UNIVERSITAS PGRI YOGYAKARTA

KONTRAK PERKULIAHAN

Nama Dosen : Dr. Marti Widya Sari, S.T., M.Eng.
Mata Kuliah : Jaringan Komputer Tingkat Lanjut
Program Studi : Informatika
Kelas/Angkatan : 22 AB
Semester : Genap
Tahun Akademik : 2024/2025

KETENTUAN /KESEPAKATAN

1) Perkuliahan dilakukan secara tatap muka (luring) / daring
2) Jika terdapat pertemuan tambahan, akan dilaksanakan pada hari Sabtu secara daring (online)
3) Kehadiran mahasiswa dalam kuliah minimal 75 % dari total pertemuan
4) Mahasiswa wajib mengikuti UTS dan UAS
5) Mahasiswa mengumpulkan tugas kuliah melalui Google Classroom
6) Dalam perkuliahan/konsultasi dengan dosen, mahasiswa wajib berperilaku sopan dan memperhatikan etika dalam berkomunikasi melalui telepon/ sms/ WhatsApp
7) PENILAIAN HASIL BELAJAR total bobot 100%, dengan rincian sebagai berikut:
    a. Kehadiran 10%
    b. Tugas 50%
    c. Quiz 20%
    d. UTS 10%
    e. UAS 10%

Yogyakarta, 12 Maret 2025

Dosen Pengampu,

Dr. Marti Widya Sari, S.T., M.Eng.
NIS. 19790327 201201 2 009

RENCANAPEMBELAJARAN SEMESTER (RPS)

(JARINGAN KOMPUTER TINGKAT LANJUT)

(Dr. Marti Widya Sari, S.T., M.Eng.)

PROGRAM STUDI INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PGRI
YOGYAKARTA
2025

RENCANA PEMBELAJARAN SEMESTER
(RPS)

Mata Kuliah : Jaringan Komputer Lanjut Semester : 3 Kode : JRK SKS : 4
Program Studi : Informatika Dosen : Dr. Marti Widya Sari, S.T., M.Eng.

Capaian Pembelajaran Program Studi (CP-PRODI) :

Memiliki kemampuan praktis untuk melakukan pengujian skala laboratorium terhadap rancangan sistem keteknikan yang didukung dengan pengambilan dan validasi data menggunakan kaidah-kaidah statistik yang benar serta hasil pengujiannya diperkuat dengan survei lapangan.

Capaian Pembelajaran Mata Kuliah (CP-MK) :

1 Mampu memahami konsep jaringan komputer dan protokol jaringan TCP/IP.
2 Mampu memahami dan menjelaskan fungsi dan cara kerja lapisan physical jaringan komputer.
3 Mampu memahami dan menjelaskan fungsi dan cara kerja lapisan data link jaringan komputer.
4 Mampu menggunakan perulangan dan percabangan untuk mengembangkan sebuah aplikasi.
5 Mampu memahami dan menjelaskan fungsi dan cara kerja lapisan network jaringan komputer.
6 Mampu memahami dan menjelaskan fungsi dan cara kerja lapisan transport jaringan komputer.
7 Mampu memahami dan menjelaskan fungsi dan cara kerja lapisan application jaringan komputer.
8 Mampu membuat, mengkonfigurasi dan menganalisis jaringan LAN Ethernet

JADWAL, URAIAN MATERI DAN KEGIATAN PERKULIAHAN

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
1	✓ Memahami kontrak kuliah; ✓ Mampu menyebutkan komponen-komponen jaringan komputer ✓ Mampu menyebutkan ukuran kiner jaringan komputer ✓ Mampu menyebutkan lapisan protokol jaringan komputer ✓ Mampu menggunakan tool pengujian kinerja jaringan komputer	➢ Kontrak Kuliah ➢ Pengantar Jaringan Komputer ➢ Kebutuhan Jaringan Komputer ➢ Pengukuran kinerja Jaringan Komputer ➢ Arsitektur Internet ➢ Lapisan protokol Jaringan Komputer ➢ Implementasi open source Jaringan Komputer	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2%)
2	✓ Mampu menjelaskan fungsi lapisan physical ✓ Mampu menyebutkan jenis data dan sinyal pada jaringan komputer ✓ Mampu menjelaskan blok transmission dan reception flow ✓ Mampu menjelaskan medium kabel dan wireless ✓ Mampu membuat pengkodean informasi dan transmisi baseband	➢ Lapisan Physical ➢ Data dan sinyal ➢ Transmission dan reception flow ➢ Medium kabel dan wireless ➢ Pengkodean informasi dan transmisi baseband ➢ Modulasi digital dan multiplexing ➢ Spread spectrum ➢ Single-Carrier vs. Multipe-Carrier ➢ MIMO	Ceramah, tanya-jawab, tugas materi kuliah.	200		b. Mengerjakan Tugas	Tugas (2%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu membedakan modulasi digital dan multiplexing ✓ Mampu menjelaskan metode spread spectrum ✓ Mampu menjelaskan perbedaan Single-Carrier vs. Multipe-Carrier						
3	✓ Mampu menjelaskan fungsi lapisan Data link ✓ Mampu menjelaskan format Framing ✓ Mampu menjelaskan sistem Addressing IPv4 dan IPv6 ✓ Mampu menjelaskan Error control dan reliability ✓ Mampu menjelaskan flow control ✓ Mampu menjelaskan fungsi Medium Access Control ✓ Mampu menjelaskan cara kerja High-Level Data Link Control ✓ Mampu menjelaskan cara kerja Point-to-Point Protocol ✓ Mampu menjelaskan cara kerja Ethernet IEEE 802.3	➢ Lapisan Data link ➢ Framing ➢ Addressing ➢ Error control dan reliability ➢ Flow control ➢ Medium Access Control ➢ High-Level Data Link Control ➢ Point-to-Point Protocol ➢ Ethernet IEEE 802.3	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
4	✓ Mampu menjelaskan cara kerja Wireless Link ✓ Mampu menjelaskan cara kerja WLAN IEEE 802.11 ✓ Mampu menjelaskan cara kerja Teknologi Bluetooth ✓ Tekn Mampu menjelaskan cara kerja ologi WiMAX ✓ Mampu menjelaskan cara kerja Bridging ✓ Mampu menjelaskan cara kerja Virtual LAN ✓ Mampu menjelaskan fungsi device driver Network Interface	➢ Wireless Link ➢ WLAN IEEE 802.11 ➢ Teknologi Bluetooth ➢ Teknologi WiMAX ➢ Bridging ➢ Virtual LAN ➢ Device driver Network Interface	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2%)
5	✓ Mampu menjelaskan lapisan protokol Internet ✓ Mampu menjelaskan konektifitas dan skalabilitas jaringan komputer ✓ Mampu menjelaskan cara kerja resource sharing ✓ Mampu menjelaskan pengalamatan Internet Protocol versi 4 ✓ Mampu menjelaskan cara kerja Network Address Translation	➢ Lapisan protokol Internet ➢ Konektifitas ➢ Skalabilitas ➢ Resource sharing ➢ Internet Protocol versi 4 ➢ Network Address Translation ➢ Internet Protocol versi 6 ➢ Address Resolution Protocol ➢ Dynamic Host Configuration ➢ ICMP	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu menjelaskan pengalamatan Internet Protocol versi 6 ✓ Mampu menjelaskan cara kerja Address Resolution Protocol ✓ Mampu menjelaskan cara kerja Dynamic Host Configuration ✓ Mampu menjelaskan cara kerja ICMP						
6	✓ Mampu membuat jaringan komputer Ethernet IEEE 802.3 sederhana yang hanya terdiri dari dua host dan terhubung secara langsung (direct link) menggunakan kabel UTP. ✓ Mampu memahami format frame dan pengalamatan pada data link Ethernet. ✓ Mampu menguji dan menganalisis kinerja jaringan Ethernet direct link. ✓ Mampu membuat jaringan komputer LAN Ethernet IEEE 802.3 menggunakan switch hub MikroTik.	➢ Praktimkum Modul-1: Jaringan LAN Ethernet (Direct link) IEEE 802.3 ➢ Praktikum Modul-2: Jaringan LAN Ethernet (Switch Link) IEEE 802.3	Tugas pendahuluan, praktikum, tugas analisis data, tugas laporan.	200		a. Mengikuti Praktikum b. Mengerjakan laporan praktikum	Prak (10 %)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu memahami format frame dan pengalamatan pada data link Ethernet IEEE 802.3. ✓ Mampu menguji dan menganalisis kinerja jaringan Ethernet swicth link.						
7	✓ Mampu membuat jaringan komputer WLAN WiFi IEEE 802.11 menggunakan wireless router MikroTik. ✓ Mampu memahami format frame dan pengalamatan pada data link WiFi IEEE 802.11. ✓ Mampu menguji dan menganalisis kinerja jaringan WLAN WiFi IEEE 802.11. ✓ Mampu membuat internetworking jaringan komputer yang terdiri atas jaringan Ethernet IEEE 802.3 dan jaringan WiFi IEEE 802.11. ✓ Mampu memahami format header packet di lapisan network.	➢ Praktikum Modul-3: Jaringan WLAN WiFi IEEE 802.11 ➢ Praktikum Modul-4: Internetworking	Tugas pendahuluan, praktikum, tugas analisis data, tugas laporan.	200		a. Mengikuti Praktikum b. Mengerjakan laporan praktikum	Prak (10 %)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu memahami IPv4 address dan metode subneting menggunakan CIDR. ✓ Mampu memahami static routing, NAT dan ARP..						
8	Mampu menjawab pertanyaan UTS.	Semua materi yang telah dipelajari sebelumnya	Ujian Tertulis	120		Menjawab semua pertanyaan	UTS (10 %)
9	✓ Mampu menjelaskan prisip routing ✓ Mampu menjelaskan cara kerja Intra-Domain routing ✓ Mampu menjelaskan cara kerja Inter-Domain rouitng ✓ Mampu menjelaskan cara kerja Multicast routing ✓ Mampu menjelaskan cara kerja Inter-Domain Multicast	➢ Prisip routing ➢ Intra-Domain routing ➢ Inter-Domain rouitng ➢ Multicast routing ➢ Inter-Domain Multicast	Ceramah, tanya-jawab, tugas materi kuliah.	200 menit		a. Mengerjakan Tugas	Tugas (2 %)
10	✓ Mampu menjelaskan fungsi lapisan transport ✓ Mampu menjelaskan perbedaan antara Node-to-node vs. end-to-end ✓ Mampu menjelaskan cara kerja Error control ✓ Mampu menjelaskan cara kerja Flow control dan congestion control	➢ Lapisan transport ➢ Node-to-node vs. end-to-end ➢ Error control dan reabilitas ➢ Flow control dan congestion control ➢ Aliran packet pada lapisan transport ➢ User Datagram Protocol ➢ Format header UDP	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2 %)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu menjelaskan cara kerja aliran packet pada lapisan transport ✓ Mampu menjelaskan fungsi User Datagram Protocol ✓ Mampu menjelaskan Format header UDP ✓ Mampu menjelaskan cara kerja Per-segment checksum ✓ Mampu menjelaskan cara kerja Transmission Control Protocol ✓ Mampu menjelaskan format header TCP ✓ Mampu menjelaskan cara kerja TCP flow control ✓ Mampu menjelaskan cara kerja TCP congestion control	➢ Per-segment checksum ➢ Transmission Control Protocc ➢ Format header TCP ➢ TCP flow control ➢ TCP congestion control					
11-12	✓ Mampu menjelaskan TCP performance ✓ Mampu menjelaskan fungsi pemograman socket ✓ Mampu menjelaskan cara kerja binding aplikasi melalui UDP dan TCP ✓ Mampu menjelaskan cara kerja protokol transport untuk aplikasi realtime ✓ Mampu menjelaskan cara kerja RTP	➢ TCP performance ➢ Pemograman socket ➢ Binding aplikasi melalui UDP dan TCP ➢ Protokol transport untuk aplikasi realtime ➢ RTP ➢ RTCP	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2%)

