**RC2**

**Capítulo 1: VLANS**

**Ethernet (802.3)**

* Most successful LAN technology
* Carrier Sense/Multiple Access
* Layer 2 -> forwarding (switching)
* Layer 3 -> routing

**Network Devices**

Switch:

* OSI Layer 2 inter-connection
* Implements VLAN
* Spanning-tree based routing (STP, RSTP, MSTP)
* Wireless Access Points
* Fowarding

Router:

* OSI Layer 3 inter-connection
* Routing
* Have extra functionalities like QoS, Security, VPN gateway, network monitoring, etc

Other devices: Firewall,VPN gateway…

**Virtual LAN (VLAN)**

* A Virtual LAN (VLAN) is a group of hosts with a common set of requirements or characteristics in the same broadcast domain.
* Independent of their physical location.
* breaking a single broadcast domain into several smaller broadcast domains
* Hosts in different VLAN do not communicate by Layer 2!! Communications are done at layer 3!! *(ip routing)*
* Vlan configured in switch
* If we try to ping from a Vlan to a different vlan we will get a Requested Time Out

**Interconnection of Switches**

1. Physical link per VLAN
2. With a single physical link using trunk ports -> frames must have a tagg (Added when forwarding to a trunk port. Read and removed when receiving a frame from a trunk port)

**IEEE802.1Q Standard**

Without vlan tag -> destination source type data

with vlan tag -> destination source tag type data

8100h|priority|CFI(0 on ethernet)|VLAN ID

**Virtual Extensible LAN (VXLAN)**

* Alternative/Complement to 802.1Q in Layer3 Switches.
* Encapsulates OSI Layer 2 Ethernet frames within Layer 4 UDP/IP datagrams
* Com o VXLAN, é possível criar uma rede lógica entre máquinas virtuais (VM - Virtual Machines) em diferentes redes. Falando mais tecnicamente, com o VXLAN, é possível conectar duas ou mais redes de camada 3 fazendo com que elas operem como se estivessem conectadas em uma rede da camada 2, ou seja, cada uma faz parte da sua própria rede, mas “dentro” do mesmo domínio.

**IP Connection between VLANs**

* To communicate between different VLAN it is required to use Layer 3 (IP Routing)
* A router with support to 802.1Q or A Layer 3 switch(virtual layer 3 interface)

End to End Vlans -> associadas a portos dispersos pela rede

Vlan1 Vlan 2 \_\_\_\_\_\_\_\_\_trunk Vlan1 Vlan2

Local Vlan:

Vlan1 Vlan 2\_\_\_\_\_\_\_\_Vlan3 Vlan 4

**VLAN Segmentation Purpose**

* Local VLANs with similar traffic/security/QoS policies should have IP (sub-)networks that can be summarized/aggregated.

Exemple: VLAN 21: 200.0.0.0/24 // VLAN 22: 200.0.1.0/24

aggregated address of VLAN21+VLAN22: 200.0.0.0/23.

* Each VLAN must have an unique IP (sub-)network and may have more than one sub-network.
* Local vlans -> por serviço/função, por localização…

->traffic should be routed(Using standard layer 3 Link or using ip routing.)

* End\_to\_end Vlans -> Services/roles that have a global scope within the network

-> Same IP network (same IP address) independently of location.

-> Same administrator of (all) equipments independent of location.

-> traffic should be switched

**Ethernet Link Aggregation**

* Multiple Ethernet links may aggregated, provide a seamless trunk connection with N times the single throughput/speed of one link (link aggreggation trunk)

**Redundant Layer 2 Network**

* Objetivo: a rede recuperar de falhas (dinamicamente).
* Por vezes, a redundância crias layer 2 Loops. E devido a isso faz com que haja um colapso de comunicação devido a um infinito frame flodding (MAC frames com broadcast adress são enviados para qualquer host).
* Switches repassam o broadcast para todos os oustros swicthes ligado e assim sucessivamente => loop => **unstable mac adress table + infinito broadcasts + duplicate frames**

**Spanning Tree Protocol (SPT)**

Este protocolo faz com que a rede bloqueie portos e forneça uma topologia loop-free com links redundantes.

Existe vários SPT protocolos:

* STP is the original IEEE 802.1D
* RSTP, or IEEE 802.1W(fasterSTP)
* Multiple Spanning Tree (MST) is an IEEE standard(MST maps multiple VLANs into the same spanning-tree instance.)
* Per VLAN Spanning Tree Plus (PVST+)(for each VLAN)!!!
* RPVST+ (per vlan)!!!

How Spt works step by step:

Uses Bellman-Ford Distributed and Asynchronous Algorithm

**Shortest path from node x to node A = custo do link do no x para o no que se segue mais curto para o no A + Shortest path from that node to node A**

Each node transmits periodically (to all its neighbors) the estimation of the cost between it and a destination R (Cost associated with each port)

Upon reception of a neighbor message, each node recalculates its own estimation of path cost to R.

