What's On Your Network?

Understanding Network Discovery

Progress® | ipswitch®

Overview: The State of the Network Today

Modern corporate networks have become much more dynamic than they used to be. Devices connect and disconnect from networks much more often, particularly in workplaces with Bring Your Own Device (BYOD) policies, where employees can connect personal devices such as laptops and cell phones. The types and varieties of devices have expanded also. In addition to computers and workstations, the typical network includes printers, copiers, routers, switches, VoIP boxes, and other managed appliances.

More importantly, all of these devices are being dynamically connected, disconnected and reconnected to your network constantly. Users demand the ability to connect whatever device they want to the network when they want so they can work where and how they want. Guest and short-term contractors come and go unpredictably and require network access to do their jobs. Even devices like printers, copiers and wireless routers that should remain stable can be connected or disconnected by individual users for a myriad of reasons. And if you think they'll ask IT before making these changes, you haven't worked with users for very long!

This constantly changing environment makes it extremely difficult for system admins and network admins to know what's connected to the network. For most of them, it can be a bit of a shock to see what is actually connected to their network – and that's a problem.

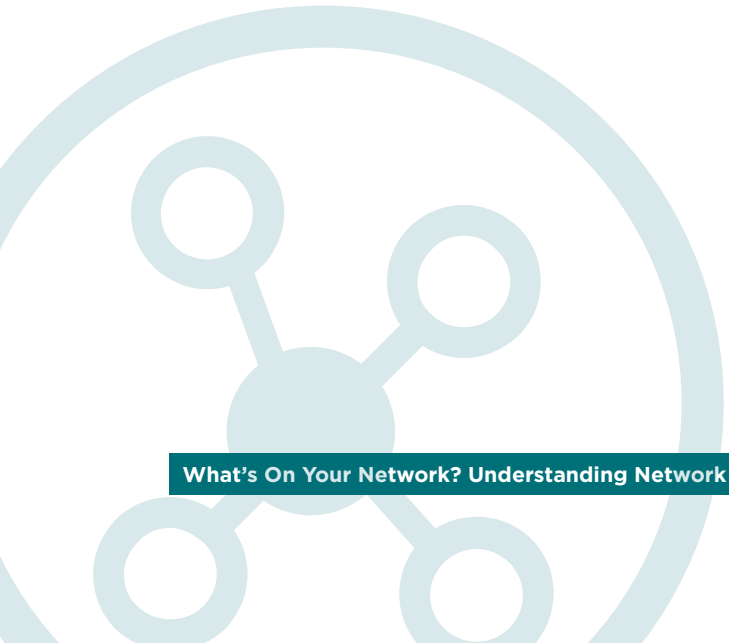
What is Network Discovery?

Network discovery is, not surprisingly, the process of finding and identifying every device, server and system on your network. Mastering IT best practices around network discovery will greatly improve how you map and monitor your IT infrastructure.

Networks these days are more dynamic than their predecessors. Tracking everything on your network manually is absolutely not realistic. For starters, just think about the changes that virtualization and live migrations have brought forth.

Instead, IT pros need to have up-to-date network inventory based upon discovery and asset management – from the physical to the virtual. We'll look into how this is done exactly later in this document, but first let's make sure we know why we're doing this in the first place.

IT pros need to have up-to-date network inventory based upon discovery and asset management – from the physical to the virtual.



The Value of Network Discovery

Sure, it's nice to know what's on your network at any given time, but does it really matter? Absolutely. There are a number of reasons why regularly discovering what's connected to your network is essential.

Asset Inventory

If you own it and manage it, you have to keep track of it. When inventory time comes around there are a few options for IT pros: physically crawl around the server closet to manually count every device or run a network discovery scan and automatically generate a network inventory report. The advantage IT has over other types of organizations is that our assets actually talk to each other. You should be able to push one button and get a complete inventory of everything attached to your network.

Troubleshooting

You can't fix it if you can't find it. Not only will a complete network discovery give you an understanding of what's connected to your network, it will put it all in context. Hard-to-diagnose problems like wireless APs that keep dropping signal suddenly become simple fixes when it's clear that too many users are trying to connect at once.

Audits

At some point, any network administrator will need to do an audit of all these connected network devices. Logging and tracking all devices is essential for configuration management, capacity planning, and security. Things will have changed even if you have been diligent in logging devices as they are connected. A network discovery tool can find and identify everything connected to your network, produce a topology of how they are connected to each other, and produce detailed reports for planning purposes.

