SUNETS TEKNISKA

TREF

REFERENSGRUPP

RAPPORT

från LAN-gruppens studieresa 2006

1 INLEDNING

Under juni 2006 besökte LAN-gruppen inom SUNETs tekniska referensgrupp fem nätverksföretag för att diskutera tekniker, standarder och produkter inom LAN-området under de kommande två till tre åren. Denna rapport sammanfattar intrycken från besöken och ytterligare undersökningar efter resan.

Detta år bestod LAN-gruppen av Per Andersson (Chalmers tekniska högskola), Kent Engström (Linköpings universitet), Conny Ohlsson (Högskolan i Kalmar) och Björn Rhoads (KTHNOC). Vi besökte följande företag i Bay Area och Sacramento:

- Juniper Networks
- Cisco Systems
- HP ProCurve Networking
- Extreme Networks
- Force10 Networks

Vi besökte också Stanford University i Palo Alto samt UCSD, SDSC och CAIDA i San Diego för att få perspektiv från fler håll än bara tillverkarna.

I november 2000 och februari 2003 gjorde tidigare LAN-grupper liknande resor.

Se http://proj.sunet.se/lanng/ för mer information om dessa.

2 ETHERNET

Vi ville diskutera den utveckling som är på gång inom Ethernet-standarderna. De frågor vi var beredda med var främst angående 10 Gbit/s på koppar och högre hastigheter än 10 Gbit/s, men det visade sig att det även pågår mycket annan utveckling inom detta område.

2.1 10 Gbit/s på koppar

När det gäller 10 GBit/s på koppar är standarden 10GBASE-T/802.3an nyligen fastställd och publicerad. 10 Gbit/s börjar närma sig gränsen för vad kabelsystemen klarar av. Det gör att det förutom höga krav på kabelsystemen också krävs avancerad kodning och en avancerad mottagare. Hastigheten uppnås genom att samtidigt sända 2500 Mbit/s i varje riktning över alla fyra paren (800 Msymboler/s med 3,125 informationsbitar per symbol via PAM16 kodning).

En ny parameter som börjar bli viktig i kabelsystemen är alien crosstalk, det vill säga överhörning mellan olika kablar (inte överhörning mellan olika par i en kabel). Målet att nå 100 meter klaras antingen med kabel av klass F (Cat 7) eller klass EA (Cat 6_A). Med befintlig kabel av klass E (Cat 6) skall man klara 55 till 100 meter. För att klara 100 meter kan det dock vara nödvändigt att sätta in speciella åtgärder för att minska alien crosstalk.

Ett annat problem är den höga effektförbrukningen: en port förbrukar i storleksordningen 5-10 W, vilket begränsar hur tätt man kan packa porterna i switcharna. För att minska problemet finns dock en short reach-variant av standarden, som klarar max 30 meter på kabel av klass F (Cat 7) eller klass EA (Cat 6_A). Effektförbrukningen kan då hållas nere och portarna packas tätare.

Patchpaneler kan bli problematiska när marginalerna för kabelstandarderna krymper. De kan behöva ersättas av switchar närmare servrarna än vad vi är vana vid idag. Det verkar inte finnas några färdiga produkter ännu. De väntas tidigast under 2007.

2.2 Bortom 10 Gbit/s

Vi var också intresserade av att höra hur det går med hastigheter högre än 10 Gbit/s som idag är den högsta standardiserade hastigheten för Ethernet. Det har inom IEEE 802.3 i somras startats en Higher Speed Study Group. Detta innebär att målen för ett eventuellt standardiseringsarbete ännu inte är klara utan skall tas fram av denna grupp.

Det intryck vi fick vid de besök vi gjorde var att man avser att ta ett tiofaldigt steg, precis som det tidigare gjorts inom Ethernetsammanhang. Det innebär att det är 100 Gbit/s som kommer att bli målet, inte 40 Gbit/s som det spekulerats om tidigare. Då själva standardiseringsarbetet inte är påbörjat och det inte heller finns andra standarder att låna teknik från, kommer det att dröja minst 3-4 år innan standarden kan vara fastställd.

2.3 Annan utveckling

Det sker även en hel del annan utveckling inom Ethernetområdet förutom högre hastigheter. En del standarder är klara eller nästan klara medan andra är i tidigare faser. Vi tar här med både IEEE 802.1 och IEEE 802.3 och listar de olika standardgrupperna uppdelade på ett antal områden.

Utökningar riktade mot operatörer

Dessa utökningar består i ökad funktionalitet för felsökning och övervakning för att kunna få den nivå som teleoperatörer är vana vid från exempelvis SDH. Det finns även funktioner för att kunna transportera hela VLAN-trunkar igenom sitt nät (så att både du som operatör och kunden kan använda VLAN på Ethernetnivå), möjligheter till trafikplanering samt möjlighet att effektivt använda Ethernet ända fram till kunden.

De delar som är intressantast för oss är förmodligen felsökning och övervakning. ”Connectivity Fault Management” innehåller bland annat ping- och traceroute-liknande funktioner på Ethernetnivån.

