Network Services, VU – Part 1

Outline

Administrative Protocols & Services

Overview / 1

- Administrative Services
  - Remote Login Facilities (RLogin, TELNET, SSH)
  - Tools (Traceroute, Ping)
  - DNS and Name Servers, ARP/RARP
  - DHCP
  - LDAP
- Basic Services
  - FTP, Usenet News (NNTP)
  - EMail (SMTP,POP3,IMAP), Spam, Phishing
  - WWW (HTTP)
  - WebDAV

Overview / 2

- HTML & XML Techologies
  - HTML, XHTML, XML, XML Schema, XPath, XQuery, XLink, XSL, CSS, JavaScript, ...
- WWW Technologies
  - Indexing (Glimpse, Harvest, Robots)
  - Dynamic Web Technologies
    - CGI, PHP, ASP, ASP.NET, Servlets, JSP, JSF,
  - Software Architectures
  - Server Configuration

Overview / 3

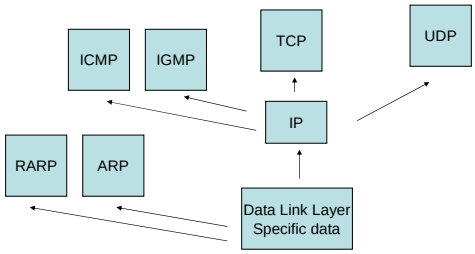
- Web services
  - Basic concepts, languages
  - SOAP, ...
- Security
  - PGP, SSL, Certificates

Prerequisites

- Basic knowledge of TCP / UDP
  - Distributed Systems (Verteilte Systeme)

Repetition – TCP/IP

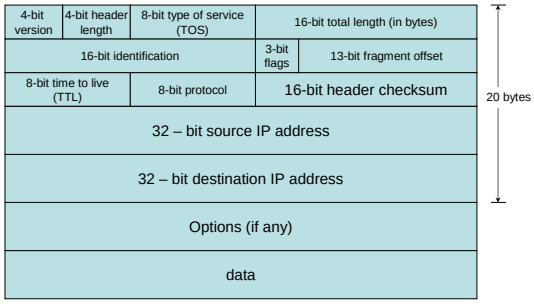
- Internet protocol layering



Repetition – TCP/IP

- Data Link Layer
  - Eg. Ethernet
  - Data Transfer within one network (adressing)
- IP
  - Connection-less protocol
  - IP Header (20-60 bytes)
  - Basis of all Internet protocols
  - Eg. Transmitted within Ethernet frames

IP Header - Example



Transmission Control Protocol TCP

- Transmitted within IP frames
- Multiple TCP endpoints – Ports
  - 1-65535
- Connection-oriented
  - Virtual circuit
- Flow control
  - Transmission speed reduction if one side is too slow

User Datagram Protocol

- Transmitted within IP protocols
- Multiple UDP endpoints – Ports
  - 1-65535
- Connection-less
- Only 8 additional bytes to IP header
  - 2 byte source ports
  - 2 byte destination port
  - 2 byte UDP length
  - 2 byte UDP checksum

Internet Control Message Protocol - ICMP

- Transmitted within IP protocols
- Response mechanism
- ICMP error message
  - Types
    - Network unreachable
    - Host unreachable
    - Port unreachable
    - ...
  - Includes original IP header as payload + first 8 byte of payload
- ICMP query messages
    - Echo request
    - Echo reply
    - ...

Internet Group Management Protocol - IGMP

- Transmitted within IP protocols
- Fixed-size
- Multicast facility of the Internet

Lecture Notes

- Slides
- RFCs (Request for Comments)
- W. Richard Stevens: "TCP/Illustrated – Volume 1"
- Aeleen Frisch: "Essential System Administration"

Remote Login Agenda

- Remote Login
- Telnet
- SSH

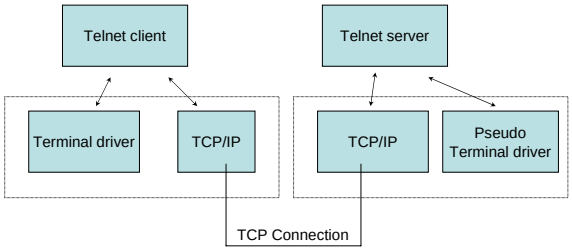
Remote Login

- Main tool for system administrators
- Not necessary to sit in front of the host
- RLogin
  - one of the first remote login tools
  - Clear-text passwords
  - Allows bypassing of passwords
    - Security Problem

