

1052 New Holland Ave  
Lancaster, PA 17601  
717-898-9654  
[www.whitewolfsecurity.com](http://www.whitewolfsecurity.com)

## **Application of OCOKA to Cyberterrain**

*By Dwight Hobbs, Lead Instructor*

## **Contents**

---

<b>Introduction</b>	<b>1</b>
<b>Background</b>	<b>1</b>
<b>Observation and Fields of Fire</b>	<b>2</b>
<b>Cover and Concealment</b>	<b>3</b>
<b>Obstacles</b>	<b>4</b>
<b>Key Terrain</b>	<b>4</b>
<b>Avenues of Approach</b>	<b>5</b>
<b>Real World Application</b>	<b>5</b>
<b>Conclusion</b>	<b>10</b>

## **Introduction**

*OCOKA and Cyberspace*

## **Background**

*Evolution of cyberspace as a terrain*

## **Observation and Fields of Fire**

*Ability to see and acquire targets and effectively engage*

## **Cover and Concealment**

*Protection from countermeasures and detection*

## **Obstacles**

*Features of a network landscape*

## **Key Terrain**

*Network features to provide key tactical advantage*

## **Avenues of Approach**

*Possible paths to reach our target*

## **Real World Application**

## **Conclusion**

# Introduction

When discussing cyberspace, and especially military operations within cyberspace, planners tend to balk at the use of standard tactics in, what is considered, the novel arena of the digital world. Papers have been written discussing the similarities of cyberspace to physical space, and the modeling of cyberterrain as merely another terrain alongside air, land and sea <sup>1</sup>. This paper will attempt to show how classic methodologies, specifically the tactical planning tool OCOKA, can be used identically to assess cyberterrain for both offensive and defensive operations.

## Background

The idea of cyberspace, and the digital world as a whole, being completely novel and separate from the physical world is one that was propagated by early adopters of digital technology as a means of illustrating that new technologies create new and different dilemmas. Ubiquity of technology, especially the widespread use of cell phones, laptop computers, and broadband access in developed countries, has helped to push back the idea of the digital world as something wholly foreign. The widespread use of these technologies by average citizens has begun to push the idea of cyber-physical convergence, the recognition that all actions within cyberspace have a tangible, physical counterpart in real space (e.g. physical cabling between points on a network, bits stored on a hard drive, pulses traveling down a fiber optic cable).

Networks are a natural method of assessing the human need of efficiently transporting information (goods, services, people, data) from place to place. Each iteration of network technology updates the network model with the most current advances to increase the capacity or speed of transporting goods. Even within the brief history of the United States, we have updated our network model several times to keep up with technology and the demand for greater information flow.

We use networks to transport everything we need for our everyday life, the terminology and science of it is all around us. The road system, railroads, the Interstate highway system, electricity lines, water pipes, phone lines, fiber optic cables. Each iteration of the network model was created with the help of the engineers from the previous model, and because of this each model bears similarity to the other models, which is where we can begin to merge them.

These systems use the same terminology and are built off the same scientific model. The time it takes for your package, or message, to reach its destination (whether you're talking about a shipment on a railroad car, a letter traveling via Pony Express, or an email) is latency. You reduce latency by creating faster networks, which is done by creating a faster medium, creating a faster route, or creating more throughput on your current medium.

Creating a faster network means updating your technology. Airplanes are faster than trains, which are faster than horses. Creating a faster route means finding, or creating, a different path between endpoints.

---

<sup>1</sup> Offensive Operations in Cyberspace, White Wolf Security, [http://www.whitewolfsecurity.com/offensive\\_ops.asp](http://www.whitewolfsecurity.com/offensive_ops.asp)

Creating a transcontinental railroad was done to bypass long shipping routes around South America to deliver goods from the east coast of the United States to the west coast. Creating more throughput means allowing more of your current network traffic to occur at the same time. Expanding a two lane highway to a four lane highway is an example of increasing throughput. When telecom companies ran long haul fiber lines across the continental US, they were doing all three things to create a faster network.

