

CSE 3214: Computer Network Protocols and Applications

1

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:

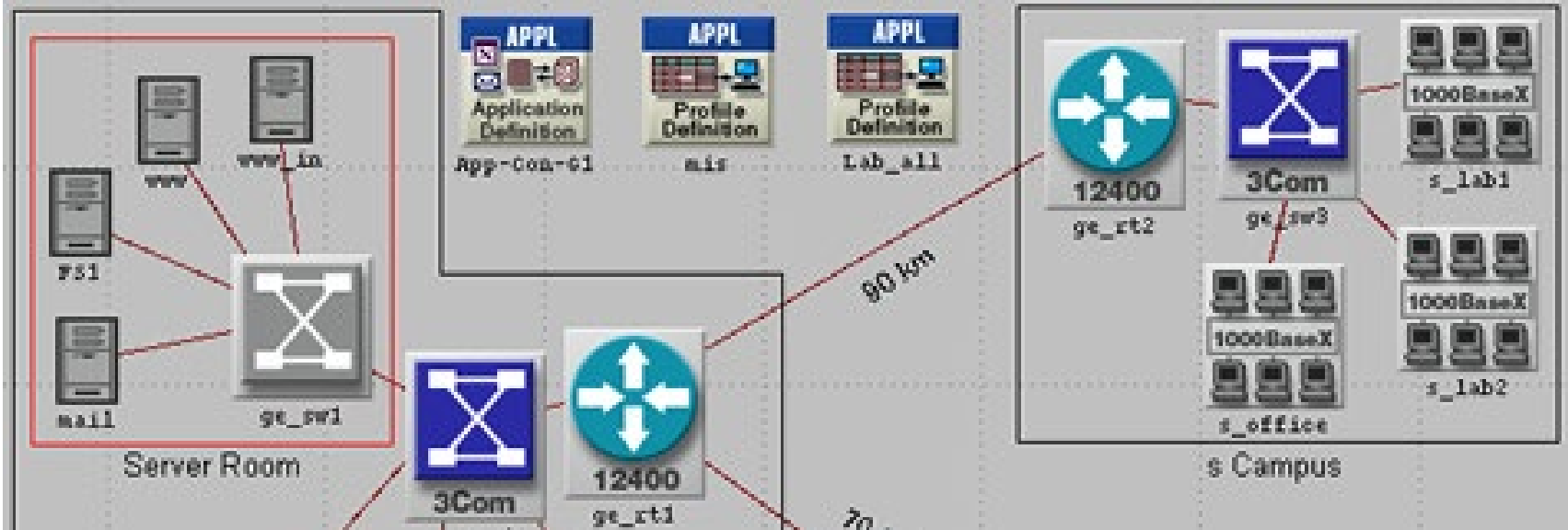
Late lab reports will not be accepted, unless a prior arrangement is made with the instructor.

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!



riverbed

Download ▶

Activate License ▶

Welcome to the
Riverbed's Modeler Academic Community

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

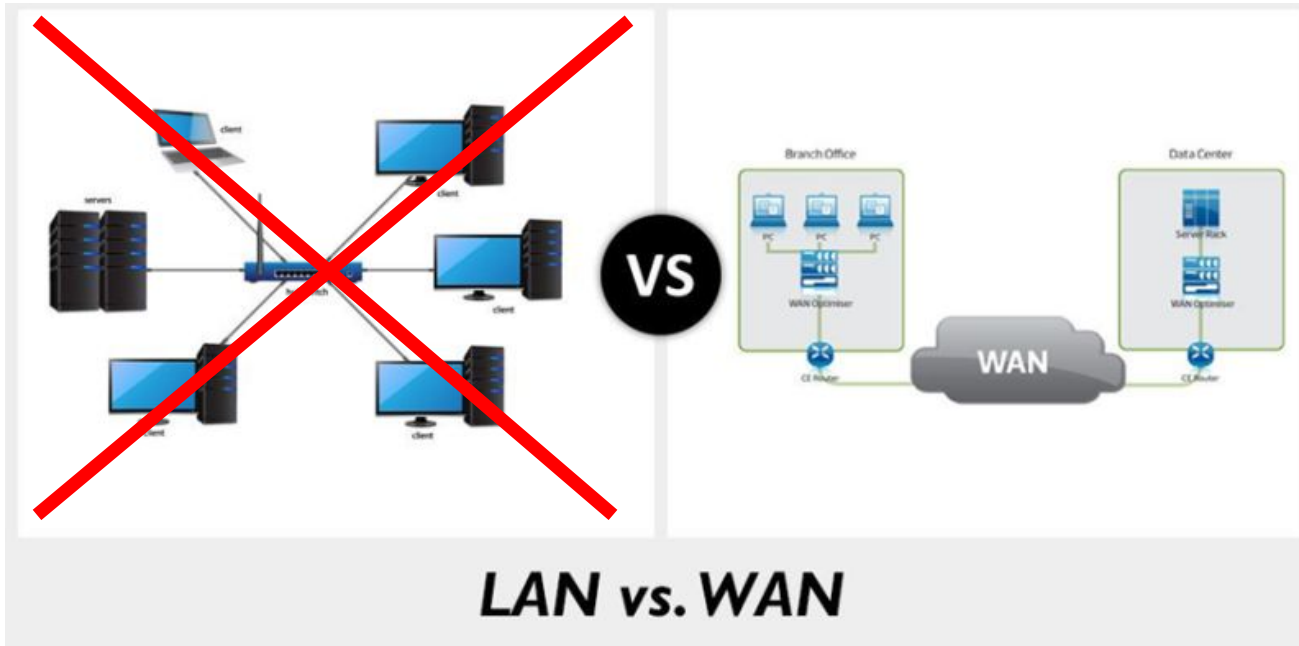
Telnet

P2P

Network Security

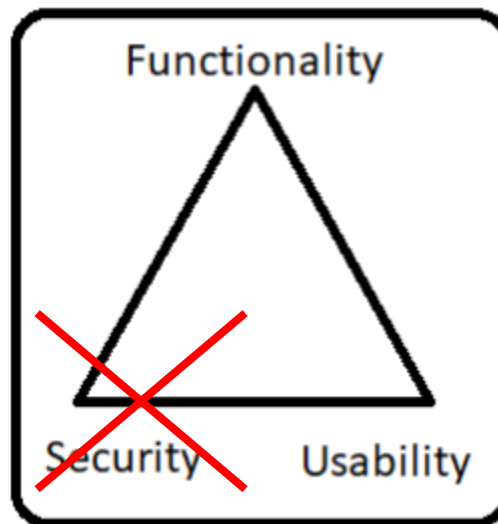
What this course is and is not about ...

