေးဟောင်းအဆောက်အဦတွေမှာ ကိစ္စရှိလို့ Network ဆင်မယ်ဆိုရင် Cable ကြိုးကို အသုံးပြုလို့မရနိုင်ဘူး။ ဘာလို့လဲဆိုတော့ သမိုင်းဝင်အဆောက်အဦဆိုတော့ နံရံမှာ Cable

ရိုက်ခွင့်ပေးမှာမဟုတ်ဘူး။ ဒီလိုနေရာမျိုးတွေမှာလည်း Wireless Network ကိုအသုံးပြုလို့ရပါတယ်။

အခုလိုအချက်အလက်တွေကြောင့် ယခုဆိုရင် Wireless Network ကိုအသုံးပြုသူတွေတဖြည်းဖြည်းများလာပြီ ဖြစ်တာကြောင့် Wireless Networking ကိုတပ်ဆင်မယ်ဆိုရင် ကုန်ကျစရိတ်ကလည်းအရင်လို မများတော့ဘဲသက်သာလာပြီဖြစ်ပါတယ်။

ပုံ ၁၂.၁



၁၂.၃ Wireless Networking အခြေခံအစားများ

Wireless Network တစ်ခုမှာ အသုံးပြုတဲ့ ပါဝင်တဲ့ Components တွေပေါ်မူတည်ပြီး Wireless Network ကိုအဓိကအားဖြင့်အုပ်စု (၃) ပိုင်းခွဲထားပါတယ်။ အဲဒါတွေကတော့-

(၁) Local Area Networks (LANs) - ဒါကတော့ ကျွန်တော်တို့သိပြီးသား သမာရိုးကျဖြစ်ပါတယ်။ အသုံးပြု သူတွေကို အချင်းအချင်းချိတ်ဆက်ပေးတာပဲဖြစ်ပါတယ်။ ဥပမာ ခုနကလို အဆောက်အဦဟောင်းတွေမှာ Cable တွေကိုချိတ်ဆက်လို့မရတဲ့၊ ခွင့်မပြုတဲ့နေရာမျိုးတွေမှာ၊ ဘယ်လိုပဲဖြစ်ဖြစ်ဗျာ။ ကျွန်တော်တို့သိခဲ့ပြီးသား LAN ကို Wireless ချိတ်ဆက်တာပဲဖြစ်ပါတယ်။

(၂) Extended LANs - ဒါကလည်းရှင်းပါတယ်။ (ဟုတ်ကဲ့ ရှင်းပါတယ်။ ဘာမှရှင်းပြမနေပါနဲ့တော့) ဒီလိုပါ။ နာမည်ကိုက Extended LAN တဲ့။ LAN တွေကိုထပ်ချဲ့တာပဲဖြစ်ပါတယ်။ ဘာလို့လဲဆိုတော့ အဖွဲ့အစည်းတွေမှာ အသုံးပြုနေတဲ့ LANs ဟာ Wire နဲ့ဖြစ်ခဲ့ရင် အကွာအဝေးက Cable ကြိုးပေါ်မူတည်ပြီး ဘယ်အထိပဲသွားလို့ရတယ် ဆိုတာမျိုးရှိပါတယ်။ ဒီ Cable ကန့်သတ်ချက်ထက်ပိုချိတ်၊ ပိုသွားချင်တာမျိုးကို LAN ကိုချဲ့ထွင်ခြင်း Extended LAN လို့ခေါ်ပါတယ်။

(၃) Mobile Computing - Mobile Computing ဆိုတာကြတော့ ပြင်ပကိုရောက်နေတဲ့ အသုံးပြုသူတစ်ယောက်က Radio ဖြစ်စေ၊ ဆယ်လူလာ တယ်လီဖုန်း Frequencies ကိုအသုံးပြုပြီး မိခင်ဌာနက Server ကိုချိတ်ဆက်အသုံးပြုခြင်းဖြစ်ပါတယ်။

ဒီနေရာမှာကွဲပြားတဲ့အချက်လေးတွေ အနည်းငယ်ပြောပြစရာရှိပါတယ်။ အဲဒါက Data က Signal တွေ သယ်ဆောင်တဲ့အကြောင်းပါ။ အပေါ်ကပြောခဲ့တဲ့အုပ်စု (၃) စုထဲက

နံပါတ် (၁) LAN နှင့် နံပါတ် (၂) Extended LAN တို့က Wireless Networking ကိုအသုံးပြုရာမှာ အဖွဲ့အစည်းအတွင်း ရုံးခန်းအတွင်းမှာပဲ ကိုယ်ပိုင်ထိန်းချုပ်တာပဲဖြစ်ပါတယ်။

ဒါပေသိ အဲလေ ဒါပေမယ့် နံပါတ် (၃) ဖြစ်တဲ့ Mobile Computing ကြတော့ ဒီ Mobile User နှင့် မိခင်ဌာနတို့အဆက်အသွယ်ရပြီး အချက်အလက်တွေပေးပို့ခြင်း၊ လက်ခံခြင်း စတဲ့ကိစ္စတွေအတွက် Third Party ရဲ့ Support လုပ်မှုတွေလိုအပ်ပါတယ်။ ဒီလို Communication ကိုဖြစ်အောင်လုပ်ပေးတဲ့ Third Party Communication Carrier တွေကတော့ GTE တို့ MCI တို့ AT & T တို့ပဲဖြစ်ကြပါတယ်။ ၎င်းတို့ဟာ Wireless Communication ဖြစ်အောင် Wireless ဖြင့် Data တွေ Voice တွေပေးပို့လို့ရအောင် ဆောင်ရွက်ပေးပါတယ်။

၁၂.၄ Wireless LAN ဆိုတာဘယ်လိုကြီးလဲ

Wireless LAN ဆိုတာ ကျွန်တော်တို့သိခဲ့ပြီးတဲ့ LAN လိုပါပဲ။ Cable ကြိုးအစား Cable မရှိဘဲ ချိတ်ဆက်ထားတာပဲဖြစ်ပါတယ်။ ဘယ်လိုချိတ်ဆက်တာလဲဆိုတော့ ကွန်ပျူတာမှာ Network Interface လိုမျိုးတစ်ခုကတော့ တပ်ဆင်ထားရဆဲပဲ။ ဒါပေမယ့်သူကမှတဆင့် Cable တွေကိုချိတ်ဆက်ထားတာမဟုတ်တော့ဘဲ အင်တာနာ (Antenna) တို့ Emitter တို့ကို ချိတ်ဆက်တာဖြစ်ပါတယ်။ ဒီတော့ အခု တစ်ခုစမှတ်ရမယ်။ Cable အစား Antenna ဆိုတာပါလာပြီဖြစ်ပါတယ်။

