Adresování a směrování v síti

Úvod

Otázka byla zpracována Filipem, takže hodně informací je takové „ble ble“. Přepsal jsem to, aby to bylo čitelné – není zač. Tato otázka si hodně bere ze všech síťových, a proto je možné využívat informací z ostatní otázek.

Aktivní síťové prvky (Maturitní otázka 24.)

Hub

Hub je aktivní prvek pracující na 1. vrstvě. Složení dat tedy nijak nemění, ani ho nijak neanalyzuje. Jeho funkce je vzít data a přeposlat je všemi porty kromě příchozího. Dnes se již využívá jen při analýze toku dat na síti.

Switch

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.

Zvláštní případem je L3 (Layer) 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.

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.

Router

Router je zařízení zprostředkovávající směrování packetů do ostatních sítí. Pracuje na 3. síťové vrstvě. Oproti L3 Switchi je jeho hlavní nevýhodou 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.

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, založené na výměně vektorových vzdáleností, a link-state, založené na stavu přenosových cest k sousedům.

Firewall

Každá síť může být napadena. K tomu abychom přidali 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.

Pasivní síťové prvky (Maturitní otázka 25.)

Kroucená dvojlinka

Kroucená dvojlinka (TP – twisted pair) je druh kabeláže, který k přenosu dat po síti používá elektrické signály. Skládá se ze 4 párů drátů, přičemž dráty v páru jsou navzájem obmotané. Díky obmotání se minimalizují hlavní nevýhody přenosu po metalických kabelech jako elektromagnetická interference - takzvané přeslechy, které by jinak mezi páry mohli vznikat. Další nevýhodou je rušení se s okolním prostředím. Během fungování kabelu je totiž do okolí vyzařováno a zároveň je z něj přijímáno elektromagnetické rušení.

Postupem času se stále se zvyšujícím požadavkem na rychlost bylo nutné zvyšovat limity kabelů. Vznikali tak různé kategorie, přičemž každá nová přinesla i zvýšený maximální objem toku dat. V domácnostech dnes nejčastěji nalezneme Cat5e, což je první kabel podporující datový tok 1Gb. Kromě něj se však můžeme občas ještě setkat s kategoriemi Cat5 – 100Mb a Cat6 – stejně jako 5e pro 1Gb.

Koaxiální kabel

Koaxiální kabel je využívaný již hodně dlouhou dobu. Takovým nejběžnějším příkladem využití je u anténní techniky, kde se používá pro vedení signálu ať už do televizoru nebo set-top-boxu. U počítačových síti je nejčastěji využíván pro připojení routeru na WAN síť. Skládá se ze dvou vodičů, které jsou od sebe oddělené nevodivým materiálem. Účelem nevodivé vrstvy je docílení soustřednosti vnějšího a vnitřního vodiče.

Optický kabel

Optický kabel je svazek optických vláken. K přenosu dat využívá světlo. Světlo je po vláknech vysíláno v takovém úhlu, aby došlo k totálnímu lomu. Výhody optických kabelů jsou značné. Hlavní z nich jsou vysoké přenosové rychlosti a dlouhá maximální vzdálenost přenosu. Dále není od věci započítat sem i jiné, na první pohled ne tak patrné výhody. Sem můžeme zařadit například odolnost proti rušení a přeslechům. Riziko odposlechů je zde díky nulovému vyzařování také minimální.

Softwarové prostředky sítí

Operační systém

Operační systém slouží jako rozhraní mezi uživatelem a zařízením. Po zapnutí počítače a provedení POST přebírá řízení chodu zařízení. V počítačových sítích jich máme hned několik. Sahají od systémů pro počítače (Windows, Linux, Mac…) přes servery (Windows, Linux), až po zařízení řídící chod sítě (Cisco IOS, ZyNOS, Linux).

PuTTY

PuTTY je program, který umožňuje využívat SSH, Telnet, a Rlogin, což jsou protokoly určené pro komunikaci. Původně byl jen pro Windows, přičemž teď už je i na Linux a další platformy.

