Infrastructure Security

Economic Governance II Project
Office of the National Chief Information Officer
Material Author Mr. Peter Moore MBCS
Presented To Iraq Government CIOs
Date March 2006 Document Number 2
Version 1 Disposition Final

Intrusion Detection Systems (IDS)

What Characterises Intrusion?

- **Unauthorised access**
- **Misuse**
- **Maliciousness**
- **Stealing**
- **Corruption**

Intrusion Detection Systems (“Scanning” for intruders)

1. A Host-based component, eg. password, configuration check, audit of systems, identify suspicious behaviour, monitor individual computers, use of ‘sniffers’;
2. A Network-based component

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Intrusion Detection Techniques

Host Based:

- **Personal firewalls – locate the host software attempting the login, can monitor all login attempts;**
- **Host Wrapper SW (NUKE, NABBER for windows); TCP-wrapper for UNIX (equivalent).**
- **Ongoing testing for known hacks; Recording of system responses**

Network Based:

- **Switch the NIC to promiscuous mode, capture all packets, then use a sniffer to identify variations in packet signature: string, port, header etc. Exceptions treated as possible intrusion.**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Proactive Detection :

1. Automation – of System Auditing and Event Log analysis
2. Batch files – eg. use NT Scheduler to create logs and post activity audit information to them
3. Login scripts – to apply updates and enforce policies at the login environment level; Also use Login scripts to note IP address and host-name for all administrative logins: check for unknowns (intruders usually unaware of login script activity).
4. Delinquent users can build the system's security profile by trying different usernames, and may also try *switchuser*.
5. SNMP scripts - SNMP used for NW management – manages, configures and reports on devices: Scripts can be used to do SNMP notification by email or system message

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Principles of Detecting Network Intruders

Provision:

1. **Checksum Analysis** : 'crackers' can use either overt or covert Trojan Horses. Overt – direct insertion, detectable by antivirus. Covert – adulteration of system utilities that then get executed at login.

2. **Audit Log Analysis** : continual assessment and monitoring of system events.

NOTES:

- Most antivirus & scanners hold file checksums, file timestamps, size and version: these can all be managed manually; Benchmark them all at system-build, and after add-ons, upgrades and patches.

- Logging only major events is poor practise. Log more than the essentials, so that you can backtrack if you find a hack.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Dummies

Dummy Usernames : Waste the Hacker's time –

- **Dummy pwd file on UNIX**
- **Dummy Admin Accounts & files with strong passwords, hacker will attempt brute-force crack (L0phtcrack, LC3, Jack the Ripper -UNIX)**
- **Change the name of the Administrator account, give it limited rights or disable it;**
- **Decoy sharable files with attractive names, containing false information, eg: "Administrative passwords", "employee salaries"; they could display a warning to the intruder or send an alarm to the Security Officer if they are accessed.**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

HONEYPOT Decoy Server

Purpose: to bait and observe an intruder, and determine his M.O.

- **Either place it outside your Firewall, or create a specific hole through your firewall that permits access to only this server so that it is a constricted single entry point.**
- **Honeypot set up in imitation of your own server: will enable learning how to protect your real server. If the honeypot gets hacked, fix the vulnerabilities and wait for the next attack.**
- **NB! If the honeypot is compromised, a hacker can use it to hack other servers**
- **Honeypot factors:**
  1. **It is unimportant unless it is attacked;**
  2. **Resource : high NW traffic and bandwidth use can compromise some security tools, but the honeypot is unaffected;**
  3. **Data Collection : minimal but high quality.**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Types of Honeypot

Decoy objects range from Applets to whole Servers:

Simple	Complex
Mimics one or a few services Limits the hacker to connecting to several ports	An entire server with its Operating System and imitation services. Confines the hacker within that server.
Low Risk, because this is a low level of engagement, but the resulting information is also low;	Higher risk, because the hacker is engaging an entire Operating System. But it will gather the most data on the hacker.

Conclusion: simple honeypot that delays the intruder and alerts the administrator, will give sufficient information, and is safer.

"Entrapment" – beware of legal issue. Hacker may argue that he was persuaded to break the law when he had no prior intention.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Classes of IDS

Signature Intrusion Detection: checking against a database of known vulnerability signatures.

- **Statistical Intrusion Detection:** identifies departures from established usage profile without knowing the cause

- **Integrity Intrusion Detection :**

Up to date Signature Database	Occurrence of a specific vulnerability signature when checking against a DB
Benchmark user profiles	Audit trail, logon frequency, RAM/ROM usage, I/O, mill time
Detection that something has changed	Cryptographic algorithms to detect alterations – eg TRIPWIRE

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Features of IDSs

1. **Unattended operations, runs in the background, alerts you to an attack in progress.**
2. **Flexible and scalable to accommodate new software and configuration**
3. **Economical and Resilient**
4. **Decomposed Intrusion Detection – detect a pattern in isolated steps carried out over an extended period.**
5. **False Positives – must be tuned out so that it does not become "wolf at the door"**
6. **False Negatives – much worse: means that it has failed!**
7. **Subversion resistant – ie. Prevent the IDS being hacked**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

1 : Application-based IDS

1. Operates at the Application layer
2. Application-specific sensors embedded in each application send data to the Intrusion Detection System
3. Scalable and Easy to control
4. Can also send logs to the IDS
5. Off-the-shelf purchase: only for common applications, but now they are becoming more a standard feature
6. In-house written applications now should include application specific sensors in the systems design.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

2 : Host-based IDS

1. Operates on a single (Operating) System, sensors are installed in the system, including audit trails and logs.
2. Administrator must be intimately familiar with the System and the Users and their habits.
3. Residing on a single host, can verify system-file integrity, issue alerts on irregularities, sniff network traffic.
4. Are intimate with the OS and access kernel-sacred data (which is of high quality requiring minimal analysis – getting this over a network is harder)
5. Are precise and verify successful attacks; they use event logs.
6. Cheap to install, in both encrypted and switched environments;
7. But It Only Works On A Single Local Host! When installed separately on multiple hosts, creates a labour-intensive maintenance overhead!
8. Can be swamped by large logs or audit trails
9. It is difficult to find an IDS that supports all the applications on a particular host.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

3 : Network-based IDS

1. Installed on a standalone device or a server, can inspect every packet.
2. When installing on a server, choose strategic servers only
3. They inspect packet header, port number, payload content (using pattern recognition to detect the syntax of known attacks.)
4. Real-Time detection of passing packets (as opposed to *ex post* examination of logs and audit trails.)
5. Placed outside the Firewall, can detect all attacks, successful and failed.
6. They cannot deal with encrypted packets
7. Are less able to predict behaviour of particular hosts
8. High-speed networks may be too fast for the IDS, which is operating in Real-Time.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

