به نام خدا

پدافند غیرعامل- مسیریاب

فهرست

مقدمه

امروزه شبکه‌های رایانه‌ای نقش بسزایی در پیشرفت علم ارتباطات دارند به نحوی که رفته رفته بستر بسیاری از ارتباطات بر اینترنت استوار می‌گردد. شاهد و مثال این مدّعا انتقال سرویس تلفن از حالت سوئیچ مداری[۱] به IP است. از سویی دیگر با گذشت زمان و پیدایش نیازهای جدید، سرویسهایی جدیدتر بر شبکه تحمیل می‌شوند (مانند کنفرانس ویدئویی) که اضافه شدن این سرویسها مستلزم افزایش پهنای باند و کاهش تأخیر در شبکه می‌باشد.

اساس اکثر شبکه‌های رایانه‌ای بر مبنای پروتکل IP است. طرح اصلی این پروتکل از سیستم پستی الهام گرفته شده است که در آن بسته در هر دفتر پستی مورد بررسی قرار می‌گیرد و مسیر بعدی آن (مقصد یا دفتر پستی بعدی) معین می‌گردد. بدیهی است که در هر دفتر پستی اطلاعاتی از مسیرها موجود است به نحوی که با مقایسه‌ی آدرس مقصد بسته می‌توان مسیر بعدی آن را به دست آورد. مثال دفاتر پستی در شبکه‌های رایانه‌ای، همان مسیریابها هستند. مسیریابها در محل تقاطع خطوط ارتباطی قرار می‌گیرند و بسته‌ها را دریافت کرده، با توجه به آدرس مقصد، آنها را به مسیرهای بعدی هدایت می‌کنند.

---

[۱] Circuit Switch

بدین ترتیب مسیریاب از اجزاء اصلی شبکه به حساب می آید لذا در معرض خطر قرار گرفتن مسیریاب می تواند یک تهدید مهم برای کشور به حساب آید، بنابراین باید به این موضوع یعنی شناسایی تهدیدات علیه آن و راهکارهای مقابله با آن بهای بیشتری داده شود. با توجه به این مهم در اینجا بعد از معرفی اجمالی مسیریاب و ساختار و وظایف آن به نقاط آسیب پذیر و تهدیدات و حملات و راهکارهای مقابله با آن پرداخته شده است.

فصل ۱ – ساختار مسیریاب

یک مسیریاب، گره ای از شبکه است که نقطه یا گره بعدی شبکه که بسته باید به سمت آن ارسال شود و در نهایت به مقصد برسد را مشخص می‌کند. هر مسیریاب حداقل به دو شبکه وصل می‌باشد. مسیریاب براساس درک کنونی خود از وضعیت شبکه‌هایی که به آن وصل است، در مورد ارسال بسته‌های اطلاعاتی تصمیم می‌گیرد.

کار اصلی مسیریاب IP، ارسال کردن بسته‌ها از یک پورت ورودی به سمت پورت یا پورت‌های خروجی مناسب می‌باشد. این فرآیند بصورت قدم به قدم انجام می‌گیرد. بدین‌صورت که مسیریاب بسته را به جایی می‌فرستد که بسته به مقصد نهایی نزدیک‌تر شود. برای این امر مسیریاب از جدول Lookup استفاده می‌کند.

یک مسیریاب باید جدولی از مسیرهای موجود و وضعیت آنها درست کند یا بدست آورد تا از طریق اطلاعات آن و با استفاده از الگوریتم‌های مسیریابی موجود بتواند بهترین مسیر را برای بسته داده شده پیدا کند.

