SOŠ a SOU NERATOVICE

V Neratovicích 29.10.2024
Výtisk jediný
Počet stránek: 12

Zpracoval:
Ing. Petr ORVOŠ

P Í S E M N Á P Ř Í P R A V A

na vyučování – IT 2

Předmět: **POČÍTAČOVÉ SÍTĚ**
Téma: **Topologie sítě, topologické diagramy, architektura sítě**
Místo: učebna
Materiální zabezpečení: písemná příprava
Metoda: výklad s ukázkou

Obsah

Síťová zobrazení

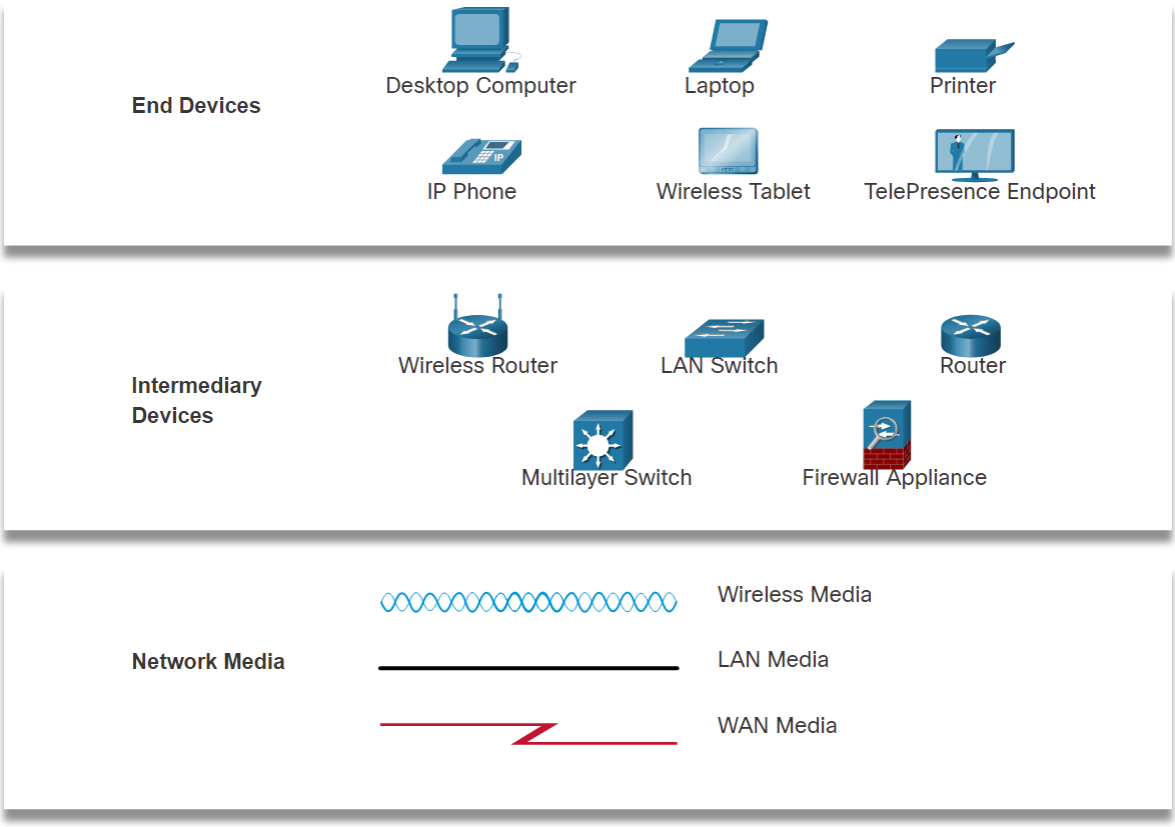
Síťoví architekti a administrátoři musí být schopni ukázat, jak budou jejich sítě vypadat. Musí být schopni snadno vidět, které komponenty se připojují k jiným komponentám, kde budou umístěny a jak budou propojeny. Diagramy sítí často používají symboly, jako jsou ty, které jsou znázorněny na obrázku, k reprezentaci různých zařízení a připojení, které tvoří síť.

Diagramy síťové topologie jsou grafické znázornění struktury a propojení jednotlivých prvků v síti. Tyto diagramy ukazují, jak jsou uzly (např. počítače, servery, směrovače, switche) v síti propojeny, jak komunikují a jak data proudí mezi nimi. Diagramy síťové topologie pomáhají vizualizovat uspořádání sítě, což je užitečné pro plánování, návrh, správu, údržbu a diagnostiku sítí.

Existuje několik základních typů síťových topologií, které mohou být znázorněny v diagramu:

1. **Topologie hvězda (Star)**: Jeden centrální uzel (např. switch nebo server) je propojen se všemi ostatními uzly. Pokud centrální uzel selže, celá síť se zhroutí.
2. **Topologie sběrnice (Bus)**: Všechny uzly jsou připojeny k jedné centrální lince (sběrnici), což je jednoduché a levné, ale může být náchylné k přetížení a selhání.
3. **Topologie kruh (Ring)**: Uzly jsou propojeny do kruhu, kde data putují jedním nebo oběma směry kolem kruhu. Nevýhodou je, že pokud jeden uzel selže, komunikace se může přerušit.
4. **Topologie síť (Mesh)**: Každý uzel je propojen s několika dalšími uzly. Může být částečně propojená nebo plně propojená, což zajišťuje redundanci a zvyšuje odolnost vůči selhání.
5. **Topologie strom (Tree)**: Kombinace topologií hvězda a sběrnice, kde jsou uzly uspořádány v hierarchii podobné stromu.
6. **Hybridní topologie**: Kombinace více topologií, přizpůsobená specifickým potřebám sítě.

