

## Socket

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

### *Destination or Client Source or Server*

IP : 192.169.1.100 IP : 192.168.1.1

Port : 6571 Port : 21

### *Destination or Client Source or Server*

IP : 192.169.1.100 IP : 192.168.1.1

Port : 6571 Port : 23

### *Destination or Client Source or Serv*

IP : 192.169.1.100 IP : 192.168.1.2

Port : 6571 Port : 23

### *Destination or Client Source or Server*

IP : 192.169.1.100 IP : 192.168.1.20

Port : 80 Port : 23

အထက်ဖော်ပြပါ socket များကဲ့သို့ IP တူ၊ port မတူ၊ Port တူ၊ IP မတူ သော connection များကြောင့် network သည် မှန်မှန်ကန်ကန် အလုပ်လုပ်ဆောင်နေခြင်း ဖြစ်သည်။ computer တစ်လုံးတွင် ချိတ်ဆက်လုပ်ဆောင်နေသော port များကို သိရှိ လိုပါက netstat ဆိုသော command မျိုးဖြင့် ကြည့်ရှုနိုင်သည်။ ထို့ကြောင့် server တစ်ခု လုပ်လိုက်တိုင်း service ပေးမည့် port ကို အထူးသတိပြုရမည် ဖြစ်သည်။ ဖော်ပြပါ protocol, Port နှင့် Socket များအလုပ်လုပ်ပုံ အကြောင်းကို အကြမ်းဖျဉ်းနားလည် သိရှိပြီးပါက TCP/IP အကြောင်းနှင့် Subnetting အကြောင်းတို့ကို ဆက်လက်လေ့လာ ကြရမည်။

## **TCP/IP (Transport Control Protocol/ Internet Protocol)**

TCP/IP သည် protocol အမျိုးအနွယ်အုပ်စုများထဲမှတစ်ခုဖြစ်ပြီး Internet နည်းပညာ တွင် အလွန်အရေးကြီးသော အချက်တစ်ချက်ဖြစ်ပါသည်။ Intranet များ တည်ဆောက် အသုံးပြုရန်လွယ်ကူစွာဆောင်ရွက်နိုင်၍ Internet ၏ အခြေခံအုတ်မြစ် ဖြစ်ပါသည်။ Internet သို့ဝင်ရောက်ဆက်သွယ်လိုလျှင်လည်းကောင်း၊ Intranet တည် ဆောက်ရာတွင်လည်းကောင်း၊ ဦးစွာမိမိ၏ server သို့မဟုတ် workstation အား TCP/IP setup လုပ်ရသည်။ Intranet အပါအဝင် Internet အလုပ်လုပ်နိုင်ရန် အဓိကအချက်အချာ ဟုပင်ဆိုနိုင်သည်။

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

## **Ethernet (Media Access Control) Address**

Ethernet network card များသည် ကိုယ်ပိုင် hardware address ရှိပြီး media access control (MAC) address အဖြစ်သိရှိကြပါသည်။ စက်ရုံမှထုတ်လုပ်စဉ် ထည့်သွင်း ပေးလိုက်ပြီး 48bits အား Hexadecimal ဖြင့်ဖွဲ့စည်းထားပါသည်။ ယင်း address ၏ ပထမ အပိုင်း ၃ ပိုင်း

ကို OUI(Organizationally Unique Identifier) ဟုခေါ်ပြီး IEEE မှခွဲဝေ သတ်မှတ်ပေးပါသည်။ ကျန်အပိုင်း ၃ ပိုင်းကို ထုတ်လုပ်သူမှ card တစ်ခုချင်းအလိုက် သတ်မှတ်ပါသည်။ ပြင်ဆင်မရဘဲ hard coded အဖြစ် NIC ပေါ်တွင်အပြီး တပ်ဆင်ထား ခြင်းဖြစ်သည်။

ဥပမာ - 1F:10:FF:FF:AE:95

#### IP Address

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

$$2^8 \cdot 2^8 \cdot 2^8 \cdot 2^8$$

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

#### Classifications

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

TCP/IP classes

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

မြန်မာနိုင်ငံအတွက် assign လုပ်ထားသည့် IP သည် 203 ဖြစ်သဖြင့် Class (C) အား အသုံးပြုထားခြင်းဖြစ်သည်။

