TUGAS COORDINATED LEARNING TOPIC 10-11

Anggota Kelompok 3

- **Edward Engelbert Wiguna**
- **Elvio Andersoon**
- **Mario Imanuel Daruranto**
- **Muhammad Addis Reza**
- **Vincent Hernandy**

layer 2 vs layer 3 comparison (Edward)

1. Layer 2 switches operate at the Data Link Layer (Layer 2) of the OSI model, while Layer 3 switches operate at the Network Layer (Layer 3).
2. Layer 2 switches are used to forward traffic between devices within a LAN (Local Area Network), while Layer 3 switches are used to route traffic between different networks.
3. Layer 2 switches use MAC addresses to make forwarding decisions, while Layer 3 switches use IP addresses.
4. Layer 2 switches are generally less expensive and less complex than Layer 3 switches.
5. Layer 3 switches can provide better network performance and scalability, especially in larger networks with multiple subnets.
6. Layer 3 switches can perform advanced routing features such as Quality of Service (QoS) and Access Control Lists (ACLs), which are not available on Layer 2 switches.
7. Layer 2 switches are typically used in access layer switches in the network topology, while Layer 3 switches are used in distribution or core switches.
8. Layer 2 switches are good for small to medium-sized networks, while Layer 3 switches are more appropriate for larger networks that require more complex routing and network segmentation.
9. Layer 3 switches can be used in place of routers in some cases, especially in smaller networks where the routing requirements are not complex.
10. When choosing between Layer 2 and Layer 3 switches, the network size, complexity, and routing requirements should be considered to determine which type of switch is most appropriate for the network.

reference:
https://www.troubleshootingcentral.com/layer-2-vs-layer-3-switches-comparison/

layer vs layer 3 comparison (Mario)

reference :

https://www.geeksforgeeks.org/difference-between-layer-2-and-layer-3-switches/

A switch is a network device that sends data packets within a local network. Unlike a hub, a switch learns which device is connected to which port and only sends the packets to the intended destination device. Layer-2 switches operate on the data link layer of the OSI model and use MAC address tables to send frames to the destination port. They are fast and used to reduce traffic on a local network. They have a single broadcast domain and can only communicate within the network.

On the other hand, layer-3 switches operate on the network layer of the OSI model and route packets using IP addresses. They can function as both layer-2 and layer-3 switches and are commonly used to implement VLANs. They take time to examine data packets before sending them to their destination and have multiple broadcast domains. Layer-3 switches can communicate both within and outside the network.

In summary, layer-2 switches are fast and used to reduce traffic on a local network. They operate on the data link layer and use MAC address tables to send frames to the destination port. Layer-3 switches, on the other hand, operate on the network layer and route packets using IP addresses. They can function as both layer-2 and layer-3 switches, have multiple broadcast domains, and can communicate within and outside the network.

Week 10 (4.6 dan 4.7) (Elvio) (Addis)

4.6 Routing in the internet

- Routing Information Protocol (RIP)

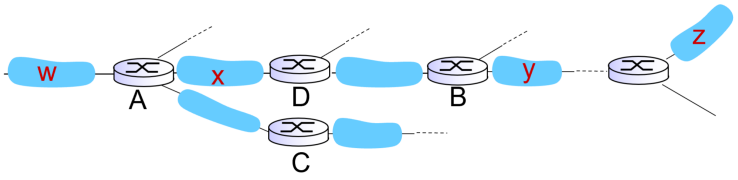
Cisco. (2005). Routing Information Protocol (RIP). Diakses melalui https://www.cisco.com/c/en/us/support/docs/ip/routing-information-protocol-rip/13788-3.html

Routing Information Protocol (RIP) adalah salah satu protokol routing yang digunakan dalam jaringan komputer untuk mengatur pengiriman paket data antara host dan router. Fungsi dari RIP adalah untuk memperbarui dan memelihara tabel routing pada setiap router dalam jaringan sehingga dapat mengetahui jalur mana yang harus diambil untuk mengirim paket data ke tujuan. Cara kerja dari RIP adalah dengan mengirimkan pesan (message) ke router lain dalam jaringan untuk memperbarui tabel routing pada router tersebut. RIP menggunakan metode perhitungan jarak yang diukur dalam hop count, yaitu jumlah hop (router yang dilalui) yang diperlukan untuk mencapai tujuan. RIP menggunakan algoritma Bellman-Ford untuk memperbarui tabel routing pada setiap router dalam jaringan. Tujuan dari RIP adalah untuk mengoptimalkan pengiriman paket data dalam jaringan dengan memilih jalur terpendek ke tujuan.