These are all examples of scale-free networks (networks with no maximum or set number of nodes). Network theory says that scale-free networks come together in high importance places known as hubs. Crossroads, intersections, railroad crossings, airports, or network routers. Points on the network that allow for the passage of large amounts of information, and which are crucial to the survival of the network.

When assessing a digital network, either for attack or defense, it's important to understand the basics of the overall network and be aware that there is nothing more mystical about a digital network than about a physical one.

## Observation and Fields of Fire

Observation is our ability to see an area and acquire targets. Whether we can see our target or not is important, but better translates to "Can we directly access our target?" Digital observation involves trust models, and is most readily affected by firewalls. Digital networks are generally segmented into "inside", or trusted, hosts and "outside", or untrusted, hosts. Hosts behind the firewall are effectively invisible to us (as something obscured by a hill or other terrain), and to attack it we would have to move our position (e.g. gain a foothold inside the network first) or move our attack upstream and attack the firewall or router (disrupting at our intersection, instead).

Fields of fire refers to our weapons' effectiveness in a given terrain. Classic OCOKA defines two types of weapons: direct fire and indirect fire. Direct fire refers to weapons that require line of sight to be effective against a target, as opposed to indirect fire which does not.

Examples of direct attacks: Software exploits (0-day bugs), password guessing, account bruteforcing, exploiting incorrect or insecure software configurations, targeted viruses or worms, rootkits

Examples of indirect attacks: Denial of Service (DoS), Distributed Denial of Service (DDoS), Distributed Reflective Denial of Service (DRDoS)

There are also some digital attacks that, while having similar physical analogues, are slightly more widespread digitally, so I'll mention them here. Both of the following attack types are types of indirect attacks. User-initiated attacks are those that cannot occur without direct user interaction. An internal user of the system must physically do something to create the attack. Proximity-only attacks are those where the attacker must be in physical proximity (which will vary depending on the attack) to effect the attack.

Examples of user-initiated attacks: Cross Site Scripting (XSS), Cross Site Request Forgery (CSRF), Malware, Spyware, Phishing, Spear-phishing

Examples of proximity-only attacks: Wireless attacks (802.11), Bluetooth attacks, RFID attacks

# Cover and Concealment

Cover refers to protection from weapons. When attacking a sufficiently advanced network there are a number of network technologies that can be expected with a high probability. Due to the adaptable nature of software some attacks can be used to provide cover while attacking. All network defense technologies were modeled after physical weapons systems.

## Perimeter walls and sentries - Firewalls

Firewalls will actively deny traffic based on a set of rules. To effectively bypass a firewall the attack must either match those rules, or the attack must be initiated from the within the firewall (to subvert the trust model).

## Tripwires and motion sensors - Intrusion Detection Systems (IDS)

IDS systems will analyze traffic looking for known attack signatures and generate alerts if attacks are detected. To effectively bypass an IDS the attack must look benign (not match a rule) or blend in with other attacks to get lost in the noise. IDS systems are fairly notorious for false positives and high volumes of alerts.

## Sentry guns (or any active automated defense system) - Intrusion Prevention System (IPS)

IPS systems will analyze traffic looking for known attack signatures and generate alerts, as well as terminating the connection to prevent an attack from succeeding. The effective methods for bypassing an IPS are the same as those for bypassing an IDS system.

Attacks against digital networks should take these systems into account, and consider methods and strategies for bypassing them. Observation before a mission can also be used to determine which, if any, of these systems are in place.

Concealment refers to protection from observation. Concealment involves avoiding detection by both host-based and network-based detection and is most directly affected by rootkit and anti-forensic technologies. The types of concealment that are usable depends on the type of systems that are being attacked, either the ultimate target or the targets that need to be compromised to reach the ultimate target.

Rootkits are the most important concealment technology. Rootkits are used to intercept signals between user programs and the underlying architecture that processes requests for those programs. Sufficiently sophisticated rootkits can operate out of sight, waiting for a signal from the owner or a certain time, even when the system is known to be compromised and is actively being scanned. Other characteristics about a target system may also make it more vulnerable to certain types of rootkits. High availability servers (those managing critical infrastructure that are meant to be running at all times) are unique targets of memory resident rootkits. Memory resident rootkits exist only in RAM, which can make them difficult to forensically analyze, and all traces of the rootkit will be destroyed if the system is powered down.

