CSE 3214: Computer Network Protocols and Applications

Course Web-Page: http://www.eecs.yorku.ca/course/3214/
(all lecture notes will be posted on this page)

Instructor: Natalija Vlajic (vlajic@cse.yorku.ca)

Office Hours: Tuesday 13:00 - 14:00 (CSB 2047)

Prerequisite: General Prerequisite + CSE 3213.
The course assumes prior knowledge of Java programming.

Textbook: "Computer Networking: A Top-Down Approach Featuring the Internet",
J. F. Kurose and K. W. Ross, Addison Wesley, 2018, 7th edition.

"Network Simulation Experiments Manual",
E. Aboelela, Morgan Kaufmann, 2012, 3rd edition.

Other Material: TCP/IP Guide, http://www.tcpipguide.com/free/t_toc.htm

Software Tools: **Riverbed Modeler** – available in LAS 2007
Wireshark

Grading Scheme:

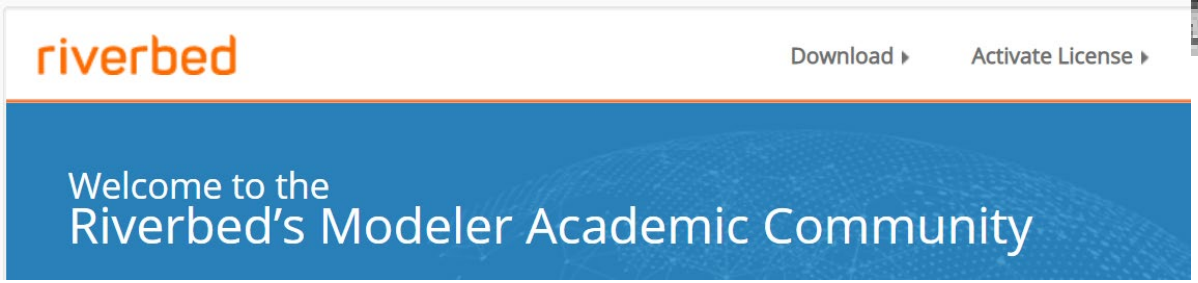
Midterm:	**35%**	**February 25 !!!**
Final:	**40%**	
4 Labs:	**16%**	**Riverbed Modeler**
Project:	**9%**	**Java Socket Programming**

Late Assignments: **Late lab reports will not be accepted, unless a prior arrangement is made with the instructor.**

Missed Midterm: **Makeups of missed midterm exams are only possible in case of medical emergencies !!!**

Course Objective: **The course will cover more advanced topics in networking, concentrating on higher-level protocols, network programming and application, multimedia, security. It complements and builds upon the material covered in CSE 3213.**

Please download ASAP!



https://cms-api.riverbed.com/portal/community_home

Course Schedule:

Network Taxonomy, Packet vs. Circuit Switching
Layers and Protocols

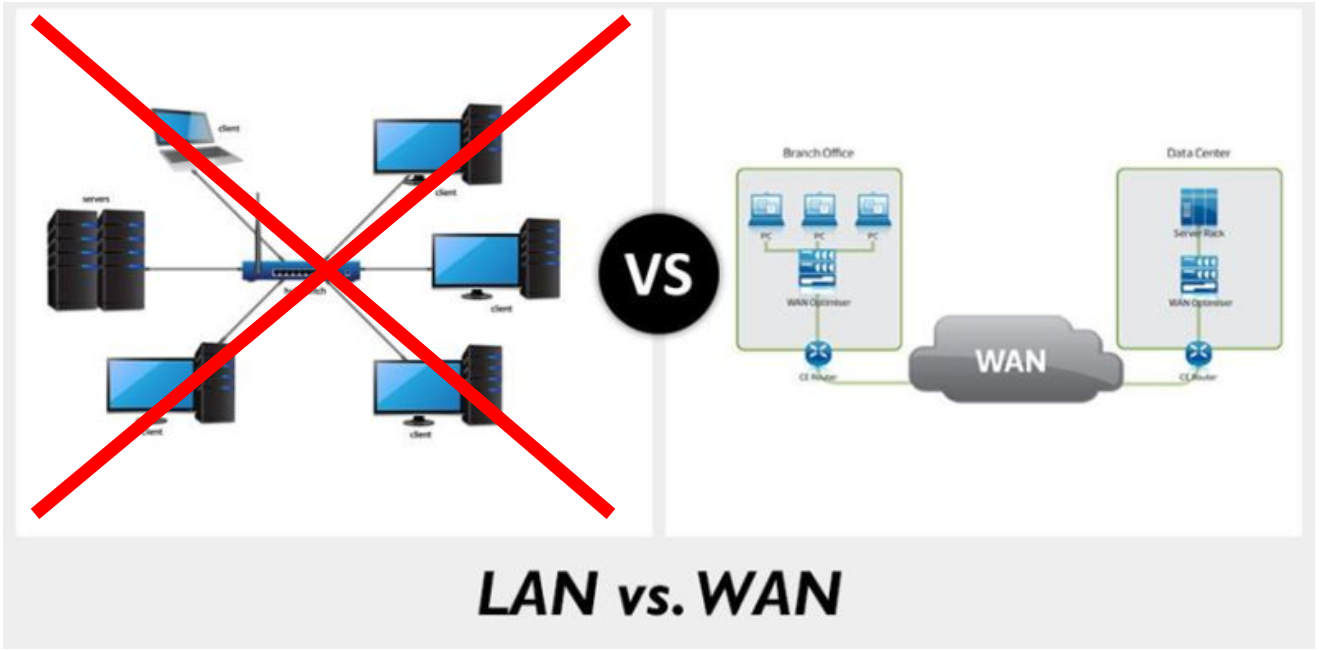
Queuing Fundamentals, Packet Delay
Network Layer and IP Protocol (IPv4 & IPv6)
IP Addressing, Subnetting and NAT
ARP
ICMP
Routing Algorithms (Link State, Distance Vector)
Routing Protocols (RIP, OSPF, BGR)
Multicasting & IGMP

Transport Layer, UDP, TCP
TCP Flow, Error and Congestion Control
Java Socket Programming