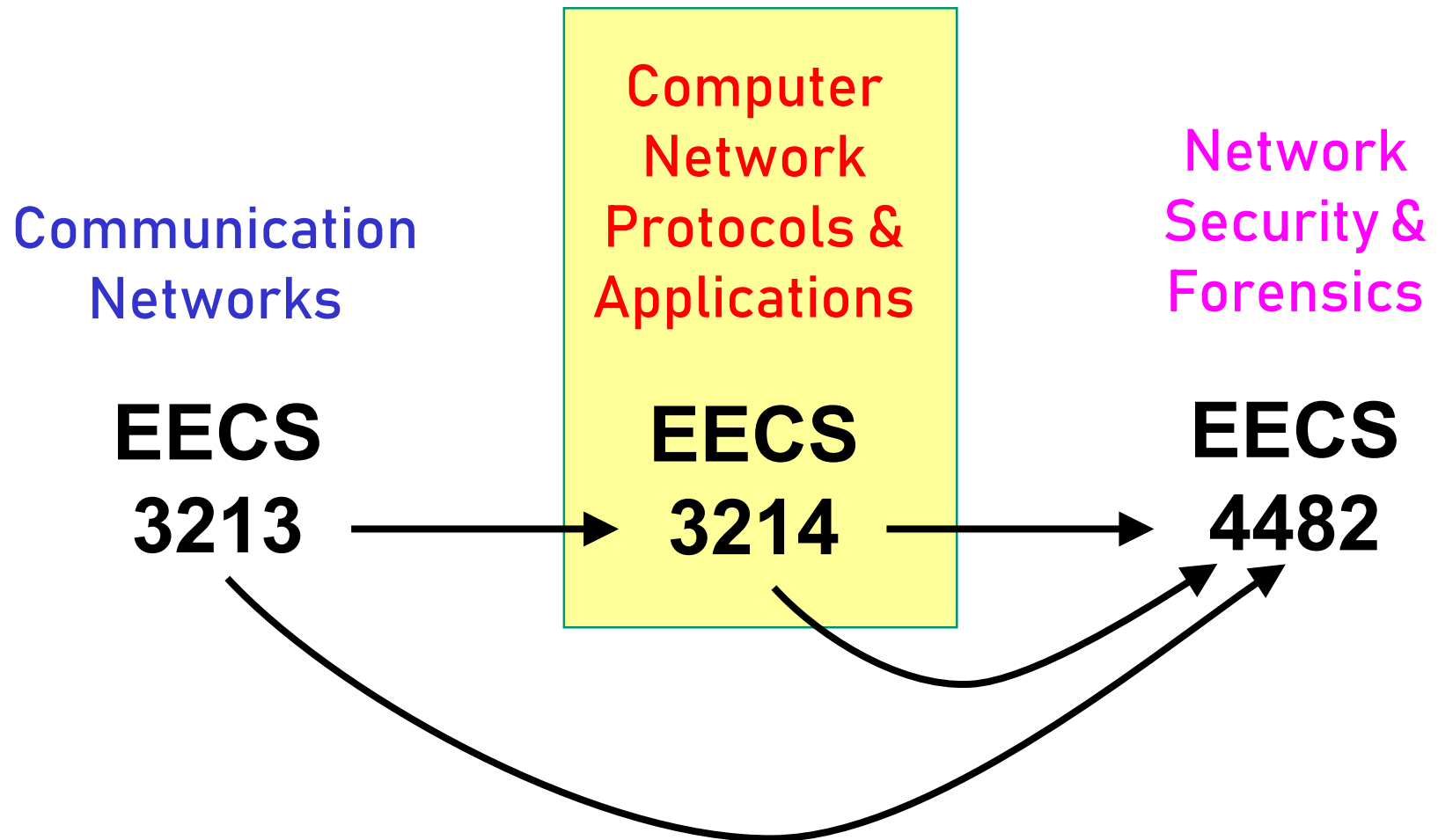
EECS
3213



EECS
3214

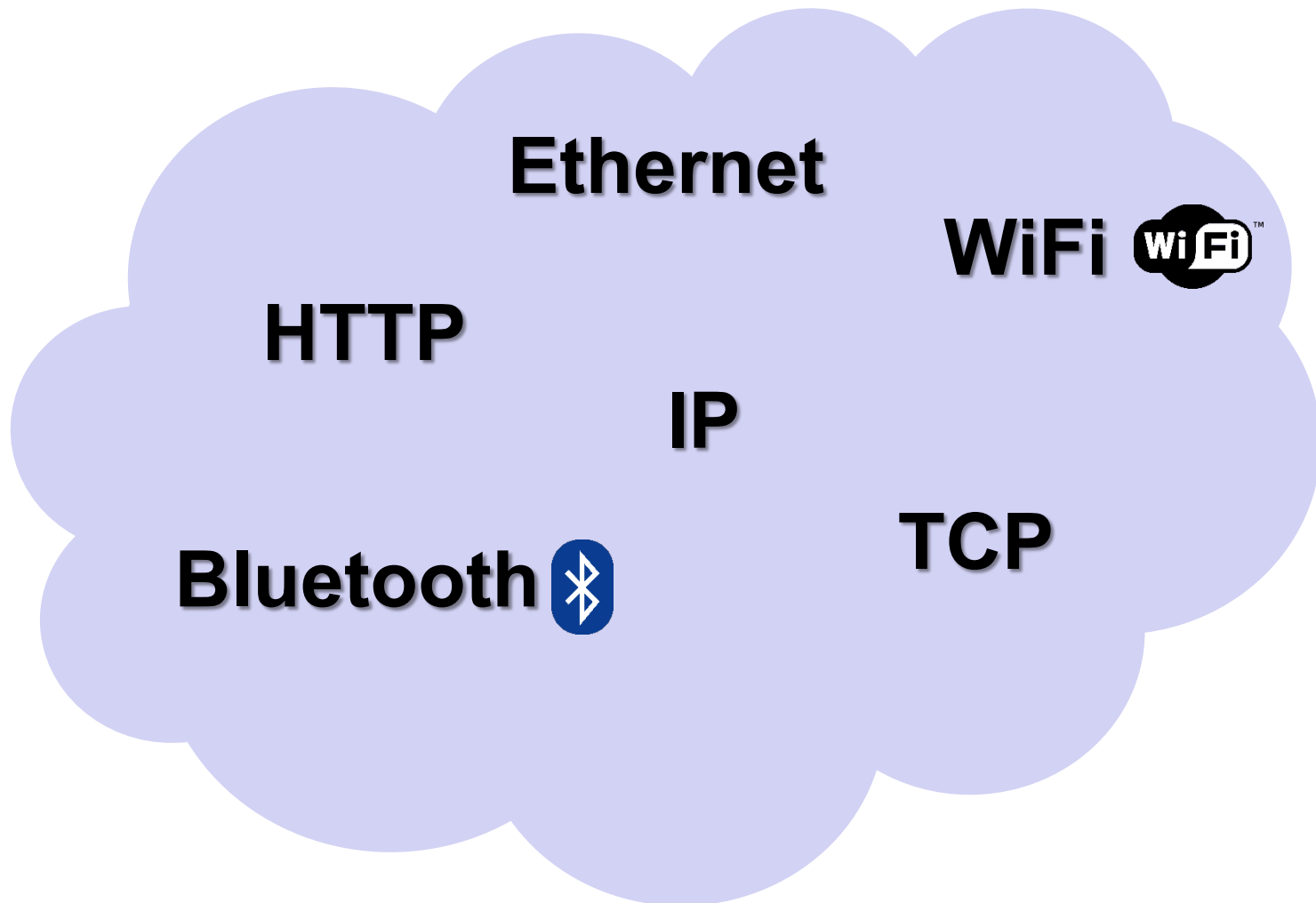
EECS
4482





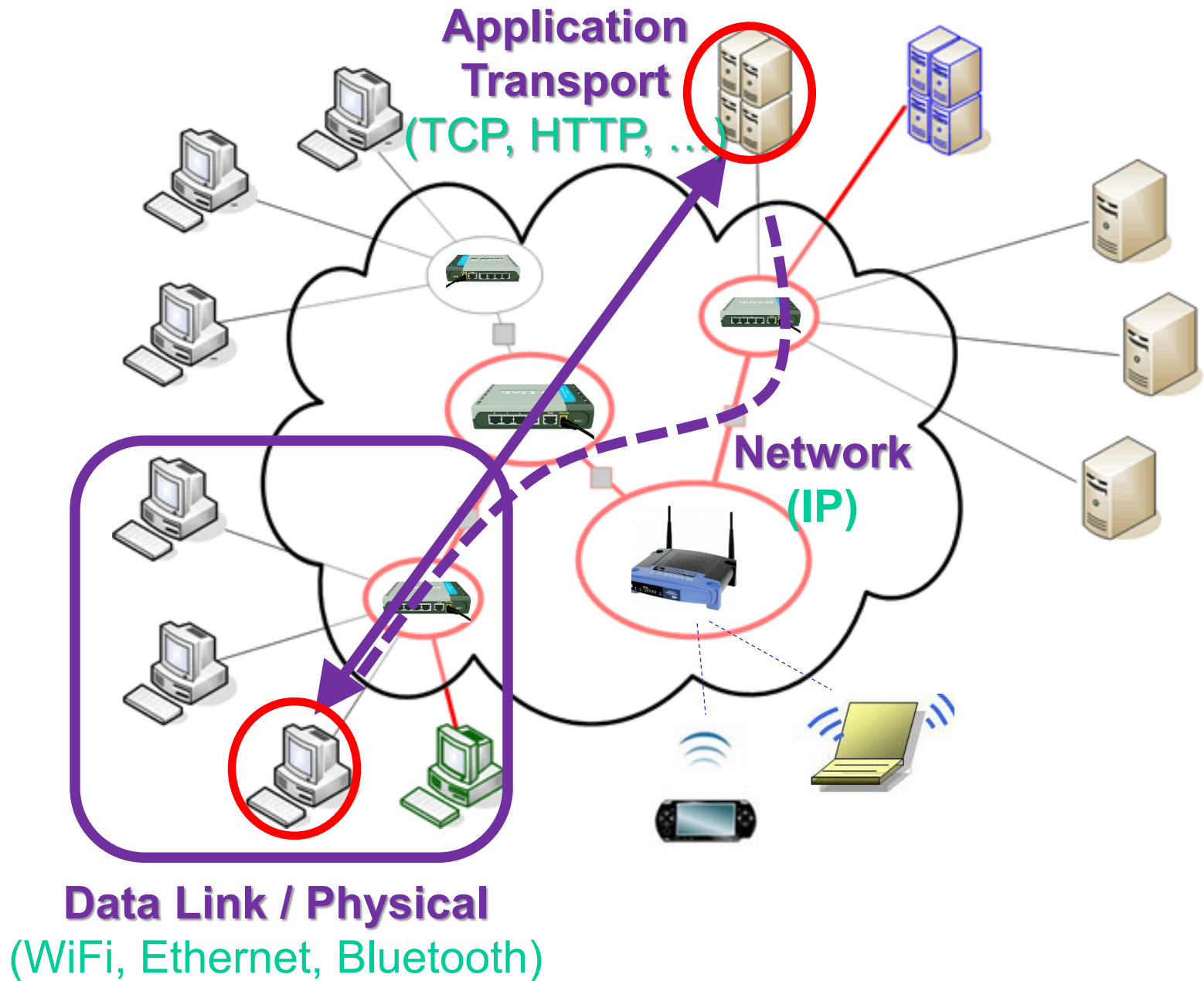
There is overlap among networking courses!

