



Network Management

for IP-based Networks

Core and extended Functionalities of the Network Management System

Content

BICS NETWORK MANAGEMENT FOR IP-BASED NETWORKS	3
1. BICS NETWORK MANAGEMENT FEATURES	4
2. CORE FUNCTIONALITIES OF THE NETWORK MANAGEMENT SYSTEM	5
2.1 Discovery	5
2.2 Topology	5
2.3 Network Monitoring	6
2.4 Device Details	7
2.5 Event- and Alarm Console	7
2.6 VLAN-Management	8
2.7 Configuration Management	8
2.8 Syslog Analyzer	9
3. EXTENDED FUNCTIONALITIES OF THE NETWORK MANAGEMENT SYSTEM	10
3.1 Flow Reporting	10
3.2 Advanced Automation	10

Purpose of this document

This document is a high-level introduction to network management in the Infraray Business Infrastructure Control Solution (BICS) for office and industrial networks.

It helps future BICS customers to understand the approach, features and integration possibilities of the BICS network management system.

This document is not a tutorial and does not replace the technical documentation. We recommend contacting Infraray to organize a live demo. Infraray will also be happy to answer any questions about the product.

BICS Network Management for IP-based Networks

For explanation, this document describes the Infraray Business Infrastructure Control Solution (BICS) as "BICS for Network Management", in short "BICS. Please note that Infraray BICS is a comprehensive platform that may include additional modules in addition to network management functionality, such as asset management, port security and a number of other important functions for corporate networks.

View, monitor and control your switches, routers, servers and other network devices.

Infraray BICS monitors and manages heterogeneous networks from a central location. The ability to operate BICS redundantly in a multi-instance network and with a large number of clients predestines the system for use in very large network environments with tens of thousands of switches and routers.

Various discovery processes are used to identify all network devices and determine the end devices connected to them.

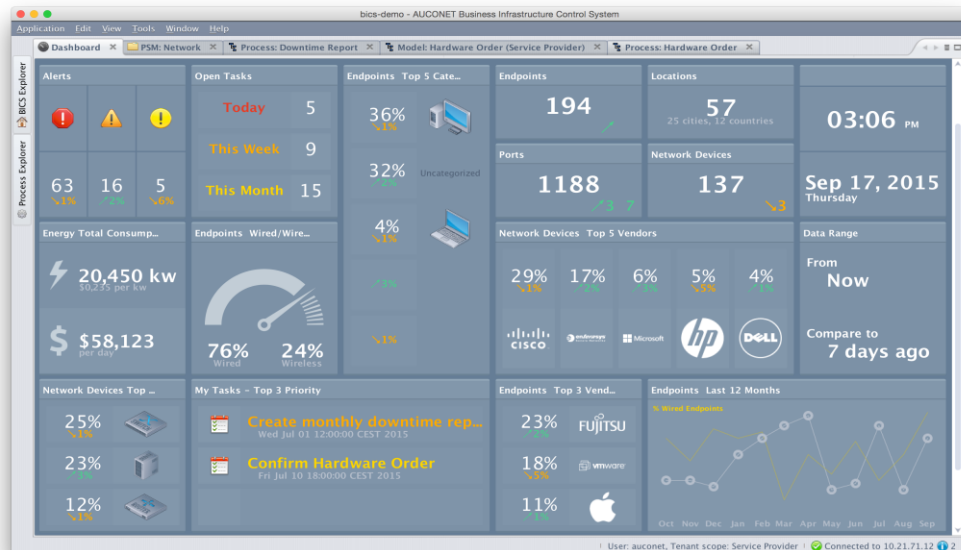
Due to the extensive BICS device library, the parameters necessary for smooth operation can be monitored for each network device from all manufacturers.

Also important for efficient and trouble-free network operation is the ability of BICS to permanently control the connections (links) between the network devices and their status or load.

1. BICS Network Management Features

Manufacturer-independent management system

- Supported management protocols: SNMP v1/2c/3, SSH, Telnet, HTTP/HTTPS
- Central alarm and event console with configurable dashboards
- Topological mapping of the network according to different criteria (locations, subnets, device types,...)