Typy síťové topologie



Obrázek 1 Přehled síťových zařízení by CISCO

Topologické diagramy

- jsou povinnou dokumentací pro každého, kdo pracuje se sítí. **Poskytují vizuální mapu toho, jak je síť propojena**.

Existují dva typy topologických diagramů:

- fyzické
- logické.

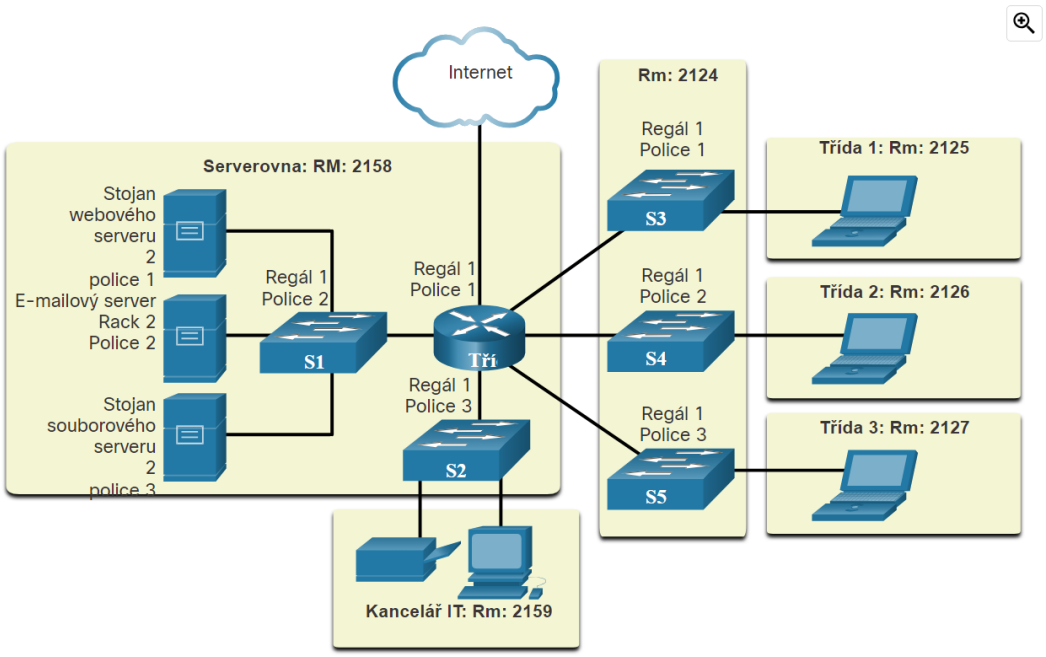
Význam diagramů síťové topologie

Diagramy síťové topologie slouží k:

- **Plánování a návrhu sítě**: Usnadňují rozhodování o tom, jakou topologii použít pro konkrétní aplikace nebo prostředí.
- **Diagnostice**: Pomáhají identifikovat potenciální problémy nebo slabá místa v síti.
- **Dokumentaci**: Slouží jako záznamy o rozložení sítě, což usnadňuje údržbu a správu.
- **Škálovatelnosti a optimalizaci**: Umožňují zhodnotit, jak může být síť v budoucnu rozšířena nebo optimalizována pro lepší výkon.

