Scotti-BYTE Enterprise Consulting Services

Networking Tutorial: The Basics of Routers, Switches and LANs

Last time we discussed the creation of Virtual Machines. Virtual Machines and bare metal physical machines normally reside on networks. A network is the thoroughfare on which traffic between computers travels.

A Wide Area Network (WAN) is a collection of smaller Local Area Networks (LANs). For this discussion, we will consider the Public Internet as the WAN and a home network as a LAN. The most common language that computers speak on networks today is Transmission Control Protocol/Internet Protocol (TCP/IP). TCP/IP was created by the Unitied States Department of Defense in the 1970's to enable computers to communicate over a network.

TCP/IP has four layers, the link layer, the IP layer, transport layer and the application layer. This was developed at the same time and is comparable to the Open Systems Interconnection model (OSI) and views computer networking in terms of abstraction layers.

OSI Model		
	Data unit	**Layer**
Host layers	7. Application	Network process to computer programs
	6. Presentation	Data representation, security encryption, convert computer code to network formatted code
	5. Session	Interhost communication, managing sessions between programs
	4. Transport	End-to-end connections, reliability and flow control
Media layers	3. Network	Path determination and logical addressing
	2. Data link	Physical addressing
	1. Physical	The physical infrastructure used to send and receive signals

For the purpose of this discussion, layer 2 is responsible for breaking information down into frames and transmitting over the physical layer. Layer 3 coordinates the parts of a data conversation to organize large files and reassemble them at the destination. This layer is also responsible for finding the best path from one network to another to ensure delivery of the data.

For our purposes, we are going to discuss the older and more prevalent TCP/IP V4 networking protocol. Home users and small businesses typically have a connection to the Internet via multi-functional device which we have come to know as a router or sometimes erroneously called the modem.

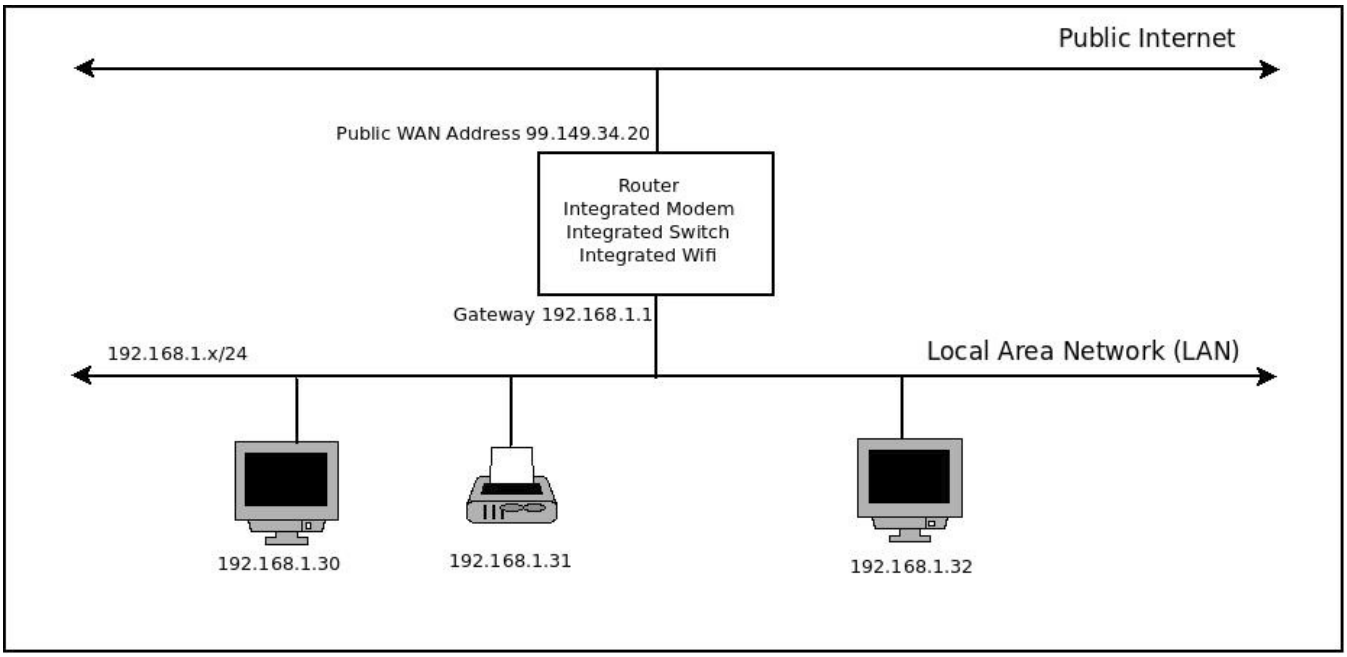
In reality, this device is normally a cable modem, a router, an ethernet switch, and a wireless access point. The job of the modem is to take the internet connection offered over a cable, telephone line, or fibre optic connection and to provide that signal on an unshielded twisted pair ethernet cable. The modem also has the job of acquiring a TCP/IP address from your Internet Service provider which is an address on the WAN (the Internet).

