Romain Fontugne

2023 Fall Semester

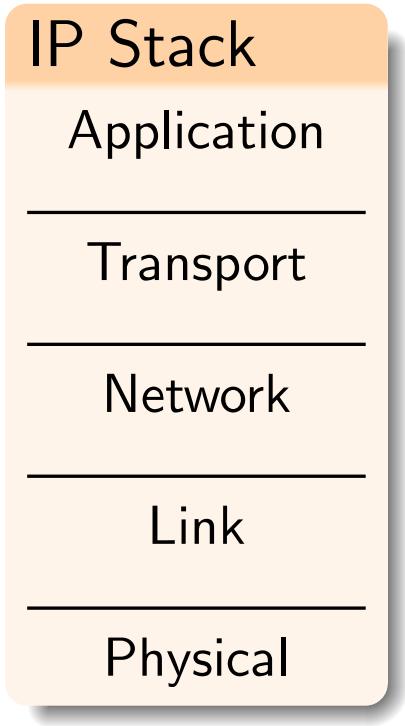
Information Network Systems

Network Monitoring

Up to now:

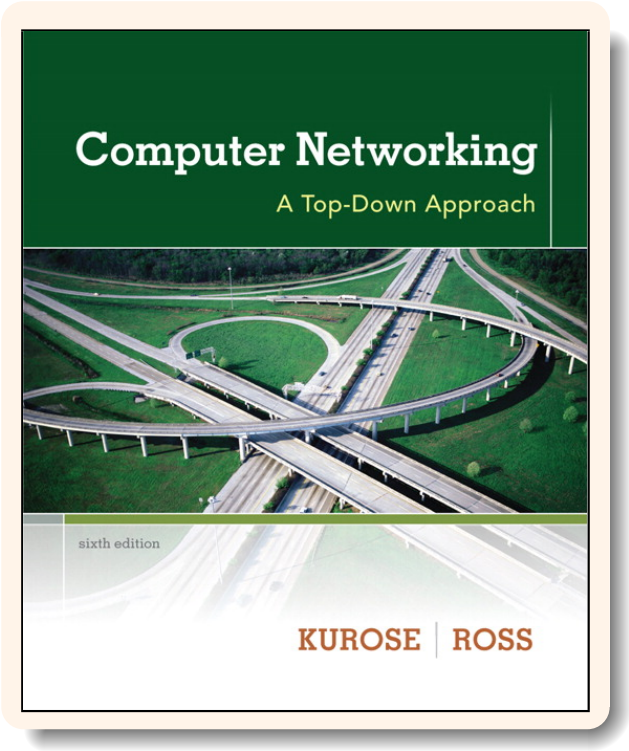
We've seen the protocol stack

- Fundamentals of Internet communications
- Details of each layer
- Main protocols used on Internet



Today's Lecture: Network Monitoring

1. Why Network Monitoring?
2. Device Monitoring
   - SNMP
3. Traffic Monitoring
   - Tcpdump and Wireshark
   - Netflow
4. Other useful stuff



Principles of Network Management

Introduction

- Network components will occasionally malfunction
- Network operators need tools to monitor, manage and control the network

Network Management

- Deployment of the hardware and software
- Monitoring of the network
- Analysis of collected data
- Feedback (then reconfiguration or new deployments...)

Motivations for Network Monitoring

Essential for Network Management

- Router and Firewall policy
- Detecting abnormal/error in networking
- Access control

Security Management

- Detecting abnormal traffic
- Traffic log for future forensic analysis

$\rightarrow$ Ensure networks operate efficiently!

Network Monitoring

Two key components to monitor:

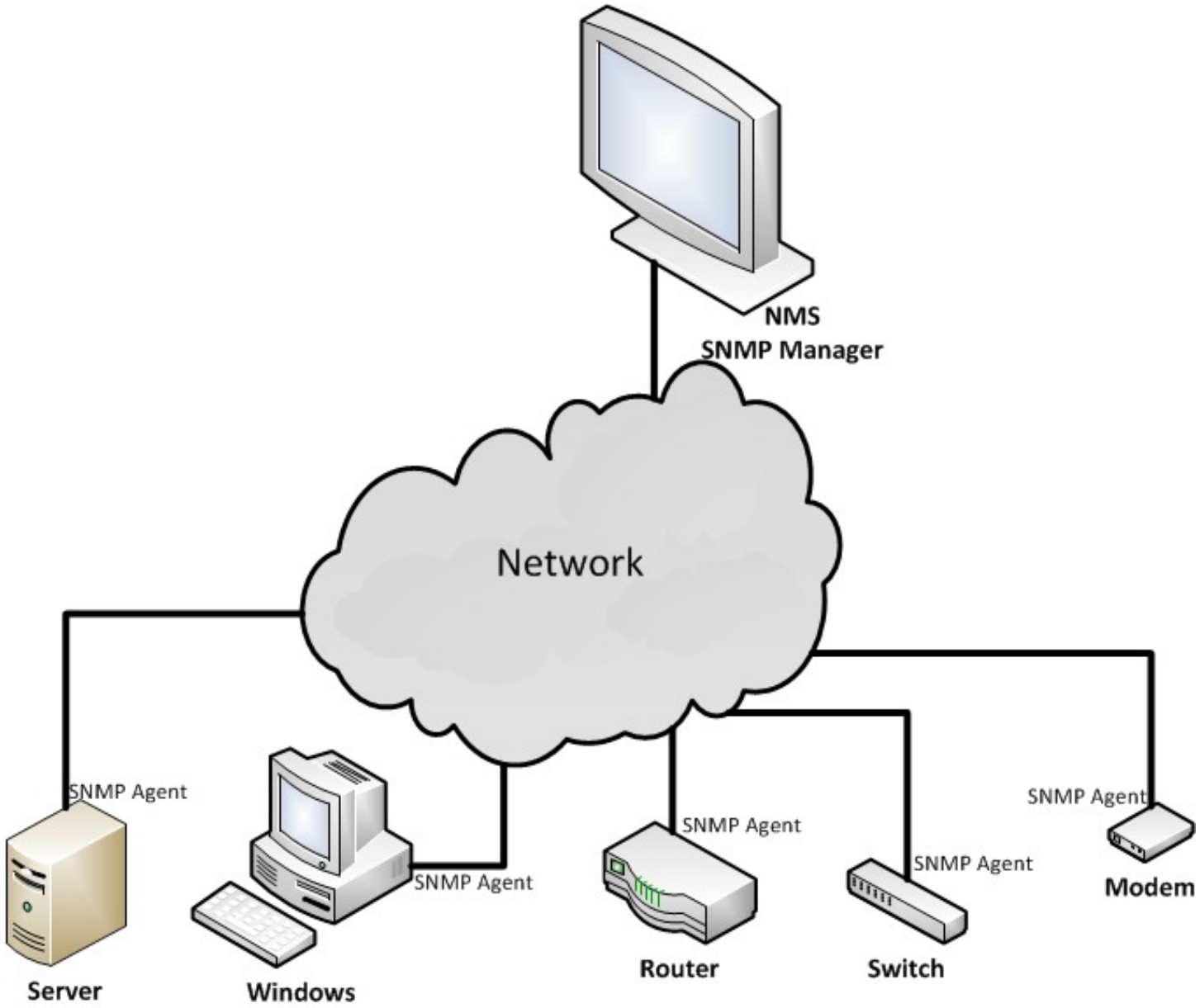
- Devices (e.g. routers, hosts, printers, ...)
  - simple network management protocol (SNMP)
- Traffic
  - packet/flow analysis: tcpdump, netflow

Simple Network Management Protocol (SNMP)

SNMP help collecting information about connected devices

- Uses port 161 and port 162 on UDP
- Each device run a program known as SNMP agent
- An agent collects information about a device
  e.g. link failures, traffic measures, ...
- Agents send data to an network management system (NMS)
  - NMS: centralized repository for information collected from managed devices
  - SNMP is a management protocol (not only monitoring): NMS also send commands to the agents

