Contents

[**Assumptions** 2](#_Toc33378679)

[Services already in space 2](#_Toc33378680)

[Network Design 2](#_Toc33378681)

[**Implementation** 3](#_Toc33378682)

[General settings 3](#_Toc33378683)

[Security configuration 5](#_Toc33378684)

[**MAC filtering** 5](#_Toc33378685)

[**DoS protection** 6](#_Toc33378686)

[**Threat Assessment** 7](#_Toc33378687)

[Top threats 7](#_Toc33378688)

[**DoS Attack** 7](#_Toc33378689)

[**Outdated Firmware** 7](#_Toc33378690)

[Mitigation 8](#_Toc33378691)

[**DoS** 8](#_Toc33378692)

[**Firmware update** 8](#_Toc33378693)

[**References** 9](#_Toc33378694)

**Device assigned**: Netgear (R7000-100PAS) Nighthawk AC1900

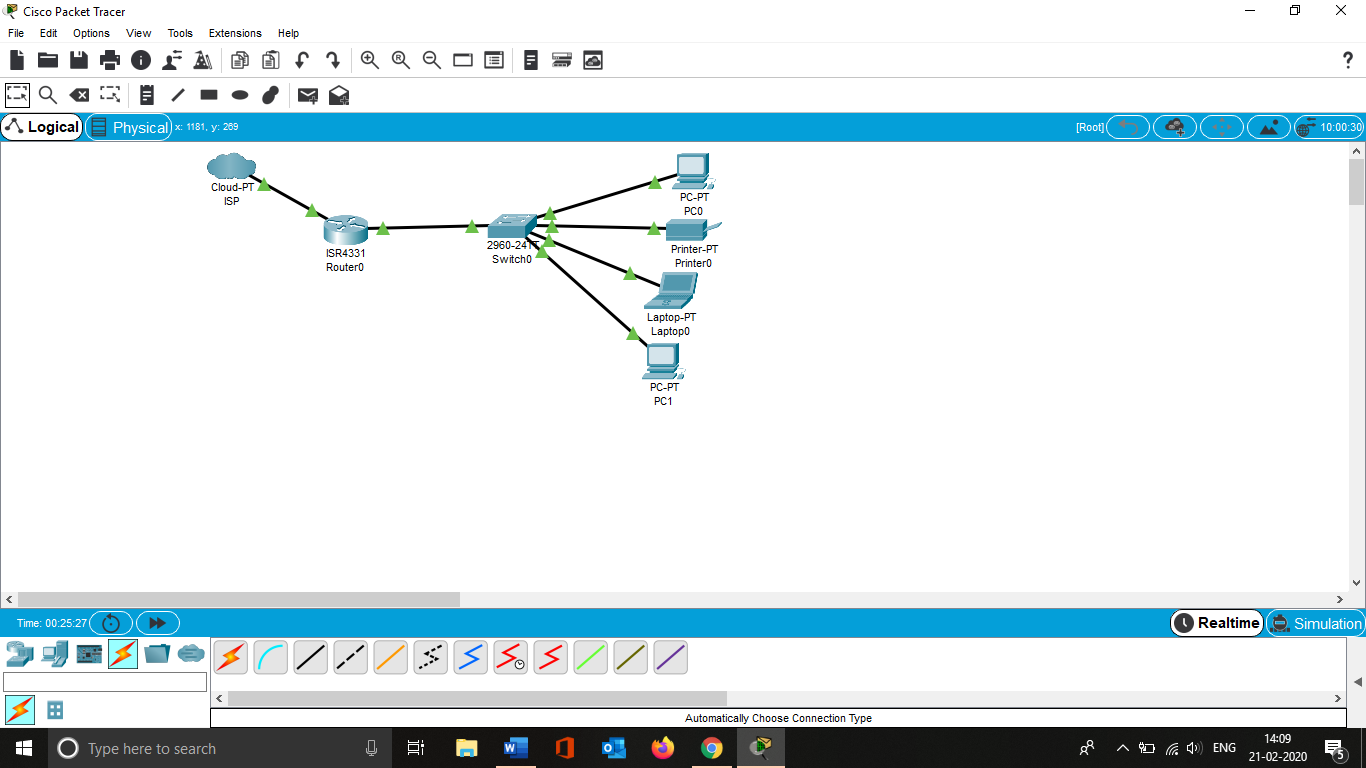
# **Assumptions**

* Since it mentioned as a small size organization the number of employees would be roughly from 10 to 50.
* Since it mentioned as internal users to access the network wirelessly it can be considered as assessing work-related things such as FTP, email.
* It is assumed that threat assessment has been conducted after the implementation of suggested security configurations.

