Select your Preferred Language from the below list

English (US) ▼

NETWORK MANAGEMENT (/SUCCESSCENTER/S/TOPIC/0TO2J000...

Polling methods used by the Orion Platform

Differences between polling methods used by Orion

FIRST PUBLISHED DATE	LAST PUBLISHED DATE
10/24/2018 6:41 PM	5/13/2021 6:19 AM

OVERVIEW

This article discusses the following kinds of polling methods to collect performance information from monitored devices:

- ICMP (https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-choosing-your-polling-method-sw1223.htm#link2) (Internet Control Message Protocol)
- SNMP (https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-choosing-your-polling-method-sw1223.htm#link3) (Simple Network Management Protocol)
- WMI (https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-choosing-your-polling-method-sw1223.htm#link4) (Windows Management Instrumentation)
- Agents (https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-choosing-your-polling-method-sw1223.htm#link5)

ENVIRONMENT

NPM 12.3;NPM 12.4;NPM 12.5;NPM 2019.4;NPM 2020.2

CAUSE

RESOLUTION

ICMP - Internet Control Message Protocol

Orion Platform products use the Internet Control Message Protocol (ICMP) to poll for status using ping and echo requests of managed devices.

- If the device is operationally up, it returns a response time and record of any dropped packets. This information is used to monitor status and measure average response time and packet loss percentage for managed devices.
  Orion Platform products only use ICMP to poll devices for status, average response time, and packet loss percentage. Other information displayed in the Orion Web Console is obtained using SNMP requests.

For more information, please visit:

- INTERNET CONTROL MESSAGE PROTOCOL (https://datatracker.ietf.org/doc/html/rfc792) (© 2021 The

Related Articles

ⓘ

No related articles yet

Articles are related if tend to be read by the same people

We'd like to hear from you.

Please submit this form to provide feedback to the Success Center team.

☺ 😐 ☹

Internet Society, available at https://datatracker.ietf.org/doc/html/rfc792 (https://datatracker.ietf.org/doc/html/rfc792), obtained on May 13, 2021)

SNMP - Simple Network Management Protocol

For most network monitoring and management tasks, SolarWinds Orion products use SNMP.

- To monitor devices on your network, you must enable SNMP on all devices capable of SNMP communications. The steps to enable SNMP differ by device, so you may need to consult the documentation provided by your device vendor.
- If SNMPv2c is enabled on a device you want to monitor, by default, SNMPv2c is used to poll the device for performance information. If you only want to poll using SNMPv1, you must disable SNMPv2c on the device to be polled.

For more information about MIBs, please visit:

- Management Information Base (MIB) for the Simple Network Management Protocol (SNMP) (https://datatracker.ietf.org/doc/html/rfc3418) (© 2021 The Internet Society, available at https://datatracker.ietf.org/doc/html/rfc3418 (https://datatracker.ietf.org/doc/html/rfc3418), obtained on May 13, 2021)

For more information about SNMP, please visit:

- An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks (https://datatracker.ietf.org/doc/html/rfc3411) (© 2021 The Internet Society, available at https://datatracker.ietf.org/doc/html/rfc3411 (https://datatracker.ietf.org/doc/html/rfc3411), obtained on May 13, 2021)

WMI - Windows Management Instrumentation

Windows Management Instrumentation (WMI) is a proprietary technology used to poll performance and management information from Windows-based network devices, applications, and components. When used as an alternative to SNMP, WMI can provide much of the same monitoring and management data currently available with SNMP-based polling with the addition of Windows-specific communications and security features.

For more information about WMI, please visit:

- About WMI (https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi?redirectedfrom=MSDN) (© 2021 Microsoft, available at https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi?redirectedfrom=MSDN (https://docs.microsoft.com/en-us/windows/win32/wmisdk/about-wmi?redirectedfrom=MSDN), obtained on May 13, 2021)

Due to specific characteristics of WMI polling requests, polling a single WMI-enabled object uses approximately five times the resources required to poll the same or similar object with SNMP on the same polling frequency.

Agents

An agent is software that provides a communication channel between the Orion server and a Windows or Linux/Unix computer. Products install plugins on agents to collect the data that the agents send back. This can be beneficial in situations such as:

- Polling hosts and applications behind firewall NAT or proxies.

- Polling nodes and applications across multiple discrete networks that have overlapping IP address space.
- Secure, encrypted polling over a single port.
- Support for low bandwidth, high latency connections.
- Polling nodes across domains where no domain trusts have been established.
- Full, end-to-end encryption between the monitored host and the main polling engine.

You can monitor servers hosted by cloud-based services such as Amazon EC2, Rackspace, Microsoft Azure, and other Infrastructure as a Service (IaaS).

After the agent is deployed as per this documentation:

- Deploy agents to nodes (https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-deploying-an-agent-sw422.htm)

Communication between the Orion server and the agent occurs over a fixed. The list of required ports for agent-based monitoring is listed in this documentation:

- Agent port requirements (https://documentation.solarwinds.com/en/success_center/orionplatform/content/core-agent-requirements-sw476.htm#ports)

This communication is fully encrypted using 3072-bit TLS encryption. The agent protocol supports NAT traversal and passing through proxy servers that require authentication.

While changing the polling method from SNMP to WMI, make sure to List Resources and select intended objects/properties for polling.

Disclaimer: Please note, any content posted herein is provided as a suggestion or recommendation to you for your internal use. This is not part of the SolarWinds software or documentation that you purchased from SolarWinds, and the information set forth herein may come from third parties. Your organization should internally review and assess to what extent, if any, such custom scripts or recommendations will be incorporated into your environment. You elect to use third-party content at your own risk, and you will be solely responsible for the incorporation of the same if any.

(https://www.youtube.com/user/solarwindsinc)

(https://www.linkedin.com/company/solarwinds)

S.COM/RESOURCES)

EMAIL PREFERENCE CENTER (HTTPS://LAUNCH.SOLARWINDS.COM/SUBSCRIPTION-CENTER.HTML)

GDPR RESOURCE CENTER (HTTPS://WWW.SOLARWINDS.COM/GENERAL-DATA-PROTECTION-REGULATION-CORE-IT)

SOLARWINDS TRUST CENTER (HTTPS://WWW.SOLARWINDS.COM/TRUST-CENTER)

Legal Documents (https://www.solarwinds.com/legal/legal-documents) Privacy (https://www.solarwinds.com/legal/privacy) California Privacy Rights (https://www.solarwinds.com/legal/privacy#california-privacy-rights) Security Information (https://www.solarwinds.com/information-security) Documentation & Uninstall Information (https://support.solarwinds.com/SuccessCenter/s/?language=en_US) Sitemap (/sitemap.xml)

Monitor hardware health

This Orion Platform topic applies only to the following products:
NAM — NPM — NTA — SAM — SRM

Get immediate insight into hardware issues on your network. Monitoring hardware health on Cisco, Dell, F5, HP, and Juniper devices informs you which of these devices are in Up, Warning, Critical, or Unknown states.