***Steps*:**

1. **Elect a root bridge** -> Switch com lowest ID

Bridge/Switch ID – each switch is identified by an 8 bytes identifier based on:

* Priority(2 bytes)
* Mac adress(6 bytes)

1. **Each non-root switch selects its root port** -> best way to root brigde (calculate rooth path\_costs to define(cost outputs) ->(**root ports**) =>**fowarding states**

* Port of the designated bridge that provides the path to the root.

1. **Remaining links choose** **a** **designated port** => **fowarding states**

* **Designated Bridge** –> Switch responsible to forward the packets from an Ethernet segment to and from the root.

**is the switch with the lowest Root Path Cost**

* Designated Port – Port of the designated bridge that connects an Ethernet segment (to which is designated).

1. All other ports are blocked (**non** **designated port)**

***States*:**

* **Disabled** -> shutdown (não recebem bpdu e nem aprendem mac adresses)(administrive actions).
* **1º Blocking** -> blocking traffic (**NOT learning** MAC address learning and **not** packet forwarding )+ recebem e **processam BPDU+ After MaxAge time without receiving BPDU, it transitions to Listening state; => after a toplogy change!!!**
* **2º Listening** -> **not** fowarding **and NOT learning mac adresses (transitional states)+**

Receives **and processes BPDU**. **When ForwardDelay timer expires the port transitions to Learning state.**

* **3º Learning** -> **not** fowarding **but learning mac adresses( transitional states)+** Receives and **processes BPDU**. **When ForwardDelay timer expires the port transitions to Forwarding state**
* **4º Fowarding** -> sending and receiving traffic + Receives and processes BPDU.

**BPDU’s**

2 tipos: configuração + topology change

message age: vai aumentado há medida que não são atualizadas informações!

Mensagens bpdus periódicas- a portas -> a cada hello time

Identificador bridge -> identificador próprio switch!!

**Topology change notification:**

**TCN-> enviado pelas portas raiz a caminho do root raiz**

**TCA -> acknowladge**

Quando os switches receberem o bit **TC=1(so a raiz pode alterar e iniciar o envio do valor TC!! Os switches reencaminham)** durante fowardelayTime+MaxAge (se a partir dai não receber mais nenhum TCN significa que estabilizou!!) e os switches têm de manter a tabela de encaminhamento com uma lifetime curta (enquanto TC=1)

**Messages Exchange**

1. At start, all bridges assume to be the root bridge.
2. Send Conf-BPDUs to all connected Ethernet segments **Raíz.Custo.ID**

**idswitch.0.idswitch**

3)calculate root bridge

**2º Capítulo**

**Objectives of Network Design**

* Network should be Modular(suporta aumento e mudanças) -> By separating the various functions that exist on a network into modules, the network is easier to design.
* Resiliente(Up-time close to 100 percent)->  The network must remain available for use under both normal and abnormal conditions.
* Flexibilidade -> the ability to modify portions of the network, add new services, or increase capacity without going through a major forklift upgrade

**Modelo Hierárquico**

It breaks the complex problem of network design into smaller and more manageable areas.

Only traffic that is destined for other networks is moved to a higher layer.

the network has now been divided into **three separate broadcast domains:**

* **Access layer ->** highlighted grants end devices access to the network. In the WAN environment, it may provide teleworkers or remote sites access to the corporate network across WAN connections + **generally incorporates Layer 2 switches and access points providing connectivity between workstations and servers +** Address Resolution Protocol (ARP) inspection+ Spanning tree

**SHOULD:** High availability -> that is default gateway redudancy using multiple connections from access switches to redundant distribution layer switches.) + Security + convergence (voice into data) + QoS (prioridades + queue )+ ip multicast + In Access layer, any path from a switch should not require another switch from the Access laye

* **The Distribution Layer** ->  aggregates the data received from the access layer switches before it is transmitted to the core layer for routing to its final distination -> é o limite entre layer 2 e layer 3. **Either a router or a multiplayer switch**. **Aggregation of LAN or WAN links +** Policy-based security + Routing services between LANs and VLANs + **Broadcast domain control, because routers or multilayer switches do not forward broadcasts. + QOS**

**Uses a combination of Layer 2 and multilayer switching** to segment workgroups and isolate network problems, preventing them from impacting the core layer.

**Connects network services to the access layer**

**The distribution layer it is usually used to terminate VLANs from access layer switches(**summarizes routes from the access layer.)

**SHOULD:** Avoid Daisy Chaining When using a L3 link!! any path between Distribution layer switches should not require a switch from the Access layer.

When using a L2 link between Distribution layer switches daisy chai nis accepatble but could overload!

* **The core Layer:** A high-speed backbone. Core is critical for connectivity, **must provide a high level of availability and adapt quickly to changes**. **Should provide scalability and fast convergence + redundacy +** Implements scalable protocols and technologies

Aggregation point for the other layers.

**Design Modular**

While the hierarchical network design works well within the campus infrastructure, networks have expanded beyond these borders.

The central campus site now requires connections to branch sites and support for teleworking employees working from home offices or other remote locations.

Um design modular separates the network into various functional network modules.

Each targeting a specific place or purpose in the network. The modules represent areas that have different physical or logical connectivity.