Telnet / 1

- Communication between
  - Any host
  - Any terminal
- RFC 854
- Network Virtual Terminal (NVT)
  - Lowest common denominator terminal
  - All Telnet terminals shall conform to NVT
  - Character device with keyboard & printer
- Data sent from keyboard to server
- Data received from server output to printer

Telnet process model



Telnet / 2

- NVT Ascii
  - 7-bit US variant used in most Internet protocols (SMTP, HTTP, FTP, ...)
- 7-bit character sent as 8-bit (high-order bit = 0)
- End-of-line symbol
  - 2-character sequence
    - CR (carriage Return)
    - LF (Linefeed)
  - In C/C#/Java notation: \r\n
- Carriage Return symbol
  - 2-character sequence
    - CR (carriage Return)
    - NUL
  - C/C#/Java notation: \r\0

Telnet / 3

- Commands
  - 0xFF (255) (= Interprete as Command)
  - Command-byte follows

Telnet Command

- Exists on every operating system
  - telnet <host> [<port>] (default port:23)
  - "Internet terminal"
  - Telnet server: telnetd
  - Windows Telnet server: start via Control Panel
- Data sent in the clear
- Passwords in the clear
  - Not widely used extensions/options for encryption
- Importance of Telnet
  - Debugging Tool
  - NVT Ascii used by most Internet protocols

Telnet Example / 1
Remote Login

telnet compaq1.infosys.tuwien.ac.at
Suse Linux release 8.1
Kernel 2.4.2
login: joe
Password:
Last login: Tue Mar 22 ... from dellpc05. ...
-bash-3.00$

Telnet Example / 2
Debug HTTP

```
telnet www.tuwien.ac.at 80
Trying 128.131.172.239...
Connected to pent21.infosys.tuwien.ac.at.
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 18 Mar 2005 15:51:59 GMT
Server: Apache/1.3.26 Ben-SSL/1.48 (Unix) PHP/4.1.0
Last-Modified: Tue, 15 Mar 2005 08:21:32 GMT
ETag: "109eb-1ae2-42369b0c"
Accept-Ranges: bytes
Content-Length: 6882
Connection: close
Content-Type: text/html

<!doctype html public "-//w3c//dtd html 3.2//en">
  <html lang="de">
<head>
<title>TU Wien</title>
<LINK rel="stylesheet" type
="text/css" href="styles/homepage.css">
...
Connection to host lost.
```

Secure Shell (SSH)

- Protocol for secure
  - Remote Login
  - Other secure network services
- Strong encryption
- Server Authentication
- Integrity protection
- May provide compression (zlib, RFC1950/1951)
- Type of service negotiated
  - Key exchange method
  - Public key algorithm
  - Symmetric algorithm
  - Message authentication algorithm
  - Hash algorithm

Secure Shell (SSH)

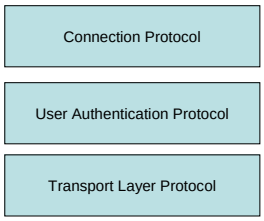
- Standard methods
  - Interactive shell sessions
  - Remote execution of commands
  - Forwarding (tunneling) arbitrary TCP/IP ports
  - X11 connections
- Channel
  - All terminal sessions, forwarded connections, ...

SSH

- 3 Protocols
  - Transport Layer Protocol [SSH-TRANS]
    - Server authentication, Condentiality, and Integrity
    - Runs over TCP/IP - Default port TCP 22
  - User Authentication Protocol
    - Authenticates Client-side user to the server
  - Connection Protocol
    - Multiplexes the encrypted tunnel into several logical channels

SSH Architecture

- Each protocol uses protocol below



SSH

- Host key
  - Each server shall have a host key
  - May have multiple host keys for multiple algorithms
  - Used during key exchange
    - Verifies that client talks to correct server
    - Client must have a priori knowledge of server's host key
    - Verification based on client's database(file) or trust certification authority

SSH Tools

- SSH programs
  - Unix + Cygwin: ssh
  - Putty.exe
  - Server: sshd
  - scp
    - secure copy
      - File transfer tool