Big Picture



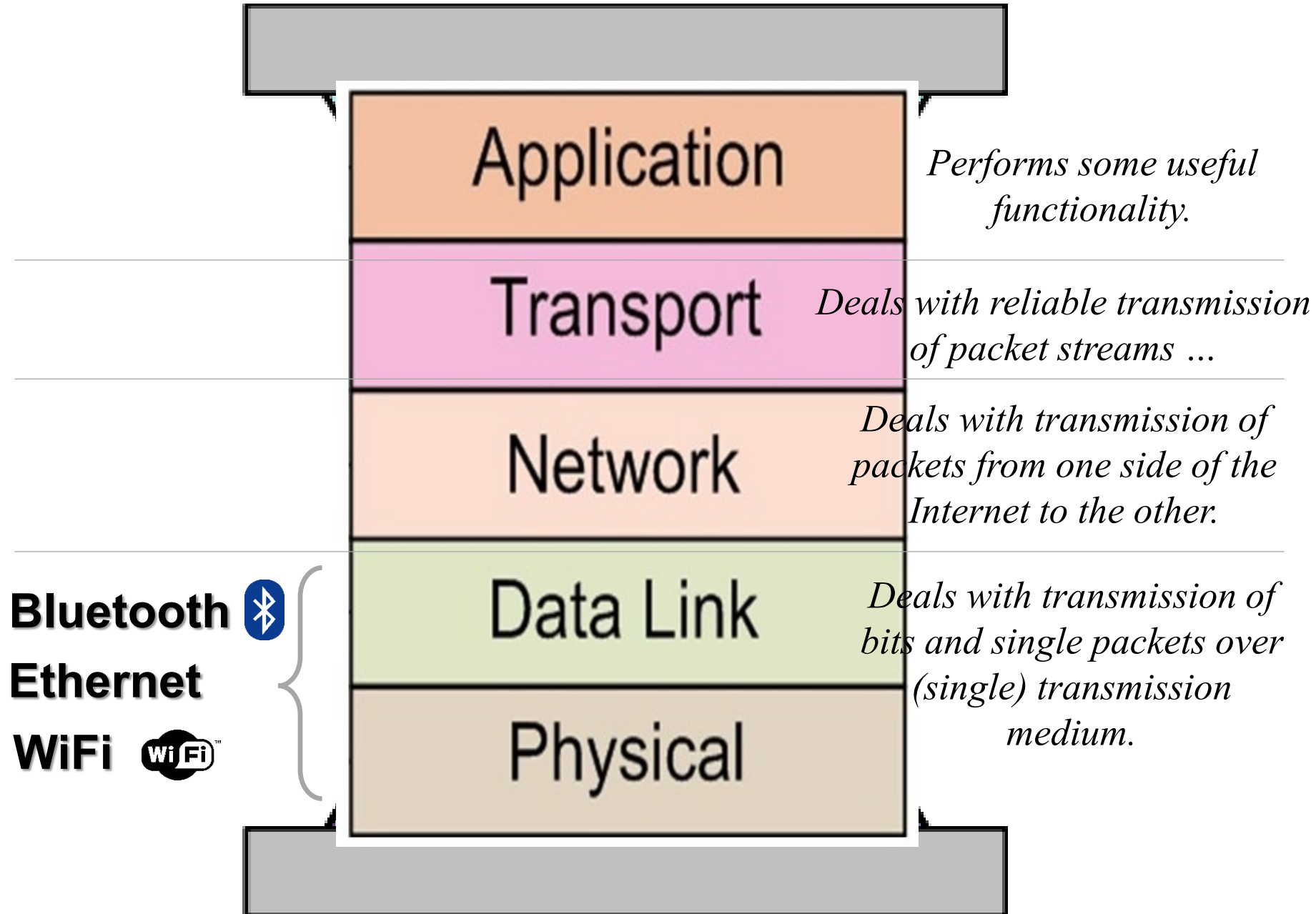
No single protocol/standard is sufficient for computer communication – they each are just ‘a piece of a bigger picture/puzzle’ ...





Internet Hourglass Model

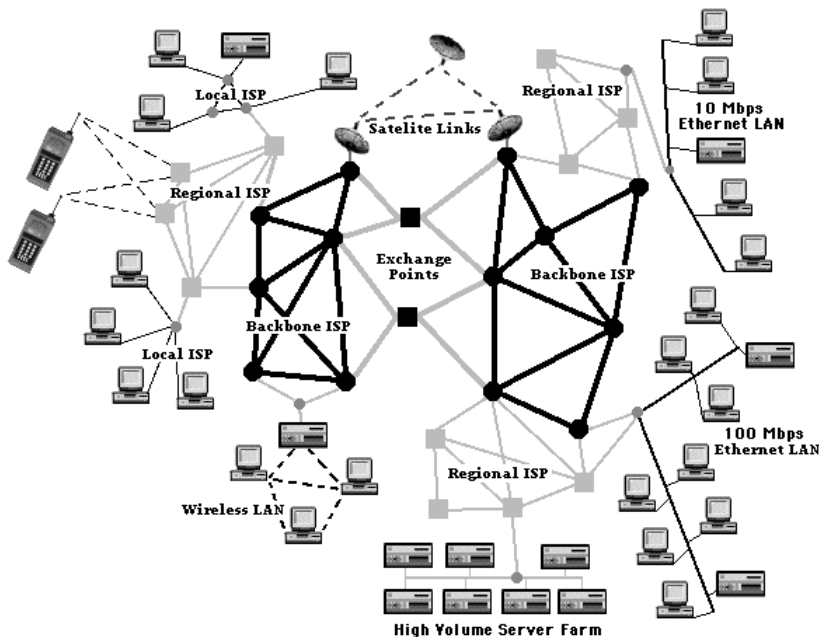
10

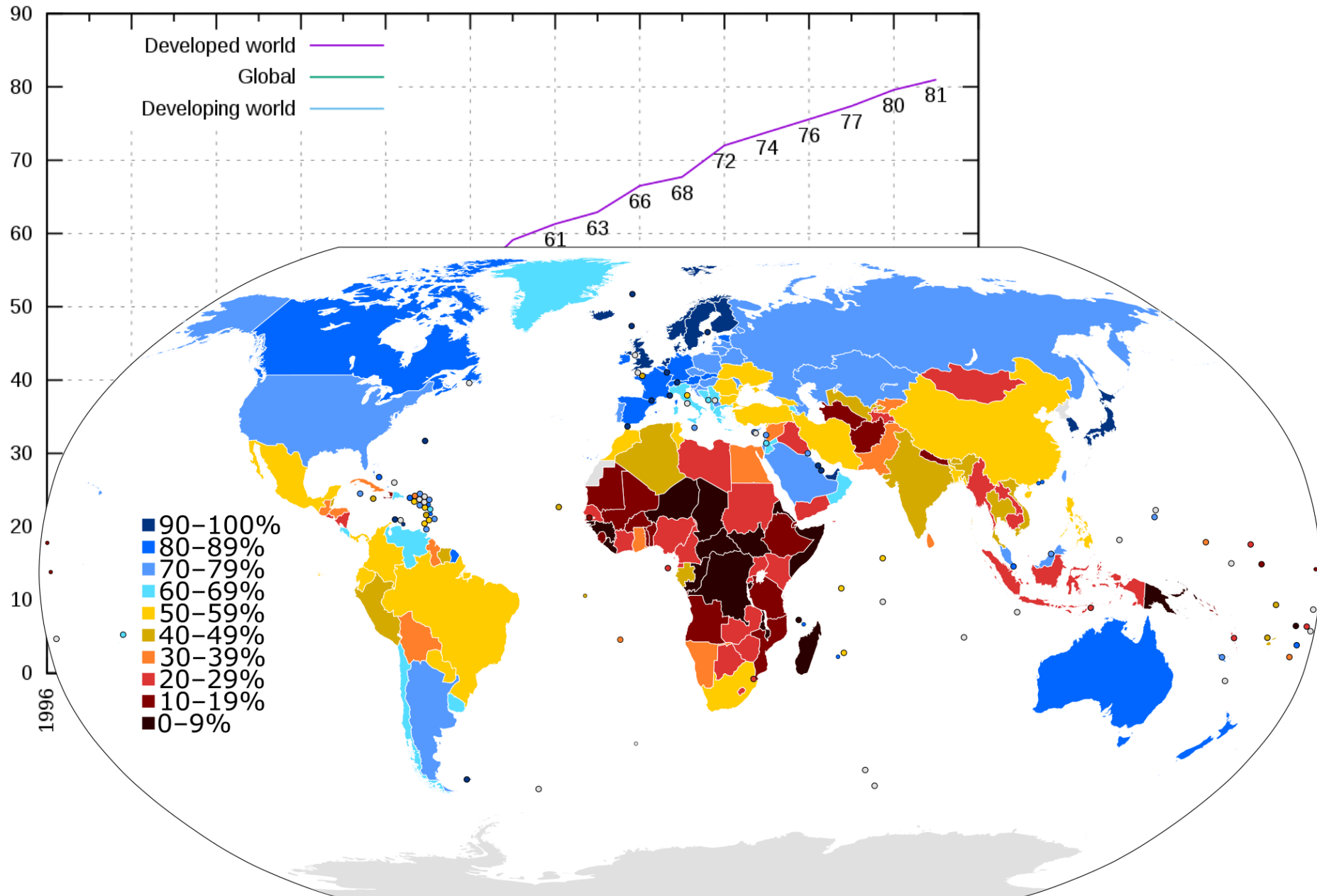


The Internet

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 ...

