Oracle® Food and Beverage Networking Excellence

Reference Guide

Oracle Food and Beverage Networking Excellence Reference Guide

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

6 Network Infrastructure 6-1

7 Networks 7-1

8 Glossary 8-1

Preface

An effective network is critical for the success of any size Point of Sale site. Successful communication between the data center containing the Simphony Servers, Point of Sale client hardware, all networked devices, and shared services (e.g., the Check and Posting Service – CAPS).

Purpose

This document provides networking reference and guidance for Simphony.

Audience

This document is intended for:

• System administrators installing Simphony

• End users of Simphony

Customer Support

To contact Oracle Customer Support, access the Customer Support Portal at https://iccp.custhelp.com/.

When contacting Customer Support, please provide the following:

- Product version and program/module name
- Functional and technical description of the problem (include business impact)
- Detailed step-by-step instructions to re-create
- Exact error message received and any associated log files
- Screen shots of each step you take

Documentation

Oracle Hospitality product documentation is available on the Oracle Help Center at

http://docs.oracle.com/en/industries/food-beverage/

Table 1 Revision History

Date	Description
March 2021	Initial Publication.
January 2022	Updated the Oracle Cloud – Connection to Applications section.
March 2023	Added the Image Locations for Kiosks section to the Cloud Connectivity chapter.
September 2023	In the Image Locations for Kiosks section, added reference to Oracle Cloud Infrastrucure IP addresses.

Date	Description
December 2023	Updated the Latency section in the Networks chapter.

1
Introduction - Reliable Network Data Flow

An effective network is critical for the success of any size Point of Sale site. Successful communication between the data center containing the Simphony servers, Point of Sale client hardware, all networked devices, and shared services (for example, the Check and Posting Service (CAPS)).

Restaurants, casinos, hotels, stadiums, and cruise ships have different network requirements: wired, wireless, hybrid, Simphony enterprise servers hosted on-site or in the cloud. This document provides network installation guidance for an efficient and effective site network.

This guide describes:

- Oracle networking expectations
- Special property considerations
- Power considerations
- Cloud connectivity
- Network infrastructure – relevant educational material
- Networks – relevant educational material

2 Oracle Networking Expectations

This chapter describes Oracle MICROS networking infrastructure expectations, wired and wireless, together for convenient reference.

Dynamic Host Configuration Protocol (DHCP)

- If DHCP is to be used within a property, it is essential that the IP addresses are reserved.
- If DHCP is to be used within a property, it is essential that NTP servers are not sent to the workstations, as CAL has a built-in time sync functionality, and this can cause conflicts.
- When DHCP is used, the lease length should be long enough to ensure that lease renewals do not happen during business hours.
- Even though DNS resolution can be implemented, the delay and overhead can cause intermittent issues. If there are no other options, it should be implemented in conjunction with fixed IP reservations.

Domain Name System (DNS)

- A local DNS server would be required if using workstation name communications rather than IP communications.
- Valid local primary and remote secondary DNS servers are required for reliable communication to the property service hosts and the enterprise server.

Spanning Tree Protocol

Only use switches that support STP to eliminate the possibility of switching loops—smart and managed switches.

Security

Firewalls

Industry Standard Recommendations

1. Document your firewall rules.
2. Establish and follow a change procedure for firewall configuration.
3. Use automation to update firewall settings.
4. Review firewall rules regularly.
5. Remove unused or overlapping firewall rules.
6. Audit your logs.
7. Organize your firewall rules to maximize speed.
8. Move some traffic blocking upstream.
9. Upgrade your firewall software and firmware.
10. Communicate with the business.

Oracle MICROS Expectations:

CAL sets firewall rules on ServiceHosts to allow communications.

See the appendix on Simphony port numbers in the *Oracle MICROS Simphony Security Guide*.

IDS and IPS

Simphony is a very "chatty" application, especially in larger deployments. Instances in the field have seen where Check Sharing is "broken" but was traced back to an unmanaged switch that was blocking notifications from CAPS because there were so many. After installation, the installer must verify that each workstation can use PMC to ‘App Ping’ every other workstation to ensure reliable two-way communications

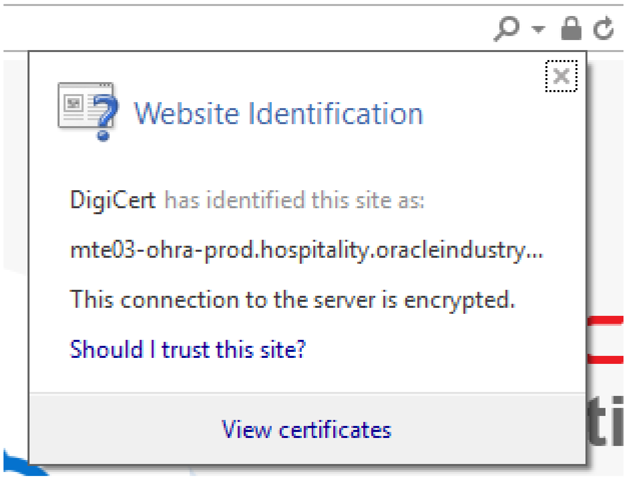
Certificates

- Only use certificates offered from trusted Certificates of Authority.
- Do not use self-signed certificates.
- TLS 1.2 is a required minimum encryption standard in Oracle data centers.
- Oracle Food and Beverage recommends using TLS for on-premise installations.

Certificate Revocation List (CRL)

To check communication to the CRL endpoint:

1. From Microsoft Internet Explorer, connect to the HTTPS webserver.
2. In the address bar, click the lock, and then click **View Certificates**:

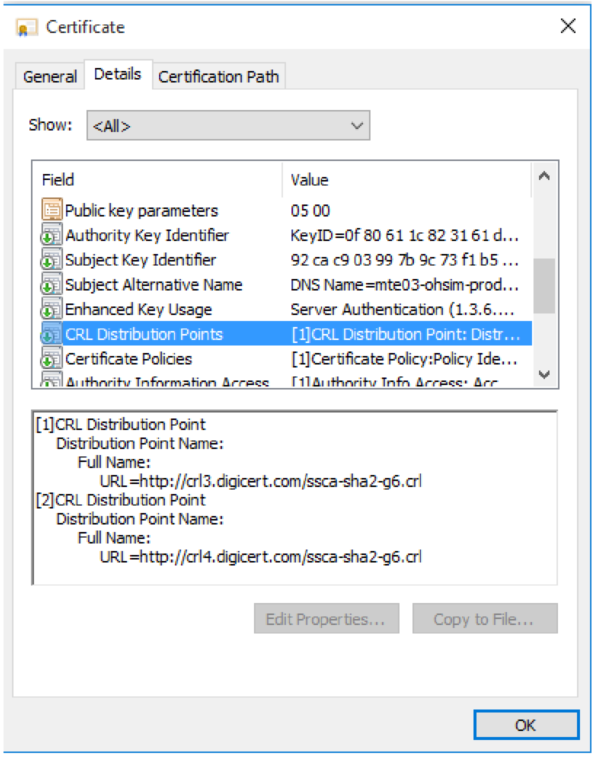


DigiCert has identified this site as:

mte03-ohra-prod.hospitality.oracleindustry...

This connection to the server is encrypted.

3. Go to the **Details** tab and then scroll to the **CRL Distribution Points** field:



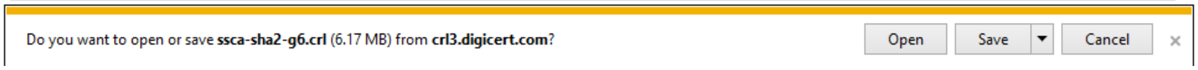
Show: <All>

Field	Value
Public key parameters	05 00
Authority Key Identifier	KeyID=0f 80 61 1c 82 31 61 d...
Subject Key Identifier	92 ca c9 03 99 7b 9c 73 f1 b5 ...
Subject Alternative Name	DNS Name=mte03-ohsim-prod...
Enhanced Key Usage	Server Authentication (1.3.6....
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Certificate Policies	[1]Certificate Policy:Policy Ide...
Authority Information Access	[1]Authority Info Access: Acc

```
[1]CRL Distribution Point
    Distribution Point Name:
        Full Name:
            URL=http://crl3.digicert.com/ssca-sha2-g6.crl
[2]CRL Distribution Point
    Distribution Point Name:
        Full Name:
            URL=http://crl4.digicert.com/ssca-sha2-g6.crl
```

4. Copy the URL mentioned in the example above, http://crl3.digicert.com/ssca-sha2-g6.crl & http://crl4.digicert.com/ssca-sha2-g6.crl

5. Go to the URL in Microsoft Internet Explorer, if access is possible. Microsoft Internet Explorer prompts you to download a copy of the CRL List:



Do you want to open or save **ssca-sha2-g6.crl** (6.17 MB) from **crl3.digicert.com**?

Proxy

Simphony workstations and tablets are "proxy aware" and can be configured in the Microsoft Windows operating system to use a proxy server when connecting to the cloud.

VLAN and VPN

A virtual local area network (VLAN) is a collection of devices on one or more local area networks (LANs) configured to interact with each other at the data link layer as though they share the same physical location. They use each device’s MAC address in the same broadcast domain.

VLANs offer a way to segment the network based on end-user needs such as resources and services and are not limited to one location. This can be one floor or multiple buildings. Communication within the group is based on logical connections as opposed to physical ones.

Switches are used to segment the network with ports assigned to a specific VLAN and each device on that VLAN connects to it through a cable.

Advantages of VLAN:

- Enables logical grouping of devices scattered across multiple physical locations
- Minimizes the need for router deployment and reduces deployment costs
- Reduces administration
- Allows easy broadcast control and segmentation

Disadvantages of VLAN:

- Does not offer inherent end-to-end security

A virtual private network (VPN) is a technology that allows for secure extension of a private network over a public network (the Internet), and it is more often related to remote access to company’s network resources. VPNs create a safe, virtual tunnel between your device and the destination—website, company resources, or customer site. The tunnel encrypts all traffic that passes through it, hides your real IP address, and makes it possible to access content. A VPN can work at the data link layer or network layer depending on the protocols used.

There are two types of VPNs:

- Client-to-Site (remote-access): The VPN connection allows remote hosts to connect to the network on as-needed basis.
- Site-to-Site: The VPN is set up to connect specific machines between two networks on an ongoing basis with no setup per communication required.

Advantages of a VPN:

- Provides high level of security through encryption
- Ensures privacy and confidentiality
- Allows to increase the overall efficiency of a network
- Allows anonymous file sharing (works with P2P networks)

Disadvantages of a VPN:

- Costlier, requiring specialized equipment such as VPN concentrator and routers
- Higher administrative overhead requiring more extensive knowledge working with security

Network Types

Wide Area Network (WAN)

- Choose a WAN that provides sufficient bandwidth for the number of workstations deployed at the location.
- Choose a WAN that scales up sufficiently during periods of high demand or peak usage.
- Choose a WAN that provides a sufficient level of network redundancy and availability should an outage occur.

Local Area Network (LAN)

- Design a LAN that provides sufficient bandwidth for the number of workstations deployed at the location.
- Design a LAN that provides a sufficient level of network redundancy or availability should a hardware outage occur. It is important to have solid two-way communications between all workstations.
- Make and maintain an updated map of the LAN network.
- Recommend running two cables per wall jack.
- Use wired network connections for devices that host shared services.
- Place shared services on highly available devices.

- Do not place shared services on devices that lose network connectivity frequently, as that negatively affects the POS client operations on other devices.

Cable Types

Twisted Pair

The following Oracle MICROS devices utilize twisted pair Ethernet cabling:

- Point of Sale workstations
- Kitchen Display Systems
- Receipt printers
- Kitchen order printers

Consider the following points:

- Interference from nearby electrical equipment.
- Shielded or unshielded Ethernet cabling.
- Distance of Ethernet cable runs.

Oracle MICROS expectations:

- Terminate Ethernet cable properly.
- Use Ethernet Category 6 Ethernet cable as the final network runs in a building.
- Keep Ethernet cable away from devices that create high levels of electrical interference.

Fiber Optic

- Use fiber optic cable for long network runs that exceed the recommended distance for Ethernet cable.
- Use fiber optic cable for network runs between buildings.
- Use fiber optic cable for network runs where electrical interference might be an issue.

Integrated Device Network (IDN)

- Cat 6 or better shielded cables between the patch panel and wall plates.

Specifications

The efficiency of a network can be affected by the speed of data throughput, maximum distance between network devices, and time delay between data transfer.

Bandwidth

Consider the following example of the Simphony the Client Application Loader (CAL) on a WAN:

When new client applications or support files are available, the CAL sends the new set of files from the enterprise application server to the clients.

A standard Simphony version service host CAL package is usually about 50 megabytes (MB) in size.

Based on that, a property with 100 workstation clients' needs to download 5000 MB of data through the Wide Area Network (WAN).

When the network bandwidth of a property cannot support simultaneous requests made by numerous clients, properties might experience bandwidth bottlenecks.

To calculate the bandwidth by workstation:

- Number of workstations = W
- W x 0.02 Mbps = Total Workstation Bandwidth during normal operations.
- W x 2 Mbps = Total Workstation Bandwidth when performing a reload of a workstation's database.

Distance

- Do not exceed the maximum distance allowed for your cabling.
- Calculate the last connection from wall jack to the device into the maximum distance.

Latency

It is recommended to install software in the cloud with the least amount of latency to the site if possible.

Hardware

Router

Router considerations:

- Install the router in a secure location such as a network closet.
- Label network ports and the cables connected to those network ports.

Switch

Switch considerations:

- Install the switch in a secure location such as a network closet.
- Label network ports and the cables connected to those network ports.
- Network Hubs are not recommended for Oracle MICROS installations.
- Unmanaged switches can be used for small Oracle MICROS installations.
- Unmanaged switches should be physically secured as port level security management is not available in these types of switches.
- Managed switches are recommended for medium to large enterprise Oracle MICROS hardware installations.

Powerline Extender

Powerline extenders are not recommended for Oracle MICROS installations.

Modem

Modem considerations:

- Install the modem in a secure location such as a network closet.
- Label all ports and the cables connected to those ports.

Installation

Cabling

Recommended Ethernet Cabling for Oracle MICROS Installations:

Category 6 Ethernet cable (CAT 6)

Recommended Fiber Optic Cabling for Oracle MICROS Installations:

Fiber is recommended for distances greater than 100 meters or as a solution to ground potential issues.

Recommended Coaxial Cabling for Oracle MICROS Installations:

RG-59 Coaxial cable

Recommended IDN Cabling for Oracle MICROS Installations:

For permanent installation between wall panels:

Category 6 Ethernet cable (CAT 6) shielded for installed wiring is preferred**.** (Category 3, 4, or 5 twisted pair cable can be used if already available.)

For wall or workstation to IDN printer:

- Oracle MICROS Part #300281-036-PT Shielded cable assembly for IDN printers: 3 feet, 6-pin to 6-pin for Oracle MICROS workstations
- Oracle MICROS Part #300281-120-PT Shielded cable assembly for IDN printers: 10 feet, 6-pin to 6-pin for Oracle MICROS workstations
- Oracle MICROS Part #300319-036-PT Shielded cable assembly for IDN printers: 3 feet, 8-pin to 6-pin for Oracle MICROS workstations
- Oracle MICROS Part #300319-120-PT Shielded cable assembly for IDN printers: 10 feet, 8-pin to 6-pin for Oracle MICROS workstations

Oracle MICROS Expectations:

- Label all cabling, patch panels, and wall jacks.
- Before cable is pulled, determine the physical location of all devices including the workstations, servers, wireless access points, IP printers, kitchen display units and order confirmation board. It is suggested that you specify the equipment location in the floor plan or riser diagram of the property.
- Ensure all horizontal cable runs from the patch panel, switch, or router to individual work area faceplates are at least 3 meters (10 feet) to no more than 90 meters (295 feet). The 3-meter minimum allows collisions to be more easily detected.
- Limiting the Ethernet cable run to 90 meters reserves 10 meters (33 feet) for patch cables at the patch panel and the networked device.

- Ensure all faceplates, modular connectors, patch panels and patch cords are the same category as the selected cable. That is, when you pull Category 6 cable, make sure all other components are rated for Category 6. If you are installing shielded cable, all other components including the patch panel must provide a location to terminate the ground wire.

