PRODUCT OF YOUTH

COMPLETE NETWORK GUIDE

CCNA MCSE MCSA MCTS

Level: Intermediate

- IPv4 Addressing
- IPv6 or IPng
- IPv4 Subnetting
- Supernetting
- IPv4 Routing
- DHCP
- DNS
- Mail Server
- NAT
- Squid Proxy

ZAW LIN YOUTH

CD Rom Included

ဘုရား

တရား

သံဃာ

ကျေးဇူး ဦးထိပ်ပန်ဆင် ရှိခိုးကန်တော့ပါ၏

❖ (ဖေဖေ)။ (မေမေ)

❖ တသီတသီ ပေးဆေး

❖ ဆရာ ဦးအေးသိမ်းဝင်း နှင့် ဆရာမ ဒေါ်တင်တင်အေး

❖ ဆရာ ကိုညီညီဝေ

❖ ကိုကြီး နှင့် ကိုကြီး

❖ (ကြီး)

ကျေးဇူး ဤဆေးညွှန်း ကန်တော့ပါ၏

အမှတ်တရ အတိတ်ဆွေးခြင်း

မတ်လ ၄ ရက်နေ့ ၁၉၉၇ ခုနှစ်

အဲ့ဒီနေ့ဟာ YOUTH Computer ကို ကျွန်တော်တည်ထောင်ဖွင့်လှစ်ခဲ့တဲ့နေ့ပေါ့။
တကယ်တော့ YOUTH ကိုစတင်တည်ထောင်တုန်းက ကျွန်တော်တစ်ယောက်တည်းမဟုတ်ဘူး။
အကြောင်းအမျိုးမျိုးကြောင့် အဲ့ဒီနေ့ကကျွန်တော်တစ်ယောက်တည်း ပြန်လည်ဖွင့်လှစ်ခဲ့တဲ့နေ့ဖြစ်တယ်။
၁၉၉၅ ခုနှစ်မှာ အပြင်မှာ ကွန်ပျူတာကွန်ရက်အနည်းငယ် လိုက်ဆင်ပေးနေပြီး ရတဲ့ပိုက်ဆံနှင့် ထမင်းစားဖို့ လုပ်နေပြီ ဖြစ်တယ်။ အခြေအနေအရ ပညာသင်ရမယ့် အရွယ်ဖြစ်ပေမယ့် အကြောင်းများစွာဟာ ကျွန်တော့်ကို လုပ်ငန်းခွင်ဖက်ကို တွန်းပို့ခဲ့တယ်။ ၁၉၉၆ မှာ ယနေ့ရေပန်းစားနေသော ကွန်ရက်နှင့်ပတ်သက်တဲ့ နိုင်ငံတကာအသိအမှတ်ပြုလက်မှတ် ကို Novell ကနေရရှိခဲ့တယ်။ အဲ့ဒီတုန်းက MCSE ဆိုတာ ရန်ကုန်မှာမရှိသေးဘူး။ နောက်တော့ အဝေးသင် တက္ကသိုလ် တက်နေရင်းနဲ့ အဒေါ်ဆီက ပိုက်ဆံချေးပြီး မိတ်ဆွေတစ်ယောက်နှင့် ပေါင်းကာ YOUTH ကိုဖွင့်ဖြစ်လိုက်တာပဲ။ မနက် ၇း၀၀နာရီ အတန်းစမှာမို့ ၆း၀၀နာရီမှာ အိမ်ကပန်ကာကြီးကို သင်တန်းအတွက်ယူလာရင်း လမ်းထိပ်ကဆိုက်ကားနှင့် အသော့လာခဲ့ပါတယ်။ အဲ့ဒါလေးဟာပထမဦးဆုံး YOUTH နှင့်ပတ်သက်တဲ့အဖြစ်အပျက်ကလေးပေါ့ဗျာ။ အသက် ၂၀ပဲ ရှိသေးတာမို့ ဒီနေ့ဒီအချိန်ရောက်လို့ နောက်ကိုပြန်လှည့်ကြည့်လိုက်တဲ့အခါကျွန်တော့်ဘဝရဲ့အကြောင်းအရာ တော်တော် များများဟာ YOUTH နှင့်ပဲ ပတ်သက်နေတာကိုတွေ့ရပါလေရဲ့။

ဒီစာအုပ်ကို ၂၀၀၉ မတ်လ ၄ရက် နေ့မှာကျရောက်မယ့် YOUTH ၁၂ နှစ်ပြည့်အတွက်အမှတ်တရ ထုတ်ဝေဖြစ်ပါတယ်။ ဒီနေ့ဒီအချိန်အထိ ရပ်တည်လို့ရအောင် ပညာသင်ပေးခဲ့တဲ့ ကျွန်တော့် ဆရာနှင့်ဆရာမတွေ၊ အခြားသောဆရာတွေရော၊ ဝိုင်းဝန်းပံ့ပိုးကြတဲ့ မရှိတော့ပြီဖြစ်တဲ့ အမေနှင့်ကိုပြီး ရပ်ဝေးကအစ်ကိုတွေ၊ ဦးလေးအဒေါ်တွေ နှင့် YOUTH ရဲ့ သက်တမ်းတစ်ဝက်မက ကျွန်တော့်ဘေးမှာအတူရှိခဲ့တဲ့ချစ်ဇနီး အိအိပြီး YOUTH ရဲ့ လက်ရှိဝန်ထမ်းနှင့် ယခင်လက်တွဲခဲ့ဖူးတဲ့ဝန်ထမ်းဟောင်းများ၊ သူငယ်ချင်းများ၊ YOUTH ရဲ့ သင်တန်းသားများအားလုံး၊ အားပေးကူညီကြတဲ့သူများ၊ စာဖတ်ပရိသတ်များအားလုံး၊ ရောင်းချပေးတဲ့ ဆိုင်ခွဲများ အားလုံးတို့ကတော့ဖြင့် ကျွန်တော်နှင့် YOUTH အတွက်ကျေးဇူးမကင်းတဲ့သူတွေပါပဲလို့ပြောကြားလိုပါတယ်။ နောက်ထပ်လည်း ကျွန်တော်နှင့် YOUTH ကို ဆက်လက်ရှင်သန်စေခြင်းငှာ အတူဝိုင်းဝန်းပံ့ပိုးပေးကြပါဦး လို့လည်းပြောချင်ပါတယ်။ သင်တန်းသားတွေအတွက်ရော၊ စာဖတ်ပရိသတ်အတွက်ရော၊ နိုင်ငံသားတွေအတွက်ပါ နည်းပညာတွေ ဖြန့်ဝေပေးဖို့ အထူးကြိုးစားနေကြောင်းလည်းပြောကြားလိုပါတယ်။ လေတိုက်လို့သစ်ရွက်ကြွေချင် တောင်လွမ်းမောတတ်တဲ့အရွယ်ကနေ လူတွေကိုဘာပဲဖြစ်ဖြစ်ပြုံးပြီးကြည့်နေနိုင်တဲ့အရွယ်အထိ YOUTH ကို ဆက်လက်ရပ်တည်နိုင်ပါစေလို့ ကျွန်တော်ကိုယ်တိုင်ကအစ ဆုမွန်ကောင်းလည်းတောင်းရင်း ဒီထက်လည်း ပိုကြိုးစားရင်းရှေ့ကိုဆက်လျှောက်ခွင့်ပြုပါ.......

နတ်လူသာဓု ခေါ်စေသော် ...

လမ်းခရီးတစ်နေရာ .

အရပ်ခေါ် ဒေါင်းသေချောင်း . အချိန်က အာရုဏ်ကျင်းစ ဝေလီဝေလင်း

ပတ်ဝန်ကျင်က ပိုးတိုးဝါးတား .

တဖြည်းဖြည်း အလင်းရောင်ရလာသည်နှင့်အမျှ ရပ်ထားသော ခရီးသွားကားကြီး ကားငယ်များထဲမှ လူများစွာသည် ဒေါင်းသေချောင်းအစပ်သို့ တဖွဲဖွဲ့ရောက်လာကြ၏။

မကြာမီပင် လယ်ထွန်စက်တစ်စီးသည် *Hi Ace* ကားတစ်စီးကိုဆွဲကာ ဒေါင်းသေချောင်းတွင်စီးဆင်းနေသော ရေအလျဉ်ကို စတင်ကူးဖြတ်လေ၏။

လူအများကပို၍အုပ်အော်သောင်းနင်းဖြစ်လေ၏။

အချို့က အံ့သြဘနန်းရှိကြလေ၏။ အချို့က မမြင်ဖူးရမရှိလေအောင် ချောင်းစပ်သို့ တိုးဝှေ့ကြည့်ကြ၏။ အချို့က ကိုယ့်ကားဘယ်တော့ချောင်းထဲဖြတ်မောင်းမလဲစုံစမ်းကြလေသည်။ ဤအချိန်မှာပင် နောက် လယ်ထွန်စက်တစ်စီးက ကားတစ်စီးကိုထပ်မံဆွဲရာ လူများပို၍ ပိုင်းအုံလာပြန်၏။ ခရီးသွားကားကြီးများကတော့ ဤချောင်းရေကို လင်းအားကြီးအချိန်ကျရင် ဖြတ်မောင်းနိုင်၏ ဟု အချို့ကဆို၏။ မည့်သို့ပင်ဤနေရာ၌ အုပ်အော်သောင်းနင်းဖြစ်လင့်ကစား . " အရှင်ဘုရား၊ အာရုဏ်ဆွမ်းများ ဘုဉ်းပြီးပလား၊ မဘုဉ်းရသေးရင် တပည့်တော် ကပ်ပါရစေဘုရား " လူအုပ်များကြားထဲမှ ဘုန်းတော်ကြီးသည် ခပ်မဆိပ်ပင် ပင့်သူ ဒါကာ၏ နောက်သို့လိုက်ကာ အနားရှိဆိုင်မှ ဒါကာ ကပ်သော ဆွမ်းကို လက်ခံတော်မူလေသည်။

ဤကာလဒါနကို လက်လွတ်မခံ ဆက်ကပ်သော ပုဂ္ဂိုလ်ကမည်သူနည်း . အကျွန်ုပ်ပင်ဖြစ်ပေသည်။

ကျေးဇူးတင်ရှိခြင်း

- ချစ်ဇနီး အိအိဖြိုး

- *YOUTH* သင်တန်းကို ဟိုနေရာပြောင်းလိုက် ဒီနေရာပြောင်းလိုက် ခဏခဏ နေရာပြောင်းနေတာတောင် *YOUTH* ရှိတဲ့နေရာ မရမက လိုက်ရှာပြီး ရောက်အောင်လာကာသင်တန်းတက်ကြတဲ့ *YOUTH* ၏ ကျေးဇူးရှင် သင်တန်းသား၊ သင်တန်းသူများ

- ကျွန်တော့် အလုပ်တွေအပေါ် စေတနာထားပြီး ဝိုင်းဝန်းလုပ်ကိုင်ပေးကြကုန်သော ကျွန်တော့်လုပ်ဖော်ကိုင်ဖက်များ။

- ကျွန်တော့် စာအုပ်တွေကို ဝယ်ယူအားပေးကျသူများအားလုံးနှင့်ရောင်းချပေးသောဆိုင်ခွဲများ
- တစ်ခါတစ်ခါ တော်တော်ကြာအောင်မတွေ့ဖြစ်ကြပြန်တဲ့ ဆရာမိုး
- ဂေါက်အိတ်တစ်အိတ်လုံး ပေးထားပြီး ဂေါက်ရိုက်ဖြစ်အောင်ပံ့ပိုးပေးတဲ့ အန်ကယ် ဦးစိန်ဝင်း
- မြ လွှာမှာနေတဲ့ ကျွန်တော် အိမ်ပေါ်ပြေးတက်နိုင်အောင် ဆေးကုပေးခဲ့တဲ့ Dr. ဦးတက်ထွန်းချစ်
- စာအုပ်တွေအကြွေးရိုက်ပေးတဲ့ ဇော်ဇော် (သီတာပုံနှိပ်တိုက်)
- *YOUTH* ပြက္ခဒိန်ကိုအိမ်မှာလာရိုက်ခွင့်ပေးသော ကိုပြည့်စုံ နှင့် မိသားစု
- သင်ဆရာ၊ မြင်ဆရာ၊ ကြားဆရာ၊ အကြံပေးဆရာ၊ အားပေးသည့်ဆရာများ
- ပါဝင်ကူညီရေးသားပေးခဲ့ သော ညီငယ် နန္ဒကြူ
- အခြားအခြားသော ကျေးဇူးတင်ထိုက်သူများအားလုံးသို့

ဖော်လင်း (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
(၁၀) PC System Administration
(၁၁) ကွန်ပျူတာ - လုပ်ငန်းခွင်ဝင် 4 in 1 အတွဲ ၁
(၁၂) ကွန်ပျူတာ - အလယ်တန်း အတွဲ ၁
(၁၃) PC Mechanics
(၁၄) ကွန်ပျူတာ - လုပ်ငန်းခွင်ဝင် အတွဲ ၂
(၁၅) ကွန်ပျူတာ - လုပ်ငန်းခွင်ဝင် အတွဲ ၃
(၁၆) ကွန်ပျူတာ - အထက်တန်း အတွဲ ၁
(၁၇) Complete Network Guide (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 စီဒီ (ညီညီထွေး၊ Rock Guitar Study Guide)
(၄) Musical Instruments Encyclopedia နိုင်ငံတကာတူရိယာများအကြောင်းသိကောင်းစရာ (အခြေခံ)
(၅) ကွန်ပျူတာဖြင့် ဂီတသံစဉ်များဖန်တီးနိုင်ရန်အသင့်ပြုလုပ်ပေးထားသော မြန်မာ့ဆိုင်းဝိုင်း Loops များ အတွဲ ၁ နှင့် ၂ စီဒီ

မာတိကာ

CHAPTER 1 IP Addressing

၁.၁	IPv4 Address အကြောင်း	- ၂
၁.၂	Types of IPv4 Address အမျိုးအစားများ	- ၄
၁.၃	IPv4 Unicast Address ဆိုတာ	- ၅
၁.၄	Hight Order Bit အကြောင်း	- ၉
၁.၅	Class A Network အကြောင်း	- ၁၁
၁.၆	Class A Network 126 အထိပဲရှိက်ရခြင်းအကြောင်း	- ၁၂
၁.၇	Class A Host အရေအတွက်	- ၁၃
၁.၈	Class B Network အကြောင်း	- ၁၄
၁.၉	Class C Network အကြောင်း	- ၁၆
၁.၁၀	Dotted Decimal Notation ဖြင့် ဖော်ပြခြင်း	- ၁၇
၁.၁၁	Prefix Length Notation ဖြင့် ဖော်ပြခြင်း	- ၁၉
၁.၁၂	Public & Private Address ဆိုတာ	- ၂၀
၁.၁၃	Illegal (ILLEGAL) Address ဆိုတာ	- ၂၅
၁.၁၄	Special IPv4 Address များ	- ၂၅
၁.၁၅	Automatic Private IP ဖယ်ထားခြင်း	- ၂၆
၁.၁၆	IPv4 Unicast Address နိဂုံးချုပ်	- ၂၈
၁.၁၇	IPv4 Multicast Address	- ၂၉
၁.၁၈	Classful and Classless Address	- ၂၉
၁.၁၉	IPv4 Broadcast Address များအကြောင်း	- ၂၉
၁.၂၀	Decimal မှ Binary သို့ပြောင်းခြင်း	- ၃၁
၁.၂၁	Binary မှ Decimal သို့ပြောင်းခြင်း	- ၃၇

CHAPTER 2 IP Version 6

၂.၁	IP Version 6 @ IPng @ IP Next Generation အကြောင်း	- ၄၀
၂.၂	IPv6 Address ပုံစံ	- ၄၃
၂.၃	Hexadecimal မှ Binary သို့ပြောင်းခြင်း	- ၄၄
၂.၄	Address ကိုချုံ့ခြင်း	- ၄၆
၂.၅	IPv6 အမျိုးအစားများ	- ၄၇
၂.၆	Anycast Address အကြောင်း	- ၄၇
၂.၇	IPv6 Unicast Address အမျိုးအစားများ	- ၄၈
၂.၈	Global Unicast Address အကြောင်း	- ၄၉
၂.၉	Link Local Address များအကြောင်း	- ၅၂
၂.၁၀	Site Local Address များအကြောင်း	- ၅၃
၂.၁၁	Zone IDs for Local Use Address အကြောင်း	- ၅၄
၂.၁၂	Unique Local Address အကြောင်း	- ၅၇
၂.၁၃	Special IPv6 Address အကြောင်း	- ၅၈
၂.၁၄	Transition Address အကြောင်း	- ၅၈
၂.၁၅	IPv4 Multicast Address အကြောင်း	- ၆၀

CHAPTER 3 IPv4 Subnetting

၃.၁	IPv4 Subnetting အကြောင်း	- ၆၄
၃.၂	ရိုးရှင်းသော Subnet ခွဲနည်း	- ၆၆
၃.၃	စိတ်ကြိုက် Subnet ခွဲခြင်း	- ၇၁
၃.၄	Subnet ခွဲပြီး Octet များကို တွက်ခြင်း	- ၇၉
၃.၅	ဖော်မြူလာကို ရှင်းပြမြ	- ၈၂
၃.၆	Decimal နည်းဖြင့် Subnetted Octet များရှာခြင်း	- ၈၄
၃.၇	Subnet တစ်ခုမှာ ရှိတဲ့ IPv4 Address အတိုင်းအတာ	- ၈၄

၃.၈ Address ကဘယ် Subnet မှာရှိနေသလည်း သို့မဟုတ် Subnet Address တွက်ခြင်း - ၉၁
၃.၉ ပထမနည်းက Prefix Length Notation - ၉၂
၃.၁၀ ဒုတိယနည်းက Subnet Mask Notation နည်း - ၉၆
၃.၁၁ Broadcast Address ကိုတွက်ခြင်း - ၉၈
၃.၁၂ Subnetting နှစ်မျိုး - ၁၀၀
၃.၁၃ VLSM ပေါ်လာရခြင်းနှင့် အသုံးပြုရခြင်းအကြောင်း - ၁၀၃
၃.၁၄ VLSM ဥပမာပေးခြင်း - ၁၀၅
၃.၁၅ VLSM နိဂုံးချုပ်ရှင်းပြခြင်း - ၁၀၈

CHAPTER 4 Supernetting or CIDR

၄.၁ Supernetting အကြောင်း - ၁၁၂
၄.၂ ဘာဖြစ်လို့ Supernet ကိုသုံးရတာလဲ - ၁၁၃
၄.၃ Supernet အလုပ်လုပ်ပုံ - ၁၁၅
၄.၄ Numeric Contiguity - ၁၁၇
၄.၅ Even Divisibility - ၁၁၈
၄.၆ Single Interface - ၁၂၃
၄.၇ Supernet ပြုလုပ်ခြင်း - ၁၂၄
၄.၈ နိဂုံးချုပ် အမေးအဖြေ - ၁၂၆

CHAPTER 5 IPv4 Routing

၅.၁ IP Routing အကြောင်း - ၁၃၂
၅.၂ Direct နှင့် Indirect Delivery ပေးပို့ခြင်းနည်း ၂ နည်း - ၁၃၃
၅.၃ Direct Delivery အကြောင်း - ၁၃၃
၅.၄ Indirect Delivery အကြောင်း - ၁၃၃

၅.၅ IP Routing Table အကြောင်း - ၁၃၅
၅.၆ Routing Table Entries အကြောင်း - ၁၃၆
၅.၇ Routes အမျိုးအစားများ - ၁၃၇
၅.၈ Static & Dynamic Routing အကြောင်း - ၁၃၈
၅.၉ Stable State အကြောင်း - ၁၄၁
၅.၁၀ Unstable State အကြောင်း - ၁၄၂
၅.၁၁ IPv4 Routing အကြောင်း - ၁၄၂
၅.၁၂ IPv4 Routing Table ပါ အကြောင်းအရာများ - ၁၄၄
၅.၁၃ Routing Determination Process အကြောင်း သို့မဟုတ် ဘယ်လမ်းကြောင်းက သွားမလဲ - ၁၄၄
၅.၁၄ Longest Match ရှင်းလင်းချက် - ၁၄၆
၅.၁၅ Lowest Metric ရှင်းလင်းချက် - ၁၄၇
၅.၁၆ Binding Order ရှင်းလင်းချက် - ၁၄၇
၅.၁၇ Next Hop Address နှင့် Interface ကို ဆုံးဖြတ်ခြင်း - ၁၄၉
၅.၁၈ Routing Table ကိုကြည့်ခြင်း - ၁၅၀
၅.၁၉ Static IPv4 Routing အကြောင်း - ၁၅၂
၅.၂၀ Dynamic IPv4 Routing အကြောင်း - ၁၅၄

CHAPTER 6 DHCP

၆.၁ ပြောချင်တာလေးတစ်ခု - ၁၅၆
၆.၂ DHCP အကြောင်း - ၁၅၇
၆.၃ DHCP အလုပ်လုပ်ပုံ - ၁၅၉
၆.၄ DHCP အကျိုးကျေးဇူး - ၁၆၃
၆.၅ DHCP Server ကို Install လုပ်ခြင်း - ၁၆၄
၆.၆ DHCP နှင့် Configuration လုပ်ခြင်း - ၁၆၇
၆.၇ Static Assignment - ၁၇၈

၆.၈ Dynamic Assignment - ၁၈၀
၆.၉ DHCP နှင့် ပတ်သက်သော အခေါ်အဝေါ်များ - ၁၈၅

CHAPTER 7 DNS

၇.၁ DNS ဆိုတာ ဘာလဲ၊ ဘာကြောင့်အသုံးပြုရတာလဲ - ၁၉၀
၇.၂ DNS Server ကို ဘယ်လို Install လုပ်မလဲ - ၁၉၂
၇.၃ DNS Server Computer Name နှင့် DNS Suffix Name ကို သတ်မှတ်ပေးပုံ - ၂၀၀
၇.၄ DNS Server ကို IP Address သတ်မှတ်ပေးပုံ - ၂၀၅
၇.၅ DNS (Domain Name System) ကို Install လုပ်ပုံ - ၂၀၉
၇.၆ DNS Server ကို Configure လုပ်ပုံနှင့် Setting သတ်မှတ်ပုံ - ၂၁၃
၇.၇ Forward Lookup Zone ထဲတွင် New Host (A) File ကိုတည်ဆောက်ပုံ - ၂၂၅
၇.၈ Reverse Lookup Zone ထဲတွင် New Ponter (PTR) File ကိုတည်ဆောက်ပုံ - ၂၂၈
၇.၉ Clent 1 အတွက် Forward Lookup Zone မှာ Naming System သတ်မှတ်ရန်အတွက် New Host (A) ကိုဖန်တီးပုံ - ၂၃၃

CHAPTER 8 Mail Server

၈.၁ Mail Server ဆိုတာဘာလဲ၊ Mail Server ကို ဘယ်လို Install လုပ်မလဲ - ၂၄၀
၈.၂ Mail Server ကို Install လုပ်ပုံ - ၂၄၀
၈.၃ Mail Server ၌ Mail Account ဖန်တီးပုံ - ၂၄၄
၈.၄ Client Computer များတွင် Mail Account Setting ထည့်ပုံ - ၂၄၈

CHAPTER 9 Network Address Translation

၉.၁	Network Address Translation ဆိုတာဘာလဲ	- ၂၅၆
၉.၂	NAT Service ကို ဘယ်လိုနေရာမျိုးမှာ အသုံးပြုလို့ရသလဲ	- ၂၅၆
၉.၃	Basic NAT နှင့် PAT အကြောင်း	- ၂၅၆
၉.၄	Basic NAT နှင့် PAT တို့ Level ကွဲသွားရခြင်းအကြောင်း	- ၂၅၇
၉.၅	SNAT နှင့် DNAT ဆိုတာ ဘာလဲ	- ၂၅၇
၉.၆	NAT အမျိုးအစားများ	- ၂၅၇
၉.၇	Network Address Translation or NAPT ဘယ်လိုအလုပ်လုပ်သလဲ	- ၂၅၈
၉.၈	NAT Server ကို Install လုပ်ပုံ	- ၂၆၂

CHAPTER 10 Proxy Server

၁၀.၁	Proxy Server ဆိုတာဘာလဲ	- ၂၆၈
၁၀.၂	Squid Proxy Service ကို Run ပုံ	- ၂၇၂
၁၀.၃	Client Computer ရဲ့ Internet Explorer ထဲမှာ Setting ချပုံ	- ၂၈၇

စာရေးသူ၏အမှာစာ

ဒီစာအုပ်လေးကတော့ YOUTH ကိုတည်ထောင်ခြင်း ၁၂ နှစ်ပြည့်အမှတ်တရထုတ်ဝေတာဖြစ်ပါတယ်။ စာအုပ်မှာ အခန်းအားဖြင့် ၁၀ ခန်းပါရှိပါတယ်။ ကျွန်တော်ထုတ်ပြီးသားစာအုပ်တွေထဲမှာ မပါသေးတဲ့အကြောင်းအရာတွေကိုရေးထားတာဖြစ်ပါတယ်။ နောက်ပြီး စာမေးပွဲဖြေမယ့်သူတွေအတွက်ရော၊ ပြင်ပလုပ်ငန်းခွင်ဝင်မယ့်သူတွေအတွက်ပါ အသုံးတည့်အောင်ရေးသားပေးထားတာဖြစ်ပါတယ်။ နောက်တစ်ခုက အင်တာနက်ဆိုင်တွေမှာ Router ကိုမသုံးဘဲ Proxy Server သုံးပြီး ကွန်ရက်ချိတ်တတ်အောင်လည်း Proxy Server အကြောင်းကိုတစ်ခန်းသီးသန့်ထည့်ပေးထားပါတယ်။ စာအုပ်မှာပါတဲ့အကြောင်းအရာတွေဟာ အိပ်ဖတ်လို့ကတော့ နားလည်မှာမဟုတ်သလို ဒီအတိုင်းကြီးထိုင်ဖတ်လည်းနားလည်ဖို့မလွယ်ပါ။ ဒါဆို ကင်းမြီးကောက်ထောင်ဖတ်ရမလားလို့တော့ မပြောလိုက်ပါနဲ့။ ကျွန်တော်ဆိုလိုချင်တာက IP Address အခန်းတွေဆို ခဲတံနှင့် စာရွက်အကြမ်းလေးနှင့်မှ အဆင်ပြေမယ်။ နောက်ပိုင်းက Server သင်ခန်းစာများကျတော့လည်း စက်နှင့် တွဲစမ်းမှ နားလည်နိုင်မှာဖြစ်ပါတယ်။ မဟုတ်လို့ကတော့ နားလည်မှာမဟုတ်ပါ။ နားမလည်တဲ့အခါကျရင်လည်း ဒီကကောင်ပဲ မေတ္တာပို့ခံရမှာဖြစ်ပါတယ်။ နောက်တစ်ခုက ဒီစာအုပ်ကိုဖတ်တဲ့သူဟာ ကွန်ရက်နှင့်ပတ်သက်လို့ အခြေခံတော့ရှိထားရမှာဖြစ်ပါတယ်။ အခြေခံအကြောင်းတွေကိုထည့်မပြောထားပါဘူး။ ဒါကြောင့်နားမလည်ရင် အခြေခံကိုပြန်လေ့လာစေချင်ပါတယ်။

ကြုံတုန်းလေးပြောပါရစေ။ သင်တန်းတစ်ခုတက်ပြီးတိုင်း အခြေခံရှိပြီလို့လည်းပြောလို့မရပါဘူး။ သင်တန်းမှာ သင်တဲ့စာတွေကိုရမှပိုင်နိုင်မှသာလျှင် အခြေခံရတယ်လို့ပြောနိုင်မှာပါ။ ကျွန်တော့်သင်တန်းမှာလည်းရှိတာပဲ ဆရာစာသင်နေရင် စိတ်မဝင်စား။ အတန်းလည်းမှန်မှန်မတက်ချင်၊ ဒါဆို ဘယ်ဆရာပဲသင်သင် အခြေခံ အားနည်းမှာပဲဖြစ်ပါတယ်။ ဒါကြောင့် သင်တန်းတစ်ခုတက်၊ ပြီးရင် Certificate လေးယူ ဒါကို အခြေခံတတ်ပြီလို့ပြောလို့မရပါဘူး။ တကယ်တတ်ဖို့သာလျှင်အရေးကြီးတာပါ။ ဘယ်သင်တန်းပဲဖြစ်ဖြစ် သင်တန်းတွေမှာ ဆရာတွေကအကောင်းဆုံးသင်ကြတာချည်းပဲ။ ဒါပေသိ သင်တန်းသားက သေချာအာရုံစိုက်လေ့လာဖို့လိုအပ်တယ်။

နောက်တစ်ခုက နိုင်ငံတကာအသိအမှတ်ပြုစာမေးပွဲအကြောင်းလေးလည်းနည်းနည်းပြောချင်တယ်။ Microsoft Certified တို့ Cisco Certified တို့ Novell Certified တို့ ဆိုတာက ဖြေတိုင်းအောင်ကျတာမဟုတ်ဘူး။ အခု အပြင်မှာသတင်းကြားတာက မေးခွန်းတွေကျက်ဖြေပြီးအောင်နေကြတယ်လို့ သတင်းကြားတာပဲ။ မေးခွန်းတွေကျက်ဖြေတာကို အပြစ်တော့ပြောလို့မရပါဘူး။ ဒါ Pretest လုပ်တာပေါ့။ ကျွန်တော်တို့ဖြေခဲ့တုန်းကလည်း Pretest လုပ်ခဲ့တာပါပဲ။ ကျွန်တော် Novell စာမေးပွဲဖြေမယ်လုပ်တော့ Bangkok က

ITIT Centre မှာ Form တွေဖြည့်ပြီး Pretest Disk လေးဝယ်လာခဲ့တယ်။ ပြီးတော့ ကျွန်တော့်အစ်ကိုတွေ အလုပ်က ကွန်ပျူတာမှာ သွားပြီး အဲ့ဒီ Pretest လေးဖြေကြည့်တာ။ နောက်တော့ ဖြေရမယ့်နေ့ကျမှ သွားဖြေတာ။ ဒီကြားထဲတော့ စာကျက်နေရတာပေါ့။ စာကျက်တယ်ဆိုတာ စာမျက်နှာ ၅၀၀ ကျော်စာအုပ်ကြီးကို ဘာသာပြန်ပြီးကျက်တာ၊ မေးခွန်းတွေကျက်နေတာမဟုတ်ဘူး။ သွားဖြေတော့ အောင်တော့အောင်တယ်။ မရတဲ့အပိုင်းတွေလည်းရှိတယ်။ သူက Report ထွက်လာတယ်။ အဲ့ဒီ Report မှာ ဘယ်အပိုင်းတွေပြန်လေ့လာပါဆိုပြီးတော့ပေါ့။ ဒီတော့ တော်တော်ခဲရာခဲဆစ်ဖြေရတာပါ။ အဓိကပြောချင်တာက စာမေးပွဲအောင်တာလည်းအောင်တာပေါ့။ တကယ်တတ်စေချင်တယ်။ မဟုတ်ရင် တကယ်တတ်ပြီး Certificate ရတဲ့သူတွေက နိုင်ငံခြားမှာပါလစာအနှိမ်ခံရတယ်။ ဒီတော့တကယ်မတတ်ရင် တိုင်းတစ်ပါးသွားအလုပ်လုပ်တဲ့အခါကျတာ ဒီလူတွေ Certificate သာရတာ ဘာမှမတတ်ဘူးဖြစ်မယ်။ ဒီလိုမဖြစ်ရလေအောင် စာမေးပွဲအောင်အောင်လည်းလုပ်ပါ။ တကယ်လည်းတတ်အောင်လုပ်ကြပါလို့ ဒီနေရာကနေတိုက်တွန်းချင်ပါတယ်။ ဒီအတွက်လည်း ဒီစာအုပ်ကိုထုတ်ပေးတာဖြစ်ပါတယ်။

နောက်တစ်ခုပြောချင်တာက ဒီစာမေးပွဲတွေရဲ့ထုံးစံအတိုင်း အောင်ရင် Certificate ထုတ်ပေးတယ် ဒါပေမယ့် မရတဲ့အပိုင်းကို Report မှာဖော်ပြထားတယ်။ ဒီစနစ်လေးကိုသဘောကျလို့ ကျွန်တော့်သင်တန်းမှာလည်းအဲ့သလိုလုပ်ထားတယ်။ သင်တန်းပြီးရင် Certificate ထုတ်ပေးတယ်။ Certificate ဆိုတာ Completion Certificate ပေါ့။ ဆိုလိုတာက သင်တန်းပြီးဆုံးကြောင်း Certificate ပေါ့။ လူတွေကတစ်ချို့အထင်လွဲနေကြတယ်။ သင်တန်းမှာ စာမေးပွဲစစ်လို့ မအောင်ရင် Certificate မထုတ်ပေးဘူးတို့ဘာတို့ပေါ့။ ကျွန်တော်ကတော့ သင်တန်းပြီးလို့ စစ်ဆေးတဲ့စာမေးပွဲကျလည်းထုတ်ပေးတယ်။ ဘာလို့လည်း ပြောပြီးပြီးလေ သူက သင်တန်းလာတတ်တာ Certificate တော့လိုချင်မှာပေါ့။ ဒီတော့ထုတ်ပေးတယ်။ ဒါပေမယ့် Certificate မှာ သူဘာတွေသင်ခဲ့တယ် ဘယ်လောက်သင်ခဲ့တယ်လို့ရေးထားတာ–တတ်တယ်လို့ရေးထားတာမှမဟုတ်တာ။ ဒါ Completion Certificate ပေါ့။ သူစာရတယ်မရဘူးဆိုတာတော့ Certificate နှင့်အတူ Report ပါတယ်။ အဲ့ဒီ Report မှာ သူဘာတွေပြန်လေ့လာရမယ်၊ ဘာတွေအားနည်းတယ်ဆိုတာပါတယ်။ သင်တန်းဆင်းပြီးကျတဲ့သူတွေကို အားနည်းတဲ့အပိုင်းပြန်သင်ပေးလိုက်တယ်။ ဒီလိုစနစ်လေးတစ်ခုတော့ထားတယ်။

နောက်တစ်ခုက ကျွန်တော် Novell Certified ဖြစ်ခဲ့တုန်းက ၁၉၉၆ ကျွန်တော့်အသက်ကလည်း ၂၀ ပဲရှိသေးတယ်။ ရန်ကုန်မှာ MCSE ဆိုသိတောင်မသိသေးဘူး။ ကျွန်တော်လည်း ဘန်ကောက်ရောက်မှသိတာ။ ဖြေပြီးပြန်လာတော့ YOUTH ကိုထောင်ရော။ ဒီတော့ ဒီစာမေးပွဲတွေက ကျွန်တော်နဲ့ မဆိုင်သလိုလည်းဖြစ်သွားတယ်။ ဒီလိုပါ တစ်မျိုးမထင်ပါနဲ့ဦး။ ဒီ Certificate တွေက Valid Date နဲ့ဗျ။ ဥပမာ MCSE ဆို 2 Years ပေါ့။ ၂ နှစ်ကျော်သွားရင် တစ်ခါ Update ပြန်လုပ်ရတယ်။ ဒီလိုမှလည်း လုပ်ငန်းခွင်မှာ အဆင်ပြေတယ်။ ကျွန်တော်က ကိုယ်ပိုင် Business လုပ်လိုက်တော့ အပြင်ပြန်ထွက်ပြီးစာမေးပွဲပြန်မဖြေဖြစ်တော့သလို၊ ကိုယ်ပိုင်အလုပ်မို့ ဖြေစရာလည်းမလိုတော့ဘူးလေ။ နောက် ကျွန်တော့် Trend က Busi-

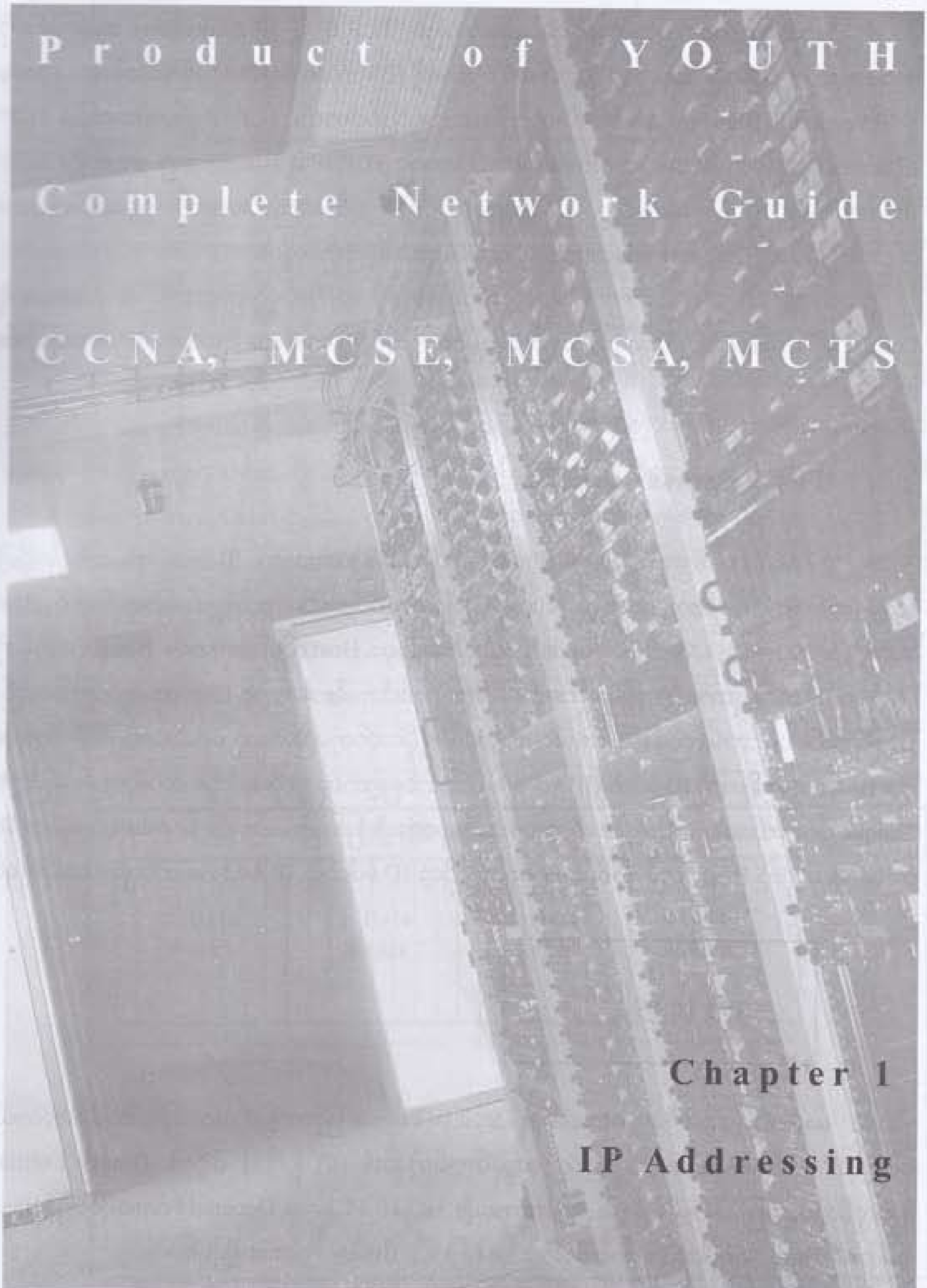
ness ကို ဦးတည်နေတာလေ။ ဘာလို့ဒီလိုပြောနေရသလဲဆိုတော့ ရယ်လည်းရယ်ရပါတယ်။ ကိုယ်က MCSA အတန်းတွေသင်တော့ တစ်ချို့ ကလေးတွေက ဒီဆရာက သူရော MCSA အောင်ပြီးသားလားပေါ့။ ရယ်ချင်တယ်ဆိုတာဒီလိုပါ MCSE/SA အောင်ပြီးမှ ဒီလိုအတန်းမျိုးတွေသင်လို့ရသလားဆိုတာပါ။ Certificate အတွက်ဆိုရင် စာမေးပွဲအောင်ပြီးသားလူ ကျွန်တော်ခေါ်ခန့်ထားလိုက်ရုံပေါ့။ ကျွန်တော့်သင်တန်းသားကျွန်တော့်စာဖတ်ပရိသတ်အတွက် ကျွန်တော့်သင်ကြားမှုကိုပြဖို့က စာမေးပွဲဖြေပြပါဆိုရင် ကျွန်တော်ဖြေချင်တာက Certified Instructor ပါ။ ဟုတ်ပါတယ်။ ကျွန်တော်က စာသင်တဲ့သူလေ။ ကျွန်တော်က သူများဆီမှာ အလုပ်သွားလျှောက်မယ့်သူမှမဟုတ်တာ။ ဒီတော့ ဖြေမယ့်ဖြေ System Engineer ဖြေမယ့်အစား Certified Instructor ပဲဖြေတော့မပေါ့။ ဒါပေမယ့်လည်းမလွယ်ဘူးလေ။ သူက English Version ပဲရှိတာ။ ဒါကြောင့် System Engineer ဖြစ်တိုင်းလည်းစာမသင်တတ်ဘူး။ သူက သူပဲကျွမ်းတာ၊ ဒါကို သူများနားလည်အောင်ပြောဆို လုပ်ပြဆိုလုပ်ပြမယ် နားလည်အောင်မပြောတတ်ဘူး။ ဒါကြောင့် ကျွန်တော့်က လူငယ်တွေကို ပေးချင်တာ သင်ကြားမှု၊ ကျွန်တော်ရဲ့ သင်ကြားမှုအတွေ့အကြုံ ၁၉၉၃ ကျွန်တော့်ဆရာဆီမှာကတည်းက စာသင်ပေးလာတာ။ အခုစာသင်လာတာ ၁၆ နှစ်ရှိပြီ။ ၁၆ နှစ်ဆိုတာကလည်း ၄ နှစ်က ဘောလုံးကန်၊ ၄ နှစ်က ပန်းချီဆရာ၊ ၃ နှစ်က ဗေဒင်ဟော စသဖြင့်လုပ်လိုက်တာမဟုတ်ဘူး။ ၁၆ နှစ်လုံး စာသင်လာတာ။ ဒီတော့ နောက်လာမယ့်လူငယ်တွေကိုပေးချင်တာ ကျွန်တော့်ရဲ့ အတွေ့အကြုံတွေ၊ ရင့်ကျက်မှုတွေ၊ သင်ခန်းစာတွေ ဒါတွေကို နားလည်အောင်သင်ပေးနိုင်ဖို့ ကျွန်တော် ကျွမ်းကျင်တယ်။ ဒီလောက်ပါပဲ။

သင်ခန်းစာတွေကိုလည်းတိုးပြီးသင်ပေးပါဦးမယ်။ စာတွေလည်းတိုးပြီးရေးပေးပါဦးမယ်။ နေလည်းတော်တော်ကောင်းသွားပါပြီ။ အရင်တုန်းက ခဏခဏနေမကောင်းတာက သွေးထဲမှာ (LDL) မကောင်းတဲ့ကိုလက်စထရောတွေများနေလို့ပါ။ ကုပေးတဲ့ဆရာဝန်တွေက အဲ့ဒါကိုမစစ်မိလို့ သွေးကြောတွေကျဉ်းလာပြီးတောင်ဖြစ်မြောက်ဖြစ် ဖြစ်နေတာပါ။ အခု ကုပေးတဲ့ ဆရာ ဒေါက်တာဦးတက်ထွန်းချစ် က ဒါကိုတွေ့သွားပြီးအခုအဆီကျဆေးနှင့် သက်သာသွားပြီး သင်တို့အတွက် စာတွေအများကြီးရေးဖြစ်လို့ ဒီစာအုပ်ဖြစ်လာတာပါ။ ကျွန်တော့်ရဲ့ စာဖတ်ပရိသတ်၊ သင်တန်းသား/သူ ကျေးဇူးရှင်အပေါင်းလည်း ကျန်းမာချမ်းသာကြပါစေလို့ဆုတောင်းအပ်ပါတယ်။ တကယ်တော့လည်း သတ္တဝါအားလုံးကျန်းမာချမ်းသာရင်အကောင်းဆုံးပါပဲဗျာ။

စေတနာများစွာဖြင့်

ဇော်လင်း

စာရေးသူ



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 1

IP Addressing

ဒီစာအုပ်အတွက် ပထမဦးဆုံးသင်ခန်းစာအဖြစ် TCP/IP ရဲ့ IP Addressing အကြောင်းကို တင်ပြပေးလိုက်ပါတယ်။ ဒီနေရာမှာ သင်ခန်းစာ ၁ အနေနဲ့ IP Version 4 (IPv4) နှင့် သင်ခန်းစာ ၂ အနေနဲ့ IP Version 6 (IPv6) ရောနှစ်မျိုးစလုံးတင်ပြပေးသွားမှာဖြစ်ပါတယ်။ TCP/IP နှင့်ပတ်သက်ပြီး TCP/IP ဟာဘာယ်လိုဖြစ်တယ်။ ဘယ်တုန်းကပေါ်ခဲ့တယ် စသဖြင့် TCP/IP ရဲ့ History တွေ၊ နောက်ပြီး TCP/IP Protocol ရဲ့ Architecture တွေကိုပြန်မပြောတော့ပါဘူး။ အဲ့ဒီအကြောင်းတွေကို ကျွန်တော်ရေးသားထုတ်ဝေခဲ့ပြီးသော Network Essentials စာအုပ်မှာရေးသားခဲ့ပြီးဖြစ်လို့ပါ။

အခုလောလောဆယ်တော့ ရှင်းပြမယ့်သင်ခန်းစာနှင့် ဆက်စပ်မှုရှိသွားအောင် IP Address ရဲ့ Format နှင့် IP Class တွေအကြောင်းအရင်ရှင်းပြချင်ပါတယ်။ IPv4 ပေါ့များ။ ပြီးတော့မှ IPv6 အကြောင်း ပြောပြမယ်။

၁. ၁ **IPv4 Address** အကြောင်း

IP Address ဆိုတာ TCP/IP Protocol ကိုအသုံးပြုထားသော IP Network တစ်ခုမှာရှိတဲ့ Host (ကွန်ပျူတာ ပရင်တာ စသဖြင့်) တွေရဲ့ ID နံပါတ်ဖြစ်ပါတယ်။ လွယ်လွယ်ပြောရရင်တော့ Host တွေရဲ့ Identifier (ID Number) ပဲဖြစ်ပါတယ်။ ဒီနေရာမှာ Host လို့ပြောရတာက Network မှာရှိတဲ့ ကိုယ်ပိုင် ID တစ်ခုရထားတဲ့ ပစ္စည်းတိုင်းကိုဆိုလိုချင်လို့ဖြစ်ပါတယ်။ အကြောင့် Host ဟာကွန်ပျူတာလည်းဖြစ်နိုင်တယ်။ ပရင်တာလည်းဖြစ်နိုင်တယ်။ IP Address ပိုင်ဆိုင်တဲ့မည် သည့် ပစ္စည်းမဆိုဖြစ်နိုင်ပါတယ်။ ၎င်း Host တွေမှာ ရှိကြတဲ့ ID နံပါတ် (IP Address) ဟာတစ်ခုနှင့်တစ်ခုတူလို့မရပါဘူး။ ထပ်လို့လည်းမရပါဘူး။ - Unique ဖြစ်ရမယ်ပေါ့များ။ Unique ဆိုတာက ထပ်တူမရှိပေါ့။ ပြန်ပြောမယ်နော်။ IP Address ဆိုတာ IP Network မှာရှိတဲ့ Host တွေရဲ့ တစ်ခုနှင့်တစ်ခုမတူညီတဲ့ ID နံပါတ်ပဲ။ IP Address တစ်ခုဥပမာပြောရရင် -

192.10.15.1

ယခုဖော်ပြထားတဲ့ IP Address မှာ Decimal Format ဖြင့်ဖော်ပြထားတာဖြစ်ပါတယ်။ တကယ်တော့ IP Address ဟာသူ့ဘာသာသူ အလုပ်လုပ်တဲ့အခါ (0) နဲ့ (1) ပဲရှိတဲ့ Binary Format နဲ့အလုပ်လုပ်တာဖြစ်ပါတယ်။ $Base_2$ လို့ခေါ်တာပေါ့။ 192.10.15.1 ဟာ Decimal Format ဖြစ်ပြီး Base နဲ့ပြောရင် $Base_{10}$ ဖြစ်ပါတယ်။ ဒီတော့ 192.10.15.1 ကို Binary Format နဲ့ပြရင် -

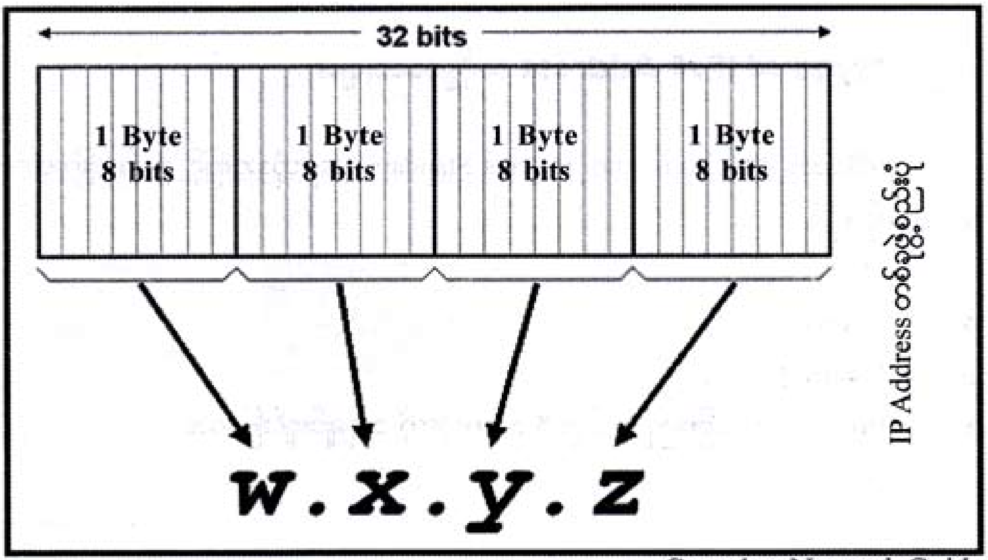
11000000.00001010.00001111.00000001

ဖြစ်ပါတယ်။

ဒါဟာ IP Address တကယ်အလုပ်လုပ်တဲ့ပုံစံဖြစ်ပါတယ်။ လူတွေကိုဖော်ပြတဲ့အခါ အဲ့ဒီပုံစံအတိုင်း ဖော်ပြမယ်ဆိုရင် မှတ်မိဖို့တယ်လွယ်မလဲ။ အဲ့ဒီအပြင် အလုပ်လုပ်ရတာလဲတွင်ကျယ်မှာမဟုတ်ဘူး။ ဒါကြောင့် Decimal ပုံစံနဲ့ပဲပြတာဖြစ်ပါတယ်။ ပြီးရင် IP Address တွေကို Decimal ကနေ Binary ပြောင်းတဲ့နည်းကို သင်ပေးမယ်။ အခုလောလောဆယ်တော့ ဒီ Decimal Format ကိုဘဲပြောပြစရာတွေရှိသေးတယ်။

ဒီ 192.10.15.1 ဆိုတဲ့ Address ကိုကြည့်ရအောင်။ 192 နဲ့ 10 ကြားမှာအစက်တစ်စက်ရှိတယ် ဆိုလို့ပြောရင်တော့ Dotted Decimal Location လို့ခေါ်တယ်။ 192 ဆိုတဲ့ ဂဏန်းဟာ Byte အရပြောရင် 1 Byte ရှိတယ်။ သူ့ကို Octet လို့လဲခေါ်တယ်။ ဒီတော့ပြောရရင် 192 ဆိုတာက Octet တစ်ခု၊ 10 ကလဲ Octet တစ်ခု၊ 15 ကလဲ Octet တစ်ခု၊ 1 ကလဲ Octet တစ်ခုဖြစ်တယ်။ Octet တစ်ခုချင်းစီကို Dot ဆိုတဲ့ အစက်ကလေးနဲ့ ခြားထားတာဖြစ်တယ်။ Octet တစ်ခုခြင်းစီဟာ 1 Byte တနည်းအားဖြင့် 8 Bit စီရှိကြပါတယ်။ ဒီတော့ IP Address တစ်ခုမှာ 4 Octet ရှိတာကြောင့် Byte အရပြောရင် 4 Byte ရှိပြီး Bit အရပြောရင် 31 Bit ရှိပါတယ်။ Octet တစ်ခုဟာအတိုင်းအတာအားဖြင့် 0 ကနေမှ 255 ထိဘဲရှိတယ်။ ဆိုလိုချင်တာက 192 ဆိုတဲ့နေရာမှာ 192 မဟုတ်ပဲတစ်ခြားဂဏန်းတစ်ခုဖြစ်ခဲ့မယ်ဆိုရင် အဲ့ဒီ ဂဏန်းဟာ 0 ကနေ 255 ထိအတွင်းပဲဖြစ်ရမယ်။

ပုံ ၁.၁



IP Address တစ်ခုဖွဲ့စည်းပုံ

Complete Network Guide

ပြန်ပြောပြမယ် IPv4 ရဲ့ IP Address တစ်ခုဟာ Decimal Format နဲ့သာဖော်ပြမယ်ဆိုရင် Octet 4 ခုရှိတယ်။ Octet တစ်ခုခြင်းစီမှာ ရှိတဲ့ဂဏန်းဟာ 0 ကနေ 255 အတွင်းဘဲဖြစ်ရမယ်။ တစ်ခုစီရဲ့ အရွယ်အစားဟာ Byte အရပြောရင် 1Byte ရှိပြီး Bit အရပြောရင် 4 bit ရှိတယ်။ ဒီတော့ IP Address မှာ 4 Octet ရှိတာကြောင့် Address တစ်ခုရဲ့ Size ဟာ Byte အရပြောရင် 4 Bytes ရှိပြီး Bit အရပြောရင် 32 bit ရှိတယ်လို့ပြောတာဖြစ်ပါတယ်။ ပုံ ၁.၁ က သင့်ကို ပိုပြီးရှင်းသွားစေမှာပါ။

Address တွေဟာ Network တစ်ခုထဲမှာ တူညီမှုမရှိရပါဘူး။ တစ်နည်းအားဖြင့်ပြောရရင် Network တစ်ခုထဲမှာရှိတဲ့ IP Address တွေဟာ တစ်ခုနှင့်တစ်ခု မတူညီရပါဘူး။ ဒီတော့က တစ်ကမ္ဘာလုံး အနှံ့သုံးနေတဲ့ World Wide IP Network ကြီးမှာ ဒီ IP Address တွေကိုတစ်ခုနှင့်တစ်ခုထပ်မသွားအောင် ဘယ်သူတွေက ကြီးကြပ်ပေးနေတာလဲဆိုတော့ IANA ဆိုတဲ့ Internet Assign Numbers Authority ဆိုတဲ့အဖွဲ့အစည်းကြီးကဖြစ်ပါတယ်။ Internet ဆိုမှ Internet နဲ့ပတ်သက်တာပြောရဦးမယ်။ အချို့သော IP Address တွေဖြစ်ကြတဲ့ 10.0.0.0/8၊ 172.16.0.0/12 နှင့် 192.168.0.0/16 စသည်တို့ကို တစ်သီးတစ်ခြားသော Private Network အတွက်ဖယ်ထားခြင်းကြောင့် ၎င်း IP Address တွေကို Internet မှာ အသုံးမပြုပါဘူး။ တစ်နည်းအားဖြင့်ပြောရရင် ၎င်း IP Address တွေကို Internet မှာတွေ့ရမှာမဟုတ်ပါဘူး။ 10.0.0.0/8 မှာ /8 ဆိုတာ Subnet Mask ကို အတိုကောက်ရေးထားတာဖြစ်တယ်။ IP Address တွေမှာသူတို့နဲ့အတူတွဲပြီးဖော်ပြလေ့ရှိတဲ့ Subnet Mask ကို အတိုကောက်ဖော်ပြချင်ရင် အခုလိုမျိုး (/) ခံပြီးဖော်ပြလို့ရတယ်။ အဲ့ဒီအကြောင်းကို ဒီသင်ခန်းစာမှာဘဲ နောက်ပိုင်းမှာရှင်းပြသွားမှာဖြစ်ပါတယ်။

အခုတစ်ခါရှင်းပြမယ့်အကြောင်းအရာက IP Class တွေရဲ့ အကြောင်းအရာပဲဖြစ်ပါတယ်။

၁.၂ **Types of IPv4 Address အမျိုးအစားများ**

ကဲဒီတော့ IP Address ဟာ Internet Standard အရ ဘုံအားဖြင့် ၃ မျိုးခွဲခြားထားတယ်ဗျ။ အဲ့ဒါက ပြောရရင် -

၁။ Unicast

၂။ Multicast

၃။ Broadcast တို့ပဲဖြစ်ကြတယ်ဗျ။ ဒီ ၃ ခုစလုံးကို ၁ ခုချင်းရှင်းပြမယ်။

၁.၃ IPv4 Unicast Address ဆိုတာ

ဒီ Unicast Address ကိုသတ်သတ်မှတ်မှတ် သတ်မှတ်ထားတဲ့ Network တစ်ခုမှာပဲ အသုံးပြုတယ်။ သူ့ကို One to One Communication လို့ခေါ်ပါတယ်။ ကျွန်တော်တို့အသုံးပြုနေတဲ့ ရင်းနှီးနေတဲ့ IP Address တွေက Unicast Address တွေပဲဖြစ်ပါတယ်။ One to One Communication ဆိုတာ တနည်းအားဖြင့် ပြောရရင် Point to Point ဖြစ်ပါတယ်။ ဆိုလိုတာက IP Address တစ်ခုကနေပို့လိုက်တဲ့ အကြောင်းအရာတစ်ခုဟာ အဲ့ဒီ ကွန်ယက်ထဲမှာပဲရှိတယ်။ နောက် IP Address တစ်ခုက လက်ခံနိုင်မယ်။ Very Simple၊ Point တစ်ခုပို့လိုက်တဲ့ အကြောင်းအရာကို နောက် Point တစ်ခုကလက်ခံနိုင်မယ်။ လက်ခံတဲ့ Point ဟာလည်း ပို့လိုက်တဲ့ Point နှင့် ကွန်ယက်တစ်ခုတည်းပဲဖြစ်ရမယ်။

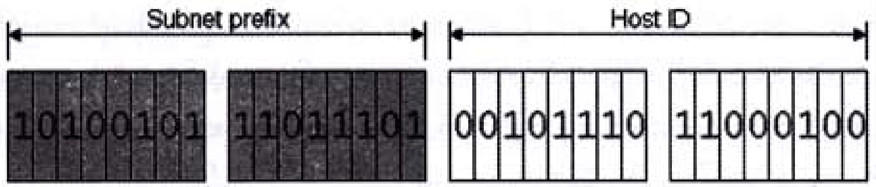
ဒီနေရာမှာ Unicast Address ကိုရှင်းရင်းနဲ့ Multicast Address အကြောင်းပြောပြသွားမယ်။ ဒါမှ Unicast အကြောင်းကိုပိုနားလည်သွားမယ်။

Multicast ဆိုတာ တစ်ခု သို့မဟုတ် တစ်ခုထက်ပိုသော Network များဆီက One to Many Communication ကိုဆိုလိုတာ ဖြစ်ပါတယ်။ Point to Point မဟုတ်ပဲ၊ Point to Many ဖြစ်ပါတယ်။ IP Address တစ်ခုကနေပေးပို့လိုက်တဲ့ အကြောင်းအရာတစ်ခုဟာ အခြားသော IP Address အများကြီးဆီကနေလက်ခံနိုင်မှာဖြစ်ပါတယ်။ လက်ခံနိုင်တဲ့ IP Address တွေဟာလည်း ပို့လိုက်တဲ့ IP Address နှင့် ကွန်ယက်တစ်ခုတည်းက ဖြစ်ချင်မှဖြစ်မယ်။ အခြားသောကွန်ယက်တွေကလည်းဖြစ်နိုင်တယ်။ ဒါကို Point to Many Communication လို့ခေါ်ပါတယ်။

ဒီတော့ Point to Point Communication ဆို Unicast ဖြစ်ပြီး၊ Point to Many Communication ဆို Multicast ဖြစ်ပါတယ်။ OK နော် OK.

ခု Unicast Address အကြောင်းပြန်ဆက်ဦးမယ်။ IPv4 ရဲ့ Unicast Address မှာ Subnet Prefix နှင့် Host ID Portion ဆိုပြီးရှိတယ်ဗျ။ အပိုင်း ၂ ပိုင်းရှိတယ်ပေါ့ဗျာ။

ပုံ ၁.၂



IP Address တစ်ခု၏ အပိုင်း ၂ ပိုင်း ဖွဲ့စည်းပုံ

❖ Subnet Prefix ဆိုတာက Network Address (Network ကိုရည်ညွှန်းသောအပိုင်း) ဖြစ်ပါတယ်။ ကွန်ယက်တစ်ခုတည်း အတွင်းမှာရှိတဲ့ Node တွေအားလုံးဟာ တူညီတဲ့ Subnet Prefix ရှိရမှာဖြစ်ပါတယ်။ ကွန်ယက်တစ်ခုတည်းမှာပဲ ရှိကြတာကို။

❖ Host ID ဆိုတာကတော့ Node (ကွန်ပျူတာ၊ ပရင်တာ) တွေရဲ့ Address ပဲဖြစ်ပါတယ်။ ဒီ Node တွေအားလုံးဟာNetwork Segmant တစ်ခုအတွင်းမှာရှိခဲ့မယ်ဆိုရင် သူတို့ရဲ့ Host ID ဟာ တစ်ခုနှင့်တစ်ခု ထပ်တူမရှိရပါဘူး။

ကဲဒီအကြောင်းတွေကို ဇကားပြေပုံစံပြန်ရှင်းပြမယ်။

ကောင်းပြီ IP Address မှာအပိုင်းအားဖြင့် နှစ်ပိုင်းရှိတယ်ဗျ။

အဲ့ဒီ နှစ်ပိုင်းကတော့ Network ပိုင်းနှင့် Host ပိုင်းပဲဖြစ်ပါတယ်။ Network ပိုင်းဆိုတာ Network ရဲ့လိပ်စာဖြစ်ပြီး Host ပိုင်းဆိုတာ အဲ့ဒီ Network မှာချိတ်ဆက်ထားတဲ့ ကိုယ်ပိုင် IP Address တစ်ခုစီရှိကြတဲ့ Computer, Printer တို့ရဲ့ လိပ်စာတွေဖြစ်ပါတယ်။ ပြန်ပြောပြမယ် IP Address တစ်ခုမှာ အပိုင်းအားဖြင့် နှစ်ခုရှိတယ်။ တစ်ပိုင်းက Network ပိုင်းဖြစ်ပြီး တစ်ပိုင်းက Host ပိုင်းဖြစ်တယ်။ တကယ်တော့ IP Address မှမဟုတ်ဘူး Network မှာသုံးတဲ့ Address တော်တော် များများမှာ ပျမ်းမျှခြင်းအားဖြင့် Network ပိုင်းနှင့် Host ပိုင်းဆိုပြီးရှိကြတယ်။ ဒီသင်ခန်းစာဟာ ပါးစပ်နှင့် ရှင်းပြရင်တောင် နည်းနည်းဝေးတာကြောင့် သင်ဟာတစ်ခေါက်ဖတ်လို့မှ နားမလည်ရင် အကြိမ်ကြိမ်ပြန်ဖတ်ဖို့တော့လိုပါတယ်။ ဥပမာပြောရရင် ကိုဇော်လင်း ဘယ်မှာနေလဲ။ ကျွန်တော်ကတော့ဖြင့် ၁၆ ရပ်ကွက်၊ အိမ်နံပါတ် ၆၉ မှာနေပါတယ်လို့ ကိုဇော်လင်း ကပြောတယ်။ ဒါကို အောက်ပါပုံစံအတိုင်း ရေးကြည့်မယ်။

၁၆း၆၉ ဟုတ်ပြီ။

၁၆း၆၉ ဟာ လိပ်စာတစ်ခုဆိုကြပါစို့။ တွေ့လား။ အဲ့ဒီလိပ်စာမှာလည်း အပိုင်းနှစ်ပိုင်းရှိတယ်။ ၁၆ ဟာ ရက်ကွက်ကို ရည်ညွှန်းတာဖြစ်ပြီး ၆၉ ဟာ အိမ်နံပါတ်ဖြစ်တယ်။ ဒါ ဥပမာပေးပြီး ရှင်းပြနေတာနော်။ အဲ့ဒီတော့ IP Address မှာ Network ပိုင်းဆိုတာက ရပ်ကွက်ကို ရည်ညွှန်းချင်တာဖြစ်ပြီး Host ကအိမ်နံပါတ်ပဲဖြစ်ပါတယ်။ ဒီအချိန်မှာ ကိုဇော်လင်း ခင်ဗျား ဘယ်မှာနေလဲလို့မေးတဲ့သူက ဟာဟုတ်လား ကျုပ်လဲ ၁၆ ရပ်ကွက်မှာနေတာဘဲ။ ဒါဆို ကျုပ်တို့က တစ်ရက်ကွက်တည်းသားတွေပေ့ါ။ ဒါပေမယ့် ကျုပ်ရဲ့ အိမ်နံပါတ်ကတော့ ၁၈ ဖြစ်တယ်။ ဒီတော့ကား သူ့ရဲ့ Address ကို ဘယ်လိုရေးမလဲ။

၁၆း၁၈ ပေ့ါ။

ဒီတော့ အဲ့ဒီနေရာမှာ ၁၆ ကရပ်ကွက်နံပါတ်ဖြစ်ပြီး ၁၈ က အိမ်နံပါတ်ဖြစ်တယ်။ တစ်နည်းအားဖြင့်

ပြောရရင် ၁၆ ဟာ Network Address ဖြစ်ပြီး၊ ၁၈ ဟာ Host Address ဖြစ်တယ်။ ဒီတော့ အဲ့ဒီလူနဲ့ ကိုဇော်လင်း ဟာ အိမ်နံပါတ်ပဲ မတူတာ။ ရပ်ကွက်ကတော့တူတယ်။ တစ်နည်းအားဖြင့်ပြောရရင် Host Address သာမတူတာ Network Address တွေတူ ကြတယ်။ ဒီအချိန်မှာဘေးကရပ်ကြည့်နေတဲ့လူ က ကျွန်တော်ကတော့ အိမ်နံပါတ် ၆၉ မှာနေတာပဲ။ ကိုဇော်လင်းနဲ့ အိမ်နံပါတ် အတူတူပဲဗျဆိုပြီးပြောလာတယ်။ တဲတဲ ဒီမှာကိုယ့်လူ အိမ်နံပါတ်တူနေရင်တော့ ရပ်ကွက်တော့မတူနိုင်ဘူး။ ဟုတ်ပါတယ်။ ကျွန်တော်က ၃ ရပ်ကွက်မှာနေပါတယ်လို့ သူကပြန်ပြောတယ်။ ဒီတော့ သူ့ရဲ့ Address ကိုရေးရင် ၃း၆၉ ပေါ့။ ကဲဒီဥပမာပေးပြီးရှင်းပြနေတာ။ ဒီဥပမာကိုဘဲ ဇာတ်ရည်လည်အောင် နိဂုံးချုပ်ပြမယ်။

ကိုဇော်လင်းရဲ့ လိပ်စာ	=၁၆း၆၉
ပထမလူရဲ့ လိပ်စာ	=၁၆း၁၈
ဒုတိယလူရဲ့ လိပ်စာ	=၃း၆၉

ကောင်းပြီ အဲ့ဒီလူသုံးယောက်ရဲ့ လိပ်စာ (း) ရဲ့ရှေ့က ရပ်ကွက်နံပါတ်။ တနည်းအားဖြင့် Network Address ဖြစ်ပြီး၊ (း) ရဲ့နောက်ကအိမ်နံပါတ်။ တနည်းအားဖြင့် Host Address ဖြစ်တယ်။ ဒီဥပမာပေးထားတဲ့ လိပ်စာသုံးခုလုံးကိုကြည့်လိုက် ထပ်တူကျနေတယ်ဆိုတာမရှိဘူး။ ရပ်ကွက်တူရင် အိမ်နံပါတ်မတူဘူး။ အိမ်နံပါတ်တူရင် ရပ်ကွက်မတူဘူး။ ဒီတော့ကား IP Address မှာလဲ Network အပိုင်းနဲ့ Host အပိုင်းဆိုပြီး နှစ်ပိုင်းရှိတယ်။

IP Address ဟာ Octet အားဖြင့် လေးခုရှိတယ်။

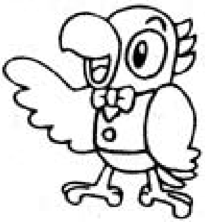
ဥပမာ192.10.15.1

ကောင်းပြီ အဲ့ဒီ ဂဏန်းလေးလုံးဟာ ဘယ်ဂဏန်းက Network ပိုင်းဖြစ်လို့ ဘယ်ဂဏန်းက Host ပိုင်းဖြစ်သလဲ။ အဲ့ဒါပြောချင်တာ။ အဲ့ဒါပဲ IP Address တစ်ခုကိုကြည့်လိုက်လျင် Octet လေးခုရှိတယ်။ ပုံ ၁.၁. ကိုပြန်ကြည့်ပါ။ အဲ့ဒီထဲက ဘယ် Octet ကတော့ဖြင့် Network Address ကိုရည်ညွှန်းလို့ ဘယ် Octet ကတော့ Host အပိုင်းကိုရည်ညွှန်းတယ်ဆိုတာ ဘယ်လိုသိနိုင်မလဲ။ ဟုတ်ကဲ့ စပြီးရှင်းပြပါတော့မယ်။

IP Address မှာ Octet လေးခုရှိတဲ့အထဲကမှ ပထမ Octet ကိုကြည့်လိုက်တာနဲ့ ဒီ Address ရဲ့ ဘယ် Octet ကတော့ဖြင့် Network Address ကိုရည်ညွှန်းပြီး၊ ဘယ် Octet ကတော့ Host ကိုရည်ညွှန်းတယ် ဆိုတာသိနိုင်ပါတယ်။

ပုံ ၁.၃

ပထမ Octet ကိုကြည့်လိုက်တာနဲ့ သိနိုင်တယ်



ဒီတော့ 192.10.15.1 မှာ 192 ကိုကြည့်လိုက်တာနဲ့ သိနိုင်တယ်လို့ဆိုလိုချင်တာဖြစ်ပါတယ်။ OK နော်။ ပထမဦးဆုံး Octet ကိုပဲကြည့်ရတာ။ ဒီပထမဦးဆုံး Octet ကိုအသုံးပြုပြီးတော့ဘဲ IP Class တွေခွဲသွားတာဖြစ်တယ်။ IP Class ဆိုတာ လွယ်လွယ်ပြောရင် အမျိုးအစားခွဲထားတာပဲ။

IP Class (5) မျိုးရှိတယ်။

၁။ Class A

၂။ Class B

၃။ Class C

၄။ Class D

၅။ Class E ဆိုပြီးတော့ဖြစ်ပါတယ်။

အမျိုးအစား ၅ မျိုးပေါ့ဗျာ။ အဲ့ဒီ Class 5 ခုထဲမှ လူတွေကိုပေးသုံးတာက Class A ရယ်၊ Class B ရယ်၊ Class C ရယ်ဘဲဖြစ်ပါတယ်။ ဒါကြောင့် လူတော်တော်များများဟာ Class D နဲ့ E ကိုမပြောကြဘူး။ အောက်ပါတို့ကိုမှတ်ထားရမယ်။

- ❖ ထိပ်ဆုံး Octet ရဲ့ ဂဏန်းဟာ (၁) ကနေမှ (၁၂၆) အတွင်းဖြစ်ခဲ့ရင် ဒါဟာ Class A ဖြစ်တယ်။
- ❖ ထိပ်ဆုံး Octet ရဲ့ ဂဏန်းဟာ (၁၂၈) မှ (၁၉၁) အတွင်းဖြစ်ခဲ့ရင် Class B ဖြစ်ပြီးတော့
- ❖ ထိပ်ဆုံး Octet ရဲ့ ဂဏန်းဟာ (၁၉၂) မှ (၂၂၃) အတွင်းဖြစ်ခဲ့ရင် ဒါဟာ Class C ဖြစ်ပါတယ်။
- ❖ ထိပ်ဆုံး Octet ရဲ့ ဂဏန်းဟာ (၂၂၄) မှ (၂၃၉) ဖြစ်ခဲ့ရင် Class D ဖြစ်ပြီး
- ❖ ထိပ်ဆုံး Octet ရဲ့ ဂဏန်းဟာ (၂၄၀) မှ (၂၅၄) ဖြစ်ခဲ့ရင် Class E ဖြစ်ပါတယ်။

ကဲဟုတ်ပြီလား။ IP Class 5 ခုရှိတယ်ဆိုပေမယ့်လည်း တကယ်တမ်းတော့ မှတ်ရမှာ Class A, B, C ပဲ။ IP Class တစ်ခုဟာ Class A ကလား၊ Class B ကလား၊ Class C ကလား သိချင်ရင် ၄င်း IP Address ရဲ့ရှေ့ဆုံး Octet ကိုပဲကြည့်ရတာပါ။

IANA အဖွဲ့ကြီးက Class A ကနေ Class C အထိပဲ သတ်မှတ်ပေးထားတာဖြစ်ပြီး Class D

ကိုတော့ Multicast အတွက်ချန်ထားပါတယ်။ Class E ကိုတော့ အနာဂတ်မှာ အသုံးပြုဖို့အတွက် ဆိုပြီး ချန်ထားပါတယ်။

အခု IP Address တစ်ခုကိုကြည့်လိုက်တာနှင့် Class A ကလား၊ B ကလား၊ C ကလား ဆိုပြီး ခွဲတတ်သွားပြီ။ ဆက်ပြောပြမှာက Class A ဆိုရင် IP Address ရဲ့ Octet လေးခုထဲက ဘယ် Octet ကတော့ဖြင့် Network ပိုင်းဖြစ်ပြီး၊ ဘယ်အပိုင်းကတော့ဖြင့် Host ပိုင်းဖြစ်တယ်ဆိုတာပဲ။ ဆက်လေ့လာကြည့်ရအောင်၊ စိတ်ဝင်စားဖို့ကောင်းပါတယ်ဗျာ။ သေချာဖတ်နော်။ မပျင်းရဘူး။ ဆက်တိုက်မဖတ်နိုင်ရင် နားနားပြီးဖတ် မှာမယ်။

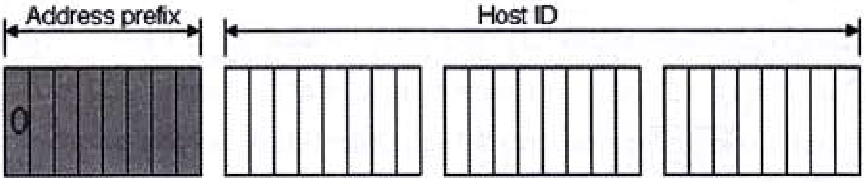
အခု Class 5 ခုရှိတဲ့အထဲကမှ Class A, B နှင့် C Address တွေရဲ့ ဘယ်အပိုင်းက Network ပိုင်း၊ ဘယ်အပိုင်းက Host အပိုင်းလည်းဆိုတာကိုပြောပြတော့မယ်။ Class A , B နှင့် C ဟာ အခုရှင်းပြတဲ့ Unicast Address အတွက်အသုံးပြုပြီး၊ Class D ကတော့ Multicast အတွက်အသုံးပြုပါတယ်။ Class E ကျတော့ တစ်ချို့လည်း Experiment အတွက်လို့ပြောတာပါပဲ။

၁.၄ **High Order Bit အကြောင်း**

IP Address မှာ သူ့ဘာသာသူ ဒီ Address ဟာ Class A ကလား၊ Class B ကလား၊ Class C ကလား ခွဲခြားဖို့အတွက် High Order Bit ကိုပုံသေ အောက်ပါအတိုင်းသတ်မှတ်ပါတယ်။ ပြန်ပြောပြမယ်။ High Order Bit ဆိုတာ 32 bits သော IP Address ရဲ့ရှေ့ဆုံး Bit တွေမှာနေရာယူပါတယ်။

❖ Class A ဆိုရင် 0 ဖြစ်ပါတယ်။ ရှေ့ဆုံး 1 bit ပဲနေရာယူတာပါ။ ဒီပုံသေပဲ။

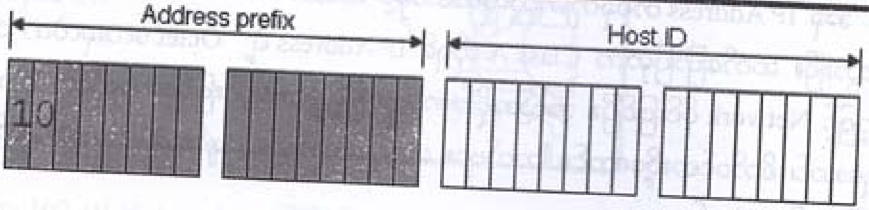
ပုံ ၁.၄



Class A ၏ High Order Bits နှင့် Network Portion & Host Portion ကိုပြသောပုံ

❖ Class B ဆိုရင် 1 0 ဖြစ်ပါတယ်။ ရှေ့ဆုံး 2 bits ယူပါတယ်။ ဒါလည်းပုံသေပဲ။

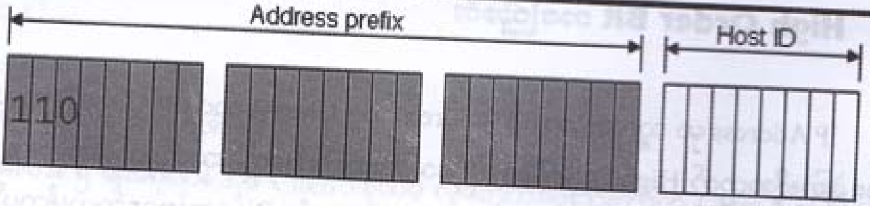
ပုံ ၁.၅



Class B ၏ High Order Bits နှင့် Network Portion & Host Portion ကိုပြသောပုံ

❖ Class C ဆိုရင် 1 1 0 ဖြစ်ပါတယ်။ ရှေ့ဆုံး 3 bitsယူပါတယ်။ ဒါလည်းပုံသေပဲ။

ပုံ ၁.၆



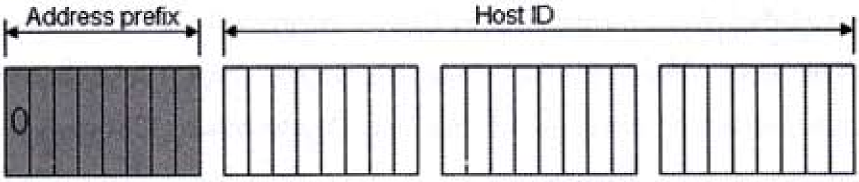
Class C ၏ High Order Bits နှင့် Network Portion & Host Portion ကိုပြသောပုံ

ဒီ High Order Bit ကိုကြည့်ပြီး IP Address တွေဟာ Class A , B, C ခွဲတာဖြစ်ပါတယ်။ ဒါသူ့ဘာသာသူကြည့်လို့နော်။ ကျွန်တော်တို့ကျတော့ ဒီလို Bit နှင့်မကြည့်ဘဲ Class A ဆိုရင် 1 ကနေ 126 အထိ၊ Class B ဆိုရင် 128 ကနေ 191 အထိ၊ Class C ဆိုရင် 192 ကနေ 223 အထိဆိုပြီး၊ ရှေ့ဆုံး Octet ရဲ့ ဂဏန်း ကိုကြည့်ပြီးခွဲတာပါ။ အခု ဒီ High Order Bit ကိုနားလည်မှ အောက်ကသင်ခန်းစာကို နားလည်မှာဖြစ်ပါတယ်။

၁.၅ Class A Network အကြောင်း

Class A Address တွေဟာ Host ပေါင်းမြောက်များစွာပါဝင်တဲ့ Network တွေအတွက် ရည်ရွယ်ပါတယ်။ IP Address တွေမှာ 4 Octets ရှိပါတယ်။ Octet တစ်ခုဟာ 1 bytes= 8 bits ဖြစ်တာကြောင့် 4 bytes ဆိုတော့ 32 bits ဖြစ်ပါတယ်။ Class A မှာ ပထမဦးဆုံး Octet ဟာ Address Prefix ဖြစ်ပါတယ်။ တနည်းအားဖြင့်ပြောရရင် Network Address ဖြစ်ပါတယ်။ ပုံကိုကြည့်ပါ။ ပုံကတော့ ရှေ့ကပုံပဲ။

ပုံ ၁.၇



Class A ၏ High Order Bits နှင့် Network Portion & Host Portion ကိုပြသောပုံ

ပုံမှာမြင်ရတဲ့အတိုင်း Octet 4 ခုကို 8 bits ပုံစံ အကန့် ၈ ကန့်နှင့် ၄ ပိုင်းခွဲပြထားပါတယ်။ အဲ့ဒီမှာ ပထမဆုံး Octet အကန့် ၈ ကန့်ဟာ Network Address ဖြစ်ပြီး ကျန် ၂၄ ကန့် (3 Octets) ကတော့ Host ID ဖြစ်ပါတယ်။ ဘယ်လိုလည်းဆိုတော့ 32 bits ထဲက ရှေ့ဆုံး 8 bits ကိုနှုတ်တော့ 24 bits ကျန်ပါတယ်။ ပြန်ပြောပြမယ် IP Address တစ်ခုမှာ 4 Octets ရှိတယ်။ 1 Octet မှာ 1 Byte တနည်း အားဖြင့် 8 bits ရှိတယ်။ Byte နှင့်မပြောတော့ဘူး။ Bit နှင့်ပြောပါ့မယ်။ ဒီတော့ အားလုံးပေါင်းရင် IP Address တစ်ခုမှာ 32 bits ရှိပါတယ်။

Class A မှာ ပထမ 8 bits ဟာ Network Address ဖြစ်ပြီး၊ ကျန် 24 bits ဟာ Host ID ဖြစ်ပါတယ်။ ဥပမာပြောရရင် 121.10.15.1 မှာ 121 ဟာ Network Address ဖြစ်ပြီး၊ ကျန်တာက Host ID ဖြစ်ပါတယ်။

Class A Network မှာ Network ပေါင်း ဘယ်လောက်ရှိလို့၊ Host ပေါင်းဘယ်လောက်ရှိတယ်ဆိုတာ တွက်ပြပါ့မယ်။ IP Address မှာ 32 bits ထဲက Class A ဟာ Network ပိုင်းအတွက် 8 bits ပဲရတာဖြစ်ပါတယ်။ အဲ့ဒီ 8 bits မှာမှ High Order Bit အတွက် ရှေ့ဆုံးမှာ 0 လို့ သတ်မှတ်ပါတယ်။ Class A Network ဆိုရင် High Order Bit ဟာ 0 ဖြစ်ပါတယ်။ ပုံမှာလည်းပြထားပါတယ်။ ဒီ High Order Bit ကိုသတ်မှတ်လိုက်တာကြောင့် ခုနကပြောတဲ့ 8 bits မှာ 7 bits ပဲကျန်ပါတော့တယ်။ 7 bits ဆိုတာ 2^7 ဖြစ်

ပါတယ်။ အဓိပ္ပာယ်က "2" ကို "7" ခါ မြှောက်ပါ။

2 x 2 x 2 x 2 x 2 x 2 x 2 = အဖြေ 128 ရပါတယ်။

ဘာဖြစ်လို့ High Order Bit ကို 1 bit စာဖယ်ရသလဲဆိုတော့ ဒီ High Order Bit ကိုကြည့်ပြီး Class A , B ,C စသဖြင့်ခွဲတာဖြစ်ပါတယ်။ ပြန်ပြောပြမယ် High Order Bit ဆိုတာ IP Class တွေခွဲဖို့ Class A ဆိုရင် အဲ့ဒီ Bit တွေရဲ့ရှေ့ဆုံးမှာ 1 bit စာနေရာယူတယ်။ အဲ့ဒီ Bit ဟာလည်း ပုံသေ "0" ပဲ။ Class A အတွက်ကိုပြောတာ။

ပြန်ချုပ်ပြီးပြောပြမယ်။ အခုပြောနေတာ Class A အတွက်ပဲ။ 32 bits ရှိတဲ့အထဲက Network အတွက် 8 bits ဖယ်။ အဲ့ဒီထဲကမှ High Order Bit အတွက် ရှေ့ဆုံး 1 bit ဖယ်ရတယ်။ ဒီတော့ Network Address အတွက် 7 bits ပဲကျန်တယ်။ အဲ့ဒီ 7 bits ကိုတွက်လိုက်တော့ 128 ရတယ်။ တကယ်ဆိုရင် ဒီနေရာမှာ 2^8((၂) ၈–ထပ်) ဖြစ်ရမှာ။ ၂– ၈ထပ်ဆို ၂၅၆ ရတယ်။ ခုတော့ High Order Bit ကို1 bit ဖယ်ရတာကြောင့် 7 bits ပဲကျန်ပြီး၊ 128 ပဲရတယ်။

၁.၆ **Class A Network 126 အထိပဲရခြင်းအကြောင်း**

ဒီတော့ Class A ဟာ 1 ကနေမှ 128 အထိရှိရမှာဖြစ်ပါတယ်။ ဒါပေမယ့် ကျွန်တော်ရှေ့မှာပြောခဲ့ဖူးတယ်။ Class A ဟာ 1 ကနေမှ 126 အထိပဲရတယ်။ တကယ်ဆို 1 ကနေမှ 128 အထိရရမှာ။ 126 အထိပဲဘာဖြစ်လို့ရသလဲဆိုတော့–

၁။ 128 ကို Binary ပြောင်းလိုက်ရင် 1 0 0 0 0 0 0 0 ရတယ်ဗျ။ Binary ဘယ်လိုပြောင်းရသလဲဆိုတာကို ကျွန်တော်နောက်တော့ ပြောပြမယ်။ ခုလောလောဆယ် 128 ကို Binary ပြောင်းရင် 1 0 0 0 0 0 0 0 ရတယ်။ အဲ့ဒီ ဂဏန်းအားလုံးမှာ ရှေ့ဆုံး ဂဏန်းက "1" ဖြစ်နေတယ်လေ။ Class A ရဲ့ High Order Bit အရ ရှေ့ဆုံး ဂဏန်းဟာ "0" ဖြစ်မှရမယ်။ ဒါကြောင့် Class A Network မှရှေ့ဆုံး Octet ကို 128 အထိပေးလို့မရဘူး။ 128 အောက်ငယ်တဲ့ ဂဏန်းတွေကို Binary ပြောင်းရင် "0" ကစတယ်။ ပြောင်းလို့ရလာတဲ့ ဂဏန်း "၈" လုံးရဲ့ရှေ့ဆုံးဂဏန်းက "0" ဖြစ်တယ်။ ဒါကြောင့် Class A Network မှ 7 Bits ကို "၂" (၇) ခါမြှောက်တော့ 128 ရသော်ငြားလည်း Class A မှာ 128 အထိပေးလို့မရဘူး။

၂။ ဒါဆို 127 အထိရနိုင်သလား။ 127 ဟာ Loopback Test (Loopback Address) အဖြစ် Reserved လုပ်ထားတာကြောင့် 127 အထိလည်းမရပြန်ဘူး။ ဒါကြောင့် Class A Network ဟာ "1" ကနေမှ "126" အထိပဲရရခြင်းဖြစ်တယ်။

အချုပ်ပြောရမယ်ဆိုရင် IP Address မှာ Octet (၄) ခုရှိတယ်။ ပထမဦးဆုံး Octet ဟာ "1" ကနေ "126" အတွင်းပဲဖြစ်ရမယ်။ ဒါကိုပြောတာ။

၁.၄ Class A Host အရေအတွက်

Network တစ်ခုမှာ Host ပေါင်းဘယ်လောက်ရှိသလဲဆိုတော့ 4 Octets ရှိတဲ့အထဲက ပထမ Octet က Network အတွက်၊ ကျန် Octet က Host ဆိုတော့ 3 Octets ဆိုတော့ 24 bits. "2" ကို 24 ခါမြှောက်ကြည့်။ 16,777,216 ရတယ်။

အဲ့ဒါ Class A Network တစ်ခုမှာရှိတဲ့ Host (ကွန်ပျူတာ၊ ပရင်တာ) ရဲ့အရေအတွက်ပဲဖြစ်တယ်။ ဒီတော့ Class A မှာ Network ပေါင်း 126 ခုပဲရှိတယ် ဆိုပေသိ အဲလေ ဆိုပေမယ့် Network တစ်ခုမှာရှိတဲ့ Host အရေအတွက်က ၁၇ သန်းနီးပါးရှိတယ်။ Network ကြီးက အကြီးကြီးပေါ့။

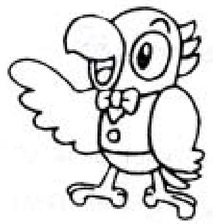
ပိုပြောသလို ဇာတ်ရည်လည်အောင်ရှင်းပြမယ်။ ကျွန်တော့်ကို IP Address တစ်ခုလောက် ရောင်းပါဗျာ။ ကဲ ရောင်းမယ်။ မင်းက ငါတို့ဆီမှာ Address လာဝယ်တဲ့သူကြားက 124 ယောက်မြောက်။ ဒါကြောင့် မင်းရဲ့ Address က 124 လို့ IANA ကပြောတယ်။ မင်းက Class A Network 124 ခုမြောက်ရမယ်။ ယူမှာလား။ ယူမယ်။ ကောင်းပြီ။ ဒါဆို မင်းရဲ့ Address က 124.x.x.x ပဲ။

x.x.x ကဘာလဲ။ မင်းတိုင်းပြည်ရောက်မှ မင်းဘာသာမင်း အစားထိုးရမယ့် Host ID နေရာပဲ။ ဆိုလိုတာက Class A Network မှာ ရှေ့ဆုံး Octet ကိုပဲ သူတို့က Control လုပ်တယ်။ ကျန်တဲ့ Octet 3 ခုက ကိုယ့်ဘာသာကို သတ်မှတ်ရမှာ။ ဒီ "x" (ကြက်ခြေခတ်) Octet တစ်ခုမှာ 8 bit, ၃ ခုဆိုတော့ 24 bits။ ဒါဆို ၂ ကို ၂၄ ခါ မြှောက်လိုက်ရင် 16,777,216 ရရော့။ ဒီတော့ Class A Network တစ်ခုပိုင်ဆိုင်သွားသူဟာ Host ပေါင်း 16,777,216 ပြန်ရောင်းလို့ရပါတယ်။ ဒါပေမယ့် သိရမှာက Host ID မှာ ရှေ့ဆုံး Address နဲ့ နောက်ဆုံး Address ကို Reserved လုပ်ထားတယ်။ အသုံးမပြုရဘူး။ ဥပမာ 124.0.0.0 နှင့် 124.255.255.255 ဖြစ်တယ်။ ဒီ Address ၂ ခုကို မသုံးရဘူး။ 0.0.0 ကို Binary ပြောင်းရင် 0 တွေချည်းပဲရတယ်။ 255.255.255 ကို Binary ပြောင်းရင် 1 တွေချည်းပဲရတယ်။ ဒီတော့ Octet 4 ခုမှာ Network Portion ဖြစ်တဲ့ ရှေ့ဆုံး Octet ကိုခဏထား။ Host ပိုင်းဖြစ်တဲ့ နောက်က Octet 3 ခုမှာ အားလုံး 0 နှင့် အားလုံး 1 ဝတဲ့ Address ၂ ခုကိုမသုံးရဘူး။ ဒါကြောင့် ၂ ကို ၂၄ ခါမြှောက်လို့ရတဲ့

16,777,216 ကနေ Address ၂ ခုကိုနုတ်တော့ 16,777,214 ပဲရတယ်။ ဒီ 16,777,214 ကသာလျှင် Class A ရဲ့ Network တစ်ခုမှရတဲ့ Host အရေအတွက်တစ်ခုပဲဖြစ်ပါတယ်။ Class A ကြီးတစ်ခုလုံးမှာရတဲ့ အရေအတွက်ကိုသိချင်လျှင် 16,777,216 ကို 126 နှင့်မြှောက်ကြည့်ပေါ့။ ဆိုလိုတာက 16,777,214 ဆိုတဲ့ Host အရေအတွက်ဟာ Class A Network တစ်ခုမှာရတဲ့ အရေအတွက်ပဲ ဖြစ်ပါသေးတယ်။

ပုံ ၁.၈

All 0 နှင့် All 1 ဒီ ရှေ့ဆုံးနှင့် နောက်ဆုံး Node နှစ်ခုကို ဖယ် ရမယ်။



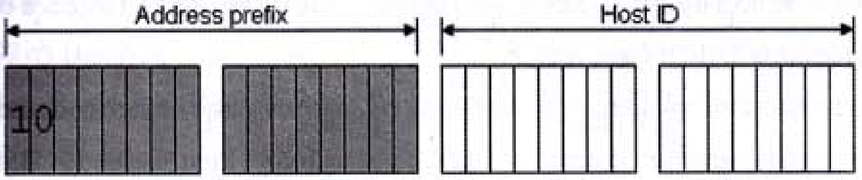
ကဲ ဒီအချိန်မှာ IANA မှာ နောက်တစ်ယောက်က ထပ်ပြီး Register လုပ်တယ်။ အေး မင်းကတော့ ၁၂၅ ယောက်မြောက်ပဲ။ ဒါကြောင့် မင်းရဲ့ Address က 125.x.x.x ပဲ။ ငါက သတ်မှတ်ပေးလိုက်တာ 125 ပဲ။ ကျန်တဲ့ ကြက်ခြေခတ်တွေက မင်းဘာသာမင်းသတ်မှတ်၊ ဒီတော့ သူက ပြန်ရောင်းတဲ့အခါ 125.0.0.0 ကို ဖယ်တယ်။ 125.255.255.255 ကိုဖယ်တယ်။ ဒီတော့ ပထမဦးဆုံးလူလာရင် 125.0.0.1 ဆိုပြီး ပေးမယ်။ နောက်တစ်ယောက်ကို 125.0.0.2 လို့ပေးမယ်။ အိုး အဲ့လေ အမျိုး တကယ်တမ်းမှာ ဘယ်သူကဒီလောက်လိုက် ပေးနိုင်မလဲ DHCP နဲ့ပေးတာပေါ့။ နောက်သင်ခန်းစာတွေကျမှ DHCP အကြောင်းရှင်းပြမယ်။

ရှင်းရဲ့လားလို့မမေးတော့ဘူး။ ရှုပ်နေမယ်ဆိုတာသိတယ်။ ပြန်ဖတ်ကြည့်မှ နားလည်မှာပါ။ လူရွှင်တော် တွေပျက်သလို ခေါင်းကို ပွတ်ပြီး ရှုပ်နေတာပဲ ဆိုတာမျိုးဖြစ်နေပြီ။ ဟိုဒင်း မဖြစ်လဲ အောက်ကိုသာဆက်သာ ဖတ် ဆုံးသွားတဲ့အခါ နားလည်လိမ့်မယ်။ တဆိတ်လောက်မေးပါရစေ။ ဟိုဒင်းမဖြစ်လဲဆိုတာဘာကိုပြောတာ လဲဟင်။ ပြော် အရေးထဲ။

၁.၈ **Class B Network အကြောင်း**

Class B ကျတော့ Network Portion က W နှင့် X ဖြစ်ပါတယ်။ Host Portion က Y နှင့် Z ဖြစ်ပါတယ်။ သူကတော့ အလယ်အလတ် Network တွေအတွက်ပါ။ တစ်ဝက်စီဖြစ်နေတာကိုး။ ကဲ ဒီတော့ စရှင်းပြီ။ IP Address မှာ 4 Octets ရှိတယ်။ ရှေ့ Octet ၂ခုက Network Address ဖြစ်ပြီး နောက် Octet ၂ခုက Host Address ဖြစ်ပါတယ်။ Bit အရပြောရင် 32 Bit ရှိတဲ့အထဲက ရှေ့ 16 Bits က Network Address ဖြစ်ပြီး နောက် 16 Bits က Host Address ဖြစ်ပါတယ်။

ပုံ ၁၉



Class B ၏ High Order Bits နှင့် Network Portion & Host Portion ကိုပြသောပုံ

ကဲ ခုနတုန်းကလိုပဲ Class A တုန်းကလိုပဲ High Order Bit ကိုပြန်စဉ်းစား Class B အရ High Order Bit ကရှေ့ဆုံးမှာ ၂ Bit ဖယ်တယ်။ ဒီတော့ Network Address က 16 Bits ရှိတဲ့အထဲက 2 Bit နုတ်တော့ 14 Bit ပဲကျန်တယ်။ 14 Bit ဆိုတော့ ၂ ကို ၁၄ ခါမြှောက် 16384 ရတယ်။ ဆိုလိုတာက Class B မှာ Network ပေါင်း ၁၆၃၈၄ ရတယ်။ Host ကျတော့ 16 Bits ရတယ်။ ၂ ကို ၁၆ ခါမြှောက်တော့ ၆၅၅၃၆ ရတယ်။ မှတ်ထားရမှာက Host ကိုတွက်တဲ့နေရာမှာ ၂ နုတ်ပေးဖို့မမေ့ပါနဲ့။ Host ID မှာ အားလုံး 0 ချည်းဖြစ်နေတဲ့ Address နှင့် အားလုံး 1 ချည်းပဲ ဖြစ်နေတဲ့ Address ကိုဖယ်ရတယ်လေ။ အဲ့ဒါအမြဲမှတ်ရမှာ။ ဒီတော့ ၆၅၅၃၆ ကနေ ၂ ကိုနုတ်တော့ ၆၅၅၃၄ ပဲရပါတယ်။ ဒီတော့ကား Class B ရဲ့ Network တစ်ခုတိုင်းမှာ Host ပေါင်း 65534 ရပါတယ်။ အဲဒါက Host, Network ကျတော့ 16384 ပဲရပါတယ်။

Class B ရဲ့ High Order Bit ဟာ 10 ဖြစ်ပါတယ်။ 128 ကို Binary ပြောင်းရင် 10000000 ရပါတယ်။ ဒီတော့ 128 ရဲ့ Binary ဖြစ်တဲ့ 10000000 ရဲ့ ရှေ့ဆုံးက 10 ဆိုတော့ High Order Bit နဲ့ကိုက်တယ်။ အဲကြောင့် Class A ရဲ့ First Octet ဟာ 1 ကနေ 126, 127 က Loopback အတွက် Reserved, ဒီတော့ Class B ရဲ့ First Octet က 128 ကနေစတယ်။ ဘယ်အထိလည်းဆိုတော့ 191 အထိဖြစ်ပါတယ်။ ကောင်းပြီ။

IANA မှာ လူတစ်ယောက်ကလာပြီး ကျွန်တော့်ကို Class B Network တစ်ခုချပေးပါ။ OK မင်းရဲ့ Address က 128.0.x.x ဖြစ်တယ်။ ရှေ့က Octet ၂ခုကို အဖွဲ့အစည်းကသတ်မှတ်ပေးလိုက်ပါတယ်။ နောက် Octet နှစ်ခုက ဝယ်တဲ့သူကသတ်မှတ်မှာ။ သူက 128.0.0.0 ကိုဖယ်တယ်။ 128.0.255.255 ကို ဖယ်တယ်။ သိတယ်နော်။ စရေးတော့ 128.0.0.1 ကစရေး။ နောက်တစ်ယောက်ကျတော့ 128.0.0.2 ပေါ့။ ဘယ်အထိရေးမလဲ 128.0.0.255 ပြီးရင် 128.0.1.1. သူက Octet နှစ်ခုကစားလို့ရတယ်လေ။ ဒီတော့ နောက်ဆုံး Octet 255 ဖြစ်ရင် ရှေ့ Octet 1 ကပြန်စတယ်။ ရှေ့ Octet 1 ဆိုတော့ 128.0.1.0 ပြန်ဖြစ် နောက်တစ်ယောက် 128.0.1.1 ဖြစ်၊ နောက်တစ်ယောက် 128.0.1.2 ဖြစ်၊ ဒီလိုနဲ့ 128.0.1.255 ဖြစ်လာ၊ ရှေ့ Octete 1 တိုး 128.0.2.0 ပြန်ဖြစ် အဲ့ဒီကနေ 128.0.2.255 ဖြစ် ရှေ့ Octet ၁ တိုး အမလေး

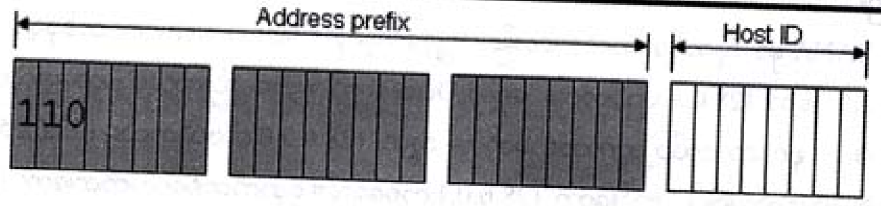
မောလိုက်တာ အားလုံး ၆၅၅၃၄ ရှိတယ်လေဗျာ၊ 128.0.0.1 ကနေ 128.0.255.254 အထိပေါ့။ တကယ်တော့ ဒီလိုဘယ်လုပ်မလဲ DHCP နဲ့ချပေးမှာပေါ့။

IANA ဘက်ကပြန်ကြည့်ရင် 128.0.x.x ကို သူ့ကိုရှောင်းရင် နောက်တစ်ယောက်ကျတော့ 128.1.x.x ပေါ့။ နောက်တစ်ယောက်က 128.2.x.x အဲ့ဒီလိုနဲ့ First Octet 191.255.x.x အထိ သူချပေးလို့ရတယ်။ အားလုံး Network ပေါင်း 16384 ရှိမယ်။ Network ပေါင်း 16384 ထဲက Network တစ်ခုတိုင်းမှာ Host ပေါင်း 65534 ရမယ်။

၁.၉ **Class C Network** အကြောင်း

Class C ကျတော့ Network Portion က W, X, Y အထိဖြစ်ပါတယ်။ Z က Host Portion ဖြစ်ပါတယ်။ သူကတော့ ကွန်ရက်အသေးစားတွေအတွက်ဖြစ်ပါတယ်။ IP Address မှာ 4 Octets ရှိတဲ့အထဲက ဘယ်ဘက်ကစယူ Octet 3 ခုက Network ပိုင်း နောက်ဆုံး Octet က Host ပိုင်းဖြစ်ပါတယ်။ ဒီတော့ Network ပိုင်းက 3 Octet, 1 Octet မှာ 8 bits ဆိုတော့ 3 Octet က 24 Bit ဖြစ်ပါတယ်။ High Order Bit ကရှေ့ဆုံး 3 Bit ဖယ်တယ်။ ဒီတော့ 24 bits က 21 bits ပဲကျန်တယ်။ 21 bits ကျန်တော့ ၂ ကို ၂၁ ခါမြှောက် 2,097,152 ရလိမ့်မယ်။ ဒီတော့ Class C မှာ Network ပေါင်း 2,097,152 တောင်ရှိတယ်။ Host ကျတော့ နောက်ဆုံး Octet တစ်ခုပဲ ရှိတော့ 8 bits ပဲရှိတယ်။ ဒီတော့ ၂ ကို ၈ ခါမြှောက်တော့ ၂၅၆ ရတယ်။ Host ကိုတွက်ရင် ရှေ့ဆုံး Address နှင့် နောက်ဆုံး Address ကို ဖယ်ပေးရတယ်။ ဆိုတော့ကား 256 ကနေ ၂ ကို နုတ်တော့ 254 ပဲ ရတယ်။ ဒီတော့ Class C မှာ Network ပေါင်း 2,097,152 ရှိတယ်ဆိုပေသိ အဲ့လေ ဆိုပေမယ့် Network တစ်ခုမှာ Host ပေါင်း ၂၅၄ လုံးပဲ ရှိပါတယ်။

၁.၁၀



Class C ၏ High Order Bits နှင့် Network Portion & Host Portion ကိုပြသောပုံ

Class C ရဲ့ High Order Bit ဟာ 110 ဖြစ်ပါတယ်။ Class C ရဲ့ First Octet ဟာ 192 ကနေ စပါတယ်။ 192 ကို Binary ပြောင်းရင် 11000000 ရပါတယ်။ ဒီတော့ 192 Binary ရဲ့ 11000000 ၏ရှေ့ဆုံး 110 ဟာ Class C ရဲ့ High Order Bit နှင့်လည်းကိုက်ပါတယ်။ Class C ရဲ့ First Octet ဟာ 192 ကနေပြီး 223 အထိရှိပါတယ်။

ခုနကလိုရှင်းပြရရင် ကျွန်တော်က Class C Network တစ်ခုဝယ်ချင် ရှိပါ။ အဲ့လေ ဝယ်ချင်လို့ပါ။ Ok ရော့ မင်းရဲ့ Address 192.0.0.x ဆိုပြီး အဲ့ဒီမှာ x က ဝယ်သူနှင့်ဆိုင်တယ်။ Host ID ကို 192.0.0 က သတ်မှတ်တဲ့ အဖွဲ့အစည်းနှင့်ဆိုင်တယ်။ ဝယ်တဲ့သူကသူ့ပြန်ဖြန့်တဲ့အခါ 192.0.0.0 ကိုဖယ်တယ်။ 192.0.0.255 ကိုဖယ်တယ်။ ပြီးရင် 192.0.0.1 ကနေစပြီးဖြန့်တယ်။ နောက်တစ်ယောက် 192.0.0.2 နောက်တစ်ယောက် 192.0.0.3 တကယ်တမ်းတော့ ဒီလိုဘယ်လုပ်နိုင်မလဲ DHCP နဲ့ပဲပေါ့။

IANA ဘက်ကျတော့ 192.0.0.x ကို စဖြန့် ပြီးရင် 192.0.1.x ပြီးရင် 192.0.2.x ရမယ်နော် ဒီလိုနဲ့ တက်တက်သွားလိမ့်မယ်။ ဒါဆို Class A, B နှင့် C မှာ Class တစ်ခုချင်းစီရဲ့ IP Address မှာ Network ပိုင်းနှင့် Host ပိုင်းကိုဘယ်လိုခွဲထားသလဲ။ Class တစ်ခုချင်းစီမှာ Network ဘယ်လောက်ရှိလို့ Host ဘယ်လောက်ရှိလဲစသဖြင့် သိသွားမှာပါ။ ဒီတော့ အနှစ်ချုပ်ကို အောက်က ဇယားလေးကိုတင်ပြရင်းနှင့် Class A, B, C ကို အဆုံးသတ်လိုက်ပါတယ်။

Class	Value for W	Address Prefix Portion	Host ID Portion	Address Prefixes	Host IDs Per Address Prefix
A	1-126	w	x.y.z	126	16,277,214
B	128-191	w.x	y.z	16,384	65,534
C	192-223	w.x.y	z	2,097,152	254

ဇယား ၁.၁ IP Address Class များ၏ Network နှင့် Host များရရှိပုံကိုပြသည့်ဇယား

၁.၁၀ **Dotted Decimal Notation** ဖြင့်ဖော်ပြခြင်း

IPv4 ရဲ့ Address တွေကို အပြည့်အစုံဖော်ပြတဲ့အခါမှာ နည်းလမ်း ၂ လမ်းရှိပါတယ်။ အဲ့ဒါကတော့

Dotted Decimal Notation နှင့် Prefix Length Notation တို့ပဲဖြစ်ပါတယ်။ အခု Dotted Decimal Notation ကိုအရင်ဖော်ပြပေးပါမယ်။

IPv4 Address မှာ Octet ၄ ခုရှိမယ်။ Address တစ်ခုဥပမာပေးမယ်။

130.100.x.x ဆိုကြပါစို့။

First Octet က 130 ဆိုတော့ Class B ပေါ့။ Class B ဆိုတော့ IANA က 130.100 ကိုသတ်မှတ်ပေးလိုက်တယ်။ ဒီ Octet ၄ ခုရှိတဲ့အထဲက ရှေ့ Octet နှစ်ခုက အသေဖြစ်သွားပြီ။ Fixed ပေါ့။ ဒါရှေ့မှာလည်း ရှင်းပြထားပြီးသားနော်။ ဒီတော့ 130.100.x.x မှာ ရှေ့ Octet ၂ ခုဖြစ်တဲ့ 130.100 က အသေ Fixed ပဲ။ နောက် Octet ၂ခုဖြစ်တဲ့ x.x ကပြောင်းလဲမှာ Variable ပေါ့။

ဒီတော့ ပြောတော့မယ်။ Class B ရဲ့ Octet 4 ခုမှာ ရှေ့ Octet နှစ်ခုက Fixed အသေပဲ။ နောက် Octet နှစ်ခုက Variable ပြောင်းလဲနိုင်တယ်။ Fixed ဖြစ်နေတဲ့ Octet နှစ်ခုကို အားလုံး 1 ချည်းပဲထား၊ Variable ဖြစ်တဲ့နောက်က Octet ၂ ခုကို 0 ချည်းပဲထား။ ဒါဆို ဘယ်လိုဖြစ်မလဲ 11111111 ဒါက 130 အတွက်၊ နောက် 100 အတွက်က 11111111 နောက် x ဖြစ်နေတဲ့ Octet နှစ်ခုက 00000000 00000000 ဆိုတော့ အကုန်လုံးပြန်စီရေးရင် –

11111111 11111111 00000000 00000000 ရပါတယ်။

အခုရှင်းပြနေတဲ့အထဲက မှတ်ရမှာ တစ်ခုတည်းပဲ။ Octet တွေမှာ IANA ကသတ်မှတ်ပေးလိုက်တဲ့ Octet က Fixed ဖြစ်တယ်။ အဲ့ဒါကို အားလုံး 1 ထား။ x ဖြစ်နေတဲ့ Variable ပြောင်းလဲနိုင်သော Octet မှာ အားလုံး 0 ထား။ ဒီတော့ 130.100.x.x အတွက် 11111111 11111111 00000000 00000000 ရတယ်။ ၎င်းတို့ကို Decimal ပြန်ပြောင်း။ 11111111 ကို Binary ကနေ Decimal ပြောင်းရင် 255 ရတယ်။ 00000000 ကို Binary ကနေ Decimal ပြောင်းရင် 0 ရတယ်။ ဒီတော့ 255.255.0.0 ရတယ်။ ဆိုတော့ကား –

130.100.x.x ကို အပြည့်အစုံဖော်ပြရင် –

130.100.x.x

255.255.0.0 ရပါတယ်။

ဒီလိုဖော်ပြတဲ့ပုံစံကို Network Mask သို့မဟုတ် Subnet Mask လို့လည်းခေါ်ပါတယ်။ ဒီတော့

Class A ရဲ့ Subnet Mask ကဘာဖြစ်မလဲ။ IP Address တစ်ခု ဥပမာပေးမယ်။

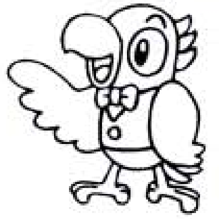
120.x.x.x ဆိုကြပါစို့။ ဒီမှာ Fixed Octet ကဘယ်သူလဲ။ 120 ပေါ့။ အဲ့ဒီ Fixed Octet ကို **အားလုံး** 1 တွေပဲထား 11111111 ဟုတ်လား။ 8 bits ကိုးဗျ။ ၁ – ၈ လုံးရမှာပေါ့။ နောက် Octet ၃ ခုကို **အားလုံး 0** ပဲထား။ ဒီတော့ –

11111111 00000000 00000000 00000000 ရလိမ့်မယ်။ ၎င်းတို့ကို Binary ပြောင်းရင် 255.0.0.0 ရလိမ့်မယ်။ ဒီတော့ 120.x.x.x ရဲ့ Subnet Mask တနည်းအားဖြင့် Class A ရဲ့ Subnet Mask က 255.0.0.0 အသေပဲ။ Class B ရဲ့ Subnet Mask က 255.255.0.0 အသေပဲ။ Class C ကျတော့ရော– IP Address တစ်ခုဥပမာပေးမယ်။

194.100.100.x ဆိုကြပါစို့။ Fixed Octet ကဘယ်သူလဲ။ 194.100.100 ပေါ့။ ဒီတော့ တွက်ပြမနေတော့ဘူး။ 255.255.255.0 ပေါ့။ ဒီတော့ 194.100.100.x ရဲ့ Dotted Decimal Notation က 194.100.100.x, 255.255.255.0 ဖြစ်ပါတယ်။

သသ

Class A ဆို 255.0.0.0
Class B ဆို 255.255.0.0
Class C ဆို 255.255.255.0
ဒါဟာ Default Subnet Mask ပဲ



၁.၁၁ **Prefix Length Notation** ဖြင့်ဖော်ပြခြင်း

အကယ်၍များကျွန်တော်တို့ဟာ IPv4 Address တွေကိုဖော်ပြတဲ့နေရာမှာ Dotted Decimal Notation ကိုမသုံးဘူးဆိုရင် Prefix Length Notation နှင့်ဖော်ပြနိုင်ပါတယ်။ Prefix Length Notation ကိုသုံးမယ်ဆိုရင်တော့ ကျွန်တော်တို့ဟာ Starting Address နှင့် Prefix Length ဆိုတာကိုသိရမယ်ဗျ။

Starting Address ဆိုတာ Dotted Decimal Position ကိုပြောတာပဲဖြစ်တယ်ဗျ။ ဒီ Starting Address ကိုဖော်ပြရာမှာ IANA ကသတ်မှတ်ပေးလိုက်တဲ့ No. ဟာအသေပဲလေ။ အဲ့ဒီ နံပါတ်ကို အဲ့ဒီ

အတိုင်းဖော်ပြလိုက် ဝယ်တဲ့သူက အစားထိုးရမယ့် Octet တွေမှာ 0 ကို အစားထိုးလိုက်ပါ။ ဥပမာ 130.100.x.x ဆိုတဲ့ Address ဆိုရင် 130.100 ဟာသတ်မှတ်ပြီးသားလေ။ အသေပဲ Fixed ပဲ။ အဲ့ဒီနံပါတ်ကို အဲ့ဒီအတိုင်းထား။ နောက် Octet က x.x ကို 0 နဲ့အစားထိုး။ ဒါဆို ဘယ်လိုဖြစ်သွားမလဲ။ 130.100.0.0 ဖြစ်သွားမှာပေါ့။ အဲ့ဒါကို Starting Address လို့ခေါ်ပါတယ်။

Prefix Length ဆိုတာကတော့ အဲ့ဒီ Starting Address မှာ Fixed အသေဖြစ်နေတဲ့ Octet တွေရဲ့ Bit အရေအတွက်ပဲ ဖြစ်ပါတယ်။ ဥပမာ 130.100.0.0 မှာ 130.100 ကအသေပဲမဟုတ်လား။ 130 ဆိုတဲ့ Octet မှာ 8 Bits ရှိတယ်။ 100 ဆိုတဲ့ Octet မှာ 8 Bits ရှိတယ်။ ဒီတော့ နှစ်ခုပေါင်း 16 Bits ရှိပါတယ်။ အဲ့ဒါကို /16 ဆိုပြီး Starting Address နောက်မှဖော်ပြရမှာဖြစ်ပါတယ်။

ဒီတော့ 130.100.0.0 ကို Prefix Length Notation အရဖော်ပြရမယ်ဆိုရင် –

130.100.0.0/16 ဖြစ်ပါတယ်။

ဥပမာ 10.x.x.x ကို Prefix Length Notation အရဖော်ပြရရင် 10.0.0.0/8 ရပါတယ်။

Prefix Length Notation ကို CIDR (Classless Inter Domain Routing) Notation လို့လည်း ခေါ်ပါတယ်။ အခု IPv4 Address တစ်ခုကို Prefix Length Notation နဲ့ရော Dotted Decimal Notation နဲ့ရောဖော်ပြပါ့မယ်။ ယှဉ်ကြည့်လို့ရအောင်ပေါ့။

ဥပမာ 131.107.x.x ဆိုပါတော့။

Prefix Length Notation --- 131.107.0.0/16 ဖြစ်ပါတယ်။
Dotted Decimal Notation --- 131.107.0.0, 255.255.0.0 ဖြစ်ပါတယ်။

ထပ်မံ၍ရှင်းပြရဦးမယ်ဆိုရင် 255.255.0.0 မှာ 255 ကို Binary ပြောင်းရင် 1111111 ရတယ်။ နောက် 255 ကို Binary ပြောင်းရင် 1111111 ရတယ်။ ဒီတော့ 1 က ၁၆ လုံးရှိတယ်။ ဒါကို အတိုကောက် /16 ဆိုပြီး 131.107.0.0/16 လို့ရေးတာဖြစ်တယ်။ ဆိုလိုတာက 131.107.0.0, 255.255.0.0 လို့ရေးမယ့်အစား 131.107.0.0/16 လို့ရေးလိုက်တာဖြစ်ပါတယ်။

ပုံ ၁.၁၂

Class A ဆို /8

Class B ဆို /16

Class C ဆို /24

၁.၁၂ **Public & Private Address** ဆိုတာ

ဒီတစ်ခါ Public Address တို့ Private Address တို့အကြောင်းရှင်းပြဦးမယ်။ တိုတိုပြောရရင်တော့ အင်တာနက်မှာအသုံးပြုနေကြတဲ့ Address မှန်သမျှဟာ Public Address ပဲဖြစ်ပါတယ်။ တနည်းအားဖြင့် ပြောရရင် သင့်ကွန်ပျူတာဟာ အင်တာနက်ကိုတိုက်ရိုက်ချိတ်ဆက်ထားမယ်ဆိုရင် အဲ့ဒီမှာ အသုံးပြုထားတဲ့ IP Address ဟာ Public Address ပဲဖြစ်ပါတယ်။ အကယ်၍ သင်ရဲ့ ကွန်ပျူတာဟာ အင်တာနက်ကို တိုက်ရိုက်ချိတ်ဆက်ထားတာမဟုတ်ဘဲ Proxy ဒါမှမဟုတ်ဘဲ Translate လုပ်ပြီးချိတ်ထားမယ်ဆိုရင်တော့ အဲ့ဒီ ကွန်ပျူတာဟာ Public Address ပဲဖြစ်ဖြစ် Private Address ပဲဖြစ်ဖြစ် အသုံးပြုနိုင်ပါတယ်။ အကယ်၍များ သင့်ရဲ့ Network ဟာ အင်တာနက်ကိုချိတ်ဆက်ထားခြင်းအလျှင်မရှိဘူးဆိုရင်တော့ သင်ဟာ IPv4 Unicast Address ကို သင်ကြိုက်သလိုကြိုက်တဲ့ Address သုံးနိုင်ပါတယ်။ ဘယ်လိုပဲဖြစ်ဖြစ်ပဲဗျာ ကမ္ဘာမှာ Private Address ဆိုပြီးသီးခြားသတ်မှတ်ထားတာရှိတယ်။ သင့်ရဲ့ Network မှာ Private Address တွေကို အသုံးပြုခြင်းဖြင့် တစ်ချိန်ချိန်မှာ ဒီ Network ကို အင်တာနက်နှင့်ချိတ်ဆက်တဲ့အခါ IP Address တွေကို ပြန်ပြင်ပေးစရာမလိုတော့ဘူးပေါ့။

ပြန်ပြောပြမယ်။ Public Address တို့ Private Address တို့ဆိုတာရှိတယ်။ သင့်ကွန်ပျူတာဟာ အင်တာနက်ကိုတိုက်ရိုက်ချိတ်ဆက်ထားရင် အဲ့ဒီ ကွန်ပျူတာမှာ သုံးနေတဲ့ IP Address ဟာ Public Address ဖြစ်ပါတယ်။ Private Address ဆိုတာ ဘယ်လိုလဲဆိုတာတော့ အခု မရှင်းပြရသေးဘူး။ အခုပြောပြချင်တာက သင့်ရဲ့ ကွန်ယက်မှာရှိတဲ့ ကွန်ပျူတာတွေကို IP Address ပေးရာမှာ –

၁။ ဒီကွန်ယက်ဟာ အင်တာနက်ကိုချိတ်ဆက်ထားတာတယ်။ ဒါပေမယ့် Proxy Server နှင့်ချိတ်ထားတာ၊ Proxy ဆိုတာ တည့်ပြောရရင် ကိုယ်စားလှယ်အဓိပ္ပါယ်ရတယ်။ ဆိုလိုတာက သင့်ကွန်ယက်မှာ ကွန်ပျူတာ ၅ လုံး ရှိတယ်။ ၅ လုံး စလုံးက အင်တာနက်ကို တိုက်ရိုက်ချိတ်ထားရင် ဒီ ၅ လုံး စလုံးရဲ့ IP Address ဟာ Public Address ပဲဖြစ်တယ်။ ခုဟာက ၅ လုံး မှာ ၁ လုံးက အင်တာနက်ကို တိုက်ရိုက်ချိတ်ထားတယ်။ ဒါဆို အဲ့ဒီ တစ်လုံးက အသုံးပြုတာ Public Address ကျန်တဲ့ ၄ လုံးက အင်တာနက်ကို ချိတ်တော့ချိတ်

ထားတယ်။ ဒါပေသိ တိုက်ရိုက်ချိတ်ထားတာမဟုတ်ဘူး။ Indirect ပေါ့။ ဘယ်ကနေဖြတ်ချိတ်တာလဲဆိုတော့ ကား - ခုနက ၁ လုံး အင်တာနက်နှင့် တိုက်ရိုက်ချိတ်ထားတဲ့ ၁ လုံးကနေ ချိတ်ဆက်ထားတာပါ။ ဒါကို Proxy ခံပြီးချိတ်တယ်လို့ပြောတာပါ။ ကိုယ်စားပေါ့ဗျာ။ ကဲ ဒီတော့ Proxy တစ်လုံးသာလျှင် Public Address ကိုအသုံးပြုတာဖြစ်ပြီး ကျန်တဲ့ ၄ လုံးက အင်တာနက်ကို တိုက်ရိုက်ချိတ်ဆက်ထားခြင်းမရှိသောကြောင့် ၎င်း ၄ လုံးဟာ Public Address သုံးသုံး Private Address သုံးသုံး သုံးလို့ရပါတယ်။ အင်တာနက်နှင့် တိုက်ရိုက်ချိတ်ထားတဲ့ ကွန်ပျူတာကတော့ Public Address ကို သုံးကိုသုံးရမှာဖြစ်ပါတယ်။

၂။ သင့်ကွန်ရက်ဟာ အင်တာနက်နှင့်ချိတ်ဆက်ထားခြင်းမရှိဘူးဆိုရင် သင်ဟာ Public သုံးသုံး Private သုံးသုံး ကြိုက်တာသုံး ရတယ်ဆိုပေမယ့် ဒီကွန်ယက်ဟာ တစ်ချိန်ချိန်မှာ အင်တာနက်ကို ချိတ်ဆက်ခဲ့မယ်ဆိုရင် အဲ့ဒီအချိန်ကျ ကွန်ယက်မှာရှိတဲ့ ကွန်ပျူတာတွေရဲ့ IP Address ဟာအင်တာနက်မှာသွားပြီး တိုက်နေမှာစိုးလို့နဂိုကတည်းက Private Address ကိုသုံးထားရင် အဲ့ဒီ အင်တာနက်ချိတ်တဲ့ အချိန်ကျ ဒီ IP တွေကို ပြန်ပြင်စရာမလိုတော့ဘူးပေါ့။