Diagramy fyzické topologie

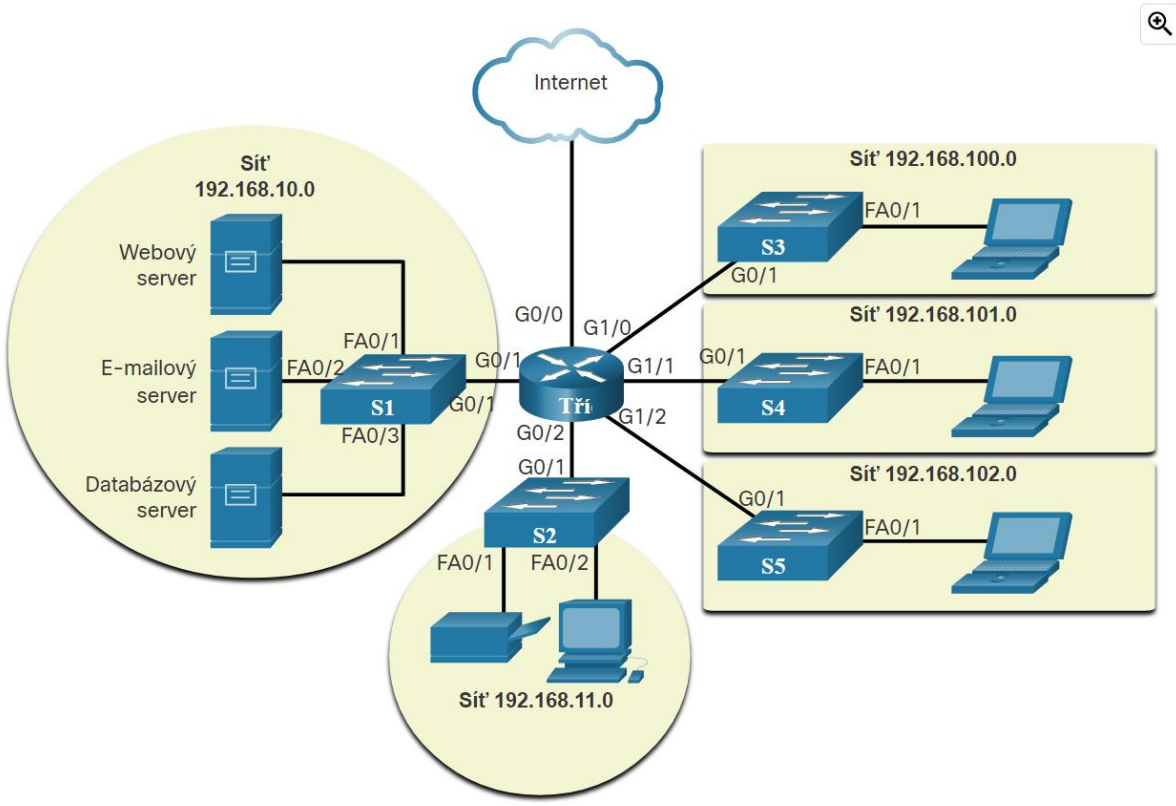
Diagramy fyzické topologie znázorňují fyzické umístění zprostředkujících zařízení a kabelovou instalaci, jak je znázorněno na obrázku. Vidíte, že místnosti, ve kterých jsou tato zařízení umístěna, jsou označeny v této fyzické topologii.



Obrázek 2 Diagram fyzické topologie by CISCO

Diagramy logické topologie

Diagramy logické topologie znázorňují zařízení, porty a schéma adresování sítě, jak je znázorněno na obrázku. Vidíte, která koncová zařízení jsou připojena, ke kterým zprostředkujícím zařízením a jaká média se používají.



Obrázek 3 Diagramy síťové topologie by CISCO

Síťová architektura

Už jste někdy byli zaneprázdněni prací na internetu, jen aby vám "vypadl internet"? Jak už víte, internet nespadl, jen jste k němu ztratili připojení. Vzhledem k tomu, že tolik lidí na světě se při práci a učení spoléhá na přístup k síti, **je nezbytné, aby sítě byly spolehlivé**. **Spolehlivost v tomto kontextu znamená více než jen vaše připojení k internetu.**

Role sítě se změnila ze sítě pouze pro data na systém, který umožňuje propojení lidí, zařízení a informací v multimediálně bohatém konvergovaném síťovém prostředí.

Aby sítě fungovaly efektivně a rostly v tomto typu prostředí, musí být síť postavena na standardní síťové architektuře.

Sítě také podporují širokou škálu aplikací a služeb. Musí fungovat přes mnoho různých typů kabelů a zařízení, které tvoří fyzickou infrastrukturu.

Termín síťová architektura v tomto kontextu odkazuje na technologie, které podporují infrastrukturu a naprogramované služby a pravidla nebo protokoly, které přenášejí data v síti.

Existují čtyři základní charakteristiky, které musí síťoví architekti řešit, aby splnili očekávání uživatelů:

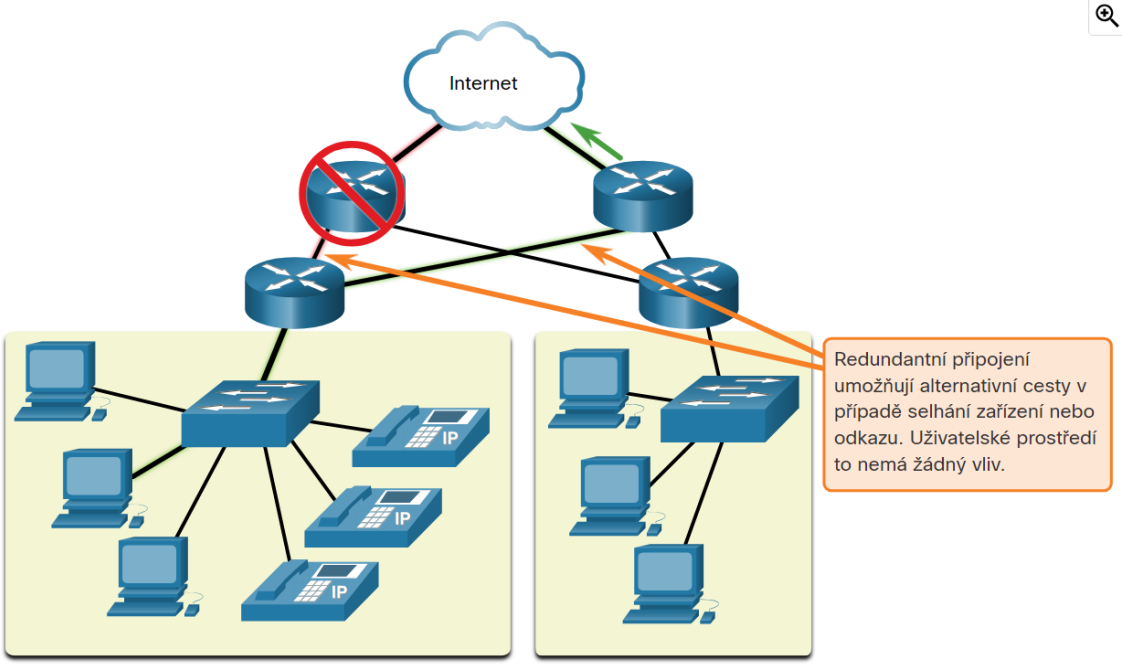
1. Odolnost proti chybám
2. Škálovatelnost
3. Kvalita služeb (QoS)
4. Bezpečnost

