MODUL MATA KULIAH

JARINGAN KOMPUTER

KP041/KP371 - 3 SKS

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR

TIM PENYUSUN

Joko Christian Chandra, M.Kom
Reva Ragam Santika, M.Kom

JAKARTA
JUNI 2020

UNIVERSITAS BUDI LUHUR
FAKULTAS TEKNOLOGI INFORMASI

MODUL PERKULIAHAN #13

JARINGAN KOMPUTER

Capaian Pembelajaran	:	Mahasiswa memahami dan menjelaskan peran dari protokol-protokol pada Application Layer
Sub Pokok Bahasan	:	1. Cara kerja DNS 2. DNS Hierarchy 3. Command Nslookup 4. Cara kerja DHCP 5. Cara kerja FTP 6. Cara kerja Server Message Box 7. Getting the data to end devices
Daftar Pustaka	:	1. Cisco Networking Academy Curriculum. (2017). CCNA Routing and Switching version 6 – Introduction To Network. Available at : https://www.netacad.com/ [Accessed 10 Feb 2019]. 2. IBM Think Academy.(2015). How It Works: Internet of Things [online]. Available at : https://www.youtube.com/watch?v=QSIPNhOiMoE [Accessed 10 Jan 2017]. 3. Hariharan. (2016). Internet of Things (IoT) Architecture for Beginners [online]. Available at :

https://www.youtube.com/watch?v=EcWhxb77Gug&t=9s [Accessed 10 Jan 2017].

4. Flanagan, Kelly. (2014). Life Simplified with connected devices [online]. Available at : https://www.youtube.com/watch?v=NjYTzvAVozo&t=7s [Accessed 26 Oct 2016]
5. Cisco.(2013).Cisco Telepresence Vision [online]. Available at : https://www.youtube.com/watch?v=NkW0hHlO7Jk [Accessed 23 Oct 2016]
6. Qualcomm.(2015). Jason Silva Says Why Wait for the Internet of Everything [online]. Available at : https://www.youtube.com/watch?v=ZLqXtwl_-YY [Accessed 17 Jan 2017]
7. SalesForce(2009). What is Cloud Computing? [online]. Available at: https://www.youtube.com/watch?v=ae_DKNwK_ms [Accessed 17 Jan 2017].
8. Rackspace.(2012). Understanding the Cloud Computing Stack: SaaS, PaaS and IaaS | CloudU [online]. Available at : https://www.youtube.com/watch?v=RN5sg5Lnyy8 [Accessed 17 Jan 2017].
9. Messer.(2012). Understanding Unicast, Multicast, and Broadcast - CompTIA Network+ N10-005: 1.3 [online]. Available at: https://www.youtube.com/watch?v=Z6O__3UEltE [Accessed 23 Mar 2014].
10. IEEEISTTV. (2012). What is IEEE? IEEE Day 2012 Edition [online]. Available at : https://www.youtube.com/watch?v=fcmCpEpg0lQ [Accessed 23 Mar 2014].
11. IETF - Internet Engineering Task Force. (2013).

Introducing the Internet Engineering Task Force (IETF) - Making The Internet Work Better [online]. Available at: https://www.youtube.com/watch?v=Fpuzl9lvOSM [Accessed 23 Mar 2014].

12. Sharma, Dinesh (2011). Understanding IP Address and Subnet Mask (A Historical Perspective) [online]. Available at : http://www.dscentral.in/2011/07/14/understanding-ip-address-and-subnet-mask/ [Accessed 17 March 2017]

13 PROTOKOL TRANSPORT LAYER

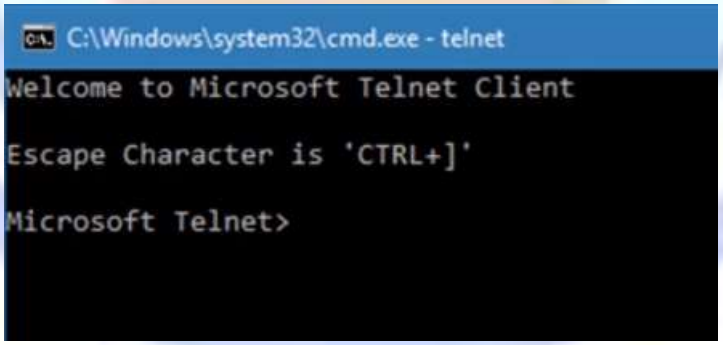
Melanjutkan dari pembahasan bab sebelumnya, pada bab ini akan dibahas protokol:

1. Teletype network (Telnet)
2. Domain Name System (DNS)
3. Dynamic Host Configuration Protocol (DHCP)
4. File Transfer Protocol (FTP)

13.1 TELNET

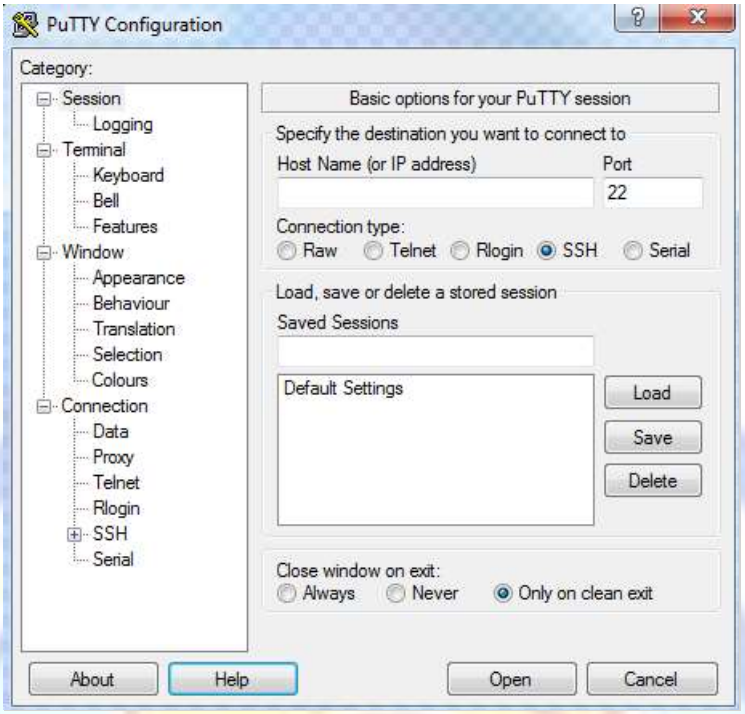
Telnet adalah protokol aplikasi yang memfasilitasi komunikasi dua arah menggunakan koneksi virtual terminal. Dikembangkan di tahun 1969 (RFC15) hingga perbaikan terakhir tahun 1983 (RFC855[1]), telnet digunakan untuk melakukan remote command-line interface. Telnet mengirimkan data menggunakan protokol TCP pada layer 4 dan tidak menggunakan kriptografi (tidak aman).