Jenis-jenis RIP terdiri dari RIP-1 dan RIP-2. RIP-1 adalah versi awal dari protokol RIP dan memiliki batasan hop count maksimum sebanyak 15. RIP-2 memiliki fitur tambahan seperti subnetting dan authentikasi, serta mampu mengatasi batasan hop count pada RIP-1 dengan memperbolehkan hop count maksimum hingga 255.

Contoh RIP :

RIP: example



routing table in router D

destination subnet	next router	# hops to dest
w	A	2
y	B	2
z	B	7
x	--	1
....	....	....

- Open Shortest Path First (OSPF)

Cisco. (2019). Open Shortest Path First (OSPF). Diakses melalui https://www.cisco.com/c/en/us/support/docs/ip/open-shortest-path-first-ospf/7039-1.html

Open Shortest Path First (OSPF) adalah protokol routing yang digunakan untuk mengatur pengiriman paket data di dalam jaringan komputer. Fungsi dari OSPF adalah untuk memilih jalur terbaik atau shortest path dalam jaringan yang menggunakan routing berbasis IP. OSPF digunakan untuk memperbarui tabel routing pada setiap router dalam jaringan sehingga dapat mengetahui jalur terpendek ke setiap tujuan. Cara kerja OSPF adalah dengan mengirimkan pesan (message) OSPF antara router yang terhubung ke jaringan OSPF. Pesan ini digunakan untuk memperbarui tabel routing pada setiap router di dalam jaringan OSPF. OSPF menggunakan algoritma Dijkstra untuk menghitung jalur terpendek atau shortest path dalam jaringan. Tujuan dari OSPF adalah untuk mempercepat pengiriman paket data di dalam jaringan dengan memilih jalur terpendek. Selain itu, OSPF juga dapat memilih jalur backup atau alternatif untuk menghindari kegagalan jalur utama dalam jaringan.

Jenis-jenis OSPF terdiri dari OSPFv1 dan OSPFv2. OSPFv1 hanya mendukung IPv4 sedangkan OSPFv2 mendukung IPv4 dan IPv6. Selain itu, OSPF juga dapat diklasifikasikan menjadi dua jenis yaitu single area OSPF dan multi area OSPF. Single area OSPF digunakan

untuk jaringan yang relatif kecil dan sederhana, sedangkan multi area OSPF digunakan untuk jaringan yang lebih besar dan kompleks.

Contoh penggunaan OSPF adalah pada jaringan WAN (Wide Area Network) yang kompleks dan terdiri dari beberapa area. OSPF sangat efektif pada jaringan WAN yang besar dan kompleks karena OSPF dapat menghitung jalur terpendek dan tercepat pada setiap area secara terpisah.

- Interior Gateaway Routing Protocol (IGRP)

Cisco. (2006). Interior Gateway Routing Protocol (IGRP). Diakses melalui https://www.cisco.com/c/en/us/support/docs/ip/interior-gateway-routing-protocol-igrp/8641-21.html

Interior Gateway Routing Protocol (IGRP) adalah protokol routing yang digunakan pada jaringan komputer yang terdiri dari beberapa router yang terhubung dalam satu domain administratif atau sistem otonom (autonomous system). Fungsi dari IGRP adalah untuk mengatur pengiriman paket data antara host dan router dalam jaringan dengan menggunakan tabel routing yang diperbarui secara dinamis. IGRP menggunakan algoritma distance vector untuk menghitung jarak terpendek antara router dan tujuan. Cara kerja IGRP adalah dengan mengirimkan pesan (message) ke router lain dalam jaringan untuk memperbarui tabel routing pada router tersebut. Setiap router akan melakukan perhitungan jarak terpendek menggunakan informasi yang diperoleh dari pesan yang diterima dari router lain dalam jaringan.

Jenis-jenis IGRP terdiri dari IGRP dan Enhanced IGRP (EIGRP). EIGRP adalah versi yang ditingkatkan dari IGRP yang memiliki fitur tambahan seperti load balancing, konvergensi yang lebih cepat, dan kemampuan untuk mengatur bandwidth dan delay pada jaringan. Tujuan dari IGRP adalah untuk memilih jalur terpendek ke tujuan dengan mempertimbangkan jarak terpendek dan kondisi jaringan. IGRP juga memastikan bahwa data dikirim melalui jalur yang aman dan dapat menghindari jalur yang bermasalah atau rusak.

Contoh penggunaan IGRP adalah pada jaringan LAN (Local Area Network) yang relatif besar atau pada WAN (Wide Area Network). IGRP sangat efektif pada jaringan yang relatif kompleks dan memiliki banyak router yang terhubung.