WireShark

WireShark, dříve známý jako Ethereal, umožňuje zkoumat data v počítačové síti. Je možné si v něm prohlédnout všechny packety které na počítač přijdou, a díky tomu analyzovat

probíhající komunikace. Ačkoliv je jeho primární účel víceméně jen diagnostický, může být využit i k ilegálním aktivitám, jako je sledování cizí komunikace.

Apache

Apache je dnes nejběžněji využívaným softwarovým webovým serverem. Má rozsáhlou škálu technologií, které se na něm dají spustit. Lze skrz něj provozovat stránky napsané mimo jiné i v Ruby nebo JS. Zároveň ho lze provozovat na všemožných platformách, ať už na Linuxu, nebo na Windows. Ve Windows je nejběžněji používán skrz program XAMPP, který kromě Apache zvládá i MySQL databázi a další funkce.

Klasifikace sítí

Klasifikace podle dosahu a rozsahu

PAN Personal Area Network

PAN je jedna z nejmenších sítí. Její využití je u malých přenosných přístrojů jako mobilní telefon (smartphone), nebo PDA dříve. Oproti ostatním typům sítí mají obvykle také nižší rychlost. Propojení je realizováno např. přes Bluetooth, nebo IR sdílení.

LAN Local Area Network

LAN sítě jsou v malém rozsahu. Většinou jsou v domácnosti nebo firemní síti v rámci budovy. Dost často se lze také setkat se zvláštním případem LAN, a tím je VLAN. Virtuální LAN umožňuje logické rozdělení LAN sítí jinak než přes fyzickou vrstvu. Jednotlivé VLAN jsou od sebe odděleny a k jejich vzájemné komunikaci je potřeba zařízení 3. vrstvy (router, L3 switch).

MAN Metropolitan Area Network

MAN je síť ve větším rozsahu, než je LAN, ale menším, než je WAN. Typicky se s tímto typem sítě setkáváme u sítí jedné organizace. Bývá to například propojení několika budov organizace v jednom městě.

WAN Wide-area network

Rozlehlým typem sítě WAN. Tento typ sítě pokrývá rozsáhle geografické území (Stát, Kontinent). Často bývá spravován různými poskytovateli telekomunikačních služeb.

GAN Global Area Network

Nejrozsáhlejším typem sítě je GAN, která pokrývá díky použití satelitů celou Zemi. Patří sem například i internet.

Dělení podle postavení zařízení

Client-server

K tomu, aby mohla client-server architektura fungovat, jsou potřeba dva účastníci. Jak už název napovídá, je potřeba klient a server. Při provozu je jeden účastník nadřazen druhému. Klient si vyžádá informace (např. Data webové stránky) a server mu je, pokud k nim má klient oprávnění, pošle. Nejčastějším příkladem je zmíněný webový server nebo herní server, kterému připojení hráči (klienti) posílají data k vyhodnocení a server pošle odpověď s výsledkem vyhodnocených dat.

Peer-to-peer

Peer-to-peer neboli rovný s rovným je síť, ve které mají všichni účastníci stejné postavení. Data mezi sebou si sdílejí klienti navzájem. Jeden klient může vyčlenit část svých prostředků ke sdílení, a další je od něj může využít. Takovým hodně známým případem peer-to-peer připojení je torrent. Klient dá ke sdílení nějaká data. Ze začátku sdílí data sám všem, co si je chtějí stáhnout. Jakmile si je ale stáhne první klient, začne sdílet taky a takhle se to dál postupuje.

Konfigurace sítě

Konfigurace sítě je zdlouhavý proces. Je potřeba ji provést pečlivě a vše naplánovat, jelikož jediný chybný krok může způsobit výpadek spojení v (celé) síti. Každá společnost používá své postupy, které se mohou lišit dokonce i mezi několika jejími zařízeními. Postupy zde uváděné jsou funkční u zařízení Cisco, přičemž principiálně to funguje všude podobně.

