




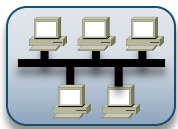
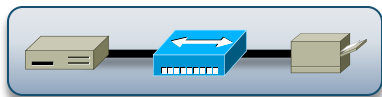
Lekce 2: Internetworking II

Jiří Peterka




propojování na L1, L2 a L3

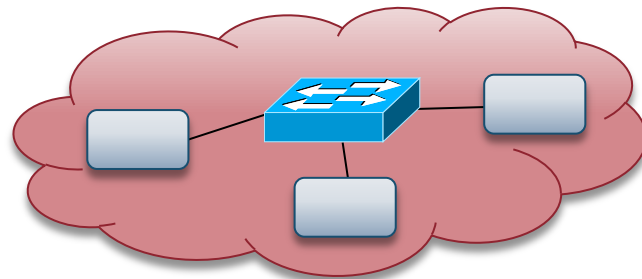
• na fyzické vrstvě (L1)

- propojují se jednotlivé uzly 
 - nebo celé segmenty (skupiny uzlů)
- propojuje se pomocí opakovačů (repeater), ev. odbočkami na „drátě“ 
- výsledkem propojení jsou segmenty 



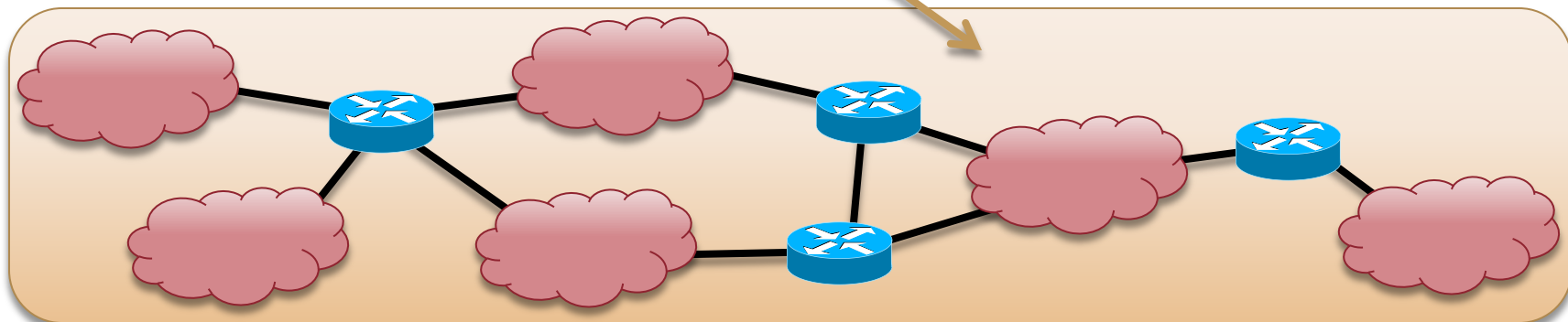
• na linkové vrstvě (L2)

- propojují se jednotlivé segmenty 
- propojuje se pomocí mostů (bridge) či přepínačů (switch) 
- výsledkem propojení je síť 





• na síťové vrstvě (L3)

- propojují se jednotlivé sítě 
- propojuje se pomocí směrovačů (router) 
- výsledkem propojení je soustava propojených sítí ( internetwork, internet) 




propojování na L1, L2 a L3


• na fyzické vrstvě (L1)

- opakovače nejsou „viditelné“ 
 - koncové uzly neví o existenci opakovačů
 - nemohou jim nic adresovat
- opakovače propouští všesměrové vysílání
 - nedokáží vůbec poznat, že jde o broadcast
- opakovače propouští kolize (v Ethernetu)
 - musí, protože nebufferují data
 - neukládají data do vyrovnávacích pamětí
- opakovače mohou propojovat pouze segmenty se stejnou přenosovou rychlostí
 - stejnou  wire speed

• na síťové vrstvě (L3)

- směrovače již jsou „viditelné“ 
 - koncové uzly jim adresují své pakety
 - koncové uzly si musí uvědomovat rozdělení do sítí a existenci „jiných sítí“ (než té jejich)
 - musí dokázat rozlišit mezi uzlem „ve vlastní síti“ a uzlem „v jiné síti“
 - koncové uzly se musí určitým způsobem podílet na směrování
- směrovače nepropouští ani kolize (v Ethernetu) ani všesměrové vysílání (broadcast)

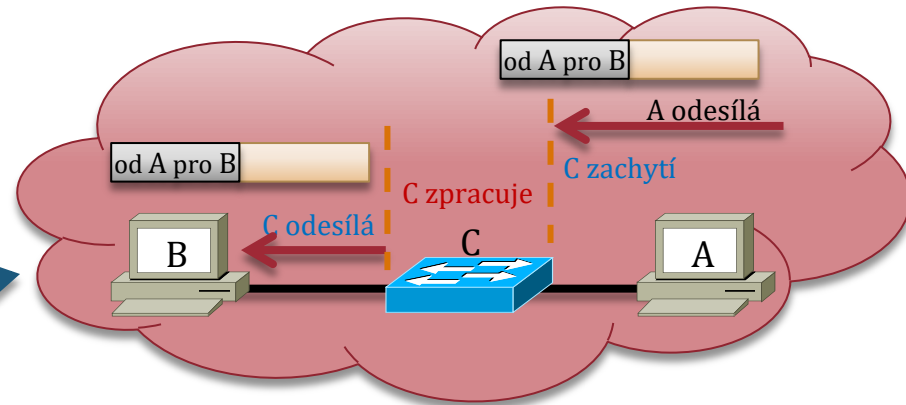
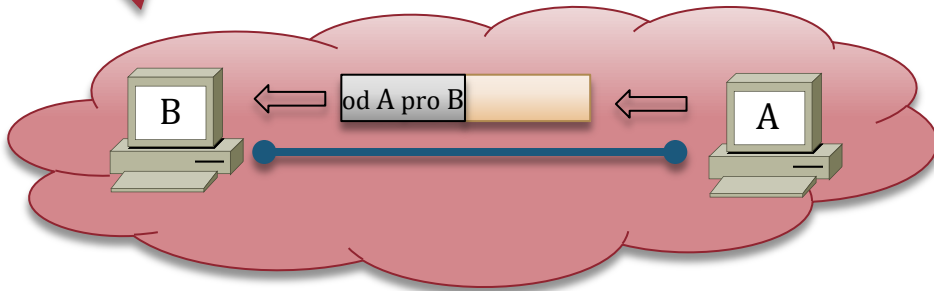
• na linkové vrstvě (L2)

- mosty ani přepínače nejsou „viditelné!“
 - koncové uzly neví o jejich existenci
 - nemohou jim nic adresovat
 - myslí si, že v rámci sítě mají propojení „každý s každým“ 
- mosty a přepínače propouští broadcast
- nepropouští kolize (v Ethernetu)
 - protože již bufferují data
- mohou propojovat segmenty s různou přenosovou rychlostí
 - protože již bufferují data

pohled koncových uzlů

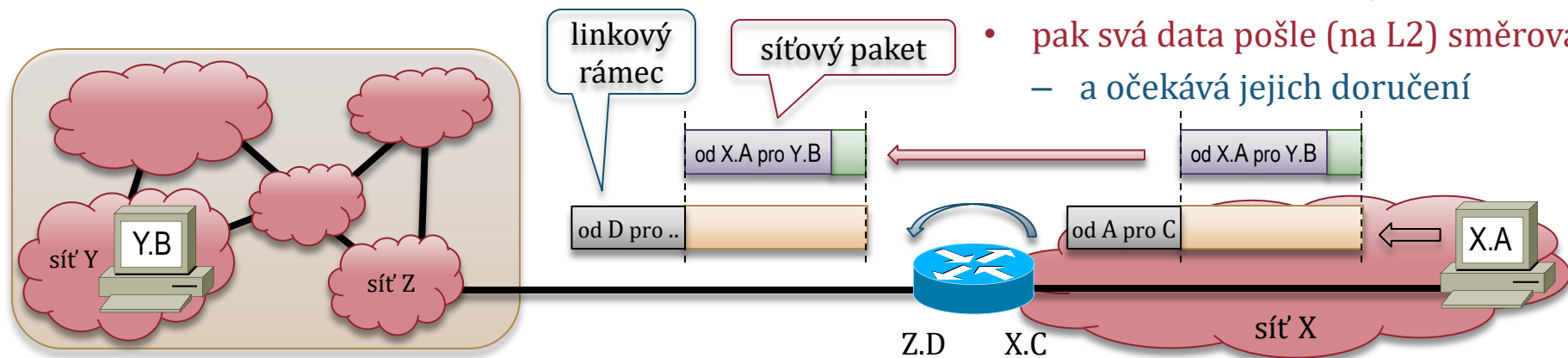
na linkové vrstvě (L2)

- koncový uzel si myslí, že má přímé spojení se všemi ostatními uzly
- proto jim své rámce (na L2) posílá přímo
 - ve skutečnosti je zachytí most či přepínač a postará se o jejich předání




na síťové vrstvě (L3)

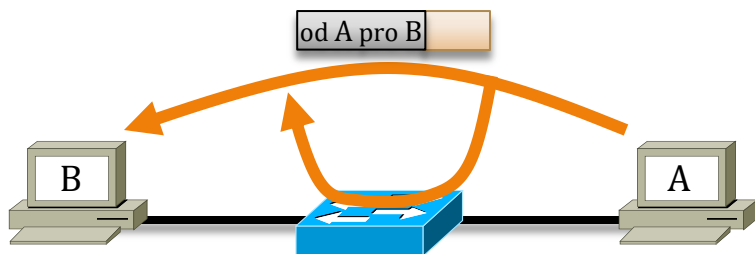
- koncový uzel (A) musí být schopen poznat, zda se cílový uzel (B) nachází ve stejné síti jako on
 - pak mu odesílá přímo (fakticky na L2)
- nebo zda se nachází v jiné síti
 - pak svá data pošle (na L2) směrovači
 - a očekává jejich doručení



rozdíly mezi přepínači a směrovači

• přepínač (nebo most)