## Services already in space

* Small size organization
* DHCP service using a local ISP
* IP range 192.168.10.0/24
* For internal users

## Network Design

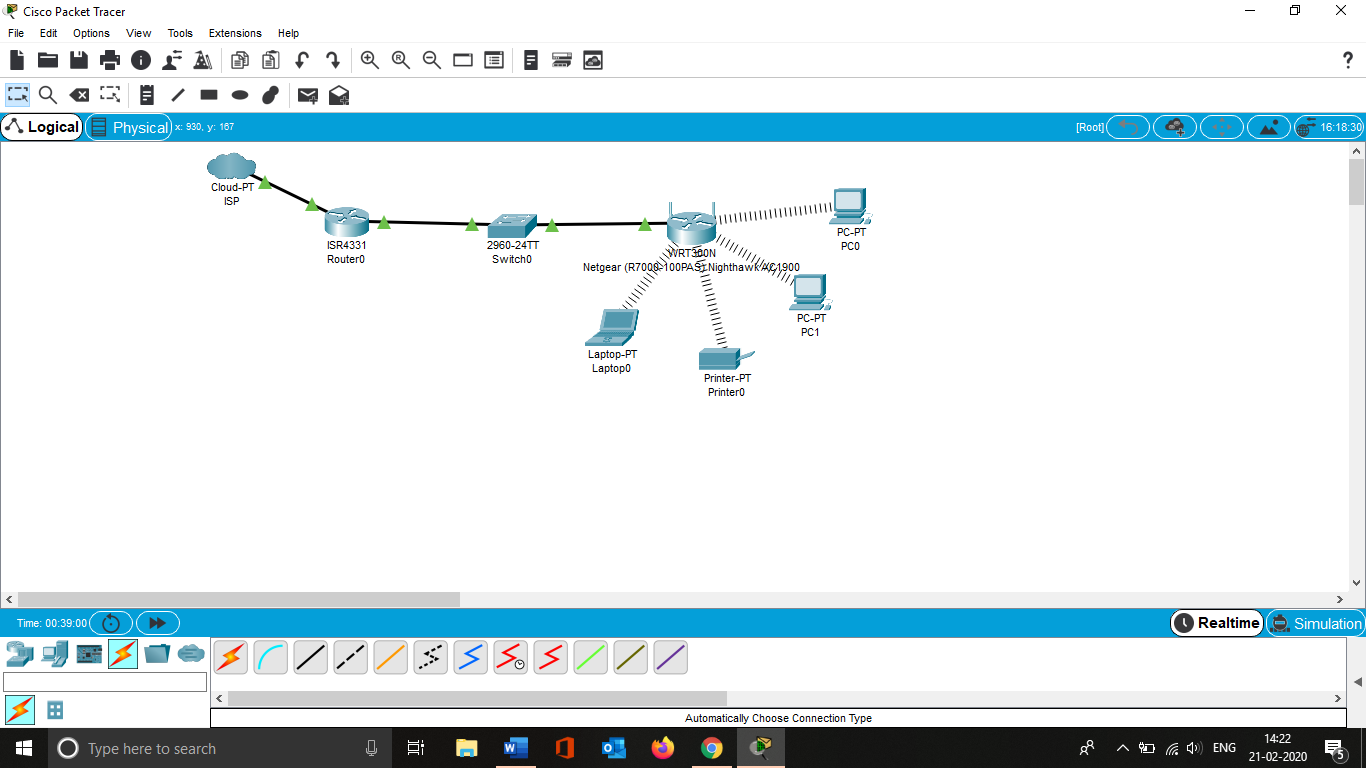


Screenshot 1 Current network design assumption

If the above network diagram is currently in a place where the ISP connected through the wired router to provide DHCP. Then the router connected to switch to provide access to the devices in the network using wired technology.

