Security policy in academic environment

Design and Implementation

Aco.Dmitrovic@SRCE.hr

Why do we need SP?

- Internet is not a friendly place any more
- “Flaming” offensive people doesn’t work
- Unwanted traffic:
  - Spam, viruses, scanning...
- Aggresive & criminal behaviour
  - Identity theft
  - Breaking in
  - DoS
  - Spying

Defense

- Learn to survive in dangerous environment
- IT Stuff must organize defense
- Policy is needed before technical solutions can be implemented

SP

- Users
  - Acceptable use policy
  - Define unacceptable behaviour

- IT stuff
  - Authority to act
  - Rules of engagement
  - Best practices

Management

- Should support SP
- Be ready to invest in
  - Hardware
  - Software
  - Education of specialists
  - Education of users

- Management and IT Stuff together must give example to other users

Goals

- *"Data are the most valuable asset"*
  - *Confidentiality*
    - Only authorized persons can access data
  - Integrity
    - Data should be correct and updated
  - *Availability*
    - 24/7

Standards

- ISO/IEC 17990:2000
- Information technology – Code of practice for information security management
  - BS 7799
- Accepted by ISO/IEC JTC

ISO 17990

- Organizational security
- Classification and control of assets
- Personnel security
- Physical security
- Communications & operations management
- Access control
- Research and development
- Business continuity managment
- Compliance

NIST

- USA
  - National Institute of Standards and Technology
- Draft: *Internet Security Policy: A Technical Guide*

Barbara Guttman, Robert Bagwill

March 26, 2002

Standards…

- ISO/IEC 15408:1999

  The Common Criteria for IT Security Evaluation

  - Production of safe software

- NIST Special Publication 800-23

  Guide to Federal Organizations on Security Assurance and Acquisition /Use of Tested/Evaluated Products

Standards…

- RFC 1855: Netiquette Guidelines

  Category: Informational

  S. Hambridge

  Intel Corp.

  28 Oct 1995

- http://www.faqs.org/rfcs/rfc1855.html

Differences

- ISO 17990 is too rigid
- NIST draft is more flexible
- Levels of risk:
  - Low
  - Medium
  - High
- For instance: →

Software import control

- Low risk:
  - Educate users about possibility that downloaded software may can be malicious
- Medium:
  - Only administrators are allowed to install software
- High:
  - CIO/CSO has to autorize instalation
  - Monthly control of installed software
  - Instalation from secure internal server
  - Compliance

Java/Active X

- Low risk:
  - Educate users about dangers
- Medium:
  - Firewall/browser blocks distribution of applets, except from confidential source
  - Applets are forbiden on production systems
- High:
  - Interactive software is forbiden

Licences

- Low risk:
  - Use of licenced SW only
  - Demo versions should be uninstalled after trial period expires
- Medium/High:
  - Only authorised personel can install SW
  - Monitoring, sanctions

Virus protection

- Low risk:
  - Educate users about dangers and protection
  - Users notify administrators when virus is found
- Medium:
  - Users are not allowed to install SW, daily scanning, rezident AV
- High:
  - CIO/SA authorizes installation, audit
  - Central installation, auto update and scanning

Password

- Static, robust, continuous authentication
- Low risk:
  - Minimal standard, rules for password use
- Medium:
  - Static autentication
  - For sensitive systems robust authentication
- High:
  - Robust or continuous authentication

E-mail

- Low risk:
  - All employees have user accounts
  - Moderate private use is allowed
  - Educate users to protect institution’s interests and reputation
  - Message content is confidential, except in case of investigation
  - Use for private commercial purposes is not allowed

E-mail...

- Medium risk:
  - For company bussines only
  - Private messages are forbidden
  - Confidential company data must not be sent by e-mail
  - Except when encripted
  - Use of authorised mail clients only
  - Use of anonymous remailer is not allowed

E-mail...

