**Pertemuan 7**

**PERANGKAT JARINGAN DAN TIPE PENGKABELAN**

1. **Tujuan Pembelajaran**

Pada Pertemuan Ini Akan Di Jelaskan Pengetahuan Dasar (Basic Science) Tentang Definisi Perangkat Jaringan Dan Tipe Pengkabelan. Anda Harus Mampu:

* 1. Mengetahui perangkat jaringan sebagai komponen fisik yang digunakan untuk menghubungkan dan mengatur komunikasi antar komputer atau perangkat dalam jaringan komputer.
  2. Mengidentifikasi perangkat jaringan utama seperti switch, router, access point, dan hub serta mengetahui peran dan fungsinya dalam arsitektur jaringan.
  3. Memahami konsep dan prinsip dasar seperti alamat MAC (Media Access Control), forwarding, dan filtering yang menjadi dasar operasi perangkat jaringan.
  4. Mengetahui hubungan antara perangkat jaringan dengan lapisan OSI (Open Systems Interconnection) dan protokol jaringan yang beroperasi pada setiap lapisan.
  5. Mengetahui karakteristik, kelebihan, dan kelemahan dari berbagai jenis kabel yang digunakan dalam jaringan komputer seperti kabel serat optik, kabel tembaga (UTP, STP), dan kabel koaksial.
  6. Memahami konsep dasar seperti kecepatan transfer data, jarak, dan ketahanan terhadap gangguan elektromagnetik (EMI) yang mempengaruhi kinerja pengkabelan.
  7. Mengetahui standar dan spesifikasi yang terkait dengan tipe pengkabelan seperti kategori kabel UTP dan jenis konektor yang digunakan.
  8. Mampu merancang, mengimplementasikan, dan mengelola infrastruktur jaringan yang sesuai dengan kebutuhan spesifik organisasi, dengan mempertimbangkan pemilihan perangkat jaringan dan tipe pengkabelan yang optimal.

1. **Uraian Materi**

**Tujuan Pembelajaran 1**

Mengetahui perangkat jaringan sebagai komponen fisik yang digunakan untuk menghubungkan dan mengatur komunikasi antar komputer atau perangkat dalam jaringan komputer.

Perangkat jaringan adalah komponen fisik yang digunakan untuk menghubungkan dan mengatur komunikasi antar komputer atau perangkat dalam sebuah jaringan komputer. Ini termasuk berbagai perangkat keras yang memungkinkan jaringan komputer berfungsi dengan baik. Berikut beberapa perangkat jaringan yang umum digunakan:

1. **Switch**: Switch adalah perangkat jaringan yang digunakan untuk menghubungkan beberapa perangkat dalam jaringan lokal (LAN). Switch bekerja pada tingkat data link layer (layer 2 dalam model OSI) dan dapat mengirimkan data hanya ke perangkat yang dituju, sehingga memungkinkan komunikasi yang lebih efisien dalam jaringan.



Gambar 1.1 Device Switch dan HUB

1. **Router**: Router adalah perangkat yang digunakan untuk menghubungkan dua atau lebih jaringan dan mengarahkan lalu lintas data antara mereka. Router bekerja pada tingkat jaringan (layer 3 dalam model OSI) dan mampu mengambil keputusan tentang rute terbaik untuk mengirimkan paket data ke tujuan yang tepat.



Gambar 1.2 Device Router

1. **Hub**: Hub adalah perangkat yang digunakan untuk menghubungkan beberapa perangkat dalam jaringan. Namun, hub tidak memiliki kemampuan untuk memahami alamat tujuan seperti switch, sehingga ketika menerima data, hub akan mengirimkannya ke semua perangkat yang terhubung, yang dapat mengakibatkan penggunaan bandwidth yang tidak efisien.
2. **Access Point (AP)**: Access point adalah perangkat yang digunakan untuk menyediakan akses ke jaringan nirkabel (Wi-Fi). AP mengubah sinyal kabel menjadi sinyal nirkabel sehingga perangkat nirkabel seperti laptop, smartphone, atau tablet dapat terhubung ke jaringan.



Gambar 1.3 Device AP/Modem/bridge

1. **Modem**: Modem adalah perangkat yang digunakan untuk menghubungkan jaringan komputer dengan jaringan luar, seperti jaringan internet. Modem mengubah sinyal digital dari komputer menjadi sinyal analog yang dapat ditransmisikan melalui media transmisi seperti kabel telepon atau serat optik, dan sebaliknya.
2. **Bridge**: Bridge adalah perangkat yang menghubungkan dua segmen jaringan lokal (LAN) untuk membentuk jaringan yang lebih besar. Bridge bekerja pada tingkat data link layer dan dapat memutuskan apakah paket data harus diteruskan atau tidak berdasarkan alamat MAC.

**Tujuan Pembelajaran 2**

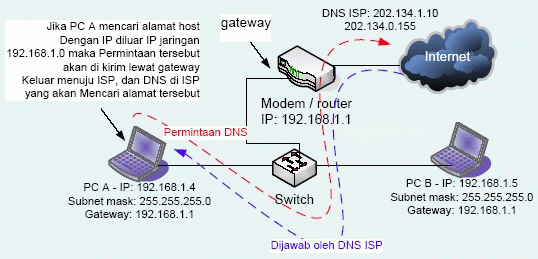
Mengidentifikasi perangkat jaringan utama seperti switch, router, access point, dan hub serta mengetahui peran dan fungsinya dalam arsitektur jaringan.

1. **Switch**: Peran switch dalam arsitektur jaringan adalah sebagai pengatur lalu lintas data di dalam jaringan lokal (LAN). Fungsinya adalah untuk menghubungkan beberapa perangkat dalam jaringan dan mengarahkan data hanya ke perangkat yang dituju. Dengan demikian, switch memastikan efisiensi komunikasi antar perangkat dalam jaringan lokal, serta meminimalkan kemacetan lalu lintas data.
2. **Router**: Router memiliki peran yang krusial dalam menghubungkan jaringan yang berbeda dan mengelola aliran data antara mereka. Fungsinya adalah untuk mengambil keputusan tentang rute terbaik untuk mengirimkan paket data ke tujuan yang tepat. Dengan melakukan ini, router memungkinkan komunikasi antara perangkat dari jaringan yang berbeda, baik itu jaringan lokal (LAN) maupun jaringan luas (WAN), seperti internet.
3. **Access Point (AP)**: Peran access point dalam arsitektur jaringan adalah sebagai titik akses untuk perangkat nirkabel ke jaringan kabel. Fungsinya adalah untuk menyediakan akses nirkabel ke jaringan, memungkinkan perangkat yang kompatibel untuk terhubung dan berkomunikasi dalam jaringan tanpa menggunakan kabel fisik. Dengan demikian, access point memungkinkan fleksibilitas dalam mengakses jaringan, terutama dalam lingkungan yang membutuhkan konektivitas nirkabel.
4. **Hub**: Meskipun hub kurang umum digunakan saat ini karena kelemahan dalam efisiensi penggunaan bandwidth, perannya dalam arsitektur jaringan adalah sebagai penyedia konektivitas dasar antara perangkat dalam jaringan. Fungsinya adalah untuk menghubungkan beberapa perangkat dalam jaringan, meskipun tidak memiliki kemampuan untuk memahami alamat tujuan seperti switch. Namun, karena kekurangannya dalam efisiensi penggunaan bandwidth, penggunaan hub biasanya digantikan oleh switch.

