Name: HARI HARA SUDHEER

STUDENT ID: W1167633

Audience

This Document provides a comprehensive understanding of the Unified Network Management of wired and wireless networks. This Document can be used by anyone who is interested in knowing about the management of networks.

The reader is expected to have basic understanding of the networking. Rest assured that you would be learning many things about how unification of wired and wireless devices happens and how it brings about effective management of the network.

This Document provides the necessities of Unified Network management and ways in which this can be achieved. The document also covers basic things about SDN.

CONTENTS

TABLE OF FIGURES

INTRODUCTION

CHAPTER 1 *GIVES A BRIEF IDEA OF THE ORGANISATION OF THE ESSAY.*

CHAPTER 2 *DESCRIBES THE CHALLENGES FACES BY THE EXISTING MANAGEMENT SYSTEMS.*

CHAPTER 3 *DESCRIBES THE SOLUTION FOR THE CHALLENGES POSED IN CHAPTER 2*

CHAPTER 4 *DISCUSSES ABOUT UNIFYING WIRED AND WIRELESS NETWORKS*

CHAPTER 5 *DESCRIBES THE UNIFIED WIRED AND WIRELESS NETWORKS ARCHITECHTURE*

CHAPTER 6 *DISCUSSES ABOUT THE DIFFERENT WAYS IN, WHICH THE UNIFIED MANAGEMENT OF WIRED AND WIRELESS NETWORK CAN BE ACHIEVED*

CHAPTER 7 *IS THE INTRODUCTION TO SDN*

CHAPTER 8,9 *HAVE ACRONYMS AND REFERENCES RESPECTIVELY.*

CHALLENGES

The number of devices used by the Enterprise Networks is growing at rapid rates these days. Different kinds of wired and wireless devices from different vendors are being used in the enterprises these days. Each device has its own set of management operations. In order to overcome the management processes of these complex network environments, there is a need to unify the network management of wired and wireless devices irrespective of the different vendors.

The business environments these days requires connectivity anywhere and anytime during the work. Mobility changes the way companies do the business. In these high competitive business environments, companies need the results immediately without delay. So for the work to happen in that pace in the business environments there is a great need to embrace the wireless networks on top of the existing wired network foundations. This helps the employees in the organization to shift from the traditional desktop to devices, which have mobility and connectivity at the same time. This enables agility in business environments without requiring much time for setup.

This makes the WLANs to become critically important for the business organizations. End users are feeling more comfort ability and flexibility in adopting the business organizations to wireless connectivity. The business organizations are recognizing the competitive advantage of business-critical mobile applications. Deploying the WLANs increase Employee comfort ability, productivity and improve the customer service that the organizations can provide to its customers.

This increasing need for wireless environments is posing new challenges for today’s network managers. Network managers need to protect their networks from security breaches and deliver a secure WLAN access for their enterprises. The enterprises needs a WLAN infrastructure that effectively uses the RF technology and which is compatible with the existing wired network infrastructure.

In some cases, the enterprises need to deploy the WLAN solution on the top of the existing wired networks to take advantage of the existing resources, tools and infrastructure as the enterprises would have invested a lot of amount on the existing infrastructure. In such cases, there is a need to develop a software system that takes the advantage of the existing infrastructure and makes way for the effective WLAN services.

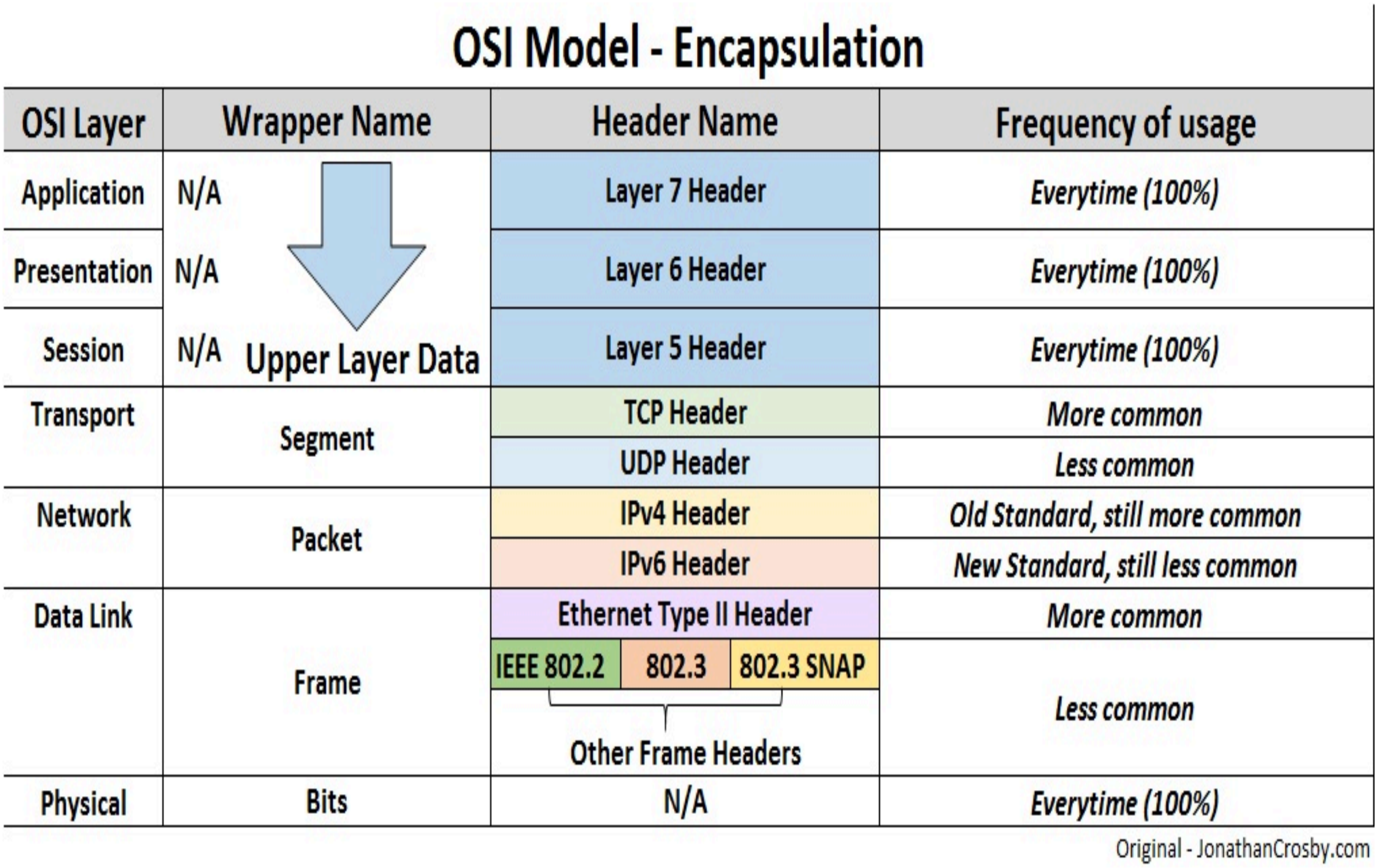
SOLUTION

Unified management of the wired and wireless networks helps in addressing these major trends and providing a solution that has intelligent and highly resilient wired and wireless network foundations on an uncompromised scale. With this solution several devices can be easily managed from a centralized management console. The Unified Wireless Network delivers the same level of reliability, security, scalability, ease of deployment, and management for WLANs that organizations expect from their wired LANs. The flexibility of the Unified Wireless Network allows network managers to design networks to meet their specific needs, when there is a need to expand the network. This provides high integrity in the network designs.

The unified network management provides rich services like common guest access; location based services and more granular security and control over the network. This innovative solution brings mobility to endpoint devices and users, providing them with network access anytime and anywhere. Apart from accessing the network rom anywhere, the network managers can monitor the networks with greater ease, find the problems caused in the network and diagnose them effectively.

UNIFYING WIRED AND WIRELESS NETWORKS

In 1984, International Organization for Standardization (ISO) developed the seven-layer model, which describes how information is transferred from one networking component to another. It breaks network communication into smaller components to make the design process easier. These advantages of the layers present in the network are being taken in achieving the unification of wired and wireless networks.



