قفل هاي ضروري براي امنيت سوئيچ در لايه ۲

سرقت اطلاعات: قصور و كم كاري در ايمن سازي ساختار سوئيچ ها مانند اين است كه از هكرها براي حمله به شبكه تان آشكارا دعوت به عمل آوريد. با اين حال مديران امنيت شبكه اغلب از اينكه ساختار لايه ۲ شبكه هايشان را محكم ببندند غفلت مي كنند.

اين راهنماي جامع روشهاي لازم و ضروري را كه شما را جهت پيكربندي صحيح و امن سازي ساختار سوئيچ تان توانا مي سازد برايتان تشريح و تبيين مي كند.

بسياري از مديران امنيت شبكه وقتي به لايه ۲ (جايي كه سوئيچ ها كار مي كنند) مي رسند، امنيت را از ياد مي برند و اين يكي از بيشترين جنبه هاي چشم پوشي از امنيت و قابليت اطمينان شبكه است. در اين مقاله من به شما نشان مي دهم كه چگونه يكي از معمول ترين اشتباهات در پيكربندي سوئيچ را اصلاح كنيد.

اگر چه من در مثالهايم از سيسكو استفاده مي كنم ولي مباحث و تكنيك هايي كه راجع به آن بحث مي كنيم در ساير كمپاني هاي تجهيزات شبكه نيز كاربرد دارد. اين رويه های امنيتي براي تمامي شبكه ها ضروري هستند خصوصاً وقتي كه از IP Phone ها استفاده شده باشد.

از SSH استفاده كرده و Telnet را غير فعال كنيد.

بديهي ترين كلمه عبوري كه روي تجهيزات سيسكو قرار مي دهيد رمز عبوري است كه با enable secret ست شده باشد. اگر اين را خالي رها كنيد سوئيچ شما در وضعيت بي دفاع قرار گرفته و هر كس مي تواند تنظيمات VLAN شما را ديده و از بين ببرد.

وقتي سوئيچ ها و ادمين هاي متعددي در شبكه داريد، بهترين كار اينست كه از مد AAA authentication و از يك user database محلي متمركز در +TACACS يا RADIUS SERVER براي مديريت سوئيچ ها و Admin هايتان استفاده كنيد.

+TACACS مي تواند مناسب تر باشد چرا كه مي تواند براي تمامي رويدادها log بيندازد و شما تاريخچه تمامي تغييراتي كه ايجاد شده و شخصي كه آن تغييرات را روي سوئيچ يا روتر شما ايجاد كرده داشته باشيد. اما مهمترين چيزي كه بايد به ياد داشته باشيد اينست كه به هيچ بهانه اي از Telnet استفاده نكرده و هميشه SSH را بر روي سوئيچ هايتان پياده كنيد.

حتي اگر image اي كه crypto-enabled باشد بر روي سوئيچ تان نداريد، تمامي image هاي رايج و امروزي به شما اجازه خواهند داد كه به سوئيچ تان SSH كنيد. هميشه يك username و password منحصر به فرد براي هر Admin ايجاد كنيد. سپس شما خواهيد توانست SSH را فعال كرده و Telnet را به خاك بسپاريد.

بر روي Native IOS سيسكو SSH را فعال كرده و Telnet را غير فعال سازيد	
دستورات	**توضيحات**
Username ***admin1*** privilege 15 password 0 ***Admin-Password***	Creates an administrator called admin1. Repeat for every admin
aaa new-model	Sets to AAA mode using a local database.
aaa authentication login default local	
aaa authorization exec default local	
aaa authorization network default local	
aaa session-id common	
ip domain name ***MyDomain.com***	Creates a name used for certificate
crypto key generate rsa	Generate digital certificate.
line vty 0 4	go in to vty configuration
transport input ssh	only permit SSH login

بخاطر داشته باشید که فرامین Native IOS مربوط به سوئیچ ها بر روی IOS روترهای سیسکو نیز کار می کند. کوتاهی در استفاده از SSH می تواند منجر به سرقت رمز عبور شده و کنترل کامل سوئیچ را به هکر بسپارد.

تضمین امنیت VTP و SNMP

ممکن است باورش سخت باشد ولی اکثر شبکه ها رمز عبور VTP Domain بر روی سوئیچ های سیسکوی خود ندارند. اگر آن را به حالت پیش فرض رها کنید، احتمالا کنترل شبکه را از دست می دهید و کل ساختار سوئیچ را روی شبکه جهانی وب برای بازدید همگان قرار می دهید.