1. When adding a device into the SolarWinds Orion database for monitoring, enable polling hardware health statistics.
2. Hardware health statistics are polled through SNMP, from a MIB tree on your devices. For Cisco devices, make sure that the correct MIB is selected.
3. Make sure the correct sensors are enabled for the nodes.

Click here to learn about hardware health monitoring requirements in SolarWinds SAM, which involves downloading third-party agent software for supported devices.

Monitored Hardware Sensors

Sensor	Up	Warning	Critical	Unknown
Fan status	🟢	🟢	⚠	⚪
Power Supply status	🟢	⚠	🔴	⚪
Temperature	🟢	⚠	🔴	⚪

Tips to Manage Your Network with Ease (Part 2) - Basics of Virtual Routing and Forwarding (VRF)

sandeep.subbaiyan over 8 years ago

In the previous blog, we discussed how VLANs can help to effectively manage workstations, security, and bandwidth allocation. Managing VLANs becomes much easier for network admins when network traffic, user access, and data transfers are isolated and routed separately. Sometimes, network admins face a scenario where devices from different VLANs are communicating with each other because their shared routers have multiple IP addresses of devices within each of them. In this scenario, it's important to take advantage of VLAN management techniques that allow you to isolate traffic, increase admin control, and share resources among users. One such technique that can be used to accomplish this type of management is called Virtual Routing and Forwarding (VFR). In this blog we'll discuss the basics of Virtual Routing and Forwarding, and how we can use this technology to easily manage Layer 3 devices in your network.

Introducing Virtual Routing and Forwarding (VRF)

VRF is a technology that allows multiple instances of a routing table to coexist within the same router at the same time. Without using multiple devices, VRF enables network engineers to increase the functionality of a single router by allowing the network paths to be segmented. This is done with virtualizing routing tables. When a packet enters a router, it is only forwarded using the routing table where the ingress and egress interfaces are associated with the same VRF.

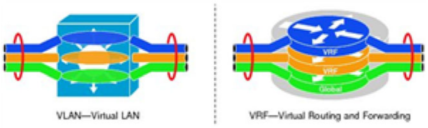


Figure 1 - VLAN vs VRF, Courtesy - Cisco®

Is it Easy to Manage Layer 3 devices with VRF?

Yes. In a VRF-configured router, each routing table will have a unique set of entries with their own forwarding detail, thus enabling a logical isolation of traffic. VRF requires a forwarding table with information on the next hop to push traffic through a specific device so that packets aren't transferred outside the VRF path. There's no need to encrypt or authenticate traffic since it's automatically segregated. Additionally, independent routing instances allow you to use the same IP addresses for different groups without conflict.

What are the Challenges in Managing a VRF enabled Network?

VRF reduces the number of the devices in your network by allowing you to share the same network resources. Usually, IT infrastructure service providers implement VRF-configured routers/switches in datacenters for multiple cascading routing instances, while supporting users. ISPs use VRF to create separate VPNs for their users, enabling scalable IP MPLS VPN services. But, if the number of VRF enabled routers increase, administrators managing huge network will find it difficult to isolate and manage each of those virtual routers independently. Without a strong framework, VRF support for your network might result in unfair scheduling of network resources and increased virtualization overhead. For service providers, VRF poses significant challenge in monitoring and analyzing user data for ingress and egress traffic that has different markers from each end of a route.

Managing VRF with Advanced Network Monitoring Tools

BORDER GATEWAY PROTOCOL (BGP) MONITORING WITH SOLARWINDS

by Raul Gonzalez | 20, Aug, 2017 | Blog Posts, Network Management, Useful Information

BGP (Border Gateway Protocol) is one of the most famous protocols that we have in networks. This protocol allows us to propagate network prefixes through the internet, and it is commonly used in big corporations and ISPs. Furthermore, it is one of the biggest sources of problems when we talk about reachability issues. This is not a surprise, as BGP is considered the most complex routing protocol.

In this blog post we are not going to talk about BGP itself (you have some links **here** and **here** to get a better understanding of the protocol itself), but about the basics of monitoring BGP within your company network, and more specifically, using **SolarWinds® Network Performance Monitor (NPM)** for this task.

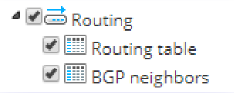
Based on my experience as SolarWinds engineer (currently), and network engineer (in the past), I would divide how to apply basic BGP monitoring into three sections:

- Peer Status
- Prefixes Received
- Routes

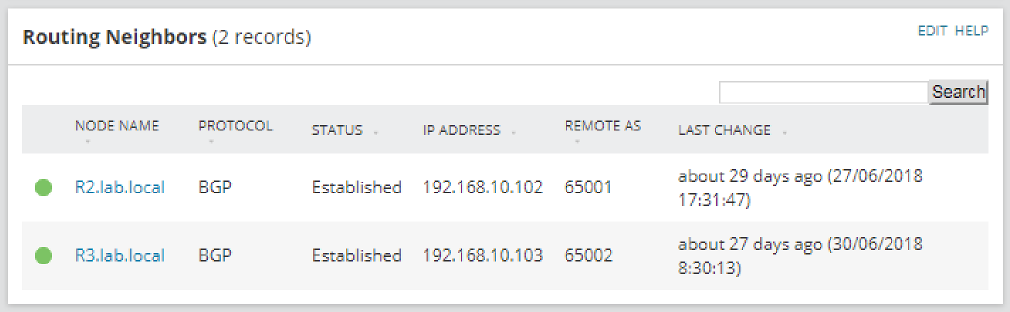
Peer Status

This is probably the most simple way to monitor BGP, and probably the most commonly used ways to do so. In order to exchange network prefixes with the rest of BGP peers, first of all, the router needs to establish a connection with them. If the status of the BGP neighbourship is not 'established', no exchange of routes will occur. There are two ways to get the status of the BGP peers: by polling some SNMP OIDs; or by receiving SNMP traps from the routers. Polling is the most important option, as this method actively asks for the status information, so we always know what the last polled state was. With SNMP Traps, we are waiting to be told of a change and on its own is not enough to know what the current state is, but is very good at telling us in real-time that neighbour changes have occurred.

