
بسم الله الرحمن الرحیم

RRAS in Windows Server ۲۰۰۳

پروژه درس مهندسی اینترنت

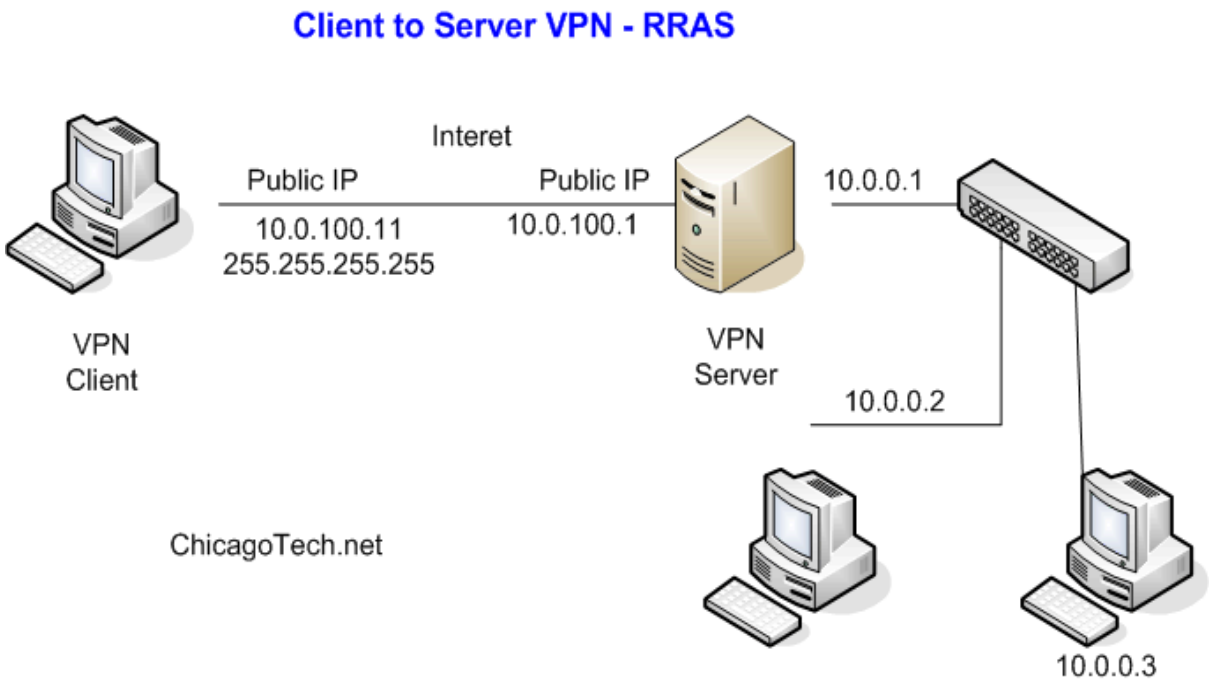
استاد محترم : غیاثی فرد

دانشجویان : محمد موسوی کیا
عباس کاشانی
غلامحسن عباسی
مهدی عزیزی

فهرست مطالب

RRAS دوکار اصلی را انجام می دهد. Remote و Routing

Remote : مثلا یک Mail Server داخلی داریم و کارمندان برای اینکه بتوانند Mail داخلی خود را چک کنند نیـاز دارنـد که به اداره Remote کنند. حال این ارتباط از طریق VPN و یا Dialup انجام می شود.



Routing: مثل IGMP – Network Router – Nat Router

RRAS را می توان با پیکر بندی های متفاوتی بکار برد. مثلا :

۱. RAS Server
۲. VPN Server
۳. Network Router
۴. DHCP Relay

مثلاً RRAS را بر روی RAS Server کانفیگ می کنیم :

شبکه ای با چندین زیر شبکه داریم و که هر سگمنت ۲۰۰ کلاینت دارد ،مشکل این است که تمام کلاینت های ما نیـاز دارنـد تا به شبکه خصوصی با استفاده از اتصال Dial Up (Private است) ،دسترسی داشته باشند.این کلاینت ها می خواهند با این کار ،ایمیل اشان را چک کنند و به منابع دسترسی داشته باشند.

راه حل : یک سرور ۲۰۰۳ که سرویس RRAS آن برروی RAS Server کانفیگ شده ، راه اندازی کنیم تا کلاینت ها بتوانند با شبکه ارتباط برقرار کنند.

Remote Access : ۱ .VPN (vpn server)

۲ .Dial Up(RAS Server)

Dial Up هزینه را بالا می برد زیرا :

۱. نیاز به چند مودم و خط تلفن دارد
۲. هزینه بالای تماس های از راه دور

RRAS به عنوان VPN Server: یک شبکه با ۵۰۰ کلاینت داریم.

مشکل قبلی را داریم ولی ارتباط از طریق اینترنت public است.

راه حل VPN Server است .

هزینه این کار : نیاز به پورت های نرم افزاری (VPN ای). ولی نیاز به خط تلفن نداریم. پس هزینه کمتر از قبل می باشد ولی باید VPN Server اینترنت پر سرعت داشته باشد و RAM های کافی تا بتوانند پورت های نرم افزای را ساپورت کنند.

RRAS به عنوان Network Router: یک شبکه با ۱۱۰ کامپیوتر داریم.

مشکل : ترافیک بر اثر نصب نرم افزارهای گوناگون ، بالا رفته و کارایی شبکه را کم کرده است.

راه حل : تقسیم شبکه به دو شبکه توسط روتر.(سگمنت AوB). روتر می تواند سخت افزاری (روترهای سیسکو) یا نرم افزاری (Win Server ۲۰۰۳ای که RRAS آن به عنوان یک روتر شبکه بر روی آن کانفیگ شده است).

سگمنت A دارای ۵۰ کامپیوتر و سگمنت B دارای ۶۰ کامپیوتر و نصب ۲ تا کارت شبکه در یک سرور ۲۰۰۳ و کانفیگ RRAS بر روی Network Router در سرور.

RRAS به عنوان NAT Router : یک شبکه با ۳۰۰ کلاینت داریم.

مشکل : اینکه تمام کلاینت ها دسترسی به اینترنت لازم دارند و ما به اندازه کافی IP Public در اختیار نداریم چون هزینه بالایی دارد.

راه حل : کانفیگ NAT در RRAS .اختصاص IP Private به تمام کلاینت های شبکه توسط واسط NAT .

دریافت چند IP Public از ISP و سپس تخصیص آنها بر روی واسط عمومی NAT .

انواع روتر :

روترها در لایه ۳ مدل OSI کار می کنند و در شبکه TCP/IP ترافیک IP ها را کنترل می کنند.

دو نوع روتر **سخت افزاری** و **نرم افزاری** داریم که نوع نرم افزاری آن مانند سرور ۲۰۰۳ که در آن سرویس RRAS به همراه پروتکل ها و واسط هایی مانند OSPF و RIP کانفیگ شده است.

سخت افزاری هم مثل روترهای سیسکو که دستورات کانفیگ بیشتری دارد. دو پروتکل آن EIGRP-IGRP

در WAN های بزرگ که ترافیک خیلی زیادی نداریم ممکن است یک روتر نرم افزاری کافی باشد مثل ISDN ولی اگر یک WAN با ترافیک بالا باشد باید از روترهای سخت افزاری که با دستورات خاص کانفیگ شده اند بهره ببریم. مانند سیسکو

مسیرها

روترها دارای یک جدول ذخیره سازی اطلاعات مسیر در زمان مسیریابی هستند.مثلاً برای رفتن به شبکه شماره ۲ باید از اینترفیس ۱ استفاده کند.

یک سری دستورات برای کار با این جداول وجود دارد .مانند دستور : route delete

تعیین مسیرها می تواند به دو صورت دستی (static) و داینامیک باشد که در روش استاتیک خیلی هوشمندانه نیست و به این دلیل در شبکه های کوچک استفاده می شود ولی روش داینامیک در شبکه های بزرگ صورت می گیرد.

داینامیک مانند : OSPF,EIGRP,IGRP,RIP

پروتکل هایی که RRAS ساپورت می کند : IP,TCP/IP,Apple Talk ولی IPX را ساپورت نمی کند.

Hop مسیری است که داده در آن توسط Router انتقال پیدا می کند.

Backbone خطوط ارتباطی اینترنت در فواصل زیاد می باشند که برای وصل شدن به خطوط با ظرفیت کمتر طراحی شده اند. اینترنت از تعداد زیادی از این Backbone ها تشکیل می شود.

RRAS Interfaces (Network Interface):

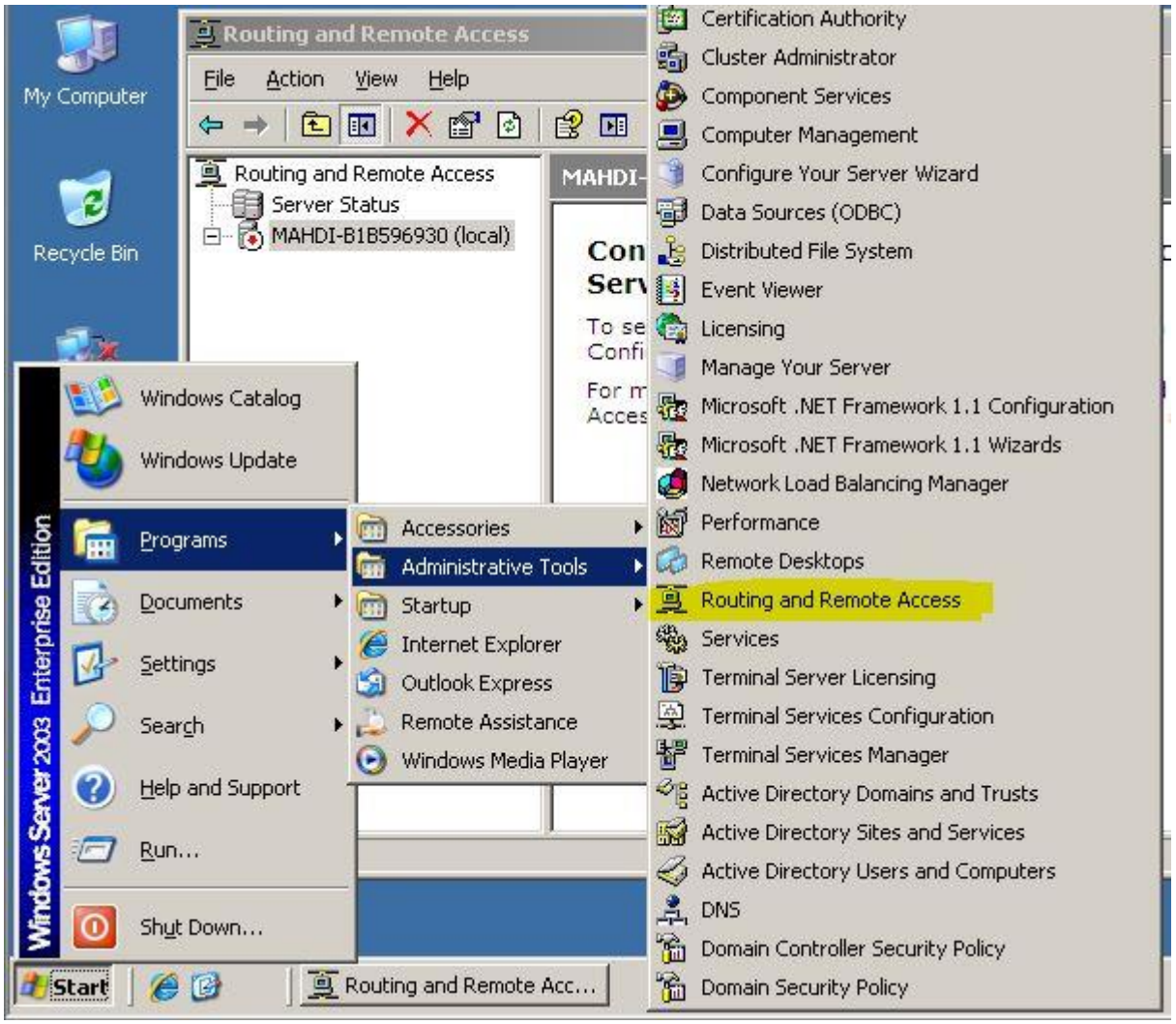
هر جا که ترافیک بین کلاینت های RAS و RAS Server قادر به عبور کردن باشد را RRAS Interfaces گویند.

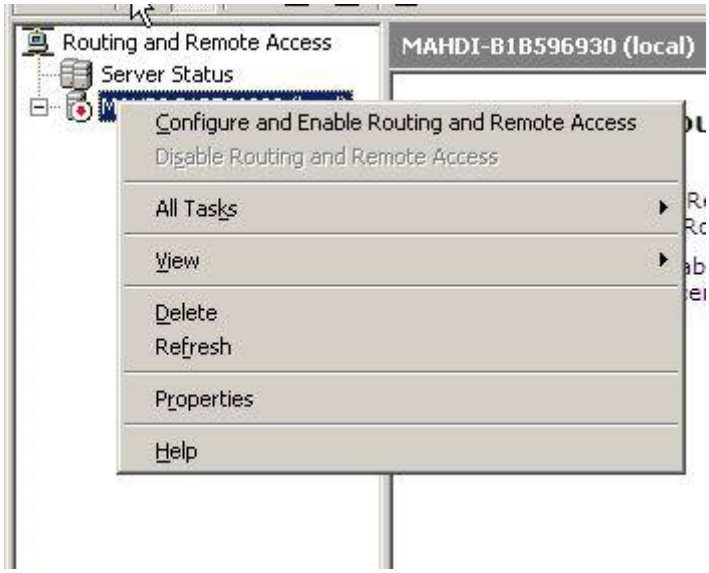
دو نوع دارد :

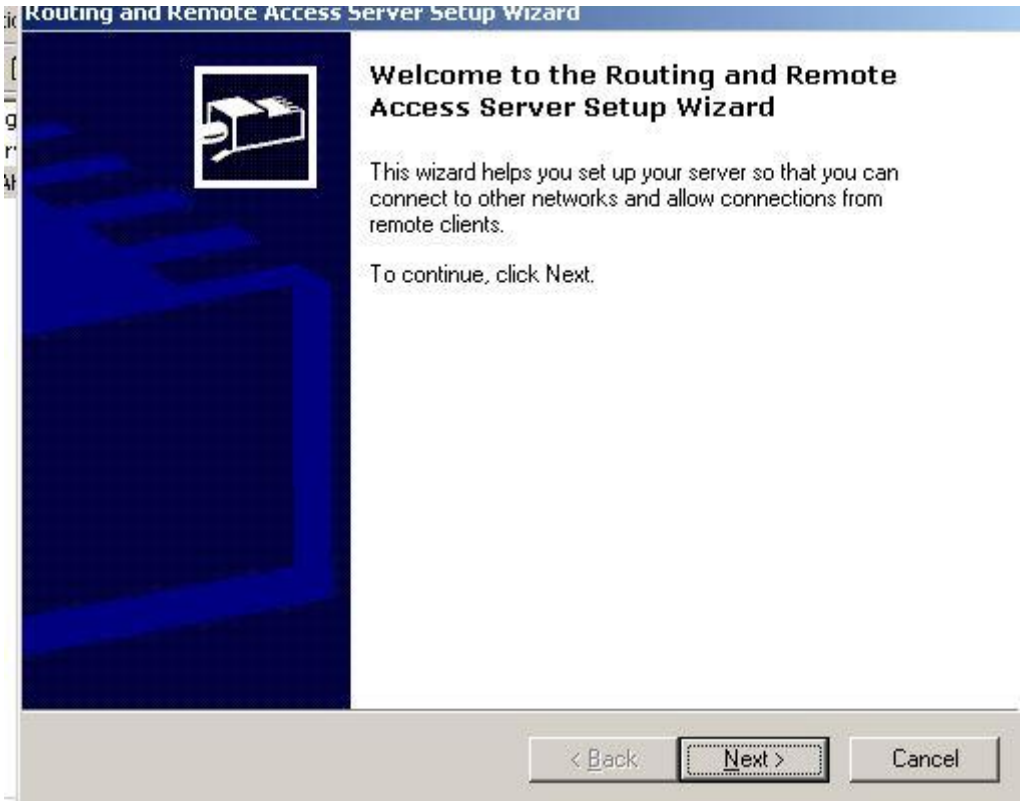
۱- فیزیکی : مودم ، کارت شبکه ای که توسط سرور ۲۰۰۳ شناسایی می شود.

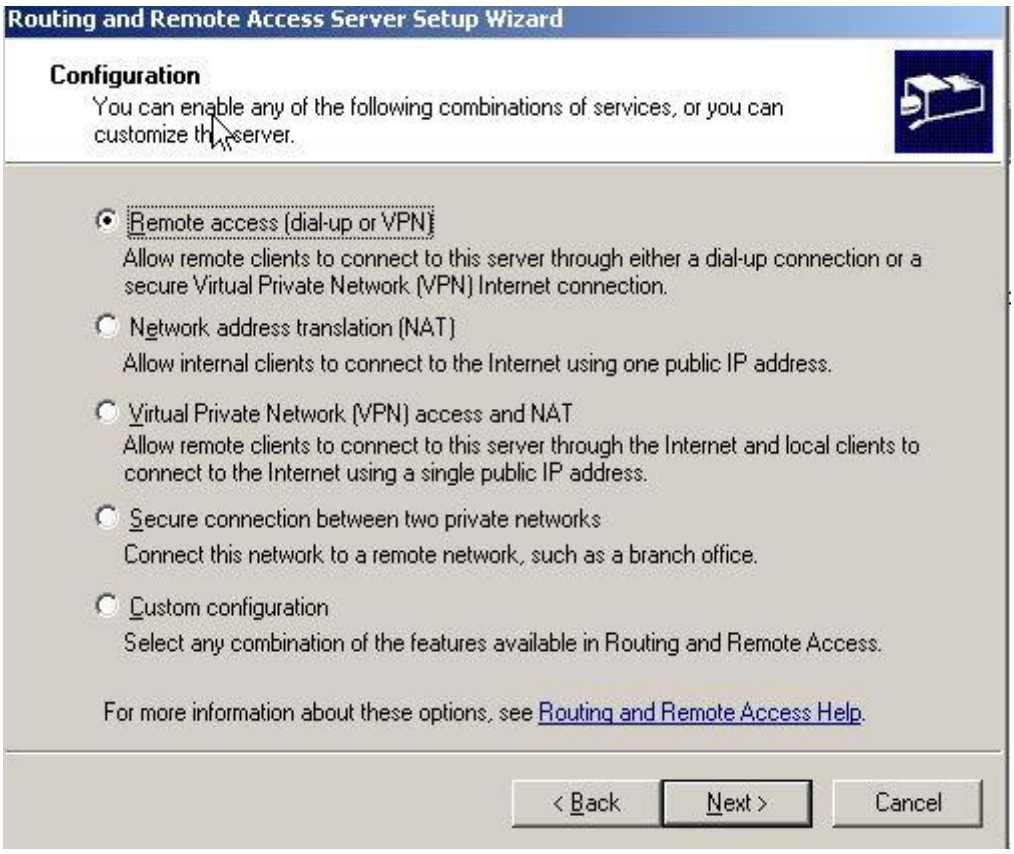
۲- اینترفیس های نیازمند به شماره گیری که از Dial Up یا VPN استفاده می کنند.

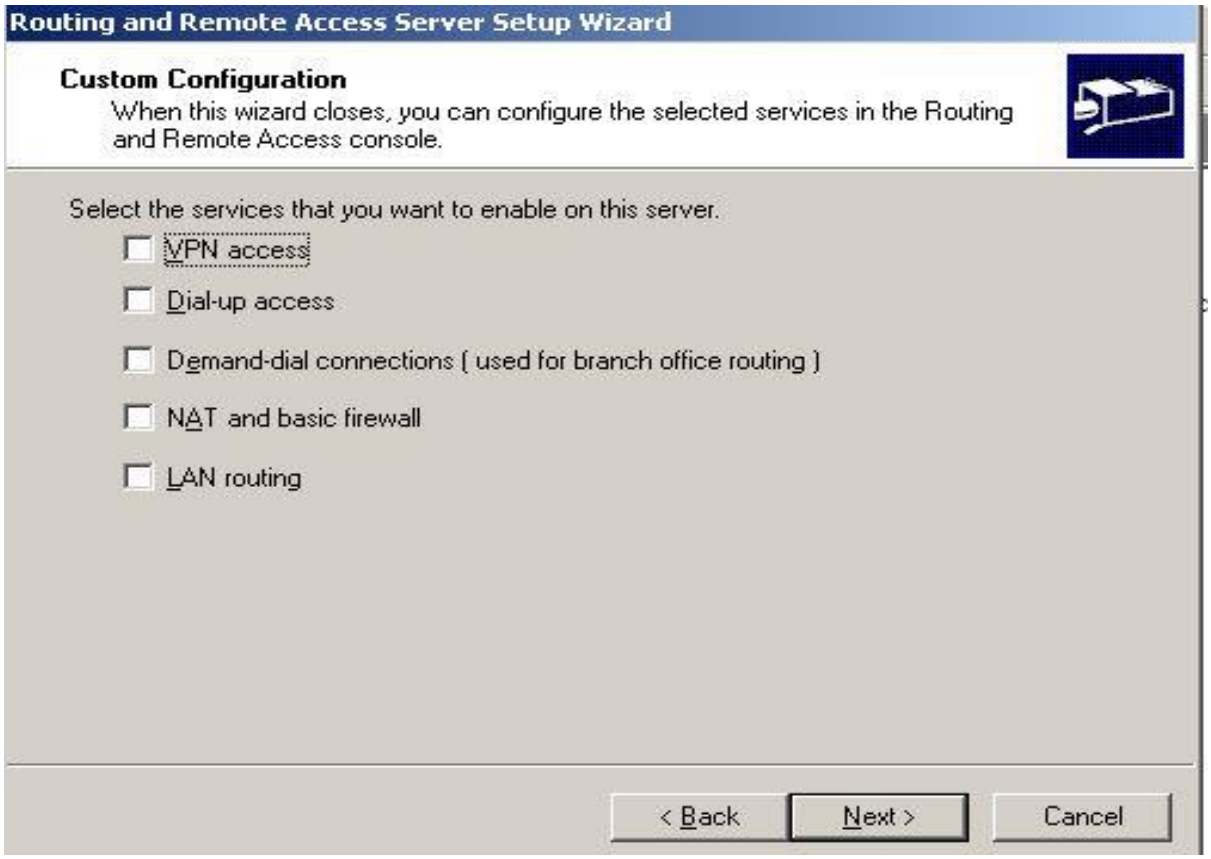
کانفیگ کردن RRAS :

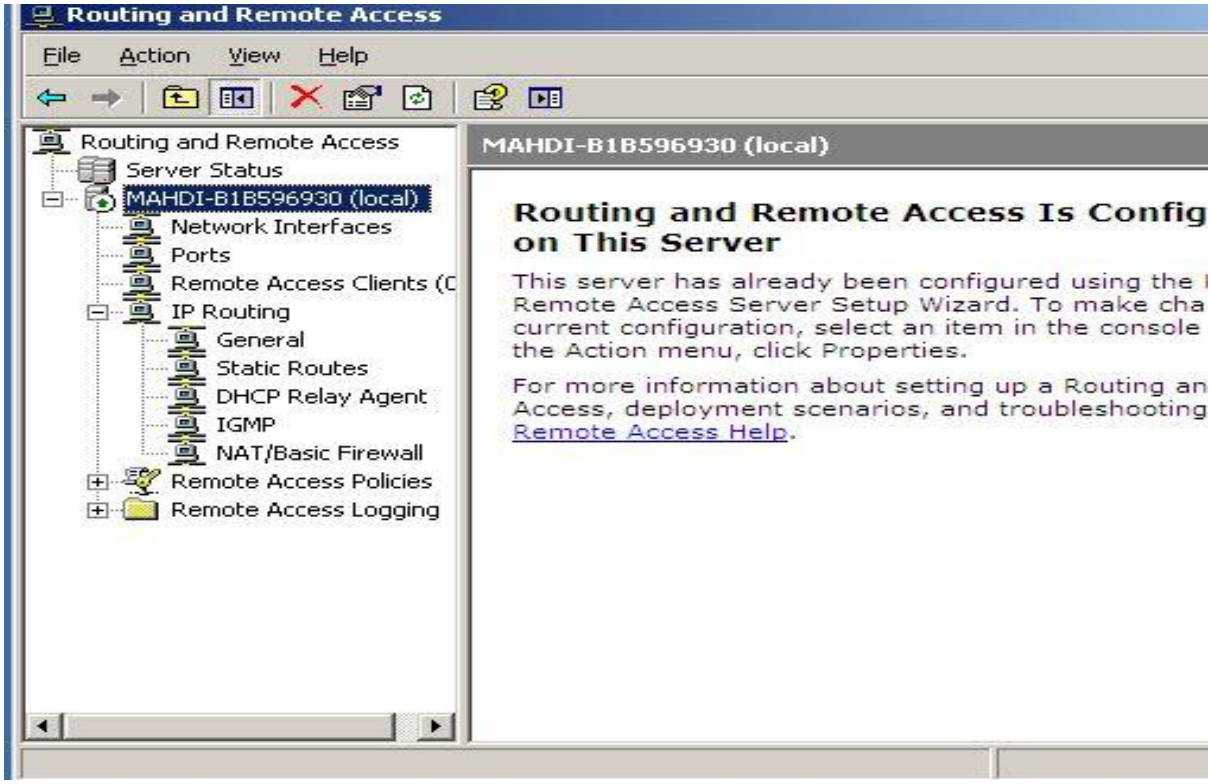



Routing and Remote Access
Server Status
MAHDI-B1B596930 (local)
Configure and Enable Routing and Remote Access
Disable Routing and Remote Access
All Tasks
View
Delete
Refresh
Properties
Help


Routing and Remote Access Server Setup Wizard
Welcome to the Routing and Remote Access Server Setup Wizard
This wizard helps you set up your server so that you can connect to other networks and allow connections from remote clients.
To continue, click Next.
< Back
Next >
Cancel


Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize th server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure Virtual Private Network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual Private Network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
For more information about these options, see Routing and Remote Access Help.
< Back
Next >
Cancel


Routing and Remote Access Server Setup Wizard
Custom Configuration
When this wizard closes, you can configure the selected services in the Routing and Remote Access console.
Select the services that you want to enable on this server.
VPN access
Dial-up access
Demand-dial connections (used for branch office routing)
NAT and basic firewall
LAN routing
< Back
Next >
Cancel

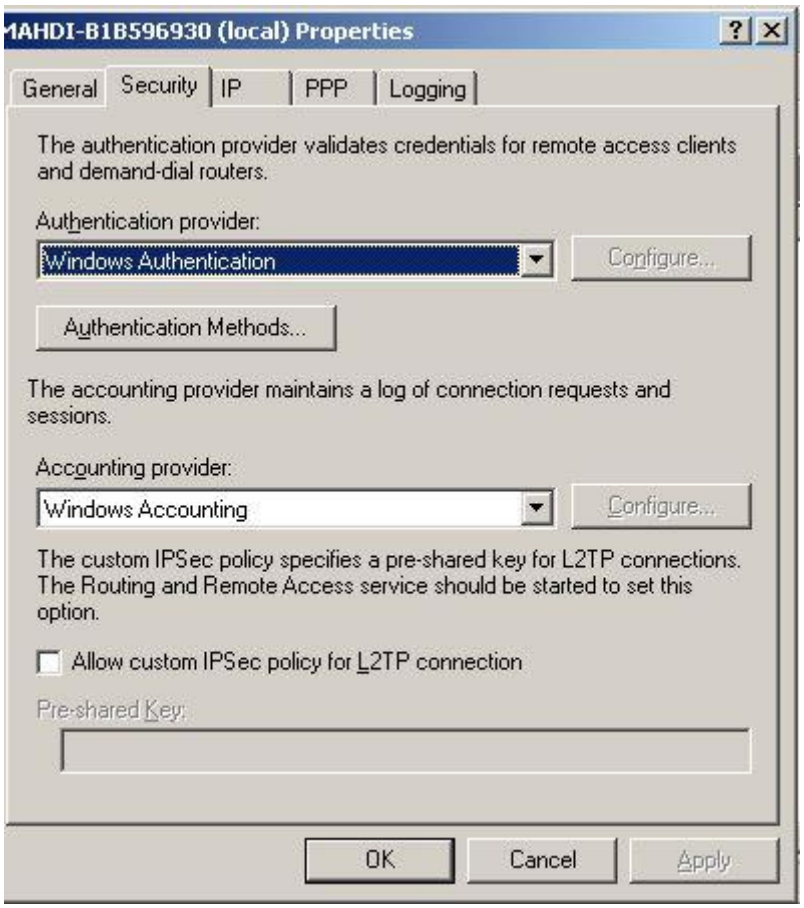


کادر properties مختص به RRAS :

دارای TABهای : **General-Security-IP-PPP-Logging**

در **تب General** می توان این کامپیوتر را بـه عنـوان Router(LAN & demand-dial) و Remote Access Server فعال کرد.

در **تب Security** می توان Authentication ها را تنظیم کرد. مثل IAS و متدهای آن مثل EAP و MS Chap V۱,V۲ EAP(Extensible Authentication Protocol) که بین RAS Server , RAS Client مذاکره انجام می دهـد. حتـی شرکت های third party می تواند EAP را متناسب با خود بنویسد.



دو نوع EAP :

۱. EAP-TLS
۲. EAP-MD۵

TLS(Transport Level Security) :

داده ها را رمزگذاری می کند ولی در شبکه work group ای که RAS دارد ساپورت نمی شود.

TLS از SSL اسـتفاده مـی کنـد. تشـخیص هویـت TLS بصـورت دوطرفـه یـا mutual اسـت.یعنی هـم سـرور، کلاینـت را Authentication می کند و هم کلاینت ، سرور را.

MS Chap , TLS بین سرور و کلاینت رمزگذاری داده را انجام می دهد .حال اگر سرور به یـک شـبکه خصوصـی دیگـر نیـز متصل باشد و کلاینت RAS بخواهد از طریق سرور RAS با آن شبکه خصوصی نیز ارتباط داشته باشد ، برای رمزنگاری داده از IP Security استفاده می کنیم.

رمزنگاری داده در زمان اتصال RAS Client , RAS Server با اتصال از راه دور به نـام SEK(Secret Encryption) Key شناخته می شود.

SEK در زمانی که فرآیند تشخیص هویت برقرار شده ، تولید می شود.

در اتصالات از راه دور دو نوع رمزنگاری داریم :

۱. MPPE(Microsoft)

از RSA استفاده می کند با رمزنگاری هایی به طول ۴۰bit,۵۶bit,۱۲۸bit

۲. DES & ۳DES

DES از کلید ۵۶bit و ۳DES سه تا کلید که هر کدام ۵۶ بیت اند بر روی ویندوزها و کلاینت های VPN است کـه در IP Security تولید می شوند.

MS Chap یک طرفه است ولی MS Chap V۲ دو طرفه است.

SPAP خیلی قدیمی است . PAP خیلی مطمئن نیست و اتصالات را هم رمزنگاری نمی کند.

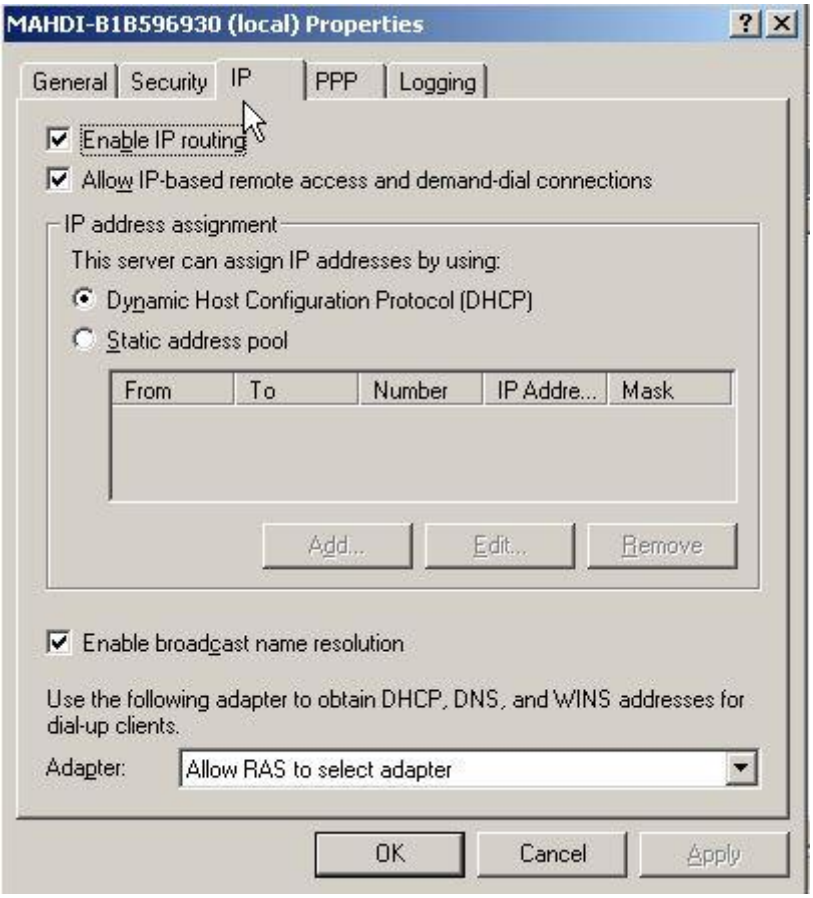
تا اینجا پروتکل های Authentication را بررسی کردیم.

تب IP :

می توان در آن به RAS Client ها اجازه داد تا به منابع LAN دسترسی داشته باشند یا نداشته باشند و همین طـور در مـورد RAS Client ها و اتصالاتی که نیازمند به شماره گیری هستند با RAS Server ارتباط داشته باشند یا نه.

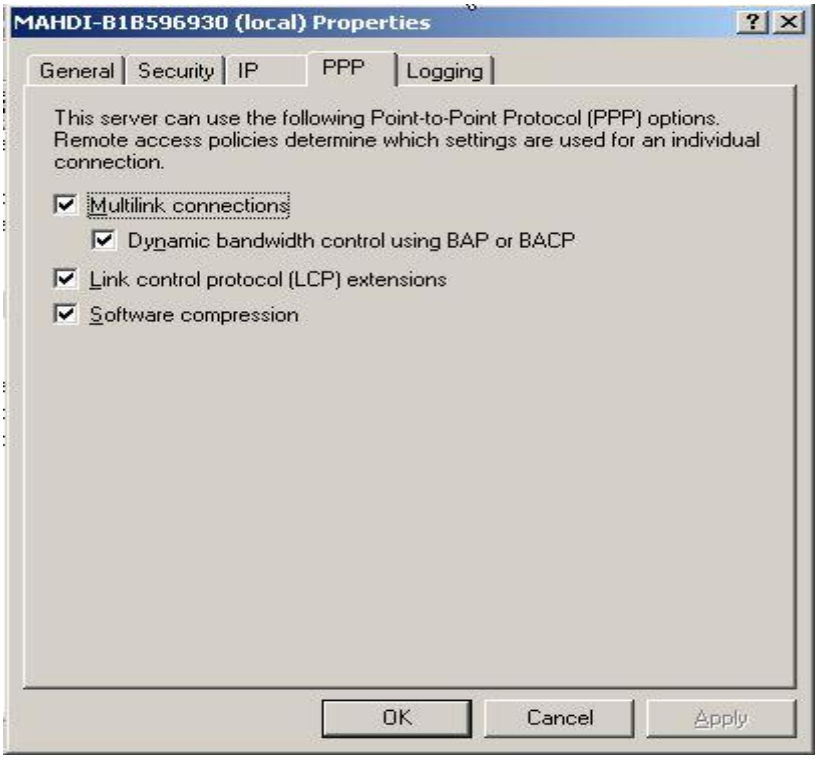
می توان نوع تخصیص IP را تعیین کرد که آیا توسط DHCP انجام شده یا به صورت دستی (static) به این منظور که RAS Client هایی که IP گرفتند بتوانند وارد شبکه شوند.

