Lecture 1: Course Overview

CS 598: Network Security

Matthew Caesar

January 15, 2013

Networks are Important

- Networks propagate information
- Information is the enemy of evildoers
  - They can no longer hide in the shadows
  - Can enable coordination against them
- Internet has become massive vector for social change
  - Arab Spring, Anonymous, Jyoti Singh, etc

Networks are Important

- Every aspect of our society is tightly coupled with the functioning of the Internet
  - Business and financial transactions, education and research, medicine, power grid and resource infrastructures
- Internet adds estimated trillions of dollars to world economy

Networks Face Threats

- The power for a single individual to cause harm, is enormous
- This problem is getting worse
  - Network crime is a $114B industry
  - Entire governments are funding cyberattacks
- Arms race between the black-hats and the white-hats
  - This battle will end someday
  - It is not clear who will win

Network Security is Challenging

- Internet is probably the biggest and most complex thing ever created
  - Complex intertwining of systems and protocols
- Complexity leads to rich variety of vulnerabilities
  - Protocol bugs, misconfiguration, DoS attacks, spam, persistent instability
- Pervasiveness leads to rich variety of attackers/attacks
  - Script kiddies, cyberwarfare, natural disasters, careless operators, entropy

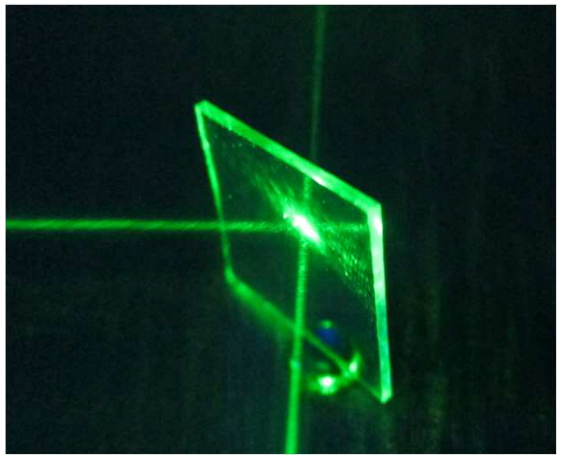
This course

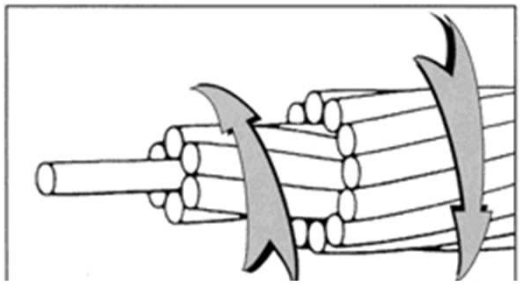
- How to protect networks from harm
  - Common threats/vulnerabilities in networks and their constituent protocols
  - Countermeasures and design principles to build resilient and secure networks
  - Very rich environment for research
- Covers network security, as well as relevant advanced networking background
  - Teaching them together makes each easier to learn
  - Knowledge of both is synergistic

Course Syllabus

- Physical network security
- Long-haul network security
- Data center and enterprise network security
- ISP network security
- Router mechanisms for security
- Internet security architectures
- Security of networked systems
- The big picture
- Hot topics in network security