- Connectivity Fault Management (802.1ag)
- Provider Bridges (802.1ad)
- Provider Backbone Bridges (802.1ah)
- Two-port MAC Relay (802.1aj)
- Ethernet in the First Mile (802.3ah)

Säkerhet

Arbetet här består dels av möjlighet att kryptera trafik (hop-by-hop) och tillhörande nyckelhantering, dels av möjligheten att säkert identifiera enheter som kopplas ihop.

Den första delen (802.1ae + 802.1af) ger möjlighet att kryptera trafiken på en enskild länk, tex mellan två switchar. Ett tänkbart användningsområde är att skydda sin trafik som går över en hyrd svartfiberförbindelse.

Den andra delen (802.1ar) ger möjlighet för nätverksutrustningar att säkert autentisera varandra för att säkra själva infrastrukturen.

- Media Access Control (MAC) Security (802.1ae)
- Media Access Control (MAC) Key Security (802.1af)
- Secure Device Identity (802.1ar)

Audio/Video

Inom 802.1 finns det en grupp ”Audio/Video Bridging Task Group” som arbetar för möjligheten att använda Ethernet för alla möjliga former av mediadistribution. Det är en hel uppsjö olika användningsområden man ser framför sig: tjänster som IP-TV, ljud och bild inom hemmet (till exempel Ethernet från ljudkällor till högtalarna), transport av USB-dataströmmar men även mera professionell användning i studios.

De standarder som det arbetas med är dels möjligheten att få synkronisering för tidskänsliga dataströmmar, som behövs för att få synkronisering mellan ljud och bild, och dels möjligheten att reservera bandbredd för dataströmmarna.

- Timing and Synchronization (802.1as)
- Stream Reservation Protocol (802.1at)

Ersättare för Spanning Tree

Det pågår arbete med att ta fram ett nytt protokoll som skulle kunna ersätta spanning-tree protokollet, ”Shortest Path Bridging”. Man tänker sig att använda ett link-state-protokoll som normalt används för routing (till exempel IS-IS) för detta.

- Shortest Path Bridging (802.1aq)

Större paket

Det finns ett förslag på större ramstorlek, fast då bara till cirka 2000 bytes för att få plats med mer headrar för alla andra nya standarder. Att formellt inom IEEE standardisera en ökning av datadelens storlek (*jumbo frames)*, verkar inte vara aktuellt.

- Frame Expansion (802.3as)

Power over Ethernet

Här handlar det om en utökning av 802.3af (Power over Ethernet) för att kunna leverera högre effekt, i första hand upp till 30W. Detta behövs till exempel för att driva accesspunkter med flera radiodelar (A/B/G) och övervakningskameror med zoom/pan.

Det var även tal om att gå upp till ännu högre effekter (60W), för att exempelvis kunna driva och ladda laptops. Detta ligger dock längre in i framtiden och det är också oklart om det är praktiskt och ekonomiskt genomförbart.

- DTE Power Enhancements (802.3at)

Flödeskontroll

Detta handlar om att införa mer avancerad flödeskontroll på Ethernetnivån. Tanken är att switchar ska kunna tala om för enskilda sändare att de ska minska hastigheten, istället för att bara kunna be den närmaste switchen att hålla tyst ett tag.

Med bättre flödeskontroll skulle Ethernet kunna erbjuda lägre fördröjningar, mindre variationer på fördröjningen och färre tappade ramar. Detta är intressant för de tillverkare som vill sälja Ethernet-teknik som ersättare för till exempel Fibre Channel och Infiniband inom SAN-världen, beräkningskluster med mera.

- Congestion Management (802.3ar)
- Congestion Notification (802.1au)

Övrigt

1 Gbit/s och 10 Gbit/s på mönsterkort, upp till 1 m, till exempel för användning i blade-servers.

- Backplane Ethernet (802.3ap)

3 WLAN

För att par år sedan var den typiska accesspunkten en fristående enhet som fungerade utan yttre stöd. Man kunde dock ha system för att underlätta konfigurering och övervakning ifall man hade många accesspunkter att sköta.

Sedan började det dyka upp produkter där all funktionalitet inte låg i en fristående accesspunkt; den delades mellan en "lättviktsaccesspunkt" och en kontrollutrustning. Detta gav lägre kostnader eftersom accesspunkterna kunde vara enklare. Samtidigt kunde man införa funktioner för att samordna nätet när en kontrollutrustning hade hand om flera accesspunkter.

Denna utveckling har fortsatt. Idag är det i princip enbart centralstyrda lösningar som leverantörerna vill sälja till oss. Fokuset är främst på att detta ger möjligheter till enklare administration och bättre funktionalitet (samordning av kanaler/uteffekter, upptäckt av främmande accesspunkter, positionering med mera) och inte lika mycket på att själva accesspunktshårdvaran ska prispressas.

