Silicon Hill

Útoky a obrana proti nim

Václav Mach, 20. Listopad 2014

Úvod

- proč bychom se měli zabývat bezpečností?
- při práci se sítí obvykle uvažujeme ISO/OSI model
- ISO/OSI model byl vytvořen tak, aby jednotlivé vrstvy fungovaly nezávisle
- kompromitace nižší vrstvy znamená potenciální kompromitaci všech vyšších vrstev
- zabezpečení je pouze tak silné jako zabezpečení nejslabší vrstvy

ARP I

příklad: A chce komunikovat s B.

A má IP 192.168.1.1, B má IP 192.168.1.2.

- musím projít všechny vrstvy OSI/OSI, začínám na aplikační
- na L3 vyplním IP adresu zdroje a cíle
- na L2 vyplním MAC adresu zdroje
- protože jsem ještě s B nekomunikoval, neznám jeho adresu na L2
- nemůžu sestavit rámec - není kompletní

ARP II

Pro zjištění adresy B na L2 použiju protokol ARP.

ARP využívá broadcast na L2, tím je zajištěno, že ho uvidí všichni.

ARP request

- SRC: 00:A0:24:30:2E:13
- DST: **FF:FF:FF:FF:FF:FF**
- DATA: Who has 192.168.1.2? Tell 192.168.1.1

ARP reply

- SRC: **00:A0:24:30:4C:23**
- DST: 00:A0:24:30:2E:13
- DATA: I have 192.168.1.2

Budu ARP používat vždy, když chci komunikovat, abych mohl vyplnit MAC adresu cíle?

