Global Information Assurance Certification Paper

Network Bridging

Understanding and preventing network bridging between different security zones.

GIAC Security Essentials Certification (GSEC) Practical Assignment (v1.4c)
Option 1 - Research Paper
Jan-Arendt Klingel
May 2, 2005

Table of Contents

1 Abstract

With wireless networks becoming a commodity for many corporations, the risk of accidentally or intentionally bridging networks with different security requirements is rising. Network bridging as described in this paper is the act of connecting different IP networks against security policies and/or the intended network design.

There are more scenarios in which unwanted network bridging can occur; following are three examples: (a) an employee working from home with access to the local and corporate network at the same time, (b) an employee working from home bridging the Internet and the corporate network, (c) a supplier connected to the corporate and supplier network at the same time.

The perimeter of networks is changing and so are the vectors a possible security threat can use. This paper explains how network bridging can occur, the risk associated with network bridging, and the measures one can take to prevent this from happening.

Examples in this paper were taken from and solutions were developed for a large manufacturing company; nonetheless, many if not all topics will apply to other companies with diverse computer networks as well.

2 Analysis

2.1 The New Network Perimeter

A common network and security architecture for corporate networks is following the concept of a strong perimeter. Firewalls and intrusion detection/protection devices protect the corporate network against cyber attacks from the outside. The corporate network very often has a flat structure consisting of one trusted zone. Data exchange with business partners is secured by using a demilitarized zone (DMZ) through which all traffic between the outside and the inside has to flow.

A good analogy for this architecture is a medieval castle. The corporate network is the castle that has high and thick surrounding walls to protect against attacks from the outside. One big but very well guarded gate is the only means of entering and leaving the castle.

New business needs make it necessary to create backdoors into the wall of the castle. The way corporations are working together with business partners is changing. A DMZ is not enough anymore to keep up with the data exchange requirements for the corporations and their partners. In the manufacturing environment, corporate employees and engineering partners are working very closely together on common projects. Suppliers are now sitting inside the castle, using the same IT infrastructure as the corporate employee. Employees work from home and extend the corporate network to their residence. Managers use the insecure Internet to connect from a hotel room back to the headquarters.

Eric Litt, CISO of General Motors, describes the situation this way:

> *"We have 325,000 employees, but we also have a huge number of partners and suppliers who need access to our network. We share our intellectual property with them. It's a necessity for us to do business."* [CISO]

Introducing backdoors into the network, based on today's business needs, creates new vectors for cyber threats. The new perimeter is pushing IT security inside the corporate network and towards the client.

The new perimeter, elevated risk that comes with introducing backdoors into the network, and endpoint security have been documented. In a recent Cisco Systems, Inc. user magazine article the new perimeter is highlighted but addressed only from a tools perspective:

> *"The perimeter has been extended and distributed, so security must be*

> *applied at each of these new ingress and egress points to avoid damaging threats, thus complicating security architectures."* [LOOM]

Based on the need for a new architecture for corporate networks, this research paper looks at how different network zones are possibly bridged in real-world environments. Bridging network zones against intended design can raise the threat level for enterprises to an unacceptable mark.

2.2 Scenarios of Network Bridging and the Associated Risk

The following subchapters expose different scenarios in which network bridging occurs. Not only will this result in a new hole in the network perimeter, there is also certain risk involved with bridging networks:

- Security requirements cannot be satisfied anymore
- Security policies may not be effective anymore
- New vectors for cyber threats are created
- Intellectual property and classified information is not protected to the same extent anymore

Especially the wireless LAN (WLAN) technology increased the risk of bridging networks lately. Modern notebooks and even PDA devices are equipped with WLAN radios to communicate with WLAN access points which follow the IEEE 802.11 standard. Often the WLAN technology comes pre-equipped[1] and is enabled by default. New measures have to be taken to make wireless networks secure.

Throughout the document the following vendor-independent IT symbols were used to visually describe different network scenarios:

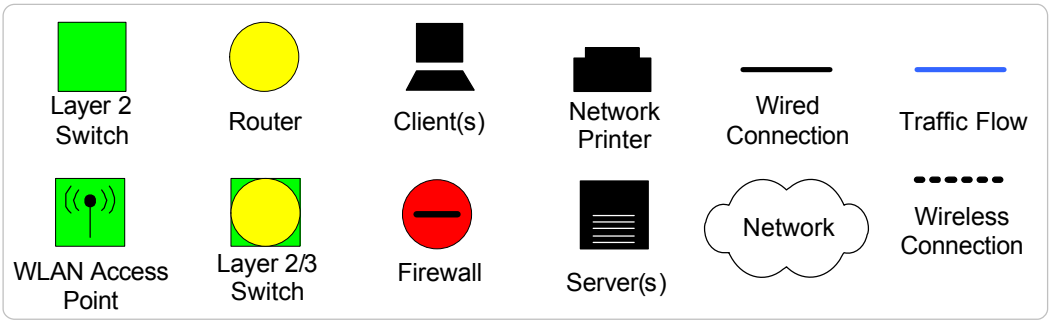


Figure 1: Legend of IT symbols

[1] An example for this can be found in Intel's PRO/Wireless Network Connection for mobile technology, see http://www.intel.com/network/connectivity/products/wireless/prowireless_mobile.htm

2.2.1 Wireless Hotspots

Wireless hotspots are convenient for the mobile workforce when on the road. They allow people access (often inexpensive) to corporate IT services when a direct connection is not available. The hotspot can become a problem when the WLAN signals leak into the corporate network and vice versa.

