Switching Features and Technologies for the Campus Network

CCNP SWITCH: Implementing Cisco IP Switched Networks

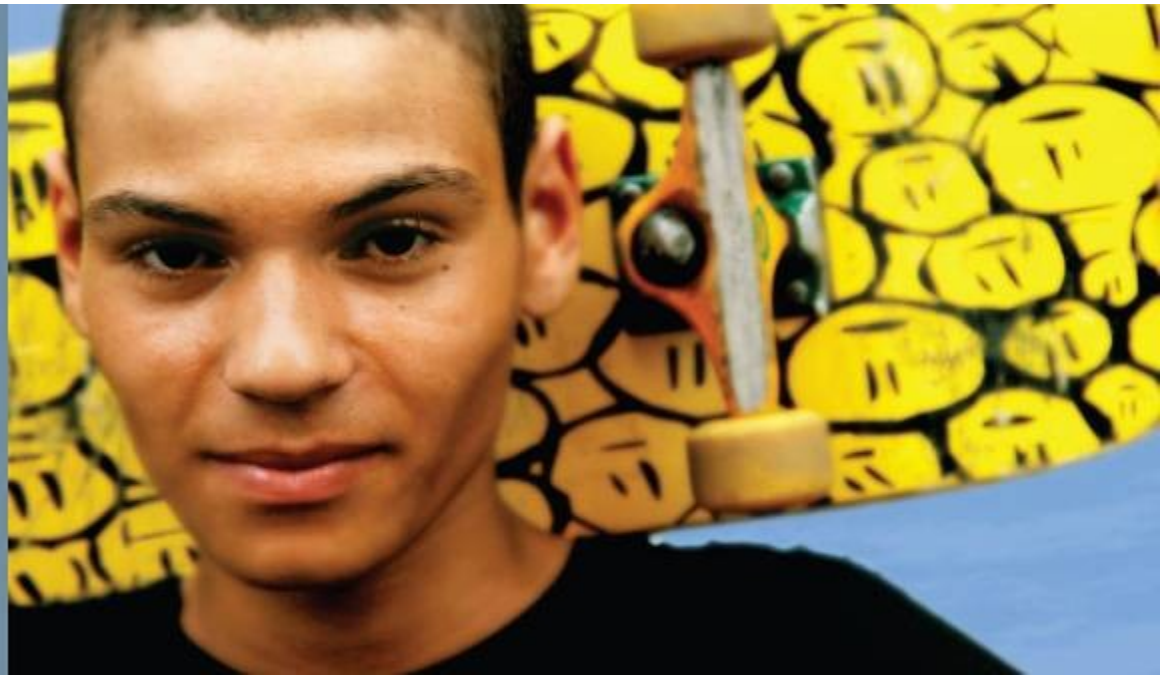
Cisco | Networking Academy®
Mind Wide Open™

Cíle kapitoly 8

Tato kapitola je věnována následujícím vlastnostem přepínačů:

- Discovery protocols
- Unidirectional Link Detection
- Power over Ethernet
- SDM templates
- Monitoring features
- IP SLA

Discovery Protocols



Discovery protokoly

Tato část kapitoly pokrývá:

- Úvod do LLDP a srovnání s CDP
- Základní konfigurace LLDP
- Vyhledání sousedů za pomoci LLDP

Úvod do LLDP

- LLDP je průmyslový standard pro objevování sousedů.
- Všechny aktuální Cisco zařízení vyjma těch zastaralých či okrajových podporují LLDP.
- Zprávy LLDP se nepřeposílají.

	CDP	LLDP
Standard	No, Cisco proprietary	Defined as IEEE 802.1AB
Runs at	Layer 2: Data link layer	Layer 2: Data link layer
Benefits	Lightweight, may contain Cisco-specific information	Highly customizable

Úvod do LLDP

Tento protokol může inzerovat podrobnosti, jako jsou informace o konfiguraci, možnosti zařízení, adresa IP, název hostitele a identita zařízení.

- LLDP se používá pro nepřeberné množství informací, není vytvořen pro odesílání informací v reálném čase, jako jsou data o výkonu nebo data čítače.
- Výhodou LLDP nad CDP je, že umožňuje kastomizaci. LLDP může nést mnoho informací, které jsou relevantní pro vaši síť.
- Jednou nevýhodou LLDP ve srovnání s CDP je, že není příliš triviální.

Úvod do LLDP

Následující seznam zachycuje několik důležitých implementačních vlastností LLDP:

- LLDP je jednosměrný.
- LLDP funguje pouze v reklamním (advertising) režimu.
- LLDP nevyžaduje monitorování změn stavu mezi uzly LLDP.
- LLDP využívá multicastový rámec Layer 2 k informování sousedů o sobě a jeho vlastnostech.
- LLDP přijímá a zaznamenává všechny informace, které obdrží o svých sousedech.
- LLDP používá 01: 80: c2: 00: 00: 0e, 01: 80: c2: 00: 00: 03 nebo 01: 80: c2: 00: 00: 00 jako cílovou adresu MAC multicast vysílání.

Vyměňované informace pomocí LLDP

Následující seznam definuje nejběžnější informace vyměňované s LLDP s přepínači kampusu:

- Název systému a popis
- Název portu a popis
- Porty VLANů a název VLAN
- Management IP adresy
- Možnosti systému (Wi-Fi, směrování, přepínání atd.)
- Napájení přes Ethernet
- Agregace spojení

Konfigurace LLDP

- CDP je v defaultním nastavení povoleno na všech zařízeních Cisco, ale LLDP může být ve výchozím nastavení povoleno nebo zakázáno v závislosti na hardwarové platformě a verzi softwaru.
- Chcete-li povolit LLDP v zařízení, použijte příkaz **lldp run** v režimu globální konfigurace. Pro zákaz používejte **no run lldp**.
- Chcete-li zakázat LLDP na konkrétním rozhraní, je třeba dát na všech rozhraních **no lldp receive** a **no lldp transmit**. Defaultně ale tyto příkazy neuvidíte.

Konfigurace LLDP

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# lldp run

Switch# show lldp

Global LLDP Information:
    Status: ACTIVE
    LLDP advertisements are sent every 30 seconds
    LLDP hold time advertised is 120 seconds
    LLDP interface reinitialization delay is 2 seconds

Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface GigabitEthernet 0/1
Switch(config-if)# no lldp transmit
Switch(config-if)# lldp receive
Switch(config-if)# end

Switch# show running-config interface GigabitEthernet 0/1
Building configuration...

Current configuration : 60 bytes
!
interface GigabitEthernet0/1
 duplex auto
 no lldp transmit
end
```

Sousedé LLDP

```
CCNP-Switch1# show lldp neighbors
Capability codes:
    (R) Router, (B) Bridge, (T) Telephone, (C) DOCSIS Cable Device
    (W) WLAN Access Point, (P) Repeater, (S) Station, (O) Other

Device ID           Local Intf     Hold-time  Capability      Port ID
CCNP-Switch2    Fa0            120        B               Eth106/1/14

Total entries displayed: 1

CCNP-Switch1# show lldp neighbor detail
------------------------------------------------
Chassis id: 68ef.bd54.abcf
Port id: Eth106/1/14
Port Description: Ethernet106/1/14
System Name: CCNP-Switch2.cisco.com

System Description:
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.