Termination

Expected Ethernet Termination for Oracle MICROS Installations:

Several methods are available for terminating the horizontal cable runs. Oracle MICROS recommends the 110 Connect system by AMP or other suppliers. This system uses the reliable 110 style punch-down RJ45 modular jack and are available in both shielded and not-shielded versions.

A second termination method is based on the 8-pin RJ45 modular "keystone" insulation displacement connector, similar to those available for MICROS IDN devices. The cable is attached to this connector by placing all conductors in the appropriate connector cap and then forcing the connector cap into place.

In addition, there are two methods for terminating the cable at the faceplate connectors using the ANSI/TIA/EIA-568-A or ANSI/TIA/EIA-568-B cabling standard.

ANSI/TIA/EIA-568-B.1-2001 specifies that horizontal cables are terminated using the T568A pin/pair assignments, or optionally terminated with the T568B bin pairs to accommodate certain cabling systems. Mixing T568A terminated horizontal cables with T568B terminated patch cords (or the reverse) is not recommended.

> **NOTE:**
>
> Pins 1-2, 3-6, 4-5, and 7-8 are +/- signal pairs twisted with each other within the cable. You must maintain these signal pairs at each end of the cable as well as the patch cables.

Expected Fiber Optic Termination for Oracle MICROS Installations:

SC Connector

Expected Coaxial Termination for Oracle MICROS Installations:

F Type Connector

Expected IDN Termination for Oracle MICROS Installations:

IDN termination method is based on the 8-pin RJ45 modular "keystone" insulation displacement connector. The cable is attached to this connector by placing all conductors in the appropriate connector cap and then forcing the connector cap into place.

RJ45 and RJ12 connectors for workstation to printer

RJ12 connectors for daisy chain of printers

RJ45 connectors for wall outlets

Wireless

Infrastructure

Expected Hardware Features:

WI-FI 3

IEEE 802.11g WI-FI 3. Supports 2.4 GHz and 5 GHz frequency bands.

WI-FI 4

IEEE 802.11n WI-FI 4

Recommended Hardware Features:

WI-FI 5

IEEE 802.11ac

Wi-Fi-5 supports higher bandwidths and MIMO.

Rogue detection feature is recommended in any wireless network infrastructure.

Rogue Interfering APs and other devices that can potentially disrupt network operations.

Configuration

5 GHz and 2.4 GHz

Can I broadcast POS SSID in 2.4 and 5 GHz band?

Broadcasting POS SSID in both bands may have a negative effect on the performance because of band steering.

Band steering lets dual-band devices detect a higher radio frequency of 5 GHz band and allows the device to automatically transmit on that band.

POS devices require a stable and constant connection to the wireless network; therefore, any network connection interruptions result in poor service.

POS SSID should always be broadcasted in a single band.

Will my POS devices work well in the 2.4 GHz band?

POS devices connected to 2.4 GHz band may operate well in some conditions, providing there are no external interferences present, access points are positioned in a correct location with a clear path of broadcast, the Wi-Fi does not suffer bottlenecks, and the SSID per AP ratio is low.

A single property with three access points spaced in the correct proximity with a low number of client connections may offer good wireless coverage and performance.

The 2.4 GHz band can experience interference from different devices such as Bluetooth, Mobile phones, and microwave ovens.

5 GHz band preference

The 5 GHz is the preferred network for most vendors, as it suffers less interference from the internal and external environment.

Common non-Wi-Fi devices such as microwaves and CCTV RF sensors do not interfere with the network broadcast.

The 5 GHz band supports over 20 non-overlapping channels, depending on the region.

The availability of more none overlapping channels gives the 5 GHz band a distinct advantage in limiting the interference caused by neighboring Wi-Fi.

Connectivity table in 2.4 GHz

- **-30 dBm**

  Reliable network coverage offering good connection and uninterrupted data flow.

- **-65 dBm**

  Good network coverage with the reliable data flow.

- **-70 dBm**

  Minimum reliable distance and coverage. POS device may start experiencing latency.

- **-75 dBm**

  POS devices experience data flow problems, network timeouts and latency. Check functions may no longer be possible.

Connectivity table in 5 GHz 802.11ac

- **-30 dBm**

  Reliable network coverage offering good connection and uninterrupted data flow.

- **-65 dBm**

  Reliable network coverage.

- **-70 dBm**

  Good network coverage with the reliable data flow.

- **-75 dBm**

  Minimum reliable distance and coverage. POS device may experience latency.

SSIDs

SSIDs are created in the wireless network infrastructure to segregate internal and external client communication.

Some organizations may create many SSIDs in the wireless environment to fulfill business needs and requirements.

How do I determine the correct number of SSIDs serviced by each AP?

The number of SSIDs per AP depend on the hardware and its manufacturing limitations.

Some vendors may support many SSIDs to save costs but that can lead to latency and disruption to the service.

How SSIDs are apportioned across access points should always be carefully evaluated and must be based on the network demand and individual SSIDs bandwidth requirements.

Determination of the correct number of SSIDs and the number of access points is a crucial step in ensuring good client communication.

Who decides on the number of broadcasting SSIDs?

The vendor or the Wi-Fi provider should make an evaluation based on the following:

- The size of the property and coverage area
- Wireless network capacity and demand
- The bandwidth requirement for each SSID
- Hardware manufacture recommendations and limitations
- The approximate number of concurrent connections per access point
- Maximum connections allowed per radio

Will my wireless network operate efficiently if I have a high number of broadcasting SSIDs?

The wireless network will not operate efficiently if:

- The number of created and broadcasting SSIDs exceeds the manufacture recommenced level
- The number of connected clients in each SSID exceeds the client number threshold
- The number of connected clients to each access point exceeds the recommended threshold

Examples of ratios that may have a detrimental impact on the client communication:

- A low number of access points with a high number of broadcasted SSIDs

  Depending on the number of connected clients such an environment may experience a high number of client connection per access points and subsequent network failures. Network latency is the most common factor in saturated wireless networks.

- Incorrect bandwidth sizing

  An incorrect bandwidth sizing per SSID may lead to poor client performance and network latency.

- A high number of clients per SSID

  POS devices connected to a congested Wi-Fi will experience poor network performance and connection failures.

Such environments can cause data flow disruption and unreliable communication.

- **List of SSIDs that can have a negative impact on the POS network:**

  VoIP: Voice over IP solutions deliver real-time audio and video services to devices within the organization however the solution can be resource heavy.

  Guest Wi-Fi connection: Guests can benefit from the internal free Wi-Fi connection when using designated apps; however, a high number of connected clients can cause network latency.

> **IMPORTANT:**
>
> It may be necessary in some environments to create a dedicated POS Wi-Fi network within the existing infrastructure by removing the broadcast of heavy demanding SSIDs to lower the number of client connections.

Channels

What is channel overlapping?

Channel overlapping is caused by a minimum of two access points positioned in very close proximity.

The overlapping level is influenced by the access point's proximity, broadcasting channel, and power output.

When two wireless devices transmit at the same time, their radio signals collide and become distorted.

Channel management may not function correctly when the number of access points in the area exceeds the recommended number of installed radios as there are only three non-overlapping channels in the 2.4 GHz frequency.

How to prevent channel overlapping?

5 GHz offers more none overlapping channels and should always be the preferred band.

In situations where the 2.4 GHz band is required, the access points should be set to channels 1, 6, and 11, as these are non-overlapping channels.

A stable network is a key requirement for POS devices to operate correctly.

Simphony requires a stable network for all functions:

- Check Creation
- Check Access
- Check Sharing
- Tender Media
- Service Total
- Remote Printing
- Fiscal Operation

- Credit Card Payment
- POSAPI functions

Roaming

Roaming occurs when a POS device moves between the access points. The event is triggered by the signal strength level threshold.

When the signal from the access point the POS device is connected to drops below a certain level, the POS device connects to the stronger access point in the area that broadcasts the designated POS SSID.

During AP (Access Point) roaming, POS devices can experience a degree of network connection disruption which can negatively impact the performance.

In some cases, the disruption can cause the POS devices to be unusable leading to complete network connection failure.

Seamless roaming within the dedicated POS broadcasting access points and areas is essential, ensuring good communication within the system.

Roaming should be tested in all locations that the POS devices operate and all access points that the POS devices connect to.

> **IMPORTANT:**
>
> Perform roaming tests using a POS device and not a third-party device because not all wireless hardware components respond identically. Tests conducted using other Wi-Fi devices may produce different results because all wireless devices respond differently in specific circumstances and conditions.

Communication disruption during roaming:

One of the symptoms of bad roaming is prolonged loss of communication to POS devices.

During the connection blackouts, POS devices cannot support any online Simphony functions and may be deemed as offline.

The period in which it takes to reconnect between the access points should be kept to a minimum.

The greater the number of lost pings the higher chances of operational disruption that can lead to problems with data sharing between the POS devices and the system.

Ping data loss should be very low at a maximum of three lost pings while roaming between the access points. A high number of lost pings may result in an interruption to the service.

> **NOTE:**
>
> Ping command can be used to verify the number of lost pings.

Several design factors can impede seamless roaming:

- A high number of access points installed in the area

  Too many access points can prevent POS devices from being able to roam as the minimum RSSI advertised by the access point exceeds the required strength.

  POS devices will not roam between the access points if the minimum signal threshold does not drop below a certain level, regardless of other access points advertised in the area.

  POS devices may roam excessively if the roaming threshold has been frequently reached.

  The power output of each access point should not exceed the required coverage causing signal overlapping.

- Authentication issues

  Network authentication issues can prevent the POS devices from authenticating smoothly when roaming between the access points.

  Authentication problems may result in network communication failures and prolonged access point connection.

Roaming Aggressiveness POS Configuration:

This setting alters the signal strength threshold at which the Wi-Fi adapter starts scanning for another candidate AP. The default value is **Medium**. Depending on the environment, one option may work better than the other.

- **Lowest:** The Wi-Fi adapter will trigger a scan for another candidate AP when the signal strength with the current AP is very low.
- **Medium-Low**
- **Medium (default):** Recommended value.
- **Medium-High**
- **Highest:** The Wi-Fi adapter triggers a scan for another candidate AP when the signal strength with the current AP is still good.

Encryption

WEP - Wired Equivalent Privacy

WEP system is highly vulnerable. Do not use.

WEP was officially abandoned by the Wi-Fi Alliance in 2004.

WPA - Wi-Fi Protected Access

WPA applications use a Pre-Shared Key PSK, known as WPA Personal, and the Temporal Key Integrity Protocol **(**TKIP).

WPA Enterprise uses an authentication server for keys and certificates.

WPA, like WEP, is vulnerable to intrusion and is no longer recommended.

Expected Encryption

WPA2. Wi-Fi Protected Access

WPA2 uses Advanced Encryption Standard AES.

WPA2-Enterprise requires a RADIUS server.

RADIUS server handles authenticating tasks for all network users' access. The authentication process is based on the 802.1X policy.

Checklist

Summary of Oracle networking expectations:

- □ DHCP: Reserved IPs
- □ DHCP: NTP filter out Workstations
- □ DHCP: Lease length sufficient length to avoid business hours
- □ DNS: Local if using names rather than IPs
- □ STP: Switches support Spanning Tree Protocol
- □ Firewall: Documented, change procedures, audits in place and followed
- □ IDS/IPS: 'Allow' rules for Simphony
- □ Certificates: Trusted, not self-signed, TLS 1.2
- □ CRL: Verify endpoint configuration
- □ Proxy: Configure proxy-aware workstations
- □ VLAN: Segment POS network
- □ WAN: Verify sufficient bandwidth, redundancy
- □ LAN: Verify sufficient bandwidth, redundancy, availability
- □ Cabling: Correct type for bandwidth needed distance used
- □ IDN: Cat 6 or better
- □ Bandwidth: Calculate bandwidth needs and verify against WAN or LAN configuration
- □ Distance: Maximum distance not exceeded in cabling runs.
- □ Latency: Measure, confirm low latency to Oracle Cloud
- □ Physically Secure: Router, switch, networking equipment in secure, limited access location
- □ Powerline extender: Do not use
- □ Termination: Proper cable termination. Replace if you suspect the cable termination is old.
- □ Wi-Fi 5 or later
- □ Wi-Fi: 5 GHz and 2.5 GHz separated by use case
- □ SSID: Separate by use case

- ❑ Wi-Fi ratios: APs per SSID, bandwidth per SSID, clients per SSID, SSIDs on premises
- ❑ Wi-Fi: No channel overlap
- ❑ Wi-Fi: Roaming tested between all geographically neighboring APs.
- ❑ Wi-Fi Encryption: WPA2 only
- ❑ Power: All network hardware supplied by conditioned power and UPS protected. See Power Considerations for more information.
- ❑ Special property considerations: Validate special property considerations for casinos, cruise, hotels, resorts, and stadiums. See Special Property Considerations for more information

.

3 Special Property Considerations

Some networking topics are specific to particular property types. The following table provides a matrix of special property considerations and the property types where those considerations apply.

	Casino	Cruise	Hotel	Resort	QSR (Chain)	TSR (Chain)	QSR (Single)	TSR (Single)	Stadium
Multiple CAPS	X			X					x
Single Server On-Prem		X	X	X					X
Load Balanced On-Prem	X			x					
Load Balanced - Self-Host	X				X	X			
Jump Mind Replication		X							
High WS Count	X	X	X	X					X
Wi-Fi Dependent						X		X	
Wi-Fi Restricted Locations (Airports)					X	X			
Wi-Fi Hindered		X							
Subnet Spans	X	X		X		X			X
Corporate Proxy			X		X	X			
Corporate WAN			X		X	X			
Likely to use "Consumer" Routing HW							X	X	
Likely to Consider DHCP	X		X				X	X	X
Wide Physical Deployment Area	X	X		X					X
Internal VPNs	X			X					
Incoming Interfaces					X	X	X	X	
Outgoing Interfaces	X	X	X	X					

Consumer Routing Hardware

Due to the size of the implementation, there is likely more on site than consumer-grade network hardware.

There will be little in place with regards to firewalls, LAN, and proxies. Consider these points:

- This is likely unsuitable for larger installations
- Security is likely provided through NAT only
- The customer is likely to need a greater level of assistance in understanding their network

Corporate Proxy or WAN

Due to the size of the implementation, it is likely that at a corporate level, a proxy solution for web filtering has been implemented.

All internet web traffic is routed through the corporate proxy configured at the workstation level. This can create a single point of failure, but it can also create issues when valid web sites are blocked, or more commonly, not explicitly allowed. Consider these points:

- Proxy must be resilient
- Proxy configuration must be on each workstation
- Proxy must have whitelisting for all relevant URL endpoints

Corporate WAN

Due to the size of the implementation, it is likely that at a corporate level, a corporate WAN has been configured.

All network traffic will route through the corporate head office, by way of MPLS or VPN. This creates a private WAN, which ensures that all traffic is routed in the way set out by the Corporate IT and Security teams. Consider these points:

- WAN must be resilient, or could be single point of failure
- WAN edge firewalls/proxies must be configured correctly
- Proxy must have whitelisting for all relevant URL endpoints

DHCP

Through experience, we have found a number of these site types use dynamic IP ranging for their workstations.

EMC configuration needs to match the DHCP configuration, either by name or fixed DHCP lease IP configuration. Consider these points:

Simphony can work with DHCP clients. While this is technically not an issue, the broader question of whether DHCP is suitable and scalable should be considered. Per the main DHCP article, Oracle MICROS Simphony requires fixed IP leases and DNS resolution to be implemented.

High WS Count per Property or Wide Deployment Area

Due to service type, or physical size, some properties will have more workstations than others.

More workstations mean more IP addresses are required, greater broadcast traffic when check sharing, a larger physical footprint, and a likelihood for wireless to be more prevalent. Consider these points:

- Workstations are more likely to span multiple IP Subnets. Firewalls and gateways should be configured so that traffic is unhindered as it traverses this.
- CAPS will be under a higher load and should be considered for install on a dedicated IIS machine.
- Wireless should be considered carefully.
- Workstation downloads and DB Updates will be downloaded multiple times. This will increase peak WAN loading.

Internal and External Interfaces

Incoming Interfaces

Due to service type, these properties will likely have incoming interfaces, such as kiosks or Internet ordering.

There are IP-based incoming channels of data to the system, rather than just the operator creating orders. This means the External Internet connection can become a key component of the ordering system, rather than just sales data collection. Consider these points:

- Firewall configurations inbound as well as outbound
- Internet connection can become mission critical

Outgoing Interfaces

Due to service type, these properties will likely have outgoing interfaces, such as Order Confirmation Boards or PMS Sales IFC.

