

# Network Security Fundamentals

---

**Steven Taylor**

President, Distributed Networking Associates, Inc.  
Publisher/Editor, Webtorials  
taylor@webtorials.com

**Larry Hettick**

Vice President, Wireline Solutions  
Current Analysis  
larry@larryhettick.com



## Thanks to the sponsor...

---

- This presentation is made possible in part due to the generous support of Nortel Networks.

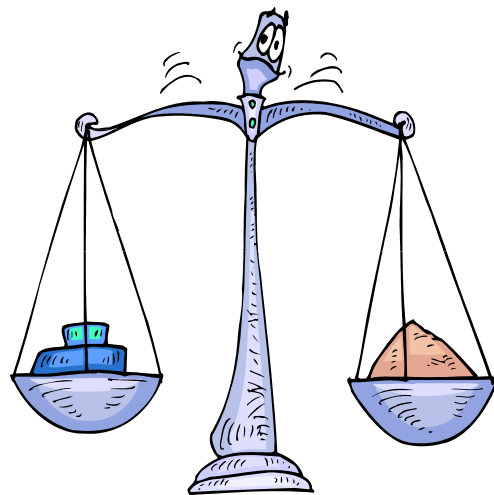


# Agenda

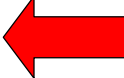
- Overview of the problem
- Various Vulnerabilities
  - Workstations
  - LANs and Switches
  - Routers and Firewalls
  - Wide Area Networks (WANs)
- The Big Picture

# Security Requirements

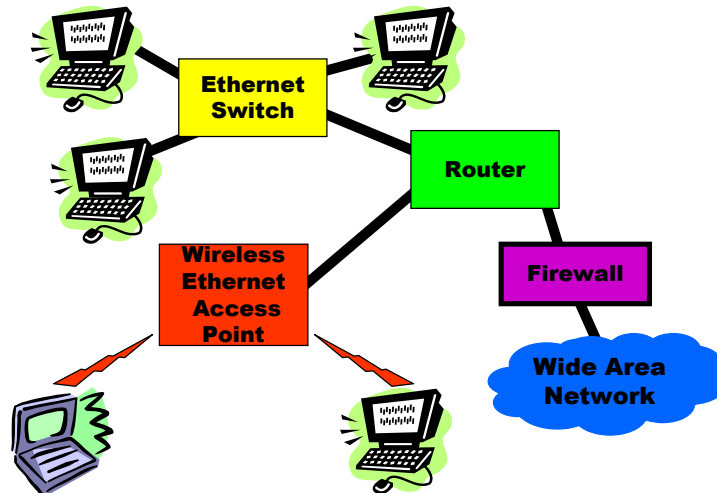
- Security is a process of balancing risks and benefits
- Some potential security threats
  - Workstations
  - LANs and Switches
  - Routers and Firewalls
  - Wide Area Networks (WANs)
  - Physical security
- Make a decision based on a realistic evaluation; not emotion



# Agenda

- Overview of the problem
- Various Vulnerabilities 
  - Workstations
  - LANs and Switches
  - Routers and Firewalls
  - Wide Area Networks (WANs)
- The Big Picture