مسیریابها جداول Lookup را از طریق اجرای پروتکل‌های مسیریابی درست می‌کنند. آنها همچنین وظایف دیگری نظیر

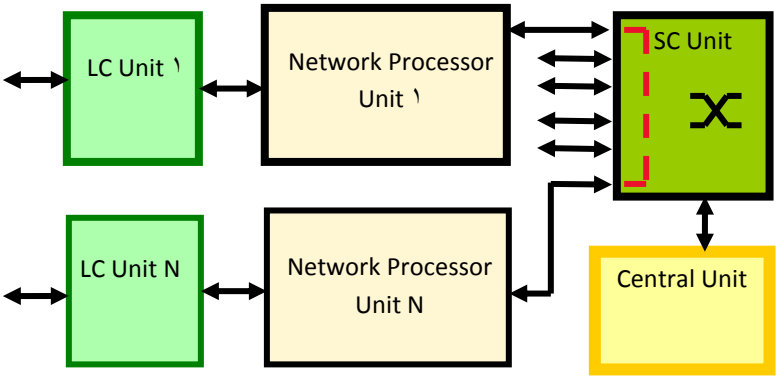
صف‌بندی و QOS[۱] نیز دارند. یک مسیریاب همچنین باید توانایی انجام عملیات مدیریت شبکه و ثبت اتفاقات آن را نیز داشته باشد.

مسیریاب از سه جزء اصلی تشکیل می‌شود که در شکل ۱ نشان داده شده است:

واحدهای کارت خط[۲]

واحدهای پردازشگر شبکه[۳] یا Forwarder

واحد مرکزی[۴]



شکل ۱: ساختار کلی و ساده شده مسیریابها

[۱] Quality of Service

[۲] LC

[۳] NP

[۴] Central Unit

بسته‌ها به واسط شبکه LC می‌رسند و توسط واحد پردازشگر شبکه پردازش می‌گردند و سپس از طریق واحد SC به پورت‌های خروجی هدایت می‌گردند (این واحد می تواند در نرم افزار پیاده سازی شود). این پورت‌ها نیز بسته را به سمت قدم بعدی هدایت می کنند تا به مقصد نهایی خود برسند. واحدهای کارت خط مسئول انجام عملیات لایه دو روی قاب‌های ورودی و استخراج بسته IP متناظر آنها می‌باشند تا سپس واحد پردازشگر شبکه آن بسته را پردازش نماید.

وظیفه اصلی واحد مرکزی،کنترل کردن کل سیستم می باشد، واحد مرکزی در مسیریاب بطور معمول عملیاتی نظیر محاسبات مسیر، به روز کردن جداول مسیریابی و مدیریت شبکه را انجام می‌دهد. این واحد همچنین پروتکل‌های مسیریابی[۱] را اجرا می‌نماید.

کارت خط شامل دو قسمت می‌باشد. قسمت واسط فیزیکی که ارتباط با خط مخابراتی را برقرار می‌نماید. قسمت دیگری در واحد کارت خط وجود دارد که مسئول انجام عملیات پروتکل لایه دو، نظیر قاب‌بندی[۲]، چک کردن CRC و ... می‌باشد.

---

[۱] routing

[۲] Framing

به محض اینکه بسته وارد واحد پردازشگر شبکه شود Parser عملیات Parsing را روی آن انجام می‌دهد که شامل شناسایی نوع بسته و بررسی قسمت‌های مهم آن می‌باشد تا معلوم شود که چه کاری باید روی آن انجام شود و توسط چه واحدهایی در آینده پردازش شود. Parser همچنین باید درست بودن بسته‌ها را قبل از ارسال به این واحدها چک نماید که این بررسی‌ها شامل چک کردن شماره و نسخه IP ، طول سرآیند[۱] IP و محاسبه Checksum است.

Classifier بسته‌ها را برحسب فیلدهای سرآیند TCP/IP نظیر پورت مقصد و آدرس IP مقصد دسته‌بندی می‌کند. واحد محاسبات سرآیند، مقدار TTL موجود در بسته را تغییر می‌دهد تا از چرخ زدن بی‌پایان بسته‌ها در اینترنت جلوگیری شود و در صورت کاهش مقدار فیلد TTL، Checksum را محاسبه می‌کند و مقادیر جدید فیلدهای TTL و Checksum را به جای مقادیر قبلی قرار می‌دهد.