SNMP Polling (Active Collection)
SolarWinds has the built-in capability to monitor the status of the BGP peers. Basically, SolarWinds gets the value of the OID 1.3.6.1.2.1.15.3.1.2, which shows the status of the BGP peers. To activate this feature, list resources on the router (Settings > Manage Nodes > *Select device* > List Resources) where you want to monitor BGP neighbours and tick the BGP neighbours option.



When this feature is enabled on a device, by default a view resource will appear on the node details page of the devices where this feature is enabled showing the status of the BGP peers, along with other information.



Routing Neighbors (2 records)

	NODE NAME	PROTOCOL	STATUS	IP ADDRESS	REMOTE AS	LAST CHANGE
●	R2.lab.local	BGP	Established	192.168.10.102	65001	about 29 days ago (27/06/2018 17:31:47)
●	R3.lab.local	BGP	Established	192.168.10.103	65002	about 27 days ago (30/06/2018 8:30:13)

SNMP Traps (Passive Collection)
SolarWinds monitors neighbour status every 5 minutes by default, which, for most of the situations, is enough. However, in some other situations, this frequency will not give us all the information at the speed we need. Using SNMP traps allows us to get the information as soon as it happens, and also can give us some extra information.

How to enable BGP traps on Cisco

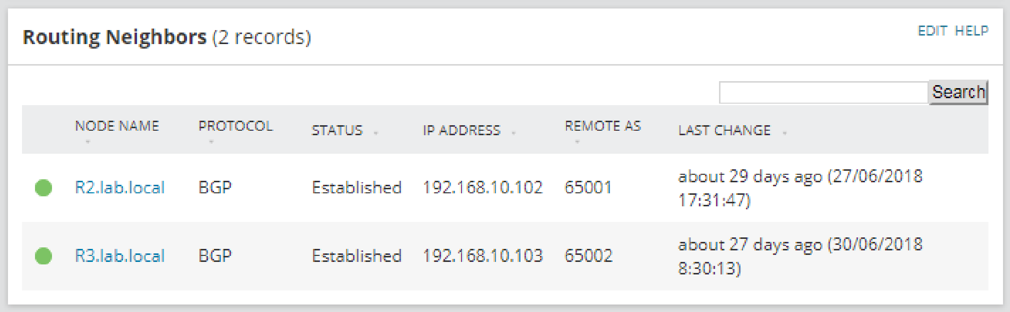
How to enable BGP traps on Juniper

There are two main SNMP traps that we want to receive when monitoring BGP:

- Backwards transition: this trap is issued when the BGP has a new status 'lower' than the last one. For example, if the peer goes from Established to Idle.
- Established State: this trap is issued when a BGP peer reaches established status
- State change: this trap will be issued every time there is a change in the peer state, either backwards or forward.

All these three SNMP traps are interesting, however, there can be the situation when some of them are sent for the same event. For example, if there is a backwards transition (established to idle) this will trigger the backwards transition trap (obviously), and the state change trap as well (there has been a change on the state of the neighborship). Or a similar situation with established state and state change.

For most of the devices compatible with BGP, there is only one specific OID that will be sent for Backwards transition, however, some vendors, such as Cisco or Juniper among others, have some other specific SNMP Trap that will be sent along with the default one. This happens because, even though there is a specific MIB branch under the standard branch (1.3.6.1.2.1) which contains event message support for the BGP protocol, which in theory will support all of the messages related to BGP events. However, there are some devices which have events not supported in this 'shared' MIB structure and therefore, have another BGP MIB branch under the private and vendor enterprises branch (1.3.6.1.4.1) allowing them to extend the event and polling structure beyond the shared standard branch.



Routing Neighbors (2 records)

	NODE NAME	PROTOCOL	STATUS	IP ADDRESS	REMOTE AS	LAST CHANGE
●	R2.lab.local	BGP	Established	192.168.10.102	65001	about 29 days ago (27/06/2018 17:31:47)
●	R3.lab.local	BGP	Established	192.168.10.103	65002	about 27 days ago (30/06/2018 8:30:13)

SNMP Traps (Passive Collection)
SolarWinds monitors neighbour status every 5 minutes by default, which, for most of the situations, is enough. However, in some other situations, this frequency will not give us all the information at the speed we need. Using SNMP traps allows us to get the information as soon as it happens, and also can give us some extra information.

How to enable BGP traps on Cisco

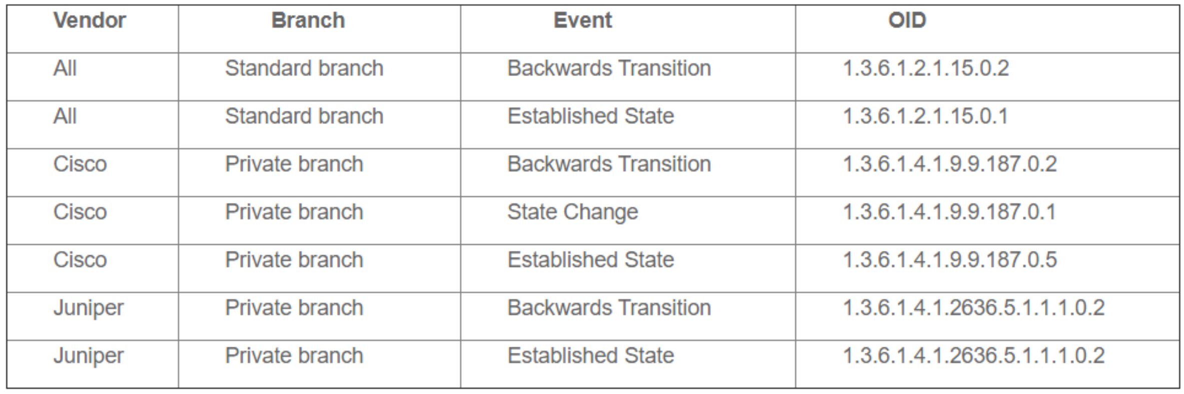
How to enable BGP traps on Juniper

There are two main SNMP traps that we want to receive when monitoring BGP:

- Backwards transition: this trap is issued when the BGP has a new status 'lower' than the last one. For example, if the peer goes from Established to Idle.
- Established State: this trap is issued when a BGP peer reaches established status
- State change: this trap will be issued every time there is a change in the peer state, either backwards or forward.