OSI Model - Encapsulation

OSI Layer	Wrapper Name	Header Name	Frequency of usage
Application	N/A	Layer 7 Header	*Everytime (100%)*
Presentation	N/A	Layer 6 Header	*Everytime (100%)*
Session	N/A Upper Layer Data	Layer 5 Header	*Everytime (100%)*
Transport	Segment	TCP Header	*More common*
		UDP Header	*Less common*
Network	Packet	IPv4 Header	*Old Standard, still more common*
		IPv6 Header	*New Standard, still less common*
Data Link	Frame	Ethernet Type II Header	*More common*
		IEEE 802.2 802.3 802.3 SNAP Other Frame Headers	*Less common*
Physical	Bits	N/A	*Everytime (100%)*

Original - JonathanCrosby.com

Fig 1.1

The second-lowest layer in the OSI Reference Model stack is the “DLL”. This layer, also sometimes just called the *link layer*. This is where wired and wireless LAN technologies such as Ethernet, Token Ring, FDDI and 802.11 (“wireless Ethernet” or “Wi-Fi’) primarily come into functionality. For example, are all sometimes called “link layer technologies”. The devices connected at this layer are what make a simple local network, which is then connected to the internetwork

Data Link Layer Sub layers: Logical Link Control (LLC) and Media Access Control (MAC)

The data link layer is often technically divided into two sub layers: *logical link control (LLC)* and *media access control (MAC)*. This split is based on the architecture used in the IEEE 802 Project, the IEEE group which works primarily on creating the standards that define many networking technologies that exist in the world today. By separating LLC and MAC functions the different network technologies are made interoperable.

Data Link Layer Functions

The key tasks that are performed at the data link layer are as follows:

Logical Link Control (LLC): Logical link control takes the responsibility for the establishment and control of logical links between local devices on a network. This is considered as a sub layer of the DLL.

This sub layer of the layer 2 delivers the services to the network layer above it and hides the rest of the details of the data link layer. This allows different technologies to work efficiently with the higher layers of the OSI model. Most local area networking technologies use the IEEE 802.2 LLC protocol.

Media Access Control (MAC): The MAC layer is responsible for connecting to the medium. Since many networks use a shared medium such as cables that are electrically connected into a single virtual medium or a wireless medium that takes the advantage of the unlicensed radio frequency, it is necessary to have rules for managing the medium to avoid conflicts. For an instance, Ethernet uses the CSMA/CD method of media access control, while WLAN uses CSMA/CA.

Data Framing: The data that the DLL gets from the higher layers is then encapsulated with the header and trailer into frames and then send those frames to the physical layer.

The fig 1.2 shows the different standards that can be used in the Layer 2 of the networking process. This kind of abstraction that exists in the layered approach helps us in breaking up the network and managing the network effectively. The DLL is the layer where the wired and wireless concepts come into action. Since after the information passes through this layer the information is encapsulated into frames and the frames are transported to the higher layer. After the transportation to higher layers it does not require any Layer 2 specific information to transport the packet thereafter. So the main networking devices where the unification of wired and wireless devices happens are the Switches, the Layer2 devices. The Switches must be capable of converging both 802.3(Ethernet) and 802.11(WLAN) frames.

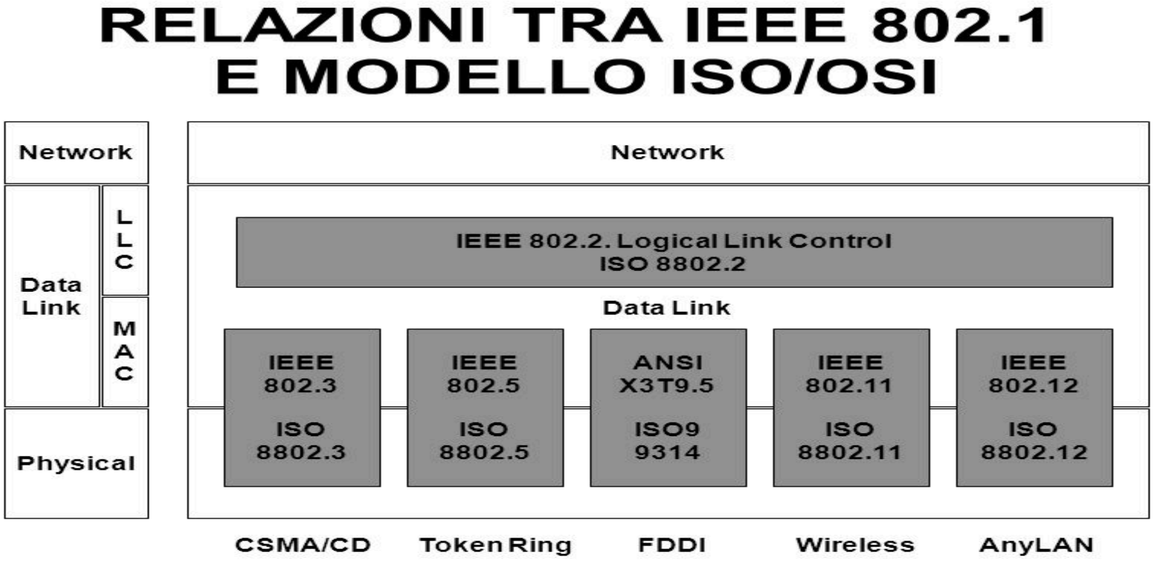


Fig 1.2

UNIFIED NETWORKS ARCHITECTURE

The Unified wired Wireless Network is composed of five interconnected elements that work together to deliver a world-class network solution for the enterprises. The five interconnected elements are Applications, Devices, Security, Unified Network topology, and Unified Network management. Beginning with a base of devices, each element adds capabilities as network grows, interconnecting with the elements above and below it to create a comprehensive, secure and scalable WLAN solution.

Here's are the five interconnected elements that are needed for the unified networks:

APPLICATIONS: Applications include wide range of Stand alone applications along with the Mobility Services such as unified cellular and voice over WLAN services, Video conference services, location-based security, asset tracking, Business and Collaboration services, Remote terminal access, VPN's and guest access.

DEVICES: Devices include Client Device, Mobile hosts, Static hosts, Converged wired and wireless switches, which serves as Access Points providing Ubiquitous network access in all environments and enhanced productivity through "plug-and-play" architecture, Routers.

SECURITY: “Out-of-the-box,” wireless security and mobility features through out the network infrastructure. A fundamental best practice of wireless LAN security is the ability to secure and control the RF environment with WLAN security policy monitoring through usage of customizable RF attack signatures to protect against common wireless threats. The wireless security features include Controlled access to the WLAN via numerous authentication and encryption policies, WPA, and mobile VPNs, WLAN IPS that detects and mitigates the impediments present in the security breached access points, unassociated client devices, and ad-hoc networks.

UNIFIED NETWORK TOPOLGY: Network Unification through out all major switching and routing platforms through secure, efficient WLAN apparatus. Integration of the wired and wireless network is critical for unified network control, scalability, security, and reliability and QOS into existing enterprise networks. Unified network provides comprehensive lifecycle management, performance assurance, and compliance for converged wired and wireless networks. The unification simplifies network management operations by providing a central platform management and visibility of applications and services across wireless, wired, campus, and branch network infrastructure.

UNIFIED NETWORK MANAGEMENT: Network Management delivers the same level of security, scalability, reliability, ease of deployment, and management for wireless LANs as available for wired LANs. The WLAN management provides clear visibility and control of the RF environment. This Increases network scalability, improves troubleshooting, and enhances productivity for network administrators, resulting in Simplified WLAN management and removes the complexity of managing the RF environment. Advanced WLAN planning, deployment, and management tools that provides centralized policies that help in maintenance of the system-level security and configuring the QOS policies. The unified network management system should have advanced troubleshooting and diagnostic tools that perform fault monitoring and make a Root cause analysis for diagnosing the network for enhanced performance.

