آموزش عملی و کاربردی CCNP TSHOOT

مؤلفان

محمدعلی بازیار

عاطفه شهریاری

نشر دانشگاهی کیان
Kian Publication

سخنی با خوانندگان

«سپس، به کاتبان و نویسندگانت بنگر و بهترین آن‌ها را بر کارهای خود بگمار... کاتبان و نویسندگانی برگزین که قدر خود را بشناسند، چون کسی که به قدر خود شناخت ندارد، دیگران را هم نمی‌شناسد.»

«برگرفته از نامه‌ی ۵۳ نهج‌البلاغه به مالک‌اشتر»

اگرچه نوشتن و پرداختن زکات علم از توصیه‌های اکید بزرگان و گواه بر کرامت اهل دانش است، اما امروزه پرداختن به انگیزه‌ها و اهداف نوشتن بیشتر جلوه می‌کند. بی‌شک این‌که چه کسی می‌نویسد مهم نیست، اما این‌که چرا و به چه پشتوانه‌ای می‌نویسد، درخور تأمل است. ما معتقدیم که چاپ روزافزون کتاب‌های به اصطلاح «زرد» که خالی از هرگونه نوآوری و بی‌توجه به استانداردهای چاپ کتاب و نیازهای مخاطبان است، حاصل تفکر بازاری مستولی بر جامعه‌ی نشر است. بی‌پرده آن‌که عنوان پر زرق و برق، دستاویز قرار دادن مضمون‌های نو با هدف فروش بالا و طویل کردن سیاهه‌ی سابقه‌ی علمی، نمی‌تواند دلیل محکمی برای چاپ و نشر کتابی باشد که خواننده‌ی مشتاق با صرف هزینه‌های نه چندان کم آن را تهیه می‌کند؛ به امید آن که چیزی از آن بیاموزد.

باید پذیرفت که انگیزه‌ی نوشتن کم از محتوای نوشته نیست و بین این دو رابطه‌ای مستقیم برقرار است. اگر انگیزه از نوشتن، تولید دانش باشد، بی‌شک نویسنده از قلم بی‌محتوا وکم‌عمق پرهیز می‌کند و اگر دغدغه‌ی دانش و فرهنگ زخم‌خورده در میان باشد، ناشر تنها به عنوان پرطمطراق بسنده نمی‌کند.

و چقدر امروزه، فرهنگ و دانش این مرز بوم که گرفتار آفت بی‌انگیزگی و زخم هوس است، نیازمند ناشران و نویسندگانی است که نیت‌شان کمک به رشد دانش و ارتقای فرهنگ جامعه است و به راستی که التیامی بر این درد نیست مگر نویسندگانی که قدر خود و دیگران را می‌دانند و خوب می‌فهمند که کتاب، ابزار سودجویی‌های مغرضانه نیست و می‌کوشند تا خود را از هرگونه عطش نام و رسم و ثروت تهی کنند.

انتشارات دانشگاهی کیان خود را بری از عیب و خطا نمی‌داند، اما همواره بیش از پیش می‌کوشیم تا در راستای تولید علم و نشر کتاب‌های پرمحتوا، دست نویسندگانی که انگیزه‌ی پاک دارند را فشرده و در کنارشان باشیم و از خداوند متعال می‌خواهیم که در این مسیر صعب و پرخطر در سایه‌ی لطف و عنایت خود از آن‌چه به عهده‌ی ما نهاده شده، سربلند و پیروز برآییم.

انتشارات دانشگاهی کیان

تقدیم به بهترین‌های من پدر و مادر

و تک ستاره درخشان زندگی، همسرم

مقدمه‌ی مؤلف

زندگی صحنه یکتای هنرمندی ماست ...
هرکسی نغمه خود خواند و از صحنه رود ...
صحنه پیوسته به جاست ...
خرم آن نغمه که مردم بسپارند به یاد.