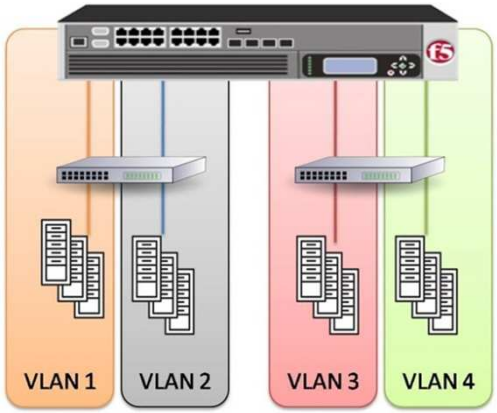
Physical Network Security

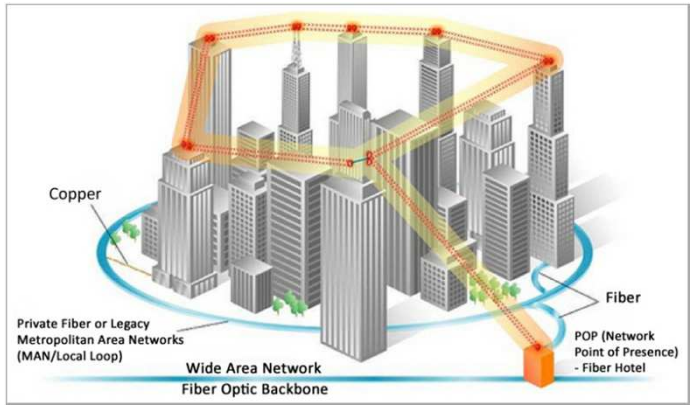


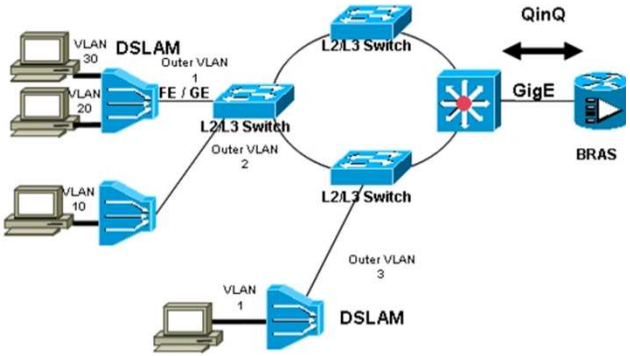


- How to keep physical communication lines secure
  - Advanced overview of copper, optical, and wireless communication
  - Long-haul networks, laying techniques, cable ratings and technologies, wire mechanics, noise/RF, TDR analysis, scattering/absorption, submarine cabling, physical wiretapping, physical attacks on cabling, satellite networks and GPS, 802.11 attacks

Data Center and Enterprise Network Security



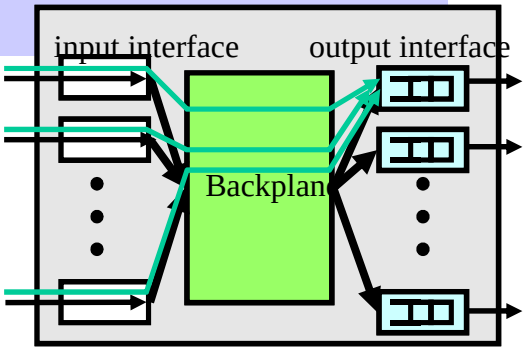


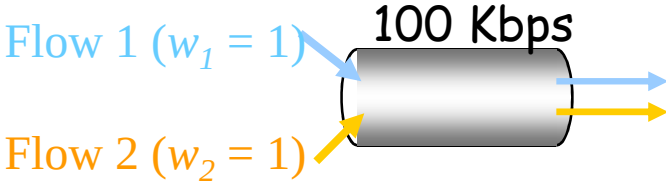


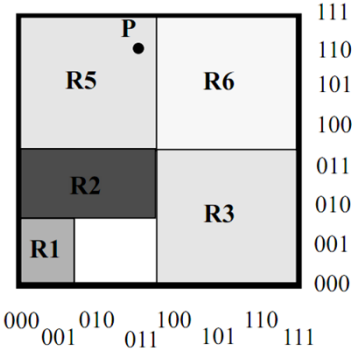
- LAN technologies: Overview of Ethernet, Spanning tree protocol, VLANs, QinQ, DHCP, DTP/VTP, Power over Ethernet, HSRP/VRRP, ACLs, firewalls, middleboxes
- LAN security mechanisms and attacks: VLAN hopping, Tag stack attack, Broadcast floods, ARP spoofing, DHCP DoS, DHCP and DNS hijacking, Spanning tree attacks, Control Plane Policing, Link Layer Security, Port/BPDU guard, 802.1AE/encryption, NetFlow, RMON

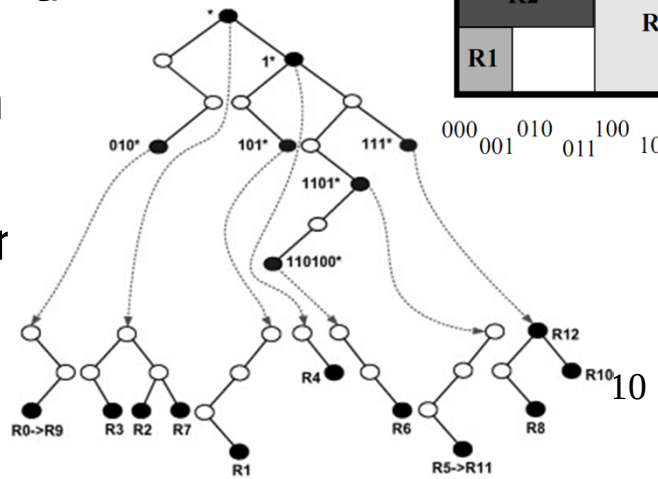
Router Mechanisms for Security

- Router memory/hardware technologies (TCAM/SRAM/DRAM) and architectures
- Matching algorithms: fixed-length and prefix matching, binary tries, patricia tries, skip counts and path compression, perfect hashing, parallel binary search
- Classification algorithms: geometric classification, hierarchical tries, set-pruning tries, crossproducting
- Scheduling algorithms: round robin, FQ, WFQ, Stochastic and self-clocked FQ, virtual clocks and fluid flow, max-min fairness, DRR,
- Intrusion detection system and patter matching algorithms: Boyer-Moore, Approximate string matching, state monitoring and reassembly