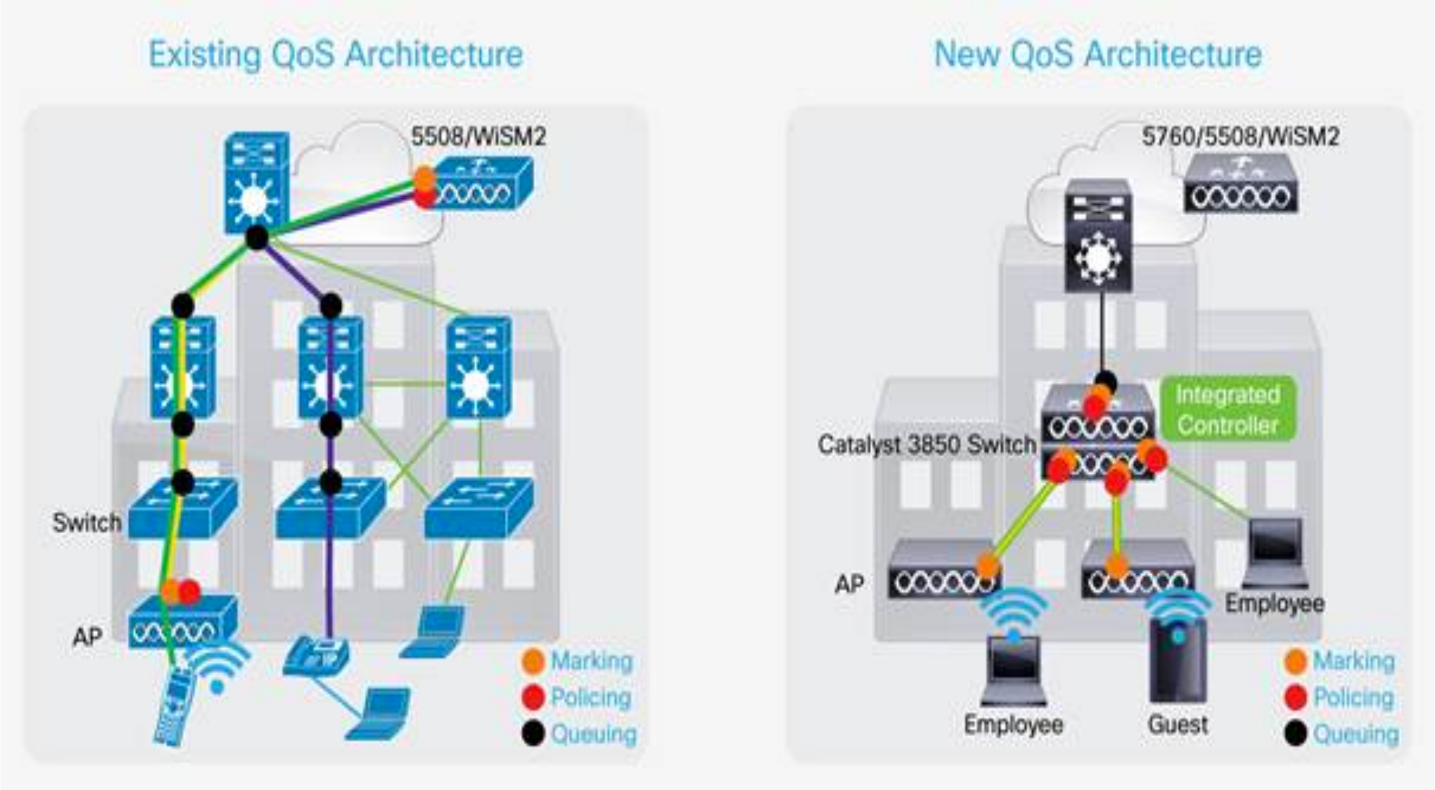


Fig 1.3

NON-UNIFIED NETWORK ARCHITECTURE:

A non-unified wireless network refers to a controller-based WLAN solution that has little to no unification with the wired network. Non-unified wireless solutions might or might not come from the incumbent data-networking provider. Deploying a WLAN from a supplier other than the incumbent data-networking provider usually results in different code, management, and user interfaces across the wired and wireless networks, resulting in a lack of benefits when compared to a unified solution. In this scenario, the wired and wireless networks remain separate, with the interface between the two being a standard Ethernet connection (Figure 1.4).

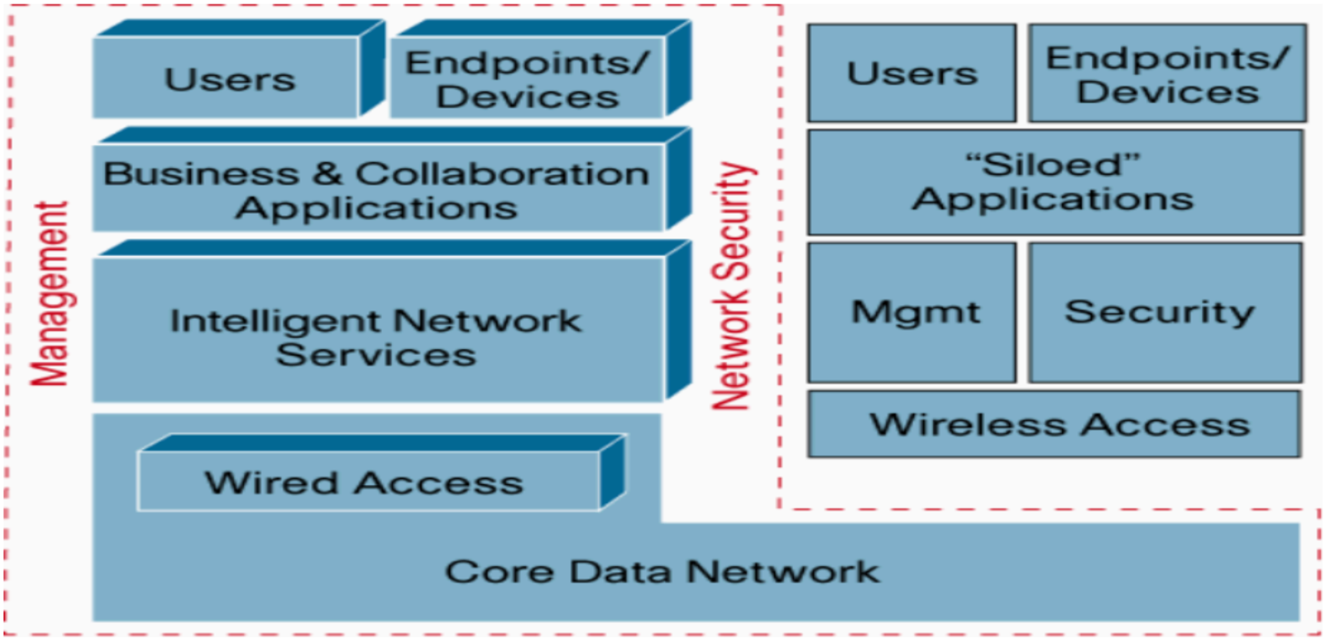


Fig 1.4

UNIFIED NETWORK ARCHITECTURE:

A unified wired and wireless architecture typically requires the wired and wireless infrastructures to be delivered from the same technology provider. In an integrated architecture, the control and management features are housed directly in the thread of the wired network. With this architecture, many of the services offered as standard features on the wired network can be extended into the wireless network because of the unification of user and management interfaces (Figure 1.5).