ကောင်းပါပြီ။ ဒီ IP Address တွေကို ICANN ကနေ Assign လုပ်ပါတယ်။ ICANN ဆိုတာ Internet Corporation for Assigned Names and Numbers ဖြစ်ပါတယ်။ အင်တာနက်ပေါ်မှာရှိတဲ့ CIDR Based Address တွေဟာ ဘယ်တော့မှ သွားတိုက်နေတာတို့၊ ထပ်တူဖြစ်နေတာတို့ ဆိုတာမရှိဘူး။ ဖြစ်လို့လည်းမရဘူး။

ICANN ဟာ IP Address ကိုလာဝယ်တဲ့ Organization အတွက် IP Address ကိုသတ်မှတ်ပေးလိုက်တဲ့အပြင် ၎င်း Address ကိုအင်တာနက် Router ထဲကိုပါထည့်ပေးထားလိုက်ပါတယ်။ ဒါမှသာလျှင် ၎င်း Organization ဟာ အင်တာနက်လမ်းကြောင်း ရရှိမှာဖြစ်ပါတယ်။ ဆိုလိုတာက ကျွန်တော်က YOUTH ကပါ။ ကျွန်တော့်ကို IP Address တစ်ခုပေးပါ။ ဥပမာပြောတာနော်။ ကဲ ကောင်းပြီ မင်းရဲ့ Address က 192.198.100.100 ဆိုပြီး သတ်မှတ်လိုက်တယ်ပေါ့ဗျာ။ အဲ့သလိုသတ်မှတ်ပေးရုံနှင့်မပြီးသေးဘူး။ ဒီ Address ကိုအင်တာနက် Router ထဲထည့်ပေးရသေးတယ်။ ဒါမှသာလျှင် Data Packet တွေဟာ ကျွန်တော်တို့ YOUTH ရှိရာ ရည်ရွယ်ရာဆီကိုရောက်လာမှာဖြစ်ပါတယ်။

ဒီတစ်ခါ Private Address ကိုရှင်းပြပါဦးမယ်။

ဒီလိုဗျ။ အင်တာနက်အသုံးပြုမှုဟာကြီးထွားလာတာနှင့်အမျှ Organization တွေရဲ့ အင်တာနက်ချိတ်ဆက်မှုဟာလည်းများပြားလာခဲ့ပါတယ်။ အဲ့ဒီ Organization တွေဟာ သူတို့ ကွန်ရက်မှာရှိတဲ့ ကွန်ပျူတာတွေ အားလုံးက အင်တာနက်ကို တိုက်ရိုက်ချိတ်ကြတာ။ ဒီတော့ Public Address သုံးစွဲမှုက များလာတာပေါ့။

ကျွန်တော်ပြောတာသဘောပေါက်လား။ ဒီ Organization မှာ ကွန်ပျူတာ အလုံး ၁၀၀ ရှိရင် အလုံး ၁၀၀ လုံးက အင်တာနက်ကို တိုက်ရိုက်ချိတ်တော့ ဒီ Organization တစ်ခုအတွက်မှာပင် Public Address က ၁၀၀ ကုန်သွားပြီ။ ဒီတော့ Public Address သုံးစွဲမှုများလာတာပေါ့။ အင်တာနက်နှင့် ချိတ်ထားတဲ့ ကွန်ယက်တိုင်းမှာ ရှိတဲ့ ကွန်ပျူတာအားလုံးရဲ့ IPv4 Address တွေဟာ ဒီ Network မှာရော အင်တာနက်မှာပါ ထပ်တူ မရှိဖို့လည်းလိုတယ်လေ။ ဒီတော့ အင်တာနက်ရဲ့ ဒီဇိုင်းနာတွေဟာ အင်တာနက်ကိုသုံးတဲ့ Organization တွေကိုလေ့လာကြည့်တဲ့အခါ Organization တော်တော်များများရော၊ ငင်းရုံးတွေမှာရှိတဲ့ ကွန်ပျူတာ တော်တော်များများရောပေါ့ သူတို့တွေဟာ အင်တာနက်ကို တိုက်ရိုက်ချိတ်ဆက်စရာမလိုဘူးဆိုတာကို သွားတွေ့ခဲ့ကြတယ်။ ဘာလို့လည်းဆိုတော့ အဲ့ဒီကွန်ပျူတာတွေ (ကွန်ပျူတာလို့ပြောရင်မလုံလောက်ဘူး Host လို့ပြောမယ်) Host တွေဟာ အင်တာနက်ရဲ့ Service တစ်မျိုးဖြစ်တဲ့ Web Access နှင့် Email လောက် အသုံးပြုကြတာမို့ ဒါတွေကိုသာ Application Layer Gateway တွေဖြစ်ကြတဲ့ Proxy Server တို့ Email Server တို့ကနေ ဖြတ်ပြီးသုံးလို့ရနေတာပဲဆိုတာကိုတွေ့ရှိခဲ့ကြပါတယ်။ OK လား။ မူးနေပြီလား။ မူးနေလည်းကောင်းသားဗျ။ ပိုက်ဆံလည်းမကုန်ဘဲ မူးနေတာပေါ့။

ဒီတော့ Organization တွေမှာရှိတဲ့ ကွန်ပျူတာတိုင်း အင်တာနက်သုံးချင်ရင်သုံး၊ ဒါပေသိ သုံးတဲ့ အလုံးတိုင်း Public Address လိုက်ပေးစရာမလိုဘူး။ အဲ့ဒီ Organization မှာရှိတဲ့ Public Address ကို မသုံးမဖြစ်သုံးဖို့လိုတဲ့ အနည်းငယ်သော Proxy, Server, Router, Firewall နှင့် Translater တွေလောက်ကိုသာ Public Address ပေးသုံးလိုက်မှာဖြစ်ပါတယ်။ အဲ့ဒီ ကွန်ယက်မှာရှိတဲ့ အင်တာနက်ကို တိုက်ရိုက်ချိတ်ဆက်ဖို့မလိုတဲ့ Host တိုင်းရဲ့ IPv4 Address ဟာ အင်တာနက်မှာ သတ်မှတ်ထားပြီးသားဖြစ်တဲ့ Public Address နှင့်သွားပြီးတူနေလို့မရဘူး။ အဲ့ဒီမှာစတာပဲ။ (ဟင် ခုမှစတယ်၊ ဒါဆိုထပ်မူးဦးမှာပေါ့) ဂလောက်လည်း စိတ်ဓါတ်မကျပါနဲ့ဗျ။ ထပ်ရှင်းပြမယ်။

အင်တာနက်ကိုသုံးတဲ့ အဖွဲ့အစည်းတိုင်းရဲ့ ကွန်ယက်မှာရှိတဲ့ Host တိုင်းဟာ Public Address ကို သုံးရင် Public Address တွေလောက်မှာမတုတ်ဘူး။ တကယ်တမ်းသုံးဖို့လည်းမလိုဘူး။ ဒါကြောင့် Public Address ကိုအဖွဲ့အစည်းတွေမှာရှိတဲ့ Proxy တို့ Server တို့ Router တို့ Translater တို့ Firewall တို့ သာလျှင်သုံးသင့်တယ်။ ဒါက တစ်ချက်။

နောက်တစ်ချက်က အင်တာနက်ကို တိုက်ရိုက်မသုံးဘဲ သွယ်ဝိုက် (သွယ်ဝိုက်ကဗိုက်လားဝိုက်လား) အို… ရှုပ်ပါတယ် ဒီလိုဗျ Indirect ပေါ့။ အင်တာနက်ကို Indirect သုံးတဲ့ Host တွေမှာ အသုံးပြုတဲ့ IPv 4 Address ဟာ Public Address တွေနှင့်သွားတူလို့မရပြန်ဘူး။ ဒီပြဿနာကိုဖြေရှင်းဖို့ရာ အင်တာနက် ဒီဇိုင်းနာတွေဟာ IPv4 Address ရဲ့ တစ်ချို့သော အပိုင်းတွေကို Private Address အဖြစ်တစ်သီးပုဂ္ဂလပိုင် Address အဖြစ် ချန်လှပ်ထားကြဖို့ဖြစ်လာပါတော့တယ်။ အဲ့ဒီ Address တွေကိုလည်း Private Address ဆိုပြီးခေါ်တွင်စေပါတယ်။ ဒီ Private Address တွေမှာရှိတဲ့ Address တွေကို Public Address မှာ

သတ်မှတ်မထားတော့ပါဘူး။ ဒီတော့ Private Address နှင့် Public Address ကသွားထပ်စရာ၊ တူနေစရာ အကြောင်းမရှိတော့ပါဘူး။ အဲ့ဒီလို တူမနေအောင်လို့လည်း တမင်တကာ Private Address ဆိုပြီး ဘယ်ကနေ ဘယ်အထိဆိုပြီး သတ်မှတ်လိုက်ကြတာပဲလေ။ ဒီတော့ အဲ့ဒီလိုသတ်မှတ်လိုက်တဲ့ Private Address တွေက

၁။ 10.0.0.0/8 တနည်းအားဖြင့် (10.0.0.0, 255.0.0.0)

ဒီ Address မှာ Host အတွက် 24 Bits တောင်ရတယ်။ အဲ့ဒီအထဲက Private Address အဖြစ် ကိုယ်ကြိုက်သလိုသုံး။ ဒီ Range ဟာ Public Address မှာမရှိဘူး။ အားလုံးရှိတာက 32 Bits လေ။ Prefix Length က 8 Bits ဆိုတော့ 32 ထဲက 8 ကိုနုတ်တော့ Host အတွက် 24 Bits ကျန်တာပေါ့။

၂။ 172.16.0.0/12 တနည်းအားဖြင့် (172.16.0.0, 255.240.0.0)

သူကျတော့ Host အတွက် 20 Bits ရတယ်။ ရှိတာက 32 Bits လေ။ 12 က Prefix Length ဆိုတော့ Host အတွက် 20 Bits ကျန်တာပေါ့။

၃။ 192.168.0.0/16 တနည်းအားဖြင့် (192.168.0.0, 255.255.0.0)

သူကျတော့ Host အတွက် 16 Bits ရတယ်။

ကဲ အထက်ပါ IPv4 Address Range များဟာ Private Address တွေဖြစ်ကြပါတယ်။ Organization တွေက အင်တာနက်ကိုချိတ်မယ်ဆိုရင် ICANN က ဒီ IP တွေကိုဘယ်တော့မှ မသတ်မှတ်ပေးသလို အင်တာနက် Router တွေထဲမှာလည်း ဒီ Private Address တွေကို သွားထည့်ထားခြင်းအလျှင်းမရှိပါဘူး။ တနည်းအားဖြင့် ပြောရရင် ဒီ Private Address တွေနှင့်အင်တာနက်ကိုချိတ်ဆက်လို့မရဘူးပေါ့များ။ ဒီတော့ကား ရုံးတွေရဲ့ ကွန်ယက်အတွင်းမှာရှိတဲ့ Host များဟာ အင်တာနက်ကိုသုံးချင်ရင် စောနက အဲ့လေ ခုနက ပြောခဲ့တဲ့ Public Address ကိုအသုံးပြုထားတဲ့ Application Layer Gateway တွေဖြစ်ကြတဲ့ Proxy Server တို့ ဒါမှမဟုတ် Network Address Translation (NAT) Device တို့ကနေအင်တာနက်ကို သုံးရမှာဖြစ်ပါတယ်။ Proxy Server ကရုံးထဲမှာရှိတဲ့ အင်တာနက်သုံးမယ့် Host တွေရဲ့ကိုယ်စားဖြစ်တာကြောင့် သူကတော့ Public Address ကိုသုံးရမှာဖြစ်ပါတယ်။ ထို့အတူ Private Address ကနေ Public Address ပြောင်းပေးတဲ့ NAT လို Device မျိုးကလည်း Public Address ကိုအသုံးပြုရမှာပဲဖြစ်ပါတယ်။

၁.၁၃ **Illegal (ILLEGAL) Address** ဆိုတာ

ဒီနေရာမှာ Illegal Address ဆိုပြီးတစ်ခုလောက်ရှင်းပြချင်သေးတယ်။ ရုံးတွေ၊ ကုမ္ပဏီတွေ အဖွဲ့အစည်းတွေမှာ ရှိတဲ့ကွန်ယက်တွေဟာ အင်တာနက်ကိုသာ အသုံးမပြုခဲ့ဘူးဆိုရင် ကြိုက်တဲ့ Address ကို သုံးလို့ရပါတယ်။ ဒါသိခဲ့ပြီးသားပါ။ အကယ်၍များပေါ့။ ဒီအဖွဲ့အစည်းဟာ နောက်ပိုင်းကျမှ အင်တာနက်ကို တိုက်ရိုက်အသုံးပြုတော့မယ်ဆိုရင် အဲဒီအဖွဲ့အစည်းတွေမှာသုံးချင်တဲ့ Host တွေရဲ့ IPv4 ရဲ့ Address တွေကိုဘယ်သုံးလို့ရတော့မလဲ။ ဆက်သုံးရင်လည်း ၎င်း Address ဟာ အင်တာနက်ရဲ့ Public Address နှင့်တိုက်ရော။

ဥပမာ Address တစ်ခု ဥပမာပေးမယ်။ 206.73.118.0 /24 ဆိုပါစို့။ ဒါကိုသင်ကသုံးမယ်။ အင်တာနက်ကို တိုက်ရိုက်မချိတ်ခင်တုန်းကတော့ ဘာမှမဖြစ်ဘူး။ အင်တာနက်ကို တိုက်ရိုက်ချိတ်လိုက်ရင် ဒီ IP ဟာ အင်တာနက်မှာဆို Microsoft ရဲ့ IP ကြီးဖြစ်နေတယ်။ အဲတော့ သင့် IP နှင့် ဒီ Microsoft ရဲ့ IP သွားတိုက်ရော။ ဒါဆို သင့် IP က Illegal Address ပဲ။ ဒီတော့ သင်က ဒီ Illegal Address နှင့် အင်တာနက်သုံးလို့ရမလားဆိုတော့ မရနိုင်ဘူး။ သင်တစ်စုံတစ်ခုကိုခေါ်လိုက်ရင် အဲဒီအကြောင်းအရာတွေဟာ သင့်ဆီကိုမရောက်ပဲ Microsoft ဆီရောက်သွားလိမ့်မယ်။ သင်က Illegal Address ဖြစ်တယ်။ 206.73.118.0 /29 ဆိုတာ ICANN က၊ ဒါကတော့ Microsoft ရဲ့ Address Prefix ပဲဆိုပြီးသတ်မှတ်ပြီးသား။ ဒီတော့ Traffic လမ်းကြောင်းက အဲဒီဆီကိုပဲသွားမှာပဲ။ သင့်ဆီကိုလာမှာ မဟုတ်ဘူး ဆိုလိုတာက သင်ဘာပဲခေါ်ခေါ် ခေါ်သမျှအကြောင်းအရာလမ်းကြောင်းဟာ Microsoft ဆီပဲရောက်သွားလိမ့်မယ်။ ဆိုလိုတာက ပို့လိုက်တဲ့ Data Packets အားလုံးကို Routers က Microsoft ဆီကို Route လုပ်လိုက်လို့ပဲဖြစ်တယ်။ ဒါကြောင့် ကျွန်တော်တို့ဟာ သင့် Intranet ကနေ Internet ကို ချိတ်မယ်ဆို Illegal Address မဖြစ်ရလေအောင် တနည်းအားဖြင့် သင်သုံးတဲ့ Public Address နှင့် သွားမတိုက်ရလေအောင် Private Address ကို အသုံးပြုရမှာဖြစ်ပါတယ်။

၁.၁၄ **Special IPv4 Address** များ

၁။ 0.0.0.0

ဒီ Address ရဲ့ အဓိပ္ပါယ်က မရှိဘူးလို့ရည်ညွှန်းတယ်။ တနည်းအားဖြင့် သတ်မှတ်ထားခြင်းမရှိသော IP Address လို့ ရည်ညွှန်းပါတယ်။ သူ့ကို ဘယ်အခါမှာသုံးသလဲဆိုတော့ IPv4 Address ကို မသတ်မှတ်ရသေးသော အခါမှာသုံးပါတယ်။ ဆိုလိုတာက သင့်ရဲ့ ကွန်ပျူတာမှာ IP Address ကို မသတ်မှတ်ရသေးဘူး။

အဲဒီလိုဆိုရင် 0.0.0.0 ပဲ။ အဲဒါကို ဘာလို့ Unspecified Address လို့ခေါ်တယ်။ သူ့ကိုနောက်တစ်မျိုး ပြန်ရှင်းပြရရင် သင့် ကွန်ပျူတာမှာ IP Address မရှိသေးလို့ မသတ်မှတ်ရသေးလို့ DHCP ကနေလှမ်းယူ နေဆဲကာလမှာ 0.0.0.0 ဖြစ်တယ်။

၂။ 127.0.0.1

သူလည်းဖယ်ထားတဲ့ Address ပဲ၊ သူ့ကိုတော့ Loopback Address လို့ခေါ်ပါတယ်။ Internet Loopback Address ပါ။ ဆိုလိုတာက Data Packets တွေကို သူ့ဆီကိုပဲ သူပြန်ပို့တာပါ။ ကိုယ့်ကိုကို ပြန်ပို့တာပါ။ သူ့ကို Ping နှင့် တွဲသုံးလို့ရပါတယ်။ Localhost ဆိုပြီးတော့လည်း သုံးလို့ရပါတယ်။

ပုံ ၁.၁၃

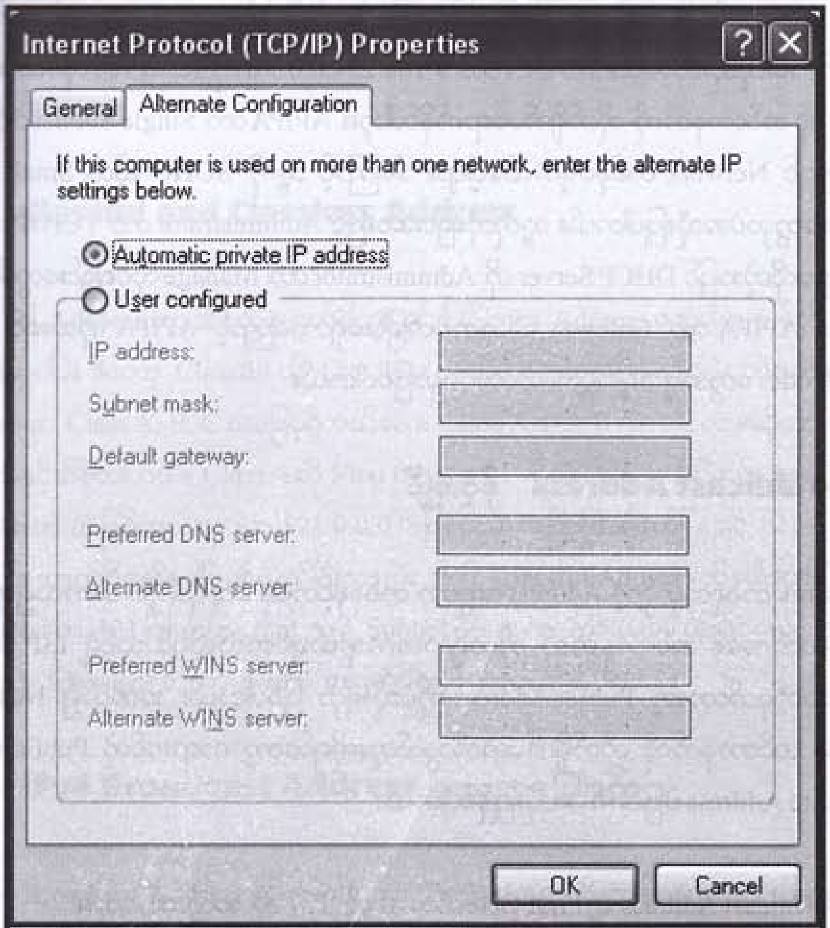
```
C:\Documents and Settings\Ko>ping localhost

Pinging CLIENT2 [127.0.0.1] with 32 bytes of data:

Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

၁.၁၅ **Automatic Private IP** ဖယ်ထားခြင်း

IP Address တွေကို အလိုအလျောက်ဝေတယ်ဆိုတာ DHCP ကိုပြောတာဖြစ်ပါတယ်။ DHCP ကို ဒီစာအုပ်ရဲ့နောက် သင်ခန်းစာတွေမှာ သင်ပေးဦးမှာဖြစ်ပါတယ်။ ခုလောလောဆယ် ဒီသင်ခန်းစာလေးဖတ် လို့ရလောက်အောင် ရှင်းပြထားရမယ်ဆိုရင် IP Address တွေကို ကွန်ပျူတာတွေရှိသမျှ အကုန်လုံးမှာ လူက Manual လိုက်ပေးနေမယ်ဆို ဝတ္တရားဟာအင်မတန်ကြီးမား များပြားမှာဖြစ်ပါတယ်။ အဲကြောင့် DHCP Server ထိုင်ပြီးကွန်ပျူတာတွေဆီကို IP Address တွေ DHCP Server အလိုအလျောက်ဝေနိုင်းလိုက်တာ ဖြစ်ပါတယ်။ ဒီသင်ခန်းစာနှင့်ပတ်သတ်လို့ပြောချင်တာစပြီ။

အကယ်၍များ ကွန်ပျူတာဟာ DHCP Server ကိုမတွေ့ခဲ့လို့ Contact လုပ်လို့မရခဲ့ဘူးဆိုရင် အဲဒီ ကွန်ပျူတာဟာ Alternate Configuration ကိုအသုံးပြုပါလိမ့်မယ်။ Alternate Configuration ဆိုတာ TCP/IP Properties Box မှာရှိပါတယ်ဗျ။

အကယ်၍များ သင့်ကွန်ပျူတာဟာ DHCP Server ကိုလည်းမတွေ့ခဲ့ဘူး။ သင်ကိုယ်တိုင်ကလည်း Automatic Private IP Address အရ TCP/IP Properties မှာ Alternate Configuration ကို ရွေးလိုက်မယ်ဆိုရင် အဲဒီကွန်ပျူတာ Windows ရဲ့ TCP/IP ဟာ APIPA ကို အသုံးပြုပါလိမ့်မယ်။



ဒီ Box ကိုပေါ်ချင်တယ်ဆိုလို့ရှိရင် TCP / IP Properties မှာ နှိပ်ပါ။ IP Address Box ပေါ်လာရင် Obtain an IP Address Automatically ကိုရွေးရမယ်။ အဲ့ဒီအခါကျအရင် Alternate Configuration Tab လေးပေါ်လာလိမ့်မယ်။ အဲ့ဒီအခါကျ Alternate Configuration ကိုရွေးလိုက်ရင် အခုမြင်နေရတဲ့ Box ပေါ်လာပါလိမ့်မယ်။

APIPA ဆိုတာ Automatic Private IP Addressing ပါ။ ဆိုလိုတာက သင်ကလည်း TCP/IP Properties မှာ Alternate Configuration ကိုရွေးထားဦးမှ အဲဒီကွန်ပျူတာကလည်း DHCP Server ကိုမတွေ့ဦးမှ။ အဲ့ဒါဆို ဒီကွန်ပျူတာရဲ့ TCP/IP APIPA ကို အသုံးပြုလိုက်တော့တာပဲ။ ဒါဆို APIPA Address ကဘာလဲ။ APIPA က 169.254.0.0 /16 တနည်းအားဖြင့် 169.254.0.0, 255.255.0.0 ဖြစ်တယ်။ အဲဒီမှာ Host IP အတွက် 16 bits ရတယ်။ ဒီတော့ APIPA က ဒီ 169.254.0.0 /16 ထဲကတစ်ခုခုကို Randomly ကျဘမ်းယူသုံးလိမ့်မယ်။ ICANN တာ ဒီ 169.254.0.0 /16 ကို Reserved လုပ်ထားပါတယ်။ ဒါကြောင့် ဒီ IP နှင့် အင်တာနက်ကို တိုက်ရိုက်မရောက်နိုင်ပါဘူး။ APIPA တာ Single Subnet ပဲရပါတယ်။ လွယ်လွယ်ပြောရင် Network တစ်ခုပဲရတယ်ပေါ့ဗျာ။ ဒါကြောင့် သူ့ကို SOHO ဆိုတဲ့ Small Office/ Home Office တွေမှာပဲအသုံးပြုပါတယ်။ သူ့ကိုသုံးခြင်းအားဖြင့် Administrator တာ TCP/IP ကို Configure လုပ်စရာမလိုတဲ့အပြင် DHCP Server ကို Administrator တာ Manage လုပ်ရခြင်းတွေပါမရှိတော့ဘူးဖြစ်ပါတယ်။ APIPA တာ Gateway ကိုသတ်မှတ်ခြင်းမရှိတာကြောင့် APIPA ကိုသုံးရင် Subnet တစ်ခုမှာရှိတဲ့ Nodes တွေအချင်းချင်းပွားလာတာပဲရမှာဖြစ်ပါတယ်။

၁.၁၆ **IPv4 Unicast Address** နှိုင်းချင်

၁။ Network တစ်ခုထဲမှာရှိတဲ့ Address တွေဟာ တစ်ခုနှင့်တစ်ခု မတူရပါဘူး။ အကယ်၍များ Host ဟာ သူ့ရဲ့ကွန်ယက်ကနေ အင်တာနက်ကို တိုက်ရိုက်ဆက်သွယ်ချင်တယ်ဆိုရင် သင့်ရဲ့ ISP ဒါမှမဟုတ် ICANN က သတ်မှတ်ထားတဲ့ Public Address ကိုပဲသုံးရမှာ ဖြစ်ပါတယ်။ အကယ်၍ Host က သူ့ကွန်ယက်ကနေ အင်တာနက်ကို တိုက်ရိုက်မဆက်သွယ်ဘူးဆိုရင်တော့ တရားဝင်တဲ့ Public Address ပဲဖြစ်ဖြစ် Private Address ပဲဖြစ်ဖြစ် အသုံးပြုနိုင်ပါတယ်။

၂။ IPv4 Unicast Address ရဲ့ First Octet ဟာ 0 နှင့် 127 ကို အသုံးမပြုရဘူး။

၃။ IPv4 ရဲ့ Unicast Address မှာ Host ID ပေးရင် သတိထားရမှာက ရှေ့ဆုံး Node နှင့် နောက်ဆုံး Node ကို မသုံးရဘူး။ ဥပမာ 192.10.15.x မှာ 192.10.15.0 နှင့် 192.10.15.255 ဆိုတဲ့ Host ID နှစ်ခုကို မသုံးရဘူး။

၁.၁၃ IPv4 Multicast Address

Multicast Address ဆိုတာ Packets တွေကို တစ်နေရာတည်းကနေ နေရာအများကြီးကို ရည်ရွယ်ထားများကြီးဆီကိုပေးပို့လိုက်တာ ဖြစ်ပါတယ်။ ဒီ IPv4 Multicast Address တွေဟာ အင်တာနက် Address Class D တွေဖြစ်ပါတယ်။ 224.0.0.0 / 4 ဖြစ်ပါတယ်။ Range အရ ပြောရရင်တော့ 224.0.0.0 မှ 239.255.255.255 ဖြစ်ပါတယ်။ ၎င်း Multicast Address တွေကို Video Conferencing မှာ အသုံးပြုကြပါတယ်။

၁.၁၀ Classful and Classless Address

ဒီ Address အသစ်တွေမဟုတ်ပါဘူး ရှင်းပြပြီးသား Address တွေပါပဲ။ သင်တို့သိပြီးသား Address တွေပါပဲ။ ဒီတော့ Classful တို့ Classless တို့ဆိုတာကအခေါ်အဝေါ်ပါပဲ။ ကဲရှင်းပြီ ဒီလိုဗျ IPv4 Address မှာ Class A, B, C စသဖြင့်ရှိတယ်လေ။ Class A လား B လား C လားဆိုတာ Octet ကိုကြည့်လိုက်တာနှင့်သိနိုင်ပါတယ်။ Class A ဆို First Octet က 1 ကနေ 126 အထိရှိမယ်။ သူ့ရဲ့ Prefix Length Notation က /8 ဖြစ်တယ်။ ဥပမာ 121.0.0.0 /8 ဖြစ်မယ်။ အပြည့်အစုံဖော်ပြရရင် 121.0.0.0, 255.0.0.0 ပဲဖြစ်မယ်။ ဟုတ်ပြီနော်။ ဒါပုံမှန်ပဲ သိပြီးသားပဲ။ ဒါကို Classful Address လို့ခေါ်ပါတယ်။ ဒီလိုလေဗျာ။ First Octet က 121 ဖြစ်တာကြောင့် သူ့ရဲ့ Subnet Mask က 255.0.0.0 ပဲဖြစ်ရမယ်။ ဖြစ်ကိုဖြစ်ရမယ်။ ဒါအသေပဲ။ Classless ဆိုတာကိုတော့ နောက်ပိုင်းမှာရှင်းပြမှာဖြစ်ပါတယ်။

၁.၁၉ IPv4 Broadcast Address များအကြောင်း

Broadcast Address ဆိုတာကျတော့ Packets တွေကို တစ်နေရာတည်းကနေ အဲဒီ Subnet ကွန်ယက်မှာရှိတဲ့ Host အားလုံးဆီကို ပို့တာဖြစ်ပါတယ်။ ဒီတော့ပြန်ပြောရရင်–

- Unicast ဆိုတာ One to One
- Multicast ဆိုရင် One to Many
- Broadcast ဆို One to All ဖြစ်ပါတယ်။

Broadcast Address များမှ အောက်ပါအတိုင်း ထပ်မံခွဲခြားထားပြန်ပါတယ်။

၁။ Network Broadcast

Classful Address ဖြစ်ရပါမယ်။ Host တွေအားလုံးကို 1 Bit ပြောင်းပစ်ပါ။ Subnet Mask အရပြောရရင် 255 ပြောင်းပါ။ ဆိုလိုတာက 131.107.255.255 ဖြစ်ပါတယ်။ ဒီတော့ 131.107.255.255 ဆိုတဲ့ Broadcast Address ကို Packets တွေပို့လိုက်ရင်ဖြင့် ၄င်း Packets တွေ 131.107.0.0, 255.255.0.0 ဆိုတဲ့ Subnet ထဲမှာရှိတဲ့ Host အားလုံးဆီကို Packet တွေ ရောက်ရှိသွားမှာ ဖြစ်ပါတယ်။

၂။ Subnet Broadcast

သူကတော့ Classless Address တွေမှာသုံးတာဖြစ်ပါတယ်။ Host ID တွေအားလုံးရဲ့ Bit တွေကို 1 ပြောင်းပစ်ပါ။ ဥပမာ 131.107.26.0 / 24 ဆိုကြပါစို့။ First Octet ဟာ 131 ဖြစ်ပါတယ်။ အကြောင့် ဒါဟာ Class B ဖြစ်ပါတယ်။ Class B ဆိုရင် ပုံမှန် 131.107.26.0 / 16 ဖြစ်ရမှာ အခု 131.107.26.0 / 24 ဖြစ်နေတယ်။ အကြောင့် ဒါဟာ Classless ဖြစ်တယ်။ တနည်းအားဖြင့် ၄င်း Network မှာဆင့်ပွား Network - Subnet ရှိနေပြီဖြစ်တယ်။ အဲဒီ Subnet အတွင်းမှာပဲ Broadcast လုပ်တဲ့ Address ကို Subnet Broadcast လို့ခေါ်တာဖြစ်ပါတယ်။ အကြောင့် 131.107.26.0 ရဲ့ Broadcast Address ဟာ 131.107.26.255 ဖြစ်ပါတယ်။

၃။ All - Subnets - Directed Broadcast

ပထမဦးဆုံးရှင်းပြတဲ့ Network Broadcast ကျတော့ဆင့်ပွား Network - Subnet မရှိတဲ့ Network တွေမှာ သုံးတာဖြစ်ပါတယ်။ Subnet Broadcast ကျတော့ Subnet အတွင်းမှာ Broadcast လုပ်တာ။ အခုပြောပြမယ့် All Subnets Directed ကျတော့ Subnet တစ်ခုတည်းက Host ကပို့လိုက်တဲ့ Packets ကရှိသမျှ Subnets တွေဆီရောက်သွားမှာဖြစ်ပါတယ်။ ပုံမှန်ဆို Subnet တစ်ခုကပို့လိုက်တဲ့ Broadcast က အဲဒီ Subnet ထဲမှာပဲရှိတဲ့ Host အားလုံးကို ရောက်တာပါ။ အခုဟာက ဒီ Subnet ထဲက Host တွင် မကတော့ဘူး ရှိသမျှ Subnet တွေဆီကိုရောက်သွားတော့တာဖြစ်ပါတယ်။ ဥပမာ 131.107.26 / 24 ဆိုရင်တော့ ဒီ Classless ကြီးဖြစ်နေပြီလေ။ First Octet က 131 ဆိုမှာတော့ Prefix Length Notation က /16 ဖြစ်ရမှာ /24 ဖြစ်နေတယ်လေ။ ဒီတော့ Classless Address ဆိုတော့ 131.107.26.0 / 24 ရဲ့ Subnet တစ်ခုဖြစ်နေတယ်လေ။ ဒီတော့ Classless Address ဆိုတော့ 131.107.26.0 / 24 ရဲ့ Subnet Broadcast အရပြောရရင် 131.107.26.255 ဖြစ်ပါတယ်။ အဲဒါဆို အဲဒီ Subnet အတွင်းပဲ Broad-

cast ဖြစ်တယ်။ အခုဟာက ရှိသမျှ Subnet အကုန်လုံးကို Broadcast လုပ်မယ့် All-Subnet-Directed ရဲ့ Broadcast Address ဖြစ်တာကြောင့် 131.107.255.255 ဖြစ်သွားပါတယ်။

၄။ Limited Broadcast

Limited Broadcast ဆိုတာ ဘယ်အချိန်မှာသုံးသလဲဆိုတော့ ကွန်ရက်ရဲ့ Subnet Prefix ကိုမသိတဲ့ အချိန်အခါမျိုးတွေမှာ အဲဒီကွန်ရက်ရဲ့ ရှိသမျှစက်တွေအားလုံးဆီကို Broadcast လုပ်ချင်တဲ့အခါမှာ အသုံးပြုပါတယ်။ ထပ်ရှင်းပြရဦးမယ်ဆိုရင် Auto Configuration တွေဖြစ်ကြတဲ့ BOOTP ဆိုတဲ့ Boot Protocal နှင့် DHCP တို့က သူ့ကို အသုံးပြုကြပါတယ်။ ဥပမာအားဖြင့် DHCP Client တွေဟာ သူတောင်းဆိုထားတဲ့ IPv4 Address ကို DHCP Server ကနေ အသိအမှတ်မပြုသေးခင် ဒီ Limited Broadcast Address ကို အသုံးပြုပြီး ကွန်ပျူတာတွေ အားလုံးဆီကို Broadcast လုပ်တဲ့အခါမှာ အသုံးပြုပါတယ်။ Limited Broadcast ကိုဖော်ပြရရင် Address ရဲ့ 32 Bits စလုံးကို 1 တွေထားပေးရမှာဖြစ်ပါတယ်။ ဆိုတော့ Limited Broadcast Address ဟာ 255.255.255.255 ဖြစ်ပါတယ်။

အချုပ်ပြန်ပြောရရင်-

၁။ 131.107.0.0 / 16 ရဲ့ Network Broadcast က 131.107.255.255
၂။ 131.107.26.0 / 24 ရဲ့ Subnet Broadcast က 131.107.26.255
၃။ 131.107.26.0 / 24 ရဲ့ All-Subnets-Directed Broadcast က 131.107.255.255 ဖြစ်ပါတယ်။
၄။ မသိတဲ့အခါမှာသုံးတာက 255.255.255.255

၁. ၂၀ Decimal မှ Binary သို့ပြောင်းခြင်း

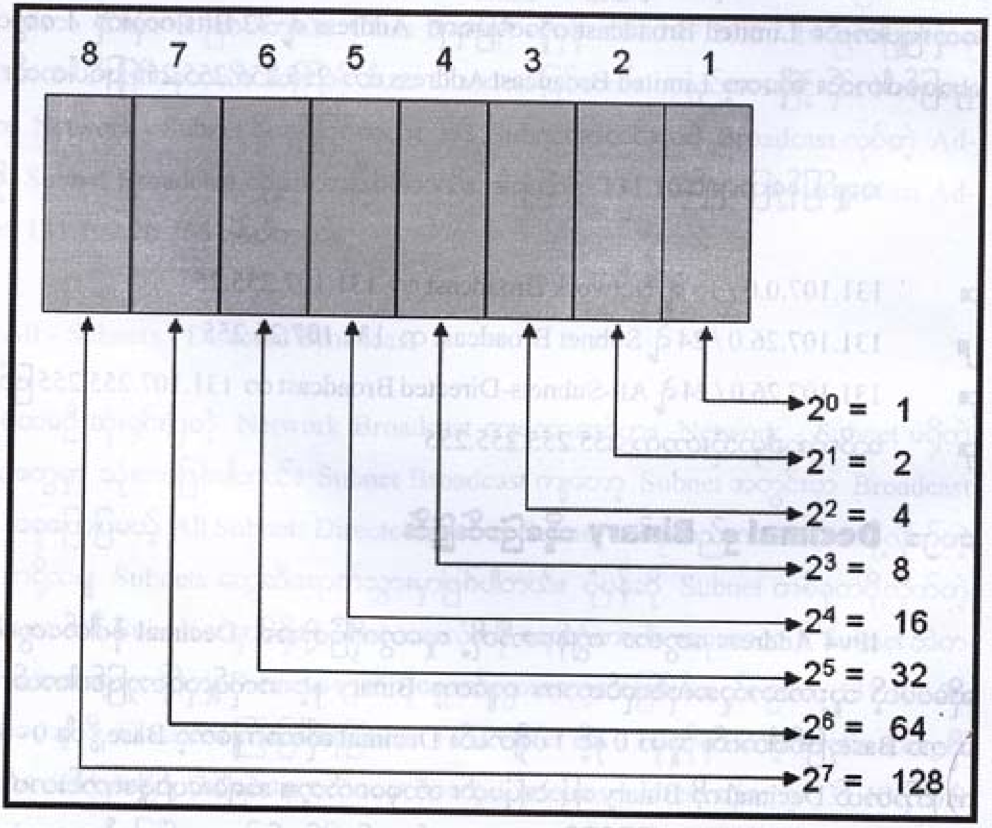
IPv4 Address တွေဟာ ကျွန်တော်တို့ လူတွေကိုပြတဲ့အခါ Decimal နံပါတ်တွေနှင့်ပြတယ် ဆိုပေမယ့် သူ့ဘာသာသူအလုပ်လုပ်တာက ကျတော့ Binary နှင့် အလုပ်လုပ်တာဖြစ်ပါတယ်။ Binary ဆိုတာ $Base_2$ ဖြစ်ပါတယ်။ သူ့မှာ 0 နှင့် 1 ပဲရှိတယ်။ Decimal ဆိုတာကျတော့ $Base_{10}$ ပါ။ 0 - 9 အထိပါ။ တဲ ကြာတယ် Decimal ကို Binary ပြောင်းပြမယ်။ ဘာမှမခက်ဘူး။ အရမ်းပျော်ဖို့ကောင်းတယ်။ စာရွက် အကြမ်းနှင့် ခဲတံ ဖြစ်ဖြစ် ဘောပင်ဖြစ်ဖြစ်ယူထား။ သချာ်တွက်ရပျင်းရင် အေးစက်နေတဲ့ အအေးတစ်ပုလင်း ဆောင်ထား။

ဒီအောက်ပါဇယားကို Decimal မှ Binary ပြောင်းတဲ့အခါမှာ အသုံးပြုမှာဖြစ်ပါတယ်။

Bit Position	8	7	6	5	4	3	2	1
	128	64	32	16	8	4	2	1

ဒီဇယားမှာ အကွက် ၈ ကွက်ရှိပါတယ်။ ဘာဖြစ်လို့လည်းဆိုတော့ IPv4 Address တာ Octet တစ်ခုမှာ 8 bit ရှိလို့ပါပဲ။ ဇယားအပေါ်မှာရှိတဲ့ 8 7 6 5 4 3 2 1 ဆိုတာ Bit တွေရဲ့ တည်နေရာကိုပြောတာ ဖြစ်ပါတယ်။

ပုံ ၁.၁၅



အကွက်တွေမှာ ရေးထားတဲ့ 128 64 32 16 8 4 2 1 မှာ –

1 ဆိုတာ = 2^0 ဖြစ်ပါတယ်
2 ဆိုတာ = 2^1 ဖြစ်ပါတယ်
4 ဆိုတာ = 2^2 ဖြစ်ပါတယ် 2 x 2 ပါ
8 ဆိုတာ = 2^3 ဖြစ်ပါတယ် 2 x 2 x 2 ပါ
16 ဆိုတာ = 2^4 ဖြစ်ပါတယ် 2 x 2 x 2 x 2 ပါ
32 ဆိုတာ = 2^5 ဖြစ်ပါတယ် 2 x 2 x 2 x 2 x 2 ပါ
64 ဆိုတာ = 2^6 ဖြစ်ပါတယ် 2 x 2 x 2 x 2 x 2 x 2 ပါ
128 ဆိုတာ = 2^7 ဖြစ်ပါတယ် 2 x 2 x 2 x 2 x 2 x 2 x 2 ပါ

အခု ဥပမာ အနေနဲ့ –

192 ဆိုတဲ့ ဂဏန်းကို Binary ပြောင်းပြမယ်။ ဇယားကွက်ကိုပဲအသုံးပြုပြီး ပြောင်းပြမယ်။ ဇယားကွက်မှာ ဘယ်ဘက်ကနေစပြီး အသုံးပြုပါမယ်။

၁။ ဘယ်ဘက်အစွန်ဆုံးမှာ 128 ဆိုတာရှိပါတယ်။ ဒီတော့ပြောင်းမယ့် ဂဏန်း 192 ကိုတည်ပြီး 128 နှင့် စားပါ။ စားလို့ရသလား။ အလီဝင်ပါသလား။ ဝင်ပါတယ်။ ဘာနှင့်လီတုန်း။ ၁ လီပါ OK ဒါဆို 128 ရဲ့ အောက်မှာ 1 လို့ရေးပါ။ ဇယားကွက်မှာ ဒီလိုဖြစ်သွားမယ်။

128	64	32	16	8	4	2	1
1							

မှတ်ချက် ။ ။ သိရမှာကပြောင်းမယ့် Decimal ဂဏန်းတွေဟာ 0 ကနေ 255 အတွင်းပဲဖြစ်မှာနော်။ IPv4 Address ရဲ့ Octet တွေမှာ အသုံးပြုတဲ့ဂဏန်းတွေဟာ 0 ကနေ 255 အတွင်းပဲဖြစ်ပါတယ်။

ကဲကောင်းပြီ 192 ကို 128 နှင့် 1 လီဝင်တော့ အကြွင်းဘယ်လောက်ရသလဲ။ 64 မဟုတ်လား။ ဟုတ်ရဲ့လား သချာ်ပါရဂူတွေနဲ့တော့ တွေ့နေပဟော့ လွယ်လွယ်လေးပါ။ 192 ကနေ 128 ကို နုတ်လိုက်ပေါ့။

၂။ ကျန်တဲ့ 64 ကို ဒုတိယအကွက်က 64 နှင့် အလီဝင်ကြည့်ပါ။ ဝင်လို့ရပါသလား။ ရပါတယ် 1 လီပါ။ ဒါဆိုရင် ဇယားကွက်မှာ 64 ရဲ့အောက်တည့်တည့်မှာ 1 လို့ရေးပါ။ ဇယားကွက်တာ ဒီလိုဖြစ်သွားမယ်။

128	64	32	16	8	4	2	1
1	1						

ကဲအကြွင်းရှိပါသလား။ အကြွင်းမရှိပါ။ အကြွင်းမရှိမှတော့ ဇယားကွက်ထဲက နောက်ဂဏန်းတွေနှင့် ထပ်စားလို့ မရတော့ပါ။ ဒီတော့ ကျန်တဲ့အကွက်တွေအားလုံးမှာ 0 တွေဖြည့်လိုက်ပါ။ ဒီတော့ ဇယားကွက်မှာ အောက်ပါအတိုင်းဖြစ်သွားလိမ့်မယ်။

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

ဒီတော့ 192 ကို Binary ပြောင်းရင် 11000000 ရပါတယ်။ သေချာစစ်နော် အားလုံးပေါင်းဂဏန်းက 8 လုံးရရမယ်။ စာမေးပွဲဖြေမယ့်သူတွေ ဒါကို သေချာလေ့ကျင့်ရမယ်နော်။ နောက်တစ်ခုပြောင်းပြမယ်။

242 ကို Binary ပြောင်းခြင်း

၁။ 242 ကို 128 နှင့်စားပါ။ အလီဝင်လို့ရပါသလား။ 1 လီရပါတယ်။ ဒါဆိုဇယားကွက်ရဲ့ 128 ရဲ့အောက်မှာ 1 လို့ရေးပါ။ ပြီးရင် 242 ထဲက 128 ကိုနုတ်ပါ။ 114 ကျန်ပါလိမ့်မယ် ဇယားကွက်ကိုလည်းကြည့်လိုက်ပါဦး။

128	64	32	16	8	4	2	1
1							

၂။ 114 ကို 64 နှင့်စား အလီဝင်လား။ ဝင်တယ် ဝင်ရင် 64 အောက်မှာ 1 လို့ရေးပြီးရင် 114 ထဲက 64 ကိုနုတ် 50 ကျန်မယ်။ ဇယားကွက်မှာ ဒီလိုဖြစ်သွားမယ်။

128	64	32	16	8	4	2	1
1	1						

၃။ အဲဒီလိုပဲ 50 ကို 32 နှင့်စား အလီဝင်လား။ ဝင်တယ်။ ဒါဆို 32 အောက်မှာ 1 လို့ရေးပြီးရင် 50 ထဲက 32 ကိုနုတ် 18 ကျန်မယ်။ ဇယားကွက်မှာ ဒီလိုဖြစ်သွားမယ်။

128	64	32	16	8	4	2	1
1	1	1					

၄။ ကျန်တဲ့ 18 ကို 16 နှင့်စား အလီဝင်လား ဝင်တယ်။ ဒါဆို 16 အောက်မှာ 1 လို့ရေးပါမယ်။ ပြီးရင် 18 ထဲက 16 ကိုနုတ် 2 ကြွင်းမယ်။ ဇယားကွက်မှာ ဒီလိုဖြစ်သွားမယ်။

128	64	32	16	8	4	2	1
1	1	1	1				

၅။ ကျန်တဲ့ 2 ကို 8 ကအလီဝင်လား၊ မဝင်ဘူး မဝင်ရင် 8 အောက်မှာ 0 လို့ရေးပါ။ ပြီးရင် အဲဒီ 2 ကို 4 နှင့် အလီဝင်ကြည့်၊ အလီဝင်လား မဝင်ဘူး မဝင်ရင် 4 အောက်မှာ 0 လို့ရေးပါ။ ဒီတော့ ဇယားကွက်မှာ ဒီလိုဖြစ်သွားမယ်။

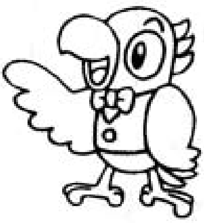
128	64	32	16	8	4	2	1
1	1	1	1	0	0		

၆။ ကျန်တဲ့ 2 ကို 2 နဲ့စား အလီဝင်လား၊ ဝင်တယ်။ ဒါဆို 2 အောက်မှာ 1 လို့ရေး၊ ကဲကုန်ပြီ အကြွင်းမရှိတော့ဘူး။ ဇယားမှာ 1 ကျန်သေးတယ် ဒီတော့ 1 အောက်မှာ 0 ပဲရေးလိုက်တော့။ ဇယားကွက်ကိုကြည့်လိုက်ပါ။

128	64	32	16	8	4	2	1
1	1	1	1	0	0	1	0

ဒီတော့ 242 ကို Binary ပြောင်းမယ်ဆိုရင် 11110010 ရပါတယ်။

0 ကို Binary ပြောင်းရင် 00000000 ရပါတယ်။ 255 ကို Binary ပြောင်းရင် 11111111 ရပါတယ်။ တရေးနိုးထ မေးလည်း သိရမယ်။ ပြောရဦးမယ်။ Binary မတတ်ရင် Network Engineer မဖြစ်နိုင်ဘူးနော်။



ကဲအောက်မှာ Decimal ကနေ Binary ပြောင်းကြည့်ဖို့ ဂဏန်းလေးလုံးကိုအဖြေနှင့်တကွပြပေးထားပါတယ်။ အဲဒါလေးတွေကို ကိုယ်တာသာကို ပြောင်းကြည့်လိုက်ပါ။ မှန်ရင်တော့ OK ပေါ့။ မမှန်ရင်တော့

နှုတ်ခွင်ပြုတာတွေ ပြန်ဖတ်ကြည့် ပြန်တွက်ကြည့်ပါ။

၁။ 165 = 10100101

၂။ 254 = 11111110

၃။ 172 = 10101100

၄။ 131 = 1000001

၁.၂ Binary မှ Decimal သို့ပြောင်းခြင်း

ဒီတစ်ခါ Binary ကနေ Decimal သို့ပြောင်းပြပါဦးမယ်။ သူက ပိုတောင်လွယ်သေးတယ်။ ဇယား ကွက်အတိုင်းပဲလုပ်ရအောင်။

၁။ 10100101 ကို Decimal ပြောင်းပြမယ်။

128	64	32	16	8	4	2	1
1	0	1	0	0	1	0	1

တကယ်တော့ 1010010 ကို သူ့အစဉ်လိုက်အတိုင်း ဇယားကွက်ထဲကို ထည့်ရိုက်လိုက်တာပါပဲ။ ပြီးရင် ဇယားကွက်မှာ 1 ရှိတဲ့ ဂဏန်းတွေ အကုန်ပေါင်းပါ။ ကဲ 1 ရှိတဲ့ ဂဏန်းတွေက 128 + 32 + 4 + 1 ဖြစ်ပါတယ်။ 128 + 32 + 4 + 1 = 165 ရပါတယ်။ လွယ်တယ်နော်။

၂။ 11111110 ကို Decimal ပြောင်းပြမယ်။ ၎င်းကို ဇယားကွက်မှာ အစဉ်လိုက်တိုင်းထည့်ပါ။ ပြီးရင် 1 ရှိတဲ့ ဂဏန်းအားလုံးပေါင်းပါ။

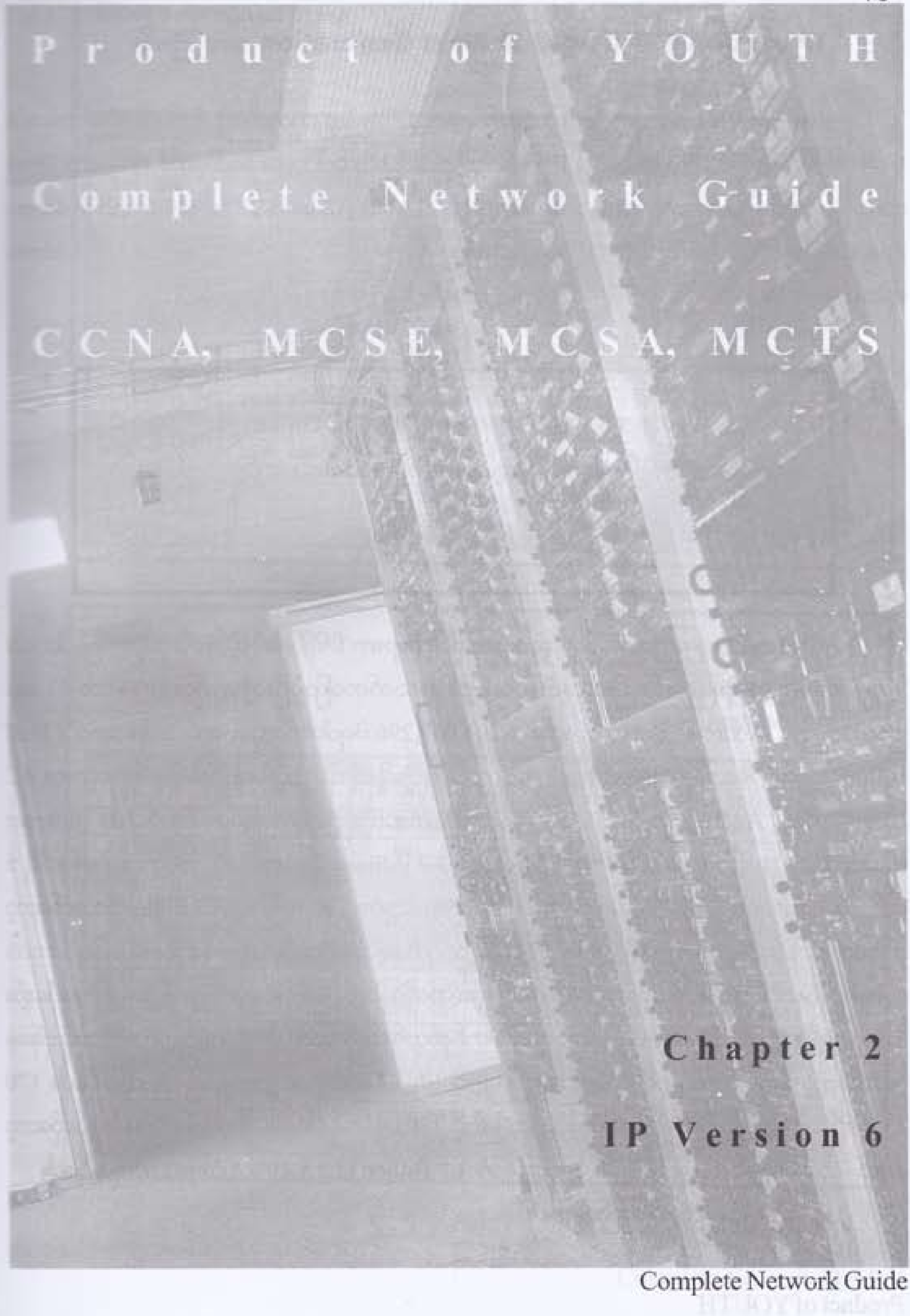
128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	0

1 ရှိတဲ့ ဂဏန်းအားလုံးပေါင်းဆိုတော့ 128 + 64 + 32 + 16 + 8 + 4 + 2 ဖြစ်ပါတယ်။ ပေါင်းရင် 254 ရပါတယ်။

၃။ 10101100 ကို Decimal ပြောင်းပြမယ်။ ၎င်းကို ဇယားအကွက်များအစဉ်လိုက်အတိုင်းထည့်ပါ။ ပြီးရင် 1 ရှိတဲ့ ဂဏန်းအားလုံးကို ပေါင်းပါ။

128	64	32	16	8	4	2	1
1	0	1	0	1	1	0	0

1 ရှိတဲ့ ဂဏန်းအားလုံးပေါင်းဆိုတော့ 128 + 32 + 8 + 4 = 172 ရပါတယ်။ ဒါပါဘဲ။ ဒီလောက်ဆို Binary ကနေ Decimal ပြောင်းတတ်ပြီဖြစ်လို့ Decimal ကနေ Binary အဖြစ်လည်း ပြောင်းနိုင်မှာ ဖြစ်ပါတယ်။



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 2

IP Version 6

၂.၁ IP version 6 @ IPng @ IP Next Generation အကြောင်း

IPv6 နှင့် IPv4 အဓိကကွာခြားတဲ့အချက်ကတော့ Size ပဲဗျ။ ဟုတ်တယ်။ ဒါကိုပဲ ဦးဆုံးပြောရမှာပဲ။ IPv4 က Size အရ 32 bits ပဲရှိတယ်။ IP v6 ကတော့ 128 bits ရှိပါတယ်။ ဒီတော့ကာ IPv6 ဟာ IP v4 ထက် 4 ဆပိုပြီးကြီးပါတယ်။ 32 bits လေးခါပေါ့ဗျာ။ 32 bits Address 2^{32} ဖြစ်တာကြောင့် Address Space ပေါင်း ဘယ်လောက်တောင်ရှိသလဲဆိုတော့ 4,294,967,296 ရှိပါတယ်။ 128 bit Address ဆိုဘယ်လောက်တောင်ဖြစ် သွားမလဲဆိုတော့ 2^{128} နော်။ ဒီတော့ အားပါးကြည့်စမ်းပါအုံး။

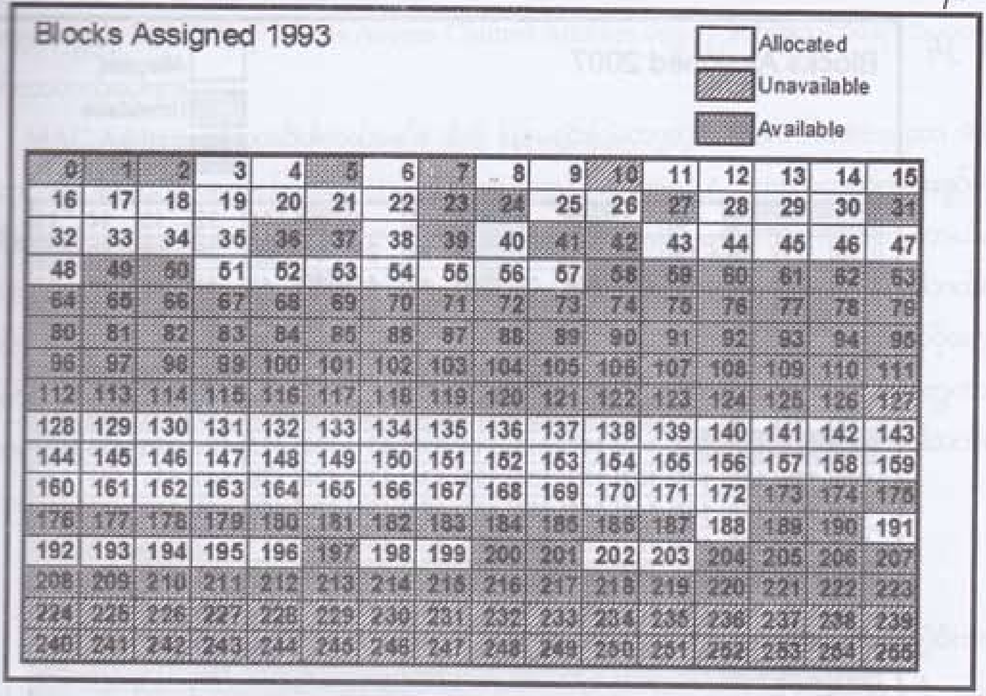
ပုံ ၂.၁

340,282,366,920,938,463,374,607,431,768,211,456 တောင်ရပါတယ်။ ချုံပြီးပြောရရင်တော့ 3.4×10^{38} ဖြစ်ပါတယ်။

IPv4 Address တွေဟာ ၁၉၇၀ ခုနှစ်နှောင်းပိုင်းနှစ်များက Designed ဆွဲထုတ်လုပ်ခဲ့တာဖြစ်ပါတယ်။ ဒီတုန်းကတော့ အသုံးပြုမှုက နည်းသေးတယ်ပေါ့ဗျာ။ အထက်ကပြောခဲ့ပြီးတဲ့အတိုင်း IPv4 ဟာ 32 bits ဖြစ်တာကြောင့် Address Space ကလည်း 4,294,967,296 ပဲရပါတယ်ဆိုပေမယ့် သန်း ၅၀၀ (Half Billion) လောက်သော Address တွေက အကြောင်းအမျိုးမျိုးကြောင့် သုံးမရပြန်ပါဘူး။ ဒီတော့ကား 4.2 Billion ဆိုတဲ့ Address မှာ 3.7 Billion လောက်သာအသုံးပြုလို့ရတာဖြစ်တယ်။ ဒီတော့ Internet ကိုအသုံးပြုတဲ့ Host တွေအတွက် ရတဲ့ Address က 3.7 Billion ဖြစ်တဲ့အထဲက ၂၀၀၇ ခုနှစ် ဇန်နဝါရီ ၁ ရက်နေ့အရပြောရရင် 2.4 Billion လောက်သော Address တွေက သုံးလို့ကုန်ပြီဗျ။ 1.3 Billion လောက်တော့ ကျန်သေးတယ်ပေါ့ဗျာ။ ဒါ ၂၀၀၇ ခုနှစ် ဇန်နဝါရီ ၁ ရက်နေ့ အဆိုနော်။ နောက်တစ်ခုပြောပြချင်တာက တစ်နှစ်တစ်နှစ်ကို Address တွေက 170 Million လောက်ထပ်ထပ်ပြီးတိုးလာတာဗျ။ ဒါပျမ်းမျှခြင်းပေါ့နော်။ ဒီတော့ ကျန်တာက 1.3 Billion ပဲ ကျန်တော့တာ။ တစ်နှစ်တစ်နှစ်ကိုလည်း 170 Million လောက်ထပ်ကုန်နေတာဆိုတော့ ဒီအတိုင်းသာဆိုရင် နောက် ၇ နှစ်ခွဲဆို IPv4 Address တွေဘာဖြစ်ပြီလဲ။ ကုန်ပြီပေါ့။ 170×10^6 ကို 7.5 နှင့်မြှောက်ကြည့်။ အဓိပ္ပာယ်က ၁ နှစ်ကို 170×10^6 Address တွေထပ်တိုးနေတယ်ဆိုတော့ နောင် 7.5 နှစ်ဆိုရင် 1.3×10^9 ပေါ့။ ဒီတော့ ရှိတဲ့ 1.3 Billion (1.3×10^9) Address ကကုန်ပြီပေါ့။

ပုံ ၂.၂၊ ၂.၃၊ ၂.၄ ကိုကြည့်လိုက်ပါ။

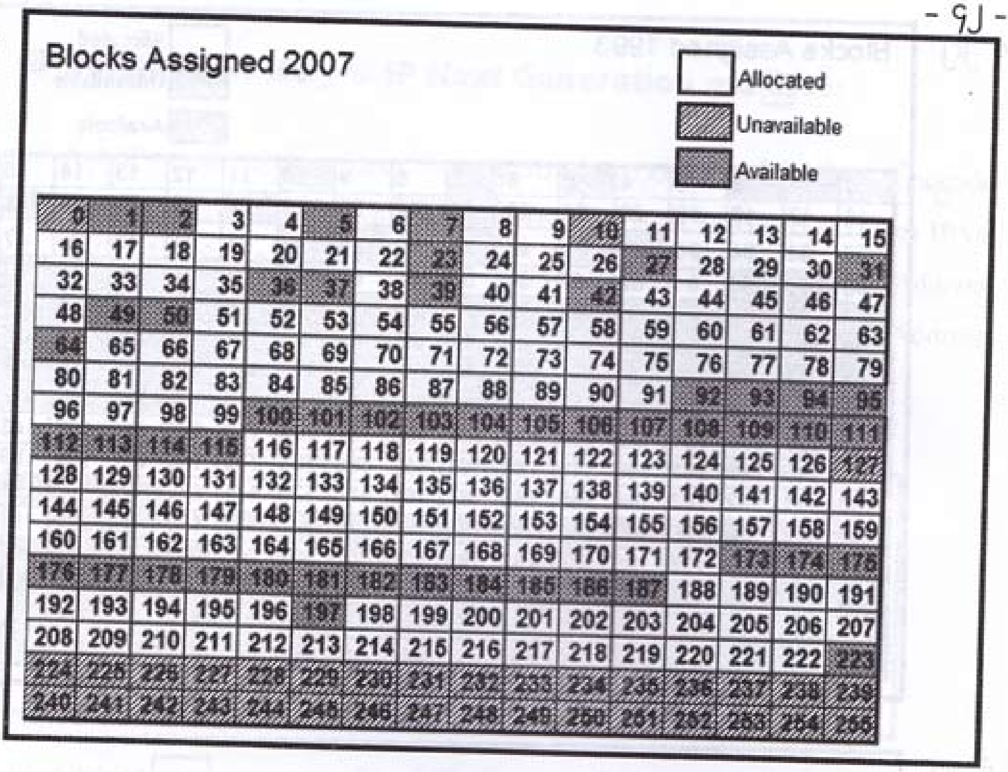
ပုံ ၂၈


Blocks Assigned 1993
Allocated
Unavailable
Available
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79
80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95
96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111
112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127
128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143
144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159
160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175
176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191
192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207
208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223
224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239
240 241 242 243 244 245 246 247 248 249 250 251 252 253 254 255

ပုံ ၂၉

Blocks Assigned 2000
Allocated
Unavailable
Available
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47
48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63
64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79
80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95
96 97 98 99 100 101 102 103 104 105 106 107 108 109 110 111
112 113 114 115 116 117 118 119 120 121 122 123 124 125 126 127
128 129 130 131 132 133 134 135 136 137 138 139 140 141 142 143
144 145 146 147 148 149 150 151 152 153 154 155 156 157 158 159
160 161 162 163 164 165 166 167 168 169 170 171 172 173 174 175
176 177 178 179 180 181 182 183 184 185 186 187 188 189 190 191
192 193 194 195 196 197 198 199 200 201 202 203 204 205 206 207
208 209 210 211 212 213 214 215 216 217 218 219 220 221 222 223
224 225 226 227 228 229 230 231 232 233 234 235 236 237 238 239

ပုံ ၂.၄



ဒီတော့ IPv6 ကျတော့ Address Space က 128 bits. 128 bits ကျတော့ 2^{128} လေ။ တွက်ကြည့်လိုက်ရင် Address Space ကနည်းနည်းလေးမှ မဟုတ်တာ။ 3 x 10^{38} ဆိုတော့ 0 က 38 လုံးတောင် ဖြစ်ပါတယ်။ ရှေ့ဆုံးဂဏန်း 1 လုံးနှင့်ဆို အားလုံးဂဏန်း 39 လုံးဖြစ်ပါတယ်။ အခုတော့ ပြောကြတာပါ။ ဒီ Address တွေသုံးမယ်ဆိုရင်တောင် တကယ်မပြောနဲ့ စိတ်ကူးရင်ပြီး သုံးရင်တောင် မနည်းမနောပဲ။

ဘယ်လောက်တောင်လဲဆိုရင် ကမ္ဘာကြီးမျက်နှာပြင် 1 မီတာပတ်လည်းတိုင်းကို 655, 570, 793, 348, 866, 943, 898, 599 ဆိုတဲ့ Address တွေပံ့ပိုးပေးနိုင်ပါတယ်။ ၄င်း ကိန်းဂဏန်းကို ချုံပြောရင် 6.5 x 10^{23} ဖြစ်ပါတယ်။ ကမ္ဘာကြီးမျက်နှာပြင်ရဲ့ 1 မီတာပတ်လည်တိုင်းကို အဲဒီလောက် Address တွေပေးနိုင်တယ်တဲ့ဗျ။ အံ့ဖွယ်တီးလူးပဲ အဲ့လေ အံ့ဖွယ်သရဲပဲ။ ဒါဆို ကမ္ဘာကြီးရဲ့မျက်နှာပြင်က ဘယ်နှမီတာရှိလဲ အင်တာနက်ထဲမှာတော့ 10^{15} x 0.510 m^2 ရှိတယ်ဗျ။ ကမ္ဘာကြီးရဲ့ Land Surface ပေါ့ဗျာ။ အဲဒီ 10^{15} x 0.510 m^2 ကို 6.5 x 10^{23} မြှောက်လိုက်ရင် 3 x 10^{38} ပြန်ထွက်ရမှာပေါ့။ ကဲထားပါလေ ဒါတွက်ပြတာပါ။ ဆက်ရအောင်

ဒီတော့ ဘာတွေဆက်ဖြစ်လာသလဲဆိုတော့ - IPv6 Address Space အရွယ်အစားကြီးလာတာနှင့်အမျှ Address တွေထားလိုမှုနှင့် လမ်းကြောင်းလွှဲခြင်း Routing လုပ်ခြင်းတို့က Efficient ဖြစ်စေဖို့ ဒီဇိုင်းဆွဲကြတဲ့အခါ ဒါဟာဘယ်လိုအကျိုးသက်ရောက်မှုတွေဖြစ်လာသလဲ ဆိုတော့ ယနေ့ခေတ်အင်တာနက်ရဲ့

Topology တွေနှင့် MAC ဆိုတဲ့ Media Access Control Address တွေကို အကျိုးသက်ရောက်မှုတွေ ရှိလာတတ်လာတယ်ပေါ့ဗျာ။

MAC Address ဆိုတာသိပါတယ်နော်။ ဒါကို ပြန်မရှင်းပြတော့ဘူး။ MAC Address ဟာ 98 Bits ရှိတယ်ဗျ။ ဒါပေမယ့် ခုနကပြောသလို IPv6 ရဲ့ကြီးမားကျယ်ပြန့်လာတဲ့ Address တွေကိုထိန်းချုပ်ဖို့ ဆော့ဖ်ဝဲဆိုင်းဆွဲစီမံမှုတွေပြုကြတဲ့အခါကျ MAC Address ကို 64 Bits အဖြစ်ပြုလုပ်ဖို့ ဖြစ်လာကြပါတယ်။ ၎င်း 64 Bits ရှိတဲ့ MAC Address ကို Networking နည်းပညာအသစ်တွေနှင့် အတူအသုံးပြုမှာ ဖြစ်ပါတယ်။ နောက်ပြီး IPv6 ဟာ Address များသတ်မှတ်ခြင်းနှင့် လမ်းကြောင်းများသတ်မှတ်ခြင်းတို့ကို အဆင့်တွေ အများကြီးနှင့် ဆင့်ပွားပုံစံပြုလုပ်ထားတဲ့အပြင် Flexible ဖြစ်အောင်လည်း ပြုလုပ်ထားပါတယ်။ ဒါတွေဟာ IPv4 တုန်းကမရှိခဲ့ပါဘူး။ ဒီအကြောင်းတွေကို နောက်ပိုင်းမှာလည်း ဆက်လက်လေ့လာရဦးမှာဖြစ်ပါတယ်။

၂.၂ IPv6 Address ပုံစံ

IPv6 ရဲ့ Address ပုံစံကို ပြောပြတော့မှာဖြစ်ပါတယ်။ IPv4 တုန်းကတော့ Address ရဲ့ပုံစံဟာ Dotted Decimal Notation ဖြစ်ပါတယ်။ IPv6 ကျတော့ 128 Bit Address မှာအပိုင်းပိုင်းခွဲထားပါတယ်။ အပိုင်း ၁ ပိုင်းချင်းဆီမှာ 16 Bit ရှိပါတယ်။ 16 Bit ရှိတဲ့ Block တစ်ခုချင်းဆီကို ဂဏန်း 4 လုံးပါတဲ့ Hexadecimal ပုံစံအဖြစ်နဲ့ပြမှာဖြစ်ပါတယ်။ Hexadecimal ဆိုတာ $Base_{16}$ ပုံစံဖြစ်ပါတယ်။ IPv6 Address ရဲ့အပိုင်း ၁ ပိုင်းချင်းဆီကို (:) Colon နှင့်ခြားထားတာဖြစ်ပါတယ်။ ဒါကြောင့်သူ့ကို Colon-Hexadecimal လို့လည်း ခေါ်ပါတယ်။ ဒီတော့ IPv6 ရဲ့ Address တစ်ခုကို ဥပမာပေးရရင် –

3FFE: 2900: D005: 0000: 02AA: 00FF: FE28: 9C5A

အဲဒီ Address မှာမှ 0 ကြီးပဲရှိတဲ့ အပိုင်းက 0 တွေဖြုတ်ပြီး ချုံ့ရေးလို့ရပါတယ်။ အပိုင်း ၁ ပိုင်းမှာ အနည်းဆုံးဂဏန်းတစ်လုံးရှိရင် ရပါပြီ။ အပိုင်းတစ်ပိုင်းချင်းစီမှာရှိတဲ့ ဂဏန်းတွေရဲ့ ရှေ့ဆုံးဂဏန်းဟာ 0 ဖြစ်နေရင်လည်း ၎င်း 0 ကိုဖြုတ်ထားလည်းရပါတယ်။

3FFE : 2900 : D005 : 0 : 2AA : FF : FE28 : 9C5A ဆိုပြီးဖြစ်သွားပါတယ်။

ဒါက 0 တွေကိုဖြုတ်ပြီး ချုံ့ရေးလိုက်တာပါ။ ဥပမာ 02AA ဆို 2AA လို့ရေးလည်းရပါတယ်။ 0 ရှေ့ကလာရင် ၎င်း 0 ကိုဖြုတ်ထားလို့ရပါတယ်။ IPv6 Address ရဲ့ အပိုင်း ၁ ပိုင်းချင်းစီမှာ ဂဏန်းက 4 လုံးရှိရမှာဆိုတော့ 2AA ကိုကြည့်လိုက်တာနှင့် ရှေ့က 0 ပဲဆိုတာ သိရမှာဖြစ်ပါတယ်။ 00FF ကို FF လို့ရေးလိုက်တာလည်း ဒီသဘောပါပဲ။

၂.၃ Hexadecimal မှ Binary သို့ပြောင်းခြင်း

Hexadecimal စနစ်ဟာ 0 ကနေ 15 ထိရှိပါတယ်။ ဆိုလိုတာက Binary ဆို 0 နှင့် 1 ပဲရှိတယ် မဟုတ်လား။ Hexadecimal က 0 ကနေ 15 ထိရှိပါတယ်။ 0 ကနေ 9 အထိကိုတော့ ဒီအတိုင်းပဲရေးပြီး 10 ကနေ 15 အထိကိုတော့ A, B, C, D, E, F ဆိုပြီးသုံးပါတယ်။ အောက်က ဇယားကိုကြည့်လိုက်ရင် ရှင်းသွားမှာပါ။

Decimal	Hexadecimal	Binary
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

■ Hexadecimal ကနေ Binary ပြောင်းတယ်ဆိုတာ Hexadecimal ကိန်းဂဏန်းတစ်ခုချင်းစီကို 4 Bit Binary ပြောင်းပေးရတာပါ။ ဥပမာပြောရရင် 03D8 ဆိုတဲ့ Hexadecimal ကို Binary ပြောင်းဖို့ရာ Hexadecimal ကိန်းဂဏန်းတစ်ခုချင်းစီဖြစ်တဲ့ 0, 3, D, 8 တို့ကို Binary ပြောင်းရမှာပါ။ ဒီတော့ –

- 0 ကို Binary ပြောင်းရင် 0000
- 3 ကို Binary ပြောင်းရင် 0011
- D ကို Binary ပြောင်းရင် 1101
- 8 ကို Binary ပြောင်းရင် 1000 ရပါတယ်။

ဒီတော့ကား 03D8 ဆိုတဲ့ Hexadecimal ဟာ Binary အရပြောရင် 0000 0011 1101 1000 ဖြစ်ပါတယ်။

ဒီတစ်ခါ 61AE ဆိုတဲ့ Hexadecimal ကို Binary ပြောင်းကြည့်ရအောင်။ ဒီတော့ အပေါ်က ဇယားကွက်ကိုကြည့်ပြီးပြောင်းကြတာပေါ့။

- 6 ကို Binary ပြောင်းရင် 0110 ရပါတယ်
- 1 ကို Binary ပြောင်းရင် 0001 ရပါတယ်
- A ကို Binary ပြောင်းရင် 1010 ရပါတယ်
- E ကို Binary ပြောင်းရင် 1110 ရပါတယ်

ဒီတော့ကား 61AE Hexadecimal ကို Binary ပြောင်းရင် 0110 0001 1010 1110 ရပါတယ်။

ဥပမာ 0000001111011000 ကို Hexadecimal ပြန်ပြောင်းရင် – ပထမဦးဆုံး ဂဏန်းတွေကို 4 လုံးစီခွဲထုတ်လိုက်ပါ။

0000 0011 1101 1000 ဆိုပြီးရပါလိမ့်မယ်။

- 0000 ကို Hexadecimal ပြောင်းရင် 0 ရပါတယ်။
- 0011 ကို Hexadecimal ပြောင်းရင် 3 ရပါတယ်။
- 1101 ကို Hexadecimal ပြောင်းရင် D ရပါတယ်။
- 1000 ကို Hexadecimal ပြောင်းရင် 8 ရပါတယ်။

0000 0011 1101 1000 ကို Hexadecimal ပြောင်းတော့ 03D8 ရပါတယ်။ နောက်တစ်ခုပြောင်းပြပါဦးမယ်။

0110000110101110 ကိုပြောင်းပြမယ်။ ပထမဦးဆုံးဂဏန်းတွေကို 4 လုံးဆီခွဲထုတ်လိုက်ပါ။ 0110 0001 1010 1110 ဆိုပြီးရပါလိမ့်မယ်။

- 0110 ကို Hexadecimal ပြောင်းရင် 6 ရပါတယ်။
- 0001 ကို Hexadecimal ပြောင်းရင် 1 ရပါတယ်။
- 1010 ကို Hexadecimal ပြောင်းရင် A ရပါတယ်။
- 1110 ကို Hexadecimal ပြောင်းရင် E ရပါတယ်။

ဒါကြောင့် 0110000110101110 ကို Binary ပြောင်းရင် 61AE ရပါတယ်။

၂.၄ Address တိုချုံ့ခြင်း

တစ်ချို့ Address တွေကျတော့ 0 တွေအများကြီးတရစပ်ပါတတ်တယ်ဗျ။ အဲသလိုမျိုးဆို Colon ကိုနှစ်ခါထပ်ပြီး Address ကိုချုံ့လိုက်လို့ရပါတယ်။ (::) ပေါ့။ ဥပမာအားဖြင့် –

FE80 : 0 : 0 : 0: 2AA : FF : FE9A : 1CA2 ဆိုကြပါစို့။
အဲဒီမှာ 0 တွေ တရစပ်ပါနေတယ်တွေ့လား။ ဒါကို ချုံ့လိုက်မယ်ဆို –

FE80 :: 2AA : FF : FE9A : 4CA2 ဆိုပြီးဖြစ်လာပါတယ်။

နောက်တစ်ခုလောက် ဥပမာပြောပြဦးမယ်။

FF02 : 0 : 0 : 0 : 0 : 0 : 2 ဆိုကြပါစို့။
ဒါဆို ဒီ 0 ရှိနေတဲ့အပိုင်းတွေကို ချုံ့လိုက်ရင် –

FF02 :: 2 ဆိုပြီးဖြစ်သွားပါတယ်။

ဒီနေရာမှာ ပြောစရာလေးတစ်ခုရှိပါတယ်။ ဥပမာဆိုကြပါစို့ FF02 : 30 : 0 : 0 : 0 : 0 : 0 : 5 အမျိုး Address ကျတော့ ချုံ့ရေးရင် သတိထားရမယ်။ ဘာလို့လည်းဆိုတော့ ဒုတိယ Block မှာ 30 ဖြစ်နေတယ်လေ။ ဒီတော့ကား ဒါကိုချုံ့လိုက်ရင် FF02 : 30 :: 5 အမိုး အဲလေ အမျိုးဖြစ်ရမယ်။ မှားတတ်တာက ဘယ်လိုမှားတတ်သလဲဆိုတော့ FF02 : 3 :: 5 ဆိုပြီး ရေးတတ်တယ်။

အဲသလိုရေးလို့မရဘူး အဲဒါမှားတယ်ပေါ့ဗျာ။

ဒီတစ်ခါ ပြန်ဖြည်ပြပေးမယ်။ ချုံထားတာကို ပြန်ဆွဲဆန့်ပြမယ်လို့ပြောတာပါ။ FF02 : 30 :: 5 ဆိုတော့ စဉ်းစားကြည့်ရအောင် IPv6 မှာ Block က 8 ခုရှိတယ်။ FF02 : 30 :: 5 ဆိုတော့ Block က FF02 ကတစ်ခု 30 ကတစ်ခု 5 က Block တစ်ခု သုံးခုရှိတယ် မဟုတ်လား။ ပုံမှန်ဆို Block က 8 ခုဆိုတော့ 8 ခုထဲက 3 ခုကိုနုတ် 5 ခုရမယ်။ အဲဒီ 5 ခုက 0 တွေပေါ့။ ဒီတော့က အဲဒီ 0 တွေကို (::) Double Colon ရှိတဲ့နေရာတွေမှာ အစားထိုးရပါလိမ့်မယ်။ ဒီတော့ FF02 : 30 : 0 : 0 : 0 : 0 : 0 : 5 ဖြစ်ပါတယ်။

ဒီလောက်ဆိုရင် IPv6 Address တွေကို ချုံပြီးရေးတတ်သွားလောက်ပါပြီ။

၂.၅ IPv6 အမျိုးအစားများ

IPv6 မှာဆိုလို့ရှိရင် Address အမျိုးအစား ၃ ခုရှိပါတယ်။ အဲဒါတွေကတော့ –

၁။ Unicast Address
၂။ Multicast Address
၃။ Anycast Address တို့ဖြစ်ကြပါတယ်။

Unicast Address နှင့် Multicast Address တို့ကျတော့ ရှေ့သင်ခန်းစာမှာလည်းပြောပြီးပါပြီ။ ဒါကြောင့် ဒီနေရာမှာ Anycast Address ကိုပဲ ပြန်ရှင်းပြပါတော့မယ်။

၂.၆ Anycast Address အကြောင်း

Anycast Address ဆိုတာ Unicast Address နှင့် Multicast Address စတဲ့ Address နှစ်ခုတို့ရဲ့ Concept ကိုပေါင်းထားတယ်လို့လည်းပြောလို့ရပါတယ်။ Unicast က ဘာပြောသလဲဆိုတော့ Unicast ဆိုတာ Address တစ်ခုကိုပဲ ဦးတည်ပြီးပို့တာ ဖြစ်ပါတယ်။ Multicast ကျတော့ Group တစ်ခုမှာရှိတဲ့ Member တိုင်းကို ပေးပို့ပေးတာပါတဲ့။

Anycast ကျတော့ Group ထဲက တစ်ယောက်ယောက်ဆီကို ပို့ပေးပါဆိုပြီးဖြစ်ပါတယ်။ ဒီနေရာမှာ Group လို့သုံးလိုက်တဲ့အတွက်ကြောင့် Multicast ရဲ့ Concept ဖြစ်သွားပါတယ်။ အဲဒီအထဲက တစ်ယောက်ယောက်ဆိုပြီးသုံးလိုက်တာကြောင့် Multicast ရဲ့ Concept က Unicast Idea ဖြစ်သွားပြန်ပါတယ်။ ဆိုလိုတာက Anycast ဆိုတာက လက်ခံသူဆယ်ယောက်ရှိမယ် ဆိုကြပါစို့ အဲဒီ ဆယ်ယောက်ထဲက

တစ်ယောက်စီကိုပဲပို့ချင်တာဖြစ်ပါတယ်။ ထပ်ရှင်းပြဦးမယ်။

(၁) လက်ခံသူတစ်ခုတည်းကို ဦးတည်ပြီးပို့ရင် Unicast
(၂) လက်ခံသူအများကြီးကို ဦးတည်ပြီးပို့ရင် Multicast
(၃) လက်ခံသူအများကြီးထဲကမှ တစ်ဦးဦးကိုပို့ချင်ရင် Anycast ဖြစ်ပါတယ်။

OK နော် ရှင်းပြစရာတစ်ခုကျန်သေးတယ်။ ဒီနေရာမှာတစ်ဦးဦးတစ်ယောက်ယောက်လို့ ဆိုထားပါတယ်။ ဒီလိုပါ အများကြီးထဲက တစ်ယောက်ကိုဆိုတာ ပေးပို့သူနှင့်အနီးဆုံးသူကိုပြောတာဖြစ်ပါတယ်။ အနီးဆုံးကို ဘာနှင့်တိုင်းတာသလဲဆိုတော့ Routing Distance နှင့်တိုင်းတာပါတယ်။

ဒီတော့ Anycast ဆိုတာပေးပို့သူနှင့် အနီးဆုံးရှိသော သူဟုပြောရပါလိမ့်မယ်။ အများကြီးထဲက တစ်ယောက်ဆိုတာပေးပို့သူနှင့် အနီးဆုံးရှိသောသူကိုပြောတာဖြစ်ပါတယ်။ လက်ခံတဲ့ Receiver က အများကြီး အဲဒီအများကြီးထဲကမှ ပေးပို့သူနှင့် အနီးဆုံးသောသူကို ပေးပို့မယ်။ ဒါဟာ Anycast ပါပဲ။ ဘိုလိုပြောရင်တော့ Send to the Closet Member of this Group ဖြစ်ပါတယ်။

Anycast Address တွေအတွက်သီးခြား Addressing ပုံစံမရှိပါဘူး။ Anycast Address တွေဟာ Unicast Address တွေပဲဖြစ်ကြပါတယ်။ ရှုပ်မသွားပါနဲ့။ Anycast Address ပုံစံရယ်လို့ သီးခြားမရှိဘဲ Unicast Address ဟာ တစ်ခုထက်ပိုသောနေရာကို ဦးတည်လိုက်တဲ့ အချိန်ကျမှ Unicast Address ဟာ Anycast Address အဖြစ်အလိုအလျောက်ဖန်တီးပေးလိုက်တာ ဖြစ်ပါတယ်။ ဒါကြောင့် Anycast Address ဟာ Unicast Address တွေပဲလို့ပြောတာဖြစ်ပါတယ်။ ခုချိန်မှာတော့ Anycast Address တွေကို Hosts တစ်ခုချင်းစီကနေ အသုံးမပြုကြသေးဘဲ Routes တွေကသာလျှင် အသုံးပြုလျက်ရှိပါသေးတယ်။

၂.၇ IPv6 Unicast Address အမျိုးအစားများ

အောက်မှာ IPv6 Unicast Address အမျိုးအစားများကိုဖော်ပြပေးထားပါတယ်။

၁။ Global Unicast Address
၂။ Link - Local Address
၃။ Site - Local Address
၄။ Unique Local Address
၅။ Special IPv6 Address

Product of YOUTH

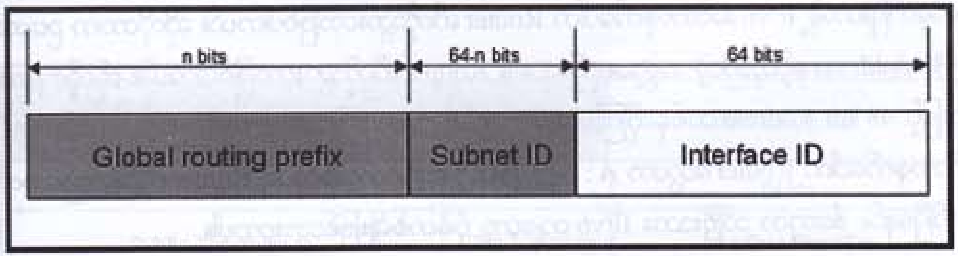
Transition Address တို့ဖြစ်ကြပါတယ်။

၂.၄ Global Unicast Address အကြောင်း

Global Unicast Address ဆိုတာ IPv4 တုန်းက ကျွန်တော်ရှင်းပြခဲ့တဲ့ Public Address နှင့် တူတူပဲဖြစ်ပါတယ်။ ၎င်းဟာ ကမ္ဘာလုံးကို Route လုပ်နိုင်တဲ့အပြင် Internet မှာရှိတဲ့ IPv6 အပိုင်းဆီကိုလည်း သွားနိုင်ပါတယ်။ အင်တာနက်မှာ IPv4 အပိုင်းရှိသလို IPv6 အပိုင်းလည်း ရှိတယ်ဗျာ။ IPv6 အပိုင်းထိ ၎င်း Address တွေကသွားနိုင်တယ်ကိုပြောတာ။ ဒါတွေက Routing ကို နားလည်မှပိုရှင်းလိမ့်မယ်။ Routing ကိုနောက်ပိုင်း သင်ခန်းစာတွေမှာ ထည့်ပေးထားပါတယ်။

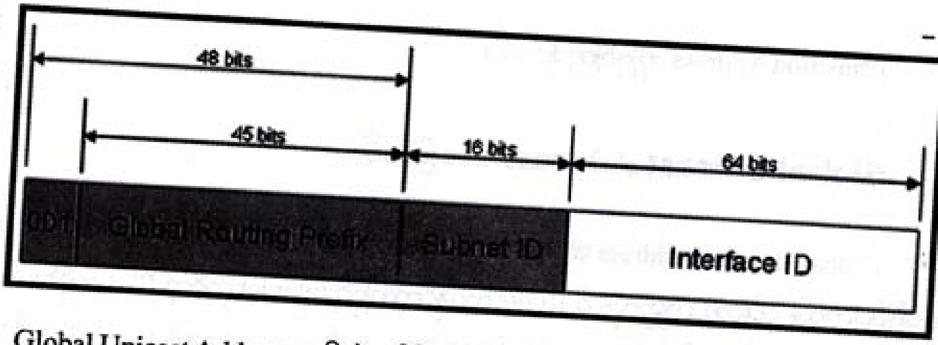
Routing လုပ်တဲ့နေရာမှာလည်း မြန်ဆန်စေဖို့အတွက် Efficient ဖြစ်တဲ့ Routing Infrastructure ရဲ့ Global Unicast Address တွေကို ပေါင်းခြင်း၊ စုပေါင်းခြင်း၊ စုစည်းခြင်း၊ Summerise လုပ်ခြင်းများ ပြုလုပ်လို့ရပါတယ်။ နောက်တစ်ခုက အခုအသုံးပြုနေတဲ့ IPv4 အင်တာနက် Routing ပုံစံ (၂) မျိုးဖြစ်တဲ့ Flat Routing ရော Hierarchical Routing ရော ၂ ခုကို ရောပြီး အခြေခံထားတဲ့ အင်တာနက် ဖြစ်ပါတယ်။ ဒါပေသိ IPv6 ကို Based လုပ်ထားတဲ့ အင်တာနက်ကျတော့ Efficient ဖြစ်ဖို့ကို အခြေခံထားတာကြောင့် Address ပိုင်းဆိုင်ရာရော Routing ပိုင်းဆိုင်ရာပါ Hierarchical ပုံစံကိုပဲ အသုံးပြုပါတယ်။ Global Unicast Address တွေဟာ IPv6 ရဲ့ အင်တာနက်တစ်ခုလုံးမှာ တစ်ခုနှင့်တစ်ခု ထပ်တူညီခြင်း၊ တူညီခြင်း မဖြစ်ရပါဘူး။ ဒါကတော့ ထုံးစံအတိုင်းပေါ့။ ခုပြောပြတဲ့ အကြောင်းအရာတွေထဲက Routing နှင့်ပတ်သတ်တာတွေက Routing သင်ခန်းစာကို ဖတ်ပြီးမှ ပိုနားလည်လာနိုင်မှာဖြစ်ပါတယ်။

ပုံ ၂၅



ဒီပုံက တကယ်တော့ Global Unicast Address ရဲ့ ယေဘုယျအားဖြင့် သတ်မှတ်ထားတဲ့ General Structrue ပဲဖြစ်ပါတယ်။ ၎င်းကို IANA က အောက်ပါပုံအတိုင်းပြန်သတ်မှတ်ပါတယ်။ ပြောရရင်တော့ သတ်မှတ်ဆဲပေါ့နော်။ ဆိုတော့ လောလောဆယ်ဒါကိုပဲ ရှင်းပြထားလိုက်မယ်။

ပုံ ၂.၆



Global Unicast Address မှာရှိတဲ့အပိုင်းတွေကို ရှင်းပြပါ့မယ်။

၁။ Fixed Portion (Set to 001)

ရှေ့ဆုံးက 3 Bit ကို 001 ဆိုပြီးသတ်မှတ်ပါတယ်။

၂။ Global Routing Prefix

Global Routing Prefix ဆိုတာက အဲဒီ Address ကိုပိုင်တဲ့အဖွဲ့အတွက်ကို ရည်ညွှန်းတာဖြစ်ပါတယ်။ IPv4 Illegal Address တုန်းကလည်းရှင်းပြခဲ့ပြီးသားဖြစ်ပါတယ်။ 206.73.118.0 / 24 ဆိုတာ IANA က Microsoft အတွက်သတ်မှတ်ထားပြီးသား အဲဒါကိုပြောတာ ဒီတော့ Global Routing Prefix က 45 Bit ရှိတယ်။ ရှေ့က အသေထားတဲ့ 3 Bit နှင့်ဆိုအားလုံး 48 Bit ဖြစ်ပါတယ်။ အဲဒီ 48 Bit အဖွဲ့အစည်းရဲ့ Site ကိုသတ်မှတ်တဲ့အပိုင်း ဖြစ်ပါတယ်။ ၎င်း 48 Bit ကိုကြည့်ပြီးစကတော့ဖြင့် ဒီအဖွဲ့အစည်းရဲ့ Site ပဲ။ ဒါကတော့ဖြင့် ဟိုအဖွဲ့အစည်းရဲ့ Site ပဲ စသဖြင့်ဖြစ်ပါတယ်။ ဒီတော့ အဲဒီ Address ကိုတစ်ခါ သတ်မှတ်ပြီးတာနဲ့ IPv6 အင်တာနက်ပေါ်က Router ဆီကိုသွားတာဖြစ်ပါတယ်။ ဆိုလိုတာက ဥပမာအားဖြင့် 48 Bit Address နှင့်တူညီတဲ့ အဖွဲ့အစည်းများ၏ Router ဆီကိုသွားတာဖြစ်ပါတယ်။ ဆိုလိုတာက ဥပမာအားဖြင့် 48 Bit Address တစ်ခုဆိုကြပါစို့ A : B : C ဟာ ကျွန်တော့်အလုပ်ရဲ့ Address ဖြစ်မယ်။ ဒါဆို အင်တာနက်ပေါ်က Router တွေဟာ A : B : C ဖြစ်တဲ့ ကျွန်တော်အလုပ်ရဲ့ Router ကိုဦးတည်လာလိမ့်မယ်။ ဟုတ်ပြီနော်။ ဒါတွေက သိပြီးသား IPv6 ကျတော့ ပုံစံတစ်မျိုးဖြစ်သွားတာပါ။

၃။ Subnet ID

Subnet ID ဆိုတာကျတော့ အဲဒီ Organisation Site ထဲက Subnet ကိုရည်ညွှန်းတာဖြစ်ပါတယ်။ ဒီ Subnet ID Field ဟာ 16 Bits ရှိပါတယ်။ ဒီတော့ကား အဲဒီ Organisation ဟာ ဒီ Subnet ID 16 Bits

ကြောင့် သူတာ Subnets ပေါင်း 65536 ကိုဖန်တီးနိုင်ပါတယ် ဒါမှမဟုတ် အဲဒီ 16 Bit ကို Subnet ခွဲသင့်သည့်တိုင် Address တွေကို Multiple Level Hierarchy ပုံစံပြုလုပ်နိုင်ပါတယ်။ တနည်းအားဖြင့်

၄င်း 16 Bit ကို Efficient ဖြစ်တဲ့ Routing Infrastructure အတွက်အသုံးပြုနိုင်ပါတယ်။ ဒီ Subnet အကြောင်းကတော့နောက်သင်ခန်းစားများ ရှင်းပြမယ့် Subnetting သင်ခန်းစာဖတ်ပြီးမှပိုနားလည်လာပါလိမ့်မယ်။

၃ Interface ID

Interface ID ကတော့ 64 bit ရှိပါတယ်။ ၄င်းဟာ အဲ့ဒီ Organization Sote အတွင်းမှာရှိတဲ့ Subnet ထဲက Interface တစ်ခု ကိုဆိုလိုတာဖြစ်ပါတယ်။

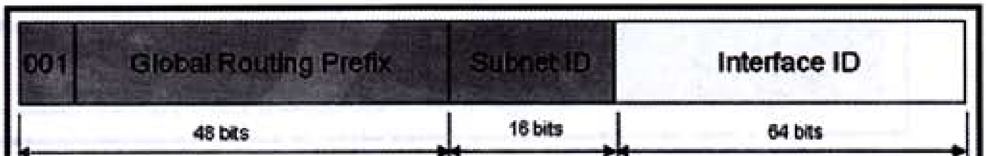
ဥပမာအားဖြင့်ပြောရရင် –

2001: DB 8: F282: 2B0: D0FE: FEE9: 4143 ဆိုတာ Global Unicast Ipv6 Address တစ်ခုဖြစ်ပါတယ်။ အဲ့ဒီ Address မှာ–

- 2001: DB8: 2A3C ဆိုတာကအဖွဲ့အစည်းရဲ့ Site ကိုရည်ညွှန်းပါတယ်။
- F282 ကတော့ အဲ့ဒီ Site ရဲ့ Subnet ကိုရည်ညွှန်းပါတယ်။
- 2B0: D0FF: FEE9: 4143 ဆိုတာကျတော့အဲ့ဒီ Site မှာရှိတဲ့ Subnet ပေါ်က Interface ID တစ်ခုဖြစ်ပါတယ်။

အခုရှင်းပြပြီးသလောက်ကို Structure ပုံစံဖြင့်ပြန်ရှင်းပြပါဦးမယ်။ Structure ဆိုတာ အပိုင်းလိုက် ခွဲရင် အပိုင်းအားဖြင့် (၃) ပိုင်းရှိပါတယ်။ အောက်က ပုံမှာကြည့်ပါ။

ပုံ ၂၇



အဲ့ဒီမှာ Public Topology ဆိုတာ Global Routing Prefix နှင့် ရှေ့က Fixed ဖြစ်နေတဲ့ High Order Bits တို့ပေါင်းတာပါ။ ဒီ Public Topology ဆိုတာ IPv6 အင်တာနက်ကိုချိတ်ဆက်ထားတဲ့အဖွဲ့အစည်းတွေကိုစုစည်းပေးထားတဲ့အပိုင်းဖြစ်ပါတယ်။

Site Topology ဆိုတာကတော့ Organisation Site ထဲက Subnet များစုစည်းထားတဲ့နေရာပါပဲ။

Interface ID ကတော့အပေါ်မှာရှင်း ပြထားတဲ့အတိုင်းဖြစ်ပါတယ်။ ဒါက Global Unicast Address ဖြစ်ပါတယ်။

Local မှာသုံးတဲ့ Local-Use Unicast Address ကျတော့တစ်ခါနှစ်မျိုးထပ်ခွဲပြန်ပါတယ်။ အဲ့ဒါက–

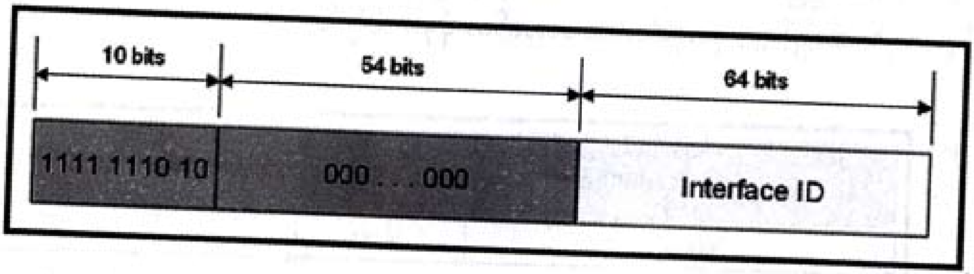
- ❖ Link- Local Address နှင့်
- ❖ Site - Local Address တို့ဖြစ်ပါတယ်။

၂.၉ **Link Local Address** များအကြောင်း

Network တစ်ခုမှာရှိတဲ့ Host တွေအချင်းချင်း ဆက်သွယ်ချင်တဲ့အခါမှာ Link Local Address ကိုအသုံးပြုပါတယ်။ Network တစ်ခုထဲမှာဆိုတော့ Router မရှိသော IPv6 ရဲ့ Network Link တစ်ခုတည်းတွင်ရှိကြသော Nodes များအကြားဆက်သွယ်တဲ့အခါမှာ ဒီ Link Local Address ကိုသုံးပါတယ်။ ၎င်းဟာတကယ်တော့ IPv4 တုန်းကပြောခဲ့တဲ့ (Automatic Private IP Address) နှင့်တူတူပဲဖြစ်ပါ တယ်။ APIPA ဆိုတာ Windows ရှိတဲ့ကွန်ပျူတာတွေမှာ Address တွေကိုအလိုအလျောက်သတ်မှတ်ပေးတာလေ။ ရှေ့သင်ခန်းစာတုန်းကပြောခဲ့တယ်နော်။

Node တစ်ခုဟာမိမိရဲ့အနီးနားမှာရှိတဲ့ Node တွေကိုရှာဖွေခြင်းဆိုတဲ့ Neighbour Discovery Process ဆိုတာရှိပါတယ်။ ၎င်း Neighbour Discovery Process တို့ဟာ Link Local Address Prefix ကို လိုအပ်ပါတယ်။

ပုံ ၂.၈



ပုံမှာမြင်တွေ့ရတဲ့အတိုင်းပါပဲ။ Link Local Address ရဲ့ ရှေ့ 64 bits ဟာအသေဖြစ်ပါတယ်။ ဒါကြောင့် Link Local Address ရဲ့ Address Prefix ကိုဖော်ပြရမယ်ဆိုရင် FE80:1/64 ဖြစ်ပါတယ်။ /64 ဆိုတာရှေ့ 64 ကအသေလို့ပြောတာဖြစ်ပါတယ်။

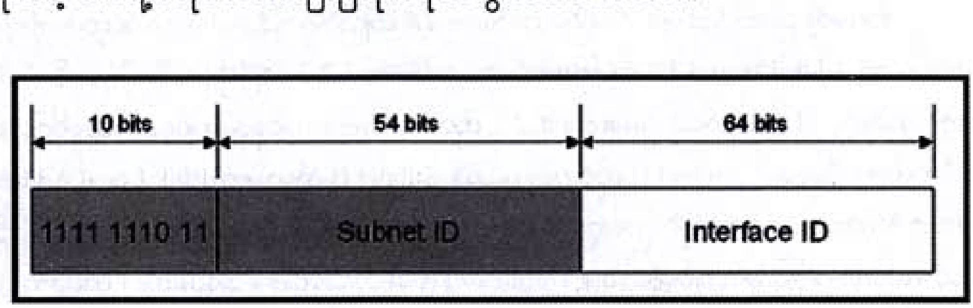
- F ကတော့ 1111 ဖြစ်ပါတယ်။
- Eကတော့ 1110 ဖြစ်ပါတယ်။
- 8 ကတော့ 1000 ဖြစ်ပါတယ်။ ဒါပေမယ့် ပုံမှာ 10 bits အထိပဲနေရာယူတာကြောင့် 1000 မှာ 10 ထိပဲနေရာယူတာပါ။ FE80 မှာသိရမှာက IPv6 ရဲ့အပိုင်း ၁ ခုမှာ 4 Digit ရှိရမယ်လေ ဒါကြောင့် FE8 အထိပဲရှိတာကို 4 Digit Hexadecimal ဖြစ်မယ် 0 ထည့်လိုက်တော့ FE80 ဖြစ်သွားတာပါ။

IPv6 ရဲ့ Router တွေဟာ Link Local Traffic တွေကိုတယ်တော့မှ Link တစ်ခုကျော်သွားအောင် Forward မလုပ်ကြပါဘူး။ ဆိုလိုတာက Link Local Traffic တွေဟာ Link တစ်ခုထဲမှာပဲရှိနေတာကိုပြောတာပါ။ ဥပမာ သင်ကဖုန်းဆက်တယ် ရှေ့က 01 ခံရင် ရန်ကုန်မြို့တွင်း 02 ခံရင် မန္တလေး ဆိုလိုတာက 01 ခံပြီးဆက်ရင်သင်ခေါ်လိုက်တဲ့ဖုန်းကရန်ကုန်မြို့တွင်းမှာပဲ Route ဖြစ်မယ်။ မန္တလေးကိုရောက်သွားစရာအကြောင်းမရှိဘူး ဘာလို့လည်းဆိုတော့ 01 ဖြစ်တဲ့အတွက် Exchange ရုံးကရန်ကုန်မြို့ပြင်ရောက်အောင် Forward မလုပ်လို့ဘဲဖြစ် တယ် ပေါက်တယ်နော်။

၂.၁၀ Site Local Address များအကြောင်း

Site Local Address ဆိုတာ IPv4 ရဲ့ Private Address Space နှင့်တူတူပဲဖြစ်ပါတယ်။ ပြန်ရှင်းပြရရင် Site Local Address တွေကို IPv6 အင်တာနက်နှင့် တိုက်ရိုက်ချိတ်ဆက်မထားတဲ့ Private Intranet တွေမှာအသုံးပြုခြင်းဖြင့် Global Address တွေနှင့် Conflict ဖြစ်ခြင်းကိုရှောင်ကြဉ်နိုင်ပါတယ်။ Site Local Address တွေဟာဒီ Site တစ်ခုအတွင်းမှာပဲအလုပ်လုပ်တာဖြစ်ပြီးတစ်ခြား Site တစ်ခုကို ရောက်ရှိသွားခြင်းအလျင်းမရှိကြပါဘူး။ ဘာဖြစ်လို့လည်းဆိုတော့ Router တွေကတစ်ခြား Site တစ်ခုဒါမှမဟုတ်လက်ရှိ Site ရဲ့ပြင်ပကိုရောက်ရှိ အောင် Forward မလုပ်ကြလို့ဘဲဖြစ်ပါတယ်။ ဒီနေရာမှာ Site ဆိုတာဘာကိုခေါ်တာလဲ ဆိုတာကိုတော့ Site ရဲ့အတိုင်းအတာပြောပြလိုက်ရင်သိသွားမယ်ထင်ပါတယ်။

ပုံ ၂၉



Site ဆိုတာအဖွဲ့အစည်းတစ်ခုရဲ့ Network တစ်ခုပဲဖြစ်ပါတယ်။ အဲ့ဒီ Network ဟာပထဝီဝင်အနေ အထားအရပဲဖြစ်ဖြစ် Topology အရပဲဖြစ်ဖြစ် Site Local Address က Link Local Address နှင့်မတူတဲ့ အချက်က Auto Configured မလုပ်တာဘဲ Link Local Address က Auto Configured လုပ်ပြီး Site Local Address က Auto Configured မလုပ်ဘူး Sateless ဒါမှမဟုတ် Stateful Address Configuration တစ်ခုခုကိုတော့သတ်မှတ်ပေးရပါတယ်။

ပုံ ၂၉ ကိုကြည့်ခြင်းအားဖြင့် Site Local Address ရဲ့ပထမ 10 bits က 1111 1110 11 ဆိုပြီး အသေဖြစ်နေတာတွေ့ရပါလိမ့်မယ်။ ဒါကြောင့် Site Local Address အားလုံးရဲ့ Address Prefix က FEC0::/10 ဖြစ်ပါတယ်။ ရှေ့ဆုံးကအသေထားတဲ့ High Order 10 bits ရဲ့နောက်မှာတော့ Subnet ID Field ရှိပါတယ်။ သူကတော့ 54 bits ဖြစ်ပါတယ်။ ၎င်း 54 bits Field ကိုအသုံးပြုခြင်းရဲ့ Organisation ထဲမှာ Subnet တွေကိုဖန်တီးပေးနိုင်ပါတယ်။ ဒီ 54 bits ဆိုတာ 254 ဖြစ်ပါတယ်။ ဒီတော့ 2 ကို 54 ခါမြှောက်လိုက်ရင်ရလာတဲ့ကိန်းဂဏန်းအရေ အတွက်အတိုင်း Subnet တွေခွဲလို့ရပါတယ်။ အဲ့ဒီလိုမှမဟုတ် လည်း Hierarchical Routing Infrastucture ကိုလည်းတည်ဆောက်နိုင်ပါတယ်။

ဒီ Subnet ID Field ရဲ့နောက်မှာတော့ Interface ID ရှိပါတယ်။ Interface ID ကတော့ 64 bits ဖြစ်ပါတယ်။

၂.၁၁ Zone IDs for Local Use Address အကြောင်း

ဒီ Local Use Address တွေဖြစ်ကြတဲ့ Link Local Address နှင့် Site Local Address တွေနှင့်ပတ်သက်ပြီး ပြောစရာတစ်ခုရှိလာ တယ်ဗျ။ အဲ့ဒါကတော့ Zone ID ပဲဖြစ်ပါတယ်။ ဒီ Local Address တွေဟာ အဖွဲ့အစည်းတစ်ခုရဲ့ Intranet တစ်ခုအတွင်းမှာ Address တွေဟာတစ်ခုနှင့်တစ်ခု ထပ်တူမရှိရဘူးဆိုတာတော့မှန်ပါတယ်။

ဒါပေမယ့် ဥပမာ Subnet တစ်ခုရှိမယ်။ Subnet A ဆိုကြပါစို့ အဲ့ဒီ Subnet A ထဲမှာပဲလှုပ်ရှားနေတဲ့ Address က Link Local Address ဖြစ်ပါတယ်။ Address 1,2,3 ဆိုပြီးရှိတယ်ပေါ့ဗျာ။ ဒီ Subnet A အတွင်းမှာရှိတဲ့ Link Local Address 1,2,3 ဟာ Address တစ်ခုနှင့်တစ်ခုထပ်တူမရှိရဘူးဆိုတာ မှန်ပါတယ်တဲ့ ဒါပေမယ့် Subnet B ဆိုတာရှိခဲ့ရင်အဲ့ဒီ Subnet B ထဲမှာရှိတဲ့ Link Local Address ဟာ Subnet A ထဲက Address နှင့်သွားတူနေလည်းကိစ္စမရှိဘူးလေ။ ဒါကိုပြောချင်တာ။ ထပ်ရှင်းပြဦးမယ်။ ဥပမာ Address ဆိုပြီးနှစ်ခုဖြစ်နေတယ်။ Duplicate ဖြစ်နေတယ်ပေါ့ဗျာ။ ဒါပေမယ့် 1 တစ်ခုက Subnet A မှာဖြစ်ပြီး နောက် 1 တစ်ခုက Subnet B ကဖြစ်နေတယ်။ ဒါဆိုကိစ္စမရှိဘူးပေါ့ဗျာ။ ဒါအရင်ကလည်း ရှင်းပြခဲ့ပူး ပါတယ်။ အခုကျွန်တော်ရှင်းပြချင်တာက ဒါမဟုတ်သေးဘူးဗျ ဒါစကားဖျာခင်းတုန်းပဲ အဲ့လေစကား

ကျွင်းကျန်တုန်းပဲရှိသေးတယ်။ ဒီလိုဗျ။ လာပြန်ပလား ဒီလိုဗျ။

ကျွန်တော်တို့က Subnet တစ်ခုမတားရှိခဲ့ရင်တနည်းအားဖြင့် Link တစ်ခုထပ်မထားရှိခဲရင် Address 1 ကိုသွားပါလို့ပြောရုံနဲ့မရတော့ ဘူး။ အဲ့ဒီ Address 1 ဟာ Subnet A ကလား B ကလားဆိုပါထည့်ပြောဖို့ လိုသွားပြီလို့ဆိုလိုချင်တာဖြစ်ပါတယ်။ တစ်နည်းအားဖြင့်အဲ့ဒီကိုယ်သွား ချင်တဲ့ Address 1 ရှိ Link ကိုပါထည့် ပြောနိုင်ဖို့လိုသွားပြီလို့ဆိုလိုတာပါ။ ဒီအတိုင်းပဲ Site Local Address ကိုထပ်စဉ်းစားကြည့်ရအောင်၊ ခုနက ပြောသလို Site တွေတစ်ခုမကရှိခဲ့မယ်ဆိုရင်ကျွန်တော်တို့ဟာ ဘယ်ကိုသွားမယ်လို့ပြောရုံနှင့်မပြီးတော့ဘူး။ ကျွန်တော်တို့သွားမယ့် နေရာကဘယ် Site မှာရှိပါတယ်ဆိုတာကိုပါထည့်ပြောဖို့လိုသွားပြီဖြစ်ပါတယ်။

ကျွန်တော်တို့တွေဟာ Zone ID ကိုအသုံးပြုပြီး Network တစ်ခုရဲ့ အပိုင်း ၁ ပိုင်း Portion ပေါ့ဗျာ တနည်းအားဖြင့်ပြောရရင် Zone ပေါ့ဗျာ။ အဲ့ဒီ Zone ကိုထည့်ပြောပေးဖို့လိုပါတယ်။

ဘယ်အခါမှာလဲ – ဘယ်အခါမှာလဲဆိုတော့ –

- Ping Command
- Tracert Command နှင့်
- Pathping Command စတဲ့ Command တွေကိုအသုံးပြုတဲ့အခါ Zone ID ကိုအသုံးပြုနိုင်ပါတယ်။

ဥပမာ– Ping IPv6Address% Zone ID ဆိုပြီးဖြစ်ပါတယ်။

အောက်ကပုံမှာကြည့် – ping fe80::5efe:169.254.25.219%11

အဲ့ဒီမှာ 11 က Zone ID ကိုပြောတာ။

ပုံ ၂၁၀

```
C:\Users\NANDA>ping fe80::5efe:169.254.25.219%11

Pinging fe80::5efe:169.254.25.219%11 from fe80::5efe:169.254.25.219%11
ytes of data:

Reply from fe80::5efe:169.254.25.219%11: time<1ms
Reply from fe80::5efe:169.254.25.219%11: time<1ms
Reply from fe80::5efe:169.254.25.219%11: time<1ms
Reply from fe80::5efe:169.254.25.219%11: time<1ms

Ping statistics for fe80::5efe:169.254.25.219%11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\NANDA>_
```

ဒီနေရာမှာမေးစရာရှိလာပါတယ်။ ကျွန်တော်တို့က Zone ID ကိုထည့်ရိုက်ဖို့ရာ ZoneID ကိုဘယ်လို သိနိုင်မလဲဆိုတာပဲဖြစ်ပါတယ်။ Link အရပြောရရင် Zone ID ဆိုတာကိုယ်သွားချင်တဲ့ Destination တည်ရှိ

နေတဲ့ Link နှင့်ချိတ်ဆက်ထားတဲ့ Interface ရဲ့ Interface Index ပဲဖြစ်ပါတယ်။ သူ့ကို ဘယ်လိုသိနိုင်မလဲဆိုတော့ -

netsh interface ipv6 show interface

ဆိုပြီး Command ရိုက်ထည့်လိုက်ခြင်းဖြင့်သိနိုင်ပါတယ်။ အဲ့ဒီလိုသိရပြီဆိုတော့မှတစ်ခါ Ping မှာငင်းကိုပြန်သုံးမှာဖြစ်ပါတယ်။ အောက်ကပုံမှာ Idx ဆိုတာ Index ဖြစ်ပါတယ်။ ၎င်းသည်ပင်လျှင် Zone ID ဖြစ်ပါတယ်။

ပုံ ၂.၁၁

```
C:\Users\NANDA>netsh interface ipv6 show interface

Idx  Met   MTU         State         Name
---  ---  ----------  ------------  --------------------------
  1   50  4294967295  connected     Loopback Pseudo-Interface 1
 10   25        1280  connected     Local Area Connection* 6
 11   25        1280  connected     Local Area Connection* 7
  8   20        1500  connected     WAN <ON BOARD>
  9   20        1500  connected     LAN <NIC CARD>
 12   10        1280  disconnected  Local Area Connection* 10

C:\Users\NANDA>_
```

Site Local Address အရပြောရင်တော့ Zone ID တာ Site Number ပဲဖြစ်ပါတယ်။ ၎င်းကိုလည်း netsh command နှင့်ကြည့်လို့ရပါတယ်။

netgh interface ipv6 show address level = verbose

ဆိုပြီးရိုက်ထည့်လိုက်ခြင်းဖြင့်သိနိုင်ပါတယ်။ ပုံ ၂.၁၂ ကိုကြည့်ပါ။

အကယ်၍များကျွန်တော်တို့ဟာ Site တွေအများကြီးမရှိဘဲ Single Site ပဲဆို ဒါတွေကိုသုံးဖို့မလိုအပ်ပါဘူး။ နောက်တစ်ခုက Global Unicast Address တွေမှာ ZoneID ကိုအသုံးပြုစရာမလိုအပ်ပါဘူး။

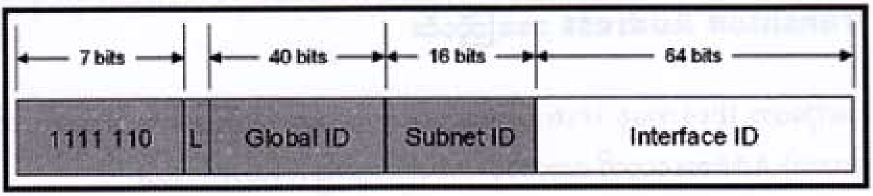
ပုံ ၂၁၂

