Switching, aggregation, High Availability

HA (High Availability) – wysoka dostępność. System o wysokiej dostępności nazywamy system, który niezależnie od stanu infrastruktury zapewnia założoną funkcjonalność.

Downtime – czas w którym system jest niedostępny dla użytkownika.

99.9% **dostępność** oznacza, że system nie działa rocznie 8.76 godziny, 43.2 minuty w miesiącu lub dziennie przez 10.1 minut!

Trunking - łączenie różnych danych w jeden kanał najczęściej w celu przesłania ich jednym połączeniem fizycznym.

802.1Q - standard **VLAN** (Virtual Local Area Network). Opisuje jak przesyłać dane z rożnych sieci przez jedno fizyczne łącze. W tym standardzie do ramki dodawane jest specjalne pole z numerem VLANu do nagłówka ramki Ethernetowej.

ISL (Inter-Switch Link) - Cisco way - ramki są enkapsulowane w dodatkowy nagłówek określający VLAN.

IST (InterSwitch Trunk) - technologia pozwalająca na polaczenie dwóch switchów (wraz z wymianą informacji o adresach, STP, ...) w jeden duży switch.

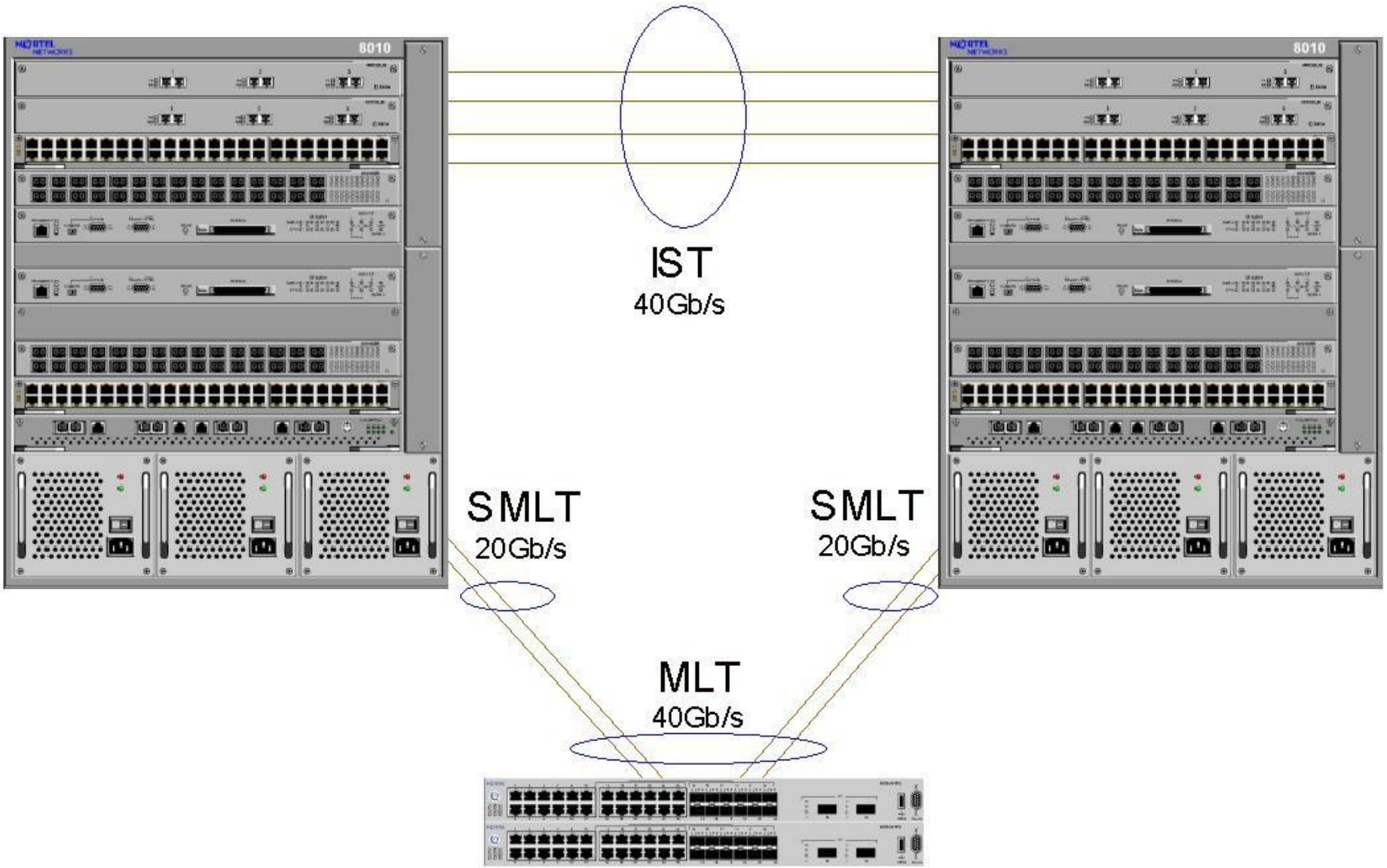
Link aggregation (802.1ad) lub **Port trunking** - określa mechanizm używania wielu fizycznych połączeń między urządzeniami jednocześnie w celu zwielokrotnienia szybkości połączania oraz redundancji.