Konfigurace základních nastavení

Velká část zařízení má nastavení, která jsou pro všechna stejná. Typickým nastavením každého zařízení připojeného k síti je jeho jméno. Dále bývá dobrým zvykem nastavit přístupové údaje a přístupová práva. Ještě je většinou potřeba nakonfigurovat způsoby připojení, např. SSH nebo Telnet. Samozřejmostí pak musí být zálohování provedené konfigurace, aby se při restartu zařízení nesmazala.

Konfigurace druhé vrstvy

Bezpečnost portů

Jedním z prvních úkonů, který by měl být při konfiguraci 2 vrstvy proveden je bezpečnost portů. Zde máme několik možností toho, jak síť chránit. To nejjednodušší a také nejlepší co můžeme ze začátku udělat je vypnout nepotřebné porty. Dalším základním doporučením bývá nastavit povolené MAC adresy. To, jak se může zařízení jednotlivé se u různých zařízení liší. Cisco zařízení nabízejí 2 možnosti. Nejzákladnější je nastavení povolených adres manuálně. Toto nastavení je nejbezpečnější, ale zároveň nejmíň pohodlné. V případě, kdy se na portu často střídají počítače bývá lepší nastavit dynamické učení se určitého počtu adres. Do doby, než je dovršen tento počet se zařízení naučí každou MAC adresu, jež se na portu objeví. Jakékoli další adresy. Třetí možnost je jen rozšíření té první, a je jí „sticky mac-address“. V tomto módu se zařízení učí MAC adresy stejně jako v dynamickém módu. Rozdíl je v tom, že se takto naučené adresy po restartu nesmažou.

V závislosti na tom pak ještě můžeme říct, co se stane, pokud se na síť pokusí připojit někdo s nepovolenou adresou. Tyto akce pak budou u každého zařízení jiné. U Cisca jsou celkem 3 možnosti. První z nich je protected, která všechny rámce zahodí. Na narušení ovšem nijak neupozorní. Další je restrict mode, ten udělá to samé jako protected, ale že narušení zaloguje. Posledním je shutdown mode, který dělá přesně to, co říká název. Při narušení fyzicky vypne port.

Konfigurace třetí vrstvy

Routovaní

Nejdůležitějším nastavením na 3. vrstvě je společně se správnou konfigurací adresace, nastavení směrování. K tomu, aby router dokázal směrovat packet k destinaci si musí nejdříve naplnit routovací tabulku. Nejzákladnější možností konfigurace je manuální zadání cesty. U Cisca je to přes příkaz „ip route <CÍLOVÁ IP ADRESA> <CÍLOVÁ MASKA> <ADRESA PROTĚJŠÍHO ROZHRANÍ nebo OZNAČENÍ ODCHOZÍ ROZHRANÍ>“. Pro výkon sítě je nejlepší varianta zadání jak adresy protějšího rozhraní, tak označení odchozího rozhraní. Tímto způsobem se také konfiguruje defaultní cesta, která slouží pro všechny packety s neznámou cílovou adresou. Výhodou je snížený dopad na výkon sítě, jelikož router nemusí hledat v routovací tabulce dvakrát.

Častěji se však setkáme s naplněním přes směrovací protokoly. Ačkoliv je jich hodně, konfigurace všech probíhá v principu stejně. To, co se nějakým způsobem konfiguruje u všech protokolů jsou sítě, které a přes které chceme sdílet. Dále bývá možnost nastavit pasivní rozhraní, což je rozhraní, přes které nejsou zasílané aktualizace tabulek. Je vhodné takto nastavit porty, které směřují ven na internet, nebo dovnitř do sítě bez dalších routerů. Důležité bývá také určit, zda chceme, aby router odesílal statické a defaultní adresy. U některých protokolů (RIP, EIGRP) zda chceme, nebo nechceme adresy automaticky sumarizovat (převést classless na classful).