# Network Architecture

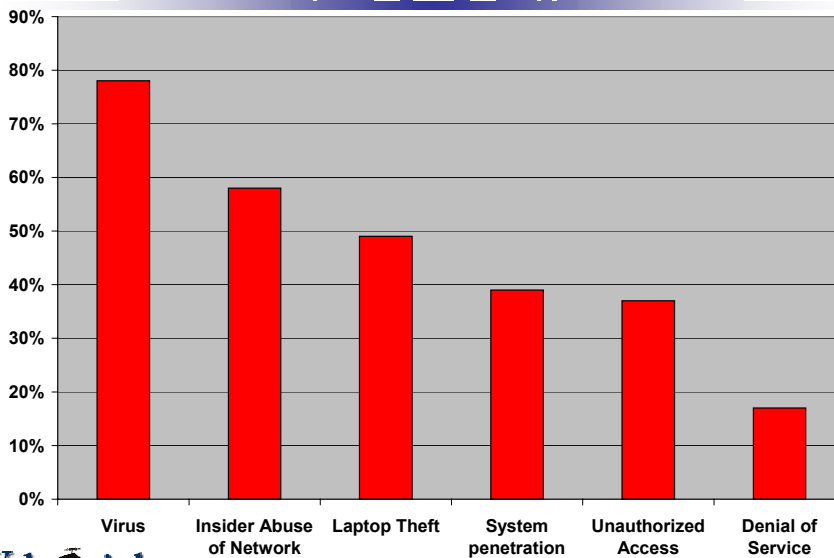


# Workstation Security



Webtorials

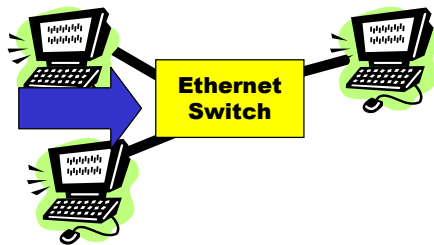
# Experienced Threats to Information Security



Webtorials

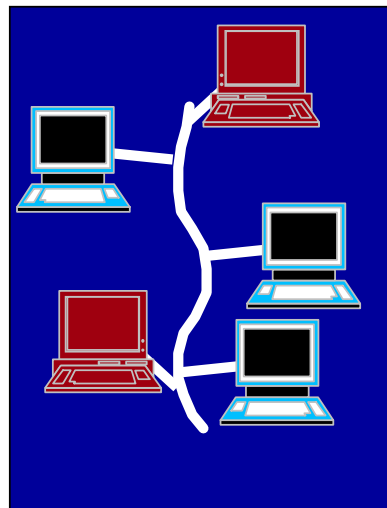
Source: CSI/FBI 2004 Computer Crime and Security Survey Results. <http://www.gocsi.com>

# LAN Security



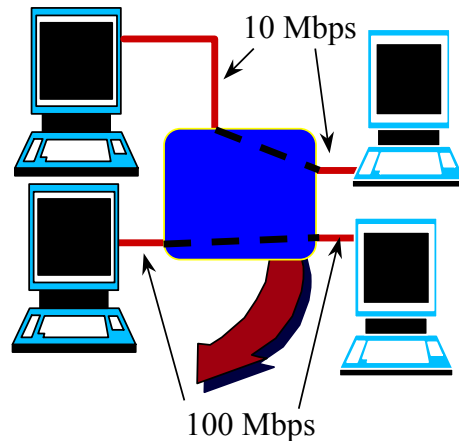
# Traditional (old) Ethernet

- Advantage
  - Shared, "broadcast" medium provides easy access
- Disadvantage
  - Shared, "broadcast" medium is a significant security risk



## Switched Ethernet

- Switched
  - Multiple paths through the switch
  - Dedicated full-speed media
- Scalable
  - Multiple speeds to match application
  - Speed Conversion
- Inherently more secure



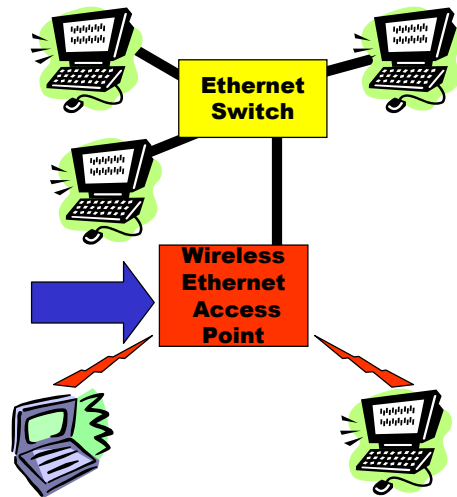
Webtutorials

## Packet sniffing...

- Can packets be sniffed?
  - Yes, if you
    - Have physical access
    - Tap the line
    - Decode Ethernet, plus IP, plus IP encoding
    - Can do this realtime
    - And you could use encryption (more later)
- Is switched Ethernet a security risk?
  - Is it worth the trouble?
  - No worse than traditional telephony
  - Depends on physical access