**Tujuan Pembelajaran 3**

Memahami konsep dan prinsip dasar seperti alamat MAC (Media Access Control), forwarding, dan filtering yang menjadi dasar operasi perangkat jaringan

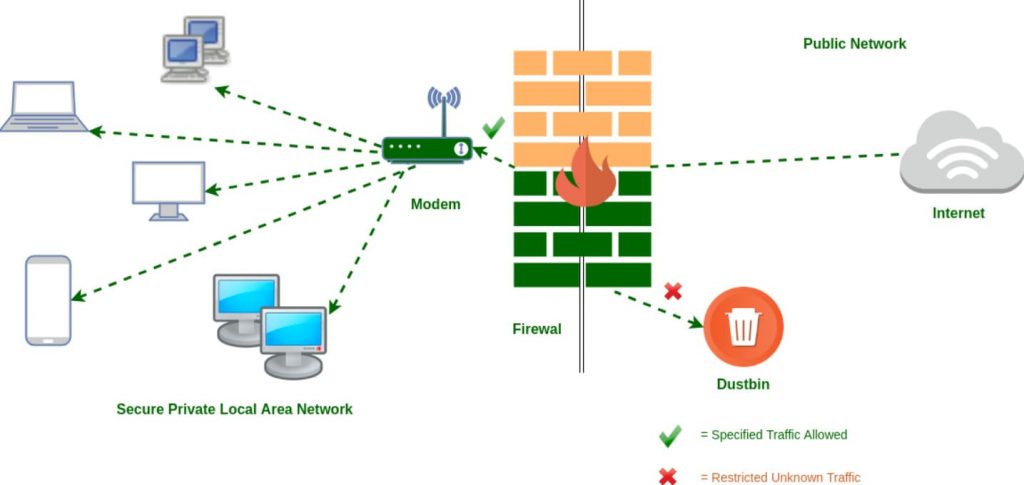
1. **Alamat MAC (Media Access Control)**:
   * Alamat MAC adalah identifikasi unik yang diberikan kepada setiap perangkat jaringan yang terhubung dalam jaringan. Ini terdiri dari 48 bit (biasanya diekspresikan dalam format heksadesimal), yang digunakan oleh perangkat jaringan untuk mengirim data ke perangkat yang tepat dalam jaringan.
   * Alamat MAC ditanamkan pada perangkat jaringan saat diproduksi dan tidak dapat diubah oleh pengguna. Ini memastikan keunikan alamat MAC di seluruh jaringan.
   * Saat sebuah perangkat ingin mengirimkan data, ia menggunakan alamat MAC tujuan untuk mengarahkan paket data ke perangkat yang tepat dalam jaringan. Ini adalah bagian penting dari proses pengiriman data dalam jaringan.
2. **Forwarding**:



Gambar 3.1 Forwarding DNS

* + Forwarding adalah proses di mana sebuah perangkat jaringan (misalnya switch atau router) mengirimkan paket data dari satu antarmuka ke antarmuka lainnya dalam jaringan berdasarkan informasi yang diperoleh dari tabel pengalihan.
  + Ketika perangkat jaringan menerima paket data, ia memeriksa alamat MAC tujuan dalam paket tersebut dan mencocokkannya dengan tabel pengalihan untuk menentukan ke antarmuka mana paket harus dikirimkan.
  + Proses forwarding memungkinkan perangkat jaringan untuk mengirimkan paket data ke tujuan dengan efisien, memastikan bahwa data mencapai perangkat yang dituju dengan cepat dan akurat.

1. **Filtering**:



Gambar 3.2 Filtering DNS

* + Filtering adalah proses di mana perangkat jaringan (seperti switch atau router) memutuskan apakah suatu paket data harus diteruskan atau dibuang berdasarkan kriteria tertentu.
  + Kriteria untuk filtering dapat berupa alamat MAC, alamat IP, jenis protokol, atau atribut lainnya dari paket data.
  + Filtering digunakan untuk mengontrol aliran lalu lintas dalam jaringan, memastikan keamanan, keamanan, dan kinerja yang optimal. Misalnya, sebuah router dapat menerapkan filtering untuk mencegah akses dari luar jaringan lokal, sementara sebuah switch dapat menggunakan filtering untuk mencegah serangan jaringan atau membatasi lalu lintas ke jalur tertentu.

**Tujuan Pembelajaran 4**

Mengetahui hubungan antara perangkat jaringan dengan lapisan OSI (Open Systems Interconnection) dan protokol jaringan yang beroperasi pada setiap lapisan.

Model OSI adalah kerangka kerja yang digunakan untuk memahami bagaimana komunikasi data terjadi dalam jaringan komputer. Ini terdiri dari tujuh lapisan yang mewakili fungsi-fungsi yang berbeda dalam proses komunikasi data. Berikut adalah hubungan antara perangkat jaringan dengan setiap lapisan OSI dan protokol yang beroperasi pada setiap lapisan:

1. **Lapisan Fisik (Layer 1)**:

* Perangkat jaringan yang beroperasi pada lapisan fisik termasuk kabel, konektor, repeater, dan perangkat jaringan lainnya yang mengatur transmisi data fisik dalam jaringan.
* Protokol yang beroperasi pada lapisan fisik termasuk Ethernet, Wi-Fi (802.11), dan protokol lainnya yang mengatur sinyal dan transmisi data fisik antara perangkat dalam jaringan.

1. **Lapisan Data Link (Layer 2)**:

* Perangkat jaringan yang beroperasi pada lapisan data link meliputi switch dan bridge. Mereka bertanggung jawab untuk mengirimkan paket data antara perangkat dalam jaringan lokal (LAN).
* Protokol yang beroperasi pada lapisan data link termasuk Ethernet (MAC), PPP (Point-to-Point Protocol), dan protokol lainnya yang mengatur pengiriman data antara perangkat dalam jaringan lokal.

1. **Lapisan Jaringan (Layer 3)**:

* Perangkat jaringan yang beroperasi pada lapisan jaringan termasuk router. Router mengarahkan lalu lintas data antara jaringan yang berbeda.
* Protokol yang beroperasi pada lapisan jaringan termasuk Internet Protocol (IP), Internet Control Message Protocol (ICMP), dan protokol lainnya yang mengatur rute dan pengiriman paket data antara jaringan.

1. **Lapisan Transport (Layer 4)**:

* Perangkat jaringan tidak umum beroperasi pada lapisan transport, tetapi perangkat lunak seperti firewall dan proxy server dapat memengaruhi lalu lintas data pada lapisan ini.
* Protokol yang beroperasi pada lapisan transport termasuk Transmission Control Protocol (TCP), User Datagram Protocol (UDP), dan protokol lainnya yang mengatur koneksi dan pengiriman data end-to-end antara aplikasi.

1. **Lapisan Sesi (Layer 5)**:

* Perangkat jaringan tidak umum beroperasi pada lapisan sesi.

1. **Lapisan Presentasi (Layer 6)**:

* Perangkat jaringan tidak umum beroperasi pada lapisan presentasi.

1. **Lapisan Aplikasi (Layer 7)**:

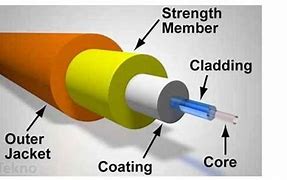
* Perangkat jaringan yang beroperasi pada lapisan aplikasi meliputi server web, server email, dan perangkat lain yang menyediakan layanan jaringan kepada pengguna akhir.
* Protokol yang beroperasi pada lapisan aplikasi termasuk HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol), dan protokol lainnya yang memungkinkan aplikasi berkomunikasi melalui jaringan.

Hubungan antara perangkat jaringan dengan lapisan OSI dan protokol yang beroperasi pada setiap lapisan memastikan bahwa komunikasi data dalam jaringan terjadi dengan efisien dan dapat diatur sesuai dengan fungsi-fungsi yang berbeda dalam model OSI.

**Tujuan Pembelajaran 5**

Mengetahui karakteristik, kelebihan, dan kelemahan dari berbagai jenis kabel yang digunakan dalam jaringan komputer seperti kabel serat optik, kabel tembaga (UTP, STP), dan kabel koaksial.

1. **Kabel Serat Optik**:
   * **Karakteristik**: Kabel serat optik menggunakan serat kaca atau plastik yang mengirimkan cahaya sebagai media transmisi data. Mereka memiliki lapisan pelindung yang kuat dan tidak rentan terhadap interferensi elektromagnetik.
   * **Kelebihan**:
     + Bandwidth yang tinggi: Kabel serat optik mampu mentransmisikan data dengan kecepatan yang sangat tinggi.
     + Tahan terhadap gangguan elektromagnetik: Kabel serat optik tidak dipengaruhi oleh interferensi elektromagnetik, membuatnya cocok untuk lingkungan yang bising secara elektromagnetik.
     + Jarak transmisi jauh: Serat optik dapat mentransmisikan data dalam jarak yang jauh tanpa degradasi sinyal yang signifikan.
   * **Kelemahan**:
     + Biaya: Kabel serat optik umumnya lebih mahal daripada kabel tembaga.
     + Kekurangan fleksibilitas: Kabel serat optik lebih rentan terhadap kerusakan fisik jika ditekuk atau ditarik dengan keras.