HTTP
DNS
Multimedia and QoS
DHCP
Electronic Mail
FTP
Telnet
P2P
Network Security

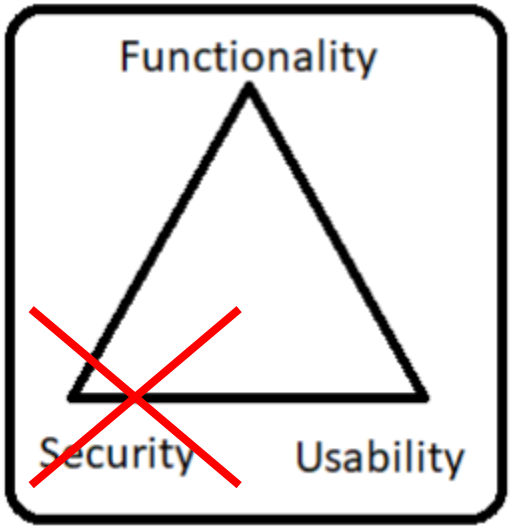
What this course is and is not about …

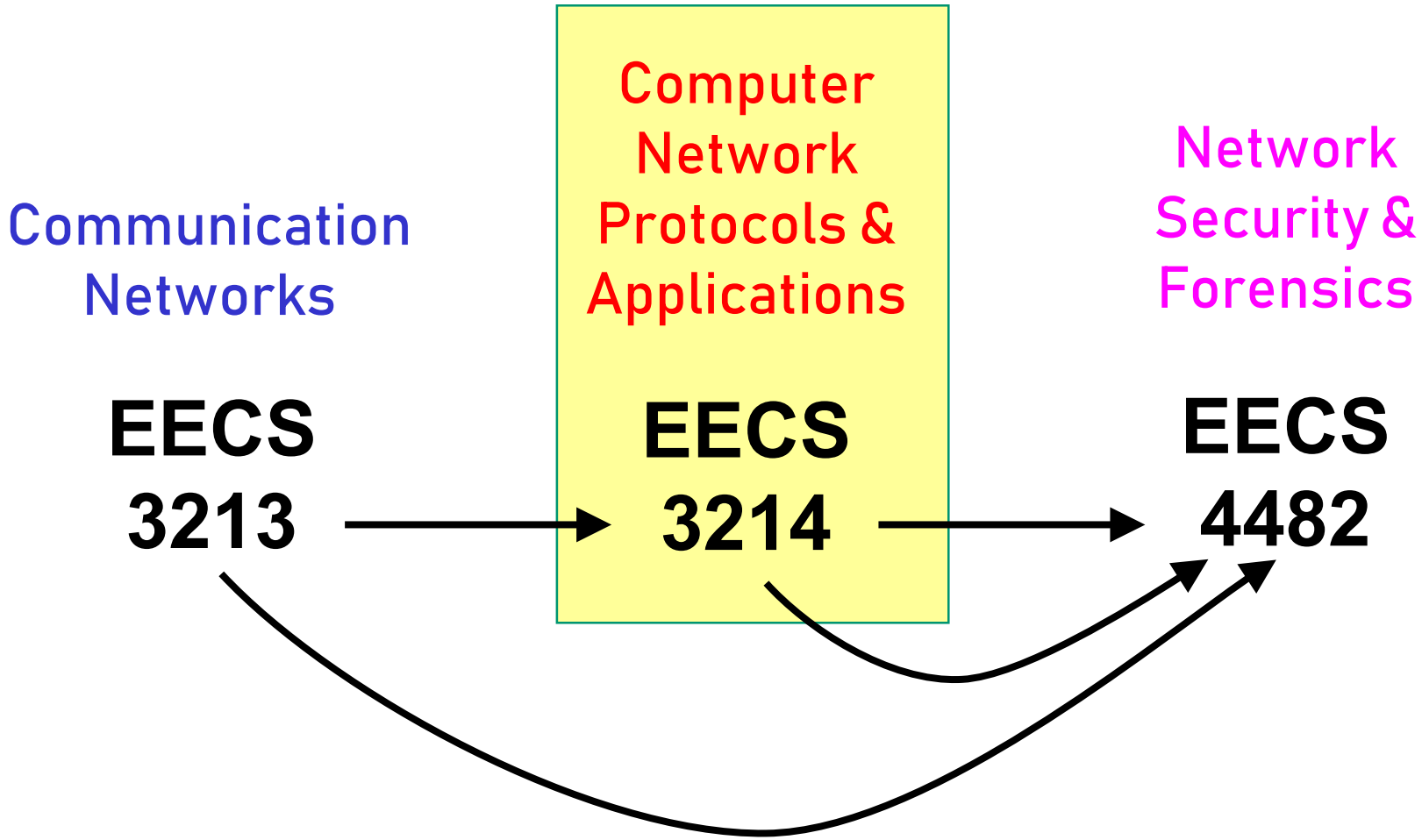
EECS 3213



EECS 3214

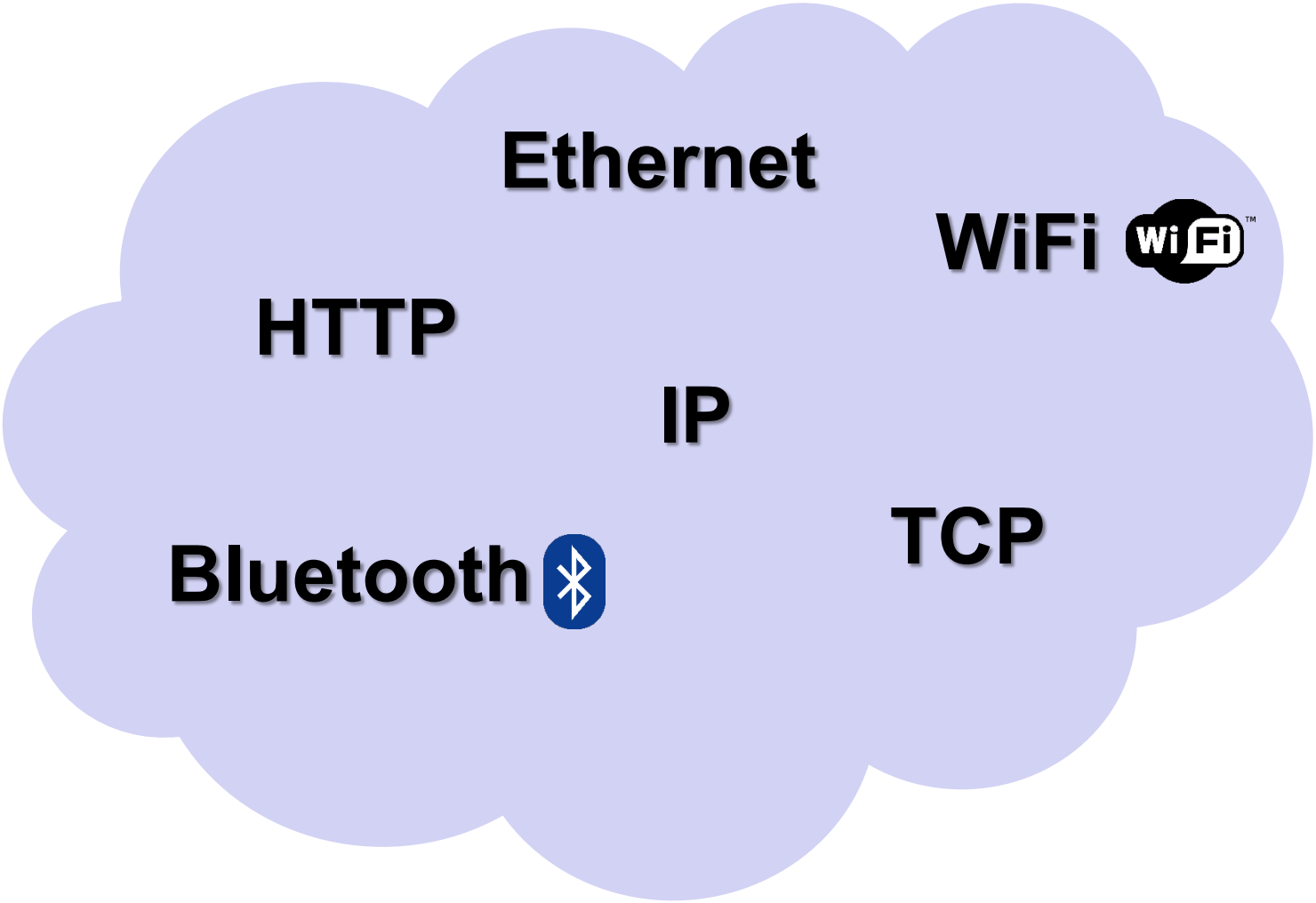
EECS 4482



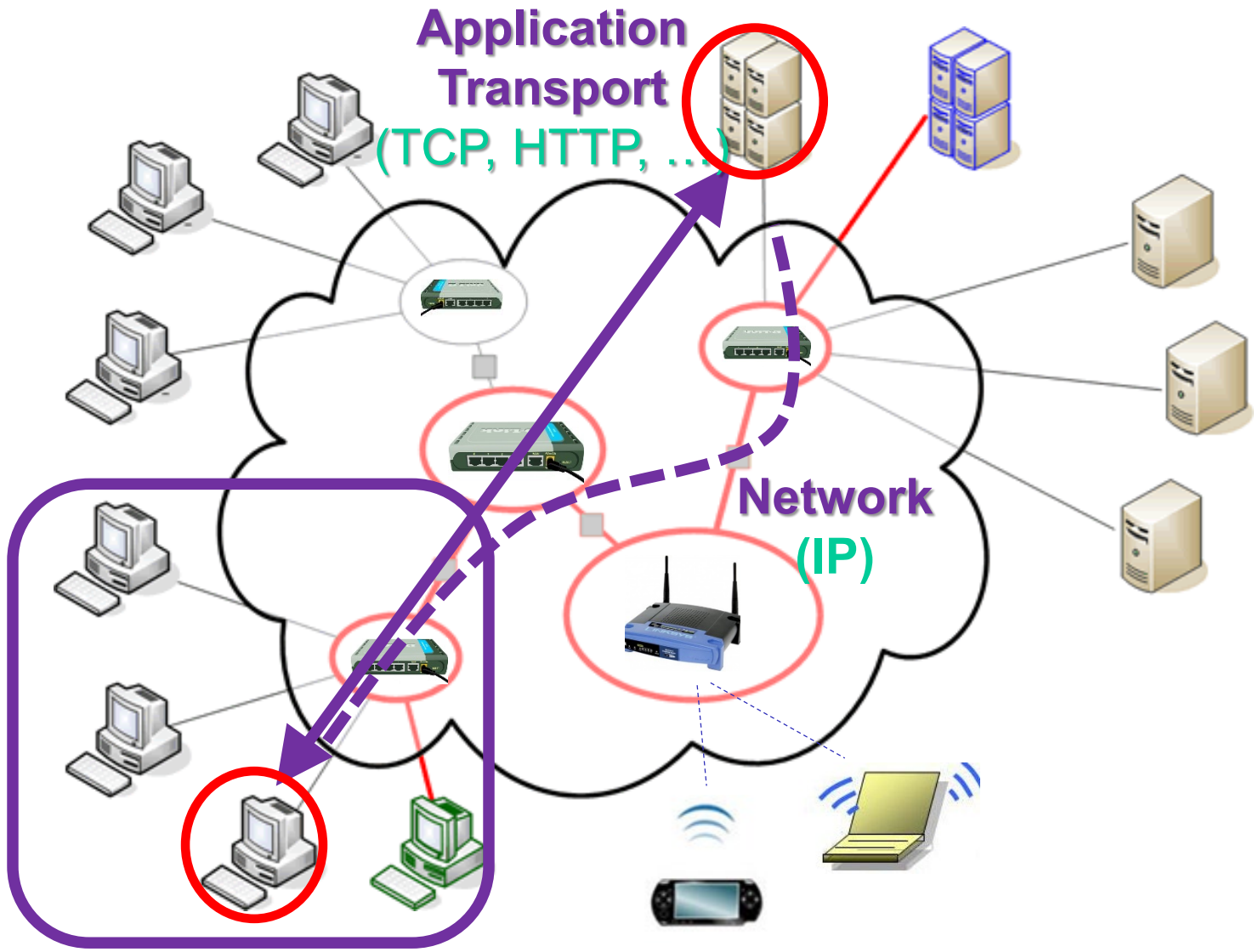


There is overlap among networking courses!

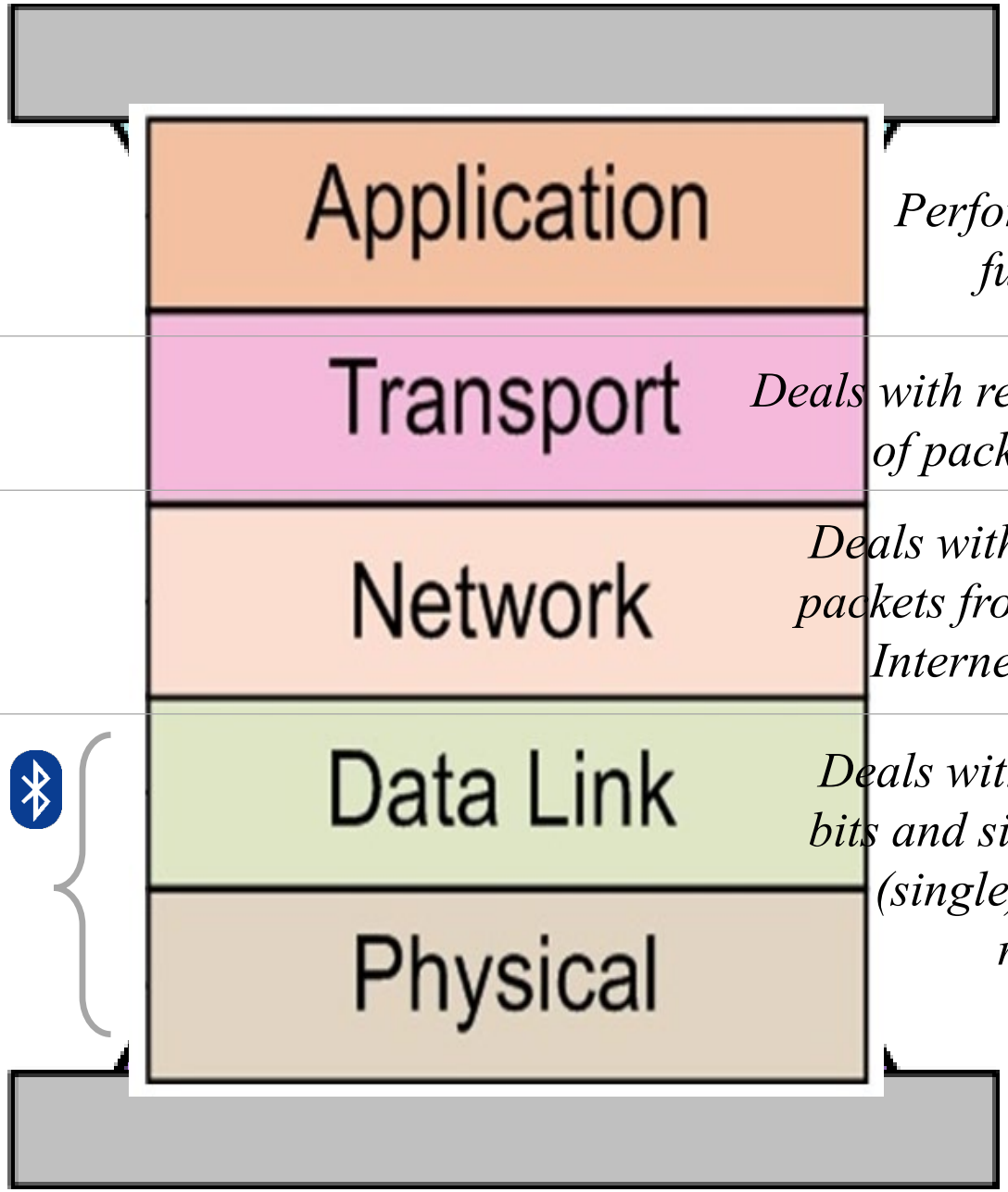
Big Picture



No single protocol/standard is sufficient for computer communication – they each are just ‘a piece of a bigger picture/puzzle’ …


Application
Transport
(TCP, HTTP, …)
Network
(IP)
Data Link / Physical
(WiFi, Ethernet, Bluetooth)

Internet Hourglass Model



Performs some useful functionality.