Telnet tersedia secara umum pada semua platform komputer, dari PC hingga smartphone, bahkan operator radio amatir. Istilah Telnet juga mengacu pada software yang mengimplementasikan sisi client dari protokol tersebut seperti pada Gambar 13.1 yang merupakan versi console dari sistem operasi. Selain tersedia langsung, juga banyak terdapat alternatif lain seperti PuTTY yang mendukung multi protokol pada Gambar 13.2.



Gambar 13.1 Tampilan layar client telnet pada console Windows

[1] https://tools.ietf.org/html/rfc855

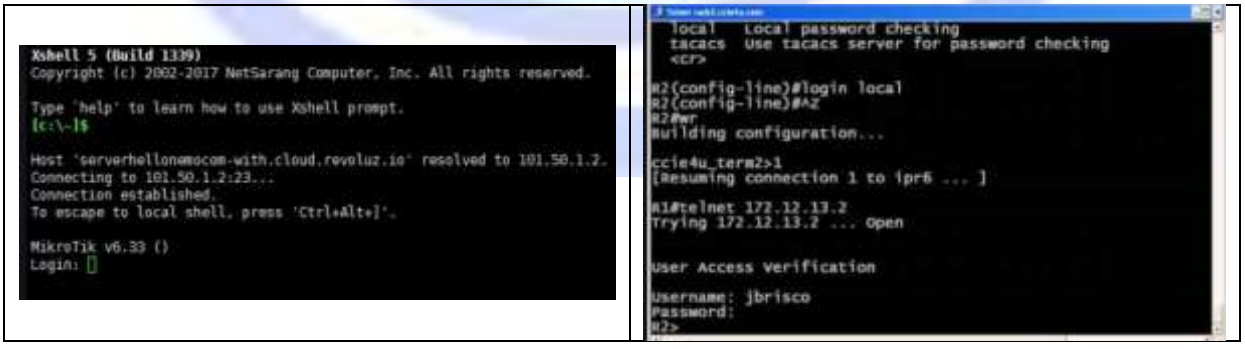


Gambar 13.2 Tampilan konfigurasi PuTTY

Protokol Telnet menggunakan port 23 (tapi bisa diganti oleh server), dan telnet client bisa dengan mudah digunakan untuk melakukan cek apakah sebuah port terbuka. Sebagai contoh, dengan telnet client, kita bisa cek apakah port 80 pada sebuah host aktif menerima koneksi.

13.1.1 Pemanfaatan Telnet

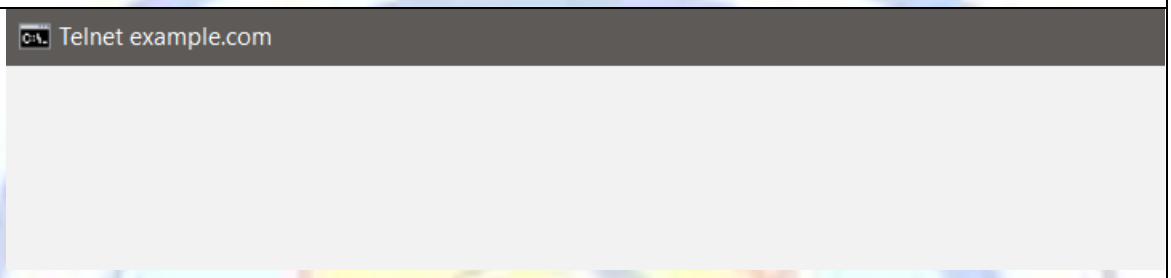
Telnet utamanya digunakan untuk remote connection. Sehingga user tidak perlu secara fisik berada di dekat host yang sedang di kontrol. Tool ini sangat berguna untuk network administrator untuk mengontrol perangkat yang berbeda melalui terminal fisik tunggal. Pada Gambar 13.3 menunjukkan contoh akses remote ke perangkat jaringan.



Gambar 13.3 Telnet ke perangkat jaringan

Pada Gambar 13.4 adalah contoh cara melakukan cek sebuah port. Pada baris 1 adalah perintah untuk membuka koneksi telnet ke server example.com (sebuah nama domain valid yang memang diijinkan untuk uji coba) pada port 80. Jika port tersebut aktif dan menerima koneksi, maka layar telnet akan menjadi kosong (lihat baris 2). Sedangkan saat mencoba mengakses port 81 pada domain example.com mengembalikan gagal (lihat baris 3) yang berarti port tersebut tertutup atau tidak dapat melayani.

1.
```
C:\Users\chris>telnet example.com 80
```

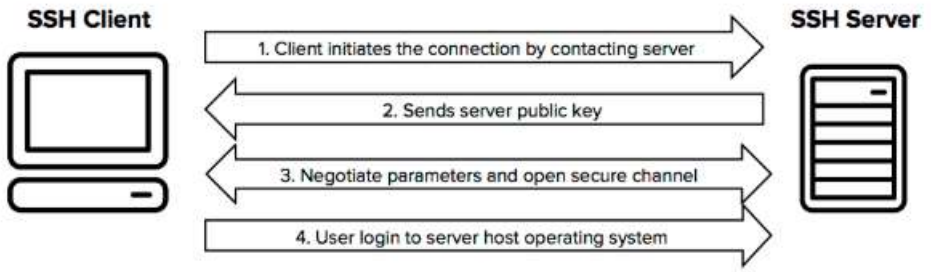
2.