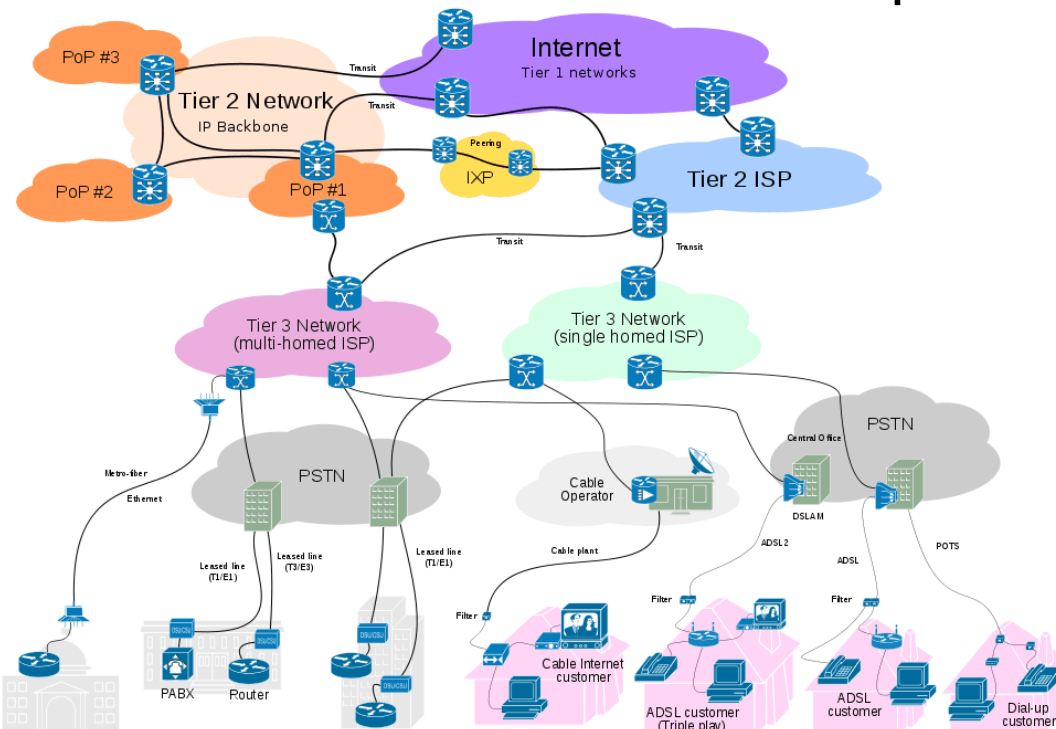




Internet Service Provider (ISP)

– 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

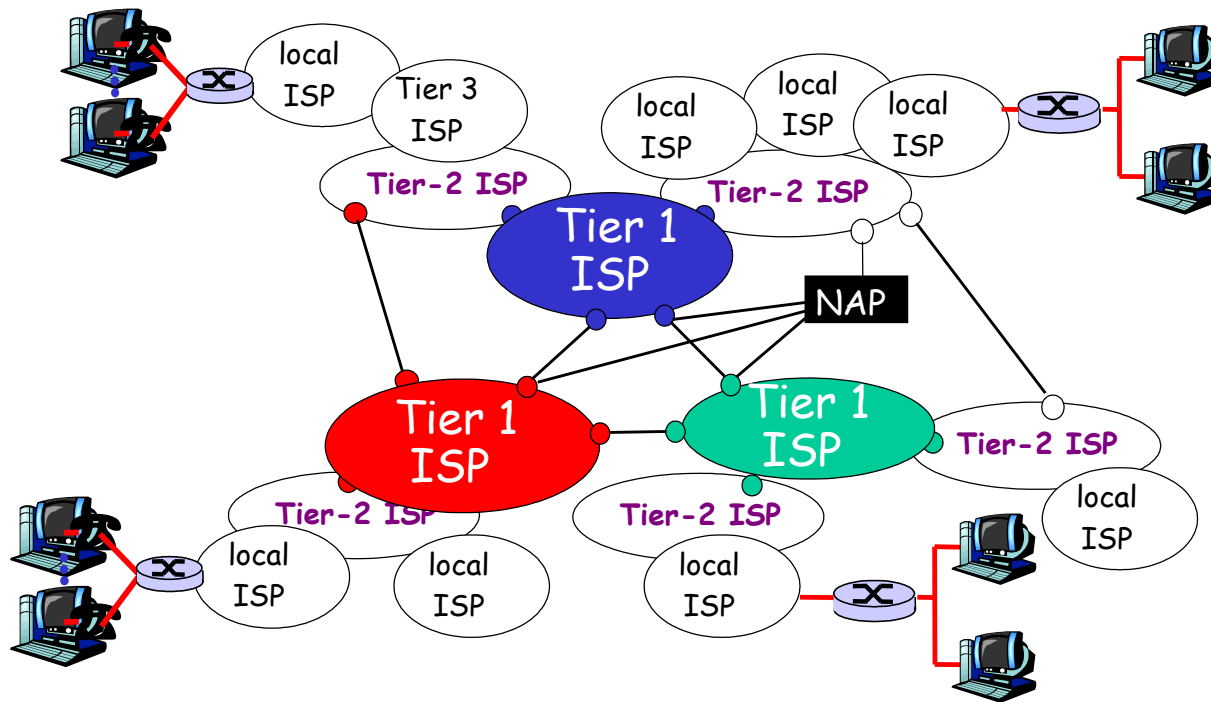


Example [routers]

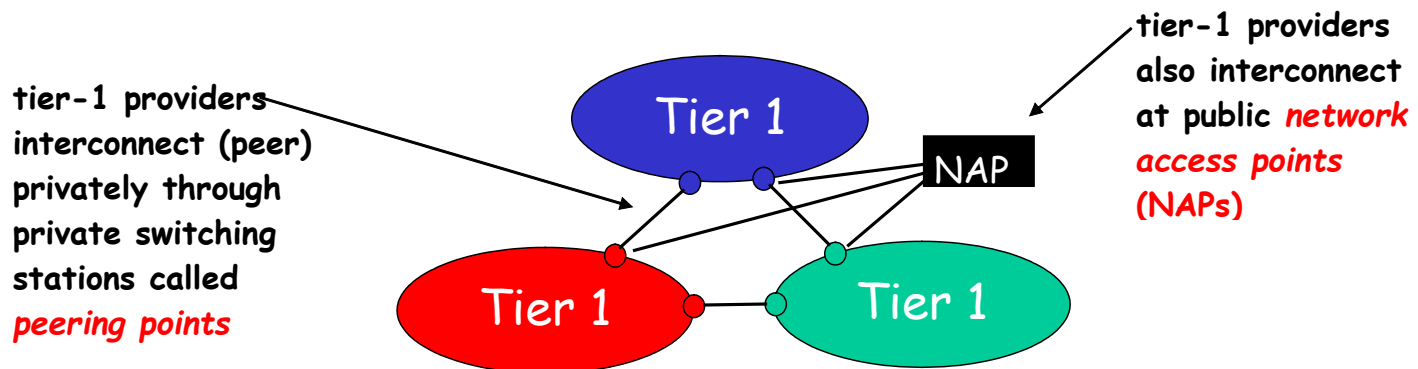


3-tiered Hierarchy of ISPs

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

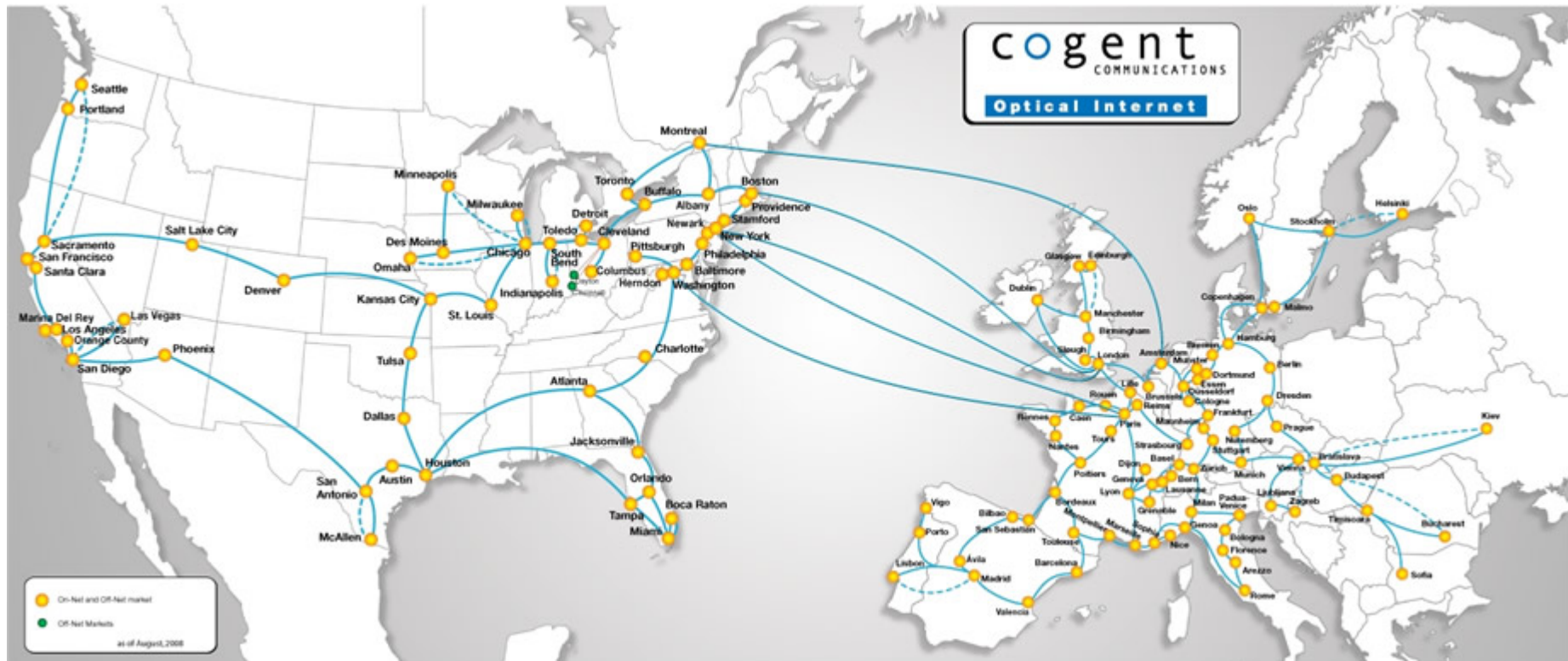


- International ISP** – Internet backbone network – one of the networks at the top of ISP-hierarchy – **has international coverage** (e.g. AT&T, CenturyLink, Sprint, Orangetheory, Tata Comm, Cogent)
- look similar to any other network (links + routers), but link speeds of 100+ Gbps - routers must be 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