Compliance

Another type of audit is the compliance audit which determines if your systems meet specific regulations. Depending upon your organization, those regulations may include PCI, HIPAA, SOX or others. Almost every organization is going to need to comply with the EU's GDPR regulation as well. That means knowing what devices are connected to your network and what software and traffic is running on them. An up-to-date network discovery lets you prove that all your devices are current with the latest patches to make them compliant – or it will let you know what you need to do to be ready for that audit.

Security

This should go without saying. If you don't know what's connected to your network you aren't going to be able to identify insecure devices like rogue wireless access points that someone has shoved under their desk. You need to know where network access can be obtained and how – and you can't do that without discovering what's connected at all times.

Mapping

Network discovery goes hand in hand with network topology mapping and are often combined as a single function. You can't generate a map of everything attached to your network without discovering all those devices first. Mapping will also help you put together a dependency structure that can be invaluable when troubleshooting. For example, if you know that a particular physical server is down, you can ignore the alerts from all the other downstream devices or virtual machines hosted on that server while you fix the more important problem. Sometimes half of the challenge of troubleshooting is working past the alert storms to find the underlying issue and a network map that shows dependencies can be invaluable.

Reporting

External auditors aren't the only ones who want to know what hardware and software assets are running on your network. Groups both within and without IT need to know what your organization is has online for budget and planning purposes. A current network discovery means you can provide a report about which security patches have been applied to all you Cisco routers (for example) the moment someone asks for it.

What Exactly Should Be Discovered?

This is where it's important to dive a touch deeper than basic device discovery. The network does not just consist of hardware, but also of the software running on that hardware and the systems, traffic and data running on top of that. It's all interlinked, interrelated and interdependent. A network discovery should find a wider variety of assets.

Physical Devices

Obviously the most basic function of network discovery is to identify every physical thing plugged into or connecting to the network. That's mostly going to be servers, switches and routers – and don't forget storage devices! But that's only the beginning.

Wireless Access Points

Technically another physical device, but they allow the connection of myriad other devices without a physical link and they pose their own unique set of challenges. Some wireless access points may not even be connected physically to your network and may be managed by a third-party via the cloud (Meraki, for example).

Virtual Devices

Virtualization has become commonplace and virtual hosts and servers are going to be a part of just about every network. Your discovery has to go beyond the physical servers to determine what virtual devices are present.

Cloud Resources

A server's still a server, even if it's on someone else's computer. All your cloud resources may be detailed separately in whatever management interface your cloud service provide offers, but that doesn't help if you're trying to get a complete inventory of your networking assets in one place. In fact, since cloud resources are considerably more 'volatile' compared to physical devices, keeping track of what assets you have is especially important.

Software

You might have 50 separate servers of the same make and model, but are they all running the latest software? And when are the licenses on that software set to expire? This is crucial information you need to know to maintain security and diagnose faults.

Applications

Another layer of software, applications are the things running on top of the server operating systems that actually do things. Your servers may all be up and running happily, but that doesn't help if the ecommerce application on those servers isn't working. You need to know what applications are on which devices (physical or otherwise) and what level of software they're using.

Traffic Flows

This one is a bit more advanced, but a good discovery tool can identify which of your devices are flow-capable and that opens the door for network traffic analysis or flow monitoring. Knowing what assets can support this makes network planning and optimization easier.

How it's done: Discovery Tools

Ok, so you're convinced you need to do a network discovery. How exactly do you do it? That may seem like a dumb question, but there are a ton of different discovery tools on the market from a wide variety of vendors. Which one(s) do you use?

The answer's going to depend upon a lot of factors, including the size and complexity of your network, the size of your budget and your specific requirements. A relatively simple tool may give you an adequate physical device inventory, but trying to map all your virtual and cloud resources will require something considerably more sophisticated. Let's take a quick look at how most discovery tools actually work.

The Basics of Device and Network Connectivity

When a device is plugged into the network, a Dynamic Host Configuration Protocol, (DHCP) server issues it an IP address. This address is unique on this network, which is not to say that there isn't a device anywhere in the world that doesn't have this same number assigned to it by its own network.

What actually is unique is the media access control (MAC) address. Every device's network adapter has a unique MAC address. So, while the IP address is determined by software, and can change, the MAC is determined by hardware, and can't be changed.

It's analogous to the difference between a password vs. a fingerprint as identification for a person. And just as multifactor identification is most secure for people, using both IP and MAC addresses gives the best view into a network.

A relatively simple tool may give you an adequate physical device inventory, but trying to map all your virtual and cloud resources will require something considerably more sophisticated.

Network Discovery, Network monitoring, and Asset Management

A network discovery tool uses several processes to investigate and understand the network of interest.