Webtutorials

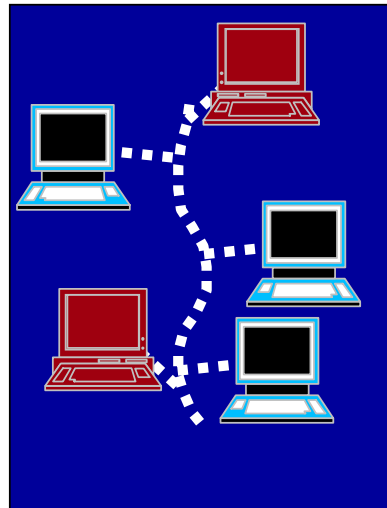
## Wireless LAN Security



Webtutorials

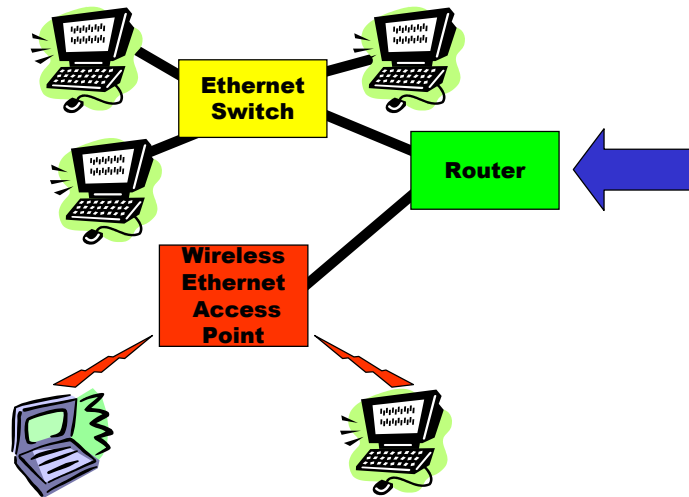
## Wireless Ethernet

- Acts like traditional Ethernet without the wire
  - Shared, "broadcast" medium provides easy access but is a security risk
- Multiple Security enhancements available
  - Security needs to be implemented carefully and



Webtutorials

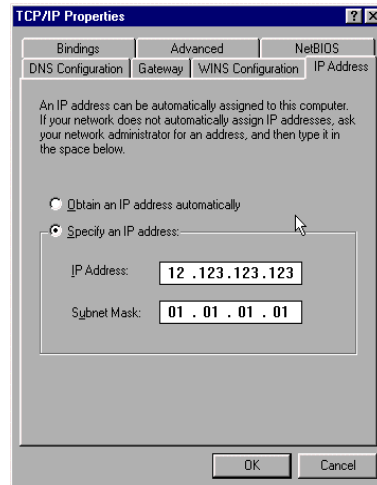
# Security and IP



Webtutorials

# IP Address Spoofing

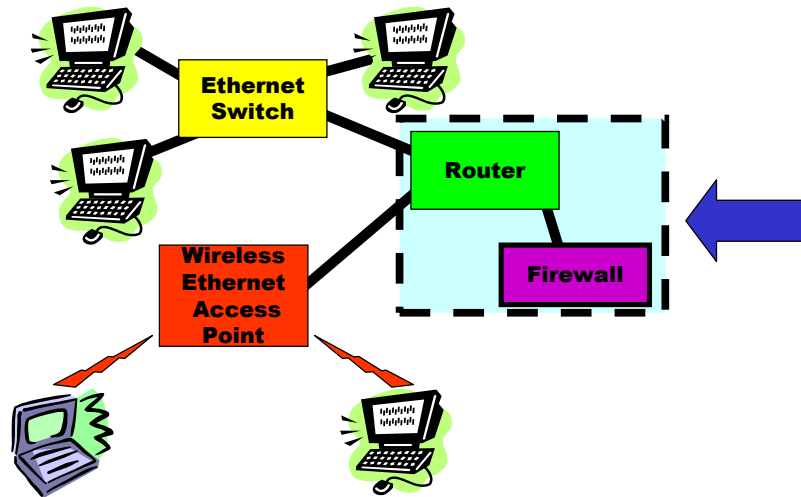
- IP address is set by the user
  - Can be spoofed
  - Need for authentication
- But this problem is mostly solved
  - Network Address Translation (NAT)
  - Additional mechanisms for advanced functions (like Session Initiated Protocol – SIP)