واحد Lookup با استفاده از جدول Lookup پورت خروجی مناسب جهت بسته را پیدا می‌کند تا بسته را به سمت قدم بعدی هدایت کند. برای بسته‌های تک‌پخشی[۲]، این عملیات براساس آدرس IP مقصد

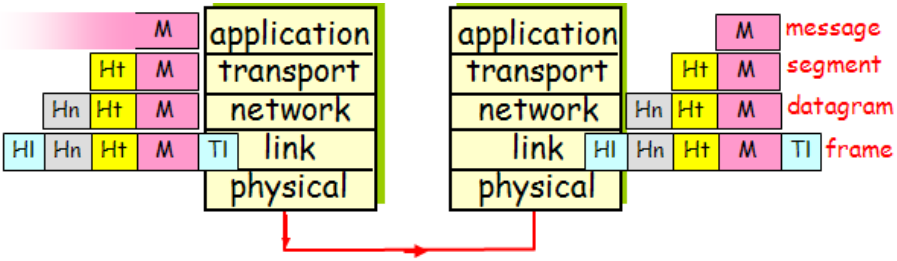
---

[۱] Header

[۲] Unicast

موجود در بسته IP و ماسک‌های زیرشبکه موجود در جدول Lookup انجام می‌شود.

مسیریاب همچنین باید آدرس فیزیکی مقصد بعدی بسته را مشخص نماید. این عمل بوسیله تطبیق دادن آدرس IP مقصد بعدی بسته به آدرس فیزیکی متناظر انجام می‌شود. پیدا کردن این آدرس‌های فیزیکی و ذخیره کردن آنها برای استفاده‌های بعدی وظیفه واحد ARP[۱] می‌باشد. بعد از این، واحد کارت خط بسته IP را برای انتقال به مقصد یا قدم بعدی آماده می‌کند یعنی سرآیند لایه دو و حتی شاید ته‌آیند[۲] لایه دو را به بسته اضافه کرده و آن را در قاب‌های لایه دو کپسوله می‌کند و آن را روی واسط فیزیکی انتقال می‌دهد.



شکل ۲ : نمایی ازعملیات انتقال بسته

[۱] Address Resolution protocol

[۲] Trailer

فصل ۲ – تقسیم بندی مسیریابها بر اساس کارکرد

مسیریابها بر اساس نوع کاربرد خود در نواحی مختلف از شبکه های رایانه ای به دسته های ذیل تقسیم می‌شوند که البته با توجه به مبنای تقسیم بندی که بر اساس معیار ظرفیت پردازش مسیریاب صورت گرفته است، امکان هر گونه تغییر در این دسته بندی با توجه به توسعه های آتی ظرفیت های شبکه ها، قابل پیش بینی است. بهر حال دسته‌بندی مسیریاب ها بر اساس کارکرد به شرح ذیل می باشد:

۱. مسیریابهای لایه هسته[۱] با ظرفیت های پردازش بیشتر از ۲ گیگابیت بر ثانیه مشهور به مسیریابهای ظرفیت بالا
۲. مسیریابهای لایه پخش[۲] با ظرفیت های پردازش بین ۶۰۰ مگابیت بر ثانیه تا ۲ گیگابیت بر ثانیه (ظرفیت متوسط)
۳. مسیریابهای لایه دسترسی[۳] با ظرفیت های پردازش کمتر از ۶۰۰ مگابیت بر ثانیه (ظرفیت پایین)

---

[۱] Core

[۲] Distribution

[۳] Access

نحوه افزایش ظرفیت پردازش مسیریابها طی دهه گذشته به شرح ذیل می باشد:

- تا سال ۱۹۹۲ به میزان ۲ گیگابیت بر ثانیه
- تا سال ۱۹۹۵ به میزان ۱۰ گیگابیت بر ثانیه
- تا سال ۱۹۹۸ به میزان ۴۰ گیگابیت بر ثانیه
- تا سال ۲۰۰۱ به میزان ۱۶۰ گیگابیت بر ثانیه
- تا سال ۲۰۰۳ به میزان ۶۴۰ گیگابیت بر ثانیه
- تا سال ۲۰۰۷به میزان ۱/۶ تا ۳/۲ ترابیت بر ثانیه

این روند رشد نمایانگر افزایش متوسط ظرفیت پردازش مسیریابها به میزان ۲/۲ طی ۱۸ ماه می باشد که قابل توجه است.