*Beneficios:*

* Failures that occur within a module can be isolated from the remainder of the network, providing for simpler problem detection and higher overall system availability
* Network changes, upgrades, or the introduction of new services can be made in a controlled and staged fashion, allowing greater flexibility in the maintenance and operation of the campus network.
* When a specific module no longer has sufficient capacity or is missing a new function or service, it can be updated or replaced by another module that has the same structural role in the overall hierarchical design.
* Security can be implemented on a modular basis allowing for more granular security control.

**Módulos:**

* **Enterpise Campus:**  Also called the distribution block, this is the most familiar element and fundamental component of a campus design + This module is where most users access the network + unified communications services, policy gateways, and more + **switches Layer 2 + distribuition layer**
* **Data Center:**  This block is responsible for managing and maintaining many data systems that are vital to modern business operations. Backup and application replication + Allows the enterprise to scale without major changes to the infrastructure
* **Branch:** Allows enterprises to extend head-office applications and services to remote locations and users or to a small group of branches( consists of the Internet edge and the WAN edge.) **Provides secure access to voice, mission-critical data, and video applications.** Should provide a robust architecture with high levels of resilience for all the branch offices
* **WAN and MAN:** Offers the convergence of voice, video, and data services + Enables the enterprise a cost-effectively presence in large geographic áreas + QoS + Layer 2 or Layer 3 communications.
* **Remote User:** Allows enterprises to securely deliver voice and data services to a remote small office/home office (SOHO) over a standard broadband access service + Allows a secure log in to the network over a VPN and access to authorized applications and services.

**Caminhos Alternativos:**

Um link adicional que forneça um caminho adicional para um 2 core switch oferece redundância e suporta uma falha de um único link ou nó

Criar triângulos: Se houver uma falha **não há necessidade** de uma routing protocol convergence

Quadrados: **há necessidade** de uma routing protocol convergence

**Se não houver uma core layer**

Os switches na distribution layer precisam e ser fully meshed.

Dificuldade em escalar.

Mais cabos.

Complexidade no routing há medida que forem sendo adicionados vizinhos.

Pode ser usado num campus que não tenha necessidade de aumentar.

**Core + distribution layer num só -> Collapsed Core Layer Architecture**

Em networks mais pequenas pode ser usado -> elimina a necessidade de extra switching hardware e simplifica a implementação da rede.

No entanto elimina as vantagens que existe nas multicamadas/ subdivisões.

**Avoid Single Points of Failure**

Com um design hierárquico pontos de falha são fáceis de evitar com links redundantes na camada de distribuição e core.

No access layer L2 switches podem ser pontos de falha unicamente para o user que esta conectado a ele. Possiveis soluções

* Solução1: hardware backup redundante -> substituir equipamento defeituoso (ativado por propriatario)(supervisão)
* Solução 2: múltiplas conexões entre cada user e diferente acess switches -> mais fios e network cards

**Avoid Too Much Redundancy**

Aumenta: complexidade, nr de portos usados e fios

**Wireless Network(s) Integration**

Nota: Wireless networking technologies should have an integration point at core or distribution layers

In terms of network architecture a WLAN can be seem as any LAN

**VLANs on Access Points**

AP have trunk ports to distribution/core switches.

VLANS can be extended to an wireless domain -> end to end (Mobility and AP roaming should not break Layer 3 connectivy + IP address should be the same → same VLAN with campus)

Each SSID can be mapped to a VLAN.

**Capítulo 3: Dynamic Routing e protocols**

**Ip routing ->** routers fazer fowarding de pacotes para redes diferentes e para isso precisam de ter conhecimento da network destino. O router sabe sempre automaticamente a network que esta ligada diretamente a ele.Para as outras networks temos:

* **Static Routing** -> manualmente configurável
* **Dynamic Routing** -> aprende de outros routers
* **Policy based routing** -> Manually routing rules that outweigh static/dynamic routing and may depend on parameters other than the destination address.

**Default Routes ->** enviar pacotes para um específico router (também tanto pode ser estático ou dinâmico)

* IPv4 default route - 0.0.0.0/0 IPv6 default route - ::/0

**Static Routing**

Não se adapta a mudanças de topologia. Por isso, se algum link falhar a routa estática não é mais valida e para isso uma nova routa estática tem de ser configurada.

Também não se dapta bem a crescimento de redes.

Quando se deve usar static route

* Quando o administrador precisa de controlo total das rotas usadas pelo router
* Backup para uma rota dinâmica
* Para usar para uma network que seja acedida so por um caminho(sem backup)
* Router conectada à ISP e precisa de uma única default route e escusa de aprender todas as rotas do ISP (sem backup)
* O router não tem cpu nem memoria suficiente para dynamic routig protocol
* Pouca largura de banda e por isso dynamic routig não é desejável

**Dynamic Routing**

Permite que a rede se ajuste a mudanças de topologias sem necessidade de haver envolvimento do administrador.

Routers trocam entre si de informação de redes e o estado de cada link/rede;

* Routers trocam de informação só com outros routers que tenham o mesmo routing protocol
* Quando existe uma mudança de topologia a nova informação é dinamicamente propagada através da rede e cada router vai atualizando a routing table.