နောက်တစ်ခုက Wireless User တွေကနေ Wired နှင့်ချိတ်ဆက်ထားတဲ့ ကွန်ယက်တွေဆီက အသုံးပြုသူတွေနှင့် Resources တွေကိုချိတ်ဆက်ဖို့အတွက်ကြတော့ Transceiver ဆိုတာလိုလာတယ်ဗျ။ ဒါကို Access Point လို့လည်းခေါ်ပါတယ်။ ပြန်ရှင်းပြပါအုံးမယ်။ Wire နှင့်ချိတ်တဲ့ကွန်ပျူတာနှင့် Wireless ကွန်ပျူတာတွေအကြား ဘာသာပြန်ဖို့အတွက် ဒီ Trnasceiver / Access Point ဆိုတာလိုအပ်ပါတယ်။ ဒီလိုပါ။ Transceiver ဆိုတာ Transmit လည်း လုပ်ပေးနိုင်တယ်ဆိုတဲ့ ပစ္စည်းနှစ်ခုပေါင်းထားတာပဲဖြစ်ပါတယ်။ ဒီပစ္စည်းက Wire နှင့်ချိတ်ဆက်ထားတဲ့ ကွန်ပျူတာနှင့် Wireless ကွန်ပျူတာအကြား ဘာသာပြန်အဖြစ် ဆောင်ရွက်ပေးမှာဖြစ်ပါတယ်။ ဒီ Access Point တာ Message တွေကို Wireless User တွေဆီကို Wireless Format ဖြင့်တိုက်ရိုက် Brand Casts လုပ်ပေးပါတယ်။ အဲဒီအပြင် Wireless User တွေဆီက

Message တွေကိုလည်း Wired ဖြင့်ချိတ်ဆက်ထားတဲ့ Connection တွေဆီတဆင့်ပြန်ပို့ ပေးနိုင်ပါတယ်။ Access Point Device တစ်ခုမှာ Antenna နှင့် Transmitter ပါရှိပြီး Wireless Traffic တွေကို ပေးပို့ခြင်း၊ လက်ခံခြင်း တို့ကိုလုပ်ပေးနိုင်တဲ့အပြင် Wire ကြိုးနှင့်ဆက်သွယ်ထားတဲ့ Connection ဘက်ကိုလည်း ချိတ်ဆက်ပေးနိုင်ပါတယ်။

ပုံ ၁၂.၂

အင်တာနာပေးနှင့် Wireless Router ကိုတွေ့ရစဉ်

တချို့ Wireless LAN တွေမှာကြတော့ ကွန်ပျူတာတစ်လုံးခြင်းစီအတွက်ဖြစ်စေ၊ ကြိုးဖြင့်ချိတ်ထားသော ကွန်ရက်ကိုဖြစ်စေ ဆက်သွယ်ပို့ဆောင်လျှက် ဒါမှမဟုတ် နံရံကပ် Transceiver အသေးလေးတွေကို အသုံးပြုကြပါတယ်။

၁၂.၅ Wireless LAN တွ ဘယ်လို Transmission လုပ်လဲ

ဒီ Wireless Communications တွေအားလုံးဟာ Network မှာ အသုံးပြုနေတဲ့ပစ္စည်းတွေ တစ်ခုနှင့်တစ်ခုအကြား အချက်အလက်တွေကိုပေးပို့ခြင်း နှင့် လက်ခံခြင်းကို Atmosphere ကနေလုပ်ဆောင်ကြရပါတယ်။ Signals တွေဟာ Waves ပုံစံနဲ့ဖြစ်ကြပြီး ဒါကို ရူပဗေဒ သဘောအရပြောရရင်တော့ Electromagnetic Spectrum လို့ခေါ်ပါတယ်။ ဒီ Spectrum ကိုဘာနှင့်တိုင်းတာသလဲဆိုတော့ (Frequencies) Frequency နှင့်တိုင်းတာပါတယ်။ ဆက်သွယ်ရာမှာဖြစ်ပေါ်နေတဲ့ Wave ဆိုတဲ့ လှိုင်းတွေကစက်ဝိုင်းတွေ လှိုဖြစ်နေတော့ CPS ပေါ့။ (Cycle per Second) လေ။သူ့ရဲ့ယူနစ်ကတော့ Radio ကိုတီထွင်ခဲ့ကြသူတွေထဲက တစ်ဦးဖြစ်သူ Heinrich Hertz ကို ဂုဏ်ပြုတဲ့အနေနဲ့ Hertz ဆိုပြီးတော့ပါ။ အတိုကောက် Hz ဖြစ်ပါတယ်။

Wireless Communication မှာဆိုရင် Frequency ဟာ Data Trammission ရဲ့ Amount နှင့် Speed ကို သက်ရောက်ပါတယ်။ ပို့လွှတ်လိုက်တဲ့အား (Power of Tramission) ဟာ Data တွေကိုဘယ်လောက်ဝေးဝေး Broadcast လုပ်နိုင်သလဲဆိုတာနှင့် လိုရာအရပ်ကိုရောက်ရှိသွားချိန်မှာ အချက်အလက်တွေ

ဟာအကောင်းအတိုင်းရှိရဲ့လားဆိုတာကို ဆုံးဖြတ်ပေးပါတယ်။ ယေဘုယျအားဖြင့်တော့ (Lower Frequency Trammission) လှိုင်းနိမ့်ထုတ်လွှတ်မှုဟာ Data တွေကိုနည်းနည်းနဲ့ ဖြည်းဖြည်းပဲသယ်နိုင်ပေမယ့် ဝေးဝေးသွားနိုင်တယ်။ (Higher Frequency Trammission) လှိုင်းမြင့်ထုတ်လွှတ်မှုကတော့ Data ကို နည်းနည်းနှင့် မြန်မြန်သယ်နိုင်ပေမယ့် ခရီးတိုပဲသွားနိုင်ပါတယ်။

ဒီ Electromagnetic Spectrum ရဲ့အလယ်ပိုင်းအပိုင်းကိုတော့ အောက်ပါအတိုင်းနာမည်ပေးပြီးတော့ ခွဲခြား သတ်မှတ်ထားပါတယ်။ အခုပြောပြထားတဲ့အုပ်စုတွေက Wireless Communicators တွေမှာအသုံးပြု တတ်တဲ့အုပ်စုတွေပဲဖြစ်ပါတယ်။

၁။ Radio - 10KHz to 1GHz

၂။ Microware - 1GHz to 500GHz

၃။ Infrared - 500KHz to 1THz

Wireless LANs တွေဟာ Data တွေကို Transmit လုပ်ခြင်းနှင့် Receive လုပ်ခြင်းတို့ကို အောက်ပါနည်းပညာ များဖြင့်ပြုလုပ်ပါတယ်။ ၎င်းတို့မှာ -