Simple Network Management Protocol (SNMP) is probably the most important. Most network devices are SNMP-enabled. It is the Internet standard protocol that provides monitoring for nodes or connection points, like servers, routers, bridges, and hubs, on an IP network. An effective discovery tool will let you run a discovery operation that will include an SNMP Smart Scan which allows a configurable depth of discovery based on a set of specified seed devices.

Windows Management Instrumentation (WMI) is the Microsoft implementation of Web-Based Enterprise Management (WBEM), which is an industry initiative to develop a standard technology for accessing management information in an enterprise environment. Between SNMP and WMI a discovery tool should be able to talk to about 95% of your network devices.

Ping is a familiar tool in network management, and automatically checks every device's status and whether it is online.

Address resolution protocol (ARP) uses SNMP to query device caches to build a database of MAC addresses. Knowing which devices are neighbors to others enables the discovery of the networks' topology.

A good tool's discovery process generates a complete inventory of all networked devices including device type, vendor, serial number, firmware and hardware rev, and the modules installed on the devices. Administrators often use this to fulfill inventory audits with automatically generated reports on the software installed on servers or network devices.

A good discover tool should also automatically assign devices roles (see below) and also identify dependencies. This dependency data can be used to suppress unnecessary alerts saving valuable troubleshooting time by minimizing false alerts.

Hardware Topology Discovery

Building network topology maps helps you gain a better understanding of your network. Effective tools use a combination of layer-2 and layer-3 topology to determine which devices are connected to which other devices. The layers come out of the classic Open Systems Interconnect (OSI) model used to both design and understand networks.

On the most basic level, layer 2 protocols discover data links and port-to-port connectivity, and work with MAC addresses. Layer 3 protocols assist in discovering neighboring devices, and work with IP addresses. For example, using Layer 3, you can query SNMP-enabled devices in order to build up a network map that includes device location, attributes, and role.

While layer-3 protocols are widely used, layer 2 protocols tend to be more proprietary, so the use of the Link Layer Discovery Protocol (LLDP) is essential to ensure that device information is available to neighboring devices from other manufacturers.

Using integrated layer-2 and layer-3 analysis gives full visibility into physical, logical, and virtual connectivity, so you can generate a topology map that accurately reflects network function.

Automatic Flow Source Discovery and Configuration

Using SNMP, a good discovery tool can determine what devices on the network are "flow capable" and automatically configure those devices to forward flow records with all appropriate timeouts and flow collector parameters configured. Effectively eliminating the need for "flow expertise" among staff who can now focus on interpreting the results and not configuring systems.

Virtual and Cloud Resources

Don't forget that your non-physical resources need to be included in your discovery! A good tool will automatically generate dynamic maps of your Hyper-V and VMware infrastructure, displaying hosts and guests, host/guest relationships, clusters, and real-time status. Ideally, this information should be displayed in context with your physical infrastructure so you can see dependencies.

Cloud-based services like AWS, Azure and Meraki's wireless controller are a bit trickier. A cloud-capable discovery tool should be able to access the relevant APIs for these cloud vendors and provide detailed information on all the cloud resources (servers, systems, APs, load balancers, etc.) you're using. Again, this information should be provided in context with the rest of your infrastructure in order to make it easier to visualize dependencies and facilitate troubleshooting.

Putting it All Together With a Discovery Tool

Now that you know how all this works, you can assess the available discovery tools out there in the market and pick the one that best suits your needs. Obviously we have our own opinion on the **best tool out there**, but your specific requirements and your budget are going to be the most important factors to consider. If all you want to know is what's actually connected to your network at this exact moment, there are a number of **free options** available that may be perfectly adequate. However, if you want dynamic network maps, virtual and cloud discovery and reporting or other capabilities, you may wish to consider a number of options. Fortunately, most vendors offer **free trials** so you can try before you buy and determine the best solution for your specific requirements. So, pick a tool and get ready to start discovering your network, right?

Not So Fast: Pre-Discovery Preparation

Planning yields better results and before your start a discovery, you need to do some basic preparation.

Credentials

While your discovery tool may be able to find everything physically connected to your network, it's not likely to be able to tell you much about that device if you don't have the credentials to that device. Having credentials can mean the difference between discovery telling you that there's a "Device" at a particular IP address or there's a "CiscoAirCt2504K9 Wireless Controller OID 1.3.6.1.4.1.9.1.1279" connected there. Every discovery tool should have the ability to enter a list of credentials before beginning a discovery.

Note that if you're trying to discover non-physical devices (you should!) you're going to need credentials for those as well. That gets a bit more interesting when it comes to cloud resources that are going to require API access. In most cases a cloud-capable discovery tool will require access to your cloud account in order to run a discovery on those devices. There should be an option to provide that information before you run the discovery scan.