This is usually not a problem for the typical hotspots in airports and hotels, but may become an issue when more and more cities are installing wireless networks for the community. Cities like Culver City, CA already offer free Internet services over standard WLAN technology [CULV]. The WLAN signal in this case covers the whole downtown business district.
A similar scenario is given with the coffee shop on the first floor of a multi-tenant building that might add a wireless LAN to its service (see chapter 2.2.2).

From the perspective of the corporation, the public hotspots and their potentially missing security standards cannot be controlled. The goal is rather to protect the corporate network and internal assets itself.

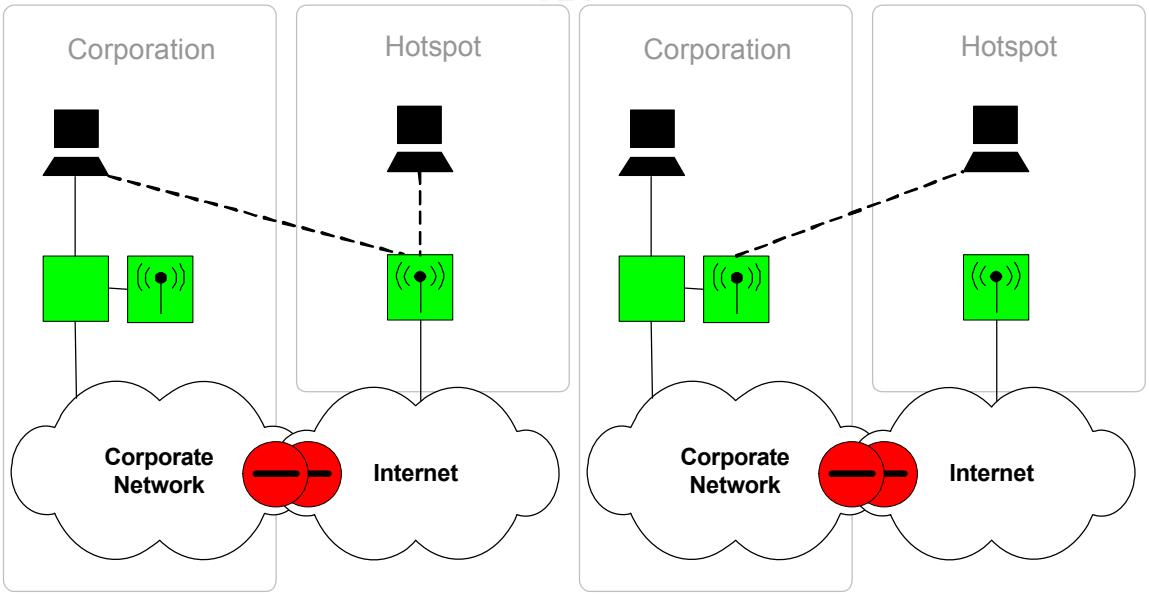


Figure 2: Wireless hotspots

Above figure shows a corporate client that picked up a signal from a hotspot (scenario A). Depending on the WLAN access point and client settings, the client may automatically try to associate with the access point. War driving showed that many, many wireless networks are either wide open or maintain

just the minimum security settings. An example of a wide-open hotspot can be seen in the next figure. Although the signal quality from this hotspot is poor, the connection still can be used to connect to the Internet.

Figure 3: Open hotspot

In this example even the default SSID of “linksys” had not been changed.

Figure 2: Wireless hotspots, scenario B, shows how network bridging can work in both directions. Here a hotspot user picked up a WLAN signal from the corporate network. There could be trivial situations in which the hotspot user is successful in bridging the networks: a) The user picked up a signal from a rough WLAN access point which does not have the necessary security settings, or b) The user picked up a signal from an open WLAN access point that is outside of the strict control of the central IT department, e.g. at a small, remote location.

2.2.2 Other Wireless Bridging Examples

It does not require a public hotspot to bridge WLAN networks. Wireless signals also leak through the walls in multi-tenant buildings. A client from corporation A could pick up a WLAN signal from corporation B, as shown in *Figure 4: Wireless bridging - multi-tenant building*.