All these three SNMP traps are interesting, however, there can be the situation when some of them are sent for the same event. For example, if there is a backwards transition (established to idle) this will trigger the backwards transition trap (obviously), and the state change trap as well (there has been a change on the state of the neighborship). Or a similar situation with established state and state change.

For most of the devices compatible with BGP, there is only one specific OID that will be sent for Backwards transition, however, some vendors, such as Cisco or Juniper among others, have some other specific SNMP Trap that will be sent along with the default one. This happens because, even though there is a specific MIB branch under the standard branch (1.3.6.1.2.1) which contains event message support for the BGP protocol, which in theory will support all of the messages related to BGP events. However, there are some devices which have events not supported in this 'shared' MIB structure and therefore, have another BGP MIB branch under the private and vendor enterprises branch (1.3.6.1.4.1) allowing them to extend the event and polling structure beyond the shared standard branch.



Vendor	Branch	Event	OID
All	Standard branch	Backwards Transition	1.3.6.1.2.1.15.0.2
All	Standard branch	Established State	1.3.6.1.2.1.15.0.1
Cisco	Private branch	Backwards Transition	1.3.6.1.4.1.9.9.187.0.2
Cisco	Private branch	State Change	1.3.6.1.4.1.9.9.187.0.1
Cisco	Private branch	Established State	1.3.6.1.4.1.9.9.187.0.5
Juniper	Private branch	Backwards Transition	1.3.6.1.4.1.2636.5.1.1.1.0.2
Juniper	Private branch	Established State	1.3.6.1.4.1.2636.5.1.1.1.0.2

NOTE: there are other SNMP traps available in some of the vendors, however, the ones above are the most important ones.

We have mentioned before that the SNMP Traps from the private branch normally extend the information available, compared to the traps from the standard branch. Let's have a closer look. For example, these are the backwards transition traps that a Cisco device will send when these events occur.

Standard branch SNMP Trap:

```
TRAP:          CES-BGP-DEFAULTS-MIB:bgpTraps.0.2 :
Last Error:    bgpPeerLastError.192.168.10.101 = BAA=,
Current Status: bgpPeerState.192.168.10.101 = idle(1),
Device Up Time: sysUpTime = 14 days 16 hours 6 minutes 34.39 seconds,
Device IP:      experimental.1057.1.0 = 192.168.10.103,
Trap Origin:    snmpTrapEnterprise = CES-BGP-DEFAULTS-MIB:bgpTraps
```

Cisco branch SNMP Trap:

```
TRAP:           CISCO-BGP4-MIB:cbgpBackwardTransition :
Last Error:     bgpPeerLastError.192.168.10.101 = BAA=,
Current Status: bgpPeerState.192.168.10.101 = idle(1),
Last Status:    cbgpPeerPrevState.192.168.10.101 = established(6),
Reason:         cbgpPeerLastErrorTxt.192.168.10.101 = hold time expired,
Device Up Time: sysUpTime = 14 days 16 hours 6 minutes 34.39 seconds,
Device IP:      experimental.1057.1.0 = 192.168.10.103,
Trap Origin:    snmpTrapEnterprise = CISCO-BGP4-MIB:ciscoBgp4MIB
```

As you may have noticed, the Cisco branch trap gives you a little bit more information, in this case, previous status and last error.

It is important to review and confirm which branch your device generates SNMP Traps for (Standard or Private) and if both utilise the Private branch as this is likely to have more information within it than the Standard branch message. The following link provides information on creating alerts within SolarWinds Orion:

How to create an alert for Traps in SolarWinds

Prefixes Received

When peering with ISPs, one of the common issues that we might have stopped receiving prefixes from the ISP router. This can be a big problem because it might be unnoticed if we only monitor the status of the BGP neighbourship.

It is also a problem when the ISP router advertises too many prefixes, as our router might start to receive more routes than the router memory can take. If this same router is peering internally with other routers that also perform critical routing functions within the network, this overhead could lead to a bad outcome for network function.

The management branch of the BGP MIB file does not contain an OID that allows us to monitor this metric, therefore we have to rely on the private branch of each vendor. This means that some vendors may give us this information and some others may not, so a review is always necessary to determine if and what the OID will be.

On the table below you will find the main metrics that we recommend to monitor via SNMP active polling.

Metric	Description
Accepted Prefixes	Allows us to know how many prefixes have been received from the BGP peer. If the number of prefixes is 0 for a long time (2 hours) this might indicate a problem with the peer.
Prefix Threshold	During the configuration of BGP on the Cisco router, we have the option to define a threshold (in %). Once the threshold is reached, the router will send a trap advertising the amount of prefixes received from a peer has exceeded the threshold. We can monitor this value in SolarWinds in order to create our own automation processes.
Maximum Prefixes Allowed	This gives us the total amount of prefixes allowed on this neighbour. One of the actions, when the limit is reached, is to bring down the BGP peer connection.
Advertised Prefixes	This monitors the prefixes we are advertising. This is important to monitor in order to know whether we are advertising too many prefixes or not enough.

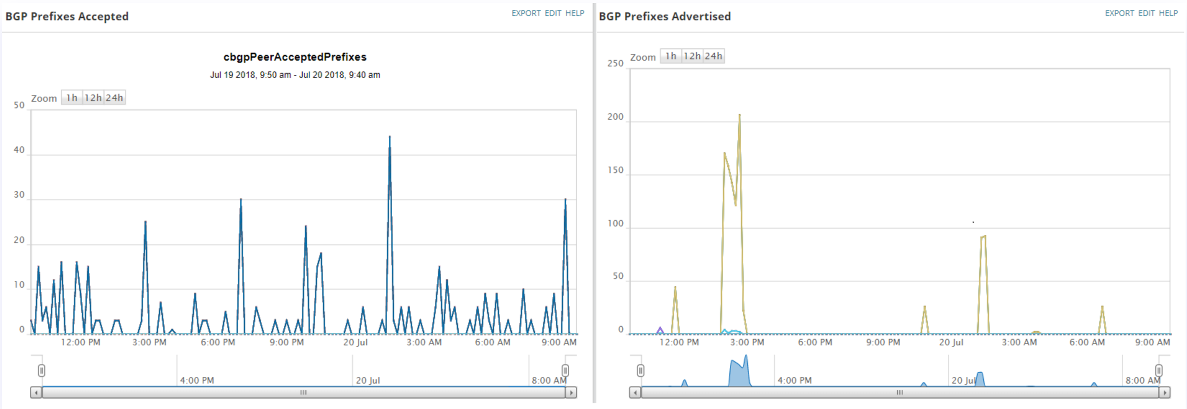
Cisco is one of the vendors that will give us the most of the metrics we need. Depending on how BGP is configured in the router, the OIDs might differ. This depends on where you are using **basic BGP** or with **address families**.