- Monitoring of the devices and their connections
- VLAN management across devices and manufacturers
- configuration management
- Intuitive user interface for central monitoring. Graphical representation of the entire network infrastructure with the possibility of drill-down from the high-level dashboard to the end device.
- Ability to analyze traffic across the network
- Seamless integration with other BICS modules:
 - Port Security Manager

- Asset management
- System Management (aka Asdis)
- Interfaces for integration with existing systems (e.g. CA Spectrum)
-

2. Core functionalities of the network management system

2.1 Discovery

The network management system uses various discovery methods to identify all devices involved in network traffic and display their connections to each other:

- Network Device Discovery
- Link Layer Discovery
- Endpoint Discovery

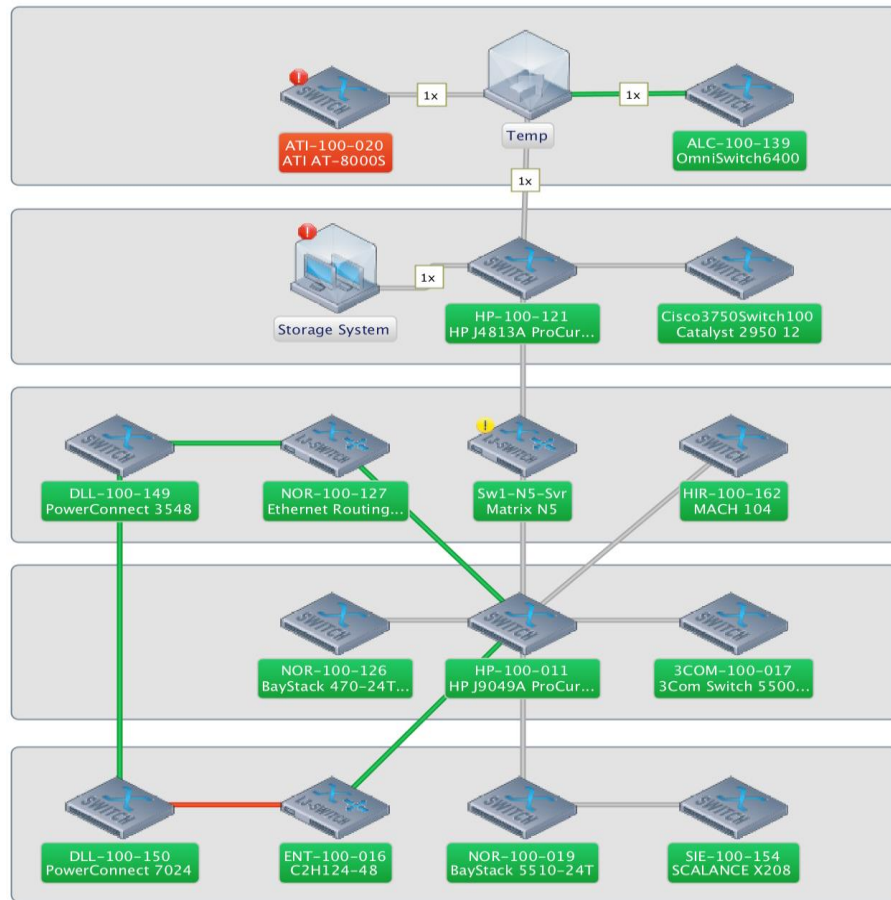
2.2 Topology

From the results of Network Device Discovery and Link Layer Discovery, BICS generates a topology of the entire network. The automatically generated graphic representation can be changed and adapted by the user according to his own needs. An integrated drawing program allows the addition of graphic elements and (background) images.

Each network device is represented by a significant icon. The label of the icon shows the manufacturer, the device type and the name of the device. The color of the label indicates the current alarm status.

Navigation between the various devices and functions is carried out via context menus, some of which can be adapted. Special hover menus allow quick access to the most important functions of the network devices.

The connections between the devices are represented by lines. The color of the lines indicates the current alarm status of the connection. Tooltips display additional information (e.g. ports involved and connection properties).



By using a hierarchical folder structure, the network topology can be adapted to local conditions and clearly arranged.

2.3 Network monitoring

The BICS Network Management System supports a variety of monitoring options

(i) Device-specific monitoring, e.g:

Availability, CPU utilization, file system utilization, temperature, power supply,...