There are IP based outgoing channels of data from the system, additional to sales data collection. Consider these points:

- Firewall configuration outbound
- Internet connection can become mission critical

JumpMind Replication

Due to regulatory requirements and physical location, these implementation types are likely to require multiple DB instances, replicated through the JumpMind product SymmetricDS.

The database and installation are customized to support the symmetric DS product.

While this is a separate product that requires a large amount of configuration and maintenance, it has a large benefit in that when there is a low stability to the cloud servers, a local instance of the cloud database is replicated. This can give the system the advantages of being local from a connectivity point of view, without removing the control of having a cloud-based instance that is administered by a central entity. Consider these points:

- Both data centers need to be secured; ensure communication between the two is clean and clear.
- There can be a much larger time delay between pressing save on the primary EMC, and this being replicated to the secondary servers.
- Upgrades will need to be planned in tandem.
- There are likely to be constraints added with regards to data maintenance and data access that would not normally exist.
- Whilst configuration can come from a central entity, reporting data is not returned to them.

Single Server On-Premise

Due to regulatory requirements, physical location or customer requirements, these implementation types are likely to have a server on site dedicated to an installation.

The cloud becomes local and resides at the address of the deployment. This simplifies data flows, but, due to the design of SSL or connected interfaces, can still require Internet access.

When a server is hosted on premise, the DNS records and SSL CRL endpoint need to be configured to be accessible by the workstations successfully. This requires an Internet connection and an internal DNS server infrastructure.

Operating system and database patching and maintenance also require more coordination than with a load balanced on-premise installation, as a server reboot requires a full cloud outage.

Load Balanced Servers On-Premise

Due to regulatory requirements, physical location or customer preference, these implementation types are likely to have a server farm on site dedicated to an installation.

Just like a single server on premise, the cloud becomes local and resides at the address of the deployment. There is, however, a load balancer sharing load amongst the application nodes. This simplifies data flows, but, due to the design of SSL or connected interfaces, can still require internet access. Consider these points:

When a server is hosted on premise, the DNS records and SSL CRL endpoint will need to be configured to be accessible by the workstations successfully. This requires an Internet connection and internal DNS server infrastructure.

Load Balanced Servers Self-Hosted

Due to regulatory requirements, physical location or customer preference, these implementation types are likely to have a server farm in a remote location across multiple properties.

Just like self-hosted on premise, when the customer hosts their own server farm in a non-Oracle data center, the customer is responsible for all aspects of the installation, including but not limited to operating system patching, application patching, load balancer configuration, SSL certificates, server firewalls, server uptime and database maintenance

When the customer hosts their own server farm in a non-Oracle data center, they are published to the Internet. IDS/IPS should be implemented along with accurate firewalls to ensure that public access is not abused.

Multiple CAPS

When a physical deployment gets to a certain size, customers might want to break down their installation to multiple logical properties within the EMC. This can assist with IT configuration, reporting, or sizing of infrastructure. For this approach, each Simphony property needs a separate CAPS machine.

Multiple CAPS machines impact the data flow from the property-level components to the cloud and at the local level between nodes. Barring misconfiguration, Property 1’s workstations should not reach out to Property 2’s workstations.

The workstation listing within the EMC should be configured in a way that ensures that IP addresses are not duplicated across properties. This is a manual effort. Where possible, using VLAN segments provides a secondary safeguard.

Multiple Subnets

Due to the building size or configuration, the IP ranges that the workstations reside on are split into multiple separate subnets.

If correct routing is not implemented as subnets are traversed, Simphony on-premise components will not communicate correctly. Consider these points:

Bi-direction subnet traffic needs to be open.

Wi-Fi-Dependent/Hindered/Restricted Property

Wi-Fi-Dependent Property

Businesses reliant on wireless technology are more likely to have a higher ratio of wireless to wired devices, and they could be operationally more dependent on Wi-Fi for all aspects of the business.

This property type could have the following impact:

- Could cause higher demand on the wireless bandwidth due to increased number of operating wireless devices.
- Internal and external communication are reliant on wireless technology.
- A high number of concurrent client connections

Consider these points:

- Sufficient bandwidth allocation
- Latency
- Robust WLAN hardware and reliable wireless technology

Wi-Fi-Restricted Property (Airports)

Businesses operating in large infrastructures such as airports, government institutions, and hospitals operate with restricted guidelines. This could have the following impact:

- IP addresses and subnets ranges will be restricted
- Multiple subnets will be provided for the hardware
- More likely to operate in a higher number of broadcasting access points
- Will have no control over AP SSID broadcast
- Higher number of shared access points
- Will have a restricted network access
- MAC address filtering could be introduced due to security requirements
- Higher number of concurrent connected clients per AP’s
- High number of broadcasted SSIDs per AP
- POS SSID broadcast could be hidden

Consider these points:

- More diligent testing may be required
- POS devices are more likely to suffer client congestion
- Limited system testing due to security restrictions
- Limited access to the system and network infrastructure

Wi-Fi-Hindered Location (Cruise Ships)

Access point’s position could be restricted due to internal structures.

Structures and heavy materials could have an impact on the wireless broadcast and performance.

Wireless interference may be more common because of complex structural design.

Some areas may not have a sufficient wireless coverage causing connection blackouts.

Offline mode is more frequent at this property type.

Consider these points:

- Disrupted check sharing process caused by frequent offline instances
- POS devices online recovery process
- Interrupted communication
- Complete communication blackouts
- Financial discrepancies caused by communication issues

4
Power Considerations

Power Requirements

AC Power

A correct installation of the AC power and grounding system is essential to minimize voltage spikes and possible damage to the network system.

In cases where grounding is not possible, an additional power conditioner may be required to meet safety requirements.

Additional information can be found in the *Oracle MICROS Site Preparation Guide*. The guide provides detailed best practice information and covers all aspects of site installation.

> **NOTE:**
>
> For more information on the power requirements please refer to chapter 23 of the site preparation guide.

Power over Ethernet (POE)

Network hardware, such as access points, can benefit from POE.

> **IMPORTANT:**
>
> By protecting a POE switch with battery backup and line conditioning, all devices connected to that switch through POE benefit from that protection. This is important for access point wireless infrastructure.

POE cabling should be categorized by the bandwidth equipment.

Ethernet cabling used with POE is limited by the same distance restrictions as with standard networking usage.

POE Power Standards

Type	IEEE Standard	Power per Device
1	802.3af	15.4 Watts
2	802.3at	30.8 Watts
3	802.3bt	60 Watts
4	802.3bt	90-95 Watts

POE can reduce the need for installation of electrical cable and outlets for networked devices in the point-of-sale environment.

These devices may benefit from POE:

- Network switches
- Wireless access points
- Credit card terminals
- CCTV devices
- RFID readers
- Smart devices

Power Conditioning

As all electrical installations experience power surges and voltage spikes, it may be necessary to consider a power conditioning solution. A power conditioner is a device designed to monitor and regulate power, delivering clean power to any electrical equipment.

Power conditioning means protecting electronic and electrical devices from electrical damage.

Several types of solutions and protective hardware can be implemented by the vendor, but in all cases, it depends on the need and the size of the property.

Like all electrical devised POS systems, it is also prone to hardware failures when operating in unprotected environments.

POS system hardware will benefit from the protected system, as it can prevent frequent hardware failures that can lead to increased costs of repair.

Hardware failures caused by electrical spikes can negatively impact business operations and can lead to financial losses; therefore, installation of protective hardware is recommended.

All electronic and electrical network devices require power protection if the environment they operate is prone to electrical spikes and surges.

Oracle point of sale systems require Oracle MICROS-approved power conditioning and uninterruptible power supplies.

Oracle MICROS-approved power conditioners that protect the point of sale and network devices must be able to isolate all negative electrical instances generated by any other equipment.

A power conditioner has a low-impedance isolation transformer to protect the equipment from common-mode voltage, which can cause everything from equipment lockups to data losses.

See the *Oracle MICROS Site Preparation Guide* for more information on power conditioners.

Surge Protectors

Surge protectors provide a degree of protection and can prevent protection from transient power spikes; however, they cannot provide complete full protection.

For full protection, use a UPS or a power conditioner.

Surge protectors are not recommended for use with networking or point of sale equipment.

Uninterruptible Power Supply (UPS)

A UPS provides emergency power in case of a utility power outage. A UPS can provide immediate power to computers. A UPS can also cleanly shut down a computer avoiding damage to hardware and software.

UPS devices are available in desktop, tower, or rack mount models. The UPS chosen depends on site-specific requirements.

The UPS provides the following:

- Battery backup
- Protection from surges
- Protection from brownouts
- Protection from voltage spikes
- Protection from electromagnetic interference

5
Cloud Connectivity

Connecting to the cloud refers to a connection between front-of-house applications to the application server tier. This includes instances of Simphony installed on-premises, in a data center, or an Oracle-hosted data center. Connection requirements from the client to the server remain the same.

API Connectivity

An application program interface (API) is a set of routines, protocols, and tools for building software applications. This allows software to interact with other software.

In Simphony, an API is leveraged to let external systems interact with the core system to support operations such as:

- Importing into Simphony from an external system
- Remote orders from a mobile app
- Exporting employee data for a third-party payroll

Import/Export API

The Simphony import/export API allows automatic importing of objects like menu items into Simphony. Objects can also be exported to external systems, such as an inventory system.

Connectivity to the Simphony Import/Export API is done by allowing access to the following URL example: (https://*ServerName*/ImportExportAPI/)

It is commonplace that working with 3rd party vendors, that they would be directed to the API documentation so they can start building and connecting.

For more information, see the Simphony Import/Export API documentation at: https://docs.oracle.com/en/industries/food-beverage/pos.html.

Labor Management API

Labor Management provides SOAP and REST APIs to retrieve information through an HTTP or HTTPS connection. The API supports the following transfer protocols to handle different sets of data:

Simple Object Access Protocol (SOAP)

You can use the SOAP APIs to modify and retrieve employee data through methods that:

- Retrieve employee details by name, external payroll ID, and payroll ID
- Retrieve portal user details Retrieve point-of-sale (POS) roles
- Create new employees and portal users
- Modify the information of existing employees and portal users
- Transfer employees from one home store to another
- Assign employees to an away store
- Terminate employees
- Place employees on leave of absence Rehire employees
- Change employee pay rates
- Create timecards for employees
- Retrieve employee timecard details
- Retrieve labor details for a location
- Retrieve location details
- Retrieve job code and job category details
- Assign magnetic card numbers for home stores

Representational State Transfer (REST)

You can use the REST API to access Reporting and Analytics Advanced modules from mobile devices and tablets through methods that:

- Retrieve all employee details for a location
- Retrieve details for one employee
- Retrieve all locations for an organization
- Retrieve information for one location
- Retrieve all timecard punches for a location
- Retrieve information for all versions of a REST API
- Retrieve information for a specific API version
- Authentication and Authorization

Authentication and Authorization

SOAP endpoints (http://*ServerName*/labor/labor?wsdl) and REST endpoints use an API token and password to authenticate client requests. You generate the token and password by creating an API user in the Reporting and Analytics portal. Create API Users provides more information. For SOAP API calls, you specify the token and password in the SOAP header as a Username Token parameter in WS-Security. For REST API calls, you specify the token and password in the HTTP request header. Authentication provides more information. All endpoints are accessible through HTTPS, which makes the communication channel secure. It is the responsibility of the client that consumes these APIs to securely store authentication credentials.

Transaction Services

Transaction services let external systems connect to a transaction services client within the property.

A transaction service client needs to be created in the EMC and attached to a workstation record.

Firewall rules should allow and forward 8080 requests to the transaction services client to consume transaction services utilizing the correct URL and TS Web Service.

An example of a URL for a transaction services client is:
http://*WorkstationIPAddress*:8080/EGateway/SimphonyPosApiWeb.asmx

Consult with your third-party vendor and provide them with a link to the Transaction Services API documentation so they can start building and communicating with transaction services.

Bandwidth Sizing Requirements

Bandwidth Overview

Bandwidth considerations consist of normal operations and reloading of a workstation's database.

Normal operations are carried out on a normal day-to-day basis. These operations include:

- Transactions
- Printing of checks
- Peer communications to the Check and Posting Service (CAPS)
- Database Synchronization (DBSync) - New information entered through the Enterprise Management Console (EMC) and synced to the workstation in a pre-set cadence.

NOTE:

DBSync times can be adjusted to be more often or less often depending on the needs of the customer.

Reloading of a Workstation Database:

Reloading or refreshing a database can invoke a larger data payload to the workstation, which increases the bandwidth usage.

All functions pull down incremental change data, unless the workstations last update time is older than the oldest record in the DB sync change table – which can happen when the client is offline for a while. When this occurs, the client does a full DB download to ensure no data is missing. The following is a list of database functions that can affect bandwidth:

- The **refresh** button uses the same mechanism as the standard DB sync, which causes the client to get the latest configuration changes in the EGateway service's cache on the application server. The update happens in the background shortly after pressing the button.
- The **refresh live** button uses the same mechanism as the standard DB sync, which causes the client to get the latest configuration changes in the EGateway service's cache on the application server. The update happens in the foreground and the operator must wait for it to complete.
- The **update** button bypasses the EGateway cache and makes the service query the database directly to pull out the configuration changes since the last definition update was obtained. The update happens in the foreground and the operator must wait for it to complete.

It can take a few minutes for the changes saved to the database to propagate to the EGateway cache and become available for download. If you want something to happen right away, use the update button. The update function stresses the database, unlike the refresh button which pulls from the data cached on the application server.

Other Considerations

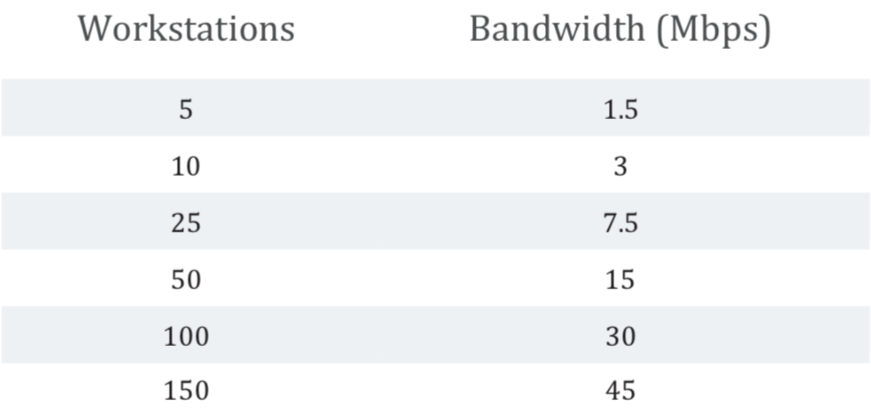
Another action to consider when considering bandwidth calculation is the use of CAL. While this is typically a one-time occurrence that happens during the installation of your Simphony system, the CAL process includes the downloading of all the configured database items as well as the entire file structure that the workstation uses to run Simphony. An example of a scenario that would cause a variance would be the total amount of workstations. If a 4-workstation system running on a 1.554 MBPS line are all running CAL at the same time, it could take 10 minutes to complete. A 200-workstation system is running on a 1.554 MBPS line are all running CAL at the same time, it could take upwards of an hour to complete.

A final consideration is the use of connections to external systems through transaction services and labor. While transaction services and labor carry a small footprint, the need for more bandwidth increases. Transaction services allows an external system (i.e., online ordering) to create a connection to the property to send orders to the Simphony POS system.

To calculate bandwidth by workstation:

- Number of physical workstations = W
- W x 0.02 Mbps = Total Workstation Bandwidth during normal operations.
- W x 2 Mbps = Total Workstation Bandwidth when performing a reload of a workstation's database.

These formulas result in the following estimations:



Workstations	Bandwidth (Mbps)
5	1.5
10	3
25	7.5
50	15
100	30
150	45

Oracle Cloud

Connection to Applications

Connectivity for the Simphony Application

Full communication to the assigned URL over port 443 is required for CAL authentication and day-to-day database sync. Failure to allow access results in installation issues and sales totals not sending from the Check and Posting Service to the cloud.

All workstations must have access to the certificate authority CRL list to ensure that CAL authentication can happen. See the Security Guide for your Simphony version for more information.