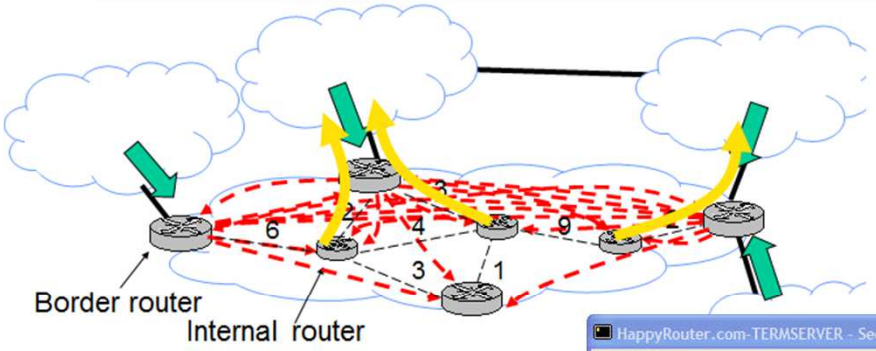




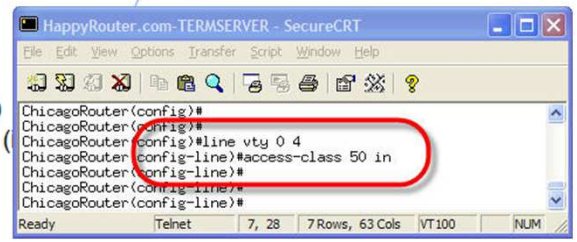


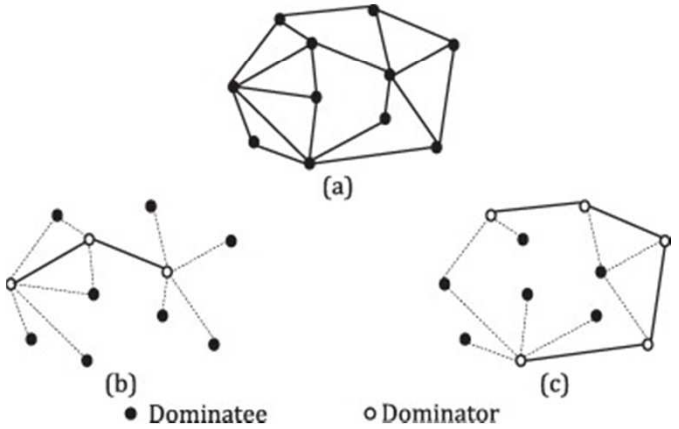
Defensive Configuration

Step	Attribute	Controlled by local or neighbor AS?
1.	Highest LocalPref	local
2.	Lowest AS path length	neighbor
3.	Lowest origin type	neither
4.	Lowest MED	neighbor
5.	eBGP-learned over iBGP-learned	neither
6.	Lowest IGP cost to border router	local
7.	Lowest router ID (to break ties)	neither



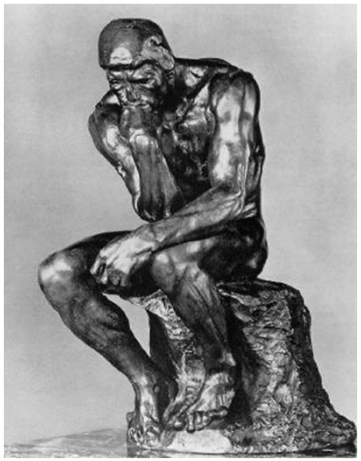
1. Provide internal reachability (**IGP**) --------
2. Learn routes to external destinations (**eBGP**)
3. Distribute externally learned routes internally (
4. Select closest egress (**IGP**) --------





- Internet routing and policy
  - BGP and OSPF, BGP decision process, intra vs interdomain routing, route redistribution, route reflection, peering, policy disputes, ECMP
  - Strategies for resilient and secure configuration
- Designing robust network topologies
  - Hub-and-spoke, backbone networks, points of presence, multi-homing, topology optimization algorithms

The Big Picture



- Ethics in networked security: Philosophical foundations (deontology, relativism, utilitarianism, social contract), codes of ethics, hot topics
- Law: Legal foundations (intellectual property law, jurisdiction and sovereignty), cybercrime, data privacy, liability law, open issues
- Regulation: Standards bodies (ITU, ICANN, IGF, etc), FCC regulations, UN regulations, open issues
- Environmental security: environmental design, mantraps, bollards, territorial surveillance, glass and fire ratings, perimiiter security, electrical power security, case study (Google)

Hot Topics in Network Security

- Security of Software-Defined Networks
- Military Security and Cyberwarfare
- Security of Big Data
- Internet Security Architectures
- Programmable Networks and Network Verification
- More to come…

Who am I?

- Faculty in CS department
- Research: networking, security, systems
- PhD from UC Berkeley in 2007
- Industrial experience at AT&T Labs, Microsoft Research, HP, Nokia DSL; helped found two startups on core networking/security systems; ongoing partnerships/tech transfer with Cisco, DARPA, NSA, Boeing
- I like designing/building/deploying large-scale software systems that are grounded in strong theoretical principles
- Office: 3118 SC

Grading

Project	60%
Class participation, lecture presentation	25%
Paper reviews	15%

- This is a graduate-level course – grade is less important than what you learn

Readings

- Goal is to read and understand core technologies in this field
  - Read required readings before class

- Write a short 1 paragraph review
  - Goal: synthesize main ideas/concepts
  - *Critique* the reading, do not summarize
  - Also list questions you had about the paper, and ask them in class discussion
  - Post your review on Piazza (CS598MCC)

Lecture

- My plan: ~55 mins lecture, ~25 mins discussion
  - I'll lead some lectures
  - Sign up for topics you'd like to present

- Lectures are not paper presentations
  - Lectures taxonomize the core concepts in an area
  - Lectures focus on fundamentals
    - A good lecture's content should be "useful" 5-10 years from now
    - Algorithms, concepts, rules of thumb, core questions; not protocol headers, historical details, etc.