Webtutorials



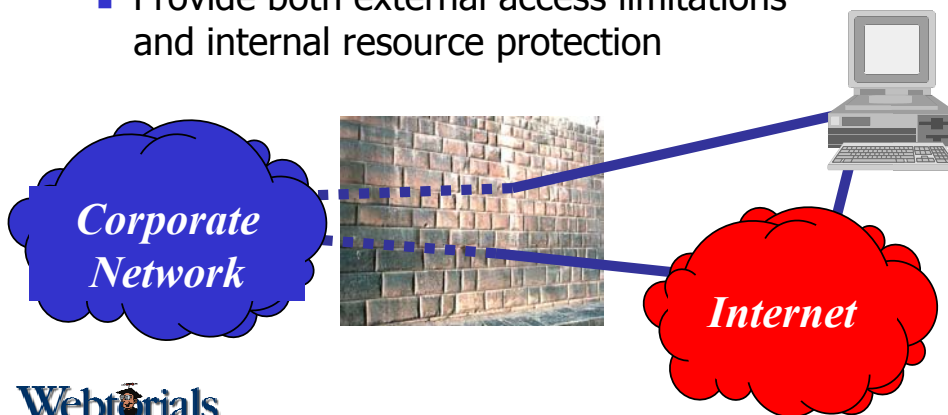
# Firewalls



Webtutorials

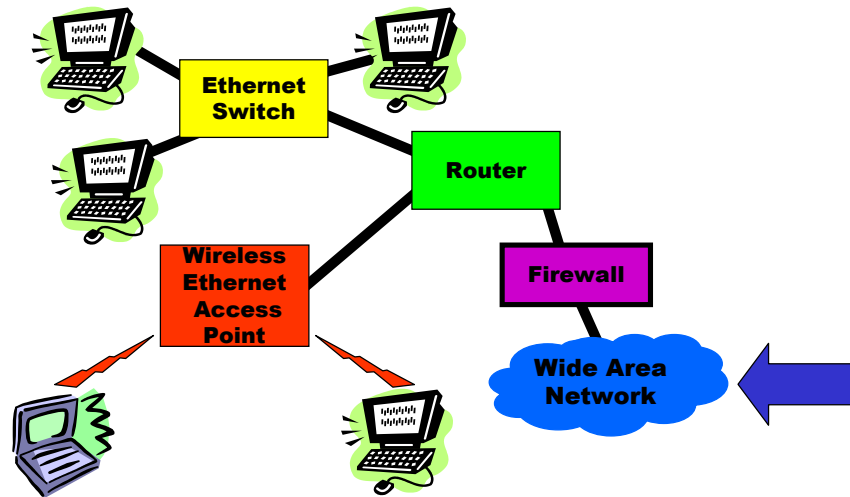
# Firewalls

- Applications to limit and control connectivity within network environments
- Provide both external access limitations and internal resource protection



Webtutorials

## WAN Security



Webtutorials

## Common WAN Services

- Private line, frame relay and ATM
- Private IP VPNs
- Internet Backbone VPNs
  - IPSec
  - SSL



Webtutorials

# Private Line, Frame Relay and ATM Security

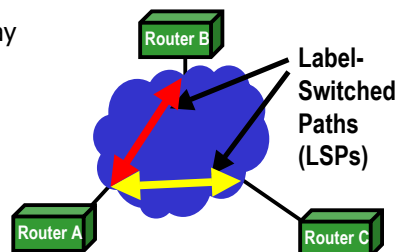
- Private lines provide dedicated bandwidth per circuit
  - TDM technology
- Frame relay and ATM PVC / SVC addresses are set by network operations
  - SVC user controls connection, not address
- At some point, you must trust the service provider(s)
  - Common issue for all nets
  - Encryption is available, but not usually required



Webtutorials

# Private IP VPNs

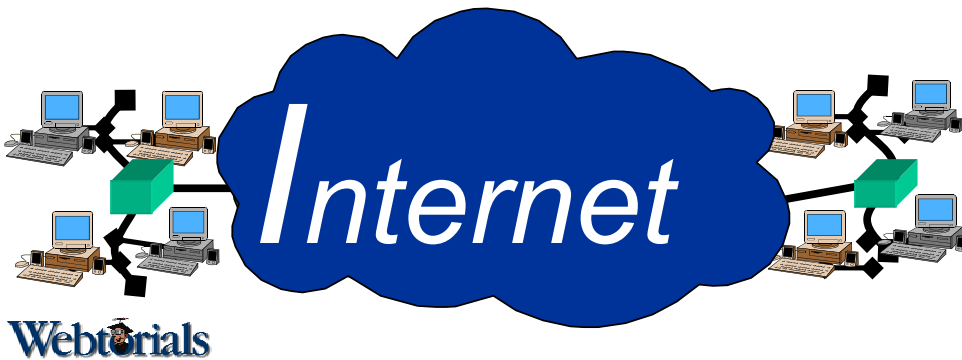
- IP-based networks that are not based on the public Internet
  - "Closed User Group" for each enterprise
- Often based on Multiprotocol Label Switching (MPLS)
  - LSPs (Virtual Circuits) automatically configured based on IP address
    - "Self-configuring" frame relay
- Sometimes deployed as "Virtual Routers"
- Security issues similar to ATM and frame relay