- High risk:
  - No private messages
  - All messages are company property
  - Company can read all messages
  - Guests, temporary workers, third parties are not allowed to use e-mail service
  - Messages must be digitaly signed
  - Use of authorized software only
  - Data retention

University

- There is no standard for academic security policy
- Different goals: education, research
- Open culture
- Resistance to limitations
- Basic policy only, users introduced to simple rules
- Users assumed to be ethical

Our problem

- How to protect data and user privacy leaving enough freedom of use?
  - Define high risk zones
    - Implement strict security policy there
  - Define low risk zones
    - Allow freedom protecting users at the same time

Typical situation

- Understaffed
- Management and IT personnel do not speak the same language
- There is no sense of value of IT assets
  - IT not used in education
- Lack of resources
- IT staff marginalized

Recommendation

- General security policy
  - Should last for years
- Rules for particular jobs
  - Can be changed more often
  - Define procedures
  - Acceptable/unacceptable behaviour
- Allocation of responsibilities, “ownership”
- Sanctions for undisciplined

Additional policies

- Acceptable use policy
- E-mail policy
- Web usage policy
- Password policy
- Incident response
- Extranet policy
- Intranet policy
- Backup policy
- Audit policy

Privacy

- Personal/private data protection
- Collecting, processing and accesing personal data should be regulated
- Compliance with national legislation
- Law can limit sharing of personal data accros state boundaries
  - Internet has no boundaries

Misuse Prevention

- Equipment belongs to organization and can be used strictly for work
- Illegal use of equipment can be prosecuted
- Legality of audit
  - Obtain permission from management
  - Inform users
  - Ask permission from users?

Organizational security

- Forum
  - Members should be IT staff and managers
  - Information security is business responsibility shared by all managers
  - Support for security initiatives
- CSO
  - is single person responsible for all security issues
  - Policy, education, organization, monitoring, implementation, incident response…

Allocating responsibilities

- Not easy in small organization
- Security personnel should be independent!

- Each user and administrator must know what is expected of him

Employee protection

- Lower the risk of mistake, theft, misuse
- Include security in job description
  - Obey security policy
  - Resource protection
  - Procedures
- Personnel control
  - Check employee history
  - Surveillance

Physical security

- Define safe zones
- Restrict physical access
- Define perimeters
- Visitors
  - Identified
  - Tagged
  - Followed to destination and back

Equipment security

- Critical equipment must be isolated in protected environment
- Restricted physical access
- Anticipate risks:
  - Fire, flooding, smoke, dust, EM radiaton
  - Theft, destruction…

Workstations

- Each PC must be professionally administered
  - by user
  - by expert
- Obligatory patching
- No services (P2P)
- Anti Virus with newest virus definitions
- “Private” computers?
  - When connected to network, they must obey the same rules

Third party

- Physical security
  - Perimeter check, credentials
  - Escort, video surveillance
  - Time limit
- Logical access
  - To confidential data
  - Computers, communication equipment
- Non disclosure agreement
- Responsibility, liability

Information classification

- Public, internal, confidential, secret…
- Handling
  - copying
  - storing
  - sending
  - access
  - destruction

Data protection

- Data destruction procedures
  - Disks, papers etc. should be physically destructed
- Clear desk & clear screen policy
  - Confidental data must not be seen on the screen or on the desk, left in the network printer
  - Password protected screen saver

Incident response

- Users have to report problems
  - Hardware problems
  - Services
  - DoS
  - Viruses
  - Wrong or incomplete data
  - Breach of confidentiality
- Call center, forms, Trouble Ticketing system

CIRT

- Educate staff
- Define procedures
- Collect evidence
- Recover
- Reporting
- Reports are confidential
- Data retention

Housekeeping

- Back-up
  - Multiple copies of important data
  - Storing at safe remote location
  - Restrict access to data copies
  - Test backup media
  - Test restore
  - Retention period
  - Procedures for media destruction
- Operator logs

Network management

- Responsibility for network separated from responsibility for computers and services
- Protect data on the network (LAN i WAN)
- Protect equipment accessible from outside
- Problems:
  - Wireless and portable devices
    - Visitors, private equipment
  - Teleworking

Mobile computing

- Policy proscribes
  - Physical protection
    - Car, hotel, konference
  - Remote access control
    - Identification, authorization
  - VPN, cryptography
  - Back-up
  - Virus protection