Minggu Ke-	Kemampuan Akhir Yang Diharapkan	Bahan Kajian (Materi Pelajaran)	Strategi Pembelajaran/Metode Pembelajaran	Waktu Belajar (menit)	Pengalaman Belajar Mahasiswa	Kriteria Penilaian (Indikator)	Bobot Nilai (%)
(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
	✓ Mampu menjelaskan cara kerja RTCP						
12-13	✓ Mampu menjelaskan fungsi Lapisan aplikasi ✓ Mampu menjelaskan cara kerja Domain Name System (DNS) ✓ Mampu menjelaskan cara kerja E-Mail ✓ Mampu menjelaskan cara kerja World Wide Web (WWW) ✓ Mampu menjelaskan cara kerja File Transfer Protocol (FTP)	➢ Lapisan aplikasi ➢ Domain Name System (DNS) ➢ E-Mail ➢ World Wide Web (WWW) ➢ File Transfer Protocol (FTP)	Ceramah, tanya-jawab, tugas materi kuliah.	200		a. Mengerjakan Tugas	Tugas (2%)
14-15	Praktikum menggunakan Packet Tracer untuk simulasi jaringan komputer	➢		200			
16	Mengerjakan Final Project	➢ UAS	Final Project	200			UAS (10 %)

Sumber Belajar/ Referensi

[1]. Computer Networks: An Open Source Approach, Ying-Dar Lin, Ren-Hung Hwang, Fred Baker, published by McGraw Hill, Feb 2011.
[2]. Computer Networking A Top Down Approach, Kurose and Ross, Pearson.

Mengetahui,	Yogyakarta, 10 September 2021
Ketua Program Studi,	Dosen Pengampu,
(Puji Handayani Putri, M.Kom)	(Marti Widya Sari, S.T., M.Eng.)
NIS.	NIS. 19790327 201201 2 009

Modul Praktikum
Jaringan Komputer Tingkat Lanjut
2023

| Program Studi S1 Informatika | Fakultas Sains dan Teknologi |
| Universitas PGRI Yogyakarta |

Dr. Marti Widya Sari, S.T., M.Eng.

HALAMAN PENGESAHAN

Disusun Oleh	Diperiksa & Dikendalikan Oleh	Disetujui oleh
Dosen Pengampu, Dr. Marti Widya Sari, S.T., M.Eng.	PPMPS, Prahenusa Wahyu Ciptadi, M.T.	Kaprodi S1 Informatika, Puji Handayani Putri, M.Kom.
Modul ini sah dan diberlakukan mulai: Tanggal 12 September 2023		

KATA PENGANTAR

Puji syukur ke hadirat Tuhan Yang Maha Kuasa, yang telah memberikan rahmat-Nya sehingga Modul Mata Kuliah Jaringan Komputer Tingkat Lanjut untuk mahasiswa Program Studi S1 Informatika Universitas PGRI Yogyakarta ini dapat diselesaikan dengan sebaik-baiknya.

Modul ini dibuat sebagai pedoman dalam melakukan kegiatan penunjang mata kuliah Jaringan Komputer Tingkat Lanjut pada Program Studi S1 Informatika Universitas PGRI Yogyakarta. Modul ini diharapkan dapat membantu mahasiswa/i dalam proses belajar mandiri. Pada setiap topik telah ditetapkan semua materi yang harus dipelajari oleh mahasiswa serta teori singkat untuk memperdalam pemahaman mahasiswa mengenai materi yang dibahas.

Penyusun meyakini bahwa dalam pembuatan Modul Mata Kuliah Jaringan Komputer Tingkat Lanjut ini masih jauh dari sempurna. Oleh karena itu penyusun mengharapkan kritik dan saran yang membangun guna penyempurnaan modul praktikum ini di masa yang akan datang.

Akhir kata, penyusun mengucapkan banyak terima kasih kepada semua pihak yang telah membantu baik secara langsung maupun tidak langsung.

Yogyakarta, 10 September 2023

Penyusun

DAFTAR ISI

HALAMAN PENGESAHAN.....2
KATA PENGANTAR 3
DAFTAR ISI.....4
[PRAKTIKUM KE-1].....5
Menginisialisasi dan Memuat Ulang Router dan Switch.....5
[PRAKTIKUM KE-2].....8
Membangun Sesi Konsol dengan Istilah Tera 8
[PRAKTIKUM KE-3].....14
Researching Networking Standards.....14
[PRAKTIKUM KE-4].....16
Membangun Kabel Crossover Ethernet 16
[PRAKTIKUM KE-5].....21
Melihat Alamat MAC Perangkat Jaringan.....21
[PRAKTIKUM KE-6].....24
Menjelajahi Karakteristik Fisik Router.....24
[PRAKTIKUM KE-7].....27
Menggunakan Kalkulator Windows dengan Alamat Jaringan.....27
[PRAKTIKUM KE-8].....30
Menghitung Subnet IPv4 30
[PRAKTIKUM KE-9].....33
Menggunakan Wireshark untuk Mengamati TCP 3-Way Handshake.....33
[PRAKTIKUM KE-10].....36
Meneliti Berbagi File Peer-to-Peer 36
[PRAKTIKUM KE-11].....38
Meneliti Ancaman Keamanan Jaringan 38

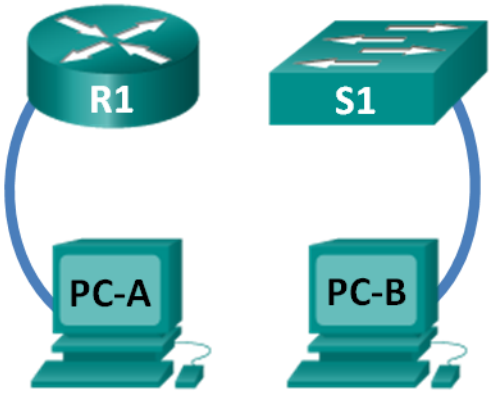
[PRAKTIKUM KE-1]

Menginisialisasi dan Memuat Ulang Router dan Switch

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu mengatur perangkat di jaringan seperti yang ditampilkan di Topologi
2. Mahasiswa mampu melakukan inisialisasi Router dan Muat Ulang
3. Mahasiswa mampu menginisialisasi Switch dan Reload

[PEMBAHASAN]



Gambar 1.1. Topologi

Sebelum memulai lab praktis CCNA yang menggunakan router atau sakelar Cisco, pastikan bahwa perangkat yang digunakan telah dihapus dan tidak ada konfigurasi startup. Jika tidak, hasil lab Anda mungkin tidak dapat diprediksi. Lab ini menyediakan prosedur detail untuk menginisialisasi dan memuat ulang router Cisco dan switch Cisco.

Catatan: Router yang digunakan dengan lab praktis CCNA adalah Cisco 1941 Integrated Services Routers (ISRs) dengan Cisco IOS Release 15.2(4)M3 (gambar universalalk9). Sakelar yang digunakan adalah Cisco Catalyst 2960s dengan Cisco IOS Release 15.0(2) (gambar lanbasek9). Router, switch, dan versi

Cisco IOS lainnya dapat digunakan. Bergantung pada model dan versi Cisco IOS, perintah yang tersedia dan output yang dihasilkan mungkin berbeda dari yang ditampilkan di lab.