(၁) Infrared

(၂) Laser

(၃) Narrowband, Single-Frequency radio

(၄) Spread - spectrum Radio တို့ဖြစ်ကြပါတယ်။

၁၂.၆ Infrared LAN အခြေခံ

Wireless နည်းပညာတွေမှာသုံးတဲ့ Infrared ဟာဝင်း Wireless ကွန်ရက်အတွင်းရှိ ပစ္စည်းများ တစ်ခုနှင့်တစ်ခု Signals များပေးပို့ရာတွင် Infrared အလင်းတန်းကိုအသုံးပြုပါသည်။ ဒီ Infrared ပစ္စည်းတွေက ပုံမှန်အားဖြင့်တော့ အတော့်ကိုသန်မာတဲ့ အားပြင်းတဲ့ Signals တွေကိုပို့လွှတ်တတ်ကြပါတယ်။ ဘာလို့လဲဆိုတော့ ရုံးတွေမှာက ဘယ်လိုပဲဖြစ်ဖြစ်အလင်းရောင်ဆိုတာရှိမှာပဲလေ။ ဒီအလင်းရောင်တွေရဲ့ Interference ကိုကာကွယ်တဲ့သဘောပဲဖြစ်ပါတယ်။ Wireless LAN မှာဆိုရင် Infrared ကသူ့ရဲ့ High Bandwidth ကြောင့်အတော်လေးကိုအသုံးတည့်ပါတယ်။ ၎င်းဟာ 10 to 100 Mbps နှုန်းနဲ့ကောင်းစွာ Tranmission လုပ်နိုင်ပါတယ်။

Infrared LAN မှာမှအဓိကအားဖြင့် အုပ်စု (၄)အုပ်စုရှိပြန်ပါတယ်။

(၁) Line of Sight Networks - သူက Transmitter နှင့် Receiver အကြား တစ်စုံတစ်ခု ပိတ်ဆို့နေလို့မရဘူး။ ရှင်းရှင်းလင်းလင်းဖြစ်နေဖို့လိုတယ်။ ပို့လွှတ်သူနှင့်လက်ခံသူအကြား တစ်စုံတစ်ခုပိတ်ဆို့

နေရင်အဆင်မပြေဘူး။

(၂) Reflective Wireless Networks – သူကကြတော့ပစ္စည်းတစ်ခုချင်းစီနားက Optical Transceivers ဆီကနေ Signal တွေကို Central Hub ဆီကိုပေးပို့ပါတယ်။ ပြီးမှရည်ရွယ်လက်ခံရာဆီကိုပြန်ပို့ပါတယ်။

(၃) Scatter Infrared Networks – သူကတစ်မျိုးဗျ။ ပေးပို့သူနှင့်လက်ခံသူတို့အကြား Signals တွေဟာ နံရံတွေ မျက်နှာကြက်တွေဆီကနေ (Bounce) ရိုက်ခြင်း၊ ပြန်ကန်ခြင်းဖြင့်ရောက်ရှိကြပါတယ်။ ဒီပေမယ့် သူကခြွင်းချက်ပေါ့နော်။ နေရာက အင်း ပေးလိုသူနဲ့လက်ခံသူနေရာက အများဆုံးမီတာ ၃၀ (ပေ ၁၀၀)လောက်ပဲကောင်းတယ်။ ဘာလို့လဲဆိုတော့ Bounce လုပ်ပြီးသွားရတာဆိုတော့ Signal ကနည်းနည်း Delay (နောက်ကျ) ဖြစ်တယ်လေ။ နောက်ပြီးနံရံကိုပြန်ကန်ပြီးသွားရတာဆိုတော့ Infrared ကပျံသွားတယ်။ ဒါကြောင့် Line of Sight လောက် Bandwidth မကောင်းဘူး။

(၄) Broadband Optical Telepoint Networks – သူကတော့ Broadband အဖြစ်ပံ့ပိုးပေးနိုင်ပါတယ်။ Broadband ဆိုတော့မြန်နှုန်းမြှင့်ပေါ့။ နောက်ပြီး Bandwidth လည်းကျယ်တယ်။ ဒီတော့ High End Multimedia သုံးတဲ့လုပ်ငန်းတွေနဲ့ဆိုအသုံးတည့်ပါတယ်။

Infrared Transmission ကို Virtual Docking တွေမှာလည်းအသုံးပြုပါတယ်။ သူက Laptops တွေ Portable Computer တွေကို Wired နှင့်ချိတ်ဆက်ထားတဲ့ Computer တွေ၊ အခြားဆက်စပ်ပစ္စည်းတွေဖြစ်ကြတဲ့ Printers တို့ဘာတို့နှင့် ချိတ်ဆက်အသုံးပြုခွင့်ရစေပါတယ်။

၁၂.၇ Laser Based LAN အကြောင်း

Laser Based Transmission ကလည်း ပေးပို့သူ (Sender) နှင့်လက်ခံသူ (Receiver) အကြား Clear Line of Sight ဖြစ်နေရပါ့မယ်။ ပိတ်ဆို့နေလို့မရဘူးပေါ့နော်။ အကယ်၍များ Solid အရာဝတ္ထုတစ်ခုဖြစ်စေ၊ လူတစ်ဦးတစ်ယောက်ကဖြစ်စေ ၎င်းအလင်းတန်းကိုပိတ်ဆို့လိုက်လို့ရှိရင် Data Transmission ကိုလည်း Block ဖြစ်သွားစေပါတယ်။ Laser အလင်းတန်းရဲ့ Radiation ဖြစ်မှုက လူကိုမထိခိုက်စေရန် Laser Based LAN ထဲက ပစ္စည်းတွေဟာ Infrared လိုပဲကန့်သတ်ချက်တွေရှိပါတယ်။

၁၂.၈ Narrow-Band, Single-Frequency Radio အကြောင်း

၎င်းက ပေးပို့သူ (Transmitter) နှင့် လက်ခံသူ (Receiver) အကြားအချက်အလက်တွေဝင်လာစေဖို့ ရောက်လာစေဖို့ ထွက်သွားစေဖို့ သတ်မှတ်ထားတဲ့ Frequency ကိုတူညီအောင် (Tune) ညှိထားဖို့လိုအပ်ပါတယ်။ ၎င်းက ဥပမာပြောရရင် Taxi Cabs တို့၊ Police Communication တို့ စတာတွေမှာဆက်သွယ်တဲ့

Power အနည်းငယ်သာသုံးစွဲခဲ့တဲ့ Two-way Radio ဆက်သွယ်ရေးဖြစ်ပါတယ်။ သူကအလင်းကိုအခြေခံပြီး ဆက်သွယ်တဲ့ ဆက်သွယ်ရေးစနစ်တွေဖြစ်ကြတဲ့ Infrared တို့ Laser တို့နဲ့မတူတဲ့အချက်က ဒီ Narrow-Band Radio စနစ်ဟာ ပေးပို့သူ (Sender) နှင့် လက်ခံသူ (Receiver) အကြား Line of Sight မလိုအပ်ဘူး။ သူတို့လိုတစ်ခုနှင့်တစ်ခုအကြား ရှင်းလင်းနေစရာ မလိုဘူး။ ပြောရမယ်ဆိုရင် ၎င်း Sender နှင့် Receiver ဟာ သူတို့ရှိသင့်တဲ့ Broadcast Range ရေယာအတွင်းမှာ ဘယ်လောက်ပဲတစ်ဦး နှင့် တစ်ဦး ဝေးဝေးရှိပါစေ ဆက်သွယ်လို့ရပါတယ်။ Line of Sight ဖြစ်ဖို့မလိုအပ်ပါဘူး။ ၎င်း Broadcast Range ဟာအများဆုံးအားဖြင့် ခန့်မှန်းခြေ မိတာ(၇၀) ပေအားဖြင့် ၂၃၀ လောက်အထိရှိပါတယ်။