در این تب می توان به RAS Client ها اجازه تفکیک اسامی منابع و نام کامپیوترها را داد.



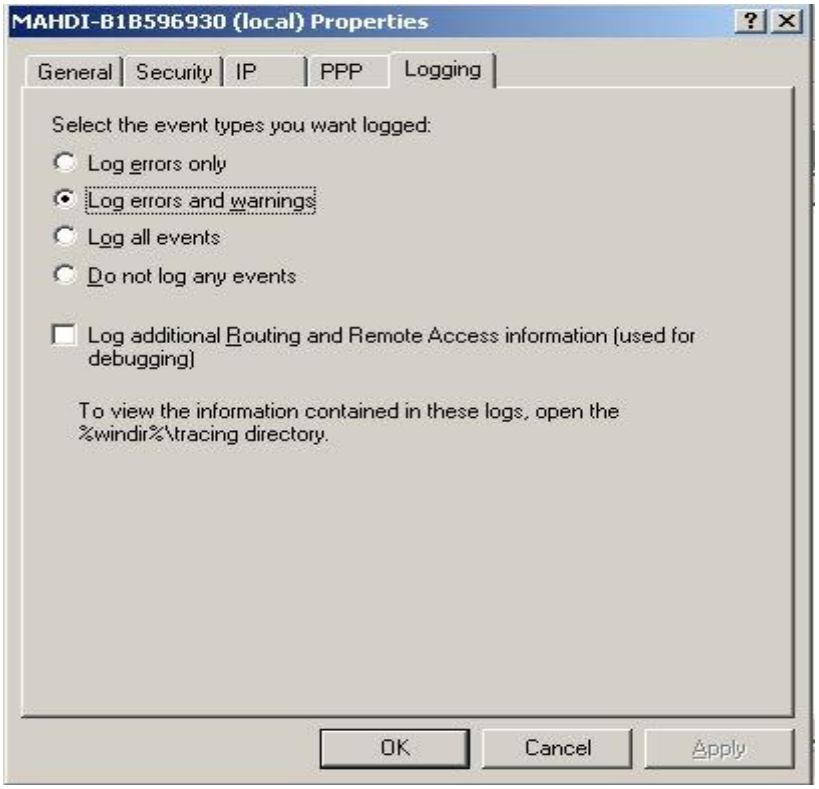
تب PPP :

می توان از چندین اتصال برای بالا بردن سرعت بین کاربر و سرور بهره برد و پهنای باند را کنترل کرد. می تـوان بـرای بهبـود ارتباط LCP را SET کرد و داده های انتقالی را برای کارایی بیشتر فشرده کرد.(PAP فقط پسور ندارد)

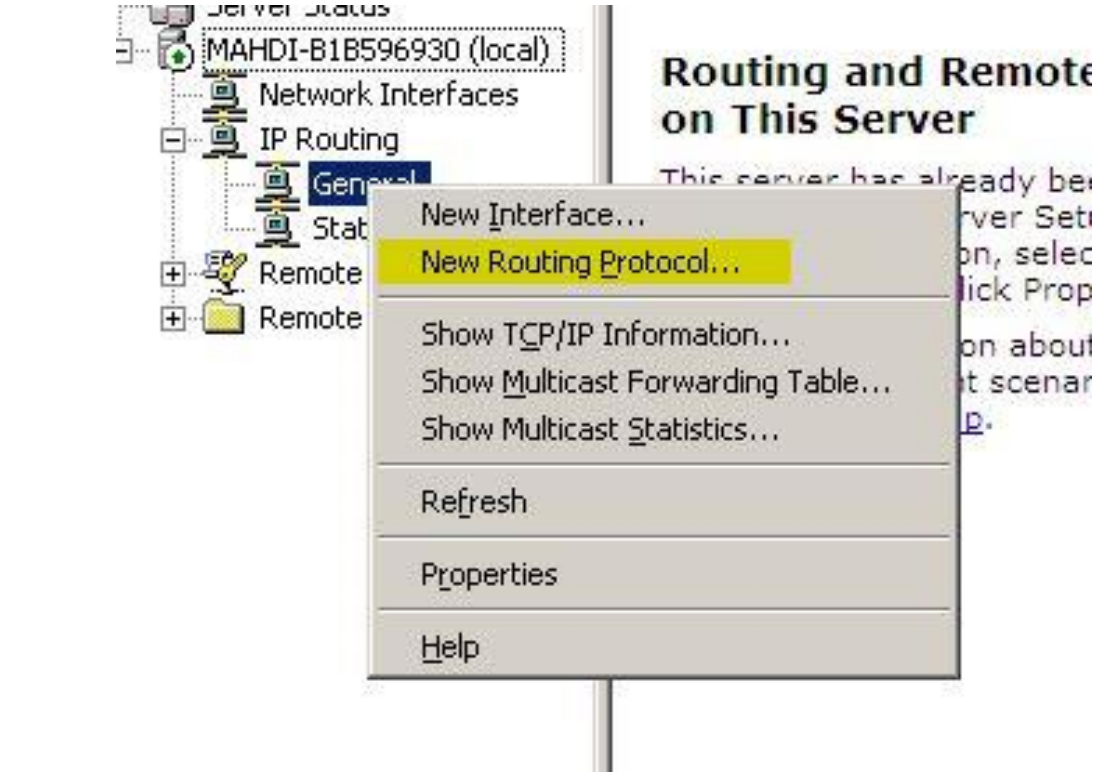


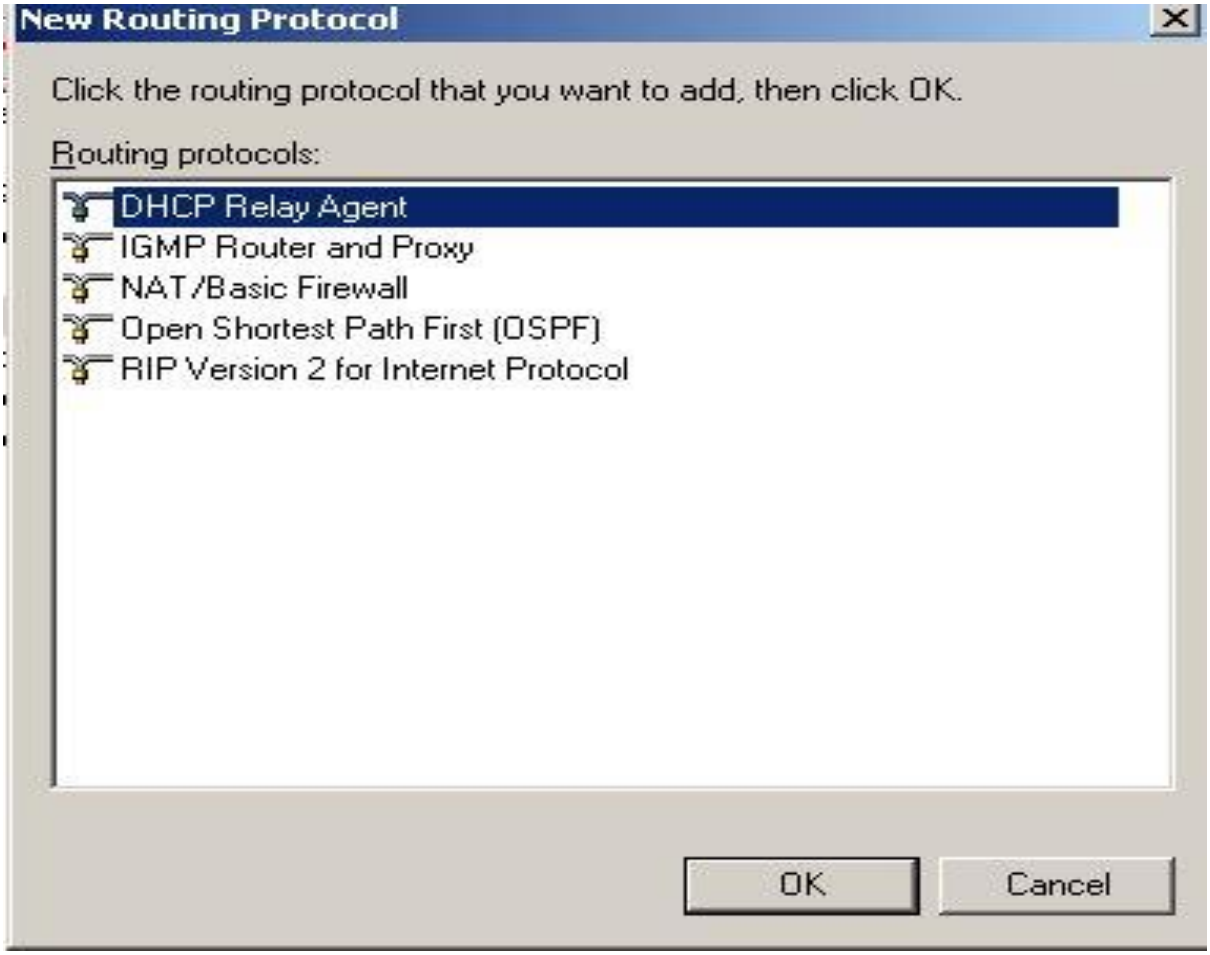
تب Logging :

تمام Log ها به صورت System Log نوشته می شوند.(برای تنظیمات و خطا یابی)



پنجره پروتکل های مسیریابی RRAS





پیکربندی NAT :

ترجمه IP شخصی به عمومی در اینترنت است که سه کامپوننت مختص به خود دارد :

۱- Translation : تبدیل IP ها به شماره پورت های TCP/UDP های مختص به پکتی که در حال انتقال بین اینترنت و شبکه خصوصی اند.

۲- Addressing : می توان به سادگی با یک DHCP Server به کامپیوترها IP,subnet mask,Gateway,IP DNS را اختصاص داد.

۳- Name Resolation :NAT می تواند مانند یک DNS Server عمل کند.(در کامپوننت قبلی مانند DHCP Server عمل کرد.)

کامپیوتر NAT از طریق RRAS کانفیگ می شود که شامل حداقل دو اینترفیس برای کانفیگ کردن NAT است :

۱. Public : برای اتصال به شبکه اینترنت

۲. Private : برای اتصال به شبکه خصوصی

نکته اینکه از IP Private ها نمی توانید برای اینترنت استفاده کنید.

IP Privateها سه تا رنج دارند:

A) ۱۰,۰,۰,۰ Subnet : ۲۵۵,۰,۰,۰

(۱۰,۰,۰,۱ to ۱۰,۲۵۵,۲۵۵,۲۵۴)

B) ۱۷۲,۱۶,۰,۰ Subnet : ۲۵۵,۲۴۰,۰,۰

(۱۷۲,۱۶,۰,۱ to ۱۷۲,۳۱,۲۵۵,۲۵۴)

C) ۱۹۲,۱۶۸,۰,۰ Subnet : ۲۵۵,۲۵۵,۰,۰

(۱۹۲,۱۶۸,۰,۱ to ۱۹۲,۱۶۸,۲۵۵,۲۵۴)

رنج B,C کابردی تر هستند.

مثالی برای چگونگی عملکرد NAT :

شبکه ای خصوصی با رنج (۱۹۲,۱۶۸,۰,۱ to ۱۹۲,۱۶۸,۰,۱۰۰) در نظر می گیریم. باید یک IP Public برای این شبکه مانند (w۱,x۱,y۱,z۱) از ISP خریداری کنیم.

اگر یکی از کاربران داخل شبکه خصوصی آدرس سایتی را وارد نماید که همان IP Web Server مقصد است مانند w۲,x۲,y۲,z۲ که IP Public است NAT تمام IP Private ها را به همان IP Public خریداری شده تبدیل کرده و سبب بر قراری ارتباط می شود و به همین صورت ولی برعکس IP Public توسط NAT به IP Private تبدیل می شود.
تمامی اطلاعات در جدولی به نام NAT Mapping Table ذخیره و نگهداری می شود.

چگونگی Translate IP در NAT :

NAT با استفاده از سه آیتم زیر این عمل را انجام می دهد :

۱- آدرس های IP ای که در IP Header هستند.
۲- شماره پورت های TCP ای که در TCP Header هستند.
۳- شماره پورت های UDP ای که در UDP Header هستند.

NAT از دید طراحی :

۱. Private Network Addressing : برای تعیین IP های شبکه خصوصی باید از سه رنج یکی را انتخاب کنیم ، ولی به صورت پیش فرض NAT از رنج ۱۹۲,۱۶۸,۰,۰ با ۲۵۵,۲۵۵,۲۵۵,۰: subnet استفاده می کند.
۲. Single or Multiple Public IP : اگر از چند IP Public استفاده می کنید، باید اینترفیس NAT Public را با رنجی از این IP ها کانفیگ کنید که NAT بتواند تبدیل IP ها را انجام دهد.
۳. Allowing Inbound Connections : برای اینکه به کاربران اینترنتی اجازه دسترسی به منابع شبکه خصوصی را بدهیم باید ابتدا روی سروری که منابع روی آن قرار دارد IP دستی کانفیگ کنیم.(سرور به وسیله DHCP به منابع IP می دهد.) سپس IP برای DNS,Gateway به آن می دهیم. بعد IP های منابع را حذف و در آخر یک پورت مخصوص کانفیگ می کنیم. یک پورت خاص یک نگاشت دستی است که برای آدرس و پورت عمومی به یک آدرس و پورت شخصی اعمال شده است. در واقع اتصال ورودی یک کاربر اینترنت را به یک آدرس خاص روی شبکه شما نگاشت می کند. با پورت خاص می توان یک وب سرور روی شبکه شخصی ایجاد کرد که از طریق اینترنت در دسترس باشد. در اینجا امنیت مهم است.زیرا شما با این پورت خاص می خواهید کاربران خارجی اطلاعات وب سرور را مشاهده کنند و نمی خواهید به منابع دیگری دسترسی داشته باشند. حتی با این پورت می توانید کاربران خارجی و داخلی به یک برنامه (بازی) ارتباط دهید.

۴. SOHO : VPN Connections from a Translate SOHO(Small Office or Home Office) یک اینترانت برای یک شبکه داخلی و شخصی استفاده می شود و می بایست از پروتکل های PPTP استفاده شود و یک اتصال VPN از یک میزبان روی شبکه SOHO به سرور VPN روی شبکه داخلی روی اینترنت ایجاد کرد .

پروتکل مسیریابی NAT یک NAT Editor برای کنترل ترافیک PPTP دارد ولی پروتکل L۲TP در اتصالات IP SEC بر روی کامپیوتر NAT کار نمی کنند.

راه اندازی NAT در شبکه SOHO :

کانفیگ کردن :

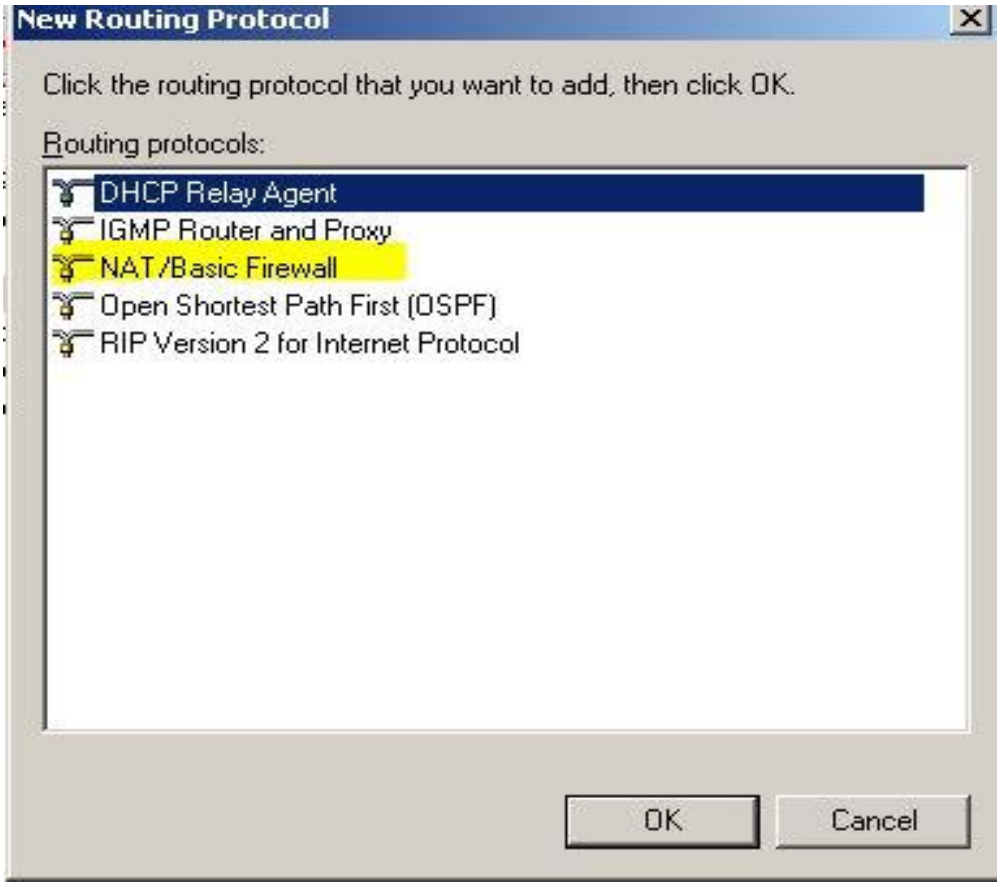
۱- NAT Router

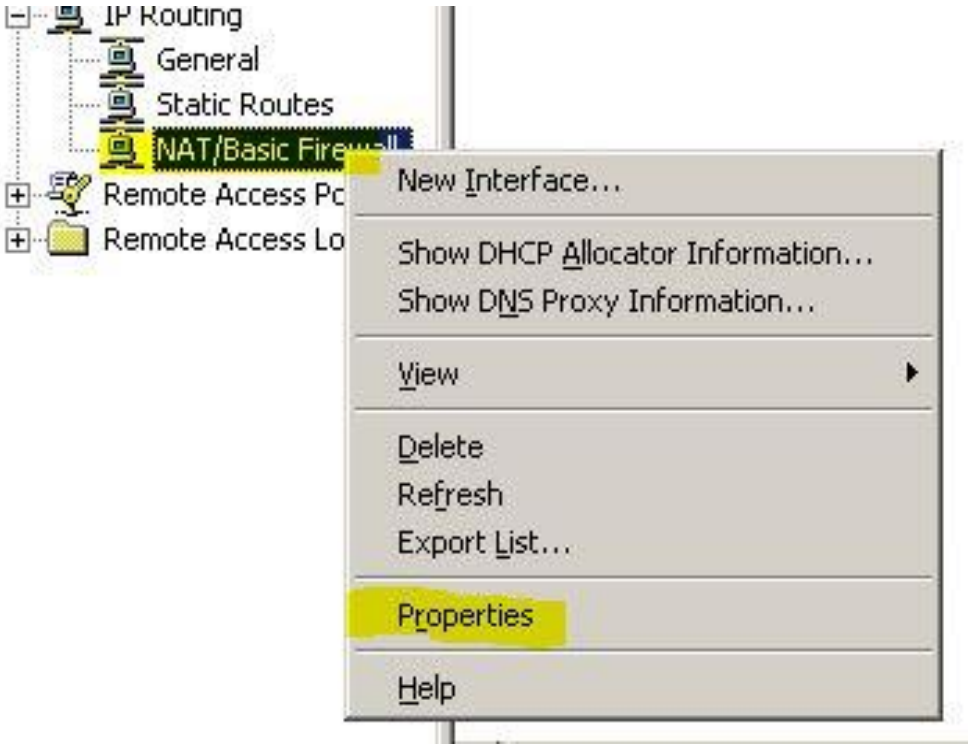
۲- کامپیوترهای کلاینت روی شبکه خصوصی بوسیله APIA .

NAT Router همان سرور ۲۰۰۳ است که حداقل دو اینترفیس شخصی و عمومی دارد.

سپس باید NAT و پروتکل هایش را کانفیگ کرد.

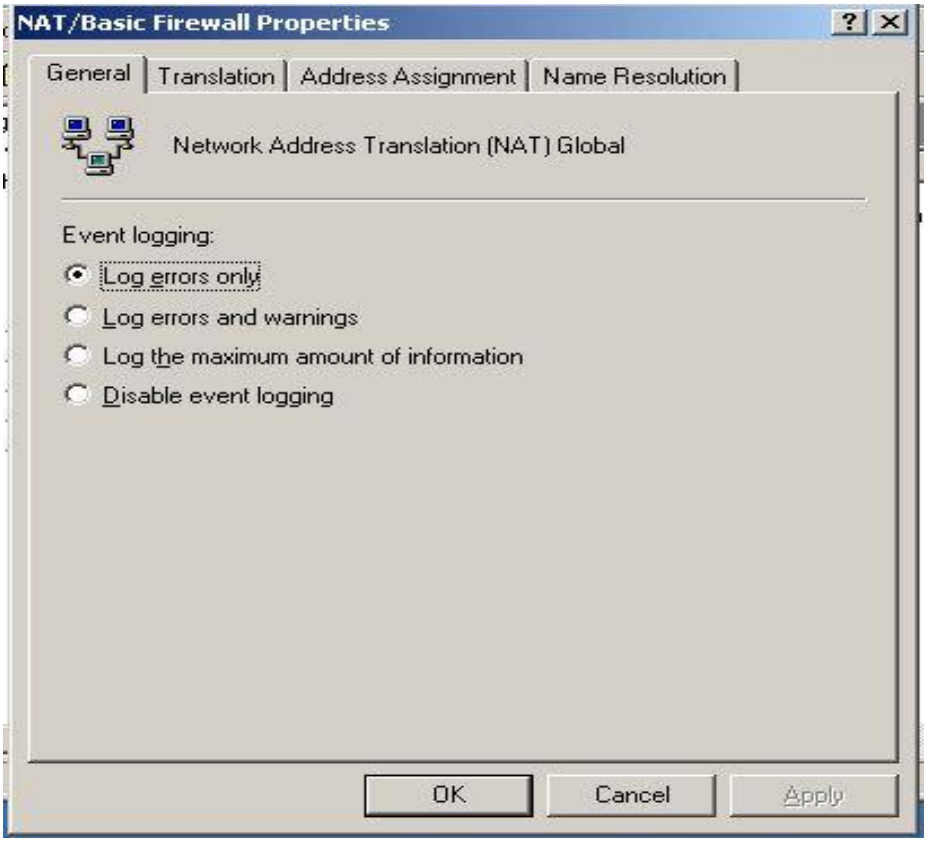
APIA(Automatic Private IP Addressing) که در اینجا NAT مانند یک DHCP عمل می کند و IP های پیش فرض مانند DNS,Gateway را به آن ها می دهد.



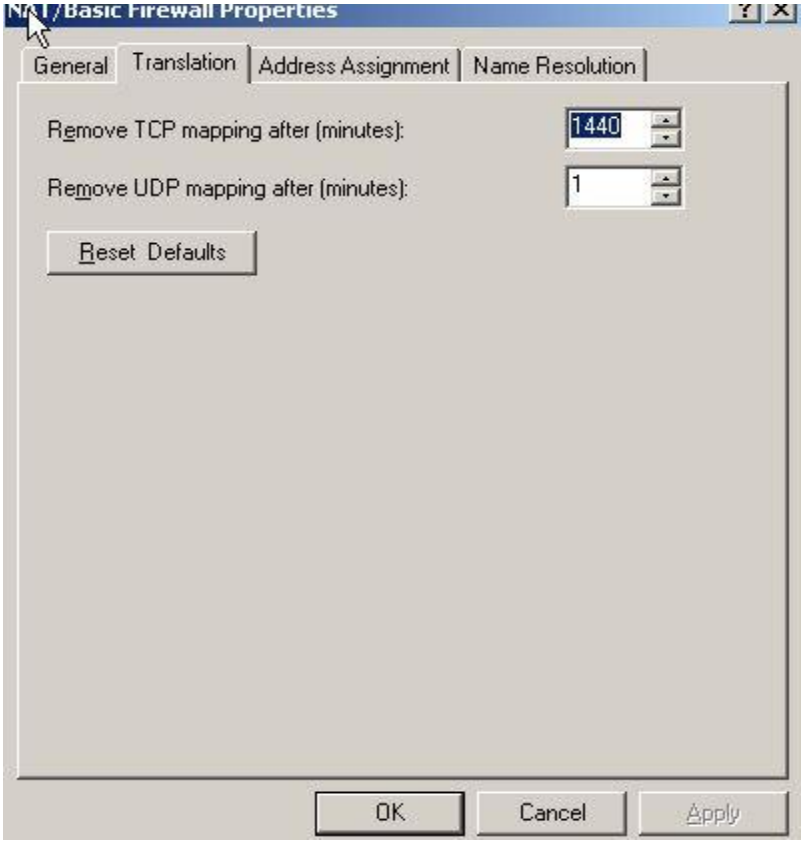


پنجره خصوصیات Nat دارای ۴ تب است : General,Translation,Address Assignment,Name Resolation

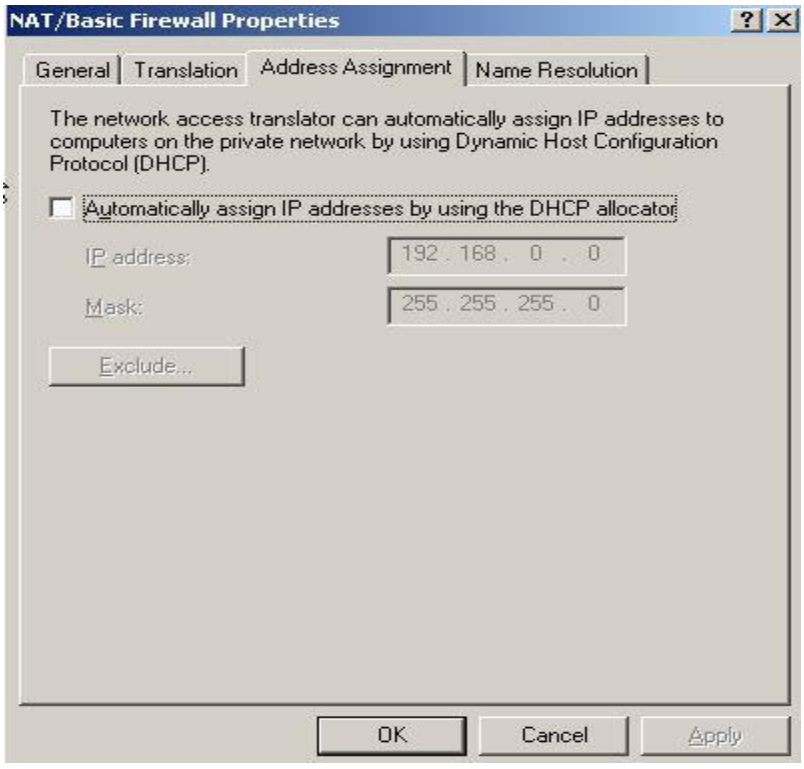
در **General** می توان Log ها و اورها را ثبت کرد.



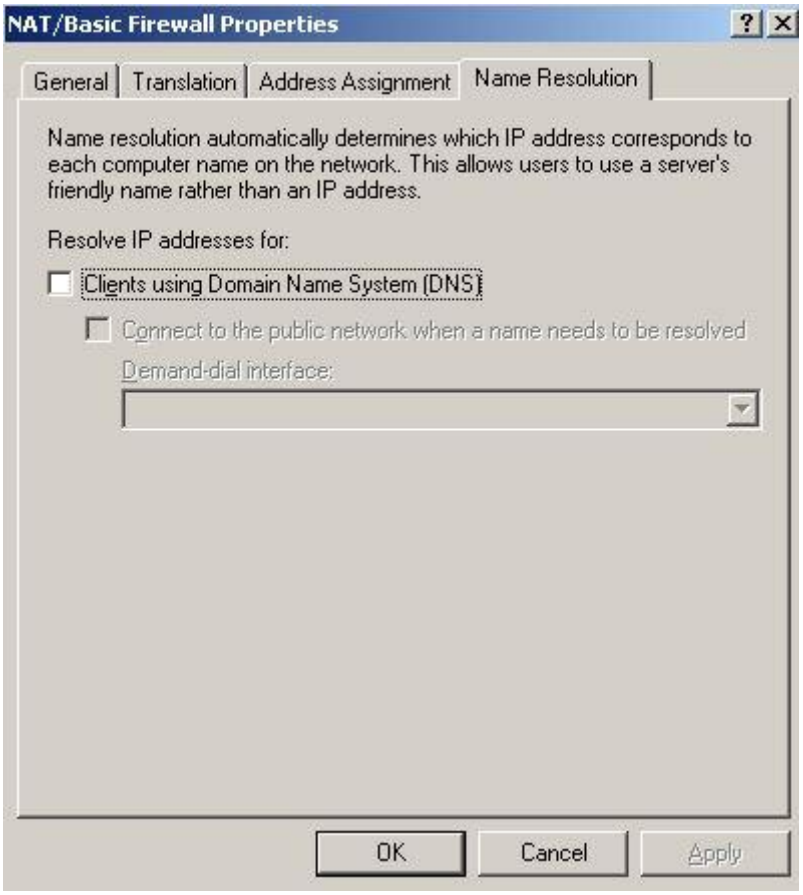
در **Translation** که می تواند جدول Mapping را پاک کند. مانند : TCP,UDP که میتوان گفت بر فرض مثال بعـد از دو دقیقه پاک شود.



در تب **Address** هم می توان آدرس DHCP Server را برای آدرس دهی به node ها را داد.



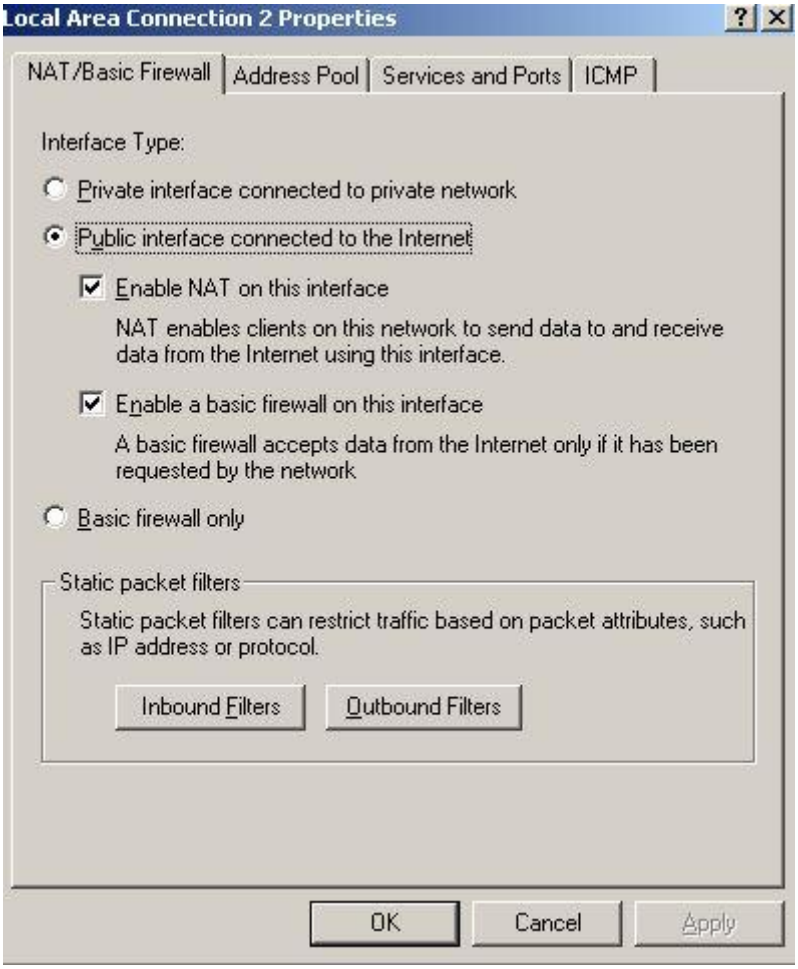
در تب **Name** وقتی که به تفکیک اسامی نیاز داریم می توان به شبکه Public متصل شد و از یک DNS بهره برد.