کتابی که در پیش رو دارید تحلیلی بر آزمون TSHOOT است که یکی از سه رکن اصلی، جهت کسب مهارت‌های دوره CCNP، می‌باشد. به طور کلی آزمون‌های پیشرفته شرکت سیسکو (Cisco Certified Network Professional) شامل سه مرحله زیر هستند:

- CCNP Route با کد آزمون 642-902
- CCNP Switch با کد آزمون 642-813
- CCNP TSHOOT با کد آزمون 642-832

در این کتاب مباحث مربوط به روش‌های عیب‌یابی و نگهداری شبکه‌های مبتنی بر دستگاه‌های سیسکو، با بیانی گویا و با استفاده از لابراتوارهایی که محیط‌های واقعی عملیاتی را شبیه‌سازی کرده‌اند، بررسی شده است. به طوری که خواننده بعد از مطالعه این مباحث به راحتی می‌تواند مشکلات احتمالی در این نوع شبکه‌ها را تحلیل و رفع کند.

مطالب بررسی شده در لابراتوارهای این کتاب شامل روش‌هایی جهت بررسی و رفع مشکلات احتمالی که مدیران شبکه در محیط‌های عملیاتی با آن مواجه خواهند شد، می‌باشد.

این مطالب همراه با توضیح مختصری از مباحث مربوط به دوره‌های CCNP Route و CCNP Switch می‌باشد. اما به صورت کلی بهتر است دانشجویان تخصص‌های مربوط به Routing و Switching را داشته باشند تا بتوانند از مطالب کتاب بهتر استفاده کنند.

کمبود منابع فارسی برای Troubleshooting شبکه‌های مبتنی بر سیسکو و آماده‌سازی دانشجویان برای آزمون CCNP TSHOOT، ما را بر آن داشت که با تلاش‌های شبانه‌روزی این کتاب را تألیف کرده و در اختیار خوانندگان و دانشجویان عزیز قرار دهیم.

«متکلم را تا کسی عیب نگیرد سخنش اصلاح نپذیرد»

روشن است که کار انسانی هیچ‌گاه تماماً بی‌عیب و نقص نخواهد بود؛ از این‌رو، منتظر دیدگاه‌های ارزشمند شما اساتید، صاحب نظران و دانشجویان عزیز و گران‌قدر هستیم.

M.ali.bazyar@gmail.com
Atefe_shahriari@yahoo.com

فهرست مطالب

فصل اول: روش‌های نگهداری و عیب‌یابی شبکه

فصل دوم: ابزارهای مورد استفاده در عیب‌یابی

فصل سوم: عیب‌یابی سوییچ‌های سیسکو

فصل چهارم: عیب‌یابی پروتکل‌های مسیریابی

فصل پنجم: عیب‌یابی سرویس‌های شبکه

فصل ششم: عیب‌یابی شبکه‌های مبتنی بر IPv6

فصل اول

روش‌های نگهداری و عیب‌یابی شبکه

در این فصل ابتدا مدل‌های کاربردی جهت Maintenance شبکه‌ها و سپس روش‌های تئوری Troubleshooting در شبکه را مورد بررسی قرار می‌دهیم.

۱-۱. MAINTENANCE

Maintenance شبکه به معنای نگهداشتن شبکه در حالت اجرایی می‌باشد. وظایفی که جهت نگهداشتن شبکه در حالت UP باید انجام شود به این شرح است:

۱) نصب و پیکربندی سخت‌افزار و نرم‌افزارهای مورد نیاز؛

۲) نظارت بر Performance شبکه و اعمال سیاست‌هایی جهت بهبود کارایی؛

۳) آینده‌نگری جهت ارتقا و رشد شبکه؛

۴) ایجاد و بروز نگهداشتن Document تنظیمات شبکه؛

۵) اعمال دستورالعمل‌های امنیتی و حفظ شبکه در مقابل تمام تهدیدات.

مطمئناً این وظایف برای هر شبکه‌ای متفاوت می‌باشد، اما به صورت کلی وظایف Maintenance شبکه به دو قسمت تقسیم می‌شود:

۱) وظایف ساخت‌یافته[1]؛

۲) وظایف وقفه‌گرا[2].

- **Structured**: در این حالت یکسری از مشکلات را در شبکه پیش‌بینی می‌کنیم و با تعریف طرحی از پیش تعریف‌شده، قبل از وقوع یک مشکل آن مسأله حل خواهد شد.
- **Interrupt–driven**: مطمئناً خیلی از موارد یا مشکلات در شبکه را نمی‌توان پیش‌بینی کرد که در این حالت مدیر شبکه در صورت وقوع یک مشکل باید به سرعت آن را حل کند.