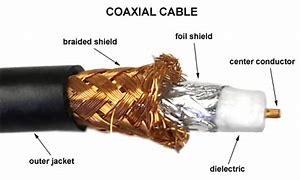
Gambar 5.1 kabel serat optik

1. **Kabel Tembaga (UTP, STP)**:
   * **Karakteristik**: Kabel tembaga terdiri dari kawat tembaga yang digunakan untuk mentransmisikan sinyal data. Ada dua jenis kabel tembaga yang umum digunakan: Unshielded Twisted Pair (UTP) dan Shielded Twisted Pair (STP).
   * **Kelebihan**:
     + Biaya: Kabel tembaga umumnya lebih murah daripada kabel serat optik.
     + Fleksibilitas: Kabel tembaga dapat ditekuk dan dipasang dengan mudah, membuatnya ideal untuk instalasi di dalam gedung atau rumah.
     + Mudah diinstalasi: Kabel tembaga lebih mudah dipasang daripada kabel serat optik.
   * **Kelemahan**:
     + Rentan terhadap interferensi elektromagnetik: Kabel tembaga rentan terhadap gangguan dari perangkat elektronik lain atau sumber interferensi elektromagnetik.
     + Jarak transmisi terbatas: Kabel tembaga memiliki jarak transmisi yang lebih pendek daripada kabel serat optik, dan sinyalnya dapat mengalami degradasi pada jarak yang lebih jauh.



Gambar 5.2 kabel STP dan UTP

1. **Kabel Koaksial**:
   * **Karakteristik**: Kabel koaksial terdiri dari inti tembaga yang dikelilingi oleh lapisan isolasi, lapisan konduktor, dan lapisan luar pelindung. Mereka digunakan untuk mentransmisikan sinyal analog dan digital.
   * **Kelebihan**:
     + Bandwidth yang cukup besar: Kabel koaksial dapat mentransmisikan data dengan kecepatan yang cukup tinggi.
     + Tahan terhadap gangguan: Kabel koaksial memiliki lapisan pelindung yang kuat, membuatnya tahan terhadap interferensi elektromagnetik.
     + Jarak transmisi yang baik: Kabel koaksial dapat mentransmisikan data dalam jarak yang cukup jauh tanpa degradasi sinyal yang signifikan.
   * **Kelemahan**:
     + Biaya: Kabel koaksial umumnya lebih mahal daripada kabel UTP, namun biasanya lebih murah daripada kabel serat optik.
     + Ukuran dan berat: Kabel koaksial lebih besar dan lebih berat dibandingkan dengan kabel tembaga atau serat optik, membuatnya sulit diinstalasi dalam ruang yang sempit



Gambar 5.3 kabel koaksial

**Tujuan Pembelajaran 6**

Memahami konsep dasar seperti kecepatan transfer data, jarak, dan ketahanan terhadap gangguan elektromagnetik (EMI) yang mempengaruhi kinerja pengkabelan.

1. **Kecepatan Transfer Data**:
   * Kecepatan transfer data merujuk pada seberapa cepat data dapat ditransfer antara perangkat dalam jaringan melalui kabel atau media transmisi lainnya.
   * Kecepatan transfer data diukur dalam bit per detik (bps) atau dalam beberapa kelipatan seperti kilobit per detik (kbps), megabit per detik (Mbps), atau gigabit per detik (Gbps).
   * Kecepatan transfer data dipengaruhi oleh berbagai faktor, termasuk jenis kabel yang digunakan, teknologi transmisi yang diterapkan, dan kondisi jaringan secara keseluruhan.
2. **Jarak**:
   * Jarak merujuk pada seberapa jauh data dapat ditransmisikan melalui kabel atau media transmisi lainnya tanpa mengalami degradasi sinyal yang signifikan.
   * Setiap jenis kabel atau media transmisi memiliki batasan jarak maksimum yang dapat ditransmisikan tanpa mengalami penurunan kualitas atau kehilangan data.
   * Kinerja kabel dalam hal jarak dapat dipengaruhi oleh berbagai faktor, termasuk tipe kabel, keadaan fisik kabel, dan teknologi transmisi yang diterapkan.
3. **Ketahanan terhadap Gangguan Elektromagnetik (EMI)**:
   * Gangguan elektromagnetik (EMI) adalah gangguan yang dihasilkan oleh sinyal-sinyal elektromagnetik eksternal yang dapat mengganggu transmisi data dalam kabel atau media transmisi lainnya.
   * Ketahanan terhadap EMI merujuk pada kemampuan kabel atau media transmisi untuk tetap stabil dan mempertahankan kualitas transmisi data meskipun terpapar oleh gangguan elektromagnetik.
   * Beberapa faktor yang mempengaruhi ketahanan terhadap EMI termasuk konstruksi kabel (seperti pelindung dan lapisan isolasi), jarak antara sumber EMI dan kabel, serta lingkungan di sekitar kabel (seperti keberadaan peralatan elektronik lainnya).

**Tujuan Pembelajaran 7**

Mengetahui standar dan spesifikasi yang terkait dengan tipe pengkabelan seperti kategori kabel UTP dan jenis konektor yang digunakan.

1. **Kategori Kabel UTP**:
   * Kategori kabel UTP merujuk pada standar yang menentukan karakteristik fisik dan kinerja kabel tembaga tanpa pelindung untuk keperluan transmisi data.
   * Standar kategori kabel UTP umumnya ditetapkan oleh Institute of Electrical and Electronics Engineers (IEEE) dan Electronic Industries Alliance (EIA).
   * Kategori kabel UTP biasanya diberi label sebagai Cat 5, Cat 5e, Cat 6, Cat 6a, atau Cat 7, dengan setiap kategori menunjukkan kemampuan transmisi data tertentu.
   * Misalnya, Cat 5 mendukung kecepatan transfer data hingga 100 Mbps, sementara Cat 6a dapat mencapai kecepatan transfer data hingga 10 Gbps.
2. **Jenis Konektor yang Digunakan**:
   * Konektor yang digunakan dalam pengkabelan jaringan komputer sering kali adalah RJ45 (Registered Jack 45), yang terdiri dari delapan pin yang dipasang dalam dua baris.
   * RJ45 adalah standar untuk konektor kabel UTP dan sering digunakan untuk menghubungkan perangkat seperti komputer, switch, router, dan access point ke jaringan.
   * Selain RJ45, ada juga konektor lain yang digunakan dalam pengkabelan jaringan, seperti konektor RJ11 yang digunakan untuk telepon atau modem dial-up, dan konektor RJ48 yang digunakan untuk koneksi T1/E1 dalam jaringan telekomunikasi.
3. **Standar Pengkabelan**:
   * Beberapa standar pengkabelan yang umum digunakan termasuk standar TIA/EIA-568 untuk pengkabelan struktural komunikasi dan standar ISO/IEC 11801 untuk pengkabelan jaringan.
   * Standar-standar ini menetapkan persyaratan untuk penginstalan kabel, konektor, dan infrastruktur jaringan lainnya untuk memastikan kinerja yang konsisten dan andal dalam jaringan komputer.

**Tujuan Pembelajaran 8**

Mampu merancang, mengimplementasikan, dan mengelola infrastruktur jaringan yang sesuai dengan kebutuhan spesifik organisasi, dengan mempertimbangkan pemilihan perangkat jaringan dan tipe pengkabelan yang optimal.