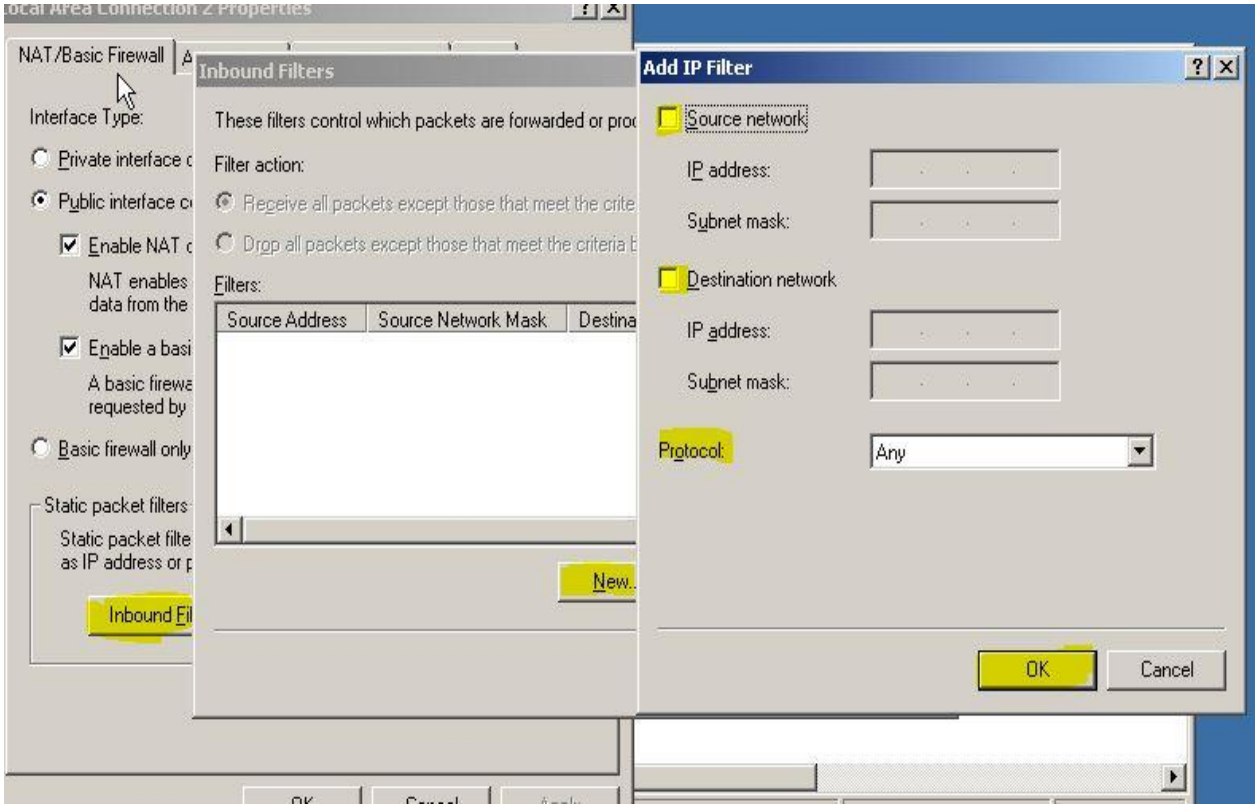


اینترفیس های NAT هم یک کادر خصوصیات دارند که می تـوان Public , Private یـا فقـط basic firewall را روی آن تنظیم کرد. در صورتی که خصوصی باشد فقط یک تب Basic دارد ولی اگر عمومی باشد به همراه Basic ، چهار تب دارد:

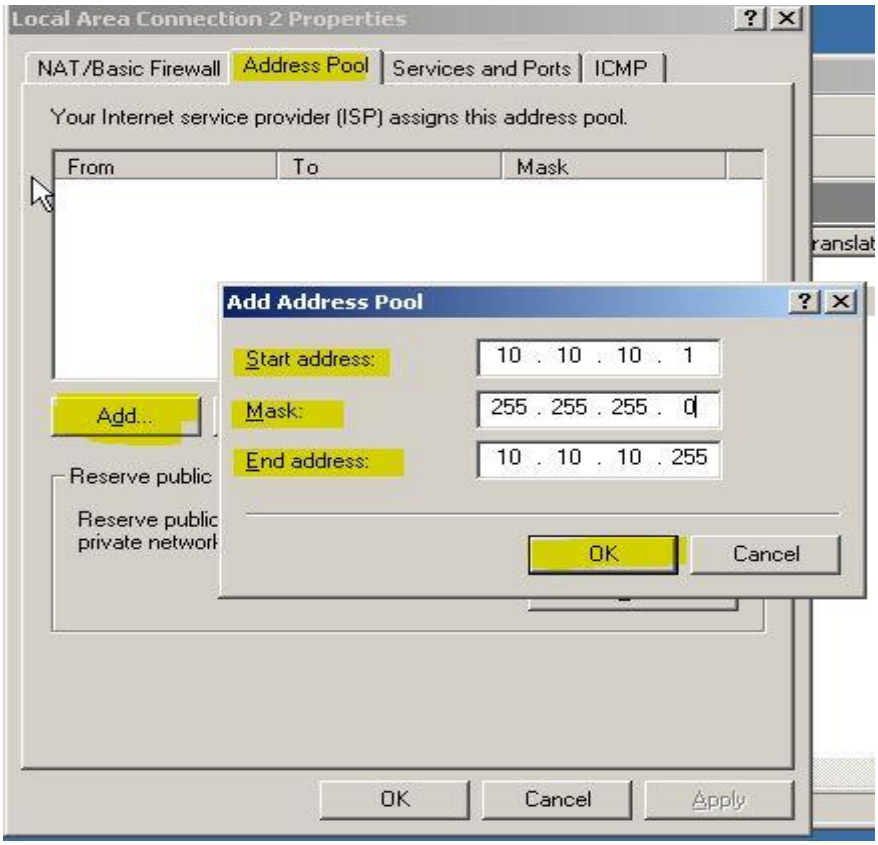
Address Pool , Service & Port , ICMP

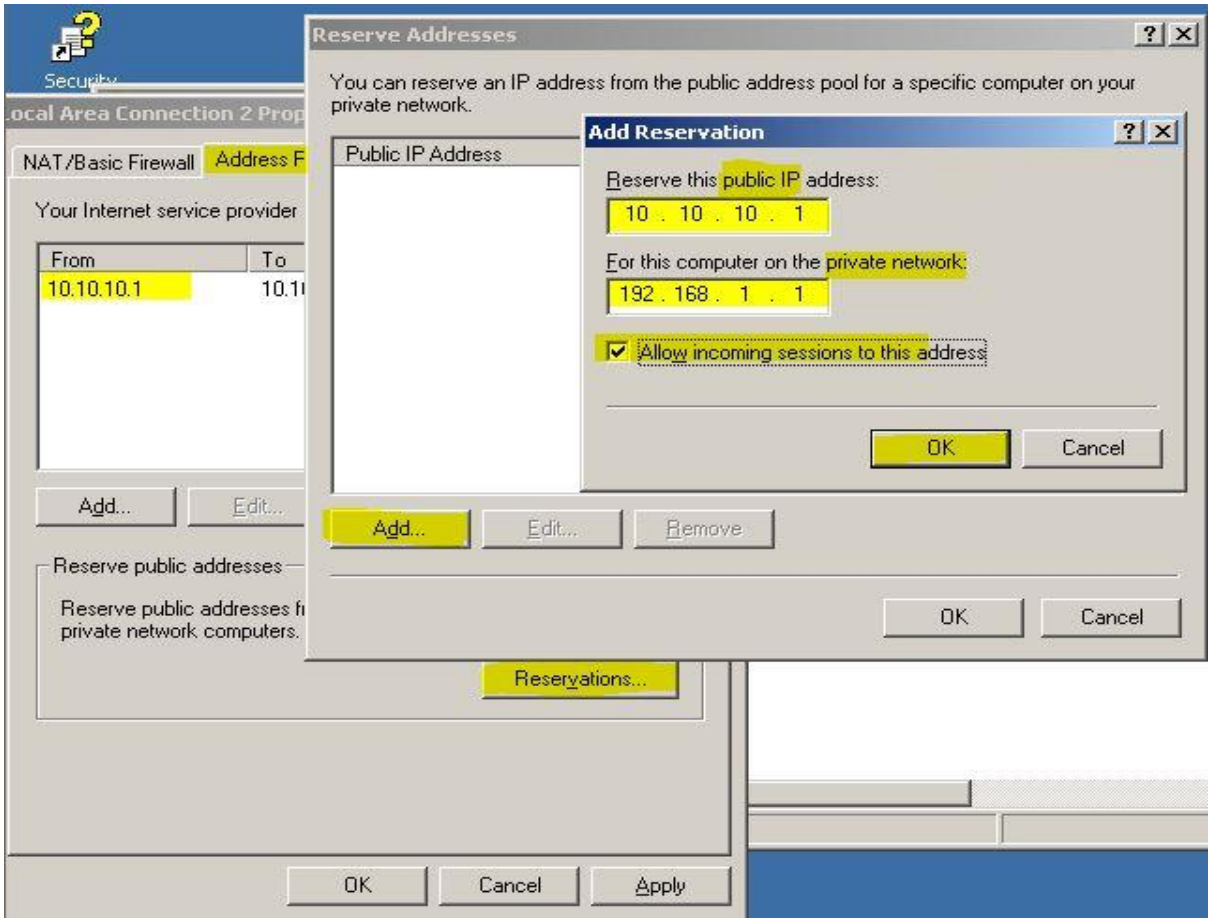
در **تب Basic** می توان بر روی پکت ها فیلترینگ اعمال کرد. مثلا روی IPهـا فیلتـر اعمـال کـرد. حتـی نـوع پروتکـل مثـل TCP,UDP,ICMP و .... این کار را با زدن دکمه های inbound و outbound اعمال کرد.


Local Area Connection 2 Properties
NAT/Basic Firewall
Address Pool
Services and Ports
ICMP
Interface Type:
Private interface connected to private network
Public interface connected to the Internet
Enable NAT on this interface
NAT enables clients on this network to send data to and receive data from the Internet using this interface.
Enable a basic firewall on this interface
A basic firewall accepts data from the Internet only if it has been requested by the network
Basic firewall only
Static packet filters
Static packet filters can restrict traffic based on packet attributes, such as IP address or protocol.
Inbound Filters
Outbound Filters
OK
Cancel
Apply

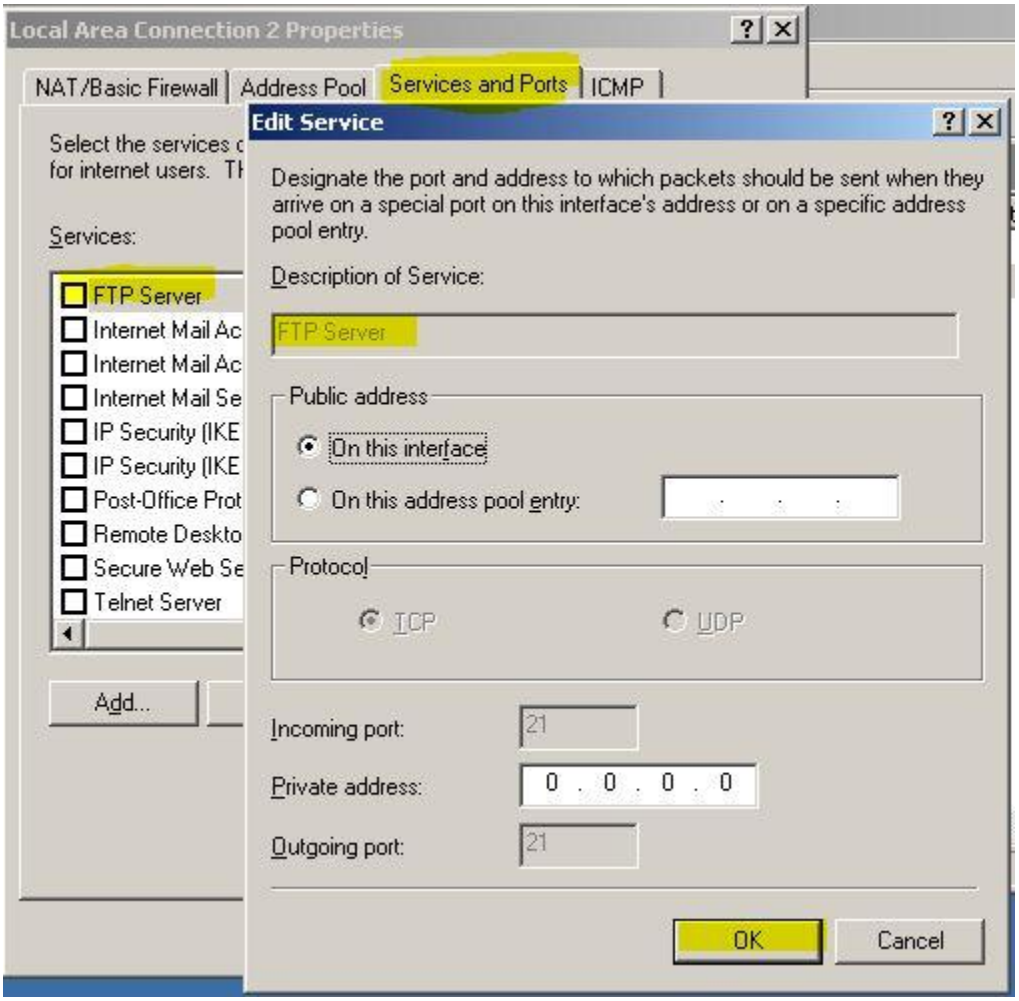

NAT/Basic Firewall
Interface Type:
Inbound Filters
These filters control which packets are forwarded or proc
Filter action:
Filters:
Source Address
Source Network Mask
New...
Add IP Filter
Source network
IP address:
Subnet mask:
Destination network
IP address:
Subnet mask:
Protocol:
Any
OK
Cancel

در **تب آدرس** می توان IP را رزرو کرد و آدرس عمومی که از ISP گرفتیم در این بخش ست می شود.

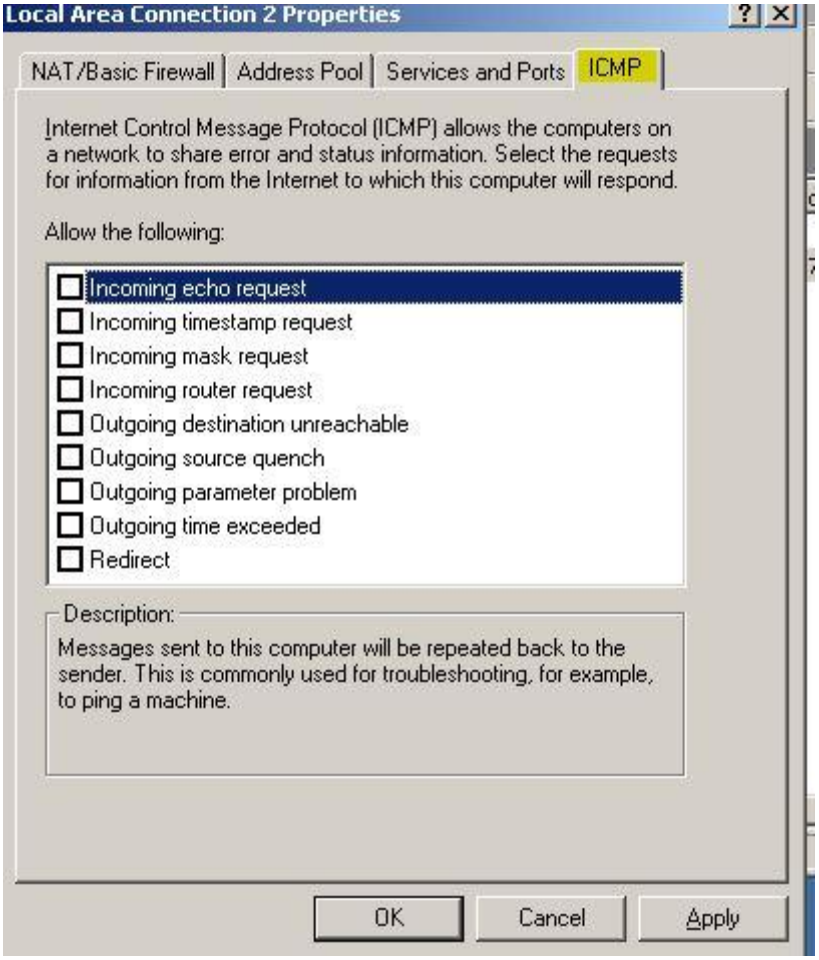




در **تب سرویس** و پورت انواع سرویس ها مثل FTP,IPsec و غیره قرار دارد و سرویس و پورت هایی که می خواهیم در اختیار کاربران خارجی(اینترنت) قرار گیرند در این تب انجام می شود.



در **تب ICMP** می توان نوع پیام هایی که می خواهید روتر NAT به آن ها پاسخ دهد را مشخص کرد. پیام های ICMP مثل Echo Request که در بخش TCP/IP توضیح داده شد. ICMP اجازه می دهد تا مبدا و مقصد اطلاعات پیام ها را برای خطا یابی به اشتراک بگذارند.



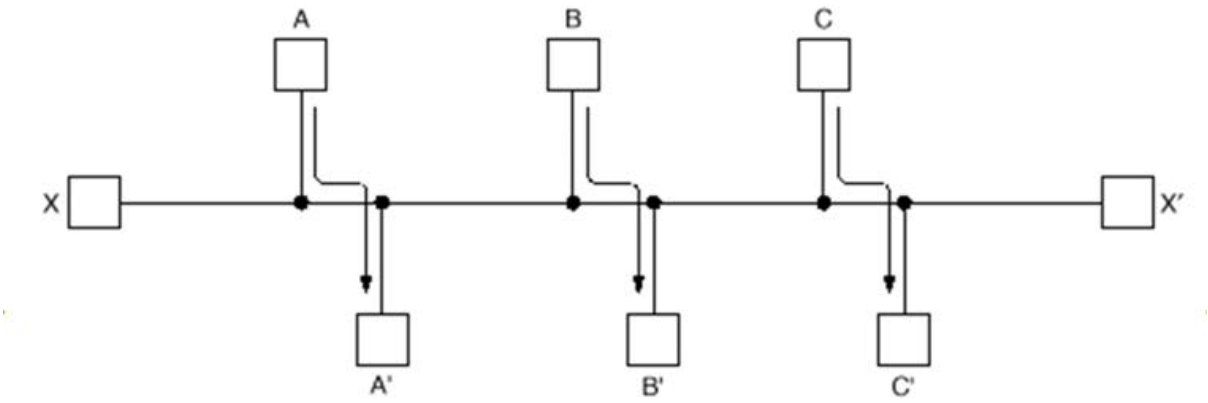
الگوریتم های مسیریابی :

وظیفه اصلی لایه شبکه ، هدایت بسته‌ها از ماشین منبع به ماشین مقصد است در اغلب زیر شبکه‌ها ، بسته‌ها باید چند جهش انجام دهند. تا به مقصد برسند. برای شبکه های پخشی،استثنایی وجود دارد، وای در اینجا نیز اگر منبع و مقصد در یک شبکه نباشد مسیر یابی مشکل محسوب می‌شود. الگورتیم هایی که مسیرها و ساختمان داده‌های مربوط به آن را انتخاب می‌کنند، موضوع مهم را طراحی لایه شبکه اند.

الگوریتم مسیر یابی بخشی از نرم افزار لایه شبکه است که تعیین می کند بسته ورودی باید به کدام خط خروجی منتقل شود. اگر زیر شبکه از داده ها گرام ها استفاده کند، این تصمیم گیری دوباره باید برای هر بسته ورودی تکرار شود ،چون تا آن موقع امکان دارد بهترین مسیر، تغییر کند اگر زیر شبکه از مدارهای مجازی استفاده کند ، تصمیمات مسیر یابی وقتی اتخاذ می شوند که مدار مجازی جدیدی استفاده گردد. از آن پس ، بسته های داده ها فقط از مسیر ایجاد شده قبلی منتقل می شوند.حالت دوم گاهی مسیر یابی تماس دارد ، زیرا مسیر در طول مدت تمسا کاربر باقی می ماند (مثل کار کردن با پایانه یا انتقال فایل) صرف نظر از این که آیا مسیرها برای هر بسته به طور مستقل انتخاب میشوند یا فقط وقتی که اتصال جدیدی

برقرار می‌شود انتخاب می‌گردند، خواصی وجود دارند. که در الگوریتم‌های مسیر یابی مطلوب‌اند صحت ، سهولت تحمل عیب، پایداری ، عدالت و بهینگی صخت وسهولت نیازی به توضیح ندارند، اما نیاز به تحمل عیب چندان روشن نیست. انتظار می رود که شبکه‌های بزرگ ، سال‌ها بدون عیب کلی سیستم به کار خود ادامه دهند. در این مدت ممکن است اشکالات سخت افزاری و نرم افزاری گوناگونی به وجود آید. میزبان‌ها مسیر یاب‌ها مسیر یاب‌ها بدون نیاز به توقف انجام انجام کارها در مسیر یاب‌ها و راه اندازی مجدد شبکه در هر بار متلاشی شدن مسیریاباز عهده تغییرات در توپولوژی و ترافیک برآید.

پایداری نیز برای الگوریتم مسیر یابی هدف مهمی است. الگوریتم های مسیر یابی وجود دارند که هرگز وجود دارندکه هرگز به حالت پایداری نمی‌رسند.مدت زمان اجرای آن بی تاثیر است عدالت وبهینگی ممکن است ساده به نظر می‌رسند یقیینا کسی با آن مخالف نیست. اماهمان طور که روشن است اهداف متناقضی دارند به عنوان مثال از این تناقض ، شکل ۱ را بینید. فرض کنید ترافیک کافی بین A و ش، بین B,B وبین C, C وجود دارد تا پیوندهای افقی را اشباع نماید برای بیشینه کردن کل جریان ترافیک X, X باید کاملا از بین برود. متاسفانه از نظر X وX عادلانه نیست بدیهی است که توافقی بین کارایی کلی و عدالت اتصال‌های منفرد لازم است.



قبل از اینکه به متوزان کردن عدالت وبهینگی بپردازیم . باید تصمیم بگیریم که چه چیزی را بهینه کنیم . بدیهی است تاخیر بسته باید کمینه شود ولی توان شبکه باید بیشینه شود. علاوه براین این دو هدف نیز با هم تضاد دارند، زیرا عملکرد هر سیستم صف بندی در حد ظرفیت تاخیر صف بندی را زیاد ی کند. اغلب شبکه ها سعی میکنند تعدداد جهشهای بسته های را کمینه نمایند زیرا کاهش تعدادجهش موجب بهبود تاخیر و نیزکاهش میزان پهنای باند مصرفی است که منجر به بهبود توان عملیاتی می‌شود.

الگوریتم‌های مسیر یابی به می‌توانند به دو دسته تقسیم شوند غیر وفقی و وفقی الگوریتم‌های غیر وفقی تصمیات مسیر یابی خود را بر اندازه گیری یا تخمین توپولوژی و ترافیک فعلی بنا نمی نهند بلکه برای انتخاب مسری جهت رسیدن از I به J برای

تمام I را به تمام J از قبل محاسبه می‌شود در حالت OFF-LINE و هنگام راه اندازی شبکه به مسیر یاب‌ها بار می‌شود این روند گاهی مسیر یابی ایستا نام دارد.

برعکس الگوریتم‌های وقفی تصمیات مسیر یابی خود را براساس تغییرات توپولوژی و ترافیک تغییر می‌دهند الگوریتم‌های وقفی ، وقتی که مسیرها را عوض می‌کنند. مثلا هر ثانیه وقتی بار تغییر می‌کند، با وقتی توپولوژی تغییر می‌کند از نظر جایی که اطلاعات را می گیرند مثلا محلی از مسیریابهمجوار یا تمام مسیریابومعیارهایی که برای بهینه سازی مورد استفاده قرارمی گیرند. (مثلا ، محلی از مسیریاب همجواریا تمام مسیر یاب ها و معیارهایی که برای بهینه سازی مورد استفاده قرار می گیرند (مثلاً فاصله ، تعداد جهشها یا زمان انتقال تقریبی با یکدیگر متفاوتاند . در بخش‌های بعدی الگوریتم‌های الگوریتمهای گوناگونی را چه ایستا و چه پویا ،مورد بررسی قرار می‌دهیم.

اصل بهینگی

قبل از پرداختن به الگوریتم توجه به مهم است که صرف نظر از توپولوژی شبکه وتر افیکی ، می توان حکمی کلی راجع به مسیرهای بهینه ارائه کرد این حکم را به عنوان اصل بهینگی شناخته می‌شود. این اصل بیا می‌کند که اگر مسیریابJ از مسیریاب I به مسیریابK در مسیریاب بهینه‌ای شناخته می کند آنگاه مسر بهینه‌ای از J و K نیز در مسیر مشابهی قرار می گیرد. برای مشاهده این موضوع ، بخشی از مسیر I به J را به بنامید و بقیه را نامگذاری کنید اگر مسیری بهتر از وجود داشت می‌توانست با الحاق شود تا مسیری از I به K بهبود بخشد، و حکم ما را می‌گوید ? بهینه است نقض کند.

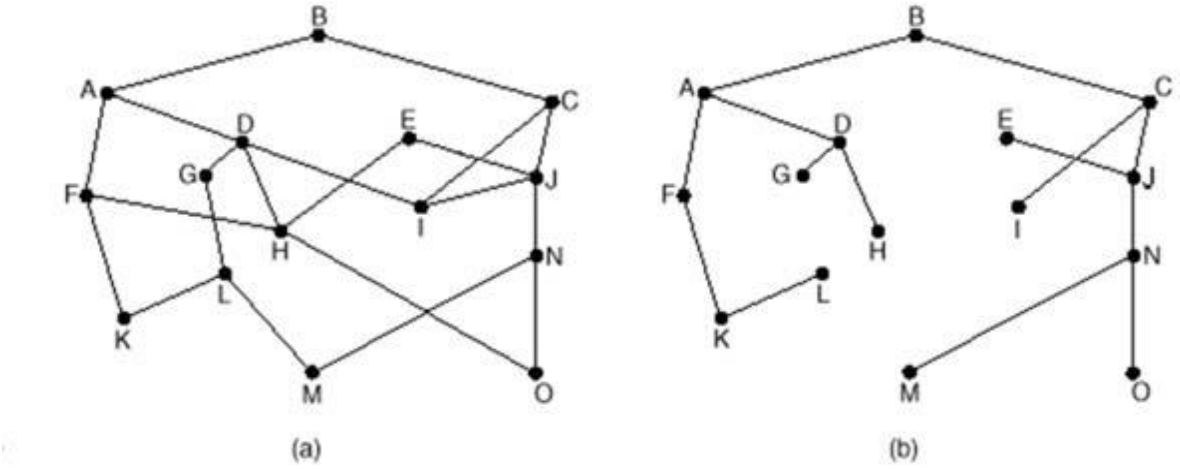
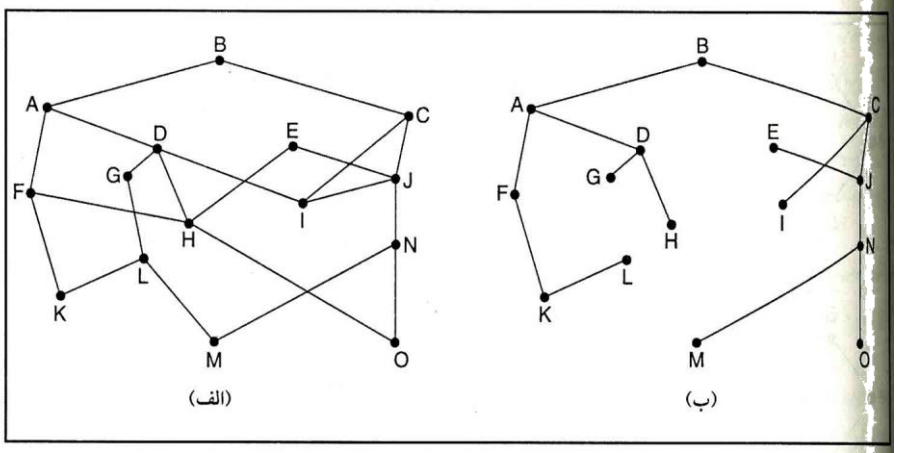


Fig. 5-5. (a) A subnet. (b) A sink tree for router *B*.



(الف) زیرشبکه. (ب) درخت بایگانی برای مسیریابِ B.

از اصل بهینگی می‌توان نتیجه گرفت که مجموعه‌ای از مسیرهای بهینه از تمام منابع به مقصدی معین ، درختی را تشکیل مید هد که ریشه اش مقصد است چنین درختی، درخت بایگانی نام دارد.شکل ۲ در این درخت مقیاس فاصله تعداد جهش ها است توجه داشته باشید. که درخت‌های دیگری با همان طول مسیر وجود داشته باشند هدف الگوریتم‌های مسیر یابی، یافتن درخت‌های بایگانی و استفاده از انها برای تمام مسیر یاب‌ها است .

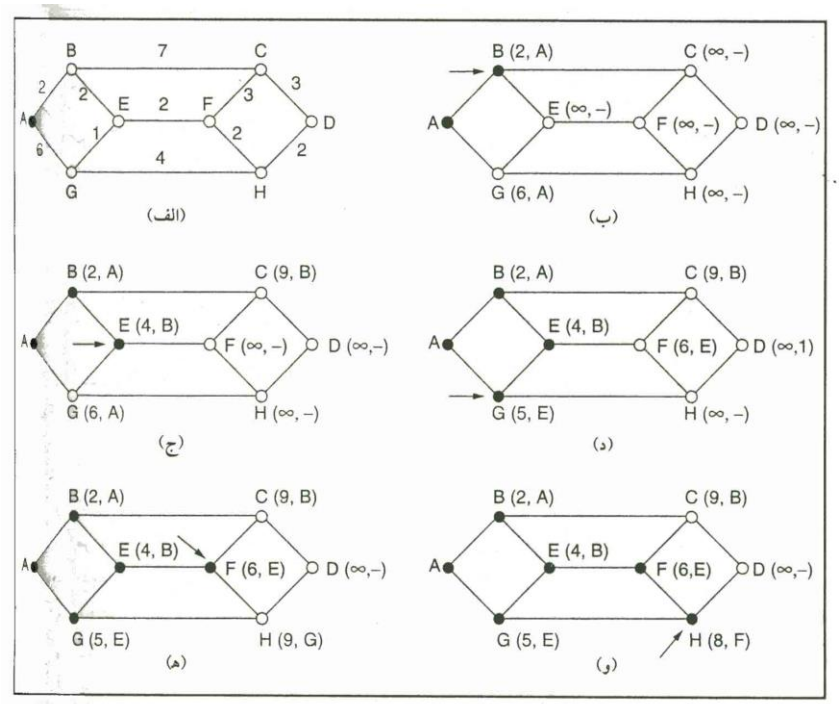
چون درخت بایگانی یک درخت است، فاقد هرگونه حلقه است. لذا هر بسته در تعداد مشخصی از جهش های دریافت می شود. در عمل همیشه به این سادگی نیست.در اثنای کار، پیوندهای ومسیریابمی توانند به طرف پایین بروند وبه طرف بالا برگردند. بنابراین امکان دارد مسیر یاب های مختلف راجع بع توپولوژی فعلی ایده های متفاوتی داشته باشند .همچنین سوال دیگری که مطرح بود این بود که آیا هر مسیریابمجبور است به طور انفرادی اطلاعات مورد نیاز جهت محاسبه درخت بایگانی را به دست آورد یا این اطلاعات توسط وسایل دیگری جمع آوری می شوند در ادامه به طور مختصر به این موضوع می پردازیم با این وجود، اصل بهینگی ودرخت بایگانی‌های معیارهایی را تهیه کردند که سایر الگوریتم‌های مسیر یابی می‌توانند براساس آنها ارزیابی شوند.

مسیر یابی کوتاه ترین مسیر

مطالعه الگوریتمهای مسیر یابی را با تکنیکی که به طور گسترده به شکل‌های مختلفی به کار می‌رود شروع می‌کنیم، زیرا الگوریتم ساده ای است ودرک آن آسان است. ایده ، ساختن گرافی از زیر شبکه است ، به طوری که ، هر گره گراف نشان

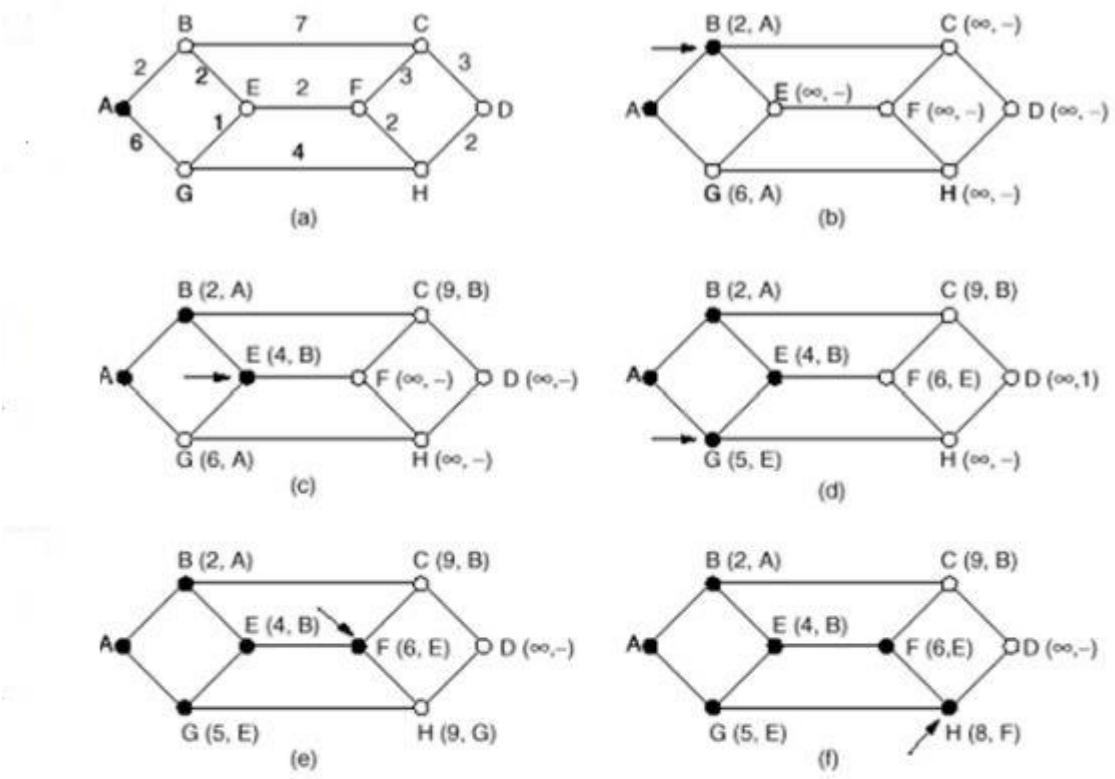
دهنده مسیریاب است و هریال نشان دهنده خط ارتباطی است (که اغلب پیوند نام دارد.) برای انتخاب مسیری بین دو مسیریابمعین ، الگوریتم ، کوتاهترین مسیر بین آنها را درگراف می‌یابد.

در مورد کوتاهترین مسیر توضیحاتی باید ارائه شود . یک راه اندازه گیری طول مسیر ، تعداد جهش است با این معیار ، طول مسیرهای ABC,ABE در شکل ۳ یکسان است.و معیار دیگر معیار دیگر فاصله جغرافیایی به کیلومتراست ، در این حالت بدیهی است که ABC خیلی طولانی تر از ABE است با فرض این که شکل با مقیاس رسم شده است.



پنج مرحلهٔ اول برای محاسبهٔ کوتاه‌ترین مسیر از A به D می‌باشد، پیکان‌ها گرهٔ کاری را نشان می‌دهند.

علاوه بر جهش‌ها و فاصله فیزیکی معیارهای دیگری نیز قابل استفاده‌اند به عنوان مثال هریال می‌تواند به میانگین تاخیر صف بندی و انتقال برای بعضی از بسته های آزمایشی برچسب گذاری شود. با این برچسب گذاری، کوتاهترین مسیر به جای مسیری به جای مسیری که با کمترین یال یا فاصله سریع تر مسیر است.



	Base Set	B	C	D	E	F	G	H
0	A	2,A	∞	∞	∞	∞	6,A	∞
1	A,B		9,B	∞	4,B	∞	6,A	∞
2	A,B,E		9,B	∞		6,E	5,E	∞
3	A,B,E,G		9,B	∞		6,E		8,F
4	A,B,E,G,F		9,B	∞				8,F
5	A,B,E,G,F,H		9,B	10,H				

در حالت کلی، برچسب‌های یال‌ها باید به صورت تابعی از فاصله ، پهنای باند، میانگین ترافیک هزینه ارتباط میانگین طول صف تاخیر اندازه گیری شده و سایر عوامل محاسبه شود. با تغییر تابع وزنی ، الگوریتم ،کوتاهترین مسیر وزن دار را براساس هریک از معیارهای فوق یا ترکیبی از آنها محاسبه می‌کند.