Odolnost proti chybám

- je to vlastnost sítě, která **omezuje počet postižených zařízení během selhání** a je navržena tak, aby umožňovala rychlou obnovu v případě takového selhání.

Tyto sítě jsou závislé na více cestách mezi zdrojem a cílem zprávy. Pokud jedna cesta selže, zprávy se okamžitě odešlou přes jiný odkaz. Mít více cest k cíli se označuje jako redundance.

Řešení:



Obrázek 4 Řešení – síť s přepojováním paketů a redundance sítě (by CISCO)

Implementace sítě s přepojováním paketů je jedním ze způsobů, jak spolehlivé sítě poskytují redundanci.

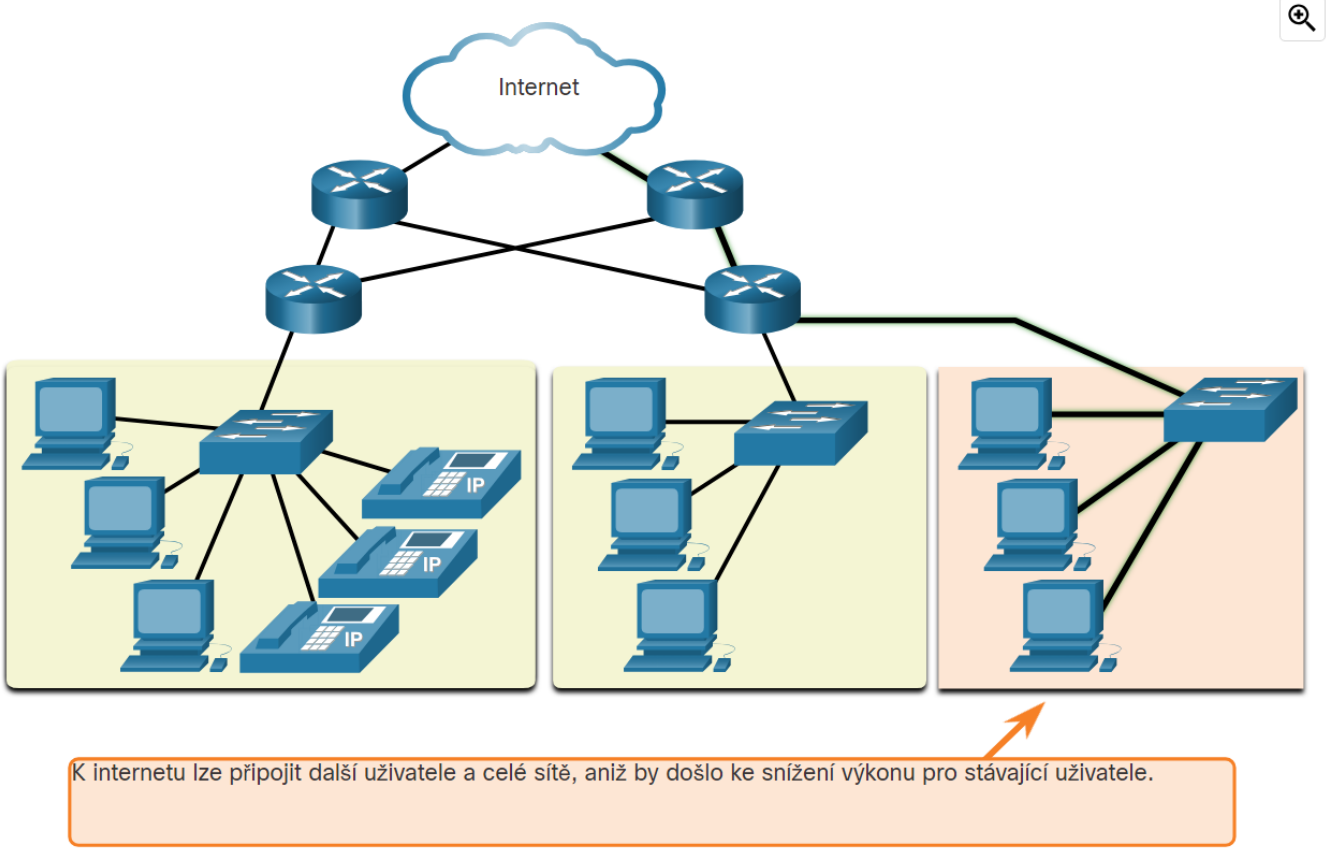
Přepojování paketů rozděluje provoz na pakety, které jsou směrovány přes sdílenou síť. Jedna zpráva, například e-mail nebo video stream, je rozdělena do několika bloků zpráv, které se nazývají pakety. Každý paket má potřebné adresační informace o zdroji a cíli zprávy. Směrovače v síti přepínají pakety na základě stavu sítě v daném okamžiku. To znamená, že všechny pakety v jedné zprávě mohou mít velmi odlišné cesty ke stejnému cíli. Z obrázku je

vidět, že uživatel si není vědom směrovače, který dynamicky mění trasu v případě selhání spojení, a není jím ovlivněn.