Private Network Address

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

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

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

Class B သည် အရွယ်အစားအလယ်အလတ်ရှိသော Network များအတွက် အသုံးပြုသည်။ Class B တွင် IP Address ၏ ပထမ octet ၂ ခုသည် Network ဖြစ်ပြီး ကျန် octets ၂ ခုသည် hosts ဖြစ်သည်။ ထို့ကြောင့် Networks 16002 ခုရှိပြီး Network တစ်ခုလျှင် hosts ပေါင်း 65025 ခုသုံးစွဲနိုင်သည်။ Class B Networks များတွင် Microsoft နှင့် Exxon တို့ ပါဝင်သည်။ ယင်းတို့မှလွဲ၍ ကျန်သူများဝင်ရောက် သုံးစွဲနိုင်ခြင်း မရှိပါ။

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

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

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

InterNIC မှသတ်မှတ်ချက်

Class Bit Allocation

A 0 Network Host

7 bits 24 bits

B 1 0 Network Host

14 bits 16 bits

C 1 1 0 Network Host

21 bits 8 bits

D 1 1 1 0 Multicasting Address

28 bits

E 1 1 1 1 Experimental

28 bits

Loopback 0 1 1 1 1 1 1 Unused

### Subnetting

Network တစ်ခုအတွင်း သေးငယ်သောအစုအဖွဲ့များအဖြစ် Network အစိတ်အပိုင်း ငယ်များ ထပ်မံခွဲခြားဖြစ်သည်။ ယင်းကဲ့သို့ဆောင်ရွက်ခြင်းအားဖြင့် လုံခြုံမှုကောင်းမွန်ခြင်း၊ IP address များပြုပြင်ထိန်းသိမ်းထားရှိနိုင်ခြင်း၊ မတူညီသော Physical media များ သုံးစွဲနိုင်ခြင်း၊ Network Traffic ထိန်းချုပ်ခြင်း၊ အနည်းဆုံးသုံးစွဲနိုင်သဖြင့် performance အများဆုံးရရှိစေခြင်း၊ သီးသန့် Network ဖြစ်စေခြင်းများ ဆောင်ရွက်နိုင်သည်။

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

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

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

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

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

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

11111111.11111111.11111111.110000  
N N N n

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

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

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

Network Number	Router Address	Broadcast Address
000 -- x.y.z.0	x.y.z.1	x.y.z.31
001 -- x.y.z.32	x.y.z.33	x.y.z.63
010 -- x.y.z.64	x.y.z.65	x.y.z.95
011 -- x.y.z.96	x.y.z.97	x.y.z.127
100 -- x.y.z.128	x.y.z.129	x.y.z.159
101 -- x.y.z.160	x.y.z.161	x.y.z.191
110 -- x.y.z.192	x.y.z.193	x.y.z..223
111 -- x.y.z.224	x.y.z.225	x.y.z.255

### Classless Internetwork Domain Routing(CIDR)

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

InterNIC Network type (CIDR)	Subnet Mask	Approximate Number of IP Address
Slash 8	255.0.0.0	16,000,000
Slash 12	255.240.0.0	1,000,000
Slash 16	255.255.0.0	65,536
Slash 20	255.255.240.0	4,096
Slash 21	255.255.248.0	2,048
Slash 22	255.255.252.0	1,024
Slash 23	255.255.254.0	512
Slash 24	255.255.255.0	256
Slash 25	255.255.255.128	128

Slash 26	255.255.255.192	64
Slash 27	255.255.255.224	32
Slash 28	255.255.255.240	16
Slash 29	255.255.255.248	8
Slash 30	255.255.255.254	4

#### Anding Method

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

192 . 168 . 0 . 5

11000000.10101000.00000000.00000101

255 . 255 . 255 . 192

11111111.11111111.11111111.11000000

-----  
11000000.10101000.00000000.00000000

ထို့ကြောင့် 192.168.0.0 (00) network ထဲတွင် ရှိသည်ကို သိနိုင်ပေသည်။

#### TCP/IP and the OSI Model

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

OSI	TCP/IP
Application Layer - 7	Application Layer - 5
Presentation Layer - 6	
Session Layer - 5	Transport Layer -4
Transport Layer -4	
Network Layer - 3	Internet Layer - 3
Data Link Layer - 2	Network Layer - 2
Physical Layer - 1	Physical Layer - 1