# **Implementation**

Implementation of wireless networking starts with placement of the wireless router as stated in the assumption currently the organization uses wired where all the devices connected to the switch. So for that, the proposed design would be the following,



Screenshot 2 Proposed design

By following the above proposal, the wireless router Netgear (R7000-100PAS) Nighthawk AC1900 will be connected to the switch then the devices can be connected to the wireless router.

## General settings

General settings such as SSID names, wireless passwords, router login credentials can be configured by connecting through the wireless router through connecting computer/laptop to the router using LAN cable or connecting wirelessly using WPS button. The detailed process as follows (Bob, 2016)

1. Once connected either through wired/wireless in browser type <http://www.routerlogin.net> to go to router’s login page where we can setup the wireless network SSID, passphrase, etc..

2. The default username name here is admin and the passphrase the is the one the user entered while connecting to the wireless.

3. In **Basic Homepage** select wireless



Figure Basic Configuration ShopKeep. (2016)

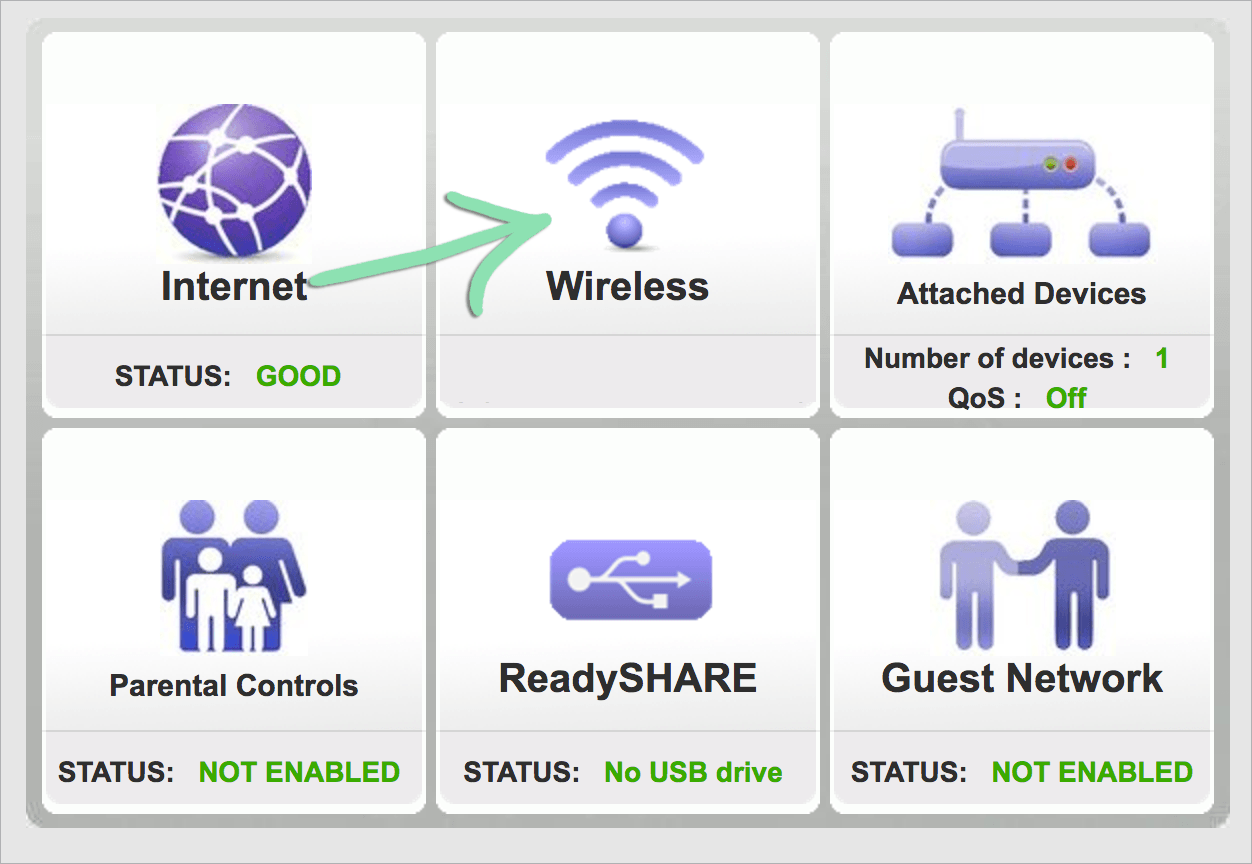


Figure Basic Configuration ShopKeep. (2016) cont..