Time remaining: 118 seconds
System Capabilities: B
Enabled Capabilities: B
Management Addresses:
    IP: 10.1.28.18
Auto Negotiation - not supported
Physical media capabilities - not advertised
Media Attachment Unit type - not advertised
Vlan ID: 46
```

Informace o provozu pomocí LLDP

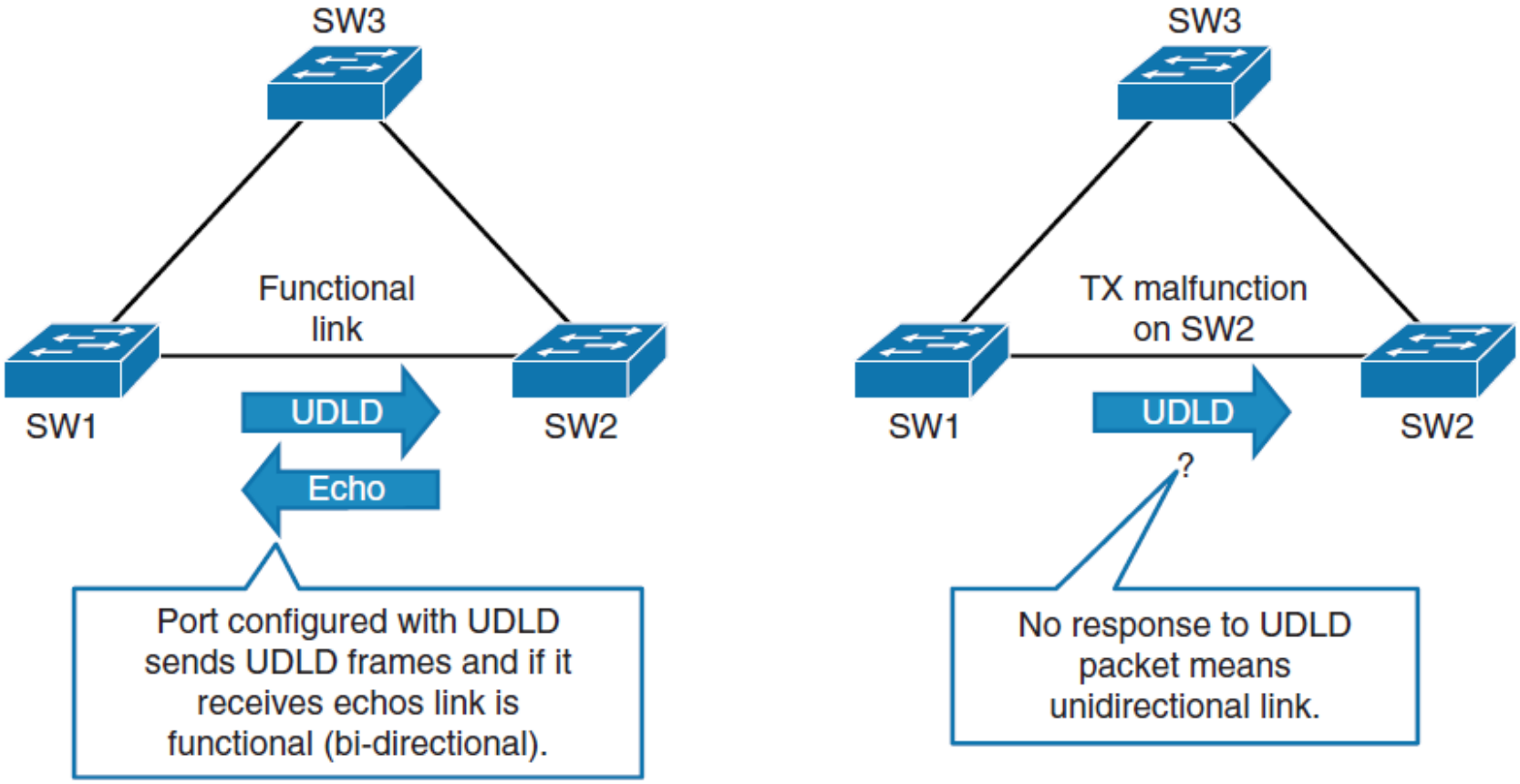
```
Switch1# show lldp traffic