If BGP is configured without address families (basic BGP), then the OIDS are the following:

Accepted Prefixes	1.3.6.1.4.1.9.9.187.1.2.1.1.1
Maximum Prefixes Allowed	1.3.6.1.4.1.9.9.187.1.2.1.1.3
Advertised Prefixes	1.3.6.1.4.1.9.9.187.1.2.1.1.4

Otherwise, if BGP has been configured with address families, then the OIDs are the following:

Accepted Prefixes	1.3.6.1.4.1.9.9.187.1.2.4.1.1
Maximum Prefixes Allowed	1.3.6.1.4.1.9.9.187.1.2.4.1.3
Prefix Threshold	1.3.6.1.4.1.9.9.187.1.2.4.1.4
Advertised Prefixes	1.3.6.1.4.1.9.9.187.1.2.4.1.6



In the above screenshots, you can see these values output in Orion in chart form, as this allows us to see the level of activity within the protocol the device is seeing.

Example of basic configuration for Cisco devices:

```
neighbor 192.168.10.101 maximum-prefix 500 80
```

- neighbor IP address is 192.168.10.101
- maximum number of prefixes allowed are 500
- when the number of prefixes received is over 80% of the maximum (500×80% = 400)

To demonstrate the differences between vendors and how available data can be different, here we are using Juniper routers and only have the options to monitor received and advertised prefixes.

Accepted Prefixes	1.3.6.1.4.1.2636.5.1.1.2.6.2.1.7
Advertised Prefixes	1.3.6.1.4.1.2636.5.1.1.2.6.2.1.10

These are the Universal Device Pollers (UnDPs) that can be imported into SolarWinds.

How to import UnDP

Routes

On this particular topic, there are two main areas that we should monitor: flapping routes, and AS path.

Flapping Routes

Monitoring flapping routes are not exclusive to BGP, we should monitor flapping routes for each single routing protocol such as OSPF or EIGRP as well. The good news here is that SolarWinds can monitor this out of the box, just make sure you are monitoring the routing table when you list resources on a router (see List Resources section above).

Custom Poller: Universal Device Poller - Juniper BGP

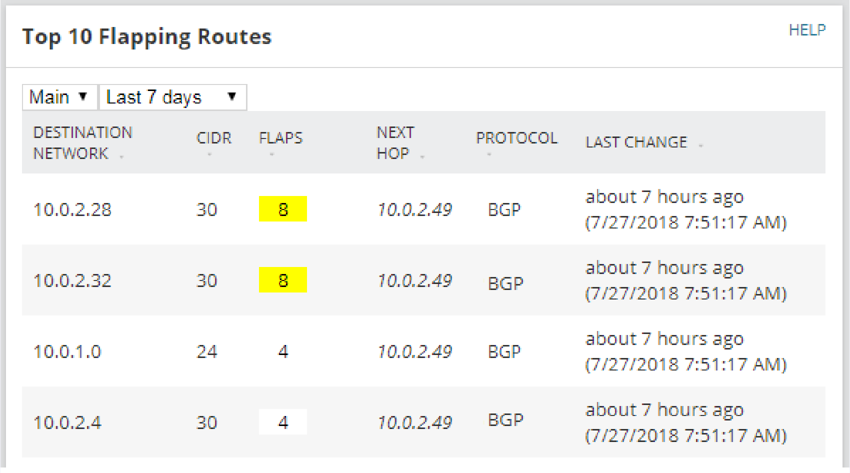
Download Our Free Custom Poller

Custom Poller: Universal Device Poller - Cisco BGP (Basic)

Download Our Free Custom Poller

Custom Poller: Universal Device Poller - Cisco BGP (AF)

Download Our Free Custom Poller



Top 10 Flapping Routes

DESTINATION NETWORK	CIDR	FLAPS	NEXT HOP	PROTOCOL	LAST CHANGE
10.0.2.28	30	8	*10.0.2.49*	BGP	about 7 hours ago (7/27/2018 7:51:17 AM)
10.0.2.32	30	8	*10.0.2.49*	BGP	about 7 hours ago (7/27/2018 7:51:17 AM)
10.0.1.0	24	4	*10.0.2.49*	BGP	about 7 hours ago (7/27/2018 7:51:17 AM)
10.0.2.4	30	4	*10.0.2.49*	BGP	about 7 hours ago (7/27/2018 7:51:17 AM)

AS Path

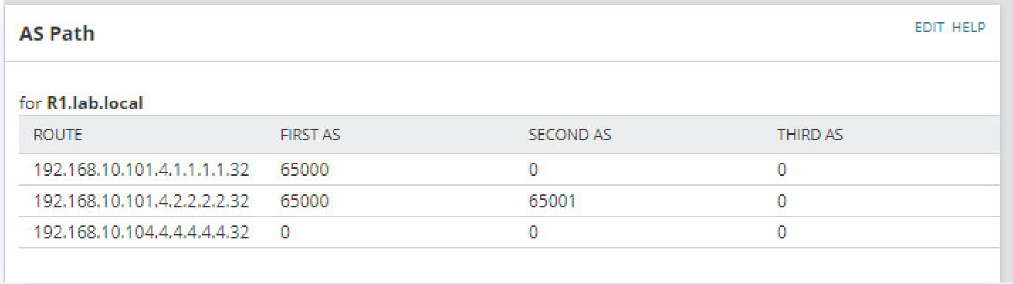
The other important metric here is the AS path. In order to know the route that the packets are following to reach a particular subnet, BGP uses the property AS path, determining the **Autonomous Systems** that the packet will go through to reach the destination. It is important to monitor the existing AS paths in order to detect any type of DDoS attack, hijacking as these are methods used to exploit the BGP protocol or merely to know the route our traffic will take.