4.7 broadcast and multicast routing

http://www.enterprisenetworkingplanet.com/netsp/article.php/3615896/Networking-101-Understanding-BGP-Routing.htm

Border Gateway Protocol (BGP) is a routing protocol used to exchange routing information between different networks on the internet. It is a complex and highly scalable protocol that is designed to manage the routing of traffic between autonomous systems (ASes). BGP is used to exchange information about the available paths that exist between different networks, allowing routers to select the best path for routing data. This information includes things like the IP address of the destination network, the number of AS hops required to reach that network, and other attributes that can be used to determine the best route. BGP is a critical component of the internet's infrastructure, as it enables the interconnection of thousands of different networks, each with their own unique routing policies and requirements. It also plays a key role in enabling internet service providers (ISPs) to exchange traffic with each other and with their customers, ensuring that data can be transmitted reliably and efficiently across the internet.

5.3 Multiple Access Protocols (Vincent)

Pada poin ini membahas dua jenis "link" dalam jaringan, yaitu point-to-point dan broadcast. Link point-to-point terdiri dari PPP untuk akses dial-up dan link point-to-point antara switch Ethernet dan host. Sementara itu, link broadcast digunakan untuk shared wire atau medium, seperti Ethernet lama, upstream HFC, dan 802.11 wireless LAN. Untuk mengatur penggunaan saluran yang dibagi, digunakanlah protokol multiple access (MAC). Protokol MAC adalah algoritma terdistribusi yang menentukan bagaimana node-node dalam jaringan berbagi saluran komunikasi. Protokol MAC juga bertanggung jawab dalam menentukan kapan suatu node dapat melakukan transmisi. Saat menggunakan protokol multiple access, komunikasi tentang pembagian saluran harus dilakukan melalui saluran itu

sendiri. Tidak ada saluran out-of-band yang dapat digunakan untuk koordinasi. Jika dua atau lebih transmisi terjadi pada saat bersamaan, akan terjadi interferensi atau tabrakan sinyal, yang disebut collision.

selanjutnya ada membahas tentang sebuah protokol multiple access yang ideal yang memiliki empat desiderata yaitu, dapat mengirimkan data pada kecepatan R bps, saat M node ingin mengirimkan data, setiap node dapat mengirimkan data pada kecepatan rata-rata R/M, protokol yang sepenuhnya terdesentralisasi tanpa kebutuhan node khusus untuk mengkoordinasikan transmisi dan sinkronisasi waktu, serta protokol yang sederhana. Selain itu, terdapat dua jenis protokol multiple access berdasarkan pembagian saluran, yaitu TDMA (time division multiple access) dan FDMA (frequency division multiple access). Pada protokol TDMA, saluran diakses secara bergantian dan setiap stasiun mendapatkan slot waktu yang telah ditentukan untuk mengirimkan paket data. Sedangkan pada protokol FDMA, spektrum saluran dibagi menjadi beberapa pita frekuensi dan setiap stasiun diberikan pita frekuensi tetap untuk mengirimkan data. Unused transmission time atau waktu transmisi yang tidak digunakan pada setiap pita frekuensi dijadikan sebagai idle atau kosong.

Slotted ALOHA adalah protokol akses berganda yang menganggap semua frame memiliki ukuran yang sama, waktu dibagi menjadi slot berukuran sama, dan node mulai mengirimkan hanya pada awal slot. Jika dua atau lebih node mengirimkan dalam slot, tabrakan terjadi dan semua node mendeteksinya. Ketika sebuah node mendapatkan frame baru, ia mentransmisikannya di slot berikutnya, dan jika tidak ada tabrakan, node tersebut dapat mengirim frame baru di slot berikutnya. Jika tidak, node mentransmisikan ulang frame di setiap slot berikutnya dengan probabilitas p hingga sukses.Slotted ALOHA memiliki beberapa keunggulan, termasuk node aktif tunggal yang dapat terus mentransmisikan pada kecepatan penuh saluran, sangat terdesentralisasi, dan sederhana. Namun, ini juga memiliki beberapa kekurangan seperti tabrakan, slot kosong, dan masalah sinkronisasi jam.

Efisiensi Slotted ALOHA adalah fraksi jangka panjang dari slot yang berhasil, dan efisiensi maksimumnya adalah 1/e atau 0,37. Sebaliknya, Pure ALOHA adalah protokol akses ganda yang lebih sederhana yang tidak memerlukan sinkronisasi. Ketika sebuah frame tiba, itu segera ditransmisikan, dan probabilitas tabrakan meningkat ketika sebuah frame yang dikirim pada t0 bertabrakan dengan frame lain yang dikirim dalam [t0-1,t0+1].