The modem then provides the WAN address to your router. The router has many jobs. The router uses a protocol called Dynamic Host Configuration Protocol (DHCP) to give every client device (computer) on your network a LAN TCP/IP address and the router tracks those addresses. The most common TCP/IP address range used on a LAN is 192.168.1.x.

The addresses in this range are referred to as private addresses since they are not publically accessible from the Internet. Another reason why private address ranges are used on LANs is because there are a limited number of Internet addresses available in the TCP/IP V4 range. Specifically, each of the four values in a dotted TCP/IP address is a number from 1 to 255. This provides a total of 4,294,967,296 addresses in this 32 bit address space. That sounds like a lot, but public addresses in this range are nearly exhausted worldwide.

TCP/IP V6 is now in use and has a 128 bit address space compared with the 32 bit address space in TCP/IP V4. The TCP/IP address space is roughly 17 billion times the size of the TCP/IP V4 address space. So, it is virtually unlimited.

The more substancial reason why routers are used is for security. The private address range on the LAN side of your network is not directly accessible from the Internet. Routers employ Network Address Translation which is a process where one or more local IP addresses can



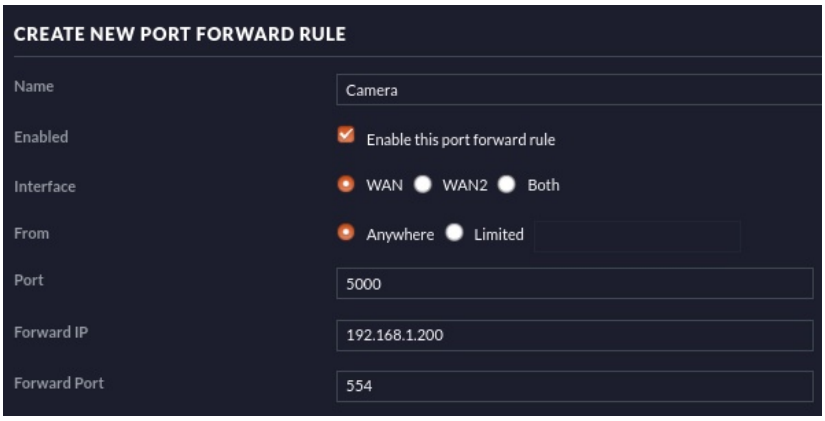
share a WAN address on the modem granted by the Internet Service Provider (ISP).
In the illustration, note that 99.149.34.20 is an example of an ISP granted WAN address. The inside private addresses are 192.168.1.30 and 192.168.1.32 for two PCs and 192.168.1.31 for a printer. The gateway at 192.168.1.1 is the address of the router and also the route or direction that a device on the LAN has to take to get to the WAN.

Communication from the LAN to the WAN is possible directly, but responses back to the LAN are handled through Network Address Translation (NAT). Most LANs have routers configured to use dynamic NAT. In this type of NAT, an unregistered IP address is translated into the registered public WAN address of the router. For example, if the PC at 192.168.1.30 wishes to go to google.com, the outbound request to google.com looks like it comes from 99.149.34.20, but the 192.168.1.30 LAN address is encapsulated in the request so that the router will know where to send the response to when the information is sent back to the router at 99.149.34.20.