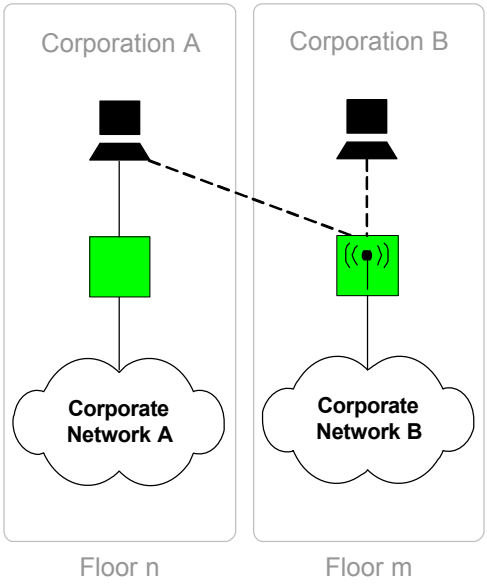


Figure 4: Wireless bridging - multi-tenant building

Although the location, orientation, and type of antenna do influence the spreading WLAN signal, it is difficult to completely block the signal outside of a certain radius without modifications to the building or room structure. WLAN signals do not follow floorplans!

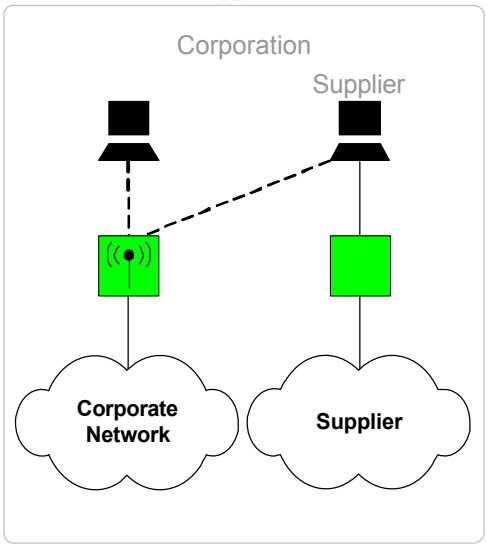


Figure 5: Wireless bridging – supplier

The above figure is one more example for WLAN bridging outside the hotspot environment. A supplier or partner connects its computer to the corporate wireless network and bridges the supplier/partner network with the corporate network. The following chapter explains this scenario in more detail.

2.2.3 Wired Bridging

Figure 6: Wired bridging, scenario A, shows an example in which a supplier is working on its own IT infrastructure but on the premise of the corporation. In today's business world there are many situations in which such a constellation makes sense, e.g. if facility management is outsourced and done by an on-site company. Also, engineering environments are often confronted with this situation as engineering partners are tied into internal processes and work shoulder to shoulder with employees of the corporation, especially in CAD/CAE. CAD/CAE workstations may come with two network ports standard, raising the risk for wired bridging with two simple patch cables.