فصل ۳ – بومی سازی مسیریاب

بررسی های به عمل آمده دربین مسیریابهای موجود در دنیا مانند سیسکو[۱]، هواوی[۲]، ونگارد[۳]، زیمنس[۴]، جونیپر[۵]، آدتران[۶]، الکاتل/لوسنت[۷] نشان می دهد که محصولات تولید شده سیسکو، در جایگاه بسیار بهتری نسبت به رقبای خود قرار دارد.

از طرفی با توجه به محدود بودن ظرفیت اتصال ایران به شبکه اینترنت، اکثر مسیریابهایی که در لبه‌ها در ایران نصب می‌گردند با سرعتی کمتر از چند مگابیت بر ثانیه کار می‌کنند و ارتباط ISP ها با شبکه اینترنت نیز در همین حد می‌باشد. همچنین بنا بر شواهد موجود، استفاده از مسیریابها در ایران در حد کاربردهای ساده‌ای مثل ارسال بسته‌ها به default gateway است. لذا استفاده از یک نمونه ساده شده ساخت داخل، به صرفه‌تر از مسیریابهای گران قیمت با ظرفیت‌های بالا و امکانات فراوان خارجی است که از اکثر قابلیت‌های آن نیز استفاده

---

[۱] Cisco

[۲] Huawei

[۳] Vanguard

[۴] Siemens

[۵] Juniper

[۶] Adtran

[۷] Alcatel/Lucent

نمی‌شود. علاوه بر این، عدم امکان پشتیبانی از محصولات خریداری شده از خارج، همواره مشکلات متعددی را بدنبال داشته است.

بر اساس مطالعات میدانی صورت گرفته و طی مصاحبه های حضوری با دست اندرکاران این حوزه در داخل کشور، چند حوزه فعال در این مورد شناسایی شده است.

از جمله این حوزه ها آزمایشگاه مسیریاب دانشگاه تهران می باشد که با تیمی متشکل از اساتید و دانشجویان مقاطع کارشناسی ارشد و دکترا، موفق به ساخت مسیریاب آزمایشگاهی در مقیاس ظرفیت پایین شده اند. این تیم فعالیتهای زیادی در نرم افزار مسیریاب انجام داده است و حتی در مواردی مانند جدولlookup الگوریتمهایی را ابداع کرده است و در محصول خود استفاده نموده است. حاصل تحقیقات این تیم، چاپ مقالات بسیاری در مجلات و کنفرانسهای معتبر علمی در ارتباط با مسیریابها و مسیریابی بوده است. این مسیریاب تحت سناریوهای مختلف تست گردیده است.

فصل ۴ – تشریح مشخصات و ویژگیهای مسیریاب

هر مسیریاب بصورت کلی از سه بخش سخت افزار خارجی، سخت افزار داخلی و سیستم‌عامل تشکیل شده است که در ادامه توضیح بیشتر راجع به آنها ارائه می شود.

❖ سخت افزار های خارجی

بخش های خارجی را می توان به صورت های زیر تقسیم کرد:

- **بدنه:** همان جعبه مسیریاب ها می باشد که در مدل های قابل نصب بر روی رک[۱] و مدل های رومیزی[۲] به بازار ارائه شده است.
- بخش اتصالی به مسیریاب: این بخش، پشت مسیریاب قرار گرفته و بخش های متعددی هستند که بنا به نوع کارکرد مسیریاب در محیط شبکه، از پورتهای متنوعی همچون پورت اترنت، فیبر نوری و....برخوردار است. ضمن اینکه منبع تغذیه مسیریاب نیز که معمولاً در حالت AC و DC فعالیت می کنند، در این قسمت جای گرفته است.