အသုံးပြုတဲ့ Frequency ပေါ်မူတည်ပြီးတော့ အရှိုးသော Frequency တွေရဲ့ Signal တွေကနံရံတွေ ပိတ်ဆို့ထား တဲ့ Solid တွေကိုကျော်မသွားနိုင်တာကြောင့် အောင်မြင်တဲ့ Transmission နှင့်လက်ခံခြင်းတို့မဖြစ်နိုင်တော့ပါဘူး။ အဲ့ဒီအပြင် အခြားသော Radio လှိုင်းတွေကြောင့်လည်း Interferance တွေဖြစ်ပေါ်စေနိုင်ပါတယ်။ နောက်တစ်ခုက ဒီ Radio LAN စနစ်နှင့်ပတ်သက်ပြီးသိထားစရာတစ်ခုက မည်သည့် Broadcast နည်းပညာမဆို ဒီ Network Communication အတွင်းမှာရှိတဲ့တစ်ဦးတစ်ယောက်ကဖမ်းယူနားထောင်နိုင်ပါတယ်။ အောက်မှာ Narrow-Band Wireless LAN နည်းပညာနှင့်ပတ်သက်လို့ Characteristics တွေဖော်ပြထားပါတယ်။ လေ့လာကြည့်ပါဦး။

Characteristics	Value
Frequency ranges	Unregulated: 902-928 MHz, 2.4 GHz, 5.72-5.85 GHz
Maximum distance	50-70 meters (164-230 feet)
Bandwidth	1-10 Mbps
Installation/maintenance	Easy to install and maintain
Interference	Highly susceptible
Cost	Moderate
Security	Highly susceptible to eavesdropping within range

နောက်တစ်ခုက Single Frequency LAN နည်းပညာအကြောင်းပြောပြပါဦးမယ်။ သူကကြတော့ Narrow Band လို Low-Power မဟုတ်တော့ဘူး။ High Power ဖြစ်သွားပြီ။ ဒီ Network အမျိုးအစားကတော့ ရေပြင်ညီအလိုက် Transmit လုပ်ရာမှာတော်တော်ဝေးဝေးထိ Transmit လုပ်နိုင်ပြီး Repeaters တို့ Bounce နည်းပညာတို့ကိုလည်းအသုံးပြုလို့ရပါသေးတယ်။ ဒီနည်းပညာက ဘာအတွက် သင့်တော်သလဲဆိုရင် Mobile User တွေနဲ့ဆက်သွယ်တဲ့အခါမျိုးတွေမှာပါ။ ဒါပေမယ့် Low-Power နည်းပညာကိုသုံးတာထက်စာရင် ပိုပြီးတော့ ကုန်ကျစရိတ်များပါတယ်။ နောက်ပြီး ဒီ Transmission အတွက်လိုအပ်တဲ့ပစ္စည်းအသုံးပြုတဲ့ပစ္စည်းတွေကလည်းဈေးကြီးတဲ့အပြင် (FCC-Federal Communication Commisson)

လိုဆင်တွေလည်းလိုအပ်ပါတယ်။ အောက်မှာ High Power ဖြစ်တဲ့ Single Frequency LAN နှင့်ပတ်သက်တဲ့ဇယားကိုလေ့လာကြည့်ပါအုံး။

Characteristics	Value
Frequency ranges	Unregulated: 902-928 MHz, 2.4 GHz, 5.72-5.85 GHz
Maximum distance	Line of sight, unless extension technologies are used
Bandwidth	1-10 Mbps
Installation/maintenance	Difficult, highly technical, requires lecensing
Interference	Highly susceptible
Cost	Expensive to very expensive
Security	Highly susceptible to eavesdropping

၁၂.၉ Spread-Spectrum LAN အခြေခံများ

သူက Spectrum ဆိုတဲ့အတိုင်း Single Frequency ကိုအသုံးမပြုဘဲ၊ Multiple Frequencies ကိုတစ်ပြိုင်တည်းအသုံးပြုပါတယ်။ ဒါကြောင့်သူကပိုပြီးစိတ်ချရတယ်။ နောက်ပြီး Interference ကြောင့်ဖြစ်ပေါ်တတ်တဲ့ထိခိုက်မှုတွေကိုလည်းလျှော့ချပေးပါတယ်။ နောက်ပြီး Multiple Frequencies ကိုအသုံးပြုတဲ့အတွက်ကြောင့် ကြားကနေ ဖမ်းယူနားထောင်ဖို့ကိုလည်း ခဲယဉ်းသွားပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ Spread-Spectrum ဆက်သွယ်ရေးဖြစ်ပေါ်ဖို့ Frequency တစ်ခုချင်းစီကိုပေါင်းပြီး အသုံးပြုရလို့ပဲဖြစ်ပါတယ်။ Spread-Spectrum Communications မှာမှ အဓိကအားဖြင့် အမျိုးအစားနှစ်မျိုးရှိပါတယ်။ အဲဒါကတော့ Frequency Hopping နှင့် Direct-Sequence Modulation တို့ပဲဖြစ်ပါတယ်။

Frequency Hopping အခြေခံများ

Frequency Hopping မှာ Transmitter နှင့် Receiver တွေဟာ Communications ဖြစ်ပေါ်စေနိုင်ဖို့ တင်းတင်းကြပ်ကြပ်(တိကျစွာ) Synchronized လုပ်ထားဖို့လိုအပ်ပါတယ်။ သူက Data တွေကို သတ်မှတ်ထားတဲ့ ပုံမှန်ကွာဝေးတဲ့ Intervals နဲ့ Multiple Frequency တွေအကြားဖြစ်ပေါ်စေပါတယ်။ ဆိုလိုတာက Data တစ်ခုက ဒီ Frequency ဆို နောက် Data တစ်ခုက နောက် Frequency တစ်ခု သူတို့နှစ်ခုဘယ်လောက်ကွာလဲ Interval ဘယ်လောက်ရှိလဲ။ နောက် Frequency တစ်ခုကလည်း အဲဒီလောက်ပဲကွာတယ်။ ဒီနေရာမှာ နောက် Frequency တစ်ခုက ဘယ်လောက်ဖြစ်မလဲဆိုတဲ့ Timing ပိုင်းဆိုင်ရာကို Hardware ပိုင်းကထိန်းချုပ်ပေးပါတယ်။