LLDP traffic statistics:
    Total frames out: 42
    Total entries aged: 0
    Total frames in: 11
    Total frames received in error: 0
    Total frames discarded: 1
    Total TLVs unrecognized: 0
```

Klíčové vlastnosti LLDP

- LLDP umožňuje aplikacím správy sítě automaticky vyhledávat a dozvědět se o síťových zařízeních.
- LLDP je průmyslová standardní alternativa k CDP.
- LLDP podporuje povolit nebo zakázat přenosové nebo přijímací schopnosti na portu.
- Pro zobrazení sousedů LLDP použijte příkaz **show lldp neighbors [detaily].**

Jednosměrná tetekce linky (Unidirectional Link Detection)

UDLD


SW3
Functional
link
SW1
UDLD
SW2
Echo
Port configured with UDLD
sends UDLD frames and if it
receives echos link is
functional (bi-directional).
SW3
TX malfunction
on SW2
SW1
UDLD
SW2
?
No response to UDLD
packet means
unidirectional link.

UDLD

- The unidirectional condition at Layer 2 is disastrous for any network because it will lead to either spanning tree not blocking on a forwarding port or a routing black hole.
- In either of these situations, the network will exhibit a total failure, become instable, and eventually create a complete loss of connectivity for end users.
- UDLD may protect the network from the following problems:
  - Transient hardware condition
  - Hardware failure
  - Optic/GBIC anomalous behavior or failure
  - Miswired cabling
  - Software defect or condition
  - Misconfigured or malfunction of inline tap or sniffer

UDLD Mechanisms and Specifics

- UDLD is supported on all current Cisco Catalyst and Nexus switches.
- UDLD functions by transmitting Layer 2 packets to the well-known MAC address 01:00:0C:CC:CC:CC.
- If the packets are not echoed back within a specific time frame, the link is flagged as unidirectional.
- Devices on both ends of the link must support UDLD for the protocol to successfully identify and disable unidirectional links.
- UDLD messages are sent at regular intervals.
  - This timer can be modified.
  - The default setting varies between platforms; however, the typical value is 15 seconds.

UDLD Behavior

- The behavior of UDLD after it detects a unidirectional link is dependent on its operation mode, either normal mode or aggressive mode. The modes are described as follows:
  - **Normal mode**
    - When a unidirectional link is detected the port is allowed to continue its operation. UDLD just marks the port as having an undetermined state. A syslog message is generated.
  - **Aggressive mode**
    - When a unidirectional link is detected the switch tries to reestablish the link. It sends one message a second, for 8 seconds. If none of these messages are sent back, the port is placed in error-disabled state.

UDLD Configuration

- To configure a Cisco Catalyst switch for UDLD normal mode, use the **`udld enable`** command.
- Similarly, to enable UDLD in aggressive mode, use the **`udld aggressive`** keyword.
- To display the UDLD status for the specified interface or for all interfaces, use the **`show udld`** [*`interface slot/number`*] privileged EXEC command.
- To view UDLD neighbors, use the **`show udld neighbors`** .
- In addition, use **`udld reset`** command to reset all the interfaces that were shut down by UDLD.
  - You can also achieve a UDLD reset by first shutting down the interface and then bringing it back up (that is, **`shut`** , then **`no shut`**).

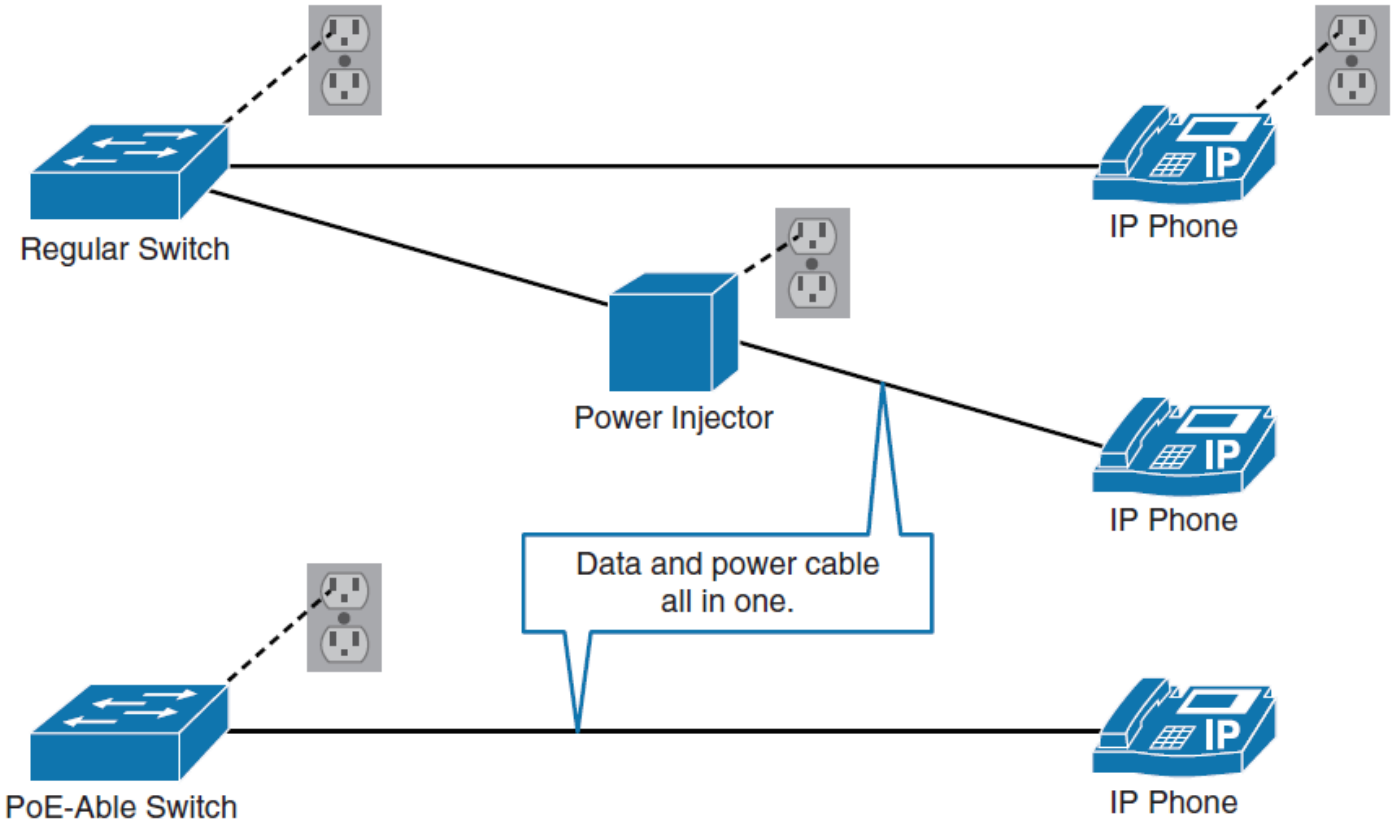
Loop Guard and UDLD Functionality Comparison

Functionality	Loop Guard	UDLD
Configuration granularity	Per-VLAN	Per-Port
Protection against STP failures caused by unidirectional links	Yes, when enabled on all non-designated ports in a redundant topology.	Yes, when enabled on all ports in the topology
Protection against STP failures that are caused by software anomalies, resulting in switches not sending bridge protocol data units (BDPUs)	Yes	No

Power over Ethernet

Power over Ethernet

- Power over Ethernet (PoE) zajišťuje zásobení proudem prostřednictvím datového kabelu.



Výhody PoE

- PoE přepínače podporují vzdálenou správu, kde napájecí adaptéry a injektory nemají.
- PoE přepínače umožňují centralizované metody zálohování.
- PoE vyžaduje méně konfigurace než lokální napájecí adaptér nebo injektor.
- PoE využívá infrastrukturu datové kabeláže – není nutný žádný další napájecí kabel, jako je tomu v případě napájecích adaptérů nebo injektorů.

Komponenty PoE

Terminologie PoE označuje tři typy komponent:

- Přepínače Cisco Catalyst a výkonové injektory
- Napájená zařízení
  Přístupové body, IP telefony a IP kamery.
  Tencí klienti, senzory, nástěnné hodiny a tak dále.
  Dokonce i přepínače mohou být napájeny samotným PoE.
- Kabely Ethernetu.
  Stejně jako u standardního Ethernetu je vzdálenost PoE omezena na 100 metrů s kabeláží kategorie 5.

Standardy PoE

IEEE 802.3af (ratifikováno 2003)

- Tato norma poskytuje interoperabilitu mezi různými dodavateli.
- Pro každé napájené zařízení je k dispozici až 15,4 W stejnosměrného proudu.

IEEE 802.3at (ratifikováno v roce 2009)

- Tento standard je vylepšením oproti standardu 802.3af a může poskytovat výkonná zařízení s výkonem až 25,5 W.
- Toto číslo může být zvýšeno na 50 W a více s implementacemi, které jsou mimo standard.
- Tento standard je také známý jako PoE + nebo PoE Plus.

Vyjednávání PoE

- Přepínače Cisco neposkytují napájení portu, pokud nezjistí potřebu koncového zařízení. To zabraňuje plýtvání zbytečnou energií a tak dále.
- S 802.3af a 802.3at se přepínač pokouší detekovat napájené zařízení dodáváním malého napětí přes ethernetový kabel.
- Přepínač pak měří odpor. Pokud je naměřený odpor 25 kΩ, je k dispozici napájené zařízení.
- Napájené zařízení může poskytnout přepínač s informacemi o třídě výkonu.
- Výchozí třída 0 se používá, pokud přepínač nebo napájené zařízení nepodporuje zjišťování výkonu

Třídy PoE

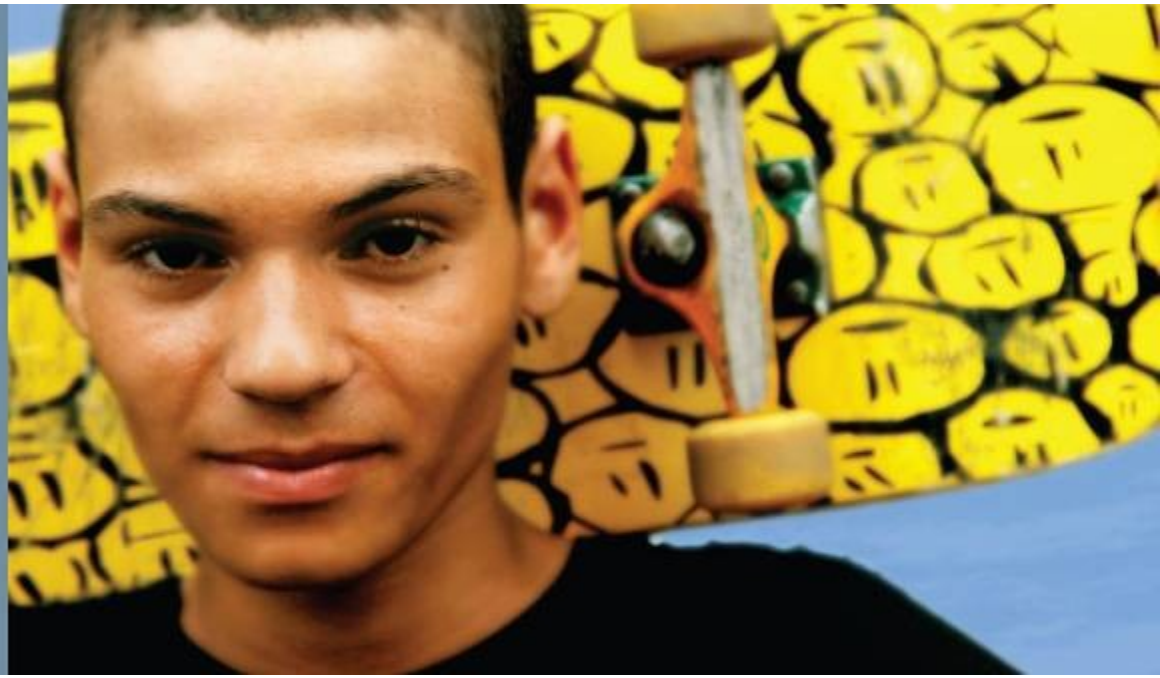
IEEE Power Class	Min. Power Output	Notes
0	15.4 W	Default class
1	4 W	Optional class
2	7 W	Optional class
3	15.4 W	Optional class
4	51 W	Valid for 802.3at devices only (that is, thin clients)

Původní metoda **Cisco Inline Power** má jiný způsob vyjednávání než oba standardy IEEE. Přepínač vysílá testovací tón **340 kHz** na ethernetovém kabelu. Tón je vysílán místo stejnosměrného napájení, protože spínač musí nejprve detekovat zařízení před jeho napájením. Nejvhodnější úroveň výkonu je pak určena výměnou informací CDP. Přepínač zjistí typ zařízení (například IP telefon Cisco) a požadavky na napájení zařízení.

Konfigurace a verifikace PoE