4 : Knowledge-based/Behaviour-based IDS

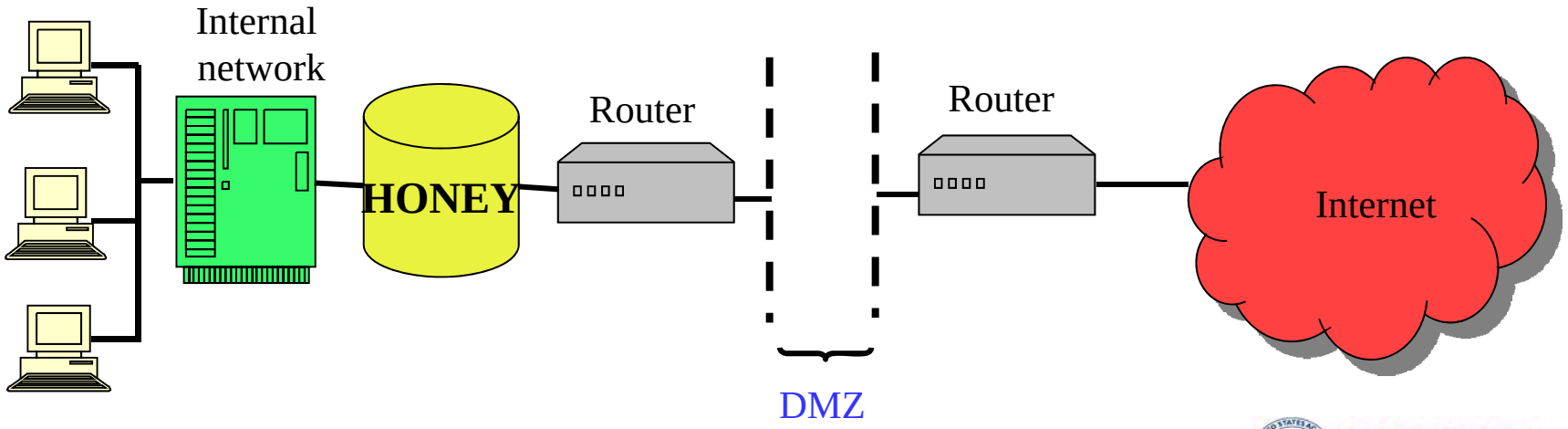
1. Attack-Signature based (similar to Application based) validating against a DB of known vulnerabilities and attack signatures;
2. This is “Misuse Detection”, whether attacks or other;
3. Fewer false positives
4. Provides detailed attack data
5. Requires regular update of the Attack-Signature DB – if it is not on the DB, it will not be detected.
6. Maintenance overhead to keep them updated
7. Not good for insider attacks
8. The “Behaviour-based” variety seldom used: detects “abnormal” user or system behaviour.
9. “Behaviour” requires regular updating.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

STRATEGIC IDS DEPLOYMENT: overview

Consider your Infrastructure and Policies:

- **Staged establishment to assess administrative overheads etc.**
- **Staff must be trained and learn to work with it.**
- **Host-based and Network-based: start with Network-based (because it is simpler), then add Host-based to priority servers.**
- **Perform a Vulnerability Audit.**
- **Locate the Honeypot close to or before the servers to be protected (topologically), at the edge of the DMZ.**



© 2006 BearingPoint, Inc. and/or its affiliate(s)

STRATEGIC IDS DEPLOYMENT: location

For NETWORK-BASED IDS, locate:

- **Put Sensors on all major routes –**
  1. **Outside the Firewall**
  2. **Between the Firewall and internal network, in the DMZ:**
     - **will detect anything that defeated the Firewall**
     - **will detect attacks on Web, FTP etc. servers in the DMZ**
     - **this monitors performance of your external Firewall**
     - **can also recognise attacks by the *outgoing* traffic from affected server**
  3. **Within a subnet**
     - **This will only detect local intrusion within the subnet: do so on high security subnets.**

For HOST-BASED IDS, locate:

- **Only on critical servers, because Host-based is tedious to install and maintain.**
- **If installed on multiple servers, then have centralised reporting and management functions.**
- **Host-based requires intimate understanding of User and System behaviour, including regular monitoring and checking.**

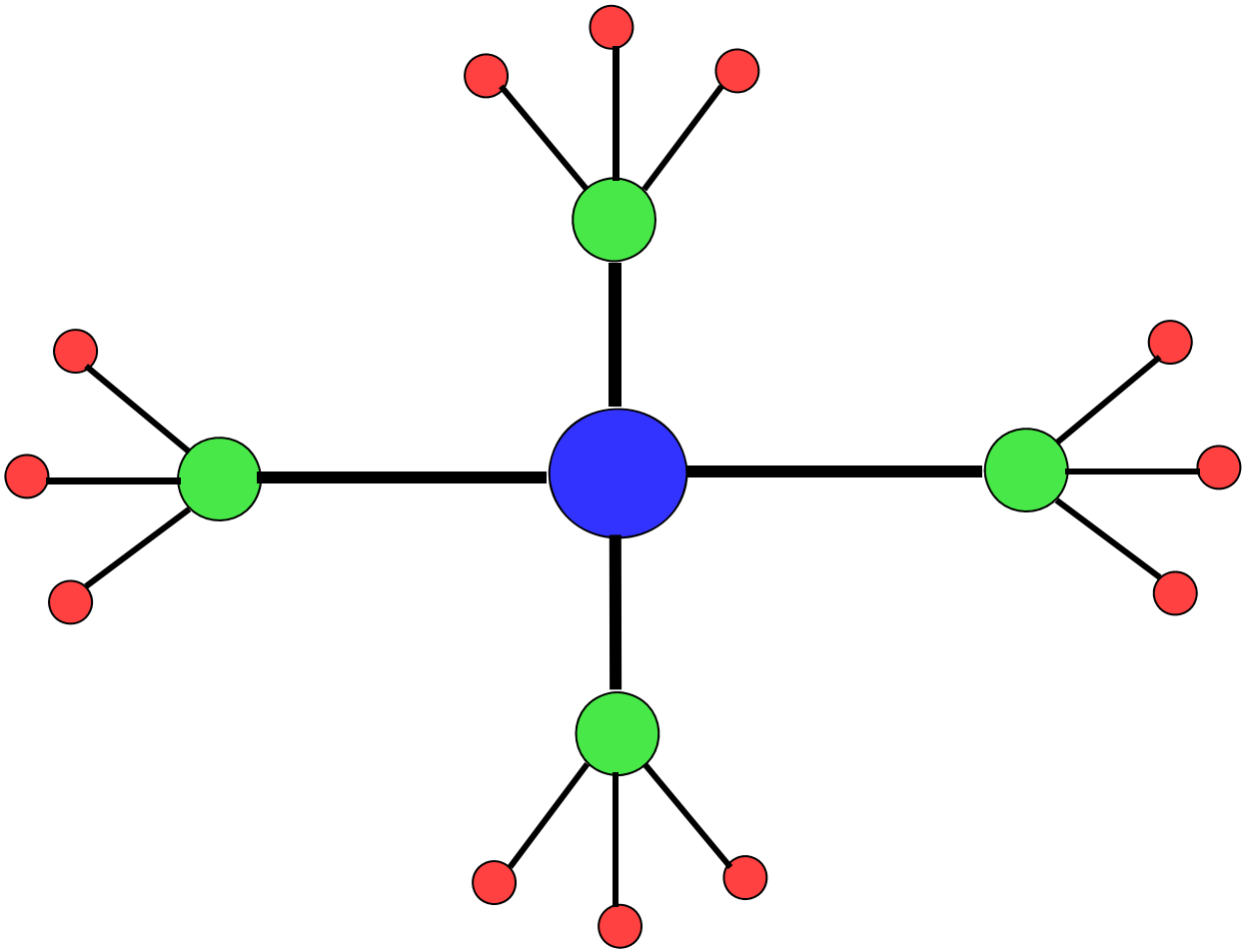
© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Have an Incident Response Procedure!