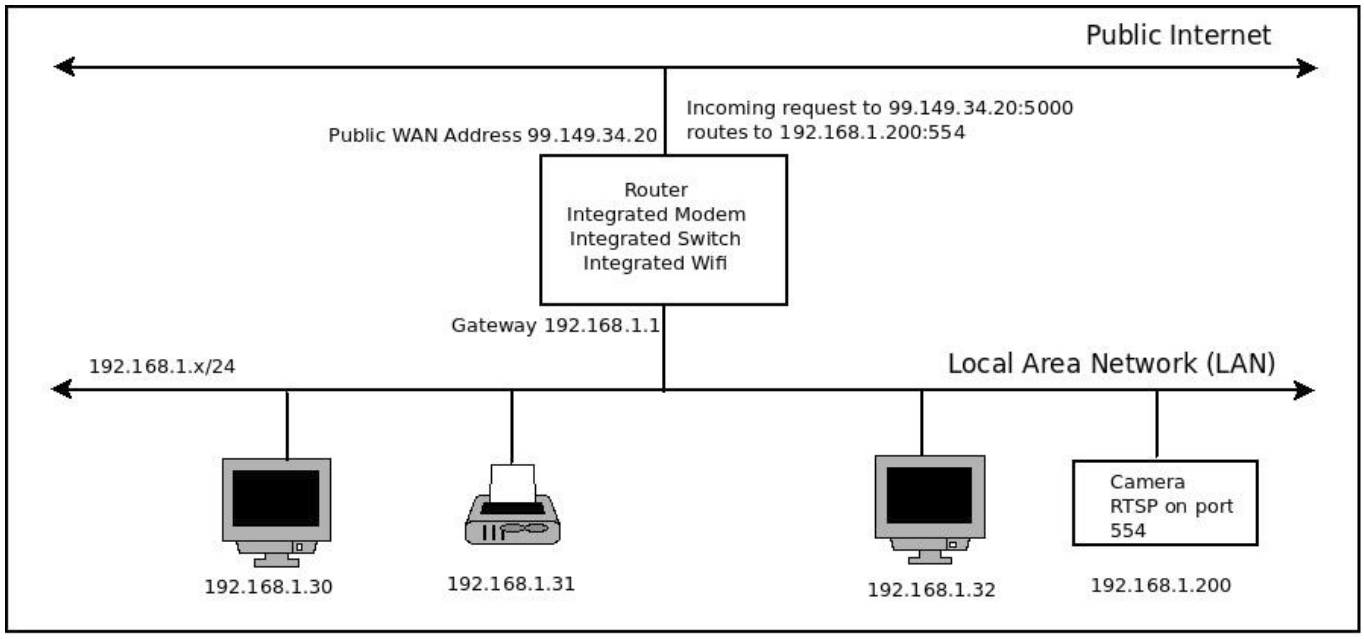
In addition to TCP/IP addresses, different types of traffic move on different IP Port numbers. Port numbers are usually utilized by applications to make connections. There are several well known application port numbers such as port 80 for http we traffic and port 21 for file transfer protocol traffic. So, a PC might be providing an Apache web server on port 8080 and the

address of the web server might be 192.168.1.100. This would be referred to as 192.168.1.100:8080.

In addition to NAT, routers also implement Port Address Translation (PAT). With PAT, TCP/IP port numbers are used to tell the router which system on the LAN is supposed to receive certain traffic. PAT is also referred to as routing pinholes or port forwarding.



Most routers allow you to define a router pinhole or port forward to use for PAT. As an example, you might have a camera running at address 192.168.1.200 speaking

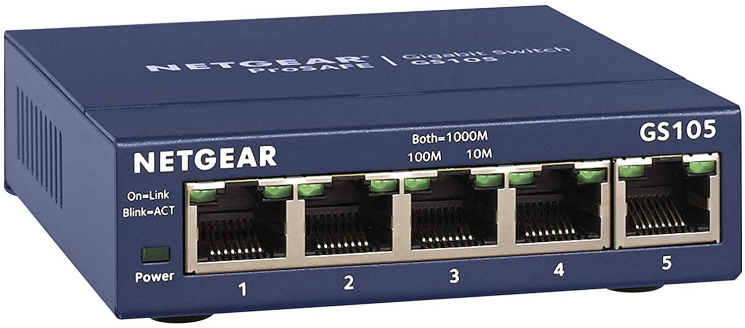


the Real Time Streaming Protocol (RTSP) which uses port 554. If you arbitrarily define port 5000 on your router to forward to 192.168.1.200 at port 554, this would allow your camera to be accessible from the public internet at 99.149.34.20:5000 in our example. Port forwarding is not the most secure way to configure your network, but it is normally one of the only options available on a typical retail router. The reason that port forwarding pinholes are not secure is that they provide a wide open pathway to the target node and port number on your LAN that you define. If you are confident in the security of your target system, then that is ok.