Anti-forensic technology is used to attack known methods of forensic investigation. When dealing with cyber-operations concealment after the fact can be equally as, or more, important than concealment

during the attack. Often, an attack will cause system degradation, which will be noticeable to operators and administrators, but still achieve the desired effect. In these cases, it might be more important that investigators cannot identify the attackers, or cannot conclusively identify the extent of the damage to the system.

The primary purpose of anti-forensic technology is to undermine specific investigative techniques, which would be useful if an attacker were certain that a compromised system would be investigated. Another function of anti-forensic technology is introducing plausible deniability to digital logs. The technology can be used to corrupt digital logs, often assumed to be infallible, in specific ways to completely remove evidence of the attackers or, similarly, to point to specific uninvolved parties as the attackers.

## Obstacles

Speaking of digital terrain, obstacles will be any network feature that we must traverse to reach our target. For the purposes of tactical planning, we are concerned with the obstacles closest to our target. Obstacles may also be present within our own network, or in an upstream provider of our ultimate target, but they will not be discussed here.

Obstacles include all network devices that process traffic and make decisions (either routing or policy-based) based on the traffic. Due to current industry trends at consolidation of networking devices, this is quickly becoming all network devices. Obstacles also include the bandwidth between two points on our path to the target, which may limit the effectiveness of our attacks, or our access to the target.

Examples of obstacles: Routers, switches, Firewalls, IDS, IPS, Bandwidth

## Key Terrain

Digital key terrain refers to any network feature that, if controlled, will provide a tactical advantage. This will change based on the layout of the target, and the target's network, but there will always be a few features that constitute key terrain.

Last-hop routers. This could also be the default gateway. Most networks are configured such that a single powerful routing device will route connections into, and out of, the network, creating a bottleneck. Controlling this device will provide access to all incoming and outgoing communications to the target network. This will be ineffective if encryption is being used, but controlling this point would also allow you to change where traffic is being sent, opening the possibility of hijacking network traffic.

Domain Controllers (or other identify verification systems). In Windows domain environments the system responsible for user authentication and access control is often set up as the domain controller. In non-Windows environments similar technologies are often used (e.g. Kerberos, LDAP). Controlling these systems will allow you to deny access to legitimate users, as well as potentially creating your own new accounts which have unrestricted access to the network.

Internal hosts. If the target is behind a firewall, and therefore unreachable from external requests, any internal host could be considered key terrain. Controlling internal hosts would make direct attacks viable, instead of relying solely on indirect attacks.

## Avenues of Approach

Digital avenues of approach represent the possible paths for reaching the ultimate target. AoAs could be any number of things which, like the physical world, will vary widely based on terrain, fortifications and nature of the target. AoAs will range from simple remote attacks over the digital network to complex multi-domain attacks involving social engineering and physical possession of the target.

Example AoAs:

- Digital attack over the Internet.
- Phishing attack emailed to users with known elevated privileges.
- “Demo” CDROMS mailed to users with malicious software loaded.
- Rootkit infected USB drives planted in a common area.
- Physical seizure of a computer system or network device.

## Real World Application

Applying OCOKA to cyberterrain is ideally done with a logical network map and a physical network topology map. Complete, accurate maps are not always available. Freely available tools can be used to map the logical network structure well enough to plan an operation. Physical topology maps will likely be guesses, without insider assistance or social engineering of knowledgeable insiders. For ease of understanding maps have been provided for the example scenarios. The following scenarios are all from an offensive viewpoint. For the purposes of these scenarios physical compromise of the building or of the network devices (via actually entering the premises and physically seizing control) will be avoided to keep the scenarios concise and focus on the cyberterrain model, although these options would certainly be available in a real world situation.