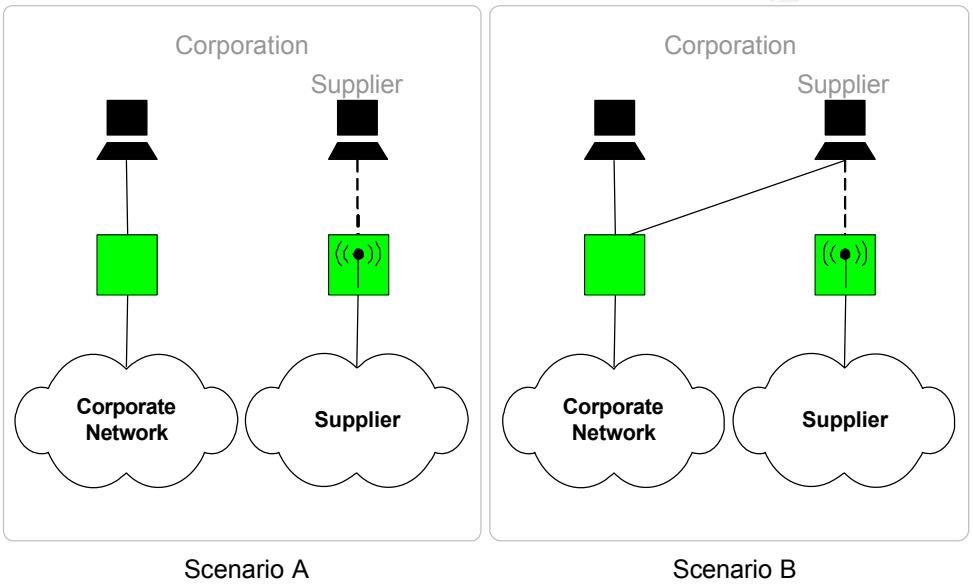


Figure 6: Wired bridging

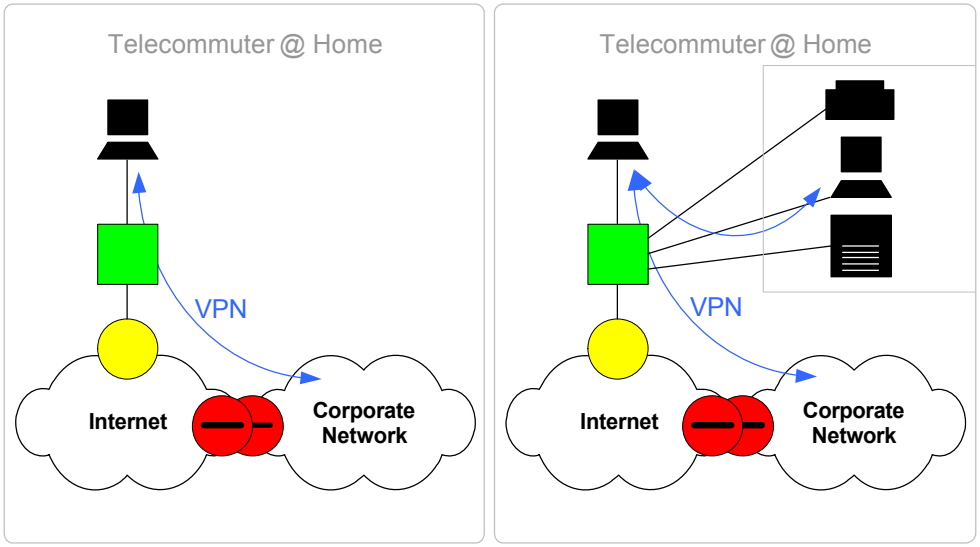
Depending on physical separation and security between employees of the corporation and the supplier, it may be possible for a supplier to plug a patch cable (inadvertently) into the wrong switch port or jack. This is shown in scenario B.

Clearly the risk of this scenario is that – with the common use of DHCP to supply IP addresses – the supplier will get an IP address, a default gateway, and maybe even more configuration settings from the corporate network. This will enable the supplier to connect to the corporate network and therefore bridge the two different networks. A new vector for malware is borne!

2.2.4 Local LAN Access

In the following example a telecommuter is using an Internet connection to connect back to the corporate network. A VPN and a client-initiated tunnel allow the telecommuter to securely access IT services in the corporate network. Typical network protocols for creating a VPN are IPSec, PPTP, and L2TP. See

e.g. [BUIL] for more details on how these VPN connections work.



Scenario A Scenario B

Figure 7: Local LAN access

Scenario A depicts the originally designed solution. An IT department controls this environment and security policies may regulate the usage of it.
In scenario B the telecommuter connects his or her private LAN to the switch and bridges the two networks[2]. Now malware from the private LAN has a vector for reaching the corporate network. As the private LAN is not under the control of the company's IT department, the telecommuter could easily violate security policies, intentionally or unintentionally.

Another concern for the company could be that the telecommuter is now able to take intellectual property or classified information – assuming that this person has access privileges - out of the corporate network. Even by accident such data could find its way into the Internet, for example if the private LAN is connected to the Internet and another family member attaches the data to an outgoing email message.

2.2.5 Split Tunneling

Modifying the example from chapter 2.2.4, the telecommuter could not only have a VPN connection back into the corporate network, but also have a route into the Internet. This scenario is commonly described as "split tunneling".

[2] In a Cisco environment, "Allow Local LAN Access" has to be set on both the ACU client and the VPN concentrator.

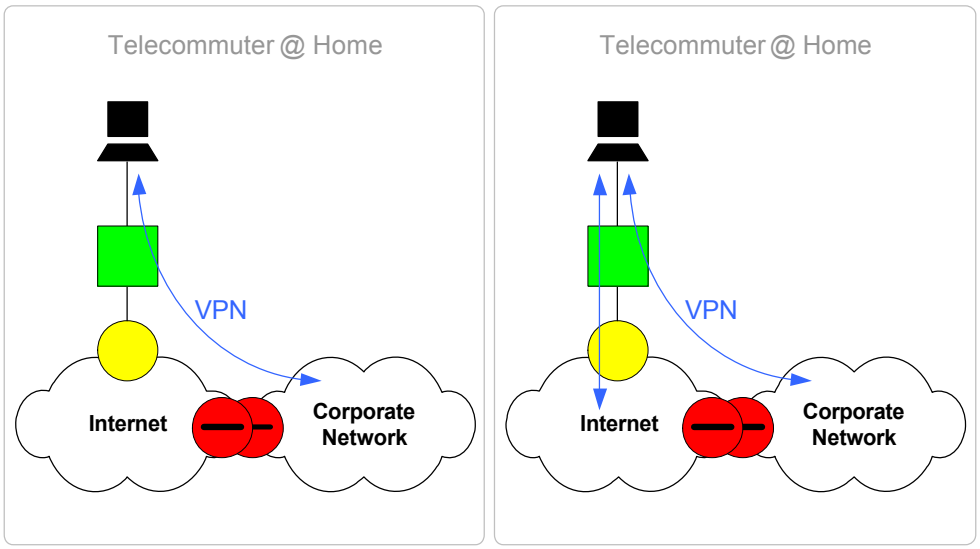


Figure 8: Split tunneling

Normally the Windows VPN client changes the metric for routes to the Internet and the local network to the highest value of 9999. This way only routes to the VPN gateway and the corporate network will be chosen. Following is part of a routing table from a client with the VPN connection established:

Active Routes:

Network Destination	Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.0.0.1	10.0.0.1	1
0.0.0.0	0.0.0.0	192.168.1.1	192.168.1.103	9999

Default Gateway: 10.0.0.1

In this example the default route to the local gateway 192.168.1.1 was replaced with the default route to the VPN gateway 10.0.0.1.