3.2 IP-telefoni över WLAN

Om vi ska köra IP-telefoni över WLAN ställer det särskilda krav. En viktig sak att tänka på är att det bara får plats ett begränsat antal telefoner per accesspunkt (från cirka tio med normal 802.11b-utrustning till cirka 30 med särskilt anpassade accesspunkter). Om för många telefoner används samtidigt i samma "cell" blir alla samtal lidande. Utrustningen (telefoner och accesspunkter) behöver också stöd för att prioritera telefonitrafiken framför annan trafik. Här ser Spectralink Voice Priority ut att vara en defacto-standard.

4 IPv6

IPv6 har ännu inte slagit igenom på bred front. Eftersom det är ett nytt nätnivå-protokoll och inte något som användaren ser direkt själv på tillämpningsnivån så kommer införandet av IPv6 att ske i bakgrunden, och om det görs rätt så kommer datoranvändare inte märka att protokollet som skickar deras paket ändras. Att införa IPv6 innebär ju för de flesta "vanliga datorer" att man lägger till ett nätnivå-protokoll utöver IPv4 och att detta används när det är möjligt.

Man kan göra försök att ta reda på när IPv4-adresserna definitivt tar slut genom att kurvanpassa dagens förbrukning och se när alla regionala IP-registries (ARIN, RIPE, med flera) inte har några adresser kvar att dela ut. Tony Hain på Cisco gör en sådan prognos med jämna mellanrum. Hans september-version förutspår att adresserna tar slut 2010. Den prognosen förutsätter att allokeringstakten fortsätter att öka som hittills. Om ökningen skulle upphöra (vilket inte anses troligt) blir slutdatumet någonstans vid år 2014.

IPv6 kommer med all sannolikhet att användas mera allmänt innan den utrustning som köps idag är utsliten. Moderna routrar och switchar har nästan alltid hårdvarustöd för IPv6 och IPv4, men än så länge är inte hårdvarustödet för att skicka paket över IPv4 och IPv6 helt likvärdigt. Om man ska köpa in hårdvara så behöver man fortfarande verifiera att det man vill köpa fungerar lika bra på IPv6 som IPv4. Högpresterande routrar och swichar har oftast samma prestanda för båda protokollen, men ju längre ut mot kanten man kommer i sitt nät ju mindre sannolikt är det att man kan förutsätta samma prestanda för IPv6 som IPv4.
När det gäller övervakning och styrning av utrustning så kan man tyvärr än så länge endast förutsätta att IPv4 är det protokoll som fungerar. Behöver man IPv6-funktionalitet här måste man kontrollera detta noga.

5 NÄTVERKS-ÅTKOMSTKONTROLL

Företagen vi besökte var alla intresserade av att diskutera säkerhet och de produkter och visioner de hade inom dessa områden. Nätverksåtkomstkontroll *(network admission control, network access control)* var ett av de hetaste områdena. Vissa aktörer har fristående produkter för nätverksåtkomstkontroll idag, medan andra har arkitekturer som ska lösa det mesta framöver när alla byggblocken är på plats.

5.1 Vad försöker nätverksåtkomstkontroll lösa?

Våra traditionella lokala nätverk är väldigt godtrogna. Om man kan koppla in en TP-sladd i rätt uttag, så anses man behörig att komma åt det nätverk som finns i switch-porten på andra sidan sladden. Det finns självklart en rad problem med denna naiva inställning. Alla nätverksuttag och sladdar sitter till exempel inte fysiskt skyddade i miljöer där bara betrodda användare kan koppla in sig.

Autentisering

När det handlar om anslutningar utifrån så har vi löst problemen genom att autentisera användare med lösenord eller ännu starkare metoder (dosor med mera) i samband med modempooler och VPN-anslutningar, men vi har länge saknat bra möjligheter att göra samma sak på våra lokala nätverk. Det bästa som varit tillgängligt länge är att styra VLAN-placering med hjälp av MAC-adress.

I samband med WLAN har problemet blivit ännu akutare. Där har möjligheten att kryptera trafiken erbjudit en möjlighet att hålla obehöriga ute. För att ge en viss åtkomstkontroll i samband med WLAN och nätverksuttag i öppna miljöer är också så kallade *captive portals* populära. Användaren måste logga in för att komma utanför det närmaste lokala nätet. Det är dock inte vanligt att ha denna teknik för samtliga datorer på nätet.

Standarden 802.1X ger en möjlighet att börja kontrollera nätverksåtkomsten för varje enhet ansluten till switchar och WLAN. Datorn och/eller användaren autentiseras via användarnamn/lösenord, certifikat eller någon annan autentiseringsteknik. Den autentiseringsserver som nätverksutrustningen pratar med avgör om enheten ska få tillträde till nätet och kan också till exempel ange vilket VLAN enheten ska hamna på.

Trots fördelarna med 802.1X har införandet av tekniken gått långsamt på många håll. När man börjar se till detaljerna så finns det en rad inkompatibiliteter och strul som gör verkligheten jobbigare än önskedrömmen, i alla fall om IT-miljön inte är en någorlunda ny, homogen Microsoft-miljö.