CSMA (Carrier Sense Multiple Access) adalah protokol tempat node mendengarkan saluran sebelum melakukan transmisi. Jika saluran dianggap diam, node mentransmisikan

seluruh frame; jika tidak, transmisi akan ditunda. Namun, tabrakan masih dapat terjadi karena penundaan propagasi. CSMA/CD (Collision Detection) adalah perpanjangan dari CSMA yang mendeteksi tabrakan dan membatalkan transmisi, mengurangi pemborosan saluran. Algoritma CSMA/CD Ethernet terdiri dari lima langkah: NIC menerima datagram, mengindera saluran, mentransmisikan jika diam, membatalkan dan mengirimkan sinyal jam jika mendeteksi transmisi lain, dan memasuki backoff biner setelah Collision Mth

"Taking turns" MAC protocols digunakan untuk berbagi saluran secara efisien dan adil di antara beberapa node. Protokol partisi saluran membagi saluran menjadi bagian-bagian yang lebih kecil, sementara protokol akses acak memungkinkan node untuk mengirimkan kapan pun mereka mau. Polling adalah protokol "taking turns" di mana node master mengundang node budak untuk mengirimkan secara bergantian. Token passing adalah protokol "taking turns" lainnya di mana token kontrol diteruskan dari satu node ke node berikutnya secara berurutan. Baik polling maupun token passing memiliki kekhawatiran tentang overhead, latensi, dan titik kegagalan tunggal.

Jaringan akses kabel memiliki banyak saluran hilir dan beberapa saluran hulu. Saluran downstream disiarkan dari satu CMTS, sedangkan saluran upstream dibagikan oleh semua pengguna melalui contention dan beberapa slot yang ditetapkan. DOCSIS adalah standar yang digunakan untuk data melalui spesifikasi antarmuka layanan kabel. Ini menggunakan FDM melalui saluran upstream dan downstream dan TDM untuk slot upstream. Slot upstream ditetapkan melalui bingkai MAP, sedangkan slot berbasis contention diakses melalui akses acak menggunakan backoff biner di slot yang dipilih.

Sumber:

- ppt
- https://www.geeksforgeeks.org/multiple-access-protocols-in-computer-network/
- https://www.javatpoint.com/multiple-access-protocols

5.4 LANs (vincent)

Alamat MAC (Kontrol Akses Media) dan ARP (Protokol Resolusi Alamat)

- Alamat IP 32-bit: alamat lapisan jaringan untuk antarmuka dan digunakan untuk penerusan lapisan 3 (lapisan jaringan).

- Alamat MAC (atau LAN atau fisik atau Ethernet): fungsi: digunakan 'secara lokal" untuk mendapatkan bingkai dari satu antarmuka ke antarmuka lain yang terhubung secara fisik (jaringan yang sama, dalam pengertian pengalamatan IP). Alamat MAC 48 bit (untuk sebagian besar LAN) dibakar dalam NIC ROM, terkadang juga perangkat lunak dapat diatur.

Ethernet adalah teknologi LAN kabel yang dominan, dengan harga murah sekitar $20 untuk NIC. Ini adalah teknologi LAN yang pertama digunakan secara luas, lebih sederhana dan lebih murah dibandingkan dengan token LAN dan ATM, serta mampu mengikuti perlombaan kecepatan dari 10 Mbps hingga 10 Gbps. Topologi fisik Ethernet terdiri dari bus dan star. Topologi bus populer hingga pertengahan 90-an, di mana semua simpul berada dalam domain tumbukan yang sama dan dapat bertabrakan satu sama lain. Sedangkan topologi star yang lebih umum digunakan saat ini memiliki switch aktif di tengah dan setiap "cabang" menjalankan protokol Ethernet yang terpisah (simpul tidak bertabrakan satu sama lain).

Struktur frame Ethernet terdiri dari beberapa bagian. Adapter pengirim akan mengkapsulasi datagram IP (atau paket protokol lapisan jaringan lainnya) dalam frame Ethernet. Preamble terdiri dari 7 byte dengan pola 10101010 diikuti oleh satu byte dengan pola 10101011. Preamble digunakan untuk menyesuaikan kecepatan jam penerima dan pengirim. Frame Ethernet juga memiliki alamat MAC sumber dan tujuan sepanjang 6 byte. Jika adapter menerima frame dengan alamat tujuan yang cocok atau dengan alamat siaran (seperti paket ARP), adapter akan meneruskan data dalam frame ke protokol lapisan jaringan, jika tidak, adapter akan membuang frame tersebut. Type menunjukkan protokol lapisan atas (biasanya IP tetapi protokol lain juga dimungkinkan, seperti Novell IPX, AppleTalk). Terakhir, CRC (Cyclic Redundancy Check) digunakan untuk mendeteksi kesalahan pada saat penerima menerima frame. Jika kesalahan terdeteksi, frame akan dibuang.