```
C:\Users\NANDA>netsh interface ipv6 show interfaces level=verbose

Interface Loopback Pseudo-Interface 1 Parameters

IfLuid                              : loopback_0
IfIndex                             : 1
Compartment Id                      : 1
State                               : connected
Metric                              : 50
Link MTU                            : 4294967295 bytes
Reachable Time                      : 20000 ms
Base Reachable Time                 : 30000 ms
Retransmission Interval             : 1000 ms
DAD Transmits                       : 0
Site Prefix Length                  : 64
Site Id                             : 1
Forwarding                          : disabled
Advertising                         : disabled
Neighbor Discovery                  : disabled
Neighbor Unreachability Detecion    : disabled
Router Discovery                    : enabled
Managed Address Configuration       : disabled
Other Stateful Configuration        : disabled
Weak Host Sends                     : disabled
Weak Host Receives                  : disabled
Use Automatic Metric                : enabled
Ignore Default routes               : disabled
```

၂.၁၂ **Unique Local Address အကြောင်း**

Site Local Address တွေဟာ Intranet Traffic Global Address တွေကိုအသုံးပြုရန်နောက်ထပ် ပုံစံတစ်မျိုးနှင့်ပံ့ပိုးပေးထားတဲ့ Private Address တွေကို Unique Local Address လို့ခေါ်ပါတယ်။ နားမလည်ရင် Site Local Address ရှင်းလင်းချက်အစပိုင်းကိုပြန်ဖတ်ကြည့်လိုက်ပါ။ ဒီတော့ Unique Local Address ဟာ Site Local Address ကပံ့ပိုးပေးထားတဲ့ Private Address ပဲဖြစ်တယ်။

ပုံ ၂၁၃



ဒီ Unique Local Address မှာ ပထမဦးဆုံးသော 7 bits ဟာဆိုရင်ဖြင့် 1111110 ဆိုပြီး အသေဖြစ်ပါတယ်။ ဒီတော့ထုံးစံအတိုင်းအား လုံးသော Unique Local Address တွေရဲ့ Address Prefix က FC00::/7 ဖြစ်ပါတယ်။ အဲ့ဒီမှာ L ဆိုတာက Flag ဖြစ်ပါတယ်။ Local လို့ခေါ်ပါတယ်။ နောက်မှာ Flag နှင့်ပတ်သတ်လို့ရှင်းပြချက်ပါရှိပါမယ်။ L က 1 bit တနေရာယူပါတယ်။ နောက်တစ်ခုကတော့ Global

ID ဖြစ်ပါတယ်။ သူကတော့ Organisation ထဲက Site တစ်ခုရည်ညွှန်းတာဖြစ်ပြီး Subnet ID တို့ Interface ID တို့ကလည်းအရင် Address တွေရှင်းပြခဲ့တုန်းက အတိုင်းပဲဖြစ်ပါတယ်။

၂.၁၃ **Special IPv6 Address အကြောင်း**

Special IPv6 Address (၂) ခုရှိပါတယ်။ ထုံးစံအတိုင်းပါပဲ။ တနည်းအားဖြင့် IPv4 အတိုင်းပါပဲ။

၁။ Unspecified Address နှင့်

၂။ Loopback Address တို့ဖြစ်ကြပါတယ်။

Unspecified Address ဆိုတာကတော့ (0 : 0 : 0 : 0 : 0 : 0 : 0 :0) ပဲဖြစ်ပါတယ်။ သူ့ကို (::) ကိုလည်းရေးနိုင်ပါတယ်။ သူ့က ဘာကိုရည်ညွှန်းတာလဲဆိုတော့ IPv4 တုန်းက 0.0.0.0 လိုပဲ မရှိဘူးဖြစ်ပါတယ်။ ဒီ Address က ဘာမှမရှိခြင်းကိုရည်ညွှန်းပါတယ်။

Loopback Address ဆိုတာကတော့ (0 : 0 : 0 : 0 : 0 : 0 : 0 : 1) ပဲဖြစ်ပါတယ်။ သူ့ကို (::1) လို့လည်းရေးနိုင်ပါတယ်။ ၎င်းကတော့ IPv4 တုန်းကတော့ 127.0.0.1 ဆိုတဲ့ Loopback Address နှင့် တူတူပဲဖြစ်ပါတယ်။ သူ့ကို Node တွေက Packets များကိုယ့်ဆီကိုပြန်ပို့တဲ့နေရာမှာ အသုံးပြုပါတယ်။ ၎င်း Loopback Address က Network ကိုဘယ်တော့မှ ရောက်ခြင်းမရှိသလို IPv6 Router တွေဆီကို ရောက်သွားခြင်းလည်း မရှိပါဘူး။

၂.၁၄ **Transition Address အကြောင်း**

၎င်းကိုတော့ IPv4 ကနေ IPv6 အဖြစ်ပြောင်းတဲ့နေရာမှာ အသုံးပြုပါတယ်။ သူနှင့်ပတ်သတ်ပြီး ရှင်းပြစရာရှိလာတဲ့ Address တွေကို အောက်မှာတစ်ခုခြင်းရှင်းပြပေးထားပါတယ်။

၁။ IPv4 Compatible Address

၎င်းရဲ့ Address ပုံစံက 0 : 0 : 0 : 0 : 0 : 0 : w . x . y . z ဖြစ်ပါတယ်။ သူ့ကို (:: w . x . y . z) လို့လည်းရေးနိုင်ပါတယ်။ အဲဒီနေရာမှာ w . x . y . z ဆိုတာဟာ IPv4 Address ရဲ့ Dotted Decimal

ကိုဖြေတာဖြစ်ပါတယ်။ ၎င်း Address ကို IPv6/ IPv4 Nodes တွေက IPv6 ကိုလှမ်းချိတ်တဲ့အခါ သုံးပါတယ်။ IPv6 / IPv4 ဆိုတာ IP Version 6 ရော IP Version 4 ရောသုံးထားတဲ့ Node တွေကိုဆိုလိုတာပါ။ ဒီတော့ပြန်ပြောရရင် IPv6 ရော IPv6 ရောသုံးထားတဲ့ Node တွေဟာ IPv6 ပဲရှိတဲ့ Node တွေကိုဆက်သွယ်တဲ့အခါမှာ သုံးတဲ့ Address ပုံစံဖြစ်ပါတယ်။ Windows Server 2003 နှင့် Windows XP မှာ IPv6 အတွက် IPv4 Compatible Address ယခုရှင်းပြနေသော Address တွေပါရှိကြသော်လည်းပဲ ၎င်းတို့ဟာ Default အရ Disable ဖြစ်နေတာပါ။ Window Server 2008 နှင့် Windows Vista တို့ကတော့ IPv6 အတွက် ၎င်း O/S တွေမှာ IPv4 Compatible Address များကို Support လုပ်ပါတယ်။

၂။ IPv4 Mapped Address

IPv4 Mapped Address ကတော့ 0 : 0 : 0 : 0 : 0 : FFFF : w . x . y . z ဆိုပြီးဖြစ်ပါတယ်။ သို့မဟုတ် (:: FFFF . w .x . y . z) ဆိုပြီးရေးလည်းရပါတယ်။ IPv4 Mapped Address ကို IPv6 Packet ရဲ့ Source Address ပဲဖြစ်ဖြစ် Destination Address ပဲဖြစ်ဖြစ် အသုံးပြုလေ့မရှိဘဲ Internally ပဲ အသုံးပြုကြပါတယ်။ ဆိုလိုတာက Node တစ်ခုရဲ့ အတွင်းမှာပဲ သူ့ကိုအသုံးပြုပြီး ဒီ Node ကနေ (source) တခြား Node (Destration) စသဖြင့်သွားခြင်းလာခြင်း Send လုပ်ခြင်းတို့ မရှိကြပါဘူး။ Windows Server 2003 နှင့် Windows XP တို့ဟာ IPv6 အတွက် IPv4 Mapped Address ကို Support လုပ်ကြပါတယ်။

၃။ 6to4 Address

6to4 Address တွေက IPv4 ရော IPv6 ရော နှစ်ခုစလုံးသုံးထားတဲ့ Node နှစ်ခုဟာ Internet ပေါ်ကနေ အချင်းချင်းဆက်သွယ်တဲ့ နေရာမှာ သုံးပါတယ်။ ၎င်း Address ဟာ Prefix အရပြောရင် 48 Bit ရှိပါတယ်။

၄။ ISATAP Address

Intra - Site Automatic Tunnel Addressing Protocol ကနေသတ်မှတ်လိုက်တဲ့ ဒီ ISATAP ဆိုတဲ့ Address ကို IPv4 ရော IPv6 ရော နှစ်ခုစလုံး Routing ဖြစ်နေတဲ့ Node နှစ်ခုဟာ Private Intranet ကိုအသုံးပြုပြီး အချင်းချင်းဆက်သွယ်တဲ့နေရာမှာ အသုံးပြုပါတယ်။

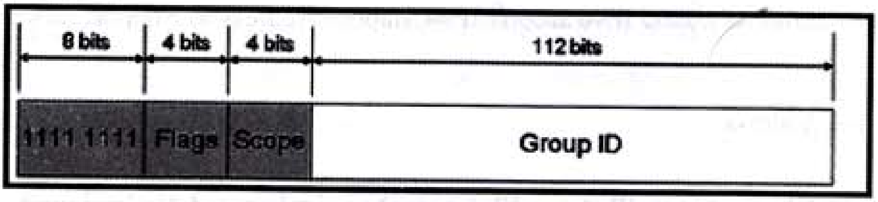
၅။ Teredo Address

သူကကျတော့ တစ်မျိုးဗျ IPv4 နှင့် IPv6 နှစ်ခုစလုံးကို Running ဖြစ်နေတဲ့ Node နှစ်ခုဟာ အင်တာနက်ကနေ အချင်းချင်းဆက် သွယ်တဲ့အခါသုံးတယ်ဆိုပေမယ့် ၎င်း Node နှစ်ခုထဲက Node တစ်ခုကဖြစ်စေ Node နှစ်ခုစလုံးဖြစ်စေ IPv4 NAT (Network Address Translation) Device ရဲ့ တခြားတစ်ယောက်တည်းရှိနေတဲ့အခါမှ အသုံးပြုတာဖြစ်ပါတယ်။

၂. ၁၅ IPv6 Multicast Address အကြောင်း

Multicast ဆိုတာကတော့ ရှေ့မှာကတည်းကရှင်းပြထားပြီးသားဖြစ်ပါတယ်။ IPv6 Multicast Address တွေရဲ့ရှေ့ဆုံး 8 Bit က 1111 1111 ဖြစ်ပါတယ်။ ဒါအသေပေါ့။ ဒါကြောင့်မို့လို့ အားလုံးသော IPv6 Multicast Address တွေရဲ့ Address Prefix က FF00 :: 18 ဖြစ်ပါတယ်။ အဲဒီ 8 Bits ရဲ့နောက်မှာတော့ Multicast Address တွေမှာ ယခင်နှင့်မတူတစ်မူထူးခြားတဲ့ အပိုင်းတွေပါဝင်လာပါတယ်။ အဲဒါတွေကတော့ Flags, Scope နှင့် Group ID တို့ပဲဖြစ်ပါတယ်။

ပုံ ၂.၁၄



၁။ Flags

လွယ်လွယ်ပြောရင် အလံပေါ့ဗျာ။ ဟုတ်ကဲ့ ရှင်းသွားတာပဲ။ ဒီလိုပါ။ တစ်စုံတစ်ခုကို ညွှန်းချင်လို့ သူက Flag ဆိုပြီးသုံးလိုက်တာပါ။ အဲဒီ Flags Field မှာ 4 Bits ရှိပါတယ်။ အကယ်၍များ Flag ဟာ 0 ဖြစ်ခဲ့ရင် ဒါဟာဘာကိုညွှန်းသလဲဆိုတော့ ဒီ Address ကို IANA က အသေမှတ်ထားတဲ့ Address အသုံးပြုထားတယ်လို့ပြောချင်တာဖြစ်ပြီး 1 ဖြစ်နေမယ်ဆိုရင်တော့ ၎င်းအလံလေးဟာ ဘာကိုညွှန်းချင်သလဲဆိုရင် Multicast Address ဟာ အသေမဟုတ်သော Multicast Address ကို အသုံးပြုထားတယ်ဆိုပြီး ဖြစ်ပါတယ်။

၂။ Scope

၎င်း Multicast Address သွားရမယ့် IPv6 Network ရဲ့ Scope အကျယ်အဝန်းအတိုင်းအတာကို ဖော်ပြတာဖြစ်ပါတယ်။ အရွယ်အစားကတော့ 4 Bits ပဲဖြစ်ပါတယ်။ Multicast Routing Protocol က ပေးပို့ပေးတဲ့ ဒီ Scope နှင့်အချက်အလက်တွေကို Router တွေက အသုံးပြုမှသာ ဒီ Multicast Traffic တွေအများကို Forward လုပ်နိုင်မှာဖြစ်ပါတယ်။ ဒီ Scope နှင့်ပတ်သတ်လို့တန်ဖိုးတွေ သတ်မှတ်ထားတာ ရှိပါတယ်။ အဲဒါတွေကတော့ –

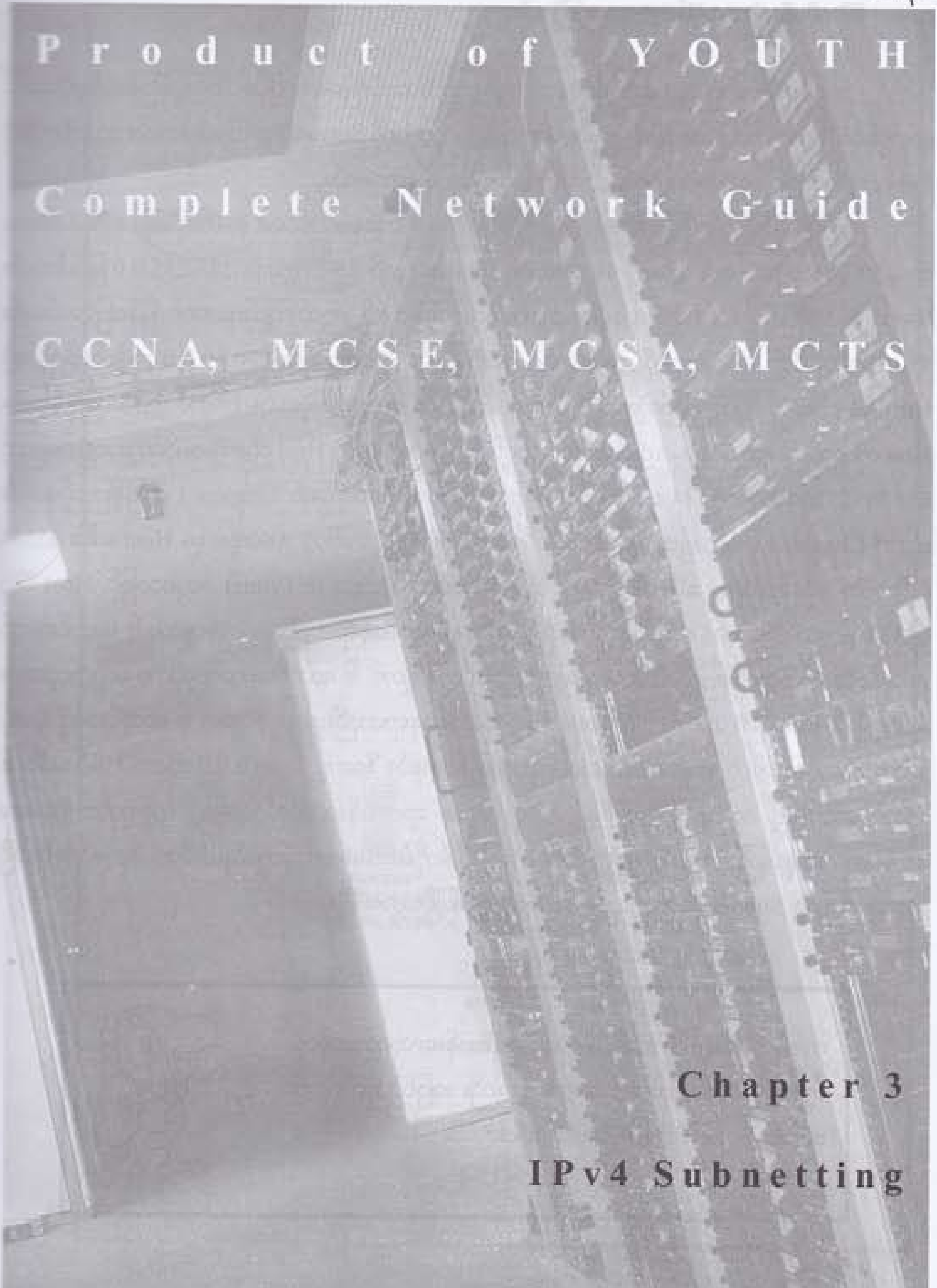
- 1 ဆိုရင် Interface - Local Scope
- 2 ဆိုရင် Link - Local Scope
- 5 ဆိုရင် Site - Local Scope တို့ဖြစ်ကြပါတယ်။

၃။ Group ID

Multicast Group ကိုသတ်မှတ်တာဖြစ်ပြီး ၎င်း Scope တစ်ခုအတွင်းမှာတော့ Unique ဖြစ်ရမှာ ဖြစ်ပါတယ်။ ၎င်းရဲ့အရွယ်အစားကတော့ 112 Bits ရှိပါတယ်။ အသေသတ်မှတ်ထားတဲ့ Group ID တွေကတော့ ၎င်း Scope နှင့်သတ်ဆိုင်ခြင်း မရှိပါဘူး။

နောက်ဆုံးနိဂုံးချုပ်အနေနဲ့ IPv4 နှင့် IPv6 တို့ရဲ့ နှိုင်းယှဉ်မှုလေးကို တစ်ဖက်မှာ ဇယားနှင့်ဖော်ပြပေးထားပါတယ်။

IPv4 Address	IPv6 Address
Internet address classes	Not applicable in IPv6
IPv4 multicast addresses (224.0.0.0/4)	IPv6 multicast addresses (FF00::/8)
Broadcast addresses: network broadcast, subnet broadcast, all-subnets directed broadcast, limited broadcast	Not applicable in IPv6
Unspecified address is 0.0.0.0	Unspecified address is ::
Loopback address is 127.0.0.1	Loopback address is ::1
Public IPv4 addresses	Global unicast addresses
Private IPv4 addresses (10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16)	Site-local addresses (FEC0::/10)
APIPA addresses (169.254.0.0/16)	Link-local addresses (FE80::/64)
Address syntax: dotted decimal notation	Address syntax: colon hexadecimal format with suppression of leading zeros and zero compression.Embedded IPv4 addresses are expressed in dotted decimal notation.
Address prefix syntax: prefix length or dotted decimal (subnet mask) notation	Address prefix syntax: prefix length notation only



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 3

IPv4 Subnetting

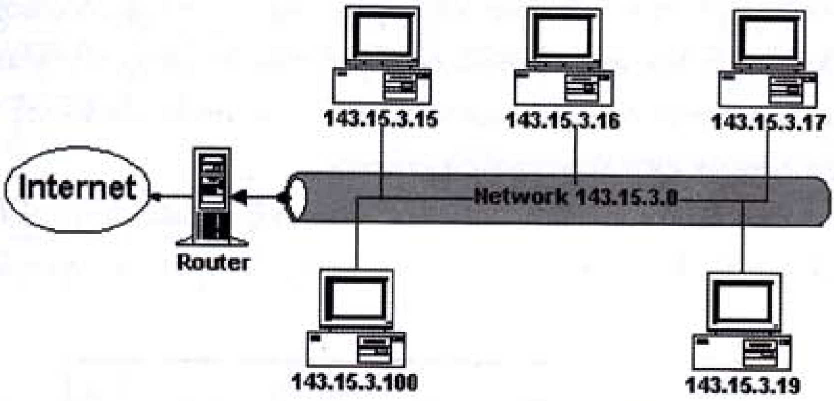
၃.၁ **IPv4 Subnetting အကြောင်း**

သင့်ရဲ့အဖွဲ့အစည်းမှာ အသုံးပြုနေတဲ့ ကွန်ရက်ကိုအသုံးပြုရတာ ပိုမိုကောင်းမွန်မြန်ဆန်မှုရှိအောင် ၄င်းကွန်ရက်ကိုပိုင်းလိုက်ပြီးဆင့်ပွား ကွန်ရက်တည်ဆောက်တာကို Subnetting လို့ခေါ်ပါတယ်။ ဘာဖြစ်လို့ဒီလို Subnet (ဆင့်ပွား Network) ခွဲရသလဲဆိုတာကို ရှင်းပြပါတော့မယ်။

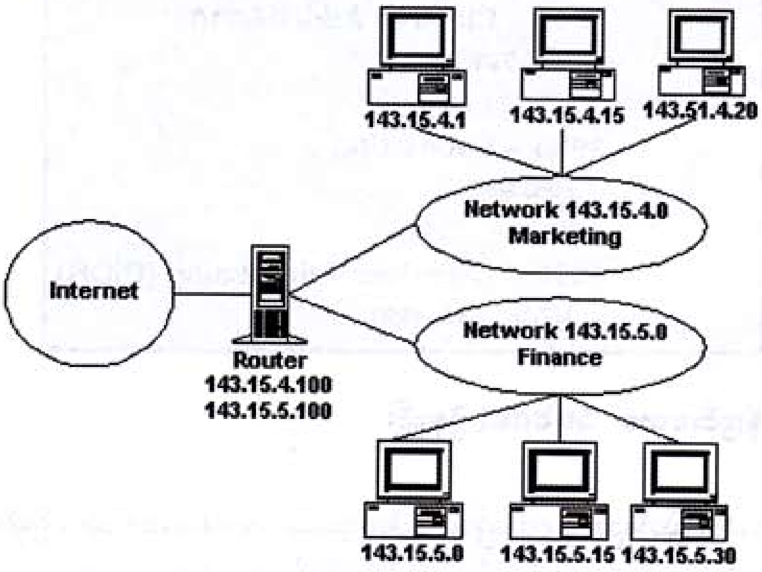
အကယ်၍သင်ဟာ IANA က Class B Address တစ်ခုကိုဝယ်လာတယ်ဆိုပါစို့။ အဲဒီ Address က 150.10.0.0 / 16 ပေါ့။ ၄င်းကို Dotted Decimal နှင့်ပြရင် 150.10.0.0, 255.255.0.0 ဖြစ်ပါတယ်။ ဒီတော့ ဒီ 150.10.0.0 မှာ Host ပေါင်း ဘယ်လောက်ရှိမလဲလို့ တွက်ကြည့်ရအောင် ပြန်ပြောမယ်နော်။ 150.10.0.0 ဆိုတဲ့ Address ကို ကျွန်တော်ဝယ်လာတယ်။ ပြီးတော့ ၄င်း 150.10.0.0 မှာချိတ်လို့ရနိုင်တဲ့ Host Address ကို တွက်ကြည့်တဲ့အခါ 2^{16} ရတယ်ဆိုတာကို တွေ့ရပါလိမ့်မယ်။ 2^{16} ဟာ 65536 ဖြစ်ပါတယ်။ Host ကိုတွက်တိုင်းမှာ ရှေ့ဆုံး Address နှင့် နောက်ဆုံး Address စတဲ့ Host နှစ်ခုကို ဖယ်ရတဲ့အတွက်ကြောင့် 65536 -2 ဆိုတော့ 65534 ရပါတယ်။ ခုပြောပြတာကို နားမလည်ရင် Chapter 1 ကိုပြန်ကြည့်ပေးပါ။ ၄င်းကို Chapter 1 မှာ ရှင်းပြထားပြီးသားပါ။ ဒီတော့ 150.10.0.0 ဆိုတဲ့ Address မှာ Host ပေါင်း 65534 ရပါတယ်။ ဆိုလိုတာက အဲဒီကွန်ရက်မှာ ကွန်ပျူတာတွေ Direct IP Printer တွေစသဖြင့် Host တွေ 65334 (၆ သောင်းကျော်) တောင်ရတယ်ဆိုတော့ ဒီနေရာတစ်နေရာတည်းမှာ ကွန်ပျူတာ ၆ သောင်းကျော် ရတယ်ဆိုတော့ စဉ်းစားကြည့်ရင် ဒီတစ်နေရာတည်းမှာ ကွန်ပျူတာ ၆ သောင်းကျော်ရှိဖို့ဆိုတာ မလွယ်ဘူးလေ။ ဒါကြောင့် ဒီ 150.10.0.0 ဆိုတဲ့ Network တစ်ခုကို တစ်နေရာတည်းမှာ ကွန်ပျူတာ ၆ သောင်းကျော်ရှိမယ့် အစား ၄င်းကွန်ရက်ကို အပိုင်းပိုင်း ပိုင်းလိုက်တာဖြစ်ပါတယ်။ ဒီတော့ 150.10.0.0 ဆိုတာ Host ပေါင်း ၆ သောင်းကျော်ရှိတဲ့ ကွန်ရက်ကြီးတစ်ခု (တစ်ခု) ကနေ ရာဂဏန်းလောက်သာရှိတဲ့ ကွန်ရက်အသေးစား လေးတွေ အများကြီး အဖြစ်ခွဲထုတ်လိုက်တာပါ။ ဒါကိုပဲ Subnet ခွဲတယ်ခေါ်ပါတယ်။ ကောင်းပါပြီ အခုဘာကြောင့် Subnet ခွဲရတာလည်းဆိုတာကို ရှင်းပြပြီးသွားပါပြီ။

ပုံ ၃.၁

ကွန်ရက်ကြီးတစ်ခု (တစ်ခု) ကနေ ရာဂဏန်းလောက်သာရှိတဲ့ ကွန်ရက်အသေးစား လေးတွေ အများကြီး အဖြစ်ခွဲထုတ်လိုက်တာပါ။ ဒါကိုပဲ Subnet ခွဲတယ်ခေါ်ပါတယ်။



အားလုံးသော Hosts တွေဟာ Network တစ်ခုထဲမှာပင်ချိတ်ဆက်ထားကြပုံ

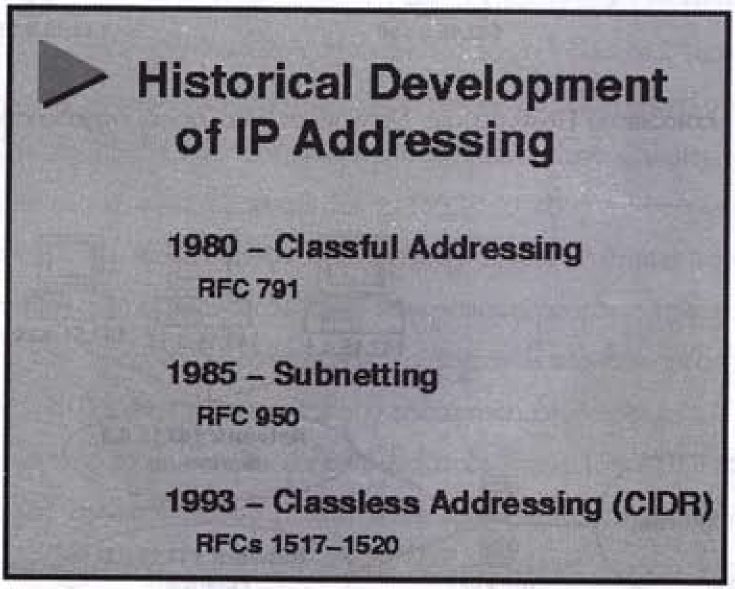


Marketing Dept. နှင့် Finance Dept. တို့ သီးခြား ကိုယ်ပိုင် Subnet များ ဖြစ်သွားပုံ

ဘာပဲဖြစ်ဖြစ် နောက်တစ်ခေါက်ပြန်ရှင်းပြမယ်။ ကွန်ရက်တစ်ခုတည်းမှာ Host တွေအများကြီးရှိတဲ့ ကြီးမားတဲ့ကွန်ရက်ကြီးကို ဘယ်သူမှအလိုမရှိကြဘူး။ ဒီကွန်ရက်ကြီးကို ကွန်ရက်ငယ်တွေအဖြစ် အပိုင်းပိုင်း ပိုင်းလိုက်ကြတယ်။ ဒီလိုကွန်ရက်ကို တစ်နိုင်တစ်ပိုင်ဖြစ်တဲ့ ကွန်ရက်ငယ်တွေပိုင်းလိုက်ခြင်းအားဖြင့် ထိန်းသိမ်းရလည်းလွယ်ကူလာသလို Preformance လည်းကောင်းလာမှာ ဖြစ်ပါတယ်။ ဒါကြောင့် Network တွေကို ဆင့်ပွား Network ဆိုပြီး Subnet ခွဲရခြင်းဖြစ်ပါတယ်။

အောက်ကပုံ ၃.၂ မှာ IP Addressing နှင့်ပတ်သက်လို့ ဘယ်နှစ်ခုနှစ်က ဘာဖြစ်ခဲ့သလဲဖော်ပြပေးထားပါတယ်။ ဒီပုံကိုကြည့်ခြင်းအားဖြင့် ၁၉၈၅ ကျမှ Subnetting ကိုစလုပ်တာကိုသိရပါမယ်။

ပုံ ၃.၂



၃.၂ ရိုးရှင်းသော Subnet ခွဲနည်း

Subnet ခွဲတဲ့နည်းကို စတင်၍ပြောပြပါတော့မယ်။ လောလောဆယ်တော့ ရိုးရှင်းတဲ့နည်းနဲ့ပဲ Subnet ခွဲပြပါ့မယ်။ Simple Subnetting ပေါ့ဗျာ။ ကျွန်တော်တို့ Class B Network တစ်ခုဖြစ်တဲ့

IP Address - 172.160.0.0

Subnet Mask - 255.255.0.0 ဆိုတဲ့ Address နှင့် ဥပမာပေးပြီး Subnet ခွဲပြပါ့မယ်။

172.160.0.0.255. မှာ Host ပေါင်း ဘယ်လောက်ရှိမလဲ၊ Host ပေါင်း ဘယ်လောက်ရှိမလဲ။။ Host ပေါင်း 2^{16} ဆိုတာ 65536 လေ။ ၎င်း 65536 ထဲမှာ ရှေ့ဆုံး Host နဲ့ နောက်ဆုံး Host ၂ လုံးကို

နှာ် ရင် ၆၅၅၃၄ ရပါတယ်။ ဟုတ်ပြီနော် Chapter 1 တုန်းက သင်ခဲ့တယ်။ မေ့သွားပြီလား။ 172.160.0.0, 255.255.0.0 ဆိုတာ 172.160.0.0/16 ဖြစ်ပါတယ်။ /16 ဆိုတာ ရှေ့က 16 bit က အသေပဲလို့ပြော တာလေ။ IPv4 Address မှာ 32 bits ရှိတာလေ။ ၎င်း 32 bits ထဲမှာ /16 ရှေ့က 16 bits က အသေပဲ လို့ပြောတာလေ။ ၎င်း 16 bits ကို နှုတ်လိုက်ပြီးနောက် 16 bits က Host Address ဖြစ်ပါတယ်။ ဒါကြောင့် 172.160.0.0 , 255.255.0.0 မှာ Host ပေါင်း 2^{16} = 65536-2 = 65534 လို့ပြောတာပါ။ ဒီကွန်ရက်ကြီးမှာ သွန်ပျတာတွေဝတဲ့ Host ပေါင်း 65534 ရှိ မှာကို မလိုလားဘူး။ ဒါကြောင့် Subnet ခွဲတယ်။ ဒါဆို Subnet Mask ကိုကြည့်ပါ။ Subnet Mask ကို အာရုံစိုက်ပါ။ Subnet Mask မှာ 255.255.0.0 ဆိုတာ ရှိပါတယ်။ အဲဒီ 255. 255.0.0 ဆိုတာက Class B Network တွေအတွက် အသေပဲဖြစ်ပါတယ်။

- ပထမ 255 က Network ကိုရည်ညွှန်းပြီး၊
- ဒုတိယ 255 ကလည်း Network ကိုပဲ ရည်ညွှန်းပါတယ်။
- တတိယ 0 ကတော့ Host ကိုရည်ညွှန်း ပါတယ်။
- စတုတ္ထ 0 ကလည်း Host ကို ရည်ညွှန်းပါတယ်။

အဲဒီထဲကမှ တတိယ 0 ကို 255 လုပ်လိုက်ရင် ၎င်းတာ Subnet Network ကို ရည်ညွှန်းသလိုဖြစ် သွားပါတယ်။

- ဆိုတော့ကား ယခင်တုန်းကတော့-

  IP Address: 172.160.0.0

  Subnet Mask: 255.255.0.0 ဖြစ်ပါတယ်။

- Subnet ခွဲလိုက်တော့ ယခုအခါ-

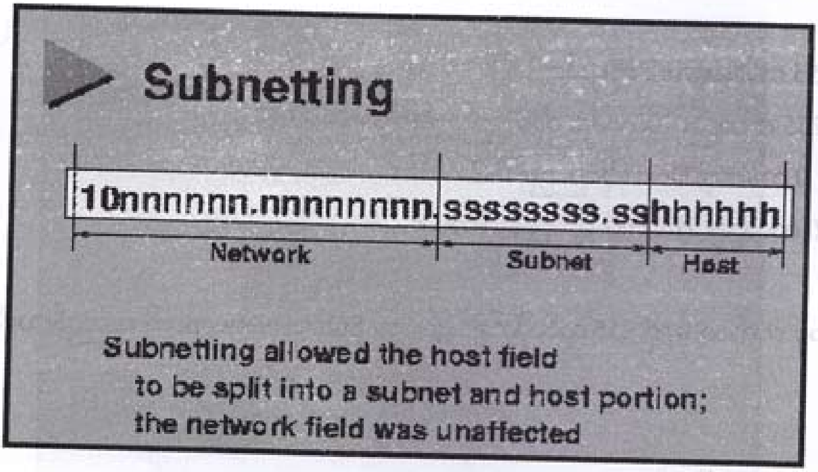
  IP Address: 172.160.0.0

  Subnet Mask: 255.255.255.0 ဆိုပြီး ဖြစ်သွားပါတယ်။

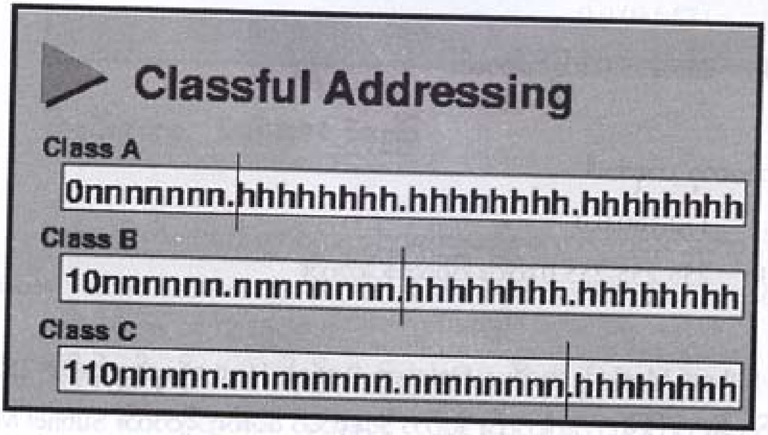
ပြန်ပြောရရင် Subnet Mask ရဲ့ တတိယ Octet က 0 ဆိုရင် Host ကိုရည်ညွှန်းပြီး၊ 255 ဆို တော့ Network ကိုရည်ညွှန်းသလိုဖြစ်သွားပါတယ်။ ဒီတော့ ဒီနေရာမှာ မေးစရာရှိတယ်။ Subnet Mask 255.255.255.0 ဆိုတော့၊ ဒါ Class B မဟုတ်ပဲ၊ Class C များဖြစ်နေမလားပေါ့။ Class C ရဲ့ Default Subnet Mask ကလည်း 255..255.255.0 ဖြစ်နေတာကိုး။ ဟုတ်ပြီ။ Subnet Mask 255.255.255.0

ဆိုတာနဲ့ Class C လို့ ပြောလို့မရပါဘူး။ တကယ်တမ်းမှာတော့ Address ရဲ့ ပထမဦးဆုံး Octet ကို ကြည့်မှသာ Class A, B, C သိနိုင်တာပါ။ အခု ဥပမာပေးရှင်းပြနေတဲ့ IP Address တာ 172.160.0.0 လေ။ အဲဒီမှာ First Octet က 172 ဆိုတော့ ဒါကိုကြည့်ခြင်းအားဖြင့် Class B လို့သိတာ လေ။ Class B တာ 128 –191 အတွင်းလေ။ ဒီတော့ Class B ဆိုရင် ၎င်းရဲ့ Default Subnet Mask က 255.255.0.0 ဖြစ်ရမယ်။ Class B ဖြစ်နေပါလျှက်နဲ့ ၎င်းရဲ့ Subnet Mask တာ 255.255.0.0 မ ဟုတ်ပဲ၊ တစ်ခြား တစ်ခုခုဖြစ်နေခြင်း၊ ဥပမာ 255.255.255.0 ဖြစ်နေရင် ဒီ Network မှာ Subnet ရှိနေပြီလို့ သိရမှာဖြစ်ပါတယ်။ အောက်မှာ ပုံ ၃.၃ Subnet ခွဲထားပုံနှင့် Subnet မခွဲခင် Classful Addressing ကိုယှဉ်ပြပေးထားပါတယ်။

ပုံ ၃.၃



ပုံ ၃.၄



ဒီနေရာမှာ n ဆိုတာ Network ကိုပြောတာပါ။ h ဆိုတာ Host ကိုပြောတာပါ။ s ဆိုတာ Subnet ကိုပြောတာပါ။ Classful တာ သူ့ရှိတဲ့အတိုင်းသုံးတာပါ။ Subnet ခွဲထားခြင်းမရှိပါ။

တဲ ဒီတစ်ခါ Subnet Mask ရဲ့ တတိယ Octet ဟာ 0 မဟုတ်ပဲ 255 ဖြစ်သွားတာကြောင့် သိရမယ့် အချက်တွေက -

၁။ Subnet Mask ရဲ့ ပထမ 255 နဲ့ ဒုတိယ 255 က IANA ကသတ်မှတ်ပြီးသား။ အသေပဲ။ Fixed ပေါ့။ /16 ဆိုတာ အဲဒါလေ။ ဒီတော့ /16 သည် ကိုယ်နဲ့ မဆိုင်ဘူး။ IANA ကို က သတ်မှတ်ပြီးသား။ ကိုယ်နဲ့ဆိုင်တာက နောက်က တတိယ Octet 0 နှင့် စတုတ္ထ Octet 0 တို့ပဲဖြစ်ပါတယ်။ ဒီတော့ တတိယ Octet 8 bits ရှိမယ်။ စတုတ္ထ Octet 8 bits ရှိမယ်။ ပေါင်း 16 bits ပေါ့။ ဒီတော့ 2^{16} ပေါ့။ 2^{16} က 65536-2 ဆိုတော့ 65534 Host ရတယ်။ ဒါရှင်းပြတာ အပ်ကြောင်းထပ်နေပြီ။

၂။ ဒီတော့ ကိုယ်နဲ့ဆိုင်တဲ့ Octet ကို 0 ကနေ 255 ထားလိုက်တော့။ ၎င်းဟာ Host Bit မဟုတ်ပဲ Network Bit ဖြစ်သွားတယ်။ Network Bit ဟာလည်း IANA က သတ်မှတ်ထားတဲ့ ရှေ့က /16 နဲ့ မဆိုင်ဘူး။ ကိုယ်နဲ့ဆိုင်တဲ့ 16 bits ထဲက 8 bits ကို Network ဘက်ပို့ပြီး၊ ကျန်တဲ့ 8 bits ကို Host မှာ ဒီအတိုင်းထားတာ။

၃။ ဒီတော့ 32 bits ရှိတဲ့ အထဲကနေ 16 bits သည် ကိုယ်နဲ့မဆိုင်။ နောက် 16 bits မှာ 8 bits သည် Network ပိုင်းဖြစ်ပြီး၊ နောက်ဆုံး 8 bits သည် Host ပိုင်းဖြစ်သွားသည်။ ဒါကြောင့် 172.160.0.0 , 255.255.0.0 ကို ဒီအတိုင်းသုံးရင် 65534 အရေအတွက်ရှိသော ကွန်ရက်တစ်ခုပဲရမယ်။ ကွန်ရက်တစ်ခု ပဲနော်။ အဲ့ဒီ ကွန်ရက်တစ်ခုမှာ Host 65534 ရမယ်။ အခုဟာက 172.160.0.0 မှာ Subnet Mask ကို 255.255.255.0 လုပ်လိုက်တော့ ကွန်ရက်ပေါင်း 2^8 ဖြစ်သွားပြီ။ Host ကလည်း 2^8 ဖြစ်သွားပါတယ်။ အဲ့ဒီ 2^8 က 2 ကို 8 ခါမြှောက်တော့ 256 ဖြစ်တာကြောင့် ၎င်းကွန်ရက်ဟာ ကွန်ရက်တစ်ခုတည်း မဟုတ်တော့ပဲ၊ ၎င်းမှာ ကွန်ရက်ပေါင်း 256 ခုတောင် ဖြစ်သွားပါတယ်။ ၎င်း ကွန်ရက်ပေါင်း 256 ခုမှာမှ ကွန်ရက်တစ်ခုချင်းစီမှာ ကွန်ပျူတာ Host ပေါင်း ဘယ်လောက်ရှိမလဲဆိုတော့ ကျန်တော်တို့မှာ 8 bits နောက်ဆုံး 8 bits ကျန်သေးတယ်လေ။ အဲ့ဒီ 2^8 ကိုတွက်လိုက်ရင် 256 ရတယ်။ ရှေ့ဆုံး Host နဲ့ နောက်ဆုံး Host ကို ဖယ်လိုက်ရင် 254 ကျန်မယ်။ ဒီတော့ ကွန်ရက်တစ်ခုမှာ Host ပေါင်း 254 ခုရပါမယ်။ အဲဒီလို 254 Host ရှိတဲ့ ကွန်ရက်ပေါင်း 256 ခုရှိပါမယ်။

ဒီတော့ကား အရင်တုန်းက ကွန်ရက်တစ်ခုပဲရှိတယ်။ အဲဒီမှာ Host 65536 ရှိတယ်။ အခု ကွန်ရက် 256 ခုရှိတယ်။ ကွန်ရက်တစ်ခုချင်းစီမှာ Host ပေါင်း 254 ရှိတယ်ဆိုတော့ ဒါက Host(၂) ခုကို နုတ်ရလို့လေ။ Host (၂) ခုကိုသာ မနုတ်ရင် 256 ခုရှိမှာပေါ့။ ဒီတော့ ကွန်ရက်တစ်ခုမှာ Host ပေါင်း 256 ခုရှိနေမယ်။ ဒီလို ကွန်ရက်ပေါင်း 256 ခုရှိနေမယ်။ ကောင်းပြီ ဒီ 256 ကို 256 နဲ့မြှောက်ကြည့်။ 65536 ပြန်ထွက်လာ

လိမ့်မယ်ဆိုတော့အတူတူပါပဲ။ 65536 Host ရှိတဲ့ ကွန်ရက်ကြီးတစ်ခုကိုယူမှာလား။ Host 254 ပဲရှိတဲ့ ကွန်ရက် 256 ခုကိုယူမလား။ ဒါပဲ .... ပြောချင်တာ ဒါပဲ။ ဒီတော့ တစ်နေရာတည်းမှာ Host ပေါင်း 6 သောင်းကျော်ရှိတဲ့ ကွန်ရက်ကြီးတစ်ခုကိုတော့မယူပါဘူး။ ကွန်ရက်တစ်ခုမှာ 254 Host ပဲရှိတဲ့ ကွန်ရက်ငယ် 256 ခုကိုပဲယူခြင်းကို Subnet ခွဲတယ်လို့ခေါ်တာ၊ ပြောတာဖြစ်ပါတယ်။

ပုံ ၃.၅

65536 Host ရှိတဲ့ ကွန်ရက်ကြီးတစ်ခုကိုယူမှာလား။
Host 254 ပဲရှိတဲ့ ကွန်ရက် 256 ခုကိုယူမလား။ ဒါပဲ ....
ပြောချင်တာ ဒါပဲ။

နောက်တစ်မျိုး ပြန်ရှင်းပြဦးမယ် . . .

ဥပမာ . . . . ပေးတဲ့ Address က –

IP Address:	172.160.0.0
Subnet Mask:	255.255.0.0.

ဒါ Before Subnetting. Subnet မခွဲခင်အချိန်ပေါ့။

ဒီတော့ ဒီနေရာမှာ Subnet ကိုပဲ အာရုံစိုက်ရအောင်။ Subnet Address ရဲ့ 255 ကို Binary ပြောင်းရင် 1 တွေရတယ်။ 0 ကို Binary ပြောင်းရင် 0 တွေရပါတယ်။ 1 ဆိုရင် Network (အတိုကောက် N လို့ရေးမယ်) ကို ညွှန်းတာဖြစ်ပြီး၊ 0 ဆိုရင် (အတိုကောက် h) Host ကို ရည်ညွှန်းတာဖြစ်ပါတယ်။

ဒီတော့–

IP Address: nnnnnnnn.nnnnnnnn.hhhhhhhh.hhhhhhhh. ဆိုလိုတာက Address မှာ 32 bits ရှိတယ်။ Subnet Mask ရဲ့ ပထမ Octet 255 ကို Binary ပြောင်းတော့ 1–၈ လုံး (11111111) ရတယ်။ ၎င်း 11111111 ရဲ့အပေါ်က Address ဟာ Network ကိုရည်ညွှန်းတာဖြစ်ပြီး 0000 0000 ရဲ့အပေါ်က IP Address က Host ကို ရည်ညွှန်းတာဖြစ်ပါတယ်။ ဒီတော့ အခုရှင်းပြနေတဲ့ 172.160.0.0 ဟာ Class B ဖြစ်တာကြောင့် Network ပိုင်းအတွက် 16 bits ရရှိပြီ။ Host ပိုင်းက 16 bits ရရှိပါတယ်။ အဲဒီ Network 16 bits ကို ဘာမှသွားလုပ်ဖို့ မစဉ်းစားနဲ့။ အဲဒါက IANA က သတ်မှတ်ပေးထားတာ။ တစ်ကမ္ဘာလုံးနဲ့ သက်ဆိုင်တာဆိုတော့ သင် ဘာမှလုပ်လို့မရဘူး။ သင်လုပ် လို့ရတာက သင်ပိုင်တဲ့ Host 16 bits ဖြစ်ပါတယ်။ အဲဒီ 16 bits ထဲက ပထမ 8 bits ကို Network ဘက်ကိုပို့လိုက်။ ဘာလို့ ပို့ရမလဲ။ 00000000 ကို 11111111

အဖြစ် Setting လုပ်လိုက်။ Decimal နဲ့ပြောရရင် 255 လို့ထားလိုက်။ ဒီတော့ Host 16 bits ရှိတဲ့ အထဲက၊ တစ်နည်းအားဖြင့် "0" –၁၆ လုံးရှိတဲ့အထဲက ပထမ သုည ၈–လုံးကို၊ တစ် ၈–လုံးထားလိုက်။ ဒီတော့ Host 16 bits မှာ 8 bits က Network Address ကို 8 bits ရောက်သွားပြီ။ Host မှာ 8 bits ပဲ ကျန်တော့ပါတယ်။ ဒါကြောင့် Subnet က 2^8 ရပြီ၊ Host ကလည်း 2^8 ရသွားတာ ဖြစ်ပါတယ်။ ဒီတော့ ဒါကို အပေါ်က ပုံစံအတိုင်းရှင်းပြရရင် . . .

-IP Address: nnnnnnnn , nnnnnnnn , nnnnnnnn , hhhhhhhh
-Subnet Mask: 11111111. 11111111 . 11111111. 00000000 ဆိုပြီးဖြစ်သွားပါတယ်။
ဒီ Subnet ခွဲပြီးသွားတဲ့အချိန်မှာ ဖြစ်သွားတဲ့ ပုံစံပါ။ ၂ ခု ပြန်ယှဉ်ပြမယ်။

- Before Subnetting (Original) ပုံစံက–

IP Address: nnnnnnnn . nnnnnnnn . hhhhhhhh. hhhhhhhh
Subnet Mask: 11111111 . 11111111 . 00000000 . 00000000

- After Subnetting (Subnet ခွဲပြီးတဲ့ ပုံစံက)–

IP Address: nnnnnnnn . nnnnnnnn . nnnnnnnn . hhhhhhhh .
Subnet Mask: 11111111. 11111111 .11111111 . 00000000

ဆိုလိုတာက IP Address ရဲ့ Third Octet ဟာ Host ရဲ့ အပိုင်းကနေ Network အပိုင်း ဖြစ်သွားတာပါ။

၃.၃ စိတ်ကြိုက် Subnet ခွဲခြင်း

Simple Subnetting ကိုရှင်းပြပြီးသွားတဲ့အခါ ဒီတစ်ခါ စိတ်ကြိုက် Subnet ခွဲနိုင်တဲ့ Advance Subnetting ဆိုတာကို ရှင်းပြပါဦးမယ်။ ဒီသင်ခန်းစာတွေဟာ ခက်သလားဆိုတော့ မခက်ဘူးဗျ။ ဒါပေမဲ့ နည်းနည်းလေး သင်္ချာပါလာတော့ လူတွေက ရုတ်တရက် နားမလည်ဘူး ဖြစ်သွားနိုင်ပါတယ်။ ဒါကြောင့် သင်တာ သင်္ချာမရရင် ခဏလေး အပြင်ထွက်၊ လမ်းလျှောက်၊ အေးစက်နေတဲ့ အအေးတစ် ခွက်လောက် သောက်လိုက်ပါဦး၊ ပြီးမှပြန်ဖတ်ရအောင်။

ဒီလိုဗျ Simple Subnetting ဆိုတဲ့ ရိုးရှင်းတဲ့ Subnet ခွဲခြင်းဟာ တစ်ကယ့်လက်တွေ့မှာ လုပ်ငန်းလိုအပ်ချက်အပေါ် တိကျစွာ Subnet မခွဲနိုင်ဘူးဗျ။ ဒီတော့ ခုနတုန်းက ရှင်းပြခဲ့တဲ့ Simple Subnetting ကိုပဲ ခဏပြန်ပြောရအောင်။ ဥပမာပေးပြီးရှင်းပြခဲ့တဲ့ Address က 172.160.0.0, 255.255.0.0 ဖြစ်ပါတယ်။ အပေါ်ကအတိုင်းပါပဲ။ ဆိုတော့ ဒီ Address ကိုကြည့်လိုက်ရင် 32 bits ရှိတဲ့ အထဲကနေပြီးတော့ 16 bits အသေဖြစ်ပြီးနောက် 16 bits က 0 ကိုပြောင်းလဲပေးနိုင်တဲ့ Host ဖြစ်ပါတယ်။ အဲဒီ Host 16 bits ထဲမှ 8 bits ကို Network ပိုင်းထားပြီး၊ ကျန်တဲ့ 8 bits ကို Host ထားတော့ Host ပေါင်း (256-2=254) ရှိတဲ့ ကွန်ရက်ပေါင်း 256 ခုဖြစ်လာတယ်လေ။ အရှေ့မှာ ရှင်းပြပြီးသား။ ဒီနေရာမှာ အထွန့်တက်စရာ တစ်ခုရှိတယ်။

အဲဒါက ဘာလဲဆိုတော့ အဲဒီ Address ကိုဝယ်ထားတဲ့ သူဟာ Subnet ခွဲလိုက်တဲ့အခါ Subnet ပေါင်း 256 ခု အလိုမရှိသလို၊ Subnet တစ်ခုမှာ ရှိတဲ့ Host ကလဲ 254 ခုမက ရှိချင်တယ်။ အဲဆို ဘယ်လိုလုပ်ကြမလဲ။ ကျွန်တော် ပြောချင်တာအဲဒါပဲ။ အဲကြောင့် Simple Subnetting ဆိုတာ တစ်ကယ့်လက်တွေ့မှာ အသုံးတည့်ဖို့သိပ်မလွယ်ဘူး။ သင်တို့နားလည်အောင်လို့သာ အရင် ရှင်းပြတာဖြစ်တယ်။ နောက်တစ်ခေါက် ထပ်ပြောပြမယ်။ 172.160.0.0, 255.255.0.0 ဆိုတဲ့ Address ကို Subnet သာမခွဲခဲ့ဘူးဆိုရင် Host ပေါင်း 65534 ရှိမယ့် ကွန်ရက်ကြီးတစ်ခုကိုရမယ်။ အဲကို မလိုချင်ဘူး။ ကွန်ရက်ကြီးကကြီးနေလို့ မလိုချင်တာ။ ဒီတော့ 172.160.0.0, 255.255.255.0 ဆိုပြီး Subnet ခွဲလိုက်တဲ့အခါ ကွန်ရက်တစ်ခုမှာ၊ တစ်နည်းအားဖြင့် Subnet တစ်ခုမှာ Host ပေါင်း 254 ရှိတဲ့ Subnet 256 ခုကိုရမယ်။ အဲဒါကိုလည်း မကျေနပ်ပြန်ဘူး။ ပထမတော့ ကွန်ရက်ကြီးကကြီးလို့၊ Subnet ခွဲလိုက်ပြန်တော့လည်း ကွန်ရက်ကသေးသွားပြန်ရော။ ကိုယ့်လိုအပ်ချက်နဲ့ မကိုက်ညီဘူးဖြစ်နေတယ်။ အဲဒီလို ကိုယ့်အဖွဲ့အစည်းရဲ့ လိုအပ်ချက်နဲ့ ကိုက်ညီတဲ့ Subnet ခွဲချင်ရင် အခု ကျွန်တော်ရှင်းပြမယ့် Advance Subnetting ကိုအသုံးပြုရမှာ ဖြစ်ပါတယ်။

ပုံ ၃.၆

Subnet ပေါင်း 256 ခု အလိုမရှိသလို၊ Subnet တစ်ခုမှာ ရှိတဲ့ Host ကလဲ 254 ခုမက ရှိချင်တယ်။ အဲကြောင့် Simple Subnetting ဆိုတာ တစ်ကယ့်လက်တွေ့မှာ အသုံးတည့်ဖို့သိပ်မလွယ်ဘူး။ အဲဒီလို ကိုယ့်အဖွဲ့အစည်းရဲ့ လိုအပ်ချက်နဲ့ ကိုက်ညီတဲ့ Subnet ခွဲချင်ရင် အခု သားသား ရှင်းပြမယ့် Advance Subnetting ကိုအသုံးပြုရမှာ ဖြစ်ပါတယ်။

ယခုအချိန်ကစပြီး Advance Subnetting ကို စတင်ရှင်းပြပါတော့မယ်။ ဥပမာပေးပြီး ရှင်းပြမယ့် Address ကတော့ –

Original IP Address: 172.160.0.0
Subnetting Mask : 255.255.0.0

ဒါက Subnet မခွဲခင် မြင်ရမယ့် မူလ Address ဖြစ်ပါတယ်။ ကောင်းပြီ။ အဲဒီ Address ရဲ့ Subnet Mask မှာ ပထမ 255 ကို Binary ပြောင်းလိုက်ရင် 11111111 ရပါတယ်။ ဘာလို့ 11111111 ရတယ်ဆိုတော့ 8 bits ကို ဒုတိယ 255 ကိုလည်း Binary ပြောင်းလိုက်ရင်၊ ထိုနည်းလည်းကောင်း 11111111 ရပါတယ်။ ဒီတော့ အားလုံးပေါင်းလိုက်ရင် တစ်ဆယ့်ခြောက်လုံးရပါတယ်။ ဒီ 16 bits က အသေပဲဖြစ်ပါတယ်။ ဒီ Address ရဲ့ Subnet Mask မှာရှိနေတဲ့ တတိယ Octet က သုည နဲ့ စတုတ္ထ Octet က သုညကို Binary ပြောင်းလိုက်ရင် သုည–ဆယ့်ခြောက်လုံးရပါတယ်။ ဒီတော့ Simple Subnetting မှာ ကျွန်တော်ရှင်းပြခဲ့တာက အဲဒီ သုည–ဆယ့်ခြောက်လုံးထဲက ပထမ သုည–ရှစ်လုံးကို Network ဘက်ကို ပို့လိုက်ပြီး ကျန်သုည–ရှစ်လုံးကို Host မှာထားလိုက်ရင် Network က 8 bits Host က 8 bits ဖြစ်သွားလိမ့်မယ်။ ဒါကိုအောက်မှာ နောက်တစ်နည်းနဲ့ ပြန်ရှင်းပြမယ်။

IP Address : nnnnnnnn . nnnnnnnn . nnnnnnnn . hhhhhhhh .
Subnet Mask: 11111111 . 11111111 . 11111111 . 00000000

Subnetting Mask : 255.255.255.0

ဆိုပြီးဖြစ်သွားမယ်။

ဒီတော့ ပြောချင်တာက တတိယ Octet ရဲ့ သုည–ရှစ်လုံးကို တစ်–ရှစ်လုံးအဖြစ်ပြောင်းပြီး Network ပိုင်းကို ပို့လိုက်မယ့်အစား သုည–သုံးလုံးကိုပဲ Network ပိုင်းကို ပို့လိုက်ရင် မရဘူးလား။ အဲဒီမေးခွန်းရှိတယ်။ ဆိုလိုတာက Host ပိုင်းမှာ ရှိနေတဲ့ သုည–ဆယ့်ခြောက်လုံး၊ တစ်နည်းအားဖြင့် 16 bits ထဲက 8 bits ကို Network ပိုင်းမှာထားပြီး၊ ကျန် 8 bits ကို Host အတွက်ထားမယ့်အစား၊ 16 bits ထဲက 8 bits ကိုပဲ Network ဘက်ကိုပို့လိုက်မယ်ဆိုရင်၊ ရှိတဲ့ 16 ထဲက 3 ကိုနှုတ်တော့၊ Host အတွက် 13 ကျန်ပါတယ်။ ရှုပ်သွားသလား။ ဒီလိုလေဗျာ။ Third Octet မှာရှိတဲ့ 8 bits ထဲက 3 bits ကို Network ဘက်ကို ပို့လိုက်တော့၊

အဲဒီမှာ 5 bits ကျန်တယ်။ အဲဒီ 5 bits နဲ့ Fourth Octet က 8 bits ပေါင်းတော့ 13 bits ပေါ့။ ဒီတော့ အားလုံး 32 bits ရှိတယ်။ အဲဒီ 32 bits ထဲက First Octet 8 bits နဲ့ Second Octet 8 bits နှစ်ခုပေါင်း 16 bits ကို ကျွန်တော်တို့က သွားထိလို့ မရသေးဘူး။ Third Octet 8 bits နဲ့ Fourth Octet 8 bits နှစ်ခုပေါင်း 16 bits ရှိတဲ့အထဲက 3 bits ကို Subnet ဘက်ပို့လိုက်တော့ 16-3 နုတ်ပြီး Host မှာ 13 bits ကျန်တယ်လို့ပြောတာဖြစ်ပါတယ်။

ပုံ ၃.၇

> တတိယ Octet ရဲ့ သုည–ရှစ်လုံးကို တစ်–ရှစ်လုံး အဖြစ်ပြောင်းပြီး၊ Network ပိုင်းကို ပို့လိုက်မယ့်အစား သုည–သုံးလုံးကိုပဲ Network ပိုင်းကို ပို့လိုက်ရင် မရဘူးလား။ ဒါဟာ Advance Subnetting ပဲဖြစ်ပါတယ်။

ကောင်းပြီ။ အဲဒီတော့ Network ကို 3 bits ပို့တော့ 2^3 ပေါ့။ 2^3 ဆိုတာ 2 ကို 3 ခါမြှောက်တာပဲ။ 2 ကို 3 ခါမြှောက်တော့ 8 ရတာပေါ့။ သိလား။ 2 x 2 x 2 လေ။ ဒီတော့ ကျွန်တော်တို့ဟာ Subnet ခွဲပြီးတဲ့အခါ Subnet ရှစ်ခုကိုရရှိပါတယ်။

အရင်တုန်းက Host ရဲ့ 16 bits မှာ 8 bits ကို Network ဘက်ပို့တော့ 2^8 ဖြစ်ပြီး၊ Network ပေါင်း 256 ခုရတယ်လေ။ အခု Host 16 bits ကနေပြီး၊ Network ဘက်ကို 3 bits ပဲပို့တော့၊ 2^8 ဆိုပြီး Subnet ရှစ်–ခုရတာပါပဲ။ ဒါဟာ Advance Subnetting ပါပဲ။ အရင်တုန်းက Host ရဲ့ 16 bits ထဲက Network နှင့်၊ Host ကို တစ်ဝက်စီပိုင်းပါတယ်။ Network ကို 8 bits၊ Host ကို 8 bits ပေါ့။ အခုတော့ အဲလိုမဟုတ်တော့ဘူး။ Host 16 bits ရှိတဲ့ အထဲက Network ကို 8 bits မပေးပဲ၊ 3 bits ပဲပေးတော့၊ Host မှာ 13 bits ကျန်ပြီး၊ Subnet တစ်ခုမှာ Host ပေါင်း 8190 စီရှိတဲ့ Subnet ပေါင်း ရှစ်–ခု ဖြစ်ပေါ်လာတာဘဲ။

❖ Before Subnetting- Subnet မခွဲခင် Original မူလ Address -

IP Adress:	nnnnnnnn . nnnnnnnn . hhhhhhhh . hhhhhhhh
Subnet mask:	11111111 . 11111111 . 00000000 . 00000000

- After Subnetting - Subnet ခွဲပြီးမြင်တွေ့ရသော Address ပုံစံ – မျဉ်းတားပြထားတယ်။

  IP Address: nnnnnnnn . nnnnnnnn . **nnn**hhhhh. hhhhhhhh

  Subnet Mask: 11111111 . 11111111 . **111**00000 . 00000000 ဆိုပြီးဖြစ်သွားမယ်။

အဲသလို 172.160.0.0, 255.255.0.0 ကို 8190 Host ရှိတဲ့ ကွန်ရက်ပေါင်း ၈–ခုအဖြစ် Subnet ခွဲလိုက်တဲ့အခါ ၎င်း Address တာဘယ်လိုပုံဖြစ်သွားမလဲဆိုတော့–

IP Address က 172.160. 0.0 ပဲ

Subnet Mask ကျတော့ 255.255.224.0 ဆိုပြီးဖြစ်သွားပါတယ်။

ဒီနေရာမှာသိရမှာက Subnet Mask နဲ့ Third Octet ဟာ အရင်လို 255 မဟုတ်ဘဲ ဘာဖြစ်လို့ 244 ဖြစ်ရသလဲဆိုတော့ 11100000 ကို Binary ကနေ Decimal ပြောင်းလိုက်လို့ပဲ။ 11100000 ကို Binary ကနေ Decimal ပြောင်းရင် 224 ရတယ်လေ။ ပြောင်းတဲ့နည်း မေ့သွားရင် ပြန်ရှင်းပြပေးမယ်။ အောက်က ဇယားကွက်ကို ကြည့်ပါ။

128	64	32	16	8	4	2	1
1	1	1	0	0	0	0	0

ကဲ ... ဒီဇယားကွက်မှာ 11100000 ကို သူ့နေရာနှင့်သူထည့်လိုက်ပါတယ်။ အဲဒီမှာ 1 ရှိတဲ့ တာနေကိုပေါင်းပါ။ ဒီတော့ 128+64+32 ဆိုပြီးရှိမယ်။ ဒါတွေကို ပေါင်းလိုက်တော့ 224 ဆိုပြီး ထွက်လာမှာ ဖြစ်ပါတယ်။ 255 ဆိုရင် စဉ်းစားကြည့်။ ဆိုလိုတာက 255 ကို Binary ပြောင်းလိုက်ရင် တစ်–၈ လုံး 11111111 ရတယ်လေ။ ဒီတော့ 255 ဆိုတာ ရှိသမျှ 8 bits စလုံး Network ဘက်ကို ပို့လိုက်တာဖြစ်လို့ Network Address အရေအတွက်ဟာ $2^8=256$ ဖြစ်သွားတာပါ။ ဒီတော့ ကွန်ရက်ပေါင်း 256 ခွဲထုတ်လိုက်သလို ဖြစ်သွားတာပါ။ အခုကျတော့ 255 အစား 224 ဆိုတော့ 224 ကို Binary ပြောင်းလိုက်ရင် 11100000 ရတယ်လေ။ အဲဒီမှာ 1 ဆိုတာ Network ပိုင်း၊ 0 က Host ပိုင်းဆိုတော့ Network ကို 3 bits ပဲ ပို့လိုက်တာပေါ့။

နောက်တစ်ခု တွက်ပြမယ်။ 8 bits ရှိတဲ့အထဲက Network ဘက်ကို 1 bit ပဲပို့လိုက်ရင်၊ Host မှာ 7 bits ကျန်မယ်။ ကျန်တဲ့ 7 bits နှင့် Fourth Octet က 8 bits ပေါင်းတော့၊ Host အတွက် က 15 bits ရတယ်။ ဒီတော့ ဇယားကိုကြည့်။

128	64	32	16	8	4	2	1
1	0	0	0	0	0	0	0

ဒီဇယားတွက်အတိုင်းသာ Subnet ခွဲလိုက်ရင် Address က ဘယ်လိုဖြစ်သွားမလဲ။

IP Address: 172. 160. 0. 0

Subnet Mask: 255.255.128.0 ဆိုပြီးဖြစ်သွားမယ်။

ဒီတော့ ဒီ Address မှာ Subnet ဘယ်နှစ်ခုရှိမလဲ။ Network ဘက်ကို 1 bit ပဲပို့ထားတော့ 2^1 ပေါ့။ 2^1 ဆိုတာ 2 ပဲလေ။ ဒီတော့ ဒီ Network မှာ Subnet 2 ခု ရှိပါတယ်။ အဲဒီ Host ရော ဘယ်လောက်ရှိမလဲ။ Host ကတော့ 15 bits ရှိမယ်လေ။ ဒီတော့ 2^{15} ပေါ့။ 2^{15} က 32768 ရပါတယ်။ အမြဲတမ်းမှတ်ထားရမှာက အရှေ့ဆုံး Host နဲ့ နောက်ဆုံး Host ကိုနုတ်ရမယ်။ ဒီတော့ 32768-2 ဆိုတော့ကား 32766 ရပါတယ်။ ဆိုလိုတာက Host ပေါင်း 32766 ရှိမယ့် Subnet ပေါင်း 2 ခုရမှာဖြစ်ပါတယ်။

ပုံ ၃.၈

> ဒီတော့ ဒီနေရာမှာမေးစရာတစ်ခုရှိတယ်။ Subnet Mask မှာဖြစ်မယ့် ဂဏန်းတွေက တရားသေ မှတ်လို့ရတာပေါ့။ ဒီဂဏန်းတွေက 128,192,224,240,248,252,254 နှင့် 255 တို့ပဲဖြစ်မှာပေါ့။

ရှုပ်သွားလား။ နားလည်တဲ့သူလည်းရှိမယ်။ တိုင်ပတ်တဲ့သူလည်းရှိမယ်။ ဒီတော့ ဂဃနဏ ရှင်းပြပေးမယ်။ ဇယားတွက်ကိုကြည့်ပါ။

128	64	32	16	8	4	2	1	
1	0	0	0	0	0	0	0	= 128

128	64	32	16	8	4	2	1	
1	1	0	0	0	0	0	0	=192

192 ဘာလို့ရလဲ။ 1 ရှိတဲ့ ဂဏန်းပေါင်းတာကို 128+69 ဆိုတော့ 192 ရတယ်။ ဒီတော့ –

IP Address: 172 .160 .0 .0

Subnet Mask: 255 .255. 192. 0 ဖြစ်ပါတယ်။ ၎င်း Address မှာ Network ဖက်ကို 2 bits ဆိုတော့၊ Network က 2^2 ဖြစ်ပါတယ်။ ဒီတော့ Subnet 4 ခုရပါတယ်။ Subnet တစ်ခုမှာ ရှိမယ့် Host အရေအတွက်ကတော့ 214 ဖြစ်ပါတယ်။ 16 bits ထဲက 2 bits နုတ်တာကို။ 2^{14}= 16384 ရပါတယ်။ 16384 ထဲက ရှေ့ဆုံး Host နဲ့ နောက်ဆုံး Host ကိုနုတ်တော့ 16382 ရပါတယ်။ 16382 Host ရှိတဲ့ Subnet လေးခုကို ရရှိမှာဖြစ်ပါတယ်။ နောက်တစ်ခုကို ကြည့်ပါဦး။

128	64	32	16	8	4	2	1	
1	1	1	0	0	0	0	0	=224

ဒါရှင်းပြပြီးသားနော်။ နောက်တစ်ခုကို ကြည့်ပါဦး။

128	64	32	16	8	4	2	1
1	1	1	1	0	0	0	0

= 240

သိတယ်နော်။ 1 ရှိတဲ့ ဂဏန်းအားလုံးပေါင်းတော့ 128 + 64 + 32 + 16 ဆိုတော့ 240 ရ တယ်။ ကိုယ့်ဘာသာကိုယ် တွက်ကြည့်ပါလား။ Network ကို ဘယ်နှစ် Bit ပို့လိုက်လဲ။ 4 bits ပို့လိုက်တာပါ။ 4 bits ဆိုတော့ 2^4 ပေါ့။ Subnet 16 ခုရမယ်။ Host ကတော့ 12 bits ရမယ်။ ဒီတော့ 2^{12} ပေါ့။ 2^{12} က 4096 ဖြစ်ပါတယ်။ ဒီတော့ Host ပေါင်း 4094 ရှိတဲ့ ကွန်ရက်ပေါင်း 16 ခုထွက်လာတာ ပါပဲ။ Host ကဘာလို့ 12 bits ရတယ်ဆိုတာသိလား။ 16 ထဲက 4 ကို နှုတ်တော့ 12 bits ရတာပေါ့။ အောက်ကပုံကို ကြည့်ရင် ပိုရှင်းလိမ့်မယ်။

IP Address: nnnnnnnn . nnnnnnnn . nnnnhhhh . hhhhhhhh

Subnet Mask: 11111111 . 11111111 . 11110000 . 00000000

ဒီတော့ အဲဒီမှာ မျဉ်းတားပြထားတယ်။ 0 တွေ ဘယ်နှစ်လုံးရှိလဲ။ 12 လုံး။ ဒါကြောင့် Host က 12 bits ရတာဖြစ်တယ်။ နောက်တစ်ခုကိုကြည့်ပါဦး။

128	64	32	16	8	4	2	1
1	1	1	1	1	0	0	0

= 248

1 ရှိ ဂဏန်းအားလုံးပေါင်းတော့ 128 + 64 + 32 + 16 + 8 ဆိုတော့ 248 ရပါတယ်။ အဲဒီမှာ Network က 5 bits ရပါတယ်။ Host က 11 bits ရပါတယ်။ Network က 2^5 ပေါ့။ ဒီတော့ Subnet ပေါင်း 32 ခုရပါတယ်။ ဒီ Subnet တစ်ခုစီမှာ Host က 2^{11} ဆိုတော့ 2048 ရပါတယ်။ အဲ့ Host 2 ခုနှုတ်တော့ 2046 ရပါတယ်။ ဒီတော့ Host ပေါင်း 2046 ရှိတဲ့ Subnet ပေါင်း 32 ခုရပါတယ်။ Address က ဘယ်လို ဖြစ်သွားမလဲ။

IP Address: 172.160.0.0

Subnet Mask: 255.255.248.0 ဖြစ်သွားပါတယ်။ နောက်တစ်ခုက–

128	64	32	16	8	4	2	1
1	1	1	1	1	1	0	0

=252

ကိုယ့်ဘာသာကိုယ် တွက်ကြည့်တော့နော်။ Network 2^6 . Host 2^{10} .

128	64	32	16	8	4	2	1
1	1	1	1	1	1	1	0

=254

ဒီတော့ Network က 2^7၊ Host က 2^9 ဖြစ်ပါတယ်။ ဒါကြောင့် သိရမှာက Subnet Mask မှာ ဖြစ်ပေါ်လာမယ့် ဂဏန်းတူတွေဟာ 128,192,229,248,252,254 နဲ့ 255 တို့ဖြစ်ပါတယ်။

အခုရှင်းပြတာက Class B Network ကို Subnet ခွဲပြတာပါ။ Class A Network နဲ့ Class C Network ကို Subnet ခွဲရင်လည်း ဒီအတိုင်းပဲဖြစ်ပါတယ်။ Class A ဆိုရင် Default Mask က 255.0.0.0 မဟုတ်လား။ အဲဒီမှာ ဒုတိယ Octet ရဲ့ 0 ကို စတင်ကစားရမှာဖြစ်သလို၊ Class C ရဲ့ Default Subnet Mask က 255.255.255.0 မဟုတ်လား။ ၎င်းရဲ့ စတုတ္ထ Octet 0 ကို ကစားရမှာ ဖြစ်ပါတယ်။

၃.၄ Subnet ခွဲပြီး Octet များကိုတွက်ခြင်း

ကဲ ခုနကတုန်းက ဘာကြောင့် Subnet ခွဲရတယ်။ Subnet ကို ဘယ်လိုခွဲရတယ်၊ ခွဲပြီးသွားတဲ့အခါမှာ ခွဲထားတဲ့ Subnet တွေမှာ Subnet ဘယ်လောက်ရလာလို့ Subnet တစ်ခုချင်းစီမှာရော Host ကဘယ်လောက်ရလာသလဲဆိုတာကို တွက်ပြခဲ့တယ်။ အခု Subnet ခွဲပြီးတဲ့အခါမှာ ဖြစ်ပေါ်လာတဲ့ Subnet တွေကို Decimal Octet နှင့်ဖော်ပြပါ့မယ်။ ဒီအတွက် နည်းနည်းတွက်ရဦးမှာဖြစ်ပါတယ်။ ဖတ်တဲ့သူတွေ

ဘယ်လိုနေမလဲမသိဘူး။ ရေးပြ၊ ရှင်းပြနေတဲ့ ကျွန်တော်မျိုးကြီးကိုယ်တိုင်ကတော့ သိပြီးသားအကြောင်းအရာ ချရေးနေတာတောင် အခု အေးစက်တောင့်တင်းနေတဲ့ အအေးတစ်ခွက်ကို ဂွပ်ကနဲ မော့ချလိုက်ပါတယ်။

Subnet ရဲ့ Octet ကို တွက်တဲ့နေရာမှာ Binary နှင့်လည်းတွက်လို့ရသလို၊ Decimal နှင့်လည်း တွက်လို့ရပါတယ်။ ၂ နည်းစလုံးကို ပြသွားမှာပါ။ လွယ်ပါတယ်။ ကျောင်းသားတစ်ယောက် ပြောသလို ဘာတဲ့ ဆရာလွယ်တယ်။ တပည့်ခက်တယ်ဆိုတာမျိုးတော့ ဖြစ်နေမလားမသိဘူး။

Address တစ်ခု ဥပမာ ပေးပြီးရှင်းပြမယ်နော်။ ဆိုကြပါစို့။

172.60.0 .0, 255.255.0.0 နှင့် ကျွန်တော် ရှင်းပြပါ့မယ်။ First Octet မှာ 172 ဆိုကတည်းက ဒါ Class B ဖြစ်တယ်နော်။ အခု Subnet 3 bits စာ ခွဲမယ်။

❖ ဒီတော့ နဂိုက -

IP Address: 172.60.0.0
Subnet Mask: 255.255.0.0

❖ Subnet 3 bits ခွဲလိုက်တော့ -

IP Address: 172. 60.0.0
Subnet Mask: 255.255.224.0 ဖြစ်သွားပါလိမ့်မယ်။

ဒီတော့ Subnet Mask ရဲ့ First Octet 255 ၏ 8 bits နှင့် Second Octet 255 ၏ 8 bits ပေါင်း 16 bits ဟာ အသေဖြစ်တယ်။ ဒီအတိုင်းထား။ Third Octet က 224 ဆိုတော့ Binary အရပြောရင် 11100000 ဖြစ်တယ်။ ဒီတော့ Subnet က 3 bits စာဆိုတော့ 2^3 ဖြစ်တယ်။ 2^3 က 8 ရတယ်။ Subnet 8 ခုရတယ်ပေါ့၊ ကောင်းပြီ။ Host ကရော။ Host က 13 bits ပေါ့။ အခုရှင်းပြမယ့် အကြောင်းအရာများ Host နှင့် မသက်ဆိုင်တော့ဘူး။ ဒါကြောင့် Host ကို ခဏဖွက်ထား။ အခု အခြားတစ်ခုဆွဲမယ်။ အဲဒီ ဇယားမှာ ပုံသေကော်လံ ၃ ခုရှိမယ်။ Ok နော်။ ပုံသေ ကော်လံ ၃ ခုရှိမယ်။ Row ကတော့ Subnet ရှိသလောက်ပေါ့။ အခု Subnet ဘယ်လောက်ရှိလဲ။ Subnet က ရှစ်ခုရှိတော့ Row က 8 တန်းဆွဲပါ။ ပြန်ပြောမယ်နော်။ ဇယားတစ်ခု တည်ဆောက်မယ်။ ဇယားက ကော်လံ ၃ ခုရှိမယ်။ အသေပဲ။ Row ကျတော့ အသေမဟုတ်ဘူး။ Row က Subnet ရှိသလောက် Subnet က 3 bits ဆိုတော့ 2^3 ကြောင့် 8

ခဲ့ရတယ်။ ဒါကြောင့် Subnet ရှစ်ခုရှိလို့ ၎င်း ဇယားမှာ Row ရှစ်တန်းရှိရမယ်။ Ok နော်။

အခုတော့ Row 8 တန်းရှိပြီး ကော်လံ 3 ခုရှိတဲ့ ဇယားတစ်ခုကို ဆွဲလိုက်ပါ။ ကျွန်တော်လည်း အောက်မှာ ဆွဲပြထားတယ်။

၁။ ပထမကော်လံမှာ Subnet အရေအတွက်အတိုင်း နံပါတ်စဉ်လိုက်ရှိမယ်။

၂။ ဒုတိယ ကော်လံမှာ Subnet ကို Binary နှင့် ပြပေးမယ်။

၃။ တတိယ ကော်လံမှာ Subnet Address အသေဖြစ်သွားတဲ့ Bit အရေအတွက်ကို Prefix နှင့် ပြမယ်။

Subnet	Binary Representation	Subnetted Address Prefix
1	10101100.00111100.0000000.00000000	172.60.0.0/19
2	10101100.00111100.00100000.00000000	172.60.32.0/19
3	10101100.00111100.01000000.00000000	172.60.64.0/19
4	10101100.00111100.01100000.00000000	172.60.96.0/19
5	10101100.00111100.1000000.00000000	172.60.128.0/19
6	10101100.00111100.1010000.00000000	172.60.160.0/19
7	10101100.00111100.1100000.00000000	172.60.192.0/19
8	10101100.00111100.1110000.00000000	172.60.224.0/19

၃.၅ ဖော်မြူလာကို ရှင်းပြပြီ

ကဲ ဇယားမှာ အဖြေတွေအားလုံးပါသွားပြီ။ ဘာဖြစ်လို့ ဒီအဖြေတွေဖြစ်ရသလဲဆိုတာကို ရှင်းပြတော့မယ်။ ပထမ Row ကိုကြည့်ပါ။

Subnet 8 ခုရှိတဲ့အထဲက ပထမ Subnet ဖြစ်တဲ့အတွက်ကြောင့် Subnet မှာ 1 ဖြစ်ပါတယ်။ ဒုတိယ ကော်လံမှာ –

- ❖ 172 ကို Binary ပြောင်းထားတာက 10101100 ဖြစ်ပါတယ်။
- ❖ 60 ကို Binary ပြောင်းထားတာက 00111100 ဖြစ်ပါတယ်။
- ❖ 0 ကို Binary ပြောင်းထားတာက 00000000 ဖြစ်ပါတယ်။
- ❖ 0 ကို Binary ပြောင်းထားတာက 00000000 ဖြစ်ပါတယ်။

ဒီနေရာမှာ 000 (သုည ခုလုံး) ကို မျဉ်းတားပြထားပါတယ်။ ဒါ ဖော်မြူလာဖြစ်ပါတယ်။ ဖော်မြူလာကို အခုပြောပြတော့မယ်။ 32 bits သုံးခုပေါင်းရှိတဲ့အထဲက First Octet 8 bits နှင့် Second Octet 8 bits တို့ နှစ်ခုပေါင်း 16 bits က အသေပဲမို့လို့ သူတို့ကို ဘာမှမလုပ်နှင့်။ နောက် 16 bits ထဲက Subnet ကို 3 bits ပေးတာမဟုတ်လား။ အဲဒီ 3 bits ကိုပဲ ကစားမှာ။ ဒါကြောင့် အဲဒီ 3 bits ကို မျဉ်းတားထားတာ။ ဒီတော့ ကျန်တဲ့ 16 bits ထဲက ၎င်း 3 bits ကိုဖျက်ပြီး၊ ကျန်တဲ့ 13 bits ကို 0 များ ထားပါ။ ဒါ အဓိက အချက်ပဲ။ အကယ်၍ Subnet ဘက်ကို 4 bits ထားရင်၊ 16 bits ထဲက 4 bits ကို ကစားပြီး၊ ကျန် 12 bits ကို 0 များအဖြစ် သတ်မှတ်ရမှာဖြစ်ပါတယ်။ ခုလောလောဆယ် ရှင်းပြနေတာ ကတော့ 3 bits မို့ 16 bits ထဲက မျဉ်းတားထားတဲ့ 3 bits ကိုကစားပြီး။ 13 bits ကို 0 များအဖြစ် သတ် မှတ်လိုက်ပါ။ ကစားရမယ့် 3 bits ကို အခုရှင်းပြမယ်။

- ❖ 1 ဆိုရင် 000
- ❖ 2 ဆိုရင် 001
- ❖ 3 ဆိုရင် 010
- ❖ 4 ဆိုရင် 011
- ❖ 5 ဆိုရင် 100
- ❖ 6 ဆိုရင် 101
- ❖ 7 ဆိုရင် 110
- ❖ 8 ဆိုရင် 111

ကဲ တတိယကော်လံကို ဆက်ပြီးရှင်းပြဦးမယ်။ ပထမ Row ကိုကြည့်။ 192.168.0.0/1 ဆိုတာကို

တွေ့လိမ့်မယ်။ အဲဒီ ဒုတိယကော်လံက Binary တွေကို Decimal ပြောင်းထားတာ။ / 19 ဆိုတာက First Octet ရဲ့ 8 bits နှင့် Second Octet ရဲ့ 8 bits ပေါင်း၊ 16 bits ရှိမယ်။ ဒါက Network Address ကို ရည်ညွှန်းတဲ့ 16 bits ဟုတ်ပြီနော်။ နောက်က 16 bits က Host Bit။ Host Bit ထဲက 3 bits ကို Network ဘက်ကို ပို့လိုက်တော့ Network ဘက်မှာ 19 bits ဖြစ်သွားပါတယ်။ /19 ဆိုတာက အဲဒီ 19 bits ကို ရည်ညွှန်းတာဖြစ်ပါတယ်။

ကောင်းပြီ။ ဒီတော့ သင်က Network ဖက်ကို 3 bits ပို့တော့ Network က $2^3 = 8$ ဆိုတော့ Subnet 8 ခု ရှိတယ်မဟုတ်လား။ ၎င်း Subnet 8 ခုရဲ့ Subnet ခွဲပြီးသား Address တွေကို Subnetted Octet လို့ ခေါ်တာဖြစ်တယ်။ ဒီတော့ Subnet 8 ခုရှိတဲ့ အတွက်ကြောင့် Subnet ခွဲပြီးသား Subnetted Octed 8 ခုထွက်လာရမယ်။ အဲဒီ 8 ခုကို တွက်ထားတာကို အခုပြောနေတာဖြစ်ပါတယ်။

ဒီတော့ 172.60.0.0 ကို Subnet 8 ခုခွဲလိုက်တဲ့အခါမှာ ရလာတဲ့ Subnetted Octet တွေက တော့ 0,32, 64, 96, 128 , 160 , 192, 224 တို့ ဖြစ်ကြပါတယ်။

ပြန်ပြောပြဦးမယ်။ 172.60.0.0, 255 255.0.0 ကို Subnet 8 ခုခွဲလိုက်တဲ့အခါ Address ဟာ 172.60.0.0 , 255.255.0 .0 ဆိုပြီးဖြစ်သွားတယ်။ ဒီတော့ သိရမှာက အဲဒီလို ခွဲထွက်လိုက်တဲ့ Subnet 8 ခုရဲ့ Subnet Address တွေက တစ်နည်းအားဖြင့် Subnetted Octet တွေက ဘာတွေလဲဆိုပြီး မေးစရာ ဖြစ်လာတယ်။ ဒီ Subnetted Octet 8 ခု တွက်တဲ့နည်း (၂) နည်းရှိတယ်။ Binary နဲ့ တွက်ပြပြီးပြီ။ အခု Decimal နဲ့ တွက်ပြမယ်။ အချို့က Binary ကို သိပ်မကျွမ်းကျင်ဘူး။ ဒီတော့ အခုတွက်ပြမယ့် Decimal နည်းက ပိုလွယ်ကောင်းလွယ်လိမ့်မယ်။

ပုံ ၃၉

ဒီတော့ Subnet ဘက်ကို 3 bits ပို့လိုက်လို့ $2^3 = 8$ ဆိုပြီး Subnet 8 ခုထွက်လာရင် 4 bits ဆိုရင် $2^4 = 16$ ဆိုတော့ Subnetted Octet 16 ခုကို တွက်ရမယ်လေ။ ဒီလိုတွက်ရမယ့် Subnet များလာရင် Binary နည်းထက်စာရင် Decimal နည်းကပိုကောင်းပါတယ်။

၃.၆ Decimal နည်းဖြင့် Subnetted Octet များရှာခြင်း

ထုံးစံအတိုင်း Subnet ၈-ခုခွဲမှာမို့ ဇယားဟာ 8 Row ရှိရမယ်။ ကော်လံကတော့ 3 ကော်လံပဲ။ ပထမကော်လံမှာ Subnet 8 ခုကို 1 ကနေ 8 အထိ အစဉ်လိုက်ရေးမယ်။

ဒုတိယကော်လံမှာ အခုရှာမဲ့ Subnetted Octet ကို ရေးပြီး၊ တတိယကော်လံမှာ Subnetted Address ကို အပြည့်အစုံရေးမယ်။

ဘာမှတော့မခက်ဘူးဗျာ။ သူ့ Formula က 2^{8-3} ပဲ။ 2^{8-3} ဆိုတော့ 2^5 ပေါ့။ ဘာလို့ရတာလဲ ဆိုတော့ 2^{8-n} က ရတာ။ အဲဒီမှာ ကိုယ်ခွဲလိုက်တဲ့ Subnet Bit ကို n မှာထားရမယ်။ ခု ကျွန်တော်တို့က 3 bits Network ဘက်ကို ပို့ထားတာဆိုတော့ ဒီ n နေရာမှာ 3 ကို အစားထိုးရင် 2^{8-n} ဆိုတော့ 2^{8-3} ပေါ့။ ဒီတော့ 2^5 ရတာ။ 2^5 ဆိုတာ 32 ဖြစ်ပါတယ်။ ဒီတော့ Subnetted Octet တွေက တစ်ခုနဲ့ တစ်ခုကြား 32 စီ ခြားသွားမယ်လို့ ပြောချင်တာဖြစ်ပါတယ်။ ဆိုတော့ 172.60.0.0 ကို 255.255.224.0 ဆိုပြီး Subnet ပိုင်းလိုက်ရင် Subnet (၈) ခုထွက်လာလိမ့်မယ်။ ထွက်လာတဲ့ Subnet (၈) ခုရဲ့ Subnetted Octet တွေဟာ တစ်ခုနှင့်တစ်ခု 32 စီကွာတာမို့ 0,32,64,96,128,160.192. 224 ဆိုပြီး ထွက်လာမှာ ဖြစ်ပါတယ်။ ပေါက်တယ်နော်။ လွယ်မှလွယ်။ မရဘူးလား၊ ပြန်ဖတ်ကြည့်ပါ။ ရှင်းရှင်းလေးပါ။

၃.၇ Subnet တစ်ခုမှာရရှိတဲ့ IPv4 Address အတိုင်းအတာ

ဒီတစ်ခါ Subnet တစ်ခုမှာရရှိတဲ့ Host တွေရဲ့ IPv4 အတိုင်းအတာတွေကို ဘယ်လို တွက်ရမလဲဆိုတာကို ဖော်ပြပေးဦးမယ်။ အဲဒီမှာလည်း နည်းလမ်း နှစ်လမ်း နဲ့ဖြစ်ပါတယ်။ ထုံးစံအတိုင်း Binary နည်းနဲ့၊ Decimal နည်းတို့ပဲဖြစ်ပါတယ်။ Subnet ရှစ်-ခုရှိတာမို့ အခုဖော်ပြမယ့် ဇယားဟာ Row 8 ခု ရှိမှာဖြစ်ပါတယ်။

ပထမကော်လံကတော့ Subnet 8 ခုအတွက် 1 ကနေ 8 အထိ အစဉ်လိုက်တိုင်း ဖြစ်ပါတယ်။ ဒုတိယ ကော်လံကတော့ အဲဒီ Subnet တွေမှာရှိမယ့် Host အရေအတွက်အတိုင်း ဘယ်ကနေ ဘယ်အထိ ရတယ်ဆိုတာကို Binary နှင့် ဖော်ပြမှာဖြစ်ပါတယ်။

တတိယကော်လံကတော့ ၎င်း Binary နဲ့ ဖော်ပြထားတဲ့ Address ကို Decimal နဲ့ ဖော်ပြပေးမှာဖြစ်ပါတယ်။ အဓိကကတော့ ဒုတိယကော်လံပဲဖြစ်ပါတယ်။

ကဲ ဒုတိယကော်လံအတွက်ပြုလုပ်ရမယ့် လုပ်ငန်းစဉ်ကတော့ -

ပထမဦးဆုံး IP အတွက်ကတော့ Host Bit တွေ အားလုံးကို 0 မှာထားပါ။ နောက်ဆုံး 1 bit ကိုတော့ 1 ထားပေးပါ။

နောက်ဆုံး IP အတွက်ကတော့ Host Bit တွေအားလုံးကို 1 ထားပါ။ နောက်ဆုံး 1 bit ကိုတော့ 0 ထားပေးပါ။ ကောင်းပြီ။ ဒါဆို ပထမဆုံး Row တွက်ကြည့်ရအောင်။

- ဥပမာပေးထားတဲ့ Address က 172.60.0.0 ဖြစ်တာကြောင့် 172 နှင့် သက်ဆိုင်သော Binary ကို ဘာမှလုပ်စရာမလို၊ ဒီအတိုင်းထား။ 60 နှင့် သက်ဆိုင်သော Binary ကိုလည်း ဒီအတိုင်းထား။ ဒီတော့ 172 ရဲ့ 8 bits နဲ့ 60 နှင့် သက်ဆိုင်သော 8 bits ပေါင်း 16 bits က ဘာမှလုပ်စရာ မလိုဘူး။ ကျန်တဲ့ 16 bits က Network ဘက်ကိုပို့ထားတဲ့ 3 bits ရှိတယ်မဟုတ်လား။ ၎င်း 3 bits မှာ ပြောင်းလဲမယ့် Binary တွေက ရှေ့မှာ Subnetted Octet ဆိုပြီး ဖော်ပြထားပြီးသား။ ဒီတော့ အဲဒီ 16 bits ထဲက 3 bits ကိုနုတ်။ 13 bits ကျန်လိမ့်မယ်။

Subnet တစ်ခုရဲ့ ရှေ့ဆုံး IP ကိုတွက်ချင်ရင်

အဲဒီ 13 bits ထဲက အရှေ့ဆုံး IP အတွက်ဆိုရင် ၎င်း 13 bits ကို အားလုံး 0 ထားပါ။ နောက်ဆုံး 1 လုံးကို 1 ထားပါဆိုတော့ 00000 00000001 ရပါတယ်။

Subnet တစ်ခုရဲ့ နောက်ဆုံး IP ကိုတွက်ချင်ရင်

နောက်ဆုံး IP အတွက်ဆိုရင် ၎င်း 13 bits ကို အားလုံး 1 ထားပါ။ နောက်ဆုံး 1 bits ကို 0 ထားပါဆိုတော့ 11111 11111110 ရပါတယ်။ ဒါပါပဲ။ ဒါလေးပါပဲ။

ဒီတော့ ပထမ Subnet အတွင်းမှာ ရှိတဲ့ Host က ဘယ် IP ကနေ ဘယ် IP အထိလဲ ဆိုတော့-

- 172 ရဲ့ Binary က 10101100, 60 ရဲ့ Binary က 001111100 ။ ဒါကို အသာထား......
- Network ဘက်ကို ပို့ထားတဲ့ 3 bits က 000
- နောက် 13 bits က 00000 00000001

ပို့ထားတဲ့ 3 bits နဲ့ 13 bits ပေါင်းရေးတော့ -

- 00000000 00000001 ဒီတော့ -
- 00000000 ကို Decimal ပြောင်းတော့ 0
- 00000001 ကို Decimal ပြောင်းတော့ 1 ဒီတော့ - အဖြေက
- 172.60.0.1 ကို ရပါတယ်။

ဒါ 172.60.0.0 ကို 255.255.224.0 နှင့် Subnet 8 ခုခွဲလိုက်တဲ့အခါမှာ ရရှိတဲ့ Subnet 8 ခုထဲက ပထမဦးဆုံး Subnet ရဲ့ First IP ပဲ ဖြစ်ပါတယ်။ ဒီတော့ Last IP ကရော -

13 bits မှာ အားလုံးကို 1 ထား နောက်ဆုံးကို 0 ထားဆိုတော့ -

11111 11111110 ရပါတယ်။ အဲဒါကို ရှေ့က Network ကို ပို့ထားတဲ့ 3 bits နဲ့ ပေါင်းတော့ -

- 00011111 1111111 ရပါတယ်။
- 00011111 ကို Decimal ပြောင်းတော့ - 31 ရပါတယ်။
- 11111110 ကို Decimal ပြောင်းတော့ - 254 ရပါတယ်။

ဒီတော့ Last IP က 172.60.31.254 ပါ။ ဒီတော့ Subnet 8 ခုရှိတဲ့အထဲက ပထမဦးဆုံး Subnet ရဲ့ First IP သည် 172.60.0.1 ဖြစ်၍
Last IP သည် 172.60.31.254 ဖြစ်ပါတယ်။

နောက်ကျန်တဲ့ Subnet တွေကိုလည်း အဲဒီလိုချတွက်ကြည့်ပါဦး။ အားလုံးကိုတော့ တစ်ဖက်ပါဇယားမှာ ဖော်ပြထားပါတယ်။

အခု ဒီတစ်ခါ၊ ဒီကိစ္စ၊ ဒီအကြောင်းကိုပဲ Decimal နည်းဖြင့်တွက်ပြပါဦးမယ်။ Binary ကို မကျွမ်းကျင်တဲ့ သူတွေက Decimal နည်းနဲ့တွက်ပေါ့။

First IP ကို ဘယ်လိုတွက်မလဲ။ နောက်ဆုံး Octet ကို 1 ပေါင်းပါ။ ဆိုလိုတာက 172.60.0.0 ကို Subnet ၈-ခုပိုင်းလိုက်တယ်။ ပထမ Subnet ရဲ့ Subnetted Address Prefix က -

172.60.0.0 / 19 ဖြစ်တယ်။ အဲဒီ 172.60.0.0 ရဲ့ Last Octet ကို 1 ပေါင်းတော့ 172.60.0. 1/ 19 ရပါတယ်။

Subnet	Binary Representation	Range of IPv4 Addresses
1	10101100.00111100.00000000.00000001 – 10101100.00111100.00011111.11111110	172.60.0.1– 172.60.31.254
2	10101100.00111100.00100000.00000001 – 10101100.00111100.00111111.11111110	172.60.32.1– 172.60.63.254
3	10101100.00111100.01000000.00000001 – 10101100.00111100.01011111.11111110	172.60.64.1– 172.60.95.254
4	10101100.00111100.01100000.00000001 – 10101100.00111100.01111111.11111110	172.60.96.1– 172.60.127.254
5	10101100.00111100.10000000.00000001 – 10101100.00111100.10011111.11111110	172.60.128.1– 172.60.159.254
6	10101100.00111100.10100000.00000001 – 10101100.00111100.10111111.11111110	172.60.160.1– 172.60.191.254
7	10101100.00111100.11000000.00000001 – 10101100.00111100.11011111.11111110	172.60.192.1– 172.60.223.254
8	10101100.00111100.11100000.00000001 – 10101100.00111100.11111111.11111110	172.60.224.1– 172.60.255.254

ဒီတော့ 172.60.32.0/19 ဆိုရင် Last Octet ကို 1 ပေါင်းတော့၊ 172. 60 .32. 1 ရပါတယ်။ 172. 60 .64 .0 / 19 ရဲ့ Last Octet ကို 1 ပေါင်းတော့၊ 172. 60 . 64 .1 ပေါ့။ ဒီတော့ Subnet

၈–ခုရဲ့ First Octet ကို တွက်ရတာ ဘာမှမခက်ဘူး။ Last Octet 1 ပေါင်းရုံပဲ။

Last IP ကို တွက်တဲ့အခါကျတော့ နောက် Subnet ID ဆီကနေ 1 နုတ်ပေးရမှာ ဖြစ်ပါတယ်။ ဒါပေမယ့် နောက်ဆုံး Subnet ကျတော့ ဒီနည်းနဲ့ တွက်လို့မရတော့ဘူး။ ကဲ တွက်ပြမယ်။

ပုံ ၃.၁၀

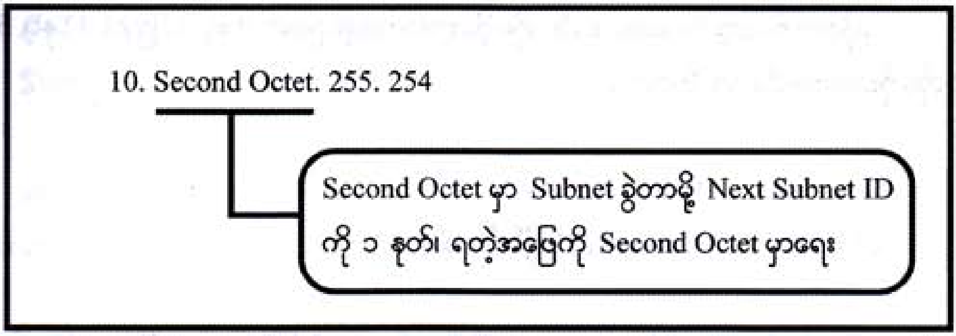
- First Octet ကို တွက်ရတာ ဘာမှမခက်ဘူး။ Last Octet 1 ပေါင်းရုံပဲ။
- Last IP ကို တွက်တဲ့အခါကျတော့ နောက် Subnet ID ဆီကနေ 1 နုတ်ပေးရမှာ
- Subnet ID ဆိုတာ 0, 32, 64, 96, 128, 160, 192, 224 ဒီ Subnet ID ပဲ။

172. 60. 0. 1 ရဲ့ Last IP ကိုတွက်တော့၊ စဉ်းစားရမှာက 172. 60. 0. 1 ရဲ့ Next Subnet ID က 172. 60. 32 . 1 လေ။ မျဉ်းတားပြထားတယ်။ 32 လေ။ ဒီတော့ 32 ထဲက 1 နုတ်တော့ 31 ပေါ့။ ဒီတော့ 172. 60 . 0 . 1 ရဲ့ Last IP က 172. 60 .31 .254 ဖြစ်ပါတယ်။ Last Octet ကတော့ အမြဲတမ်း 254 ပဲ ဖြစ်မှာလေ။ ဒီတော့ နားလည်ရမှာက Next Subnet ID ပဲ။ ဒါကဘာကိုပြောတာလဲဆိုတော့ 0, 32, 64, 96, 128, 160, 192, 224 ဒီ Subnet ID ပဲ။ ဒီတော့ 0 ကနေကြည့်ရင် Next Subnet ID ဆိုတာ 32 ပဲလေ။ 32 ဖက်ကနေကြည့်ရင် Next Subnet ID ဟာ 64 ပဲဖြစ်ပါတယ်။ ဒီတော့ 0 ဆိုတဲ့ ပထမ Subnet အတွက် Last IP ဟာ 64 ထဲက 1 နုတ်တော့ 63 ရတယ်။ ဒီတော့ 172. 60 . 63 . 254 ဖြစ်ပါတယ်။ တကယ်တော့ ဒါတွေဟာ လွယ်လွယ်လေး။ သင်တို့ ဖတ်လို့ နား မလည်ရင် ဒါ လုပ်နေကျမဟုတ်လို့သာ နားမယဉ်တာဖြစ်ပြီး အခေါက်ခေါက် အခါခါ ပြန်ဖတ်ရပါမယ်။ ပြီးတော့ စာရွက်အကြမ်းနဲ့ ခဲတံလည်း ရှိရမှာဖြစ်ပြီး ချတွက်မှသာ နားလည်မှာဖြစ်ပါတယ်။ အိပ်ယာပေါ်ဖက်လို့ကတော့ စိတ်ချ မပူနဲ့ အိပ်ပျော်မှာ။

သတ်မှတ်ချက်တွေကို ပြောရမယ်ဆိုရင် –

၁။ ခွဲထားတဲ့ Subnet ဟာ First Octet မှာ ဆိုလို့ရှိရင် ၎င်း Last IP ဟာ Next Subnet ID-1. 255 .255. 254 ဖြစ်ပါတယ်။ ဆိုလိုတာက 255. 255 . 254 က အသေပေါ့။ ကိုယ်က First Octet မှ Subnet ခွဲတာကို။ နောက်တစ်ခုကို ကြည့်ရင် ပိုရှင်းသွားလိမ့်မယ်။

၂။ ကိုယ်က Second Octet မှာ Subnet ခွဲတာဆိုရင် ရှေ့ဆုံး Octet က ဒီအတိုင်းဖြစ်မယ်။ ထားပါတော့ ဒီတော့ 10. Next Subnet ID-1.255.254 ဖြစ်မယ်။



၃။ အကယ်၍ ကိုယ်က Subnet ကို တတိယ Octet မှာခွဲရင် အခုလိုပေါ့။ 172.60 ဆိုပါစို့။ ဒီ 172.60 ကို ဒီအတိုင်းထား။ 172.60.Next Subnet ID -1.254 ဖြစ်ပါတယ်။

၄။ Fourth Octet ကနေ ခွဲခဲ့သည်ရှိသော်၊ ဥပမာ 192 . 168 . 100 . Next Subnet ID-2 ဖြစ်ပါတယ်။ သတိထား အနုတ် ၂ နော်၊ အနုတ် ၁ မဟုတ်ဘူး။

ကောင်းပြီ။ အခု Subnet 8 ခု ခွဲထုတ်လိုက်တာ ၎င်း Subnet တစ်ခု အတွင်းမှာရှိတဲ့ IPv4 Address Range ကိုတွက်တဲ့နည်း ပြောပြနေတာဖြစ်ပါတယ်။ First IP က ဘာလဲ။ Last IP ကဘာလဲပေါ့။ အခု Decimal နည်းနဲ့ Last IP တွက်တဲ့နေရာမှာ နောက်ဆုံး Subnet 8 ခုမြောက် Subnet ရဲ့ Last IP ကို ကျတော့ -

ခြွင်းချက်။ ။အောက်ပါနည်းအတိုင်း တွက်ရမှာဖြစ်ပါတယ်။

သူ့ရဲ့ Formula ကတော့-

Subnet ID + i - 1 ဖြစ်ပါတယ်။ Subnet ID ကို i နှင့်ပေါင်း ၁ ပြန်နုတ်ဖြစ်ပါတယ်။

❖ Subnet ID များကတော့ အခု Subnet 8 ခုအတိုင်း ပြောရရင် 0, 32, 64 , 96 , 128 , 160 , 192, 224 တို့ဖြစ်ပါတယ်။

❖ i ဆိုတာကတော့ Increment ပါ။ တိုးတိုးသွားတာပေါ့။ ဥပမာ 0 နှင့် 32 ကြား 32 နှင့် 69 ကြား 32 တိုးတိုးသွားတယ်လေ။ ဒီတော့ –

Subnet ID + i -1

244 + 32 - 1 = 256 - 1 = 255 ဖြစ်ပါတယ်။

၈ ခုမြောက် Subnet ရဲ့ ID က 224 ဖြစ်တယ်လေ။ ဒါကြောင့် 224 ကို 32 နှင့်ပေါင်းတာ 32 ဆိုတာ Subnet တစ်ခုနှင့်တစ်ခုက 32 များတာကို။ နောက်ဆုံး Subnet ရဲ့ Last IP ကိုတွက်တဲ့အခါ အချုပ်ပြန်ပြောရရင် –

၁။ အကယ်၍ Subnet ဟာ First Octet မှာ ခွဲထားတာဆိုရင် –
Subnet ID + i - 1 . 255. 255. 254 ဖြစ်ပါတယ်။

၂။ အကယ်၍ Subnet ဟာ Second Octet မှာခွဲတာဆိုရင် –
ဥပမာ Frist Octet က 10 ဆိုပါစို့။ ဒါဆို 10. Subnet ID + 1-1 . 255. 254 ဖြစ်ပါတယ်။

၃။ အကယ်၍ Subnet ဟာ Third Octet မှာခွဲတာဆိုရင် –
ဥပမာ အခုတွက်ပြနေတဲ့ 172.60 လို့ပေါ့။ ဒီတော့ –
172. 60 . Subnet ID+i - 1 . 254 ဖြစ်ပါတယ်။

၄။ အကယ်၍ Subnet ဟာ Fourth Octet မှာ ခွဲတာဆိုရင် –
194.168.100. Subnet ID + i - 2 ဖြစ်ပါတယ်။ ဘာလို့ -2 ဖြစ်ရသလဲဆိုတော့ 254 အထိပဲ ရှိရမယ်လေ 255 က ဖယ်ရမှာလေ။ ရှေ့ဆုံး Host 0 နှင့် နောက်ဆုံး Host 1 ကို ဖယ်ရတာ ဖြစ်ပါတယ်။ ရှေ့ဆုံး Host 0 ဆိုတာ Binary အရပြောရင် 00000000 ဖြစ်ပါတယ်။ ဒါကို All Zero လို့ပြောတာ ဖြစ်ပါ

ဘယ်။ နောက်ဆုံး Host ကတော့ 11111111 ဖြစ်ပါတယ်။ ဒါကို All One လို့ခေါ်ပါတယ်။ ဒီ All Zero, All One Host နှစ်ခုကို မရေရပါဘူး။ ဒါကြောင့် နောက်ဆုံးတွက်ချက်မှုမှာ -1 အစား -2 ဖြစ်ရခြင်းဖြစ်ပါတယ်။

၃.၈ Address တခုဘယ် Subnet မှာရှိနေသလဲ သို့မဟုတ် Subnet Address တွက်ခြင်း

အခုရှင်းပြနေတဲ့ 172.60.0.0 , 255.255 .224.0 ဆိုတဲ့ ဥပမာနဲ့ပဲ ရှင်းပြမှာဖြစ်ပါတယ်။ ၎င်းဥပမာမှာ Subnet 8 ခုရှိပါတယ်။ ၎င်း Subnet တွေကတော့ ရှေ့မှာရှင်းပြဖော်ပြခဲ့ပြီးတဲ့အတိုင်း –

- 172.60.0.0/19
- 172.60.32.0/19
- 172.60.64.0/19
- 172.60.96.0/19
- 172.60.128.0/19
- 172.60.160.0/19
- 172.60.192.0/19
- 172.60.192.0/19
- 172.60.224.0/19 တို့ဖြစ်ကြပါတယ်။ ဒီ Subnet 8 ခုပေါ့နော်။ အခုရှင်းပြမှာက ကျွန်တော်က Address တစ်ခုပေးမယ်။ အဲဒီ Address က ဘယ် Subnet မှာ ရှိနေသလဲဆိုတာကို ရှာကြည့်မှာ ဖြစ်ပါတယ်။ ဒါတော့ Subnet Address ရှာခြင်းပေါ့။ ကဲကောင်းပြီ။ မေးခွန်းစမေးပြီ။

IP Address: 172. 60 .100 . 70

Subnet Mask: 255. 255. 224 . 0 ဆိုတဲ့ Address ဟာ ဘယ် Subnet မှာ ရှိသလဲ။

ဆိုလိုတာက ၎င်း Address သည် အထက်ပါ Subnet 8 ခုထဲက ဘယ် Subnet မှာ ရှိနေသလဲလို့ မေးနေတာဖြစ်ပါတယ်။ ဒီမေးခွန်းဟာ MCSA (Microsoft Certified System Administrator) ရဲ့ Exam Code 291 : Windows Server 2003 Infrastructure မှာ မေးတတ်တဲ့ မေးခွန်းပုံစံဖြစ်ပါတယ်။ အဲဒီအပြင် ဒီသင်ခန်းစာတွေဟာ Cisco Certified Network Associate ဆိုတဲ့ CCNA Exam အတွက် အခြေခံကျတဲ့

သင်ခန်းစာတွေဖြစ်ပါတယ်။

ကဲ- IP Address: 172. 60 . 100 . 70
Subnet Mask: 255. 255. 224 . 0 ဟာဘယ် Subnet ရှိလဲ။

ရှင်းနေတာပဲ။ 172. 60 .96 . 0 /19 တနည်းအားဖြင့် 172. 60 .96 .0 , 255 . 255 .224 . 0 ဆိုတဲ့ Subnet မှာ ရှိနေတာပေါ့။ ဒီတော့ ဒီမေးခွန်းရဲ့အဖြေက -

IP Address 172.60.96.0
Subnet Mask 255.255.224.0 ဖြစ်ပါတယ်။

တနည်းအားဖြင့် Subnet 8 ခုရဲ့ ၄ ခုမြောက် Subnet ပေါ့။ ဒီလိုလေဗျာ။ ဒီ ၄ ခုမြောက် Subnet က 172.60.96.0/19 မဟုတ်လား။ ၎င်း Subnet ရဲ့ IP Address Range က 172.60.96.0 / 19 မဟုတ်လား။ ၎င်း Subnet ရဲ့ IP Range က 172.60.96.1 ကနေ 172.60.127.254 အထိ ရှိတယ်လေ။ ခု ကျွန်တော်တို့ကို ပုစ္ဆာ ကမေးတဲ့ Address က 172.60.100.70 ဆိုတဲ့ ၎င်းမှာ 100 ကိုကြည့်။ 100 က 96 နှင့် 127 ကြားမှာ ရှိနေတာလေ။ ဒါကြောင့် 172.60.100.70 /19 ဆိုတဲ့ Subnet မှာ ရှိနေပါတယ်လို့ ဖြေလိုက်ရုံပါပဲ။ ဒါတော့ ဒါပေါ့လေ။ ဒါပေမဲ့ သိရမှာက ဒါတွက်နည်းအမှန်မဟုတ်ဘူးဂျ။ ခုဟာက Subnet ၈-ခုပဲရှိတာလေ။ Subnet အများကြီးသာရှိရင် အဲ့ဒီ Subnet တွေလိုက်တွက်နေတာတင် အချိန်စေ့သွားမှာ။ ဒီတော့ကား Subnet Address ရှာတဲ့နည်းဆိုတာကို အခု ရှင်းပြတော့မယ်။ ထုံးစံအတိုင်းပဲ နည်းလမ်းနှစ်လမ်းနဲ့ တွက်ပြမယ်။ စိတ်ဆိုးသွားလား။ သင်ပြောချင်နေတယ် မဟုတ်လား။ စာရေးဆရာရယ် ၁ နည်းပဲပြလည်း စိတ်မဆိုးပါဘူး ဆိုပြီး။ ကဲထားပါလေ။ ကျွန်တော်က စေတနာနဲ့ပါဂျ။

၃.၉ ဒေသမနည်းက Prefix Length Notation

ဒီနည်းက နည်းနည်းလွယ်တယ်။ Logical AND တို့ Logical OR တို့မပါဘူး။ ဒါကြောင့် AND, OR Operation တွေ လေ့လာစရာမလိုဘူး။ ကဲ ချရအောင်။ ဟဲ့ဟဲ့ - ဘာလဲဗျ ချရအောင်။ ဖဲယားကွက်ချဖို့ ပြောတာပါဗျာ။ ဖယားကွက် ကော်လံက ၄ ကွက်၊ အတန်းက ၃ တန်း ဖယားချလိုက်ပါ။

172	60	100	70

ပထမတန်းမှာ အစုတွက်မဲ့ ပုစ္ဆာ က IP Address လို့ ထည့်လိုက်ပါ။ ပြီးရင် သူ့ရဲ့ Prefix Length က /19 ဖြစ်ပါတယ်။ အဲဒီ 19 ကို 8 နှင့် အခါခါ ပေါင်းပါ။ ဆိုလိုတာက 8 နှင့် 8 ပေါင်း 16 ရမယ်။ 16 နှင့် 8 ပေါင်းရင် 24 , 24 ဆို မဖြစ်တော့ဘူး။ 19 ထက်ကြီးသွားပြီ။ ဒီတော့ 16 ကို 3 ပေါင်း။ ဒါဆို 19 ရမယ်။ ဆိုလိုတာက 19 သည် 8+8+3 ဖြစ်ပါတယ်။ ၎င်းကို ဒုတိယတန်းမှာ ထည့်လိုက်ပါ။

172	60	100	70
8	8	3	0

19 ကို ဖြစ်အောင် 8 တွေနှင့် ပေါင်းလာတာ ဖြစ်ပါတယ်။ ဘာလို့ 8 နဲ့ ပေါင်းလဲ။ 8 bits ကိုး။ ပြီးရင် 8 အပေါ်က ဂဏန်းနဲ့ 0 အပေါ်က ဂဏန်းကို တွက်စရာ မလိုတူးလို့မှတ်ပါ။ ဒီတော့ ဒီ 8 အပေါ်က ဂဏန်းတွေကို ဒီအတိုင်းချရေးပါ။ 0 ပေါ်က ဂဏန်းကျတော့ 0 လို့ပဲ ရေးပါ။

172	60	100	70
8	8	3	0
172	60		0

တစ်ပေါက်ပဲလိုတော့တယ်။ (ဖဲသမားနဲ့တော့လာတွေ့နေပြီ။) ရှင်းပြဖို့။ ကဲစပြီဗျို့။ 100 ကို Binary ပြောင်းပါ။ Binary ပြောင်းတတ်သေးလား။ 100 ကို 128 စီ ဝင်လားတို့၊ ဘာတို့လေ။ ကဲ မေ့သွားရင် ကိုယ့်ဘာသာကိုယ် နောက်ကြောင်းပြန်လှည့်ကိုယ့်ဆရာရှာ။ ဒါတွေ မရဘဲနဲ့တော့ 291 တို့ဘာတို့ ဖြေဖို့ မကြိုးစားနှင့်။ ကဲ လေကြောက ရှည်ပြန်ပြီ။ ဒါတွေမရဘဲ စာမေးပွဲအောင်တဲ့သူတွေ ရှိနေပြီ။ ဟယ်တော်လိုက်တာ။ အံ့ပါရဲ့ အံ့ပါရဲ့။ ကဲ ထားပါ။

100 ကို Binary ပြောင်းရင် 01100100 ရပါတယ်။ 100 ဆိုတာက 64+32+4 ကိုးဗျ။ စိတ်မရှိနဲ့ဗျ။ သချ်ာတွေ ပြန်တွက်ရင်း၊ ငယ်မူပြန်ချင်လာလို့ပါ။

ကောင်းပြီ။ 01100100 မှာ 011 ဆိုတဲ့ 3 bits စာကိုဖယ်။ ဘာကိုကြည့်ပြီး ဖယ်တာလဲ။ စောနက အဲလေ ခုနက 19 ကို 8+8+3 မဟုတ်လား။ အဲဒီက 3 ကိုပြောတာ။ ဒီနေရာမှာ 3 ဖြစ်တာကြောင့် 100 ရဲ့ Binary 01100100 ထဲက ရှေ့ 3 bits ကို ဖယ်တာဖြစ်တယ်ဗျ။ ကောင်းပြီ။ 011 ကို ဖယ်ပြီး ဘာလုပ်ရမလဲ။ 8 bits ပြည့်အောင်၊ ကျန်တဲ့ 5 bits ကို 0 တွေ ဖြည့်လိုက်။ ဒါဆို 01100000 ဆိုပြီး ရပါလိမ့်မယ်။ ၎င်းကို Decimal ပြန်ပြောင်းလိုက်။ လူရွှင်တော်တွေပြောသလိုခေါင်းကိုကုတ်ပြီး ရှုပ်နေတာပဲလို့ မပြောလိုက်ပါနဲ့။ ပျော်ဖို့ကောင်းပါတယ်ဗျ။

01100000 ကို Decimal ပြန်ပြောင်းတော့ 1 ရှိတဲ့ ဂဏန်းပေါင်းပေ့ါ။

128	64	32	16	8	4	2	1	
0	1	1	0	0	0	0	0	= 96 ရပါတယ်။

ဒီတော့ ခုနက ဇယားကွက်ရဲ့ လွတ်နေတဲ့ အပေါက်တစ်ကွက်မှာ ၎င်း 96 ကို ဖြည့်လိုက်ပါ။

172	60	100	70
8	8	3	0
172	60	96	0

ဒီတော့ကား IP Address 172.60.100.70 /19 သို့မဟုတ် Subnet Mask 255. 255 .224 . 0 ဆိုသည့် Host သည် Subnet 8 ခုထဲက 4 ခုမြောက်သော Subnet ဖြစ်တဲ့ 172.60.96.0/19 တွင် တည်ရှိပါသည်။ အဖြေက 172.60.96.0 ဖြစ်ပါတယ်။ ဒါ Subnet Address ရှာတာပါ။

နောက် Address တစ်ခုလောက်တွက်ကြည့်ရအောင်။

IP Address 172. 60. 207.47

Subnet Mask 255. 255. 224. 0 ကိုတွက်ကြည့်ရအောင်။ ကဲ ချမယ် လာပြန်ပလား။ ဇယားကွက် ချမယ်လို့ပြောတာပါဂျ။ ဂဏန်းပေါင်းတောင် လူကို ဖဲသမားများမှတ်နေသလားမသိပါဘူး။

172	60	207	47
8	8	3	0
172	60		0

ကဲ ပေါက်နေတဲ့တစ်ကွက်ကိုတွက်ဖို့ရာ 207 ကို Binery ပြောင်းပါ။ 207 က 128+64+8+4+2+5 ဖြစ်ပါတယ်။ ဒီတော့ Binery အရ ပြောရင် 1100111 ဖြစ်ပါတယ်။ ထုံးစံအတိုင်း 3 ကိုကြည့်ပါ။ 1100111 ထဲက 3 bits ကိုဖယ်တော့ 110 ရပါတယ်။ ကျန်တဲ့ 5 bits ကို 0 တွေ ဖြည့်လိုက်ပါ။ 11000000 ရပါလိမ့်မယ်။ 11000000 ကို 1 ရှိတဲ့ ဂဏန်းပေါင်းပါ။

128	64	32	16	8	4	2	1
1	1	0	0	0	0	0	0

= 192 ရပါတယ်။

ဒီတော့ 192 ကို ပေါက်နေတဲ့ တစ်ကွက်မှာ ဖြည့်ပါ။

172	60	207	47
8	8	3	0
172	60	192	0

ဒီတော့ အဖြေက 172. 60 .192 . 0 ဖြစ်ပါတယ်။ ဆိုလိုတာက 172.60.207.47/19 ဆိုတဲ့ Host က Subnet ၈ ထဲက ၅ ခုမြောက်သော Subnet ဖြစ်တဲ့ 172. 60 . 192. 0 ဆိုတဲ့ Subnet မှာရှိပါတယ် ။

၃. ၁၁ ခုတိယနည်းက **Subnet Mask Notation** နည်း

ဒီနည်းကို Bitwise Operation နည်းလို့လည်း ခေါ်ပါတယ်။ Logical AND Operation ကိုတော့ နားလည်ရမှာ ဖြစ်ပါတယ်။ ဒီတော့ AND Operation ကိုအရင် ရှင်းပြမယ်။ အောက်ကဇယားကိုကြည့်ပါ။

Bit Combination	Result
1 AND 1, 1 နှင့် 1 နှင့်ဆို	1
1 AND 0, 1 နှင့် 0 နှင့်ဆို	0
0 AND 0, 0 နှင့် 0 နှင့်ဆို	0
0 AND 1, 0 နှင့် 1 နှင့်ဆို	0

လွယ်ပါတယ်။ လာပြန်ပါလား လွယ်ပါတယ်။ တကယ်လွယ်ပါတယ်ဗျ။ တစ်ခုပဲမှတ်ရုံပဲ။ 1 နှင့် 1 နှင့် ဆို 1 ကျန်တာ 0 ပဲ။ ဂလိုလေး မှတ်ထားပေါ့။

ကဲ စပြီ။

IP Address က 172.60.100.70

Subnet Mask က 125.255.224.0

၎င်းတို့ကို Binary ပြောင်းပစ်ပါ။

IP Address Decimal:	172.60.100.70	→	10101100	11111100	01100100	01000110
Subnet Mask:	255. 255. 224. 0	→	11111111	11111111	11100000	00000000
၎င်းတို့ကို Binary AND လိုက်ပါ။		→	10101100	00111100	01100000	00000000

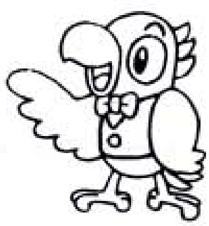
ဆိုပြီး အဖြေထွက်လာပါတယ်။ ၎င်းတို့ကို Decimal ပြောင်းလိုက်တော့ –

10101100	00111100	01100000	00000000	
172	60	96	0	ရပါတယ်။

တကယ်တော့ Binary AND ရဲ့ သဘောတရားအရ 1 နှင့် 1 ဆို 1 ရတာကြောင့် 255 ကို Binary ပြောင်းတော့ 1 တွေကြီးပဲရတယ်။ ဒါကြောင့် 255 နှင့် 255 အပေါ်က ဂဏန်းကို တွက်စရာမလိုဘူး။ 11111111 နှင့် AND တဲ့ မည်သည့် Binary မဆို သူ့မူရင်းအတိုင်းပဲ ပြန်ထွက်တယ်။ 0 ကို Binary ပြောင်းလို့ 00000000 နှင့် ဘယ် Binary ပဲလာပြီး AND ပါစေ။ သူ့ မူရင်းအတိုင်းပဲ ပြန်ထွက်တယ်။ ဒါကြောင့် 255. 255. 224 . 0 မှာ 255. 255. 0 ကို တွက်စရာမလိုဘဲ၊ 224 တစ်ခုတည်းကိုသာ တွက်လျှင်ရကြောင်းပါခင်ညာ။ ဒီတော့ အဖြေက 172.60.96.0 ရပါတယ်။

ပုံ ၃-၁၂

11111111 နှင့် AND တဲ့ မည်သည့် Binary မဆို သူ့မူရင်းအတိုင်းပဲ ပြန်ထွက်တယ်။ 0 ကို Binary ပြောင်းလို့ 00000000 နှင့် ဘယ် Binary ပဲလာပြီး AND ပါစေ။ သူ့ မူရင်းအတိုင်းပဲ ပြန်ထွက်တယ်။ ဒါကြောင့် 255 နှင့် 0 ကိုပြောင်းစရာမလိုဘူး။



နောက် Address တစ်ခု တွက်ပြဦးမယ်။ 172.60. 207. 47 ဆိုတဲ့ IP Address ရှိတဲ့ Host ဟာ ဘယ် Subnet မှာများ ရှိနေမလဲ တွက်ကြည့်မလား။

IP Address: 172.60. 207.47

Subnet Mask: 255.255.224.0

207 ၏ Binary	→	11001111 ဖြစ်ပါတယ်။
224 ၏ Binary	→	11100000 ဖြစ်ပါတယ်။
Binary AND	→	11000000 ဖြစ်ပါတယ်။

၎င်းကို Decimal ပြောင်းသော် 192 ရပါတယ်။ ဒီတော့ အဖြေက 172.60.207.47, 255.255.224.0 ဆိုတဲ့ Address ကို ပိုင်ဆိုင်ထားတဲ့ Host ဟာ 172. 60. 192. 0 ဆိုတဲ့ Subnet 8 ခုမြောက် Subnet မှာ ရှိနေကြောင်းပါခင်ဗျား။

၃. ၁၁ **Broadcast Address ကို တွက်ခြင်း**

Broadcast Address ဆိုတာ Subnet တစ်ခုထဲမှာရှိတဲ့ Host တွေ အားလုံးဆီကို Information အကြောင်းအရာတွေ အားလုံး ရောက်သွားအောင် ပေးပို့နိုင်တဲ့ IP Address ကို ခေါ်တာဖြစ်ပါတယ်။ ဆိုလိုတာက ကိုယ်ပေးချင်တဲ့ Information တွေကို အဲဒီ Broadcast Address ဆီပို့လိုက်ရင်၊ ၎င်း Subnet မှာရှိတဲ့ Host တွေအားလုံးဆီကို ရောက်သွားပါလိမ့်မယ်လို့ ပြောချင်တာပါ။ သူ့ကို ဘယ်နေရာမှာ သုံးသလဲဆိုရင် ရှင်းပါတယ်။ Message တစ်ခုကို Subnet တစ်ခုတည်းမှာရှိတဲ့၊ Host တွေအားလုံးဆီကို ရောက်စေချင်တဲ့အခါမှာသုံးတာပေါ့။

အခု Broadcast Address ကို Bitwise နည်းနဲ့ တွက်ပြမယ်။ ဥပမာ Address တစ်ခုပေးမယ်။

IP Address က	150.10.10.10
Subnet Mask က	255.255.252.0 ဆိုကြပါစို့။

၎င်း Address ရဲ့ Broadcast Address ကို တွက်ချင်ရင် –

၁။ ပထမဦးစွာ ၎င်း Address ဟာ ဘယ် Subnet မှာ ရှိသလဲဆိုတဲ့ Subnet Address ကို အရင်ရှာပါ။ ရရင် ၎င်း Address ကို Binary ပြောင်းပါ။

၂။ ၎င်း Address ရဲ့ Subnet Mask ကို Binary ပြောင်းပါ။ ပြီးရင် ပြောင်းထားတဲ့ Binary ဂဏန်းများကို

ပြောင်းပြန်လှန်ပါ။ ဆိုလိုတာက 0 ဆို 1 ဖျာ၊ 1 ဆို 0 ဖျာ။

၃။ အဆင့် ၁ က Binary နှင့် အဆင့် ၂ က Binary ကို Logical OR Operation ပြုလုပ်ပေးရမယ်။ OR Operation ဆိုတာက -

0 OR 0 = 0 , 0 နှင့် 0 ဆို 0
1 OR 0 = 1 , 1 နှင့် 0 ဆို 1
0 OR 1 = 1 , 0 နှင့် 1 ဆို 1
1 OR 1 = 0 , 1 နှင့် 1 ဆို 0

၄။ ထွက်လာသော Binary ကို Decimal ပြန်ဖွဲ့ပါက Broadcast Address ကို ရပါပြီ။ နောက်တစ်နည်း ရှိသေးတယ်ဗျ။ ဒါပေသိ၊ ရှုပ်သွားမှာစိုးလို့ ဒီတစ်နည်းပဲ ဖော်ပြပေးလိုက်ပါတယ်။

IP Address: 150 . 10 .10 .10
Subnet Mask: 255 . 255. 252. 0 ကို Subnet Address ရှာလိုက်ရင် -

Subnet Mask အပေါ်က ဂဏန်းတွေကို ဒီအတိုင်းပြန်ရေး။ နောက်တစ်ခု Subnet Mask 0 ဆို 0 ပြန်ရေး။ ဒီတော့ 150. 10. ? . 0 ကိုရမယ်။ ? နေရာကို ကိုယ့်ဘာသာ ကိုယ်ရှာကြည့်လိုက်။ 8 ရလိမ့်မယ်။ မရှာတတ်ရင် Subnet Address တွက်တဲ့ နည်းကိုပြန်ဖတ်။ ကောင်းပြီ။ ကဲ Subnet Address က 150. 10. 8 .0 ရပါတယ်။ ၎င်းကို Binary ပြောင်းရအောင်။

Subnet Address: 150. 10. 8 .0 ➔ 10010110. 00001010. 00001000 . 00000000

၏ Binary

Subnet Mask 255.255.252.0 ➔ 0000000. 0000000. 0000011. 11111111

ရဲ့ Binary ကို အကြမ်းမှာချတွက်။

ပြီးရင် ၎င်းကိုပြောင်းပြန်လှန်

Binary OR ➔ 10010110. 00001010. 00001011. 11111111

၎င်းကို Decimal ပြောင်းရင် 150. 10.11.255 ရပါတယ်။ ၎င်းဟာ ဒီပုစ္ဆာရဲ့ Broadcast Address ပဲ ဖြစ်ပါတယ်။

၃.၁၂ **Subnetting** နှစ်မျိုး

Subnetting ဘယ်နှစ်မျိုးရှိသနည်းဟု မေးလာပါက Subnetting ၂ မျိုးရှိသည်ဟုပင်ဖြေရမည်ဖြစ်ပါသည်။ ၎င်း ၂ မျိုးမှာ -

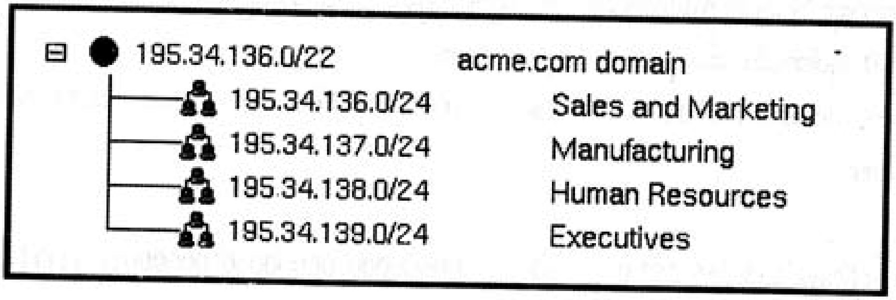
၁။ Static Length Subnetting နှင့်

၂။ Variable Length Subnetting တို့ဖြစ်ကြပါသည်။

❖ **Static Length Subnetting** ဆိုသည်မှာ

အားလုံးသော Subnetworks တွေဟာ Subnet Mask တစ်ခုကိုပဲ အသုံးပြုပြီး Network တစ်ခုအတွင်းမှာပဲရှိခဲ့ရင် ဒါကို Static Length Subnetting လို့ခေါ်ပါတယ်။ အခု သင်ခန်းစာအထိ ကျွန်တော်ရှင်းပြခဲ့တဲ့ Subnetting မှန်သမျှဟာ Static Lengtn Subnetting တွေပဲဖြစ်ကြပါတယ်။ အောက်မှာ Static Length Subnetting နှင့်ပတ်သက်ပြီးရှင်းပြထားတဲ့ ပုံတွေကို ဆက်လေ့လာကြည့်ရအောင်။

ပုံ ၃.၁၃



ဒီပုံမှာဆိုကြည့်လိုက် Network က 195.34.136.0/22 ဖြစ်ပါတယ်။ /22 ဆိုတာသိတယ်နော်။ အဲ့ဒါကို Host ဖက်ကနေ 2 bits ချေးလိုက်တော့ /24 ဖြစ်သွားတယ်။ 2 bits ဆိုတော့ $2^2 = 4$ ပေါ့။ ဒါကြောင့် အောက်မှာ Subnets 4 ခုကိုတွေ့ရလိမ့်မယ်။ /24 ဆိုတော့ 8 bits ကျန်တယ်။ $2^8 = 256$ ရပါတယ်။ Host ဆိုတော့ ၂ ခုတ်ပေးရတော့ ၂၅၄ ပဲကျန်ပါတော့တယ်။ ဒီတော့ 254 Hosts ရှိတဲ့ Subnets 4 ခု

ခဲ့တယ်ပေါ့။ ဒါအရင်ကတည်းကသိခဲ့ပြီးသား။ အဲ့ဒါကိုပဲ Static Length Subnetting လို့ခေါ်ပါတယ်။ ဒီ Static Length နှင့် Variable Length ကတွဲရှင်းပြမှ ပိုပြီးနားလည်မှာဖြစ်ပါတယ်။ ဒီတော့ Variable Length အကြောင်းရှင်းတဲ့ အခါ ပုံ နောက်တစ်ပုံနှင့်ထပ်ရှင်းပြပါဦးမယ်။ ခု ဘာဆက်ပြောပြမလဲဆိုတော့ Static Length Subnetting နှင့်ပတ်သက်တဲ့ အချက် (၂) ချက် ကိုဆက်ပြောပြပါဦးမယ်။

၁။ လွယ်ကူစွာသတ်မှတ်လို့ရခြင်း Easy to Configure ဖြစ်ပါတယ်။

၂။ RIP2 ဆိုတဲ့ Routing Information Protocol ဟာ Variable Length Subnetting ကို Support လုပ်သကဲ့သို့ Static Length Subnetting ကိုလည်း Support လုပ်ပါတယ်။ ဒါပေမယ့် RIP1 ကတော့ Static Length Subnetting ကို ပဲ Support လုပ်ပါတယ်။

❖ Variable Length Subnetting ဆိုသည်မှာ

မတူညီတဲ့ Subnet Masks တွေကိုအသုံးပြုထားတဲ့ Sub Networks တွေဟာအကယ်၍များ Network တစ်ခုတည်းမှာရှိနေခဲ့ရင် ဒါကို Variable Length Subnetting လို့ခေါ်ပါတယ်။ ပြန်ပြောပြမယ်နော်။

Network တစ်ခုတည်းမှာ ဘယ်လောက်ပဲ Subnets တွေရှိနေရှိနေ အဲ့ဒီ Subnets တွေဟာတူညီတဲ့ Subnet Masks တစ်ခုကိုပဲအသုံးပြုခဲ့ရင် ဒါကို Static Length Subnetting လို့ခေါ်ပါတယ်။

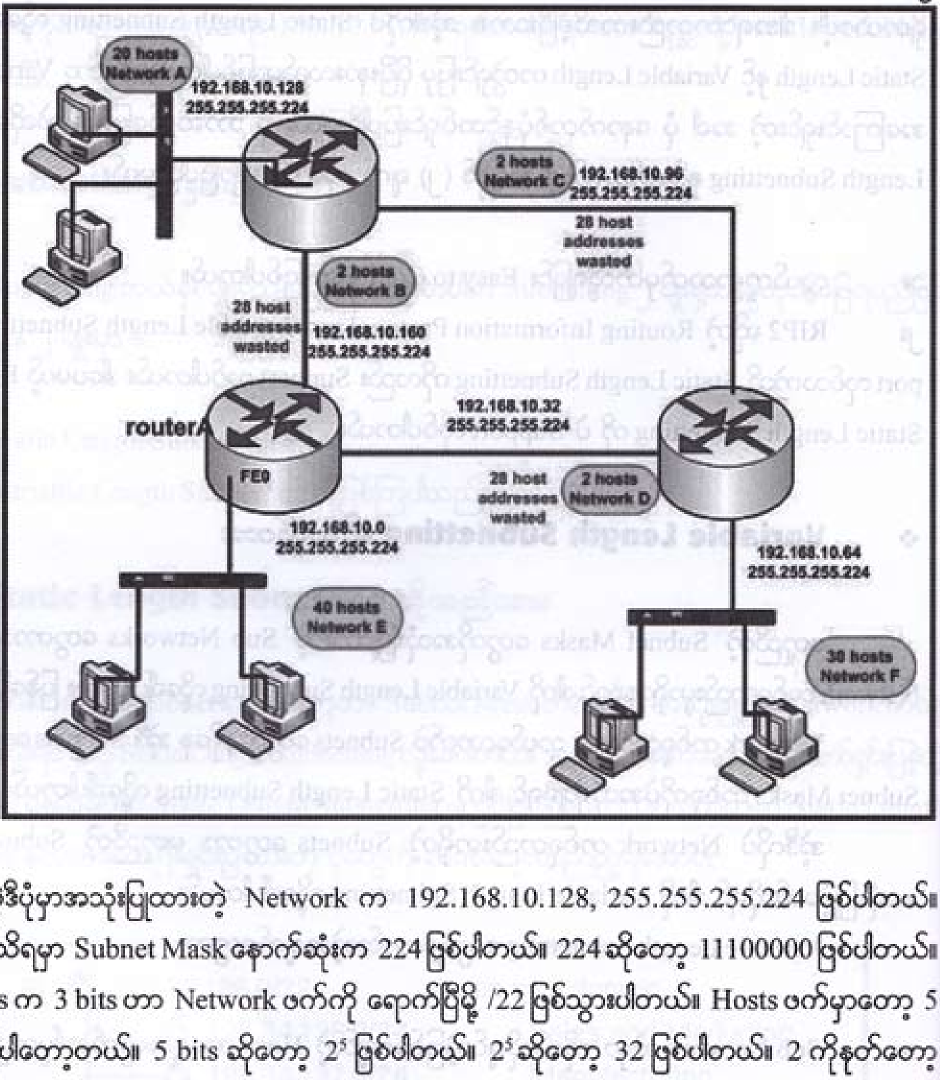
အဲ့ဒီလိုပဲ Network တစ်ခုတည်းမှာရှိတဲ့ Subnets တွေဟာ မတူညီတဲ့ Subnet Mask ကို အသုံးပြုခဲ့မယ်ဆိုရင် ဒါကို Variable Length Subnetting လို့ခေါ်ပါတယ်။

Variable Length Subnetting တွေရဲ့ကောင်းတဲ့အချက်တွေက -

၁။ Sub Network ထဲမှာ ကိုယ်လိုချင်တဲ့ဖြစ်စေချင်တဲ့ Hosts အရေအတွက်ပေါ်မူတည်ပြီး IP Address တွေကိုသတ်မှတ်နိုင်ပါတယ်။

၂။ နောက်တစ်ခုက IP Address တွေဟာ အလဟဿ ဆုံးရှုံးသွားခြင်းမျိုးမဖြစ်နိုင်ပါဘူး။ အောက်က ပုံကိုလေ့လာကြည့်ရအောင်။

ပုံ ၃.၁၄



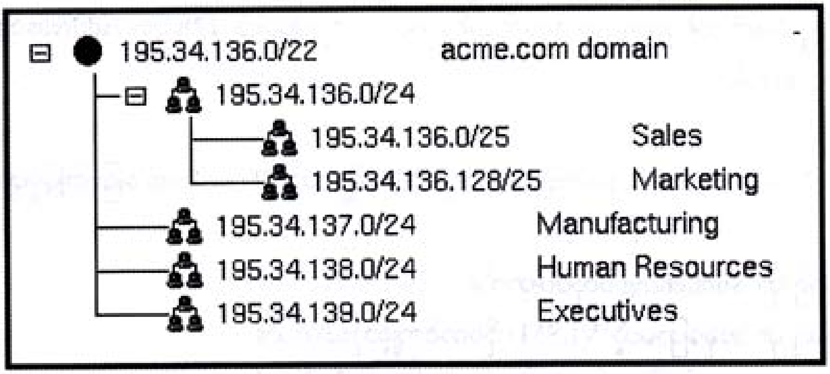
အဲဒီပုံမှာအသုံးပြုထားတဲ့ Network က 192.168.10.128, 255.255.255.224 ဖြစ်ပါတယ်။ ဒီနေရာမှာ သိရမှာ Subnet Mask နောက်ဆုံးက 224 ဖြစ်ပါတယ်။ 224 ဆိုတော့ 1110000 ဖြစ်ပါတယ်။ Host 8 bits က 3 bits ဟာ Network ဖက်ကို ရောက်ပြီးမို့ /22 ဖြစ်သွားပါတယ်။ Hosts ဖက်မှာတော့ 5 bits ပဲကျန်ပါတော့တယ်။ 5 bits ဆိုတော့ 2^5 ဖြစ်ပါတယ်။ 2^5 ဆိုတော့ 32 ဖြစ်ပါတယ်။ 2 ကိုနုတ်တော့ Hosts မှာ 30 ကျန်ပါတယ်။ ဒီတော့ Network မှာ Network A, B, C, D, E, F ဆိုပြီးရှိပါတယ်။ ပုံမှာပေါ့နော်။ ဒီ Network တစ်ခုချင်းစီမှာ Hosts 30 ဆီရတယ်။

❖ ဒါပေမယ့် Network B ကိုကြည့်လိုက် Hosts က ၂ ခုပဲလိုတာဖြစ်ပါတယ်။ ဒီတော့ Hosts ပေါင်း 28 ခုစာ Address တွေဟာ Waste ဖြစ်ကုန်ပါတယ်။ Network D မှာလည်းဒီအတိုင်းပဲဖြစ်ပါတယ်။

❖ Network E မှာကျတော့ လိုအပ်တဲ့ Hosts က 40 ဖြစ်ပါတယ်။ စသဖြင့်ပေါ့။ ဒီတော့ ဒီပုံက Static Length Subnetting ကိုရှင်းပြထားတာဖြစ်ပါတယ်။ သူဆိုလိုချင်တဲ့သဘော က Static Length

Subnetting ဟာ Hosts အရေအတွက် ကို တူညီစွာရတယ်။ ဒါကြောင့် ဒီ Network ကတော့ ဒီလောက် Hosts ပဲလိုချင်တယ် ဟို Network ကတော့ ဒီလောက် Host ပဲလိုချင်တယ် စသဖြင့် Network တစ်ခုနှင့် တစ်ခုဟာ Host အရေအတွက်မတူကြဘူး။ ဒီတော့ လိုအပ်ချက်နှင့် မကိုက်ညီဘူးပေါ့။ အောက်ကပုံတစ်ပုံကို ဆက်လေ့လာကြည့်ရအောင်။

ပုံ ၃.၁၅



ဒီပုံရဲ့ ဆိုလိုရင်းကိုရှင်းပြပါဦးမယ်။ မူရင်း Network က 195.34.136.0/22 ဖြစ်ပါတယ်။ ဒီရုံးရဲ့လိုအပ်ချက်က Subnets 5 ခုလိုအပ်ပါတယ်။ Subnets 5 ခုမှာ 3 ခုက 254 Hosts လိုအပ်တယ်ဆိုကြပါစို့။ ဒါပေမယ့် ၂ ခု ကတော့ 254 Hosts မလိုအပ်ပါဘူး 126 Hosts ပဲလိုအပ်ပါတယ်။

ဒီတော့ Hosts ဖက်က 2 bits ချေးပါတယ်။ 2^2 ဆိုတော့ 4 ပေါ့။ ဒီတော့ Network 4 ခုရပါတယ်။ Hosts က 8 bits ကျန်ပါတယ်။ 2^8 ပေါ့။ 2^8 က 256 ပါ။ 256 ကနေ ၂ ကိုနုတ်တော့ 254 ရပါတယ်။ ကောင်းပြီ၊ 195.34.136.0/24 ကိုထပ်ပြီးတော့ ပိုင်းလိုက်တာ ဒီတော့ 195.34.136.0/25 ဖြစ်သွားတယ်။ ဒီတော့ Hosts မှာ 2^7 ပဲရှိတော့တယ်။ 2^7=128-2 ပါ။ ဒီတော့ 195.34.136.0./24 ဆို Hosts က 256 ရမယ်။ အခုအဲ့ဒါကိုထပ်ခြမ်းခြမ်းလိုက်တော့ 128-2=126 Hosts ရှိတဲ့ Network ၂ခု ဖြစ်သွားပါတယ်။ ဒါကြောင့် Variable Length Subnetting ဟာ ကိုယ့်ရဲ့ လိုအပ်ချက်နှင့် ကိုက်ညီအောင် Subnets ကိုခွဲနိုင်တာ ဖြစ်ပါတယ်။

၃.၁၃ VLSM ပေါ်လာရခြင်းနှင့်အသုံးပြုရခြင်းအကြောင်း

၁။ နံပါတ် ၁ ကတော့ Addressing Crisis ပေါ့။ Address ကိုသုံးစွဲသူတွေဟာ များလာပြီး Address တွေကမလောက်ငတော့ဘူးဖြစ်နေတာပါ။

၂။ အသုံးမပြုရသေးသော IPv4 Class B Address တွေဟာလည်းကုန်လုနီးပါးဖြစ်နေခြင်း၊ Class C ကလည်းဘာမှရှိတာမဟုတ်ဘဲကိုး။

၃။ Internet Routing Tables ရဲ့ Size ကလျှင်မြန်စွာကြီးထွားလာခြင်းကလည်းတစ်ကြောင်း၊ ဒီအကြောင်းတွေကြောင့် VLSM ပေါ်ပေါက်လာရခြင်းနှင့် သူ့ကိုအသုံးပြုရခြင်းပဲဖြစ်ပါတယ်။ နောက်သူ့ကို သုံးရတဲ့ ရည်ရွယ်ချက်တစ်ခုကတော့ နောက်သင်ခန်းစာမှာ ပြောပြမယ့် 128 bits Address Space ရှိတဲ့ IPv6 အတွက်ပဲဖြစ်ပါတယ်။

❖ IPv4 Address ကုန်လုနီးပါးဖြစ်ခြင်းအတွက် အချို့သော Short Term ဖြေရှင်းပြမှုများ -

၁။ ၁၉၈၅ မှာ Subnetting စလုပ်ပါတယ်။
၂။ ၁၉၈၇ မှာ အခုပြောမယ့် VLSM ကိုစတင်ကျင့်သုံးပါတယ်။
၃။ ၁၉၉၃ မှာ နောက်ပြောမယ့် CIDR ကို စတင်ကျင့်သုံးပါတယ်။
၄။ နောက်တော့ Private IP Address
၅။ နောက်တော့ NAT ဆိုတဲ့ Network Address Translation တို့ပဲဖြစ်ပါတယ်။

ပုံ ၃.၁၆

အားလုံးကို တကယ်တမ်းဖြေလည်စေဖို့က IPv6 ပဲဖြစ်ပါတယ်။

ဒီတော့ကား VSLM ဆိုတာရှင်းပါတယ်။ နည်းနည်းလေးစဉ်းစားကြည့်ရအောင်။ တကယ့် Real World ပြင်ပလောကမှာ တူညီတဲ့ Hosts အရေအတွက်နဲ့ Subnets များရှိကြသည်ဆိုတာ ဖြစ်ဖို့ဘယ်လွယ်မလဲ။ ဆိုလိုတာက I mean, Subnet တွေဟာတစ်ခုနှင့်တစ်ခု တူညီတဲ့ အရေအတွက်ရှိချင်မှရှိမယ်။ ဒီလိုမရှိတာကိုက SLSM (Static) ပုံစံ တူညီတဲ့ Host အရေအတွက်နှင့် Subnet တွေပိုင်းလိုက်တော့ Address တွေ Waste ဆုံးရှုံးကုန်တာပေါ့။

