# Internet

## 4.0 Switch

Opera a livello della TCP/IP

| Task | IOS Command |
|---|---|
| Enter global configuration mode | S1# **configure terminal** |
| Enter interface configuration mode | S1(config)# **interface FastEthernet 0/1** |
| Configure the interface duplex | S1(config-if)# **duplex full** |
| Configure the interface speed | S1(config-if)# **speed 100** |
| Return to privileged EXEC mode | S1(config-if)# **end** |
| Save the running config to the startup config | S1# **save running-config startup-config** |

| Switch Verification Commands | |
|---|---|
| **Task** | **IOS Command** |
| Display interface status and configuration | S1# **show startup-config** |
| Display current running configuration | S1# **show running-config** |
| Display information about flash file system | S1# **show flash** |
| Display system hardware and software status | S1# **show version** |
| Display history of command entered | S1# **show history** |
| Display IP information about an interface | S1# **show ip interface** [interface-id]<br>S1# **show ipv6 interface** [interface-id] |
| Display the MAC address table | S1# **show mac-address-table**<br>S1# **show mac address-table** |

### Switching in Networking

In ogni porta sono associati due termini, uno di ingresso (**Ingress**) ed uno di uscita (**Exgress**).
Uno switch usa la sua tavola degli indirizzi MAC per inidirzzare i payloads.
Uno switch ha un processo a due passaggi:

- 1. Learn: esamina l'indirizzo in ingresso e ne aggiunge l'indirizzo MAC se non è nella tavola e resetta il time out a 5 minuti se la fonte è nella tavola
- 2. Forward: esamina l'indirizzo della destinazione, se essa ha un indirizzo MAC registrato nella tavola, indirizza i dati alla porta specifica, se invece l'indirizzo *non* è nella tavola, tutte le interfacce vengono interrogate eccetto la porta della fonte.

### Metodi di Switch Forwarding

Gli switch utilizzano dei software su applicazioni specifiche integrate (ASICs - application-specific-integrated-circuit) per prendere decisioni veloci.
Uno switch utilizza uno dei due metodi per fare forwarding decisions dopo che riceve un frame:

- **Store-and-forward switching** - riceve l'intero frame e si assicura che sia valido (utilizzato molto in Cisco).
- **Cut-through switching** - reindirizza il frame immediatamente dopo aver determinato l'indirizzo MAC della destinazione di un frame in arrivo e della porta in uscita.

BER = Bit Error Rate = $\frac{1}{x}$, (Ethernet) , BER $\cong 10^{-12}$

### Domini di Collisione

Gli switches eliminano i *domini di collisione* e riducono la *congestione*
Duplex = quando due dispositivi comunicano in contemporanea, creando una collisione
Quando esiste una duplex completa sul collegamento, i domini di collisione vengono eliminati.
Se esistono uno o più dispositivi in *half-duplex* ci sarà (...)

### Broadcast Domains

Si estende attraverso tutti i dispositivi di Layer 1 o i Layer 2 della LAN.

## 4.1 VLANs

Le VLAN sono connessione logiche con dispositivi simili. Mettere vari dispositivi in varie VLANs ha le seguenti caratteristiche:

- Permette la segmentazione dei vari gruppi di dispositivi sugli stessi switches
- Permette un'organizzazione più gestibile:
  - Broadcasts, multicasts e unicasts sono isolati nelle VLAN individuali
  - Ogni VLAN ha il suo univoco range di *IP addressing*

I benefici di usare le VLAN sono:

- **Domini di broadcast ridotti**: Dividere le LAN riduce il numero di domini di broadcast
- **Sicurezza migliorata**: Solo gli utenti nelle stesse VLAN possono comunicare tra loro
- **Efficienza IT migliorata**: Le VLAN possono raggruppare dispositivi con specifiche simili

- **Costi ridotti**: Un singolo switch può supportare multipli gruppi o VLANs
- **Performance migliori**: Piccoli domini di Broadcast riducono il traffico migliorando la larghezza di banda
- **Gestione semplificata**: Gruppi simili avranno bisogno di applicazioni simili