Datorkontroll

Att bara fokusera på om användaren är behörig når i alla fall inte ända fram. Även om användaren är behörig att komma åt nätet, så är det inte säkert att hans eller hennes dator är välkommen om den är infekterad med elak kod, saknar antivirus-program eller är osäker för att den saknar väsentliga patchar.

Vi skulle alltså vilja verifiera att datorn är OK innan vi släpper in den på nätet. Det är detta som lösningarna för nätverksåtkomstkontroll gör. De flesta lösningarna kombinerar detta med att också autentisera användarens (och/eller datorns) identitet.

5.2 Fristående produkter kontra arkitekturer

En grundläggande skiljelinje går än så länge mellan det vi i denna rapport har valt att kalla fristående produkter och det som vi kallar arkitekturer.

Fristående produkter

Detta är lösningar som man kan köpa idag i form av en eller flera "burkar", koppla in på nätet och ha en fungerande lösning för nätverksåtkomstkontroll om ens nät och datorer uppfyller kraven som lösningen ställer.

Dessa lösningar passar miljöer där IT-driften inte är helt centraliserad och man måste ta ett visst ansvar för säkerheten även på "okända" datorer.

Exempel i denna kategori är:

- Extreme Networks Sentriant AG
- Cisco NAC Appliance (även känd som Cisco Clean Access)
- Juniper Unified Access Control

Vi förväntar oss att de som idag leverar fristående produkter har en plan för hur dessa i framtiden ska passa ihop med arkitekturerna.

Arkitekturer

Här handlar det inte så mycket om enskilda "burkar" att köpa nu. Fokus ligger istället på protokoll och funktioner som byggs in i operativsystem och nätverksutrustning på längre sikt. Arkitekturerna ska också göra det möjligt för olika företag att leverera olika delar av lösningen.

Lösningar baserade på arkitekturna kommer från början att passa bäst i en miljö med centraliserad IT-drift, där "okända" datorer antingen ska nekas åtkomst helt eller förpassas till ett gästnät där ingen centralt ansvarar för dem.

Det finns tre arkitekturer:

- Network Admission Control (NAC) Framework från Cisco
- Network Access Protection (NAP) från Microsoft
- Trusted Network Connect (TNC) från Trusted Computing Group

5.3 Vilka delar består en lösning för nätverksåtkomstkontroll av?

När man studerar de olika lösningarna för nätverksåtkomstkontroll så finner man vissa gemensamma saker som de alla "handlar om", oavsett om det rör sig om fristående produkter eller lösningar baserade på arkitekturerna:

Dator som vill komma åt nätet

Till syvende och sidst handlar nätverksåtkomstkontroll om att kontrollera datorerna som vill komma åt nätet innan man släpper in dem. För att kunna kontrollera saker som inte är åtkomliga utifrån kräver lösningarna stöd av programvara (ofta kallad *agent*) på datorn som vill bli insläppt. För att göra det smidigare erbjuder vissa system nedladdning av agenten till den dator som saknar det (till exempel som MSI-paket, ActiveX-kontroll eller Java-applet). Det varierar mellan lösningarna vilka operativsystem det finns agenter för.

Hur hanteras då en dator som saknar agent? Kan man skilja en Linux-dator som saknar agent från en Windows-dator där användaren låtit bli att installera agenten? Lösningarna skiljer sig åt här. Vissa av lösningarna har möjligheten att via OS-detektion och portscanning utifrån åtminstone gissa operativsystem och undersöka förekomsten av "farliga portar" när agent saknas. Andra lösningar hänvisar direkt till "nödlösningar" med undantagslistor för IP-adresser, MAC-adresser, CDP-information med mera.

I arkitekturerna kan andra än agent-leverantören lägga till funktionalitet. Tillverkaren av ett antivirus-program kan till exempel skapa en agent-plugin som kontrollerar status för antivirus-progammet (Är det installerat? Körs det? Vilken version av virusdefinitionerna finns? osv.) Arkitekturerna definierar därför API mellan agent och agent-plugins.

Utrustning som kontrollerar åtkomst till nätet

Lösningarna måste ha möjlighet att upptäcka nya datorer på nätet. När de sedan kontrollerat datorn måste de också ha möjlighet att styra nåtåtkomsten baserat på resultatet av kontrollen. Godkända datorer ska tillåtas komma åt det interna nätet, underkända datorer ska komma åt de resurser som behövs för att bli godkända igen, gäster ska inte komma åt det interna nätet, osv.

Enklare lösningar kan låta en utrustning sitta mellan det skyddade nätet och resten av nätet. På så sätt kan nya datorer upptäckas (genom flödeskontroll, DHCP-sniffning, ARP-sniffning osv). Utrustningen kan också med filterlistor, ARP-förgiftning, URL-omdirigering med mera stoppa trafik från datorer som ska begränsas.