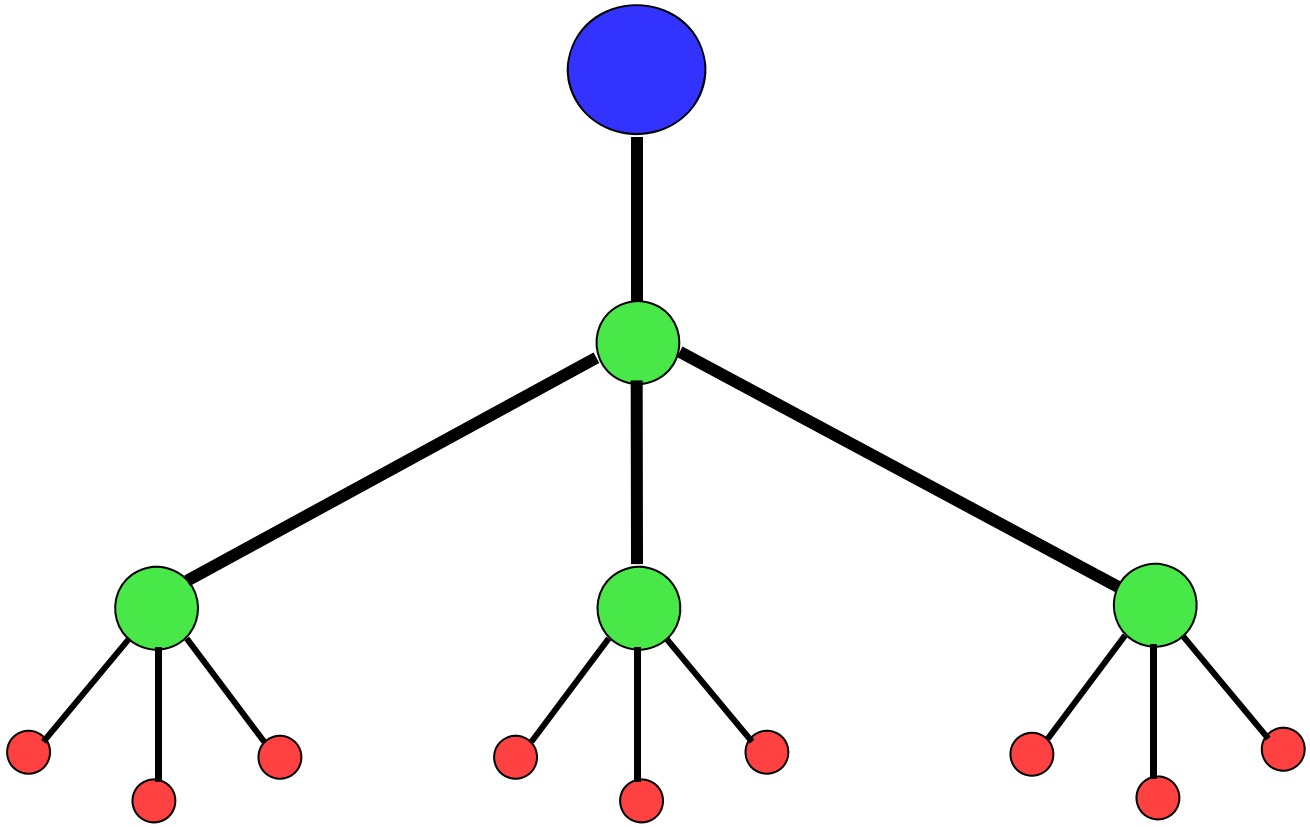
Network Technologies Review

EXTENDED STAR TOPOLOGY



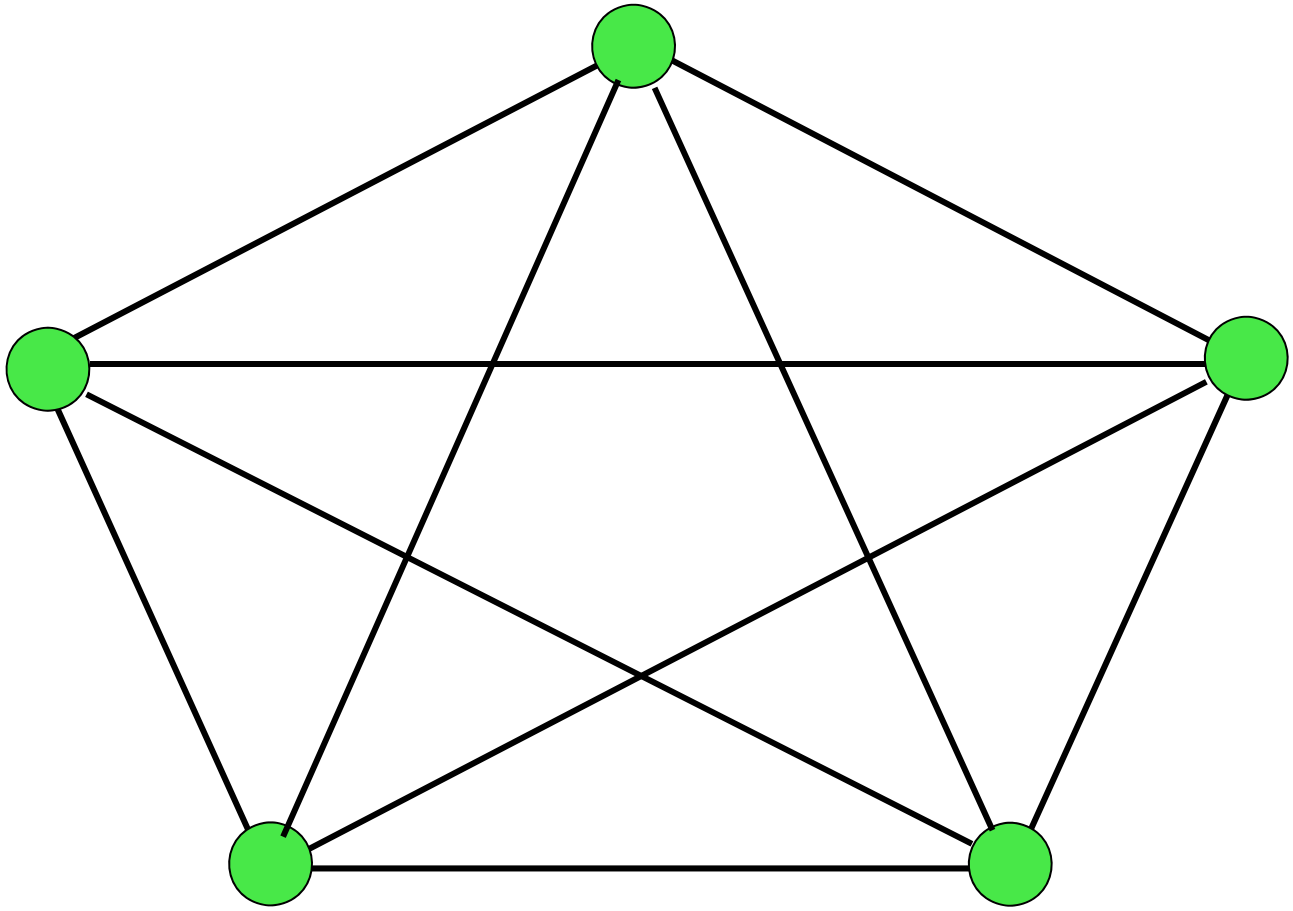
© 2006 BearingPoint, Inc. and/or its affiliate(s)

HIERARCHICAL TOPOLOGY



© 2006 BearingPoint, Inc. and/or its affiliate(s)

MESH or PLEX TOPOLOGY



© 2006 BearingPoint, Inc. and/or its affiliate(s)

Components and Symbology (1)

HOST : any device directly connected to a network segment ie. Requiring all seven OSI layers;

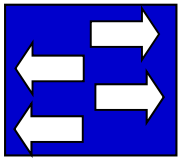
NIC & MAC ADDRESS : Network interface card with resident Media Access control address (6 or 8 Byte), Datalink, layer 2.

TRANSCEIVER : eg. connect router to network, copper to optical, layer 1

HUB and REPEATER : ethernet multi-port, passive, layer 1; The step from coaxial to UTP, also called a **Concentrator**