Deals with reliable transmission of packet streams …

Deals with transmission of packets from one side of the Internet to the other.

Deals with transmission of bits and single packets over (single) transmission medium.

Bluetooth

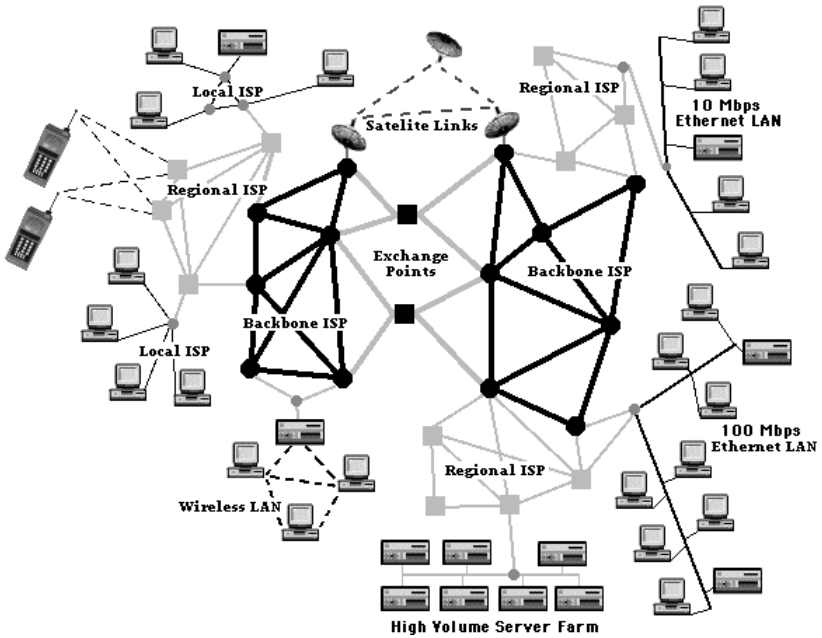
Ethernet

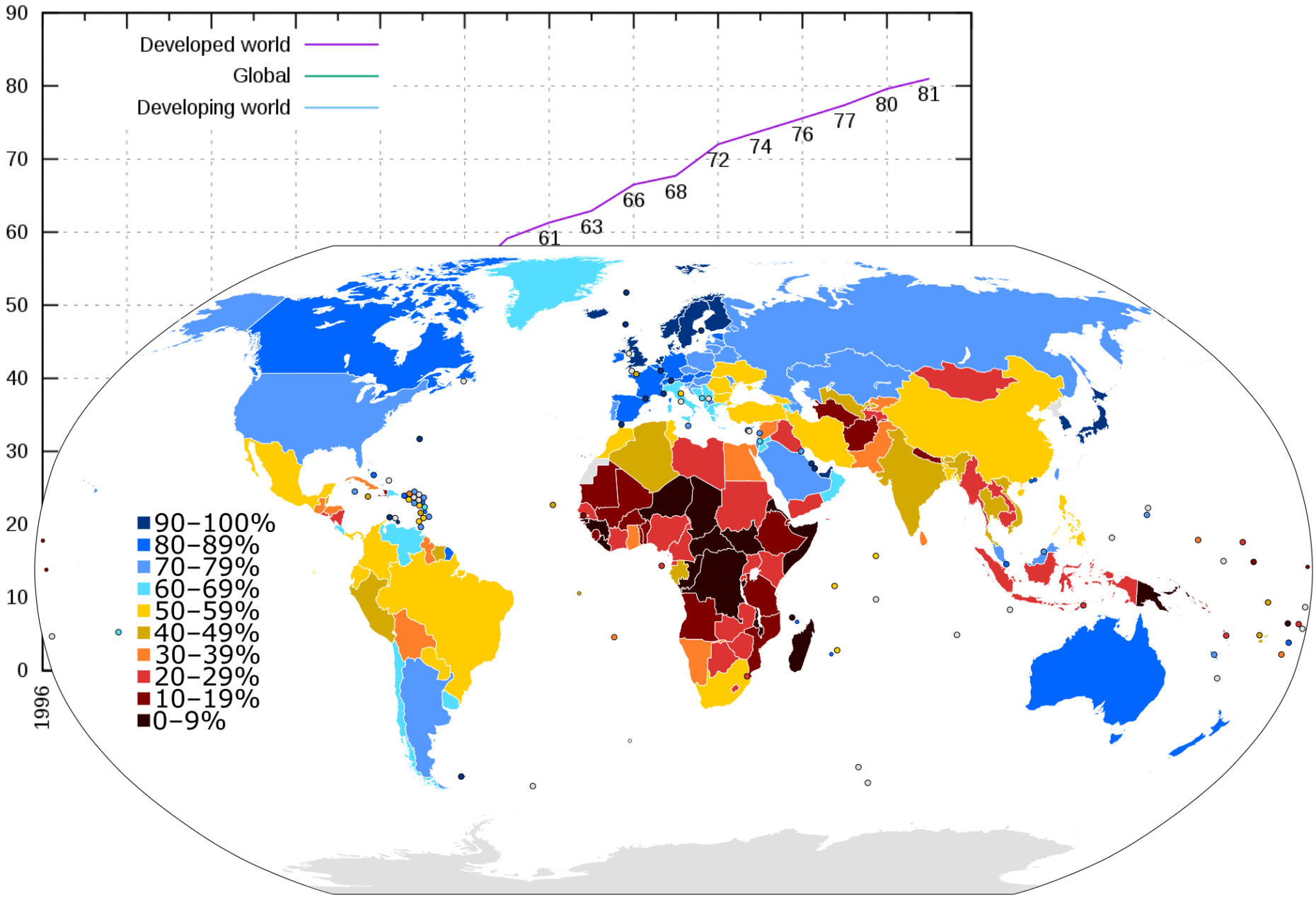
WiFi

The Internet

The Internet – **most notable datagram packet-switching WAN**

- **evolved from the ARPANET** (network of computers operated by several universities doing military research) **initially developed in 1969**
- **component networks differ in terms of their underlying technology and operation**
- **spread over 200+ countries**
- **made up of 100,000s of interconnected networks, 10,000,000s of interconnected hosts, and 1,000,000,000s of users**
- **still grows …**





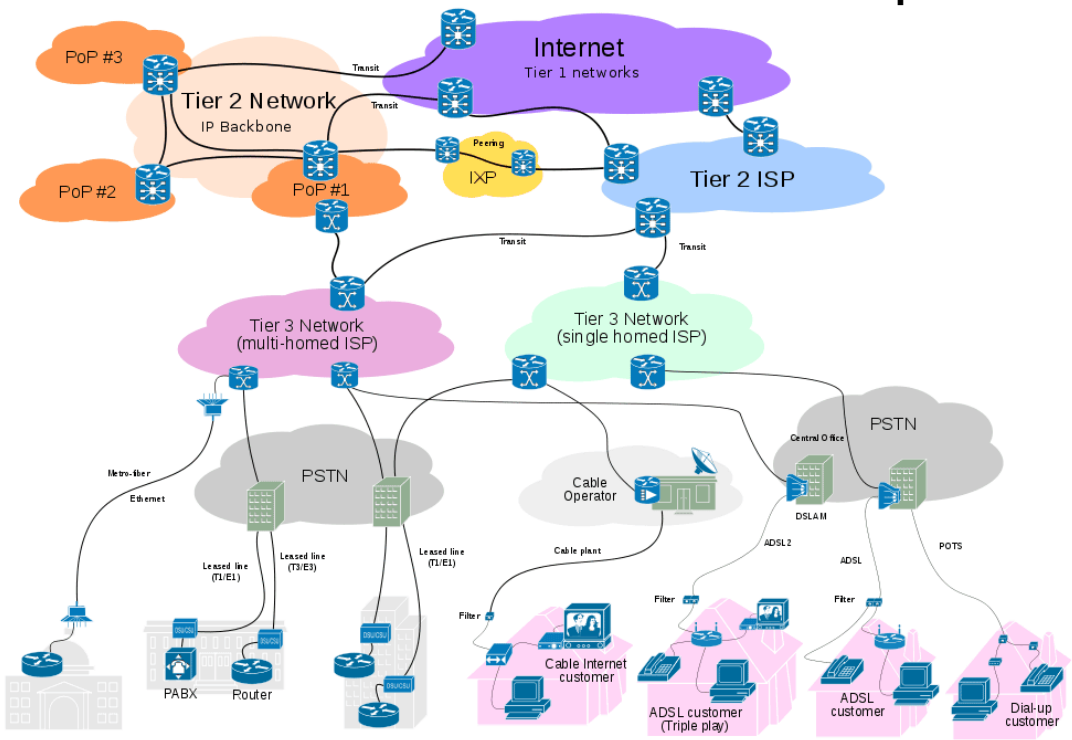
https://en.wikipedia.org/wiki/List_of_countries_by_number_of_Internet_users

The Internet (cont.)

Internet Service Provider (ISP)

– Internet Access Provider – allows users or other networks to connect to the Internet

- 3-tiered hierarchy of interconnected ISPs keeps the Internet together
- lower-tier ISPs provide access to home users cable, DSL, high-speed LANs, etc.
- upper-tier ISPs provide access to lower-tier ISPs – they consist of high-speed routers and high--speed fiber-optic links



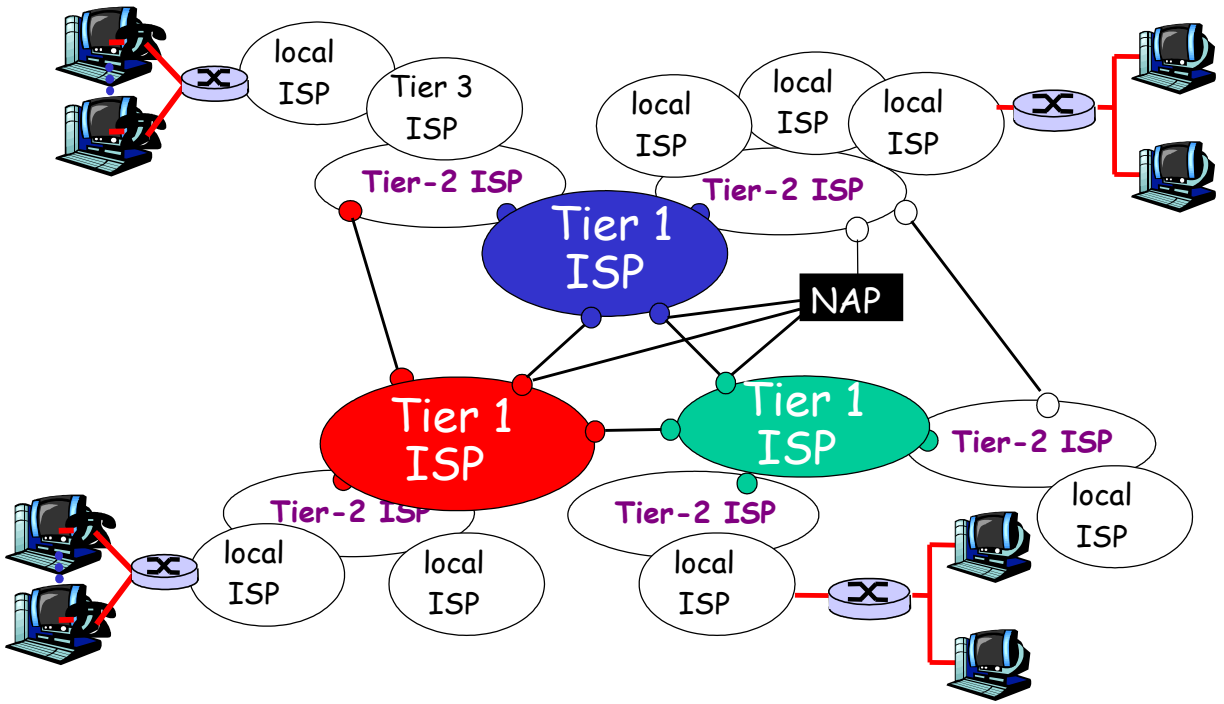
The Internet (cont.)