၈.၁၄ VLSM ဥပမာပေးခြင်း

157.54.0.0/16 Address နှင့် ဥပမာပေးပြီးတွက်ပြပါ့မယ်။ အဲ့ဒီ အဖွဲ့အစည်းမှာပေါ့နော်။ 157.54.0.0/16 မူရင်း Address ရှိမယ်။ Class B ကြီးပေါ့။ ဒီတော့ သူက Host အရေအတွက်ထဲက တစ်ဝက်ကို နောက်သုံးဖို့ Reserve လုပ်ထားချင်တယ်။ ကဲအချက်နှင့်ပြောပြမယ်။ သူလုပ်ချင်တာက -

၁။ တစ်ဝက်ကို သိမ်းထားချင်တယ်။

၂။ ကျန်တစ်ဝက်ထဲကမှ အဲ့ဒီ အဖွဲ့အစည်းရဲ့ 15 Sites အတွက် 15 Address ပေးချင်တယ်။ ၎င်းမှာ Network တစ်ခုချင်းစီမှာ Hosts က 2000 လောက်စီရှိမယ်။

၃။ နောက်တော့ Subnets 8 ခုရှိမယ်။ အဲ့ဒီမှာ Host က 250 လောက်ရှိမယ်။ ဒီ (၃) ချက်ကိုပြေလည်အောင်တွက်ပြမယ်။

ကဲစပြီဗျို့-

၁။ 157.54.0.0/16 ကို Host ဘက်က 1 bit ယူလိုက်။ 157.54.0.0/17 ဖြစ်သွားလိမ့်မယ်။ /16 က Network က 16 bit လေ။ Host- 16 bit လေ။ Host 16 bits က 1 bit ကို Network ဘက်ပို့တော့ Network က /17 ဖြစ်သွားတာပေါ့။ 1 bit ပို့တော့ Subnet ဘယ်နှစ်ခုရမလဲ။ $2^1=2$ ပေါ့။ ဒီတော့ Subnet (၂) ခုထွက်လာပါတယ်။ ၎င်း Subnet (၂) ခုကတော့ -

157.54.0.0/17 နှင့် 157.54.128.0/17 ဖြစ်ပါတယ်။

ဒီတော့ သူက Address တစ်ဝက်ကို သိမ်းထားချင်တာဆိုတော့ 127.54.0.0/17 ကိုသိမ်းထားလိုက်ဗျာ။ 127.54.128.0/17 ကို သုံးဗျာ။

Subnet No	Address Prefix (Dot ပုံစံ)	Address Prefix (Prefix Length)
1 (ဖယ်ရန်)	157.54.0.0, 255.255.128.0	157.54.0.0/17
2 (သုံးရန်)	157.54.128.0, 255.255.128.0	157.54.128.0/17

Hosts က 1 bit Network ဖက်ကိုပို့တော့ Subnet mask က 255.255.0.0 or /16 အစား 255.255.128.0 or /17 ဖြစ်သွားတယ်နော်။ Host မှာကျန်တာက 15 bits ပေါ့။ ကဲ ဖြစ်စေချင်တာ ၃ ခုထဲက ၁ ခုတော့ပြီးသွားပြီ။

၂။ Network တစ်ခုမှာ 2000 Hosts ပါဝင်တဲ့ Address ပေါင်း 15 ခုလိုချင်တာကို။ ဒီတော့ အပေါ်က (၂) ပိုင်းပိုင်းထားတဲ့ Network နှစ်ခုထဲက 157.54.0.0/17 ကိုသိမ်းထားတာကြောင့် 127.54.128.0/17 ကို တစ်ခါထပ်ပိုင်းမယ်။ ဘယ်လောက်ပိုင်းမလဲ။ 4 bits စာပိုင်းမယ်။ Host ကနေ 4 bits ယူလိုက်။ ဒီတော့ /17 ကနေ /21 ဖြစ်သွားလိမ့်မယ်။

❖ 4 bits မယူခင် –

157.54.128.0 ,	255.	255.	128.	0
	11111111	11111111	1000000	00000000

❖ 4 bits ယူပြီး –

157.54.128.0 ,	255.	255.	248.	0
	11111111	11111111	11111000	00000000

ဒီလို 4 bits ကို Host ဖက်ကနေ Network ဖက်ကိုယူလိုက်တာကြောင့် Network မှာ တိုးသွားသလို Hosts မှာ 4 bits လျော့သွားပါတယ်။ $2^4 = 16$ ဖြစ်ပါတယ်။ ဒါကြောင့် –

မူလက – 157.54.0.0/16
ဒါကိုနှစ်ပိုင်းခွဲလိုက်တော့ –157.54.0.0/17 နှင့်
–157.54.128.0/17 ဆိုပြီးဖြစ်လာတယ်။

–157.54.128.0/17 ကို 4 bits ခွဲလိုက်တော့
157.54.128.0/21 ဆိုပြီး Network ၁၆ ခုထပ်ကွဲသွားတယ်။

၄င်းတို့က တော့–

Subnet Number	Address Prefix (Dotted Decimal)	Address Prefix (Prefix Length)
1	157.54.128.0, 255.255.248.0	157.54.128.0/21
2	157.54.136.0, 255.255.248.0	157.54.136.0/21
3	157.54.144.0, 255.255.248.0	157.54.144.0/21
4	157.54.152.0, 255.255.248.0	157.54.152.0/21
5	157.54.160.0, 255.255.248.0	157.54.160.0/21
6	157.54.168.0, 255.255.248.0	157.54.168.0/21
7	157.54.176.0, 255.255.248.0	157.54.176.0/21
8	157.54.184.0, 255.255.248.0	157.54.184.0/21
9	157.54.192.0, 255.255.248.0	157.54.192.0/21
10	157.54.200.0, 255.255.248.0	157.54.200.0/21
11	157.54.208.0, 255.255.248.0	157.54.208.0/21
12	157.54.216.0, 255.255.248.0	157.54.216.0/21
13	157.54.224.0, 255.255.248.0	157.54.224.0/21
14	157.54.232.0, 255.255.248.0	157.54.232.0/21
15	157.54.240.0, 255.255.248.0	157.54.240.0/21
16	157.54.248.0, 255.255.248.0	157.54.248.0/21

4 bits ကို Network ဖက်ကိုပို့လိုက်တော့ Host မှာ 11 bits ပဲကျန်တော့တယ်။ ကနဦး 1 bits ဦး Network ကို ၂ ပိုင်း-ပိုင်းတယ်။ တစ်ပိုင်းကို သိမ်းထားပြီး။ တစ်ပိုင်းကို 4 bits ပို့ကာ 16 ပိုင်းထပ်ပိုင်းတယ်။ ဒီတော့ မူလက 16 bits ရှိတာ 1 bit တစ်ခါ၊ 4 bits တစ်ခါနုတ်တော့ 16 bits ကနေ 11 bits ပဲကျန်တယ်။ 2^{11} တာ ဒီ Network 16 ခုရဲ့ တစ်ခုချင်းစီမှာရှိတဲ့ Hosts အရေအတွက်ဖြစ်လာတယ်။ 2^{11}=2048 ဖြစ်ပါတယ်။ 2048 ထဲက 2 နုတ်တော့ 2046 ရပါတယ်။ ဒီတော့ 2046 Hosts အရေအတွက်ရှိတဲ့ Network 16 ခုကို ရရှိပြီ ဖြစ်တဲ့အတွက် ဒုတိယအချက်လည်းပြီးဆုံးပြီဖြစ်ပါတယ်။

၃။ နံပါတ် ၂ အချက်မှာ သူလိုချင်တာက Network 15 ခုတည်းပါ။ အခုဟာက 16 ခုဖြစ်နေတယ်။ ဟုတ်ပါတယ်။ ပိုနေတဲ့ 2046 Hosts ရှိတဲ့ Network တစ်ခုကနေ ဒီနံပါတ် (၃) အချက်ဖြစ်တဲ့ 250 Host ရှိကြကုန်သော နောက်ထပ် Network ၈ ခုကိုလိုချင်တာဖြစ်ပါတယ်။

ဒီတော့ကား ခုနက ခွဲထားတဲ့ Network 16 ခုထဲက 15 ခုကိုသုံးပြီး နောက်ဆုံးတစ်ခုဖြစ်တဲ့ 157.54.248.0/21 ကိုထပ်ပြီးပိုင်းပါ့မယ်။ ဒီတစ်ခါ 3 bits ပိုင်းပါမယ်။

❖ 3 bits မယူမီ –

157.54.248.0,	255.	255.	248.	0
	11111111	11111111	11111000	00000000

❖ 3 bits ယူပြီး –

157.54.248.0,	255.	255.	255.	0
	11111111	11111111	11111111	00000000

ဒီတော့ကား Host ဖက်ကနေ Network ဖက်ကို 3 bits ချေးလိုက်တာကြောင့် Network မှာ 3 bits တိုးသွားသလို Hosts မှာလည်း 3 bits လျော့သွားပါတယ်။ Network ကိုချေးလိုက်တဲ့ 3 bits ဟာ 2^3 ဖြစ်တာကြောင့် 2^3=8 ဖြစ်ကာ Network 8 ခုထွက်လာပါတယ်။ Hosts မှာကျတော့ စောနတုန်းက အဲ့လေ ခုနတုန်းက 11 bits ကနေ 3 bits ပေးလိုက်တော့ 8 bits ပဲကျန်ပါတယ်။ ၎င်း 8 bits သည် 2^8 =256-2 =254 Hosts ဖြစ်ပါတယ်။ ဒါကြောင့် Network တစ်ခုမှာ Hosts ပေါင်း 254 ခုစီရှိတဲ့ Network 8 ခုကို ထပ်မံရရှိပါတယ်။ ၎င်း Network (၈) ခု ကို တစ်ဖက်ပါဇယားမှာဖော်ပြပေးထားပါတယ်။

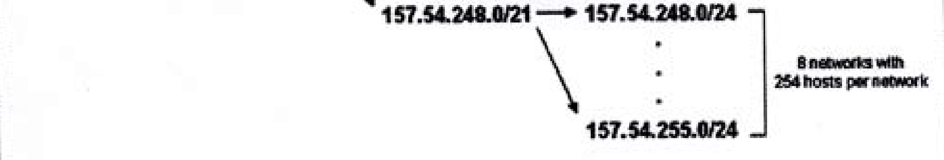
၃. ၁၅ VLSM နိဒိုးချုပ်ရှင်းပြခြင်း

ဒီတော့ကား ဒီ Network တွေဟာ ဆင့်ကဲဆင့်ကဲ လိုအပ်ချက်တွေအရခွဲထုတ်သွားတယ်။ ဒါကြောင့် Subnet Mask တွေလည်းမတူတော့တဲ့ Subnet တွေအများကြီးဖြစ်လာတယ်ဟုတ်လား။ Subnet Mask ကမူလက /16 တနည်းအားဖြင့် 255.255.0.0 နောက်တော့ /17 ဖြစ်လာတယ်။ တနည်းအားဖြင့် 255.255.128.0 ဖြစ်လာတယ်။ အဲ့ဒါကို ထပ်ခွဲတော့ /21 ဖြစ်တယ်။ တနည်းအားဖြင့် 255.255.248.0 အဲ့ဒါကို တစ်ခါထပ်ခွဲပြန်တော့ /24 ဖြစ်လာတယ်။ တနည်းအားဖြင့် 255.255.255.0 ပေါ့။ ဒီတော့ Subnet

Subnet Number	Subnet Prefix (Dotted Decimal)	Subnet Prefix (Prefix length)
1	157.54.248.0, 255.255.255.0	157.54.248.0/24
2	157.54.249.0, 255.255.255.0	157.54.249.0/24
3	157.54.250.0, 255.255.255.0	157.54.250.0/24
4	157.54.251.0, 255.255.255.0	157.54.251.0/24
5	157.54.252.0, 255.255.255.0	157.54.252.0/24
6	157.54.253.0, 255.255.255.0	157.54.253.0/24
7	157.54.254.0, 255.255.255.0	157.54.254.0/24
8	157.54.255.0, 255.255.255.0	157.54.255.0/24

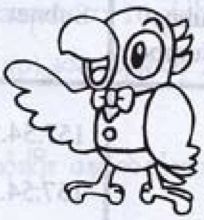
တွေအများကြီး။ Mask တွေလည်းမတူဘူး။ ဒါပေမယ့် ကွန်ယက်တစ်ခုအောက်မှာပဲ ခွဲခြမ်းပြီးထွက်သွားတာ။ Subnet မှာရှိတဲ့ Hosts တွေရဲ့ အရေအတွက်ကလည်း တစ်ခုနှင့်တစ်ခုမတူဘူး။ အရွယ်တွေက ကြီးရာက နေတဖြည်းဖြည်းသေးသွားတယ်။ ဒီလို Subnet Mask မတူတဲ့ Subnet တွေဟာ Network တစ်ခုတည်းမှာ ရှိနေတာကိုပဲ Variable Length Subnetting လို့ခေါ်တာဖြစ်ပါတယ်။ ဒါကိုပုံနှင့်တကွရှင်းပြထားပါတယ်။

ပုံ ၃.၁၇



ကွန်ရက်တစ်ခုမှာ အရေအတွက်မတူညီတဲ့ Host တွေရှိနိုင်တဲ့ Variable Length Subnetting ကိုတွေ့ရစဉ်

ပုံ ၃.၁၇

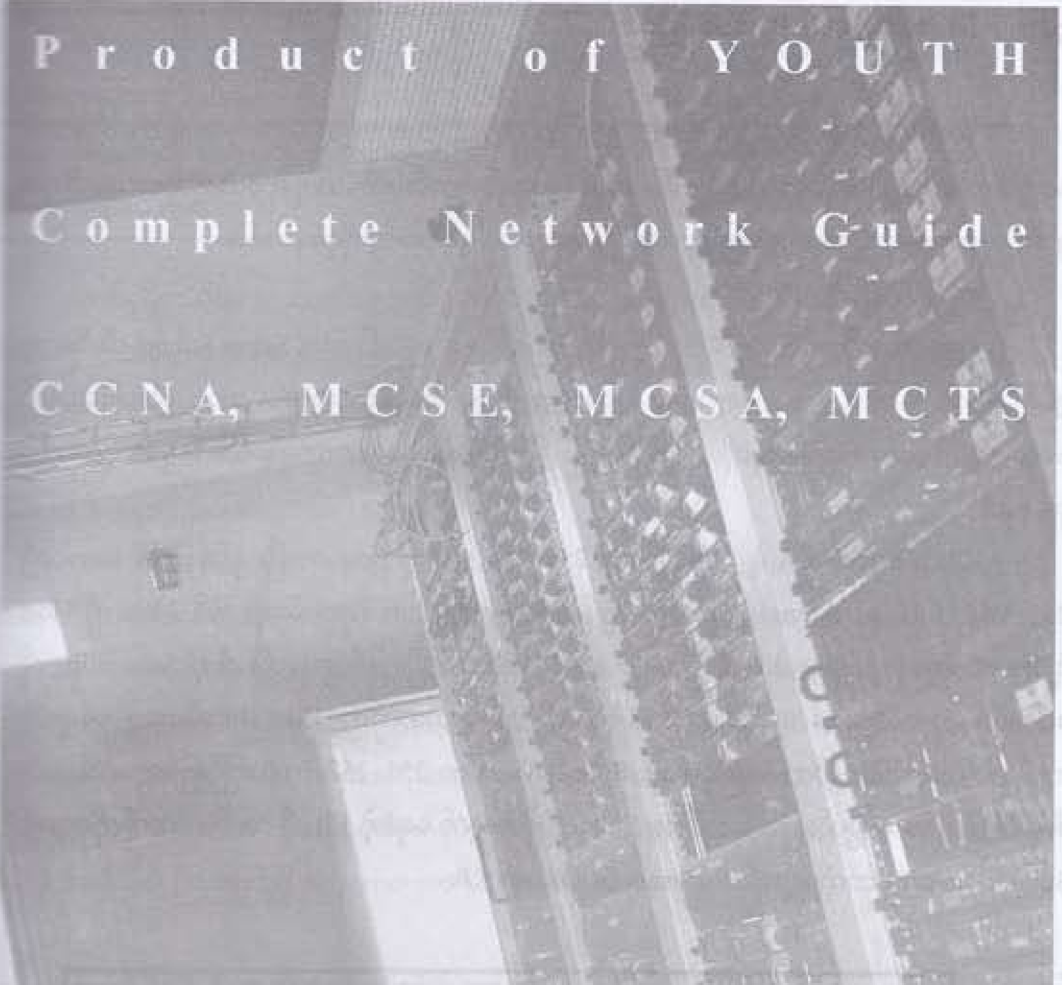


နောက်သင်ရမည့် သင်ခန်းစာကျရင်လည်းသိလာဦးမှာပါ။ အခုထဲ က ပြောရရင် Routing မှာ ဒီ VLSM ကို IP Version 1 ဖြစ်တဲ့ RIP1 (Routing Information Protocol) ဟာ Support မလုပ်နိုင်ပါဘူး။ ဒီ VLSM ကို Support လုပ်တဲ့ သူတွေကတော့ -

၁။ IP Version 2 အတွက် RIP ပါ။ (RIP 2) လို့လည်းခေါ်ကြတယ်။

၂။ OSPF ဆိုတဲ့ Open Shortest Path First နှင့်

၃။ BGP V4 ဆိုတဲ့ Border Gateway Protocol Version 4 တို့ပဲဖြစ်ကြပါတယ်။



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 4

Supernetting or CIDR

၄.၁ Supermetting အကြောင်း

ဒီတစ်ခါ လာပြန်ပဟေ့– Subnetting တောင်မဟုတ်တော့ဘူး။ ဘာတဲ့ Supernetting တဲ့။ ကျွန်တော်တော့ ဒီစာအုပ် ရေးပြီးရင် ဘယ်မှာသွားပြီး အပန်းဖြေရရင်ကောင်းမလဲမသိဘူး။ ဖတ်တဲ့သူတော့မသိဘူး။ ရှင်းတဲ့သူက နားလည်အောင်ရှင်းပြဖို့ ခေါင်းစဉ်ခွဲတာကအစ ခေါင်းတွေကိုပူနေတာပဲ။

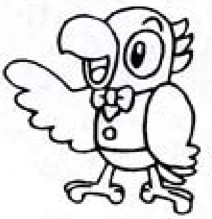
ကဲ . . . စပြီဗျာ . . .

ကျွန်တော်တို့ဟာ Subnetting ကို ရှင်းပြခဲ့ပြီးပါပြီ။ အခုရှင်းပြမှာက Super Subnet ပါ။ ဒီတော့ ရှင်းပြခဲ့ပြီးတဲ့ Subnet နဲ့ Supernetting နဲ့ ဘာကွာသလဲ။ ဒါအရေးကြီးတယ်။ ဘာမှ ရှင်းမပြသေးခင် Subnet နဲ့ Supernet ကွာခြားပုံကို၊ " မြန်းကနဲ " မြင်လိုက်ရင် သင်အားတက်မယ်။ မဟုတ်လို့ကတော့ မူးနေမှာ။

Class B Network ရဲ့ Mask ဖြစ်တဲ့ 255. 255. 0.0 ကို ဥပမာပေးပြီး ရှင်းပြမယ်။ အကယ်၍ 255 . 255 . 0 . 0 မှာ Subnet ခွဲဖို့အတွက် ကျွန်တော်တို့ဟာ 2 bits ချေးမယ်ပေါ့။ အဲဒီ 2 bits ကို Host ရဲ့ Bit က ချေးရင် Subnet Mask ဟာ 255 . 255. 192. 0 ဆိုပြီး ဖြစ်သွားမယ်။ ဒါကို Subnetting လို့ ခေါ်တယ်။ အကယ်၍များ သင်ဟာ အဲဒီ 2 bits ကို လက်ယာဘက်က Host Bit ဆီကနေ မချေးပဲနဲ့ ဘယ်ဘက် Network ဆီက ချေးလိုက်ရင် Subnet Mask က 255. 252. 0 . 0 ဆိုပြီးဖြစ်သွားလိမ့်မယ်။ ဒါဆို Subnet ပဲ။ အလွယ်ပြောရင် သင်ဟာ Subnet ခွဲဖို့အတွက် ချေးတဲ့ Bit ကို လက်ယာဘက်ကိုချေးရင် Subnet ပဲ။ လက်ဝဲဘက်ချေးရင် Supernet ပဲ။ Ok နော် Ok .

ပုံ ၄.၁

ဘယ်ဘက်ကစူးစူး၊ ညာဖက်က စူးစူး အဲ ယောင်လို့နော်
ဘယ်ဘက်ကချေးရင် Supernet နော်
ညာဘက်ကချေးရင် Subnet နော်
ဒါပဲနော် ရှုပ်နေတာပဲလို့ ပြောရဘူး။



Class B:	255.	255.	0.	0
Subnet Mask:	11111111	111111111	00000000	00000000
	16 Bit Network		Host 16 Bit	

2 bits Borrow ကို လက်ယာဘက် Host မှ 2 bits ငှားခြင်းက Subnet	11111111. 11111111. 1100000. 00000000 255. 255. 192. 0
2 bits Borrow ကို လက်ဝဲဘက် Network ပိုင်းမှ ငှားခြင်းက Supernet	11111111. 11111100 . 00000000 . 00000000 255. 252. 0. 0

တစ်ခုရှိတယ်ဗျ။ (တစ်ဝက်လောက်ပေးပါ)။ ဟာ . . အရေးထဲ။ ကျွန်တော်တို့တွေက IP Address တို့ Subnet Mask တို့ပေးတဲ့နေရာမှာ၊ ဘယ်မှာပဲ ကြည့်လိုက်ကြည့်လိုက် Subnet Mask ဆိုတာကိုပဲ တွေ့ရမယ်။ Supernet Mask ဆိုပြီး တွေ့ရမှာ မဟုတ်ဘူး။ ဒီတော့ Supernet Mask ဆိုတာ အခေါ်အဝေါ် တစ်ခုပဲ။ လက်ယာဘက်က ချေးရင် Subnet။ လက်ဝဲဘက်ကချေးရင် Supernet ။ ပြောချင်တာက Supernet ပဲဖြစ်ဖြစ် Subnet ပဲဖြစ်ဖြစ် Subnet Mask ပဲ။

ကောင်းပြီ။ Supernetting ကို Classless Inter- Domain Routing (CIDR)- (အသံထွက် စိုက်ဒါး) ဆိုပြီး ခေါ်သေးတယ်ဗျ။ ရှေ့မှာ ရှင်းပြခဲ့ပြီးသား။ Classful နှင့် Classless ဆိုတာလေ။ Classful မဟုတ်ရင် Classless ပဲ။ Classless ဆိုတာ Class မရှိဘူးပေါ့ဗျာ။ IP Address ရဲ့ ရှေ့ဆုံး Octet ကို ကြည့်လိုက်ရင် Class B ဆိုပါစို့။ သူ့ရဲ့ Subnet ကိုကြည့်လိုက်ရင် Class B ပုံစံ မဟုတ်ပြန်ဘူး။ အဲဒီ Classless ပဲ။ ဒီတော့ CIDR ဆိုတာ Classful မဟုတ်တဲ့ Subnet ခွဲခြင်းပဲ။ တကယ်တမ်းပြောရရင် CIDR ဆိုတာ အယူအဆ အခေါ်အဝေါ်တစ်ခုပဲ။ ၎င်းဟာ Subnet အမှမဟုတ်၊ Supernet လုပ်ခြင်းပဲ။ အဲပေမဲ့ ဘယ်မှာပဲ ကြည့်ကြည့် Supernet ဟာ CIDR ပဲလို့ ပြောလေ့ရှိတယ်။

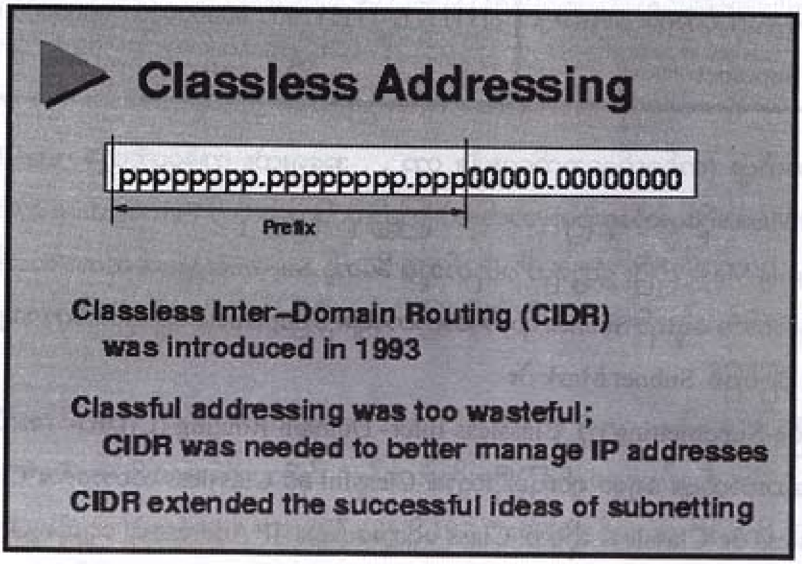
၄.၂ ဘာဖြစ်လို့ Supernet ကိုသုံးရတာလဲ

ဘာဖြစ်လို့လည်းဆိုတော့ Supernet က 32 bits IP Address တွေကို ချဲ့ထွင်တာပဲ ဖြစ်တယ်။ ၎င်း Supernet ကို 1993 မှာတီထွင်ခဲ့ကြတယ်။ ဘာလို့လဲ။ အင်တာနက်အသုံးပြုမှုတွေက အရမ်းများလာတယ်။ ဒီတော့ IP Address တွေက မလောက်တော့ဘူး။ Classful Address လို့ပြောတာ။ ဒီ Classful Address အတိုင်းသာသုံးမယ်ဆိုရင် Address တွေ ဆုံးရှုံးမှုအရမ်းများတယ်။ IP Address တွေကလည်း မလောက် တော့ဘူး။ ဒီအချိန်မှာ CIDR ဆိုတဲ့ Supernet ဆိုတာ ပေါ်လာတာပဲ။

တနည်းအားဖြင့် သင်ဟာ Network တစ်ခုတည်းမှာပဲ Host တွေ အများကြီးလိုချင်တယ်။ နောက်ပြီး လက်ရှိကလည်း Classful Configuration ထဲမှာဖြစ်နေတယ်ဆိုရင် Supernet ကိုအသုံးပြုဖို့လိုလာ

ဖြစ်တယ်။

ပုံ ၄.၂



ဥပမာပေးပြီးပြောပြမယ်။ Class C Address ဆိုရင် 192. 0. 0 . 0 ကနေ 223 . 255. 255 .255 ဆိုပြီး Address တွေရှိမယ်။ အဲဒီအထဲကမှ Class C Block တစ်ခုဖြစ်တဲ့ 192. 168. 1. 0 ကို ကြည့်လိုက်။ Address တွေဟာ 192. 168.1.0 ကနေ 192.168.1.255 အထိရလိမ့်မယ်။ ဒီတော့ အထဲမှာ Address ပေါင်း 254 ခုရှိလိမ့်မယ်။ ဆိုလိုတာက ဒီ Network တစ်ခုတည်းမှာပဲ ကိုယ်က Address ပေါင်း 254 မကလိုချင်ပြီဆိုရင်တော့ သင်ဟာ Supernet ကို ပြုလုပ်ဖို့လိုလာပြီ ဖြစ်ပါတယ်။ အဲဒီလို Host Address တွေ အများကြီးလိုချင်လာတဲ့အခါ Supernet ကို ပြုလုပ်ဖို့ Bits တွေငှားတဲ့အခါ Network Portion က ငှားရတာ ဖြစ်ပါတယ်။

Supernet နဲ့ ပတ်သက်ပြီး ပြောပြချင်သေးတာတွေက Internet စကားနဲ့ ပြောရင် Supernet ဆိုတာ Network တစ်ခုတည်းမှာ Subnetwork Address တွေတရစ်စပ်တည်းဖြစ်ပေါ်နေတာပါပဲ။ ဒီတော့ IP Address တွေဟာ Block တစ်ခုနှင့်တစ်ခုကြားလွတ်သွားတဲ့ IP Address မရှိတော့ပဲ တရစပ်ဖြစ်သွားတာပါ။ ဆိုတော့ကား များပြားလှတဲ့ Network Address တွေကို ကြီးမားတဲ့ ကွန်ရက်ကြီးတစ်ခုဖြစ်အောင် ပြုလုပ်ခြင်းဖြစ်ပါတယ်။ ဒီတော့ကောင်းတာက Single Network ဖြစ်သွားခြင်းကြောင့် Routing Table ကိုဖြတ်ရတဲ့ Entries တွေလျော့သွားတာပေါ့။ ဆိုလိုတာက Routing လမ်းကြောင်းများ ပေါင်းစည်းခြင်းကြောင့် Internet Routing Table မှာဖြတ်ရတဲ့ Routing နှင့်ပတ်သက်တဲ့ Entries တွေလျှော့ချပစ်နိုင်ခြင်းကြောင့်

Performance လည်းပိုကောင်းလာပါတယ်။

ဘယ်လောက်ပဲရှင်းပြရှင်းပြ သည်းအူပြောင်းပြန်၊ အူလည်ချာလည်ဖြစ်နေမှာပဲ ဆိုတာသိနေတာမို့ နောက်တစ်နည်းနှင့်ရှင်းပြပါဦးမယ်။ Supernet ဆိုတာ IPv6 မပေါ်ခင်အချိန်အထိ IPv4 32 bits Address ကို သက်တမ်းရှည်အောင် လုပ်ပေးတာဖြစ်ပါတယ်။ Internet Class ရဲ့ Class B ကလည်းကုန်တော့မယ်။ Class C မှာကလည်း Address တွေက ဒီလောက်အများကြီးရှိတာကမဟုတ်။ ဒီအချိန်မှာ Supernet က ခေါ်ပေါက်လာရတာပဲ။ ဒီတော့ Supernet အကြောင်းရှင်းပြရင် Class C နှင့်ပဲ ရှင်းပြလေ့ရှိတယ်။ ဒီတော့ Supernet ပေါ်လာရခြင်းအကြောင်းတွေကတော့ -

၁။ Class B Network Address Space များ ကုန်ခါနီးလာခြင်း။

၂။ Class C Network မှာကလည်း Address Space အနည်းငယ်ပဲရှိခြင်း။

၃။ Internet Routors တွေထဲမှာရှိတဲ့ Routing Table တွေဟာ Software ကပဲဖြစ်စေ၊ လူကပဲဖြစ်စေ ထိန်းချုပ်နိုင်တဲ့ အင်အားထက်ပို၍ ကြီးထွားလာခြင်း။

၄။ IPv4 ရဲ့ 32 bits Address တွေက ကုန်ခါနီးလာပြီ။ IPv6 မပေါ်ခင် 32 bits Address ကို သက်တမ်းပိုဆက်စေလိုခြင်းတို့ကြောင့်ပဲဖြစ်ပါတယ်။

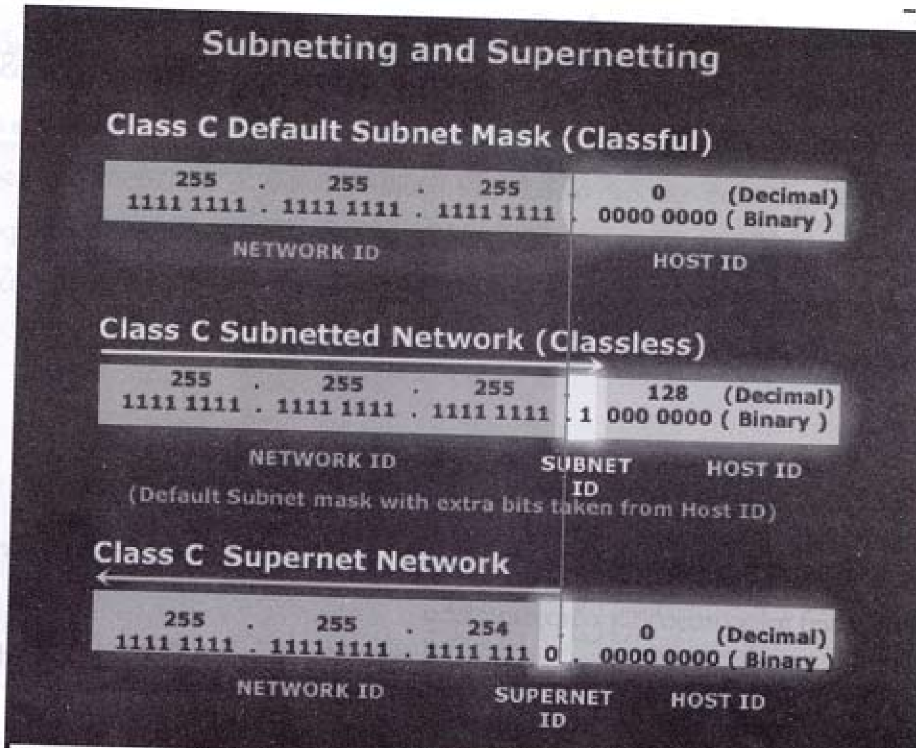
၄.၃ Supernet အသေးစိတ်

Supernet ဆိုတာ Class C Network တွေကို အပိုင်းပိုင်းခြင်းမဟုတ်ပဲ ပေါင်းစည်းခြင်းဖြစ်တာကြောင့် Supernet ဟာ Subnet နှင့် ပြောင်းပြန်ဖြစ်ပါတယ်။ ပြန်ပြောပြမယ်။

Subnet ဆိုတာ Network တွေကိုအပိုင်းလိုက် အပိုင်းလိုက်ခွဲထုတ်ပစ်တာ။ ဘာလို့လဲ။ ဥပမာ Class B Network တစ်ခုမှာ Host ပေါင်း 65536 - 2 = 65334 ရှိတယ်။ ဒီတော့ ဒီလောက်ကြီးတဲ့ Network ကိုအလိုမရှိဘူး။ Host တွေလျှော့လိုက်ပြီး ကွန်ရက်ငယ်တွေ တိုးပွားလာအောင် Network အကြီးကြီးကို Network ငယ်တွေအဖြစ် အပိုင်းပိုင်းလုပ်ပစ်လိုက်တာ Subnet ပဲဖြစ်ပါတယ်။

Supernet ဟာ Subnets နှင့်ပြောင်းပြန်။ Class C မှာကြည့်လိုက်။ Class C Network တစ်ခုမှာ Host က 254 ပဲရှိတယ်။ ဒီတော့ Class C Network တစ်ခုမှာ 254 Host ထက်ပိုလိုချင်လာရင် 254 Host ရှိတဲ့ Class C နှစ်ခုကိုပေါင်းလိုက်။ ဒါဆို 512 Host ရှိတဲ့ Class C Network တစ်ခုကိုရရှိတယ်။ တနည်းအားဖြင့် 284 Host ရှိတဲ့ Class C Network နှစ်ခုကိုပေါင်းပစ်လိုက်တာ Supernet ပဲ။ ဒါကြောင့် အချုပ်ပြောရရင် -

ပုံ ၄.၃



အထက်ပါပုံဟာ Classful Network, Classless Subnet နှင့် Classless Supernet တို့ကို bits များ ခွဲခြမ်းခြင်းပြထားတဲ့ပုံဖြစ်ပါတယ်။ Subnetting ဆိုရင် bits ကို ညာဖက် Host က ယူတာပါ။ Supernet ဆိုရင် Bits ကို ဘယ်ဘက်က Network ပိုင်းကယူတာပါ။

Class C မှာပဲကြည့်။ 254 Host ရတယ်။ Class C Network တစ်ခုမှာ အဲ့ဒါကို Subnet ပိုင်းရင် Host တွေနည်းသွားပြီး Network တွေများလာတယ်။

အကယ်၍ Subnet မဟုတ်ပဲ Supernet ဆိုရင် Network တွေနည်းသွားပြီး၊ Host တွေများလာတယ်။ ဟုတ်ပြီနော်။ ဒီလောက်ဆို Supernet ကိုနားလည်လောက်ပြီလို့ထင်တယ်။ ကျွန်တော့်အတွက်ကတော့ တရှင်းပြရတာပျော်စရာပါပဲ။ အမေ့အဖွားတွေကလည်း ဆရာမတွေ၊ အမေကလည်းဆရာမ၊ အဖေ့အဖေကလည်း ဆရာ၊ အဖေ့ ညီ၊ ညီမတွေကလည်း ဆရာ၊ ဆရာမ၊ ဆရာ၊ ဆရာမ မဟုတ်တဲ့ အဒေါ်တွေကလည်း ဆရာတွေနှင့် အိမ်ထောင်ကျ။ ဒီကြားထဲ အစ်ကိုအကြီးဆုံးက အရင်က အင်္ဂလိပ်ဆရာ။ ဒီတော့ကျွန်တော်မျိုးကြီး မောင်ဇော်လင်းက ဘယ်လောက်ပဲ သင်တန်းသားတွေကို တရှင်းပြရ၊ ရှင်းပြရ မောသွားတယ်ဆိုတာမရှိဘူး။

သူတို့ကိုဘယ်လိုသိပြပေးရမလဲ။ ဘယ်လိုပြောရင်နားလည်မလဲ ဆိုတာကိုလည်း ကျွန်တော်ကောင်းကောင်း သိတယ်။

Supernet ပြုလုပ်တဲ့အခါမှာ လိုက်နာရမည့် စည်းကမ်းချက် (3) ခုရှိတယ်ဗျ။ သေချာဖတ်နော်။ လေကျယ်တာမဟုတ်ဘူး။ ဒီအကြောင်းကို နားလည်ရင် CCNA စာမေးပွဲအတွက် အထောက်အကူဖြစ်မယ်။ ဒီအကြောင်းက Network Engineer ဖြစ်တဲ့သူတိုင်းလည်းမသိသလို Certified ဖြစ်တဲ့သူတိုင်းလည်းမသိဘူး။ တဲ အဲ့ဒီ ဥပဒေသ (၃) ခုကတော့ -

၁။ Numeric Contiguity

၂။ Even Divisibility

၃။ Single Interface စသဖြင့် စည်းကမ်းချက် ဥပဒေသ (၃) ခုရှိပါတယ်။ Supernet ကိုလုပ်ဖို့ရာ ဥပဒေ ၃ ချက် ကို အခုတစ်ခုချင်း ရှင်းပြပါ့မယ်။

၄.၄ **Numeric Contiguity**

Supernet ဆိုတာ ပေါင်းစည်းတာ။ ဒီလိုပေါင်းစည်းဖို့ Network Address တွေဟာ တစ်စပ်တည်း ဖြစ်ဖို့လိုအပ်ပါတယ်။ ဒီ ဥပဒေ ၃ ခုမှာ ဒီအချက်က ဘယ်လိုပြောရမလဲ အရေးကြီးတယ်ပေါ့။ အဲ့လိုဆိုတာထက် အခြားအချက်တွေထက်ပို Sensitive ဖြစ်တယ်ပေါ့ဗျာ။ သူဆိုလိုချင်တာက Network နှစ်ခုကို ပေါင်းမယ်ဆို အဲ့ဒီပေါင်းမယ့် Network နှစ်ခုက Adjacent ပေါ့။ ကပ်လျက်ဖြစ်နေရမယ်။ ကပ်လျက်မဟုတ်တဲ့ Network တွေကို ပေါင်းမယ်ဆိုကြားထဲက Network တွေပါပေါင်းပစ်မှရမယ်။ ဒါဆို Network ကပိုတော့ ကြီးသွားမှာပေါ့။ တစ်ဖက်က ဇယားကိုကြည့်လိုက်ပါ။

အဲဒီဇယားမှာ /24 ဆိုတဲ့ Network က Class C Network လေ။ အဲဒါကို /24 ကနေ /27 လုပ်လိုက်တော့ 3 bits Subnet ဖြစ်သွားတာပေါ့။ ဒါကြောင့် /24 က Base ဖြစ်တယ်။ /27 က Subnet ခွဲထုတ်လိုက်တာ။ 32 bits ဆိုတော့ $2^3 = 8$ ပေါ့။ Subnet 8 ခုရပါတယ်။ Subnet 0 ကနေ 7 အထိဆိုပြီး ပြထားပါတယ်။

- Subnet 0 ဟာ Subnet 1 နှင့် တရစ်စပ်တည်းဖြစ်ပါတယ်။ Subnet 1 ကျတော့ Subnet 0 နှင့် 2 အကြားရှိတာကြောင့် 0 နှင့် 2 နှင့်ပါတစ်ရစပ်တည်းဖြစ်ပါတယ်။ ကဲဒီတော့ Subnet 1 နှင့် 3 ကိုပေါင်းချင်တယ်ဆို တနည်းအားဖြင့် Supernet လုပ်ချင်တယ်ဆိုလုပ်လို့ မရဘူး။ ဘာဖြစ်လို့လဲ။ ကြားထဲမှာ Subnet 2 ကြီးရှိနေလို့ပါ။ ကပ်လျက်ပဲပေါင်းလို့ရမယ်ဆိုတာ ဒါကိုပြောတာ။

Subnet Number	Decimal Address	Contiguous With Which Numbers
Base	192.168.64.0/24	Not applicable
Subnet 0	192.168.64.0/27	1
Subnet 1	192.168.64.32/27	0 and 2
Subnet 2	192.168.64.64/27	1 and 3
Subnet 3	192.168.64.96/27	2 and 4
Subnet 4	192.168.64.128/27	3 and 5
Subnet 5	192.168.64.160/27	4 and 6
Subnet 6	192.168.64.192/27	5 and 7
Subnet 7	192.168.64.224/27	6

Prefix Length /24 အတွင်းရှိ တရစပ်ဖြစ်နေသော Subnets များကိုတွေ့ရစဉ်

❖ ဒီတော့ 1 နှင့် 3 ဆိုတဲ့ Subnet ကိုပေါင်းချင်ရင် 1, 2, 3 ၃-ခုစလုံးပေါင်းပစ်ရမလို ဖြစ်နေပါတယ်။ ဒါပထမသိရမယ့် အချက် ၁ ချက် ဒီတစ်ချက်တည်းလားဆိုတော့ မဟုတ်သေးဘူး။ နောက်ထပ် အချက် ၂ ချက်ရှိသေးတယ်။

၄.၅ **Even Divisibility**

ဒုတိယအချက်က Supernet အလုပ်ခံရမယ့် Address က စုံကိန်းနှင့် စားလို့ပြတ်ရမယ်။ အကြွင်းမရှိရဘူး။ ဆိုလိုတာက Network Address တွေကို Bit တွေပြောင်းလိုက်တဲ့အခါ ၎င်း Bit တွေဟာ နောက်Address တစ်ခုရဲ့ Bit နှင့် သွားကိုက်နေဖို့လိုအပ်တယ်ဗျ။ ဒါကိုအခုလို ပြောပြလို့ကတော့ နားမလည်ဘူးဆိုတာသိတယ်။ ဥပမာနှင့် ရှင်းပြမှုဖြစ်မယ်။

ဒီလိုဗျ Subnet နှစ်ခုကိုပေါင်းဖို့ရာ ပထမ Address နဲ့ တတိယ Octet ကို 2 နှင့်စားရင် အကြွင်းမရှိ ပျက်ရမှာဖြစ်ပါတယ်။ ဒါက Subnet ၂ ခုပေါင်းချင်ရင် 8 နဲ့ကစားရမှာဖြစ်ပါတယ်။ ဥပမာကြည့်ရအောင်။ Class C Address တစ်ခုဖြစ်တဲ့ 198.41.15.0 နှင့် 198.41.16.0 ဆိုတဲ့ Subnet နှစ်ခုဟာ ပေါင်းလို့မရဘူး။ ၎င်း Address နှစ်ခုရဲ့ ပထမ Address က 198.41.15.0 ၎င်းရဲ့ တတိယ Octet က 15 ကို 2 နှင့်စားရင်

မြှတ်ဘူး။ အဲကြောင့်ပေါင်းလို့မရတာ။ နောက်ဥပမာတစ်ခုကို ထပ်ပြောပြမယ်။ 198.41.18.0 နှင့် 198.41.19.0 ဒီ Subnet နှစ်ခုပေါင်းလို့ရလားဆို ရတယ်။ ဘာဖြစ်လို့လဲဆိုတော့ ပထမ Address တစ်ခုဖြစ်တဲ့ 198.41.18.0 ရဲ့ တတိယ Octet က ၂ နှင့် စားရင်ပြတ်လို့ဖြစ်ပါတယ်။ ဒီတစ်ခါတော့ Binary နှင့်ဖော်ပြပေးပါမယ်။ Class C ရဲ့ Address နှစ်ခုဖြစ်တဲ့ 198.41.78.0 နှင့် 198.41.79.0 ကိုကြည့်ပါ။ ၎င်းတို့ရဲ့ ပထမ Address တစ်ခုဖြစ်တဲ့ 198.41.78.0 ကိုကြည့်။ တတိယ Octet က 78 မဟုတ်လား။ ၎င်း 78 ကို 2 နှင့်စားရင် ပြတ်တာတော့သိတယ်။ အဲပေမယ့် ဒီတစ်ခါ Binary နှင့်ပြမှာ။ 78 ကို Binary ပြောင်းလိုက်ရင် 01001110 ရတယ်။ 79 ကို Binary ပြောင်းလိုက်ရင် 01001111 ရတယ်။ ဒီ Binary နှစ်ခုကိုကြည့်လိုက် တစ်ဆက်တည်း လည်းဖြစ်နေတယ်တွေ့လား။ ပထမဦးဆုံး စည်းမျဉ်းနှင့်လည်းကိုက်ညီတယ်။

❖ 198.41.18.0 နှင့် 198.41.19.0 ကိုတွက်ကြည့်ရအောင်။

၎င်းတို့နှစ်ခုမှာ 198.41.18.0 တာ ပထမ Address ဖြစ်တယ်။ ၎င်း Address ရဲ့ တတိယ Octet ကို 2 နှင့်စား။ ဘာဖြစ်လို့ 2 နဲ့စားရသလဲဆို ၎င်းတို့နှစ်ခုကိုပေါင်းချင်လို့။ 18 ကို 2 နှင့်စားရင်ပြတ်လား။ အကြွင်းမရှိပြတ်တယ်။ 18, 19, 20 ဒီသုံးခုကို Binary ပြောင်းကြည့်။ 21 ကိုရေပါ။

❖ 18 ၏ Binary 00010010
❖ 19 ၏ Binary 00010011
❖ 20 ၏ Binary 00010100
❖ 21 ၏ Binary 00010101

ဒီတော့ အဲဒီမှာကြည့်လိုက်ရင် Binary ရဲ့သဘောအရ 18 ဟာ 19 နှင့်တစ်အုပ်စုထဲဖြစ်တယ်။ 18 နဲ့နောက်ဆုံးက 10၊ 19 ရဲ့နောက်ဆုံးက 11၊ အဲကြောင့် 198.41.18.0 နှင့် 198.41.19.0 ကပေါင်းလို့ရတယ်။ အဲပေသိ 19 ရဲ့ နောက်ဆုံး Binary 11 နှင့် 20 ရဲ့ နောက်ဆုံး Binary 00 ကအုပ်စုမတူပြန်ဘူး။ အဲကြောင့် 198.41.19.0 နှင့် 198.41.20.0 ကတွဲလို့မရ၊ ပေါင်းမရပြန်ဘူး။ တစ်ခါ 20 နဲ့နောက်ဆုံး Binary 0 0 နှင့် 21 ရဲ့ နောက်ဆုံး Binary 01 ကို ပြန်ကြည့်ရင် အုပ်စုကတစ်တွဲပြန်ဖြစ်နေပြန်ရော။ အဲဒါကြောင့် ဒီစည်းမျဉ်းက Octet ကို စုံကိန်းနှင့် စားရင်ပြတ်တဲ့ ဂဏန်းမှာ Supernet လုပ်လို့ရတာပါ။ ဒီတော့ Supernet ကိုပေါင်းတဲ့အခါ 1 bit ချေးတိုင်း 2 တိုးတာမို့ စုံကိန်းဖြစ်နေတာပါ။

နားမလည်တော့ပြန်ဘူးမဟုတ်လား။ အဲဒီဟာက Binary မသိလို့ နားမလည်တာကိစ္စမရှိဘူး။ နားလည်အောင်ရှင်းပြမယ်။ Class C နှင့်ပဲရှင်းပြရမှာပဲ။ Class C ရဲ့ Default Subnet Mask ဘယ်လောက်

လဲ။

255.255.255.0 ပါ။ ဟုတ်ပြီ။ 255.255.255.0 ကို Prefix နှင့်ပြရင် 124 ဖြစ်တယ်။ 8 bits ခုခါလာတာကိုး။ ကဲ Class C ရဲ့ Default Subnet Mask ရဲ့အဓိပ္ပါယ်တာ ဒီ Network မှာ Subnet မရှိဘူး။ Network တစ်ခုပဲရှိတယ်လို့ ရည်ညွှန်းတာဖြစ်ပါတယ်။ အဲဒီ Network မှာ Host ဘယ်လောက်ရှိသလဲ။ 2^8 ပေါ့။ 32 bits ရှိတဲ့အထဲက 24 bits က Network ကိုး။ ဒီတော့ကျန်တဲ့ 8 bits က Host ပေါ့။ $2^8 = 256 - 2$ ဆိုတော့ 254 ပေါ့။ 254 Host ရှိတဲ့ Network တစ်ခုပေါ့။

အဲဒီအချိန်မှာ Supernet လုပ်မယ်။ ဒီတော့ Network ဘက်က 1 bit ချေးပါ။ Subnet ဆို Host ဘက်ကချေးတာ Supernet က Network ဘက်ကချေးတာ။ ဒီတော့ Network ဖက်မှာ 24 bits မကျန်ဘဲ 23 bits ပဲကျန်တယ်။ 1 Bit ပဲချေးလိုက်တာနော်။ ဒီတော့ 2^1 ပေါ့။ $2^1 = 2$ လေ။ ဒါကြောင့် စုံကိန်းပဲလာတယ်လို့ပြောတာ 2 bits ချေးကြည့်ပါလား။ 24 bits အထဲက 2 bits ချေးတော့ Network မှာ 22 bits ပဲကျန်တယ်။ 2 bits ချေးတော့ 2^2 ပေါ့။ 2^2 က 4 ပေါ့။ ဒီတော့ 2 ဆိုပြီးတော့ 3 မလာဘူး။ 4 လာတယ်။ ပြီးရင် 8 လာလိမ့်မယ်။ ပြီး 16 လာလိမ့်မယ်။ ဒီတော့ Supernet 2 ခုပေါင်းမယ်။ 4 ခုပေါင်းမယ်။ 8 ခုပေါင်းမယ်။ စသည်ဖြင့်ပေါ့။ ကဲအောက်က ဇယားကိုကြည့်ရအောင်။

Class C			
CIDR Block	Supernet Mask	Number of Class C Networks	Number of Hosts
/14	255.252.0.0	1024	262144
/15	255.254.0.0	512	131072
/16	255.255.0.0	256	65536
/17	255.255.128.0	128	32768
/18	255.255.192.0	64	16384
/19	255.255.224.0	32	8192
/20	255.255.240.0	16	4096
/21	255.255.248.0	8	2048

Product of YOUTH

CIDR Block	Supernet Mask	Number of Class C Networks	Number of Hosts
/22	255.255.252.0	4	1024
/23	255.255.254.0	2	512
/24	255.255.255.0	1	254
/25	255.255.255.128	1/2	126
/26	255.255.255.192	1/4	62
/27	255.255.255.224	1/8	32
/28	255.255.255.240	1/16	16
/29	255.255.255.248	1/32	8
/30	255.255.255.252	1/64	4

အဲဒီဇယားမှာကြည့်.....

/24 255.255.255.0 1 254

ဒါဟာ Class C ရဲ့ Classful Network ပဲ။ သူ့ရဲ့အောက်ကိုကြည့် 125, 126 စသဖြင့် ဒါဟာ Class C Network ကြီးကို Subnet တွေ ပိုင်းလိုက်တာ။ /25 ကျတော့ Class C Network ကြီးက နှစ်ပိုင်းဖြစ်သွားပါတယ်။ ဒီတော့ Subnet နှစ်ခုဖြစ်သွားတာပေ့ါ။ နဂို Network တစ်ခုတည်းတုန်းက Host က 254 ရတယ်ဆိုတော့ အခု Subnet နှစ်ခုခွဲလိုက်တော့ Subnet တစ်ခုချင်းစီမှာ 126 ခု စီပဲရတော့တာပေ့ါ။ ဒီနေရာမှာသိရမှာက Subnet ခွဲလိုက်တိုင်းမှာ All 0 bit နှင့် All 1 bit ကို Subnet ID နှင့် Broadcast Address အတွက်ဖယ်ရတာကြောင့် Subnet တစ်ခုတိုင်းမှာ Host ဟာ ၂ ခုလျော့လျော့သွားပါတယ်။

ကဲ အဲဒီလိုနှင့် အောက်ကိုဆက်ကြည့်သွား။ CIDR Prefix Length တွေကြီးလာလေ Network အရေအတွက်များလာလေ။ Host အရေအတွက်နည်းလာလေ။ ဒီ /24 ရဲ့ ညာဖက်ကိုရောက်သွားတိုင်း /25 /26 ဖြစ်သွားတိုင်း၊ ဒါဟာ Subnet ပဲ။

/24 255.255.255.0 ရဲ့အပေါ်ကိုကြည့် /23 ဖြစ်သွားတယ်။ Network က 1 bit လျော့သွားမယ်။

Subnet Mask က (တနည်းအားဖြင့် Supernet Mask) 255.255.255.0 မဟုတ်တော့ဘဲ 255.255.254.0 ဖြစ်သွားတယ်။ ပြောတော့ Class C ဒါပေမယ့် Class C ဖြစ်ပါလျက်နဲ့ 255.255.254.0 ဆိုတော့ Classless (Class မရှိတော့သလိုဖြစ်သွားတာပေါ့) ပေါ့။ ဒီတော့ Network မှာ /24 ကနေ /23 ဆိုတော့ 1 bit လျော့သွားသလို၊ Host ဖက်မှာလည်း 8 bits ကနေ 9 bits ဖြစ်သွားတယ်လေ။ ဒါကြောင့် Host အရေအတွက်က 254 မဟုတ်တော့ဘဲ 512 ဖြစ်သွားတာပါ။ 512 ဆိုတာ 2^9 လေ။

ဒီနေရာမှာသတိထားမိလား။ ၂ နုတ်စရာမလိုတော့ဘူး။ ဘာလို့လဲဆိုတော့ Host ပေါင်း ၂၅၆ အရေအတွက်ရှိတဲ့ Network နှစ်ခုကို ပေါင်းလိုက်လို့။ ဒါကြောင့် Number of Class C Network မှာ 2 ဖြစ်သွားတာ။ ဒီလိုပဲ /24 ကနေ /23, ပြီးတော့ /22 ဒီလို 1 bit စီရွေ့သွားတိုင်းမှာ 2^1, 2^2, 2^3, 2^4 စသဖြင့်ဖြစ်သွားတာ၊ 2^1ဆိုရင် 2 ရတယ်။ 2^2 ဆိုရင် 4 ရတယ်။ 2^3 ဆိုရင် 8 ရတယ်။ စသဖြင့်ပေါ့။ ဇယားကိုကြည့်လိုက်ရင်ရှင်းသွားမှာပါ။ 2 ဆိုရင် Network နှစ်ခုပေါင်းတာ၊ 4 ဆိုရင် Network လေးခုပေါင်းတာ၊ Network နှစ်ခုပေါင်းတော့ Host က 256 နှင့် 256 ပေါင်းပြီး 512 ဖြစ်လာတာဖြစ်ပါတယ်။ ဒီတော့ Number of Class C Network မှာ 2 တို့ 4 တို့ 8 တို့က ပေါင်းထားတဲ့ Network အရေအတွက်ပဲ။ အစွန်ဆုံးက Number of Host က Network တွေကိုပေါင်းလိုက်ခြင်းကြောင့်ရလာတဲ့ Host အရေအတွက်ပဲဖြစ်ပါတယ်။

နောက်တစ်ခုက အကယ်၍ ကွန်ရက်ကို Subnet တွေအဖြစ် အပိုင်းပိုင်း ပိုင်းလိုက်ရင် တပိုင်းချင်းစီမှာ Host 2 ခုစီဖယ်ရတာကြောင့် Host တွေလည်း ဆုံးရှုံးပါတယ်။ ဘာလို့လည်း Subnet ၁ ခုမှာ ထိပ်ဆုံး All 0 နှင့် နောက်ဆုံး All 1 ဆိုတဲ့ Host က ဖယ်ထားရတယ်။ Subnet ၂ ခုဆို Host ၄ ခုဆုံးရှုံးမှာဖြစ်ပါတယ်။ အခုဟာက Subnet ၂ ခုပေါင်းလိုက်တော့ Host ၂ ခုစီ 4 ခုဆုံးရှုံးမယ့်အစား 2 ခုပဲ ဆုံးရှုံးပါတော့မယ်။ ဥပမာအားဖြင့် ပြောပြဦးမယ် 203.31.218.0 ဆိုတဲ့ Network တစ်ခုနှင့် 203.31.219.0 ဆိုတဲ့ Network တစ်ခုတို့ပေါင်းတဲ့အခါ

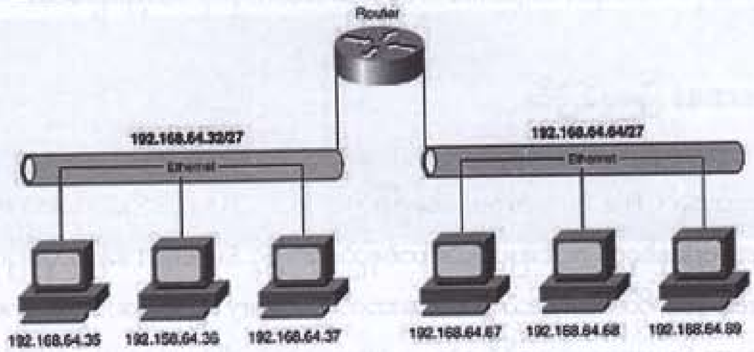
203.31.218.0 မှာ 203.31.218.0 ဆိုတဲ့ Address နှင့် 203.31.218.255 ဆိုတဲ့ Address ကိုသုံးလို့မရဘူးလေ။ အဲသလိုပဲ 203.31.219.0 မှာ 203.31.219.2 နှင့် 203.31.219.255 ဆိုတဲ့ Address ကသုံးမရဘူးလေ။ ဒီ 0 ကို Binary ပြောင်းရင် 0 to 8 လုံးရလို့ All 0 လို့ခေါ်တာဖြစ်ပြီး၊ 255 ကို Binary ပြောင်းရင် 1 to 8 လုံးရတာမို့ All 1 လို့ ခေါ်တာဖြစ်ပါတယ်။ ဒီ Address နှစ်ခုကို ဖယ်ထားရမယ်လေ။ *Network က ၂ ခုဆိုတော့ Address 4 ခုဆုံးတာပေါ့။ အကယ်၍ 203.31.218.0 နှင့် 203.31.219.0* ဆိုတဲ့ Address နှစ်ခုကိုပေါင်းလိုက်ရင် Supernet ဖြစ်သွားမယ်။ အဲဒီအခါကျတော့ 203.31.218.0 ကနေ 203.31.219.255 ဆိုပြီး Network တစ်ခုတည်းဖြစ်သွားရော။ ဒီတော့ဖယ်ရတော့မယ့် Host လျော့သွားတာပေါ့။ အဲဒီအပြင်ကြားမှာခြားနေတဲ့ Address လည်းမရှိဘဲ တရစပ်ဖြစ်သွားတယ်။ 203.31.218.0 နှင့် 203.31.219.0 တို့ဟာ သီးခြားစီဖြစ်နေရင် 203.31.218.255 နှင့် 203.31.219.0 တို့လိုဖယ်ထားရခြင်းကြောင့် ကြားထဲမှာခြားသွားတယ်။ ဒီတော့ Network နှစ်ခုပေါင်းလိုက်တော့ ကြားထဲမှာ ခြားမနေတော့ဘူးပေါ့။

Product of YOUTH

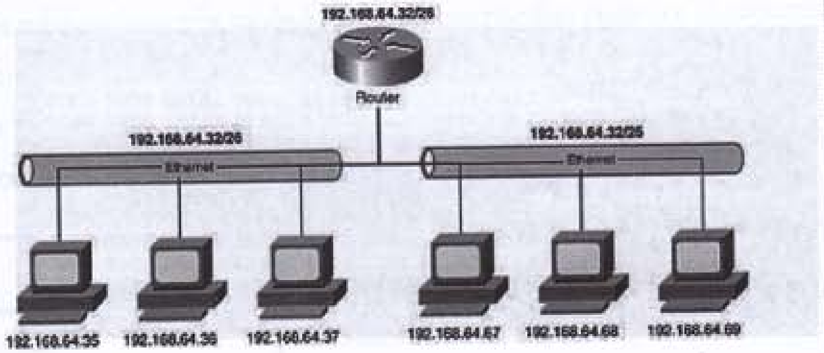
၄.၆ **Single Interface**

နောက်ဆုံးတစ်ချက်ကတော့ Supernet အဖြစ်ပေါင်းလိုက်မယ့် Subnet တွေဟာ Interface တစ်ခုထဲမှာဘဲချိတ်ဆက်ထားရမယ်။ ဒီနေရာမှာ Interface ဆိုတာ Router ကိုပြောတာဆိုတော့ အောက်ကပုံကို ကြည့်လိုက်ရင် ရှင်းသွားလိမ့်မယ်။

ပုံ ၄၄



Subnets နှစ်ခု Router ဆီကို သီးခြား Network အဖြစ်ဝင်ရောက်ကြစဉ်



Supernetting ပြုလုပ်ပြီးစဉ် Network နှစ်ခုဟာ တစ်ခုတည်းအဖြစ် Router ကို ဝင်ရောက်စဉ်

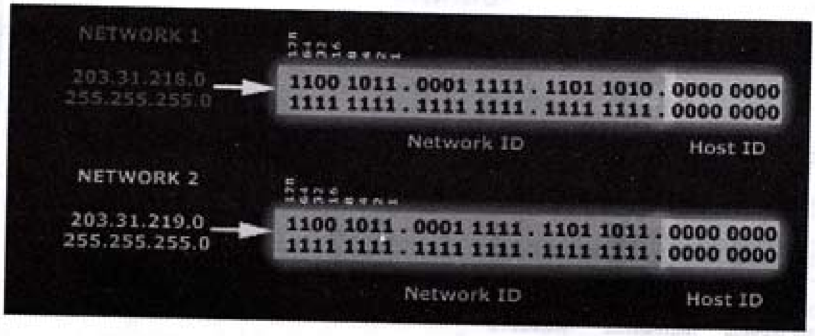
ဒီနေရာမှာ တကယ်ပြောစရာအကြောင်းတစ်ခုရှိသေးတယ်။ အဲဒါကဘာလဲဆိုရင် Router တွေဟာ

Static Routing သို့မဟုတ် RIP2R ဆိုတဲ့ Classless Routing Protocol ကိုအသုံးပြုရလိမ့်မယ်။ Classless Routing Protocol က Subnet Mask နဲ့ပတ်သတ်တဲ့ အကြောင်းအရာအချက်အလက်တွေကိုသာမက Supernet နဲ့ ပတ်သတ်တဲ့ အချက်အလက်တွေဟာ Supernet Mask Information တွေကို သယ်ဆောင်မပေးနိုင်ဘူး။ ဒီတော့ Supernet ကိုပြုလုပ်ဖို့ရာ Router ရဲ့ Rom Version က 3.0.7 ရဲ့နောက်ပိုင်းဖြစ်ခဲ့မယ်ဆိုရင်လည်း ကောင်းတာ Supernetting ပတ်သတ်လို့ လုပ်ဆောင်ချက်အပြည့်အစုံပါပြီးသားဖြစ်ပါတယ်။ ဒီနေရာ RIT ဆိုတာ Routing Information Protocol ဖြစ်ပါတယ်။ ကဲ ဥပဒေသသုံးချက်စလုံးလည်း ရှင်းပြပြီးဆိုတော့ အခုတစ်ခါတည်း Supernet တစ်ခုတည်ဆောက်ပုံကို ဖော်ပြပါဦးမယ်။

၄.၇ **Supernet** ပြုလုပ်ခြင်း

ကျွန်တော်အခု Class C Network နှစ်ခုဖြစ်တဲ့ 203.31.218.0, 255.255.255.0 နှင့် 203.31.219.0 ဆိုတဲ့ Network နှစ်ခုကို ပေါင်းပြပါမယ်။ တစ်နည်းအားဖြင့် Supernet အဖြစ်လုပ်ပြပါမယ်။ ပထမဦးစွာ ၎င်း Address နှစ်ခုကိုထင်သာမြင်သာအောင် အောက်မှာ Binary ပြောင်းပြပေးထားပါတယ်။ ဒီနေရာမှာ အထူးသတိထားရမှာ Supernet မပြုလုပ်မီ ၎င်း Address နှစ်ခုရဲ့ Subnet Mask ဟာ 255.255.255.0 ဖြစ်ပါတယ်။ တနည်းအားဖြင့် Class C Classful Network တွေဖြစ်ကြပါတယ်။

ပုံ ၄.၅



Supernet တစ်ခုတည်ဆောက်တယ်ဆိုတာ တကယ်တော့အလွယ်လေးပါဗျာ။ အောက်ကပုံကို ကြည့်လိုက်။ အဓိကထားကြည့်ရမှာ Subnet Mask ပဲ။ အဲဒီ Subnet Mask မှာမှ တတိယ Octet ကိုသေချာကြည့်။ တတိယ Octet ရဲ့ Subnet ကိုခွဲလိုက်တဲ့အခါကျတော့ ဒီ တတိယ Octet ရဲ့ Subnet Mask Binary က 11111110 ဖြစ်သွားမယ်။ တကယ်တော့ တစ်–ရှစ်လုံးထဲက၊ နောက်ဆုံး Bit ကို သုည–

ပြောင်းလိုက်တာပဲ။ သုညလို့ဆိုရင် ဒါက Host အပိုင်းဖြစ်သွားပြီလေ။ တစ်–တွေက Network အပိုင်းပေါ့။ ဒီတော့ Supernet မခွဲခင်တုန်းက Network ID ဟာ 24 bits ရှိပြီး၊ Host ID က 8 bitd ရှိပါတယ်။ အခု Supernet ကိုခွဲလိုက်တဲ့အခါကျတော့ Network ID ဟာ 23 bits ဖြစ်သွားပြီး၊ Host ID က 9 bits ဖြစ်သွားပါတယ်။ ဒါကြောင့် Host အရေအတွက် $2^9 = 512$ ဖြစ်သွားပါတယ်။ Network ID ကို Binary ကနေ Decimal အဖြစ်ပြန်ပြောင်းတဲ့အခါ Subnet Mask ဟာ 255.255.255.0 မဟုတ်တော့ဘဲ 255.255.254.0 ပဲဖြစ်သွားပါတယ်။

ပုံ ၄၆

အခုလို Class C Network နှစ်ခုပေါင်းပြီး Supernet အဖြစ်ပြုလုပ်လိုက်တာဟာ တကယ်တမ်းကျတော့ Network နှစ်ခုကိုပေါင်းပြီး ကြီးမားတဲ့ Network တစ်ခုဖန်တီးလိုက်တာပါပဲ။ အရင်တုန်းကတော့ Network တစ်ခုမှာ All 0 ဆိုတဲ့ ရှေ့ဆုံး Address အဖြစ်လည်းကောင်း၊ All 1 ဆိုတဲ့ Network ကို Broker Address အဖြစ်လည်းကောင်း အသုံးမပြုဘဲ ဖယ်ထားရတဲ့အခါမှာ Network နှစ်ခုဆိုတော့ Address လေးခုဖယ်ထားရမှာပေါ့။ အခုလို Supernet လုပ်ပြီးသွားတဲ့အခါမှာတော့ Address ကိုလေးခုဖယ်စရာမလိုတော့ဘဲ၊ နှစ်ခုကိုဘဲ ဖယ်ရတော့မှာဖြစ်ပါတယ်။ အောက်ပါဇယားကို ကြည့်လိုက်ရင် ပိုပြီးတော့ ရှင်းသွားမှာဖြစ်ပါတယ်။

ITEM	VALUE
Supernet range	203.31.218.0 - 203.31.219.255
Subnet Mask	255.255.254.0
Supernet Network Address	203.31.218.0
Supernet Broadcast Address	203.31.219.255
Supernet 0	203.31.218.0

ITEM	VALUE
Supernet 1	203.31.219.0
Valid IP Address range	203.31.218.1 - 203.31.219.254
Reserved IP Addresses	203.31.218.0, 203.31.219.255

၄.၈ နိဂုံးချုပ်အမေးအဖြေ

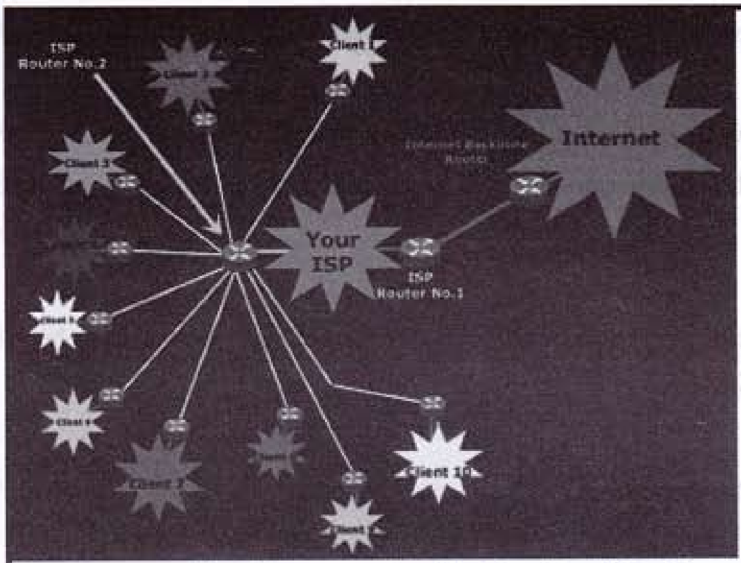
၁။ IPv4 Address Class များ၏ ကန့်သတ်ချက်က အဘယ်နည်း။

IPv4 Address Class များ၏ ကန့်သတ်ချက်ကတော့ –

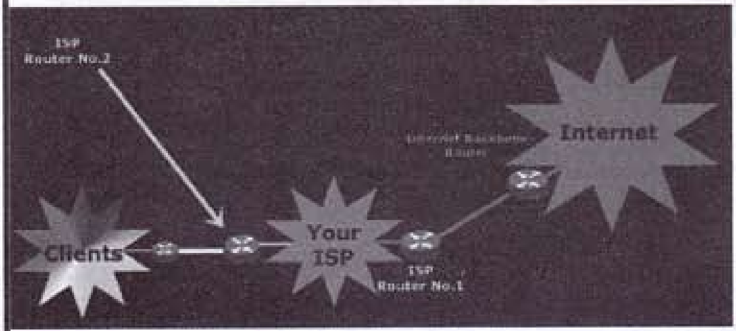
(က) IP Address များ အလဟသ ဆုံးရှုံးမှုများပြားခြင်း။
(ခ) Network တစ်ခုချင်းစီကနေ Router ရဲ့ Routers Table ထဲကို Routing Information တွေက တစ်နေ့ရာစီကနေ့လာကြတော့ Routing Table ကြီးလာတယ်။ ဒါ IPv4 Address Class တွေရဲ့ မကောင်းတဲ့အချက်ပဲ။ ဒီနေရာမှာ Routing Table ကြီးလာတာ အပေါ်မှာလည်းပြောပြခဲ့ပြီးပြီ။ Router တစ်ခုမှာ Subnet နှစ်ခုခွဲထားမယ်ဆို အဲဒီ Subnet တစ်ခုချင်းစီကနေ Routing Information တွေ Router ဆီလာကြတယ်။ ဒီ Network နှစ်ခုကို ပေါင်းလိုက်တဲ့အခါကျတော့ Router ဆီကိုချတဲ့ Information တွေက Network နှစ်ခု မဟုတ်ဘဲ Network တစ်ခုထဲကဆိုတော့ Routing Table Size ကိုလျှော့ချနိုင်တာပေါ့။ Routing Table ရဲ့ Size လျော့လာတော့ Performance လည်းပိုကောင်းလာတာပေါ့။ ပုံ ၄၇ ကိုကြည့်ပါ။

၂။ IPv4 Address Class ကိုသုံးတဲ့အခါမှာ IP Address တွေအများကြီးဘာကြောင့်ဆုံးရှုံးရတာလဲ

ဒါက ခုနကမေးခွန်း နံပါတ် (၁) ရဲ့ အဖြေ (က) ကို ပြန်ရှင်းထားတာပါ။ ဥပမာဆိုကြပါစို့။ သင်တာကွန်ပျူတာ အဲ Host ပေါ့ဗျာ.. Host 300 ရှိဖို့လိုတယ်ပေါ့။ ဒီတော့ ဒီ Hosts 300 ရှိဖို့အတွက် သင်တာ Class B Network တစ်ခုဝယ်လိုက်ရင် Class B Network မှာ Hosts ပေါင်း 2^{16-2} =65534 တောင်



Supernetting မပြုလုပ်မီ Router ထဲအဝင်ကြမ်းပုံကိုတွေ့မြင်ရစဉ်



Supernetting ပြုလုပ်ပြီး Routing Information များစုစည်းသွားသည့်ပုံ

ရှိပါတယ်။ လိုတာက Hosts ပေါင်း 300 ထဲပါ။ Hosts ပေါင်း 300 ကို Class B Network ယူလိုက်တော့ 65539 ထဲက 300 ကို နုတ်၊ ကျန်တဲ့ Address တွေဟာ အလဟဿ ဆုံးရှုံးသွားပါမယ်။ ဒီတော့ တိုလိုလုပ်ပါလာ။ အဲဒီလိုလုပ်ပါလား။ Class B Network မယူနဲ့။ Class C Network ၂ ခုယူလိုက်။ အဲ့သလိုဆို Class B Network ၂၃ ကိုရလိမ့်မယ်။ ဒါပေမယ့် Class C Network ကလည်း အများကြီးမှ မရှိတာ။ ဒီလိုသာ နှစ်ခုယူမယ်ဆို Class C Network တွေ လှစ်ကနဲ ကုန်သွားမှာပေါ့။ ဒီအချက်တွေကို ကြည့်ခြင်းအားဖြင့် IP Address တွေဟာ အလဟဿ ဆုံးရှုံးကုန်တယ်ဆိုတာကို တွေ့နိုင်မှာပါ။

၃။ ဒီ IP Addressing ရဲ့ ကန့်သတ်ချက်တွေကို ဖြေရှင်းတဲ့ နည်းလမ်းရှိလား။

က။ IP Latest Version ဖြစ်တဲ့ IP Version 6 ဟာ ဒီအတွက်အဖြေပဲဖြစ်ပါတယ်။ IP v6 ကို IP Next Generation (IPng) လို့လည်းခေါ်ပါတယ်။ ဒီစာအုပ်မှာပဲ IPv6 အကြောင်းကို ရှင်းပြတဲ့သင်ခန်းစာ ပါရှိပြီးဖြစ်ပါတယ်။

ခ။ နောက်တစ်ခုကတော့ အခုဒီသင်ခန်းစာမှာပင်ရှင်းပြနေတဲ့ CIDR ဆိုတဲ့ Classless Inter Domain Routing ပဲဖြစ်ပါတယ်။

၄။ ဒါဆို CIDR ကရောဘာလဲ။

CIDR ဆိုတာ Classless Inter Domain Routing ဖြစ်ပါတယ်။ သူက ပုံမှန် IP Address Class တွေ ဖြစ်ကြတဲ့ Class A, Class B နှင့် C တို့ကို အသုံးမပြုဘဲ Network တစ်ခုမှာ လိုချင်တဲ့ Host အရေအတွက် ကိုမူတည်ပြီး IP Address သတ်မှတ်တဲ့ နည်းကိုပြောတာ ဖြစ်ပါတယ်။

၅။ ဒါဆို Classful IP Addressing နှင့် Classless IP Addressing ဘာကွာလဲ။

အဓိက ကွာခြားတာကတော့ IP Address ရဲ့ Network ID Portion အတွက် Bits ကိုသတ်မှတ်တာကွာသွားတာဖြစ်ပါတယ်။ Classful IP Addressing မှာဆိုရင် Network ID Portion အတွက် သတ်မှတ်ထားတဲ့ Bits တွေက 8, 16 နှင့် 24 တို့ပဲဖြစ်ပါတယ်။ Classless မှာကျတော့ Network ID အတွက် Bits ကို မည်သည့် ဂဏန်းမဆိုသတ်မှတ်နိုင်ပါတယ်။

၆။ CIDR IP Address မှာ Network ID ကိုဘယ်လို သတ်မှတ်မလဲ။

CIDR IP Addressing မှာ Classful လိုပဲ ရှေ့က Bits က Network ကိုရည်ညွှန်းပြီး 32 bits ထဲက Network အတွက်ဖယ်ပြီး၊ ကျန်တာက Host Bits ဖြစ်ပါတယ်။ ဆိုလိုတာက Network က 26 bits ယူလိုက်ရင် Host အတွက် 6 bits ပဲကျန်ပါတယ်။ ဒါပေမယ့် သိရမှာက Network Bits ဟာ Classful လို 8,16,24 မဟုတ်တဲ့ 1 ကနေ 31 အတွင်း မည်သည့်ဂဏန်းမဆို ဖြစ်နိုင်ပါတယ်။ ဘယ်လောက် ဖြစ်မလဲဆိုတာကတော့ Network မှာ Hosts ဘယ်လောက်ထားမလဲပေါ်မူတည်ပြီး တွက်ရမှာ ဖြစ်ပါတယ်။

၇။ ဒါဆို CIDR Notation မှာ IP Address ဟာ ဘယ်လိုပုံစံရှိနေမလဲ။

CIDR Notation မှာ အပေါ်က ပြောခဲ့ပြီးတဲ့အတိုင်း A.B.C.D/n ဆိုပြီး ဖြစ်နေမှာပါ။ ဥပမာ 192.9.205.22/18 ဆိုပြီးတော့ပါ။ ဒီနေမှာ /18 ကNetwork Bits ဖြစ်ပြီး။ ကျန်တဲ့ 14 bits ကတော့ Hosts အရေအတွက် ဖြစ်ပါတယ်။

၈။ CIDR ရဲ့ အကျိုးကျေးဇူးကဘာလဲ။

ဒါကတော့ IPv4 Address Class တွေရဲ့အားနည်းချက်၊ မေးခွန်း နံပါတ် ၁ ရဲ့ အဖြေနှင့် ဆန့်ကျင်ဘက်ပဲဖြစ်ပါတယ်။

တ။ CIDR က IP Address Space တွေကို ထိရောက်စွာ ထိန်းချုပ်နိုင်တယ်။ အသေးစိတ် သတ်မှတ်နိုင်ပါတယ်။ ဆိုလိုတာက -

Host ပေါင်း ၅၀၀၀ လိုတဲ့ အဖွဲ့အစည်းဟာ Class C ကို ယူလို့မရနိုင်ပါဘူး။ Class C မှာ Hosts က 254 ပဲရှိပါတယ်။

Class B ကိုယူရင်လည်း Hosts က 65534 တောင်ရှိနေပါတယ်။ ဒီတော့ ဒီနေရာမှာ Hosts တွေ ပုပ်ကုန်ပါလိမ့်မယ်။ အကောင်းဆုံးကတော့ CIDR ကိုသုံးပါ။ /19 ကိုသုံးလိုက်ပါ။ /19 ဆို 32 ထဲက 19 ကို နုတ် 13 ကျန်ပါတယ်။ ဒီ 13 က 2^{13} ပါ။ ဆိုတော့ Host ပေါင်း 8190 ရပါတယ်။ /19 ဆိုတာ Network Bits လေ။ 32 ထဲက 19 နုတ်တော့ 13 ကျန်တာပေါ့။ ဒီတော့ 2^{13} က Host Bits ဖြစ်ပါတယ်။ 2^{13} က 8190 Hosts ကို ရစေပါတယ်။ လိုအပ်တဲ့ Hosts က 5000 ပါ။ ဒါဆို 2^{12} ဆိုရင် ရော 2^{12} က 4096 ပဲရှိပါတယ်။ လိုချင်တဲ့ Hosts က 5000 ဆိုတော့ 2^{12} နှင့် အဆင်မပြေနိုင်ပါ။ ဒါကြောင့် Network ကို 19 bits ထားပြီး 13 bits ကို Host အတွက်ထားတာပါ။

ခ။ CIDR ဟာ Network တွေကို ပေါင်းလည်းပေါင်းပစ်နိုင်တာကြောင့် Routing Table Entries တွေကိုလည်း လျှော့ချနိုင်ပါတယ်။ မေးခွန်း၁ ရဲ့ (ခ) မှာ ရှင်းပြခဲ့ပြီးပါပြီ။

၉။ CIDR က IP Address ရဲ့ ကန့်သတ်ချက်တွေကို အကုန်လုံးပြေလည်စေနိုင်မှာလား။

မပြေလည်နိုင်ပါဘူး။ အားလုံး တနည်းအားဖြင့် IP Address မလောက်ငှမှုတွေ ကန့်သတ်ချက်တွေဟာ IPv6 ကျမှပြေလည်သွားမှာဖြစ်ပါတယ်။

YOUTH Computer Co.,Ltd,
Training & Multimedia Production
6-A၊ ပန်းဆိုးတန်း Office Tower ၊ ပန်းဆိုးတန်း (အလယ်)၊ ကျောက်တံတား။ ဖုန်း- ၂၅၄၈၉၃

စစ်ကိုင်း - အပ်ချုပ်စုရပ်၊ စစ်ကိုင်းမြို့ ။ ဖုန်း - ၀၇၂-၂၁၂၄၉၊ ၀၇၂-၂၁၉၆၂
လားရှိုး - ရပ်ကွက် - ၁၂၊ လားရှိုးလုံလမ်း၊ နယ်မြေ (၇)၊ လားရှိုးမြို့

Practical A+ (Hardware & System)

ကွန်ပျူတာပြုပြင်ထိန်းသိမ်းခြင်းအပိုင်းကို သင်ကြားသည်။

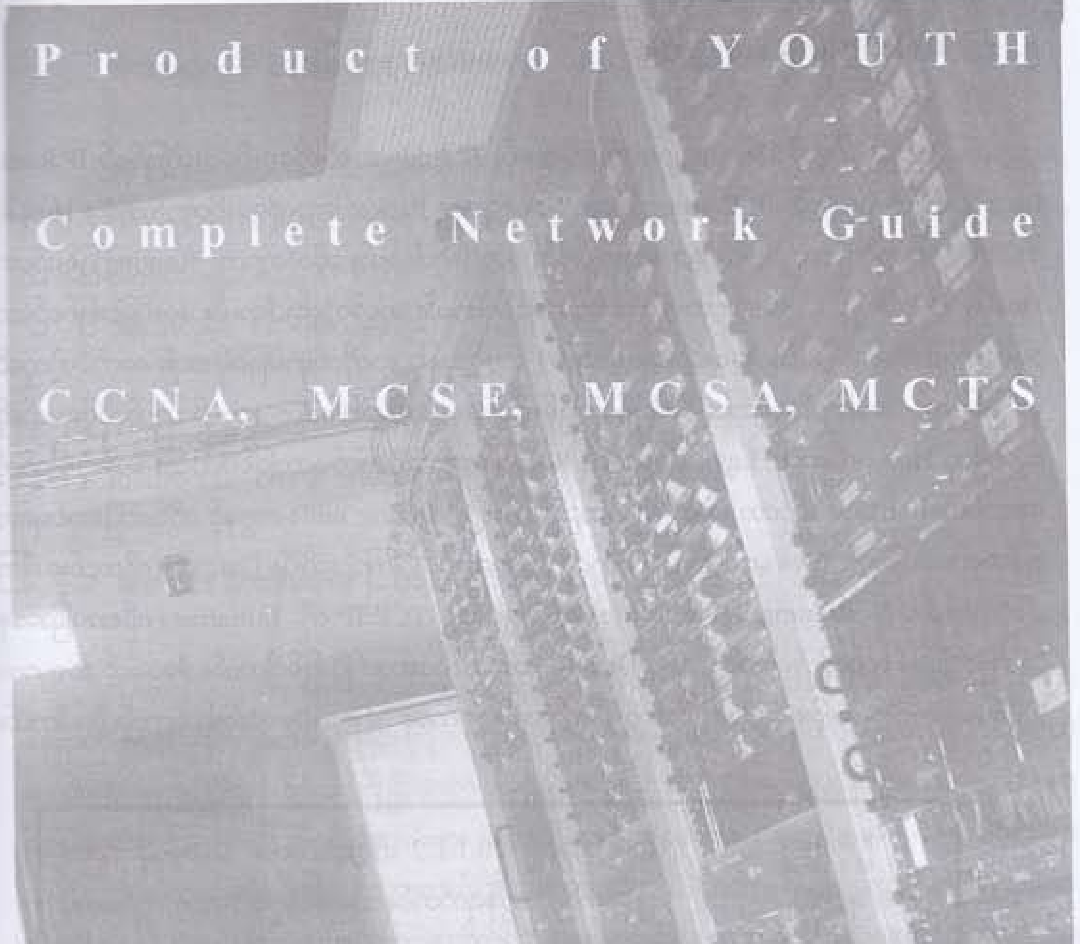
PC Overview, Assembling Parts, CMOS Setup & Configuration, Peripheral Device Overview, Installing Operating System, Device Over Installing, Configuration, Application Installing, Antivirus Concept & Installing, Disk & File Management, Hardware Maintenance, System Administration စသည့် သင်ခန်းစာများပါဝင်သည်။ တတွေ့ရေ လက်တွေ့ပါ အထူးသင်ကြားပေးသည်။ အခြေခံကောင်းသွားစေရမည်။

Network Engineering - Enterprise

ကွန်ပျူတာကွန်ရက်ပိုင်းကိုလုပ်ငန်းခွင်ဝင်နိုင်အောင်သင်ကြားပေးသည်။

Windows Server 2003 in Details, Installation, Administration, Security Permission, Monitoring, Network+, Cable Installation, Wireless Installation, DFS, DHCP, DNS, Mail, NAT, Gateway, FTP, Squid Proxy သင်ခန်းစာများပါဝင်သည်။ IP Addressing, Subnetting များပါထည့်သွင်းသင်ကြားသည်။ Dual Core 2.5, 1 GB, 160 GB, 17 "LCD, များဖြင့်လေ့ကျင့်ရမည်။ တတွေ့လက်တွေ့ပိုင်ပြီးအခြေခံနိုင်စေရမည်။

Product of YOUTH



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

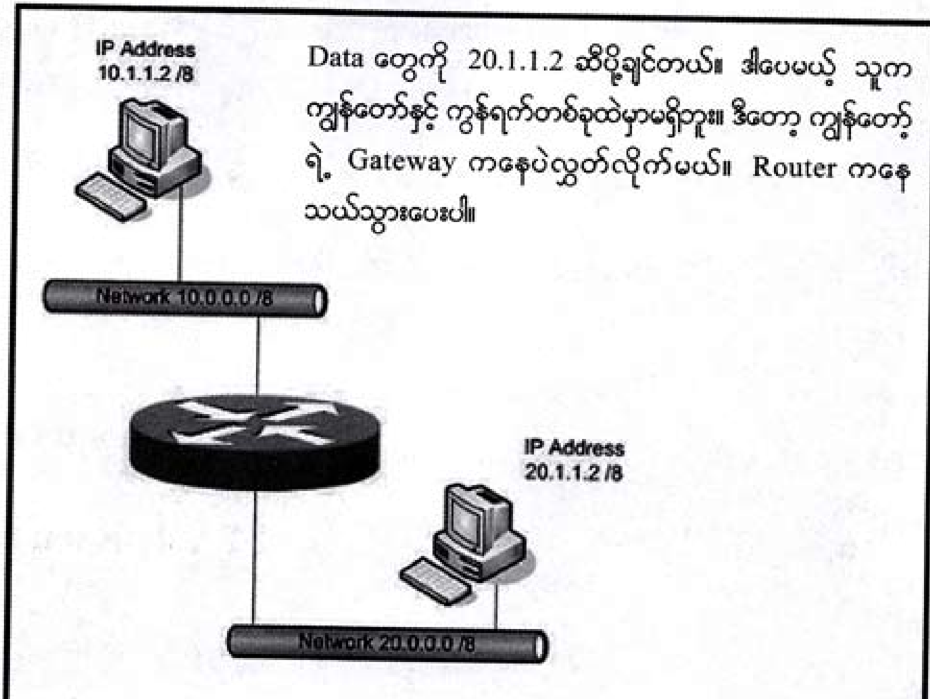
Chapter 5

IPv4 Routing

၅. ၁ IP Routing အကြောင်း

Packet တွေကို Destination (ပေးလို့ရမယ်) IP Address ဆီကိုပေးပို့ပေးတဲ့ဖြစ်စဉ် IP Routing လို့ခေါ်ပါတယ်။ ဒီလို IP Routing ပြုလုပ်ခြင်းတွေဟာ Packet တွေကိုပေးပို့တဲ့ Sender Host ရဲ့ TCP/IP မှာတွေ့ရှိရသလို IP Router တွေမှာလည်း တွေ့ရှိနိုင်ပါတယ်။ ဆိုလိုတာက Routing ဖြစ်စဉ်ဟာ Host ရဲ့ TCP/IP နှင့် IP Router မှာပဲပြုလုပ်ကြတာဖြစ်ပါတယ်။ ဟုတ်ကဲ့ရှင်းပါတယ်။ ပေးပို့ခြင်းဖြစ်စဉ်ဟာ ဥပမာ စာတစ်စောင်ပို့မယ်။ ဒီပေးပို့ခြင်းဖြစ်စဉ်ဟာ ပေးပို့သူနှင့် စာတိုက်မှာပဲဖြစ်မှာပေါ့။ လက်ခံတဲ့သူဆီမှာ ဖြစ်စရာမှ အကြောင်းမရှိတာ။ ဒီလိုဖြစ်တဲ့ ဖြစ်စဉ်တစ်ခုချင်းစီမှာ Packet တွေကို ဘယ်လိုပို့ရမယ်ဆိုတဲ့ကိစ္စကို Host ဖက်က IP Layer ဒါမှမဟုတ် Router တွေကဆုံးဖြတ်ရတာဖြစ်ပါတယ်။ ဒီလိုဆုံးဖြတ်တဲ့နေရာမယ် IP Layer တွေဟာ ထဲမှာ သိမ်းဆည်းထားတဲ့ Routing Table တွေနှင့် တိုင်ပင်ပြီးလုပ်ရတာဖြစ်တယ်။ ဒါကြောင့် IPv4 မှာ Routers တွေကို ထွက်ရာလမ်းကြောင်းဆိုပြီး Gateway လို့လည်းခေါ်ကြပါသေးတယ်။ ဒီ Routing Table Entries တွေကတော့ TCP/IP ကို Initialize (စဦးအခြေအနေသတ်မှတ်ခြင်း) လုပ်လိုက်တဲ့အချိန်မှာပင် Default အရ တည်ဆောက်ပြီးဖြစ်ပါတယ်။ ဒါပေမယ့် သိရမှာက ဒီ Entries တွေကို အလိုအလျောက် ထည့်သွင်းလို့ရသလို၊ လူကနေ Manually လည်းရိုက်ထည့်လို့ရပါတယ်။

ပုံ ၅.၁



၅.၂ Direct နှင့် Indirect Delivery ပေးပို့ခြင်းနည်း ၂ နည်း

IP Packet တွေကိုပေးပို့တဲ့နေရာမှာ အောက်မှာဖော်ပြထားတဲ့နည်းလမ်း ၂ လမ်းထဲက တစ်နည်းနည်းကိုသုံးကြရပါတယ်။ ဒီလိုမှသာလျှင် ၎င်း IP Packet တွေဟာနောက်ဆုံးရည်ရွယ်ရာ၊ သို့မဟုတ် ကြားကနေတစ်ဆင့်ထပ်ပို့ပေးမယ့် IP Router ဆီကိုရောက်သွားကြမှာဖြစ်ပါတယ်။

ဒီနည်းလမ်း ၂ လမ်းက တော့–

၁။ Direct Delivery (တိုက်ရိုက်ပေးပို့ခြင်း) နှင့်

၂။ Indirect Delivery (တစ်ဆင့်ခံပေးပို့ခြင်း) တို့ပဲဖြစ်ပါတယ်။

၅.၃ Direct Delivery အကြောင်း

Direct Delivery ဆိုတာကတော့ Subnet နှင့် တိုက်ရိုက်ချိတ်ဆက်ထားတဲ့နောက်ဆုံး ပေးပို့ရမယ့်နေရာကို Host မှတိုက်ရိုက်ပေးပို့ခြင်း သို့မဟုတ် ၎င်းနောက်ဆုံး နေရာသို့ရောက်ဖို့ တစ်ဆင့်ပဲလိုတော့တဲ့ Router ကနေ ပေးပို့ခြင်းဖြစ်တာကြောင့် ၎င်းကို ပေးပို့တဲ့ Host နှင့် IP Router တွေမှာ ဒီဖြစ်စဉ်တွေကိုတွေ့ရမှာဖြစ်ပါတယ်။ ဒါကသိပ်ကို ရိုးရှင်းပါတယ်ဗျာ။ သင်အိမ်ကနေ အလုပ်ကိုသွားတယ်။ အိမ်ကနေ Bus ကားတစ်ဆင့်ပဲစီးရတယ်။ ရုံးကိုရောက်သွားတယ်။ ဒီနေရာမှာ အိမ်က Sending Host၊ ရုံးက Final Destination Host နှင့် Final Destination အကြား တိုက်ရိုက် Bus ကားစီးသွားတာ၊ လမ်းမှာ Bus ကားပြောင်းစီးတာမဟုတ်ဘူး။ ဒါဟာ Direct Delivery ဖြစ်ပါတယ်။ နောက်တစ်မျိုးရှင်းပြမယ်။ သင်ကရုံးကိုလာတယ်။ တာမွေမှာကားပြောင်းစီးရတယ်။ ဒါတင်ပဲလားဆိုတော့ မဟုတ်သေးဘူး။ လှည်းတန်းမှာ တစ်ခါကားပြောင်းစီးရသေးတယ်။ ပြီးမှ ရုံးကိုရောက်တာ။ ဒီတော့ လှည်းတန်းနှင့် ရုံးကတိုက်ရိုက်ဆက်သွယ်ထားတာဖြစ်တယ်။ ပြောရရင် လှည်းတန်းသည် Router၊ တာမွေသည် Router၊ ဒါမှမဟုတ် နောက်ဆုံး Final Destination က လှည်းတန်း Router ကနေလာတာပါ။ ဒါကြောင့် ဒါကြောင့် လှည်းတန်း Router နှင့် သင့်ရုံးသည် Direct Delivery ဖြစ်ပါတယ်။

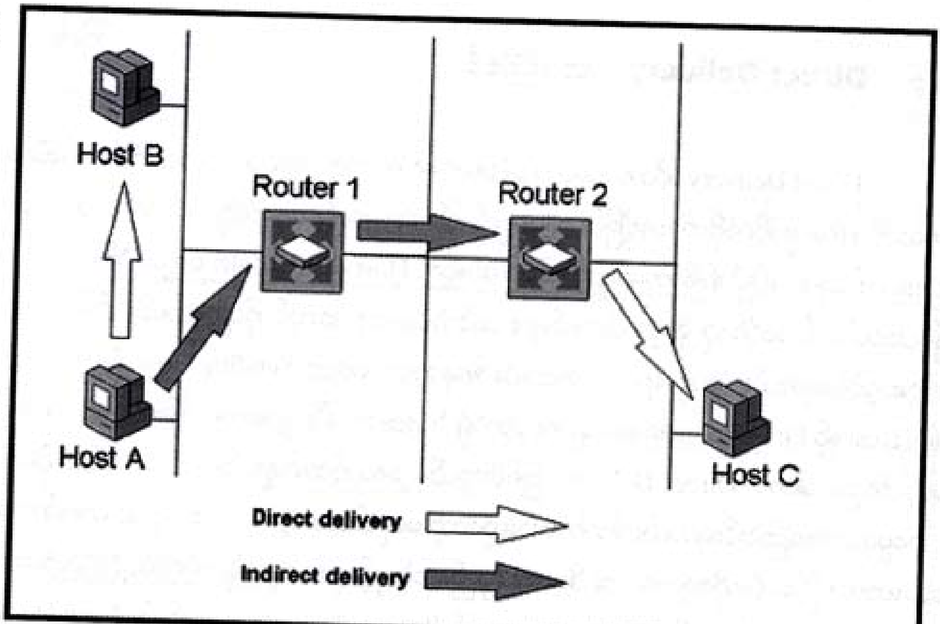
၅.၄ Indirect Delivery အကြောင်း

IP Node က Packet တွေကို တစ်ဆင့်ခံ Node ဆီကိုပို့ပေးခြင်းကို Indirect Delivery လို့ ခေါ်ပါတယ်။ ဒီနေရာမှာ IP Node ဆိုတာ ခုနကပြောသလိုပဲ ပေးပို့တဲ့ Sending Host ဒါမှမဟုတ်၊ IP

Router ပဲဖြစ်ပါတယ်။ တစ်ဆင့်ခံ Node ဆိုတာ IP Router ပဲဖြစ်ပါတယ်။ အပေါ်ကရှင်းပြတဲ့အတိုင်းပြန်ရှင်းပြမယ်။ အိမ်ကနေထွက်လာ တာမွေကိုရောက်လာ။ တာမွေကနေကားပြောင်းစီးတော့ လှည်းတန်းကိုရောက်ပေါ့။ ရှိရှိ လှည်းတန်းကနေကားပြောင်းစီးတော့ ၉း၀၀ ကျုံးကိုရောက်ပေါ့ ရှိရှိ။ ဪ အရေးထဲ Dance နေပြန်ပြီ။ ကဲထားပါ။ Direct Delivery ဆိုတာကျတော့ လှည်းတန်းကနေ ရုံးကိုပြောတာ။ Indirect Delivery ဆိုတာ အိမ်ကနေ တာမွေ၊ တာမွေကနေ လှည်းတန်း။ ဒါ Indirect Delivery ပဲဖြစ်ပါတယ်။ Final ရောက်ရမယ့် Destination က Subnet မှာတိုက်ရိုက်ချိတ်ဆက်ထားတာမဟုတ်တာကြောင့် Router တွေကနေ တစ်ဆင့်လာရခြင်းဖြစ်ပါတယ်။

ဒီနေရာမှာ သိရမှာက အစွန်းတစ်ဖက်ကနေ အဆုံးတစ်ဖက်ကိုသွားရမှာ။ IP Routing ဟာ Direct ရော၊ Indirect ရောပေါင်းပြီး Delivery လုပ်တာဖြစ်ပါတယ်။ ဥပမာအောက်ကပုံကိုကြည့်ပါ။

ပုံ ၅.၂



ဒီပုံမှာဆိုလို့ရှိရင် Host A ကနေ Host B ကို Packet တွေပေးပို့တဲ့နေရာမှာ Direct ပေးပို့ခြင်း Direct Delivery ဖြစ်ပါတယ်။ အကယ်၍များ Host B ကိုမပို့ပဲ Host C ကိုပေးပို့မယ်ဆိုရင်တော့ Host A ကနေ Router 1 ဆီကို Indirect Delivery ပို့ရမှာဖြစ်ပါတယ်။ Router 1 ကနေ Router 2 ဆီကိုလည်း Indirect Delivery ပဲဖြစ်ပါတယ်။ Router 2 ကနေ Host C ဆီကိုတော့ Direct Delivery ဖြစ်ပါတယ်။ အခုဆိုရင် သင်ခန်းစာဟာလည်း လွယ်နေတာကြောင့် Direct Delivery နှင့် Indirect Delivery ကို နားလည်လောက်ပြီထင်ပါတယ်။

Product of YOUTH

၅.၅ **IP Routing Table** အကြောင်း

Routing Table ဆိုတာ IP Node တိုင်းမှာရှိပါတယ်။ အဲ့ဒီ Routing Table မှာဘာတွေရှိကြသလဲဆိုတော့ IP Destinations တွေနှင့် ပတ်သက်တဲ့အချက်အလက်တွေ၊ Packet တွေဟာ အဲ့ဒီ Destination တွေဆီကို ဘယ်လိုရောက်နိုင်မလဲ။ Directly လား။ Indirectly လား စတဲ့အချက်အလက်တွေပါရှိပါတယ်။ ဒီနေရာမှာ Destination ဆိုတာ ကိုယ်ကလွဲရင် ကျန်တာ Destination ဖြစ်နိုင်တာပဲလေ။ အားလုံးသော IP Node တွေဟာ IP Routing ရဲ့အချို့သောအလုပ်တွေကို လုပ်ရတာကြောင့် IP Node တိုင်းမှာ Routing Table ရှိရပါတယ်။ ပြောရမယ်ဆိုရင် TCP/IP Protocol ကိုသုံးတဲ့ မည်သည့် Node မဆို Routing Table ရှိရပါတယ်။ ၎င်း Table မှာ Node တွေက သတ်မှတ်ထားတဲ့ Default Entries တွေအစဉ်လိုက်တိုင်းရှိ နေပါတယ်။ ဘာတွေလဲ။ ဒီနေရာမှာ သုံးထားတဲ့ Entries ဆိုတဲ့စကားကဘာကိုရည်ညွှန်းတာလဲ။ အပေါ်မှာပြောပြီးပြီ။ Routing Table ထဲမှာဘာတွေရှိသလဲ။ အဲ့ဒါတွေကို ချုံပြီးပြောတာ။ Entries ဆိုပြီး။ ကောင်းပြီ။ ဒီ Entries တွေက ဘယ်ကရောက်လာတာလဲ။ IP Node တွေက Default ထည့်ထားတာ ဒီ Table တွေမှာ အဲ့ဒါတွေအပြင် Administrator တွေက Manually ထပ်ထည့်ထားတာလည်းရှိနိုင်ပါတယ်။ ဒါမှမဟုတ် Automatic ပေါ့။ အလိုအလျောက် Table ထဲရောက်လာတဲ့ Entries တွေလည်းရှိနိုင်ပါတယ်။ အဲ့ဒါတွေက ဘာတွေလဲ။ IP Node တွေက၊ Router တွေကပို့လွှတ်တဲ့ Routing နှင့်ပတ်သက်တဲ့ အချက်အလက် Message တွေကို သူ့ဘာသာသူနားထောင်တာပေါ့။ အဲ့ဒီ Entries တွေက Table ထဲ အလိုအလျောက် ရောက်လာတာပေါ့။ ဒီတော့ အချက်နှင့်ပြန်ပြောပြရင် -

၁။ Node တွေက Default သတ်မှတ်တဲ့ Entries တွေ

၂။ Administrator က TCP/IP Tools တွေသုံးပြီး Manually ရိုက်ထည့်တာတွေ

၃။ Listen လုပ်ခြင်းကြောင့် အလိုအလျောက်ရောက်လာတာတွေပဲဖြစ်ပါတယ်။

IP Node ဟာ Packet တွေပေးပို့တဲ့အခါ Routing Table ကိုဘာအတွက်အသုံးပြုရသလဲဆိုတော့-

၁။ Next-Hop IP Address ကဘယ်သူလဲဆိုတာကြည့်ခြင်း

ဒါကိုရှင်းပြမယ်။ Direct Delivery မှာဆိုရင်တော့ Next-Hop IP Address ဆိုတာ IP Packet ထဲက Destination Address ကိုပြောတာဖြစ်ပြီး Indirect Delivery ဆိုရင်တော့ Next-Hop IP Address ဆိုတာ Router ရဲ့ IP Address ပဲဖြစ်ပါတယ်။ လွယ်ပါတယ်ဗျာ။ Direct ဆိုရင် ကိုယ်ဆင်းရမယ့်မှတ်

တိုင်ပေါ့။ Indirect ဆိုရင် ကားပြောင်းစီးရမည့်မှတ်တိုင်ပေါ့။ တာမွေလား၊ လှည်းတန်းလား၊ အခုနက ရှင်းပြခဲ့တယ်။ အရင်ပြောင်းစီးရမည့် မှတ်တိုင်က တာမွေဆို တာမွေပေါ့။ တာမွေကိုရောက်တော့ Next-Hop IP Address က လှည်းတန်းဖြစ်သွားရော။ နောက်ပြန်ရမည့် မှတ်တိုင်လေ။ Next လေ။ တာမွေကနေကြည့်ရင် လှည်းတန်းက Next ပေါ့။

၂။ Next-Hop Interface

သူကတော့ Packet တွေကိုပေးပို့မယ့် Interfaceဟာ Physical လား၊ Logical လား သတ်မှတ်မယ့် Interface ဖြစ်ပါတယ်။ အောက်မှာ အခေါ်အဝေါ်တွေကို ပြန်ရှင်းပြထားပေးတယ်။ ဖတ်ကြည့်လိုက်ရင် ပိုနားလည်သွားမှာပါ။

၅.၆ Routing Table Entries အကြောင်း

Routing Table ထဲကိုရောက်ရှိတဲ့၊ ထည့်သွင်းတဲ့ အကြောင်းအရာများကို Entry လို့ခေါ်ပါတယ်။ Routing Table ထဲက Entry တွေမှာ ပုံမှန်အားဖြင့်ရှိတတ်ကြတဲ့ Field တွေကိုတော့အောက်မှာ ဖော်ပြပေးထားပါတယ်။

၁။ Destination

IP Address ဒါမှမဟုတ် IP Address Prefix တစ်ခုဖြစ်ပါတယ်။

၂။ Prefix Length

သူကတော့ Destination မှာရှိတဲ့ Address တွေရဲ့ Address Range ပဲဖြစ်ပါတယ်။

၃။ Next-Hop

Packet ကိုပေးပို့ရမယ့် IP Address ဖြစ်ပါတယ်။

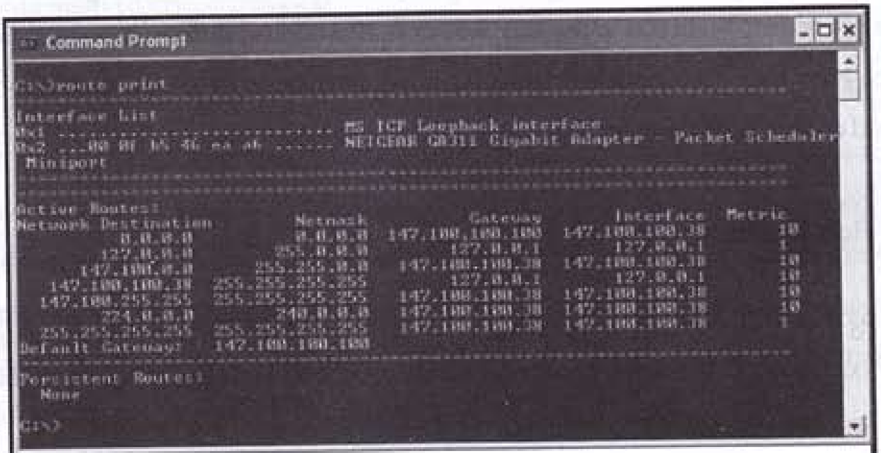
၄။ Interface

IP Packet ကိုပေးပို့ပေးမယ့် Network Interface ဖြစ်ပါတယ်။ ဥပမာ Router

၅။ Metric

Metric ဆိုတာကိုယ်သွားရမယ့်လမ်းကြောင်းမှာ Router ဘယ်နှစ်ဆင့်ခံထားသလဲ။ တနည်းအားဖြင့် Hop ဘယ်နှစ်ခုရှိသလဲဆိုတာကိုဖော်ပြတာဖြစ်ပါတယ်။ ဒီတော့ ကိုယ်သွားရမည့်လမ်းကြောင်းကို ဘယ်က နေသွားရင် အဆင်အပြေဆုံးဖြစ်မလဲ။ အနီးဆုံးဖြစ်မလဲဆိုတာကိုသိနိုင်တာပေါ့။ ဒီနေရာမှာ Hop ဆိုတာ ကားပြောင်းစီးရမယ့်နေရာ တစ်ဆင့်ခံကိုပြောတာ ရုံးကိုရောက်ဖို့တာမွေကနေ တစ်ဆင့်၊ လှည်းတန်းကနေ တစ်ဆင့် ကားပြောင်းစီးရမယ်။ ရန်ကင်းကနေဆို တစ်ဆင့်ပဲစီးရမယ်။ ဒါဆို ဘယ်ကသွားမလဲပေါ့။ အနီးဆုံး လမ်းကြောင်းကိုသိဖို့ Hops ဘယ်နှစ်ခုရှိသလဲဆိုတာကိုသိရမယ်။ Metric ဆိုတာ Hop ကိုဖော်ပြတာပါ။ ရည်ရွယ်ရာရောက်ဖို့ ကြားထဲမှာဖြတ်သွားရမယ့် Hops ကိုဖော်ပြတာဖြစ်ပါတယ်။

ပုံ ၅.၇



Routing Table ကိုတွေ့ရပုံ

၅.၇ **Routes** အမျိုးအစားများ

ဒီတစ်ခါပြောပြမယ့်အကြောင်းအရာကတော့ Routing Table Entries တွေကသိမ်းပေးထားတဲ့ Routes အမျိုးအစားများကို ဖော်ပြပေးထားပါတယ်။

၁။ Directly-Attached Subnet Routes

Subnet တွေမှာတိုက်ရိုက်ချိတ်ထားတဲ့ Node တွေရှိမယ်။ ဒီလို Subnets တွေအတွက် Route (လမ်းကြောင်း) တွေကို Directly-Attached Subnet Route လို့ခေါ်ပါတယ်။ ဒီ Route အမျိုးအစားမှာဆိုရင်

Next-Hop Field ဟာ Blank ကွက်လပ်တစ်ခုလည်းဖြစ်နိုင်သလို အဲ့ဒီ Subnet မှာရှိတဲ့ Interface (ဥပမာ Router) ရဲ့ IP Address လည်းဖြစ်နိုင်ပါတယ်။ ဆိုလိုတာက တိုက်ရိုက်ဆက်သွယ်မှုမှာ Next-Hop ဆိုတဲ့ တစ်ဆင့်ခံတွေမရှိကြဘူးလေ။ ဒါကြောင့် Next-Hop Field ဟာ Blank ဖြစ်နေနိုင်တယ်လို့ပြောတာပါ။

၂။ Remote Subnet Routes

ဒါကကျတော့ နံပါတ် ၁ နှင့် ဆန့်ကျင်ဘက်ဖြစ်ပါတယ်။ Subnet မှာ Node တွေဟာ တိုက်ရိုက်ချိတ်ဆက်ထားခြင်းမရှိဘူး။ ၎င်း Node တွေကိုသွားချင်ရင် Router တွေကနေတစ်ဆင့် ဖြတ်သန်းသွားရမယ်။ ဒီလို Subnets မျိုးအတွက် Router အမျိုးအစားကိုတော့ Remote Subnet Route လို့ခေါ်ပါတယ်။ ဒီလို Route မှာ Next Hop Field ဟာ အနီးနားက Router ရဲ့ IP Address ဖြစ်ပါတယ်။ ဥပမာ အိမ်ကထွက်လာတယ်။ Next Hop ကတာမွေပေါ့။ ဒီတာမွေ Router ရဲ့ IP ကိုပြောတာ။ တာမွေကိုရောက်ရင် Next Hop Field က လှည်းတန်း Router ပေါ့။

၃။ Host Routes

သွားရမယ့် IP Address ကိုပြောတာဖြစ်ပါတယ်။ ဥပမာ ဒီ Host ကိုသွားပါ။ ဟို Host ကိုသွားပါ။ ဒီလို သတ်သတ်မှတ်မှတ် IP Address တစ်ခုကိုပဲ Route လုပ်တာကို Host Route လို့ခေါ်တာဖြစ်ပါတယ်။

၄။ Default Route

သတ်မှတ်ထားတဲ့ Subnet Route ပဲဖြစ်စေ၊ Host Route ပဲဖြစ်စေ၊ မရှိတဲ့အခါမှာ ၎င်း Default Route ကိုသုံးပါတယ်။ ဒီတော့ Default Route မှာဆိုလို့ရှိရင် Next Hop ရဲ့ Address ဟာ ပုံမှန်အားဖြင့်တော့ Default Gateway သို့မဟုတ် Default Router ရဲ့ Address ပဲဖြစ်ပါတယ်။

၅.၈ **Static & Dynamic Routing** အကြောင်း

IP Packets တွေဟာ Network နှင့် Router တွေအကြား လွယ်ကူလျင်မြန်စွာ ထိရောက်စွာ Route လုပ်နိုင်ဖို့ အတွက် Routers တွေကသိကိုသိနေရမည့်အချက်တွေရှိပါတယ်။ အဲ့ဒါက အပေါ်မှာရှင်းပြခဲ့တဲ့ Remote Subnet Routes နှင့်ပတ်သက်တဲ့အကြောင်း ဒါမှမဟုတ် သေချာစွာ Setting ချထားသော Default Route နှင့်ပတ်သက်တဲ့အကြောင်းတွေပဲဖြစ်ပါတယ်။ ဒါကို မသိတဲ့ Router က ထိရောက်တဲ့Routing

လုပ်နိုင်မှာ မဟုတ်ပါဘူး။ ပိုဆိုးတာက Network ကကြီးလာလေ၊ Network Administrator တွေရင်ဆိုင်လာရတဲ့ ကိစ္စတစ်ခုရှိတယ်ဗျ။ အဲ့ဒါက Routing Tables ကို ဘယ်လိုကိုင်တွယ်ထိမ်းသိမ်းကြ မလဲပေါ့။ ဒီ IP Router တွေမှာရှိတဲ့ Routing Table တွေကိုကောင်းစွာ ထိန်းသိမ်းနိုင်မှ IP Traffic တွေက အကောင်းဆုံးလမ်းကြောင်းကနေ သွားနိုင်မှာဖြစ်သလို Fault Tolerance လည်းလုပ်နိုင်မှာဖြစ်ပါတယ်။ ဆိုလိုတာက – "ဒီအချိန်ဆို ဒီလမ်းကကျောင်းဆင်းချိန်ကားပိတ်တယ်။ ဟိုဖက်ကသွားမယ်။" စသဖြင့်ပေါ့။

ဒီတော့ကား၊ အခုဘာပြောချင်သလဲဆိုတော့ ဒီ Routing Table Entries တွေကို ဘယ်လိုထိမ်းသိမ်းရသလဲ။ ထိန်းသိမ်းနည်းတွေကရော။ ဟုတ်ကဲ့ပါ။ နည်းလမ်းကတော့ ၂ နည်းရှိပါတယ်။ အဲ့ဒါတွေကတော့–

၁။ Manually (လူကလုပ်ပေးရခြင်း)

ကနဦးသိရမှာက Network Administrator တွေက Manually ရိုက်ထည့်မှ ပြောင်းလဲမှုဖြစ်တယ်။ မဟုတ်ရင် မပြောင်းဘူးဆိုတဲ့ Routing Table ပါရှိတဲ့ Router မျိုးတွေကို Static IP Router လို့ခေါ်ပါတယ်။ Static Routing တွေမှန်သမျှဟာ Network Administrator တွေကနေမှ Routing Table တွေကို Manually Maintain လုပ်ရမှာဖြစ်ပါတယ်။ Static Routes တွေဟာ Fault Tolerance လည်းမပါရှိသလို Remote Routes လည်းလုပ်နိုင်ခြင်းမရှိပါဘူး။ ဆိုတော့ အကယ်၍များ Static Router တစ်ခုက Fail ဖြစ်ခဲ့မယ်ဆိုရင် သူ့အနီးအနားက Router ဟာ ဘာကြောင့် သူ Fail ဖြစ်သွားရတာလဲဆိုတာကိုလည်း Detect မလုပ်ပါဘူး။

၂။ Automatically (အလိုအလျောက်)

Dynamin IP Routers တွေကျတော့ ဒီလိုဗျ။ Routers တွေ အချင်းချင်း Routing Information ကိုဖလှယ်နိုင်ကြတယ်ဗျ။ အဲ့လိုဖလှယ်လိုက်တာနဲ့ Routing Tables တွေဟာ အလိုအလျောက် Change သွားကြပါတယ်။ Dynamin Routing က Routing Protocol တွေဖြစ်ကြတဲ့–

၁။ RIP ဆိုတဲ့ Routing Information Protocol နှင့်

၂။ OSPF ဆိုတဲ့ Open Shortest Path First တို့ကိုအသုံးပြုပြီး Routing Tables တွေက Dynamically Update လုပ်နိုင်ပါတယ်။ Dynamic Routes တွေဟာ Remote Route ကိုလုပ်နိုင်စွမ်း ရှိတဲ့အပြင် Fault Tolerance ကိုလည်းလုပ်နိုင်စွမ်းတယ်။ အကယ်၍များ Dynamin Route ဟာ Fail ဖြစ်ခဲ့မယ်ဆိုရင်တော့

အနီးအနားက Router က ဘာကြောင့် ဖြစ်ရတယ်ကို Detect လုပ်ပါတယ်။ ပြီးတာနဲ့ Network မှာရှိတဲ့ အခြားသော Router တွေဆီကို Routing Information တွေပြောင်းလဲပြီးပို့လိုက်တာပဲဖြစ်ပါတယ်။

ဒီနေရာမှာ Dynamic Routing နှင့်ပတ်သက်ပြီး ထပ်ပြောရမယ်ဆိုလို့ရှိရင် –

၁။ Dynamic Routing ဟာ Routing Table Entries တွေကို အလိုအလျောက် Update လုပ်ပါတယ်။ ဒီတော့ အဲ့ဒီလို Routing Table တွေကို Dynamically Configure လုပ်ပေးနိုင်တဲ့ Router တွေကို Dynamic Router လို့ခေါ်တာပေါ့။

ပုံ ၅.၄

Router ကိုတွေ့ရစဉ်

၂။ Dynamic Routers တွေဟာ Routing Table တွေကို Routing Protocol တွေသုံးပြီး အလိုအလျောက် တည်ဆောက်ခြင်း၊ Maintain လုပ်ခြင်းတို့ပြုလုပ်ကြပါတယ်။ အဲ့ဒီ အပြင် Routing Information တွေပါတဲ့ အမြဲတမ်း အချိန်ပိုင်းအလိုက် ဖြစ်ပေါ်နေသော Message များမှတစ်ဆင့် သို့မဟုတ် လိုအပ်မှုဖြစ်ပေါ်လေ့ရှိသော Message များမှလည်း Routing Information တွေကို ရယူကာတည်ဆောက်နိုင်ပါတယ်။ Router တွေဟာ ပုံမှန်အားဖြင့်တော့ ကနဦး သတ်မှတ်ထားတဲ့ Configuration တွေကလွဲလို့ အနည်းငယ်တော့ ပြန်ပြီး Maintanance လုပ်ရတာပဲ။ ဆိုလိုတာက ကနဦး Setting တွေလုပ်ထားတာလည်း လုပ်ထားတာကတစ်ပိုင်း၊ Routers တွေဟာ လုပ်နေစဉ်မှာ Ongoing ပေါ့။ Setting တွေပြန်သတ်မှတ်ရတာမျိုးရှိတတ်တယ်။ ဘယ်လောက်ပြန်ပြင်ဖို့လိုသလဲဆိုတော့ Network အရွယ်အစားပေါ်မူတည်ပြီးပြောင်းလဲတယ်။ ကြီးရင်များတယ်။ ငယ်ရင်နည်းတယ်။ ဒါပဲပေါ့။

၃။ ဒီတော့ကား ပြန်စဉ်းစားကြည့်လိုက်။ Dynamic Router ကိုသုံးတာပိုကောင်းတာပေါ့။ ဆိုလိုတာက Router တွေဟာ ကနဦး Configuration လုပ်ပြီးရင် ဘာမှ ဆက်လုပ်စရာမလိုဘူးဆိုအကြောင်းမဟုတ်ဘူး။

ဆိုလိုတာက တစ်ခါပဲ အပင်ပန်းခံရမယ်။ အခုဟာက ကနဦး သတ်မှတ်ချက်တွေအပြင် Running ဖြစ်နေစဉ် Ongoing Maintain လုပ်ရတယ်ဆိုတော့ Network သေးသေးကြီးကြီး ကိုယ်ကလိုက်ပြင်ပေးရတော့မယ်။ ဒီတော့ ဒီလိုလိုက်ပြင်ပေးစရာမလိုတဲ့ Dynamic Router ကိုပဲရွေးချယ်ရမှာပဲ။

၄။ IPv 4 မှာ အသုံးများတဲ့ Routing Protocol တစ်မျိုးကိုဖော်ပြရမယ်ဆိုရင် RIP, OSPF နှင့် BGP4 ဆိုတဲ့ Border Gateway Protocol တို့ပဲဖြစ်ကြပါတယ်။ သူတို့ကို ဘယ်နေရာမှာအသုံးပြုကြသလဲ။ Routers တစ်ခုနှင့်တစ်ခုကြားပေါ့။ နောက်ပြီး Network တွေမှာ Traffic တွေကျပ်လာတဲ့အခါတွေမှာပေါ့။ ဒီတော့ကား ကျွန်တော်တို့တွေဟာ Routing Protocol တွေကို ရွေးချယ်တဲ့နေရာမှာ သေသေချာချာကို စဉ်းစားဖို့လိုတယ်။ ဘာတွေကိုစဉ်းစားရမှာလဲ။ သူဟာဘယ်လောက်တောင် Sense လုပ်နိုင်သလဲ။ တစ်ခုခုကို အမှားဖြစ်ခဲ့ရင် ဘယ်လောက်တောင်မြန်မြန် Recover လုပ်နိုင်သလဲ။ နောက်တစ်ခုက Router ကနေ Routing Information တွေကို Network တစ်လျှောက်ဘယ်လိုပို့လွှတ်စေမှာလဲ။ ဒီအချက်တွေပေါ်မူတည်ပြီး ဘယ်လို Routing Protocol သုံးမလဲစဉ်းစားရမှာဖြစ်ပါတယ်။

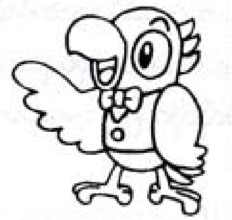
၁၁.၉ Stable State အကြောင်း

ဒီတစ်ခါ Network Converged ဆိုတဲ့အခေါ်အဝေါ်ကိုရှင်းပြမယ်။ Network မှာရှိတဲ့ အားလုံးသော Router တွေရဲ့ Routing Table တွေမှာ Routing Information တွေပြည့်စုံမှန်ကန်စွာရှိလာပြီဆိုမှ Network ဟာ Stable ဖြစ်လာတာပါ။ ဒါဟာ Converged ဖြစ်တဲ့အချိန်ပဲပေါ့။ ဆိုလိုတာက Network တစ်ခုလုံးဟာ အတူတစ်ကွဖြစ်သွားပြီးလို့ အဓိပ္ပာယ်ရပါတယ်။ အဲ့ဒီ အချိန်ကျမှသာလျှင် Network မှာအားလုံးသော Packets တွေဟာ အကောင်းဆုံးလမ်းကြောင်းတွေနှင့် ပေးပို့ Route လုပ်နိုင်ကြမှာဖြစ်ပါတယ်။ Coverged မဖြစ်ခင် Routers တွေဟာ ဘယ် Router ကနေသွားရင် Final Destination ကို အနီးဆုံးဖြစ်မယ်ဆိုတာကို မသိကြသေးပါဘူး။ ဥပမာပေးပြီးရှင်းပြမယ်။

လူတစ်ယောက်က အိမ်မှာပဲ နေတယ်။ ဒါပေမယ့် သူ့အိမ်ရှေ့ကဖြတ်သွားတဲ့ သူတိုင်းကို ဘယ်က လာလဲ၊ ဘယ်ကိုသွားမလို့လဲ၊ ဒီလိုမေးခြင်းအားဖြင့် သူ့မှာ ဘယ်မှမသွားရဘဲနဲ့ ဒီမြို့မှာ ဘယ်အိမ်တွေ၊ ဘယ်လမ်းတွေရှိတယ်ဆိုတာသိလာတယ်။ တကယ်တမ်း သူသွားမယ့်အခါကျ ဘယ်ကိုသွားချင်တယ်ပေါ် မူတည်ပြီး။ ခုနက သူ Learn လုပ်ထားတယ်။ ဘယ်အိမ်ဟာ ဘယ်လမ်းမှာ ရှိတယ်၊ ဘယ်လိုသွားရင် ရောက်တယ်ဆိုတာ သူ Learn လုပ်ထားတယ်။ ဒီတော့ သူဘယ်ကိုသွားချင်တယ်ပေါ်မူတည်ပြီး သူဘယ်လို သွားရမယ်ဆိုတာ သူကောင်းကောင်းသိသွားတယ်။ ဒါကိုပြောတာ။ Network ဟာ Converged ဖြစ်တဲ့အခါ Router တွေဟာ သူတို့သွားရမယ့်နေရာကို ဘယ်ကနေသွားရင် အနီးဆုံးလည်းဆိုတာကို သိလာကြတာပေါ့။

ပုံ ၅-၅

အနော်က ကြက်တူရွေးဆိုတော့ သိတယ်မဟုတ်လား။ ဖြတ်သွားသမျှလူ စပ်စုတာလေ။ တော့လူ ဘယ်ကလာလို့ ဘယ်ကိုသွားမလို့လဲ လို့မေးလိုက်ရင် သူဘယ်ကလာတာ ရော ဘယ်ကိုသွားမယ်ဆိုတာကိုပါသိသွားတယ်လေ။ ဒါကို Router အနေနဲ့ပြောရင် Learn လုပ်တယ်ခေါ်တာပေါ့။



၅.၁၀ Unstable State အကြောင်း

ဒီတစ်ခါ Network Converged မဖြစ်လို့ Network တာမတည်ငြိမ်ဘူး ဖြစ်တယ်ဆိုတဲ့Unstable State အကြောင်းပြောပြပါမယ်။ အကယ်၍ Router ပဲဖြစ်ဖြစ်၊ ချိတ်ဆက်မှုပဲဖြစ်ဖြစ်၊ Final ဖြစ်သွားပြီဆိုရင် Network က Routing Table တွေကို ပြန် Update လုပ်ပြီး Configured ပြန်လုပ်ရပါတယ်။ Network ကြီးတစ်ခုလုံးကိုပေါ့။ အဲ့ဒီလို Network ကြီးတစ်ခုလုံးကို Converged ပြန်လုပ်နေပြီး Network ဟာ Converged မဖြစ်ခင်အချိန်ထိဟာ Unstable State ဖြစ်နေတယ်။ Network ဟာ မတည်ငြိမ်ဘူး ဖြစ်နေတယ်ပေါ့။ ဒီလိုဖြစ်နေတဲ့အချိန်တွေကို Convergence Time လို့ခေါ်ပါတယ်။ ဒီအချိန်တွေက တနည်းအားဖြင့် ဒီ Convergence Time ဟာ ဘယ်လောက်ကြာမြင့်မယ်ဆိုတာ အတိအကျမရှိပါဘူး။ ဘယ်ပေါ်မူတည်သလဲဆို Routing Protocol ပေါ်မူတည်ပါတယ်။ နောက်ပြီး Failure ဖြစ်တဲ့အပေါ်မှာ လည်းမူတည်ပါတယ်။ ဘယ်လို Failure မျိုးလည်းပေါ့။ ဥပမာ - Router က Fail ဖြစ်တာလား။ ချိတ်ဆက်မှု Link ကပဲ Fail ဖြစ်တာလားပေါ့။ အဲ့ဒီပေါ်မူတည်ပြီး Convergence Time က ကြာချင်ကြာမယ်။ မြန်ချင် မြန်မယ်။

၅.၁၁ IPv4 Routing အကြောင်း

အခုပြောပြမှာက IP v4 Routing နှင့် ပတ်သက်တဲ့အကြောင်းအရာတွေပဲဖြစ်ပါတယ်။ ဒါဆိုရှေ့က ပြောခဲ့တဲ့ အကြောင်းအရာတွေကရော။ ရှေ့ကပြောခဲ့တဲ့အကြောင်းအရာတွေက Routing နှင့်ပတ်သက်တဲ့ ဘုံ General အကြောင်းအရာတွေဖြစ်ပါတယ်။ ဒီတော့ IPv4 Routing ရှိမယ်ဗျာ။ IPv6 Routing ရှိမယ်ဗျာ။ ဒီတော့ အခုရှင်းပြမှာက IPv4 Routing နှင့်ပတ်သက်တဲ့အကြောင်းအရာတွေပဲဖြစ်ပါတယ်။ ဒီစာအုပ်မှာ IPv6 နှင့်ပတ်သက်တဲ့အကြောင်းအရာတွေကိုတော့ ထည့်မပေးထားသေးပါဘူး။

အသုံးပြုတဲ့ Windows ဟာ TCP/IP Protocol ကို ပံ့ပိုးတယ်ဆိုရင်ဖြင့် IPv4 Routing Table ကိုအသုံးပြုပြီးဖြစ်ပါတယ်။ တစ်ချို့အကြောင်းအရာတွေကတော့ ရှေ့မှာရှင်းပြခဲ့ပြီးတဲ့ အကြောင်းအရာတွေလိုပါပဲ။ Routing Tables ဟာ Packets တွေ Destination ကိုရောက်ဖို့ Destination နှင့်ပတ်သက်တဲ့ Information တွေကိုသိမ်းထားရတယ်တို့၊ ဒီ Tables တွေမှာလည်း Node တွေကနေသတ်မှတ်ထားတဲ့ Configuration တွေဟာ Default Entries အဖြစ်ရှိနေတယ်ဆိုတာတို့၊ အဲ့ဒီ Entries တွေကို TCP/IP Tools ဖြစ်တဲ့ Route.exe နှင့်ထည့်လို့ရတယ်ဆိုတာတို့ ဒါမှမဟုတ်လည်း Routing Protocol နှင့် Dynamically ထည့်လို့ရတယ်ဆိုတာတို့ပေါ့ဗျာ။

Packets တွေဟာပေးပို့တဲ့အခါမှာ Destination ကိုအသုံးပြုပြီး ဆုံးဖြတ်ရတဲ့ကိစ္စ ၂ ခုရှိပါတယ်။ အဲ့ဒါကတော့-

၁။ Next-Hop IPv4 Address နှင့်
၂။ Next-Hop Interface တို့ပဲဖြစ်ပါတယ်။

ရှေ့မှာတော့ဖော်ပြခဲ့ပြီးပြီ။ ဒါပေမယ့်ပြန်ပြောပြမယ်။

Next-Hop IPv4 Address ဆိုတာ-

- Direct Delivery ဆိုရင် Packet ထဲက Destination IPv4 Address
- Indirect Delivery ဆိုရင် Router ရဲ့ IPv4 Address ဖြစ်ပါတယ်။

Next-Hop Interface ဆိုတာ-

Physical Interface ဖြစ်ချင်ဖြစ်မယ်။ Logical Interface ဖြစ်ချင်ဖြစ်မယ်။ Physical ဆိုတာ Network Card ဒါမှမဟုတ်၊ Logical ဆိုတာ Tunneling Interface စသဖြင့်ဖြစ်ပါတယ်။

အဲ့ဒီလို Next-Hop Address နှင့် Interface ကို စုံစမ်းသိရှိဆုံးဖြတ်ပြီးတဲ့အခါ ၄င်း Packet ကို TCP/IP ရဲ့ အစိတ်အပိုင်းတစ်ခုဖြစ်တဲ့ Address Resolution Protocol (ARP) ကိုပေးပို့လိုက်ပါတယ်။

၅.၁၂ IPv4 Routing Table ဝါအကြောင်းအရာများ

Windows ရဲ့ TCP/IP အတွက် IPv4 Routing Table Entry တွေမှာပါရှိသော Field များကို ဖော်ပြရမယ် ဆိုရင် –

၁။ Destination

၂။ Network Mask

၃။ Next-Hop

၄။ Interface

၅။ Metric တို့ပဲဖြစ်ကြပါတယ်။ သူတို့နှင့်ပတ်သက်တာတွေကို ရှေ့မှာပြောပြခဲ့ပြီးဖြစ်လို့ ထပ်မပြောတော့ပါဘူး။ ဒီအကြောင်းအရာတွေကိုမြင်ချင်ရင် Route Print ဆိုတဲ့ Command ကို သုံးပြီးကြည့်လို့ရပါတယ်။ ဒါကို နောက်မှာ ဥပမာနှင့်ပြောပြပါ့မယ်။

နောက်တစ်ခုက Routing Table Entries တွေမှာပါတဲ့ Routes အမျိုးအစားတွေဖြစ်ပါတယ်။ သူတို့တွေကတော့–

၁။ Directly Attached Subnet Route

၂။ Remote Subnet Route

၃။ Host Route နှင့်

၄။ Default Route တို့ပဲဖြစ်ကြပါတယ်။ ဒီနေရာမှာလည်း အရင်ကရှင်းပြထားပြီးသား အတိုင်းမို့ထပ်မရှင်းပြတော့ပါဘူး။ ပြောစရာက Host Route မှာ Network Mask က 255.255.255.255 ဖြစ်ပါတယ်။ Default Route ကျတော့ Destination က 0.0.0.0 ဖြစ်ပြီး Network Mask ကလည်း 0.0.0.0 ဖြစ်ပါတယ်။ ဒါလေးကလွဲလို့ ရှေ့ကပြောတဲ့အကြောင်းအရာတွေနှင့် အတူတူပဲဖြစ်ပါတယ်။

၅.၁၃ Route Determination Process အကြောင်း သို့မဟုတ် ဘယ်လမ်းကြောင်းကသွားမလဲ

Route Determination Process ဆိုတာ –

Packet တွေကို Forward လုပ်ဖို့ရာ ဘယ် Routing Table Entry ကို အသုံးပြုရမလဲဆိုတာကို

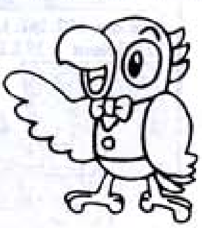
အောက်ပါအချက်များကို သုံးပြီးဆုံးဖြတ်ရပါတယ်။ ဒီ ဖြစ်စဉ်ကို Route Determination Process လို့ခေါ်ပါတယ်။

၁။ နံပါတ် (၁) အနေနဲ့ကတော့ Routing Table ထဲမှာရှိတဲ့ Entry တစ်ခုချင်းစီအတွက် IPv4 ဟာ Destination IPv4 Address နှင့် Network Mask ကို Logical AND ပါတယ်။ ဒီအကြောင်းက Subnetting မှာပြောခဲ့ပြီးပါပြီ။ အဲ့ဒီလို Destination Network Address နှင့် Network Mask ကို Logical AND လိုက်တယ်ဆိုရင် Subnet Address ထွက်လာပါလိမ့်မယ်။ ဒီတော့မှ ဒီ Address နှင့် ဒီ Entry ဟာ ဘယ် Subnet မှာရှိနေလည်းသိမှာပေါ့။ အဲ့ဒီလို တွက်လိုက်လို့ ထွက်လာတဲ့အဖြေကို Destination Field နှင့်တိုက်ဆိုင် စစ်ဆေးခြင်း ပြုလုပ်ပါတယ်။

၂။ IPv4 က အဲ့ဒီလို တိုက်ဆိုင်စစ်ဆေးပြီး သကာလ Longest Match ဖြစ်တဲ့ Route ကိုရွေးချယ်လိုက်ပါတော့တယ်။ ဒီနေရာမှာ Longest Route ကို ရှင်းပြမှဖြစ်မှာပါ။ လောလောဆယ်တော့ ဆက်ပြောရမယ်ဆိုလို့ရှိရင် ပထမအဆင့် ၁ မှာ Subnet ကိုရှာလိုက်တယ်။ ရတဲ့ Subnet နှင့် Destination နှင့် တိုက်ဆိုင်စစ်ဆေးတဲ့အခါ အဖြေဟာတစ်ခုမကတိုက်ဆိုင်နေရင် Longest Match ဖြစ်တဲ့ Route ကိုရွေးပါတယ်။ ဘာလို့ Longest Match ဖြစ်တဲ့ Route ကိုရွေးရတာလဲ။ ပြီးရင်ရှင်းပြမယ်။ အဲ့လို Longest Match ဖြစ်တဲ့ Route ကလည်း တစ်ခုမက ရှိခဲ့မယ်ဆိုရင် Router ဟာ Lowest Metric ဖြစ်တဲ့ Route ကိုရွေးပါတယ်။ Lowest Metric ကအကောင်းဆုံးလမ်းကြောင်းပဲပေါ့။ အဲ့ဒါမှ တစ်ခါ Lowest Metric ပါတူနေခဲ့ရင် IPv4 ဟာ Binding Order မှ ပထမဖြစ်တဲ့၊ ပထမဦးစွာ Bind လုပ်ထားတဲ့ Interface ကိုပဲရွေးချယ်လိုက်ပါတော့တယ်။

ပုံ ၅.၆

- ပထမ Subnet ကိုရှာတယ်။
- တစ်ခုမကတိုက်ဆိုင်နေရင် Longest Match Route ကိုရွေးတယ်။
- အဲ့ဒါမှ Longest Match ကတိုက်နေရင် Lowest Metric ဖြစ်တဲ့ Route ကိုရွေးပါတယ်။
- Lowest Metric ပါတိုက်နေခဲ့ရင် Binding Order ကိုကြည့်ပြီးရွေးချယ်ပါတယ်။



၅. ၁၄ **Longest Match** ရှင်းလင်းချက်

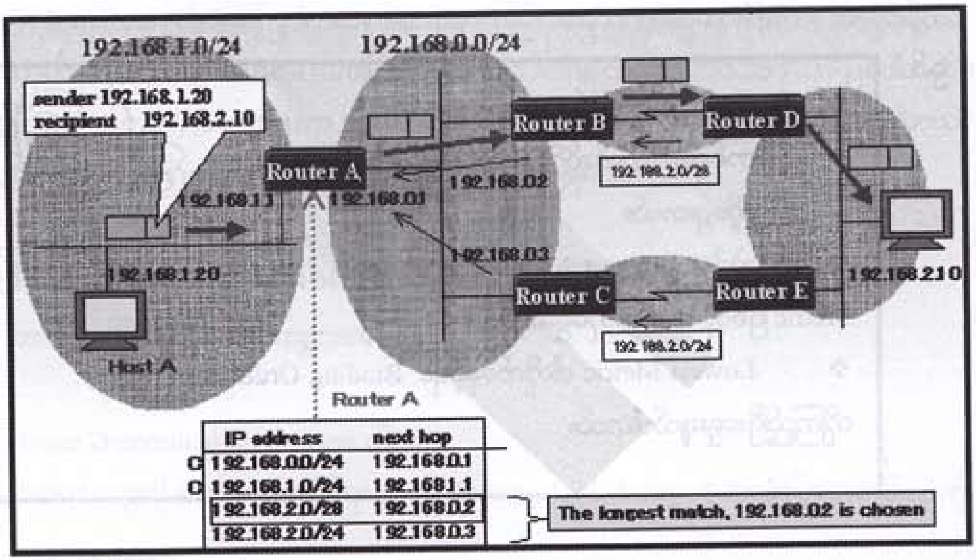
Longest Match ဆိုမှမဟုတ် Longest Prefix Match ကို Maximum Prefix Length Match လို့လည်းခေါ်ပါတယ်။ အဓိပ္ပာယ်ကတော့ Subnet Mask မြင့်တာကိုပြောတာဖြစ်ပါတယ်။ ဥပမာ Address က 192.168.20.19 ဆိုကြပါစို့။ ဒီတော့ Router က 192.168.20.19 ကို သွားဖို့လမ်းကြောင်းရွေးတဲ့အခါ အထက်မှာဖော်ပြသလို အဆင့် ၂ ဆင့်လုပ်ရပါတယ်။ ဒီ ၂ ဆင့်ထဲက ပထမ အဆင့်က Network Address နှင့် Subnet Mask Longical AND တယ်လို့ ကျွန်တော်အပေါ်မှာပြောခဲ့ပါတယ်။ ရတဲ့အဖြေကို တိုက်ဆိုင်စစ်ဆေးတယ်လို့ပြောခဲ့ပါတယ်။ ရတဲ့အဖြေက Subnet Address ဖြစ်ပါတယ်။ ဒီတော့ 192.168.20.19 ကို အဖြေရှာလိုက်တော့ -

192.168.20.16/28 နှင့်

192.168.0.0/16 ကိုသွားတွေ့တယ်ဆိုပါစို့။

ဒီတော့ Router က 192.168.20.19 ကိုသွားဖို့ 192.168.20.16/28 ကနေလည်းသွားလို့ရတယ်။ 192.168.0.0/16 ကနေ လည်းသွားလို့ရတာဖြစ်ပါတယ်။ ဒီနေရာမှာ Longest Prefix က /28 ဖြစ်ပါတယ်။ /28 က /16 နှင့် ယှဉ်လိုက်ရင် Highest Prefix ဖြစ်ပါတယ်။ ဒါကြောင့် /28 သည် Longest Match ဖြစ်ပါတယ်။ ဒီတော့ 192.168.20.19 ကို Router က Route လုပ်ဖို့ 192.168.20.16/28 ကိုရွေးချယ်ပါလိမ့်မယ်။

ပုံ ၅.၇



ဒီပုံမှာဆိုလို့ရှိရင် ပေးပို့သူ Sender က 192.168.1.20 ဖြစ်ပါတယ်။ လက်ခံမယ့်သူက 192.168.2.10 ဖြစ်ပါတယ်။ ဒီတော့ အထွက် Router မှာ Routing Table ရှိပါတယ်။ အဲ့ဒီ Table ကိုကြည့်လိုက်ရင် 192.168.2.10 ဆိုတဲ့ လက်ခံမယ့်သူဟာ 192.168.2.0/28 နှင့် 192.168.2.0/24 အတွင်းမှာရှိတာကြောင့် ပေးပို့သူဖက်က Packet ဟာ ဘယ်လမ်းကြောင်းကလာလာ လာလို့ရပေမယ့် Longest Match ဖြစ်တဲ့ 192.168.2.0/28 ကနေပဲ လာမှာဖြစ်ပါတယ်။

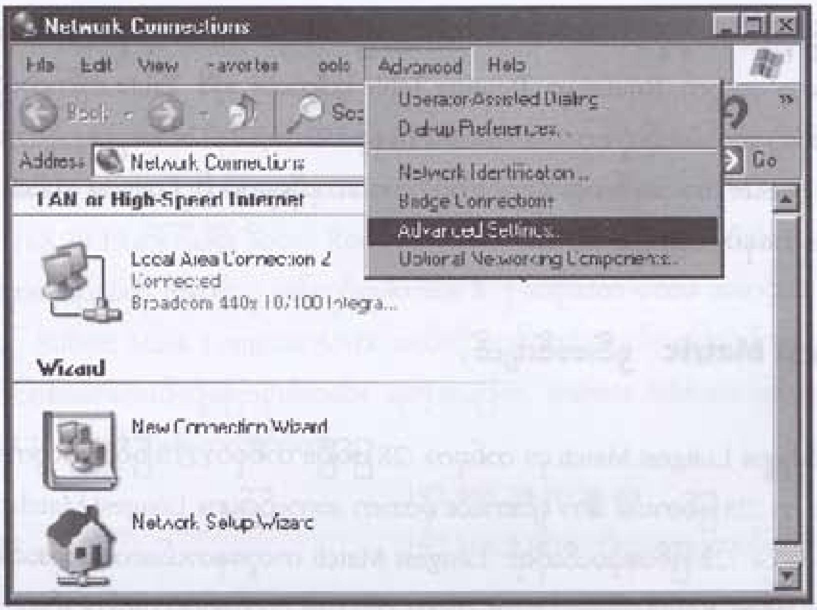
၅.၁၅ **Lowest Metric** ရှင်းလင်းချက်

အကယ်၍များ Longest Match မှာ တစ်ခုက /28 ဖြစ်ပြီး၊ တစ်ခုက /16 ဖြစ်တဲ့အတွက်ကြောင့် Longest Match က /28 ဖြစ်တယ်။ ဒါက ရှင်းတယ်။ ခုဟာက အကယ်၍များ Longest Match က /28 နောက်တစ်ခုကလည်း /28 ဖြစ်နေခဲ့မယ်ဆိုရင် Longest Match ကတူနေတယ်လေ။ ဒီလိုအချိန်မျိုးမှာ Longest Metric ဖြစ်တဲ့ Route ကိုရွေးပါတယ်။ ဆိုတာ ကိုသွားဖို့ ဘယ်နှစ်ခါကားပြောင်းစီးရသလဲ။ ၂ ခါလား၊ ၃ ခါလား။ ၂ ခါဆိုရင် အကြိမ်အရေအတွက် နည်းမယ်။ ဒါဆို ၂ ခါပဲရှိတဲ့ Metric ဟာ Lowest Metric ဖြစ်ပါတယ်။ ဒီတော့ Longest Match ချင်းတူရင် Lowest Metric ဖြစ်တဲ့ Route ကိုရွေးမှသာ ဒါအကောင်းဆုံး Best Route ဖြစ်မှာဖြစ်ပါတယ်။

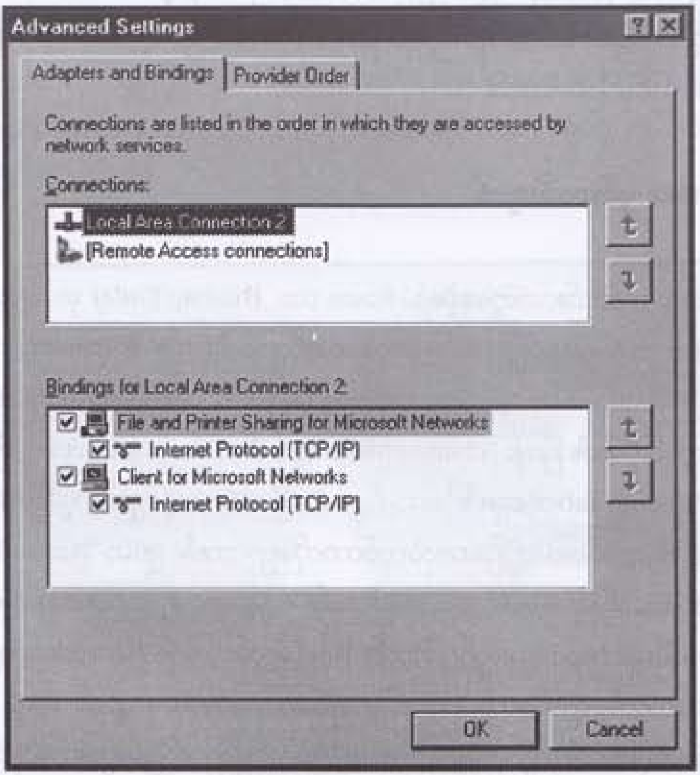
၅.၁၆ **Binding Order** ရှင်းလင်းချက်

အဲ့ဒီအချိန်မှာ Metric ကလည်းလာတူနေခဲ့ရင် Route ဟာ Binding Order မှာ ပထမဦးစွာ Bind လုပ်ထားတဲ့ Interface ကိုပဲရွေးချယ်ပြီး Route လုပ်တော့မှာဖြစ်ပါတယ်။ ဒီ Binding ကိုတော့ Network Connection ရဲ့ Advance Setting ကနေ ဝင်ပြီးကြည့်ရှုနိုင်ပါတယ်။ Control Panel ထဲက Network Connection ထဲကိုဝင်လိုက်ပါ။ ပြီးရင် Advance Menu အောက်က Advance Setting ကိုရွေးပါ။ အဲ့ဒီအခါကျ Adapter and Binding Tab ကိုရွေးပါ။ အောက်မှာ Connection ကိုရွေးပါ။ အဲ့ဒီမှာBinding Order ကိုတွေ့ရပါလိမ့်မယ်။ Bind ဆိုတာ တွဲပြီးအလုပ်လုပ်တာကိုပြောတာပါ။ ဥပမာ Network Card ဟာ Protocol, Client, Servers တို့နှင့် Bind လုပ်ထားရပါတယ်။ ကျွန်တော်တို့ ငယ်ငယ်က Network ချိတ်ရင် Card ကို Driver တင်ပြီးရင် Bind သွားလုပ်ရပါတယ်။ Bind မလုပ်ထားရင် Network မတွေ့ပါဘူး။ နောက်ပိုင်း Windows 98 လောက်ရောက်တော့ Driver တင်ပြီးတော့ အလိုအလျောက် Bind လုပ်ပြီး သားဖြစ်လာတာကြောင့် နောက်ပိုင်း သင်တန်းမှာတောင် Bind ကိုမသင်ဖြစ်သလိုဖြစ်သွားတယ်။ ၁၉၉၈

ပုံ ၅.၇


Network Connections
File
Edit
View
Favorites
Tools
Advanced
Help
Back
Address
Network Connections
Go
Operator-Assisted Dialing
Dial-up Preferences...
Network Identification...
Bridge Connections
Advanced Settings...
Optional Networking Components...
LAN or High-Speed Internet
Local Area Connection 2
Connected
Broadcom 440x 10/100 Integra...
Wizard
New Connection Wizard
Network Setup Wizard

ပုံ ၅.၈


Advanced Settings
Adapters and Bindings
Provider Order
Connections are listed in the order in which they are accessed by network services.
Connections:
Local Area Connection 2
[Remote Access connections]
Bindings for Local Area Connection 2:
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Client for Microsoft Networks
Internet Protocol (TCP/IP)
OK
Cancel

လောက်တုန်းက ဂျာမန်ကုမ္ပဏီမှာ Network သွားဆင်တာ ဖြစ်ချင်တော့ Network မတွေ့လို့ အဲ့ဒီ ဂျာမန်ကြီးက "အင်း Bind ကို ပြန်စစ်ဆေးကြည့်ဦး" လို့ ပြောတာကို အမှတ်သွားရမိလေရဲ့။

လမ်းကြောင်းရွေးချယ်ခြင်း Route ပြီးဆုံးတဲ့အခါ IPv4 ဟာ Routing Table ထဲက Single Route ကိုရွေးချယ်လိုက်ပါတယ်။ အကယ်၍များ ဒီ ဖြစ်စဉ်ကြီးကိုပြုလုပ်ပြီး လမ်းကြောင်းရွေးချယ်ခြင်းဟာ Fail ဖြစ်ခဲ့မယ်ဆိုရင်တော့ IPv4 ဟာ Routing Error ဖြစ်ပြီးဆိုပြီးထအော်ပါလိမ့်မယ်။ Router ဟာ ICMP ဆိုတဲ့ Internet Control Message Protocol ဆီကို Destination ဆီမရောက်နိုင်ဘူးဆိုတဲ့ Destination Unreachable Host, Unreachable Message ကို Send လုပ်တဲ့ Host ဆီပို့ပြီး Packets ကို Cancel လုပ်ပစ်လိုက်ပါလိမ့်မယ်။

၅. ၁၇ Next Hop Address နှင့် Interface တို့ဆုံးဖြတ်ခြင်း

Routing Table ထဲမှ Router ကိုဆုံးဖြတ်ပြီးတဲ့အခါ IPv4 ဟာ Next Hop Address နှင့် Interface ကိုဆုံးဖြတ်ဖို့ အောက်ပါကိစ္စတွေကိုလုပ်ဆောင်ရမှာဖြစ်ပါတယ်။

၁။ Direct Delivery ဖြစ်ခဲ့မယ်ဆိုရင်

❖ IPv4 ဟာ Packet ရဲ့သွားရမယ့် Destination IPv4 Address ကို Next-Hop Address အဖြစ်သတ်မှတ်လိုက်ပါတယ်။

❖ IPv4 ဟာ Interface Field ထဲမှာ Address သတ်မှတ်ထားတဲ့ Interface ကို Next-Hop Interface အဖြစ်သတ်မှတ်လိုက်ပါတယ်။

ကျွန်တော်ကရုံးကိုအိမ်ကနေတိုက်ရိုက်သွားမယ်ဆိုရင် ရုံးလိပ်စာဟာ Next Hop Address ပဲဖြစ်တယ်။ IPv4 Interface ဆိုတာလည်း ဒီအတိုင်းပဲ။ အဲ့ဒီကွန်ပျူတာရဲ့ Network Card ပဲဖြစ်တယ်။

၂။ Indirect Delivery ဖြစ်ခဲ့မယ်ဆိုရင်

❖ IPv4 ဟာ Next Hop Field ထဲမှာရှိတဲ့ IPv4 Address ကို Next Hop Billion အဖြစ်သတ်မှတ်လိုက်ပါတယ်။

Interface Field ထဲမှာ သတ်မှတ်ထားတဲ့ Address ပိုင်ရှင် Interface ကို IPv4 ဟာNext Hop Interface အဖြစ်သတ်မှတ်လိုက်ပါတယ်။ ဥပမာ Router ရဲ့ Address။

၅. ၁၈ **Routing Table ကိုကြည့်ခြင်း**

Windows Server 2003 မှာပဲဖြစ်ဖြစ်၊ Windows XP မှာပဲဖြစ်ဖြစ် Command Prompt ကနေ Route Print ဒါမှမဟုတ် netstat-r ဆိုပြီးရိုက်ထည့်လိုက်မယ်ဆိုရင် ကိုတွေ့ရမှာဖြစ်ပါတယ်။

ပုံ ၅.၁၀