Webtutorials

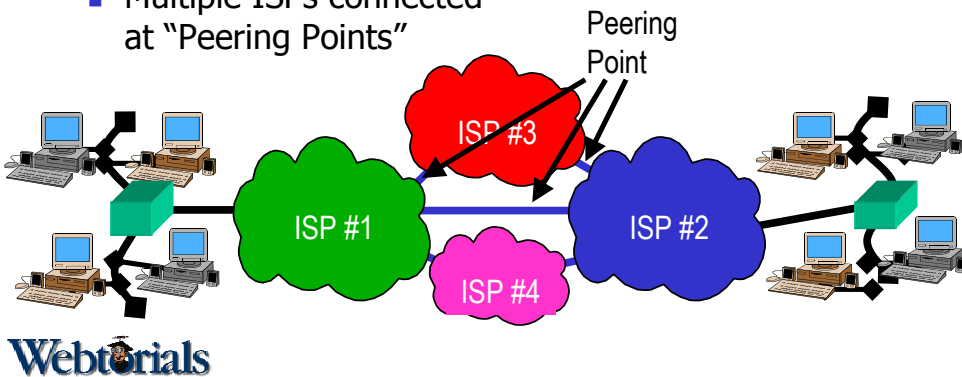
# Internet Backbone VPNs

- Uses IP as the "UNI" to the network
- Any-to-Any connectivity
- No inherent security



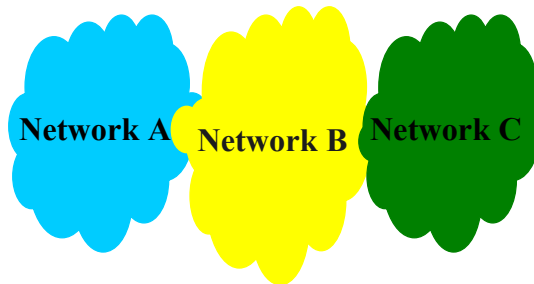
# Internet Backbone VPNs

- Uses IP as the "UNI" to the network
- Any-to-Any connectivity
- No inherent security
- Multiple ISPs connected at "Peering Points"