Teleworking

- Risks:
  - Theft, information leak
  - Direct access to Intranet
- Policy:
  - Physical security at home
  - Safe communication
  - Defines the work that can be done remotely
  - Rules for family members and guests
  - Revoke equipment and and access rules when job is done

Systems development and maintenance

- Application security
  - Check input data
  - Kontrola obrade (rizik gubitka integriteta podataka)
  - Authentication, authorization
  - Check output data
  - Cryptography
    - Digital subscription
    - Non repudiation

Development, testing, production

- Must be strictly separated!
- Different network segments,different people
- Only thoroughly tested software goes in production
- Do not use real data in testing!
- Remove development tools from production servers
- Temporary passwords for installation

Key management

- Protection of cryptographic keys
  - Unauthorized change
  - Destruction
  - Revealing
- Procedures for
  - Key generation
  - Storing keys and their copies
  - Revocation

Success factors

- SP adapted to local culture
- Management support
- Distribution of responsibilities
- Incident reporting
- Educate users and IT stuff
  - Cooperation instead of giving orders
- Feedback, revision

Tech staff profile

- Autonomy, self motivation
- Desire to achieve
- Resistance to imposed rules
- Keeping in touch with latest technology
- Primarily identify with profession, then with organization
- Friendly discussion preferred to (bureaucratic) submission of written reports

Blessing White research 1995-98

Managers need special education

Towards conclusion

- Security standards can not be mechanically copied
- Impossible to make rules for everything
- It hinders development
- SP is for worst case situations
  - Creates distrust
  - Each employee and visitor are treated as potential source of problems

But…

- Security policy
  - Should be understood as process
  - Creates awareness
  - Predicts problems, simplifies solutions
  - Prevents repetition of mistakes
  - Discovers good procedures

  - Should not be used to prosecute people

My challenge

- People are the most valuable resource!
- Corporations treat people as replacable resource
- Define procedures to hire less capable, cheaper workforce
- Easiest way to lower risk is not to forbid everything

Implementation

- Gradual, localized
- Do not put rules above people
  - Solve problems, do not punish everybody with complicated procedures
- Employees should be introduced to SP
- Use each opportunity to educate users
  - To do their job in a secure way
  - To recognize and report incidents

Misconceptions

- Security can be left to administrators
- Users can take care of their systems
- Technology can solve all problems
  - Don’t worry, we have firewall
- We are safe because we have security policy
- Insufficient explanations for end users
- No cooperation between separate workgroups
- Security is separate activity
- Policies are not revised
- If we spend more on security, we will be safer

Security team

- Security specialists educate others
  - Job can be done in a secure way
  - Rise awareness
  - Test vulnerabilities
  - Help users politely, not push themselves and pose as smart guys
  - Each workgroup chooses one member as security specialist