---

[۱] Rack Mount

[۲] Desktop

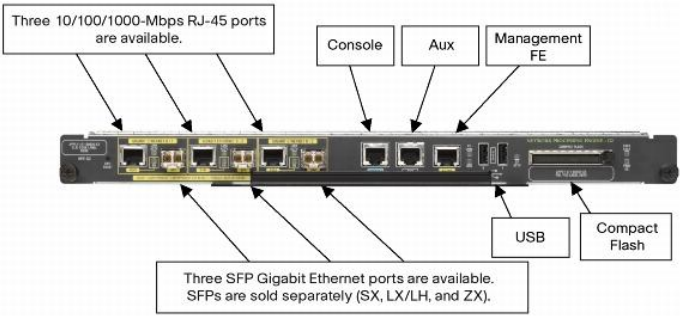
- پورت کنسول: تنظیم کردن[۱] مسیریاب به صورت دستی و مستقیم از این طریق صورت می‌گیرد. این تنظیم به خاطر دشوار بودن حرکت دادن مسیریاب ها در رک، معمولا یک بار و در بیرون با پورت کنسول صورت می گیرد و در مراجعات بعدی از روش های مختلف مثل Telnet انجام می پذیرد. کنسول مسیریاب با رنگ بندی خاصی تنظیم می شود.
- ماژول ها و کارت های واسط: از جمله مهمترین آنها کارت واسط WAN است که پشت مسیریاب قرار دارد، اما بسته به نوع مسیریاب می توان آنها را جدا یا اضافه کرد.
- حافظه خارجی[۲]: در این بخش اطلاعات تنظیم[۳] و سیستم عامل ذخیره می شودکه البته بسته به نوع نیازمندی های کاربر قابل ارتقاء می باشد.

---

[۱] Configuration

[۲] Flash Memory

[۳] Config



شکل ۷ : نمایی از سخت افزار خارجی مسیریاب

❖ سخت افزار های داخلی

تجهیزات داخلی مسیریاب با تجهیزات داخلی یک رایانه تفاوت چندانی ندارند. همه مسیریابها از ماردبورد، پردازشگر، حافظه ها و ... استفاده می کنند.

در ادامه به تشریح بیشتر اجزای داخل مسیریاب خواهیم پرداخت.

- CPU: اگر بخواهید سرعت پردازنده های کامپیوترهای شخصی را با مسیریاب‌ها مقایسه کنید حتماً تعجب خواهید کرد، چرا که حتی سریع‌ترین مسیریابها که می‌توانند درستون فقرات شبکه‌های اینترنتی استفاده شوند و طبعاً می‌بایست حجم بسیار وسیعی از ترافیک اینترنت را در زمان بسیار کوتاهی پردازش نمایند، سرعتی در حدود ۲۰۰ مگاهرتز دارند. ولیکن

از آنجایی‌که مسیریاب‌ها واسط گرافیکی کاربر ندارند و در محیط متنی کار می کنند و همچنین به دلیل تک‌منظوره بودن این پردازنده‌ها، این سرعت برای این منظور کفایت خواهد کرد.

- حافظه: در مورد حافظه هم می توان گفت که تمامی آنها از نوع DRAM [۱] هستند که در ماژول های SIMM [۲] قرار می گیرند و همانگونه که حافظه های یک رایانه قابل ارتقاء می‌باشد، این نوع از حافظه ها نیز می توانند ارتقاء یابند. این حافظه ها عبارتند از:
  - ✓ RAM: برای ذخیره اطلاعات حین کار، به کار می‌رود
  - ✓ ROM: در این نوع حافظه یک تصویر قابل بوت از سیستم عامل مسیریاب[۳] قرار می گیرد و در مراحل اولیه روند بوت مسیریاب مورد استفاده قرار می گیرد
  - ✓ Flash Memory: همانند هارددیسک درPC ها می‌باشد و برای ذخیره کل IOS[۴] مورداستفاده قرار می‌گیرد. ضمناً برای ذخیره فایل‌های پیکربندی نیز از این حافظه استفاده می‌شود