Example **[routers]**

The Internet (cont.)

3-tiered Hierarchy of ISPs

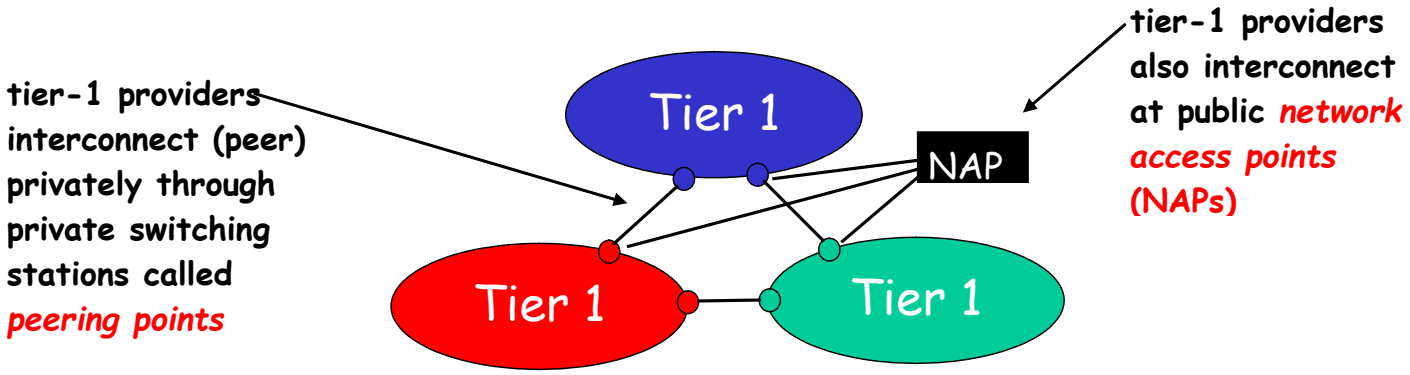
- **Tier-1:** **International / National ISPs**
- **Tier-2:** **Regional ISPs**
- **Tier-3:** **Local ISPs**



The Internet (cont.)

International ISP – **Internet backbone network – one of the networks at the top of ISP-hierarchy – has international coverage (e.g. AT&T, CenturyLink, Sprint, Orang, Tata Comm, Cogent)**

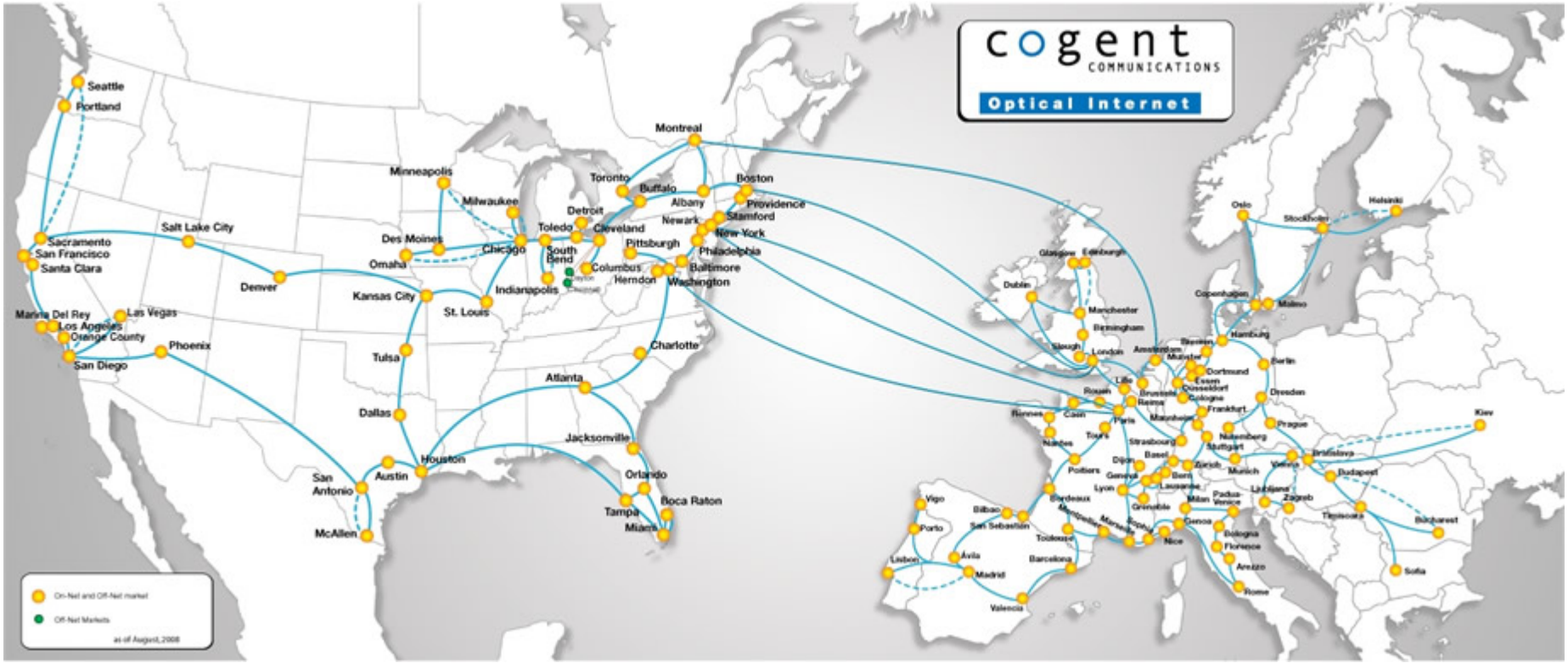
- **look similar to any other network (links + routers), but link speeds of 100+ Gbps - routers must be able to forward packets at extremely high rates**
- **directly connect to each of the other tier-1 ISPs; also connect to a large number of tier-2 ISPs and other customer networks**
- **NAP – set of high-speed routers through which routers from different tier-1 ISP can exchange traffic**
- **NAP can be owned and operated by a third-party telecom company or by an Internet backbone provider**



Delay and Routes in the Internet (cont.)

Example **[Cogent Network Map]**

"Cogent's worldwide Tier 1 optical IP network is one of the largest of its kind, with direct IP connectivity to more than 6,840 AS (Autonomous System) networks around the world and over 199 Tbps internetworking capacity."

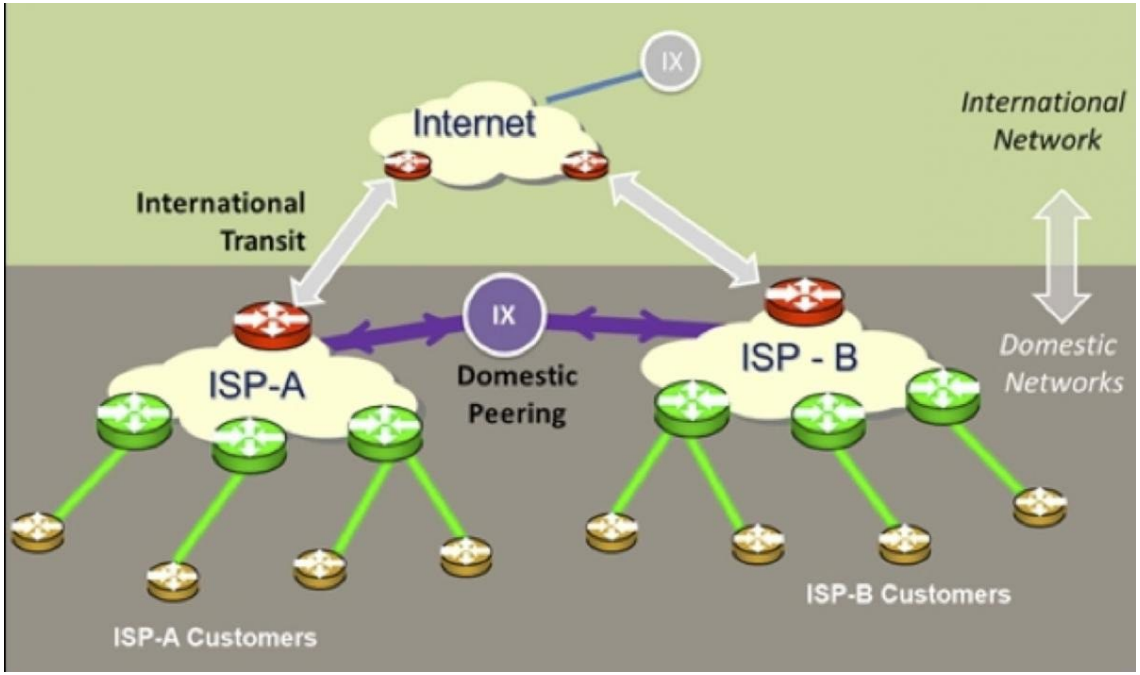


https://www.cogentco.com/en/network

The Internet (cont.)