1. **Analisis Kebutuhan**: Mulailah dengan memahami kebutuhan dan tujuan organisasi. Pertimbangkan jumlah perangkat yang akan terhubung ke jaringan, jenis aplikasi yang akan dijalankan, kebutuhan bandwidth, keamanan, dan skalabilitas.
2. **Perencanaan Jaringan**: Berdasarkan analisis kebutuhan, rancang arsitektur jaringan yang sesuai. Tentukan topologi jaringan, termasuk lokasi perangkat seperti switch, router, dan access point. Pertimbangkan juga penggunaan VLAN (Virtual Local Area Network) untuk mengelompokkan perangkat yang serupa.
3. **Pemilihan Perangkat Jaringan**: Pilih perangkat jaringan yang sesuai dengan kebutuhan organisasi. Ini termasuk switch, router, access point, modem, dan perangkat lainnya. Pastikan perangkat tersebut memiliki fitur yang diperlukan seperti kecepatan transfer data yang cukup, kemampuan routing yang sesuai, dan dukungan untuk keamanan jaringan.
4. **Pemilihan Tipe Pengkabelan**: Berdasarkan kebutuhan jaringan, pilih jenis pengkabelan yang optimal. Pertimbangkan faktor-faktor seperti kecepatan transfer data, jarak, ketahanan terhadap gangguan elektromagnetik (EMI), dan biaya. Misalnya, untuk jaringan yang membutuhkan kecepatan tinggi dan jarak jauh, kabel serat optik mungkin menjadi pilihan yang baik.
5. **Implementasi Infrastruktur Jaringan**: Setelah perencanaan, implementasikan infrastruktur jaringan sesuai dengan desain yang telah dibuat. Pasang perangkat jaringan, hubungkan mereka dengan kabel yang sesuai, dan konfigurasikan setiap perangkat sesuai dengan kebutuhan.
6. **Pengujian dan Pemeliharaan**: Lakukan pengujian menyeluruh untuk memastikan bahwa infrastruktur jaringan berfungsi dengan baik dan sesuai dengan harapan. Selain itu, lakukan pemeliharaan rutin seperti pemantauan kinerja jaringan, pembaruan perangkat lunak, dan penanganan masalah yang muncul.
7. **Skalabilitas dan Pertumbuhan Masa Depan**: Pertimbangkan kebutuhan pertumbuhan organisasi di masa depan. Pastikan infrastruktur jaringan dapat dengan mudah diperluas atau ditingkatkan sesuai dengan perkembangan organisasi dan teknologi.

Dengan merancang, mengimplementasikan, dan mengelola infrastruktur jaringan dengan cermat sesuai dengan kebutuhan spesifik organisasi, Anda dapat memastikan bahwa jaringan komputer bekerja secara efisien, andal, dan dapat mendukung kegiatan bisnis yang berkelanjutan

1. **Jurnal Yang berhubungan dengan perangkat jaringan dan tipe pengkabelan**
2. Review jurnal 1

|  |  |
| --- | --- |
| Judul Penelitian | pelatihan jaringan dan troubleshooting komputer  untuk menambah keahlian perangkat desa mukti  karya kabupaten mesuji |
| Penulis | WIDYA LAKSMI |
| Tahun | 2022 |
| Tujuan Penelitian | memberikan pelatihan dalam bidang Jaringan sekaligus troubleshooting komputer. Harapannya adalah dengan memberikan pengetahuan tersebut akan bermanfaat bagi pegawai dalam menangani permasalahan yang terjadi baik pada jaringan komputer ataupun pada komputer tersebut  ini. |
| Subjek Penelitian | Desa Mukti Karya |
| Metode Penelitian | Metode literature digunakan dalam penelitian ini yaitu metode metode deskriptif. |
| Analisis |  |
| Kelebihan Penelitian | Pemahaman yang Komprehensif: Pegawai akan memiliki pemahaman yang lebih baik tentang bagaimana jaringan komputer berfungsi dan bagaimana komputer terhubung dalam jaringan. Mereka juga akan memahami berbagai masalah yang mungkin timbul dan cara menangani mereka.  Efisiensi dalam Penanganan Masalah: Dengan pengetahuan yang lebih luas tentang jaringan dan komputer, pegawai akan dapat dengan cepat mengidentifikasi dan memecahkan masalah yang muncul. Mereka tidak perlu mengandalkan teknisi eksternal untuk setiap masalah kecil yang timbul.  Penghematan Biaya: Dengan kemampuan untuk menangani masalah secara internal, organisasi dapat menghemat biaya yang akan dikeluarkan untuk memperbaiki masalah teknis. Mereka tidak perlu membayar layanan teknisi eksternal setiap kali ada masalah |
| Kelemahan Penelitian | Waktu dan Sumber Daya: Memberikan pelatihan yang mencakup dua bidang sekaligus dapat membutuhkan waktu dan sumber daya yang lebih besar. Ini mungkin memerlukan penjadwalan dan alokasi sumber daya yang hati-hati untuk memastikan bahwa pelatihan berjalan lancar.  Tingkat Pemahaman yang Mendalam: Materi yang mencakup jaringan komputer dan troubleshooting komputer memerlukan pemahaman yang mendalam tentang kedua bidang tersebut. Ini dapat menjadi tantangan bagi instruktur untuk menyampaikan materi dengan cara yang dapat dipahami oleh semua peserta, terutama jika ada perbedaan dalam tingkat pengetahuan dan pengalaman mereka.  Potensi Kelebihan Informasi: Pelatihan yang mencakup banyak topik dapat menyebabkan peserta merasa kelebihan informasi atau kewalahan. Ini bisa mengurangi efektivitas pelatihan karena peserta mungkin kesulitan menyerap dan memahami semua informasi yang disampaikan. |