الگوریتم‌های متعددی برای محاسبه کوتاهترین مسیربین در گره گراف شناسایی شده‌اند یکی از این الگوریتمهای به دیکسترا ۱۹۹۵ نسبت داده می‌شود. هر گره دارای برچسب هایی در پرانتز است که فاصله آن تا گره منبع، از طریق بهترین مسیر شناخته شده نیست لذا تمام گره ها دارای بر چسب بی نهایت هستند .با ادامه اجرای الگوریتم وپیدا شدن مسیرها، امکان دارد برچسب‌ها تغییر کنند تا مسیرهای بهتری منعکس نمایند. برچسب ممکن است موقتی یا دائمی باشد. در آغاز ، تمام

برچسب‌ها موقتی‌اند وقتی مشخص شد که برچسبی کوتاهترین مسیر بین منبع به آن گروه تمام برچسب‌ها مو قتی اندوقتی مشخص شد که برچسبی کوتاهترین مسیر بین منبع به آن گره را نمایش می‌دهد، دائمی می‌شود و از آن پس تغییر نمی‌کند.

برای اینکه که مشخص شود الگوریتن برچسب گذاری چگونه کار می کند. گراف وزن دار بدون جهت شکل ۳ الف را در نظر بگیرید. که وزن ها ، مثلا فاصله را نشان می دهد می خواهیم کوتاهترین مسیر از A به D را بیابیم. با علامت گذاری گره A به عنوان گره ثابت که به صورت دایره پر نشان شده است. شروع می کنیم. سپس نوبت ، تمام همجوار A همجوار A گره کاری را تست می کنیم .هر کدام را با فاصله آن به A مجددا برچسب می‌دهیم. هر وقت گره‌ای مجددا برچسب دهی شد، آن رابا گره اس که کار از آنجا آغاز شد برچسب می‌دهیم به این ترتیب می توانیم مسیر نهایی را بازسازی کنیم. با بررسی تمام گره‌ها همجوار A تمام گره هایی را که در کل گراف به طور موقت برچسب دهی شدند بررسی می‌کنیم و گره‌ای که دارای کوچک ترین برچسب است دائمی می‌کنیم. (شکل ۳- ب) این گروه به عنوان گره کاری جدید انتخاب می‌شود.

اکنون از B شروع می کنیم و تمام گره هایی همجوار آن را مورد بررسی قرار می دهیم. اگر مجموع برچسب در B و فاصله B تا گره‌ای که باید در نظر گرفته شود کمتر از برچسب موجود در ان گره باشد کوتاهترین مسیر پیدا شده ، این گره مجددا برچسب گذاری می‌شود.

پس از این تمام کره ها همجوار گره کاری بررسی شدند و گره های موقتی تغییر کردند ، کل گراف مورد جست وجو قرار می‌گیرد تا گره‌ای موقتی با کمترین مقدار برچسب گذاری می‌شود

برای پی بردن به عملکرد الگوریتم شکل ۳ ج را ببینید در این شکل، E دائمی است فرض کنید مسیر AXYZA کوتاهتر از ABE باشد دو امکان وجود دارد: یا گره Z به عنوان گره دائمی منظور شده است یا نشده است اگر دائمی باشد E تاکنون بررسی شده است در سیکلی بعد از ان که Z دائمی شد. لذا AXYZE از دید ما خارج نبوده است و نمی تواند مسیر کوتاهتری باشد

اکنون حالتی را در نظر بگیرید که هنوز بر چسب Z موقتی باشد.برچسب موجود در Z بزرگتر یا مساوری برچسب در E است که در این حالت XYZE نسبت به ABC مسیر کوتاهتری نیست، یا کمتر از E است که در این حالت Z وE تاکنون بررسی مورد جستجو قرار می‌گیرد.

این الگوریتم در شکل ۴ آمده است متغیرهایی عمومی N و DIST گراف را توصیف می‌کنند و قبل از فراخوانی SHORTEST PATH مقدار می گیرند . تنها بین برنامه والگوریتمی که تشریح شد این است که کوتاهترین مانند کوتاهترین مسیر از Sبه T محاسبه شده است .چون کوتاهترین مسیر از T به S در گراف بدون جهت است مهم نیست که از کدام طرف شروع کنیم مکر اینکه کوتاهترین مسیر متعددی وجود داشته باشد که در آن حالت جست و جستجوی معکوس مسیر دیگری را انتخاب می نماید. دلیل جستجوی معکوس این است که هرگره با گره قبلی خود (به جای گره بعدی) برچسب گذاری می شود. هنگام

کپی کردن مسیر نهایی در متغیر خروجی PATH مسیر، معکوس می شود با معکوس کردن جستجو این دو اثر خنثی می شود. پاسخ به ترتیب درستی تولید می‌گردد.

الگوریتم غرق کردن

الگوریتم ایبستای دیگر غرق کردن است که درآن، هر بسته ورودی به تمام خطوط خروجی به جز خطی که از آن آمده است ارسال می‌شود. این الگوریتم ،بسته‌های تکراری زیادی در واقع نامحدود ایجاد می‌کند. مگر اینکه تدبیری اندیشیده شود که این کار را کند نماید یکی از این مقیاس ها قرار داردن شمارنده جهش در سرآیندهر بسته است مقدار این شمارنده در هر جهش بسته یک واحد کم می‌شود. وقتی که این شمارنده به صفر رسید بسته دور انداخته می‌شود ایده آل این است که مقدار اولیه شمارنده جهش برابر با طول مسیر از منبع به مقصد قرار گیرد. اگر فرستنده طول مسیر را نداند، می تواند مقدار آن را برابربا بدترین حالت، یعنی ، قطر کامل زیرشبکه، قرار دهد،

```
#define MAX_NODES 1024                  /* maximum number of nodes */
#define INFINITY 1000000000             /* a number larger than every maximum path */
int n, dist[MAX_NODES][MAX_NODES];/* dist[i][j] is the distance from i to j */

void shortest_path(int s, int t, int path[])
{ struct state {                        /* the path being worked on */
    int predecessor;                    /* previous node */
    int length;                         /* length from source to this node */
    enum {permanent, tentative} label; /* label state */
 } state[MAX_NODES];

 int i, k, min;
 struct state *p;

 for (p = &state[0]; p < &state[n]; p++) { /* initialize state */
    p->predecessor = -1;
    p->length = INFINITY;
    p->label = tentative;
 }
 state[t].length = 0;  state[t].label = permanent;
 k = t;                                 /* k is the initial working node */
 do {                                   /* Is there a better path from k? */
    for (i = 0; i < n; i++)             /* this graph has n nodes */
        if (dist[k][i] != 0 && state[i].label == tentative) {
            if (state[k].length + dist[k][i] < state[i].length) {
                state[i].predecessor = k;
                state[i].length = state[k].length + dist[k][i];
            }
        }

    /* Find the tentatively labeled node with the smallest label. */
    k = 0; min = INFINITY;
    for (i = 0; i < n; i++)
        if (state[i].label == tentative && state[i].length < min) {
            min = state[i].length;
            k = i;
        }
    state[k].label = permanent;
 } while (k != s);

 /* Copy the path into the output array. */
 i = 0;  k = s;
 do {path[i++] = k; k = state[k].predecessor; } while (k >= 0);
}
```

الگوریتم دیکسترا برای محاسبه کوتاه‌ترین مسیر در گراف.

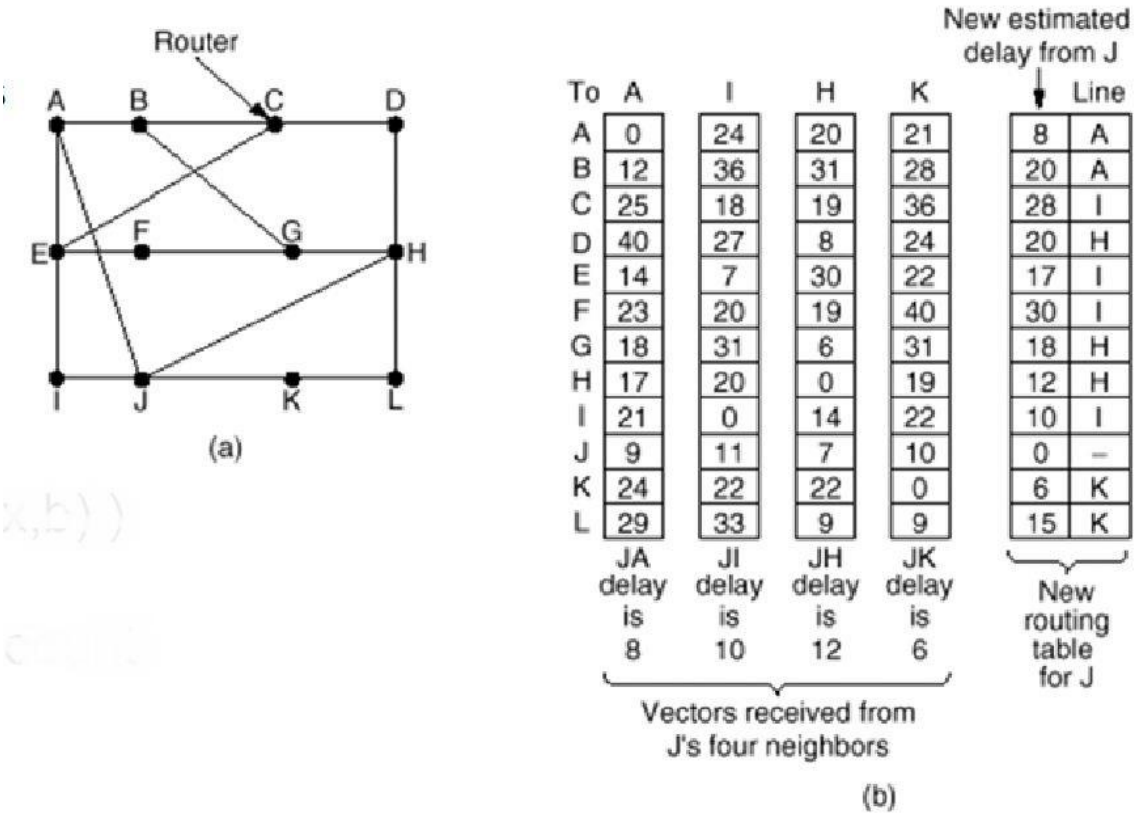
تکنیک دیگر برای محدود کردن الگوریتم غرق کردن این است که بسته هایی که تاکنون ارسال شده‌اند مشخص باشند، تا مجددا ارسال نگردند یک روش انجام این کار این است که مسیریابمنبع ، در بسته هایی که از میزبانهایش دریافت می کند شماره ترتیبی را قرار دهد در این صورت هر مسیریابه ازای هر مسیریابمنبع به لیستی نیاز دارد تا مشخث کند کدام شماره ترتیب هایی که تاکنون از منبع ارسال شدند دریافت گردیدند. اگر بسته ورودی در آن لیست موجود باشد: ارسال نشده است.

برای جلوگیری از رشد بی رویه لیست، هر لیست باید دارای شمارنده‌ای به نـام K باشـد،معنایش ایـن اسـت کـه تمـام شـماره ترتیب‌ها از ۱ تا K مشاهده شده‌اند وقتی بسته‌ای دریافت می‌شود، به راحتی می‌توان تشخیص داد که این آیا تکراری اسـت یـا خیر اگر تکراری باشد، از آن صرف نظر می گردد. علاوه بر این ،به لیست کامـل کمتـر ازK نیـازی نیسـت،زیرا K آن را خلاصـه می‌کند.

شکل خاصی از الگوریتم غرق کردن که عملی تر است غرق کردن انتخابی نام دارد. در این الگوریتم،مسـیر یـاب هـا هـر بسـته ورودی را به تمام خطوط خروجی نمی‌فرستند ، فقط به خط هایی می‌فرستند که تقریبا درجهت درستی منتقل می‌شوند کمتر اتفاق می‌افتد بسته‌ای که می‌خواهد به غرب برود به خطی در قسمت شرق ارسال شود، مگر این که توپولوژی ویـژه‌ای بـه کـار گرفته شود ومسیریابه این حقیقت مطمئن باشد.

الگوریتم غرق کردن، در اغلب کاربردها عملی نیست، اما کاربردهایی دارد به عنوان مثال در کاربردهیای نظامی ، که لازم است در هر لحظه بیت هایی برای بسیاری از مسیر یاب ها ارسال شود، الگوریتم غرق کردن توانمند نوسـازی شـوند سـومین کـاربرد غرق کردن همواره کوتاهترین مسیر را انتخاب می‌کند، زیرا تمام مسیرهای ممکن را به طور موازی آزمایش می‌کنـد در نتیجـه هیچ الگوریتم دیگری نمی‌تواند تاخیر کمتری ایجاد نماید. اگر سربار حاصل ازخود فرایند غرق کردن را نادیده بگیریم.

مسیر یابی بردار فاصله (Distance Vector)

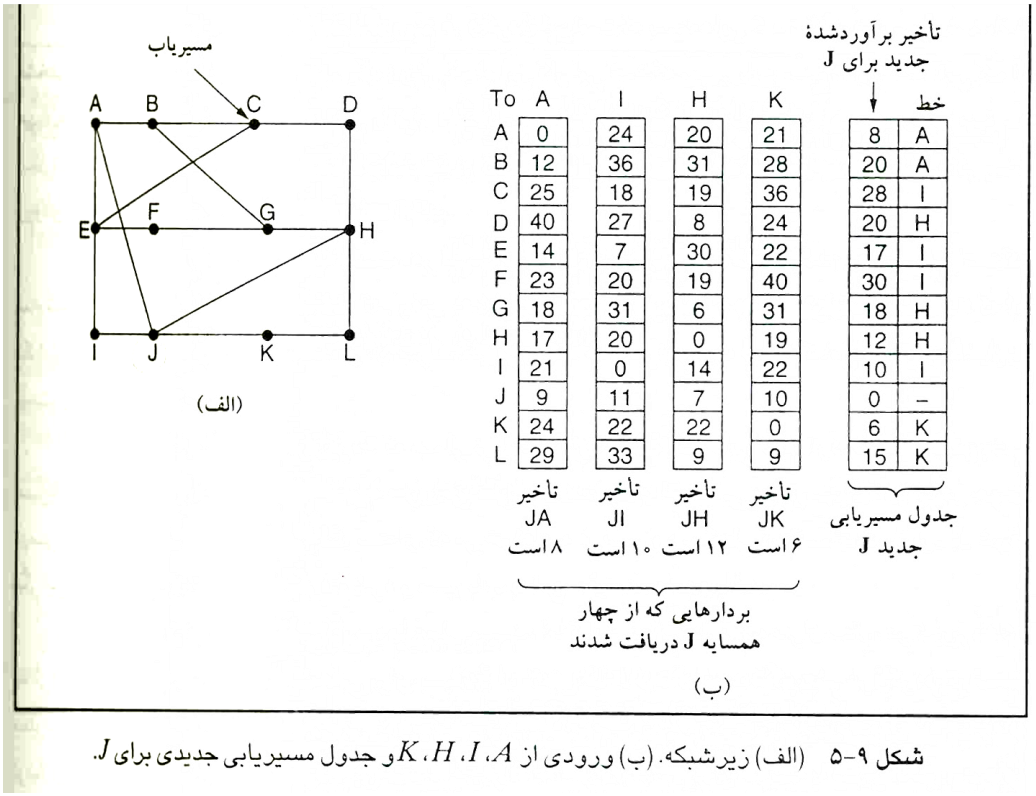


شبکه هایی کامپیوتری مدرن به جای الگوریتمهای مسیر یابی ایستا از الگوریتم مسیریابی پویا استفاده می‌کنند، زیرا الگوریتم‌های ایستا بار فعلی شبکه را در نظر نمی‌گیرند و دو الگوریتم پویا به نامهای مسیر یابی بردار فاصله و مسیر یابی حالت پیوند، عمومیت بیشتری دارند در این بخش به الگوریتم مسیر یالی بردار فاصله و در بخش بعدی به الگوریتم مسیر یابی حالت پیوند می‌پردازیم.

در الگوریتمهای مسیریابی بردار فاصله هر مسیریابجدول یا برداری دارد که بهترین فاصله به هر مقصد را نگهداری می کند خطی را که برای رسیدن به آن مقصد لازم است مشخص می‌کند. این جدولها از طریق تبادل اطلاعات با همسایه‌ها بازسازی می‌شوند.

الگوریتم مسیر یابی بردار فاصله به اسامی دیگر نیز خوانده می شود. ازجمله الگوریتم مسیر یابی بلمن –فورد و الگوریتم و الگوریتم فورد – فورکرسون که نامگذاری آنها را نام مخترعین آنها بلمن ۱۹۷۵- فورد و فوکرسون، ۱۹۶۲ اقتباس شده است. این الگوریتم مسیر یابی ARPANET اولیه بود و تحت نام RIP در اینترنت مورد استفاده قرارگرفت.

درمسیر یابی بردار فاصله ، هر مسیر باب دارای جدول است که به ازای هر مسیر در زیر شبکه یک وارده دارد این وارده دو بخش است : خط خروجی پیشنهادی برای استفاده از آن مقصد و تخمینی از زمان یا فاصله به آن مقصد مقیاس مورد استفاده ممکن است تعداد جهش‌ها ، زمان تاخیر به میلی ثانیه ، بسته هایی که در مسیر در صف قرار گرفته‌اند یا چیزهایی مشابه آن‌ها باشند.

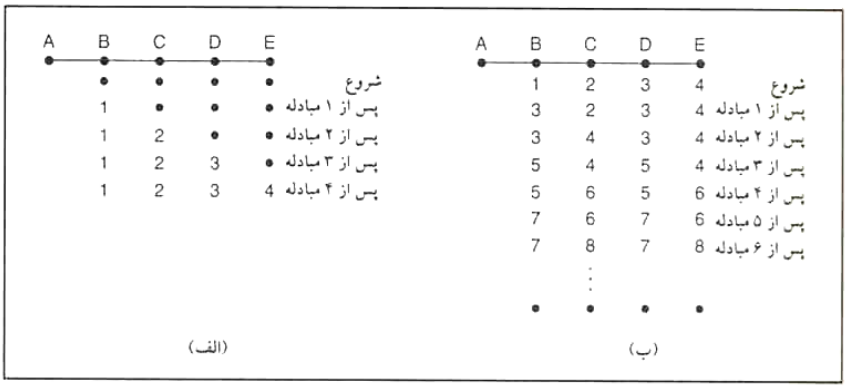


شکل ۹-۵ (الف) زیرشبکه. (ب) ورودی از A، I، H، K و جدول مسیریابی جدیدی برای J.

فرض می‌شود که مسیریابفاصله خود تا هر همسایه اش را می‌داند و اگر مقیاس ، جهش باشد، فاصله فقط یک جهش است اگر مقیاس طول صف باشد مسیر باب هر صف را بررسی می‌کنداگر مقیاس تاخیر باشد، مسیر باب می‌تواند آنرا مستقیما با بسته ECHO خاصی از هر طرف گیرنده ارسال می‌شود اندازه گیری کند.

به عنوان مثال ، فرض کنید تاخیر به عنوان مقیاس به کار می‌رود و مسیریاب، تاخیر به هر همسایه خودش را می‌داند . هر مسیریابدر هر T میلی ثانیه لیستی از تاخیرهای تخمینی خود را به هر مقصد را ارسال می کند ولیست مشابهی از هر همسایه خود دریافت می‌کند فرض کنید یکی از این جدول‌ها از همسایه‌ها X می‌رسد، به طوری که X زمان رسیدن به مسیریاب I باشد که X آن را تخمین زده است اگر مسیریابداند تاخیر تا X برابر با M میلی ثانیه باشد، می‌داند که اگر بخواهد از طریق X به مسیریابI برسدX+M میلی ثانیه طول می‌کشد. با انجام این محاسبات برای هر همسایه‌های مسیریابمی‌تواند بهترین تخمین را تشخیص دهد و می تواند از این تخمین و خط متناظر در جدول مسیر یابی جدید استفاده نماید توجه داشته باشیدو که جدول مسیر یابی قبلی، در محاسبه به کار نمی‌آید.

این فرآیند بازسازی در شکل ۵ آمده است بخش الف زیر شبکه‌ای را نشان می‌دهد چهار ستون اول بخش (ب) بردارهایی تاخیری را که از همسایه هایی مسیریابJ آمده‌اند نشان می‌دهد تاخیر از A به B برابر با ۱۲ میلی ثانیه و از A به C برابر با ۲۵ میلی ثانیه و از A به D برابر ۴۰ میلی ثانیه و غیره است فرض کنید تاخیرهایی J به همسایه هایش A,H,I,A به ترتیب عبارتست از ۸و۱۰و۱۲و۶ میلی ثانیه .



شکل ۱۰-۵ مسئلهٔ بی‌نهایت‌گرایی.

چگونگی محاسبه مسیر جدید از J به G را در نظر بگیرید J می‌داند که می‌تواند با ۸ میلی ثانیه تاخیر بـه A برسـد و A بـا ۱۸ میلی ثانیه به G می‌رسد لذا J می‌داندکه اگر بخواهد از طریق A به G برسد ۲۶ میلی ثانیه طول می‌کشد. به طـور مشـابه بـه تاخیر رسیدن به J را در جدول ،۱۸ میلی ثانیه ثبت می‌کند و آن، از طریـق H اسـت محاسـبه مشـابهی بـرای تمـام مقصـدها صورت میگیرد به طوری که جدول مسیر یابی جدید را به صورت آخرین به صورت اخرین ستون شکل در می‌آید.

مسئله بی نهایت گرایی

مسیر یابی بردار فاصله از نظرو تئوری کار می‌کند، اما در عمل مشکل جدی دارد با این که پاسخ صحیح می‌دهد، ولی به کندی عمل میکند به ویژه به خبرهای خوب، واکنش سریع ولی به خبرهای بد واکنش نشان می‌دهد مسیر یابی را در نظر بگیرید کـه بهترین مسیر آن را به X بزرگ باشد، ادگر در مبادله بعدی ، همسایه A ناگهان تاخیر اندکی بـه X را گـزارش کنـد، مسـیریاباز خطی که به A می‌آید برای ارسال ترافیک به X استفاده می‌کند در یک مبادله بردار، اخبار خوب پردازش می‌شوند.

برای مشاهده چگونگی انتشارخبرهای خوب، زیر شبکه پنج گره‌ای خطی شکل ۶ رادر نظر بگیرید،که درآن تعداد جهش‌ها به عنوان مقیاس است فرض کنید A از همان اول از کار افتاد و تمام مسیر یاب‌های دیگر این را می‌دانند بـه عبـارت دیگـر تمـام آنها تاخیرهای رسیدن به A رت بخ صورت بی نهایت ضبط کرده اند

وقتی A را به کار می‌افتد . سایر مسیر یاب‌ها از طریق مبادله بردار ، آگاه مس شوند برای سـهولت فـرض کنـیم زنـگ بزرگـی وجود دارد که برای شروع همزمان مبادله بردار در تمام مسیر یاب‌ها به صدا در می‌آید در زمان مبادله نخست B می‌فهمـد کـه همسایه چپ آن تا A آن را تاخیری ندارد صفراست سپس B در جدول مسیر یابی خود ثبت می‌کند که A تـا همسـایه چـپ ، یک جهش فاصله دارد سایر مسیر یاب‌ها فکر می‌کنند که A هنوز از کار افتاده است در این لحظـه وارده هـایی جـدول مسـیر یابی A در سطر دوم شکل ۶ برابر است الف لذا جدول مسیر یابی را بازسازی می‌کند تا مسیری به طول ۲ را نشان دهد اما D

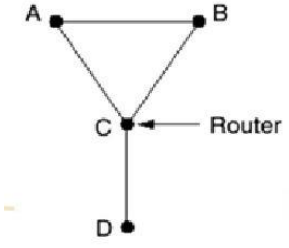
و E تاکنون خبرهای جدید را نشنیده اندن بدیهی است که خبرهای جدید با سرعت یک جهش درهر مبادله بخش می‌شود در زیرشبکه های که طولانی ترین مسیر که ان به طول N جهش است. در N مبادله هرکسی از خطوط از خطوط و مسیریاب هایی که تازه فعال شده‌اند باخبر می‌شود.

اکنون وضعیت شکل ۶ (ب) را در نظر می‌گیریم در این شکل تمام خطوط و مسیریاب‌ها در آغاز فعال‌اند وفاصله مسیر یاب‌های Aتا, E,D,C,B به ترتیب عبارتند از ۱و۲,۳و۴ ناگهان A از کار می‌افتد یا خط بین A, B قطع می‌شود از دید B فرقی نمی‌کند که کدامیک اتفاق افتاده است.

در مبادله اولین بسته، B چیزی از A نمی شنود خوشبختانه C می گوید نگران نباشید من مسیری به طول ۲ به A دارم لذا B می‌داندکه مسیر C از طریق خود B می‌داند که C ممکن است ده خط خروجی داشته باشد .که هر کدام دارای مسیرهای مستقلی به A هستند که طول آنها ۲ است در نتیجه B فکر می‌کند که می‌تواند از طریق C به A برسد با مسیرهای به طول ۳ در مبادله اول E,D وارده‌های خود را برای A را بازسازی میکنند.

در مبادله دوم C در می یابدکه هریک از همسایه هایش ادعا میکنند که طول مسیر انها را به A برابر با ۳ است یکی از آنها به طور تصادفی انتخاب می‌کندو فاصله جدید به A را برابر با ۴ منظور می‌کند سطر سوم از شکل ۶ الف مبادله‌های بعدی نتایج بقیه شکل ۶ الف را تولید میکنند.

از این شکل پیدا است که چرا خبرهای بد کندی ارسال می‌شوند : هیچ مسیر یابی مقداری بیش از کمترین مقدار تمام همسایه هایش را ندارد گاهی تمام مسیر یاب‌ها بی نهایت بار کار می‌کنند.به همین دلیل ، عاقلانه است که بی نهایت را برابر با طولانی ترین مسیر به علاوه ۱ قرار داد اگر مقیاس تاخیر زمان باشدو حد بالایی تعریف شده‌ای وجود ندارد لذا برای با طولانی ترین مسیر با تاخیر طولانی مثل مسیر از کار افتاده رفتار نشود وجود نداردلذا برای اینکه با مسیری با تاخیر طولانی، مثل مسیر از کار افتاده نشود ،نیاز به حد بالایی است لذا این مسئله بی نهایت گرایی نام دارد تلاش زیادی برای حل آن انجام شد ، ولی هیچ کدام موفق نبوده اند. مسئله مهم این است که وقتی X به Y می گوید مسیری در اختیار دارد،Y نمی تواند بفهمد که آیا خودش در آن مسیر قراردارد یا خیر .

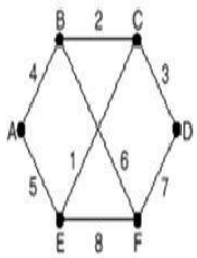


A	B	C	D	E	
∞	∞	∞	∞	∞	Initially
1	∞	∞	∞	∞	After 1 exchange
1	2	∞	∞	∞	After 2 exchanges
1	2	3	∞	∞	After 3 exchanges
1	2	3	4	∞	After 4 exchanges

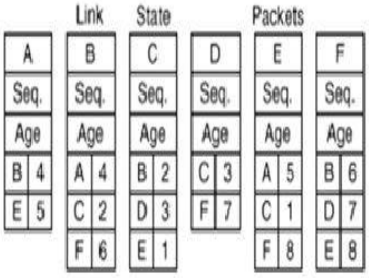
(a)

A	B	C	D	E	
	1	2	3	4	Initially
	3	2	3	4	After 1 exchange
	3	4	3	4	After 2 exchanges
	5	4	5	4	After 3 exchanges
	5	6	5	6	After 4 exchanges
	7	6	7	6	After 5 exchanges
	7	8	7	8	After 6 exchanges
		⋮			
	∞	∞	∞	∞	

مسیر یابی حالت پیوند(Link State)



(a)



(b)

Fig. 5-15. (a) A subnet. (b) The link state packets for this subnet.

Source	Seq.	Age	Send flags A	Send flags C	Send flags F	ACK flags A	ACK flags C	ACK flags F	Data
A	21	60	0	1	1	1	0	0	
F	21	60	1	1	0	0	0	1	
E	21	59	0	1	0	1	0	1	
C	20	60	1	0	1	0	1	0	
D	21	59	1	0	0	0	1	1	

Fig. 5-16. The packet buffer for router *B* in Fig.5-15.

مسیر یابی فاصله تا سال ۱۹۷۹ در ARPANET مورد استفاده قرار گرفت و از ان پس جای خود را به مسیر یابی حالت پیوند داد. و مشکل عمده موجب مرگ آن شد. یکی از این که مقیاس تاخیر، طول صف بود و هنگام انتخاب مسیریاب‌ها پهنای باند را در نظر نمی گرفت در آغاز تمام خطها KBPS۵۶ بودند لذا پهنای باند موضوع مهمی نبود اما وقتی بعضی از خطوط به KBPS۲۳۵ وبعضی دیگر به ۱/۵۵MBPS تغییر یافتند عدم توجه به پهنای باند را به عنوان مقیاس در نظر گرفت اما مشکل دوم نیز وجود داشت، یعنی الگوریتم برای همگرا شدن به زمان زیادی نیاز دارد . بی نهایت گرایی به این دلایل الگوریتم دیگری به نام مسیریابی حالت پیوند جای ان را گرفت اکنون شکلهای گوناگونی از مسیر یابی حالت پیوند مورد استفاده قرار میگیرد.

ایده مسیر یابی حالت پیوند ساده است ودر پنج بخش بیان می‌شود هر مسیریابباید:

۱-همسایه هایش را تشخیص داده و آدرس شکبه‌ها آنها را بداند.

۲-تاخیر با هزینه تا همسایه هایش را اندازه گیری کند.

۳- ایجاد بسته‌ای که اطلاعات به دست آمده از همسایه‌ها را نگهداری کند.

۴-این بسته‌ها را به تمام مسیریاب‌ها ارسال نماید.

۵-کوتاهترین مسیر به هر مسیر دیگر را محاسبه کند.

در نتیجه کل توپولوژی و تمام تاخیرها به طور آزمایشی اندازه گیری می‌شود وبه مسیر یاب‌های دیگر توزیع می‌گردد. سپس الگوریتم‌های دیکسترا می‌تواندبرای یافتن کوتاهترین مسیرها را به مسیر یاب‌ها دیر مورد استفاده قرار گیرد هریک از پنج مرحله را به تفضیل مورد بررسی قرار می‌دهیم.

کسب اطلاعاتی راجع به همسایه‌ها

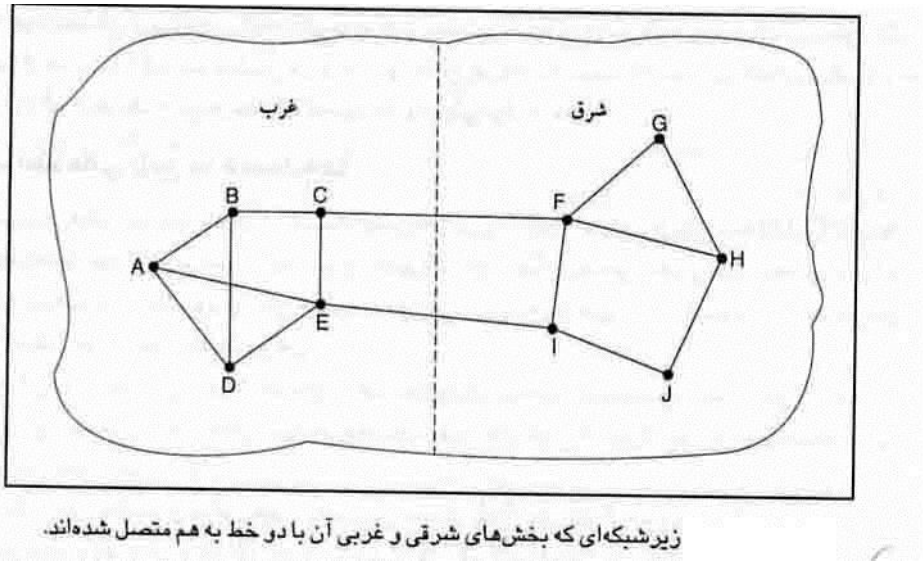
وقتی مسیر فعال شد، اولین کارش این است که همسایه اش را بشناسد این کار با ارسال بسته HELLO ویژه ای به هر خط نقطه به نقطه انجام می‌شود. انتظار می‌رود مسیریابطرف دیگر پاسخی بدهد وخود را معرفی کند این اسامی باید منحصر به فرد باشند زیرا وقتی مسیریاب دور،می یابدبه F متصل اندباید مشخص کند که آیا منظور هر سه ، همان F است یا خیر؟

وقتی دو یا چند مسیریابا شبکه های محلی را به هم متصل باشند. وضعیت کمی پیچیده تر است. شکل ۷ الف شبکه محلی را با سه مسیریابA,C,F نشان می دهد که مستقیما به آن متصل‌اند هرکدام از این مسیریاب‌ها به یک یا چند مسیریاب دیگر متصل شده‌اند .

یک روش مدل سازی شبکه محلی این است که به عنوان یک گروه در نظر گرفته شود شکل(۷ ب)در اینجا گره جدید و مصنوعی به نام N را معرفی می کردیم . که F,C,A به آن متصل اند امکان رفتن از A به C در شبکه محلی ، با مسیر ANC مشخص شده است.

اندازه گیری هزینه خط

در الگوریتم مسیر حالت پیوند لازم است. هر مسیریاباندازه تاخیر تا همسایه هایش را بداند. و یا حداقل ، اندازه تقریبی آن مشخص باشد مستقیم، ترین راه برای تعیین این تاخیر، ارسال بسته ECHO ویژه ای در خط است که طرف دیگر آن را فوراً برگرداند، با اندازه گیری زمان رفت وبرگشت و تقسیم ان بردو ، مسیریابفرستنده می تواند تخمین معقولی از تاخیر را به دست اورد حتی برای نتایج بهتر، این کار می توان چند بار انجام داد و میانگین را مورد استفاده قراردارد. در این روش به طور ضمنی فرض می‌شودکه تاخیرها متقارن اند. درحالی که همیشه این طور نیست.



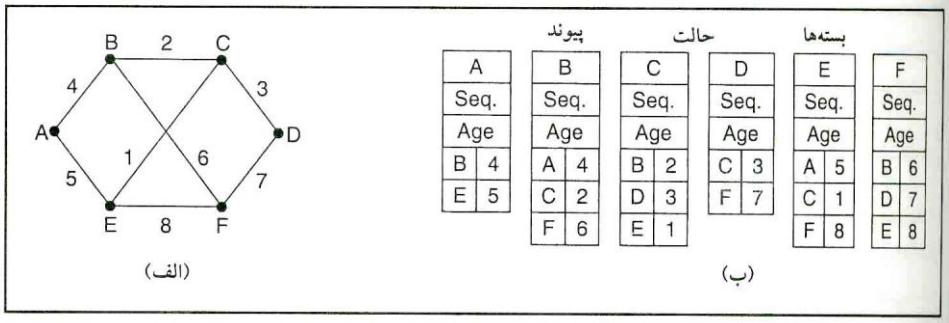
زیرشبکه‌ای که بخش‌های شرقی و غربی آن با دو خط به هم متصل شده‌اند.

موضوع جالب این است که آیا هنگام اندازه گیری تاخیر، با را باید درنظر گرفت یا خیر برای در نظـر گـرفتن بـار، تـایمر رفـت وبرگشت باید از زمانی که ECHO در صف قرار می‌گیرد. شروع به کار کند برای صرف نظر از بار،تـایمر رفـت وبرگشـت بایـد از زمانی که ECHO به جلوی صف رسیده باشد.