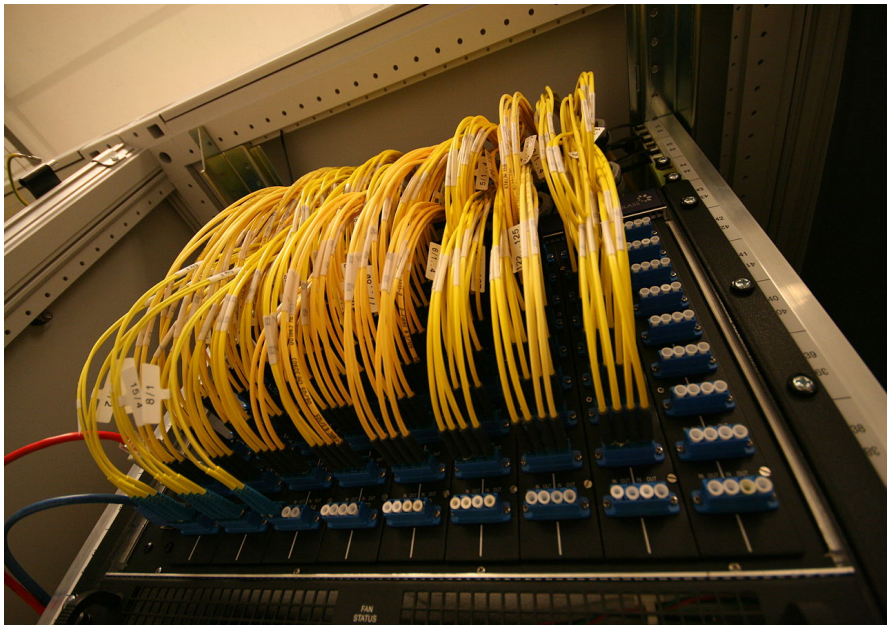
Network Access Point (NAP) – old term/concept.

Internet Exchange Point (IXP) – new term/concept = **physical infrastructure through which different IP networks (ISP, CDN, etc.) exchange traffic directly**



Can be used to 'connect' lower tier ISP directly, in which case IXPs reduce the portion of an ISP's traffic that must be delivered via their upstream transit providers, thereby reducing the average per-bit delivery cost of their service.

https://en.wikipedia.org/wiki/Internet_exchange_point



The main building of the London Internet Exchange (LINX)

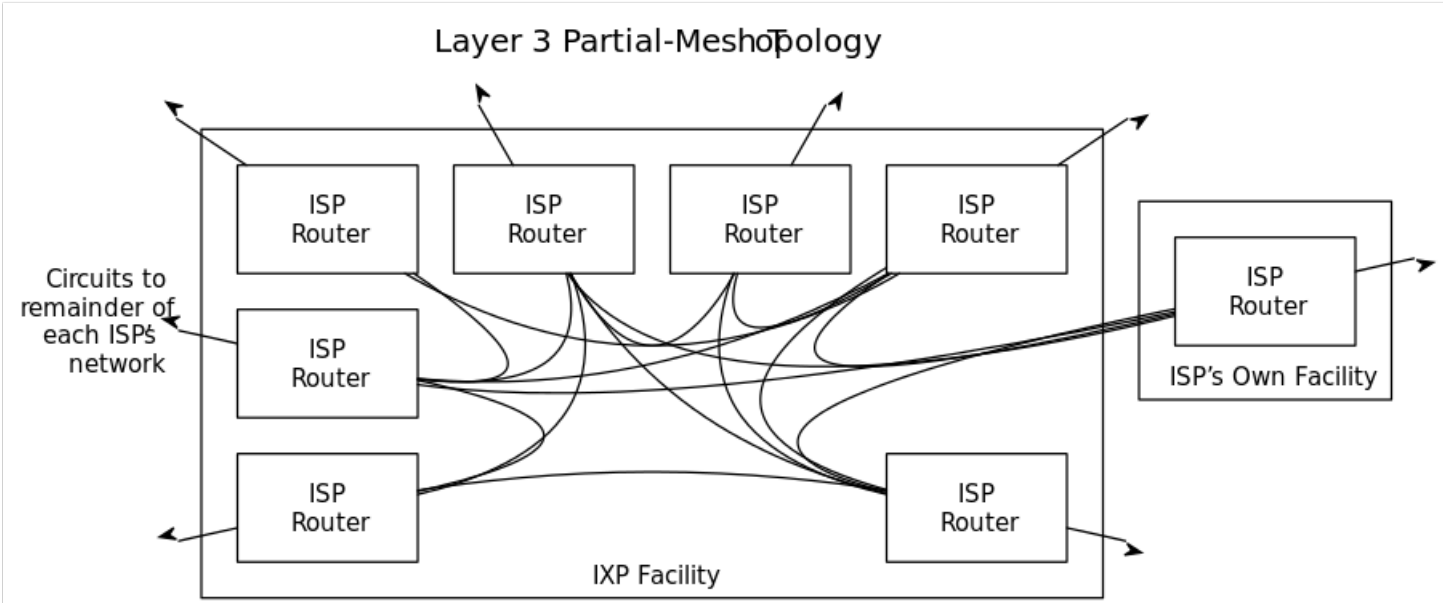
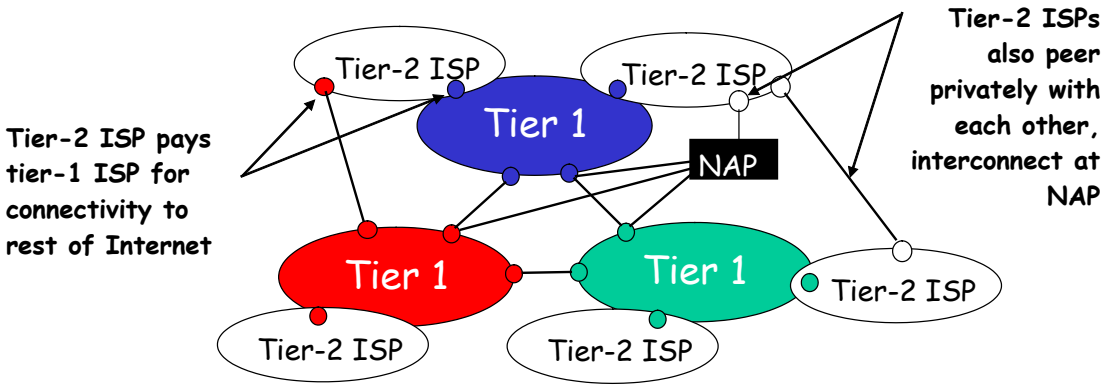


Diagram by Bill Woodcock, Packet Clearing House, released for use on Wikipedia

The Internet (cont.)

Regional ISP – **smaller ISP that connects to one or more tier-1 ISPs and possibly other tier-2 ISPs – have national coverage (e.g. Bell, Rogers)**

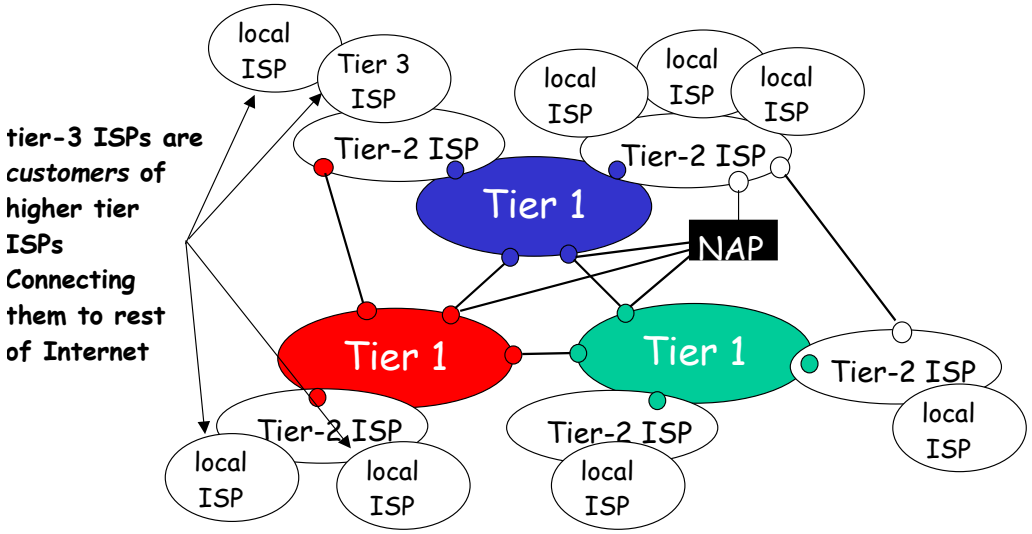
- **to reach the global Internet, a tier-2 ISP needs to connect to and route traffic through one of the tier-1 ISP**
- **tier-2 ISP is *customer*, tier-1 ISP is *provider* – *provider* charges *customer* a fee**
- **a tier-2 ISP can also connect directly to other tier-2 network without having to pass through a tier-1 network**
- **some tier-1 are also tier-2 providers, selling Internet access directly to end users (e.g. Sprint, AT&T, …)**



The Internet (cont.)

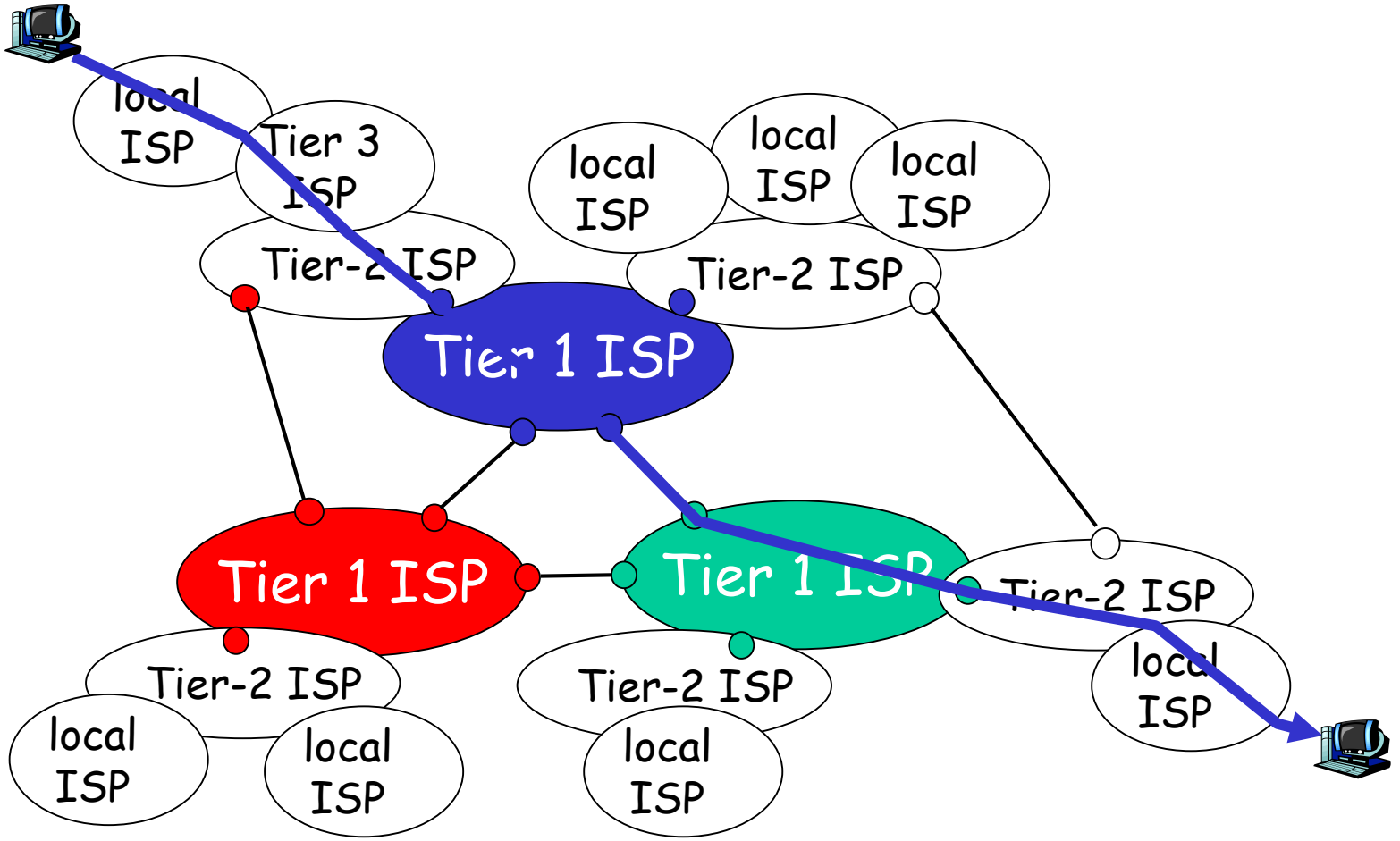
Local ISP – **small ISP that connects to the Internet via one or more tier-2 ISPs and provides access to end users**