3.
```
C:\Users\chris>telnet example.com 81
Connecting To example.com...Could not open connection to the host, on
port 81: Connect failed
```

Gambar 13.4 Menggunakan telnet client untuk cek port

13.1.2 Evolusi Telnet : SSH

Karena sifat Telnet yang tidak aman, maka pada tahun 1995 dikembangkan masih protokol Secure Shell (SSH) dengan standar terakhir disempurnakan pada tahun 2006 (RFC4250[2]). SSH menggunakan kriptografi dan sesi negosiasi dilakukan sebelum login dapat dilakukan. SSH juga menggunakan TCP pada layer 4 dengan nomor port default 22



Gambar 13.5 Kerangka kerja buka koneksi SSH

[2] https://tools.ietf.org/html/rfc4250

Saat ini yang disarankan adalah menggunakan SSH ketimbang telnet. Dan protokol SSH sendiri sudah menjadi standar de-facto di dunia jaringan komputer. Semua admin jaringan menggunakannya. SSH bahkan diturunkan menjadi protokol seperti SSH File Transfer Protocol (SFTP), yang akan dibahas di sub bab berbeda.

13.1.3 Tentang GUI remote connection

Saat ini untuk melakukan Graphical User Interface remote connection (ada grafisnya) dapat menggunakan protokol /aplikasi berikut (propietary + open):

1. Virtual Network Computing (VNC)
2. Xwindow Protocol
3. Google Web toolkit (salah satu komponennya)
4. MozillaXul
5. JavaApplet
6. Remote Desktop Protocol (RDP- oleh Microsoft)
7. Team Viewer (kombinasi banyak protokol)

GUI remote connection sangat berguna untuk melakukan akses GUI sebuah host dari jarak jauh, sehingga tetap dapat menggunakan antar muka yang nyaman (tidak text based seperti pada telnet dan SSH) meskipun tidak secara fisik ada di dekat host yang di-remote. Selain untuk bekerja, GUI remote connection juga memudahkan proses troubleshooting dan dapat digunakan untuk transfer file.

13.2 Domain Name

Manusia pada dasarnya tidak mudah mengingat angka. Coba sebutkan nomor induk kependudukan (NIK) Anda, apakah hafal? (9 dari 10 orang tidak hafal). Sedangkan pengalamatan IP yang digunakan sebagai identifier unik sebuah host dalam jaringan internet menggunakan angka (sesungguhnya malah angka biner 101011010 ... hingga 32 digit panjangnya, pada IPv6 malah jadi 128 digit). Jadi diperlukan sebuah metode untuk memudahkan manusia mengingat identifier tersebut, lahirlah ... DNS.

DNS pada dasarnya hanya membuat catatan mengenai nama Domain (nama yang mudah manusia ingat seperti budiluhur.ac.id) dan hubungannya dengan identifier resmi pada konektivitas jaringan internet (IPv4 atau IPv6). Server DNS

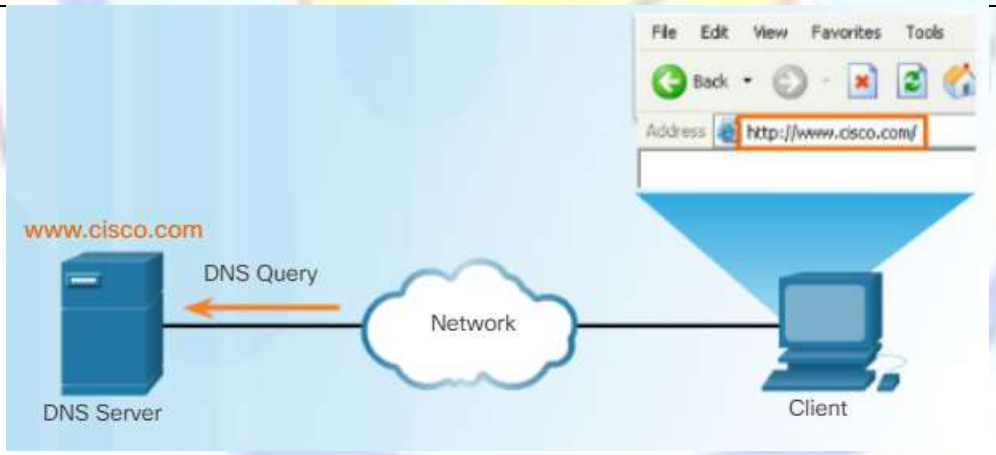
berfungsi untuk melakukan tugas resolve (memberikan jawaban dari sebuah pertanyaan) agar protokol IP pada perangkat anda bisa membuat paket IP kepada server tujuan. Jadi setiap kali anda mengakses sebuah alamat domain (baik melalui web, email, ftp, atau layanan lain), sebenarnya perangkat anda akan mencari dahulu alamat IP nya. Baru bisa membuat paket datanya (layer 3).

13.2.1 Pola kerja DNS

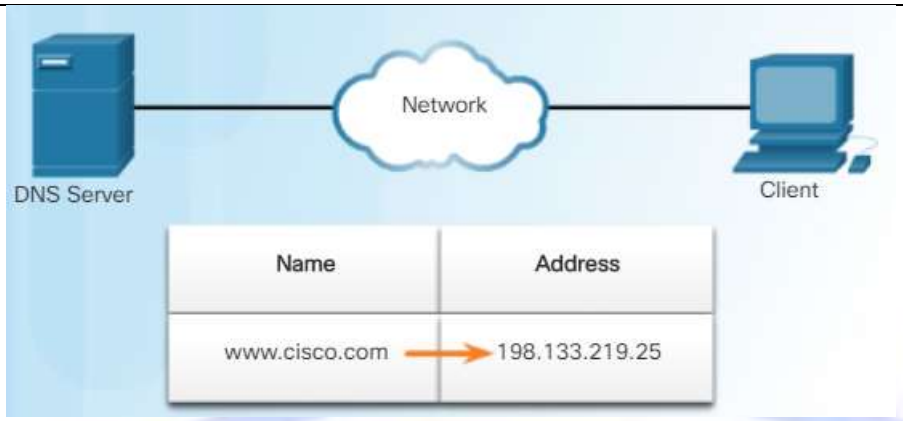
Ilustrasi pada Gambar 13.6 menunjukkan komunikasi antara client dan DNS server saat client mau membuka halaman web pada domain cisco.com:

1. 