Lecture: Steps

- Choose one of my lecture topics, or propose your own
  - Pick a partner
- Lecture covers an area, not a paper
  - You will need to perform a literature survey to learn the area
  - You will need to think deeply about what topics grad students should know from that area
- Three checkpoints:
  - Send me a 1 paragraph proposal, outline, draft of slides
  - Details on website
- I am here to help you

Project Expectations

- Aim high!
  - A good project could become the basis for
    - Publication: PETS, HotCloud, CoNEXT, ACSAC, NDSS, HotNets, CCS, etc. deadlines coming up.
    - Ph.D. thesis
  - Focus on *impact*
- Your project need not be Oakland-quality but should be conference-worthy with a little more effort
- I am here to help you
- New project ideas posted in a few weeks

Research Project: Steps

- Choose one of my project ideas or you can come up with your own
- Pick your project, partner, and submit a one-page proposal describing
  - The problem you are solving
  - Your plan of attack with milestones and dates
- Have a one-on-one meeting with me to discuss your project topic
- Give 2 short (5-10 minute) presentations on your progress
- Poster session
- Submit project papers at end of semester

Send me the following information

- Tonight, please fill out the following survey

- https://docs.google.com/spreadsheet/viewform?formkey=dGxqcEpCWVBqQzZKMWlLRGFQS3c3Mmc6MQ

- Also, make sure you're on the course mailing list
  - You should receive an email from me by end of today

Rest of Today

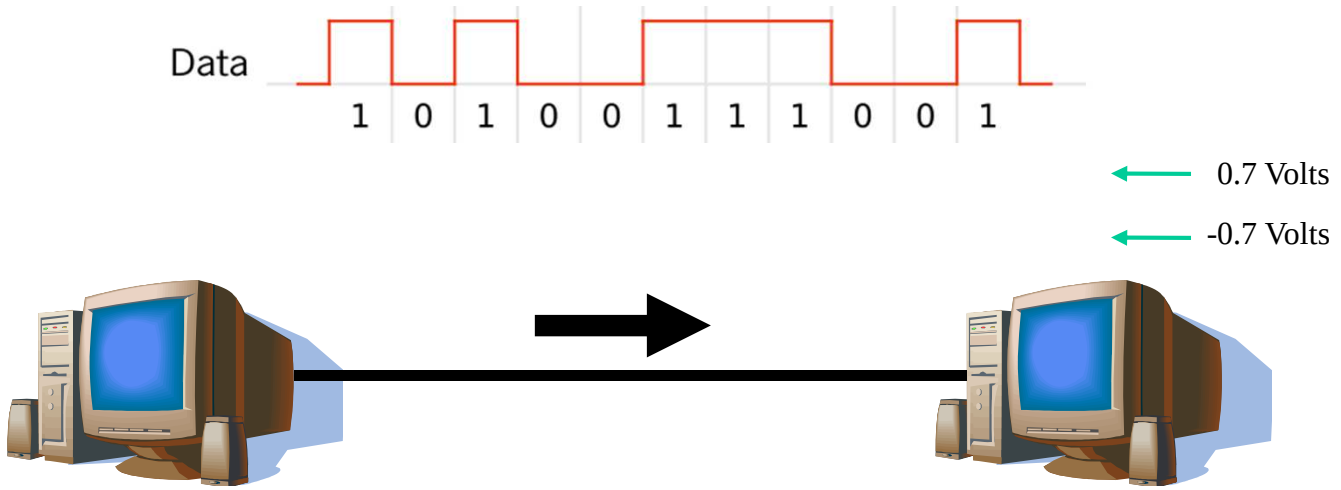
- Background on networking

The Internet

- Global scale, general purpose, heterogeneous technologies, public, computer network