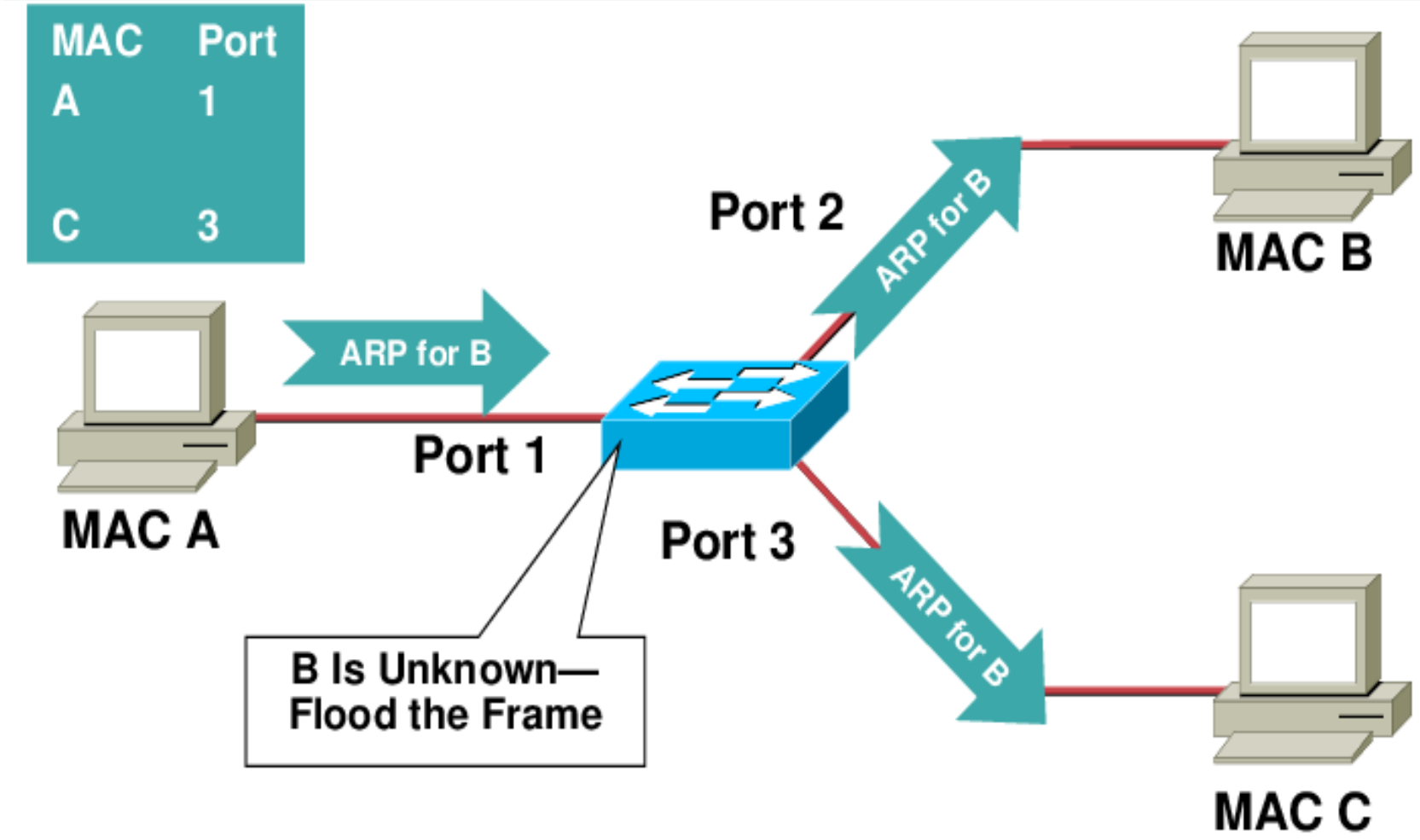
ARP III

Abych si mohl povídat zároveň s B i C, použiju přepínač.

Proces přepínání

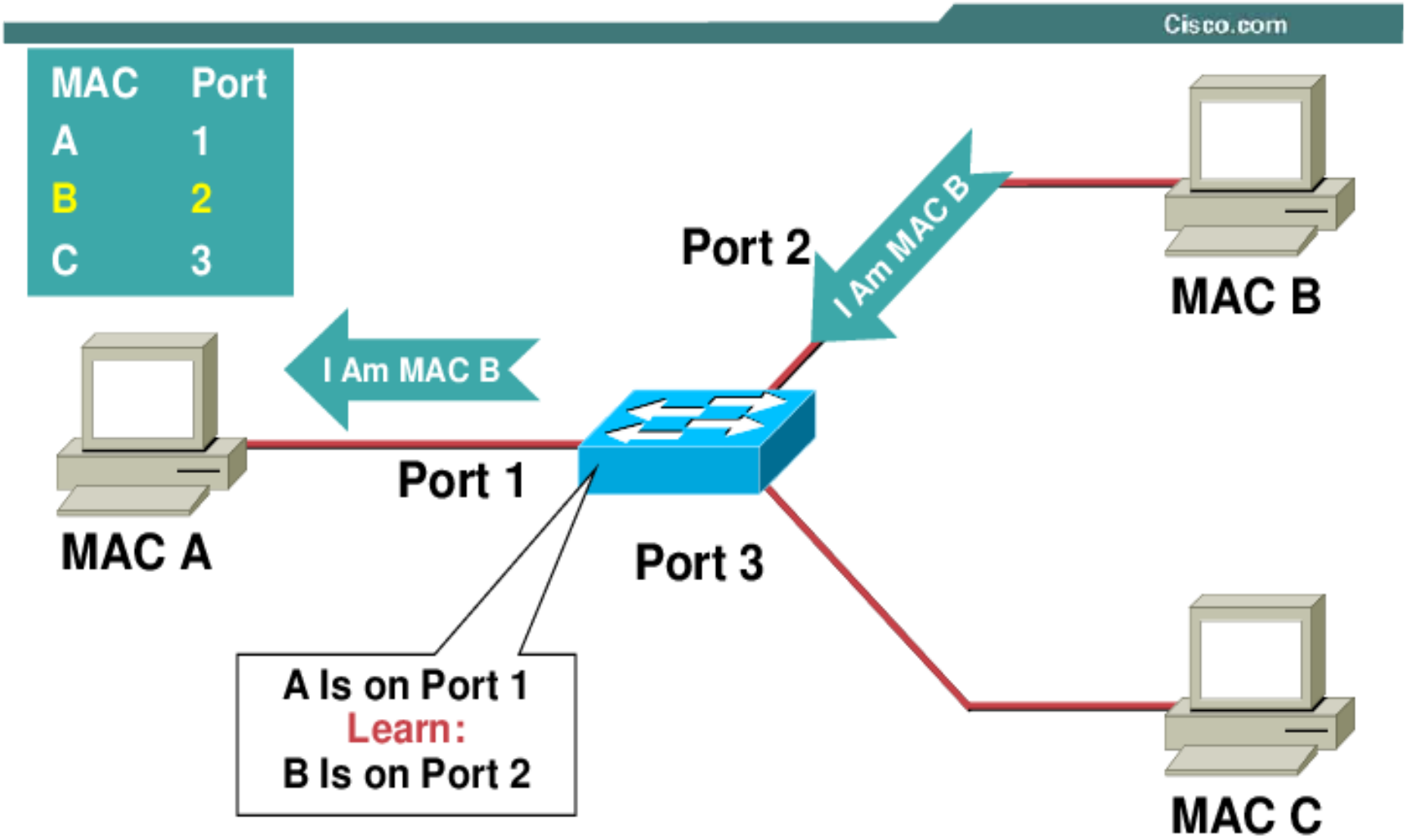
- příchozí rámec - do tabulky si zapíšu na jakém portu a adresu odesílatele
- pokud znám adresáta, pošlu na výstupní port
- broadcast je poslám na všechny porty, kromě portu odkud byl přijat
- co se stane, pokud neznám adresáta a nejde o broadcast?