Sumber Daya yang Dibutuhkan

• 1 Router (Cisco 1941 dengan perangkat lunak Cisco IOS
• 1 Switch (Cisco 2960 dengan gambar Cisco IOS Release 15.0(2)
• 2 PC (Windows 7 atau 8 dengan program emulasi terminal
• Kabel konsol untuk mengonfigurasi perangkat Cisco IOS melalui port konsol

Bagian 1: Mengatur Perangkat di Jaringan seperti yang Ditampilkan di Topologi

Langkah 1: Kabel jaringan seperti yang ditunjukkan pada topologi.

Pasang kabel konsol ke perangkat yang ditunjukkan pada diagram topologi.

Langkah 2: Nyalakan semua perangkat di topologi.

Tunggu hingga semua perangkat menyelesaikan proses pemuatan perangkat lunak sebelum pindah ke Bagian 2.

Bagian 2: Inisialisasi Router dan Muat Ulang

Langkah 1: Hubungkan ke router.

Langkah 2: Hapus file konfigurasi startup dari NVRAM.

Langkah 3: Muat ulang router.

Keluarkan perintah muat ulang untuk menghapus konfigurasi lama dari memori. Saat diminta Lanjutkan dengan memuat ulang, tekan Enter untuk mengonfirmasi pemuatan ulang. Menekan tombol lain akan membatalkan pemuatan ulang.

Langkah 4: Abaikan dialog konfigurasi awal.

Setelah router dimuat ulang, Anda akan diminta untuk masuk ke dialog konfigurasi awal. Masukkan no dan tekan Enter.

Langkah 5: Hentikan program instal otomatis.

Anda akan diminta untuk menghentikan program autoinstall. Tanggapi ya lalu tekan Enter.

Bagian 3: Menginisialisasi Switch dan Reload

Langkah 1: Sambungkan ke sakelar.

Konsol ke sakelar dan masuk ke mode EXEC yang diistimewakan.

Langkah 2: Tentukan apakah ada jaringan area lokal virtual (VLAN) yang dibuat.

Gunakan perintah show flash untuk menentukan apakah ada VLAN yang telah dibuat di switch.

Langkah 3: Hapus file VLAN.

Langkah 4: Hapus file konfigurasi startup.

Gunakan perintah erase startup-config untuk menghapus file konfigurasi startup dari NVRAM. Saat Anda diminta untuk menghapus file konfigurasi, tekan Enter untuk mengonfirmasi penghapusan. (Menekan tombol lain akan membatalkan operasi.)

Langkah 5: Muat ulang switch

Muat ulang switch untuk menghapus informasi konfigurasi lama dari memori. Saat Anda diminta untuk memuat ulang switch, tekan Enter untuk melanjutkan memuat ulang. (Menekan tombol lain akan membatalkan pemuatan ulang.)

Langkah 6: Abaikan dialog konfigurasi awal.

Setelah sakelar dimuat ulang, Anda akan melihat prompt untuk masuk ke dialog konfigurasi awal. Ketik no pada prompt dan tekan Enter.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-2]

Membangun Sesi Konsol dengan Istilah Tera

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Mengakses Cisco Switch melalui Serial Console Port
2. Mahasiswa mampu Menampilkan dan Mengonfigurasi Pengaturan Perangkat Dasar
3. Mahasiswa mampu Mengakses Router Cisco Menggunakan Kabel Konsol Mini-USB

[PEMBAHASAN]

Berbagai model router dan switch Cisco digunakan di semua jenis jaringan. Perangkat ini dikelola menggunakan koneksi konsol lokal atau koneksi jarak jauh. Hampir semua perangkat Cisco memiliki port konsol serial yang dapat Anda sambungkan. Beberapa model terbaru, seperti Integrated Services Router (ISR) G2 1941 yang digunakan di lab ini, juga memiliki port konsol USB.

Di lab ini, Anda akan mempelajari cara mengakses perangkat Cisco melalui koneksi lokal langsung ke port konsol, menggunakan program emulasi terminal yang disebut Tera Term. Anda juga akan mempelajari cara mengonfigurasi pengaturan port serial untuk koneksi konsol Tera Term. Setelah Anda membuat koneksi konsol dengan perangkat Cisco, Anda dapat menampilkan atau mengonfigurasi pengaturan perangkat. Anda hanya akan menampilkan setelan dan mengonfigurasi jam di lab ini.

Catatan: Router yang digunakan dengan lab praktis CCNA adalah Cisco 1941 ISR dengan Cisco IOS Release 15.2(4)M3 (gambar universalk9). Sakelar yang digunakan di laboratorium adalah Cisco Catalyst 2960s dengan Cisco IOS Release 15.0(2) (gambar lanbasek9). Router, switch, dan versi Cisco IOS lainnya

dapat digunakan. Bergantung pada model dan versi Cisco IOS, perintah yang tersedia dan output yang dihasilkan mungkin berbeda dari yang ditampilkan di lab. Lihat Tabel Ringkasan Antarmuka Router di bagian akhir lab untuk pengidentifikasi antarmuka yang benar.

Catatan: Pastikan sakelar dan router telah dihapus dan tidak ada konfigurasi startup. Jika Anda tidak yakin, hubungi instruktur Anda.

Sumber Daya yang Dibutuhkan

- 1 Router (Cisco 1941 dengan perangkat lunak Cisco IOS, rilis gambar universal 15.2(4)M3 atau sebanding)
- 1 Switch (Cisco 2960 dengan gambar Cisco IOS Release 15.0(2) lanbasek9 atau sebanding)
- 1 PC (Windows 7 atau 8 dengan program emulasi terminal, seperti Tera Term)
- Rollover (DB-9 ke RJ-45) kabel konsol untuk mengonfigurasi sakelar atau router melalui port konsol RJ-45
- Kabel Mini-USB untuk mengkonfigurasi router melalui port konsol USB

Bagian 1: Mengakses Cisco Switch melalui Serial Console Port

Anda akan menyambungkan PC ke sakelar Cisco menggunakan kabel konsol rollover. Koneksi ini akan memungkinkan Anda mengakses CLI dan menampilkan pengaturan atau mengonfigurasi sakelar.

Langkah 1: Sambungkan sakelar Cisco dan komputer menggunakan kabel konsol rollover.

sebuah. Sambungkan kabel konsol rollover ke port konsol RJ-45 sakelar.

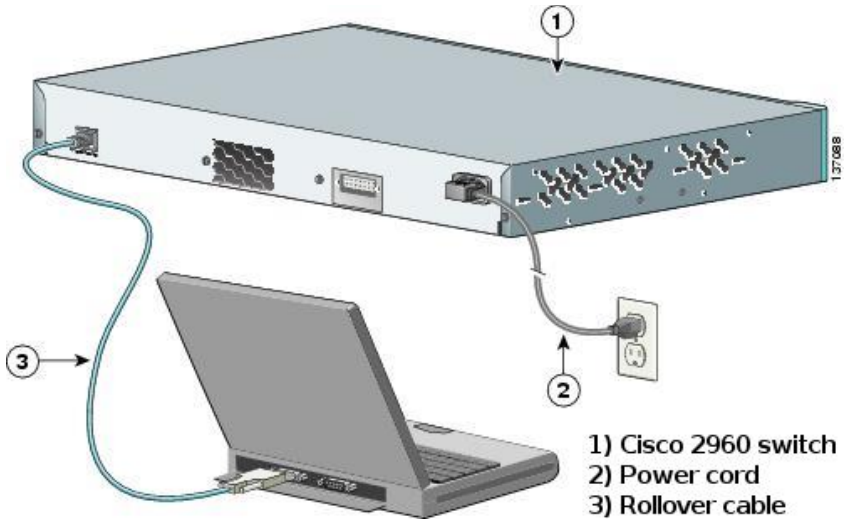
b. Sambungkan ujung kabel lainnya ke port serial COM di komputer.

Catatan: Port serial COM tidak lagi tersedia di sebagian besar komputer. Adaptor USB-ke-DB9 dapat digunakan dengan kabel konsol rollover untuk koneksi

konsol antara komputer dan perangkat Cisco. Adaptor USB-ke-DB9 dapat dibeli di toko elektronik komputer mana pun.

Catatan: Jika menggunakan adaptor USB-ke-DB9 untuk menyambungkan ke port COM, Anda mungkin perlu menginstal driver untuk adaptor yang disediakan oleh produsen komputer Anda. Untuk menentukan port COM yang digunakan oleh adaptor, silakan lihat Bagian 3 Langkah 4. Nomor port COM yang benar diperlukan untuk terhubung ke perangkat Cisco IOS menggunakan emulator terminal di Langkah 2.

c. Nyalakan sakelar Cisco dan komputer.



Langkah 2: Konfigurasikan Tera Term untuk membuat sesi konsol dengan sakelar.

Tera Term adalah program emulasi terminal. Program ini memungkinkan Anda untuk mengakses keluaran terminal sakelar. Ini juga memungkinkan Anda untuk mengonfigurasi sakelar.

Bagian 2: Menampilkan dan Mengonfigurasi Pengaturan Perangkat Dasar

Di bagian ini, Anda diperkenalkan dengan mode eksekutif pengguna dan istimewa. Anda akan menentukan versi iOS, menampilkan pengaturan jam, dan mengonfigurasi jam pada sakelar.