SNMP: Overview



SNMP Limitations for Monitoring Network Events

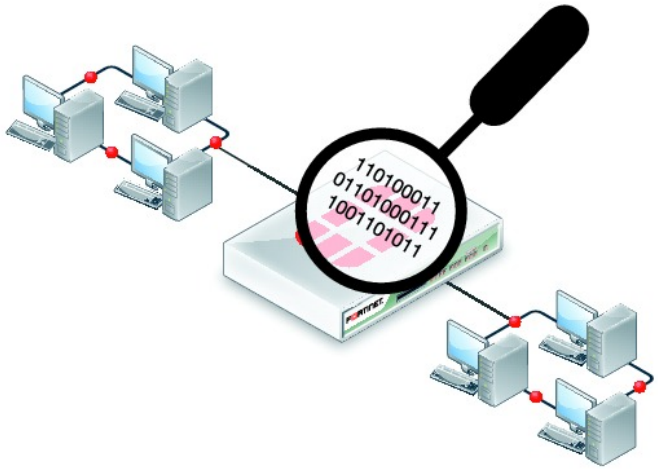
SNMP provides useful information about devices

- For example, report a router is receiving usually large volume of traffic
- Could be due to the failure of another router? remote attack? flash crowd?
- Difficult to find out only with SNMP as it reports only device related information
- Need detailed view of the traffic

Traffic Monitoring

Traffic Monitoring

- Monitor traffic between devices
- Really useful for:
  - Comprehensive view of network traffic
    e.g. to improve the performance of an application/network
  - Detecting abnormal events (a.k.a. network traffic anomalies)
    e.g. remote attacks, router failures
  - Debugging/detecting incorrect behavior



Network Traffic Anomaly

Major Types of Network traffic anomaly

Anomaly	Description
Alpha Flows	Large volume point to point flow
DoS	Distributed or single-source DoS attack
Flash Crowd	Unusual burst of traffic to single destination
Port Scan	Probes to many destination ports
Network scan	Probes to many destination addresses on particular ports
Outage events	Traffic shifts due to equipment failures or maintenance
Worms	Scanning for vulnerable hosts (similar to network scan)

Traffic Monitoring, Anomaly Detection: How it works?

Methodology

- Selection of key locations in the network (e.g. routers, end-hosts)
- Installation of monitoring devices/software also known as network taps
- Capturing and collecting traffic in a repository
- Analysis of the collected data

Tcpdump

The most popular tool for capturing packets

- Unix-based command-line tool used to intercept packets
- Reads “live traffic” from interface specified using -i option
- or from a previously recorded trace file specified using -r option (You create these when capturing live traffic using -w option)

Filtering:

- Include filtering to get just the packets of interest
- e.g. tcpdump -i eth0 ”(udp or tcp) and port 53”

Wireshark

GUI for tcpdump

- Much more user friendly
- Provide handy tools to navigate in the captured traffic

$\rightarrow$ demo

Nota bene:

Look at libpcap if you need a library to manipulate captured traffic in your programs

Netflow

Another useful way to capture traffic

- Collect IP flows (not packet)
- A flow can contain different information
  e.g. host and port src, host and port dst, number of packets and bytes, timestamps (start and end)
- Implemented in many routers
- Collecting flows compress/aggregate the collected traffic...
- ... but it loses some details

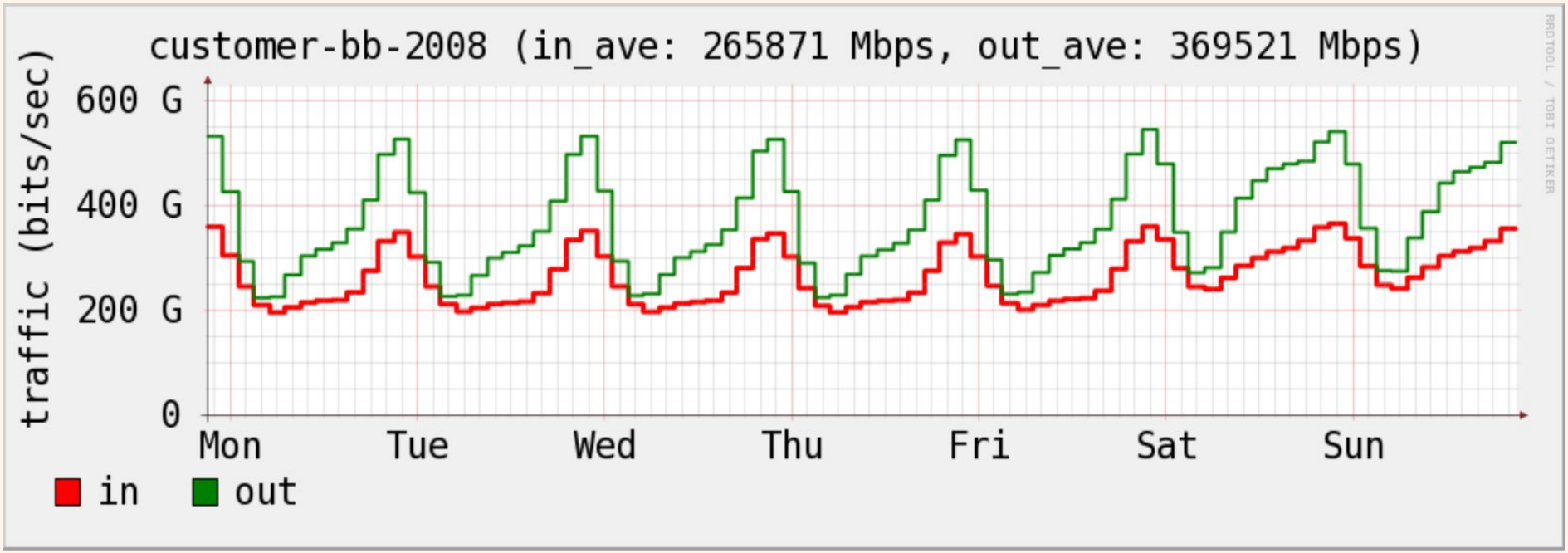
Warning!