Normal CAM Behavior 1/3



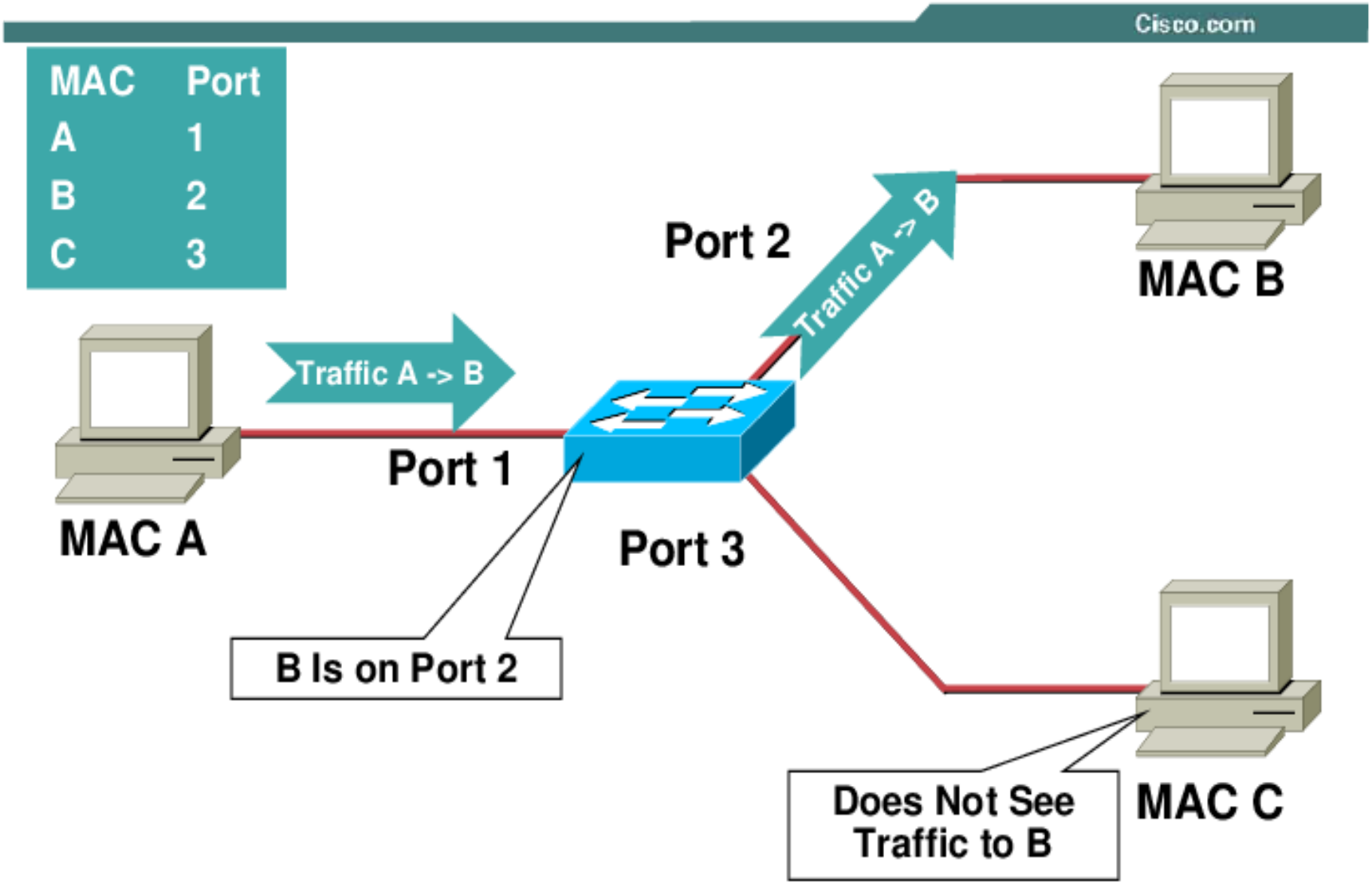
© 2005 Cisco Systems, Inc. All rights reserved.