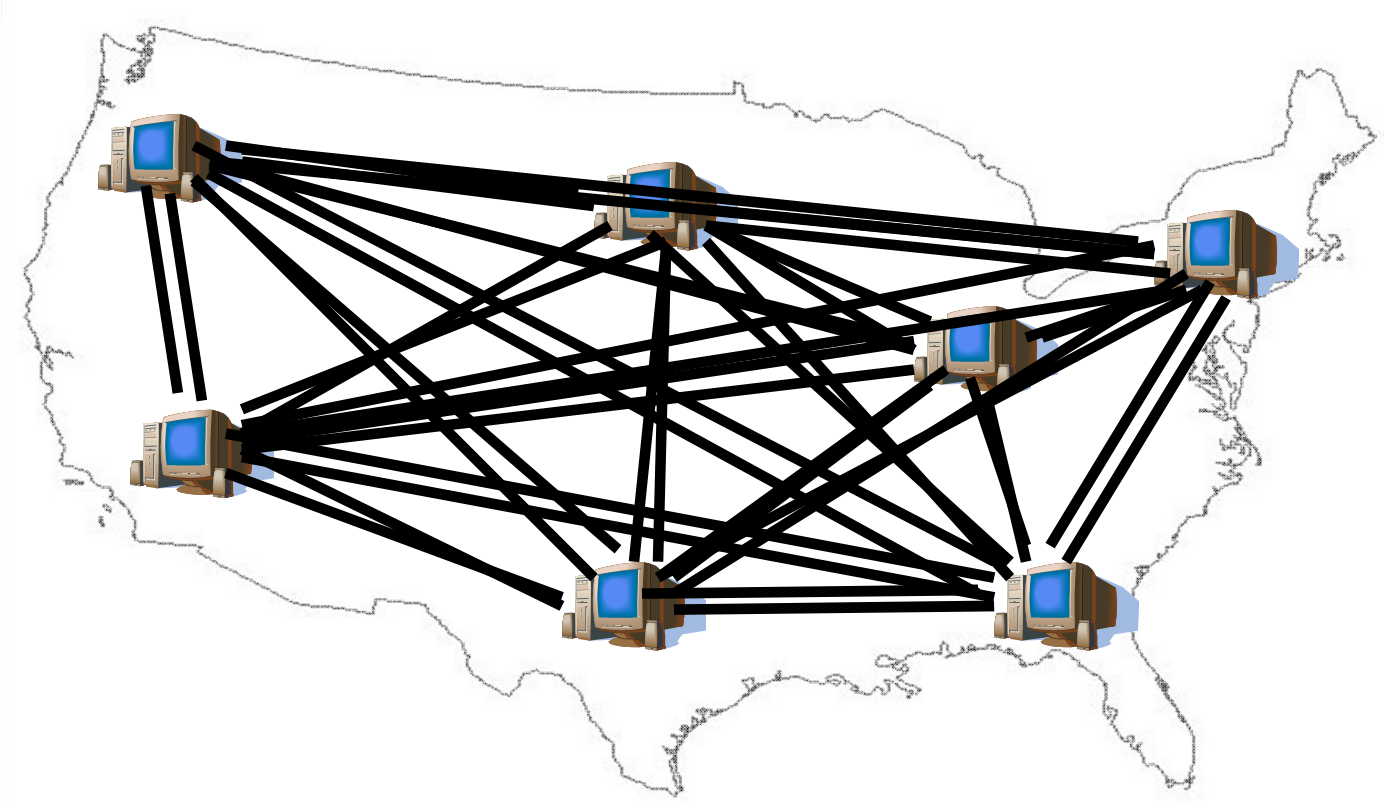
- Vast distributed system comprising
  - 650 million hosts (potentially malicious)
  - >26,000 ISPs (potentially competing)

How can Two Hosts Communicate?



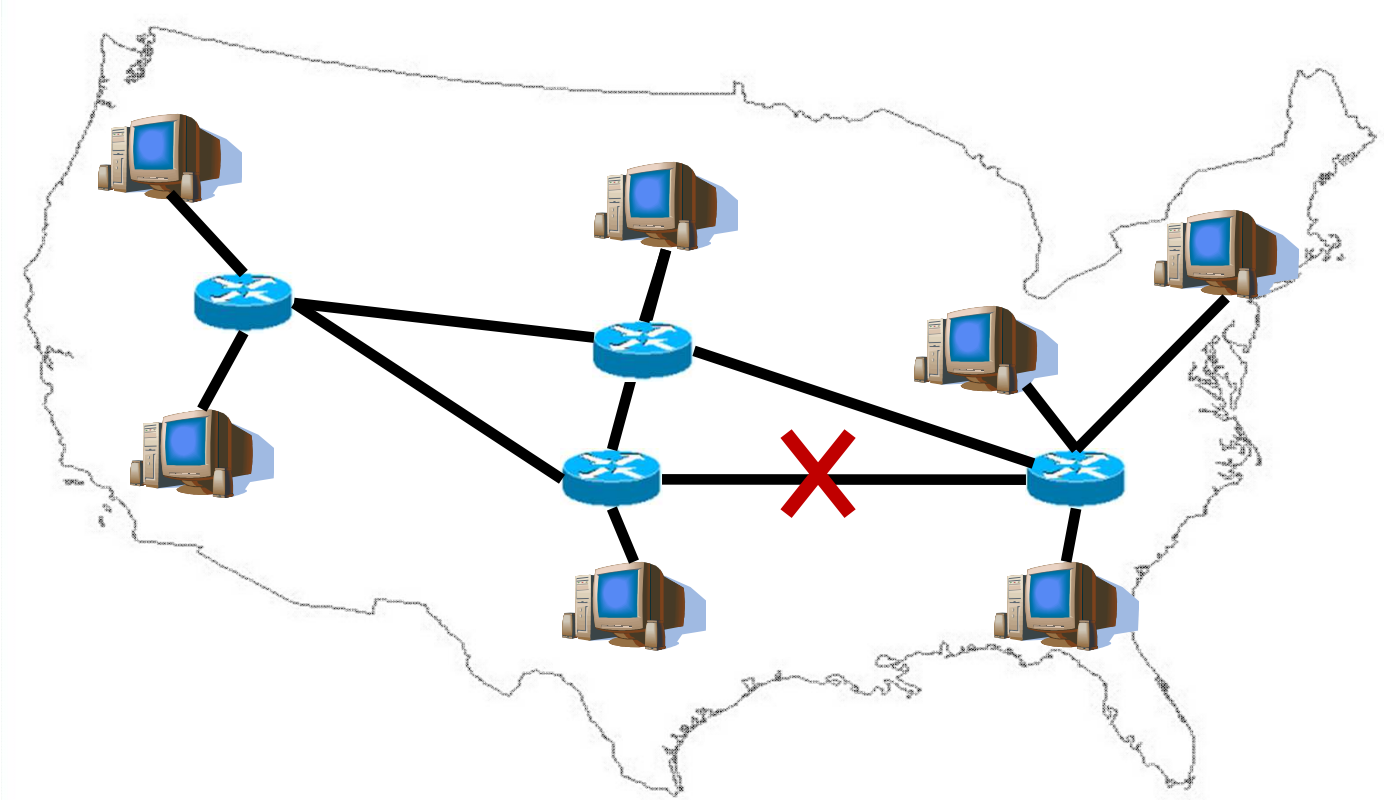
- Encode information on modulated "Carrier signal"
  - Phase, frequency, and amplitude modulation, and combinations thereof
  - Ethernet: self-clocking Manchester coding ensures one transition per clock
  - Technologies: copper, optical, wireless