4. After that select the Name, type of security (WPA2-PSK, WPA/WPA2 Enterprise), and Password. (For the scenario given I suggest to use WPA2-PSK.

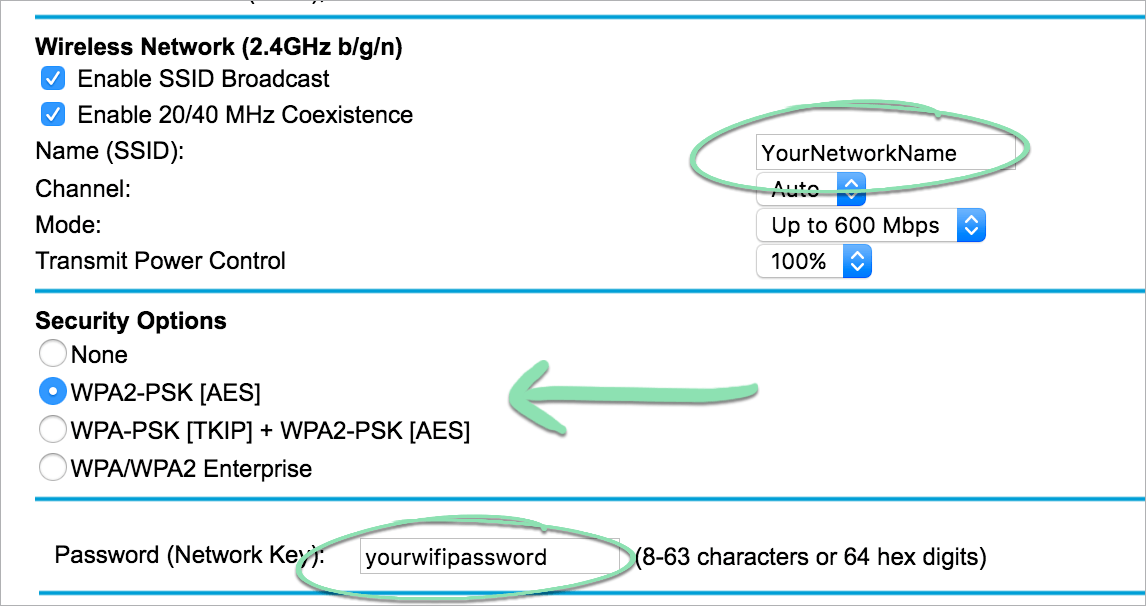


Figure Basic configuration ShopKeep. (2016) cont...

5. Then select **apply** to save the settings.

## Security configuration

The router assigned here is has several security options but when considering the given scenario, the appropriate configuration would be using MAC filtering. Because it stated that the extension of the wireless network provide access to the internal users.

### **MAC filtering**

So, in order to do the MAC filter configuration, the process is,

1. Connect to the router either from Mobile or computer

2. In browser, enter the URL <http://www.routerlogin.net> then a login Windows will appear. Enter the login credentials.

3. choose **ADVANCED > Security > Access Control**. Then an Access Control page appears.

4. Choose the **Turn on Access Control check box**

(User must choose this check box before specifying an access rule and can use Allow or Block options. If the check box is not selected even the blocked devices can connect to the network)