Škálovatelnost

Škálovatelná síť se rychle rozšiřuje, aby podporovala nové uživatele a aplikace. Dělá to bez snížení výkonu služeb, ke kterým přistupují stávající uživatelé.

Obrázek znázorňuje, jak lze novou síť snadno přidat do stávající sítě. **Tyto sítě jsou škálovatelné, protože návrháři dodržují uznávané standardy a protokoly.** Dodavatelé softwaru a hardwaru se tak mohou soustředit na zlepšování produktů a služeb, aniž by museli navrhovat novou sadu pravidel pro provoz v síti.



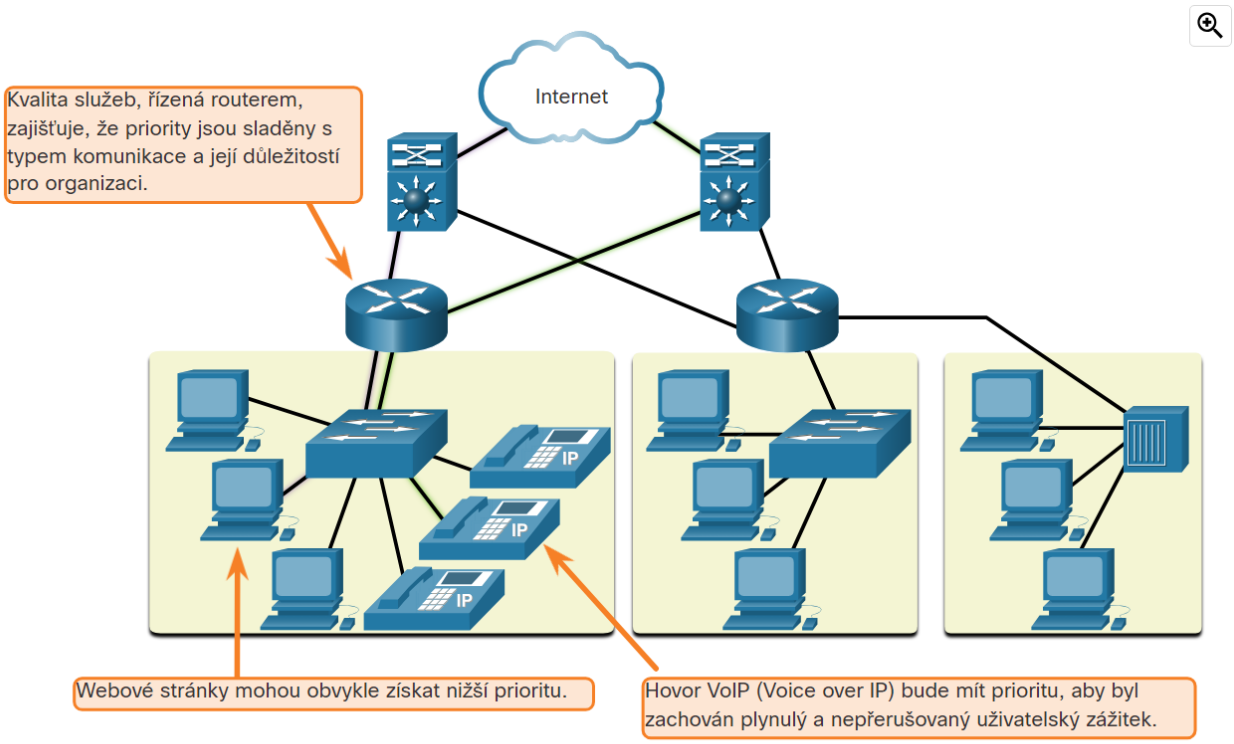
Obrázek 5 Škálovatelnost sítě (by CISCO)

Kvalita služeb (QoS – Quality of Service)

Kvalita služeb (QoS) je v dnešní době stále větším požadavkem na sítě. Nové aplikace dostupné uživatelům přes sítě, jako jsou hlasové a živé video přenosy, vytvářejí vyšší očekávání ohledně kvality poskytovaných služeb. Zkoušeli jste někdy sledovat video s neustálými přestávkami a pauzami? Vzhledem k tomu, že se datový, hlasový a video obsah nadále sbližuje do stejné sítě, **QoS se stává primárním mechanismem pro řízení přetížení a zajištění spolehlivého doručování obsahu všem uživatelům.**

K přetížení dochází, když poptávka po šířce pásma překročí dostupné množství. Šířka pásma sítě se měří počtem bitů, které lze přenést za jednu sekundu, nebo bity za sekundu (bps).
Při pokusech o simultánní komunikaci v síti může poptávka po šířce pásma sítě převýšit její dostupnost, což vytváří přetížení sítě.