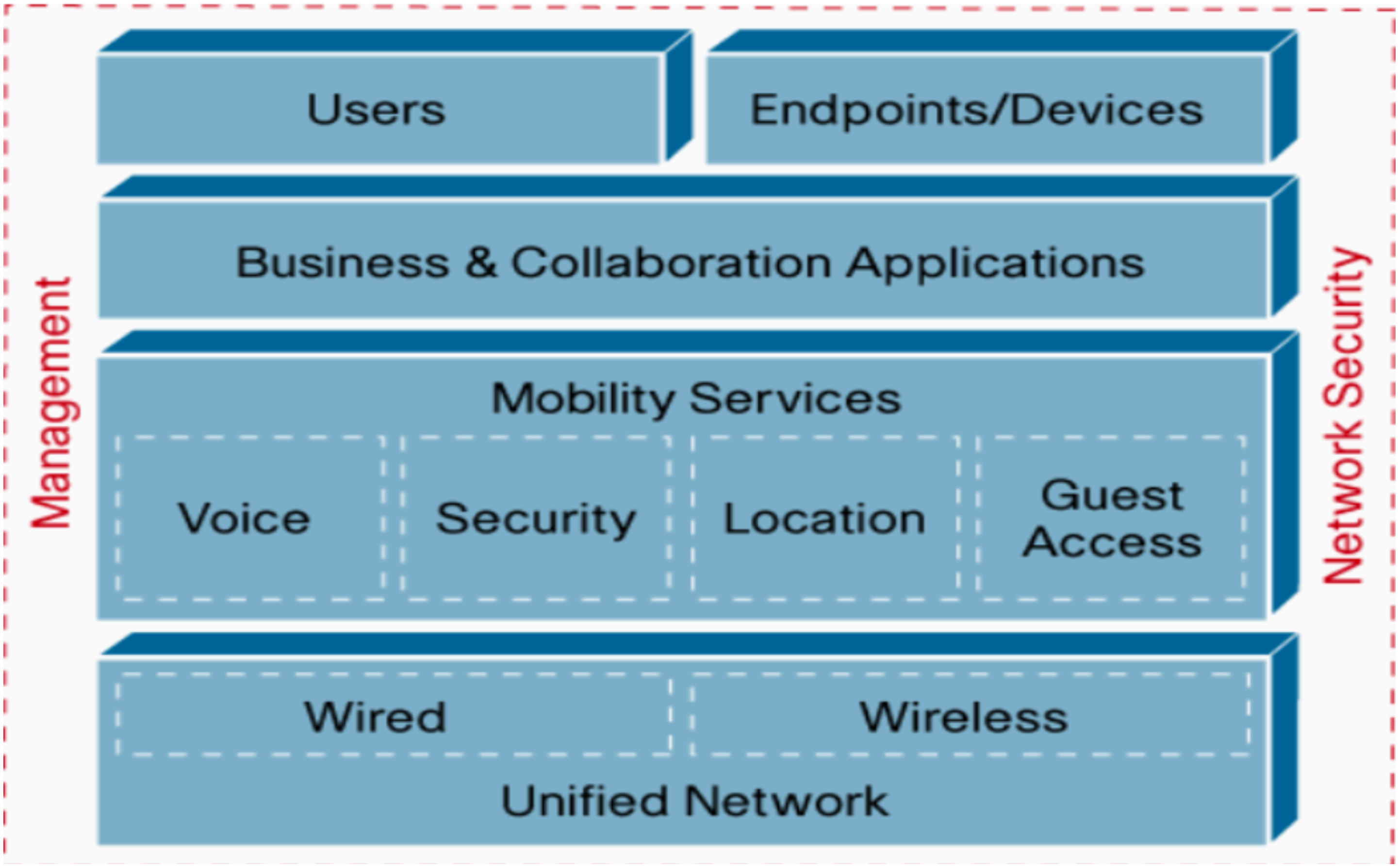
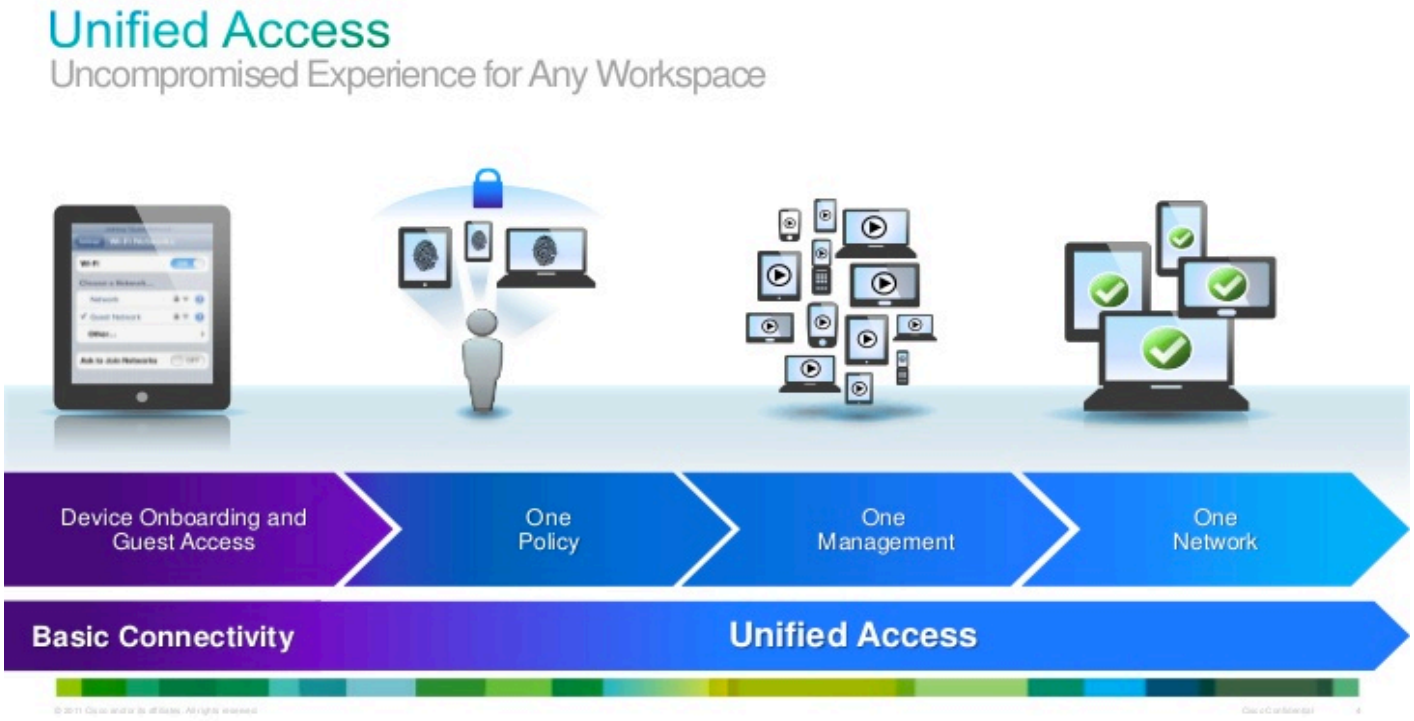


Fig 1.5

UNIFIED NETWORK MANAGEMENT

Unified network management is the administration of all types of networks through a single interface. The Unification of the entire network into one helps in creating one network, one management, one policy which makes way for achieving simple, intelligent network platform with great amount of business agility and operational efficiency with consideration of scalability for the networks.



Unified Access

Uncompromised Experience for Any Workspace

Fig 1.6

A natural question to ask is: why not diagnose performance problems by using the existing wireless and wired network management system separately?

For example, consider the case where there is no unification of the wired and wireless networks and the network administrator is trying to diagnose the network by calculating the time required for fetching a particular URL of the two hosts, wired desktop host and a wireless laptop simultaneously on both the platforms separately. Consider the laptop was moved between rooms every 5 minutes.

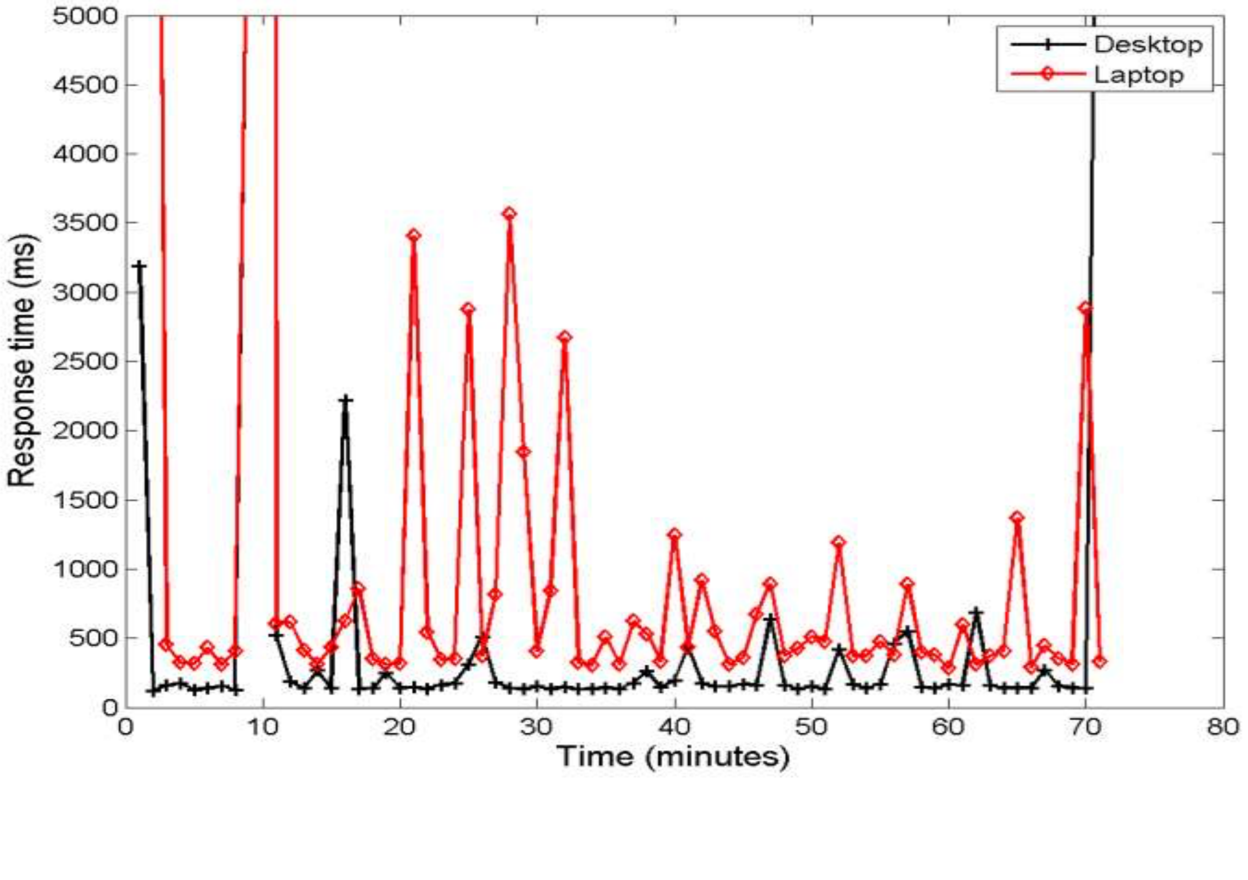


Fig 1.7

Case1: If the administrator sees some problem in wired desktop host.