### *Scenario 1*

A mail server housing the email of several key executives contains valuable information. The affected executives cannot know that the mail server has been compromised, as this could affect the validity of the information gathered. Figure 6-1 and 6-2 show the logical and physical network diagrams.

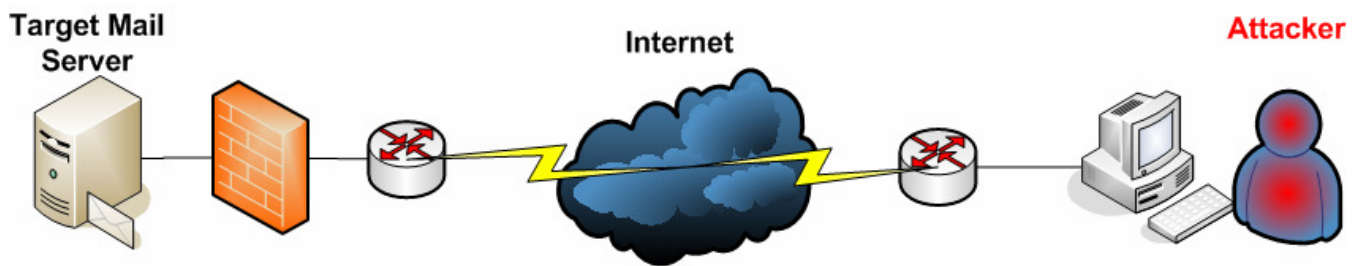


Figure 6-1 – Logical Network Diagram (Scen. 1)

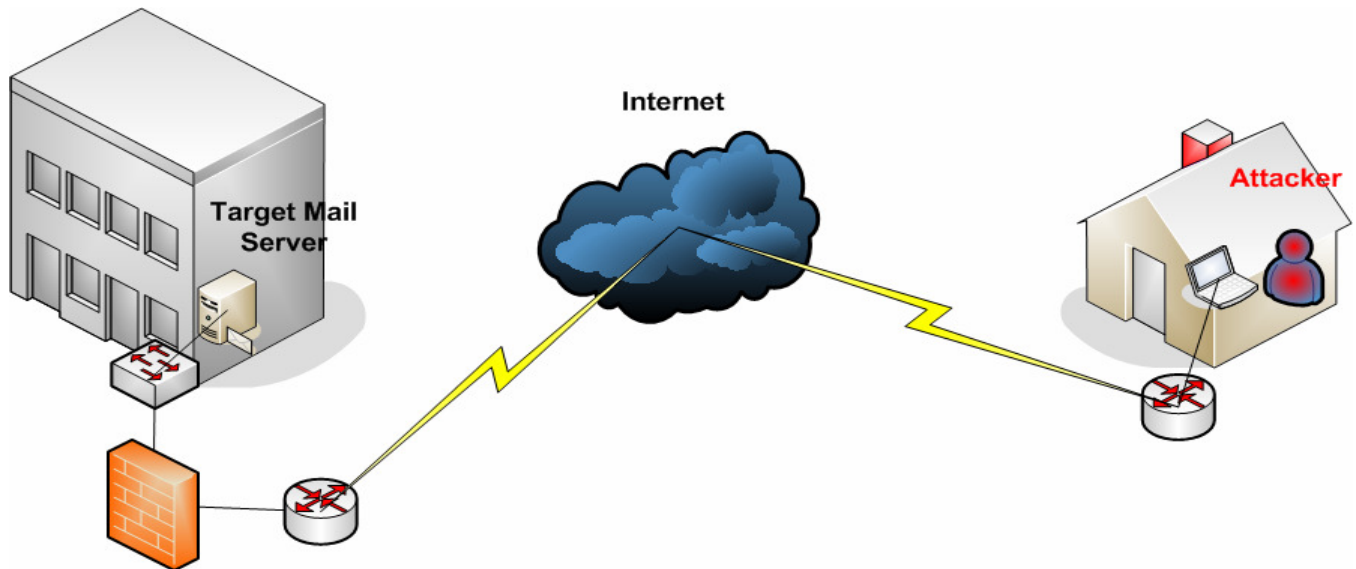


Figure 6-2 – Physical Network Diagram (Scen. 2)

**Observation** – Our target is a dedicated publicly accessible mail server. It is outside the firewall and readily accessible to us from any remote location. This opens our target to direct and indirect attacks.

