Aktivní síťové prvky

Úvod

O: Filipova super otázka. Zaflexil! Ale neudělal dobrý formát, takže vlastně -5 bodů. Sorry jako.

F: Tak pardón, pokusím se polepšit. Jen mi prosím tě neber mých 100+ procent :D

Rozdělení a vlastnosti podle ISO/OSI

Fyzická vrstva

Zařízení na této vrstvě nijak nezasahují do složení dat. Primárně jde o zařízení zesilující nebo kopírující jednotlivé bity.

Linková vrstva

Zařízení na této vrstvě pracují s jednotkou zvanou rámec (frame). Přepínání (switching) probíhá pouze na úrovni LAN, přičemž k adresaci se používá MAC adresa. Tato adresa by měla být pro všechny zařízení na světa unikátní. 24b je přiděleno jednotlivým výrobcům. Ze zbývajících 24b přidělují adresy každému vyrobenému zařízení.

Síťová vrstva

Na síťové vrstvě probíhá směrování mezi jednotlivými sítěmi. K adresování se používá adresa IPv6, nebo IPv4. Ty jsou blíže vysvětleny u otázky 19.

Transportní vrstva

Na této vrstvě se pracuje s TCP a UDP porty. TCP a UDP jsou dva protokoly které značí způsob, jakým by měli jednotlivé koncové body komunikovat. Stavebním kamenem TCP je tzv. Three-way handshake. Stručně řečeno je to procedura, při které se nejdříve naváže spojení, potvrzené oběma stranami. Poté se teprve začínají zasílat další data. U dat se ještě pomocí očíslování kontroluje, zda došli všechny. Pokud ne, žádá se o znovu zaslání.
Výhodou je, že získáme kompletně sestavenou strukturu. Zřejmou nevýhodou je ale prodleva a overhead zvýšený nutnou kontrolou. Typickým příkladem užití je u HTTP a HTTPS.
Oproti tomu UDP data nekontroluje ani nenavazuje spojení. Pokud je tedy nutné ověření chybějících dat, musí se to provést programově na SW úrovni. Sníží se tím zatížení sítě v situacích, kdy je potřeba co nejrychlejší odezva, nebo není potřeba kompletní datová struktura (VoIP, Online hry).

Relační – Aplikační

Tyto vrstvy jsem shrnul do jedné, jelikož nemají dedikovaná zařízení. Starají se o to, jakým způsobem bude vypadat výsledná datová struktura, o jejíž přenos se poté budou starat. Formátuje jednotlivá data a šifruje je.

Aktivní prvky na jednotlivých vrstvách ISO/OSI

Fyzická vrstva

Typickým příkladem fyzické vrstvy je zesilovač. Ten vezme signál příchozí z jedné strany, a odešle ho stranou druhou. Je díky němu možné posílat data na delší vzdálenost, než by tomu bylo pouze s použitím daného kabelu.
Hub je druhým příkladem. Data, která obdrží, rozešle všemi porty. Ačkoliv se dnes již běžně nepoužívá, může být použit k diagnostice sítě (viz. Poslední část dokumentu).

Linková vrstva

Switch je typickým zařízením pracujícím na 2. vrstvě. Switch se používá k propojení většího počtu zařízení ve vnitřní síti. Jeho hlavní předností je poměr cena/port, kdy je za stejnou cenu schopný nabídnout x-krát větší množství portů než router. Jeho funkce je podobná hubu. Dosah obou je v rámci místní sítě. Switch však na rozdíl od hubu rozesílá rámce pouze cílovému bodu.

Síťová vrstva

Zástupce třetí vrstvy je především router. Je to zařízení zprostředkovávající směrování packetů do ostatních sítí. Zvláštní případem je L3 (Layer 3) switch, který v sobě kombinuje funkce L2 switche a routeru.
Je tedy schopen základního směrování. Využíván bývá nejčastěji pro routování v LAN, pokud je potřeba směrovat mezi VLAN. Pro routování v rozsahu WAN je stále lepší router. Oproti L3 Switchi je hlavní nevýhodou routeru zvýšená cena v poměru k počtu portů. Výměnou za to ale dostaneme dodatečné funkcionality, užitečné při směrování po WAN.
Rozdíl ve směrování mezi routerem a L3 switchem spočívá v prostředcích které užívají. Rozhodování routeru probíhá většinou na úrovni softwaru, zatímco u L3 Switche jsou k tomu specializované ASIC procesory. Dostupné cesty jsou zapsány ve směrovací tabulce. O plnění tabulky se stará administrátor buď manuálně, nebo dynamicky pomocí nakonfigurovaného protokolu.

Transportní vrstva

Každá síť může být napadena. K tomu abychom dodali naší síti na bezpečnosti můžeme přidat Firewall. Firewall pracuje na 4. vrstvě a stará se o to, aby do sítě prošla jen specifikovaná data. Firewall vezme port, který je příchozím datům přiřazen. V závislosti na něm rozhodne, zda data pustit. Jako takový jednoduchý firewall může v SW rovině posloužit například ACL, nebo firewall zabudovaný v OS.