The administrator could have two components to blame now. One is congestion in the wired network and another potentially indicating congestion in a server involved in providing the requested URL.

The administrator could go wrong in deciding the area where the problem could have happened in the case of non-unified communications.

Case2: If the administrator sees some problem in wireless laptop host.

The administrator could have two components to blame now. One is potentially indicating problems in the wireless connectivity and another indicating congestion in a server involved in providing the requested URL.

Even in this case, the administrator could have absolutely no idea to decide on which part the problem potentially persists.

Unsurprisingly, both the wired and wireless host sees significant variation in the response time. Interestingly, however, the wireless host sometimes sees the variation, potentially indicating problems in the wireless connectivity, and sometimes the variation is seen only in the wired host, potentially indicating congestion in the wired network.

The answer is that a management system that looks at only the wired network or the wireless network is likely to misinterpret some of the spikes in the response time and blame the wrong network component. A single system that jointly manages and diagnoses both aspects simultaneously has much better odds of correctly finding the cause of observed problems. Hence there is a need for the convergence of the wired and wireless traffic into single devices, which in turn helps in diagnosing the problems in the network efficiently.

Current enterprise network management systems use separate tools to manage their wired and wireless networks. In an environment where a large number of users are nomadic and connect to the corporate network using a variety of different networks, debugging application performance problems using separate tools is both difficult and frustrating. There are many problems affecting the performance of the clients. The solution for these problems is to deploy the new equipment that is capable of achieving the convergence of the wired and wireless networks. But the disadvantage with this kind of implementation is it turns out to be very expensive. There are many products capable of monitoring the existing non-unified system as unified wired and wireless networks and diagnosing the problems in the networks without deploying an additional, expensive, Wi-Fi monitoring infrastructure.

There are many end-to-end network management systems, which needs to be installed on the networking devices and nomadic hosts and monitor the performances. The software can monitor application-level performance problems and hence can make the network administrator's task easy in diagnosing the problems. This kind of implementation potentially minimizes the difficulties associated with diagnosis of the wireless networks in the enterprises and provides good monitoring capabilities.

The main features that distinguish this management software on the existing enterprise network management systems are joint consideration of the wired and wireless systems and the dynamics of the network topology. The network management system successfully manages the performance of networking services and applications running on nomadic hosts. It is based on recent research, which takes into account the network service dependency extraction, fault diagnosis, and wireless network monitoring. It keeps track of the physical locations of end devices and this tracking is a very important component of its strategy as it dynamically adapts to the frequent topology changes brought about by end-node movement.

The system does not need any hardware to monitor. It is essentially designed as user level software with the removal of burden of additional hardware deployment. It will be deployed on every device on the segment of the organization's network, which is intended to monitor. The system detects and correctly diagnoses a variety of performance issues, including poor Wi-Fi coverage, congestion in wired networks, and misconfigured DNS entries. The key thing that the system does is root-cause analysis. This system easily out-performs state- of-art systems that do not take nomadic users into account.

The architecture of the system is shown in the figure below. It mainly consists of two components, *Agent* that runs on the device in the network that needs to be monitored, and the *Inference Engine* that accepts data from these agents. The Inference Engine retrieves the data at regular intervals and analyzes the data to determine the root cause analysis. The inference engine uses this root cause analysis for generating the inference graph that depicts the performance of the systems, which have the software installed. The inference graph helps in identifying the problems associated with the changes in the topology of the network, and sends the diagnostic alerts to the network operator.

TYPICAL ARCHITECHTURE OF THE SYSTEM

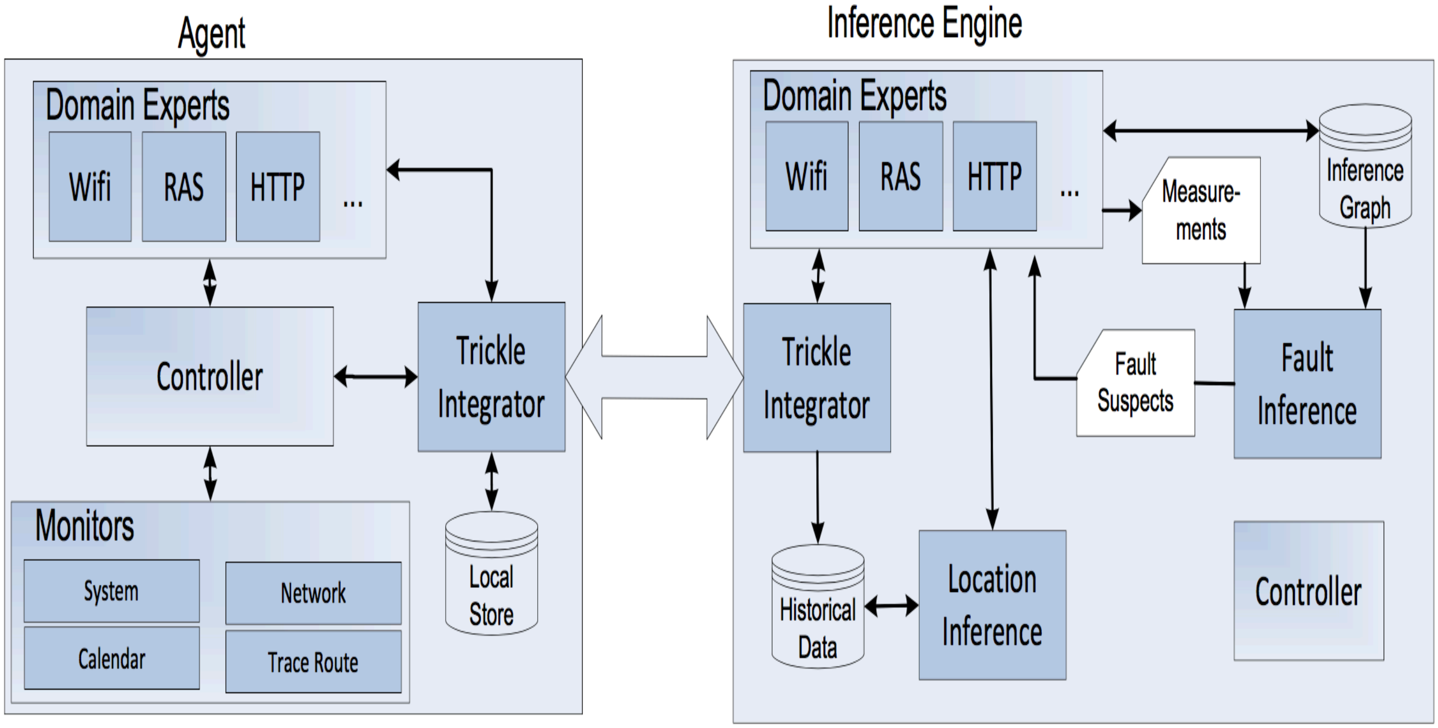


Fig 1.8

The agent is a very easy application that can be deployed on the devices that are in the network, wired or wireless and needs monitoring. It is a lightweight application that runs in background of the device and does not take up much of the RAM of the device and utilizes very limited power for its functionality. The total amount of data pushed to the Inference Engine for each observation is less than 1K bytes and hence pushing data to server takes very negligible amount of the users network bandwidth. The agent has different components such as *Monitors, Domain Experts, and Trickle Integrator.*

MONITORS:

Monitors gather the information about the system, user activity and network connectivity and then send this data to *Controller*. There can be different types of monitors in the agent. The monitors can be developed independently and dynamically added to the agent as a software upgrade. This lets us to choose the constraints that need to be monitored in different devices. However the Agents contains four monitors in common. They are System monitor, Calendar monitor, Network monitor, and Trace Route monitor.

