သတင်းအချက်အလက်ဆက်သွယ်ရေးစနစ်

Networking

၁။ သတင်းဆက်သွယ်ရေးကွန်ယက်စနစ်တွင် အခြေခံအကျဆုံးအဆင့်မှာ ကွန်ပျူတာ (၂)လုံးပါဝင်၍တစ်လုံးနှင့်တစ်လုံးအား Cable ဖြင့်ဆက်သွယ်ထားပြီး Data နှင့် အခြားသော Resource များအား မျှဝေသုံးစွဲ (Share) နိုင်ခြင်းပင်ဖြစ်သည်။

၂။ တစ်ကိုယ်ရည်သုံးကွန်ပျူတာများတွင် Word Processing, Spreadsheets, Graphics နှင့် အခြားသော သတင်းအချက်အလက်များကို လိုသလိုဆောင်ရွက်နိုင်သော်လည်း Data များ လျှင်မြန်စွာ မျှဝေသုံးစွဲနိုင်မှု မရှိပေ။ကွန်ယက်(Network) ချိတ်ဆက်ထားခြင်း မရှိပါက Hard Copy အဖြစ် Print Out ထုတ်ပြီး သုံးစွဲခြင်း၊ တည်းဖြတ်ခြင်းများ ဆောင်ရွက်ရမည်ဖြစ်သည်။ အကောင်းဆုံးမှာ Floppy Disks များတွင် မိတ္တူကူးယူပြီး ဆောင်ရွက်ခြင်းဖြစ်သည်။ ယင်းကဲ့သို့ဆောင်ရွက်နေခြင်းအား Stand-alone envioronment သို့မဟုတ် Sneaker Network ဟုခေါ်သည်။

၃။ ကွန်ပျူတာများ၊ ပရင်တာများ ချိတ်ဆက်ပြီး Data များအား မျှဝေသုံးစွဲ (Share) ဆောင်ရွက်ခြင်းကို ကွန်ယက်(**Network**)ဟုခေါ်ပြီး ကွန်ပျူတာများ၏ အရင်းအမြစ်များ မျှဝေသုံးစွဲနိုင်ရန် ချိတ်ဆက်ရေး စိတ်ကူးကြံဆသည့်အသိသညာကို (**Networking**) ဟု ခေါ်ဆိုပါသည်။

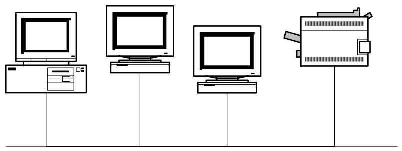
၄။ ကွန်ယက် ချိတ်ဆက်သုံးစွဲသဖြင့် Share Data Resources များအားမျှဝေနိုင်ခြင်းသာမကဘဲ Online Communications (sending messages back and forth, or e-mail) အဖြစ်ဆောင်ရွက်နိုင်သည်။ မျှဝေသုံးစွဲနိုင်သော အရင်းအမြစ်များတွင် Data, Applications နှင့် Peripherals များပါဝင်သည်။ Peripherals မှာ ရုပ်ဝတ္ထုပစ္စည်းများဖြစ်ပြီး External disk drive, Printers, Mouse, Modem နှင့် Joystick စသည့်များပါဝင်သည်။

The Types of Networks

၅။ ကွန်ယက်တည်ဆောက်ရာတွင်အသုံးပြုမည့်လုပ်ငန်းအနေအထားအလိုက်အောက်ပါအတိုင်း အမျိုးအစား (၂)မျိုးရှိသည်-

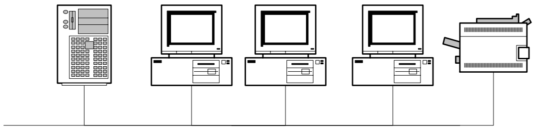
(က) Peer – to – Peer Network
(ခ) Server – based Network

Peer- to- peer Network



ဥပမာ- **Microsoft window workgroup**

Server-based Network



ဥပမာ- **Microsoft Windows 2000 Advance Server &**
Windows 2000 Proof Clients

၆။ **Peer-to-Peer Network** ကို တစ်နည်းအားဖြင့် Workgroup(a small group of people)ဟုခေါ်ပြီး သုံးစွဲသူ ၁၀ ဦး (ကွန်ပျူတာ ၁၀ လုံး)အောက်သာ သုံးစွဲသင့်သည်။ Peer-to-Peer Network တွင် ကွန်ပျူတာတိုင်းသည် Server နှင့် Client အဖြစ် ဆောင်ရွက်ပါသည်။သို့သော်လည်းServerအဖြစ်မရပ်တည်နိုင်ဘဲသုံးစွဲသူတိုင်းက ကွန်ယက် အတွင်း စီမံခန့်ခွဲမှုကို ဆောင်ရွက်နိုင်သည်။

၇။ **Server – based Network** တွင် Server သည် Dedicated Server ဖြစ်သည်။ စီမံခန့်ခွဲမှုနှင့် လုံခြုံမှုပိုင်းတို့ကို ထိန်းချုပ်ထားနိုင်ပြီး ကွန်ယက်အရွယ်အစား(Size)နှင့် ဆက်သွယ်မှုလမ်းကြောင်း(Traffic)တို့အား လုပ်ငန်းလိုအပ်ချက်အပေါ် မူတည်ပြီး ဆောင်ရွက်နိုင်သည်။ လုပ်ငန်းဆောင်ရွက်လိုမှုအရ Server များသည် Specialized Servers အနေဖြင့် File Server, Printer Server, Web Server, Mail Server, Communication Server များအဖြစ် တည်ဆောက်လေ့ရှိသည်။

၈။ **Peer-to-Peer Network** နှင့် **Server–based Network** သည် ကွဲပြားသော စွမ်းဆောင်ရည်များရှိပြီး ကွန်ယက်များသည် အောက်ဖော်ပြပါ များပြားသော အချက်အလက်များပေါ် တည်မှီသည် -

(က) Size of the Organization

(ခ) Level of security required

(ဂ) Type of business

(ဃ) Level of administrative support available

(င) Amount of network traffic

(စ) Needs of the network users

(ဆ) Network budget

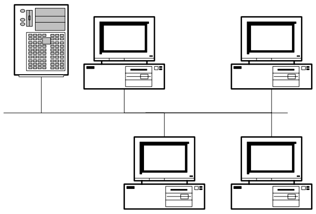
Network Design

၉။ ကွန်ယက်များချိတ်ဆက်ရာတွင် Physical Design များအား Topology ဟုခေါ်ပြီး အခြေခံအားဖြင့် အောက်ပါနည်း(၃)နည်းဖြင့် ဆောင်ရွက်သည်-

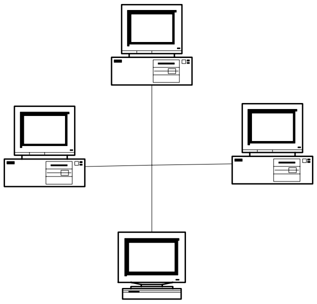
(က) Bus Topology

(ခ) Star Topology

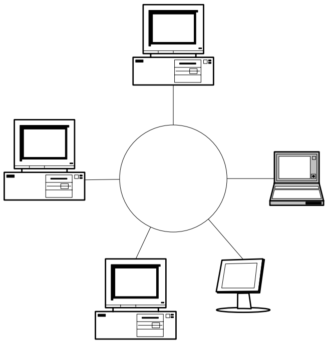
(ဂ) Ring Topology



Bus topology



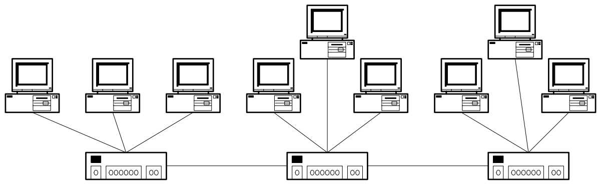
Star Topology



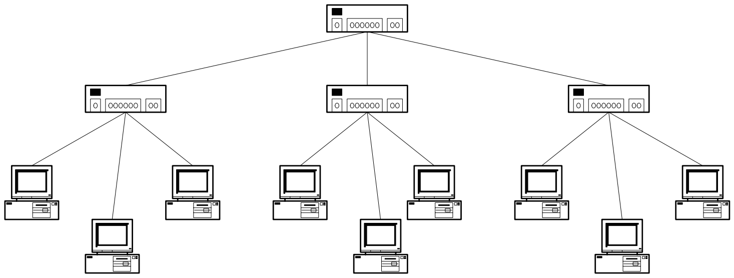
Ring Topology

၁၀။ ကွန်ယက်အား တစ်ဖြောင့်တည်းရှိသော Cable ပေါ်တွင် အစိတ်အပိုင်းများအလိုက် ဝင်ရောက်ချိတ်ဆက်ထားပါက Bus စနစ်ဖြစ်ပြီး၊ အမှတ်တစ်နေရာမှ သို့မဟုတ် Hub/ Switch တစ်ခုမှနေ၍ အစိတ်အပိုင်းများအလိုက် ခွဲဖြာချိတ်ဆက်ထားခြင်းသည် Star စနစ် ချိတ်ဆက်ခြင်းဖြစ်သည်။ အဝိုင်းပုံသဏ္ဌာန်ရှိသော Cable တွင် ကွန်ပျူတာများ ကွန်ယက် ချိတ်ဆက်ပါက Ring စနစ်ဖြစ်သည်။ ကွန်ယက်ချိတ်ဆက်မှု Topology အပေါ် မူတည်၍ အားနည်းချက်/အားသာချက်များ ရှိသော်လည်း လက်တွေ့ ကွန်ယက်ချိတ်ဆက်ရာတွင် အခြေခံစနစ် (၃)မျိုးသာမကဘဲ ရှုတ်ထွေးရောနှော နေလေ့ရှိသည်။

Star Bus Network



Star Ring Network



Network Cabling – (The physical media)

၁၁။ ကွန်ယက်ချိတ်ဆက်ရာတွင် အဓိကအားဖြင့် Cable အုပ်စု (၃)စုရှိသည်-

(က) Coaxial

(ခ) Twisted-pair

(ဂ) Fiber-optic

Coaxial Cable

၁၂။ Coaxial Cable များသည် Twisted-pair နှင့် Fiber-optic cable များထက် Interference နှင့် Attenuation ပိုများသည်။ အမျိုးအစားအားဖြင့် ၂ မျိုးရှိပြီး ယင်းတို့မှာ-

(က) Thin (Thinnet)(10Base2)(RG-58)

(ခ) Thick (Thicknet)(10Base5)(RG-8)

၁၃။ Thinnet သည် Cable ၏ Copper အချင်းမှာ .25 inch ရှိပြီး ၁၈၅ မီတာ(၆ဝ၇-ပေ) အကွာအဝေးထိသုံးစွဲနိုင်ပြီး BNC connectors (Bayonet Nut Connector / British Navel Connector)သုံးစွဲရသည်။ Thicknet ၏ အချင်းမှာ .5 inch ရှိပြီး ၅ဝဝ မီတာ(၁၆၄ဝ-ပေ)ထိ သုံးစွဲနိုင်သည်။

Twisted-pair Cable

၁၄။ အမျိုးအစားအားဖြင့် ၂ မျိုးရှိပြီး ယင်းတို့မှာ-

(က) Unshielded Twisted – pair (UTP)(10BaseT)

(ခ) Shielded Twisted – pair (STP)

၁၅။ UTP များသည် EIA/TIA 568(Electronic Industries Association and the Telecommunication Industries Association) ၏ စံပြုထားသော ဝါယာ ဖြစ်သည်။ UTP အား သုံးစွဲသူနှင့် သုံးစွဲမည့်လုပ်ငန်းများအလိုက် Catagories (၅)မျိုးထုတ်လုပ်သည်-

(က) Category-1 (တယ်လီဖုန်းကေဘယ်လ်အဖြစ် သုံးပြီး Voice သာ အသုံးပြုနိုင်၍ Data အသုံးမပြုနိုင်ပါ)။(RJ-11)

(ခ) Category-2 (4 Mbps သုံးနိုင်၍ 4 Twisted-pairs ဖြစ်သည်)။

(ဂ) Category-3 (10 Mbps သုံးနိုင်၍ 4 Twisted-pairs with three twists per foot ဖြစ်သည်)။

(ဃ) Category-4 (16 Mbps သုံးနိုင်၍ 4 Twisted-pairs ဖြစ်ပါသည်)။

(င) Category-5 (Up to 100 Mbps သုံးနိုင်၍ 4 Twisted-pairs of copper wire ဖြစ်သည်)။ (RJ-45)(Registered Jack), Cat 5 E, etc…

(စ) Category-6 (1000 Mbps သုံးနိုင်၍ 4 Twisted-pairs of copper wire ဖြစ်သည်) (၁၉၉၈ ခုနှစ် ဒီဇင်ဘာလမှစတင်သုံးစွဲခဲ့ပါသည်)။

ယနေ့အချိန်အခါတွင် Network ချိတ်ဆက်မှုအား Cat 5 E နှင့် Cat 6 Cabel များသာ အသုံးပြုကြသည်။