How can many hosts communicate?



- Naïve approach: full mesh
- Problem:
  - Obviously doesn't scale to the 570,937,778 hosts in the Internet (estimated, Aug 2008)

How can many hosts communicate?



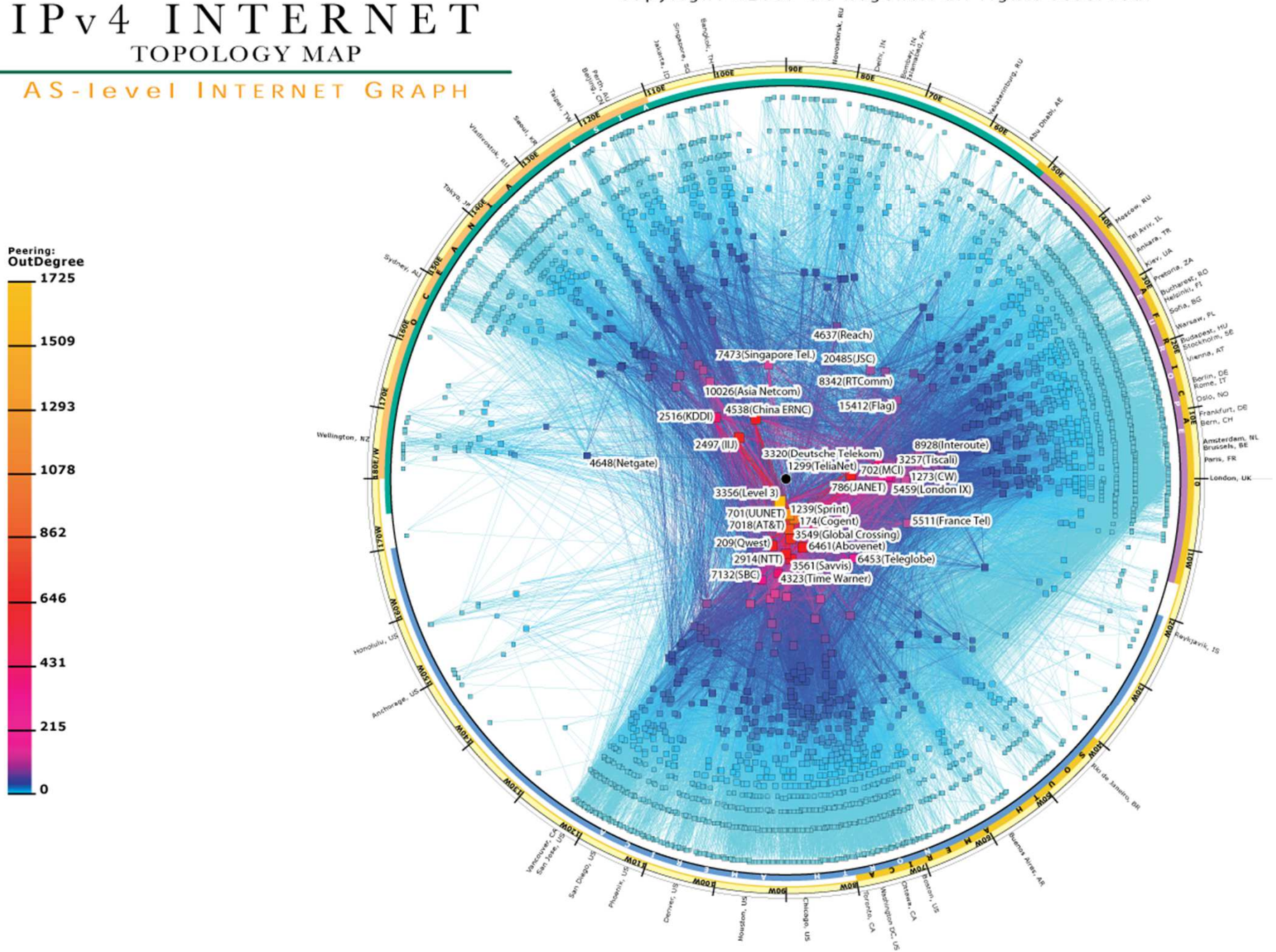
- Multiplex traffic with routers
- Goals: make network robust to failures and attack, maintain spare capacity, reduce operational costs
  - More on "topology" in Lectures 2,3