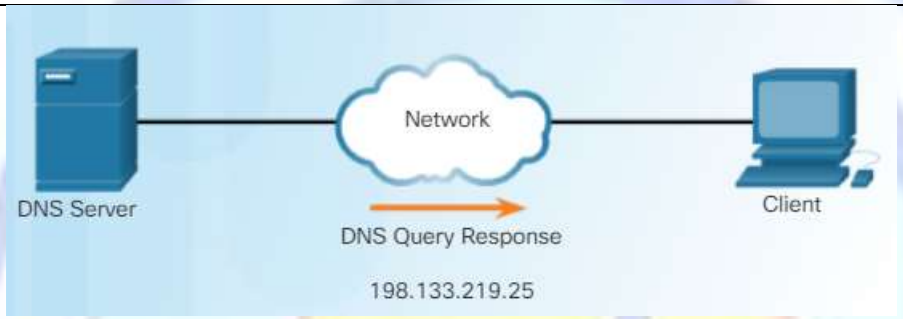
Client menerima input dari user untuk membuka halaman web www.cisco.com

2. 

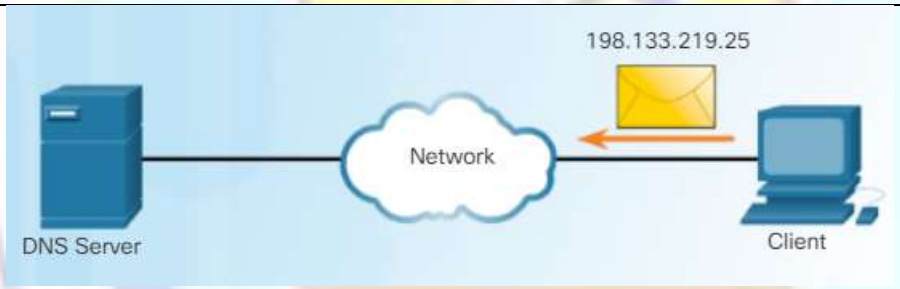
Client mengirimkan permintaan DNS Query ke server DNS

3. 

Server DNS melakukan resolve nama domain

4. 

Server DNS mengirimkan jawaban ke Client

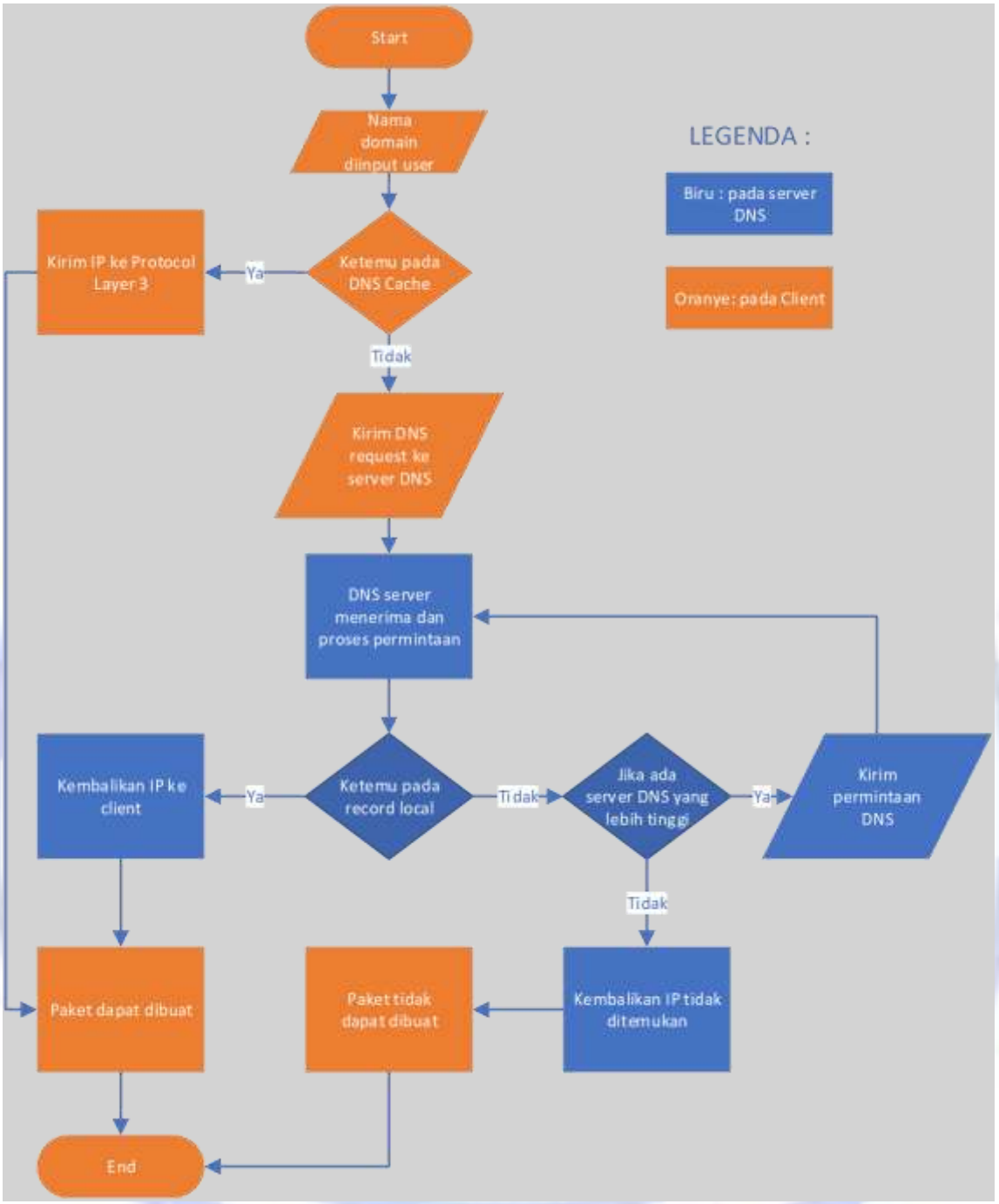
5. 