```
Switch(config-if)# power inline {auto | never}
! Configures the switch port to automatically negotiate inline power levels or to
  turn off PoE
Switch# show power inline
Module          Available                    Used                 Remaining
                  (Watts)                   (Watts)               (Watts)
---------      -----------                ----------           -----------
1                 420.0                       92.4                  327.6
Interface      Admin    Oper      Power   Device             Class      Max
                                  (Watts)
-----------  ------    -----     ------  ----------------   ------     -----
Gi1/0/1        auto     off         0.0   n/a                  n/a       15.4
Gi1/0/2        auto     on         15.4   AIR-LAP1142N-E-K9      3       15.4
Gi1/0/3        auto     on         15.4   AIR-LAP1142N-E-K9      3       15.4
Gi1/0/4        auto     on         15.4   AIR-LAP1142N-E-K9      3       15.4
Gi1/0/5        auto     on         15.4   AIR-LAP1142N-E-K9      3       15.4
Gi1/0/6        auto     on         15.4   AIR-LAP1142N-E-K9      3       15.4
Gi1/0/7        never    off         0.0   n/a                  n/a       15.4
<...output omitted>
! Displays information about PoE on a switch
```

Šablony (templates) SDM



Šablony SDM (Switching Database Manager)

Po dokončení této sekce na šablonách služby SDM budete moci provést následující:

- popsat typické typy šablony SDM
- změnit šablonu SDM
- popsat bezpečnostní opatření, která je třeba učinit při změně šablony SDM

Šablony SDM upravují systémové prostředky, například CAM a TCAM.

Příklad

Nejběžnější výchozí modifikací akce SDM je nasazení kombinace protokolu IPv4 a protokolu IPv6 (duální zásobník), protože funkce IPv6 není s výchozí šablonou podporována.

Typy šablon SDM

Defaultní

Výchozí šablona. Tato šablona poskytuje mix tras pro unicast směry, connocted a host tras.

Routing

tuto šablonu zvolte, pokud zařízení provádí směrování v distribuční části sítě nebo jádru sítě. Zařízení je schopno přenášet mnoho tras, ale pouze pro IPv4.

Access

Tuto šablonu povolíte, pokud máte mnoho VLAN. Tato šablona zase redukuje zdroje alokované pro směrování.

Typy šablon SDM

VLAN

Použijete ji, pokud máte velké podsítě s mnoha adresami MAC.

Dual IPv4 and IPv6

Tuto šablonu povolíte, pokud chcete zapnout možnosti zařízení IPv6. Při povolení této šablony musíte vybrat mezi defaultním nastavením, směrováním a sítí VLAN:

default
Další prostor je vyhrazen pro směrování a zabezpečení protokolu IPv6. Pro unicast vrstvy 2 je méně rezervovaného prostoru.

routing
Více místa je vyhrazeno pro směrování IPv6 než směrování IPv4.

VLAN
Vhodné pro použití v prostředí s dvojitým stackem se spoustou VLAN.

Zobrazení zdrojů SDM

```
Switch# show sdm prefer
 The current template is "desktop default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  6K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    8K
  number of directly-
  number of indirect
  number of IPv4 poli
  number of IPv4/MAC
  number of IPv4/MAC
```