1. Review jurnal 2

|  |  |
| --- | --- |
| Judul Penelitian | ANALISIS DAN PERANCANGAN JARINGAN LOCAL  AREA NETWORK PADA LAB KOMPUTER DI SMK  NEGERI 5 KOTA SERANG |
| Penulis | Bayu Prasetya Julandra, Putri, Ali Mabruri |
| Tahun | 2022 |
| Tujuan Penelitian | mengembangkan teknologi yang telah ada beserta sistemnya, serta tindakan yang akan di lakukan jika akan melakukan penambahan teknologi jaringan yang akan diintegrasikan ke dalam sebuah jaringan komputer yang terkoneksi dengan jaringan internet. |
| Subjek Penelitian | Perancangan Jaringan Local Area Network |
| Metode Penelitian | Metode literature digunakan dalam penelitian ini yaitu metode metode deskriptif. |
| Analisis |  |
| Kelebihan Penelitian | **Peningkatan Efisiensi**: Dengan melakukan penelitian ini, akan ada peningkatan efisiensi dalam penggunaan sumber daya jaringan. Dengan merencanakan infrastruktur yang tepat, seperti topologi yang efisien dan penggunaan perangkat keras yang sesuai, penggunaan jaringan dapat dioptimalkan.  **Peningkatan Kinerja**: Dengan perancangan yang tepat, kinerja jaringan dapat ditingkatkan. Hal ini termasuk kecepatan transfer data yang lebih tinggi, koneksi yang lebih stabil, dan waktu henti yang lebih sedikit, yang semuanya berkontribusi pada pengalaman pengguna yang lebih baik.  **Peningkatan Keamanan**: Dalam penelitian ini, keamanan jaringan dapat menjadi fokus utama. Dengan menerapkan langkah-langkah keamanan yang tepat, seperti firewall dan enkripsi, serta pengaturan otorisasi yang baik, dapat mengurangi risiko serangan cyber dan akses tidak sah ke jaringan.  **Peningkatan Daya Tahan**: Dengan merancang jaringan yang tahan terhadap kegagalan, seperti dengan menerapkan sistem redundansi dan perencanaan pemulihan bencana, laboratorium komputer akan memiliki tingkat ketersediaan yang tinggi. Hal ini memastikan bahwa kegiatan pembelajaran tidak terganggu oleh gangguan jaringan yang tidak terduga.  **Peningkatan Pengalaman Pengguna**: Dengan memiliki jaringan yang handal dan efisien, pengguna laboratorium komputer, baik siswa maupun staf, akan memiliki pengalaman yang lebih baik dalam menggunakan sumber daya teknologi. Hal ini dapat meningkatkan produktivitas dan kesenangan dalam belajar dan mengajar.  **Peningkatan Manajemen Jaringan**: Melalui penelitian ini, staf administratif dan teknis dapat meningkatkan keterampilan mereka dalam manajemen jaringan. Mereka akan memiliki pemahaman yang lebih baik tentang bagaimana jaringan beroperasi dan bagaimana cara merawatnya, yang akan membantu dalam pemeliharaan rutin dan pemecahan masalah.  **Penghematan Biaya Jangka Panjang**: Meskipun memerlukan investasi awal, penelitian ini dapat menghasilkan penghematan biaya jangka panjang. Dengan merencanakan infrastruktur yang tepat dan menghindari perbaikan darurat akibat kegagalan jaringan, institusi dapat menghemat biaya perawatan dan pemeliharaan.  **Peningkatan Prestasi Sekolah**: Dengan memiliki fasilitas teknologi yang canggih dan handal, seperti laboratorium komputer dengan jaringan LAN yang baik, sekolah dapat meningkatkan citra mereka dan menarik minat siswa dan tenaga pendidik yang berkualitas, yang pada akhirnya dapat meningkatkan prestasi sekolah secara keseluruhan. |
| Kelemahan Penelitian | **Biaya Awal yang Tinggi**: Perancangan dan implementasi jaringan LAN yang canggih sering kali memerlukan biaya awal yang signifikan untuk perangkat keras, perangkat lunak, dan tenaga kerja ahli. Hal ini dapat menjadi beban keuangan yang cukup besar bagi sekolah, terutama jika anggaran terbatas.  **Kesulitan Implementasi**: Proses implementasi jaringan LAN yang kompleks bisa menjadi sulit dan memakan waktu. Memasang perangkat keras, konfigurasi perangkat lunak, dan memastikan semua komponen berfungsi dengan baik memerlukan pengetahuan dan keterampilan teknis yang tinggi.  **Dukungan Teknis yang Diperlukan**: Setelah jaringan LAN diimplementasikan, dukungan teknis yang berkelanjutan akan dibutuhkan untuk memelihara dan memperbaiki jaringan jika terjadi masalah. Ini mungkin memerlukan sumber daya manusia tambahan atau mengontrak layanan dukungan eksternal, yang dapat menambah biaya operasional.  **Ketergantungan pada Infrastruktur Fisik**: Jaringan LAN yang dirancang secara fisik rentan terhadap gangguan eksternal seperti kerusakan kabel, pemadaman listrik, atau bencana alam. Ini dapat menyebabkan gangguan layanan dan membutuhkan waktu dan biaya tambahan untuk perbaikan.  **Tantangan dalam Pemeliharaan dan Pembaruan**: Jaringan LAN yang kompleks memerlukan pemeliharaan rutin dan pembaruan perangkat lunak untuk menjaga keamanan dan kinerja yang optimal. Mengelola pemeliharaan dan pembaruan ini dapat menjadi tugas yang menantang dan memakan waktu bagi staf IT sekolah.  **Kesesuaian dengan Standar dan Regulasi**: Perancangan jaringan LAN harus mematuhi berbagai standar dan regulasi yang berlaku, terutama dalam hal keamanan data dan privasi. Memastikan kesesuaian dengan persyaratan ini dapat membutuhkan upaya tambahan dan biaya.  **Keterbatasan Kapasitas dan Skalabilitas**: Meskipun jaringan LAN yang direncanakan dengan baik dapat memenuhi kebutuhan saat ini, mereka mungkin menghadapi keterbatasan kapasitas atau skalabilitas di masa depan jika jumlah pengguna atau permintaan layanan meningkat secara signifikan.  **Tantangan Keselamatan Digital**: Jaringan LAN yang kompleks rentan terhadap berbagai ancaman keamanan digital, seperti serangan malware, phishing, atau serangan DDoS. Memastikan keamanan jaringan yang kuat dan melindungi data sensitif menjadi tantangan tambahan. |

SOAL

1. Jelaskan perbedaan antara switch dan router dalam konteks jaringan komputer. Apa fungsi masing-masing perangkat tersebut?
2. Mengapa perangkat kecil seperti hub menjadi kurang umum digunakan dalam jaringan modern? Apa kelebihan switch dibandingkan dengan hub?
3. Apa yang dimaksud dengan topologi jaringan bintang? Jelaskan kelebihan dan kelemahan dari topologi ini, serta kapan sebaiknya digunakan.
4. Jelaskan apa itu kabel UTP (Unshielded Twisted Pair) dan kabel STP (Shielded Twisted Pair). Apa perbedaan utama antara keduanya dan kapan sebaiknya menggunakan masing-masing jenis kabel?
5. Apa yang dimaksud dengan pengkabelan straight-through dan crossover? Kapan kita menggunakan masing-masing jenis kabel ini?
6. Jelaskan perbedaan antara kabel kategori 5e (Cat 5e) dan kategori 6 (Cat 6). Mengapa Cat 6 menjadi pilihan yang lebih baik dalam banyak implementasi jaringan?
7. Bagaimana cara mendeteksi dan memperbaiki gangguan kabel dalam jaringan LAN? Sebutkan beberapa masalah umum yang dapat terjadi pada kabel jaringan.
8. Apa yang dimaksud dengan penggunaan kabel fiber optic dalam jaringan komputer? Jelaskan kelebihan dan kelemahan dari penggunaan kabel serat optik dibandingkan dengan kabel tembaga.
9. Bagaimana cara memilih jenis pengkabelan yang tepat untuk kebutuhan jaringan tertentu? Apa faktor-faktor yang perlu dipertimbangkan dalam pemilihan kabel dan konektor yang sesuai?
10. Jelaskan bagaimana cara memasang konektor RJ-45 pada ujung kabel UTP. Apa langkah-langkah yang harus diikuti untuk memastikan koneksi yang benar dan andal?

Daftar Pustaka

Bayu Prasetya Julandra, P. A. (2022). ANALISIS DAN PERANCANGAN JARINGAN LOCAL AREA NETWORK PADA LAB KOMPUTER DI SMK NEGERI 5 KOTA SERANG. *Engineering And Technology International Journal*, 1-14.

LAKSMI, W. (2022). PELATIHAN JARINGAN DAN TROUBLESHOOTING KOMPUTER. *Jurnal WIDYA LAKSMI*, 1-6.

Samuel Jeremia Sihombing, A. P. (2021). PEMBUATAN APLIKASI BERBASIS ANDROID UNTUK PEMBELAJARAN PENGKABELAN LAN. *e-Proceeding of Applied Science*, 1-6.

\

**Pertemuan 8**

**PENGALAMATAN INTERNET PROTOCOL (IP)**

1. **Tujuan Pembelajaran**

Pada Pertemuan Ini Akan Di Jelaskan Pengetahuan Dasar (Basic Science) Tentang Definisi pengalamatan internet protocol (IP). Anda Harus Mampu:

* 1. Memahami konsep dasar Pengalamatan Internet Protocol (IP), termasuk struktur alamat IP, fungsi, dan jenis-jenisnya.
  2. Menguasai proses pengalamatan dalam jaringan komputer, termasuk pembagian dan pengaturan alamat IP, subnetting, dan supernetting.
  3. Mampu menganalisis kebutuhan jaringan dan merancang skema pengalamatan IP yang efisien dan sesuai dengan kebutuhan.
  4. Mampu mengimplementasikan dan mengelola pengalamatan IP dalam konteks jaringan komputer yang kompleks, termasuk konfigurasi perangkat jaringan dan routing.
  5. Memahami keamanan dalam pengalamatan IP, termasuk teknik-teknik mitigasi risiko seperti firewall, VPN, dan deteksi intrusi

1. **Uraian Materi**

**Tujuan Pembelajaran 1**

Memahami konsep dasar Pengalamatan Internet Protocol (IP), termasuk struktur alamat IP, fungsi, dan jenis-jenisnya.

Pengalamatan Internet Protocol (IP) adalah fondasi dari komunikasi di Internet. IP menyediakan cara untuk mengirim dan menerima data di antara perangkat yang terhubung ke jaringan. Memahami konsep dasar IP sangat penting dalam memahami bagaimana internet berfungsi.

1. **Struktur Alamat IP**

Alamat IP adalah serangkaian angka biner yang digunakan untuk mengidentifikasi perangkat di jaringan. Ada dua versi utama alamat IP: IPv4 dan IPv6.

* **IPv4**: Alamat IPv4 terdiri dari 32 bit, biasanya dinyatakan dalam format desimal seperti **192.168.0.1**.
* **IPv6**: Alamat IPv6 menggunakan 128 bit, dan biasanya ditulis dalam format heksadesimal seperti **2001:0db8:85a3:0000:0000:8a2e:0370:7334**.