**Cover and Concealment** – Since we are dealing with a dedicated server we can expect that it handles a large volume of traffic. Some of our direct attacks might be able to work effectively even while setting off IDS alarms. The firewall may block some of our attacks, so alternate methods will need to be planned.

Rootkits are viable for concealment after gaining access to both maintain access and hide our activity from administrators. Anti-forensics is useful if we want to avoid our target guessing who initiated the attack. If this is not a concern, anti-forensics are unnecessary as detection of an attack means corruption of our usable data.

**Obstacles** – For this scenario our only obstacles will be the router closest to the mail server (and possible IDS/IPS systems) and the firewall. For this attack all other digital obstacles are negligible.

**Key Terrain** – Key terrain in this scenario would be the router closest to the mail server. Compromising this router would give us access to all incoming and outgoing emails. Controlling the router is not

necessary for completion of the mission, as the mail server can still be controlled directly, so the router is not critical terrain.

**Avenues of Approach** – For this scenario indirect attacks don't fit our objective. User-initiated attacks might be effective, but if we want to ensure we get the email of all the executives who access the server we would need to use a spear-phishing tactic which wouldn't guarantee success. Our useful avenues are direct compromise of the server over the Internet or direct compromise of the router over the Internet.

## Scenario 2

An employee of the company processes critical company finance information at his workstation, Host A. Our goal is to gain access to the finance information and transmit it outside the secure internal network. Figures 7-1 and 7-2 show the logical and physical diagrams.

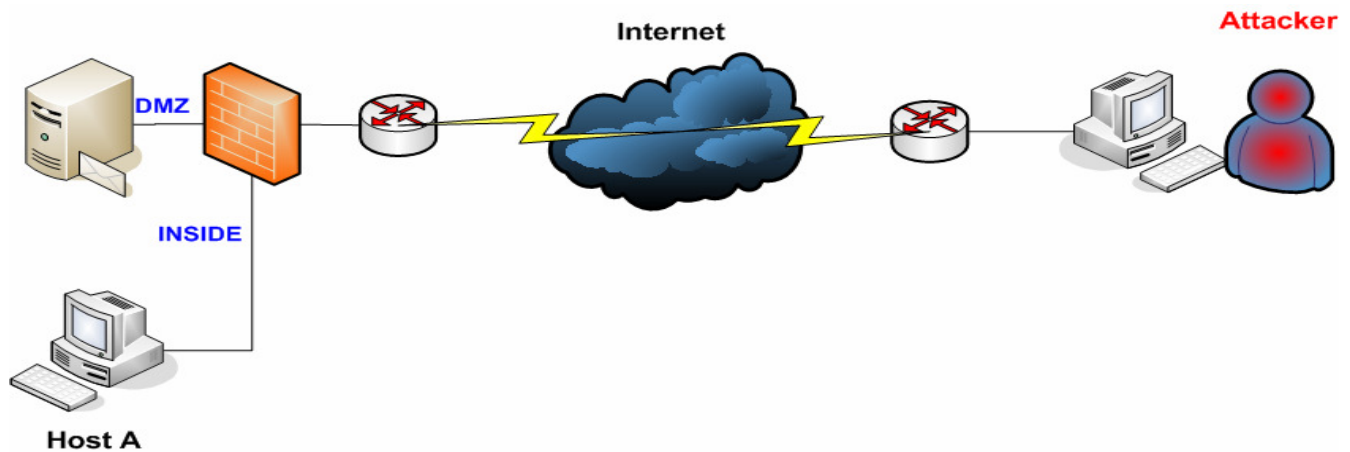


Figure 7-1 – Logical Network Diagram (Scen. 2)