Despite the normal configuration, split tunneling can be enabled on the VPN client allowing the user to connect both to the corporate network and the Internet at the same time. This is shown in scenario B.

Microsoft describes the security problem associated with split tunneling in [SPLI]:

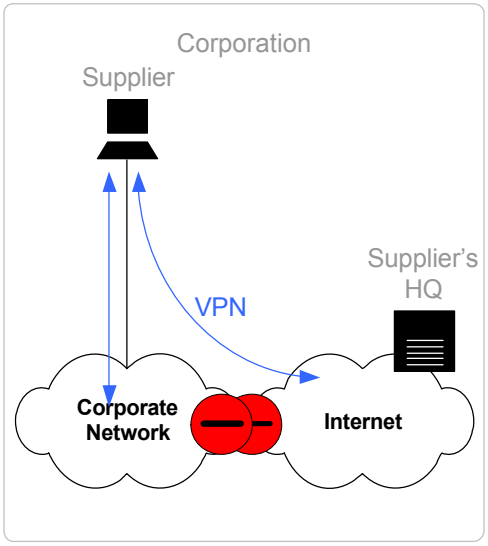
> *"When a VPN client computer is connected to both the Internet and a private intranet and has routes that allow reachability to both networks, the possibility exists that a malicious Internet user might use the connected VPN client computer to reach the private intranet through the authenticated VPN connection. This is possible if the VPN client computer has IP routing enabled. IP routing is enabled on Windows XP-based computers by setting the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\Tcpip \Parameters\IPEnableRouter registry entry to 1 (data type is*

REG_DWORD).”

Another aspect of split tunneling is that the telecommuter in this example may bypass security policies by accessing the Internet directly. Most companies have an interest in applying access control, content control, and maybe even accounting to the Internet connection that is provided.

Although split tunneling can offload Internet traffic from the corporate network, the technique will poke a hole through the perimeter security.

The example in this subchapter can be used to illustrate another possible security threat: A supplier who is working on the premise may need a VPN connection back to the supplier’s headquarters:



Scenario C

Figure 9: Split tunneling - supplier

Here the two networks are bridged and even without routing enabled on the supplier’s computer, data could travel from one network to the other.

Split tunneling can also occur together with public hotspots, e.g. at the airport or at a hotel. The computer user can have a connection into the Internet to check the flight status and at the same time a connection into the corporate network, secured by a VPN.

The lesson to learn about a VPN is that is does not validate the traffic inside the tunnel. Viruses or worms can also travel through a tunnel, next to legitimate traffic.

3 Mitigation Techniques

3.1 Network Segmentation

Architects realized that the concept of one trusted zone for the corporate network has to be extended. Different zones have different security requirements; rules and policies determine the allowed traffic flow between zones.

There are different ways to look at network segmentation. One is to separate logical business units and install control units between these zones. In a manufacturing environment the body shop, the paint shop, and assembly could be three different network zones with different security requirements. Rule sets on the control units would determine which source can communicate with which destination. A control unit could be a stand-alone firewall, a firewall blade in the switch, or a simple ACL on a router.
All of the examples in chapter 2.2 show how networks are bridged in the client access layer[3] of the network where control and security is typically less than in other layers. From a design perspective it makes sense to install the control units where the first layer 3 network devices are, usually the distribution layer:

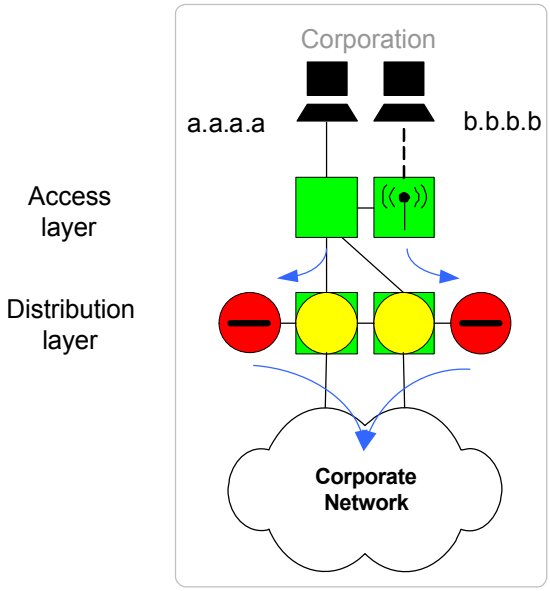


Figure 10: Network segmentation - control units

Controlling mainly the “inbound” traffic from areas where network bridging usually occurs prevents part of the bridging problem. *Figure 10: Network segmentation - control units* shows how the distribution layer will only allow network traffic from IP network a.a.a.a and b.b.b.b into the corporate network.