Mer avancerade lösning tar hjälp av switcharna i nätet för detektering och/eller begränsning. Exempelvis kan oanvända uttag placerat på ett VLAN som lösningen övervakar. När en dator upptäckts, testats och funnits vara

OK, kan den placeras på ett VLAN för godkända datorer, så att all trafik nu inte måste passera den särskilda åtkomstkontrollutrustningen.

Arkitekturerna använder 802.1X (eller besläktade EAP-över-UDP i vissa fall för Cisco NAC) för att få switchar och accesspunkter att detektera och styra nätåtkomsten på Ethernet och WLAN.

System som bestämmer om åtkomst får ske

Spindeln i nätet är en eller flera servrar som bestämmer om en dator ska godkännas på nätet eller ej. I enklare lösningar kan detta vara samma burk som också detekterar och filtrerar trafiken. I mera avancerade lösningar är detta en separat burk.

Arkitekturerna har 802.1X eller EAP-över-UDP i bottnen. Det innebär att switchar och accesspunkter behöver prata RADIUS med en access-server för att kontrollera om en dator ska släppas in eller inte. Denna access-server blir i arkitekturerna centralpunkten där beslut tas om nätåtkomst baserat inte bara på autentiseringen, utan också på resultatet av datorkontrollen.

Arkitekturerna har också stöd för att låta externa moduler kontrollera det data som kommer från agent-plugins. I exemplet med antivirus-företaget, så skapar de inte bara en agent-plugin, utan också en motsvarande modul som access-servern kan använda för att kontrollera om svaren innebär att datorn är OK. Exempelvis kan versionen på virusdefinitionerna enligt agent-pluginen jämföras med senaste tillgängliga. Arkitekturerna definierar här API eller protokoll för kopplingen mellan access-servern och kontrollmodulerna.

System för extern kontroll

Data från agenterna kan som beskrivits ovan kompletteras med kontroll av datorn utifrån. I vissa av lösningarna ingår stöd för till exempel OS-detektion och portscanning i själva lösningen från början. Cisco NAC Framework definierar istället ett protokoll (GAME) som gör det möjligt att koppla in system för kontroll (*audit*) i ramverket.

System för åtgärdande

Någon form av stöd för åtgärdande *(remediation)* av de problem som upptäckts ingår i lösningarna. Exempel:

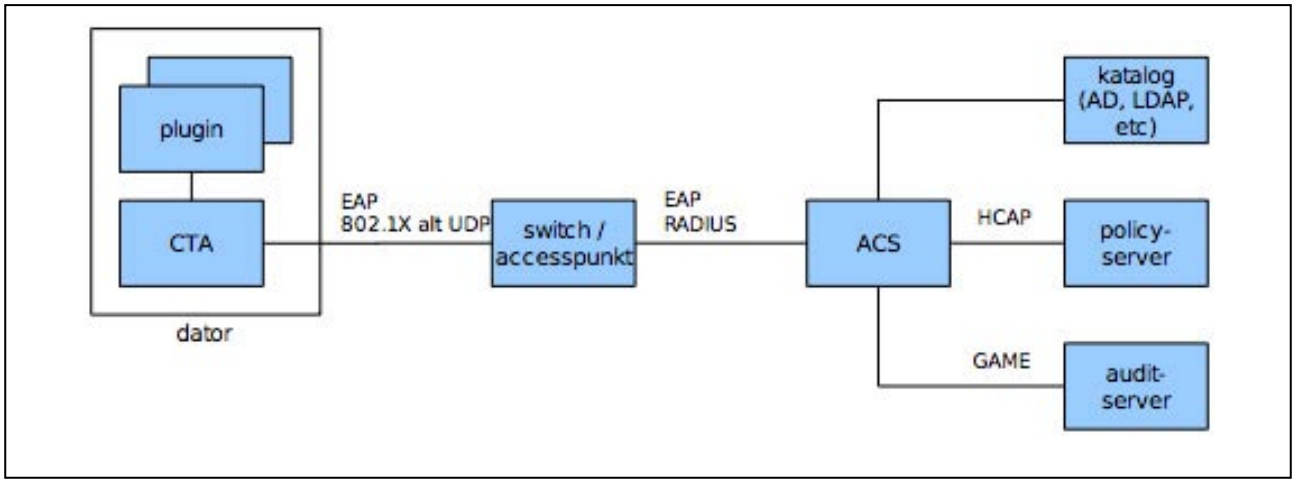
- Användaren får ett meddelande om vad som behöver göras.
- En webbläsare startas på användarens dator och pekar på rätt URL.
- Automatisk uppdatering av virusdefinitioner inleds via agent-plugin för antivirus-programmet.
- Datorn tas omhand av ett existerande system för patch-distribution som integrerats med nätverksåtkomstsystemet.

Under tiden som åtgärdandet pågår måste datorn ha så mycket nätkontakt att den kan komma åt de resurser som behövs.

5.4 De tre arkitekturerna

Network Admission Control (NAC) Framework från Cisco

NAC är Ciscos arkitektur för nätåtkomst-kontroll. Cisco har kontrollen över protokoll och APIer, men samarbetar med ett stort antal partners.