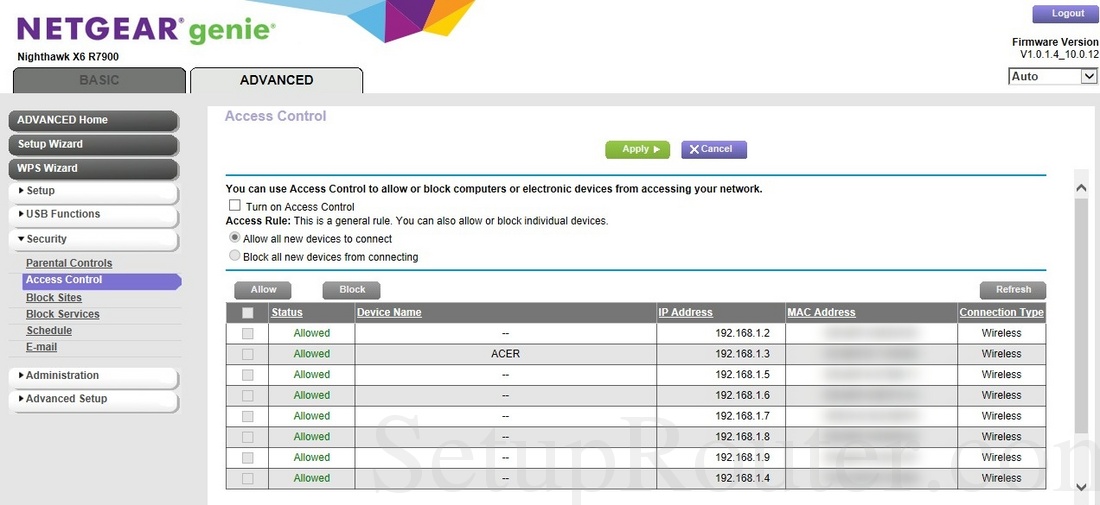


Figure Advanced settings ShopKeep. (2016)

5. After that the user must choose the following option,

* **Block all new devices from connecting**

Using this setting the user should enter the new device’s MAC address for both Ethernet connection and Wireless connection in the allowed list.

6. Once it completed click the **apply** and the changes take effect.

### **DoS protection**

Another advanced security features available in the given Wireless router is Dos Protection. Enabling this option would be advisable for the organisation. This feature prevents the LAN network from DoS attacks such as using Syn flood, Smurf Attack, Ping of Death,etc..

To enable this option user should login to their router configuration page in their browser then have to select this option under **ADVANCED > Setup > WAN Setup** then click the checkbox **Disable Port Scan and DoS Protection** then click **Apply** button to save the configuration.

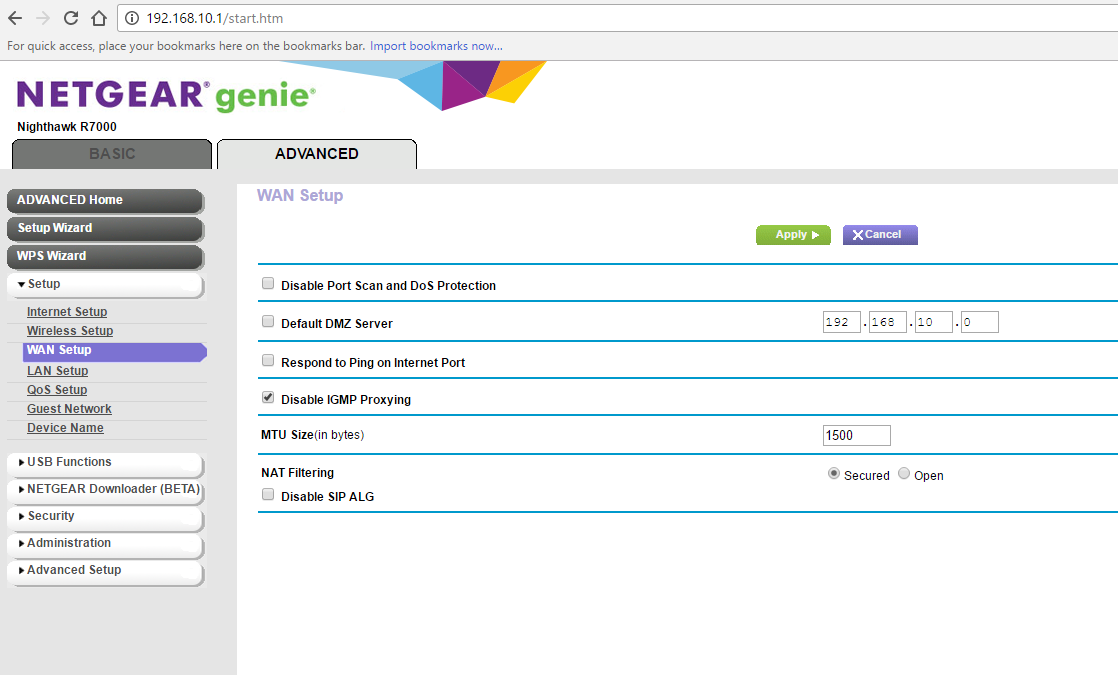


Figure Advanced settings SamLabrador. (2017) cont...

# **Threat Assessment**

## Top threats

There are several types of attacks that can cause severe damage in QoS in a wireless network. For the given scenario and requirement, the considerable top threats are DoS attack, and outdated firmware.