BRIDGE :

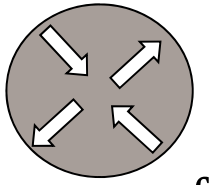
Layer 2, filtering and routing of local traffic between 2 network segments; superceded by router

SWITCH : 

Layer 2 multiport bridge

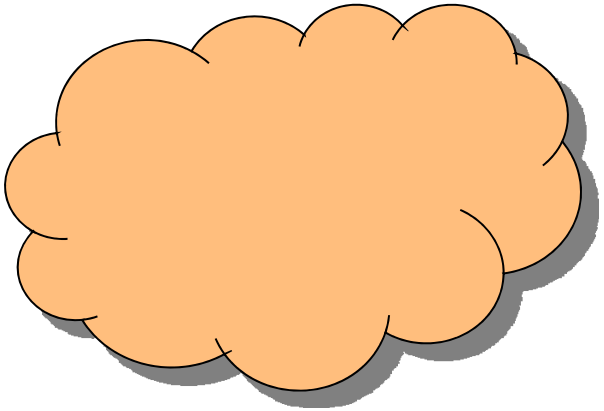
© 2006 BearingPoint, Inc. and/or its affiliate(s)

Components and Symbology (2)

ROUTER :  Network layer, OSI 3, path selection.

Used in convergence of Ethernet, Token Ring and FDDI protocol routing.

Incoming packets are layer 3 data. Router examines, chooses route and then assigns port, based upon the *network address* group (this is **not** the MAC address)

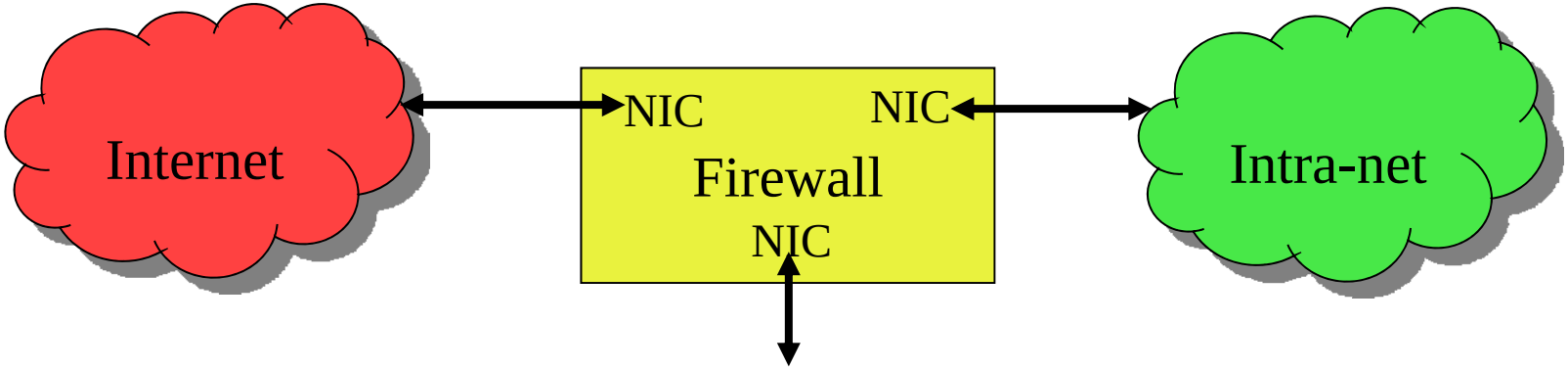


CLOUD CONNECTION, covers all 7 OSI layers

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Filtering, Firewalls and Proxy Technologies