Client dapat membuat paket ke server cisco dan mengirimkannya.

Gambar 13.6 Kumpulan ilustrasi proses resolve DNS

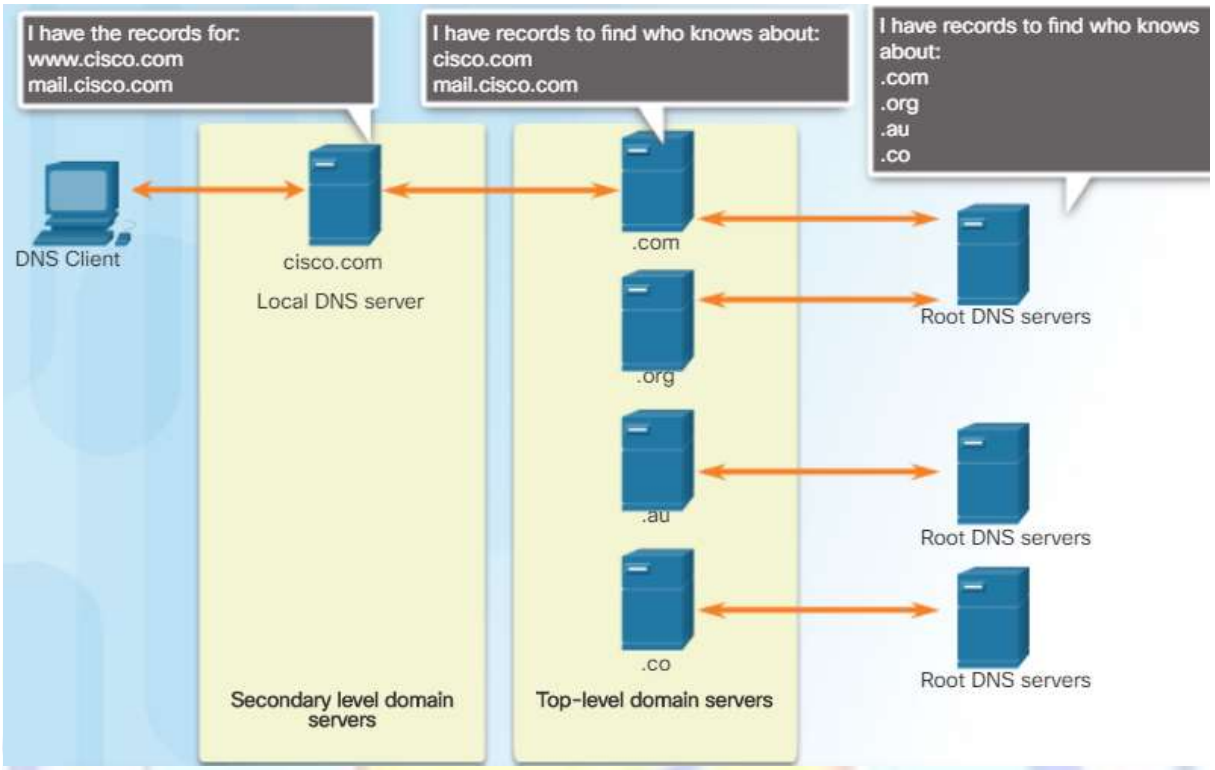
Saat Client melakukan query, server DNS akan memproses pertanyaan tersebut dan mencari ke record internal. Jika tidak ditemukan maka akan ditanyakan ke server yang lebih tinggi (dapat berjenjang).

Umumnya jawaban dari server yang lebih tinggi yang didapat akan disimpan (durasi tergantung konfigurasi masing masing server) untuk menjawab query yang sama di masa mendatang.



Gambar 13.7 Ilustrasi sederhana proses kerja DNS

Ilustrasi hubungan kerja antara server DNS dapat dilihat pada Gambar 13.8.



Gambar 13.8 Ilustrasi kerja antar server DNS

DNS server menyimpan berbagai jenis informasi untuk melakukan resolusi nama. Record ini mencakup nama, alamat, dan tipe record, sebagian tipenya adalah:

1. A => alamat IPv4 perangkat
2. AAAA => alamat IPv6 perangkat (disebut quad A)
3. NS => Authoritative name server
4. MX => Mail exchange record

13.2.2 Format pesan DNS

DNS menggunakan TCP dan UDP pada port 53, permintaan client ke server umumnya menggunakan UDP, sehingga format pesan yang kecil dan sederhana dibutuhkan.

Format pesan DNS sama untuk semua tipe query client dan server, semua tipe error, dan semua transfer informasi antar server disusun dalam struktur yang sama (baik saat dikirim oleh client, maupun balasan dari server) dengan struktur berikut:

Header	Informasi header DNS
Question	Pertanyaan kepada name server

Answer	Jawaban dari pertanyaan
Authority	Informasi siapa yang bertanggung jawab
Additional	Informasi tambahan

13.2.3 Aplikasi dan Tool DNS

Aplikasi DNS server de-facto saat ini adalah BIND versi 9 pada tahun 2000 (versi 10 belum diterima penuh public dan menjadi projek open source). BIND dikembangkan di University of California di Berkeley tahun 1980 an.

Beberapa perintah yang terkait dengan layanan DNS:

1. (Windows) informasi DNS dapat ditampilkan dengan perintah : `ipconfig /displaydns`
2. (Windows) menghapus catatan DNS cache dapat dilakukan dengan perintah : `ipconfig /flushdns`
3. (Windows) melakukan pertanyaan DNS ke server : `nslookup {nama domain}`
4. (Linux) melakukan pertanyaan DNS ke server : `dig {nama domain}`
5. Pada linux tidak ada proses DNS caching di level OS, kecuali caching service diisntall 9Systemd-Resolved, DNS Masq, atau NSCD), sehingga perintah untuk melihat dan menghapus DNS cache sangat bervariasi tergantung distro linux dan service yang digunakan. Misalnya pada distro Debian dengan NSCD : "`sudo service nscd status`"
6. Pada Machintos, perintah manipulasi DNS pada client sangat bervariasi dari satu versi OS ke yang lainnya. Contoh : OS X Yosemite menggunakan "`sudo discoveryutil mdnsflushcache`" sedangkan di OS X mavericks, Mountain Lion dan Lion menggunakan "`sudo killall -HUP mDNSResponder`".