```
Switch# show sdm prefer
 The current template is "desktop IPv4 and IPv6 default" template.
 The selected template optimizes the resources in
 the switch to support this level of features for
 8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                  2K
  number of IPv4 IGMP groups + multicast routes:    1K
  number of IPv4 unicast routes:                    3K
  number of directly-connected IPv4 hosts:          2K
  number of indirect IPv4 routes:                   1K
  number of IPv6 multicast groups:                  1.125k
  number of directly-connected IPv6 addresses:      2K
```

Výběr té pravé šablony SDM

- Doporučujeme změnit šablonu SDM pouze tehdy, máte-li k tomu dobrý důvod.
- Před změnou šablony prozkoumejte, zda je změna nutná, nebo zda je to jen řešení pro špatné volby návrhu.
- Jako další osvědčený postup vždy prozkoumejte množství používaných systémových prostředků, než začnete uvažovat o změnách šablony SDM.
- Chcete-li ověřit, kolik prostředků systému je používáno, použijte příkaz **show platform tcam utilization**.
- Pokud se využití TCAM blíží maximu pro některý z parametrů, zkontrolujte, zda některá z dalších funkcí šablony nemůže optimalizovat tento parametr:

  show sdm prefer {access | default | dual-ipv4-a-ipv6 | routing | vlan}.
- Dalším běžným důvodem pro změnu šablony SDM je skutečnost, že se vám nedostává určitého zdroje. *Např, použití přepínače ve velké doméně vrstvy 2 s mnoha ACL může vyžadovat změnu šablony na access* SDM.

Závěr

- Chcete-li ověřit, kolik prostředků je používáno, použijte příkaz **show show platform tcam**.
- Chcete-li ověřit šablonu SDM, která je právě používána, použijte příkaz **show sdm prefer**.
- Chcete-li změnit šablonu na duální zásobník, použijte příkaz **sdm prefer dual-ipv4-and-ipv6 default**.
- Při změně šablony SDM je nutné přepínač znovu reloadnout.

Monitoring

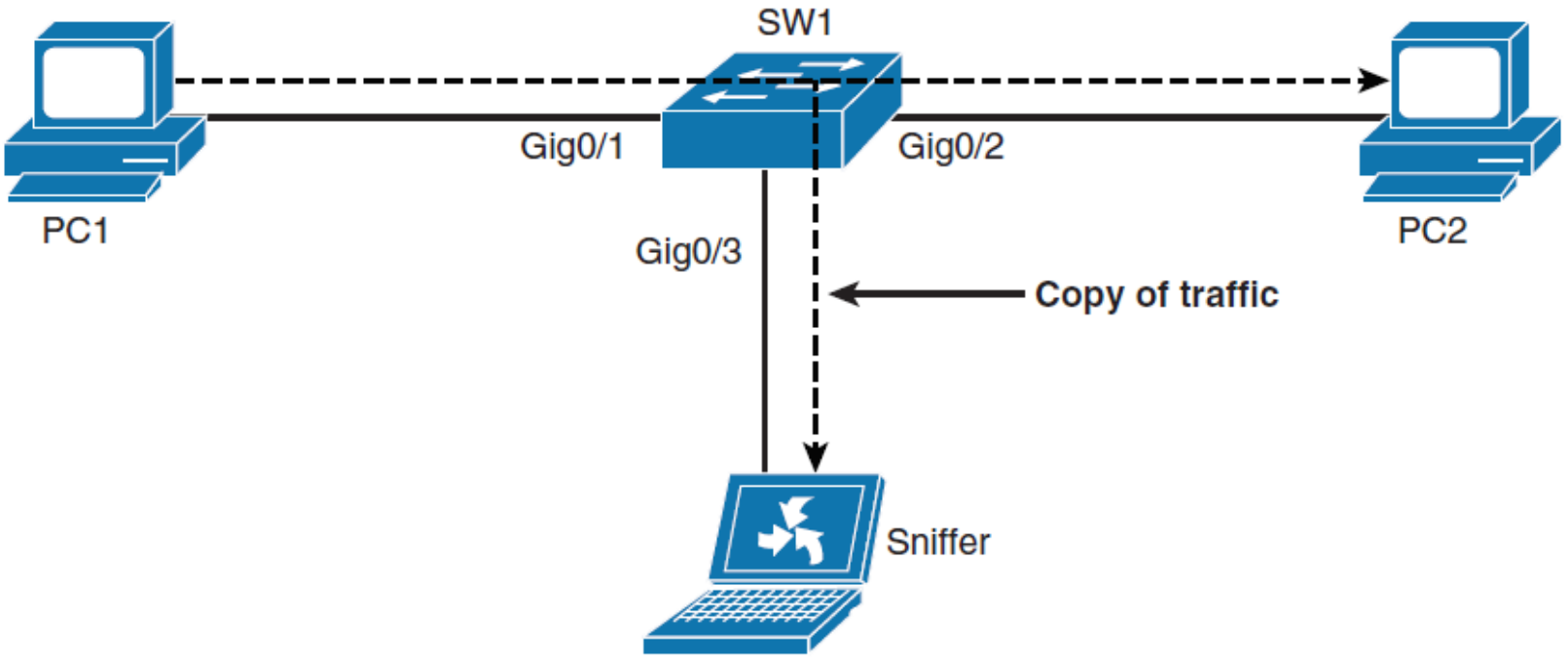
Vlastnosti monitoringu

Po dokončení této lekce budete schopni splnit tyto cíle:

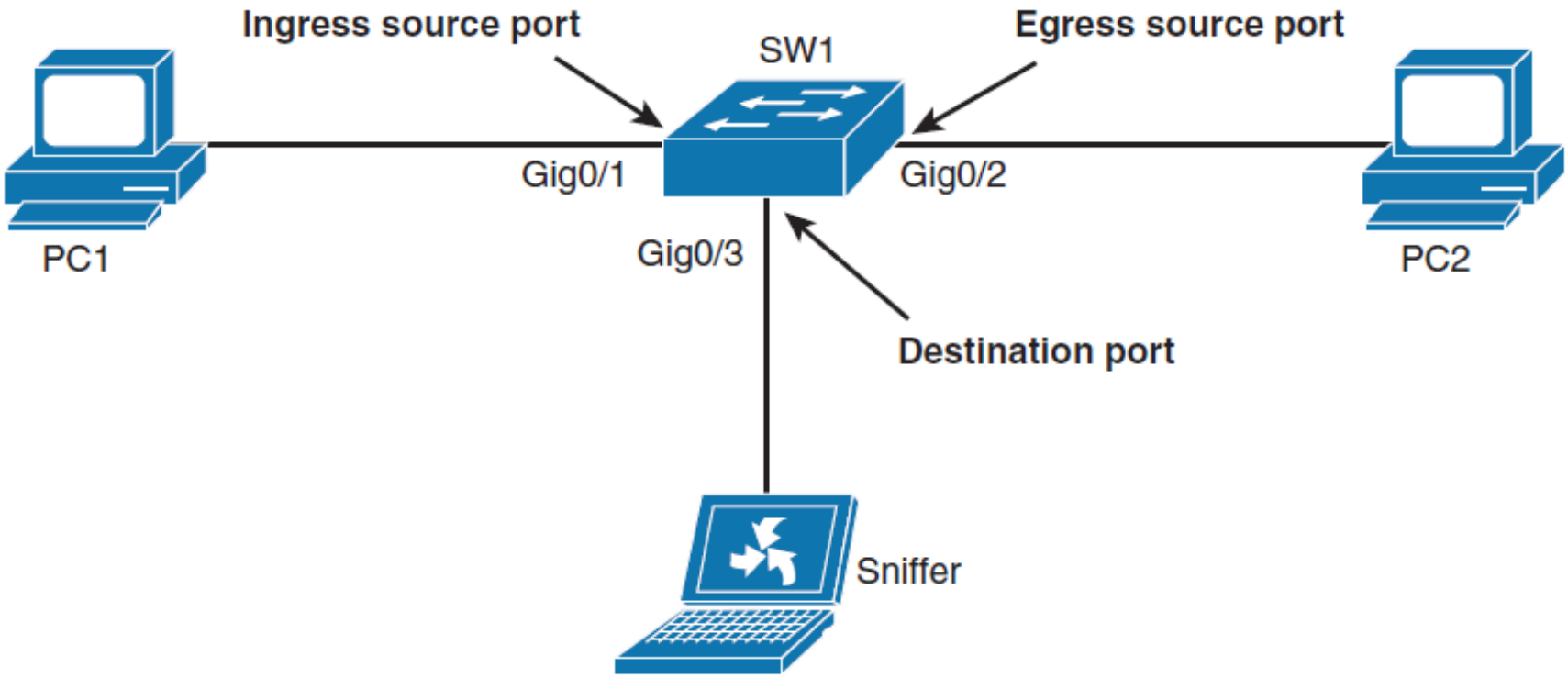
- popsat SPAN
- popsat terminologii SPAN
- popsat různé verze SPANu
- nakonfigurovat SPAN
- ověřit lokální konfiguraci SPAN
- nakonfigurovat RSPAN
- zkontrolovat konfiguraci RSPAN

Přehled SPAN a RSPAN

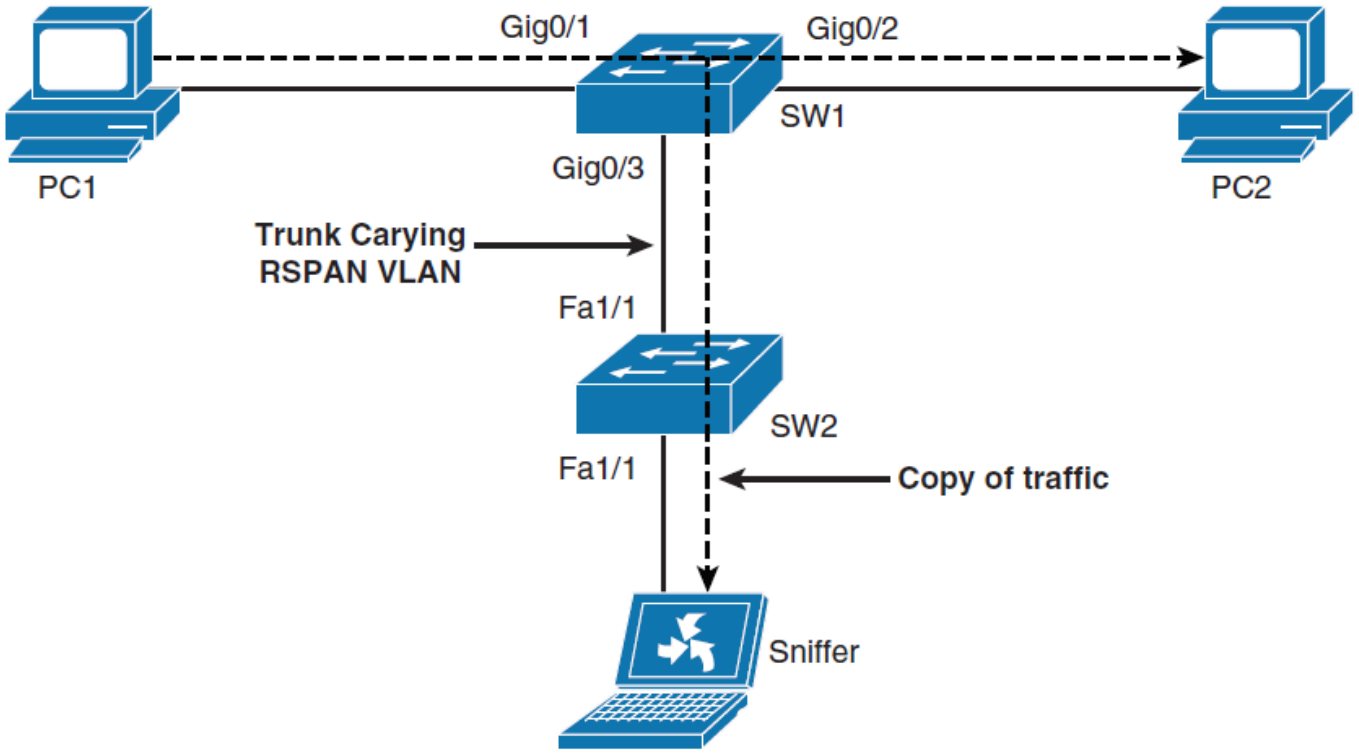
- **SPAN session:** Asociace zdrojového portu s cílovým.
- **Source VLAN:** monitoring VLAN.



Terminologie SPAN



Přehled Remote SPAN



- Vzdálený SPAN podporuje zdrojové a cílové porty na různých přepínačích, zatímco místní SPAN podporuje pouze zdrojové a cílové porty na stejném přepínači.

Složení RSPAN

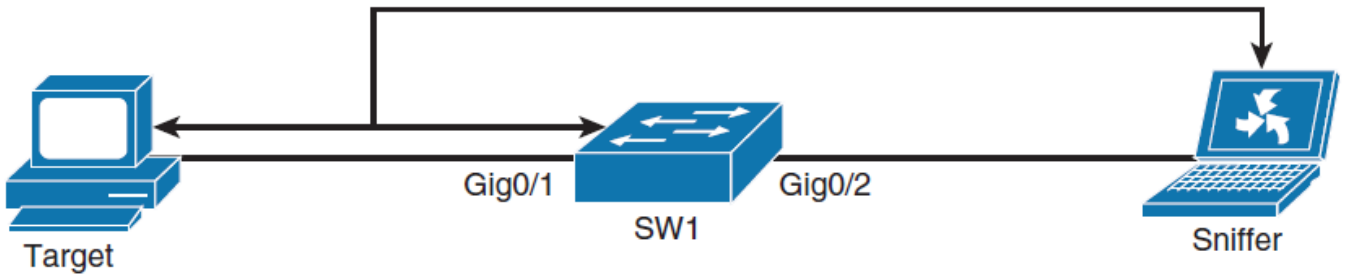
- RSPAN source session
- RSPAN VLAN
- RSPAN destination session

SPAN dodržuje následující pravidla

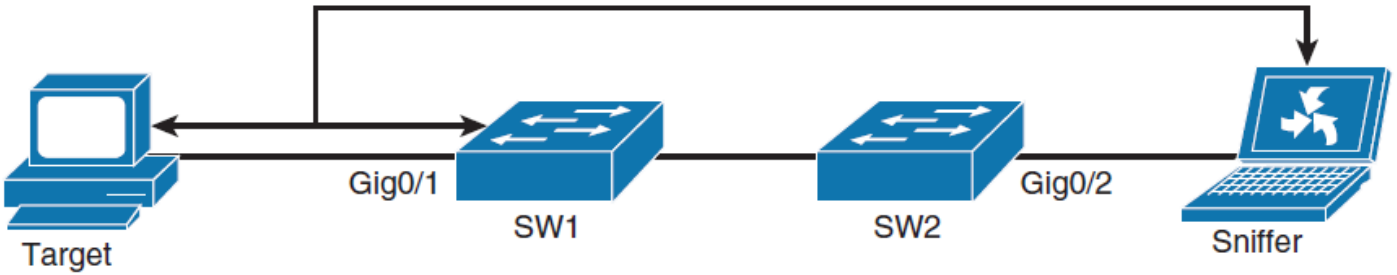
- Cílový port nemůže být zdrojový port nebo naopak.
- Počet cílových portů je závislý na platformě; některé platformy umožňují více než jeden cíl.
- Cílové porty nepůsobí jako normální porty a neúčastní se spanning stromu a tak dále.
- cílovým místem protéká normální provoz. Dávejte pozor, abyste k cílovému portu SPAN nepřipojovali kromě koncového zařízení nic dalšího.

Konfigurace SPAN