### **DoS Attack**

The primary threat that the organisations would possibly encounter while extending the wireless network is **DoS attacks** (Geier, 2003)**.** This attack can be conducted using the technique Packet-based brute force DoS. Where the intruder sends huge volume of packets to the server and cause it to go down. According to research (CALYPTIX, 2017) 35% of attacks on network are DoS and Brute force attack. Wireless DoS attacks (Compton, 2008) can be done in any layer for instances hacker can create strong electromagnetic ways that can collide and affects the wireless routers signal/performance strength and so on.

### **Outdated Firmware**

Same as any other softwares, router’s firmware also should be updated regularly. Router’s firmware (Techopedia, n.d.) is basically a pre-installed software that’s responsible for network protocol, security mechanism. In other words, it’s like operating system of the router. As like usual softwares the manufactures of the routers also release the updates for the router firmware. Purpose of updating the firmware is to increase the performance of the product and as well as to prevent from new security vulnerabilities.

There are several updates released by the assigned manufacture can be found online (MITRE, 2017).

## Mitigation

### **DoS**

When considering mitigation for the DoS different strategy can be applied in different layer for example, for physical layer placement of wireless router will be a recommended strategy (Compton, 2008). Placing the router in proper height will prevent hackers from reaching it easily.

To prevent DoS in further layers it’s advisable to enable DoS prevention mode in the router. Not all the router models have this feature.

For the given model the DoS prevention option can be enabled which is a vital mitigation strategy that can be applied here. To option can be found under **ADVANCED > Setup > WAN Setup** then click the checkbox **Disable Port Scan and DoS Protection** then click **Apply** button to save the configuration.

### **Firmware update**

In general, there are 2 ways to update the firmware. One is by configuring auto update and second one is manually search for the update and applies it. These 2 options can be found in all the routers. Updating the firmware in regular basis is a recommended mitigation strategy for this threat.

For the assigned router firmware updating can be performed only by manually.

In the assigned model user can either manually check for the update in router’s menu or download from internet and upload it. The settings can be found under **ADVANCE->Administration->Router update**

# **References**

Bob. (2016). R7000 Nighthawk Wireless Router Setup | ShopKeep Support. Retrieved from <https://www.shopkeep.com/support/hardware/r7000-nighthawk-smart-wireless-router-setup>

CALYPTIX. (2017). Top 8 Network Attacks by Type in 2017. Retrieved from <https://www.calyptix.com/top-threats/top-8-network-attacks-type-2017/>

Compton, S. (2008). SANS Institute: Reading Room - Wireless Access. Retrieved from <https://www.sans.org/reading-room/whitepapers/wireless/80211-denial-service-attacks-mitigation-2108>

Geier, J. (2003). Denial of Service a Big WLAN Issue. Retrieved from <https://www.esecurityplanet.com/trends/article.php/2200071/Denial-of-Service-a-Big-WLAN-Issue.htm>

MITRE. (2017). CVE-2016-6277 : NETGEAR R6250 before 1.0.4.6.Beta, R6400 before 1.0.1.18.Beta, R6700 before 1.0.1.14.Beta, R6900, R7000 before 1.0.7.6.B. Retrieved from <https://www.cvedetails.com/cve/CVE-2016-6277/>

Techopedia. What is Router Firmware? - Definition from Techopedia. Retrieved from <https://www.techopedia.com/definition/3177/router-firmware>

Netgear. (2019). *Netgear User manual Nighthawk AC1900 Smart WiFi Router Model R7000* [Ebook]. San Jose, CA 95134, USA: Netgear. Retrieved from <https://www.downloads.netgear.com/files/GDC/R7000/R7000_UM.pdf>

For Images from Figure 1 to Figure 4

ShopKeep. (2016). *How to Set Up the R700 Nighthawk Smart Wireless Router with ShopKeep* [Video]. Retrieved from <https://www.youtube.com/watch?v=xOXrp4ASJZE&feature=youtu.be>

For Figure 5

SamLabrador. (2017). *IP Passthrough with AT&& Gigapower Pace 5268 to Netgear AC1900 r7000* [Image]. Retrieved from <https://community.netgear.com/t5/image/serverpage/image-id/14924i9339D2A4005CC7BF?v=1.0>