Normal CAM Behavior 2/3



© 2005 Cisco Systems, Inc. All rights reserved.

Normal CAM Behavior 3/3



© 2005 Cisco Systems, Inc. All rights reserved.

Teorie ARP útoku

ARP flooding

- pouze v ipv4, v ipv6 NDP
- útočník podvrhne svou mac adresu a následně komunikuje do sítě
- podvržením docílí "otrávení" arp tabulky oběti
- některá zařízení akceptují odpověď bez předešlého požadavku
- cíle útoku: DoS, MitM, odposlech, ..

Teorie ARP útoku

ARP flooding

- pouze v ipv4, v ipv6 NDP
- útočník podvrhne svou mac adresu a následně komunikuje do sítě
- podvržením docílí "otrávení" arp tabulky oběti
- některá zařízení akceptují odpověď bez předešlého požadavku
- cíle útoku: DoS, MitM, odposlech, ..

DoS: Úspěšné odříznutí sítě od internetu pomocí ARPu, který oznamuje, že default gw je na neexistující L2 adrese.

MitM: Pro směrovač v lokální síti se utočník bude tvářit jako obět, pro obět se bude tvářit jako směrovač.

odposlech: ukážeme si

Setup & útok

Setup

- Cisco catalyst 2950
- (DHCP server)
- (Wireshark na koncových stanicích pro názornost)
- webserver pro názornost výsledku