Když je objem provozu větší než to, co lze přenést po síti, zařízení budou držet pakety v paměti, dokud nebudou k dispozici zdroje pro jejich přenos.



Obrázek 6 QoS v síti (řízená routerem)

Na obrázku jeden uživatel požaduje webovou stránku a další telefonuje. Se zavedenou politikou QoS může router řídit tok dat a hlasového provozu, přičemž v případě přetížení sítě upřednostní hlasovou komunikaci. QoS se zaměřuje na upřednostňování časově citlivého provozu. Důležitý je typ návštěvnosti, nikoli její obsah.

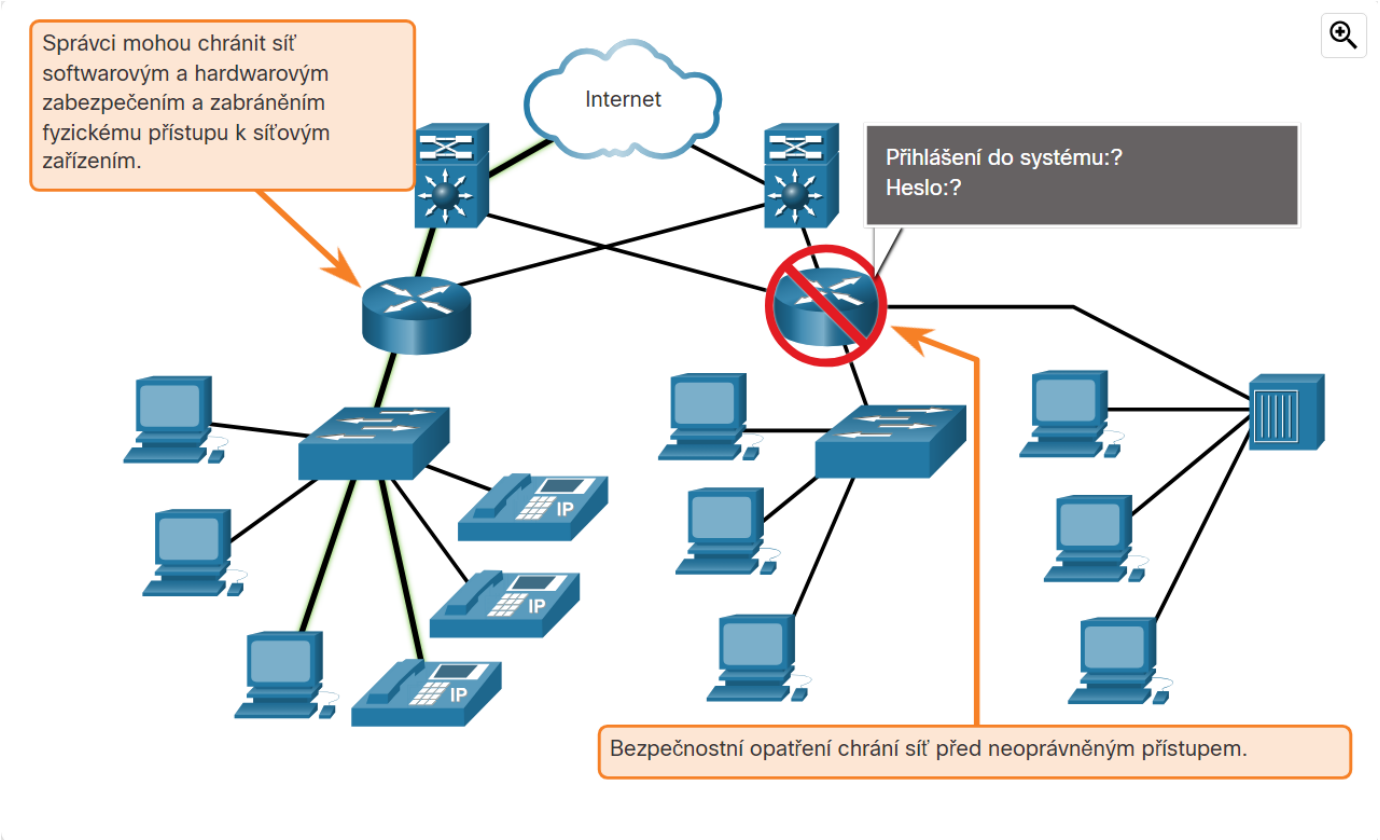
Bezpečnost sítě

Síťová infrastruktura, služby a data obsažená na zařízeních připojených k síti jsou klíčovými osobními a obchodními aktivy.

Správci sítě musí řešit dva typy problémů se zabezpečením sítě:

- bezpečnost síťové infrastruktury;
- bezpečnost informací.

Zabezpečení síťové infrastruktury zahrnuje fyzické zabezpečení zařízení, která poskytují připojení k síti a zabránění neoprávněnému přístupu k softwaru pro správu, který je na nich umístěn, jak je znázorněno na obrázku.