- **local ISP can be**
  - **(1) company that just provides Internet service**
  - **(2) corporation that supplies service to its own employees**
  - **(3) college or university that runs its own network**

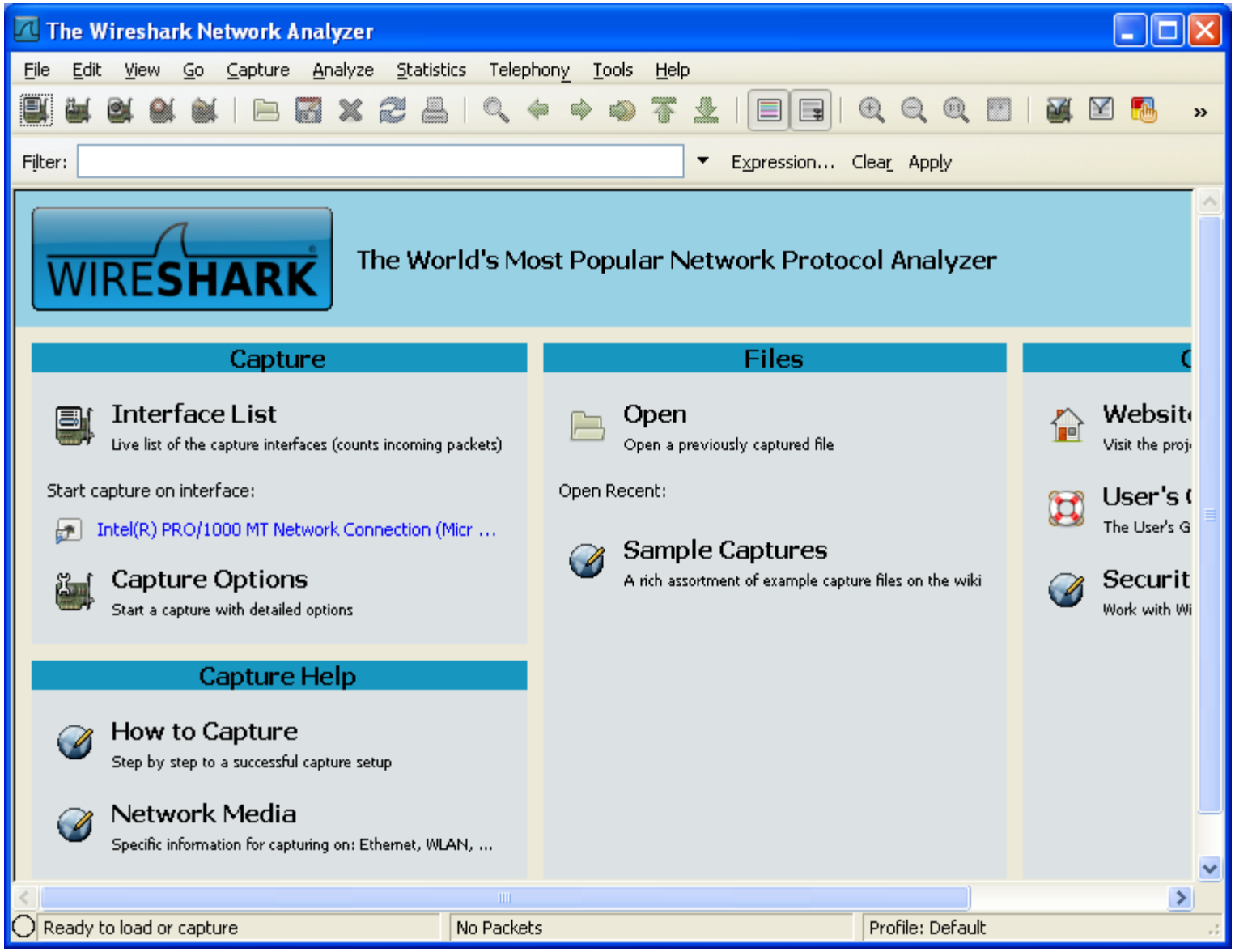


The Internet (cont.)

Packet Routing in the Internet – **each packet passes through many networks before reaching its destination**



Wireshark


The Wireshark Network Analyzer
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply
WIRESHARK
The World's Most Popular Network Protocol Analyzer
Capture
Interface List
Live list of the capture interfaces (counts incoming packets)
Start capture on interface:
Intel(R) PRO/1000 MT Network Connection (Micr ...
Capture Options
Start a capture with detailed options
Files
Open
Open a previously captured file
Open Recent:
Sample Captures
A rich assortment of example capture files on the wiki
Capture Help
How to Capture
Step by step to a successful capture setup
Network Media
Specific information for capturing on: Ethernet, WLAN, ...
Ready to load or capture
No Packets
Profile: Default

Network Monitoring & Protocol Analysis

Network Monitoring & Protocol Analysis – process of capturing network traffic and inspecting it closely to determine type and amount of data:

a) traveling through your network, or

b) arriving at your computer

- network/protocol analysis is also known as '**sniffing**'

Network Analyzer (Packet Sniffer) – standalone hardware device or software installed on a computer – **decodes data packets of common protocols and displays their content in human-readable format**

- network analyzers are either free and commercial
- **differences between network analyzers include**:

a) number of supported protocol decodes

b) quality of packet decodes

c) user interface

d) graphing and statistical capabilities

Network Monitoring & Protocol Analysis (cont.)

Network Analyzer Application:

1) As an educational resource when learning about protocols.
2) Analyzing operations of applications & protocols they rely on.
3) Debugging in development stage of network programming.
4) Network intrusion detection.

…

5) Monitoring 3rd party traffic to steal data or learn more about their network.

Common Network Analyzer:

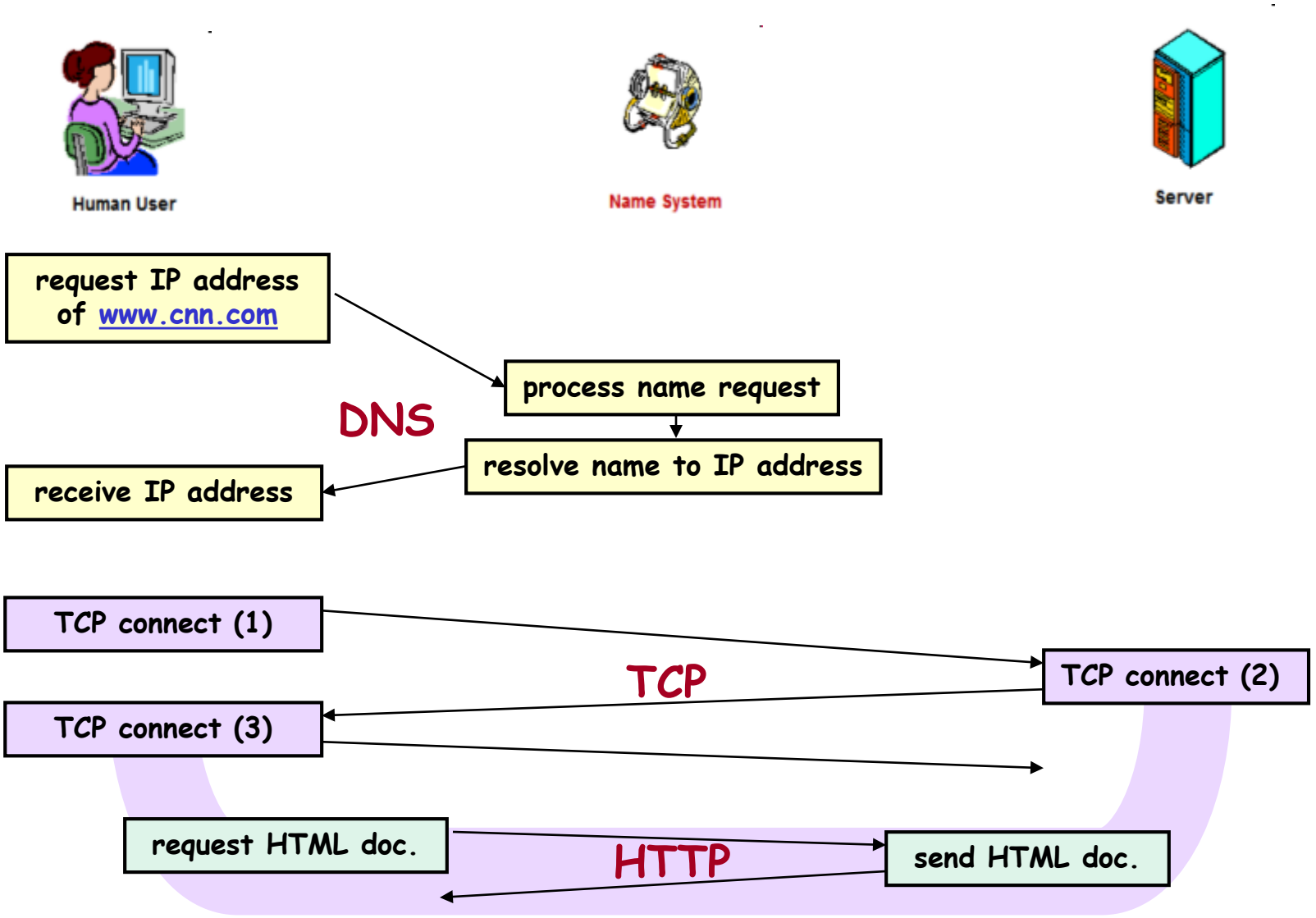
Wireshark

- freeware
- runs on Windows, Linux, Mac, etc.
- decodes hundreds of protocols
- nice GUI