از فرامین زیر در محیط global configuration یا در محیط VLAN Database که در image های قدیمی سیسکو استفاده می شود برای بستن تنظیمات VTP استفاده کنید.

اطمینان حاصل کنید که از رشته کاراکتر و password منحصر به فرد به جای آرگومانهای نمونه استفاده می کنید.

پیکربندی VTP برای Native IOS سیسکو	
دستورات	**توضیحات**
vtp domain ***My-VTP-name***	set the VTP name
vtp password ***My-VTP-password***	set the VTP password
vtp pruning	turn on VTP pruning

همچنین می بایست رمز SNMP (ترجیحاً SNMP ورژن ۳) را تنظیم کنید که همان تنظیم Password است. در این مقاله راهنمایی کاملی از مدیریت SNMP سیسکو می خوانید.

در اینجا یک مثال از چگونگی پیکربندی سرور SNMP به صورت Read-only و Read-Write با password های مناسب در محیط Conf t برای شما آورده ایم.

پیکربندی SNMP برای Native IOS سیسکو	
دستورات	**توضیحات**
snmp-server community ***MYRead-Only-string*** ro 50	Set read-only string for SNMP requests coming from ACL 50
snmp-server community ***MYRead-Write-string*** rw 51	Set read-write string for SNMP requests coming from ACL 51
access-list 50 permit ***IPaddress-ro***	Creates ACL of read-only SNMP servers. More than one permitted.
access-list 51 permit ***IPaddress-rw***	Creates ACL of read-write SNMP servers. More than one permitted.

اگر به هیچ وجه قصد ندارید که از SNMP استفاده کنید می بایست آن را با دستور no snmp-server در محیط global configuration از کار بیندازید و تمامی دستورات قبلی SNMP را نادیده بگیرید.

بستن اساسی پورت

سوئیچ ها می بایست به مفهوم least-privilege (حداقل امتیازات ویژه) مانند سایر چیزها در مبحث امنیت متعهد باشند. بهترین راه برای نصب کردن یک سوئیچ این است که در ابتدا، تمامی پورتها را خاموش کرده و همانطور که پیش می رویم به فراخور نیاز آنها را روشن سازیم.

از این گذشته می بایست هر پورت را در یک VLAN بلااستفاده که راه به جایی نداشته و default gateway هم ندارد قرار دهید. می توانید یک VLAN به نام "unused" با یک شماره مشخص مثل ۳۳۳ ساخته و همه پورتها را در آن VLAN قرار دهید. در مثال زیر یک سوئیچ ۴۸ پورت با IOS سیسکو داریم.

بستن اساسی پورت برای Native IOS سیسکو	
دستورات	**توضیحات**
int range FastEthernet0/1 – 48	Go in to interface 1 – 48
switchport access vlan 333	Sets port to VLAN 333
switchport mode access	Turns off auto VLAN trunking
Shut	Turns off port

لازم است که این کار برای همه سوئیچ ها انجام شود که می تواند بسته به مدل سوئیچ و نوع OS آن متنوع و متغیر باشد. اگر از برخی اقسام Stacking استفاده می کنید می بایست آن را برای هر Stack انجام دهید.

سپس همینطور که سرورها را وصل می کنید پورتها را "no shut" کرده و آنها را در VLAN مناسب قرار داده یا حتی اگر واقعا نیاز باشد آنها را به پورتهای trunk تبدیل کنید.

زمانی که VLAN ها را به سرورها و کامپیوترها اختصاص می دهید، به هیچ وجه از VLAN 1 که به صورت پیش فرض Native VLAN بوده و یا هر VLAN ای که به صورت دستی آن را Native کرده اید استفاده نکنید.

اجتناب از بکارگیری Native VLAN برای سرورها و کامپیوترها و سایر تجهیزات، حملات VLAN hopping را با شکست مواجه خواهد ساخت.

اگر این فرایند ابتدایی بستن پورتها را انجام ندهید، تمامی پورتهای سوئیچ در حالت پیش فرض در VLAN 1 خواهند بود. افراد زیادی هستند که به این شکل از سوئیچ ها استفاده می کنند که این یک اشتباه فاحش است.