**Routing Tables**

An IP address may have multiple matches on a Routing Table:

Example:

192.168.1.12 Will match:

– 192.168.1.0**/25** via ...

– 192.168.1.0/24 via ...

– 192.168.0.0/23 via ...

– 192.168.0.0/16 via ..

Router will choose entry **with the largest network prefix** **(most specific network**).

– i.e., 192.168.1.0**/25** via ...

Routing tables podem ter mais de um caminho para cada rede e por isso o trafico é dividido por entradas ou então por pactoes (sessões tcp, UDP ports…).

**Administrative Distance**

Muitos protocolos têm estruturas e algoritmos específicos que são incompatíveis com outros protocolos.

Ou seja, uma rede que use vários protocolos de routing precisa de saber trocar informação entre os routers para conseguir escolher o melhor caminho

**Administrative Distance(value)**

Para escolher o melhor caminho (decidir entre diferentes protocolos para o mesmo destino **(mesmo prefixo de rede e mascara)**

O que tiver menor valor administrativo é o melhor!

Example:

**Static [1/1] 192.168.1.0/24 via … ← Chosen!**

RIP [**120**/1] 192.168.1.0/24 via …

OSPF [**110**/1] 192.168.1.0/24 via ..

NOTE:

**Based on the default administrative distances, routers use static routes over any dynamically learned route.** However, this default behavior might not be the desired behavior.

For example, when you configure a static route as a backup to a dynamically learned route, you do not want the static route to be used as long as the dynamic route is available.

**Floating Static Routes**

Floating static routes are static routes that have an administrative distance greater than the administrative distance of another static route or dynamic routes. They are very useful when providing a backup to a primary link

The administrative distance of a static route can be increased to make the route less desirable than that of another static route or a route learned through a dynamic routing protocol. In this way, the static route “floats” and is not used when the route with the better administrative distance is active. However, if the preferred route is lost, the floating static route can take over, and traffic can be sent through this alternate route.

A static route that appears in the routing table only when the primary route goes away is called a floating static route.

**RIP default administrative distance is 120**

Static Routes default administrative distance is 1.

**To create a floating static route (to backup a RIP route) the administrative distance should be greater than 120. For example: 200.**

**Autonomous Systems**

**Conjunto de routers/networks com o mesmo tipo de politica de routing e com o mesmo tipo de administração**

Interior gateways protocols(IGP’s) -> RIPv1, RIPv2, OSPF, IS-IS and EIGRP (internal routing) serve para otimizar performance de routing

Exterior gateway protocols(EGPS) -> BGP serve para optimizar a performance do routing de forma a que ele obdeça a politicas de segurança,económicas e políticas.

**Tipo de networks**

* *Trânsito/Transport* -> interligar redes + routers trocam informação
* *Stub*: usado para uma única rede de router ou então para múltiplas redes de routeres se e só se os routers não trocarem informações deles.(interfaces passivas!!). Só passa tráfego de e para os seus próprios hosts

**Distance Vector versus Link State Protocols**

->Routers aprendem a topologia completa da rede e usam um algoritmo centralizado para descobrir o caminho melhor para as redes.

->Flooding process para obter a informação da topologia

-> so existe outra vez troca de informação quando existe uma mudança de topologia.

Exemplos: OSPF, IS-IS

->Cada router aprende o melhor caminho para a rede baseado na informação mandada periodicamente pelos seus vizinhos(network + cost para essa rede).

->Bellman-Ford algorithm

Exemplos: RIPv1, RIPv2, IGRP, EIGRP

**RIP -> Routing Information Protocol**

* Distance vector protocol
* Each router maintains a list of known networks and, for each network, an estiamtion of the cost to reach it -> distance vector
* Each router periodically send to its neighboring routers its own distance vector (partially or complete) – announcement/update.
* Each router uses the distance vector sent by its neighbors to update its own distance vector.
* The path cost to a destination is given by the number of routers/**hops** in the path
* 1 hop -> 1 router
* **Maximum cost is 15.**
* **A cost of 16 is considered infinite (or unattainable destination)**
* For each destination (network) learned, it adds an entry to that network that uses the path (or paths) with the lowest cost, using as next-hop the neighboring router(s) that announced that network with that lowest cost path.

**RIP -> Routing Information Protocol version 1**

* Classfull protocol : não anuncia as subnetworks masks só o prefixo de rede e por isso as mascaras de rede são assumidas baseado na receção da rede de mascara (que o router recebeu).
* Usa o broadCast 255.255.255.255 para enviar updates e anúncios e todos os networks devices devem os processar
* Não suporta autenticação
* A tag Next hop vai sempre a 0 e a subnetmask também
* Dst: 255.255.255.255 -> local broadcast-> It is never forwarded by routers that are connected to other networks. So it will never reach people on the (external) internet.