RIP Routing Information Protocol

Nejstarší směrovací protokol, avšak pořád použitelný v menších sítích kvůli své jednoduché konfiguraci. Typově je distance vektor a používá speciální algoritmus pro určení nejkratší cesty k síti. Používá hop-count (počet přeskoků) jako ochranu proti smyčkám na síti (max 15 hopů). Každý router vysílá aktualizované směrové tabulky každých 30 s. Zaostává za ostatními směrovacími protokoly, kvůli pomalému zjišťování informací a rozšiřitelností. Jsou 2 verze RIP(v1/v2).
První verze je pouze classful, takže používá základní třídy jako A/B/C, takže nemůžeme mít podsítě.
Druhá verzi už je classless, ale je i zpětně kompatibilní na classful. Vysílá celou tabulku všem ostatním pomocí multicastu.
RIPng je rozšíření pro IPv6.

OSPF Open Shortest Path First

Směrovací protokol fungující na link-state (každý směrovač zná strukturu celé sítě). Je beztřídní, nepodporuje sumarizaci. Činnost OSPF je rozdělena do tří částí – správa sousedských relací, šíření směrovacích informací a určování nejkratších (optimálních) cest. OSPF bylo vytvořeno k vybrání nejkratší cesty, aby byla vypočítaná s ohledem na rychlost, zpoždění a load. Jsou tři verze.

EIGRP

Protokol, který byl navržen společností Cisco. EIGRP posílá pouze přírůstkové aktualizace, což snižuje zátěž zařízení a množství dat, které musí být předány. Téměř všechny routery obsahují směrovací tabulku, která obsahuje pravidla, podle kterých se směruje provoz v síti. V případě, že cesta k cíli není platná, provoz se ukončí.

Adresace

Nastavení IP adresy bývá nejčastěji provedeno přes DHCP. K tomu, aby bylo možné počítači adresu přidělit, je potřeba nastavit DHCP server. Nastavení serveru se skládá z tzv. poolů. Každý pool je jedna síť, pro kterou má být přidělitelná adresa. Obsahuje IP adresu sítě, masku sítě, DNS server a výchozí bránu. Počet poolů, které lze nastavit je závislý na zařízení. Zároveň by se měly ještě nastavit adresy, které chceme z přidělovacího procesu vynechat. Konfigurace klienta se také liší závisle na zařízení. Principiálně je to ale vždy jen o tom povolit přidělení adresy pomocí DHCP.

U zařízení, ke kterým klienti ze sítě přistupují (FTP server, tiskárny) bývá lepší nastavit adresu staticky. Stejně jako u DHCP se konfigurace liší zařízení od zařízení. V principu jde ale jen o to všechny části adresace na rozhraní „naťukat“ ručně.

Access list

Access list je jakýsi filtr určující povolený provoz. Funkce access listu vypadá asi takto. Na rozhraní přijde packet. V případě že je k rozhraní připojen ACL si zařízení zjistí, zda se nějaký záznam shoduje s daty uváděnými v packetu. Cisco zařízení čtou data shora. První záznam, který najdou, považují za platný.

Ke správné konfiguraci je potřeba vědět, jak funguje tzv. wildcard maska. Ta funguje přesně naopak od masky síťové. Na místech, kde je v masce nula se bity musí shodovat. Tam kde je jednička na hodnotě bitů nezáleží.

NAT

NAT je technologie která slouží pro převod interní adresy na veřejnou. Jsou tři druhy, statický, dynamický a PAT, přičemž PAT je spíše otázkou 4. vrstvy. Konfigurace se může u různých systému více či méně lišit. Zde je bude uveden postup u zařízení Cisco. Všechny tři typy mají část konfigurace společnou. Zásadní částí konfigurace je označení vnitřních a vnějších rozhraní. Vnitřní rozhraní je to, ze kterého chceme překládat adresy. U vnějšího se děje to samé, akorát naopak. Dále už se konfigurace značně rozchází. U statického překladu se vytváří seznam, ve kterém je v každém záznamu přiřazena jedna lokální adresa k jedné veřejné. Konfigurace dynamického NATu a PATu je relativně stejná. Nejdříve se nastaví seznam adres, na které můžeme překládat. Poté je potřeba vytvořit access list, jenž definuje adresy s povoleným překladem. Nakonec už se jen přiřadí ACL k seznamu adres. U PATu je to stejné, jen ještě propojení ACL s veřejnými adresami označíme jako PAT, u Cisca slovíčkem overload. Jedinou výjimkou může být případ, kdy se místo seznamu použije adresa odchozího zařízení. Principiálně to ale i zde funguje stejně.