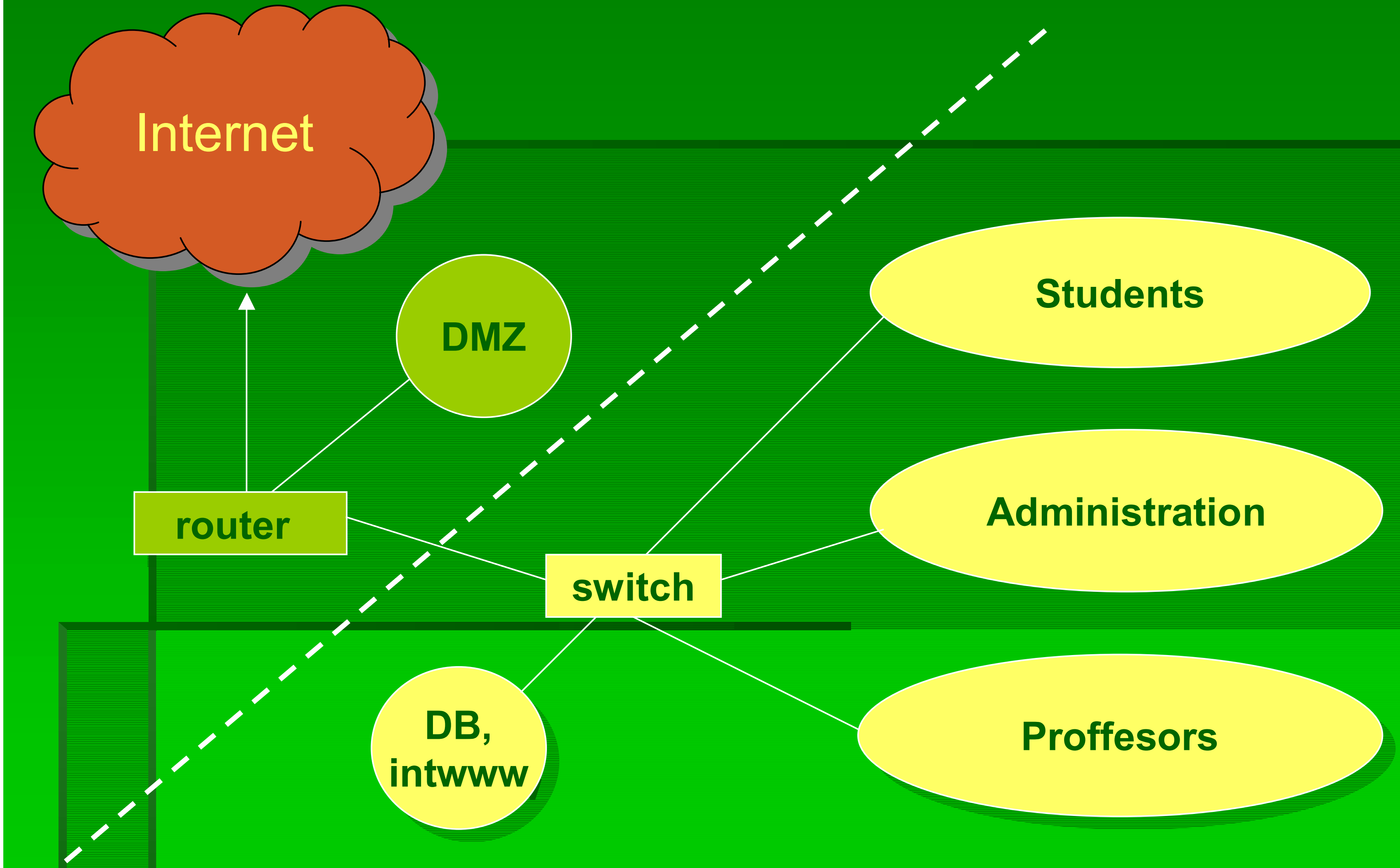
Implementation

- What are we protecting?
  - Inventory
    - Network connections
    - Hardware
    - Software
- Define critical resources
  - Should be in safe zone