---

1. Structured Tasks
2. Interrupt-driven

نکته: در روش‌های نگهداری از شبکه، استفاده از مدل Structured که در آن طرحی جهت کاهش DownTime وجود دارد بسیار مؤثر می‌باشد.

باید خاطرنشان کرد که مدل‌های شناخته‌شده‌ای جهت Maintenance شبکه وجود دارد که می‌توان از یکی از آنها که با سیاست‌های سازمان شما بیشتر مطابقت دارد استفاده کنید.

در ادامه برخی از این مدل‌ها را مورد بررسی قرار خواهیم داد:

- **FCAPS**

این مدل توسط سازمان استاندارد جهانی ISO ایجاد شده است و معرف مجموعه‌ای از وظایف به شرح زیر می‌باشد.

۱) **F**ault Management:

جهت مدیریت خطاها، دستگاه‌های شبکه اعم از Router، Switch، Firewall و ... را به گونه‌ای پیکربندی خواهیم کرد که چنانچه خطایی (به‌طور مثال down شدن یک Interface) رخ دهد، پیغامی به صورت e-mail به مدیر شبکه ارسال شود.

۲) **C**onfiguration Management:

جهت مدیریت تنظیمات، شبکه را به گونه‌ای پیکربندی خواهیم کرد که برای هر تغییر در شبکه یک log در سرور مشخصی ایجاد شود که قبل از انجام تنظیمات از این اطلاعات استفاده خواهیم کرد.

۳) **A**ccounting Management:

با استفاده از مدیریت گروه‌های کاربری، محاسبات جهت استفاده کاربران از شبکه‌ی Wireless و هزینه‌ای که کاربران باید پرداخت کنند، مدیریت خواهد شد.

۴) **P**erformance Management:

جهت مدیریت کارایی شبکه، باید Performance تمام لینک‌های LAN و WAN تحت نظارت قرار بگیرند.

۵) **S**ecurity Management:

جهت مدیریت امنیت شبکه، باید یکسری سیاست‌های امنیتی ایجاد شود و با استفاده از Firewall، یا VPN و یا با استفاده از AAA (احراز هویت کاربران، مجوز کاربران، گزارش عملکرد کاربران) و دیگر سیستم‌های جلوگیری از نفوذ، این سیاست‌ها اجرا شوند.

- **ITIL**: **IT I**nfrastructure **L**ibrary

این مدل مجموعه‌ای از روش‌های مدیریتی سرویس‌های IT می‌باشد و تمرکز آن بر روی سرویس‌های IT مورد نیاز در تجارت می‌باشد.

- **TMN**: **T**elecomunication **M**anagement **N**etwork

این مدل از روش‌های Maintenance شبکه، زیرمجموعه‌ای از مدل FCAPS است که توسط سازمان ITU-T برای مدیریت ارتباطات در شبکه، معرفی گردیده است.

- **Cisco Lifecycle Services**

شرکت سیسکو مدلی جهت Maintenance شبکه ارائه داده است که در فازهای زیر پیاده‌سازی می‌شود:

۱) **Prepare**: آماده‌سازی؛

۲) **Plan**: طرح و برنامه؛

۳) **Design**: طراحی؛

۴) **Implement**: پیاده‌سازی؛
۵) **Operate**: بهره‌برداری؛
۶) **Optimize**: بهینه‌سازی.

نکته: انتخاب هر کدام از این مدل‌ها وابسته به نوع شبکه و یا تجارت شماست. شما می‌توانید از این مدل‌ها به عنوان یک Template استفاده کنید و بر اساس نیازهای شبکه‌ی خود مدل خاصی را ایجاد کنید.

یکسری وظایف مشترک در میان تمام مدل‌های Maintenance شبکه وجود دارد که در ادامه به بررسی این وظایف خواهیم پرداخت:

۱) **تغییرات پیکربندی**

تنظیمات در شبکه‌ها همیشه به صورت ثابت[1] نمی‌مانند. گاهی اوقات نیاز است که برای کاربران میهمان و یا کاربرانی که از شرکت شما به مکان دیگری منتقل می‌شوند تغییراتی را در پیکربندی جهت دسترسی آنها به منابع شبکه ایجاد کنید.