Domain Names & DNS -Agenda

- Domain Names (RFC 1034+1035)
- HOSTS.TXT (RFC 952+953) Domain Name Service

Domain Names

- Naming of Resources
- Internet IP based
  - Problems:
    - IP addresses (123.25.33.44) difficult to remember
    - May change
- DNS
  - Name resolution
    - Host name (www.myserver.com) -> IP
  - Back resolution
    - IP -> Host name
  - Additional information about hosts

HOSTS.TXT

- Pre-DNS: HOSTS.TXT
  - /etc/hosts
  - Original facility
- Stores address mappings
  - IP to Domain
- Disadvantage:
  - Load on central server
  - Bandwidth for distribution proportional to (number of hosts)*(number of hosts)
  - Name clashes

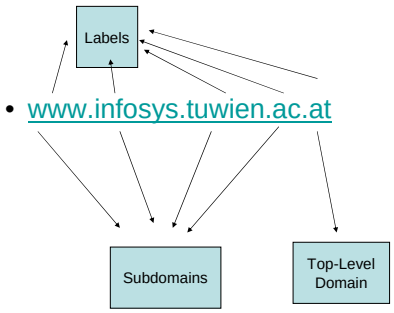
DNS / 1

- Domain Name Service
- Primary Goals
  - Consistent name space
  - Distributed by design
    - Multiple servers
    - Hierarchically, organizations may maintain their own servers
  - Names shall be used to get
    - Host addresses
    - Mailbox Data
    - Other, yet undefined information
  - Access to data critical
  - Instantaneous updates less important

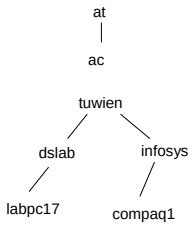
DNS - Elements

- Domain Name Space & Resource Records
  - Specification for a name space
  - Structured as a tree
    - Each node and leaf corresponds to a resource set
  - Query Operations attempt to extract specific types of information
- Name Servers
  - Hold information about the domain tree's structure
  - May cache any information of the whole domain tree
  - In general holds information about a subset
    - Name server is an AUTHORIY for this subset
  - Authoritative information organized as
    - ZONES
- Resolvers
  - Programs that extract information from Name Servers

Domain Name

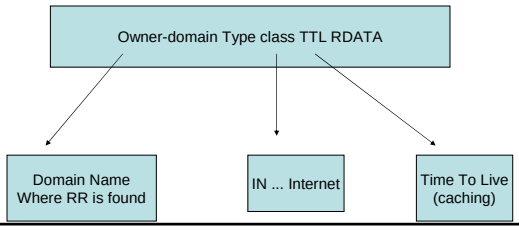


Domain Name



DNS Resource Records

- Resource Record (RR)
  - Stored in DNS/Name Servers
- Syntax



Resource Records / 1

Type	RData	Description	Example
A	32 bit IP address (IPv4)	Allows IP Resolution	IN A labpc17 IN A 128.131.172.175
CNAME	Domain name	Additional alias names	CNAME mail CNAME pent789. tuwien.ac.at
HINFO		Identifies CPU and OS used by host	HINFO "Nintendo GameBoy" "AIX"
NS	Host name	Authorative Name server	IN NS dns.infosys.tuwien.ac.at.
MX	Preference value + host name acts as mail exchange	Host willing to act as Mail exchange for the owning domain	IN MX pent223.dslab.tuwien.ac.at 10

Resource Records / 2

Type	RData	Description	Example
PTR	A domain name	Pointer to another part of the domain name space	0.0 IN PTR tunet-net.infosys.tuwien.ac.at.
SOA	Multiple fields (serial number, refresh,retry, expire time,minimum for TTL)	Identifies start of a zone of authority (Start Of Authority)	@ IN SOA dns.infosys.tuwien.ac.at.infosys.tuwien.ac. (000000001; Serial 10800; Refresh 3600; Retry 432000; Retry 86400; Minimum)

Resource Records Example

```
$TTL 2d
@ in SOA ns.xyz.com. myhost.xyz.com.
(
   200504070 ; serial = zone file version
  8h ; refresh – slaves check for updates
  1200; retry – retry a failed update
  4w; expire – discard zone data
  3600; cache lifetime for negative answers
)
xyz.com.          IN   NS   ns.xyz.com.
ns.xyz.com.       IN   A    192.168.20.1
myhost.xyz.com    IN   A    192.168.20.5
```