Langkah 1: Menampilkan versi gambar IOS sakelar.

a. Setelah sakelar menyelesaikan proses pengaktifannya, pesan berikut ini ditampilkan. Masukkan n untuk melanjutkan.
b. Saat Anda berada dalam mode pengguna EXEC, tampilkan versi iOS untuk sakelar Anda.

Langkah 2: Konfigurasi Clock

Saat Anda mempelajari lebih lanjut tentang jaringan, Anda akan melihat bahwa mengonfigurasi waktu yang tepat pada sakelar Cisco dapat membantu saat Anda memecahkan masalah. Langkah-langkah berikut secara manual mengonfigurasi jam internal sakelar.

Bagian 3: (Opsional) Mengakses Router Cisco Menggunakan Kabel Konsol Mini-USB

Jika Anda menggunakan router Cisco 1941, atau perangkat Cisco IOS lainnya dengan port konsol mini-USB, Anda dapat mengakses port konsol perangkat menggunakan kabel mini-USB yang terhubung ke port USB di komputer Anda.

Catatan: Kabel konsol mini-USB adalah jenis kabel mini-USB yang sama yang digunakan dengan perangkat elektronik lainnya, seperti hard drive USB, printer USB, atau hub USB. Kabel mini-USB ini dapat dibeli dari Cisco Systems, Inc. atau vendor pihak ketiga lainnya. Harap verifikasi bahwa Anda menggunakan kabel mini-USB, bukan kabel micro-USB, untuk menyambungkan ke port konsol mini-USB pada perangkat Cisco IOS.

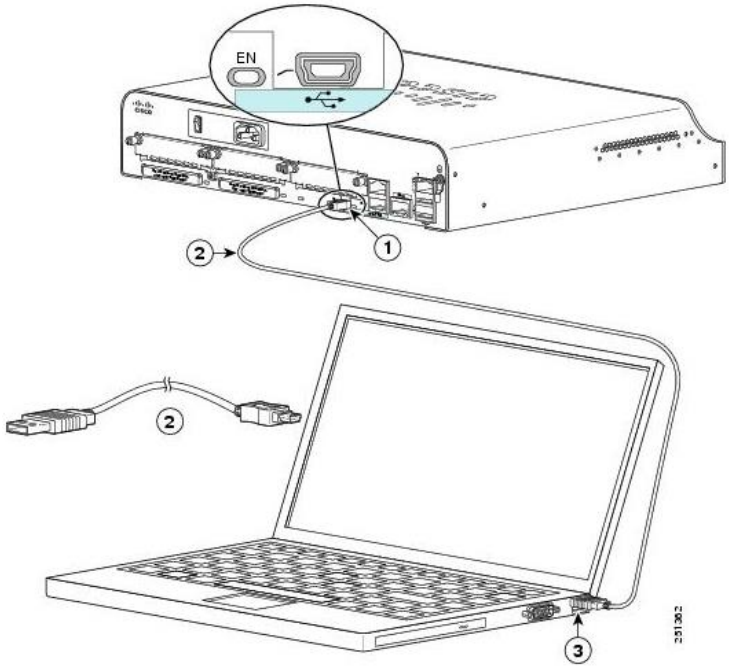
Catatan: Anda harus menggunakan port USB atau port RJ-45. Jangan gunakan kedua port secara bersamaan. Ketika port USB digunakan, port ini diprioritaskan daripada port konsol RJ-45.

Langkah 1: Siapkan koneksi fisik dengan kabel mini-USB.

a. Sambungkan kabel mini-USB ke port konsol mini-USB di router.

b. Sambungkan ujung kabel lainnya ke port USB di komputer.

c. Nyalakan router dan komputer Cisco.



1) USB 5-pin mini Type-B console port
2) USB 5-pin mini Type-B to USB Type-A Console Cable
3) USB Type-A connector

Langkah 2: Pastikan konsol USB sudah siap.

Jika Anda menggunakan PC berbasis Microsoft Windows dan indikator LED port konsol USB (berlabel EN) tidak menyala hijau, instal driver konsol USB Cisco.

Driver USB harus diinstal sebelum menyambungkan PC berbasis Microsoft Windows ke perangkat Cisco IOS dengan kabel USB. Driver dapat ditemukan di www.cisco.com dengan perangkat Cisco IOS terkait.

Catatan: Anda harus memiliki akun Cisco Connection Online (CCO) yang valid untuk mengunduh file ini.

Catatan: Tautan ini terkait dengan router Cisco 1941. Namun, driver konsol USB tidak spesifik untuk model perangkat Cisco IOS. Driver konsol USB ini hanya berfungsi dengan router dan sakelar Cisco. Komputer memerlukan reboot setelah menyelesaikan penginstalan driver USB.

Catatan: Setelah file diekstraksi, folder tersebut berisi instruksi untuk instalasi, penghapusan, dan driver yang diperlukan untuk sistem operasi dan arsitektur yang berbeda. Silakan pilih versi yang sesuai untuk sistem Anda.

Ketika indikator LED untuk port konsol USB berubah menjadi hijau, port konsol USB siap diakses.

Langkah 3: (Opsional) Aktifkan port COM untuk PC Windows 7.

Jika Anda menggunakan PC Microsoft Windows 7, Anda mungkin perlu melakukan langkah-langkah berikut untuk mengaktifkan port COM:

a. Klik ikon Mulai Windows untuk mengakses Panel Kontrol.

b. Buka Pengelola Perangkat.

c. Klik link pohon Ports (COM & LPT) untuk mengembangkannya. Klik kanan ikon Port Serial USB dan pilih Perbarui driver Perangkat Lunak

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-3]

Researching Networking Standards

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu melakukan Penelitian Organisasi Standar Jaringan
2. Mahasiswa memiliki Pengalaman Internet dan Jaringan Komputer

[PEMBAHASAN]

Menggunakan mesin pencari web seperti Google, teliti organisasi nirlaba yang bertanggung jawab untuk menetapkan standar internasional untuk Internet dan pengembangan teknologi Internet.

Bagian 1: Penelitian Organisasi Standar Jaringan

Di Bagian 1, Anda akan mengidentifikasi beberapa organisasi standar utama dan karakteristik penting, seperti jumlah tahun berdiri, ukuran keanggotaan mereka, tokoh sejarah penting, beberapa tanggung jawab dan tugas, peran pengawasan organisasi, dan lokasi kantor pusat organisasi.

Gunakan browser web atau situs web untuk berbagai organisasi untuk meneliti informasi tentang organisasi berikut dan orang-orang yang berperan penting dalam pemeliharaannya.

Anda dapat menemukan jawaban atas pertanyaan di bawah ini dengan mencari akronim dan istilah organisasi berikut: ISO, ITU, ICANN, IANA, IEEE, EIA, TIA, ISOC, IAB, IETF, W3C, RFC, dan Wi-Fi Alliance.

Bagian 2: Renungkan Pengalaman Internet dan Jaringan Komputer

Luangkan waktu sejenak untuk memikirkan tentang Internet saat ini dalam kaitannya dengan organisasi dan teknologi yang baru saja Anda teliti. Kemudian jawab pertanyaan berikut.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-4]

Membangun Kabel Crossover Ethernet

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Menganalisis Standar Kabel Ethernet dan Pinout
2. Mahasiswa mampu Membangun Kabel Crossover Ethernet
3. Mahasiswa mampu Menguji Kabel Crossover Ethernet

[PEMBAHASAN]

Di lab ini, Anda akan membuat dan mengakhiri kabel crossover Ethernet dan mengujinya dengan menyambungkan dua PC dan melakukan ping di antara keduanya. Anda pertama-tama akan menganalisis standar Asosiasi Industri Telekomunikasi/Asosiasi Industri Elektronik (TIA/EIA) 568-A dan 568-B dan bagaimana penerapannya pada kabel Ethernet. Anda kemudian akan membuat kabel crossover Ethernet dan mengujinya. Terakhir, Anda akan menggunakan kabel yang baru saja Anda buat untuk menghubungkan dua PC secara bersamaan dan mengujinya dengan melakukan ping di antara keduanya.

Catatan: Dengan kemampuan penginderaan otomatis yang tersedia di banyak perangkat, seperti sakelar Router Layanan Terpadu (ISR) Cisco 1941, Anda mungkin melihat kabel langsung terhubung seperti perangkat.

Bagian 1: Menganalisis Standar Kabel Ethernet dan Pinout

TIA/EIA telah menetapkan standar pemasangan kabel unshielded twisted pair (UTP) untuk digunakan di lingkungan pemasangan kabel LAN. TIA/EIA 568-A dan 568-B menetapkan standar pemasangan kabel komersial untuk instalasi LAN; ini adalah standar yang paling umum digunakan dalam pemasangan kabel LAN untuk organisasi dan mereka menentukan kabel warna mana yang digunakan pada setiap pin.

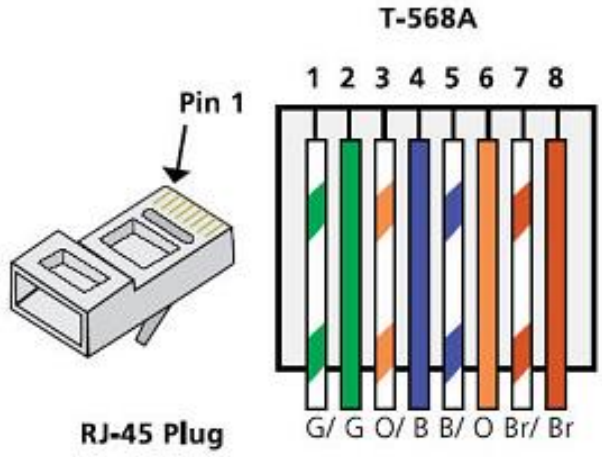
Dengan kabel crossover, pasangan kedua dan ketiga pada konektor RJ-45 di salah satu ujung kabel dibalik di ujung lainnya, yang membalikkan pasangan kirim dan terima. Pinout kabel adalah standar 568-A di satu ujung dan standar 568-B di ujung lainnya. Kabel crossover biasanya digunakan untuk menghubungkan hub ke hub atau switch ke switch, tetapi juga dapat digunakan untuk menghubungkan dua host secara langsung untuk membuat jaringan sederhana.