۲) **تعویض سخت‌افزار**

سخت‌افزارهای قدیمی باید با تجهیزات جدید جایگزین شوند.

۳) **تهیه نسخه پشتیبان**

باید از آخرین تنظیمات دستگاه‌ها به صورت زمان‌بندی‌شده نسخه‌ی پشتیبان تهیه شود تا در صورت بروز مشکل با استفاده از Backup تهیه‌شده به سرعت مشکل را برطرف کرد.

۴) **بروز رسانی‌های نرم‌افزار**

نرم‌افزارها و سیستم‌عامل‌های شبکه باید بروز نگاه داشته شوند، چرا که نسخه‌های قدیمی از نرم‌افزارها ممکن است از لحاظ امنیتی آسیب‌پذیر باشند.

۵) **نظارت**

همیشه نیاز به جمع‌آوری اطلاعات درباره‌ی ترافیک شبکه و همچنین میزان استفاده از پهنای باند وجود دارد. با استفاده از این اطلاعات می‌توان مشکلات شبکه را حل کرد و همچنین طرحی برای ارتقای شبکه در آینده فراهم کرد.

۱-۲. Trouble Shooting

در این مبحث به معرفی روش‌هایی جهت عیب‌یابی در شبکه‌ها خواهیم پرداخت.

به صورت کلی بروز مشکلات در شبکه به دلایل مختلفی می‌تواند باشد، اعم از:

- عامل انسانی که تنظیمات را به اشتباه انجام داده است؛
- سخت‌افزارهایی که دچار مشکل شده‌اند؛
- نرم‌افزارهای جدیدی که دارای اشکالاتی می‌باشند؛
- تغییر در الگوهای ترافیک که ممکن است باعث ایجاد ازدحام در شبکه شود.

برای رفع این خطاها روش‌های مختلفی وجود دارد که برخی مؤثرتر از روش‌های دیگر است. در ادامه به بررسی تعدادی از این روش‌ها خواهیم پرداخت.

1. Static

۱-۲-۱. مراحل عیب‌یابی شبکه

عیب‌یابی به صورت کلی شامل سه مرحله می‌باشد:

۱) **گزارش مشکل (Problem Report)**

۲) **تشخیص مشکل (Diagnosis)**

۳) **راه حل برای مشکل (Solution)**

گزارش مشکل: در ابتدا کاربران مشکلات را به مدیر شبکه گزارش می‌کنند و یا اینکه مدیر شبکه از طریق نظارت بر گزارش‌های رخداد[1] سیستم به مشکل موجود پی خواهد برد.

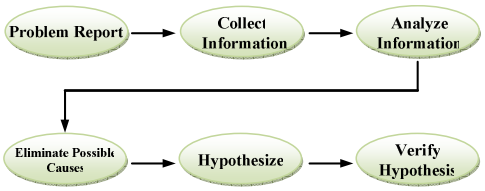
تشخیص مشکل: در مرحله‌ی بعد، مدیر شبکه باید با استفاده از روش‌هایی، علت اصلی مشکل را تشخیص دهد. این مرحله از مهمترین مراحل در Troubleshooting یک شبکه می‌باشد. در ادامه چند روش جهت تشخیص مشکلات در شبکه را بررسی خواهیم کرد.

راه‌حل برای مشکل: پس از طی مراحل قبل، مدیر شبکه با استفاده از دانش و تجارب خود بهترین راه‌حل را برای برطرف کردن مشکل به‌وجود آمده بکار می‌گیرد.

۱-۲-۲. روش‌های عیب‌یابی شبکه

۱-۲-۲-۱. روش عیب‌یابی ساخت‌یافته[2]

روند تشخیص مشکل به این شرح خواهد بود:



- **جمع‌آوری اطلاعات**

در اغلب اوقات کاربران اطلاعات دقیقی از مشکل ایجاد شده به مدیر شبکه نمی‌دهند. به طور مثال می‌گویند **" کامپیوتر من کار نمی‌کند!"**. بنابراین نیاز به جمع‌آوری اطلاعات دقیق‌تر از کاربران و یا استفاده از ابزارهای مانیتورینگ شبکه وجود خواهد داشت.