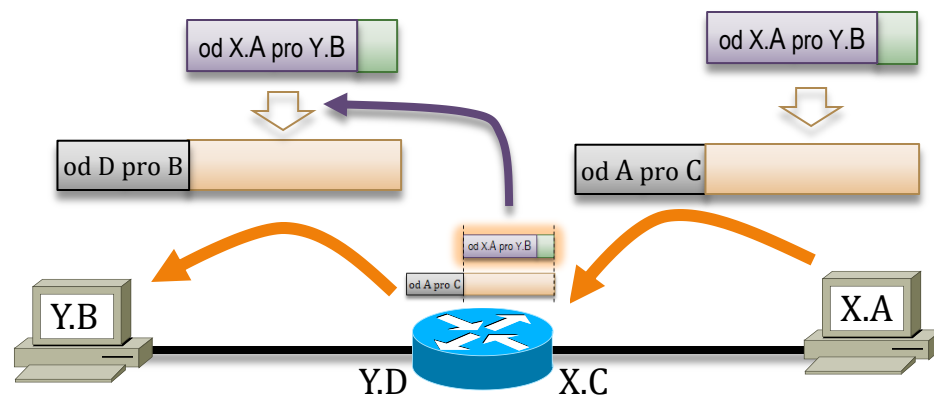
- manipuluje s linkovými rámcí 
 - s těmi, které mu nejsou určeny
 - které „zachytává“ díky speciálnímu nastavení svého síťového rozhraní
 - tzv. promiskuitní režim




- již nezkontroluje „náklad“ linkových rámců
 - například IP pakety
- rozhoduje se jen podle linkových adres
 - např. ethernetových adres
- v odchozím směru odesílá „původní“ (nezměněné) linkové rámce
 - s „původními“ linkovými adresami
 - zde: A, B

• směrovač

- manipuluje s linkovými rámcí 
 - které jsou mu explicitně adresovány



- zkoumá „náklad“ linkových rámců
 - „vybaluje“ z rámců síťové pakety a zkoumá jejich obsah 
 - zajímají ho síťové adresy, podle kterých se rozhoduje o dalším směru přenosu paketu (provádí **směrování**)
 - zde: X.A (odesílatel), Y.B (příjemce)
- při odesílání síťových paketů je opět vkládá do linkových rámců
 - a odesílá na linkovou adresu příjemce (B)

rozdíly mezi přepínači a směrovači

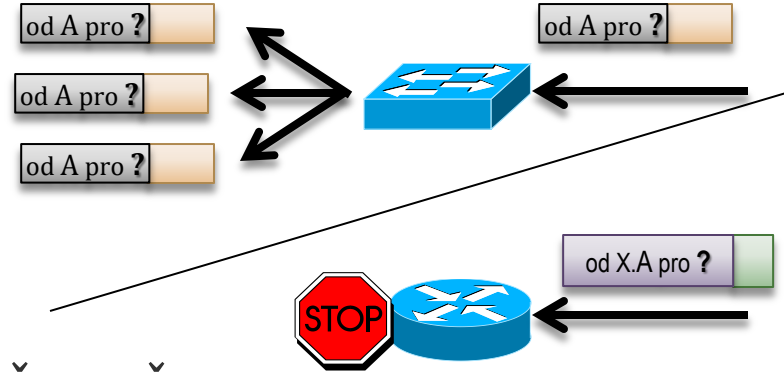
• přepínač (nebo most)

– funguje na principu **forward if not local**

- pokud nemá (pozitivní) informaci o tom, že linkový rámec může zastavit (filtrovat)
 - že je „lokální“ (v „příchozím“ segmentu)
- pak jej předá dál (forwarduje)
 - pokud nemá k dispozici informace o tom, kde se nachází příjemce, nemůže jít o cílené předávání
 - jen do příslušného cílového segmentu
 - ale musí jej předat do všech „odchozích“ segmentů
 - jde vlastně o záplavu/broadcast, kdy se přepínač chová jako opakovač

– nevýhoda:

- pokud cílový uzel neexistuje (nebo jen neodpovídá), přepínač se chová jako opakovač
 - rozesílá rámec na všechny strany
 - plýtvá přenosovou kapacitou



• směrovač

– funguje na principu **forward if proven distant**

- síťový paket předává dál (forwarduje) pouze tehdy, pokud má (pozitivní) informaci o tom, že je určen „vzdálenému“ uzlu
 - a současně „ví, kam jej poslat“
 - jinak se síťovým paketem nedělá nic
 - musí jej zahodit
 - nedokáže jej zpracovat
- ### – výhoda:
- pokud cílový uzel/cílová síť neexistuje, směrovač nic nepředává dál
 - neplýtvá přenosovou kapacitou

broadcast doména, L2 broadcast

• připomenutí:

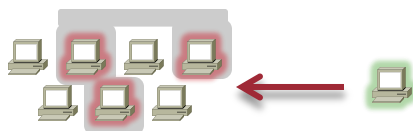
– **unicast**: přenos k 1 příjemci

- příjemcem je právě 1 uzel



– **multicast**: přenos k N příjemcům

- příjemcem je skupina uzlů, tzv. **multicast(ová) skupina**



– **broadcast** (všesměrové vysílání):
přenos ke všem uzlům

- příjemce jsou všechny uzly v rámci určité oblasti – tzv. **broadcast domény**



• broadcast doména

– definice: *oblast, v rámci které se šíří všesměrové vysílání / broadcast*

– v praxi: konkrétní síť

- celek na úrovni síťové vrstvy (L3)

– „to, co je propojeno pomocí mostů/přepínačů“

- **existuje více druhů broadcastu (všesměrového vysílání)**

a) L2 broadcast

- vysílání linkových rámců, které mají jako cílovou adresu broadcastovou (linkovou) adresu

– v Ethernetu: samé 1

- `FF:FF:FF:FF:FF:FF`

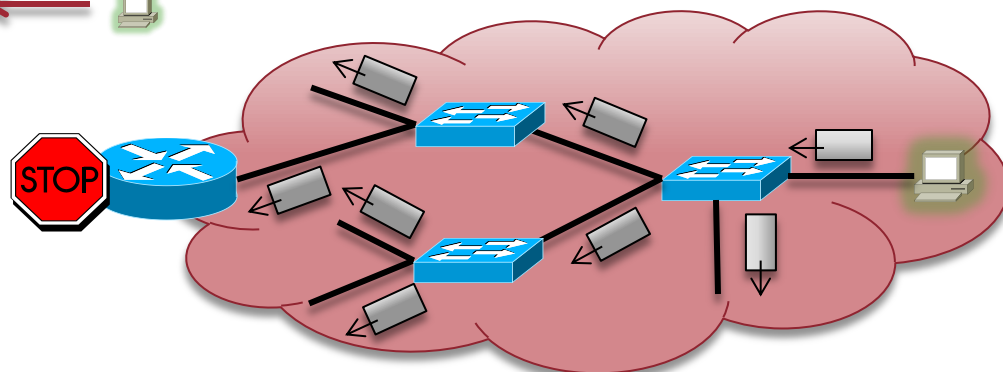


- efekt: broadcast doménou je daná síť

– síť, ve které se nachází odesílatel

– jinými slovy:

- mosty a přepínače propouští L2 broadcast
- směrovače zastavují L2 broadcast





← broadcast doména pro L2 broadcast →

(místní) L3 broadcast

- další druh broadcastu (všesměrového vysílání):