IP adresa a MAC adresa

MAC

MAC adresa se využívá k přepínání rámců na druhé vrstvě ISO/OSI. Skládá se ze šesti osmibitových čísel, přičemž zápis je nejčastěji hexadecimálně. Dala by se rozdělit na dvě částí. První polovina je určena k identifikaci jednotlivých výrobců síťových zařízení. Druhá pak slouží k unikátnímu přiřazení adresy zařízení. Adresa jako taková by měla být u každého zařízení unikátní, avšak existují způsoby, jakým si ji uživatel může změnit. V tomto případě není unikátnost zaručena a v případě, kdy se sejdou dva klienti na jedné síti může být

chování na druhé vrstvě problematické. Zvláštním případem adresy je broadcast. Broadcast MAC adresa slouží ke kontaktu všech zařízení na stejné broadcast doméně. Poznáme jí podle toho, že má nastavené všechny bity na 1 (FF:FF:FF:FF:FF:FF).

IP Adresa

IP adresa slouží k adresaci na 3. síťové vrstvě, a je součástí protokolu IP nacházejícím se na stejné vrstvě. Používají se 2 její verze, přičemž obě si rozebereme níže. Při směrování packetů se používá IPv(4/6) adresa společně se síťovou maskou. Ta má stejnou velikost jako jednotlivé IP adresy, a bity v ní nastavené na 1 jsou po sobě jdoucí. Využívá se k procesu "ANDování". Procesem ANDování se získá adresa sítě tak, že se vezme adresa sítě s maskou sítě a porovnají se jednotlivé bity. Tam kde je u obou bitů 1 se nechá 1. Jinde je bit 0. Lze pak snadno zjistit, zda packet, který přijde, patří do dané sítě.

IPv4

První dnes používanou verzí je IPv4. IPv4 je složena ze čtyř osmibitových čísel. Je to jeden z nejdéle používaných protokolů pro adresaci, a bohužel jeho zásoby pomalu dochází. V minulosti se nepočítalo s tak rychlím nárůstem zařízení následkem čehož byla zvolena "pouze" 32bit adresa. K tomu, aby se snížilo tempo vyčerpání IPv4 adres se využívá mnoho technologií.

Hlavní z nich je NAT (dnes nejčastěji PAT). Technologie NATu umožňuje přidělit jedné síti (typicky jedna domácnost/kancelář) jednu vnější adresu a uvnitř sítě používat privátní adresaci. Při kontaktu vnějšího světa je pak vnitřní adresa přeložena na veřejnou adresu. U dnes nejčastěji používaného PATu je pro komunikaci ještě přiřazen port TCP/UDP.

IPv6

Všem je jasné, že k úplnému vyčerpání IPv4 dříve nebo později dojde. Navíc je poslední dobou čím dál nutnější, typicky např. Kvůli IoT, dát jednotlivým zařízením unikátní adresu. Z tohoto důvodu vznikla verze IPv6, která má velikost 128bit. Nabízí tedy 2^{128}-1 adres. Je tedy možné dát každému zařízení na světě unikátní adresu, a stejně jich ještě hodně zbyde. I zde se ovšem můžeme setkat se soukromými sítěmi, přičemž IANA pro ně rezervovala fc00::/7.

IPv6 zatím není mezi lidmi tolik rozšířená. V kombinaci se vzájemnou nekompatibilitou s verzí 4 pak vzniká problém, kdy se část klientů není schopná připojit k druhé části. Některé OS nám naštěstí dovolují mít pro rozhraní přidělenou jak IPv4, tak IPv6, díky čemuž se dříve popsanému problému předejde. Jsou tu ještě další možnosti zmírňující problém s přechodem, jako je IPv6 Tunnelling, který umožňuje přenos IPv6 po IPv4 infrastruktuře.