1. **Fungsi Alamat IP**

Alamat IP memiliki beberapa fungsi utama:

* **Identifikasi**: Alamat IP mengidentifikasi setiap perangkat yang terhubung ke jaringan. Ini memungkinkan perangkat untuk saling berkomunikasi.
* **Rute**: Alamat IP memungkinkan data untuk dikirimkan ke tujuan yang tepat melalui jaringan yang kompleks.
* **Lokasi**: Alamat IP dapat digunakan untuk memperkirakan lokasi fisik perangkat di jaringan.

1. **Jenis-Jenis Alamat IP**

Ada beberapa jenis alamat IP yang perlu dipahami:

* **Alamat IP Publik**: Ini adalah alamat yang dapat diakses dari internet. Setiap perangkat yang terhubung langsung ke internet memiliki alamat IP publik unik.
* **Alamat IP Pribadi**: Alamat IP yang digunakan di dalam jaringan lokal, tidak dapat diakses secara langsung dari internet. Contohnya termasuk **192.168.x.x** dan **10.x.x.x**.
* **Alamat IP Dinamis**: Alamat IP yang ditugaskan kepada perangkat untuk jangka waktu tertentu. Ini dapat berubah setiap kali perangkat terhubung ke jaringan.
* **Alamat IP Statis**: Alamat IP yang tetap ditugaskan kepada perangkat dan tidak berubah.

1. **Protokol IP dan TCP/IP**

Protokol Internet Protocol (IP) adalah salah satu dari sekumpulan protokol yang membentuk TCP/IP, yang merupakan standar komunikasi di Internet. TCP/IP memungkinkan perangkat untuk berkomunikasi di jaringan, termasuk pengalamatan, pengiriman data, dan pengiriman pesan error.

.

**Tujuan Pembelajaran 2**

Menguasai proses pengalamatan dalam jaringan komputer, termasuk pembagian dan pengaturan alamat IP, subnetting, dan supernetting.

* 1. **Pembagian Alamat IP**

Pembagian alamat IP adalah proses menetapkan alamat IP kepada setiap perangkat di jaringan. Ada dua jenis pembagian utama: statis dan dinamis.

* **Pembagian Statis**: Administrator jaringan secara manual menetapkan alamat IP kepada setiap perangkat. Ini umumnya digunakan untuk perangkat seperti server yang memerlukan alamat yang konsisten.
* **Pembagian Dinamis**: Alamat IP ditugaskan kepada perangkat secara otomatis menggunakan protokol seperti DHCP (Dynamic Host Configuration Protocol). Ini memungkinkan pengelolaan jaringan yang lebih efisien dan fleksibel.
  1. **Subnetting**

Subnetting adalah teknik untuk membagi sebuah jaringan besar menjadi beberapa subnet yang lebih kecil. Ini membantu dalam mengoptimalkan penggunaan alamat IP dan meningkatkan efisiensi jaringan.

* **Manfaat Subnetting**:
  + Mengurangi lalu lintas jaringan dengan membatasi jumlah perangkat dalam satu subnet.
  + Meningkatkan keamanan dengan memisahkan berbagai bagian jaringan ke dalam subnet yang terpisah.
  + Mengoptimalkan penggunaan alamat IP dengan memperkenalkan pembagian alamat IP berdasarkan kebutuhan.
  1. **Supernetting**

Supernetting adalah teknik yang bertentangan dengan subnetting, di mana beberapa alamat IP atau subnet digabungkan menjadi satu entitas yang lebih besar. Ini digunakan untuk mengurangi overhead routing dalam jaringan yang besar.

* **Manfaat Supernetting**:
  + Mengurangi tabel routing dengan menggabungkan beberapa subnet menjadi satu entitas yang lebih besar.
  + Mengurangi jumlah entri dalam tabel routing di router, yang menghemat sumber daya dan meningkatkan efisiensi routing.
  1. **Pengaturan Alamat IP**

Pengaturan alamat IP melibatkan konfigurasi perangkat dengan alamat IP yang sesuai dengan jaringan yang digunakan. Ini dapat dilakukan secara manual oleh administrator jaringan atau secara otomatis menggunakan protokol konfigurasi seperti DHCP.

* **DHCP (Dynamic Host Configuration Protocol)**: Protokol ini memungkinkan perangkat untuk secara otomatis mendapatkan alamat IP, subnet mask, gateway, dan informasi konfigurasi lainnya dari server DHCP di jaringan

**Tujuan Pembelajaran 3**

Mampu menganalisis kebutuhan jaringan dan merancang skema pengalamatan IP yang efisien dan sesuai dengan kebutuhan

1. **Analisis Kebutuhan Jaringan**

Sebelum merancang skema pengalamatan IP yang efisien, langkah pertama yang penting adalah melakukan analisis kebutuhan jaringan. Ini melibatkan pemahaman mendalam tentang:

* **Jumlah Perangkat**: Menentukan berapa banyak perangkat yang akan terhubung ke jaringan, termasuk perangkat fisik (komputer, printer, router, switch) dan perangkat virtual (server, mesin virtual).
* **Lokasi Fisik**: Memahami di mana lokasi perangkat-perangkat tersebut akan ditempatkan dalam jaringan, apakah di satu lokasi fisik atau tersebar di beberapa lokasi.
* **Trafik Jaringan**: Mengidentifikasi pola trafik jaringan yang ada atau yang diharapkan, seperti komunikasi antara departemen, akses ke server, dan akses ke internet.
* **Kebutuhan Aplikasi dan Layanan**: Memahami aplikasi dan layanan yang akan digunakan dalam jaringan, termasuk apakah ada kebutuhan khusus seperti VoIP, video streaming, atau penyimpanan data besar.

1. **Perancangan Skema Pengalamatan IP**

Setelah analisis kebutuhan jaringan selesai, langkah selanjutnya adalah merancang skema pengalamatan IP yang efisien dan sesuai dengan kebutuhan. Hal ini melibatkan beberapa pertimbangan:

* **Pengelompokan Logis**: Mengelompokkan perangkat-perangkat ke dalam subnet berdasarkan fungsi, lokasi, atau departemen untuk mengoptimalkan manajemen jaringan dan keamanan.
* **Penggunaan Alamat IP**: Memilih jenis alamat IP yang tepat (publik atau pribadi), serta menggunakan alamat IPv4 atau IPv6 sesuai dengan kebutuhan.
* **Penggunaan Subnetting**: Menerapkan subnetting untuk membagi jaringan besar menjadi subnet-subnet yang lebih kecil, memperhatikan jumlah perangkat dalam setiap subnet dan meminimalkan lalu lintas jaringan.
* **Pengaturan DHCP**: Menentukan konfigurasi DHCP yang sesuai untuk menugaskan alamat IP secara dinamis kepada perangkat di jaringan, termasuk rentang alamat IP yang tersedia dan masa berlaku peminjaman alamat.
* **Keamanan**: Memperhatikan aspek keamanan dalam perancangan skema pengalamatan IP, seperti membatasi akses antar subnet dan menerapkan kontrol akses yang tepat.

1. **Uji Coba dan Evaluasi**

Setelah merancang skema pengalamatan IP, penting untuk melakukan uji coba dan evaluasi untuk memastikan bahwa skema tersebut memenuhi kebutuhan jaringan dengan baik. Ini melibatkan simulasi atau implementasi skema dalam lingkungan jaringan yang sesungguhnya, diikuti dengan pengujian fungsionalitas dan kinerja.

**Tujuan Pembelajaran 4**

Mampu mengimplementasikan dan mengelola pengalamatan IP dalam konteks jaringan komputer yang kompleks, termasuk konfigurasi perangkat jaringan dan routing.

1. **Implementasi Pengalamatan IP**

Implementasi pengalamatan IP melibatkan konfigurasi perangkat jaringan, termasuk router, switch, dan perangkat lainnya, untuk mendukung komunikasi antara perangkat dalam jaringan. Langkah-langkah utama dalam implementasi pengalamatan IP meliputi:

* **Konfigurasi Perangkat Jaringan**: Menetapkan alamat IP pada antarmuka perangkat jaringan yang sesuai dengan skema pengalamatan yang telah dirancang sebelumnya.
* **Konfigurasi Routing**: Mengatur tabel routing pada router untuk memastikan bahwa data dapat diarahkan dengan benar antara subnet-subnet dalam jaringan.
* **Konfigurasi DHCP**: Mengatur server DHCP untuk menugaskan alamat IP secara dinamis kepada perangkat dalam jaringan.