System Monitor: The system monitor reports various system properties, which include information about whether, the system's battery is being charged and the type of network it is currently connected to such as wired or wireless. It also reports information such as system log and whether a user is currently active on the system. If there is no user input for a particular amount of time, which can be set by the network administrator, then the user is considered to be idle. It keeps getting updated at regular intervals of time.

Calendar Monitor: The Calendar Monitor reports information about the time and location of accepted meetings from the users enterprise calendar. Both the location and time works in sync. This information is used to bootstrap the location engine.

__Network Monitor__: The Network Monitor reports information about network connectivity of all the interfaces that the system holds. This information includes IP and MAC addresses, gate- ways, DNS and default gateway servers, and ping times to the first hop router. If the Network Monitor detects that the system is connected to the network via a wireless interface, it periodically collects information such as the AP the interface is associated with, other APs it can detect and the signal strengths of their beacons. The monitor also generates messages that are specific to the wireless interface. For example, if the wireless client is handed off form one AP to another, it generates a HANDOFF message and keeps track of the network change related events from the system, such as network address change.

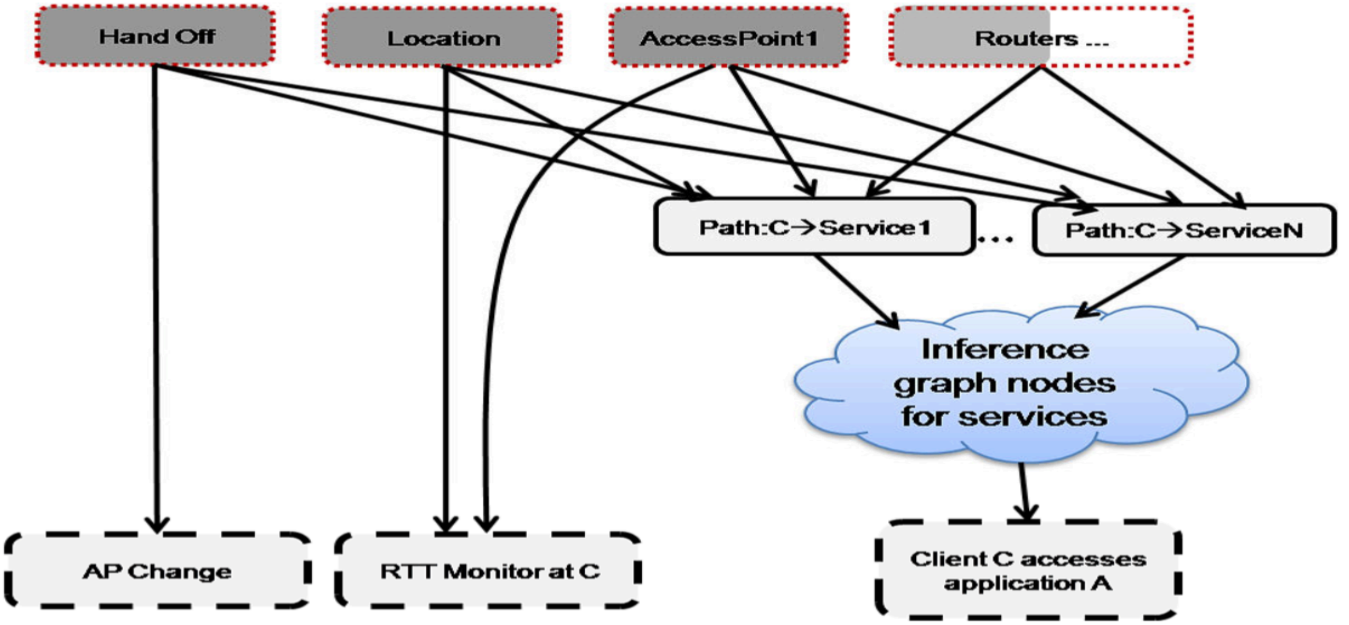


Fig 1.9

TRACE ROUTE MONITOR: This monitor uses *trace route* to discover the network path between the client and the other machines to which it is sending packets.

This data that is gathered by the Monitors is processed by *Domain Experts* that encapsulate the special logic required to deal with different problem domains. The *Domain Experts* generate data for the inference graph and performance observations. The agent sends all this data to the Inference Engine over a transport called the *Trickle Integrator* that is designed to cope with intermittent and variable connectivity.

DOMAIN EXPERTS:

A typical Domain Expert has code both on the host, as part of the Agent, and on the Inference Engine. Domain Experts respond to triggers such as change in IP address, or AP handoff event information that it gets from the Monitors. Upon such changes, the Domain Expert on the client notifies the Domain Expert on the Inference Engine of the triggering event. The Domain Expert is a kind of database, which gets the updates regularly from the agents. The updates are entered as tuples. It automatically gets updated on the Inference engine too. Every time the information in the Domain experts on the inference engine updates, the Inference Engine updates the Inference Graph appropriately. For example, when an AP Handoff event occurs, the Wi-Fi Domain Expert on the agent notifies its counterpart on the Inference Engine. The Inference Engine then updates the Inference Graph to account for the change in topology. There are many kinds of Domain experts.

Wi-Fi Expert: The Wi-Fi Expert is manages the details of how wireless connectivity performance of applications running on a mobile node. The information gathered by the Monitors in the agents helps the experts find out the correct AP it is connected to and location information. Hence, for every client whose location can be determined, the Wi-Fi Expert adds a new root cause and observation nodes to the Inference Graph in a particular pattern called as *graph gadget*. The inference engine consists of the information about the root cause node for each location. So, the network administrator alerts the clients in that location about the probable problems associated with that location.

RAS Expert: The RAS Expert manages the VPN connections from remote users. When a particular tries to connect to the enterprise network via VPN connection, the software adds that to the inference graph. The agent uses the ping generated RTT measurement between the client and the RAS server and adds a root cause node that represents the health of the RAS server in use and a root cause node that represents the quality of the Internet path between the client and the RAS server to guide the inference graph when deciding whether the problem is in the Internet path. All clients connecting via the same RAS server share the RAS server node.

HTTP Expert: The HTTP Expert monitors the response time of webservers when URLs are fetched, and reports these to the Inference Engine. The Inference Graph uses these as observations about the application’s health. The HTTP expert has an automated system to fetch URL’s automatically for testing the health of a particular application. Based on the response times received by the different devices in a particular area, the inference engine generates an inference graph to notify the agents about the problems happening during the URL fetching process.

Network Expert: The Network Expert computes the network topology-related dynamic part of the inference graph whenever a network change event occurs on the client. It is responsible for filling in two types of information. First, it computes network path to network services by using topology discovery techniques, such as trace route. Second, it detects changes in location-dependent network services, such as the DNS and Kerberos servers. The Network Expert counterpart on the Inference Engine updates this information in the inference graph.

Service Expert: The Service Expert is a special kind of domain expert that runs only on the Inference Engine, and has no client counter part. The Service Expert is responsible for building a static, service-level dependency graph for all networked applications. The service name and the server that is providing that service identify a service. For example, a website is identified by its URL and the web server hosting it. The Service Expert gets the data needed to construct the dependency graph from a variety of sources. The static dependency graph is combined with dynamic information from other domain experts, such as the Network Expert and the Wi-Fi Expert, to build an inference graph.

The Domain Expert architecture is a technique that will be employed for handling different types of domains where the changes occurrences are faster. Since the changes are learnt through them helps in generating the inference graph quickly.