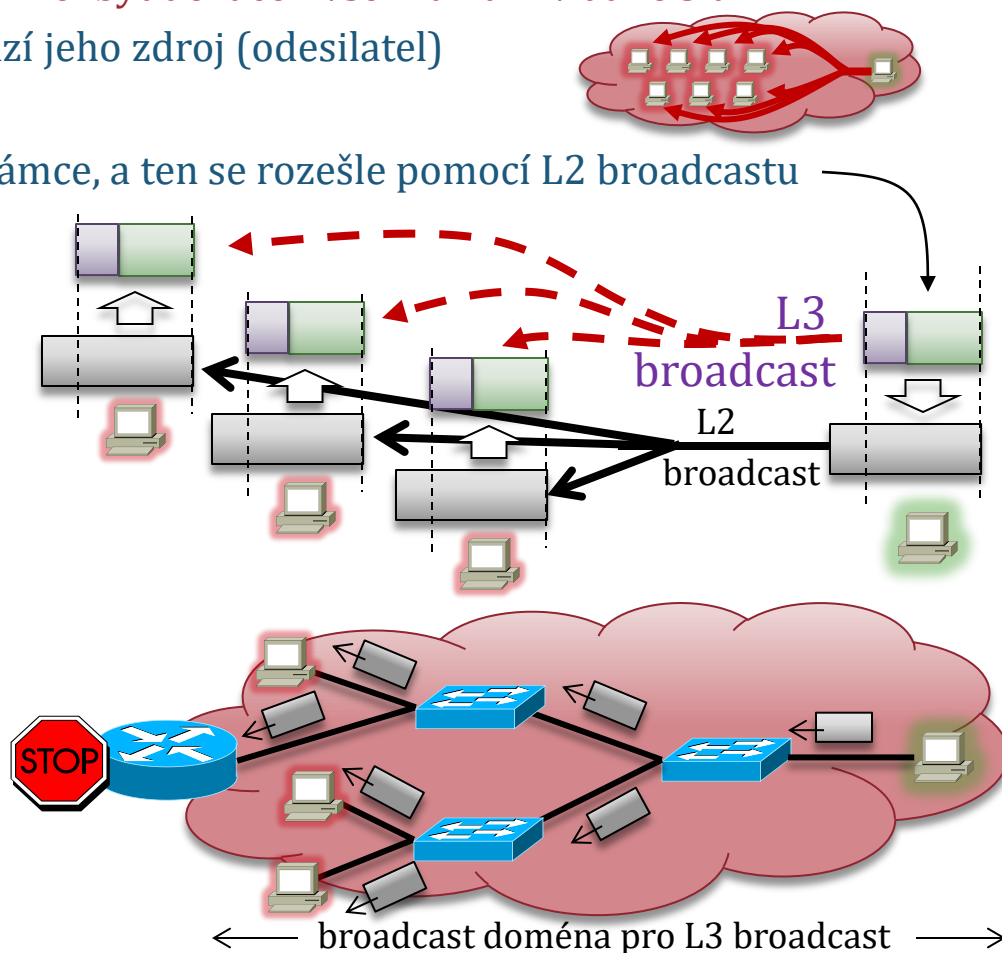
b) (obyčejný, místní) L3 broadcast

- týká se šíření síťových (L3) paketů 
 - zatímco L2 broadcast se týká šíření linkových (L2) rámců 
- paket, odeslaný jako „L3 broadcast“, by měl být doručen všem uzlům v dané síti
 - tedy ve stejné síti, ve které se nachází jeho zdroj (odesílatel)
- praktická realizace
 - síťový paket se vloží do linkového rámce, a ten se rozešle pomocí L2 broadcastu

praktický efekt je stejný jako u L2 broadcastu

– příklad (TCP/IP a Ethernet)

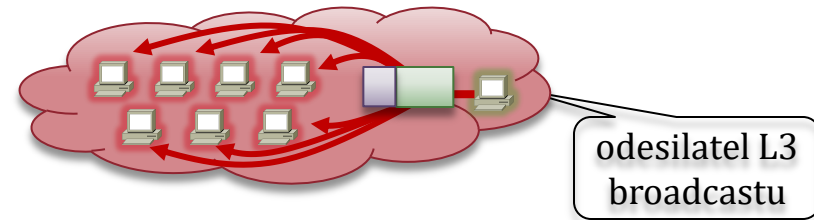
- IPv4 paket je odeslán na „broadcastovou“ IP adresu
 - 255:255:255:255 (32x samé 1)
- odesílatel vloží paket do ethernetového (linkového) rámce
 - a odešle jej na ethernetovou „broadcastovou“ adresu
 - FF:FF:FF:FF:FF:FF (48x samé 1)
 - tento rámec přijmou všechny uzly v dané síti
 - a vybalí si z něj vložený IPv4 paket



cílený L3 broadcast

– připomenutí: (obyčejný, místní) L3 broadcast

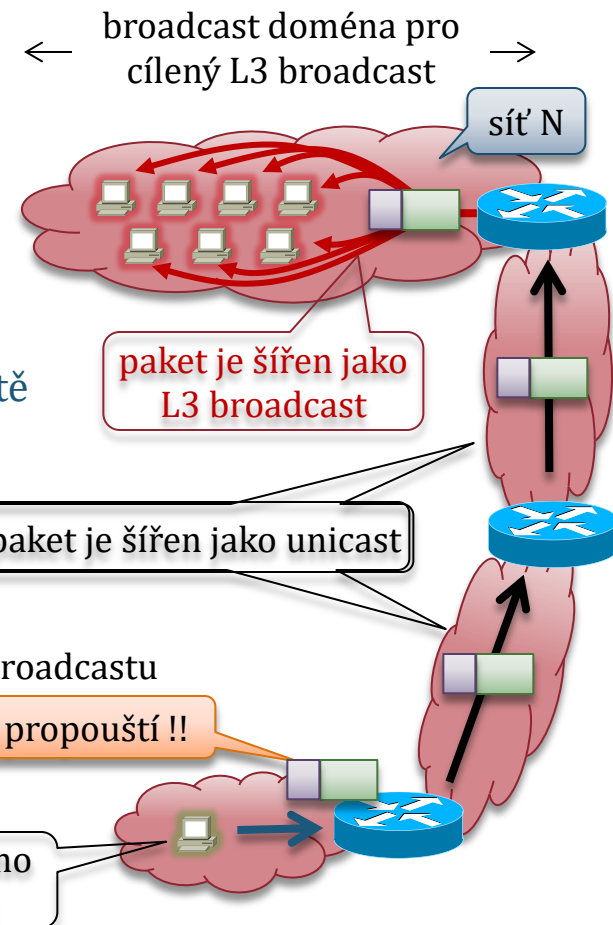
- šíří se v dané síti
 - v síti, kde se nachází jeho zdroj (odesílatel)
 - viz předchozí slide



• další druh broadcastu (všesměrového vysílání):

c) cílený L3 broadcast (🇬🇧 L3 directed broadcast)

- šíří se v zadané cílové síti
 - jiné, než je síť, ve které se nachází zdroj (odesílatel)
- praktická realizace:
 - síťový paket je odeslán ze sítě svého odesílatele
 - je přenášen jako unicastový paket (v 1 exempláři)
 - síťový paket je postupně směrován (přenesen) do cílové sítě
 - stále jako unicastový paket (v 1 exempláři)
 - **směrovače jej propouští (nezastavují, směrují) !!!!**
 - v cílové síti se z něj stává (L3) broadcastový paket
 - a je doručen všem uzlům v cílové síti
 - je vložen do linkového rámce, který je rozeslán pomocí L2 broadcastu



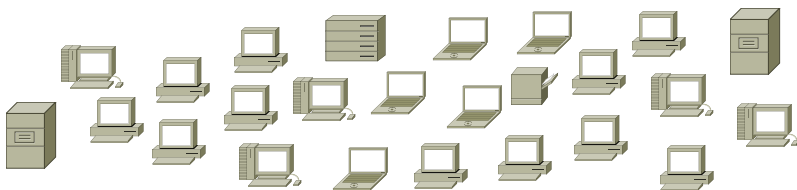
– příklad (TCP/IP):

- IPv4 paket je odeslán na „cílenou broadcastovou IP adresu“
 - ve formátu <N>:111...111
 - kde N je síťová část adresy cílové sítě

jak členit sítě a jejich soustavy?

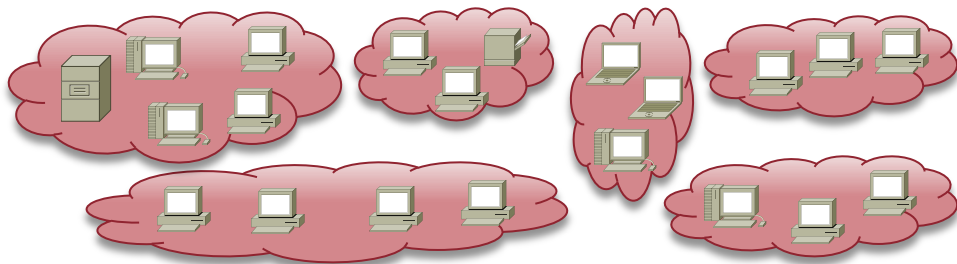
• důležitá otázka:

- když máme větší počty uzlů
 - pracovních stanic, serverů, periférií atd.



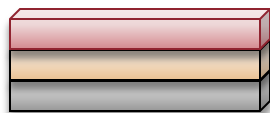
– na jaké (menší celky/skupiny) je rozdělit?

- na jaké sítě, do jakých segmentů?



– jak tyto celky/skupiny vzájemně propojit?

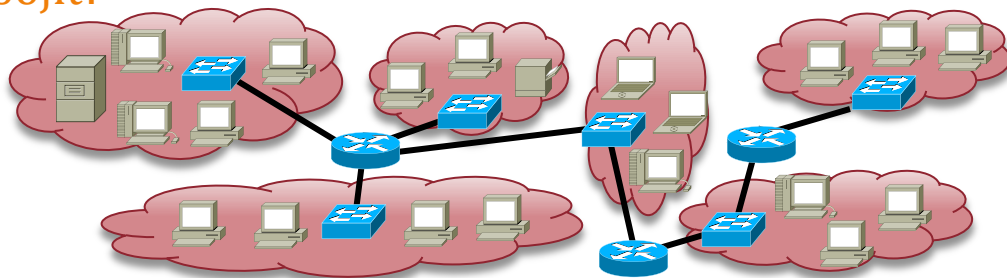
- na jaké vrstvě?
- pomocí jakých aktivních prvků?



• faktory, na kterých záleží

- pro rozhodování o odpovědích
- co a jak dělají uživatelé?
 - jaké služby využívají?
 - email, web,
 - jaké používají aplikace?
 - jak tyto aplikace fungují?
 - s kým/čím komunikují
 - s jakými servery, kde se nachází
- jaké jsou požadavky na přístup, ochranu a bezpečnost
 - kdo kam smí a kam nesmí
 - jaký provoz je přípustný a jaký nikoli
 - jaká jsou nebezpečí a hrozby

–



jak členit sítě a jejich soustavy?