```
E:\WINDOWS\system32\CMD.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

E:\Documents and Settings\Administrator>route print

IPv4 Route Table
===========================================================================
Interface List
0x1 ........................... MS TCP Loopback interface
0x10003 ...c0 10 18 ca 17 74 ...... Broadcom 440x 10/100 Integrated Controller
===========================================================================
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
        127.0.0.0        255.0.0.0        127.0.0.1       127.0.0.1       1
       172.10.0.0      255.255.0.0      172.10.10.1     172.10.10.1      20
      172.10.10.1  255.255.255.255        127.0.0.1       127.0.0.1      20
   172.10.255.255  255.255.255.255      172.10.10.1     172.10.10.1      20
        224.0.0.0        240.0.0.0      172.10.10.1     172.10.10.1      20
  255.255.255.255  255.255.255.255      172.10.10.1     172.10.10.1       1
===========================================================================
Persistent Routes:
  None

E:\Documents and Settings\Administrator>
```

အခုဥပမာပြထား တဲ့ Routing Table ဟာဆိုလို့ရှိရင် အဲ့ဒီမှာ -

- Network Card တစ် Card ပဲစိုက်ထားပါတယ်။
- IPv4 Address က 172.10.10.1 ဖြစ်ပြီး Subnet Mask က 255.255.0.0 (/16)ဖြစ်ပါတယ်။ Default Gateway ကတော့ 172.10.10.1 ဖြစ်ပါတယ်။

-IPv6 Install လုပ်ထားခြင်းမရှိပါဘူး။

ဒီအခုပြထားတဲ့ ဇယားမှာ ဆိုလို့ရှိရင် Interface နှစ်ခုရှိပါတယ်။ တစ်ခုကတော့ အမှန်တကယ် ဒီကွန်ပျူတာမှာစိုက်ထားတဲ့ Network Card ဖြစ်တဲ့ Broadcom 440x 10/100 Integrated Controller ကတစ်ခု၊ နောက်တစ်ခုက Internal Loopback Interface ဖြစ်တဲ့ MS TCP Loopback Interface ကတစ်ခု ပေါင်းနှစ်ခုဖြစ်ပါတယ်။

အခု တွေ့မှာရှိတဲ့ အကြောင်းအရာတွေကို တစ်ပိုင်းချင်းရှင်းပြပါဦးမယ်။

၁။ Routing Table ထဲက ပထမဦးဆုံးဖြစ်တဲ့ First Entry ကိုကြည့်မယ်ဆိုရင် -

Network Destination	Netmask	Gateway	Interface	Metrix
127.0.0.0	255.0.0.0	127.0.0.1	127.0.0.1	1

၄င်း Route သည် Loopback Network Route ဖြစ်ပါတယ်။ Network Destination ဖြစ်တဲ့ 127.0.0.0 Address ကနေလာတဲ့ IP Packet တွေအားလုံးသွားဖို့ရန်အတွက် Next - Hop (or) Gateway Address သည် 127.0.0.1 ဖြစ်ပြီး ၄င်း Next - Hop (or) Gateway Address တွေကိုသွားနိုင်ရန် Interface IP Address သည် 127.0.0.1 ဖြစ်တယ်လို့ ဆိုလိုထားတာဖြစ်ပါတယ်။

၂။ ဒုတိယမြောက် Second Entry ကိုကြည့်မယ်ဆိုရင် -

Netmask Destination	Netmask	Gateway	Interface	Metrix
172.10.0.0	255.255.0.0	172.10.10.1	172.10.10.1	20

၄င်း Route သည် Netmask Route ဖြစ်တယ်။ Network Destination ဖြစ်တဲ့ 172.10.0.0 ကနေလာတဲ့ IP Packet အားလုံးသွားနိုင်ဖို့ရန် Next - Hop (or) Gateway Address သည် 172.10.10.1 ဖြစ်ပြီး။ ၄င်း Next - Hop (or) Gateway Address တွေသွားနိုင်ရန် Interface ရဲ့ IP Address သည် 172.10.10.1 ဖြစ်တယ်လို့ဆိုလိုထားတာ ဖြစ်တယ်။

၃။ တတိယမြောက် Third entry ကိုကြည့်မယ်ဆိုရင် -

Network Destination	Network	Gateway	Interface	Metrix
172.10.10.1	255.255.255.255	127.0.0.1	127.0.0.1	20

၄င်း Route သည် Host Route ဖြစ်တယ်။ Network Destination ဖြစ်တဲ့ 172.10.10.1 ကနေလာတဲ့ IP Packet တွေအားလုံးသွားနိုင်ဖို့ရန် Next - Hop (or) Gateway Address သည် 127.0.0.1 ဖြစ်ပြီးလည်းကောင်း Next - Hop (or) Gateway Address တွေသွားနိုင်ရန် Interface ရဲ့ IP Address သည် 127.0.0.1 ဖြစ်တယ်လို့ ဆိုလိုထားတာဖြစ်တယ်။

၄။ စတုတ္ထမြောက် Fourth Entry ကိုကြည့်မယ်ဆိုရင်–

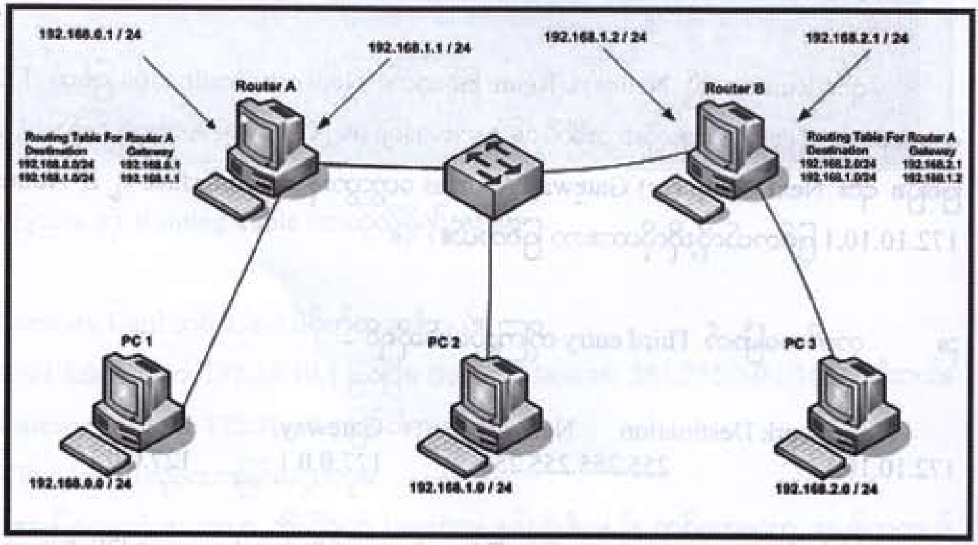
Network Destination	Netmask	Gateway	Interface	Metrix
172.10.255.255	255.255.255.255	172.10.10.1	172.10.10.1	20

၎င်း Route သည် Host Route ဖြစ်တယ်။ Network Destination ဖြစ်တဲ့ 172.10.255.255 ကနေလာတဲ့ IP Packet တွေအားလုံးသွားနိုင်ဖို့ရန် Next - Hop (or) Gateway Address သည် 172.10.10.1 ဖြစ်ပြီးလည်းကောင်း Next - Hop (or) Gateway Address တွေသွားနိုင်ရန် Interface ရဲ့ IP Address သည် 172.10.10.1 ဖြစ်တယ်လို့ ဆိုလိုထားတာဖြစ်တယ်။

ဘယ်လိုလဲဗျ – Routing Table ထဲမှာပါရှိတဲ့ Entry တွေရဲ့သဘောတရားကို နားလည်သွားပြီလား။ အကယ်၍နားမလည်သေးဘူးဆိုရင် အစတစ်ခေါက်လောက်သေသေချာချာ ပြန်ဖတ်ကြည့်ပါ။

၅.၁၃ **Static IPv4 Routing** အကြောင်း

ပုံ ၅.၁၁



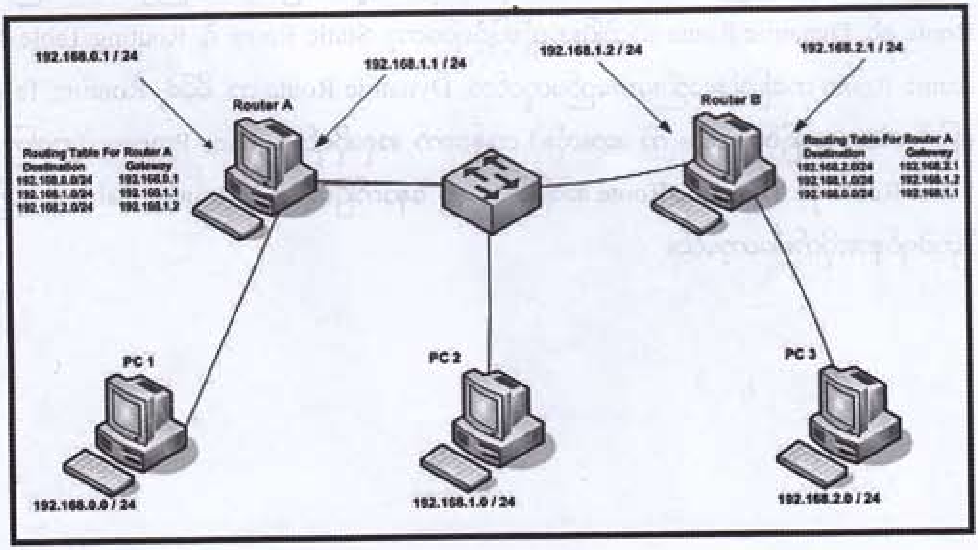
ကျွန်တော်အခုဖော်ပြထားတဲ့ Router A နဲ့ Router B တို့ရဲ့ Routing Table ကအခုကြည့်မယ်ဆိုရင် Router A နဲ့ Router B သည် Network မိနေပါတယ်။ PC1 နဲ့ Router A လည်း Network မိတယ် PC2 နဲ့လည်း Router A လည်း Newtwork မိတယ်။ သို့သော် Router A ရဲ့ Routing Table အရ P1 နဲ့ PC3 တို့ကတော့ Network မမိသေးပါဘူး။

Router B သည်လည်း Router A နဲ့ Network မိတယ်။ PC2 နဲ့ Router B လည်း Network မိတယ်။ PC3 နဲ့ Router B လည်း Network မိတယ်။ ဒါကြောင့် PC2 နဲ့ PC3 လည်း Network မိတယ်။ သို့သော် Router B ရဲ့ Routing Table အရ PC3 နဲ့ PC1 တို့ကတော့ Network မမိသေးပါဘူး။ OK PC1 နဲ့ PC3 က အခုလက်ရှိ Router A နဲ့ Router B တို့ရဲ့ Routing Table အရဆိုရင် Network မမိသေးပါဘူး။ ဒီတော့ Network မိချင်တယ်ဆိုရင်ဘာလုပ်ရမလဲ ကျွန်တော်တို့တွေ Routing Table ထဲမှာ PC1 နဲ့ PC3 Network မိဖို့ရန် Router A နဲ့ Router B မှာ Router တွေထပ်ထည့်ပေးရမယ်။ ဒါမှ Network မိမှာဖြစ်တယ်။ အဲဒီလိုမျိုး Route ကိုထည့်ချင်တယ်ဆိုရင်တော့ အသုံးပြုရမယ့် Command က–

Route add <Destination Address> <Netmask> <gateway> Enter

၎င်း Command ကိုအသုံးပြုပြီး Route တွေကို Add လုပ်လို့ရပါတယ်။

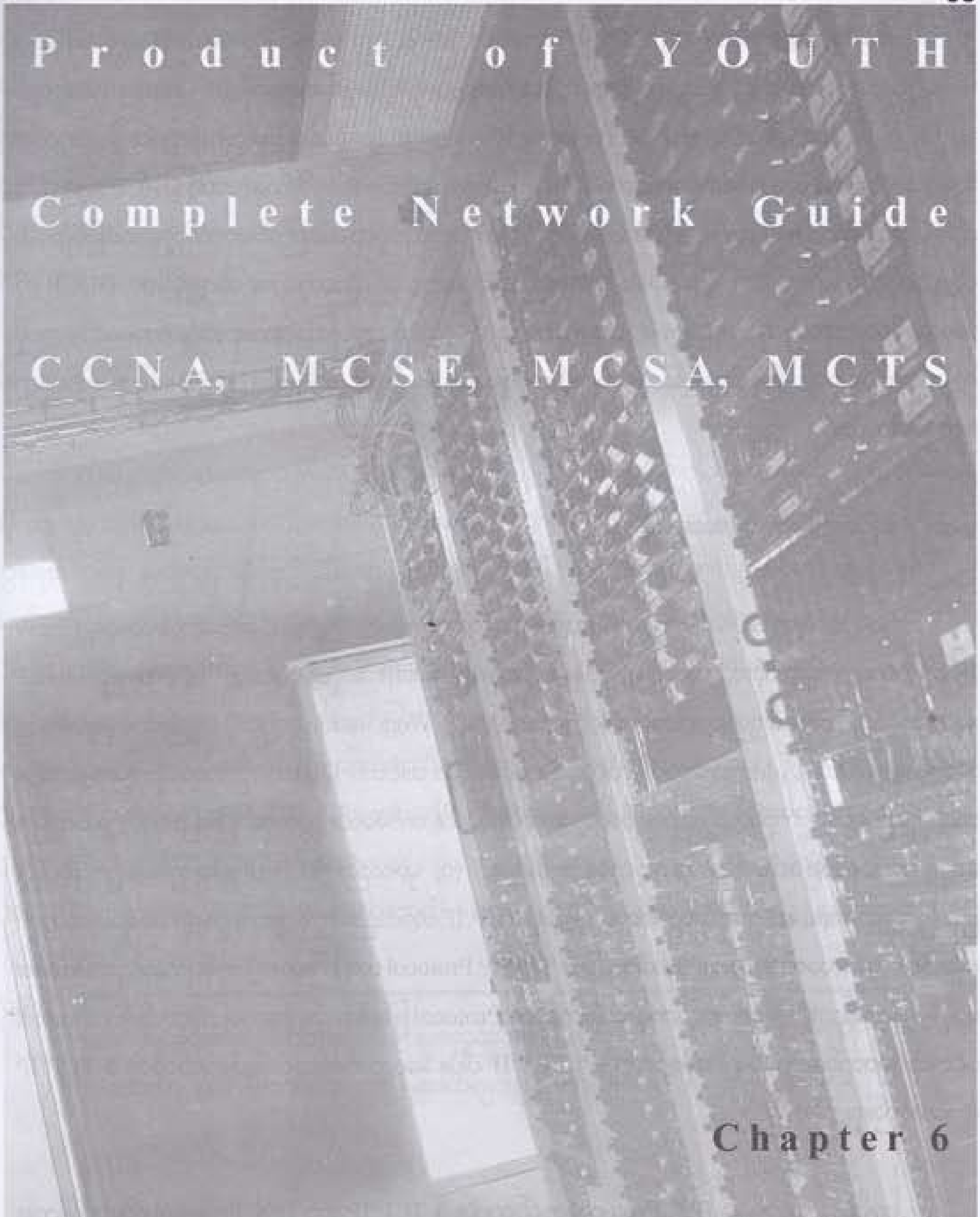
ပုံ ၅.၁၂



ကျွန်တော်အခုဖော်ပြထားတဲ့ Route A နဲ့ Route B တို့ရဲ့ Routing Table အရကြည့်မယ်ဆိုရင် Route A နဲ့ Route B တို့သည် Network မိတယ်။ PC1, PC2, PC3 အားလုံးတို့သည် Network မိသွားပါပြီ။ ဘာကြောင့်လဲဆိုရင် Router A ထဲမှာ Dertination Network လုပ်လိုက်ပြီး Router B ထဲမှာတော့ Destination Network တွင် 192.168.0.0 Network 255.255.255.0 နှင့် Gateway ကို 192.168.1.1 ကို Route လုပ်ထားလိုက်လို့ PC1 နှင့် PC3 တို့ပါ။ Network မိသွားရခြင်းဖြစ်ပါတယ်။ ကဲဒီလောက်ဆိုရင် Routing Table နဲ့ပတ်သတ်တာတွေကို ကောင်းကောင်းလေးနားလည်သွားလောက်ပါပြီ။ အခုကျွန်တော်ဖော်ပြခဲ့တဲ့ Route လုပ်တဲ့ ပုံစံကတော့ Static Route ပဲဖြစ်ပါတယ်။

၅. ၂၀ Dynamic IPv4 Routing အကြောင်း

Dynamic Route ကိုသုံးမယ်ဆိုရင် Dynamic Routing Protocal တွေဖြစ်တဲ့ RIP (Routing Information Protocol) နှင့် OSPF (Open Shortest Path First) တို့ကိုအသုံးပြုရမှာဖြစ်ပါတယ်။ အကယ်၍ ကိုယ်က Dynamic Routing ကိုအသုံးပြုမယ်ဆိုရင် Routing Table သည်အလိုအလျောက်ပြောင်းလဲပေးသွားမှာဖြစ်ပါတယ်။ ကျွန်တော်အခုထပ်ပြီးပြောပြပါဦးမယ်။ Static Route နဲ့ Dynamic Routing ကို (၂) မျိုး တွဲပြီးတော့ အသုံးပြုမယ်ဆိုရင် အသုံးပြုလို့ရပါတယ်။ သို့သော် Dynamic Route ရဲ့သဘောတရားအရ Dynamic Route သည် Routing Table ကို အလိုအလျောက်ပြောင်းပေးမည်ဖြစ်သော်လည်း Static Route နှင့် Dynamic Route ကိုတွဲပြီးအသုံးပြုခဲ့ရင်တော့ Static Route ရဲ့ Routing Table ကို Dynamic Route ကပြောင်းလည်းပေးမည်မဟုတ်ဘဲ Dynamic Route က မိမိရဲ့ Routing Table ကိုပဲ ပြောင်းလဲသွားမှာဖြစ်ပါတယ်။ ကဲ အားလုံးပဲ ကျွန်တော် အခုဆိုရင် Routing Process ရဲ့အကြောင်းတွေ Static Route နှင့် Dynamic Route အကြောင်းတွေ နောက်ပြီးသူတို့ရဲ့ Routing Table အကြောင်းကို ဒီမှာပဲရပ်နားလိုက်ပါတော့မယ်။


Product of YOUTH
Complete Network Guide
CCNA, MCSE, MCSA, MCTS
Chapter 6
DHCP

ဒီသင်ခန်းစာကတော့ Microsoft ရဲ့ Windows Server 2003 ပေါ်မှာ Dynamic Host Configuration Protocol Server ကို Install လုပ်ပြီး ကွန်ရက်အတွင်းရှိ ကွန်ပျူတာများကို IP Address ပေးရာတွင် ယခု Install လုပ်လိုက်တဲ့ DHCP Server ကနေ IP Address များခွဲဝေပေးမှာဖြစ်ပါတယ်။ ဒီတော့ကား ဒီသင်ခန်းစာရဲ့ အဓိကဇာတ်ကောင်ကတော့ DHCP ဖြစ်တယ်ပေါ့ဗျာ။ ဒါပေသိ ယခုလက်ရှိ DHCP အကြောင်းကို ဖတ်တဲ့သူဟာ Networking နှင့်ပတ်သက်လို့ အခြေခံရှိထားပြီးသူဆို အကြောင်းမဟုတ်ဘူး။ အခြေခံရှိတယ်လို့ ကိုယ့်ကိုကိုယ် ထင်ထားပြီး အခြေခံအားနည်းတဲ့သူတွေလည်းရှိတော့ကား အကျွန်ုပ်က DHCP ကို အသေးစိတ် သင်တို့ကို မရှင်းပြခင် ၎င်းနှင့်ဆက်နွယ်နေသော အကြောင်းအရာအချက်အလက်တွေကို ကွင်းဆက်မိအောင် ပြန်ရှင်းပြပါ့မယ်။ မကျဉ်းမကျယ်လေးပေါ့ဗျာ။ သိပြီးသားသူများ ကျော်ဖတ်လိုက ဖတ်နိုင်ပါတယ်။

၆.၁ ခြေဥချင်တာလေးတစ်ခု

အကယ်၍များပေါ့နော်။ သင်ဟာ Intranet လေးတစ်ခုလောက်များတပ်ဆင်တော့မယ်ဆိုရင် TCP/IP ကို သင်ဟာ ရိုးရိုးသုံးလို့မရပါဘူး။ (ဆန်းဆန်းသုံးရမှာလား)။ ဒီလိုပါ သင်ဟာ TCP/IP ကို DHCP အကူ အညီနှင့် သုံးရတော့မှာဖြစ်ပါတယ်။ ဒီလိုမှ Server တွေ Workstation တွေစတဲ့ ပစ္စည်းတစ်ခုချင်းစီတွေ အတွက်မှန်ကန်တဲ့ Address တွေကို သတ်မှတ်တဲ့နေရာမှာ သင်ဟာ DHCP ကိုသာအသုံးမပြုခဲ့ရင် အင်း ဘယ်လိုပြောရမလဲ။ တည့်တည့်ပြောရရင်တော့ အလုပ်ရှုပ်မယ်။ ခက်ခဲမယ်။ သွယ်ဝိုက်ပြီးပြောရရင် လွယ်ကူခြင်းတွေနဲ့ ဝေးနေမှာဖြစ်ပါတယ်။ ဒီတော့ကား သင်ခန်းစာ (၁) မှာလည်း TCP/IP အကြောင်းပြောပြခဲ့ပါပြီ။ ပြန်ပြောရရင် Intranet ဟာ ကြီးထွားလာတာနဲ့အမျှ TCP/IP ဟာလည်း ကွန်ပျူတာကွန်ရက်အများစုအတွက် မရှိမဖြစ် လိုအပ်လာတဲ့ Protocol ဖြစ်ပါတယ်။ ဒီ TCP/IP Protocol ဟာ ကြီးမားတဲ့ ကွန်ရက်အတွက်ပဲဖြစ်စေ၊ ကွန်ရက်သေးသေးပဲဖြစ်စေ၊ အင်မတန်အသုံးတည့်တဲ့ Protocol ဖြစ်ပါတယ်။ ခုနကပြောခဲ့သလိုပါပဲ၊ Intranet လေးတစ်ခုတည်ဆောက်မယ်ဆိုရင်လည်း ဒီ TCP/IP ပါပဲ။ ဒီလောက်အဆင်ပြေပါတယ်ဆိုတဲ့ ဒီ TCP/IP ရဲ့ အားနည်းချက်ကတော့ -

အင်း . . .ပြောရရင် IPX Protocol ဟုတ်တယ်။ ဒီ TCP/IP ဟာ IPX Protocol လိုမဟုတ်ဘူး။ ဒါ TCP/IP ရဲ့ အားနည်းချက်နော်။ TCP/IP ဟာ IPX Protocol လိုမဟုတ်ဘူးတဲ့။ ဘာကွာလို့တုန်း။ ဟုတ်ကဲ့ပြော ပါ့မယ်။ TCP/IP Protocol ဟာဖြင့် Address လိပ်စာတွေနှင့် Setting သတ်မှတ်ခြင်း (Configuration) တွေကို ကွန်ပျူတာတစ်လုံးချင်းစီ၊ တနည်းအားဖြင့် ကွန်ရက်မှာရှိတဲ့ ကွန်ရက်နှင့်ချိတ်ဆက်ထားတဲ့

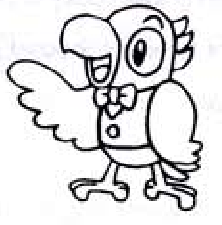
ပစ္စည်းတိုင်းစီမှာ လိုက်သတ်မှတ်ပေးဖို့ပဲလိုတာပါပဲ။ ဒါဟာ တကယ်တမ်းပြန်တွက်ကြည့်မယ်ဆိုရင် System Administrator တွေအတွက် အလွန်တရာကြီးမားတဲ့ System Administration အလုပ်ကြီးပဲ ဖြစ်ပါတယ်။ ပြန်ပြောပြမယ်။ TCP/IP Protocol ဟာ IPX Protocol လိုမဟုတ်ဘူး။ TCP/IP ဟာ ကွန်ရက်များရှိတဲ့ ကွန်ရက်နှင့် ချိတ်ဆက်ထားတဲ့ ပစ္စည်းတိုင်းကိုလိုက်ပြီး Address တွေ၊ Setting တွေ လိုက်သတ်မှတ်ပေးရတယ်။ ဒါဟာ Network ကြီးလာလေ အလုပ်တာဝန်ပိုများ၊ ပိုရှုပ်လာလေပဲ။ ဒါဟာ TCP/IP ရဲ့ အားနည်းချက်ပဲ။

၆.၂ **DHCP အကြောင်း**

ကဲပြောချင်တာလေးတွေလဲပြောပြီးပြီဆိုတော့ အခု DHCP အကြောင်းစပြောတော့မယ်။ DHCP ဆိုတာ Dynamic Host Configuration Protocol ဖြစ်တယ်။ သူ့ကို ဘယ်နေရာမှာသုံးသလဲဆိုတော့ ကွန်ရက်တစ်ခု အတွင်းမှာရှိကြတဲ့ Client Node တွေရဲ့ TCP/IP Configuration များကို ဗဟိုစနစ်ဖြင့် သတ်မှတ်ခြင်း၊ ထိန်းချုပ်ခြင်း တွေလုပ်ပေးတယ်။ ဒိုလိုပြောရင်တော့ Centralized ပေါ့ဗျာ။ ဆိုလိုတာက Client Node တစ်ခုချင်းစီမှာ TCP/IP Configuration တွေကို လိုက်လံသတ်မှတ်နေစရာမလိုဘဲ၊ DHCP Server တစ်ခုထဲကနေ ဗဟိုစနစ် နဲ့သတ်မှတ်ခြင်း၊ ထိန်းချုပ်ခြင်းတွေလုပ်ပေးတာဖြစ်တယ်။ ရှင်းအောင်ထပ်ပြောမယ်ဗျာ။ ခွဲတမ်းချတယ်ပေါ့။ ဒါဟာ တော်တော်ကို အလုပ်ရှုပ်သက်သာသွားတာဗျ။ ကွန်ရက်ထဲမှာရှိတဲ့ Client တစ်ခုချင်းစီကိုသာ TCP/IP Address တွေ လိုက်ပေးရမယ်ဆိုရင် ဘယ်သက်သာမလဲဗျာ။ ကွန်ရက်ရဲ့ Client တစ်ခုချင်းစီမှာ TCP/IP Address ကို ကိုယ်တိုင်ကိုယ်ကျ လိုက်လံသတ်မှတ်နေစရာမလိုတော့ဘဲ DHCP Server ကနေ TCP/IP Address တွေကို Client တွေဆီ ခွဲတမ်းချသတ်မှတ်လိုက်မှာဖြစ်ပါတယ်။

ပုံ ၆.၁

အခုရှင်းပြသလောက်ကိုမှ သင်နားမလည်သေးဘူးဆိုရင်
သင်ဟာ TCP/IP အကြောင်းကို ပြန်ဖတ်ရမှာ ဖြစ်ပါတယ်။



ကဲ - ဒီတော့ကား သင်ဟာ သင့်ရဲ့ ကွန်ရက်အတွင်းမှာရှိတဲ့ Client တွေဟာ လက်တစ်ဆုပ်စာထက် များနေပြီ ဆိုရင်တော့ အချိန်ကုန်သက်သာစေဖို့ Setting ချမှတ်နေစဉ်ကာလမှာ ကြုံတွေ့ရတတ်တဲ့ ပြဿနာ အခက်အခဲများကို လျှော့ချနိုင်ဖို့၊ TCP/IP Network ကို ထိန်းချုပ်ရာမှာတွေ့ရတတ်တဲ့ ပြဿနာတွေကို လျှော့ချဖို့ DHCP ကိုသာသုံးလိုက်ပါတော့လို့ ကျွန်တော်က ပြောချင်ပါတယ်။ DHCP ကလုပ်ပေးနိုင်တာတွေ ကို ပြောရမယ်ဆိုရင် -

၁။ သူက Server ကနေ Client PC တွေကိုပေးမယ့် TCP/IP Address တွေကို ဘယ်ကနေမှ ဘယ်အထိ ဆိုပြီး သတ်မှတ်ပေးထားနိုင်တယ်ဗျ။ အဲဒါကို DHCP စကားအရပြောရင် Scopes လို့ခေါ်တယ်။ ပြန်ပြောပြမယ်။ အဲဒီ Scopes အထဲမှာ ဘာတွေရှိသလဲဆိုရင် TCP/IP Address တွေရှိတယ်ဗျ။ Server ကနေ Client တွေ ဆီ ကို TCP/IP Address တွေထုတ်ပေးတယ်ဆိုတာ အဲ့ဒီကနေထုတ်ပေးတာပေါ့။ ဒီတော့ကား DHCP Server ကို Install လုပ်တဲ့အခါကျရင် သင်က Scopes တွေကိုသတ်မှတ်ပေးရလိမ့်မယ်။

၂။ DHCP Server က TCP/IP Address တွေကိုပဲ ချုပ်ကိုင်ပေးတာမဟုတ်ဘူးဗျ။ သူနှင့်ဆက်နွယ်နေတဲ့ အားလုံးသော Configuration Setting တွေ၊ ပြောရရင်တော့ Subnet Mask တို့၊ Default Router တို့၊ DNS Server တို့၊ စတဲ့ တနည်းအားဖြင့် TCP/IP ကို ကောင်းစွာအလုပ်လုပ်ဖို့လိုအပ်တဲ့ အရာမှန်သမျှ အားလုံးကိုလည်း ထိန်းချုပ်ပေးပါတယ်။

၃။ DHCP ဟာ TCP/IP Router အများစုမှာ အလုပ်လုပ်နိုင်စွမ်းရှိတဲ့အပြင်၊ Subnet ပေါ်မူတည်၍ ဖြစ်ပေါ်လာသော IP Address များကိုလည်း သတ်မှတ်နိုင်စွမ်းရှိတာကြောင့် သင့်ရဲ့ Computer ကို လက်ရှိ သုံးနေတဲ့ Subnet ကနေဖြုတ်ပြီး၊ အခြား Subnet မှာ သွားတပ်ခဲ့ရင်တောင်၊ ၎င်း Computer အတွက် Address ကို ပြန်လည်၍ သတ်မှတ်ပေးစရာမလိုပါဘူး။ ဆိုလိုတာက Subnet တစ်ခုမှာရှိတဲ့ Computer ကို အခြား Subnet တစ်ခုမှာပြောင်းရွှေ့တပ်ဆင်မယ်ဆိုရင် ၎င်း Computer ရဲ့ IP ကိုပြန်လည်သတ်မှတ်ပေးဖို့ မလိုပါဘူး။

၄။ Address တွေဟာ DHCP Server ကနေ Client တွေဆီကိုခွဲတမ်းချရာမှာ ၎င်း Address တွေကို Server က အချိန်အတိုင်းအတာတစ်ခုထိ အငှားချထားတာဖြစ်ပါတယ်။ ဒိုလိုပြောရရင်တော့ Leased ပေါ့ဗျာ။ ဒီတော့ ဥပမာအားဖြင့် IP Address တစ်ခုဟာ အငှားချထားပြီးမှ အချိန်အတော်ကြာထိအောင်

သုံးဖြစ်ခဲ့ဘူးဆိုရင် ၎င်း IP Address ကို DHCP က ပြန်သိမ်းထားလိုက်ပါတယ်။ ဒီတော့ကား IP Address မလောက်တာလဲ မဖြစ်တော့ဘူးပေ့ါ။ ဘိုလိုပြောရင်တော့ Recover ပြန်ဖြစ်သွားတာပေ့ါဗျာ။ ထပ်ရှင်းပြမယ်။ Server ကနေ Client တွေဆီကို IP Address တွေ အငှားချထားတယ်။ အငှားချထားပြီးမှ မသုံးတာကြာတဲ့ IP Address တွေကို Server ကပြန်သိမ်းထားလိုက်တယ်လို့ပြောချင်တာဖြစ်ပါတယ်။ ဒီလိုလုပ်ခြင်းအားဖြင့် အသုံးမလိုတဲ့နေရာက ပြန်သိမ်းပြီး၊ အသုံးလိုတဲ့နေရာကို ပြန်လည်အငှားချမှာဖြစ်ပါတယ်။

ဒီလောက်ဆိုရင် DHCP အကြောင်းသဘောပေါက်လောက်ပြီထင်ပါတယ်။ ဒါပေမယ့်လည်း ရှင်းပြစရာတွေကရှိသေးတယ်ဗျ။ အားလုံးရှင်းပြပြီးသွားတော့မှဘဲ DHCP Server ကို Install လုပ်တဲ့နည်း ရှင်းပြပေးမယ်။ အဲ ခု ဘာအကြောင်းကိုပြောပြမလဲဆိုတော့ DHCP ဘယ်လိုအလုပ်လုပ်တယ်ဆိုတဲ့ အကြောင်း ပြောပြပေးမယ်။

၆.၃ DHCP အလုပ်လုပ်ပုံ

အခုကျွန်တော်က DHCP အလုပ်လုပ်ပုံ ရှင်းပြဖို့ရာ သင့်ရဲ့စိတ်ထဲမှာ DHCP Server Install လုပ်ထားတဲ့ ကွန်ရက်တစ်ခုကို မျက်စိထဲမြင်လိုက်။ ဟုတ်ပြီ။ ဒီတော့ ကွန်ရက်တစ်ခုရှိမယ်။ ကွန်ရက်ထဲမှာ DHCP Server ရှိမယ်။ Client တွေလဲရှိမယ်။

၁။ Client ကွန်ပျူတာဟာ Power ဖွင့်လိုက်တဲ့အချိန်မှာ ၎င်းဟာ ကွန်ရက်မှာရှိတဲ့ Computer တွေအားလုံးမြင်စေ၊ ကြားစေ၊ သိစေမယ့် Broadcast Packet ပို့လိုက်ပါတယ်။ ဘယ်ကိုပို့လွှတ်လိုက်တာလဲ။ DHCP Server ဆီကိုပေါ့။ အဲဒီ Broadcast Packet ထဲမှာဘာပါလဲဆိုတော့ IP Address ကိုတောင်းခံတဲ့ DHCP Request ပါတယ်ဗျ။ ပြန်ပြောပြမယ်နော်။ ကွန်ရက်ထဲမှာရှိတဲ့ (အာရုံထဲမှာမြင်နေလိုက် ကွန်ရက်တစ်ခုကို မြင်နေလိုက်) ကွန်ရက်တစ်ခုမှာရှိတဲ့ DHCP ကို အလိုရှိသော Broadcast Packet ကို DHCP Server သို့ပို့လွှတ်လိုက်ပါတယ်။ လွယ်လွယ်ပြောရရင်ဗျာ။ ကျွန်တော်ကဖြင့် ခင်ဗျားဆီကနေ Address တစ်ခု အလိုရှိပါတယ်ပေ့ါ။

၂။ DHCP Server က အဲ့ဒီ Broadcast Packet လေးကို လှမ်းယူလိုက်ပါတယ်။ အဲ့ဒီလိုလှမ်းယူပြီးသကာလ DHCP Server ဟာ သူပေးပိုင်ခွင့်ရှိတဲ့၊ တနည်းအားဖြင့် သူ့မှာရှိတဲ့ Address တွေအများကြီးထဲက IP Address တစ်ခုကို ၎င်းကွန်ပျူတာဆီကို ပေးပို့လိုက်ပါတယ်။ တနည်းအားဖြင့် သတ်မှတ်လိုက်ပါတယ်။

ဆိုလိုတာက DHCP Server မှာ ကျွန်တော်တို့က ဒီကွန်ရက်မှာ အသုံးပြုမယ့် IP Address တွေကို ဘယ်ကနေ ဘယ်အထိဆိုပြီး ကနဦးတည်းက၊ တနည်းအားဖြင့် DHCP Server ကို Install လုပ်ကတည်းက ပြောပြထား။ သတ်မှတ်ထားပြီးသားဖြစ်တယ်။ အဲဒီလို ကျွန်တော်တို့သတ်မှတ်ပေးထားတဲ့ ဘယ်နေရာမှ ဘယ်အထိသို့ဆိုတဲ့ IP Address တွေ ကို Scope လို့ခေါ်ပါတယ်။ အဲဒီ Scope ထဲက တစ်ခုသော IP Address ကိုတောင်းခံလာတဲ့ ကွန်ပျူတာအတွက် သတ်မှတ်ပေးလိုက်တာဖြစ်ပါတယ်။

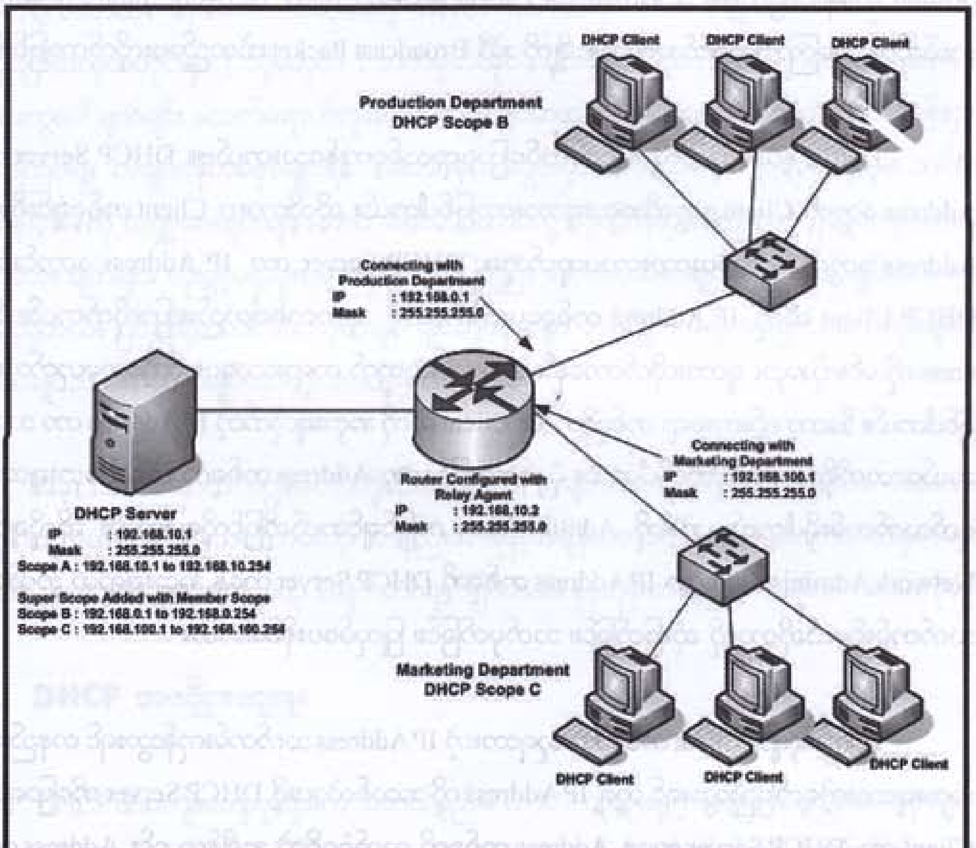
၃။ ဒီနေရာမှာသိရမှာက ကိုယ့်ရဲ့ကွန်ရက်မှာ ဆင့်ပွား Network ရှိမယ်ဆိုရင် တနည်းအားဖြင့် TCP/IP Class မတူတဲ့၊ သီးခြား Network ရှိခဲ့မယ်ဆိုရင် ကျွန်တော်တို့ဟာ ၎င်း Network နှစ်ခုအတွက် DHCP Scope ကိုသီးခြားစီပေးရမှာဖြစ်ပါတယ် ရှုပ်နေလား။ ထပ်ရှင်းပြဦးမယ်။ လွယ်လွယ်ဘဲပြောမယ်ဗျာ။ သီးခြားကွန်ရက်နှစ်ခုအတွက် DHCP Scope ကိုလည်း သီးခြားစီထားပေးရမှာဖြစ်ပါတယ်။ နောက်ထပ် သိရမယ့် အချက်တစ်ခုက သင်ဟာ အဲ့ဒီကွန်ရက်တွေမှာ Router ကိုအသုံးပြုခဲ့မယ်ဆိုရင် အဲ့ဒီ Router ဟာ DHCP ကို Support လုပ်တဲ့ Router ဖြစ်ရပါမယ်။ ကောင်းပြီ။ Router သုံးထားတဲ့ ကွန်ရက်မှာ DHCP ကိုသုံးတယ်ဆိုရင်တော့ Client က လာတယ်ဆိုတဲ့ DHCP ကိုတောင်းခံသော Broadcast Packet မှာ ဒီတောင်းခံမှုဟာ ဘယ် Network ကလာတယ်ဆိုတဲ့ Information လေးကို Router က ၎င်း Broadcast Packet မှာ ထပ်ထည့်ပေးရပါတယ်။ ဒီတော့မှသာလျှင် DHCP Server က ယခုတောင်းခံလာတဲ့ Client ဟာ ဘယ် Network မှာ ရှိတယ်ဆိုတာကို သိမှာဖြစ်ပြီ။ DHCP Server က IP ကိုမှန်ကန်တဲ့ Scope ကနေပေးနိုင်မှာဖြစ်ပါတယ်။

အဟမ်း – ရှုပ်သွားပြီ မဟုတ်လား။ မမြင်ရလဲသိနေတယ်လေ။ နောက်တစ်ခေါက်ထပ်ရှင်းပြပေးမယ်။ နားမလည်တဲ့နေရာကနေ နောက်တစ်ခေါက်ပြန်ဖတ်ဆိုလဲ သင်တို့ကဖတ်ကြမှာမဟုတ်ဘူး။ ဒါကိုလဲသိနေတယ်လေ။ ကဲ..ပြောနေကြာတယ် ပြန်ရှင်းပြီ။

သင်ရဲ့ရုံးမှာ ကွန်ရက်တစ်ခုရှိမယ်။ သင်က Marketing Department အတွက် IP ကို ဘယ်ကနေမှ ဘယ်အထိဆိုပြီးပေးမယ်။ Production Department အတွက်ကျတော့ ၎င်း IP နဲ့မတူတဲ့ အခြားသော IP Range တစ်ခုပေးမယ်။ အဲဒီတော့ကား ဒီကွန်ရက်မှာ Class မတူတဲ့ IP ကို သုံးလိုက်တာကြောင့် Marketing Department နဲ့ Production Department ဟာ Network Submask တစ်ခုစီကွဲထွက်သွားတယ်။ အဲဒီအတွက် DHCP Server မှာ သင်ဟာ Marketing Department အတွက် Scope တစ်ခု၊ Produc-

tion Department Scope တစ်ခုစီ သတ်မှတ်ပေးရမယ်။ Marketing Department ကွန်ရက် Submask ထဲက ကွန်ပျူတာ တစ်လုံး ဟာ DHCP Server ဆီမှာ Address တစ်ခုကိုတောင်းခံရင် DHCP Server ဟာ ၎င်း Marketing Submask အတွက် ကျွန်တော်တို့သတ်မှတ်ပေးထားတဲ့ Scope ထဲမှ IP Address တစ်ခုကို ထုတ်ပေးပါတယ်။ ဒီလောက်ဆို သဘောပေါက်လောက်ပြီလို့ထင်ပါတယ်။ မပေါက်သေးဘူး ဆိုရင်တော့ သင်ဟာ TCP/IP သင်ခန်းစာကိုပြန် လေ့လာရဦးမှာဖြစ်ပါတယ်။ နောက်တစ်ခုက ဒီလိုအခြေ အနေမျိုးမှာ သင်ဟာ DHCP ကို Support လုပ်တဲ့ Router ကိုသုံးခဲ့မယ်ဆိုရင် မျက်စိထဲမှာမြင်ကြည့်လိုက်။ Marketing Network Subnet Mask ထဲက ကွန်ပျူတာ တစ်လုံးဟာ IP Address တစ်ခုကိုတောင်းခံတဲ့ Broadcast Packet ကို DHCP Server ဆီကို လွှတ်လိုက်ပြီး ၎င်း Packet လေးဟာ Router ကိုဖြတ်ပြီးမှ DHCP Server ဆီကိုရောက်မှာ။

ပုံ ၆.၂



ဒီတော့ကား- ၎င်း Broadcast Address လေးဟာ Marketing Network Submask ထဲက ထွက်လာတယ်ဆိုတဲ့ အကြောင်းကို DHCP Server ဆီကိုသွားမယ့် Broadcast Packet ထဲမှာ Router ကနေ ထပ်မံဖြည့် စွက်လိုက်တယ်။ ဘယ်လိုဖြည့်စွက် လိုက်တာလဲဆိုတော့ အခုတောင်းခံတဲ့ Client ဟာ Marketing Network Subnet ထဲကပါဆိုပြီးတော့ ဖြစ်ပါတယ်။ အဲဒါမှလဲ DHCP Server က သူ့ဟာ သူ့ဆီမှာရှိတဲ့ Scope နှစ်ခုထဲက Marketing Scope ဆီက IP Address တစ်ခုကို ထုတ်ပေးမှာဖြစ်ပါတယ်။ မျက်စိထဲမြင်ကြည့်ရအောင်။ Router ကသာ ဒီ Packet လေး ဘယ် Submask ဆီကလာပါတယ် ဆိုတာကို ထည့်မပြောရင် DHCP Server ဟာသူ ထုတ်ပေးရမယ့် IP Address ကို Marketing Scope ဆီက ထုတ်ပေးရမလား။ Production Scope ကထုတ် ပေးရမလားဆိုပြီး ဖြစ်ပါလိမ့်မယ်။ အဲ့ဒီလို မဖြစ်ရလေအောင် Router ဟာ DHCP Server ဆီကို ဦးတည်ပြီး သွားနေတဲ့ Broadcast Packet လေး သူ့ဆီကနေအဖြတ်မှာ (Router ကနေအထွက်မှာ) ဒီ Broadcast Packet လေးဟာ ဘယ် Network Submask ဆီကဖြစ်ပါ တယ်ဆိုတဲ့ အကြောင်းအချက်အလက်အချို့ကို အဲ့ဒီ Broadcast Packet ထဲထည့်ပေးလိုက်တာဖြစ်ပါတယ်။

၄။ DHCP နဲ့ပတ်သက်လို့ နောက်ထပ်ပြောစရာတစ်ခုကျန်သေးတယ်ဗျ။ DHCP Server ဟာ IP Address တွေကို Client တွေဆီအငှားချထားတာဖြစ်ပါတယ်။ ဆိုလိုတာက Client တစ်ခုချင်းစီအတွက် Address တွေကိုအသေပေးထားတာမဟုတ်ဘူး။ DHCP Server ဟာ IP Address တောင်းခံလာတဲ့ DHCP Client ဆီကို IP Address တစ်ခုပေးလိုက်တာနဲ့ သူကတစ်ခါတည်းပြောလိုက်တယ်။ ဒီ Address ကို မင်းကိုအငှား ချထားလိုက်တာနော်။ အမြဲတမ်းအတွက် တရားသေပေးလိုက်တာမဟုတ်ဘူးဆိုတာ ဖြစ်ပါတယ်။ ဒီတော့ စဉ်းစားစရာ တစ်ခုရှိတယ်။ Client ဆီကို အငှားချလိုက်တဲ့ IP Address ဟာ သက်တမ်း ဘယ်လောက်ရှိသလဲပေါ့။ ဟုတ်ပါတယ်။ ပုံမှန်အားဖြင့်တော့ Address တစ်ခုကို တစ်ခါအငှားချထားရင် ၃ ရက်သက်တမ်းရှိပါတယ်။ အဲ့ဒါကို Administrator ကပြင်ချင်တယ်ဆိုပြင်လို့ရပါတယ်။ ဆိုလိုချင်တာက Network Administrator ဟာ IP Address တစ်ခုကို DHCP Server ကနေ အငှားချရာမှာ ဘယ်လောက် သက်တမ်းရှိမယ်ဆိုတာကို ဆုံးဖြတ်ခြင်း၊ သတ်မှတ်ခြင်း၊ ပြုလုပ်ပေးနိုင်ပါတယ်။

ဆိုကြပါစို့ဗျာ။ Client တစ်ခုဟာ သူရထားတဲ့ IP Address သက်တမ်းကုန်သွားရင် တနည်းအားဖြင့် အငှားချထားတဲ့ရက်ပြည့်သွားရင် သူ့ရဲ့ IP Address ကို အသစ်လဲပေးဖို့ DHCP Server ကိုပြောရပါတယ်။ Client ဟာ DHCP Server ကနေ Address တစ်ခုကို လက်ခံရရှိတဲ့ အချိန်မှာ ၎င်း Address လေးဟာ ဘယ်နှစ်ရက်ပဲ သက်တမ်းရှိတယ်။ တနည်းအားဖြင့် အငှားချထားတဲ့ရက်ကို Client က သိနေပါတယ်။

ဥပမာ (၃) ရက်ဆိုကြပါစို့။ ဒီအငှားချထားတဲ့ (၃) ရက်အတွင်းမှာ Client ဟာ ၎င်း IP Address အတွက် DHCP Server ဆီကိုသွားသွားပြီးကြည့်နေစရာမလိုပါဘူး။ ဘာလို့လဲဆိုတော့ သူရရှိထားတဲ့ IP Address ဟာ (၃) ရက်သက်တမ်းရှိနေလို့ပါပဲ။ အဲဒီလို (၃) ရက်ပြည့်သွားတဲ့အခါကျတော့ အိမ်ရှင်အိမ်ငှားစာချုပ်လိုပေါ့ဗျာ။ ခင်ဗျားအငှား ချထားတာတော့ ရက်ပြည့်သွားပြီ။ ကျုပ်ကို Address အသစ်ပေးပါဆိုပြီး DHCP Client ကနေပြီး DHCP Server ဆီကိုအကြောင်းကြားရပါတယ်။

အကယ်၍များပေါ့ဗျာ။ အဲဒီလိုအကြောင်းကြားလိုက်တာကို DHCP Server ကများ လစ်ဟင်းခဲ့လို့ မသိခဲ့ဘူးဆိုရင် ၎င်းဟာသက်တမ်းကုန်နေပြီဖြစ်တဲ့ IP Address ကို Client ကနေပြန်ယူပြီး DHCP Server အတွင်းက IP Address များသိမ်းထားသောနေရာသို့ပြန်သွင်းပြီး သိမ်းလိုက်ပါတယ်။ အခ်ပွါယ်က လိုတဲ့အခါ ပြန်သုံးလို့ရအောင်ပေါ့။ အခုပြောတဲ့အချက်အလက်တွေကို ကြည့်ခြင်းအားဖြင့် ကျွန်တော်တို့သိရမယ့်အချက် တစ်ချက်ရှိလာတယ်။ အဲ့ဒါကဘာလဲဆိုတော့ DHCP Server မှာ DHCP နဲ့ပတ်သက်တဲ့ Setting တွေကိုပြောင်းလိုက်တိုင်းမှာ (သို့မဟုတ်) သတ်မှတ်လိုက်တိုင်းမှာ အဲ့ဒီသတ်မှတ်ချက်တွေဟာ DHCP Client တွေပေါ် ချက်ချင်း မသက်ရောက်ဘူးဆိုတာကိုပဲ။ ဥပမာအားဖြင့်ပြောရရင်ဗျာ..တိုက်ခန်းတစ်ခန်းငှား တယ်ဆိုကြပါစို့။ စာချုပ်ကိုတစ်နှစ်ချုပ်ရင် အဲဒီတစ်နှစ်အတွင်းမှာ သင်ဟာဈေးကိုပြင်ခွင့်မရှိဘူး။ သင်က တိုက်ခန်းငှားခကို လျှော့ပေးချင်လျှင်တောင် အဲလေ..ယောင်လို့ တိုက်ခန်းငှားခကို ထပ်တိုးချင်လျှင်တောင် လို့ပြောတာ။ ချက်ချင်း တိုးခွင့်မရှိဘူး။ တစ်နှစ်စာချုပ်ပြည့်ပြီး နောက်ထပ်စာချုပ် အသစ်ထပ်ချုပ်မှသာလျှင် တက်ခွင့်ရှိတယ်။ ပြင်ခွင့်ရှိတယ်။ ဒီတော့စာချုပ် ချုပ်တဲ့နေရာမှာ တစ်ချို့က ဈေးအပြောင်းအလဲလုပ်ချင်လို့ တစ်နှစ်မချုပ်ဘဲ ခြောက်လချုပ်တာတို့ ဘာတို့ရှိလာတယ်။

အခု DHCP မှာလဲ ကျွန်တော်တို့စဉ်းစားရမယ့် အချက်တစ်ချက်ရှိတယ်။ အဲ့ဒါက Address တွေကို အငှားချထားမယ့် သက်တမ်းကို၊ တနည်းအားဖြင့်အချိန်ကာလကို ဘယ်လောက်သတ်မှတ်မလဲ ဆိုတာပဲ။ ဒါဟာ သေချာစဉ်းစားရမယ့် အချက်တစ်ချက်ဖြစ်တယ်။ ခုနတုန်းကပြောတဲ့ စာချုပ်သက်တမ်းလိုပေါ့။

၆.၄ DHCP အကျိုးကျေးဇူး

DHCP ၏အကျိုးကျေးဇူးများက အဘယ်နည်း။ DHCP ကိုသုံးရတဲ့ အခြေခံအကြောင်းတရားများ– DHCP ကိုသုံးခြင်းအားဖြင့် လူကနေမှ Computer တစ်လုံးချင်းဆီကို ကိုယ်တိုင်ကိုယ်ကျ IP

Address လိုက်ပေးစရာမလိုတော့တာကြောင့် အမှားဖြစ်မှုတွေလျော့နည်းသွားတာပေါ့ဗျာ။ လူကလိုက်ပြီး ကျွန်ပျူတာ တစ်လုံးချင်းစီကို IP လိုက်ပေးရင် IP ထပ်တာတို့ ဘာတို့ဖြစ်တတ်တယ်ပေါ့ဗျာ။ အဲ့ဒီအပြင် Network ကို Administrator လုပ်ရတဲ့ အလုပ်တွေလည်း လျော့ကျသွားတာပေါ့။ ဥပမာပြောရရင် -

❖ TCP/IP Configuration တွေကို ဗဟိုစနစ်နဲ့အလိုအလျောက် ထိန်းချုပ်နိုင်တယ်။ တနည်းအားဖြင့် ပြောရရင် TCP/IP Configuration တွေကို ဗဟိုစနစ်ကနေ သတ်မှတ်နိုင်စွမ်းရှိတယ်ပေါ့ဗျာ။

❖ အဲဒီအပြင် အခြားအခြားသော TCP/IP Configuration တွေကို DHCP Option သုံးပြီး အပြည့်အဝ သတ်မှတ်နိုင်စွမ်းလဲရှိပါတယ်။

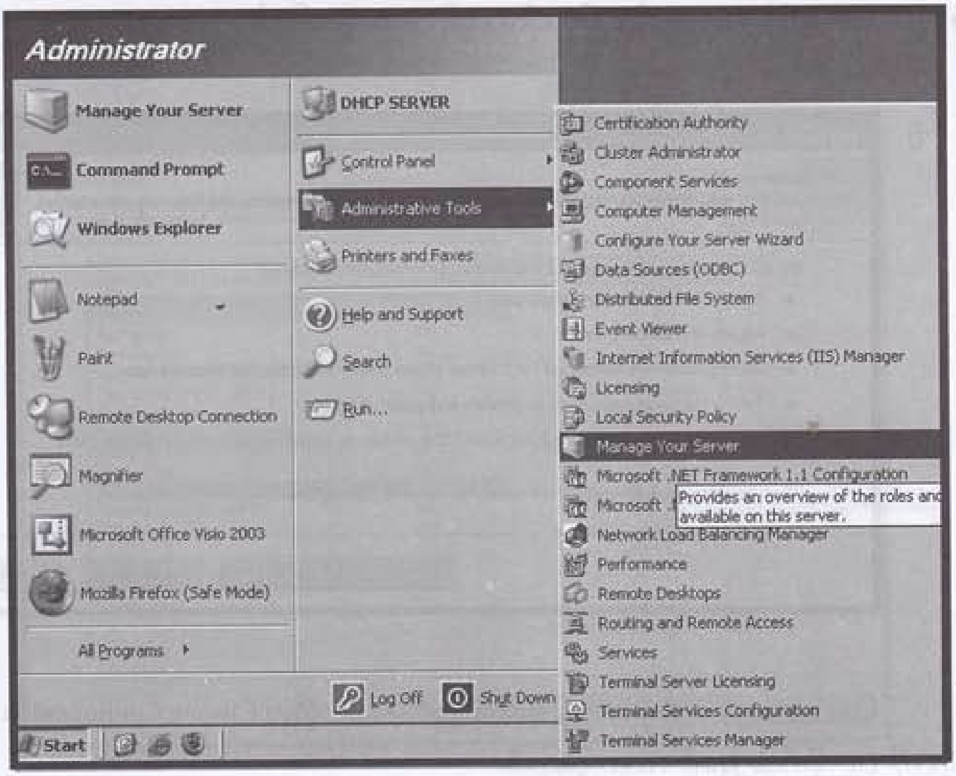
❖ နောက်တစ်ခုပြောရမယ်ဆိုရင် နေရာအစုံကို သယ်သွားသယ်လာလုပ်ကြတဲ့ Portable Computer တွေ လွယ်လွယ်ပြောရရင် Laptop တွေပေါ့ဗျာ။ သူတို့က Wireless Network တွေမှာ ဟိုနေရာမှာ သုံးလိုက်၊ ဒီနေရာမှာ သုံးလိုက် သုံးကြမှာမဟုတ်လား။ ဒီလိုရွှေ့ပြောင်းနေတဲ့ Computer Client တွေအတွက် IP သတ်မှတ်တဲ့ နေရာမှာ ပိုမိုမြန်ဆန်လွယ်ကူသွားတာပေါ့။

၆.၅ DHCP Server ကို Install လုပ်ခြင်း

ခန့်တန်းခန့် - ဇာတ်လမ်းကအခုမှစတယ်။ သင်တို့က တစ်ခုခုဆို လုပ်ကြည့်လိုက်ရမှ၊ ထိုင်ပြီး ဖတ်နေရင် ပျင်းလာရော။ ဒီတော့ Server ကိုလည်း Install ကလုပ်ချင်လှပြီ။ ကျုပ်ကလည်းစကားကြောက ရှည်နေတော့ ပျင်းနေပလားတောင်မသိဘူး။ ကဲစပါပြီဗျာ။

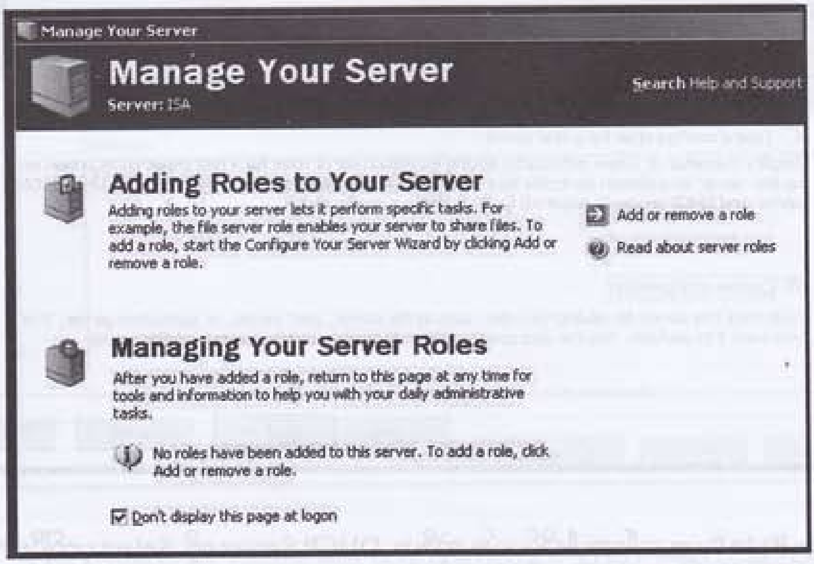
၁။ DHCP Server ကို Install လုပ်ဖို့ရာ ပထမဦးစွာ Manage Your Server ကိုသွားရမှာဖြစ်ပါတယ်။ Start Menu အောက်က All Programs အောက်က Administrative Tools အောက်က Manage Your Server ကိုသွားပါ။

ပုံ ၆.၃



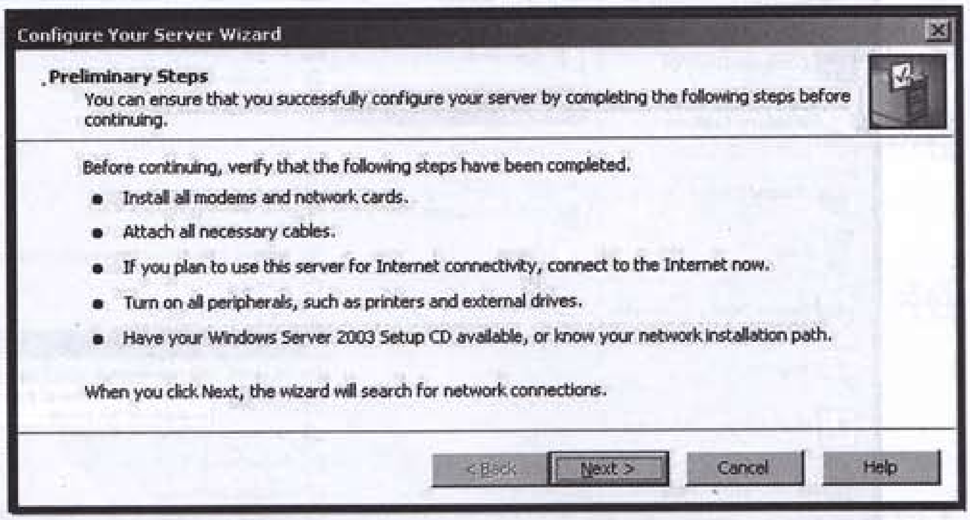
၂။ ပြီးလျှင် Add or Remove a Role ကိုသွားပါ။

ပုံ ၆.၄



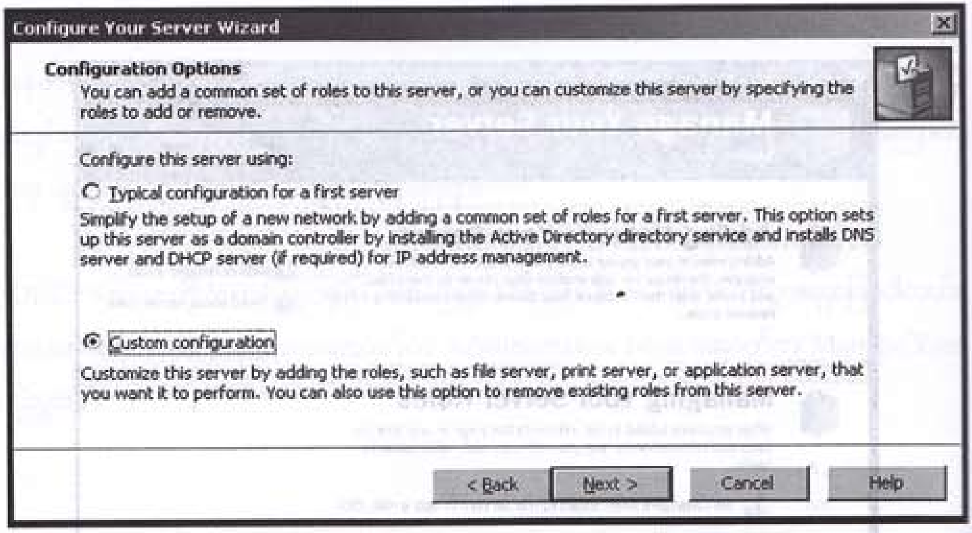
၃။ Preliminary Steps ဆိုသည့်ပုံပေါ်လာလျှင် Next လို့ပဲပြောပါ။

ပုံ ၆.၅



၄။ Configuration Option Dialog Box ပေါ်နေလိမ့်မယ်။ အဲ့ဒီမှာ Custom Configuration Check Box ကို On လိုက်ပါ။ ပြီးရင် Next လို့ပြောပါ။

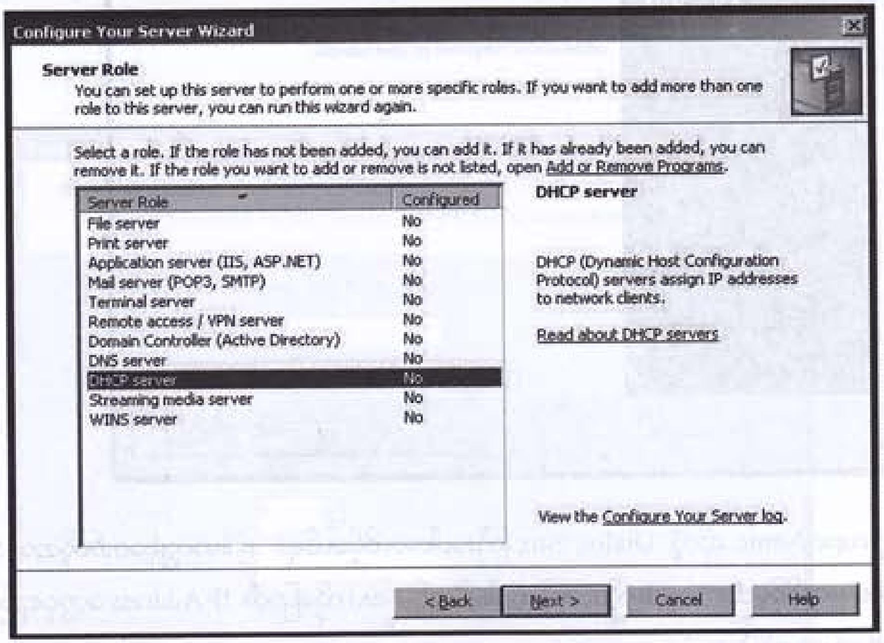
ပုံ ၆.၆



၅။ Server Role Page ပေါ်လာပါလိမ့်မယ်။ အဲ့ဒီမှာ DHCP Server ကို Select မှတ်ပြီး Next ကို

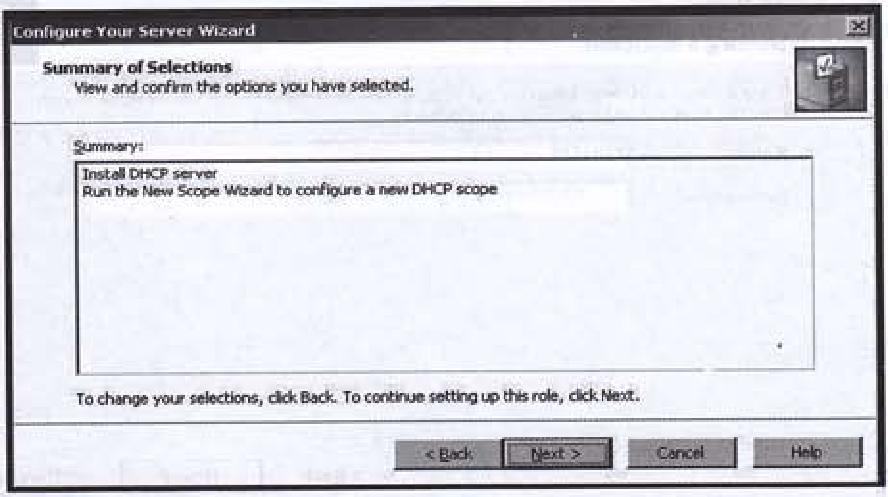
နှိပ်ပါ။

ပုံ ၆.၇



၆။ Summary Dialog Box ပေါ်လာရင် Next မှာနှိပ်ပေးပါ။

ပုံ ၆.၈

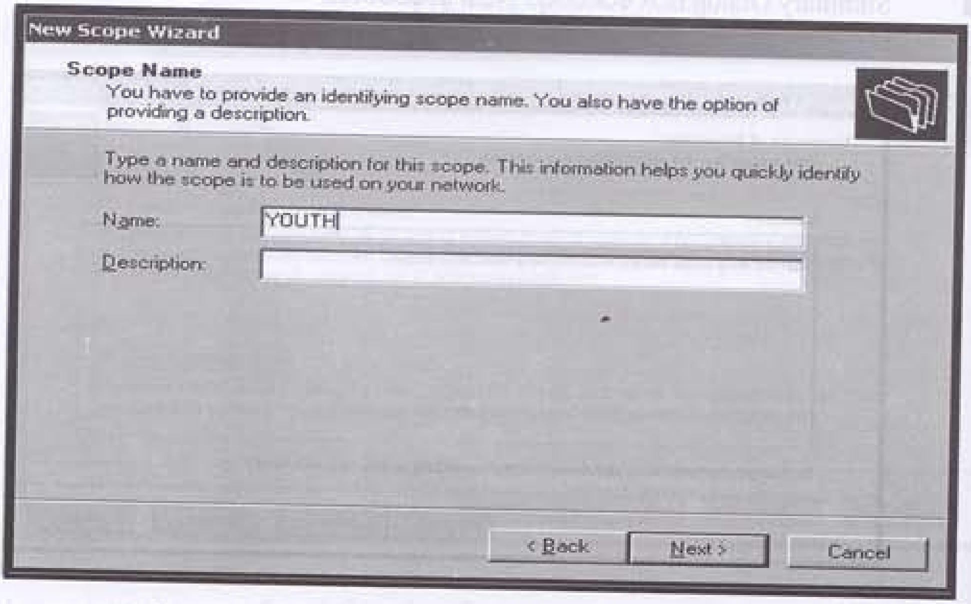


၇။ New Scope ပေးဖို့ Dialog Box ပေါ်လာပါလိမ့်မယ်။ အဲ့ဒီမှာ Next လို့ပြောပါ။

ပုံ ၆.၉

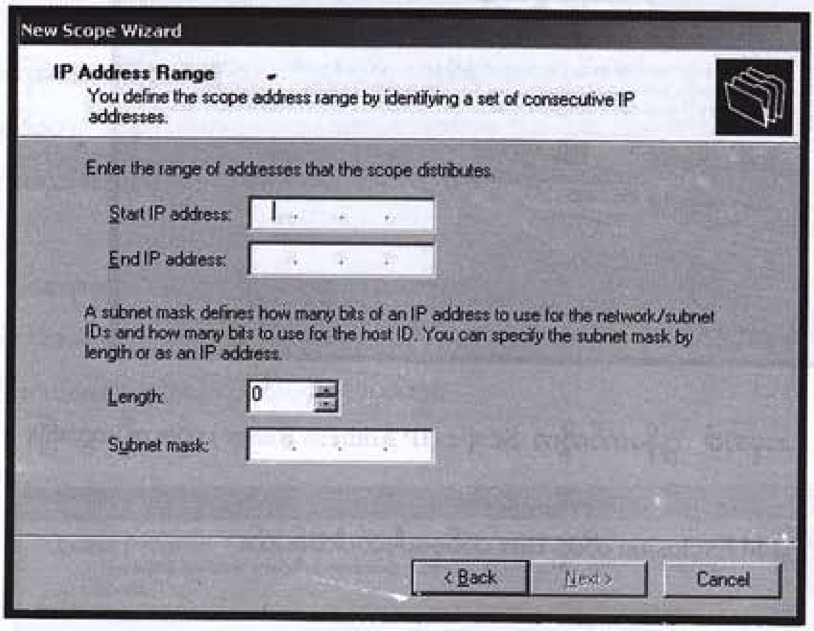
၈။ Scope Name ဆိုတဲ့ Dialog Box ကြီးပေါ်လာလိမ့်မယ်ဗျ။ အဲ့ဒီမှာကျွန်တော်တို့တာ Scope Name ကို ပေးရလိမ့်မယ်။ Youth လို့ပေးလိုက်ပါ။ ပြီးရင် Next လို့ပြောပါ။ IP Address တွေစုစည်း ထား တဲ့နေရာကို ပြောတာဖြစ်တယ်။

ပုံ ၆.၁၀



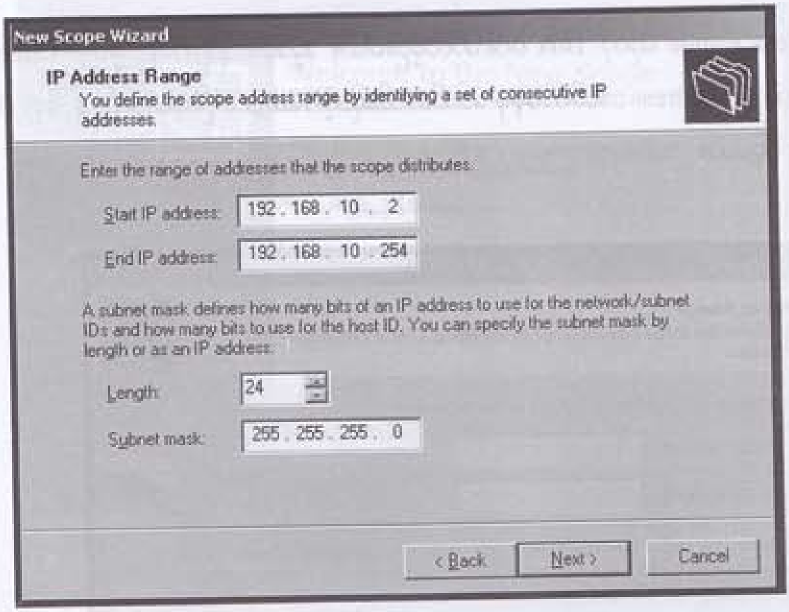
၉။ IP Address Range ဆိုတဲ့ Box ပေါ်လာလိမ့်ဦးမယ်။ အဲ့ဒီမှာ ခုနကပြောခဲ့တဲ့ Youth ဆိုတဲ့ Scope မှာထားရှိမယ့် IP Address ဘယ်ကနေမှ ဘယ်အထိဆိုတဲ့ Range ကိုပေးရမယ်။ အဲ့ဒီမှာ Subnet Mask ကိုလဲပေးရလိမ့်မယ်။

ပုံ ၆.၁၁



၁၀။ ကျွန်တော်တို့က ဒီနေရာမှာ Start IP Address ကို 192.168.10.2 လို့ပေးမယ်။ End IP Address ကို 192.168.10.254 လို့ပေးလိုက်ရအောင်။ ဒါဆို အခုကျွန်တော်တို့ IP Address Range ကိုပေးလိုက်ပါပြီ။ ဘယ်ကနေဘယ်အထိလဲ 2 ကနေမှ 254 အထိဖြစ်ပါတယ်။ အောက်က Subnet Mask ကတော့ သူ့ဘာသာ သူပေါ်လာမှာဖြစ်ပါတယ်။ ပြီးရင် Next လို့ပြောရအောင်။

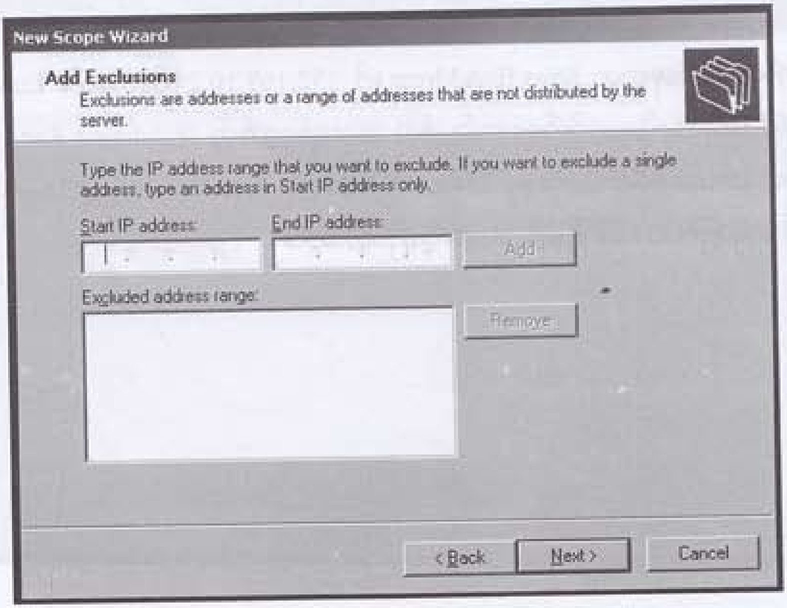
ပုံ ၆.၁၂



ကဲ. . . .အခုအခါ ကျွန်တော်တို့က Scope (IP Address Range) လို့ပေးပြီးသွားပြီ။

၁၀။ ဒီတစ်ခါ Add Exclusion ဆိုတဲ့ Box တစ်ခုပေါ်လာပါလိမ့်မယ်။

ပုံ ၆.၁၃

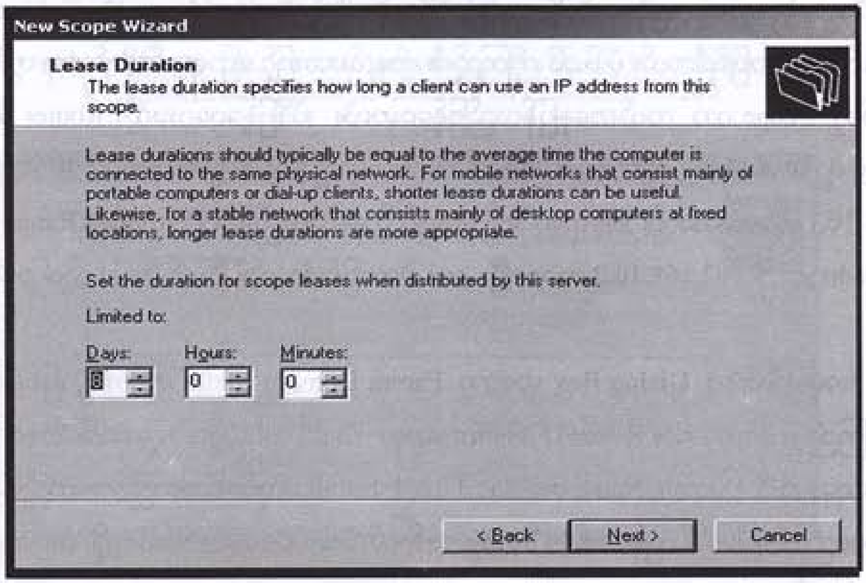


Exclusion ဆိုတာ DHCP Server ကနေ အငှားမချစေချင်တဲ့ အသုံးမပြုစေချင်တဲ့ Address တွေကိုပြောတာဖြစ်ပါတယ်။ အပေါ်က IP Address Range ထဲကမှ ဒီနံပါတ်၊ ဒီ IP တွေကိုတော့ဖြင့် အငှား မချစေချင်ဘူး။ ဒီ IP တွေကို ဖယ်ထားပေးပါဆိုပြီး ဒီနေရာမှာပြောပေးရမှာဖြစ်ပါတယ်။ ပြီးရင် Next လို့ပြောပါ။

၁၂။ Lease Duration ဆိုတဲ့ Dialog Box တစ်ခုပေါ်လာပါလိမ့်မယ်။ Lease Duration ဆိုတာ အငှား ချမယ့် အချိန်ကာလလေ။ ရှေ့မှာပြောခဲ့ဖူးတယ်လေ။ အိမ်ငှားမယ်။ ၆ လ ငှားမှာလား၊ ၁ နှစ်ငှားမှာလား ဆိုတာလေ။ ဒီတော့ ဒီနေရာမှာက Lease Duration ကပုံမှန် 8 ရက်ဗျ။ ကျွန်တော်တို့က ဒီနေရာမှာရက် 30 ထားလိုက်မယ်။ Days မှာ 30 လို့ပြောပါ။ ပြီးမှ Next ပြောပါ။

ဒီနေရာမှာ သိရမှာက ကိုယ့်ရုံးတွေ၊ ဘာတွေအပြောင်းအလဲနည်းမယ့် နေရာတွေဆို Lease Duration ကိုတိုးပေးထား။ ရက်များများထားပေါ့ဗျာ။ ဥပမာ Remote Connection တွေ၊ Laptop တွေဆိုရင်တော့ Lease Duration ကိုရက်အကြာကြီးမပေးသင့်ပါဘူး။

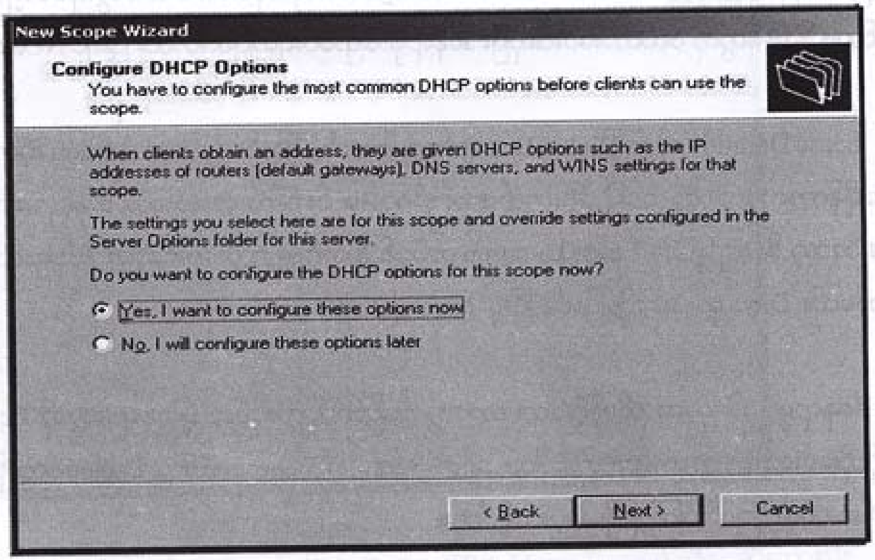
ပုံ ၆.၁၄



၁၃။ အခုတစ်ခါပေါ်လာတဲ့ Box ကတော့ DHCP Options ဆိုတဲ့ Dialog Box ပဲဖြစ်ပါတယ်။ သူကမေး တာက မင်း DHCP Options တွေကို အခု Configure လုပ်မလား၊ နောက်မှလုပ်မလားဆိုပြီးမေးနေတာ ဖြစ်ပါတယ်။ ကျွန်တော်တို့ကတော့ အခုပဲ Configure လုပ်မှာမို့ Yes ဆိုပြီး ရွေးကာရှေ့ဆက်သွားရမှာ

ဖြစ်ပါတယ်။ Yes ကိုရွေးပြီး Next လို့ပြောပါ။

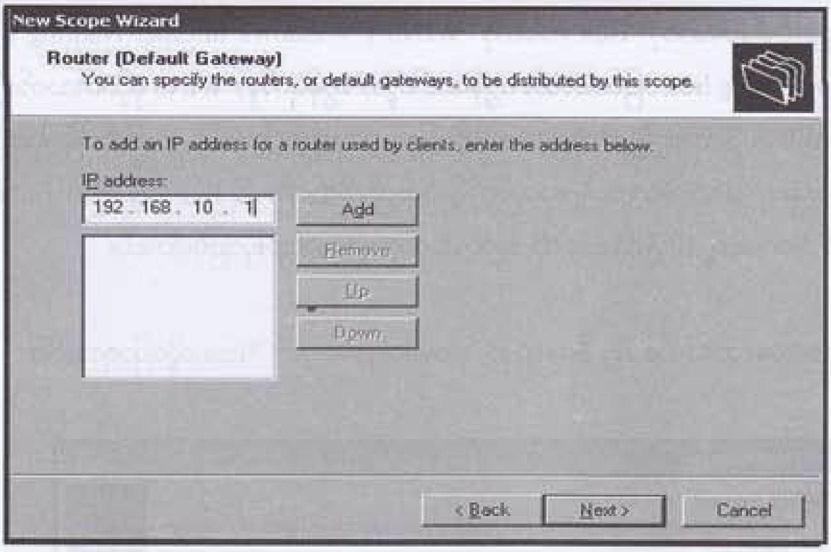
ပုံ ၆.၁၅



၁၄။ ဒီအဆင့်မှာတော့ ကျွန်တော်တို့ဟာ လက်ရှိကွန်ရက်ရဲ့ Router ဒါမှမဟုတ် Gateway ရဲ့ IP Address ကိုပေးရမှာဖြစ်ပါတယ်။ ပုံ ၆.၁၆ ကိုကြည့်ပါ။ တနည်းအားဖြင့် ပြောရမယ်ဆိုရင် အခု ကျွန်တော်တို့ ပေးလိုက်တဲ့ Scope ဟာ ဘယ်ကနေပြန်လည်ဖြန့်ဝေမှာလဲ။ အဲဒီဖြန့်ဝေပေးမယ့် Router ဒါမှမဟုတ် Gateway ရဲ့ IP Address ကိုပေးရမှာ ဖြစ် ပါတယ်။ အခုကျွန်တော်တို့ ဒီနေရာမှာ IP Address ကို 192.168.10.1 လို့ပေးရအောင်။ ဒီနေရာမှာ ဒီလို ပေးချင်လို့ ခုနကတည်းက IP Address Range (Scope) မှာ IP Address ကို 192.168.10.2 ကနေစပြီး ပေး ခဲ့တာဖြစ်ပါတယ်။ ပြီးရင် Next လို့ပြောပါ။

၁၅။ ဒီအခုပေါ်လာတဲ့ Dialog Box မှာတော့ Parent Domain Name ကိုပေးရမှာဖြစ်ပါတယ်။ ပုံ ၆.၁၇ ကိုကြည့်ပါ။ ဒီတော့ကား Parent Domain နေရာမှာ Youth.com လို့ပေးရအောင်။ ဒီနေရာမှာတစ်ခု သတိထားရမှာက ဒီ Domain Name ဟာ သင် DHCP Install မလုပ်ခင်ကတည်းက တည်ရှိခဲ့တဲ့ Domain ရဲ့နာမည်ဖြစ်ရပါ့မယ်။ ကျွန်တော်က ဒီစာအုပ်တစ်အုပ်လုံးမှာ Domain Name ကို Youth.com နဲ့ပဲ ပြသွားမှာ ဖြစ်ပါတယ်။

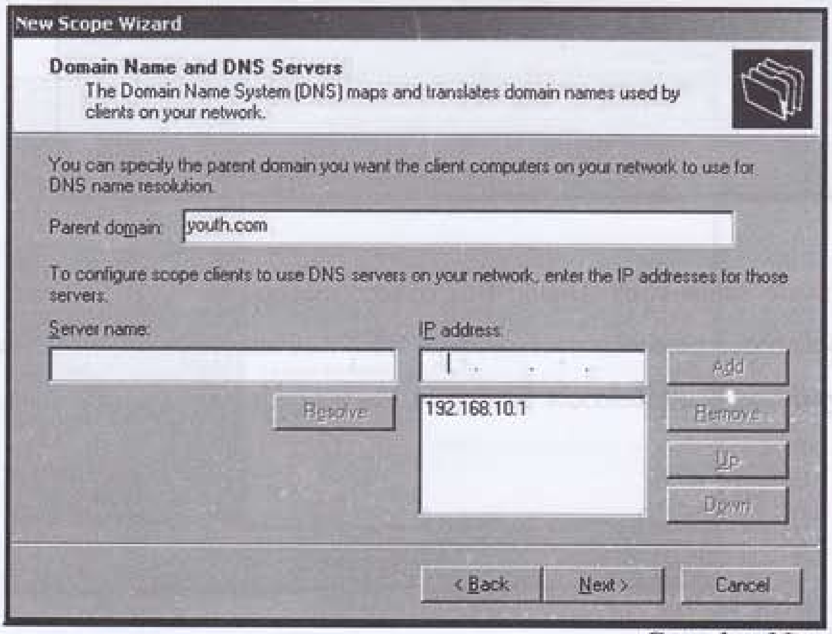
ပုံ ၆.၁၆



ထို့အတူ Server Name ဟာလည်း ယခင်ကတည်းကရှိခဲ့တဲ့ Server Name ပဲဖြစ်ပါတယ်။ Server Name ကိုတော့ Server လို့ပဲပေးရအောင်။ သင်ဒီအကြောင်းတွေကို စမ်းသပ်တဲ့အခါ ဒီ Domain Name တို့ Server Name တို့ဟာ သင့်ကွန်ရက်မှာရှိတဲ့အတိုင်း ဖြစ်ရမှာနော်။ ကျွန်တော်ပြောတာနှင့်မဆိုင်ဘူး။

IP Address ကိုတော့ 192.168.10.1 လို့ပေးရအောင်။ ပြီးရင် Next ကိုနှိပ်ပါ။

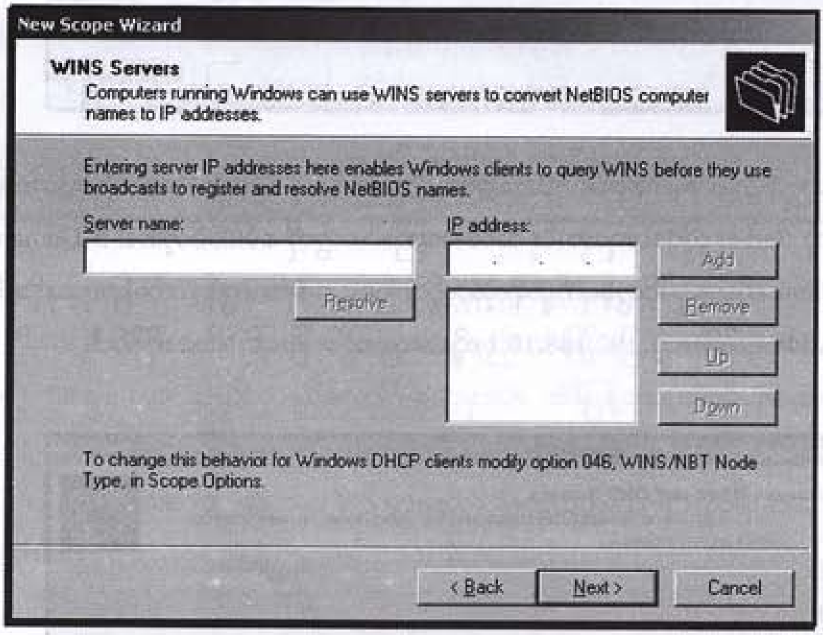
ပုံ ၆.၁၇



၁၆။ အခုတစ်ခါပေါ်လာတဲ့ Box ကတော့ WINS (Windows Internet Naming System) နှင့်ပတ်သက်တဲ့ Dialog Box ပဲဖြစ်ပါတယ်။ ကျွန်တော်တို့က ကွန်ရက်မှာ WINS နှင့်ပတ်သက်တဲ့ Server ရှိခဲ့ရင် အခု WINS Server ရဲ့ IP Address ကိုပြောပေးရမှာဖြစ်ပါတယ်။ ဘယ်လိုပြောရမလဲဆိုတော့ Server Name မှာ WINS Server ရဲ့ နာမည်ကိုရိုက်ထည့်လိုက်၊ ပြီးရင် Resolve ဆိုတဲ့ Button မှာနှိပ်လိုက်ရင် အဲ့ဒီ Server ရဲ့ IP Address ကို သူ့ဘာသာသူ ရှာပေးသွားမှာဖြစ်ပါတယ်။

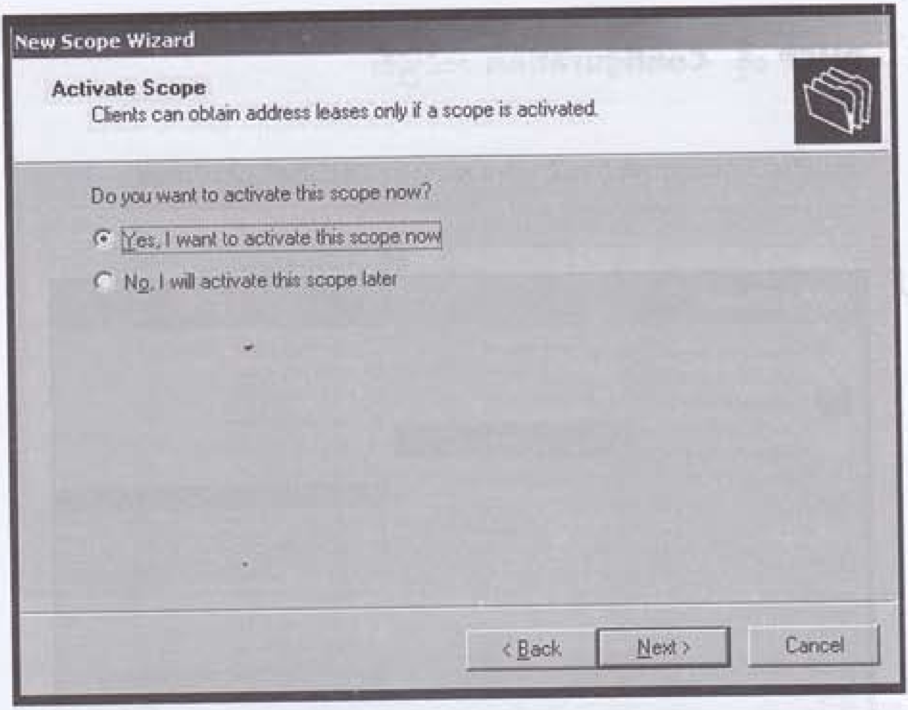
အခုလောလောဆယ်တော့ ဒီနေရာမှာ ဘာမှမပြောတော့ဘဲ Next လို့ပြောရအောင်။

ပုံ ၆.၁၈



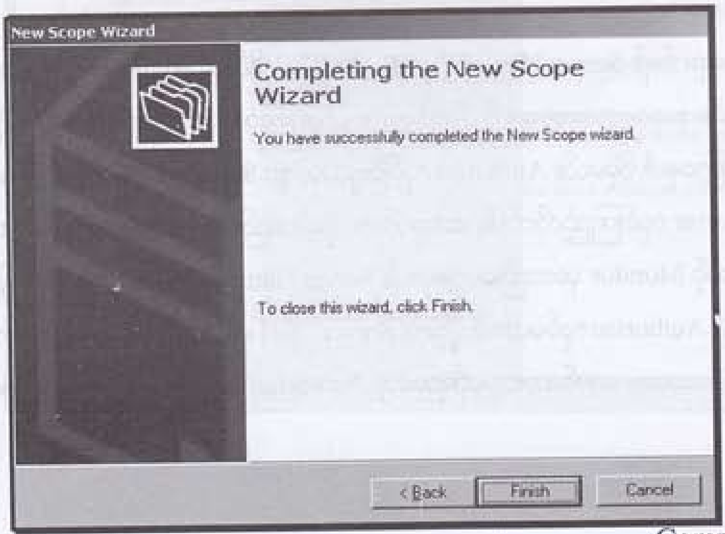
၁၇။ Activate Scope ဆိုတဲ့ Dialog Box ကတော့ အခုကျွန်တော်တို့ပေးထားခဲ့တဲ့ Scope ကိုအသက်သွင်း တော့မလား၊ စတင်တော့မလားပေါ့ဗျာ။ အဲ့ဒီလို Activate လုပ်မှသာလျှင် Client တွေဆီကို Address တွေအငှားချ နိုင်မှာဖြစ်ပါတယ်။ ဒီတော့ကား Yes မှာရွေးပြီး Next လို့ပြောပါ။

ပုံ ၆.၁၉



၁၈။ နောက်ဆုံးပေါ်လာတဲ့ Dialog Box ကတော့ ပြီးဆုံးပြီဆိုတဲ့ Box ပါပဲ။ Finish မှာ Click တစ်ချက်နှိပ်ပါ။ နောက်ထပ် Box တစ်ခုပေါ်လာပါလိမ့်ဦးမယ်။ အဲ့ဒီမှာလည်း Finish လို့ပြောပေးပါ။

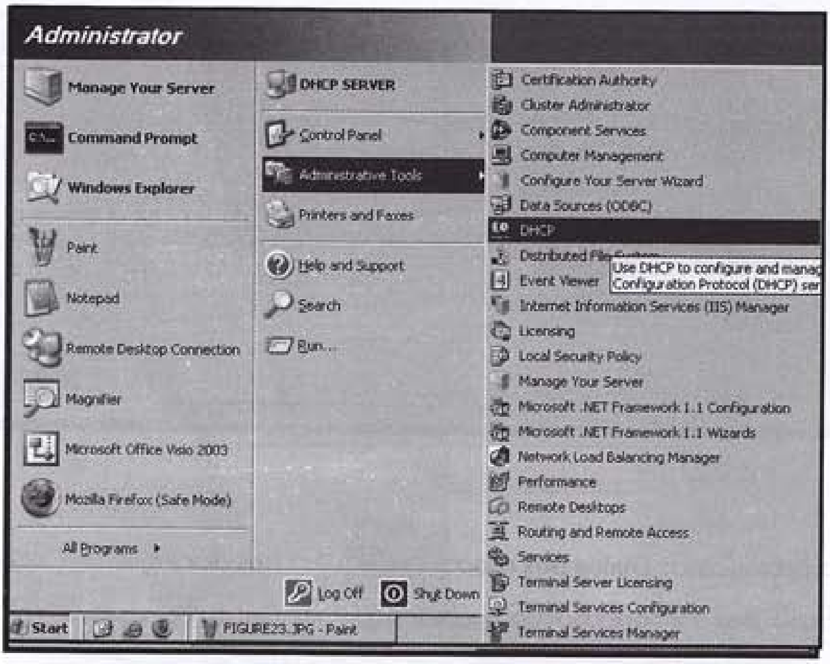
ပုံ ၆.၂၀



၆.၆ DHCP ထို Configuration လုပ်ခြင်း

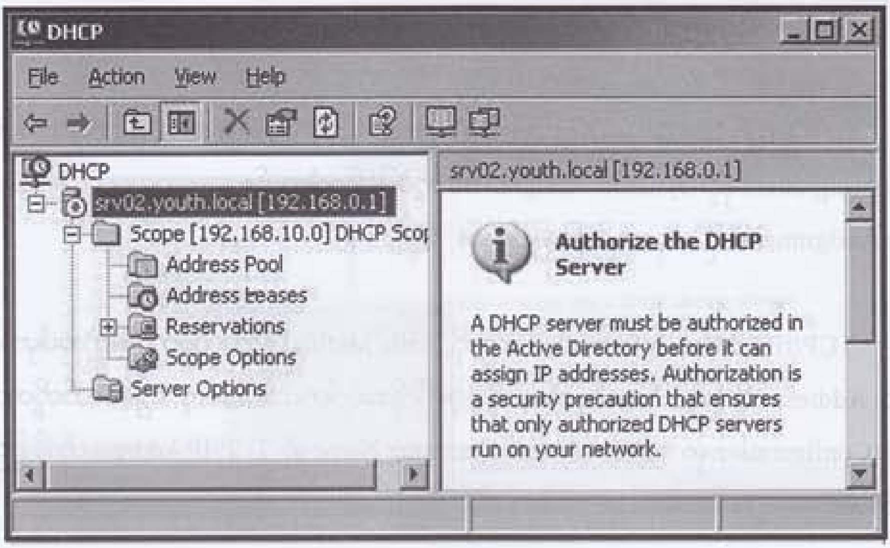
၁။ ပထမဦးစွာ Administrative Tools အောက်က DHCP ကို ဝင်လိုက်ပါ။

ပုံ ၆.၂၁

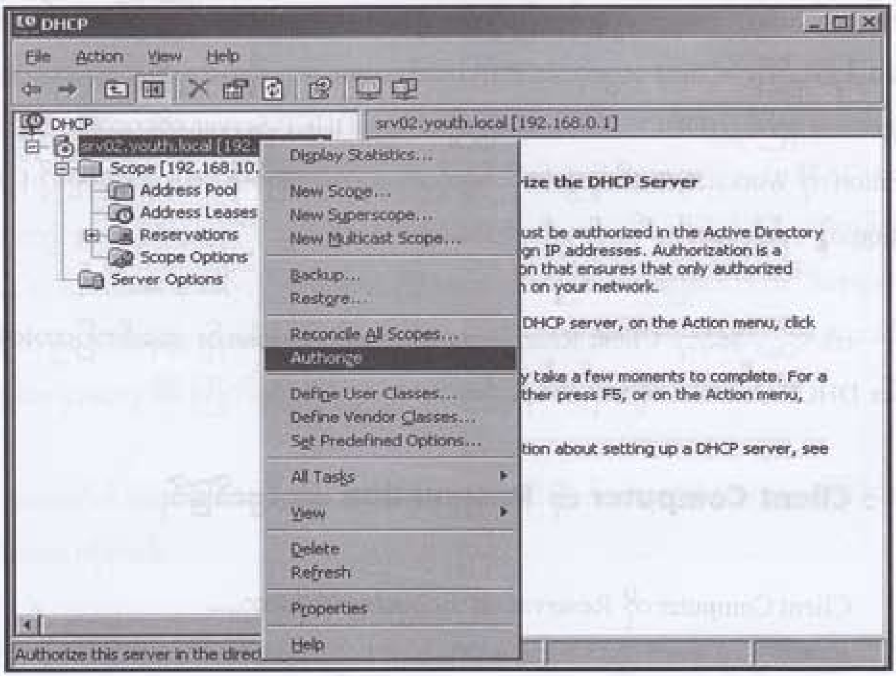


၂။ DHCP ထဲကိုရောက်ရင် Server Name ပေါ်မှာ Right Click နှိပ်ပြီး Authorise ပြုလုပ်ရပါတယ်။ ပုံမှာလည်းပြထားပါတယ်။ အခုလောလောဆယ် Authorise မလုပ်ရသေးတာကြောင့် DHCP ရဲ့ Status မှ Not Authorised လို့ပြောနေပါလိမ့်မယ်။ Authorise လုပ်ပြီးမှသာလျှင် Status မှာ Running လို့ ပေါ်လာမှာဖြစ်ပါတယ်။ ကဲ Authorise လုပ်ကြည့်လိုက်ပါ။ အောက်က ပုံမှာလည်းပြပေးထားပါတယ်။ Status မှာ Running ဖြစ်သွားပါပြီ။ သင့် Monitor မှာလည်းတွေ့ရမှာပါ။ Server Name ရဲ့ ဘယ်ဘက်ခြမ်းမှာ မြှားအစိမ်းလေးကိုတွေ့ရမှာပါ။ အဲ့လို Authorise လုပ်မယ်ဆိုလျှင်ရှိရင် Server 2003 မှာ Active Directory တင်ထားဖို့လိုအပ်ပါတယ်။ Active Directory မတင်ထားဘူးဆိုရင်တော့ Authorise/Unauthorise လုပ်စရာမလိုပါဘူး။

ပုံ ၆.၂၂


DHCP
File Action View Help
DHCP
srv02.youth.local [192.168.0.1]
Scope [192.168.10.0] DHCP Scop
Address Pool
Address Leases
Reservations
Scope Options
Server Options
srv02.youth.local [192.168.0.1]
Authorize the DHCP Server
A DHCP server must be authorized in the Active Directory before it can assign IP addresses. Authorization is a security precaution that ensures that only authorized DHCP servers run on your network.

ပုံ ၆.၂၃


DHCP
File Action View Help
DHCP
srv02.youth.local [192.
Scope [192.168.10.
Address Pool
Address Leases
Reservations
Scope Options
Server Options
srv02.youth.local [192.168.0.1]
Display Statistics...
New Scope...
New Superscope...
New Multicast Scope...
Backup...
Restore...
Reconcile All Scopes...
Authorize
Define User Classes...
Define Vendor Classes...
Set Predefined Options...
All Tasks
View
Delete
Refresh
Properties
Help
Authorize this server in the direc

၆. ၇ **Static Assignment**

DHCP တွင် IP Address တွေ Assign လုပ်ရမှာ နည်းလမ်း (၂) လမ်း ရှိပါတယ်။ အဲဒါကတော့- Static Assignment နှင့် Dynamic Assignment တို့ပဲဖြစ်ကြပါတယ်။
Static Assignment ကို အရင်ပြောပြပါ့မယ်။

TCP/IP Address Information တွေကို Static Method နှင့်သတ်မှတ်ပေးတဲ့အခါမှာ ကျွန်တော်တို့ဟာ Address ကို ကြိုတင်သတ်မှတ်ပေးဖို့ လိုကိုလိုအပ်ပါတယ်။ ဒီတော့ ကျွန်တော်တို့ဟာ DHCP Server Configuration မှာ MAC Address, Computer Name နှင့် TCP/IP Address တို့ကို ဖြည့်ပေးရမှာ ဖြစ်ပါတယ်။

DHCP Server ဟာ ၎င်း Station အတွက် IP Address တောင်းဆိုမှုကိုလက်ခံရရှိတဲ့အခါမှာ ၎င်းဟာ တောင်းခံတဲ့ Station ရဲ့ (ခုနကဖြည့်ထားတဲ့) MAC Address ကိုကြည့်ပြီး (၎င်း MAC Address ပေါ်မူတည်ပြီး) Client တွေကို TCP/IP Information တွေကိုသတ်မှတ်လိုက်ပါတယ်။ ဒီ Static Assignment နည်းမှာ DHCP Server ဟာဖြည့်ထားတဲ့ DHCP Server ကိုကြည့်ပြီး TCP/IP Configuration ကို Workstation ဆီ ပို့လွှတ်လိုက်ရုံကိုသာ လုပ်ရတာဖြစ်ပါတယ်။ ဒီ ဖြစ်စဉ်ကို Client Reservation လို့ ခေါ်ပါတယ်။

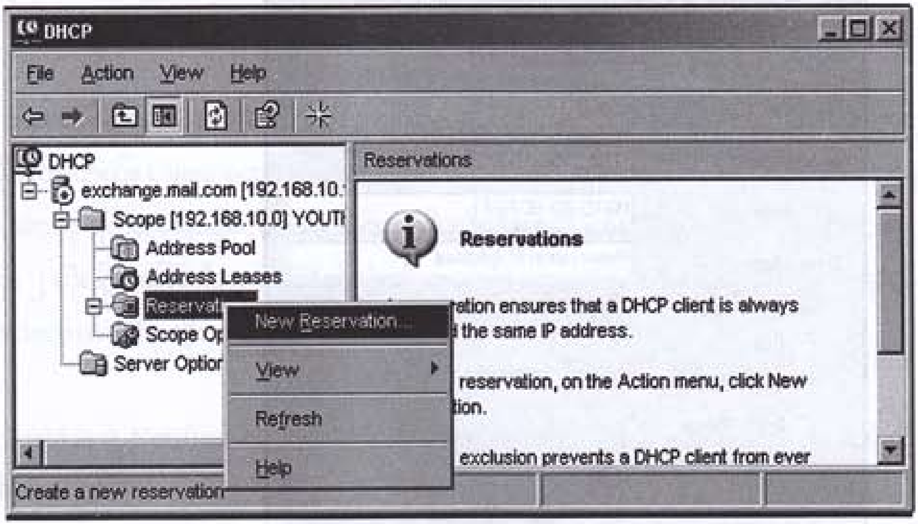
တဲ. . . . ဒီတော့ Client Reservation ဆိုတာကိုလုပ်ပြပါမယ်။ အပေါ်ကပြထားတဲ့ ပုံ ၆.၂၃ အတိုင်း DHCP Console ကို ရောက်နေရပါ့မယ်။

၆. ၇. ၁ **Client Computer ကို Reservation သတ်မှတ်ခြင်း**

Client Computer ကို Reservation သတ်မှတ်မယ်ဆိုတော့.....

၁။ DHCP Console ထဲက Scope Folder ကို ဖြန့်ချပါ။ ပြီးရင် Reservation Folder ပေါ်မှာ Right Click နှိပ်။ ပြီးရင် New Reservation ကို နှိပ်ပါ။

ပုံ ၆.၂၄

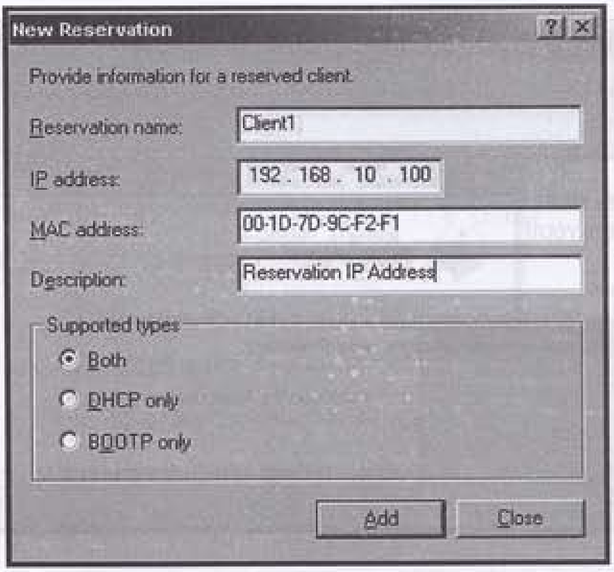


၂။ ဒါဆိုရင် New Reservation ဆိုတဲ့ Dialog Box ပေါ်လာပါမယ်။ အဲ့ဒီ New Reservation Dialog Box ထဲက Reservation Name မှာမိမိ သတ်မှတ်ချင်တဲ့ ကွန်ပျူတာရဲ့ နာမည်ကိုပေးပါ။ ကျွန်တော်ကတော့ Client1 ဆိုတဲ့ နာမည်ပဲသတ်မှတ်ပေးထားပါတယ်။ IP Address နေရာမှာ မိမိသည် DHCP Server မှ Static IP Address Assinge ချချင်တဲ့ ကွန်ပျူတာအတွက် IP Address ကိုထည့်ပါ။ ကျွန်တော်ကတော့ 192.168.10.100 ဆိုတဲ့ IP Address ကိုပဲ သတ်မှတ်ပေးထားပါတယ်။ အခုပြောမယ့် MAC Address နေရာကတော့ အရေးကြီးတယ်ဗျ။ အဲ့ဒီ MAC Address နေရာမှာထည့်ရမှာသည် Client ကွန်ပျူတာရဲ့ Network Connection မှာပါရှိတဲ့ Physical Address ကိုထည့်ပေးရမှာဖြစ်ပါတယ်။ ဒီနေရာမှာတော့ ကျွန်တော်က ဥပမာအနေနဲ့ ကျွန်တော့ Client ကွန်ပျူတာရဲ့ Physical Address ကိုပဲထည့်ပြပေးထားပါတယ်။ Description မှာတော့ မိမိ ကြိုက်နှစ်သက်ရာ နာမည်ကို ရိုက်ထည့်ပေးနိုင်ပါတယ်။

၃။ အထက်ပါ အချက်အလက်တွေအားလုံး ပြည့်စုံသွားပြီဆိုရင်တော့ Add Button ကိုနှိပ်ပါ။ ပြီးရင် Close Button ကိုနှိပ်ပါ။

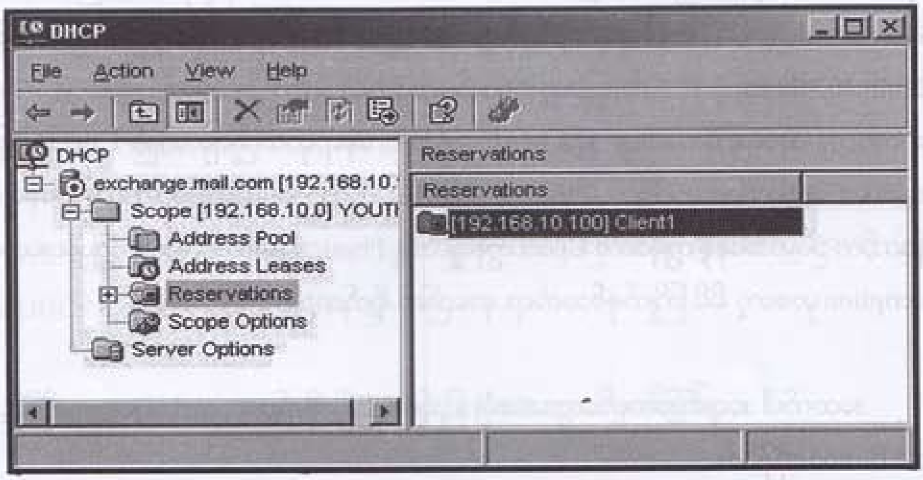
မှတ်ချက်။ ။ MAC Address နှင့် Physical Address သည် အတူတူပဲဖြစ်သည်။ Network Card တိုင်းမှာ Physical Address ပါရှိသည်။ Network Card တိုင်းရဲ့ Physical Address သည် တစ်ခုနှင့်တစ်ခု မတူညီကြပါ။

ပုံ ၆.၂၅



Reservation သတ်မှတ်ပေးပြီးပြီဆိုရင်တော့ ပုံ ၆.၂၆ အတိုင်းမြင်တွေ့ရမှာ ဖြစ်ပါတယ်။ ဒါဆိုရင်တော့ Client ကွန်ပျူတာအတွက် Reservation သတ်မှတ်တာပြီးဆုံးသွားပါပြီ။

ပုံ ၆.၂၆



၆.၈ **Dynamic Assignment**

ဒီသင်ခန်းစာ တစ်လျှောက်လုံးပြောပြခဲ့တဲ့ DHCP Server မှ IP Address များ အငှားချထားခြင်းဆိုတာဟာ ဒီ Dynamic Assignment ကိုပြောနေတာဖြစ်ပါတယ်။ ဒါကြောင့် သူ့ကို အစအဆုံး ပြန်ရှင်းပြမနေ

တော့ဘဲ Client တွေကနေ IP Address များရယူခြင်းကိုသာ ရှင်းပြသွားမှာဖြစ်ပါတယ်။

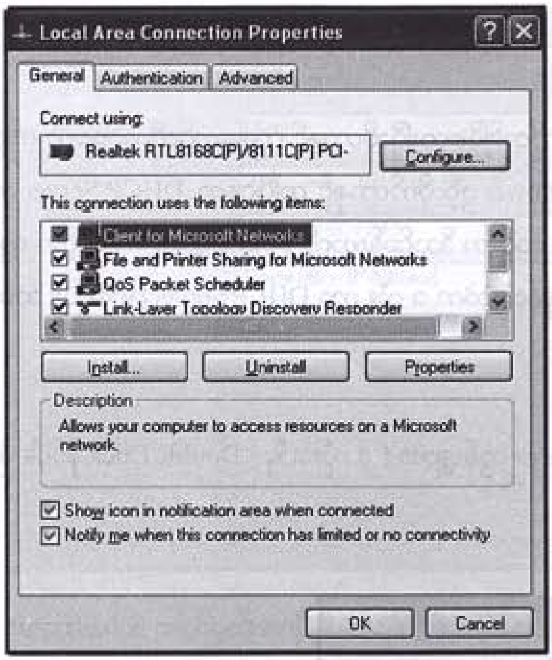
တကယ်တော့ DHCP Server ကိုတင်ပြီးသွားပြီဆိုတာနှင့် ကျွန်တော်တို့လုပ်ရမယ့် ကိစ္စတွေက ပြီးသွားပြီ ဖြစ်ပါတယ်။ Client တွေဟာ Power ဖွင့်လိုက်တာနှင့် တပြိုင်နက် DHCP Server ကနေ IP Address တွေကို ရယူသွားမှာဖြစ်ပါတယ်။ သင်ဟာ ဒီသင်ခန်းစာကို စမ်းသပ်ဖို့အတွက် သင့်မှာ ကွန်ပျူတာ အနည်းဆုံး ၂ လုံး ရှိရမှာဖြစ်ပါတယ်။ အဲဒီနှစ်လုံးထဲက ၁ လုံး ဟာ DHCP Server ဖြစ်နေပြီး၊ အခုသင်ဟာ Client (Windows XP) ကိုလာလိုက်ပါ။

၁။ Taskbar ရဲ့ Notification Area မှာ ကွန်ပျူတာ (၂) လုံးပေါ်မှာ Double Click နှိပ်ပါ။ ပုံ (၆.၂၇) ပေါ်လာပါလိမ့်မယ်။

ပုံ ၆.၂၇

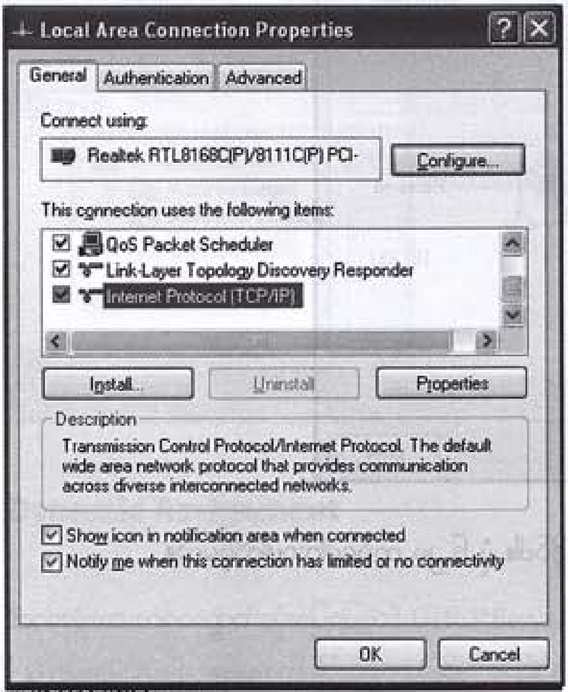
၂။ ပြီးရင် အဲဒီမှာ Properties ကိုနှိပ်ပါ။ ပုံ ၆.၂၈ ထပ်ပေါ်လာပါလိမ့်မယ်။

ပုံ ၆.၂၈



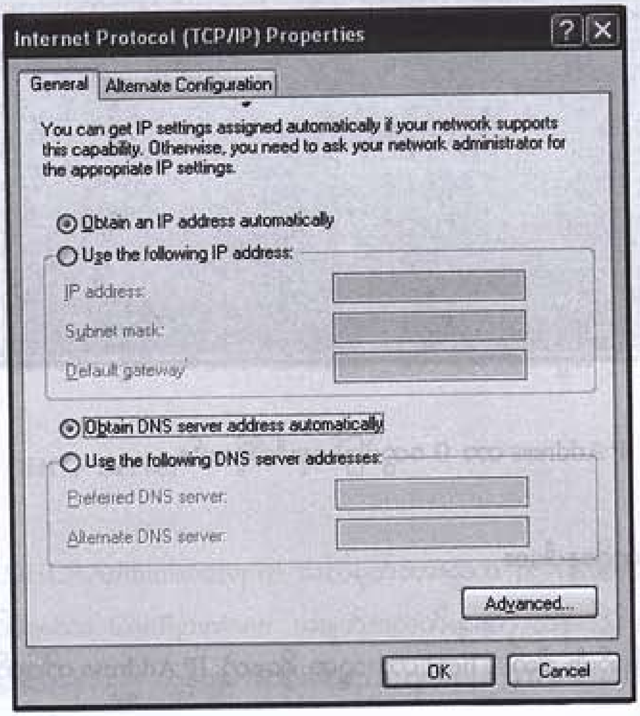
၃။ အဲဒီမှာ TCP/IP ကိုရွေးပါ။ ပြီးရင် Properties ကိုရွေးပါ။ ပုံ ၆.၂၉ ပေါ်လာပါလိမ့်မယ်။

ပုံ ၆.၂၉



၄။ အဲဒီမှာ IP Address ကို Manually ပေးတာမဟုတ်ဘဲ Obtain an IP Address Automatically လို့ပြောပါ။ ပြီးရင် OK ပြောပါ။ ဒါဆို Client ဟာ သူ့ရဲ့ IP Address ကို DHCP Server ကနေရယူသွားတော့မှာဖြစ်ပါတယ်။ ပုံ ၆.၃၀ ကိုကြည့်ပါ။

ပုံ ၆.၃၀



၅။ တအောင့်ကြာတဲ့အခါ တနည်းအားဖြင့် Client ဟာ IP Address ကို DHCP Server ကနေ ရယူပြီးတဲ့ အချိန်လောက်မှာ........

❖ Command Prompt ကိုသွား။