[3] Using i.e. Cisco’s hierarchical campus design, http://www.cisco.com/application/pdf/en/us/guest/netsol/ns24/c643/cdccont_0900aecd800d8129.pdf

A network zone for the purpose of this document is a well confined area in the access layer of the corporate network. This could be the sum of internal clients connected to the network in a given building. Another zone could be the supplier or partner from chapter 2.2.2 working in the same building but with different security requirements. The public hotspot from chapter 2.2.1 would be an outside zone in which security requirements cannot be defined.

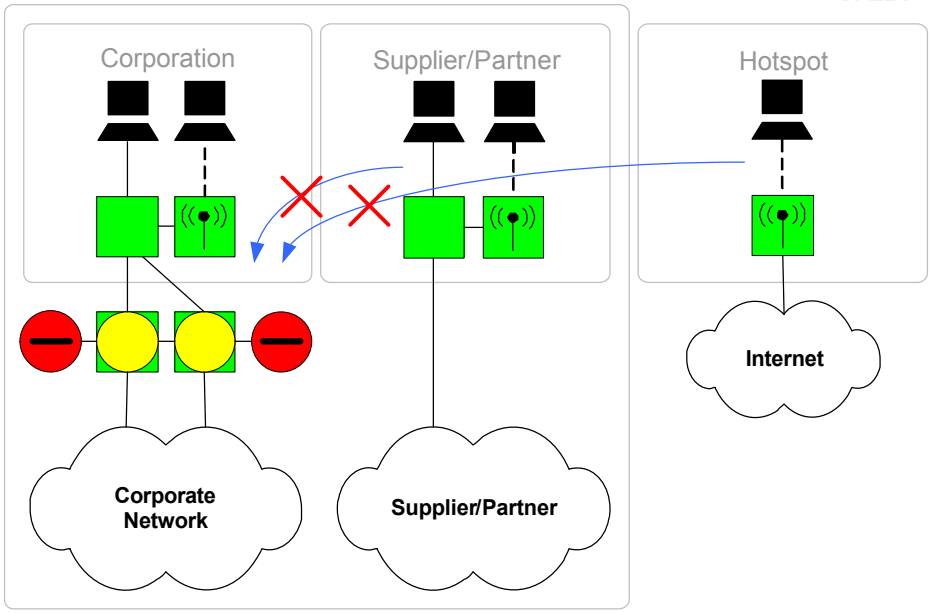


Figure 11: Network segmentation - inbound rule base

In the above figure a “corporation zone” is next to a “supplier/partner” and a “hotspot” zone. Inbound rules on the control units of the “corporation zone” do not allow traffic from the two latter zones to reach the corporate network. In the event that network bridging occurs, it would only allow a single client from a different zone to be bridged - but not the networks they are attached to.
So even if the supplier has configured the client as a router, traffic from the NIC to which the “supplier zone” is connected could not pass the distribution layer of the “corporation zone”.

Unfortunately this does not protect a client from the “corporate zone” from bridging into another zone. On Windows clients the following registry settings can be configured to contain the problem:

1) IPEnableRouter=0x0 - Disable IP forwarding
2) DisableBridging=0x1, DisableSTP=0x1 - Don’t allow a “network bridge” on a client

Creating hardware profiles could be a solution, too. As long as the client is connected to the corporate network the hardware profile in use would not include the wireless NIC.

3.2 Port Security

Normal network behavior on switch and hub ports is that access control does not take place. As soon as a client is plugged into an enabled network port the link is up and an IP connection gets established. Port security defines an access control method for these network ports.

The National Security Agency created an unclassified document in 2004 that summarizes the different methods of applying port security to Cisco switches, see [CISC]. The document explains the vulnerabilities for certain switch features and shows appropriate countermeasures.

By controlling access to network ports, unwanted network bridging can be prevented, both on wired and wireless networks. Two examples for network port security are described:

3.2.1 MAC-level security

Switches are able to allow access to a network based on a given or learned MAC address. Either the administrator tells the switch which MAC address to expect on a certain port or the switch is configured to dynamically learn secure MAC addresses. If the number of secure MAC addresses is reduced to one, then only one client per port can connect to the network. Dynamically learning secure MAC addresses is called “sticky MAC” by Cisco. The configuration steps for both types of MAC security are explained in [POR3]. Other switch vendors have similar features, but the functionality is always the same: Allow access to a network based on MAC addresses.

How does this help with network bridging? Network bridging from a zone with lower security requirements into one with higher security requirements will not occur if network ports in the latter network are protected by MAC-level security. That being said, a supplier from *Figure 6: Wired bridging* could not bridge into the corporate network if certain MAC addresses are preconfigured.