- **neexistuje žádný jednoznačný návod na to, jak postupovat**

- **pouze určitá doporučení**

- která se ale s postupem času vyvíjí

- kvůli tomu, jak se mění chování uživatelů, i charakter jimi využívaných služeb a způsob jejich fungování

- **příklady doporučení (když jde o):**

- **rychlost, propustnost, kapacitu**

- vhodné řešení: **na L2**

- pomáhá segmentace

- rozdělování na co nejmenší segmenty
- podle generovaných datových toků

- propojování segmentů pomocí přepínačů

- **nevýhody a nebezpečí:**

- vznikají „příliš velké“ ploché sítě

- jde o velké broadcast domény
 - každý jednotlivý broadcast „spotřebuje“ hodně kapacity
- mohou být problémy s přidělováním adres

- obtížné zajištění ochrany a práv/oprávnění

- kam kdo smí přistupovat
- jaký provoz je přípustný a jaký nikoli

-



- **přístupová práva, ochranu, bezpečnost**

- vhodné řešení: **na L3**

- vhodné je členění do různých sítí

- podle práv, zabezpečení atd.
- tak, aby sítě byly homogenní

- co do práv/zabezpečení svých uzlů

- a jejich propojování pomocí směrovačů

- plus aplikace firewallů

- **nevýhody a nebezpečí:**

- vyšší nároky na propustnost směrovačů

- nedosahují propustnosti přepínačů
 - jsou optimalizovány spíše na „logiku“ (v rámci směrování)

- vyšší celková složitost

- složitější soustava vzájemně propojených sítí



pravidlo 80:20

- „zvykové pravidlo“ z dob před nástupem Internetu a cloud computing-u
 - kdy uživatelé pracovali především s „místními“ zdroji
 - zejména: servery, umístěnými ve vlastní síti/soustavě sítí (internetu)
 - typicky: se servery v rámci školní či firemní sítě (soustavy sítí / internetu)
 - nikoli se servery umístěnými „vně“ (v Internetu / externím cloudu)
 - podle tohoto pravidla se rozdělovaly uzly do různých sítí
- podstata pravidla:
 - 80% provozu by mělo být místní
 - ve smyslu: zůstat v dané síti, coby „místní“ broadcast doméně (a nešířit se dál)
 - 20% provozu může být „vnější“
 - směřovat do jiných sítí, ať již v rámci vlastní soustavy sítí (internetu), nebo do Internetu

prochází jen skrze



a

– 80% provozu by mělo být místní

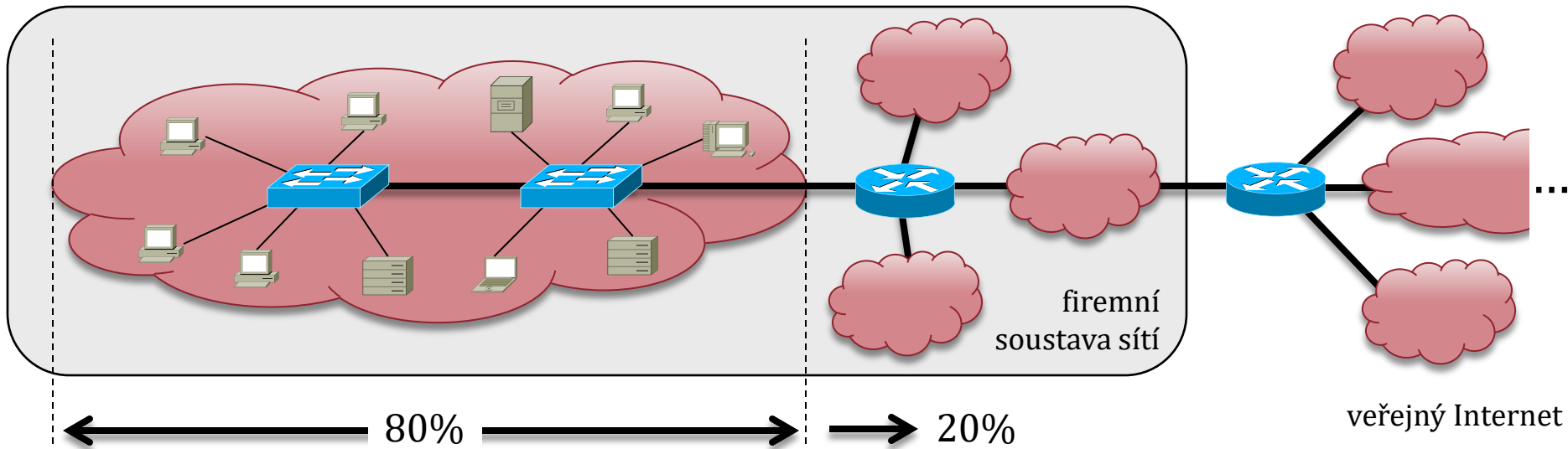
• ve smyslu: zůstat v dané síti, coby „místní“ broadcast doméně (a nešířit se dál)

– 20% provozu může být „vnější“

prochází i skrze



• směřovat do jiných sítí, ať již v rámci vlastní soustavy sítí (internetu), nebo do Internetu

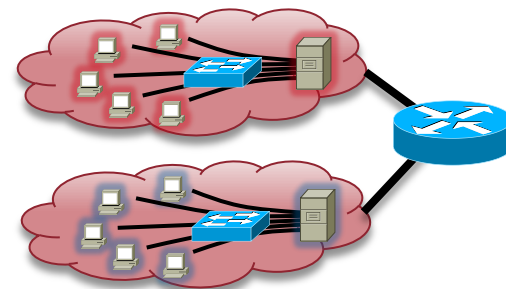


předpoklady pravidla 80:20

- **podle pravidla 80:20 se seskupovaly uzly do sítí**

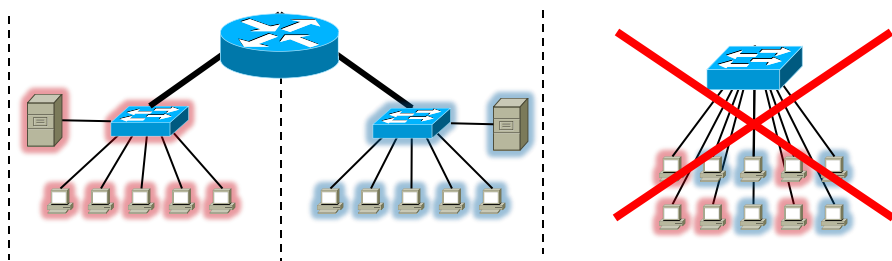
- pracovní stanice uživatelů, kteří používali stejné služby, se zapojovaly do stejné sítě
- spolu se servery, které tyto služby poskytovaly
 - předpoklad: uživatelé budou pracovat hlavně s těmito servery
 - 80% procent provozu směřuje k těmto serverům

dnes již neplatí !!!!



- **má to smysl / jde to dělat takto:**

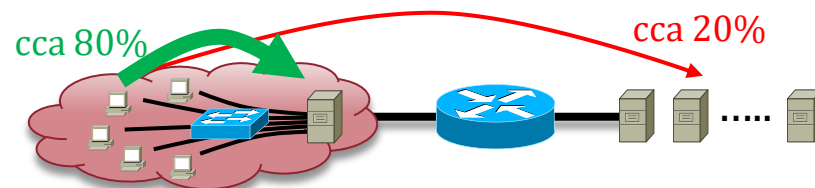
- pokud jsou všechny uzly fyzicky umístěny „vhodně blízko sebe“
 - v dosahu opakovačů nebo přepínačů
 - a naopak zde nejsou „jiné“ uzly
 - které by používaly jiné služby, a měly by patřit do jiných sítí



- pokud tento předpoklad není splněn

- dá se to řešit pomocí sítí VLAN
 - kde rozdělení do sítí není závislé na fyzickém umístění

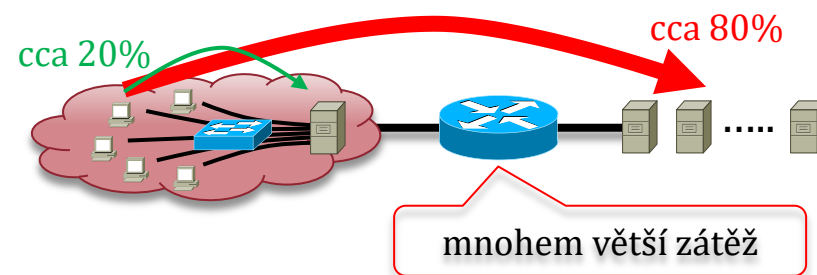
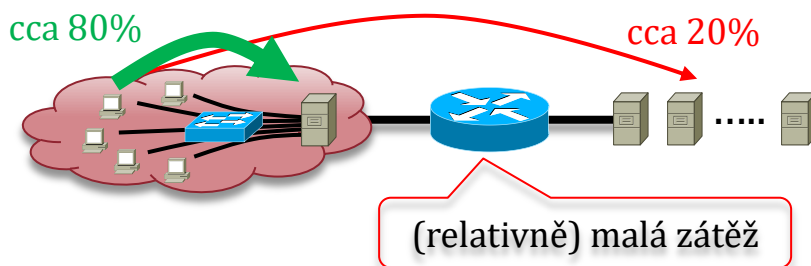
- pokud uživatelé v maximální míře používají „vlastní“ služby
 - příslušné servery se nachází ve stejné síti
- pokud uživatelé v minimální míře používají „cizí“ služby
 - servery, které tyto služby poskytují, se nachází v jiných sítích



- pokud tyto předpoklady nejsou splněny, roste zátěž směrovačů
 - objem provozu skrze směrovače

pravidlo 20:80

- s nástupem Internetu a cloud computingu se poměry obrátily
 - z pravidla 80:20 se stalo pravidlo 20:80
 - většina provozu směřuje „ven ze sítě“ (80%), a jen malá část zůstává „uvnitř sítě“ (20%)



