GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Facing Security on a Boosted *RREN* Backbone

Author: Carlos Fragoso Mariscal

GSEC Practical v.1.4b – Option 1 – April 2003

Networks live in a stressful evolutional ' *life cycle'* where technology pushes on continuous changes. Regional Research & Educational Networks (*RRENs*) because of its research purposes are supposed to be in possession of the latest networking advances.

This paper describes security challenges that should be faced when a layer -2 WAN backbone, mainly based on Asynchronous Transfer Mode (*ATM*), becomes a brand new layer -2/3 one based correspondingly on Ethernet and IP. A new door opens to next -generation services deployment scenario.

Index

1. Introductory thoughts
2. Landscape and Roles
3. Evolutional Issues
4. L2 - Ethernet Issues
    a. Functionalities
    b. Threat Mitigation
5. L3 - IP Issues
    a. Functionalities
    b. Threat Mitigation
6. Conclusion
7. References

---

1. Introductory thoughts

Mankind's history is a continuous effort to evolve the knowledge where information is its most valuable asset. Computers and networks were born as terrific tools to boost that evolution through resources sharing and information accessibility.

Internet has become a worldwide puzzle where each piece is like a small kingdom with the strong need of being well -linked with the rest of the world despite their different purposes (commercial, educational, entertainment, etc). A Regional Research & Educational Network (RREN) is one of those kingdoms where information and resources are shared by the local community but also has a common export and import

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

policy. Networks are neither technological nor topological static because if a RREN wants to be a healthy community, providing a strong connectivity is as much important as having valuable contents. That is why its 'life cycle' must be taken seriously and its evolution milestones carefully planned.

It seems great being a part of that big puzzle, but is it all that great? The answer is NO, it is NOT! Read this wisely thought of an Internet pioneer extracted from "*Cisco System's ISP Boot camp*" (introduction slide p.4) [ISR-BG01]:

> *"The wonderful thing about the Internet is that you're connected to everyone else. The terrible thing about the Internet is that you're connected to everyone else."* – Vinton Cerf

Fig. 1 - Internet representation extracted from "*Atlas of CyberSpaces*" (belongs to Warriors of the Net video) [OTH-AC01]

Internet growth corrupted its initial trust model making security one of the main topics that should be faced not only when a new network is created but also when changes are applied.

Let me describe a funny comparison: if you were medieval king (IT Manager), you would like your kingdom (network) to be a competitive place where products (packets) can be successfully exchanged (internally and externally). Your knig hts (Security/Network staff) would be in charge of protecting your kingdom from becoming a battlefield (hacking attacks).

---

2. Landscape and Roles

It is always very important to know your environment in detail to find out its requirements, necessities, r estrictions. The more you know it, the better you will face any matter. Sometimes it is known as '*in-the-business'* knowledge (cumulative *know-how*).

In this section it is going to be described the landscape of a RREN and the different entities that you shou ld know about.

At this point you will more or less know what is a RREN. Yes! The network with research purposes mentioned a few lines ago. But, do you know who participates on it? Take a look at *Figure 2*:

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

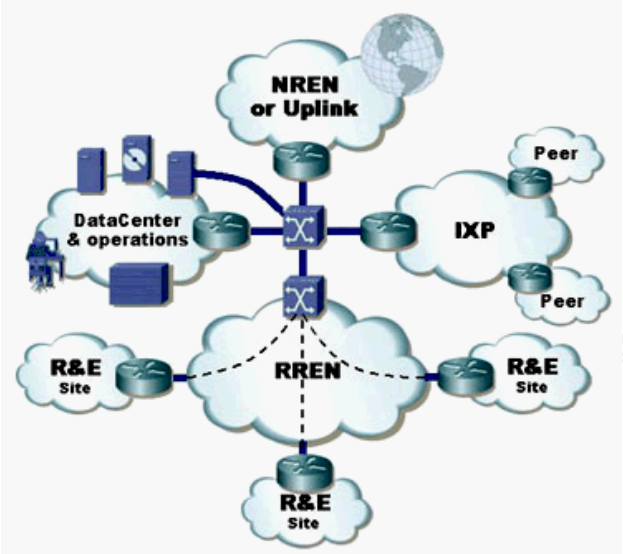

Fig. 2 - RREN (ATM-based backbone) and external entities

A RREN is usually integrated by the following entities:

- Research and Educational Institutions (R&E)

  In a commercial environment they would be known as '*customers*'. They are independent from each other but could be geographically dispersed in many sites. They are supposed to take advantage of the network for worldwide connectivity and research projects with external and local R&E entities.

  It is important to know that each one has its own different security policies.

- Telecommunications Provider (Telco)

  Provides the communication links: core, access for each R&E site and transport to the central core equipment. They live on layer 1 and 2 of the Open Systems Interconnection (OSI) tower.

- Network Operation & Management Center (NOC)

  Management and technical staff that operates the network. It is usually the intermediary with the Telco for link fails, bandwidth upgrades, maintenance operations, and so on.

  If they operate at layer 3 (IP transit provider) then they would also be involved in the security chain, in any other case they only manage connectivity.

- Supercomputing and Internet Services Center

  Provides shared resources that could be used by R&E institutions for its projects (*saving by sharing*): computing, remote storage, web housing/hosting, etc.

  Its main advantages are cost and high-speed direct connection to the backbone preventing R&E access links saturation.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

It has its own security policy, although it is commonly suited for easing R&E access to services (lightly distributed trust).

- Regional government (research area)

  It finances a part or the total cost of the network (infrastructure, operation/management), commonly the core network, NOC and Supercomputing/Internet Services, then each R&E pays only for its access link.

An example of RREN could be *Anella Científica* (*Scientific Ring*) located in Catalonia. More information could be found at Supercomputing Center of Catalonia (CESCA) website [REN-CS01].

As mentioned before, a RREN is not only a lonely island. Its external relationships are performed through the following peers:

- National Research and Educational Network (NREN)

  If exists, it acts as a hub for the different RRENs and R&E sites without a RREN on its area. It provides a backbone for layer 3 (IP) transit.

  They are always a part of the security chain, they usually force R&E institutions to sign an Acceptable Use Policy (AUP) when they join in the network.

  An example of NREN could be RedIRIS (Spanish NREN). More information at their website [REN-RI01].

- Transit Providers (Carriers/Uplinks)

  Telco companies and ISP's providing billed IP transit for the network. They are used by a NREN when a RREN does not exists for transit purposes or as a backup transit provider.

- Internet Exchange Point (IXP) Peers

  They are usually used to exchange geographically located traffic. On this way you alleviate uplink transit. The non-profit ones are usually participated by RREN / NREN's.

  An example of IXP where a RREN exchanges traffic is the CATalonian Neutral Internet exchange (CATNIX). You could take a look at how much traffic is exchanged on its website [OTH-CT01].

Oh my god! Too much information? Let's talk a little bit about it.

The important thing to know is that our big kingdom is also divided in small kingdoms. They are quite independent and each one owns a different security policy.

Considering a network like the one illustrated in Fig.2, the security is a matter among each R&E and uplink entities (NREN, IXP) and also between R&E's (distributed security topology). There should be an Acceptable Use Policy document for each external entity, especially for NREN because of research purposes.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. Evolutional Issues

Let me ask you something. What could happen concerning security if there is a technological evolution on the backbone? You will surely answer that such change should not matter at all. It is not really true.