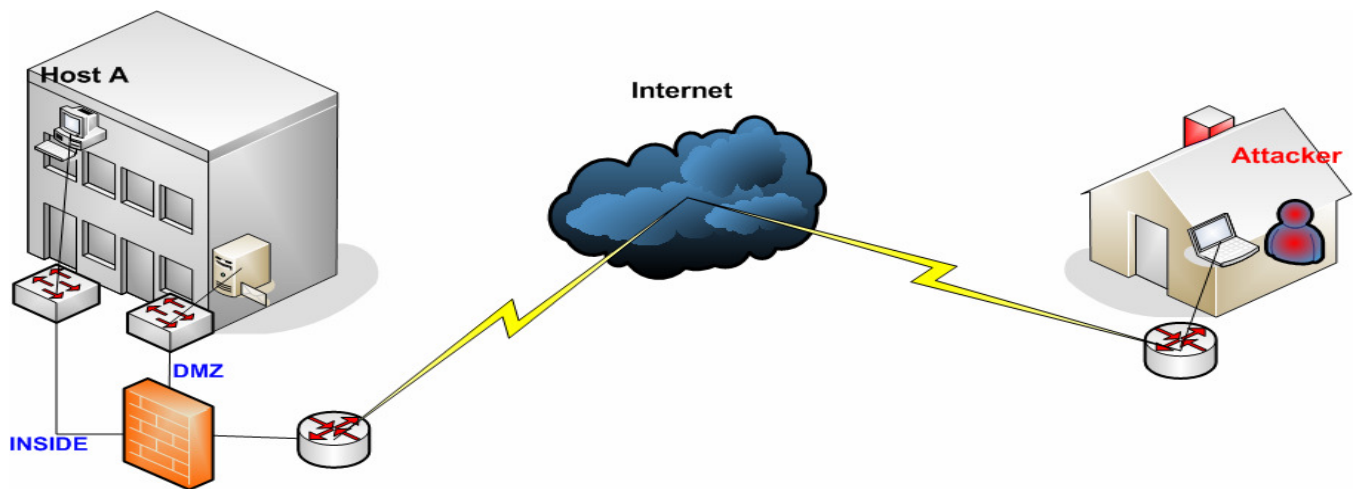


Figure 7-2 – Physical Network Diagram (Scen. 2)

**Observation** – Our target is behind a firewall and cannot be directly accessed from external networks. This closes the door on direct attacks and leaves us with only indirect attacks as an option.

**Cover and Concealment** – Our indirect attack will have to come from the inside out to be effective for our mission, so any successful attack will bypass external IDS/IPS sensors. Firewall rules are also generally more lax from the inside-out. In the event that an internal IDS/IPS present, or that restrictive egress filtering rules (which restrict traffic flowing out of the network) are present in the firewall, using an encrypted communication channel should shield our communications from any system or network administrators. The nature of encryption makes it difficult for anyone, even legitimate security hardware devices, to eavesdrop on communications. Even if the network is thoroughly secured and transmitting the encrypted data out of the network does trigger an alert, there would be no way to discern exactly what was transmitted.

**Obstacles** – For this attack our obstacles will be the router, firewall, and any IDS/IPS systems present. More specifically, our obstacles are the egress filtering rules of all of these devices, which will be difficult to discern beforehand. Once we gain access to the target we could use it to gain more information about the network, but the more information we gain in this way the more noise we create on the network, which in turn increases our likelihood of detection.

**Key Terrain** – There is no key applicable terrain in this scenario. Compromising the router or firewall might give us information, or allow us to change rules, but with our given objective none of the terrain points are necessary for the completion of the mission.

**Avenues of Approach** – For this scenario we have to rely on indirect attacks to guarantee success. Denial of Service attacks won't achieve the desired affect. This leaves us with User-Initiated attacks and Proximity attacks. Observation hasn't provided any clues that wireless is used in the target building, so proximity attacks are not viable, which leave just User-Initiated attacks.