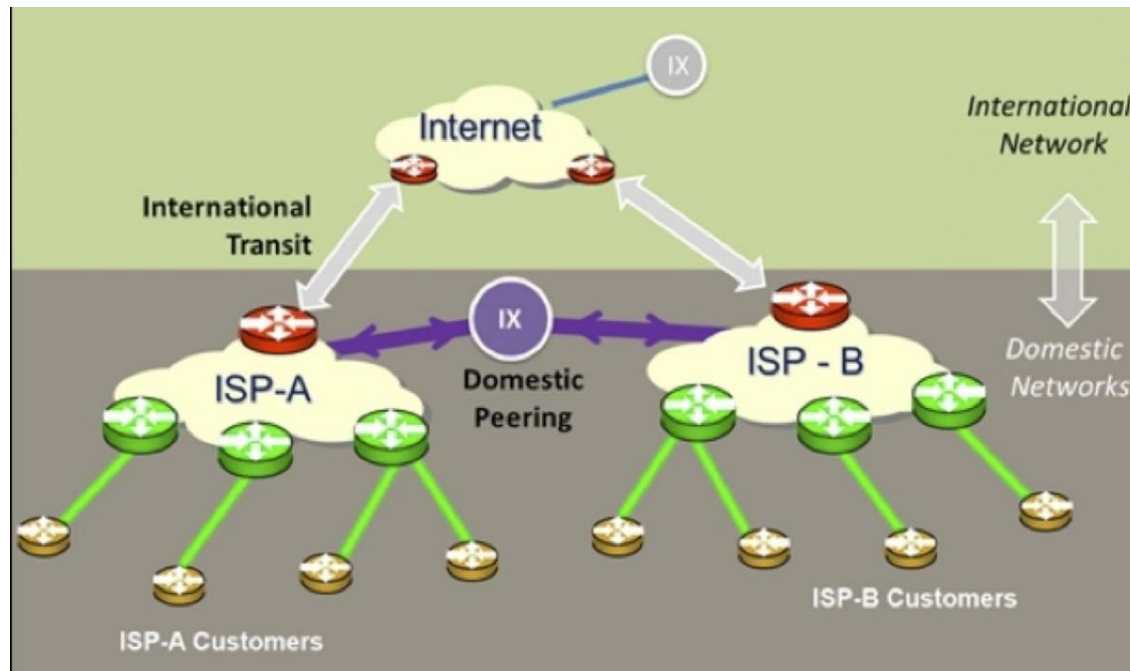
Example [Cogent Network Map]

“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.”



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

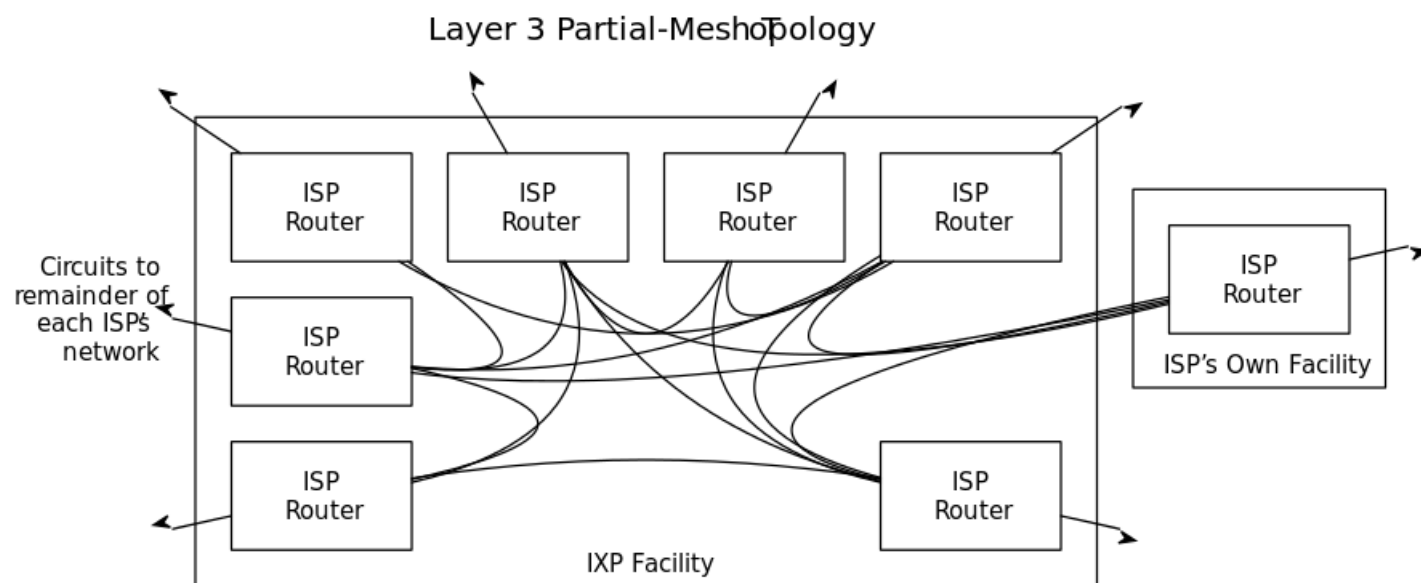
Internet Exchange Point (IXP) – new term/concept = **physical infrastructure** through which different IP networks (ISP, CDN, etc.) exchange traffic directly



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.

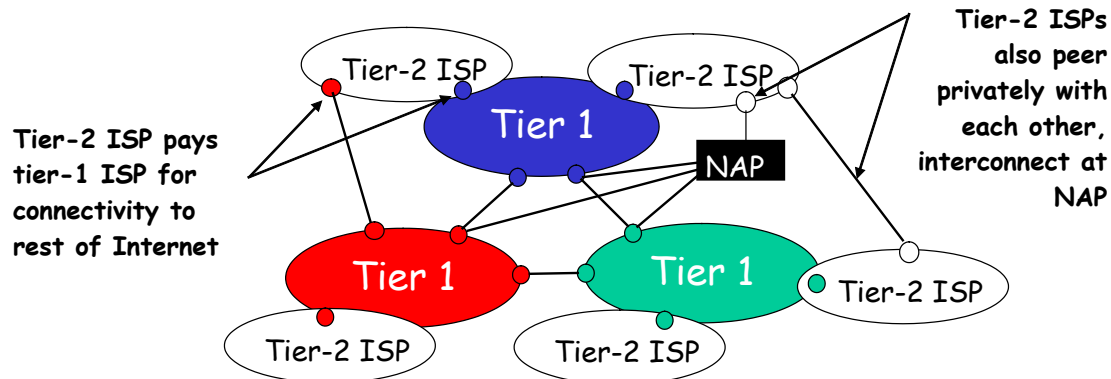


The main building of the London Internet Exchange (LINX)



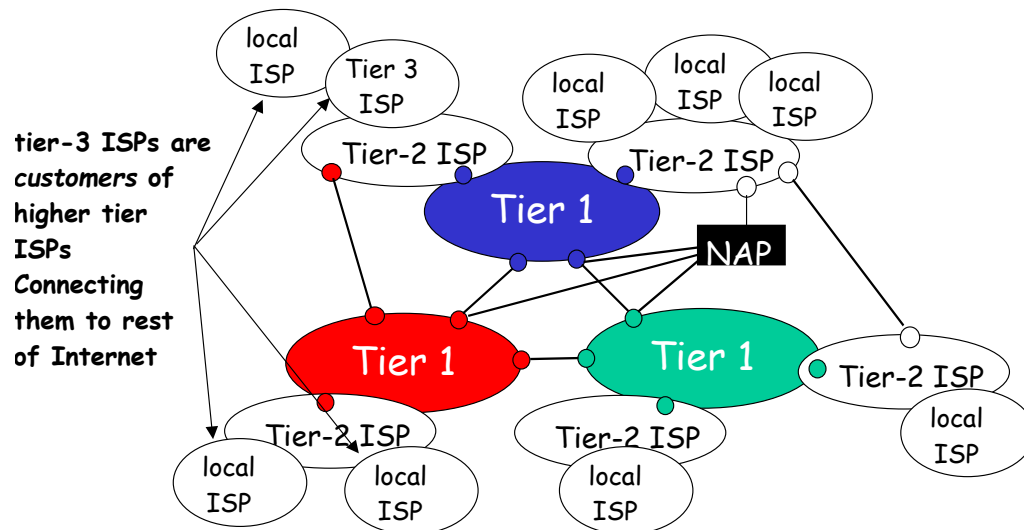
Regional ISP – smaller ISP that connects to one or more tier-1 ISPs and possibly other tier-2 ISPs – **have national coverage** (e.g. Bell, Rogers)

- 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, ...)