Setup & útok

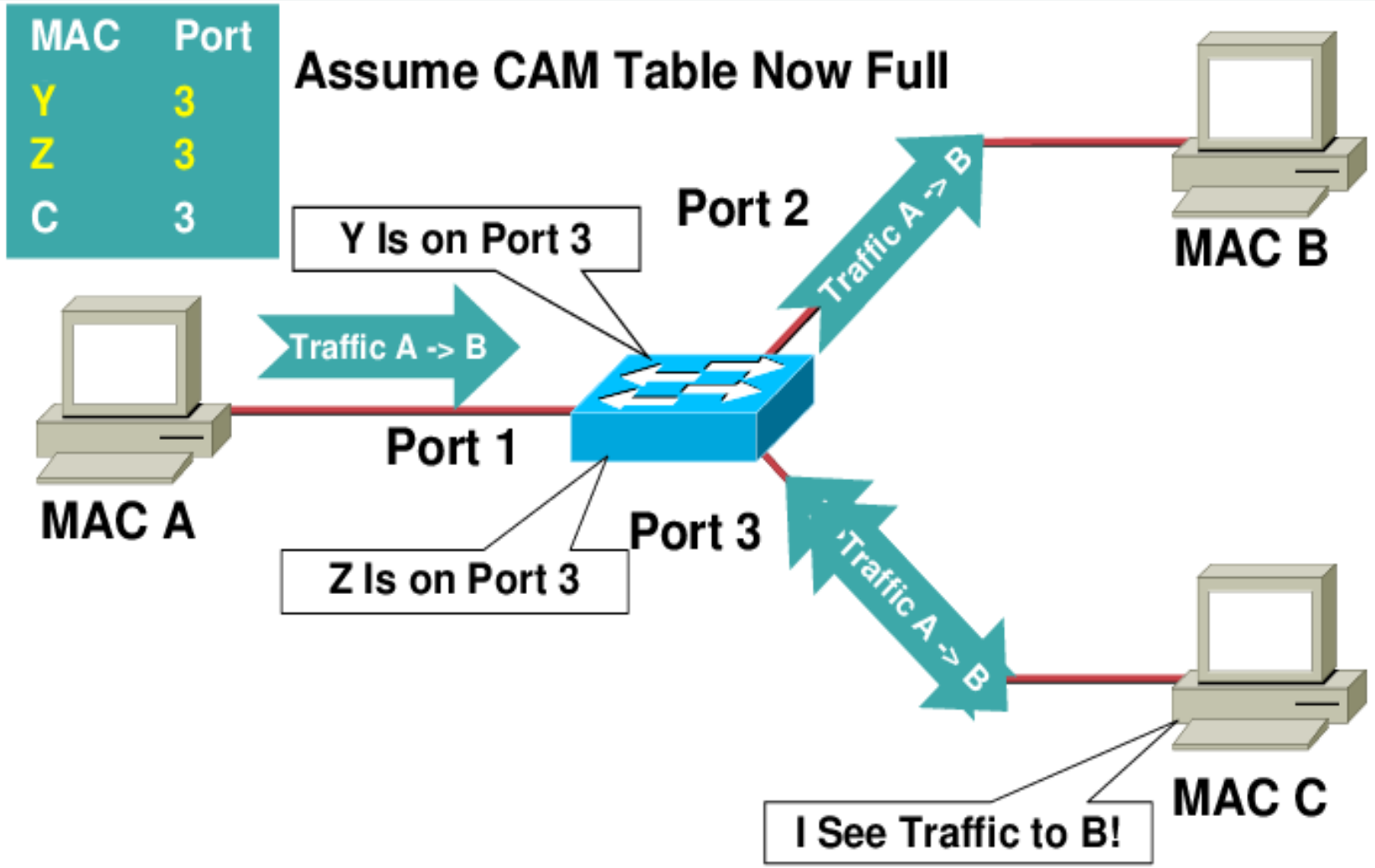
Setup

- Cisco catalyst 2950
- (DHCP server)
- (Wireshark na koncových stanicích pro názornost)
- webserver pro názornost výsledku

Útok

- útočník začně komunikovat z různých MAC adres
- dojde k zaplnění tabulky MAC adres přepínače
- rámce pro adresy, které přepínač nezná bude posílat všude

CAM Overflow 2/3



© 2005 Cisco Systems, Inc. All rights reserved.

Obrana

Koncové stanice

- statické arp tabulky, ignorování veškerých arp odpovědí
- je nutná dodatečná konfigurace, náročná údržba
- nepoužitelné pro dynamickou síť
- specializovaný sw pro obranu

Infrastruktura

- statické záznamy - manuální specifikace adresy na port
- dynamické záznamy - pomocí "sticky" security
- možnost konfigurace události při security-violation
- směrovače - dynamic arp inspection

DHCP I

Fáze přidělování adres

- DISCOVER - klient dává na vědomí svou existenci
- OFFER - server nabídne klientovi adresu
- REQUEST - klient požádá o nabízenou adresu
- ACK - server potvrdí žádost klienta

DHCP options - například dns servery, default gw, ..

DHCP starvation attack

Různé cíle útoku: MitM, podvržení DNS, ...

Setup

- Cisco catalyst 2950
- DHCP server
- (Wireshark na koncových stanicích pro názornost)