User-initiated attacks can be planned with many variations. Calling the employee working on Host A and convincing him (via social engineering) to browse to a malicious website. Sending a phishing email to the employee with a link to a malicious website. Sending regular mail to the employee with a web address in a flyer, or a thumb drive with "demo" software pre-loaded. Any way to convince the user to actively give up the security of their network by browsing to a malicious website controlled by the attacker is a viable strategy.

### Scenario 3

Employees in the field are using mobile devices to stay in touch with headquarters, and report information on current operations in the field. The attacker wants to cut off this feed to cause employees in the field to break down and stop working. Figures 9-1 and 9-2 show the logical and physical diagrams.

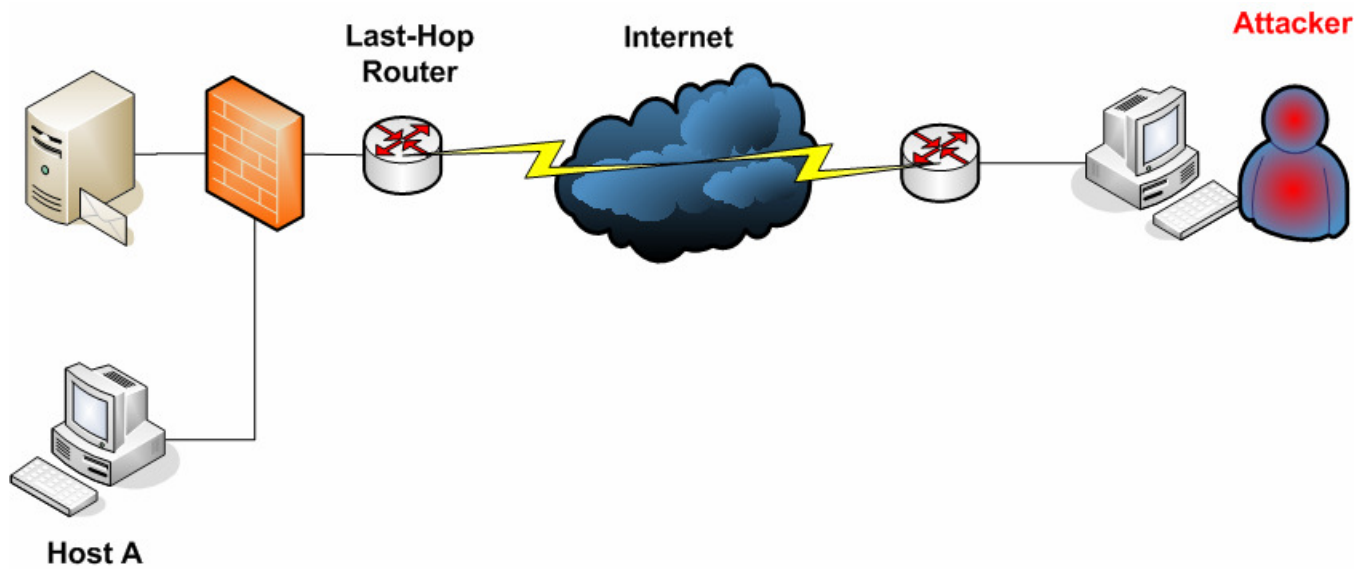


Figure 9-1 – Logical Network Diagram (Scen. 3)