Name Servers

- Repositories that make up the domain database
- Divided into 'zones'
  - Distributed among name servers
- Primary task of name servers
  - Answer queries using data in its zones
    - Answer created using only local data
    - Or Referral to other name servers
- Name server typically supports one/more zones
- Domain database divided
  - By class
  - By "Cuts" in the name space between nodes
    - Cut between adjacent nodes in the domain tree
  - Allows partioning at points where an organization wants control

Resolvers

- Programs that ask DNS queries
- Typical functions:
  - Host name to host address translation
  - Host address to host name translation
  - General lookup

Internationalized Domain Names

- Internationalized Domain Names
  - Allow domain names to use non-ASCII characters
- Internationalized Domain Names in Applications (IDNA, RFC 3490)
  - Allows country-specific domain names (e.g Umlaute)
    - Without changing DNS protocol or DNS server
  - Translates to domain names with ASCII only chars
    - Domain name parts consists of ACE labels (ASCII compatible Encoding)
    - Uses NAMEPREP & Punycode (RFC 3491+RFC 3492)
  - österreich.at
  - "xn—sterreich-z7a.at"
    - Xn = ACE-Prefix
    - "ö" encoded as 'z7A'
- Supported by Browsers
  - Mozilla > 1,4
  - Netscape 7.1
  - Opera 7
  - IE only with plugin

Dynamic Host Configuration Protcol (DHCP)

- RFC 2131
- Passing configuration information to hosts
  - On TCP networks
- Based on BOOTP (RFC 951)
  - DHCP allows transmission of larger options
- UDP as transport protocol
  - DHCP server port 67
  - DHCP client port 68

DHCP Goals

- Delivery of host-specific configuration parameters
  - from a DHCP server to a host
  - key-value pairs stored at server
- Allocation of network addresses to host
  - Eg. Client requests use of an IP address

DHCP Address assignment

- Automatic assignment
  - Permanent IP address to a client
- Dynamic allocation
  - Assignment of IP address for a limited time
  - Reassigning free IP addresses
- Manual allocation
  - Client's IP address assigned by the network administrator

DHCP Client-Server Protocol

- Assumption
  - client does not know its IP address!

1. Client broadcasts message "DHCPDISOVER" on local physical subnet
   - Client's hardware address (eg. Ethernet)
2. (Multiple) Server respond DHCPOFFER messages
   - Includes client's IP address
   - Client's Lease (expiration time)
3. Client chooses one Server that sent DHCPOFFER
   - Verification of server parameter
   - Sends DHCPREQUEST message
4. Server sends DHCPACK
   - Contains configuration parameters

DHCP Hints

- Information valid as long as lease
  - No guarantee IP address is valid any longer
- Client may send RENEW messages
  - Timer watches lease expiration
  - Gets a new lease from DHCP server

Address Resolution Protocol

- IP addresses
  - Make only sense to TCP/IP protocol suite
  - Data link layer protocols own addressing
- ARP
  - Provides a mapping between two different forms of addresses
  - Ethernet
    - RFC 826
    - 32-bit IP and 48-bit ethernet
    - Ethernet specific protocol
  - Exists in every TCP/IP implementation
    - Automatically without intervention of Administrator

Reverse Address Resolution Protocol

- RARP
  - Hardware-Address to IP
  - RFC 903
- Original task
  - Optain IP address on booting
    - Only IP address
  - Today replaced by DHCP

Simple Tools
(Traceroute, Ping, TCPDump)

Ping / 1

- Based on ICMP
  - Sends an ICMP echo query request to a particular host
  - Receives ICMP echo reply
  - Identifier transmitted
    - Often sender process number (=ping process)
  - Sequence number
    - Identification of the packet
    - Incremented at each send
- Exists on all operating systems
- Ping often blocked by firewalls