Routers are also referred to as firewalls because they block inbound traffic from the Internet to your LAN devices. From a security perspective, this is not secure because you may have devices on your LAN that make connections to servers on the Internet that provide unintentional access to your LAN remotely. Most people run firewalls on their LAN computers also, virus protection, spyware protection and ad-blockers but even with all these measures, retail routers do not provide the necessary protection. The best security posture is to block all unauthorized traffic at the router and not all routers can do that. Better quality routers provide Internet Prevention System (IPS), Geographical IP filtering (GeoIP), and Deep Packet Inspection (DPI), and DNS filtering. All these measures allow for much better inbound and outbound traffic control from the LAN.

Another function that a combo router provides is an ethernet switch. If you look at the back of your router and you have four or five additional ports other than the connection to your ISP, those are switch ports. Switch ports allow you to connect more than one computer to your Internet connection. Many routers have these additional switch ports that let you plug in multiple computers, printers, and other devices. These switch ports are "unmanaged" ports. Unmanaged ports are swtich ports that "repeat" all traffic of the device plugged into them to all the other ports. This allows any device on the network to communicate with any other device. This sounds like a great idea, but not always desireable.

For example, you may have a device that has so much communication that it creates so much traffic on the network to the point that it negatively impacts the performance of the other systems connected to your LAN. Also, as described above, you may have an Internet camera, Smart Speaker, or Smart Thermostat that could be providing unintended access to the other systems on your network.



It is also common to add an inexpensive unmanaged switch external to your router when you need more ports. These are great devices, but they do nothing for traffic management or security.

The alternative is to acquire a "managed switch". A managed switch goes beyond layer 2 bridging as described above and can perform many of the functions of a router at layer 3. The Netgear switch pictured is an unmanaged layer 2 swtich and performs only the bridging function. A managed switch, also referred to as a layer 3 switch can support IP routing and supports VLANs. A VLAN is a virtual LAN. A VLAN is a way of creating another network separate from your primary LAN. Your primary LAN is usually referred to as VLAN 1. More advanced routers and managed switches allow the definition and routing of VLANs.

The switch pictured at right is a managed switch that allows the configuration and management of VLANs.

A practical use of a VLAN might be placing all of your Internet cameras on a separate VLAN so that those cameras do not share the network with your computers.

Once you have a secondary VLAN established, a more advanced router can define rules which dictate what traffic is allowed to move between networks. An example might be that a camera on the camera VLAN should be accessible from your main LAN but not vice versa.

Another example, might be to have another VLAN for guests. This has the advantage of allowing a guest access to the Internet but not to your local LAN. A guest network might provide a separate wifi SSID with a different password. A lot of routers support a guest network, but they do so with rudimentary filtering and not a separate VLAN. The separate VLAN assures security. Also, since you can define routing rules, you could potentially offer your printer on your LAN for access to guests but without access to anything else.

This leads to our final discussion which is wifi access. Typical home routers are combo devices that combine a modem, router, switch, and wireless access point as was mentioned earlier and pictured at right. If the wireless access point (WAP) is internal to your router, the radio signal will radiate from where it is located. Most people have their router where the ISP installed it in their home and that is clearly not optimal.

A better solution would be to have a separate WAP installed at a central location in the home or maybe even have multiple WAPs installed to provide broader and redundant coverage for the wifi signal. Wifi is a radio signal and walls, floors and distance effect the strength and reliabilty of that signal. You will have to run a wire from the router to the access point, but the multitude of wireless devices in most homes will benefit.

In addition, better WAPs provide mesh networking when you use more than one WAP which provides seamless switching to the WAP with the strongest signal as you move from place to place in the home.

Just like managed switches, managed WAPs provide built-in capability to offer SSIDs on different VLANs for security and flexibility.

In summary, it is advisable to own a separate cable modem, router, switch and one or more wireless access points. If possible, make the jump to a managed switch and a router that handles layer three switching. This allows not only for better operation and enhanced security, but also allows for incremental and less costly upgrades as technology advances.