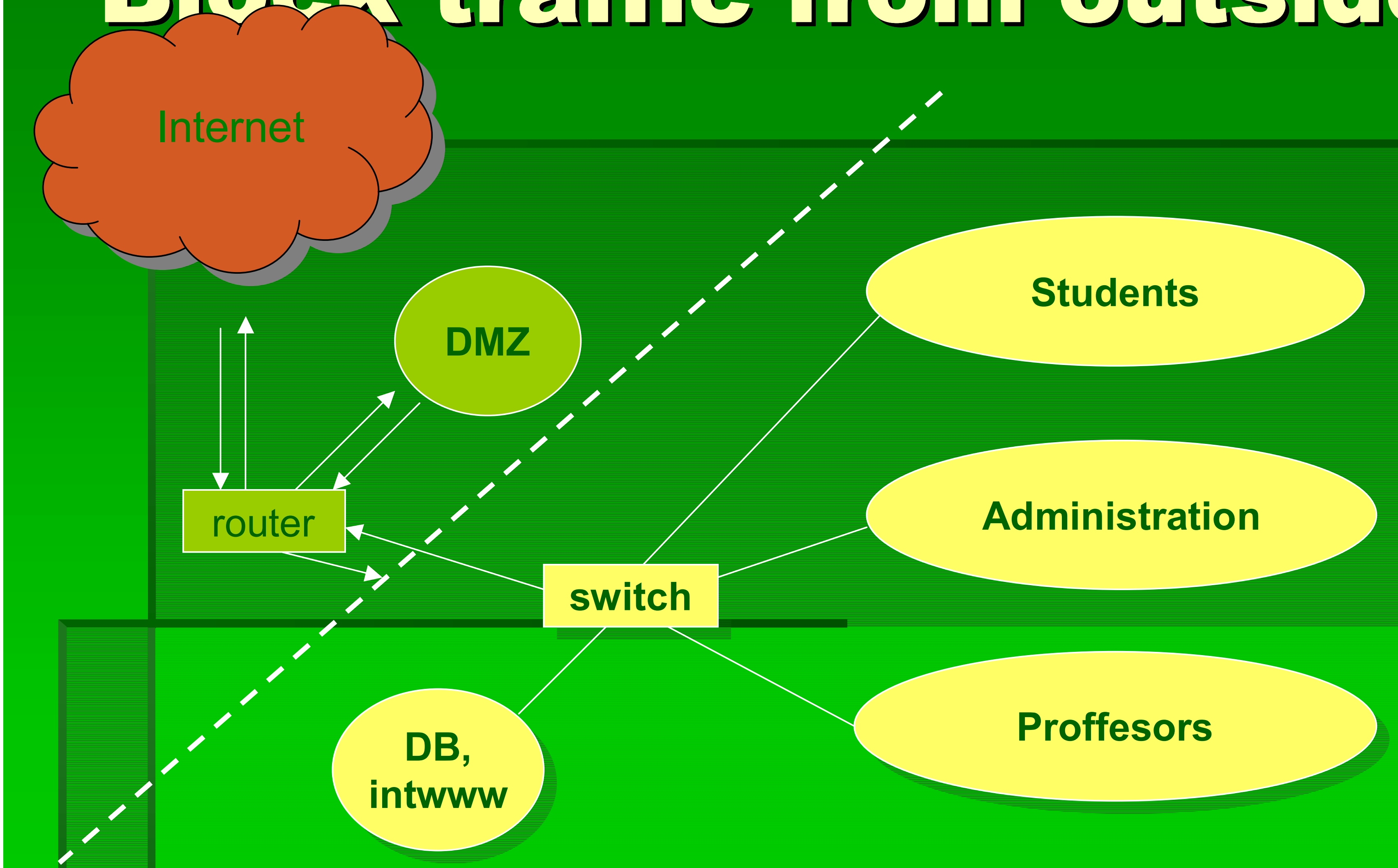
Network

- Needs reorganization

- DMZ
- Intranet
  - Subnets for workgroups
  - Visitors, mobile equipment..
- Extranet


Internet
DMZ
router
switch
Students
Administration
DB,
intwww
Proffesors

Block traffic from outside



Anti spoofing

- At perimeter block incomming private and local addresses
- LAN: 161.53.x.0/24, interface serial 0