(ii) Port-specific monitoring, such as

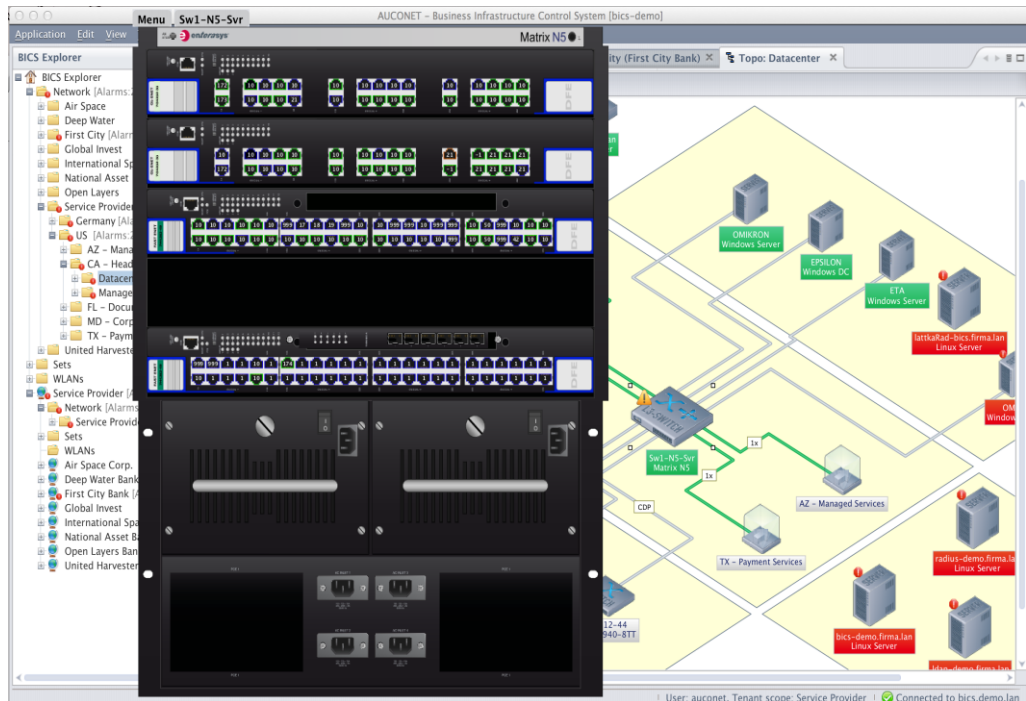
Bandwidth utilization, transmission errors,...

(iii) Connection-specific monitoring, such as

Availability, redundancy, ...

2.4 Device details

Detailed information about the current status of a network device:

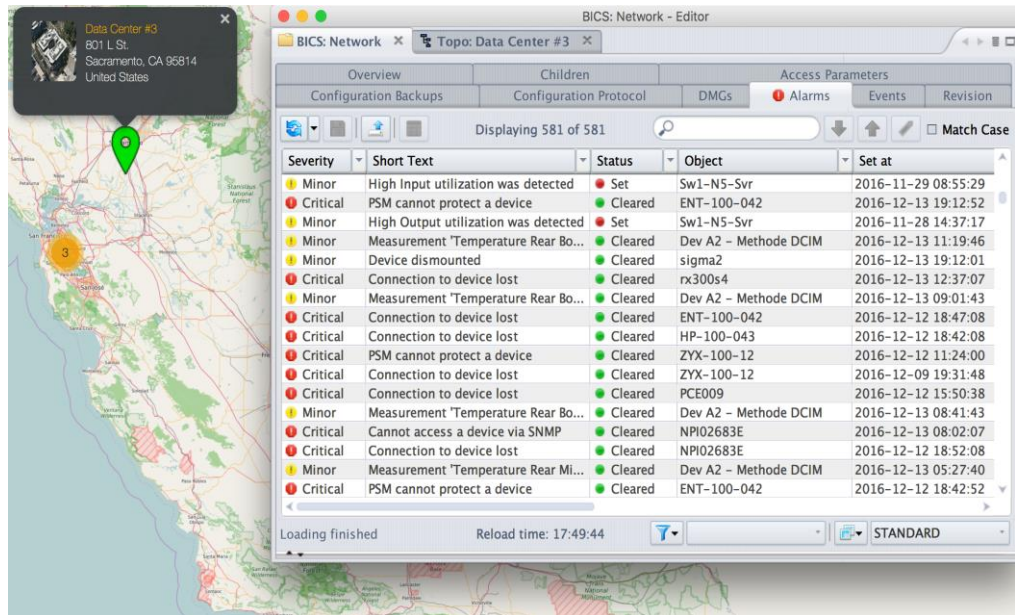


- Special, device type-specific views of individual device parameters.
- Photorealistic display of the network device with active drill-down options for displaying port information (bandwidth utilization, transmission errors, connected end devices, VLAN information,...) and equipping of optional components (e.g. HDDs, power supplies, plug-in modules)