Take a look at the following picture:

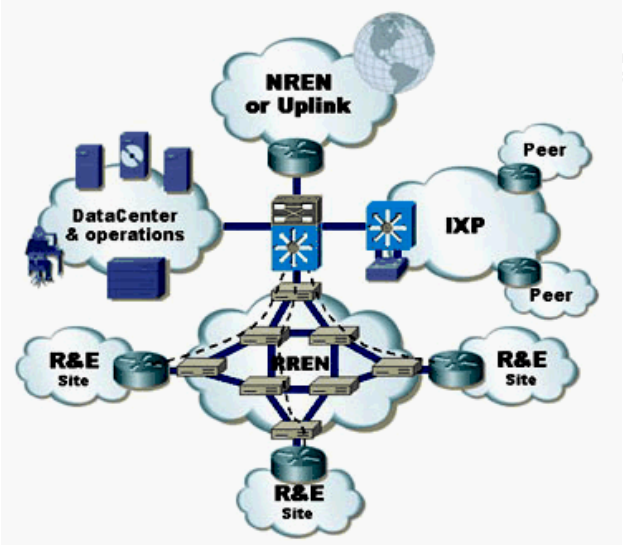

Fig.3 - RREN (Ethernet backbone with an IP core) and external entities

Wow! Looks great, doesn't it? The old, expensive and rigid ATM backbone has been replaced by one of those trendy Ethernet Metropolitan Area Networks (*MetroEthernet*). I am sure that most of you are familiar with Ethernet in LAN environments, so imagine its benefits applied to a backbone: low cost, high speed links (10/100 Mbps, 1/10Gbps), 10GigE), troubleshoot ease, scalability, and what about security? Well, we will talk about it in next section (L2 – Ethernet issues). In case you want more information about Ethernet evolution, there is a great presentation from the University of Hampshire [ETS-HK01].

Despite Ethernet, it may seem more or less the same but there is a big change. The RREN has grown up and now owns its own IP core (a scalable and functional multilayer switch). I have got good and bad news, which one would you like to know first? Okay, the good one is that this new topology allows to deploy a lot of new generation technologies based on IP. The bad one is that security matters have dramatically raised.

Now the RREN has become a direct uplink for the R&E sites. There are three sentences extracted from *"Cisco System's ISP Bootcamp"* (introduction slide p.10 -13) [ISR-BG01] that describes that:

> *"ISP protects itself from the customers and the Internet"*
>
> *"Protects customers from the Internet"*
>
> *"Protects Internet from their customers"*

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

What I want you to know is that scaling up one layer in OSI tower means some security and management changes:

- The NOC role becomes more important because now has to deal with routing matters between the R&E institutions and the previously mentioned external entities.
- A kind of Computer Emergency Response Team (CERT) or security department inside the NOC must be created in order to coordinate security incidents and face security attacks on our new '*battlefield*'.
- An Acceptable Use Policy must be created that suits the RREN and also the relationships with the external entities, specially uplink ones.
- New procedures, checklists and documentation must be created in order to support the new responsibilities. Remember this sentence extracted from SANS Security Essentials Courseware: "If it isn't written, it doesn't exist".

Although it is an old website, you could find very interesting ISP resources "*Resources for Network Operators & ISPs*" from Merit Network Inc. [ISR-MN01].

As IT professionals we must be prepared to face new threats: denial of service attacks (*DoS*), injecting bad traffic doing spoofing, core equipment compromise attempts, etc.

Now it is time to talk deeper about technology. The next two sections describes the main functionalities and threats of layer 2 technology (Ethernet) and layer 3 protocol (IP).

L2 – Ethernet Issues

Since Ethernet was born in 1973 at Xerox Corporation's Palo Alto Research Center, it has been a quite well-known technology because of its predominant paper in LAN environments (coexisting with IBM Token Ring technology). The Institute of Electrical and Electronical Engineers (IEEE) standardized it as part of the 802.3 group.

It is a data-link technology that specifies a frame communication over a shared medium where multiple nodes are able to talk. It provides addressing (MAC addresses) and access mechanisms to minimize collisions (CSMA/CD). A short tutorial about Ethernet could be found at "*HowStuffworks*" website for further information [ETS-NP01].