- **důsledek**
 - významně rostou požadavky na celkovou propustnost směrovačů
 - aby zvládaly výrazně větší datové toky, které skrze ně prochází
- **možná řešení:**
 - použití L3 přepínačů (L3 switch)
 - které mají větší propustnost a nejsou úzkým hrdlem
 - zjednodušeně:
 - mají stejnou propustnost jako (L2) přepínače
 - (logicky) fungují jako směrovače
 - nasazení sítí VLAN
 - cíl: udržet propojení na linkové vrstvě (L2)
 - ale: zmenšit broadcast domény
 - lze realizovat „na menší vzdálenosti“
 - pro „místní“ provoz
 - tam, kde vše (je) může být propojeno pomocí přepínačů

směrovače vs. L3 přepínače

• směrovač (router):

- je optimalizován na logické funkce
 - směrování, aplikace přístupových práv,
- je vybaven „dalšími“ schopnostmi
 - monitorování dat. provozu, management
- jeho logické funkce jsou realizovány v SW
 - obvykle má vlastní operační systém
 - CISCO: IOS
- není (tolik) optimalizován na rychlost a propustnost
 - původně po něm nebyla (tolik) požadována
 - viz pravidlo 80:20
- má větší směrovací tabulky
 - dokáže pracovat s většími objemy směrovacích informací, podporuje BGP,
- má (obvykle) větší buffery pro data
 - dokáže bufferovat více síťových paketů
- může mít síťová rozhraní různých typů
 - Ethernet, SDH, SONET, E1/T1,

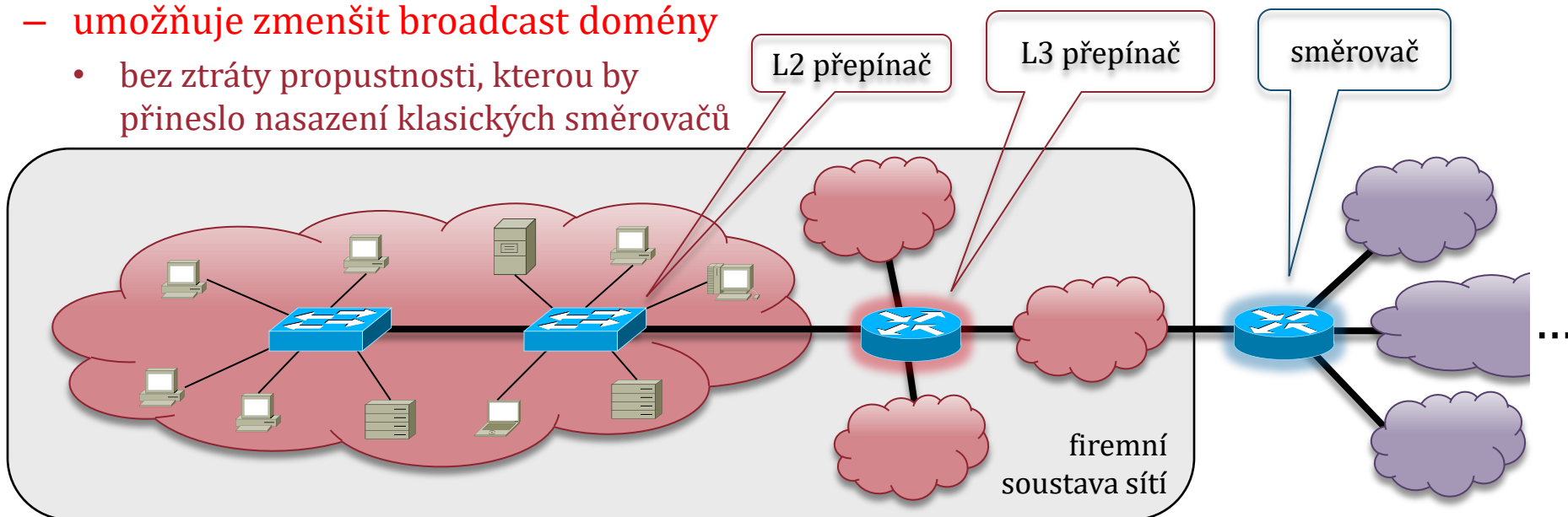
• L3 přepínač (L3 switch)

- L3 = funguje na síťové vrstvě
 - tj. manipuluje se síťovými pakety
 - rozhoduje se (směruje) podle síťových adres (např. IP adres)
- přepínač (switch) = je optimalizován na rychlost a propustnost
 - a typicky realizován v HW
 - aby mohl fungovat „rychlostí drátu“
 - „at wire speed“
- má menší směrovací tabulky a buffery
 - nezvládá větší objemy směrovacích informací,
- má obvykle jen ethernetová rozhraní
- jeho „další funkce“ jsou omezeny nebo nejsou vůbec dostupné
 - například naplňování přístupových práv, monitorování, správa,

zjednodušená představa: je to běžný (L2) přepínač, doplněný o schopnost práce na L3

směrovače vs. L3 přepínače

- **L3 switch je určen pro „propojení“**
 - v rámci homogenního prostředí
 - hlavně: pro vzájemné propojení jednotlivých (L3) sítí v rámci LAN či MAN
 - kde “panují stejné poměry”
 - kde jsou používány stejné přenosové technologie
 - na L2: jen Ethernet
 - kde se pracuje s malými objemy směrovacích informací
 - které se tak často nemění
 - umožňuje zmenšit broadcast domény
 - bez ztráty propustnosti, kterou by přineslo nasazení klasických směrovačů
- **směrovač je určen pro „přechod“**
 - pro přechod mezi různými prostředími
 - hlavně: pro napojení sítí „menších“ sítí (sítí LAN, ev. MAN) na „velké“ sítě (WAN)
 - kde je kladen důraz na přizpůsobení, logické oddělení, správné rozhodování, ...
 - kde se pracuje s většími objemy informací, různými protokoly (i směrovacími), ...
 - umožňuje „napojení na jiné sítě“



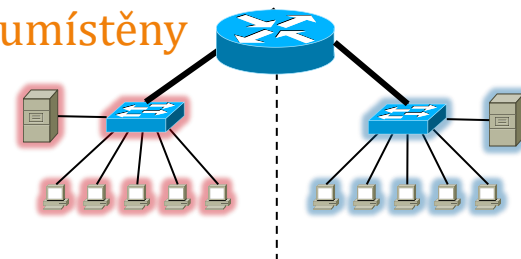
sítě VLAN (Virtual LAN)

- **VLAN (Virtual LAN) je řešení pro situaci:**

- kdy je potřeba členit uzly do sítí nezávisle na jejich fyzickém umístění
 - ale podle logických kritérií (příslušnost ke skupině/kategorii uživatelů, přístupová práva, používané služby a servery,)
- je třeba „řídit“ velikost broadcast domén (aby se příliš nerozrůstaly)

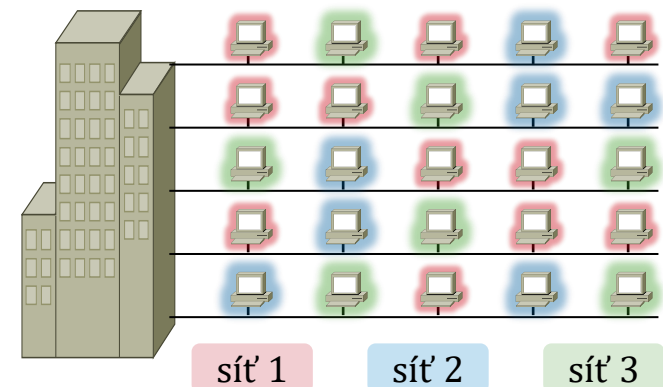
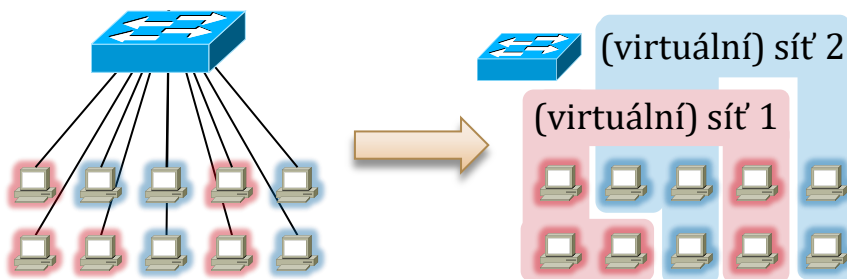
- **situace bez sítí LAN**

- uzly musí být zařazovány do sítí podle toho, kde jsou fyzicky umístěny
 - „kam od nich vede kabeláž“ – ke kterému přepínači a směrovači
 - fyzické umístění nemusí korespondovat s logickými kritérii !!!