EtherChannel - technologia agregowania połączeń ethernetowych w jeden "kanał". Wyróżniamy rodzaje:

- statyczny
- **LACP** (Link Aggregation Control Protocol) – Uniwersalny protokół agregacji
- **PaGP** (Port Aggregation Protocol) - Cisco way, tylko switche Cisco

MLT (Multi Link Trunking) – technologia agregowania połączeń (Nortel-way)

SMLT (Split Multi-link Trunking) - standard Nortel-a służący do tworzenia agregowanych połączeń przy użyciu dwóch różnych switchów. Switche dzielą informacje za pomocą IST.



SMLT

Bonding (Bonding Interface) - agregacja linków w linuxie

4 podstawowe tryby:

mode=0 (balance-rr) - round-robin - ramki idą sekwencyjnie przez wszystkie porty (pierwszym potem następnym, nastepnym, ...)

mode=1 (active-backup) - tylko jeden port jest aktywny, inny włącza się w przypadku awarii. W tym trybie tylko jeden mac jest "widzialny" dla switcha.

mode=2 (balance-xor) - (sMAC xor dMAC) % #slaves - używa tego samego portu dla danego adresu mac

mode=3 (broadcast) - transmituje cały ruch używając wszystkich interfejsów

mode=4 (802.3ad) - link-aggregation

balance-rr, balance-xor, broadcast - działają z wszystkimi switchami z EtherChannel
active-backup - działa z każdym switchem
802.1ad - działa ze switchami które wspierają 802.1ad i LACP

```
# modprobe bonding mode=1 miimon=100 downdelay=200 updelay=200
# ip link set dev bond0 addr 00:80:c8:e7:ab:5c
# ip addr add 192.168.100.33/24 brd + dev bond0
# ip link set dev bond0 up
# ifenslave bond0 eth0 eth1
```

```
      |                                  |
      |port3                        port3|
+-----+----+                      +-----+----+
|          |port2       ISL      port2|          |
| switch A +--------------------------+ switch B |
|          |                          |          |
+-----+----+                      +-----++---+
      |port1                        port1|
      |            +-------+              |
      +------------+ host1 +--------------+
              eth0 +-------+ eth1
```

Gdzie najczęściej używamy tych technologii?

SMLT, IST, MLT – Switche core-owe, centra danych
LACP, Bonding, EtherChannel – połączenia switchy, połączenia serwerów
802.1q – wszędzie gdzie trzeba odseparować część sieci – np. podsieci

RSTP (Rapid Spanning-Tree Protocol) – *[dla przypomnienia]* Szybszy protokół „drzewa rozpinającego” słuzący zapobieganiu powstawania pętli w sieci. Urządzenia wymieniają się informacjami za pomocą **BPDU** (Bridge Protocol Data Unit).

W przypadku posiadania VLANów:

PVST (Per-VLAN Spanning Tree), **MSTP** (Multiple Spanning Tree Protocol) – Spanning tree wewnątrz VLANu.

R-PVST (Rapid Per-VLAN Spanning-Tree Protocol) – połączenie RSTP oraz PVST

Ataki na *STP: można udawać tzw. Root role, wysyłać fałszywe ramki konfiguracyjne BPDU, i/lub DoSować BPDU. Metody obrony: **BPDU** guard. (=> dygresja o DHCP)

Więcej o VLAN-ach:

W 802.1q występuje pojęcie **tagowania** portów, ramek. Tagowanie odnosi się do umieszczania w ramce ethernetowej informacji o tym do którego VLAN-a należy.

Port tagowany – to taki port na którym cały ruch dostaje informację o VLANie.

Trunk – port(y) którym wysyła się więcej niż jeden VLAN. Pozwala to zaoszczędzić porty przy łączeniu VLANów.

Komunkacja pomiędzy VLANami odbywać się może tylko w trzeciej warstwie – jest więc realizowana za pomocą routerów (ew. switchy L3).

Trunk najczęściej transportuje ruch ze switcha do innego switcha lub routera.

VLANy w Linuxie:

`# vconfig eth0 2` ← Dodanie interfejsu eth0 do VLANa 2.

VLANy w Cisco:

```
interface FastEthernet 0/2
  switchport access vlan 2
```

← dodanie portu 2 do vlana 2

VLANy w MikroTik:

`add name=test vlan-id=2 interface=ether1` ← dodanie ether1 do vlana 2

```
#show interfaces FastEthernet 0/1 switchport ← informacje o trunku na 1 porcie
Name: Fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (VLAN0001)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1-5
Pruning VLANs Enabled: 6-1001
```

VLAN hopping – atak polegający na generowaniu tagowanych ramek ethernetowych – dzięki czemu podszywamy się pod przełącznik możemy wysłać pakiety do innego VLAN-a, a nawet podsłuchać inne VLANy.

Metoda ta może się czasem nie powieść, gdyż switch usuwa informację o VLANie z pakietów. Można więc wykorzystać „double tagging” - dodajemy taga dwa razy. Ten typ ataku zakłada, że tego drugiego taga odczyta następny switch.

Fajne narzędzie, do atakowania większości w/w metod:

=> Yersinia (http://www.yersinia.net/)