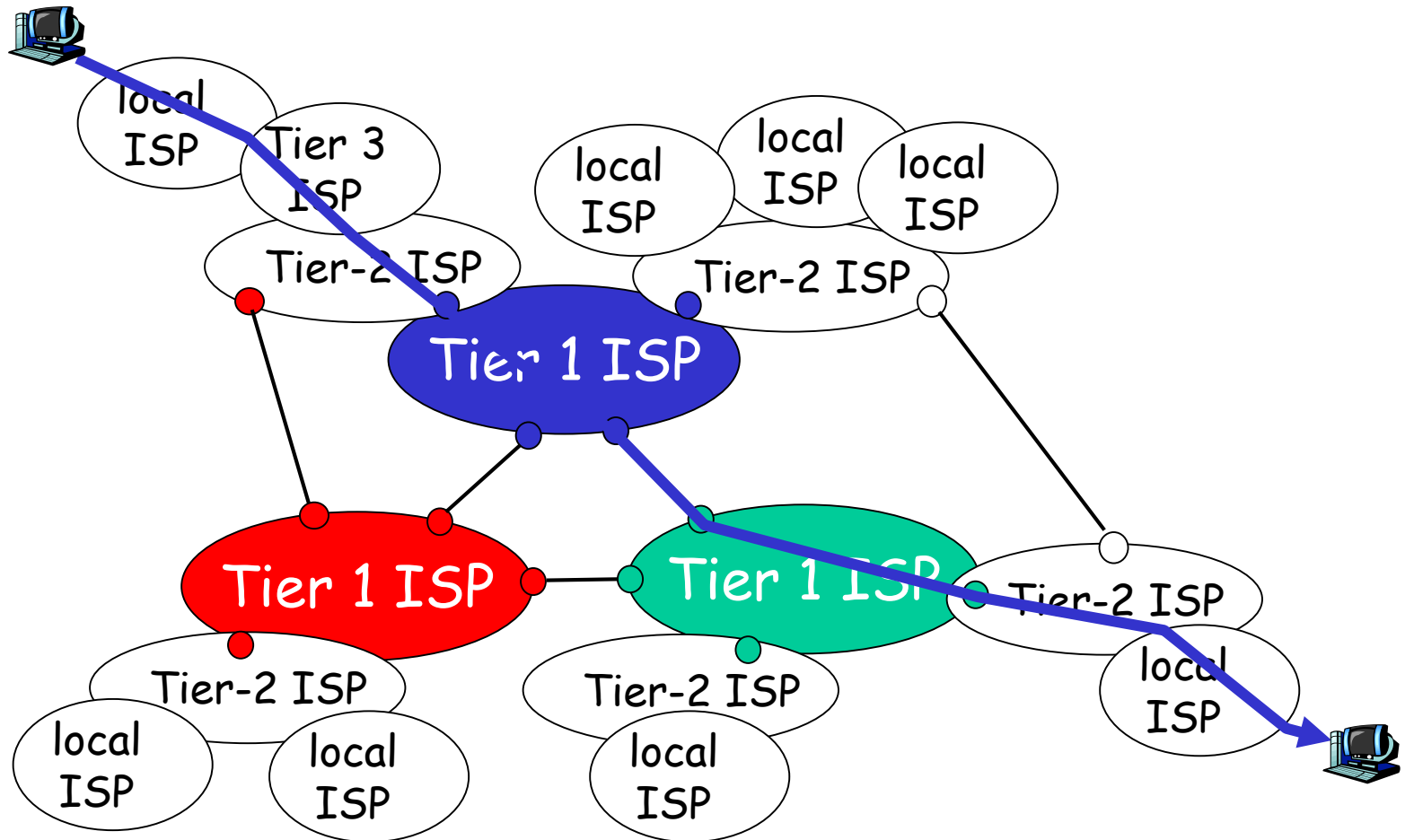


Local ISP – small ISP that connects to the Internet via one or more tier-2 ISPs and provides access to end users

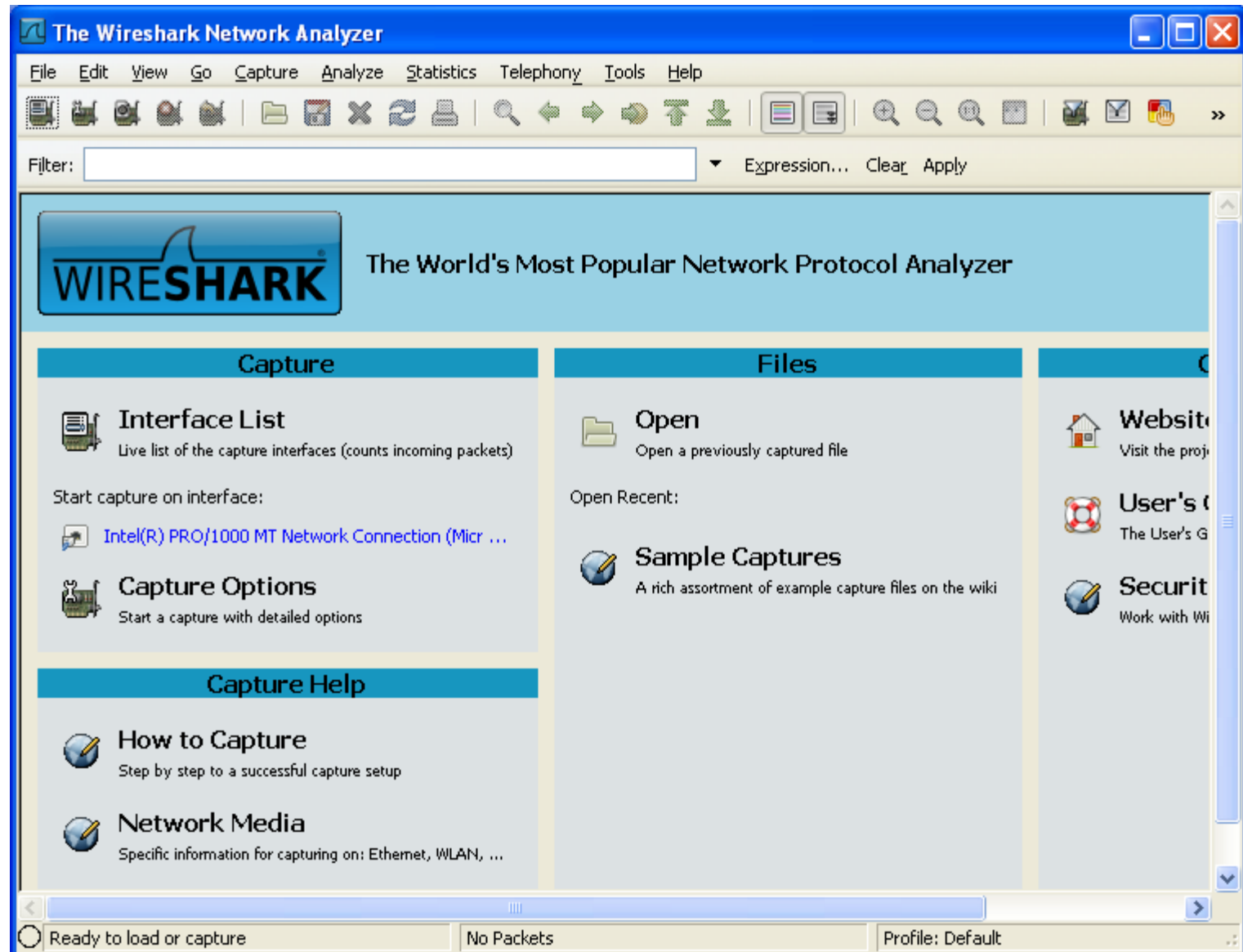
- local ISP can be
 - (1) company that just provides Internet service
 - (2) corporation that supplies service to its own employees
 - (3) college or university that runs its own network



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



Wireshark



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 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

26

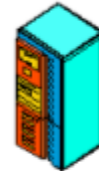
Example [retrieval of www.cnn.com web page]