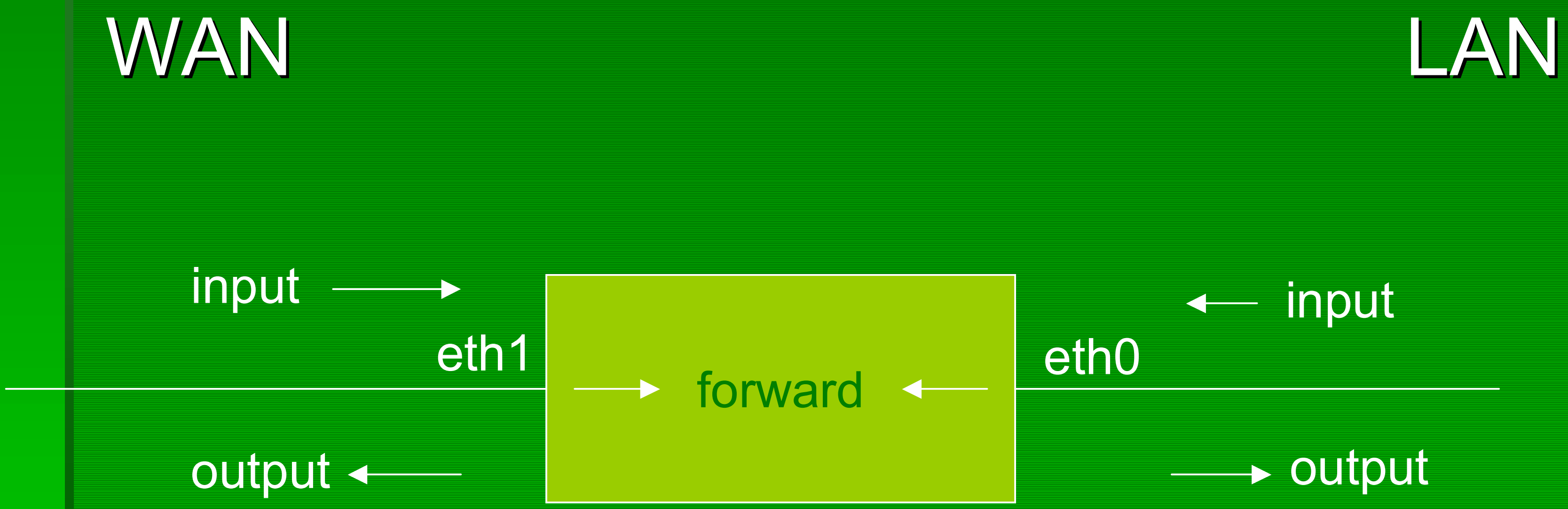
```
access list IN ...
deny   ip 10.0.0.0 0.255.255.255 161.53.x.0 0.0.0.255
deny   ip 172.16.0.0 0.15.255.255 161.53.x.0 0.0.0.255
deny   ip 192.168.0.0 0.0.255.255 161.53.x.0 0.0.0.255
deny   ip 127.0.0.0 0.255.255.255 161.53.x.0 0.0.0.255
deny   ip 161.53.x.0 0.0.0.255 161.53.x.0 0.0.0.255
permit ip any any
```

Anti spoofing...