Although MAC-level security installs a safeguard against unauthorized access and network bridging, it does not fully prevent attacks against switches. MAC addresses can be sniffed or retrieved through social engineering and switches may be overwhelmed with frames in a way that the switch will forward all traffic, ignoring secure MAC addresses and VLAN definitions.

3.2.2 Port security using IEEE 802.1X

802.1X is a standard both by the IEEE and ANSI that adds access control to 802-based networks like an Ethernet network (see [POR2]). The standard can be used for both wired and wireless networks to secure unauthorized access to network ports.

Three parts make for an 802.1X network: A client that wants to connect to the network (the “supplicant”), a network device like a router, switch or WLAN access point (the “authenticator”) that controls link-layer access and forwards authentication requests to an authentication server (the “authentication server”). Although the 802.1X standard does not specify the communication between the authenticator and authentication server, the latter is typically a RADIUS server like Cisco’s ACS server[4]. Authentication requests are transported via the Extensible Authentication Protocol (EAP) between authenticator and authentication server. A special version of EAP, EAP encapsulation over LAN (EAPOL), got defined to carry authentication requests between the supplicant and the authenticator in Ethernet, 802.11, or Token Ring frames.

The principal idea behind 802.1X is that the network port of an authenticator does not allow IP traffic but only authentication requests through if a client wants to connect. These authentication requests are initiated by the supplicant. The authenticator then forwards the request to an authentication server which validates the request. Depending on the credentials of the user the authentication server sends a positive or negative message back to the authenticator. In case of a positive message the authenticator would enable the port for normal use. In case of a negative message the port will be closed.

The following figure shows a simplified protocol diagram of a supplicant trying to connect to the network after receiving an “EAP Request/Identity” message. As soon as the supplicant receives the positive acknowledgement from the authenticator it is part of the network and can receive/send normal IP traffic.

[4] See product description at http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html

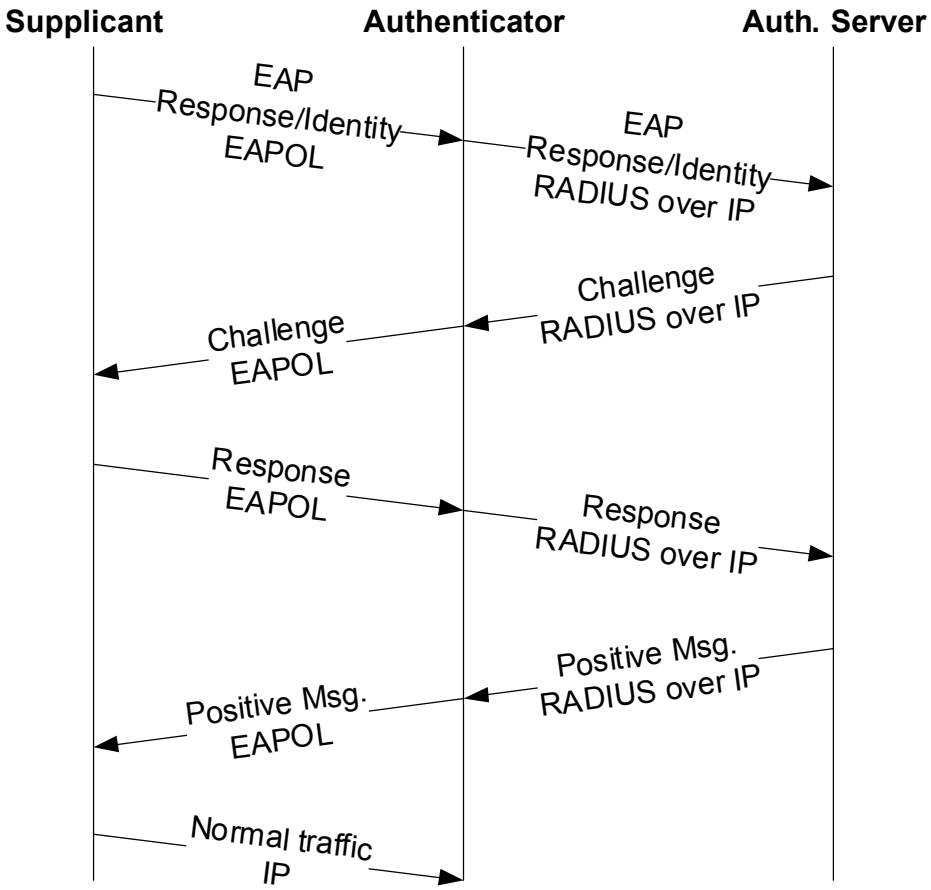


Figure 12: 802.1X protocol

Some vendors also implemented a “guest VLAN” which can be assigned to clients that don’t have the necessary supplicant installed.

Similar to the previous chapter, port security using 802.1X controls which clients are allowed to the network and which clients have no or limited access. If clients cannot easily connect to network devices in neighboring zones which are protected by 802.1X, network bridging can be prevented.