In Cisco, we can monitor the AS path using the following OID 1.3.6.1.4.1.9.9.187.1.1.1.1.8 and for Juniper, it is 1.3.6.1.4.1.2636.5.1.1.3.5.1.4

If you are testing this metric with Cisco, it is necessary to convert the default HEX format of the output into a format which is more human readable. This can be performed using the SQL query within the Orion widget; Custom Table.

Custom Script: SQL Query AS Path

Download Our Free Custom Script



AS Path

for **R1.lab.local**

ROUTE	FIRST AS	SECOND AS	THIRD AS
192.168.10.101.4.1.1.1.1.32	65000	0	0
192.168.10.101.4.2.2.2.2.32	65000	65001	0
192.168.10.104.4.4.4.4.4.32	0	0	0

NOTE: this SQL script has been only tested for 16-bit AS numbers, not for 32-bit AS numbers. It also only includes up to the third AS, however, it could be edited to work with 32-bit AS numbers and more AS in the path.

And that's all I wanted to share with you guys and gals. I hope this has been informative for you, and don't hesitate to contact me with any question or ideas that you may have regarding the use of SolarWinds.

Raul Gonzalez

Technical Manager

Raul Gonzalez is the Technical Manager at Prosperon Networks. As a Senior SolarWinds and NetBrain Engineer for over seven years, Raul has helped hundreds of customers meet their IT monitoring needs with SolarWinds and NetBrain Solutions.

Custom Poller: Universal Device Poller - Juniper BGP

Download Now

EIGRP Neighborship Requirements and Conditions

This tutorial explains EIGRP neighborship requirements (Active hello packets, AS number and K-values) and EIGRP neighbor discovery process in detail with examples including essential EIGRP neighborship configuration values (EIGRP passive interface, EIGRP Adjacency and EIGRP AS Numbers).

Essential configuration values

EIGRP Router doesn't trust anyone blindly. It checks following configuration values to insure that requesting router is eligible to become his neighbor or not.

Active Hello packets

AS Number

K-Values

This tutorial is second part of our article "EIGRP Routing Protocol Explained with examples". You can read other parts of this article here.

EIGRP Tutorial – Basic concept explained

This is the first part of article. In this part we explained basic concepts of EIGRP such as Features and characteristics of EIGRP, Neighbor Table, Topology Table, Routing Table, Protocol Dependent Modules, Metric, RTP, DUAL, Autonomous System and Administrative Distance.

EIGRP Metric K Values Explained with Examples

This is the third part of this article. EIGRP uses composite metric calculation formula to calculate the best path. Bandwidth, reliability, delay, load and MTU are the components of formula. In this part we will explain these components with formula in easy language with examples.

EIGRP Configuration Step by Step Guide

This is the last part of this article. IGRP is a classless protocol wearing classful mask. Unless we configure it properly it acts like classful protocol. In this part we will learn how to configure EIGRP routing protocol properly. At the end of this article we will include most commonly used EIGRP commands with descriptions.

Active Hello packets

EIGRP uses hello packets to maintain the neighborship between routers. It uses them for neighbor discovery and recovery process. Hello packets are periodically sent from all active interfaces.

By default when we enable EIGRP routing, all interfaces (that meet network command criteria) become participate of it. EIGRP allows us to exclude any interface from it.

Passive interface

passive-interface command is used to exclude an interface from EIGRP. Passive interface command is a double edged sword. If used carelessly, it could bring entire network down. Once you marked an interface as passive, EIGRP will never send a hello packet from it. And we know that hello packet is first condition of EIGRP neighborship. In this situation EIGRP neighborship will not take place on this interface.

routers will become neighbors only when they see each other's hello packets on a common network.

EIGRP sends hello packets from all active interfaces in hello interval. Hello interval is a time duration that EIGRP takes between two hello packets. Default hello interval for high bandwidth link is 5 seconds. For low bandwidth links, hello interval is 60 seconds.

- Ethernet, Token Ring, Point to Point serial links, HDLC leased lines are the examples of high bandwidth link.
- Multipoint circuits, Multipoint ATM, Multipoint Frame Relay, ISDN and BRIs are the example of low bandwidth links.

An EIGRP router must receive hello packets continuously from its neighbors. If it does not receive hello packets from any neighbor in hold down time, it will mark that neighbor as dead.

Hold time is the time duration that an EIGRP router waits before marking a router dead without receiving a hello packet from it. Typically hold down time is three times of hello interval. So for high bandwidth link it would be 15 seconds and 180 seconds for slow bandwidth link. We can adjust hold down time with *ip hold-time eigrp* command.

EIGRP uses multicast and unicast for hello packets delivery. It uses 224.0.0.10 IP address for multicast. Since hello packets do not have any important routing information, they need not be acknowledged.

Basically Hello packets perform two essential functions of EIGRP.

- Find another EIGRP router in network and help in building neighborship.
- Once neighborship is built, check continuously whether neighbor is alive or not.

Adjacency

Neighborship is referred as adjacency in EIGRP. So when you see New Adjacency in log, take it for new neighborship. It indicates that a new neighbor is found and neighborship with it has been established.

AS Number

An AS is a group of networks running under a single administrative control. This could be our company or a branch of company. Just like Subnetting AS is also used to break a large network in smaller networks.

AS creates a boundary for routing protocol which allow us to control how far routing information should be propagated. Beside this we can also filter the routing information before sharing it with other AS systems. These features enhance security and scalability of overall network.

Basically AS concept was developed for large networks. Routing protocols which were developed for small networks such as RIP do not understand the concept of AS systems.

There are two types of routing protocols IGP and EGP.

- **IGP** (Interior Gateway Protocol) is a routing protocol that runs in a single AS such as RIP, IGRP, EIGRP, OSPF and IS-IS.
- **EGP** (Exterior Gateway Protocol) is a routing protocol that performs routing between different AS systems. Nowadays only BGP (Border Gateway Protocol) is an active EGP protocol.

To keep distinguish between different autonomous systems, AS numbers are used. An AS number start from 1 and goes up to 65535. Same as IP addresses, AS numbers are divided in two types; Private and public.