Simphony Cloud Services are available through the Oracle Cloud Infrastructure (OCI) Load Balancer as a Service (LBaaS) technology based on TCP specifications. In some scenarios - particularly for larger properties or enterprises (where a substantial number of devices are connecting to the Simphony Cloud Service via a single NAT address) - certain customer firewall devices can have default configurations that conflict with these standards resulting in issues with specific Simphony workstation functionalities, such as DB Download. Oracle recommends using the following configurations listed below when available on the customer firewall device:

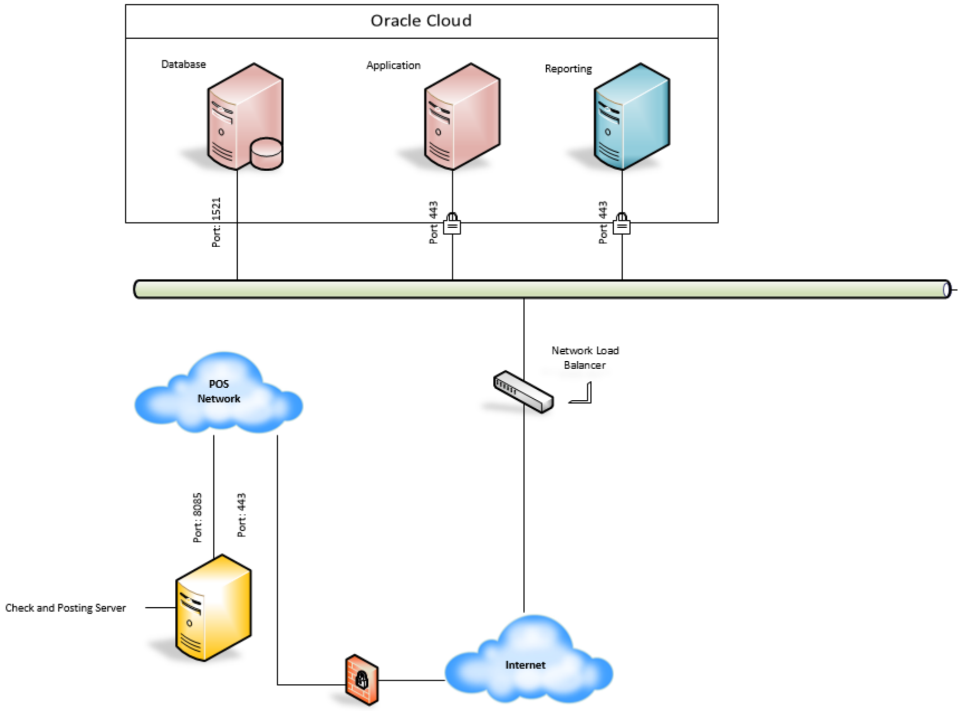
- TCP Time Wait Recycle – ENABLED
- TCP Time Wait – 60 seconds or greater
- TCP Sequence Randomization – DISABLED

Image Locations for Kiosks

To ensure Kiosks can display images that have been configured through the EMC, and which are hosted in the Oracle Cloud, connectivity must be provided to the regional image repository associated with your Simphony installation. For more information on allowing access to Oracle Cloud-hosted services, see IP Address Ranges.

Connectivity for Oracle MICROS Reporting and Analytics

Full communication through HTTP and HTTPS to the Reporting and Analytics server is needed for reporting. For Oracle Cloud customers, this URL is provided to you after server provisioning has been completed. For self-installed Simphony systems, this is the fully qualified domain name (FQDN) or server name.



Peer to Peer Network Connectivity

Check and Posting

Check and Posting uses port 8080 by default. It is recommended to change this port when running ServiceHost as a service or running CAPS on IIS.

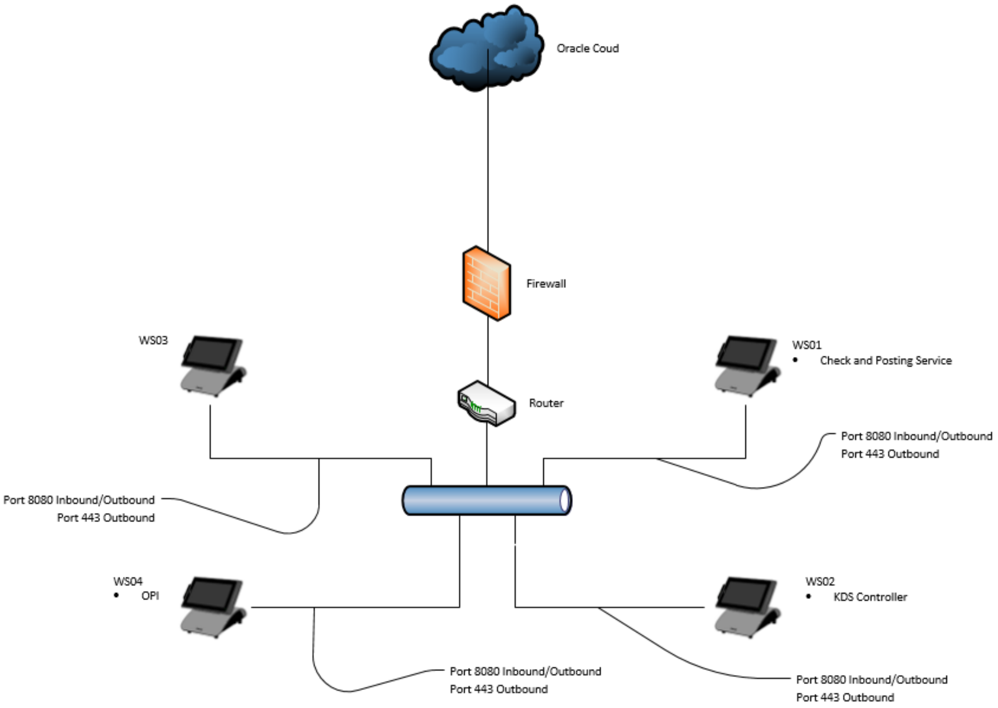
See **Property Parameters** in the Enterprise Management Console (EMC) to determine which port is being used for the Check and Posting Service (typically 8071, 8080, or 8085 depending on how CAPS is configured. This information is also provided to you by Oracle Consulting at the time of installation of the CAPS server.

Workstations

Workstations (ServiceHost) use port 8080 for peer-to-peer communications through the Simphony EGateway service.

Best Practice

As a best practice, set up your workstations to use the IP address (using Static IPs) as the host name in EMC. This is especially useful when in a network where DNS is set up incorrectly, if at all.


Oracle Coud
Firewall
Router
WS03
WS01
• Check and Posting Service
Port 8080 Inbound/Outbound
Port 443 Outbound
Port 8080 Inbound/Outbound
Port 443 Outbound
WS04
• OPI
WS02
• KDS Controller
Port 8080 Inbound/Outbound
Port 443 Outbound
Port 8080 Inbound/Outbound
Port 443 Outbound

Web Services

Labor Management Web Service

The web service runs on the Reporting and Analytics server that allows incoming connections to a specified labor URL.

The web service should be able to connect to:

- http://*ServerName*/labor/labor?wsdl
- https://*ServerName*/labor/labor?wsdl

If you have connection to your Oracle MICROS Reporting and Analytics server, you will have connection to the labor web service.

Optimally, each store should connect via a persistent IP network, alternatively and as a backup a dial-up IP connection may be used. The interface does not require each store have a public and/or static IP address allowing connection via more economic third-party ISP services. The interface is transport layer independent and as such supports many different IP connection methods such as DSL, frame, satellite, ISDN, cable and dial-up.

Gift and Loyalty Service

Oracle MICROS Gift and Loyalty lets you use loadable cards (gift cards) and create loyalty programs for patrons.

The Gift and Loyalty service runs on its own server to allow the Simphony system and web sites to connect to it.

The POSI posts a SOAP request to the iOS, which processes it and returns a SOAP response. Typically, the iOS requires one to two seconds to process the request before returning the response. Typical end-to-end transaction times using HTTPS over a broadband connection are 4-10 seconds. This includes the time required to perform the HTTPS authentication.

```
rintln(requestXml);

CRC32 crc = new CRC32();

crc.update(requestXml.getBytes("UTF-8"));

String crcValue = Long.toHexString(crc.getValue()).toUpperCase();

System.out.println(crcValue);
```

Optimally, each store should connect through a persistent IP network. As a backup, a dial-up IP connection can be used. The interface does not require each store have a public or static IP address allowing connection through more economic third-party ISP services. The interface is transport layer independent and as such supports many different IP connection methods such as DSL, frame, satellite, ISDN, cable and dial-up.

6

Network Infrastructure

This chapter provides contextual information that supplements information in Oracle Networking Expectations.

Network infrastructure refers to the resources network or internet connectivity, management, business operations and communication possible. Components include hardware and software systems that manage communication between users, services, applications, and processes.

The primary components of a network can be broken down into three categories:

- Hardware: Cables, LAN cards, switches, routers, wireless routers, and more
- Software: Network security applications, firewalls, operating systems, network management, network operations, and more
- Services: IP addressing, Load Balancing, Security protocols, wireless protocols, LAN service protocols (such as VLAN, VPN, Spanning Tree Protocol), and more

For hardware, software, and services to function together in a seamless manner, there are standardized processes, which enable any component in the network to operate no matter the component developer. Hardware, applications, services, and protocols should all work together. The Open Systems Interconnect (OSI) Model is the framework developed by the International Organization for Standardization (ISO) to give every network part a common reference point.

The OSI model is described as follows:

Layer 7 (Application; for example, SNMP, HTTP, FTP): Most of what the user interacts with is at this layer. Web browsers and other internet-connected applications (like Skype or Outlook) use Layer 7 application protocols.

Layer 6 (Presentation; for example, encryption, ASCII, PNG, MIDI): This layer converts data to and from the Application layer. In other words, it translates application formatting to network formatting and vice versa. This allows the different layers to understand each other.

Layer 5 (Session; for example, Syn/Ack, NetBIOS): This layer establishes and terminates connections between devices. It also determines which packets belong to which text and image files.

Layer 4 (Transport; for example, TCP, UDP, port numbers): This layer coordinates data transfer between system and hosts, including error-checking and data recovery.

Layer 3 (Network; for example, IP, Routers, Ethernet, Wi-Fi): This layer determines how data is sent to the receiving device. It’s responsible for packet forwarding, routing, and addressing.

Layer 2 (Data Link; for example, MAC, Switches, Fiber Optic): Translates binary (or BITs) into signals and allows upper layers to access media.

Layer 1 (Physical; for example, cable, RJ45): Actual hardware sits at this layer. It transmits signals over media.

What are the benefits of a planned Network Infrastructure?

Scalability. A solid network infrastructure supports the growth of your business without having to redesign your network.

Cost-effectiveness. A well-designed infrastructure will result in fewer network disruptions helping to keep down overall cost.

Security. Managed network services provide enhanced security and protection from interruptions like spam, malware, and viruses, while also keeping your data safe and secure.

Efficiency. Creating a secure network infrastructure minimizes downtime and ensures that productivity remains as consistent as possible.

Location. Network infrastructure enables sites to be connected to your network, no matter the location.

The following network topics are discussed in this chapter:

- Dynamic Host Configuration Protocol (DHCP)
- Domain Name Space (DNS)
- Load Balancing
- Spanning Tree Protocol (STP)
- Security

Dynamic Host Configuration Protocol (DHCP)

DHCP is a mechanism for centralizing the Internet Protocol (IP) and network parameter assignment within a network segment. A workstation configured to use DHCP service operates in four main phases:

- Server discovery: DHCP client sends a broadcast DHCPDISCOVER message onto the network subnet to any listening DHCP servers
- IP lease offer: when a DHCP server receives the DHCPDISCOVER message, it reserves an IP address and makes a lease offer by sending a DCHPOFFER message back to the DHCP client
- IP lease request: DHCP client replies to the offer with a DHCPREQUEST message broadcast back to the server requesting the DHCP offer
- IP lease acknowledgement: DHCP server receives the DHCPREQUEST message and send a DHCPPACK packet back to the client which includes the lease duration and configuration information such as IP address, subnet mask, default gateway, Domain Name Service (DNS)

If using MAC reservations on the DHCP server, regardless of the lease length, the IP address for a NIC would always be the same. This removes the need for DNS resolution at the workstation at the expense of configuration on the DHCP server.

Why would I want to use MAC Reservations, rather than just assigning IPs manually?

DHCP as a protocol, can define a Proxy Auto Configuration (PAC) endpoint, as well as a static IP Routes. In complex LAN configurations, as found in casinos, resorts, and stadiums, this can be seen as a large plus.

Windows CAL (running on Microsoft Windows 7 or higher operating system) can use PAC scripts.

Why would I not want to use DHCP?

When a client uses DHCP, primarily the IP Address is not fixed, and, depending on the lease length, can change at varying points in the day. This can cause issues with Peer-to-Peer communications. One way around this is using DNS Name resolution, however, this then means every message sent to a workstation, requires a confirmation from the DNS Server/Cache that the IP address has not changed, and is still valid. This can add Lag.

Domain Name System (DNS)

IP addresses are utilized over TCP/IP networks. Every computer in a network has a name. Names are easier to remember than IP addresses. DNS is a protocol that converts these FQDN (fully qualified domain name) to IP addresses. DNS servers maintain a directory of domain names and IP address mappings. This allows for both name to IP address and IP address to name resolution within the network. This means rather than attempting to connect to an IP address, a client can submit a resolution request to a DNS Server.

When a client submits a domain name to a DNS server for resolution, the server will either resolve the name to an IP within its local cache or reach out to a further node to obtain the IP for the client.

Why would I want to use DNS?

DNS is a core feature of IP networking today. Without DNS, SSL Certificates cannot be validated against a valid domain, as well as load balancing difficulties and IP sharing not being possible in data centers.

Valid DNS configuration is as much a requirement as having an internet connection itself.

Why would I not want to use DNS?

A DNS client is reliant on a DNS Server being available when a request is made. For local traffic, this could create a single point of failure, or a bottleneck.

Do I need to host my own DNS Server?

A local DNS Server would be required if the workstations are communicating via workstation Name, rather than by IP.

Load Balancing

Load balancing refers to efficiently distributing incoming network traffic across a group of backend servers, also known as a server farm or server pool.

Modern high-traffic websites must serve hundreds of thousands, if not millions, of concurrent requests from users or clients and return the correct text, images, video, or application data, all in a fast and reliable manner. To cost-effectively scale to meet these high volumes, modern computing best practice generally requires adding more servers.

A load balancer acts as the “traffic cop” in front of your servers and routing client requests across all servers capable of fulfilling those requests in a manner that maximizes speed and capacity utilization and ensures that no one server is overworked, which could degrade performance. If a single server goes down, the load balancer redirects traffic to the remaining online servers. When a new server is added to the server group, the load balancer automatically starts to send requests to it.

Load Balancing Algorithms

Different load balancing algorithms provide different benefits; the choice of load balancing method depends on your needs:

- Round Robin: Requests are distributed across the group of servers sequentially.
- Least Connections: A new request is sent to the server with the fewest current connections to clients. The relative computing capacity of each server is factored into determining which one has the least connections.
- Least Time: Sends requests to the server selected by a formula that combines the fastest response time and fewest active connections. Exclusive to NGINX Plus.
- Hash: Distributes requests based on a key you define, such as the client IP address or the request URL. NGINX Plus can optionally apply a consistent hash to minimize redistribution of loads if the set of upstream server’s change.
- IP Hash: The IP address of the client is used to determine which server receives the request.
- Random with Two Choices: Picks two servers at random and sends the request to the one that is selected by then applying the Least Connections algorithm (or for NGINX plus the Least Time algorithm, if configured).

X-Forwarded- Headers

When using a load balancer, it is not the clients that are connecting to the application servers, but the load balancer in the middle. The application servers lose the metadata as to who is connecting to them and how. The X-Forwarded- HTTP Header set allows this data to be added back in and consumed. This is important for some applications, and useful for others. The following X-Forwarded- Headers are recommended to be configured for all Oracle Food and Beverage web applications:

- X-Forwarded-For
- X-Forwarded-Scheme <<Scheme/Proto?>>
- X-Forwarded-Proto <<Scheme/Proto?>>
- X-Forwarded-Host

Spanning Tree Protocol

Switches can be used to create redundant connections in a network. If proper controls are not in place, redundant connections can cause switching loops. Consider the following example:

Three switches in a network are connected: Switch A, Switch B and Switch C. Switch A receives an unknown unicast from a PC and forwards it to Switch B and C. If the destination MAC address is not known by either Switch B or C, the unicast is sent back to Switch A and the same process repeats again and again until the traffic brings down the network.