Datorer som ska komma åt nätet kör agentprogramvaran *Cisco Trust Agent*. För närvarande finns agenten till Windows (NT 4.0, 2000, XP, 2003) och Linux (RedHat Enterprise 3.x och 4.0). Det finns också möjlighet att använda 802.1X-supplikanter som utökats med NAC-stöd.

För att kontrollera antivirus, personlig brandvägg med mera behövs agent-plugins från respektive leverantör.

NAC kräver i praktiken att nätverksutrustningen (switchar, routrar och/eller accesspunkter) som ska kontrollera åtkomsten till nätet kommer från Cisco och har en tillräckligt sen mjukvaruversion.

Spindeln i nätet som kontrollerar åtkomsten är Cisco Secure Access Control Server (ACS), Ciscos RADIUS-server som har utökats för sin nya roll i NAC. Cisco har definierat protokollet HCAP för kommunikationen mellan ACS och moduler från tillverkare som kontrollerar sin del av datorns tillstånd. Man har också definierat protokollet GAME för att kunna prata med tredjepartslösningar för kontroll av datorer som saknar agent. Bilden kompliceras en aning av att NAC finns i tre "smaker" med variande stöd på olika nätverksutrustningar:

- NAC-L3-IP innebär att åtkomstkontroll hanteras av en router eller VPN-koncentrator när den ser trafik som indikerar att en ny dator har dykt upp. Kommunikationen mellan routern och agenten sker med EAP-över-UDP (som Cisco uppfunnit). Åtkomstbeslutet baseras bara på datorkontrollen och inte på något autentisering av dator eller användare. Begränsning av trafik för "underkända" sker genom nedladdning av accesslista för IP-adressen.
- NAC-L2-IP innebär att åtkomstkontroll hanteras av en switch när den ser ARP- eller DHCP-frågor på porten. Även här används EAP-över-UDP, åtkomstkontrollen tar inte hänsyn till autentisering av dator eller användare och trafikbegränsningen sker med en accesslista som appliceras på porten.
- NAC-L2-802.1X innebär att 802.1X används, tillsammans med "vanliga" EAPoLAN för kommunikationen mellan switchen och agenten. Åtkomstbeslutet tar också hänsyn till autentisering av dator och/eller användare.Begränsning av trafik sker genom placering på rätt VLAN

Läs mer på http://www.cisco.com/go/nac/

Network Access Protection (NAP) från Microsoft

NAP är Microsofts motsvarighet till Cisco NAC Framework. Det server-stöd som behövs kommer i Windows Server "Longhorn" (för närvarande planerad till senare halvan av 2007) och kommer att fungera med klienter som kör Windows Vista eller Windows Server "Longhorn". Microsoft har också lovat klientstöd för Windows XP SP2.

Agenten heter här NAP Agent. Till sin hjälp har den ett antal System Health Agents (SHA) som kontrollerar olika delar av systemets hälsotillstånd. Det finns också en eller flera Enforcement Clients (EC) som har hand om kommunikationen med nätverksutrustningen och servrarna. NAP definierar APIer för kommunikationen med SHA och EC så att andra än Microsoft ska kunna leverera sådana komponenter.

Hjärtat i systemet är Network Policy Server (NPS) på Windows Server "Longhorn". NPS är efterföljaren till IAS. Det handlar alltså om en RADIUS-server, precis som hos Cisco NAC Framework där Cisco Secure ACS har samma roll. På serversidan kan det finnas moduler, System Health Validators (SHV), som var och en kontrollerar hälsouppgifterna från motsvarande SHA på klienten. NAP definierar ett API (istället för ett nätprotokoll som Cisco HCAP) för den kopplingen, men modulerna kan såklart prata ett godtyckligt protokoll mot en extern server om kontrollen ska göras på en annan dator än NPS-servern.

I NAP ingår också begreppet Health Certificate Server (HCS). Agenten kan kontakta HCS, skicka sina hälsouppgifter till den och får ett hälsocertifikat tillbaka (sedan HCS kontrollerat hälsouppgifterna med NPS). Detta kan sedan så länge det är giltigt användas istället för att skicka fullständiga hälsouppgifter.

Dokumentationen talar om fyra olika sätt att begränsa nätåtkomsten i samband med NAP (som var och en hanteras av en egen EC):

- **IPsec**: Godkända datorer kan få ett hälsocertifikat (se ovan). Detta använda ihop med IPsec för att kommunicera med andra datorer på nätet. Andra datorer på nätet kräver hälsocertifikat för att prata med en dator, men

undantag för de resurser som också måste vara tillgängliga under testning och vid åtgärdande.

- **802.1X**: Switchar eller accesspunkter med 802.1X-stöd används för att detektera datorer och begränsa åtkomst. Detta är den metod som mest liknar Ciscos NAC-L2-802.1X eller TNC.

- **VPN**: VPN-klienten skickar med hälsoinformation via VPN-servern till NPS vid uppkopplingsförsök. VPN-servern begränsar vid behov klientens kommunikation.