ထပ်ရှင်းပြရမယ်ဆိုရင် Frequency တိုင်းမှာ Data တာမပါရှိတဲ့ Data ပါရှိတဲ့ Frequency နှင့် နောက်တစ်ခါ Data ပြန်ပါရှိလာတဲ့ Frequency တာ (Interval) အကွာအဝေးတစ်ခုခြားနေပါတယ်လို့ ဆိုလိုချင်တာဖြစ်ပါတယ်။ ဒီလိုအကြောင်းကြောင့်မို့လည်းကြားကနေဖြတ်ပြီး နားထောင်ဖို့ခဲယဉ်းပါတယ်။ ဒါပေမဲ့လည်း ဒီ Frequency Hopping နည်းပညာကတစ်ကြိမ်မှာ Frequency တစ်ခုကိုသာအသုံးပြုတာကြောင့် Bandwidth က 1Mbps ပဲရှိပါတယ်။ တစ်ခါတစ်ရံဒီထက်တောင်နည်းပါသေးတယ်။ တစ်ခါတစ်ရံမှာတော့ ပြောရမယ်ဆိုရင် တကယ့်ကိုတစ်ခါတစ်ရံမှာပါ 2Mbps အထိရတတ်ပါတယ်။

Direct-Sequence အခြေခံ

သူကြတော့ Data တွေကို တိကျတဲ့ (Fixed Size) Size တစ်ခုအဖြစ် တနည်းအားဖြင့် Segment ပေါ့ ပိုင်းလိုက်တယ်။ ၎င်းကို Chips လို့ခေါ်တယ်။ ပြီးတာနဲ့တစ်ပြိုင်နက် မတူညီတဲ့ Frequencies တွေကို အသုံးပြုပြီး Data တွေကို Transmit လုပ်ပါတော့တယ်။ ဒီနေရာမှာထူးဆန်းတာက လက်ခံတဲ့ဖက်က Equipment တွေက ဘယ် Frequencies ကိုစောင့်ကြည့်ရမယ်၊ ရောက်ရှိလာတဲ့ Chips တွေထဲက Data ကိုအစီအစဉ်တကျဖြစ်အောင်ဘယ်လိုပြန်ပြီးစီစဉ်ရမယ်။ ဘယ်လိုပြန်ဖွဲ့ရမယ်ဆိုတာသိကြတယ်ဗျ။ နောက်တစ်ခုထူးဆန်းတာရှိသေးသဗျ။ အဲ့ဒါက လမ်းကနေကြားဖြတ်နားထောင်လို့မရအောင် Data တွေကိုပို့တဲ့အခါမှာ တကယ့် Real Data နှင့် Data အတုတွေကိုကြားညှပ်ပြီး ပို့သဗျ။

Characteristics	Value
Frequency ranges	Unregulated: 902-928 MHz, 2.4 GHz
Maximum distance	Limited to cell boundaries, but often extends over several miles
Bandwidth	1-2 Mbps for frequenc-hopping, 2-6 for direct-sequence
Installation/maintenance	Depends on equipment; ranges from easy to difficult
Interference	Moderately resistant
Cost	Inexpensive to moderate
Security	Not very susceptible to eavesdropping

၁၂.၁၀ Wireless Extended LAN အခြေခံ

Wireless Networking ပစ္စည်းတစ်ခုကိုအသုံးပြုပြီးတော့ ကျွန်တော်တို့ဟာ Cable ကိုအသုံးပြုထားတဲ့ ကွန်ရက်တွေရဲ့ကန့်သတ်ထားတဲ့ Network အလျားကိုချဲ့ထွင်လို့ရပါတယ်။ ကျွန်တော်ရှေ့မှာတုန်းကတည်းကပြောခဲ့ဖူးတယ်လေ။ Cable ကြိုးနဲ့ဆင်တဲ့ကွန်ရက်ဆိုတာက Cable တွေရဲ့အများဆုံး Data

သယ်သွားနိုင်တဲ့ပေါ်မူတည်ပြီး ကန့်သက်ချက်ရှိတယ်။ ဒီကန့်သက်ချက်ထက်ကြီးတဲ့ ကျယ်တဲ့ Network တစ်ခုကိုရရှိဖို့အတွက် ကျွန်တော်တို့ဟာ Wireless Bridges ကိုအသုံးပြုရပါမယ်။ ၎င်း Wireless Bridge ကိုအသုံးပြုပြီး ဘယ်လောက်ထိတောင် Network ကိုချဲ့လိုက်လို့ရသလဲ ချိတ်လို့ရသလဲဆိုရင် မိုင်နဲ့ပြောရင် (၃)မိုင် ကီလိုမီတာနှင့်ပြောရင် ၄.၄ အထိလောက်ရပါတယ်။

ဒီ LAN Bridge တွေက Line of Sight ကိုပဲဖြစ်စေ၊ Broadcast Transmission ကိုပဲဖြစ်စေ အသုံးပြုပြီးတော့ နေရာ (ဥပမာ အဆောက်အဦ) အချင်းချင်းကိုချိတ်ဆက်လို့ရပါတယ်။ ဒီအမျိုးအစားထဲက Spreed Spectrum Radio, Infrared နှင့် Laser-Based Equipment တွေဟာ ဈေးကွက်မှာရရှိနေပြီဖြစ်ပါတယ်။ အဲ့ဒီအပြင် အဝေးကြီး ချိတ်ဆက်ပေးနိုင်မယ့် Longer Range Wireless Bridge တွေလည်း ရရှိနိုင်ပြီဖြစ်ပါတယ်။ ၎င်းဟာ Ethernet နှင့် လည်းရရှိသလို Token Ring အနေနှင့်လည်းရှိပါတယ်။ အကွာအဝေးကတော့ ၂၅ မိုင်အထိရရှိပါတယ်။ ဒီတော့ Longer Range Wireless Bridge တွေလည်းရှိသလို Shorter Range Wireless Bridge တွေလည်းရှိတာကြောင့် ကိုယ့်လိုအပ်ချက်နှင့်ကိုယ်သုံးရမှာဖြစ်ပါတယ်။ ဘာလို့လည်းဆိုတော့ Longer Range Wireless Bridge တွေက Shorter Range ထက်ဈေးပိုကြီးနေလို့ဖြစ်ပါတယ်။ အောက်မှာ Wireless Extended LAN နှင့်ပတ်သက်တာတွေကိုလည်း လေ့လာကြည့်ပါဦး။

Characteristics	Value
Frequency ranges	Spread-spectrum, infrared, laser
Maximum distance	1-3 miles for short-range, up to 25 miles for long-range
Bandwidth	1-6 Mbps for spread-spectrum, 2-100 for infrared and laser
Installation/maintenance	Depends on equipment; ranges from easy to difficult
Interference	Highly resistant
Cost	Inexpensive to moderate
Security	Not very susceptible to eavesdropping