**RIP -> Routing Information Protocol version 2**

* Classless protocol: incluem o prefixo de rede e mascara
* Usa **o endereço multicast 224.0.0.9** para enviar anúncios e updates para routeres que usem este protocolo – single hop
* Suporta autenticação mas usange so message digest e clear text password -> não é seguro
* No entanto, continua com routas classfull (sumarize ) -> por exemplo : 3 redes 10.1.1.0/24 + 10.1.2.0/24 + 10.1.3/24 = 10.0.0.0/8 **para isso não acontecer tem que se escrever um comando no-auto summary**
* **Dst: 224.0.0.9 -> para todos os routers que tenham este protocolo**

**Contagem para o infinito**

Quando ocorre falhas antes de o algoritmo conseguir converger! A solução para isto é o **split-horizon**

**Each Router, in each interface, announces only the networks in which that interface is not used to provide the best path to that destination.**

* Prevents any routing loops that involve two routers.
* Sem split horizon são mandados todos os detalhos e métricas para todas as redes (para ela própria inclusive)

**RIP Message Types**

* **Rip response:** Distance vector announcement/update message(contem o vetor de distancia). Mandado de 30 em 30 segundos. Pode também ser mandado em resposta a uma rip request -> a responsa vai exclusivamente ao router que mandou o pedido!!
* **Rip response v2:** new fields-> Subnet mask + Route tag+ next hop: 0.0.0.0 indicates that the packets ,must be routed to the router that sent the RIP message + **com split horizon o next hop vai sempre a 0!!**
* **Rip Request**: Sent by a router that was recently started (bootstrap) or, when the validity of some of the distance vector information has expired (default timeout = 180 seconds or It may request specific information (a specific network) or, the complete neighbor distance vector

**Triggered Updates**

* Prevents any routing loops that involve more than two routers.
* **Whenever a router changes the metric for a route, it is required to send update messages almost immediately, even if it is not yet time for one of the regular update message.**
* Neighboring routers update routing tables faster and overall convergence is faster. Including entries that were removed by timeout

**RIPng for IPv6 Routing**

* Similar to IPv4 RIPv2
* Differences:
* Uses IPv6 for transport. **Uses link-local addresses** (not the global ones)
* Uses multicast group address FF02::9 (all-RIP-routers) as the destination address for RIP updates.
* IPv6 prefix, next-hop IPv6 link-local addres
* Routers always add the cost of the interface to the metric received. Metric is sum of “output interfaces” costs to destination and not number of hops. If all costs are 1, metric is number of “output interfaces” to destination.

**RIPng Path Costs**

* **Each router link/interface has an associated RIPng cost.**
* **The total cost between a router and a network is given by the sum of all RIPng costs of the (routers) output interfaces along the path**
* **Routers to access directly connect networks never use RIPng paths**

**---------------------------------------------------------------------------------------------------**

**Open Shortest Path First (OSPF) Protocol**

* Open-standard protocol
* Link-state routing protocol (Respond quickly to network changes)
* Send triggered updates when a network change occurs,
* Send periodic updates, known as link-state refresh, at long time intervals, such as every 30 minutes
* Routers running OSPF collect routing information from all other routers in the network (or from within a defined area of the network)
* And then each router independently calculates its best paths to all destinations in the network, **using Dijkstra’s (SPF) algorithm.**

**OSPF Necessary Routing Information**

Todos os routers (link-states) devem guardar:

* Os seus vizinhos -> esta informação é guardada na OSPF table/adjancency datebase
* **Todos os routers que existem nessa rede e as suas redes-> através de LSA’s** -> estas LSA’s são guardadas numa **table/database called** **LSDB**
* **Os melhores caminhos para cada destino** (cada router calcula independentemente)-> **tambem guardado nas tabelas** **LSDB**
* E posteriormente estes caminhos são mandados para a routing table (fowarding database)
* **Os pacotes que são recebidos no router são enviados baseado na informação da routing table**

**Link-State Protocol Operation**

* Link-state routing protocols generate routing updates only when a change occurs in the network topology
* **The device that detected the change creates a Link-State Advertisement (LSA)** concerning that link
* Each router stores the LSA, forwards the LSA to neighboring devices and updates its Link-State DataBase (LSDB).

**LSDB + SPF algorithm (Dijkstra’s algorithm) = routing table**

* Each router selects the best paths from their SPF tree and places them in their routing table

**Link-State Advertisement (LSA)**

* LSAs report the state of routers and the links between routers
* Link-state information must be synchronized between routers.
* There is a method for acknowledging their delivery -> **reliable**
* LSAs are flooded throughout the area (or throughout the domain if there is only one área
* LSAs have a sequence number and a set lifetime, so each router recognizes that it has the most current version of the LSA.
* LSAs are periodically refreshed to confirm topology information before they age out of the LSDB

**OSPF Router ID (RID)**

* **The highest IPv4 address of all router interfaces** at the moment of the OSPF process activation or A value administratively defined
* If a physical interface address is being used as the router ID, and that physical interface fails, and the router (or OSPF process) is restarted, the router ID will change.
* Administratively defining the RID or using loopback interfaces for the router ID forces the router ID to stay the same, regardless of the state of the physical interfaces.