Ping / 2

```
joe@mail:~$ ping localhost
PING mail (127.0.0.1): 56 data bytes
64 bytes from 127.0.0.1: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 127.0.0.1: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 127.0.0.1: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 127.0.0.1: icmp_seq=3 ttl=64 time=0.0 ms

--- mail ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Traceroute / 1

- Determines the route to a specified target host (via hosts and routers)
- IP header has 8-bit TTL (Time-to-live) field
  - Sender initializes this field to some value
  - Usually 64
  - To avoid endless loops
- Router detects IP datagram with TTL 0 or 1
  - Router throws away the datagram
  - Sends an ICMP message "time exceeded" to originating host
  - TTL > 1 datagram forwarded and TTL decremented by 1
- Today firewalls often block ICMP messages

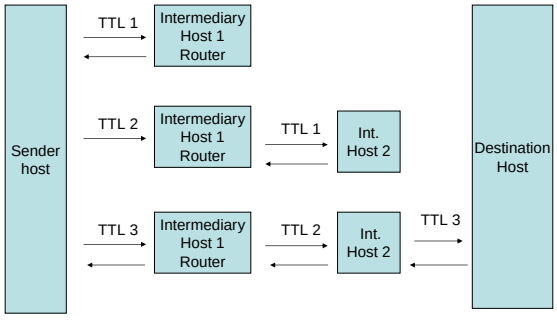
Traceroute / 2

- Traceroute functionality (Pseudocode)

```
boolean hostFound = false;
int port = 30000; // no host shall have a service running this port
int ttl = 0;

while(!hostFound) {
  try {
      ttl = ttl + 1;
      sendUPD(targetHost, port, ttl)
  } catch (ICMP_TTLExceeded ttlExcptl) {
       System.out.println("Host:"+ttlExcpt.host);
  } catch (ICM_PortUnreachable pue) {
       System.out.println("Final port reached!");
       hostFound = true;
  }
}
```

Traceroute / 3



Traceroute example

```
/users/home6/e9425196 36% traceroute www.apache.org
traceroute: Warning: Multiple interfaces found; using 193.170.75.14 @ lan2
traceroute to www.apache.org (192.87.106.226), 30 hops max, 40 byte packets
1  193.170.75.254 (193.170.75.254)  1.357 ms  1.247 ms  1.251 ms
2  192.35.243.25 (192.35.243.25)  0.774 ms  0.782 ms  0.852 ms
3  defcon-in.kom.tuwien.ac.at (192.35.241.35)  0.751 ms  0.454 ms  0.451 ms
4  192.35.241.116 (192.35.241.116)  0.637 ms  0.732 ms  0.750 ms
5  193.171.13.9 (193.171.13.9)  1.440 ms  1.440 ms  1.233 ms
6  193.171.23.33 (193.171.23.33)  1.411 ms  1.748 ms  1.618 ms
7  aconet.at1.at.geant.net (62.40.103.1)  1.955 ms  1.712 ms  2.148 ms
8  at.de2.de.geant.net (62.40.96.58)  13.938 ms  14.032 ms  14.421 ms
9  de2-2.de1.de.geant.net (62.40.96.54)  13.668 ms  24.610 ms  14.290 ms
10  de.nl1.nl.geant.net (62.40.96.102)  20.278 ms  24.153 ms  20.409 ms
11  surfnet-gw.nl1.nl.geant.net (62.40.103.98)  20.475 ms  20.693 ms  20.463 ms
12  PO11-0.CR1.Amsterdam1.surf.net (145.145.166.33)  20.519 ms  20.312 ms  30.719 ms
13  PO0-0.AR5.Amsterdam1.surf.net (145.145.162.2)  20.465 ms  22.724 ms  20.615 ms
14  Te1-1.SW14.Amsterdam1.surf.net (145.145.140.158)  20.362 ms  20.828 ms  20.284 ms
15  * * * *
```

Dig / Nslookup

- nslookup hostname
- dig hostname
  - Queries name server for DNS information
  - Query on alternative Nameserver (required for Lab)
    dig @1.2.3.4 hostname

TCPDump

- Logs all network device traffic
  - IP and non-IP
  - Requires Administrator / root permissions
  - Pretty printing of
    - Protocol internals
    - IP – Hostname resolution

Other tools

- Generic
  - netstat
    - Displays network usage statistics
- Unix
  - hostname
    - Name of local system
  - ifconfig
    - Information about network interfaces
  - Nslookup, dig
    - DNS translations (resolver tasks)
  - arp
- Windows
  - ipconfig