همینطور که تجهیزات را به پورتها وصل می کنید بهتر است از دستور "description **My-Port-Name**" در IOS سیسکو برای برچسب زدن بر روی هر پورت استفاده کنید.

در IOS سیسکو Catalyst از دستور "set port name 3/34 **My-Port-Name**" برای برچسب زدن به پورتها استفاده می شود.

استفاده از سرورهای گزارش گیری SNMP نظیر Solarwinds یا HP OpenView بسیار مفید خواهد بود چرا که توضیحات توصیفی پورت در هنگام گزارش گیری مشخص می شوند. این بهترین شکل مستندسازی است که وجود دارد به خاطر اینکه حقیقتاً کاربرد دارد.

آنهایی که در بستن اولیه پورتها کم کاری می کنند، به همگان اجازه می دهند که به سوئیچ هایشان ترانک کرده و به هر VLANی که می خواهند متصل شوند.

محدود کردن Trunking در VLAN

هنگامی که بر روی یک پورت VLAN trunking فعال می شود، آن پورت ترانک شده بایستی تعداد VLAN ها را حداقل کرده و فقط آن VLAN هایی که بایستی در سوئیچ پوشش داده شوند اجازه عبور داشته باشند.

در مثال زیر یک پورت ترانک را به نحوی تنظیم می کنیم که فقط VLAN های ۱۲ تا ۱۴ و ۲۰ تا ۲۲ اجازه عبور داشته باشند.

محدود کردن VLAN trunking برای Native IOS سیسکو	
دستورات	**توضیحات**
interface GigabitEthernet1/0/2	Enter second gigabit port on Cisco 3750
switchport mode trunk	Turns on trunking mode
Switchport trunk encapsulation dot1q	Sets trunk type to IEEE 802.1q

switchport trunk allowed Vlan 12-14, 20-22	Only allow VLANs 12-14 and 20-22

در Native IOS سیسکو همه VLAN ها تا وقتی که آنها را تغییر نداده ایم بلاک هستند. کوتاهی در محدود کردن اجازه عبور VLAN ها بر روی پورتهای ترانک بدین معنی است که تجهیزات متصل به پورتها علیرغم میل شما اجازه اتصال به VLAN های بیشتری خواهند داشت.

STP BPDU guard و STP Root guard

هکرها می توانند انواع حقه ها را با ارسال ترافیک BPDU به نمایش گذارند که باعث می شود محاسبات مجدد VLAN STP (که حداقل ۳۰ ثانیه برای پاک شدن زمان می برد)، تحمیل شود. این کار به آنها اجازه می دهد که به تعداد نامحدودی حملات DOS (denial of service) را ترتیب دهند. آنها همچنین می توانند وانمود کنند که STP root هستند و از این طریق ترافیک را دزدیده و منحرف سازند.

BPDU guard و Root guard می توانند از این نوع حملات ممانعت به عمل آورند.

BPDU guardو Root guard برای Native IOS سیسکو	
دستورات	**توضیحات**
spanning-tree portfast bpduguard	Enables BPDU guard on the switch
spanning-tree guard root	Enables Root guard on the switch
spanning-tree rootguard	Alternative command for some IOS versions

توجه داشته باشید که می بایست Root guard و BPDU guard را روی پورتهایی که به دیگر سوئیچ ها متصل است غیر فعال سازید.

سهل انگاری در پیاده سازی این ویژگی های امنیتی به هکرها اجازه خواهد داد که BPDU DOS(denial of service) را روی تمامی ساختار سوئیچ اجرا کرده و احتمالاً ترافیک را قطع کنند.

جلوگیری از بمباران CAM Table و DHCP

هکرها می توانند از این مزیت که سوئیچ ها و سرورهای DHCP تعداد محدودی آدرس MAC و IP می توانند در خود نگهداری کنند، سوء استفاده کنند. یک هکر می تواند آدرس MAC خود را تغییر داده تا از این طریق تعداد آدرس IP بیشتری از سرور DHCP درخواست کرده و همه آدرسهای IP را در ظرف محدود DHCP تصاحب کند. هکر همچنین می تواند با تغییر سریع آدرس MAC خود ظرفیت CAM Table را بر روی هر سوئیچی به سرعت تکمیل کند.