هر دو روش بحث هایی را می طلبد معنای به حساب آوردن تاخیرهای مربوط به ترافیک ، این است که وقتی مسیریاب دو خط با پهنای باند مساوی را در پیش روا داشته باشد، به طوری که یکی از آنها همواره تحت بار سنگین قراردارد و دیگری این ایـن طور نباشد مسیر مربوط به خط فاقد بار را به عنوان مسیر کوتاهتر در نظر می گیرد. این روش کارایی بهتری دارد متاسـفانه بـا در نظر گرفتن بار در محاسبات تاخیر مخالفت هایی صورت گرفت زیر شبکه شکل ۸ را در نظر بگیرید که به دو بخش شرقی و غربی تقسیم شده است و توسط دو خط CF-, EI به هم متصل شده‌اند فرض کنید بیشترین ترافیک بین شرق غرب از خـط ترافیک شرقی – غربی از طریق EI منتقل می شودو بار ان افزون می گردد. در نتیجه در بازسازی بعدی، CF کوتـاهترین مسـیر خواهد بود. لذا امکان دارد جدول های مسیر یابی شدیدا تغییر می کنندو منجر به مسیر یابی غیر عادی و بسـیاری از مشـکلات دیگر شوند. اگر از بار صرف نظر شودو فقط پنهای باند منظور گردد، این مشکل نمی‌آید از طرف دیگر بـار مـی‌توانـد در هـر دو خط پخش شود. اما این راه حل ، بهترین مسیر را مورد استفاده قرار نمی دهد با این وجود برای اجتناب از برخـورد در انتخـاب بهترین مسیر، معقول است که بار در چندین خط توزیع شود.

ساخت بسته‌های حالت پیوند

وقتی اطلاعات مورد نیاز برای مبادله جمع آوری شد قدم بعدی هر مسیریاب این است که بسته‌ای حاوی تمام داده‌هـا ایجـاد کند. در ابتدای هر بسته،هویت فرستنده قرار می گیرد، سپس شماره ترتیب و سن قرار دارد و تعدادی از همسایه‌ها به دنبال آن قرار می گیرند راجع به سن قرار دارد در ادامه توضیح داده خواهد شد. برای هر همسایه ، تاخیر در خطوط نشان داده شـده‌انـد بسته حالت ۱بوندمتناظر با هر شش مسیریابدر شکل ۹ (ب) آمده است.



(الف) زیرشبکه. (ب) بسته‌های حالت‌پیوند مربوط به زیرشبکه (الف).

ساخت بسته های حالت پیوند ساده است. بخش مشکل ان تعیین زمان ساخت آن ها است یک راه حل این است که به طور دوره ای ساخته شوند. یعنی ،در فواصل زمانی ایجادگردند. روش دیگر این است که وقتی رویدادهای مهمی مثل از کار افتادن خط یا همسایه وفعال شدن دوباره انها یا تغییر خواص آن، اتفاق می‌افتد ایجاد گردد.

توزیع بسته‌های حالت پیوند.

جالب ترین بخش الگوریتم توزیع قابل اعتماد بسته های حالت پیوند است وقتی بسته ها توزیع شدند و درخط قرار گرفتندمسیر یاب‌ها اولین بسته هایی را که دریافت می‌کنند، تغییر می‌دهند. در نتیجه مسیر یاب‌های مختلف ممکن است نسخه هایی گوناگونی از توپولوژی را به کار گیرند،و این کار منجر به ناسازگاری حلقه های، ماشین‌های غیر قابل دستیابی و سایر مشکلات شوند.

ابتدا، الگوریتم توزیع اولیه رامورد بحث قرار می‌دهیم. سپس اصلاحاتی را انجام دهیم ایده اصلی ، استفاده از الگوریتم غرق کردن برای توزیع بسته های حالت پیوند است برای کترل غرق کردن هر بسته حاوی شماره ترتیبی است که با ارسال هر بسته، یک واحد افزایش می‌یابد.وقتی بسته حالت پیوند دیگری دریافت می‌شود ،با لیستی از بسته‌ها که تاکنون دیده شده‌اند مقایسه می‌شود اگر بسته‌ای دریافت شود. به هر خطی به جز خطی که از ان آمده است، توزیع می‌گردد.و اگر تکراری باشد،صرف نظر می‌شوداگر بسته‌ای دریافت شود که شماره ترتیب آن کوچک تر از بالاترین شماره‌ای باشد که تاکنون مشاهده شده است به دلیل کهنه بودن رد می‌شود. زیر مسیریابداده‌ها جدیدی دارد.این الگوریتم دارای مشکلات خاصی است اما این مشکلات قابل کنترل‌اند یکی این که اگر شماره‌ها تمام شدند، بسته هایی بعدی از اول شماره گذاری شوند راه حل این مشکل، استفاده از شماره ترتیب ۳۲ بیتی ۳۲ بیتی است اگر در هر دقیقه یک بسته حالت پیوند ایجاد شود.۱۳۷سال طول می کشد تا چرخش صورت می‌گیرد. لذا از این حالت می‌توان صرف نظر کرد.

دوم اینکه اگر مسیریاباز کار افتد و شماره ترتیب خود را از دست می دهد. اگر مجدداً از صفر شروع کند، بسته بعدی به عنوان بسته تکراری رد خواهد شد.

سوم اینکه اگر شماره ترتیب خراب شود و ۵۴۰،۶۵ به جای ۴(خطای یک بیتی) دریافت شود ، بسته های ۵ تا ۵۴۰،۶۵ به علت کهنگی رد می‌شوند زیرا فرض می‌شود که شماره ترتیب باید ۵۴۰،۶۵ باشد.

راه حل این مشکلات این است که سن هر بسته بعد از شماره ترتیب قرار داده می شود و هر ثانیه یک واحد از آن کسر گردد . وقتی که سن به صفر رسید. از اطلاعات حاصل از آن مسیریاب صرف نظر می شود. فرض کنید در هر ۱۰دقیقه بسته جدیدی می رسد. لذا مهلت اطلاعات مسیریاب وقتی تمام می شود که مسیریاب غیر فعال شود یاشش بسته متوالی از بین رفته باشد، البته این حالت رویداید نامحتملی است هرمسیریاب در فرآیند غرق کردن اولیه، از فیلد سن یک واحد می کاهد لذا اطمینان حاصل می‌شود که هیچ بسته‌ای نمی‌تواند از بین برود و یا مدت زمان زیادی زنده بماند (بسته‌ای که سن آن به صفر باشد. نادیده گرفته می‌شود.)

اصلاحاتی در این الگوریتم توانمندی ان را زیاد می کند وقتی بسته حالت پیوند به مسیریابمی آید تا ارسال شود فورا برای انتقال در صف قرار نمی گیرد.بلکه به ناحیه نگهدارنده‌ای می‌رود تا مدت کوتاهی را منتظر بماند. اگر قبل از انتقال آن ، بسته دیگری از همان منبع برسد، شماره ترتیب آنها مقایسه می‌شود اگر باهم برابر باشند بسته تکراری نادیده گرفته می‌شود اگر مساوی نباشند قدیمی تر، نادیده گرفته می‌شود اگر مساوی نباشند. قدیمی تر نادیده گرفته نادیده گرفته خواهد شد. برای حفاظت در مقابل خطاها مسیریاب مسیریابتمام بسته‌های حالت پیونداعلام وصول می‌شوند وقتی خط آزاد می‌شود ناحیه نگهدارنده به طریق نوبتی پیمایش می‌شود. تا بسته با اعلام وصولی را برای ارسال انتخاب نماید.

ساختمان داده‌ای که مسیریابB برای زیر شبکه شکل ۱۳-۵ الف استفاده می کند در شکل ۱۰ آمده است هر سطر ، متناظر با بسته حالت پیوندی است که از راهع رسید و هنوز به طور کامل پردازش نشده است. جایی که بسته از انجا ارسال شد و شماره ترتیب وسن ، داده های ان درجدول ذخیره می شود به علاوه نشانگرهای ارسالی و اعلام وصول برای هر سه خط B وجود دارند به ترتیب به F,C,A معنای نشانگرهای ارسالی این است که بسته باید به خط تعیین شده ارسال گرددو معنای نشانگرهای اعلام وصول این است که باید در آنجااعلام وصول شوند.

در شکل ۱۰ بسته حالت پیوند مستقیما از A رسیده است. لذا همانطور که با بیت‌های نشانگر نشان داده شده است باید به C, F ارسال شود. و به A اعلام وصول گردد. به طور مشابه بسته‌ای از F باید به A و C ارسال شود و به F اعلام وصول گردد.

اما، وضعیت در بسته سوم که از E می‌آید. این بسته دوباره می‌آید یک بار از طریق EAB و یک بار از طریق EFB در نتیجه فقط باید به C ارسال گردد، اما باید به A و F اعلام وصول شود (همانطور که با بیت‌ها مشخص شده است.)

	نشانگرهای اعلام وصول			نشانگرهای ارسال					
داده‌ها	F	C	A	F	C	A	سن	ترتیب	منبع
	۰	۰	۱	۱	۱	۰	۶۰	۲۱	A
	۱	۰	۰	۰	۱	۱	۶۰	۲۱	F
	۱	۰	۱	۰	۱	۰	۵۹	۲۱	E
	۰	۱	۰	۱	۰	۱	۶۰	۲۰	C
	۱	۱	۰	۰	۰	۱	۵۹	۲۱	D

بافر بسته برای مسیریاب B در شکل ۱۳-۵.

اگر بسته ها اولیه هنوز دربافر باشد و بسته تکراری دریافت شود،بیتها باید تغییر کنندو به عنوان مثال اگر قبل از این که وارده چهارم موجود در جدول ارسال شود. یک کپی از حالت c برسد این شش بیت به ۱۰۰۰۱۱ تغییر می کند تا نشان دهد که بسته باید به f اعلام وصول شود ، ولی نباید به آنجا ارسال گردد.

محاسبه مسیرهای جدید

وقتی مسیریابمجموعه کاملی از بسته های حالت پیوند را جمع اوری کرد، می تواند گراف کامل زیر شبکه را ایجادنماید ،زیرا همه پیوندها نمایش داده می شوند در واقع هر پیوند دوبار نمایش داده مس شود در هر جهت یکبار از میانگین دو منقدار یا از هرکدام به طور جداگانه می‌توان استفاده کرد.

اکنون الگوریتم دیکسترا را می‌توان اجرا کرد تا کوتاه ترین مسیر به همه مقصدها را بیاید نتایج این الگوریتم می‌تواندر جدول مسیر یابی قرار گیرد و عمل عادی از سر گرفته شود.

برای زیر شبکه‌ای با n مسیریاب که هرکدام k همسایه داشته باشد حافظه لازم را برای ذخیره داده ورودی متناسب با kn است این موضوع در شبکه‌های بزرگ می‌تواند مشکل زا باشد زمان محاسبه نیز ممکن است زیاد باشد با این وجود مسیر یابی حالت پیوند در بسیاری از حالتهای عملی به خوبی کار می‌کند.

به هر حال مشکلات نرم افزاری و سخت افزاری این الگوریتم می‌تواند موجب بروز خساراتی شود در الگوریتم‌های دیگر نیز همین طور است به عنوان مثال اگر مسیریابی خطی را فاقد آن است تقاضا کند؛ یا خطی را که دارای آن است از دست بدهد، گراف زیر شبکه‌های درست نخواهد بود. اگر مسیریاب در ارسال بسته‌ها شکست بخورد یا در حین ارسال ،آنها را خراب می‌کند.مشکلاتی پیش می‌آید. نرم افزاری و سخت افزاری این الگوریتم می‌تواند موجب بروز خساراتی شود در الگوریتمهای دیگر در همین طور است به عنوان مثال اگر مسیر یابی خطی را فاقدآن است تقاضا کند، یاخطی را که دارای آن است از دست بدهد گراف زیرشبکه درست نخواهد بود. اگر مسیریابدر ارسال بسته ها شکست بخورد یا در حین ارسال ، آنهارا خراب

کند،مشکلات پیش می آید، سرانجام، اگر حافظه کافی وجود نداشته باشد.یا محاسباتی مسیریابی را به درستی انجام ندهد، اتفاقات بدی خواهد افتاد وقتی شبکه دارای ده‌ها یا صدها هزار گره باشد شکست گاه به گاه مسیریاب اهمیت می‌یابد در این خصوص باید سعی کرد خسارت را کاهش داد. پرلمن (۱۹۸۸) این مشکلات و راه حل‌های آنها را به تفضیل بحث کرد.

مسیر یابی حالت پیوند در شبکه های واقعی به طور گسترده به کار رفته است ، لذا مثال هایی در رابطه با آن ارائه شده اند، قرار داد ospf به طور فزاینده‌ای در زیر شبکه‌ای به کار گرفته می‌شود، از الگوریتم‌های حالت پیوند استفاده می‌کند ospf که به طور فزاینده‌ای در زیر شکبه به کار گرفته می‌شود ، از الگوریتم حالت پیوند استفاده می‌کند.

قرارداد حالت پیوند مهم دیگر is-is(سیستم میانی - سیستم میانی) نام دارد که برای شبکه dec طراحی شد وبعداً iso آنرا پذیرفت تا در قرارد داد لایه شبکه بی اتصال خود یعنی clnp به کار گیرد از آن پس ، اصلاح شد تا به سایر قرار دادها به خصوص ip خدمات ارائه کند is-is در بسیاری از ستونهای فقرات اینترنت به کار گرفته شد از جمله در ستون فقرات nsfnat قدیمی و در بعضی از سیسمتهای سلولی دیجیتال مانند cdpd نیز به کاررفت شبکه novel از شکل تغییر یافته ای از is-is(nlsp برای مسیر یابی بسته‌های ipx استفاده می‌کند .

اساسا is-is تصویری از توپولوژی مسیریاب را توزیع می‌کند که از آن کوتاهترین مسیرها محاسبه می‌شوند هر مسیر یاب، در اطلاعات حالت پیوند خود، اعلام می‌درد که به کدام آدرسهای لایه شبکه مستقیما دسترسی دارداین آدرس ها، می‌توانند : از متد خود ایستایی مربوط به بازسازی‌های حالت پیوند غرق کردن ،مفهوم مسیریاب تعیین شده در شبکه مستقیماًدسترسی دارد این آدرس‌ها می‌توانند ip-ipx-apple talk یا بسیاری از آدرس‌های لایه شبکه را پشتیبانی کند.

ospf بسیاری از ابداعاتی را که is-is طراحی کرده پذیرفت ospe چند سال بعد از iS-IS طراحی شد این ابداعات عبارتند از متدخود ایستایی مربوط به بازسازی های حالت پیوند غرق کردن،مفهموم مسیریابتعیین شده در شبکه محلی ،و متد محاسبه وپشتیبانی تقسیم مسیر و مقیاس های چندگانه ، درنتیجه تفاوت اندکی بین IS-IS و oSPF وجود دارد. مهمترین اختلاف این است که IS-IS طوری رمز گذاری شده است که می‌توان به طور همزمان اطلاعاتی راجع به قراردادهایی که لایه شبکه چندگانه را انتقال داد، این ویژگی در OSPF وجود ندارد این امتیاز در محیطهای قرارداد چندگانه بزرگ ،ارزشمند است.

مسیریابی سلسله مراتبی

با بزرگ شدن اندازه شبکه، جدول‌های مسیر یابی مسیریابنیز به تناسب آن رشد می‌کنند. با بزرگ شدن اندازه جدول‌های ، نه تنها حافظه مصرف شده بیشتر می‌گردد ، بلکه زمان لازم برای جست وجو درجدول بیشتر می‌شود. و برای گزارش وضعیت آنها

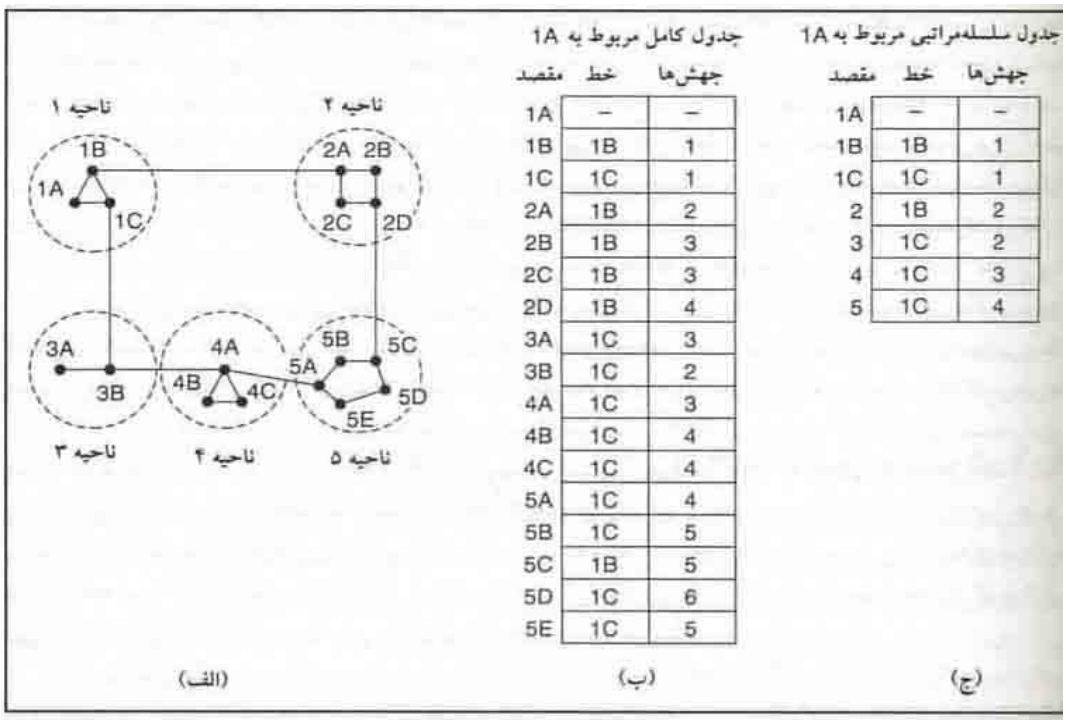
به پنهای باند بیشتری نیاز است . ممکن است شبکه های به حدی رشد که دیگر امکان نداشته باشد.که هر مسیر باب برای هـر مسیریاب دیگر دارای یک وارده باشد ، لذا مسیر یابی به صورت سلسله مراتبی انجام می‌شود. مانند شبکه تلفن.)

وقتی مسیر یابی سلسله مراتبی به کار گرفته می‌شود ، مسیر یاب‌ها به ناحیه هایی تقسیم می‌شوند به طوری که هر مسیریابدر ناحیه خودش تمام جزئیات مربوط به چگونگی ارسال بسته‌ها به مقصدها را می‌داند اما از ساختار داخلی سایر ناحیه خبر ندارد. وقتی شبکه‌های مختلفی به هم وصل می‌شوند. طبیعی است که باید به صورت ناحیه‌های جداگانه در نظر گرفته شوند تـا نیـاز نباشدمسیر یاب‌های موجود دریک شبکه ، از ساختار توپولوژیکی مسیر یاب‌های دیگر اطلاع داشته باشند.

درشبکه‌های بزرگ،امکان دارد سلسله مراتب دو سطحی کافی باشد، امکان دارد لازم باشد که ناحیه‌ها به صورت خوشه‌ها دسته بندی شوند، خوشه‌ها به منطقه هایی تقسیم تقسیم شوندو غیره این روند آنقدر ادامه می‌یابد تا دیگر اسمی بـرای گـروه بنـدی وجود نداشته باشند. به عنوان مثال از سلسله مراتب چند سطحی ،فکر کنید که بسته چگونه مـی توانیـد ترافیـک را بـه مسـیر یابهای محلی دیگر هدایت کند، اما ترافیک ها خارج از ایالت را به مسـیریابلوس انجلـس مـی فرسـتد.مسـیریاب لـوس آنجلـس می‌تواند ترافیک را به مسیریاب‌های محلی دیگر هدایت کند،اما ترافیـک‌هـای ناحیـه‌ای را بـه نیوریـک مـی‌فرسـتند.مسـیریاب نیویورک می تواند طوری برنامه نویسی شود که کل ترافیک را به مسـیریابی در کشـور مقصـدی کـه مسـئول کنتـرل ترافیـک ناحیه‌ای است ، مثل نایروبی ، هدایت کند، سرانجام ،بسته به سمت پایین درخت در کنیا حرکت می‌کند تا به مالیندی برسد.

شکل ۱۱ یک مثال کمی از مسیریابی در سلسله مراتب دو سطحی با پنج ناحیه را نشـان مـی‌دهـد. جـدول مسـیریابی کامـل مربوط به مسیریاب A۱ دارای ۱۷ وارده است(شکل ۱۱)(ب) وقتی مسیریابی‌های محلی،وارده‌های ،وجود دارد،امـا ناحیـه‌هـای دیگر در یک مسیر باب جمع شده‌اند لذا کل ترافیک ناحیه ۲ از طریق خط A۲B-۱ منتقل می‌شود اما بقیه ترافیـک از راه دور ،از طریق خط B۳C-۱ منتقل خواهد شد مسیر یابی‌ها در هر ناحیه،صرفه جویی در فضای جدول بیشتر می‌شود.

با این صرف جویی ،باید تاوانی را پس داد و آن، افزایش طول مسیر است به عنوان بهترین مسیر از A۱ به SC از طریق ناحیـه ۲ است ،اما در مسیر یابی سلسله مراتبی ،۵ از طریق ناحیه ۳ منتقل می‌شود زیرا این کار برای اغلـب مقصـدها در ناحیـه پـنج بهتر است .



جدول کامل مربوط به 1A

مقصد	خط	جهش‌ها
1A	–	–
1B	1B	1
1C	1C	1
2A	1B	2
2B	1B	3
2C	1B	3
2D	1B	4
3A	1C	3
3B	1C	2
4A	1C	3
4B	1C	4
4C	1C	4
5A	1C	4
5B	1C	5
5C	1B	5
5D	1C	6
5E	1C	5

جدول سلسله‌مراتبی مربوط به 1A

مقصد	خط	جهش‌ها
1A	–	–
1B	1B	1
1C	1C	1
2	1B	2
3	1C	2
4	1C	3
5	1C	4

مسیریابی سلسله مراتبی.

وقتی شبکه منفردی بسیار بزرگ می‌شود این سوال مطرح است: سلسله مراتب چند سطح باید داشته باشد؟ بعنوان مثال زیر شبکه ای با ۷۲۰ مسیریاب را در نظر بگیرید. اگر سلسله مراتبی وجود نداشته باشد، هر مسیریاب به ۷۲ وارده جدول نیاز دارد اگر زیر شبکه به ۲۴ ناحیه ۳۰ مسیریابی تقسیم شود هر مسیریاب نیازمند ۳۰ وارده محلی و ۲۳ وارده راه دور است که مجموع آن ۵۳ وارده است. اگر سلسله مراتب سه سطحی انتخاب شود، با هشت دسته که هر کدام حاوی ۹ ناحیه از مسیریاب ها باشند هر مسیریاب برای مسیریابی محلی به ۱۰ وارده نیاز دارد و برای مسیریابی به سایر نواحی در دسته خود به ۸ وارده نیاز دارد و برای خوشه های راه دور به ۷ وراده نیاز دارد که در مجموع برابر با ۲۵ است. کامون و کلینراک (۱۹۷۹) کشف کردند که بهترین تعداد سطوح در زیر شبکه‌ای با N ln است که به ازا هر مسیریاب به N ln وارده نیاز دارد. آنها همچنین نشان دادند که افزایش میانگین طول مسیر در اثر مسیریابی سلسله مراتبی اندک است و اغلب قابل قبول خواهد بود.

مسیریابی پخشی(Broadcast)

در بعضی از کاربردها میزابانها می خواهند پیام هایی را به تمام یا بعضی از میزبانها ارسال کنند، بعنوان مثال خدمات توزیع گزارشات هواشناسی، بازسازی های بازار سهام، یا برنامه رادیویی روزمره، با عمل پخش به تمام ماشینها و خواندن اطلاعات توسط آن ماشینها بهتر کار می‌کنند ارسال همزمان بسته‌ای به تمام مقصدها، پخش کردن نام دارد. برای انجام آن راههای گوناگونی پیشنهاد شدند.

یک روش پخش که نیاز به ویژگی خاصی از زیر شبکه ندارد، این است که منبع، بسته متفاوتی را به تمام مقصدها بفرستد.ای روش نه تنها پهنای باند زیادی را مصرف می‌کند بلکه لازم است منبع لیست کاملی از تمام مقصدها را داشته باشد در عمل این راه حل ممکن است، تنها امکان باشد، اما روش مطلوبی نیست.

روش دیگر، غرق کردن است. گرچه غرق کردن برای ارتباطات نقطه به نقطه مناسب نیست، ولی برای پخش می‌تواند قابل قبول باشد به ویژه اگر هیچکدام از روشهای تشریح شده زیر، قابل استفاده نباشند. مشکل غرق کردن به عنوان تکنیک پخش این است که بسته‌های زیادی تولید می‌کند و پهنای باند بسیاری را مصرف می‌نماید. این مشکلات در به کار گیری آن بعنوان الگوریتم مسیریابی نقطه به نقطه نیز مطرح اند.

الگوریتم سوم مسیریابی مقصدهای چندگانه است. اگر این روش به کار گرفته شود، هر بسته یا حاوی لیستی از مقصدها است یا حاوی نگاشت بیتی است که نشان دهنده مقصد است. وقتی بسته‌ای به مسیریاب می‌رسد مسیریابها تمام مقصدها را کنترل می‌کند تا مجموعه‌ای از خطوط خروجی مورد نیاز را تعیین نماید (خط خروجی در صورتی مورد نیاز است که بهترین مسیر به حداقل یکی از مقصدها باشد) مسیریاب نسخه جدیدی از بسته را برای تمام خطوط خروجی که مورد استفاده قرار گرفتند تولید می‌کند و در هر بسته فقط مقصدهایی را قرار می‌دهد که خط را به کار می‌گیرند. در نتیجه مجموعه مقصد بین خطوط خروجی تقسیم می‌شود. پس از تعداد کافی از جهش‌ها، هر بسته فقط یک مقصد را با خود می‌برد و می‌توان با آن مثل بسته معمولی برخورد کرد. مسیریابی مقصدهای چندگانه مانند بسته هایی است به طور جداگانه آدرس دهی شدند، مگر هنگامی که چند بسته از یک مسیر هدایت شوند که در این صورت یکی از آنها کل هزینه را می‌پردازد و بقیه مجانی عبور می‌کنند.

چهارمین الگوریتم پخشی، برای مسیریاب آغازگر پخش، از درخت بایگانی استفاده می‌کندۀ یا از هر درخت پوشای مناسب استفاده می‌نماید. درخت پوشا زیر مجموعه‌ای از زیرشبکه است که تمام مسیریابها را در بر می‌گیرد و فاقد حلقه است. اگر هر مسیریاب بداند کدامیک از خطوط متعلق به درخت پوشا است، می‌تواند بسته دریافتی را بر روی تمام خطوط درخت پوشا به جز خطی که بسته از آن رسیده است کپی نماید این روش از پهنای باند به خوبی استفاده می‌کند؛ و کمترین تعداد بسته‌های مورد نیاز برای انجام این کار را تولید می‌نماید. این روش از پهنای باند به خوبی استفاده می‌کند و کمترین تعداد بسته‌های خمورد نیاز برای انجام کار را تولید می نماید. تنها مشکل این است که هر مسیریاب باید اطلاعاتی راجع به درخت پوشا داشته باشد. گاهی این اطلاعات وجود دارند (مثلا، در مسیریابی حالت پیوند)، اما گاهی نیز وجود ندارد (مثلا در مسیریابی بردار فاصله).

آخرین الگوریتم پخشی، حتی هنگامی که مسیریابها اطلاعاتی راجع به درختهای پوشا نداشته باشند، سعی می کند رفتار الگوریتم قبلی را تخمین بزند. این ایده، پیشروی مسیر معکوس نام دارد و بسیار ساده است. وقتی بسته پخشی به مسیریاب می‌رسد مسیریاب کنترل می‌کند آیا بسته دریافت شده از منبع از همان خطی آمدکه بسته‌ها در حالت عادی برای آن منبع

پخش ارسال می‌شوند یا خیر. اگر اینطور باشد، احتمال این که بسته پخشی خودش بهترین مسیر را از منبع طی کند بسیار زیاد است و اولین نسخه‌ای است که به مسیریاب می‌رسد به این ترتیب مسیریاب نسخه‌هایی از آن را به تمام خطوی به جز خطی که از آن آمده است می‌فرستد اما اگر بسته پخشی برای رسیدن به منبع از خطی غیر از خط بهینه وارد شود بسته بعنوان بسته تکراری نادیده گرفته می‌شود.

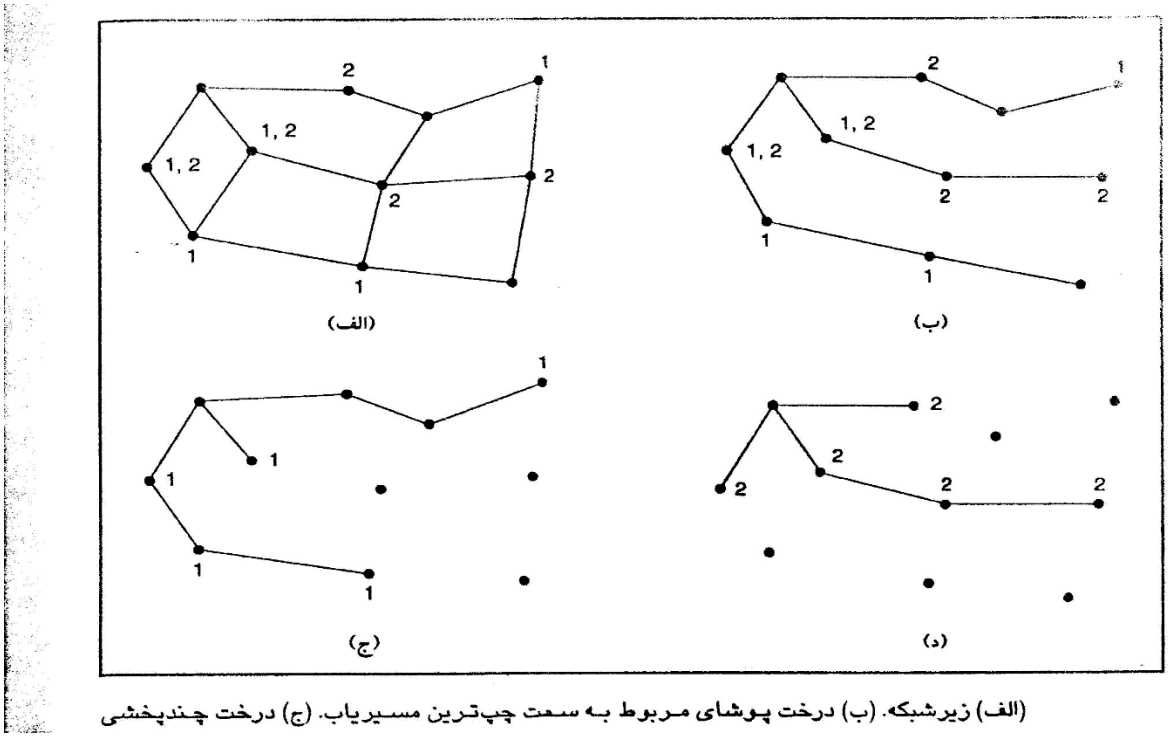
نمونه‌ای از الگوریتم پیشروی مسیر معکوس در شکل ۱۲ آمده است. قسمت (الف) زیرشبکه را نشان میدهد، قسمت (ب) درخت بایگانی مربوط به مسیریاب I آن زیر شبکه را نشان می دهد و قسمت (ج) چگونگی عملکرد الگوریتم مسیر معکوس را نشان می‌هد در جهش اول U بسته هایی را به N , H , H , F می‌فرستد (که در سطر دوم درخت نشان داده شده است). هر کدام از این بسته‌ها از مسیر بهینه به I دریافت می‌شونهد (با فرض اینکه مسیر بهینه در درخت بایگانی باشد) و دور حرف آن دایره‌ای کشیده شده است. در جهش دوم هشت بسته تولید می‌شوند؛ هر مسیریابی که در جهش اول بسته‌ای را دریافت کرد، دو بسته تولید می‌کند. ضمن تولید تمام این هشت بسته به مسیریاب‌های ملاقات نشده قبلی می‌رسند که پنج بسته از آنها در امتداد خط بهینه به مقصد می‌رسد. از شش بسته‌ای که در جهتش سوم تولید می‌شود فقط سه تا از مسیر بهینه می‌رسند (در K , E , C) و بقیه تکراری‌اند. پس از پنج جهش و ۲۴ بسته، پخش خاتمه می‌یابد در حالی که اگر درخت بایگانی دنبال می‌شد چهار جهش و ۱۴ بسته لازم بود.

امتیاز مهم پیشروی مسیر معکوس این است که کارایی خوبی دارد و پیاده سازی آن ساده است. لازم نیست مسیریابها اطلاعاتی راجع به درختهای پوشا داشته باشند، و در هر بسته نیازی به سربار لیست مقصدها یا نگاشت خصی نیاز ندارد، در حالی که فرایند غرق کردن به این راهکار نیاز دارد (شمارنده جهش درهر بسته و اطلاع قبلی از قطر زیر شبکه، یا لیستی از بسته هایی که تا کنون از هر منبع دریافت شده اند.)

مسیریابی چند پخشی

در بعضی از کاربردها فرایندهای مستقل از هم به صورت گروهی کار می‌کنند مانند گورهی از فرایندهای سیستم بانک اطلاعاتی توزیعی را پیاده سازی می‌کنند. در مواد اغلب لازم است یکی از فرایندها پیامی را به سایر اعضای گروه ارسال نماید. اگر گروه کوچک باشد، می تواند پیام نقطه نقطه را به تمام اعضا صادر کند. اگر گروه بزرگ باشد، این راهبرد گران تمام می‌شود. گاهی می‌توان از پخش استفاده کرد، اما استفاده از پخش برای اطلاع دادن به ۱۰۰۰ ماشین در شبکه‌ای با میلیونها گره کارآمد نیست، زیرا اغلب گیرنده‌ها علاقه‌ای به پیام ندارند (حتی در حالت بدتر، علاقه دارند و تصور دیدن آن را ندارند.) بنابراین باید بتوانیم پیام ها را به گروهی بفرستیم که اندازه آن گروه از نظر عددی بزرگ باشد ولی در مقایسه با کل شبکه کوچک باشد.

ارسال پیام به چنین گروهی چند پخشی نام دارد و الگوریتم مسیریابی آن، مسیریابی چند پخشی نامیده می‌شود. در این بخش یکی از روشهای مسیریابی چند پخشی را بررسی می‌کنیم.



(الف) زیرشبکه. (ب) درخت پوشای مربوط به سمت چپ‌ترین مسیریاب. (ج) درخت چندپخشی

برای انجام چند پخشی نیاز به مدیریت گروه است روشهایی برای ایجاد و حذف گروه لازم است و نیاز به فرایندهایی برای اتصال به گروه و ترک آن است. انجام این کارها به عهده الگوریتم مسیریابی نیست. آنچه که به الگوریتم مربوط می شود این است که وقتی فرایندی به گروه ملحق می شود، آن را به میزبان خود خبر می دهد. توجه به این نکته مهم است که مسیریابها می دانند کدام میزبان آنها به کدام گروه تعلق دارند. یا میزبانها باید تغییر در گروه را به اطلاع مسیریابها برسانند، یا مسیریابها هر از چند گاهی از میزبانها درخواست کنند. در هر دو روش مسیریابها می فهمند که میزبانهای آنها در چه گروه هایی قرار دارند. مسیریابها به همسایه‌های خود خبر می‌دهند و بدین ترتیب اطلاعات از طریق زیرشبکه انتشار می‌یابد.