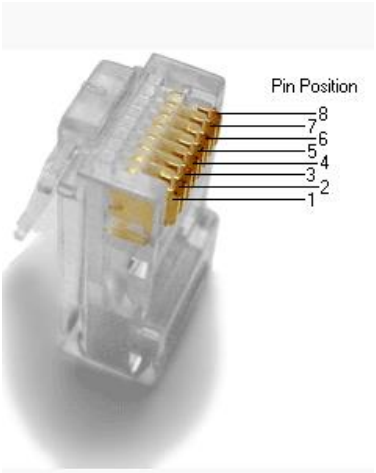
Langkah 1: Analisis diagram dan tabel untuk kabel Ethernet standar TIA/EIA 568-A.

Tabel dan diagram berikut menampilkan skema warna dan pinout, serta fungsi empat pasang kabel yang digunakan untuk standar 568-A.

Catatan: Dalam penginstalan LAN menggunakan 100Base-T (100 Mb/s), hanya dua pasang dari empat pasang yang digunakan.

Diagram berikut menampilkan bagaimana warna kabel dan pinout sejajar dengan jack RJ-45 untuk standar 568-A.

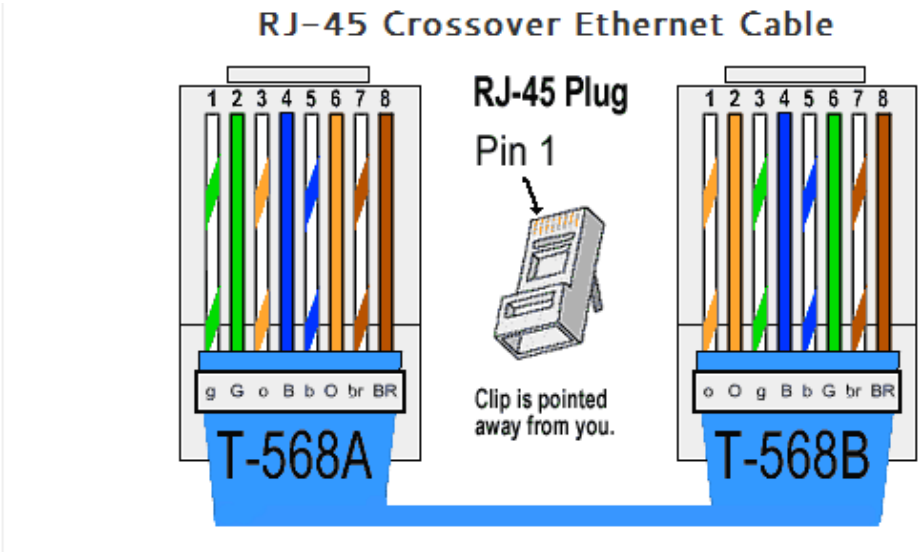




Langkah 2: Analisis diagram dan tabel untuk kabel Ethernet standar TIA/EIA 568-B.

Bagian 2: Membangun Kabel Crossover Ethernet

Kabel crossover memiliki pasangan kedua dan ketiga pada konektor RJ-45 di salah satu ujungnya, terbalik di ujung lainnya. Pinout kabel adalah standar 568-A di satu ujung dan standar 568-B di ujung lainnya. Dua diagram berikut mengilustrasikan konsep ini.



Langkah 1: Buat dan akhiri ujung kabel TIA/EIA 568-A.

sebuah. Tentukan panjang kabel yang dibutuhkan. (Instruktur Anda akan memberi tahu Anda panjang kabel yang harus Anda buat.)

Catatan: Jika Anda membuat kabel di lingkungan produksi, pedoman umumnya adalah menambahkan panjang 12 inci (30,48 cm) lagi.

b. Potong seutas kabel sesuai panjang yang diinginkan dan gunakan penarik kawat Anda, lepaskan selubung kabel sepanjang 5,08 cm (2 in.) dari kedua ujungnya.

c. Pegang empat pasang kabel yang dipilin dengan erat di tempat jaket dipotong. Atur ulang pasangan kabel ke dalam urutan standar pengkabelan 568-A. Lihat diagram, jika perlu. Berhati-hatilah sebisa mungkin untuk mempertahankan lilitan kabel; ini memberikan pembatalan kebisingan.

d. Ratakan, luruskan, dan sejajarkan kabel menggunakan ibu jari dan telunjuk Anda.

e. Pastikan kabel kabel masih dalam urutan yang benar untuk standar 568-A. Dengan menggunakan pemotong kawat Anda, pangkas keempat pasang dalam garis lurus hingga 1,25 hingga 1,9 cm (1/2 hingga 3/4 inci).

f. Tempatkan konektor RJ-45 di ujung kabel Anda, dengan cabang di bagian bawah mengarah ke bawah. Masukkan kabel dengan kuat ke konektor RJ-45. Semua kabel harus terlihat di ujung konektor pada posisi yang tepat. Jika kabel tidak memanjang hingga ujung konektor, cabut kabel, atur ulang kabel seperlunya, dan masukkan kembali kabel ke konektor RJ-45.

g. Jika semuanya sudah benar, masukkan konektor RJ-45 dengan kabel ke crimper. Crimp down cukup keras untuk memaksa kontak pada konektor RJ-45 melalui isolasi pada kabel, sehingga menyelesaikan jalur penghantar.

Langkah 2: Bangun dan akhiri ujung kabel TIA/EIA 568-B.

Ulangi langkah 1a hingga 1g menggunakan skema pengkabelan warna 568-B untuk ujung lainnya.

Bagian 3: Menguji Kabel Crossover Ethernet

Langkah 1: Uji kabelnya.

Banyak penguji kabel akan menguji panjang dan pemetaan kabel. Jika penguji kabel memiliki fitur peta kabel, ia memverifikasi pin mana di salah satu ujung kabel yang terhubung ke pin mana di ujung lainnya.

Jika instruktur Anda memiliki penguji kabel, uji fungsionalitas kabel crossover. Jika gagal, tanyakan kepada instruktur Anda terlebih dahulu apakah Anda harus memasang ulang kabel dan menguji ulang.

Langkah 2: Hubungkan dua PC bersama-sama melalui NIC menggunakan kabel crossover Ethernet Anda.

sebuah. Bekerja sama dengan partner lab, atur PC Anda ke salah satu alamat IP yang ditampilkan di Tabel Pengalamatan (lihat halaman 1). Misalnya, jika PC Anda adalah PC-A, alamat IP Anda harus disetel ke 192.168.10.1 dengan subnet mask 24-bit. Alamat IP mitra Anda harus 192.168.10.2. Alamat gateway default dapat dibiarkan kosong.

b. Menggunakan kabel crossover yang Anda buat, sambungkan kedua PC bersama-sama melalui NIC mereka.

c. Pada prompt perintah PC-A, ping alamat IP PC-B.

Catatan: Firewall Windows mungkin harus dinonaktifkan sementara agar ping berhasil. Jika firewall dinonaktifkan, pastikan Anda mengaktifkannya kembali di akhir lab ini.

d. Ulangi proses dan ping dari PC-B ke PC-A.

Dengan asumsi pengalamatan IP dan firewall bukan masalah, ping Anda akan berhasil jika kabel dibuat dengan benar.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-5]

Melihat Alamat MAC Perangkat Jaringan

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu mengkonfigurasi Perangkat dan Verifikasi Konektivitas
2. Mahasiswa mampu Menampilkan, Menjelaskan, dan Menganalisis Alamat MAC Ethernet

[PEMBAHASAN]

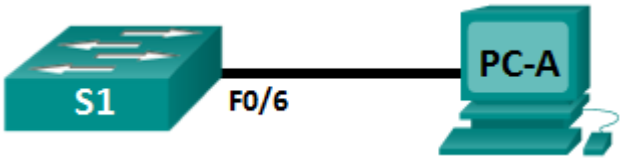
Setiap perangkat di LAN Ethernet diidentifikasi oleh alamat MAC Layer 2. Alamat ini diberikan oleh pabrikan dan disimpan di firmware NIC. Lab ini akan mengeksplorasi dan menganalisis komponen yang menyusun alamat MAC, dan bagaimana Anda dapat menemukan informasi ini di sakelar dan PC.

Anda akan menyambungkan peralatan seperti yang ditunjukkan pada topologi. Anda akan mengonfigurasi sakelar dan PC agar sesuai dengan tabel pengalamatan. Anda akan memverifikasi konfigurasi Anda dengan menguji konektivitas jaringan.

Setelah perangkat dikonfigurasi dan konektivitas jaringan diverifikasi, Anda akan menggunakan berbagai perintah untuk mengambil informasi dari perangkat untuk menjawab pertanyaan tentang peralatan jaringan Anda.

Catatan: Sakelar yang digunakan adalah Cisco Catalyst 2960s dengan Cisco IOS Release 15.0(2) (gambar lanbasek9). Sakelar lain dan versi Cisco IOS dapat digunakan. Bergantung pada model dan versi Cisco IOS, perintah yang tersedia dan output yang dihasilkan mungkin berbeda dari yang ditampilkan di lab.