- **Public AS Numbers**: - We only need to use public numbers if we connect our AS with Internet backbone through the BGP routes. IANA (Numbers Authority) controls the public AS numbers.
- **Private AS Numbers**: - Private AS numbers are used to break our internal network into the smaller networks.

EIGRP routers that belong to different ASs don't become neighbors therefore they don't share any routing information.

So our second condition that needs to be fulfilled in order to become EIGRP neighbor is the same AS number. Two routers will become neighbors only when they see same AS number in each other's hello packets.

K Values

EIGRP may use five metric components to select the best route for routing table. These are Bandwidth, Load, Delay, Reliability and MTU. By default EIGRP uses only two components; Bandwidth and delay. With K-Values we can control which components should be used in route metric calculation. For five metric components we have five K values.

K Values	Metric components

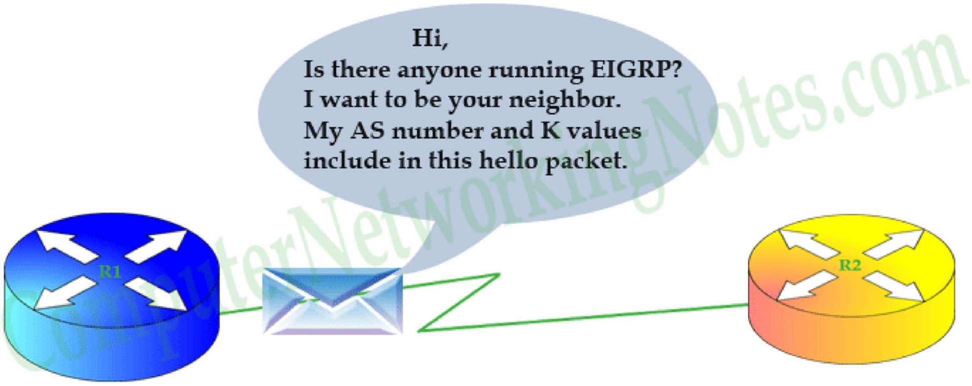
K2	Load
K3	Delay
K4	Reliability
K5	MTU

Two routers must use same K Values in order to become the EIGPR neighbor. For example if one router is using three K- Values (K1, K2 and K3) while second router is using default K values (K1 and K3) then these two routers will never become neighbor.

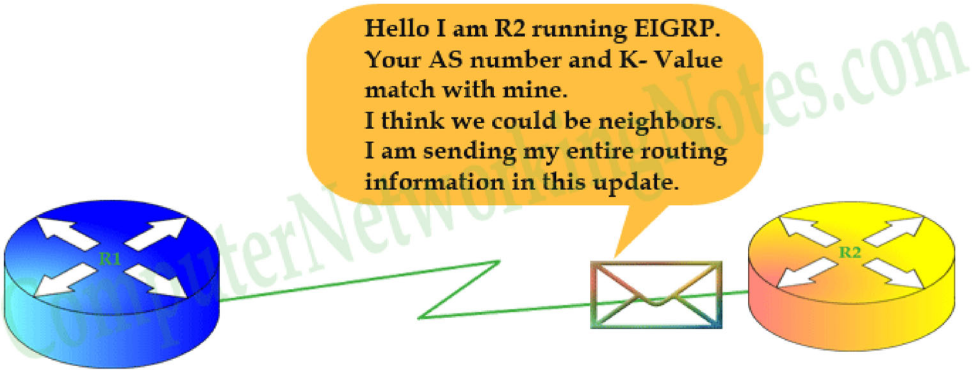
In order to become EIGRP neighbor two routers must use same K values.

EIGRP Neighbor Discovery process

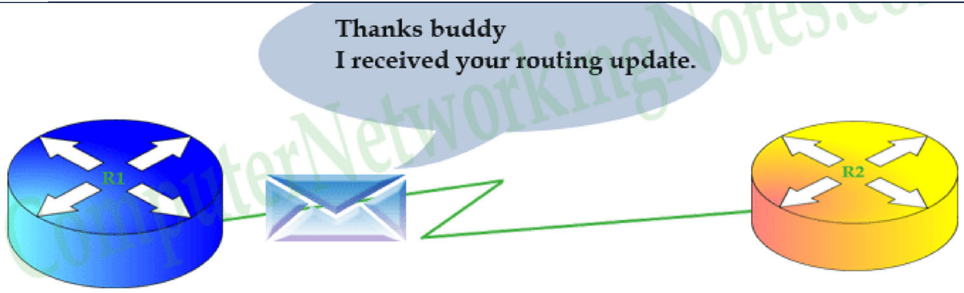
Step 1:- First router R1 sends a hello packet from all active interfaces. This packet contains essential configuration values which are required to be a neighbor.


Hi,
Is there anyone running EIGRP?
I want to be your neighbor.
My AS number and K values
include in this hello packet.
R1
R2

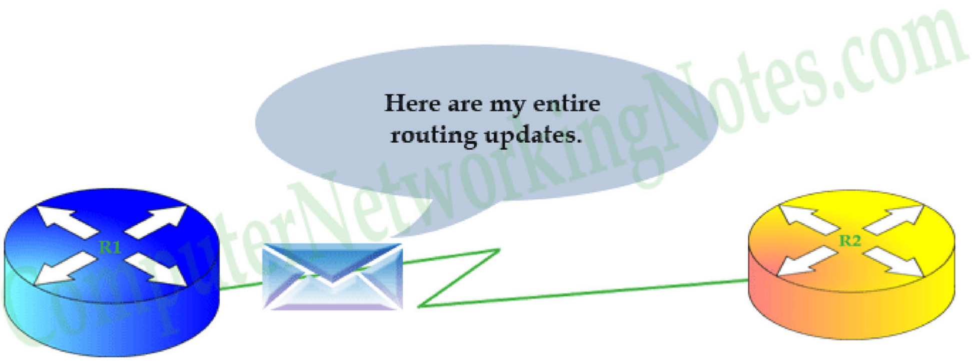
Step 2:- Receiving router R2 will compare these values with its own configuration values. If both necessary values match (AS number and K-values), it will reply with a routing update. This update includes all routes information from its routing table excluding one route. The route which it learned from the same interface that bring hello packet to it. This mechanism is known as split horizon. It states that if a router receives an update for route on any interface, it will not propagate same route information back to the sender router on same port. Split horizon is used to avoid routing loops.