وقتی ظرفیت CAM Table بر روی سوئیچ تکمیل شود، آن سوئیچ عملاً به یک Hub تبدیل می شود.

علاوه بر این تنزل رتبه اساسی، سوئیچ مجبور است که هر تغییر در شبکه را بر روی تمامی پورتها اعلام عمومی (broadcast) کند که این کار هکرها را قادر می سازد که از هر دستگاهی روی سوئیچ استراق سمع کنند. درست مثل اینکه با یک Hub سر و کار دارند.

برای جلوگیری از حملات DHCP و CAM Table می بایست port security را شبیه مثال زیر پیکربندی کنید:

جلوگیری از بمباران DHCP و CAM Table روی Native IOS سیسکو	
دستورات	**توضیحات**
int range FastEthernet 0/1 – 48	Go in to interface 1 – 48
switchport port-security	Turns on port security
switchport port-security maximum 5	Allow up to 5 MAC addresses
switchport port-security violation protect	Drop packets beyond 5 MAC addresses

switchport port-security aging time 2	
switchport port-security aging type inactivity	

این مراحل را سایر پورتها و سوئیچ ها تکرار کنید. توجه داشته باشید که روی پورتهایی که به سایر سوئیچ ها متصل هستند می بایست port security را غیر فعال کنید.

ممانعت از DHCP spoofing، MAC spoofing و IP spoofing

ARP spoofing و IP spoofing هکرها را قادر می سازد که خود را به جای دیگری وانمود ساخته و ترافیک را به سرقت ببرند. DHCP spoofing یک هکر را قادر می سازد تا کلاینتهای غیر شک برانگیز را تحت یک IP range جعلی در اترنت قرار داده که می بایست به واسطه هکر جریان یافته و به نقاط امن شبکه دست یابند.

هر سه متد بدین منظور طراحی شده اند که جریان ترافیک شبکه را به سرقت برند تا هکر بتواند همه انواع اطلاعات محرمانه را در شبکه داخلی sniff کند.

شما می توانید بواسطه راه اندازی DHCP snooping ، Dynamic ARP inspection و IP Source guard از این گونه حملات در شبکه جلوگیری کنید.

جلوگیری از DHCP,ARP,IP spoofing روی Native IOS سیسکو	
دستورات عمومی	**توضیحات**
ip dhcp snooping vlan 1-1000	Turn on DHCP snooping for VLANs 1-1000
ip dhcp snooping	Turn on DHCP snooping
no ip dhcp snooping information option	
ip arp inspection vlan 1-1000	ARP inspection on VLAN 1-1000
ip arp inspection log-buffer entries 1024	
ip arp inspection log-buffer logs 1024 interval 10	
دستورات اینترفیس میزبان	**توضیحات**
int range FastEthernet 0/1 – 48	Go in to interface 1 – 48
no ip arp inspection trust	Locks down host ports for ARP
ip arp inspection limit rate 15	Sets ARP pps inspection rate
ip verify source vlan dhcp-snooping	Turns on IP Source Guard
دستورات اینترفیس کلاینت DHCP	**توضیحات**
no ip dhcp snooping trust	Don't allow DHCP server
ip dhcp snooping limit rate 10	Limits rate of DHCP requests
از دستورات زیر فقط برای پورتهای DHCP مورد اطمینان و پورتهایی که به سایر سوئیچ های مطمئن وصل هستند استفاده کنید. دستورات زیر برخی از دستورات بالا را نقض می کنند. اشتباه در اجرای دستورات زیر برای اتصالات معتبر سوئیچ و سرورهای DHCP، شبکه و DHCP را از کار خواهد انداخت.	
دستورات اینترفیس سرور DHCP	**توضیحات**
ip dhcp snooping trust	This port allows DHCP servers
Switch Interface Commands	**Description**
ip arp inspection trust	Unlocks port used to connect to trusted switches

توجه داشته باشید که OS مربوط به سیسکو Catalyst ویژگی anti-spoofing را پشتیبانی نمی کند. بنابراین بهتر است از سیستم عامل کاتالیست به Native IOS مهاجرت کنید. Anti-spoofing یکی از مؤلفه های بسیار مهم در پدافند لایه ۲ است که ساختار سوئیچ را در برابر تهدیدهای LAN داخلی استحکام می بخشد.
تهدیدات داخلی بایستی به اندازه تهدیدات خارجی جدی گرفته شوند زیرا یک کامپیوتر داخلی که با malware ها و rootkit ها توافق نامه امضا کرده! تهدیدات خارجی را به تهدیدات داخلی تبدیل می کند.