- **princip virtuální sítě (VLAN)**

- již neplatí, že: *to, co je propojeno na linkové vrstvě (L2), je jednou sítí*
- místo toho:
 - přepínač (podporující VLAN) může propojovat uzly, „patřící“ do různých sítí
 - a tím i do různých broadcast domén

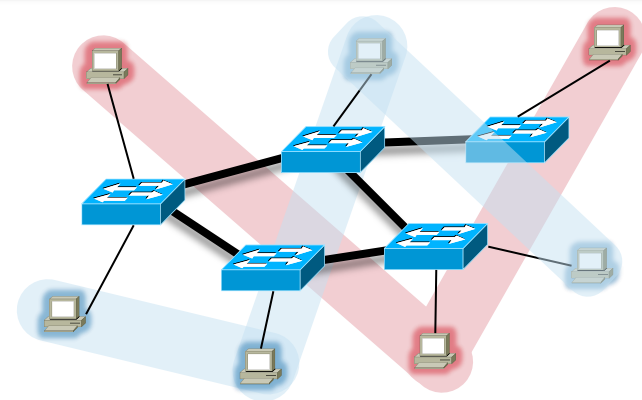
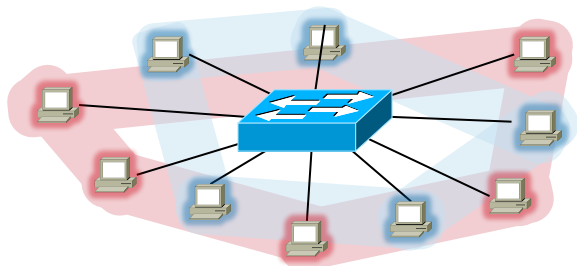


lokální a end-to-end VLAN

- **existuje více variant sítí VLAN**
 - které se liší hlavně svým účelem a cílem
 - ale hranice mezi nimi nejsou příliš ostré (jednoznačné)

- **lokální VLAN**

- spojuje (řadí do jedné sítě) „geograficky blízké“ uzly
 - hlavním cílem je minimalizovat velikost broadcast domény
 - typicky v dosahu jediného (L2) přepínače, nebo (malé) skupiny přepínačů
- uzly v lokální VLAN síti nemusí mít „společné zájmy“
 - a nemusí generovat více „lokálního“ provozu než „vnějšího“
 - spíše zde platí pravidlo 20:80
 - jen 20% provozu je lokální

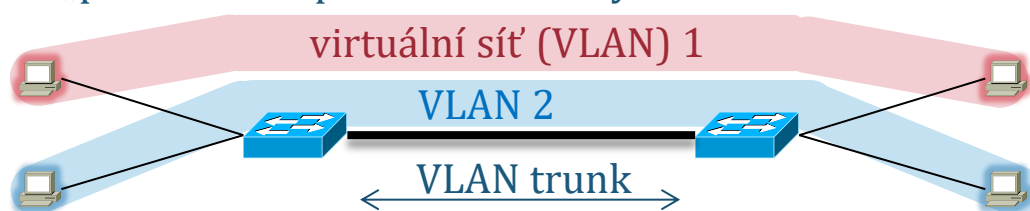


- **end-to-end VLAN**

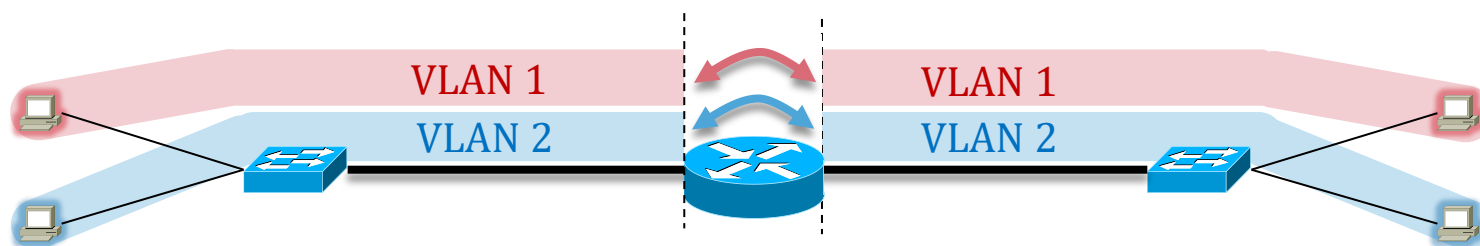
- spojuje (řadí do jedné sítě) „geograficky rozptýlené uzly“
 - sdružuje uživatele se stejnými právy/zájmy/chováním/zařazením
 - mohou být i „daleko od sebe“
 - např.: „všichni studenti na univ. kampusu“
- dělá se hlavně kvůli snadné správě uživatelů a nastavení přístupových práv
 - rozložení provozu pro tyto sítě VLAN může být jakékoli
 - 80:20, stejně jako 20:80

VLAN trunking, směrování mezi VLAN

- sítě VLAN se mohou „rozkládat“ i přes více přepínačů
 - pak je ale mezi nimi nutný tzv. VLAN trunking
 - řešení, kdy 1 spoj mezi více přepínači přenáší provoz, který spadá do více různých VLAN
 - a nedochází k „promíchání“ provozu od různých VLAN



- sítě VLAN mohou „procházet“ i skrze směrovače (či L3 přepínače,)
 - směrovače ale musí takovéto řešení (sítě VLAN) podporovat



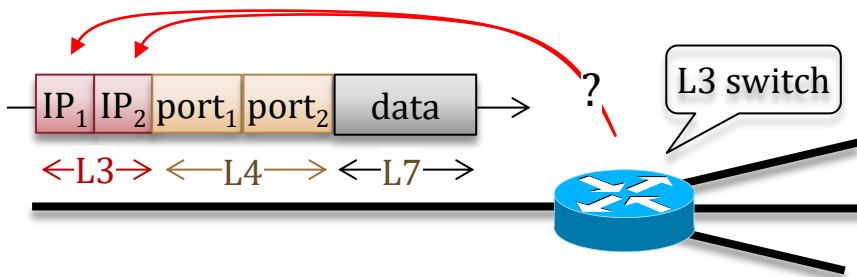
- pro směrování mezi různými sítěmi VLAN je nutný směrovač (L3 přepínač)
 - který může vystačit i s jedním rozhraním
 - skrze které dokáže předávat síťové pakety mezi různými sítěmi VLAN



L4 a L7 přepínače

- **připomenutí: L3 přepínač**

- manipuluje se sítovými pakety
- řídí se sítovými (L3) adresami



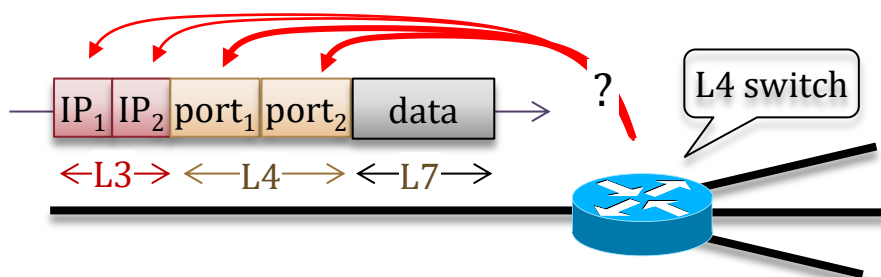
- **vedle toho existují také:**

- **L4 přepínače** (🇬🇧 L4 switch)

- fungují na síťové (L3) vrstvě
 - manipulují se sítovými pakety
- rozhodují se podle sítových (L3) adres **i podle transportních (L4) adres**
 - v TCP/IP: dle IP adres i dle čísel portů

- **výhoda**

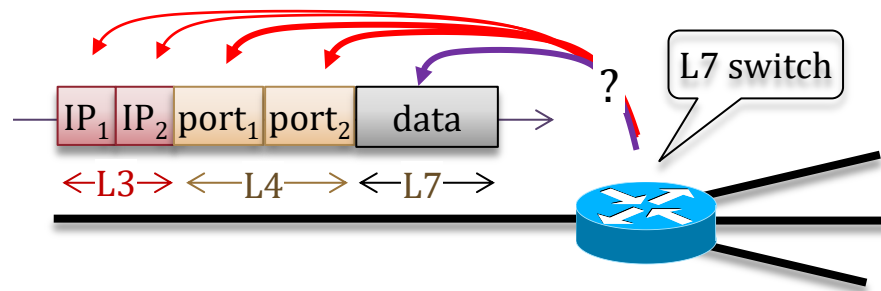
- dokáží rozlišovat různé druhy provozu (podle čísla portu) a „nakládat s nimi“ různě
 - např. směrovat požadavky na WWW servery jinak než DNS dotazy



- **L7 přepínače** (🇬🇧 L7 switch)

- fungují na síťové (L3) vrstvě
 - manipulují se sítovými pakety
- rozhodují se podle sítových (L3) adres, **podle transportních (L4) adres a také podle aplikačních (L7) dat**
 - v TCP/IP: (např.) dokáží vzít v úvahu, že
 - jde o požadavek na WWW server
 - dle portu č. 80 (L4 adresy)
 - jaké konkrétní URL je požadováno
 - dle obsahu požadavku GET a dalších údajů na aplikační (L7) vrstvě

těž:
content
switch



využití L4/L7 přepínačů

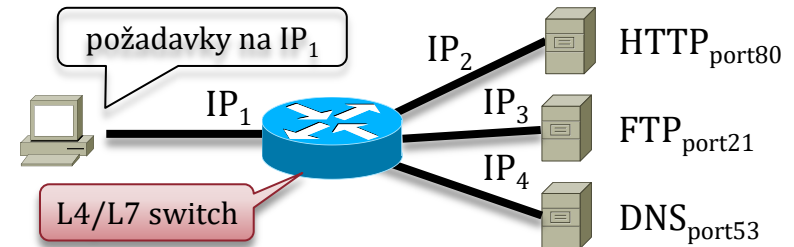
- **L4 a L7 přepínače se hodí pro 2 různé skupiny účelů:**

- řízení datového provozu (traffic management)