Firewall and Proxy – Review (1)



Demilitarised Zone, Web, Mail, FTP servers

- Should be installed by the Security Officer and can also be placed between internal network segments as a bulkhead;
- Filter:
  - MAC addresses;
  - "Dynamic State List": real-time table, Firewall-maintained, will only forward incoming packets that are a response awaited by an initiator behind the Firewall;
  - ACLs, Access Control Lists: IPs and IP ranges that are allowed and disallowed.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Firewall and Proxy – Review (2)

NAT – Network Address Translation, Firewalls and Routers;

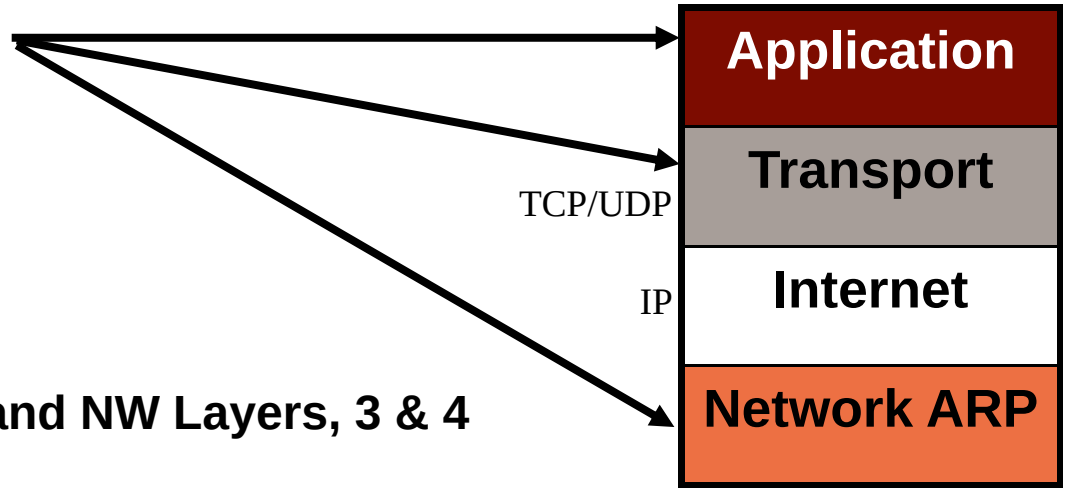
- **Uses various combinations of IP/port number to provide mapping between internal (non-routable) IP ranges, and external (ISP-allocated) IPs (overloaded IP);**
- **Solves IP address shortage;**
- **Hides internal addresses;**
- **Transparent to users;**
- **Protects internal hosts, especially from 'worms';**
- **Disrupts end-to-end connectivity and foxes some protocols;**
- **Configuration maintenance overhead.**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Firewall and Proxy – Review (3)

TCP/IP protocol layers



<u>FIREWALL</u> is Transport and NW Layers, 3 & 4

<u>PROXY</u> is Application Layer 7, can examine full packet contents for malware

- **Firewall often installed on the Proxy server**
- **Proxy is <u>not</u> transparent to users**
- **Proxy can impose content restrictions by keywords, and does caching of frequent-use pages, permits central NW administration, labour-intensive to maintain.**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Operating System Risks

Operating Systems Risks

Even bad administration habits are an OS risk.

1. **Passive hack eg. Keylogger:** a trojan that records every user keystroke.
   - Usually goes unnoticed, but an active attack is being planned!

2. **Active hack – ie. Malicious!**
   - *Replay attack* – record sensitive NW data then replay it with alterations to achieve unauthorised access.
   - *Insider* – the greatest threat! – data threat, and disruption threat.
   - *Spoofing* – copy a trusted IP address, or replace a trusted application with a malware version;
   - *Trapdoor attack* – alteration of OS or applications code, eg alter the outer environment script or the administrator's directory so that additional code executed at login, giving hacker access;
   - *DOS Attack* – denial of service, by causing it to crash or flood;
   - *Trojan Email Attachments*

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Port-scanning and Footprinting : NMAP

NMAP freeware, ***stealthy*** scans of host stacks over the network**:** open ports, services and operating systems (*footprint)* for vulnerabilities!

Hacker use of NMAP :

- **Full TCP/IP handshake scanning of ports – can be detected on logs by the administrator**
- **SYN scan "half connection" DOS attack – detectable by "SYNLOGGER"**
- **PING scan to reveal hosts & IPs**
- **IP Protocol scans to determine the IP protocols used on NW.**

Administrator use of NMAP :

- **Detecting Trojans on the NW – Trojans listen on UDP ports, NMAP can scan UDP ports.**

Other Stealthy port scanners :

- "Stealth" ; "FIN";
- "XmasTree"; "NULL"

© 2006 BearingPoint, Inc. and/or its affiliate(s)

WINDOWS Operating System Issues: NT-Based 1

a. **Banner Scraping:**
   - TELNET commands reply with OS banner in reply –change the default banner information – change all installation defaults!
   - "Security through Obscurity" – hide sensitive accounts, eg. Administrator, where it is possible to detect all usernames
   - Lookout for : Default Services
     - Default Permissions
     - Default administrative shares.

b. **NB. Must be actively configured – defaults are vulnerable!**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

WINDOWS Operating System Issues: NT-Based 2

a. **Default Shares: C$, D$, Admin$, IPC$;**

- These shares are created whenever Windows boots
- Windows should be configured to remove these shares from the Registry key at each boot:

- Edit: HKey LocalMachine\system\currentcontrolset\lanmanserver\parameters

  and Autoshareserver key

  set DWORD value to 0

- OR : use *autoexnt.bat* to specify the "*netshare*" command to delete the shares

b. **Default permissions vulnerabilities:**

- The "EVERYONE" group gives unrestricted network permission, including external : replace or restrict the "EVERYONE" group!