The framework of the Domain Experts is designed in a way that the Graph Gadgets added by the each expert are compos able. For an instance, a client tries to work from the nearby coffee shop and connects his device to the enterprise network through the RAS, then the agent adds both Wi-Fi expert and RAS expert in this case to monitor both performances

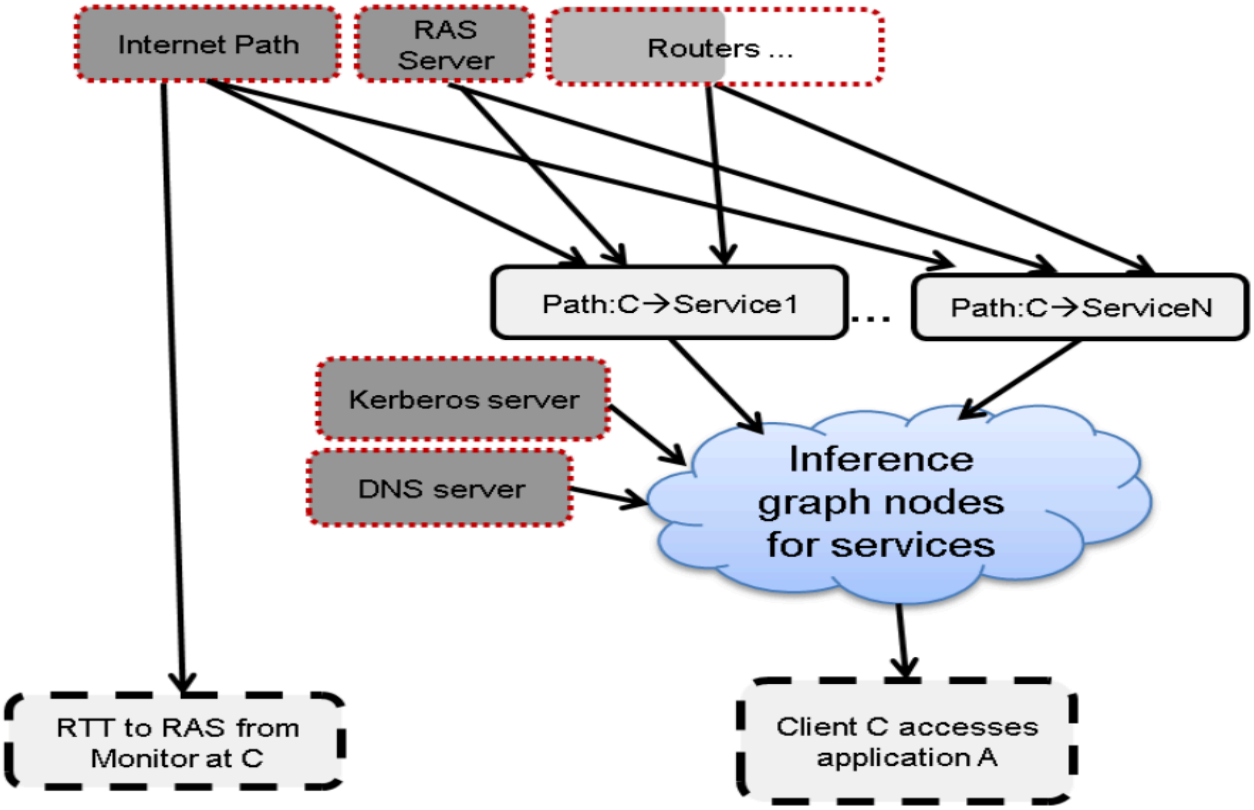

Internet Path
RAS Server
Routers ...
Path:C→Service1
...
Path:C→ServiceN
Kerberos server
DNS server
Inference graph nodes for services
RTT to RAS from Monitor at C
Client C accesses application A

Fig 1.10

TRICKLE INTEGRATOR:

The trickle integrator serves as a local store for the client. When there is no connectivity between the agent and the inference engine, the tuples of data created by domain experts is passed on to trickle integrator through controller. Whenever the client has connectivity, the data that is stored in the local store of the trickle integrator is pushed to the Inference Engine.

CONTROLLER:

The Controller is the agent's lightweight workflow engine. It provides a publisher-subscriber service to moderate the interactions between *Monitors*, *Domain Experts*, and the Trickle Integrator. All messages between the components agent take the form of tuples: a list of fields and their values. The experts and monitors register *triggers* with the Controller. Whenever the Controller processes a message matching a trigger, it invokes the associated callback with the message as an argument. The Controller itself generates messages to mark important events, such as agent startup and expiration of a periodic timer. The agent generates a START message on startup. Then it generates a PERIODIC TIMER message every polling interval, which triggers the monitors to generate messages encapsulating their measurements. In addition to the messages generated by the agent, the monitors also register for system- wide events such as network address change and wireless hand-off event.

INFERENCE ENGINE:

The Inference engine holds the responsibility of monitoring the health if the agents registered with it. The Inference engine stores all the data that it received from the agents. Using this information it generates the Inference Graph to generate a list of probable causes whenever it identifies performance problems, and subsequently raises alerts. It uses the Inference graph and the service-level dependency graph, it sends the different kinds of information like the their location with respect to the network topology and root cause node analysis data for that particular location. The inference engine has Location inference and Fault inference in addition to the experts, controllers and trickle integrators. The roles of the experts, controllers and trickle integrators are similar to that of in agents. The Inference engine does the fault diagnosis and generates an Inference graph.

FAULT INFERENCE:

The Fault Inference module is responsible fro gathering the information produced by the agents in the system and diagnose the problems and generate the root cause analysis report. This resulting fault suspects from the root cause analysis data is then sent to the network administrators. It mainly consists of two components. One is the Location inference module, which determines the location priors. This is invoked once a day and it gets updated when there are any changes in the location. The other one is the Inference module, which is responsible for the updating the inference graph based on the data from the agents. Once invoked, the inference module updates the Inference Graph, computes the state of the observation devices, and then runs the inference algorithm to determine a list of fault suspects.

LOCATION INFERENCE:

The physical location of a wireless client may have a strong impact on its network performance. Thus, management tools designed for wireless networks must include an integrated location estimation system. The location inference module stores the location profiles rather than the (x, y, z) coordinates. There is a profile defined for a particular Office in the buildings. The profile for each office consists of a list of APs (i.e. their BSSIDs) that are visible from that location along with the distribution of observed signal strength of each AP. The distribution that is followed here is Gaussian distribution.

Determining Client Location:

The client's location is exactly determined using the observations sent by the client's domain experts. As part of the observations, the Wi-Fi Monitor running on each client submits the list of APs seen by the client, along with their signal strengths. The location inference module of the inference engine makes use of many distribution models to correlate the signal strength that it received from the domain expert of the client with the stored profiles data to determine the exact location. The profiles of the offices are generated automatically and stored in the location inference module. The Location inference module uses the calendar service to cross check the location of the devices. For an instance consider that a meeting is being scheduled in Meeting room located in a particular office. If the Inference engine gets this data through the calendar expert, it cross verifies the locations it has detected for each person attending the meeting. It ensures better service and verification for the results it has generated.