**OSPF Adjacencies**

1. A router running a link-state routing protocol must first establish neighbor adjacencies**, by exchanging hello packets with the neighboring routers** -> The router sends and receives Hello packets to and from its neighboring routers. **The destination address is typically a multicast address**
2. Routers declare the neighbor up when the exchange is complete(as checking whether the neighbor is in the same area, using the same hello interval, and so on.)
3. Two OSPF routers on a point-to-point serial link, usually encapsulated in HighLevel Data Link Control (HDLC) or Point-to-Point Protocol (PPP), form a full adjacency with each other.
4. However, OSPF routers on broadcast networks, such as LAN links**, elect one router as the designated router (DR)** and another as the backup designated router (BDR**)( All other routers on the LAN form full adjacencies with these two routers and pass LSAs only to them)**

**DR(Designated Router) and BDR(Back upDesignated Router) Election**

1. The first OSPF router to boot becomes the Designated Router (DR).
2. The second router to boot becomes the Backup Designated Router (BDR).
3. If multiple routers boot simultaneously, The DR it will be the router with the highest priority. The BDR the second. The OSPF priority is a administratively defined parameter(In case of tie, it will be chosen the router with the highest Router ID (RID))
4. When the DR fails, the BDR assumes the role of DR. **The BDR does not perform any DR functions when the DR is operating.** The choice of the new BDR is done according to some criteria of the initial election.
5. **After the election, the DR and BDR maintain that role, independently of which routers join the OSPF process.**
6. **The ID of an OSPF Network is the IP address of the network's Designated Router (DR) interface.**

**OSPF LS Database (LSDB)**

Esta database esta organizada em 2 tabelas:

Router Link States :Routers related information table->The routers are identified by theirs RID.

* Cada router contem informação das redes diretamente contectadas aquele router!!
* **Link state id == Router ID ou então a networkID**
* **Number of links -> routeres ligados**
* **Tipo de network**
* **Designated Router address: 20.20.20.2 -> networkdID**
* Router Interface address -> interface ip address

Net Link states -> networks/links information table -> identificadas com ID tambem

**OSPF Packets**

* Hello - **Discovers neighbors** and builds adjacencies between them.

For the Hello packet - **Contains a list of known neighbors**(adjacent routers with which this router has established bidirectional communicatio) + **Router ID** + **Hello and dead intervals**(The hello interval specifies how often, in seconds, a router sends hello packets (10 seconds is the default on multiaccess networks). The dead interval is the amount of time in seconds that a router waits to hear from a neighbor before declaring the neighbor router out of service (the dead interval is four times the hello interval by default). + **área ID** (To communicate, two routers must share a common segment, and their interfaces must belong to the same OSPF area on that segment. These routers will all have the same link-state information for that area.) + **router priority +** DR and BDR IP addresses + Authentication password + Stub area flag

**Hello Interval, Dead Interval, Area ID, Authentication Password and Stub Area Flag fields must match on neighboring routers for them to establish an adjacency!!!!!**

* Database Description (DBD) - Checks for database synchronization between routers.

For the DBD packet - Contains a summary of the LSDB, which includes all known router Ids and their last sequence number, among several other fields.

* Link-State Request (LSR) - Requests specific link-state records from another router.

For the LSR packet - Contains the type of LSU needed and the router ID of the router that has the needed LSU

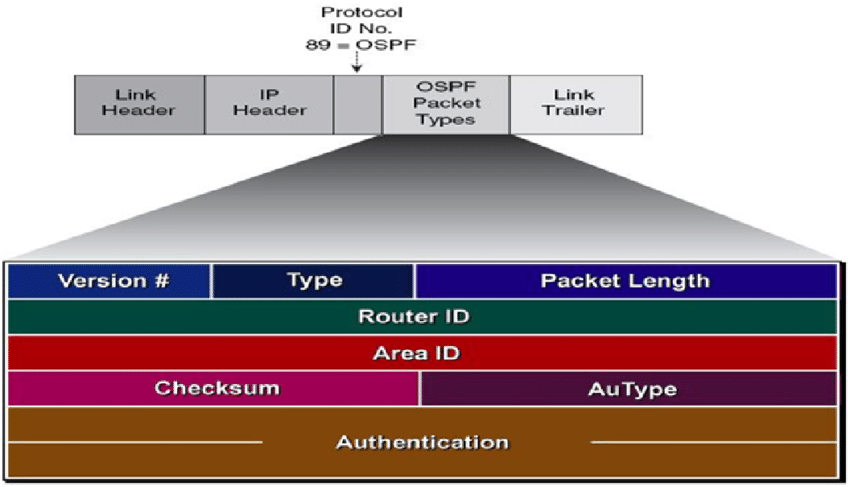
* Link-State Update (LSU) - Sends specifically requested linkstate records.

For the LSU packet - Contains the full LSA entries. Multiple LSA entries can fit in one OSPF update packet

* LSAck - Acknowledges the other packet types

For the LSAck packet - This data field is empty.

**OSPF Packet Format**



**Version Number:**

Set to 2 for OSPF Version 2, the IPv4 version of OSPF.