မှတ်ချက်။ ။ Wireless Bridges တွေဟာအမြဲတမ်းနှစ်ခုတစ်စုံနဲ့လာပါတယ်။ ၎င်းပစ္စည်းနှစ်ခုစလုံးဟာ Repeater သကဲ့သို့ အတူတကွပူးပေါင်းပြီးအလုပ်လုပ်ကြပါတယ်။ တစ်ခုက Wired ကြိုးဖြင့်ချိတ်ဆက်ထားသော ကွန်ရက်ဘက်ကနေပြီး နောက်တစ်ခုက နောက် Wired ကြိုးဖြင့်ချိတ်ဆက်ထားသော ကွန်ရက်ဘက်ကနေ အသီးသီးနေကြပြီး Transmit လုပ်ကြပါတယ်။ ဒါကြောင့် ဒီပစ္စည်းတွေကို Half Repeators လို့လည်းခေါ်ပါတယ်။ Lower Bridged နှင့် Infrared ကိုအသုံးပြုထားတဲ့ Wireless Bridge တွေကို Optical Half Repeators လို့ခေါ်တတ်ကြပြီး Spread Spectrum ကိုအခြေခံထားရင်တော့ Radio Half Repeators လို့ခေါ်ပါတယ်။

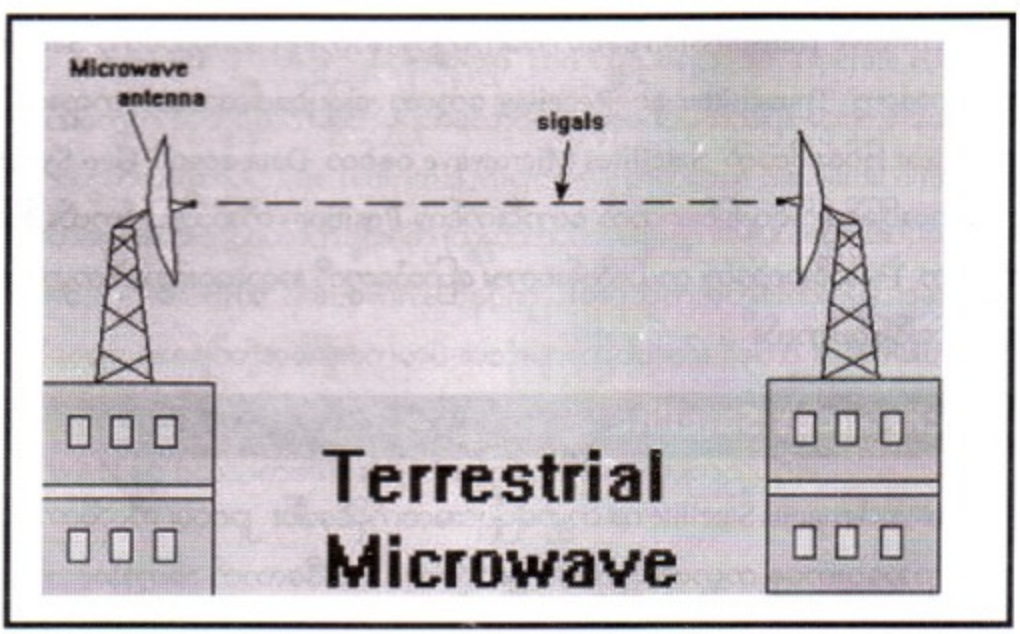
၁၂.၁၁ Microwave Networking အခြေခံများ

Microwave စနစ်နှင့် Data တွေက Transmit လုပ်တာက Radio ကိုအခြေခံထားတဲ့ စနစ်တွေထက်စာရင် ပိုပြီးတော့ Transmission Rate ပိုမြန်ပါတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ Frequencies ကမြင့်တယ်လေ။ နောက်ပြီး Line of Light လည်း Clear ဖြစ်တယ်။ Microwave နှင့်ဆက်သွယ်ရေးပြုလုပ်တော့မယ်ဆိုရင် FCC ထောက်ခံချက်တွေလိုတယ်။ လိုင်စင်တွေလိုတယ်။ အဲကြောင့် Radio စနစ်ထက်စာရင်ကုန်ကျစရိတ်ပိုများပါတယ်။ Microwave စနစ်မှာထင်ရှားတဲ့စနစ်နှစ်ခုကတော့ Terrestrial နှင့် Satellite တို့ဖြစ်ကြပါတယ်။

Terrestial Microwave

Terrestrial ဆိုတဲ့အဓိပ္ပါယ်က "ကမ္ဘာပေါ်မှတင်" လို့ဆိုလို့ရသဗျ။ ဒီလိုပြောလိုက်တာနှင့် စာဖတ်သူ Microwave တိုင်တွေကို မျက်စိထဲပြေးမြင်တယ်မဟုတ်လား။ ဟုတ်ပါတယ်။ ဒီတိုင်တွေက ကမ္ဘာမြေပေါ်မှာတင်ရှိတာလေဗျာ။ ဒီတော့ Microwave Tower တိုင်ကြီးတွေကို ရည်ရွယ်ရာတွေဆီကို ရောက်ရှိစေဖို့ Line of Sight ဖြစ်စေဖို့ ဒီတာဝါတိုင်တွေကို တောင်ထိပ်တွေ၊ အိမ့်မဟုတ် အဆောက်အဦအရှည်ကြီးတွေပေါ်မှာ အိမ့်မဟုတ်ရှင်းရှင်းလင်းလင်းဖြစ်တဲ့နေရာတွေမှာ တည်ဆောက်ထားကြတာပေါ့။ ဒီ Transmission က Line of Sight Transmission ဖြစ်ပါတယ်။ ဒီ Terrestrial Microwave စနစ်တာပေးပို့သူနှင့်လက်ခံသူကို ချိတ်ဆက်မိစေရန် High Frequency Signals ကိုအသုံးပြုပါတယ်။ ဒီ Microwave စနစ်မှာတာဝါတိုင်တွေကို အသုံးပြုပြီး ထပ်ဆင့်ထပ်ဆင့်လွှာခြင်းဖြင့် Signal ကို Extend ဖြစ်ကာ ကမ္ဘာ့တိုက်ကြီးတစ်တိုက်၏ အကွာအဝေးကို ပို့လွှတ်လို့ရပါတယ်။

ပုံ ၁၂.၃



ဒီ Microwave စနစ်ကိုကြတော့ ဘယ်မှာသုံးလဲဆိုတော့ Cable နှင့်ချိတ်ဆက်ပြီးဆက်သွယ်ရင်လည်း ကုန်ကျစရိတ်များမယ့်အကွာအဝေးလည်းဖြစ်နေတယ်။ အဲ့ဒီနေရာမှာဆက်သွယ်ရမယ့် Traffic အနေအထားကလည်း အရမ်းအကျပ်ကြီးမဟုတ်ဘူး။ အနေတော်လောက်ရှိမယ်ဆိုတဲ့အခါမျိုးမှာ ဒီစနစ်ကိုသုံးပြီး ဆက်သွယ်သမှုပြုကြပါတယ်။ ဒီစနစ်မှာက တစ်ခုရှိတာက ဒီတာဝါတိုင်ပေါ့ ပြောရရင် ပို့လွှတ်သူ Transmitter နှင့်လက်ခံသူ Receiver တို့ဟာ ကောင်းမွန်စွာ Data တွေရှိ၊ ရောက်ရှိစေဖို့ Align ဖြစ်ဖို့တော့လိုပါတယ်။ LAN တွေမှာအသုံးပြုဖို့ Power အနည်းငယ်သာအသုံးပြုတဲ့ Short Range Microwave စနစ်တွေလည်းရှိပါတယ်။ ဒါပေမယ့်သူတို့က Transmitter နှင့် Receiver အကြားလုံးဝ Clear Line of Shight ဖြစ်ဖို့လိုပါတယ်။ အောက်မှာ Terrestrial Microwave LAN / WAN နှင့်ပတ်သက်တာတွေဖော်ပြပေးထားပါတယ်။