Fiber Optic Cable

၁၆။ ဖန်မျှင်(သို့မဟုတ်)ပလက်စတစ်မျှင်ဖြင့် ပြုလုပ်ထားပြီး အလင်းလှိုင်းဖြင့် သတင်းအချက်အလက်များကို သယ်ဆောင်သည်။ အသုံးပြုနိုင်သည့် Bandwidth ကျယ်ပြန့်၍ စွမ်းအားကျဆင်းမှုနည်းပါးသော်လည်း ကွန်ယက်များတွင် Fiber Cable များ Installation ပြုလုပ်ရာတွင် ကြိုးဆက်ခြင်း၊ တွဲဖက်သုံးစွဲရသည့်ပစ္စည်းများ အဆင့်မြင့် Equipment များဖြစ်ရန်လိုအပ်ခြင်း၊ Fiber နည်းပညာ ကျွမ်းကျင်ပညာရှင်များ လိုအပ်ခြင်းတို့သည် Disadvantage ပင်ဖြစ်သည်။ သို့သော်လည်း Network Backbone အနေဖြင့် Fiber Optic Cabel ကိုသာ သုံးစွဲသင့်ပါသည်။

Ethernet

၁၇။ Ethernet သည် LAN Impletation တွင် အသုံးများပြီး တွင်ကျယ်သော နည်းပညာဖြစ်သည်။ Ethernet ၏ standard များမှာ-

(က) **Ethetnet and IEEE 802.3** ။ Coaxial Cable များပေါ်တွင် အမြန်နှုန်း 10Mbps ဖြင့် အချက်အလက်များကို ပို့ဖမ်းနိုင်သည်။

(ခ) **100-Mbps Ethernet** ။ Twisted-pair cable များပေါ်တွင် အမြန်နှုန်း 100Mbps ဖြင့် အချက်အလက်များကိုပို့ဖမ်းနိုင်ပြီး Fast Ethernet အဖြစ်သိရှိကြသည်။

(ဂ) **1000-Mbps Ethernet** ။ Fiber နှင့် Twisted-pair cable များပေါ်တွင် အမြန်နှုန်း 1000Mbps ဖြင့် အချက်အလက်များကို ပို့ဖမ်းနိုင်ပြီး Gigabit Ethernet အဖြစ် သိရှိကြသည်။

Ethernet နှိုင်းယှဉ်ဇယား

Characteristic	10Base5	10Base2	10BaseT	10BaseFL	100BaseT
Speed(Mbps)	10	10	10	10	100
Max Segment length (m)	500	185	100	2000	100
Media	50-Ohn Coax (thick)	50-Ohn Coax (thin)	UTP Cable	Fiber-Optic	UTP Cable
Topology	Bus	Bus	Star	Point-to-Point	Bus

Commom Ethernet Cable Types

EThernet Name	Cable Type	Max; Speed (Mbps)	Max; Transmission Distance(Segment/m)	Note
10Base5	Coax	10	500	Uses vampire taps to connet devices to cable
10Base2	Coax	10	185	Also called Thinnet, a very popular implementation of Ethetnet over coax
10BaseT	UTP	10	100	
100BaseT	UTP	100	100	
100BaseVG	UTP	213(Cat 5) 100(Cat 3)		
100BaseT4	UTP	100	100	Required 4 pairs of Cat 3,4,or 5 UTP cable
100BaseTX	UTP STP	100	100	2 pairs of Cat 5 UTP or STP
10BaseF	Fiber	10	Varies(ranges from 500 to 2000m)	Ethernet over fiber-optic implementation
100BaseFX	Fiber	100	2000	100Mbps Ethernet over fiber-optic implementation

Ethernet Cable Descriptions

၁၈။ Ethernet cable အမျိုးအစားများအားပုံသဏ္ဍာန်အားဖြင့် N<signal>X ဖြင့်ဖော်ပြကြသည်။ N သည် ဂဏာန်းဖြင့်ရေးသားပြီး ပို့လွှတ်နိုင်မှုနှုန်း(transmission speed) Megabits per second ကိုလည်းကောင်း၊ <signal> သည် signaling type ဖြစ်သော baseband သို့မဟုတ် broadband ကိုလည်းကောင်း၊ X သည် ethernet cable အမျိုးအစားကိုလည်းကောင်း ကိုယ်စားပြုဖော်ပြသည်။ ဥပမာအားဖြင့် 10BaseT ဟုသုံးနှုန်းရာ၌ 10 သည် 10Mbps ဖြစ်ပြီး Base သည် Baseband ၊ T သည် twisted pair ၏ 10Mbps တွင်သုံးစွဲသော Category 3,4,5 UTP ကို ဖော်ပြခြင်းဖြစ်သည်။

Type of Network Connectivity Devices

၁၉။ Network ချိတ်ဆက်နိုင်ရန် ကြားခံပစ္စည်း(Media)နှင့် ဆက်သွယ်မှု(Connections) များသည် ပုံသဏ္ဍာန်မျိုးစုံရှိပြီး ယင်းတို့မှာ-

(က) **Network Interface Card (NIC)** ။ Expansion card ဖြစ်၍ Computer တွင် PCI (Peripheral component interconnection) slot ၌ တပ်ဆင်ပြီး Computer အား Network နှင့်ချိတ်ဆက်ရသည်။ အချို့သော motherboard များတွင် built in ပါရှိ သည့်အပြင် တချို့သော Notebook များတွင် printer port (သို့) PC card slot တွင် NIC adapter များအား ချိတ်ဆက် အသုံးပြုရသည်။

(ခ) **Router** ။ မတူညီသော Networkများ ချိတ်ဆက်လျှင် physical media အဖြစ် သုံးစွဲသည်။ Network အစိတ်အပိုင်းမှ Internet သို့ချိတ်ဆက်ရာ၌ သုံးစွဲရသည်။ RIP(Routing Interface Protocol)ကို သုံးစွဲ၍ Network level တွင် အလုပ်လုပ်သည်။

(ဂ) **Gateway** ။ မတူညီသော Network များ ချိတ်ဆက်ရာတွင် Gateway အဖြစ် Hardware နှင့် Software များကိုသုံးစွဲရသည်။ Gateway ကို Device အဖြစ် လုံးဝကွဲပြားခြားနားသော LAN နှင့် Mainframe ချိတ်ဆက်ရာတွင် သုံးသည်။ LAN သည် Distributed Processing, Baseband Communication နှင့် ASCII Character Set ကိုသုံးပြီး Mainframe သည် Centralized Processing, Broadband နှင့် Baseband Communications နှင့် EBCDIC Character Set ကိုသုံးစွဲ သည်။ LAN Protocol အဖြစ် Gateway Software ကိုသုံးစွဲပြီး Mainframe နှင့် အလားသဏ္ဍာန်တူစေရန် ပြောင်းလဲပြုလုပ်ပေး သည်။ Gateway Device သည် အလွန်ရှုပ်ထွေးသော Network devices များဖြစ်သည်။ အဘယ်ကြောင့်ဆိုသော ပြောင်းလဲပြုလုပ်ပေးခြင်းများကို OSI model ၏ layers များစွာ၌ ပြုလုပ်ရခြင်းကြောင့်ဖြစ်သည်။ Gateway များတွင် BGP(Border Gateway Protocol) ကိုသုံးစွဲရပြီး Router ကဲ့သို့ပင် ပြုလုပ်သည်။ Router/Gateway တွင် interface အနည်းဆုံး (၂)ခု ပါရှိမည် ဖြစ်သည်။

(ဃ) **Hubs/Switch** ။ Physical layer Device (Concentrator) ဖြစ်ပြီး များပြား စွာသော Network Devices ချိတ်ဆက်ရာတွင် ဗဟိုအချက်အချာနေရာ၌ ချိတ်ဆက်ရန် သုံးစွဲသည်။ Network Design ၏ Star Topology တွင်

သုံးစွဲလေ့ရှိသည်။ 4 ports, 8 ports, 16 ports, 24 ports စသည်ဖြင့် တည်ဆောက်ထားပြီး port တစ်ခုမှ အချက်အလက်များကို လက်ခံပြီး ကျန် ports များမှချိတ်ဆက်ထားသော Network Devices များသို့ အချက်အလက်များအား ထပ်ဆင့်ပေးပို့သည်။ Switch သည် Point to Point ဆောင်ရွက်ပေးနိုင်ခြင်းကြောင့် ရှုပ်ထွေးမှုမရှိပဲ လျင်မြန်မှုရှိသဖြင့် Switch ကိုသာ သုံးစွဲသင့်ပါသည်။

(င) **Bridge** ။ တူညီသော Protocol သုံးစွဲထားသည့် နှစ်ခု သို့မဟုတ် နှစ်ခုထက်ပိုသော Network များအား Dedicated Line ဖြင့် End to End ချိတ်ဆက်ထားခြင်းဖြစ်သည်။

Access Points

၂၀။ Access Point ဆိုသည်မှာ Transceiver ပင်ဖြစ်သည်။ အချက်အလက်များအား ထုတ်လွှင့်ခြင်းနှင့် ဖမ်းယူခြင်းအား ဆောင်ရွက်နိုင်ပြီး ပတ်ဝန်းကျင်ရှိ ကွန်ပျူတာများနှင့် သတင်းအချက်အလက်များ ပေးပို့/ဖမ်းယူခြင်းအား ကြိုးမဲ့ကွန်ယက်၊ ကေဘယ်လ် ကွန်ယက်များအတွင်း ဆောင်ရွက်နိုင်သည်။

Transmission Technique

၂၁။ Wireless LANs များတွင် အချက်အလက်များအားအောက်ဖော်ပြပါနည်းစနစ် (၄)နည်းဖြင့် ထုတ်လွှင့်သည် -

(က) Infrared

(ခ) Laser

(ဂ) Narrow-band(Signal frequency) Radio

(ဃ) Spread-spectrum Radio

Wi-Fi(Wireless Fidelity) ဝိုင်ဖိုင်နည်းပညာ

၂၂။ Wi-Fi ဆိုသည်မှာအီလက်ထရောနစ်နှင့်လျှပ်စစ်ဆိုင်ရာနည်းပညာများစွာတို့ အတွက် စံနှုန်းသတ်မှတ်ပေးသော နိုင်ငံတကာအဖွဲ့အစည်းဖြစ်သည့် Institute of Electrical and Electronic Engineers **(IEEE)** မှ ကြိုးမဲ့ကွန်ယက်များအတွက် သတ်မှတ်ထားသော IEEE

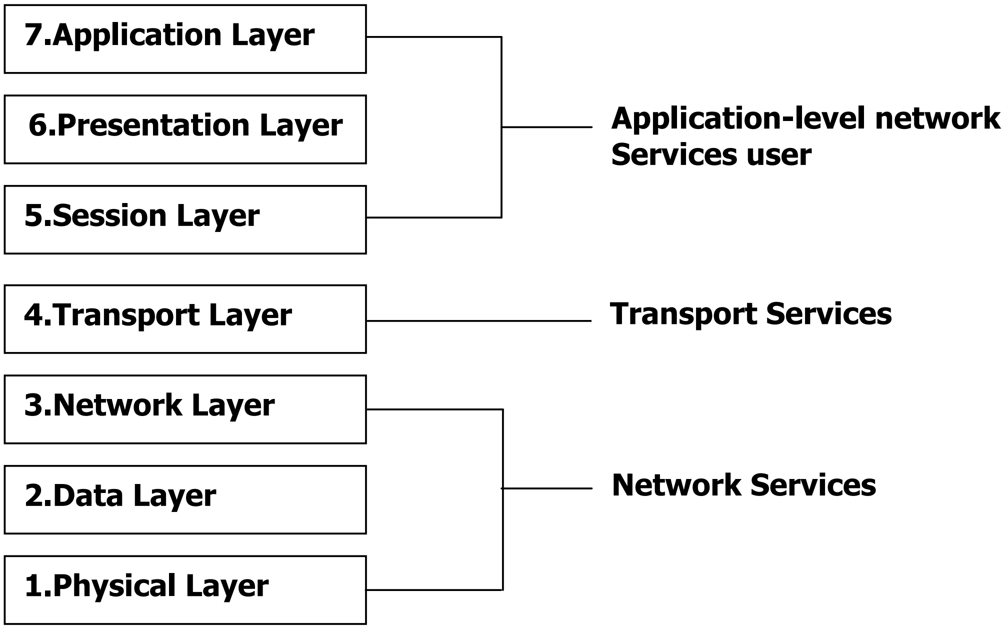
802.11 b စံလှိုင်းနှုန်းပင်ဖြစ်သည်။ IEEE 802.11 b သည် သတင်းအချက်အလက် ပို့လွှတ်နှုန်း 11 Mbps ဖြင့် လှိုင်းနှုန်း 2.4 GHz (ISM band) အတွင်း ဆက်သွယ်နိုင်သည်။ လက်ရှိသုံးစွဲနေသော DSL Broadband ထက်လျှင်မြန်မှုရှိသည်။