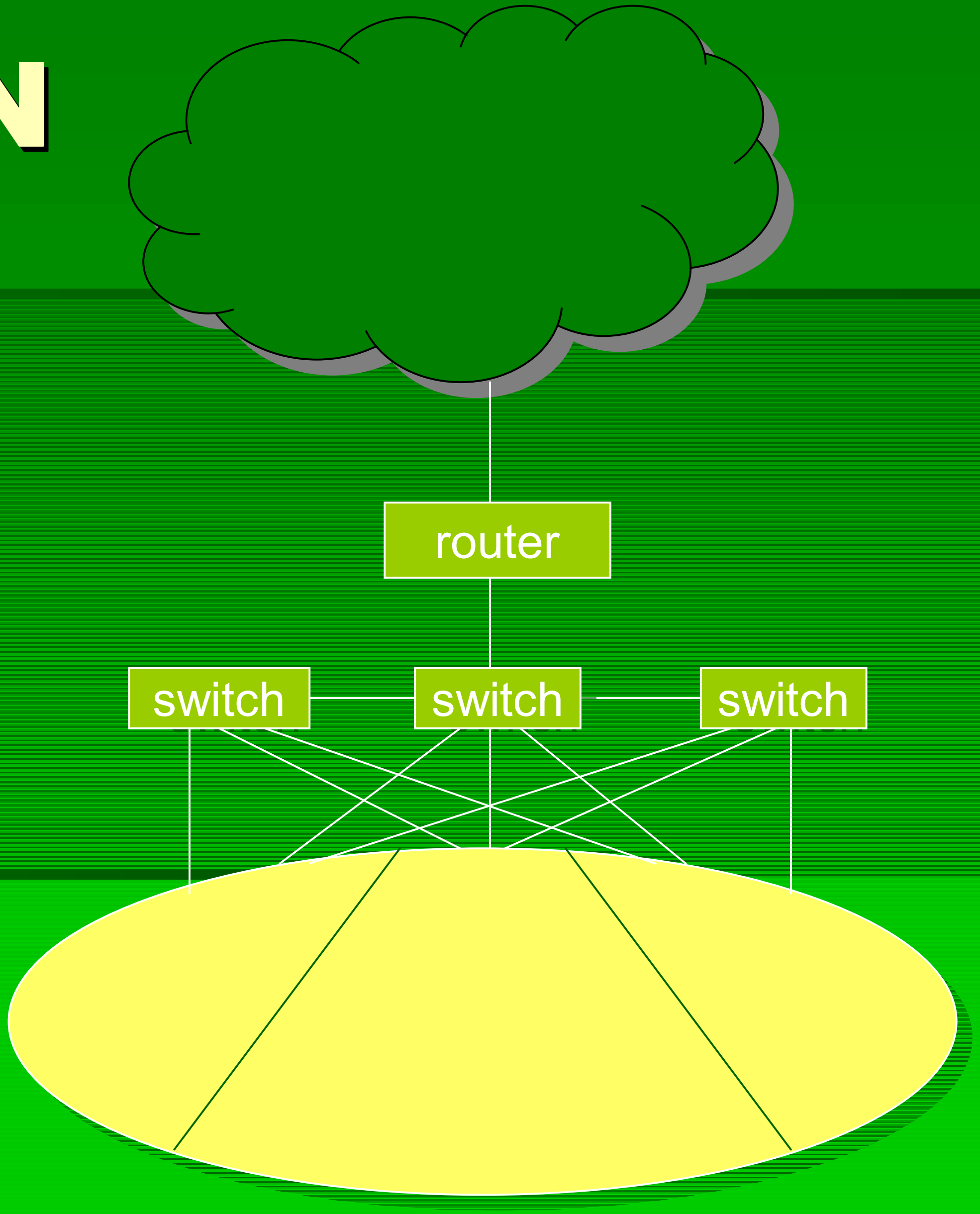
- Block outgoing source addresses that are not used in LAN
- Interface ethernet 1

```
access list OUT ...
permit ip 161.53.x.0 0.0.0.255 any
deny   ip any any log
```

Direction



VLAN



VLAN tagging & trunking

- VLAN tag in Ethernet frame
  - 802.1q
  - Linux supports it
- Extend VLAN over multiple switches
- Trunking port to connect switches
  - Ethernet frame encapsulated in trunking protocol

Inexpensive firewall

- **Dual homed host**
- **Linux w. multiple ethernet cards**

```
# ip forwarding
sysctl -w net/ipv4/ip_forward=1
# forwarding and NAT
iptables -t nat -A POSTROUTING -o $INET_IFACE
  -j SNAT -to-source $INET_IP
# masquerading
iptables -t nat -A POSTROUTING -o eth0 -j
  MASQUERADE
```

Throughput

- PCI bus
  - 33 MHz x 32 bits = 1Gb
  - 66 MHz
- PCI-X
  - 66, 133, 266, 533 MHz

Hide www server

- Server in private network
- Port 80 accessible from outside

```
iptables -t nat -A PREROUTING -p tcp -d
  161.53.x.3 \ --dport 80 -j DNAT --to
  192.168.4.3:80
```

Free IDS

- AIDE – detects changes in disk files
- SNORT – inspects packets, detects attacks
- CARNet projects
  - AIDE ARMS
  - SNORT Central

Literature

- University of California, Davis, LAN design
http://net21.ucdavis.edu/newvlan.htm

- Standard 802.1q, PDF doc, 211 pg.
http://standards.ieee.org/getieee802/download/802.1Q-1998.pdf

- Linux implementation
http://www.candelatech.com/~greear/vlan.html

On line resources

- CISCO Network Security Glossary

http://business.cisco.com/glossary/

- CISCO Design Implementation Guide

http://www.cisco.com/warp/public/cc/pd/si/casi/ca3500xl/prodlit/lan_dg.htm

- IBM Multisegment LAN Design Guidelines

http://publib-b.boulder.ibm.com/Redbooks.nsf/RedbookAbstracts/gg243398.html