OSI Model တွင် higher layer မှလေ့လာလျှင် Application layer ၌ data base ၊ e-mail ၊ terminal-emulation programs များပါဝင်ပါသည်။ Presentation layer တွင် data များကို formatted ၊ presented ၊ converted နှင့် encoded များပြုလုပ်ပါသည်။ Session layer တွင် ဆက်သွယ်မှု နှင့် ပြုပြင်ထိန်းသိမ်းခြင်းများကို ပေါင်းစပ်ညှိနှိုင်း ပေးပါသည်။ Performing security ၊ logging နှင့် administrative functions များလိုအပ် ပါသည်။ Transport layer သည်

message များအလိုက်ပို့လွှတ်နေသော protocols များ၏ အမှားအယွင်းများကို စစ်ဆေးပေး ပါသည်။ Network layer သည် data-routing protocol များအလိုက် သတင်းအချက်အလက် များအား သက်ဆိုင်ရာ destination node သို့ မှန်ကန်စွာရောက်ရှိရေးဆောင်ရွက်ပေးသည်။ Data Link layer သည် node တစ်ခုမှ တစ်ခုသို့ data များစီးဆင်းမှု နှင့် တစ်ပြိုင်နက် data blocks များ မှန်ကန်စေရေး ဆောင်ရွက်ပေးသည်။ Physical layer သည် ဆက်သွယ်ရေးဆိုင်ရာ စက်မှုပိုင်းပစ္စည်းများဖြစ်သော transmission medium နှင့် Interface hardware များကို ဖော်ပြခြင်းဖြစ်သည်။

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

#### **Using the Address Resolution Protocol (ARP)**

ARP ၏ အဓိက function မှာ TCP/IP address မှ Physical address ခေါ် MAC(media access control) address သို့ broadcast လုပ်၍ပြောင်းလဲ ဖော်ပြပေးခြင်းဖြစ်သည်။ မိမိတို့ ကွန်ယက်အတွင်းရှိ server တစ်လုံး သို့မဟုတ် default Gateway တစ်ခုမှ မည်သည့် IP များ ကို frequently access လုပ်ပေးနေသည် ဆိုသော ARP table မှ Address list ကို ဖတ်ယူခြင်းဖြစ်သည်။ ပိုင်း ARP Table တွင် မည်သည့် IP သည် မည်မျှကြာအောင် access ဖြစ်နေသည်ဆိုသည်ကိုပါ သိရှိနိုင်သည်။ ထို့ကြောင့် ARP Table တွင် Dynamic entry နှင့် Static entry ယူ၍ နှစ်မျိုးပါဝင်နေသည်။ Dynamic Entry သည် Request လုပ်လာသော IP address ၏ MAC address ကို သိရှိပြီးဆိုသည်နှင့် တပြိုင်တည်း ARP Table တွင် ထည့်သွင်းဖန်တီးပြီး ဖြစ်သည်။ Static Entry သည် Dynamic Entry ကဲ့သို့ လုပ်ဆောင်ချက် တူညီသော်လည်း ပိုင်းလုပ်ဆောင်ချက်ကို ARP utility ကို အသုံးပြုပြီး Manually ဆောင်ရွက်ရသည်။ အထူးဂရုပြုရန်မှာ ARP Utility သည် Server base Network တွင်သာ အကျိုးဝင်မည် ဖြစ်သည်။

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

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

ARP -s inet\_addr eth\_addr [if\_addr]  
 ARP -d inet\_addr [if\_addr]  
 ARP -a [inet\_addr] [-N if\_addr]  
 -a Displays current ARP entries by interrogating the current protocol data. If inet\_addr is specified, the IP and Physical addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each ARP table are displayed.  
 -g Same as -a.  
 inet\_addr Specifies an internet address.  
 -N if\_addr Displays the ARP entries for the network interface specified by if\_addr.  
 -d Deletes the host specified by inet\_addr. inet\_addr may be wildcarded with \* to delete all hosts.  
 -s Adds the host and associates the Internet address inet\_addr with the Physical address eth\_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.  
 eth\_addr Specifies a physical address.  
 if\_addr If present, this specifies the Internet address of the interface whose address translation table should be modified. If not present, the first applicable interface will be used.  
 Example:  
 > arp -s 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.  
 > arp -a .... Displays the arp table.

နိဂုံး

Networking စာစောင်မှာ Windows Platform ပေါ်တွင် အခြေခံရေးသားထားခြင်းဖြစ်ပြီး Network Operator တစ်ဦးအတွက် Network Operation နှင့် Troubleshooting ဆောင်ရွက် နိုင်ရန်အတွက်ဖြစ်ပါသည်။ အခြားသော Platforms များအတွက်လည်း အခြေခံကျသဖြင့် Network Operator တစ်ဦးအနေဖြင့် မဖြစ်မနေသိရှိထားရမည့် အကြောင်းအရာ အချက် အလက် များ ဖြစ်ပြီး System Administrator / Network Administrator မရှိသည့် Network များကို တာဝန်ယူရသူအနေဖြင့် ကျွမ်းကျင်စွာသိရှိနားလည်စေရန်အတွက် ရည်ရွယ်ရေးသား ခြင်း ဖြစ်ပါသည်။