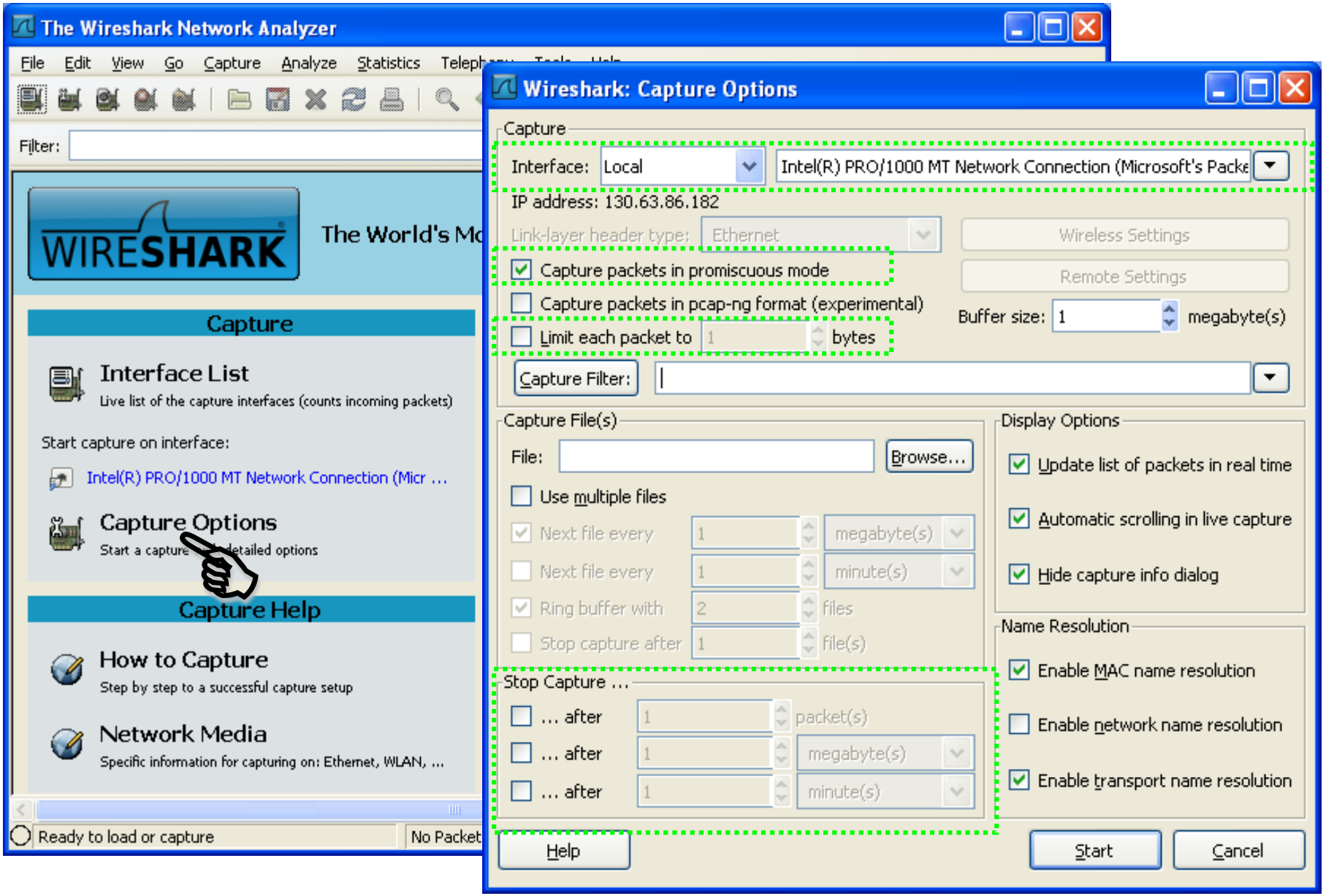
Snort, WinDump / TcpDump, Dsniff, etc.

Wireshark Network Analyzer

Example [retrieval of www.cnn.com web page]

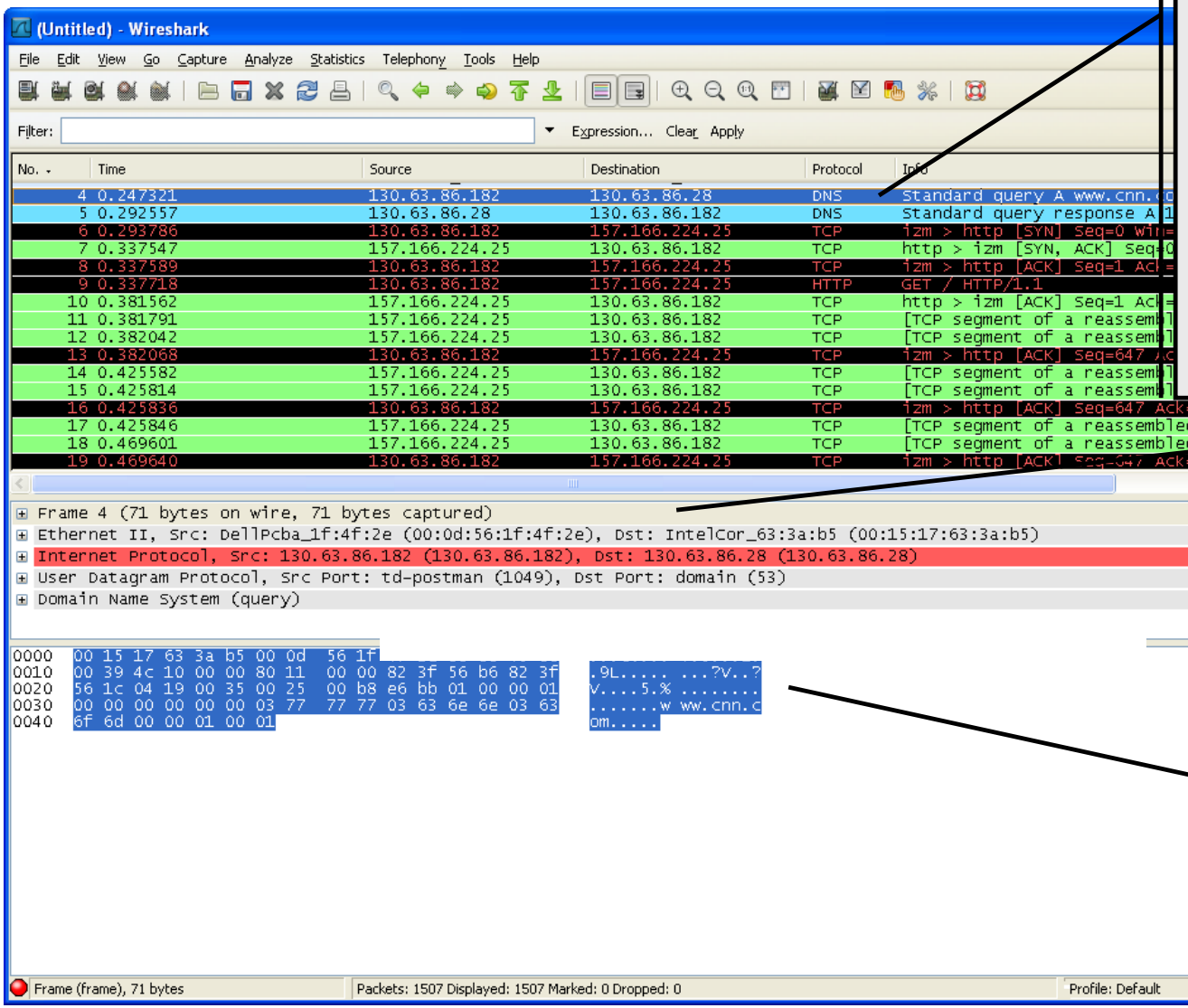


Wireshark Network Analyzer (cont.)



Wireshark Network Analyzer (cont.)

Wireshark Display Window – captures traffic in three panes



SUMMARY

Displays one line summary for each captured packet:

1) time
2) source address
3) destination address
4) info about highest-layer protocol

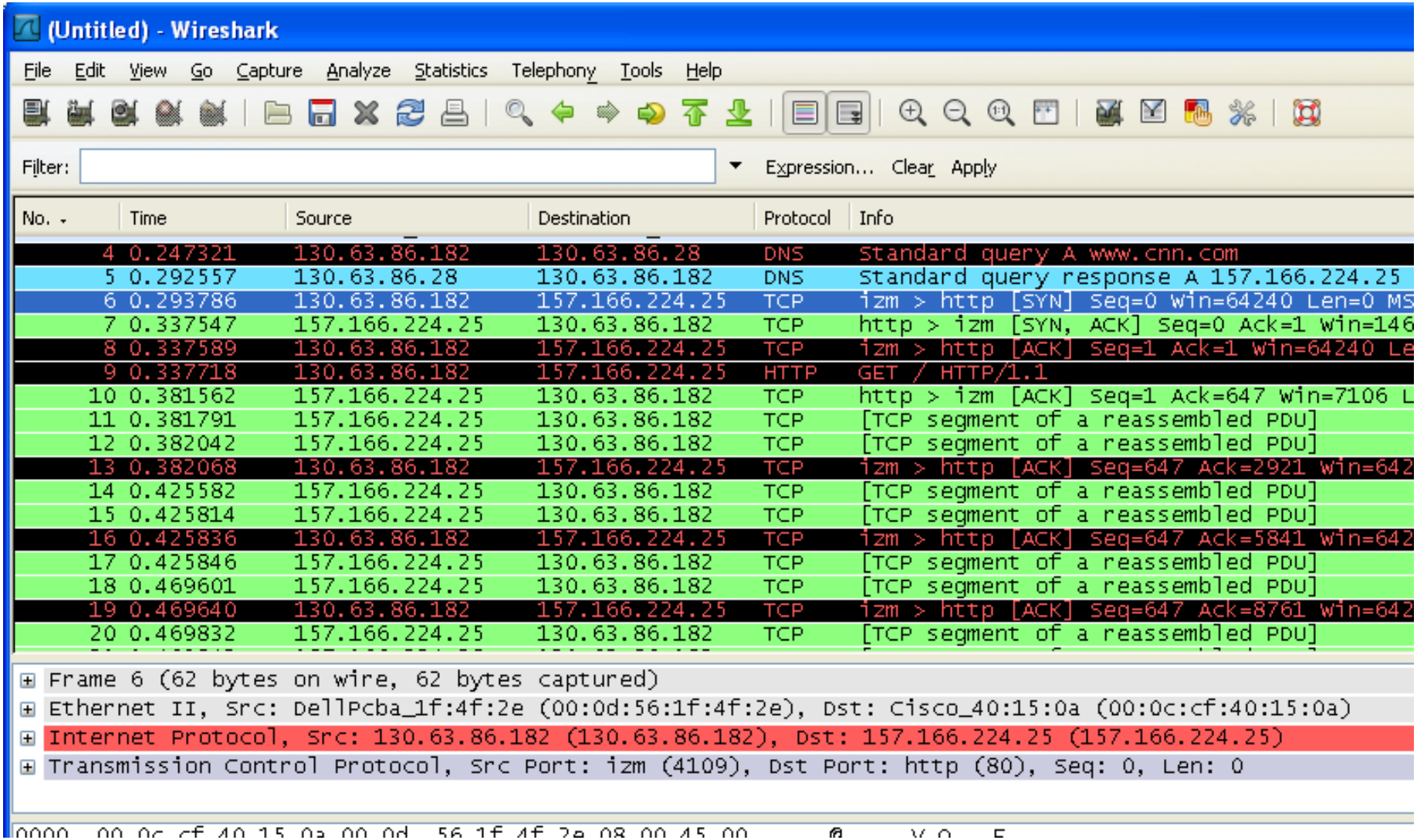
DETAIL

Provides all the details for each of the layers contained inside the captured packet in a tree-like structure.