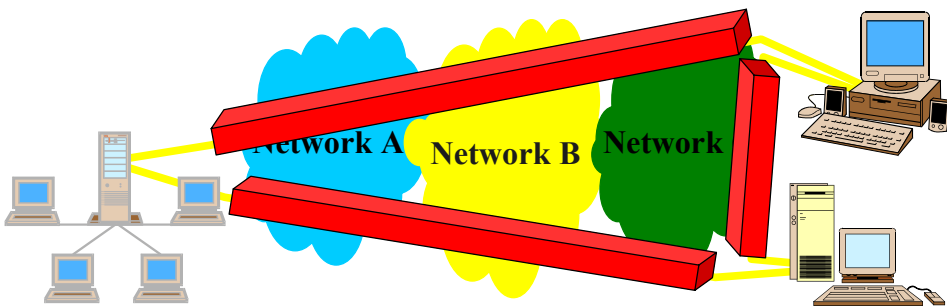
# IPSec VPNs

- Internet transport layer



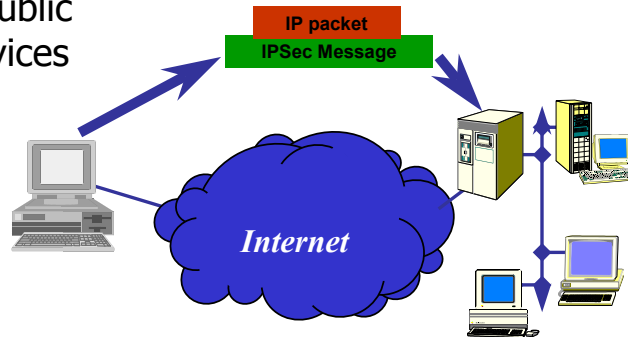
# IPSec VPNs

- Internet transport layer
- "Tunnels" through the Internet



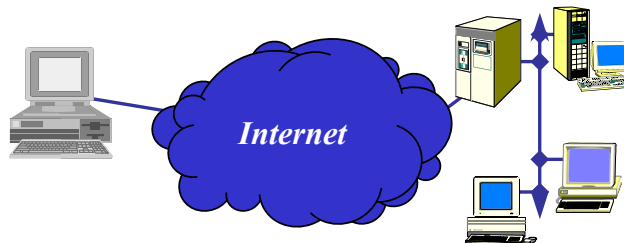
# What is IPSec?

- Encapsulation method that encrypts IP packets between two points inside another IP message
- Authenticates and secures VPNs over public IP services



# What is SSL?

- Similar to IPSec
  - Similar encryption algorithms
- Browser based
  - Authenticates between browser and server



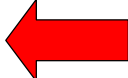
# Choosing a WAN Architecture

---

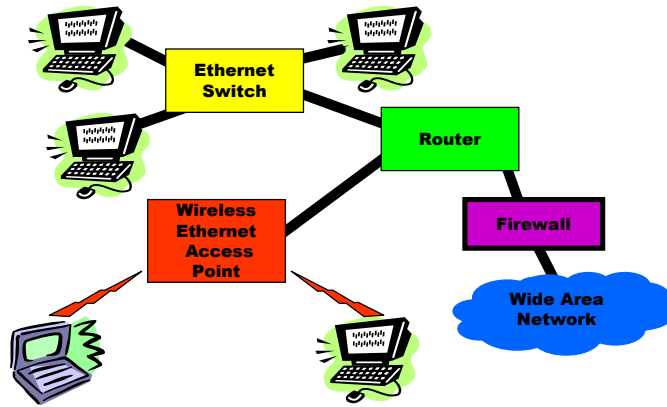
- All methods “work”
- All methods can be secure
- One size doesn’t fit all
- Corporate “religion” is a major decision-making factor

# Agenda

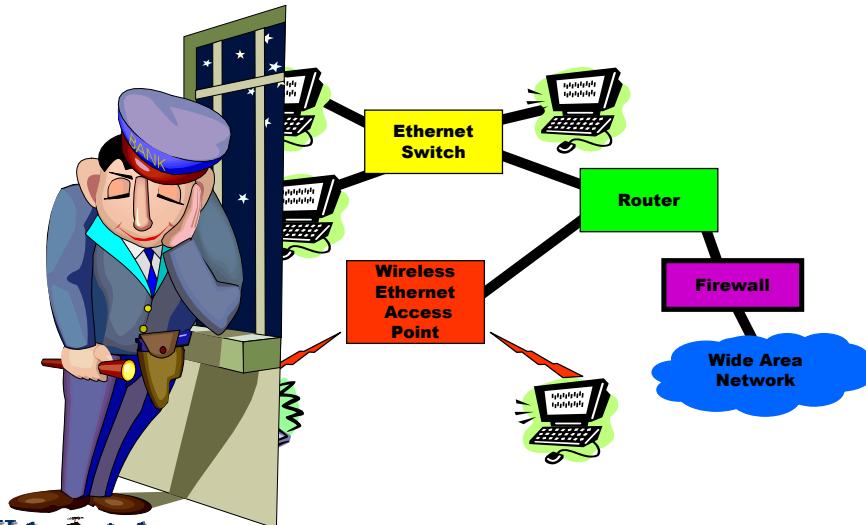
---

- Overview of the problem
- Various Vulnerabilities
  - Workstations
  - LANs and Switches
  - Routers and Firewalls
  - Wide Area Networks (WANs)
- The Big Picture 

# This is Your Network



# Who's guarding the door?





# Thank you!

---

- Summary
  - Overview of the problem
  - Various Vulnerabilities
    - Workstations
    - LANs and Switches
    - Routers and Firewalls
    - Wide Area Networks (WANs)
  - The Big Picture
- For more information
  - Webtorials
    - <http://www.webtorials.com>
  - Nortel Networks
    - Sponsor of this presentation
    - <http://www.nortelnetworks.com>