၂၃။ IEEE 802.11 standard တွင် b, a, g နှင့် i တို့ရှိပါသည်။ IEEE 802.11 a သည် သတင်းအချက်အလက် ပို့လွှတ်နှုန်း 54Mbps ဖြင့် လှိုင်းနှုန်း 5 GHz (SHF band) အတွင်း ဆက်သွယ်သည်။ရုပ်သံများ၊ ဗီဒီယိုပုံရိပ်များပေးပို့ရာတွင် ပိုမိုကြည်လင်ပြတ်သားပြီး အရွယ်အစားကြီးမားသော File များကို လျှင်မြန်စွာ ပေးပို့နိုင်သည်။

၂၄။ IEEE 802.11 g သည် သတင်းအချက်အလက် ပို့လွှတ်နှုန်း 54Mbps ဖြင့် လှိုင်းနှုန်း 2.4 GHz (ISM band) အတွင်းဆက်သွယ်ပါသည်။ IEEE 802.11 b ထက် လှိုင်းနှုန်းတာကျယ်ပြန့်သည့်အတွက် ရုပ်သံများဗီဒီယိုပုံရိပ်များပေးပို့ရာတွင် ပိုမိုကြည်လင်ပြတ်သားပြီး အရွယ်အစားကြီးမားသော File များ၊ Web site များကို တစ်ခဏ အတွင်းဆက်သွယ်ဖလှယ်နိုင်ပါသည်။ IEEE 802.11 i သည် IEEE 802.11 g နှင့်တူညီပြီး လုံခြုံမှုစနစ် ပိုမိုကောင်းမွန်စေရန် ဆောင်ရွက်ထားပါသည်။ အခြားစနစ်များတွင် အသုံးပြု သော WEP (Wired Equivalent Privacy) ၏ လုံခြုံမှုအားနည်းချက်များကို ပြုပြင်ပြီး ကြားဖြတ်ဖော်ထုတ်ခြင်းမပြုနိုင်သော အဆင့်မြင့်ဝှက်စာ - AES (Advanced Encryption Standard) တစ်နည်းအားဖြင့် WAP2 (Wi-Fi Protected Access-2) တည်ဆောက်ထားခြင်း ဖြစ်သည်။

OSI Model ၊ 802 Networking Model

၂၅။ A Layered Architecture ။ Open Systems Interconnection(OSI) Networking Model တွင် သတင်းအချက်အလက်များဆက်သွယ်ရာတွင် အလွှာ(Layer)-၇ လွှာဖြင့် ခွဲခြားထားပါသည်။Layer တစ်ခုခြင်းအလိုက်အပြန်အလှန်တည်မှီနေပြီးမတူသော ကွန်ယက်အတွင်း ဆက်သွယ်ချိတ်ဆက်နိုင်ရန် စက်ပစ္စည်းကရိယာများ(Equipments)၊ လုပ်နည်းသညာ/လုပ်ငန်းသညာများ(Protocols)၊ စွမ်းဆောင်ရည်များပေါ် မူတည်သည်။



IEEE 802 Categories

802.1	LAN / MAN Management (and Media Access Control Bridges) (Internetworking)
802.2	Logical Link Control
802.3	Carrier-Sense Multiple Access with Collision Detection (CSMA/CD) (Ethetnet)(Bus Topology)
802.4	Token Bus LAN
802.5	Token Ring LAN
802.6	Metropolitan Area Network (**D**istributed **Q**ueue **D**ual **B**us)
802.7	Broadband Local Area Networks
802.8	Fiber Optic LANs and MANs
802.9	Integrated Services (Voice/Data) LAN Interface
802.10	Network Security
802.11	Wireless LAN
802.12	Demand Priority Access Method

TCP/IP Fundamentals

၂၆။ Network များချိတ်ဆက်ရာတွင် protocols ၊ ports နှင့် sockets များအား သိရှိထားရမည်ဖြစ်သည်။ အားလုံးသည် physically မဟုတ်ဘဲ logically ဖြစ်သည်။

Protocols

၂၇။ Protocol ဆိုသည်မှာ language တစ်မျိုးဖြစ်ပြီး အမျိုးမျိုးကွဲပြားခြားနားနေသည့် file system များ၊ OS အမျိုးမျိုး အသုံးပြုသည့် Communication Device များ အချင်းချင်း ချိတ်ဆက်နားလည် အသုံးပြုနိုင်သည့် application programmer များရေးသားထားသော language ဖြစ်သည်။ ထို့ကြောင့် network device များအသုံးပြုသော language ဟု အတိုချုပ်ပြောနိုင်သည်။ Protocol သည် ရုပ်သဘော မဆောင်သည့် rule များ၊ Specification များ ဖြစ်ပြီး Communication field အလိုက် အမျိုးမျိုးကွဲပြားခြားနားနေသည့် protocol အမျိုးအစား ထောင်၊ သောင်းမက ရှိသည်။ Protocol များအနက် Computer Internet Communication Field တွင် အသုံးများသော Protocol အချို့နှင့် အသုံးပြုသည့် ကဏ္ဍအလိုက် အောက်တွင် အတိုချုံး ဖော်ပြထားသည်-

- TCP/IP (Transport Control Protocol/Internet Protocol)
- UDP (User Datagram Protocol)
- SMTP (Simple Mail Transport Protocol)
- POP (Post Office Protocol)
- ICMP (Internet Control Message Protocol)
- HTTP (Hyper Text Transport Protocol)
- IPX (Internet Packet Exchange)
- SLIP (Serial Line Interface Protocol)
- PPP (Point to Point Protocol)
- NETBIOS (Network Basic Input/Output System)
- NetBEUI (NETBIOS Extended User Interface)
- ARP (Address Resolution Protocol)
- BGP (Border Gateway Protocol)
- Telnet (Terminal Networking Protocol)
- FTP (File Transfer Protocol)

- NNTP (Network News Transport Protocol)
- AppleTalk (Protocol Suite for Apple Macintosh)
- RS232

TCP/IP

၂၈။ Protocol များအနက် TCP/IP (Transport Control Protocol/ Internet Protocol) သည် Internet ကြီး တစ်ခုလုံးကို မောင်းနှင်ထိန်းချုပ်နေထားသော protocol ဖြစ်သည်။ Network ချိတ်ဆက်ရာတွင်သုံးစွဲသော protocol လည်းဖြစ်သည်။

SMTP

၂၉။ Simple Mail Transport Protocol (SMTP) သည် Mail များပို့လွှတ်ရာတွင် အသုံးပြုသော protocol ဖြစ်သည်။

POP

၃၀။ Post Office Protocol သည် Mail များ receive လုပ်ရာတွင် အသုံးပြုသည်။

ICMP

၃၁။ Network Connection ရှိ/မရှိ စမ်းသပ်ရာတွင် ICMP(Internet Control Message Protocol) ကို အသုံးပြုသည်။ **`Ping`** command အသုံးပြုခြင်းမျိုးတွင်း သုံးသည့် protocol ဖြစ်သည်။ Ping လုပ်သည် ဆိုသည်မှာ မိမိ request လုပ်သော IP မှ reply ပြန်ဖြေခြင်း ပင်ဖြစ်သည်။

HTTP

၃၂။ World Wide WEB (www) အတွက် WEB browser များတွင် အသုံးပြုသော Hyper Text Transport Protocol (HTTP) ဖြစ်သည်။ ယခင် Novell ကဲ့သို့သော OS များတွင် HTTP အစား IPX(Internet Packet Exchange Protocol) ကို အသုံးပြုခဲ့ကြသည်။

SLIP/PPP

၃၃။ Serial Line Interface protocol (SLIP) သည် Modem ဖြင့် serial phone line များကို အသုံးပြု၍ Internet ချိတ်ဆက် အသုံးပြုရာတွင် Modem က အသုံးပြုသော protocol ဖြစ်သည်။ SLIP သည် Graphical interface မရသည့်အတွက်ကြောင့် နောက်ပိုင်းတွင် SLIP အစား Graphical interface ရပြီး SLIP function အသုံးပြုနိုင်သော PPP(point to Point Protocol) ကို အသုံးပြုလာကြသည်။

NETBIOS

၃၄။ (Network Basic Input/Output System) NETBIOS သည် work group များအတွင်း အသုံးပြုသော protocol ဖြစ်ပြီး Net BEUI သည် NETBIOS ကို extension လုပ်ထားသော protocol ဖြစ်သည်။

ARP

၃၅။ Network Interface Card (NIC) များ၏ physical Address (MAC address) များ Logical Address များကို Bind လုပ်ပေးသော protocol ကို ARP (ADDRESS Resolution Protocol) ဟုခေါ်သည်။

BGP & RIP

၃၆။ BGP နှင့် RIP များသည် Router များ၏ လမ်းကြောင်းကို သတ်မှတ်ပေးရာတွင် အသုံးပြုသော protocol ဖြစ်သည်။

Telnet

၃၇။ VNC ကဲ့သို့သော remote communication software များတွင် Telnet (Terminal networking protocol) ကိုအသုံးပြုသည်။

FTP

၃၈။ FTP(File Transfer Protocol) သည် file များကို transfer ပြုလုပ်ရာတွင် independence အဖြစ်ဆုံး protocol ဖြစ်သည်။

RS232

၃၉။ com1, com2 ကဲ့သို့သော communication port များက အသုံးပြုသော protocol များဖြစ်ကြသည်။ Hardware flow ကို ထိမ်းချုပ်သော protocol အမျိုးအစားတွင် ပါဝင်သည်။

၄၀။ TCP/IP, SMTP, HTTP စသော protocol များသည် Transport ကိုထိန်းချုပ်သော protocol အမျိုးစားထဲတွင် ပါဝင်ပြီး PPP များကို serial line များ၏ flow များတွင် အသုံးပြုကြသည်။ E-Mail များသည် SMTP, POP, IMAP အစရှိသော protocol များကို အသုံးပြုကြပြီး နောက်ပိုင်းတွင် HTTP ကိုပါ support လုပ်ပေးလာနိုင်သည်။ ယခုအချိန်တွင် NEWS များအတွက်ပါ ရည်ရွယ်၍ NNTP(Network NEWS Transport Protocol) ကို support လုပ်ပေးလာနိုင်သည်။ Internet Explorer ကဲ့သို့ WEB browser များသည် HTTP,NNTP, FTP စသည်တို့ကို support လုပ်ပေးနိုင်သည့်အပြင် local files

များကိုပါ support လုပ်ပေးနိုင်သည်။ ယခုခေတ်ကာလတွင် WEB browser များသည် protocol တော်တော်များများကို support လုပ်ပေးနိုင်လာပြီ ဖြစ်သည်။

၄၁။ Internet တစ်ခုလုံးကို protocol များဖြင့် လှုပ်ရှားသက်ဝင်စေသည့် သဘောကို သိရှိရန်အတွက် protocol များနှင့်ပတ်သက်၍ port များအကြောင်းကိုလည်း သိရှိထားမှ ဖြစ်ပေမည်။

Ports

၄၂။ Port ဆိုရာတွင် ၎င်းတို့သည်ကိုင်တွယ်၍ မရသော logical များဖြစ်ကြပြီး Communication endpoint ဖြစ်သည်။ port number များသည် 16-bit ရှိသည့်အတွက် port အရေအတွက် 2^{16} (0 to 65536) ရှိသည်။ prot number 0 to 1024 ကို well known port များအဖြစ် IANA (Internet Assigned Numbers Authority) မှ သတ်မှတ်ပေးထားသည်။ ဥပမာအားဖြင့် အသုံးများသော well known port အချို့ကို ဖော်ပြထားသည်။

Service	**Port Number**
FTP	**21**
Telnet	**23**
SMTP	**25**
DNS	**53**
WWW	**80**
POP3	**110**
Proxy	**8080**
IRC	**6667**
IMAP	**143**

၄၃။ အခြေအနေအကြောင်းအရာ တစ်စုံတစ်ခုကြောင့် Standard သတ်မှတ်ပေးထားသော port number များကို အသုံးမပြုဘဲ မိမိနှစ်သက်ရာ port number မှ service ပေးလိုလျှင်လဲရသည်။ များသောအားဖြင့် port number 1025 မှ 65536 အထိကို client များက randomize အသုံးပြုကြသည်။ Port များနှင့် protocol များအကြောင်း သိရှိပြီးလျှင် ၎င်းတို့၏ပေါင်းစည်း ဆောင်ရွက်၍ Internet အား မည်သို့မည်ပုံ အဆင်ပြေချောမွေ့အောင် လည်ပတ်စီးဆင်း စေသည့် အကြောင်းကို ဆက်လက်သိရှိရန် လိုအပ်ပေသည်။

Socket

၄၄။ Communication Devices နှစ်ခု ချိတ်ဆက်မိတိုင်း socket ဖြစ်သည်။ device တစ်ခုက destination ဖြစ်လျှင် ကျန် device တစ်ခုက source ဖြစ်သည်။ destination ၏ IP + Port နှင့် Device ၏ IP + Port နှစ်ခုပေါင်းလျှင် socket တစ်ခုဖြစ်သည်။

Destination or Client		***Source or Server***	
IP	: 192.169.1.100	IP	: 192.168.1.1
Port	: 6571	Port	: 21

Destination or Client		***Source or Server***	
IP	: 192.169.1.100	IP	: 192.168.1.1
Port	: 6571	Port	: 23

Destination or Client		***Source or Serv***	
IP	: 192.169.1.100	IP	: 192.168.1.2
Port	: 6571	Port	: 23