The main limitations of Ethernet were related with scalability and distance. They are no longer limitations because technological advancement supplied them with switching, full-duplex communication and high-speed long-distance links. That is why it is becoming the '*everywhere*' data-link technology: simplicity, cost, ubiquity and SPEED! (Thank God!)

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Functionalities

It is not the purpose of this paper describing Ethernet in detail, but you should know some concepts related with Ethernet switching:

- Virtual LAN (VLAN)

  It is one of the most important concepts. It allows to logical separate communications by means of tagging datagrams (802.1q or other vendor proprietary like Cisco's ISL). The formal definition extracted from the standard is:

  > *"VLANs facilitate easy administration of logical groups of stations that can communicate as if they were on the same LAN … Traffic between VLANs is restricted. Bridges forward unicast, multicast, and broadcast traffic only on LAN segments that serve the VLAN to which the traffic belongs."* [ETS-IE01] p.2

  The ports are now in trunk (tagged frames) or access (normal) mode that gives us a lot of flexibility. Trunk port between switches, between switch and a router, and why not between a switch and a host. For instance, Linux Operating System VLAN 802.1q implementation (kernel patch) downloadable at [ETS-BG01].

  Some protocols were born to ease management: Dynamic Trunk Protocol (DTP) and Virtual Trunk Protocol (VTP). The first one gives ports the choice to negotiate the trunking and the second one to pass VLAN management information between switches.

- Spanning Tree Protocol (STP)

  It is a great feature created to avoid loops. It works by creating a topology map, electing a root bridge and then electing in every switch one port in 'forwarding' state on each segment. The rest are in 'shutdown' state but can be activated in case of link failures (providing redundancy).

  Without STP if there were any loop, then a *"broadcast storm"* could happen. When a switch receives a broadcast, it is forwarded through all the ports (on the same VLAN of course), so if a loop exists broadcasts would enter it and get multiplied.

Threat Mitigation

You must take a look at two great papers published at past BlackHat 2002 Conference that focus on L2 Ethernet attacks and their mitigation called "Hacking Layer 2: Fun with Ethernet switches" [ETS-SC01] and "*Putting 2 and 2 Together: Designing Security into your Network Infrastructure*" [ETS-SD01]. Some of the attacks described here were extracted from that documentation:

- MAC Flooding

  The attacker floods the switch with spoofed MAC entries in order to fill up the switch table causing a hub behavior because of overloaded state.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Mitigation: limiting the number of MAC's to be learnt on each port, static MAC configuration (administrative burden)

- VLAN Hopping

  The attacker injects traffic to another VLAN either negotiating its port to trunk (talking DTP with the switch) or crafting double tagged frames (externally tagged with the VLAN ID of where a trunk nati vely belongs to). The first case is a bi-directional communication, the second one is only unidirectional (from attacker to victim).

  Mitigation: disabling DTP or only enabled where necessary, use of an exclusive native VLAN for each trunk.

- STP

  Attacker sends constantly BPDUs (Bridged PDUss: switch management frames) to force root bridge recalculation of the Spanning Tree Protocol (30-45 sec) causing a denial of service.

  Attacker sends BPDUs to become the root bridge and then attacker like a transit switch (sniffing). It is required a dual homed attacker on two different switches.

  Mitigation: disable expect of root guard BPDUs where not necessary.

- VTP

  The attacker acts as a VTP Server sending crafted management frames forcing to delete VLANs (DoS).

  Mitigation: disable VTP or enable authentication mechanisms.

- Other

  ARP spoofing, rogue DHCP, CDP (Cisco Discovery Protocol) attacks.

  Mitigation: monitoring network activity and disabling unneeded services.

As you have seen, Ethernet opens the door to many new kind o f attacks (some still unknown). Some of them would be very unlikely to happen but it is always recommendable to secure configure equipment without trusting the Ethernet switch of the Telco provider and where the datagrams comes from. Remember that the secu re combinations of the configuration will minimize risk (defense-in-depth ever).