Catatan: Pastikan sakelar telah dihapus dan tidak memiliki konfigurasi pengaktifan. Jika Anda tidak yakin, tanyakan pada instruktur Anda.



Bagian 1: Konfigurasi Perangkat dan Verifikasi Konektivitas

Di bagian ini, Anda akan mengatur topologi jaringan dan mengonfigurasi pengaturan dasar, seperti alamat IP antarmuka dan nama perangkat. Untuk nama perangkat dan informasi alamat, lihat Tabel Topologi dan Pengalamatan.

Langkah 1: Kabel jaringan seperti yang ditunjukkan pada topologi.

a. Pasang perangkat yang ditunjukkan pada topologi dan kabel seperlunya.

b. Nyalakan semua perangkat di topologi.

Langkah 2: Konfigurasikan alamat IPv4 untuk PC.

a. Konfigurasikan alamat IPv4, subnet mask, dan alamat gateway default untuk PC-A.

b. Dari prompt perintah pada PC-A, ping alamat sakelar.

Langkah 3: Konfigurasikan pengaturan dasar untuk sakelar.

Pada langkah ini, Anda akan mengonfigurasi nama perangkat dan alamat IP, serta menonaktifkan pencarian DNS di sakelar.

Langkah 4: Verifikasi konektivitas jaringan

Setiap perangkat di LAN Ethernet memiliki alamat MAC yang diberikan oleh pabrikan dan disimpan di firmware NIC. Alamat MAC Ethernet panjangnya 48-bit. Mereka ditampilkan menggunakan enam set digit heksadesimal yang biasanya dipisahkan oleh tanda hubung, titik dua, atau titik. Contoh berikut menunjukkan alamat MAC yang sama menggunakan tiga metode notasi yang berbeda:

00-05-9A-3C-78-00 00:05:9A:3C:78:00 0005.9A3C.7800

Catatan: Alamat MAC juga disebut alamat fisik, alamat perangkat keras, atau alamat perangkat keras Ethernet.

Anda akan mengeluarkan perintah untuk menampilkan alamat MAC pada PC dan sakelar, dan Anda akan menganalisis properti masing-masing.

Langkah 1: Analisis alamat MAC untuk NIC PC-A.

Sebelum Anda menganalisis alamat MAC pada PC-A, lihat contoh dari NIC PC yang berbeda. Anda dapat mengeluarkan perintah ipconfig /all untuk melihat alamat MAC NIC Anda. Contoh output layar ditunjukkan di bawah ini. Saat menggunakan perintah ipconfig /all, perhatikan bahwa alamat MAC dirujuk sebagai alamat fisik. Membaca alamat MAC dari kiri ke kanan, enam digit hex pertama mengacu pada vendor (produsen) perangkat ini. Enam digit hex pertama (3 byte) ini juga dikenal sebagai pengidentifikasi unik organisasi (OUI). Kode 3-byte ini diberikan ke vendor oleh organisasi IEEE. Untuk menemukan pabrikan, Anda dapat menggunakan alat seperti www.macvendorlookup.com atau buka situs web IEEE untuk menemukan kode vendor OUI yang terdaftar.

Langkah 2: Analisis alamat MAC untuk antarmuka S1 F0/6.

Anda dapat menggunakan berbagai perintah untuk menampilkan alamat MAC di sakelar.

Langkah 3: Lihat alamat MAC di sakelar.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-6]

Menjelajahi Karakteristik Fisik Router

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Memeriksa Karakteristik Eksternal Router
2. Mahasiswa mampu Memeriksa Karakteristik Internal Router Menggunakan Perintah Tampilkan

[PEMBAHASAN]

Di lab ini, Anda akan memeriksa bagian luar router untuk mengetahui karakteristik dan komponennya, seperti sakelar daya, port manajemen, antarmuka LAN dan WAN, lampu indikator, slot ekspansi jaringan, slot ekspansi memori, dan port USB.

Anda juga akan mengidentifikasi komponen internal dan karakteristik IOS dengan konsol ke dalam router dan mengeluarkan berbagai perintah, seperti tampilkan versi dan tampilkan antarmuka, dari CLI.

Catatan: Router yang digunakan dengan lab praktis CCNA adalah Cisco 1941 Integrated Services Routers (ISRs) dengan Cisco IOS Release 15.2(4)M3 (gambar universalalk9). Router lain dan versi Cisco IOS dapat digunakan. Bergantung pada model dan versi Cisco IOS, perintah yang tersedia dan output yang dihasilkan mungkin berbeda dari yang ditampilkan di lab.

Catatan: Pastikan router telah dihapus dan tidak memiliki konfigurasi startup. Jika Anda tidak yakin, hubungi instruktur Anda.

Bagian 1: Memeriksa Karakteristik Eksternal Router

Gunakan gambar di bawah ini, serta pemeriksaan langsung Anda sendiri pada bagian belakang router Cisco, untuk menjawab pertanyaan berikut. Jangan ragu untuk menggambar panah dan lingkari area gambar yang mengidentifikasi bagian-bagiannya dengan benar.

Catatan: Perute yang digambarkan pada gambar di bawah ini adalah perute Cisco 1941, yang mungkin berbeda dari pembuatan dan model perute di akademi khusus Anda. Anda dapat menemukan informasi dan spesifikasi perangkat untuk router seri Cisco 1941 di situs web Cisco.com.

Langkah 1: Identifikasi berbagai bagian dari router Cisco.

Gambar yang ditunjukkan pada langkah ini adalah backplane Cisco 1941 ISR. Gunakan untuk menjawab pertanyaan di langkah ini. Selain itu, jika Anda memeriksa router model yang berbeda, ruang telah disediakan di sini bagi Anda untuk menggambar backplane dan mengidentifikasi komponen dan antarmuka.

Langkah 2: Periksa aktivitas router dan lampu status.

Bagian 2: Memeriksa Karakteristik Internal Router Menggunakan Perintah Tampilkan

Langkah 1: Buat koneksi konsol ke router dan gunakan perintah show version.

Langkah 2: Gunakan perintah show interface untuk memeriksa interface jaringan.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-7]

Menggunakan Kalkulator Windows dengan Alamat Jaringan

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Akses Kalkulator Windows
2. Mahasiswa mampu Konversi antar Sistem Penomoran
3. Mahasiswa mampu Mengkonversi Alamat Host IPv4 dan Subnet Mask menjadi Biner
4. Mahasiswa mampu Menentukan Jumlah Host dalam Jaringan Menggunakan Pangkat 2
5. Mahasiswa mampu Mengkonversi Alamat MAC dan Alamat IPv6 ke Biner

[PEMBAHASAN]

Teknisi jaringan menggunakan bilangan biner, desimal, dan heksadesimal saat bekerja dengan komputer dan perangkat jaringan. Microsoft menyediakan aplikasi Kalkulator bawaan sebagai bagian dari sistem operasi. Kalkulator versi Windows 7 menyertakan tampilan Standar yang dapat digunakan untuk melakukan tugas aritmatika dasar seperti penjumlahan, pengurangan, perkalian, dan pembagian. Aplikasi Kalkulator juga memiliki kemampuan pemrograman, ilmiah, dan statistik tingkat lanjut.

Di lab ini, Anda akan menggunakan tampilan Pemrogram aplikasi Kalkulator Windows 7 untuk mengonversi antara sistem bilangan biner, desimal, dan heksadesimal. Anda juga akan menggunakan fungsi kekuatan tampilan Ilmiah untuk menentukan jumlah host yang dapat dialamatkan berdasarkan jumlah bit host yang tersedia.

Bagian 1: Akses Kalkulator Windows

Di Bagian 1, Anda akan terbiasa dengan aplikasi kalkulator bawaan Microsoft Windows dan melihat mode yang tersedia.

Langkah 1: Klik tombol Mulai Windows dan pilih Semua Program.

Langkah 2: Klik folder Aksesoris dan pilih Kalkulator.

Langkah 3: Setelah Calculator terbuka, klik menu View.

Bagian 2: Konversi antar Sistem Penomoran

Pada tampilan Windows Calculator Programmer, tersedia beberapa mode sistem bilangan: Hex (Hexadecimal atau basis 16), Des (Desimal atau basis 10), Okt (Oktal atau basis 8), dan Bin (Biner atau basis 2).

Kita terbiasa menggunakan sistem bilangan desimal yang menggunakan angka 0 sampai 9. Sistem bilangan desimal digunakan dalam kehidupan sehari-hari untuk semua transaksi penghitungan, uang, dan keuangan. Komputer dan perangkat elektronik lainnya menggunakan sistem penomoran biner dengan hanya angka 0 dan 1 untuk penyimpanan data, transmisi data, dan perhitungan numerik. Semua perhitungan komputer pada akhirnya dilakukan secara internal dalam bentuk biner (digital), terlepas dari bagaimana tampilannya.

Salah satu kelemahan bilangan biner adalah bahwa bilangan biner yang setara dengan bilangan desimal besar bisa sangat panjang. Hal ini membuat mereka sulit untuk membaca dan menulis. Salah satu cara untuk mengatasi masalah ini adalah dengan menyusun bilangan biner menjadi kelompok empat sebagai bilangan heksadesimal. Angka heksadesimal adalah basis 16, dan kombinasi angka dari 0 hingga 9 dan huruf A hingga F digunakan untuk mewakili biner atau desimal yang setara. Karakter heksadesimal digunakan saat menulis atau menampilkan alamat IPv6 dan MAC.