DHCP starvation attack

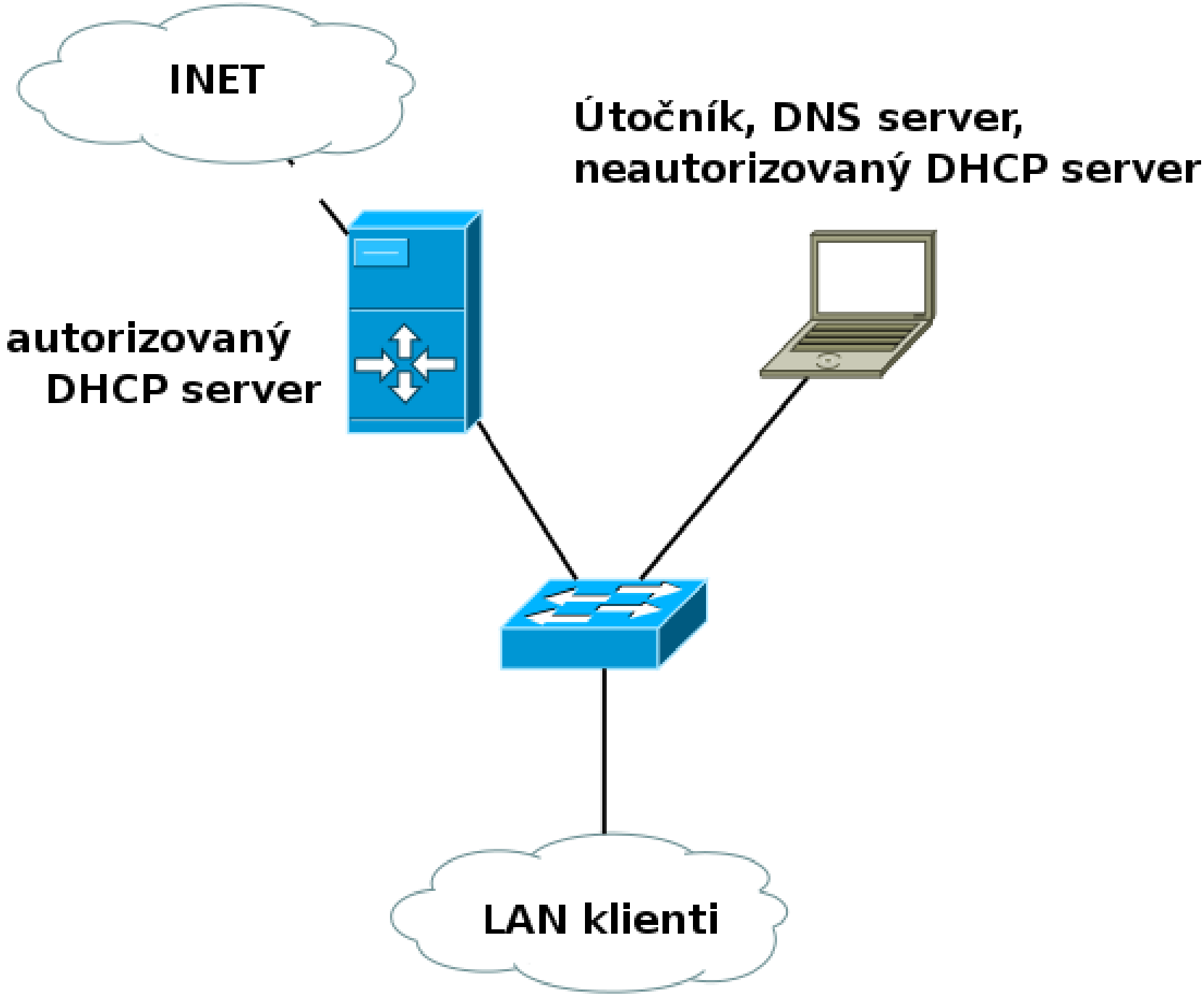
Různé cíle útoku: MitM, podvržení DNS, ...

Setup

- Cisco catalyst 2950
- DHCP server
- (Wireshark na koncových stanicích pro názornost)

Útok

- útočník vyčerpá celý rozsah přidělovaných adres - dojde k "zablokování" legitimního DHCP serveru
- vytvoří vlastní neautorizovaný dhcp server
- dále může distribuovat informace klientům na základě cíle útoku
- z velké části závislé na správném načasovaní vzhledem k lease time


INET
Útočník, DNS server,
neautorizovaný DHCP server
autorizovaný
DHCP server
LAN klienti

Obrana

- port-security - obdobně jako v předchozím případě
- DHCP snooping - definujeme, které porty jsou trusted
- na non-trusted portech jsou odpovědi od DHCP serverů zahazovány