The Spanning Tree Protocol (STP) identifies links in the network and shuts down the redundant ones eliminating possible switching loops. Switches that support STP have the protocol enabled by default. STP-enabled switches use a frame called a BPDU (bridge protocol data unit) to communicate with all switches, keep track of changes in the MAC address table and prevent potential loops in the network.

Security

Network security is any activity designed to protect the usability and integrity of your network and data.

- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

The following are some of the key threats that affect the site:

- Service disruption: Botnets, malware, adware, spyware, viruses, DoS attacks (buffer overflows and endpoint exploitation), Layer-2 attacks, and DDoS on services and infrastructure.

- Unauthorized access: Intrusions, unauthorized users, escalation of privileges, IP Spoofing, and unauthorized access to restricted resources.
- Data disclosure and modification: Sniffing, man-in-the-middle (MITM) attacks of data while in transit.
- Network abuse: Peer-to-peer and instant messaging abuse, out-of-policy browsing, and access to forbidden content.
- Data leak: From servers and user endpoints, data in transit and in rest.

The following are the key requirements to be satisfied for a secure site design:

- Service availability and resiliency
- Prevent unauthorized access, network abuse, intrusions, data leak, and fraud
- Ensure data confidentiality, integrity, and availability
- Ensure user segmentation
- Enforce access control
- Protect the endpoints
- Protect the infrastructure

This section discusses the following topics:

- Firewalls
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- Certificates
- Proxy
- Virtual Local Area Network (VLAN) and Virtual Private Network (VPN)

Firewalls

Firewalls prevent unauthorized access of a third-party in a private network. These are the network security systems (hardware- and software-based) that monitor and control the traffic flow between the Internet and the private network based on a set of user-defined rules. Firewalls shield the computer network of an organization against unauthorized incoming or outgoing access and renders the best network security.

There are three basic types of firewalls that are used by companies to protect their data and devices to keep destructive elements out of network, viz. Packet Filters, Stateful Inspection and Proxy Server Firewalls.

Packet Filters

Packet Filter Firewall controls the network access by analyzing the outgoing and incoming packets. It lets a packet pass or block its way by comparing it with pre-established criteria like allowed IP addresses, packet type, port number, etc. Packet filtering is suitable for small networks, but it gets complex when implemented in larger networks. These types of firewalls cannot prevent all types of attacks. They can neither tackle the attacks that use application layers vulnerabilities, nor can they fight against spoofing attacks.

Stateful Inspection

Stateful Packet Inspection (SPI), which is also sometimes called dynamic packet filtering, is a powerful firewall architecture that examines traffic streams from end to end. These smart and fast firewalls use an intelligent way to stop unauthorized traffic by analyzing the packet headers and inspecting the state of the packets along with providing proxy services. These firewalls work at the network layer in the OSI model and are more secure than basic packet filtering firewalls.

Proxy Server Firewalls

Also called the application level gateways, Proxy Server Firewalls are the most secure type of firewalls that effectively protect the network resources by filtering messages at the application layer. Proxy firewalls mask your IP address and limit traffic types. They provide a complete and protocol-aware security analysis for the protocols they support. Proxy Servers offers the best Internet experience and results in the network performance improvements.

No matter which firewall you select, ensure it is properly configured, as any loophole can cause more damage than no firewall at all. Create a secure network and deploy a suitable firewall to limit the access to your computer and network.

IDS and IPS

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)

Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) are both parts of the network infrastructure. IDS/IPS compare network packets to a cyber threat database containing known signatures of cyberattacks and then flag matching packets. The main difference between them is that IDS is a monitoring system, while IPS is a control system. IDS don't alter the network packets in any way, whereas IPS prevents the packet from delivery based on the contents of the packet, much like how a firewall prevents traffic by IP address.

Intrusion Detection Systems (IDS): Analyze and monitor network traffic for signs that indicate attackers are using a known cyber threat to infiltrate or steal data from your network. IDS systems compare the current network activity to a known threat database to detect several kinds of behaviors like security policy violations, malware, and port scanners.

Intrusion Prevention Systems (IPS): Live in the same area of the network as a firewall, between the outside world and the internal network. IPS proactively deny network traffic based on a security profile if that packet represents a known security threat.

Both IDS and IPS read network packets and compare the contents to a database of known threats. The primary difference between them is what happens next. IDS are detection and monitoring tools that don't act on their own. IPS is a control system that accepts or rejects a packet based on the ruleset. IDS requires a human or another system to look at the results and determine what actions to take next, which could be a full-time job depending on the amount of network traffic generated each day. IDS makes a better post-mortem forensics tool for the CSIRT to use as part of their security incident investigations.

The purpose of the IPS is to catch dangerous packets and drop them before they reach their target. It's more passive than an IDS, simply requiring that the database gets regularly updated with new threat data.

Point of emphasis: IDS and IPS are only as effective as their cyberattack databases. Keep them updated and be prepared to make manual adjustments when a new attack breaks out in the wild and/or the attack signature isn't in the database.

IPS and IDS vs Firewalls

Not having an IPS system results in attacks going unnoticed. A firewall does the filtering, blocking, and allowing of addresses, ports, service, but also allows some of these through the network. However, this means that the access allowed is just let through, and firewalls cannot tell whether that traffic is valid and normal. This is where the IPS and IDS systems come into play.

So, where firewalls block and allow traffic through, IDS and IPS detect and look at that traffic in close detail to see if it is an attack. IDS and IPS systems have sensors, analyzers, and GUIs to do their specialized job.

IPS and IDS Systems

IPS and IDS systems are used for the following types of attacks:

- Policy Violations: Rules, protocols and packet designs that are violated. An example would be an IP packet that are incorrect in length.
- Exploits: Attempts to exploit a vulnerability of a system, application, or protocol. An example would be a buffer overflow attack.
- Reconnaissance: Is a detection method that is used to gain information about system or network such as using port scanners to see what ports are open.
- DOS, DDOS: This is when an attack attempts to bring down your system by sending a vast number of requests to it such as SYN flood attacks.

Certificates

A certificate is a digital file containing information issued by a trusted Certificate of Authority (CA) that indicates the server or website endpoint communication is secured using an encrypted connection.

Certificate Types

- Domain-Validated (DV): Checked against a domain registry to prove ownership of the site but does not offer any identifying organizational information. The CA can typically validate through email, DNS, or HTTP. Easy to validate and least secure because very little information is required.
- Organization-validated (OV): Checked against a domain registry to prove ownership of the site, as well as location, particular country, state, and city. The CA can typically validate through email, DNS, or HTTP. Takes longer to validate and more secure than domain-validated since more information is required.
- Extended Validation (EV): Checked against a domain registry to prove ownership of the site, as well as location, particular country, state, and city. In addition, the certificate authorities only grant these kinds of certificates after they have received

documents that prove two things: the company is legally registered and location of a company and the consistency between those records. The CA can typically validate through email, DNS, or HTTP. Takes the longest to validate and most secure.

Simphony architecture supports both the server side and client side of authentication. Server authentication is accomplished via configuring the HTTPS connection by installing a TLS 1.2-compliant certificate on the server issued by Certification Authority. Client-side authentication is required for Simphony operations and cannot be disabled.

Simphony Workstation Authentication:

- Credentials are transmitted over an encrypted Transport Layer Security (TLS) channel to the application server.
- After the application server validates the credentials, an authentication token is issued that is returned to an encrypted channel back to the client.
- The token is stored by the client in an encrypted format inside its protected storage.
- All subsequent messages from the client to the server contain a security header that is encrypted with the public half of the key contained within the authentication token.
- The server stores a private key for each authenticated client in the database and can verify authenticity of an incoming request.

What is Transport Layer Security (TLS)?

TLS is a cryptographic protocol that provides end-to-end communications security over networks and is widely used for internet communications and online transactions. It is an Internet Engineering Task Force (IETF) standard intended to prevent eavesdropping, tampering, and message forgery. Common applications that employ TLS include Web browsers, instant messaging, e-mail, and voice over IP.

Many businesses use TLS to secure all communications between their Web servers and browsers regardless of whether sensitive data is being transmitted.

TLS’s predecessor, Secure Socket Layer (SSL) was developed by Netscape in 1995. SSL version 1.0 and 2.0 contained many security flaws that prompted a complete redesign of the protocol. In 1996, Netscape released SSL version 3.0 which was the basis for TLS1.0. In 1999, the PCI Council suggested the eventual deprecation of SSL as TLS 1.0 was a significant upgrade to SSL 3.0.

TLS vs. SSL

TLS is more efficient and secure than SSL because it has stronger message authentication, key-material generation, and other encryption algorithms. For example, TLS supports pre-shared keys, secure remote passwords, elliptical-curve keys and Kerberos whereas SSL does not. TLS and SSL are not interoperable, but TLS does offer backward compatibility for older devices still using SSL.

The TLS protocol specification defines two layers. The TLS record protocol provides connection security, and the TLS handshake protocol enables the client and server to authenticate each other and to negotiate security keys before any data is transmitted.

The TLS handshake is a multi-step process. A basic TLS handshake involves the client and server sending “hello” messages, and the exchange of keys, cipher message and a finish message. The multi-step process is what makes TLS flexible enough to use in different applications because the format and order of exchange can be modified.

CRL

Certificate Revocation List (CRL) is a mechanism for a certificate authority to revoke a Signed Certificate if they find it has been issued in error or believe that the Private Key could have been compromised.

When the CA responds to the CSR, and signs the certificate, a data "Field" is added to the SSL Certificate that contains the CRL Distribution Endpoint(s).

At this endpoint, there is a new file published at an interval defined by the CA. As a certificate is deemed to be revoked/invalid by the CA, they add the Certificate signature to the CRL list on the publish date.

If the HTTPS Client finds the SSL certificate within the CRL list, it will be understood as invalid and no longer trusted by the client.

Depending on the configuration of the Client, failure to reach the CRL endpoint can be treated in the same way as finding the SSL Certificate on the CRL List. Although this is a temporary false positive, it will prevent communication.

The CAL Client, Labor Management Driver and Gift and Loyalty drivers all treat a failure to reach a CRL endpoint as an untrusted SSL Server

For Online Certificate Status Protocol (OSCP), rather than the SSL certificate advertising where to download a list of "Invalid" certificates, an OCSP responder is advertised. When the certificate hash is passed, a valid or invalid response is returned.

OCSP stapling is where the server asks the OCSP responder for a validation hash itself, and for a set period of time, sends this to the client. This removes the need for the client to download a potentially large CRL List.

Simphony does not support OCSP and OCSP stapling.

Proxy

A proxy server sits between client and external network server resources. The proxy receives requests to resources from the client and forwards them to the appropriate resource. This keeps the client protected from unwanted network traffic.

The most common types of proxy servers are SSL, FTP, HTTP, and anonymous.

SSL (Secure Socket Layer) Proxy Server: Intervenes in the connection between the sender and the receiving resource to help prevent unwanted intrusion such as hacking of personal or financial data transmitted over the internet.

FTP (File Transfer Protocol) Proxy Server: Used in different applications where data is uploaded to a server. In advanced mode, FTP offers advanced security such as cache function and encryption methods which make the transmission process more secure.

HTTP (Hypertext Transmission Protocol) Proxy Server: Provides for the caching of web pages and files to allow faster access. HTTP can work with SSL to provide a more secure connection denoted by HTTPS.

Anonymous Proxy Server: Provides privacy while browsing the Internet.

VLAN and VPN

A virtual local area network (VLAN) is a collection of devices on one or more local area networks (LANs) configured to interact with each other at the data link layer as though they share the same physical location. They use each device's MAC address in the same broadcast domain.

VLANs offer a way to segment the network based on end-user needs such as resources and services and are not limited to one location. This can be one floor or multiple buildings. Communication within the group is based on logical connections as opposed to physical ones.

Switches are used to segment the network with ports assigned to a specific VLAN and each device on that VLAN connects to it via cable.

Advantages of VLAN:

- Enables logical grouping of devices scattered across multiple physical locations
- Minimizes the need for router deployment and reduces deployment costs
- Reduces administration
- Allows easy broadcast control and segmentation

Disadvantages of VLAN:

- Does not offer inherent End-to-End security

A virtual private network (VPN) is a technology that allows for secure extension of a private network over a public network (the Internet), and it is more often related to remote access to company's network resources. VPNs create a safe virtual tunnel between your device and the destination—website, company resources, and customer site. The tunnel encrypts all traffic that passes through it, hides your real IP address, and makes it possible to access content. VPN can work at the data link layer or network layer depending on the protocols used.

There are two types of VPNs:

- Client-to-Site (Remote-access): The VPN connection is designed to allow remote hosts to connect to the network on as-needed basis.
- Site-to-Site: The VPN is set up to connect specific machines between two networks on an ongoing basis with no setup per communication required.

Advantages of a VPN:

- Provides a high level of security through encryption
- Ensures privacy and confidentiality
- Allows to increase the overall efficiency of a network
- Allows anonymous file sharing (works with P2P networks)

Disadvantages of a VPN:

- Costlier, requiring specialized equipment such as VPN concentrator and routers
- Higher Administrative overhead requiring more extensive knowledge working with security

7
Networks

This chapter provides contextual information that supplements information in Oracle Networking Expectations.

A computer network is a group of computers that use a set of common communication protocols over digital interconnections for sharing resources located on or provided by the network nodes.

Simphony is installed in wired, wireless, and hybrid networks.

Wired Networks

Wired network design is a critical component of Point-of-Sale sites. Wired networks use cables to connect other communication devices such as switches and routers to ensure customer transactions move successfully from workstation to server and changes in the database on the server are pushed down to the workstations.

A wired network provides the following benefits:

- Faster data speed
- Less interference
- Connect devices at longer distances
- Increased security
- More control over device connections

Network Types

A network consists to two or more computers connected to share resources.

Wide Area Network (WAN)

A Wide Area Network (WAN) is the largest type of network, often spanning global regions. Access to a wide area network is leased from a service provider.

Cloud software WAN requirements should be based upon the pipeline demands of the business. If demands on the point-of-sale system are constant throughout the day, a WAN type that can supply enough bandwidth for this expected usage could be considered. If the demands on the point-of-sale system fluctuate between steady use and periods of high demand, then the WAN selected must be able to handle the increased bandwidth needs of the periods of high demand use.

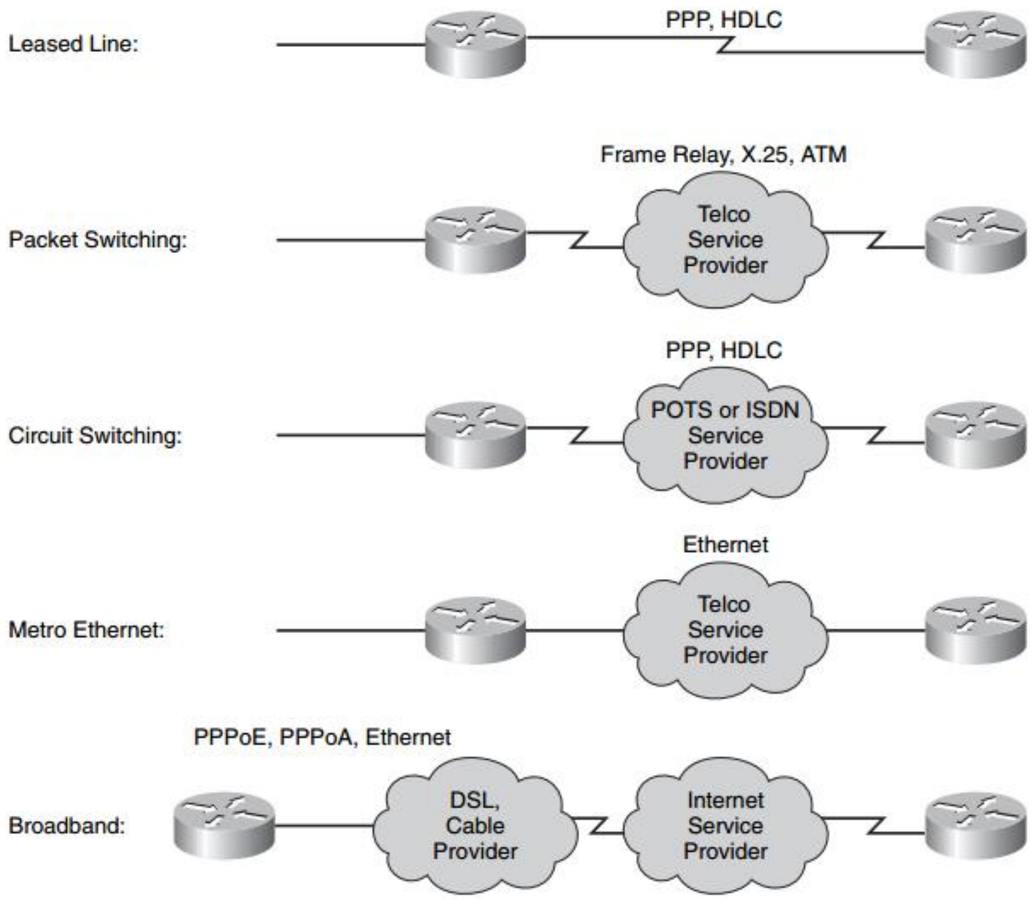
Point of sale software upgrades and software deployments are events requiring increased bandwidth.