- **DHCP**: DHCP-klienten skickar med hälsoinformation i DHCP Discover-meddelanden. DHCP-servern rådfrågar NPS om klienten är godkänd. Om inte, så skickas en kombination av 255.255.255.255-nätmask och statiska routes som gör att klienten bara får kontakt med de resurser som behövs för åtgärdande.

Microsoft har ett partnerprogram på NAP på liknande sätt som Cisco har för NAC. Av företagen som vi besökte finns Extreme Networks med här, och man var tidiga med att demonstrera interoperatibilitet mellan sina switchar och NAP.

Läs mer på http://www.microsoft.com/nap/

NAC och NAP ihop

I september 2006 meddelade Cisco och Microsoft att man kommer att samarbeta för att se till att NAC och NAP fungerar ihop. Av det whitepaper som publicerades framgår bland annat:

- NAP Agent som kommer att ingå i Windows Vista ska fungera för NAC också, så att Cisco Trust Agent inte behövs där.

- Från början behövs både en Cisco Secure ACS och en Microsoft NPS i en blandad miljö. ACS skickar hälsouppgifterna vidare till NPS för beslut.

- Cisco Secure ACS kommer förstå hälsocertifikat.

Samarbetet är logiskt. Microsoft tar hand om klientsidan. Ingen annan lär ha bättre möjlighet att integrera agenter med Windows än de har. De tar också huvudansvaret för serverdelen av hälsokontrollen. Cisco kan koncentrera sig nätverksutrustningen, deras huvudområde, och NAC-stödet där.

Trusted Network Connect (TNC) från Trusted Computing Group

TNC är ett försök att utveckla öppna protokoll för nätverksåtkomstkontroll inom Trusted Computing Group (TCG). Gruppen, som har en rad företag som medlemmar, är mest känd för sitt försök att standardisera TPM-chip för lagring av nycklar, lösenord, certifikat med mera på moderkortet för att möjliggöra *trusted computing*. Detta är inte helt okontroversiellt, då många befarar att tekniken kan användas av dator- och mjukvarutillverkare för att begränsa vad användare kan göra med sin egen dator.

TNC innehåller i princip samma grundkomponenter som NAC och NAP. Agenten kallas TNC Client och får hjälp av ett antal Integrity Measurement Components (IMC) för att ta reda på datorns hälsotillstånd. Servern kallas TNC Server och tar hjälp av ett antal Integrity Measurement Verifiers (IMV) för att kontrollera uppgifterna från motsvarande IMCer. För kommunikationen mellan klient och IMC samt mellan server och IMV finns APIer specifierade för Windows och Unix.

TNC använder EAP över 802.1X för Ethernet/WLAN eller EAP över IKEv2 för VPN.

En rad företag deltar i arbetet med TNC, till exempel Juniper, Extreme, IBM, Symantec och Nortel. Den kritiska frågan är om TNC kommer att fungera i praktiken och stödjas av tillräckligt många leverantörer så att det kan bli ett realistiskt alternativ till NAC och NAP som Cisco och Microsoft nu kan marknadsföra tillsammans. Cisco har hela tiden visat litet intresse för TNC. Microsoft är däremot medlemmar i TCG och har tidigare pratat om att införa TNC-stöd i Windows.

Läs mer på https://www.trustedcomputinggroup.org/groups/network/

IETF Network Endpoint Assessment (NEA)

IETF är engagerade i nätverksåtkomstkontroll genom Network Endpoint Assessment (NEA). Målet är inte att hitta på en fjärde arkitektur. Istället vill man identifiera likheter mellan arkitekturerna och försöka hitta protokoll som kan standardiseras för att möjliggöra interoperatibilitet mellan arkitekturerna.

5.5 Problem och begränsningar

Nätverksåtkomstkontroll löser givetvis inte alla säkerhetsproblem på våra nätverk. Bland begränsningarna finns bland annat:

- Lösningarna inriktar sig i första hand på att hjälpa välvilligt inställda (men kanske okunniga) användare att uppfylla de säkerhetskrav som vi ställer på datorer som ska in på nätet. Användare som anstränger sig för att kringgå kontrollerna kan få in en osäker dator på nätet.

- Lösningarna är inte fokuserade på att kontrollera vad datorn gör när den väl godkänts på nätet. I framtiden kommer vi kanske se mer integrering med "reaktiva" system för den delen.

- Det varierar huruvida lösningarna bara kontrollerar datorns hälsotillstånd, eller också innefattar autentisering av användaren och/eller datorn. Om det senare saknas så skyddar systemet inte mot elaka obehöriga användare med korrekt uppsäkrade datorer.

- De svagare formerna av system för att begränsa åtkomsten för datorer som inte uppfyller kraven kan vara lätta att kringå, till exempel genom att sätta adressen manuellt om spärren består av en DHCP-server som vägrar dela ut riktiga adresser till underkända datorer eller genom att använda en annan dators IP-adress om spärren består av filter på IP-adressnivå. Till viss del kan dessa metoder "stärkas" genom att man använder switch-finesser som DHCP- och ARP-snooping.