1. **Manajemen Pengalamatan IP**

Manajemen pengalamatan IP melibatkan pemeliharaan dan pengawasan alamat IP dalam jaringan untuk memastikan ketersediaan, keamanan, dan efisiensi. Beberapa tugas manajemen yang penting meliputi:

* **Pemantauan Penggunaan Alamat IP**: Memantau dan melacak penggunaan alamat IP dalam jaringan untuk mengidentifikasi konflik atau kebutuhan perluasan subnet.
* **Manajemen Alamat IP**: Mengelola pemberian dan penghapusan alamat IP, termasuk menetapkan alamat IP statis kepada perangkat tertentu dan mengelola daftar alamat IP yang tersedia.
* **Keamanan Pengalamatan IP**: Menerapkan langkah-langkah keamanan untuk melindungi pengalamatan IP dari serangan, termasuk penggunaan teknik seperti VLAN (Virtual Local Area Network) dan akses kontrol.
* **Perencanaan Kapasitas**: Memperkirakan kebutuhan alamat IP di masa depan dan merencanakan kapasitas jaringan yang sesuai.

1. **Troubleshooting**

Manajemen pengalamatan IP juga melibatkan identifikasi dan penyelesaian masalah yang terkait dengan pengalamatan IP, seperti konflik alamat IP, kesalahan konfigurasi, atau gangguan jaringan. Troubleshooting memerlukan pemahaman mendalam tentang protokol jaringan, alat-alat pemecahan masalah, dan praktik terbaik dalam pemecahan masalah jaringan

.

**Tujuan Pembelajaran 5**

Memahami keamanan dalam pengalamatan IP, termasuk teknik-teknik mitigasi risiko seperti firewall, VPN, dan deteksi intrusi.

Keamanan dalam pengalamatan IP adalah aspek penting dalam menjaga integritas, kerahasiaan, dan ketersediaan data dalam jaringan. Berikut ini adalah penjelasan yang lebih lengkap tentang keamanan pengalamatan IP serta teknik mitigasi risiko yang umum digunakan:

* 1. **Ancaman terhadap Pengalamatan IP**
  + **Penyusupan (Intrusion)**: Penyerang dapat mencoba masuk ke dalam jaringan dengan menggunakan teknik seperti penggunaan alamat IP palsu atau mencoba menebak kombinasi alamat IP yang valid untuk mendapatkan akses yang tidak sah.
  + **Serangan DDoS (Distributed Denial of Service)**: Penyerang dapat melancarkan serangan DDoS dengan membanjiri jaringan dengan lalu lintas data yang tidak sah, menyebabkan kegagalan layanan dan mengganggu ketersediaan jaringan.
  + **Spoofing Alamat IP**: Penyerang dapat menggunakan teknik spoofing alamat IP untuk menyamar sebagai perangkat atau server yang sah, dengan tujuan melakukan serangan atau mencuri informasi sensitif.
  1. **Teknik Mitigasi Risiko**
  + **Firewall**: Firewall adalah barisan pertahanan utama dalam jaringan yang dapat memonitor dan mengontrol lalu lintas data berdasarkan aturan yang ditetapkan. Ini membantu dalam melindungi jaringan dari serangan seperti penyusupan dan serangan DDoS dengan memblokir atau membatasi akses yang tidak sah.
  + **VPN (Virtual Private Network)**: VPN menyediakan saluran komunikasi yang aman di jaringan publik dengan mengenkripsi data yang dikirim antara perangkat. Hal ini membantu dalam melindungi kerahasiaan data dan mencegah serangan pengintai serta spoofing alamat IP.
  + **Deteksi Intrusi (IDS/IPS)**: Sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) digunakan untuk mendeteksi dan mencegah serangan yang mencurigakan atau berbahaya dalam jaringan. Mereka mengawasi lalu lintas jaringan untuk pola yang tidak normal dan memberikan peringatan atau mengambil tindakan preventif jika terdeteksi ancaman.
  + **Penyaringan Paket (Packet Filtering)**: Menggunakan perangkat atau perangkat lunak yang dapat melakukan penyaringan paket data berdasarkan alamat IP sumber dan tujuan. Ini memungkinkan administrator jaringan untuk memblokir lalu lintas yang berasal dari alamat IP yang tidak dikenal atau mencurigakan.
  + **Pemantauan dan Analisis Log**: Melakukan pemantauan dan analisis terhadap log aktivitas jaringan secara teratur dapat membantu dalam mendeteksi pola serangan atau aktivitas mencurigakan, sehingga tindakan dapat diambil dengan cepat untuk merespons ancaman tersebut.

1. **Jurnal Yang berhubungan dengan Pengalamatan Internet Protocol (IP)**
2. Review jurnal 1

|  |  |
| --- | --- |
| Judul Penelitian | KOMPARASI PERFORMA METODE 6TO4 DAN KOMBINASI  L2TP/IPSEC UNTUK IMPLEMENTASI IPV6  PADA JARINGAN KOMPUTER |
| Penulis | Adhitya Nugraha, Muhammad Joyo Satrio, Junta Zeniarja |
| Tahun | 2020 |
| Tujuan Penelitian | melakukan komparasi antara mekanisme transisi tunneling (teknik 6to4) dengan teknik VPN (L2TP/IPSec) IPv6 untuk membandingkan hasil performa throughput, delay dan packet loss |
| Subjek Penelitian | IMPLEMENTASI IPV6 PADA JARINGAN KOMPUTER |
| Metode Penelitian | Metode literature digunakan dalam penelitian ini yaitu metode metode deskriptif. |
| Analisis |  |
| Kelebihan Penelitian | Kontribusi pada Pengetahuan: Penelitian ini dapat memberikan wawasan yang berharga tentang performa dan efektivitas dua metode yang berbeda untuk mengimplementasikan IPv6 dalam jaringan komputer. Hal ini akan membantu dalam memperkaya pengetahuan tentang implementasi IPv6 dan memperluas pemahaman tentang kelebihan dan kelemahan dari masing-masing metode.  Memberikan Pilihan Alternatif: Dengan membandingkan dua metode yang berbeda, penelitian ini dapat memberikan pilihan alternatif kepada organisasi atau individu yang ingin mengadopsi IPv6 dalam jaringan mereka. Mereka dapat membuat keputusan yang lebih terinformasi berdasarkan hasil penelitian ini untuk memilih metode yang paling sesuai dengan kebutuhan dan lingkungan jaringan mereka.  Mendukung Pengambilan Keputusan: Hasil dari penelitian ini dapat menjadi dasar bagi para pengambil keputusan dalam mengimplementasikan IPv6 dalam jaringan mereka. Dengan memahami perbandingan performa antara metode 6to4 dan kombinasi L2TP/IPsec, mereka dapat membuat keputusan yang lebih tepat dalam merencanakan dan mengimplementasikan infrastruktur IPv6.  Mendorong Inovasi dan Pengembangan Teknologi: Dengan mengevaluasi dan membandingkan performa dua metode yang berbeda, penelitian ini dapat mendorong inovasi dan pengembangan teknologi lebih lanjut dalam konteks implementasi IPv6. Ini dapat mengarah pada peningkatan kualitas dan efisiensi metode yang ada, serta mendorong pencarian solusi baru yang lebih baik.  Penerapan yang Lebih Efisien: Dengan memahami kelebihan dan kelemahan dari masing-masing metode, organisasi atau individu dapat menerapkan IPv6 dengan lebih efisien dan efektif. Mereka dapat menghindari risiko atau masalah yang mungkin timbul dengan menggunakan metode yang kurang cocok untuk kebutuhan mereka |
| Kelemahan Penelitian | Keterbatasan Generalisasi: Hasil dari penelitian ini mungkin tidak dapat secara langsung diterapkan pada semua konteks atau lingkungan jaringan. Kondisi jaringan yang berbeda, seperti ukuran, topologi, dan kebutuhan spesifik, dapat mempengaruhi hasil penelitian. Oleh karena itu, generalisasi dari hasil penelitian mungkin terbatas pada lingkungan atau kondisi tertentu.  Keterbatasan Fokus: Penelitian ini hanya membandingkan dua metode tertentu, yaitu 6to4 dan kombinasi L2TP/IPsec. Ada banyak metode lain yang digunakan untuk mengimplementasikan IPv6 dalam jaringan komputer. Oleh karena itu, penelitian ini mungkin tidak memberikan gambaran lengkap tentang semua opsi yang tersedia.  Keterbatasan Metrik Penilaian: Penelitian ini mungkin terbatas pada sejumlah metrik penilaian tertentu untuk mengevaluasi performa kedua metode. Metrik penilaian yang dipilih dapat mempengaruhi interpretasi hasil penelitian dan mungkin tidak mencakup semua aspek yang relevan dalam penilaian performa.  Keterbatasan Waktu dan Sumber Daya: Penelitian ini mungkin terbatas oleh waktu dan sumber daya yang tersedia. Pengumpulan data yang memadai, pengujian yang cermat, dan analisis yang mendalam membutuhkan investasi waktu dan sumber daya yang signifikan.  Keterbatasan Dampak Praktis: Meskipun penelitian ini dapat memberikan wawasan yang berharga, namun dampak praktis dari hasil penelitian mungkin terbatas jika tidak disertai dengan rekomendasi yang jelas atau panduan implementasi yang konkret |