Complete Network Assets : XO Communications

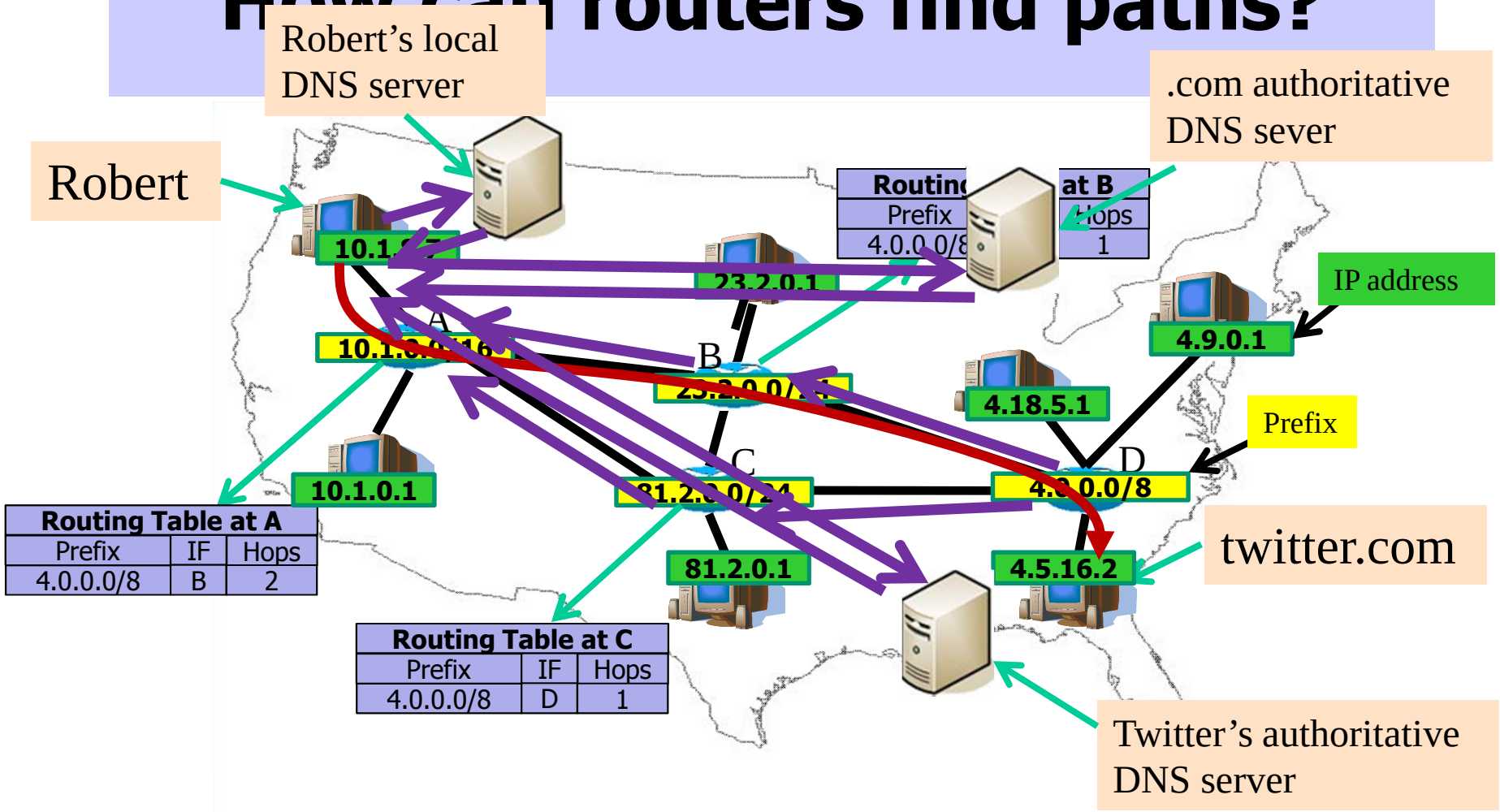
LEGEND

OC-12 Market Uplinks	Data Center IP OC-12c Uplink	Core IP Node	Class 5 Voice Switch	Local Voice Footprint
OC-3 Market Uplinks	OC-48 IP Backbone	Metro IP Node	Sonus Gateway	XO Market
Diversely Routed OC-48Transport	OC-48 IP Market Uplink	Private Peering IP Node	Longhaul Termination (All Bandwidths)	Network Management Center
OC-192 BLSR Rings	OC-192 Backbone Circuit	Public Peering IP Node	Longhaul Termination (OC-48 & Above Only)	Private Line Backbone
GigE	Peering Backbone Circuit	Data Center		