برای مسیریابی چند پخشی، هر مسیریاب، درخت پوشایی را ایجاد می کند که تمام مسیریابهای موجود در زیر شبکه را در بر گیرد. بعنوان مثال در شکل ۱۳ (الف) زیر شبکه ای با دو گروه ۱ و ۲ وجود دارد. بعضی از مسیریابها به میزبانهایی دست یافتند که متعلق به یک یا هر دو گروه است (همانطور که در شکل آمده است). درخت پوشای مربوط به مسیریاب سمت چپ، در شکل ۱۳ (ب) آمده است.

وقتی فرایندی بسته چند پخشی را به گروهی می فرستد، اولین مسیریاب، درخت پوشای خود را بررسی کرده آن را هرس می کند. برای این کار تمام خطوطی را که به میزبانهایی می روند که عضو این گروه نیستند حذف می کند. در مثال مورد نظر ما

شکل ۱۳ (ج) درخت پوشای هرس شده مربوط به گروه ۱ را نشان می دهد. شکل ۱۳ (د) درخت پوشای هرس شده مربوط بـه گروه ۲ را نشان می‌دهد. بسته‌های چند بخضی فقط از طریق درخت پوشای مناسبی ارسال می‌گردند.

راه‌های گوناگونی برای هرس کردن درخت پوشا وجود دارد. ساده ترین آنها وقتی مورد استفاده قرار می‌گیـرد کـه از مسـیریاب حالت پیوند استفاده گردد و هر مسیریاب از توپولوژی کامل زیر شبکه آگاهی داشته باشد از جملـه بدانـد کـدام مسـیریاب بـه کدام گروه‌ها تعلق دارند. سپس درخت پوشا را می‌توان با شروع از انتها هر مسیر و ادامه دادن به سمت ریشه هرس کـرد بـرای این کار باید تمام مسیریابهایی را که متعلق به گروه مورد نظر نیستند حذف کرد.

در مسیریابی بردار فاصله باید از روش دیگری برای هرس کردن استفاده کرد الگوریتم اصلی پیشروی مسیر معکوس اسـت امـا هر گاه مسیریاب فاقد میزبانی به گروه خاصی متعلق باشد و به مسیریابهای دیگر متصل نباشد پیام چند پخشی برای آن گـروه را دریافت می‌کند، آن گروه با پیام PRUNE پاسخ می‌دهد و به فرستنده می‌گوید که بسته‌های چند بخشـی دیگـری نفرسـتد. وقتی این پیامها به تمام ورودی‌های یک مسیریاب برسند که در بین میزبان‌هایش فاقد اعضای گروه اسـت ایـن مسـیریاب نیـز می‌تواند با PRUNE پاسخ می‌دهد. در این صورت زیر شبکه به طور بازگشتی هرس می‌شود.

یکی از عیب‌های این الگوریتم این است که در شبکه‌های بزرگ به خوبی کار نمی‌کند فرض کنید شبکه‌ای دارای n گروه است و هر گروه به طور متوسط دارای m عضو است. برای هر گروه m درخت هرس شده پوشا باید ذخیره گردد و در نتیجـه تعـداد کل درختها mn است. وقتی گروه‌ها بزرگ باشند حافظه زیادی برای ذخیره همه درختها لازم است.

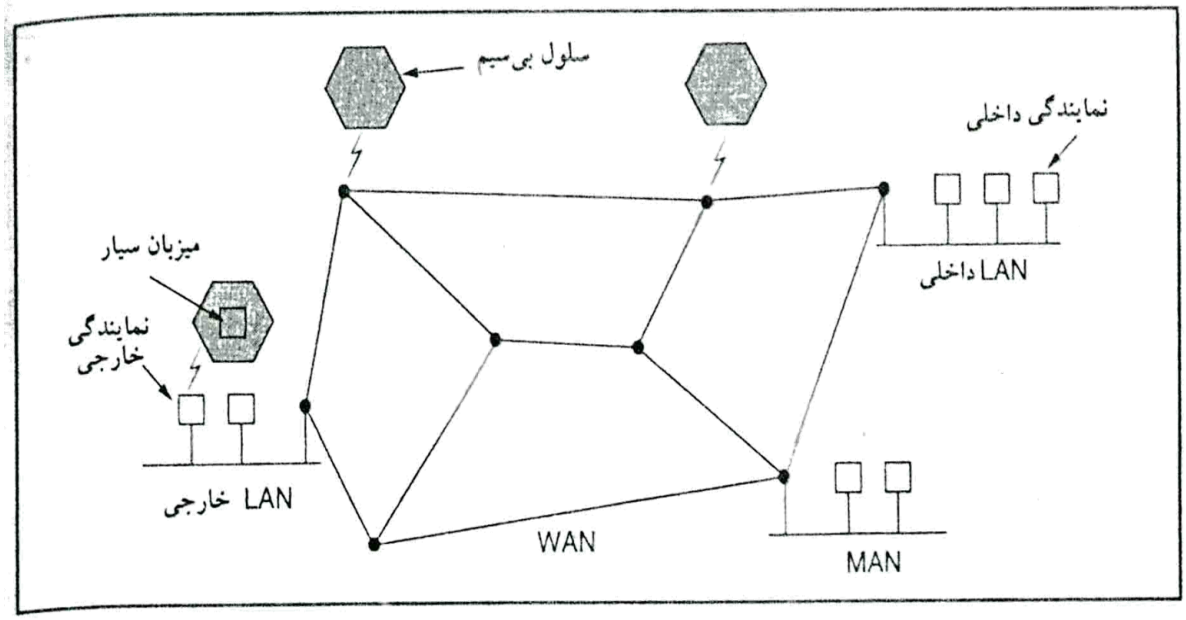
طراحی دیگر از درختهای هسته‌ای (بالاردای و همکاران ۱۹۹۳) استفاده کرده است. در اینجا در هر گـروه یـک درخـت پوشـا محاسبه می‌شود، به طوری که ریشه (هسته) در نزدیک به وسط گروه قرار دارد. برای ارسال پیام چند بخشی میزبـان آن را بـه هسته می‌فرستد و چند پخشی در سراسر درخت پوشا انجام می‌شود. گرچه این درخت برای تمام منابع بهینـه نیسـت کـاهش m درخت به یک درخت در هر گروه موجب صرفه جویی در حافظه می‌شود.

مسیریابی برای میزبانهای سیار

امروزه، میلیونها نفر کامپیوترهای قابل حمل دارند و علاقه مندند در هر جا که هستند پست الکترونیکی خـود را بخواننـد و بـه سیستم فایل معمولی خود نیز دسترسی داشته باشند. این میزبانهای سیار موجب پیچیدگی جدیدی مـی‌شـوند: بـاری هـدایت بسته‌ای به میزبان سیار، شبکه باید ابتدا آن را بیابد موضوع ملحق شدن میزبان‌های سیار به شبکه خیلـی جـوان اسـت امـا در اینجا برخی از مشکلات را مطرح کرده راه حل‌های ممکن را ارائه می‌کنیم.

مدل میانی که طراحان از آن استفاده می‌کنند در شکل ۱۴ آمده است در اینجـا یـک شـبکه گسـترده وجـود دارد کـه حـاوی مسیریابها و میزبانها است. شبکه‌های محلی و شهری و سلول‌های بی سیم به این شبکه گسترده متصل‌اند.

میزبان‌هایی که حرکت نمی‌کنند (ثابت اند) از طریق سیم‌های مسی یا فیبر نوری به شبکه وصل می‌شوند. بر عکس دو نوع میزبان دیگر وجود دارند. میزبانهای مهاجر میزبانهای ثابتی‌اند که گاهی از یک سایت ثابت به سایت ثابت دیگر منتقل می‌شوند اما فقط وقتی از شبکه استفاده می کنند که به طور فیزیکی به آن وصل باشند. میزبانهای متحرک کسانی هستند که در حال حرکت نیز به شبکه متصل اند. این دو نوع میزبان را میزبانهای سیار می‌نامند.



شبکهٔ گسترده‌ای که شبکه‌های محلی و شهری و سلول‌های بی‌سیم به آن متصل‌اند.

فرض می‌شود تمام میزبانها موقعیت داخلی ثابتی داشته باشند که هرگز تغییر نکند. میزبانها آدرس داخلی ثابتی نیز دارند که محل آنها را مشخص می‌کنداین حالت را با شماره تلفن ۱-۲۱۲-۵۵۵۱۲۱۲ مقایسه کنید که نشان دهنده ایالات متحده (کد کشور۱) و جزیره مان هاتان (۲۱۲) است. هدف مسیریابی در سیستمی با میزبانهای سیار، عبارت است از: ارسال بسته ها به میزباهای سیار به کمک آدرسهای داخلی آنها، و خواندن بسته‌ها توسط میزبانها در هر جایی که هستند.

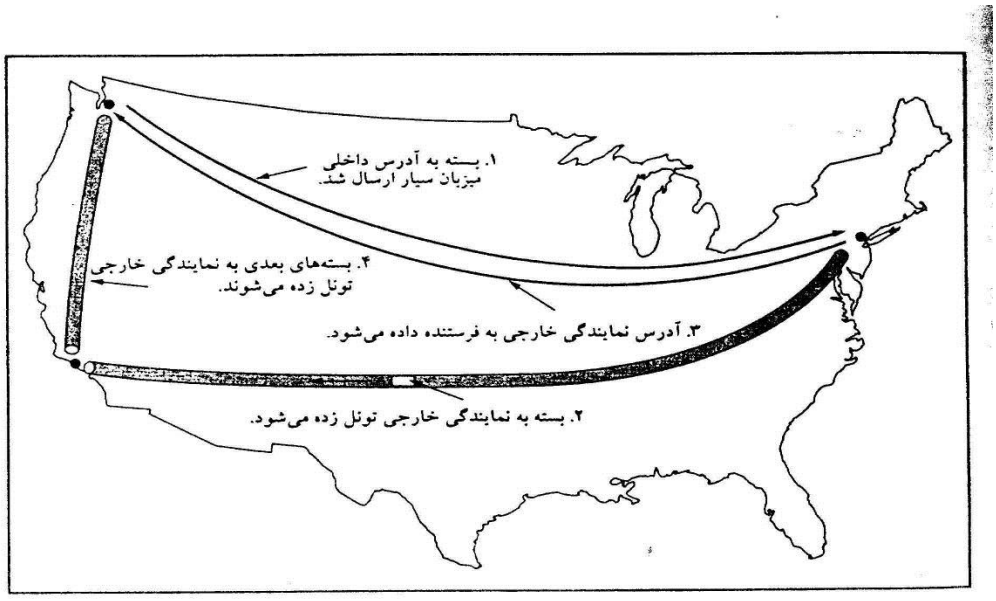
در مدل شکل ۱۴ جهان (از نظر جغرافیایی) به واحدهای کوچکی تقسیم شده است. این واحدها را ناحیه می نامیم به طوری که هر ناحیه یک شبکه محلی یا سلول بی سیم است هر ناحیه دارای یک یا چند نمایندگی خارجی است است که فرایندهایی هستند که تمام میزبانهای سیار ناحیه را نگهداری می کند بعلاوه هر ناحیه دارای نمایندگی داخلی است. این نمایندگی میزبانهایی را که خانه شان در این ناحیه قرار دارد ولی فعلا با ناحیه دیگری در حال ملاقات‌اند نگهداری می‌کند.

وقتی میزبان جدیدی وارد ناحیه ای شود، چه از طریق اتصال به آن (مثل وصل شدن به شبکه محلی)، یا سرگردان بودن در سلول، کامپیوترش باید خودش را با نمایندگی خارجی ثبت نماید. روند ثبت به صورت زیر انجام می‌شود:

۱. هر نمایندگی خارجی به طور تناوبی بسته‌ای را پخش می‌کن تا وجود و آدرس خود را اعلام کند. میزبان سیار تازه وارد ممکن است منتظر یکی از این پیامها باشد اما اگر در مدت معدین چنین پیامی نرسد، میزبان سیار می‌تواند بسته‌ای را پخش کند و بگوید آیا هیچ نمایندگای خارجی وجود دارد؟

۲. میزبان سیار، با نمایندگی خارجی ثبت می شود برای این کار آدرس داخلی خود آدرس لایه پیونده داده فعلی، و اطلاعات سری دیگر را ارائه می‌کند.

۳. نمایندگی خارجی با نمایندگی داخلی میزبان سیار تماس برقرار می کند و می گوید یکی از میزبانهای شما در این جاست، پیامی از نمایندگی خارجی به نمایندگی داخلی، حاوی آدرس شبکه نمایندگی خارجی است. همچنین حاوی اطلاعات سری است تا نماینگی داخلی را متقاعد کند که میزبان سیار واقعا وجود دارد.



مسیریابی بسته برای کاربران سیار.

۴. نمایندگی داخلی اطلاعات سری را که حاوی مهر زمان است، بررسی می‌کند تا ثابت کند در چند ثانیه قبل تولید شده است. اگر راضی باشد، به نمایندگی خارجی می‌گوید که پیشروی نماید.

۵. وقتی نمایندگی خارجی اعلام وصولی را از نمایندگی داخلی دریافت می کند یک وارده در جدول خود ایجاد می نماید و اطلاع می‌دهد که میزبان سیار ثبت شده است.

ایده آل ان است که وقتی کاربری ناحیه را ترک می کند، باید اطلاع دهد تا از ثبت خارج شود، اما اغلب کاربران به طور غیر منتظره، کامپیوترهای خودشان را خاموش می‌کنند.

وقتی بسته‌ای به میزبان ارسال می‌گردد به شبکه محلی داخلی کاربر هدایت می‌شود زیرا چیزی است که آدرس، انجام آن را می‌طلبد، مانند آنچه که در مرحله ۱ از شکل ۱۵ نشان داده شده است اینجا فرستند در شهر شمال غربی سیتل می‌خواهد

بسته‌ای را از طریق ایالات متحده در نیویورک به یک میزبان بفرستد. بسته‌های ارسال شده به میزبـان سـیار در LAN داخلـی خود در نیویورک، توسط نمایندگی داخلی متوقف می شود. سپس نمایندگی داخل، محل جدید (موقتی) میزبان سیار را جست و جو می‌کند و آدرس نمایندگی خارجی را می‌یابد که میزبان سیار را جست وجو می‌کند و آدرس نمایندگی خارجی را می‌یابد که میزبان سیار را اداره می‌کند.

نمایندگی داخلی دو کار را انجام می‌دهد اول اینکه بسته را د فیلد بار مفید بسته یرونـی تـر بسـته بنـدی مـی‌کـن و آن را بـه نمایندی خارجی می‌فرستد (مرحله دو در شکل ۱۵) این راهکار را تونل سازی می‌نامند؛ در ادامه آن را بیشتر مورد بحـث قـرار می‌دهیم. پس از گرفتن بسته بسته بندی شده نمایندگی خارجی بسته اصلی را از فیلد بار مفید جدا می‌کد و آن را بـه صـورت قاب پیوند داده‌ای به میزبان سیار می‌فرستد.

دوم اینکه نمایندگی داخلی به فرستنده می‌گوید از این پس بسته‌ها را با قراردادن آنها در فیلد بار مفید بسته‌هایی کـه صـریحاً به نمایندگی خارجی آدرس دهی می شوند، به میزبان سیار ارسال نماید (به جای اینکه آنهـا را بـه آدرس داخـل کـاربر سـیال ارسال کند (مرحله ۳) اکنون بسته‌های بعدی می‌توانند مستقیما از طریق نمایندگی خارجی (مرحله ۴) به میزبان هدایت شوند (با نادیده گرفتن موقعیت داخلی).

الگوهای مختلفی که عرضه شدند تفاوت هایی با هم دارند اول اینکه چه مقدار از این قرارداد توسط مسیریابها و چقـدر توسـط میزبان‌ها انجام می‌شوند و در حالت دوم توسط کدام لایه در میزبان‌ها انجام می‌گیرد دوم اینکه در الگوهـای انـدکی مسـیریابها در بین راه آدرسهای تطبیق شده را ثبت می کنند، لذا می توانند قبل از رسیدن ترافیک بـه موقعیـت داخلـی، از آن جلـوگیری کرده مجددا آن را هدایت نمایند سوم اینکه در بعضی از الگوها به هر مهمان آدرس موقت منحصر به فردی نسبت داده می‌شود در بعضی دیگر آدرس موقت به نمایندگی اشاره می‌کند ه ترافیک مربوط به تمام مهمانها را کنترل می‌نماید.

چهارم اینکه الگوها در چگونگی ترتیب بسته هایی که به یک مقصد آدرس دهی شدند و باید به مقصد دیگری تحویل شـوند بـا هم فرق می کنند یک روش تغییر آدرس مقصد و ارسال مجدد بسته اصلاح شده است. روش دیگـر ایـن اسـت کـه کـل بسـته آدرس محلی و هر چیز دیگر می توانند در فیلد بار مفید بسته دیگری که به آدرس موقتی ارسال شده است، بسته بندی گـردد. سرانجام الگوها از نظر حفاظت با یکدیگر متفاوت اند. به طور کلی وقتی میزبان یا مسیریابی پیامی به این شکل را دریافت کند: اکنون شروع کن، لطفا تمام نامه‌های کیلاس را به من بفرست، ممکن است با دو پرسش مواجـه باشـد: بـا چـه کسـی صـحبت می‌کند و آیا این ایده ایده خوبی است یا خیر.

مسیریابی در شبکه‌های موقتی

تا کنون با چگونگی مسیریابی در حالتی که میزبانها سیار و مسیریابها ثابت باشند آشنا شدید حالت دیگر این است که خود مسیریابها سیار باشند. بعضی از این موارد عبارت‌اند از:

۱. وسایل نقلیه نظامی در میدان جنگ که هیچ ساختمانی وجود ندارد

۲. ناوگان کشتی‌ها در دریا

۳. کارکنان اضطراری در هنگام وقوع زلزله که ساختمانها را خراب کرده است

۴. گردهمایی افرادی با کامپیوترهای کیفی در منطقه‌ای که فاقد ۸۰۲,۱۱ است.

در همه این موارد و موارد مشابه، هر گروه متشکل از یک مسیریاب و یک میزبان است که معمولا در یک کامپیوتر قرار دارند. شبکه هایی از گره‌ها که در نزدیک یکدیگر قرار می‌گیرند. شبکه‌های موقتی یا MANET (شبکه‌های موردی همراه) نام دارند. آنها را به طور مختصر شرح می‌دهیم.

تفاوت شبکه‌های موقتی با شبکه‌های سیمی این است که تمام قوانین مربوط به توپولوژی‌های ثابت همسایگان ثابت ومشخص رابطه ثابت بین آدرس IP و مکان، و غیره باید نادیده گرفته شوند. مسیریابها از نقطه ای به نقطه دیگر جا به جا می شوند. در شبکه سیمی اگر مسیریاب، مسیر معتبری به مقصد داشته باشند، این مسیر همواره معتبر خواهد بود (مگر اینکه سیستم خراب شود) در شبکه های موقتی توپولوژی ممکن است همواره تغییر کند. در نتیجه مطلوب بودن و اعتبار مسیرها بدون هیچ اخطاری تغییر می‌کند. بدیهی است که این شرایط موجب می‌شود مسیریابی در شبکه‌های موقتی کاملا متفاوت از شبکه‌های ثابت باشد.

الگوریتم های مسیریابی گوناگونی برای شبکه های موقتی پیشنهاد شدند. یکی از جالب ترین الگوریتمها AODV (بردار فاصله موقتی بر حسب تقاضا) نام دارد. شکلی از الگوریتم بردار فاصله بلمن- فورد است که در محیط سیار کار می کند و محدودیت پهنای باند و طول باطری را در این محیط در نظر می گیرد. ویژگی غیر عادی دیگر این است که الگوریتم تقاضا است یعنی فقط در صورتی که کسی بخواهد بسته‌ای را به مقصدی بفرستد، مسیری به آن مقصد را می‌یابد.

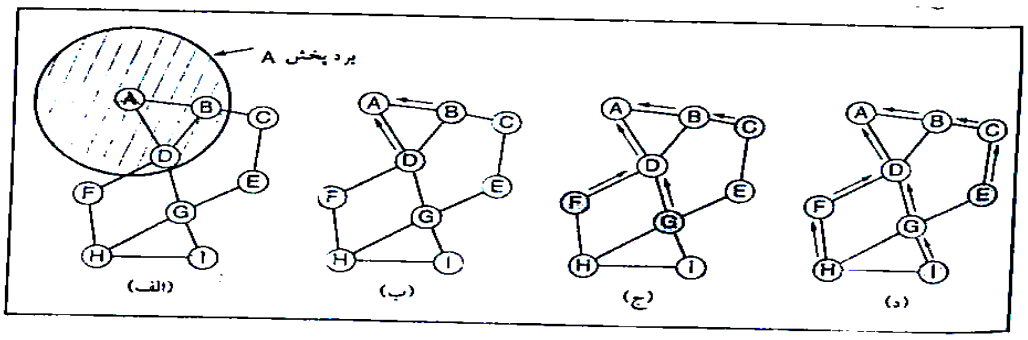
کشف مسیر

شبکه موقتی را در هر لحظه می توان به وسیله گرافی از گره ها (مسیریاب ها+ میزبانها) توصیف کرد. دو گره در صورتی متصل به هم هستند که بتوانند مستقیما با استفاده از رادیوهای خود با یکدیگر ارتباط برقرار کنند (در این صورت در گراف یالی بین آنها وجود دارد). چون ممکن است یکی از آنها خیلی قوی تر از دیگری باشد ممکن است A به B متصل باشد اما B به A

متصل نباشد. اما برای سهولت فرض می‌کنیم تمام اتصالها متقارن هستند. توجه داشته باشید که اگر دو گره در رادیوی یکدیگر باشند به معنای این نیست که به هم متصل هستند.

برای توصیف این الگوریتم شبکه موقتی شکل ۱۶ را در نظر بگیرید که در آن فرایندی در گره A می‌خواهد بسته‌ای را به گره I بفرستد. الگوریتم AODV در هر گره دارای جدولی است که کلید آن مقصد است و اطلاعاتی راجع به آن مقصد ارائه می کند از جمله کدام همسایه باید بسته را بفرستد تا به مقصد برسدو فرض کنید، A در جدول خود جست و جو می کند و وارده‌ای را برای I نمی یابد. اکنون باید مسیری را به I را کشف کند. چون این الگوریتم در صورت نیاز مسیرها را کشف می کند، الگوریتم تقاضا نام دارد.

برای یافتنI گره A بسته ROUTE REQUEST خاصی را می‌سازد و آن را پخش می‌کند. این بسته به B و D می‌رسد (شکل ۱۵- الف). علت این که D , B در گراف به A وصل هستند این است که A می‌تواند با آنها ارتباط برقرار کند. به عنوان مثال از F به A یالی وجود ندارد زیرا نمی‌تواند سیگنال رادیویی A را دریافت کند. لذا F به A وصل نیست.



(الف) برد پخش A. (ب) پس از این‌که B و D پخش A را دریافت کردند. (ج) پس از این‌که C ،F و G پخش A را دریافت کردند. گره‌های سایه‌دار گیرنده‌های جدید هستند. فلش‌ها، مسیرهای معکوس ممکن را نشان می‌دهند.

شماره جهش	شماره ترتیب مقصد	شماره ترتیب منبع	آدرس مقصد	شناسه تقاضا	آدرس منبع

فرمت بسته ROUTE REQUEST در شکل ۱۹ آمده است. این فرمت حاوی آدرسهای منبع و مقصد (معمولا آدرس IP آنها) است که مشخص می کند چه کسی برای چه کسی جست و جو می کند. شناسه تقاضا یک شمارنده محلی است و توسط هر گره ای نگهداری می شود و هر وقت ROUTE REQUEST پخش می شود یک واحد به آن اضافه می شود فیلدهای آدرس

منبع و شناسه تقاضا، یک بسته ROUTE REQUEST منحصر به فرد را مشخص می کنند کـه بـه گـره‌هـا اجـازه مـی‌دهنـد بسته‌های تکراری را حذف کنند.

هر گره علاوه بر شمارنده شناسه تقاضا شمارنده دنباله ای دارد که هر وقت ROUTE REQUEST فرستاده شد (یا پاسخی بـه ROUTE REQUEST داده شد) یک واحد به آن اضافه می شود. تقریبا مثل ساعت عمل مـی کنـد و بـرای تخشـیص مسـیر جدید از مسیر قدیم به کار می رود. فیلد چهارم در شکل ۱۹ شماره ترتیب A اسـت و فیلـد پـنجم جدیـدترین مقـدار شـماره ترتیب I است که A آن را دیده است. فیلد شمارنده جهش مشخص می کند که بسته تا کنون چنـد جهـش انجـام داد. مقـدار اولیه آن صفر است.

وقتی بسته ROUTE REQUEST به گره ای می رسد به صورت زیر پردازش می شود:

۱. جفت (شناسه تقاضا و آدرس منبع) در یک جدول سابقه محلی جست و جو می شود تا مشخص شـود آیـا ایـن درخواسـت قبلا دیده و پردازش شد یا خیر. اگر تکراری باشد، نادیده گرفته می شود و پردازش متوقف می گردد اگـر تکـراری نباشـد ایـن جفت در جدول سابقه قرار می گیرد و پردازش ادامه می یابد.

۲. گیرنده مقصد را در جدول مسیر خود جست و جو می کند اگر مسیر تـازه ای بـه مقصـد شـناخته شـود. بسـته ROUTE REPLY به منبع ارسال می شود تا به آن بگوید چگونه به مقصد برسد. معنای مسیر تازه این است که شماره ترتیب مقصد کـه در جدول مسیریابی ذخیره شده است بزرگتر یا مساوی شماره ترتیب مقصد موجود در بسته ROUTE REQUEST است. اگر کمتر باشد مسیر ذخیره شده قدیمی تر از مسیر قبلی است که منبع برای مقصد داشته است در نتیجه مرحله ۳ اجرا می شود.

۳. چون گیرنده مسیر تازه ای به مقصد نمی رساند به فیلد شـمارنده جهـش یـک واحـد اضـافه مـی کنـد و بسـته ROUTE REQUEST را پخش می کند داده ها را نیز از بسته استخراج و آن را بعنوان وارده جدید در جدول مسیر معکوس خود ذخیره می کند این اطلاعات برای ساختن مسیر معکوس به کار می روند لذا پاسخ می تواند بعدا به منبع برسـد. فلشـها در شـکل ۱۶ برای ساخت مسر معکوس به کار می روند برای وارده مربوط به مسیر معکوس جدیدی که ساخته شد، تایمری شـروع بـه کـار می کند وقتی تایمر از کار افتاد وارده حذف می شود.

D , B نمی دانند I در کجا قرار دارد، لذا هر کدام از آنها وارده ای را برای مسیر معکوس ایجاد می کنند کـه بـه A اشـاره مـی کند (مثل فلش های ۱۶) بسته را در حالی پخش می کنند که فیلد شماره جهش آن ۱ اسـت. پخـش حاصـل از B بـه D , C می رسد. C وارده ای را در جدول مسیر معکوس خود ایجاد می کند و آن را پخش می کند در حالی که D آن را بعنوان پخش تکراری رد می کند. به طور مشابه پخش حاصل از D توسط B رد می شود. پخش D توسط G , F پذیرفته و ذخیره می شـود. (شکل ۱۶ ج) پس از اینکه I , H , E پخش را دریافت کردند، ROUTE REQUEST به مقصدی می رسد کـه مـی دانـد I در

کجا قرار دارد (یعنی خود I) شکل (۱۶ د) را ببینید توجه کنید کـه گرچـه پخـش هـا در سـه مرحلـه گسسـته نشـان دادیـم. پخش‌های حاصل از گره‌های مختلف هماهنگ نیستند.

طول عمر	شمارنده جهش	شماره ترتیب مقصد	آدرس مقصد	آدرس منبع

فرمت بسته ROUTE REQUEST.

در پاسخ به تقاضای ورودی I یک بسته ROUTE REPLY را می‌سازد (شکل ۱۸) آدرس منبع، آدرس مقصد، شمارنده جهش از تقاضای ورودی کپی می‌شوند، اما شماره ترتیب مقصد از شمارنده اش به حافظه منتقل می‌شود. فیلد شمارنده جهش برابر با صفر می‌شود. فیلد طول عمر مشخص می‌کند که مسیر چه مدت معتبر است. این بسته یک بسته تک پخشی به گـره‌ای اسـت که بسته ROUTE REPLY از آن آمده است که در اینجا G است. سپس مسیر معکوس را به D طی می‌کند و به A مـی‌رسـد. در هر گره شمارنده جهش یک واحد اضافه می‌شود لذا گره می‌تواند تشخیص دهد که چقدر از مقصد I فاصله دارد.

در هر گره میانی در مسیر معکوس بسته بررسی می‌شود اگر یک یا چند شرط زیر برقرار شود آن گره به عنوان مسیری به I در جدول مسیریابی محلی ذخیره می‌شود:

۱. هیچ مسیری به I شناخته نشده باشد
۲. شماره ترتیب مربوط به I در بسته ROUTE REPLY بزرگتر از مقدار موجود در جدول مسیریابی است
۳. شماره‌های ترتیب برابرند ولی مسیر جدید کوتاه تر است

بدین ترتیب تمام گره‌های موجود در مسر معکوس مسیری به I به طور رایگان یاد می‌گیرند. گـره هـایی کـه بسـته ROUTE REPLY را گرفتند ولی در مسیر معکوس نبودند (H , F , E , C ,B در مثال ما)، با انقضای مدت تـایمر مربـوط، وارده‌هـا را از جدول مسیر معکوس حذف می‌کنند.

لذا فرایند کشف مسیر به این صورت اصلاح می‌شود. برای یافتن مقصد، فرستنده یک بسته ROUTE REPLY را می‌فرستد که طول عمر آن ۱ است. اگر در مدت زمان معقولی پاسخ دریافت نشود، بسته ROUTE REPLY دیگری ارسال می‌شود. ایـن بـار طول عمر برابر با ۲ خواهد بود. دفعات بعد طول عمر برابر با ۳ و ۴ و ۵ و غیره خواهد شد به این ترتیب جست و جـو بـه طـور محلی انجام می‌شودو به طور فزاینده فراگیرتر می‌شود.

نگهداری مسیر

چون گره‌ها می‌توانند جا به جا شوند یا خاموش شوند توپولوژی خود به خود تغییر می‌کند. بعنوان مثـال در شـکل ۱۶ اگـر G خاموش شود، A متوجه نمی‌شود که برای رسیدن به I استفاده می‌کرد. (ADGI) معتبر نیست. الگـوریتم بایـد ایـن موضـوع را اداره کند. هر گره به طور تناوبی پیام Hello می‌فرستدد. انتظار می‌رود هر یک از همسایه هایش به آن پاسخ دهند. اگـر هـیچ

پاسخی دریافت نشود، پخش کننده متوجه می شود که همسایه ها از برد آن خارج شدند و دیگر به آن متصل نیستند به طور مشابه، اگر سعی کند بسته‌ای به همسایه‌ای بفرستد که پاسخ نمی‌دهد یاد می‌گیرد که این همسایه دیگر وجود ندارد.

این اطلاعات برای از بین بردن مسیرهایی به کار می‌روند که دیگر کار نمی‌کنند. برای هر مقصد ممکن، هر گره‌ای مثل N همسایه هایی را نگهداری می کند که برای آن بسته هایی را که در اثنای آخرین ثانیه فرستادند تا به آن مقصد ارسال شوند. این همسایه‌ها را همسایه‌های فعال N برای آن مقصد می‌نامند. N برای انجام این کار از جداول مسیریابی استفاده می‌کند که کلید آن مقصد است و حاوی گره خروجی برای رسیدن به مقصد، شمارنده جهش به مقصد، جدیدترین شماره تریب مقصد و لیست همسایه های فعال آن مقصد است. نمونه ای از جدول مسیریابی برای گره D در توپولوژی مثال ما در شکل ۱۹ – الف آمده است.

وقتی یکی از همسایه‌های N غیر قابل دسترسی می‌شود، Nجدول مسیریابی خود را بررسی می‌کند تا مشخص کند کدام مقصدها مسیرهایی دارند که از همسایه ناپدید شده استفاده می کنند برای هر کدام از این مسیرها به همسایه های فعال اطلاع داده می‌شود که مسیر آن‌ها از طریق N نامعتبر است و باید از جداول مسیریابی آنها حذف شود. سپس همسایه‌های فعال به طور بازگشتی به همسایه‌های فعال خود خبر می‌دهند و غیره. این روند ادامه می یابد تا تمام مسیرهایی که به گره ناپدید شده بستگی دارند از تمام جدولهای مسیریابی حذف شوند.

بعنوان مثالی از نگهداری مسیر، مثال قبلی خود رادر نظر می‌گیریم اما فرض می‌کنیم G خاموش می‌شود. توپولوژی تغییر یافته در شکل ۱۹-ب آمده است وقتی D می‌فهمد که G ناپدید شد، به جدول مسیریابی خود نگاه می‌کند و می‌بیند که G در مسیرهایی به I , G, E استفاده شده است. اجتماع همسایه‌های فعال مربوط به این مقصدها مجموعه {A,B} است. به عبارت دیگر، A و B در بعضی از مسیرهای خود به G وابسته اند ولذا باید به آنها اطلاع داده شود که این مسیرها دیگر معتبر نیستند. D با ارسال بسته هایی این خبر را به آنها می‌دهد که باعث می‌شود آنها جدول‌های مسیریابی خودشان را نوسازی کنند. علاوه بر این، D وارده‌های مربوط به E، G و I را از جدول مسیریابی خود حذف می‌کند.

تفاوت عمده بین الگوریتم AODV و بِلْمَن- فورد این است که در AODV گره ها به طور تناوبی پخش هایی را که حاوی جدول‌های مسیریابی آنها باشد، انجام نمی‌دهند. این تفاوت منجر به صرفه جویی در پهنای باند و مصرف باطری می‌شود.

ADOV قادر است مسیریابی پخشی و چندپخشی را انجام دهد. مسیریابی در شبکه‌های موردی، موضوع پژوهش است.

جست و جوی گره در شبکه‌های نظیر به نظیر

یک پدیده نسبتاً جدید، شبکه نظیر به نظیر است که در آن تعداد زیادی از افراد منابع مشترکی استفاده می‌کنند. معمولاً این افراد اتصال دائمی سیمی با اینترنت دارند. اولین کاربرد گسترده فناوری نظیر به نظیر جرم گروهی بود: ۵۰ میلیون کاربر

Napster آوازهایی با حق کپی رایت را بودن مجوز مالکین کپی رایت مبادله کردند و دادگاه با وجود اختلاف نظرهای زیاد، Napster را متوقف کرد. با این وجود، فناوری نظیر به نظیر، کاربردهای جالب و قانونی دارد. مشکلاتی مثل مسیریابی دارد، ولی این مشکلات با آن چه که تاکنون مطالعه کردیم متفاوت هستند. با این وجود، مروری سریع به آن‌ها خواهیم داشت.