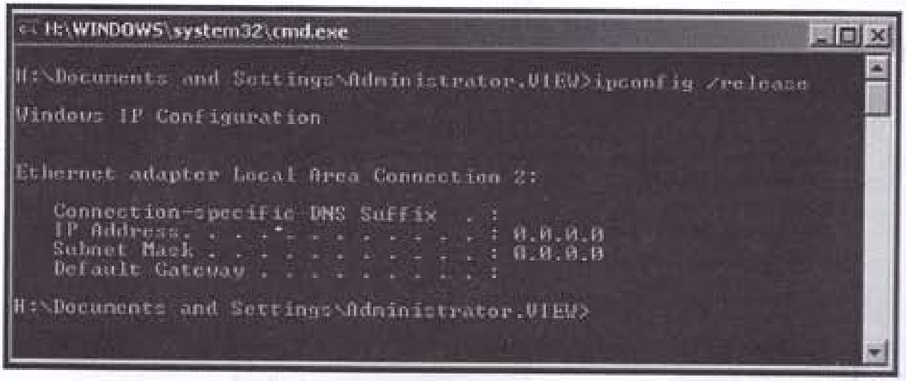
❖ Ipconfig လို့ရိုက်ပါ။ ဒါဆို DHCP ကနေ အငှားချထားလိုက်တဲ့ IP Address ကို သင်မြင်တွေ့ရပြီပေါ့။

၆။ ဒီအကြောင်းနှင့် ဆက်နွယ်ပြီးတော့ ပြောပြစရာ (၂)ခု ရှိပါတယ်။ တစ်ခါတည်း လုပ်ကြည့်ရအောင်။

❖ Command Prompt မှာရှိနေပါစေ။

❖ Ipconfig /release လို့ရိုက်ပါ။ ဒါဆို အခု Client ဟာ သူ့မှာ လက်ရှိအသုံးပြုနေတဲ့ IP Address ကို ဖြုတ်ချလိုက်ပြီးဖြစ်တယ်။

ပုံ ၆.၃၁



❖ အဲ့ဒီမှာကြည့်လိုက်ပါ။ IP Address ဟာ 0 တွေပဲဖြစ်နေပါလိမ့်မယ်။

၇။ Command Prompt မှာရှိနေပါစေ။

❖ Ipconfig /renew လို့ရိုက်ပါ။ ဒါဆို Client ဟာ သူ့မှာ ရှိနေတဲ့ IP Address ကိုဖြုတ်ချပြီး IP Address အသစ်လဲပါလိမ့်မယ်။

ပြီးရင် Ipconfig လို့ ပြန်ရိုက်ကြည့်ပါ။ အသစ်ဖြစ်ပေါ်လာတဲ့ IP Address ဟာ ယခင် IP Address ပဲဖြစ်နေပါလိမ့်မယ်။ DHCP ကပေးတာဟာ Dynamic Assignment ဖြစ်တာကြောင့် ကိုယ် လိုချင်တဲ့ နံပါတ်တော့ မရဘူးပေါ့ဗျာ။ ဒါပေမယ့် အခု ရလာတဲ့ IP Address ဟာ သက်တမ်းအသစ် ဖြစ်သွားပါတယ်။ သူ့သက်တမ်း ဟာ ၈-ရက်ရှိတယ်။ သုံးလာတာ ၅-ရက်ရှိပြီ။ သက်တမ်း ၃-ရက် ပဲကျန်တော့ တယ်။ အခု Ipconfig/release လုပ်လိုက်တာကြောင့် အခုရလာတဲ့ IP Address ဟာ ယခင် နံပါတ်အတိုင်း ဖြစ်နေသည့်တောင် အဲလေ ဖြစ်နေသည့်တိုင်၊ သက်တမ်း (၈) ရက်ပြန်ဖြစ်သွားပါသတဲ့။

ပုံ ၆.၃၂

အခု DHCP နှင့်ပက်သတ်နေတဲ့ အခေါ်အဝေါ်တွေ ထပ်ရှင်းပြပါဦးမယ်။

၆.၉ DHCP နှင့် ပတ်သတ်သော အခေါ်အဝေါ်များ

၁။ DHCP Server

DHCP Administrator က သတ်မှတ်ထားသော IP Address များ၊ ၎င်း IP Address များနှင့် ဆက်နွယ်နေသော Configuration အချက်အလက်များကို ထိန်းသိမ်းထားပေးသော DHCP Server Running ဖြစ်နေသည့် ကွန်ပျူတာကိုခေါ်သည်။ ၎င်းသည် DHCP Client က တောင်းခံသမျှကိုလည်း ပံ့ပိုးပေးရသည်။

၂။ DHCP Client

IP Configuration နှင့် ပက်သက်သည်များကို DHCP ကနေတောင်းခံသည့် ကွန်ပျူတာကို ခေါ်ပါသည်။

၃။ Scope

DHCP Server Service ကနေ DHCP Clients တွေဆီကို အငှားချထားမယ့် IP Address

Range (ဘယ်ကနေ ဘယ်အထိဆိုတဲ့ IP Address) ကိုခေါ်တာဖြစ်ပါတယ်။

၄။ Lease

DHCP ကနေ DHCP Client ဆီကို ပေးသုံးခွင့်ပြုထားတဲ့ IP Address ရဲ့ သတ်တမ်းပဲဖြစ်ပါတယ်။ အငှားချထားတဲ့ အချိန်ကာလကိုပြောတာဖြစ်ပါတယ်။

၅။ Reservation

ဒီကွန်ပျူတာ (DHCP Client) ကိုတော့ဖြင့် ဒီ IP Address ကိုပဲ တစ်သမတ်တည်း ပေးမယ်လို့ သတ်မှတ်ထားခြင်းကိုခေါ်တာဖြစ်ပါတယ်။ Static Assignment လို့လည်းခေါ်ပါတယ်။

၆။ Exclusion

DHCP Server Service ကနေမှ ဒီကနေ ဒီအထိသို့ ဒီ IP Address ကိုတော့ဖြင့် အငှားမချထားချင်ဘူး။ ပေးမသုံးစေချင်ဘူးဆိုပြီး ဖယ်ထားတဲ့ IP Address များကို ခေါ်တာဖြစ်ပါတယ်။ လွယ်လွယ်ပြောရရင် ပေးမသုံးစေချင်သော IP Address များဖြစ်ပါတယ်။

၇။ Unauthorized DHCP Server

DHCP Server ဟာ သူ့အလိုအလျောက် Authorise မဖြစ်ပါဘူး။ သူ့ကို Install လုပ်ပြီးတောင် အသုံးပြုဖို့ရာ Administrator ကသက်သက်ကို Authorise လုပ်ပေးရပါတယ်။ အဲဒီလို Authorise လုပ်မပေးဘူးဆိုရင် Unauthorise DHCP Server ဖြစ်နေပါလိမ့်မယ်။

၈။ Superscope

Network တစ်ခုတည်းအတွင်းမှာရှိတဲ့ Clients တွေကို DHCP Server ကနေ Address တွေ

အငှားချရာမှာ၊ တစ်ခုထက်ပိုတဲ့ Scope တွေကနေ အငှားချခြင်းကို Superscope လို့ခေါ်ပါတယ်။ ပြန်ပြောပြမယ်။ တစ်ခုထက်ပိုတဲ့ Scope ကနေ Address တွေ အငှားချခြင်းကို Super Scope လို့ခေါ်တယ်။

၉။ Multicast IP Address

IP Address တစ်ခုတည်းကနေ ပို့လွှတ်လိုက်တဲ့ Data တွေကို IP Address အများကြီးဆီမှ တနည်းအားဖြင့် Client အများကြီးဆီမှ လက်ခံနိုင်ခြင်းကို ဆိုလိုတာဖြစ်ပါတယ်။ ဒါကို Point to Multipoint Communication လို့ခေါ်ပါတယ်။ အဓိပ္ပါယ်ကတော့ ကွန်ပျူတာ တစ်ခုလုံးကနေ အများကြီးဆီသို့လို့ ဆိုလိုပါတယ်။ ဒီလို Transmission မျိုးကို Media Transmission တွေမှာ အသုံးပြုလေ့ရှိပါတယ်။ ဥပမာ Video Conferencing လိုမျိုးပေါ့။

၁၀။ Multicast Scope

DHCP Client တွေဆီကို သတ်မှတ်ပေးမယ့် Multicast IP Address အတိုင်းအတာ Range ကို ခေါ်တာဖြစ်ပါတယ်။

၁၁။ · BOOTP

DHCP နှင့် ပုံစံတူ ယခင်က အသုံးပြုခဲ့သော Protocol တစ်ခုဖြစ်ပါတယ်။ DHCP က BOOTP ပေါ် အခြေခံထားတာ ဖြစ်ပါတယ်။ BOOTP ဟာ ကနဦးတုန်းကတော့ Disk မရှိတဲ့ Workstation တွေ Boot လုပ်ပေးနိုင်ဖို့ ရည်ရွယ် Design ဆွဲခဲ့တာဖြစ်ပါတယ်။

YOUTH Computer Co.,Ltd,
Training & Multimedia Production
6-A၊ ပန်းဆိုးတန်း Office Tower ၊ ပန်းဆိုးတန်း (အလယ်)၊ ကျောက်တံတား၊ ဖုန်း– ၂၅၄၈၉၃

စစ်ကိုင်း – အပ်ချုပ်စုရပ်၊ စစ်ကိုင်းမြို့ ။ ဖုန်း – ၀၇၂-၂၁၂၄၉၊ ၀၇၂-၂၁၉၆၂
လားရှိုး – ရပ်ကွက် – ၁၂၊ လားရှိုးလုံလမ်း၊ နယ်မြေ (၇)၊ လားရှိုးမြို့

Advance Network Engineering

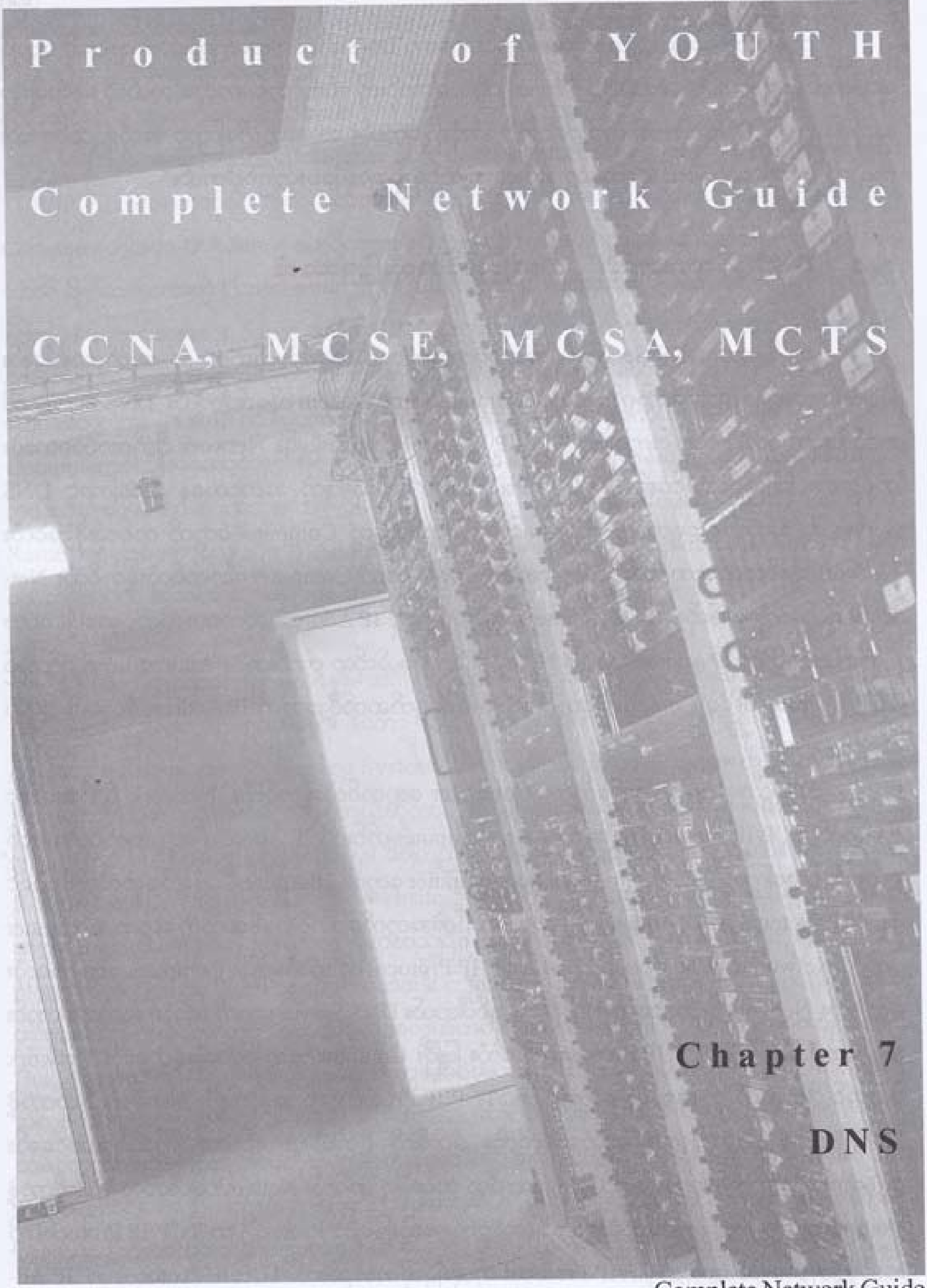
(IIS) Internet Information Service, (DNS) Domain Name Server, (NAT) Network Address Tranlation, (DHCP) Dynamic Host Configuration Protocol, (ISA) Internet Security And Acceleration Server 2006, Exchange Server 2003 စသည့်သင်ခန်းစာများကို အသေးစိတ်သင်ကြားပေးသည်။

MCSA သင်တန်းများ

70-620 (Windows Vista Configuration), 70-290 (Microsoft Windows Server 2003 Environment), 70-291 (Microsoft Windows Server 2003 Network Infrastructure), 70-284 (Exchange Server 2003), 70-351 (Internet Security and Acceleration Server 2006), 70-299 (Windows Server 2003 Network) စသည့် သင်ခန်းစာ များကို အသေးစိတ်သင်ကြားပေးသည်။ လက်တွေ့တကယ်တတ်အောင်သင်ကြားပေးခြင်းဖြစ်ပါသည်။ ပြီးမှ မေးခွန်းပုံစံပောင်းများနှင့် Pretest လုပ်ပါသည်။ မေးခွန်းများကို အလွတ်ကျက်သင်ပေးခြင်းမဟုတ်ပါ။

Dual Core 2.5, 1 GB, 160 GB, 17 "LCD, များဖြင့်လေ့ကျင့်ရမည်။ စာတွေ့လက်တွေ့ပိုင်ပြီး အခြေခံခိုင်စေရမည်။ လက်တွေ့လုပ်ငန်းခွင်ဝင်နိုင်စေရမည်။

Product of YOUTH



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 7

DNS

ကျွန်တော်အခုပြောချင်နေတဲ့အကြောင်းကတော့ DNS ဆိုတဲ Server ကြီးအကြောင်းကို ပြောပြချင်ပါတယ်။ ကျွန်တော်ကလေ DNS Server ကြီးအကြောင်းကို ရှင်းပြရုံတင်မကဘူး။ ဘယ်လို နေရာမျိုးမှာ အသုံးပြုရမယ်။ DNS Server ကိုဘာကြောင့် အသုံးပြုရတယ်။ ဘာအတွက်ကြောင့် အသုံးပြုသင့်တယ်။ ဘယ်လို Install လုပ်ရမယ်ဆိုတာတွေ အားလုံးအဆင့်ဆင့် ရှင်းပြပေးမှာဖြစ်ပါတယ်။

၇.၁ DNS ဆိုတာဘာလဲ၊ ဘာ့ကြောင့်အသုံးပြုရတာလဲ

ကဲ ဒီတော့ DNS Server ရဲ့ အရှည်ကောက် ဘယ်လိုခေါ်တယ်ဆိုတာကို စမှတ်ထားပါနော်။ DNS Server ရဲ့အရှည် ကောက်ကတော့ Domain Name System လို့ခေါ်ပါတယ်။ DNS Server ကို အသုံးပြုရတဲ့ အကြောင်းရင်းကတော့ TCP/IP Protocol ကိုအသုံးပြုပြီး Network ချိတ်တာကစတာပဲ။ ကဲစဉ်းစား ကြည့်ရအောင်နော်။ TCP/IP Protocol ကို အသုံးပြုတဲ့ အဆင့်ကနေ ဘာကြောင့် DNS Server ကို အသုံးပြုလာရတာလဲ လို့ပြောရင် ကျွန်တော်တို့တွေ Computer တွေကို တစ်လုံးနဲ့တစ်လုံး Network ချိတ်ဆက်တော့မယ်ဆိုတာနဲ့ ဘာစလုပ်မလဲ။ ဟဲဟဲ Computer တွေတစ်လုံးနဲ့တစ်လုံး Network ချိတ်တော့ မယ်ဆိုတော့ Computer တွေအားလုံးကို IP Address လိုက်ပေးလိုက်ရမှာပေ့ါ။ ဟော Computer တွေကို IP Address ပေးပြီး Network ချိတ်ရမယ်ဆိုက တည်းက IP Address ပေးလို့ရဖို့သည် TCP/IP Protocol ရှိမှ Computer တွေကို Network ချိတ်ဆက်ဖို့အတွက် IP Address တွေပေးလို့ရမှာ လေ။

အဲဒီတော့ ကျွန်တော်တို့တွေက Computer တွေတစ်လုံးနဲ့တစ်လုံး Network ချိတ်ဆက်နိုင် ဖို့အတွက် TCP/IP Protocol ကို အသုံးပြုပြီး Computer တိုင်းကို IP Address တွေ သတ်မှတ်ပေးကြ ရမှာပေ့ါ။ ဘာကြောင့် TCP/IP Protocol ရှိမှ Computer တွေကို IP Address ပေးလို့ရမှာလဲလို့ပြောရင် TCP/IP Protocol က IP Address နဲ့ပဲ အလုပ်လုပ်တဲ့အတွက်ကြောင့် ကျွန်တော်တို့တွေက Computer တွေကို Network ချိတ်တော့မယ်ဆိုတာနဲ့ TCP/IP Protocol ကို အသုံးပြုပြီး Computer တွေ တစ်လုံး နဲ့တစ်လုံး Network မိအောင်ချိတ်ဆက်နိုင်မှာ ဖြစ်ပါတယ်။ DNS Server တွေကို အသုံးပြုရတဲ့အကြောင်း အရင်းကလည်း အဲဒီ TCP/IP Protocol ကိုအသုံး ပြုပြီး Computer တွေ တစ်လုံးနဲ့တစ်လုံး Network မိအောင် ချိတ်ဆက် တဲ့နေရာက စတာပဲ။ ဟ...TCP/IP Protocol ကို အသုံးပြုပြီး Network ချိတ်တာနဲ့ DNS Server အသုံးပြုတာနဲ့ကဘာဆိုင်လို့လဲ။ ဒါကဒီလို ရှိတယ်ဗျ။ စဉ်းစား ကြည့်ရအောင်နော်။ ကျွန်တော်တို့တွေ တစ်ကမ္ဘာလုံးမှာ Computer တွေ တစ်လုံးနဲ့ တစ်လုံး Network ချိတ်တော့ မယ်ဆိုတာနဲ့ Computer တွေ Network ချိတ်ဆက် ဖို့ရန်အတွက် အသုံးပြုရတဲ့ Protocol က TCP/IP Protocol ကို အသုံးပြုတယ်လေ။ ဟော..TCP/IP Protocol ကိုသုံးပြီဆိုကတည်းက TCP/IP Protocol က IP Ad-

Product of YOUTH

dress နဲ့ အလုပ်လုပ်တယ်လေ။ TCP/IP Protocol က IP Address နဲ့အလုပ်လုပ်တယ် ဆိုတော့ ကျွန်တော်တို့ ကမ္ဘာမှာ Network ချိတ်ဆက်ထားတဲ့ Computer တွေရဲ့ အရေအတွက်ကို ကြည့်မယ်ဆိုရင် မရေမတွက်နိုင်အောင်ကို များပြားလွန်းလှတယ်လေ။

အဲဒီလို များပြားလှတဲ့ Computer တွေ တစ်လုံးနဲ့တစ်လုံး Network ချိတ်ဆက်ထားတာက TCP/IP Protocol ကိုသုံးပြီး ချိတ်ဆက်ထားတယ်။ TCP/IP Protocol ကို အသုံးပြုပြီဆိုကတည်းက Computer တိုင်းမှာ IP Address တွေရှိတာပေါ့။ ဒီလိုဆိုရင် ကျွန်တော်တို့ တစ်ကမ္ဘာလုံးမှာ မရေတွက်နိုင်အောင် ချိတ်ဆက်ထားတဲ့ Computer တွေရဲ့ IP Address တွေကို မှတ်ထားရမယ်ဆိုရင် ဘယ်သူမှ မှတ်ထားနိုင်ကြမှာ မဟုတ်ဘူးလေ။ ဒီတော့ အဲဒီလို IP Address တွေကို မမှတ်သားထားနိုင်တော့ အဲဒီ IP Address တွေကို မှတ်ထားစရာမလိုတော့ဘဲ နာမည်ကိုပဲ မှတ်ထားလို့ ရတဲ့စနစ်ကို ကျင့်သုံးကြတာပေါ့။ ဟော..တွေ့လား။ TCP/IP ကို အသုံးပြုပြီး Network တော့ ချိတ်ထားပါတယ်။ Network ချိတ်ဆက်တဲ့ Computer အလုံးအရေအတွက် တွေက မရေတွက်နိုင်အောင်များပြားလွန်းတော့ IP Address တွေကို ဘယ်သူမှ မှတ်မထားနိုင်ကြဘူး။ အဲဒီလို IP Address ကို မှတ်မထားနိုင်ပေမယ့် အဲဒီ IP Address ကို Name တစ်ခုဖြစ်အောင်လုပ်ပြီး၊ IP Address ကိုမမှတ်ဘဲ IP Address ကိုပေးထားတဲ့ Name ကိုပဲ မှတ်မယ်ဆိုရင်တော့ အဆင်ပြေသွားပြီပေါ့။ ဟုတ်တယ်မှတ်လား။

ကဲကဲ သေသေချာချာမှတ်နော်။ အဲဒီ IP Address တွေကို နာမည်သတ်မှတ်ပေးချင်တယ်ဆိုရင် DNS Server ကို အသုံးပြုရမယ်နော်။ ဒီတော့ DNS Server ကို အသုံးပြုရတာသည် IP Address တွေကို နာမည် ပေးဖို့ရန်အတွက် Naming System ပေါ့ဗျာ။ အဲဒီအတွက်အသုံးပြုရတာပဲ ဖြစ်တယ်။ DNS Server ကို ဘာကြောင့် Install လုပ်ရတယ်ဆိုတာကို Example အနေနဲ့ တစ်ခုပြောပြမယ်။ Internet ပေါ့ဗျာ။ ကျွန်တော်တို့ တွေ Internet ပေါ်မှာ မိမိကြည့်ချင်တဲ့ Website တစ်ခုကို ကြည့်မယ်ဆိုရင် Internet Explorer ထဲက Address Bar မှာ Website Name ကို ရိုက်ထည့်ပေးရမယ်လေ။ ကဲ ဒီတော့ www.google.com ဆိုတဲ့ နာမည်ကို ရိုက်ထည့်ပြီး၊ Enter Key ကိုနှိပ်လိုက်မယ်ဆိုရင် Internet Explorer ထဲမှာ Google Web Page ကျလာမှာပေါ့။ ကျွန်တော်ပြောချင်တာက အဲဒီ www.google.com ဆိုတဲ့ နာမည်ကို ကျွန်တော်တို့က မှတ်မိနေလို့ အလွယ်တကူ Google WebSite ကို ကြည့်လို့ရတာဖြစ်တယ်။ But...ဒါပေမယ့် www.google.com ဆိုတဲ့ နာမည်ရဲ့နောက်ကွယ်မှာ အလုပ်လုပ်တာက IP Address က အလုပ်လုပ်သွားတာ ဖြစ်တယ်။ အဲဒီလို IP Address အလုပ်လုပ်တာသည် www.google.com Website တစ်ခုတည်း အလုပ်လုပ်တာမဟုတ်ဘူး။ ကျွန်တော်တို့ Internet ပေါ်မှာ ကြည့်နေတဲ့ Website တိုင်း၊ Website တိုင်း၊ ရဲ့နောက်ကွယ်မှာ အလုပ်လုပ်တာသည် IP Address ကပဲ အလုပ်လုပ်သွားတာ ဖြစ်တယ်။ သဘောပေါက်လားတော့ မသိဘူး။ ကျွန်တော် ဆိုလိုချင်တာ ကလေ၊ အဲ့ဒီ Website Name ကိုခေါ်လို့ရဖို့

အတွက် နောက်ကွယ်ကနေ အလုပ်လုပ်သွားတဲ့ IP Address ကို နာမည်ပေးထားတဲ့ Website Name ပဲဖြစ်တယ်။ အဲ့ဒီလိုမျိုး IP Address ကို နာမည်ပေးလို့ရဖို့ကလည်း DNS Server ရှိမှနာမည်ပေးလို့ရမှာ ဖြစ်ပါတယ်။ ဒါကြောင့် ကျွန်တော်တို့တွေဟာ IP Address ကို နာမည်ပေး ဖို့ရန်အတွက် DNS Server ကိုထိုင်ပြီး၊ IP Address တွေကို နာမည်ပေးတဲ့စနစ်ကို ကျင့်သုံးကြတာပဲ ဖြစ်ပါတယ်။

ကဲ ဒီလောက်ဆိုရင် DNS Server ကို ဘာကြောင့်အသုံးပြုရတယ်ဆိုတာ သဘောပေါက်နားလည် မယ်လို့ ထင်ပါတယ်။ ထပ်ပြီး မှတ်ထားလိုက်ပါဦးနော်။ DNS Server ဆိုတာ IP Address တွေကို နာမည် ပေးထားတဲ့ Server ဖြစ်တယ်။ Network အသင့်ချိတ်ဆက်ထားတဲ့ Computer အလုံးအရေအတွက် တွေ များလာလို့ IP Address ကိုမှတ်ရတာ အဆင်မပြေဘူးဆိုရင် DNS Server ထိုင်ပေးရမယ်ဆိုတာ မမေ့နဲ့နော်။ ကျွန်တော်ခုနက Example အနေနဲ့ ရှင်းပြခဲ့တဲ့ www.google.com ဆိုတဲ့ Domain Name ရဲ့နောက် ကွယ်မှာ အလုပ်လုပ်နေတဲ့ IP Address ကိုကြည့်မယ်ဆိုရင်တော့ အောက်ပါပုံထဲက Command ကိုအသုံး ပြုပြီး ကြည့်လို့ရပါတယ်။

ပုံ ၇.၁

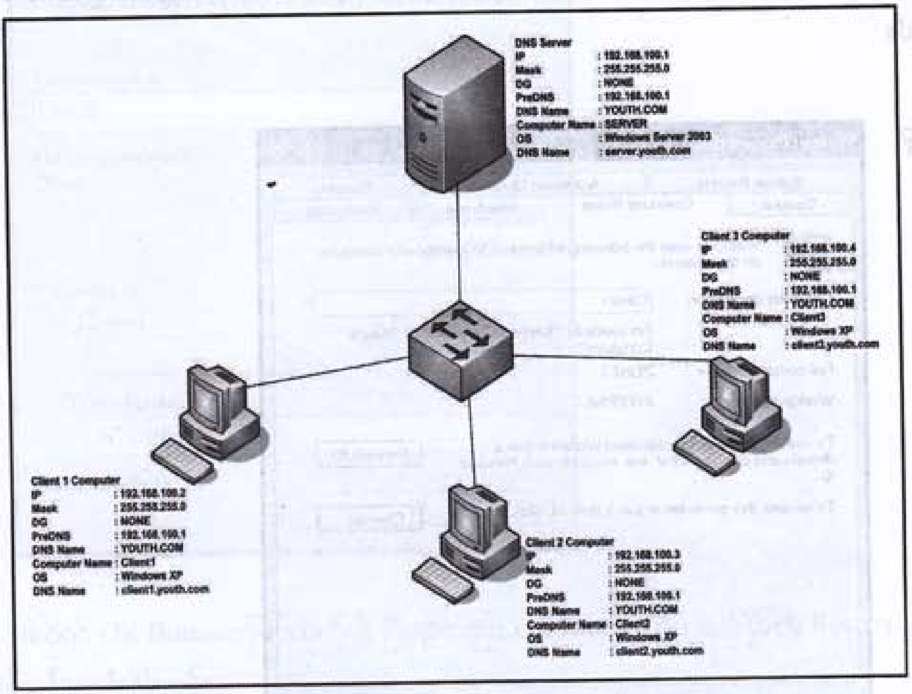
မှတ်ချက်။ ။မိမိကြည့်ချင်တဲ့ Website ရဲ့ IP ကိုသိချင်ရင်လည်း ၎င်း Command ကိုပဲ အသုံးပြုပြီး ကြည့်လို့ရပါတယ်။

၇.၂ DNS Server ကို ဘယ်လို Install လုပ်မလဲ

ကဲအခုဆိုရင် ကျွန်တော် DNS Server ရဲ့အကြောင်းကို ရှင်းပြပြီးပြီဆိုတော့ ကျွန်တော်အောက်မှာ ဆွဲပြထားတဲ့ Diagram ထဲကအတိုင်း DNS Server ကိုထိုင်ပြီး၊ Client တွေရဲ့ IP Address တွေကို

Naming System နဲ့အသုံးပြုလို့ရအောင် Step by Step Configuration ကိုလိုက်လုပ်ကြည့်ရအောင်။

ပုံ ၇.၂



အခု ကျွန်တော်ဆွဲပြထားတဲ့ Diagram အတိုင်း ကျွန်တော် DNS Server Installation လုပ်ပုံ အဆင့်ဆင့်ကို ဖော်ပြပေးသွားမှာ ဖြစ်ပါတယ်။

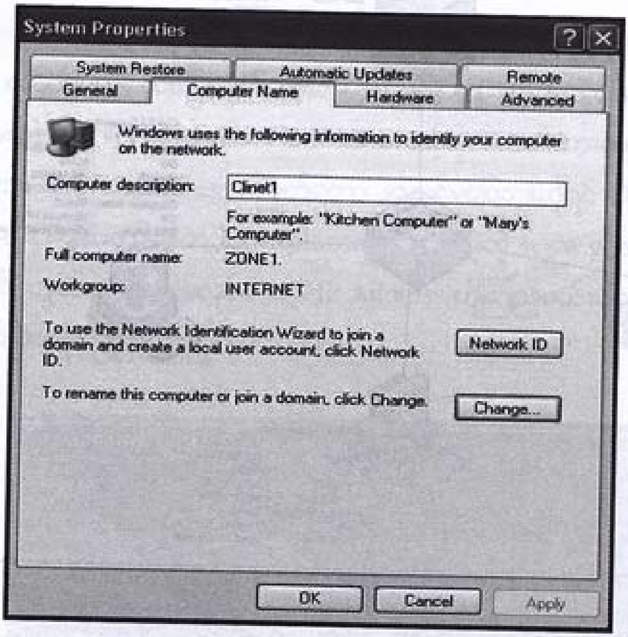
❖ Step Number 1

ပုံမှာပြထားတဲ့အတိုင်းပဲ Client Computer တွေရဲ့ Name ကို Client 1, Client 2, Client 3 ဆိုပြီးပေးပါ။ ပြီးရင်၄င်းတို့ကို IP Address ကိုထည့်ပေးပါ။ ကျွန်တော် Example အနေနဲ့ Client 1 Computer တစ်လုံးကိုပဲ ဘယ်လို Setting ချရမယ်ဆိုတာပဲ ပြပေးပါမယ်။ ကျန် Client Computer များဖြစ်တဲ့ Client 2 နဲ့ Client 3 ကိုလည်း Client 1 အဆင့်အတိုင်း Diagram ထဲမှာပါတဲ့ Computer Name တွေ၊ IP Setting တွေကို သတ်မှတ်ပေးရပါမယ်။

Client 1 Computer Name ပေးပုံ....

❖ My Computer (Right Click) >> Properties >> Click Computer Name Tab ထဲသို့ သွားပါ။

ပုံ ၇.၃



၁။ အဲဒီအခါ Computer Name Tab ထဲကိုရောက်မယ်။ ပြီးရင် Change Button ကိုထပ်နှိပ်လိုက်ပါ။ Computer Name ကိုပြောင်းမယ့် Box ပေါ်လာပါလိမ့်မယ်။ Computer Name နေရာမှာ Client 1 လို့ နာမည် ပေးပါ။

၂။ အောက်မှာ ပြထားတဲ့ ပုံ (၇.၄) ထဲကအတိုင်း Client 1 လို့ Computer Name ပေးပြီးပြီဆိုရင်တော့ OK Button လေးကို နှိပ်လိုက်ပါ။ မိမိရဲ့ Computer ကို Restart ချခိုင်းရန် Box လေးတစ်ခု ပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၄

❖ ဒါဆိုရင် OK Button ကိုနှိပ်လိုက်ပါ။ ပြီးရင်လည်း OK Button ကိုပဲ ထပ်နှိပ်ပါ။ Restart ချ မယ့် Box ထပ်ပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၅

ပုံ ၇.၆

❖ Yes Button ကို Click လုပ်ပါ။ Computer ကို Restart ချသွားပါလိမ့်မယ်။ Restart ချပြီး ပြန်တက်လာရင်တော့ မိမိပြောင်းလဲခဲ့တဲ့ Computer Name ပေါ်နေတာကို အောက်ပါအတိုင်းတွေ့ရပါလိမ့်မယ်။

ပုံ ၇.၇

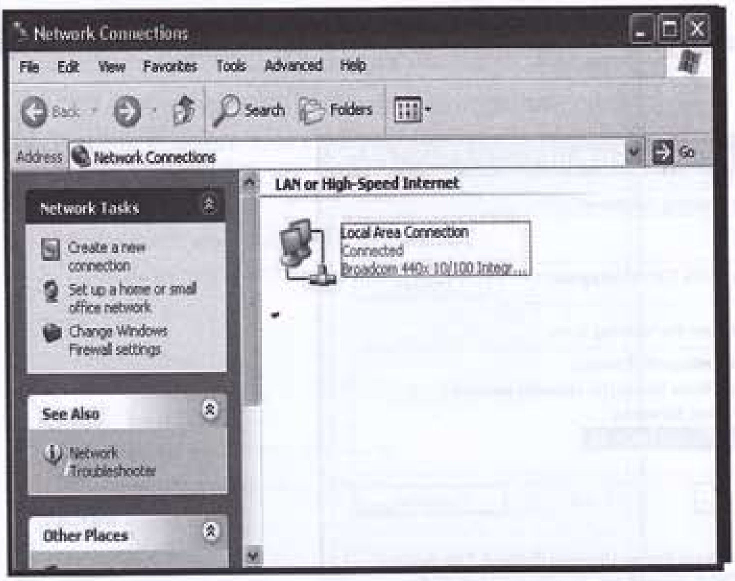
မှတ်ချက်။ ။ Client 1 Computer Name ပြောင်းလဲပုံကို သိပြီဆိုရင် ၎င်းအစဉ်အတိုင်းပဲ Client 2, Client 3 Computer Name တို့ကိုလည်း ပြောင်းလဲပေးပါ။

Client 1 Computer ကို IP Address ပေးပုံ.....

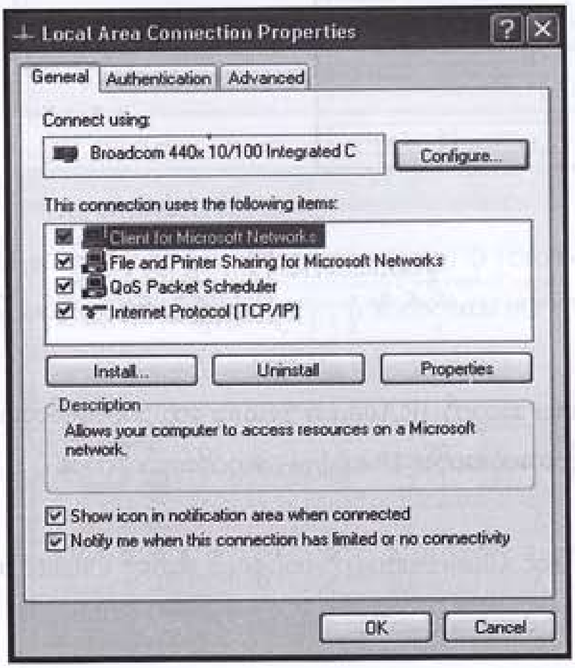
၁။ Desktop ပေါ်မှာရှိတဲ့ My Network Place Icon လေးပေါ်မှာ Right Click နှိပ်ပြီး Properties ကို ထပ်နှိပ်ပါ။ အဲဆိုရင် တစ်ဘက်မှာပြထားတဲ့ ပုံ(၇.၈) ပုံစံအတိုင်းပေါ်လာတာကို တွေ့ပါမယ်။

၂။ ၎င်း Local Area Connection ကို Right Click နှိပ်ပြီး Properties ထပ်နှိပ်ပါ။ အောက်ပါ ပုံ (၇.၉) အတိုင်း Local Area Connection Properties Box ပေါ်လာတာကို တွေ့ရပါလိမ့်မယ်။

ပုံ ၇.၈



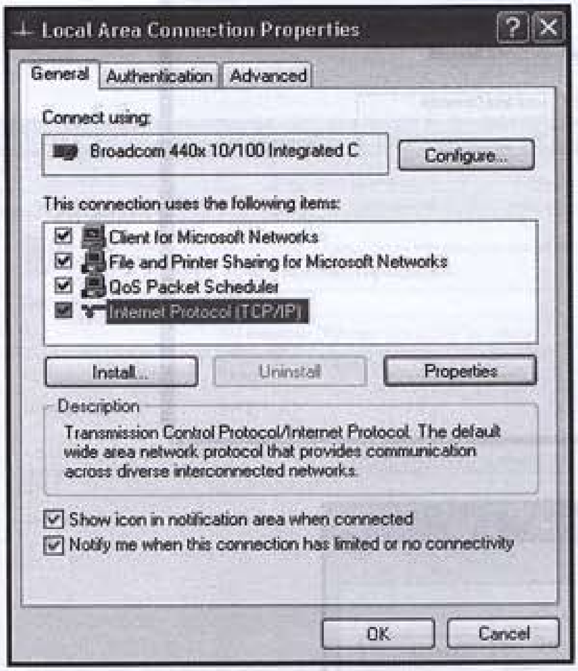
ပုံ ၇.၉



၃။ ၄င်း Local Area Connection Properties Box ရဲ့ General Tab ထဲက This Connection uses the following items:section ထဲကမှ–

❖ Internet Protocol (TCP/IP) ကို Select မှတ်ပြီး Properties Button ကိုနှိပ်လိုက်ပါ။

ပုံ ၇.၁၀

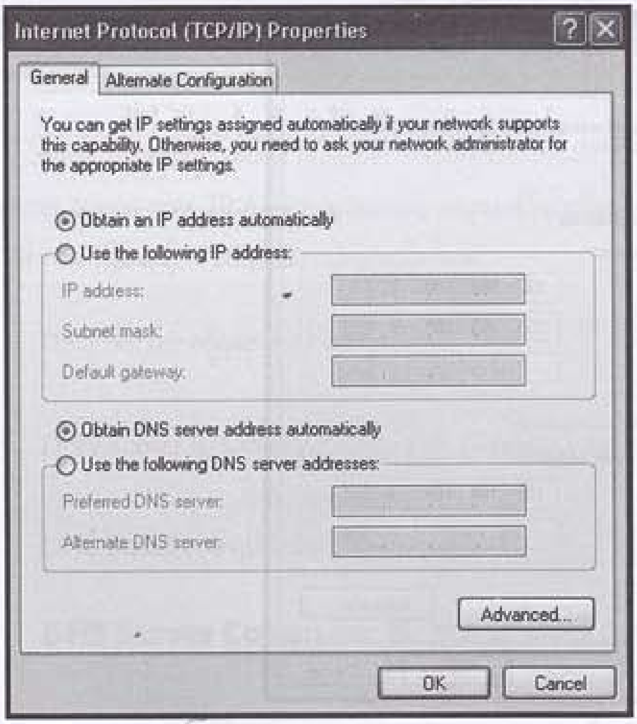


❖ အဲဒါဆိုရင် တစ်ဘက်မှာဖော်ပြထားတဲ့ ပုံ (၇.၁၁) ထဲကအတိုင်း ပေါ်လာပါလိမ့်မယ်။ Use the following IP Address: Check Box ကို On ပေးလိုက်ပါ။ ပုံ (၇.၁၂) အတိုင်းပေါ်လာပါလိမ့်မယ်။

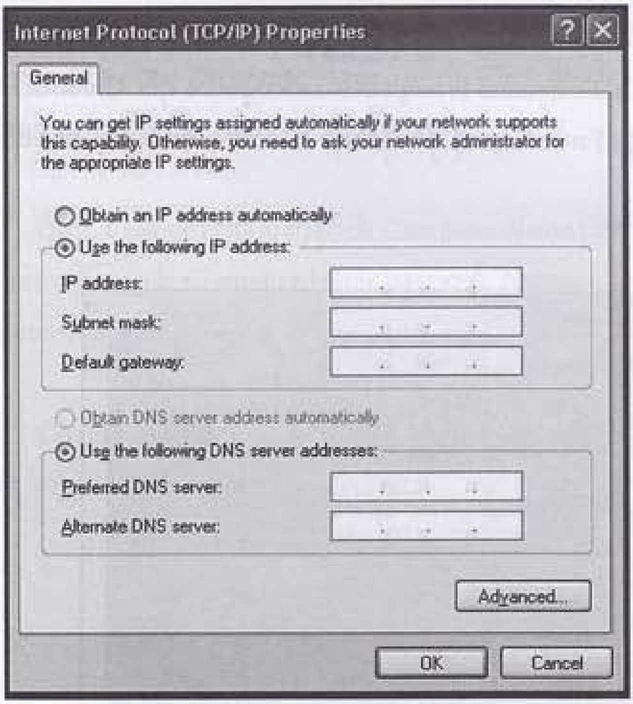
❖ ဒါဆိုရင် မိမိ Client 1 Computer အတွက် IP Address Setting တွေ သတ်မှတ်လို့ရပါပြီ။ ပုံ (၇.၁၃) မှာပြထားတဲ့ Diagram ထဲမှာ ပြထားတဲ့အတိုင်း IP Address တွေကိုထည့်လိုက်ပါ။

❖ ပြီးရင် OK Button ကိုနှိပ်ပါ။ ပြီးရင် Close Button ကို ထပ်နှိပ်ပါ။ ဒါဆိုရင် Client 1 အတွက် IP Setting ထည့်တာပြီးသွားပါပြီ။

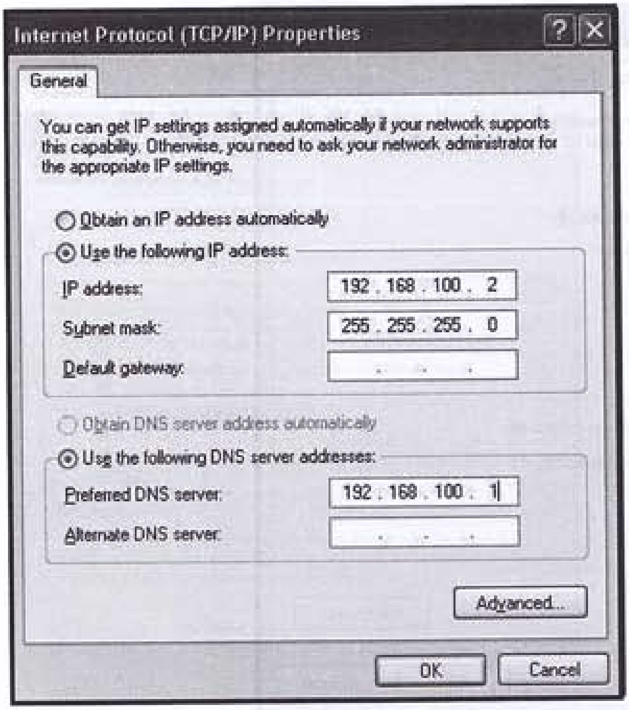
ပုံ ၅-၁၁


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

ပုံ ၅-၁၂

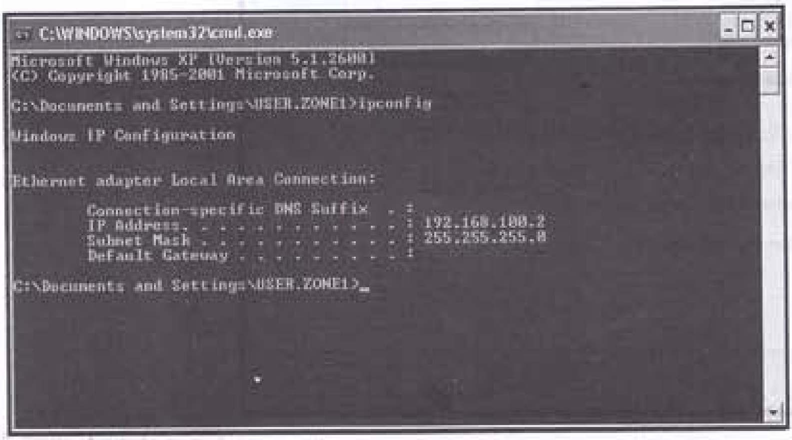

Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

ပုံ ၇.၁၃



၄။ တကယ်လို့ မိမိရဲ့ IP Address Setting တွေကို ကြည့်ချင်ရင် Start >> Run Box ထဲတွင် cmd ကိုရိုက်ပြီး OK ကို Click လုပ်ပါ။ Command Prompt ပေါ်လာပါလိမ့်မယ်။ ၎င်း Command Prompt Box ထဲတွင် ipconfig လို့ရိုက်ပြီး၊ Enter Key ကို နှိပ်လိုက်ရင် မိမိသတ်မှတ်ပေးခဲ့တဲ့ IP Address တွေကိုဖော်ပြပေးပါလိမ့်မယ်။

ပုံ ၇.၁၄



မှတ်ချက်။ ။ Client 2, Client 3 တို့ကိုလည်း အထက်ပါအတိုင်း IP Address Setting တွေကို သတ်မှတ်ပေးပါ။

၅။ ကဲကဲ... ဘယ်လိုလဲခင်ဗျ။ Diagram ထဲမှာပြထားတဲ့အတိုင်း Client Computer တွေအားလုံးကို Computer Name တွေ၊ IP Address Setting တွေပေးပြီးပြီလို့ထင်ပါတယ်။ အဲလိုပေးပြီးပြီဆိုရင်တော့ DNS Server ထိုင်မယ့် Computer ကိုသွားလိုက်ပါ။

၆။ DNS Server ကိုရောက်ရင်တော့ -

- DNS Server ရဲ့ Computer Name ကို Server လို့ပြောင်းပါ။ DNS Suffix ကိုထည့်ပါ။
- DNS Install လုပ်ရပါမယ်။

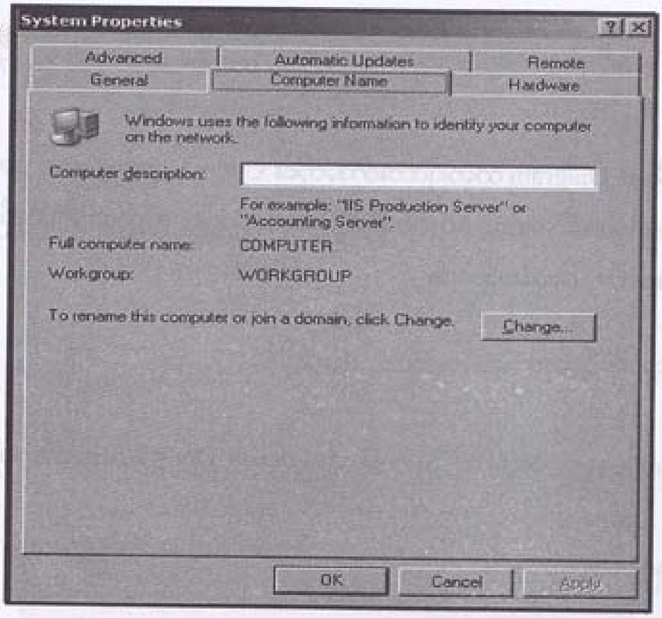
၇. ၃ DNS Server Computer Name နှင့် DNS Suffix Name တို့သတ်မှတ်ပေးပုံ

၁။ DNS Server ထိုင်မယ့် Computer ရဲ့ Desktop ပေါ်က My Computer ကို Right Click နှိပ်ပါ။ ပြီးရင် Properties ကိုထပ်နှိပ်ပါ။ System Properties Box ပေါ်လာပါလိမ့်မယ်။ အဲဒီ System Properties Box ထဲက Computer Name Tab ကို Click နှိပ်လိုက်ပါ။ တစ်ဘက်မှာပြထားတဲ့ ပုံ ၇.၁၅ အတိုင်းတွေ့ရပါလိမ့်မယ်။

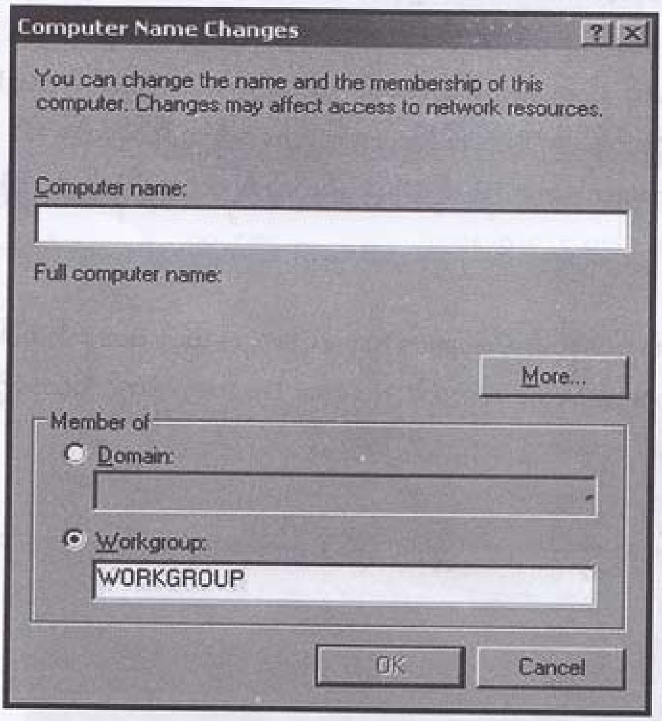
၂။ ပြီးရင် Change Button ကိုနှိပ်ပါ။ Computer Name Changes ဆိုတဲ့ Box ပေါ်လာပါလိမ့်မယ်။ ပုံ (၇.၁၆) ကိုကြည့်ပါ။ Computer Name နေရာတွင် Network Diagram ထဲတွင် ပြထားတဲ့ Server Computer Name ကိုရိုက်ထည့် မှာဖြစ်လို့ Server ကိုရိုက်ထည့်ပါ။

၃။ Computer Name နေရာမှာ Server လို့ရိုက်ထည့်ပြီးရင် More Button ကို Click ထပ်နှိပ်ပါ။ ပုံ ၇.၁၇ မှာပြထားပါတယ်။

ပုံ ၇.၁၅


System Properties
Advanced
Automatic Updates
Remote
General
Computer Name
Hardware
Windows uses the following information to identify your computer on the network.
Computer description:
For example: "IIS Production Server" or "Accounting Server".
Full computer name:
COMPUTER
Workgroup:
WORKGROUP
To rename this computer or join a domain, click Change.
Change...
OK
Cancel
Apply

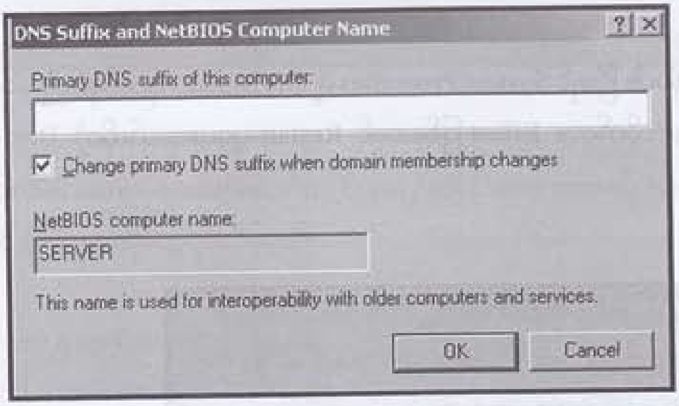
ပုံ ၇.၁၆


Computer Name Changes
You can change the name and the membership of this computer. Changes may affect access to network resources.
Computer name:
Full computer name:
More...
Member of
Domain:
Workgroup:
WORKGROUP
OK
Cancel

ပုံ ၇.၁၇

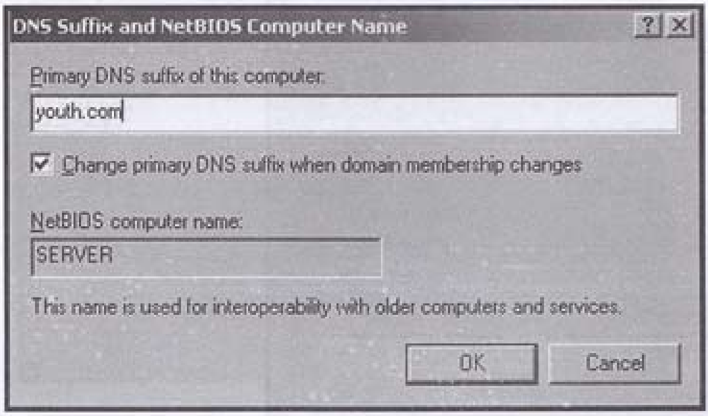
၄။ အောက်မှာပြထားတဲ့ ပုံထဲက Primary DNS Suffix of this Computer နေရာတွင် youth.com ကိုထည့်ပေးပါ။ ၎င်း youth.com သည် DNS Name ဖြစ်ပါတယ်။ သေသေချာချာ မှတ်ထားနော်။ အဲဒီနေရာမှာ ထည့်ခဲ့တဲ့ DNS Suffix သည် DNS ရဲ့ Name ဖြစ်တယ်။

ပုံ ၇.၁၈



၅။ ပြီးရင် OK Button ကိုနှိပ်ပါ။ Full Computer Name တွင် server.youth.com ကို ပေါ်နေပါလိမ့်မယ်။ OK Button ကိုနှိပ်ပါ။ Computer Name Change အား Effect ဖြစ်အောင် Restart ချမယ်ဆိုတဲ့ Box ပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၁၉



ပုံ ၇.၂၀

၆။ OK Button ကိုပဲနှိပ်ပါ။ ပြီးရင် System Properties ရဲ့ OK Button ကိုထပ်နှိပ်ပါ။ မိမိရဲ့ Computer System ကို Change လိုက်တာ Effect ဖြစ်အောင် Restart ချပေးရမယ်ဆိုတဲ့ Box ကျလာပါလိမ့်မယ်။

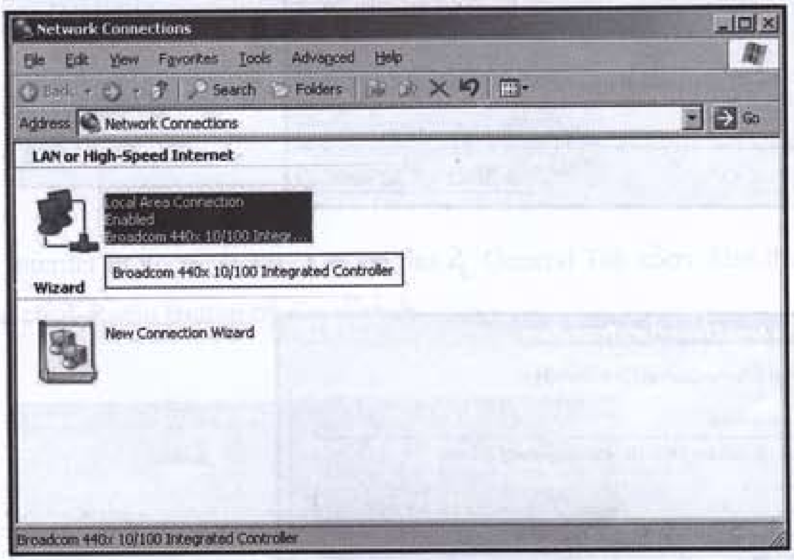
ပုံ ၇.၂၀

၇။ Yes Button ကိုပဲ နှိပ်လိုက်ပါ။ ဒါဆိုရင် Computer ကို Restart ချသွားပါလိမ့်မယ်။ မိမိရဲ့ Computer Restart ကျပြီး ပြန်တတ်လာပြီဆိုရင်တော့ Computer Name Change လိုက်တာ Effect ဖြစ်သွားပါပြီ။

၇.၄ DNS Server တို့ IP Address သတ်မှတ်ပေးပုံ

၁။ DNS Server ရဲ့ IP Address ကိုသတ်မှတ်မယ်ဆိုရင် My Network Place ကို Right Click နှိပ် >> Properties ထဲကိုဝင် >> ဒါဆိုရင် Network Connection Box ပေါ်လာမယ်။

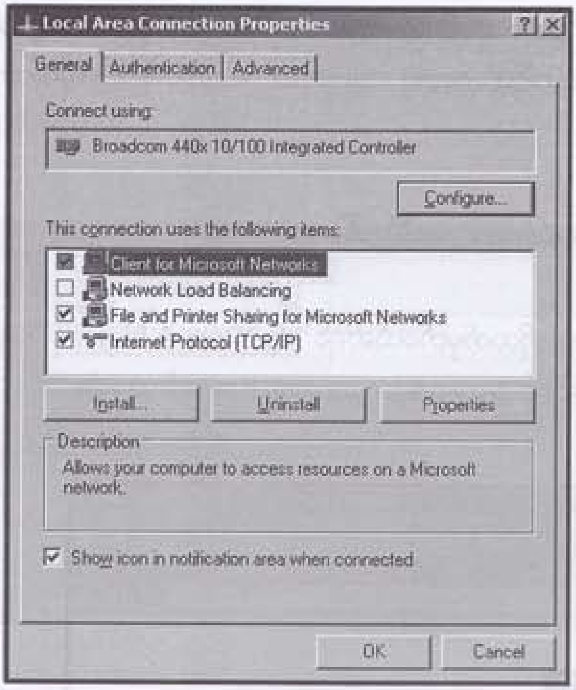
ပုံ ၇.၂၂



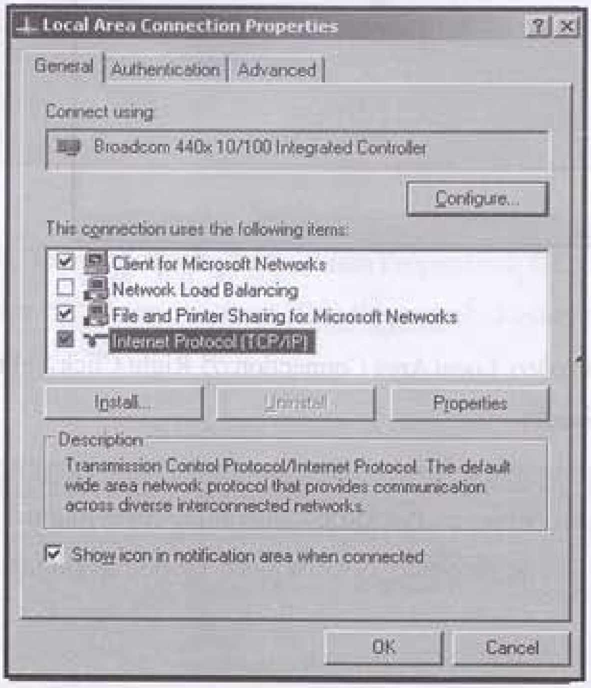
၂။ ၎င်း Network Connection ထဲက Local Area Connection ကို Right Click >>Properties ထဲကို ဝင်ပါ။ ပုံ ၇.၂၃ ကိုတွေ့ရပါလိမ့်မယ်။

၃။ Local Area Connection Properties ထဲကိုဝင်ပြီးရင် General Tab ထဲက Internet Protocol (TCP/IP) ကို Select မှတ်လိုက်ပါ။ ပုံ ၇.၂၄ အတိုင်းတွေ့ရပါမယ်။ ပြီးရင် Properties Button ကို နှိပ်ပါ။ ပုံ ၇.၂၅ ကိုကြည့်ပါ။

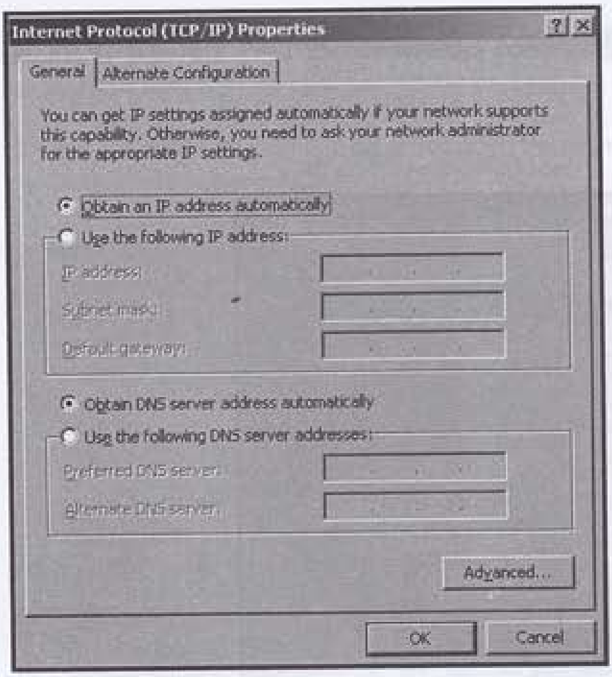
ပုံ ၇.၂၃


Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
Network Load Balancing
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Allows your computer to access resources on a Microsoft network.
Show icon in notification area when connected
OK
Cancel

ပုံ ၇.၂၄

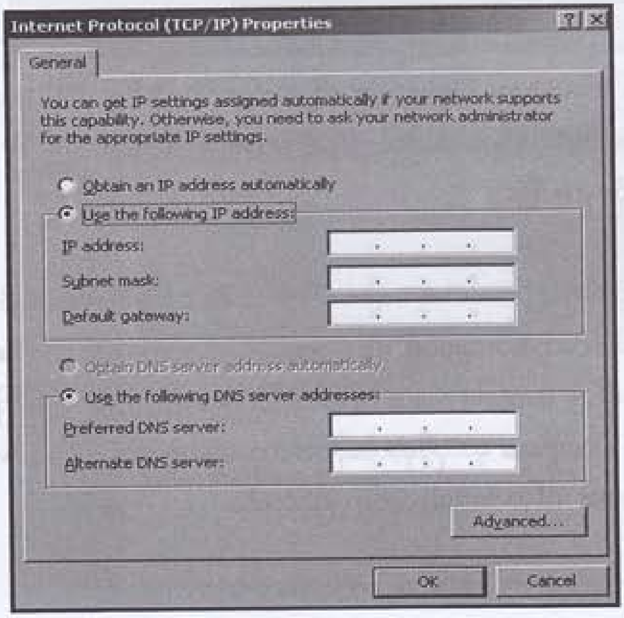

Local Area Connection Properties
General
Authentication
Advanced
Connect using:
Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
Client for Microsoft Networks
Network Load Balancing
File and Printer Sharing for Microsoft Networks
Internet Protocol (TCP/IP)
Install...
Uninstall
Properties
Description
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK
Cancel

ပုံ ၇.၂၅



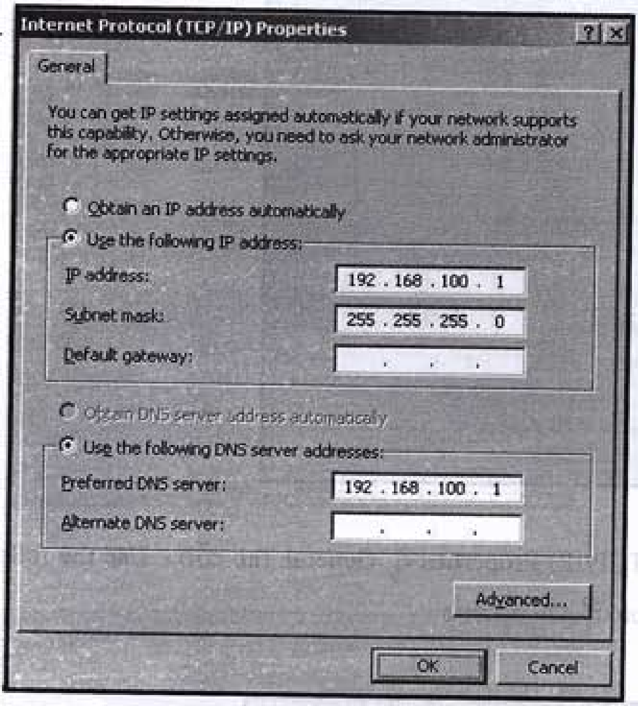
၄။ Internet Protocol(TCP/IP) Properties ရဲ့ General Tab ထဲက Use the following IP Address: ဆိုတဲ့ Radio Button ကို On လိုက်ပါ။

ပုံ ၇.၂၆



၅။ ပြီးရင် Network Diagram ထဲမှာ ပြထားတဲ့အတိုင်း DNS Server ရဲ့ IP Address တွေကို သတ်မှတ်ပေးပါ။

ပုံ ၇.၂၇



၆။ DNS Server အတွက် IP Address Setting တွေကို သတ်မှတ်ပြီးပြီဆိုရင် OK Button ကေ... ကိုနှိပ်ပါ။ ပြီးရင် Close Button ကိုထပ်နှိပ်ပါ။ ဒါဆိုရင် DNS Server Computer ကို IP Addr... Setting သတ်မှတ်ထားပြီး ပြီးဆုံးသွားပါပြီ။

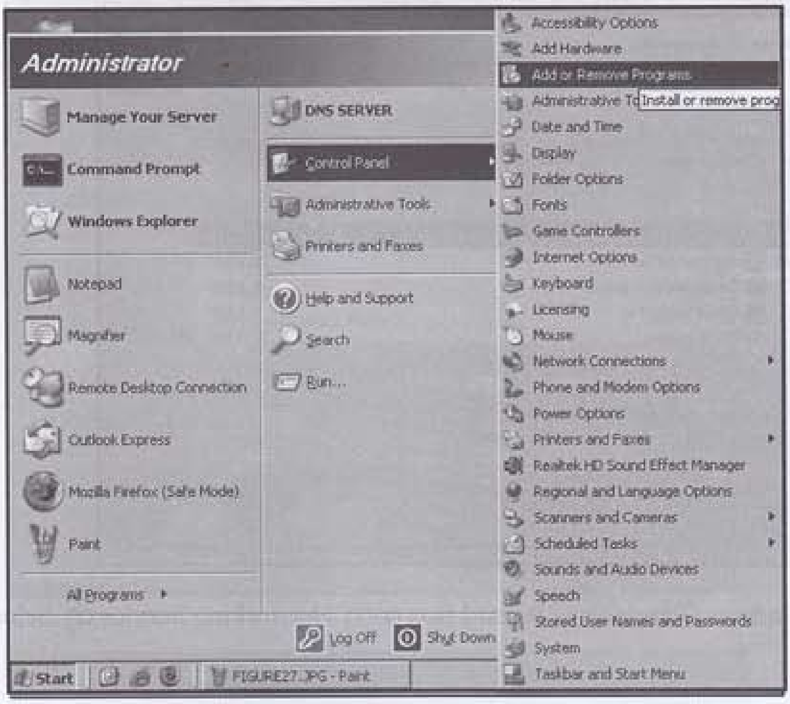
OK...အထက်မှာ ပြခဲ့တဲ့အတိုင်း Client 1, Client 2, Client 3 နှင့် DNS Server အသီးသီး... IP Address တွေ၊ Computer Name တွေအားလုံးပေးပြီးပြီ။ Computer တွေဟာလည်း တစ်လုံးနဲ့တစ်... Network မိနေပြီဆိုရင်၊ DNS ဆိုတဲ့ Domain Name System Service ကို Install လုပ်ကြရအောင်... DNS ကို Install လုပ်မှာ ဘယ် Computer မှာလုပ်မှာလဲဆိုပြီးတော့ မမေးနဲ့နော်။ Windows Server 2003 တင်ထားတဲ့ DNS Computer ပေါ်မှာ Install လုပ်မှာ ဖြစ်တယ်။

ကဲ....စလိုက်ကြရအောင်–

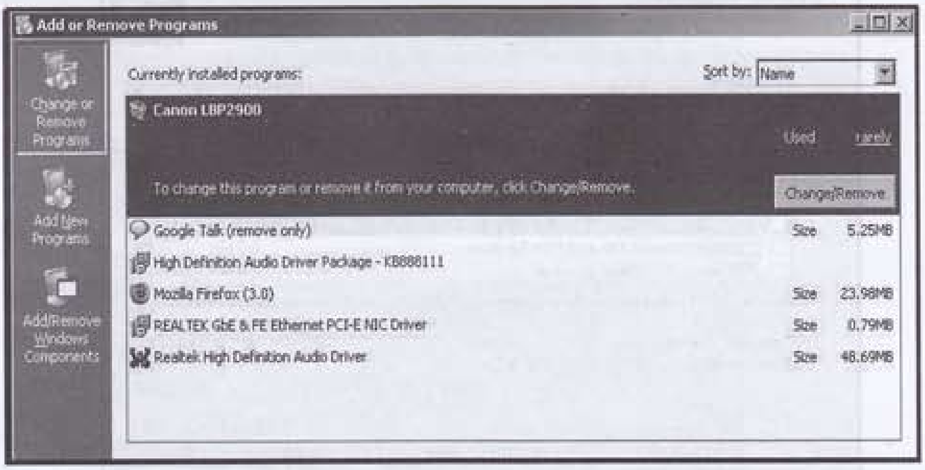
၇.၅ DNS (Domain Name System) ကို Install လုပ်ပုံ

၁။ Start >> Control Panel >> Add or Remove Programs ထဲသို့သွားပါ။

ပုံ ၇.၂၈

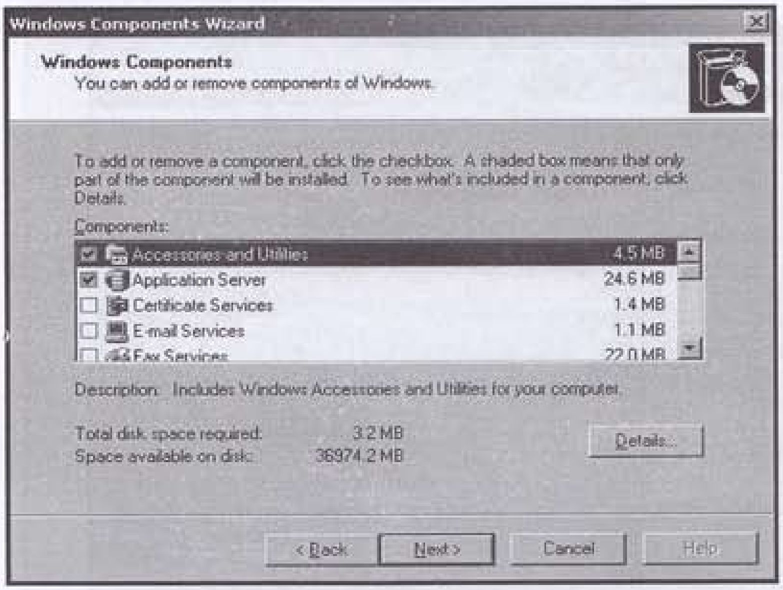


ပုံ ၇.၂၉



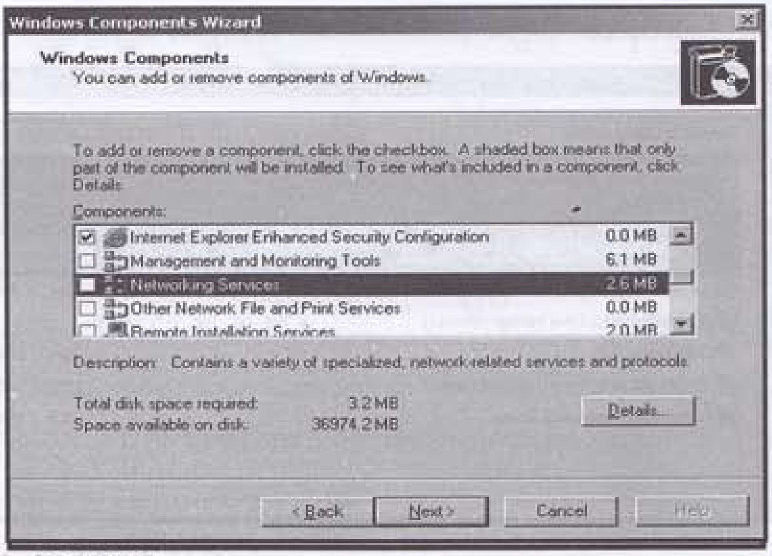
၂။ ပြီးရင် Add/Remove Program ထဲက Add/Remove Windows Component လေးကိုနှိပ်လိုက်ပါ။ Windows Setup မှာ Please Wait ကိုခဏပြပြီးရင်၊ Windows Component Wizard Box လေးပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၃၀



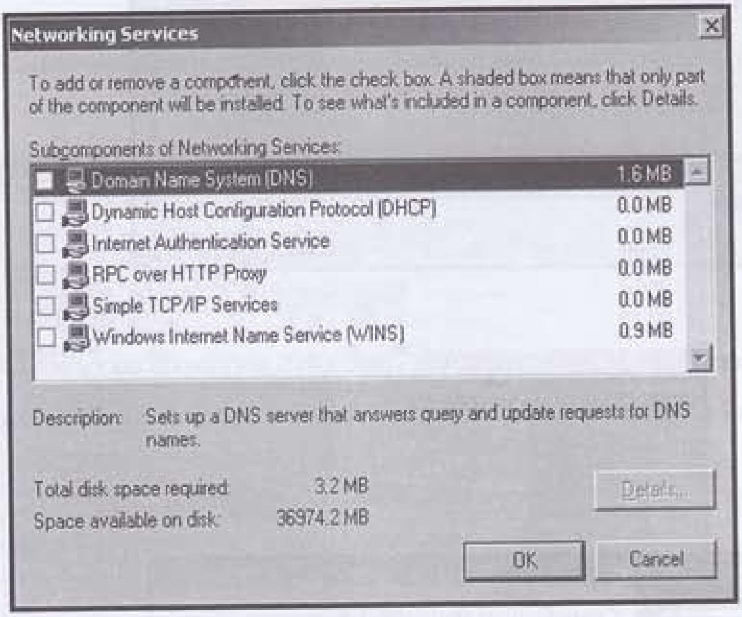
၃။ ၄င်း Windows Components Wizard Box ထဲက Networking Service ကို Select မှတ်။

ပုံ ၇.၃၁

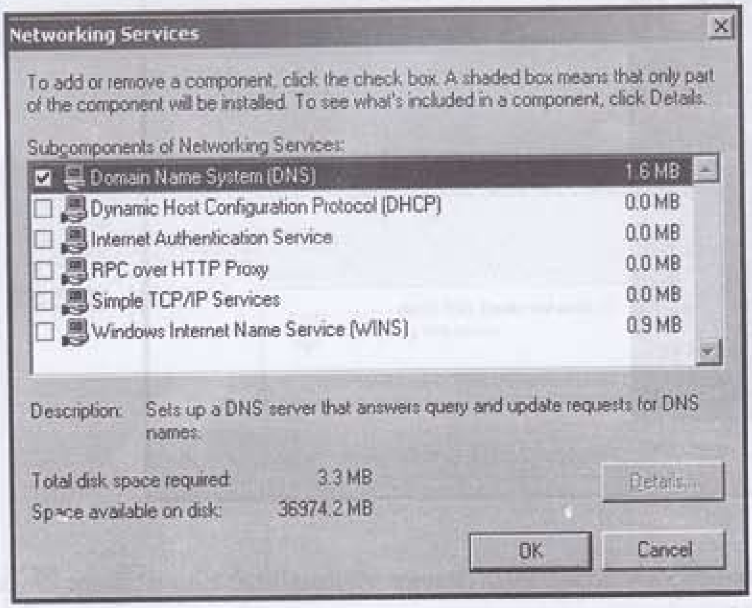


၄။ ပြီးရင် Detail Button ကိုနှိပ်ပါ။ Network Service Box ပေါ်လာမယ်။ ၄င်း Network Service Box ထဲက Domain Name System (DNS) ဆိုတာ ပေါ်လာမယ်။ ၄င်းရဲ့ဘေးက Check Box ကို On ပေးပါ။ ပုံ ၇.၃၂ နှင့် ၇.၃၃ အတိုင်းဖြစ်သွားမယ်။

ပုံ ၇.၃၂

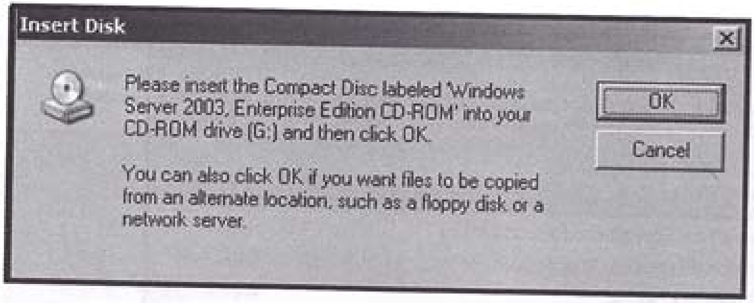


ပုံ ၇.၃၃



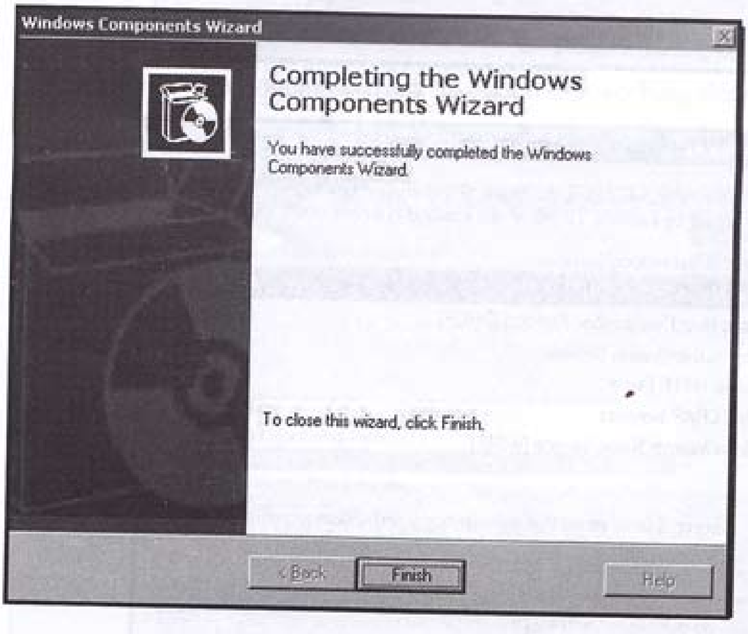
၅။ ပြီးရင် OK Button ကိုနှိပ်ပါ။ နောက်ပြီး Next Button ကိုထပ်နှိပ်ပါ။ DNS Service တွေကို Install လုပ်ပါလိမ့်မယ်။ ၄င်း Install လုပ်တဲ့အဆင့်တွင် မိမိတင်ထားခဲ့တဲ့ Windows Server 2003 CD ကိုပြန်တောင်းပါလိမ့်မယ်။

ပုံ ၁.၃၄



၆။ Windows Server 2003 CD ကိုထည့်ပေးပါ။ ပြီးရင် DNS Service ကို ဆက်လက်ပြီး Install လုပ်ပါလိမ့်မယ်။ Install လုပ်ပြီးတာနဲ့ Completing the Windows Components Wizard ပေါ်လာပါလိမ့်မယ်။

ပုံ ၁.၃၅



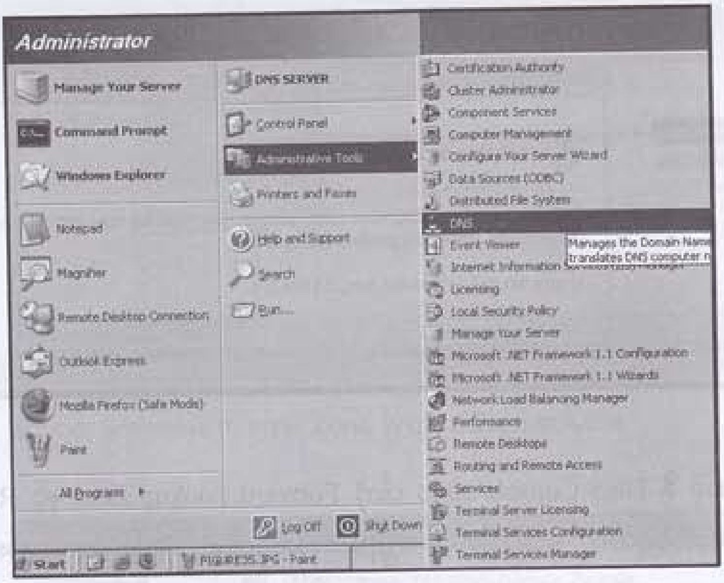
၇။ Finish Button ကိုနှိပ်ပါ။ အဲဒီဆိုရင် DNS Service ကို Install လုပ်တဲ့အဆင့်ပြီးသွားပြီဖြစ်ပါတယ်။

တဲ...DNS Server ကို Install လုပ်ပြီးသွားပြီဆိုရင်ဖြင့် DNS Server ကို ဘယ်လိုမျိုး Setting တွေချရမယ်၊ ဘယ်လိုမျိုး Configuration လုပ်တယ်ဆိုတာတွေကို ထပ်ဖတ်ကြည့်လိုက်ကြပါဦး။

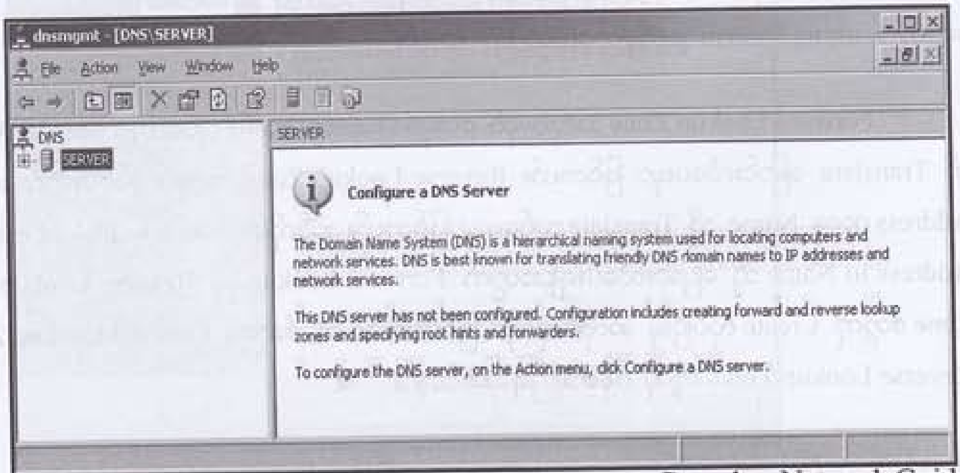
၇.၆ DNS Server ကို Configure လုပ်ပုံနှင့် Setting သတ်မှတ်ပုံ

၁။ Start >> Administrative Tools >> DNS Console ကိုဖွင့်လိုက်ပါ။

ပုံ ၇.၃၆

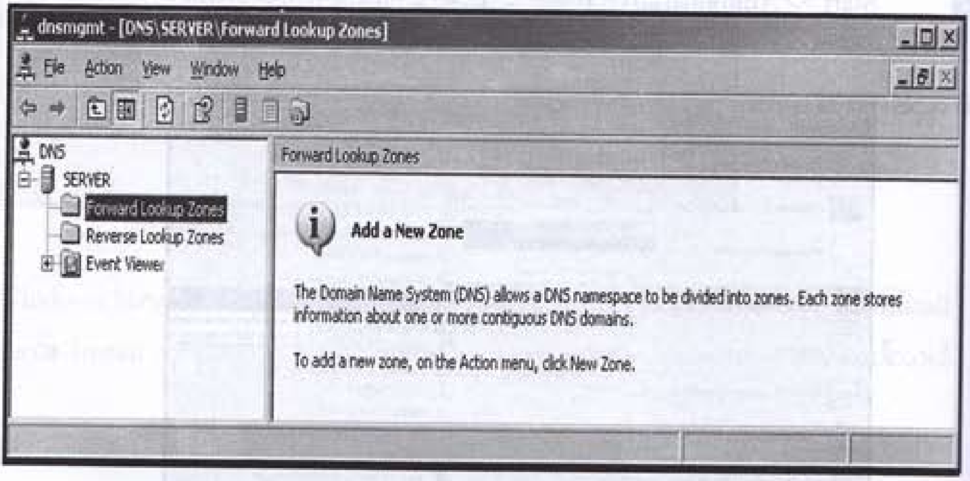


ပုံ ၇.၃၇



၂။ ကဲ ဒါဆိုရင် အထက်ပါပုံ ၇.၃၇ အတိုင်း DNS Server Console ပေါ်လာပါလိမ့်မယ်။ ၎င်း DNS Server Console ထဲက Server လို့ပေါ်နေတာသည် ကျွန်တော်တို့တွေ သတ်မှတ်ထားခဲ့တဲ့ Computer ရဲ့ Name ဖြစ်ပါတယ်။ ၎င်း Server Node ကို ဖြန့်ချလိုက်ရင် Forward Lookup Zone , Reverse Lookup Zone နဲ့ Event Viewer တို့ကို တွေ့ရမှာ ဖြစ်ပါတယ်။

ပုံ ၇.၃၈



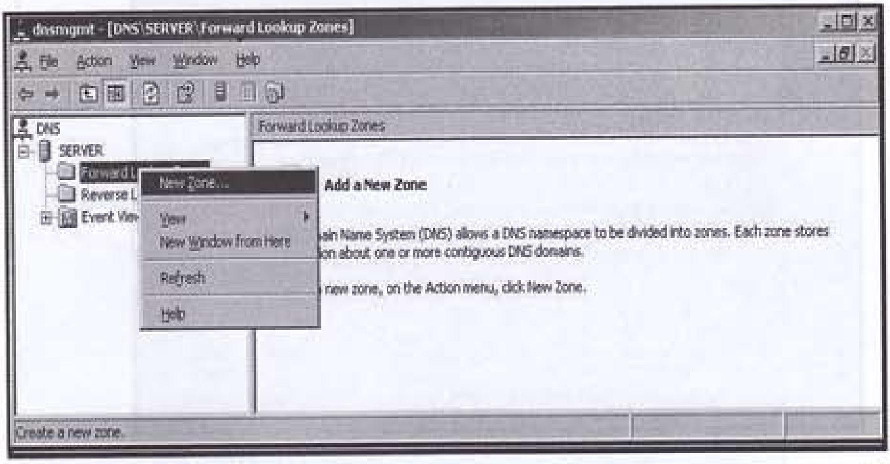
ကဲ ကျွန်တော်အခု ဒီ DNS Console ထဲမှာ ပါတဲ့ Forward Lookup Zone နှင့် Reverse Lookup Zone ရဲ့ လုပ်ဆောင်ချက်ကို ရှင်းပြပါမယ်။ ကျွန်တော်အထက်မှာ ရှင်းပြခဲ့တယ်နော်။ DNS Server ဆိုတာ IP Address တွေကို Naming System သတ်မှတ်ပေးတဲ့ Server ဖြစ်တယ်။ ဒီတော့ အဲဒီ DNS Console ထဲမှာ ပါလာတဲ့ Forward Lookup နှင့် Reverse Lookup Zone က IP Address တွေကို Naming System သတ်မှတ်ပေးမှာ ဖြစ်ပါတယ်။

Forward Lookup Zone အလုပ်လုပ် ပေးမှာ ကတော့ Name (နာမည်) ကနေ IP Address ကို Translate ပြောင်းလဲပေးမှာ ဖြစ်တယ်။ Reverse Lookup Zone အလုပ်လုပ်ပေးမှာကတော့ IP Address ကနေ Name သို့ Translate လုပ်ပေးမှာဖြစ်တယ်။ အဲဒီလိုမျိုး Name to IP Address နှင့် IP Address to Name သို့ ပြောင်းလဲပေးရန်အတွက် Forward Lookup နှင့် Reverse Lookup တို့တွင် Zone တွေကို Create လုပ်ပြီးမှ အလုပ်လုပ်မှာ ဖြစ်ပါတယ်။ ကဲ ဒါဆိုရင် Forward Lookup Zone နဲ့ Reverse Lookup Zone တို့ကို ဖန်တီးကြရအောင်နော်။

၇.၆.၁ **Forward Lookup Zone ကိုဖန်တီးပုံ**

၁။ DNS Console ထဲက Server Node ကို ဖြန့်ချပြီးရင် Forward Lookup Zone ကို Right Click နှိပ်ပြီးရင် New Zone ကို Click လုပ်ပါ။

ပုံ ၇.၃၉

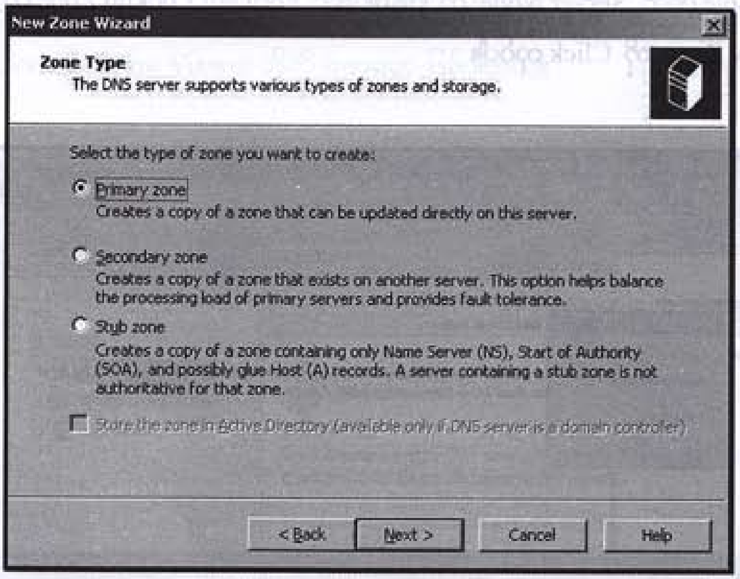


၂။ ဒါဆိုရင် Welcome to New Zone Wizard Page ပေါ်မယ်။

ပုံ ၇.၄၀

၃။ Next ကို Click လုပ်ပါ။ Zone Type Page ပေါ်မယ်။

ပုံ ၇.၄၁



၄။ အဲဒီ Zone Type Page မှာ–

(၁) Primary Zone
(၂) Secondary Zone
(၃) Stub Zone ဆိုပြီး 3 မျိုးတွေ့ရပါမယ်။

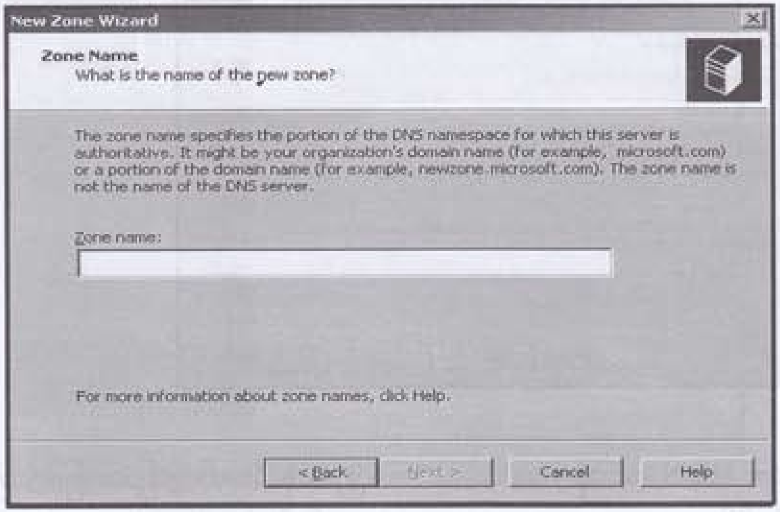
(၁) Primary Zone ဆိုတာ DNS ကို Primary Zone အနေနဲ့ ဖန်တီးထားတာဖြစ်တယ်။

(၂) Secondary Zone ဆိုတာ DNS ကို Secondary Zone အနေနဲ့ ဖန်တီးထားတာဖြစ်တယ်။ ဒါပေမယ့် DNS ကို Secondary Zone အနေနဲ့ ဖန်တီးမယ်ဆိုရင် Primary Zone ရှိမှရပါမယ်။

(၃) Stub Zone ဆိုတာက DNS Server တွေကို Name Space တွေကို Share ယူသုံးမယ့် Zone ဖြစ်ပါတယ်။

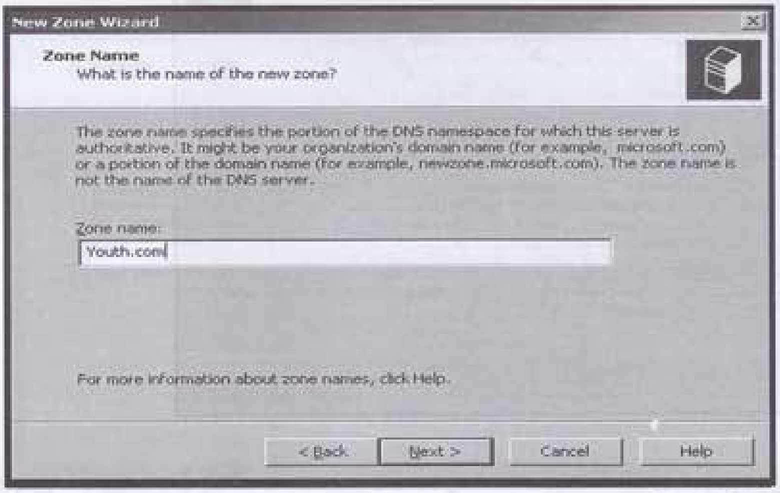
၅။ ကဲ ဒီတော့ ကျွန်တော်တို့က DNS Server ကို အခုမှစပြီး Create လုပ်တာဖြစ်လို့ Zone Type Page မှာ Primary Zone ဘေးက Radio Button ကို On ပေးရပါမယ်။ ပြီးရင် Next ကို နှိပ်ပါ။ Zone Name Page ပေါ်မယ်။

ပုံ ၇.၄၂

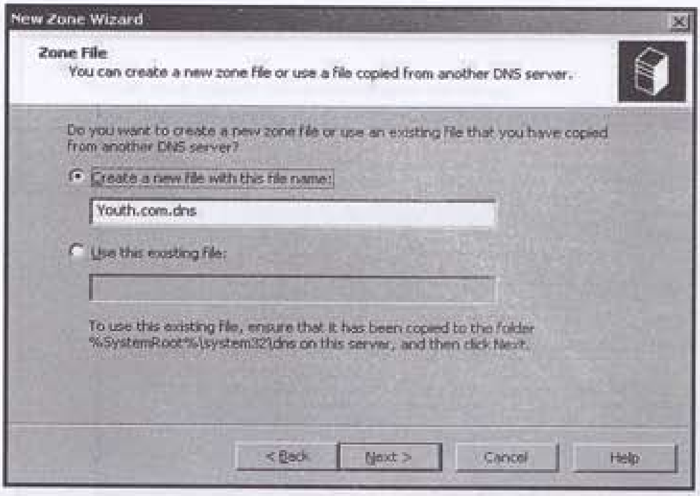


၆။ ၄င်း Zone Name နေရာတွင် ထည့်ပေးရမယ့် Name သည် DNS Suffix Name ဖြစ်တယ်။ ကျွန်တော် အထက်မှာပြခဲ့တဲ့ Diagram ထဲကအတိုင်းပဲ DNS Name ကို ထည့်လိုက်ပါမယ်။

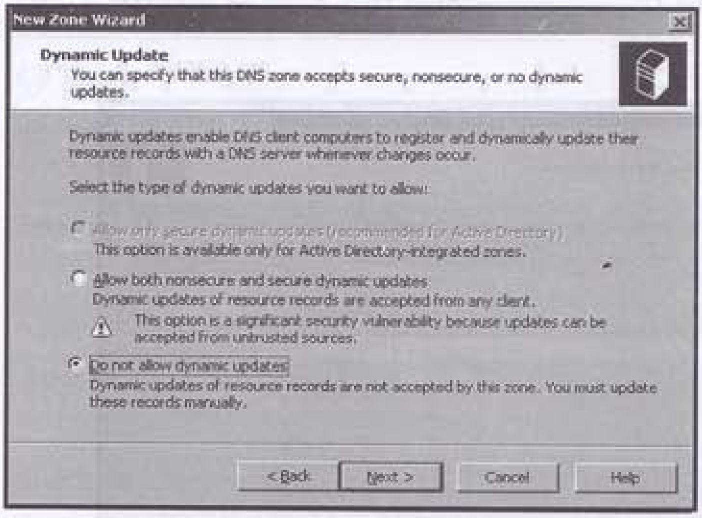
ပုံ ၇.၄၃



၇။ ပြီးရင် Next ကိုနှိပ်ပါ။ Zone File Page ပေါ်မယ်။

ပုံ ၇.၄၄ 

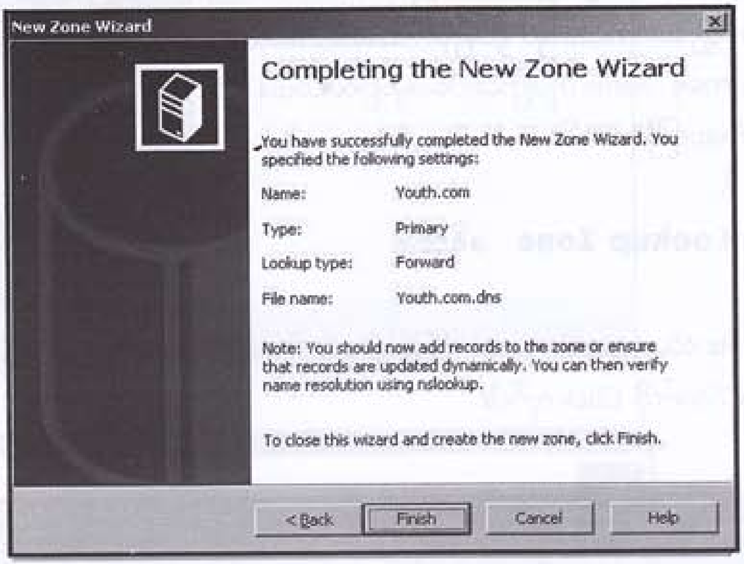
၈။ မိမိရဲ့ Zone File Name ကို youth.com.dns ဆိုပြီး ဖန်တီးမယ်လို့ပြောတာဖြစ်ပါတယ်။ ၎င်း Zone File သည် မိမိ Forward Lookup Zone ထဲမှာဖန်တီးတဲ့ Host Record File တွေကို သိမ်းဆည်းပေးမယ့် Zone File ဖြစ်ပါတယ်။ Next ကိုနှိပ်ပါ။ Dynamic Update Page ပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၄၅ 

၉။ ၎င်း Page သည် Client Computer တွေက DNS Server ဆီသို့ Dynamic Update လုပ်ခွင့်

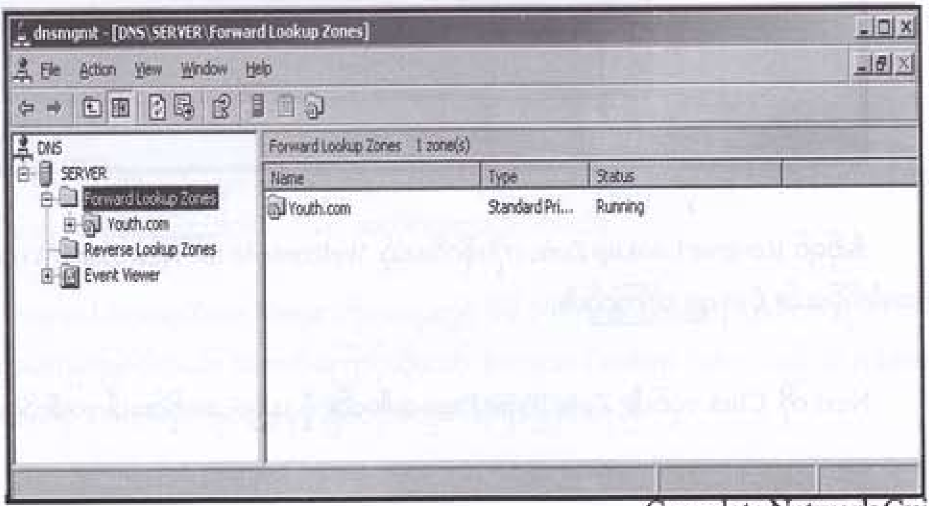
ပြုမယ်၊ မပြုဘူးလို့ပြောတာဖြစ်တယ်။ Do not Allow Dynamic Update ကိုပဲ ရွေးပြီးသွားပါ။ ပြီးရင် Next ကိုနှိပ်ပါ။ အဲဒီဆိုရင် Completion the New Zone Wizard Page ပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၄၆



၁၀။ Finish ကိုနှိပ်ပါ။ ကဲကဲ အဲဒီဆိုရင်တော့ ကျွန်တော်တို့တွေ Forward Lookup Zone ကို တည်ဆောက်ခြင်း ပြီးသွားပါပြီ။ အဲဒီ Forward Lookup Zone တည်ဆောက်တာပြီးသွားပြီဆိုရင် Forward Lookup Zone ကို ဖြန့်ချလိုက်ပါ။ ကျွန်တော်တို့ ဖန်တီးခဲ့တဲ့ youth.com ဆိုတဲ့ Zone ကိုတွေ့ရပါလိမ့်မယ်။

ပုံ ၇.၄၇

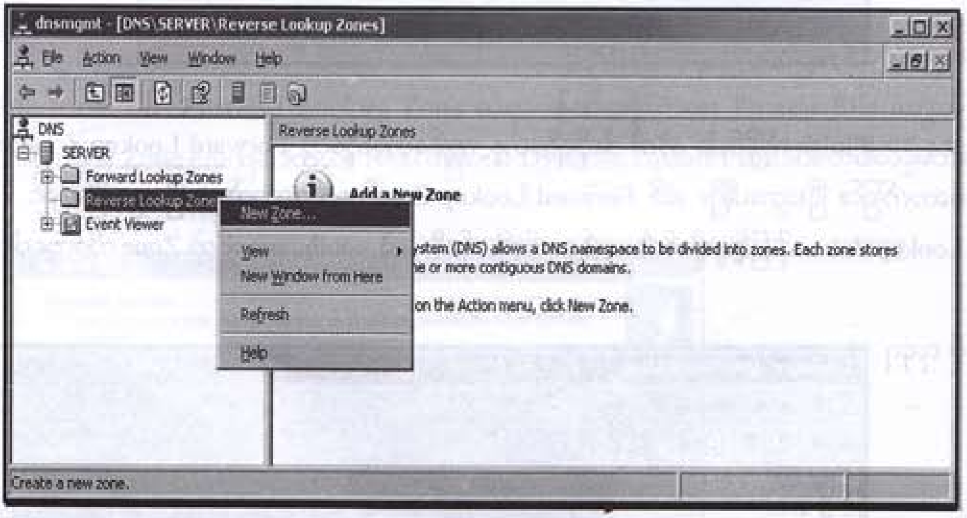


ကဲ ဒါဆိုရင်တော့ အခုကျွန်တော်တို့ DNS Zone ထဲက Forward Lookup Zone ကို တည်ဆောက်တာတော့ ပြီးသွားပါပြီ။ ဒါပေမယ့် ကျန်သေးတယ်ဗျ။ အကုန်လုံးပြီးသွားတာတော့ မဟုတ်သေးဘူး။ ကျွန်တော်တို့တွေ ဘာဆက်လုပ်ပေးဖို့ ကျန်သေးလဲဆိုရင် Reverse Lookup Zone ကို တည်ဆောက်ပေးဖို့ကျန်သေးတယ်လေ။ ကျွန်တော်အထက်မှာ ရှင်းပြခဲ့တယ်နော်။ Forward Lookup Zone ရဲ့ လုပ်ဆောင်ချက်က IP Address ကနေ Name ကိုပြောင်းလဲပေးမှာဖြစ်ပါတယ်။ ကဲ ဒီတော့ Reverse Lookup Zone ကိုထပ်ပြီး ဖန်တီးပေးကြရအောင်။

၇.၆.၂ **Reverse Lookup Zone** ဖန်တီးပုံ

၁။ DNS Console ထဲက Server Node ကိုဖြန့်ချပြီးရင် Reverse Lookup Zone ကို Right Click နှိပ်ပြီးရင် New Zone ကို Click လုပ်ပါ။

ပုံ ၇.၄၈

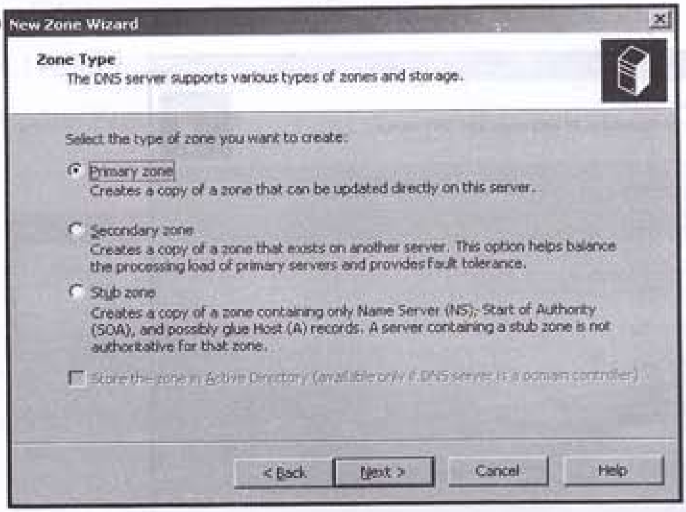


၂။ ဒါဆိုရင် Reverse Lookup Zone ကိုဖန်တီးမယ့် Welcome to the New Zone Wizard Box ပေါ်လာပါလိမ့်မယ်။ ပုံ ၇.၄၉ ကိုကြည့်ပါ။

၃။ Next ကို Click လုပ်ပါ။ Zone Type Page ပေါ်မယ်။ ပုံ ၇.၅၀ အတိုင်းပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၄၉

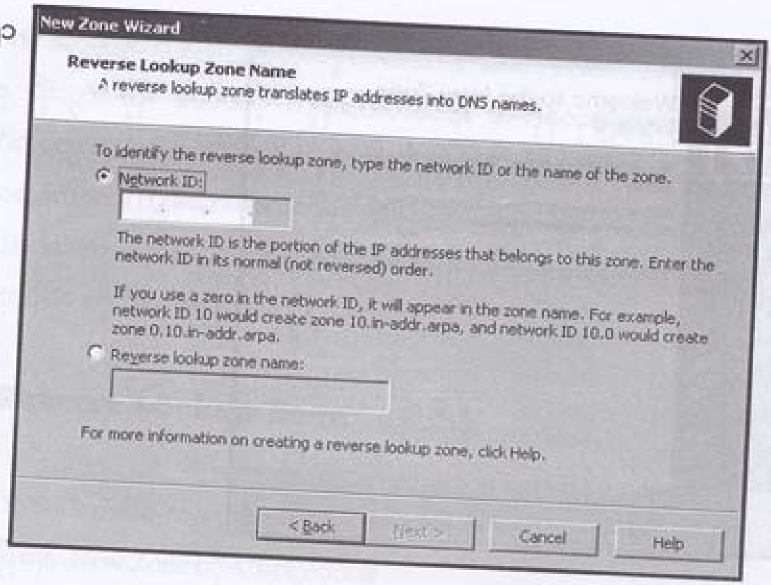
ပုံ ၇.၅၀



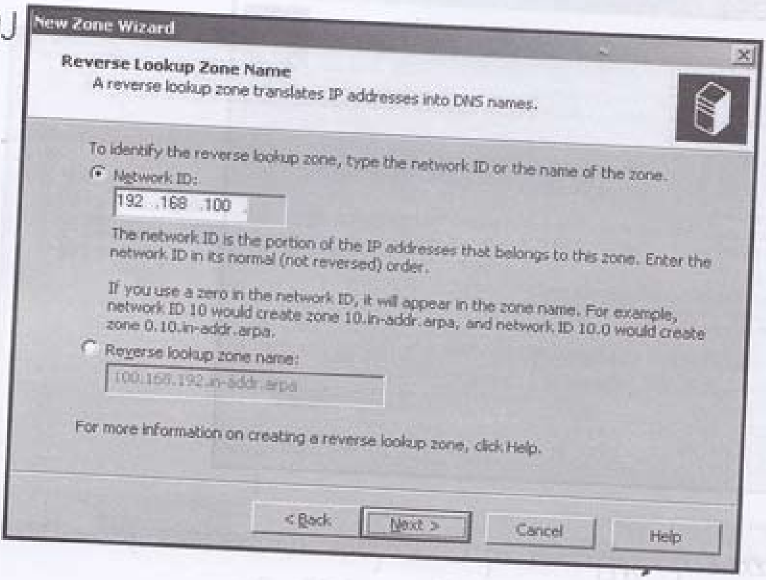
၄။ Primary Zone ကိုပဲရွေးပြီး Next ကို Click လုပ်ပါ။ Reverse Lookup Zone Name Page ပေါ်လာမယ်။ တစ်ဘက်မှာပြထားတဲ့ ပုံ ၇.၅၁ အတိုင်းတွေ့ရပါလိမ့်မယ်။

၅။ Reverse Lookup Zone Name ကိုပေးရာတွင် မိမိ Network Card IP Address ရဲ့ 3 Octet ကိုပြန်ထည့်ပေးရမှာဖြစ်ပါတယ်။ အဘယ်ကြောင့်ဆိုသော် Reverse Lookup Zone သည် IP Address ကနေ Name ကို Translate လုပ်ပေးမှာ ဖြစ်တဲ့အတွက်ကြောင့်ဖြစ်သည်။

ပုံ ၇.၅၁

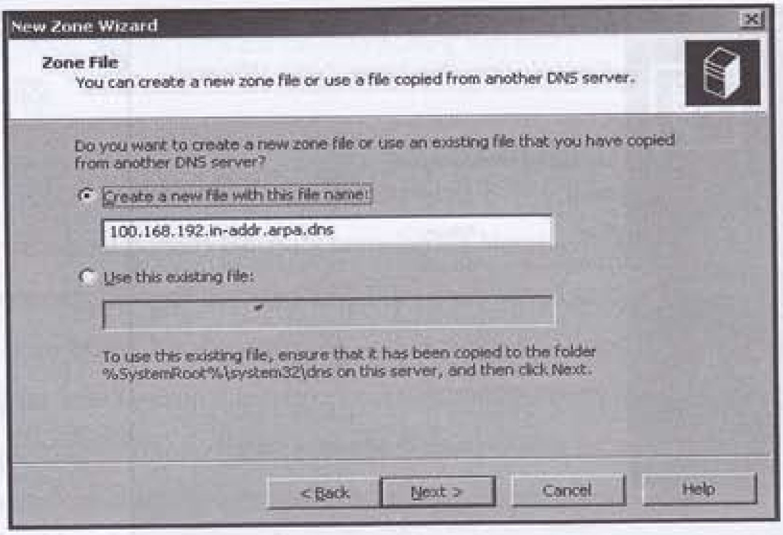


ပုံ ၇.၅၂



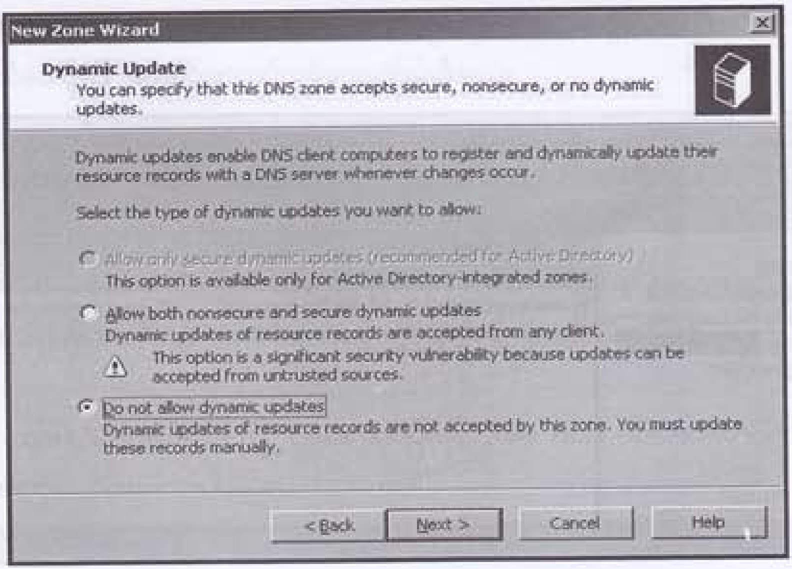
၆။ အထက်မှာပြထားတဲ့ ပုံ (၇.၅၂) မှာမြင်ရတဲ့အတိုင်း Reverse Lookup Zone Name ကိုပေးရာတွင် မိမိ Network Card ရဲ့ IP Address 3 Octet ကို ထည့်ပြီးသွားရင် Next ကို Click လုပ်ပါ။ Zone File Page ပေါ်မည်။

ပုံ ၇.၅၃



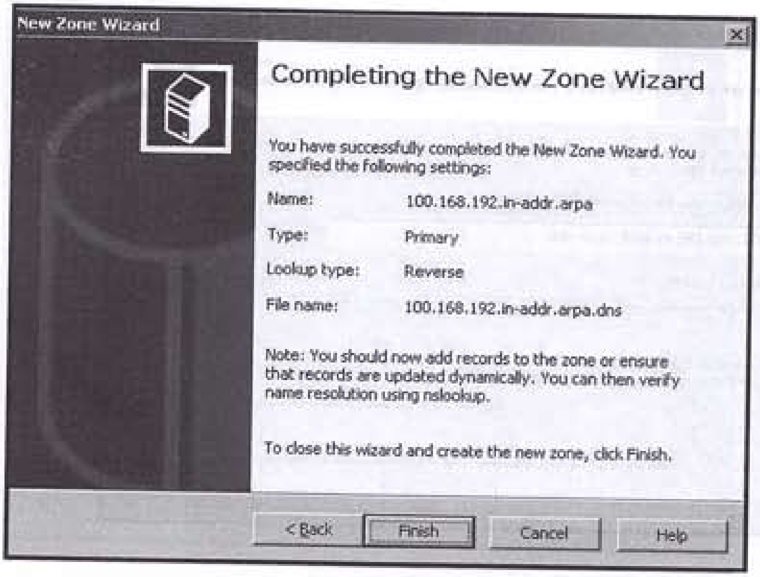
၇။ ငင်း Zone File Page သည် DNS Server ရဲ့ Reverse Lookup Zone File ကို 100.168.192.in-addr.arpa.dns ဆိုတဲ့ Name နဲ့ ဖန်တီးမယ်ပြောတာဖြစ်တယ်။ Next ကိုနှိပ်ပါ။ Dynamic Update Page ပေါ်မည်။

ပုံ ၇.၅၄



၈။ Do not allow dynamic updates ကိုပဲ ရွေးပြီး Next ကိုနှိပ်ပါ။ Completing the New Zone Wizard Page ပေါ်မယ်။

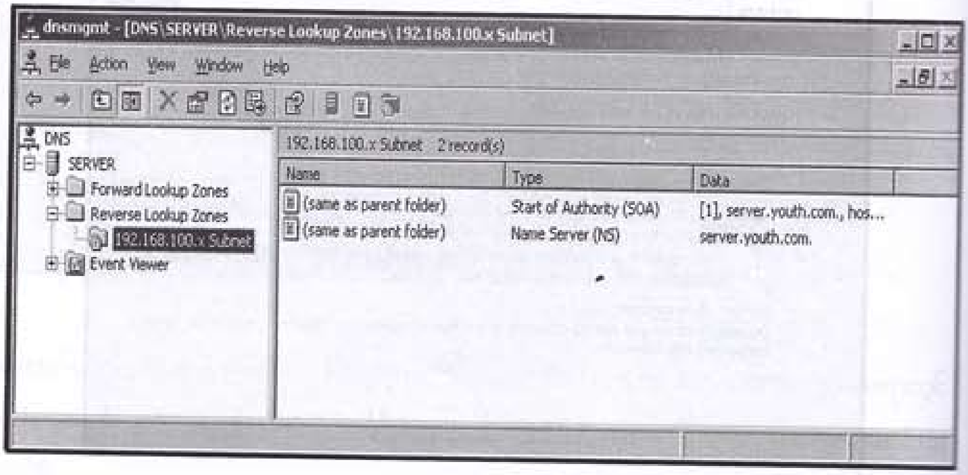
ပုံ ၇.၅၅



၉။ Finish ကိုနှိပ်ပါ။ ကဲ ဒီလိုဆိုရင် Reverse Lookup Zone ကို ဖန်တီးတာပြီးသွားပါပြီ။

၁၀။ အဲဒီ Reverse Lookup Zone ဖန်တီးပြီးသွားပြီဆိုရင်တော့ Reverse Lookup Zone ကိုဖြန့်ချလိုက်ပါ။

ပုံ ၇.၅၆



၁၀။ 192.168.100.x Subnet ဆိုတဲ့ Zone ကိုတွေ့ရမှာ ဖြစ်ပါတယ်။

ကဲကဲ အခုဆိုရင် Forward Lookup Zone နဲ့ Reverse Lookup Zone နှစ်ခုကို ဖန်တီးတာတော့ ပြီးသွားပါပြီ။

အခုပေမယ့် ကျွန်တော်တို့ အခုဖန်တီးတာသည် Forward Lookup Zone နှင့် Reverse Lookup Zone ကိုပဲ ဖန်တီးလိုက်တာ ဖြစ်တယ်။ တကယ်တမ်း Name to IP Address, IP Address to Name ကို ပြောင်းလဲပေးဖို့ရန်အတွက် အလုပ်လုပ်မယ့် File တွေကို မတည်ဆောက်ပေးရသေးဘူးဗျ။ အဲဒီ လို Name to IP, IP to Name အလုပ်လုပ်ပေးမယ့် File တွေကို တည်ဆောက်ပေးဖို့လည်း Forward Lookup Zone နဲ့ Reverse Lookup Zone ကိုတည်ဆောက်ပေးထားမှ ရမှာ ဖြစ်ပါတယ်။ ဘာကြောင့် တည်ဆောက်ပေးမှရမှာလဲဆိုရင် ကျွန်တော်တို့တွေ ဖန်တီးလိုက်မယ့် Name to IP, IP to Name ပြောင်းလဲ ပေးမယ့် File လေးကို သိမ်းဆည်းဖို့ရန်အတွက် တည်ဆောက်ပေးရခြင်းဖြစ်ပါတယ်။ အဲဒီ File တွေကို Record File လို့ခေါ်ပါတယ်။

ကဲ ဒီတော့ အဲဒီ Record File တွေကို တည်ဆောက်ကြရအောင်။

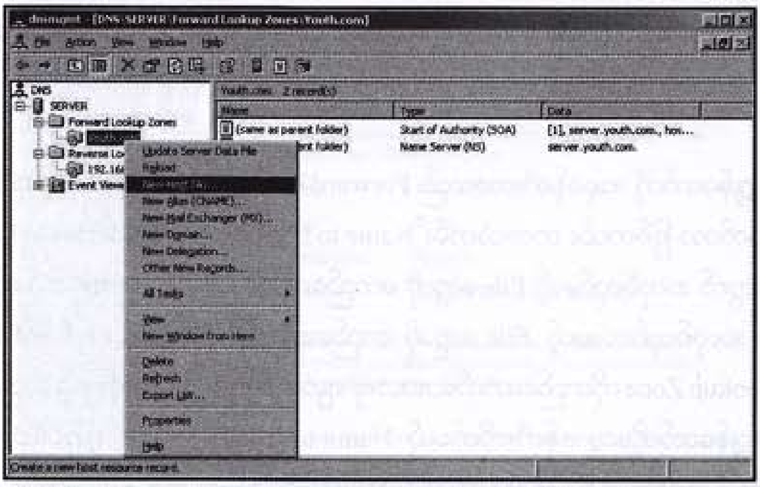
Forward Lookup Zone ထဲမှာ တည်ဆောက်ပေးရမယ့် Record File သည် New Host (A) File ဖြစ်တယ်။ ၎င်း New Host (A) File အလုပ်လုပ်ပေးတာသည် Name ကနေ IP Address ကို ပြောင်းလဲပေးဖို့ရန် အတွက် အလုပ်လုပ်ပေးမှာဖြစ်ပါတယ်။

၇.၇ **Forward Lookup Zone ထဲတွင် New Host (A) File ကိုတည်ဆောက်ပုံ**

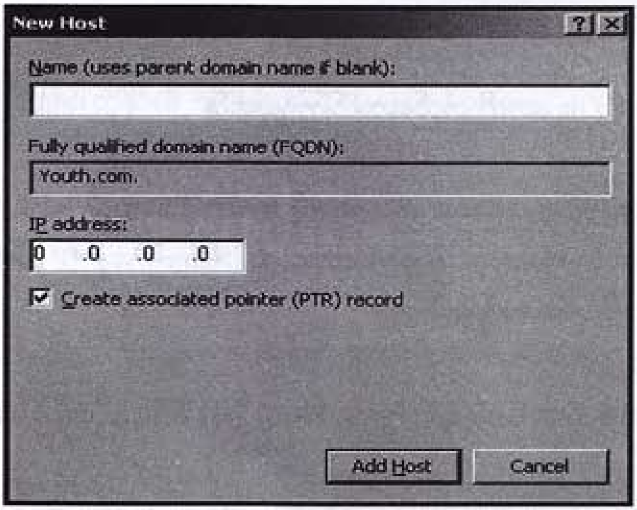
၁။ DNS Server Console ကိုဖွင့်ပါ။ ပြီးရင် Forward Lookup Zone ထဲက youth.com ပေါ်မှာ Right Click နှိပ်ပါ။ ပြီးရင် New Host (A) ကိုရွေးပါ။ ပုံ ၇.၅၇ ကိုကြည့်ပါ။

၂။ ၎င်း New Host A ကို Click လုပ်ပြီးရင် New Host Box ပေါ်လာပါလိမ့်မယ်။ ပုံ ၇.၅၈ မှာပြထားတဲ့အတိုင်းပေါ်လာပါမယ်။

ပုံ ၇.၅၇



ပုံ ၇.၅၈



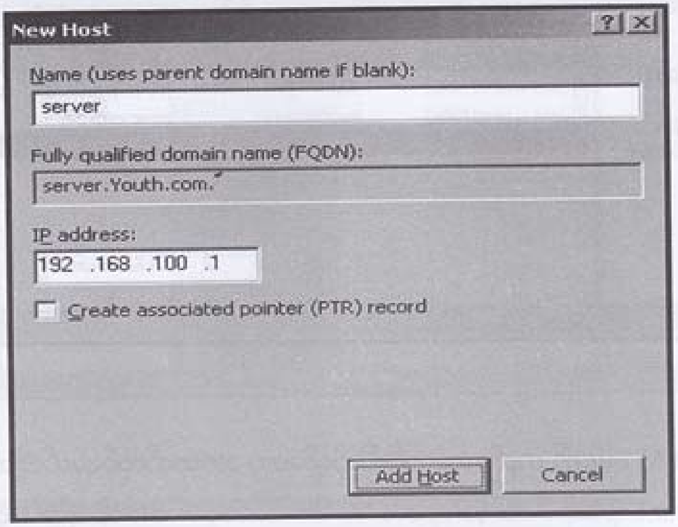
၃။ New Host Box ထဲက Name နေရာတွင် Server လို့ထည့်ပါ။ မိမိက Server လို့ထည့်လိုက်တာနဲ့ တပြိုင်နက်တည်း FQDN သည်လည်း server.youth.com ဆိုပြီး ပြောင်းသွားပါမယ်။

၄။ IP Address နေရာတွင် DNS Server ရဲ့ Address ကို ထည့်ပါ။ ၎င်း File သည် Name to IP Address ကို Translate လုပ်ပေးမှာ ဖြစ်ပါတယ်။

၅။ Create Associated Pointer Check Box ကို "On" ထားရင် ဖြုတ်လိုက်ပါ။ အကယ်၍ "On" ထားခဲ့ရင်တော့ Reverse Lookup Zone ထဲတွင် New Pointer PTR ကို ဖန်တီးပေးစရာ မလိုတော့ပါဘူး။

ဒါဆိုရင် DNS ဆိုပြီး Box တစ်ခုပေါ်လာမယ်။ ပုံ ၇.၆၀ ပါ။

ပုံ ၇.၅၉

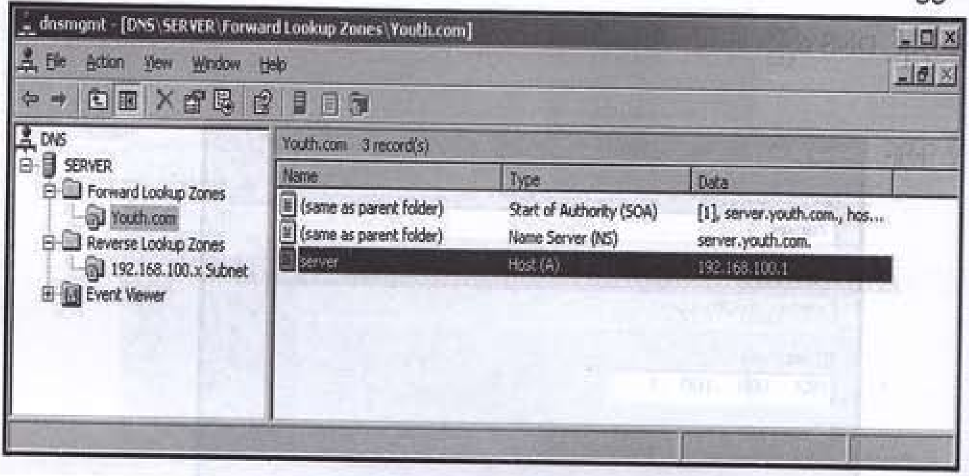


ပုံ ၇.၆၀

၄င်း Box သည် server.youth.com ဆိုတဲ့ Record File ကို Create လုပ်တာပြီးဆုံးသွားပြီလို့ပြောခြင်းဖြစ်ပါတယ်။

၆။ OK Button ကိုနှိပ်ပါ။ ပြီးရင် New Host Box ထဲက Done Button ကို နှိပ်လိုက်ပါ။ New Host(A) File ကိုတည်ဆောက်တာပြီးသွားပါပြီ။

ပုံ ၇.၆၁



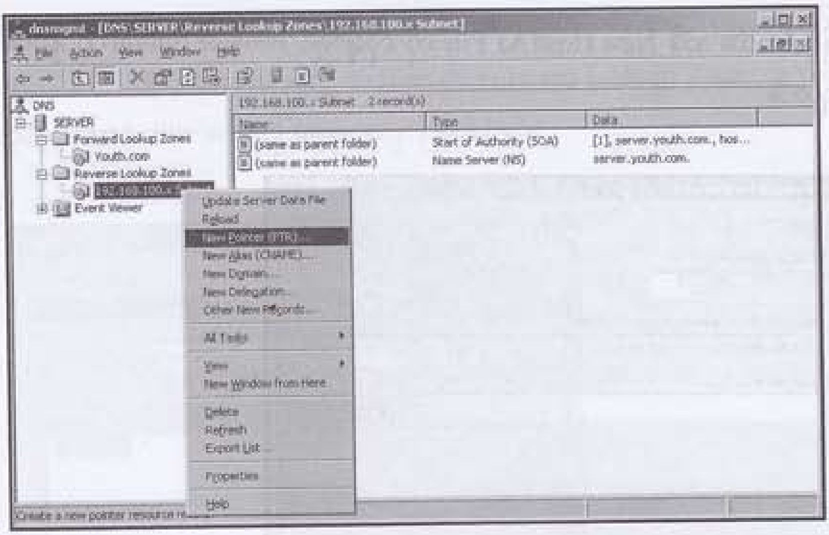
အဲဒီလို New Host(A) File ကို တည်ဆောက်ပြီးပြီဆိုရင်တော့ ဘာဆက်လုပ်ရမယ်လို့ထင်သလဲ။ ကျန်သေး တယ်နော်။ Reverse Lookup Zone မှာလည်း IP Address ကနေ Name ကို ပြောင်းလဲပေးမယ့် Record File ကို တည်ဆောက်ပေးရမယ်။ Record File Name ကတော့ New Pointer PTR File ဖြစ်တယ်။

၇.၈ **Reverse Lookup Zone ထဲတွင် New Ponter (PTR) File ကိုတည်ဆောက်ပုံ**

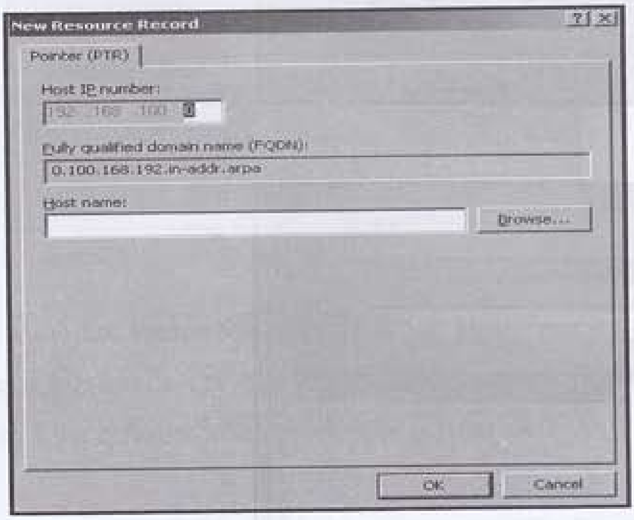
၁။ DNS Server Console ကိုဖွင့်ပါ။ ပြီးရင် Reverse Lookup Zone ထဲက 192.168.100.x Subnet ပေါ်မှာ Right Click နှိပ်ပါ။ ပြီးရင် New Pointer (PTR) ကိုပဲရွေးပါ။ ပုံ ၇.၆၂ မှာပြထားပါတယ်။

၂။ ၄င်း New Pointer (PTR) ကို Click လုပ်ပြီးရင် New Reverse Record Box ပေါ်လာပါလိမ့်မယ်။ ပုံ ၇.၆၃ ကိုကြည့်ပါ။

ပုံ ၇.၆၂



ပုံ ၇.၆၃

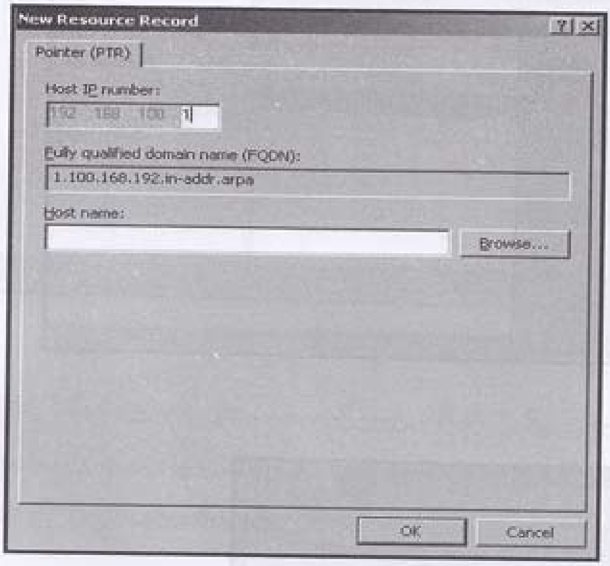


၃။ New Resource Record Box ထဲက Host IP Number တွင် IP Address ကို (192.168.100.1) DNS Server ရဲ့ IP Addresss ကိုထည့်ပေးပါ။ ၎င်း IP Number ကိုထည့်လိုက်တာနဲ့ FQDN သည် 100.168.192.in-addr.arpa ကနေ 1.100.168.192.in-addr.arpa လို့ပြောင်းသွားပါလိမ့်မယ်။ ပုံ ၇.၆၄ ကိုတွေ့ရမှာပါ။

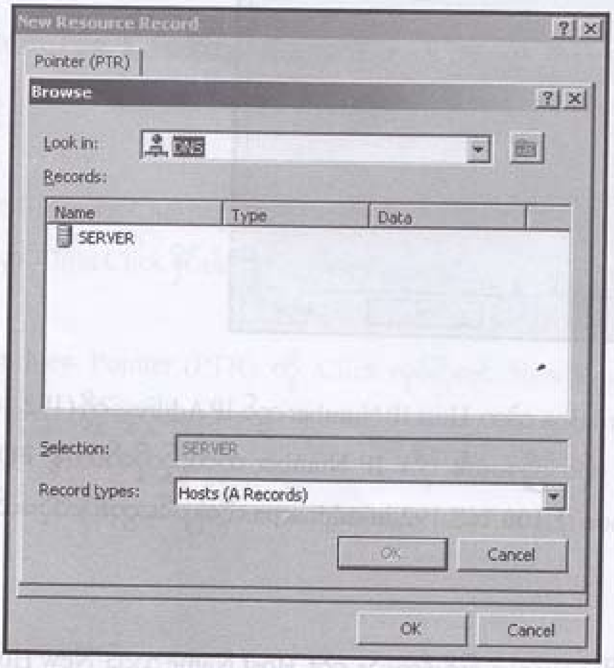
၄။ ပြီးရင် Host Name ကိုရှာပေးရမှာ ဖြစ်ပါတယ်။ ၎င်း Host Name သည် New Host(A) File

ကိုပြောတာဖြစ်ပါတယ်။ အဲဒီ New Host(A) File ကို လိုချင်ရင် Browse Button ကို နှိပ်ပါ။ ပုံ ၇.၆၅ အတိုင်းတွေ့ရမှာပါ။

ပုံ ၇.၆၄

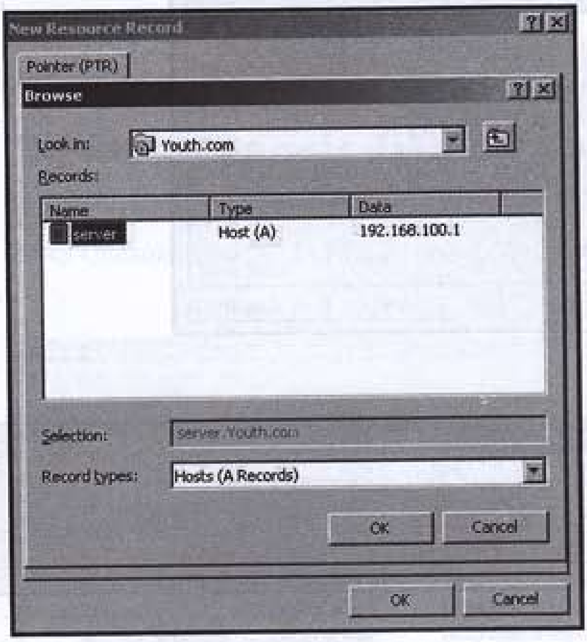


ပုံ ၇.၆၅



၅။ Browse ဆိုတဲ့ Box ပေါ်လာပါလိမ့်မယ်။ အဲဒီ Box ထဲက Record Types: သည် New Host (A Records) File ကိုရှာနိုင်းတာဖြစ်လို့ Server >> Forward Lookup Zone >> youth.com >> Server ဆိုတဲ့ HostA File လေးကို ရွေးပေးရမှာဖြစ်ပါတယ်။

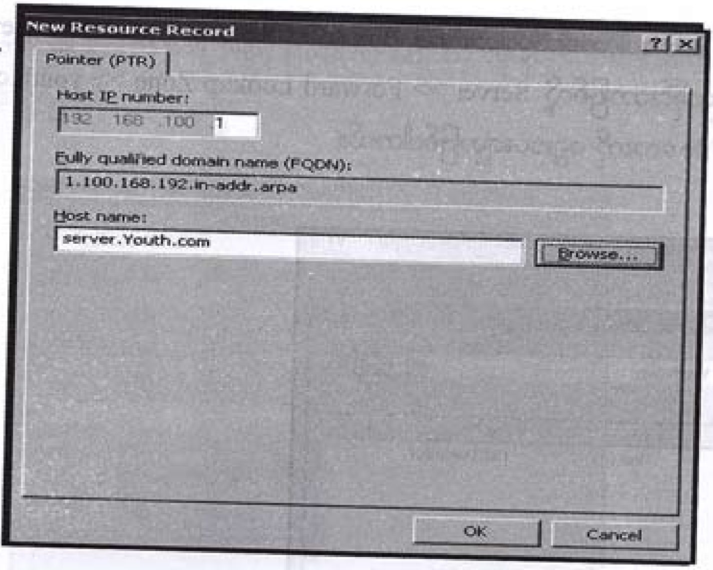
ပုံ ၇.၆၆



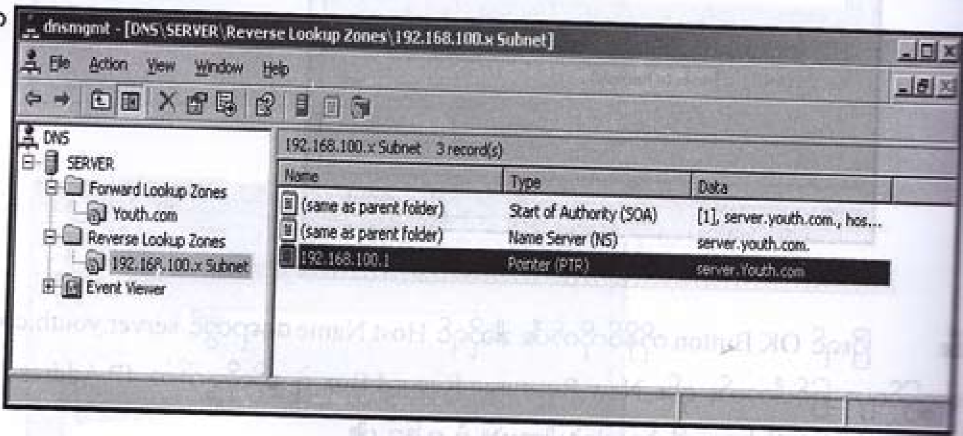
၆။ ပြီးရင် OK Button ကိုနှိပ်လိုက်ပါ။ အဲဆိုရင် Host Name နေရာတွင် server.youth.com ဆိုပြီး တွေ့မြင်ရမှာ ဖြစ်ပါတယ်။ ၎င်း New Resource Record Box ရဲ့ ဆိုလိုချက်က IP Address နဲ့ Host Name ကို Link ချိတ်ပေးလိုက်တာဖြစ်ပါတယ်။ ပုံ ၇.၆၇ ပါ။

၇။ OK Button ကို နှိပ်လိုက်ပါ။ New Pointer (PTR) File ကိုဖန်တီးပြီးတာတွေ့ရပါလိမ့်မယ်။ တစ်ဘက်မှာပြထားတဲ့ ပုံ ၇.၆၈ ကိုကြည့်လိုက်ပါ။

ပုံ ၇.၆၇



ပုံ ၇.၆၈



ကဲ ကောင်းပြီ။ ဒါဆိုရင်တော့ DNS Server ရဲ့ IP Address အတွက်တော့ Naming System သတ်မှတ်ပြီးသွားပါပြီ။ ဒါပေမယ့် ကျွန်တော်ဆွဲပြထားတဲ့ Diagram လေးကိုလည်း ပြန်ကြည့်လိုက်ဦး။ Client တွေအတွက်ကတော့ သူတို့ IP Address ကို Name သတ်မှတ်ပေးရအောင်။

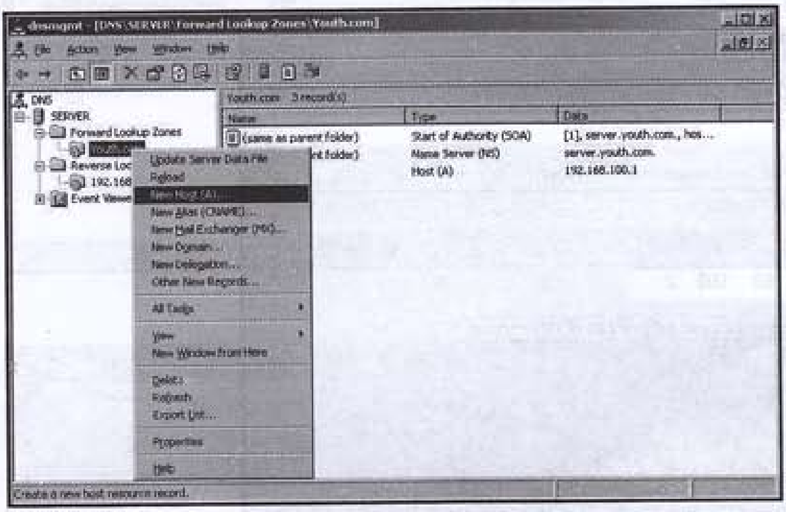
Forward Lookup Zone ထဲက New Host(A) File ရဲ့ လုပ်ဆောင်ချက်နှင့် Reverse Lookup Zone ထဲက New Pointer (PTR) ရဲ့ လုပ်ဆောင်ချက်က ဘာတွေကို လုပ်ဆောင်ပေးတယ်ဆိုတာ ကျွန်တော် ပြောခဲ့တယ်နော်။ ကောင်းပြီ။ ဒီလိုဆိုရင် Client Computer တွေအတွက်လည်း Naming

System သတ်မှတ်ပေးရအောင်။ But...ဒါပေမယ့် ကျန်တော်အခု Client 1 အတွက် Naming System သတ်မှတ်ပေးတာကိုပဲ ပြမှာ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုတော့ Client 2 နဲ့ Client 3 ကိုသတ်မှတ်မယ်ဆိုရင်လည်း Client 1 ကလုပ်ခဲ့တဲ့ ပုံစံအတိုင်းပဲလုပ်ရမှာဖြစ်လို့ပါ။ ကဲ Client 1 ကို Name သတ်မှတ်တာ စလိုက်ရအောင်။

၇.၉ Client 1 အတွက် Forward Lookup Zone မှာ Naming System သတ်မှတ်ရန်အတွက် New Host(A) ကိုဖန်တီးပုံ

၁။ DNS Console ထဲက >> Forward Lookup Zone >> New Host(A) ကိုနှိပ်ပါ။

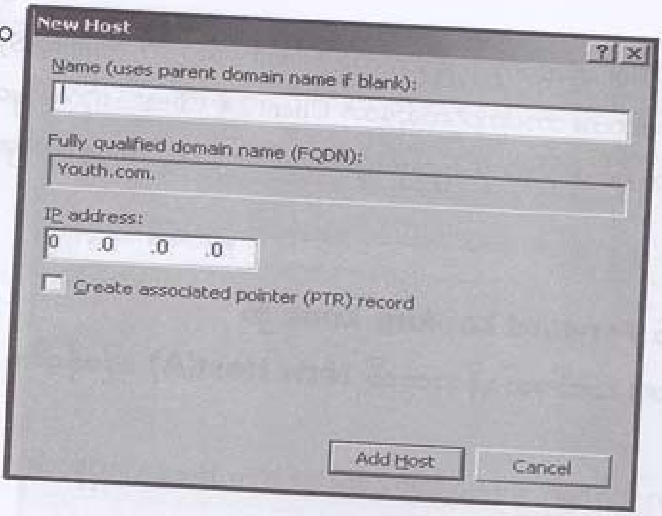
ပုံ ၇.၆၉



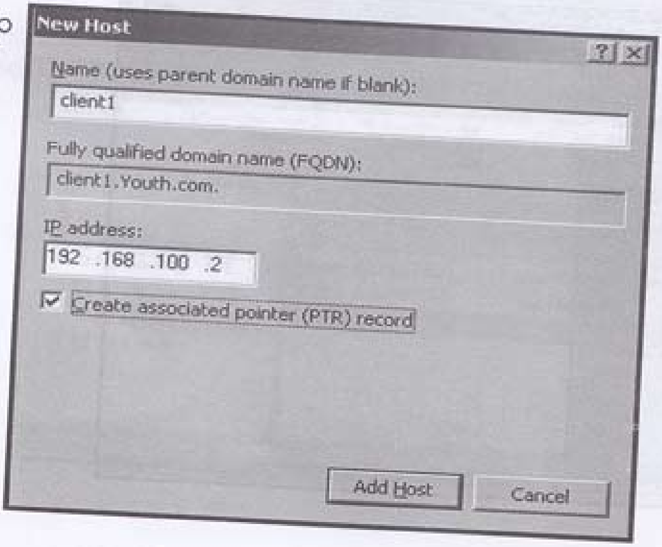
၂။ ဒါဆိုရင် New Host Box ပေါ်လာပါလိမ့်မယ်။ ပုံ ၇.၇၀ ကိုတွေ့ရပါလိမ့်မယ်။

၃။ ၄င်း New Host Box ထဲက Name နေရာတွင် Client 1 Computer ရဲ့ Computer Name ကို ထည့်ပေးပါ။ IP Address နေရာမှာ Client 1 Computer ရဲ့ IP Address ကို ထည့်ပေးပါ။ ပုံ ၇.၇၁ အတိုင်းတွေ့ရမယ်။

ပုံ ၇.၇၀



ပုံ ၇.၇၁



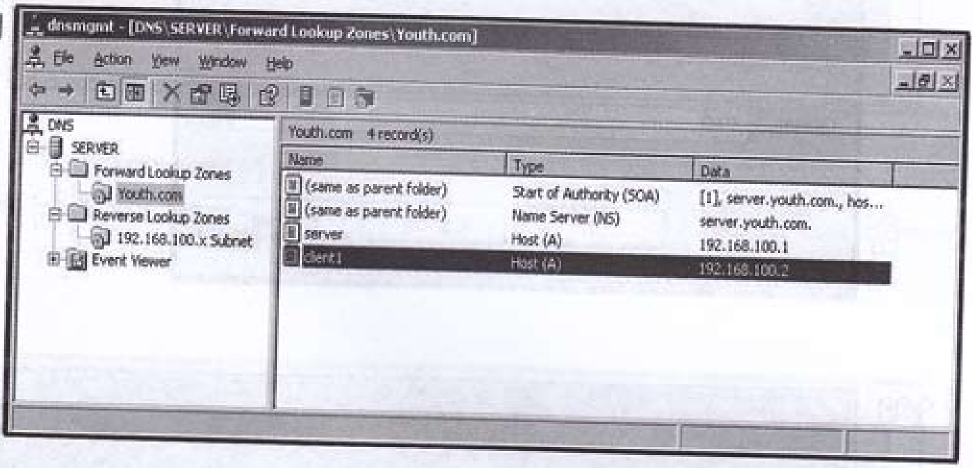