Set to 3 for OSPF Version 3, the IPv6 version of OSPF.

**Router ID**

Defines which router is the packet’s source.

**Data, contains different information, depending on the OSPF packet type:**

**Discovering the Network Routes**

**Master -> DR router**

**Slave -> BDR router**

**Only the DR exchanges and synchronizes link-state information with the routers to which it has established adjacencies!!!**

**The master and slave routers exchange one or more DBD packets.**

* A DBD includes information about the LSA entry header that appears in the router’s LSDB.
* The entries can be about a link or about a network.
* **Each LSA entry header includes information about the link-state type, the address of the advertising router, the link’s cost, and the sequence number.**
* **The router uses the** sequence number to determine the “newness” of the received link-state information.

It acknowledges the receipt of the DBD using the LSAck packet(It compares the information it received with the information it has in its own LSDB.)

If the DBD has a more current link-state entry, the router sends an LSR to the other route and The other router responds with the complete information about the requested entry in an LSU packet.

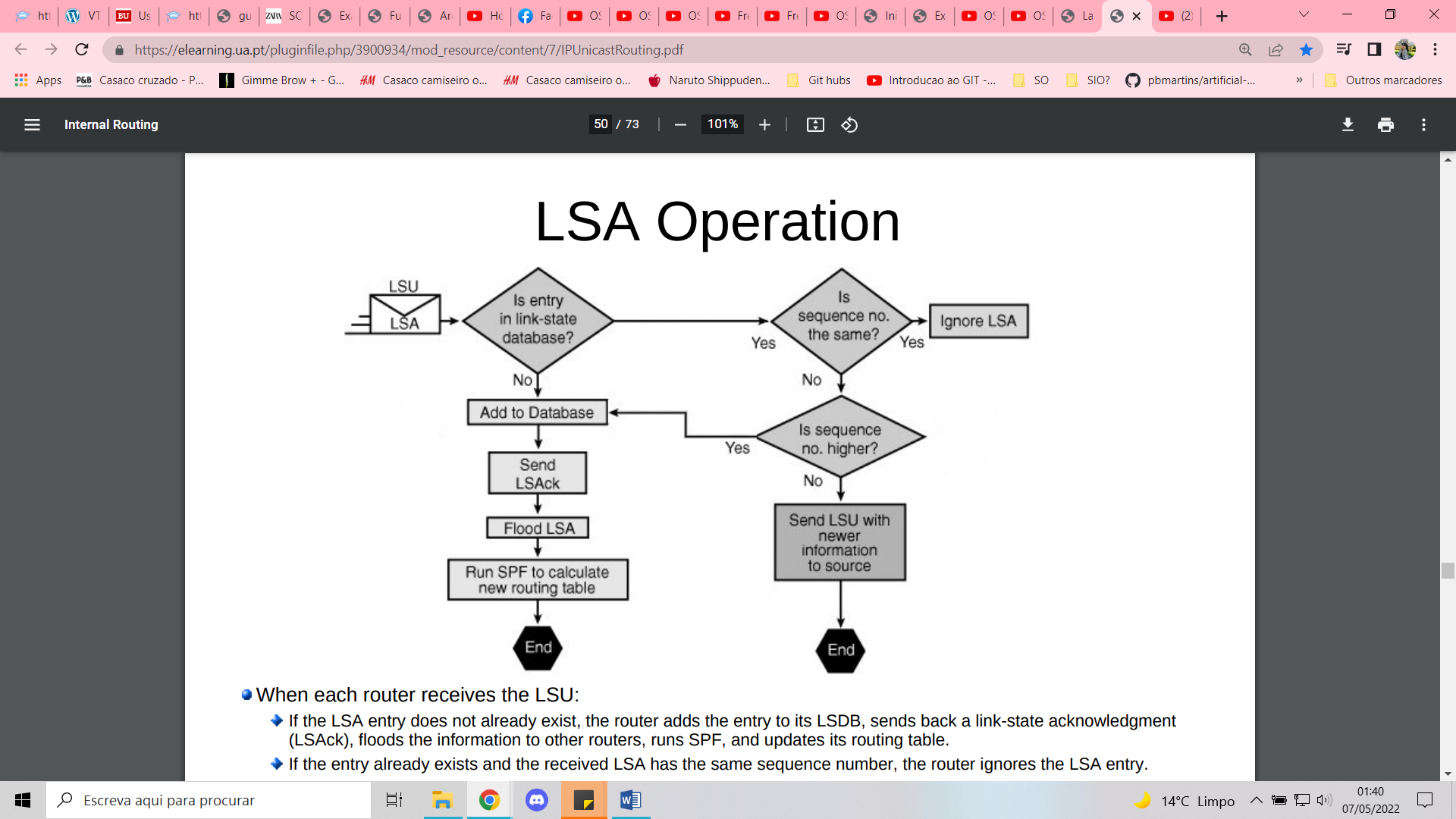
Again, when the router receives an LSU, it sends an LSAck.