Relační – Aplikační

Kromě zařízení, jenž všichni známe, jako je PC, smartphone, televize atp. bych uvedl jedno méně obvyklé. NAS zpřístupňuje naše data na internetu 24/7. Kromě FTP přístupu často nabízí další služby, jako DLNA nebo Apache server. Kromě jejich multifunkčnosti je jejich předností nízká cena a spotřeba. Nevýhodou je jejich výkon, který se bohužel nevyrovná plnohodnotnému serveru. Pro domácí použití je však více než dostatečný.

Principy přepínání a směrování

Přepínání

Přepínání je proces, při kterém jsou posílány rámce po místní síti. Principiálně probíhá zhruba takto. Je vytvořen rámec. Rámec obsahuje počáteční a konečnou adresu. Při příchodu rámce od zatím neznámého počítače si zařízení vytáhne source adresu a vloží ji do tabulky kde si ji i přiřadí k portu ze kterého přišla. V tabulce je pak ještě uložený čas kdy si switch naposledy data obnovil. Pokud po určitý čas nepřijdou od daného zařízení žádná data, záznam si smaže. Ve chvíli, kdy přijdou data pro cíl, který nezná, je pošle všemi porty. Po odpovědi, jestli nějaká přijde, udělá to samé jako při příchodu původního rámce akorát s počítačem, který odpovídá.

Metody pro přeposílání rámců se používají dvě. První z nich je cut-through. Tato metoda vezme rámec, a hned jak zná cílovou MAC ho odešle. Výsledkem je snížená latence výměnou za zvýšené riziko chybovosti způsobené vynecháním kontroly rámce. Opakem je Store-And-Forward. Store-And-Forward počká, než má všechny data, zkontroluje si je a jestli je vše v pořádku a až pak data odešle.

Směrování

Směrování probíhá tímto způsobem. Na zařízení přijde packet. Z toho si zjistí, jaká je cílová IP adresa. Adresu sítě, do které cílová adresa spadá, se pokusí vyhledat ve směrovací tabulce. Pokud záznam najde, pošle ho cestou k němu přiřazenou. V opačném případě data zahodí.

Směrovací algoritmy

Způsoby směrování se dají klasifikovat na několik druhů. Dnes jsou nejvíce používanými izolované a distribuované směrování. V izolovaném směrování routery fungují zcela samostatně. Patří sem například záplavové směrování, jenž rozesílá packety všemi porty kromě příchozího. Kromě toho se dá uvést například tzv. “hot-potato” směrování. To spočívá v tom, že router packet vezme a odešle ho portem s nejkratší frontou. Oproti tomu při distribuovaném směrování směrovače spolupracují. Zařadit se sem dají různé dynamické směrovací protokoly. Variantami jsou distance-vektor (Bellman-Fordův algoritmus), založené na výměně vektorových vzdáleností, a link-state (Dijkstra's algorithm), založené na stavu přenosových cest k sousedům.

Diagnostika sítí

Diagnostika je u sítí stejně jako u jiných částí IT celkem „pain in the ass“. K tomu, aby to tak nebolelo existuje několik nice-to-know funkcí.

Takovou, kterou asi každý zná je ping. Ping slouží ke zjištění dostupnosti jiného počítače. Většina systémů ho má už nějak integrovaný, a pro ty co nemají jistě existují nějaké dodatečné programy. Problém zde může nastat ve chvíli, kdy má cílová adresa zablokovaný port pro ping ve firewallu. V tom případě nedostaneme úplně relevantní data.

Co nám ale pomůže zde je traceroute. Ten zasílá informace o tom, jak daleko data došla. To znamená, že když se data dostanou až k bodu před cílem, a cíl nebude odpovídat, víme že je chyba u něj. Také tak můžeme zjistit, kde v síti nastal výpadek.

Programem, který ne každý zná je Wireshark. Je to program pro Windows, Mac a Linux umožňující prohlédnout všechna data jež přijdou na počítač. Můžeme tak, například za pomoci hubu, sledovat zatížení sítě a dále ho optimalizovat.

Kromě těchto tří věcí existuje několik doporučení. Prvním je kontrola HW. Jedním z nejčastějších důvodů, proč něco nefunguje, bývá špatně zapojený kabel, nebo spálený zdroj a tak podobně. Na zařízeních jsou většinou nějaké kontrolky, signalizující jeho stav. Pokud svítí nějakou jinou barvou, než by měli, je „best-practice“ se podívat do manuálu. Pokud nesvítí, je na čase zařízení vyměnit nebo opravit.
Tento odstavec jsme napsali hlavně pro Kevina, který 5minut řešil proč mu nefunguje router, když ho neměl v zásuvce ☺. Já měl rozbitý kabel a trvalo to jen hodinu, než jsem na to přišel. Also nemažte please firmware ze serveru => s Fílou jsme to otestovali za vás ☺.