Destination or Client		***Source or Server***	
IP	: 192.169.1.100	IP	: 192.168.1.20
Port	: 80	Port	: 23

၄၅။ အထက်ဖော်ပြပါ socket များကဲ့သို့ IP တူ၊ port မတူ၊ Port တူ၊ IP မတူ သော connection များကြောင့် network သည် မှန်မှန်ကန်ကန် အလုပ်လုပ်ဆောင်နေခြင်း ဖြစ်သည်။ computer တစ်လုံးတွင် ချိတ်ဆက်လုပ်ဆောင်နေသော port များကို သိရှိလိုပါက netstat ဆိုသော command မျိုးဖြင့် ကြည့်ရှုနိုင်သည်။ ထို့ကြောင့် server တစ်ခုလုပ်လိုက်တိုင်း service ပေးမည့် port ကို အထူးသတိပြုရမည် ဖြစ်သည်။

၄၆။ ဖော်ပြပါ protocol, Port နှင့် Socket များအလုပ်လုပ်ပုံ အကြောင်းကို အကြမ်းဖျဉ်းနားလည် သိရှိပြီးပါက TCP/IP အကြောင်းနှင့် Subnetting အကြောင်းတို့ကို ဆက်လက်လေ့လာကြရမည်။

TCP/IP (Transport Control Protocol/ Internet Protocol)

၄၇။ TCP/IP သည် protocol အမျိုးအနွယ်အုပ်စုများထဲမှတစ်ခုဖြစ်ပြီး Internet နည်းပညာ တွင် အလွန်အရေးကြီးသော အချက်တစ်ချက်ဖြစ်ပါသည်။ Intranet များတည်ဆောက် အသုံးပြုရန်လွယ်ကူစွာဆောင်ရွက်နိုင်၍ Internet ၏ အခြေခံအုတ်မြစ်ဖြစ်ပါသည်။ Internet သို့ဝင်ရောက်ဆက်သွယ်လိုလျှင်လည်းကောင်း၊ Intranet တည်ဆောက်ရာတွင်လည်းကောင်း၊ ဦးစွာမိမိ၏ server သို့မဟုတ် workstation အား TCP/IP setup လုပ်ရသည်။ Intranet အပါအဝင် Internet အလုပ်လုပ်နိုင်ရန် အဓိကအချက်အချာဟုပင်ဆိုနိုင်သည်။

၄၈။ ၁၉၇၃ ခုနှစ်တွင်စတင်အဆိုပြုတင်ပြခဲ့၍ ၁၉၈၃ ခုနှစ်ထိ စံသတ်မှတ်သောအဆင့်ဖြင့် ဖွံ့ဖြိုးတိုးတက်ပြီးကျယ်ပြန့်စွာ အသုံးပြုနိုင်ခြင်းမရှိသေးသော်လည်း ယင်းနှစ်မှာပင် ARPAnet မှဆက်သွယ်မှုအားလုံးကို TCP/IP အားတရားဝင်သုံးစွဲခြင်းဖြင့် Internet ၏ ရှေ့ပြေးဖြစ်ခဲ့ပါသည်။ TCP/IP သည် ပညာရေးနယ်ပယ်တွင် စတင်ပျံ့နှံ့ခဲ့ပြီးမှ Internet နှင့် Intranet များတွင် သုံးစွဲမှုကြီးထွားခဲ့ခြင်းဖြစ်ပါသည်။ များစွာသော hardware နှင့် software platforms များတွင် TCP/IP သည် လွတ်လပ်စွာသုံးစွဲနိုင်ပြီး အနှောက်အယှက်ဖြစ်မှုများ ကင်းစေသည်။

Ethernet (Media Access Control) Address

၄၉။ Ethernet network card များသည် ကိုယ်ပိုင် hardware address ရှိပြီး media access control (MAC) address အဖြစ်သိရှိကြပါသည်။ စက်ရုံမှထုတ်လုပ်စဉ် ထည့်သွင်းပေးလိုက်ပြီး 48bits အား Hexadecimal ဖြင့်ဖွဲ့စည်းထားပါသည်။ ယင်း address ၏ ပထမအပိုင်း ၃ ပိုင်း ကို OUI(Organizationally Unique Identifier) ဟုခေါ်ပြီး IEEE မှခွဲဝေသတ်မှတ်ပေးပါသည်။ ကျန်အပိုင်း ၃ ပိုင်းကို ထုတ်လုပ်သူမှ card တစ်ခုချင်းအလိုက်သတ်မှတ်ပါသည်။ ပြင်ဆင် မရဘဲ hard coded အဖြစ် NIC ပေါ်တွင်အပြီး တပ်ဆင်ထားခြင်းဖြစ်သည်။

ဥပမာ - 1F:10:FF:FF:AE:95

IP Address

၅၀။ ကမ္ဘာအရပ်ရပ်ရှိ computer များအချင်းချင်း မှန်ကန်စွာ ချိတ်ဆက်အသုံးပြုနိုင်ရန် အတွက် IP address ဖြင့် management ပြုလုပ်သည်။ IP address များသည် 32-bit ရှိပြီး 8-bit (၄)ခု အား dot ဖြင့်ခွဲထားသည့်အတွက် dotted decimal သို့မဟုတ် quad decimal ဟုခေါ်ပါသည်။တစ်ခါတစ်ရံတွင် 8-bits အပိုင်း ၁ ခုအား individual byte သို့မဟုတ် octet ဟုလည်းခေါ်ကြပြီး အသုံးပြုနိုင်သောတန်ဘိုးအားဖြင့် 1 မှ 254 အထိ ရှိသည်။ 0 နှင့် 255 မှာ အရံအဖြစ်ထားရှိပြီး 0 မှာ network address ဖြစ်ပြီး 255 မှာ broadcast address ဖြစ်သည်။

$$2^8 \quad . \quad 2^8 \quad . \quad 2^8 \quad . \quad 2^8$$

2^{32} = 4.5 billion ရှိပြီး minimun range 0 . 0 . 0 . 0 မှ maximum range 255 . 255 . 255 . 255 အထိရှိသည်။ Internet ပေါ်တွင် ပုံမှန် IP address များကို InterNIC(Internet Network Information Center) မှ ခွဲဝေသတ်မှတ်ပေးပါသည်။ တစ်ဦးချင်းတိုက်ရိုက် ချိတ်ဆက်ပါက InterNIC မှရယူရမည် သို့မဟုတ် မိမိ၏ ISP(Internet Service Provider) မှ လိုင်းခြုံမှုရှိမှသာ fully qualified address အားရယူရမည်။ သို့သော် Intranet တစ်ခုအား တည်ဆောက်ထားပြီး ပြင်ပလောကဖြစ်သော Internet နှင့် ချိတ်ဆက်ရန်မလိုအပ်ပါက InterNIC တွင် မှတ်ပုံတင်ရန်မလိုအပ်ပေ။

Classifications

၅၁။ များပြားလှသော IP address များအား Internet နှင့်ချိတ်ဆက်သုံးစွဲပါက မှားယွင်းမှု မရှိစေရေးအတွက် class များနှင့် ခွဲခြားထားခြင်းကို သိရှိရန်လိုအပ်ပါသည်။ IP address များ၏ ပထမဦးဆုံးအတွဲ (first octet) ကို ကြည့်ပြီး အောက်ပါအတိုင်း ခွဲခြားထားသည်။

TCP/IP classes

Range of IP Address	Class of IP Address
0 to **127**	**A**
128 to **191**	**B**
192 to **223**	**C**
224 to **239**	**D**
240 to **255**	**E**

၅၂။ မြန်မာနိုင်ငံအတွက် assign လုပ်ထားသည့် IP သည် 203 ဖြစ်သဖြင့် Class (C) အားအသုံးပြုထားခြင်းဖြစ်သည်။

Private Network Address

Class of IP Address	IP Address	
A	**10.0.0.0**	
B	**172.16.0.0**	
C	**192.168.0.0**	
Local Loopback	**127.0.0.1**	**Local Host**

၅၃။ အထက်ဖေါ်ပြပါ IP Address များသည် Internet တွင် route မလုပ်ပါ။127.0.0.1 သည်လည်း Internet ပေါ်တွင် routing လုပ်မပေးပါ။ အဘယ်ကြောင့် ဆိုသော် ယင်း IP သည် **`local loop back`** အတွက် သတ်မှတ်ထားခြင်းကြောင့် ဖြစ်သည်။ မိမိစက်ရဲ့ network function ၊ network interface card (NIC) ကောင်း/မကောင်း စစ်ဆေးသော address ဖြစ်သည်။ နောက်ပိုင်းတွင် 127.X.X.1 သည် local loop back စမ်းသပ်နိုင်ရန် အတွက် သီးသန့် IP အဖြစ်သတ်မှတ်ထားသည်။

၅၄။ Class A သည်အလွန်ကြီးမားသော Network များအတွက်သာအသုံးပြုသည်။ Octets များသည် Network နှင့် host/node ခွဲခြားနိုင်သည်။ Class A တွင် IP Address ၏ First octet သည် Network ဖြစ်ပြီး ကျန် octets ၃ ခုသည် hosts ဖြစ်သည်။ ထို့ကြောင့် Networks 126 ခုရှိပြီး Network တစ်ခုလျှင် hosts ပေါင်း 16,581,375 ခုသုံးစွဲနိုင်ပါသည်။ ဥပမာအားဖြင့် Class A Networks များတွင် General Elctric ၊ IBM ၊ Hewlett Packard ၊ Apple ၊ DEC ၊ Xerox ၊ Columbia University နှင့် MIT စသည့်တို့ ပါဝင်ကြသည်။ ဖြစ်နိုင်ချေ ရှိသည်မှာ ယင်းတို့မှလွဲ၍ ကျန်သူများဝင်ရောက်သုံးစွဲနိုင်ခြင်းမရှိပါ။

၅၅။ Class B သည် အရွယ်အစားအလယ်အလတ်ရှိသော Network များအတွက် အသုံးပြု သည်။ Class B တွင် IP Address ၏ ပထမ octet ၂ ခုသည် Network ဖြစ်ပြီး ကျန် octets ၂ ခုသည် hosts ဖြစ်သည်။ ထို့ကြောင့် Networks 16002 ခုရှိပြီး Network

တစ်ခုလျှင် hosts ပေါင်း 65025 ခုသုံးစွဲနိုင်သည်။ Class B Networks များတွင် Microsoft နှင့် Exxon တို့ ပါဝင်သည်။ယင်းတို့မှလွဲ၍ ကျန်သူများဝင်ရောက် သုံးစွဲနိုင်ခြင်း မရှိပါ။

၃၆။ Class C သည် သေးငယ်သော Network များတည်ဆောက်ရာတွင်သုံးသည်။ Class C တွင် IP Address ၏ ပထမ octets ၃ ခုသည် Network ဖြစ်ပြီး ကျန် octet ၁ ခုသည် hosts ဖြစ်သည်။ ထို့ကြောင့် Networks ပေါင်း 1,999,996 ခုရှိပြီး Network တစ်ခုလျှင် hosts အများဆုံး 254 ခုသုံးစွဲနိုင်ပါသည်။ Class C Networks တွင် ဝင်ရောက်သုံးစွဲနိုင်သည်။

၃၇။ Class D သည် special multicasting address ဖြစ်ပြီး networks အဖြစ် အသုံးမပြုနိုင်ပေ။ ဖြစ်နိုင်ချေ address မှာ 268 million ဖြစ်သည်။

၃၈။ Class E သည် experiments များအတွက်အရံအဖြစ်ထားရှိသည်။ လက်ရှိအသုံးပြုနေတဲ့ IP address များသည် IP version 4 ဖြစ်သည်။ အနာဂါတ်တွင် IP version (6) ကိုသုံးစွဲနိုင်ရန် ကြိုးပမ်းလျက်ရှိပါသည်။ IP version (6) သည် 2^{128} ဖြစ်သည့်အတွက် ကမ္ဘာကြီး၏ ၁ စတုရန်းမီတာ အကျယ်တွင် IP address (1) billion ချပေးနိုင်မည် ဖြစ်သည်။

InterNIC မှသတ်မှတ်ချက်

<table>
<tr><td>Class</td><td colspan="9">Bit Allocation</td></tr>
<tr><td>A</td><td>0</td><td colspan="2">Network</td><td colspan="6">Host</td></tr>
<tr><td colspan="10">7 bits 24 bits</td></tr>
<tr><td>B</td><td>1</td><td>0</td><td colspan="3">Network</td><td colspan="4">Host</td></tr>
<tr><td colspan="10">14 bits 16 bits</td></tr>
<tr><td>C</td><td>1</td><td>1</td><td>0</td><td colspan="5">Network</td><td>Host</td></tr>
<tr><td colspan="10">21 bits 8 bits</td></tr>
<tr><td>D</td><td>1</td><td>1</td><td>1</td><td>0</td><td colspan="5">Multicasting Address</td></tr>
<tr><td colspan="10">28 bits</td></tr>
<tr><td>E</td><td>1</td><td>1</td><td>1</td><td>1</td><td colspan="5">Experimental</td></tr>
<tr><td colspan="10">28 bits</td></tr>
<tr><td>Loopback</td><td>0</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>Unused</td></tr>
</table>