Security/Privacy Issues

- Tcpdump/Wireshark/netflow can allow you to monitor other people's traffic
- WARNING: Do NOT use these to violate privacy or security

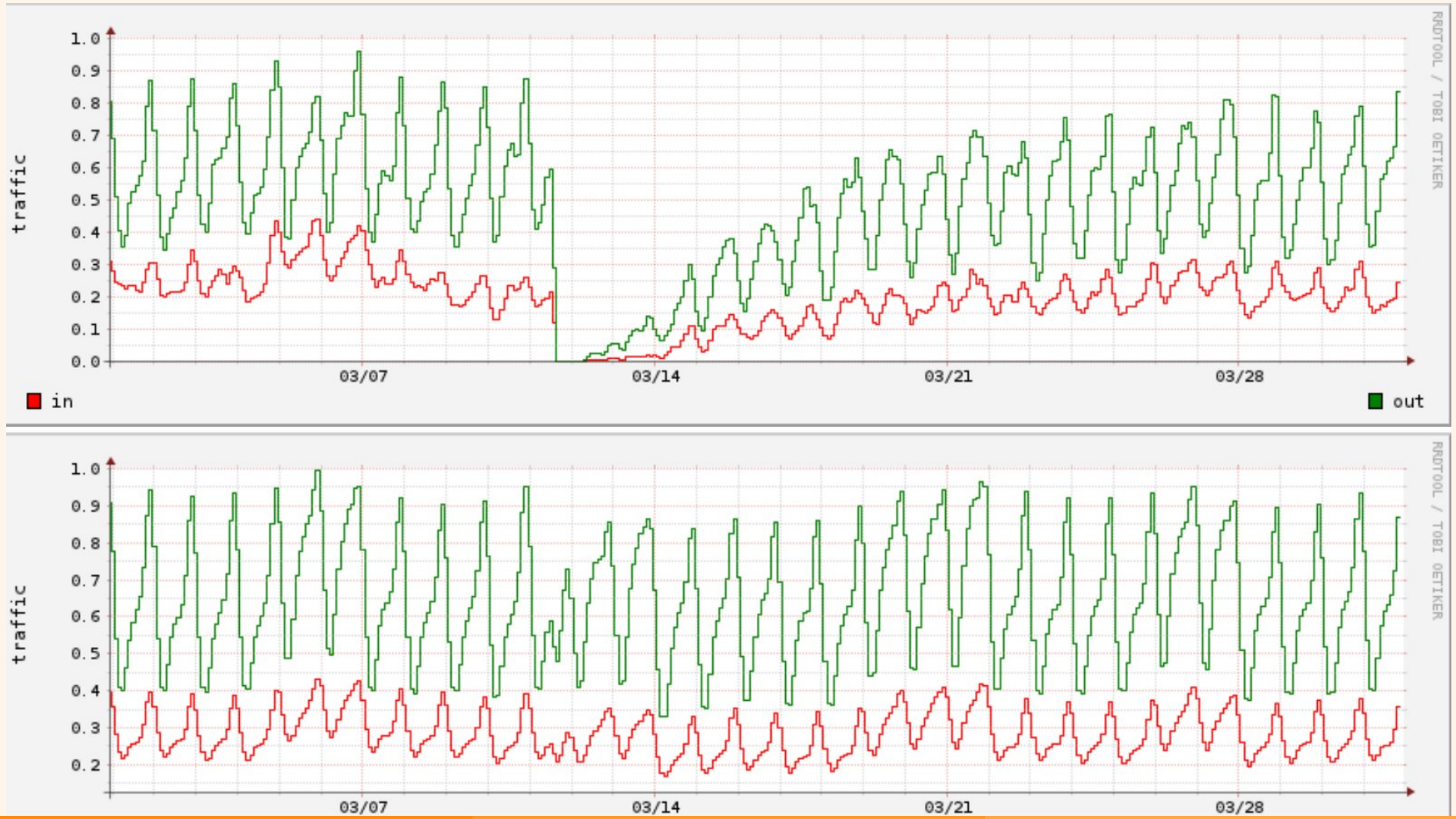
Examples:

Traffic volume in a Japanese ISP



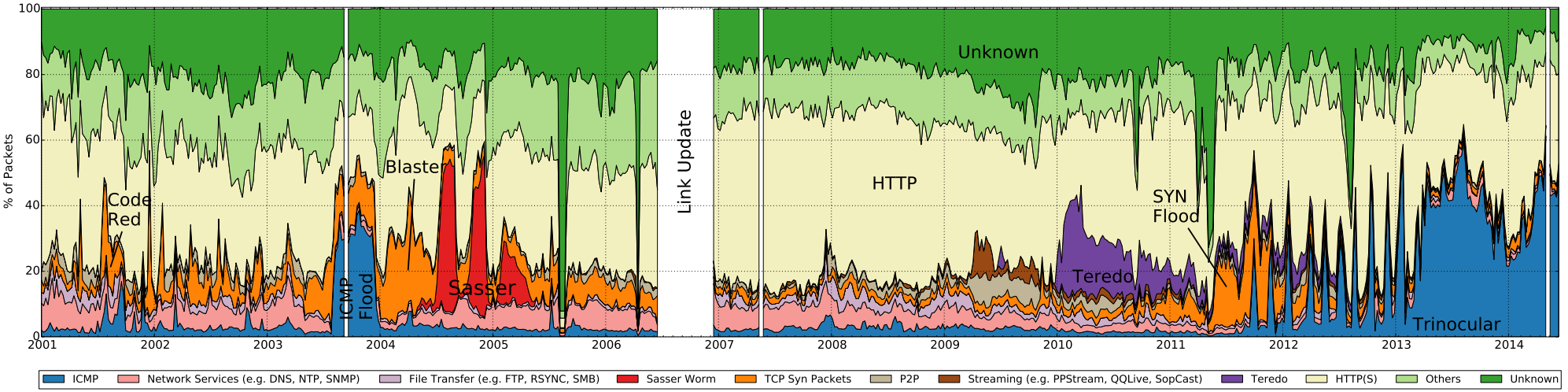
Examples:

Traffic for March 2011, Miyagi prefecture (top) and nationwide (bottom)



Examples:

Trans-Pacific traffic breakdown: (MAWI Archive)



In the news

NSA is also capturing traffic...

Basic commands

Network Interface Configuration

- **ifconfig**(linux), or ipconfig (windows)
- List your network interfaces
- Turn on/off your interfaces
- Display your MAC and IP addresses
- Set your IP address

Other useful tools:

All available on Unix/Linux

- **telnet**: Interactive TCP connection
  e.g. telnet www.cnn.com 80
  GET /index.html HTTP/1.1
- **traceroute**: check path between two end-hosts
- **dig**: query dns servers
  e.g. dig www.cnn.com
- **nmap**: check open ports on a computer
  e.g. nmap www.cnn.com

Network Monitoring: Summary

Today's lecture covered:

- SNMP
- Tcpdump/Wireshark
- Netflow
- Some useful tools

Next week: Cryptography

- How to make sure nobody can read our packets?