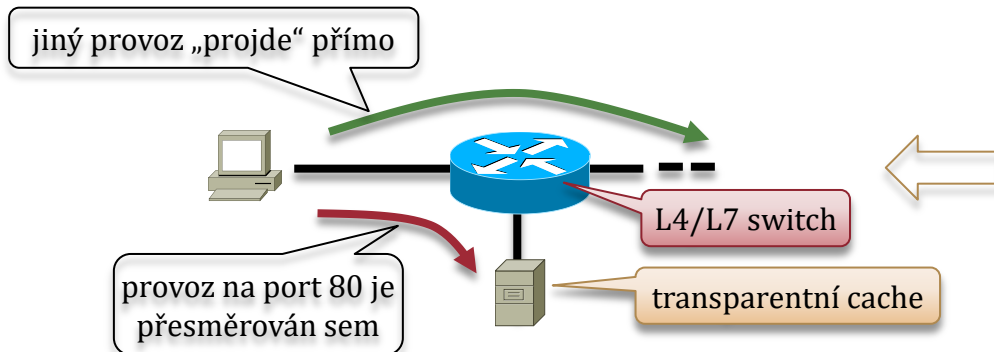
- různé „zacházení“ s různými druhy provozu
 - typicky: podle cílového portu
- například:
 - multimediální data mají přednost před ostatními
 - prioritizace dle druhu provozu
 - blokování určitého provozu
 - např. P2P přenosů, VOIP komunikace
 - objemové limity/kvóty na různé druhy provozu
 - např. v rámci FUP (Fair Use Policy)

- rozdílné směrování

- může být ještě spojeno s (rozdílným) překladem adres (NAT-em)
- například:
 - rozdělování požadavků na různé služby mezi servery, poskytující různé služby

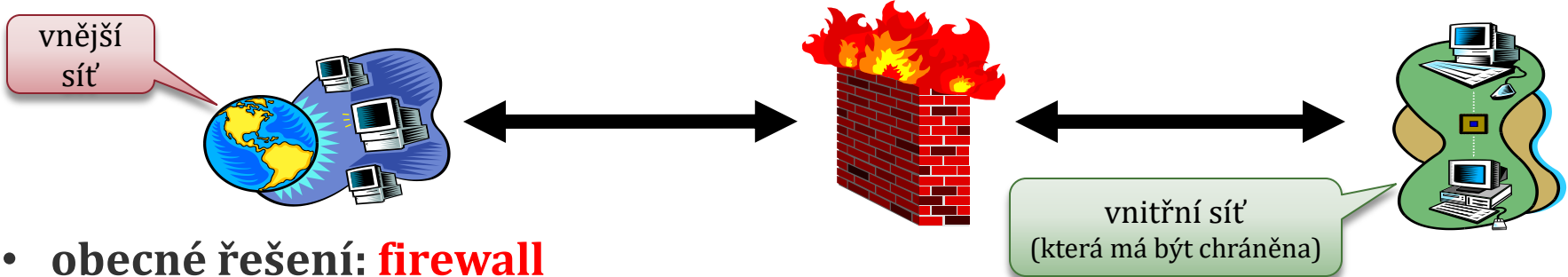


- rozdělování požadavků na služby stejného typu mezi různé instance serverů stejného typu (např. serverové farmy)
 - obdoba anycast-u u IPv6
- rozklad zátěže (load balancing)
 - využití více přenosových cest
- transparentní cache
 - pomocí přesměrování požadavků na port 80
- přesměrování DNS dotazů
-



firewall

- významným úkolem internetworkingu je (dnes) také řízení přístupu
 - nikoli ve smyslu „řízení přístupu ke sdílenému médiu“ (řešenému na L2)
 - ale ve smyslu toho:
 - aby se uživatelé (resp. datový provoz) dostali jen tam, kam mají právo se dostat
 - neboli:
 - blokování neoprávněného přístupu, povolení (umožnění) oprávněného přístupu

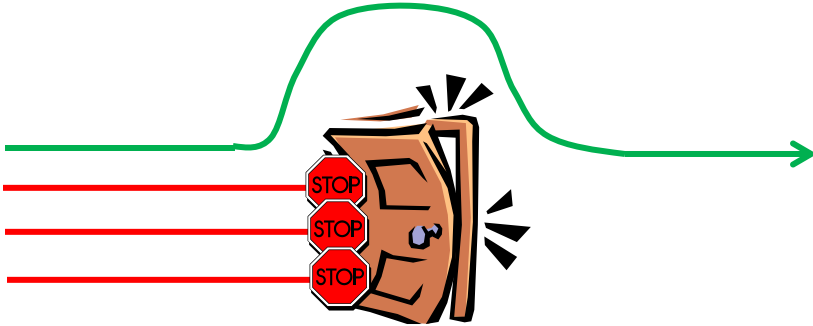


- obecné řešení: **firewall**
 - tak se (obecně) označuje řešení, které implementuje požadovaná pravidla přístupu
 - firewall může realizován jako:
 - kombinace SW a HW
 - jen v SW
 - jen jako sada (organizačních) opatření
 - firewall může být:
 - „společný“ (firemní, školní, domácí, ...) – chrání celé sítě (a více uživatelů)
 - „individuální“ (osobní) – chrání jen jednoho uživatele



princip fungování firewallů

- firewally mohou využívat dva různé přístupy ke svému fungování

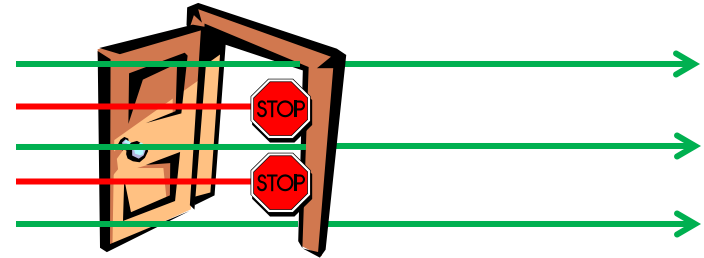


- „vše je blokováno, ale něco je povoleno“

- nejprve: vše se zablokuje
- následně: povolí se konkrétní „pozitivní“ výjimky
 - charakteru povolení

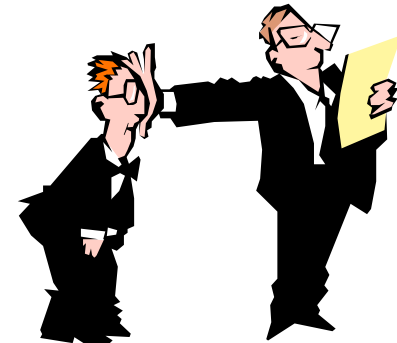
- otázky:

- jak dosáhnout „zablokování všeho“
 - tak, aby následně bylo možné specifikovat výjimky?
- jak dosáhnout „zablokování něčeho“
 - tak, aby vše ostatní mohlo řádně fungovat?
- na jaké úrovni / jakou formou specifikovat výjimky?



- „vše je povoleno, ale něco je blokováno“

- nejprve: vše se nechá povolené
- následně: zakáže se konkrétní „negativní“ výjimky
 - charakteru zákazu



DMZ: demilitarizovaná zóna

- obvyklé řešení pro firewally, fungující na principu „vše je zakázáno, něco je povoleno“

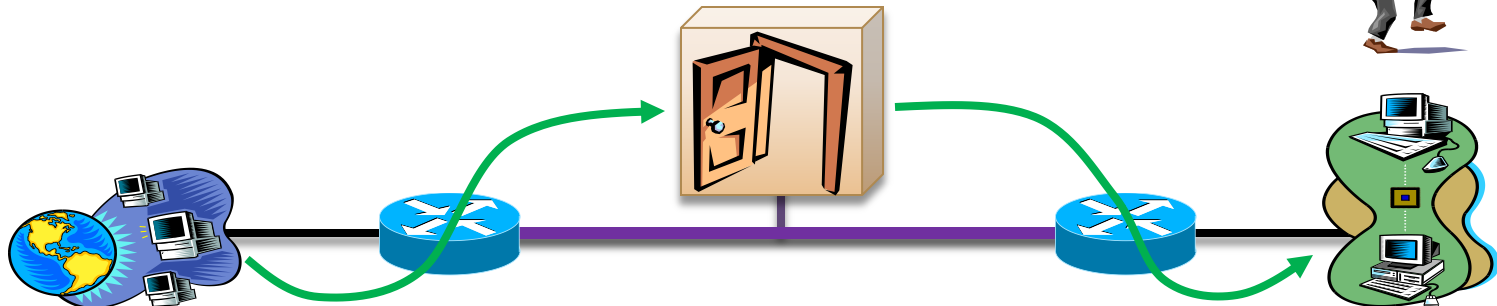
– mezi vnější sítí a vnitřní sítí se vytvoří tzv. **demilitarizovaná zóna (DMZ)**

- tato demilitarizovaná zóna není průchozí (není povolen žádný provoz „skrz“ DMZ)
 - povolen je pouze takový provoz, který začíná či končí uvnitř DMZ
 - tím je implementováno pravidlo „vše je zakázáno“



– do demilitarizované zóny se umístí „brány“, které předávají povolený provoz

- brána kontroluje provoz: pokud je povolený, „pustí jej“ dál
 - ve skutečnosti (aby byl možný průchod „skrz“ DMZ)
 - příchozí provoz „končí“ na bráně uvnitř DMZ
 - odchozí provoz „začíná“ na bráně uvnitř DMZ



příklad: HTTP proxy brána

• příklad praktického nasazení:

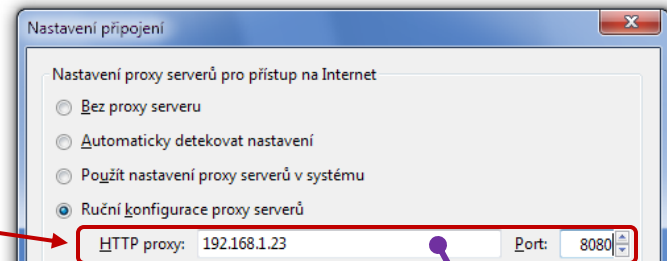
- v DMZ je brána, fungující na úrovni aplikační vrstvy (L7): **HTTP proxy brána**
 - kvůli L7 je taková brána vždy „aplikačně závislá“ (specifická pro konkrétní aplikaci/službu)
 - zde pro WWW, resp. protokol HTTP
- princip fungování:
 1. WWW klient (browser) ve vnitřní síti pošle svůj požadavek (HTTP request) proxy bráně
 - jelikož ta nefunguje transparentně, musí být browser nastaven tak, aby „znal“ proxy bránu
 - a posílal příslušný požadavek proxy bráně, místo přímo cílovému serveru (to by neprošlo přes DMZ)
 2. proxy brána sama vygeneruje vlastní požadavek na cílový server
 3. proxy brána přijme odpověď cílového serveru
 4. proxy brána odpoví (předá odpověď) browseru ve vnitřní síti

obdobně se řeší
i další služby
(FTP, mail, DNS,)

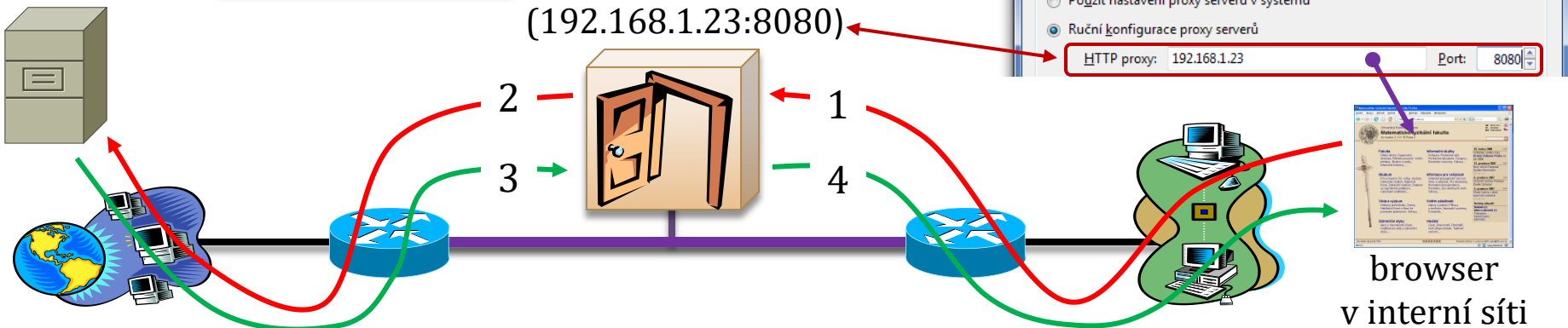
cílový
WWW
server

může fungovat i
jako HTTP cache

HTTP proxy
(192.168.1.23:8080)



browser
v interní síti

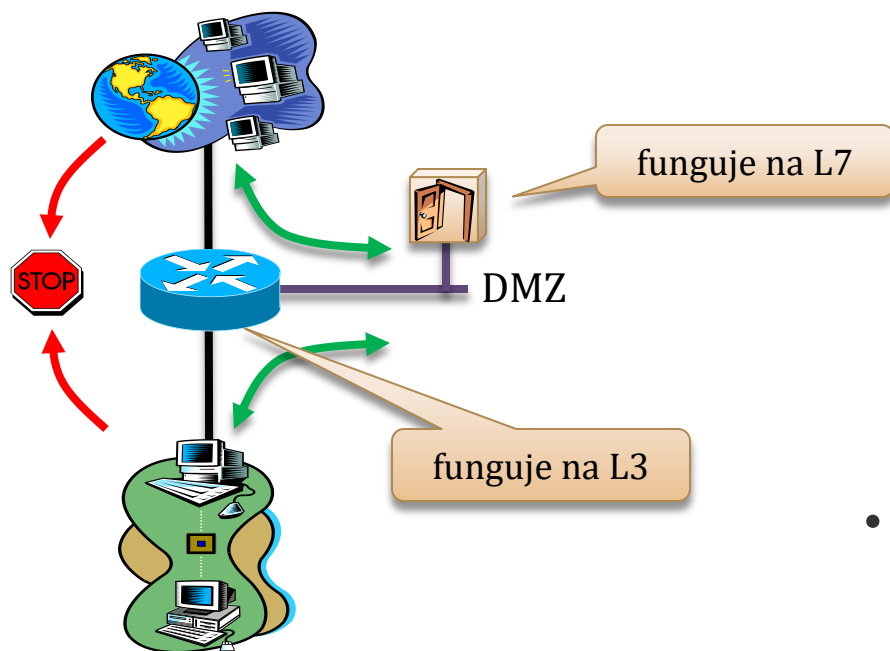


aplikační firewally (s proxy bránami)

- řešení se 2 směrovači je typické spíše pro větší firemní sítě

- lze vystačit i s 1 směrovačem

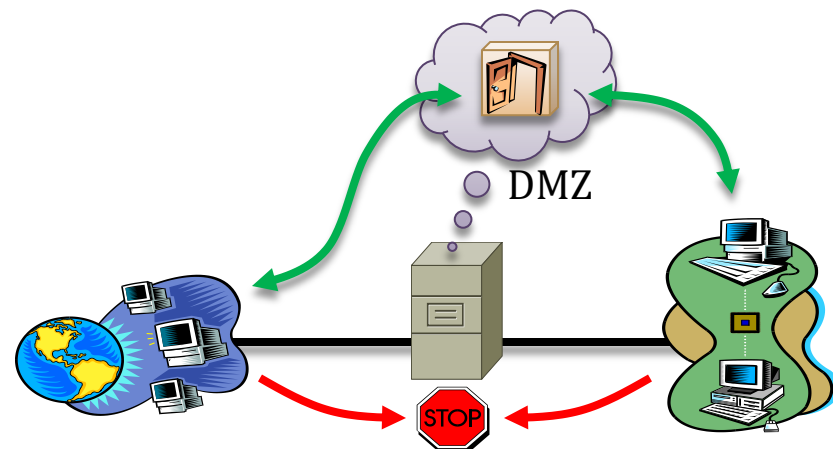
- který má síťová 3 rozhraní



- směrovač je nastaven tak, aby zakazoval „přímý průchod“ z vnější do vnitřní sítě
 - povolen je pouze takový provoz, který začíná či končí na tom rozhraní, které plní roli DMZ
 - kde mohou být umístěny proxy brány

- firewall na principu DMZ lze realizovat i bez směrovače

- DMZ se vytvoří v SW, v rámci uzlu který propojuje vnější a vnitřní síť



- společná vlastnost řešení s DMZ

- blokování funguje na síťové vrstvě (L3)

- povolování je řešeno na aplikační vrstvě (L7), pomocí proxy bran

- pro každou službu/aplikaci musí být jiná (specifická) proxy brána !!!

proto se také hovoří o **aplikačních firewallech**

paketové filtry

- **další možné řešení firewallů**

- **blokování i povolování se odehrává na úrovni síťové vrstvy (L3)**

- tedy na úrovni manipulace se síťovými pakety (např. IP pakety)
 - proto se takovéto řešení obecně označuje jako paketový filtr

- **možné varianty paketových filtrů:**

- **mohou fungovat na obou možných principech**

- „vše je zakázáno, něco je povoleno“ i „vše je povoleno, něco je zakázáno“
 - rozdíl je prakticky jen ve způsobu formulace pravidel pro blokování/povolení

- **mohou využívat (také) informace, dostupné na vyšších vrstvách**

- vychází především z informací, dostupných na L3 (adresa odesílatele, adresa příjemce, ...)
 - ale mohou se rozhodovat například i podle čísel portů (L4), případně i URL (L7) apod.

- **mohou fungovat na bezstavovém nebo stavovém principu**

- bezstavový paketový filtr posuzuje každý paket samostatně, bez ohledu na jiné pakety
 - bez ohledu na „historii“, reprezentovanou jinými (dříve přenesenými) pakety
 - nedokáže odhalit např. DOS a DDOS útoky, protože nevnímá „zvýšený souběh“ požadavků
- stavový paketový filtr bere ohled na historii (již přenesené pakety)
 - dokáže odhalit více nežádoucích situací (zejména různé souběhy)

- **může jít o běžný směrovač**

- s „posíleným“ operačním systémem, který zajišťuje funkce paketového filtru
- nebo o speciální jednoúčelové zařízení, či o běžný počítač s vhodným SW



SPI:
Statefull Packet
Inspection

ACL (Access Control List)

- **obecné označení pro „seznamy pravidel“, které specifikují konkrétní pravidla blokování či povolování**
 - jsou určeny hlavně pro firewally charakteru paketových filtrů
 - podle obsahu ACL se konkrétní paket buďto povolí (propustí), nebo zakáže (zastaví)
- **„standardní“ seznamy ACL**
 - jejich pravidla se ptají pouze na to, odkud paket přichází
 - zabývají se pouze L3 adresou jeho odesílatele (zdrojovou IP adresou)
 - neptají je, kam síťový paket směřuje
 - paketové filtry, které používají tyto (standardní) seznamy ACL, by měly být umístěny co nejbliže cílovým uzlům
- **„rozšířené“ seznamy ACL**
 - jejich pravidla se ptají i na další věci
 - např. na cílovou adresu, na číslo portu / druh služby, transportní protokol atd.
 - mohou být dále podmíněné např. denní dobou
 - paketové filtry, které používají tyto (rozšířené) seznamy ACL, se obvykle umísťují co nejbliže ke zdroji provozu