Subnetting

၅၉။ Network တစ်ခုအတွင်း သေးငယ်သောအစုအဖွဲ့များအဖြစ် Network အစိတ်အပိုင်းငယ်များ ထပ်မံခွဲခြင်းဖြစ်သည်။ ယင်းကဲ့သို့ဆောင်ရွက်ခြင်းအားဖြင့် လုံခြုံမှုကောင်းမွန်ခြင်း၊ IP address များပြုပြင်ထိန်းသိမ်းထားရှိနိုင်ခြင်း၊ မတူညီသော Physical media များ သုံးစွဲနိုင်ခြင်း၊ Network Traffic ထိန်းချုပ်ခြင်း၊ အနည်းဆုံးသုံးစွဲနိုင်သဖြင့် performance အများဆုံး ရရှိစေခြင်း၊ သီးသန့် Network ဖြစ်စေခြင်းများ ဆောင်ရွက်နိုင်သည်။

၆၀။ IP address ကဲ့သို့ပင် subnet mask သည် 4 octets address ပင်ဖြစ်သည်။ Octets များသည် Network နှင့် host/node ကိုဖော်ပြနိုင်သည်။ default subnet mask များမှာ အောက်ပါအတိုင်း ဖြစ်သည်။ Off bits များမှာ host address များဖြစ်သည်။

Class	IP Address	Default SubNet mask	Subnet Mask Bit Pattern
A	N . n . n . n	255 . 0 . 0 . 0	11111111 00000000 00000000 00000000
B	N . N . n . n	255 . 255 . 0 . 0	11111111 11111111 00000000 00000000
C	N . N . N . n	255 . 255 . 255 . 0	11111111 11111111 11111111 00000000

၆၁။ IP block တစ်ခုမှ subnet ခွဲခြားလိုပါက host address bits အား network address bits တွင် သုံးလိုသော subnetwork ပေါ်မူတည်၍ ထပ်ပေါင်းထည့်ခြင်းဖြစ်သည်။ တစ်နည်းအားဖြင့် network address နှင့် host address ခွဲခြားထားသည့်နေရာမှ ညာဘက်သို့ bits ထပ်ပေါင်းခြင်းဖြင့် network များတိုးလာမည်ဖြစ်သည်။ သို့သော် host အရေအတွက် လျော့ကျသွားမည်ဖြစ်သည်။

၆၂။ မည်သည့်အချိန်တွင် default subnet များကို အသုံးမပြုပဲ subnet mask တန်ဖိုးပြောင်းလဲ၍အသုံးပြုရသည်ကို Class C ဆက်လက်ဖော်ပြပါမည်။ မိမိတွင် Internet မှ qualify ဖြစ်သည့် network address တစ်ခုသာရှိပြီး မိမိက subnet လေးခု လိုချင်သည်ဆိုလျှင် subnet mask ကို ပြောင်းလဲအသုံးပြုရပါသည်။ ဥပမာ- 192.168.0.X ဆိုသော IP block တစ်ခုကို မိမိအတွက် ပေးခဲ့လျှင် 255.255.255.0 ဟူသော default subnet mask တစ်ခုတည်းသာရှိပြီး မိမိတွင် Network address တစ်ခုသာရှိမည်ဖြစ်သည်။

255	255	255	0
11111111	11111111	11111111	00000000
N	N	N	n

၆၃။ node အပိုင်းက "0" များကို Network အပိုင်းဖြစ်စေရန် လုပ်ဆောင်လျှင် network များ ပိုထွက်လာမည် ဖြစ်သည်။ ဥပမာ- node အပိုင်းမှ 2-bit ယူလိုက်မည်ဆိုရင် ယခင် network အပိုင်းက "0"-bit ရှိနေရာမှ 2-bit ရှိလာမည်ဖြစ်သည်။ သို့သော် node အပိုင်းတွင်မူလ 8-bit ရှိနေရာမှ 2-bit ယူလိုက်သည့်အတွက် 6-bit သာကျန်တော့မည် ဖြစ်သည်။

11111111.11111111.11111111.<u>11</u>0000

N N N n

၆၄။ node အပိုင်းတွင် 00, 01, 10, 11 ဆိုသော address (၄)ခု ပေါ်ထွက်လာမည်ဖြစ်သည်။ ဒီ network (၄)ခုအတွက် node အပိုင်းမှာ 00000000 ကနေ 111111 သို့ ပြောင်းလဲသွားမည် ဖြစ်သည်။ ဒီနေရာတွင် node အပိုင်းသည် "0" တွေချည်း ဖြစ်၍မရသလို၊ "1" တွေချည်းလည်းဖြစ်၍မရဆိုသော theory ကို မေ့ထား၍မရပေ။ Theory အရ 2^6=64 ပဲရှိသည့်အတွက် node အပိုင်းတွင် 1 to 62 သာသုံးလို့ရမည် ဖြစ်သည်။ Subnet mask သည် 255.255.255.192 သို့ပြောင်းသွားမည်ဖြစ်သည်။

Network Number	Router Address	Broadcast Address
00 -- x.y.z.0	x.y.z.1	x.y.z.63
01 -- x.y.z.64	x.y.z.65	x.y.z.127
10 -- x.y.z.128	x.y.z.129	x.y.z.191
11 -- x.y.z.192	x.y.z.193	x.y.z.255

၆၅။ Class C network တွင် subnets ၈ ခုခွဲပါက subnet mask မှာ 255.255. 255.224 ဖြစ်ပြီး subnet address များမှာအောက်ပါအတိုင်းဖြစ်သည်။

Network Number	Router Address	Broadcast Address
000 -- x.y.z.0	x.y.z.1	x.y.z.31
001 -- x.y.z.32	x.y.z.33	x.y.z.63
010 -- x.y.z.64	x.y.z.65	x.y.z.95
011 -- x.y.z.96	x.y.z.97	x.y.z.127
100 -- x.y.z.128	x.y.z.129	x.y.z.159

101 – x.y.z.160	x.y.z.161	x.y.z.191
110 – x.y.z.192	x.y.z.193	x.y.z..223
111 – x.y.z.224	x.y.z.225	x.y.z.255

Classless Internetwork Domain Routing(CIDR)

၆၆။ InterNIC မှသတ်မှတ်ထားသော Class A ၊ B ၊ C ၏ address ဖြင့်ဖော်ပြခြင်း မပြုဘဲ " Slash x " ဖြင့်ဖော်ပြသော method ကို CIDR (cider) ဟုခေါ်ပါသည်။ X သည် network address bits ကိုဖော်ပြခြင်းဖြစ်သည်။

InterNIC Network type (CIDR)	Subnet Mask	Approximate Number of IP Address
Slash 8	255.0.0.0	16,000,000
Slash 12	255.240.0.0	1,000,000
Slash 16	255.255.0.0	65,536
Slash 20	255.255.240.0	4,096
Slash 21	255.255.248.0	2,048
Slash 22	255.255.252.0	1,024
Slash 23	255.255.254.0	512
Slash 24	255.255.255.0	256
Slash 25	255.255.255.128	128
Slash 26	255.255.255.192	64
Slash 27	255.255.255.224	32
Slash 28	255.255.255.240	16
Slash 29	255.255.255.248	8
Slash 30	255.255.255.254	4

Anding Method

၆၇။ 192.168.0.5 ဟူသော address သည်မည်သည့် network တွင် ပါဝင်သည်ဆိုခြင်းကို သိလိုလျှင် network address bits နှင့် subnet mask bits ပေါင်းခြင်းဖြင့်သိရှိနိုင်ပေသည်။

```
   192    .    168    .     0     .     5
11000000.10101000.00000000.00000101
   255    .    255    .    255    .    192
11111111.11111111.11111111.11000000
-----------------------------------------------
11000000.10101000.00000000.00000000
```

ထို့ကြောင့် 192.168.0.0 (00) network ထဲတွင် ရှိသည်ကို သိနိုင်ပေသည်။

TCP/IP and the OSI Model

၆၈။ ကွန်ပျူတာနှင့် ကွန်ပျူတာ ဆက်သွယ်မှုတွင် OSI Model တွင် layer (၇)ခုဖြင့် ခွဲခြား ဆက်သွယ်ပြီး TCP/IP သည် layer (၅)ခုသာ အသုံးပြုသည်။

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>Application Layer - 7</td><td rowspan="3">Application Layer - 5</td></tr>
<tr><td>Presentation Layer - 6</td></tr>
<tr><td>Session Layer - 5</td></tr>
<tr><td>Transport Layer -4</td><td>Transport Layer -4</td></tr>
<tr><td>Network Layer - 3</td><td>Internet Layer - 3</td></tr>
<tr><td>Data Link Layer - 2</td><td>Network Layer - 2</td></tr>
<tr><td>Physical Layer - 1</td><td>Physical Layer - 1</td></tr>
</table>

၆၉။ OSI Model တွင် higher layer မှလေ့လာလျှင် Application layer ၌ data base ၊ e-mail ၊ terminal-emulation programs များပါဝင်ပါသည်။ Presentation layer တွင် data များကို formatted ၊ presented ၊ converted နှင့် encoded များပြုလုပ်ပါသည်။ Session layer တွင် ဆက်သွယ်မှု နှင့် ပြုပြင်ထိန်းသိမ်းခြင်းများကို ပေါင်းစပ်ညှိနှိုင်း ပေးပါသည်။ Performing security ၊ logging နှင့် administrative functions များလိုအပ် ပါသည်။ Transport layer သည် message များအလိုက်ပို့လွှတ်နေသော protocols များ၏ အမှားအယွင်းများကို စစ်ဆေးပေးပါသည်။ Network layer သည် data-routing protocol များအလိုက် သတင်းအချက်အလက်များအား သက်ဆိုင်ရာ destination node သို့ မှန်ကန်

စွာရောက်ရှိရေးဆောင်ရွက်ပေးသည်။ Data Link layer သည် node တစ်ခုမှ တစ်ခုသို့ data များစီးဆင်းမှု နှင့် တစ်ပြိုင်နက် data blocks များ မှန်ကန်စေရေး ဆောင်ရွက်ပေးသည်။ Physical layer သည် ဆက်သွယ်ရေးဆိုင်ရာ စက်မှုပိုင်းပစ္စည်းများဖြစ်သော transmission medium နှင့် Interface hardware များကို ဖော်ပြခြင်းဖြစ်သည်။

၇၀။ TCP/IP ၏ layer (၅)ခုတွင် အမြင့်ဆုံး layer မှာလည်း Application Layer ပင်ဖြစ်ပြီး FTP ၊ Telnet စသော အသုံးချမှုများကို အပြန်အလှန်ဆောင်ရွက်မှုပေးပါသည်။ Transport layer တွင် ပို့လွှတ်နေသော data packet များအတွင်းသို့ TCP နှင့် အခြားသော protocol များကို ပေါင်းထည့်ခြင်းဆောင်ရွက်ပါသည်။ Internet layer တွင် packet များအတွင်းသို့ IP information ပေါင်းထည့်ခြင်းဆောင်ရွက်ပါသည်။ Network Interface layer သည် Physical layer နှင့် interface လုပ်ပေးပါသည်။ Physical layer သည် ဆက်သွယ်ရေးဆိုင်ရာ စက်မှုပိုင်းပစ္စည်းများဖြစ်သော transmission medium နှင့် Interface hardware များကို ရည်ညွှန်းခြင်းပင်ဖြစ်သည်။

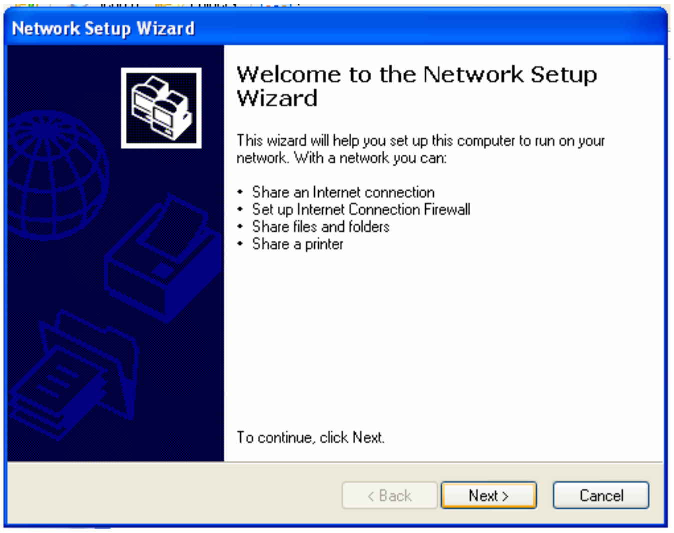
Configuring TCP/IP on Windows Work Groups

၇၁။ ကွန်ပျူတာများ၊ ပရင်တာများကို Network ချိတ်ဆက်ပြီး Data များအား မျှဝေသုံးစွဲ (Sharing) ဆောင်ရွက်နိုင်ရန် Network Setup ဆောင်ရွက်ပြီးမှ TCP/IP အား Installation ပြုလုပ်ရသည်။ ယင်းသို့ဆောင်ရွက်နိုင်ရန် Operating System ကို Windows တစ်မျိုးမျိုး နှင့် NIC card တပ်ဆင်ပြီးဖြစ်ရမည်။ Windows 98 Client / Windows NT Workstation Client ၊ Windows XP Client များတွင် Network Setup ဆောင်ရွက်ရာ၌ အနည်းငယ် ကွဲပြားခြားနားပါသည်။ Windows XP Client အား အောက်ပါအဆင့်များဖြင့် တည်ဆောက်ရသည် -