၄။ Client 1 Computer Name => Client1, Client1 Computer ရဲ့ IP Address => 192.168.100.2 ထည့်ပေးပါ။ ပြီးရင် Create Associated Pointer PTR Record ရဲ့ Check Box လေးကိုပါ "On"ပေးမယ်။

၅။ ပြီးရင် Add Host ကိုနှိပ်။ OK လို့ပြော။ ပြီးရင် Done ကိုနှိပ်ပါ။ အဲဒီဆိုရင် Client 1 အတွက် Naming Setting သတ်မှတ်တာပြီးသွားပါပြီ။

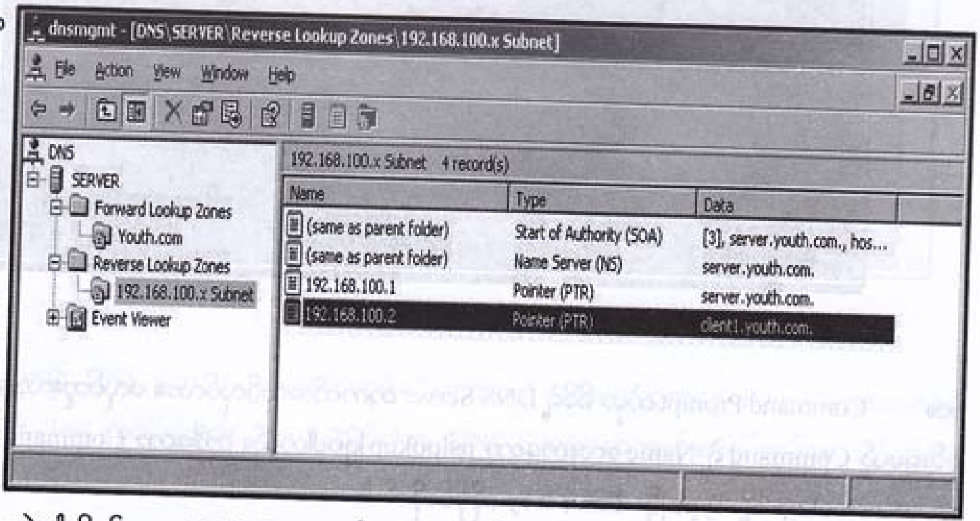
၆။ Reverse Lookup Zone ထဲမှာလည်း Client 1 အတွက် Host(A) Record File ကို မြင်တွေ့ရမှာဖြစ်ပါတယ်။ အဘယ့်ကြောင့်ဆိုသော် Client 1 အတွက် New Host(A) ဖန်တီးတုန်းက Create Associated Pointer PTR Record Check Box ကို "On" ထားခဲ့လို့ဖြစ်ပါတယ်။

မှတ်ချက်။ ။တကယ်လို့ Create Associate Pointer PTR Record File ကိုမတွေ့ရင် DNS Console Page ထဲမှာ Right Click နှိပ်ပြီး Refresh လုပ်ကြည့်ပါ။ တွေ့ရပါလိမ့်မယ်။

ပုံ ၇.၄၃



ပုံ ၇.၄၄

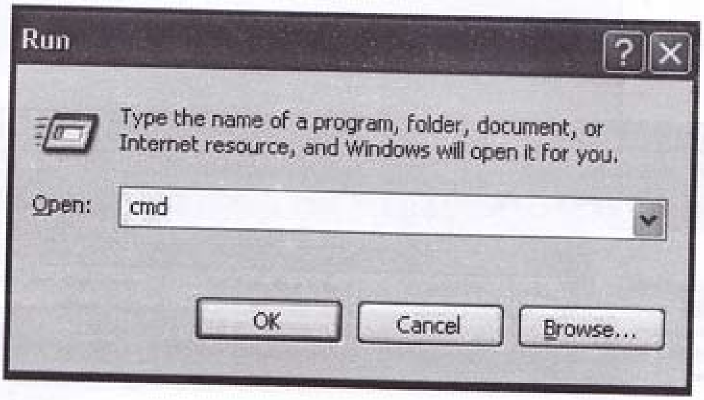


၇။ ကဲ ဒါဆိုရင်တော့ DNS Server ကို Install လုပ်တာတွေ၊ DNS Server ကို Configure လုပ်တာတွေအားလုံးပြီးဆုံးသွားပါပြီ။ ဒါပေမယ့် DNS Server တကယ်အလုပ်လုပ်နေလား။ မလုပ်ဘူးလား

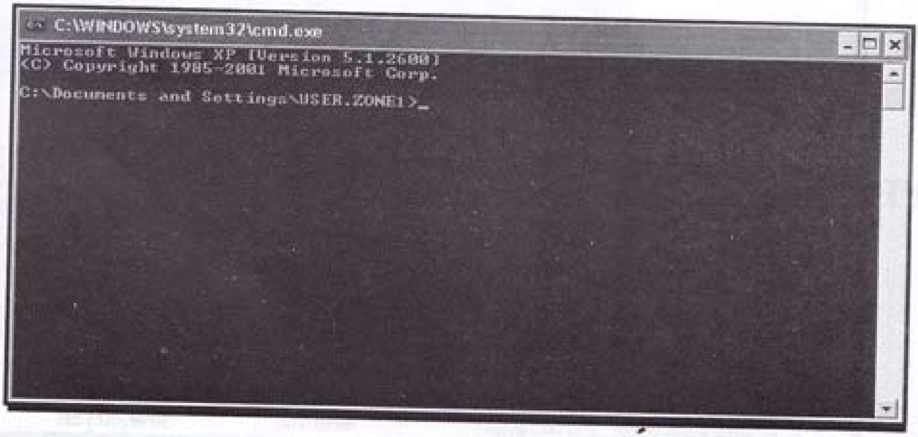
ဆိုတာကိုသိရအောင် Client 1 Computer ကနေ Test လုပ်ကြည့်ရမှာ ဖြစ်ပါတယ်။

၉။ Client 1 Computer ကနေ Test လုပ်မယ်ဆိုရင် အရင်ဦးဆုံး လုပ်ရမှာကတော့ Run Box ထဲမှာ cmd လို့ရိုက်ပြီး OK ကို နှိပ်လိုက်ပါ။ ဒါဆိုရင် Command Prompt ပေါ်လာပါလိမ့်မယ်။

ပုံ ၇.၇၄

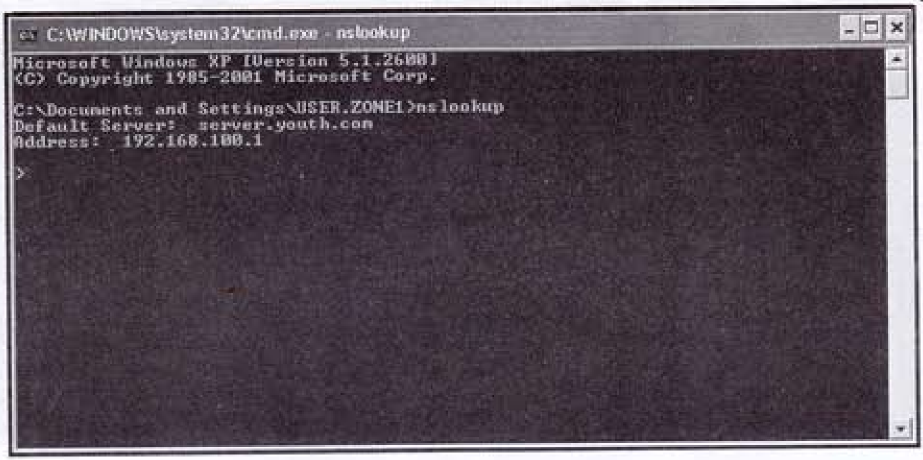


ပုံ ၇.၇၅



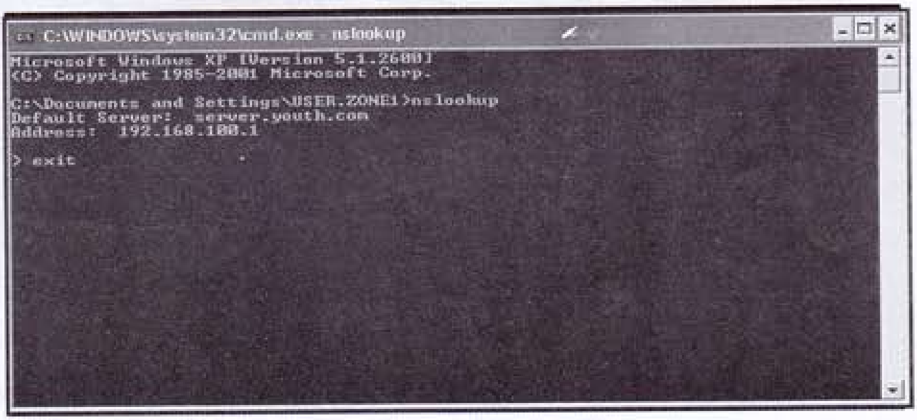
၁၀။ Command Prompt ထဲမှာ မိမိရဲ့ DNS Server တကယ်အလုပ်လုပ်လား၊ မလုပ်ဘူးလားဆိုတာကို စမ်းရမယ့် Command ရဲ့ Name လေးကတော့ nslookup ဖြစ်ပါတယ်။ ကဲဒီတော့ Command Prompt ထဲ မှာ nslookup လို့ Type ပြီး Enter Key ကိုနှိပ်လိုက်ပါ။

ပုံ ၇.၇၆



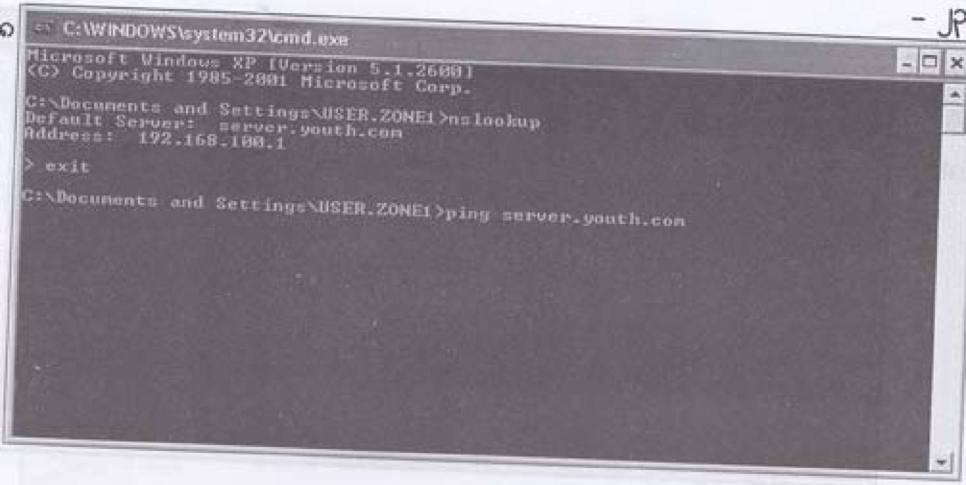
၁၁။ DNS Server ရဲ့ Name နဲ့ IP Address ကို ပြနေပြီဆိုရင်တော့ မိမိရဲ့ DNS Server တကယ်အလုပ်လုပ်သွားပြီ ဖြစ်ပါတယ်။ အဲ့ဒီ DNS Server Command Mode ထဲက ထွက်ချင်ရင်တော့ Exit ဆိုပြီးတော့ ရိုက်ပါ။

ပုံ ၇.၇၇

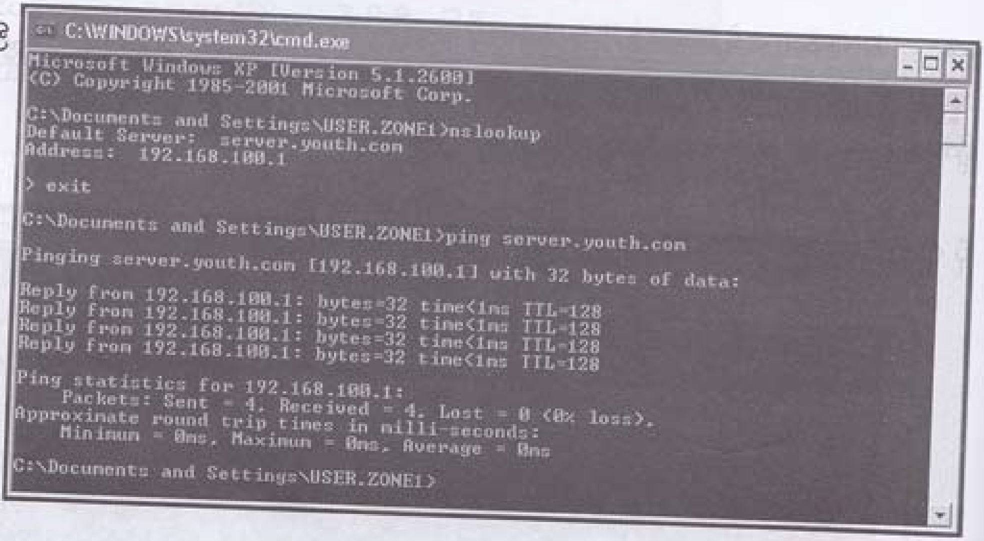


၁၂။ ပြီးရင် DNS Server ရဲ့ Name ကိုပဲ Command Prompt ထဲကနေ Ping Command ကို အသုံးပြုပြီး Test လုပ်ကြည့်ပါ။ Reply လုပ်ပါက DNS Server တကယ်အလုပ်လုပ်နေတယ်ဆိုတာ သေချာသွားပါပြီ။

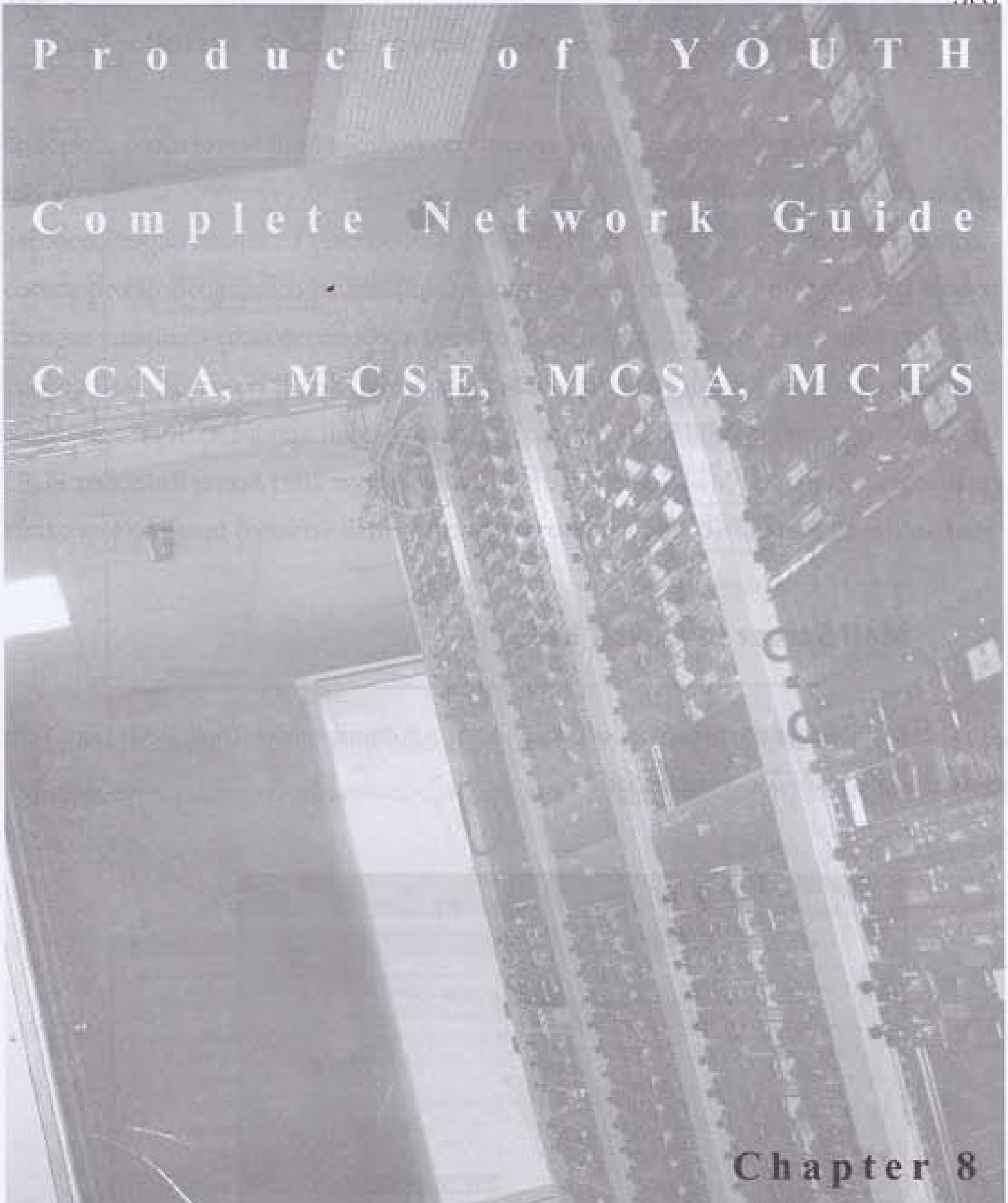
ပုံ ၇.၇၈



ပုံ ၇.၇၉



❖ ကဲ အားလုံးပဲ DNS Server ဆိုတာဘာလဲ။ DNS Server ကို ဘယ်လို Install လုပ်ရမလဲ။ DNS Server ထဲမှာ IP Address တွေကို ဘယ်လိုမျိုး Naming System သတ်မှတ်ပေးရမယ်ဆိုတာ နားလည် သဘောပေါက်သွားပြီလို့ ထင်ပါတယ်။ DNS Server အကြောင်းကို ဒီနေရာမှာပဲ ရပ်နားလိုက်ပါတော့မယ်။



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 8

Mail Server

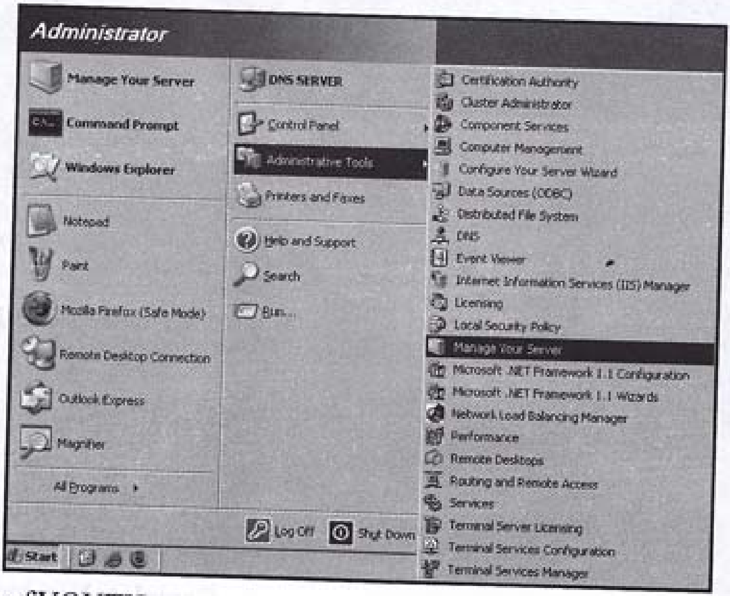
၈.၁ **Mail Server** ဆိုတာဘာလဲ၊ **Mail Server** ကိုဘယ်လို **Install**လုပ်မလဲ

Mail Server ဆိုတာဘာလဲ။ Mail Server ဆိုတာဘာပါလိမ့်။ Mail Server ဆိုတာ ဘာဖြစ်မယ်ထင်ပါသလဲ။ Mail Server ဆိုတာ ဒီလိုရှိတယ်။ ကွန်ပျူတာတွေဟာ တစ်လုံးနဲ့တစ်လုံး အပြန်အလှန် Net -work ချိတ်ဆက်ထားကြမယ်ပေ့ါ။ အဲဒီလို Network ချိတ်ဆက်ထားတဲ့ Computer တွေဟာ တစ်လုံးနဲ့တစ်လုံး Data တွေကို ဖလှယ်လို့တော့ရတယ်။ ဒါပေမယ့် Computer တွေတစ်လုံးနဲ့တစ်လုံး စာပို့ချင်တယ်ဆိုရင်တော့ Mail Server ရှိမှ ပို့လို့ရမှာ ဖြစ်ပါတယ်။ ကျွန်တော်ဆိုလိုချင်တာကတော့ Computer တွေသည် တစ်လုံးနှင့်တစ်လုံး အပြန်အလှန် Mail ပို့ချင်တယ်ဆိုလို့ရှိရင် Mail Server ရှိမှသာလျှင် Mail ပို့လို့ရမှာ ဖြစ်ပါတယ်။ ကျွန်တော်တို့ Mail Server ကို အသုံးပြုမယ်ဆိုရင် Mail Service ကို Run ပေးရပါမယ်။ ကျွန်တော်အခု Run ပြမယ့် Mail Server ကတော့ Windows Server 2003 Server Role ထဲက POP3 Mail Service ကို Run ပြမှာဖြစ်ပါတယ်။ ကဲဒီတော့ ကျွန်တော်တို့ Mail Server ကို Install လုပ်ကြရအောင်။

၈.၂ **Mail Server** ကို **Install** လုပ်ပုံ

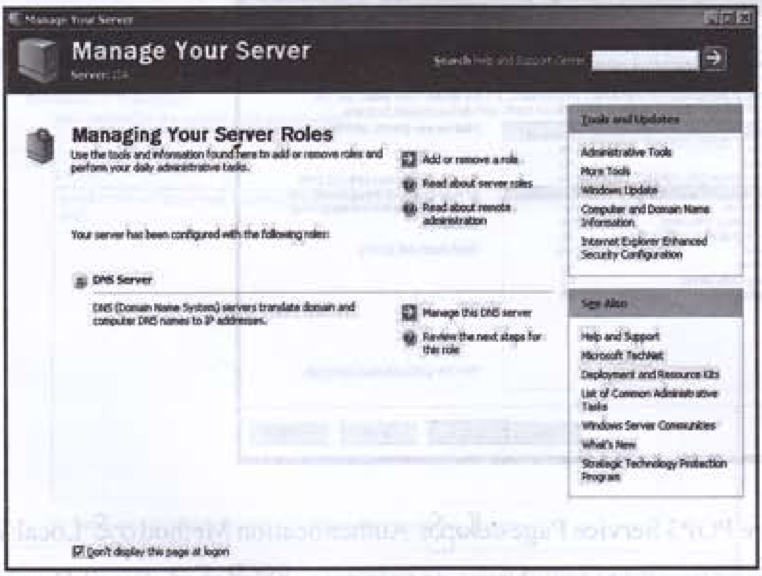
Mail Server ကို Install လုပ်မယ်ဆိုရင် Start > Administrative Tools > Manage Your Server ထဲကိုသွားပါ။ ပုံ ၈.၁ တွင်ကြည့်ပါ။

ပုံ ၈.၁



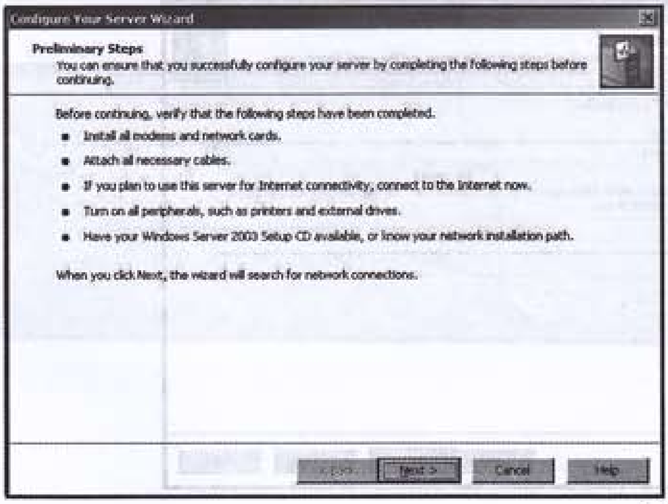
ပြီးရင် Manage Your Server Page ထဲတွင် Add or Remove Button ကို နှိပ်ပါ။ ပုံ ၈.၂ တွင်ကြည့်ပါ။

ပုံ ၈.၂



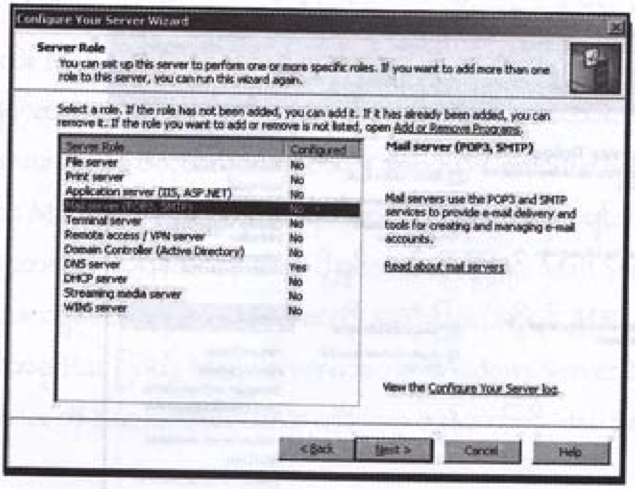
Preliminary Steps Page ဖြစ်ပါတယ်။ ၎င်းအဆင့်သည် မိမိရဲ့ Computer ထဲမှာ Cable တွေ၊ Modem, Network တွေကို စစ်ဆေးမယ်လို့ပြောတဲ့ အဆင့်ဖြစ်ပါတယ်။ Next ကို Click လုပ်ပါ။ ပုံ ၈.၃ တွင်ကြည့်ပါ။

ပုံ ၈.၃



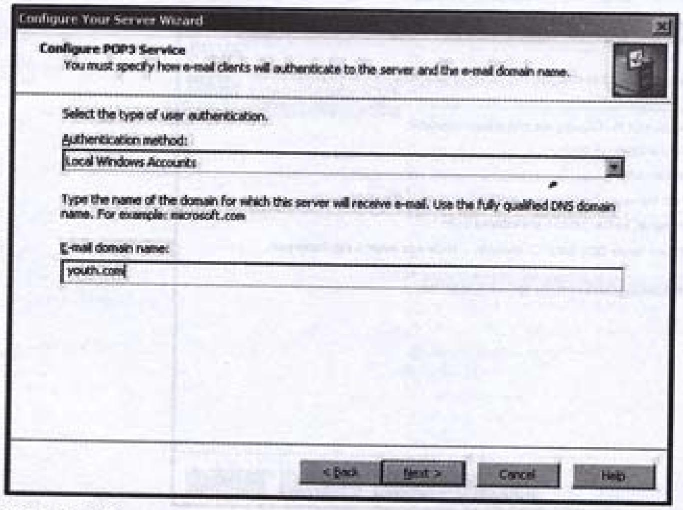
Server Role Page ပေါ်လာပါလိမ့်မယ်။ ကျွန်တော်တို့ အခု Install လုပ်မယ့် Server သည် Mail Server (POP3,SMPT) ကိုပဲရွေးပြီး Next Button ကိုနှိပ်ပါ။ ပုံ ၈.၄ တွင်ကြည့်ပါ။

ပုံ ၈.၄



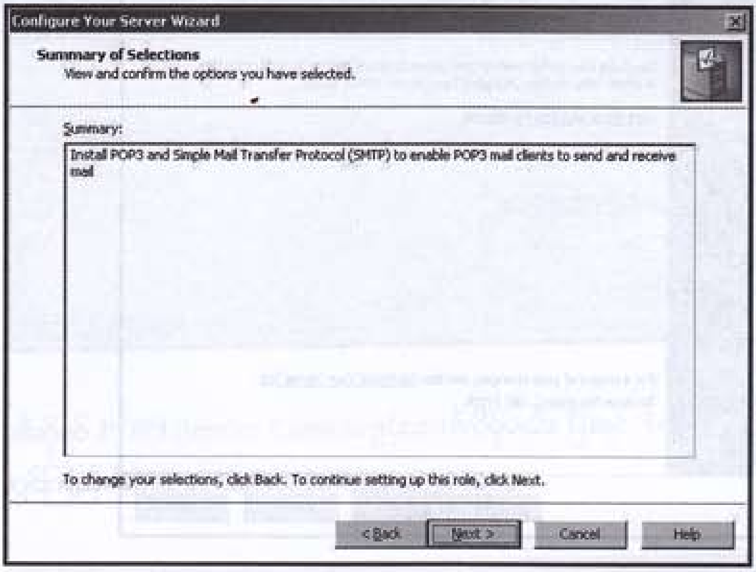
Configure POP3 Service Page ပေါ်မည်။ Authentication Method တွင် Local Windows Accounts ပဲထားခဲ့ပါ။ Email Domain Name နေရာမှာတော့ မိမိကြိုက်တဲ့ Email Domain Name ကိုသတ်မှတ်ပေးလို့ရပါတယ်။ ဥပမာ – youth.com လို့ပေးခဲ့ပါမယ်။ ၎င်း Domain Name သည် "username@youth.com" ဆိုပြီး မိမိရဲ့ Email Domain ဖြစ်သွားမှာဖြစ်တယ်။ ပြီးရင်တော့ Next Button ကိုနှိပ်ပါ။ ပုံ ၈.၅ တွင်ကြည့်ပါ။

ပုံ ၈.၅



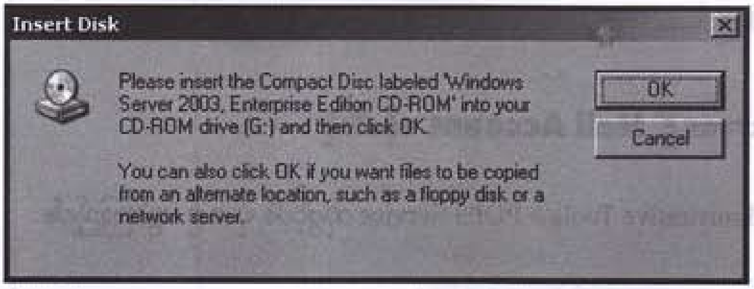
Summary of Selections Page ပေါ်မယ်။ ၎င်း Page တွင် POP3 နှင့် SMTP Service ကို Install လုပ်မယ်လို့ပြောတာဖြစ်ပါတယ်။ Next Button ကိုပဲ Click လုပ်ပါ။ ဒါဆိုရင် POP3 Service ကို Install လုပ်ပါမယ်။ ပုံ ၈.၆ တွင်ကြည့်ပါ။

ပုံ ၈.၆



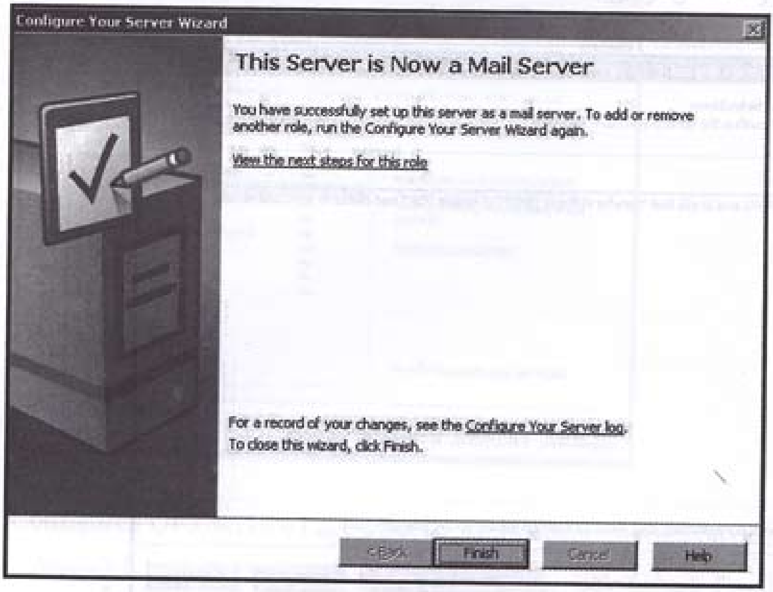
၎င်းသည် POP3 Service Component ကို Install လုပ်ဖို့ရန်အတွက် Windows Server 2003 CD ကို ပြန်တောင်းတာ ဖြစ်သည်။ မိမိ Windows တင်ထားတဲ့ Windows Server အခွေကို ထည့်ပေးလိုက်ပါ။ ဒါဆိုရင် ဆက်ပြီး POP3 Service ကို Install လုပ်သွားပါလိမ့်မယ်။ ပုံ ၈.၇ တွင်ကြည့်ပါ။

ပုံ ၈.၇



POP3 Service ကို Install လုပ်တာပြီးသွားပြီဖြစ်ပါတယ်။ ကဲ --- ဒီလိုဆိုရင် အခုကျွန်တော်တို့ အသုံးပြုနေတဲ့ Server ကြီးဖြစ်သွားပါပြီ။ Finish Button ကိုနှိပ်လိုက်ပါ။ ပုံ ၈.၈ တွင်ကြည့်ပါ။

ပုံ ၈.၈



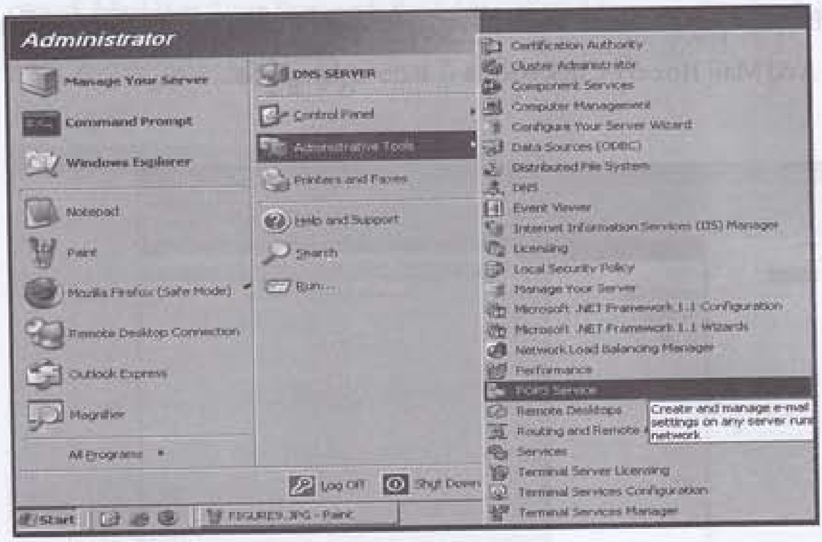
Mail Server ကြီးဖြစ်သွားပြီဆိုတော့ POP3 နှင့် SMTP Service Run သွားပြီပေါ့နော်။ ဒါဆိုရင် Client Computer တွေသည် တစ်လုံးနဲ့ တစ်လုံးအပြန်အလှန် E-Mail ပို့လို့ရဖို့ရန်အတွက် ကျွန်တော်တို့တွေက Mail Server ထဲမှာ Mail Account တွေကို ဖန်တီးပေးထားမှ Client Computer တွေက တစ်လုံးနှင့်တစ်လုံးအပြန်အလှန် Mail ပို့လို့ရမှာ ဖြစ်တယ်။

ကဲ --- အဲဒီတော့ Client Computer တွေ Mail ပို့လို့ရအောင် E-Mail Account ဖန်တီးပေးပုံလေးကတော့ ဒီလိုပါ---

၈. ၃ Mail Server ၌ Mail Account ဖန်တီးပုံ

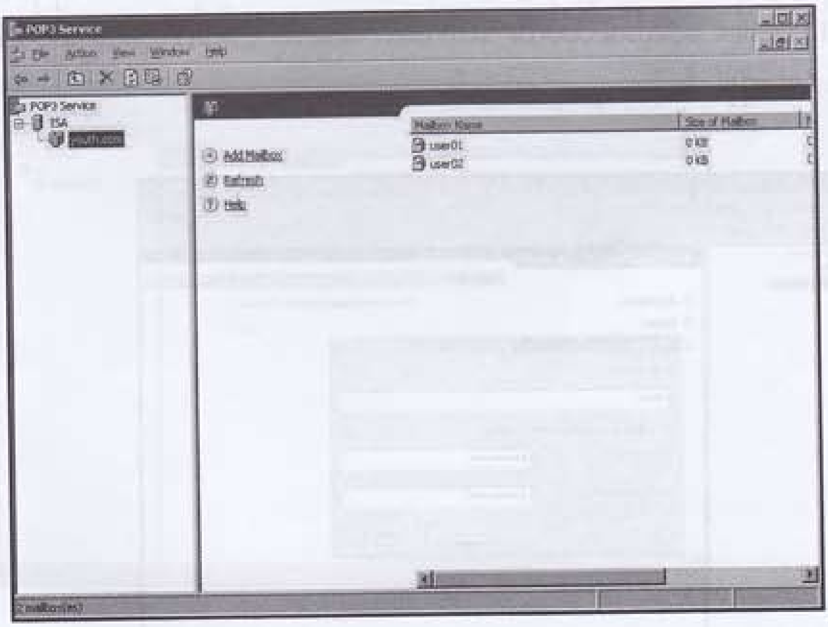
Start > Adimistrative Tools > POP3 Service ကိုဖွင့်ပါ။ ပုံ ၈.၉ တွင်ကြည့်ပါ။

ပုံ ၈.၉



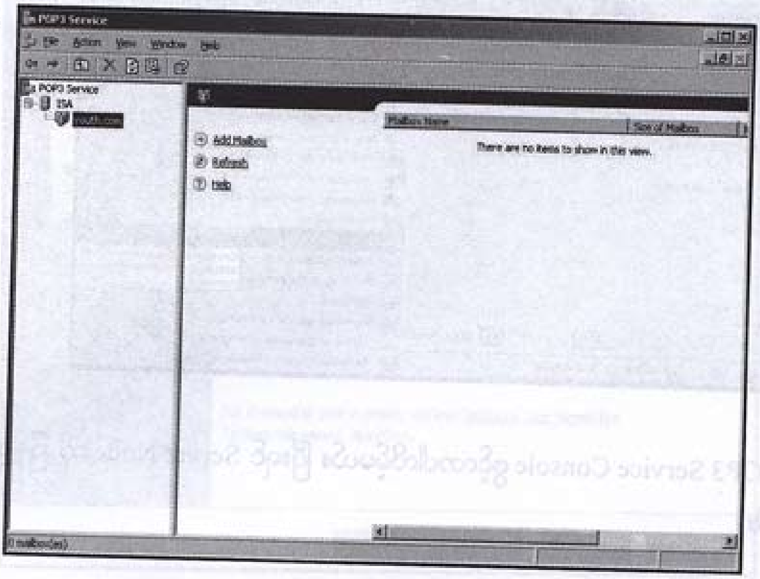
ဒါဆိုရင် POP3 Service Console ပွင့်လာပါလိမ့်မယ်။ ပြီးရင် Server Node ကို ဖြန့်ချလိုက်ပါ။ ပုံ ၈.၁၀ တွင်ကြည့်ပါ။

ပုံ ၈.၁၀



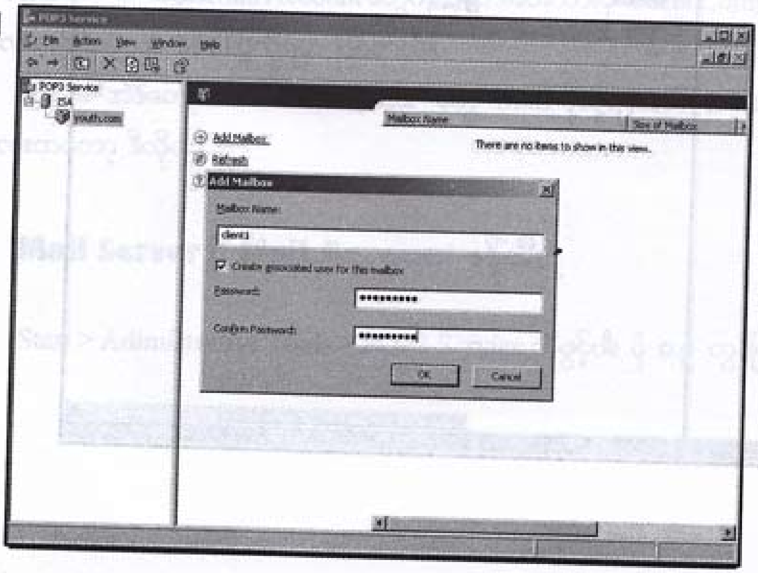
youth.com ဆိုတဲ့ Domain Name ကိုတွေ့ရပါလိမ့်မယ်။ ၎င်း Domain Name ပေါ်မှာ Select လုပ်ပါ။ ပြီးရင် Add Mail Box ကို Click လုပ်ပါ။ ပုံ ၈.၁၁ တွင်ကြည့်ပါ။

ပုံ ၈.၁၁



Add Mailbox ပေါ်လာပါလိမ့်မယ်။ Mail Box Name ကို Client1 လို့ပေးပြီးရင် Password ပေးပါ။ ပြီးရင် OK ကိုနှိပ်ပါ။ ပုံ ၈.၁၂ တွင်ကြည့်ပါ။

ပုံ ၈.၁၂

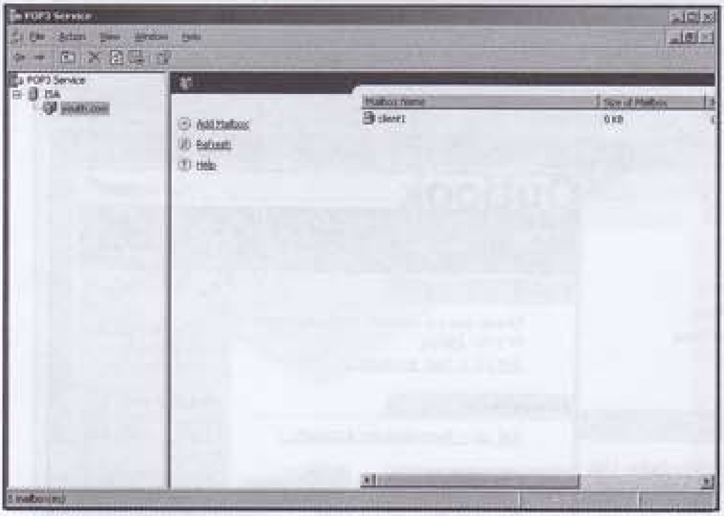


ထိုအခါ Mail Box Uses Successfully Added ဆိုတဲ့ Message ကိုတွေ့ရပါမယ်။ OK Button ကိုပဲနှိပ်ပါ။ ပုံ ၈.၁၃ တွင်ကြည့်ပါ။

ပုံ ၈.၁၃

ဒါဆိုရင် Client1 ဆိုတဲ့ Mail Account ကို Create လုပ်ပြီးပါပြီ။ ပုံ ၈.၁၄ တွင်ကြည့်ပါ။

ပုံ ၈.၁၄



မှတ်ချက်။ ။အထက်ပါအဆင့်အတိုင်းပဲ Client2 ဆိုတဲ့ Mail Account တစ်ခုထပ်ဖွဲ့ပေးပါ။ Mail အပြန်အလှန်ပို့ရန်အတွက်ဖြစ်သည်။

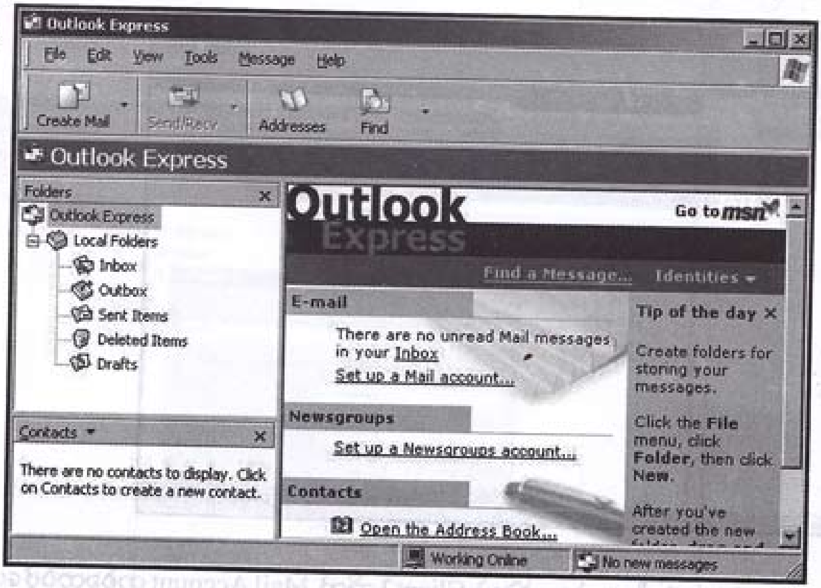
၈.၄ Client Computer များတွင် Mail Account Setting ထည့်ခြင်း

Client Computer များမှာ Mail Account Setting ထည့်ပေးရတာကတော့ Mail Server နဲ့ချိတ်ထားတဲ့ Client တွေ Email ပို့လို့ရဖို့ရန်အတွက်ပဲ ဖြစ်ပါတယ်။ ဘာကြောင့်လဲဆိုရင် Client Computer တွေသည် Email ပို့လို့ရဖို့ရန်အတွက် Email Setting သတ်မှတ်ထားမှ Computer တွေဟာ တစ်လုံးနဲ့တစ်လုံး အပြန်အလှန် Mail ပို့လို့ရမှာပဲ ဖြစ်ပါတယ်။ ကဲအခု — ကျွန်တော်က Client 1 မှာ Mail Account Setting ဘယ်လိုထည့်ပေးရမယ်ဆိုတာ ဖော်ပြပေးပါမယ်။

Client 1 Computer ကိုသွားပါ။ ပြီးရင် Start > Outlook Express ကိုဖွင့်ပါ။

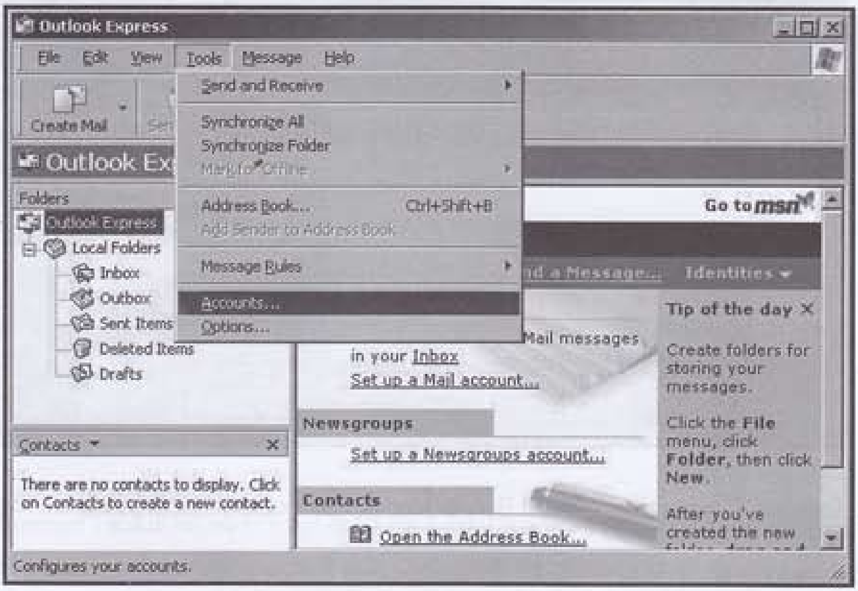
၎င်း Outlook Express Program သည် Mail Server နှင့် Network မိနေပါက ၎င်း Mail Server မှပေးတဲ့ Mail Service ကိုလက်ခံရန် အသုံးပြုရတဲ့ Program ဖြစ်ပါတယ်။ အခြား Email Service ကိုလက်ခံပေးတဲ့ Program များလည်း ရှိပါတယ်။ ဥပမာ – Outlook Express , Microsoft Outlook Express တို့ပဲဖြစ်ပါတယ်။ ကောင်းပြီ — အဲဆိုရင် အခု Outlook Express Program ထဲမှာ ဆက်လက်ပြီး လုပ်ရမှာကတော့ —– ပုံ ၈.၁၅ တွင်ကြည့်ပါ။

ပုံ ၈.၁၅



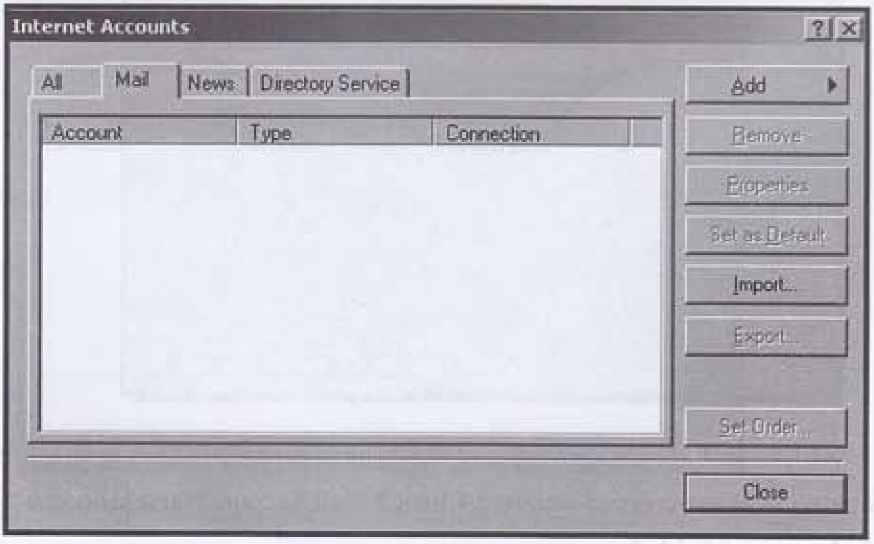
Outlook Express Program ထဲက Tools ကိုနှိပ်ပါ။ ပြီးရင် Accounts ကိုနှိပ်ပါ။ ပုံ ၈.၁၆ တွင်ကြည့်ပါ။

ပုံ ၈.၁၆



Internet Accounts Box ထဲက Mail Tab ကို Click လုပ်ပါ။ ပြီးရင် Add Button ကိုနှိပ်ပါ။ ပုံ ၈.၁၇ တွင်ကြည့်ပါ။

ပုံ ၈.၁၇

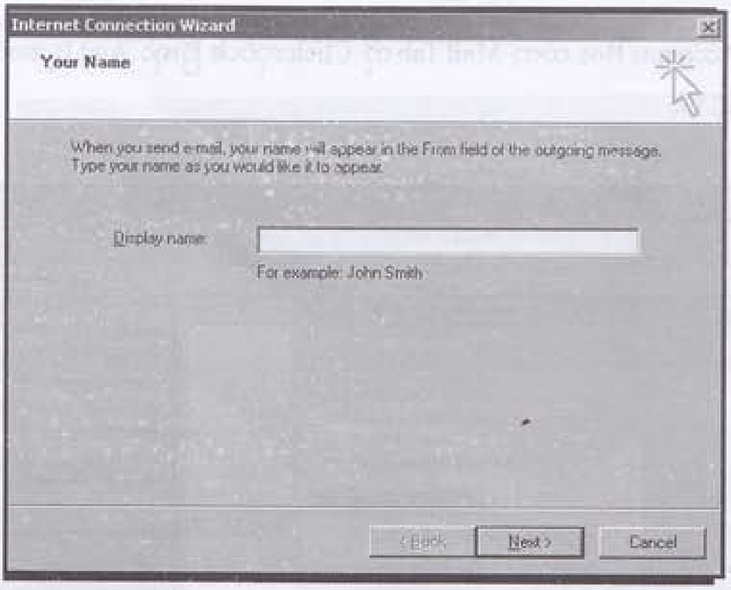


၄င်း Add Button ထဲက Mail Button ကိုနှိပ်ပါ။ ပုံ ၈.၁၈ တွင်ကြည့်ပါ။

ပုံ ၈.၁၈

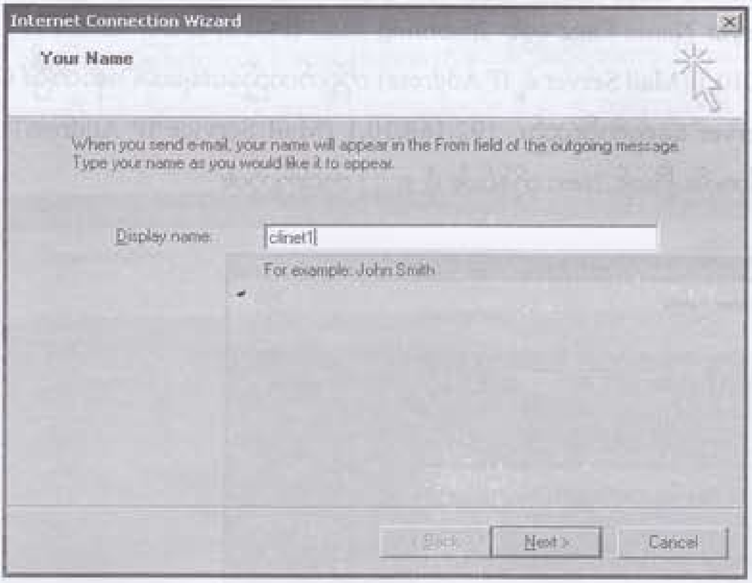
ဒါဆိုရင် Internet Connection Wizard Box ပေါ်လာပါမယ်။ ပုံ ၈.၁၉ တွင်ကြည့်ပါ။

ပုံ ၈.၁၉



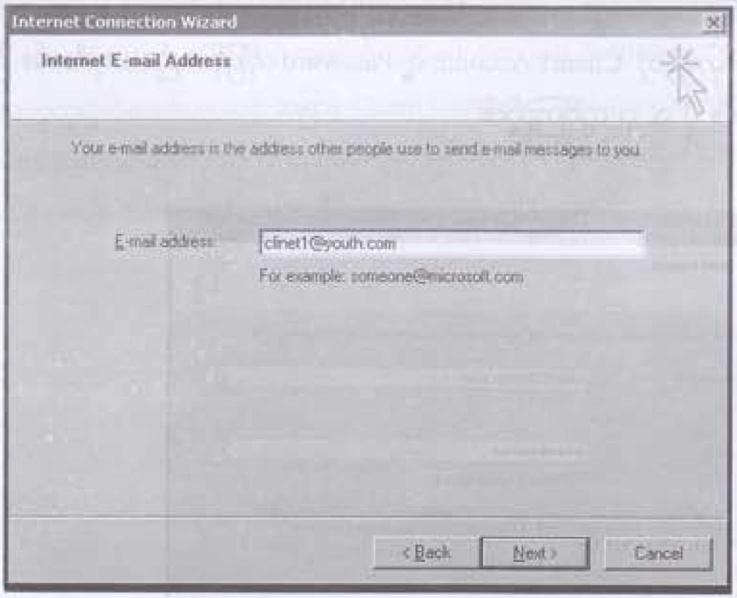
၄င်း Box ထဲက Your Name Page ထဲက Display Name နေရာတွင် Client 1 ကိုရိုက်ထည့်ပါ။ ၄င်း Name သည် Mail Server မှာ ဖွဲ့ထားတဲ့ Client 1 Mail Account Name ဖြစ်တယ်။ ပြီးရင် Next ကိုနှိပ်ပါ။ ပုံ ၈.၂၀ တွင်ကြည့်ပါ။

ပုံ ၈.၂၀



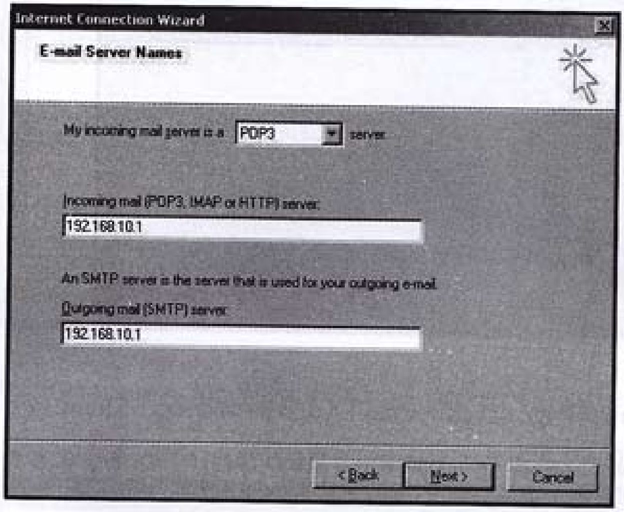
Internet Email Address Page ပေါ်မယ်။ Email Address နေရာတွင် Client 1@youth.com ဆိုပြီး မိမိရဲ့ Email Address အပြည့်အစုံကို ရိုက်ထည့်ပေးပါ။ ပြီးရင် Next ကိုနှိပ်ပါ။ ပုံ ၈.၂၁ တွင်ကြည့်ပါ။

ပုံ ၈.၂၁



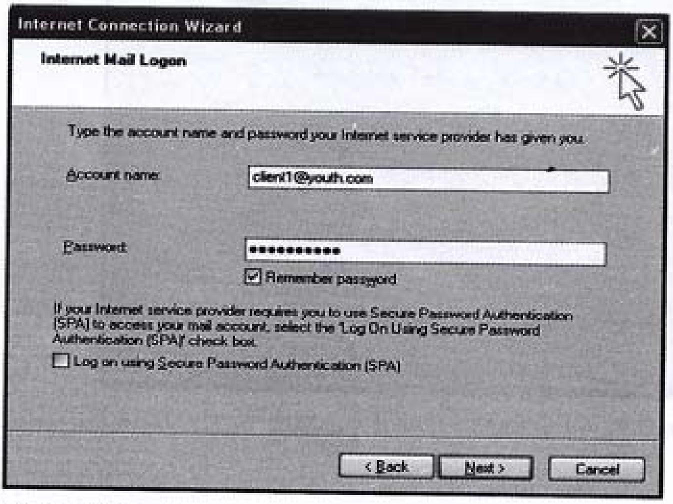
Email Server Name Page တွင် Incoming Mail (POP3, IMAP or HTTP) Server: နေရာတွင် 192.168.10.1 (Mail Server ရဲ့ IP Address) ကိုရိုက်ထည့်ပေးရမယ်။ နောက်ပြီး Outgoing Mail (SMTP) Server နေရာတွင်လည်း 192.168.10.1 (Mail Service IP Address) ကိုပဲရိုက်ထည့်ပေးရမှာ ဖြစ်ပါတယ်။ ပြီးရင် Next ကိုနှိပ်ပါ။ ပုံ ၈.၂၂ တွင်ကြည့်ပါ။

ပုံ ၈.၂၂



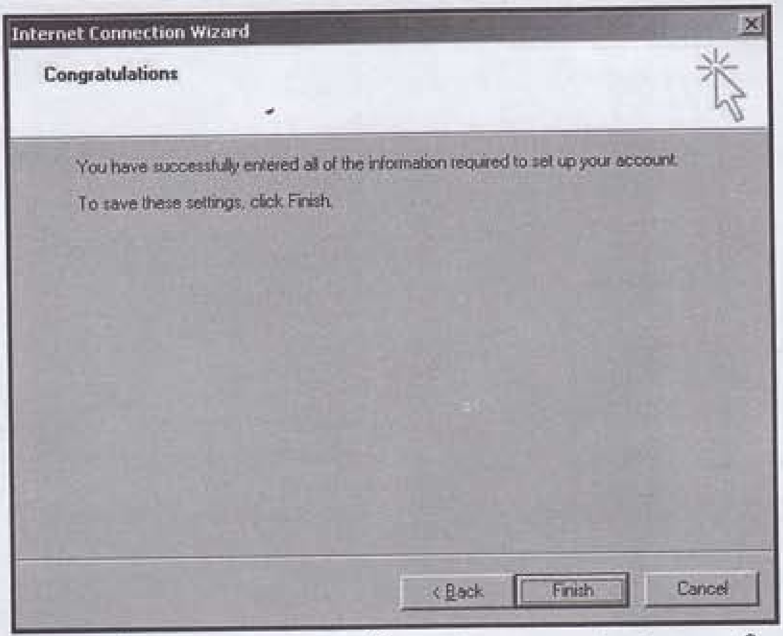
Internet Mail Logon တွင် Account Name: Client1@youth.com နှင့် Password နေရာတွင် မိမိရဲ့ Email Server မှာဖွင့်ခဲ့တဲ့ Client1 Account ရဲ့ Password ကိုပြန်ထည့်ပေးရပါမယ်။ ပြီးရင်တော့ Next Button ကိုနှိပ်ပါ။ ပုံ ၈.၂၃ တွင်ကြည့်ပါ။

ပုံ ၈.၂၃



Congratulations Page ပေါ်ပါမယ်။ ၄င်းသည်မိမိ Mail Account ကိုဖန်တီးတာ ပြည့်စုံသွားပြီ လို့ပြောတာ ဖြစ်ပါတယ်။ Finish Button ကိုနှိပ်ပါ။ ဒါဆိုရင်တော့ Email Account Setting ဖန်တီးတာပြီးသွားပြီ ဖြစ်လို့အောက်ပါပုံအတိုင်း တွေ့ရပါမယ်။ ပုံ ၈.၂၄ တွင်ကြည့်ပါ။

ပုံ ၈.၂၄



ကဲ အားလုံးပဲ -- Client 1 အတွက် Email Account Setting ချတတ်သွားပြီဆိုရင် မိမိနဲ့ Network အတူတူချိတ်ဆက်ထားတဲ့ အခြား Client Computer များမှာလည်း Mail Server ဖွဲ့ထားတဲ့ Mail Account Setting များကို လိုက်ထည့်ပေးရမှာ ဖြစ်ပါတယ်။ ပြီးရင်တော့ Computer တွေတစ်လုံးနဲ့ တစ်လုံး အပြန်အလှန် Email ပို့လို့ရသွားပါပြီ။

YOUTH Computer Co., Ltd.
Training & Multimedia Production

YOUTH COMPUTER CENTRE

6–A၊ ပန်းဆိုးတန်း Office Tower၊ ပန်းဆိုးတန်း(အလယ်)၊ကျောက်တံတား၊ဖုန်း-၂၃၄၈၉၃

Centre 3 - တိုက် (၂၉)၊ အခန်း (၁၀၄)၊ ဒလမ်း B Block၊ ၉၄ ရပ်ကွက်၊ သုဝဏ္ဏလမ်းပြင်မြို့တော်၊ ဖုန်း - ၀၁-၅၆၇၂၈၀

စစ်ကိုင်း - အင်းချပ်ရပ်၊ စစ်ကိုင်းမြို့။ ဖုန်း - ၀၇၂-၂၁၂၅၉၊ ၀၇၂ - ၂၁၉၆၂

လားရှိုး - ရပ်ကွက် - ၁၂၊ လားရှိုးလုံလမ်း၊ နယ်မြေ (၇)၊ လားရှိုးမြို့။

နာမည်ကျော် အဆိုတော်၊ တေးရေးဆရာ၊ အင်ဂျင်နီယာ၊ တက်သစ်အဆိုတော်နှင့်ဂီတကိုစိတ်ဝင်စားနေကြသူအပေါင်းတို့ တက်ရောက်ခဲ့ကြသော YOUTH Computer ၏

+ Digital Audio & Sound Effect Course,
+ Digital Audio Recording Course,
+ Music Production Course,
+ Digital Audio Editing Course,
+ Electro Dance & Hip Hop Course

များကိုတက်ရောက်ခြင်းဖြင့်အမှန်တကယ်တတ်မြောက်မှုကိုရယူပါ။ မြန်မာနိုင်ငံ၏ လူငယ်ထု အများစုအား ကွန်ပျူတာဖြင့်ဂီတဆက်စပ်ပေးခဲ့သည်။

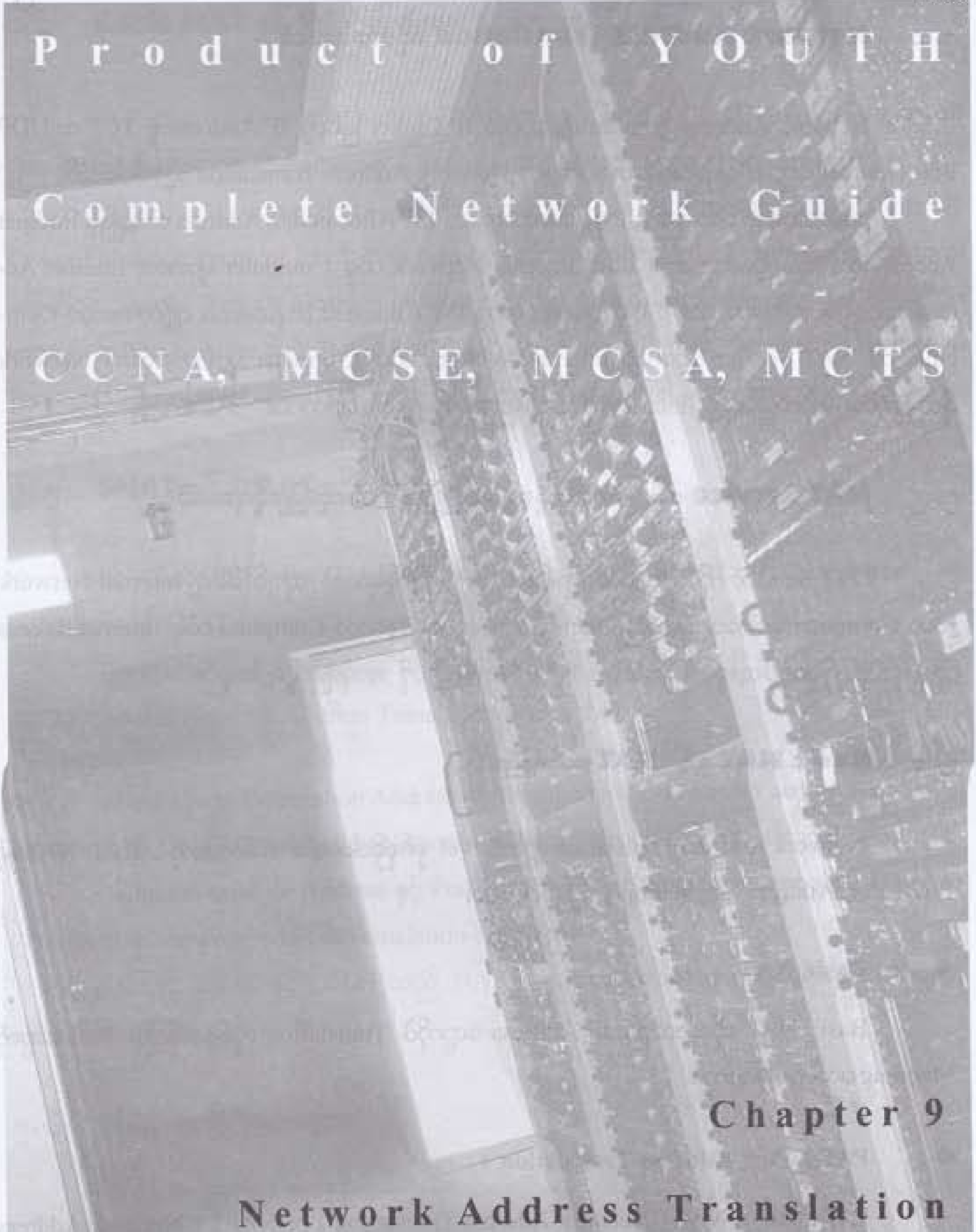
[illegible]

MYINT MOE AUNG
မြင့်မိုးအောင်

1. Digital Audio & Sound Effect (ကွန်ပျူတာဖြင့်ဂီတ သံစဉ်များဖန်တီး တတ်အောင်သင်ကြားပေးသည်။) Acid 6, Sound Forge 8, FL Studio 7, Single Track Recording စသည့်သင်ခန်းစာများပါဝင်သည်။
2. Electro Music (Hip Hop, Dance) (Hip Hop နှင့် Dance သီချင်းများဖန်တီးတတ်အောင်သင်ကြားသည်။) Acid 6, Sound Forge 8, FL Studio 7, Single Track Recording, Propellerhead Reason 2.0 စသည့်သင်ခန်းစာများပါဝင်သည်။
3. Music Production (More Music Theory) (ကွန်ပျူတာဖြင့် ဂီတသံစဉ်များဖန်တီးရာတွင် Music Arrangement များပါထည့်သွင်းသင်ကြားသည်။) Acid 6, Sound Forge 8, FL Studio 7, Single Track Recording, Propellerhead Reason 3.0, Pratical Project စသည့်သင်ခန်းစာများပါဝင်သည်။

Website: www.myanmarloops.com

Product of YOUTH



Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 9

Network Address Translation

၉. ၁ **Network Address Translation ဆိုတာဘာလဲ**

Network Address Translation ဆိုတာ IP Packet ဖြစ်တဲ့ IP Address နဲ့ TCP or UDP Port Number တွေကို ပြောင်းလဲပေးနိုင်တာကို Network Address Translation လို့ခေါ်ပါတယ်။

ဥပမာအားဖြင့် မိမိသည် ISP မှချပေးထားသော ISP Allocated IP Address တစ်ခုဖြင့် Internet Access ကိုလက်ခံခွင့်ရသောအခါ မိမိရဲ့ Internal Network ထဲမှ Computer များအား Internet Access လုပ်ခွင့်ပေးချင်ပါက ၄င်း ISP မှ ချပေးထားတဲ့ ISP Allocated IP Address ရရှိထားသော Computer ကို NAT Service ဖွင့်ပေးပြီးInternal Network ထဲမှ Computer များအားလုံးကို Network ချိတ်ဆက်ပေးလိုက်ခြင်းဖြင့် Internet ကို အသုံးပြုခွင့် ကိုရရှိမှာဖြစ်ပါတယ်။

၉. ၂ **NAT Service ကို ဘယ်လိုနေရာမျိုးမှာ အသုံးပြုလို့ရသလဲ**

NAT Service ကို ဘယ်လိုနေရာမျိုးမှာ အသုံးပြုလို့ရသလဲ ဆိုရင် မိမိရဲ့ Internal Network ထဲမှာ Computer များအားလုံးသည် Internet Access ရရှိနေသော Computer ထဲမှ Internet Access ကို ပြန်လည်၍မျှဝေခံစားခွင့် ရရှိချင်ပါက NAT Services ကို အသုံးပြုလို့ရပါသည်။

၉. ၃ **Basic NAT နှင့် PAT အကြောင်း**

Network Address Translation တွင် Level နှစ်ခုရှိပါတယ်။ အဲဒါကတော့ - Basic NAT နှင့် PAT (Port Address Translation) တို့ဖြစ်ပါတယ်။

❖ **Basic NAT**

Basic NAT ဆိုတာသည် IP Address တွေကိုပဲ Translation လုပ်ပေးနိုင်ပြီး Port တွေကို Mapping မလုပ်ပေးနိုင်ပါဘူး။

❖ **PAT (Port Address Translation)**

PAT ကိုတော့ NAT (Network Address Translation) or NAPT (Network Address Port Translation) လို့လဲ ခေါ်ကြပါတယ်။ ၄င်းသည် IP Address နှင့် Port Number နှစ်ခုလုံးကို Translation လုပ်ပေးနိုင်ပါတယ်။

၉.၄ Basic NAT နှင့် PAT တို့ Level ကွဲသွားရခြင်းအကြောင်း

IP Packet တွေအားလုံးမှာ Source IP Address နှင့် Destination IP Address တွေကိုယ်စီရှိကြပါတယ်။ ဒါကြောင့် ၎င်း IP Address နှင့် Destination IP Address တွေကို Translate လုပ်လို့ရပါတယ်။ သို့သော် အချို့ IP Packet တွေမှာ Port Number မရှိကြပါဘူး။ ဥပမာအားဖြင့်ပြောရရင် ICMP (Internet Control Message Protocol) သည် Port Number မရှိပါဘူး။ အဲဒီလို Port Number မရှိတဲ့ Protocol တွေဆိုရင် Source Port နှင့် Destination Port Number တွေကို Translate လုပ်ပေးဖို့ မလိုပါဘူး။ အကယ် ၍ Port Number ရှိတဲ့ Protocol တွေဆိုရင်တော့ Source Port နှင့် Destination Port Number တွေကို Translate လုပ်ပေးရမှာဖြစ်ပါတယ်။ ဒါကြောင့် NAT မှာ Level နှစ်မျိုး ကွဲသွားရခြင်းဖြစ်ပါတယ်။

၉.၅ SNAT နှင့် DNAT ဆိုတာဘာလဲ

❖ SNAT ဆိုတာ Source IP Address နှင့် Source Port Number တွေကို Translation လုပ်ပေးတာကို SNAT (Source Network Address Translation) လို့ ခေါ်တယ်။

Computer များရဲ့ IP Address နှင့် Port Number များကို မူလပုံစံသို့ ပြောင်းလဲပေးတာသည် SNAT (Source Network Address Translation) ဖြစ်သည်။

❖ DNAT ဆိုတာ Destination Address နှင့် Destination Port Number တွေကို Translation လုပ်ပေးတာကို DNAT (Destination Network Address Translation) လို့ ခေါ်တယ်။

Computer များရဲ့ IP Address နှင့် Port Number များကို လမ်းညွှန်ပေးတာသည် DNAT (Destination Network Address Translation) ဖြစ်သည်။

ဒါကြောင့် SNAT နှင့် DNAT သည် NAT Service ကိုလုပ်ဆောင်တဲ့ နေရာမှာ တပြိုင်နက် လုပ်ဆောင်ပေးကြပါတယ်။

၉.၆ NAT အမျိုးအစားများ

NAT အမျိုးအစား လေးမျိုးရှိပါတယ်။

❖ Full Cone NAT
❖ Restricted Cone NAT

- Port Restricted Cone NAT
- Symmetric NAT တို့ ဖြစ်ပါတယ်။

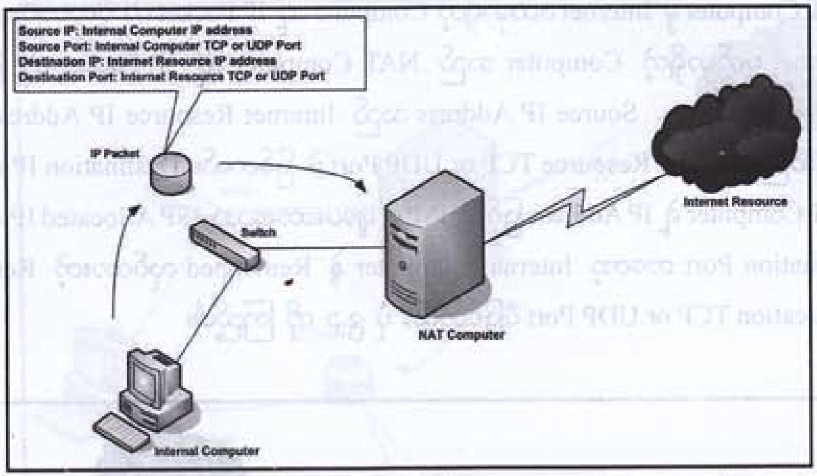
၉.၇ Network Address Translation or NAPT ဘယ်လိုအလုပ်လုပ်သလဲ

ကျွန်တော်တို့က Internet Access ရရှိနေတဲ့ Computer မှာ NAT Service ကို ဖွင့်ပေးလိုက်ပြီး မိမိရဲ့ Private LAN ထဲမှာရှိတဲ့ Computer များက ၎င်း NAT Service ဖွင့်ထားတဲ့ Computer နဲ့ ချိတ်လိုက်တဲ့အခါမှာ Private LAN ထဲမှာရှိတဲ့ Computer များအားလုံး Internet Access တော့ရသွားတာမှန်တယ်။ ဒါပေမယ့် NAT Service ကဘယ်လိုအလုပ်လုပ်ပြီး Internet Access ကို ရသွားလဲဆိုတာက စဉ်းစားစရာတစ်ခုပဲပေါ့။ အဲဒီတော့ ကျွန်တော်က NAT Service ဘယ်လို အလုပ်လုပ်တယ်ဆိုတာကို ရှင်းပြပါ့မယ်။

NAT အလုပ်လုပ်တဲ့ပုံစံကတော့ ကျွန်တော်တို့ရဲ့ Internal Network သည် Internet Resource နဲ့ချိတ်ဆက်မယ်။ အဲဒီအခါမှာ ကျွန်တော်တို့ Internal Network ထဲမှာ ရှိတဲ့ Computer တစ်လုံးမှ IP Packet ဖြစ်တဲ့ IP Address နှင့် TCP or UDP Port ကို ဖန်တီးပြီး Internet Access ကိုလက်ခံထားတဲ့ NAT Service ဖွင့်ထားသော Computer ဆီသို့ IP Packet ကိုပို့လွှတ်လိုက်တယ်။ အဲဒီလို ပို့လွှတ်တဲ့အခါမှာ Source IP Address ကတော့ ကျွန်တော်တို့ Internal ထဲကIP Packet ကို ပို့လွှတ်တဲ့ Computer ရဲ့ IP Address ဖြစ်ပြီး Source Port ကတော့ ၎င်း Computer မှ ပို့လွှတ်တဲ့ Source Application ရဲ့ TCP or UDP Port အတိုင်းပဲဖြစ်တယ်။

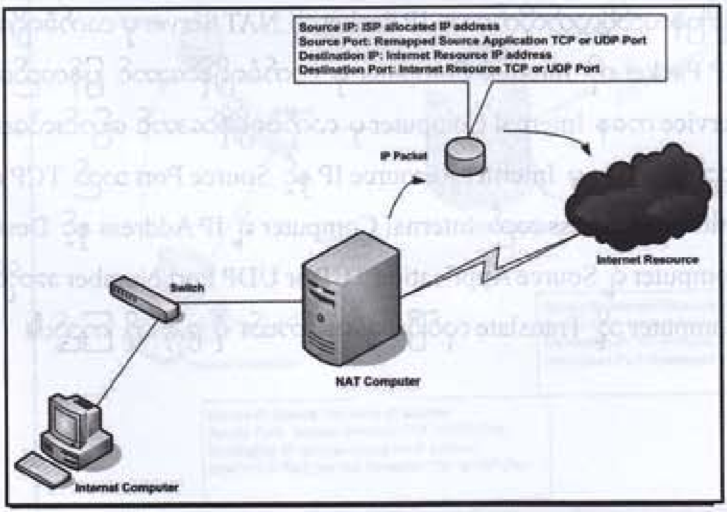
ကျွန်တော်ဆိုလိုချင်တာက Source IP Address နှင့် Source TCP or UDP Port သည် Internal ထဲမှာ ရှိတဲ့ Computer တစ်လုံးမှ NAT Source ဖွင့်ထားသော Computer ဆီသို့ ဆိုလိုတာဖြစ်တယ်။ အဲဒီတော့ IP Packet တွေသည် Data ကိုပို့တဲ့ နေရာမှာ Source နဲ့ Destination နှစ်မျိုးတွဲပို့ရတယ်လေ။ Destination ဆိုတာကတော့ Source Address ကို ဘယ်သို့ ရောက်အောင်ပို့မယ်ဆိုတဲ့နေရာကို Destination လို့ခေါ်တာပေါ့။ အဲဒီတော့ Source IP Address ပို့ချင်တဲ့နေရာက Destination ဖြစ်တဲ့ Internet Resource ဆီကို ပို့ချင်တယ်။ ဒီတော့ Destination IP Address သည် Internet Resource ရဲ့ ICP or UDP Port ပဲ ဖြစ်သွားတာပေါ့။ ပုံ ၉.၁ ကိုကြည့်ပါ။

ပုံ ၉.၁



Internal ထဲက Computer မှ ပို့လွှတ်လိုက်တဲ့ IP Packet သည် NAT ဖွင့်ထားသော Computer ဆီသို့ ရောက်လာတဲ့အခါမှာ NAT Service သည် Internet ဖက်ကိုထွက်မယ့် IP Packet ကို ပြောင်းလဲပေးရပါတယ်။ NAT Servic က Internet ဖက်ကို ထွက်မယ့် IP Packet ကို ပြောင်းလဲပေးတဲ့ ပုံစံသည် Source IP Address ကို ISP ကချပေးထားတဲ့ ISP Allocated IP Address နှင့် Source Port ကိုတော့ Internal Computer ရဲ့ Source Application TCP or UDP Port နဲ့ Remapped လုပ်ထားတယ်။ Destination IP Address သည် Internal Resource ရဲ့ IP Address ဖြစ်ပြီး Destination Port ကတော့ Internet Resource ရဲ့ TCP or UDP Port နဲ့ပဲ Internet ဖက်သို့ IP Packet ကို ပို့လွှတ်လိုက်ပါတယ်။ ပုံ ၉.၂ ကို ကြည့်ပါ။

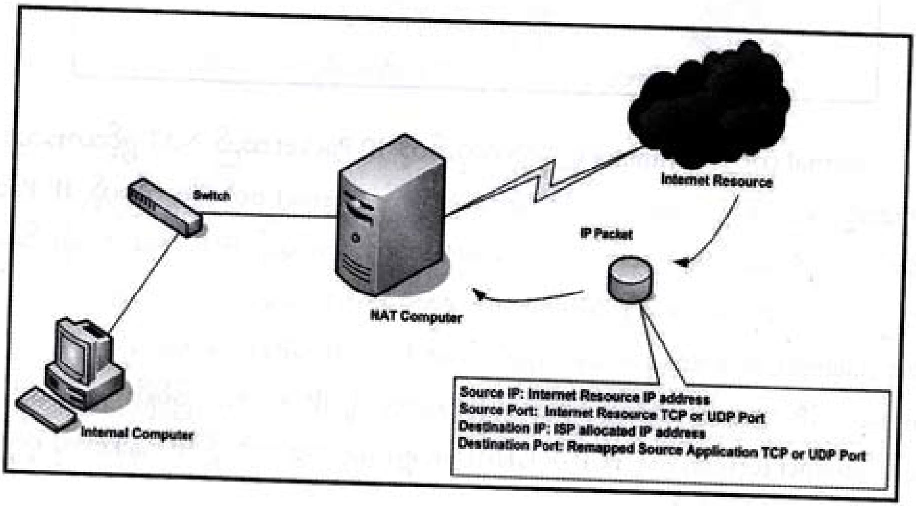
ပုံ ၉.၂



NAT Computer မှ Internet ဖက်မှာရှိတဲ့ Computer သို့ IP Packet ကို ပို့လွှတ်ပြီးတဲ့အခါမှာ

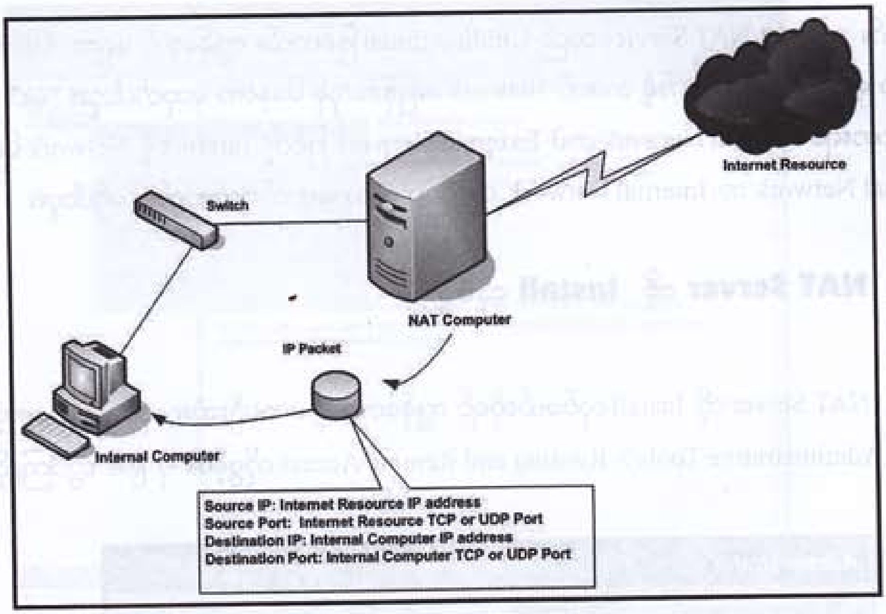
Internet ဖက်မှာရှိတဲ့ Computer သည် NAT Computer သို့ IP Packet ကို ပြန်လည် ပို့လွှတ်ပေးတဲ့ ပုံစံကတော့ - Source IP Address သည် Internet Resource IP Address ဖြစ်ပြီး Source Port သည် Internet Resource TCP or UDP Port ပဲ ဖြစ်တယ်။ Destination IP Address ကတော့ NAT Computer ရဲ့ IP Address ဖြစ်တဲ့ ISP မှ ချပေးထားသော ISP Allocated IP Address ဖြစ်ပြီး Destination Port ကတော့ Internal Computer နဲ့ Remapped လုပ်ထားတဲ့ Remapped Source Application TCP or UDP Port ပဲဖြစ်တယ်။ ပုံ ၉.၃ ကို ကြည့်ပါ။

ပုံ ၉.၃

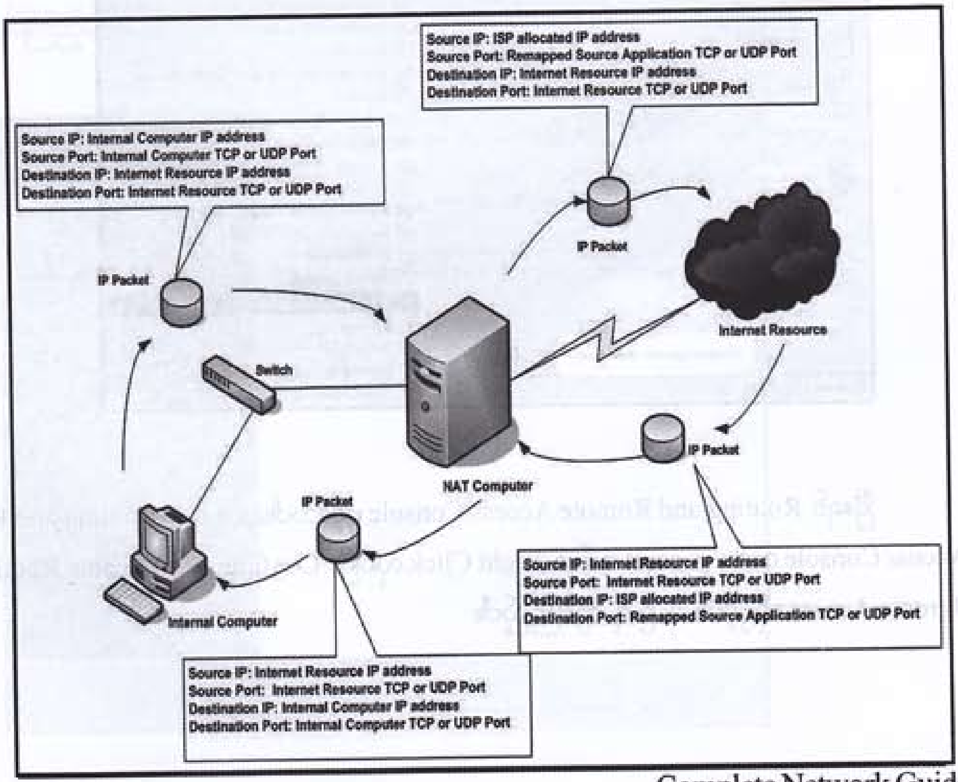


Internal ဖက်မှ ပြန်လည်ပို့လွှတ်လိုက်သော IP Packet ကို NAT Server မှ လက်ခံရရှိသောအခါ NAT Service သည် IP Packet ကို Internal Computer မှ လက်ခံရရှိနိုင်အောင် ပြန်လည်ပြောင်းလဲပေးရပါတယ်။ NAT Service ကနေ Internal Computer မှ လက်ခံရရှိနိုင်အောင် ပြောင်းလဲပေးတဲ့ ပုံစံ Source IP Address သည် Internet မှ Internet Resource IP နှင့် Source Port သည် TCP or UDP Port ပဲဖြစ်ပြီး Destination IP Address သည် Internal Computer ရဲ့ IP Address နှင့် Destination Port သည် Internal Computer ရဲ့ Source Application TCP or UDP Port Number အတိုင်း NAT Service မှ Internal Computer သို့ Translate လုပ်ပြီး ချပေးပါတယ်။ ပုံ ၉.၄ ကို ကြည့်ပါ။

ပုံ ၉.၄


Internet Resource
Switch
NAT Computer
IP Packet
Internal Computer
Source IP: Internet Resource IP address
Source Port: Internet Resource TCP or UDP Port
Destination IP: Internal Computer IP address
Destination Port: Internal Computer TCP or UDP Port

ပုံ ၉.၅

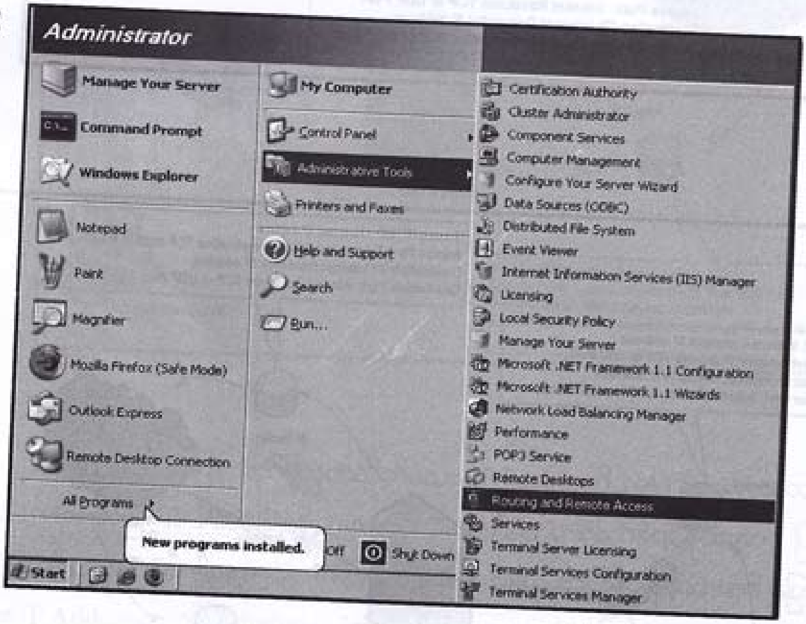

Source IP: ISP allocated IP address
Source Port: Remapped Source Application TCP or UDP Port
Destination IP: Internet Resource IP address
Destination Port: Internet Resource TCP or UDP Port
Source IP: Internal Computer IP address
Source Port: Internal Computer TCP or UDP Port
Destination IP: Internet Resource IP address
Destination Port: Internet Resource TCP or UDP Port
IP Packet
IP Packet
Internet Resource
Switch
IP Packet
NAT Computer
IP Packet
Internal Computer
Source IP: Internet Resource IP address
Source Port: Internet Resource TCP or UDP Port
Destination IP: ISP allocated IP address
Destination Port: Remapped Source Application TCP or UDP Port
Source IP: Internet Resource IP address
Source Port: Internet Resource TCP or UDP Port
Destination IP: Internal Computer IP address
Destination Port: Internal Computer TCP or UDP Port

မှတ်ချက်။ ။ NAT Service သည် Unidirectional ဖြစ်တယ်။ ကျွန်တော် ရှေ့က Routing Process မှာ ရှင်းပြခဲ့သလို တဖက်နဲ့ တဖက် Network အပြန်အလှန် မိနေတာ မဟုတ်ပါဘူး။ NAT Service ကို ဖွင့်ထားရင် Internal Network ကပဲ External Network ဖြစ်တဲ့ Internet နဲ့ Network မိမှာဖြစ်ပြီး External Network က Internal Network ထဲကိုတော့ လာရောက်ချိတ်ဆက်ခွင့်မရှိပါဘူး။

၉.၈ NAT Server ကို Install လုပ်ပုံ

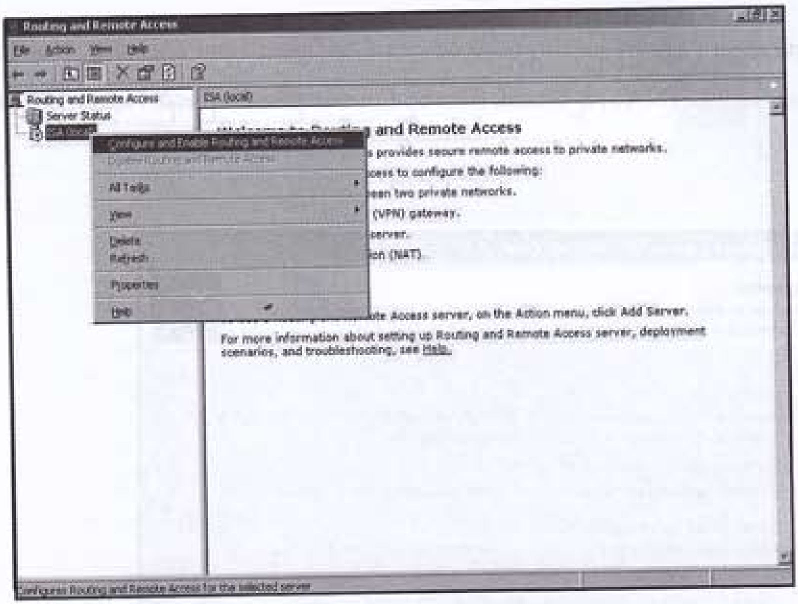
NAT Server ကို Install လုပ်မယ်ဆိုရင် ကျွန်တော်တို့ ပထမဦးဆုံးစလုပ်ရမှာကတော့ - Start > Administrative Tools > Routing and Remote Access ကိုဖွင့်ပါ။ ပုံ ၉.၆ တွင်ကြည့်ပါ။

ပုံ ၉.၆



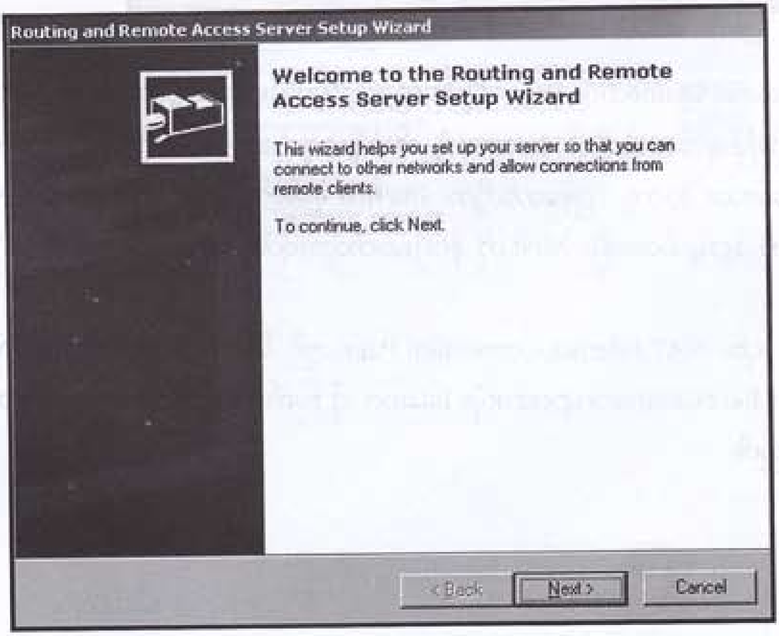
ပြီးရင် Routing and Romote Access Console ပွင့်လာပါမယ်။ ၎င်း Routing and Remote Access Console ထဲက (Local) ပေါ်မှာ Right Click လုပ်ပြီး Configure and Enable Routing and Remote Access ကိုဖွင့်ပါ။ ပုံ ၉.၇ တွင်ကြည့်ပါ။

ပုံ ၉.၇



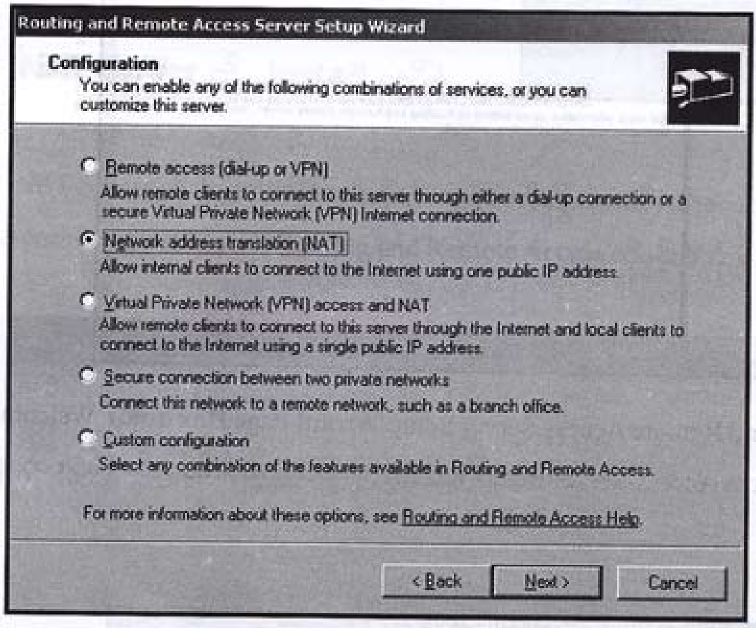
Routing and Remote Access Server Setup Wizard Page Box ပေါ်ပြီး Welcome to the Routing and Remote Access Server Setup Wizard ကို မြင်တွေ့ရပါလိမ့်မယ်။ Next ကို နှိပ်ပါ။ ပုံ ၉.၈ တွင်ကြည့်ပါ။

ပုံ ၉.၈



Configuration Page ကို မြင်တွေ့ရပါမယ်။ ၎င်း Configuration Page ထဲက Network Address Translation Service (NAT) ရဲ့ Check Box ကို On ပေးရပါမယ်။ ပြီးရင် Next ကိုနှိပ်ပါ။ ပုံ ၉.၉ တွင်ကြည့်ပါ။

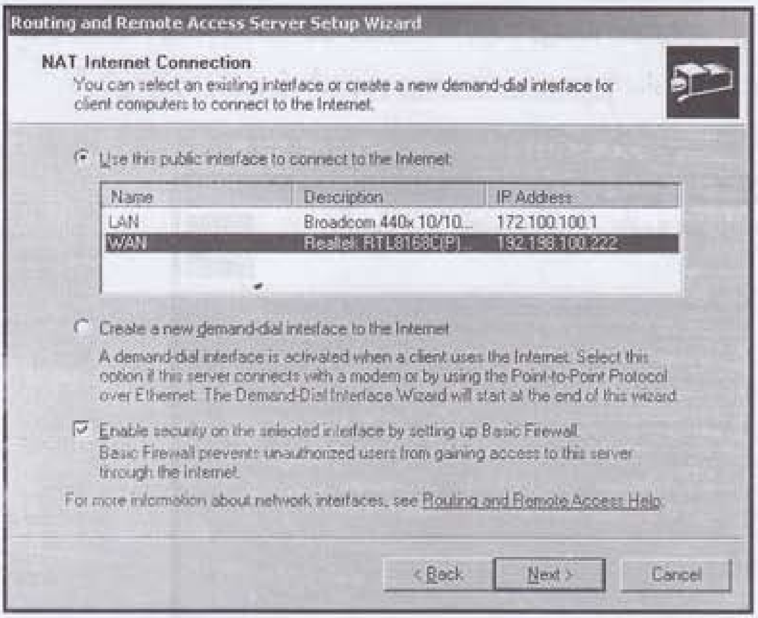
ပုံ ၉.၉



NAT Internet Connection Page ကိုမြင်တွေ့ရပါလိမ့်မယ်။ ဒီအဆင့်က အရေးကြီးတယ်နော်။ ဒီအဆင့်က ဘာကိုပြောချင်တာလဲဆိုရင် Internet နဲ့ တိုက်ရိုက်ချိတ်ဆက်ထားတဲ့ Network Interface Card ကိုရွေးခိုင်းနေတာ။ ဒီတော့ ကျွန်တော်တို့က Internet နဲ့တိုက်ရိုက်ချိတ်ဆက်ထားတဲ့ Network Interface Card ကို ရွေးချယ်ထားပြီး Next ကို နှိပ်ပြီးဆက်သွားရပါမယ်။

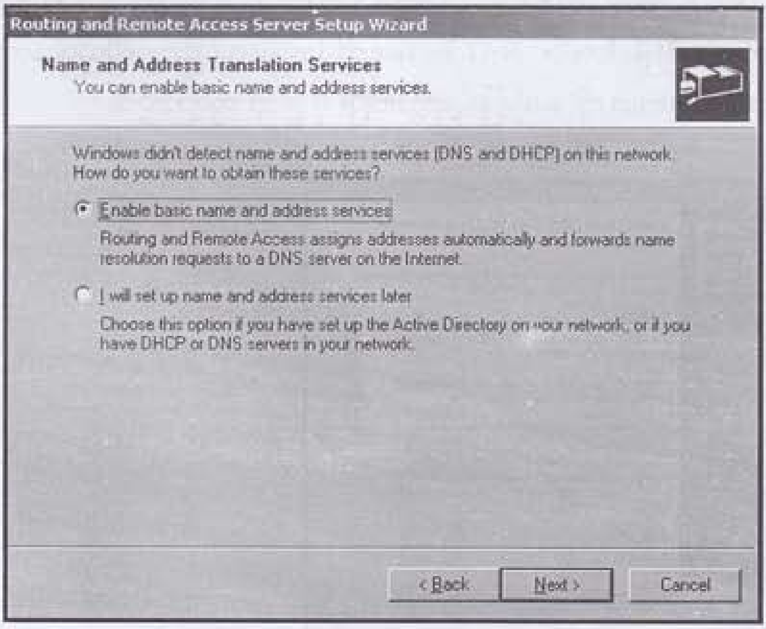
မှတ်ချက်။ ။၎င်း NAT Internet Connection Page တွင် မိမိရွေးချယ်ပေးလိုက်တဲ့ Network Card မှားသွားရင် Client Computer များအားလုံး Internet ကို လက်ခံအသုံးပြုလို့ရမှာမဟုတ်တော့ပါဘူး။ ပုံ ၉.၁၀ တွင် ကြည့်ပါ။

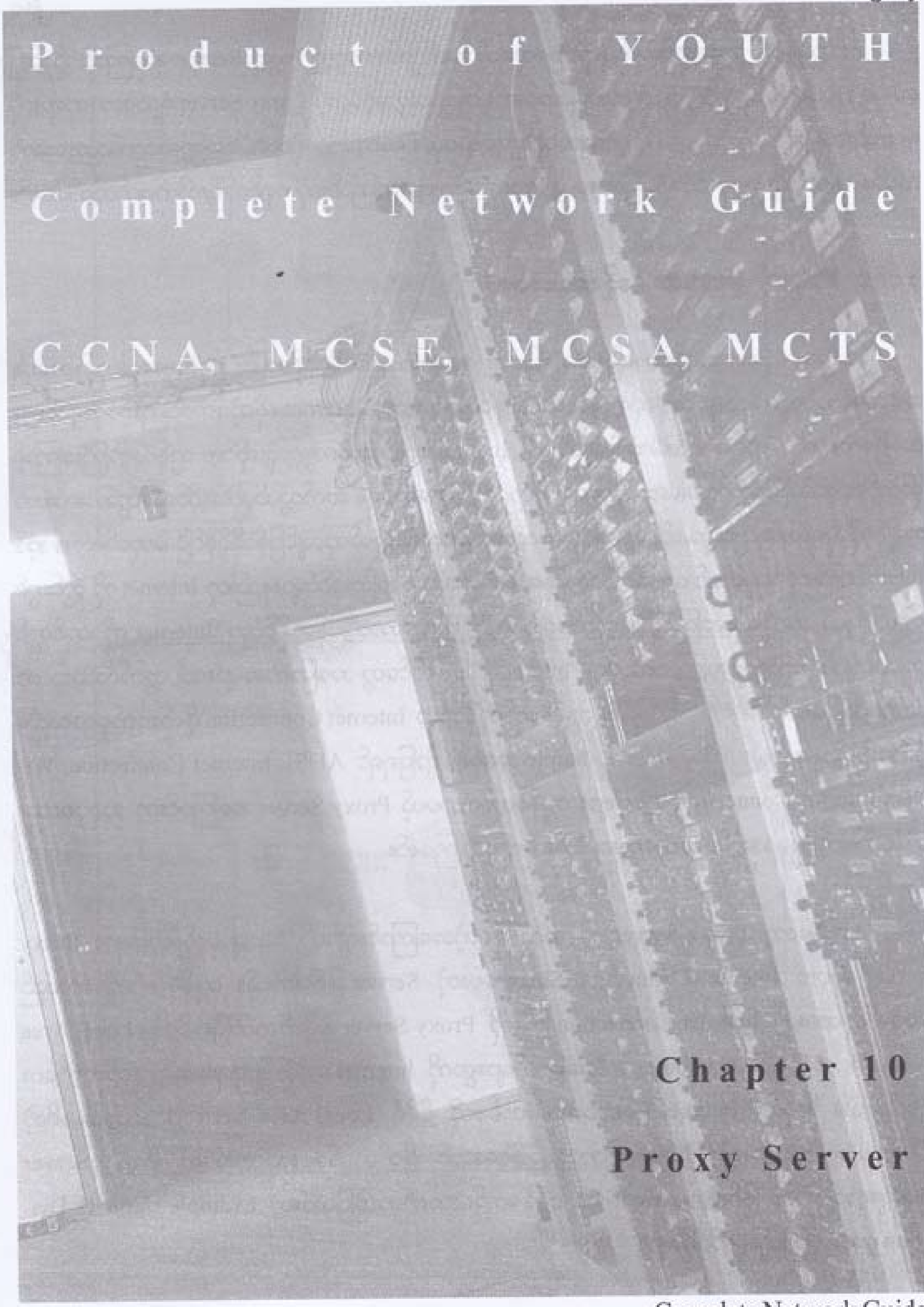
ပုံ ၉.၁၀



Name and Address Translation Services Page ပေါ်မယ်။ အဲဒီနေရာမှာ Enable Basic Name and Address Services Check Box ကိုပဲ On ပြီးဆက်သွားရပါမယ်။ Next ကိုနှိပ်ပါ။ ပုံ ၉.၁၁ တွင်ကြည့်ပါ။

ပုံ ၉.၁၁





Product of YOUTH

Complete Network Guide

CCNA, MCSE, MCSA, MCTS

Chapter 10

Proxy Server

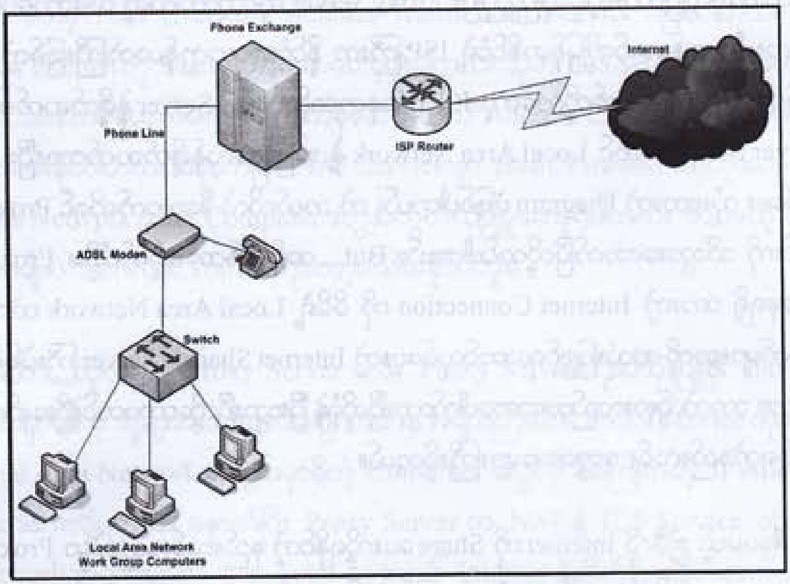
ကျွန်တော် အခုဆက်လက်ပြီးရှင်းပြပေးမယ့် အကြောင်းကတော့ Proxy Server အကြောင်းကိုရှင်းပြပေးမှာ ဖြစ်ပါတယ်။ Proxy Server အကြောင်းကိုရှင်းပြပေးမှာဆိုတော့ Proxy Server ရဲ့သဘောတရားကို ပထမဦးဆုံး နားလည်သဘောပေါက်အောင်ရှင်းပြမယ်နော်။ ကဲကဲ– အာရုံတစ်ပါးအခြားမထွက်သွားအောင် သတိလေးကပ်ပြီး ကျွန်တော်ရှင်းပြပေးမယ့် Proxy Server အကြောင်းကို ဂရုစိုက်ပြီးလိုက်ဖတ်လိုက်ပါနော်။

၁၀.၁ **Proxy Server** ဆိုတာဘာလဲ

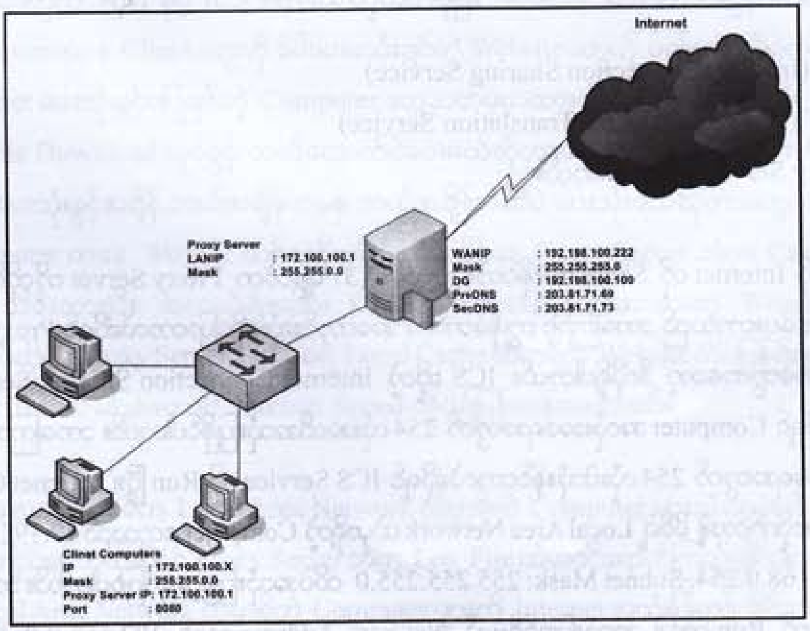
Proxy Server ကိုဝတင်ပြီးအသုံးပြုရတဲ့ အကြောင်းက ဒီလိုရှိတယ်။ ဟိုးရှေးရှေးတုန်းကပေါ့။ အဲလေယောင်လို့။ ဒီလိုဗျ။ အခုဆိုကျွန်တော်တို့ နိုင်ငံအနှံ့အပြား Internet ဆိုတဲ့ကောင်ကြီးက ခေတ်စားလာပြီလေ။ အဲ့ဒီ "အိုင်အန်တီအီးအာအန်အီးတီ" Internet ဆိုတဲ့ တစ်ကမ္ဘာလုံးဆိုင်ရာ ကွန်ယက်ကြီးကြောင့် နိုင်ငံတိုင်း၊ နိုင်ငံတိုင်းမှာ စီးပွားရေး၊ လူမှုရေး၊ ပညာရေး၊ ကျန်းမာရေး၊ ဆက်သွယ်မှုပိုင်းဆိုင်ရာတွေအားလုံးဟာ အချိန်တိုတိုလေးအတွင်းမှာ ထိုင်ရာကနေ ထသွားစရာမလိုပဲ လွယ်ကူလျင်မြန်သိရှိနိုင်ပြီ မဟုတ်လား။ အဲ့ဒီ Internet ကြီးကို အခုဆိုရင် ကျွန်တော်တို့ မြန်မာနိုင်ငံမှာလည်း အခြားနိုင်ငံများနည်းတူ Internet ကို တွင်တွင်ကျယ်ကျယ် အသုံးပြုလာကြပါပြီ။ ဘယ်လောက်ထိ ကျွန်တော်တို့မြန်မာနိုင်ငံမှာ Internet ကို တွင်တွင်ကျယ်ကျယ် အသုံးပြုလာကြသလဲဆိုရင် Internet Cafe ဆိုင်တွေ အမြောက်အများပေါ် ထွက်လာတာ ကသက်သေပြနေပါတယ်။ ကဲ အဲ့ဒီတော့ ကျွန်တော်တို့နိုင်ငံမှာ Internet Connection ချိတ်ဆက်မှုကလည်း ပုံစံအမျိုးမျိုးနှင့် ပေါ်ထွက်လာပါပြီ။ Example အနေနဲ့ပြောပြရရင် ADSL Internet Connection, Wi-Max Internet Connection တို့ပေါ့ဗျာ။ ကျွန်တော်ပြောမယ့် Proxy Server အကြောင်းက အခုမှစတာ။ ကဲဆက်ဖတ်ကြရအောင်။ သတိလေးကပ်ပြီးလိုက်ဖတ်ကြနော်။

ကဲဒီတော့ Proxy Server ကို အသုံးပြုရတဲ့အကြောင်းရင်းကို သေချာမှတ်ထားနော်။ Proxy Server ဆိုတာ Internet Connection Share ပေးတဲ့ Server ဖြစ်ပါတယ်။ ကျွန်တော်တို့တွေသည် မိမိဝယ်ယူထားတဲ့ Internet Connection ကြီးကို Proxy Server နဲ့ချိတ်ဆက်ပြီး မိမိရဲ့ Local Area Network ထဲမှာရှိတဲ့ Computer ပေါင်းမြောက်များစွာကို Internet အသုံးပြုလို့ရအောင် ချိတ်ဆက်ပေးနိုင်ပါတယ်။ ဒီလိုမျိုး Internet Connection တစ်ခုကို မိမိရဲ့ Local Area Network အတွင်းမှာရှိတဲ့ Computer များအားလုံး Internet အသုံးပြုနိုင်အောင် ချိတ်ဆက်ပေးလိုက်တာက Proxy Server ရဲ့ကျေးဇူးကြောင့်ပဲ ဖြစ်ပါတယ်။ ကဲကဲ.... ကျွန်တော်အောက်မှာဆွဲပြထားတဲ့ Example Network Diagram လေးကိုကြည့်လိုက်ပါဦးဗျာ။

ပုံ ၁၀.၁


Phone Exchange
Internet
Phone Line
ISP Router
ADSL Modem
Switch
Local Area Network
Work Group Computers

ပုံ ၁၀.၂


Internet
Proxy Server
LANIP : 172.100.100.1
Mask : 255.255.0.0
WANIP : 192.198.100.222
Mask : 255.255.255.0
DG : 192.198.100.100
PreDNS : 203.81.71.69
SecDNS : 203.81.71.73
Clinet Computers
IP : 172.100.100.X
Mask : 255.255.0.0
Proxy Server IP: 172.100.100.1
Port : 8080

ကျွန်တော်အခုဆွဲပြထားတဲ့ပုံကိုကြည့်ပြီး Proxy Server ဆိုတာဘာလဲလို့ သဘောပေါက်သွားပြီလား။ ရှင်းရှင်းလေးပါ။ ကျွန်တော်တို့မြန်မာနိုင်ငံရဲ့ ISP ကြီးက နိုင်ငံတကာကွန်ယက်ကြီးဖြစ်တဲ့ Internet ကြီးနဲ့ ချိတ်ဆက်ပါတယ်။ ကျွန်တော်တို့ကတော့ ISP ကနေတဆင့် Proxy Server နဲ့ချိတ်ဆက်ထားတယ်။ ၎င်း Proxy Server ကနေတစ်ဆင့် Local Area Network နဲ့ အပြန်အလှန်ချိတ်ဆက်ထားပြီး Internet Connection ကိုပေး သုံးထားတဲ့ Diagram ပဲဖြစ်ပါတယ်။ ကဲ ဘယ်လိုလဲ ဒီလောက်ဆိုရင် Proxy Server ကြီးရဲ့ အကြောင်းကို သိသွားလောက်ပြီလို့ထင်ပါတယ်။ But....ထပ်မှတ်ထားလိုက်ပါဦး။ Proxy Server ဆိုတာ ISP ကနေရရှိ ထားတဲ့ Internet Connection ကို မိမိရဲ့ Local Area Network ထဲက Computer ပေါင်းမြောက်များစွာကို အသုံးပြုခွင့်ရအောင်လုပ်ပေးတဲ့ Internet Sharing Server ကြီးပဲဖြစ်ပါတယ်။ Proxy Server ဟာ ဘာလဲလို့နားလည်သဘောပေါက်သွားပြီဆိုရုံနဲ့ ပြီးသွားပြီလို့တော့မထင်နဲ့ဦးနော်။ Internet ကို Share ပေးလို့ရတဲ့နည်းလမ်း တွေကအများကြီးရှိတယ်။

But....ဒါပေမယ့် အဲ့ဒီလို Internet ကို Share ပေးလို့ရနိုင်တဲ့ နည်းလမ်းတွေထဲမှာ Proxy Server ကိုထိုင်ပြီးတော့ Internet ကို Share ပေးသုံးတဲ့ နည်းလမ်းကတော့ အကောင်းဆုံးပါပဲ။ Internet ကို Share ပေးလို့ရတဲ့ နည်းလမ်းတွေကတော့-

၁။ ICS (Internet Connection Sharing Service)

၂။ NAT (Network Address Translation Service)

၃။ Proxy Server တို့ပဲဖြစ်ပါတယ်။

အဲ့ဒီလို Internet ကို Share ပေးနိုင်တဲ့နည်းလမ်း (3) မျိုးထဲက Proxy Server ကိုထိုင်ပြီးတော့ Internet Share ပေးတာသည် ဘာကြောင့် ကျွန်တော်က အကောင်းဆုံးလို့ပြောတာလဲဆိုရင် Proxy Server ရဲ့ အားသာချက်တွေကတော့ ဒီလိုရှိပါတယ်။ ICS ဆိုတဲ့ Internet Connection Sharing Service ကို အသုံးပြုမယ်ဆိုရင် Computer အလုံးအရေအတွက် 254 လုံးအထိအသုံးပြုနိုင်ပါတယ်။ ဘာကြောင့် Computer အလုံးအရေအတွက် 254 လုံးပဲသုံးနိုင်တာလဲဆိုရင် ICS Service ကို Run ပြီး Internet Connection Share ပေးလိုက်တာနဲ့ မိမိရဲ့ Local Area Network ထဲမှာရှိတဲ့ Computer တွေသည် IP:192.168.0.1 ကနေ IP:192.168.0.254, Subnet Mask: 255.255.255.0 ထိပဲအသုံးပြုခွင့်ရမှာဖြစ်ပါတယ်။ ဘာ့ကြောင့်ဆိုတော့ ICS ကို Run တာနဲ့ အသုံးပြုခွင့်ရှိမယ့် Network Address သည် 192.168.0.0 ပဲဖြစ်တဲ့အတွက်ကြောင့်ဖြစ်ပါတယ်။ နောက်ပြီး ICS Service နဲ့ Internet Connection ကို Share ပေးတာသည် Network Traffic ကိုမထိန်းနိုင်ပါဘူး။ နောက်ထပ် Internet Connection ကို Share လုပ်ပေးနိုင်တဲ့ Product of YOUTH

Service ကတော့ NAT (Network Address Translation) Service ပဲဖြစ်ပါတယ်။ NAT Service ဆိုတာလည်း Internet ကို Share ပေးနိုင်တာတော့မှန်ပါတယ်။ သူက ICS Service လိုမျိုးတော့ 192.168.0.0 Network Class တစ်ခုထက်မက မိမိကြိုက်နှစ်သက်တဲ့ IP Address Class တွေကို သတ်မှတ်ပြီး Internet ကို Share ပေးနိုင်ပါတယ်။ နောက်ပြီး NAT Service မှာ Basic Firewall ပါရှိတဲ့အတွက်ကြောင့် မိမိရဲ့ Local Area Network ထဲက Computer တွေအတွက်လုံခြုံမှုတော့ရှိပါတယ်။ ဒါပေမယ့် NAT သည် ICS Service လိုမျိုးပဲ Network Traffic ကိုတော့မထိန်းနိုင်ပါဘူး။

ဟော....သူလာပြီ။ Proxy Server လေ။ Proxy Server ကိုအသုံးပြုပြီး Internet ကို Share ပေးတဲ့နေရာမှာတော့ သူ့ရဲ့အားသာချက်တွေကတော့ အများကြီးပါပဲ။ Proxy Service ကိုသုံးမယ်ဆိုရင်လေ မိမိရဲ့ Local Area Network အတွင်းမှာရှိတဲ့ Computer တွေကို မိမိကြိုက်တဲ့ IP Address Class တွေကိုသတ်မှတ်ပေးလို့ရတယ်။ နောက်ပြီး Proxy Server က NAT နဲ့ ICS Service တို့လိုမိမိရဲ့ Local Area Network အတွင်းထဲက Computer တွေသည် Internet နဲ့တိုက်ရိုက်ချိတ်ဆက်ထားတာမဟုတ်ပဲ Proxy Server ကနေဖွင့်ပေးထားတဲ့ Web Proxy Service ပေးတဲ့ Port တစ်ခုထဲကနေပဲ လက်ခံယူသုံးတာဖြစ်တဲ့အတွက် NAT နှင့် ICS Service တို့ထက်ပိုပြီး Security အားကောင်းမွန်ပါတယ်။ နောက်ပြီး Proxy Server ကနေ Client တွေကို မိမိပေးမသုံးချင်တဲ့ Website တွေကို ပိတ်ထားလို့ရတယ်။ နောက်ပြီး မိမိ Internet ပေးသုံးခွင့်မပြုချင်တဲ့ Computer တွေသတ်မှတ်ထားလို့ရတယ်။ နောက်ပြီး မိမိက Client တွေကို File Download လုပ်ခွင့် ဘယ်လောက်ပဲပေးမယ်ဆိုတာတွေ၊ နောက်ပြီး မိမိက Client တွေကို Internet ပေးသုံးခွင့်အချိန် ဘယ်အချိန်ကနေ၊ ဘယ်အချိန်အထိပဲ ပေးသုံးမယ်ဆိုတာတွေ၊ နောက်ပြီး Client Computer ကနေ Website တစ်ခုကိုခေါ်သုံးတဲ့အချိန်မှာ Proxy Server ထဲက Cache ထဲမှာ ၎င်း Website သိမ်းထားပြီး၊ အကယ်၍အခြား Client Computer သည်အလားတူ Website ကိုပဲထပ်၍ ကြည့်ရှုမယ်ဆိုရင် Proxy Server သည်မိမိရဲ့ Local Cache ထဲမှာရှိတဲ့ Website ကိုပဲပြန်၍ချပေးတဲ့အတွက် Network Traffic မဖြစ်တော့ပဲ Internet Speed ကိုပို၍မြန်ဆန်စေပါတယ်။

နောက်ပြီး မိမိက Local Area Network ထဲမှာရှိတဲ့ Computer များသုံးသွားတဲ့ Website တွေကိုပြန်ပြီးကြည့်ချင်တယ်ဆိုရင် Proxy Server ထဲက Log File ထဲမှာဝင်ရောက်ကြည့်ရှုနိုင်ပါတယ်။ နောက်ပြီး မိမိရဲ့ Local Area Network ထဲမှာရှိတဲ့ Computer များကို Internet အသုံးပြုရာ၌ မိမိသတ်မှတ်ထားတဲ့ User Name နှင့် Password ကိုသိမှ Internet အသုံးပြုခွင့်ရအောင်ပြုလုပ်တာတွေ၊ နောက်ပြီး ... နောက်ပြီး ....နောက်ပြီးတော့.... Proxy Server ကိုအသုံးပြုတဲ့ အားသာချက်တွေအများကြီးရှိတယ်။ ကဲဒီတော့ Internet

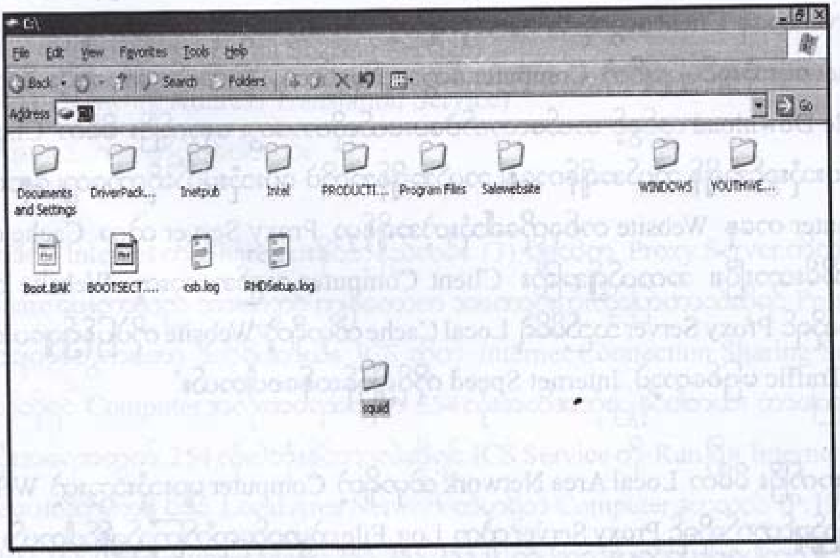
ကို Share ပေးတဲ့ Server ကိုအသုံးပြုမယ်ဆိုရင် Proxy Server ရဲ့အားသာချက်တွေကို သတိရလိုက်ပါ နော်....။ ကဲကဲ Proxy Server ကိုညွှန်းလိုက်တာ တော်တော်လေးတောင် လက်ညောင်းသွားပြီ။ ဒီတော့ ဆက်မရေးတော့ပဲ ဒီနားမှာပဲ နားလိုက်တော့မယ်နော်။ Proxy Server ကို Install လုပ်ပုံလုပ်နည်း Step By Step တွေကိုဆက်လက်ဖတ်ရှုပါဦးခင်ဗျာ။

မှတ်ချက်။ ။ NAT Server နှင့် Proxy Server ကိုနှစ်မျိုး တွဲထိုင်မယ်ဆိုရင်တော့ ပိုမိုကောင်းပါတယ်။ Proxy Server ကိုအသုံးပြုမယ်ဆိုရင် Proxy Server ထိုင်မယ့် Computer ထဲမှာ Network Card နှစ် Card စိုက်ထားရပါမယ်။

၁၀.၂ **Squid Proxy Service ကို Run ပုံ**

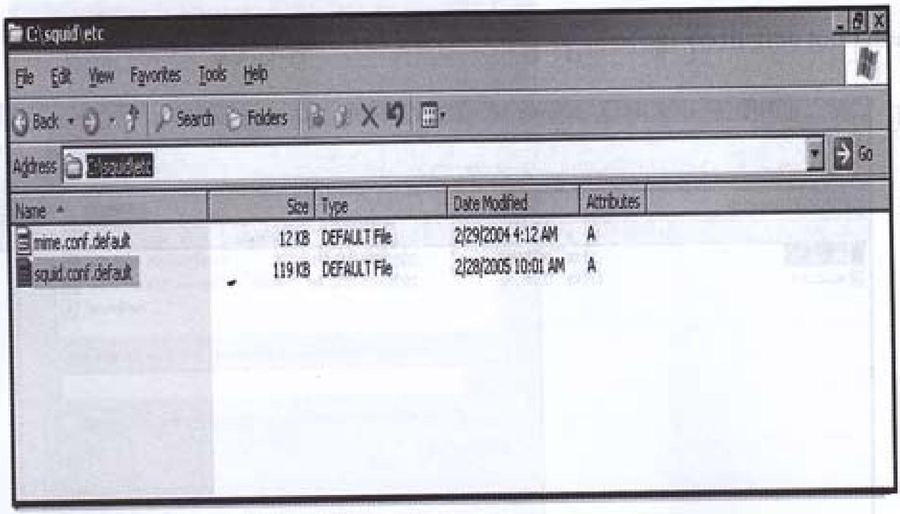
❖ Squid Folder ကို My Computer ထဲက C: Drive အောက်ထဲသို့ Copy ကူးထည့်ပါ။ ပုံ ၁၀.၃ တွင်ကြည့်ပါ။

ပုံ ၁၀.၃



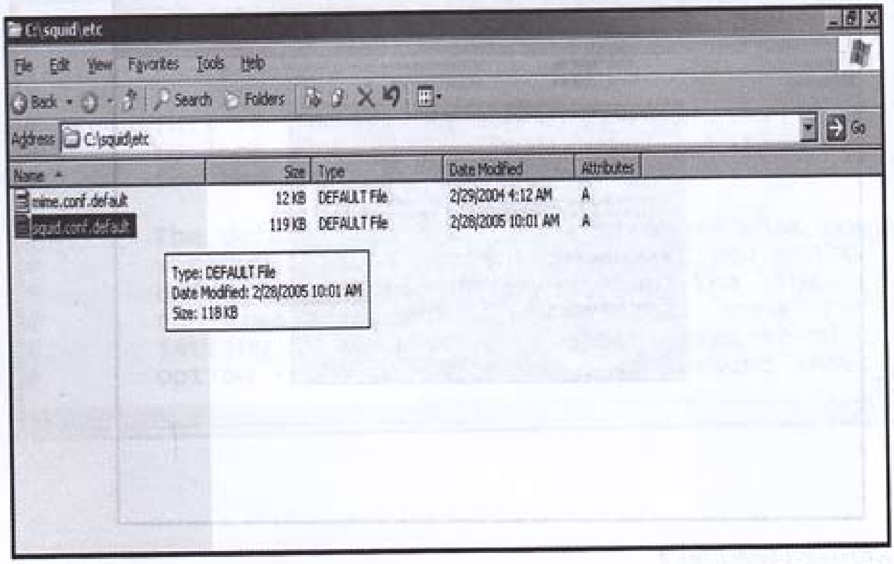
❖ ၎င်း Squid Folder ထဲက etc Folder ထဲကို ရောက်အောင်ဝင်ပါ။ ပုံ ၁၀.၄ တွင် ကြည့်ပါ။

ပုံ ၁၀.၄



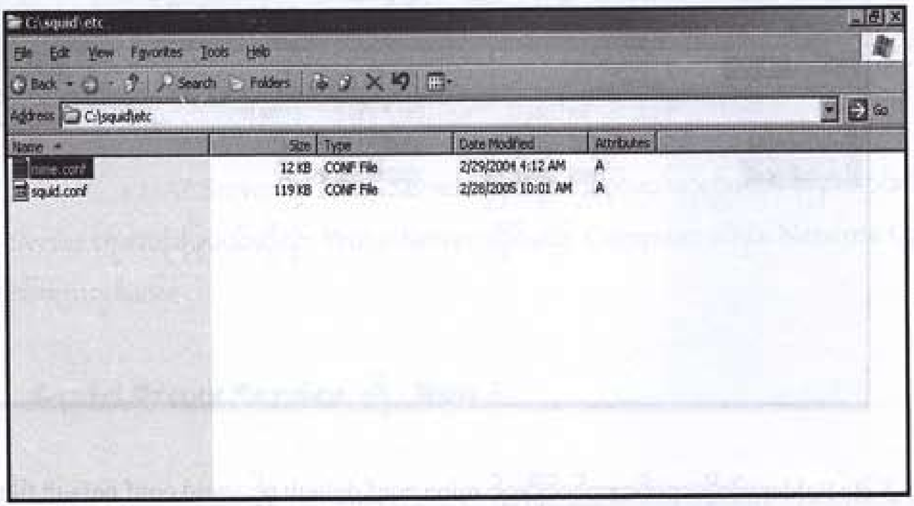
etc Folder ထဲသို့ရောက်အောင်ဝင်ပြီးရင် mine.conf.default နှင့် squid.conf.default file နှစ်ဖိုင်ကို တွေ့ရပါလိမ့်မယ်။ ၎င်းဖိုင်နှစ်ဖိုင်သည် squid service ကို Run လို့ရစေရန်အတွက် ဝင်ပြင်ပေးရမယ့် Configuration File ဖြစ်တယ်။ ဒါကြောင့် အဲဒီဖိုင်နှစ်ဖိုင် Squid Proxy Service Run လို့ရအောင် နံပါတ် (၁) အနေနဲ့လုပ်ရမှာကတော့ အဲဒီဖိုင်နှစ်ဖိုင်စလုံးရဲ့ Name တွေကို ပြောင်းပေးရပါမယ်။ သူတို့ Default ပါတဲ့ File Name mine.conf.default နှင့် squid.conf.default တို့ကို mine.conf နှင့် squid.conf ဆိုတဲ့ File Name ပြောင်းပေးရမှာ ဖြစ်ပါတယ်။ ပုံ ၁၀.၅ တွင်ကြည့်ပါ။

ပုံ ၁၀.၅



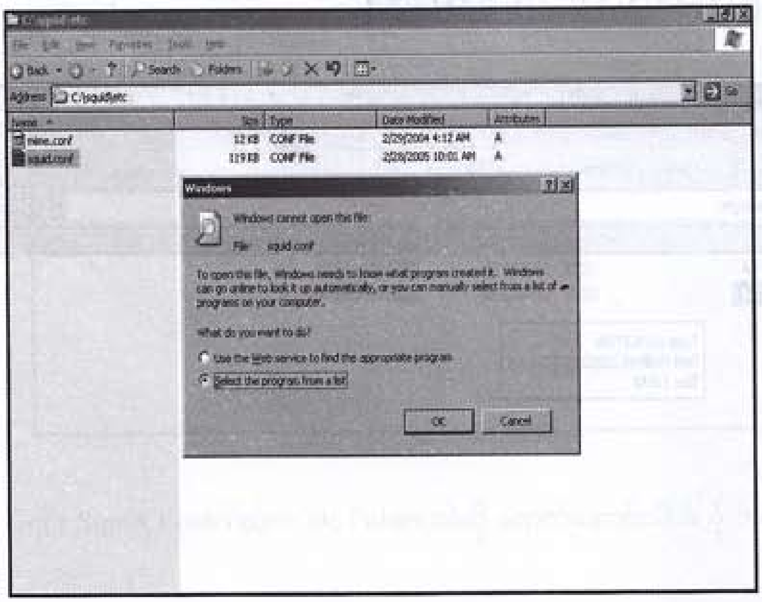
(.default) dot default ကို ဖျက်ပစ်ရမှာ ဖြစ်ပါတယ်။ ပုံ ၁၀.၆ တွင်ကြည့်ပါ။

ပုံ ၁၀.၆

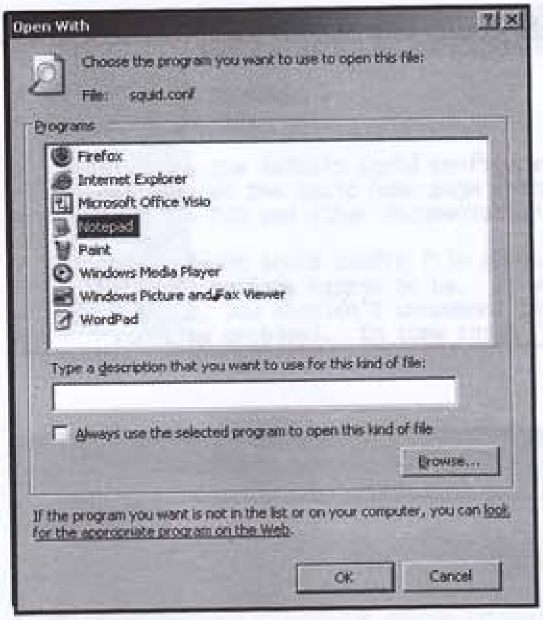


❖ ကဲ mine.conf နှင့် squid.conf လို့ File Name ကိုပြောင်းပြီးရင်တော့ squid.conf ကို Double Click နှိပ်ပြီးဖွင့်လိုက်ပါ။ အဲဒီအခါမှာ squid.conf File ကိုဘယ် Program နဲ့ဖွင့်မယ်လို့လာမေးပါလိမ့်မယ်။ Noadpad File ကိုရွေးပြီး ဖွင့်ပေးရမှာ ဖြစ်ပါတယ်။ ပုံ ၁၀.၇ နှင့် ပုံ ၁၀.၈ ကို တွဲကြည့်ပါ။

ပုံ ၁၀.၇

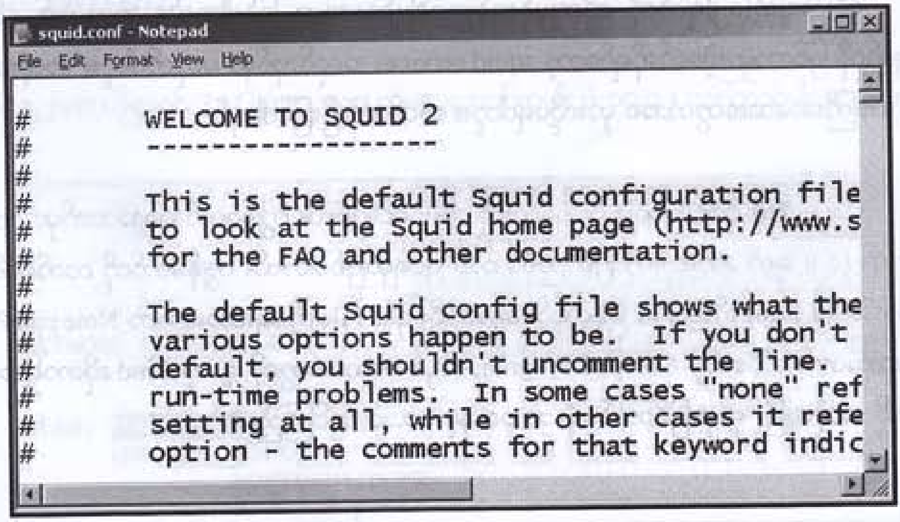


ပုံ ၁၀.၈



Note Pad File ကိုရွေးပြီး OK ကိုနှိပ်လိုက်ပြီဆိုတာနဲ့ "Welcome to Squid 2" ဆိုတဲ့ စာတန်းနဲ့ ရှတ်ရှက်ခတ်နေတဲ့ စာတွေကိုတွေ့ရပါလိမ့်မယ်။ အဲဒီစာတွေကို ကြည့်ပြီး သိပ်လည်းလန့်မသွားပါနဲ့ဦး။ ပုံ ၁၀.၉ တွင်ကြည့်ပါ။

ပုံ ၁၀.၉



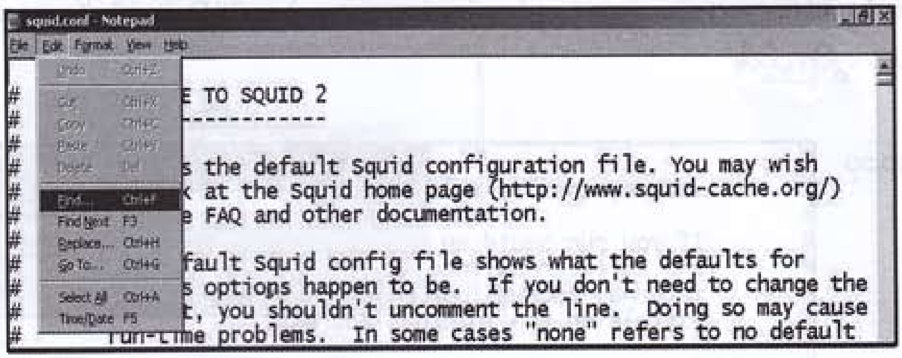
ကျွန်တော် အဲဒီ squid.conf.file ထဲက ဝင်ပြင်ရမယ့် အချက်တွေကို အရင်ဦးဆုံး ဖော်ပြပေးပါမယ်။ အဲဒီဝင်ပြင်ရမယ့် အချက်တွေကတော့ –

1.http_port
2.cache_mem
3.cache_dir
4.cache_access_log
5.cache_log
6.cache_store_log
7.emulate_httpd_log
8.always_direct
9.never_direct
10.http_access
11.dns_nameservers
12.visible_hostname

၎င်းအချက်(၁၂)ချက်ကို တိကျမှန်ကန်စွာဝင်ပြင်ပေးရမှာ ဖြစ်ပါတယ်။ အကယ်၍ ၎င်းအချက် (၁၂)ချက်ကို ပြင်တာမှားခဲ့မယ်ဆိုရင်တော့ squid services အလုပ်လုပ်မှာ မဟုတ်ပါဘူး။ စာလုံးပေါင်းတွေ၊ စာလုံးအကြီးအသေးတွေကအစ မှားလို့မရပါဘူး။ သတိထားပြီးပြင်ပါနော်။

OK -- ဒီလိုဆိုရင် ပြင်ရမယ့်ပုံစံလေးကို အရင်ရှင်းပြမယ်။ ကျွန်တော်အခုအထက်မှာ ဖော်ပြထားတဲ့အချက် (၁၂) ချက် အားလုံးကို ပြီးပြည့်စုံအောင် ပြင်ရမှာဖြစ်ပါတယ်။ ကျွန်တော်တို့ လက်ရှိဝင်ပြင်မယ့် File က squid.comf ဆိုတဲ့ File ဖြစ်တယ်။ နောက်ပြီး ၎င်း File ကိုရေးထားတာက Note pad Program နဲ့ ရေးထားတာ။ အဲဒီတော့ Notepad Program ထဲမှာ စာသားတွေကို ရှာတဲ့ Find ဆိုတာရှိတယ်။ အဲဒီ Find ကို အသုံးချပြီး ရှာမှာဖြစ်တယ်။ ပုံ ၁၀.၁၀ နှင့် ၁၀.၁၁ တွင်ကြည့်ပါ။

ပုံ ၁၀.၁၀

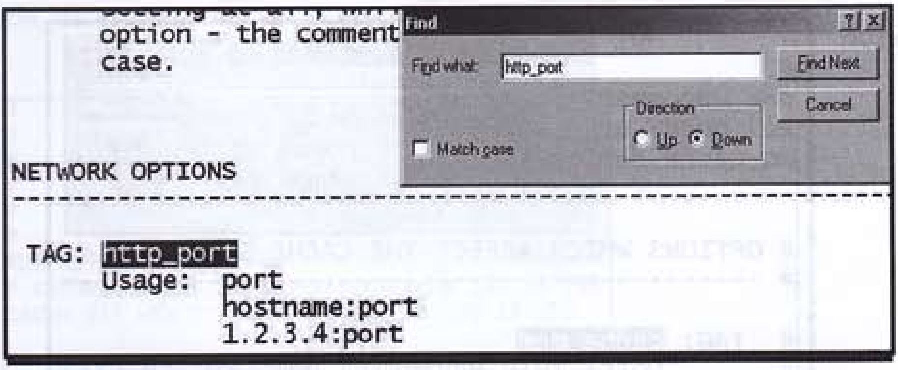


ပုံ ၁၀.၁၁

ငှင်း Find Box ထဲမှာ ကျွန်တော်ရေးသားထားတဲ့ အချက် (၁၂)ချက်ကို တစ်ခုချင်းစီ ရိုက်ထည့်ပြီး ရှာရမယ်ဖြစ်ပါတယ်။ ကဲ အဲဒီလိုဆိုရင် Find Box ကိုအသုံးချပြီး squid.conf File ထဲက ကျွန်တော်တို့ပြင်ရမယ့် အချက်တွေကို ရှာကြရအောင် --

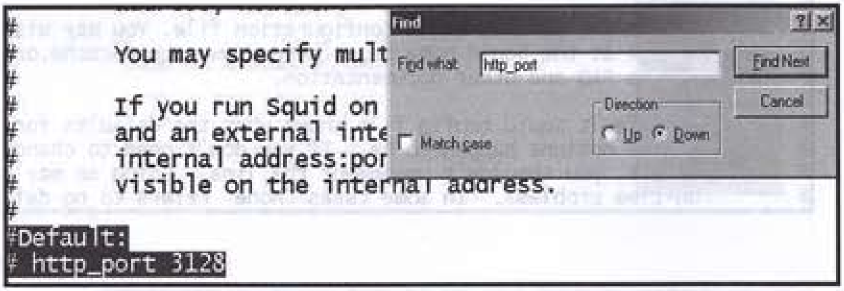
1. http_port ကိုရှာရင် TAG:http_port ကိုတွေ့အောင်ရှာပါ။ ပုံ ၁၀.၁၂ တွင်ကြည့်ပါ။

ပုံ ၁၀.၁၂



၄င်း TAG:http_port ကိုတွေ့တာနဲ့ သူ့ရဲ့အကြောင်းတွေအောက်က "# Default" ကိုတွေ့အောင်ရှာပါ။ ပုံ ၁၀.၁၃ တွင်ကြည့်ပါ။

ပုံ ၁၀.၁၃



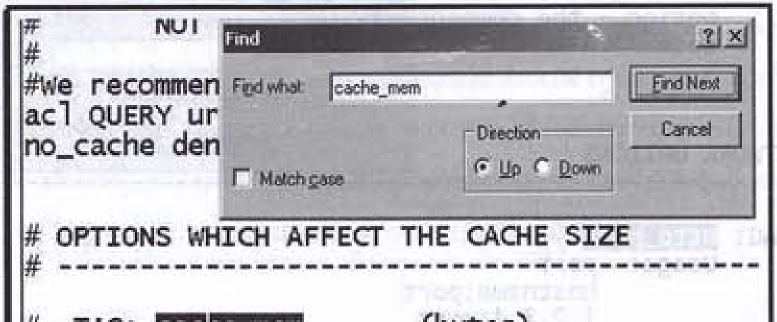
#Default စာတန်းကိုတွေ့ပြီဆိုတာနဲ့ သူ့ရဲ့အောက်က စာကြောင်းသည် ကျွန်တော်တို့ပြင်ရမယ့် စာကြောင်းနေရာဖြစ်ပါတယ်။ အောက်မှာ ပြထားတဲ့ပုံအတိုင်း ပြင်လိုက်ပါ။ ပုံ ၁၀.၁၄ တွင်ကြည့်ပါ။

ပုံ ၁၀.၁၄

Default အောက်မှာ မိမိပြင်မယ်ကြောင်းအရာတွေကို ရိုက်ထည့်ပေးရမှာဖြစ်တယ်။

2. cache_mem ကိုပြင်ပုံ

ပုံ ၁၀.၁၅

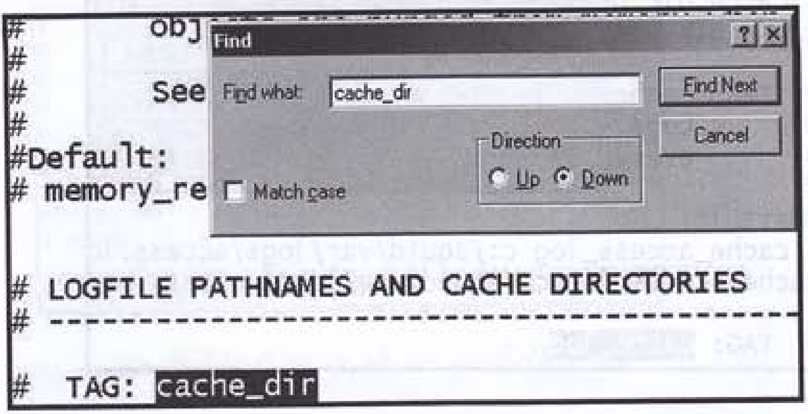


ပုံ ၁၀.၁၆