There is a useful template for a secure configuration of Catalyst Switches at Qorbit's website [SCE-SG01], and also (of course) a great one for 6500 Series at Cisco's website [SCE-CS01].

L3 – IP Issues

Talking about IP is talking about the history of the Internet because since the beginning of ARPANet (proposed by the Advanced Research Projects Agency), the first 'IP' network, has been the most widely used protocol (TCP/IP Protocol Stack).

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

One of the main reasons why TCP/IP became important was because the Department of Defense (DoS) included them as military standards. And it will became popular when the University of Berkley developed the TCP/IP Unix Stack as a public domain software.

Functionalities

As it was previously told in Ethernet section, is not the purpose of this paper describing the protocols in detail. Moreover TCP/IP is quite well - known and widely explained on SANS Courseware.

The functionalities described here are new protocols that work on IP layer and that are allowing to deploy next generation services (VoIP, videoconferencing, etc).

- QoS

  It means Quality of Service, and it groups packet tagging, algorithms for queuing and congestion avoidance, etc.

- Traffic Engineering/MPLS

  A trendy concept that means flowing the traffic where you want it to flow. It is usually combined with QoS techniques to provide traffic classification (different services).

- VPN

  Virtual Private Networking is a mechanism to supply private communications over public networks.

Threat Mitigation

If you operate with an core IP network, you will enjoy quite a lot two a geek paper that explains very clear security on IP Backbones from Securité.org [IPS-SE01].

- Routing Protocols (Internal/External) Injections

  Attacks on routing protocols consists on injecting false routing updates to manipulate the path of traffic either causing a DoS.

  Mitigation: log changes between neighbour routers, activate passive interfaces where possible, routing filters (only announce/get what is necessary), activate password authentication (where possible)

- DoS/DDoS

  It is aim is to saturate the victim's pipe. It is very difficult to stop and it is going to be the main reason for a NOC staff headache.

  Mitigation: Network Egress/Ingress Filtering (packet filtering) to avoid spoofing. Coordination with uplinks and exchange peers, Rate - limiting, Unicast RPF, black holes (routes to null0)

  For further information visit "*Network Ingress Filtering – Defeating DoS Attacks with IP Source Address Spoofing*" at [IPS-IE01] and "*Denial of Service (DoS) Attack Resources" at* [IPS-GC01].

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

It is not always a matter of prevention, but also detection and applying a solution. Worms and DoS attacks would be more and more regular in daily operation but it is a collaborative work between you and the layered-3 peers. Don't forget Netflow's (at least in Cisco equipment) features on routers, that could allow you to identify strange flow behaviors (often attacks).

There are new and interesting techniques, such as injecting filters to routes (setting next hop to null0) through an iBGP 'trigger router'. That could filter any route in many routers dynamically without administrative burden.

Filters should be applied at edges: CPE, IXP, Uplinks. But will be also useful in cases you are not allowed to do it. Imagine that one day you can't find the person who configures the router on a E&S Site and a attack is eating their pipe!

More information about secure configuration on " *Cisco Routers at NSA Cisco Router Configuration Guides"* [SCE-NS01]

---

6. Conclusion

Most of the comments are done in -line during this paper. As you could have seen, a change of technology not only implies knowing the new security issues but also management issues.

I hope that your vision on RREN environments is now much more clear and you can understand its differences with any commercial ISP network.

Thank you!