جالب بودن سیستم‌های نظیر به نظیر به این دلیل است که کاملاً توزیعی اند. تمام گره‌ها متقارن‌اند و کنترل مرکزی یا سلسله مراتبی وجود ندارد. در سیستم نظیر به نظیر، هر کاربر اطلاعاتی داردکه ممکن است برای کاربران دیگر مفید باشد. این اطلاعات ممکن است برای کاربران دیگر مفید باشد. این اطلاعات ممکن است نرم افزار رایگان، موسیقی، عکس و غیره باشد. اگر تعداد کاربران زیاد باشد، یکدیگر را نمی شناسند و نمی دانند اطلاعات مورد نیازشان را از کجا تهیه کنند. یک راه حل استفاده از بانک اطلاعاتی مرکزی است، اما به دلایلی ممکن نیست (مثلاً هیچ کس علاقه مند به میزبان و نگهداری آن نباشد). لذا، مسئله این است که وقتی بانک اطلاعاتی یا ایندکس مرکزی وجود ندارد، کاربر چگونه گره ای را پیدا کند که حاوی اطلاعات مورد نظرش باشد.

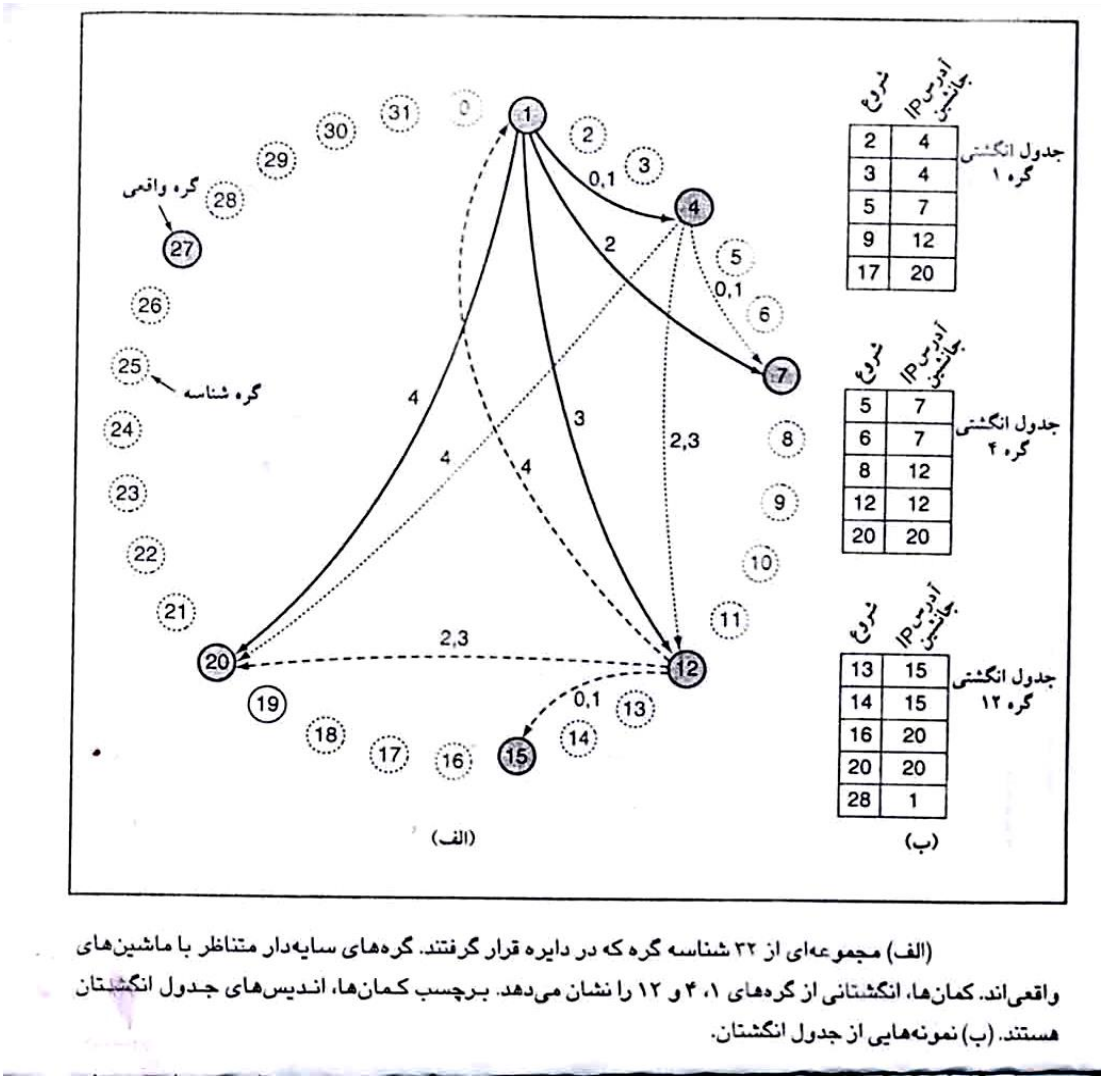
فرض می کنیم هر کاربر یک یا چند قلم داده مثل آواز، عکس، برنامه، فایل و غیره دارد و کاربران دیگر می‌خواهند از آن‌ها استفاده کنند. هر قلم دارای نام اسکی است. کاربر فقط رشته اسکی را می‌شناسد و می‌خواهد بداند آیا کسانی آن‌ها را کپی کردند یا خیر. چنانچه کپی کرده باشند، آدرس IP آنها را بداند.

به عنوان مثال، یک بانک اطلاعاتی توزیعی تبارشناسی را در نظر بگیرید. هر تبارشناس چند رکورد on-line برای اجداد و خویشاوندان دارد که ممکن است شامل عکس، صوت یا برش های ویدیوی فرد باشد. چند نفر ممکن است یک جّد پدری داشته باشند، لذا رکوردهای مربوط به یک جد ممکن است در چندین گره وجود داشته باشد. نام رکورد، نام فرد به شکل کانونی است. در نقطه‌ای از این بانک اطلاعاتی، تبارشناس می‌بیند که جد پدری او در آرشیو قرار دارد و جد پدری تو ساعت جیبی طلایی خود را برای نوه اش به ارث گذاشت. اکنون تبارشناس نام نوه را می‌داند و می‌خواهد بداند که آیا تبارشناس دیگری رکوردی برای آن دارد یا خیر. بدون وجود بانک اطلاعاتی متمرکز چگونه می‌توان این موضوع را تشخیص داد؟

الگوریتم های متعددی برای حل این مسئله ارائه شدند. الگوریتم کورد (دابک و همکاران، ۲۰۰۱) را بررسی می کنیم. سیستم کورد از چندین کاربر تشکیل شده است که هرکدام دارای چندین رکورد ذخیره شده هستند و آمادگی دارند که قطعاتی از ایندکس را برای استفاده دیگران ذخیره کنند. هر گره کاربر، دارای یک آدرس IP است که می تواند با استفاده از تابع درهم سازی، hash به یک عدد m بیتی درهم سازی شود. کورد از SHA-۱ برای تابع hash استفاده کرد. SHA-۱ در رمز نگاری استفاده می‌شود که در فصل ۸ بحث می‌شود. در حال حاضر می‌گوییم تابعی است که یک رشته بیتی طول متغیر را به عنوان آرگومان می گیرد و یک عدد تصادفی ۱۶۰ بیتی را تولید می کند. لذا می توانیم هر آدرس IP را به عدد ۱۶۰ بیتی تبدیل کنیم که نامش شناسه گره است.

از نظر مفهومی، کل ۲ شناسه گره به ترتیب صعودی در یک دایره بزرگ چیده شدند. بعضی از آن‌ها متناظر با گره‌های کاربران هستند، ولی اغلب آن‌ها این طور نیستند. در شکل ۲۴-۵ (الف) دایره شناسه گره را برای ؟؟؟ دادیم (فعلاً کمان‌های وسط را حذف کردیم). در این مثال،گره هایی با شناسه ۱،۴،۷،۱۲،۱۵،۲۰، ۲۷

متناظر با گره‌های واقعی‌اند و سایه دار شده اند. بقیه وجود ندارند.



(الف) مجموعه‌ای از ۳۲ شناسه گره که در دایره قرار گرفتند. گره‌های سایه‌دار متناظر با ماشین‌های واقعی‌اند. کمان‌ها، انگشتانی از گره‌های ۱، ۴ و ۱۲ را نشان می‌دهد. برچسب کمان‌ها، اندیس‌های جدول انگشتان هستند. (ب) نمونه‌هایی از جدول انگشتان.

تابع k) successor) را به عنوان شناسه اولین گره واقعی بعد از k در جهت عقربه ساعت در دایره تعریف می‌کنیم. به عنوان مثال،)successor۶=(۷ ،)successor۸=(۱۲ و)successor۲۲=(۲۷ است.

اسامی رکوردها (اسامی آواز، اسامی اجداد و غیره) توسط تابع hash درهم سازی شدند تا یک عدد ۱۶۰ بیتی به نام کلید تولید شود. لذا برای تبدیل name (نام اسکی رکورد) به کلید، از عبارت key=hash(name) استفاده می‌کنیم. اگر شخصی، رکورد تبارشناسی برای name داشته باشد و بخواهد آن را برای دیگران مهیا کند، ابتدا یک دوتایی متشکل از (آدرس IP وname) می‌سازد و سپس از successor(hash(name)) می خواهد این دوتایی را ذخیره کند. اگر برای این نام، چندین رکورد (در گره‌های مختلف) وجود داشته باشند، دوتایی آن‌ها در گره یکسانی ذخیره می‌شود. به این ترتیب، ایندکس به طور

تصادفی در گره‌ها توزیع می‌شود. برای تحمل عیب می‌توان از p تابع درهم سازی مختلف استفاده کرد تا هر دوتـایی را کـه در p گره ذخیره کند. اما این موضوع را در این جا بررسی نمی‌کنیم.

اگر بعداً کاربری بخواهد name را جست و جو کند، آن را درهم سازی می‌کند تا کلید را به دست آورد و سپس با اسـتفاده از successor(key) آدرس IP گره‌ای را می‌یابد که دوتایی‌های ایندکس آن را ذخیره کرده است. مرحله اول سـاده اسـت ولـی مرحله دوم ساده نیست. برای این که بتوان آدرس IP گره متناظر با کلید خاصی را پیدا کرد، هر گره باید ساختمان داده هـایی را به منظور سرپرستی ذخیره کند. یکی از این ها آدرس IP گره جانشین آن در دایره شناسه گـره اسـت. بـه عنـوان مثـال، در شکل ۲۴-۵، گره جانشین ۴، و گره ۱۲ گره جانشین ۷ است.

اکنون جست وجو میتواند به این صورت ادامه یابد. گره متقاضـی، بسـته‌ای را بـه گـره جانشـینی کـه حـاوی آدرس IP اسـت می‌فرستد. علاوه بر این، کلید مورد جست و جو را نیز به آن ارسال می‌کند. اکنون بسته در حلقه پخش می‌شود تا جانشینی را پیدا کند که شناسه گره به دنبال آن است. آن گره بررسی می کند که آیا اطلاعاتی دارد که با کلید تطبیق کنـد یـا خیـر. اگـر داشته باشد مستقیماً آن را به گره متقاضی می‌فرستد که آدرس آن را دارد.

به عنوان اولین بهینه سازی، هر گره می‌توانست آدرس‌های IP گره‌های جانشین و پیشین را نگهداری کند و در نتیجه تقاضاها هم در جهت عقربه‌های ساعت و هم در جهت خلاف عقربه‌های ساعت (بسته به این که کـدام مسـیر کوتـاه تـر اسـت) ارسـال شوند. به عنوان مثال، گره ۷ در شکل ۲۴-۵ می‌توانست برای یافتن شناسه گره ۱۰ در جهت عقربه‌های سـاعت و بـرای یـافتن شناسه گره ۳ در خلاف جهت عقربه‌های ساعت حرکت کند.

حتی حرکت در دو جهت نیز با جست و جوی خطی در سیستم نظیر به نظیر کارآمد نیست، زیرا میانگین گره های مـورد نیـاز در هر جست و جو، است. برای افزایش سرعت جست و جو، هر گروه جدولی به نام جـدول انگشـت دارد. جـدول انگشـت m وارده دارد که اندیس آن از ۰ تا m-۱ است و هر کدام به یک گره واقعی اشاره می کنند. هر وارده دارای دو فیلد است: start و آدرس IP مربوط به successor(start) . این جدول‌ها در شکل ۲۴-۵ (ب) آمده اند. مقادیر فیلدهای مربـوط بـه وارده i در گره k به صورت زیر محاسبه می‌شود،

(به پیمانه start=k+)

آدرس IP مربوط به successor(start[i])

توجه کنید که هر گره، آدرس‌های IP تعداد نسبتاً کمی از گره‌ها را ذخیره می‌کند و اغلب این‌ها نیز از نظر شناسه گره بـه هـم نزدیک هستند.

با استفاده از جدول انگشت، جست و جوی key در گره k به این صورت انجام مـی شـود. اگـر key بـین k و successor(k) باشد، آنگاه گره successor(k) حاوی اطاعاتی راجع به key خواهد بود و جست و جو خاتمه می یابد. وگرنه، جـدول انگشـت

جست و جو می‌شود تا وارده‌ای را پیدا کند که فیلد start آن نزدیک ترین جانشین key است. سپس تقاضا مستقیماً به آدرس IP در آن وارده جدول انگشت ارسال می شود تا از آن بخواهد که جست و جو را ادامه دهد. چون نزدیک تر به key ولی کمتر از آن است، مزیتش این است که قادر پاسخی را با تعداد اندکی از تقاضاهای دیگر ارائه کند. در واقع، چون هر جست و جو، فاصله تا مقصد را نصف می‌کند، می‌توان نشان داد میانگین جست و جو است.

به عنوان اولین مثال، جست و جوی =key۳ را در گره ۱ در نظر می‌گیریم. چ.ن گره ۱ می‌داند گره ۳ بین آن و جانشین آن یعنی ۴ قرار دارد، گره مطلوب ۴ است و جست وجو خاتمه می یابد و آدرس IP گره ۴ برگردانده می شود. به عنوان دومین مثال، جست و جوی =key۱۴ را در گره ۱ در نظر می گیریم. چون ۱۴ بین ۱ و۴ نیست، از جدول انگشت استفاده می شود. نزدیک ترین گره پیشین ۱۴، گره ۹ است. لذا تقاضا به سمت آدرس IP وارده ۹، یعنی گره ۱۲ پیش می‌رود. گره ۱۲ می‌بیند که ۱۴ بین آن جانشین آن، یعنی ۱۵ قرار دارد و در نتیجه آدرس IP گره ۱۵ برگردانده می‌شود.

به عنوان سومین مثال، جست وجوی =key۱۶ را در گره ۱ در نظر بگیرید. تقاضا به گره ۱۲ ارسال میشود. ولی گره ۱۲ پاسخ را نمی‌داند. نزدیک ترین گره قبل از ۱۶ جست و جو می‌کند و ۱۴ را می‌یابد که آدرس IP گره ۱۵ را ارائه می‌کند. سپس تقاضا به این جا ارسال می‌شود. گره ۱۵ می‌بیند که ۱۶ بین آن و جانشین یعنی ۲۰ قرار دارد و در نتیجه آدرس IP گره ۲۰ را برمی گرداند و در مسیرش به گره ۱ برمی گردد.

چون گره‌ها در هر زمان اضافه و کم می‌شوند الگوریتم کورد می‌باست این عملیات را اداره کند. فرض می‌کنیم وقتی سیستم شروع به کارکرد به اندازه کافی کوچک بود و گره‌ها می‌توانستد مستقیما اطلاعات را مبادله کنند و اولین دایره و جدولهای انگشت را بسازند. از این پس نیاز به روبه خودکار است وقتی گره جدیدی مثل r می خواهد اضافه شود، باید با یک گره موجود تماس بگیرد و از او بخواهد آدرس IP مربوط به successor(r) را برایش جست و جو کند. سپس گره جدید از successor(r) می خواهد گره پیشین آن را بیابد. سپس گره جدید از هر دو می خواهد r را بین آنها در دایره اضافه کند. بعنوان مثال اگر گره ۲۴ در شکل ۲۰ بخواهد اضافه شود از هر گره‌ای می‌خواهد (successor۲۴) را بیابد که گره ۲۷ است. پس از گره ۲۷ گره پیشین آن را می پرسد که ۲۰ است. سپس حضورش را به هر دو اعلان می‌کند. ۲۰ از ۲۴ به عنوان جانشین خود و ۲۷ از ۲۴ به عنوان پیشین خود استفاده می کند. علاوه بر این گره ۲۷ این کلیدها را در بازه ۲۴-۲۱ تحویل می‌دهد که اکنون متعلق به ۲۴ هستند. اکنون ۲۴ اضافه شده است.

اکنون بسیاری از جدول های انگشتی نادرست‌اند. برای اصلاح آنها، هر گره یک فرایند پس زمینه را اجرا می کند که با فراخوانی تابع successor، هر انگشت را دوباره حساب می کند وقتی یکی از این تقاضاها به گره جدیدی می رسد وارده انگشت متناظر آن نوسازی می‌شود.

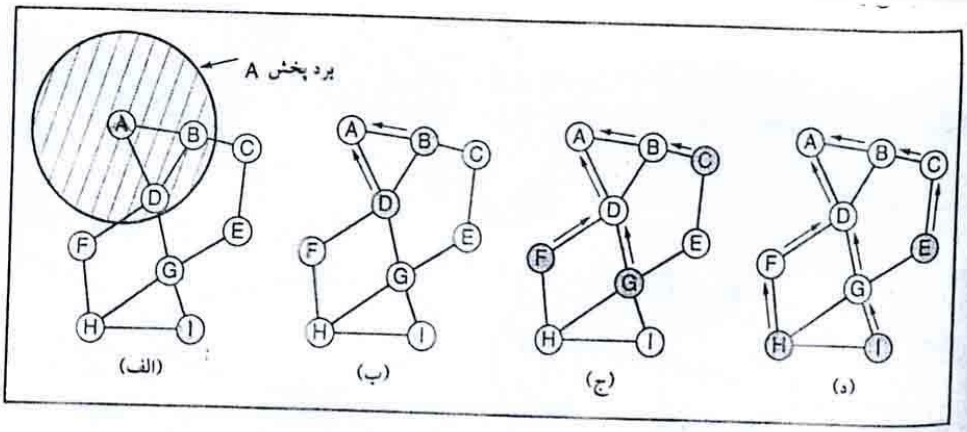
اگر گره‌ای به خوبی دایره را ترک کند، کلیدهایش را به جانشین خود تحویل می‌دهد و خروج خود را به گره پیشین خود خبر می‌دهدو گره پیشین می‌تواد به گره جانشین گره خارج شده وصل شود. وقتی گره‌ای خراب می‌شود مشکل پیش می‌آید. زیرا، گره پیشین آن دیگر جانشین معتبری ندارد. برای حل این مسئله هر گره نه تنها جانشین مستقیم خود را نگه می‌دارد، بلکه تعداد s جانشین معتبری ندارد. برای حل اینکه مسئله هر گره نه تنها جانشین مستقیم خود را نگه می دارد، بلکه تعداد s جانشین مستقیم خود را نگه می دارد تا در صورتی که -s۱ گره متوالی با شکست مواجه شود، بتواند به گره جانشین مناسبی وصل شود.

کورد خواست سیستم فایل توزیعی و سایر کاربردها را ایجاد کند و تحقیق در این زمینه ادامه دارد.

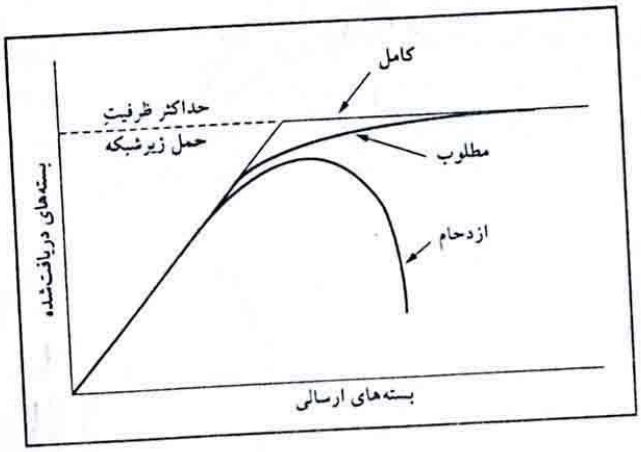
الگوریتم کنترل ازدحام

وقتی بسته های بسیار زیادی (در قسمتی از) زیر شبکه وجود داشته باشد کارایی کاهش می یابد این وضعیت ازدحام نام دارد. شکل ۲۱ این حالت را نشان می‌دهد. وقتی تعداد بسته هایی که توسط میزبانها به زیر شبکه ارسال می‌شوند، به اندازه ظرفیت حمل آن باشد، تمام آن (به جز آن‌هایی که تحت تاثیر خطای انتقال قرار می‌گیرند) به مقصدهایشان تحویل داده می‌شوند و تعداد بسته‌های تحویل شده متناسب با تعداد ارسالی است با افزایش بی رویه ترافیک، مسیریابها نمی‌توانند از عهده آن برآیند، و بسته هایی از بین می‌روند و بر مشکل افزوده می‌شود. در ترافیک زیاد، کارایی بسیار پایین می‌آید، و تقریبا هیچ بسته‌ای تحویل داده نمی‌شود.

ازدحام به دلایل زیادی به وجود می آید. اگر ناگهان چند بسته از سه یا چهار خط ورودی بیایند و همگی بخواهند به یک خط خروجی بروند، صفی تشکیل خواهد شد



(الف) برد پخش A. (ب) پس از این‌که B و D پخش A را دریافت کردند. (ج) پس از این‌که F، C و G پخش A را دریافت کردند. گره‌های سایه‌دار گیرنده‌های جدید هستند. فلش‌ها، مسیرهای معکوس ممکن را نشان می‌دهند.



در ترافیک زیاد، ازدحام زیاد می‌شود و کارایی پایین می‌آید.

ازدحام به دلایل زیادی به وجود می‌آید. اگر ناگهان، چند بسته از سه یا چهار خط ورودی بیایند و همگی بخواهند به یک خط خروجی بروند، صفی تشکیل خواهد شد. اگر حافظهٔ کافی برای ذخیره و آنها

کانفیگ کردن و مدیریت پروتکل های مسیر یابی :

وقتی یک استراتژی مسیر یابی برنامه ریزی می کنید تفاوت بین اتصالات LAN و WAN مهم است. اغلب LAN ها چندین Subnet دارند.Host های هر سابنت می خواهند با Host های کاربران دیگر که روی سابنت های دیگری هستند تبادل

اطلاعات کنند. برای اینکه اجازه دهید کاربران در سابنت های متفاوت با هم در ارتباط باشند ، شما نیـاز بـه نـوعی تکنولـوژی مسیر یابی دارید.

RRAS سه فیلد کلیدی دارد :

- DHCP Relay Agent
- RIP V۲
- OSPF

توپولوژی های مسیر یابی :

- Star
- Mesh
- Ring

مسیریابی پویا : روترها از پروتکل های مسیریابی داینامیک (RIP,IGRP,OSPF) برای به روز کردن جـول خـود اسـتفاده مـی کنند.

مسیر یابی Distance Vector :

مانند RIP اطلاعات مسیرها بین روترهایی که از این مورد استفاده می کنند رد و بدل می شود. در DV به این صورت است که منظور از Distance این است که پکت ها برای انتقال از یک روتر به روتر دیگر باید یک مسافت را طی کننـد. ماننـد حرکـت آن ها بعد از دو HOP (مسیری است که داده درآن توسط روتر انتقال می یابد) که جهت آن ها هم مشخص می شود.

مزایای DV این است که خیلی راحت کانفیگ شده و کار می کند.

معایب آن :

- جدول های مسیر یابی آن ها بسیار بزرگ می شود.
- در شبکه های بزرگ ترافیک بالا می رود.
- به علت بزرگ بودن جدول ها خاصیت گسترش پذیری را از دست می دهند.
- غیر همزمان و غیر تصدیق اند.
- می تواند باعث ایجاد حلقه شود که در نتیجه پکت سرگردان می شود.

مسیریابی Link State :

مثل OSPF که شرایط مسیر را نیز در نظر می گیرد. LS اطلاعات شرایط مسیر را به طور مستقیم یا مالتی کست ارسال می کند نه به صورت Broadcast که باعث ترافیک زیاد شود.

روترهای LS از یک DB برای ذخیره اطلاعات استفاده می کنند و LS برخلاف DV همزمان است و تصدیق دارد.

مزایای LS :

- جدول مسیریابی کوچک و جستجوی بهتر دارد.
- قابل گسترش است.
- حلقه و سرگردانی پکت ندارد.

معایب :

- پیچیده اند و باید به خوبی درک شوند.
- کانفیگ کردن آن ها مشکل است.
- ممکن است حجم DB آن ها زیاد شده و پردازش آن ها مشکل شود. به DB آن ها LSA(Link State Advertisement) گویند.

RIP ها در شبکه های بزرگ هر ۳۰ ثانیه یک آگهی ارسال می کنند که سبب اقزایش ترافیک می شود.

RIP : یک DV که متریک آن HOP های بین فرستنده و گیرنده است که تعداد HOP های RIP نباید بیشتر از ۱۵ تا شود.

مثلا مسیر HOP۱ با HOP۳ میتواند متفاوت باشد ولی RIP قادر به تشخیص این سرعت ها نیست.

پس RIP نمی تواند کیفیت و شرایط یک مسیر را بدهد. بنابراین در شبکه های کوچک استفاده می شود. کانفیگ RIP راحت است. دو نوع RIP ورژن ۱ و ۲ داریم.

V۱ : از پکت های IP Broadcast برای اطلاع رسانی استفاده می کند. Broadcast ترافیک ایجاد می کند.

V۲ : از پکت های IP Broadcast یا Multicast برای اطلاع رسانی استفاده می کند.

Triggered Update (راه اندازی) :

وقتی رخ می دهد که توپولوژی شبکه تغییر کند و جدول های اطلاعاتی مسیرها آپدیت شوند. روترهای RIP می توانند از طریق یک TU هم تبادل اطلاعاتی داشته باشند. مثلا یک شبکه با ۱۰۰۰ کلاینت داریم و ۱۰ تا RIP V۲ داریم. زمانی که یک روتر از کار بیافتد روتر ۱ به روتر ۵ آگهی داده و جول مسیریابی خود را آپدیت می کند که مسیری جدید انتخاب کند.

در سرور ۲۰۰۳ می توان هر دو ورژن RIP را کانفیگ کرد. همچنین الگوریتم های TU را اعمال کرد. می توان مسیرها را فیلتر کرد. بهتر است RIP ها حداکثر ۱۴ تا باشند.

مثلا دو تا سایت داریم و دو اتصال بین آن ها وجود دارد. یکی T۱ با سرعت بالا و cost=۱ (پیش فرض) و دیگری ماهواره ای و کم سرعت و cost=۲ (پیش فرض) بهترین مسیر برای استفاده همیشه T۱ است ولی اگر از کار بیافتد در این صورت از لینک ماهواره ای استفاده می شود. پس cost اولویت است و بهتر است از ورژن ۲ استفاده کرد. البته در صورتی که روترها از ورژن ۲ پشتیبانی کنند. اکثر آن ها از ورژن ۲ پشتیبانی می کنند و همینطور میتوان ترکیبی از هر دو ورژن را استفاده کرد.

محدودیت های V۱ :

- از VLSM,CIDR نمیتوان استفاده کرد.
- اگر می خواهید از ترکیب ۱ و ۲ استفاده کنید باید اینترفیس ها را به درستی کانفیگ کرده باشید.

Authentication V۲ :

می توان با یک Password برای امنیت بیشتر بین روترها تشخیص هویت اعمال کرد. که باید این کلمه عبور بر روی تمامی اینترفیس های ورژن ۲ اعمال شود. به حروف نیز حساس است.

RIP برای IPsec :

برای بالا بردن امنیت RIP می توان از RIP V۲ Authentication و Peer Security و Route Filters و Neighbors استفاده کنید.

Authentication V۲ بوسیله کلمه عبور از ورود روترهای هکر به شبکه جلوگیری کرده که این کلمه عبور یک متن واضح (Plaintext) است و مشکل اینجا است که با اسنیف کردن شبکه (که جریان انتقال پکت ها را کنترل می کند مانند Network Monitor Microsoft) می توان اطلاعات را پیدا کرد. این Authentication V۲ در تب جنرال ، اینترفیس اعمال می شود.

Peer Security : به صورت پیش فرض RIP تمامی آگهی ها که از هر منبعی ارسال شده را قبول می کند. حال میتوان لیست روترهایی که می توان قبول کرد را تعیین کرد که به این لیست Peer گویند که در تب Security اعمال شده است.

Route Filters : در تب Security می توان مسیرها را برای دسترسی به سایت های مختلف فیلتر کرد.

Neighbors : در تب Neighbors برای جلوگیری از ترافیک RIP ، می تـوان آگهـی هـا (Announcement) هـا را بـه صورت Unicast ارسال کرد.

راه اندازی RIP :

۱- یک نقشه از توپولوژی و IP های شبکه را که شامل بخش ها و میزبان ها است را بکشید.

۲- برای اینکه پکت بتواند به IP شبکه برسد به هر نود یک IP منحصر به فرد بدهید.

۳- IP آدرس را به هر کدام از اینترفیس روترها اختصاص بدهید.

۴- برای هر اینترفیس روتر ورژن RIP را تعیین کنید. در ورژن ۲ پکت ها به صورت مالتی کست یا بـراد کسـت ارسـال می شود.

تست شبکه RIP :

۱. توسط راست کلیک بر روی RIP و انتخاب Show Neighbors چک می کنیم که پکت های RIP به همسایه ها ارسال شده است یا نه.

۲. از طریق راست کلیک بر روی Static Roters و انتخاب Show IP Routing Table جدول های روترهـای RIP را چک می کنیم.

۳. می توان از دستورات ping و tracert استفاده کرد.

کانفیگ یک RIP برای IP Router :

۱- کانفیگ RRAS به عنوان یک روتر که حداقل باید این سیستم دو تا کارت شبکه داشته باشد به منظور subnet۱ و subnet۲.

۲- نصب پروتکل RIP که یکسری گزینه به ما می دهد .

۳- ایجاد اینترفیس های RIP که یکسری مشخصات دارد.

کانفیگ RIP۲ :

۱- کنسول RRAS و راست کلیک روی general و انتخاب new routing protocol و انتخاب RIP۲.

۲- کنسول RRAS و راست کلیک روی پروتکل RIP و انتخاب properties که دو تب general , security دارد.

ایجاد اینترفیس های RIP :

در کنسول RRAS روی روترمان IP routing را انتخاب و بر روی RIP راست کلیک مـی کنـیم و new interface را زده سپس می توان این واسط جدید را کانفیگ کرد که دارای چهار تب است :

General , Security , Neighbors , Advanced

در تب جنرال و فیلد آپشن مد دو حالت داریم :

۱. Autostatic : پیش فرض است برای اتصالات demand dial که RIP۲ آپدیت هایش را فقط وقتـی ارسـال مـی کند که روتر مقصد آن ها را تقاضا کند.

۲. Periodic: برای اتصالات LAN به صورت پیش فرض است و RIP۲ آپدایت هایش را هر ۳۰ ثانیه به همسـایه هـای فعـالش مـی فرسـتد. در تـب جنـرال در قسـمت outgoing packet protocol مـی تـوان نـوع پروتکـل (RIP۱,RIP۲,silent RIP) را انتخاب کرد که با انتخاب آن این RIP روتر آپدیت ها را از دیگر روترها قبول می کند ولی آپدیت خودش را به روترهای دیگر نمی دهد. در این تب اولویت ها (cost) ها مشخص می شـود. مـی تـوان بـر روی تبلیغات (Announce) برچسب و پسورد قرار داد.

در تب **امنیت** می توان مسیرها را مشخص و فیلتر کرد و لیست روترها را تعیین نمود.

در تب **همسایه ها** می توان فعالیت روتر با روترهای همسایه اش را تعیین کرد که سه گزینه دارد.

در تب **Advance** معمولا با گزینه های پیش فرض آن کار می شود.

برای کانفیگ RIP می توان از دستورات netsh نیز استفاده کرد.

OSPF :

شرایط مسیر را نیز بررسی می کند. مثلا تعداد HOP ها ، سرعت انتقال اتصالات مورد نظر ، تأخیرهایی که به خـاطر ترافیـک شبکه ایجاد شده ، با cost هایی که مدیر شبکه اعمال می کند. مثلا دو تا شبکه داریم که با دو اتصال (یکی T۱ کـه ارزان تـر است چون ماهانه پرداخت شده و دیگری ISDN که گران است و هر دقیقه شارژ می شود.) حال مدیر شبکه می خواهد اتصال پیش فرض T۱ باشد. OSPF به صورت داینامیک مسیرها را انتخاب می کند. حتی اگر ISDN سرعتش بالاتر و ترافیک هـم داشته باشد باز هم از OSPF T۱ می رود که ترافیک کمتری داشته باشد.

در OSPF هیچگاه Loop نداریم و وقتی شبکه گسترش یافت OSPF به راحتی قابل گسترش است. حتی با تغییر توپولوژی و پروتکل ها دوباره می توان به راحتی OSPF را کانفیگ کرد.

OSPF در سرور ۲۰۰۳ :

فیلتر کردن مسیرها ، به صورت داینامیک تمام تنظیمات OSPF را کانفیگ می کند. .....

پایگاه داده Link State :

روترهای OSPF نقشه شبکه را بعد از تغییراتی که در توپولوژی شبکه اتفاق می افتد را نگه می دارند.

برای تمامی روترها OSPF این نقشه یکنواخت می شود و جدول های مسیریابی روترها از آن بهره می برند.

همجواری (Adjacency) :

روترهای نزدیک به هم ، پایگاه داده هایشان را با هم یکنواخت می کنند. وقتی تغییرات این پایگاه داده ها دریافت شد ، این جدول های مسیریابی دوباره آپدیت می شوند.

از نظر حافظه و لود کردن پروسسور ، OSPF سنگین است و اندازه پایگاه داده آن به مرور بزرگ می شود.

هر کدام از این Areaها خودشان یکسری روتر داخلی دارند. حال از طریق روتر OSPF به Area دیگری متصل می شوند.

اصطلاحات OSPF :

Routing Area : مثل یک سایت یا شبکه تصورش کنید که درای اتصالات پرسرعت است. هر Area یک ID منحصر به فرد دارد و هر Area با یک محدوده ای از IP ها است.

Backbone Area(Area ۰) : وقتی OSPF نصب می شود به صورت اتوماتیک بوجود می آید که مرکز اصلی مسیر یابی OSPF است و تمامی Area ها به صورت معمول به آن متصلند. ID آن همیشه یا ۰,۰,۰,۰ یا ۰ Area است.

Internal Routing : مختص به مسیردهی است که داخل یک Area رخ می دهد.

Internal Router : مسیردهی داخلی را انجام داده و تمام اینترفیس های روتر داخلی به شبکه ای که در آن قرار دارد متصلند.(شبکه داخلی)

ABR(Area Border Router) : پکت ها را بین Area ها منتقل می کند. اینتر فیس های آن ها می توانند به Backbone Area نیز متصل شوند.