DHCP Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol slouží k dynamickému přidělování adres klientům na síti. Jak to ale celé funguje? Klient, který se připojí na síť pošle žádost DHCP serveru. DHCP serverem bývá v domácnostech router/modem, ve firmách to může být i klasický server. Pokud je na síti více serverů, využije informace od toho, který odpoví jako první. Kromě adresy ještě v závislosti na konfiguraci serveru může dostat adresu výchozí brány a DNS serveru/serverů.

U IPv6 je situace ještě trochu složitější. V základní konfiguraci si klient přiděluje adresu pomocí SLAAC, což je protokol sloužící právě k tomuto účelu. Klient dostane od routeru zprávu s Prefixem, délkou prefixu a dalšími nezbytnými informacemi. Klient si poté náhodně vygeneruje zbytek adresy.

Co se DHCPv6 týče, to má 2 druhy, mezi kterými se rozlišuje v závislosti na tzv. Flagu uvedeném v packetu. Prvním je stateless DHCP. Při tomto nastavení klient využije adresaci od routeru stejně jako u SLAAC, ale dodatečné informace si vyžádá od DHCP serveru. Další možností je stateful DHCP. Tato volba říká klientovi, že má od serveru získat všechny informace včetně úplné adresy. DHCP server si navíc vede záznamy o všech přidělených adresách, čímž se ještě více minimalizuje riziko kolizí na síti.

DNS

DNS se stará o překlad textových jmen adres na číselné IP adresy. Díky tomu si uživatel nemusí pamatovat, že adresa pro seznam.cz je 77.75.77.53. Funguje to tak, že ve chvíli, kdy uživatel zadá jmennou adresu se pošle žádost DNS serveru o IP adresu destinace. Ve chvíli, kdy dostane odpověď s cílovou adresou, začne posílat data k cíli.

Síťové protokoly

Komunikace na síti je dnes velice rozmanitá. Je zde mnoho zařízení od veliké variace výrobců, s velkým rozsahem určení a funkcí. Není tedy dobrý nápad, aby si každý výrobce implementoval svoje řešení komunikace. Z tohoto důvodu vzniklo několik protokolů, které mají komunikaci na síti standardizovat. Je tu ovšem i několik proprietárních, ty zde rozebrané nebudou.

Ethernet

Ethernet je soubor technologii provozujících první a druhou vrstvu ISO/OSI. Dává nám i prostředky, po kterých může být provozován provoz i vyšších vrstev. Určuje především kabeláž a dnes je již dominantní technologií, přičemž největším konkurentem mu je Wi-Fi.

Internet Protokol

Internet Protokol je nejběžnější protokol používaný pro adresaci na síťové vrstvě. Máme dvě verze, a těmi jsou IPv4 a IPv6 popsané výše. Obecně by se dalo říct, IP je souborem pravidel, díky kterému je možné doručení packetů z počátku do destinace.

Internet Control Message Protocol

Dalším hojně využívaným protokolem je Internet Control Message Protocol neboli ICMP. Tento protokol slouží k informování o určitém stavu na síti. Ačkoliv věcí, ke kterým ho lze využít existuje více, zde budou uvedeny ty nejhlavnější. Jedním z nejčastějších využití je tzv. potvrzení hosta. To se využívá při tzv. “pingu”, který se používá pro ověření spojení mezi dvěma počítači. Dalším jeho využitím je informování protějšku o chybě spojení, nejčastější kódy jsou tyto

1. Net unreachable
2. Host unreachable
3. Protocol unreachable

4. Port unreachable

Posledním využitím je oznámení o vypršení TTL (počet maximálních skoků packetu).

Telnet

Telnet, celým jménem teletype network, je protokol, který umožňuje připojení dvou počítačů v textové formě. Je nešifrovaný a pro vzdálenou komunikaci ho dnes již z větší části nahradil protokol SSH. Jako stejnojmenný program je součástí operačního systému Windows a různých unixových systémů, díky čemuž je stále po ruce.