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

WINDOWS Operating System Issues: NT-Based 3

NT Default Services :

1	Workstation
2	Server
3	NetLogon
4	Eventlog
5	Alerter
6	Plug and play
7	Spooler
8	Messenger
9	Remote procedure call
10	Computer browser
11	TCP/IP NetBIOS Helper
12	Licence Logging
13	DHCP client

DoS attack

Social Engineering attack

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

WINDOWS Operating System Issues: W2K additionals

Additional options and services introduce new vulnerabilities. Active Directory uses **ACL**s to define network permissions – modify the ACL rights to prevent hacking.

DNS Client	Workstation
Task Scheduler	Server
COM	NetLogon
Protected Storage	Eventlog
RunAs	Licence Logging
Event	Plug and play
IPSec Policy Agent	Print Spooler
Systems Event Notification	Messenger
Network Connections	Remote procedure call
Removable Storage	DHCP client
Local Disk Manager	TCP/IP NetBIOS Helper
Remote Registry Server	Alerter
Distributed Link Tracking Client	Computer browser

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

LINUX SECURITY THREATS

Article handout on this subject.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Operating Systems Security Standards (1)

ISO & International Electrotechnical Commission IEC
- ISO/IEC 17799 (BS 7799) : Risks and controls :

1. **Network Security Threats**
2. **Securing Networks**
3. **Audit of Processes and File Systems**
4. **Anti-virus**
5. **Risk Assessment**
6. **Information Management**
7. **Legal and other issues**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Operating Systems Security Standards (2)

USA National Computer Security Centre (NCSC)
- Trusted Computer Systems Evaluation Criteria (TCSEC)
"Orange Book", Grades OS Security levels thus:

Level A highest	Level B	Level C	Level D Lowest
A1 Mathematically proven to be secure	B1	C1	No security at all, eg. DOS
A2	B2	C2	
A3	B3	C3	
Etc.	Etc.	Etc.	

© 2006 BearingPoint, Inc. and/or its affiliate(s)

TCSEC Ratings examples

Rating	Features
B1	Includes Security and Access controls that segment resources
B2	HW level security segment + protected memory
B3	Data-hiding and layering service
C1	No separate User Accounts, basic access only
C2	Identifies Users, protects data and resources

- **Common Criteria (CC) standard for Operating Systems integrates all the other standards, provides technical guidance for assessing Security and Products**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Windows NT – 2K – 2003 Architecture: Security Components

1. **Administrator Resources - the following mailing lists :**
   - Win2KSecAdvice
   - BestofSecurity
   - BugTraq
2. **Secure the following six areas of Windows-derivative OSs :**

Administration
Access Control
Auditing
Encryption
Ministry Corporate Security Policy
User Authentication

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Windows NT – 2K – 2003 Architecture: Security Features

- **Is an *object-based* OS, where data, processes, programs, system resources – are all system objects controlled by a single access point;**
- **Discretionary Access Control – ie. Specific to User;**
- **Restricts access to objects already in use by another application (restricts object re-use);**
- **Uses *Access Tokens*, *Security Descriptors*, *Secure IDS (SIDs)*, *Access Control Lists (ACLs)*;**

Security Subsystems:

Windows Task Manager

GINA

Security Support Provider Interface
Local Security Authority (LSA)
Win Logon
Security Account Manager (SAM)
Netlogon Server
Graphical Identification & Authentication Pkgs

These invoke other subsystems in the form of .dlls

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Windows NT – 2K – 2003 Architecture: Security Functions

Subsystem	Function
Security Support Provider	Provide Secure Authenticated Connections for Applications and service requests: ■ Verify the Users Information sent to GINA ■ Send SID to LSA for inclusion in the Access Token
GINA	Defines in the Registry the Secure Authentication Sequence (default MSGINA.dll)
LSA (Protected Windows Subsystem)	Loads the authentication software, creates Access Token, Manages: ■ User accounts ■ Trust relationships ■ Audit ■ Service accounts
NETlogon Server	Finds a Domain Controller, Authenticates the User, get the SID and Access Rights
SAM	Security Account Manager in the Registry of every machine, regulates users & permissions

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

IMPROVING OPERATING SYSTEM SECURITY

1. ***Patch*** **- temporary 'fix'**
2. ***Bug-fix*** **- permanent 'fix'**
3. ***MS Hot Fix*** **- permanent fix of a specific bug released between service packs**
4. ***MS Service Pack*** **- Cumulative total of all prior service packs**
   - *Fixes*
   - *Patches*
   - *Additional Features, More advanced tools*

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

Unnecessary Windows Services :

- **Disable needless Windows services :**
  Eg. 'scheduler' service is vulnerable as it has full system permissions;

- **It is better to Disable than Delete,**
  Delete will remove from OS and Registry
  If you delete, take a SYSTEM BACKUP first!
  - otherwise it requires a full OS re-install to replace any missing Service;

- **Only if this is not a Domain Controller!**

- **Set Autostart Services to Manual**
  This is a useful alternative to disablement. Especially if another autostart service depends on it, it will still start automatically.

Alerter
Clipbook Server
Computer Browser
DHCP client
Directory Replicator
Messenger
Remote Procedure Call Locator
SNMP Trap Service
Spooler
Telephony Service

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

More Windows Server Details

1. **Server caches user logon information and credentials for use when Domain Controller unavailable. Disable this cache so it cannot be hacked**
2. **Guest Account: Disable it *and* assign it a secure password;**
3. **Prevent the previous username appearing by default in the login box;**
4. **Any Windows user can, by default, install a printer driver (permitting the ingress of Trojans!) Restrict this ability to install printer drivers;**
5. **Rename the Administrator Account; Create a spoof "Administrator" account with a strong password and no rights;**
6. **Limit the access to shared resources (printers, ports etc.) to Administrators as a group; then create non-but share rights for specific users;**
7. **Obliterate the system pagefile at system closedown (by default it remains)**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Unnecessary UNIX Daemons :

- **Depends on the specific vendor implementation**
- **Install all relevant patches, especially if using the following Daemons:**

SMTP
TeLNet
Trivial FTP
Sendmail

© 2006 BearingPoint, Inc. and/or its affiliate(s)