13.2.4 Pengayaan

Pada OS windows, proses resolve nama domain dilakukan pertama kali bukan melalui server DNS, melainkan pada file

`C:\Windows\System32\drivers\etc\hosts`

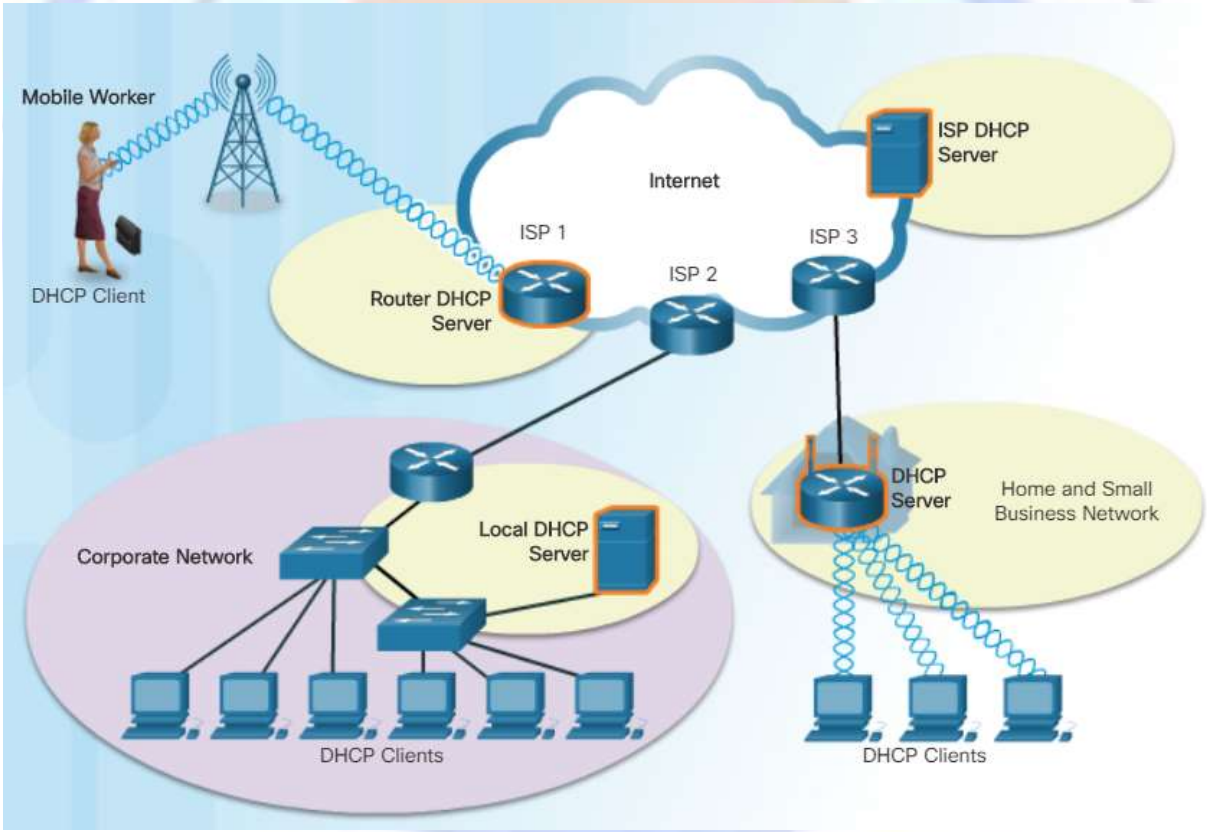
Jika tidak ditemukan pada file tersebut, barulah dicari di DNS cache, dan bila tidak ditemukan baru ditanyakan kepada server DNS.

Bentuk layanan DNS lain yang juga dapat berupa DNS terenkripsi (sedang diupayakan oleh komunitas penggiat anonimitas dan keamanan data agar menjadi standar yang digunakan), yang mencegah DNS spoofing. silahkan mencari tahu sendiri tentang DNSCrypt.

13.3 Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Confirmation protocol memungkinkan perangkat mendapatkan IP address dan informasi lain secara otomatis dari DHCP server. Service ini mengatur pemberian IP, subnet mask, gateway dan parameter lain.

Sifat DHCP merupakan lease (penyewaan) dan tidak bersifat tetap, sehingga hanya cocok untuk client, karena sebuah server harus memiliki ip static. DHCP bekerja dengan protokol TCP dan port 67. Gambar 13.9 Menunjukkan ilustrasi penggunaan DHCP pada jaringan.



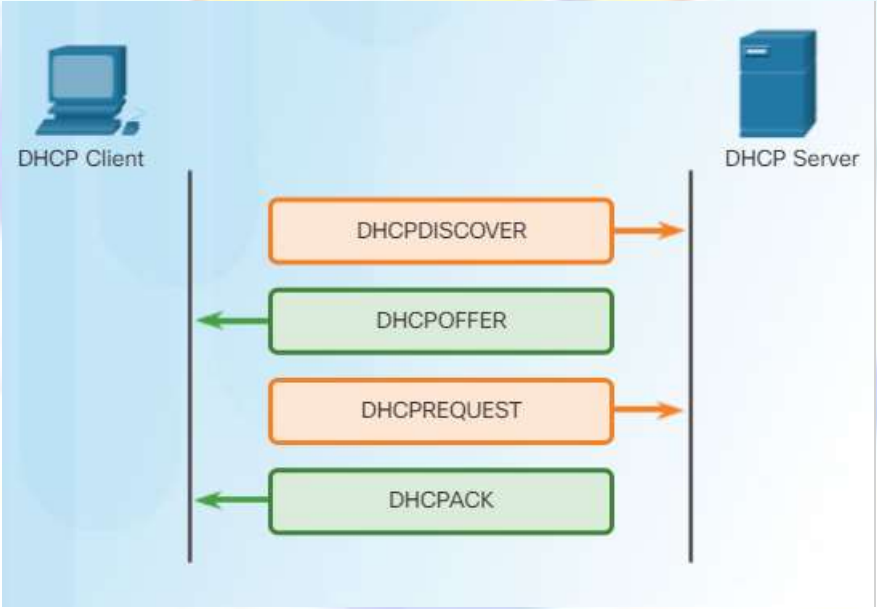
Gambar 13.9 Ilustrasi penggunaan DHCP dalam jaringan