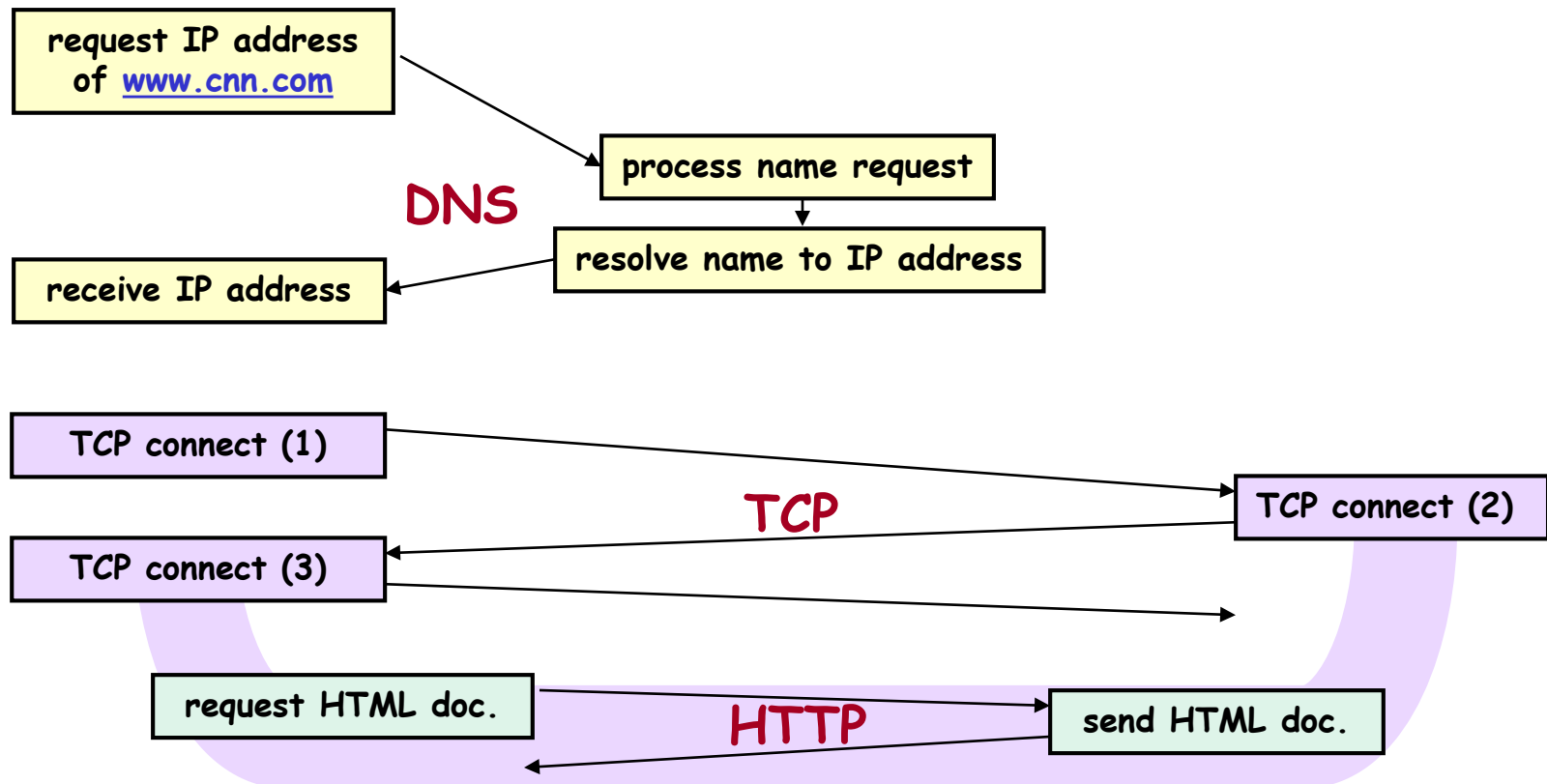
Human User



Name System

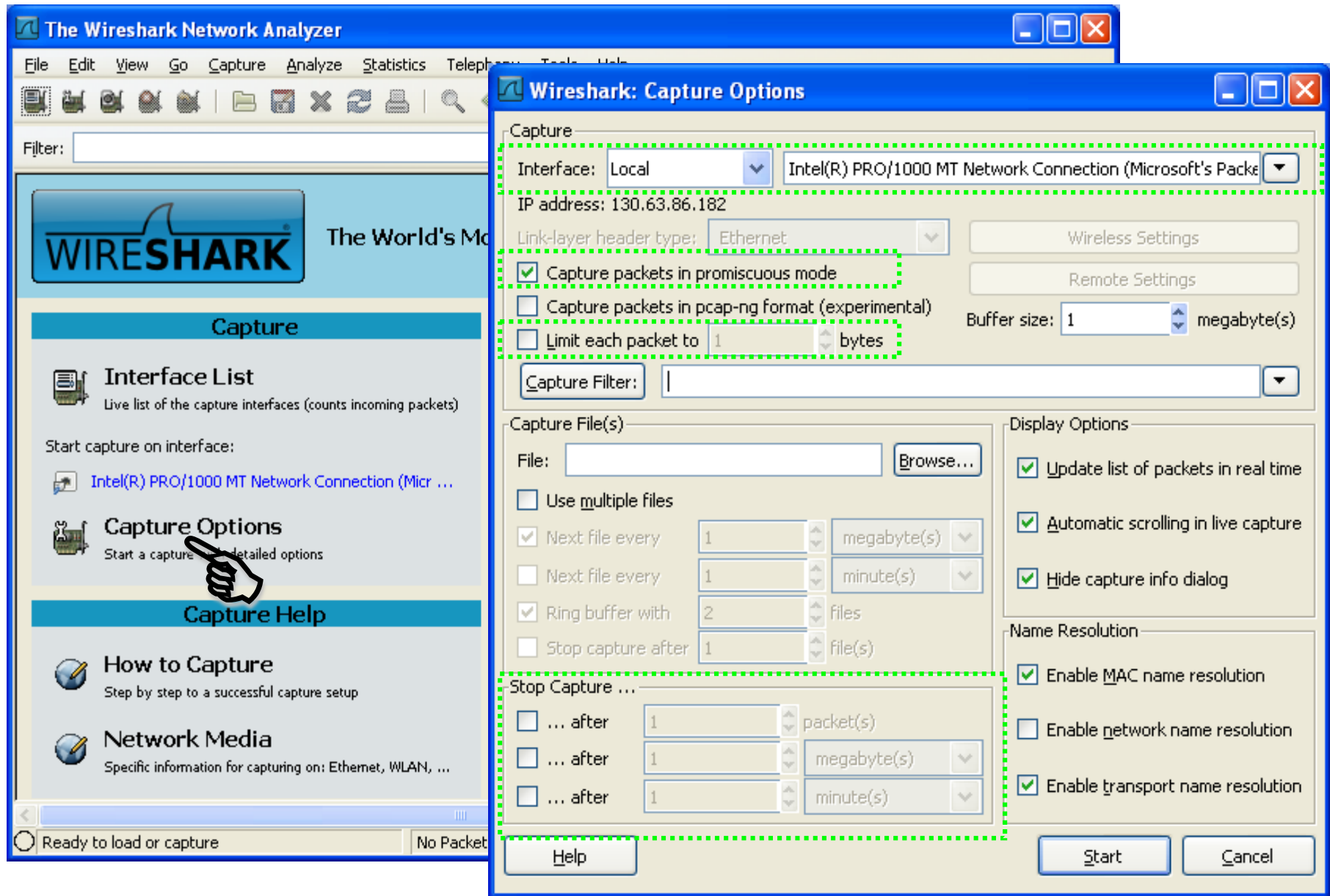


Server



Wireshark Network Analyzer (cont.)

27



Wireshark Display Window – captures traffic in three panes

The screenshot shows the Wireshark interface with the following components:

- Packet List:** A table of captured packets with columns for No., Time, Source, Destination, Protocol, and Info.
- Packet Details:** A tree-like structure showing the layers of the selected packet (Frame 4).
- Packet Bytes:** A pane showing the raw data in hexadecimal and ASCII.

No.	Time	Source	Destination	Protocol	Info
4	0.247321	130.63.86.182	130.63.86.28	DNS	Standard query A www.cnn.c
5	0.292557	130.63.86.28	130.63.86.182	DNS	Standard query response A 1
6	0.293786	130.63.86.182	157.166.224.25	TCP	izm > http [SYN, Seq=0 win=
7	0.337547	157.166.224.25	130.63.86.182	TCP	http > izm [SYN, ACK] Seq=0
8	0.337589	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=1 Ack=
9	0.337718	130.63.86.182	157.166.224.25	HTTP	GET / HTTP/1.1
10	0.381562	157.166.224.25	130.63.86.182	TCP	http > izm [ACK] Seq=1 Ack=
11	0.381791	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembl
12	0.382042	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembl
13	0.382068	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ac
14	0.425582	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembl
15	0.425814	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembl
16	0.425836	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ac
17	0.425846	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled
18	0.469601	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled
19	0.469640	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ac

Frame 4 (71 bytes on wire, 71 bytes captured)

- Ethernet II, Src: DellPcba_1f:4f:2e (00:0d:56:1f:4f:2e), Dst: IntelCor_63:3a:b5 (00:15:17:63:3a:b5)
- Internet Protocol, Src: 130.63.86.182 (130.63.86.182), Dst: 130.63.86.28 (130.63.86.28)
- User Datagram Protocol, Src Port: td-postman (1049), Dst Port: domain (53)
- Domain Name System (query)

Packet Bytes:

```
0000  00 15 17 63 3a b5 00 0d 56 1f
0010  00 39 4c 10 00 00 80 11 00 00 82 3f 56 b6 82 3f
0020  56 1c 04 19 00 35 00 25 00 b8 e6 bb 01 00 00 01
0030  00 00 00 00 00 00 03 77 77 77 03 63 6e 6e 03 63
0040  6f 6d 00 00 01 00 01
```

Packet Details:

9L.....?V..?
v....5.%.....
.....w ww.cnn.c
om.....

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.)