Device Roles

While not essential, adding device roles can save you a lot of time going forward. You probably have more than one wireless AP, for example and it makes sense to categorize every one of those APs with a device role specific to its function. That way if you're trying to figure out which of your APs need a software update (for example) you can run a discovery only for that particular device role. It's also extremely useful for ongoing network monitoring and management as you can apply changes by role rather than for each individual device. If your discovery tool supports it, assign roles to like devices during discovery to make those devices easier to manage going forwards. Most discovery tools will include a library of common device types or even allow you to develop custom roles to your requirements.

Discovery Frequency

A discovery is a snapshot of the now, and as we mentioned earlier the network is constantly changing. Unless you have a very small and static network, you're going to want to run regular discoveries in order to track those changes and keep on top of things. The question then becomes how often to run a discovery? Again, that's going to depend upon your goals and the size of your network. A discovery can take a while and put a not-insignificant load on your network, so you probably don't want to run one every ten minutes. But you may want one daily. Or weekly, monthly or even hourly – it's all going to depend on what you are trying to find out and how much/how often you're willing to slow down your network. Most network discovery tools will include the ability to automatically run discoveries on a set schedule, so consider what's going to work for you and then put that schedule into effect once you know what a discovery is going to do to your network in terms of performance, response time, etc. Just bear in mind that frequent discoveries are NOT a replacement for continuous network monitoring. Which leads us to one clear conclusion.

Conclusion: Integrated Discovery & Monitoring with WhatsUp Gold

A network discovery is an important and essential first step, but it is only the first step in an ongoing process. Unless you just need a snapshot of what's connected right this second, the question that inevitably arises is what are you going to do with this information? Network discovery is usually an integral part of ongoing network monitoring and network management, and that's another subject entirely. However, it's not necessarily another solution entirely: all network monitoring tools should include a robust network discovery capability. So, when considering what tool you want to use to discover your network, think one step further and ask yourself what you want to do to all these devices once you've found them. One integrated solution that lets you discover, monitor and report on your network may just be the **killer app** you never realized you needed. That application is WhatsUp Gold.

WhatsUp Gold is a powerful network monitoring solution that lets you discover, map and monitor your network in minutes. It features powerful Layer 2/3 discovery which can be initiated from an IP Range Scan or SNMP Smart Scan of a core router's Bridge Table and generates a detailed map of the core, Windows, wireless and virtual infrastructures as well as cloud resources.

The discovery process also generates a complete inventory of all networked devices including device type, vendor, serial number, firmware and hardware rev, and the modules installed on the devices. WhatsUp Gold customers often use this feature to fulfill inventory audits with automatically generated reports on the software installed on servers or network devices.

WhatsUp Gold is a powerful network monitoring solution that lets you discover, map and monitor your network in minutes.

At the completion of the discovery process, WhatsUp Gold automatically assigns devices roles that specify what data to collect and remedial actions that are enabled. You can easily modify default device roles and sub-roles or create new ones with the Device Role Editor. The discovery process also identifies dependencies that are marked on the map as directional arrows. With a couple of mouse clicks, dependency data can be used to suppress unnecessary alerts saving valuable troubleshooting time by minimizing false alerts.

With WhatsUp Gold you can go beyond basic discovery to see connectivity and dependencies. WhatsUp Gold creates a detailed interactive map of your entire networked infrastructure which you can use to see network devices, servers, virtual machines, cloud and wireless environments in context. Click on any device to get immediate access to a wealth of related network monitoring settings and reports. See how everything is connected and get answers faster.

A completely unrestricted version of WhatsUp Gold that includes all features is available for a **free trial here**. However, if you are only planning to take advantage of WhatsUp Gold's discovery features then you may want to check out **WhatsUp Gold Starter Edition**. This is a version of WhatsUp Gold with a free one-year license that's been restricted to monitor only five devices. However, note that this only applies to monitoring; WhatsUp Gold Starter Edition will discover your entire network exactly the way the full version does. So why not give WhatsUp Gold a try for yourself? You have nothing to lose and you may just discover an incredibly useful tool along with what's connected to your network.

For Your Free Trial of WhatUp Gold Visit:
https://www.ipswitch.com/forms/free-trials/whatsup-gold

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, award-winning machine learning that enables cognitive capabilities to be a part of any application, the flexibility of a serverless cloud to deploy modern apps, business rules, web content management, plus leading data connectivity technology. Over 1,700 independent software vendors, 100,000 enterprise customers, and 2 million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.