Ethernet switch adalah perangkat pada link-layer yang memiliki peran aktif dalam mengirimkan dan menerima frame Ethernet. Switch ini dapat menyimpan dan meneruskan frame Ethernet, serta melakukan pemeriksaan terhadap alamat MAC pada frame yang masuk dan memilih untuk meneruskan frame tersebut ke salah satu atau beberapa link keluar. Untuk meneruskan frame pada segmen yang sama, switch menggunakan metode akses CSMA/CD. Meskipun switch memiliki peran aktif dalam jaringan, host pada jaringan tidak menyadari keberadaan switch karena switch bersifat transparan. Keunggulan lain dari Ethernet switch adalah bahwa perangkat ini dapat langsung digunakan (plug-and-play) dan mempelajari sendiri konfigurasi jaringan tanpa perlu konfigurasi manual dari administrator.

Switch memungkinkan terjadinya transmisi simultan yang lebih dari satu. Host memiliki koneksi langsung dan khusus ke switch, dan switch akan menyimpan paket dalam buffer. Protokol Ethernet digunakan pada setiap link masuk, tetapi tidak ada tabrakan (collision) karena setiap link memiliki collision domain sendiri dan menggunakan mode full duplex. Proses switching memungkinkan transmisi A-to-A' dan B-to-B' secara simultan tanpa tabrakan. Setiap switch memiliki tabel forwarding yang memetakan alamat MAC host ke interface untuk mencapainya, seperti routing table. Switch dapat belajar sendiri mengenai host yang dapat dicapai melalui interface mana, dan menyimpan informasi tersebut dalam tabel forwarding. Ketika sebuah frame diterima, switch akan mencatat lokasi pengirim pada tabel forwarding. Ketika switch dihubungkan satu sama lain, proses self-learning tetap berlaku, sehingga switch akan mempelajari cara mengirim frame ke tujuan melalui switch lain.

Switch dan router sama-sama menggunakan metode store-and-forward dalam mengirimkan paket data. Namun, perbedaan terletak pada lapisan jaringan yang diperiksa. Router adalah perangkat pada lapisan jaringan yang memeriksa header jaringan, sedangkan switch adalah perangkat pada lapisan link yang memeriksa header link. Kedua perangkat juga memiliki tabel forwarding. Namun, router menghitung tabel forwarding dengan menggunakan algoritma routing dan alamat IP, sedangkan switch mempelajari tabel forwarding dengan menggunakan metode flooding, learning, dan alamat MAC.

Penggunaan satu domain broadcast pada jaringan LAN dapat menimbulkan masalah keamanan, privasi, dan efisiensi, karena semua lalu lintas broadcast pada lapisan 2 (ARP, DHCP, alamat MAC tujuan yang tidak diketahui) harus melintasi seluruh jaringan LAN. Oleh karena itu, VLAN (Virtual Local Area Network) digunakan untuk membagi jaringan fisik menjadi beberapa jaringan virtual yang terpisah. Switch yang mendukung fitur VLAN dapat dikonfigurasi untuk mendefinisikan beberapa jaringan virtual di atas satu infrastruktur jaringan fisik. VLAN dapat dikonfigurasi berdasarkan port, di mana port switch dikelompokkan menjadi beberapa switch virtual terpisah. Ini memungkinkan isolasi lalu lintas antar port dan memungkinkan pengaturan VLAN berdasarkan alamat MAC endpoint. Port VLAN juga dapat diatur secara dinamis, sehingga memungkinkan pengalokasian port antar VLAN secara fleksibel. Forwarding antar VLAN dilakukan melalui routing seperti halnya dengan switch terpisah, namun beberapa vendor menyediakan kombinasi switch dan router dalam satu perangkat. VLAN dapat mencakup beberapa switch fisik melalui port trunk. Trunk port digunakan untuk mengirimkan frame antar VLAN yang terdefinisi pada

beberapa switch fisik. Untuk ini, protokol 802.1q menambahkan informasi header tambahan pada frame yang diteruskan melalui port trunk.

Sumber:

- ppt