```
Switch1(config)# monitor session 1 source interface GigabitEthernet 0/1
Switch1(config)# monitor session 1 destination interface GigabitEthernet 0/2

Switch1# show monitor

Switch# show monitor
Session 1
---------
Type                   : Local Session
Source Ports           :
    Both               : Gi0/1
Destination Ports      : Gi0/2
    Encapsulation      : Native
          Ingress      : Disabled
```

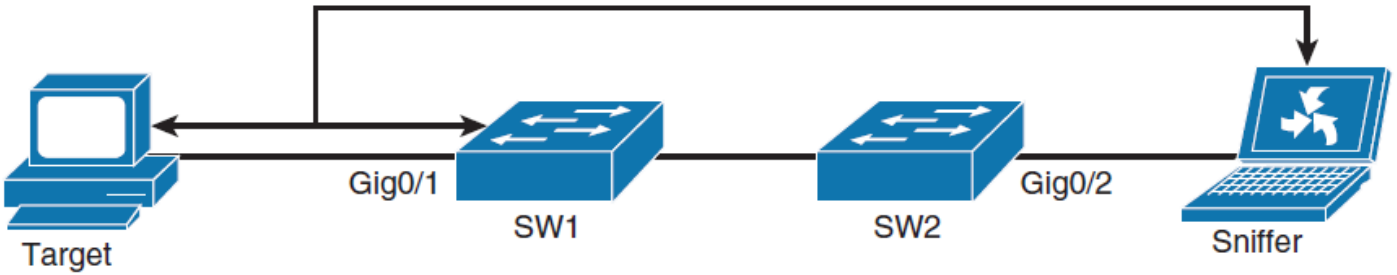


Konfigurace RSPAN 1/2



- SW1(config)# **vlan 100**
- SW1(config-vlan)# **name RSPAN-VLAN**
- SW1(config-vlan)# **remote-span**
- SW1(config-vlan)# **exit**
- SW1(config)# **monitor session 2 source interface Giga0/1**
- SW1(config)# **monitor session 2 destination remote vlan 100**

Konfigurace RSPAN 2/2



- `SW2(config)# vlan 100`
- `SW2(config-vlan)# name RSPAN-VLAN`
- `SW2(config-vlan)# remote-span`
- `SW2(config-vlan)# exit`
- `SW2(config)# monitor session 2 destination interface Giga 0/2`
- `SW2(config)# monitor session 2 source remote vlan 100`

Verifikace RSPAN