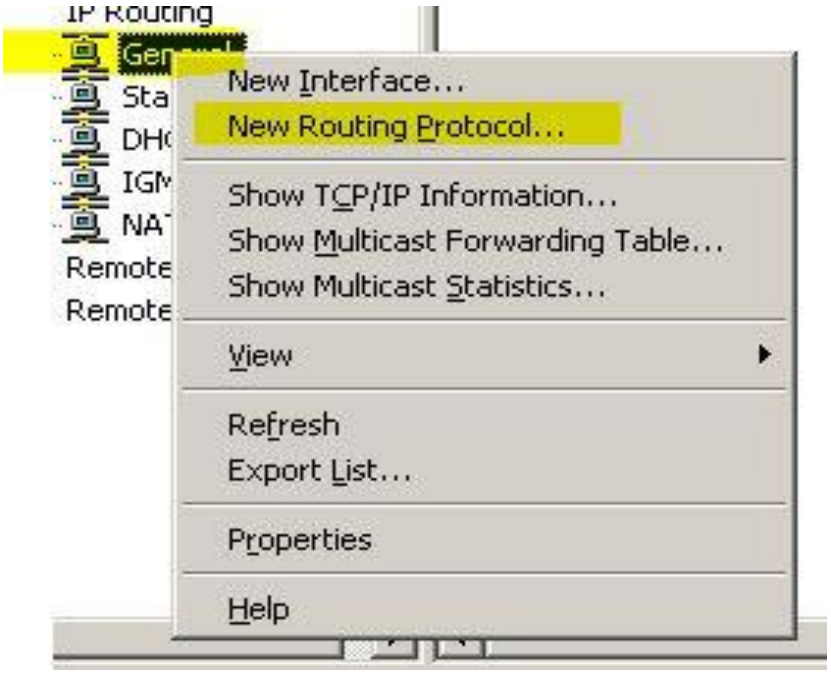
AS(Auotonomous System) : تمامی Routing Area ها را در بر می گیرد که تحت کنترل یک شرکت AS است.

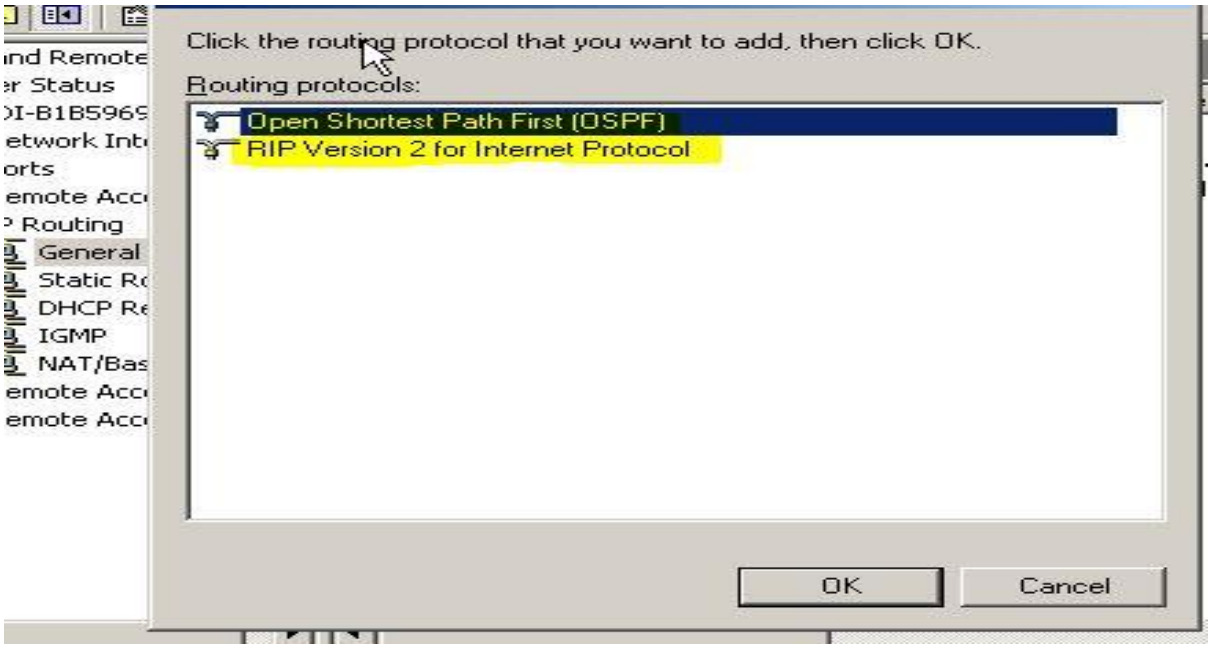
AS Boundary Router : بین یک AS با AS دیگر ارتباط برقرار می کند. مثل اینترنت که به آن ASBR گوییم.

کانفیگ کردن Packet Filters :

با آن می توان ترافیک IP (بسته ها) را در روتر کنترل کرد. روی هر اینترفیس روتر می توان آن را اعمال کرد. مثلا تعیین مـی کنیم که از یک مسیر برود به غیر از یکی و بلعکـس یـا بسـته بخصوصـی را فیلتـر کنـد. مـی تـوان ترافیـک اینتـرفیس هـای Inbound(ورودی) و Outbound(خروجی) را کنترل کرد.

کانفیگ کردن Rip و ospf



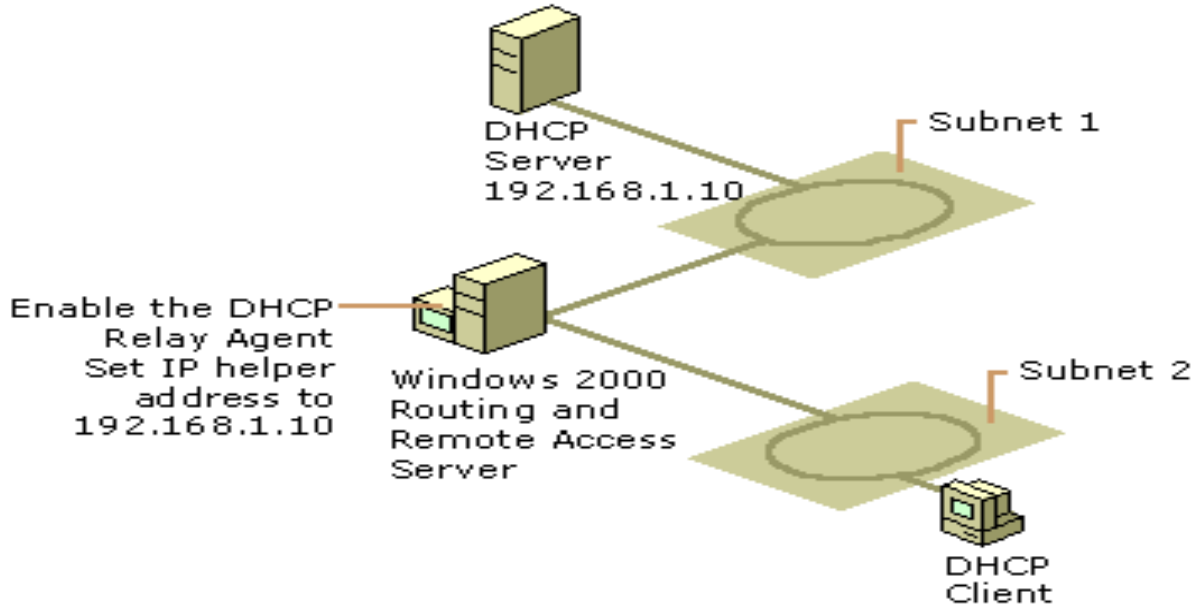


کانفیگ کردن DHCP Relay :

برنامه ای کوچک است که پیام های مختص به DHCP/BOOTP را بین سرورها و کلاینت های DHCP در Subnet های متفاوت رله (باز پخش) می کند. برای اینکه یک روتر بتواند Relay کند باید استاندارد RFC ۱۵۴۲ را ساپورت کند. DHCP Relay Agent روی روترها اعمال می شود. مثلا یک شبکه ای با چندین Subnet(سگمنت) داریم.

مثلا در یک سگمنت ، سرور DHCP و کلاینت DHCP داریم و رد سگمنت دیگر فقط کلاینت های DHCP داریم.

حال روتر در سگمنت ۲ مثل یک DHCP سرور عمل کرده و اطلاعات کلاینت های B , C را به سرورDHCP ارسال می کند. در سرور DHCP ، Scope ها تعیین می شود و IP اول تا آخر در آن ها مشخص می شود. مثلا از ۵,۵,۵,۵ شروع و در ۵,۵,۵,۱۰۰ خاتمه می یابد که تقریبا ۹۵ تا کامپیوتر را در بر می گیرد و میتوان به آن ها IP در این محدوده اختصاص داد. بر روی DHCP باید New Scope انجام داد.



BOOTP(پروتکل خود راه انداز) :

مبتنی بر UDP/IP که اجازه می دهد تا میزبان بوت شدن خودش را به صورت پویا و بدون نظارت کاربر ، پیکر بندی کند. BOOTP وسیله برای اطلاع میزبان از آدرس IP اختصاصی خودش ، IP آدرس میزبان سرور بوت ارائه می دهد و نام فایل را در حافظه بارگذاری و اجرا می کند. کلاینت با این پروتکل از DHCP ، IP می گیرد.

سرور ۲۰۰۳ وقتی به صورت یک روتر کانفیگ می شود ، استاندارد RFC ۱۵۴۲ را نیز ساپورت می کند.

توجه کنید که روترها به طور پیش فرض DHCP Broadcatsرا عبور نمی دهند ولی اگر Broadcast را روی آن اعمال کنیم پس BOOTP را هم ساپورت می کند.

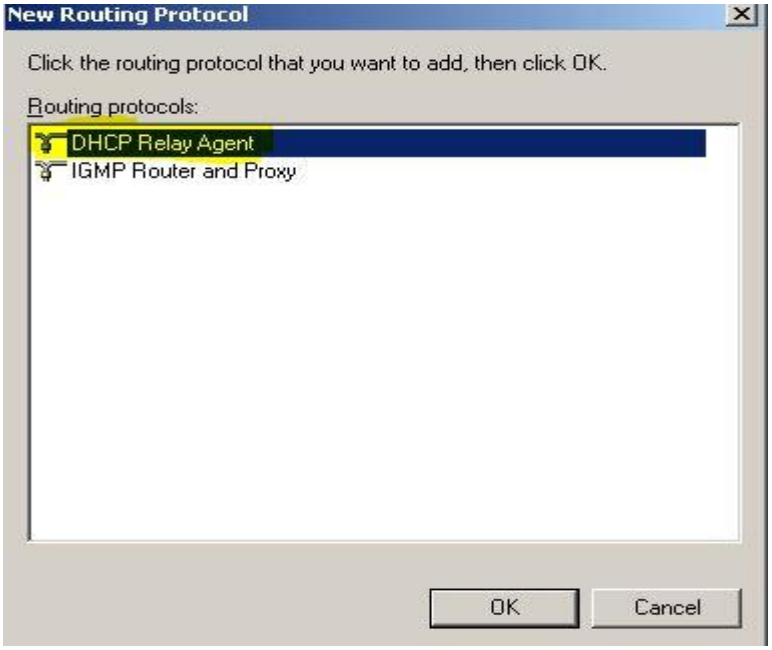
کانفیگ کردن DHCP Relay :

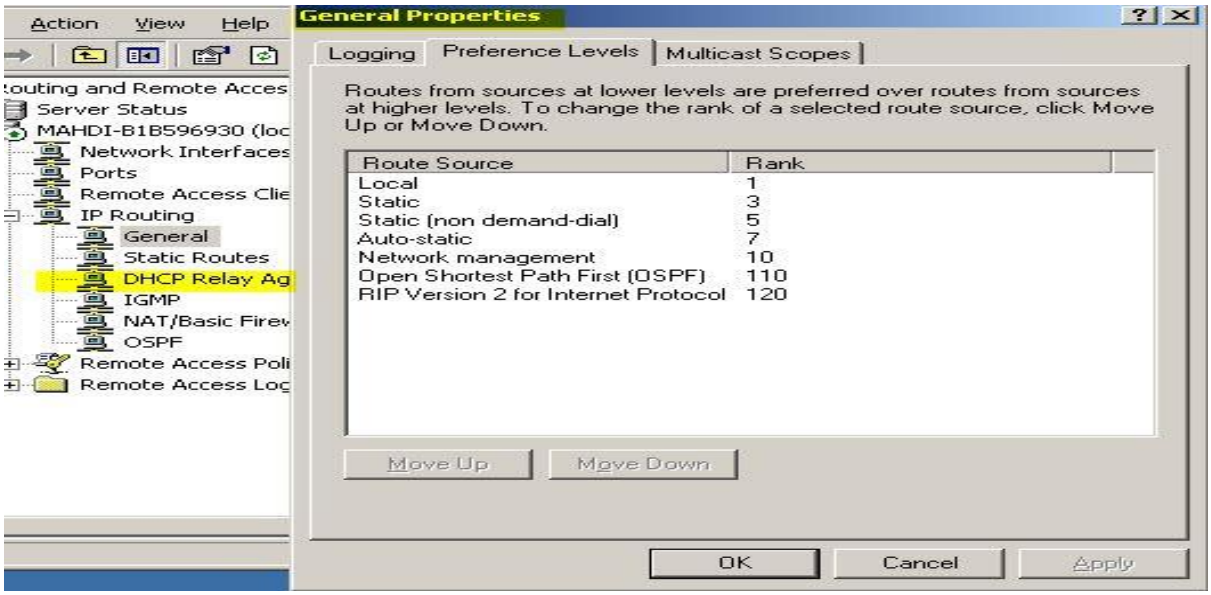
۱- اضافه کردن DHCP Relay Agent

۲- کانفیگ کردن خواص آن

۳- فعال کردن آن روی اینترفیس روتر

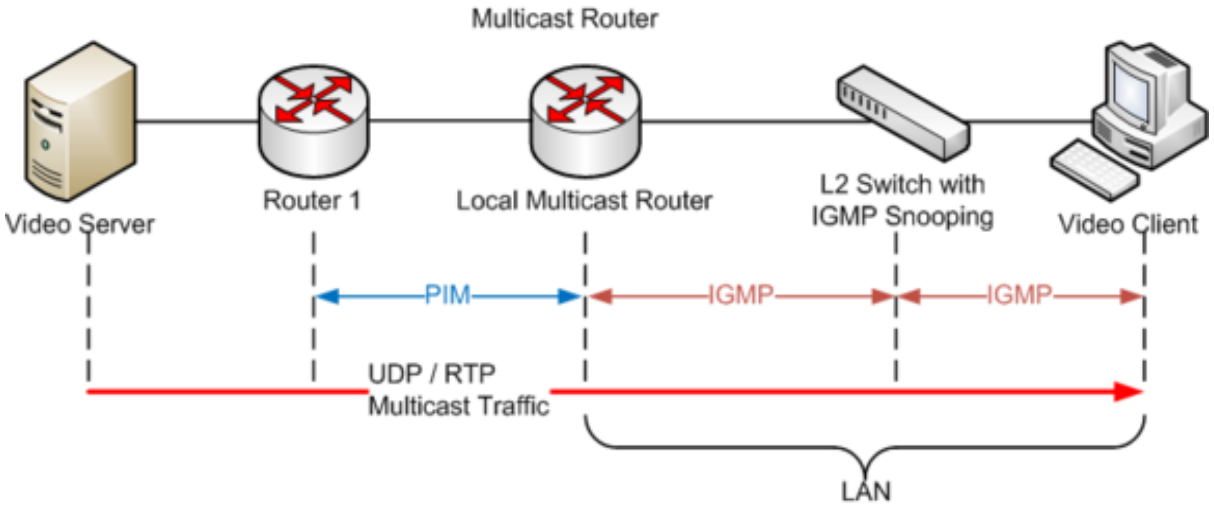
در تب جنرال در پنجره خواص آن لیست سرورهای DHCP (که اطلاعات را به آن ارسال می کند).





پروتکل IGMP : لایه Internet

Internet Group Managment Protocol (IGMP) ، پروتکلی است که مدیریت لیست اعضاء برای IP Multicasting ، در یک شبکه TCP/IP را بر عهده دارد . IP Multicasting، فرآیندی است که بر اساس آن یک پیام برای گروهی انتخاب شده از گیرندگان که گروه multicat نامیده می شوند ؛ ارسال می گردد . IGMP لیست اعضاء را نگهداری می نماید .



Pim یک پروتکل مسیریابی چند منظوره، که امکان ارسال broadcast را می دهد.

Igmp سه ورژن دارد:

IGMPv2 packet structure[7]

+	Bits 0–7	8–15	16–31
0	Type	Max Resp Time	Checksum
32	Group Address		

IGMPv3 membership query[10]

bit offset	0–3	4	5–7	8–15	16–31
0	Type = 0x11			Max Resp Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address [1]				
128	Source Address [2]				
	. . .				
	Source Address [N]				

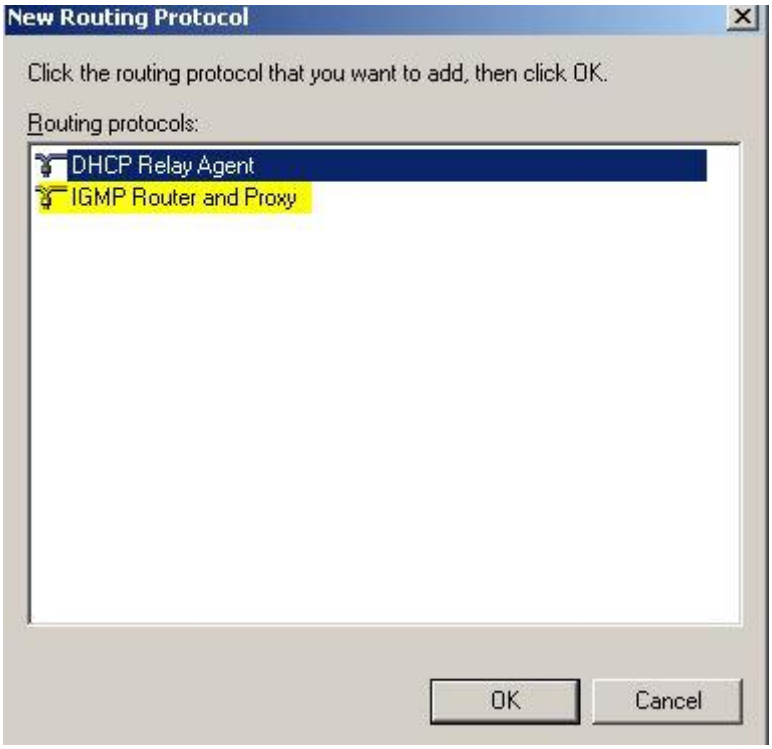
مدیریت IP Multicasting

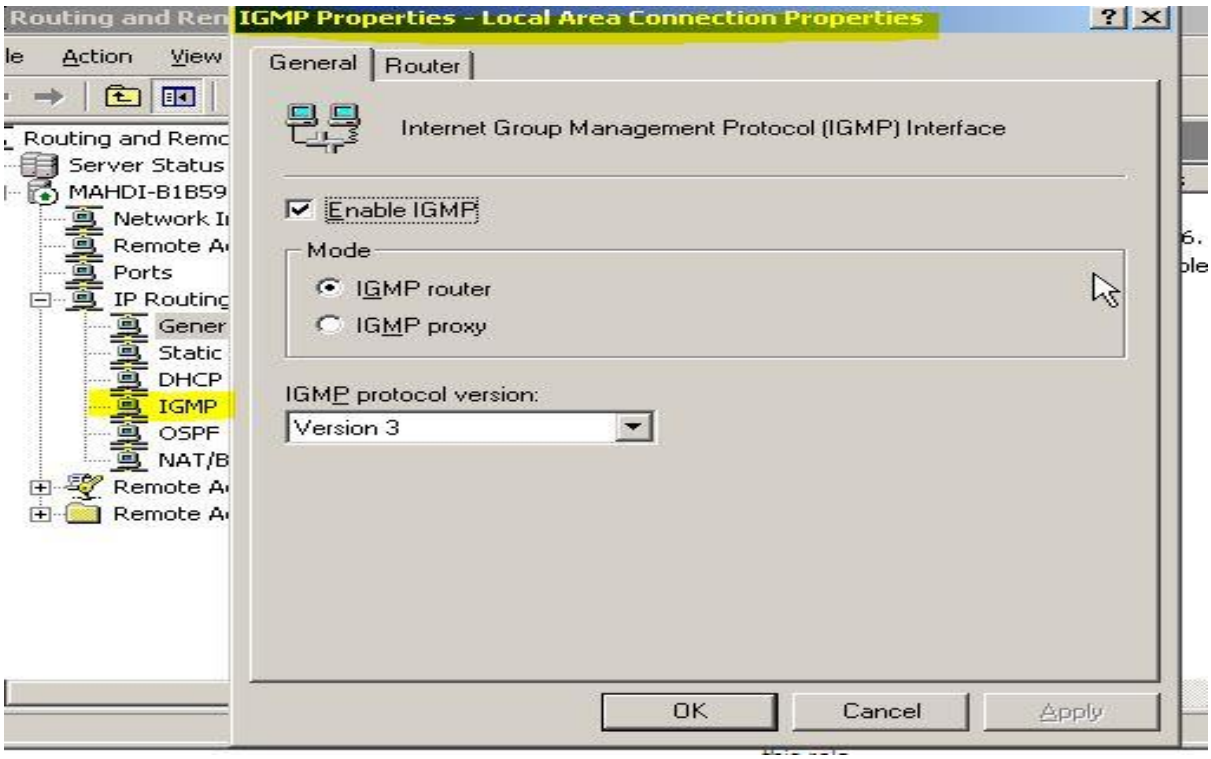
تمامی اعضاء یک گروه multicast ، به ترافیک IP هدایت شده به یک آدرس Multicast IP ، گوش داده و بسته های اطلاعاتی ارسال شده به آن آدرس را دریافت می نمایند. زمانیکه چندین کامپیوتر نیازمند دستیابی به اطلاعاتی نظیر Streaming media باشند، یک آدرس IP رزوشده برای multicasting استفاده می گردد. روترها که بمنظور پردازش multicast پیکربندی می گردند، اطلاعات را انتخاب و آنها را برای تمامی مشترکین گروه multicast ارسال (Forward) می نمایند . بمنظور رسیدن اطلاعات Multicast به گیرندگان مربوطه ، هر یک از روترهای موجود در مسیر ارتباطی می بایست ، قادر به حمایت از Multicasting باشند . کامپیوترهای مبتنی بر سیستم عامل وینوز ۲۰۰۰ ، قادر به ارسال و دریافت IP Multicast ، می باشند .

Igmp از این دو پروتکل استفاده می کند.

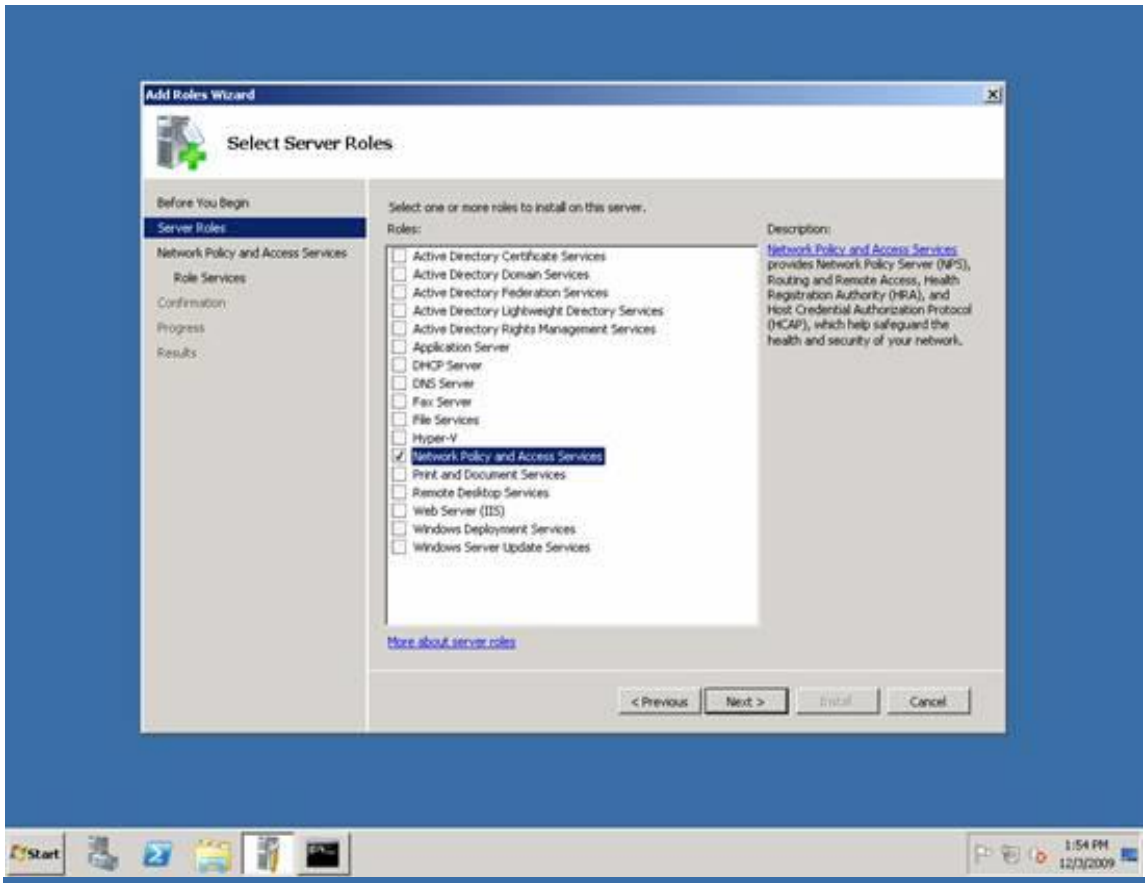
Cisco Group Management Protocol یا **CGMP** که پروتکل اختصاصی سیسکو است که بین روترها و سوئیچ های سیسکو از آن استفاده می شود. اگر cgmp روی روتر و سوئیچ تنظیم شده باشد، بروی آن روتر امکان ارسال multicast پکت ها ایجاد می شود.

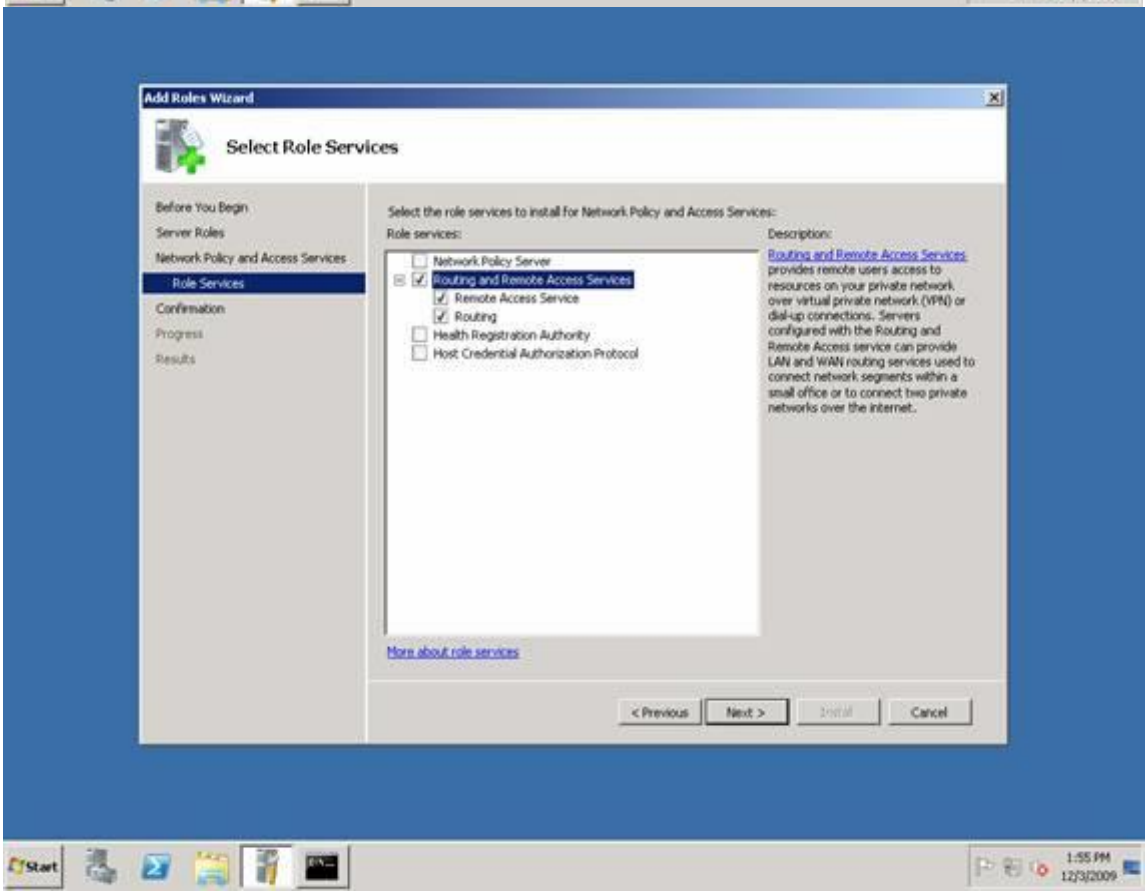
IGMP Snooping : پروتکلی استاندارد و شبیه به Cgmp و برای گوش دادن igmp می باشد.

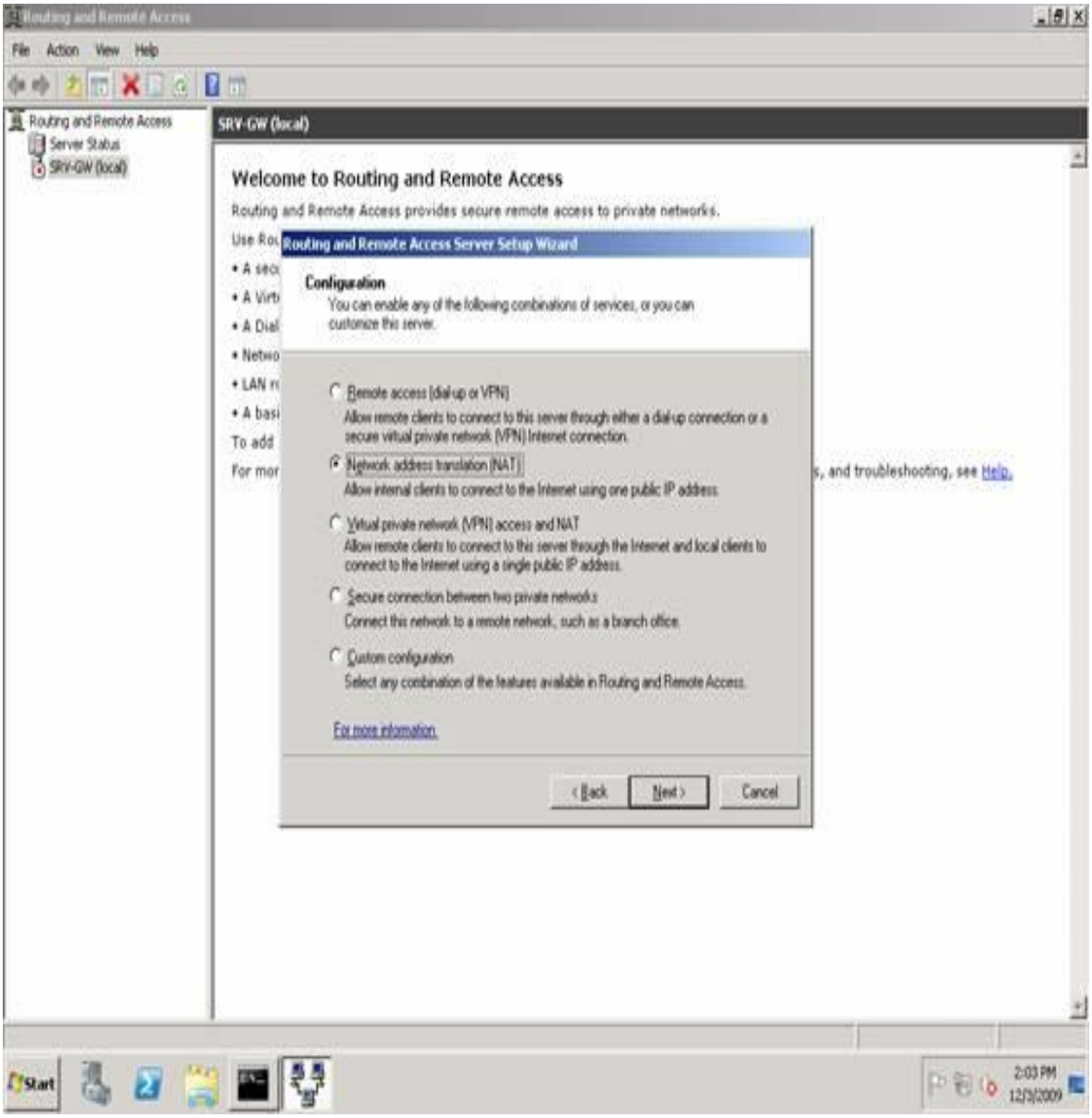

New Routing Protocol
Click the routing protocol that you want to add, then click OK.
Routing protocols:
DHCP Relay Agent
IGMP Router and Proxy
OK
Cancel


Routing and Ren
le Action View
Routing and Remc
Server Status
MAHDI-B1B59
Network I
Remote A
Ports
IP Routing
Gener
Static
DHCP
IGMP
OSPF
NAT/B
Remote A
Remote A
IGMP Properties - Local Area Connection Properties
General
Router
Internet Group Management Protocol (IGMP) Interface
Enable IGMP
Mode
IGMP router
IGMP proxy
IGMP protocol version:
Version 3
OK
Cancel
Apply

RRAS in Windows Server ۲۰۰۸






Routing and Remote Access
File Action View Help
Routing and Remote Access
Server Status
SRV-GW (local)
SRV-GW (local)
Welcome to Routing and Remote Access
Routing and Remote Access provides secure remote access to private networks.
Routing and Remote Access Server Setup Wizard
Configuration
You can enable any of the following combinations of services, or you can customize this server.
Remote access (dial-up or VPN)
Allow remote clients to connect to this server through either a dial-up connection or a secure virtual private network (VPN) Internet connection.
Network address translation (NAT)
Allow internal clients to connect to the Internet using one public IP address.
Virtual private network (VPN) access and NAT
Allow remote clients to connect to this server through the Internet and local clients to connect to the Internet using a single public IP address.
Secure connection between two private networks
Connect this network to a remote network, such as a branch office.
Custom configuration
Select any combination of the features available in Routing and Remote Access.
For more information
< Back
Next >
Cancel
Start
2:03 PM
12/3/2009

منابع :

- **MCSA / MCSE ۷۰-۲۹۱ Server ۲۰۰۳ Network Infrastructure I**
- **Data Communication Networks/M. R. Pakravan (Department of Electrical Engineering Sharif University of Technology)**
- **http://en.wikipedia.org/**