- Lösningarna är mycket beroende av agenterna för att kunna kontrollera de enheter som vill in på nätet. Här behövs stöd för fler operativsystem, men också stöd för skrivare, IP-telefoner med mera. Detta är särskilt tydligt när autentisering av enheten ingår som en del av lösningen. Om skrivarna t.ex. inte kan "logga in", så måste man med undantagsfunktionerna godkänna allt som ser ut som skrivare, och riskerar då att sänka skyddsnivån.

- Lösningar som klumpar ihop infekterade datorer på ett karantänsnät kan medföra att dessa ännu effektivare "kors-smittar" varandra med olika former av elak kod. Extra illa kan detta bli om oinfekterade datorer med säkerhetshål placeras på samma nät som redan infekterade datorer. Här kan tekniker som "privata VLAN" och liknande användas för att stoppa detta.

Lösningarna ställer krav på nätverksstrukturen som det kan vara värt att fundera på även om man inte planerar att införa nätverksåtkomstkontroll inom en nära framtid:

- Switchar och accesspunkter ska ha stöd för 802.1X (eller Cisco-specifika protokoll som EAP-over-UDP för Cisco NAC) för att man ska kunna använda dem som en del av en lösning framöver.

- Lösningar som bygger på att datorer hamnar i olika VLAN baserat på hälsotillstånd gör att mängden VLAN i nätet ökar. Dessa VLAN måste antingen transporteras över nätet eller routas lokalt.

6 SÄKERHET I ÖVRIGT

6.1 Sniffning, IDS-system och liknande vid höga hastigheter

Det blir svårare att sniffa nätet i realtid med vanliga datorer när de förbindelser som är intressanta att övervaka blir snabbare (10 Gbps och uppåt). Vi blev uppmärksammade på två intressanta spår under våra företagsbesök:

- Force10 Networks har en produkt (P-Series) som använder parallel hårdvara för att implementera regler baserade på IDS-systemet Snort. Den trafik som sorteras ut av hårdvaran kan sedan analyseras vidare i mjukvara på vanligt sätt.
- Extreme Networks CLEAR-Flow-teknik ger möjlighet att i switchen matcha trafik mot olika villkor och att skicka vidare den utvalda delmängden av trafiken till IDS-utrustning.

Cisco erbjuder också lösningar där deras IDS-system körs på ett "blad" i en Catalyst-switch.

6.2 Konsolidering av säkerhetsfunktioner

En trend vi såg hos flera leverantörer var att säkerhetsrelaterade funktioner, som tidigare erbjudits via olika fristående utrustningar, istället kombinerades i "security appliances". De funktioner det gäller kan vara IDS, IPS, brandvägg, VPN, webbproxy med innehållskontroll, med mera.

7 KOMPLEXITET OCH HANDHAVANDE

När vi har pratat med de olika tillverkarna har vi märkt att man har olika inställning till var i nätet som intelligensen ska finnas. De som satsar på större avancerade switchar (till exempel Cisco med Catalyst-serien och Force10 Networks) pratar gärna om funktionalitet på den nivån. Andra (till exempel HP ProCurve) talar hellre om intelligens i switcharna längst ut och en snabb och tillförlitlig men mindre komplicerad kärna.

Force10 Networks, som satsar hårt på stora switchar med många portar, påpekar gärna att om man kan klara sig med färre antal swicthar för en viss mängd portar, så bli komplexiteten mindre och antalet hopkopplingsförbindelser som behövs minskar. Detta reducerar kostnaden.

En genomgående trend är mera modulär programvara på switchar och routrar. Istället för en helt egen monolitisk programvara för allt, så bygger tillverkarna nätverksfunktionerna ovanpå ett kommersiellt realtidsoperativsystem eller ovanpå ett fritt operativsystem (Linux eller någon BSD-variant).

Detta innebär också att det finns större möjligheter för tillverkarna att framöver erbjuda patchar (istället för hela utbytes-versioner) när till exempel kritiska säkerhetshål upptäcks. Hela utrustningen behöver kanske inte heller startas om när en patch appliceras. Om felet till exempel ligger i hanteringen av något protokoll på hög nivå, så kan ju den koden i ett mera modulärt system bytas ut utan att koden som kontrollerar switchmotorn behöver påverkas.

Extreme Networks talade mycket om öppenhet. Man erbjuder ett XML-baserat API för att styra switcharna från annan programvara på mera avancerade sätt än SNMP-skrivning tillåter. Man låter också partners leverera programvara som exekveras på själva switcharna.

8 SLUTORD

Vi vill passa på att tacka de som hjälpt oss med resan och rapporten, framför allt företagen som tagit emot oss och låtit oss träffa insatta och intressanta personer. Vi vill också tacka Börje Josefsson, som planerade en stor del av det praktiska inför resan men sedan inte kunde följa med oss, samt Anders Nilsson på Umeå universitet som hjälpt till med information om nätverksåtkomstkontroll.