```
SW1# show monitor

Session 2
---------
Type                   : Remote Source Session
Source Ports           :
    Both               : Gi0/2
Dest RSPAN VLAN        : 100


SW2# show monitor



---------
Type                   : Remote Destination Session
Source RSPAN VLAN      : 100
Destination Ports      : Gi0/2
    Encapsulation      : Native
          Ingress      : Disabled
```

IP SLA

Cíle podkapitoly IP SLA

Po dokončení této části budete rozumět následujícím:

- Základní použití IP SLA
- Co je zdrojem a responderem protokolu IP SLA
- Základní příklad konfigurace protokolu ICMP IP SLA a konfigurace UDP

Úvod do IP SLA

- SLA (service level agreement) je smlouva mezi poskytovatelem sítě a jejími zákazníky nebo mezi oddělením sítě a interními firemními zákazníky. Poskytuje zákazníkům záruku o úrovni uživatelské zkušenosti.
- SLA může obsahovat specifika o dohodách o připojení a výkonu služby koncového uživatele od poskytovatele služeb.
- SLA obvykle popisuje minimální úroveň služby a očekávanou úroveň služby.

Úvod do IP SLA

- SLA lze také použít jako základ pro plánování rozpočtů a pro zdůvodnění výdajů na síť.
  Celkově lze říci, že funkce IP SLA poskytuje zpětnou vazbu o dosažitelnosti sítě v reálném čase. Pro funkce, jako je hlas a video, je důležitá dostupnost sítě se stabilním jitterem a latencí.
  IP SLA poskytuje zpětnou vazbu nezbytnou k zajištění toho, aby síť mohla udržovat aplikace v reálném čase, stejně jako důležité aplikace, jako je webový portál nebo objednávky.

Dodatečné použití IP SLA

Další funkce a použití pro IP SLA jsou následující:

- Monitorování dostupnosti sítě typu edge-to-edge
- Sledování výkonu sítě a viditelnost výkonu sítě
- Monitorování hlasu přes IP (VoIP), videa a virtuální privátní sítě (VPN)
- Monitorování SLA
- Zdraví IP služeb sítě
- Monitorování sítě MPLS
- Odstraňování problémů s provozem sítě

Volby (options) IP SLA

```
Switch(config-ip-sla)# ?
IP SLAs entry configuration commands:
      dhcp          DHCP Operation
      dns           DNS Query Operation
      exit          Exit Operation Configuration
      ftp           FTP Operation
      http          HTTP Operation
      icmp-echo     ICMP Echo Operation
      path-echo     Path Discovered ICMP Echo Operation
      path-jitter   Path Discovered ICMP Jitter Operation
      tcp-connect   TCP Connect Operation
      udp-echo      UDP Echo Operation
      udp-jitter    UDP Jitter Operation
```

Zdroj a responder IP SLA

- Zdrojem je zařízení Cisco IOS, které odesílá pakety sond.
- Cílem sondy může být jiné zařízení Cisco nebo jiný síťový cíl, jako je webový server nebo IP host.
- Ačkoli cílem většiny testů může být libovolné IP zařízení, přesnost měření některých testů může být vylepšena pomocí IP SLA respondéru.
- Responderem IP SLA je zařízení, které spouští software Cisco IOS.
- Responder přidá časové razítko do odeslaných paketů, takže zdroj IP SLA může brát v úvahu jakoukoliv latenci, ke které došlo, když respondér zpracovává testovací pakety.
- Aby tento test fungoval správně, je třeba synchronizovat hodiny zdroje i odpovídače pomocí protokolu **NTP** (Network Time Protocol).

Konfigurace IP SLA

Chcete-li implementovat měření výkonu sítě IP SLA, musíte provést následující úlohy:

Krok 1. Pokud je to nutné, povolte responder IP SLA.

Krok 2. Konfigurujte požadovaný typ operace IP SLA.

Krok 3. Nakonfigurujte všechny dostupné možnosti pro daný typ operace.

Krok 4. V případě potřeby nakonfigurujte prahové podmínky.

Krok 5. Naplánujte operaci ke spuštění a poté nechte operaci běžet po určitou dobu, abyste shromáždili statistiky.

Krok 6. Zobrazení a interpretace výsledků operace pomocí Cisco IOS CLI nebo systému pro správu sítě (NMS) pomocí SNMP.

Příklad konfigurace IP SLA ICMP Echo

```
Switch(config)# ip sla 12
Switch(config-ip-sla)# icmp-echo 192.168.139.134
Switch(config-ip-sla-echo)# frequency 30
Switch(config-ip-sla-echo)# exit
Switch(config)# ip sla schedule 5 start-time now life forever
Switch(config)# end
```

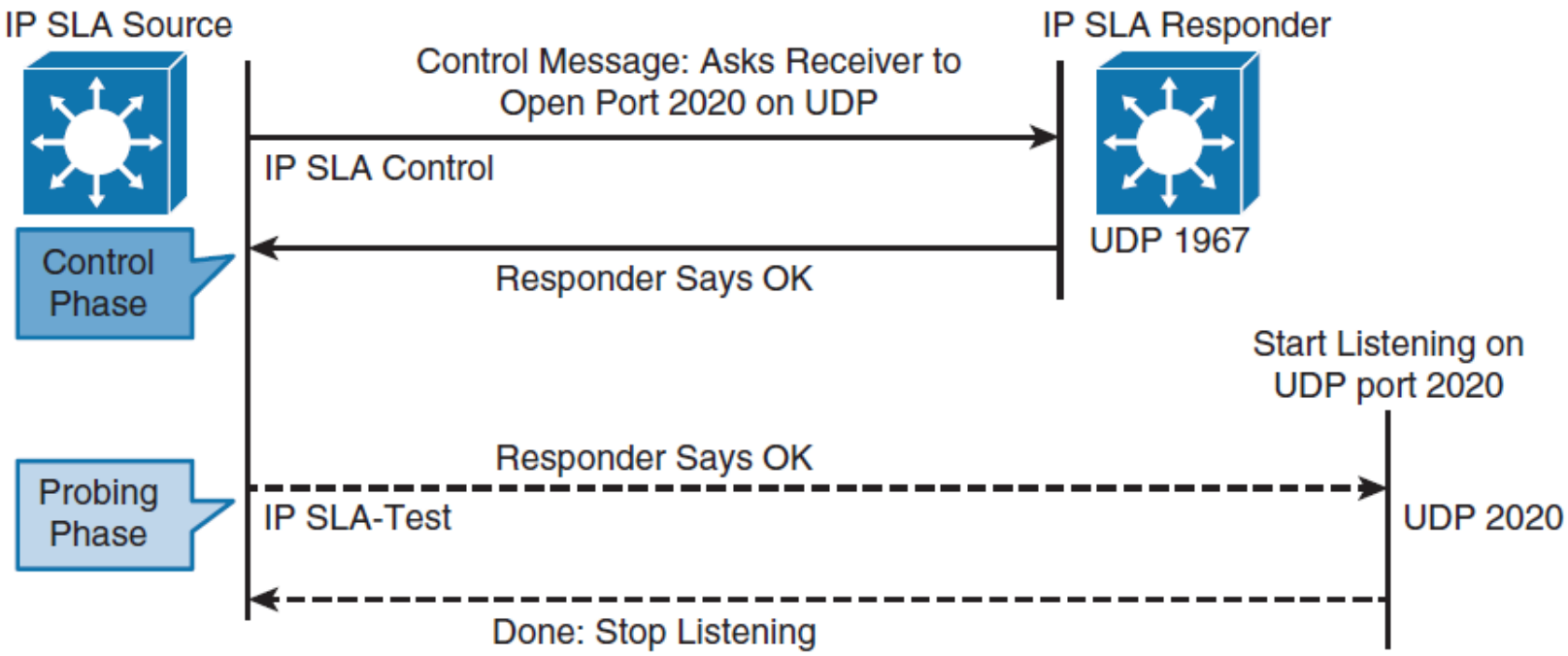
Verifikace konfigurace IP SLA