### 4.2 VLAN Definitions

Inter-VLAN Routing

- Legacy Inter-VLAN routing - Legacy, non ha un buon scaling
- Router-on-a-stick
- Layer 3 switch using switched virtual interfaces (SVI)

### Trunking

Fondamentale nelle architetture VLAN

## Modulo 14: Routing Concepts

L'instradamento è l'operazione per cui il router decide dove inoltrare un pacchetto. Ogni volta che un router, da qualsiasi delle sue interfacce, riceve un pacchetto, performa un'operazione di *routing* per capire dove inoltrare il pacchetto. Ha quindi due funzioni importanti: decide dove deve andare il pacchetto, e poi lo manda a destinazione.
La **Routing Table** è una struttura composte di righe che ci informano su delle determinate destinazioni, ed eventuali salti da effettuare per raggiungerle (collegamento diretto altrimenti). Il *longest match* indica, usando i bit più significativi, quante destinazioni hanno un numero simile di bit significativi (?).

Due tipi di reti:

- Directly Connected Networks
- Remote Networks: Reti che non sono direttamente connesse al router

### 14.2 Packet Forwarding

Il primo passo per il router è ricevere un pacchetto sulla sua interfaccia, ovvero ricevere un qualsiasi frame (es. frame ethernet). Il passo successivo è quello di estrarre l'indirizzo di destinazione del pacchetto IP. Dopodiché l'indirizzo verrà preso e confrontato con tutte le entries della Routing Table, il match migliore (ovvero il destinatario connesso direttamente al router per esempio) verrà preso in considerazione (?). 5. Il router non ha ricevuto nessun match, allora il pacchetto verrà scartato (da riscrivere kek).

Tree meccanismi di Packet Forwarding:

- **Process Switching** ....

- **Fast Switching**: ....
- **Cisco Express Forwarding** (**CEF**): .....

## Routing Table Principes

// TODO: Camera roll picture //

## Route Sources

Una routing table contiene una lista di routes alle reti conosciute, derivate dalle seguenti:

- Directly Connected networks
- Static routes
- Dynamic routing protocols

La sorgente per ogni route è identificata da un codice. Alcuni codici comuni sono:

- L - local
- C - connected
- S - static
- O - OSPF (Open Shortest Path Next)
- * - default route(?)

// TODO Ipv4, Ipv6, Image Legend //

// Administrative Distance //

## 14.3

// Static or Dynamic? //

Il Route dinamico è generalmente meno sicuro di quello statico, poiché nel primo caso è più facile potersi mettere in ascolto.

## Dynamic Routinc Protocol Concepts

Ci sono due approcci per implementare algoritmi di routing:

- **Distance Vector**: tutti i router condividono con i vicini la distanza che hanno calcolato dalle altre reti, dopodiché aggiungono il costo che vedono dal router dal quale ahnno ricevuto le informazioni (semplice ma presenta problemi di convergenza)
- **Link State**: tutti i router diffondono le informazioni riguardanti le reti direttamente connesse agli altri router (ciascuno condivide la propria routing table), tutti i router costruiscono l'intera topologia (complesso ma più veloce)

Questi algoritmi sono stati sviluppati e diffusi a partire dal 1990 circa (subendo lievi modifiche nel tempo, mantenendo però la logica di base).
Un'algoritmo di routing calcola continuamente i percorsi "migliori" per indirizzare i frame, ciascun protocollo ha la sua definizione di "percorso migliore".

Il **Load Balancing** è una strategia che permette di bilanciare il traffico tra due o più destinazioni differenti, dipende dalla configurazione del router. Non sempre il balancing è equo e le percentuali possono essere distribuite diversamente.