The WAN type selected should handle all bandwidth activities to the satisfaction of the customer. The following table describes WAN connectivity options:

Available Options for WAN Connectivity

Type	Available Options
Leased Line	T1, E1, T3, E3
Packet Switched	Frame Relay, Cell Relay/ATM
Circuit Switched	SONET/SDH, ISDN
Ethernet	VPLS, Metro
Broadband	Cable, Fiber Optic, DSL

DIAGRAM OF WAN CONNECTIVITY



The following are WAN topologies:

- Point to Point
- Hub and Spoke / Star
- Partial Mesh
- Full Mesh

Local Area Network (LAN)

A Local Area Network (LAN) is a localized collection of networked-connected devices.

Questions to consider for LAN environments:

- Are workstations placed in close proximity to one another?
- Will there be long cable runs between installation areas on the property?
- Will there be remote or satellite areas that may be permanent or temporary?

Simphony Point of Sale Networking

For reliability and ease of troubleshooting, all current Oracle MICROS products use 100/1000 BaseT networking topology based on twisted pair cabling. The benefits of this include:

- Reduced cable costs

The installation of cable costs far more than the cable itself. The wide appeal of 100/1000 BaseT is that it supports using existing telephone wiring, which saves on installation costs. However, most sites do not have enough existing high-quality twisted pair cable available to support a network installation, so more cable must be pulled anyway. The use of existing telephone wiring requires Oracle MICROS approval.

- Troubleshooting management, fault isolation, and security

Troubleshooting is easier with the Ethernet star topology. A single workstation or printer is connected to a single port on the hub, switch, or router, allowing the behavior of each connection to be individually monitored. LED indicators on each port provide immediate feedback on the link integrity and speed. A failure is quickly isolated, and the remaining Ethernet devices continue to operate while the problem is being addressed. Adding or moving devices is as simple as installing a wall plate or plugging into a pre-wired connection at the switch or patch panel. In small or low-cost installations, the single point of concentration, point-to-point connectivity, and link status LEDs make diagnosing a problem on a 100/1000 BaseT network much easier than checking an entire length of coax cable for a break.

Consider the following points:

- Number of workstations
- Workstation placement within a property
- Managed switch vs unmanaged switch
- Power over Ethernet requirements (other switches or devices Wi-Fi access points and credit card payment terminals)
- Level of redundancy / availability necessary

Simphony Shared Services

Oracle MICROS Simphony point of sale uses the concept of shared services. Workstations that run shared services are recommended to be placed on LAN network segments with high availability.

- Check and Posting service

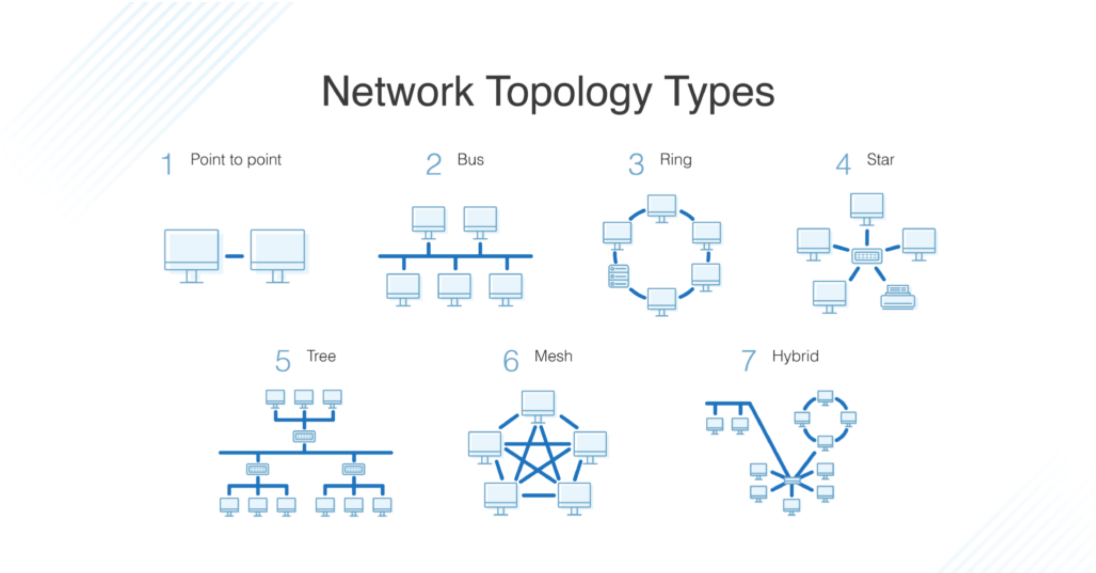
- Backup Check and Posting service
- Transaction service
- Distributed Client Access Loader service
- Kitchen Display Controller service
- Backup Kitchen Display Controller service

Types of LAN Connectivity

- Ethernet
- Fast Ethernet
- 1 Gigabit Ethernet
- Token Ring
- FDDI
- ATM

LAN Topologies

- Point to point
- Bus
- Ring
- Star
- Tree
- Mesh
- Hybrid



Cable Types

Cables connect two or more computers or networking devices together to move data through the network.

The following data cable types are found in a typical Oracle MICROS Simphony point of sale installation and are discussed in this section:

- Twisted pair
- Fiber optic
- Coaxial
- Integrated Device Network (IDN)

Twisted Pair

In twisted pair cabling, two conductors are twisted together to provide shielding from electromagnetic interference.

Types of Ethernet cable consists of Unshielded Twisted Pair - UTP and Shielded Twisted Pair - STP. Ethernet cables are terminated with an RJ45 connector.

An Ethernet cable can be attached to a patch panel and to wall jacks.

All Oracle MICROS Workstations contain at least one 8-pin modular port designated for communication with Ethernet networks.

Solid Wire Cable

An Ethernet cable can consist of a few solid copper cables. The copper in these cables is of a thicker gauge and makes these types of Ethernet cables ideal for permanent installation.

Stranded Wire Cable

An Ethernet cable can consist of many strands of copper cables. The copper in these cables is of a thinner gauge and makes these types of Ethernet cables flexible and ideal for wall jack to workstation connections.

Unshielded Cable

Unshielded cables are manufactured without any additional insolation or protection from electromagnetic interference.

Shielding materials such as meshes, or aluminum foil are not used in the production of unshielded cables.

Unshielded cables can suffer from data flow disruption caused by all kinds of electrical interference.

Unshielded network cables should never be installed next to any electrical source as the magnetic field generated by the electrical installation may disrupt the data flow.

Shielded Cable

Shielded cables are manufactured with the intention of reducing any external magnetic interference. These Ethernet cables may come with a drain cable which provides a mechanism for grounding the cable.

Sources of Interference

Sources of interference include:

- Fluorescent lighting
- Electric motors
- Transformers
- Electrical cabling

Examples of UTP/STP Ethernet Cable

- Category 5e Ethernet
- Category 6 Ethernet

Ethernet cabling is placed into categories that define the quality of both the cable as well as related connection hardware such as faceplates, modular connectors, and patch cables.

Several categories of UTP and related connection hardware are defined for a structured cabling system. Several cable suppliers now offer the STP equivalent of Category 6 cables and connection hardware. Each category is briefly defined below.

The Category 5e standard was formally defined in 2001. Category 5e represents an incremental improvement over Category 5 with tighter specifications designed to support full-duplex Fast Ethernet and Gigabit Ethernet. Most current MICROS terminals support Gigabit Ethernet.

Category 5e cable performance characteristics and certification methods are defined in ANSI/TIA/EIA-568-B.2-2001.

Category 6, ratified in June 2002 (ANSI/TIA/EIA-568-B.2-1), provides higher performance than Category 5e with more stringent specifications for crosstalk and system noise in addition to supporting a bandwidth up to 250Mhz. Category 6 cable is standardized for Gigabit Ethernet, a port included on all current MICROS workstations.

Category 6a cable, or Augmented Category 6, was defined in February 2009 in ANSI/TIA-568-C.1 and is characterized to operate at 500 MHz with improved alien crosstalk characteristics.

Ensure the installation and termination of Category 6 or 6a cables and connection hardware meet the required specifications.

In sites with a high amount of electromagnetic interference (EMI), shielded cables are required. The shielding reduces the effect of EMI on data carried by the cable. Maintain the shielding from one cable end to another using a drain wire in the same sheath as the twisted pairs.

Examples of Ethernet Data Transmission Capacity

Name	IEEE Standard	Media
Fast Ethernet	802.3u	100Base-TX 100Base-FX
Gigabit Ethernet	802.3z	1000Base-T 1000Base-SX 1000Base-LX
10 Gigabit Ethernet	802.3ae	10GBase-SR 10GBase-LX4 10GBase-LR/ER 10GBase-SW/LW/EW

Despite shielding, grounding, and bypassing, metallic cable can behave like antennas, making them susceptible to RF noise. The greater the length of the cable, the greater the possibility it will be subject to interference from nearby electrical equipment.

Metallic cables are subject to an effect that produces voltage potentials between the cable and electrical ground. This can occur in large buildings or campus environments where equipment is powered from multiple AC power panels that are not operating at the same AC ground potential.

Fiber Optic

Fiber optic cables have conductors made of glass, rather than metal. A typical fiber cable is composed of a glass core that carries the light signals. The core is encased in cladding that keeps the light contained in the core.

No electrical impulses are carried over a fiber optic cable as in a metal cable. Instead, the electrical impulses are converted to pulses of light that indicate whether a bit is 1 or a 0.

Signals on metal cables and the light in fiber optic cable travel at approximately the same speed, but light meets less resistance as it travels along the cable. Therefore, light signals go further with less attenuation. Fiber optic links on simple LANs can run without a repeater to distances of more than 3.5 kilometers.

Fiber-based cabling systems are more reliable than metallic cabling systems because they are immune to electrical noise generated by support equipment in the building.

Fiber is recommended for distances greater than 100 meters or as a solution to ground potential issues. A number of cost-effective media converters conforming to this standard are available. Many use fiber connectors that are easy to terminate.

NOTE:

Fiber optic cables can be used switch to switch. Fiber optic cables can be used with fiber to Ethernet converters.

Coaxial

Coaxial cable is a type of shielded cable. It consists of a single copper wire that is surrounded by layers of insulation. Coaxial cable is commonly used by Cable TV and Internet providers.

Common types of Coaxial Cable are RG-59 and RG-6. The RG-6 coaxial cable uses a lower gauge of copper wire and has better insulation than the RG-59 coaxial cable. Coaxial cables are terminated with a threaded F-type connector.

Quick Service Restaurants and Table Service Restaurants might get their Internet access from a service provider that could terminate the restaurant's WAN access with a coaxial connection.

Coaxial termination can be converted to Ethernet cables with a Cable Modem or MoCA enabled Router.

Name	Media
Coaxial	RG-59 RG-6

> **NOTE:**
>
> Coaxial cables can be used with MoCA to Ethernet converters.

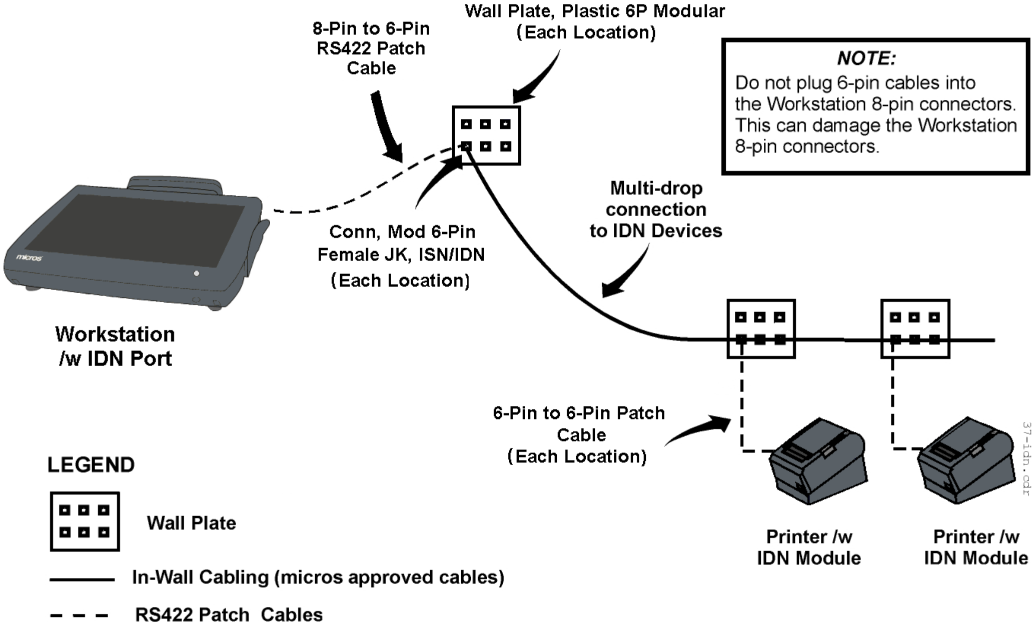
Integrated Device Network (IDN)

Integrated Device Network is the Oracle MICROS proprietary network module that allows for a localized network. Commonly used in the connection of one or more receipt / order printers to an Oracle MICROS workstation.

A local IDN network consists of a workstation driving one or more devices connected in a daisy chain over IDN cable runs.

A remote IDN network consists of a workstation driving one or more devices connected in a daisy chain over twisted pair cable at distances of up to 4000 feet from the workstation. This configuration requires in-wall cable runs, faceplates, and patch cables at the workstation driving the network and as well as each device.

The following diagram shows an example of driving a small network of IDN printers from any workstation with an IDN port using shielded category 6 or better cable and connection hardware (Categories 3, 4 or 5 cable can be used if already available). The workstation that drives IDN printers is shown at the left of the illustration. One 8-Pin to 6-Pin IDN patch cable is connected between the 8-pin IDN ports on the workstation to one of the 6- pin connectors on the local module.



A patch cable is then installed between the remaining 6-pin connector on local IDN printer and the faceplate connector to convert the IDN transmit/receive pairs into ANSI/TIA/EIA-568-A compatible transmit/receive pairs.

Install a pair of Category 6 or better shielded cables between the patch panel and the two connectors on the wall plate near each printer location. The dual run to the faceplate is required to obtain cable certification since a daisy chain configuration is not part of Ethernet topology. Terminate the drain wire of each cable run at the patch panel.

To maintain the IDN daisy chain, install Category 6 or better patch cables at the patch panel. At each remote printer location, install a pair of patch cables to maintain the daisy chain at the printers. The last printer in the chain requires only one patch cable.

IDN cable runs are terminated at the workstation with a RJ45 connector and at the network module or wall plate with a RJ12 connector.

All MICROS Workstations contain at least one 8-pin modular port designated for driving IDN devices.

Specifications

The efficiency of a network can be affected by the speed of data throughput, maximum distance between network devices and time delay between data transfer.

These topics are discussed in this section:

- Bandwidth
- Distance
- Latency

Bandwidth

Bandwidth is the throughput capacity of a network medium or protocol.

Variations in the network signals can cause degradation on the network.

Sources of degradation can be cables that are too long or wrong cable type.

Name	Data Rate
Fast Ethernet	100 Mbps
Gigabit Ethernet	1 Gbps
10 Gigabit Ethernet	10 Gbps
Cable	10-100 Mbps
Fiber Optic	10 Gbps
T1	1.544 Mbps
Fast Ethernet	100 Mbps
E1	2.048 Mbps

Distance

Cabling distance is the specified maximum length a particular cable type can be run without signal degradation.

Types of cable used in a LAN include Ethernet, coaxial and fiber optic.