Sistem penomoran oktal pada prinsipnya sangat mirip dengan heksadesimal. Bilangan oktal mewakili bilangan biner dalam kelompok tiga. Sistem penomoran

ini menggunakan angka 0 sampai 7. Bilangan oktal juga merupakan cara mudah untuk merepresentasikan bilangan biner besar dalam kelompok yang lebih kecil, tetapi sistem penomoran ini tidak umum digunakan.

Bagian 3: Mengkonversi Alamat Host IPv4 dan Subnet Mask menjadi Biner

Alamat Internet Protocol versi 4 (IPv4) dan subnet mask direpresentasikan dalam format desimal bertitik (empat oktet), seperti masing-masing 192.168.1.10 dan 255.255.255.0. Ini membuat alamat ini lebih mudah dibaca oleh manusia. Setiap oktet desimal di alamat atau topeng dapat dikonversi menjadi 8 bit biner.

Bagian 4: Menentukan Jumlah Host dalam Jaringan Menggunakan Pangkat 2

Diberi alamat jaringan IPv4 dan subnet mask, bagian jaringan dapat ditentukan bersama dengan jumlah host yang tersedia di jaringan.

Bagian 5: Mengkonversi Alamat MAC dan Alamat IPv6 ke Biner

Alamat Media Access Control (MAC) dan Internet Protocol versi 6 (IPv6) direpresentasikan sebagai digit heksadesimal agar mudah dibaca. Namun, komputer hanya memahami digit biner dan menggunakan digit biner ini untuk perhitungan. Pada bagian ini, Anda akan mengubah alamat heksadesimal ini menjadi alamat biner.

Langkah 1: Ubah alamat MAC menjadi digit biner.

Langkah 2: Ubah alamat IPv6 menjadi digit biner.

Alamat IPv6 juga ditulis dalam karakter heksadesimal untuk kenyamanan manusia. Alamat IPv6 ini dapat dikonversi ke bilangan biner untuk penggunaan komputer.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-8]

Menghitung Subnet IPv4

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Menentukan Subneting Alamat IPv4
2. Mahasiswa mampu Menghitung Subnetting Alamat IPv4

[PEMBAHASAN]

Kemampuan untuk bekerja dengan subnet IPv4 dan menentukan informasi jaringan dan host berdasarkan alamat IP dan subnet mask yang diberikan sangat penting untuk memahami bagaimana jaringan IPv4 beroperasi. Bagian pertama dirancang untuk memperkuat cara menghitung informasi alamat IP jaringan dari alamat IP dan subnet mask yang diberikan. Saat diberi alamat IP dan subnet mask, Anda akan dapat menentukan informasi lain tentang subnet tersebut.

Bagian 1: Menentukan Subneting Alamat IPv4

Di Bagian 1, Anda akan menentukan alamat jaringan dan broadcast, serta jumlah host, dengan alamat IPv4 dan subnet mask.

REVIEW: Untuk menentukan alamat jaringan, lakukan binary ANDing pada alamat IPv4 menggunakan subnet mask yang disediakan. Hasilnya akan menjadi alamat jaringan. Petunjuk: Jika subnet mask memiliki nilai desimal 255 dalam oktet, hasilnya akan SELALU menjadi nilai asli oktet tersebut. Jika subnet mask memiliki nilai desimal 0 dalam oktet, hasilnya SELALU 0 untuk oktet tersebut.

Bagian 2: Menghitung Subnetting Alamat IPv4

Saat diberi alamat IPv4, subnet mask asli, dan subnet mask baru, Anda akan dapat menentukan:

• Alamat jaringan subnet ini

• Alamat broadcast dari subnet ini

• Kisaran alamat host dari subnet ini

• Jumlah subnet yang dibuat

• Jumlah host per subnet

Contoh berikut menunjukkan contoh masalah beserta solusi untuk memecahkan masalah ini:

Diketahui	
Host IP Address:	172.16.77.120
Original Subnet Mask	255.255.0.0
New Subnet Mask:	255.255.240.0
Carilah	
Number of Subnet Bits	4
Number of Subnets Created	16
Number of Host Bits per Subnet	12
Number of Hosts per Subnet	4,094
Network Address of this Subnet	172.16.64.0
IPv4 Address of First Host on this Subnet	172.16.64.1
IPv4 Address of Last Host on this Subnet	172.16.79.254
IPv4 Broadcast Address on this Subnet	172.16.79.255

Mari kita analisis bagaimana tabel ini diselesaikan.

Subnet mask aslinya adalah 255.255.0.0 atau /16. Subnet mask baru adalah 255.255.240.0 atau /20. Perbedaan yang dihasilkan adalah 4 bit. Karena 4 bit dipinjam, kita dapat menentukan bahwa 16 subnet dibuat karena 24 = 16.

Mask baru 255.255.240.0 atau /20 menyisakan 12 bit untuk host. Dengan 12 bit tersisa untuk host, kami menggunakan rumus berikut: 212 = 4.096 – 2 = 4.094 host per subnet.

Binary ANDing akan membantu Anda menentukan subnet untuk masalah ini, yang menghasilkan jaringan 172.16.64.0.

Terakhir, Anda perlu menentukan host pertama, host terakhir, dan alamat broadcast untuk setiap subnet. Salah satu metode untuk menentukan rentang host adalah dengan menggunakan matematika biner untuk bagian host dari alamat tersebut. Dalam contoh kita, 12 bit terakhir dari alamat adalah bagian host. Host pertama akan memiliki semua bit signifikan yang disetel ke nol dan bit yang paling tidak signifikan disetel ke 1. Host terakhir akan memiliki semua bit signifikan yang disetel ke 1 dan bit yang paling tidak signifikan disetel ke 0. Dalam contoh ini, bagian host dari alamat berada di oktet ke-3 dan ke-4.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-9]

Menggunakan Wireshark untuk Mengamati TCP 3-Way Handshake

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Mempersiapkan Wireshark untuk Menangkap Paket
2. Mahasiswa mampu membedakan Tangkap, Temukan, dan Periksa Paket

[PEMBAHASAN]

Di lab ini, Anda akan menggunakan Wireshark untuk menangkap dan memeriksa paket yang dibuat antara browser PC menggunakan HyperText Transfer Protocol (HTTP) dan server web, seperti www.google.com. Ketika sebuah aplikasi, seperti HTTP atau FTP (File Transfer Protocol) pertama kali dimulai pada sebuah host, TCP menggunakan jabat tangan tiga arah untuk membuat sesi TCP yang andal antara kedua host. Misalnya, ketika PC menggunakan browser web untuk menjelajahi internet, jabat tangan tiga arah dimulai, dan sesi dibuat antara host PC dan server web. Sebuah PC dapat memiliki beberapa sesi TCP aktif secara simultan dengan berbagai situs web.

Bagian 1: Mempersiapkan Wireshark untuk Menangkap Paket

Di Bagian 1, Anda akan memulai program Wireshark dan memilih antarmuka yang sesuai untuk mulai menangkap paket.

Langkah 1: Ambil alamat antarmuka PC.

Untuk lab ini, Anda perlu mengambil alamat IP PC Anda dan alamat fisik kartu antarmuka jaringan (NIC), juga disebut alamat MAC.

Langkah 2: Mulai Wireshark dan pilih antarmuka yang sesuai.

Bagian 2: Tangkap, Temukan, dan Periksa Paket

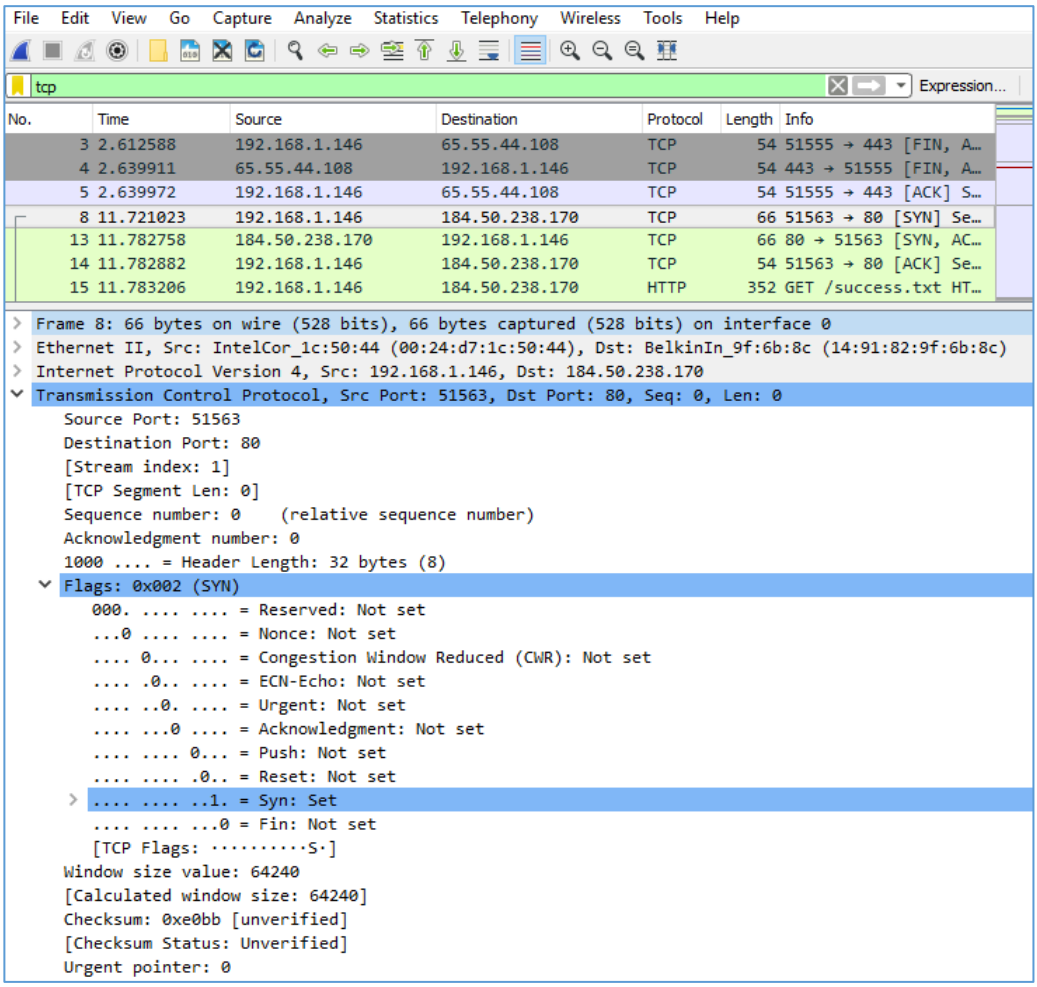
Langkah 1: Tangkap datanya.