محدود کردن اندازه دامنه STP

این یکی از جنبه های ساختار سوئیچ است که اغلب نادیده گرفته می شود. یک دامنه STP نباید اجازه داشته باشد که بیش از حد بزرگ و پیچیده شود.
بسیار مشاهده شده است که در شبکه های برخی سازمانها یک کاربر به تنهایی کل شبکه آن سازمان را با هزاران کامپیوتر و تلفن های IP متعدد پیاده کرده و از کار انداخته است. آنهم فقط به خاطر اینکه به صورت کاملاً تصادفی به یک سوئیچ رومیزی plug کرده و بصورت کاملاً تصادفی با یک کابل CAT-5 ، loop ایجاد کرده است.
همان شبکه یک VLAN پیچیده و مبهم با وسعت کل سازمان دارد و زمانی که هر چیزی در دامنه STP یک درخواست BPDU ارسال می کند که محاسبات مجدد STP را در بر دارد، کل شبکه سازمان به مدت ۳۰ ثانیه از کار افتاده که این مورد ممکن است بارها در طور روز اتفاق بیفتد. این توقف در شبکه برای data به اندازه کافی مضر است اما بیاد داشته باشید که ساختار IP telephony نیز از کار می افتد که بسیار ناگوار است. صدها نفر از کارکنان به این دلیل که دسترسی به data و تلفن شبکه ندارند نمی توانند کار خود را انجام دهند.
به منظور جلوگیری از ایجاد توپولوژی STP پیچیده و بزرگ، می بایست به جای سوئیچ کردن ترافیک، آن را route کنید. در حقیقت، این بدان معناست که به جای استفاده از سوئیچ های لایه ۲ که فقط سوئیچ کردن را بلد بوده و routing را بلد نیستند می بایست از سوئیچ های لایه ۳ استفاده کنید.
همچنین این بدین معنی است که VLAN ها نمی توانند در سوئیچ هایی که به دامنه STP آنها تعلق ندارند گسترش یابند.
این نوع تغییر ساختار به معنی طراحی مجدد تمامی شبکه داخلی سازمان است و کار ساده ای نیست. اما این نتایج می بایست قبل از توسعه شبکه IP telephony در نظر گرفته شوند.

نگهداری و بروزرسانی نرم افزار سوئیچ به آخرین ورژن های موجود

یکی از بزرگترین اشتباهات در بحث امنیت شبکه اینست که مردم فکر کنند ساختار سوئیچ و روتینگ شبیه لوله کشی ساختمان است که هرگز نیاز به دستکاری نداشته باشد. لیکن در صورتی که یک سوئیچ یا روتر سیسکو را با نرم افزاری که بیش از ۶ ماه از عمر آن گذشته راه اندازی کرده اید، احتمال دارد برخی آسیب پذیری های امنیتی روی روتر یا سوئیچ تان داشته باشید.
شاید تعجب کنید اما افرادی هستند که بر روی تجهیزات سیسکو image های سه یا چهار ساله دارند و اصلاً هم به فکر بروزرسانی آنها نیستند.
همواره همانطور که سرورها و کامپیوترهای خود را بروزرسانی می کنید تجهیزات شبکه خود را نیز با آخرین نرم افزارهایی که از فروشندگان مجاز سخت افزار دریافت می کنید به روز نگه داشته و همیشه بدنبال بروزرسانی های جدید نیز باشید.
همه مهندسان امنیت و شبکه باید همیشه از خود بپرسند "آخرین باری که من نرم افزارهای تجهیزات شبکه را به روز کرده ام چه زمانی بوده است؟" همچنین طرحی که شامل کارهای ضروری و بلند مدت است تهیه کرده و به مدیر سازمان ارائه دهند.
قبل از اینکه حادثه بدی به وقوع بپیوندد کارهای لازم را برنامه ریزی و اجرا کنید.