2.5 Event- and alarm console

All relevant network monitoring events are summarized and displayed in a central alarm and event console. BICS comes with a large number of predefined events and alarms as delivered. If required, the user can add his own events and alarms or adapt existing ones or define further evaluation rules in order to create finely granulated escalation scenarios.

There are various filter options for displaying alarms, so that depending on the task area and authorization, the user only sees the alarms relevant to him.



Alarms and events can be forwarded to external systems (e.g. via email, trap, syslog message). Various rules can be defined for this, depending on the alarm type, the device and the time of the alarm, among other things.

2.6 VLAN-Management

VLAN management allows the authorized user to create VLANs on network devices and perform port assignments in a generic, manufacturer-independent manner without using the command line interface of the network devices.

VLAN management works across devices and manufacturers so that global VLAN overviews are possible.

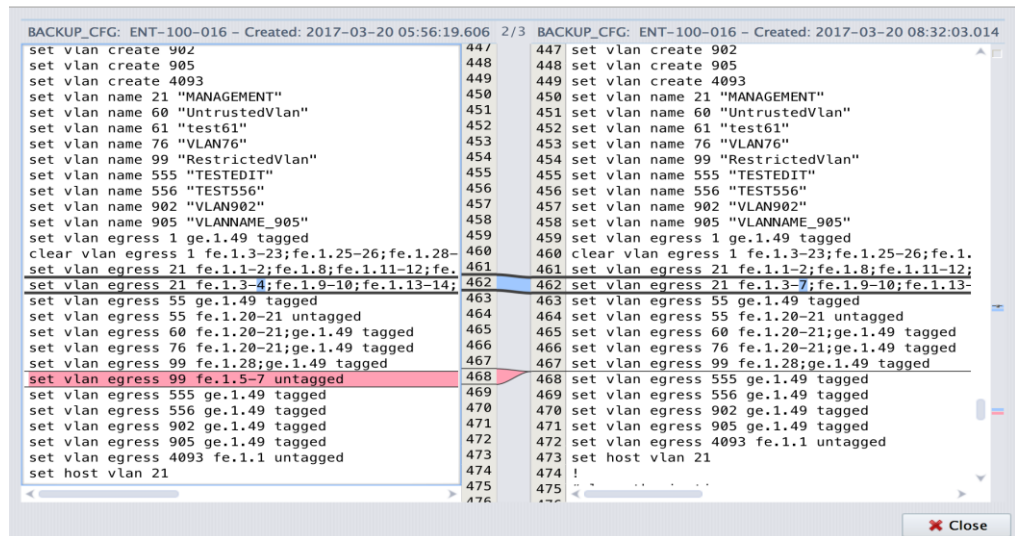
2.7 Configuration Management

The configuration management enables the backup of the current configurations of all network devices.

It is possible to check/alarm for changes in the current configuration compared to the last configuration or a reference configuration:

- (i) Time-controlled at a certain distance (e.g. every night at 1 am)
- (ii) Once on user request
- (iii) Automatically after changing the configuration