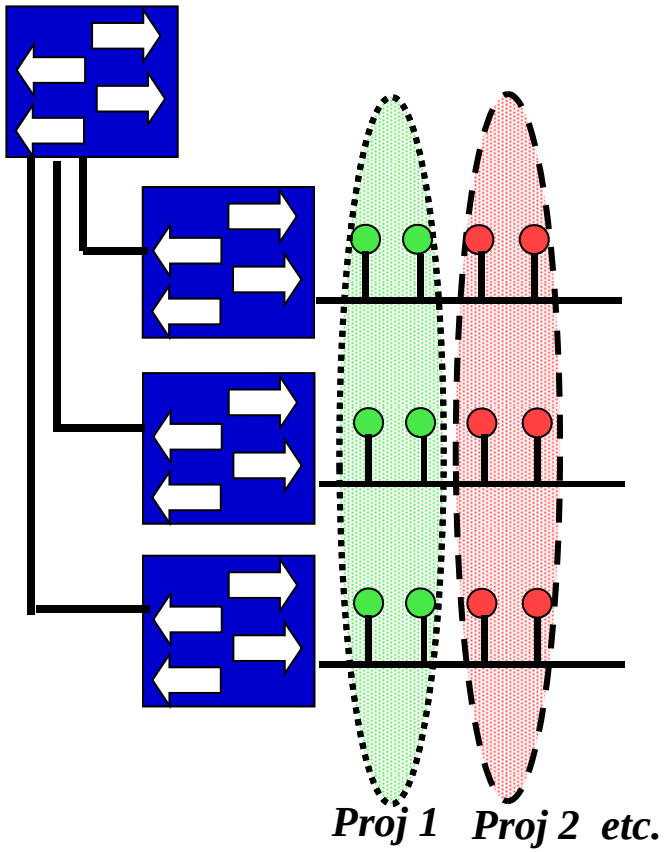
USAID FROM THE AMERICAN PEOPLE

SECURITY TOPOLOGIES - VLAN

VLAN

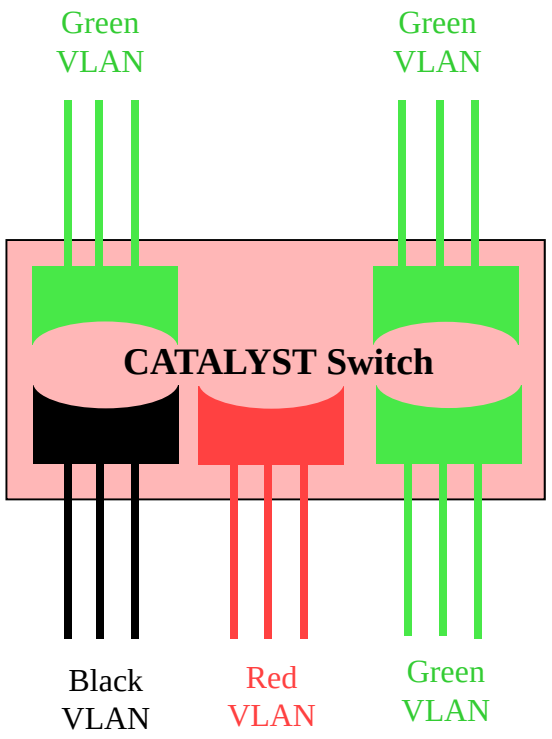
Virtual LAN technology, based on multiple NW segments, cascaded switches, and logical user-groups:

- **Connects Logical Workgroups**
- **Each port switch is on <u>only 1 VLAN</u>**
- **Broadcasts are to individual VLANs only**
- **VLAN = one or more switches**
- **Inter-building, or across a WAN**
- **Like multiple virtual bridges in a box**
- **This is a CISCO-based architecture**



© 2006 BearingPoint, Inc. and/or its affiliate(s)

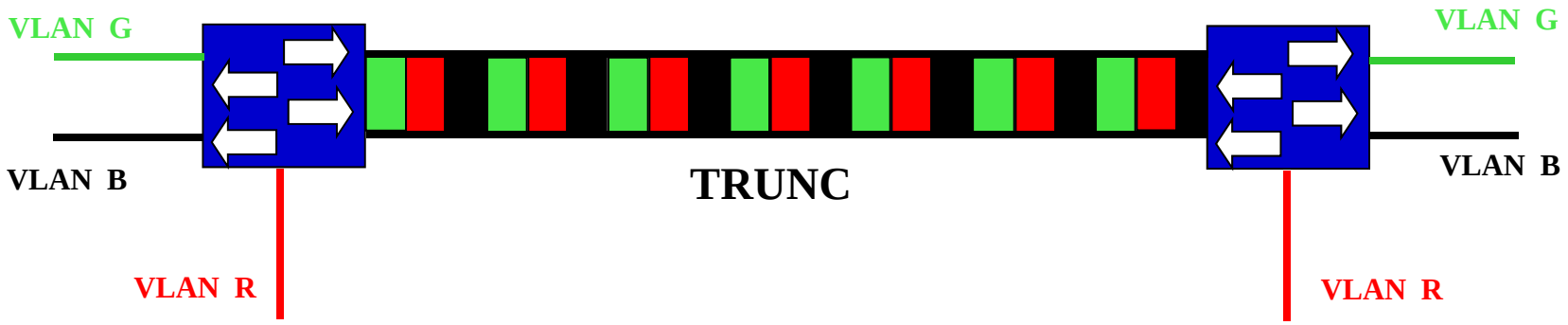
Multiple Virtual Bridges in a Box



- **Catalyst Switch**, configures multiple VLANs in a single piece of hardware;
- This is **CISCO** proprietorial technology. Each VLAN configured on the switch implements address-learning, forwarding/filtering decisions, and loop-avoidance mechanisms, as if it were a separate physical bridge;
- The software only forwards data to ports on the same VLAN as the originator;
- Uni-, multi-, and broadcast is limited to a single VLAN;

© 2006 BearingPoint, Inc. and/or its affiliate(s)

CATALYST Switches in Series



In order to span switches (as opposed to cascading switches), CATALYST requires a special trunc;

*****

2. Dynamic Membership Mode CATALYST Ports,

1. VMPS - VLAN Membership Policy Server: this must be installed on a CATALYST 5000 or other server (*Not* on the 1900 series switch itself).