3.3 Securing Mobile Users and Telecommuters

Mobile users and telecommuters can be protected with measures that are outlined in the following list.

- Don’t allow clients to become a router or bridge (see chapter 3.1 on how to do this)
- Make the WLAN access points of telecommuters secure: don’t advertise the SSID, don’t rely on static WEP for data encryption, and use EAP-based authentication with port security
- Secure the network ports of telecommuter’s equipment. Most network

devices like DSL routers are coming with more than the necessary ports on their embedded switches. Apply safeguards outlined in chapter 3.2 or simply shut down the ports that are not needed
- Don't allow clients of telecommuters access to the local LAN. If access to network printers or scanners is necessary, consider the use of Bluetooth bridges
- Don't allow the use of split tunnels. Rather, route Internet traffic through the corporate proxy and firewall where controls can be applied. Make sure that the default route in the routing table points towards the VPN gateway as the next hop
- Make the use of VPN tunnels mandatory for the mobile workforce connecting to the corporate network via the Internet
- Don't allow clients to connect to networks other than the company's IP address range
- Don't allow clients to connect to WLAN access points other than the ones provided by the company
- Let the mobile workforce connect back to the corporate network via dial-in service providers that offer secure, private line-like networks. One example for a service like this is MCI's Corporate Remote Access[5], another one is Sprint's Remote Access Solution[6].

Sometimes a combination of these measures is necessary to completely protect the corporation.

[5] See http://global.mci.com/us/enterprise/data/remoteaccess/
[6] See http://www.sprint.com/business/products/products/remoteAccessSolution_enterprise_tabC.jsp

4 Conclusion

The awareness for network bridging issues is slowly rising. At the moment the author is not aware of a second public research paper that addresses this issue isolated from other IT topics. With the changing network perimeter, companies have to think about new strategies, architectures, and solutions to fight the newly created threat vectors.

IT architectures that only look at the classic core-distribution-access layers are not able to cope with the new network perimeter. Even the “Enterprise Composite Network Model” from Cisco does not reflect recent changes in the perimeter.

A possible future holds network zones that communicate with each other on well-defined paths. Security will be an essential part of every member in each zone, down to the single client. Policies define who is allowed to communicate with whom and how. Bridging zones is only possible by design at security gateways that link zones with each other.

For now, network bridging can be prevented by following the solutions that are outlined in this document. Even if not all possible scenarios of network bridging are listed, it should give a good, comprehensive overview of the topic.

5 References

[BUIL] Kosiur, Dave. Building and Managing Virtual Private Networks. John Wiley & Sons. Hoboken: October 15, 1998. ISBN 0-4712-9526-4

[CISC] A. Borza et.al. Cisco IOS Switch Security Configuration Guide. Fort Meade: June 21, 2004. National Security Agency. Report I33-010R-2004 <http://www.nsa.gov/snac/os/switch-guide-version1_01.pdf>

[CISO] "CISO keeps his eyes on the road". eWeek. January 3, 2005: 28+

[CULV] Culver City. Los Angeles: 2005. Wireless Hotspot, Inc. <http://www.wirelesshotspot.com/culvercity.php>

[LOOM] Barry, David. "Looming Security Challenges". PACKET. Q1 2005. Cisco Systems. ISSN 1535-525-2542: 19+

[POR2] Meador, William J. "Port-based authentication with IEEE Standard 802.1x". July 8, 2004. Information Security Writers <http://www.infosecwriters.com/text_resources/pdf/8021x.pdf>

[POR3] Configuring Port Security. Cisco Systems. Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide, 12.2(20)EWA <http://www.cisco.com/en/US/products/hw/switches/ps4324/products_configuration_guide_chapter09186a00802c30af.html>

[SERV] Server and Domain Isolation Using IPSec and Group Policy. March 17, 2005. Microsoft <http://www.microsoft.com/technet/security/topics/architectureanddesign/ipsec/default.mspx>

[SPLI] Split Tunneling for Concurrent Access to the Internet and an Intranet. October 2003. Microsoft <http://www.microsoft.com/technet/community/columns/cableguy/cg1003.mspx>

6 Abbreviations

ACL	Access Control List
ANSI	American National Standards Institute
CAD	Computer Aided Design
CAE	Computer Aided Engineering
CISO	Chief Information Security Officer
DMZ	Demilitarized Zone
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EAPOL	EAP encapsulation over LAN
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPsec	Internet Protocol secure
IT	Information Technology
GSEC	GIAC Security Essentials Certification
LAN	Local Area Network
L2TP	Layer 2 Tunneling Protocol
MAC	Media Access Control
NAC	Network Admission Control
NIC	Network Interface Card
PDA	Personal Digital Assistant
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication of Dial-In User Services
SSID	Service Set Identifier
VLAN	Virtual LAN
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WLAN	Wireless LAN

7 Table of Figures