```
Switch# show ip sla configuration 22
IP SLAs, Infrastructure Engine-II.

Entry number: 12
Owner:
Tag:
Type of operation to perform: echo
Target address: 192.168.139.134
Source address: 0.0.0.0
Request size (ARR data portion): 28
Operation timeout (milliseconds): 5000
Type Of Service parameters: 0x0
Vrf Name:
Schedule:
    Operation frequency (seconds): 60
    Next Scheduled Start Time: Pending trigger
    Group Scheduled : FALSE
    Randomly Scheduled : FALSE
    Life (seconds): 3600
    Entry Ageout (seconds): never
    Recurring (Starting Everyday): FALSE
    Status of entry (SNMP RowStatus): notInService
Threshold (milliseconds): 5000
Distribution Statistics:
    Number of statistic hours kept: 2
    Number of statistic distribution buckets kept: 1
    Statistic distribution interval (milliseconds): 20
History Statistics:
    Number of history Lives kept: 0
    Number of history Buckets kept: 15
    History Filter Type: None
Enhanced History:
```

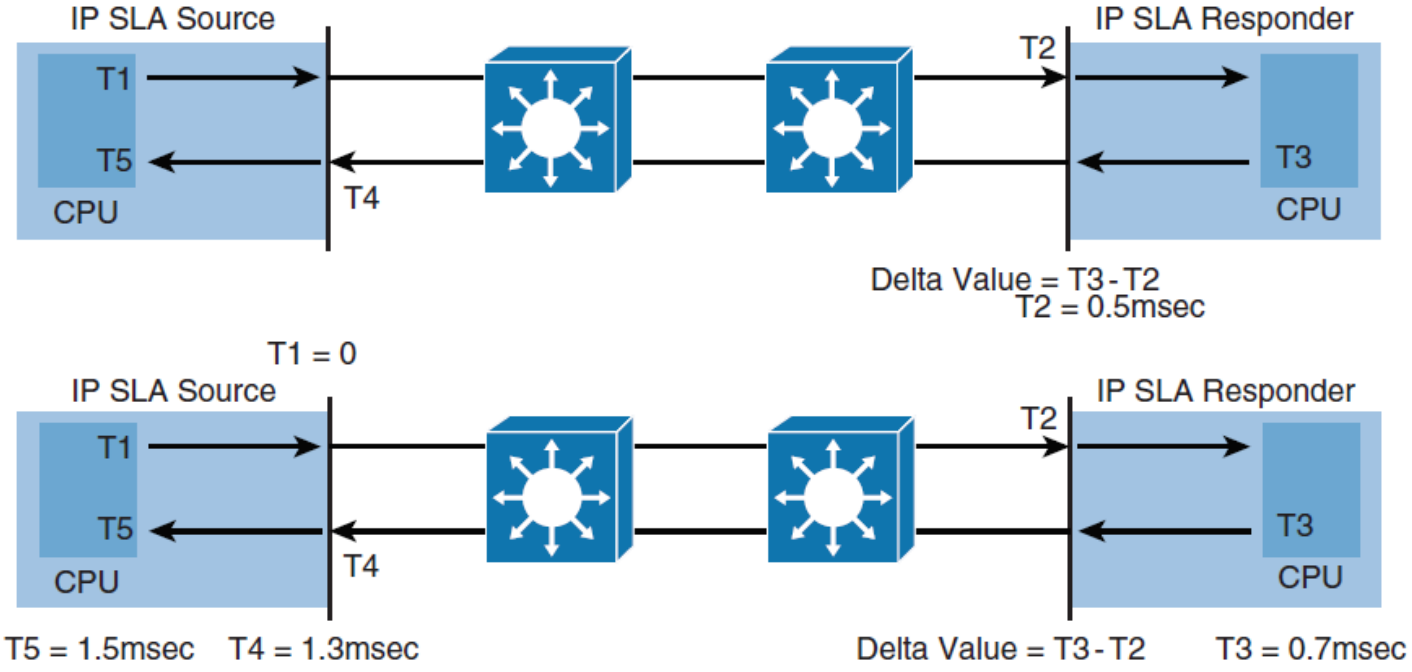
Verifikace konfigurace IP SLA

```
HQ# show ip sla statistics
IPSLAs Latest Operation Statistics

IPSLA operation id: 22
        Latest RTT: 1 milliseconds
Latest operation start time: 13:31:26 EST Mon Aug 11 2014
Latest operation return code: OK
Number of successes: 32
Number of failures: 0
Operation time to live: Forever
```

Operace s responderem IP SLA



Časová razítka IP SLA



Doba T1 je zadávána od 0 v milisekundách (pro jednoduchost)

The RTT (round-trip time) v tomto příkladu je kalkulována jako

RTT = T5 – (T5-T4) - (T3-T2) =

1.5msec – (1,5ms -1,3 ms) – (0,7 ms – 0,5 ms) = 1,1ms.

Konfigurace autentizace pro IP SLA

```
Switch(config)# key chain MYKEY
Switch(config-keychain)# key 1
Switch(config-keychain-key)# key-string SuperSecretPWD
Switch(config)# ip sla key-chain MYKEY
```

Příklad IP SLA UDP Jitter

```
Switch(config)# ip sla 1
Switch(config-ip-sla-jitter)# udp-jitter 192.168.1.2 65000 num-packets 20
Switch(config-ip-sla-jitter)# request-data-size 160
Switch(config-ip-sla-jitter)# frequency 30
Switch(config-ip-sla-jitter)# exit
Switch(config)# ip sla schedule 1 start-time after 00:05:00
Router(config)# ip sla responder
```

- Switch(config-ip-sla)# **udp-jitter** *dest-ip-add dest-udp-port*
  [**source-ip** *src-ip-add*] [**source-port** src-udp-port]
  [**num-packets** *num-of-packets*] [**interval** *packet-interval*]

- **request-data-size 160 (size in bytes - payload)**

Souhrn kapitoly 8

- LLDP a starší funkce CDP jsou užitečné pro objevování sousedních sousedství a jejich detailů.
- Funkce agresivního režimu UDLD je užitečná při přidávání odolnosti (resilience) do sítí, aby se zabránilo katastrofám v případě nenormálního chování.
- SPAN a RSPAN jsou běžné funkce ladění a provozu, které jsou také využívány k zachycení provozu pro síťové analýzy.
- IP SLA

Lab kapitoly 8

- **CCNPv7.1 SWITCH Lab8.1 IP SLA SPAN**