Configuration management also enables a saved configuration or a reference configuration to be loaded onto an existing, new or replaced network device.



```

BACKUP_CFG: ENT-100-016 - Created: 2017-03-20 05:56:19.606 2/3
set vlan create 902
set vlan create 905
set vlan create 4093
set vlan name 21 "MANAGEMENT"
set vlan name 60 "UntrustedVlan"
set vlan name 61 "test61"
set vlan name 76 "VLAN76"
set vlan name 99 "RestrictedVlan"
set vlan name 555 "TESTEDIT"
set vlan name 556 "TEST556"
set vlan name 902 "VLAN902"
set vlan name 905 "VLANNAME_905"
clear vlan egress 1 fe.1.3-23;fe.1.25-26;fe.1.28-
set vlan egress 21 fe.1.1-2;fe.1.8;fe.1.11-12;fe.
set vlan egress 21 fe.1.3-4;fe.1.9-10;fe.1.13-14;
set vlan egress 55 ge.1.49 tagged
set vlan egress 55 fe.1.20-21 untagged
set vlan egress 60 fe.1.20-21;ge.1.49 tagged
set vlan egress 76 fe.1.20-21;ge.1.49 tagged
set vlan egress 99 fe.1.28;ge.1.49 tagged
set vlan egress 99 fe.1.5-7 untagged
set vlan egress 555 ge.1.49 tagged
set vlan egress 556 ge.1.49 tagged
set vlan egress 902 ge.1.49 tagged
set vlan egress 905 ge.1.49 tagged
set vlan egress 4093 fe.1.1 untagged
set host vlan 21

BACKUP_CFG: ENT-100-016 - Created: 2017-03-20 08:32:03.014
447 set vlan create 902
448 set vlan create 905
449 set vlan create 4093
450 set vlan name 21 "MANAGEMENT"
451 set vlan name 60 "UntrustedVlan"
452 set vlan name 61 "test61"
453 set vlan name 76 "VLAN76"
454 set vlan name 99 "RestrictedVlan"
455 set vlan name 555 "TESTEDIT"
456 set vlan name 556 "TEST556"
457 set vlan name 902 "VLAN902"
458 set vlan name 905 "VLANNAME_905"
459 set vlan egress 1 ge.1.49 tagged
460 clear vlan egress 1 fe.1.3-23;fe.1.25-26;fe.1.
461 set vlan egress 21 fe.1.1-2;fe.1.8;fe.1.11-12;
462 set vlan egress 21 fe.1.3-7;fe.1.9-10;fe.1.13-
463 set vlan egress 55 ge.1.49 tagged
464 set vlan egress 55 fe.1.20-21 untagged
465 set vlan egress 60 fe.1.20-21;ge.1.49 tagged
466 set vlan egress 76 fe.1.20-21;ge.1.49 tagged
467 set vlan egress 99 fe.1.28;ge.1.49 tagged
468 set vlan egress 555 ge.1.49 tagged
469 set vlan egress 556 ge.1.49 tagged
470 set vlan egress 902 ge.1.49 tagged
471 set vlan egress 905 ge.1.49 tagged
472 set vlan egress 4093 fe.1.1 untagged
473 set host vlan 21
474 !
475
476
    
```

2.8 Syslog Analyzer

This enables the evaluation of messages from network devices that were sent in Syslog format.

Selected messages can be forwarded to the central event and alarm console via a filter mechanism, whereby parts of the message are transferred to separate event parameters for further processing.

BICS can also use this function to generate messages in Syslog format itself and send them to other Syslog servers.

3 Extended functionalities of the Network Management System

3.1 Flow Reporting

Flow reporting supports the user in analyzing the data stream within the network. The following questions can be answered, for example:

- Which terminal causes the most traffic over a certain line?
- Which application generates the most traffic over a particular line?
- Which devices communicate with each other via which applications?
- Which deviations from "normal" communication behavior can be identified?

3.2 Advanced Automation

Advanced Automation is an optional configuration management function. It extends BICS by the possibility to define recurring more complex configuration tasks, to implement them for the individual device types and manufacturers and then to provide and execute them as a generic configuration option across devices and manufacturers without a user having to be able to operate the command line interfaces.

- Configuration tasks steps can be performed at a specific time and repeatedly.
- All changes made by "Advanced Automation" are recorded so that they can be traced for each individual device.

www.infraray.com

About Infraray

Infraray was founded in 1998 by a German team of engineers with many years of experience in IT Operation Management. The company offers solutions for information technology and offers solutions for network management, network security, IT infrastructure management, cloud, network automation and business infrastructure control.

Infraray BICS is the next-generation ITOM platform for controlling large and heterogeneous corporate networks. BICS not only offers network infrastructure management for all devices and end devices of the manufacturers, but also serves as the basis for a new generation of IT infrastructure management.

Infraray became part of the Beta Systems Group in early 2018.

© Infraray GmbH. All rights reserved.



Infraray GmbH

Stromstr. 5

10555 Berlin / Germany

Tel. +49 (0)30 726 118 0

info@infraray.com