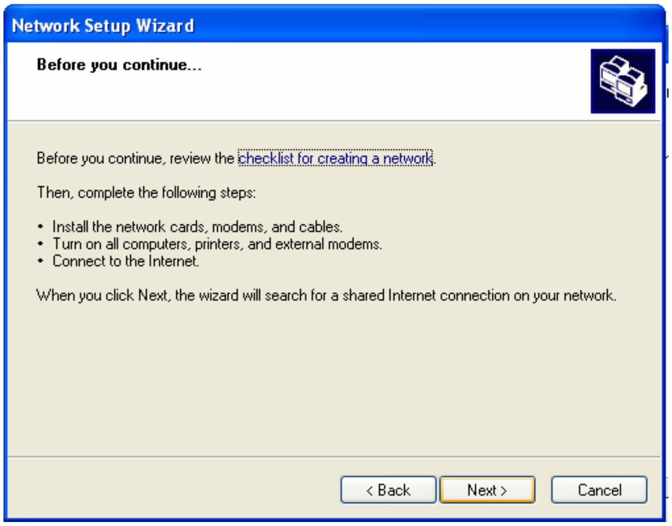
Start ⇨ Control Panel ⇨ Network and Internet connection ⇨ Network connection အားအဆင့်အလိုက်သွားရမည်။ ယင်းနောက်-

Network connection dialog box ၏ Network Tasks(Left pane) တွင်ရှိ Set up a home or small office အား Click လုပ်ပြီး Network setup wizard သို့ဝင်ရမည်။

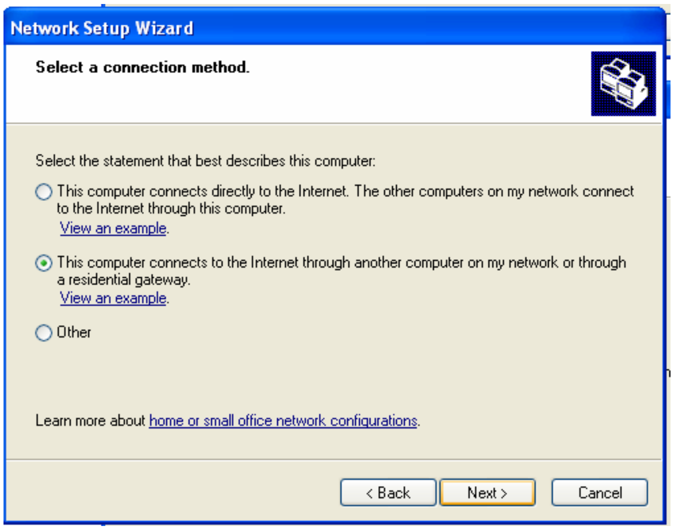
ယင်းနောက် Next button အား click လုပ်ပြီး နောက်တစ်ဆင့်သွားရမည်။



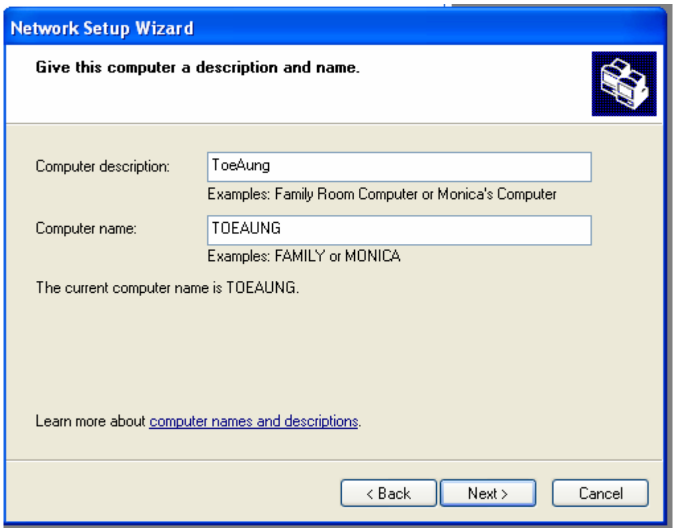
NIC card ၊ modem ၊ printers ၊ အခြားသောကွန်ပျူတာများနှင့် တပ်ဆင်ပြီး ဖြစ်ပါက Next button အား click လုပ်ပြီး နောက်တစ်ဆင့်သွားရမည်။



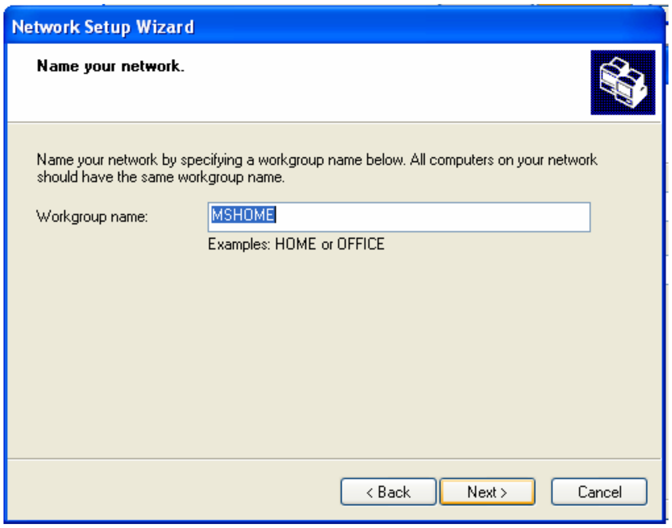
မိမိဆက်သွယ် လိုသောနည်းလမ်းအား ရွေးချယ်ပြီး Next button အား click လုပ်ပြီး နောက်တစ်ဆင့်သို့ ထပ်မံသွားရမည်။



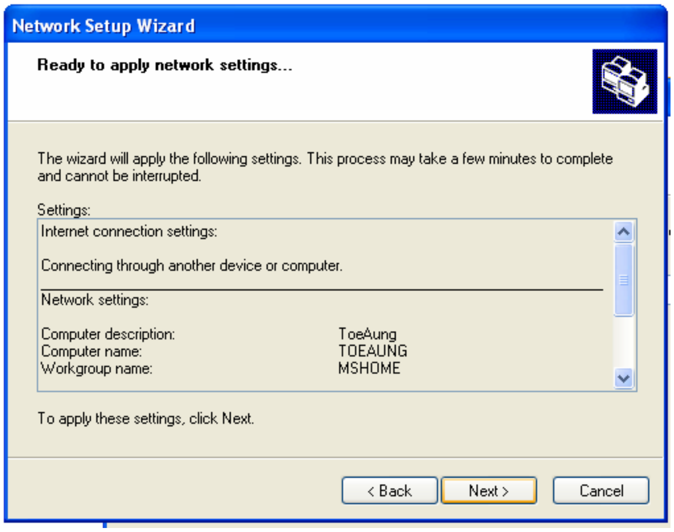
ယင်းနောက် ကွန်ပျူတာ၏ description နှင့် name များပေးရသည်။ Network ချိတ်ဆက်ပါက အမည် နှင့် အမှတ်အသားများအား ကွန်ပျူတာ တစ်လုံးစီတွင်သီးသန့် ဖြစ်ရမည်။ မတူညီရပေ။



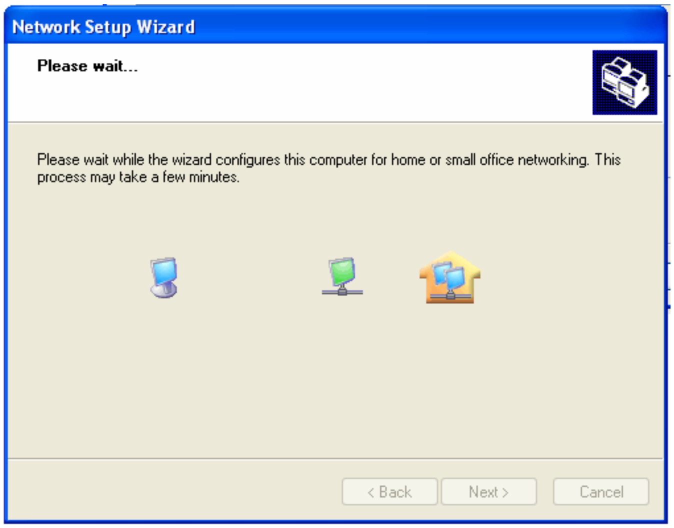
ဤအဆင့်တွင် Workgroup ၏ အမည်ပေးရသည်။ Default name သည် MSHOME ဖြစ်ပါသည်။



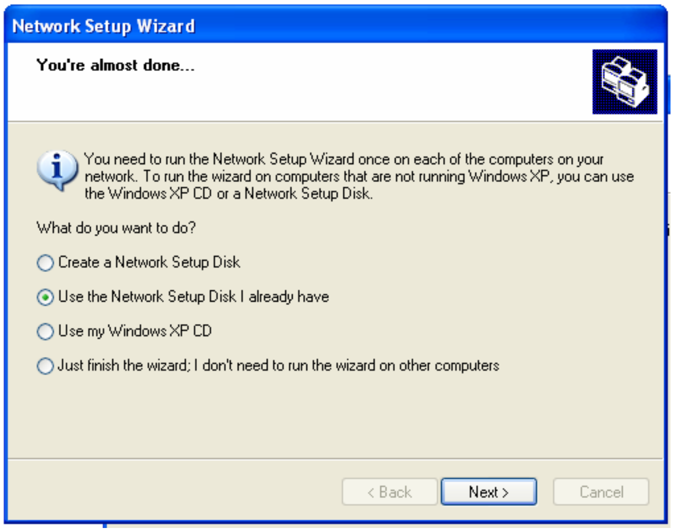
မိမိဆောင်ရွက်ခဲ့သော Network setting အား ပြန်လည်စစ်ဆေးနိုင်ပြီး ပြင်ဆင်လိုပါက back ကိုရင်း၊ အတည်ဖြစ်ပါက next ကိုရင်းရွေးချယ်ရမည်။



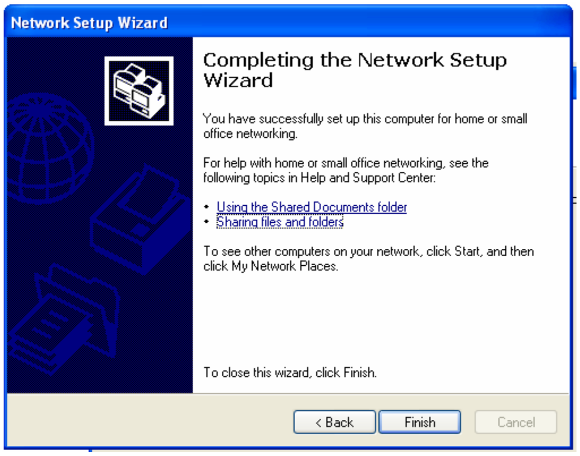
Network setting များ ဆောင်ရွက်နေခြင်းဖြစ်ပြီး အချိန်အနည်းငယ်စောင့်ဆိုင်းရသည်။



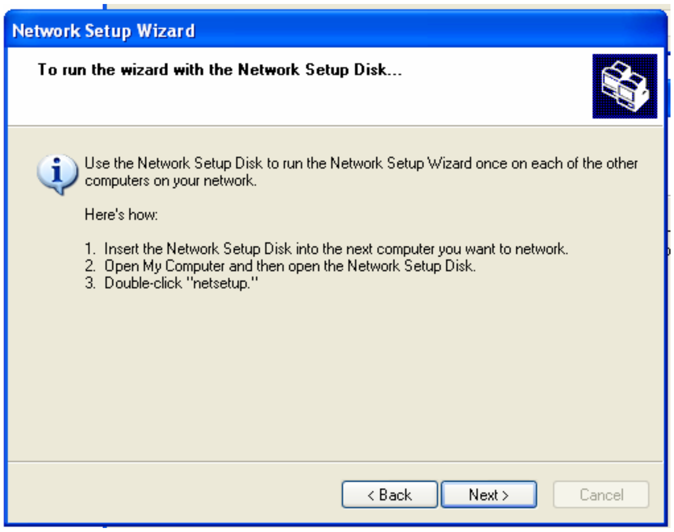
ထို့နောက် Network Setup Disk ဆောင်ရွက်လိုလျှင် သို့မဟုတ် ဆောင်ရွက်ပြီးဖြစ်လျှင် သို့မဟုတ် CD အားအသုံးပြုလျှင် သို့မဟုတ် အခြားကွန်ပျူတာများတွင်အသုံးပြုရန် မလိုအပ်လျှင် စသည်များမှ လိုအပ်သည်ကိုရွေးချယ်ပြီး Next button အား click လုပ်ရမည်။



Network Setup Disk ဆောင်ရွက်ထားပါက အခြားကွန်ပျူတာတွင် ၎င်း disk ထည့်သွင်းပြီး netsetup ဆောင်ရွက်နိုင်သည်။