Name	Maximum Distance
Ethernet	100 meters
Fast Ethernet	100 meters to 2000 meters
Gigabit Ethernet	100 meters to 5000 meters
10 Gigabit Ethernet	300 meters to 40 kilometers
Coaxial	500 meters
Fiber Optic	60 kilometers

If a greater length of cable is required to connect devices, a switch or extender is required to extend the distance or reach of the network segment.

The actual distance that a cable support could be much less depending upon the amount of interference generated by the installation site.

Latency

Latency refers to a time delay; for example, the gap between the time a device requests access to a network and the time it receives permission to transmit.

Latency is the measurement of time taken for network packages to traverse a network and is a function of several factors, most notably distance from the data center, access technology, last-mile bandwidth and network contention. It is the single biggest factor that affects perceived application performance.

Latency can be tested from the proposed Simphony site by running a web-based speed test or by running a Traceroute to the proposed Simphony datacenter. Both tests measure network latency from the client network to the datacenter over the public Internet.

These tests can verify that the Simphony location is using the most efficient path available.

Hardware

Network hardware connects multiple devices together to share common resources in a local area or access them across the globe.

This section discusses the following topics:

- Router
- Gateway
- Switch
- Network Interface Card (NIC)
- Powerline Extender
- Modem

Router

A router is a networking device that functions as a gateway to forward data packets between computer networks.

The router will be situated between the WAN and the LAN. It may be connected to a modem, ONT or CSU/DSU on the WAN side and networking switches on the LAN side.

Points to consider:

- Routers may be supplied by the provider of the WAN network access.
- May want to upgrade the router to one with capabilities not offered by device supplied by the provider of the WAN network access.

Gateway

Gateways provide connectivity between networks. The connectivity could be between the WAN and the LAN. For this setup, the gateway functionality would be performed by a router.

The connectivity could be between multiple LAN networks for between the LAN network and the WAN network. Here the gateway functionality could be performed by a router, switch or computer.

Switch

Hubs are used for connecting multiple Ethernet segments together. Hubs extend the distance of a network connection further than the limits of each length of Ethernet cable. Hubs have fallen out of favor for networking because they relay all communication to all of their network ports. Newer devices such as switches can manage the communication so that it is only transmitted to the intended device on a specific port.

An unmanaged switch can manage the network communication so that it is only transmitted to the intended device on a specific port. The purpose of a switch is to extend the distance of a network connection further than the limits of each length of Ethernet cable. The unmanaged switch is more efficient that the hub as it can "learn" the mac addresses of connected devices and route messages only to the correct destination.

A managed switch gives the end user greater control over the LAN network and is recommended for medium to large point of sale networks. Initially a managed switch will function like an unmanaged switch but can be configured through an interface to do much more. These switches provide the ability to control the flow and performance of the communication on a network.

- -Virtual LAN - VLAN
- -Precise monitoring
- -Quality of Service - QOS

Smart switches are an evolving technology. This is like a cross-over from unmanaged switch to be managed. They come with some manageable features, Quality of Service (QoS) and security but considered a lite version compared to the full featured manageable switches.

Network Interface Card (NIC)

A NIC is a computer networking card used to connect a device to a network. The NIC may be an onboard addition to a computer’s motherboard, a plug-and-play expansion slot addition to a computer's motherboard. NIC's can also take the form of a USB pluggable device that may be added to a computer.

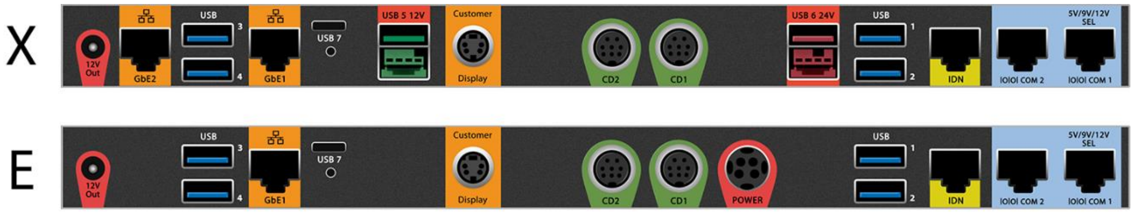
NIC's of most Oracle MICROS hardware used with Simphony are equipped with a 10/100/1G Ethernet port.

Oracle MICROS devices with onboard NIC cards:

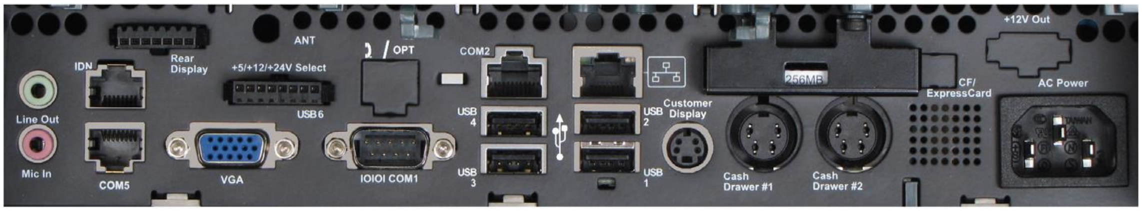
- Point of Sale Workstations
- Kitchen Display Systems
- Receipt Printers
- Kitchen Order Printers
- Kiosks

The following diagrams show ports on the back of Oracle MICROS workstations:

Primary I/O Panel of the Oracle MICROS Workstation 625X/655X and 625E with a single or dual Gigabit Ethernet port.



Primary I/O Panel of the Oracle MICROS Workstation 5A with a single 10/100/1000 Ethernet port.



Points to consider:

- Configuration settings for the network card
- Maximum speed of the network card

Powerline Extender

Powerline extenders are network adapters that use existing electrical cabling for the transmission of network communication. A minimum of two powerline adapters are required. While powerline adapters are affordable and effective for home use, they are not recommended for use by point-of-sale networks.

Modem

A cable modem serves as a connection between a cable provider's WAN access and a router for the LAN.

A DSL modem serves as a connection between a DSL/ADSL line WAN and a router for the LAN.

A Channel Service Unit (CSU) or Data Service Unit (DSU) is a modem-like interface that serves as a connection between a leased line WAN and a router for the LAN. It may also be available as a module that can be inserted into a networking router.

Points to consider:

- Placement of the modem to avoid electrical interference.
- Cabling between modem and WAN.

- Cabling between modem and router for LAN.
- Connectors on each end of cabling being used by the modem.

Installation

Network cables should be installed properly with the correct termination.

These topics are discussed in this section:

- Cabling
- Termination

Cabling

UTP Cable Installed in Metal Conduit

To install UTP cabling in a grounded metal conduit, consider the following:

- Use conduit composed of ferrous metal. Aluminum conduit is unacceptable as it provides little or no protection from EMI.
- Use conduit throughout the system from junction box to junction box to ensure an adequate ground return path.

PVC Conduit

When cables are buried below the floor level, the use of PVC Conduit is permitted. When using PVC conduit in concrete flooring, the following guidelines apply:

- Locate the PVC conduit at least six inches below the surface of the floor.
- Locate the PVC conduit at least six inches from other nearby conduits.

Cable Damage

The possibility of mechanical damage to cables is generally apparent at the time of installation. This includes outdoor runs of cable, as sunlight, rain, and mechanical flexing due to wind causes the cable to deteriorate. Do not kink or tightly bend the cable; the bend radius should be at least four times the outside cable diameter.

Lightning

Lightning does not need to directly strike the cabling to cause damage or disruption to the system. Nearby lightning strikes produce strong electromagnetic fields that can induce voltages on the data transmission cables causing disruptions or damage. Use a grounded ferrous metal conduit for areas subject to frequent thunderstorm activity. In cases where shielded cables installations in geographical are used, reduce the effects of lightning by placing the cable runs as close to ground level as possible.

Electrical Motors

Motors of various sizes are found in a typical restaurant or hotel site. Use a grounded ferrous metal conduit when running cabling at distances less than two feet from motors that are 1/4 horsepower or smaller, or less than six feet from motors larger than 1/4 horsepower.

Radio Frequency Interference (RFI)

The probability of RFI varies in accordance with many factors, including transmitter power, location, construction materials used in the building, and the physical placement of the power and data transmission cables.

Wireless

Designing and verifying a solid wireless network is critical to reliable POS operations which are susceptible to packet loss and latency. This section will provide details of site considerations, site surveys, AP choice, SSID design, channel selection, roaming consideration, Wi-Fi encryption, and testing and debugging strategies.

Site Considerations

A wireless site survey is a process that is part of the design and implementation of a wireless network.

Results from a wireless site survey will determine the strategic position of the access points, a delivery of the required Wi-Fi coverage, POS bandwidth requirements, roaming and quality of service.

A wireless site survey is a necessary step in understanding the infrastructure of a wireless network.

The purpose of any wireless site survey is to identify any Wi-Fi interfering obstacles that could negatively impact the WLAN performance.

For more details, refer to chapter 4.

Failure to conduct a wireless site survey may result in poor network performance.

All site surveys are performed by the vendor with the intention of providing the best possible outcome for the enterprise.

The vendor will take into consideration different factors when designing and implementing a wireless network infrastructure which will be based on the survey results and the business requirements.

There are several guidelines on how to conduct a wireless site survey, but every vendor will use different techniques and types of software when conducting a survey.

An initial survey should be conducted in an empty environment as part of the evaluation process and prior to any wireless hardware installation.

A wireless survey should then be repeated in real-life conditions when the interference from the environment and the Wi-Fi demand is the highest.

IMPORTANT:

All mobile and electronic devices connected to the wireless network will influence the network performance so conducting performance tests during the highest demand window is vital to truly evaluate the network limits and performance.

The results of a survey conducted in an empty property cannot be used as a performance benchmark and cannot be compared with the results of a survey conducted in a busy environment.

Access Point (AP) Position

Access points should always be installed following the results of a comprehensive site survey and should never be installed in random places.

Incorrect positioning of an access point may have a detrimental effect on the radio broadcasts and only offer a poor network performance.

The correct number of access points should be based on several unique factors in an individual property and should never be estimated and a standard template should never be used.

Several factors should be considered when designing the wireless network:

- Wireless network purposes being supported: POS, voice, video, CCTV.
- Wireless network capacity and demand
- Bandwidth requirement: VOIP, video calling, security cameras.
- Number of SSIDs Service Set Identifier
- The approximate number of concurrent connections per access point. Some APs degrade performance with as few as 20 devices.
- Maximum allowed connections per radio
- Heavy wireless demand environments: Customers using network, VOIP.
- Overlapping factors that compound each other.
- Access points proximity. APs can interfere with each other.
- Neighboring access points: interference, channel overlap.
- AP maximum power output

NOTE:

Outdoor access points need to be able to reach a large area to be effective. Some vendors offer specific access points that are built for use in outdoor environments as these offer the best outdoor coverage for the business.

Wi-Fi Interference

Wi-Fi interference is an unintended signal emitted from any source other than the WLAN infrastructure.

Interference can impair the normal function of the WLAN and should always be identified and mitigated.

Interference is a common phenomenon in a wireless network and in some cases, it cannot be avoided.

Interference can reduce the network's performance and availability as the wireless signals can be intercepted or blocked by various factors or even preventing devices from connecting to the wireless network efficiently.

Interference from Non-Wi-Fi Devices

Some non-network devices, such as microwave ovens, cordless phones, or wireless CCTV installations can interfere with wireless channels. Most often, these devices will use the 2.4 GHz frequency.

Co-Channel Interference

Interference represents the total amount of competing in-band signals that prevent the access points from accepting the intended signal with clarity.

The extreme proximity of so many client devices on adjacent and non-adjacent channels increases interference levels and therefore, impacting the performance across the WLAN.

The correct design of a wireless network ensures that all connected devices have sufficient uninterrupted communication while mitigating the potential for collisions and limiting the impact of interference.

Internal Structures

The building materials of the structures where the access points operate can cause varying degrees of wireless signal interference or blockage. Concrete, brick, and other dense materials can block Wi-Fi signals. These obstacles should be taken into consideration when installing access points.

Mitigating Interference

A detailed site survey should always be conducted to identify and mitigate any interference and potential Wi-Fi signal issues.

POS devices require a good level of uninterrupted bandwidth and a clear path of communication with the CAPS and an external environment.

Failure to recognise and resolve interference may lead to poor Wi-Fi connection and unstable performance that can lead to financial loss and discrepancies.

An interference survey should include the POS SSID and all access points that the devices connect to.

When testing the interference levels in the environment where the POS devices operate, the tester should always use POS devices as a benchmark of any negative influences on the performance.

Tests conducted using other Wi-Fi devices may produce different results as all wireless devices respond differently in specific circumstances and conditions.

The testing should be carried out in all locations where the POS devices operate such as:

- Kitchens
- Corridors
- Offices
- POS devices charging stations

Size and Scale

All venues regardless of their size may experience poor wireless performance if any of the basic best practice conditions have not been followed.

Large venues may require the installation of several wireless controllers and hundreds of access points where small venues may just be operating with two or three access points.

Regardless of the operational size and requirements, all infrastructures can experience problems.

Wireless network performance can be compromised by intentional and unintentional influences, and it is the responsibility of the provider and the vendor to ensure that all negative aspects have been eliminated.

Smaller venues are susceptible to wireless coverage and neighboring wireless flooding.

Large venues and installations are more likely to experience the following problems. Pay special attention to these areas when designing and verifying an installation:

- Channel overlapping
- Excessive number of access points
- High network demand
- Bandwidth sizing issues
- Network latency
- Client management issues
- DHCP issues
- DHCP lease

Infrastructure

The communication from the controller to the access points can be disrupted by electromagnetic fields, if the data cables are installed close to any devices that emit such fields.

Shielded cabling is recommended as it can prevent any interference.

Unshielded network cables should never be installed next to any electrical source as the magnetic field generated by the electrical installation may disrupt the data flow.

Interference noise can be introduced in cabling by the following sources:

- Fluorescent lighting
- Electric motors
- Transformers
- Electrical installations

Testing, Validation, Debugging

Testing

Taking Measurements

The coverage area of the access points should be measured by checking the data rate or the signal strength quality for all broadcasting access points at all distances and areas instead of focusing only on the signal strength in the **heat map open-plan view**.

Understanding Wi-Fi Heat Maps

Open plan heat map refers to the entire area field view which will show the overall Wi-Fi coverage however, this type of measuring function will not allow for monitoring of an individual SSID MAC addresses "Media Access Control Address".

Recognizing SSIDs

Each access point (AP) will broadcast the SSID “Service Set Identifier” MAC address which should not be confused with the access point hardware MAC address.

The Wi-Fi monitoring application cannot be used to monitor an individual access point but all SSIDs that the (AP) broadcasts.

Access points can be configured to broadcast several individual SSIDs, these can include open public networks, internal staff networks, and the dedicated POS network.

Grouping All SSIDs

Not all wireless networks are visible, so the analysis of visible and hidden SSIDs is necessary to recognize and group all networks that are configured to broadcast by the individual access point.

Grouping of all MAC addresses should be performed to estimate the correct number of individual networks in a specific area as some neighboring broadcasting SSIDs can also be visible in the designated areas.

A wireless network map can be created using the analysis of the following:

- Hidden and visible MAC address in the 2.4 GHz and 5 GHz band
- Hidden and visible SSID channels in the 2.4 GHz and 5 GHz band
- Amplitude dBm of the hidden and visible SSIDs channels in the 2.4 GHz and 5 GHz band

Creating MAC Address Map

Creating a Wi-Fi map using the MAC addresses in the 2.4 GHz and the 5 GHz band

SSID MAC addresses can be grouped by identifying and comparing similarities between them.

The example below shows similarities between the MAC addresses from four different SSIDs that originate from a single access point.

2.4 GHz Band

SSID1 MAC Address 1C:59:9B:A6:74:01 Hidden SSID Channel 1

SSID2 MAC Address 1C:59:9B:A6:74:02 Visible SSID Channel 1

SSID3 MAC Address 1C:59:9B:A6:74:03 Hidden SSID Channel 1

SSID4 MAC Address 1C:59:9B:A6:74:04 Visible SSID Channel 1

5 GHz Band

SSID1 MAC Address 1C:59:9B:A6:74:20 Hidden SSID Channel 46

SSID2 MAC Address 1C:59:9B:A6:74:21 Visible SSID Channel 46

SSID3 MAC Address 1C:59:9B:A6:74:22 Hidden SSID Channel 46

SSID4 MAC Address 1C:59:9B:A6:74:23 Visible SSID Channel 46

Creating hidden and visible SSID channel saturation map in the 2.4 GHz and the 5 GHz band

The channel saturation factor should only be considered for changes if the dBm level is similar in a specific area in which the testing is taking place.