DATA

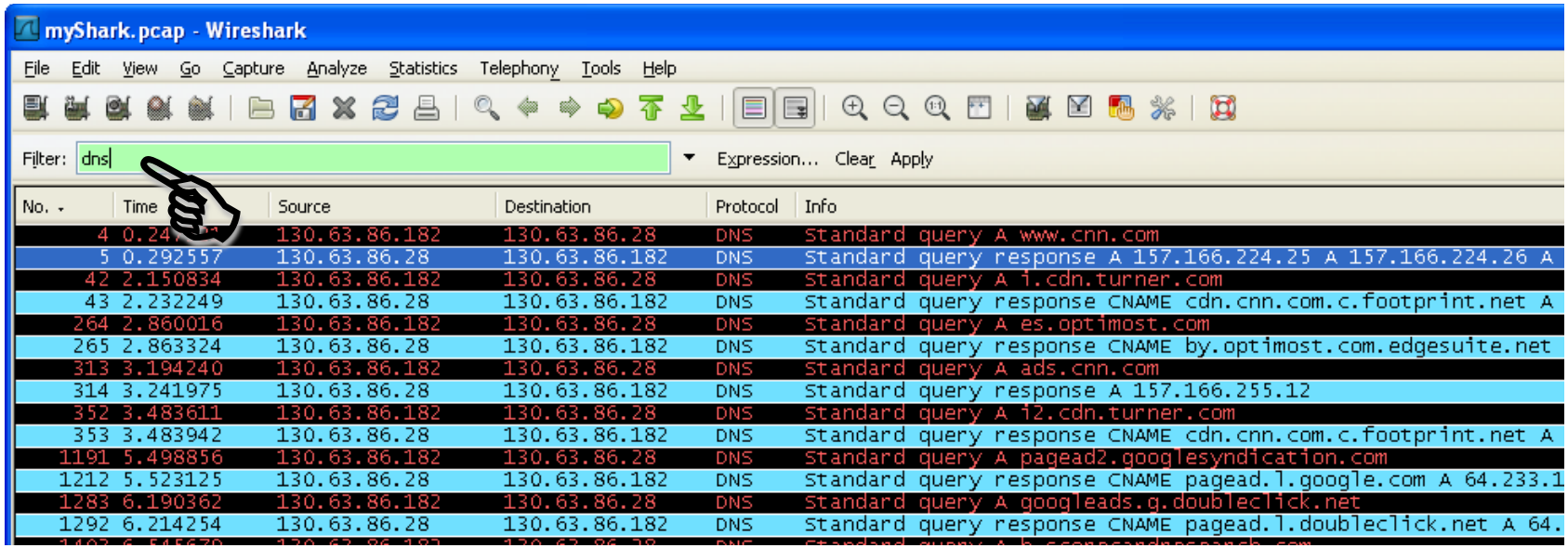
Displays the raw captured data both in hexadecimal and ASCII format.

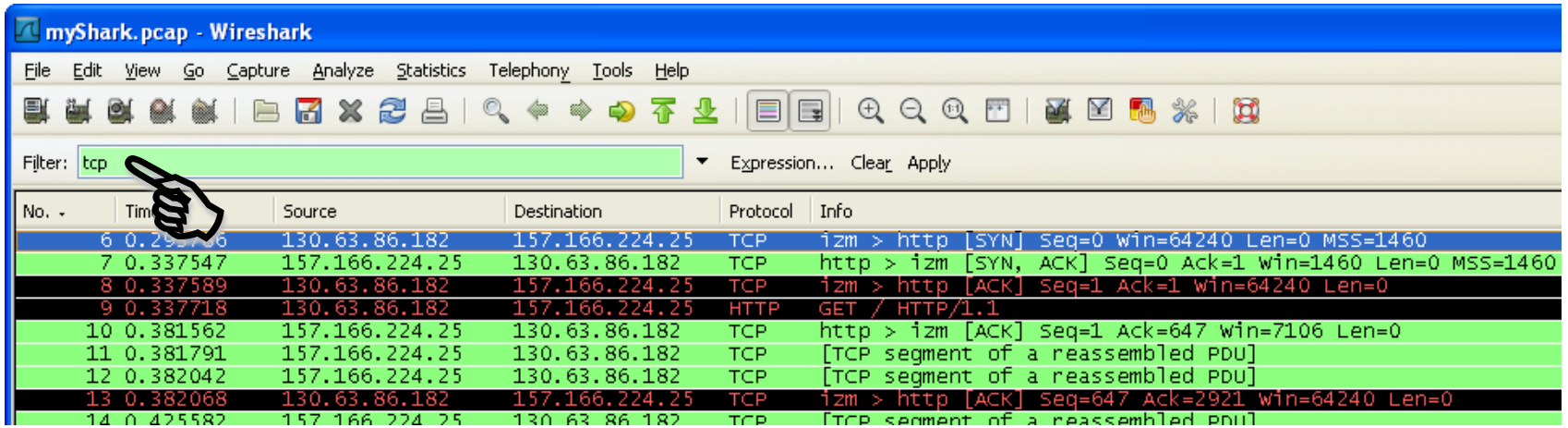
Wireshark Network Analyzer (cont.)



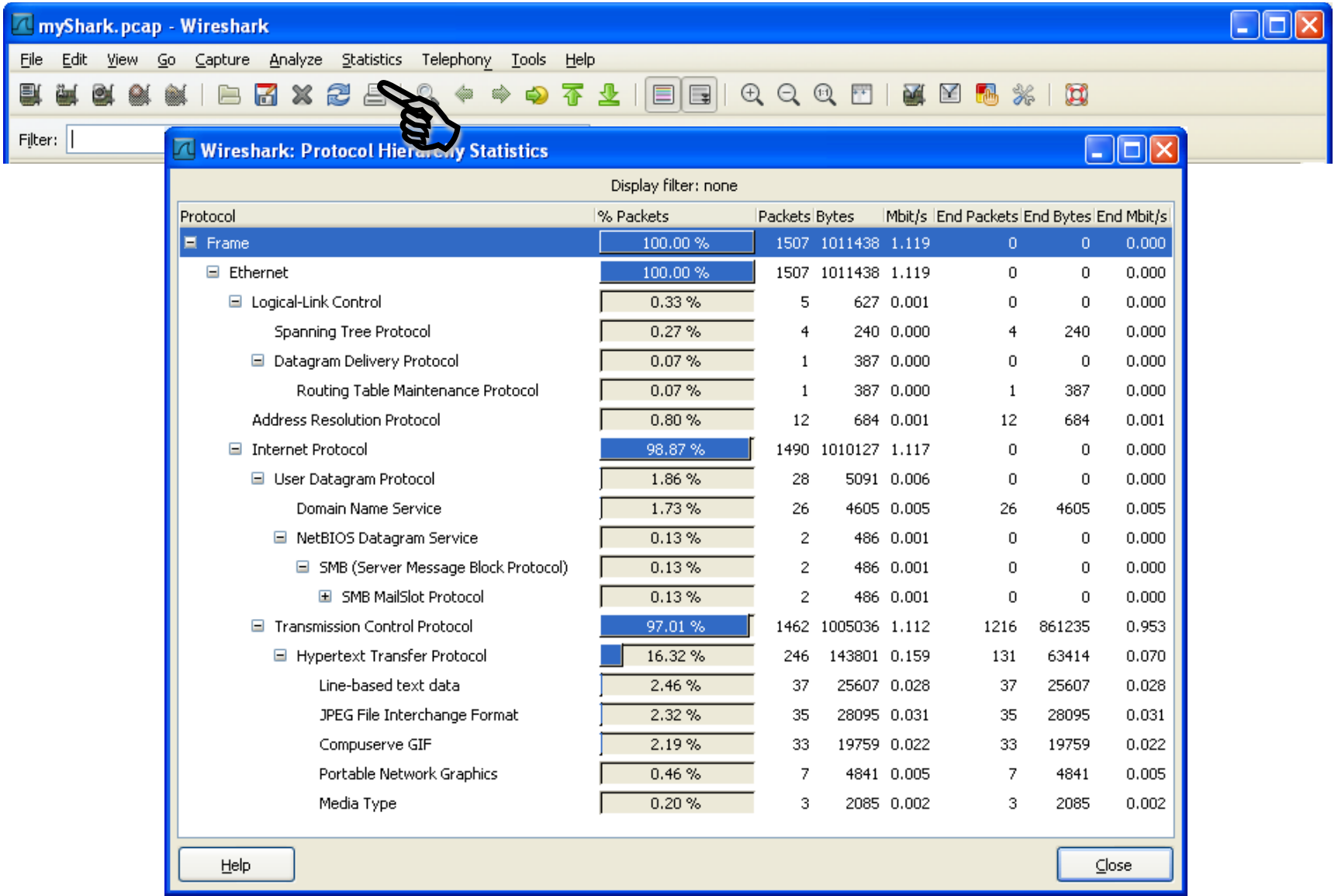
Wireshark Network Analyzer (cont.)

Wireshark Display Filter Feature





Wireshark Statistics Summary Feature



Protocol	% Packets	Packets	Bytes	Mbit/s	End Packets	End Bytes	End Mbit/s
Frame	100.00 %	1507	1011438	1.119	0	0	0.000
Ethernet	100.00 %	1507	1011438	1.119	0	0	0.000
Logical-Link Control	0.33 %	5	627	0.001	0	0	0.000
Spanning Tree Protocol	0.27 %	4	240	0.000	4	240	0.000
Datagram Delivery Protocol	0.07 %	1	387	0.000	0	0	0.000
Routing Table Maintenance Protocol	0.07 %	1	387	0.000	1	387	0.000
Address Resolution Protocol	0.80 %	12	684	0.001	12	684	0.001
Internet Protocol	98.87 %	1490	1010127	1.117	0	0	0.000
User Datagram Protocol	1.86 %	28	5091	0.006	0	0	0.000
Domain Name Service	1.73 %	26	4605	0.005	26	4605	0.005
NetBIOS Datagram Service	0.13 %	2	486	0.001	0	0	0.000
SMB (Server Message Block Protocol)	0.13 %	2	486	0.001	0	0	0.000
SMB MailSlot Protocol	0.13 %	2	486	0.001	0	0	0.000
Transmission Control Protocol	97.01 %	1462	1005036	1.112	1216	861235	0.953
Hypertext Transfer Protocol	16.32 %	246	143801	0.159	131	63414	0.070
Line-based text data	2.46 %	37	25607	0.028	37	25607	0.028
JPEG File Interchange Format	2.32 %	35	28095	0.031	35	28095	0.031
Compuserve GIF	2.19 %	33	19759	0.022	33	19759	0.022
Portable Network Graphics	0.46 %	7	4841	0.005	7	4841	0.005
Media Type	0.20 %	3	2085	0.002	3	2085	0.002

Wireshark Network Analyzer (cont.)

ipconfig -all – **reveals own MAC & IP address, and IP address of DNS & DHCP server …**