Hello I am R2 running EIGRP.
Your AS number and K- Value
match with mine.
I think we could be neighbors.
I am sending my entire routing
information in this update.
R1
R2

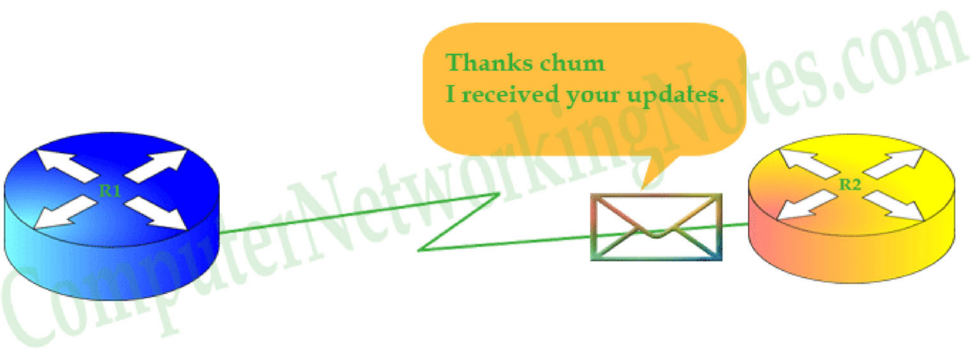
Step 3:- First router will receive R2's routing update and sends an acknowledgement message back to R2.



Step 4:- R1 will sync its EIGRP topology table with routing information that it received in routing update. It will also send a routing update containing all route information from its routing topology to R2.



Step 5:- R2 will respond with an acknowledgement message. It will also sync its EIGRP topology table with routing information that it received in routing update.



At this point, the two routers have becomes neighbor. Now they will maintain this neighborship with ongoing hello packets. If they see any change in network, they will update each other with partial updates.

EIGRP Network Discovery process step 6

Partial update contains information only about the recent change.

That's all for this part. In this part we explained how two routers become EIGRP neighbors. In next part we will see how EIGRP routers select the route for routing table.

By ComputerNetworkingNotes Updated on 2018-08-06 00:41:51 IST

EnergyWise devices

This topic explores how you can use Network Configuration Manager in conjunction with Network Performance Monitor to enable and manage your Cisco EnergyWise devices.

What is EnergyWise?

EnergyWise is Cisco's response to the call to cut energy costs, address environmental concerns, and adhere to government directives around green technologies. By purchasing EnergyWise capable devices and enabling their energy-saving features, you can retain business critical systems in a fully powered state while allowing less critical power over ethernet (PoE) devices to power down or drop into standby during off hours.

EnergyWise gives you the ability to control your energy cost. NCM gives you the ability to remotely apply recurrence policies and schedule power usage, helping you use less power. And, SolarWinds NPM allows you to monitor your energy use and power levels. SolarWinds perfectly partners with Cisco and the EnergyWise technologies to help you save more and monitor your savings.

Manage and enable EnergyWise nodes

Cisco devices that support the EnergyWise technology can be enabled and their EnergyWise settings managed through the NCM integration with NPM.

Before completing the following procedure, EnergyWise nodes must be managed in both NCM and SolarWinds NPM. You must discover and add nodes to the Orion Platform, and then manage the nodes with NCM.

1. Click Settings > All Settings.
2. Under Node & Group Management, click Manage Nodes.
3. Select the Cisco node for which you want EnergyWise enabled, and click More Actions > Manage EnergyWise.
4. Click Enable EnergyWise on these nodes.
5. Specify the values on the Manage EnergyWise Node page.
6. Click Execute Config Actions.

Manage Power over Ethernet ports

Power over Ethernet (PoE) devices are connected to your devices on an interface and are managed at the interface level. Before completing the following procedure, you must have added your EnergyWise capable nodes to both NCM and NPM.

1. Click Settings > All Settings.
2. Under Node & Group Management, click Manage Nodes.
3. Expand the Cisco node containing the interface you want to configure.
4. Select the interface you want to enable EnergyWise, and click More Actions > Manage EnergyWise.
5. Click Enable EnergyWise on these nodes.
6. Specify the values on the Manage EnergyWise Interface page.
7. Click Execute Config Actions.

Networks are expanding exponentially, and manual device discovery and mapping is becoming increasingly impossible. With technologies like virtualization, remote access, mobile and cloud computing dynamically altering networks, an automated layer 2/3 Discovery tool holds the key to **network device discovery** and mapping difficulties.

By discovering and mapping your networks in real-time, a layer 2/3 discovery tool ensures your knowledge of network topology, device attributes and changes remain up-to-date.

Tools like **WhatsUp Gold** function across both Layer 2 and Layer 3 to create dynamic topological maps of your network.

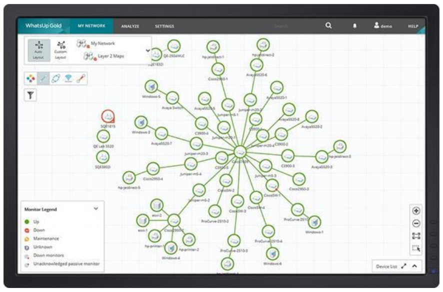
Layer 3 Discovery

Layer 3 discovery techniques include: SNMP-based discovery (where SNMP-enabled devices exchange device information); Active probes approach (where target probe executables are sent out to query the network), and route analytics (using protocols like EIRGP and OSPF).

While Layer 3 discovery lets administrators visualize the network, a drilled-down view of the network can be obtained through Link Layer Discovery, which shows the interconnections in each switch, down to individual port connections, subnet, spanning tree information and VLAN details.

Layer 2 Discovery

Layer 2 discovery protocols, including the proprietary CDP, and JDP, and the vendor-neutral **LLDP**, automatically discover, deploy and monitor switches, hubs, bridge ports and VLANs. Problem detection and root cause analytics now become infinitely easier – Layer 3 discovery locates and identifies the malfunctioning network device, while Layer 2 details show the switch port/interface the problem has originated from.



WhatsUp Gold Automated Layer 2/3 Discovery

WhatsUp Gold leverages SNMP Smart Scan, IP Range Scan, WMI, ICMP, SSH, VMware Scan, ARP Cache Discovery and Ping Sweep to automatically build integrated Layer 2 and Layer 3 maps. By correlating Layer 3 discoveries with Layer 2 details, WhatsUp Gold offers a complete and granular view of the network.

Monitor Everything in Your Network