13.3.1 Cara kerja DHCP

Saat sebuah perangkat ingin terhubung ke jaringan, dari sudut pandang layer 3 harus mendapatkan identifier khusus (alamat IP), sehingga perangkat tersebut akan menyewa IP dari DHCP server. Server DHCP harus menjamin bahwa IP yang disewakan bersifat unik, dan administrator dapat mengubah range IP address yang

akan disewakan ke client. Umumnya ISP menggunakan DHCP untuk mengalokasikan alamat IP bagi pengguna layanannya (termasuk layanan seperti indihome dan first media) .Berikut adalah detil prosesnya:

1. Client yang terhubung jaringan akan mengirimkan paket DHCP DISCOVER (secara broadcast) untuk mendapat perhatian DHCP server.
2. Server DHCP membalas dengan DHCP OFFER, yaitu sebuah pesan penawaran dengan ip address, dns, gateway, dan lama lease.
3. Client akan broadcast pesan DHCP REQUEST packet yang mengidentifikasikan server mana (jika lebih dari satu server DHCP yang menawarkan) dan lease mana yang diterima.
4. Server akan mengirim DHCP ACK yang menandakan persetujuan.
5. Jika masa sewa telah habis, atau sebab lain ip tidak dapat digunakan, server akan mengirim DHCP NAK message (Negative Acknowledgement). Dan proses pendapatan ip diulangi dari DHCP DISCOVER.
6. Untuk pembaruan dari ip yang hampir habis masa lease nya, client mengirim DHCP REQUEST.



Gambar 13.10 Ilustrasi proses penyewaan IP dengan DHCP

Untuk dicatat bahwa "Client" tidak harus selalu sebuah end device (komputer, smartphone, smartTV, dll), tetapi juga dapat berupa perangkat intermediate seperti Router access point yang kemudian memiliki DHCP server sendiri untuk memberikan sewa ke perangkat wireless (Sebagai client DHCP untuk media kabel, sebagai server

DHCP untuk media nirkabel, atau media sebaliknya, atau kedua media kabel, atau kedua media nirkabel).

13.3.2 Pengayaan : DHCP v6

Pada jaringan dengan IPv6, dapat digunakan DHCPv6 , namun penggunaannya sangat ditentukan oleh konfigurasi pada Router IPv6 yang mengirimkan RA (agar lebih jelas baca bab terkait IPv6). Selain model pesan diatas, DHCPv6 juga mendukung tambahan SOLICIT, ADVERTISE, INFORMATION REQUEST, dan REPLY. Detil operasinya tidak dibahas disini karena diluar dari ruang lingkup kurikulum, jika anda tertarik dapat membaca disini[3].

13.3.3 Pengayaan: Keamanan terkait layanan DHCP

Pengguna layanan jaringan dapat "ditipu" oleh server DHCP gadungan. Hal ini bisa terjadi karena client yang "meminta dan mempercayai tawaran" dari sebuah DHCP server. Keamanan yang paling ideal tentunya mensyaratkan semua client memasukkan IP secara manual, namun ini tidak dapat dilakukan khususnya pada jaringan wireless, dan menuntut user client mengetahui dasar konfigurasi jaringan (suatu hal yang membuat "alergi" banyak pengguna awam). Salah satu cara cukup efektif dalam mencegah keberadaan server DHCP "gadungan" pada jaringan wired adalah mengatur port security pada manageable switch, sehingga hanya port tertentu yang diijinkan mengirimkan paket DHCP OFFER.

Pengamanan pada jaringan wireless lebih sulit, karena penyerang biasanya menyiapkan access point gadungan sekaligus dengan DHCP server gadungannya. Sehingga pertahanan terbaik adalah edukasi user untuk selalu berhati-hati saat menghubungkannya pada sebuah jaringan wireless (khususnya yang "gratis").

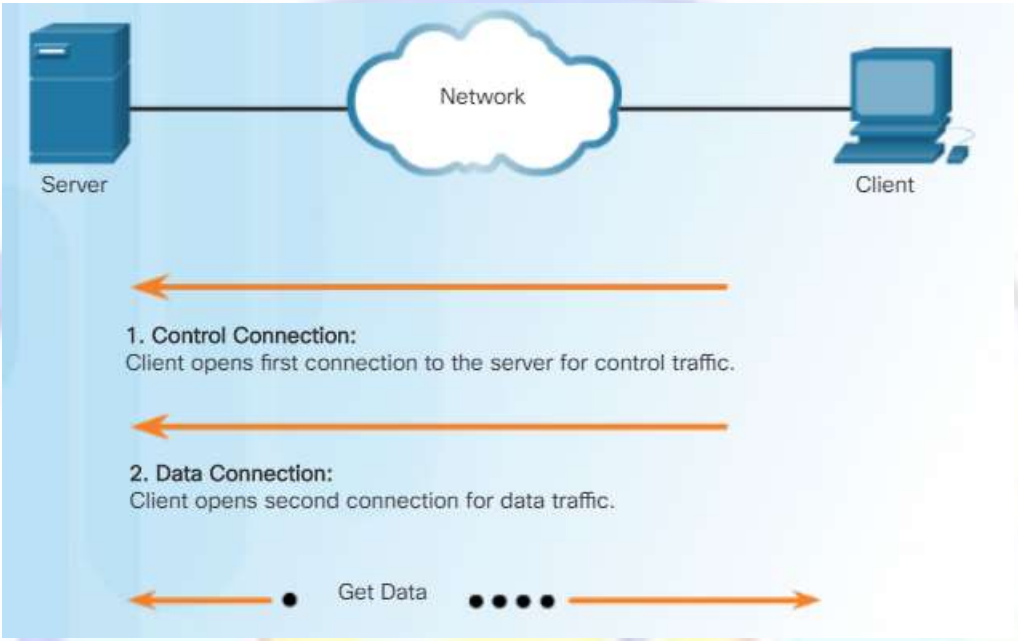
13.4 File Transfer Protocol (FTP)

File Transpor Protokol) digunakan untuk transfer file. Protokol ini di standarkan pada RFC 959 tahun 1985 dan merupakan salah satu protokol "tua" yang masih banyak digunakan saat ini. Mendapatkan update di tahun 1998 untuk mendukung IPv6.