Obrázek 7 Způsoby zajištění bezpečnosti sítě

Správci sítě musí také chránit informace obsažené v paketech přenášených po síti a informace uložené na zařízeních připojených k síti.
Aby bylo možné dosáhnout cílů zabezpečení sítě, existují tři základní požadavky:

1. **Důvěrnost** – znamená, že k datům mají přístup a jejich čtení pouze zamýšlení a oprávnění příjemci.
2. **Integrita** – zajišťuje uživatelům, že informace nebyly změněny při přenosu, z místa původu do místa určení.
3. **Dostupnost** – zajišťuje uživatelům včasný a spolehlivý přístup k datovým službám pro oprávněné uživatele.

Bezpečnostní hrozby

Síťová bezpečnost je nedílnou součástí počítačových sítí bez ohledu na to, zda se jedná o síť v domácnosti s jedním připojením k internetu nebo o společnost s tisíci uživateli. Zabezpečení sítě musí brát v úvahu prostředí, stejně jako nástroje a požadavky sítě. Musí být schopna zabezpečit data a zároveň umožnit kvalitu služeb, kterou uživatelé od sítě očekávají.

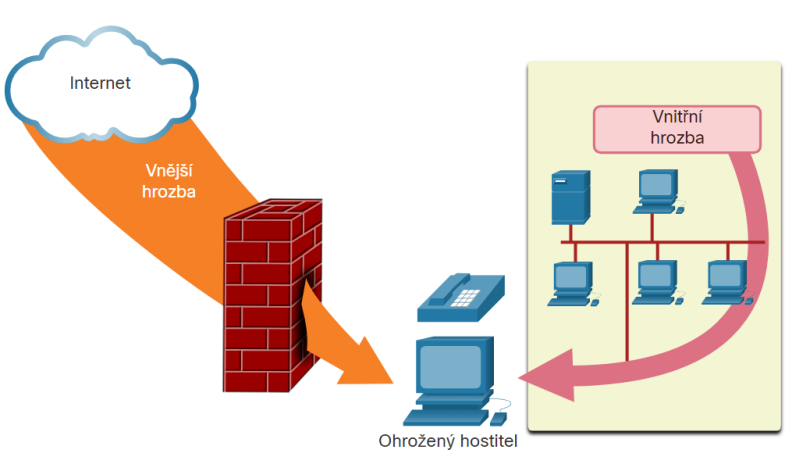
Zabezpečení sítě zahrnuje protokoly, technologie, zařízení, nástroje a techniky za účelem ochrany dat a zmírnění hrozeb.

Druhy hrozeb mohou být externí nebo interní. Mnoho externích bezpečnostních hrozeb sítě dnes pochází z internetu.

Existuje několik běžných externích hrozeb pro sítě:

- **Viry, červi a trojské koně** – obsahují škodlivý software nebo kód spuštěný na uživatelském zařízení.
- **Spyware a adware** – jedná se o typy softwaru, které jsou nainstalovány na zařízení uživatele. Software pak tajně shromažďuje informace o uživateli.
- **Útoky nultého dne (Zero-day attacks)** – označované také jako útoky nulté hodiny a dochází k nim první den, kdy se zranitelnost stane známou.
- **Útoky aktérů hrozeb (Threat actor attacks)** – osoba se zlými úmysly napadá uživatelská zařízení nebo síťové zdroje.
- **Útoky odmítnutí služby (Denial of service attacks, DoS)** – tyto útoky zpomalují nebo způsobují pád aplikací a procesů na síťovém zařízení.
- **Zachycování a krádež dat** – Tento útok zachycuje soukromé informace ze sítě organizace.
- **Krádež identity** – tento útok krade přihlašovací údaje uživatele za účelem přístupu k soukromým datům.

Stejně důležité je vzít v úvahu vnitřní hrozby. Existuje mnoho studií, které ukazují, že k nejčastějším únikům dat dochází kvůli interním uživatelům sítě. To lze přičíst ztraceným nebo odcizeným zařízením, náhodnému zneužití zaměstnanci a v obchodním prostředí dokonce i škodlivým zaměstnancům. S vyvíjejícími se strategiemi BYOD jsou podniková data mnohem zranitelnější. Při vývoji bezpečnostní politiky je proto důležité řešit vnější i vnitřní bezpečnostní hrozby, jak je znázorněno na obrázku.



Obrázek 8 Hlavní dva druhy ohrožení bezpečnosti v síti (by CISCO)

Bezpečnostní řešení

Žádné řešení nemůže 100 % ochránit síť před různými hrozbami, které existují. Z tohoto důvodu by mělo být zabezpečení implementováno ve více vrstvách s využitím více než jednoho bezpečnostního řešení. Pokud jedna bezpečnostní komponenta nedokáže identifikovat a ochránit síť, mohou uspět ostatní.

Implementace zabezpečení domácí sítě

Je obvykle spíše základní. Typicky ji implementujete na koncových zařízeních, ale i v místě připojení k internetu, ale můžeme se spolehnout i na smluvní služby od ISP.