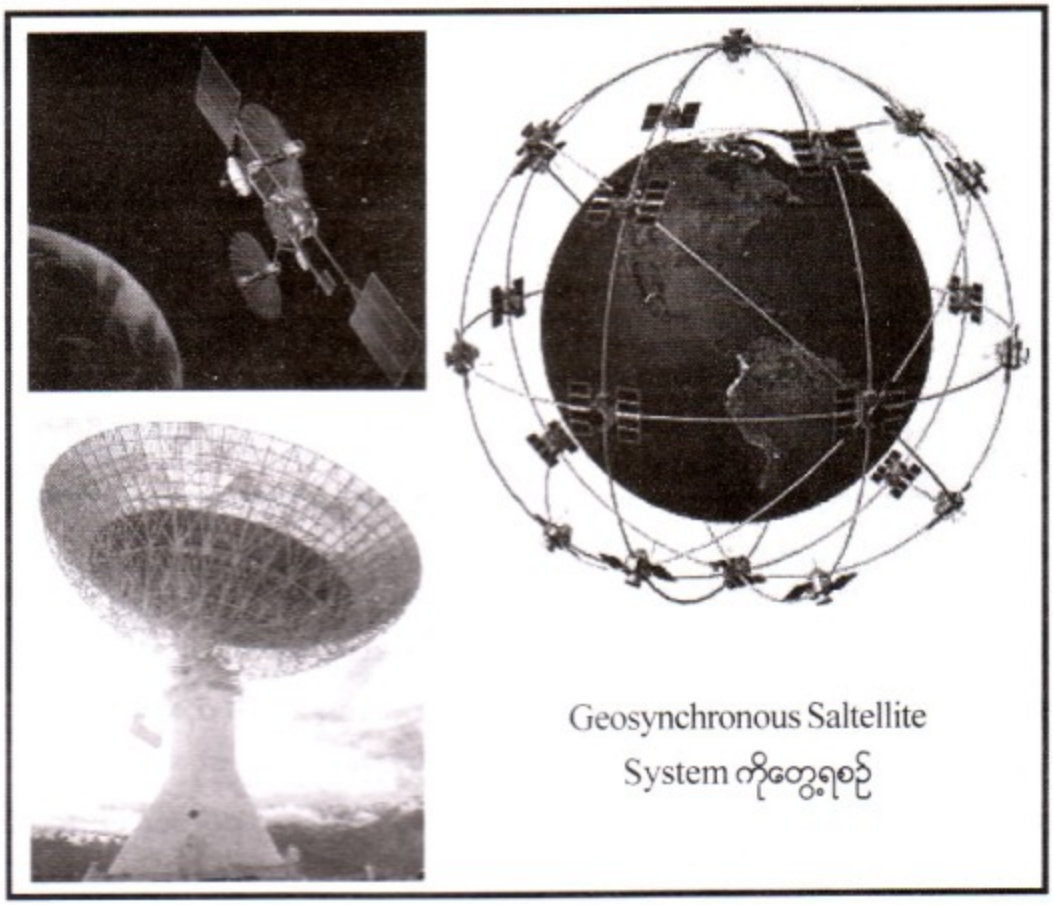
Characteristics	Value
Frequency ranges	4-6 GHz or 21-23 GHz
Maximum distance	Typically from 1 to 50 miles
Bandwidth	1-10 Mbps
Installation/maintenance	Difficult
Interference	Vanes with respect to power and distance; longer distances
Cost	more prone to weather disturbances Expensive
Security	Highly susceptible, but signals usually encrypted

Microwave Transmission စနစ်မှာအဓိကကျတဲ့နောက်စနစ်တစ်ခုကတော့ Satellite ပဲ ဖြစ်ပါတယ်။ သူကတော့ Transmitter နှင့် Receiver တွေဟာ မြေပြင်ပေါ်ကသဘောတရားလို Line of Sight က Clear ဖြစ်နေဖို့ထက် Satellites Microwave စနစ်က Data တွေကို Geo Synchronous Satellites မှပေးပို့ခြင်းနှင့် ရယူခြင်းအတွက် ကောင်းကင်က Positions ကိုအသုံးပြုပါတယ်။ ဒီလိုနဲ့ ကမ္ဘာတစ်ဖက်ခြမ်းက TV အစီအစဉ်တွေ၊ တယ်လီဖုန်းစကား ပြောသံတွေကို အလွန်ဝေးကွာတဲ့ ကမ္ဘာတစ်ဖက်ခြမ်းက ကြားရမြင်ရပြီဖြစ်ပါတယ်။

Geosynchronous Satellite

Geosynchronous Satellite က ကမ္ဘာမြေပြင်အထက်မိုင်ပေါင်း ၂၀၀၀၀၊ ကီလိုမီတာဖြင့်ပြောလျှင် ၅၀၀၀၀ အကွာအဝေးကနေ ကမ္ဘာကိုလှည့်ပတ်လျှက်ရှိပါတယ်။ အဲဒီလောက် အကွာအဝေးကြီးကြောင့် ပြောစရာတစ်ခုဖြစ်လာတာက Delay ပဲ။ Delay က 0.5 ကနေ 5 စက္ကန့်အတွင်းအပြောင်းအလဲတော့ရှိမယ်။