The router adds the new link-state entries to its LSDB

**Maintaining Routing Information**

Flooding process:

* **A router notices a change in a link state and multicasts an LSU packet**(which includes the updated LSA entry with the sequence number incremented) to 224.0.0.6.
* This address goes to all OSPF DRs and BDRs. **On point-to-point links, the LSU is multicast to 224.0.0.5.)**
* An LSU packet might contain several distinct LSAs.
* The DR receives the LSU, processes it, acknowledges the receipt of the change and floods the LSU to other routers on the network using the OSPF multicast address 224.0.0.5.
* After receiving the LSU, each router responds to the DR with an LSAck.
* To make the flooding procedure reliable, each LSA must be acknowledged separately.
* **If a router is connected to other networks, it floods the LSU to those other networks by forwarding the LSU to the DR of the other network** (or to the adjacent router if in a point-topoint network).
* **That DR, in turn, multicasts the LSU to the other routers in the network.**
* **The DR receives the LSU, processes it, acknowledges the receipt of the change and floods the LSU to other routers on the network using the OSPF multicast address 224.0.0.5.**
* The router updates its LSDB using the LSU that includes the changed LSA.
* It then recomputes the SPF algorithm against the updated database after a short delay and updates the routing table as necessary.



**OSPF Path Costs**

Each router link/interface has an associated OSPF cost

The total cost between a router and a network is given by the sum of all OSPF costs of the (routers) output interfaces along the path.

Routers to access directly connect networks never use OSPF paths.

**OSPF Hierarchical Routing**

Large LSDB. Because the LSDB covers the topology of the entire network, each router must maintain an entry for every network in the area, even if not every route is selected for the routing table.

Frequent SPF algorithm calculations. In a large network, changes are inevitable, so the routers spend many CPU cycles recalculating the SPF algorithm and updating the routing table.

Large routing table. OSPF does not perform route summarization by default. If the routes are not summarized, the routing tables can become very large, depending on the size of the network.

Link-state routing protocols usually reduce the size of the Dijkstra calculations by partitioning the network into areas.

Using **multiple OSPF areas has several important advantages**

* Reduced frequency of SPF calculations(Detailed route information only exists within each area It is not necessary to flood all link-state changes to all other areas.)
* Rather than send an update about each network within an area, a router can advertise a single summarized route or a small number of routes between areas, thereby reducing the overhead associated with updates when they cross areas.
* Smaller routing tables.

**OSPF Two-Layer Area Hierarchy**

1. **Backbone área->** An OSPF area whose primary function is the fast and efficient movement of IP packets. The backbone area interconnect with all other OSPF áreas. The backbone area is also called OSPF area 0. **Hierarchical networking defines area 0 as the core to which all other areas connect (directly or virtually).**
2. **Regular (non backbone) área**-> An OSPF area whose primary function is to connect users and resources. By default, a regular area does not allow traffic from another area to use its links to reach other áreas

**OSPF Routers Types**

A router can be more than one router typ

1. **Internal router**
   1. Routers that have all of their interfaces in the same area.
   2. All routers within the same area have identical LSDBs
2. **Backbone router**
   1. Routers that sit in the perimeter of the backbone area 0 and that have at least one interface connected to area 0.
   2. Backbone routers maintain OSPF routing information using the same procedures and algorithms as internal routers.
3. **Area Border Router (ABR)**
   1. Routers that have interfaces attached to multiple areas, maintain separate LSDBs for each area to which they connect, and route traffic destined for or arriving from other areas.
4. **Autonomous System Boundary Router (ASBR)**
   1. Routers that have at least one interface attached to a different routing domain (such as another OSPF autonomous system or a domain using other routing protocol).

**Stub Areas**

Configuring a stub area reduces the size of the LSDB inside an area, resulting in reduced memory requirements for routers in that área

Routers within the stub area also do not have to run the SPF algorithm as often because they will receive fewer routing updates.

Routing from these areas to a route external to the OSPF autonomous system is based on a default route (0.0.0.0). Stub area ABR when receives an external LSA, sends a 0.0.0.0 LSA to the stub area. If a packet is addressed to a network that is not in the routing table of an internal router, the router automatically forwards the packet to the ABR that originates a 0.0.0.0 LSA.

**Areas Virtual Links**

Virtual Links can be used to connect a discontiguous Area 0.

Virtual Links can be used to connect an area to the backbone Area

**OSPF LSA Types**

1. **Type 1 (Router LSA)** - Every router generates router-link advertisements for each area to which it belongs. Router-link advertisements describe the states of the router’s links to the area and are flooded only within a particular area. All types of LSAs have 20-byte LSA headers. One of the fields of the LSA header is the link-state ID**. The link-state ID of the type 1 LSA is the originating router’s ID.**
2. Type 2 (Network LSA) - DRs generate network link advertisements for multiaccess networks, which describe the set of routers attached to a particular multiaccess network. Network link advertisements are flooded in the area that contains the network. The link-state ID of the type 2 LSA is the DR’s IP interface address.
3. Types 3 and 4 (Summary LSA) - ABRs generate summary link advertisements. Summary link advertisements describe the following inter-area routes

**OSPF AREA Types**