Základní bezpečnostní komponenty pro domácí nebo malou kancelářskou síť:

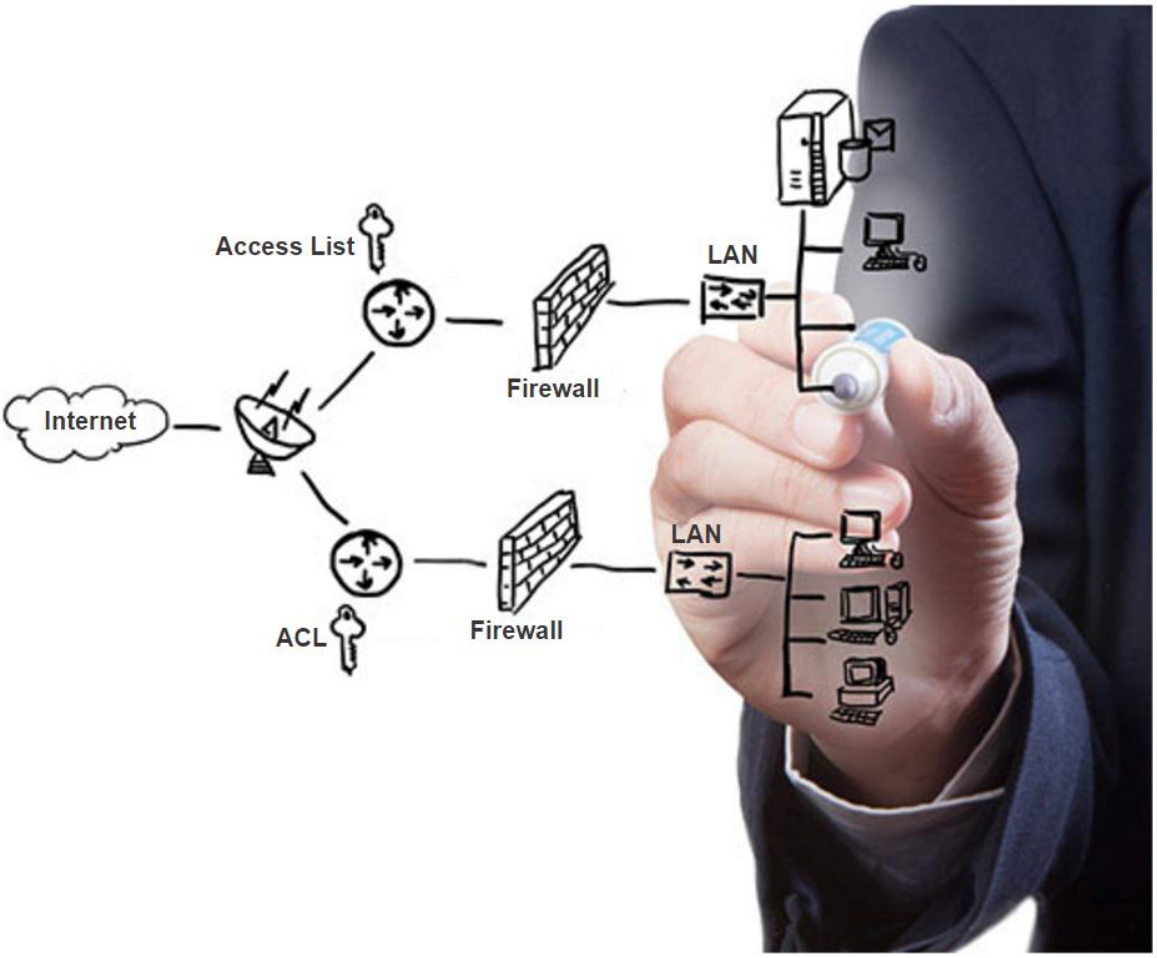
- **Antivirus a antispyware** – aplikace pomáhají chránit koncová zařízení před infikováním škodlivým softwarem.
- **Filtrování firewallu** – blokuje neoprávněný přístup do a ze sítě. To může zahrnovat systém brány firewall založený na hostiteli, který zabraňuje neoprávněnému přístupu ke koncovému zařízení, nebo základní filtrovací službu na domácím routeru, která zabraňuje neoprávněnému přístupu z vnějšího světa do sítě.

Implementace zabezpečení sítě pro podnikovou síť

Skládá z mnoha komponent zabudovaných do sítě, které monitorují a filtrují provoz. V ideálním případě všechny komponenty spolupracují, což minimalizuje údržbu a zvyšuje bezpečnost. Větší sítě a podnikové sítě používají antivirus, antispyware a filtrování firewallu, ale mají i další bezpečnostní požadavky:

- **Vyhrazené systémy firewallů** – poskytují pokročilejší funkce firewallu, které dokážou filtrovat velké objemy provozu.
- **Seznamy řízení přístupu (ACL – Access Control List)** - ty dále filtrují přístup a přesměrování provozu na základě IP adres a aplikací.
- **Systémy prevence narušení (IPS – Intrusion Prevention Systems)** - Identifikují rychle se šířící hrozby, jako jsou útoky nultého dne nebo nulté hodiny.
- **Virtuální privátní sítě (VPN – Virtual Private Networks)** – poskytují vzdálený přístup do organizace.

Požadavky na zabezpečení sítě musí brát v úvahu prostředí, stejně jako různé aplikace a výpočetní požadavky. Domácí i firemní prostředí musí být schopno zabezpečit svá data a zároveň umožnit QoS, kterou uživatelé očekávají od každé technologie. Implementované bezpečnostní řešení musí být navíc přizpůsobitelné rostoucím a měnícím se trendům sítě.



Obrázek 9 Ilustrace zabezpečení sítě (by CISCO)