SSH

Jak již název Secure Shell napovídá, je to protokol sloužící pro zabezpečenou/šifrovanou komunikaci v TCP/IP sítích. Jeho určením je nahradit nezabezpečený Telnet. Jeho využití je pro zabezpečené připojení k příkazovému řádku, kopírování souborů, nebo jakémukoliv jinému přenosu dat.

TCP

Společně s protokolem IP je TCP jedním ze základních stavebních prvků sítě. Stará se o vytvoření a udržování spojení mezi počátečním a koncovým bodem. Komunikace je zahájena pomocí tzv. Three-way-handshake. Tato technika vypadá asi takto. Host-A pošle hostovi B žádost, že chce komunikovat. Host B odpoví, že žádost přijmul, a že chce navázat spojení. Host A už jen odpoví, že odpověď přijmul, a že od teď je spojení navázáno. Ukončení probíhá v podobném duchu. Na rozdíl od UDP zajišťuje, že budou všechna data doručena, a že budou ve správném pořadí.

UDP

UDP je protokol, jenž v určitých případech zaručuje oproti TCP o něco menší zátěž na síť. Na rozdíl od TCP nenavazuje spojení, a tak není zaručené doručení všech dat. Kontrolu lze stále částečně provádět softwarovou nadstavbou. Díky své nátuře je UDP vhodné pro služby, kde spíše než na celistvosti dat, záleží na rychlosti doručení. Typickým příkladem využití je u online her nebo audio/video chatu.

HTTP/HTTPS

HTTP a HTTPS jsou protokoly sloužící primárně pro přenos hypertextových souborů po internetu. Kromě toho se dnes již vyvinuli do formy, ve které je schopný přenášet i další data. Běžně už se tak používá pro přenos dalších dat jako je XML. Pro komunikaci používají různé hlavičky, přičemž každá slouží pro jiný účel. Nejznámější z nich jsou asi POST a GET.

SMTP

SMTP je dnes nejpoužívanější protokol pro odesílání emailů. Zprávy přes něj odeslané jsou doručeny do schránky cíle. Ze schránky si je klient může stáhnout pomocí protokolů POP nebo IMAP.

POP a IMAP

POP a IMAP jsou protokoly, přes které si klient může z emailové schránky zobrazit doručené zprávy. Hlavní rozdíl mezi nimi je ten, že u POP si musí klient všechny emaily stáhnout ze serveru, zatímco u IMAP klient pracuje se soubory přímo na serveru.

FTP, FTPS a SFTP

Všechny tři protokoly jsou variace jednoho, přičemž všechny slouží pro souborů mezi klientem a serverem. Nejzákladnějším z nich je FTP. Samo o sobě nemá žádné šifrování, není tedy příliš bezpečné pro přenos citlivých dat bez dalších opatření, jako je VPN. Lépe je na tom FTPS, které zajišťuje šifrovanou komunikaci mezi serverem a klientem. SFTP (SSH File Transfer Protocol, nikoliv Simple File Transfer protokol) je stejně jako FTPS šifrované. Rozdíl je v tom, že k šifrování používá SSH, a ke komunikaci je většinou používaný příkazový řádek.

Reference

Bouška, P. (2009). *Cisco IOS 8 - ACL - Access Control List*. Retrieved from samuraj-cz: https://www.samuraj-cz.com/clanek/cisco-ios-8-access-control-list/

Cisco. (2018). *Introduction to networks*. Retrieved from Netacad: https://static-course-assets.s3.amazonaws.com/ITN51/en/index.html

Cisco. (2018). *Routing and Switching Essentials*. Retrieved from Netacad: https://static-course-assets.s3.amazonaws.com/RSE6/en/index.html

One bit hosting. (nedatováno). *Jaký je rozdíl mezi POP3 a IMAP*. Načteno z onebithosting: https://www.onehelp.cz/onebit/kb/cs/pop3-vs-imap

Pedagogická fakulta MU. (nedatováno). *teps-01.pdf*. Načteno z ped.muni.cz: http://www.ped.muni.cz/wtech/03_studium/teps/teps-01.pdf