# Module 15: IP Static Routing

## Static Routes

- Standard static route
- Default static route
- Floating static route
- **Summary static route**: si usa quando abbiamo più reti, facciamo una summary e la mettiamo a /22 (?), quindi in un qualche modo fa un sommario di route più piccole che si possono raggruppare tutte assieme [non importante nel corso]

## Next-Hop Options

- Next-Hop Route: viene specificato solo l'indirizzo IP di next-hop
- Directly connected static route: (...)
- Fully sepcified static route: specificata in maniera completa

// TODO: Dual-Stack Topology //

Abbiamo 3 route remote, una /24 [IPv4], l'altra /64 [IPv6], configurando il router R1 si può verificare che il router riconosce immediatamente le route connesse ( verificabile con **show ip route | begin Gateway** ), di conseguenza verificando nella route table si può verificare che la rete in R2 è connessa mediante l'interfaccia seriale **Serial0/1/0**, tuttavia non può comunicare direttamente con la LAN di R3.

## 15.2 Configure IP Static Routes

In una **next-hop static route**, solo il *next-hop IP address* viene specificato, per esempio nella topologia di prima, R1 dovrà avere 3 next-hop settati manualmente ( usando il comando **ip route** [**IPv4**] [**Subnet Mask**] ). Discorso analogo può esser fatto nel protocollo IPv6, ovviamente l'unica differenza sarà il formato.

Una **fully specified static route** necessita invece di avere l'interfaccia ed il next-hop specificati ( **ip route** [**IPv4 Address**] [**Subnet Mask**] [**Interfaccia**] [**IP Next-Hop**] ). Nel caso del protocollo IPv6 invece, non solo l'interfaccia avrà un indirizzo GUA, ma anche un LLA (IPv6 Link-local Address), di conseguenza nella configurazione andranno specificati entrambi ( **ipv6 route** [**IPv6 Address/Subnet Mask**] [**Exit Interface**] [**Next-Hop**] ).
Per verificare una route statica si può andare nella route table ( show ip route static ) e vedere se l'interfaccia ha una S sulla sinistra.

## 15.3 Floating Static Routes

Sono path di backup ed entrano in gioco quando le route principali non sono disponibili. Di prassi si mette una distanza di 5, ma è sufficiente che sia un valore maggiore di 1. La distanza amministrativa si può impostare dal comando "ip route", aggiungendola come argomento finale.

## 15.4 Configure Static Host Routes

Si può configurare per dirigere il traffico ad una destinazione specifica. Utilizza un indirizzo IP e una subnet di 255.255.255.255 (/32) nei protocolli IPv4 ed una prefix length di /128 nei protocolli IPv6.

# Modulo 1: Single-Area OSPFv2 Concepts

## 1.1 OSPF Features and Characteristics

OSPF appartiene ad una categoria **link-state routing protocol**. Link si riferisce a tutti i collegamenti a coppie di router ( seriali o link-access ). Ciascuno di questi sara una rete logica di tipo /n. L'obiettivo dell'OSPF è di far sapere al router lo stato del link a cui è direttamente connesso. Ogni collegamento tra router è un <<link>> per OSPF.
I router che utilizzano OSPF utilizzano 5 tipologie di messaggi per garantire lo scambio di informazioni di routing:

- **Hello Packet**
- **Database description packet**
- **Link-state request packet**
- **Link-state update packet**
- **Link-state acknowledgment packet**

I messaggi di OSPF vengono usati per creare e mantenere 3 database OSPF:

- Adjacency Database: (...)
- Link-State Database (LSDB): (...)
- Forwarding Database: (...)

Queste tabelle sono di fatto "vive", quindi ogni volta che la tabella viene aggiornata, viene ricalcolata la topologia mediante un'algoritmo. In realtà quest'algoritmo è solo una parte dell'algoritmo **SPF** (Shortest-Path First) che calcola le route più ottimali possibili per ogni nodo.

OSPF si può implementare in due modi:

- Single area OSPF
- Multiarea OSPF

La seconda presenta routing tables più piccole, un ridotto aggiornamento del link-state ed una ridotta frequensza di calcoli riguardanti l'algoritmo SPF.

OPSFv3 è l'equivalente di OSPFv2 implementato però per i protocolli IPv6.