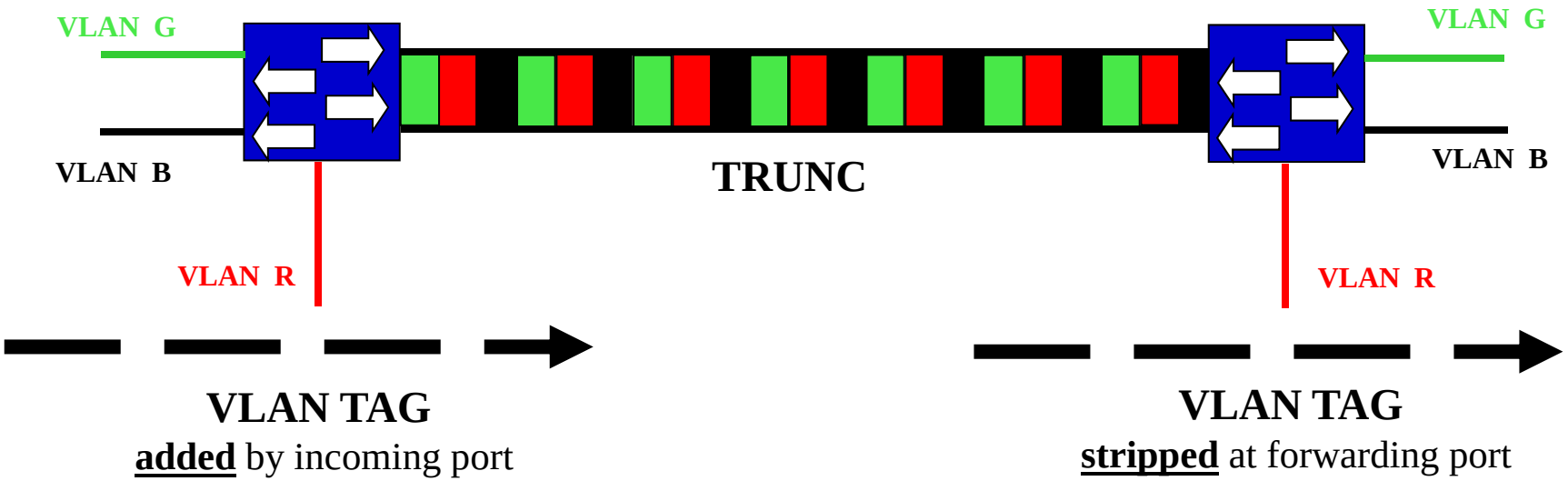
2. VMPS maintains a table of <u>MAC address :: VLAN assignment</u>

3. When a frame arrives on a dynamic port, the MAC address is used to determine the source VLAN;

- A dynamic port may only be on one VLAN at a time;
- Multiple hosts may be active on a dynamic port only if they are on the same VLAN.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

ISL Protocol from CISCO (OSI Layer 2: Datalink)



- **Inter-Switch VLAN (ISL) routing information:**
  is a CISCO protocol to maintain VLAN information over multiple switches, by adding a VLAN TAG to passing frames;
- **ISL frame-tagging**
  is a low latency mechanism to MUX traffic from multiple VLANs over a single physical path.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

ISL VLAN Features

1. Security! – each VLAN is a separate secure domain, like implementing firewalls on a single physical infrastructure;
2. Provides virtual LANs while maintaining full ethernet wire speed in half or full duplex;
3. ISL implements VLANs over a backbone, and works point-to-point;
4. Transparent to clients and servers. Frame contents are irrelevant;
5. All switches, routers and NICs must be ISL-capable;
6. An ISL-configured router can send data inter-VLAN;
7. ISL encapsulates the frame at the datalink level adding a 26 byte ISL Header, and a 4 byte CRC;
8. Implements the Spanning Tree Protocol;

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

SECURITY TOPOLOGIES - NAT

NETWORK ADDRESS TRANSLATION - NAT

- **RFC 1631 "IP Network Address Translator" – to fix IP address depletion using a Border Router.**
- **Converts non-routable IP to a registered routable IP**

1. Static NAT – simple 1:1 internal:external IP mapping;

2. Dynamic NAT – border router configured with the internal IPs that must be translated, and which pools of addresses can be used as externally-visible addresses.

3. Load Sharing NAT – TCP load distribution feature that maps each new incoming connection to a different router in a round robin.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

NAT Uses

1. Security! – Makes your internal host addressing invisible outside;
2. Use NAT when :
    1. Internal clients do not have global IPs;
    2. Or – change of ISP requires you renumber your network;
    3. Or – merging two intranets with duplicate IPs;
    4. Or – simple load sharing and maintenance.

NAT uses the fact that a minority of hosts in the stub domain communicate outside the domain at a given time, so only few need translation at a time; Addition of new hosts is also easy.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

NAT Pros and Cons

ADVANTAGES	DISADVANTAGES
▪Conserves Legal Registered Address by DHCP pools. ▪Reduces Address Overlap. ▪Increases Internet flexibility. ▪Reorganisation does not require address renumbering – "Deprivatisation" can be done without renumbering IPs.	▪ Switching Delay (translation latency) 1. Does this IP need translation? 2. Alter the IP header 3. Maybe alter TCP header also; ▪ No end-to-end IP trace possible – but this means a hacker also finds it hard to determine source and destination IPs; ▪ Some applications do not work with NAT: they must use either qualified domain names or Static IP.

© 2006 BearingPoint, Inc. and/or its affiliate(s)

Content Summary

1. **Intrusion Detection Systems**
   - Proactive Detection
   - Login Scripts
   - Principles of Detecting
   - Audit Analysis
   - Distracting Intruders
   - Intrusion Detection and Analysis
   - Features of IDS
   - Application Level IDS
   - Host Level IDS
   - Network Level IDS
   - Knowledge-based IDS
   - IDS Deployment
   - (Securing Voice Article)
2. **Incident Management** (Incident Response Article)
3. **Network Topologies and Protocols**
   - Network Infrastructure Hardware
4. **Filtering, Firewall and Proxy Technologies**
   - Proxy Firewall
   - Packet Filtering and ACL
   - Network Address Translation
   - Proxy Services
5. **Operating Systems Risks**
   - Introduction to Operating Systems Risks
   - NMAP
   - NT and W2K-based Issues
   - Defaults are Vulnerable
   - NT and W2K Default Services
   - Linux Security Threats (Article)
   - The Importance of OS Security
   - Orange Book
   - Securing the OS (Windows &c.)
     - Windows Security Architecture
       - Services
   - Tools and Scripts to Test OS Security
   - Improving OS Security
   - Patches and Maintenance
   - Unnecessary Services
   - More Windows Details (Registry Article)
   - Unnecessary UNIX Daemons
6. **Security Topologies**
   - VLAN
     - CAT 1900 Series Switch
     - ISL Protocol
     - Security Value
   - Network Address Translation - Uses
   - Network Address Translation – Pro and Con
7. **Content Summary**

© 2006 BearingPoint, Inc. and/or its affiliate(s)

USAID FROM THE AMERICAN PEOPLE

BearingPoint™

Business and Systems Aligned. Business Empowered.™