---

[۱] Dynamic Ram

[۲] Single Line Memory Module

[۳] IOS Image

[۴] Internetwork Operating System

- ✓ NVRAM[1]: مسیریابها از فایلی به نام Startup Config برای نگهداری تنظیمات ابتدایی پیکربندی مسیریاب استفاده می کنند و این فایل در این حافظه نگهداری می شود و پس از این‌که در روند بوت به داخل RAM دستگاه مسیریاب بارگذاری شد Running Config نامیده می‌شود

- واسطها: واسطها یا لینک‌های هر مسیریاب برای ارتباط با دنیای خارج در قالب پورت‌ها و ماژول‌ها که برای انعطاف‌پذیری مسیریابها درجهت انجام وظایف گوناگون قابل استفاده و تغییر است و داخل اسلات‌های توسعه قرار می گیرند.

❖ سیستم عامل مسیریاب (IOS)

IOS نرم افزاری است که از آن به منظور کنترل مسیریابی و سوئیچینگ دستگاه های بین شبکه ای استفاده می گردد. آشنائی با IOS برای تمامی مدیران شبکه و به منظور مدیریت و پیکربندی دستگاه هائی نظیر مسیریاب و یا سوئیچ الزامی است.

[1] Non-Volatile RAM

فصل ۵ – بررسی نقاط آسیب پذیر مسیریاب

آسیب پذیری های مربوط به مسیریاب در چهار لایه تقسیم بندی می شوند که عبارتند از:

۱. دسترسی فیزیکی: با داشتن دسترسی فیزیکی، نفوذگر می تواند کنترل کامل مسیریاب را در دست بگیرد. بنابراین نامشخص بودن وضعیت دسترسی افراد به مسیریاب، یک آسیب پذیری عمده محسوب می شود.
۲. نرم افزارهای داخلی و پیکره بندی اولیه: در صورتی که نفوذگر موفق به نفوذ در این لایه گردد، کنترل دو لایه بالاتر را برعهده خواهد گرفت. نقاط آسیب پذیر این لایه بیشتر نشانی واسط های موجود بر روی مسیریاب، رمزهای عبور، کنترل دسترسی به درگاه های پیکربندی و عدم تعیین روش های تغییر در پیکره بندی ثابت می باشد.
۳. پیکره بندی پویای مسیریاب: درمورد نقاط ضعف این لایه، نوع بروزشدن جداول مسیریابی و همچنین امنیت پروتکل مسیریابی از جایگاههای مهم آسیب پذیری است.
۴. ترافیک داده های مسیریاب: و بالاخره در این لایه، آدرس ها و پروتکل هایی که مجوز عبور دارند و یا سرویس های ارائه شده محل تهدید می باشد.

فصل ۶ – تشریح تهدیدات و حملات الکترونیکی بر روی مسیریاب

بطور کلی هدف اصلی اغلب حملات صورت گرفته بر روی سامانه های الکترونیکی و به خصوص مسیریابها، دسترسی غیرمجاز به این تجهیزات بوده تا با استفاده از آن، در کار سرویس دهی این سامانه ها ایجاد اختلال کرده یا آن را از کار بیندازند. نتایج حاصل از بررسی آمار آسیب پذیریهای از نوع دسترسی به سیستم طی سالیان اخیر نشان داد که این روند رو به افزایش است و همچنین در سال ۲۰۰۶ برترین رتبه از نظر نحوه نفوذ، به حملاتی داده شد که امکان دسترسی غیرمجاز به سامانه ها را مهیا می ساختند.

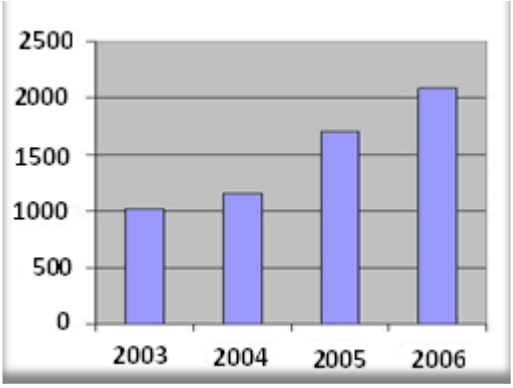
در حوزه شبکه های رایانه ای، تهدیدات در چهار دسته کلی شنود، وقفه، تغییر و جعل تقسیم بندی شده اند. حال در یک تقسیم بندی دیگر، چهار نوع حمله بر روی مسیریاب تعریف شده که عبارتند از:

- هک کردن DNS [۱]
- تخریب و تغییر سوء در جدول مسیریابی
- عملکرد نادرست مسیریاب در قبال بسته های داده
- حملات DoS [۱]

[۱] Domain Name System

مثالهای عینی متناظر با این نوع حملات بسیار گسترده بوده و پیامدهای چنین حملاتی نیز بسیار متنوع می باشند؛ به عنوان مثال برخی از پیامدهای این نوع حملات عبارتند از:

- مسیریابی اشتباه بسته های IP
- افشاء اطلاعات محرمانه
- تزریق اطلاعات جعلی یا تغییر یافته به شبکه
- خراب شدن عملیات مسیریابی در اثر ترجمه غلط آدرسها
- مختل شدن فعالیتهای شبکه با DoS
- دو تکه شدن شبکه و ایجاد ازدحام[۲] در شبکه



[۱] Denial of Service

[۲] Congestion

شکل ۹: افزایش آسیب پذیریهای از نوع دسترسی به سیستم طی سالیان اخیر

فصل ۷ – ملاحظات پدافند غیر عامل

با توجه به تهدیدات و حملاتی که به طور خلاصه در فصل قبل گفته شد، برای مقابله با آنها باید راهکار و تدابیری اندیشید که در این فصل به بعضی از این ملاحظات به اختصار اشاره می نماییم.

- اتخاذ تدابیر مناسب جهت بکارگیری مسیریاب های ستون فقرات شبکه در اتاق های شیلد با پوشش کلیه باندهای فرکانسی
- برقراری کنترل های دسترسی لازم جهت نظارت بر ترافیک ورودی و خروجی مسیریاب ها
- طراحی توپولوژی شبکه بصورت مقاوم در برابر انواع نفوذ
- بکارگیری قطعات سخت افزاری مطمئن در ساخت داخلی مسیریاب ها
- استفاده از پروتکل های امنیتی در مسیریابی شبکه
- ایجاد نظام کنترل دسترسی با امنیت بالا به منابع شبکه
- غیرفعال کردن سرویس مدیریت از راه دور مسیریاب ها در مواقع غیر ضروری

- ایجاد پروتکل های امنیتی مناسب بر روی سرویس مدیریت از راه دور
- ایجاد موانع مناسب جهت جلوگیری از اعمال نفوذ در سرویس مدیریت از راه دور مسیریاب
- استفاده از مسیریابهای پشتیبان جهت جلوگیری از وقفه در فعالیت شبکه
- نظارت دائم بر روی فعالیت مسیریاب به منظور کشف هرگونه فرآیند غیر عادی
- ایجاد سیستم گزارش گیری از ترافیک شبکه

همچنین برای کاهش تهدیدهای موجود در شبکه، می‌توان از ابزار و روشهای متنوعی استفاده کرد که به سه دسته تقسیم می شوند:

- ابزار و روش‌های "تصدیق هویت" کاربران
- ابزار و روش‌های پیشگیری[۱]، شناسایی و نشان دادن واکنش در برابر نفوذهای الکترونیکی شامل سیستم های تشخیص نفوذ و رویدادنامه‌ها، دیواره‌های آتش و تله‌های نرم‌افزاری و سخت‌افزاری می باشد.

---

۱ Prevention

- ابزار و روش‌های تامین امنیت ارتباطات نیز شامل شبکه های خصوصی، شبکه های خصوصی مجازی، مودم‌های امن و رمزنگاری داده‌ها می باشد.

و در آخر باید خاطر نشان کرد از منظرهای مختلف عملیاتی، اقتصادی و امنیتی و بطور کل بر اساس ضوابط و معیارهای پدافند غیرعامل در این زمینه، ساخت مسیریاب بومی بهترین راهکار مقابله با تهدیدات می باشد.