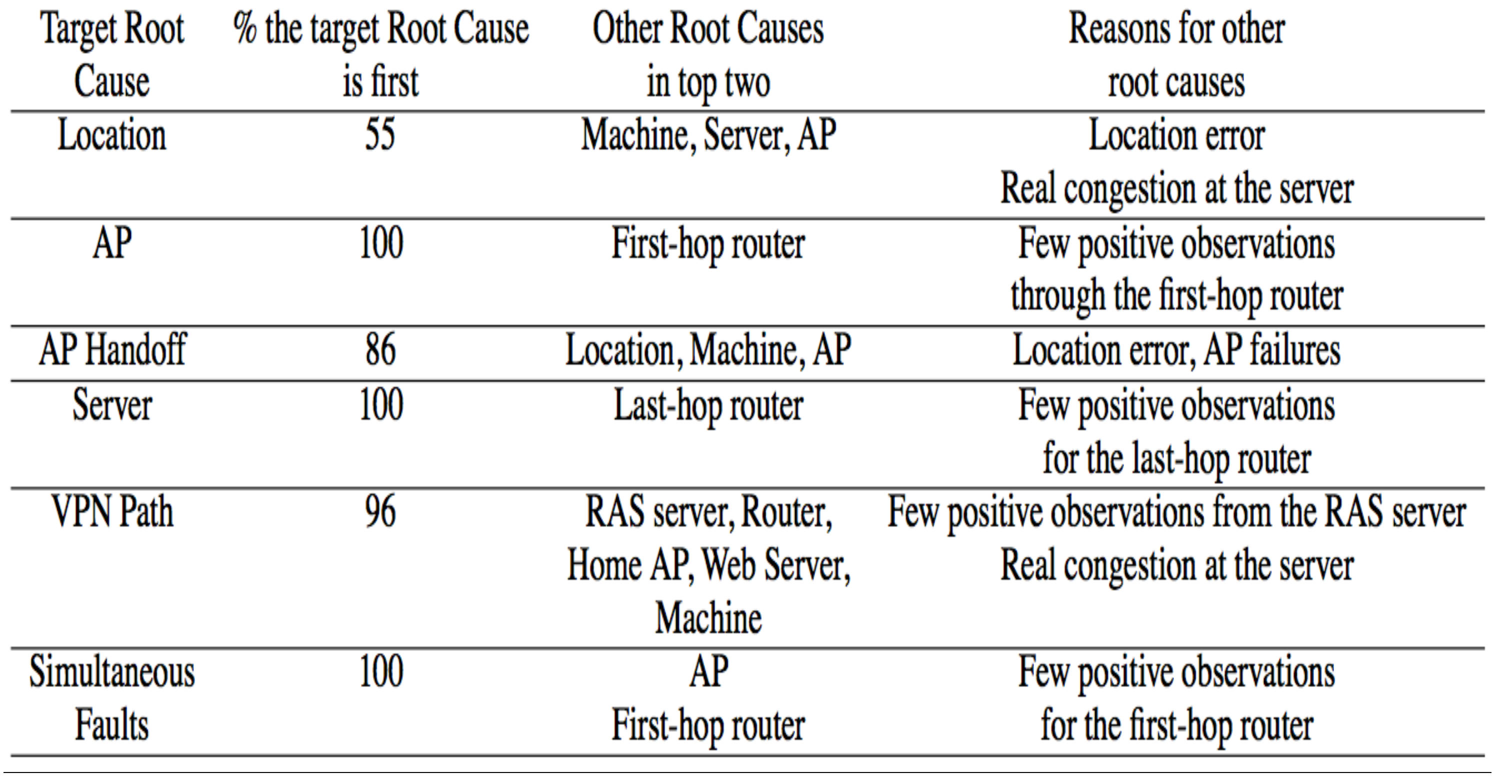
Computing the Inference Graph:

The Inference Engine controller orchestrates the construction of the Inference Graph by the various Domain Experts through a publish-subscribe system. The service expert generates the basic inference graph. Each Domain Expert subscribes to be notified whenever the devices add a graph gadget. Upon receiving such notification, the Domain Expert makes its own alterations to graph. This process repeats until no further changes are made to the graph, at which point the graph is ready to use for inference.

Diagnosing Faults:

Given an Inference Graph, prior probabilities for locations, and the up and down status of the observations, the system uses the Ferret inference algorithm described compute the root causes that are most likely responsible for the down observations. These root causes are returned as the fault suspect list to the network managers and administrators.

The figure 1.11 shows a sample root causes analysis data and the possible fault suspects.



Target Root Cause	% the target Root Cause is first	Other Root Causes in top two	Reasons for other root causes
Location	55	Machine, Server, AP	Location error Real congestion at the server
AP	100	First-hop router	Few positive observations through the first-hop router
AP Handoff	86	Location, Machine, AP	Location error, AP failures
Server	100	Last-hop router	Few positive observations for the last-hop router
VPN Path	96	RAS server, Router, Home AP, Web Server, Machine	Few positive observations from the RAS server Real congestion at the server
Simultaneous Faults	100	AP First-hop router	Few positive observations for the first-hop router

Fig 1.11

SDN

“Unified wired and wireless is great, but with SDN it's amazing”. Unifying the networks is definitely a great move but with SDN it definitely adds value to the business. By treating the network as a whole, the users experience of the wireless users can be greatly improved on par with the wired users. The complexities involved in the network operations can be brought down to a great extent. SDN helps in achieving ease of management, QOS, Security of use for the unified wired and wireless access network.
In a traditional environment, where there is no SDN deployed, the network administrator has to do all kinds of tasks on the networking devices through the CLI. This makes it so complex for the network administrator.

Every networking device has a control pane and the data pane. The control pane is the brain of the device. It essentially does all the functionality to perform the operations such a routing, switching. The data pane deals with how the packets are forwarded. Technically SDN is defined, as the separation of the control pane and data pane from the networking devices, where networking devices can be updates using different protocols.

SDN can be achieved in three different ways. They are:

1. Open SDN

In this the SDN is achieved using open flow protocol.

2. SDN via API's

In this the functionality of the SDN is achieved using the rich API's. Developers can manipulate the networking devices using the API.

3. SDN via OVERLAYS

In this the SDN is achieved using the network overlay tunnels.

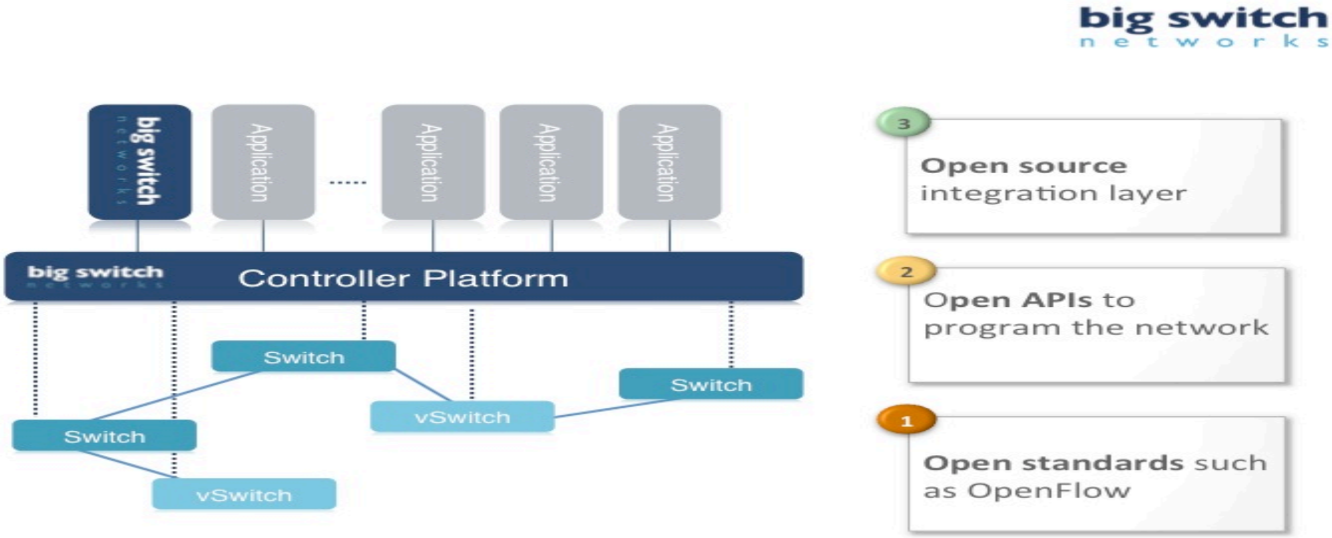


Fig 1.12

An effective, integrated, wireless SDN solution will allow us to maintain:

1.End-to-end application QOS, enabling enforceable service-level agreements.

2.Seperating the management from the functionality of the devices.

3.The ability to use different products from different vendors.

ACRONYMS

WLAN	-	*Wireless Local Area Network.*
RF	-	*Radio Frequency*.
LAN	-	*Local Area Network.*
OSI	-	*Open Systems Interconnection.*
VPN	-	*Virtual Private Network.*
WPA	-	*Wi-Fi Protected Access.*
QOS	-	*Quality Of Service.*
RAM	-	*Random Access Memory.*
URL	-	*Uniform Resource Locator.*
AP	-	*Access Point.*
DNS	-	*Domain Name Service.*
RAS	-	*Remote Access Server.*
HTTP	-	*Hypertext Transfer Protocol.*
BSSID	-	*Basic Service Set Identifier.*
SDN	-	*Software Defined Networking.*
CLI	-	*Command Line Interface.*
API	-	*Application Programming Interface.*

REFERENCES

- http://www.researchgate.net/publication/221164636_Change_is_hard_adapting_dependency_graph_models_for_unified_diagnosis_in_wiredwireless_networks
- http://computernetworkingnotes.com/osi-layer-modals/advantage-of-osi-layer.html
- http://www.tcpipguide.com/free/t_DataLinkLayerLayer2.htm
- http://www.integra1.net/io.nsf/html/WEBB7ZLT5J/$FILE/Cisco+Wireless+networks+Q&A.pdf
- http://www.cisco.com/web/AP/wireless/pdf/overview.pdf
- http://searchnetworking.techtarget.com/tip/Integrated-wireless-network-management-systems-work-across-infrastructures