၇၂။ ယင်းကဲ့သို့ဆောင်ရွက်ပြီးပါက Workgroup အတွင်း Shared ပေးထားသော files ၊ folder ၊ printers များအား သုံးစွဲ၍ရသကဲ့သို့ မိမိမှပေးထားသော sharing files နှင့် folder များအား အခြားသူများမှ ဝင်ရောက်သုံးစွဲ၍ရမည်ဖြစ်သည်။ Network အတွင်းရှိ အခြားကွန်ပျူတာများအား ဝင်ရောက်သုံးစွဲလိုပါက **Start ➩ My Network Places** တွင် တွေ့မြင်ရမည်ဖြစ်သည်။ ယင်းနောက် TCP/IP အား install ပြုလုပ်ရသည်။

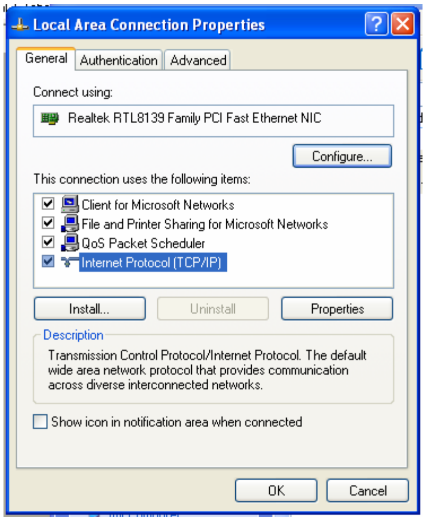


TCP/IP Properties

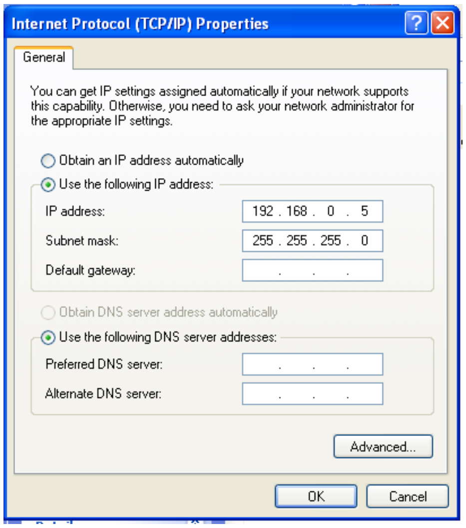
၇၃။ Internet protocol အသုံးပြုပြီး Network အား တည်ဆောက်လျှင် အောက်ပါ အဆင့်များ အတိုင်း ဆောင်ရွက်ရသည်-

Start ➪ Control Panel ➪ Network and Internet connection ➪ Network connection အားအဆင့်အလိုက်သွားရမည်။ ယင်းနောက်-

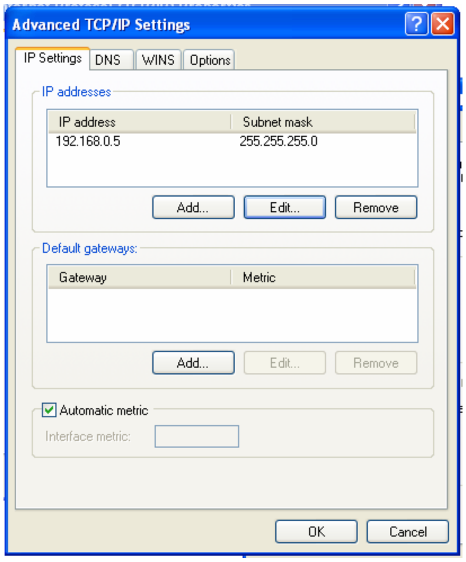
Network connection dialog box တွင်ရှိ Local Area Connection အားရွေးချယ်ပြီး Right Click နှိပ်ပါက Pop-Up menu တွင်ရှိ Properties ထပ်မံရွေးချယ်ရမည်။



ထို့နောက် General Tab တွင် မိမိချိတ်ဆက်ထားသော NIC အမျိုးအစားအား တွေ့မြင်ရပြီး အဆက်အသွယ်အတွင်း သုံးစွဲလိုသည့် Client ၊ Files နှင့် Printers Sharing များအား ရွေးချယ်ရမည်။ Internet Protocol (TCP/IP) အား Select လုပ်ပြီး properties အား click လုပ်ရမည်။



Use the following IP address option အား check လုပ်ပြီး network တွင် သတ်မှတ်ထားသော IP address ၊ Subnet mask နှင့် Gateway သုံးစွဲထားပါက Default Gateway များအား ထည့်သွင်းရမည်။ DNS server သုံးစွဲထားပါက Use the following DNS server address option အား check လုပ်ပြီး Preferred DNS server address ထည့်သွင်းရမည်။ DNS server အား နှစ်ခုသုံးစွဲထားပါက Alternate DNS server address ကိုပါထည့်သွင်းရမည်။



၇၄။ Advanced Button အား click လုပ်ပြီး IP setting Tab တွင် IP ၊ Subnet mask ၊ Gateway setting များအား ထပ်မံထည့်သွင်းခြင်း၊ ပြင်ဆင်ခြင်း ၊ ဖယ်ရှားခြင်းများ ဆောင်ရွက်နိုင်ပါသည်။ DNS ၊ WINS ၊ Option Tab များတွင်လည်း သက်ဆိုင်သည်များအား ထပ်မံထည့်သွင်းခြင်း၊ ပြင်ဆင်ခြင်း၊ ဖယ်ရှားခြင်း၊ရွေးချယ်ခြင်းများအား ဆောင်ရွက်နိုင်ပါသည်။ မိမိအနေဖြင့်ဆောင်ရွက်နိုင်သောအဆင့်ဖြစ်ပြီး အသေးစိတ် သိရှိနားလည်နိုင်ရန် TCP/IP Fundamentals ကိုလေ့လာရမည်ဖြစ်သည်။

TCP/IP Utility

၇၅။ IP များကို အသုံးပြုချိတ်ဆက်နေသော ကွန်ယက်တစ်ခုအတွင်းရှိ TCP/IP များ၏ connectivity ကို စမ်းသပ်ရန်အတွက် utilities များစွာရှိသည့်အနက် အသုံးများပြီး လက်တွေ့နယ်ပယ်တွင် အသုံးဝင်သော utility commands များမှ အချို့နှင့် အသုံးပြုပုံတို့အား အောက်တွင် ဖော်ပြထားပါသည်။ ၎င်း commands များသည် Windows

OS Platform အသုံးပြုသော Wondows workstation များတွင် built in ပါဝင်သော function များဖြစ်သည်။

- **ARP**
- **netstat**
- **nbstat**
- **FTP**
- **Ping**
- **ipconfig/winipcfg**
- **tracert**
- **Telnet**

The `ipconfig` Utility

၇၆။ `ipconfig` Utility ၏ အဓိက function မှာ မိမိ NIC ၏ address နှင့် Default Gateway, WINS စသည်တို့ကို ဖော်ပြခြင်းပင် ဖြစ်သည်။

```
C:\>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.168.0.6
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
```

၇၇။ `ipconfig` တွင်လည်း switch များရှိပြီး ၎င်းတို့ကို **`ipconfig /?`** command သုံး၍ ကြည့်ရှုနိုင်မည် ဖြစ်သည်။

```
     USAGE:
          ipconfig [/? | /all | /renew [adapter] | /release
                   [adapter] |/flushdns | /displaydns |
                   /registerdns |/showclassid adapter |
                   /setclassid adapter [classid] ]
```

The `Ping` Utility

၇၈။ `ping` utility သည် TCP/IP ၏ အဓိက အခြေခံအကြဆုံး command line utility တစ်ခု ဖြစ်သည်။ `ping` ကို destination နှင့် host အကြား အပြန်အလှန် ဆက်သွယ်မှု

ရှိမရှိ စစ်ဆေးရာတွင်သုံးသည်။ ၎င်း command line ၏ syntax မှာ အောက်ပါအတိုင်း ဖြစ်သည်။

၇၉။ **ping <hostname or IP address>** `ping` သည် ICMP protocol ကို အသုံးပြုသည်။ မိမိက စက်တစ်လုံးအား ping ၍ request လုပ်မည် ဆိုပါက ICMP protocol က response ပြန်လည် ပေးမည် ဖြစ်သည်။

ဥပမာ-

```
C:\>ping 192.168.0.5

Pinging 192.168.0.5 with 32 bytes of data:

Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128
Reply from 192.168.0.5: bytes=32 time<1ms TTL=128


Ping statistics for 192.168.0.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

၈၀။ အထက်တွင် 192.168.0.5 ဆိုသော destination စက်ကို ping ရာတွင် IP connection ရှိနေကြောင်း reply ပြန်လာသည်ကို တွေ့ရှိရမည် ဖြစ်သည်။ `ping` command တွင်လည်း အခြား utility များကဲ့သို့ switch များရှိသည်။ ထို switch များ၏ အသုံးပြုပုံကို သိရှိလိုပါက command prompt တွင် အောက်ပါအတိုင်း ရိုက်နှိပ်ကြည့်ပါ သိရှိနိုင်မည် ဖြစ်သည်။

```
ping -?
```

၈၁။ ထိုသို့ရိုက်နှိပ်လိုက်ပါက အောက်ပါအတိုင်း switch အသုံးပြုပုံ description ကို မြင်တွေ့နိုင်သည်။

```
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;
                   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.
```

၈၂။ ping လုပ်ရာတွင် အထူးသတိပြုရမည် မှာ destination host ၏ address နေရာတွင် 127.0.0.1 ကို ping မည်ဆိုပါက ၎င်းသည် local loop back ဖြစ်သဖြင့် မိမိစက်ကို ပြန်၍ ping ခြင်းနှင့် အတူတူပင်ဖြစ်သည်။ ထို့ကြောင့် မိမိစက်ရှိ NIC ကောင်း၊မကောင်း စစ်ဆေးရာတွင် သုံးသည်။

Using `netstat`

၈၃။ netstat သည် TCP/IP connection ကို စစ်ဆေးကြည့်ရှုရာတွင် အလွန်အသုံးဝင်သော command line utility တစ်ခုဖြစ်သည်။ အဘယ်ကြောင့်ဆိုသော် netstat သည် IP connection ကို check လုပ်ရာတွင် inbound နှင့် outbound နှစ်မျိုးစလုံးမှ မိမိစက်နှင့် ချိတ်ဆက်နေသော IP connection များကို ကြည့်ရှုနိုင်သောကြောင့် ဖြစ်သည်။ ထို့အပြင် netstat ၏ အားသာချက်တစ်ခုမှာ data packet တို့၏ sent and received status ကိုပါကြည့်ရှုနိုင်ပြီး loss data packet ၏ ပမာဏနှင့် error များကိုပါ ဖော်ပြပေးထားသည်။

၈၄။ netstat utility ကို မည်သည့် option မှ မပါဝင်ပဲ netstat ချည်းသက်သက် ရိုက်သွင်း အသုံးပြုမည် ဆိုပါက မိမိစက်နှင့် connection active ဖြစ်နေသော လာရောက်

ချိတ်ဆက်နေသည့် စက်များ၏ port နှင့် IP address များကို တွေ့မြင်နိုင်မည် ဖြစ်ပြီး အောက်ပါအတိုင်း တွေ့မြင်နိုင်မည်ဖြစ်သည်။

Active Connections

Proto	Local Address	Foreign Address	State
TCP	bigideaice:1035	203.81.65.23:5226	ESTABLISHED
TCP	bigideaice:5226	203.81.65.23:1035	ESTABLISHED
TCP	bigideaice:1028	203.81.65.27:80	ESTABLISHED
TCP	bigideaice:1029	203.81.65.23:80	ESTABLISHED

၈၅။ netstat ကို မည်သည့် option မှ မပါဝင်ပဲ Command Prompt တွင် ရိုက်သွင်းလိုက်သောအခါတွင် အထက်ပါအတိုင်း မြင်တွေ့နိုင်ပြီး Proto Column list တွင် ချိတ်ဆက်အသုံးပြုနေသော Protocol type ကို ဖော်ပြထားပါသည်။ ထို့နည်းတူ Local Address column သည် မိမိစက်၏ IP address နှင့် လာရောက်ချိတ်ဆက်ခံသော Port number ကို ဖော်ပြထားသည်။ Foreign Address တွင် လာရောက်ချိတ်ဆက် အသုံးပြုသော စက်များ၏ address နှင့် အချိတ်ဆက်ခံရန် access ပေးသော port တို့ကို ဖော်ပြထားပါသည်။ State column သည် connection တစ်ခုစီ၏ status ကို ဖော်ပြသည်။

၈၆။ netstat utility ၏ out put ကို ၎င်း utility တွင် ပါဝင်သော Option/Switch များကို အသုံးပြု၍ ပြောင်းလဲ ကြည့်ရှုနိုင်သည်။ ၎င်း switch များမှာ အောက်ပါအတိုင်း ဖြစ်သည်။

- **-a**
- **-e**
- **-r**
- **-s**
- **-n**
- **-p**

၈၇။ အထက်ပါ switch များကို အသုံးပြုရာတွင် netstat command ကို command prompt တွင် ရိုက်သွင်းပြီး space တစ်ခုခြားကာ မိမိအသုံးပြုလိုသော switch ကို ရိုက်သွင်းရမည်။

ဥပမာ-