---

7. References

Research & Educational Networks – [REN]

[REN-CS01] – CESCA. *"Anella Científica, Catalonian REN"*
URL: http://www.cesca.es/comunicacions/anella.html

[REN-RI01] – RedIRIS. *"Spanish NREN"*
URL: http://www.rediris.es/red/

Ethernet Security - [ETS]

[ETS-HK01] – Kaplan, Hadriel. Noseworthy, Bob. " *Ethernet Evolution 10Mbps to 10,000Mbps"*. 29 September 2000. University of New Hampshire.
URL: http://www.iol.unh.edu/training/ge/ethernet_evolution_index.html

[ETS-NP01] – Pidgeon, Nick " *How Ethernet Works"*, HowStuffWorks
URL: http://computer.howstuffworks.com/ethernet.htm

[ETS-IE01] – LAN/MAN Standars Comitee *"Virtual Bridged Local Area Networks"* IEEE 802.1Q. 8 December 1998
URL: http://standards.ieee.org/getieee802/download/802.1Q_-1998.pdf

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

[ETS-SC01] - Covery, Sean (Cisco). "*Hacking Layer 2: Fun with Ethernet Switches*" BlackHat USA 2002 Conference
URL: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-convery-switches.pdf

[ETS-SD01] – Dugan, Stephen. "*Putting 2 and 2 Together: Designing Security into your Network Infrastructure*" BlackHat USA 2002 Conference
URL: http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-dugan-layer.ppt

[ETS-BG01] – Greear, Ben Greear (Candela Technologies) "*802.1q VLAN Implementation for Linux 1.7*"
URL: http://www.candelatech.com/~greear/vlan.html

[ETS-DT01] Taylor, David "*Are there vulnerabilities in VLAN implementations*" SANS Intrusion Detection FAQ
URL: http://www.sans.org/resources/idfaq/vlan.php

IP Security - [IPS]

[IPS-SE01] - Fisback, Nicolas. Lacoste, Sebastien (Securité.org) "*Protecting your IP Network Infraestructure*," v.1.05. Black Hat Briefing Amsterdan 2001
URL: http://www.securite.org/presentations/secip/BHAMS2001_-SecIP-v105-full.ppt

[IPS-IE01] - Ferguson, P. Senie, D. – "*Network Ingress Filtering – Defeating DoS Attacks with IP Source Address Spoofing*" – IETF RFC2827
URL: http://www.ietf.org/rfc/rfc2827.txt

[IPS-GC01] – Chapman, Brent "*Network (In)Security Through IP Packet Filtering*, GCA"
URL: http://www.greatcircle.com/pkt_filtering.html

[IPS-FS01] Ferguson, P. Senie, D – "*Denial of Service (DoS) Attack Resources*"
URL: http://www.denialinfo.com/

Secure configuration for Equipment – [SCE]

[SCE-SG01] – Gill, Stephen (Qorbit) "*Catalyst Secure Template*" v. 1.21
URL: http://www.qorbit.net/documents/catalyst_-secure-template.pdf

[SCE-CS01] - Cisco Systems. "*Configuring Network Security for Cisco Catalyst 6500 Series*"
URL:http://www.cisco.com/en/US/products/hw/switches/ps708/products_configuration_guide_chapter09186a008007e70d.html

[SCE-NS01] - National Security Agency, "*Cisco Security Recommendation Guides*"
URL: http://nsa1.www.conxion.com/cisco/guides/cis_-securityguides.zip

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ISP Security Resources - [ISR]

[ISR-BG01] Green, Barry (Cisco Systems). *"ISP Security Bootcamp"*. v.2.8
URL: ftp://ftp-eng.cisco.com/cons/isp/security/ISP_Security_Bootcamp/

[ISR-MN01] Merit Network Inc, " *Resources for Network Operators & ISPs"*
URL: http://www.merit.edu/ipma/docs/isp.html

Other - [OTH]

[OTH-AC01] Dodge, Martin. Kitchin, Rob. (Cybergeography Research)
"*An Atlas of Cyberspaces"*
URL: http://www.cybergeography.org/atlas/

[OTH-CT01] CATNIX. "Catalonian Neutral Internet Exchange"
URL: http://www.catnix.net/EN/

© SANS Institute 2003, Author retains full rights.