The saturation level may change depending on the tester and the access point position therefore, it cannot be assumed that all areas will suffer channel saturation when only one specific area has been identified.

Channel saturation will vary in different areas, and it is dependent on three factors:

- Number of access points installed in the area
- Number of access points in the neighboring area
- Access points configured with static channels

The example below shows channel 1 saturation with varied amplitude dBm signal level broadcast from several access points in the area.

The dBm level varies significantly between the SSIDs and this example does not represent a problem for devices where the roaming threshold has been set correctly.

POS devices operating in this area sample will connect to the strongest broadcasting access point and only switch to another access point (AP) when a stronger signal is detected by the device.

2.4 GHz Band

SSID1 MAC Address 1C:59:9B:A6:74:01 Hidden SSID Channel 1 dBm -30

SSID2 MAC Address 1B:01:00:C6:80:AB Visible SSID Channel 1 dBm -65

SSID3 MAC Address 1A:00:02:01:AA:03 Hidden SSID Channel 1 dBm -78

SSID4 MAC Address AA:60:9C:A1:04:C1 Visible SSID Channel 1 dBm -81

5 GHz Band

SSID1 MAC Address 1C:59:9B:A6:74:AA Hidden SSID Channel 46 dBm -30

SSID2 MAC Address 1B:01:00:C6:80:AB Visible SSID Channel 46 dBm -65

SSID3 MAC Address 1A:00:02:01:AA:AC Hidden SSID Channel 46 dBm -78

SSID4 MAC Address AA:60:9C:A1:04:A4 Visible SSID Channel 46 dBm -81

Creating hidden and visible SSID amplitude dBm map in the 2.4 and the 5 GHz band

The example below demonstrates a channel overlapping broadcast by four individual access points positioned in close proximity.

Typically, this type of configuration is a result of a poorly configured Wi-Fi network or manual channel assignment.

Devices connected to these access points can experience interference, which can lead to connection instability.

In this scenario, each access point should be given a unique channel depending on the distance from another AP in the area.

2.4 GHz Band

SSID1 MAC Address 1C:59:9B:A6:74:01 Hidden SSID Channel 1 dBm -55

SSID2 MAC Address 1B:01:00:C6:80:AB Visible SSID Channel 1 dBm -58

SSID3 MAC Address 1A:00:02:01:AA:03 Hidden SSID Channel 1 dBm -52

SSID4 MAC Address AA:60:9C:A1:04:C1 Visible SSID Channel 1 dBm -54

5 GHz Band

SSID1 MAC Address 1C:59:9B:A6:74:AA Hidden SSID Channel 46 dBm -55

SSID2 MAC Address 1B:01:00:C6:80:AB Visible SSID Channel 46 dBm -58

SSID3 MAC Address 1A:00:02:01:AA:AC Hidden SSID Channel 46 dBm -52

SSID4 MAC Address AA:60:9C:A1:04:A4 Visible SSID Channel 46 dBm -54

Debugging

When troubleshooting POS device performance issues, always collaborate with the Wi-Fi provider, as only a small part of the entire infrastructure can be intercepted using external tools.

Logs and reports obtained from the Wi-Fi provider always play a big part in troubleshooting the problem because not all information can be captured when externally observing the wireless network behavior.

The approach should be divided into the following sections:

- **Entire Wireless Enterprise**

  Learn about the entire wireless network and do not focus only on the POS network.

  Obtain information from the wireless provider about the entire infrastructure.

- **POS Network Focus**

  Segregate the POS network from the enterprise and test its position within the infrastructure.

  Perform tests from within the POS environment instead of focusing on the entire network.

  Test POS network performance using POS devices and follow the communication path.

- **POS Data Capture**

  Gain an understanding of the POS data traffic and follow its complete path.

  Use appropriate tools to capture data and seek assistance from the wireless provider when access to the internal network is limited.

- **Monitoring**

  The monitoring tests should always be carried out during peak times when the network demand is the highest.

  Expand the monitoring field to all POS devices during the tests to capture more data.

  Do not use a single POS device for monitoring as the results may be skewed by the POS device itself.

  Do not use any other Wi-Fi capable hardware when testing the wireless performance as not all devices respond identically.

8 Glossary

Symbols and Numbers

802.XX
IEEE Standard for port-based Network Access Control

A

AC power
AC stands for alternating current which means the current constantly changes direction

Access Point
A networking device that allows for multiple wireless devices to connect to a network

ADSL
Asymmetric Digital Subscriber Line
A type of broadband networking technology

AES
Advanced Encryption Standard

AP
Access Point
A networking device that allows for multiple wireless devices to connect to a network

Application layer
An application layer is an abstraction layer that specifies the shared communications protocols and interface methods used by hosts in a communications network

API
Application programming interface

Asynchronous
Data transmitted intermittently or not at the same intervals

ATM
Asynchronous Transfer Mode

Authentication
A security measure designed to verify the identity of a transmission

B

Backbone
Core networking component that interconnects different computer networks

Band
Band is a specific range of frequencies in the radio frequency spectrum

Bandwidth
Bandwidth is the maximum rate of data transfer across a given path. Bandwidth may be characterized as network bandwidth

Bps
Bits per second

Broadband
High-capacity bandwidth network transmission

Bus
A bus topology is a topology for a Local Area Network in which all nodes are connected to a single cable

C

CA
Certificate authority

Cable Modem
A cable modem is a device that operates over coax cable

Cabling
The media used for transmission of data in computer networking

CAL
Client application loader

CAPS
Check and Posting Service

CAT 6

Category 6 Ethernet cable

CCTV
Closed circuit television

CCTV RF

- Closed circuit television Radio Frequency
  Passive Infrared
- Microwave
- Dual Technology Motion Sensors

Channel
A Wi-Fi channel is a medium through which wireless networks can send and receive data

Cloud
On-demand availability of computer system resources

Coaxial cable
Coaxial cable is a type of shielded cable. It consists of a single copper wire that is surrounded by layers of insulation. Coaxial cable is commonly used by Cable TV and Internet providers

CRL
Certificate Revocation List Channel

CRL Endpoint
An extension which describe the endpoint to acquire the CRL, which is issued by the CA that signed this certificate

CSIRT
Computer Security Incident Response Team

CSR
Certificate signing request

CSU
Channel Service Unit

D

DB
Database

DBSync
Database Synchronization

DHCP
Dynamic Host Configuration Protocol

DOS\DDOS
An attack attempts to bring down your system by sending a vast number of requests to it such as SYN flood attacks

Downlink
Connection from data communications equipment towards data terminal equipment

DSL
Digital subscriber line

DSU
Data Service Unit

Dual-Band in Wireless
A device capable of operating and broadcasting in two different frequencies 2.4GHz and 5GHz

E

E-1
A leased-line connection (Europe) capable of carrying data at 2,048,000 bits-per-second

E-3
A leased-line connection (Europe) capable of carrying data at 34,386,000 bits-per-second

EMC
Enterprise Management Console

EMI
Electromagnetic magnetic interference

Encryption
The process of converting data into a cipher or code in order to prevent unauthorized use

Ethernet
A system that is used for connecting several computer systems to form a local area network. Ethernet can use protocols to control the passing of information and to avoid simultaneous transmission by two or more systems

F

Fast Ethernet

Fast Ethernet physical layers carry traffic at the nominal rate of 100 Mbit/s

FDDI
Fiber Distributed Data Interface

Fiber Optic
Refers to the medium and the technology associated with the transmissions of information as light impulses

Firewall
A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules

Flow Control
Flow control is the management of data flow between computers

FQDN
Fully qualified domain name

Frame Relay
Frame Relay is a packet switching technology that fragmented into transmission units called frames and sent in high-speed bursts through a digital network

FTP
File transfer protocol

F-Type Connector
A connector for termination of coaxial cable

G

Gateway
A device used to connect two different networks

Gbps
Gigabits per second

Gigahertz
A measure of frequency equivalent to one thousand million (109) cycles per second

H

Hash
Distributes requests based on a key you define, such as the client IP address or the request URL

Hop
A measure that is used to identify the number of routers that separate two hosts. If three routers separate a source and destination, the hosts are four hops away from each other

Host
A network host is any device, or a computer connected to a computer network. A network host provides services, information resources, and applications to users or other nodes on the network

HTTP
Hypertext Transfer Protocol

Hub
Network hub, is a connection point for devices in a network

Hub and Spoke
Transport topology optimization in which traffic planners organize routes as a series of "spokes" that connect outlying points to a central hub

Hybrid LAN topology
Hybrid topology is an interconnection of two or more basic network topologies

I

IDN
Integrated Device Network

IDS
Intrusion Detection Systems

IETF
Internet Engineering Task Force

IFC
Interface

IP Address
The location of a device on a TCP/IP network. The IP Address is either a number in dotted decimal notation which looks something like (IPv4), or a 128-bit hexadecimal string such as (IPv6)

IP Hash
IP hash of an IP address is an encrypted version of the IP address

IP Header
An IP header is header information at the beginning of an IP packet which contains information about IP version, source IP address

IP Lease
A DHCP lease is a temporary assignment of an IP address to a device on the network

IPS
Intrusion Prevention Systems

IPv4
A version of the internet protocol that supports a 32-bit address space. IPv4 is sometimes referred to simply as IP

IPv6
A version of the internet protocol that supports a 128-bit address space

ISDN
Integrated Services Digital Network

ISP
Internet service provider

J

Jitter
SymmetricDS by Jump Mind
Jump Mind is for Cruise market, allows for expected WAN outages for hours at a time when out to sea

K

Kbps
Kilobits per second

KDS
Kitchen Display Systems

L

LAN
Local area network

LAN Topology
Topology refers to the shape of a local area network (LAN) or other communications system

Layer
The network layer is a portion of online communications that allows for the connection and transfer of data

Latency
Delays in processing network data

Leased Line
A leased line is a private telecommunications circuit between two or more locations provided according to a commercial contract

Load Balancing
Load balancing refers to the process of distributing a set of tasks over a set of resources

M

MAC Address
A unique address that is assigned to a network interface. The MAC address is used for communication on the physical network segment

Managed Switch
A managed switch allows user input configuration

Mbps
Megabytes per second

Mesh
A mesh network is a network topology in which the infrastructure nodes connect directly, dynamically, and non-hierarchically to as many other nodes as possible

Mesh – Full
Full mesh topology occurs when every node has a circuit connecting it to every other node in a network

Mesh – Partial
Partial mesh topology includes only some nodes with multiple connections

MoCA
Multimedia over Coax Alliance

Modem
Device used for communication between the digital data of a computer and the analogue signal of a telephone line

N

NAT
Network Address Translation
The translation of an IP address used within one network to a different IP address known within another network

NetBIOS
NetBIOS is an acronym for Network Basic Input - Output System

Netmask
A 32-bit (bit mask) that shows how an address is to be divided into network, subnet, and host parts

Network Switch
A network switch is networking hardware that connects devices on a computer network by using packet switching to receive and forward data to the destination device

Nginx
Web server that can be used as a reverse proxy, load balancer, mail proxy and HTTP cache

NGINX Plus
NGINX Plus is a software load balancer, web server, and content cache built on top of open source

NIC
Network Interface Card

Node
A node is either a redistribution point or a communication endpoint

NTP servers
The Network Time Protocol is a networking protocol for clock synchronization between computer systems

O

OSCP
Online Certificate Status Protocol

OSI model
These firewalls work at the network layer in the OSI model and are more secure than basic packet filtering firewalls

OSCP

Online Certificate Status Protocol

P

PAC scripts
A Proxy Auto-Configuration file is a JavaScript function that determines whether web browser requests HTTP, HTTPS, and FTP go directly to the destination or are forwarded to a web proxy server

Packet
A group of information that is transmitted as a unit over communication lines. Contains a MAC header and a payload, and possibly also contain an IP header

Payload
The data that is carried in a packet. The payload does not include the header information that is required to get the packet to its destination

PMC
Property Management Console
PMS
Property management system

POE
Power over Ethernet

P2P
Peer to Peer

Point to point
Point to Point topology is a topology that connects two nodes directly together

POS
Point of Sale

Power Conditioner
Device intended to monitor and improve the quality of the power

Powerline Extender
Powerline extenders are network adapters that use existing electrical cabling for the transmission of network communication

Proxy Server
A proxy server acts as a gateway between you and the internet

PSK
Pre-shared key

Q

QoS
Quality of Service

QSR
Quick Service Restaurant

R

R&A
Report and Analytics

Redundancy
Network redundancy involves adding additional instances of network devices and lines of communication to help ensure network availability

REST
Representational State Transfer

RFI
Radio Frequency Interference

RFID reader
Radio-frequency identification reader

Ring
A ring network is a network topology in which each node connects to exactly two other nodes

RJ12
RJ12 is a 6P6C wiring standard

RJ45
RJ45 is a type of cable used for Ethernet networking

RJ-45 Connector
A connector for termination of Ethernet cable

Roaming
Roaming occurs when a device moves between the access points

Round Robin
Algorithm employed by process and network schedulers in computing

Router
A router is a networking device that functions as a gateway to forward data packets between computer networks

S

SC Connector
A fiber-optic cable connector that uses a push-pull latching mechanism

SDH
Synchronous Digital Hierarchy is a standard technology for synchronous data transmission on optical media

SD-WAN
Software-Defined WAN

Segment
A network segment is a portion of a computer network

Shielded
Shielded cables are manufactured with the intention of reducing any external magnetic interference. These Ethernet cables may come with a drain cable which provides a mechanism for grounding the cable

Smart Switch
Smart switches offer network performance improving features and greater control over data transmission

SNMP
Simple Network Management Protocol

SOAP
Simple Object Access Protocol

SONET
Synchronous Optical Network

SPI
Stateful Packet Inspection

SSID
Service Set Identifier

SSL
Secure Socket Layer

SSL Server
Protocol for web browsers and servers that allows for the authentication

Star
A star network is an implementation of a spoke–hub distribution paradigm in computer networks

STP
Spanning Tree Protocol

Subnet Mask
IP address provides two pieces of information for a host (computer): Network ID and Host ID. The Subnet mask is used to distinguish theses portions so that at data packet is routed to a specific host on the correct network

SymmetricDS
SymmetricDS is open-source software for database and file synchronization

T

T-1
A leased-line connection (North America) capable of carrying data at 1,544,000 bits-per-second

T-3
A leased-line connection (North America) capable of carrying data at 44.736,000 bits-per-second

TCP
Transmission Control Protocol

Termination
Cable Termination is a connection of the wire or fiber to a device

Throughput
Refers to the amount of material or items passing through a system or process

TKIP
Temporal Key Integrity Protocol

TLS
Transport Layer Security

Token Ring
Token Ring is a computer networking technology used to build local area networks

Topology
Layout or design of a computer network

Tree
A tree network, or star-bus network, is a hybrid network topology in which star networks are interconnected via bus networks. Tree networks are hierarchical, and each node can have an arbitrary number of child nodes

TSR
Table Service Restaurant

Twisted Pair
Type of wiring in which two conductors are twisted together to provide shielding from electromagnetic interference

U

UDP
User Datagram Protocol

Unmanaged Switch
Network Switch that does not allow user configuration input

Uplink
A communications link to a satellite or a device

UPS
Uninterruptible Power Supply

Device used to supply backup power

URL
Uniform Resource Locator

V

VLAN
A virtual LAN is a broadcast domain that is partitioned and isolated in a computer network at the data link

VOIP
Voice over IP

VPLS
Virtual Private LAN Service

VPN
Virtual Private Network
A single, secure, logical network that uses tunnels across a public network such as the Internet

W

WAN
Wide Area Network

WAP
Wireless Application Protocol

WEP
Wired Equivalent Privacy

Wi-Fi
Wireless Fidelity

Windows CAL
Client Access License

WLAN
Wireless Local Area Network

WPA
Wi-Fi Protected Access

X

X-Forwarded Headers
X-Forwarded Headers is a standard header is used for identification of the originating IP address of a client connecting to a web server through an HTTP proxy or a load balancer

X-Forwarded Host
X-Forwarded Proto is a standard header is used for identification of HTTP or HTTPS protocol

X-Forwarded Proto
X-Forwarded Host is a standard header used for identification of original host requested by the client in the Host HTTP request header