```
netstat -a
```

The –a Switch

၈၈။ -a switch ကို အသုံးပြုလျှင် nestat command သည် TCP/IP connection အားလုံးနှင့် UDP(user Datagram Protocol) connection အားလုံးကို ဖော်ပြသည်။

ဥပမာ-

```
C:\>netstat -a

Active Connections

Proto     Local Address            Foreign Address    State
TCP       bigideaice:epmap         0.0.0.0:0          LISTENING
TCP       bigideaice:microsoft-ds  0.0.0.0:0          LISTENING
TCP       bigideaice:1025          0.0.0.0:0          LISTENING
TCP       bigideaice:1035          0.0.0.0:0          LISTENING
UDP       bigideaice:epmap         *:*
UDP       bigideaice:microsoft-ds  *:*
UDP       bigideaice:isakmp        *:*
UDP       bigideaice:1027          *:*
UDP       bigideaice:1029          *:*
UDP       bigideaice:ntp           *:*
UDP       bigideaice:1900          *:*
```

၈၉။ UDP များသည် Windows Workstation များအတွင်း NetBIOS name များကို broadcasting လုပ်ရန်အတွက် အသုံးပြုနေခြင်းဖြစ်သည်။ broadcast လုပ်သည်ဟု ပြောနိုင်ရခြင်းမှာ Foreign Address (or) Destination address ၏ list တွင် *.* ဖြစ်နေသောကြောင့် ဖြစ်သည်။ *.* ဆိုသည်မှာ any address, any port ဟု ဆိုလိုသည်။ တနည်းအားဖြင့် ဆိုရသော် ပွင့်ပြီး အားလပ်နေသော port များ ဖြစ်သည်။ ၎င်း port များကို အသုံးပြု မှီခို၍ မလိုလားအပ်သော အနှောက်အယှက်များဖြင့် မိမိစက်ကို ဒုက္ခပေးနိုင်သည်။ ထို့ပြင် UDP သည် connection တစ်ခု မဟုတ်ပဲ oriented protocol သာ ဖြစ်သည်။ ထို့ကြောင့် connection stat တွင် ဘာမှ ဖော်ပြထားခြင်း မရှိပေ။

The -e Switch

၉၀။ -e switch သည် မိမိစက်၏ NIC မှ data packet မည်မျှ transmit လုပ်ပြီး၊ မည်မျှ received လုပ်နေသည်ကို ကြည့်ရှုနိုင်သကဲ့သို့ error များ၊ packets summary များကို သိနိုင်သည်။

ဥပမာ-

```
C:\>netstat -e
Interface Statistics

                              Received            Sent

Bytes                            25390           25390
Unicast packets                    118             118
Non-unicast packets                  0               0
Discards                             0               0
Errors                               0               0
Unknown protocols                    0
```

The -r Switch

၉၁။ ၎င်း switch သည် Workstation အတွင် route လုပ်နေသော routing table ကို ဖော်ပြပေးနိုင်သည်။ အကယ်၍ မိမိ computer သည် NIC တစ်ခုထက်ပို အသုံးပြုထားသော proxy သို့မဟုတ် Gateway တစ်ခု ဖြစ်နေပါက ၎င်း command သည် များစွာ အရေးပါသည်။ ထိုသို့ မဟုတ်ပဲ သာမန် stand alone PC သို့မဟုတ် client တစ်ခု ဖြစ်ခဲ့မည် ဆိုပါက ၎င်း utility သည် route လုပ်နေမှုကို ဖော်ပြမည် မဟုတ်ပေ။

ဥပမာ-

```
C:\>netstat -r
```

The -s Switch

၉၂။ **-s** switch ကို အသုံးပြုခြင်းဖြင့် များစွာသော TCP, UDP, IP, ICMP(Internet Control Message Protocol) တို့၏ status ကို ဖော်ပြမည် ဖြစ်သည်။ အောက်တွင် **-s** ကို အသုံးပြုခြင်ဖြင့် မြင်တွေ့နိုင်မည့် output ဥပမာ အချို့ကို ဖော်ပြလိုက်ပါသည်။

```
C:\>netstat -s
IPv4 Statistics
```

```
  Packets Received                   = 55
  Received Header Errors             = 0
  Received Address Errors            = 3
  Datagrams Forwarded                = 0
  Unknown Protocols Received         = 0
  Received Packets Discarded         = 0
  Received Packets Delivered         = 55
  Output Requests                    = 55
  Routing Discards                   = 0
  Discarded Output Packets           = 0
  Output Packet No Route             = 0
  Reassembly Required                = 0
  Reassembly Successful              = 0
  Reassembly Failures                = 0
  Datagrams Successfully Fragmented  = 0
  Datagrams Failing Fragmentation    = 0
  Fragments Created                  = 0

ICMPv4 Statistics

                            Received    Sent
  Messages                  0           0
  Errors                    0           0
  Destination Unreachable   0           0
  Time Exceeded             0           0
  Parameter Problems        0           0
  Source Quenches           0           0
  Redirects                 0           0
  Echos                     0           0
  Echo Replies              0           0
  Timestamps                0           0
  Timestamp Replies         0           0
  Address Masks             0           0
  Address Mask Replies      0           0

TCP Statistics for IPv4

  Active Opens                        = 3
  Passive Opens                       = 1
```

```
  Failed Connection Attempts          = 2
  Reset Connections                   = 0
  Current Connections                 = 2
  Segments Received                   = 51
  Segments Sent                       = 47
  Segments Retransmitted              = 4

UDP Statistics for IPv4

  Datagrams Received    = 4
  No Ports              = 0
  Receive Errors        = 0
  Datagrams Sent        = 4
```

The –n Switch

၉၃။ -n switch ကို အခြား switch များနှင့် ရောနှော အသုံးပြုမည်ဆိုပါက Network address များနေရာတွင် number အနေဖြင့် ဖော်ပြမည် ဖြစ်သည်။

ဥပမာ-

```
c:\>netstat –a –n
```

The –p Switch

၉၄။ -s ကို အသုံးပြုပြီး netstat ကို ကြည့်ရှုသည့်အခါတွင် TCP, UDP, ICMP, IP စသည်ဖြင့် များစွာသော အသုံးပြုနေသည့် protocol များ၏ status ကို ဖော်ပြမည်ဖြစ်သည်။ အကယ်၍ ICMP တစ်ခုတည်းကိုသာ ကြည့်လိုသည်ဆိုပါက -p နှင့် တွဲပြီး သုံးရမည်ဖြစ်သည်။ -p သည် switch တစ်ခုခုနှင့် တွဲသုံးရသော command line utility ဖြစ်သည်။

ဥပမာ-

```
C:\>netstat -s -p ICMP
ICMPv4 Statistics
                            Received    Sent
 Messages                   0           0
 Errors                     0           0
 Destination Unreachable    0           0
 Time Exceeded              0           0
 Parameter Problems         0           0
```

```
Source Quenches          0          0
Redirects                0          0
Echos                    0          0
Echo Replies             0          0
Timestamps               0          0
Timestamp Replies        0          0
Address Masks            0          0
Address Mask Replies     0          0
```

၉၅။ အထက်တွင် မြင်တွေ့ရသည်မှာ -s switch ကို အသုံးပြုလျှင် protocol များစွာ၏ status ကို မြင်တွေ့ရမည် ဖြစ်သောလည်း -p ICMP နှင့် တွဲသုံးသောကြောင့် ICMP တစ်မျိုးတည်းကို သာ filter လုပ်ပြီး ကြည့်ရှုနိုင်သည်။ အကယ်၍ IP သို့မဟုတ် TCP တစ်မျိုးမျိုးကို ကြည့်ရှုလိုပါကလဲ ICMP နေရာတွင် IP သို့မဟုတ် TCP အစားသွင်းရိုက်ပြီး ကြည့်ရှုနိုင်သည်။

The `tracert` Utility

၉၆။ `Tracert` Utility သည် TCP/IP trace route (traert) command line utility ဖြစ်ပြီး Internet သို့ TCP/IP packet မည်မျှလွှင့်ထုတ် နေသည်၊ လွှင့်ထုတ်ခဲ့သည်တို့ကို trace လိုက်ကြည့်နိုင်ခြင်းဖြစ်သည်။ `tracert` ကို command prompt တွင် ရိုက်နှိပ်ပြီး space ခြားကာ မိမိသိလိုသော DNS သို့မဟုတ် server တစ်ခုခု၏ name သို့မဟုတ် IP ကို ရိုက်သွင်းရမည်။

ဉပမာ-

```
C:\>tracert www.yahoo.com
Tracing route to www10.yahoo.com (204.74.93.10)
over a maximum of 30 hops:
     1    110 ms    96 ms     107 ms    fgo1.corpcomm.net
     2    96 ms     126 ms    95 ms     someone.corpcomm.net
trace complete.
```

Using the Address Resolution Protocol (ARP)

၉၇။ ARP ၏ အဓိက function မှာ TCP/IP address မှ Physical address ခေါ် MAC(media access control) address သို့ broadcast လုပ်၍ပြောင်းလဲ ဖော်ပြပေးခြင်း ဖြစ်သည်။ မိမိတို့ ကွန်ယက်အတွင်းရှိ server တစ်လုံး သို့မဟုတ် default Gateway

တစ်ခုမှ မည်သည့် IP များ ကို frequently access လုပ်ပေးနေသည် ဆိုသော ARP table မှ Address list ကို ဖတ်ယူခြင်းဖြစ်သည်။ ၎င်း ARP Table တွင် မည်သည့် IP သည် မည်မျှကြာအောင် access ဖြစ်နေသည်ဆိုသည်ကိုပါ သိရှိနိုင်သည်။ ထို့ကြောင့် ARP Table တွင် Dynamic entry နှင့် Static entry ယူ၍ နှစ်မျိုးပါဝင်နေသည်။ Dynamic Entry သည် Request လုပ်လာသော IP address ၏ MAC address ကို သိရှိပြီဆိုသည်နှင့် တပြိုင်တည်း ARP Table တွင် ထည့်သွင်းဖန်တီးပြီး ဖြစ်သည်။ Static Entry သည် Dynamic Entry ကဲ့သို့ လုပ်ဆောင်ချက် တူညီသော်လည်း ၎င်းလုပ်ဆောင်ချက်ကို ARP utility ကို အသုံးပြုပြီး Manually ဆောင်ရွက်ရသည်။ အထူးဂရုပြုရန်မှာ ARP Utility သည် Server base Network တွင်သာ အကျိုးဝင်မည် ဖြစ်သည်။

၉၈။ ARP ကို စတင်ရန်အတွက် Command Prompt တွင် **ARP** ဟူသော command ကို ရိုက်သွင်းရပါမည်။ ထိုသို့ ရိုက်သွင်းလိုက်ပါက ARP utility ၏ switch များနှင့် အသုံးပြုပုံ descriptions များ ပေါ်လာမည် ဖြစ်သည်။ ARP Command သည် Stan alone Computer များတွင် အသုံးမပြုနိုင်သကဲ့သို့ Client များတွင်လည်း သက်ရောက်မှု မရှိလှပေ။ DHCP server ကဲ့သို့သော server တွင် ၎င်း tool ဖြင့် Local ARP Table ကို ကြည့်ပြီး TCP/IP address နှင့် နှင့် MAC Address များကို ကိုက်ညီပြီး duplicate မဖြစ်စေရန် resolved လုပ်ပေးနိုင်သည်။ ARP Command ၏ အသုံးပြုသော Switch များကို အောက်တွင် ဖော်ပြထားသည်။

```
Displays and modifies the IP-to-Physical address translation
tables used by
address resolution protocol (ARP).

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.
Example:
  > arp -s 157.55.85.212   00-aa-00-62-c6-09   .... Adds a
  static entry.
  > arp -a  .... Displays the arp table.
```

နိဂုံး

Networking စာစောင်မှာ Windows Platform ပေါ်တွင် အခြေခံရေးသားထားခြင်းဖြစ်ပြီး Network Operator တစ်ဦးအတွက် Network Operation နှင့် Troubleshooting ဆောင်ရွက်နိုင်ရန်အတွက်ဖြစ်ပါသည်။ အခြားသော Platforms များအတွက်လည်း အခြေခံကျသဖြင့် Network Operator တစ်ဦးအနေဖြင့် မဖြစ်မနေသိရှိထားရမည့် အကြောင်းအရာအချက်အလက်များဖြစ်ပြီး System Administrator / Network Administrator မရှိသည့် Network များကို တာဝန်ယူရသူအနေဖြင့် ကျွမ်းကျင်စွာသိရှိနားလည်စေရန်အတွက် ရည်ရွယ်ရေးသားခြင်းဖြစ်ပါသည်။

မှီငြမ်းကိုးကားစာစောင်များ

- Microsoft Network Essential Edition 3.
- Network + David Groth And Tim Catura
- Network, Data Base Security And Standardization .
  Japan Information Technology Engineers Examination Center
- Hand On Training Of U Wai Lin Kyaw (MCF).