- **تجزیه و تحلیل اطلاعات**

بعد از جمع‌آوری اطلاعات شروع به تحلیل آن‌ها خواهیم کرد تا ببینیم چه چیزی اشتباه است. ما می‌توانیم این اطلاعات را با اطلاعاتی که قبلاً جمع‌آوری شده است و یا با تنظیمات دستگاه‌های مشابه مقایسه کنیم.

---

1. Log
2. Structured Troubleshooting Approach

- **از بین بردن علل احتمالی**

جهت از بین بردن علل احتمالی مشکلات در شبکه، نیاز به دانش کامل از شبکه و تمام پروتکل‌هایی که در آن دخیل هستند، وجود دارد.

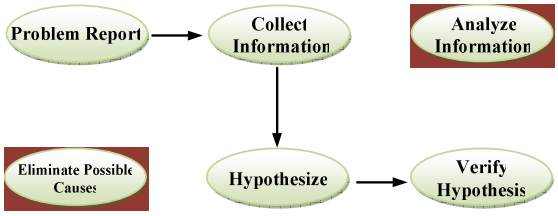
- **فرضیه**

پس از اینکه علل احتمالی مشکلات را در شبکه بررسی کردیم در این مرحله آن علتی که احتمال وقوع آن بیشتر می‌باشد را به عنوان علت اصلی مشکل انتخاب می‌کنیم.

- **بررسی فرضیه**

در این مرحله فرضیه‌ی انتخاب شده در مرحله قبل را بررسی می‌کنیم چنانچه این فرضیه اشتباه باشد یک علت احتمالی دیگر را انتخاب و بررسی خواهیم کرد. در غیراین‌صورت مشکل را برطرف می‌کنیم.

۱-۲-۲-۲. روش Shoot From The Hip



این روش را معمولاً افرادی که تجربه Troubleshooting در شبکه‌ها را دارند استفاده می‌کنند. به دلیل تجربه این افراد، دو بخش تجزیه و تحلیل اطلاعات و بررسی اشکالات احتمالی حذف می‌شود.

۱-۲-۲-۳. روش‌هایی جهت حذف علل احتمالی یک مشکل

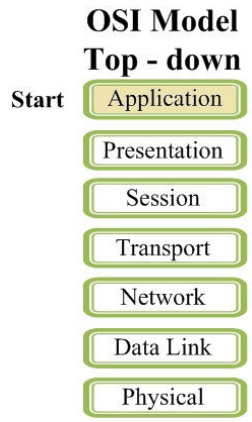
از بین تمام مراحل Troubleshooting شبکه، مرحله از بین بردن علل احتمالی یک مشکل[1] بسیار مهم است. چندین روش به شرح زیر برای انجام این کار وجود دارد:

- **Top – down**؛
- **Bottom – up**؛
- **Divide and conquer**؛
- **Follow the traffic path**؛
- **Spot the difference**؛
- **Replace components**.

۱) **Top–down**: در این روش، از بالاترین لایه‌ی مدل OSI (Application) شروع کرده و به سمت پایین‌ترین لایه، تمام موارد را بررسی خواهیم کرد.

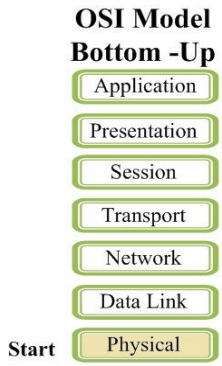
در این روش فرض می‌کنیم که چنانچه هر کدام از لایه‌ها بدون مشکل وظایف خود را انجام دهند، تمام لایه‌های زیرین آن نیز بدون مشکل خواهند بود. در این مدل در ابتدا نحوه‌ی دسترسی به Applicationهای موجود در شبکه بررسی می‌شود.