## 1.2 OSPF Packets

### Hello Packet

OPSF Type 1 Packet corrisponde all'Hello Packet, che hanno lo scopo di trovare i vicini e stabilirne l'adiacenza

### Link-State Updates

Inviano aggiornamenti sul routing OSPF. Un paccketto LSU può contenere diverse tipologie di advertisement (...?)

## 1.3 OSPF Operation

Ci sono 7 stati attraversati da un router nei quali opera l'OSPF.

- Down State: il router non riceve Hello Packets, di conseguenza l'interfaccia non sta funzionando, quindi va in Init State
- Init State: l'Hello Packet viene ricevuto dal vicino e contiene il Router ID del mandante, passa poi al Two-Way State
- Two-Way State: (...)
- ExStart State: (...)
- Exchange State: i router decidono chi passerà le informazioni sul DBD (DataBase Description), mediante un algoritmo si decide chi inizia e chi ascolta, dopodiché si avrà la fase vera e propria dello scambio delle DBD, se sono richieste ulteriori informazioni si passa in Loading State, altrimenti transiziona al Full State

- Loading State: LSR e LSU vengono usate per ottenere ulteriori informazioni di route
- Full State: (...) Porcaccio dio

### The need for a DR

// TODO Immagine e sistemare paragrafo//
Numero di Adiacenze: $n(n-1)/2$
n = numero di routers

## Dijkstra and Bellman-Ford algorithms

### Components of OSPF

Il router costruisce la routing table dalla topology table basata sulla Dijkstra SPF (shortest-path-first). SPF è un agoritmo basato sul costo cumulativo per raggiungere una destinazione. L'SPF crea un'albero piazzando ogni router alla radice e caclolandone il shortest-path ad ogni nodo.

### Bellman-Ford Algorithm

Calcola il costo più basso per raggiungere una destinazione, tuttavia permette di poter scegliere una strada piuttosto che un'altra ( in caso di percorsi con costo uguale ).
Bellman-Ford ha una complessità computazionale maggiore rispetto a Dijkstra, perciò generalmente si preferisce il secondo rispetto al primo.

## Modulo 2: Single-Area OSPFv2 Configuration

### Router IDs

Un router ID OSPF è un valore a 32-bit, rappresentato in forma di indirizzo IPv4. Viene usato unicamente per definire il router. (...)

I router derivano il router ID in base a 3 criteri:

- 1. L'ID viene configurato direttamente usando il comando OSPF "router-id rid" router configuration mode.
- 2. Il router sceglie l'indirizzo IPv4 più grande (...)
- 3. Il router sceglie l'indirizzo IPv4 (...)

### Wildcard Mask

Rappresenta l'inverso della Subnet Mask e rappresenta il numero di host.

# Modulo 3.7: TCP and UDP Vulnerabilities

// Risistemare tutto il paragrafo //

## TCP Attacks

TCP instaura una connessione affidabile, garantendo che i pacchetti arrivino a destinazione.

## TCP SYN Flood Attack

L'attaccante fa leva sul fatto che il protocollo debba attendere un'ACK per sincronizzarsi, lasciando però di fatto il SYN in sospeso, creando un disservizio ed impedendo ad altre connessioni di accedere al servizio.
Per terminare una sessione TCP si usano degli exchange a 4 steps:

- Quando il client non ha più dati da mandare in stream, manda un segmento con la flag FIN attiva
- Il server manda un ACK per notificare l'arrivo del pacchetto (...)
- (...)
- (...)

## ARP Cache Poisoning

ARP è un protocollo che serve a trovare una corrispondenza tra l'indirizzo IP e l'indirizzo MAC.
La cache ARP può essere usata per lanciare vari attacchi di tipo "man-in-the-middle"

## DNS Attacks

IL DNS deve rispondere a delle richieste di tipo "DNS" (?)

## DHCP

(...)

# Modulo 3.10. Crittografia

## ???

# Modulo 4: ACL Concepts

Le ACL sono delle **access control entries** (**ACE**s) che permettono di controllare che tipo di traffico far passare attraverso una certa interfaccia.