29

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
4	0.247321	130.63.86.182	130.63.86.28	DNS	standard query A www.cnn.com
5	0.292557	130.63.86.28	130.63.86.182	DNS	standard query response A 157.166.224.25
6	0.293786	130.63.86.182	157.166.224.25	TCP	izm > http [SYN] Seq=0 win=64240 Len=0 MS
7	0.337547	157.166.224.25	130.63.86.182	TCP	http > izm [SYN, ACK] Seq=0 Ack=1 win=146
8	0.337589	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=1 Ack=1 win=64240 Le
9	0.337718	130.63.86.182	157.166.224.25	HTTP	GET / HTTP/1.1
10	0.381562	157.166.224.25	130.63.86.182	TCP	http > izm [ACK] Seq=1 Ack=647 win=7106 L
11	0.381791	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
12	0.382042	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
13	0.382068	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ack=2921 win=642
14	0.425582	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
15	0.425814	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
16	0.425836	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ack=5841 win=642
17	0.425846	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
18	0.469601	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
19	0.469640	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ack=8761 win=642
20	0.469832	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]

Frame 6 (62 bytes on wire, 62 bytes captured)

Ethernet II, Src: DellPcba_1f:4f:2e (00:0d:56:1f:4f:2e), Dst: Cisco_40:15:0a (00:0c:cf:40:15:0a)

Internet Protocol, Src: 130.63.86.182 (130.63.86.182), Dst: 157.166.224.25 (157.166.224.25)

Transmission Control Protocol, Src Port: izm (4109), Dst Port: http (80), Seq: 0, Len: 0

0000 00 0c cf 40 15 0a 00 0d 56 1f 4f 2e 08 00 45 00

Wireshark Network Analyzer (cont.)

Wireshark Display Filter Feature

myShark.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: **dns** Expression... Clear Apply

No. ↓	Time	Source	Destination	Protocol	Info
4	0.241111	130.63.86.182	130.63.86.28	DNS	Standard query A www.cnn.com
5	0.292557	130.63.86.28	130.63.86.182	DNS	Standard query response A 157.166.224.25 A 157.166.224.26 A
42	2.150834	130.63.86.182	130.63.86.28	DNS	Standard query A i.cdn.turner.com
43	2.232249	130.63.86.28	130.63.86.182	DNS	Standard query response CNAME cdn.cnn.com.c.footprint.net A
264	2.860016	130.63.86.182	130.63.86.28	DNS	Standard query A es.optimost.com
265	2.863324	130.63.86.28	130.63.86.182	DNS	Standard query response CNAME by.optimost.com.edgesuite.net
313	3.194240	130.63.86.182	130.63.86.28	DNS	Standard query A ads.cnn.com
314	3.241975	130.63.86.28	130.63.86.182	DNS	Standard query response A 157.166.255.12
352	3.483611	130.63.86.182	130.63.86.28	DNS	Standard query A i2.cdn.turner.com
353	3.483942	130.63.86.28	130.63.86.182	DNS	Standard query response CNAME cdn.cnn.com.c.footprint.net A
1191	5.498856	130.63.86.182	130.63.86.28	DNS	Standard query A pagead2.googleadsyndication.com
1212	5.523125	130.63.86.28	130.63.86.182	DNS	Standard query response CNAME pagead.l.google.com A 64.233.1
1283	6.190362	130.63.86.182	130.63.86.28	DNS	Standard query A googleads.g.doubleclick.net
1292	6.214254	130.63.86.28	130.63.86.182	DNS	Standard query response CNAME pagead.l.doubleclick.net A 64.

myShark.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter: **tcp** Expression... Clear Apply

No. ↓	Time	Source	Destination	Protocol	Info
6	0.292706	130.63.86.182	157.166.224.25	TCP	izm > http [SYN] Seq=0 win=64240 Len=0 MSS=1460
7	0.337547	157.166.224.25	130.63.86.182	TCP	http > izm [SYN, ACK] Seq=0 Ack=1 win=1460 Len=0 MSS=1460
8	0.337589	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=1 Ack=1 win=64240 Len=0
9	0.337718	130.63.86.182	157.166.224.25	HTTP	GET / HTTP/1.1
10	0.381562	157.166.224.25	130.63.86.182	TCP	http > izm [ACK] Seq=1 Ack=647 win=7106 Len=0
11	0.381791	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
12	0.382042	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]
13	0.382068	130.63.86.182	157.166.224.25	TCP	izm > http [ACK] Seq=647 Ack=2921 win=64240 Len=0
14	0.425582	157.166.224.25	130.63.86.182	TCP	[TCP segment of a reassembled PDU]

Wireshark Statistics Summary Feature

myShark.pcap - Wireshark

File Edit View Go Capture Analyze Statistics Telephony Tools Help

Filter:

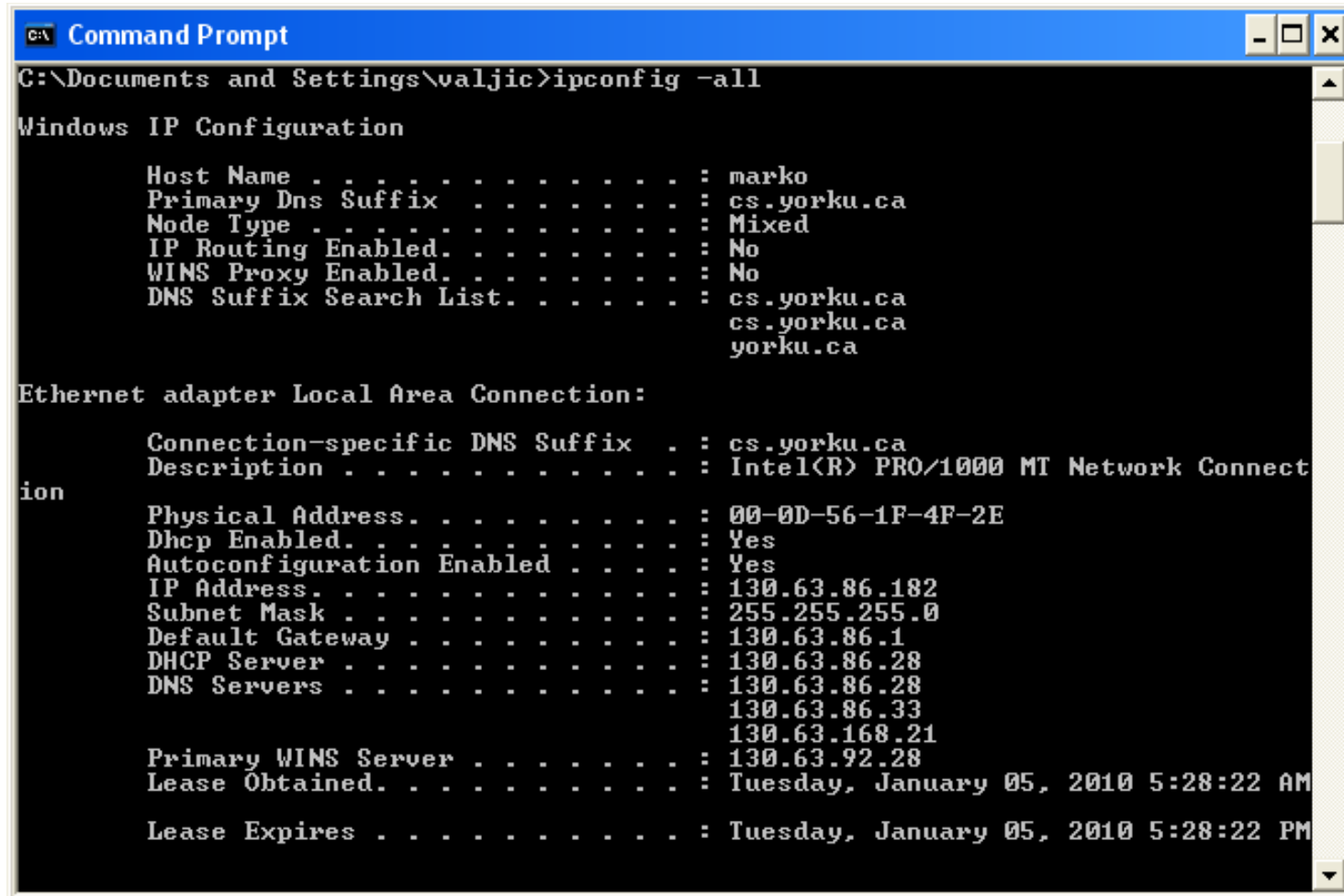
Wireshark: Protocol Hierarchy Statistics

Display filter: none

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

Help Close

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



```
C:\> Command Prompt
C:\Documents and Settings\valjic>ipconfig -all

Windows IP Configuration

    Host Name . . . . . : marko
    Primary Dns Suffix . . . . . : cs.yorku.ca
    Node Type . . . . . : Mixed
    IP Routing Enabled. . . . . : No
    WINS Proxy Enabled. . . . . : No
    DNS Suffix Search List. . . . . : cs.yorku.ca
                                      cs.yorku.ca
                                      yorku.ca

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : cs.yorku.ca
    Description . . . . . : Intel(R) PRO/1000 MT Network Connect
ion
    Physical Address. . . . . : 00-0D-56-1F-4F-2E
    Dhcp Enabled. . . . . : Yes
    Autoconfiguration Enabled . . . . : Yes
    IP Address. . . . . : 130.63.86.182
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 130.63.86.1
    DHCP Server . . . . . : 130.63.86.28
    DNS Servers . . . . . : 130.63.86.28
                           130.63.86.33
                           130.63.168.21
    Primary WINS Server . . . . . : 130.63.92.28
    Lease Obtained. . . . . : Tuesday, January 05, 2010 5:28:22 AM
    Lease Expires . . . . . : Tuesday, January 05, 2010 5:28:22 PM
```