Langkah 2: Temukan paket yang sesuai untuk sesi web.

Jika komputer baru saja dihidupkan dan tidak ada aktivitas dalam mengakses internet, Anda dapat melihat seluruh proses dalam keluaran yang diambil, termasuk Address Resolution Protocol (ARP), Domain Name System (DNS), dan TCP three-way jabat tangan. Jika PC sudah memiliki entri ARP untuk gateway default, maka itu berarti dimulai dengan kueri DNS untuk menyelesaikan www.google.com.

Langkah 3: Periksa informasi di dalam paket termasuk alamat IP, nomor port TCP, dan bendera kontrol TCP.

Catatan: Anda mungkin harus menyesuaikan ukuran jendela atas dan tengah dalam Wireshark untuk menampilkan informasi yang diperlukan.



[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-10]

Meneliti Berbagi File Peer-to-Peer

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Identifikasi Jaringan P2P, Protokol Berbagi File, dan Aplikasi
2. Mahasiswa mampu Meneliti Masalah Berbagi File P2P
3. Mahasiswa mampu Meneliti Litigasi Hak Cipta P2P

[PEMBAHASAN]

Komputasi peer-to-peer (P2P) adalah teknologi canggih yang memiliki banyak kegunaan. Jaringan P2P dapat digunakan untuk berbagi dan bertukar file, dan materi elektronik lainnya.

Penggunaan jaringan P2P untuk mengunggah, mengunduh, atau membagikan materi berhak cipta, seperti film, musik, dan perangkat lunak, dapat melanggar hak pemilik hak cipta. Dalam konteks berbagi file P2P, pelanggaran dapat terjadi saat satu orang membeli salinan resmi dan kemudian mengunggahnya ke jaringan P2P untuk dibagikan dengan orang lain. Baik individu yang membuat file tersedia maupun mereka yang membuat salinan dapat ditemukan telah melanggar hak pemilik hak cipta dan mungkin melanggar undang-undang hak cipta.

Masalah lain dengan berbagi file P2P adalah sangat sedikit perlindungan untuk memastikan bahwa file yang dipertukarkan di jaringan ini tidak berbahaya. Jaringan P2P adalah media ideal untuk menyebarkan malware, seperti virus komputer, worm, trojan horse, spyware, adware, dan program berbahaya lainnya. Di lab ini, Anda akan meneliti perangkat lunak berbagi file P2P yang tersedia dan mengidentifikasi masalah yang dapat muncul dari penggunaan teknologi ini.

Bagian 1: Identifikasi Jaringan P2P, Protokol Berbagi File, dan Aplikasi

Di Bagian 1, Anda akan meneliti jaringan P2P dan mengidentifikasi protokol dan aplikasi P2P yang populer.

Langkah 1: Tentukan jaringan P2P.

Bagian 2: Meneliti Masalah Berbagi File P2P

Di Bagian 2, Anda akan meneliti pelanggaran hak cipta P2P dan mengidentifikasi masalah lain yang dapat terjadi dengan berbagi file P2P.

Langkah 1: Teliti pelanggaran hak cipta P2P.

Langkah 2: Identifikasi protokol dan aplikasi berbagi file P2P.

Bagian 3: Meneliti Litigasi Hak Cipta P2P

Di Bagian 3, Anda akan meneliti dan mengidentifikasi tindakan hukum historis yang terjadi sebagai akibat dari pelanggaran hak cipta P2P.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

[PRAKTIKUM KE-11]

Meneliti Ancaman Keamanan Jaringan

[CAPAIAN PEMBELAJARAN]

1. Mahasiswa mampu Jelajahi Situs SANS
2. Mahasiswa mampu Identifikasi Ancaman Keamanan Jaringan Terbaru
3. Mahasiswa mampu Merinci Ancaman Keamanan Jaringan Tertentu

[PEMBAHASAN]

Untuk mempertahankan jaringan dari serangan, administrator harus mengidentifikasi ancaman eksternal yang menimbulkan bahaya bagi jaringan. Situs web keamanan dapat digunakan untuk mengidentifikasi ancaman yang muncul dan memberikan opsi mitigasi untuk mempertahankan jaringan.

Salah satu situs paling populer dan tepercaya untuk bertahan dari ancaman keamanan komputer dan jaringan adalah SysAdmin, Audit, Jaringan, Keamanan (SANS). Situs SANS menyediakan banyak sumber daya, termasuk daftar 20 Kontrol Keamanan Kritis teratas untuk Pertahanan Cyber Efektif dan mingguan @Risk: Buletin Peringatan Keamanan Konsensus. Buletin ini merinci serangan dan kerentanan jaringan baru.

Di lab ini, Anda akan membuka dan menjelajahi situs SANS, menggunakan situs SANS untuk mengidentifikasi ancaman keamanan jaringan baru-baru ini, meneliti situs web lain yang mengidentifikasi ancaman, serta meneliti dan menyajikan detail tentang serangan jaringan tertentu.

Bagian 1: Menjelajahi Situs SANS

Di Bagian 1, navigasikan ke situs web SANS dan jelajahi sumber daya yang tersedia.

Langkah 1: Temukan sumber daya SANS.

Arahkan ke www.SANS.org. Dari halaman beranda, sorot menu Sumber Daya. Buat daftar tiga sumber daya yang tersedia.

Langkah 2: Temukan tautan ke Kontrol Keamanan Kritis.

Kontrol Keamanan Kritis yang tercantum di situs web SANS adalah puncak dari kemitraan publik-swasta yang melibatkan Departemen Pertahanan (DoD), Asosiasi Keamanan Nasional, Pusat Keamanan Internet (CIS), dan Institut SANS. Daftar tersebut dikembangkan untuk memprioritaskan kontrol keamanan siber dan pengeluaran untuk DoD. Itu telah menjadi inti dari program keamanan yang efektif bagi pemerintah Amerika Serikat. Dari menu Resources, pilih Critical Security Controls, atau serupa.

Langkah 3: Temukan menu Nawala.

Sorot menu Resources, pilih Newsletters. Jelaskan secara singkat masing-masing dari tiga buletin yang tersedia.

Bagian 2: Identifikasi Ancaman Keamanan Jaringan Terbaru

Di Bagian 2, Anda akan meneliti ancaman keamanan jaringan baru-baru ini menggunakan situs SANS dan mengidentifikasi situs lain yang berisi informasi ancaman keamanan.

Langkah 1: Temukan @Risk: Arsip Buletin Peringatan Keamanan Konsensus.

Dari halaman Nawala, pilih Arsipkan untuk @RISK: Peringatan Keamanan Konsensus. Gulir ke bawah ke Volume Arsip dan pilih buletin mingguan terbaru. Tinjau bagian Masalah Keamanan Terbaru yang Terkemuka dan File Malware Paling Populer. Buat daftar beberapa serangan baru-baru ini. Jelajahi beberapa buletin terbaru, jika perlu.

Langkah 2: Identifikasi situs yang menyediakan informasi ancaman keamanan terkini.

Selain situs SANS, identifikasi beberapa situs web lain yang menyediakan informasi ancaman keamanan terkini.

Bagian 3: Merinci Serangan Keamanan Jaringan Tertentu

Di Bagian 3, Anda akan meneliti serangan jaringan tertentu yang telah terjadi dan membuat presentasi berdasarkan temuan Anda. Lengkapi formulir di bawah ini berdasarkan temuan Anda.

Langkah 1: Lengkapi formulir berikut untuk serangan jaringan yang dipilih.

Langkah 2: Ikuti panduan instruktur untuk menyelesaikan presentasi.

[TUGAS PRAKTIKUM]

Buat laporan resmi dengan melakukan capture hasil pekerjaan anda dengan analisis yang benar menggunakan simulasi Packet Tracer.

Selamat Datang **MARTI WIDYA SARI [0527037901],** **Dosen** **Log Out**

NILAI AKHIR

ISIAN HASIL STUDI MAHASISWA

NO	NIM	MAHASISWA	NILAI
1	22111100010	AHMAD FAUZIL ADHIM	E
2	22111100013	ARYA NANDA EKA PUTRA	A-
3	22111100019	MARSELUS BUNAI	A-
4	22111100034	ERIKA AMALIA	A
5	22111100036	DWI ENDAH WAHYUNI	A
6	22111100053	MARTINUS MOMOT	A-
7	22111100060	LIO XLANDO R	B

Batal Simpan