[3] https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/whitepaper_c11-689821.html

13.4.1 Bagaimana FTP bekerja

Client akan membuka koneksi pertama dengan server pada port TCP 21. yang selanjutnya digunakan untuk mengontrol traffic. Selanjutnya dibuka koneksi kedua pada port TCP 20 (jenis koneksi Active) atau nomor port yang lain (jenis koneksi Passive) yang berfungsi sebagai jalur pengiriman data, dan dibuka setiap kali ada file yang ditransfer.



Gambar 13.11 Ilustrasi kerja protokol FTP

Pengiriman data melalui FTP dapat menggunakan salah satu dari 4 bentuk representasi berikut:

1. ASCII cocok untuk teks, representasi karakter akan dikonversi (jika dibutuhkan) dari format mesin pengirim ke representasi 8 bit ASCII, untuk kemudian dikonversi lagi (jika dibutuhkan) ke representasi karakter mesin penerima. Perlu diingat bahwa tidak setiap OS menggunakan representasi karakter yang sama (contoh termudah adalah file text dibuat Windows tidak sama persis dengan file text yang dibuat di Linux).
2. Image mode (atau Binary), data dikirimkan byte -by -byte. Sehingga clone persis didapatkan, ini adalah metode yang disarankan.
3. EBCDIC untuk antar host dengan EBCDIC character set
4. Local mode, untuk dua host dengan konfirurasi identik mengirimkan data dalam format propietary.

FTP mendukung otentikasi dengan login dan password (jika diaktifkan), sedangkan saudara terdekatnya: TFTP (Trivial File Transfer Protocol) pada RFC 1350 tidak mendukung keamanan. TFTP menggunakan protokol UDP pada layer 4 nya, dan digunakan utamanya untuk meletakkan file ke remote host atau booting dari LAN.

Untuk menggunakan layanan FTP, diperlukan FTP server dan FTP client. Berikut adalah contoh dari aplikasi yang dimaksud.

Tabel 13.1 Daftar aplikasi untuk FTP

	GUI	**CLI**
SERVER	1. FileZilla Server 2. Cerberus FTP server 3. Microsoft IIS versi >=7 4. Crush FTP Server 5. NAS lite	1. ProFTPD 2. Crush FTP Server 3. vsftpd
CLIENT	1. FileZilla 2. WinSCP 3. Firefox 4. CoreFTP 5. CuteFTP 6. FTP Commander	1. Windows command prompt 2. Curlftpfs 3. Lftp

13.4.2 FTP yang lebih aman

Karena FTP standar tidak menggunakan kriptografi, maka tidak ada pengamanan dari data yang dikirimkan. Hacker yang berhasil "menyadap" lalu lintas FTP dapat melihat dengan jelas seluruh data yang lewat (termasuk username dan password). Juga rentan terhadap serangan bentuk lain. Sehingga disarankan untuk menggunakan alternatif berikut:

1. FTPS (FTP Secure atau FTP-SSL) yang menambahkan fungsi kriptografi Transport Layer Security (TLS).

2. SFTP[4] (Secure Shell File Transfer Protocol), yang merupakan ekstensi dari protokol SSH. Pada protokol ini, lalu lintas FTP di kirim melalui kanal SSH, sehingga memanfaatkan fungsi kriptografi SSH.
3. Menggunakan FTP dibalik VPN yang aman, sehingga memanfaatkan fitur keamanan yang digunakan pada VPN tersebut.

13.5 Assessment

Kerjakan soal-soal berikut ini:

1. Jelaskan contoh pemanfaatan dari protokol Telnet dan SSH!
2. Mengapa protokol SSH lebih disarankan dibandingkan protokol Telnet? Jelaskan!
3. Mengapa perlu ada layanan DNS?
4. Apa perintah yang harus diketikkan pada console OS windows untuk mencari tahu alamat IP dari domain "example.com" ?
5. Dapatkan kita mengakses sebuah layanan web tanpa menggunakan nama domain? Misalnya https://{alamat ip publik disini}.
6. Berdasarkan soal sebelumnya, uji cobakan langsung pada browser anda (berkoneksi internet) dengan 5 alamat IP publik dari domain kesukaan kalian (jika perlu,cari tahu dulu IP publiknya dengan perintah pencarian). Apakah seluruhnya dapat diakses langsung dengan IP publik? Diskusikan dengan teman anda dan cari tahu kenapa.
7. Proses mendapatkan IP dari DHCP memerlukan beberapa langkah. Jelaskan!
8. Dapatkah sebuah laptop terhubung ke jaringan wireless yang tidak ada layanan DHCP nya? Jelaskan !
9. Berapa port yang dibuka pada FTP standar? Dan apa saja fungsinya?
10. Cari informasi lebih mendalam terkait bagaimana FTPS bekerja, buatlah bagan/ ilustrasi yang menjelaskan proses buka koneksi hingga data dapat dikirim!

[4] Sesungguhnya ada SFTP yang lain :simple FTP (tidak aman), pada RFC 913 yang sudah jarang digunakan.

FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS BUDI LUHUR
Jl. Raya Ciledug, Petukangan Utara, Pesanggrahan
Jakarta Selatan, 12260
Telp: 021-5853753 Fax : 021-5853752
http://fti.budiluhur.ac.id