ပုံ ၁၂.၄



ဘယ်ပေါ်မူတည်သလဲဆိုတော့ ပေးပို့သူ နှင့် ရယူသူအကြား Network တွေကိုဘယ်လောက်အထိ ခုန်သွားရသလဲဆိုတာပါပဲ။ ဥပမာ ရုပ်မြင်သံကြား ကနေ TV လိုင်းတစ်ခုကို တိုက်ရိုက်ဖမ်းကြည့်နေ။ အဲ့ဒီအစီအစဉ်ကိုပဲ နောက် TV တစ်ခုကနေ Satellite နှင့်ဖမ်းပြီး စောင့်ကြည့် Satellite ကဖမ်းပြီးကြည့်တာ နည်းနည်းနောက်ကျနေလိမ့်မယ်။ ဒီ Satellite နှင့်ပတ်သက်တာကတော့ အဖွဲ့အစည်းတစ်ခုချင်းစီအနေနဲ့ဆိုရင် ငွေကြေးအရမဖြစ်နိုင်တာကြောင့် ဒီ Satellite ကို တစ်ကမ္ဘာလုံးဆိုင်ရာ ဆက်သွယ်ရေးအဖြစ် Operate လုပ်ကြပါတယ်။ ဒါကြောင့် ကုမ္ပဏီတွေက သူတို့ရဲ့ဆက်သွယ်မှုပြုသလောက် အချိန်ပေါ်ပေါ်မူတည်ပြီး ငွေကြေး ပေးသွင်းခြင်းဖြင့် အချက်အလက်တွေကိုပေးပို့ကြပါတယ်။ Terrestrial Microwave ထက်စာရင် Satellite Communiactions က နေရာတိုင်းကနေ တစ်ဦးတစ်ယောက်ချင်းစီကို (သူ့မှာသာလက်ခံဖို့ပစ္စည်းရှိခဲ့မယ်ဆိုရင်ပေါ့) ဆက်သွယ်ပေးဖို့တတ်နိုင်ပါတယ်။ Terrestrial Microwave စနစ်ကို ပေးပို့သူကအတွင်းကအကြောင်းအရာများကိုလက်ခံသူပဲသိစေချင် ရစေချင်တဲ့အခါမျိုးတွေမှာပဲ အသုံးများကြပါတယ်။ ဒီတော့ ဒီ Terrestrial က LAN လည်းရမယ်။ WAN လည်းရမယ်။ Satellite ကတော့ WAN ပဲရမှာဖြစ်ပါတယ်။ တစ်ဖက်မှာ Satellite Microwave WAN နှင့် ပတ်သက်တဲ့အကြောင်းအရာတွေကိုလေ့လာကြည့်ပါဦး။

Characteristics	Value
Frequency ranges	11-14 GHz
Maximum distance	Global reach
Bandwidth	1-10 Mbps
Installation/maintenance	Prohibitively difficult
Interference	Prone to EM interference, jamming, atmospheric disturbances
Cost	Prohibitive
Security	Not ver susceptible to eavesdropping

ဒီ Wire ကြိုးတွေမရှိတော့တဲ့ Wireless နည်းပညာဟာ တဖြည်းဖြည်းတိုးတက်လာခြင်း ကောင်းမွန်လာခြင်းတို့နဲ့ အတူတစ်ပြိုင်နက် အသုံးပြုမှုများပြားလာခြင်းကြောင့် ဈေး (ကုန်ကျစရိတ်) လည်း သက်သာလာပါတယ်။ Wireless နည်းပညာဘက်ကပြောမယ်ဆိုရင်လည်း တိုးတက်မှုတွေများပြားလွန်း လှပါတယ်။ Wireless နှင့်ပတ်သက်လို့ကတော့ ဒီလောက်ပါပဲ။

ဖြိုးဝါဖြို။

၁။ အခြေခံကနေ အလယ်အလတ်တန်းအထိဖတ်နိုင်အောင်ရည်ရွယ်ပြီးရေးသားထားပါတယ်။

၂။ လူစွမ်းအားအရင်းအမြစ်ဖွံ့ဖြိုးသည်ထက်ဖွံ့ဖြိုးလာအောင် ရည်သန်ပြီး ခန္ဓာထဲက ရှိသမျှအားတွေ အကုန်ထုတ်သုံးကာ မျက်စေ့ပြုတ်ထွက်မတတ် အပတ်တကုတ်ပြုစုထားတာဖြစ်ပါတယ်။ စာရွက်ချေးလေးငဲ့ပြီး ဒီလောက်နှင့်အဆုံးသတ်လိုက်တာပါ။ ဆက်ရေးရင်ရပါသေးတယ်။ ဒီကြားထဲ နေမကောင်းလို့ ဆေးရုံ ၅ ရက်တက်လိုက်ရပါသေးတယ်။ ဆေးဝိုးကုန်ကျစရိတ်ကို ပို့ပေးတဲ့ ချစ်လှစွာသော အစ်ကို နှစ်ယောက်နှင့် မရိုး နှစ်ယောက်ကို အထူးကျေးဇူးတင်ပါတယ်။

ဆေးရုံမှာလိုအပ်တာမရှိရအောင်ပြုစုပေးတဲ့ ချစ်ဇနီး အိအိဖြိုး နှင့် တယ်တယ်၊ မာမား၊ ယောက်ဖလေး ချစ်မင်း၊ ယောက်ဖကြီး ကိုမော်၊ ခယ်မလေးများ၊ တူမလေးများနှင့် မုန့်တွေယူလာပြီး သတင်းမေးလာကြသော ဆွေတော်မျိုးတော်အပေါင်းတို့ကိုလည်းကျေးဇူးတင်ပါတယ်။

၃။ မျိုးဆက်သစ်လူငယ်တွေ စာများများဖတ်ကြပါ။ ဒါမှလည်းစာအုပ်တွေပိုရောင်းရမှာပါ။ အဲလေ ဒါမှလည်း နည်းပညာတွေတတ်ကျွမ်းတဲ့ လူဘောင်အဖွဲ့အစည်းတွေပေါ်ထွန်းလာမှာဖြစ်ပါတယ်။

၄။ မသိသေးတဲ့သူတွေဖတ်ဖို့ရေးထားတာကြောင့် သိပြီးသားသူတွေဖတ်ရင် လွယ်ကူနေပါလိမ့်မယ်။

၅။ ထုံးစံအတိုင်း လိုအပ်တာရှိရင်ခွင့်လွှတ်ပေးကြပါ။ အရင်စာအုပ်တွေထက်ပိုကောင်းအောင်တော့ အစစအရာရာကြိုးစားထားပါတယ်။ စာရိုက်ပေးတဲ့ သူတွေကိုလည်း စာလုံးပေါင်းအမှားနည်းအောင်ရိုက်ကြဖို့၊ ပြန်စစ်ကြဖို့ ကြိုးကြပ်နေတဲ့ကြားက ကျွန်တော်မျက်စေ့ပါဝါကြောင့် စာလုံးပေါင်းအမှားတွေ တွေ့ရင်သည်းခံပေးကြပါဦး။ အမြဲတမ်းကောင်းအောင်ကြိုးစားပေးနေတယ်ဆိုတာကိုတော့ အကြွင်းမရှိယုံစေချင်ပါတယ်။

၆။ စာအုပ်တွေအကြွေးရိုက်ပေးတဲ့ ဇော်ဇော် (သိတာပုံနှိပ်တိုက်) ကိုဘယ်လိုကျေးဇူးတင်မှန်းမသိဘူး။

၇။ ကျွန်တော်စာအုပ်တွေကို ဝယ်ယူဖတ်ရှုကြသူ ကျေးဇူးရှင် မိတ်ဟောင်းမိတ်သစ်များအားလုံး ကိုယ်စိတ်နှစ်ဖြာ ကျန်းမာချမ်းသာကြပါစေ။

ကျေးဇူးတင်စွာဖြင့်

ဇော်လင်း

စာရေးသူ

၈ ဖေဖော်ဝါရီ ၂၀၀၇