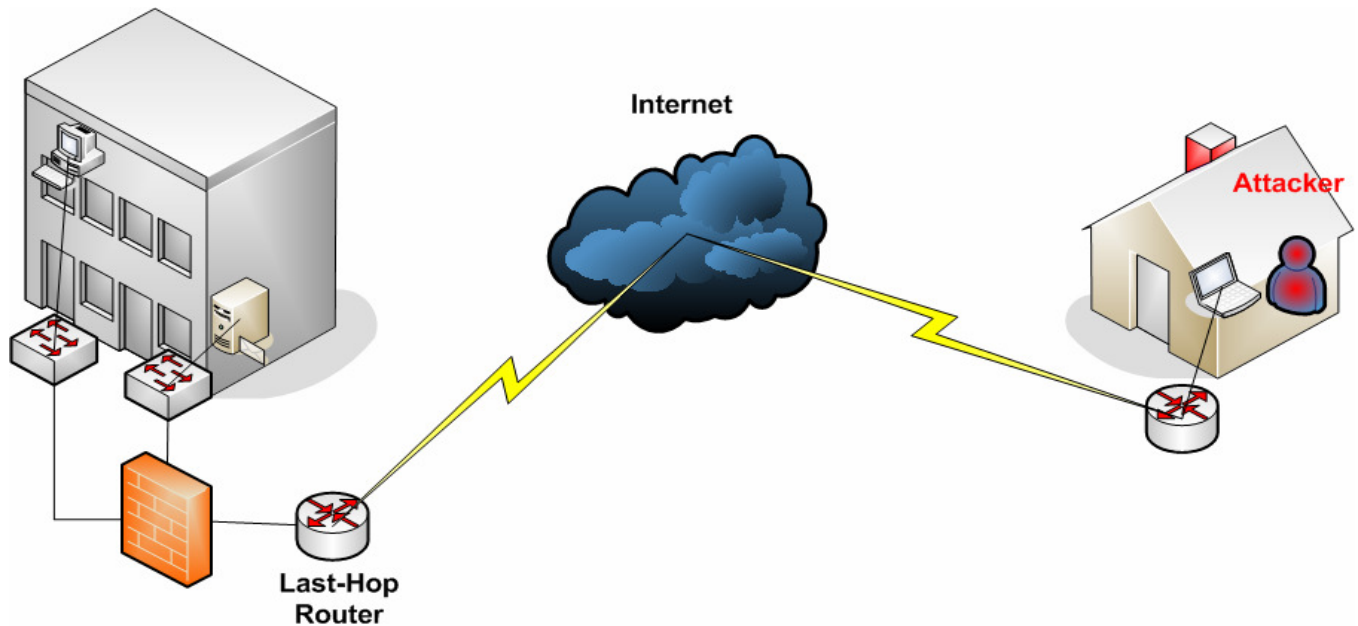


Figure 9-2 – Physical Network Diagram (Scen. 3)

**Observation** – Our target is the last-hop router of our target network. By definition it must be accessible from the Internet. This opens it to both direct and indirect attacks.

**Cover and Concealment** – Our target in this case is the Last-Hop Router, and through it the network as a whole. If a direct attack is used we may have to try and avoid an IDS/IPS system sitting outside the router. The goal of the mission is noticeable disruption, so at some point the attack will be in the open. The direct attack will work if we can maintain access after compromising, if our attack is found and fixed, we may not be able to find a new flaw quickly enough and service will be restored.

If we opt for an indirect attack, opening the door for Distributed Denial of Service (DDoS) and Distributed Reflective Denial of Service (DRDoS) cover is negligible. These attacks are the equivalent of full frontal assaults, opening as much firepower as is available and attempting to crush the Last-Hop Router under the weight. An indirect attack of this type will be loud and noticeable. Anti-forensic techniques can still be used to attempt to mask the true attacker.

**Obstacles** – If a direct attack is used an IDS/IPS may be present. If an indirect attack is used the only relevant obstacle is the bandwidth of the link between the Last-Hop Router and the Internet. The distributed attacks will try and saturate this link, which will prevent incoming and outgoing communications.

**Key Terrain** – If a direct attack is used the Last-Hop Router is critical terrain. If an indirect attack is used there is no key terrain.

**Avenues of Approach** – For this scenario we have two primary avenues of approach. The direct attack will concentrate on subverting the Last-Hop Router and using the access gained to wreak havoc on the target network. The indirect attack will concentrate on flooding the network with traffic, as much as is available to the attacker, to cause serious degradation of network quality and prevent messages from being transmitted to or from the target network.

## Conclusion

While this paper is not meant to be an exhaustive list of all digital attacks it should be clear that the same considerations that go into planning an operation in the real world can be applied, using the same methodology, to the digital world. The scenarios in this paper have been deliberately kept simple to maintain focus on the process and not all possible attacks, but this process could easily be applied to more complex situations, or to the defensive posture.