```
#
#Default:
# cache_mem 8 MB
cache_mem 100 MB
```

3. cache_dir ပြင်ပုံ။ ပုံ ၁၀.၁၇ နှင့် ၁၀.၁၈ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၁၇

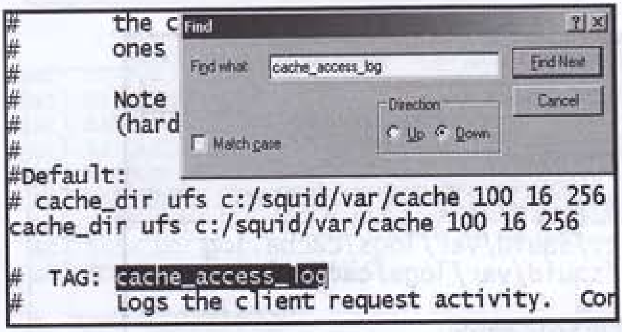


ပုံ ၁၀.၁၈

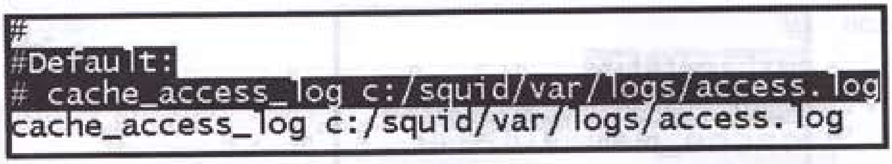
```
#
#Default:
# cache_dir ufs c:/squid/var/cache 100 16 256
cache_dir ufs c:/squid/var/cache 100 16 256
```

4. cache_access_log ကိုပြင်ပုံ။ ပုံ ၁၀.၁၉ နှင့် ၁၀.၂၀ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၁၉

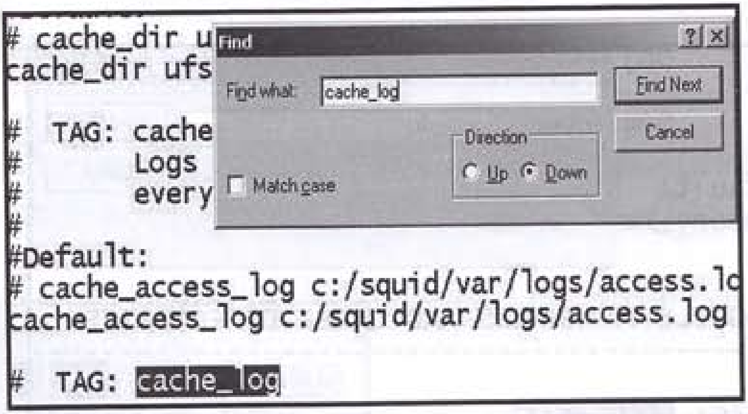


ပုံ ၁၀.၂၀

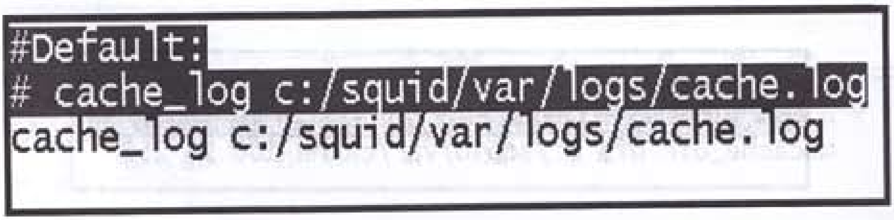


5. cache_log ပြင်ပုံ။ ပုံ ၁၀.၂၁ နှင့် ပုံ ၁၀.၂၂ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၂၁

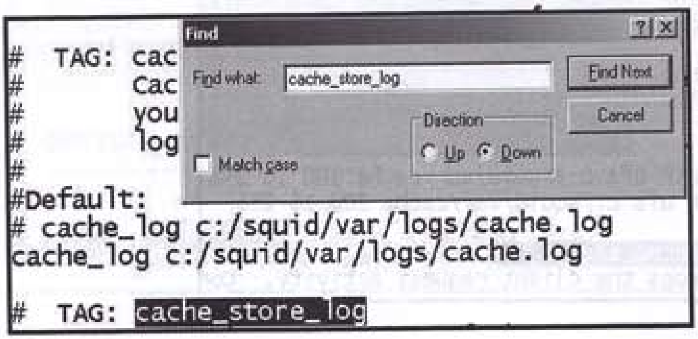


ပုံ ၁၀.၂၂

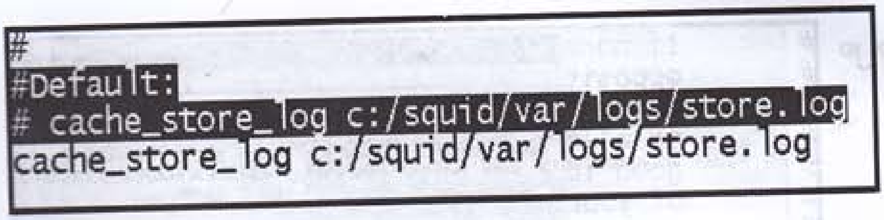


6. cache_store_log ကိုပြင်ပုံ။ ပုံ ၁၀.၂၃ နှင့် ပုံ ၁၀.၂၄ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၂၃

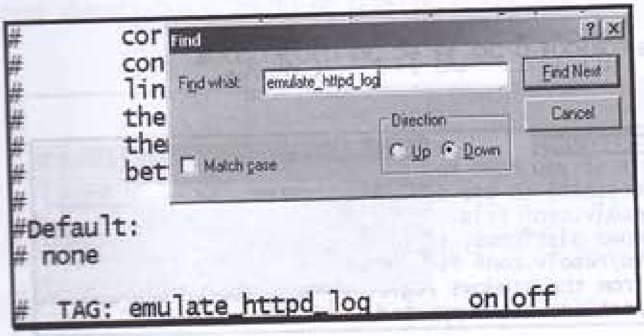


ပုံ ၁၀.၂၄



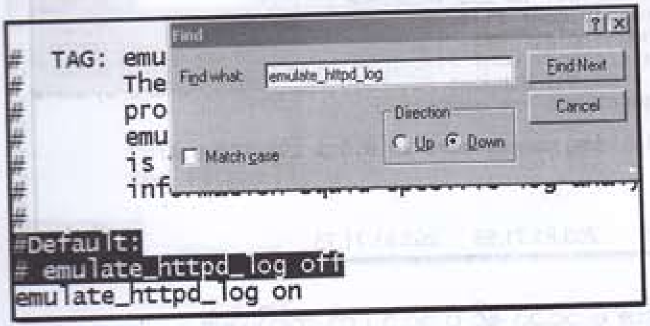
7. emulate_httpd_log ကိုပြင်ပုံ။ ပုံ ၁၀.၂၅ နှင့် ၁၀.၂၆ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၂၅

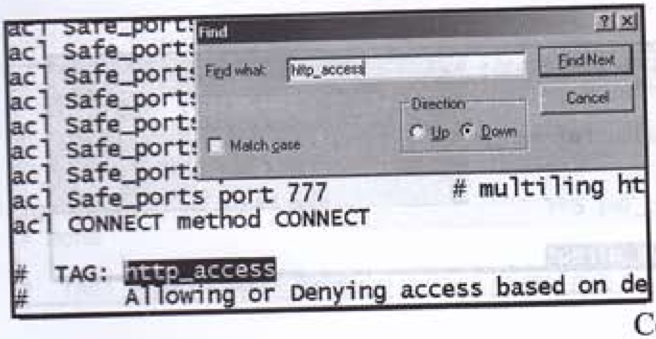


8. http_access ကိုပြင်ပုံ။ ပုံ ၁၀.၂၇ နှင့် ၁၀.၂၈ ကိုတွဲကြည့်ပါ။

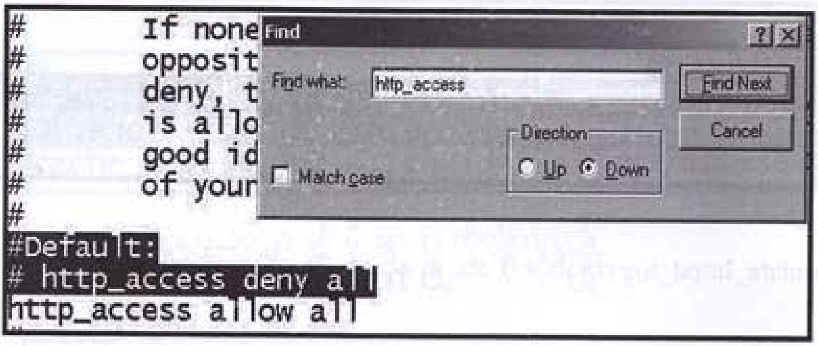
ပုံ ၁၀.၂၆



ပုံ ၁၀.၂၇

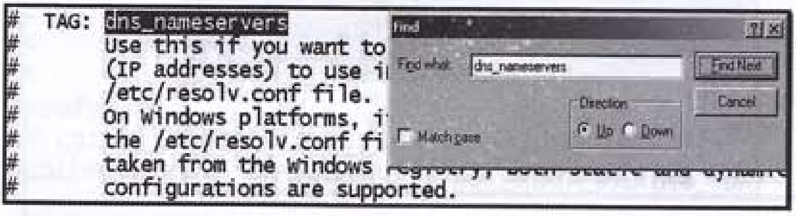


ပုံ ၁၀.၂၈

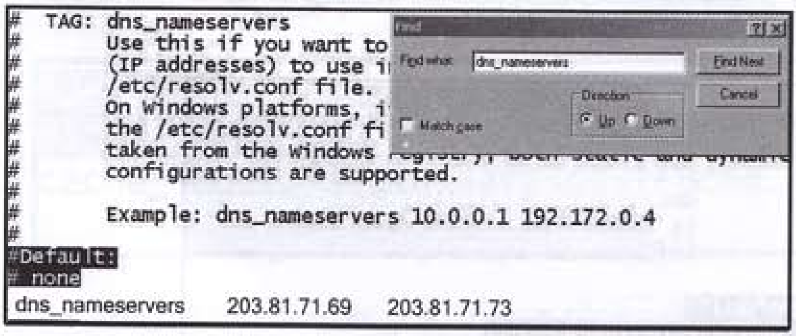


9. dns_nameservers ကိုပြင်ပုံ။ ပုံ ၁၀.၂၉ နှင့် ၃၀ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၂၉

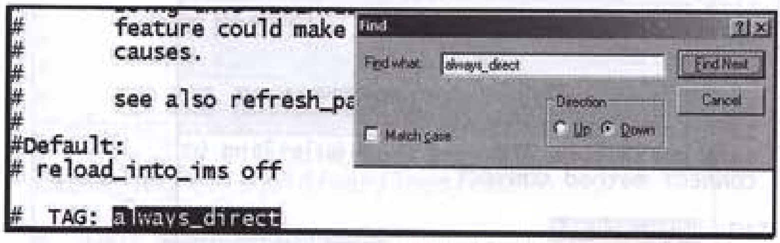


ပုံ ၁၀.၃၀

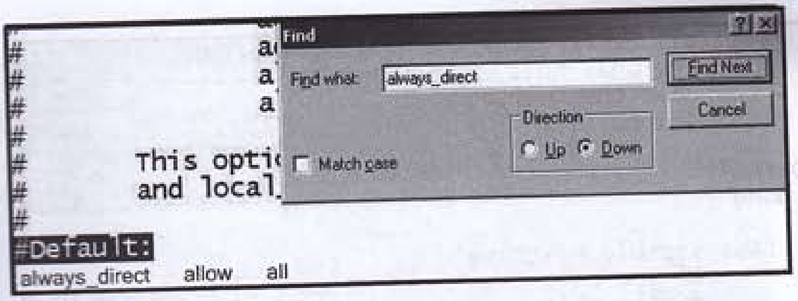


10. always_direct ပြင်ပုံ။ ပုံ ၁၀.၃၁ နှင့် ပုံ ၁၀.၃၂ ကို တွဲကြည့်ပါ။

ပုံ ၁၀.၃၁

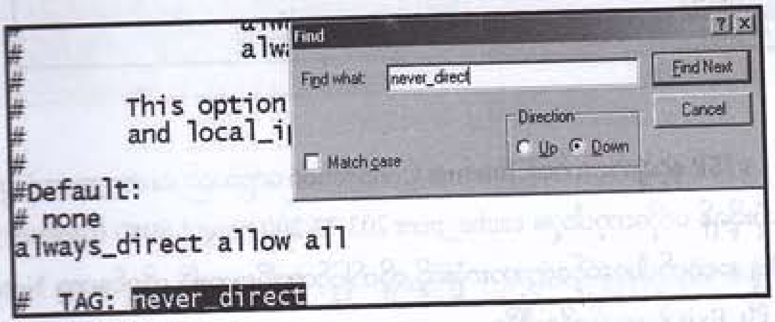


ပုံ ၁၀.၃၂

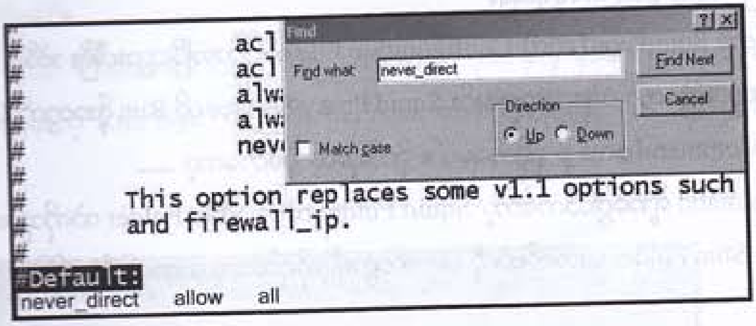


11. never_direct ဖြစ်ပုံ။ ပုံ ၁၀.၃၃ နှင့် ပုံ ၁၀.၃၄ ကိုကြည့်ပါ။

ပုံ ၁၀.၃၃

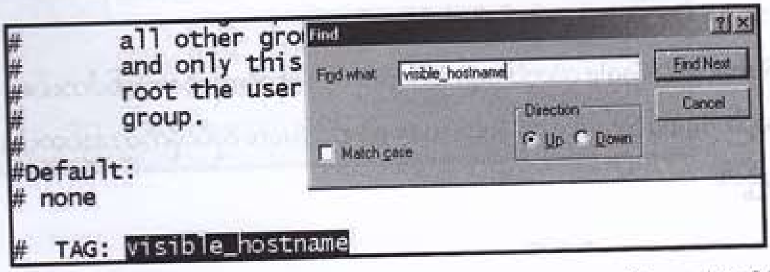


ပုံ ၁၀.၃၄

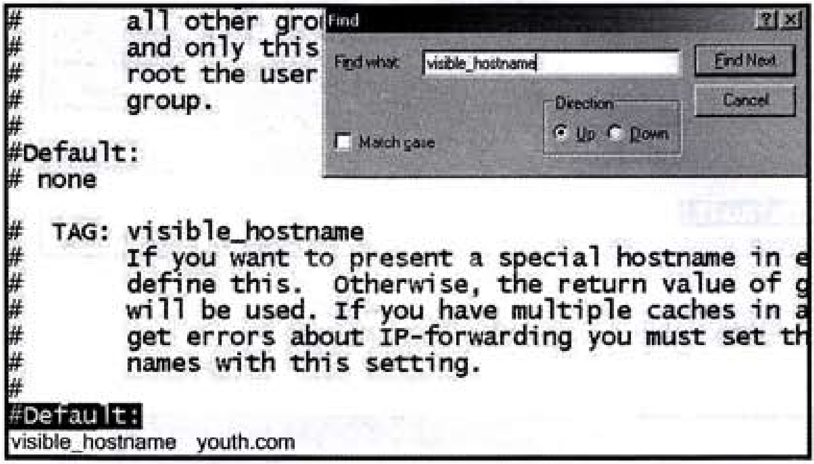


12. visible_hostname ကိုဖြစ်ပုံ။ ပုံ ၁၀.၃၅ နှင့် ၁၀.၃၆ ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၃၅



ပုံ ၁၀.၃၆



မှတ်ချက်။ ။ ISP နှင့်ချိတ်ဆက်တဲ့ Internet Connection တွေသည် cache_peer နဲ့သွားရပါမယ်။ always_direct သုံးဖို့ရန် မလိုတော့ပါဘူး။ cache_peer 203.72.200 parent 8080 0 default no_query ကဲ... ဘယ်လိုလဲဗျ အထက်ပါအဆင့်တွေအားလုံးကို လိုက်ပြင်တာပြီးသွားပြီ ဆိုရင်တော့ Notepad Program ကို Save ပြီး Exit နဲ့ ထွက်လိုက်ရပါပြီ။

ဒါဆိုရင်တော့ Squid.conf ဆိုတဲ့ Configuration File ကိုပြင်တာပြီးသွားပါပြီ။ အဲဒီ Configuration File ကိုပြင်ပြီးသွားရုံနဲ့တော့ မရသေးဘူးနော်။ Squid Proxy Service ကို Run ဖို့အတွက် Command Line ထဲကိုဝင်ပြီး Command လေး ၃ ခုရိုက်ရမယ်။ ရိုက်ရမယ့် ပုံစံကတော့ ....

၎င်း Command ရဲ့အဓိပ္ပါယ်ကတော့ Squid Folder ထဲက Sbin Folder ထဲကိုသွားတဲ့ Command ဖြစ်ပါတယ်။ Sbin Folder အောက်ထဲကို ရောက်သွားပြီဆိုရင်တော့ အောက်ပါအတိုင်းတွေ့ရပါမယ်။

ပြီးရင် ဘာဆက်လုပ်ရမလည်းဆိုရင် Squid Proxy Service Run ဖို့ရန်အတွက် ရိုက်ပေးရမယ့် Command တွေကတော့ ....

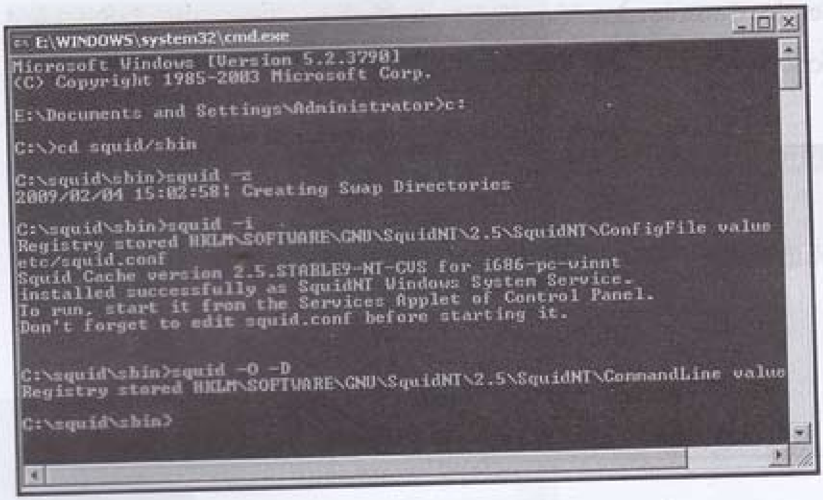
squid - z သည် Swap Directories ကိုဖန်တီးပါလိမ့်မယ်။

squid - i သည် Service Console ထဲတွင် Squid Service ကိုဖန်တီးလိုက်တာဖြစ်ပါတယ်။

squid - O - D သည် Squid Service ကို Registary ထဲတွင် Store လုပ်လိုက်တာဖြစ်တယ်။

ပုံ ၁၀.၃၇ တွင်ကြည့်ပါ။

ပုံ ၁၀.၃၇

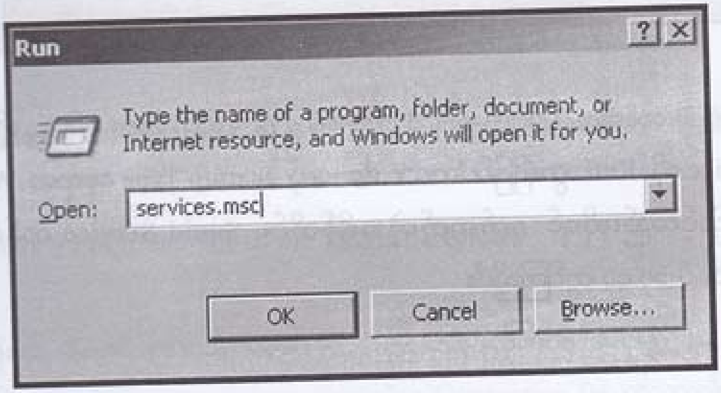


မှတ်ချက်။ ။Squid - z Command ကိုရိုက်လို့ Error ပြခဲ့ရင် Squid.conf File ကိုပြင်တာမှားနေလို့ဖြစ်ပါတယ်။ သေသေချာချာပြန်စစ်ဆေးပါ။

Squid -O -D Command တွင် (-O) အိုအကြီး (-D) ဒီအကြီးဖြစ်သည်။ အကြီးအသေးမှားရင် Error ပြပါလိမ့်မယ်။

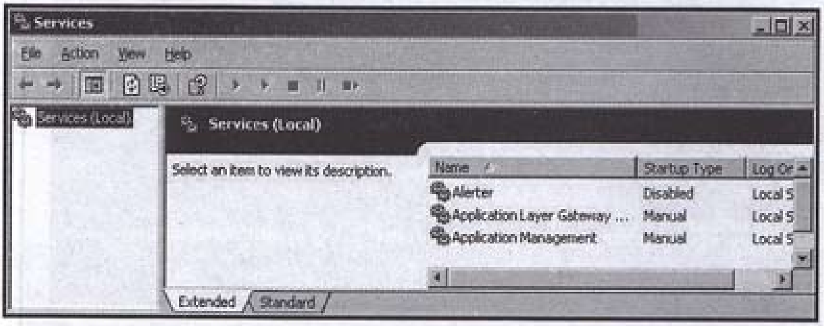
ကဲ ...... Command Line ထဲမှ ကျွန်တော် ပုံ၁၀.၃၇ မှာဖော်ပြထားတဲ့အတိုင်း အားလုံးမှန်သွားပြီဆိုရင်တော့ Run Box ကို ဖွင့်ပြီး Service.msc လို့ရိုက်ပြီးရင် OK လို့ပြောလိုက်ပါ။ ပုံ ၁၀.၃၈ တွင်ကြည့်ပါ။

ပုံ ၁၀.၃၈

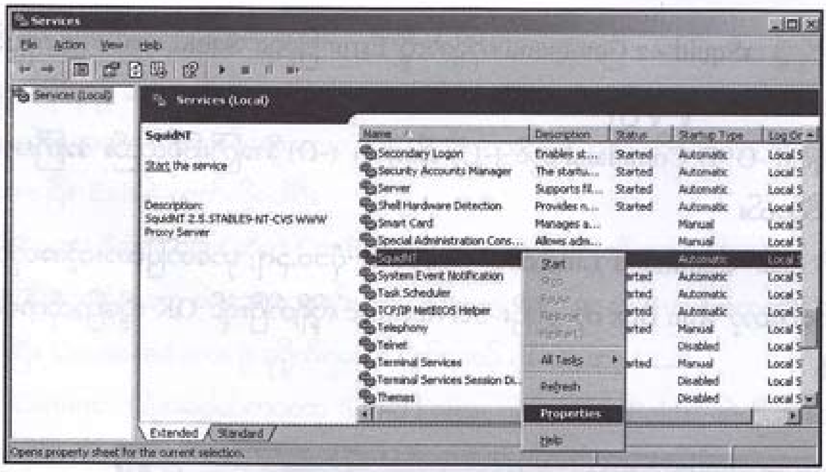


ပြီးရင် အဲဒီ Service Console ထဲက "SquidNT" ကိုရှာပြီးရင် သူ့ရဲ့ Properties ထဲကိုသွားပါ။ ပုံ ၁၀.၃၉ နှင့် ပုံ ၁၀.၄၀ တို့ကိုတွဲကြည့်ပါ။

ပုံ ၁၀.၃၉

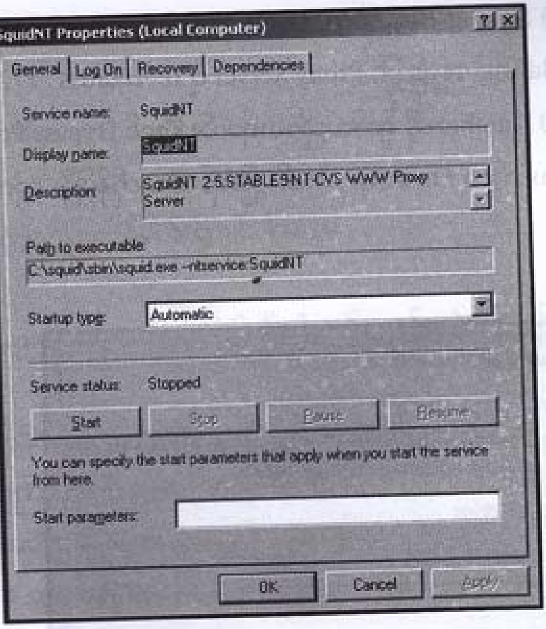


ပုံ ၁၀.၄၀



၎င်း SquidNT Properties (Local Computer) Dialog Box ထဲက Start Button ကိုနှိပ်လိုက်ပါ။ ဒါဆိုရင် Squid Service ကို Run သွားပြီဖြစ်ပါတယ်။ ဒါပေမယ့် Startup Type နေရာမှာ Automatic ပဲထားခဲ့ပါ။ ဘာကြောင့်လည်းဆိုရင် စက်တက်တဲ့အချိန်တိုင်း Squid Service တန်းပြီး Run နေအောင်လို့ဖြစ်ပါတယ်။ ပုံ ၁၀.၄၁ တွင်ကြည့်ပါ။

ပုံ ၁၀.၄၃



OK .... Squid Proxy Service ကလည်း Run နေပြီဆိုတော့ Client Computer တွေ Internet အသုံးပြုရန်အတွက် ဘယ်လိုမျိုး Setting ထည့်ပေးရမယ်ဆိုတာ ကိုကြည့်လိုက်ပါဦး။ မှတ်ချက်–ကျွန်တော်အရှေ့မှာဖော်ပြခဲ့တဲ့ ပုံ ၁၀.၂ ရဲ့ Network Diagram ထဲကအတိုင်းပဲ Client တွေကို Setting ချပြပါမယ်။

Client တွေမှာ ဘာ Setting ချပေးရမှာလဲဆိုရင် Internet Explorer (or) Browser တွေထဲမှာ Setting ချပေးရမှာဖြစ်ပါတယ်။ အဲဒီတော့ ၎င်း Setting ကို Internet အသုံးပြုမယ့် Client Computer တိုင်းမှာ ထည့်ပေးရပါမယ်။

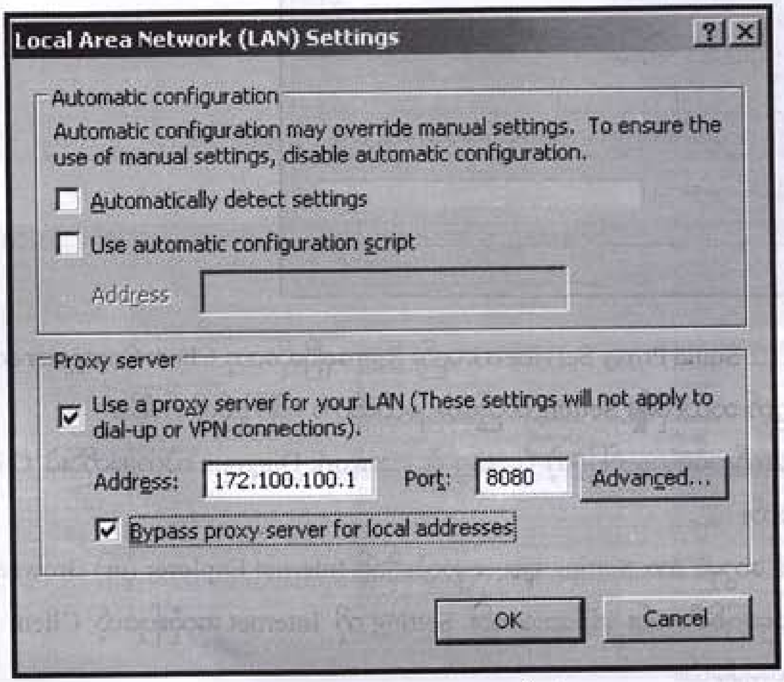
၁၀.၃ Client Computer ရဲ့ Internet Explorer ထဲမှာ Setting ချခြင်း

Start > Program > Open the Internet Explorer

ပြီးရင် Tools ထဲက Internet Options ကိုနှိပ်လိုက်ပါ။ အဲဆိုရင် Internet Options Box ပေါ်လာပါလိမ့်မယ်။ ၎င်း Internet Option Box ထဲက Connection Tab ကိုသွားပါ။ ပြီးရင် LAN Setting Button ကိုနှိပ်ပါ။ Local Area Network (LAN) Setting Box ပေါ်လာမယ်။

ၚ္ငင်း Local Area Network (LAN) Setting Box ထဲက Use a Proxy Server for your LAN ရဲ့ Check Box ကို On ပေးပါ။ ပြီးရင် Address: နေရာတွင် Proxy Server ရဲ့ IP Address : 172.100.100.1 ကိုထည့်ပြီးရင် Port : နေရာတွင် 8080 Number ကို ရိုက်ထည့်ပေးရမယ်။ ပြီးရင် Bypass Proxy Server for Local Addresses ရဲ့ Check Box ကိုလဲ On ပေးခဲ့ရပါမယ်။ ပြီးရင် OK ကိုနှိပ်ပြီး ထွက်လိုက်ပါ။ ပုံ ၁၀.၄၂ တွင်ကြည့်ပါ။

ပုံ ၁၀.၄၂



ဒီဆိုရင်တော့ Client Computer များအားလုံးသည် ကျွန်တော်တို့ Run ပေးလိုက်တဲ့ Proxy Server ကနေတစ်ဆင့် Internet Access ကို ယူသုံးလို့ရသွားပါပြီ။

ကဲ ...... အားလုံးပဲ Proxy Server ရဲ့အကြောင်းကိုလဲ လက်ညောင်းအောင်ကို ရှင်းပြပြီးပြီ ----- Proxy Server ကို ဘယ်လို Run ရမလဲဆိုတဲ့ Step By Step တွေကိုလည်း ပြောပြပြီးပြီ .... အားလုံးပဲ အဆင်ပြေနိုင်ပါစေလို့ မျှော်လင့်ပါတယ်။ လက်လည်းအရမ်းညောင်းနေပြီ။ Proxy Server ကတော့ ဒီနေရာမှာပဲ အပြီးသတ်လိုက်ပါတယ်။

Product of YOUTH

နိဂုံး

၁။ ကျေးဇူးတင်ကြလိမ့်မယ်လို့ထင်ပါတယ်။

၂။ ရေးရတာအတော်လေးပင်ပန်းပါတယ်။ တစ်ဖက်ကလည်းအတန်းတွေစာသင်ရသေးတာကိုး။

၃။ အခုကတော့ လူစွမ်းအားအရင်းအမြစ်တွေ စက်ရုံကရိုက်ထုတ်သလို တစ်ထောင်းထောင်းနှင့်ထွက်စေဖို့ပါ။ ဒါကြောင့် သင်တန်းမတက်နိုင်တဲ့သူတွေလည်းသိအောင် စာအုပ်တွေကို စဉ်ဆက်မပြတ်ထုတ်ပေးနေတာဖြစ်ပါတယ်။ သိသူဖော်စား မသိသူကျော်သွား အဲ့လေ သိချင် ဝယ်ဖတ်ပေါ့ဗျာ။ မဖတ်တဲ့သူကတော့ အနီးနားမှာ ပညာတွေရှိရက်နဲ့ သူ့အတွက်ကတော့ ဝေးနေမှာဖြစ်ပါတယ်။

၄။ ထုံးစံအတိုင်းအကောင်းဆုံးလုပ်ခဲ့ပါတယ်။ လိုနေတာလေးတွေခွင့်လွှတ်ပေးပါ။

၅။ အားပေးနေသမျှ စာတွေကိုလည်း ကြိုးစားပြီးရေးနေပါဦးမယ်။

၆။ အားလုံးကိုယ်စိတ်နှစ်ဖြာ ကျန်းမာချမ်းသာကြပါစေ။

ကျေးဇူးတင်စွာဖြင့်

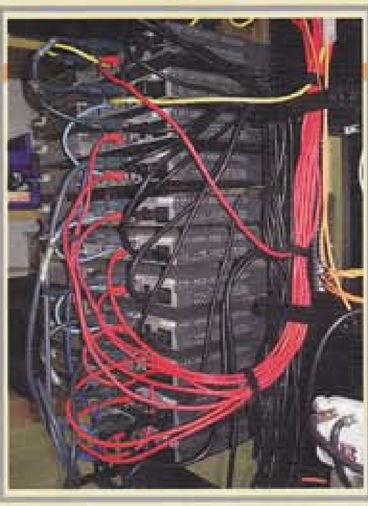
ဇော်လင်း

စာရေးသူ

၂၁ ဖေဖော်ဝါရီ ၂၀၀၉

Complete Network Guide

CCNA MCSE MCSA MCTS



IPv4 Addressing, DHCP, IPv6 or IPng, DNS,
IPv4 Subnetting, Mail Server,
Supernetting, NAT, IPv4 Routing, Squid Proxy

ZAW LIN YOUTH

CD Rom Included

ကွန်ပျူတာကွန်ရက်ကို စိတ်ဝင်စားတဲ့သူများ။

ကွန်ပျူတာကွန်ရက် Diploma သင်တန်းတက်နေသူများ။

ကွန်ပျူတာပညာဖြင့် အသက်မွေးဝမ်းကျောင်းပြုလိုသူများ။

ကွန်ပျူတာတက္ကသိုလ် ကျောင်းသား/ ကျောင်းသူများ။

နိုင်ငံတကာ အသိအမှတ်ပြု စာမေးပွဲဖြေဆိုမည့်သူများ။

နိုင်ငံတကာတွင် Network Engineer အဖြစ်အလုပ်လုပ်ကိုင်လိုသူများ။

Internet ဆိုင် ဖွင့်ထားသူများဖတ်ရန် အထူးသင့်လျော်သည်။