مطلب نهایی

امنیت لایه ۲ یکی از مؤلفه های امنیت اطلاعات است که اغلب مورد چشم پوشی قرار گرفته و در ممیزی های امنیت شبکه نیز فراموش می شود. بویژه وقتی که ممیزی ها به جای پرداختن به پیاده سازی واقعی، بیشتر بر روی سیاست های امنیتی (policy) متمرکز شوند. هکرها نگرانی راجع به سیاست های امنیتی نداشته و بیشتر به دنبال حفره های امنیتی هستند که برایشان آماده شده است. حملات لایه ۲ اولین چیزی است که یک هکر بعد از گرفتن دسترسی root یک کامپیوتر در داخل شبکه، روی آن کار می کند. جنبه دیگر حملات لایه ۲ که اغلب از آن چشم پوشی می شود، شرکت هایی هستند که امنیت شبکه بی سیم بر مبنای VPN ایجاد کرده اند.

تا زمانی که به کلاینت های تأیید اعتبار نشده و بی اسم اجازه داده می شود که به access point ای که مستقیماً به یک سوئیچ داخلی وصل است و توسط VLAN از هم جدا شده اند وصل شوند می بایست امنیت در لایه ۲ را به فراموشی بسپاریم.

بسیار مشکل خواهد بود که آدرسهای MAC ای که از access point می آیند را محدود کنیم. به همین دلیل است که بسیار توصیه می شود امنیت شبکه بی سیم مبتنی بر VPN می بایست از امنیت شبکه بی سیم مبتنی بر 802.1x اجتناب کرده و دور شود. فراتر از این رویه های بستن و محدود کردن که توضیح داده شد، مرحله بعدی در امنیت لایه ۲ سوئیچ، نسخه کابلی از امنیت 802.1x شبکه LAN می باشد. خوشبختانه همان ساختاری که برای تأیید اعتبار LAN بی سیم استفاده می شود برای تأیید اعتبار LAN کابلی نیز استفاده می شود.

امنیت مبتنی بر پورت اساساً این را می گوید که حتی اگر به یک پورت plug کنید، تا زمانی که ثابت نکنید چه کسی هستید و آیا مجاز به اتصال به شبکه هستید یا خیر، اجازه دسترسی به ساختار سوئیچ لایه ۲ را ندارید.اگر چه سازمانهای متعددی امنیت شبکه بی سیم مبتنی بر 802.1x را پیاده سازی کرده اند، بسیاری از آنها نسخه کابلی 802.1x را پیاده نکرده اند.

ویندوز XP تنظیمات 802.1x شبکه بی سیم را به صورت خودکار اجرا کرده ولی تنظیمات 802.1x شبکه کابلی را خیر. به همین خاطر بهتر است سیستم عامل خود را به ویستا یا 7 که تنظیمات 802.1x کابلی و بی سیم را به طور خودکار اجرا می کنند، تغییر دهید.

علاوه بر امکانات اضافه شده 802.1x، ویستا و 7 یک کلاینت NAP (Network Access Protection) که نسخه مایکروسافتی استاندارد NAC (Network Access Control) است را نیز اضافه نموده اند. NAP یا NAC مفهوم امنیت مبتنی بر پورت 802.1x را گرفته و پا را فراتر گذاشته و نه تنها قبل از اجازه به کلاینت برای ورود به شبکه، عملیات Authentication و Authorization را انجام می دهند، بلکه سلامت کلاینت را نیز بررسی می کنند.

اگر یک کلاینت بتواند ثابت کند که کیست و آیا مجاز است یا خیر، او هنوز باید موضوع دیگری را هم اثبات کند و آن اینست که آیا سالم است یا خیر؟

کنترل سلامت شبکه (NAC health) معمولا به عنوان یک وصله (patch) تمام و کمال برای لغزشهای امنیتی تعریف شده که علاوه بر اینکه یک فایروال مناسب مبتنی بر میزبان است، یک آنتی ویروس بروزرسانی شده نیز می باشد.

اگر یک کلاینت مجاز از تست سلامت مردود شود، در یک قرنطینه در درون شبکه ایزوله قرار می گیرد، تا زمانی که بتواند مجدداً با آپدیت های مناسب، متقاضی ورود به شبکه اصلی شود.

شبکه ایده آل امروزی شبکه ای است که تمامی فرایندهای قفل کردن و محدودسازی که در این مقاله توضیح داده شد را پیاده سازی کرده باشد.

شبکه ایده آل فردا تمامی ویژگی های این مقاله به علاوه NAP و NAC را پیاده سازی خواهد کرد.