1. Eliminate Possible Cause



۲) **Bottom - up**: در این روش از پایین‌ترین لایه‌ی مدل OSI (Physical) شروع کرده و به سمت بالاترین لایه، تمام موارد را بررسی خواهیم کرد.

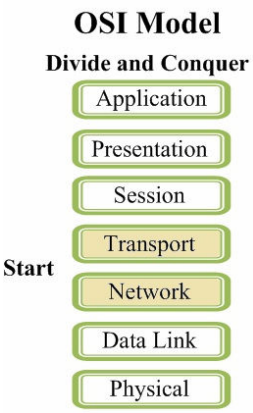
به عبارتی در ابتدا به بررسی کابل‌ها و کانکتورها خواهیم پرداخت. سپس به لایه‌ی بالاتر (Data Link) رفته و مواردی اعم از تنظیمات Ethernet، تنظیمات Spanning – Tree، تنظیمات Port Security و تنظیمات VLANها را بررسی خواهیم کرد و سپس لایه‌ی بالاتر (Network) و موارد مربوط به تنظیمات آدرس‌های IP، تنظیمات Access Listها پروتکل‌های Routing و... را بررسی می‌نماییم. این روش بسیار کامل است اما در عین حال وقت‌گیر است و برای کسانی که تجربه‌ی زیادی در عیب‌یابی شبکه ندارند، کاربرد دارد؛ چرا که در این روش تمام مشکلات احتمالی بررسی و برطرف خواهد شد.



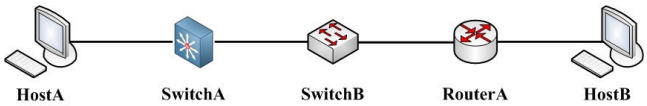
۳) **Divide and conquer**: در این روش از لایه‌های میانی مدل OSI شروع به بررسی موارد مختلف خواهیم کرد.

برای اجرای این روش با استفاده از دستور Ping یک بسته ICMP را از یک دستگاه به دستگاه دیگری ارسال می‌کنیم. چنانچه در نتیجه این دستور نشان داده شود که ارتباط با مقصد برقرار است (بسته به مقصد رسیده باشد)، به این نکته می‌رسیم که لایه‌های یک تا سه از مدل OSI مشکلی ندارند، بنابراین تمرکز خود را برای عیب‌یابی بر روی لایه‌های بالاتر مدل OSI قرار می‌دهیم.

چنانچه در نتیجه این دستور نشان داده شود که ارتباط با مقصد برقرار نیست (بسته به مقصد نرسیده باشد)، شروع به عیب‌یابی لایه‌های پایین مدل OSI می‌نماییم.



۴) **Follow the traffic path**:



این روش بسیار کاربردی است. در ابتدا سعی در ارسال بسته ICMP از HostA به HostB می‌کنیم. اگر ارتباط با مقصد برقرار نباشد تمام دستگاه‌های موجود در مسیر یکی پس از دیگری باید بررسی شوند.

به این صورت که ابتدا تنظیمات SwitchA بررسی می‌شود، چنانچه این تنظیمات مشکلی نداشته باشند، به سراغ دستگاه بعد (SwitchB) رفته و پیکربندی آن را مرور می‌کنیم و در صورتی‌که پیکربندی این دستگاه بدون عیب باشد، در نهایت تنظیمات RouterA را بررسی خواهیم کرد.

۵) **Spotting the difference**: این روش بسیار ساده است و در مواقعی کاربرد دارد که چندین دستگاه با تنظیمات مشابه در شبکه وجود داشته باشند. چنانچه یکی از دستگاه‌ها دچار مشکل شود با بررسی اختلاف در تنظیمات، به مشکل به‌وجود آمده پی خواهیم برد. این روش را معمولاً افرادی که تجربه زیادی در بحث عیب‌یابی شبکه ندارند استفاده می‌کنند.

۶) **Replace Component**: این روش، آخرین روش جهت حل مشکلات است. سناریوی زیر را در نظر بگیرید. چنانچه رایانه‌ی موجود در شبکه توانایی دسترسی به منابع شبکه را نداشته باشد، می‌توان تمام تجهیزات را با دستگاهی دیگر که از لحاظ سخت‌افزاری به آن اطمینان دارید، تعویض کنید.