IPv4 INTERNET
TOPOLOGY MAP
AS-level INTERNET GRAPH

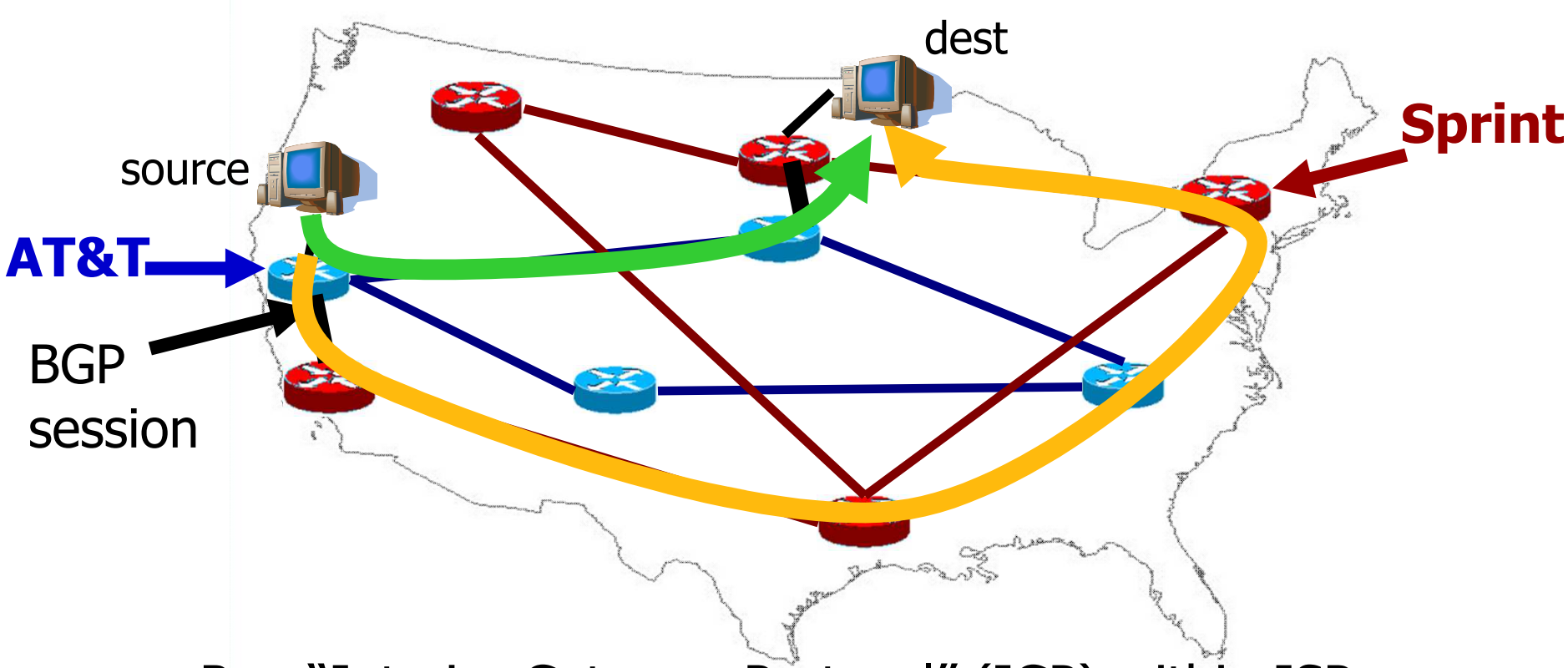


How can routers find paths?



- Hosts assigned topology-dependent addresses
- Routers advertise address blocks ("prefixes")
- Routers compute "shortest" paths to prefixes
- Map IP addresses to names with DNS
- More on "Routing" and "Naming" in Lectures 3,4,7

Intra- vs Inter-domain routing



- Run "Interior Gateway Protocol" (IGP) within ISPs
  - OSPF, IS-IS, RIP
- Use "Border Gateway Protocol" (BGP) to connect ISPs
  - To reduce costs, peer at exchange points (AMS-IX, MAE-EAST)

Do IP networks manage themselves?

- In some sense, yes:
  - TCP senders send less traffic during congestion
  - Routing protocols adapt to topology changes
- But, does the network run *efficiently*?
  - Congested link when idle paths exist?
  - High-delay path when a low-delay path exists?
- How should routing adapt to the traffic?
  - Avoiding congested links in the network
  - Satisfying application requirements (e.g., delay)
- … essential questions of traffic engineering

What if hosts misbehave?

- Easy to send traffic to anyone else: even if they don't want it!
  - spam, DoS, phishing, worms,
- Possible defenses:
  - Monitoring+filtering: detect attack and install filters to drop traffic
  - Capabilities: only accept traffic that carries a "capability"
- More in Lectures 20-21

How can researchers study networks?

- Techniques: Measurement, Simulation, Emulation, Deployment
- Testbeds: Planetlab, Emulab, ns-2,
- Data sources: Abilene Observatory, Routeviews, CAIDA
- Software: Click, Quagga, and XORP software routers
- If you've got an idea, this course will help you figure out how to evaluate it

Summary

- Course administrivia
- Course topic highlights
- Details on web site:
  http://www.cs.illinois.edu/~caesar/netsec