1. Review jurnal 2

|  |  |
| --- | --- |
| Judul Penelitian | Implementasi IPv6 Menggunakan Routing Information Protocol  (Studi Kasus : STMIK HORIZON) |
| Penulis | Wahyudi, Tania Ananta Dewi |
| Tahun | 2022 |
| Tujuan Penelitian | Menghubungkan jaringan yang terdapat pada STIKES dan STMIK HORIZON hingga kedua jaringan tersebut dapat berkomunikasi dan mengirim paket data satu dengan yang lain berbasis IPv6 |
| Subjek Penelitian | Routing Information Protocol |
| Metode Penelitian | Metode pengembangan jaringan yang digunakan dalam penelitian ini adalah PPDIOO (Prepare, Plan, Design, implement, Operate dan Optimize) (Cisco, 2010) merupakan metode perancangan jaringan dari Cisco atau biasa disebut sebagai siklus hidup layanan jaringan Cisco yang dirancang untuk mendukung  berkembang. jaringan. |
| Analisis |  |
| Kelebihan Penelitian | Relevansi: Penelitian ini memiliki relevansi yang tinggi karena membahas implementasi IPv6, yang saat ini menjadi topik penting dalam dunia jaringan komputer mengingat semakin berkurangnya alamat IPv4 yang tersedia.  Penerapan dalam Konteks Spesifik: Studi kasus ini dilakukan di STMIK HORIZON, sehingga hasil penelitian akan memberikan pemahaman yang lebih konkret tentang implementasi IPv6 dalam lingkungan pendidikan tinggi atau institusi pendidikan tertentu.  Kontribusi pada Pengetahuan: Penelitian ini dapat memberikan kontribusi baru terhadap literatur dalam bidang implementasi IPv6, khususnya dalam menggunakan Routing Information Protocol (RIP). Metode implementasi yang digunakan dan hasil evaluasi dapat menjadi sumber pengetahuan yang berharga bagi profesional jaringan dan peneliti di masa mendatang.  Dampak Praktis: Hasil dari penelitian ini dapat memiliki dampak praktis yang signifikan bagi STMIK HORIZON atau institusi serupa dalam memperbarui infrastruktur jaringan mereka menuju IPv6. Hal ini dapat meningkatkan efisiensi dan keandalan jaringan serta mempersiapkan institusi untuk masa depan yang semakin mengadopsi IPv6.  Peluang Pengembangan: Penelitian ini juga dapat membuka peluang untuk pengembangan lebih lanjut, baik dalam hal peningkatan implementasi IPv6 di STMIK HORIZON maupun dalam konteks penelitian lebih lanjut mengenai penggunaan RIP dalam implementasi IPv6. |
| Kelemahan Penelitian | Keterbatasan Umumisasi: Hasil penelitian yang berasal dari studi kasus di STMIK HORIZON mungkin tidak sepenuhnya dapat digeneralisasikan ke lingkungan jaringan yang berbeda. Variabilitas dalam infrastruktur jaringan, ukuran jaringan, atau kebutuhan spesifik institusi lain dapat membuat hasil penelitian tidak sepenuhnya relevan.  Keterbatasan Metodologi: Metode yang digunakan dalam penelitian, terutama dalam hal implementasi IPv6 menggunakan RIP, mungkin memiliki keterbatasan tertentu. Misalnya, mungkin ada metode alternatif yang lebih efektif atau lebih efisien yang tidak dieksplorasi dalam penelitian ini.  Keterbatasan Teknis: Implementasi IPv6 menggunakan RIP mungkin memiliki keterbatasan teknis tertentu, seperti skala yang terbatas atau kinerja yang kurang optimal dalam kondisi jaringan tertentu. Hal ini bisa membatasi kepraktisan atau efektivitas dari solusi yang diusulkan.  Keterbatasan Evaluasi: Evaluasi terhadap implementasi IPv6 menggunakan RIP mungkin tidak mencakup semua aspek yang relevan atau tidak memberikan gambaran yang lengkap tentang kinerja dan efektivitas solusi tersebut. Hal ini bisa menjadi hambatan dalam memahami secara menyeluruh manfaat dan keterbatasan dari solusi yang diusulkan.  Keterbatasan Penerapan: Penelitian ini mungkin menghadapi tantangan dalam penerapan implementasi IPv6 menggunakan RIP di lingkungan yang sebenarnya. Faktor-faktor seperti keterbatasan sumber daya, dukungan organisasi, atau perubahan kebijakan dapat menghambat kesuksesan implementasi. |

SOAL

1. Jelaskan konsep dasar dari alamat IP (Internet Protocol) dan perannya dalam jaringan komputer. Mengapa alamat IP penting dalam proses komunikasi antar perangkat di internet?
2. Apa yang dimaksud dengan IPv4 dan IPv6? Jelaskan perbedaan utama antara kedua versi protokol tersebut dan mengapa transisi dari IPv4 ke IPv6 menjadi penting.
3. Bagaimana cara mengklasifikasikan alamat IP berdasarkan kelasnya dalam IPv4? Jelaskan masing-masing kelas dan rentang alamat IP yang termasuk di dalamnya.
4. Jelaskan perbedaan antara alamat IP statis dan dinamis. Kapan sebaiknya menggunakan masing-masing jenis alamat IP dalam suatu jaringan?
5. Apa yang dimaksud dengan DHCP (Dynamic Host Configuration Protocol)? Jelaskan peran DHCP dalam alokasi alamat IP dinamis dalam jaringan komputer.
6. Jelaskan proses yang terjadi saat sebuah perangkat menghubungkan ke jaringan dan memperoleh alamat IP menggunakan DHCP.
7. Bagaimana cara mengkonfigurasi alamat IP statis pada sebuah perangkat? Jelaskan langkah-langkahnya dan kapan sebaiknya menggunakan konfigurasi alamat IP statis.
8. Apa yang dimaksud dengan subnetting dalam konteks pengalamatan IP? Mengapa subnetting penting dalam pengelolaan jaringan yang efisien?
9. Bagaimana cara menghitung jumlah host dan subnet yang mungkin dalam sebuah jaringan dengan menggunakan subnetting? Jelaskan langkah-langkahnya.
10. Apa itu NAT (Network Address Translation) dan bagaimana cara kerjanya? Jelaskan peran NAT dalam memungkinkan beberapa perangkat dalam sebuah jaringan lokal untuk berbagi satu alamat IP publik

Daftar Pustaka

Adhitya Nugraha, M. J. (2020). KOMPARASI PERFORMA METODE 6TO4 DAN KOMBINASI L2TP/IPSEC UNTUK IMPLEMENTASI IPV6 PADA JARINGAN KOMPUTER. *CESS*, 1-6.

Wahyudi, T. A. (2022). Implementasi IPv6 Menggunakan Routing Information Protocol (Studi Kasus : STMIK HORIZON). *Teknologi Informasi*, 1-6.